Bansilal Ramnath Agarwal Charitable Trust's
Vishwakarma Institute of Technology
(An Autonomous Institute affiliated to Savitribai Phule Pune University)

Department of Information Technology

IT-Bulletin

Feb-2023

'Digital Forensic Framework'

HIGHLIGHTS

"Digital Forensics: What No One Is Talking About"

"Data is the pollution problem of Information age, and Protecting PRIVACY is the environmental challenge "

"Digital Forensics is the process of preservation, identification, extraction, and documentation of computer evidence"

- What is Digital Forensics?

A subset of cyber security known as "digital forensics" or "digital forensic science" focuses on the extraction and examination of data from digital devices and cyber-attacks. Originally used as a synonym for computer forensics, the term "digital forensics" has come to refer to the analysis of any devices that hold digital data.

Digital forensics' origins may be traced to the personal computer revolution of the late 1970s, but it wasn't until the early 2000s that nations like the United States started implementing national regulations.

Seizure, forensic imaging, and analysis of digital material are among the five divisions that make up today's technical division of an investigation.

- What is the Purpose of Digital Forensics?

The most typical application of digital forensics is to prove or disprove a claim in a criminal or civil court:

1.Criminal cases: Investigations into any illegal action carried out by cybercriminals are considered criminal charges. Digital forensic examiners and law enforcement organizations often handle these situations.

2.Civil cases: A type of digital forensics known as electronic discovery was used to resolve contractual disputes between businesses or to safeguard the rights and property of people (eDiscovery).

"Digital Forensics: What No One Is Talking About"

The wide range of data carriers, the massive amount of data they retrieve, and the various data formats.Electronic forensic investigation, also known as eDiscovery, is the process of searching, sorting, and presenting a large amount of information in a short period of time in accordance with the requirements of a specific authority. It is critical that the investigation be conducted in a responsible and transparent manner so that the results of the forensic investigation can be used by all stakeholders.

- Rules of Digital Forensics

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

Rule 1: An examination 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.

- What is the Digital Forensics Investigation Process?

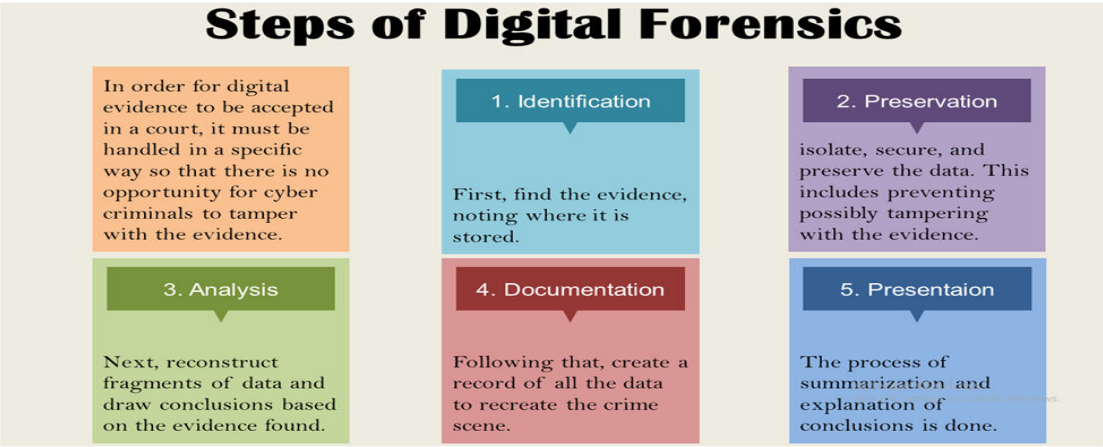


Fig.1 Steps of Digital Forensic

"Digital Forensics: What No One Is Talking About"

- What Tools Do Digital Forensic Examiners Use?

In 1980, forensicinvestigator was forced to do live analysis, using existing sysadmin tools to extract evidence.This later said as evidence tampering, modifying data on the disk. In 1989 this was the need recognized by software at the Federal Law Enforcement Training Center and resulted in the creation of IMDUMP and SafeBack. There is now a trend toward live memory forensics utilising tools like WindowsSCOPE and mobile device technologies.

