Annual ADFSL Conference on Digital Forensics, Security and Law

2014 Proceedings

May 28th, 3:20 PM

Testing and Evaluating The Harmonised Digital Forensic Investigation Process in Post Mortem Digital Investigation

Emilio R. Mumba
Department of Computer Science, University of Pretoria, emmy_emiray@yahoo.co.uk

H. S. Venter
Department of Computer Science, University of Pretoria, hventer@cs.up.co.za

TESTING AND EVALUATING THE HARMONIZED DIGITAL FORENSIC INVESTIGATION PROCESS IN POST MORTEM DIGITAL INVESTIGATIONS

Emilio Raymond Mumba
emmy_emiray@yahoo.co.uk

H.S. Venter
hventer@cs.up.co.za

Department of Computer Science
University of Pretoria
Private Bag X20, Hatfield 0028
Pretoria, South Africa

ABSTRACT

Existing digital forensic investigation process models have provided guidelines for identifying and preserving potential digital evidence captured from a crime scene. However, for any of the digital forensic investigation process models developed across the world to be adopted and fully applied by the scientific community, it has to be tested. For this reason, the Harmonized Digital Forensic Investigation Process (HDFIP) model, currently a working draft towards becoming an international standard for digital forensic investigations (ISO/IEC 27043), needs to be tested.

This paper, therefore, presents the findings of a case study used to test the HDFIP model implemented in the ISO/IEC 27043 draft standard. The testing and evaluation process uses an anonymised real-life case to test each subprocess (grouped in classes) of the HDFIP model to show that it maintains a structured and precise logical flow that aims to provide acceptance, reliability, usability, and flexibility. The case study used also helps to analyse the effectiveness of the HDFIP model to ensure that the principles of validity and admissibility are fulfilled. A process with these properties would reduce the disparities within the field of digital forensic investigations and achieve global acceptance and standardization**.**

Keywords: Digital forensics (DF), harmonized digital forensic investigation process (HDFIP), ISO/IEC 27043, investigation process.

1. INTRODUCTION

Over the years, digital forensics (DF) has developed into a discipline that is in need of a comprehensive digital forensic investigation process model. Different researchers have proposed over one hundred different investigation process models up to date (Ball, 2007). However, the various models proposed over all these years lack experimental testing and evaluation (Selamat et al, 2008). The importance of testing and evaluating a harmonized investigation process model lies in ensuring that the model adheres to the requirements (standards) of the scientific community within DF. Such a tested and evaluated investigation process model will also support the development of new techniques and procedures in the digital forensic domain.

Furthermore, according to Ademu and Imafidon (2012), it is vital that investigation process models be peer-reviewed, tested and validated in a scientific manner. The use of the Daubert rule (1993) in the United States of America's court system, for example, allows the presentation of potential digital evidence before a jury if the methodology used is consistent, hence validating the potential evidence

collected. The Daubert rule (1993) also provides guidelines and insight into the requirements of an investigative process in the United States of America's courts.

In the case of digital forensics, standardizing an investigation process model will assist digital forensic practitioners and organizations in developing suitable policies and procedures in a forensically sound manner. The term 'forensically sound' refers to using a method that does not change the data residing on the hard disk which is being duplicated (Daubert, 1993). Besides, the need for a standardized and tested investigation process model in digital forensics will improve on any investigation undertaken by ensuring common investigation processes and procedures. This will further reduce the disparities currently being experienced in digital forensic investigations.

The presentation in this paper, therefore, provides the findings and recommendation after testing and evaluating the HDFIP model, which is part of the draft international standard ISO/IEC 27043 (2014). Note that 'testing' does not refer to conducting testing as understood in the field of software engineering, but rather to evaluating the efficiency and contribution of the HDFIP model. The fundamental purpose of ISO/IEC 27043 is to promote good-practice methods and processes for forensic investigation of potential digital evidence. In addition, it also provides a framework that can act as a teaching aid in DF and assist in legal matters.

This paper is structured as follows: Section 2 presents background concepts of the investigation process models as well as of the harmonized digital forensic investigation process model. Section 3 explains the methodology and a case study, while Section 4 highlights the findings and recommendations. Finally, Section 5 provides a conclusion to this paper.

2. BACKGROUND

In this section, the authors present background concepts of different digital forensic investigation process models as well as the HDFIP model.

Digital forensic investigations can be categorised into different types, including: post mortem digital forensics, live digital forensics, network forensics, and mobile forensics.

