



NAME: Adithya Baragi S

INTRODUCTION TO DIGITAL FORENSICS

Digital forensics is the process of identifying, preserving, analyzing, and presenting digital evidence in a way that is legally acceptable. The core principles include:

- Integrity – evidence must not be modified
- Authenticity – evidence must be original and verifiable
- Repeatability – procedures should be replicable
- Legality – must comply with legal standards and warrants

Types of Digital Evidence

Digital evidence exists in various forms:

- **Volatile Data**
 - Stored in RAM, cache, or active network sessions
 - Lost when power is removed
- **Non-Volatile Data**
 - Hard disks, SSDs, USBs, mobile phones
- **Remote/Cloud Evidence**
 - Emails, messages, social media, IoT logs, SaaS accounts

Basic Investigation Process

A standard digital forensic investigation includes:

1. Identification – Locating sources of potential evidence
2. Preservation – Write blockers, disk imaging
3. Analysis – File carving, keyword search, timeline creation
4. Documentation – Screenshots, notes, tool logs
5. Presentation – Forensic report for legal or management review

Evidence Handling

Best practices include:

- Write Blockers – Prevent accidental modification
- Hashing – MD5, SHA-1, SHA-256 for integrity verification
- Secure Storage – Anti-static bags, locked containers, access logs

Documentation Methods

Proper documentation includes:

- Timestamps
- Tools used (version, commands)
- Observations and screenshots
- Case identifiers

Tool Introduction

Common digital forensics tools:

- **FTK Imager** – Disk imaging



- **Autopsy/The Sleuth Kit** – Disk analysis
- **Wireshark** – Network traffic capture
- **RegRipper** – Windows Registry analysis

DIGITAL FORENSICS — COMPLETE MOCK PRACTICAL ASSIGNMENT

Task 1: Create a Forensic Image of a E:Drive Using FTK Imager

Explain the steps to create a forensic image using FTK Imager and record the hash values.

Steps:

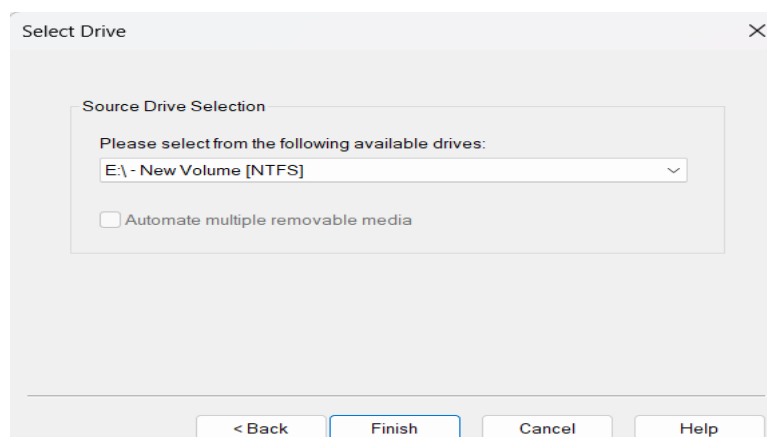
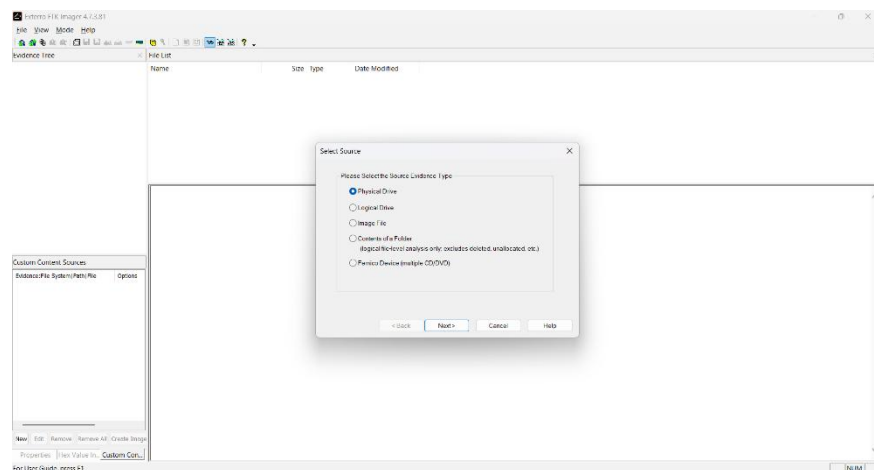
1. Open FTK Imager → File → Create Disk Image
2. Choose Physical Drive → Select the USB
3. Select Output Format: E01
4. Enter Evidence Details (Case #, Examiner Name)
5. Choose storage location
6. Enable MD5 and SHA-256 hash generation
7. Start imaging

