

EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028

Aim: To study the fundamentals of computer forensics and explore various forensic tools used for digital investigations.

Tools:

- Autopsy (open-source forensic analysis tool)
- FTK Imager (forensic imaging)
- Wireshark (network analysis)
- Volatility (memory forensics)

Algorithm (High-level):

1. Identify the different categories of forensic tools.
2. Install and set up the chosen forensic tools on lab systems.
3. Perform a sample operation with each tool:
 - Imaging a drive with FTK Imager.
 - Analyzing deleted files and metadata in Autopsy.
 - Capturing packets with Wireshark.
 - Analyzing RAM dump with Volatility.
4. Document the findings with screenshots and observations.

Procedure:

1. Create a lab case folder /CaseID/ForensicTools/.
2. Launch **FTK Imager** → acquire an image of a removable drive → save hash log.
3. Open **Autopsy** → create a new case → add the acquired image → run ingest modules.

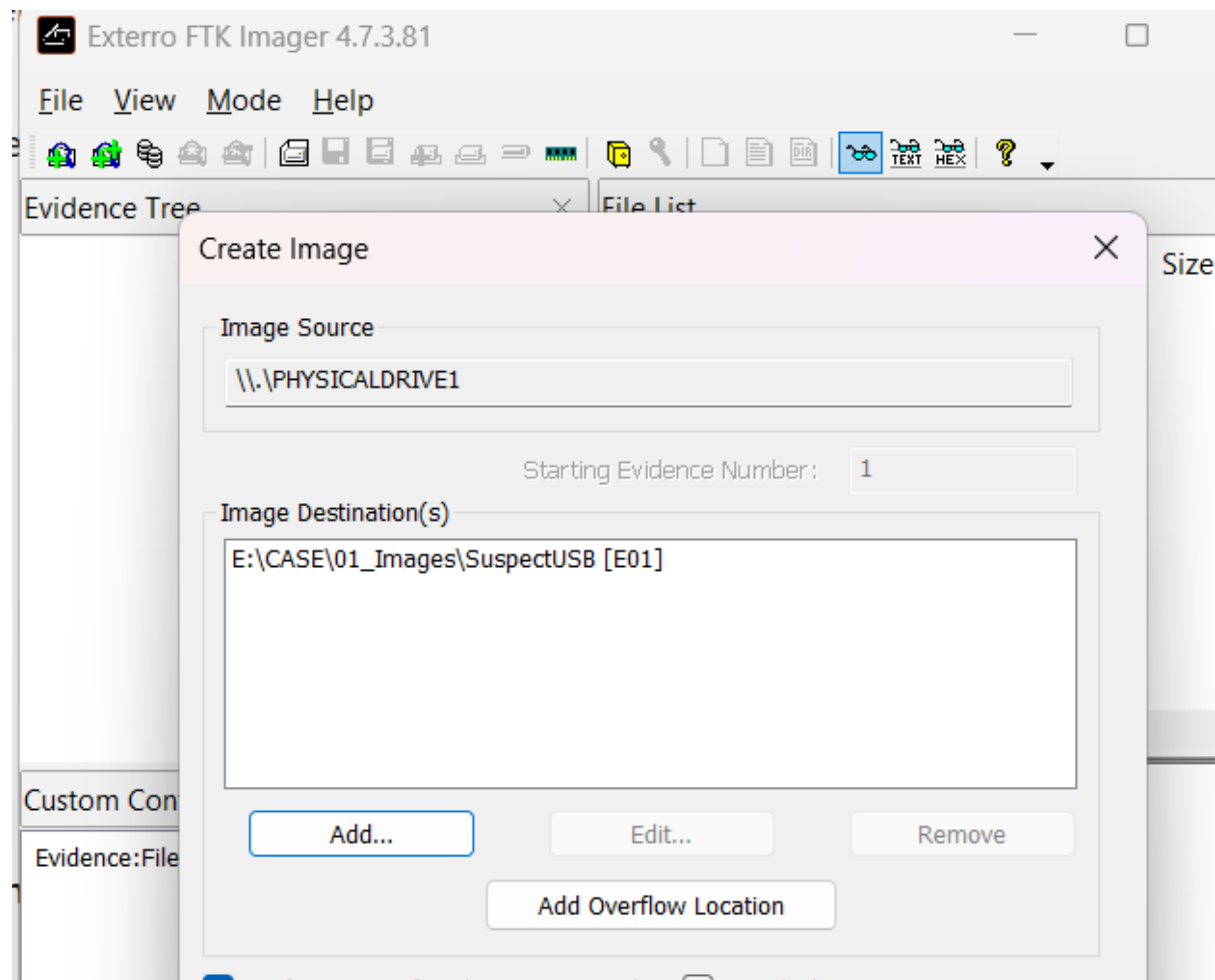
EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028

4. Install and open **Wireshark** → capture live traffic for 2–3 minutes → apply filters for http or dns.
5. Open **Volatility** → run pslist on a sample memory image → export process list.
6. Record observations: screenshots of tool dashboards, outputs, and key findings.

