International Journal of Information Technology and Management

Vol. VIII, Issue No. XII, May-2015, ISSN 2249-4510

AN ANALYSIS UPON VARIOUS PROCESS AND MODEL OF DIGITAL FORENSIC INVESTIGATION

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

An Analysis upon Various Process and Model of Digital Forensic Investigation

Patel Hiteshkumar Gunvantbhai[1] Dr. Jigar Patel[2]

[1]Research Scholar, Mewar University, Chittorgarh, Rajasthan, India

[2] Associate Professor, Kalol Institute of Management, GTU, Gujarat, India

Abstract – Computer Forensics is essential for the successful prosecution of computer criminals. For a forensic investigation to be performed successfully there are a number of important steps that have to be considered and taken. The aim of this paper is to define a clear, step-by-step framework for the collection of evidence suitable for presentation in a court of law. Existing forensic models will be surveyed and then adapted to create a specific application framework for single computer, entry point forensics.

The research introduces a structured and consistent approach for digital forensic investigation. Digital forensic science provides tools, techniques and scientifically proven methods that can be used to acquire and analyze digital evidence. The digital forensic investigation must be retrieved to obtain the evidence that will be accepted in the court. This research focuses on a structured and consistent approach to digital forensic investigation. This research aims at identifying activities that facilitate and improves digital forensic investigation process. Existing digital forensic framework will be reviewed and then the analysis will be compiled. The result from the evaluation will produce a new model to improve the whole investigation process.

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

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. 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.

Over the past few years, computer forensics has risen to the fore as an increasingly important method of identifying and prosecuting computer criminals. Prior to the development of sound computer forensics procedures and techniques, many cases of computer crime were left unsolved. There are many reasons why an investigation might not lead to a successful prosecution, but the predominant one is a lack of preparation. The organization investigating the suspicious behavior often lacks the tools and skills required to successfully gather evidence. Individuals attempting to investigate such suspicious activity may also lack the financial resources financial resources or tools to conduct such an investigation adequately and ensure that the evidence is undisputable in all circumstances. Moreover, there are instances when all of the above have been adequately put in place by an organization, but, due to a lack of training and correct procedure, the evidence collected can easily be disputed.

As a result, computer forensics seeks to introduce cohesion and consistency to the wide field of extracting and examining evidence obtained from a computer at a crime scene. In particular, the extraction of evidence from a computer is performed in such a way that the original incriminating evidence is not compromised. This is also useful when presenting a case without the support of legal expertise, as is often the situation since many organizations and individuals do not have in-house or personal legal representation.

There is an old saying that prevention is better than cure. When applied to forensic frameworks this would seem to imply that preparation is the key to conducting a successful forensic investigation. Although preparation is important, it is impossible to be prepared for all types of behavior. A sound base of previous knowledge and experience will always help, but a suggestion or documented case is not a complete resolution to solving a problem.

The number of forensic models that have been proposed reveals the complexity of the computer forensic process. Most focus on either the investigation itself or emphasize a particular stage of the investigation frameworks this would seem to imply that preparation is the key to conducting a successful forensic investigation. Although preparation is important, it is impossible to be prepared for all types of behaviour. A sound base of previous knowledge and experience will always help, but a suggestion or documented case is not a complete resolution to solving a problem.

The number of forensic models that have been proposed reveals the complexity of the computer forensic process. Most focus on either the investigation itself or emphasize a particular stage of the investigation.

Kruse and Heiser refer to a computer forensic investigation methodology with three basic components. They are: acquiring the evidence; authenticating the evidence, and analyzing the data. These components focus on maintaining the integrity of the evidence during the investigation.

The United States of America's Department of Justice proposed a process model for forensics. This model is abstracted from technology. This model has four phases: collection; examination; analysis, and reporting. There is a correlation between the 'acquiring the evidence' stage identified by Kruse and Heiser and the 'collection' stage proposed here. 'Analyzing the data' and 'analysis' are the same in both frameworks.

