iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VI Month of publication: June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35544

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

A Survey on Digital Forensic Investigation Practitioners Approach and Challenges

Prof. Sachin Babulal Jadhav[1], Prof. Manoj Raosaheb Gaikwad[2], Prof. Y.S. Modhe[3]
[1, 2, 3]*Department of Computer Technology, Sanjivani K.B.P. Polytechnic, Kopargaon, Maharashtra, India*

Abstract: Digital crimes are taking place over the entire world. For any digital crime which commit at any part of world, computer or any electronic devices are used. The devices which are used to commit the crime are useful evidences which must be identified and protected for further use. The crimes involving electronic devices are called as cyber-crime. To investigate such crimes, a scientific procedures needs to be followed. The data collection, analysis, preservation and presentation of digital evidence is must in order investigate the cybercrime. This paper highlights the practices that are used worldwide in the investigation process of cyber-crime. Keywords: Digital Forensics, Analysis, Investigation, models of investigation.
Keywords*: *Digital Forensics, Analysis, Investigation, models of investigation, Cyber security.

I. INTRODUCTION

There are around 50 billion devices that are connected to internet in the year 2020 and more are added per hour. For individuals and organizations, computers have become mandatory to run a successful business. It is not enough to have an isolated computer which does not connect to the internet; Businesses need networked computers for communication with other businesses. This exposes them to the outside world. Cybercriminals use computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. They can easily get data and snip the information which are available in computers. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks. The cyber-crime involves phishing attacks, email scams, denial of service (DOS), hacking, phone phreaking, Virus, Trojans, Malware, social engineering attacks, etc. When cybercrime takes place, one can get help from forensics professionals to solve problems and recover the vital business and personal information stolen.

Digital forensics refers to the investigation of digital system, usually during a court of law, when an individual is under interrogation for breaching data or information. Digital forensics recovers information using complex tools so as to bring an individual to justice for being exploited or tampered his or her private information. Forensics science proved to be a well-established science that pays vital role in criminal justice systems. It is applied to both criminal and civil action. Digital forensics is a branch of forensic science that involves the recovery and investigation of digital evidence found in digital devices, often in relevance with computer crime[1]. Digital forensics starts with the identification of crime if its a digital crime, recovery of evidences, investigation of physical crime scene, validation about integrity of digital evidence and presentation of understandings regarding digital evidence that are collected from computers or other digital storage devices from crime scene[1].

A. Goals of Digital Forensic Investigation

The main objective computer forensic investigation is to examine digital evidence and to ensure that they have not been tampered in any manner. To achieve this goal investigation must be ready to handle all below obstacles [11]:

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 could also be stored in damaged device but the investigator searches the information in working devices.
5) Major obstacle is that, each and each case is different identifying the techniques and tools will take long time.
6) The digital data found should be shielded from being modified. It is a very important and difficult task to prove that the data that is being examined has not tampered.
7) Common procedures for investigation and standard techniques for collecting and preserving digital pieces of evidence are desired.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

II. DIGITAL EVIDENCES

The field of cyber security includes events and situations that provide a successful and satisfactory courtroom experience [2]. Investigation of a computer security incident leads to legal proceedings, such as court proceeding, where the digital evidence and documents obtained are likely used as exhibits within the trial. To meet the wants of the judging body and to face up to or face any challenges, it's essential to follow the evidence-handling procedure. Also, it is necessary to ensure that the evidence-handling procedures chosen are not difficult to implement at your organization as this can sometimes become an overhead for an organization. While investigating cyber security cases, we are sometimes not sure about whether an material evidence such as a chip, the floppy disk could be considered as evidence. In today's world we are using digital devices in everything and everywhere, to help individuals and organizations to communicate with local and global organizations easily. Most people think that computers, cell phones, PDA's are the sources for digital evidence, but any piece of electronic that can process the data or information can be used for a criminal activity. For example, video games can carry encrypted and encoded messages between criminals or terrorists and even consumer appliances, like a refrigerator, microwave oven, smart TV, can also be used to store and carry illegal contents such as images with embedded messages. The important thing to note here is that investigators should recognize and collect potential files, pictures, and other digital evidence relevant to crime. Digital evidence sometimes called Electronic evidence is any kind of information that is stored or transmitted in digital form that one can produced in a court case trial[3]. Before accepting digital evidence a court will determine if the evidence has any relevance with the incident, whether it is authentic and whether a copy is suitable or the original device is required. Digital evidence is additionally defined as information and data useful to an investigation that's stored on, received or transmitted by an electronic device. This evidence are often acquired when electronic devices are seized and secured for examination.

