COMMON PHASES OF COMPUTER FORENSICS INVESTIGATION MODELS

Yunus Yusoff, Roslan Ismail and Zainuddin Hassan

College of Information Technology, Universiti Tenaga Nasional,
Selangor, Malaysia
yunusy@uniten.edu.my, roslan@uniten.edu.my, zainuddin@uniten.edu.my

ABSTRACT

The increasing criminal activities using digital information as the means or targets warrant for a structured manner in dealing with them. Since 1984 when a formalized process been introduced, a great number of new and improved computer forensic investigation processes have been developed. In this paper, we reviewed a few selected investigation processes that have been produced throughout the years and then identified the commonly shared processes. Hopefully, with the identification of the commonly shard process, it would make it easier for the new users to understand the processes and also to serve as the basic underlying concept for the development of a new set of processes. Based on the commonly shared processes, we proposed a generic computer forensics investigation model, known as GCFIM.

KEYWORDS

Computer Forensic Models, Computer Forensic Investigation

1. INTRODUCTION

The increasing criminal activities using digital information as the means or targets warrant for a structured manner in dealing with them. As more information is stored in digital form, it is very likely that the evidence needed to prosecute the criminals is also in digital form.

As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence [1]. The process or procedure adopted in performing the computer forensic investigation has a direct influence to the outcome of the investigation. Choosing the inappropriate investigative processes may lead to incomplete or missing evidence. Bypassing one step or switching any of the steps may lead to inconclusive results; therefore give rise to invalid conclusions. Evidences captured in an ad hoc or unstructured manner may risks of not being admissible in the court of law.

It is indeed very crucial for the computer forensics investigator to conduct their work properly as all of their actions are subjected to scrutiny by the judiciary should the case be presented in the court. The presence of a standard structured process does in a way provide a suitable mechanism to be followed by the computer forensic investigators.

Over the years, there were a number of investigation models being proposed by various authors. Based on our observation, some of the models tend to be applicable to a very specific scenario while other may be applied to a wider scope. Some of the models tend to be quite detail and others may be too general. It may be a bit difficult or even confusing, especially to the junior forensic investigator to adopt the correct or appropriate investigation model. It is of our intention to analyse the various available models and extract the common phases and propose a

new general purpose model so that we can have a common starting model that would be applicable to any scenarios.

1.1. Terminologies

In the course of performing the reviews, we have discovered that different terms were used by various authors, in order to reflect the processes taken to perform the proposed investigation. Among the terms used were *model*, *procedure*, *process*, *phase*, *tasks*, etc. In order not to be drawn into a lengthy discussion as to which terms is best to be used, we choose to still maintain whatever terms used by the original authors, when describing their respective processes. However, when conducting comparison and indentifying common characteristics, we need to use one term only (for the purpose of standardization) and chose the term "model" to represent the entire activities performed in a computer forensic investigation. The term "phase" is used to represent the high level component of the investigation model and the term "tasks" is used to represent activities to be performed in each of the phases.

2. INVESTIGATION PROCESS REVIEWED

The number of suggested and proposed investigation models is not small, as such, it would be quite a daunting exercise to review them all. We have indeed, selected the models to be reviewed based on the chronological order, ensuring at least one proposed model per year. We are not suggesting that the selected models are better or superior than the other models that were also introduced in the same year. Our objective is to identify and extract the phases in the investigation models rather than selecting which model is the best.

2.1. Computer Forensic Investigative Process (1984)

Pollitt [2] [3] has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable. It comprises of 4 distinct phases.
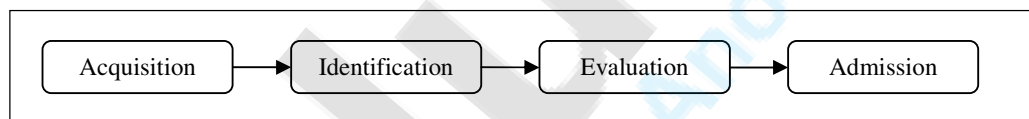

Figure 1: Computer Forensic Investigative Process

In **Acquisition** phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by **Identification** phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human. The **Evaluation** phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, **Admission**, the acquired & extracted evidence is presented in the court of law.

2.2. DFRWS Investigative Model (2001)

In 2001, the 1st Digital Forensics Research Workshop (DFRWS) [4] proposed a general purpose digital forensics investigation process. It comprises of 6 phases.
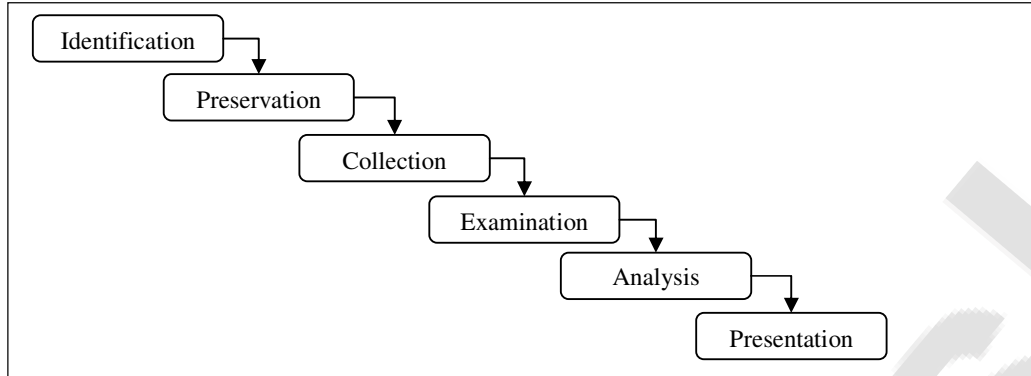
Figure2: DFRWS Investigative Model

DFRWS Investigative model started with an **Identification** phase, in which profile detection, system monitoring, audit analysis, etc, were performed. It is immediately followed by **Preservation** phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody. This phase is crucial so as to ensure that the data collected is free from contamination. The next phase is known as **Collection**, in which relevant data are being collected based on the approved methods utilizing various recovery techniques. Following this phase are two crucial phases, namely, **Examination** phase and **Analysis** phase. In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc, were performed. The last phase is **Presentation**. Tasks related to this phase are documentation, expert testimony, etc.

