Mobile Forensics using the Harmonised Digital Forensic Investigation Process

Emilio Raymond Mumba
ICSA Research Group
Department of Computer Science,
University of Pretoria,
Private Bag X20, Hatfield 0028,
Pretoria, South Africa
emmy_emiray@yahoo.co.uk

H.S. Venter
ICSA Research Group
Department of Computer Science,
University of Pretoria,
Private Bag X20, Hatfield 0028,
Pretoria, South Africa
hventer@cs.up.ac.za

***Abstract* - Mobile technology is among the fastest developing technologies that have changed the way we live our daily lives. Over the past few years, mobile devices have become the most popular form of communication around the world. However, bundled together with the good and advanced capabilities of the mobile technology, mobile devices can also be used to perform various activities that may be of malicious intent or criminal in nature. This makes mobile devices a valuable source of digital evidence. For this reason, the technological evolution of mobile devices has raised the need to develop standardised investigation process models and procedures within the field of digital forensics. This need further supports the fact that forensic examiners and investigators face challenges when performing data acquisition in a forensically sound manner from mobile devices. This paper, therefore, aims at testing the harmonised digital forensic investigation process through a case study of a mobile forensic investigation. More specifically, an experiment was conducted that aims at testing the performance of the harmonised digital forensic investigation process (HDFIP) as stipulated in the ISO/IEC 27043 draft international standard through the extraction of potential digital evidence from mobile devices.**

Keywords— Harmonised Digital Forensic Investigation Process (HDFIP), mobile device, mobile forensics, ISO/IEC 27043.

I. Introduction

In the opinion of the authors, mobile devices have become the main form of communication around the world, as the world becomes ever more digitally connected. Cyber-crime activities over mobile devices, however, are also increasing steeply [7] as result. This rapid growth and development of mobile devices allows users nowadays to perform tasks similar to those of traditional desktop computers.

The increased processing power, functionality of mobile devices and memory size has enhanced communication among users around the world [20]. This increase of memory capacity has contributed to the disparities faced in mobile forensics. Such disparities faced by investigators include the retrieval of potential digital evidence using predefined investigative processes and procedures from different models of mobile devices [16], [26].

Mobile devices such as smart phones, tablets and personal digital assistants (PDAs) nowadays can store large amounts of information. This information includes documents, videos, music, GPS locations, call logs, Multimedia Messaging Service (MMS) and Short Messaging Service (SMS) messages [24].

In mobile forensics, there is a shortfall of investigative process models that have been tested and verified. Testing is required to verify that a process model meets the standards of the digital forensic realm. The harmonised digital forensic investigation process (HDFIP) is put through a testing process on an endeavour to reduce the disparities currently existing within digital forensic investigations.

A digital forensic investigative process model such as the HDFIP model can be used in criminal cases that involve mobile devices such as the 2014 Oscar Pistorius murder trial [31] and Shrien Dewani murder trial [32] in South Africa.

Current frameworks and techniques exist to retrieve and analyse mobile device data but lack scientific testing. Therefore, the HDFIP is utilised during the extraction of potential digital evidence from a mobile device during an investigation. This study uses a mobile forensic investigation, with the aim of the testing of the harmonised digital forensic investigation process ISO/IEC 27043 [11] to determine whether the process model is suitable for mobile forensic investigations.

The remainder of the paper is structured as follows. Section II provides background on digital forensics and a description of the HDFIP model. Section III presents an overview of a case study for testing the Harmonised Digital Forensic Investigation Process. Section IV presents the testing of the harmonised digital forensic investigation process model. In Section V a performance evaluation of the Harmonised Digital Forensic Investigation Process model is provided**.** Section VI provides related work on digital forensics investigation process models, thereafter, the conclusion is presented in Section VII.

II. Background

This section provides a definition of digital forensics as well as a definition for mobile forensics. In addition, a brief description of mobile device data acquisition techniques used by digital forensic investigators is presented.

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

A. *Digital Forensics*

Digital forensics is defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the sole purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations [8].

Authors use the term ‘forensically sound’ to refer to methods that does not change the data residing on the hard disk which is being duplicated [29]. The following paragraph gives a definition of mobile forensics and the possible sources of potential evidence.

B. *Mobile forensics*

Mobile forensics is defined as the science of recovering potential digital evidence from mobile devices [12] using similar techniques as for digital forensic investigations. Mobile forensics is also considered a branch of digital forensics that deals specifically with mobile devices such as smart phones, tablets, iPad and cellular devices.

