ANALYSIS OF DEVELOPMENT PHASES IN DIGITAL FORENSICS MODEL

SNEHIL VIDWARSHI, NIDHI CHANDRA

M.tech (CS&E), Amity University, Noida, (U.P.)
Assistant Professor (CS & E), Amity University, Noida, (U.P.)
E-mail: snehil.cse@gmail.com, srivastava5@gmail.com

Abstract-The forensics behind computers often called as the digital forensic or computer forensics holds behind a vast network of investigation which includes various methods of investigation of the evidence found. This paper begins from the basic definition of what does computer forensics mean, why and for what purpose this particular field has been emerged and the facts and challenges being faced under this area. Digital forensics acts as a tool which can give a sequential chain of processes which leads to an efficient investigation method. In this paper, the present scenario of investigation methods are presented and discussed in detail. Digital forensics deals with the different types of crimes that can be performed using computers. So, at various stages changes are required in the models made for the investigation purposes.

Keywords-Digital Forensic Investigation, Investigation Model, Crime Scene Detection, Evidence Analysis.

I. INTRODUCTION

The usage of computer technology is becoming mandatory in almost every sector be it technology, education health, finance, etc. Computers not only provide us with accurate data but can also be exploited very easily and gives efficient result. On one hand it serves as the basic requirement and helps in complex functionalities, but on the other hand the crimes are increasing in parallel. Many a times obtaining the root cause of crime becomes a complicating task. Due to this accelerated rate in computer enormity, a proper mechanism under law was needed urgently to handle such mishaps. Computer Forensics thus treated as an arena which has established itself as a responsive factor to crimes conducted by computers. It can be noted that a computer system can be treated as a target, it means that the harm is to be done to that particular computer system or as a weapon to perform the crime i.e. through computer the harm or attack is planned. Digital Forensics, a branch under computer forensics is more specific field. Here, the mechanism for carrying out the investigation is professional. The bodies who are involved in enforcement of laws; the administrative department of networks and even the private investigators nowadays rely on the professional functioning of forensic examination techniques because of being more accurate. The digital forensic investigation is generally carried out as a method of extraction from the hard disk or other available storage site. A retrieval mechanism is employed. Many types of models came into existence and some are in use under the computer forensics field. The paper discuss about the preliminary models first arose and then how the further development took place. The model in present use have both its advantages and disadvantages which will also be discussed in this paper under literature review section. Computer forensics deal with a number of models starting from the very basics to the complex ones. The models takes into consideration are Lee et al, Casey (2004), Carrier and Spafford, Baryamureeba, Ciardhua in (2004), Cohen (2009), Kruse & Heiser, Reith, Carr & Gunch model, DFRWS. The arena of digital forensic is vast, at the same time a huge number of criminal acts are also possible. Digital forensics has been created in such a way which enables any corporate or authorised agency to carry out the investigation process. Digital forensics also known as computer forensics is moreover a scientifically method which deals with proper procedures which comprise of obtaining the evidence when any crime is reported then comes the preserving phase and then documentation is being made.

A most basic formulation of digital forensics is

When a crime has taken place, for the more step is to locate the scene and obtain the evidences as much as possible. In general crime scene the worth common example is to obtain the fingerprint of the culprit but at the same time it is possible that knowingly or unknowingly the evidence has been erased. So, there is an urgent need for preserving the evidence once it is obtained. At this scenario there comes the need for preserving and securing the evidence which is/are fragile in nature. Loss of any small/big evidence may restrict the process of investigation. In case of computer world, it is bit
difficult and sensitive method to look after the evidence making sure the integrity is being maintained. Also, in networks, hard findings are difficult to obtain as crime has been planned though computers. An organised methodology is in demand which enables the digital forensic investigation to act more professionally. Hacking and other malicious activities become easy when a person knows the technical knowhow of computer network system. In count of law digital or electronic evidence do have significant importance only gathering them is not an easier task thus the digital forensics come into action. Computer forensics has got both pros & cons. Due to drastic demand of this technology a huge amount of data is available over internet which is both beneficial and threaten. Frauds in corporate world, intellectual property, breaching of contracts, recovery of asset are some among the areas where proper forensic investigation will prove helpful. The analyst under forensic dept. works in way so that the evidences gathered are in a format which is admirable in court.

