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.

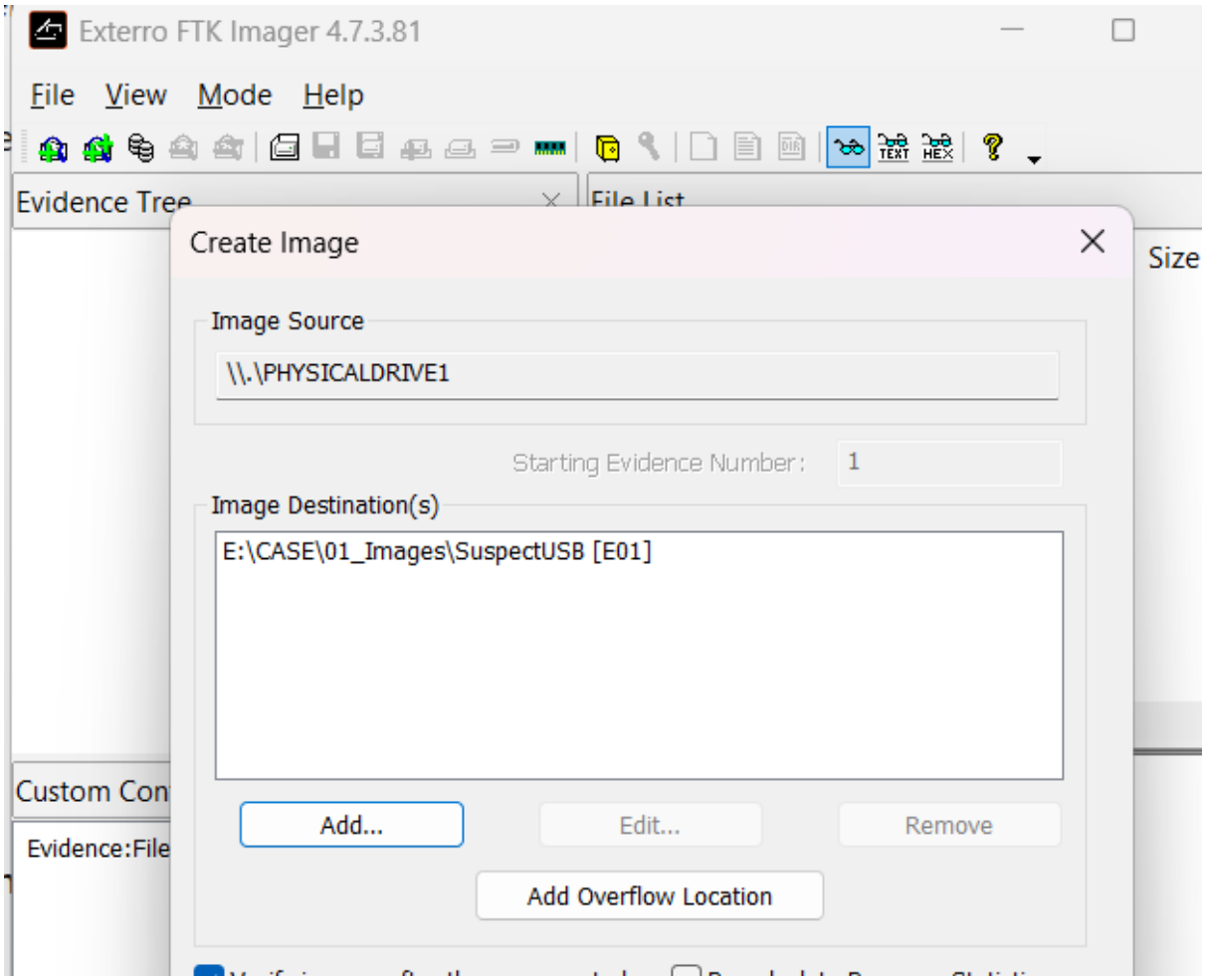
EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

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.

