

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:

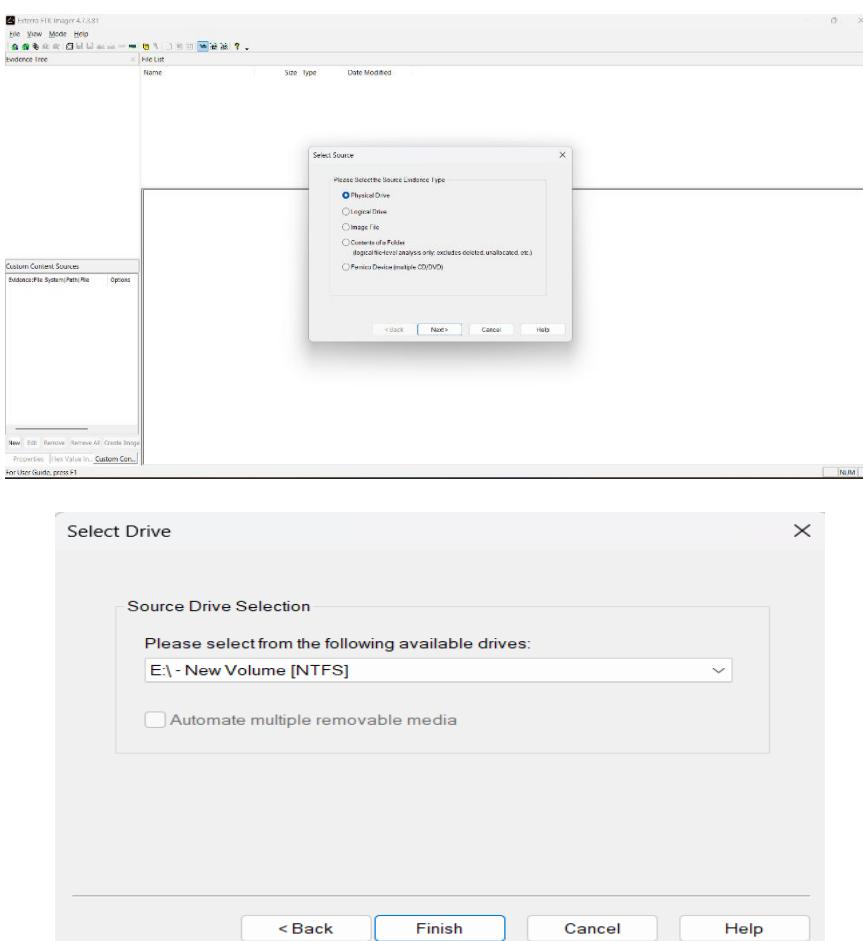
1. Open FTK Imager → File → Create Disk Image
2. Choose Physical Drive → Select the USB
3. Select Output Format: E01
4. Enter Evidence Details (Case #, Examiner Name)
5. Choose storage location
6. Enable MD5 and SHA-256 hash generation
7. Start imaging

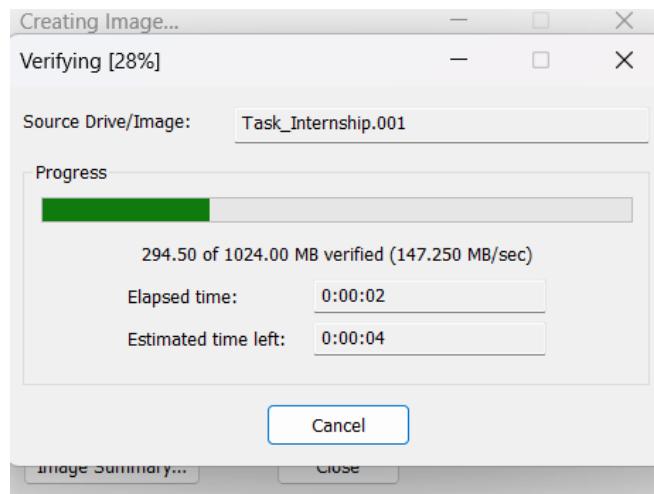
Recorded Hash Values:

- 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:

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

Result:

Hashes matched → Evidence integrity maintained.

