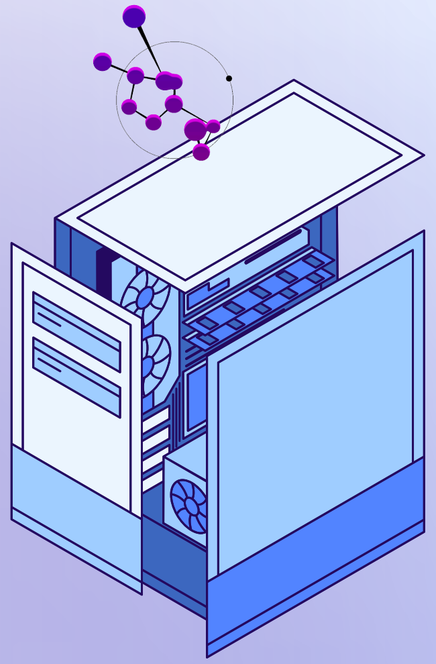
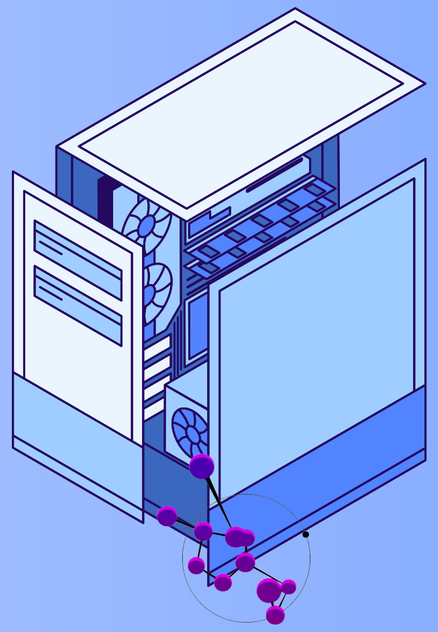
LINUX ARTIFACT ANALYSIS

INTRODUCTION



Artifact analysis on a Linux system involves examining traces left behind by users, applications, or attackers. It is a crucial step in cybersecurity, digital forensics, and incident response.



WHAT IS AN ARTIFACT ?

Artifact is any data created or modified through interaction with the system.

Examples:

- Log files
- Command history
- Modified system files
- Active processes or network connections

