Experiment No. 12

12.1 Aim:

Email and the Cloud Evidence: Geolocation of IP Address, Analyzing Email Headers, Recovering Browser Search History

Example Scenario:

A report indicates that a user may have sent suspicious emails and searched for information related to a fraud case.
As the digital forensics investigator, your tasks are:

1. Identify the physical or approximate location of IP addresses found in email headers or server logs.

2. Read and interpret email headers to determine the sending path and originating IPs.

3. Recover the suspect's recent browser search history to confirm intent or establish a timeline.

Tasks:

1. Gather Evidence Sources

- Obtain emails to examine (.eml files, raw headers from webmail, or .msg files).

- Collect server logs or cloud access logs if available.

- Acquire the suspect's browser profile or create a forensic image of the suspect's system if working from a seized machine.

2. Extract Email Headers

- For webmail (Gmail / G Suite), copy the email's full header.
- Save a copy of the full raw header as evidence.

3. Analyze Email Headers

- Use **G Suite Toolbox** to paste the copied email header.
- The tool will provide parsed results, including sender IP, message path, and authentication checks (SPF, DKIM, DMARC).
- Record candidate IP addresses for geolocation and further investigation.

4. Geolocate IP Address(es)

- Use https://whatismyipaddress.com/ip-lookup to map IPs to approximate geographic locations.
- Record details: country, region/state, city, ISP, and approximate latitude/longitude.
- Preserve results as screenshots or exported reports.

5. Recover Browser Search History

- Use **MyLastSearch.exe** on the suspect's system to retrieve recent browser search entries.
- Save the results, including URLs and timestamps, for evidence.

6. Correlate Evidence

- Match timestamps from email headers, IP geolocation, and browser search history.

- Identify searches made before or after sending suspicious emails to confirm intent.
- Note supporting artifacts like attachments, downloads, or cached pages.

7. Preserve and Verify Evidence

- Generate hash values (MD5/SHA1) for exported headers, browser search results, or forensic images.
- Maintain a detailed evidence log / chain-of-custody documenting acquisition details.

8. Report Findings

Include in the report:

- Extracted headers
- Identified IPs
- Geolocation screenshots
- Recovered browser search entries with timestamps
- Investigative conclusions
- Highlight limitations (e.g., approximate geolocation, possible header forgery).

12.2 Lab Outcome:

- Learn to extract email headers, parse and geolocate IP addresses, and recover browser search history.
- Correlate artifacts to build a timeline and support investigative conclusions.

12.3 Learning Objectives:

- Extract and preserve email headers for forensic analysis.
- Identify and interpret IP addresses in email headers.
- Use geolocation tools to estimate IP locations.
- Recover browser search history using **MyLastSearch.exe.**
- Correlate email, IP, and browser evidence into a coherent investigative timeline.

12.4 Requirements:

Hardware

- Forensic workstation or laptop
- External storage for evidence images and exports

Software / Tools

- **G Suite Toolbox** for analyzing email headers
- https://whatismyipaddress.com/ip-lookup for IP geolocation
- **MyLastSearch.exe** for browser search recovery
- **Wireshark** (optional, for network-level corroboration)
- **Autopsy / FTK Imager / Magnet / Belkasoft** (for acquiring system images if needed)
- **Hashing utility (MD5/SHA1)**

- **Text editor** for notes and reporting

12.5 Related Theory:

Email Headers

Email headers contain metadata about a message, including sender, recipient, date/time, and the servers it passed through.
"Received:" lines indicate the path the email took, often showing the originating IP address.
Authentication fields like SPF, DKIM, and DMARC help verify whether the email is legitimate or potentially forged.

IP Geolocation

IP geolocation maps an IP address to an approximate geographic location using ISP and registry data.
It provides details like country, city, and ISP, but it is not precise—especially if the sender uses VPNs, proxies, or Tor.
Geolocation helps investigators narrow down the region from which an email was sent.

Browser Search History

Browsers store visited URLs and search queries locally, often in SQLite databases (e.g., Chrome History, Firefox `places.sqlite`).
Many browsers also sync this data to cloud accounts if enabled.
Recovered history provides timestamps and content, helping establish the suspect's intent or activities.

Limitations & Cautions:

- Email headers can be manipulated.

- IP geolocation may reflect the VPN/proxy exit point, not the actual sender.

