Unit-3 Basics of Digital Forensic

3.1 Digital Forensics

3.1.1 Introduction to Digital Forensics

Forensics science is a well-established science that pays vital role in criminal justice systems. It is applied to both criminal and civil action. Digital forensics sometimes known as digital forensic science, is a branch of forensic science encompassing the recovery and investigationof material found in digital devices, often in relation to computer crime.

Digital forensics includes the identification, recovery, investigation, validation, andpresentation of facts regarding digital evidence found on computers or similar digital storage media devices.

3.1.2 History of Forensic

1. Field of pc forensics began in 1980s when personal computers became a viable possibility for the buyer.

2. In 1984, an associate Federal Bureau of Investigation program was created, which was referred to as magnet media program.

3. It is currently referred to as Computer Analysis and Response Team (CART).

4. Michael Anderson, the Father of Computer Forensics, came into limelight during his period.

5. International Organization on Computer Evidence (IOCE) was formed in 1995.

6. In 1997, the great countries declared that law enforcement personnel should be trained and equipped to deal with sophisticated crimes.

7. In 1998, INTERPOL Forensic Science symposium was apprehended.

8. In 1999, the FBI CART case load goes beyond 2000 case examining, 17 terabytes of

information.

9. In 2000, the first FBI Regional Computer Forensic Laboratory was recognized.

10. In 2003, the FBI CART case load exceeds 6500 cases, examining 782 terabytes of information.

3.1.3 Rule of Digital Forensics

While performing digital forensics investigation, the investigator should follow the given rules:

Rule 1. An examinaṭion should never be performed on the original media.

Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.

Rule 3. The copy of the evidence must be an exact, bit-by-bit copy. (Sometimes referred to as a bit-stream copy).

Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified.

Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.

Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

3,14 Definition of Digital Forensics

Digital forensics is a series of steps to uncover and analyses electronic data through scientific method. Major goal of the process is to duplicate original data and preserve original evidence and then performing the series of investigation by collecting, identifying and validating digital information for the purpose of restructuring past events.

3.1.5 Digital Forensic Investigation

Digital forensic investigation (DFI) is a special type of investigation where the scientific procedures and techniques used will be allowed to view the result- digital evidence- to be admissible in a court of law.

3.1.6 Goals of Digital Forensic Investigation:

The main objective computer forensic investigation is to examine digital evidences and to ensure that they have not been tampered in any manner. To achieve this goal investigation must be able to handle all below obstacles:

1. Handle and locate certain amount of valid data from large amount of files stored in computer system.

2. It is viable that the information has been deleted, I such situation searching inside the file is worthless.

3. If the files are secured by some passwords, investigators must find a way to read the protected data in an unauthorized manner.

4. Data may be stored in damaged device but the investigator searches the data in working devices.

5. Major obstacle is that, each and every case is different identifying the techniques and tools will take long time.

6. The digital data found should be protected from being modified. It is very tedious to prove that data under examination is unaltered.

7. Common procedure for investigation and standard techniques for collecting and preserving digital evidences are desired.

3.2 Models of Digital Forensics

3.2.1 Road map for Digital Forensic Research (RMDFR)

Palmar designed a framework with the following indexed processes shown in Figure 3.1.