Kruse has, however, neglected to include a vital component: reporting. This is included by the Department of Justice framework. The Scientific Crime Scene Investigation Model proposed by Lee consists of four steps. They are: recognition; identification; individualization, and reconstruction. These steps only refer to a part of the forensic investigation process. These steps all clearly fall within the 'investigation' stage of the process; there is neither a 'preparation' nor 'presentation' stage either side.

Casey proposes a framework similar to Lee. This framework focuses on processing and examining digital evidence. The steps included are: recognition; preservation; classification, and reconstruction. In both Lee and Casey's models, the first and last steps are identical. Casey also places the focus of the forensic process on the investigation itself.

The Digital Forensics Research Working Group (DFRW) developed a framework with the following steps: identification; preservation; collection; examination; analysis; presentation, and decision. This framework puts in place an important foundation for future work and includes two crucial stages of the investigation. Components of an investigation stage as well as presentation stage are present.

In the digital forensics investigation practices, there are over hundreds of digital forensics investigation procedures developed all over the world. Each organization tends to develop its own procedures. Some focused on the technology aspects in data acquisition, some focused on data analysis portion of the investigation.

As many of these procedures were developed for tackling different technology used in the inspected device, when underlying technology of the target device changes, new procedures has to be developed.

The majority of organization relies deeply on digital devices and the internet to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. Recent study demonstrates that in 2008, 98% of all document created in organization were created electronically (Sommer 2009). According to Healy (2008) approximately 85% of 66 million U.S. dollars was lost by organizations due to digital related crime in 2007. Panda labs (2009) show that in 2008, Ehud Tenenbaum was extradited from Canada on suspicion of stealing $1.5million from Canadian bank through stolen credentials and infiltrated computers. Williams (2009) states on cybercrime report, a complex online fraud which scammed over £1 million pounds from taxpayers in 2009.

This research focuses on a structured and consistent approach to digital forensic investigation procedures.

The research questions for the research are formulated with the aim to map out a structured and consistent approach and guideline for digital forensic investigation. This research focuses on identifying activities that facilitate digital forensic investigation, emphasizing on what digital crimes are and describing the shortcomings of current models of digital forensic investigation.

FUNDAMENTAL PRINCIPLE

In IT Security field, there are a lot of technological aspects, such as access control, biometrics, encryption, network security, security algorithm, etc. Each of them has its specific methodology and school of thoughts, but they all rely on one set of fundamental principles. That is, the core IT Security fundamentals – Confidentiality, Integrity and Availability.

With this core principle, different areas of IT Security are linked together. IT Security development, assessment and audit view across different organizations all rely on the core IT Security fundamental principle.

Similarly, digital forensics investigation should also have a core principle that enables the practitioners to view the underlying concept across different digital forensics investigation procedures. Digital Forensics Investigation is a process to determine and relate extracted information and digital evidence to establish factual information for judicial review.

To accomplish this requirement, its fundamental principle includes Reconnaissance, Reliability, and Relevancy.

- Reconnaissance: Similar to what needs to be performed before ethical hacking, a digital forensics investigator needs to exhaust different methods, practices and tools that were developed for particular operating environment to collect, recover, decode, discover, extract, analyze and convert data that kept on different storage media to readable evidence. No matter where data are stored, digital forensics investigators should be revealing, and focusing retrieval of the truth behind the data.

- Reliability: Extracting of data is not simply copying of data using Windows Explorer or saving files to a disk. Chain of evidence should be preserved during extracting, analyzing, storing and transporting of data. In general, chain of evidence, time, integrity of the evidence and the person relationship with the evidence could be collectively considered as the non-repudiation feature of digital forensics. If the evidence cannot be repudiated and rebutted, then the digital evidence would be reliable and admissible for judicial review.

- Relevancy: Even though, evidence could be admissible, relevancy of the evidence with the case affects the weight and usefulness of the evidence. If the legal practitioner can advise on what should be collected during the process, time and cost spent in investigation could be controlled better.