Today, there seem to be solitary applications such as Wireshark, a network sniffer, and HashKeeper, a tool for speeding up database file analysis. In addition, commercial systems with many functions and reporting abilities, such as Encase or CAINE, a complete Linux distribution built for forensics applications, are available.

In general, tools can be broken down into the following ten categories:

1. Disk and data capture tools
2. File viewers
3. File analysis tools
4. Registry analysis tools
5. Internet analysis tools
6. Email analysis tools
7. Mobile devices analysis tools
8. Mac OS analysis tools
9. Network forensics tools
10. Database forensics tools

- What are the Different Branches of Digital Forensics?

Computer forensics is no through over with digital forensics. It is becoming deeply concerned with data originating from various digital devices like as tablets, smartphones, flash drives, and even cloud computing.

"Digital Forensics: What No One Is Talking About"

In general, we may divide digital forensics into five categories:

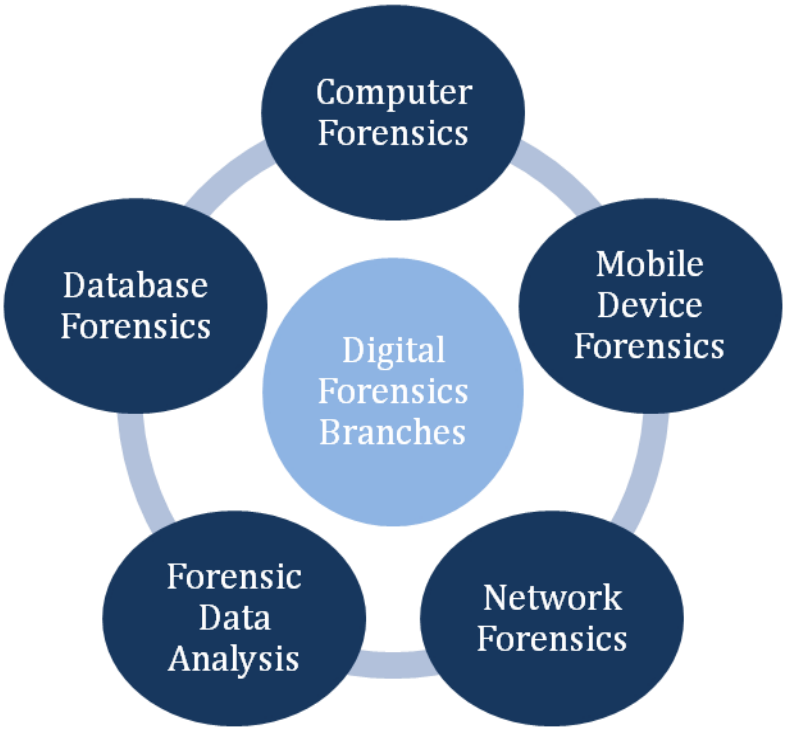


Fig 2.Different Branches of Digital Forensics

- What is Digital Evidence?

1. What is the chain of custody in computer forensics?

In digital forensics, the chain of custody is indeed described as the forensic link, the paper trail, or the chronological documentation of digital evidence. It denotes the gathering, control sequence, transmission, and analysis. It also records whom accessed the forensic evidence, the day and time it was gathered or transmitted, and the reason for the transfer.

2. Why is it critical to keep the chain of custody intact?

Maintaining the chain of custody is critical to preserving the integrity of the electronic evidence and preventing contamination, which might change the integrity of the electronic evidence. If electronic evidence is not maintained, it may be contested and deemed inadmissible in court.

"Digital Forensics is an exact science– not the procedures but the results"

EDEWEDE ORIWOH

"Digital Forensics: What No One Is Talking About"

- Procedure to Establish the Chain of Custody

Chain of custody prevents evidence from being tainted; it thus establishes trustworthiness of items brought into evidence.