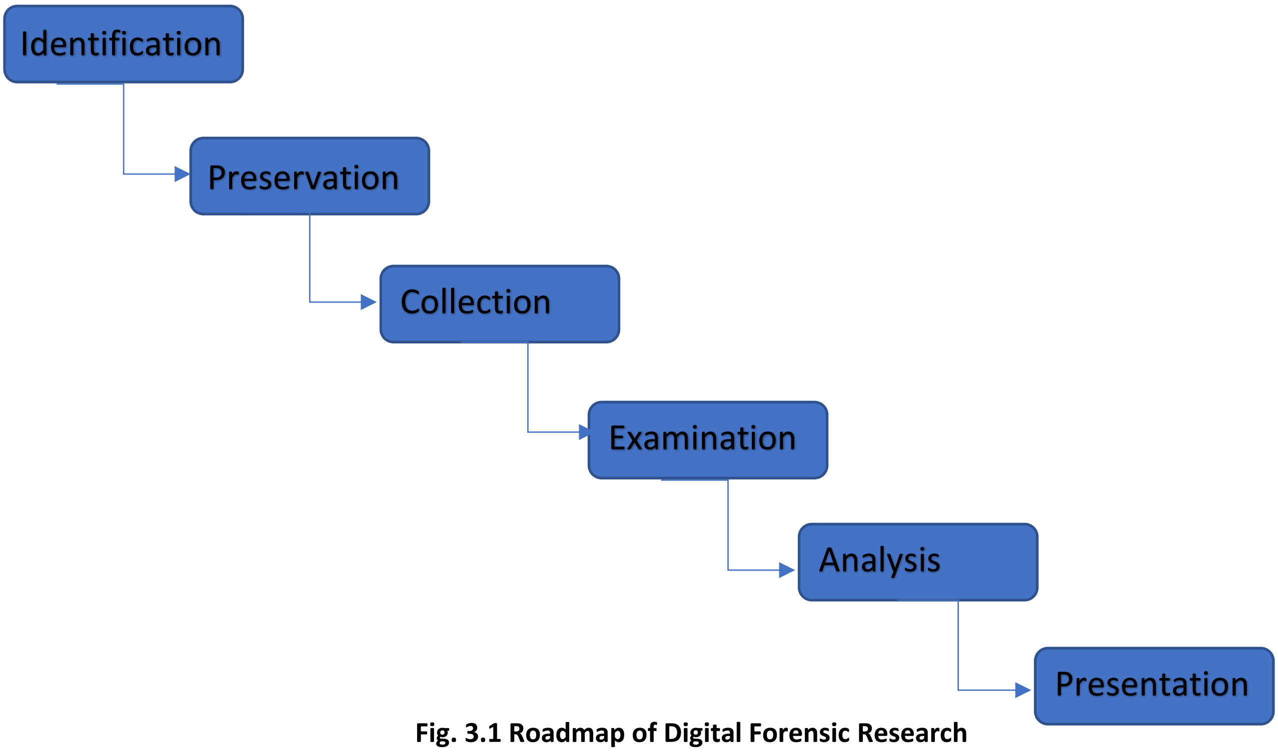


Fig. 3.1 Roadmap of Digital Forensic Research

Six Phases of RMDFR are as follows:

1. Identification: It recognizes an incident from indicators and determines its type.

2. Preservation: Preservation stage corresponds to \freezing the crime scene". It consists in stopping or preventing any activities that can damage digital information being collected. Preservation involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.

3. Collection: Collection stage consists in finding and collecting digital information that may be relevant to the investigation. Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium. Collection máy involve removal of personal computers from the crime scene, copying or printing out contents of files from a server, recording of network traffic, and so on.

4. Examination: Examination stage consists in a \in-depth systematic search of evidence" relating to the incident being investigated. The outputs of examination are data objects found in the collected information. They may include logfiles, data files containing a in specific phrases, times-stamps, and so on.

