A Review and Comparative Study of Digital Forensic Investigation Models

Kwaku Kyei, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl

Information Systems Security Department
Concordia University College of Alberta, Edmonton T5B 4E4, Canada
kwaku.kyei.f@gmail.com,
{pavol.zavarsky,dale.lindskog,ron.ruhl}@concordia.ab.ca

Abstract. In this paper we present a review and comparative study of existing digital forensic investigation models and propose an enhanced model based on Systematic Digital Forensic Investigation Model. One significant drawback in digital forensic investigation is that they often do not place enough emphasis on potential admissibility of gathered evidence. Digital forensic investigation must adhere to the standard of evidence and its admissibility for successful prosecution. Therefore, the techno-legal nature of this proposed model coupled with the incorporation of best practices of existing models makes it unique. The model is not a waterfall model, but iterative in nature helping in successful investigation and prosecution. The result of the study is expected to improve the whole investigation process including possible litigation.

Keywords: forensic investigation process, digital evidence, information sharing.

1 Introduction

Forensic computing and cybercrime investigation emerged as a result of increase in computer or digital crime due to the development of the Internet and proliferation of computer technology. The advancement in technology and the rise in online communication have not only brought about increase in criminal activity (with the use of the computer either a tool or target or both in committing crime) but also poses a challenge to law enforcement agencies on how to investigate these complex and sophisticated crimes. Various investigation models have been developed since 1984 (when the FBI laboratory and other law enforcement agencies began to develop programs to examine computer evidence). Some of these are for incident response and others are for court admissibility, but all were developed in an attempt to investigate and where necessary prosecute offenders. Unfortunately, not much has been achieved since the success rate for the prosecution is less than two percent [1].

The methods and procedural rules governing evidence gathering and investigation in these models vary from place to place. Since cybercrime is often transnational and borderless in nature offenders take advantage of these gaps to avoid arrest and prosecution [2]. Digital forensics is relatively new compared to other forensic

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 314–327, 2013.

disciplines, and therefore there is no common standard of investigation. Each organization and country tend to adopt its own procedures, some focused on the technology aspect, and relegate legalities to the background [3], some focused on the data analysis portion of the investigation or other aspect of the process.

This paper presents a comparative study of the recent Systematic Digital Forensic Investigation Model [4] and other existing models based on the frame of reference (number of phases and activities in the existing models) and try to enhance it by filling in the gaps and omissions identified to make it more comprehensive and suitable for both investigation and prosecution.

2 Review of Previous Models

A number of digital forensic models have been developed for investigations since 1984; some of these focused on either incident response or investigation or emphasize a particular phase or activity of an investigation. Below are brief descriptions of the model development process from 2001 to 2012, see also Fig.1 – Fig.3.

A. Digital Forensic Investigation Model 2001

Kruse & Heiser (2001) came up with a model [5] which has three phases, namely acquiring evidence, authenticating the evidence and analyzing the evidence, popularly referred to as the three A's of digital forensics. This model is concerned with integrity of the evidence, and was designed for incident response.

B. Digital Forensic Research Workshop 2001

The DFRW model [6] is a collective document created at a Research Workshop organized in Utica USA in 2001.The model was made up of seven phases, namely Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. One significant feature of the model was that it was an improvement over previous models because it covered some of the stages others did not cover, such as the presentation stage. It also laid the foundation for digital forensic investigation and a framework for future research.

C. Abstract Digital Forensic Model 2002

Reith, Carr and Gunsch reviewed the DFRW and improved it by adding three more components, which were missing in the previous models. This model [7] was the most comprehensive of the three because it had all the activities of DFIM and DFRW and also added Preparation, Approach Strategy and Return of Evidence. Figure 1 shows the mapping of common elements in the three models and the additions are highlighted in ADFM.

D. Integrated Digital Investigation Model 2004

The Integrated Digital Investigation Model (IDIP) [8] has five phases, namely Readiness (Operational and infrastructural readiness), Deployment (Detection and notification; and confirmation and authorization), Physical Crime Scene Investigation, Digital Crime Scene Investigation and Review. The model applied the normal traditional investigation approach and integrated it into digital forensic investigation. This was quite innovative, especially the reconstruction procedure in both physical and digital crime scene, which is a strategy used to detect cyber criminals [9].

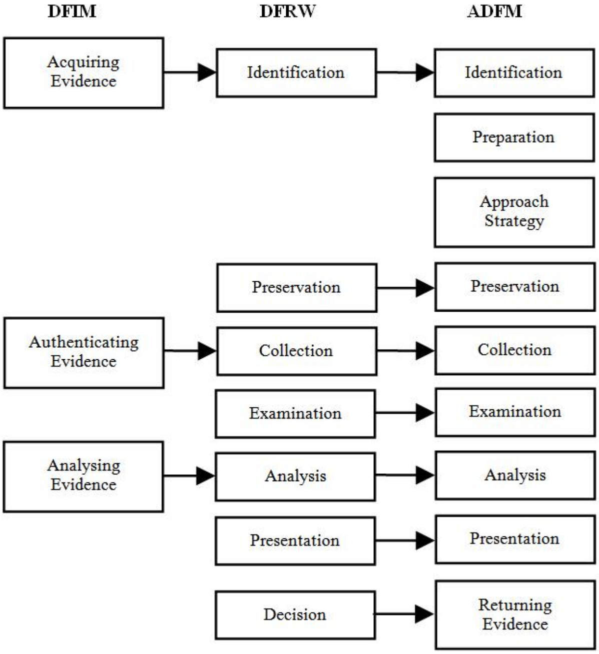


Fig. 1. The digital forensic investigation phases in the DFIM, DFRW and ADFM models

