Testing the Harmonised Digital Forensic Investigation Process Model using an Android Mobile Phone

Stacey Omeleze[1] and H. S. Venter[2]

ICSA Research Group
Computer Science Department
University of Pretoria
Lynnwood Road, Pretoria, South Africa
[1] staceyaomeleze@gmail.com
[2] hventer@cs.up.ac.za

***Abstract*—Mobile forensics is a branch of digital forensics relating to the recovery of digital evidence from mobile devices under forensically sound conditions. Mobile forensics is considered to be at an infant stage with different investigation process models being applied. The biggest challenge in many of the available digital forensic investigation process models lies in their lack of testing before being fully applied to mobile forensics. Furthermore, for any proposed digital forensic investigation process model to be approved by the scientific community, it has to be tested. The Harmonised Digital Forensic Investigation (HDFI) process model is currently in the working draft stage towards becoming an international standard for digital forensic investigations (ISO/IEC 27043), thus the need for its testing. In this paper, the (HDFI) process model is tested using an Android mobile phone. The selection of an Android mobile phone is motivated by the fact that Android mobile phones have the greatest share of the mobile market index. In the last three years, for example, the market share index for mobile phones put Android mobile devices at 75% of the entire smartphone market. Through observing the findings of the test using an Android mobile phone, this paper demonstrates that conducting mobile forensics using the HDFI process model produces satisfactory results.**

Keywords*—Mobile forensics, Android mobile phone, harmonised digital forensic investigation process model, (ISO/IEC 27043), mobile forensic framework, digital forensics investigation procedure.

I. INTRODUCTION

Mobile forensics is a branch of digital forensics relating to the recovery of digital evidence from mobile devices in a forensically sound manner that will stand up to any formal judicial enquiry [1][5]. Digital forensic science is a rapidly evolving discipline, which applies a variety of scientific principles to enhance digital evidence and data recovery [15]. The computing techniques used today are flexible and scalable with an increased capacity in response time. These capabilities are geared towards an increased demand by users for faster processing speed, portability, accessibility and, of course, less expensive devices [4]. Users' demand for more powerful devices is increasing by the day, as the advent of internet availability on portable devices, such as mobile phones, continues to expand [5]. Mobile phones are among the fastest-growing technologies. This growth can be attributed to the way we live our daily lives, engage in business transactions and the increasing uptake of mobile phones by organisations for convenient communication with clients and business partners. This is becoming ever more possible with the uptake of cloud computing. Users have convenient access to software and storage as a service such as iCloud, Dropbox and Google Drive, via their mobile phones [2]. This also implies that users can now keep track of their activities in real time via their mobile phones. However, the number of criminal-related cases involving mobile phones is growing by the day, resulting in a source of potential evidence for digital forensic investigations [5][11]. The testing of the harmonised digital forensic investigation (HDFI) process model is the first attempt to unify the disparities in digital forensic investigations. These tests of the HDFI process model, when successfully approved by the ISO/IEC, will further solidify the digital forensic investigation processes, thereby increasing the credibility of cases investigated, especially for court proceedings. This can be visualised, for example, when a legal counsel decides to re-investigate a case where digital forensic investigation findings were previously disputed. However, when such a process model is applied, the subsequent findings should produce the same result as the original investigation. This can only be achieved when there exists a standardised digital forensic investigation process model that has been tested. The digital forensic investigation of mobile phones is at its infant stage, therefore there is need to test this model in order for it to become an international standard.

This paper, uses an Android mobile phone as a testbed to verify the workability of the HDFI process model with mobile phones. Testing is carried out on a real-world case. In addition, this paper explores the strengths and weakness (if any) of the HDFI process model when applied to mobile phone forensics.

The remainder of this paper is structured as follows: Section II presents background concepts and elaborates on the HDFI process model. Section III briefly describes the methodology applied, while Section IV introduces the case scenario. Section V describes the investigation that was carried

out on the Android mobile phone using the HDFI process model. Section VI discusses some observations and presents some findings. Finally, section VII concludes this paper.

II. BACKGROUND

This background section introduces a description of mobile devices with a more detailed presentation of Android phones, especially focusing on the features that affect mobile forensics. It also gives a brief summary of the harmonised digital investigation process model as presented in the ISO/IEC 27043 [1].

