International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

A New Approach of Digital Forensic Model for Digital Forensic Investigation

P.V.S. Sriram

Asst. Professor, Dept. of M.C.A, K.B.N College, Vijayawada

Abstract— 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.

Keywords – Case Relevance; Exploratory Testing; Automated Collection; Pre-Analysis; Post-Analysis; Evidence Reliability

I. INTRODUCTION

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.

II. BACKGROUND AND RELATED WORK

Nikkel (2006) defined digital forensic as the use of scientifically derived and proven methods toward the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. The term digital forensics comprises a wide range of computer activity. Not just evidence from computer, e.g. disk drive and computer memory, but including all sorts of generic media, cell phones, memory sticks, PDA's, network traffic etc. The methodologies from physical forensics are adopted into digital forensics, specific forensic software is created, and comprehensive knowledge is obtained by digital forensic specialist to defeat digital criminality.

Digital Evidence and its Characteristics

Carrier and Spafford (2006) defined digital evidence as a digital data that supports or refutes a hypothesis about digital events or the state of digital data. This definition includes evidence that may not be capable of being entered into a court of law, but may have investigative value, this definition is in agreement to Nikkel, (2006) definition that states, digital evidence as a data that support theory about digital events.

Evidence can be gathered from theft of or destruction of intellectual property, fraud or anything else criminally related to the use of a digital devices. Evidence which is also referred to as digital evidence is any data that can provide a significant link between the cause of the crime and the victim (Perumal, 2009).

Characteristics of digital evidence

Digital evidence is by nature fragile. It can be altered, damaged or destroyed by improper handling or improper examination. It is easily copied and modified, and not easily kept in its original state, precaution should be taken to document, collect, preserve and examine digital evidence (Carrier, 2003)

Digital evidence is a data of investigative value that is stored on or transmitted by a digital device. Therefore digital

evidence is hidden evidence in the same way that Deoxyribonucleic Acid (DNA) or fingerprint evidence is hidden. In its natural state, digital evidence cannot be known by the content in the physical object

(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011

Investigative reports may be required to explain the examination process and any limitation (Pollitt, 2007).

Digital Devices types

Figure 1: Difference examples of Digital Devices

III. EXSITING DIGITAL FORENSIC INVESTIGATION MODELS

The Digital Forensic Research Workshops (DFRWS) 2001

The first DFRWS was held in Utica, New York (2001). The goal of the workshop was to provide a forum for a newly formed community of academics and practitioners to share their knowledge on digital forensic science. The audience was military, civilian, and law enforcement professionals who use forensic techniques to uncover evidence from digital sources. The group created a consensus document that drew out the state of digital forensics at that time. The group agreed and among their conclusions was that digital forensic was a process with some agreed steps. They outline processes such as identification, preservation, collection, examination, analysis, presentation and decision. (Palmer 2001). As shown in figure 4 below the grey boxes at the top of their matrix were identified by the group as fundamental processes, although many will debate the forensic nature of each step of the process. This can be called a comprehensive or an enhanced model of the DOJ model as mentioned above because it was able to cover stages that were not covered in any previous model, such as presentation stage. The main advantage of DFRWS is that it is the first large-scale organization that is lead by academia rather than law enforcement, this is a good direction because it will help define and focus the direction of the scientific community towards the challenge of digital forensic, butthe FRWS model is just a basis for future work.

The Forensic Process Model (2001)

According to Ashcroft (2001) the U.S National Institute of Justice (NIJ) published a process model in the Electronic Crime Scene Investigation. The document serves as a guide for the first responders. The guide is intended for use by law enforcement and other responders who have the responsibility for protecting an electronic crime scene and for the recognition, collection and preservation of digital evidence. The forensic process consists of four phases such as:

Collection: This involves the search for, recognition of, collection of, and documentation of electronic evidence.

Examination: The examination process helps to make the evidence visible and explain its origin and significance. It includes revealing hidden and obscured information and the relevant documentation.

Analysis: This involves studying the product of the examination for its importance and probative value of the case.

Reporting: This is writing a report, outlining the examination process and information gotten from the whole investigation.

Abstract Digital Forensic Model (2002)

Reith, Carr and Gunsch (2002) examined a number of published models/framework for digital forensics. The basis of this model is using the ideas from traditional (physical) forensic evidence collection strategy as practiced by law enforcement (e.g. FBI). The authors argued that the proposed model can be term as an enhancement of the DFRWS model since it is inspired from it. The model involves nine components such as:

Identification – it recognises an incident from indicators and determines its type. This component is important because it impacts other steps but it is not explicit within the field of forensic.

Preparation – it involves the preparation of tools, techniques, search warrants and monitoring authorisation and management support.

Approach strategy – formulating procedures and approach to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim

Preservation –it involves the isolation, securing and preserving . D. The Integrated Digital Investigation Process Model (IDIP) 2003

Carrier and Spafford (2003) proposed a model, which the authors provide a review of previous work and then map the digital investigative process to the physical investigation process. The model known as the Integrated Digital

Investigation Process was organized into five groups consisting of 17 phases.

Enhanced Digital Investigation Process (2004)

Baryamueeba and Tushaba (2004) suggested a modification to Carrier and Spafford's Integrated Digital Investigation Model (2003). In the model, the authors described two additional phases which are trace back and dynamite which seek to separate the investigation into primary crime scene (computer) and secondary crime scene (the physical crime scene). The goal is to reconstruct two crime scenes to avoid inconsistencies.

