ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

# Survey on Different Phases of Digital Forensics Investigation Models

Priya S. Patil[1], Prof. A. S. Kapse[2]

P. R. Patil College of Engineering and Technology, Amravati, India

**ABSTRACT:** Most forensics models focus on the investigative process and its different phases and are characterized by a rather informal and intuitive approach. When a formalized process been introduced, in 1984, a new and improved computer forensics investigation processes have been developed. A digital forensics investigation is a process that used science and technology to examine digital objects and tests theories, which can be entered into a court of law, to answer questions about events that occurred. There is various digital forensics investigation models which consist different phases. The interchanging one or any steps may lead the incomplete results hence wrong interpretation and conclusion. In this paper we reviewed a few investigation processes or models; discuss the phases and identifying common phases.

**KEYWORDS**: Digital Forensic process, Computer Forensic Models.

## I. Introduction

A digital forensic is an investigation process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. In 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence [1].The procedure adopted in performing the computer forensic investigation has a direct influence to the outcome of the investigation. Digital forensics is the use of scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources. [3]. The digital forensic process can be categorized into four different phases namely collection, examination, analysis and reporting [4, 5].When introduced the initial digital forensic model in 1984, after that too many models has been described efficient methods to investigate a digital crime Scene [1].Now a days when crime takes place in form of digital devices it has been very important to identified the crime and justified the crime [6]. Although authors has been proposed very effective model or a framework to identify the digital evidence or digital data.

Choosing the inappropriate investigative processes may lead to incomplete or missing evidence or data. Switching one step or bypassing any of the steps may lead to inconclusive results; therefore give rise to invalid conclusions. The evidences captured in an unstructured manner may risks of not being admissible in the court of law. It may be difficult or even confusing, to the junior forensic investigator to adopt the correct or appropriate investigation model.

The digital forensics investigations needed for examine digital objects and tests theories, which can be entered into a court of law, to answer questions about events that occurred. The digital forensics is used for identification, preservation, extraction and documentation of digital evidence. The digital forensic process used in Law enforcement, Military. The computer forensics is used to investigate a wide variety of criminal activity, including fraud, cyber stalking, murder, and child pornography. It providing the evidence capturing and reconstruction of process or providing the properties of reliability, authenticity and testability in indentify the computer crimes and fraud. It will serve a standard and reference for investigate the computer crime and fraud for computer forensic [6]. Not only a systematic way but also provides a complete solution for computer crime which is important need of the current changeable world.

## II. Related work

Computer and network forensics methodologies consist of three basic components that refers to as the three computer forensics investigations. These are: acquiring the evidence while ensuring that the integrity is preserved, authenticating the validity of the extracted data, which involves that it is as valid as the original and analyzing the data while keeping its integrity. Some process model that put the three factors into consideration includes the Forensics Process Model and the Abstract Digital Forensics Model and the Integrated Digital Investigation Model [1]. It is claimed that digital forensics is a process that can be modeled with some reasonably established phases. Most proposed forensic models have focused on “the investigative process and the different phases, they addressed the complexity of an investigation and the features and functionality of devices, and the concrete principles of an investigation” [11].

The methodology for dealing with digital evidence investigation so that the results be scientifically reliable and legally acceptable has proposed by pollitt [7]. It consist 4 distinct phases. In 2001, G. Palmer held the 1st Digital Forensics Research Workshop (DFRWS) and proposed a general purpose digital forensics investigation process [8]. After the DFRWS investigation model, Reith, Carr and Gunsch [9], proposed an enhanced model known as Abstract Digital Forensic Model. In 2003, the integrated digital Investigation Process was proposed by Carrier and Spafford [10]. The Enhanced Digital Investigation Process Model introduced a Traceback phase. This enables the investigator to trace back all the way to actual devices or computer used by the criminal to perform the crime. A frequently cited definition for Digital Forensic Science is that of the Digital Forensic Research Workshop (DFRWS) of 2001: “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, 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”[12].

