Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations

Reza Montasari[1(✉)], Pekka Peltola[2], and David Evans[1]

[1] Derby University, Derby, UK
{r.montasari,d.f.evans}@derby.ac.uk
[2] Nottingham University, Nottingham, UK
pekka.peltola@nottingham.ac.uk

Abstract. Contrary to traditional crimes for which there exists deep-rooted standards, procedures and models upon which courts of law can rely, there are no formal standards, procedures nor models for digital forensics to which courts can refer. Although there are already a number of various digital investigation process models, these tend to be ad-hoc procedures. In order for the case to prevail in the court of law, the processes followed to acquire digital evidence and terminology utilised must be thorough and generally accepted in the digital forensic community. The proposed novel process model is aimed at addressing both the practical requirements of digital forensic practitioners and the needs of courts for a formal computer investigation process model which can be used to process the digital evidence in a forensically sound manner. Moreover, unlike the existing models which focus on one aspect of process, the proposed model describes the entire lifecycle of a digital forensic investigation.

Keywords: Computer forensics · Digital forensic investigations · Process model · Computer crime · Formal framework · Incident response

1 Introduction

Nowadays, the nature of evidence presented in courts of law tends to be less likely paper-based considering the ubiquitous nature of information technology [1, 16]. Evidence of computer crime differs from that related to traditional crimes for which there are well established standards and procedures [1, 16, 17]. There does not exist a comprehensive digital investigation process model that is widely accepted by the digital forensic community and courts of law and which covers the entire lifecycle of digital forensic investigation processes. In many cases, digital forensic practitioners rely mainly on ad-hoc tools to carry out digital investigation. Examples of ad-hoc models include models developed by authors in [1–6]. The lack of a standardized digital investigation process model is not an isolated flaw within the field of digital forensic science. Cohen [7] states that the entire field of digital forensic still lacks agreements in fundamental areas. This might be due to the fact that the digital forensic field is still a very new discipline. A study conducted by Cohen [7, 8] on the level of

H. Jahankhani et al. (Eds.): ICGS3 2015, CCIS 534, pp. 83–95, 2015.
DOI: 10.1007/978-3-319-23276-8_8

consensus in foundational elements of digital evidence investigation revealed that the use of common definitions and common language are lacking.

The fact that there exists a lack of common definitions and language is also pointed out by other researchers such as [1–3, 9, 10]. Moreover, many other researchers in the field have increasingly been calling for scientific approaches and formal methods for describing the computer investigation processes [8, 11–14]. By implementing an integrated and comprehensive computer investigation process model, this paper will be of great value to the computer forensic practitioners. Moreover, as Adams et al. [1] state, the development of such a model will establish a starting point from which other investigators and researchers in the field will be able to continue to advance the field's scientific credentials.

2 Related Work

2.1 Background

The main objective of a Computer Forensic Investigation Process Model or CFIPM is to assist the investigator in explaining how particular digital evidence is found on a device [1, 9, 20]. Although various CFIPMs exist in the current literature, the CFIPM processes and terminology have not been formally standardized up to date. Previously attempts to standardize the computer investigation process models appear to have failed due to various reasons. The main rationale behind these failed attempts is the fact that the authors have utilised their own terminology without attempting to identify the most common language that can be accepted unanimously by the digital forensic investigators.

The Table 1 describes the phases covered within the conducted research up to date. Like any other types of evidence, courts of law do not assume that digital evidence is valid and reliable without some empirical testing in relation to theories and techniques associated with its production [1, 18]. Courts of law take a careful notice of the way and process in which the digital evidence acquisition and storage were carried out [7, 18, 19]. The concept of admissibility refers to the fact that the courts need to verify whether the digital evidence is sound to be placed before a jury and will help to deliver a solid base in terms of making a decision in the case [20]. Courts in the U.K. and U.S. require the investigators and "proponent" of digital evidence to lay the proper foundation for its admissibility. They are concerned with the reliability and authenticity of such digital evidence [20, 21]. However, if forensic investigator is not able to present his/her evidence in a coherent and understandable way to the layperson such as judge and jury, the case may be lost [22]. The complexity of methodologies and software used to extract digital evidence requires the digital investigator to explain the evidence in such a way that judge and jury understand it [19].