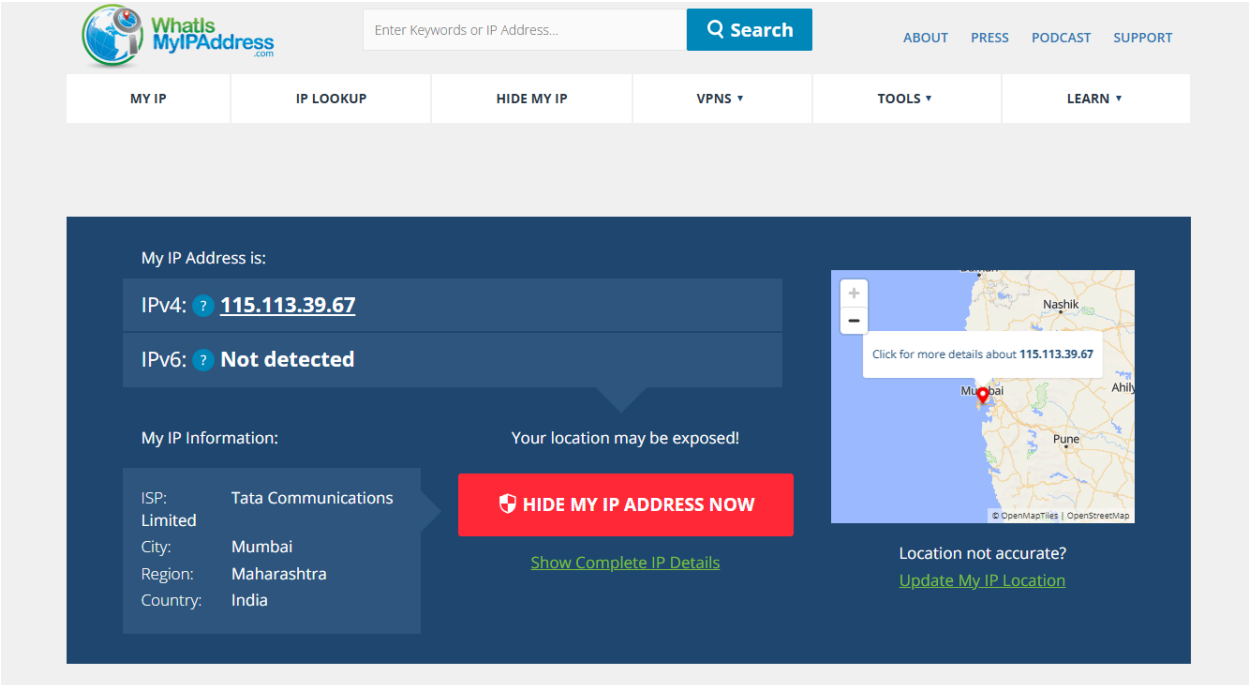
- Cloud-synced data may require legal authority to access.
- Always maintain chain-of-custody and verify evidence integrity using hash values (MD5/SHA1).

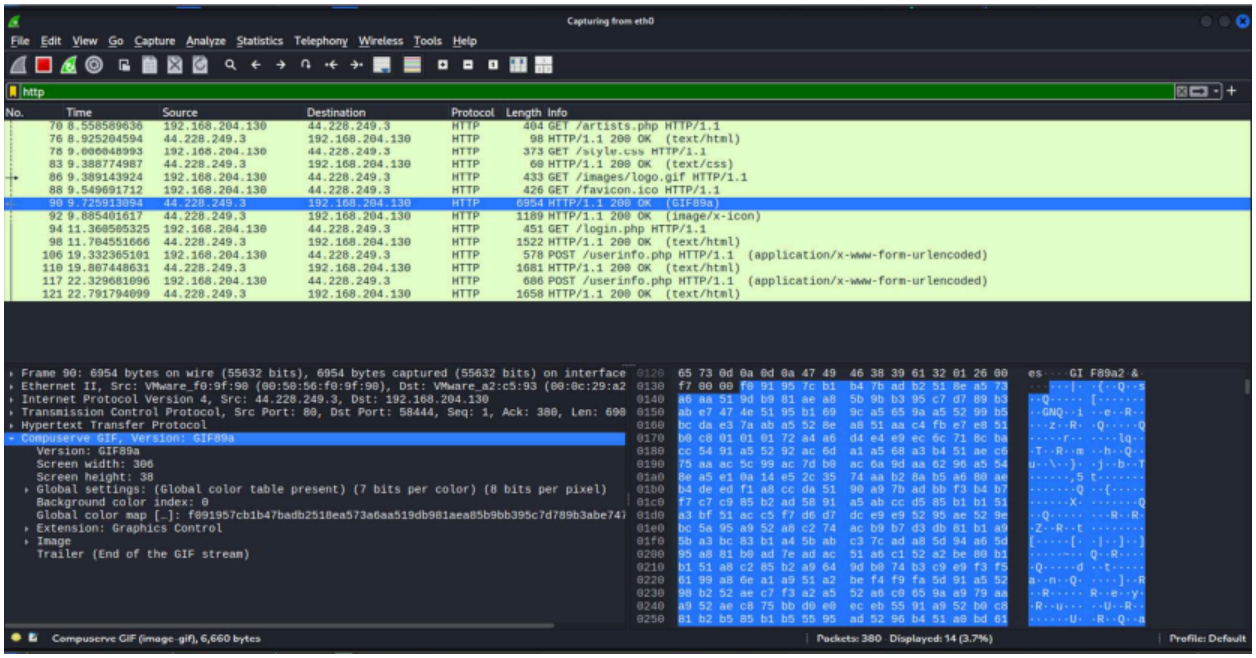
Purpose in Forensics:

