Digital Forensic Model Based On Malaysian Investigation Process

Sundresan Perumal[1]

Faculty Of Science & Technology Islamic Science University Of Malaysia

Summary
With the proliferation of the digital crime around the world, numerous digital forensic investigation models already being develop .In fact many of the digital forensic investigation model focus on technical implementation of the investigation process as most of it develop by traditional forensic expert and technologist. As an outcome of this problem most of the digital forensic practitioners focus on technical aspect and forget the core concept of digital forensic investigation model .In this paper we are introducing a new digital forensic model which will be capture a full scope of an investigation process based on Malaysia Cyber Law .The proposed model is also compared with the existing model which currently available and being apply in the investigation process.

Key words:
Digital Forensic, Cyber Law, Digital Crime, Forensic Practitioner, Technologist.

1. Introduction

With the proliferation of the digital crime around the world, numerous digital forensic investigation models already being develop. In the digital forensic investigation practices, there are over hundred of digital forensic investigation procedures developed all over the world .Each organization and country tend to develop its own procedures ,some focused on the technology aspect, some focused on data analysis portion of the investigation[2][9].

Whenever conducting a computer investigation for potential criminal violations of the law the legal process will only depend on local cyber law. In general all the cases will only follow these three steps: The Complaint, The Investigation and The Prosecution (Fig. 1).

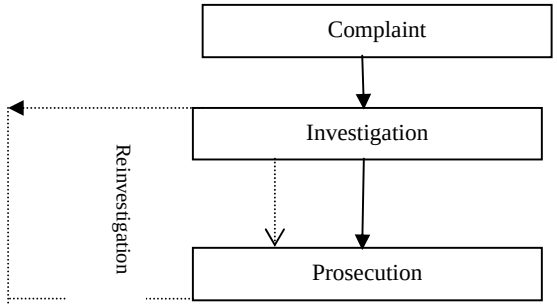

Fig.1 The Investigation and the Prosecutions

Manuscript received August 5, 2009
Manuscript revised August 20, 2009

This paper present a complete digital forensic investigation model based on Malaysian investigation process. This model identifies most of the missing process formation in the digital forensic model. This newly proposed model also will be compare with the existing model in the next section .This proposed model focus on data acquisition process and also on fundamental stages in conducting a complete forensic analyzation.

2. Existing Model.

As there have been several model which already establish in the digital forensic industries but they are largely restricted themselves to the investigation of the crime scene and the evidence, and so are less extensive in their scope [10] every digital forensic have their own negative and positive attributes. Table 1 shows a list of complete digital forensic investigation model.

2.1 Kruse & Heiser Digital Forensic investigation Model.

Kruse&Heiser(2001) have discuss that computer forensic is the coherent application of methodical investigation technique to solve crime cases. As in their model it involve three basic stages that is acquiring evidence, authenticating the evidence and analyzing the evidence [6].Fig 2 show the breakdown of the Kruse&Heiser model.

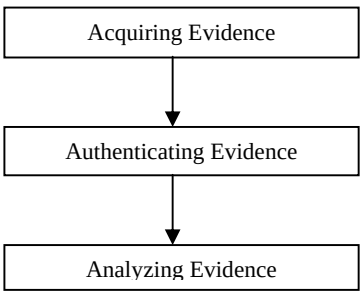

Fig 2- Kruse&Heiser Model

Table 1 shows a list of complete digital forensic investigation model.

Model Name	Inventers	Years	Number of Stages
Computer Forensic Process	M.Pollitt	1995	4 Stages
Generic Investigation Process	Palmer	2001	7 Stages
Abstract Model of the Digital Forensic Procedures	Reith ,Carr, & Gunsh	2002	9 Stages
An Integrated Digital Investigation Process	Carrier & Spafford	2003	17 Stages
End To End Digital Investigation	Stephenson	2003	9 Stages
Enhance Integrated Digital Investigation Process	Baryamureeba & Tushabe	2004	21Stages
Extended Model of Cyber Crime Investigation	Ciardhuain	2004	13 Stages
Hierarchical ,Objective Based Framework	Beebe & Clark	2004	6 Stages
Event Based Digital Forensic Investigation Framework	Carrier & Spafford	2004	16 Stages
Forensic Process	Kent K ,Chevalier , Grance , & Dang	2006	4 Stages
Investigation Framework	Kohn , Eloff ,& Oliver	2006	3 Stages
Computer Forensic Field Triage Process Model	K.Roger,Goldman,Mislan,Wedge & Debtota	2006	4 Stages
Investigation Process model	Freiling & Schwittay	2007	4Stages

2.2 The Scientific Crime Scene Investigation Model by Lee.

Lee et.al(2001) have proposed a model which consist of four stages, it is recognition, identification, individualization and reconstruction [10]. Fig 3 shows the Lee Scientific Crime Scene Investigation Model .This model is focusing on a systematic and methodical way of investigating any digital crime cases, the barrier of the model is analyzing part of digital forensic process only, this have made a limitation in the digital forensic investigation, as not be focusing on the data acquisition neither preparation and presentation.