- Post mortem digital forensics (also known as dead digital forensics) is the process of conducting an investigation on an unpowered device (Ademu et al., 2011).
- Live digital forensics, on the other hand, deals with extracting system data before disconnecting the digital device's power source, in order to preserve memory and information that would be lost using the post mortem approach (McDougal, 2006).
- Network forensics deals with preserving and collecting digital evidence in a connected digital environment (Jansen and Ayers, 2006).
- Mobile forensics is the science of recovering digital evidence from a mobile device like a smartphone (Jansen and Ayers, 2006).

Due to the vast number of digital forensic investigation process models, the standardization of an investigation process model in digital forensics has become a matter of priority. Existing digital forensic investigation process models show notable disparities, such as the number of phases and the scope of models (Valjarevic and Venter, 2012); hence the need for standardization. Table 1, for example, presents some of the process models developed over the years, with different models comprising different numbers of phases.

From Table 1, it is clear that there exist a number of digital forensic investigation process models, stemming from different researchers and organizations. The different number of phases in each proposed model adds to the disparities among the investigation models. However, Valjarevic and Venter (2012) proposed the harmonization of the investigation process models, with the main aim of developing a process model that encapsulates all other models that currently exist. The outcome of the effort of Valjarevic and Venter (2012) was the HDFIP model. The proposed HDFIP takes into

consideration legal recommendations and requirements on a global level (Valjarevic and Venter, 2012).

Table 1 Digital Forensic Investigation Process Models and Frameworks

Process model name	References	Number of phases
A Road Map for Digital Forensic Research	DFWRS (2001)	7 phases
An examination of digital forensic models	Reith et al (2002)	9 phases
Electronic Crime Scene Investigation - A Guide for First Responders	DOJ (2001)	8 phases
Getting Physical with the Digital Investigation Process	Carrier et al (2003)	5 groups, 17 phases
Incident Response & Computer Forensics	Mandia et al (2003)	11 phases
A Hierarchical, Objectives-Based Framework for the Digital Investigation Process	Beebe et al (2005)	6 phases
An Extended Model of Cybercrime Investigations	Cuardhuain (2004)	12 phases
Fundamentals of Digital Forensic Evidence. Chapter in *Handbook of Information and Communication Security*.	Cohen (2011)	11 phases
A Chapter in Forensic Analysis, in: *Handbook of Digital Forensics and Investigation*.	Casey et al (2010)	4 phases
Good Practice Guide for Computer-Based Evidence	ACPO (2008)	13 phases
Harmonized Digital Forensic Investigation Process (HDFIP) model	Valjarevic and Venter (2012)	14 phases

The HDFIP model consists of five classes, as depicted in Figure 1: the readiness processes class, the initialisation processes class, the acquisitive processes class, the investigation processes class, and the concurrent processes class. These are also incorporated and presented in the draft international standard ISO/IEC 27043. The subsections that follow explain in brief the five different classes, together with the various processes in each class, as applicable.

2.1 The Readiness Class

Digital forensic readiness is the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation (Palmer, 2001). The readiness class is, however, optional to the remainder of the process, as it concerns mainly the voluntary participation of an organization rather than the role of the investigator(s) involved in an investigation. For this reason, this paper does not discuss the readiness class of the HDFIP model in any further detail.

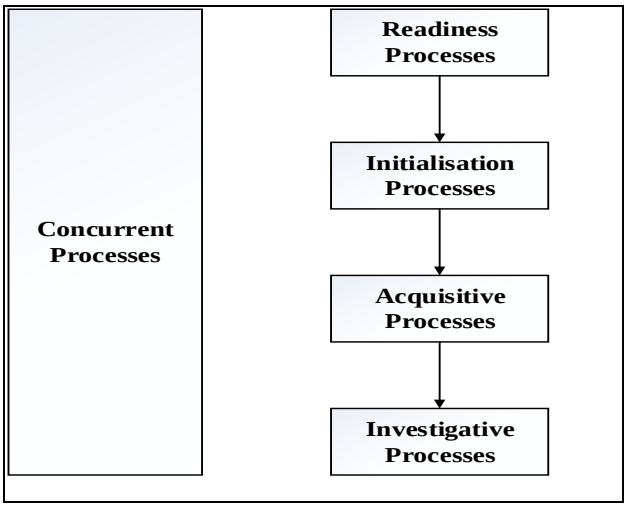

Figure 1 Classes of HDFIP Model (ISO/IEC 27043, 2014)

2.2 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 and in its course the investigators become physically involved in the investigation. This class comprises the subprocesses briefly discussed as follows.