A Mobile device consists of several parts, which are known to preserve data. Different models of mobile devices vary on where the data is stored. Data can be stored on (a) a subscriber identity module (SIM) card, (b) an internal memory module, (c) additional modules for services such as GPS location and, (d) memory cards [26]. Memory in mobile devices can be either volatile or non-volatile. Volatile memory requires power to maintain the stored data. Such memory includes random access memory (RAM) [26]. On the other hand, non-volatile memory retains data even when power is turned off.

Mobile forensic investigations are carried out using certain techniques. It is important for the purposes of this paper to provide a brief overview of those techniques.

C. *Mobile device data Acquisition Techniques*

The acquisition of digital data from a mobile device involves the use of two main techniques by forensic tools and unique especially to mobile devices, namely logical acquisition and physical acquisition. Jansen and Ayers [12] define logical acquisition as a bit-by-bit copy of logical storage objects such as directories and files that reside on a logical store. An example of a logical store is a file system partition.

Physical acquisition is defined as a bit-by-bit copy of an entire physical store. An example of a physical store is a memory chip.

In the following section, the author’s present the HDFIP model which comprises of varies processes as proposed by [11], [30].

D. *Harmonised Digital Forensic Investigation Process (ISO/IEC 27043*

The harmonised digital forensic investigation process

model is a generic model in the process of standardisation by the International Standard Organisation ISO/IEC 27043 [1].It consists of five classes namely: the readiness processes, initialisation processes, acquisitive processes, investigation processes and concurrent processes as stipulated in the international draft standard ISO/IEC 27043 [11]. This background provides an overview of the HDFIP and the various classes which are comprised of a number of processes. The sub sections that follow explain in brief the five different classes together with the various processes in each class where applicable.

1) *The readiness class*

Palmer [8] defines digital forensic readiness as the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation. The readiness class is, however, optional to the remainder of the process model as it affects mainly the voluntary partaking of an organization rather than involving any investigator(s) in an investigation. For this reason, this paper does not discuss any further details of the readiness class of the HDFIP model.

2) *The initialisation class*

The initialisation class deals with the initial commencement of the digital investigation. Moreover, the initialisation class is the second class in the HDFIP. During this class, the investigators become physically involved in the investigation. This class comprises of four processes explained in the sub-section to follow.

Incident detection process is the classification of the incident into the different types of digital forensic investigations such as mobile forensic, network forensic, post mortem forensic, and cloud forensic investigations. Within the incident detection process, an incident description provides a written or a spoken account of the event. An incident can be detected through an intrusion detection system in a network, log analysis and human finding.

First response process involves the first steps taken after an incidence is detected. ISO/IEC 27035 [9] and ISO/IEC 27037 [10] provide more information on incident responses.

The *planning process* allows the investigator to perform all possible planning required during the digital investigation process and development of proper procedures, defining of methodologies, tools to be used and appropriate human resources.

Thereafter, *preparation process* allows the investigator to prepare the required equipment and tools needed for the investigation

3) *The acquisitive class*

The acquisitive class consists of processes that help in potential evidence acquisition. This class is the third class of the HDFIP and includes processes as described below:

Potential digital evidence identification process, this is conducted at the incident scene and is a critical part of the investigation as potential evidence is identified and labelled during this process. Thereafter, the evidence is collected for analysis in a later process, and ensuring that the evidence is collected in a forensically sound manner so as to preserve its integrity during *potential digital evidence collection process.*

Potential Digital evidence acquisition process, during this process, ISO/IEC 27037 [10] is used as a guideline that assists in observing proper legal procedure. This ensures that potential digital evidence is admissible at all times. Digital evidence acquisition process is optional and can also be performed in the investigative class.

Potential Digital evidence transportation process, during this process the digital evidence collected in the previous process is transported to a location where storage and analysis may be done. *Potential Digital evidence storage and preservation process,* is required if analysis cannot be conducted immediately or if there are legal requirements to store the digital evidence for a certain period.

4) The investigative class

The investigative class deals with uncovering the potential digital evidence. Data analysis is part of the investigative class. This class is made up of the following processes described below:

Potential digital evidence acquisition is the same as explained in the acquisition class. *Digital evidence examination and analysis process* deals with the examination and analysis of the digital evidence with the use of several techniques to identify digital evidence as well as reconstruction if required. The hypothesis of the case under investigation is identified during this process. ISO/IEC 27042 [25] provides guidelines on examination and analysis,

Digital evidence interpretation process involves the interpretation of results obtained from the digital evidence examination and analysis process. Interpretation utilise scientifically proven methods and techniques to explain facts found during the digital evidence examination and analysis process. Thereafter, during the *reporting process,* the results from the digital evidence interpretation process is compiled and presented as a report written as simple as possible, clear, concise and unambiguous.