A. Mobile Devices

In recent years, computing has shifted gear to better operating capacities. Businesses have also adopted a faster, easier and wider means of delivering products and services to their clients [3]. This has been accelerated by the availability of smart phones with high capabilities and the processing speed of a personal computer (PC). Mobile phones have a high storage capacity that stores data locally, like on the Subscriber Identity Module (SIM) card, the flash memory, the secure digital (SD) card and the embedded multi media card (eMMC). A SIM card is made up of a processor and electronic erasable programmable read only memory (EEPROM) with an encryption key that stores the subscriber's information and enables secure communication. The EEPROM serves as the internal memory of the device as well as the storage memory. With constant growth in technological development, such as stated by Moore's law [4], every eighteen months a new electronic circuit appears that renders computer technology cheaper. However, the economic impact of mobile phone technology has created the need for phone manufacturers to expand the capacity of these devices, by increasing the storage capacity and operation speed and create more scalable and user friendly interfaces [3][6]. These added features further enhance the use of multimedia messaging services (MMS), emails, photographs, camera and video-embedded functions, amongst other content-rich features, that create the need for larger and faster external flash memory [11]. In order to achieve this, the architecture of mobile phones are built with compactness, mobility and simple functionality in mind [5].

B. Android Mobile Devices

Android mobile phones are a group of phones from different manufacturers with the same operating system (OS). Android is an open-source operating system based on the Linux kernel 2.6 OS. An Open Alliance group was formed to enable the development of software that can enable compatibility and connectivity within the various mobile phone models. The Android mobile platform has risen from its inception in October 2008 to being the most popular mobile operating system today. However, there are slight differences incorporated by the various manufacturers [17][11]. It is a highly competitive smart phone in the market with a 75% market share index [3][6]. Android's success can be attributed to the large community of developers using customised versions of Java programming language with about 700,000 apps in the Google play apps stores by the time of writing this paper. Android application development is based on the Java programming language, using the Android software development kit (SDK), which includes the debugger, libraries, emulator, documentation, sample codes and tutorial. One of the noticeable features of the Android phone, as with other mobile phones, is the touch screen. Other features include the low cost, customisable, lightweight OS that is not built from scratch, but rather fine-tuned. Furthermore, Android supports the popular Eclipse integrated development environment (IDE) using the Android development tools (ADT) plugin [11].

In terms of mobile forensics, the use of Linux OS in Android phones serves as a noticeable advantage. In conducting forensic investigations, the investigator can apply the Linux OS commands such as dd, as applicable to a desktop computer with a Linux OS installed [11], when the device is rooted. But its security features make forensic investigation more difficult. For its security, Android mobile phones make use of a sandbox mode [11]. The sandbox houses the user's applications and also serves as a security mechanism to protect the user from unauthorised access of the system applications. This increases the access control of the device and makes forensic investigation more difficult if the device is turned off and requires the user's password. An application installed without the user's permission cannot access resources outside the sandbox. This can be an issue, thereby generating the need to apply extreme forensics. A need for extreme forensics can occur during data acquisition, when all techniques for data acquisition such as logical, physical and chip-off is applied during an investigation process without getting sufficient information [17][11]. In forensic extraction, where physical and logical acquisition is not yielding the required result, there may be need to install software on the mobile device (with authorization) for further evidence extraction [17].

C. Android Data Acquisition Techniques

There are two types of data acquisition techniques in mobile phone forensic investigations; the logical and the physical data acquisition.

I The logical Acquisition: This is the extraction of data in the logical file allocation storage area of the mobile phone. In Android, the following options are applied in extraction. i) Android debugs bridge (ADB) pull. ii) Backup analysis. iii) The AFLogical [21]. There are several logical data extraction software packages provided by the major forensic kit vendors such as MicroSystematics XRY, EnCaseNeutrino, FTK, Cellebrite universal forensic extraction devices (UFED) and Paraben Device Seizure [21]. However, the logical extraction of Android mobile phones can be done as discussed below:

- i ADB Pull command: The ADB Pull command Is used for copying some of the files such as the unencrypted applications and browse history, from the device to a forensically ready computer system for further analysis via the command shell of the android phone, because in most Android devices, root access is not available [11][20][21].
- ii Backup analysis: Backup analysis is used to examine the data in the cloud. This is useful in a case where the device's entire data is backed up using the back up apps. This option provides the knowledge that some

data are backed up in the cloud with the name of the type of cloud in use.

iii AFLogical Application: AFLogical is an application by one of the leading digital forensic developers - viaForensic. It extracts using content provider, and is able to access the user's contacts, calendar, social media, SMS/MMS and email accounts[11][21][18].