2.3. Abstract Digital Forensics Model (ADFM) (2002)

Inspired by DFRWS investigative model, Reith, Carr & Gunsch [5], proposed an enhanced model known as Abstract Digital Forensic Model. In this model, the author introduced three additional phases, thus expanding the number of phases to nine.
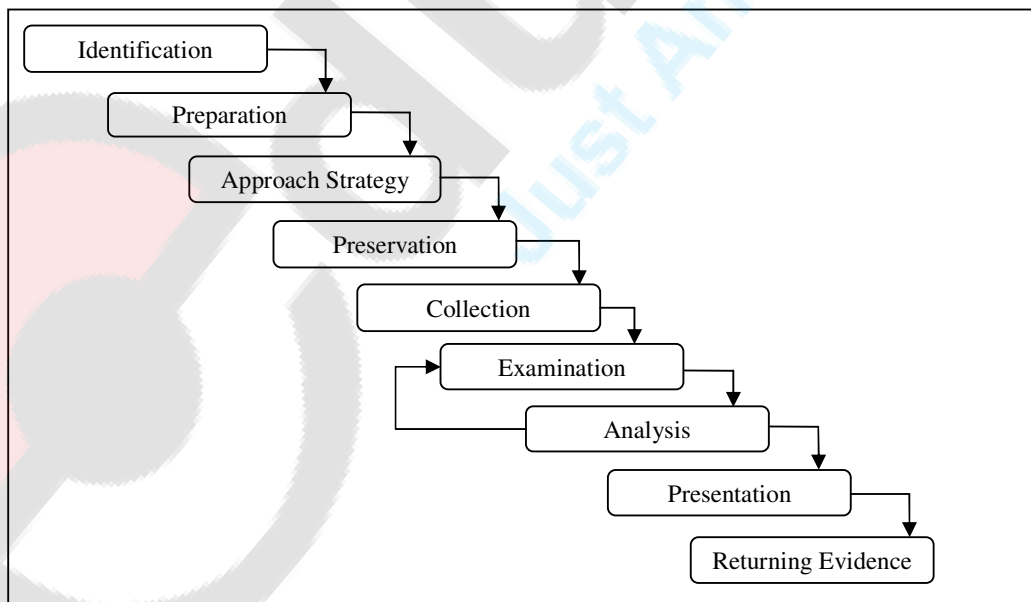

Figure 3: Abstract Digital Forensics Model

The 3 significant phases introduced in this model were Preparation, Approach Strategy and Returning Evidence. In Preparation phase, activity such as preparing tools, identify techniques and getting management support, were done. Approach Strategy was introduced with the objective to maximize the acquisition of untainted evidence and at the same time to minimize any negative impact to the victim and surrounding people. In order to ensure that evidences are safely return to the rightful owner or properly disposed, the Returning Evidence phase was also introduced.

The 1st phase in ADFM is **Identification** phase. In this phase, the task to recognize and determine type of incident is performed. Once the incident type was ascertained, the next phase, **Preparation**, is conducted, followed by **Approach Strategy** phase. Physical and digital data acquired must be properly isolated, secured and preserved. There is also a need to pay attention to a proper chain of custody. All of these tasks are performed under **Preservation** phase. Next is the **Collection** phase, whereby, data extraction and duplication were done. Identification and locating the potential evidence from the collected data, using a systematic approach are conducted in the next following phase, known as **Examination** phase. The task of determining the significant of evidence and drawing conclusion based on the evidence found is done in **Analysis** phase. In the following phase, **Presentation** phase, the findings are summarized and presented. The investigation processes is completed with the carrying out of **Returning Evidence** phase.

2.4. Integrated Digital Investigation Process (IDIP) (2003)

This investigation process was proposed by Carrier & Spafford [6] in 2003, with the intention to combine the various available investigative processes into one integrated model. The author introduces the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of a crime or incident exists.
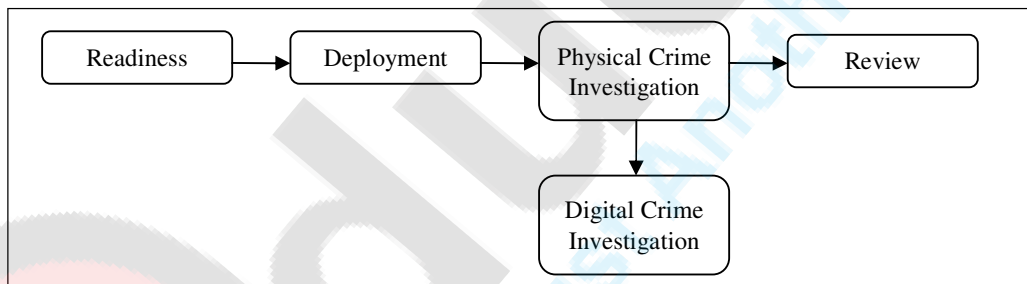