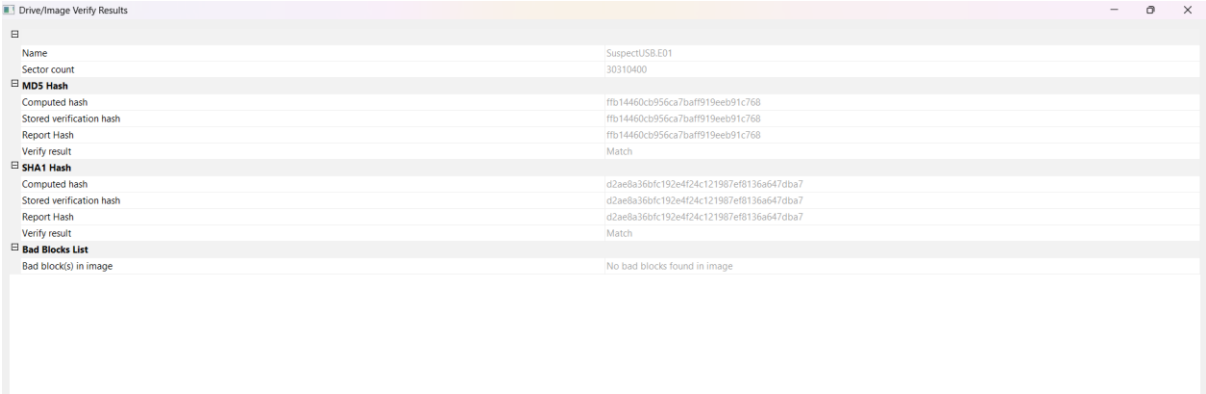
Output:



