IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114142

Digital Forensic

Suwarna Nimkarde[1], Shobhana Gaikwad[2]

Lecturer, Computer Technology, Bharati vidyapeeth Institute of Technology, Navi Mumbai, India[1]

Lecturer, Computer Technology, Bharati vidyapeeth Institute of Technology, Navi Mumbai, India[2]

Abstract: The technological advancements to be depicted in the course called emerging trends was a challenging task and therefore it was decided to prepare a learning material with the involvement of industrial and academic experts for its uniformity in the aspect of delivery, implementation and evaluation.

Keywords: RMDFR, ADFM, EEDIP, IDIP, EMCI.

I. INTRODUCTION

Advancements and applications of Computer Engineering and Information Technology are ever changing. Emerging trends aims at creating awareness about major trends that will define technological disruption in the upcoming years in the field of Computer Engineering and Information Technology. IoT, Digital Forensics and Hacking are some emerging areas which are covered in this course and are expected to generate increasing demand as IT professionals and open avenues of entrepreneurship. Considering the necessity of Artificial intelligence (AI) which is an area of computer science that emphasizes the creation of intelligent machines that work and reacts like humans, it is important for Diploma to be aware of AI concept.

Forensic science is well established science that plays important role in criminal justice systems Its applied to both criminal and civil action. Forensics means legal or related to courts. Digital forensics (also known as digital forensic science) can be defined as a branch of forensic science that identify, analyse , recover and investigate digital evidences found in digital devices. These digital evidences are often in relation with computer crime.

II. HISTORY OF DIGITAL FORENSIC

Field of PC forensic began in 1980's when personal computer become cheap to buy. In 1984 an associated Federal Bureau of Investigation program was created, which was referred as magnet media program. It is currently called as Computer Analysis and Response Team(CART).Michael Anderson, the Father of Computer Forensic, came into limelight during this period. International Organization on Computer Evidence(IOCE) was formed in 1995.In 1997, the great countries declared that law enforcement personnel should be trained and equipped to deal with sophisticated crimes .In 1998, INTERPOL Forensic Science symposium was apprehended. In 1999, the FBI CART case load goes beyond 2000 cases examining , 17 TB of information. In 2000, the first FBI Regional Computer Forensic Laboratory was recognized. In 2003, the FBI CART case load exceed 6500 cases, examining 782TB of information.

III. PROCESS OF DIGITAL FORENSIC

Identification

- It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).
- Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

- In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis

- In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found.

Documentation

- In this step, a record of all the visible data must be created. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation

- In this last step, the process of summarization and explanation of conclusions is done.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114142

IV. RULES OF DIGITAL FORENSIC

1. An examination should never be performed on original media.
2. A copy is made onto forensically sterile media. New media should always be used if available
3. The copy of the evidence must be exact, bit-by-bit copy.
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.
5. The examination should be conducted in such a way as to prevent any modification of the evidence.
6. The chain of custody of all evidence must be clearly maintained to provide an audit log of who might have accessed the evidence and at what time.

V. DIGITAL FORENSIC INVESTIGATION

- It describes an investigation where digital device forms part of the incident.
- The successful outcome of DFI is the presentation of digital evidence
- Digital Forensic Investigation(DFI) is a special type of investigation where the scientific procedures and techniques used will be allowed to view results-digital evidence-to be admissible in a court of law
- According to the Oxford online dictionary, the term forensic is defined as "relating to the investigation of crime" OR "relating to courts of law".
- From this definition it is clear that the ultimate goal of a digital forensic investigation is to present some form of evidence in a court of law using the correct legal procedures with scientific backing.

VI. GOALS OF DIGITAL FORENSIC INVESTIGATION

The main objective of digital 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; in such situation searching inside 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

VII. MODELS OF DIGITAL FORENSIC INVESTIGATION

Name of Author	Name of the Model
G. Palmar	Digital Forensic Research Workshop (DFRWS) Investigative Model or Road Map for Digital Forensic Research (RMDFR)
M. Reith, C. Carr and G. Gunsh	Abstract Digital Forensics Model(ADFM)
B. Carrier and E. H. Safford	Integrated Digital Investigation Process (IDIP)
P. Stephenson	End to End digital Investigation Process(EEDIP
S. O. Ciardhuain	An Extended Model for Cybercrime Investigation
J. Kohn, H. P. Eloff and Olivier	UML Modeling of Digital Forensic Process Model(UMDFPM)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114142

VIII. ROAD MAP FOR DIGITAL FORENSIC RESEARCH(RMDFR)

Identification: It recognizes an incident from indicators and determines its type.
-Crime detection
Preservation: Preservation stage corresponds to freezing crime scene.
-It means preventing any activity that can damage digital information being collected.
e.g. preventing people from using the computers so that digital evidence will not be tampered.
-Isolating, securing and preserving data
Collection: Collection stage consists finding and collecting digital information that may be relevant to investigation.
- collecting digital information means either collection of equipment containing the information or recording the information on some other medium.
-collection may involve removal of personnel computers from crime scene, copying or printing contents of files, etc.
-All acquired digital evidence is duplicated, and the physical scene is recorded, based on standardized procedures,
Examination: which involves an in-depth systematic search of evidence relating to the suspected crime?
-Evidence traceability and hidden data must be discovered
Analysis: determine probative value of the examined evidence
-determine whether or not sufficient evidences are available to prove crime in the court
Presentation: It involves the summary and explanation of conclusions.
-prepare document of evidences found during investigation process and present to court