E. Enhanced Digital Investigation Process Model 2004

The Enhanced Digital Investigation Process Model (EDIP) [10] seeks to enhance integrated digital investigation process model by adding two additional steps: Trace back and Dynamite. Figure 2 shows mapping of common elements between the two models. Deployment phase in EDIP has physical and digital crime scenes, which are separate phases in IDIP and in addition introduced other useful activities like Detection & Notification, Confirmation and Submission. Trace back and Dynamite (reconstruction) would enable the investigator to trace the primary crime scene, from the footprint obtained from the secondary crime scene with the sole objective of identifying the possible suspect or criminal, which was a weakness in the earlier model.

F. Extended Model of Cybercrime Investigation 2004

The EMCI model [11] was developed by Seamus O Ciardhuain, who has considerable experience not only in cybercrime investigation but also as a researcher, network administrator and developer of training for investigators in forensic computing. It is made up of thirteen (13) steps, namely Awareness, Authorization, Planning, Notification, Search for and identify evidence, Collection of evidence, Transport of evidence, Storage of evidence, Examination of evidence, Hypothesis, Presentation of hypothesis, Proof/Defense of hypothesis and Archive Storage (used for dissemination of information). The model provides a better understanding of the investigation process and captures most of the information flow for cybercrime investigation.

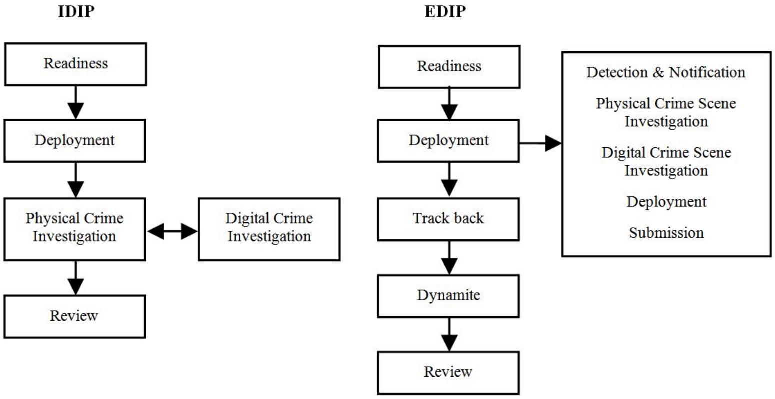

IDIP
Readiness
Deployment
Physical Crime Investigation
Digital Crime Investigation
Review
EDIP
Readiness
Deployment
Track back
Dynamite
Review
Detection & Notification
Physical Crime Scene Investigation
Digital Crime Scene Investigation
Deployment
Submission

Fig. 2. Digital forensic investigation phases in IDIP and EDIP models

G. Digital Forensic Model Based on Malaysian Investigation Process 2009

In 2009, S. Perumal developed investigation model [12] based on cybercrime laws in Malaysia. The model consists of seven phases namely Planning, Identification, Reconnaissance, Transport & Storage, Analysis, Proof & Defense, and Archive Storage. It enhanced existing models by incorporating a live and static data acquisition process that focuses on volatile data. It also introduced data mining in the archive storage.

H. Digital Forensic Model for Digital Forensic Investigation 2011

Inikpi developed another model, (DFMDFI) [13] which was generalized into a 4-tier iterative approach. The first tier was made up of preparation, identification, authorization and communication. The second tier consisted of rules such as collection, preservation and documentation. The third tier was made up of rules like examination, exploratory testing and analysis and the fourth tier has result, review and report. What is significant about this model is that it is iterative, therefore one can revisit any activity or phase when it becomes necessary.

I. The Systematic Digital Forensic Investigation Model 2011

Agawal et al. (2011) [4] developed another model, the SDFIM, that organizes the digital forensic investigation process into eleven phases as outlined in Fig. 3.

Phase 1: Preparation

The preparation phase includes getting the initial understanding of the problem through assessment, and the right equipment. This phase is used to obtain authorization and approval, search warrant, and legal notice must also be given to those concerns and finally appropriate strategy should be developed.

