WORKING MECHANISMS OF DIGITAL FORENSICS IN CYBERCRIME INVESTIGATION

Ayush.S.Bhelaye[1], R.S. Durge[2]

[1]B.E. (CSE) student, Department of Computer Science & Engineering, Dr. Rajendra Gode Institute of Technology & Research, Amravati, Maharashtra, India.

[2]Guide, Department of Computer Science & Engineering, Dr. Rajendra Gode Institute of Technology & Research, Amravati, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS44227

ABSTRACT

Because digital forensics allows professionals to locate, gather, store, examine, and present digital evidence, it is essential to contemporary cybercrime investigations. The functioning processes of digital forensics, including evidence collecting, forensic imaging, hashing, analysis tools, and reporting, are the exclusive subject of this study. The study demonstrates how forensic specialists use organized techniques and instruments to recreate cyber events while maintaining data integrity and admissibility in court.

Keywords: Digital Forensics, Cybercrime, Evidence Analysis, Forensic Tools, Investigation Process.

1. INTRODUCTION

A subfield of forensic science called "digital forensics" is concerned with locating, protecting, evaluating, and presenting digital evidence in a way that complies with the law. It gives investigators a methodical way to identify the series of digital actions that culminate in a crime in the context of cybercrime investigations. By bridging the gap between technology and law, the field makes sure that evidence retrieved from networks, computers, and mobile devices is genuine and verifiable. Professionals can guarantee accuracy and procedural soundness throughout criminal investigations by having a solid understanding of digital forensics' functioning principles.

2. METHODOLOGY AND WORKING

A scientific and methodical approach to digital forensics guarantees that digital evidence is identified, preserved, collected, examined, and presented in a way that is legally acceptable. In order to preserve data authenticity from the time of capture until it is presented in court, the procedure combines technological accuracy, forensic tools, and procedural integrity.

2.1 Overview of Forensic Workflow

Understanding the incident's type and extent—whether it involves malware infection, cyber fraud, illegal access, or data theft—is the first step in the digital forensic process. After defining it, investigators create a forensic plan that details the tools, data sources, and procedures for managing evidence. This methodical process guarantees consistency of outcomes and guards against evidence contamination.

2.2 Identification and Preservation

Finding possible evidence sources, such as hard drives, USB devices, cell phones, cloud storage, or network logs, is the process of identification. The goal of preservation is to safeguard the integrity of data while it is being collected. To make sure the evidence doesn't change, investigators employ write blockers, cryptographic hashing methods (MD5, SHA-1, SHA-256), and chain-of-custody documents. Because any alteration might make the evidence legally invalid, this step is essential.

2.3 Acquisition and Imaging

Following the preservation of evidence, forensic specialists use programs like FTK Imager, EnCase, or the Linux utility dd to produce forensic images, which are bit-by-bit duplicates of digital media. These pictures capture residual, concealed, and erased data that is inaccessible to regular users. By ensuring that all investigations are conducted on copies, imaging protects the original data for later validation. The identical integrity is confirmed by comparing the hash values of the picture and the source.

2.4 Examination and Analysis

In order to find actions pertinent to the case, digital data must be extracted and interpreted during the examination phase. Investigators carry do the following tasks: • File system analysis (Autopsy, Sleuth Kit)

Rebuilding the timeline and keywords

These procedures provide proof of system breach, user behavior, attack time, and data exfiltration routes. AI- assisted tools and automation speed up pattern recognition and lessen manual labor.

2.5 Documentation, Reporting, and Presentation

Following technical analysis, every discovery is methodically recorded. Reports contain the following: a description of the instruments utilized; detailed procedures; screenshots or analysis logs; chain-of-custody information; and evidence summaries appropriate for presenting in court.

Clear, accurate, and repeatable reports that adhere to accepted forensic standards like ISO/IEC 27037 and NIST recommendations are required. Investigators must be able to attest to the integrity, validity, and dependability of every piece of evidence that is offered in court.

2.6 Integrated Workflow Summary

Digital forensics' operational process may be summed up as an ongoing cycle:

1. Identification of the incident and characterization of its scope.

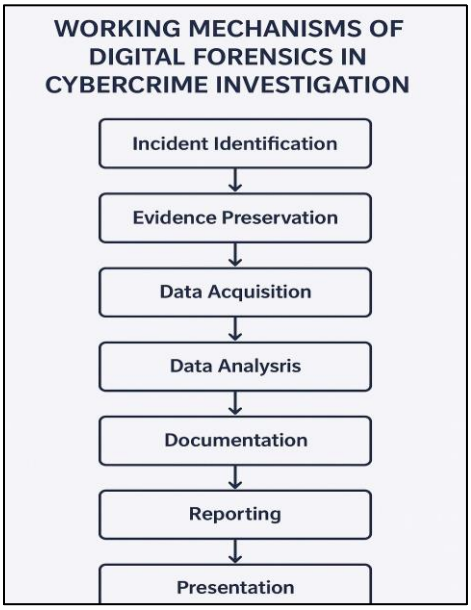
2. Identification and preservation of the evidence

3. Forensic imaging and data collection

4. A thorough examination and correlation of the artifacts

5. Legal presentation, reporting, and interpretation

This iterative procedure guarantees that each digital item is meticulously analyzed, reducing mistakes and preserving forensic integrity. To manage the enormous scope and complexity of contemporary cybercrime investigations, current systems increasingly incorporate cloud forensics capabilities, automated artifact categorization, and machine learning.



3. RESULTS AND DISCUSSION

The effectiveness of tools, the precision of evidence collection, and adherence to protocol norms all affect the operational outcomes of digital forensic investigations. The speed and precision of analysis have increased with the use of artificial intelligence and forensic automation. According to case studies, organized processes facilitate the quick detection of cybercriminal trends and the traceability of online activity. The results also highlight the significance of standardized laboratory settings and qualified specialists.

4. TOOLS USED IN DIGITAL FORENSICS

Specialized tools are used in digital forensics to assist investigators in correctly and effectively gathering, analyzing, and presenting evidence. The capacity of these technologies to maintain data integrity and guarantee legal admissibility led to their selection.

[1] Tools for disk and data acquisition: These are used to make precise duplicates of digital media without changing the original data. FTK Imager, EnCase Forensic, X-Ways Forensics, and dd are examples of common tools.

[2] File & System Analysis Tools: These tools aid in user activity tracking, file system inspection, and data recovery from deletion. Autopsy, Sleuth Kit, Magnet AXIOM, and ProDiscover are a few examples.

[3] Memory & Volatile Data Tools: These are used to examine system memory and find hidden programs or live invasions. Among the tools are Rekall, Redline, and Volatility Framework.

[4] Tools for Network and Cloud Forensics: Help in tracking and examining data movement in cloud and network environments. X1 Social Discovery, NetworkMiner, and Wireshark are well-known tools.

[5] Mobile Forensic Tools: Crucial for obtaining texts, call records, and app information from cellphones. Oxygen Forensic Suite, MOBILedit Forensic Express, and Cellebrite UFED are often used tools.

[6] Reporting Tools: Used to keep the chain of custody intact and provide organized, court-ready reports. Belkasoft Evidence Center and FTK Reporting Modules are two examples of tools that guarantee authenticity and documentation.

Tool Validation: To ensure dependability, repeatability, and legal acceptability, all tools must adhere to NIST CFTT and ISO/IEC 27037 standards.

5. CONCLUSION

The foundation of cybercrime investigations is made up of digital forensics' operational procedures. Every step, from identifying digital evidence to final reporting, guarantees the conclusions' legal acceptability and scientific integrity. Automation, AI-based analysis tools, and technological breakthroughs all contribute to the discipline's ongoing evolution. In addition to supporting law enforcement, a strong forensic foundation increases public confidence in digital justice systems.

6. REFERENCES

[1] Nelson, B., Phillips, A., & Steuart, C. (2020). Guide to Computer Forensics and Investigations. Cengage Learning.

[2] Casey, E. (2019). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

[3] Carrier, B. (2017). File System Forensic Analysis. Addison-Wesley.

[4] Palmer, G. (2001). A Road Map for Digital Forensic Research. Digital Forensic Research Workshop (DFRWS).

[5] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3).