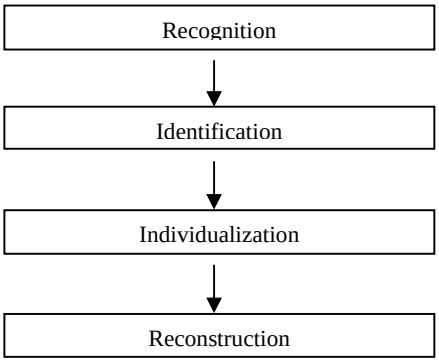

Fig 3 –Lee's Scientific Crime Scene Investigation Model

2.3 Casey Digital Forensic Frameworks

Casey(2004) has proposed a model which consists of four stages where recognition, preservation, classification and reconstruction Fig 4 shows Casey digital forensic framework[4]. As can see that this model has a similarity with Lee model in the initial stage and in the last stage. Casey also places a major concern of the forensic process on the investigation itself.

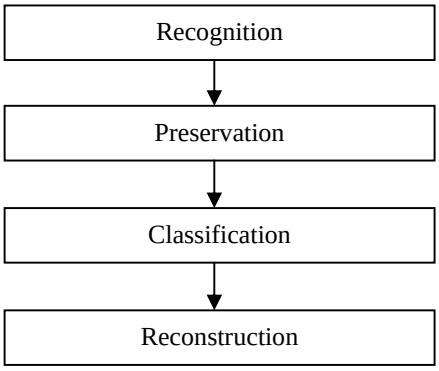

Fig 4 –Casey Digital Forensic Framework Model

2.4 DFRWS (Digital Forensic Research Workshop)

Digital forensic research workshop have develop a model with the following steps, identical, preservation, collection ,examination ,analysis, presentation and decisions[10][9].Fig 5 shows Digital Forensic Research Workshop Model.

This model can be classified as a compressive model since it's tend to cover some of the stages which not been brought in any previous model, such as presentation stage.

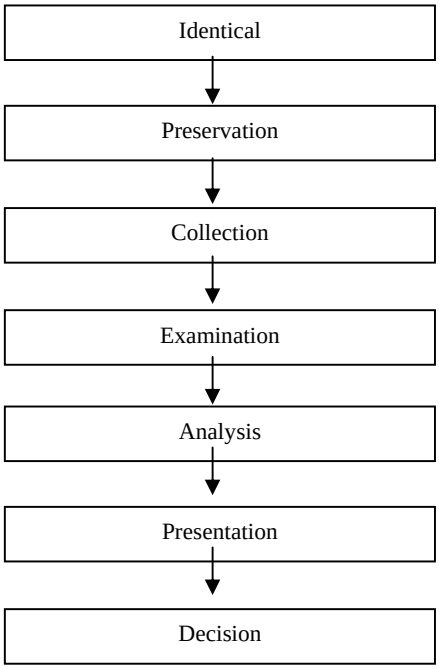

Fig 5 –DFRWS Investigation Model

2.5Reith, Carr and Gunch Model.

Reith,Carr and Gunch have also come up with another model which have included some of the missing components from the previous model which all the while been suggested. Reith model consist of preparation, approach, strategy, preservation, collection, examination, analysis, presentation, and returning evidence[7].Based on the stages above the model has focused in depth concerning investigation procedures.

2.6Seamus O Ciardhuain Extended Model of Cybercrime Investigation.

Seamus O Ciardhuain model was the most latest and covered quite number of process. The model include the following activities such as awareness, authorization, planning, notification, search for and identify evidence, collections of evidence, transport of evidence, storage of evidence, examinations of evidence, hypothesis, presentation of hypothesis, proof/defense of hypothesis, and dissemination of information [10].This model have to be applied in the context of an organization before it will be possible to make a clear details of the process [10].

3.0 Why Do Malaysian Criminal Justice Need a Digital Investigation Model.

As in Malaysia the computer crime have become central issues especially collecting the electronic evidence and gathering the needed information from the suspected computer. As computer forensic is a new regulation in Malaysia, there is a little consistency and standardization in the court and industry sector. As a result it is not yet recognized as a formal 'Scientific' discipline in Malaysia [12].