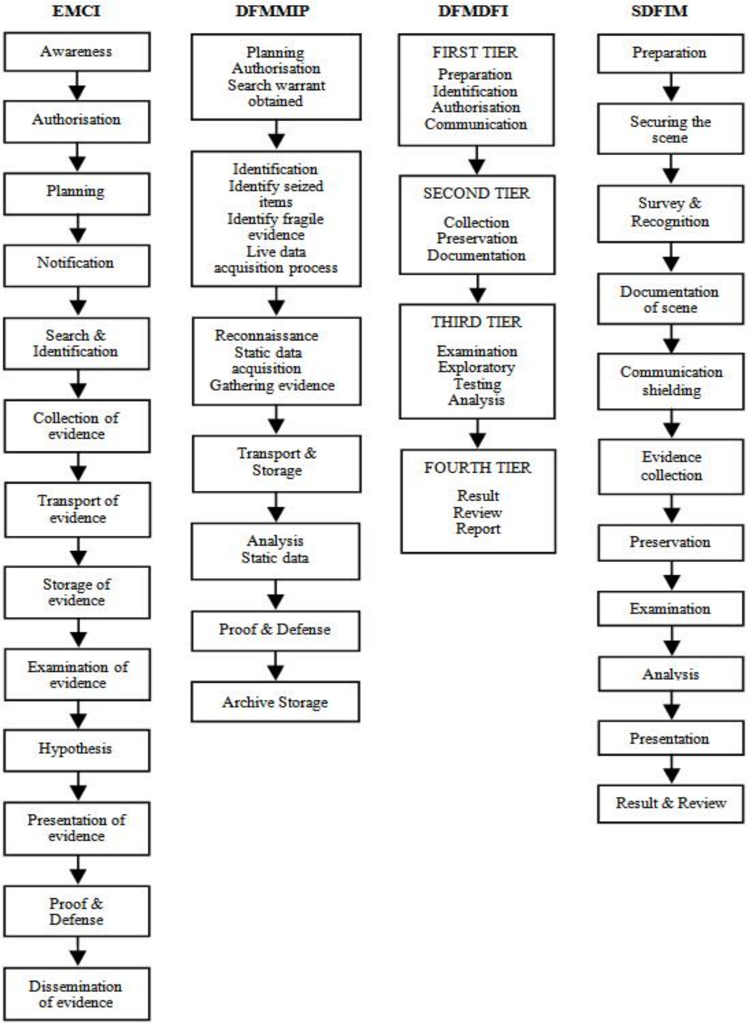


Fig. 3. Digital forensic investigation phases in EMCI, DFMMIP, DFMDFI and SDFIM models

Phase 2: Securing the Scene

The second phase primarily deals with securing the crime scene from unauthorized access and preserving the evidence from being contaminated.

Phase 3: Survey and Recognition

Survey and Recognition Phase involves an initial survey conducted by the investigators for evaluating the crime scene, identifying potential sources of evidence and formulating an appropriate search plan.

Phase 4: Documenting the Scene

Phase four involves proper documentation of both physical and digital crime scenes along with photographing, sketching, and crime-scene mapping.

Phase 5: Communication Shielding

Communication Shielding occurs prior to evidence collection. At this stage, all further possible communication options of the devices should be blocked. Even if the device appears to be in an off state, some communication features like wireless or Bluetooth may be enabled. This may result in overwriting the existing information and hence such possibilities should be avoided.

Phase 6: Evidence Collection

The evidence includes both volatile and non-volatile. The necessary precautionary measures must be taken to ensure its integrity.

Phase 7: Preservation

Preservation includes copies of digital evidence, packaging, transportation, and storage. Appropriate procedure and environmental conditions to maintain the chain of custody should be followed and documented to ensure the electronic evidence collected is not altered or destroyed.

Phase 8: Examination

Examination involves examining the content of the collected evidence by a forensic specialist and extracting information for presentation in court. This is made up of volatile and non-volatile evidence. According to the author, hashing technique like md5 must be used to authenticate the data.

Phase 9: Analysis

Analysis is more of technical review conducted by the investigative team on the basis of the result of the examination of the digital evidence and reconstructing the event data based on the guidelines recommended by the National Institute of Justice.

Phase 10: Presentation

Presentation phase is where a report consisting of detailed summary of the various steps taken during the investigation and the conclusion arrived at is presented to the appropriate authorities. It is presented to the court of law when a crime is committed or corporate management when it is an incident

Phase 11: Result and Review

At the final stage of the investigation, an evaluation is made and the result is used to update or improve any shortcoming experienced during the investigation.

Agawal et al (2011) performed a comparative analysis of some selected models and came out with a model that is probably one of the most detailed to date. The advantages of his model over others are listed in the following section.

3 Advantages and Limitations of the SDFIM

The model is not only comprehensive in scope because it captured almost all the important activities of the existing models but it is also based on forensic laws and the guidelines recommended by National Institute of Justice.

The model addresses the issue of collecting digital evidence from either volatile data or live response or both, which others with the exception of DFMMIP did not. This is a major concern for cybercrime investigation and equally important ingredient for prosecution.

In spite of these advantages, the model has the following limitations. For example it focused on the technical aspect of the investigation, (examination and analysis). However, all other aspects of the process both pre and post investigation processes must be considered equally if a comprehensive and detailed model is to be achieved.

The model revealed some similarities in some of the phases which could be regrouped to make it more coherent. For example, Survey and Recognition could be part of Preparation, Documenting the Crime Scene and Communication Shielding could also be part of Securing the Crime Scene, since these two independent phases in this model in reality are part of Securing Crime Scene. Examination and Analysis could also be combined. The model used these terms as separate activities but their definitions are not only similar but also complement each other and it can create confusion when separated.

SDFIM did not cover all aspects of cybercrime investigation as shown in Table 2 but mainly focuses on the process of obtaining digital evidence. According to Computer Crime Research Centre, [14] cybercrime is defined as crimes committed on the Internet using the computer as either a tool or a targeted victim. To effectively investigate such a crime, especially in a network environment which is a borderless or distributed system, one needs to trace the footprint from the secondary crime scene to determine the primary crime scene. [15] [9]. This was completely missing.