During the *Presentation process* the document complied in the reporting process is presented to the various stakeholders in any other forms such as multimedia presentation or expert witness testimony. *Investigation closure process* concludes the investigation and a decision made based on the validity of the hypothesis formulated during the presentation process. The interactive properties of the HDFIP allow the investigator to retrace to a specific process to validate the evidence presented [23].

5) The concurrent class

The concurrent class comprises of processes that continue alongside all other processes. The processes within this class run parallel with all the other processes discussed in the first four classes of the HDFIP model. The concurrent processes aim to achieve and maintain integrity, confidentiality and availability whilst achieve higher efficiency of the investigation. This also ensures that the digital evidence collected during the investigation is admissible in any court of law.

The concurrent processes outlined in the following sections ensure that consistency is maintained during the investigation.

Obtaining authorization process is process that ensures investigators obtained the proper authorization from authorities and all legal provisions are abided by during the investigation. *The documentation process* improves efficiency by ensuring clearly documentation of all steps undertaken during a digital forensic investigation. Moreover, documentation is conducted for each process of the HDFIP.

The *Managing Information flow process*, during this process, information flow must exist between the various processes and the stakeholders during the digital investigation. *Preserving the chain of custody process* ensures that all legal requirements are met and properly documented. *Preserving digital evidence process* assists in maintaining and achieving original digital evidence and preserving the integrity of all the procedures adhered to from the start of the digital investigation.

Interaction with physical investigation process involves the dependence and interconnection with the physical investigation. This activity defines the relationship between the digital investigation and the physical investigation.

Figure 1 below illustrates the interdependence of the various processes and provides an overview of the iterative structure of the HDFIP model.

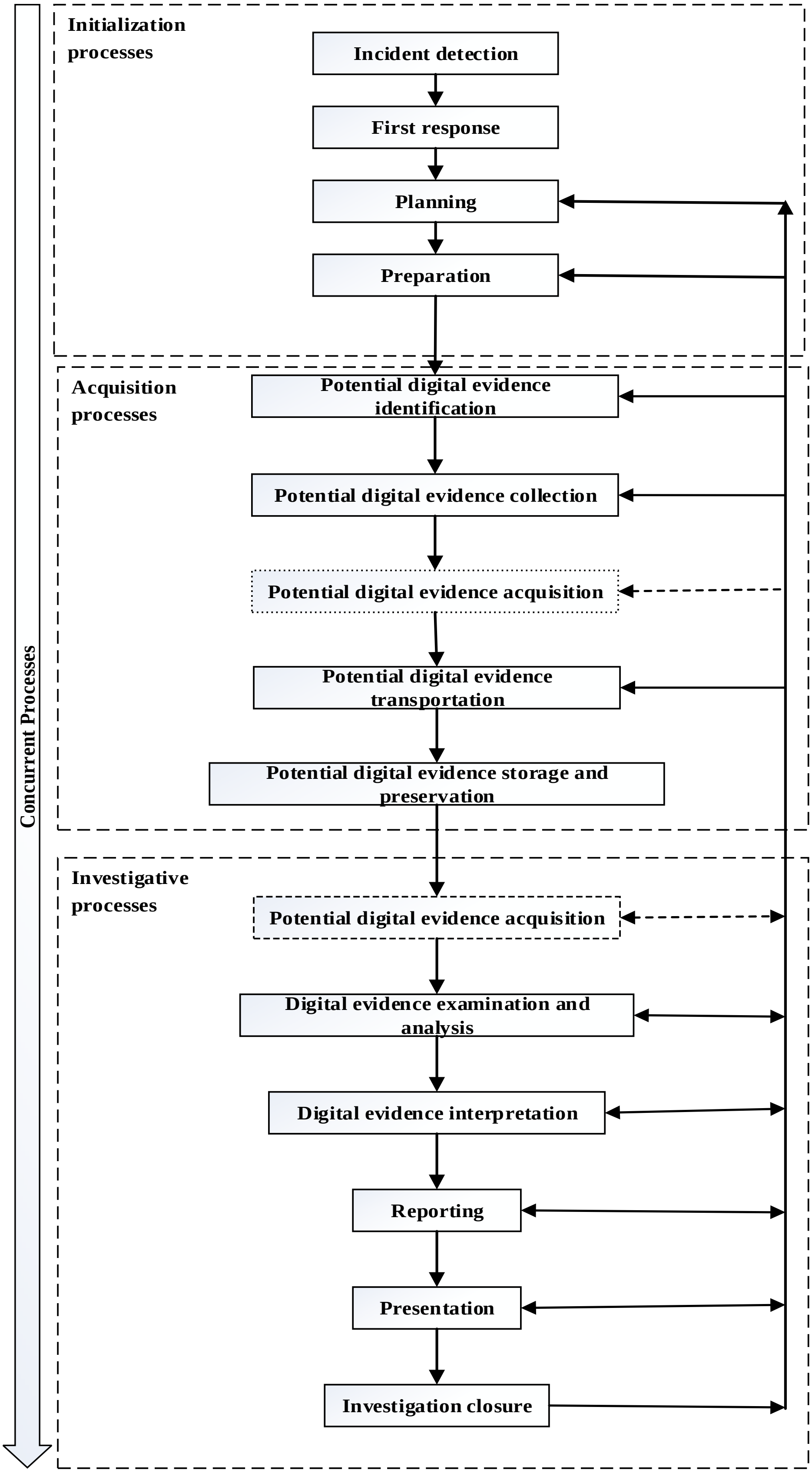
Initialization processes
Incident detection
First response
Planning
Preparation
Acquisition processes
Potential digital evidence identification
Potential digital evidence collection
Potential digital evidence acquisition
Potential digital evidence transportation
Potential digital evidence storage and preservation
Investigative processes
Potential digital evidence acquisition
Digital evidence examination and analysis
Digital evidence interpretation
Reporting
Presentation
Investigation closure
Concurrent Processes

