Comparative Analysis of Digital Forensic Models

Fakeeha Jafari and Rabail Shafique Satti

***Abstract*—Digital forensic is the study of scientifically proven methods that results in the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence [1]. Just like computer forensics, digital forensic is also a very wide branch. Different tools, techniques, frameworks and models have been presented to study the basics of digital forensics. The focus of this research is to study different models and the steps that have been proposed by the authors in order to implement these models, the steps that are involved in the investigation process and finally make a comparative study that which of the model is the best among them.**

***Index Terms*—Abstract model, DFRWS, EIPID, IPID, NOJ.**

I. Introduction

In this world of technology, as the number of people is growing, the numbers of digital devices such as computers are also growing rapidly. These computers are interconnected with each other in the form of networks and exchanging huge amount of data. These computers are responsible for cyber fraud and cyber crime. Digital forensic is the technique that is responsible for reconstruction of the crime digitally after being happened. In the field of forensics, there exist different techniques and models for investigation purpose.

It has been observed that in order to implement the digital forensic process, different models have been proposed that include different phases for the investigation purpose. The focus of most of the digital forensic investigation process models is to provide an effective investigation process and the steps that will provide a concrete principle of investigation. Each and every model contains pros and cons and also each of the models has some similarities as well as differences with each other.

In this modern era it is really very important to understand the concept of "Digital Forensic Investigation Model". Currently this area is considered as a good area in the academic research, which provides different techniques and procedures to promote this field. Reconstructing the evidences from the source is the major definition of digital forensics. Digital forensic models proposed step wise procedures or ordered procedure in order to go through with the digital evidences. These models can provide a thorough investigation process in order to provide admissible evidence in court [1]. 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.

Manuscript received October 19, 2014; revised December 20, 2014.

Fakeeha Jafari is with the Department of Computer Sciences, Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan (e-mail:fakeehajafari@gmail.com).

Rabail Shafique Satti is with the Department of Software Engineering, Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan (e-mail:emailrabail@gmail.com).

II. 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:

A research paper entitled "*A New Approach of Digital Forensic Model for Digital Forensic Investigation*" [2] was published. The focus of this research was to propose a structured as well as consistent approach for digital forensic investigation. In order to improve the investigation process, a new model has been proposed that aims at identifying the activities and helps improve the investigation process. The authors have also discussed the existing models proposed by different authors like: The SDFIM model, IDIP model, The Forensic Process Model etc. Different models have different phases in order to perform digital investigation and keeping in mind about these models, a new model has been proposed. According to this proposed model, the authors have divided the investigation process into four tiers based on the phases. The first tier consists of four phases i.e. preparation, identification, authorization and communication. The second tier consists of three phases which includes: collection, preservation and documentation. The third tier also consists of three phases such as examination, exploratory testing and analysis and finally the fourth tier consisting of presentation phase.

The authors proposed a paper entitled "*An Examination of Digital Forensic Models*" [3]. The focus of this paper was to develop a process of digital forensics. The authors have proposed an abstract model after comparing different forensic methodologies. The new model also discussed the shortcomings of the existing models. Basically the proposed model is the enhancement of the DFRW. The phases included in DFRW are: identification, Preparation, Approach strategy, preservation, collection, examination, analysis, presentation and returning evidence. The above given phases are not like other traditional methods to collect the investigation. One of the major characteristics of this model is that it is applicable for the devices of past present and future. The model provides the basis for analyzing new digital/electronic technology as well as provides law enforcement framework applicable in the court of law.

A research paper was published entitled "*An Extended Model of Cybercrime Investigations*" [4]. According to this paper a cybercrime investigation model was proposed in

DOI: 10.7763/JACN.2015.V3.146

order to provide real time investigation. Existing models were studied in this research. We can say that the proposed model is the extended study of the existing models by addressing some of the activities that are absent in these existing models. Unlike other models, this model represents the flow of information in the investigation. Information flow means the flow of investigation. Step by step activities have been done in order to go for investigation. This model provided an educational tool and the work would be explained to the non specialists by the investigators. The major application of this model is to maintain the information flow of the investigation between the overlapping investigations. Some of the steps were the same as the other process models like identification, collection and presentation. Some of the other phases were authorization, notification, hypothesis etc. Therefore the flow information proves this model more comprehensive than the other previous models.

