International Journal of Management, IT & Engineering
Vol. 8 Issue 6, June 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

DIGITAL FORENSIC MODELS: A COMPARATIVE ANALYSIS

Dr. Sudesh Rani[1*]

Keywords:

Lucent model;

Abstract model;

DFRWS;

EIPID;

IPID;

NOJ.

Abstract

With increase in new and ever evolving technologies like internet and information technology in the 21st century , the digital crimes are also increasing . the evidence of such crimes which are technology driven are in digital form and need to employ technology inclined techniques to uncover evidence that are admissible in court. Digital forensics applies digital investigation and analysis techniques to help in detection of digital crimes . Digital forensics provide the investigation techniques identification, preservation, collection, validation , analysis documentation and presentation of digital evidences. Different models have been presented to study the basics of digital forensics. Methods used for digital forensic investigation play an important role because inappropriate model choice may result in incomplete of missing evidence. In this paper we study different models. Their strengths and weaknesses and finally make a comparative study that which model is best among them.

[1*] **Asstt. Prof. (Comp. Sc.),Govt. College, Hisar, Haryana, India**

1. Introduction

Forensic computing and cybercrime investigation emerged as a result of increase in computer or digital crime due to the development of the Internet and proliferation of computer technology. The advancement in technology and the rise in online communication have not only brought about increase in criminal activity (with the use of the computer either a tool or target or both in committing crime) but also poses a challenge to law enforcement agencies on how to investigate these complex and sophisticated crimes.

Digital forensic is a step – wise application of scientific methodologies or well – defined techniques to investigate crime(s) perpetuated with the aid of a digital devices or targeted at a digital device to retrieve evidence admissible at the court of law [1]. In digital forensic investigation, the sanctity and integrity of the evidence herein referred to as digital evidence is very paramount thereby driving home the need to give a critical attention to the process or procedure used in the acquisition of the evidence [8].

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 [2]. 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 [10]. The steps or phases that are common in all the process models are:

- **Collection:** Evidences can be collected in this phase
- **Examination:** Examination on the basis of origin.
- **Analysis:** The inspection of examination phase.
- **Reporting:** Conclusion of all the phases.

This paper begins with a review of some notable existing digital forensics investigative models, analyze those existing model to identify the strength and some weakness inherent in those investigative models, formulate a schematic framework to guide the selection of an investigative model.

2. Background

Different authors have proposed different models in the field of digital forensics in order to go through with the digital evidences. The work of different authors with respect to this field is given below:

2.1 Kruse and Heiser Model(Lucent)

This model was developed by Kruse et al (2001) and popularly christened the "3As". Thus, the model has three phases which are Acquisition, Authenticating and Analysis phases. Pivotal to this model is the need to ensure data integrity and validity, hence the following guidelines were enumerated;

- Acquire evidence without alteration or damage to the original evidence
- Authentication of the recovered evidence to ensure consistency with the data originally seized.
- Analyze the data without modification ensuring integrity

This model therefore calls for full and proper documentation of the investigation process as a way of attaining integrity of the data and also to correctly reverse the process in case of any eventually.

Advantages

1. It aims at retrieving data of evidential value whilst ensuring its integrity and validity
2. It is a simple model with few number of phases

Disadvantages

The phases within the model appear to be silence on the presentation and admissibility of the evidence in the court of law.

2.2 US National Institute of Justice model (NIJ)

Is a four step – wise model comprising of the collection, examination, analysis and reporting phases. The collection phase deals with the acquisition of diverse forms of evidence, the examination phase performs retrieval of digital evidence of probative value from the collected evidence. The interpretation of the results derived from the examination phase with the aid of appropriate techniques and methodologies is performed at the analysis phase[10]. The fourth and final stage include activities such as presentation of evidence, tools and procedures used as well as formulation of guidelines and recommendation for improvements if any.

Advantages

1. Inculcates a phase which deals with the presentation of results at the court of law
2. Phases analogous to the Kruse and Weiser model thereby reducing the level of difficulty in usage

Disadvantages

The model is not exhaustive with respect to other forms of digital technologies. Eg: Cyber computing, Internet of Things (IoTs), etc.

2.3 The Digital Forensic Research Workshop model (DFRWS)

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).

Advantages

1. It provides a standard and consistent forensic framework
2. Serve as a framework on which other forensic models are developed
3. Ease of use and easily comprehensible by both technical and non – technical users

Disadvantages

Due to its general nature, it becomes relatively difficult to test and implement. Moreover, it appears to be a bit rigid.