Authors in [20, 23, 24] argue that while the actual mechanics of digital forensics are different from the better-known physical and medical forensics, the processes of all forensic sciences are fundamentally the same. Cohen [7, 8] states that judges need to keep out the poor-quality digital evidence from the courtroom. Regardless of the digital evidence or physical evidence, a forensic report must contain conclusions that can be reproduced by independent third parties. Reports based on accurately documented digital sources are much more likely to withstand the judicial scrutiny than opinions based on less reliable sources [25]. In the absence of something better, judicial systems might apply methods used to test scientific evidence into digital evidence presented before them [19, 26]. The digital forensic discipline was developed without any initial research required for a thorough scientific ground essential for permitting digital forensic evidence [27–29]. In 2004, Meyers et al. [28] warned that digital forensics is branded as "junk science" because of the absence of certifications, standards or peer-reviewed methods. Although this reference dates back to 2004, the issue of the lack of standardisation and consensus concerning process models regarding terminology, phases and types of activities within a process model still remain. This is pointed out by the latest reference such as [1, 7–10].

A careful and detailed examination of the literature has revealed a gap that there does not exist a comprehensive digital investigation process model which is widely accepted by the digital forensic community and courts of the law. The existing models are considered to be ad-hoc tools as opposed to formal models [1–3, 7, 8, 23, 24, 30–35]. For instance, Beebe et al. [33] state that a more comprehensive and generally accepted framework is needed to enhance scientific rigor and to facilitate education, application and research. Referring to the level of consensus in foundational elements of digital investigation process amongst researchers in the field, Cohen [8] states that the use of common language is lacking, and the consensus can be found present only after the definitions are made explicit. The United States Computer Emergency Readiness Team [30] states, "Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry." Ciardhuáin [34] states that a complete and inclusive model should have general advantages for IT managers, auditors and others who are not necessarily implicated with the legal process because of growing occurrences of crimes implicating computers. Ciardhuáin [34] further states, "A comprehensive model of cybercrime investigations is important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators". This is further supported by the authors in [1, 9]. Moreover, Zainudin et al. [10] state that one of the most significant problems that digital investigators encounter is the absence of standardisation in the field of computer forensics. Karyda et al. [36] state that utilising ad-hoc methods and tools for the extraction of digital evidence can undermine the reliability and credibility of digital evidence.

Therefore, to deal with these shortcomings and to fill the gap, we propose an Integrated Computer Investigation Process Model ICFIPM which deals with the process of digital evidence in computer crime investigations. Very few researchers have previously attempted to develop standardised computer investigation process models. These attempts have failed due to various reasons [1–3, 9, 10]. One of the reasons is due to the fact that researchers tend to use their own terminology and different types of activities in the models. Moreover, the existing models are not complete by covering the entire processes involved in a computer crime investigation. For example, the model developed by Adams et al. [1] is based only on the "Analysis" phase and partially on the "Preparation" phase. The model does not include phases related to Preparation, Incident Response or Documentation.

2.2 Review of the Existing Models

Due to the space constraint, it is not possible to present a description of all the previously developed Computer Forensics Process Models which were reviewed by the authors prior to developing the proposed model. Although a description of only four reviewed models is provided in this paper, it should not be denoted that the proposed model is based on only these four models. On the contrary, the proposed model is the integration of almost all the existing developed models. Nevertheless, a comprehensive analysis of these models is represented in Table 1.

Carrier et al. (2003). The model proposed by Carrier et al. [15] is called "An Integrated Digital Investigation Process". This model is organised into 5 groups consisting of Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation and Review. Although this model dates back to 2003, it is still one of the most prominent DFPMs to date [1, 9]. This is due to the fact that it included physical crime scene investigation in the model and drew a clear distinction between physical crime scene and digital crime scene investigation. However, the model's practicality in real life has been challenged by other digital forensic experts such as authors in [9, 37]. This model has not differentiated the primary crime scene (where the digital crime initiates) from the secondary crime scene (the target computer). This is not part of the physical or digital forensic investigation in this model. Therefore, computer forensic investigation based on this model will not consist of the outcome of the nefarious activity; this will affect the reconstruction of events and subsequently results in incomplete findings in the presented report [9].

Baryamureeba et al. (2004). Baryamureeba et al. [37] proposed "The Enhanced Integrated Digital Investigation Process (EIDIP)". This model is built upon the previous model proposed by Carrier et al. [15]. The phases of this model include: Readiness, Deployment, Traceback, Dynamite and Review phases. In their model, Baryamureeba et al. [37] aim to address the flaw in Carrier et al.'s [15] model by including an investigation of the primary and secondary crime scenes. Baryamureeba et al. [37] adds a new sub-phase in which the primary crime scene is identified in the Traceback phase [9]. Moreover, in this model, reconstruction is conducted after all the evidences have been collected. Apart from differentiating between primary and secondary crime scene, this model offers no other contributions.