II Physical Acquisition: This is a method of acquiring images such as deleted data or lost data for data recovery. In Android mobile phones, there are several techniques generally applied for physical extraction as listed below.

i Joint test action group (JTAG) is the hardware component used with the wiring and testing device (part of the mobile forensic tool kit). It is connected to the central processing unit (CPU) of the mobile phone, to enable extraction directly from the phone chips.

ii Chip-off is a process of completely removing the needed chip off the phone's mother board. Chip-off is only employed in exceptional cases because the organisational policy must be consulted or a court order granted. Chip-off requires this higher clearance with the chain of custody dually signed to perform this physical extraction. Chip-off is done by physically removing the NAND logic gate (which is a combination of AND and NOT logic gate) flash chip and read the NAND memory with the NAND reader (NAND reader is part of the forensic tool kit) [20] for further data analysis.

iii The AFPhysical is one of the viaForensic software techniques [9] used for physical acquisition. The program acquires root privilege from the device, finds the NAND flash drive partition and images it and then uploads the binaries of the target device. Once the root privilege is acquired on a device, every other acquisition method can be applied [11][20] [21]. Acquiring root privilege in Android devices is quite a task, but possible.

D. Digital Forensics Process Model

A process model is a defined standard or method of getting things done by applying scientific methods [10]. However, in digital forensic science, which is a relatively new discipline in forensic science that deals with digital evidence involving digital devices, investigations are focused on devices that hold data electronically like mobile phones, computers, cameras, gaming sand box, flash memory and storage devices [15] [17][18].

At the time of this compilation, testing on various devices is in progress to verify the applicability of the HDFI process model to these digital devices. These tests include, the dead and live forensic of computer systems, network forensics, servers, various mobile phones, washing machines and virtual machines. These tests are being carried out to further validate the HDFI process model as a standard for digital forensics investigation. This paper focuses on testing the harmonised digital forensic investigation process model with mobile phones, with an emphasis on the Android mobile phone.

E. Harmonised Digital Forensics Investigation (HDFI) Process Model

The harmonised digital forensic investigation (HDFI) process model is a generic model in the process of standardisation by the International Standard Organisation ISO/IEC 27043 [1]. It comprises much of the various previous models by absorbing most of the phases in their frameworks [18]. Most significantly in the HDFI process model, there is the introduction of some parallel actions as part of the HDFI process model which are carried out concurrently with the investigation process [18]. These concurrent processes are the activities that usually occur in forensic investigations and contributes immensely to the entire investigation. These parallel actions include information flow, documentation, obtaining authorisation, preservation of chain of custody and evidence preservation. The concurrent processes, harness the integrity of findings and adheres to the preservation of the chain of custody in dealing with evidence, at every level of the investigation.

The investigation processes in the HDFI process model is briefly discussed below, while a more detailed description of the HDFI process model can be found in Alexander and Venter [18][1].

i Incident Detection Process: This is one of the initialisation process class of the HDFI process model. This occurs when an incident is discovered, and investigation is initiated for findings [1]. The incident detection mechanism could be in the form of intrusion detection in a network, log-analysis and human findings.

ii First Response Process: This is also an initialisation process class of the HDFI process model. It deals with the first awareness of an incident, acknowledging the incident and starting the process by involving the stakeholders. This can be achieved by a system or an individual and involves further reporting to the system administrator or the stakeholders or investigator.

iii Planning Process: This process is the planning of the needed techniques, human resources and tools to carry out a investigation successfully. The incident detection and the first response phases are the impetus to begin the planning process.

iv Preparation Process: This involves the preparing of all the necessary equipment, tools, resources and training needed to perform a digital forensic investigation process.

v Incident Scene Documentation Process: This is a process that occurs at the incident scene location. In the harmonised digital forensic investigation process model, the incident scene documentation is important as some cases are escalated from one investigator to another as the investigation proceeds. This is because the first respondent in most cases is not always the investigator of a case, therefore the documentation of the scene of the incident should be clear and precise to promote easy hand-over, maintain chain of custody, evidence preservation and continuity in an investigation process. Proper documentation should involve the clear labelling of the evidence, photographs and video coverage recording of the scene, taking every scene at it appear on first contact. This is to effectively preserve the chain of custody as the investigation continues.

vi Potential Digital Evidence Identification Process: The evidence in the case for investigation is properly identified,

and labeled distinctively with name and non-identical serial number attached to every item identified at the scene. This is for easy identification and recognition, especially when there is more than one device found at the scene.

vii Digital Evidence Collection Process: This applies after the identification of the evidence, when collection is necessary for further analysis. During collection the integrity of the evidence must be preserved to enable making a formal conclusion later. The evidence collection procedures, applicable to a device such as a mobile phone, may be different from other branches of forensics like network forensics, live forensics or dead forensics.

viii Digital Evidence Transportation Process: This involves the movement of the evidence from one location to another for the purpose of further analysis. The transportation method chosen must adhere to the preservation of the chain of custody taking into account the volatile nature of the data and device in question.