Even though the model is designed to investigate cyber-crime, in reality it can only be useful for computer crime (computer fraud) on a standalone machine where the computer is used as repository of evidence but not as a tool or target or both, due to the absence of Trace back and Dynamite [10] as explained earlier. Therefore, it cannot be applicable to a distributed system or complex architectures or network.

4 Gap Analysis Based Enhanced Digital Forensic Investigation Model

The weaknesses and limitations of the existing models are shown in Table 2. It is evident that the existing models did not address all the concerns or capture all the activities necessary for investigating and prosecuting cybercrime from start to finish. Most of them focus too much on processing digital evidence or the investigation process at the expense of other steps. The motivation for an enhanced model is based on the fact that digital forensics and for that matter cybercrime investigation involve not just a single computer but multiple or distributed computers, and successful investigation of such crime requires access to evidence from various sources. However, the existing forensic models including the SDFIM, do not sufficiently take into consideration these various sources of evidence and the need to correlate them both for the purpose of reconstruction and prosecution.

The proposed model is made up of six phases and is depicted in the flow chart in Fig. 4. It fills in the relevant gaps that were omitted from the existing models (as indicated in column II of Table 2) and also introduces Information Sharing shown in Table 3, which is an important ingredient for effective investigation and prosecution.

One unique feature about the proposed model which is an improvement over existing models is that, it has all the advantages of the existing models but in addition addresses the limitations of SDFIM. For example, SDFIM has eleven phases some of which overlapped, as explained in the previous section. In the proposed model, the phases have been regrouped as shown in Table 4 for efficiency and consistency.

The inclusion of honeypots/honeynet, intrusion detection and prevention systems and like tools supporting traceability and reconstruction for ongoing investigation will enable the security investigators to trace the primary crime scene from the footprint obtained from the secondary crime scene with the sole objective of identifying the possible suspect(s) or criminal(s) in a distributed or borderless environment.

Technicalities alone as mentioned in the previous paragraph is not sufficient for successful investigation and prosecution unless is backed by forensic laws, cooperation and collaboration from law enforcement agencies from both the primary and secondary crime scenes. This is achieved through information sharing and criminal profiling which are very significant for they equipped the law enforcement agency not only to develop investigative strategy but also effective interviewing technique.

4.1 Proposed Model: Enhanced Systematic Digital Forensic Investigation Model (ESDFIM)

In this section, the proposed model will be discussed. The model consists of six major phases and the structure is illustrated in Fig. 4 and Fig.5.

A. Preparation Phase

Preparation phase is where all the work and activities that needs to be done before the actual investigation takes place. It includes but not limited to the studying applicable forensic laws and guidelines, obtaining search warrant, management support, planning, and setting up appropriate strategy and tools to be used. Monitoring devices like Intrusion Detection System, Intrusion Prevention systems, Honeypot/Honeynet and like tools may sometimes be used as detective and preventive techniques depending on the nature of the crime. These were completely missing in the existing models.

B. Acquisition and Preservation Phase

Acquisition and preservation phase is where the evidential life cycle starts from and the tasks performed include securing the crime scene, identifying and collecting both volatile and non-volatile evidence, labeling & packaging, transporting, image acquisition, storage and preservation of evidence. In general this phase is where relevant data are captured, stored and made available for the next phase. It is therefore important that every item searched and seized including access control, system and network architectures is legally obtained (plain view, search warrant, consent, etc.) and properly documented (chain of custody) in conformity to the evidential rule [16], [17], [18] [23] [24]. The existing models did not capture most of these activities.

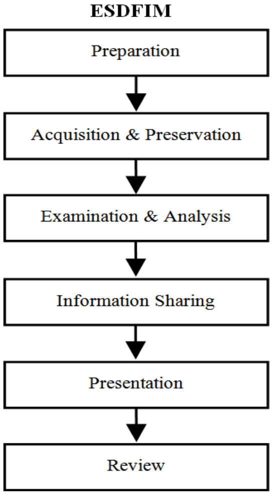


Fig. 4. Digital forensic investigation phases in the proposed model

C. Examination and Analysis Phase

Examination and analysis is where forensic examiners and experts look for digital evidence (Digital Evidence is defined by Carrier and Spafford [8] as digital data that supports or refutes a hypothesis about digital event or the state of digital data) by examining and analyzing the content of various digital devices which were legally seized and properly preserved. This is where the detail and technical job is done using approved guidelines and accredited forensic tools in order to identify the source of crime and ultimately trace whoever did it. The evidence to be generated will depend on the scope of engagement; the nature of the crime and also on the initial hypothesis and the result may or may not contradict the initial hypothesis, in order to prove culpability in the court of law [19].

D. Information Sharing Phase

Information sharing is the ability to exchange data between various countries, organizations, people, and technology (according to Techopedia.com). This weapon which is effectively used within the social networking sites and the hacking community could be applicable in digital forensic investigation. [20]. The effectiveness of this tool however depends on certification of the information, mutual trust and understanding among law enforcement agencies, common cybercrime laws and investigation models being used in both countries else it will have a cascading effect on prosecution. One important advantage of information sharing is the ability to get full criminal profile of the suspect(s) [17] [21], which will effectively equip the law enforcement agencies to develop investigative strategy and effective interviewing techniques [22].This form of cooperation and information sharing can contribute effectively towards successful prosecution.

