International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Introduction to Digital Forensics (Cyber Forensics)

Md. Sohel Rana[1], Md. Mehadi Hasan[2], Md. Moneruzzaman[3]

[1]Programmer, Power Division, Dhaka, Bangladesh, E-mail: soheltee@gmail.com.
[2]System Analyst, Jiban Bima Corporation, Dhaka, Bangladesh, Email: mehadi.jbc@gmail.com.
[3]Programmer, Derectorate of Posts, Dhaka, Bangladesh, E-mail: mone15_cse@yahoo.com.

DOI: https://doi.org/10.55248/gengpi.4.1223.123427

ABSTRACT:

Crimes occurred within electronic or digital domains, mainly within cyberspace, have become a common trend. Criminals are using technology to commit their crimes and make new challenges for attorneys, law enforcement agents, judges, security professionals and military. Digital forensics has become a vital instrument in recognizing and solving computer-assisted and computer-based crime. This paper delivers a brief overview to digital forensics.

Keywords: Cyber forensics, digital forensics, computer forensics, network forensics, cybercrime.

I. INTRODUCTION

Digital Forensics is the process of identification, preservation, extraction, and documentation of computer based evidence which can be used by the law enforcement agency or court of law. It is a science of ruling evidence from digital media like a mobile phone, computer, server, network or printer. It offers the forensic team with the greatest techniques and tools to solve complex digital-related cases. Digital Forensics assistances the forensic team to inspect, analyzes, identifies, and preserves the digital evidence living on various sorts of electronic devices.

II. OBJECTIVES OF DIGITAL FORENSICS

Here are some essential objectives of Digital forensics:

- It helps to analyze, recover and preserve computer and related tools in such a manner that it supports the investigation agency to represent them as evidence in a court of law.
- It helps to hypothesize the motive behind the crime and uniqueness of the main culprit.
- Designing procedures at a supposed crime scene which supports you to ensure that the digital evidence found is not corrupted.
- Data duplication and acquisition: Recovering deleted partitions and deleted files from digital media to citation the evidence and authorize them.
- Helps you to recognize the evidence quickly, and also permits you to estimate the potential influence of the malicious action on the victim
- Generating a computer forensic report which deals a complete report on the inquiry process.
- Conserving the evidence by succeeding the chain of custody.

III. PRINCIPLES OF DIGITAL FORENSICS

The Following Figure Shows the Basic Principles of Digital Forensics:

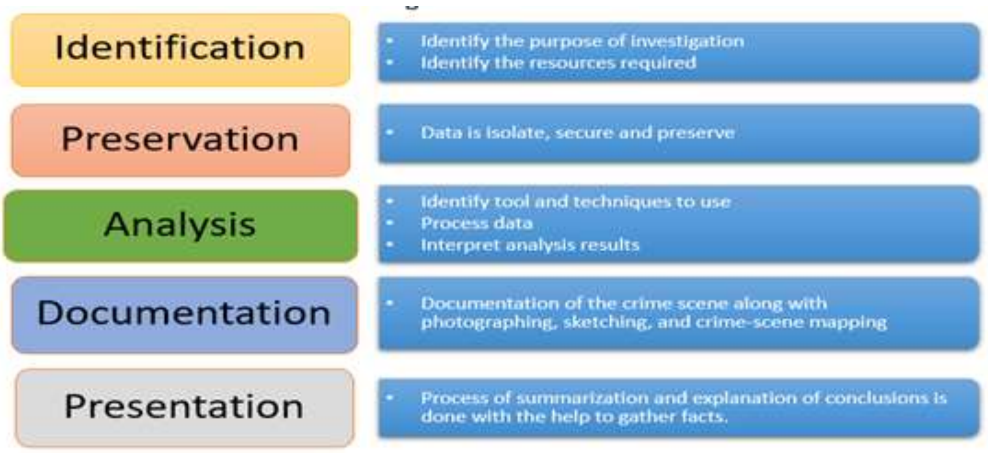
Identification
Identify the purpose of investigation
Identify the resources required
Preservation
Data is isolate, secure and preserve
Analysis
Identify tool and techniques to use
Process data
Interpret analysis results
Documentation
Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation
Process of summarization and explanation of conclusions is done with the help to gather facts.

Fig- Basic Principles of Digital Forensics

Identification:

This is the first step in forensic process. The identification process generally includes belongings like what kind of evidence is present, how it is stored that means which format, and finally where it is stored. Electronic storage media can be Mobile phones, personal computers, PDAs, etc.

Preservation:

In this phase, data is secured, isolated, and preserved. It contains preventing people from spending the digital device to facilitate digital evidence is not altered.

Analysis:

In this step, investigation representatives reconstruct fragments of data and lure conclusions based on evidence originate. Though, it might take several iterations of examination to provision a particular crime theory.

Documentation:

In this procedure, a record of all noticeable data must be created. It helps in restoring the crime scene and appraising it. It contains suitable documentation of the crime scene along with sketching, crime-scene mapping and photographing.

Presentation:

In Final step, the process of explanation and summarization of conclusions is done. Though, it should be written in an amateur’s terms using distracted terminologies. All distracted terminologies should mention the specific details.

IV. TYPES OF DIGITAL FORENSICS

The types of digital forensics are:

Disk Forensics:

It treaties with mining data from storage media by modifying, searching active, or deleted files.

Network Forensics:

It is a sub-branch of digital forensics. It is connected to analysis and monitoring of computer network traffic to gather important information and lawful evidence.

Wireless Forensics:

It is a division of network forensics. The main goal of wireless forensics is to deals the tools need to analyze and collect the data from wireless device or network traffic.

Database Forensics:

It is a subdivision of digital forensics linking to examination and study of databases and their associated metadata.

Malware Forensics:

This division deals with the proof of identity of malicious code, to study viruses, their payload, worms and malware.

Email Forensics

Contracts with analysis and recovery of emails, calendars, including deleted emails, and contacts.

Memory Forensics:

It is the process of collecting data from RAM, Cache, SSD, and HDD in raw format and then model the data from raw dump.

Mobile Phone Forensics:

It primarily deals with the analysis and examination of mobile devices. It supports to recover phone and SIM contacts, incoming, and outgoing SMS/MMS, call logs, audio, videos, etc.

V. CHALLENGES

Challenges faced by Digital Forensics

- The increase of Personal Computer and widespread use of internet access
- Easy availability of hacking tools
- Absence of physical evidence creates prosecution difficult.
- The huge volume of storage space into TB (Terabytes) that makes this examination job hard.
- Any technological modifications need an upgrade or alterations to solutions.

VI. CONCLUSION

The forensic investigation of electronic systems has definitely been a huge achievement in the identification of computer-assisted and cyber-crime. Organizations are engaging an increasing significance on the need to be fortified with proper incident management capabilities to handle abuse of systems. Computer forensics is a precious tool in the process of investigation. The field of computer forensics has grown up significantly in the last decade. Driven by industry, attention was primarily placed upon emerging tools and techniques to help in the practical solicitation of the technology.

VII. REFERENCES

[1] https://www.oreilly.com/library/view/computer-forensics a/9781849281607/Text/backmatter01.html

[2] https://www.unodc.org/e4j/en/cybercrime/module-4/index.html

[3] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego, CA: Academic Press, 3rd edition, 2011, chapter 1.

[4] https://en.wikipedia.org/wiki/Digital_forensics

[5] S. L. Garfunkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, 2010, pp. S64-S73.

[6] The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics 1st Edition by John Sammons.

[7] Cybercrime and Digital Forensics: An Introduction by Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar.

[8] Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T. S. Ho, Shujun Li.