DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4218

Volume 8, No. 7, July – August 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A PROPOSED STRUCTURED DIGITAL INVESTIGATION AND DOCUMENTATION MODEL (DIDM)

Arfiya S Siddique, M AfsharAlam, Osama Chaudhary
Department of CSE
Jamia Hamdard,New Delhi, India

Abstract: Digital Forensic investigation is the step wise process based on scientifically proven methods. Many advancements are taking place in this area also in the past researchers have developed some working model of investigation. However, with change in technology the models are turning obsolete. In this research we defined digital forensics, nature of evidence. The features of exiting models have been summarized. A possible structured investigation model has been proposed with refinement at each stage. To support the findings sample checklist and forms has been drafted. The sample are adaptable and can be modified. The improvisation has been added upon the review by theprofessional cyber forensic investigator.

Keywords:Digital Forensics, Investigation, Models, Evidence, Checklist, Evidence Seizure Form, DIDM

1.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. [1]

According to a report by Digital Strategy Consulting, India, the main changes in internet access have happened in the last five years and the internet has become an essential part of office life, and plays a key role in many homes in India. The massive Indian market is changing fast. Internet access is mainstreaming among professionals and the use of mobile is intensifying. The pace of change continues to be rapid with digital channels constantly growing in volume and strength. [2] India is the third biggest country in terms of internet users in the world, with a highly social and mobile audience. It's estimated as many as 121 million Indians are logged onto the internet.

This research focuses on studying the different existing model and map out the consistent approach to digital forensic investigation which is effective and approachable. The research aims to design the possible format and bring about the changes in existing forms. We have also mentioned the cost associated with latest cyber breach over the past two years. The highlight of the research is the proposed model, The Digital Investigation and Documentation Model(DIDM).

2.LITERATURE REVIEW

Evidence Investigation guide, clearly states that digital forensic is the utilization of scientifically proven method in order to carry out investigation at electronic crime scene.

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. A lot has been adopted from physical forensics into digital forensics, specific software has been created to carry out investigation result and inclusive knowledge is received by digital forensic specialist to fight digital crimes. [3][4]

2.1 Digital Evidence

Digital evidence is the information and data which is of value in and investigation involving digital devices which needs to be preserved. This evidence is procured when information or electronic gadgets are seized and secured for examination.

An evidence can be secured from any criminal act related to the use of digital devices any crime scene including destruction of intellectual property, scam or even kidnapping. Any data which provide information about the crime scene and can provide significant link is an evidence and if the information is procured from an electronic source it's a digital evidence. [6]

2.2 Digital evidence

Digital evidence is fragile in nature. Information contained in it can be easily modified, destroyed or may get damaged. Care should be taken while dealing digital evidence.

It can be easily copied, altered so after securing evidence. Evidence needs to stored cautiously.

Digital evidence can be compared to Deoxyribonucleic Acid(DNA) or finger print evidence as information could be stored anywhere in that piece of device. You cannot predict the content from physical appearance. [3][4]

2.3 The DFRWS MODEL

The Digital Forensic Research Workshops was held to provide a forum for newly formed community of academics and practitioners to share their knowledge of forensic. The DFRW model agreed for the following processes such as identification, preservation, collection, examination, analysis, presentation and decision, but the DFRWS model was just a basis for future work. [5]

2.3The Forensic Process Model

According to the very first edition of Evidence Investigation guide 2001 by National institute of Justice. The forensic process consists of four phases collection, examination, analysis and reporting. The ***collection*** phase involves exploring, recognizing, collecting and documenting of electronic evidence. The ***Examination*** process is to make evidence visible and analysis of origin and importance of evidence. It includes deep study of evidence and extracting hidden information out of it. The ***analysis*** phase is the study of result of examination and taking out the important out of it. The ***reporting*** is writing the findings and framing the examination process in the best way possible so that it clearly states the analysis. [6]

2.4 Abstract Digital Forensic Model

In our research we have found that,Abstract Digital Forensic Model is most talk about model, many authors have drawn comparison based on Abstract Model. Fakeeha and Rabail(2015) mentioned that this model is the enhancement of DFRWS.[7][8] They clearly mentioned that the advantage of this model are

- It provides consistent and standard approach for digital investigation
- It provides with the methodologies which can are applicable for the future digital technology
- Its allows the non-digital simplicity to work in existing technology
- It also provides nonvolatile storage
- The major disadvantage of this model is that it does not say anything about chain of custody
- The categories are not of practical use

2.5 The Integrated Digital Investigation Model

Carrier and Spafford proposed a model, which they consider as the improvisor of previous work process. The model was organized into five groups consisting of 17 phases. In this model, physical investigation is modelled into digital investigation.

2.6 Enhanced Digital Investigation Process MODEL

Baryamueeba and Tushaba come up with the modification in the previous model IDIP. integrated digital investigation model was made the basis for this new design. Tw new phases in addition to the existing IDIP model were introduced; trace back phase and dynamite phase. The objective of these phase was to introduce reconstruction of the crime scene at the end investigation at every stage. Trace back was the main key feature of this model. Basically, EIDIP flows in the manner, readiness phase being the first similar to IDIP, deployment phase then comes the trace back phase instead of review phase, after the trace back phase comes the dynamite phase, and lastly the review phase. [9]

2.7 The Systematic Digital Forensic Investigation Model Srdfim

According to this model developed by keeping in view the past models. Like the previous work done by the other authors this model is also based on the study of other models. The model focuses on the investigation cases of computer forensic and cybercrime. The application model focuses on the investigation cases of computer frauds of eleven stages. The main focuses provide a mechanism in which framework could be implemented on the basis of technology. The model provides a systematic way to analyze the cyber fraud and cybercrime according to the technology used in that country.

3. COST ASSOCIATED WITH LATEST DIGITAL CRIME

According to the research released by IBM and Ponemon in the year 2015 in which 350 companies majorly from the USA, Germany, India, Italy, Canada, Brazil, the UK, France, Australia, United Arab and Saudi Arabia, Canada says that the average cost of the breach faced by these companies increased by 23% leading to the average loss of $3.79 million. Cost paid for stolen record and data which contains sensitive and confidential information increased by 6%, from $145 in 2014 to $154 in 2015 [10]. Another report by ITRC number of breaches in 2016 increased by 1,093, with total of 36,601,939 records compromised costing $7.01 million in average, according to new research from the Ponemon institute. The average mean cost of
most disruptive breaches till April 2017 in $1757.92.

4. PROPOSED MODEL

In our research, we analyze that often the investigation went wrong or is not conducted in proper manner. So here based on our findings we have propose a forensic investigation model which can further be improvised. We concluded that preparation is the most crucial step of investigation for a first responder so it needs to carry out at the very first step itself, then the verification or divination phase, then the seizure phase, next packaging and transportation, then investigation, followed by analysis and result and finally the documentation. The flow Chart of proposed model has been given below.

