www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 500-501

e-ISSN : 2583-1062
Impact Factor : 7.001

DIGITAL FORENSICS IN CYBERCRIME INVESTIGATION

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

[1,2]Department of Computer Science Engineering, Sant Gadge Baba Amravati University, India.

DOI: https://www.doi.org/10.58257/IJPREMS44212

ABSTRACT

Digital forensics has emerged as a crucial element of contemporary cybercrime investigation, bridging the divide between digital technology and law enforcement. The importance, procedures, and approaches of digital forensics in locating, conserving, evaluating, and presenting electronic evidence are examined in this work. It draws attention to the function of forensic methods and tools in identifying online dangers including identity theft, hacking, and data breaches. Along with discussing the ethical and legal issues surrounding the management of digital evidence, the study highlights the necessity of standard operating procedures. According to the findings, digital forensics improves cybersecurity frameworks across industries and supports criminal prosecution.

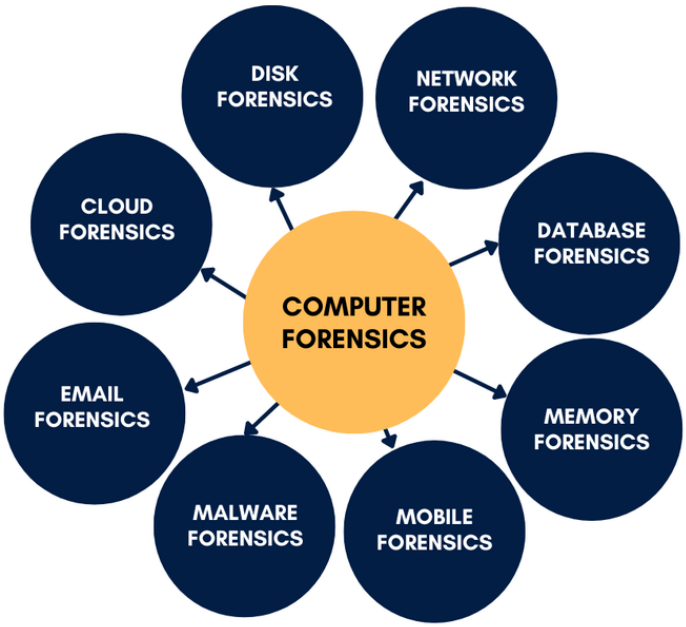
Keywords: Digital Forensics, Cybercrime, Evidence Analysis, Cyber Investigation, Cybersecurity.

1. INTRODUCTION

Digital forensics is super important in today's cybercrime investigations. It really helps connect law enforcement with the tech world. In order to locate, preserve, analyze, and present electronic evidence, this study examines the importance, procedures, and methodology of digital forensics. It emphasizes how important forensic methods and tools are for identifying online dangers like identity theft, hacking, and data breaches. The report also highlights the need for standardized methods and addresses the ethical and legal issues surrounding the management of digital evidence. The results imply that digital forensics enhances cybersecurity in addition to supporting criminal prosecution.

2. METHODOLOGY

The methodical procedure used in digital forensics investigations guarantees the validity of the evidence. Digital evidence is identified, preserved, analyzed, and presented as part of the technique. Finding the sources of digital data, such as PCs, cellphones, or cloud storage, is the first step. Preservation uses forensic imaging technologies and write blocks to guarantee data integrity. To retrieve pertinent data, the analysis step uses specialist software such as EnCase, FTK, and Autopsy. Lastly, investigators compile their findings into a report that may be presented in court. To preserve the legitimacy of the evidence, a proper chain of custody must be maintained throughout this procedure.



3. MODELING AND ANALYSIS

Several models are used in digital forensics to expedite cyber investigation. The digital forensic investigation framework, which comprises stages including acquisition, inspection, analysis, and reporting, is the most widely used model. By examining network packets, log files, and file information, analytical tools aid in incident reconstruction.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 500-501

e-ISSN : 2583-1062
Impact Factor : 7.001

To find patterns of harmful activity, investigators frequently use timeline analysis and data correlation tools. Using artificial intelligence for anomaly detection and predicted threat identification is another aspect of modeling in digital forensics. These methods minimize physical intervention while improving the precision and effectiveness of investigations.

4. RESULTS AND DISCUSSION

The success rate of solving cybercrimes has increased dramatically with the use of digital forensic tools in cybercrime investigation. The findings show that organized forensic techniques produce accurate and repeatable results in court cases. Effective training, the utilization of cutting -edge tools, and interdisciplinary cooperation between law enforcement and IT specialists are discussed as critical success elements. Nevertheless, there are still issues with managing encrypted data, legal restrictions, and developing technologies like cloud computing and the Internet of Things. It need ongoing research, legal adaption, and international collaboration among digital investigators to address these problems.

5. CONCLUSION

Because digital forensics offers a methodical and scientific approach to evidence management, it is essential in the fight against cybercrime. By detecting flaws, it improves cybersecurity in addition to assisting criminal justice. various methods of attack. According to the study's findings, digital forensic frameworks need to change as technology advances. Justice and the preservation of confidence in digital ecosystems depend on ongoing advancements in forensic tools as well as legal and ethical norms.

6. REFERENCES

[1] Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations. Cengage Learning.

[2] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

[3] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3), 1 –12.

[4] Carrier, B. (2005). File System Forensic Analysis. Addison -Wesley.

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