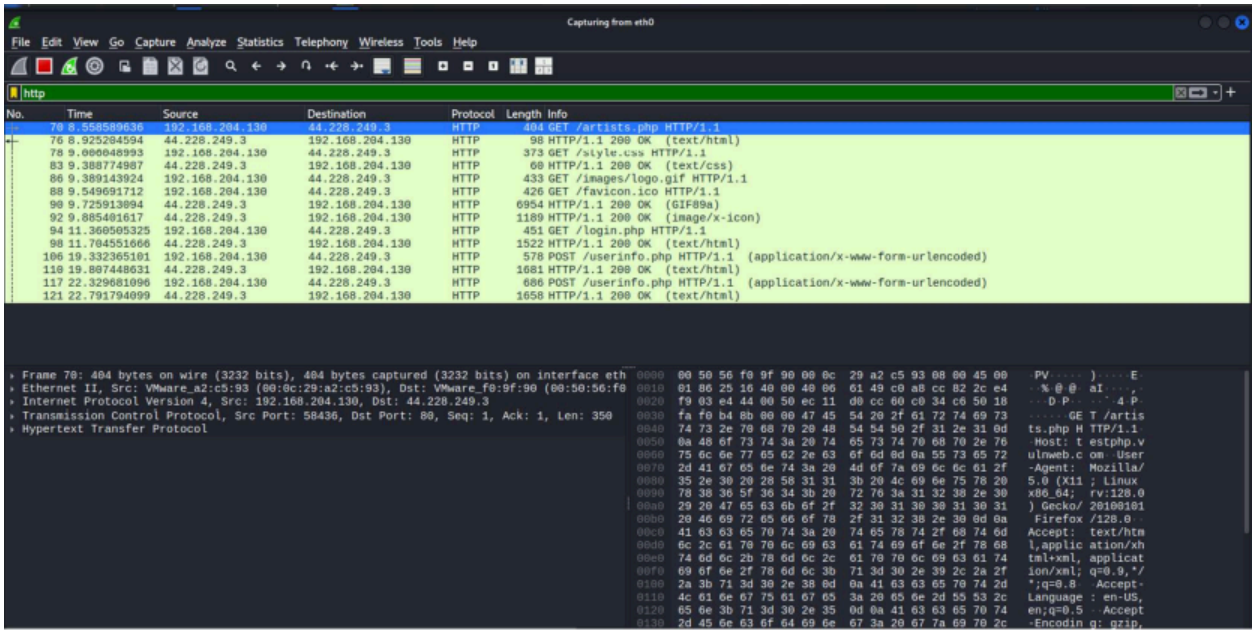
By combining email headers, IP geolocation, and browser search history, investigators can build a timeline, confirm intent, and correlate digital evidence while ensuring it remains admissible in court.