Figure 4: Integrated Digital Investigation Process

The process started with a phase that require for the physical and operational infrastructure to be ready to support any future investigation. In this **Readiness** phase, the equipments must be ever ready and the personnel must be capable to use it effectively. This phase is indeed an ongoing phase throughout the lifecycle of an organization. It also consists of 2 sub-phases namely, *Operation Readiness* and *Infrastructure Readiness*. Immediately following the Readiness phase, is **Deployment** phase, which provide a mechanism for an incident to be detected and confirmed. Two sub-phases are further introduced, namely, *Detection & Notification* and *Confirmation & Authorization*. Collecting and analyzing physical evidence are done in **Physical Crime Scene Investigation** phase. The sub-phases introduced are *Preservation*, *Survey*, *Documentation*, *Search & Collection*, *Reconstruction* and *Presentation*. **Digital Crime Scene Investigation** is similar to Physical Crime Scene Investigation with exception that it is now focusing on the digital evidence in digital environment. The last phase is **Review** phase. The whole

investigation processes are reviewed to identify areas of improvement that may results in new procedures or new training requirements.

2.5. Enhanced Digital Investigation Process Model (EDIP) (2004)

As the name implies, this investigative model is based on the previous model, Integrated Digital Investigation Process (IDIP), as proposed by Carrier & Spafford. The Enhanced Digital Investigation Process Model, also known as EDIP [7] introduces one significant phase known as Traceback phase. This is to enable the investigator to trace back all the way to the actual devices/computer used by the criminal to perform the crime.
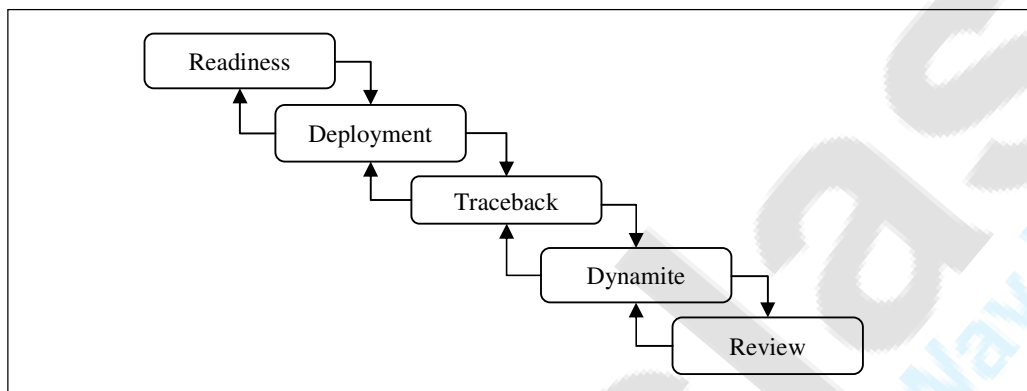

Figure 5: Enhanced Digital Investigation Process Model

The investigation process started with **Readiness** phase and the tasks performed are the same as in IDIP. The second phase, **Deployment** phase, provides a mechanism for an incident to be detected and confirmed. It consists of 5 sub-phases namely *Detection & Notification*, *Physical Crime Scene Investigation*, *Digital Crime Scene Investigation*, *Confirmation* and lastly,*Submision*. Unlike DIP, this phase includes both physical and digital crime scene investigations and presentation of findings to legal entities (via Submission phase). In **Tracebak** phase, tracking down the source crime scene, including the devices and location is the main objective. It is supported by two sub-phases namely, *Digital Crime Scene Investigation* and *Authorization* (obtaining approval to perform investigation and accessing information). Following Traceback phase is **Dynamite** phase. In this phase, investigation are conducted at the primary crime scene, with the purpose of identifying the potential culprit(s). Consist of 4 sub-phases, namely, *Physical Crime Scene Investigation*, *Digital Crime Scene Investigation*, *Reconstruction* and *Communication*. In Reconstruction sub-phase, pieces of information collected are put together so as to construct to possible events that could have happened. The Communication sub-phase is similar to the previous Submission phase. The investigation process ended with **Readiness** phase and the tasks performed are the same as in IDIP.