Figure 1: Harmonised Digital Forensic Investigation Process model [11]

III. A CASE STUDY FOR TESTING THE HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS

In this section of the paper, the methodology used to test the HDFIP model and a case study are presented, which involve a real-life case in which all the processes of the HDFIP model, as shown in Figure 1, were applied during the investigation. The authors used the methodology as stipulated in ISO/IEC 27043 [11] to conduct this investigation. During the investigation, all digital forensic regulations were adhered to and followed as stipulated by the HDFIP model.

This section provides a brief description of the case study. The case study investigates a Blackberry mobile device (Research In Motion BlackBerry 9300 Curve). This case study is based on a real-world case that occurred, however, this case study is anonymised by using fictitious names instead of the real ones throughout the study.

South Africa's advertising industry is one the fastest growing industries in the world. Because of this growth, advertising companies are increasing their work force as competition becomes fierce where protection of intellectual property rights is vital to a company's success and survival. Most advertising companies have very tight non-compete agreements in place with their employees to ensure the protection of company assets, including intellectual property.

In this case study, Chana Advertising Company (CAC) holds intellectual property rights for the advertising concepts developed by their creative team. Non-compete agreements are in place to deter an employee from stealing intellectual property from an employer and creating a competing entity using the former employer's concepts.

CAC learnt of the formation of a competing company by its former employees. The head of human resources of CAC contacted Digital H Investigations (DHI), as they believed that communications regarding the new venture had taken place on a company asset (a Blackberry mobile device) formerly used by the employee. To confirm this suspicion, DHI was instructed to carry out a digital forensic investigation on the said mobile phone.

DHI found that most cases involving the infringement of a non-compete agreement and the theft of intellectual property, mostly involves former employees using company assets such as laptops or a smart phone, as was suspected in this case, to correspond with co-conspirators. It was suspected that the digital communications might still be present on the particular phone in the form of text messages, however, it might possibly have been deleted. Despite the possible deletion of the data, in most cases, an experienced digital forensics expert can recover the deleted data.

The following sub section provides an insight into the application of the HDFIP model to this case study in a bid to uncover potential digital evidence of the said suspected communications on the particular mobile phone involved.

IV. TESTING THE HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS MODEL

The HDFIP [11] model is utilized throughout the investigation conducted. During this investigation the term 'investigators' is used to refer to the authors who conducted the investigation and not to refer to digital forensic investigators in general. The following sub sections explain the implementation of the HDFIP sub process to the case study in detail.

A. *Incident detection process*

The incident was detected by the HHR (HOH) of CAC, who noted the creation of a competing entity. The HOH further enquired and uncovered that one of the founders was a former employee of CAC. The HOH reported the incident to CAC top management, who contacted DHI to conduct a digital forensic investigation

B. *First response process*

The first response process involves measures taken by the first responder. The first responder ensured that the mobile device was isolated from the network, to prevent incoming calls and messages that could potentially alter the potential evidence residing on the mobile device. The first responder from CAC contacted DHI to collect the mobile device.

C. *Planning process*

During this process, the HOH of CAC provided the investigators with descriptions of the case to be investigated. During this process the investigators documented all required resources and equipment. The resources and equipment were listed in the process to follow, specifically to suit a mobile forensic investigation. The investigators obtained authorization from CAC to extract potential digital evidence from the mobile device.