## III. Digital Forensic Process

A digital forensic process uses science and technology to examine digital objects and develops and tests theories. The digital forensics process can be categorized into four different phases as collection, examination, analysis and reporting [5].

Collection: The first phase of digital forensics process is collection phase. The first step in the forensic process is to identify, label, record, and acquire data from the possible sources of relevant data.

Examination: The next phase is to examine collected data, which involves assessing and extracting the relevant pieces of information from the collected data.

Analysis: The next phase of the process is to analyse the results of the examination. Extracted and relevant data has been analysed to draw conclusion.

Reporting: The final phase is reporting the results of analysis; this is the process of preparing and presenting the outcome of the analysis phase.

### A. Computer Forensic Investigative Process (1984)

Methodology for dealing with digital evidence investigation was proposed by pollitt [7]. It has 4 distinct phases.

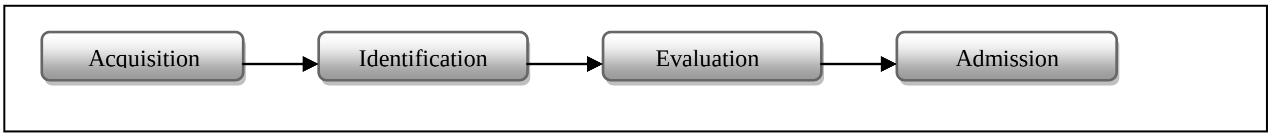

Figure 1: Computer Forensic Investigative Process

In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human. The Evaluation phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, Admission, the acquired & extracted evidence is presented in the court of law [2].

### B. DFRWS Investigative Model (2001)

G. Palmer held the 1st Digital Forensics Research Workshop (DFRWS) and proposed a general purpose digital forensics investigation process [8]. It has 6 phases.

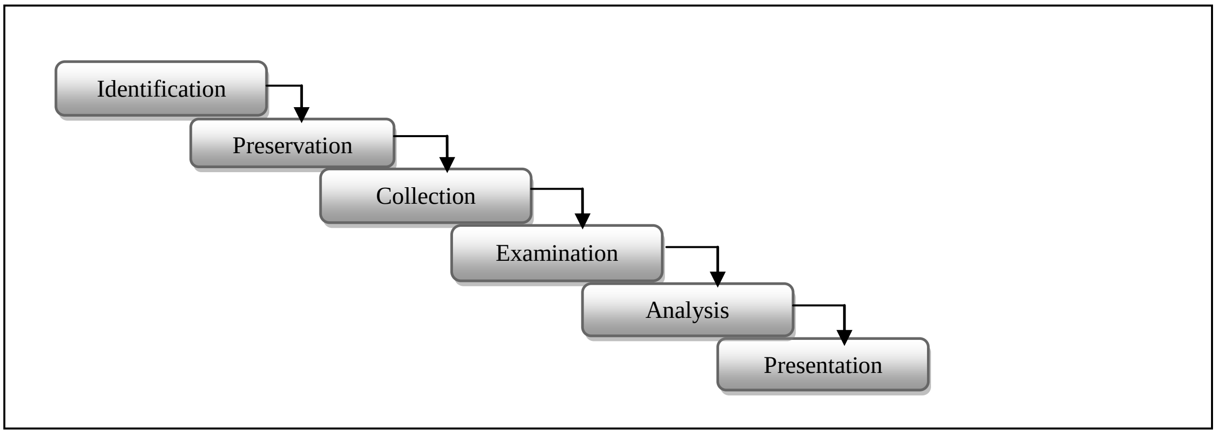

Figure2: DFRWS Investigative Model

DFRWS Investigative model started with an Identification phase, in which profile detection, system monitoring, audit analysis, etc, were performed. It is immediately followed by Preservation phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody. This phase is crucial so as to ensure that the data collected is free from contamination. The next phase is known as Collection, in which relevant data are being collected based on the approved methods utilizing various recovery techniques. Following this phase are two crucial phases, namely, Examination phase and Analysis phase. In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc, were performed. The last phase is Presentation. Tasks related to this phase are documentation, expert testimony, etc [2].

