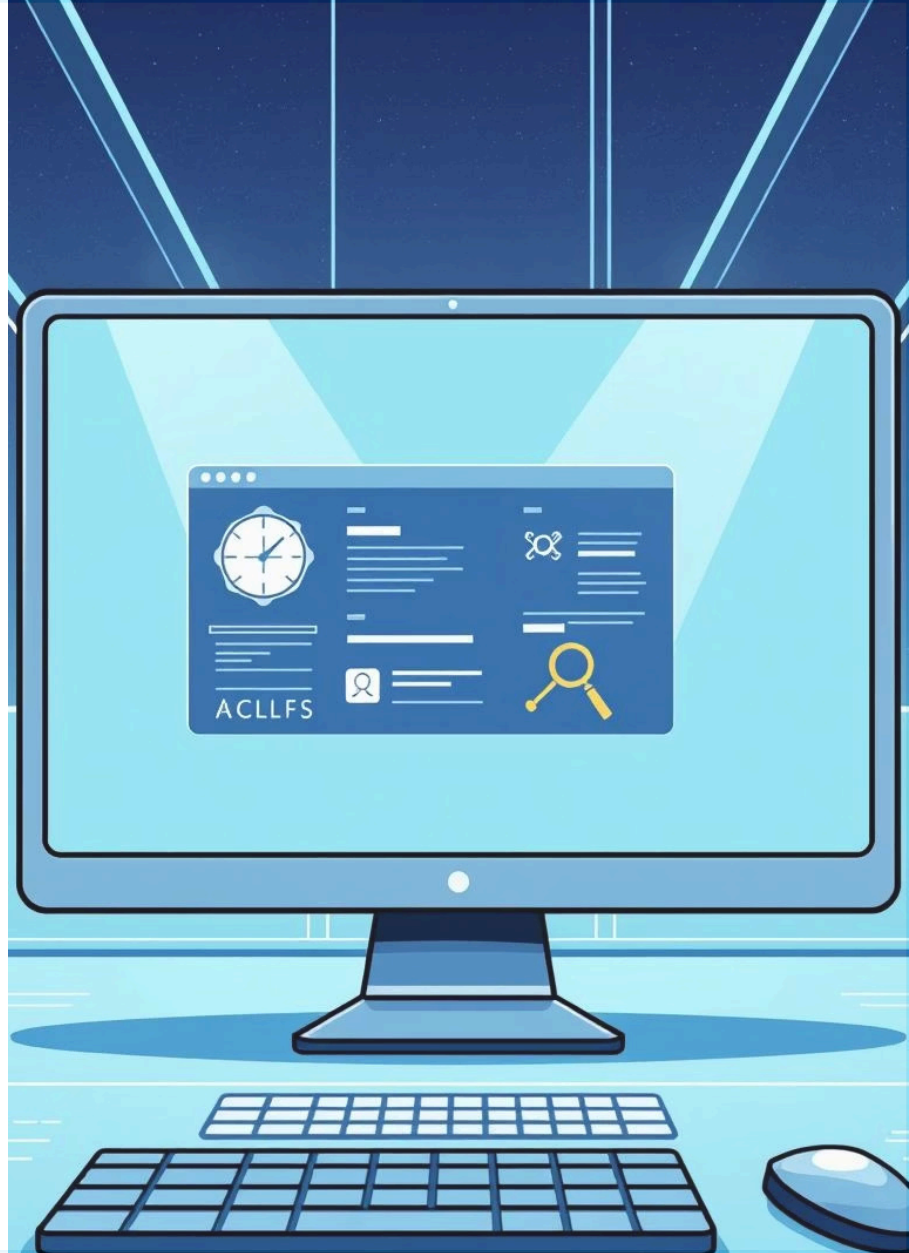
Familiarizing Autopsy for Windows – A Free Forensics Tool

Presented by: Akhil K Babu



What is Autopsy?

Free & Open-Source

A robust digital forensics platform with no licensing costs.