2.6. Computer Forensics Field Triage Process Model (CFFTPM) (2006)

The CTTTPM [8] proposes an onsite approach to providing the identification, analysis and interpretation of digital evidence in a relatively short time frame without the need to take back the devices or media back to the lab. Nor does it require taking the complete forensic images. The CFFTPM consist of 6 primary phases that are then further divided into another 6 sub-phases
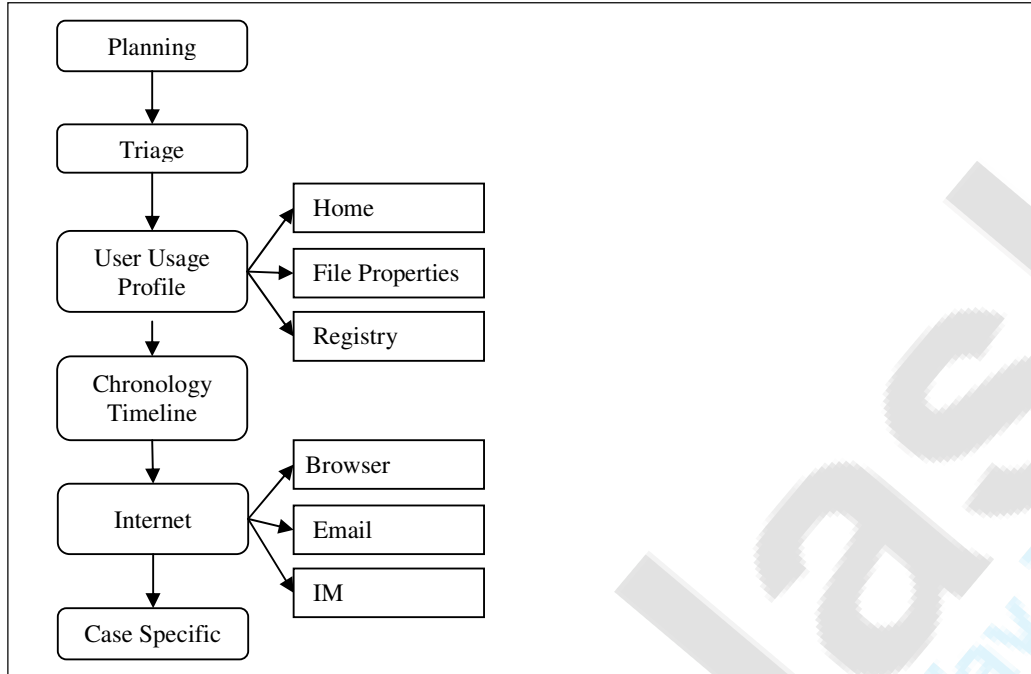
Figure 6: Computer Forensics Field Triage Process Model

CFFTPM started with a familiar phase, **Planning** phase. Proper planning prior to embarking an investigation will surely improve the success rate of an investigation. Following Planning phase is **Triage** phase. In this phase, the evidence are identified and ranked in terms of importance or priority. Evidence with the most important and volatile need to be processed first. The **User Usage Profile** phase focus its attention to analyse user activity and profile with the objective of relating evidence to the suspect. Building the crime case from chronological perspective by making use of MAC time (for example) to sequence the probable crime activities is the main objective of **Chronology Timeline** phase. In the **Internet** phase, the tasks of examining the artefacts of internet related services are performed. Lastly, in Case Specific Evidence phase, the investigator can adjust the focus of the examination to the specifics of the case such as the focus in child pornography would indeed be different than that of financial crime cases.

2.7. Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) (2009)

In 2009, Perumal, S. [9] proposed yet another digital forensic investigation model which is based on the Malaysian investigation processes. The DFMMIP model consist of 7 phases.
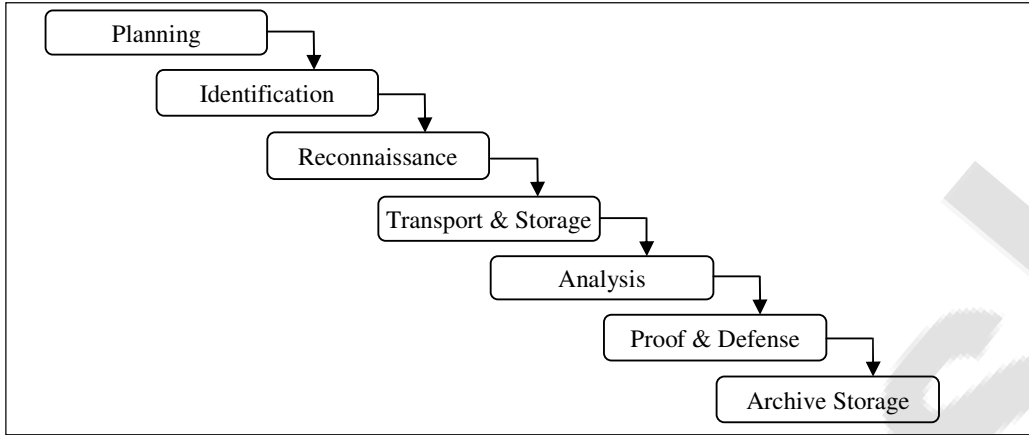
Figure 7: DFMMIP model

Upon completion of the 1st phase, **Planning**, the next phase, **Identification**, followed. After that, **Reconnaissance** phase is conducted. This phase deals with conducting the investigation while the devices are still running (in operation) which is similar to performing live forensics. The author argued that the presence of live data acquisition that focuses on fragile evidence does increase the chances of positive prosecution. Before data can be analyzed, they must be securely transported to the investigation site and be properly stored. This is indeed done in **Transport & Storage** phase. Once the data is ready, **Analysis** phase is invoked and the data will be analyzed and examined using the appropriate tools and techniques. Similar to the Presentation phase in the previous models, the investigators will be required to show the proof to support the presented case. This is done in **Proof & Defense** phase. Finally, Archive Storage phase is performed, whereby relevant evidence are properly stored for future references and perhaps can also be used for training purposes.

3. OTHER INVESTIGATION PROCESS REVIEWED

Due to the impractically of reviewing more models with the same details as above, we have decided to create this section to still discuss on other investigation models. However, in this section, we only highlight the phases which are the uppermost level of the investigation process. There are also presented in the chronological order and the fact they are discussed in this section does not indicate that they are inferior to those investigation processes discuss in Section 2.