DIGITAL FORENSIC PROCESS

A digital forensic process uses science and technology to examine digital objects and develops and tests theories. The digital forensics process can be categorized into four different phases as collection, examination, analysis and reporting.

Collection: The first phase of digital forensics process is collection phase. The first step in the forensic process is to identify, label, record, and acquire data from the possible sources of relevant data.

Examination: The next phase is to examine collected data, which involves assessing and extracting the relevant pieces of information from the collected data.

Analysis: The next phase of the process is to analyse the results of the examination. Extracted and relevant data has been analysed to draw conclusion.

Reporting: The final phase is reporting the results of analysis; this is the process of preparing and presenting the outcome of the analysis phase.

A. Computer Forensic Investigative Process (1984) -

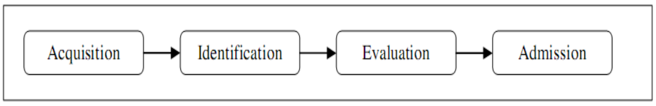


Figure 1: Computer Forensic Investigative Process

Methodology for dealing with digital evidence investigation was proposed by Pollitt. It has 4 distinct phases. 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.

B. DFRWS Investigative Model (2001) –

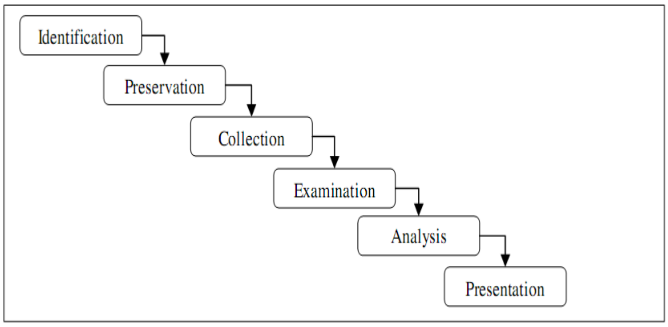


Figure 2: DFRWS Investigative Model

G. Palmer held the 1st Digital Forensics Research Workshop (DFRWS) and proposed a general purpose digital forensics investigation process. It has 6 phases. 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.

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

- Reith, Carr & Gunsch, proposed an enhanced model known as Abstract Digital Forensic Model. In this model, there is three additional phases than DFRWS, thus expanding the number of phases to nine.

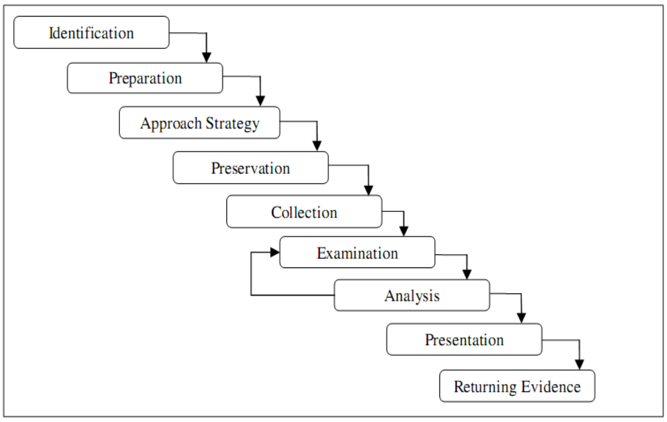


Figure 3: Abstract Digital Forensics Model

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.

D. Integrated Digital Investigation Process (IDIP) (2003) -

Integrated Digital investigation process was proposed by Carrier & Safford in 2003, 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 an incident or crime exists.

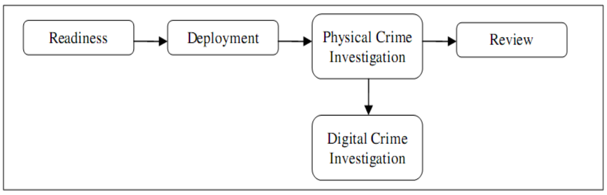


Figure 4: Integrated Digital Investigation Process

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.