GUI for Sleuth Kit

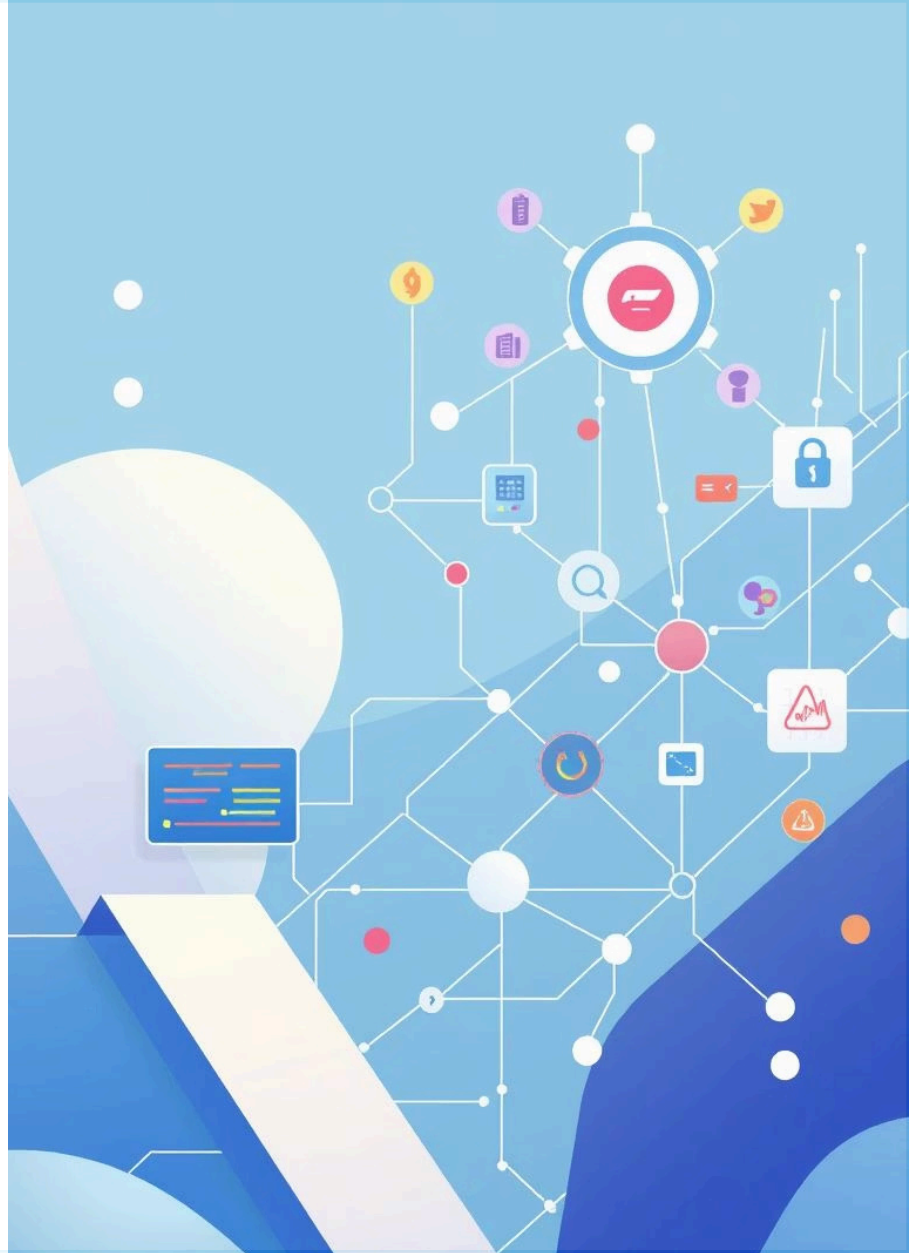
Provides a user-friendly graphical interface for the powerful command-line tools of The Sleuth Kit.

