Exp:01 **Name: Hemanth kumar**

Roll no:231901010

Study of Computer Forensics and Different Tools Used for Forensic Investigation

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)

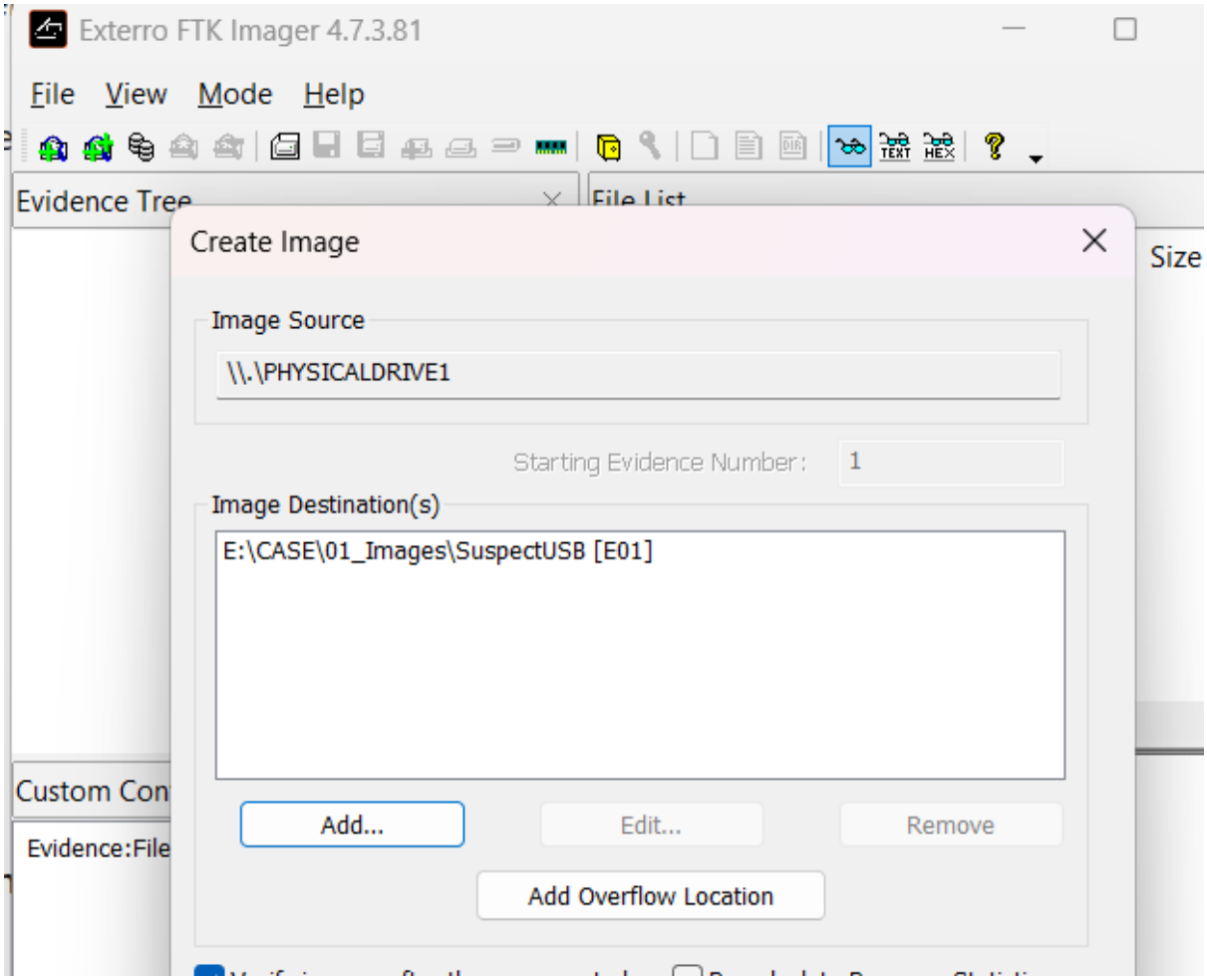
Algorithm (High-level):