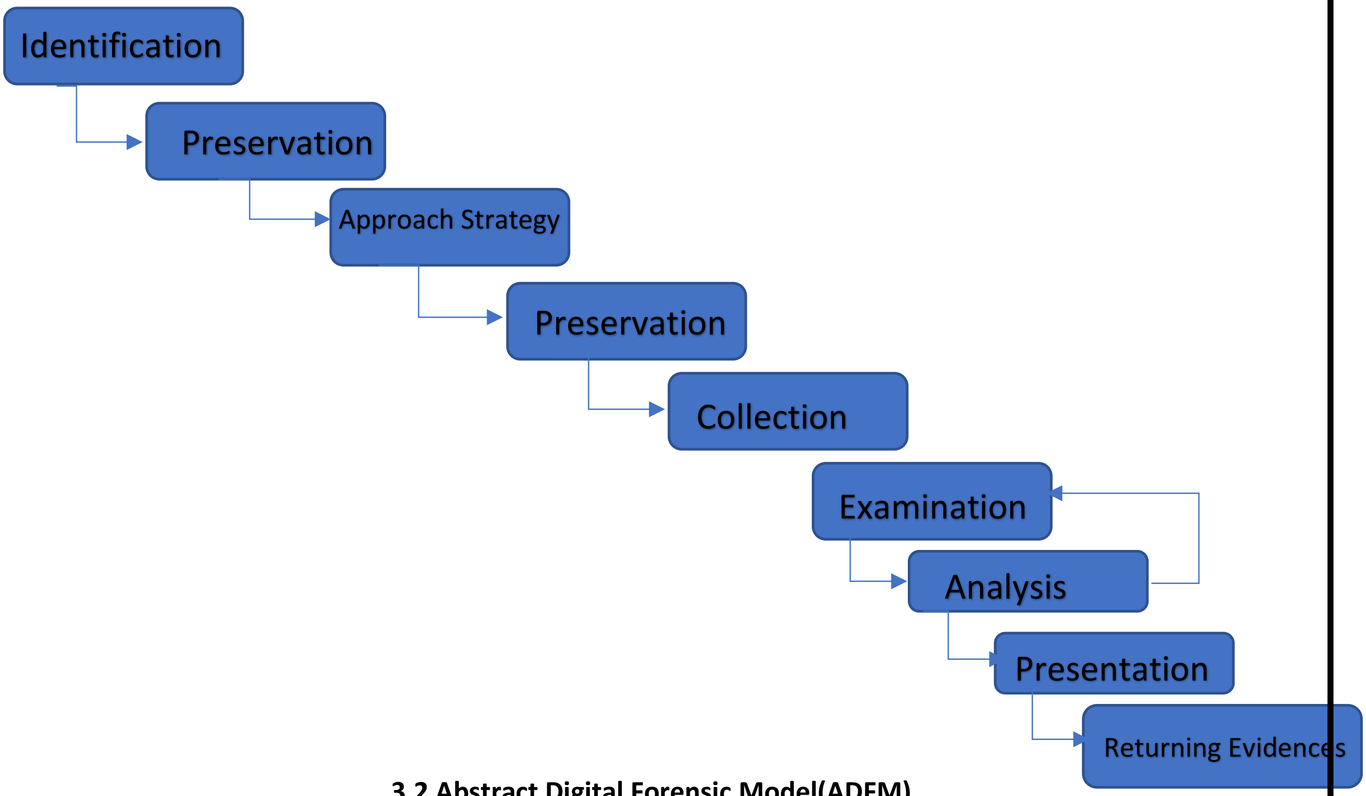
5. Analysis: The aim of analysis is to "draw conclusions based on evidence found".

6. Reporting: This entails writing a report outlining the examination process and pertinent and

data recovered from the overall investigation.

3.2.2 Abstract Digital Forensic Model (ADFM)

Reith, Carr, Gunsh proposed Abstract Digital Forensic model in 2002.



3.2 Abstract Digital Forensic Model(ADFM)

Phases of ADFM model are as follows:

1. Identification -it recognizes an incident from indicators and determines its type.

2. Preparation -it involves the preparation of tools, techniques, search warrants and monitoring authorization and management support

3. Approach strategy -formulating procedures and approach to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

4. Preservation-it involves the isolation, securing and preserving the state of physicaland digital evidence.

5. Collection -This is to record the physical scene and duplicate digital evidence usingstandardized and accepted procedures

6. Examination -An in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence.

7. Analysis -This determines importance and probative value to the case of the examined product

8. Presentation -Summary and explanation of conclusion

9. Returning Evidence -Physical and digital property returned to proper owner.

3.2.3 Integrated Digital Investigation Process (IDIP)

DFPM along with5 groups and 17 phases are proposed by Carrier and Safford. DFPM is named the Integrated Digital Investigation Process (IDIP). The groups are indexed as shown in following Figure 2.3.