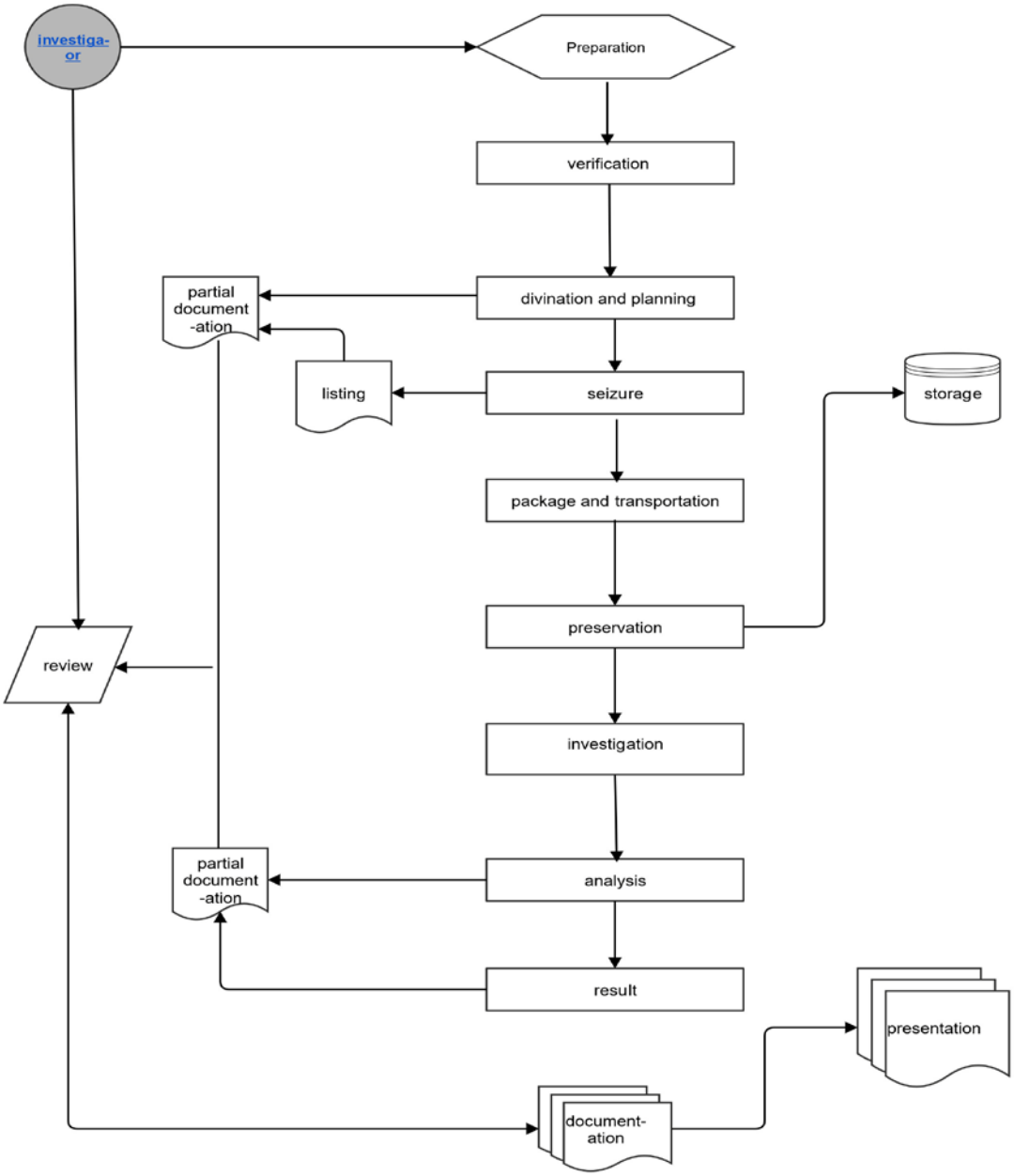

Figure 1 DIDM Model

5.THE DIGITAL INVESTIGATION AND DOCUMENTATION MODEL

The proposed model is based on the findings of research. Different stages of model have been defined and describe as per the model we have proposed. However, standard stages have the same meaning and procedure as mentioned in section 2, by the other authors. Our focus and modification have been defined in the following sections.

5.1 Guide for Stage 1: Preparation

Preparation phase in the key phase of proposed model. In the preparation phase the investigator needs to thoroughly revise the do's and don'ts, review the needful for investigation, review the toolkit, maintain the checklist before arriving at the crime scene.

5.1.2 Preliminaries

- ✓ Checklist the investigation tools. cardboard boxes, notepad, gloves, markers, evidence inventory logs, evidence tape, camera, non-magnetic tools.
- ✓ Verify search authority, consents and warrants warrant, ensure what level of analysis and what files you can examine (i.e., Does the warrant cover e-mail, unopened e-mail, etc. [11]
- ✓ Test the toolkits Encase, Celebrite (updates, latest version etc) for the proper functioning, create boot disk for forensics software.

Table 1 Preparation Checklist

Proposed Checklist

Items	Frequency	Description
Cardboard Boxes	**10*sample**	***checked etc.**
Evidence Tape		
Paper Evidence Bags		
Notepad		
Markers		
Evidence Inventory Logs		
Camera		
Non-Magnetic Tools		
Crime Scene Tape		
Antistatic Bags		
Faraday Bags		
Aluminum Foil		
Collection Tools		
Investigation Checklist		
Tools Tested		****updated as per 2017 version etc.**

5.2 Description of Stage 2: Verification

Verification here in this model is similar to identification and verification phase similar to that in other investigation models. Verification of the incident is important to carry out the investigation. It is important to first verify the incident and determine the scope and dimension of incident to understand the nature of case as it helps in next step. In order to formulate the planning verification is important.

5.3 Description of Stage 3: Planning and Divination

Planning start with the gathering of data after successful verification of the incident it is important to outline the investigation procedure to carry the investigation properly and to conclusively. Planning and Divination is to what kind of incident it is, whether you first need to carry out network analysis, system analysis or mobile analysis for the crucial evidence. The volatile evidence or the key evidences of the investigation. Now the noteworthy part of this model is the partial documentation. An investigator needs to document the initial planning strategy of the investigation which will reviewed by the investigator himself before the further stage.