ix Digital Evidence Storage Process: The storage occurs when the potential evidence cannot be analysed immediately. While being stored, the preservation of the integrity of the evidence as well as the chain of custody must be observed.

x Digital Evidence Analysis Process: The evidence analysis is one the investigative processes in the process class of the harmonised digital forensic investigation process model, where the hypothesis of the case under investigation is identified. There are several techniques that can be applied for evidence analysis, but these techniques must be forensically sound. An attempt is made to set the scene, by re-constructing the scene and implement a mechanism to solve the puzzle of the case. Since evidence analysis holds a great importance to the investigation, it must be accorded due diligence. The need for fairness and professionalism must be observed.

xi Digital Evidence Interpretation Process: The analysed digital evidence needs to be interpreted based on the information accumulated in the case under investigation. The interpretation of digital evidence is essential to enable the investigator sort the importance pieces of evidence in a hierarchical form. The most important piece of evidence is analysed at the beginning and the least significant at the end. This separation is necessary in drawing up a conclusion to the findings. However, in all case, there is the need to apply scientifically proved methods during interpretation of analysed evidence.

xii Report Writing Process: Reporting the investigation findings can be in the form of an expert witness's testimony, presentation and interpretation to the stakeholders for further hypothesis development, or as an input to another inquiry. Reports should list all evidence examined in the order of importance to the processed case. Furthermore, the reporting language must be clear and understandable to all stakeholders involved which can something include, the jury, the accused and the legal counsel. The report should be preserved for a reasonable amount of time for future reference and decision making.

xiii Presentation Process: The presentation of digital forensic findings may be in the form of a multimedia presentation, documented account or expert witness's testimony. It should be simple, precise and communicate the message effectively. The presentation of evidence found during an investigation, must include the photograph of the scene, the timestamp and date of the incident and should be presented with all the stakeholders present. According to Cohen[17], the evidence presentation process is one of the most significant sub process of the digital forensic investigation. This is so, because the use of language by the investigator or the presenter, may determine the admissibility of the evidence in court. Cohen further states that there is the need to identify experts' opinion/testimony and what the forensic evidence portray. The expert's testimony is crucial as well as the presentation technique [17].

xiv Investigation Conclusion Process: The investigation closes after the presentation. However, a decision should be made as regards the evidence storage. The interactive nature of the HDFI process model allows the investigator to re-visit the sub processes of the of the HDFI process model for further examination, especially when there is need for a new input, that could further enhance the case even at case closure when there is need to challenge the hypothesis applied to validate/back-up the findings. The decision as to what to do with the evidence is made and the case closed.

III. METHODOLOGY APPLIED

The testing of the HDFI process model was conducted with commercial mobile forensics software of the Micro Systemation (MSAB) XRY V6.5 Mobile Forensic tool kit [12] at the digital forensic laboratory of Risk Diversion Pty Ltd., in the Computer Science Department, University of Pretoria, South Africa. Those involved in the testing of the HDFI process model applied the steps in the order described above. The scenario employed in this testing of the HDFI process model constitutes a real case. However, due to the confidentiality agreement in place between the researcher and Risk Diversion, the scenario described in this paper has some details of the case withheld or rendered anonymous. It concentrates on the application of the HDFI process model to mobile devices using an Android mobile device as our case study.

IV. CASE SCENARIO

The case that this paper examined is the suspicion of a phishing attack using scareware, targeted at bank X customers via short message services (SMS). A scareware is a form of malicious software (malware) developed with the intention to scare the user and lure them to a phishing website for subsequent attacks. A phishing attack is a malware used to get details of individuals or organisations for further security exploitation and subsequent attacks [7]. The mobile device with the SMS scare ware is a Samsung mobile Galaxy S2 phone belonging to the customer X of bank X. The suspect/attacker distributes scareware to bank X clients via a SMS.

The suspect/attacker sent scareware SMSs to the clients, mimicking Bank X by requesting the clients to click on the sent link to update their account details or else lose their database with the bank. The unsuspecting Bank X customer clicked on the link and eventually fell victim to a phishing attack. The suspect further performed an unauthorised transaction on the customer's bank account as a result of the bank X customer details collected. A transaction's alert received by the bank's customer that he/she never initiated raised the customer's suspicion, the customer then reported the incident to bank X.

V. TESTING THE HARMONISED DIGITAL FORENSICS INVESTIGATION PROCESS MODEL

The investigators applied the HDFI process model throughout the investigation. The HDFI process model is tested using the Android mobile phone by applying the HDFI process model step by step as listed above. This paper uses the term nvestigatoro imply the digital forensic investigator involved in conducting the investigation of this case study at each sub process of the HDFI process model. The investigators observed the chain of custody, with proper documentation in all the HDFI sub processes and these are each discussed in detail in the sections to follow.