Beebe et al. (2005). Beebe et al. [33] proposed a model, "A Hierarchal, Objectives-Based Framework for the Digital Investigation Process". This model consists of Preparation, Incident Response, Data Collection, Data Analysis, Findings Presentation and Incident Closure Phases. Beebe et al. [33] suggest the concept of objectives-based tasks in which the investigative goals are utilised to select the analysis tasks.

Although in contrast with other models, this model is more detailed by introducing sub-phases and objectives-task hierarchical structures, it still has various shortcomings. These include the fact that its first-layer phases are mainly non-iterative not allowing the investigators to return to the previous phases. Moreover, as the authors themselves state, the model's low level details is not complete as the model includes sub-tasks only

Table 1. Analysis of the existing digital investigation process models up to date.

No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Authors	Pollitt	Casey	Lee et al.	Palmer et al.	Reith et al.	Mandia et al.	Carrier et al.	Stephenson	Ciardhuáin	Casey et al.	Baryamureeba et al.	Carrier et al.	Beebe et al	Kohn et al.	Kent et al.	Ieong, R	Freiling, F	Grobler et al.	Zainudin et al.	Alharbi et al.	Yusoff et al.	Ćosić et al.	Agarwal et al.	Roger et al.	Valjarevic et al.	Saleem et al.
Year	1995	2000	2001	2001	2002	2003	2003	2003	2004	2004	2004	2004	2005	2006	2006	2006	2007	2010	2010	2011	2011	2011	2012	2012	2012	2014
Digital Investigation Process Model	Computer forensics: an Approach to Evidence in Cyberspace	Digital Evidence and Computer Crime	Model of Scientific Crime Scene Investigation	DFRWS – Investigative Process for Digital Forensic Science	An Abstract digital Forensics Model	Incident Response & computer Forensics	An Integrated Digital Investigation Process	End to End digital Investigation Process	An Extended Model of Cybercrime Investigations	Digital Evidence and Computer Crime	The Enhanced Digital Investigation Process Model	An Even-Based Digital Forensic Investigation Framework	A Hierarchical, Objectives-Based Framework for the Digital Investigations Process	Framework for a Digital Forensic Investigation	Guide to Integrating Forensic Techniques into Incident Response	FORZA – Digital Forensics Investigation Framework That Incorporates Legal Issues	A Common Process Model for Computer Forensics and Incident Response	A Multi-Component View of Digital Forensics	A Digital Forensic Investigation Model for Online Social Networking	The Proactive and Reactive Digital Investigation Process: A systematic Literature Review	Common Phases of Computer Forensics Investigations Models	Chain of Digital Evidence Based Model of Digital investigation Process	Systematic Digital Investigation Process Model	Multi-Perspective Cybercrime Investigation Process Modeling	Harmonised Digital Investigation Process Model	Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles
Readiness							✓				✓						✓	✓								
Identification	✓		✓	✓	✓					✓				✓	✓			✓	✓	✓		✓		✓		
Detection				✓			✓				✓		✓				✓							✓	✓	
Preservation		✓	✓	✓	✓			✓		✓	✓		✓		✓	✓				✓	✓		✓	✓	✓	✓
Evidence Collection			✓	✓	✓	✓		✓	✓		✓		✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓
Examination				✓	✓				✓				✓	✓	✓							✓	✓			✓
Analysis				✓	✓	✓				✓	✓		✓	✓	✓		✓	✓			✓		✓		✓	✓
Evidence Acquisition	✓									✓					✓	✓		✓		✓	✓			✓		
Preparation					✓								✓									✓			✓	✓
Approach Strategy					✓				✓				✓	✓			✓									
Forensic Duplication																	✓									
Recovery						✓		✓		✓			✓				✓									
Survey						✓	✓				✓		✓			✓			✓				✓			
Interview																✓										
Deployment							✓				✓															
Approved Methods				✓				✓		✓																
Authorisation				✓		✓	✓	✓	✓	✓												✓			✓	
Harvesting																	✓									
Organisation																	✓									
Classification		✓																								
Sampling				✓				✓																		
Seizure				▨				▨		✓						✓		✓								
Data Reduction				✓				✓		✓							✓									
Compression		✓	✓	✓				✓																		
Presentation			✓	✓	✓		✓		✓		✓		✓	✓			✓	✓	✓		✓		✓	✓	✓	✓
Documentation		✓	✓	✓			✓				✓	✓		✓		✓		✓					✓		✓	
Live Data Collection																							✓	✓		
Trace Back											✓					✓										
Dynamite											✓															
Decision/Resolution				✓													✓						✓			
Returning Evidence					✓																					✓
Physical Crime Scene Investigation							✓				✓	✓						✓						✓		
Digital Crime Scene Investigation							✓				✓	✓						✓						✓		
Review							✓				✓								✓				✓			
Operational Readiness							✓																			
Infrastructure Readiness							✓																			
Notification							✓		✓		✓			✓					✓							
Evidence Search							✓		✓	✓	✓			✓				✓	✓							
Event Reconstruction		✓	✓				✓				✓	✓	✓					✓				✓				
Awareness/Report									✓				✓													
Hypothesis									✓										✓							
Proof & Defence									✓										✓							
Confirm							✓				✓		✓					✓								
Record															✓											
Package													✓		✓											
Transport									✓				✓	✓					✓		✓	✓			✓	
Store									✓				✓	✓					✓		✓	✓			✓	
Communication											✓															
Incident Response													✓				✓	✓							✓	
System Restoration																		✓								
Evaluation	✓		✓																							
Incident Closure													✓					✓				✓		✓		
Dissemination									✓																	