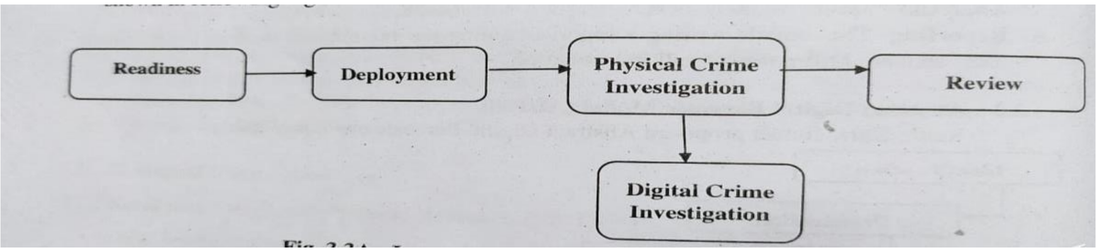


Fig. 3.3An Integrated Digital Investigation Process

The phases of IDIP are as follows:

1. Readiness phase The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:

2. •Operations Readiness phase

• Infrastructure Readiness phase

3. Deployment phase The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

- Detection and Notification phase; where the incident is detected and then appropriate people notified.
- Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

4. Physical Crime Investigation phase The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident.

It includes six phases:

- **Preservation phase;** which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
- **Survey phase;** that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
- **Documentation phase;** which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and' important details of the crime scene are preserved and recorded.
- **Search and collection phase;** that entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin.
- **Reconstruction phase;** which involves organizing the results from the analysis done and using them to develop a theory for the incident.
- **Presentation phase;** that presents the physical and digital evidence to a court or corporate management.

5. Digital Crime Investigation phase The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence.

The six phases are:

• **Preservation phase;** which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.

• **Survey phase;** whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.

• **Documentation phase;** which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.

• **Search and collection phase;** whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user's activities and identity.

• **Reconstruction phase;** which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses.

• **Presentation phase;** that involves presenting the digital evidence that was found to the physical investigative team.

It is noteworthy that this DFPM facilitates concurrent execution of physical and digital investigation.

6. Review phase this entails a review of the whole investigation and identifies areas of improvement. The IDIP model does well at illustrating the forensic process, and also conforms to the cyber terrorism capabilities which require a digital investigation to address issues of data protection, data acquisition, imaging, extraction, interrogation, ingestion/normalization, analysis and reporting. It also highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

3.2.4 End to End Digital Investigation Process (EEDIP)

This model is proposed by Stephenson compriases of six major mechanism within framework. EEDIP stands for End-to-End Digital Investigation Process which ensures investigation operation from beginning to end.

The phases of EEDIP are as follows:

1. **Identification phase** involves identifying the nature of incident from possible known indicators, Indicators are experience investigator.
2. **The preervation phase** includes condensing the investigation and finding till date
3. **The collection phase** includes documentation of the physical seene and replication the digital evidence using approved standard procedure.
4. **Examination phase** involves obtaining and studying the digital evidence .Method of extraction is used for reconstructing data from the media.
5. **In the analysis phase** the vitally of the documented evidence is explored and conclusions are drawn by integrating chunk of data.
6. **A The presentation phase** involves summarizing the evidences found in the process of investigation.