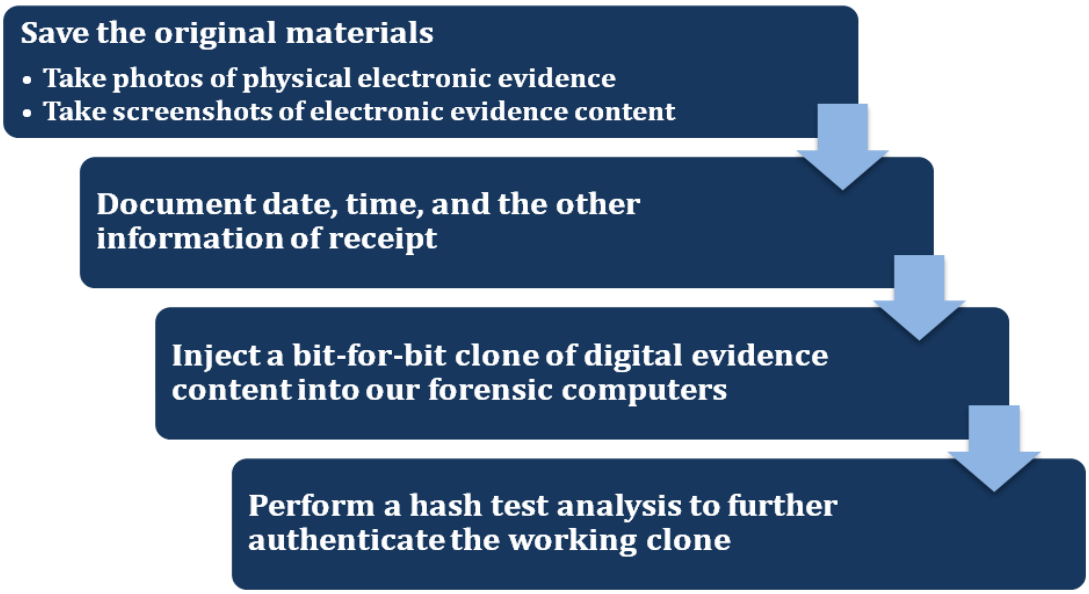


Fig.3 Procedure to Establish the Chain of Custody

- Digital Evidences may be in the form:

1. Email Messages (may be deleted one also)
2. Office file
3. Deleted files of all kinds
4. Encrypted file
5. Compressed files
6. Temp files
7. Recycle Bin
8. Web History
9. Cache files
10. Cookies
11. Registry
12. Unallocated Space
13. Slack Space
14. Web/E-Mail server access Logs
15. Domain access Logs

"Digital Forensics: What No One Is Talking About"

- Summary

In summary, digital forensics is the preservation, identification, extraction, and documenting of computer evidence for use in legal proceedings.

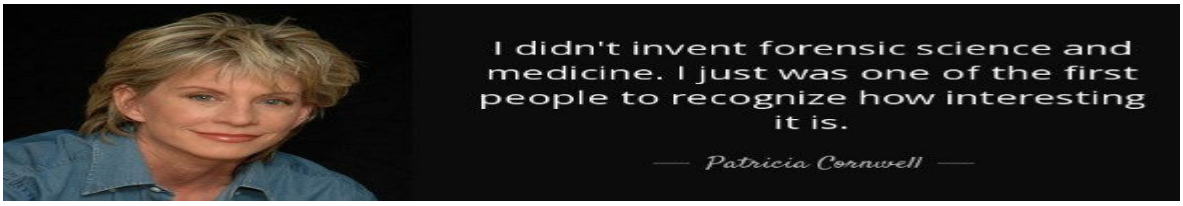
The digital forensics process consists of the following steps: 1) Identification, 2) Preservation, 3) Analysis, 4) Documentation, and 5) Presentation.

Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Email Forensics, Memory Forensics, and more forms of Digital Forensics exist.

Digital forensic science may be employed in circumstances such as 1) Intellectual property theft, 2) Industrial espionage, and 3) Cybercrime. 3) Labor conflicts, 4) Fraud investigations

- References

1. https://en.wikipedia.org/wiki/Digital_forensics#Application
2. https://www.upguard.com/blog/digital-forensics#toc-6
3. https://www.geeksforgeeks.org/digital-forensics-in-information-security/
4. https://www.guru99.com/digital-forensics.html
5. https://www.studocu.com/in/document/marathwada-mitra-mandals-polytechnic/computer-science/dfh-qb-forensic-imp-questions/34580069
6. https://www.helpnetsecurity.com/2007/07/20/the-rules-for-computer-forensics/
7. https://www.eccouncil.org/what-is-digital-forensics/
8. https://www.dataexpert.eu/blogs/digital-forensics-blogs/



Student Editor: Prithviraj Deshmukh, Sanika Divekar, Sanket Jadhav, Tejas Pacharne (B.Tech-IT)

HOME TOP