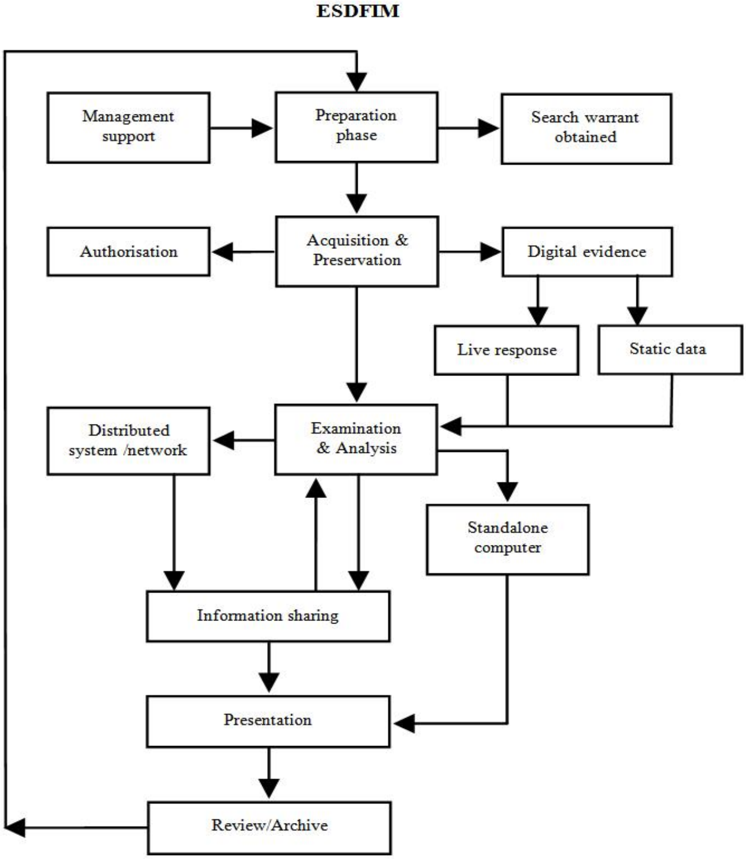


Fig. 5. Complete flow of a digital forensic investigation in the proposed model

E. Presentation Phase

The result of the examination and analysis phase is compiled and presented to the authority concerned. This is the critical stage of the investigation since the whole evidence can either be accepted or rejected. The admissibility of the evidence before the court of law for example depends on certain factors including but not limited to whether the evidence is materially and properly preserved, (chain of custody or evidence), whether the evidence is relevant, properly identified and legally obtained, whether the language used in the presentation is simple and concise to be understood by the judge or the jury or whether the prosecution and his team can defend and prove intent, motive, identity or any error or mistake against the challenges and criticism of the accused/defendant's team. It is important to remember that the critical point in this phase is to present the findings to convince and prove your case before the trial judge or jury in a court of law.

F. Review Phase

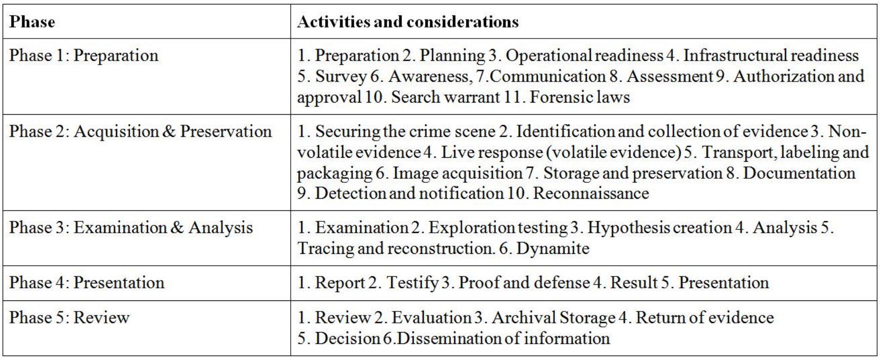
The whole investigation is evaluated and areas of improvement identified. From the beginning of the investigation to court proceedings, and the result are used for future improvement. The experience gained and lessons learnt are shared and used to train new staff. Cases are also classified according to its status and remarks made in respect of whether the case is completed, suspended, pending and ongoing. This is done to guide future events such as a court appeal, reappearance of an acquitted person or for a reference. Evidence and exhibits which are returnable are given to their owners.

A unique feature of the proposed model is that it is not waterfall model but iterative in nature and therefore one has the ability to go back to the previous activity or phase when it becomes necessary that in doing so will help in the successful investigation and prosecution.