for the Analysis phase. Beebe et al. [33] call for their model to be extended by including sub-phases for other first-layer phases included in the model.

Ciardhuain (2004). The model developed by Ciardhuain [34] is considered to be the most comprehensive model proposed to date [1, 7, 9, 13]. This model consists of Awareness, Authorisation, Planning, Notification, Search for and identify evidence, Collection of evidence, Transport of evidence, Storage of evidence, Examination of evidence, Hypothesis, Presentation of hypothesis, Defense of hypothesis, Dissemination of information phases. The terminology used in this model is similar to the terminology used in the previously proposed models. Although this model is considered to be the most comprehensive model proposed to date, it has various shortcomings. The model is mainly aimed at information flow and the digital investigations within the field of commerce. It is not designed in a way which can be implemented in different settings. Moreover, the model does not allow the investigators to return to the previous phases.

2.3 Discussion of the Existing Models

The existing DFIPMs are not complete in that they do not cover the entire digital investigation processes. Moreover, they have differing approaches by lacking common terminology, language and the types of activities that are widely agreed upon by the digital forensic community. For example, a comparison of the set of activities included under Examination phase in Casey's [20] model and Cohen's [9] model respectively revels the problem in terms of standardization.

Casey:

Examination: Recovery → Harvesting → Reduction → Classification

Cohen

Examination: Analysis → Attribution → Reconstructing

As seen, clearly not a single sub-process within the two identified sets has the same meaning. A possible explanation for this discrepancy is that the interpretations of the terms examine and analysis has been exchanged by the authors [9]. Therefore, in order to acquire the digital evidence in a forensically sound manner, it essential to develop a model based on scientific and formal methods.

3 Methodology

In order to create a consistent research environment and to carry out a successful research, various methodologies were considered. The reason for selecting Design Science Research Process (DSRP) methodology over other alternatives lies in the fact that it is especially suited for the task of designing and developing a new process model. Armstrong [38] states that design science is an ideal approach in the problem domain of digital forensic evidence with its focus on designing solutions [1]. Researchers within information system research have been widely applying the DSRP. Moreover, this methodology has been previously adopted by other researchers in similar situations and has proved to be effective [1, 39, 40]. The DSRP is related to the development and subsequent evaluation of IT artefacts within an organisational environment in order to solve specific problems [39, 41]. The artefacts in question can consist of models, constructs and methods [1].