### Table I. Shows a list of complete digital forensic investigation model.

<table>
<thead>
<tr>
<th>MODEL NAME</th>
<th>INVENTERS</th>
<th>YEARS</th>
<th>NUMBER OF STAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Forensic Process</td>
<td>M. Pollitt</td>
<td>1995</td>
<td>4 stages</td>
</tr>
<tr>
<td>Generic Investigation Process</td>
<td>Palmer</td>
<td>2001</td>
<td>7 stages</td>
</tr>
<tr>
<td>Abstract model of the Digital forensic Procedures</td>
<td>Reith, Carr, and Gunsh</td>
<td>2002</td>
<td>9 stages</td>
</tr>
<tr>
<td>An Integrated Digital Investigation Process</td>
<td>Carrier and Spafford</td>
<td>2003</td>
<td>17 stages</td>
</tr>
<tr>
<td>End to End Digital Investigation</td>
<td>Stephenson</td>
<td>2003</td>
<td>9 Stages</td>
</tr>
<tr>
<td>Enhance Integrated Digital Investigation Process</td>
<td>Baryamureeba and Tushabe</td>
<td>2004</td>
<td>21 stages</td>
</tr>
<tr>
<td>Extended Model of Cybercrime Investigation</td>
<td>Clardhuain</td>
<td>2004</td>
<td>13 Stages</td>
</tr>
<tr>
<td>Hierarchical, Objective Based Framework</td>
<td>Beebe and Clark</td>
<td>2004</td>
<td>6 Stages</td>
</tr>
<tr>
<td>Event Based Digital forensic Investigation</td>
<td>Carrier and Spafford</td>
<td>2004</td>
<td>16 Stages</td>
</tr>
<tr>
<td>Forensic process</td>
<td>Kent K, Chevalier, Grance and Dang</td>
<td>2006</td>
<td>4 Stages</td>
</tr>
<tr>
<td>Investigation Framework</td>
<td>Kohn, Eloff and Oliver</td>
<td>2006</td>
<td>3 Stages</td>
</tr>
<tr>
<td>Computer Forensic Field Triage Process Model</td>
<td>K. Roger, Goldman, Mislam, Wedge and Debotta</td>
<td>2006</td>
<td>4 Stages</td>
</tr>
<tr>
<td>Investigation Process Model</td>
<td>Freiling and Schwittay</td>
<td>2007</td>
<td>4 Stages</td>
</tr>
</tbody>
</table>

## II. ADVANTAGES AND DISADVANTAGES

Computer forensic provides an ease of searching and analysing huge amount of data in very short span of time. Data which are lost or deleted while committing crime or done intentionally to secure culprit can be retrieved through forensic tool. Searching keywords in various languages from hard storages at an efficient rate is possible as crime has no particular language to deal with retrieval of lost data becomes substantial evidence in law session. Thus linking the missing chain of evidence and reshaping the crime scene, admissibility of vidence without any modification is critical and sometimes gives a setback when evidence is no more in original format. Another disadvantage of digital forensic is the high cost of data retrieving. Being fairly new not everyone understands the concept of forensic process, thus integrity and confidentiality must be highly maintained. It should also be noted that evidence can be captured once due to high use of network thus demand high security.

## III. LITERATURE SURVEY

The process of forensic investigations seems easy having there to four basic steps. But in detail, every step comprise of subparts. More professionally computer forensics deals with two major area- the first one being the monitoring task of network traffic which is a continuous task & look after any suspicious activity and the other area deals with
enforcement of law where the captured data (if obtained & from the network traffic) is analysed in order to produce digital evidence for usage in legal procedures. A team of forensic analyst is at first set up to carry out the investigation, capturing information can be any of the networks; Public or private. Constructing the path from the data captured can lead to know the root of any such attack.