CATEGORIES OF

ARTIFACTS

User Account Artefacts

User Account Files

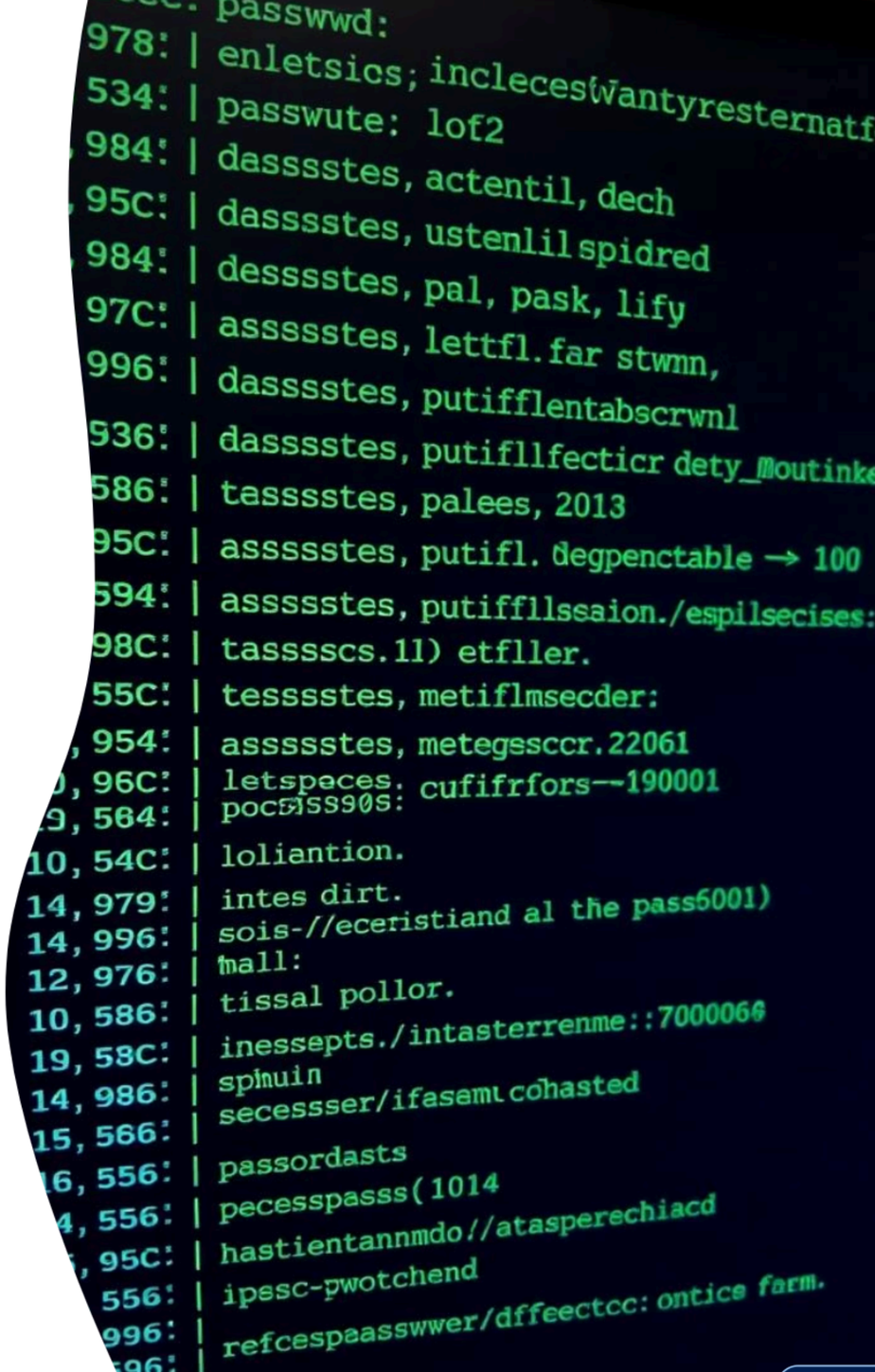
/etc/passwd and /etc/shadow store user and password hashes.

Login History

Commands like last analyze login/logout events from wtmp and btmp logs.

Suspicious Activity

Checking anomalies in login patterns reveals compromised accounts.