The incident detection process involves the classification of the incident into the different types of digital forensic investigation 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 an oral account of the event. The first response process involves the first steps taken after an incident is detected. ISO/IEC 27035-2 (2014) and ISO/IEC 207037 (2014) provide a standardization of the incident response process.

The planning process allows the investigator to perform all the possible planning required during the digital investigation process, as well as the development of proper procedures, the defining of methodologies, the choice of tools to use, and the appropriate human resources that should be involved in the investigation. Thereafter, the preparation process allows the investigator to prepare the required equipment (hardware and software) for the investigation.

2.3 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 subprocesses as follows.

The incident scene documentation process involves full documentation of the incident scene, through the use of activities such as sketches, photographs, videos and labelling of all the potential evidence. The potential digital evidence identification process is conducted at the incident scene and is a critical part of the investigation, as potential evidence is identified during this process. The digital evidence acquisition process is conducted immediately after the identification of potential digital evidence. ISO/IEC 27037 (2014) provides guidelines that can be used during this process.

During the next process, i.e., the digital evidence transportation process, the digital evidence is transported to a location where storage and analysis may be conducted. The potential digital evidence can be transported using physical or electronic means. Evidence transported electronically requires special precautions to preserve the integrity and chain of custody. Special precautions include encrypting and digitally signing the potential digital evidence. After this process, a digital evidence

storage process is required if analysis cannot be conducted immediately or if there are additional legal requirements to store the digital evidence for a certain period.

2.4 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 subprocesses described below.

The digital evidence examination and analysis process examines and analyses the digital evidence using various techniques to identify digital evidence as well as perform a reconstruction if required. The hypothesis of the case under investigation is formulated during this process. ISO/IEC 27042 (2014) provides guidelines on examination and analysis.

The digital evidence interpretation process involves the interpretation of results obtained from the digital evidence examination and analysis process. The interpretation process utilises scientifically proven methods and techniques to explain the findings of the digital evidence examination and analysis process. Thereafter, during the reporting process, the results from the digital evidence interpretation process are compiled and presented as a report, written as simply as possible in clear, concise and unambiguous text.

During the presentation process, the document compiled in the reporting process is presented to the various stakeholders in any suitable form such as multimedia presentation or expert witness testimony. The investigation closure process concludes the investigation, and a decision is made to determine the relevance of the potential digital evidence presented to the stakeholders and whether to use this potential evidence in the case at hand.

2.5 The Concurrent Class

The concurrent class comprises processes that continue concurrently with all other processes. In other words, the subprocesses within the concurrent class run in parallel with all the other processes discussed so far in the four classes of the HDFIP model, as depicted in Figure 1. The concurrent processes aim to achieve and maintain integrity, confidentiality and availability whilst aiming to 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 following subprocesses in the concurrent class ensure that consistency is maintained during the investigation. They are briefly explained as follows.

Obtaining authorization is a process that ensures that investigators have obtained the proper authorization from the authorities and that all legal rules are abided by during the investigation.

The documentation process improves efficiency and a higher probability of a successful digital investigation. Moreover, documentation is produced for each of the subprocesses within the HDFIP.

The information flow process advocates that information flow should exist between the various processes and stakeholders during the digital investigation. Preserving the chain of custody is a subprocess which ensures that the legal requirements are met and properly documented in order to assist in obtaining and maintaining the original digital evidence, and to preserve the integrity of all the procedures followed from the start of the digital investigation.

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

3. RELATED WORK

Note that there exist other standards supporting the HDFIP model, some of which have already been mentioned in the previous section. These standards include the following:

- ISO/IEC 27035 (2014) - Part 1: Deals with the principles of incident detection management.
- ISO/IEC 27035 (2014) - Part 2: Deals with guidelines to plan and prepare for an incident response.
- ISO/IEC 27035 (2014) - Part 3: Deals with guidelines for incident response operations.
- ISO/IEC27037 (2012): Provides guidelines for identification, collection, acquisition and preservation of digital evidence.
- ISO/IEC 27040 (2014): Provides details on storage security.
- ISO/IEC 27041 (2014): Provides guidelines for the assurance for digital evidence investigation methods.
- ISO/IEC 27042(2014): Provides guidelines for the analysis and interpretation of digital evidence.