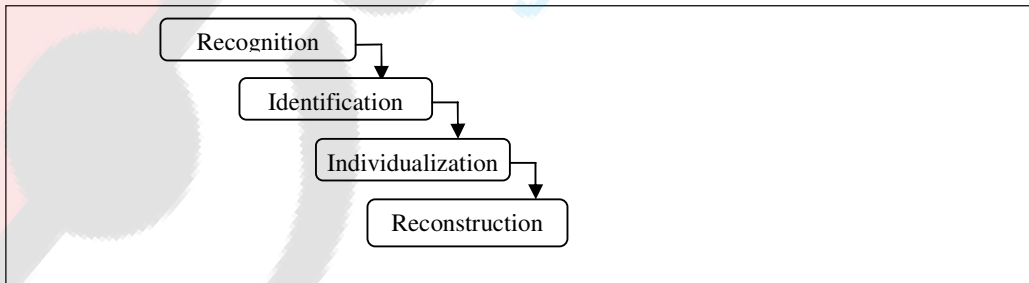### 3.1. Scientific Crime Scene Investigation Model (2001) [10]

Figure 8: SCSI

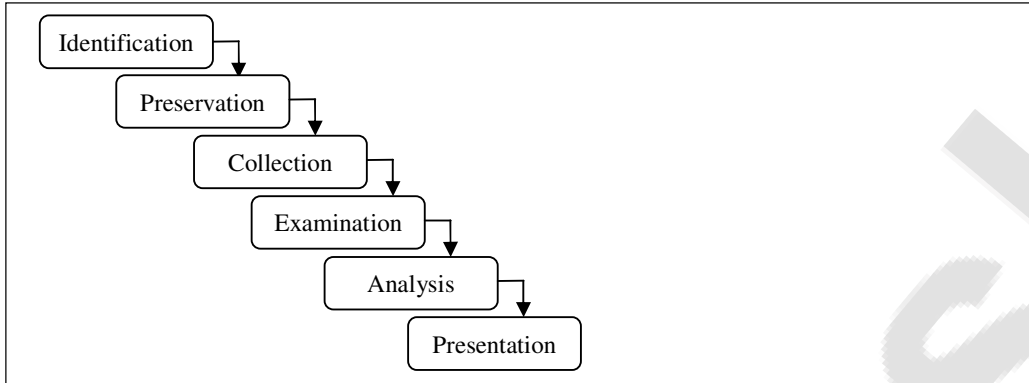### 3.2. End to End Digital Investigation (2003) [11]

Figure 9: EEDI

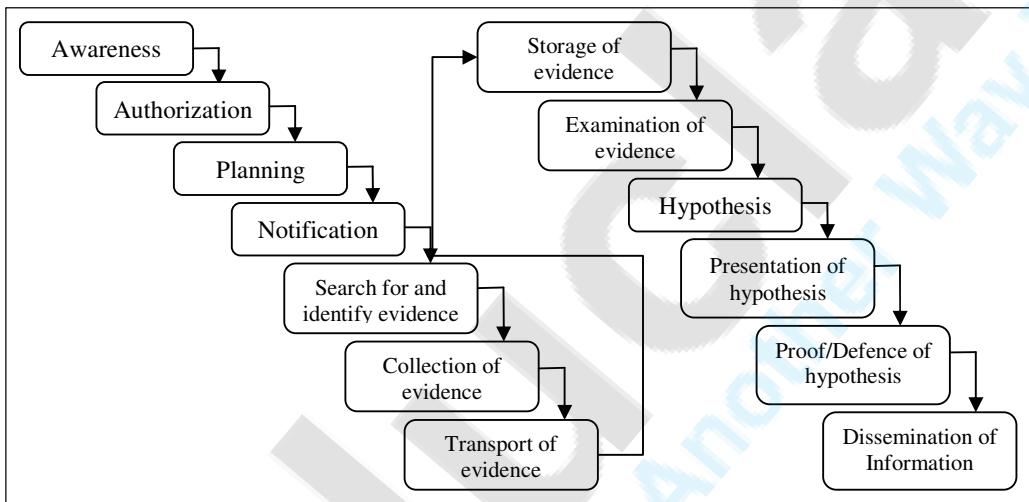### 3.3. Extended Model of Cybercrime Investigation (2004) [10]

Figure 10: EMCI

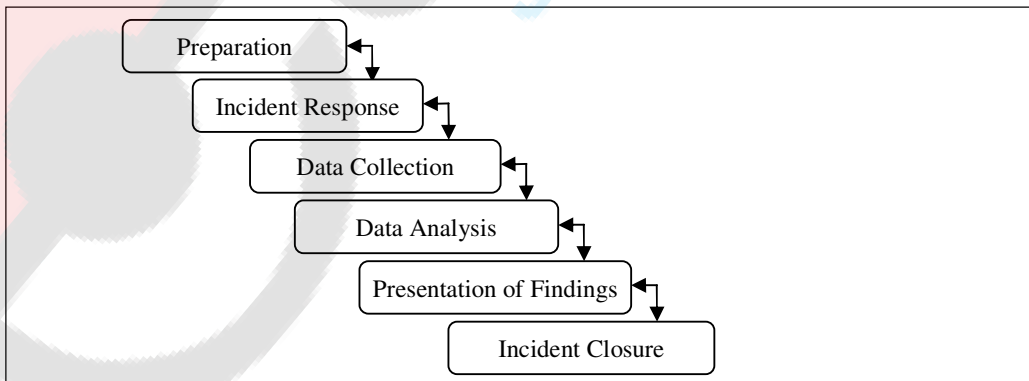### 3.4. A Hierarchical, Objective-Based Framework for the Digital Investigations Process (2004) [12]