Command History Artefacts

1 History Files

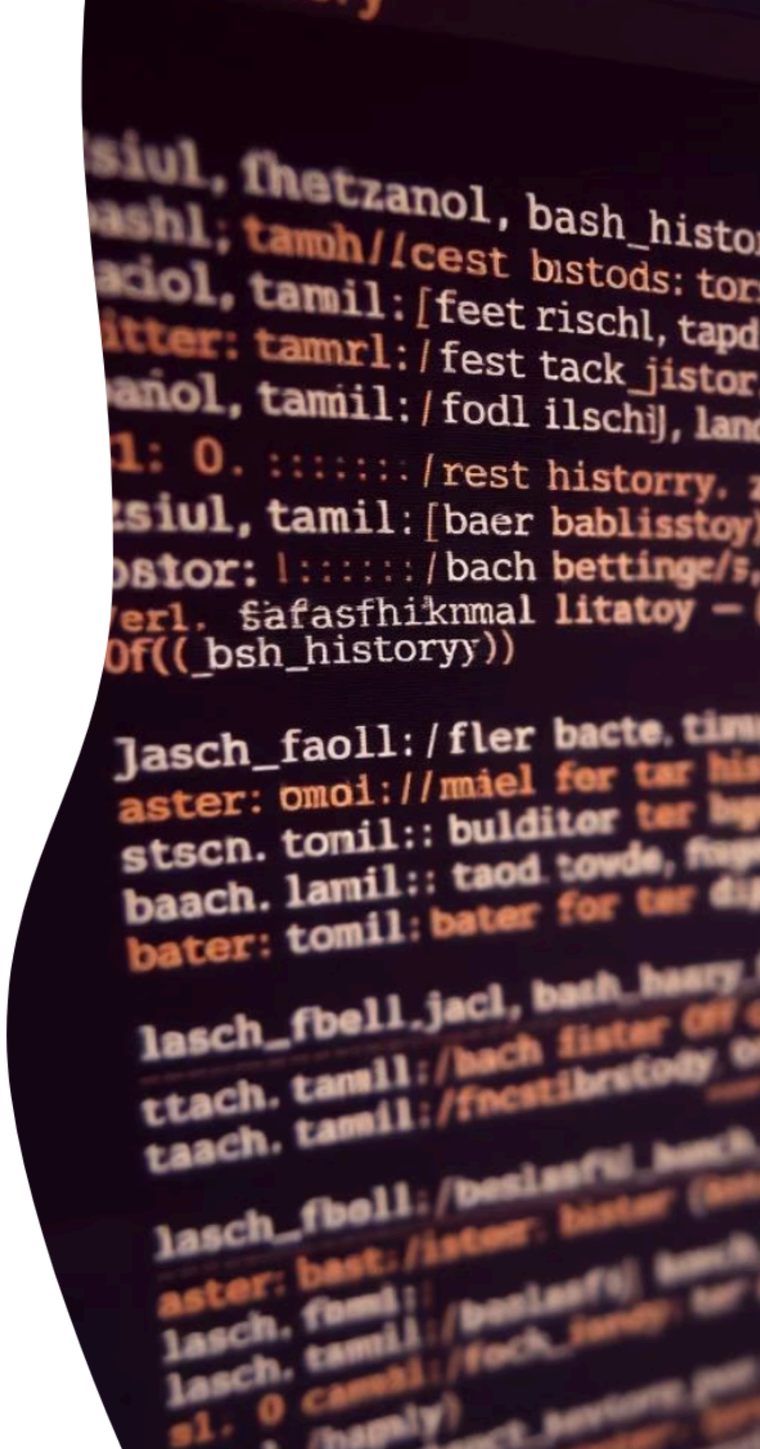
.bash_history and .zsh_history log user commands for auditing.

2 Suspicious Commands

Reviewing history reveals commands that may indicate malicious intent.

3 Recovery Techniques

Deleted histories can sometimes be restored from shell memory buffers.



File System Artefacts

Timestamps

Modification, access, and change times track file activity.

Deleted Files

Tools like extundelete help recover deleted data effectively.

Metadata Analysis

Examining metadata exposes unusual or tampered file behaviours.

Log File Artefacts

System Logs

/var/log/syslog, auth.log, and kern.log monitor system activity and security.

Application Logs

Logs from Apache, Nginx, and MySQL help trace web and database events.

Intrusion Analysis

Reviewing logs uncovers abnormal behaviours and intrusion evidence.