Together, all these standards, most of which are still in the draft stage, deal with some of the subprocesses defined in the ISO/IEC 27043 draft standard.

The HDFIP model takes all these standards into consideration, which also ensures that the HDFIP model maintains the integrity of the potential evidence extracted during an investigation process. The standards provide guidelines to the investigators for the use of each of the subprocesses defined in the HDFIP model, more specifically, during a digital investigation. Table 2 shows where these standards are applicable within the HDIFP model. The ticks (√) in table 2 indicate which ISO/IEC standards are applicable in the corresponding processes of the HDFIP.

For example, ISO/IEC 27035-1 (where '-1' refers to part 1 of ISO/IEC 27035) is applicable in the HDFIP during the incident detection process and the first response process. This observation indicates the importance to digital forensic investigators of consulting other standards before and during the use of the HDFIP model as shown in Table 2, so as to produce a forensically sound investigation.

Table 2 shows how the HDFIP model is complemented by other existing standards and documents that provide more insight into how an investigator can proceed during a digital forensic investigation.

Table 2 Applicability of Standards to Investigation Processes of the HDFIP

HDFIP (ISO/IEC 27043) processes	**ISO/IEC 27035-1**	**ISO/IEC 27035-2**	**ISO/IEC 27035-3**	**ISO/IEC 27037**	**ISO/IEC 27040**	**ISO/IEC 27041**	**ISO/IEC 27042**
Incident detection	√		√			√	
First response	√					√	
Planning		√				√	
Preparation process		√				√	
Incident scene documentation				√		√	
Potential digital evidence identification				√		√	
Digital evidence acquisition				√		√	
Digital evidence transportation					√	√	
Digital evidence storage					√	√	
Digital evidence analysis			√			√	√
Digital evidence interpretation			√			√	√
Report writing			√			√	√
Presentation			√		√	√	√
Investigation closure					√	√	√

The next section describes the methodology and case study used in the paper.

4. METHODOLOGY AND CASE STUDY

In this section of the paper, the methodology is used in testing and evaluating the HDFIP model, as well as a case study involving a real-life case in which all the processes of the HDFIP model (as shown in Figure 2), are discussed and applied.

In the course of the investigation process, all the concurrent processes were considered, namely obtaining authorization, defining the information flow, preserving the chain custody, preserving digital evidence, interaction with the physical investigation, and documentation. Note that the concurrent processes are discussed separately from any other process, to provide a full description of the interaction with the investigation processes. In the context of this paper, the authors themselves were part of the investigators.

The testing and evaluating process described in this paper is limited to the scope of a post mortem digital investigation process. The events in the scenario have been anonymised for the sake of privacy and confidentiality.