2.4 Abstract Digital Forensics Model (ADFM)

Reith, Carr and Gunsch (2002) examined a number of published models/framework for digital forensics [3]. 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: In this** phase where the type of incident is determined based on the indicators recognized from the incident.
- **Preparation: It** deals with tools and technique preparation, search warrants, and monitoring authorizations and management support to further investigation.
- **Approach Strategy: this phase starts** with the aim of maximizing the collection of untainted evidence while minimizing impact to the victim.
- **Preservation: it involves** activities such as isolation, securing and preserving the state of physical and digital evidence are undertaken.
- **Collection: in this** phase, the physical scene and duplicate digital evidence is recorded using standard and acceptable procedures.
- **Examination:** In – depth procedural search of evidence relating to the suspected crime is undertaken at this phase to prepare detailed documentation for analysis.
- **Analysis: this** determine significance, reconstruct fragments of data and draw conclusions based on evidence found and also to support a crime theory.
- **Presentation: F**indings are collated to provide explanation of conclusions which is mostly done in such a way that a layperson can comprehend.
- **Returning Evidence: E**nsure physical and digital property is returned to proper owner and determining what criminal evidence must be removed.

Advantages

1. Diverse methodology suitable for array of digital devices
2. This methodology can easily be appreciated by non – technical observers
3. Potential for incorporating non-digital, electronic technologies within the abstraction

Disadvantages

1. The generality of the model may pose some practical challenge.
2. There is no easy or obvious methodology for testing the model

2.5 Integrated Digital Investigation Process (IDIP)

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 [5]. The model known as the Integrated Digital Investigation Process was organized into five groups consisting of 17 phases organized into five (5) groups which are the readiness phase, deployment phase, physical crime scene investigation phase, digital crime scene investigation phase and the review phase.

Discussion

It is an out and out model which considers the dual investigative nature of the digital forensic investigation by including the digital and the physical crime scene investigation phases. The model envisaged that although the crime was perpetrated using a digital device as a means or target, the forensic investigation encompass both physical and digital crime scenes hence the need to include them in the investigations.

Replication in digital environment is relatively easier, making it easier to create a complete forensically sound image backup for analysis in the lab. Unlike many process models that focus primarily on the digital evidence, the interaction existing between the digital and physical environment is vividly highlighted in this model.

2.6 The Enhanced Digital Investigation Process Model (EDIP)

Baryamueeba and Tushaba (2004) suggested a modification to Carrier and Spafford's Integrated Digital Investigation Model (2003) [6]. 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. This model has five major phases namely, readiness, deployment, trace back, dynamite and review. The model starts with the readiness phase which deals with operations and infrastructure readiness, the needed human capacity is properly trained and equipped to deal with the situation. The **deployment** phase provides mechanism for the detection and confirmation of an incident. This phase has five sub – phases which includes detection and notification, physical crime scene, digital crime scene, confirmation and the submission sub – phases. The **traceback** phase tracks down the operations of the suspect's physical crime scene and has two sub – phases; digital crime scene investigation and authorization phase. Succeeding the traceback phase is the **Dynamite** phase which conducts investigation at the primary crime scene with the aim of collecting and analyzing items that were discovered at the scene to enhance the apprehension of potential culprits. The entire investigative process is reviewed and possible areas of improvement is identified in the **Review** phase.

Advantages

1. The model provides a wide spectrum to include electronic and non – digital technologies.
2. Create consistent and standardized framework for digital forensic development
3. This investigative model framework is suitably applicable to future digital technologies.

Disadvantages

1. Additional sub – phases introduces some ambiguity with respect to the activities performed.
2. There seems to be duplication of activities. E.g. Digital crime scene investigation activity appears under the Deployment phase, Traceback phase, as well as Dynamite phase.

2.7 The Systematic digital forensic investigation model (SRDFIM)

This model was developed with the aim of helping forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner [7]. 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.

In this 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 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:

The model identifies the need for interaction. Investigator should have consistent interaction with all resources for carrying out the investigation. Better case goal can be defined.

Another advantage of the model is exploratory testing.

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.

Disadvantages:

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.

3. Comparative Analysis

As previously been discussed that all the models have advantages as well as disadvantages, a omparative analysis of these models on the basis of their advantages, disadvantages and the steps that are involved in each and every model will be done.