A paper has been published entitled "*Getting Physical with the Digital Investigation Process*" [5]. A model has been proposed that is applicable to the corporate sector as well as to the law enforcement. The proposed model basically integrates the physical crime scene with the digital crime scene investigation in order to identify the person who is responsible for the digital crime. If talk about the law enforcement model, it provides electronic crime scene investigation. The phases included in this model includes: preparation, collection, examination, analysis and reporting. The abstract model has been proposed for the corporate sector based on the traits that are common in most of the models. The phases that are included in this phase are: identification, preparation, approach strategy, preservation, collection, analysis, presentation, and return evidence. The proposed model uses most of the same phases as described earlier, it uses the theory that computer itself is a crime scene whereas apply the digital crime scene investigation techniques. The author divided the process into five groups that containing seventeen phases given below: Readiness Phases, Deployment Phases, Physical Crime Scene Investigation Phases, Digital Crime Scene Investigation Phases and Review Phase. Therefore the focus of the research is to treat computer as a crime scene just like a body and undergo the same procedure and investigation that would be carried out for a body. And each phase required the technical requirements for interaction between the physical and digital investigation identification.

Two authors proposed a paper about the digital forensic model entitled "*The Enhanced Digital Investigation Process Model*" [6]. In this paper the overview of different models i.e. forensics process model, abstract digital forensics model and integrated digital investigation model (IDIP) have been discussed and on the basis of that a new model has been proposed based on IDIP. There are three major phases of IDIP i.e. readiness phase, deployment phase and review phase. The proposed model named enhanced integrated digital investigation model (EIDIP) has following phases: readiness phase, deployment phase, trace back phase dynamite phase and the review phase. The proposed model has extended the deployment phase of IDIP by introducing physical as well as digital crime investigation and adds a new phase of trace back. One of the features is to implement reconstruction phase at the end of all the investigation rather than two reconstructions.

The authors published a research paper entitled "*Systematic Digital Forensic Investigation Model*" [7]. Like other papers proposed by different authors, this paper also comprised of studying different models and proposed a new model based on the previous results. The paper proposed a comparison of different models and on basis of that proposed model, a systematic model of digital forensic procedure emerged. One of the major advantages of this proposed model is to provide a mechanism in which the frameworks can be implemented in the countries on the basis of technology. The model provides a systematic way to analyze the cyber fraud and cyber crimes according to the technology used in the respective country.

A paper entitled "*Modeling the Forensics Process*" [8] published**.** The authors proposed a model without comparing the previous or existing models. According to this paper a flow based model was proposed. This flow tells the exact and accurate direction in which the information or evidences were separated into different streams of flow. The proposed abstract model discusses the stages that would be helpful in separating the flow stream. The phases include: create, release, transfer, arrive, accept, and process.

A paper named "*Models of Models: Digital Forensics and Domain-Specific Languages*" [9] published. The focus of this research is that that the domain specific languages are very important part of digital investigation. The use of domain specific variables and the domain specific language helps a lot in the digital investigation process.

III. Comparative Analysis

As its previously been discussed that all the models have advantages as well as disadvantages, a comparative 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.

A. Model 1

The model was proposed by Ademu Inikpi O. *et al.* [2]. They basically studied different existing models like DFRWS, forensic process model, abstract digital forensic model, IDIP, Extended and enhanced model and SRDFIM etc and then proposed a new model. The advantages of this proposed model are:

- It provides a consistent framework in order to identify the research and development areas for digital investigation.
- Consistent means that the investigator will interact with the available resources.
- Testing is exploratory based. The testers have used their own methods of testing for the investigation purpose.
- The researchers interact with the tools optimally.

The disadvantages of the proposed model include:

- Generality of the model is not explicit.