Also, in order to represent the proposed Integrated Computer Forensic Investigation Process Model (ICFIPM) discussed in this paper in a uniform and consistent manner, we considered various visual and formal representations. These consisted of UML Activity, Use Case Diagrams and Finite State Machines. However, we decided to use Sequential Logic formulated by More et al. [42]. The reason for choosing this representation is due to the fact that ordering of the phases and sub-phases are critical in the proposed model. Kohn et al. [9] state, “In order for the circuit to evaluate true, all the conditions of the previous states must be true.” This means that the circuit will fail if the current state is not positively completed [9, 42]. This will enable the investigator to revisit previous steps in the process; however, he or she will not be able to continue if a step is not complete or fails. The ordering of the phases and sub-phases are critical in the proposed model. This is because the circuit outcome is dependent on the input and the current internal state – note that in this context, we refer to a phase or sub-phase as a circuit. This methodology has been previously applied in Kohn et al. [9] work and has proved to be effective. In their work, Kohn et al. [9] adapt the sequential logic notation formulated by More et al. [42] in order to represent each of the DFPMs in which Kohn et al. [9] replace the list values with the process steps. We aim to utilize the sequential logic notation adapted by Kohn et al. [9].

4 Contribution of the Paper

This paper proposes a computer forensics process model which rationalizes terminology as well as synthesizes phases and activities included in a process model. The model is simple enough to use, by having generalised methods that the judicial members or company management can use to relate technology to non-technical observers.

5 Proposed Computer Forensics Model

All the prominent models developed since 1997 up to 2014 have been critically analysed. This was to identify and integrate the essential components and terminology agreed upon by the digital forensic community to include in the proposed model. The rationale in doing so is multifaceted. Firstly, we aimed to leverage the benefits and advantages of previously proposed models. Secondly, in any type of community, it is important to create synergic interaction between different points of view. As the authors in [1, 7–9, 33] state, any framework institutionalized through subsequent intellectual discourse and practical use must take into account differing perspectives, approaches and vernacular. Therefore, we have integrated the previously proposed models to the new uniform model. The soundness of a digital investigation process model is “a function of usability and acceptability” [33]. Therefore, in order to acquire usability and acceptability, we integrated phases, sub-phases, principles and objectives. Phases and sub-phases are obvious; they are individually separate steps in the process which can sometimes be a function of time and are inevitably sequential or sometimes iterative approach. In contrast, principles are encompassing procedures, guidelines and methodological approaches that encompass some or all the eight specified main phases of the proposed model as well as its sub-phases. Principles as opposed to phases are not distinct and discrete steps in the process. Rather, they are aims and objectives needed to be achieved throughout the process. Chain of custody and proper documentations are examples of principles. The phases of a model are tied together through the process model flow accompanied by its investigative principles such as information flow and case management [15, 20, 33, 34].

The proposed model (Fig. 1) shows information flow through phases. Case management and investigative objective are the general factors defining the nature of the phases within the model. First layer phases are distinct and discrete. They are clearly defined, and obvious delineation exists between them. In other words, each given phase has a clear event which initiates it and clear output as the conclusion of the phase [33]. Phases occur in order and are chronological. Some first layer phases are non-iterative within the extent of a single accident.

5.1 Readiness Phase

Forensic Readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation [9, 43, 44]. Organisations need to take certain important steps to prepare to use digital evidence. These include: improved system and staff monitoring, physical and procedural equipment and means to preserve data to evidential standards of admissibility, processes and procedures to ensure that the staff recognise the importance and legal activities of evidence, and appropriate legal advice and interfacing with law enforcement.

5.2 Identification Phase

Identification phase is where the incident or a digital crime is detected and reported either to the incident response team in an organisational context or to the police in the case of ordinary individuals.

5.3 Incident Response Phase

Various activities are involved in this phase. It is the first responders who typically arrive at the crime scene. Every investigation is different, and it is unlikely to decide what the first responders will encounter at the crime scene. In this phase, the potential suspects need to be detained. The first responders will then need to assess and confirm the incident and notify the incident to the right authority i.e. management in the company or police. Based on the result of this phase right equipment and personnel are deployed and a response strategy is drawn.