4. Findings

Eight models for digital investigation are studied comparative analysis of these models is done on the basis of steps, advantages and disadvantages. The comparison (on the basis of steps involved) of Lucent model, NIJ model, DOJ model, DRFWS model, Abstract model, IDIP model, EIDIP model, and SRDFIM model is given in Table I:

TABLE I: COMPARATIVE ANALYSIS OF DIGITAL FORENSIC PROCESS MODELS (on the basis of steps invoved)

Steps	**Lucent**	**NIJ**	**DOJ**	**DRFWS**	**Abstract**	**IDIP**	**EIDIP**	**SRDFIM**
Collection	√	√	√	√	√	√	√	√
Examination	√	√	√	√	√			√
Analysis	√	√	√	√	√			√
Reporting		√	√					√
Preparation			√		√			√
Approach Strategy					√			
Preservation				√	√	√	√	√
Presentation				√	√	√	√	√
Identification				√	√			√
Return Evidence					√			
Decision				√				
Review						√	√	√
Reconstruction						√	√	
Documentation						√	√	√
Authorization						√	√	√
Survey						√	√	
Trace Back							√	
Dynamite							√	
Communication								√
ExploratoryTesting								√

- On the basis of steps or phases involved in these process models it can be concluded that SRDFIM model is the best suitable amongst all of the other models because of the following reasons:

- SRDFIM model provide complete and concrete steps in order to perform digital investigation.

- NIJ model and DOJ model have very limited steps; therefore they are not appropriate in order to perform digital investigation thoroughly. The analysis phase of NIJ is improperly define and ambiguous.

- Communication shielding is the step which is very important in order to secure the evidence from unauthorized access by blocking all the devices such as WIFI, USB, cables etc after the digital crime has happened. And only SRDFIM model is the only model that is providing that step among all these process models.

- Though IDIP model has seventeen and EIDIP model has nineteen steps but there are repetitions of steps in these process models that will make these models extensive and time consuming with respect to the investigation. They both focus on physical as well as digital investigation and physical investigation is not a concern of this research.

- In abstract model the third phase (Approach strategy) is the duplication of its second phase (Preparation).

On the basis of advantages and disadvantages some of the characteristics of these process models have also been mapped. The comparison is given in the form of table.

TABLE II: COMPARATIVE ANALYSIS OF FORENSIC MODELS (With Respect to Attributes)

Attributes	Lucent	NIJ	DOJ	DRFWS	Abstract	IDIP	EIDIP	SRDFIM
Iterative model							√	√
Linear model		√	√	√	√	√		
Exploratory model								√
Chain of Custody				√		√	√	√
Applicable for law enforcement		√	√	√	√	√	√	√
Applicable for corporate sector						√	√	√

On the basis of these attributes it has been observed that SRDFIM is the most suitable model for digital investigation becauseThis is the only model that is providing exploratory testing which means that the researchers have their own methods for testing.

SRDFIM is the iterative model and divided the investigation into four tiers. EIDIP is also an iterative process but it has not divided the investigation into different tiers.

Allocable for both law enforcement as well as the corporate sector where as the models i.e; NIJ, DOJ, DFRWS and abstract models are only applicable for the law enforcement.

5. Conclusion

Different forensics investigation models are developed to provide accurate and authenticated digital evidence which is admissible in court of law. However, all these models have some advantages and disadvantages. This paper reviewed some common forensics investigation models, enumerated their advantages and disadvantages and make a comparative analysis of these models to guide the investigators in choosing the appropriate model(s) which will yield maximum result with respect to the case under investigation.

6. References

7. 1] Shrivastava, G., Sharma, K. and Dwivedi, A., "Forensic computing models: technical overview," in *Proc. ISI Thompson Conference*, 2012.

[2] Ademu, I., Imafidon, C. and Preston, D., "A new approach of digital forensic model for digital forensic investigation," *International Journal of Advanced Computer Science and Applications,* vol. 2, no. 12, 2011.

[3] Reith, M., Carr, C. and Gunsch, G., "An examination of digital forensic models," *International Journal of Digital Evidence,* vol. 1, issue 3, 2002.

[4] Ciardhuáin, S., "An extended model of cybercrime investigations," *International Journal of Digital Evidence*, vol. 3, issue 1, 2004.

[5] Spafford, B., "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, issue 2, 2003.

[6]Baryamureeba, V., and Tushabe, F., "The enhanced digital investigation process model," May 27, 2004.

[7] Agarwal, A., Gupta, M., Gupta, S., and Gupta, S., "Systematic digital forensic investigation model," 2011.

[8] Fedaghi, S., and Babtain, B., "Modeling the forensics process," *International Journal of Security and Its Applications*, vol. 6, no. 4,
October 2012.

[9] Phillip, D. and Bradford, G., "Models of models: digital forensics and domain-specific languages," June 10, 2009.

[10] Beeba N. and Clark, J., "A hierarchical, objectives-based framework for the digital investigations process," in *Proc. Digital Forensics Research Workshop,* Baltimore, Maryland, August 2004.