

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

Madhesh M A

231901029

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.

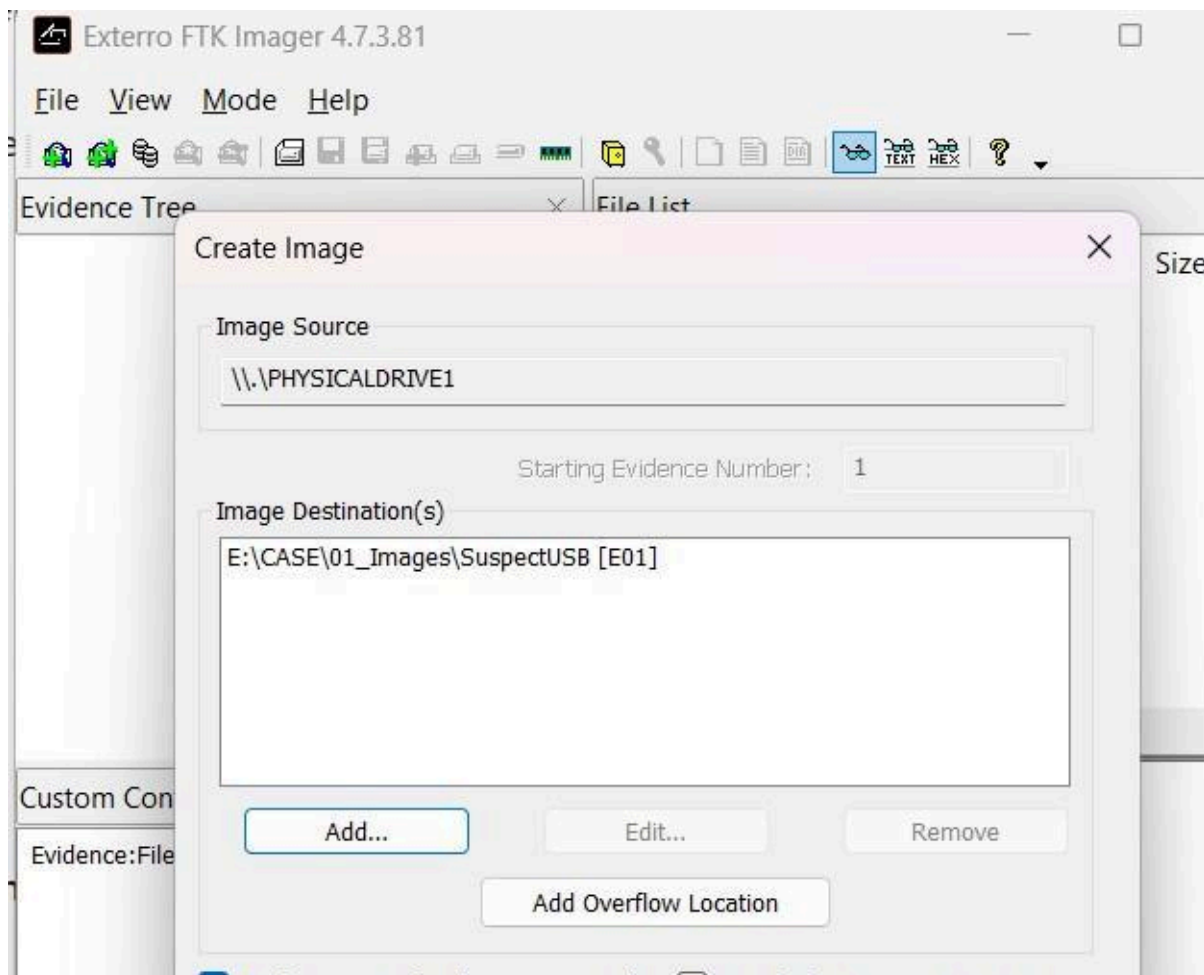
Procedure:

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

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

Drive/Image Verify Results	
Name	SuspectUSB.E01
Sector count	30310400
MDS Hash	
Computed hash	ffb14460cb956ca7ba1f919eeb91c768
Stored verification hash	ffb14460cb956ca7ba1f919eeb91c768
Report Hash	ffb14460cb956ca7ba1f919eeb91c768
Verify result	Match
SHA1 Hash	
Computed hash	d2ae8a36bfc192e4f24c121987ef8136a647d9a7
Stored verification hash	d2ae8a36bfc192e4f24c121987ef8136a647d9a7
Report Hash	d2ae8a36bfc192e4f24c121987ef8136a647d9a7
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Add Data Source

Steps

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

Select Data Source

Path:
E:\CASE\01_Images\SuspectUSB.E01

Browse

☐ Ignore orphan files in FAT file systems

Time zone:
(GMT+5:30) Asia/Calcutta

Sector size:
Auto Detect

Bitlocker Password (optional):

Hash Values (optional):
MD5:
SHA-1:
SHA-256:

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

< Back

Next >

Finish

Cancel

Help

USB Deleted File Recovery - Autopsy 4.22.1

Case View Tools Window Help

+ Add Data Source + Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
All 3972 Results

Data Sources

- SuspectUSB.E01_1 Host
 - SuspectUSB.E01
 - \$orphanfiles (1778)
 - \$carvedfiles (2)
 - \$unalloc (11)
 - 001-canon (9)
 - 005 GRADING EXAM (0)
 - 01-all (99)
 - 1B UK Level 2 (5)
 - _AI (0)
 - _PT (0)
 - _tock (0)
 - ABACUS BT SCHOOL CURRICULUM (0)
 - ABACUS CERTIFICATE LIST (0)
 - ABACUS COMPETITION QUESTION PAPERS (0)
 - ANNUAL DAY 2019 (0)
 - ANNUAL DAY 2022 (82)
 - ANNUAL DAY SONGS 2023 (0)
 - ARKA KIDS (5)
 - ARKA KIDS ANNUAL DAY SONGS 2024 (16)
 - ARKA KIDS ANNUAL DAY SONGS 2025 (14)
 - BRITE LEVEL 2 FINAL (0)
 - CARD PAYMENT DETAILS (0)
 - L8 UK Level 2 (0)
 - LEARNING BOX (12)
 - MATH SYLLABUS (0)
 - Miscellaneous (0)
 - Photos (0)
 - SIVARANGINI (0)
 - students database (0)
 - System Volume Information (6)
 - WORKSHEETS (0)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
X_U08-KALA LHASMAMP3				2024-01-10 13:33:38 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:33 IST	2632941	Unallocated
X_009-DiD Vs New dance.mp3				2024-02-06 13:04:54 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:39 IST	7081823	Unallocated
X_010 LIFT MUSIC.mp3				2024-02-15 17:35:14 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:40 IST	2049599	Unallocated
X_011-TEACHERS DANCE.mp3				2024-02-15 17:54:58 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:42 IST	5830231	Unallocated
X_012- FORMATION DANCE.mp3				2024-02-13 20:00:12 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:42 IST	2949544	Unallocated
X_013-Jana_Gana_Mana_National_Anthem_of_getmp3				2022-03-31 15:48:02 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:48 IST	2628098	Unallocated
X_ELEVATOR BEEP SOUND.mp3				2024-02-15 17:38:38 IST	0000-00-00 00:00:00	2024-03-05 00:00:00 IST	2024-02-15 18:11:49 IST	127566	Unallocated
X_-\$Arka Kids Annual Day - 2024.pptx				2024-02-15 18:16:18 IST	0000-00-00 00:00:00	2024-02-15 00:00:00 IST	2024-02-15 18:15:55 IST	165	Unallocated
X_- \$Arka Kids Annual Day - 2024.pptx				2024-02-16 14:19:10 IST	0000-00-00 00:00:00	2024-02-16 00:00:00 IST	2024-02-16 14:15:50 IST	165	Unallocated
X_.cste.txt				2025-10-12 22:24:26 IST	0000-00-00 00:00:00	2025-10-12 00:00:00 IST	2025-10-12 22:24:23 IST	104	Unallocated
X_.est.png				2025-10-12 22:25:16 IST	0000-00-00 00:00:00	2025-10-12 00:00:00 IST	2025-10-12 22:25:15 IST	740	Unallocated
X_rdtUinfF.Rit				2030-03-12 08:16:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	591819886	Unallocated
X_rdtUinfF.Rit				2036-03-15 10:32:20 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	591819886	Unallocated
X_rdtUinfF.Rit				2030-03-12 08:16:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	591819886	Unallocated
X_.01-ALL				2019-01-31 14:09:38 IST	0000-00-00 00:00:00	2020-02-17 00:00:00 IST	2019-02-14 17:23:18 IST	0	Unallocated
X_.SC_1926.JPG				2019-01-31 15:30:18 IST	0000-00-00 00:00:00	2019-02-16 00:00:00 IST	2019-02-14 17:23:18 IST	11922943	Unallocated
X_.SC_1927.JPG				2019-01-31 15:30:22 IST	0000-00-00 00:00:00	2019-02-16 00:00:00 IST	2019-02-14 17:23:20 IST	12727004	Unallocated

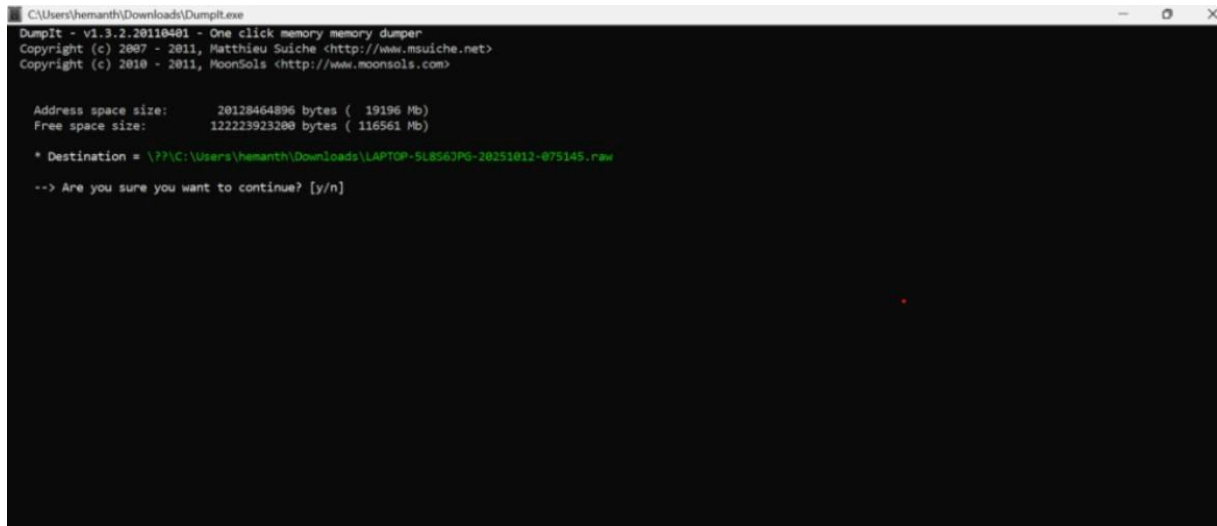
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is a GET request to `/streaming/non-tonic202009120streaming10xtruss20definitions.1.0_smalllanguages.11vetri.zip HTTP/1.1` with a length of 476 bytes.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the `GET /wreshark-labs/HTTP-wireshark-file2.html HTTP/1.1` request, including the request version, accept headers, user-agent, and host.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The packet details pane is expanded to show the `GET` method and the `URI` field, which contains the path `/wreshark-labs/HTTP-wireshark-file2.html`. The `Accept` header is set to `text/html, application/xhtml+xml, */*`, and the `User-Agent` is `Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; WOW64; Trident/5.0)`. The `Host` field is `gaia.cs.umass.edu`.

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



```
C:\Users\hemanth\Downloads\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msliche.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 = \\?\C:\Users\hemanth\Downloads\LAPTOP-5L856JPG-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.