The screenshot displays two windows from FTK Imager. The left window, titled 'Drive/Image Verify Results', contains a table of verification results:

Sector count		2097152
MD5 Hash		
Computed hash	Report Hash	e6ddb8c5a70c5fa4b9a61543e002d3eb
Verify result		Match
SHA1 Hash		
Computed hash	Report Hash	376699a74da763bd03d19f9367d686c
Verify result		Match
Bad Blocks List		
Bad block(s) in image		No bad blocks found in image

The right window, titled 'Image Summary', provides detailed case information and physical evidence details:

Created By: Exterro® FTK® Imager 4.7.3.81
Case Information:
Acquired using: AD4.7.3.81
Case Number: 012
Evidence Number: 011
Unique description: INTrenship
Examiner: Adithya
Notes: Started the practical thing

Information for C:\Users\Adith\OneDrive\Desktop\Task_Internship:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 2,097,152
[Physical Drive Information]
Removable drive: False
Source data size: 1024 MB
Sector count: 2097152
[Computed Hashes]
MD5 checksum: e6ddb8c5a70c5fa4b9a61543e002d3eb

**Task 3: Analyze the Disk Image Using Autopsy**

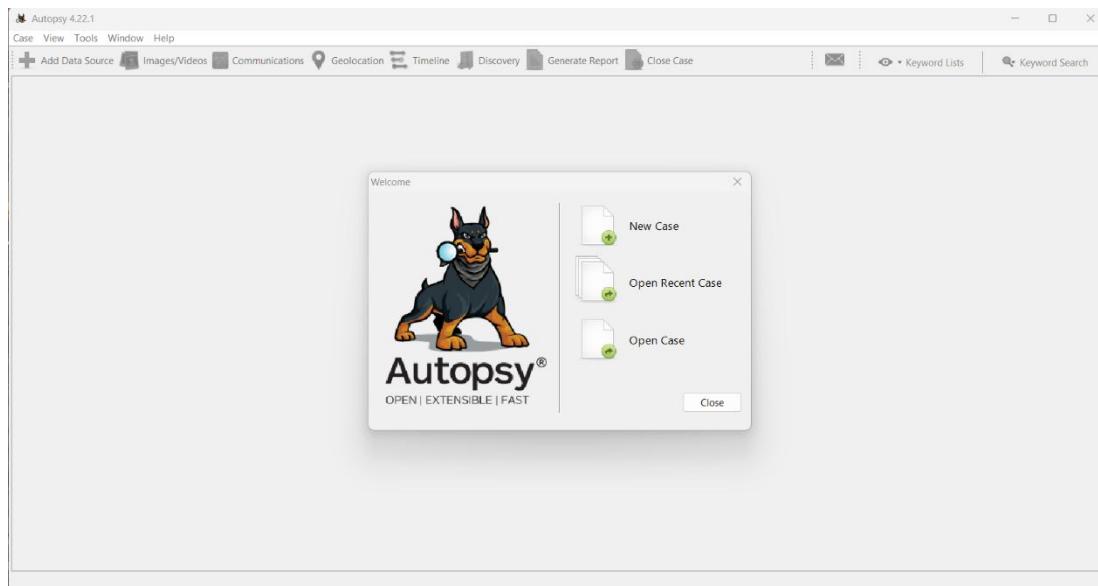
Identify deleted files, hidden folders, and any suspicious activity.