B. Model 2

According to the model proposed by Reith Mark, Carr Clint and Gunsch Gregg [3], different existing models have been studied and a new model has been proposed. Basically

this model is the enhancement of DFRWS model. The advantages of this proposed model is (shown in Table I):

- For digital investigation provide consistent and standard approach.
- The methodologies are applicable for the future digital technologies.
- The model allows the non digital to incorporate in the existing technology.
- The judiciary can relate the technology to the non technical observers.
- Provide nonvolatile storage.

The disadvantages are:

- It is not the obvious model for testing.
- One of the major disadvantages is that the model does not touch the chain of custody.
- The categories are not for the practical use.

TABLE I: ACTIVITIES INVOLVED IN PROPOSED MODEL AND DRFWS MODEL [3]

Activities in proposed model	*DRFWS model*
Identification	
Preparation	×[1]
Approach Strategy	
Preservation	×
Collection	×
Examination	×
Analysis	×
Presentation	×
Returning Evidence	×

C. Model 3

TABLE II: COMPARISON OF PROPOSED MODEL WITH DIFFERENT FORENSIC MODELS [4]

Activity in new model	***MODEL***			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				✓
Authorisation				
Planning				✓
Notification				
Search/Identification	✓	✓	✓	✓
Collection	✓	✓	✓	✓
Transport				
Storage				
Examination	✓	✓	✓	✓
Hypothesis	✓		✓	✓
Presentation	✓		✓	✓
Proof/Defence			✓	
Dissemination				

The merits and demerits of the model were proposed by Ciardhu án S éamus Ó. [4], after comparing it with the existing models. The demerits are:

- Step by step activities can be recorded in the form of chain of custody but this can only be applicable if the information about the legal investigators is known.
- Experienced staff is required for the investigation.

The merits are:

- Provide consistent as well as structural framework.
- The flow of information in the investigation process is explicit.
- Tools can be used for the examination of evidences.
- Exploratory research
- Due to the exploratory research, the participants have knowledge of the subject.

A comparison of the proposed model with the existing models is based on the activities (shown in Table II).

D. Model 4

Carrier Brian and Spafford Eugene H. [5] proposed a model based on the previous work done by different authors. The advantages are given below (shown in Table III):

- The model is applicable for both law enforcement and for corporate sector.
- The proposed model is the integration of the law enforcement process model and the abstract process model.
- Gives accurate results for digital investigation process.
- Appropriate for collecting the evidence from the live computer.

Some of the disadvantages are given below:

- Adequate recourses are required in order to perform digital investigation.
- The difficulties faced by the digital investigators are the same as the physical investigators in terms of survey and research. For example, both of them have the difficulty in finding the small type of things like a hair on carpet or deleting the files from a 100 GB file system.

TABLE III: PHASES IN PROPOSED MODEL AND THE EXISTING MODELS [5]

PHASES			
New proposed model (IDIP)	*Incident response model*	*DOJ model*	*Abstract model*
Operation readiness	Pre incident preparation	Preparation	Identification
Infrastructure readiness	Detection of incident	Collection	Preparation
Detection and notification	Initial response	Examination	Approach strategy
Confirmation and authorization	Response strategy formulation	Analysis	Preservation
Preservation (physical[2])	Duplication	Reporting	Collection
Survey (physical)	Investigation		Examination
Documentation (physical)	Secure investigation		Analysis
Search and collection (physical)	Network monitoring		Presentation
Reconstruction (physical)	Recovery		Return evidence
Presentation (physical)	Reporting		
Preservation (digital[3])	Follow up		
Survey (digital)			
Documentation (digital)			
Search and collection (digital)			
Reconstruction (digital)			
Presentation (digital)			
Review			

[1] The cross symbol in the table shows the presence of that activity or phase

[2] Physical shows "physical investigation crime scene phases"

[3] digital shows "digital investigation crime scene phases"

E. Model 5

Baryamureeba Venansius and Tushabe Florence [6] proposed a model named EIDIP. The model is the integration of two model i.e. forensic process model and abstract process model. Basically it is the enhanced version of the IDIP. The extra phase that is included in the proposed model is the "trace back" phase which is not present in the previous models. The comparison of IDIP and EIDIP models are given Table IV:

TABLE IV: COMPARISON OF IPID MODEL AND EIPID MODEL

Phases in IDIP Model	***Phases in EIDIP Model***
Readiness Phase	×
Deployment phases	×
Physical crime scene investigation phases	×
Digital crime scene investigation phases	×
Trace back phases	
Dynamite phases	
Review phase	×

F. Model 6

Agarwal Ankit, Gupta Megha, Gupta Saurabh and Prof. Gupta [7] proposed a model by comparing it with the other existing models. Rather than telling the advantages and disadvantages, a comparison has been shown in the form of Table V about the phases of different models i.e.; (DRFWS model, abstract model and IDIP model).