Figure 11: HOBF

3.5. Framework for a Digital Forensic Investigation(2006) [13]
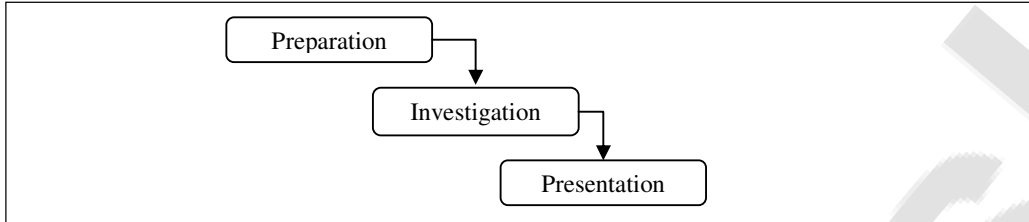

Figure 12: FDFI

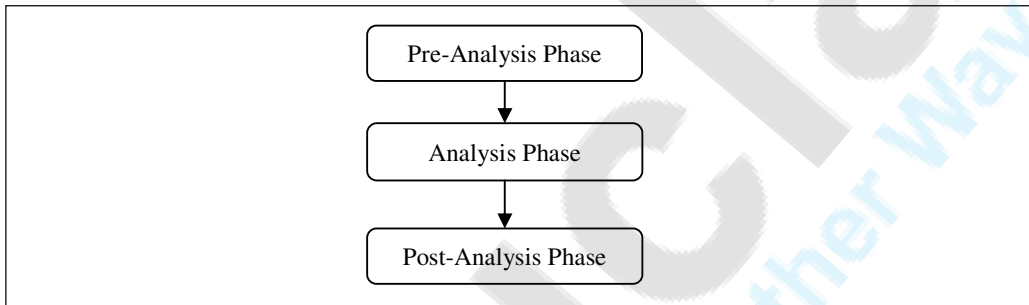## 3.6. Common Process Model for Incident and Computer Forensics (2007) [14]

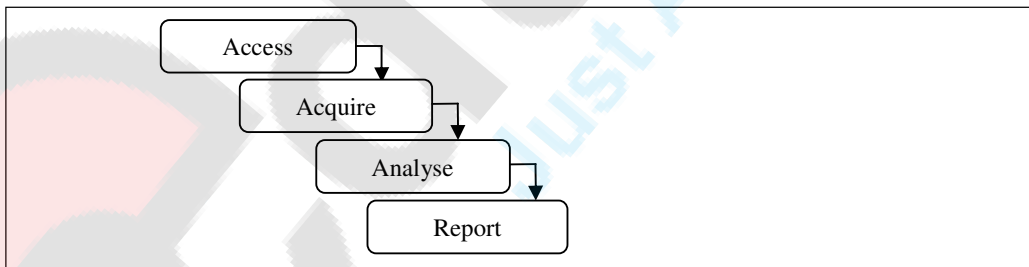Figure 13: CPMICF

3.7. Dual Data Analysis Process (2007) [15]

Figure 14: DDAP

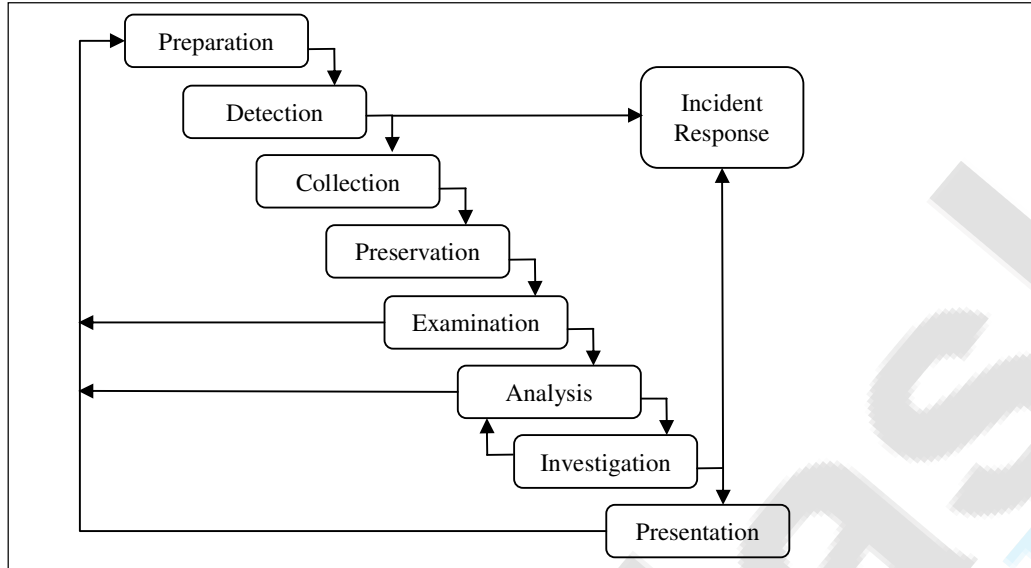## 3.8. Network Forensic Generic Process Model (2010) [16]

Figure 15: NFGP

4. IDENTIFYING COMMON PHASES

In order to identify the common phases shared by all of the presented models, we started by assigning the investigation models with unique id and sorted them in chronological order. The result is displayed in Table 1, below.