There should be a proper methodology and procedure to be followed by forensic investigator who focuses more into efficiency, accuracy and how to preserve the fragile evidence. There should be a biggest concern for every forensic investigator for the fragile evidence because this is not like normal evidence during an investigation. For example, if one looks at the traditional investigation for case where there are some fingerprints in the glass suddenly someone mistakenly wipes it out, the evidence is gone. This situation is synonymous for a computer when it involved in any crime scene. In computer related crime there are not going to be any silver bullet holes for us to summarize where an intruder has gained illegal access and there are not going to be any drops of blood stain for us to trace the hacker. This research sought to demonstrate a model, in order to enhanced and secure the way to conduct a digital forensic investigation especially for Malaysia computer criminal justice .

4.0 The Proposed Model

In the previous section few most commonly used model being presented but the question is why do we still need another digital forensic investigation model? Currently the existing model did not focus on all the cyber crime investigation aspect, they mainly focus on processing the digital evidence[10],[1].Most of the existing model design, does not show the information process flow focusing on issue such as chain of custody. The largest gap in most of the presented model is no attention been paid on the fragile evidence and also on data acquisition process.

With the absent of this type of stages the, model won't be stable enough to be used in cyber crime investigation. The major stages are as below:

1) Planning
   -Authorization.
   -Search warrant Obtained.

2) Identification
   - Identified seized Items.
   -Identify fragile evidence.
   (Live Data Acquisition) ⟵ Process

3) Reconnaissance
   (Static Data Acquisition)⟵ Process
   -Gathering Evidence.
   (Static Data Acquisition) ⟵ Process
   -Transport &Storage.

4) Analysis.
   (Static Data Acquisition) ⟵ Process

5) Result.
6) Proof & Defense.
7) Diffusion of Information.

Fig 6 shows the complete flow of an investigation for the newly proposed model. Every process which is discussed has to pass from one stage to another without skipping any stages. The stages details are discuss below

4.1Planning
The planning stages consist of two sub procedures that is authorization and obtaining search warrant. Getting a authorization from the local enforcement team and obtaining a search warrant to seize any items from the location falls under planning stages as it is a compulsory process in every cyber crime investigation, in some cases a verbal authorization have to be obtain by the company management before the digital forensic investigator proceed with the detailed investigation on the company computer system.

4.2Identification
The identification stage also consists of two sub procedures that is identify seized items and identify fragile evidence. In identify seized item's we need to recall the Locard exchange principal where anyone, or anything entering a crime scene takes something of the crime scene with them, they also leave behind something of themselves when the depart[5].The process of identifying all the electronic equipment used by the suspect mostly one of the interest to the investigator. Another most important sub procedures will be identifying fragile evidence. In this process to pull or not to pull the plug is the concern of most of the forensic investigator as traditionally computer forensic expert have followed the process of shutting down the system in order to preserve the evidence from the potential data tempering .The misconception is that computer forensic is not same as physical forensic. As the live acquisition processes have to be conducted if the computer system is on. There
is a lot of advantage of conducting "Live" analysis rather than" Postmortem". Live acquisition process is to retrieve the file time stamp, registry key, swap files, and memory details. All the above mention is falls in fragile evidence category as most probably will change or will lost upon the plugging the power cable.

4.3 Reconnaissance

In this stages the understanding of the meaning "Reconnaissance" is more important as this word stands for exploration conducted to gain information .As we know that today ,most of the company have huge computer network at a single location .Some company might have branch in several location in a city ,country, or continent and it wouldn't be practical if it is tend to be for a forensic analyzer have to respond to every site and pull the computer off and conduct the forensic analysis. In this stage gathering the necessary evidence is very important rather than removing the system out form the network, as for example if the server which we wanted to analyze is responsible in handling day to day operation of the company, it would be impossible to remove the server from the network and conduct the analyzation which directly will affect the company operation. Another factor is about the server storage as we know, when it comes to server storage the capacity will be huge in size and it wouldn't be practical to image entire sever storage for an example if the server storage size is about 500TB and the forensic analyzer intended to image the entire drive by using ICS MASSter Solo-3 which can duplicate the storage at 3GB in a minute so:

500TB *1,099,511,627,776KB
=5,497,558,138,880,00KB

5,497,558,138,880,00KB/3221225472KB (3GB)
=170667 Total Minutes

170667/60(1hour)
=2845hour

2845/24(1day)
= 119days

Based on the calculation it shows that to image the entire storage of a server which have a capacity of 500TB It would take about 4months. In this situation the analyzer have to encrypt the entire hard disk volume and then proceed with the imaging, in the later part he have to decrypt it before conducting static data acquisition.

