

Experiment 1

Aim:

To study the basics of computer forensics and explore different tools used in forensic investigations.

Procedure:

- Understand the fundamental concept of Digital Forensics, which involves identifying, collecting, examining, analyzing, and presenting digital evidence.
- Learn about various phases of digital forensics and the international legal framework of cybercrime.
- Explore the forensics environment including hardware and software, storage devices, operating systems, file systems, metadata, password security, encryption, and hidden files.
- Discuss the technical complexities involved in digital evidence handling.
- Study popular forensic tools including:
 - Commercial suites like EnCase, Forensic Tool Kit (FTK), and ProDiscover.
 - Open-source forensic suites like The Sleuth Kit (TSK), Helix, and Knoppix.
 - Field tools like FTK Imager, Log Parser Lizard GUI, and Autopsy forensics platform.
- Gain conceptual knowledge on how these tools are used for forensic imaging, data recovery, and forensic investigations.

Result:

- Successfully understood the theoretical foundation and environment of digital forensics.
- Familiarized with multiple forensic tools commonly used by professionals.
- Gained an overview of evidence collection, the importance of forensically sound imaging, and challenges in analyzing digital evidence.
- Enhanced preparedness for practical forensic investigations by understanding the capabilities and applications of key forensic tools.