5.3.1 Prepare the Plan

Plan out the necessary and place all the initial details in this. Formulate the keywords. Prepare an analysis worksheet. Record important information. Frame the possible suitable strategy according to the resources you have and knowledge of the investigation team. Keep the track of important step in later stages too.

5.4 Description of Stage 4: Seizure

Figure out the possible source of data, if volatile or non-volatile, maintain the integrity and ensure chain of custody. Collect the data which is even near to suspicious. The volatile data changes over the time. Maintain the order in which the data is to be collected. One of the suggested way/order in which volatile data needs to be acquired is network connections, ARP cache, login sessions, running processes, open files and the contents of RAM and other pertinent data – all this data needs to be collected using trusted binaries and not the ones from the impacted system. We have proposed a checklist for the investigator which would help during the seizure of evidence. This checklist would help the investigator to keep a check so that he does not miss out anything.

**Note: Possible evidence at the investigating crime scene is out of scope of this research however in this research we proposed to include the checklist at the seizure phase so the investigator does not miss out any important evidence. Sometimes seemingly insignificant data/source could provide great lead in the investigation.

Table 2 Chain of Custody Checklist

Proposed ChainOf Custody Checklist	
Date and time of Digital Evidence	
System Findings	
Network Connection Details	
ARP Cache	
Login session **Name** **Password** **Session duration** **Site** **Etc**	**Notes:**
Running Processes	
Open Files	
Ram Content **XYZ** **ABC**	**Notes:**
Pertinent Data	
Current date and time	
Note the time zone	
Significant problems/broken items	
Notes and Papers	
Others	

5.5 Description of Stage 5: Packaging and Description

Packaging of evidence is on the very same ground mentioned by National Institute of Justice in the Guide for The First Responder [3], all the actions related to the previous step including packaging must be documented. The investigator must ensure that the evidence is collected, labeled, packaged and transported properly. We analyze from the NIJ's guide for the first responder that digital evidence must be labelled properly. Labelling details should be mentioned in the final document.

So that the situation can be reframed easily. We have come up with the possible evidence description. In our research, we come across many evidence description form. However, Pete Williams Evidence Seizure Form is the basis of our proposed form [12]. We have analyzed that time zone and temperature could play a key role in later analysis of evidence. As some evidence may show variations in different time zone and at different temperature.

Table 3 Evidence Description Form

Proposed Evidence Description Form **Case No:**

Investigator's Detail

Name	
Email	
Phone	

Evidence Collection

Crime Scene Code:	**Collected By:**
Date:	**Time:** **Time Zone:** **Current Temperature: **at the time of arrival** **Seized Temperature: **at the time of Seizing the evidence**

Evidence Details

Evidence No	**Device**	**Manufacturer**	**Model Details**

5.6 Description of Stage 6: Preservation

The preservation of the collected digital artifacts is important so to maintain the integrity of the evidence as long as the case is closed. While preserving the artifacts care must be taken and so that the evidence may not get tempered or lost at any stage in further analysis. Often a time evidence needs to be reexamine if the court of law does not find the report produced by the investigator satisfactory. CDW-G's digital evidence management [13] mentioned that Files must be locked from read/write privileges, with the access privileges only given to the investigator or the examiner. Paper files must be stored in container locked and secure, providing access to the investigator or the analyst only. House the evidence system software on the internal network. It's important to ensure that the analyst follow up with the guidelines and maintains the confidentiality of the report and analysis themselves.

To avoid cross contamination, it has been found that in most equipped labs and stores one analyst computer per case is a ground rule. So, each time a clean OS and tools are loaded back onto the analyst computer at a fresh case analysis.

5.7 Overview of Stage 7: Investigation

The investigation phase is the important phase of whole procedure it is the examination of the evidence collected and seized. Carry out at the well-equipped Forensic labs by the trained professionals. Analysis phase is the establishing the findings of investigation and categorizing it under different forensics examination category listed by NIJ. Or it can be reevaluated after the findings.

5.8 Overview of Stage 8: Analysis

In our model, we propose the review of the findings of analyst by the investigator/the first responder. Its noteworthy here that the analyst need not to provide the extreme data of his findings to the investigator. The briefing could be cross examined.

5.9 Brief of Stage 9: Documentation Phase and Review Process

Documentation Phase plays very important role in the court of law. So, proper guidelines and instruction must be followed while documenting the investigation. We suggest that the language use should be easy to understand. In our model, we focus on the review process of the document. We proposed that thorough review of the document is important. The investigator and the analyst both must review the document before final presentation. Stage 10 i.e The Presentation phase is the final draft which should be acceptable at the court of law.