C. **Abstract Digital Forensics Model (ADFM) (2002)**

Reith, Carr & Gunsch [9], proposed an enhanced model known as Abstract Digital Forensic Model. In this model, there is three additional phases than DFRWS, thus expanding the number of phases to nine.

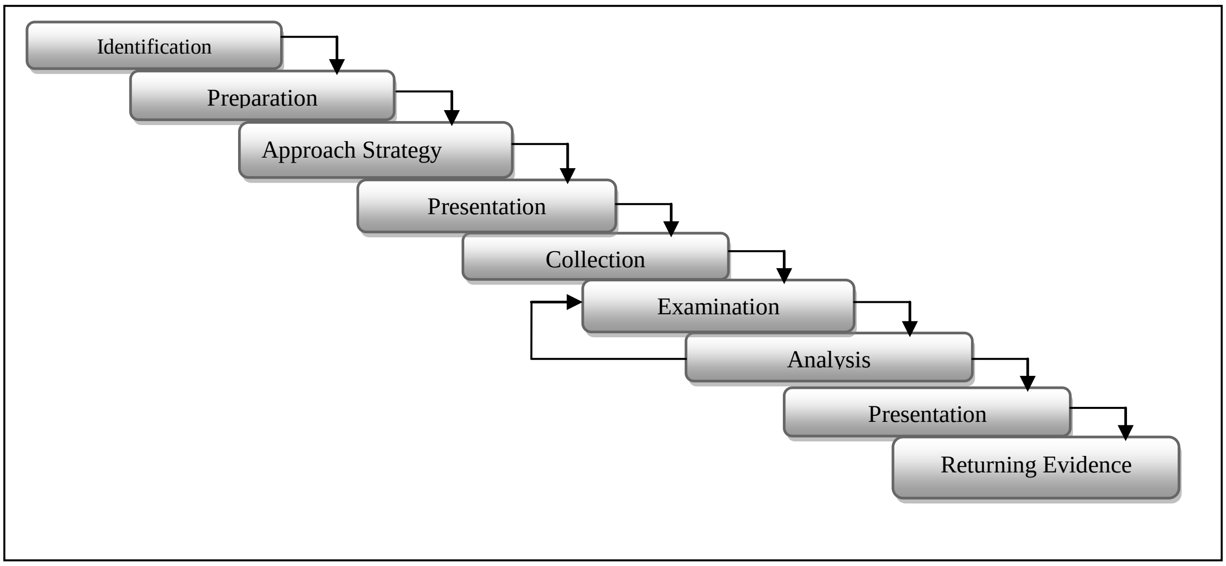

Figure 3: Abstract Digital Forensics Model

The 3 significant phases introduced in this model were Preparation, Approach Strategy and Returning Evidence. In Preparation phase, activity such as preparing tools, identify techniques and getting management support, were done. Approach Strategy was introduced with the objective to maximize the acquisition of untainted evidence and at the same time to minimize any negative impact to the victim and surrounding people. In order to ensure that evidences are safely return to the rightful owner or properly disposed, the Returning Evidence phase was also introduced [2].

The 1st phase in ADFM is Identification phase. In this phase, the task to recognize and determine type of incident is performed. Once the incident type was ascertained, the next phase, Preparation, is conducted, followed by Approach Strategy phase. Physical and digital data acquired must be properly isolated, secured and preserved. There is also a need to pay attention to a proper chain of custody. All of these tasks are performed under Preservation phase. Next is the Collection phase, whereby, data extraction and duplication were done. Identification and locating the potential evidence from the collected data, using a systematic approach are conducted in the next following phase, known as Examination phase. The task of determining the significant of evidence and drawing conclusion based on the evidence found is done in Analysis phase. In the following phase, Presentation phase, the findings are summarized and presented. The investigation processes is completed with the carrying out of Returning Evidence phase [2].