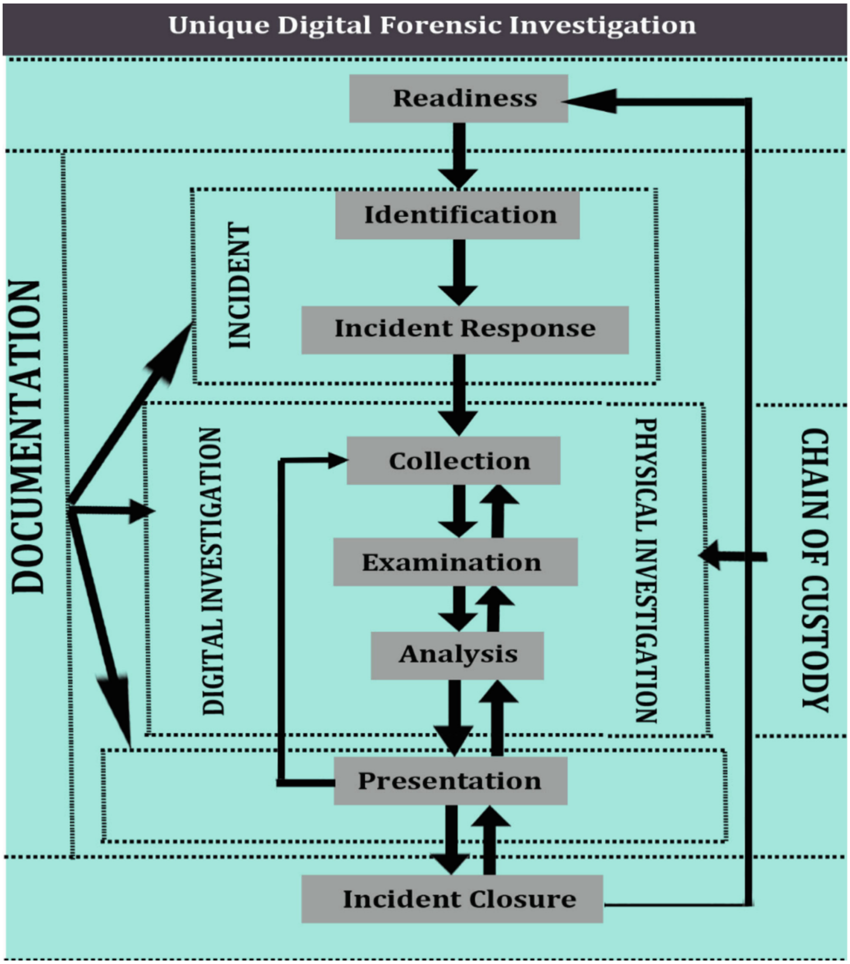

Fig. 1. The proposed integrated computer forensic investigation process model

5.4 Collection Phase

The collection phase involves searching the physical crime scene and identifying the digital media containing potential digital evidence. Upon the identification, the examiner performs a live digital data acquisition by imaging the volatile data and authenticating it using checksum verifications (MD5 and SHA1). This is to ensure the legal validity of the digital evidence. If the digital media cannot be seized in cases of server in large organisations, then the examiner also needs to perform a live digital data acquisition of the logical drive of the server. If the search warrant permits the removal of the digital media, the media is seized and taken away for laboratory digital data acquisition.

5.5 Examination Response

In this phase, the digital forensic examiner conducts the laboratory static digital data acquisitions on the seized digital media. He/she then performs a detailed examination of the images of the volatile and static data already collected. Examination is the process where the digital investigator makes the digital evidence visible or extracts the data into human readable form [9]. Files such as partially deleted files are identified from the original digital media through the Examination phase. Obscured data which might be hidden or deleted is processed by utilizing sound digital forensic techniques and tools such as FTK or Encase to carry out effective investigation. After the data is rendered visible, it is then harvested by giving a logical structure to the entire data set. The deleted files processed during the examination will become visible to the extent that they were discovered during examination [7, 9, 15, 20]. The investigator will then need to authenticate the raw data to ensure that the copied raw data is the same as the original data. The harvested data can then be mounted and read by the original file system such as NTFS.

5.6 Analysis Phase

After the examination has been carried out, the digital investigator needs to construct a hypothesis of what occurred. The extent of the formality of the hypothesis is dependent on the type of investigation. The digital investigator should expect to backtrack to the Examination phase because the investigator develops more detailed understanding of the events resulting in investigation in the first place. During this phase, the digital evidence is organised to accelerate the digital forensic investigation by concentrating on identified incident type and data categorised. Moreover, during this phase, the investigator should perform a detailed investigation of the organised data and test it against the hypothesis which he/she has formulated. During this phase, the legal validity of potential digital evidence is questioned by taking into account admissibility, weight and relevance [9, 15, 20, 34].

5.7 Presentation Phase

The developed hypothesis needs to be presented to people other than the investigators. For a law enforcement case, the hypothesis will be placed before a jury whereas as an internal company investigation puts the presentation before the management for a decision to be taken. Other activities involved in this phase include proof and defence. Often the hypothesis will be challenged; the defence will provide a contrary hypothesis before the jury. The investigators will need to prove the validity of their hypothesis and defend it against criticism and challenge. If the challenges are successful, the digital investigator will then need to backtrack to earlier stages in order to acquire and examine more evidence and to develop a better hypothesis.