A set of sequential steps from the beginnings of the investigation process are as follows:

1. Evidence trap
2. Authenticity check
3. Analyse & Study
4. Presentation in law in digital form

When the team is setup, the analyst follows the previously mentioned steps. The first frame the evidence which can be obtained through tracking network or log files. The availability should be in digital form once the acquiring phase is over, the authenticity is checked so that it becomes assured that the evidence is related to any crime. Then comes the analysis phase which reveals some other important aspects of evidence and then a proper documentation is prepared to present in the court of law.

A. Techniques and Tool Requirements

Some issues need to be thoroughly understood while preparing for the forensic investigation process.

1. Workstation setup: A team of well knowledgeable analyst.
2. Software required in digital forensics.
3. Hardware tools required.
4. Warrants criteria and terms.

Types of investigation:

1. Public investigation
2. Private investigation

A digital forensic investigation demands equipped team of analyst with proper availability of software and hardware needs. Since, the crime is planned through computer, no hard proof is available. Only digital media can be obtained and it should be maintained in a way that will get acceptance in court. As mentioned, a team of analyst is prepared and a workstation is setup where the investigation process will be carried out. A lot number of crimes like malicious activity, Dos attack, Data intrusion, malware and other cyber. Crime need to be investigated which ask for various types of software and hardware tools. Thus for an efficient investigation the workstation must have all these availabilities. Types of investigation is another important aspect that should be cleared to the analyst. Though not much but there are some change in the procedure of public and private investigation.

B. Existing Investigation Model - An Overview

All the models has background functioning into three vital stages - Complaint, Investigation and prosecution. A number of models exist in this field having its pros and cons and many have proposed other models overcoming some of the loopholes of existing model.

1) Kruse & Heisn (2001)

Model was developed in order to solve the cases of crime. The three fundamental step of three A's i.e., Acquiring, Authenticating and analysing the suspicious data (evidence) found. But the model restricts to the preliminary stages only and does not provide detailed study of the evidence found.

2) The Scientific Crime Scene Investigation Model

In the same year (2001), Lee et.al proposed a four phased model having recognition step then comes identification, individualization and reconstruction [11]. This approach is more systemic for detecting crime scenes. The only restriction to this model is that it is confined to analysis part only but does not tell about the other functions like acquiring data, preparing the missing links or presentation in digital form to the court of law. The model in graphical format can be represented as follows

![Lee Model](image)

Fig. 3. Lee Model Where we can study the phases in detail in this sequence.

a. Recognition Phase

This stage observes the traffic over network for any susceptible packet which may have some link to any crime and can be treated as a potential evidence. Once such packets are collected, the preservation (sub step) is followed to avoid any modification in the evidence.

b. Identification phase

Shows how the evidence is related i.e. biological, chemical, physical component and then comparison takes place.
c. Individualization
As the name suggests, tries to build a link between the individual or any group or case to that of the evidence found.

d. Reconstruction
In this procedure of analysing the collected fact and figures (evidence) and try to link up with other available events in a manner to create the possible scene that could happen. Though the model has appropriate phases to deal with the investigation process, it has been criticized because it deals only with the physical aspect of crime investigation but does not hold the overall processing of digital forensic investigation.

3) Casey Model
Casey gives another forensic model which has the scope to work in more than one investigation environment including individual computer systems and networked systems as well. The model can be seen in this following figure.