5 Comparison of the Proposed Model with Existing Models

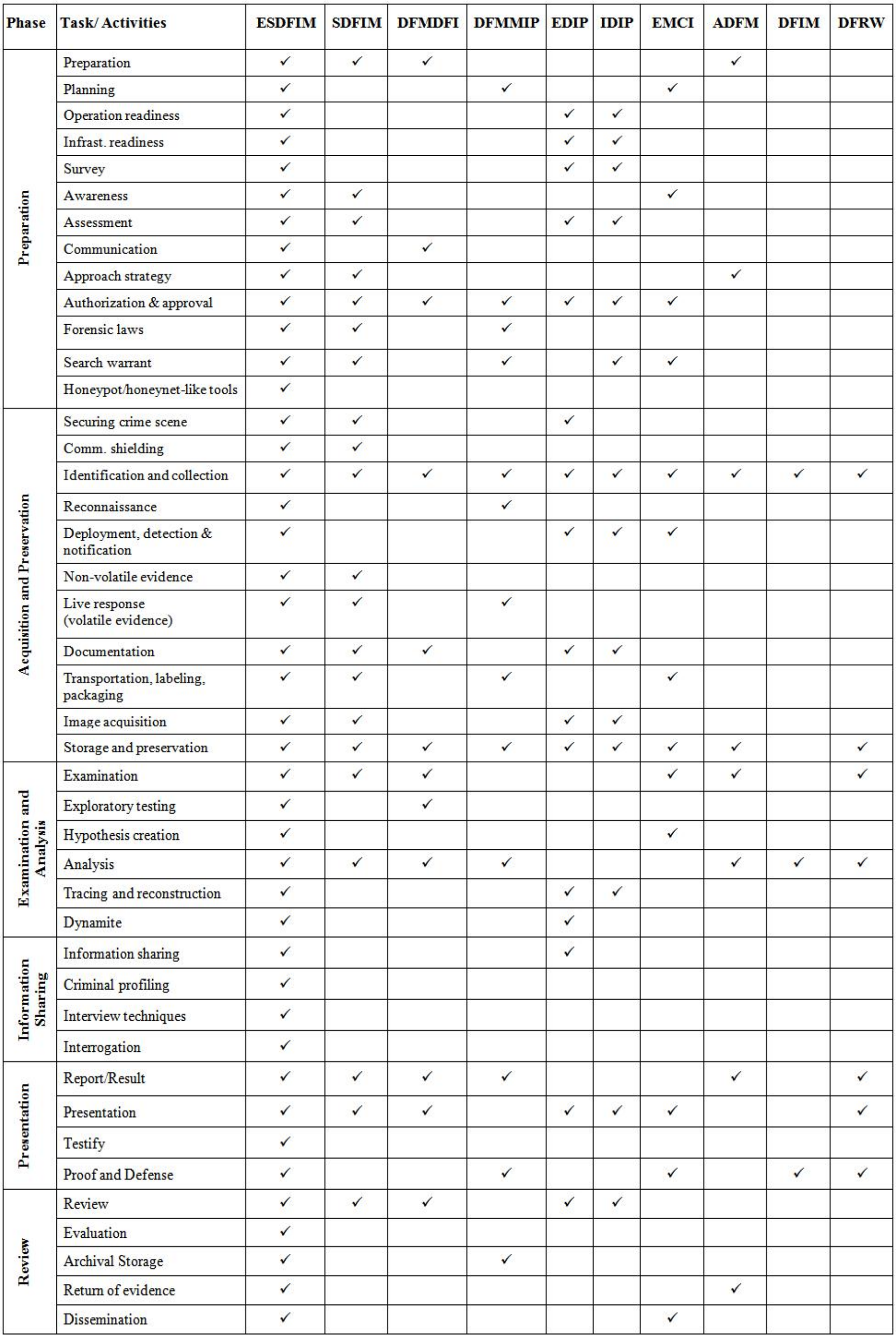
A significant drawback in digital forensic investigation is that often not enough emphasis is placed on potential admissibility of the gathered evidence. Digital forensic investigation must adhere to the standard of evidence and its admissibility for successful prosecution. Therefore the techno–legal nature of the proposed model, coupled with the incorporation of best practices of existing models, will not only equip law enforcement agencies in their fight against computer criminals in both proactive and reactive ways but will also lead to successful prosecution. The following tables show our comparison of the proposed ESDFIM with the models discussed in this paper. Note that all relevant activities from previous models are included in the proposed model.

Table 1. Summary of phases and activities in existing digital forensic investigation models



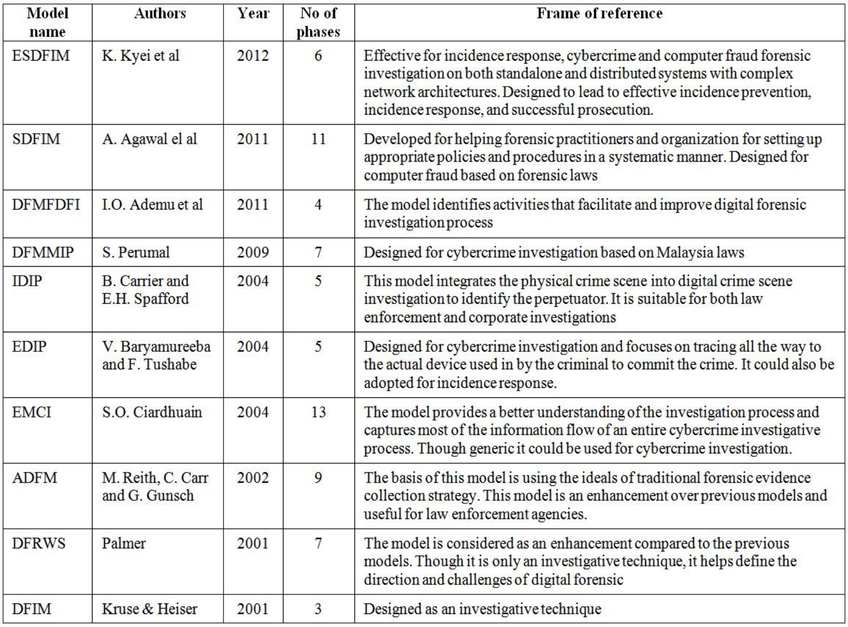
Phase	Activities and considerations
Phase 1: Preparation	1. Preparation 2. Planning 3. Operational readiness 4. Infrastructural readiness 5. Survey 6. Awareness, 7.Communication 8. Assessment 9. Authorization and approval 10. Search warrant 11. Forensic laws
Phase 2: Acquisition & Preservation	1. Securing the crime scene 2. Identification and collection of evidence 3. Non-volatile evidence 4. Live response (volatile evidence) 5. Transport, labeling and packaging 6. Image acquisition 7. Storage and preservation 8. Documentation 9. Detection and notification 10. Reconnaissance
Phase 3: Examination & Analysis	1. Examination 2. Exploration testing 3. Hypothesis creation 4. Analysis 5. Tracing and reconstruction. 6. Dynamite
Phase 4: Presentation	1. Report 2. Testify 3. Proof and defense 4. Result 5. Presentation
Phase 5: Review	1. Review 2. Evaluation 3. Archival Storage 4. Return of evidence 5. Decision 6.Dissemination of information