A. Incident Detection Process

In applying the incident detection process on the case presented, the bank X customer detected the incident when s/he received the SMS. The customer reported the subsequent debit transaction that occurred in her/his account to the bank X manager since the transaction never originated from the customer. The customer also noted that this unauthorised transaction occurred after the update of the account details as requested by the suspect, who is mimicking the bank. The customer X also reported the incident of the scareware.

B. First Response Process

The first responder of this case is the bank X manager. This occurred when the customer reported the scareware incident to the bank. The bank manager subsequently secured and preserved the evidence, that is, the mobile device with the scareware messages as received by the customer for further forensic analysis. The bank manger applied the flow of information by reporting the incident to the authorities.

C. Planning Process

In planning the investigation of this incident, the investigator employed a parallel action by getting authorization from the mobile network provider, to obtain the mobile phone activity history of customer X. The investigator documented all that was necessary in planning for all the needed equipment to achieve the goal of retracing the SMS. The mobile network provider had to be contacted to assist in the location of the sender of the SMS as well.

D. Preparation Process

In the preparation process, the needed equipment was, the XRY complete toolkit for mobile device examinations, a XRY license key USB stick, a write blocker, a forensically cleaned USB drive, a Dell Desktop PC with Windows OS 8, a SIM adapter, a forensically cleaned hard drive and empty DVD [12]. Authorization was obtained for the call and SMS logs as well as the data bundle history from the mobile service provider. This assisted the examination of the evidence collected during analysis by comparing the details of the SMS received (from the suspect), the suspect's phishing website details and the mobile activity history to be used in the analysis process following later.

E. Incident Scene Documentation

The investigator provided the documentation from interviewing the first respondent and photographed the evidence with the timestamp, type and size of the device, at the incident scene detection. This preserved the evidence and chain of custody [17].

F. Potential Digital Evidence Identification Process

The investigator that responded to the incident first, identified the potential evidence as the mobile phone. The investigator handed in the device to the laboratory with the documentation of the identified evidence after the collection and transportation. At the laboratory, the receiving investigator identified the mobile phone as the crucial evidence, specifying and documenting the serial number (MER7823e83), device name (Samsung) and device model (S2). The device was then photographed and documented. The mobile phone were booked by signing a custody release and received form.

G. Digital Evidence Collection Process

In some cases the evidence collection process requires the logical and physical form of data extraction, but in this case the logical data extraction technique produced the necessary evidence. The SMS, call and browser history contained the evidence which was located in the storage compartments of the mobile phone. The evidence was collected using a commercial product that is used for mobile forensic data extraction. After extraction, a search was made through the entire data extracted using the provided keywords. The information deduced was compared to the browser history; call log, and time stamp with the call log and SMS history provided by the mobile phone network service provider. The investigating officer documented the process that s/he applied, which were in line with a forensically sound collection process. A forensically sound data collection refers to the action when all necessary caution is applied to preserve the potential evidence, including the preservation of its integrity. The mobile phone was sealed in a faraday bag. A faraday bag is an interference-blocking container that can eliminate any possible interference from the mobile phone network service provider and it also protects the mobile phone from remote accessing or wiping.

H. Digital Evidence Transportation Process

The investigator transported the evidence to the laboratory in a forensically sound condition, preserving the integrity of the evidence. The investigator preserved the evidence integrity of the mobile device by turning off the phone and placing it in a faraday bag for transportation to the laboratory.

I. Digital Evidence Storage Process

Evidence can be stored when analysis may not occur immediately after transportation to the laboratory location. However, mobile phones are volatile and need analysis as quickly as possible [21]. However, in this case study, the potential evidence was not stored, rather the analysis of the evidence commenced immediately, since all the needed equipment were already in place and authorization had been granted. This case study was accorded high priority as it involved bank customers, bank's integrity and finance.

J. Digital Evidence Analysis Process

In the analysis of the android mobile phone, the logical extraction technique is applied. The choice of logical extraction was made based on the location of evidence required for the investigation, that is, the SMS, call logs and calendar events on the device. The extraction of the information was done in three different stages. Firstly, with the phone still turned off, it is then connected to the PC via the XRY USB cable. This is a special USB cable in the XRY tool kit that is specifically designed for logical extraction. In the XRY tool kit, there is a USB cable for most mobile devices available today. It allows for the extraction of data from the mobile phone's various storage locations and then place the. In this investigation the extracted data is stored on a forensically cleaned hard drive and a 'forensic master' copy is made. The forensic master copy was then kept aside and a mirror of the master copy is used as the working copy for the analysis. A cryptographic hash message digest (MD5) was used to further preserve data integrity and consistency with the original evidence. The copies made are used so that the original evidence is handled as little as possible in order to minimise the risk of contaminating the original evidence.