### D. **Integrated Digital Investigation Process (IDIP) (2003)**

Integrated Digital investigation process was proposed by Carrier & Spafford [10] in 2003, to combine the various available investigative processes into one integrated model. The author introduces the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of an incident or crime exists.

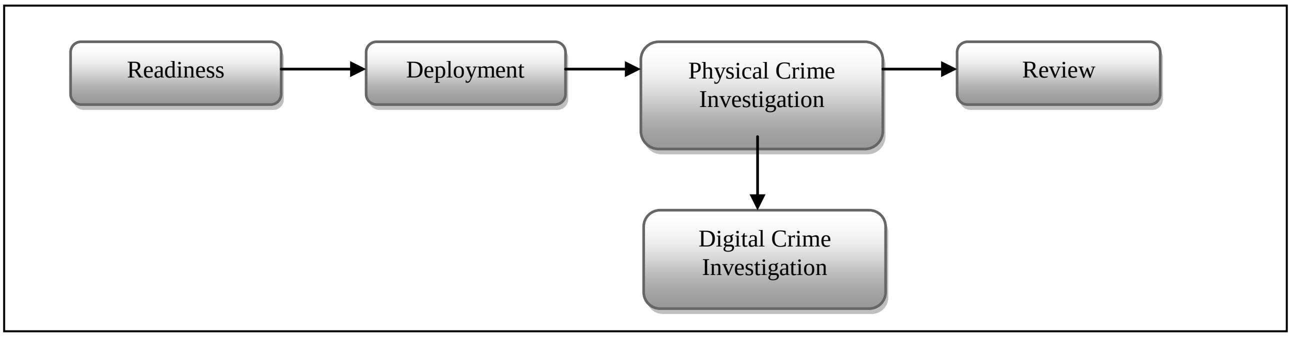

Figure 4: Integrated Digital Investigation Process

The process started with a phase that require for the physical and operational infrastructure to be ready to support any future investigation. In this Readiness phase, the equipments must be ever ready and the personnel must be capable to use it effectively. This phase is indeed an ongoing phase throughout the lifecycle of an organization. It also consists of 2 sub-phases namely, Operation Readiness and Infrastructure Readiness. Immediately following the Readiness phase, is Deployment phase, which provide a mechanism for an incident to be detected and confirmed. Two sub-phases are further introduced, namely, Detection & Notification and Confirmation & Authorization. Collecting and analysing physical evidence are done in Physical Crime Scene Investigation phase. The sub-phases introduced are Preservation, Survey, Documentation, Search & Collection, Reconstruction and Presentation. Digital Crime Scene Investigation is similar to Physical Crime Scene Investigation with exception that it is now focusing on the digital evidence in digital environment. The last phase is Review phase. The whole investigation processes are reviewed to identify areas of improvement that may results in new procedures or new training requirements [2].

## IV. Recognising Common Phases

To identify the common phases shared by all of the presented models, we assigning the model no. to investigation models and sorted them. The result is shown in Table 1.

Table 1: Investigation models

| Model No. | Year | Name |
|---|---|---|
| Mdl1 | 1984 | Computer Forensic Investigative Process |
| Mdl2 | 2001 | DFRWS Investigative Model |
| Mdl3 | 2002 | Abstract Digital Forensics Model |
| Mdl4 | 2003 | Integrated Digital Investigation Process |

Then in next step we extract all of the phases within each of the investigation processes. Extracted phases were assigned with phase no. as unique id. The result is shown in Table 2.