D. *Preparation process*

During the preparation process, the investigators prepared all relevant equipment requirements ranging from hardware to software tools. The resources and equipment for this particular case included the XRY complete package (Micro Systemation). The XRY complete package comprises of the XRY application software and license key, write-protected universal memory card reader, Windows OS 7, a Subscriber Identity Module (SIM) identity-cloner, XRY complete mobile phone cable kit and XRY communication unit. Other resources required included a digital video disc (DVD) used to provide a copy of potential evidence to the various stakeholders. A desktop computer, running the Windows 7 operating system. A faraday bag used to package and isolate the mobile device from the network during potential digital evidence collection and preservation process. A digital camera used to document the potential evidence and crime scene [17].

E. *Potential digital evidence identification process*

During potential digital evidence identification, the investigators identified the potential evidence as the mobile device, which was the potential source of digital evidence. In this scenario, it was quite obvious that this device contain the potential digital evidence, however, in different scenarios there might potentially be more potential digital evidence as well as latent potential digital evidence, such as written notes, fingerprints etc. involved.

The investigators identified the potential evidence and documented the details of the mobile device as a BlackBerry 9300 Curve. Preserving digital evidence included examination of the device for any physical damage, documenting the identifying details such as model, serial number (i.e. International Mobile Equipment Identity (IMEI) number). The investigators documented date and time zone related information.

F. Potential digital evidence collection process

During the acquisition of the potential evidence, the mobile device was collected as potential evidence and clearly labelled and placed in a faraday bag as part of the documentation concurrent process, which is discussed later. This assisted in maintaining the chain of custody and information flow.

G. Potential Digital evidence transportation process

During the digital evidence transportation, the mobile device was physically transported to laboratory in a secure and forensically sound manner. The chain of custody was observed and followed during the transportation.

H. Potential Digital evidence storage and preservation process

Digital evidence is stored if analysis cannot be conducted immediately. The digital evidence is stored in a secured locker. The chain of custody and preservation of the integrity of evidence was maintained by ensuring that an evidence ledger (chain of custody) was kept to keep trace of evidence.

I. Potential digital evidence acquisition process

During potential digital evidence acquisition a copy of each of the potential digital evidence sources is produced. During this process the potential digital evidence is extracted from the following sources: mobile device internal memory, SIM card memory, and SD memory.

Potential evidence extraction from the mobile device was conducted using the XRY extractor tool. The mobile device was connected to a desktop using a cable for the acquisition of all the data residing on the mobile device. A logical acquisition was conducted on the internal memory of the mobile device. The acquisition retrieved data which comprised of the type of Operating System, make, model of the mobile device, web bookmarks, contacts, SMS messages, pictures, audio, video, documents, MMSs, email, calendar, tasks, and notes.

Thereafter, the investigators also conducted a logical acquisition on the SIM card. The investigators extracted potential evidence from the SIM card by cloning the original SIM card. The investigator used a SIM cloner to create a duplicate SIM card consisting of the critical data residing on the original SIM card designed to isolate the mobile phone from the mobile network [27]. This practice is very similar to using a write blocker when acquiring data from a hard drive. The investigators then placed this specially-cloned SIM card into the mobile device so as to avoid any further update or changes to the potential evidence residing on the mobile device. Potential evidence extracted from the cloned SIM card includes the Network code from International Mobile Subscriber Identity (IMSI), mobile number, contacts on the SIM card, and SMS messages on the card. The cloned SIM cards hold two essential identities that were retrieved during this process, namely the Integrated Circuit Card Identifier (ICCID) and IMSI.

The acquisition of potential evidence from the SD memory card was conducted using a physical acquisition. The use of logical and physical acquisition allows for the recovery of any deleted data that once resided on the memory SD card, such data consisted of contacts, MMS messages and files (pictures, music, documents, sound clips, and videos).

The investigators followed all legal requirements during this process while seeking consultation from ISO/IEC 27037 [10] in order to conduct these acquisitions legally and accurately. Potential digital evidence acquisition is a critical process as the evidence extracted may become inadmissible if such proper acquisition procedures are not adhered to. The potential digital evidence collected can be verified by using ISO/IEC 27041 [28]. Each step and method used is documented clearly and in detail by the investigators.