However, not all the required data is extracted while the device is turned off, therefore, a second search was made on each of the storage locations of the mobile phone, namely the SIM, eMMC, and the SD card, when the device was turned on. To achieve this, the SIM card was removed, and then cloned with a 'dummy' SIM card. The cloned SIM is used when the device is turned on. This is done such that the cloned SIM mimics the original network service provider's SIM, the difference being the inability of the cloned SIM to receive network communication from the mobile network provider, there by disallowing any communication in or out from the mobile phone to the network service provider. This is to further preserve the evidence integrity.

Finally, the third extraction was made with the aid of the eMMC card reader, which is part of the XRY tool kit. The eMMC card reader was attached to the PC and this extraction was made from the eMMC(flash memory card) while separated from the mobile phone.

K. Digital Evidence Interpretation Process

The analysed digital evidence needs to be interpreted based on the information accumulated for the case under investigation. In this particular case the information extracted from the various locations was further separated by sorting and selecting the necessary information, such as the SMS, URL browser details of the Samsung S2 mobile phone around the time the scare ware was send until after the unauthorised bank transaction took place. The interpretation of the digital evidence is essential to enable the investigator to sort the importance of evidence in a hierarchical form by placing the most important piece of evidence at the top and the least significant at the lower position. The SMS used by the Attackers to lure the bank customers to their phishing website, was therefore, placed in the top position in the hierarchy of evidence alongside the activity on the phishing website. The extracted evidence was interpreted with the aid of timestamp, the SMS tracker agent and the GPS location view. The SMS tracker is an external software tool used to track SMSs back to its origin. In this investigation, this option was applied with authorisation. The URL included in the SMS by the attacker, also pointing to the phishing websites, helped narrow down the search in apprehending the attackers. It was this evidence interpretation sub process that led to drawing up a conclusion to the findings.

L. Report Writing Process

Reporting is the process of providing a detailed summary of all the steps taken to reach a conclusion of the case investigated. In the reporting, the detailed processes applied during the investigation are explained in simple language, that is understood by all the stakeholders. The stakeholders in this case, are the physical investigation team, the bank officers, the bank client and the legal parties. The first documentation was received from the incident detection sub process with the attached photographs taken at the incident scene. Processes that enhance the authenticity of the investigation such as the evidence handling forms, stating who did what, and how it was done at each stage of the investigation were also included in the report of the findings. The results of the XRY mobile forensics tool kit used was documented and reported and how the extracted potential evidence was sorted using the keywords. Finally, the investigation team presented all this documented evidence collected from the mobile device to the stakeholders. This included the data attributed to the device as obtained from the mobile phone's network service provider and the data obtained from the device, during the evidence sorting.

M. Presentation Process

The investigator presented the sorted evidence, in the order of priority and relevance to the case, along with the written report, to the stakeholders. This presentation is also based on the report given in the reporting sub process above. This written presentation was simple and understandable to the stakeholders. This investigation attempted to identify the case of scareware to bank X customers. The information retrieved was details of call history with calls made, received and missed, and SMSs received, sent and deleted. Addresses on the phone contact list and the mobile phone's own number was also found.

The interpretation of the URL and the location of the GPS of the mobile device of the receiver (Customer X) from the sender (the Attacker) further assisted the investigation in finding the location of the perpetrator of the act of spamming the bank X customers and identified the location of the Attacker. The history of the internet browser of the attacker revealed several attempts to access several bank account details belonging to random victims that had received SMSs from the suspect.

At the analysis of the information found in the mobile phone listed above, it was found to be consistent with a scareware sent via SMS to the customer of bank X who had reported the unauthorised transaction in his/her account [7].

N. Investigation Conclusion Process

The conclusion process occurred after the presentation of the findings to the stakeholders. The mobile phone was

returned to the customer of bank X. The evidence and information found by the investigators, was sufficient for the investigation team to prosecute the scareware suspects and remand them in custody.

O. The Concurrent Processes

The concurrent processes are the processes of activities that are applied throughout the investigation process such as, obtaining authorization which occurred in order to get the mobile network to provide the phone details and history of the suspect. Documentation is also an essential aspect of the concurrent processes, and this was done from the first response to the case closure. The documentation of the processes of investigation is necessary to preserve information flow. The chain of custody was observed during the sign-off, or at the returning of the evidence, which was the mobile device. There was constant interaction among the investigators for updates on the case.