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

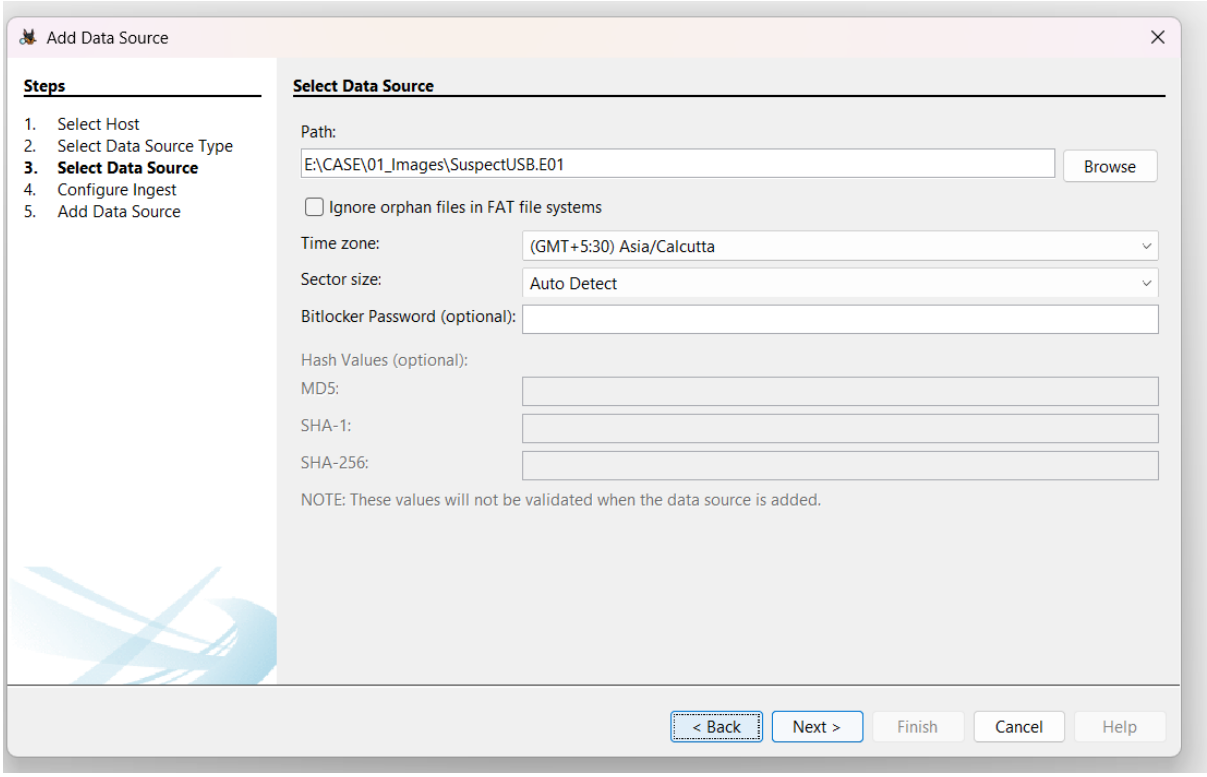
Madhan kumar B

231901028



Drive/Image Verify Results

Name	SuspectUSB.E01
Sector count	30310400
MD5 Hash	
Computed hash	ffb14460cb956ca7baff919eeb91c768
Stored verification hash	ffb14460cb956ca7baff919eeb91c768
Report Hash	ffb14460cb956ca7baff919eeb91c768
Verify result	Match
SHA1 Hash	
Computed hash	d2ae8a36bfc192e4f24c121987ef8136a647dba7
Stored verification hash	d2ae8a36bfc192e4f24c121987ef8136a647dba7
Report Hash	d2ae8a36bfc192e4f24c121987ef8136a647dba7
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:

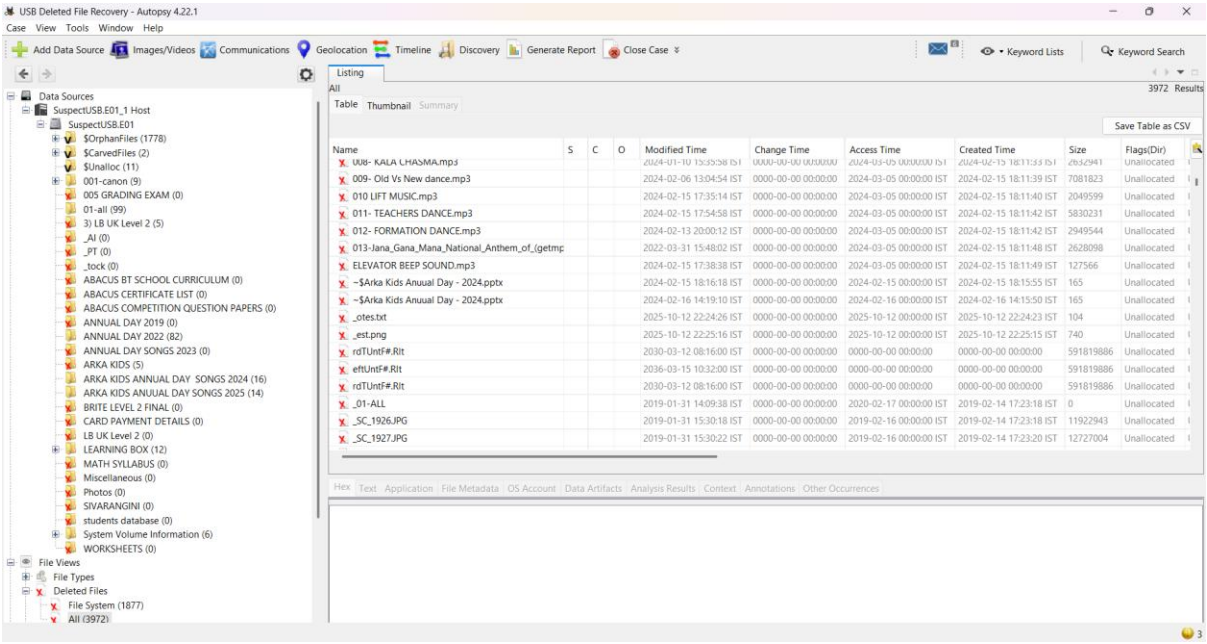
NOTE: These values will not be validated when the data source is added.

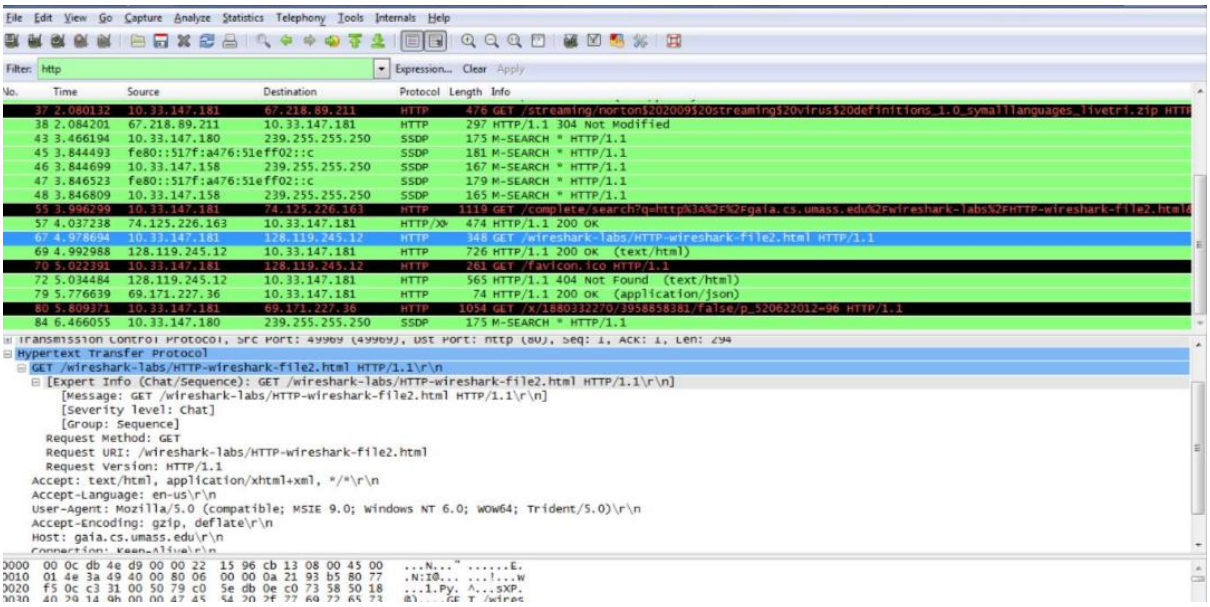
< Back | Next > | Finish | Cancel | Help

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

Madhan kumar B

231901028

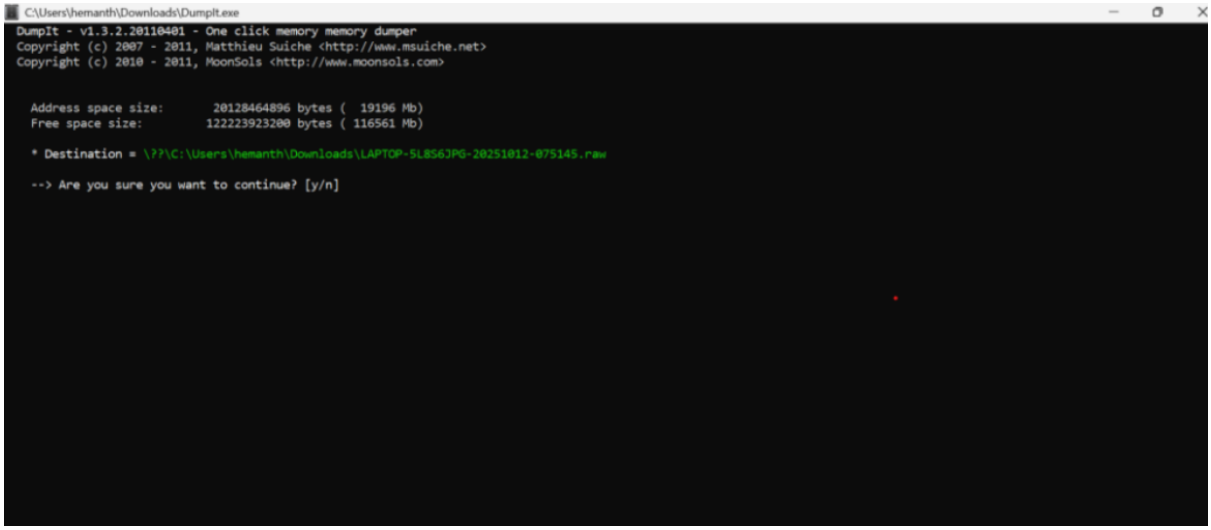




EXP NO:1 Study of Computer Forensics and Different Tools Used for Forensic Investigation

Madhan kumar B

231901028



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.