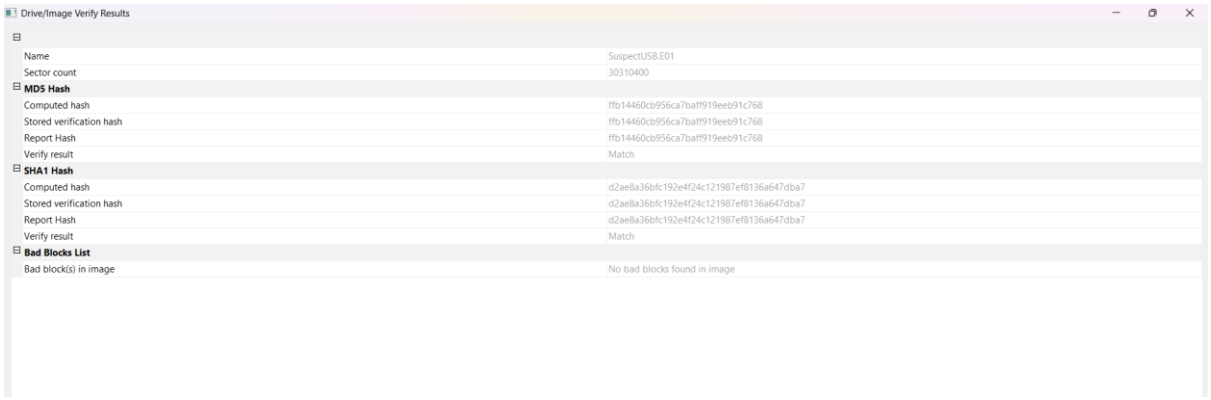
1. Identify the different categories of forensic tools.
2. Install and set up the chosen forensic tools on lab systems.
3. Perform a sample operation with each tool:
    - Imaging a drive with FTK Imager.
    - Analyzing deleted files and metadata in Autopsy.
    - Capturing packets with Wireshark.
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

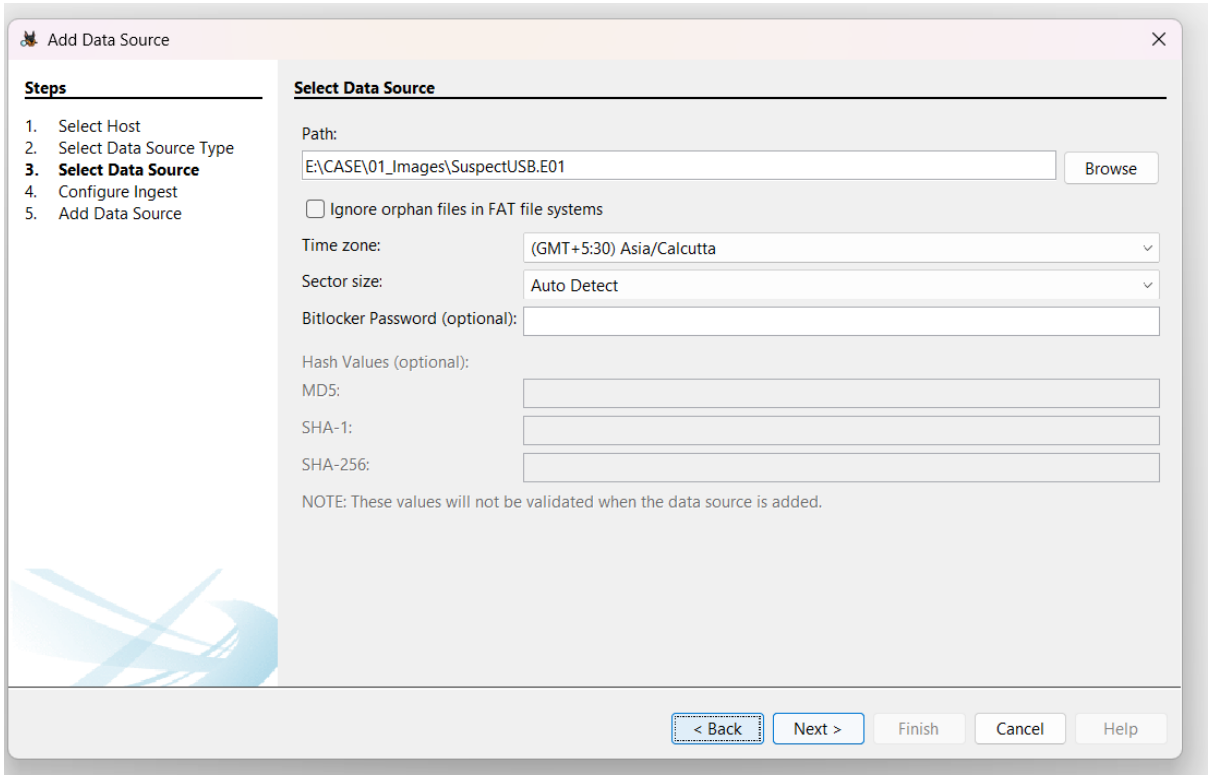
Procedure:

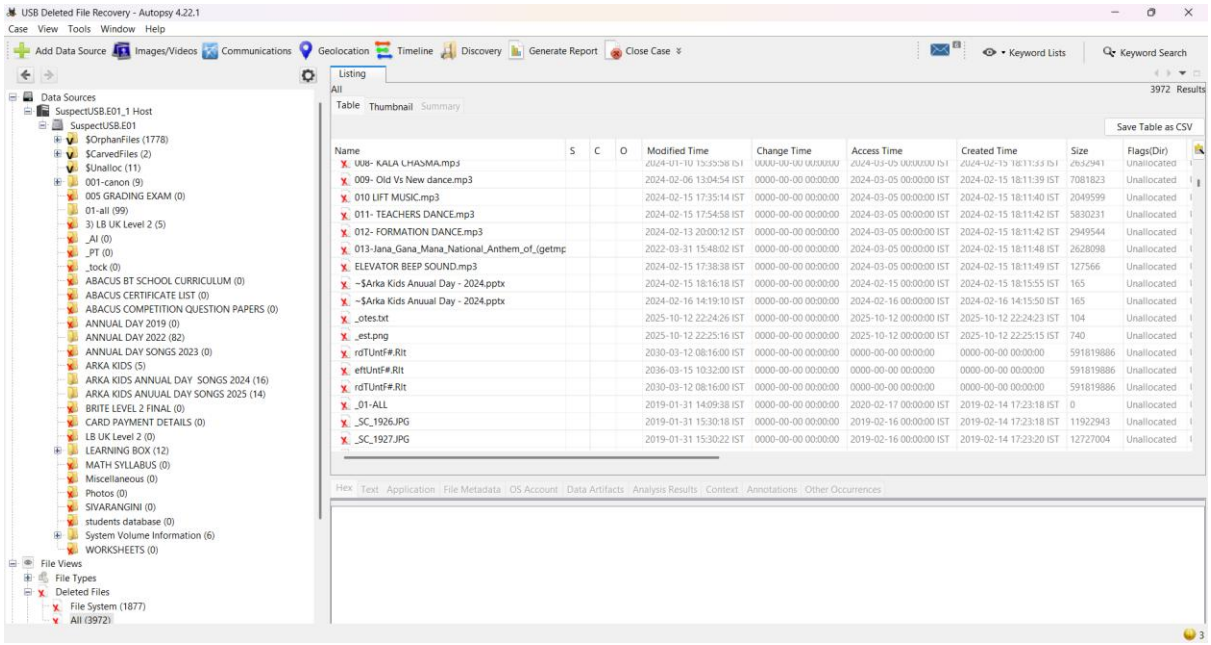
1. Create a lab case folder /CaseID/ForensicTools/.
2. Launch **FTK Imager** → acquire an image of a removable drive → save hash log.
3. Open **Autopsy** → create a new case → add the acquired image → run ingest modules.
4. Install and open **Wireshark** → capture live traffic for 2–3 minutes → apply 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.