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

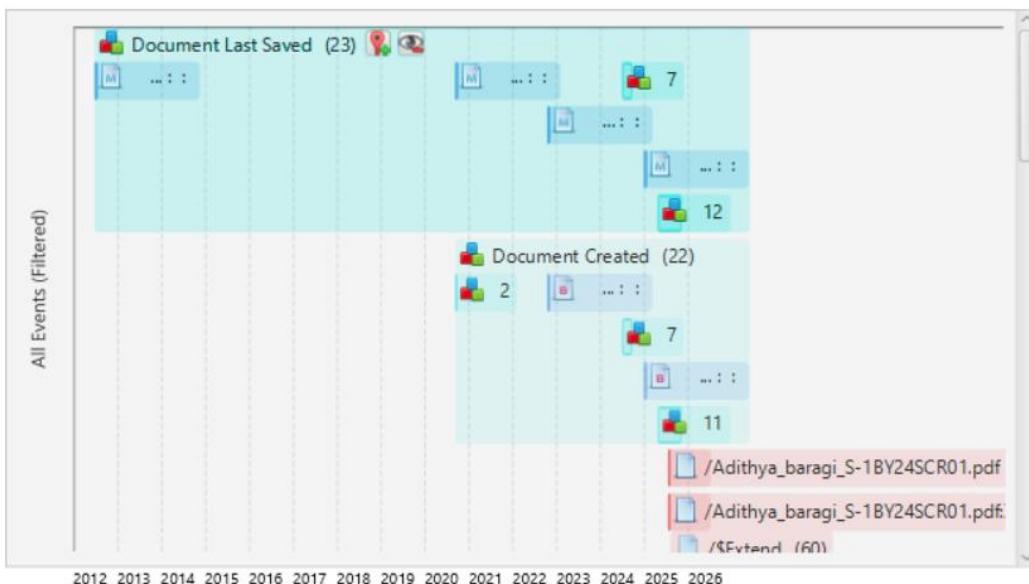
Case: 013
Case Number: 012
Number of data sources in case: 1
Notes: ksmckoks
Examiner: Adithya

Image Information:

Task_Internship.001
Timezone: Asia/Calcutta
Path: C:\Users\Adithya\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 4: Wireshark Analysis

Examine the network_traffic.pcap file and identify suspicious network activity.

Filters used:

- http
- tcp.port == 80
- ftp
- dns

Suspicious Findings:

1. HTTP Data Exfiltration

Detected an HTTP POST request to an unknown IP:

- Destination: 185.212.44.91
- URI: /upload.php
- Packet shows file upload data.

No.	Time	Source	Destination	Protocol	Length	Info
458 9. 243327743	192.168.1.111	34.197.221.82	192.168.1.111	HTTP	374	GET /404error.htm HTTP/1.1
471 9. 305017860	34.197.221.82	192.168.1.111	192.168.1.111	HTTP	282	HTTP/1.1.200 OK (text/plain)
2567 19. 769898289	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	355	GET / HTTP/1.1
2571 20. 028900180	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2625	HTTP/1.1.200 OK (text/html)
2600 21. 422306364	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	40	HTTP/1.1.200 OK (text/html)
2602 23. 496444078	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2825	HTTP/1.1.200 OK (text/html)
2604 23. 629314579	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	374	GET /style.css HTTP/1.1
2606 23. 913896715	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2892	HTTP/1.1.200 OK (text/css)
2607 23. 913896715	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	29	HTTP/1.1.200 OK (text/html)
2617 24. 178483683	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	434	GET /images/logo.gif HTTP/1.1
2620 24. 382885336	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	966	HTTP/1.1.200 OK (image/x-icon)
2632 24. 455651299	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	1814	HTTP/1.1.200 OK (GIF89a)
2633 24. 455651299	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	29	HTTP/1.1.200 OK (text/html)
2679 33. 011159798	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2825	HTTP/1.1.200 OK (text/html)
2848 49. 441323940	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	466	GET /categories.php HTTP/1.1
2848 49. 697925696	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2813	HTTP/1.1.200 OK (text/html)
2852 49. 697925696	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	694	POST /aristos.php HTTP/1.1
2856 49. 576805493	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2870	HTTP/1.1.200 OK (text/html)
2856 49. 717993277	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	462	GET /cart.php HTTP/1.1
2857 49. 761799066	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	2925	HTTP/1.1.200 OK (text/html)
2859 49. 685983798	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	466	GET /login.php HTTP/1.1
2860 49. 685983798	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	281	HTTP/1.1.200 OK (text/html)
2869 54. 685983646	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	598	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2871 54. 6859842636	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	76	HTTP/1.1.200 OK (text/html)
2967 75. 538117389	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	694	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2984 75. 576805493	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	407	HTTP/1.1.200 OK (text/html)
2914 77. 974248311	192.168.1.111	44.228.249.3	192.168.1.111	HTTP	694	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2919 77. 342360686	44.228.249.3	192.168.1.111	192.168.1.111	HTTP	86	HTTP/1.1.200 OK (text/html)