6. DISCUSSION

The proposed model and proposed checklist at different stages of models are based on the analysis of the research work mention in section and also on the past cybercrime and investigation procedure adopted by the investigators. Recent trends in cybercrime investigation bring us to this conclusion of introducing checklist and forms at various stages of investigation. For a Digital Investigation and Documentation Model (DIDM) proposed the validity comes from the evaluation of investigation officer who are continuously involved in the various forensic investigation. The model work flow and clear perspective of the DIDM comes from the flow chart for the 10 stages. We consider preparation as very crucial key step for the investigation. Documentation being the next important part with continuous review. The model has been reviewed by Cyber Forensic Investigator after his feedback and review necessary changes has been made to the model.

7. ADVANTAGES OF MODEL

Advantages of this model are that the review by the first responder the investigating officer will increase the transparency of the whole investigation phase. The investigators remark and review will enhance the documentation. Investigators review in a way is an authenticating factor of the investigation process in terms of the final result. As he may only conclude that the report has been drafted out of the evidence (unaltered evidence) seized at first from the crime scene.

8. DISADVANTAGES OF MODEL

The possible disadvantage of this model is that the updatable review could make the procedure consume more time. The partial documentation being the advantage of this model could would also made the documentation complex and time consuming. Next being the verification stage.

9. CONCLUSION

We have introduced the DIDM model it is digital forensic preparation model that can be implemented by the investigator. We deliberately highlighted the Preparation stage as the key process of investigation. We consider the fact that proper preparation by the investigator could bring a lot of betterment in the later stages of investigation. We have design a suitable checklist format which could ease down the preparation step. Next in the planning stage we have given importance to the partial documentation. As it lays the foundation of the investigation. Planning out the possible strategy could make the seizing process interesting and effective. We considered documentation of planning is important so it must be reviewed and further included in the final documentation. In the next step of seizure, seizing the evidence and listing them is the highlight of the model. Preservation stage is associated with the storage. Preservation has been discussed in the previous section of this paper.
The end is the documentation and presentation stage. Since the acceptance and final result of the case depends on the court of law. Document must be reviewed before the presentation. However, we conclude the fact that any model can quickly turn obsolete with the rapid change in the technology and even more quick advancement in the crime conduct.

10. ACKNOWLEDGMENT

We would also like to show our gratitude to ***Mr. Santosh Khadsare***, (Cyber Forensic Investigator, Ministry of Defence, Indian Army) for sharing his pearls of wisdom with us during the this research, and we thank him for his review and insights.

11. REFERENCES

[1] Inikpi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston, A New Approach of Digital Forensic Model for Digital Forensic Investigation, (JACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011
[2] A repot accessible at http://www.digitalstrategyconsulting.com/india
[3] U.S. Department of Justice Office of Justice Programs National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, pp. vii-ix, 2008
[4] Jia-Rong Sun, Mao-Lin Shih, Min-Shiang Hwang, A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure, International Journal of Network Security, Vol.17, No.5, PP.497-509, Sept. 2015
[5] VenansiusBaryamureeba, Florence Tushab, The Enhanced Digital Investigation Process Model, The Digital Forensic Research Conference DFRWS 2004 Available (online) https://dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf
[6] U.S. Department of Justice Office of Justice Programs National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, First Edition, 2001
[7] Sabah Al-Fedaghi and Bashayer Al-Babtain, Modeling the Forensics Process, International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012
[8] FakeehaJafari and RabailShafiqueSatti, Comparative Analysis of Digital Forensic Models, Journal of Advances in Computer Networks, Vol. 3, No. 1, March 2015
[9] Baryamureeba, V. Tushabe, F. (2004) The Enhanced digital investigation process (2004) Available (online): http://www.dfrws.org/2004/bios/day1/tushabeEIDIP.pdf
[10] Larry Ponemon, Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis' Available(online) https://securityintelligence.com/cost-of-a-data-breach-2015/
[11] Nathan Judish, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations pp.15-18,2008
[12] Available(online) http://www.technoid.net/uni/fit/multi-form.pdf
[13] https://fedtechmagazine.com/sites/default/files/wp_digital_evidence.pdf Available(online) pp.5,6,
[14] Agarwal, M. Gupta, S. Gupta, and S. Gupta, "Systematic digital forensic investigation model," 2011