![Casey Model](Image)

This model is somewhat similar to the previously mentioned Lee model. Although the models differ in the term of examining digital evidence which was restricted to only non-digital data types. The two steps i.e. recognition and the last one of reconstructing evidence are same as that of Lee model. Here two phases are different namely preservation followed by classification. The preservation stage is further sub divided into two basic task; the first one is the collection which ask for proper documentation which will help in maintaining the integrity of the evidence. Classification is related to individualize or relate the evidence to any particular event beneficial to the crime case. The other phases are carried out in the same manner as in Lee model. An extension of Casey model had also come up with more stages like assessment, identification and seizure, recovering, harvesting.

4) Carrier and Spafford
The model proposed by Carrier and Spafford includes five stages and then each stage is further detailed in sub stages giving it a lengthy view but has significance of each step. The logical representation in a linear sequential way distinguishes it from the previously described two digital forensic investigation model. They named the model as an integrated digital forensic model.

![Carrier and Spafford Model](Image)

Since every coming model is a step better than the previous one or have tried for a betterment in its approach giving new sub processes, we have not elaborated the same steps every time in each model as the basic steps are the same and can be seen from previous discussion. The steps which are new are discussed here. The step readiness tells about the requirement analysis in terms of building the workstation, any operational need or could be any operational form. Deployment stage conveys the notifying process once the detection of evidence is done. Authorizing the evidence that it belongs to the crime event part is necessary because one cannot pick up any data or packet over network and show it as an evidence to produce in court. Proper analysis is required. Only after confirmation of authenticity the further steps are initiated. It should be noted that the two phases namely physical investigation and the digital investigation take place in parallel. A number of issues are considered in the model processing. Acquisition of data extracting data detail, normalizing facts and figures, analysing, and presentation are some of the issues to which the model look after during the investigation process. This model do provide method for performing the digital investigation which is indeed a significant contribution but the results can be seen through practical implementation only. This model has logical implementation and run two processes simultaneously. There is no particular problem with this model but it gives scope to further optimizing the investigation procedure with a lesser number of steps.

5) Baryamureeba
As discussed in the previous section, this model of Baryamureeba can be considered as an elongation to the Carrier and Spafford model. Baryamureeba named it as Enhanced version of forensic model. He called it as Enhanced Integrated Digital Investigation Process (EIDIP).
The model can be depicted as follows.

![Diagram of the Baryamureeba Model](image)

The EIDIP model has five basic stages as shown in the above cyclic figure. These are readiness, deployment, trace back, dynamite and review phase. The first two phases i.e. readiness and deployment phase are same as of previous models. Here, a new term Trace back is introduced. Trace back phase tries to break down the phase so that the sequence of events can be tracked in order to find the devices deployed to commit the crime. A reconstruction is done to find the relevant details for this the host computer where the evidence was found taken into consideration. A number of hardware and software are needed and a virtualized environment is set up to carry out investigation process. While collecting the evidence a prominent phase arises that is safeguarding the evidence so that no modification can occur. For this, preservation phase come up into action which uses the method of duplicating the data so that if one data gets altered another set of evidence remain safe.

Dynamite phase is about looking after the preliminary scenic conditions. Evidences are collected and analysed and a hypothesis is then build by studying evidences at various points that what could have actually happened. This model of Baryamureeba is an extended task of Carrier model which was earlier proposed as a waterfall model and also allowed back tracking but did not implemented. This model of Baryamureeba does include this phase of back track so that moving back to previous phases would be possible for making any changes or only for a review purpose.

6) Ciardhuain DFPM
He proposed a DFPM model which is more compact and comprehensive in nature. It includes all the relevant phases of previously mentioned models. He called the phases as activities. The model is a linear representation and enable a proper flow of processing. The model being comprehensive avoid repetition of steps many times but allows where ever needed, which in turn helps in betterment of efficiency. The activities involved in the model can be seen as the stages of a water fall model, this is because activities are followed in a systematic manner. The model can be represented as give below.