Table 1: Investigation processes/models

ID	Year	Name
M01	1995	Computer Forensic Investigative Process
M02	2001	DFRWS Investigative Model
M03	2001	Scientific Crime Scene Investigation Model
M04	2002	Abstract Digital Forensic Model
M05	2003	Integrated Digital Investigation Process
M06	2003	End to End Digital Investigation
M07	2004	Enhance Digital Investigation Process
M08	2004	Extended Model of Cybercrime Investigation
M09	2004	A Hierarchical, Objective-Based Framework for the Digital Investigation
M10	2006	Computer Forensic Field Triage Process Model
M11	2006	Framework for a Digital Forensic Investigation
M12	2007	Dual Data Analysis Process
M13	2007	Common Process Model for Incident and Computer Forensics
M14	2009	Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)

M15	2010	Network Forensic Generic Process Model

Once the investigation processes were identified, the next step is to extract all of the phases within each of the investigation processes. Extracted phases were assigned with unique id. Phases with similar tasks are grouped together. The result is displayed in Table 2, below.

Table 2: List of phases

ID	Name of phases	Available in
P01	Access	M12
P02	Acquisition	M01,M12
P03	Admission	M01
P04	Analysis	M02,M04.M13, M14,M06,M09,M15
P05	Approach Strategy	M04
P06	Archive Storage	M14
P07	Authorization	M08
P08	Awareness	M08
P09	Case Specific Analysis	M10
P10	Chronology Timeline Analysis	M10
P11	Collection	M02,M04.M06.M08,M09,M15
P12	Deployment	M05,M07
P13	Detection	M15
P14	Digital Crime Investigation	M05
P15	Dissemination of Information	M08
P16	Dynamite	M07
P17	Evaluation	M01
P18	Examination	M02,M04,M06,M08,M15
P19	Hypothesis creation	M08
P20	Identification	M01,M02,M04, M14,M03,M06
P21	Incident Closure	M09
P22	Incident Response	M09,M15
P23	Individualization	M03
P24	Internet Investigation	M10
P25	Investigation	M11, M15
P26	Notification	M08
P27	Physical Crime Investigation	M05

P28	Planning	M10, M14,M08
P29	Post-Analysis	M13
P30	Pre-Analysis	M13
P31	Preparation	M04,M09,M11,M15
P32	Presentation	M02,M04,M06,M08,M09,M11,M15
P33	Preservation	M02,M04,M06,M15
P34	Proof & Defense	M14,M08
P35	Readiness	M05,M07
P36	Recognition	M03
P37	Reconnaissance	M14
P38	Reconstruction	M03
P39	Report	M12
P40	Returning Evidence	M04
P41	Review	M05,M07
P42	Search & Identify	M08
P43	Traceback	M07
P44	Transport & Storage	M14,M08
P45	Triage	M10
P46	User Usage Profile Investigation	M10

Based on the above list of phases (Table 2), it is apparent that a number of those phases do indeed duplicated or overlapped each other. Taking into account of the tasks performed in each of the phases, and not just relying on the actual naming, we were able to observe that the phases can be grouped into 5 generic grouping namely, pre-process, acquisition & preservation, analysis, presentation and post-process. Table 3 below demonstrate how the phases were grouped into their respective generic grouping.

Table 3: Generic Phases

Generic Phases	Available phases
1 Pre-Process	P01, P05, P07, P08, P26, P28, P30, P31, P35, P36,
2 Acquisition & Preservation	P02, P11, P12, P13, P20, P30, P33, P42, P44
3 Analysis	P04. P09, P10, P13, P14, P16, P17, P18, P19, P23, P24, P25, P27, P37, P38, P42, P43, P45, P46
4 Presentation	P03, P29, P32, P34, P39,
5 Post-Process	P06, P15, P21, P22, P40, P41,

Based on our study of other investigation models, not discussed in here, each of their recommended phases can also be placed in at least one of the above generic phases. Therefore, we proposed the below generic investigation process, to be known as Generic Computer Forensic Investigation Model (GCFIM). Figure 1.6 below, illustrate the proposed GCFIM.
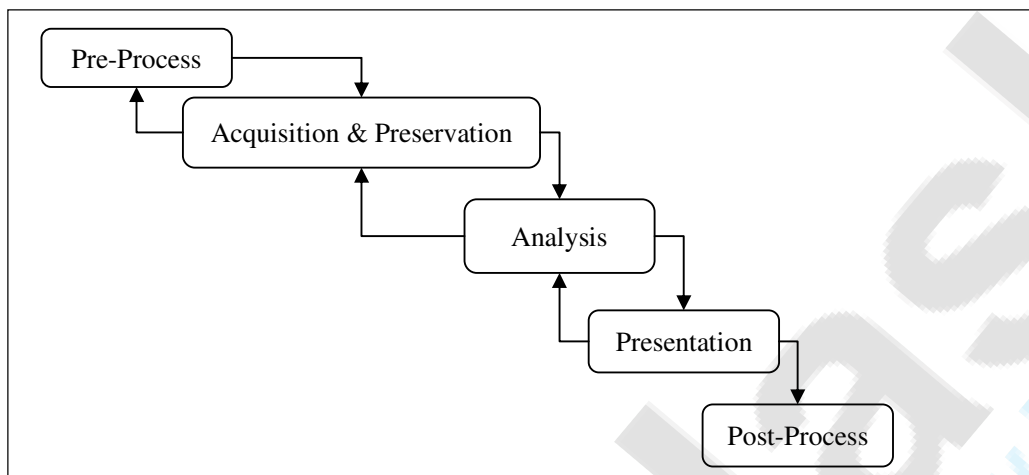

Figure 16: Generic Computer Forensic Investigation Model (GCFIM)

Phase 1 of GCFIM is known as *Pre-Process*. The tasks performed in this phase relates to all of the works that need to be done prior to the actual investigation and official collection of data. Among the tasks to be performed are getting the necessary approval from relevant authority, preparing and setting-up of the tools to be used, etc.