E. 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 & Safford. The Enhanced Digital Investigation Process Model, also known as EDIP [7] introduces one significant phase known as Trace back 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.

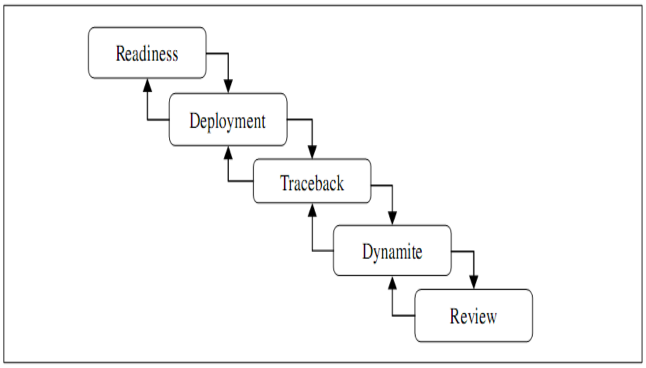


Figure 5: Enhanced Digital Investigation Process Model

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, Submission. Unlike DIP, this phase includes both physical and digital crime scene investigations and presentation of findings to legal entities (via Submission phase). In **Trackback** 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 Trace back phase is **Dynamite** phase. In this phase, investigations 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.

F. 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.

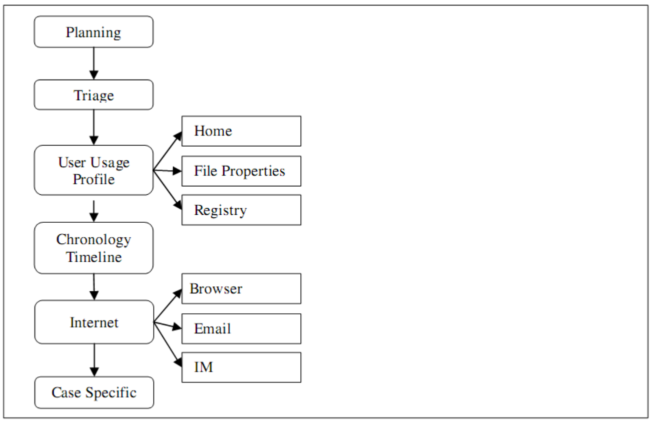


Figure 6: Computer Forensics Field Triage Process Model

The CFFTPM consist of 6 primary phases that are then further divided into another 6 sub-phases 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 focuses 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.

G. 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 consists of 7 phases.

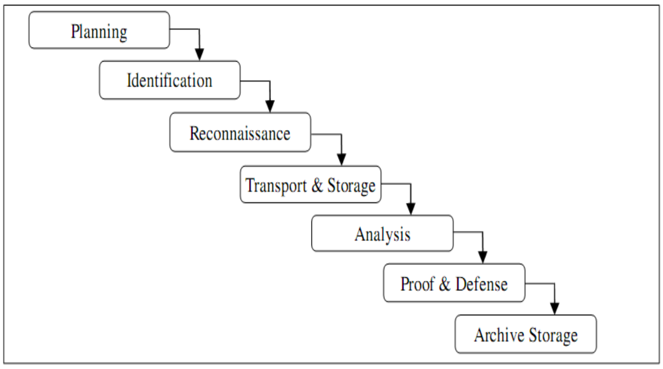


Figure 7: DFMMIP model

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 is properly stored for future references and perhaps can also be used for training purposes.

THE DIGITAL INVESTIGATION PROCESS MODEL

We will now describe the process model that we propose. This model is based on the phases that are documented for investigating physical crime scenes. The phases are applied to a digital crime scene, where we consider the digital crime scene investigation to occur as a subset of a physical crime scene investigation. The general concepts of this model have already been published. It is organized into five categories of phases, as shown in Figure 8.