4.4 Transport & Storage
All the evidence collected has to be located in a safe place as it is important that the evidence is safe from tempering and need to preserve the integrity of the evidence.

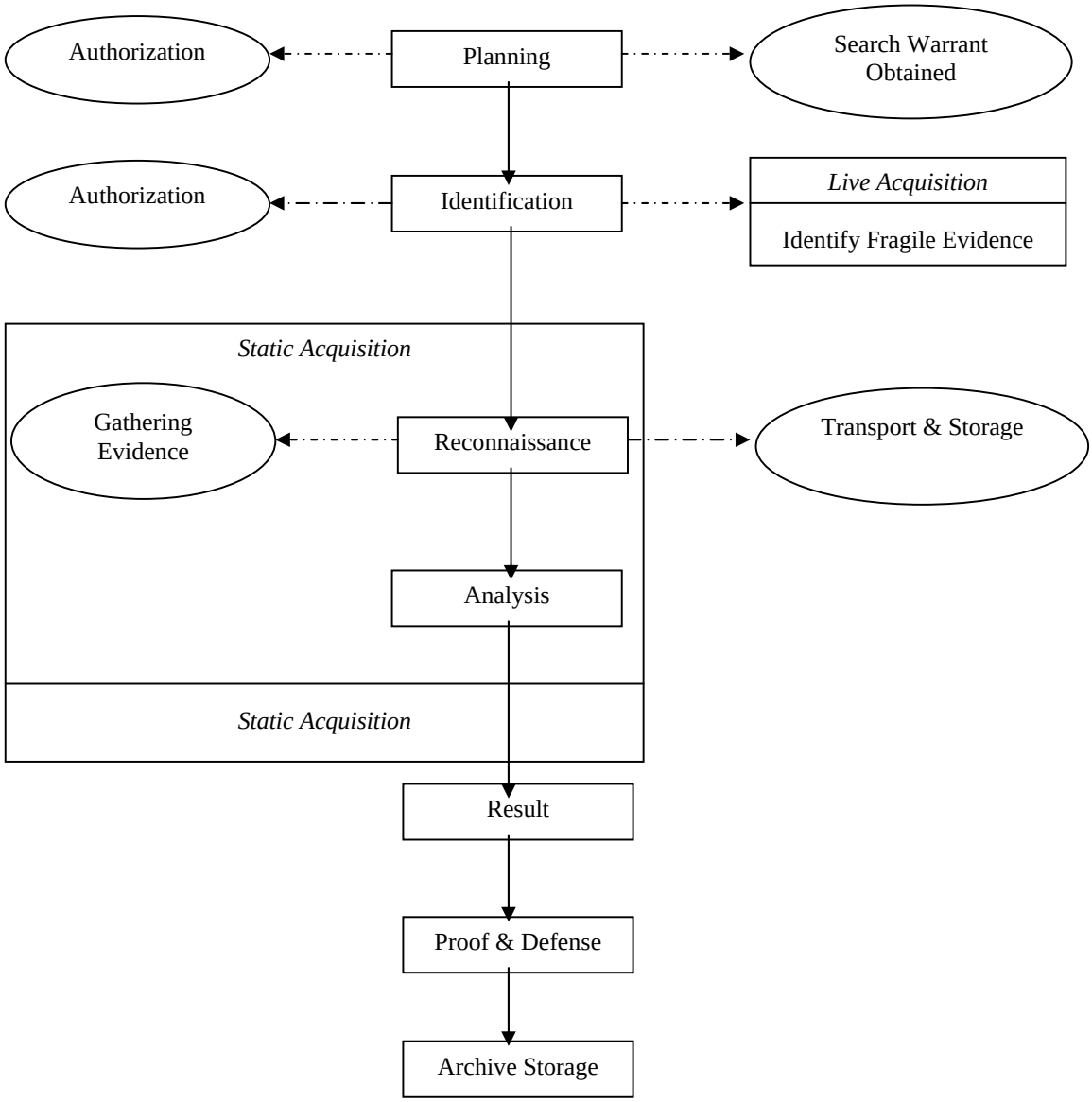

Fig 6 shows the complete flow of an investigation for the newly proposed model.

4.5Analysis

Analysis technique is another complicated process as the analyzer has to build a toolbox of utilities to analyze the data and correlate the data into a coherent picture. A piece of evidence discovery may not be strong enough to stand on its own, but may be the item that provides the next lead.