J. Digital evidence examination and analysis process

During digital evidence examination and analysis process, the investigators conduct an examination of the data acquired from the digital evidence and an analysis of the potential evidence recovered from the mobile device's various memory acquisitions. The examination and analysis techniques of the potential evidence that the investigators performed included timeframe construction , extraction of hidden data , extraction of application files and ownership details This process was used to determine the significance of the digital evidence extracted from the mobile device to this specific case study. The significance was determined by grouping the potential evidence according to the file format such documents, emails, and SMS.

The investigators documented each and every step in a forensically sound manner by carefully adhering to the HDFIP model as shown in figure 1. Due to the volatile nature of the mobile device the investigators ensured that the potential source of digital evidence was handled with critical care. By ensuring that the mobile device remained isolated from the network to avoid any change to the data residing on it. The investigators took into account the physical state of the potential source of evidence, by conducting a physical inspection of the mobile device.

K. Digital evidence interpretation process

The interpretation of the digital evidence extracted from the mobile device proved to be of significance, the investigators categorised the evidence according to the significance of the case. The investigators concentrated on the potential evidence extracted from the mobile device. The evidence of interest included emails, documents, contacts, and SMS messages, which were first priority in the case as these may have been used main forms of communication means. During the digital evidence interpretation process the investigators narrowed down the significant data within certain documents, call logs, SMS messages and MMS messages that of were of importance to this case.

L. *Reporting process*

The results obtained from the interpretation process showed that the former employee of CAC used the mobile device for stealing intellectual property to create a competing entity. The investigators compiled a report detailing all the processes and all the different techniques used during the investigation, as suggested by the HDFIP model within ISO/IEC 27043, as depicted in Figure 1. Relevant information concerning the process that was followed, the extraction methods, tools, and techniques used was clearly stated within the report. The interaction with the potential evidence by the investigators was elaborated on within the report, in a forensically sound manner, hence providing accountability by the investigators. The investigators presented the report to all the relevant stakeholders involved in this particular case.

M. *Presentation process*

The investigators presented the findings of digital evidence analysed during the digital evidence interpretation process in the form of expert reports to the various stakeholders. The report contained evidence that proved a violation of the Non-compete agreements in the form of emails and SMS messages.

During the presentation process the investigators confirmed that all the processes, as defined in ISO/IEC 27043, were used to verify that the investigation was conducted in a forensically sound manner. The detailed report was, therefore, compiled by the investigators involved in the investigation.

N. *Investigation closure process*

The investigation closure was conducted after presentation of the report. Thereafter, the mobile device and potential digital evidence collected during the investigation process was returned to Chana Advertising Company (CAC). The findings could then be used in a prosecution case at the discretion of CAC against their former employee.

The following sub sections provide an overview of the HDFIP model's performance during the mobile forensic investigation conducted.

V. Performance Evaluation of the Harmonised Digital Forensic Investigation Process Model of ISO/IEC 27043

The HDFIP model as defined in ISO/IEC 27043 worked effectively for a mobile device as explained in detail in the previous section. As a result, it is assumed that the HDFIP model can be applicable to other mobile devices as it is a generic process model. In order to ensure full performance of the process model, investigators with adequate knowledge and skills are required to produce reliable and admissible potential digital evidence.

The documentation process has proved to be vital during the testing as it was applicable to each process of the HDFIP model. Another observation noted is that the investigators should always prepare according to the type of digital forensic investigation as this does not only preserve the integrity of the potential evidence, but also the creditability of the investigators conducting the investigation.

During the investigation, the HDFIP model showed effectiveness as well as flexibility, adaptability, integrity, comprehensiveness, and accountability, which was a result of the model's interdependence among the various classes and processes. Using the HDFIP model, the investigators noted that the results acquired during the investigation cannot be sufficient if only some process within the HDFIP is considered. To produce an adequate digital forensic report, each process of the HDFIP must be considered in order to have a complete understanding and representation of the incident in question.

The concurrent processes were fully applicable during the testing of HDFIP model by ensuring that the investigators followed the proper legal processes and procedures. The investigators obtained authorization, documented each interaction with the physical and digital evidence, preserved the digital evidence's integrity, managed the information flow between the processes and preserved the chain of custody of potential digital evidence throughout the investigation.

The processes of the HDFIP were derived from and harmonised with other process models and guidelines, which implies that during its development other frameworks, theories and process models where consulted intensively, hence arriving at such a holistic process model that takes into consideration all types of digital forensic investigations.

Table I shows the different types of criteria taken into consideration during the investigation. Table I maps out where each process fulfilled a particular criteria during the mobile forensic investigation. An X is used to mark the applicability of the criteria to the processes. Table I assists in showing how reliable the HDFIP model was during a mobile forensics investigation as it adhered to these criteria used to evaluate digital forensic process models as stated by [4].