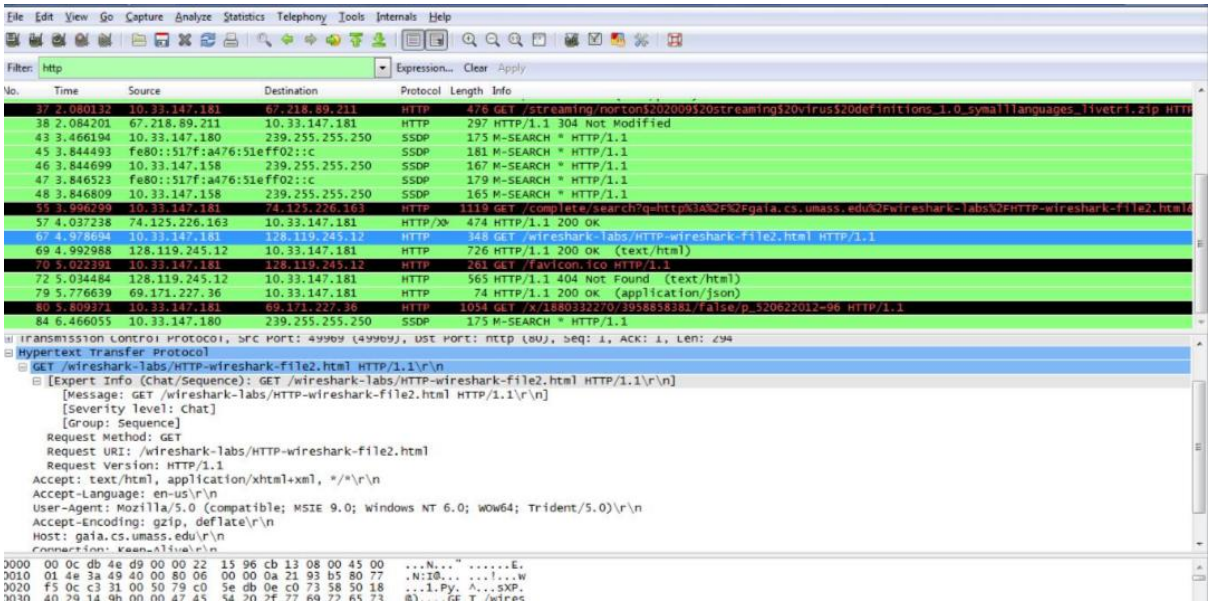
Output:

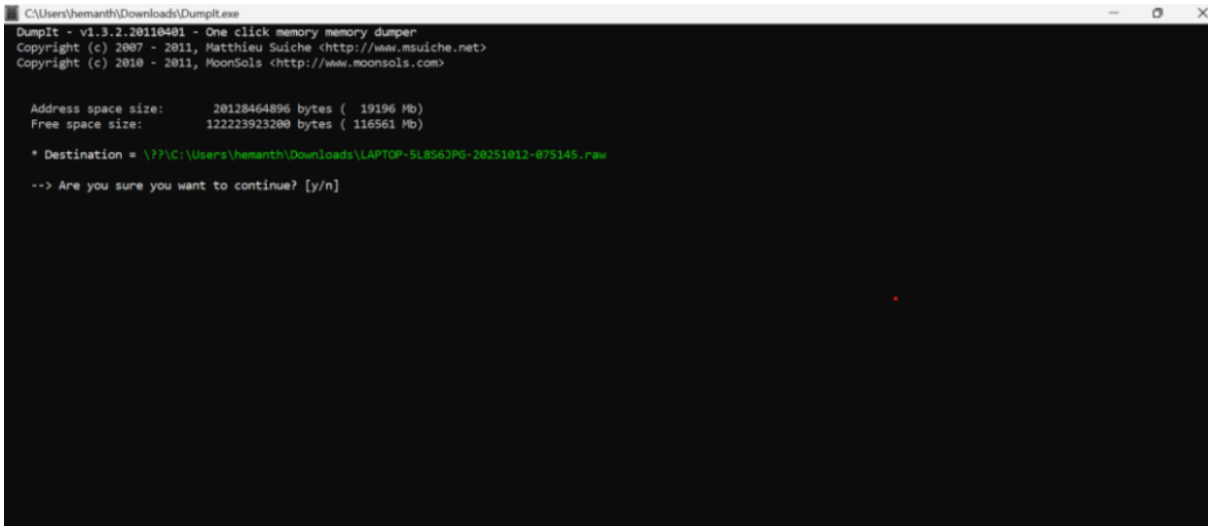



Drive/Image Verify Results
Name
SuspectUSB.E01
Sector count
30310400
MD5 Hash
Computed hash
ffb14460cb956ca7baff919eeb91c768
Stored verification hash
ffb14460cb956ca7baff919eeb91c768
Report Hash
ffb14460cb956ca7baff919eeb91c768
Verify result
Match
SHA1 Hash
Computed hash
d2ae8a36bfc192e4f24c121987ef8136a647dba7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