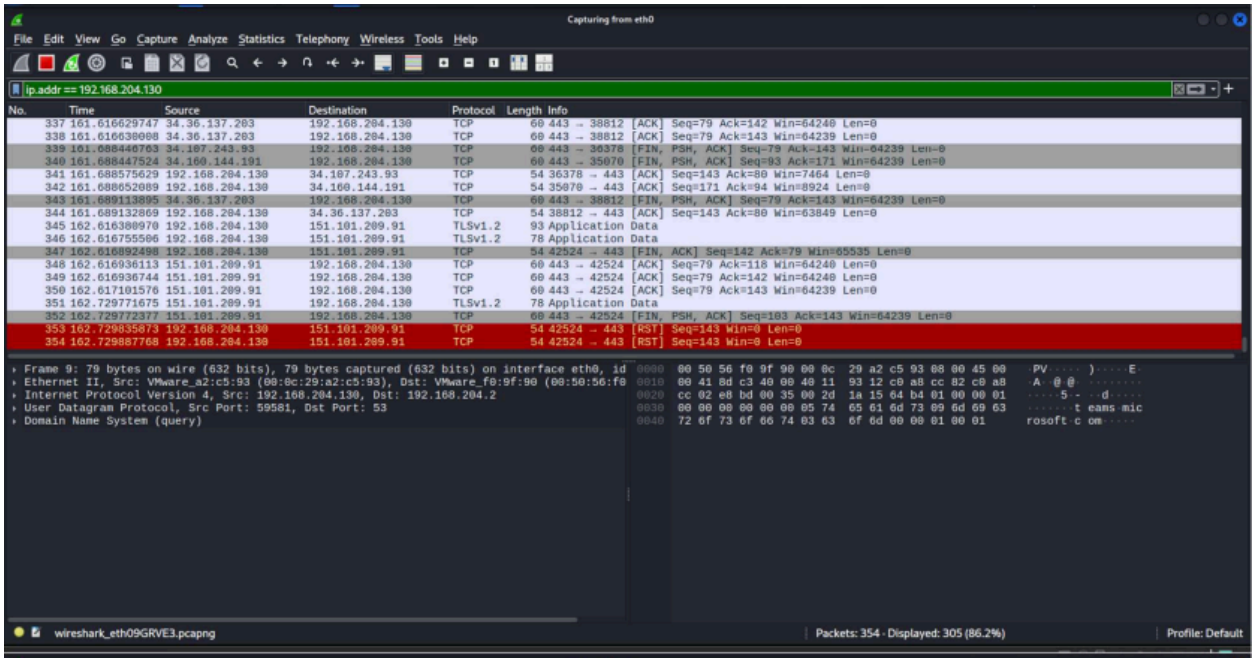
12.6 Output:

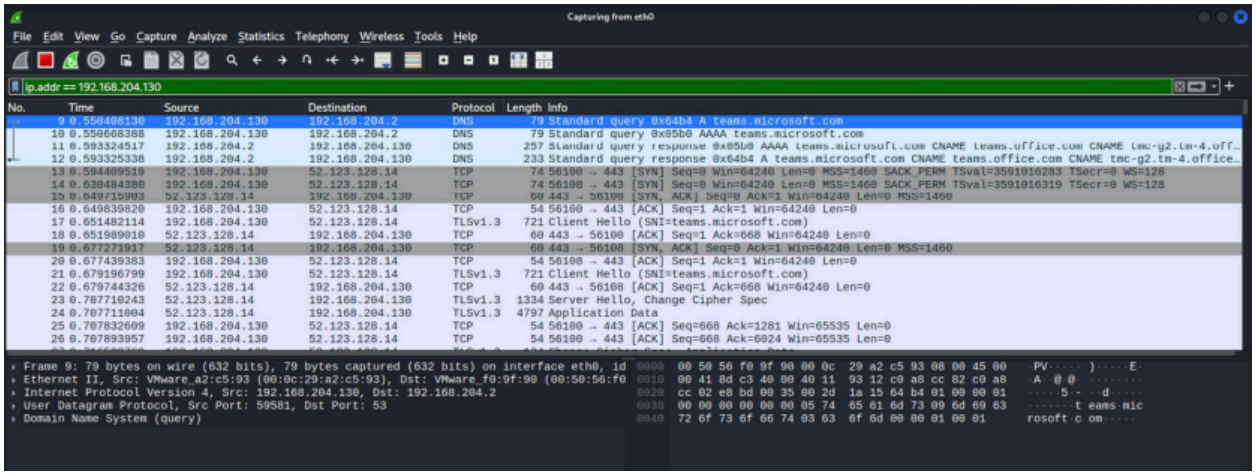
(Attach screenshots or data outputs of header analysis, IP lookup, and browser search recovery.)