Table I**:** Various Criteria met by the HDFIP

HDFIP (ISO/IEC 27043) processes	**Flexi-bility**	**Adaptive -ness**	**Integrity**	**Comprehensive -ness**	**Effectiveness**	**Accountability**
Incident detection				X		X
First response		X		X	X	X

Planning	X	X	X		X	X
Preparation		X	X	X	X	X
Incident scene documentation	X		X		X	X
Potential digital evidence Identification			X	X	X	X
Digital evidence acquisition		X	X	X		X
Digital evidence transportation	X		X	X	X	X
Digital evidence storage	X			X		X
Digital evidence analysis			X	X	X	X
Digital evidence interpretation			X	X		X
Report writing			X	X	X	X
Presentation	X	X	X	X		X
Investigation closure	X	X	X	X	X	X

VI. RELATED WORK

This section presents investigation process models proposed by various authors. The models proposed have been used not only for digital forensic investigations but also in different areas such as, development of training materials, and identification of research areas [3]. Table II presents models used to determine if a mobile forensic investigation is applicable, thereafter the investigators identified a number of strengths and weaknesses of the process models in Table II.

Table II: Digital investigation process models

Author's Name	**Process Model Names**	**Strength**	**Weakness**
ACPO, [2]	Good practice guide for computer-based electronic evidence internet	Four principles based on electronic evidence	Three of the four principles are not applicable to mobile device forensics
Mandia, [14]	Incident response: Investigating computer crime	Suited for live systems and system restoration	Extraction of potential evidence from a Mobile devices cannot be conducted while in a live state
U.S Department Of Justice[18],[6]	A guide for first responders	Focuses on the first responder and emphasizes on the collection potential evidence	Limited attention on the examination and analysis processes
Carrier and Spafford,[3]	Getting physical with the digital investigation process	Focuses on data protection and acquisition, imaging, extraction, interrogation, normalisation, analysis and reporting	Focus mainly on physical crime scene.
Ramabhadran,	Forensic investigation process model for Windows Mobile	Tailored to specifically suit	Non-applicable to other types of digital forensic

[22]	devices	Windows mobile devices.	investigations
Goel, Tyagi and Agarwal [7]	Smartphone forensic investigation process model	Emphasizes the specific flow of information and details of the mobile devices	Documentation is only conducted as a single process, which limits information gathering

The digital investigation process models in Table II where used to show whether a mobile forensic investigation could be conducted using these models. The strengths and weaknesses of these digital investigation process models clearly show that these digital investigation models cannot be applied to mobile forensic investigation. The disparities stated in Table II indicates the need for a generalized process model that presents a holistic approach applicable to all types of digital forensic investigations. From this need, the HDFIP model, as described in ISO/IEC 27043, has been devised by means of a harmonisation effort in research conducted by [30].

VII. Conclusion

The problem statement addressed in this study was the need for a digital forensic investigative process model that provides support for forensic examiners and investigators facing challenges when performing data acquisition from mobile devices. The HDFIP addresses these challenges faced by investigators. It also ensures that integrity, availability, flexibility, adaptiveness, integrity, comprehensiveness, effectiveness, accountability and confidentially are maintained. The HDFIP is well-structured and applicable to mobile forensic. Hence, this process model can be used during potential evidence acquisition from mobile devices in a forensically sound manner. Further testing using HDFIP has been conducted on an Android mobile phone by [21].

The research presented in this paper highlights the testing of the HDFIP model using a Blackberry mobile device case study. The question was whether the HDFIP model would be effective enough for conducting a digital forensic investigation on a mobile device. The HDFIP model proved to be effective during the investigation through the concurrent processes which ensured that documentation, interaction with physical evidence, preserving digital evidence and obtaining authorization where adhered to. Knowing that mobile forensics is still a relatively a new field, this paper addressed the need for a harmonised investigative process on mobile devices. Such a process model can resolve both the present and future disparities faced by digital forensic examiners and investigators in the acquisition of potential digital evidence on mobile devices, thereby creating a lasting uniformity in the domain of digital forensic investigative process models.

Acknowledgment

This work is based on the research supported in part by the National Research Foundation of South Africa (Grant specific unique reference number TP13081227420). The Grant holder acknowledges that opinions, findings and conclusion or recommendations expressed in any publication generated by NRF supported research are that of the author(s) and that the NRF accepts no liability whatsoever in this regard.

References

[1] Al-Zarouni, M. (2006), Mobile Handset Forensic Evidence: a challenge for Law Enforcement Proceedings of the 7th Australian Digital Forensics Conference.