5.8 Incident Closure

The final phase of the proposed model is the Incident Closure phase, where the case is officially closed. The result of the investigation is utilised to review the existing policies and procedures of the organisation. The original digital evidence either must be destroyed or must be returned to its rightful owner. In this phase, lessons should be learnt, and recommendations be made. A case study should be developed to assist future investigations. The case study can consist of i.e. the type of attack and perpetrator's skills set etc. Dissemination is an important activity in this phase; some information might be made available within the organisation whereas other information might be more widely disseminated. This information also will influence future investigations as well as policies and procedures.

6 Conclusions and Future Work

Various digital investigation process models in the literature were identified and compared. The results revealed that none could be considered standard since they all have differing approaches. The essential and most agreed-upon components of the existing models were identified and incorporated into the new model. Although the model is represented in its first-layer phases, the final product of this research will be a model which represents the detailed model consisting of sub-phases and activities. We contend that our model is not just a merging of the existing models. We have clarified the terminology and have added further essential phases to the model.

The proposed model will be standardized by identifying and incorporating into the proposed model the terminology and activities that the researchers and practitioners in the field of digital forensic community agree upon. Similarly, in order to make the model generic in a way which it can be used in different fields of digital forensic and for any type of cybercrime, we will combine different models developed separately for different fields of digital forensic including law enforcement, third party providers of digital forensic services and incident response. The proposed model in this paper has been presented in its high level phases (first-layer). As a future work, the authors are in the process of extending the proposed model to consist of the lower lever sub-phases. This is to conduct further research in order to determine components and activities which are widely accepted by the computer forensics experts for inclusion in the extended process model.

After the extension of the proposed model, it will then be evaluated and tested in two stages in order to assess its usability and utility. The first stage involves using two sets of digital forensic experts within academia and industry, and the second stage involves carrying out a closed network attack and apply the proposed process model to a case study.

References

1. Adams, R., Hobbs, V., Mann, G.: The advanced data acquisition model (ADAM): a process model for digital forensic practice. J. Digit. Forensics Secur. Law **8**(4), 25–48 (2014)
2. Bulbul, H., Yavuzcan, H., Ozel, M.: Digital forensics: an analytical crime scene procedure model (ACSPM). Forensic Sci. Int. **233**(1), 244–256 (2013)
3. Agarwal, A., Gupta, M., Gupta, S., Gupta, C.: Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. **5**(1), 118–130 (2011)
4. Ieong, R.S.C.: FORZA–digital forensics investigation framework that incorporate legal issues. Digit. Investig. **3**, 29–36 (2006)
5. Grobler, C.P., Louwrens, C.P., Sebastiaan, von Solms, H.: A multi-component view of digital forensics. In: ARES 2010 International Conference on Availability, Reliability, and Security. IEEE (2010)
6. Ademu, I., Imafidon, C., Preston, D.: A new approach of digital forensic model for digital forensic investigation. Int. J. Adv. Comput. Sci. Appl. **2**(12), 175–178 (2011)
7. Cohen, F.: Putting the science in digital forensics. J. Digit. Forensics Secur. Law **6**(1), 7–14 (2011)
8. Cohen, F.: Update on the State of the Science of Digital Evidence Examination. In: Proceedings of the Conference on Digital Forensics, Security & Law, pp. 7–18 (2012)
9. Kohn, M., Eloff, M., Eloff, J.: Integrated digital forensic process model. Comput. Secur. **38**, 103–115 (2013)
10. Zainudin, N., Merabti, M., Liwellyn-Jones, D.: Online social networks as supporting evidence: a digital forensic investigation model and its application design. In: International conference on Research and Innovation in Information Systems (ICRIIS), Kuala Lumpur, 23–24 November, pp. 1–6. IEEE (2011)
11. Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G.: Bringing science to digital forensics with standardized forensic corpora. Digit. Investig. **6**, S2–S11 (2009)
12. Carlton, H., Worthley, R.: An evaluation of agreement and conflict among computer forensic experts. In: 42nd Hawaii International Conference on System Sciences (HICSS), Hawaii, 5–8 January. IEEE, Hawaii (2009)
13. Pollitt, M.: Applying traditional forensic taxonomy to digital forensics. In: Ray, I., Shenoi, S. (eds.) Advances in Digital Forensics IV, vol. 285, pp. 17–26. Springer, New York (2008)
14. Leigland, L., Krings, A.: A formalization of digital forensics. Int. J. Digit. Evid. **3**(2), 1–32 (2004)
15. Carrier, B.: Defining digital forensic examination and analysis tools using abstraction layers. Int. J. Evid. **1**(4), 1–12 (2003)
16. Stanfield, A.: Computer Forensics, Electronic Discovery and Electronic Evidence. LexisNexis Butterworths, Chatswood (2009)
17. Smith, R., Grabosky, P., Urbas, G.: Cyber Criminals on Trial. Cambridge University Press, Cambridge (2009)
18. Mason, S.: Electronic Evidence: Disclosure, Discovery & Admissibility. LexisNexis Butterworths, London (2007)
19. Kessler, C.: Judges' awareness, understanding, and application of digital evidence. Ph.D. thesis. Nova Southeastern University (2010)
20. Casey, E.: Digital Evidence and Computer Crime Forensic Science, Computers and the Internet, 3rd edn. Elsevier, San Diego (2011)
21. The Law Reform: The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales (2009). http://lawcommission.justice.gov.uk/docs/cp190_Expert_Evidence_Consultation.pdf. Accessed 20 Jan 2015