Network Artefacts

Network Config

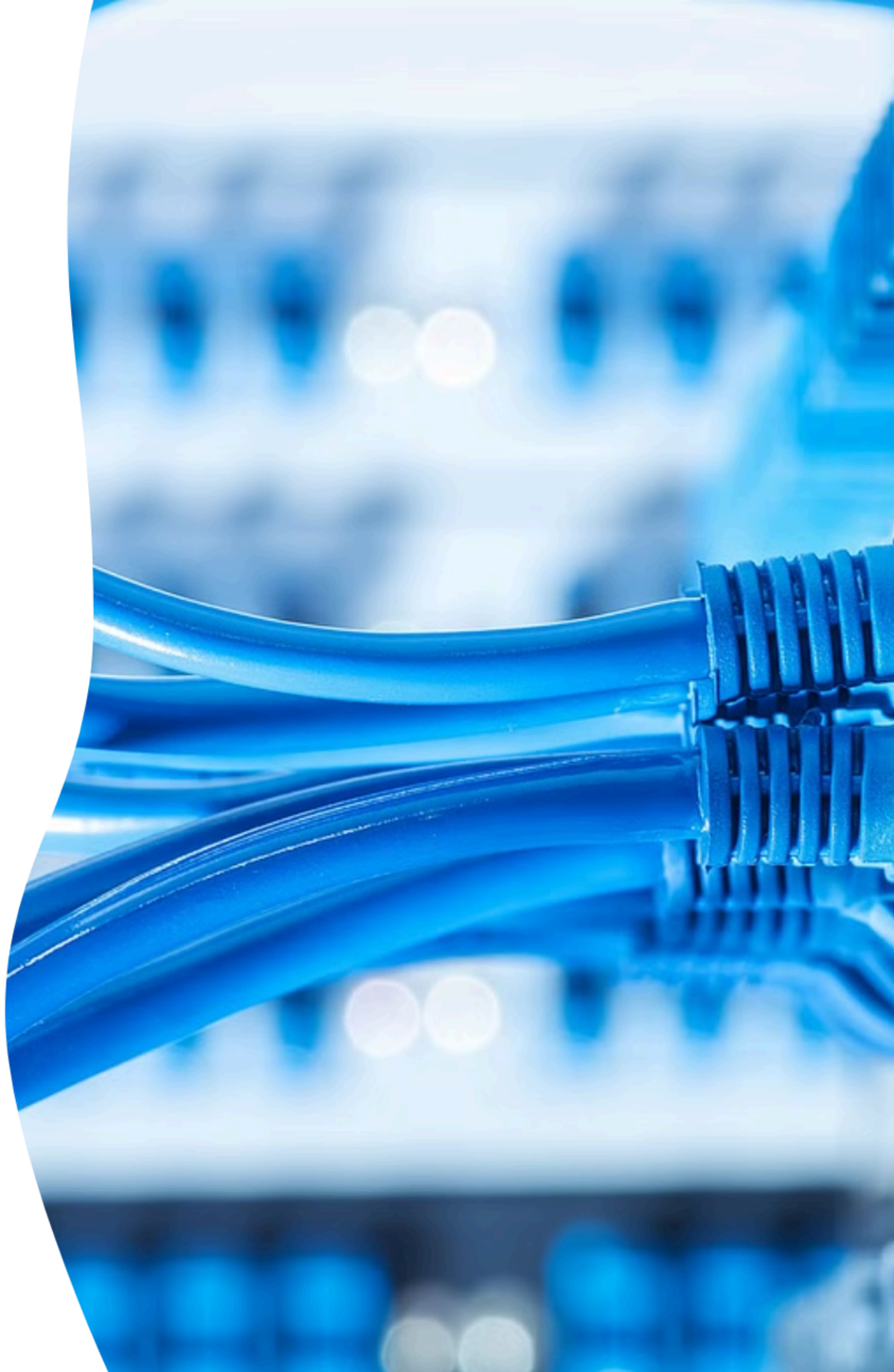
/etc/network/interfaces and /etc/resolv.conf define network settings.

Active Connections

Tools like netstat, ss, and tcpdump reveal current network traffic.

Malicious Traffic

Analysing connections helps identify suspicious or unauthorised activity.