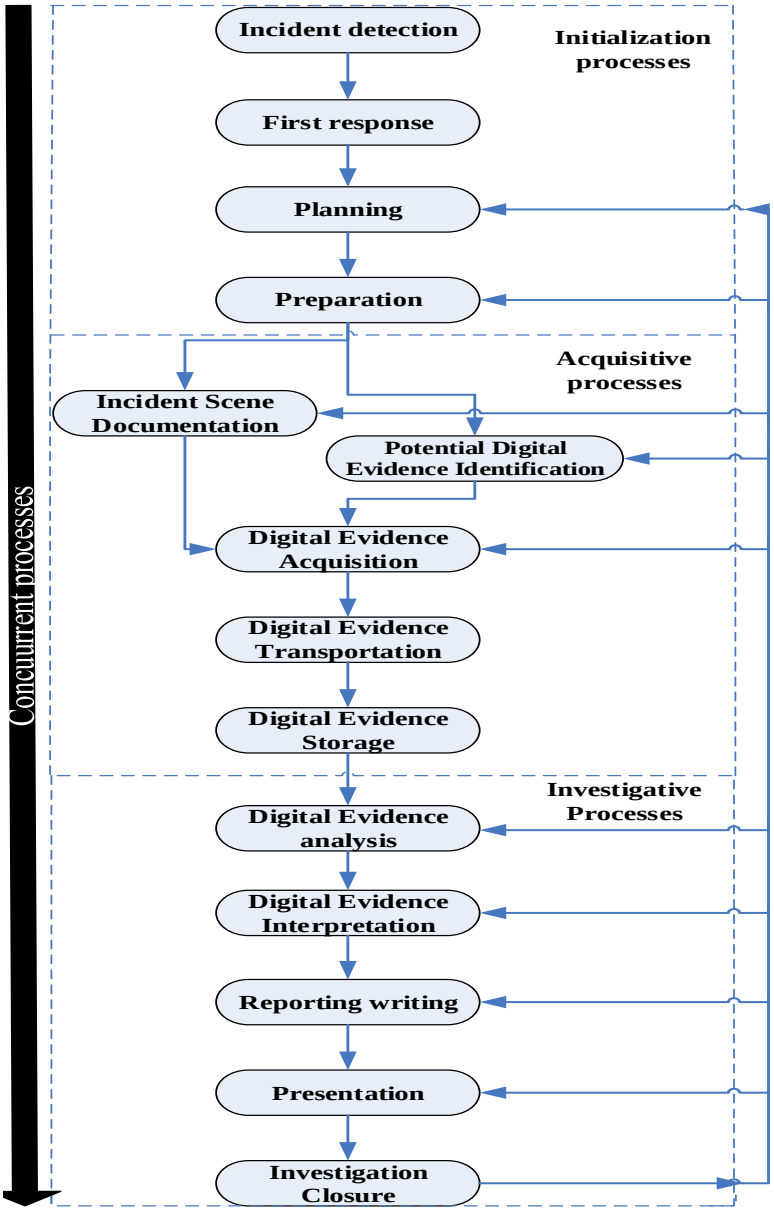

Figure 2 Harmonized Digital Forensic Investigation Process (ISO/IEC 27043, 2014)

In Figure 2, arrows are also used to depict the concurrent class mentioned earlier in this paper.

For the sake of testing and evaluating the HDFIP model, the scenario used was as follows: Company X suspected one of their employees of using company resources to download pornographic material during office hours. Company X regards any form of pornography as illegal and unacceptable, according to their user policy.

The system administrator detected this incident when he noticed a constant visit to a particular pornographic website. He immediately notified the head of the department, who then requested company H (Digital H) which conducts digital forensic investigations, to investigate the allegation. The authors teamed up with Digital H as part of the investigative team and used the HDFIP model for the case study described.

The motivation to use the HDFIP model as presented in Figure 2 in this case study was to test its performance in a number of real-life cases before it becomes an international standard in digital forensics. Each of the processes within the HDFIP model is fully applied to the case study. In the subsections to follow, each process is briefly explained in the context of the scenario used in this paper. This is done to determine how applicable and effective the HDFIP model is for a post mortem digital forensic case.

4.1 Initialisation Class

This class consists of incident detection, first response, planning, and preparation processes. From figure 1, the initialisation class is second in the HDFIP model, preceded by the readiness class. Note that, as mentioned earlier, the readiness class is beyond the scope of this paper and thus not discussed in the present context. It is in the initialisation class that the investigators were physically involved in the investigation process. During the initialisation class, the investigators carried out various procedures before the commencement of the digital investigation involving the case study. Each of the processes used by the investigators is discussed in the subsections that follow.

4.1.1 Incident Detection Process

During the incident detection process, the system administrator of Company X detected constant visits to a particular pornographic website during routine system maintenance. There was also an indication of frequent downloads of pornographic material during office hours, from the same website. It was also evident to the system administrator from the network logs that there were frequent visits to the same website as well as excessive amounts of data downloads.

According to the company policy, once an employee exceeds his or her monthly data allowance, the system administrator must inform the head of department so that the employee can be investigated for misuse of company resources. A potential investigation involves application of digital forensic techniques to aid understand the incident detected by the system administrator.

4.1.2 First Response Process

The first response involves measures taken by the first responder. The system administrator was the first to respond in this case. He noticed the unusual network traffic to a particular website while conducting system maintenance. As a first responder, he retrieved all the logged files and securely stored them, as required company policy. The system administrator also stored the log files safely, awaiting further investigation by the Digital H investigative team.

4.1.3 Planning Process

During this process, the investigators used the descriptions of the incident as provided by the head of department and the system administrator, to plan the investigation process. This included the required resources, which in this context were the equipment and software listed in Table 3. Other resources required for this particular case study included documentation material, authorization forms and registration forms. These documents assist in information flow and documenting authorization as permitted by the head of department.

4.1.4 Preparation Process

During the preparation process, the investigators prepared all relevant equipment requirements, ranging from hardware to software. The resources and equipment used are described in Table 3.