Output:



EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028

Drive/Image Verify Results	
Name	SuspectUSB.E01
Sector count	30310400
MD5 Hash	
Computed hash	ffb14460cb956ca7baaff919eeb91c768
Stored verification hash	ffb14460cb956ca7baaff919eeb91c768
Report Hash	ffb14460cb956ca7baaff919eeb91c768
Verify result	Match
SHA1 Hash	
Computed hash	d2ae8a36bfc192e4f24c121987ef9b136a647dba7
Stored verification hash	d2ae8a36bfc192e4f24c121987ef9b136a647dba7
Report Hash	d2ae8a36bfc192e4f24c121987ef9b136a647dba7
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Bitlocker Password (optional):

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028

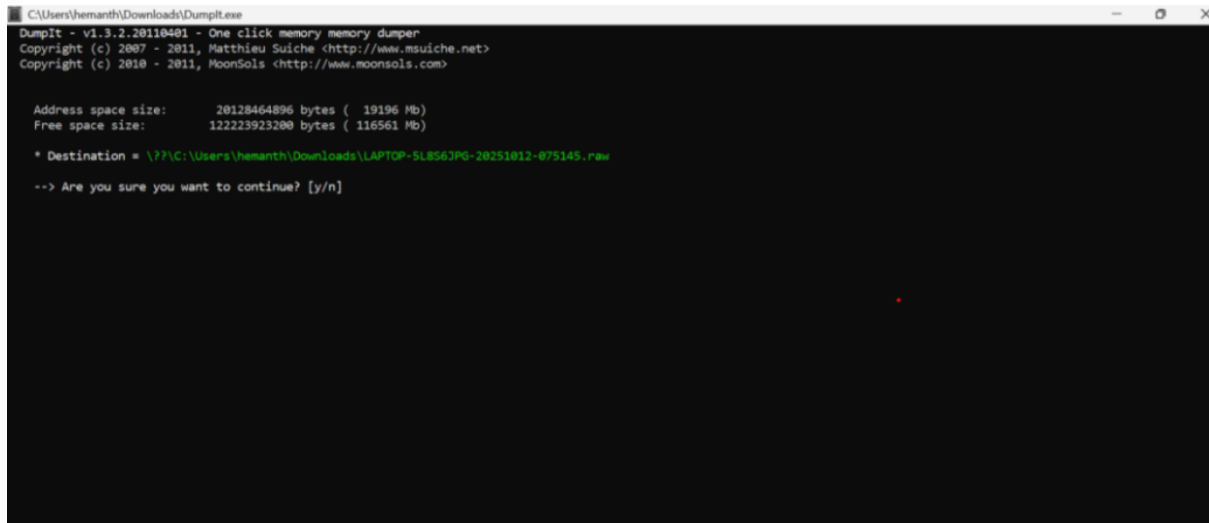
The screenshot displays the Autopsy 4.22.1 interface for USB Deleted File Recovery. The left sidebar shows the file tree structure under 'SuspectUSB.E01 Host'. The main pane shows a list of recovered files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The list includes various files such as '008- KALA LHASMA.mp3', '009- Old Vs New dance.mp3', '010 LIFT MUSIC.mp3', '011- TEACHERS DANCE.mp3', '012- FORMATION DANCE.mp3', '013-Jana_Gana_Mana_National_Anthem_of_igetmp', 'ELEVATOR BEEP SOUND.mp3', '~\$Arka Kids Annual Day - 2024.pptx', '~\$Arka Kids Annual Day - 2024.pptx', '_otes.txt', '_est.png', 'rdTUnf#Rit', 'eftUnf#Rit', 'rdTUnf#Rit', '_01-ALL', '_SC_1926.JPG', and '_SC_1927.JPG'.

The screenshot displays the Wireshark network traffic analysis interface. The top pane shows a list of captured packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 37, Time 2.080132, Source 10.33.147.181, Destination 67.218.89.211, Protocol HTTP, Length 476). The bottom pane shows the raw packet data in hexadecimal and ASCII.

EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028



```
C:\Users\hemanth\Downloads\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size: 20128464896 bytes ( 19196 Mb)
Free space size: 122223923200 bytes ( 116561 Mb)

* Destination = \\?P:\C:\Users\hemanth\Downloads\LAPTOP-5L8563PQ-20251012-075145.raw

--> Are you sure you want to continue? [y/n]
```

Conclusion:

The exercise successfully introduced core concepts of computer forensics and provided hands-on familiarity with key tools across the investigation lifecycle. We created a verified disk image with FTK Imager, examined artifacts and deleted data in Autopsy, captured and filtered live network traffic in Wireshark, and extracted volatile evidence from a memory image using Volatility—each step documented with hashes, screenshots, and observations. Together, these activities demonstrated a defensible workflow for acquiring, analyzing, and reporting digital evidence that can be replicated in future investigations.