Tools for Artefact Analysis

Autopsy

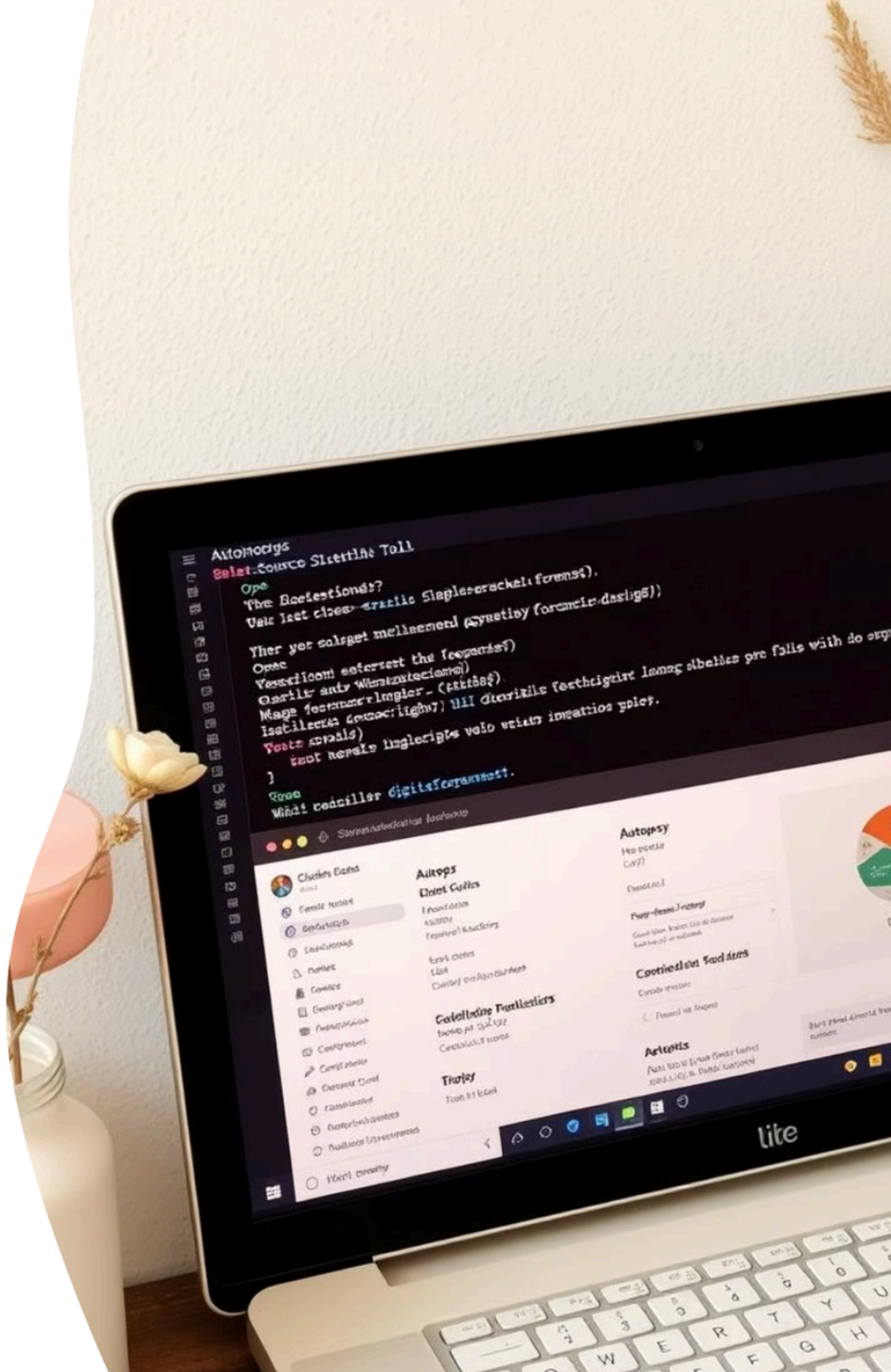
User-friendly open-source platform for digital forensic investigations.

The Sleuth Kit

Command-line tools for in-depth file system and artefact analysis.

Log Analysis

Unix tools grep, awk, and sed assist in parsing and filtering logs.



THANK YOU!