Extended model of cyber crime investigation

Ciardhuain (2004) argues that the existing models are general models of cybercrime investigation that concentrate only on processing of evidence in cybercrime investigation. The model shown provides a good basis for understanding the process of investigation and captures most of the information flows. Even though the model was generic, it concentrated on the management aspect.

Case-Relevance Information Investigation (2005)

Ruibin, Yun and Gaertner (2005) identified the need of computer intelligence technology to the current computer forensic framework. The authors explained that computer intelligence is expected to offer more assistance in the investigation procedures and better knowledge reuse within and across multiple cases and sharing. First concept that was introduced by the authors is the notion of Seek Knowledge which is the investigative clues which drive the analysis of data. Another concept described by the authors is the notion of Case-Relevance. They used this notion to describe the distinctions between computer security and forensics even defining degrees of case relevance.

Digital Forensic Model based on Malaysian Investigation Process (2009)

Perumal (2009) proposed a model that clearly defines 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 has been included in the model to focus on fragile evidence.

The Systematic digital forensic investigation model SRDFIM (2011)

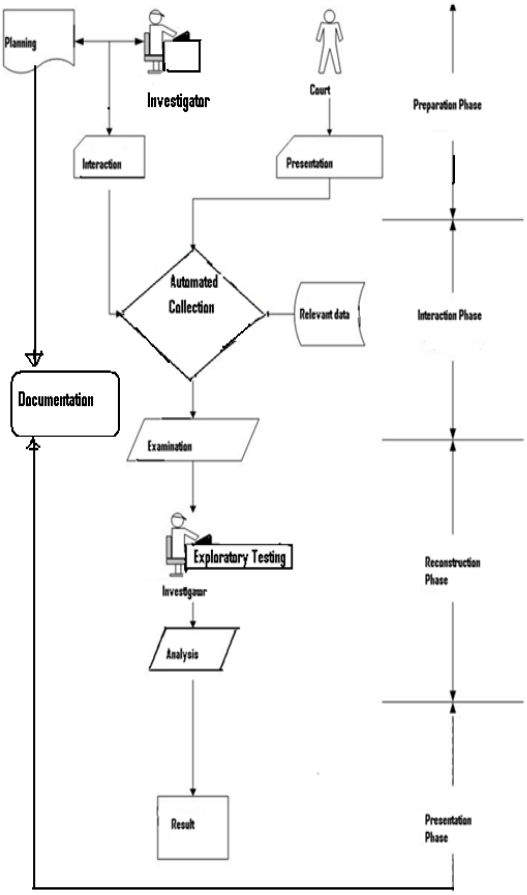
Agawal et al (2011) developed a model with the aim of helping forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner. The proposed model in this paper explores the different processes involved in the investigation of cybercrime and cyber fraud in the form of an eleven stage model. The model focuses on investigation cases of computer frauds and cyber-crimes. The application of the model is limited to computer frauds and cyber-crimes.

IV. PROPOSED MODEL

In the proposed model the digital forensic investigation process will be generalised into 4 tier iteratve approach. The entire digital forensic investigation process can be conceptualized as occuring iterativly in four different phases. The first tier which is the

Figure 2: Proposed digital forensic investigation Model

preparation or inception phase occur over the course of an



investigation from assessment to final presentation phase. The first tier will have 4 rules for digital forensic investigation which involves preparation, identification, authorisation and communication. The second tier will have rules such as

collection, preservation and documentation, the third tier will have rules consisting examination, exploratory testing, and analysis, the 4th tier which is the presentation phase have rules such as result, review and report.

Advantages and Disadvantages of Proposed Model

The model has the advantages obtained from existing model and then expands its scope and provides more advantages. A structured and consistent framework is vital to the development of digital forensic investigation and the identification of areas in which research and development are needed.

The model identifies the need for interaction. Investigator should have consistent interaction with all resources for carrying out the investigation.

Knowing the need of the client/victim and determing to meet the need is important. Better case goal can be defined. Optimal interaction with tools used by investigator is very important. Tools need to be used by people who know how to use them properly following a methodology that meets the legal requirement associated with the particular jurisdiction.

Another advantage of the model is exploratory testing. Investigators need to have the patience, to stay on the target and have to learn any new techniques while performing an investigation. Very little testing has been formalized in this field for the specific need of digital forensic, investigators wishing to be prudent should undertake their own testing methods and this should be a normal part of the process used in preparing for legal matters and this should also meet the leal requirement of the jurisdiction

The model can also help capture the expertise of investigation as a basis to the development of advanced tools incorporating techniques such as automated digital evidence collection.

Generality of the model is not explicit. It must be applied in the context of a crime before it will be possible to make clear the details of the process.

V. 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.

VI. REFERENCES

[1] Agrawal, A. Gupta, M. Gupta, S. Gupta, C. (2011) Systematic digital forensic investigation model Vol. 5 (1) Available (online): http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf Accessed on 30th June 2011

[2] Ashcroft, J (2001) Electronic Crime Scene Investigation: A guide for first responders Available (online): https://www.ncjrs.gov/pdffiles1/nij/187736.pdf Access on 20th October 2011

[3] Baryamureeba, V. Tushabe, F. (2004) The Enhanced digital investigation process (2004) Available (online): http://www.dfrws.org/2004/bios/day1/tushabeEIDIP.pdf Accessed on 15th June 2011

[4] Carrier, B. Spafford, H. (2006), Getting physical with digital forensic process Vol. 2 (2) Available) online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76..pdf Accessed on 20th August 2011

[5] Carrier, B. (2003) Defining digital forensic examination and analysis tools using abstraction layers Vol. 1 (4) Available (online): http://www.cerias.purdue.edu/homes/carrier/forensics Accessed on 20th September 2011