No.	Time	Source	Destination	Protocol	Length	Info
426 9. 246138571	192.168.1.111	34.197.221.82	192.168.1.111	TCP	74	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=184868228 TSecr=184468228 WS=1024
459 9. 266939269	34.197.221.82	192.168.1.111	192.168.1.111	TCP	74	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=184868228 TSecr=184468228 WS=256
457 9. 269598352	192.168.1.111	34.197.221.82	192.168.1.111	TCP	66	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=184868251 TSecr=2865275528
478 9. 385917728	34.197.221.82	192.168.1.111	192.168.1.111	TCP	74	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2865275564 TSecr=184468265
471 9. 385918789	34.197.221.82	192.168.1.111	192.168.1.111	HTTP	282	HTTP/1.1.200 OK (text/plain)
471 9. 385918789	34.197.221.82	192.168.1.111	192.168.1.111	TCP	66	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=184468265 TSecr=2865275564
2569 19. 494158252	192.168.1.111	44.228.249.3	192.168.1.111	TCP	74	SYN=32 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933318690 TSecr=9 WS=1024
2570 19. 494158252	192.168.1.111	44.228.249.3	192.168.1.111	TCP	69	HTTP/1.1.Keep-Alive ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933318690 TSecr=9 WS=1024
2562 19. 5376741946	34.197.221.82	192.168.1.111	192.168.1.111	TCP	66	(TCP) Keep-Alive ACK=80 - 59932 [ACK] Seq=217 Ack=311 Win=288898 Len=9 Tsvl=2865285886 TSecr=184468288
2564 19. 744636132	192.168.1.111	44.228.249.3	192.168.1.111	TCP	74	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=293331859 TSecr=9 WS=1024
2566 19. 769498981	34.197.221.82	192.168.1.111	192.168.1.111	TCP	74	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=293331859 TSecr=9 WS=1024
2567 19. 769498981	192.168.1.111	44.228.249.3	192.168.1.111	TCP	69	HTTP/1.1.200 OK (text/html)
2568 20. 091275198	44.228.249.3	192.168.1.111	192.168.1.111	TCP	74	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933318859 TSecr=9 WS=128
2601 20. 091275198	44.228.249.3	192.168.1.111	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933318859 TSecr=9 WS=128
2572 20. 928124897	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933318142 TSecr=32465239877
2597 22. 977983446	192.168.1.111	44.228.249.3	192.168.1.111	TCP	74	SYN=35 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933322099 TSecr=9 WS=1024
2598 23. 227964466	44.228.249.3	192.168.1.111	192.168.1.111	TCP	74	SYN=35 ACK=192.168.1.111:443 Win=1468 SACK_PERM TSval=2933322099 TSecr=9 WS=128
2600 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	69	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	405	GET / HTTP/1.1
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	405	POST / HTTP/1.1
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	405	PUT / HTTP/1.1
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	405	DELETE / HTTP/1.1
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	405	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	HTTP/1.1.200 OK (text/html)
2601 23. 228346364	192.168.1.111	44.228.249.3	192.168.1.111	TCP	66	SYN=34 ACK=192.168.1.111:443 Win=1468 SACK_Perm TSval=2933322099 TSecr=9 WS=128
2601 23. 228346364	192.168.1.111	44.228.249.3	19			

Task 5: Extract Registry Artifacts Using RegRipper

Analyze the NTUSER.DAT hive and extract user activity.

Command:

Regripper -r NTUSER.DAT -f ntuser

```
[kali㉿box]:~/Desktop$ 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
- 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