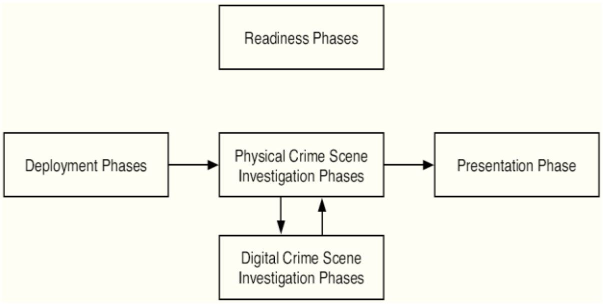

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Presentation Phase
Digital Crime Scene Investigation Phases

Figure 8: Graphical representation of the major categories of phases in the framework.

Readiness Phases: Includes the operations readiness phase that trains the appropriate people and tests the tools that will be used to investigate a system. The infrastructure readiness phase configures the equipment to help ensure that the needed data exists when an incident occurs. For example, in a corporate or military environment this could include adding network monitoring tools and increasing the logging levels.

Deployment Phases: Includes the detection and notification phase where the incident is detected by the victim or another party and the investigators are alerted. For example, a network intrusion could be detected by an intrusion detection system and a contraband incident could be detected using the logs or communications of the suspect. This category of phases also includes the confirmation and authorization phase where the investigators receive authorization to conduct the investigation. In a corporate environment, this could include the incident response team doing a brief analysis of a system to confirm that it has indeed been compromised. If it is a critical system, additional permission may be needed before a full analysis can be conducted. In a law enforcement environment, the officer may need to obtain a search warrant before the investigation can progress.

Physical Crime Scene Investigation Phases: After authorization for the investigation has been granted, the physical investigation begins and the physical objects at the crime scene where a digital device exists are examined. It is in this set of phases where physical evidence will be collected that could link a person to the suspect computer activity. This set of phases includes the search for physical evidence and the reconstruction of physical events. When a physical object is found that may have digital evidence in it, a digital investigation begins. This phase will receive and correlate the analysis results from one or more digital crime scene investigations.

Digital Crime Scene Investigation Phases: Includes the phases that examine the digital data for evidence. This set of phases is actually a subset of the physical crime scene investigation phases and the conclusions that are made from the digital investigation will be used in the physical investigation. An investigation occurs for each self-contained digital device. We will examine this phase in more detail in this paper. In general, this process involves the preservation of the system, the search for digital evidence, and the reconstruction of digital events.

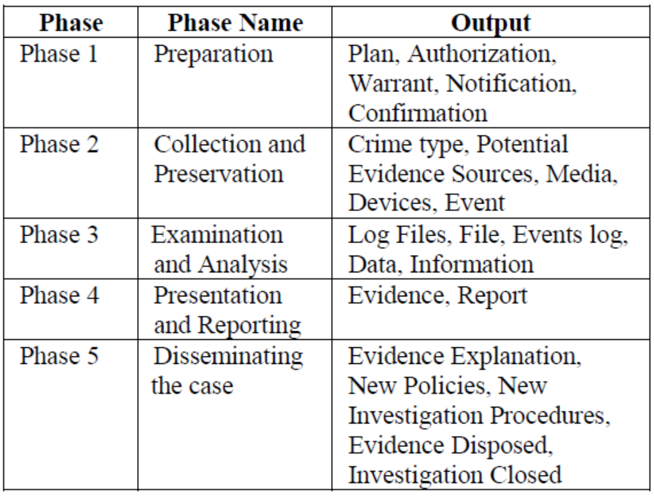
Presentation Phase: After theories have been developed and tested about the events related to the incident, the results must be presented to either a corporate audience or a court of law. This phase deals with that process.

MAPPING PROCESS

This paper proposes a map of Digital Forensic Investigation Framework (DFIF) by grouping and merging the same activities or processes that provide the same output into an appropriate phase. This mapping process is designed in order to balance the process on achieving the overriding goal that can produce concrete evidence for presentation in a court of law. In this research, the steps implemented to design mapping process of the DFIF are as the following:

Step 1 - Identify existing frameworks - In this step, the phases, activities/processes and output for each framework is analyzed.