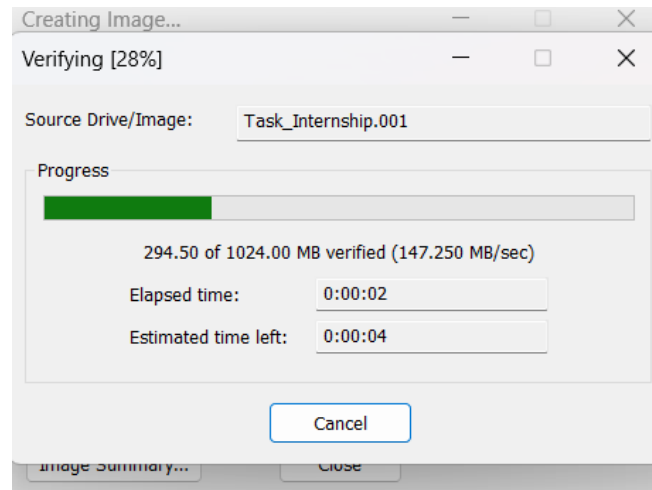
Recorded Hash Values:

- MD5: 3f5a1c1ab64d1c90888b923fa20d884e
- SHA-256: af92b1c8961d884dbc154e0ca80deb01454bc1dbd9458f771e7d5c6e4e301a25

Conclusion:

Image successfully created with verified integrity.





Task 2: Verify Image Integrity

Why is hashing important and how do you verify the integrity of the image?

Importance:

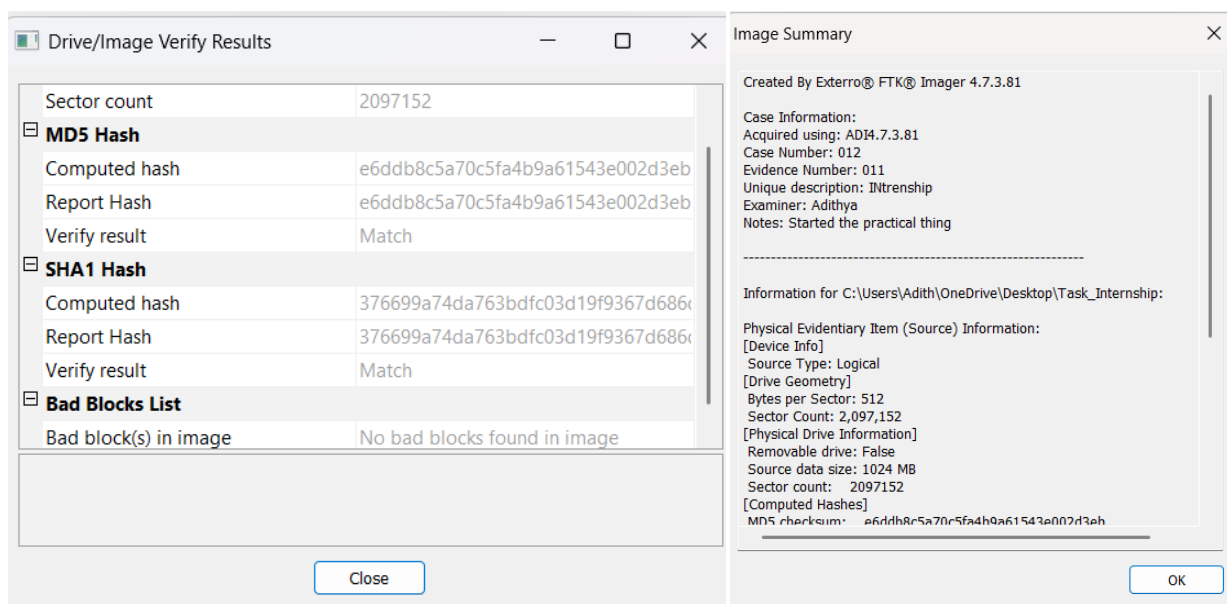
- Ensures the evidence was not altered
- Proves authenticity in court
- Maintains the chain of custody

Verification Steps:

1. Open FTK Imager → File → Verify Image
2. Load suspect_usb.E01
3. FTK recalculates MD5/SHA-256
4. Compare with imaging time hashes

Result:

Hashes matched → Evidence integrity maintained.





Task 3: Analyze the Disk Image Using Autopsy

Identify deleted files, hidden folders, and any suspicious activity.