A. Digital Evidence Characteristics

1) Is latent means it is not visible as in case of physical evidence, it needs to be discovered like fingerprints or DNA
2) it can bypass jurisdictional boundaries easily
3) they can be altered, damaged, destroyed or get corrupt if not handled properly
4) Can be time sensitive

There are many sources of digital evidence; the types are divided into three major forensic categories of devices where evidence are often found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence-gathering processes, tools and concerns, and differing types of crimes tend to lend themselves to at least one device or the other.

Some of the favored electronic devices [4] which are potential digital evidence are: HDD, CD/DVD media, backup tapes, USB drive, biometric scanner, camera, smart phone, open-end credit, PDA, etc.

B. Forms of Digital Evidences

Text message, emails, pictures, videos and internet searches are commonest sorts of Digital evidences. The digital evidence are used to establish a credible link between the attacker, victim, and the crime scene. Some of the information stored in the victim's computer or other devices can be used as digital evidence [5] such as IP address allocated, system log files & remote log details, browsing history data, emails, images, video recordings etc.

Other Digital Evidences may be in the form: Email Messages (may be deleted one also), Office file, Deleted files of all kinds, Encrypted file, Compressed files, Temp files, Recycle Bin, Web History, Cache files, Cookies, Registry, Unallocated Space, Slack Space, Web/E-Mail server access Logs, Domain access Logs, etc.

III. FORENSIC INVESTIGATION PRACTICES

A. Road Map for Digital Forensic Research (RMDFR)

Palmar designed a framework[6][7][8] with the following indexed processes shown in Figure-1.

Figure 1: RMDFR Model of forensic Investigation

The procedures used in Forensics are used by all the investigators. The basic steps of this forensic model are Identification, Preservation, Collection, Examination, Analysis and Presentation.

The Six Phases of RMDFR are as follows:

The process of investigation starts with the identification phase and sequentially produces the report of the investigation. Let's sees each phase in detail.

1) Identification: In this phase, investigators are made aware of an incident that happened. From available indicators, it is determined that if it needs to carry digital investigation.
2) Preservation: The preservation stage corresponds to isolate the crime scene location. It consists of stopping or preventing all activities that can tamper with digital information. Preservation involves preventing people from using computers during collection, stopping ongoing deletion processes if any, and choosing the scientific way to collect information from the scene.
3) Collection: The collection stage starts with finding and collecting digital information that may be relevant to the investigation. As digital information is stored in electronic systems all the pieces of equipment containing the information, or recording is identified and seised. The collection involves taking custody of laptops, personal computers CCTV footage from the crime scene, also taking photographs, copying or printing out the files from a server computer, recording of network traffic, and so on.
4) Examination: The examination stage carries a systematic analysis of evidence related to the incident. The result of the examination is data objects of interest found in the collected evidence. It may include log files, data files containing in specific phrases, times-stamps, encoding, and so on.
5) Analysis: In this phase conclusions are drawn based on evidence found[7]. The analysis phase links the sequence of facts related to the incident. This phase records all the facts, objects and to justify their decision.
6) Presentation: In this phase a detailed report regarding the incident is written. It may recreate the crime scene with the report. Each and every step taken in the investigation, person involved in the investigation, an authority who are handling evidence is recorded with a time stamp. The detailed report is then submitted to the court.

B. *Abstract Digital Forensic Model (ADFM)*

Reith, Carr, Gunsh proposed Abstract Digital Forensic model in 2002.This model is inspired form the previous model. It consist of total 9 phases [8][9][10]. Three additional phases are preparation, Approach strategy and returning the evidence.