Table 3 List of Resources and Equipment Prepared for the Investigation

Resources (Item)	Purpose of the Resources
• Two forensically clean drives	Used as a destination to store the imaged hard disk for processing. The second drive is a backup used to store the copy of the imaged hard disk, in case the destination drive is corrupted or compromised.
• Tableau TD2 forensic duplicator (2013)	Used for imaging the hard disk without compromising it.
• Hardware-based write blocker device	This ensures that Windows does not alter the suspect's hard disk when attached to the computer.
• A blank DVD	Used to provide a copy of the potential digital evidence obtained during the investigation.
• A digital camera	A digital camera used to take photographic images of the evidence and crime scene.
• A faraday bag	A faraday bag used to package potential digital evidence during the digital evidence collection process.
• A USB Dongle	A USB Dongle plugged into the investigator's computer in order to run Access Data FTK in full mode.
• Forensic Toolkit (FTK) 3.2 imager	FTK imager used to preview recoverable data from a disk. It is also used to create perfect copies, called forensic images.
• Software products keys	Ensures that the software application is genuine

4.2. Acquisitive Processes

This class includes incident scene documentation, potential digital evidence identification, digital evidence collection, digital evidence transportation, and digital evidence storage processes. During the processes in this class, the investigators physically interacted with the all the materials necessary to supplement the investigation process, providing for each of the HDFIP model processes in the case study. These processes make up the third class within the HDFIP model and are explained in the subsections to follow.

4.2.1 Incident Scene Documentation Process

During this process, the investigators took photos and videos of the scene. Documentation of the scene was conducted, information flow was facilitated and the chain of custody of the digital evidence was observed by ensuring that none of the items found at the workstation were tampered with. In the process of documenting the scene, investigators have the option of utilising sketches to complement notes, photos and videos taken during this process. Sketches serve the purpose of providing accurate information concerning the scene documented. In this paper, though, due to the nature of case study, the investigators did not draw any sketches, as it was unnecessary at the time of the investigation. The investigators, however, took photos and videos of the incident scene, which in this case were of the investigated employee's workstation. After completing the scene documentation, the investigators proceeded to evidence identification.

4.2.2 Potential Digital Evidence Identification Process

During potential digital evidence identification process, the investigators identified the potential evidence to be collected, as well as the log files retrieved by the first responder. The investigators

identified the desktop computer as the physical source of potential evidence. The desktop was using the Windows XP operating system, professional edition. The hard disk identified was a SATA (Serial Advanced Technology Attachment). SATA is a computer bus interface that connects host bus adapters to mass storage devices such as hard-disk drives. The hard-disk file system type was NTFS (New Technology File System), of 80-gigabyte storage capacity.

4.2.3 Digital Evidence Acquisition Process

During the collection of potential evidence, the investigators documented all the potential evidence. Collected potential evidence was clearly labelled and all the serial numbers of the potential evidence identified during potential digital evidence identification process. The head of the department signed an acknowledgement receipt for the potential evidence collected. The collection of the potential evidence involved packing the evidence for transportation into evidence bags (faraday bags have a unique identification number) and labelling each item correctly as it was collected from the incident scene.

4.2.4 Digital Evidence Transportation Process

During the digital evidence transportation process, the investigator can transport a physical device by following the traditional procedures, or transport captured digital evidence remotely using a secured transportation link (FTP/TCP). The transportation of the potential digital evidence collected for this case study was from Company X located in Midland to the Digital H offices located at the University of Pretoria. Digital H used a private vehicle to transport the potential digital evidence collected from Company X. The investigators were present during the transportation of the potential evidence collected.

4.2.5 Digital Evidence Storage Process

On arrival, the seized desktop and the hard disks were stored in a secured locker. Access to the locker was limited to the investigator handling the case. An evidence ledger was opened to keep track of the evidence brought in and of who interacted with the potential evidence. Photos of the potential evidence were taken, showing that the evidence had not been tampered with during transportation and that the hard disk was placed in a faraday bag. The evidence was stored and ready for further investigation.

4.3. Investigative Class

The investigative class comprises the processes of digital evidence analysis, digital evidence interpretation, reporting, presentation, and investigation closure. Data analysis and uncovering the digital evidence were conducted during the investigation. Each of the identified processes in this class is explained in the subsections that follow and cover the fourth class of the HDFIP model.

4.3.1 Digital Evidence Analysis Process

The potential evidence is moved from the locker and the chain of custody is maintained by ensuring that the potential evidence is signed out and documented. Photos of the potential digital evidence are taken again to show that the faraday bag was not tampered with while in storage. To maintain the integrity of the photos a logbook is kept to show and maintain the chain of custody and the state of the evidence. The faraday bag was opened and the hard disk containing the potential evidence was removed and documented. Access Data FTK Imager 3.2 (2013) was used to image the hard disk, a physical acquisition was conducted on the hard disk. Note that physical acquisition is a method for acquiring images such as deleted data or lost data for data recovery.

The file format of the image used was (E01). A pre-hash (MD5 and SHA1 checksum) was also conducted on the image. This pre-hash is conducted at the beginning of the imaging process. A back-up hash was conducted to verify that the original image had not changed. The pre-hash and backup

hash are both conducted by the investigator. A third party conducts a third hash value called post-hash, to verify that the image has not been tampered with in any way possible. The hard disk containing the image was processed using the Access Data FTK 4.0 toolkit (2013) to conduct an analysis of the data retrieved, as requested by Company X. The analysis managed to extract potential digital evidence such as electronic documents, photos, internet history and videos.

The hard disk was imaged using image type format of E01. E01 is a complex format that requires more time to generate the required image. A hard disk of high volume will definitely require more imaging time than a hard disk of low volume; hence imaging time will vary based on the size of the hard disk. The hard disk was imaged externally as it was connected to a hardware-based write blocker. The imaging speed varies with the size of the hard disk. The size of the hard disk involved in this case study was 80 gigabyte. The process that follows is the interpretation of the digital evidence extracted during the analysis process.

4.3.2 Digital Evidence Interpretation Process

The interpretation of the data recovered from the hard disk showed that the suspect in question was abusing company resources for personal purpose, and had further violated the company's policy of disallowing pornography downloading. The data extracted was 40 gigabyte in volume during the digital evidence analysis process. A copy of the potential evidence recovered was provided and a report was compiled.

4.3.3 Reporting Process

The results obtained from the interpretation process showed that the employee of Company X had violated company policy with regard to internet usage. The evidence found included photos, documents and videos. The investigators wrote a report detailing all the processes and all the different techniques used during the investigation. Relevant information concerning the findings was clearly stated in the report. The interaction with the potential evidence by the investigators was elaborated on in a forensically sound manner, hence providing accountability by the investigators. The investigators presented the report to all the stakeholders involved in this particular case.

4.3.4 Presentation Process

The presentation process involves presenting data analysed from the digital evidence interpretation process, which can be presented in the form of expert reports, depositions, and testimony to the various stakeholders. The report contains all the documentation and processes carried out during the investigation process. It is very important that during the presentation process all the processes are used to verify that the investigation was conducted in a forensically sound manner. Therefore, the investigators involved in the case study did a presentation of the report compiled before the investigation closure process.

4.3.5 Investigation Closure Process

All the evidence collected during the investigation process was returned to Company X. Company X proceeded to make a decision based on the company's policy. Digital H archived the case for future reference after the investigators had logged the case file as completed and filed it with other post mortem digital forensics investigation cases.

5. FINDINGS AND RECOMMENADATIONS OF THE HDFIP

This section of the paper discusses the overall effectiveness and properties of the HDFIP model. The case study used provided insights into the effectiveness of the HDFIP model. The findings and recommendations focus on the HDFIP and not on the case study used in this paper. During the testing and evaluation process, the HDFIP model was found to be efficient as it allowed the investigators to account for every action conducted through the iterative structure of the investigative process. The

concurrent processes ensured that each step conducted during the investigation was documented and each interaction was accounted for by clearly adhering to the rules and norms of conducting a forensically sound investigation.

The HDFIP model inherits a number of properties from already existing theories, frameworks and process models. The properties inherited by the HDFIP model assisted in the development of new principles called the concurrent processes, as shown in Figure 2. The concurrent processes were adequately adaptable during the post mortem digital forensic investigation. More importantly, the concurrent processes assisted in the preservation of integrity, confidentiality and availability of the potential evidence.

The HDFIP model was found to be effective and applicable when used during a post mortem digital investigation. Moreover, the processes allow for interdependence among the individual classes. During the investigation, the investigators retraced back to the digital evidence analysis process to verify that the potential evidence acquired had not been compromised and the image extracted matched the hash values generated during the digital evidence analysis process.

Since it is a draft standard, it is hoped that the HDFIP model will eventually be adopted internationally, making it easier to compare and contrast the results of digital investigations, even when performed by different investigators or organizations across different jurisdictions (Sitaraman and Venkatesan, 2006).

Note that it would have been possible to investigate this case study using models other than the HDFIP model shown in Table 1. However, the HDFIP model would be more effective, due to the harmonization effort that went into it and the properties inherited by the HDFIP model from all those other models. The HDFIP model comprises 14 harmonized phases (subprocesses) as indicated in Table 1, encapsulating all of the existing processes.

6. CONCLUSION

The problem addressed in this paper was the lack of testing and evaluation of digital forensic investigative process models before their fully being applied in the domain. The harmonized digital forensic investigation process model was thus tested, with the results presented in this paper. The HDFIP model adequately accommodated the testing and evaluation of the post mortem digital forensic investigation.

The authors believe that this paper is a stepping stone towards the standardization of the digital forensic investigation process, the HDFIP being a model that contributes to the reduction of disparities currently being experienced within the field of digital forensics. In the authors' opinion, the harmonized digital forensic investigation process successfully maintained the properties and features that are of importance during an investigation process such as integrity, confidentiality and availability. This investigation was conducted focused on a post mortem investigation. Further testing and evaluation on other types of digital investigation environments such as live digital forensics, mobile forensics, and network forensics, needs to be conducted using the HDFIP.

Future work is intended to include more comprehensive testing and evaluation over many different case studies, in order to test and evaluate the potential error rate of the HDFIP model (Daubert, 1993).

ACKNOWLEDGMENT

This work is based on research supported in part by the National Research Foundation of South Africa (Grant specific unique reference number (UID) 85794). The Grant holder acknowledges that opinions, findings and conclusion or recommendations expressed in any publication generated by NRF-supported research are those of the author(s) and that the NRF accepts no liability whatsoever in this regard.

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 HDFIP model with various devices, as described above.

REFERENCES

Access Data FTK 4.0. (2013). http://www.accessdata.com/products/digital-forensics/ftk

ACPO Good Practice Guide for Computer-Based Evidence. (2008). Retrieved from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Ademu, I. & Imafidon, C. (2012). The need for digital forensic investigation framework. *International Journal of Engineering Science & Advanced Technology*, *2*(3), pp 388-392.

Ademu, I.O., Imafidon, C.O., & Preston, D.S. (2011). A new approach of digital forensic model for digital forensic investigation. *International Journal of Advanced Computer Science and Applications* (*IJACSA*), *2*(12), 175-178.

Ball, C. (2007). Computer forensics for lawyers who can't set a digital clock. Retrieved from http://www.craigball.com/_OFFLINE/CF4_0807.pdf

Beebe N. L., & Clark G. J. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, Digital Investigation 2.

Carrier, B., and Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2) [Electronic version].

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

Eoghan, C., & Curtis W. R. (2010). Chapter from Forensic Analysis in Handbook of Digital Forensics and Investigation.

Cohen, F. (2011). Fundamentals of digital forensic evidence. *Handbook of Information and Communication Security*.

ISO/IEC 27035. (2014). Information technology – Security techniques – Information security incident management.

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

ISO/IEC 27040. (2014). Information technology – Security techniques – Storage Security.

ISO/IEC 27041. (2014). Information technology – Security techniques – Assurance for digital evidence investigation methods (draft).

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

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

Jansen, W., & Ayers, R. (2006). Guidelines on cell phone forensics. *National Institute of Standards and Technology*, Special publication, 800-101.

McDougal, M. (2006). Live forensics on a windows system: Using windows forensic toolkit (WFT), Fool Moon Software and Security. Retrieved from http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf

Mandia, K., Prosise, C., & Pepe. (2003). Incident Response & Computer Forensics (2nd Ed.). McGraw-Hill/Osborne, Emeryville.

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

Reith, M. Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence.*

SATA, Serial Advanced Technology Attachment. Retrieved from http://www.hdat2.com/

Seamus, O., & Cuardhuain. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1).

Selamat, S.R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework, *International Journal of Computer Science and Network Security*, *8*(10), 163-169.

Sitaraman, S., & Venkatesan, S. (2006). Computer and Network Forensics. *Digital Crime and Forensic science in cyberspace*, 55-74.

The U.S. Department of Justice. (2001). *Electronic crime scene investigation: A guide for first responders.*

Valijarevic, A., & Venter, H.S. (2012). Harmonised digital forensic investigation process model. Proceedings of the Annual Information Security for South Africa (ISSA, 2012) Conference.