After loading suspect_usb.E01 into Autopsy:

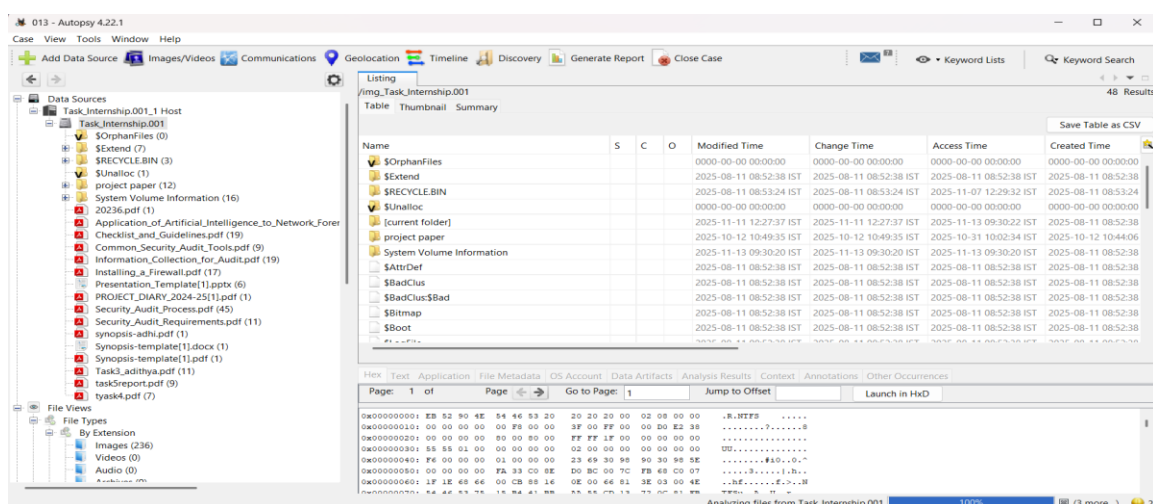
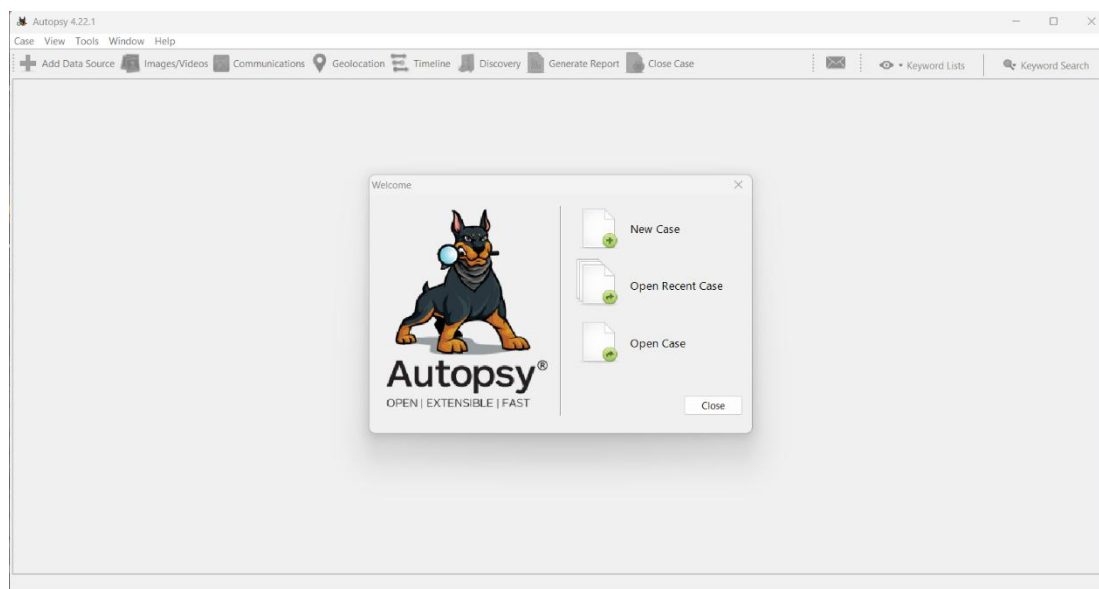
Findings:

1. Deleted Files Recovered

File Name	Status	Description
client_data.xlsx	Deleted	Confidential client file
keylogger.exe	Deleted	Malicious executable

Recovered using:

Data Artifacts → Deleted Files → Recover





2. Hidden Folder Detected

- Folder Name: .secret_docs
- Found under: /USBDrive/.secret_docs/
- Contained:
 - trade_secrets.txt
 - project_confidential.pdf

3. Timeline Analysis

Time range shows:

- USB inserted at: 2025-02-18 10:42:33
- Suspicious deletions at: 2025-02-18 10:46:10

REPORTLINK:

<file:///D:/013/Reports/013%20HTML%20Report%2011-13-2025-10-00-00/report.html>

Report Navigation

- Case Summary
- Keyword Hits (46)
- Metadata (23)
- Recycle Bin (1)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- Web Downloads (14)

Autopsy Forensic Report

HTML Report Generated on 2025/11/13 10:00:00

Case:	013
Case Number:	012
Number of data sources in case:	1
Notes:	ksmckoks
Examiner:	Adithya