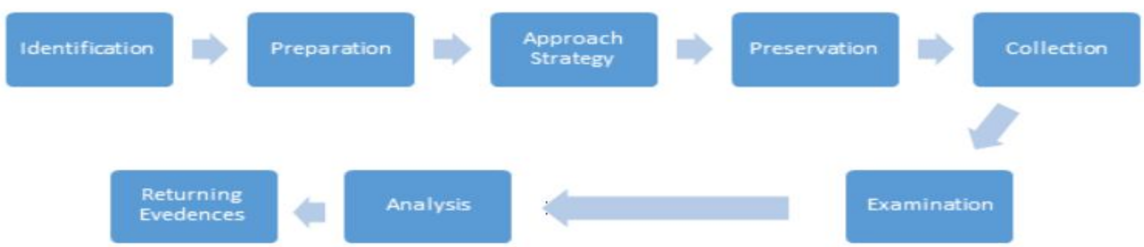


Figure 2: Abstract Digital Forensic Model

Phases of ADFM model are as follows:

1) Identification -In this phase incident is identified for potential of digital crime. If observed the involvement of digital devices in crime then investigators are notified.
2) Preparation -This involves the preparation of tools, techniques, search warrants, and authorization to carry out an investigation. All legal formalities are completed.
3) Approach strategy -Formulating procedures and approaches to be used in order to maximize the collection of evidence while minimizing the impact on the victim.
4) Preservation-it involves the isolation, securing and preserving the state of physical and digital evidence.
5) Collection -This is to record the physical scene and duplicate digital evidence using standardized 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 phase derives the conclusion of the case of the examined.
8) Presentation -Summary and explanation of the conclusion
9) Returning Evidence -Physical and digital devices collected as evidence are returned to the owner of devices.

IV. CHALLENGES IN DIGITAL FORENSICS

There are many issues and challenges that an investigator has faces while investigating the cyber-crime. Some of issues and challenges are as follows:

A. Data or Information Inconsistency

The Data and information recovered from the crime scenes may be inconsistent and misleading. Data is generally destroyed after the crime which makes finding genuine evidence is big challenge in the digital forensic investigation.

B. Size of Evidence

The amount of data recovered from the crime scene plays an important role in the investigation. Less data is practically not useful.

C. Encrypted Data

The data recovered at crime scene may be in the encrypted form which makes difficulties in solving the case. Investigator has to ensure about exact decryption method and original evidence should be unaltered.

D. Technology Updates

The investigator should be equipped with latest and updated practices in investigation process. Proper and regular training regarding is required to investigator to know the new practices.

E. Security-Awareness

The training of individuals and staff in an organization about the security awareness is must. Lack of awareness about security measures is mostly identified cause of cyber-crime.