Phase 2 is known as *Acquisition & Preservation*. Tasks performed under this phase related to the identifying, acquiring, collecting, transporting, storing and preserving of data. In general, this phase is where all relevant data are captured, stored and be made available for the next phase.

Phase 3 is known as *Analysis*. This is the main and the center of the computer forensic investigation processes. It has the most number of phases in its group thus reflecting the focus of most models reviewed are indeed on the analysis phase Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime.

Phase 4 is known as *Presentation*. The finding from analysis phase are documented and presented to the authority. Obviously, this phase is crucial as the case must not only be presented in a manner well understood by the party presented to, it must also be supported with adequate and acceptable evidence. The main output of this phase is either to prove or refute the alleged criminal acts

Phase 5 is known as *Post-Process*. This phase relates to the proper closing of the investigation exercise. Digital and physical evidence need to be properly returned to the rightful owner and kept in safe place, if necessary. Review of the investigative process should be done so that the lesson can be learnt and used for improvement of the future investigations.

Instead of moving sequentially from one phase to another, the ability to go back to the previous phases must always be present. We are dealing with the situations that are forever changing in terms of the crimes scenes (physical and digital), the investigative tools used, the crime tools

used and the level of expertise for the investigators. As such, it is much desired to be able to go back to the previous phases that we have done, not only to correct any weaknesses but also to acquire new things/information.

We wish to note that phase numbered P22 (in Table 2) was put in Post-Process phase (in Table 3) which is due to our belief, that action or response to any incident should be done after the incident was properly analyzed and presented to the authority. Nevertheless, should the investigator found a very risky and high impact incident, prerogative is up to the investigator to take any proper immediate actions. However, this is a deviation to a normal process and should be treated on a case to case basis.

5. CONCLUSIONS

Based on the presented computer forensic investigation processes, we are able to extract the basic common investigation phases that are shared among all models. The differences are in the content of each phase whereby certain scenario may require certain levels or types of details steps. Based on the grouping of the overlapping and similar phases, we have proposed, a new model, Generic Computer Forensic Investigation Model (GCFIM). We hope that GCFIM can serve as the basic and high level investigation models for any future computer forensic investigation. It should also serve as a good starting point for the development of new computer forensic investigation methodology.

REFERENCES

[1]   M. G. Noblett, M. M. Pollitt & L. A. Presley, (2000) "Recovering and Examining Computer Forensic Evidence", Forensic Science Communications, Vol. 2, No. 4.

[2]   M. M. Pollitt, (1995) "Computer Forensics: An Approach to Evidence in Cyberspace", in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491.

[3]   M. M. Pollitt, (2007) "An Ad Hoc Review of Digital Forensic Models", in Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), Washington, USA.

[4]   G. Palmer, (2001) "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York.

[5]   M. Reith, C. Carr & G. Gunsh, (2002) "An Examination of Digital Forensics Models", International Journal of Digital Evidence, Vol. 1, No. 3.

[6]   B. Carrier & E. H. Spafford, (2003) "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol. 2, No. 2

[7]   V. Baryamereeba & F. Tushabe, (2004) "The Enhanced Digital Investigation Process Model", in Proceeding of Digital Forensic Research Workshop, Baltimore, MD.

[8]   M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota, (2006) "Computer Forensic Field Triage Process Model", presented at the Conference on Digital Forensics, Security and Law, pp. 27-40.

[9]   P. Sundresan, (2009) "Digital Forensic Model based on Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol. 9, No. 8.

[10]   S. Ciardhuain, (2004) "An Extended Model of Cybercrime Investigation", International Journal of Digital Evidence, Vol. 3, No. 1, pp. 1-22.

[11]   P. Stephenson, (2003) "A Comprehensive Approach to Digital Incident Investigation.", Information Security Technical Report, Vol. 8, Issue 2, pp 42-52.

[12]   N. L. Beebe & J. G. Clark, (2004) "A Hierarchical, Objective-Based Framework for the Digital Investigations Process", in Proceeding of Digital Forensic Research Workshop (DFRWS), Baltimore, Maryland.

[13]   M. Kohn, J. H. P. Eloff, & M. S. Olivier, (2006) "Framework for a Digital Forensic Investigation", in Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa.

[14]   F. C. Freiling & B. Schwittay, (2007) "Common Process Model for Incident and Computer Forensics", in Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgard, Germany, pp. 19-40.

[15]   D. Bem & E. Huebner, (2007) "Computer Forensic Analysis in a Virtual Environment", International Journal of Digital Evidence, vol. 6, no. 2, pp. 1-13.

[16]   E. S. Pilli, R. C. Joshi, & R. Niyogi, (2010) "Network Forensic frameworks: Survey and research challenges," Digital Investigation, Vol. 7, pp. 14-27.

Authors

Yunus Yusoff is currently pursuing a PhD in the field of computer forensics focusing on the trustworthiness of digital evidence. Prior to joining education field, he has extensive working experience in banking industry, managing a department specializing in the information security and disaster recovery.