Step 2 - Construct phase name - In this step, phase name is constructed based on the activities/processes and output analyzed from step 1. Five phases has been named (i.e. Phase 1 – Phase 5)



Phase	Phase Name	Output
Phase 1	Preparation	Plan, Authorization, Warrant, Notification, Confirmation
Phase 2	Collection and Preservation	Crime type, Potential Evidence Sources, Media, Devices, Event
Phase 3	Examination and Analysis	Log Files, File, Events log, Data, Information
Phase 4	Presentation and Reporting	Evidence, Report
Phase 5	Disseminating the case	Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Investigation Closed

Table 1: Summarization of the Output Mapping.

Step 3 – Mapping the process - An analysis has been done in this step where the appropriate activities/processes and output is mapped into the new phase name.

CONCLUSION

Digital evidence must be admissible, precise, authenticated and accurate in order to be accepted in the court. Digital evidence is fragile in nature and they must be handled properly and carefully. A detailed digital forensic procedure provides important assistance to forensic investigators in gathering evidence admissible in the court of law.

In completing the proposed research, I will learn how apply the proposed system to digital forensic investigation. Bearing this in mind, my expected result, are firstly, to develop a model from relevant domains and bodies of theory of digital forensic and secondly a set of implementable guidelines of digital forensic investigation will be identified.

The digital forensic community needs a structured framework for rapid development of standard operational procedures that can be peer – reviewed and tested effectively and validated quickly.

Digital forensic practitioners can benefit from the iterative structure proposed in this research to build forensically sound case and also for the development of consistent and simplified forensic guides on digital forensic investigation that can be a guideline for standard operational procedure and a model for developing future technology in digital forensic investigation.

This paper starts with the digital forensic process then moves on the digital forensic investigation models. Here, we have discussed Computer Forensic Investigative Process, DFRWS Investigative Model, Abstract Digital Forensics Model and Integrated Digital Investigation Process. Each phase has a clear goal and requirements and procedures can be developed accordingly. Each model must be evaluated with respect to how it can handle different types of investigations. Based on the digital forensic investigation processes, we are able to extract the basic common investigation phases that are shared among all models.

REFERENCES

- Agrawal, A. Gupta, M. Gupta, S. Gupta, C. (2011) Systematic digital forensic investigation model Vol. 5 (1)

- B. Carrier & E. H. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol. 2, No. 2,2003.

- Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process

Model. *Proceeding of Digital Forensic Research Workshop*. Baltimore, MD.

- Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital forensics research workshop (DFRWS); 2004.

- Brian Carrier and Eugene H. Spafford. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Fall 2003.

- 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.

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

- 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.

- M. M. Pollitt, “Computer Forensics: An Approach to Evidence in Cyberspace”, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491,1995.

- Reith, M., Carr, C. and Gunsch, G.:An Examination of Digital Forensic Models, International Journal of Digital Evidence. Fall 2002, Volume 1, Issue 3, 2002.

- Sabah Al-Fedaghi and Bashayer Al-Babtain, “Modeling the Forensics Process”, International Journal of Security and Its Applications, Vol. 6, No. 4, pp. 97-108, October, 2012.

- Sindhu. K. K. and Dr. B. B. Meshram, “A Digital Forensic Tool for Cyber Crime Data mining”, IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498,Vol.2, No.1, pp. 117-124, 2012.

- Stuart James and Jon Nordby, editors. Forensic Science: An Introduction to Scientific and Investigative Techniques. CRC Press, 2003.

- Venansius Baryamureeba and Florence Tushabe, ”The Enhanced Digital Investigation Process Model”,Asian Journal of Information Technology, 5(7), pp. 790-794, 2006.

- Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, ” Common Phases Of Computer Forensics Investigation Models”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, pp. 17-31, June 2011.