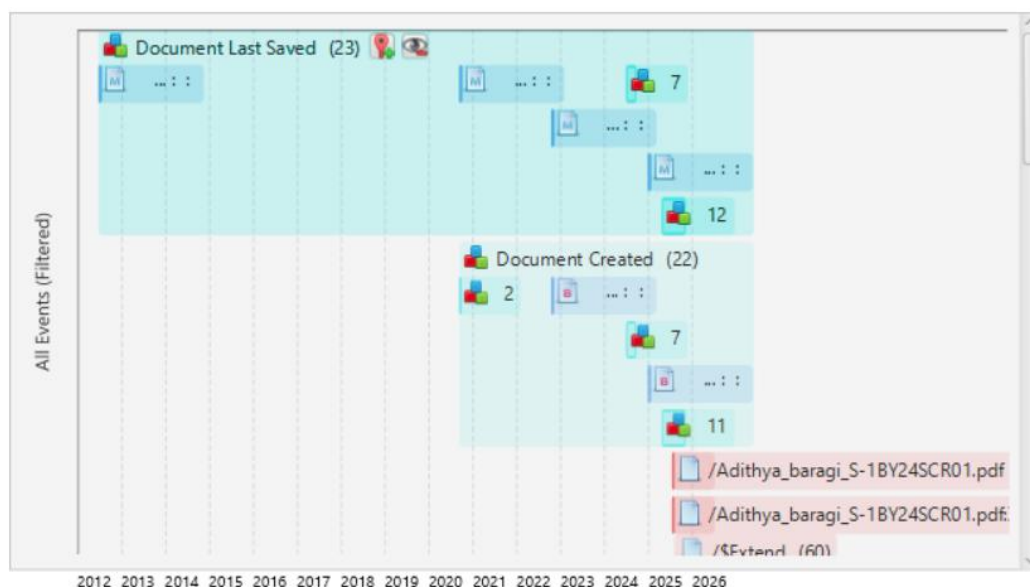
Image Information:

Task_Internship.001

Timezone: Asia/Calcutta
Path: C:\Users\Adith\OneDrive\Desktop\Task_Internship.001

Software Information:

Autopsy Version:	4.22.1
Android Analyzer Module:	4.22.1
Android Analyzer (aLEAPP) Module:	4.22.1
Central Repository Module:	4.22.1
DJI Drone Analyzer Module:	4.22.1
Data Source Integrity Module:	4.22.1





Task 5: Extract Registry Artifacts Using RegRipper

Analyze the NTUSER.DAT hive and extract user activity.

Command:

Regripper -r NTUSER.DAT -f ntuser

```
(kali@kali:~)$ regripper -r NTUSER.DAT -f ntuser
Parsed Plugins file.
Error in adoberdr: Can't locate /usr/lib/regripper/plugins/adoberdr.pl at /usr/bin/regripper line 193.
adoberdr complete.

Launching allowedenum v.20200511
allowedenum v.20200511
(NTUSER.DAT, Software) Extracts AllowedEnumeration values to determine hidden special folders
Error in allowedenum: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/allowedenum.pl line 53.
allowedenum complete.

Launching appassoc v.20200515
appassoc v.20200515
(NTUSER.DAT, Software) Gets contents of user's ApplicationAssociationToasts key
Error in appassoc: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/appassoc.pl line 41.
appassoc complete.

Launching appcompatflags v.20200525
appcompatflags v.20200525
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.
Error in appcompatflags: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/appcompatflags.pl line 66.
appcompatflags complete.

Launching appkeys v.20200517
appkeys v.20200517
(NTUSER.DAT, Software) Extracts AppKeys entries.
Error in appkeys: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/appkeys.pl line 45.
appkeys complete.

Launching applets v.20200525
applets v.20200525
(NTUSER.DAT) Gets contents of user's Applets key
Error in applets: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/applets.pl line 45.
applets complete.

Launching apppaths v.20200511
apppaths v.20200511
(NTUSER.DAT, Software) Gets content of App Paths subkeys
Error in apppaths: Unable to open 'NTUSER.DAT': No such file or directory at /usr/lib/regripper/plugins/apppaths.pl line 53.
```

Task 6: Chain of Custody Documentation

Prepare a chain-of-custody entry for the USB drive.

Field	Entry
Evidence ID	DF-USB-2025-001
Evidence Type	USB Drive (16GB)
Collected By	Adithya B
Date/Time	18 Feb 2025, 11:15 AM
Location	Cybercrime Lab 2
Hash (SHA-256)	af92b1c8961...6e4e301a25
Transferred To	Lead Examiner
Purpose	Disk imaging & analysis
Remarks	Sealed in anti-static bag