22. Wiles, J. (ed.): The Best Damn Cybercrime and Digital Investigations Book Period: Syngress Publishing Palmer, Gary (2001). A road map for digital forensic research. First Digital Forensic Research Workshop, Utica, New York (2007)
23. Turnbull, B.: The adaptability of electronic evidence acquisition guides for new technologies. In: Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia and Workshop
24. Calhoun, C.: Scientific Evidence in Court: Daubert or Frye, 15 Years Later, vol. 23(37). Legal Backgrounder, Washington, DC (2008)
25. Peisert, S., Bishop, M., Marzullo, K.: Computer Forensics. In: Forensis', Third International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, California, USA (2008)
26. Meyers, M., Rogers, M.: Computer forensics: the need for standardization and certification. Int. J. Digit. Evid. **3**(2), 1–11 (2004)
27. Carrier, B.: Open source digital forensic tools: the legal argument' (2002). http://www.digital-evidence.org/papers/opensrc_legal.pdf. Accessed 6 Jan 2014
28. US-CERT: Computer Forensics (2012). http://www.us-cert.gov/reading_room/forensics.pdf
29. Yussoff, Y., Roslan, I., Zainuddin, H.: Common phases of computer forensics investigation models. Int. J. Comput. Sci. Inf. Technol. **3**(3), 17–31 (2011)
30. Trcek, D., Abie, H., Skomedal, A., Starc, I.: Advanced framework for digital forensic technologies and procedures. J. Forensic Sci. **55**(6), 1471–1479 (2010)
31. Beebe, N., Clark, J.: A hierarchical, objectives-based framework for the digital investigations process. Digit. Investig. **2**(2), 147–167 (2005)
32. Ciardhuáin, O.: An extended model of cybercrime investigations. Int. J. Digit. Evid. **3**(1), 1–22 (2004)
33. Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models. Int. J. Digit. Evid. **1**(3), 1–12 (2002)
34. Karyda, M., Mitrou, L.: Internet forensics: legal and technical issues. In: 2nd International Workshop on Digital Forensics and Incident Analysis, Samos (Greece), pp. 3–12 (2007)
35. Baryamureeba, V., Florence, T.: The enhanced digital investigation process model. In: Proceedings of the Fourth Digital Forensic Research Workshop (2004)
36. Armstrong, C., Armstrong, H.: Modeling forensic evidence systems using design science. In: IFIP WG 8.2/8.6 International Working Conference, Perth, Western Australia (2010)
37. Hevner, A., Chatterjee, S.: Design Research in Information Systems. Springer, New York (2010)
38. Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., Bragge, J.: The design science research process: a model for producing and presenting information systems research. In: Design Science Research in Information Systems and Technology (DESRIST 2006), 24–25 February, Claremont, CA (2006)
39. Rogers, M., Goldman, J., Mislan, R., Debrota, S., Wedge, T.: Computer forensics field triage process model. In: Conference on Digital Forensics, Security and Law (2006)
40. Nair, B.S.: Digital Electronics and Logic Design, 6th edn. Prentice Hall, New Delhi (2006)
41. Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digit. Evid. **2**(4), 1–28 (2004)
42. Tan, J.: Forensic Readiness (2001). http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf. Accessed 20 Jan 2015