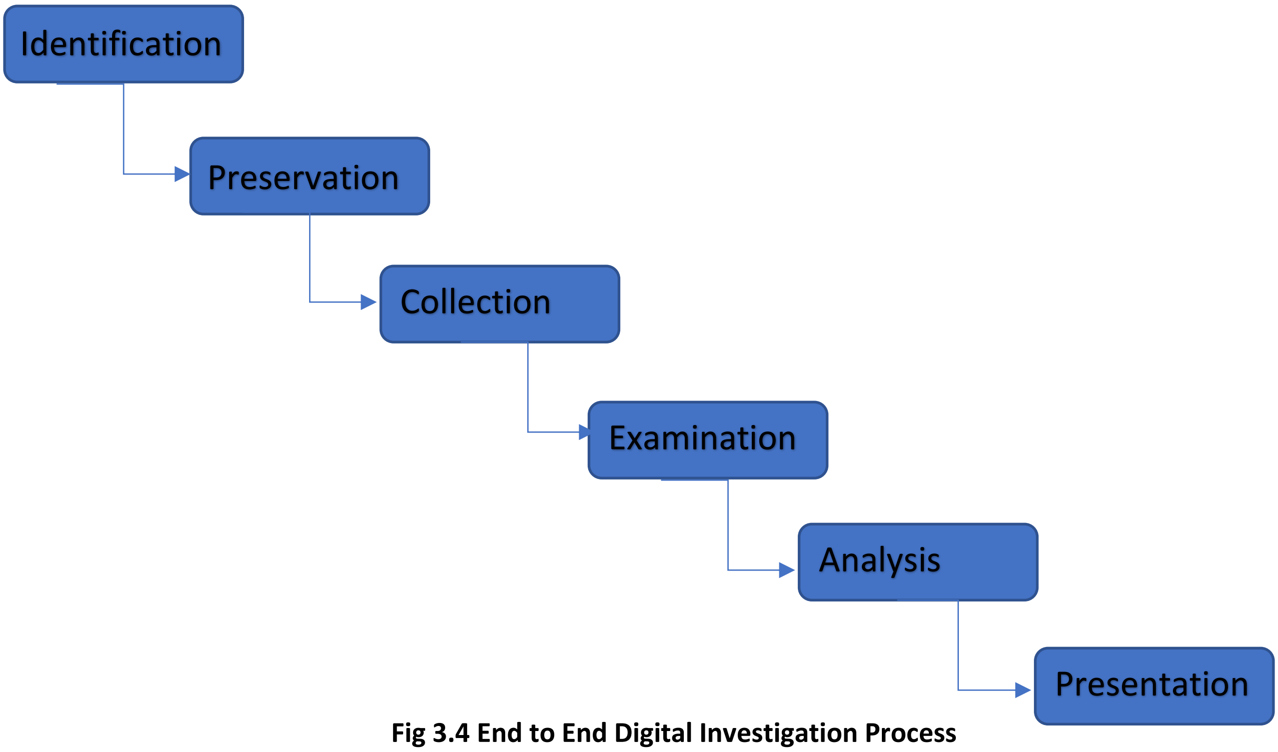


Fig 3.4 End to End Digital Investigation Process

3.2.5 An Extended Model of Cybercrime Investigation (EMCI)

The DFPM proposed by S. O. Ciardhuain- an Extended Model of Cybercrime Investigation (EMCI)- is more likely the most comprehensive till date.

Phases of EMCI: The EMCI follows waterfall model as every activity occurs in sequence. The sequence of examine, hypothesis, present, and prove/defend are bound to be repeated as the evidence heap increases during the investigation.

1. Awareness is the phase during which the investigator are informed that a crime ha staken place; the crime is reported to some authority. An intrusion detection system may also triggered such awareness.

2. Authorization is the stage where the nature of investigation has been identified and the unplanned authorization may be required to procced and the authorization is obtain internally or externally.

3. Planning is impacted by information from which and outside the organization that will affect the investigation. Internal factors are the organization policies, procedures, and former investigative knowledge while outside factors consist of legal and other requirements not known by the investigators.