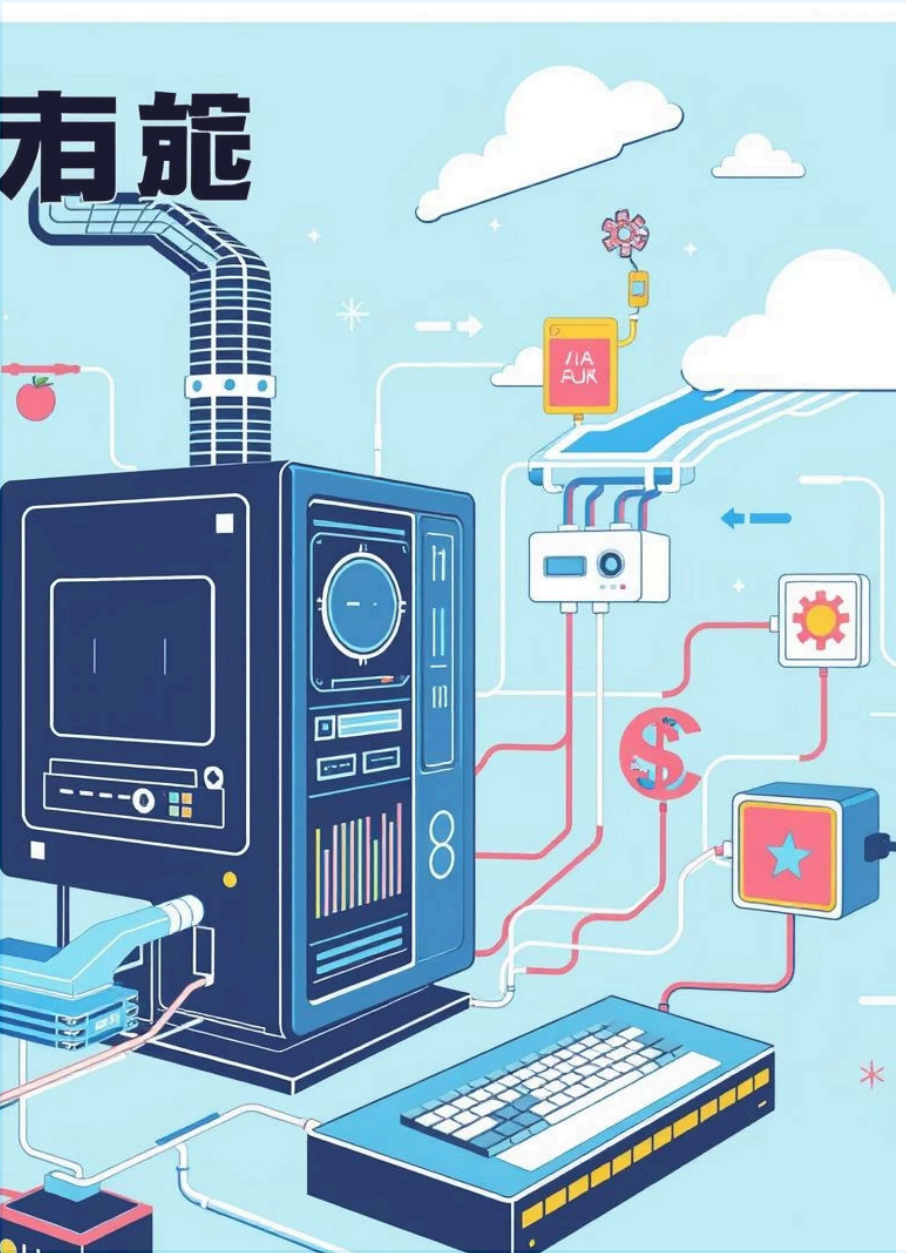
Versatile Analysis

Capable of disk image analysis, file recovery, keyword searching, and more.

Widely Utilized

A trusted tool for law enforcement, government agencies, and private forensic analysts globally.





Installation & Requirements

Operating System

Compatible with Windows 7, 10, and 11.

Download Source

Obtain the official installer from autopsy.com.

Memory (RAM)

4GB minimum; 8GB+ recommended for optimal performance with larger cases.

Installation Process

A straightforward, guided installation similar to standard Windows applications.

Java Runtime

A suitable Java Development Kit (JDK) is bundled within the installer.

Disk Space

Ensure ample disk space for case files and extracted data.

Using Autopsy – Key Steps

Create a Case

Define a new case with a unique name and examiner details. This organizes all your forensic data.

Add Data Source

Integrate raw disk images (E01, DD), logical drives, or individual files for analysis.

Analyze Data

Perform deep dives into file systems, web artifacts, registry entries, and create detailed timelines.

Generate Report

Compile findings into comprehensive HTML or CSV reports for legal and technical presentation.

Core Features

Timeline Analysis

Visualize events chronologically to reconstruct user activity and system interactions.

Keyword & Hash Filtering

Efficiently search for specific terms and identify known malicious files using hash sets.

Deleted File Recovery

Undelete and examine files marked for deletion, often revealing critical evidence.

Web & Registry Analysis

Extract browser history, cookies, email artifacts, and crucial Windows Registry data.

Report Generation

Create professional, customizable reports suitable for legal proceedings and investigative summaries.

Autopsy: Advantages & Limitations

Advantages

Cost-Effective

Being free and open-source makes it accessible for all users, regardless of budget.

User-Friendly Interface

The intuitive GUI lowers the barrier to entry for new forensic analysts and students.

Educational Value

Excellent for training and academic environments due to its comprehensive features and accessibility.

Limitations

Limited Mobile Support

Primary focus on disk image analysis; less robust for direct mobile device forensics.

Performance on Large Cases

Can be slower when processing extremely large disk images or numerous data sources.

Plugin Dependency

Advanced functionalities sometimes require additional plugins, extending setup time.

Conclusion

Autopsy stands as a **powerful and free digital forensics tool**.

It is **ideal for academic learning** and basic to intermediate investigations.

A **must-know tool** for anyone pursuing a career in Cyber Forensics.