Table 2: list of phases

| Phase No. | Name of phases | Model No. (Available in) |
|---|---|---|
| Ph1 | Acquisition | M1 |
| Ph2 | Admission | M1 |
| Ph3 | Analysis | M2, M3 |
| Ph4 | Approach Strategy | M3 |
| Ph5 | Collection | M2, M3 |
| Ph6 | Deployment | M4 |
| Ph7 | Digital Crime Investigation | M4 |
| Ph8 | Evaluation | M1 |
| Ph9 | Examination | M2, M3 |
| Ph10 | Identification | M1, M2, M3 |
| Ph11 | Preservation | M2, M3 |
| Ph12 | Presentation | M2, M3 |
| Ph13 | Preparation | M3 |
| Ph14 | Physical Crime Investigation | M4 |
| Ph15 | Readiness | M4 |
| Ph16 | Returning Evidence | M3 |
| Ph17 | Review | M4 |

## V. Conclusion

This paper starts with the digital forensic process then moves on the digital forensic investigation models. Here, we have discussed Computer Forensic Investigative Process, DFRWS Investigative Model, Abstract Digital Forensics Model and Integrated Digital Investigation Process. Each phase has a clear goal and requirements and procedures can be developed accordingly. Each model must be evaluated with respect to how it can handle different types of investigations. Based on the digital forensic investigation processes, we are able to extract the basic common investigation phases that are shared among all models.

10.15680/ijircce.2015.0303018

## REFERENCES

1. Venansius Baryamureeba and Florence Tushabe, ”The Enhanced Digital Investigation Process Model”,Asian Journal of Information Technology, 5(7), pp. 790-794, 2006.
2. Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, ” Common Phases Of Computer Forensics Investigation Models”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, pp. 17-31, June 2011.
3. Ms. Smita M. Nirkhi, Dr.R.V.Dharaskar, Director Dr.V.M.Thakre, “DATA MINING: A PROSPECTIVE APPROACH FOR DIGITAL FORENSICS”, International Journal of Data Mining & Knowledge Management Process (IJDKP) Vol.2, No.6, pp. 41-48, November 2012.
4. Mr.Sushilkumar Chavhan and Ms. S. M. Nirkhi, “Visualization Techniques for Digital forensics: A Survey”, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6, pp.74-78, December-2012.
5. Sindhu. K. K. and Dr. B. B. Meshram, “A Digital Forensic Tool for Cyber Crime Data mining”, IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498,Vol.2, No.1, pp. 117-124, 2012.
6. Dr.Dhananjay Kalbande and Nilakshi Jain, “COMPARATIVE DIGITAL FORENSIC MODEL”, International Journal of Innovative Research in Science,Engineering and Technology (ISO 3297: 2007 Certified Organization) Vol. 2, Issue 8, pp.4314-3419, August 2013.
7. M. M. Pollitt, “Computer Forensics: An Approach to Evidence in Cyberspace”, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491,1995.
8. G. Palmer, "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York, 2001.
9. M. Reith, C. Carr & G. Gunsh, “An Examination of Digital Forensics Models”, International Journal of Digital Evidence, Vol. 1, No. 3, 2002.
10. B. Carrier & E. H. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol. 2, No. 2,2003.
11. Sabah Al-Fedaghi and Bashayer Al-Babtain, “Modeling the Forensics Process”, International Journal of Security and Its Applications, Vol. 6, No. 4, pp. 97-108, October, 2012.
12. Anamika Joshi, Dr. D. S. Bhilare,”Digital Forensics: Emerging Trends and Analysis of Counter-Security Environment”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 3, Issue 12, pp. 1116- 1120, December 2013.

## BIOGRAPHY

**Miss. Priya S. Patil** is a scholar of M.E.(Computer Science and Engineering),at P.R. Patil College of Engg. And Technology, Amravati, SGBAU, India.

**Prof. A. S. Kapse** is Asst. Professor in P.R. Patil College of Engg. And Technology, Amravati, SGBAU, India. He received Master of Engineering (CSE) degree in 2011 from GCOE (autonomous), Aurangabad, MS, India.

10.15680/ijircce.2015.0303018