[2] ACPO v4.0: Good Practice Guide for Computer-Based Electronic Evidence Internet, http://www.7safe.com/electronic_evidence/#

[3] Carrier, B., and Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), 1-20.

[4] Casey, E. (2004). Digital evidence and computer crime. Elsevier academic press.

[5] Lesemann, D.J., Mahalik, H. (2008). Forensic Preservation of handheld devices. Information system Security Association Journal November.

[6] Electronic Crime Scene Investigation, (2008): A Guide for First Responders. U.S Department of Justice.

[7] Goel, A., Tyagi, A., and Agarwal, A. (2012). Smartphone Forensic Investigation Process Model. International Journal of Computer Science & Security (IJCSS), 6(5), 322.

[8] Palmer, G. (2001). A Road Map for Digital Forensic Research. DFRWS Technical Report DTR-T001-01, Report from the first Digital Forensic Research Workshop (DFRWS).

[9] ISO/IEC 27035, (2011). Information technology Security techniques Information security incident management.

[10] ISO/IEC 27037, (2012). Information technology Security techniques Guidelines for identification, collection, acquisition, and preservation of digital evidence.

[11] ISO/IEC 27043, (2014), Information Technology, Security techniques, Incident Investigation processes and principles Committee draft.

[12] Jansen, W. and Ayers, R. (2007). Guidelines on cell phone forensics, NIST Special publication 800-101.

[13] Kleiman, D. (2011). The official CHFI study guide (exam 312-49): for computer hacking forensic investigator. Syngress.

[14] Mandia, K. (2001). Incident response: investigating computer crime. McGraw-Hill Professional.

[15] Mcillan, J.E.R., Glisson, W.B., and Bromby, M. (2013). Investigation the increase in mobile phone evidence in criminal activities. 46th Hawaii International Conference on System Sciences.

[16] Mohtasebi, S., Dehghantanha, A. & Broujerdi, H.G. (2011), Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone, International Journal of Digital Information and Wireless Communications (IJDIWC), vol. 1, no. 3, pp. 651-655

[17] Micro Systemation (MSAB) http://www.msab.com/index?gclid=CNzK2Njc2rwCFWoOwwodzBcAjA

[18] National Institute of Justice, US Dept Justice, Office of Justice Programs, & United States of America. (2008). Electronic Crime Scene Investigation: A Guide for First Responders.

[19] NIST Publication 800-101: Recommendations of the National institute of Standards and Technology Internet, http://csrc.nist.gov/publication/nistpubs/800-101/SP800-101.pdf

[20] Owen, P., Thomas, P., and D.McPhee, D. (2010), An Analysis of the Digital Forensic Examination of Mobile Phones. Fourth International Conference on Next Generation Mobile Applications, Services and Technologies

[21] Omeleze, S. and Venter, H.S. (2013), Testing the Harmonised Digital Forensic Investigation Process Model-Using an Android Mobile Phone, Proceedings of the Annual Information Security for South Africa (ISSA 2013) Conference.

[22] Ramabhadran, A. 2007, Forensic investigation process model for Windows Mobile devices, Retrieved May, vol. 11, pp. 2009.

[23] Valijarevic, A. and Venter, H.S. (2012), Harmonised Digital Forensic Investigation Process Model, Proceedings of the Annual Information Security for South Africa (ISSA, 2012) Conference.

[24] Willassen, S. (2003), Forensics and the GSM mobile telephone system. International Journal of Digital Evidence Spring 2003, Volume 2, Issue 1.

[25] ISO/IEC 27042, (2014), Guideline for the analysis and interpretation of digital evidence committee draft.

[26] Lesemann, D. and Mahalik, H. (2008), Dialing Up and Drilling Down: Forensic Preservation of Handheld Devices, ISSA Journal, p.22l, November 2008.

[27] Micro systemation http://www.msab.com/xry/xry-sim-id-cloner

[28] ISO/IEC 27041, (2014) Information technology Security techniques, Guidance on assuring the suitability and adequacy of investigative methods.

[29] Daubert v. Merrell Dow Pharmaceuticals, (1993) Inc. 509 U.S. 579.

[30] Valijarevic, A. and Venter, H.S. (2012), Harmonised Digital Forensic Investigation Process Model, Proceedings of the Annual Information Security for South Africa (ISSA, 2012) Conference.

[31] Oscar Pistorius murder trial http://www.sowetanlive.co.za/news/2014/04/08/inside-the-oscar-pistorius-trial---2

[32] Shrien dewani murder trial http://www.dailymaverick.co.za/article/2014-04-06-the-killing-of-anni-more-than-just-shrien-dewani-in-the-dock/#.U25olCjlaSo