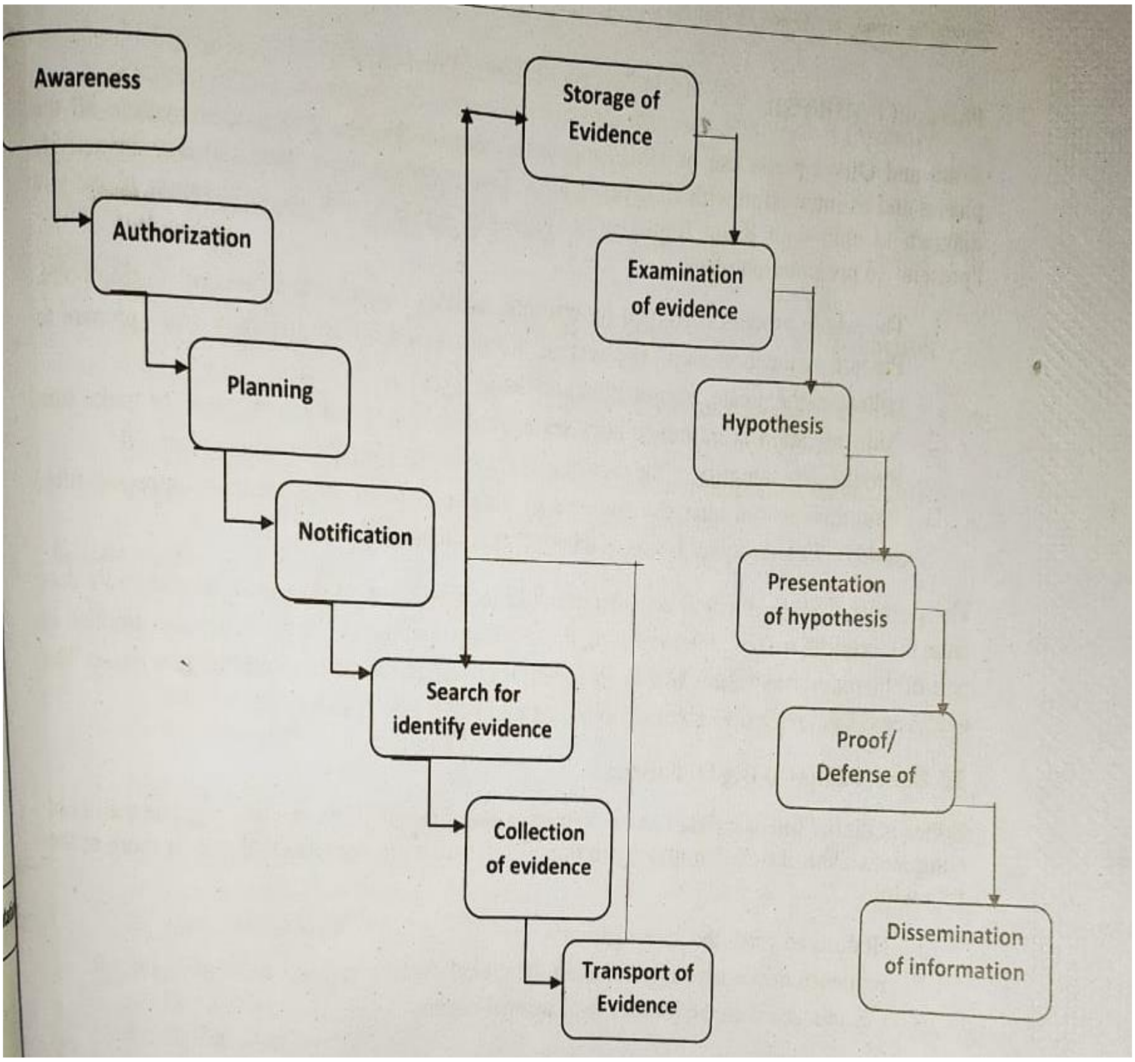


Fig. 3.4 an Extended Model of CyberCrime Investigation(EMCI)

3.2.6 UML modeling of digital forensic process model(UMDFPM)

Kohn, Eloff and Oliver purpose the UML Modeling of digital forensic process model, apt as paradigm for modeling forensic process.