Table 2. Comparison of the proposed ESDFIM model with existing digital forensic investigation models



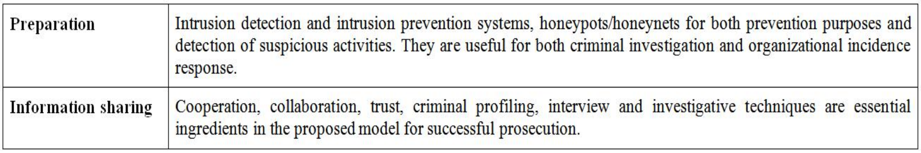
Phase	Task/ Activities	ESDFIM	SDFIM	DFMDFI	DFMMIP	EDIP	IDIP	EMCI	ADFM	DFIM	DFRW
Preparation	Preparation	✓	✓	✓					✓		
	Planning	✓			✓			✓			
	Operation readiness	✓				✓	✓				
	Infrast. readiness	✓				✓	✓				
	Survey	✓				✓	✓				
	Awareness	✓	✓					✓			
	Assessment	✓	✓			✓	✓				
	Communication	✓		✓							
	Approach strategy	✓	✓						✓		
	Authorization & approval	✓	✓	✓	✓	✓	✓	✓			
	Forensic laws	✓	✓		✓						
	Search warrant	✓	✓		✓		✓	✓			
	Honeypot/honeynet-like tools	✓									
Acquisition and Preservation	Securing crime scene	✓	✓			✓					
	Comm. shielding	✓	✓								
	Identification and collection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Reconnaissance	✓			✓						
	Deployment, detection & notification	✓				✓	✓	✓			
	Non-volatile evidence	✓	✓								
	Live response (volatile evidence)	✓	✓		✓						
	Documentation	✓	✓	✓		✓	✓				
	Transportation, labeling, packaging	✓	✓		✓			✓			
	Image acquisition	✓	✓			✓	✓				
	Storage and preservation	✓	✓	✓	✓	✓	✓	✓	✓		✓
Examination and Analysis	Examination	✓	✓	✓				✓	✓		✓
	Exploratory testing	✓		✓							
	Hypothesis creation	✓						✓			
	Analysis	✓	✓	✓	✓				✓	✓	✓
	Tracing and reconstruction	✓				✓	✓				
	Dynamite	✓				✓					
Information Sharing	Information sharing	✓				✓					
	Criminal profiling	✓									
	Interview techniques	✓									
	Interrogation	✓									
Presentation	Report/Result	✓	✓	✓	✓				✓		✓
	Presentation	✓	✓	✓		✓	✓	✓			✓
	Testify	✓									
	Proof and Defense	✓			✓			✓		✓	✓
Review	Review	✓	✓	✓		✓	✓				
	Evaluation	✓									
	Archival Storage	✓			✓						
	Return of evidence	✓							✓		
	Dissemination	✓						✓			

Table 3. Comparison of phases and objectives in the proposed ESDFIM model with the existing digital forensic investigation models



Model name	Authors	Year	No of phases	Frame of reference
ESDFIM	K. Kyei et al	2012	6	Effective for incidence response, cybercrime and computer fraud forensic investigation on both standalone and distributed systems with complex network architectures. Designed to lead to effective incidence prevention, incidence response, and successful prosecution.
SDFIM	A. Agawal el al	2011	11	Developed for helping forensic practitioners and organization for setting up appropriate policies and procedures in a systematic manner. Designed for computer fraud based on forensic laws
DFMFDFI	I.O. Ademu et al	2011	4	The model identifies activities that facilitate and improve digital forensic investigation process
DFMMIP	S. Perumal	2009	7	Designed for cybercrime investigation based on Malaysia laws
IDIP	B. Carrier and E.H. Spafford	2004	5	This model integrates the physical crime scene into digital crime scene investigation to identify the perpetuator. It is suitable for both law enforcement and corporate investigations
EDIP	V. Baryamureeba and F. Tushabe	2004	5	Designed for cybercrime investigation and focuses on tracing all the way to the actual device used in by the criminal to commit the crime. It could also be adopted for incidence response.
EMCI	S.O. Ciardhuain	2004	13	The model provides a better understanding of the investigation process and captures most of the information flow of an entire cybercrime investigative process. Though generic it could be used for cybercrime investigation.
ADFM	M. Reith, C. Carr and G. Gunsch	2002	9	The basis of this model is using the ideals of traditional forensic evidence collection strategy. This model is an enhancement over previous models and useful for law enforcement agencies.
DFRWS	Palmer	2001	7	The model is considered as an enhancement compared to the previous models. Though it is only an investigative technique, it helps define the direction and challenges of digital forensic
DFIM	Kruse & Heiser	2001	3	Designed as an investigative technique

Table 4. New elements in the proposed digital forensic investigation model



Preparation	Intrusion detection and intrusion prevention systems, honeypots/honeynets for both prevention purposes and detection of suspicious activities. They are useful for both criminal investigation and organizational incidence response.
Information sharing	Cooperation, collaboration, trust, criminal profiling, interview and investigative techniques are essential ingredients in the proposed model for successful prosecution.

6 Conclusion

The objective of this paper is to review, analyze and identify gaps in the existing models in order to develop a holistic digital forensic investigation model which will enable law enforcement agencies to correctly investigate and successfully prosecute cybercriminals. It is believed that adoption of best practices from previous models and the inclusion of honeypot/honeynets etc, information sharing, criminal profiling as well as effective interview and interrogative techniques make it more detailed and comprehensive than the previous models. The new model, the enhanced systematic digital forensic investigation model, is expected to be not only useful to law enforcement agencies and organizations' incident response teams, but will also provide a basis for the development of useful forensic tools.

References

1. Boateng, R., et al.: Cyber Crime and Criminality in Ghana: Its Forms and Implications. In: Proceedings of the 16th Americas Conference on Information Systems (2010)
2. Smith, R.G., Grabosky, P.N., Urbas, G.: Cybercriminals on trial. Cambridge University Press (2004) ISBN: 9780521840477
3. Kent, K., Chevalier, S., Grance, T., Dang, H.: NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response (2006)
4. Agarwal, A., et al.: Systematic Digital Forensic Investigation Model (2011), http://www.cscjournals.org/csc/manuscript/journals/IJCSS/Volume5/Issue1/IJCSS-438.pdf
5. Kruse, W.J., Heiser, G.: Computer Forensics: Incident Response Essentials. Addison-Wesley (2002) ISBN 0-201-70719-5
6. Palmer, G.: A Road Map for Digital Forensic Research. Technical Report DTR-T001-01, DFRW, Report From the First Digital Forensic Research Workshop, Utica, NY (2001)
7. Reith, M., Carr, C., Gunsch, G.: An Examination of Digital Forensic Models. International Journal of Digital Evidence 1(3) (2002)
8. Carrier, B., Spafford, E.H.: Getting Physical with the Investigative Process. International Journal of Digital Evidence 2(2) (Fall 2003)
9. Lee, H., Palmbach, T., Miller, M.: Henry Lee's Crime Scene Handbook, Academic Press (2001) ISBN-13: 978-0124408302
10. Baryamureeba, V., Tushabe, F.: Enhanced Digital Investigation Process Model, Digital Forensic Research Workshop, Baltimore, MD, USA (2004)
11. Ciardhuáin, S.O.: An Extended Model of Cybercrime Investigations. In:International Journal of Digital Evidence 3(1) (Summer 2004)
12. Perumal, S.: Digital Forensic Model Based on Malaysian Investigation Process. IJCSNS International Journal of Computer Science and Network Security 9(8) (August 2009)
13. Ademu, I.O., Imafidon, C.O., Preston, D.S.: A New Approach of Digital Forensic Model for Digital Forensic Investigation. (IJACSA) International Journal of Advanced Computer Science and Applications 2(12) (2011)
14. Aghatise, E.J.: Computer Crime Research Center Cybercrime Definition (2006)
15. Carrier, B.: File System Forensic Analysis, Addison-Wesley (2005) ISBN 0-321-26817-2
16. Bunting, S.: Mastering Windows Network Forensic and Investigation, 1st edn. Sybex (2007) ISBN-13: 978-0470097625
17. Cressey, D.R.: Other People's Money: Study in the Social Psychology of Embezzlement. Wadsworth Publishing Company (1972) ISBN-13: 978-0534001421
18. Cosic, J., Baca, M.: A Framework to (Im)Prove "Chain of Custody" in Digital Investigation Process. In: Proceedings of the CECIIS, Varazdin, Croatia (2010)
19. Roger, M.K.: A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study. University of Manitoba, Winnipeg (2001)
20. Biros, D.P., et al.: Information Sharing: Hackers vs. law enforcement. In: Proceedings of the 9th Australian Information Warfare and Security Conference, Perth, Australia (2008)
21. Stephenson, P.: Modeling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence 2(2) (Fall 2003)
22. Turvey, B.: Criminal Profiling: An Introduction to behavioral evidence analysis, 4th edn. Elsevier (2012) ISBN 978-0-12-385243-4
23. ACFE Fraud Examiners Manual, Canadian Edition (2012)
24. Association of Chief Police Officers (ACPO): Good Practice Guide for Computer based Electronic Evidence (2006)