![Diagram of the Ciardhuain DFPM Model](image)

The initial step is the awareness activity which makes investigator aware of some mishaps and that needs to be investigated. Before starting investigating it is mandatory to report the crime to authorized authority which is can grant permission to carry out investigation. Authorization can be taken by any internal body or it can be external also depending upon the type of crime i.e. public or private. Plan phase requires knowledge from both the internal and external environment. Internal factors may include the policies, rules and regulation of any organization that need to be followed by the analyst. External factors are generally not in control of any investigator as they are mostly related to the legal section.

Notification activity is something that gives a sense of informing the bodies concerned that an investigation will be carried out over a crime or any subject. Search and notification activity tries to find out for more clues where the actual evidence was found. Collection tells about the seizure of evidence in the physical form. At this stage the evidence along with the system comes under surveillance of investigation and returned once the process is finished. It is not always safe to keep the evidence at the place where it is previously found so in order to provide more safety the evidence is transported under the transport phase to a safer place and then the investigation is carried out. Any type of mistake or negligence can corrupt the evidence found which will lead to failure in admissibility in court. So the throughout process of investigation on digital forensic is treated as very sensitive. Hypothesis phase
as the name suggests is an environment created by the analyst or investigator in order to link up the possible set of events that can complete the chain of incident that resulted into crime. There could be many hindrance while thinking for such sets of incidents as some internal or external factor may not support the incident because of unavailability of digital representation. So it is not that much easy task to think of any such set of incidents, careful measures need to be taken with proper convictions.

Presentation is the proper submission of evidence in the required format to legal officers or in court of law.

Proof of dissemination phase gives the analyst or the investigator a challenge to prove that the sequences he has created are correct and the crime has happened in that particular sequence. Dissemination is the final submission of the documented evidence in the court in digital format.

7) Cohen Model

This is another model for digital forensic investigation process which aims mainly on the digital evidence. The model comprise of seven distinct phases carried out in a sequential manner. The model can be represented as follows.

![Fig. 8. Cohen Model](image)

1. Analysis
2. Interpretation
3. Attribution
4. Reconstruction

The analysis phase tells about understanding of the crime and type of investigation that should be carried out. Beebe and Clark (2004) propose an iterative sub process listing as survey, extract and examine during analysis [11]. The next step is interpretation in which the results are visualised in a way that provide relevant legal solution. The attribution activity is the method of extracting or concluding the causes or phenomenon that leads to commit crimes. In reconstruction phase as we have seen earlier, the missing links are identified in a way so that a proper set of events are found and give proper results.

8) Digital Forensic Research Workshop (DFRWS)

This model has given a model which consists of following steps. The steps are somewhat similar to other models and included few new phases namely identical and decision stage [10]. This model is comprehensive by its features.

![Fig. 9. Digital Forensics Research Workshop Model](image)

CONCLUSION

Computer technology is a readily available thing and is found everywhere and for every small and big purpose. Making things easy, calculations, planning, security and other issues all are handled by this technology only. When it is this much easy to use then there is also a huge scope of using it for wrong purpose or to commit crime. Things become more complex when the evidence is not in physical form and need to be captured in digital form. To deal with such situations and to provide a high sense of security, Computer Forensics has come to existence. In particular, Digital Forensic deals with such particular crime investigation which requires evidence to be shown in court. This paper has discussed about the available digital forensic investigation model, their steps or phases along with the restricted areas. One cannot say that a particular model is best among all. Since the technology is advancing day by day so is the level of crime where the computer system can be exploited as a target or in most of the cases as a tool to harm or commit such kind of malicious activity. In the discussed models and the available models which are in use at present have some limitation and still need to be optimised at some or the other levels. It is not possible that a model is finalised to deal with all computer crime
investment because the analysis phase will vary from case to case. But an approach can be found out to minimise the risk of such crimes and maximise the efficiency without compromising the integrity of stakeholder or the evidence. The crime section is so vast that at any step a total new technology may be required to deal with it. Future work will be to study and analyse the proposed model with that of existing model and comparing the issues, advantages and loopholes and proposing a new model covering all investigating steps making it comprehensive and optimum.

REFERENCES