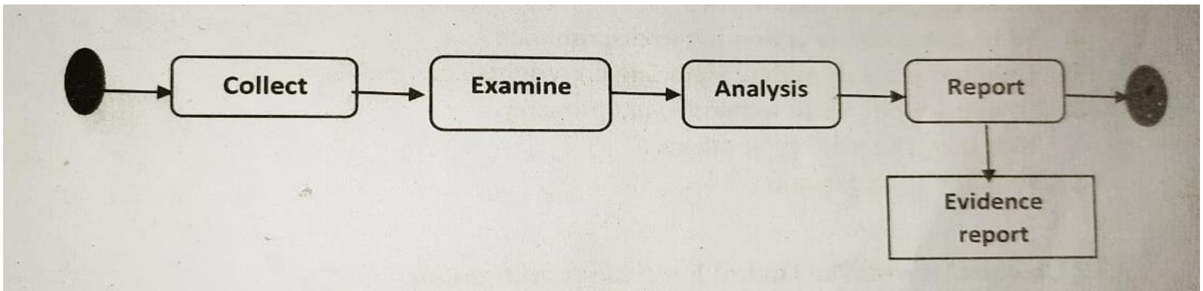


Fig 3.6 UML modeling of digital forensic process model

Phases of UMDFPM:

Kohn and Oliver made use of UML and case diagram (Figure 2.6) to demonstrate all the phases and its interaction with all investigators. Two processes have been added to the activity diagram to club with Kohn framework. These are "prepare" in the preparation phase and "present" in presentation phase.

1. The whole process is trigged by criminal activity, which constitutes of starting point, Prepare is the first step. The rest of the processes follow logically from prepare to collect, authenticate, examination and the analyze.

2. Authentication is introduce between examination and collection phase to make sure that the data integrity of the data before the examination is started is preserved.

3. Examination can alter the contents of data such as in the case of compressed files hidden files and other forms of data incomprehension.

The primary investigator will consider whether to analyze more data or to extract more data from the original source. After reaching this decision points an evidence report is compiled part of the report procedure. Whole document is compiled during the investigation phase. The evidence document is the output of investigation phase.

3.3 Ethical issues in Digital Forensic

Ethics in digital forensic field can be defined as set of moral principles that regulate the use of computers. Ethical decision making in digital forensic work comprises of one or more of the following:

1. Honesty towards the investigation

2. Prudence means carefully handling the digital evidences

3. Compliance with the law and professional norms.

3.3.1 General ethical norms for investigator

Investigator should satisfy the following points:

1. To contribute to the society and human being

2. To avoid harm to others

3. To be honest and trustworthy

4. To be fair and take action nót to discriminate

5. To honor property rights, including copyrights and patents

6. To give proper credit to intellectual property

7. To respect the privacy of others

8. To honor confidentiality

9.

3.3.2 Unethical norms for Digital Forensic Investigation

Investigator should not:

1. Uphold any relevant evidence

2. Declare any confidential matters or knowledge

3. Express an opinion on the guilt or innocence belonging to any party

4. Engage or involve in any kind of unethical or illegal conduct

5. Deliberately or knowingly undertake an assignment beyond him or her capability

6. Distort or falsity education, training, credentials

7. Display bias or prejudice in findings or observation

8. Exceed or outpace authorization in conducting examination

References:

• Digital Forensic by Dr. Nilakshi Jain and Dr. Dhanjay Kalbande Wiley publication ISBN:978-81-265-6574-0

• 2.https://www.academia.cdu/34925415/Computer_Forensics_Digital_Forensic_Analysis_Methodology

• http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0C1681D4A48C19E12DFD6B781B18532?doi=10.1.1.258.7882&rep=rep1&type=pdf

Sample Multiple Choice Questions:

1. Digital forensics is all of them except:

a) Extraction of computer data

b) Preservation of computer data

c) Interpretation of computer data

d) Manipulation of computer data

2. IDIP stands for

a) Integrated Digital Investigation Process

b) Integrated Data Investigation Process

c) Integrated Digital Investigator Process

d) Independent Digital Investigator Process

3. Who proposed Road map model?

a) G. Gunsh

b) S. Ciardhuain

c)J. Korn

d)G. Palmar

4. Investigator should satisfy the following point:

a) Contribute to the society and human being

b) Avoid harm to others

c) Honest and trustworthy

d) All of the above