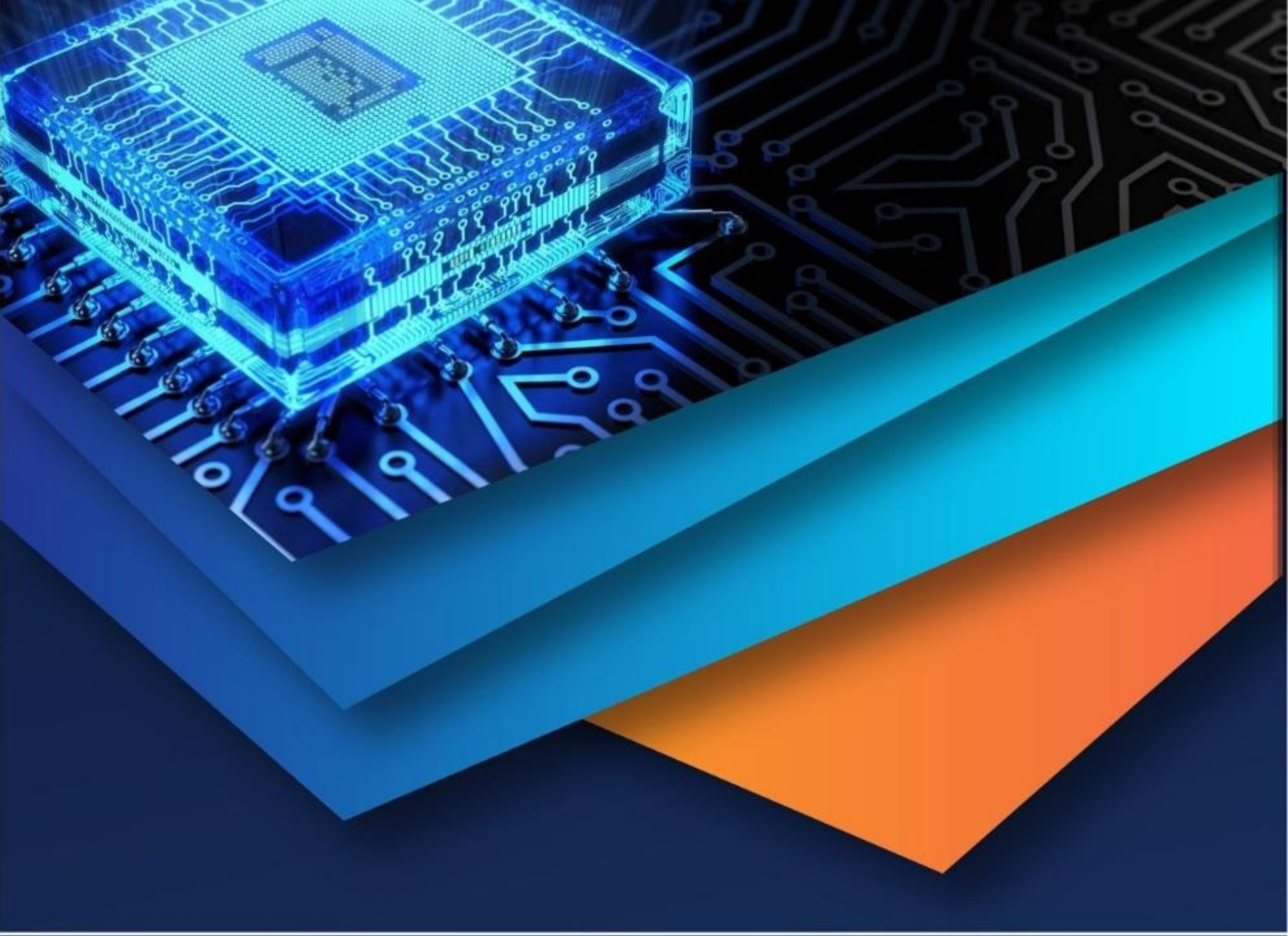
These are some of the challenges the investigators face. The list is still incomplete and will add many challenges as cases are investigated and solved

V. CONCLUSIONS

Forensic investigation is playing major role in scientific investigation of digital crime. The practices discussed in this paper are followed by majority of investigators worldwide. In the coming days we are observing lots of cases registered as digital frauds under cyber-crimes even all the security measures taken,. Hackers will find a way to break the system same time forensic practices will be updated and will improve in various areas. There is a need for more portable and rapid forensic investigation practices. Till that time awareness about security measures is a must for everyone. As said "To catch a thief, think like thief". More accurate practices are expected to be developed in the coming future which will fasten the process of investigation.

REFERENCES

[1] 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_Methodolo
[3] http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0C1681D4A48C19E12DFD6B781B18532? doi=10.1.1.258.7882&rep=rep1&type=pdf
[4] Malek Harbawi and Asaf Varol, "The Role of Digital Forensics in Combating Cybercrimes".
[5] M. Al Fahdi, N.L. Clarke and S.M. Furnell, "Challenges to Digital Forensics: A survey of researchers & practitioners attitudes and opinions.
[6] B.Skaggs, B. Blackburn, G. Manes, S. Shenoi, "Network Vulnerability Analysis".
[7] Prashant S. Shinde and Prof. Shrikant B. Ardhapurkar , "Cyber Security Analysis using VulnerabilityAssessment and penetration Testing".
[8] Abirami Sivaprasad and Smita Jangale, "A Complete study on Tools and Techniques for digital Forensic Analysis".
[9] Andrw Jones and Stilianos Vidalis and Nasser Abouzakhar, "Information Security and digital forensics in the world of cyber physical systems".
[10] Arun V. Sathanur and David J. Haglin, "A novel centrality Measure for network-wide cyber vulnerability assessment".
[11] Arni Ariani, John Lewis and Pradeep K. Ray, "The vulnerability assessment for Emergency response Plans".



10.22214/IJRASET

INDEX COPERNICUS
45.98

ISRA JIF
IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY