IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, December 2025
Impact Factor: 7.67

Computer Forensics Investigation

Prof. Shweta Hedaoo[1], Mr.Bhavesh Ugale[2], Mr.Prajwal Gandhare[3]
Guide,Computer Science and Engeneering Department[1]
Student, Computer Science and Engeneering Department[2-5]
Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, India

Abstract: *This research explores the systematic science of identifying, preserving, examining, and presenting digital evidence in a legally acceptable manner. In an era of escalating cyber threats, computer forensics has become a vital component of modern investigative techniques for solving crimes such as data breaches and cyber fraud. This paper details a modular forensic investigation system design and evaluates the application of industry-standard tools like FTK Imager and Autopsy through simulated cybercrime cases. The study emphasizes the critical nature of maintaining the chain of custody and data integrity to ensure legal admissibility..*

Keywords: Digital Forensics, Cybercrime Investigation, Data Integrity, Chain of Custody, Forensic Tools

I. INTRODUCTION

The modern digital era has seen a sharp rise in digital crimes, leaving behind electronic evidence that is crucial for solving crimes if properly analyzed. Computer forensics involves a systematic approach to uncovering data from digital devices while ensuring evidence integrity is maintained. Investigators must balance technical expertise in file systems and networks with legal standards like the chain of custody.

II. Problem Statement

Cybercriminals increasingly use anti-forensic techniques, such as encryption and file obfuscation, to hide their footprints. A major challenge in the field is retrieving and analyzing digital evidence from complex systems while ensuring it remains legally admissible. Digital evidence is volatile and can be easily modified or deleted if not handled with specialized tools.

II. LITERATURE SURVEY

The proposed forensic investigation system utilizes a modular architecture to ensure security and efficiency:

- Evidence Acquisition Module: Uses hardware write-blockers and imaging tools (e.g., FTK Imager) to create bit-by-bit copies of data without altering original media.
- Data Storage Module: Securely stores forensic images with metadata and hash values (MD5, SHA-256) to ensure integrity.
- Analysis Module: Employs software like Autopsy and Wireshark for file system exploration, timeline reconstruction, and network traffic analysis.
- Reporting Module: Generates structured findings for legal professionals and stakeholders.

III. SYSTEM ARCHITECTURE & PROPOSED METHODOLOGY

Through simulated investigations of data breaches and file deletions, the study demonstrated that user-centered forensic tools, such as Autopsy, improve investigator efficiency and reduce cognitive load. Adhering to Standard Operating Procedures (SOPs) and rigorous documentation proved essential for maintaining the chain of custody..

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, December 2025
Impact Factor: 7.67

IV. DETAILED MODULE DESCRIPTION

Through simulated investigations of data breaches and file deletions, the study demonstrated that user-centered forensic tools, such as Autopsy, improve investigator efficiency and reduce cognitive load. Adhering to Standard Operating Procedures (SOPs) and rigorous documentation proved essential for maintaining the chain of custody.

V. CONCLUSION AND FUTURE SCOPE

The research underscores the necessity of bridging theoretical knowledge with practical application in digital forensics. As technology evolves, future work must focus on emerging forensic tools, automated analysis techniques, and the growing challenges of cloud and network forensics.

REFERENCES

[1]. B. Carrier, File System Forensic Analysis, Addison-Wesley Professional, 2005.
[2]. E. Casey, Digital Evidence and Computer Crime, Academic Press, 2011.
[3]. B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, Cengage Learning, 2014.
[4]. NIST, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, 2006