VI. FINDINGS AND OBSERVATIONS

In the HDFI process model, the potential evidence identification and potential evidence collection can be in the physical or logical form. The potential evidence identification and collection phase of this investigation was achieved in the logical form. This is because all the evidence needed in a mobile device is stored within the mobile device's storage units such as the SD card, SIM card and the phone's hardware memory [18]. However, in the application of the HDFI process model to mobile forensics, the identification of evidence is not physically visible but rather the logical accessing of the device to identify potential evidence [5]. One of the observations of this paper concerns the transportation mechanism of the evidence. The movement of a mobile phone from incident scene to a location for further analysis is a crucial aspect of the investigation, and if not handled with optimum care, may render the entire investigation invalid. However, in the test carried out, the transportation of the potential evidence was done in a forensically sound condition.

This paper finds the incident scene documentation as a very important phase of the harmonised digital forensics investigation process model for all devices, especially for mobile devices where more than one investigator are involved [19]. During this investigation, there was need to hand over the investigation to another investigator. With a well documented chain of custody and hand over notes, written in clear and understandable language for easy continuity, the HDFI process model is a model that has adequately accommodated the investigation of an Android mobile phone. However, as earlier stated, there are various versions of Android devices and the Mobile industry is experiencing great economic growth therefore, changes that may occur in future is not accommodated in this test, rather the current state of the device used, is implemented[3][6].

During this investigation, one of the findings made is that each sub process of the HDFI process model are inputs to the other sub processes. However, for each sub process to link successfully to the next sub process, requires the full application of the concurrent activities. These are the aspects of the HDFI process model, that further harness the inclusion of mobile phones in the model and also the integrity of the investigations. The most critical element of these concurrent activities is the documentation process, which forms the coherency between all the sub processes. Good documentation which is passed on from one stage to the next is essential in maintaining information flow and ensuring that the chain of custody is adequately observed. Otherwise there is the danger of potential evidence contamination. Mobile phones are volatile and a change in content information by an intruder may not be quickly noticed. However, with the chain of custody, evidence preservation and the sign-off on every document at every level of the investigation implemented, this activity is deterred. In this testing, the documentation was handled with utmost caution and information flow was adhered to. In mobile forensic investigations, a break in information flow, documentation, evidence handling or chain of custody can render a case inconclusive or invalid when presented to stakeholders.

Another positive strength of the HDFI process model is the ability of the investigation process to continue at any sub process, since there is adequate documentation at all sub processes. In this investigation, the use of documentation was observed from the first responder to the closure of the case. The poor information delivered by customer X to bank X staff, proved a little tedious to process. However, with the mobile device that received the SMS available and the message intact, along with the documentation of the mobile phone activity as presented by the mobile network service provider to the investigators, this challenge was overcome.

While the HDFI process model does work well for an Android phone, there is one potential difficulty, in that it needs the total co-operation and understanding between the different personnel involved in the investigation. In most cases the investigating team is comprised of different professionals with varying roles and expertise. For example, in this case study the first responder was a bank manager, who passed the investigation over to a law enforcement agent, who in turn passed it over to an IT professional who conducted the test. The IT professional then documented and presented the findings to the various stakeholders. Because of all the various personnel involved there is the potential for the investigation to breakdown in the handover between them. It is due this potential flaw, that this paper has continually emphasised the importance of proper documentation that is easily understood by professionals from different fields. With proper documentation at all sub processes in the HDFI process model, this potential flaw can be prevented from being actualised.

The testing of the HDFI process model was carried out using an android mobile phone following the described processes above, and in the opinion of this paper, the investigation shows that the HDFI process model successfully incorporated an Android mobile phone with no major difficulty. This paper, therefore, claims that the HDFI process model accommodates the investigation of Android devices, and therefore mobile devices in general, effectively, as long as the concurrent processes are strictly implemented from the beginning of an investigation to its conclusion.

VII. CONCLUSION AND FUTURE WORK

The HDFI process model adequately accommodated the Android mobile phone in this testing, however, there is need to adhere to the concurrent processes such as documentation, preservation of chain of custody, preservation of evidence and obtaining authorization. As with any organisational policy, the overall policy is usually at a high level, thereby allowing the use of procedures and standards to interpret them in more descriptive forms[8]. There is a need for further in-depth analysis of each sub processes of the HDFI process model with a detailed procedure of how a sub-process can be applied to accomplish a digital forensics investigative task. This description can be in the form of procedures or standards with detailed processes generated from the HDFI process model. For further study therefore, there is need to evaluate each of the sub processes to come up with a standardised step by step procedure that can be applied in various fields of digital forensic science.