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
Keyword Lists Keyword Search
Data Sources
SuspectUSB.E01_1 Host
SuspectUSB.E01
$OrphanFiles (1778)
$CarvedFiles (2)
$Unalloc (11)
001-canon (9)
005 GRADING EXAM (0)
01-all (99)
3) LB UK Level 2 (5)
_AI (0)
_PT (0)
_tock (0)
ABACUS BT SCHOOL CURRICULUM (0)
ABACUS CERTIFICATE LIST (0)
ABACUS COMPETITION QUESTION PAPERS (0)
ANNUAL DAY 2019 (0)
ANNUAL DAY 2022 (82)
ANNUAL DAY SONGS 2023 (0)
ARKA KIDS (5)
ARKA KIDS ANNUAL DAY SONGS 2024 (16)
ARKA KIDS ANUUAL DAY SONGS 2025 (14)
BRITE LEVEL 2 FINAL (0)
CARD PAYMENT DETAILS (0)
LB UK Level 2 (0)
LEARNING BOX (12)
MATH SYLLABUS (0)
Miscellaneous (0)
Photos (0)
SIVARANGINI (0)
students database (0)
System Volume Information (6)
WORKSHEETS (0)
File Views
File Types
Deleted Files
File System (1877)
All (3972)
Listing
All
3972 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir)
009- Old Vs New dance.mp3 2024-02-06 13:04:54 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:39 IST 7081823 Unallocated
010 LIFT MUSIC.mp3 2024-02-15 17:35:14 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:40 IST 2049599 Unallocated
011- TEACHERS DANCE.mp3 2024-02-15 17:54:58 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:42 IST 5830231 Unallocated
012- FORMATION DANCE.mp3 2024-02-13 20:00:12 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:42 IST 2949544 Unallocated
013-Jana_Gana_Mana_National_Anthem_of_(getmp 2022-03-31 15:48:02 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:48 IST 2628098 Unallocated
ELEVATOR BEEP SOUND.mp3 2024-02-15 17:38:38 IST 0000-00-00 00:00:00 2024-03-05 00:00:00 IST 2024-02-15 18:11:49 IST 127566 Unallocated
~$Arka Kids Anuual 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
~$Arka Kids Anuual 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
_otes.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
_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
rdTUntF#.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
eftUntF#.RIt 2036-03-15 10:32:00 IST 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 591819886 Unallocated
rdTUntF#.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
_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
_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
_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


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
37 2.080132 10.33.147.181 67.218.89.211 HTTP 476 GET /streaming/norton%202009%20streaming%20virus%20definitions_1.0_symalllanguages_livetri.zip HTTP
38 2.084201 67.218.89.211 10.33.147.181 HTTP 297 HTTP/1.1 304 Not Modified
43 3.466194 10.33.147.180 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
45 3.844493 fe80::517f:a476:51eff02::c SSDP 181 M-SEARCH * HTTP/1.1
46 3.844699 10.33.147.158 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
47 3.846523 fe80::517f:a476:51eff02::c SSDP 179 M-SEARCH * HTTP/1.1
48 3.846809 10.33.147.158 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
55 3.996799 10.33.147.181 74.125.226.163 HTTP 1119 GET /complete/search?q=http%3A%2F%2Fgaia.cs.umass.edu%2Fwireshark-labs%2FHTTP-wireshark-file2.html&
57 4.037238 74.125.226.163 10.33.147.181 HTTP/XML 474 HTTP/1.1 200 OK
67 4.978694 10.33.147.181 128.119.245.12 HTTP 348 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
69 4.992988 128.119.245.12 10.33.147.181 HTTP 726 HTTP/1.1 200 OK (text/html)
70 5.022391 10.33.147.181 128.119.245.12 HTTP 261 GET /favicon.ico HTTP/1.1
72 5.034484 128.119.245.12 10.33.147.181 HTTP 565 HTTP/1.1 404 Not Found (text/html)
79 5.776639 69.171.227.36 10.33.147.181 HTTP 74 HTTP/1.1 200 OK (application/json)
80 5.809371 10.33.147.181 69.171.227.36 HTTP 1054 GET /x/1880322270/3958858381/false/p_520622012=96 HTTP/1.1
84 6.466055 10.33.147.180 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
Transmission Control Protocol, Src Port: 49969 (49969), Dst Port: http (80), Seq: 1, Ack: 1, Len: 294
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Message: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Accept: text/html, application/xhtml+xml, */*\r\n
Accept-Language: en-us\r\n
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; WOW64; Trident/5.0)\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
0000 00 0c db 4e d9 00 00 22 15 96 cb 13 08 00 45 00 ...N..." ......E.
0010 01 4e 3a 49 40 00 80 06 00 00 0a 21 93 b5 80 77 .N:I@.. ...!...w
0020 f5 0c c3 31 00 50 79 c0 5e db 0e c0 73 58 50 18 ...1.Py. ^...sXP.
0030 40 29 14 9b 00 00 47 45 54 20 2f 77 69 72 65 73 @)....GE T /wires



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.