4.6Proof & Defense

In this process hypothesis will not go unchallenged, a contrary hypothesis and supporting evidence will be placed before a jury[10].The analyzer have to proof the validity of the case with his findings, if it is tend to be unsuccessful then the forensic analyzer have to rollback the whole process of anlyzation and have to obtain more evidence and construct a new report.

4.7Archive Storage

This stage is to store all the evidence which may need to be used as reference in near future and also might need to be used for training purposes. By applying this concept which known as data mining it would be an advantage for other country analyzer or authorities in a situation where the case might have relation with their investigation. It

also can be used for some cases where the convicted repeal in the court for reprosecution.

5.0 Comparison with existing model

Table 2 shows a comparison of the stages task in the proposed model with those existing model discussed in this paper. It shows very clearly that some of the stages were not given attention and missing in the existing model .The process flow were not made transparent enough to be followed by the existing model.

Table 2 - Comparison of the stages task in the proposed model with those existing model.

Task in new model		Kruse & Heiser	Lee et al	Casey	DFRWS	Reith et al	Seamus
Planning	Authorization						✓
	Search Warrant Obtained						
Identification	Identified Seized Items	✓	✓	✓	✓	✓	✓
	Live Acquisition						
	Identify Fragile Evidence						
Reconnaissance	*Static Acquisition*		✓	✓	✓		✓
	Gathering Evidence						
	Transport & Storage	✓			✓		✓
Analysis		✓	✓	✓	✓	✓	✓
Result			✓		✓	✓	✓
Proof & Defense					✓		✓
Archive Storage							✓

6.0 Conclusion

Nothing can be successful accomplished without a formal process or formal model, also need to keep in mind that crimes are not solved until they are successfully prosecuted. From the digital forensic investigation proposed model it have clearly define that the investigation process will lead into a better prosecution as the very most important stages such as live data acquisition and static data acquisition been implant in the model to focus on fragile evidence. The proposed models also have focused on data mining in the stages of archive storage. After an explanation from the proposed model it can be classified as a comprehensive model for Malaysian digital forensic investigators.

7.0 Future Work

As currently the model have focused into fragile data acquisition and archive storage, in future would like to focus more on integrated memory data acquisition technique, and on evidence data mining system. With the data mining system all the digital forensic analyzer will have a central knowledge sharing portal which can be very helpful for their training purposes or to be share by state, central, national or international police for any digital forensic investigation purposes.

References

[1] Baryamureeba, V., Tushabe, F.:The Enhanced Digital Investigation Process Model.Makere University Institute of Computer Science, Uganda 2004.

[2] Brill AE, Pollitt M. The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. Journal of Digital Forensic Practice 2006; 1:3-11.

[3] Broucek, v., Turner, P.: Computer Incident Investigation e-Forensic Insight on Evidence Acquisition. In: Gattiker, U.E. (ed.) EICAR Conference Best Paper Proceeding EICAR Luxembourg, Grand Duchy of Luxembourg 2004.

[4] Casey, E.: Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic Press, 2004.

[5] Carrier, B. D. : A Hypothesis-based Approach to Digital Forensic Investigations. CERIAS Tech Report 2006-06, Purdue University, Center for Education and Research in Information Assurance and Security, West Lafayette.
[6] Michael Kohn, Jhp Eloff, Ms Olivier. Framework for Digital Forensic Investigation: Information and Computer Security Architectures Research Group (ICSA), University of Pretoria.
[7] Reith, M., Carr, c. and Gunsch, G.: An Examination of Digital Forensic Model, International of Digital Evidence .Fall 2002, Volume 1, Issue 3,2002.
[8] McKemmish, R.: What is Forensic Computing? Canberra Australian Institute of Criminology ,1999.
[9] Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib.:Mapping Process of Digital Forensic Investigation Framework. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.
[10] Seamus O Ciardhuain. An Extended Model of Cybercrime Investigation. Journal of Digital Evidence Summer 2004; Volume 3, Issue 1.
[11] Stephenson, P. : A Comprehensive Approach to Digital Incident Investigation. Elsevier Information Security Technical Report. Elsevier Advanced Technology .2003.
[12] Zahari Yunus.The New Frontier For Terrorist, CyberSecurity Malaysia .STAR In-Tech. 1 July 2008.

Sundresan Perumal is currently a PhD student at University Science Islam Malaysia. He holds Bachelor Of Computer Science (Hons) and a Master Degree in Information Technology from University of Nottingham. His research interest includes E-government security model, digital forensic, advanced file carving, and data mining. He is a member of International Digital Forensic Association, PECAMP, and International Congress of E-Government.