IX. ABSTRACT DIGITAL FORENSIC MODEL(ADFM)

1. Identification: It recognizes an incident from indicators and determines its type.
2. Preparation: where tools, techniques, search warrants, monitoring authorization and management support are prepared,
3. Approach strategy: that develops a approaches and procedures to use in order to maximize the collection of the evidence while minimizing the impact to the victim.
4. Preservation: It involves the isolation, securing and preserving the state of physical and digital evidences.
5. Collection: All acquired digital evidence is duplicated, and the physical scene is recorded, based on standardized procedures.
6. Examination: It involves an in-depth systematic search of evidence relating to the suspected crime.
7. Analysis: The probative value of the examined evidence is determined in Analysis phase (drawing conclusions based on evidence found)
8. Presentation: It involves summarizing the evidences found in the investigation process and present evidences to court
9. Returning evidence: closes the investigation process by returning physical and digital evidence to the proper owner.

X. END-TO-END DIGITAL INVESTIGATION PROCESS(EEDIP)

The phases of EEDIP are as follows:
1. Identification: It involves identifying nature of incident from indicators.
2. Preservation: It includes considering the investigation and findings till date.
3. Collection: It includes documentation of the physical scene and duplication of digital evidence using approved standard procedures.
4. Examination: It involves obtaining and studying the digital evidence.
-Digital data are rarely extracted at the crime scene and digital evidence is preferably gathered in a forensic laboratory
5. Analysis: The probative value of the examined evidence is determined in Analysis phase (drawing conclusions based on evidence found)
6. Presentation: It involves summarizing the evidences found in the investigation process and present evidences to court

XI. AN INTEGRATED DIGITAL INVESTIGATION PROCESS(IDIP)

- This model was first proposed by Carrier and Safford in 2003
- This model is an integration of digital investigation process to the physical investigation process.

This model is organized into 5 groups consisting of 17 phases
Phases of IDIP are as follows:
1. The **Readiness Phases** ensure that human competences and technical infrastructures are able to fully carry the whole investigation process;

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114142

This stage is subdivided to two phases:

- Operation Readiness: provide all training and equipment for investigators.
- Infrastructure Readiness: provide needed infrastructure for investigators.

2. The first phase is followed by **Deployment phases**; the goal of this phase is to Provide a mechanism to detect and confirm an incident, and

This stage is also subdivided to two phases:

- Detection and notification: where incident is detected and appropriate people are notified.
- Confirmation and Authorization: once a crime or incident is confirmed, at this phase authorization must be received to fully investigate the-digital- crime scene.

Phases of IDIP are as follows:

3. Followed immediately by **Physical Crime Scene Investigation** phase where investigator collect and analyze physical evidence

This phase consists of six sub-phases:

- **Preservation:** Which preserve the physical crime scène
- **Survey:** Which involves investigator walk through physical crime scene and identify pieces of physical evidence
- **Documentation:** Which involves taking photographs, sketches and videos of the crime scene
- **Search & Collection:** Which involves in depth search and collection of scene is performed, so that additional physical evidences are identified
- **Reconstruction:** Which involves organizing the results from the analysis done and develop theory for incident
- **Presentation:** Present physical evidences to a court
- **Phases of IDIP are as follows :**

4. This phase is followed by a **Digital Crime Scene Investigation Phases** where investigator collect all digital evidence

This phase consists six 'identical' phases:

- **Preservation:** This phase preserve the digital crime scène
- **Survey:** This phase collects digital evidence
- **Documentation:** It involves documenting every acquired evidence
- **Search & Collection:** Which involves in depth analysis of digital evidence
- - Software tools are used to recover hidden, deleted and corrupted files
- **Reconstruction:** Which involves putting the pieces of digital puzzle together and developing investigative hypotheses
- **Presentation:** that involves presenting the digital evidences to the physical investigation team in the case the investigation was not performed by the same team.
- **5. Review:** In which whole investigation processes is reviewed and identifies areas of improvement

XII. CONCLUSION

The technological advancements to be depicted in the course called emerging trends was a challenging task and therefore it was decided to prepare a learning material with the involvement of industrial and academic experts for its uniformity in the aspect of delivery, implementation and evaluation.

REFERENCES

[1]. Digital Forensic 2017 Edition Dr Nilakashi Jain,Dr Dhananjat R Kalbande Wiley Publishing Inc ISBN: 978-81-265-6574-0
[2]. The Basics of Digital Forensic jhon Sammons Elsevier ISBN:978-1-59749-661-2
[3]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997 .
[4]. Agrawal, R., Jain, R.C., Jha, M.P. and Singh, D. (1980): Forecasting of rice yield using climatic variables. Indian Journal of Agricultural Science, Vol. 50, No. 9, pp. 680-684
[5]. Lee, S., Cho, S.& Wong, P.M., (1999) : Rainfall prediction using artificial neural network.— J. Geog. Inf. Decision Anal. 2, 233–242 1998.
[6]. C. —Rainfall Prediction Using Neural Fuzzy Technique.
[7]. C. Hamzacebi, "Improving artificial neural networks' performance in seasonal time Series Forecasting", Information Sciences 178 (2008), pages: 4550-4559.
[8]. Jianye Liu; Jiankun Yu, Research on Development of Android Applications, 4th International Conference on Intelligent Networks and Intelligent Systems, 15 December 2011.