TABLE V: COMPARISON OF EXISTING MODELS WITH PROPOSED MODEL [7]

Activity in new model	***DRFWS model***	***Abstract model***	***IDIP Model***
Preparation		×	×
Securing the scene	×		×
Survey and recognition	×	×	×
Document the scene			×
Communication shielding			
Evidence collection			
Volatile evidence collection	×	×	×
Non volatile evidence collection	×	×	×
Preservation	×	×	×
Examination	×	×	×
Analysis	×	×	×
Presentation	×	×	×
Result and review			×

G. Model 7

The model proposed by Ray Daniel A, Bradford Phillip G. [9] does not compare with any existing model. The model just tells the flow based methodology. According to this paper a flow based model has been proposed. This flow tells the exact and accurate direction in which the information or evidences are separated into different streams of flow. The phases of this abstract model are different from the previously discussed phases.

H. Findings

Almost ten process models for digital investigation in this research is read and out of these ten, seven process models are selected and comparative analysis of these models is done on the basis of steps, advantages and disadvantages. The comparison (on the basis of steps involved) of NIJ model, DOJ model, DRFWS model, IDIP model, EIDIP model, Abstract model and SRDFIM model is given in Table VI:

TABLE VI: COMPARATIVE ANALYSIS OF DIGITAL FORENSIC PROCESS MODELS

Steps	*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							×
Exploratory Testing							×

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 VII: COMPARATIVE ANALYSIS OF FORENSIC MODELS W.R.T DIFFERENT ATTRIBUTES

Attributes	*NIJ*	*DOJ*	*DRFWS*	*Abstract*	*IDIP*	*EIDIP*	*SRDFIM*
Iterative Model						×	×
Linear Model	×	×	×	×	×		
Exploratory Testing							×
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 because:

- This 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.

IV. CONCLUSION

For a digital evidence to be proved in the court it is necessary that evidence should be structured, consistent, complete and admissible. In order to prove evidence in the court the investigation should be thorough, complete and structured. The tools, techniques and models should be appropriate and up to date.

In this research different models have been studied regarding digital forensic investigation process and the conclusion can be drawn that SRDFIM model is the best suitable amongst all of the other models. Comparison have been done of all the models with each other on the basis of advantages, disadvantages and the steps, activities and phases involved in each of the model and conclusion can be drawn that SRDFIM model provide iterative approach, best suitable for future technologies in terms of digital investigation, provide exploratory testing and provide a structured framework for digital investigation [10].

REFERENCES

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

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

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

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

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

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

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

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

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

Fakeeha Jafari was born in Sialkot, Pakistan. She is a higher education scholar in the field of computer engineering. She received her bachelor's degree in the field of computer sciences in 2008 from Fatima Jinnah Women University Rawalpindi, Pakistan and further pursued her master's degree in the field of computer engineering from CASE (Center for Advanced Studies in Engineering) Islamabad, Pakistan, in 2014. She is currently employed at Fatima Jinnah Women University, Pakistan. Her areas of interest are computer networks, information security, cyber forensics, and digital image processing.

Rabail Shafique Satti was born in Rawalpindi, Pakistan. She is a higher education scholar in the field of computer engineering. She is a registered software engineer with Pakistan Engineering Council since 2007. She further pursued her MS degree in the field of computer engineering from the Center for Advanced Studies in Engineering (CASE), Islamabad, in 2014. She is currently employed at Fatima Jinnah Women University, Pakistan. Her areas of interest are computer networks, information security, cyber forensics, and data mining.