ACKNOWLEDGMENT

The authors wish to thank the digital forensics team of Risk Diversion Pty (LTD) for the collaboration with the ICSA research group at the University of Pretoria. Furthermore, we would like to thank them for allowing the use of their equipment during the testing scenarios of the HDFI process model with various devices as mentioned above, and in particular giving us full access to the Macro systematic XRY mobile forensics toolkit during the Android mobile phone testing.

REFERENCES

[1] *http://www.iso27001security.com/html/27043.html* ISO/IEC 27034 Information technology Security techniques Application security (part 1 published, rest in DRAFT)

[2] Brian J.S. Che, Curtis Franklin, Jr.(2010) *Cloud Computing Technologies and Strategies of the Ubiquitous Data Center* Publication: CRC Press Taylor Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742. International Standard Book Number: 978-1-4398-0612-8

[3] Jenny C. A, Isaac M. M (2007) *Mobile Phones and Economic Development in Africa Journal of Economic Perspectives* businessinnovation.berkeley.edu/Mobile_Impact/Aker-Mbiti_mobile$_p h$

[4] Gordon E. Moore(1965) *Cramming more components onto integrated circuits with unit cost falling as the number of components per circuit rises, by 1975 economics may dictate squeezing as many as 65,000 components on a single silicon chip* Electronics, Volume 38, Number 8, April 19, 1965

[5] Andrew Hoog, Katie Strzempka(2011) *iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices* Syngress ISBN: 978-1-59749-659-9

[6] What is the Impact of Mobile Telephony on Economic Growth - a Report for the GSM Association

[7] Michael Sikorski, Andrew Honig(2012) *PRACTICAL MALWARE ANALYSIS - The Hands-On Guide to Dissecting Malicious Software* William Pollock , ISBN-10: 1-59327-290-1, ISBN-13: 978-1-59327-290-6 San Francisco, CA 94103

[8] Michael E.W, Herbert J.M (2009) *Management of Information Security 3rd edition* Course Technology, Boston, M 02210, USA. ISBN-13: 978-0-8400-3160-0, 10: 0-8400-3160-2

[9] Wayne Jansen, Rick Ayers(May 2007) *Guidelines on Cell Phone Forensics* Recommendations of the National Institute of Standards and Technology NIST Special Publication 800-101, National Institute of Standards and Technology - Computer Security Division Information Technology Laboratory, U.S. Department of Commerce, May 2007

[10] Bunge, Mario Augusto (1998) *Philosophy of science (Science and Technology Studies)) publisher: Springer-Verlag. ISBN 0-7658-0415-8 (set: pbk. : alk. paper).-ISBN 0-7658-0413-1* Fifth printing 2009 Rev. ed. of: Scientific research. Berlin, New York:

[11] Andrew Hoog(2011) *Android Forensics Investigation, Analysis, and Mobile Security for Google Android* published by Syngress is an imprint of Elsevier 225 Wyman Street, Waltham, MA 02451, USA ISBN: 978-1-59749-651-3

[12] Micro Systemation (MSAB) XRY emph http://www.msab.com

[13] Derrick G. Kourie, Bruce W. Watson (2012) *T*he Correctness-by-Construction Approach to Programming Springer Heidelberg Dordrecht London New York, Springer-Verlag Berlin Heidelberg, 2012

[14] Clements, Paul Felix Bachmann, Len Bass, David Garlan, James Ivers, Reed Little, Paulo Merson, Robert Nord, Judith Stafford (2010). *Documenting Software Architectures: Views and Beyond, Second Edition*. Boston: Addison-Wesley, 2010

[15] Marwan AlZarouni (2006) *A Mobile Handset Forensic Evidence: a Challenge for Law enforcement* Australian Digital Forensic Conference Security Research Institute Conference, October, 2006

[16] *Google Projects for Android. code.google.com. Google Inc. 2011.*

[17] Dr. Fred Cohen (2009) *Digital Forensic Evidence Examination* Publisher: Fred Cohen and Associates out of Livermore 2009 3rd Edition, ISBN-10: 1878109448 — ISBN-13: 978-1878109446

[18] Aleksandar V, Venter H. S (2012) *Harmonised Digital Forensic Investigation Process Model* IEEE Conference Publications

[19] Karie, N. M, Venter H. S (2013) *Towards a General Ontology for Digital Forensic Disciplines* Journal of Forensic Sciences, 2013(In Press)

[20] Wayne Jansen, Rick Ayers (2007) *Guidelines on Cell Phone Forensics* Recommendations of the National Institute of Standards and Technology-Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology(NIST), Gaithersburg, MD 20899-8930, May, 2007

[21] Salvatore Fiorillo (2009) Information Security Consultant *Theory and practice of flash memory mobile forensics* Australian Digital Forensics Conference Security Research Institute ConferencesEdith Cowan University, 2009