Digital Forensics using Sleuth Kit Autopsy in Cyber Crime Investigation

Introduction

In today's digital era, almost every crime involves a digital footprint. Criminals often use computers, smartphones, USB drives, cloud storage, or social media to plan, execute, or hide illegal activities. To uncover this hidden evidence, investigators rely on **Digital Forensics** — a scientific process that involves the identification, preservation, analysis, and documentation of digital evidence.

One of the most widely used forensic tools for disk image analysis is **Autopsy**, a GUI-based application built on top of **The Sleuth Kit**. As demonstrated in **Experiment No. 13**, Autopsy allows investigators to analyze hard drives, recover deleted files, examine timestamps, search keywords, and generate admissible forensic reports.

What is a Sleuth Kit Autopsy?

Sleuth Kit is an open-source digital investigation framework that provides command-line tools to analyze disk images and file systems such as FAT, NTFS, ext, and ISO.
Autopsy is its graphical interface, making digital forensic investigation easier for law enforcement, cyber experts, and students.

Key Features of Autopsy (As per Experiment)

Feature	Purpose
Timeline Analysis	Shows chronological file activities to identify suspicious behavior.
Hash Matching	Verifies file integrity and detects known malicious or illegal files.
File Recovery	Recovers deleted or hidden files from disk partitions.
Keyword Search	Helps investigators search for specific terms or evidence inside files.
Web Artifacts Analysis	Extracts browser history, cookies, downloads, and bookmarks.
Report Generation	Creates detailed HTML, CSV, and text-based forensic reports for legal presentation.

How Autopsy is Used in Investigations (As per Lab Steps)

1. **Creating a Case:**
   Investigators begin by launching Autopsy and creating a new case with case details (Case Name, Description, Investigator Name).
2. **Adding Disk Image:**
   A forensic disk image (like .dd, .img, .E01) is imported. This image is acquired earlier using tools like FTK Imager or dd command.
3. **Verifying Integrity (Hashing):**
   Autopsy calculates MD5/SHA-1 hash values to ensure the image is unaltered — crucial for maintaining the chain of custody.
4. **Analyzing Disk Contents:**
   - Browse through file directories.
   - Recover deleted files.
   - View file metadata (creation, modification, and access time).
5. **Keyword Search & Evidence Discovery:**
   Investigators use keywords like *"password", "secret", "bitcoin", "account"* to locate sensitive data.
   In the experiment, searching the word "million" helped locate the related file.
6. **Generating Reports:**
   Autopsy creates ASCII, HTML, hash lists, and event reports that can be used in court.

Applications in Real Cybercrime Cases

Crime Type	How Autopsy Helps
Financial Fraud	Recovers deleted spreadsheets, transaction data, emails.
Cyberbullying & Harassment	Extracts chat logs, social media history, browser searches.
Intellectual Property Theft	Finds copied files, USB usage logs, timestamps.
Terrorism & Organized Crime	Recovers communication logs, plans, encrypted data.
Child Exploitation Cases	Locates illegal media files and performs hash matching with known criminal databases.

Advantages of Using Sleuth Kit Autopsy

- Free and open-source
- Court-admissible forensic reports
- Cross-platform (Windows, Linux, MacOS)
- Supports multiple file systems and disk formats
- User-friendly with powerful backend capability

Challenges in Using Autopsy

Challenge	Description
Requires Technical Knowledge	Investigators must understand file systems and digital evidence handling.
Large Data Handling	Analyzing terabytes of data can be time-consuming.
Encrypted Drives	Cannot access locked or heavily encrypted files without keys.
Proper Chain of Custody	Evidence must be collected legally to be admissible in court.

Future of Forensics with Autopsy and AI

- AI-assisted file classification (detecting illegal images, documents)
- Integration with cloud storage forensics (Google Drive, OneDrive)
- Automated report generation and suspect behavior prediction
- Mobile forensics module for Android/iOS devices
- Blockchain-based evidence tracking for better chain-of-custody

Conclusion

Sleuth Kit Autopsy is a powerful tool in the field of digital forensics and is widely used in cybercrime investigation agencies worldwide. It helps investigators recover deleted files, analyze disk images, extract browser histories, perform keyword searches, and finally generate evidence-based reports. As per the experiment PDF, learning this tool builds a strong foundation for students and professionals in cybercrime investigation.

By combining Autopsy with proper forensic methodologies and legal procedures, digital evidence can be accurately retrieved, preserved, and presented in court — helping bring cybercriminals to justice.