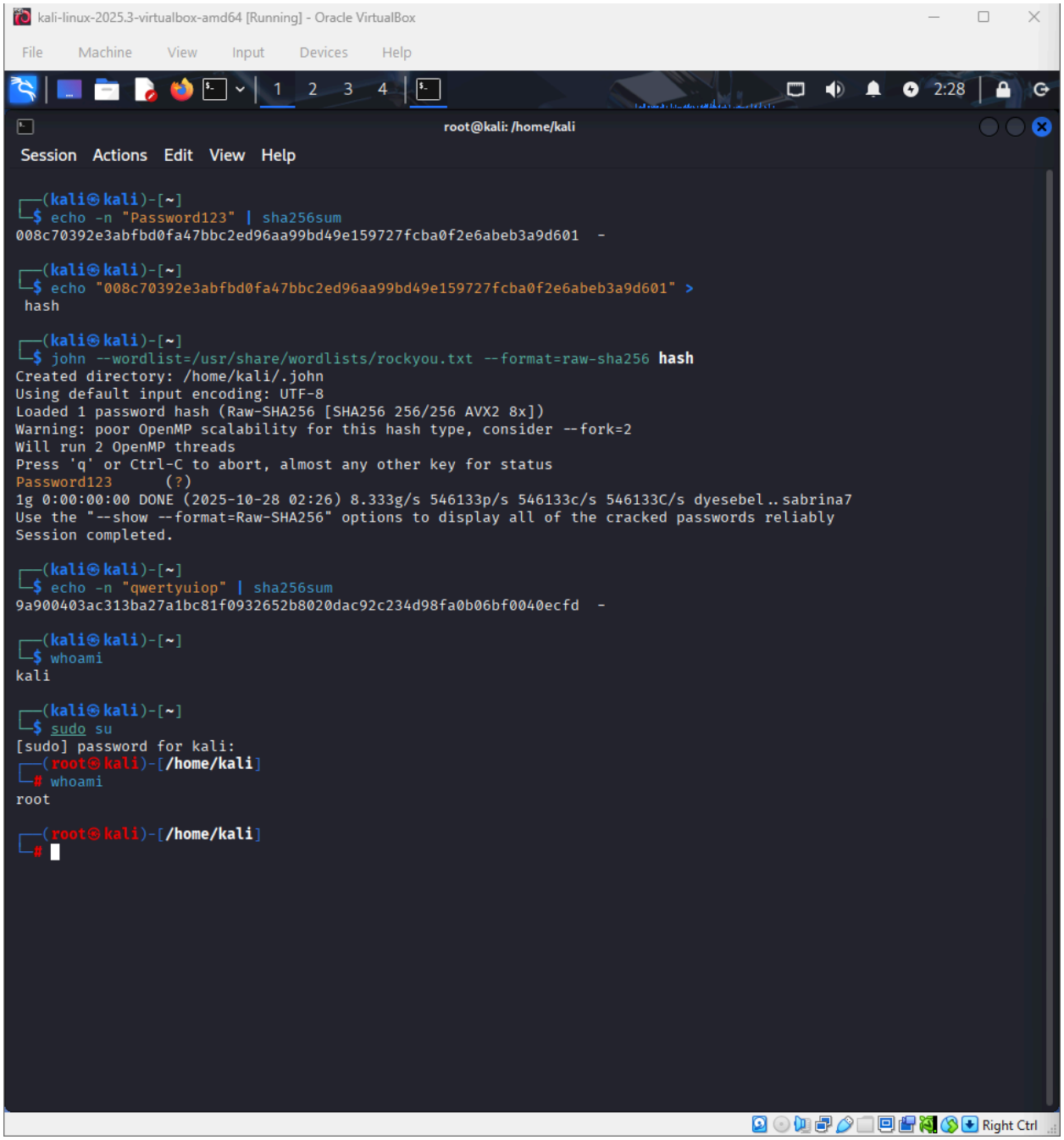


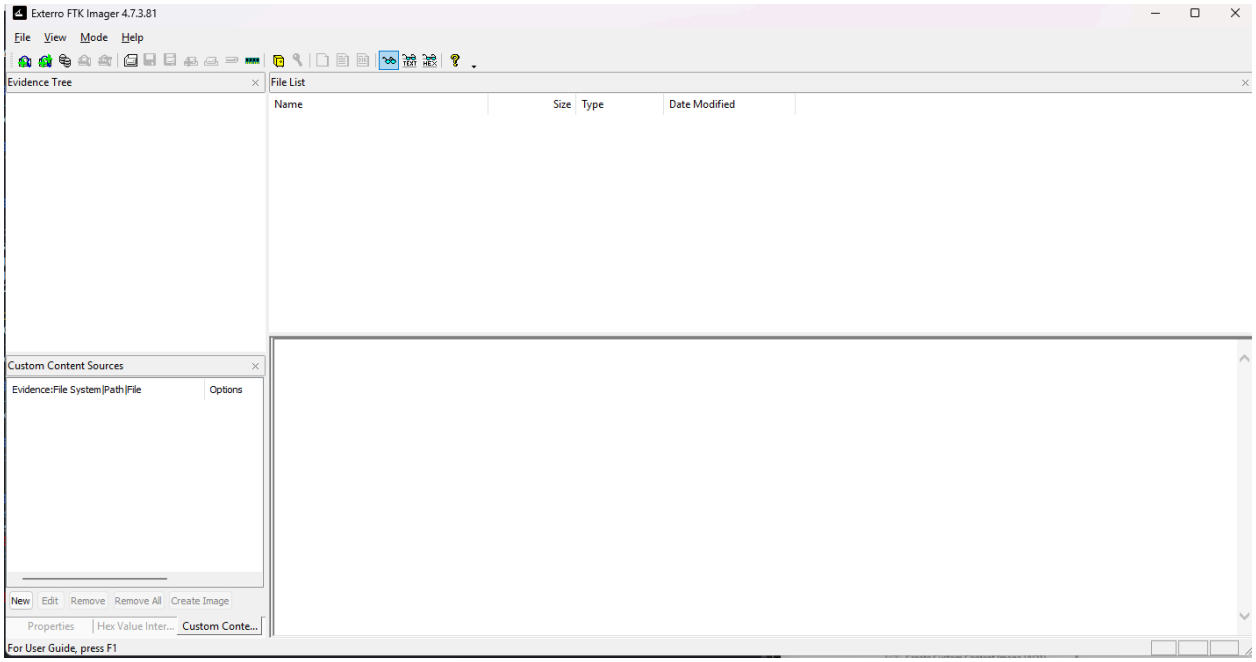

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
70 8.558589636 192.168.204.130 44.228.249.3 HTTP 404 GET /artists.php HTTP/1.1
76 8.925204594 44.228.249.3 192.168.204.130 HTTP 98 HTTP/1.1 200 OK (text/html)
78 9.000048993 192.168.204.130 44.228.249.3 HTTP 373 GET /style.css HTTP/1.1
83 9.388774987 44.228.249.3 192.168.204.130 HTTP 60 HTTP/1.1 200 OK (text/css)
86 9.389143924 192.168.204.130 44.228.249.3 HTTP 433 GET /images/logo.gif HTTP/1.1
88 9.549691712 192.168.204.130 44.228.249.3 HTTP 426 GET /favicon.ico HTTP/1.1
90 9.725913094 44.228.249.3 192.168.204.130 HTTP 6954 HTTP/1.1 200 OK (GIF89a)
92 9.885401617 44.228.249.3 192.168.204.130 HTTP 1189 HTTP/1.1 200 OK (image/x-icon)
94 11.360505325 192.168.204.130 44.228.249.3 HTTP 451 GET /login.php HTTP/1.1
98 11.704551666 44.228.249.3 192.168.204.130 HTTP 1522 HTTP/1.1 200 OK (text/html)
106 19.332365101 192.168.204.130 44.228.249.3 HTTP 578 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
110 19.807448631 44.228.249.3 192.168.204.130 HTTP 1681 HTTP/1.1 200 OK (text/html)
117 22.329681096 192.168.204.130 44.228.249.3 HTTP 686 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
121 22.791794099 44.228.249.3 192.168.204.130 HTTP 1658 HTTP/1.1 200 OK (text/html)
Frame 90: 6954 bytes on wire (55632 bits), 6954 bytes captured (55632 bits) on interface
Ethernet II, Src: VMware_f0:9f:90 (00:50:56:f0:9f:90), Dst: VMware_a2:c5:93 (00:0c:29:a2
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.204.130
Transmission Control Protocol, Src Port: 80, Dst Port: 58444, Seq: 1, Ack: 380, Len: 690
Hypertext Transfer Protocol
Compuserve GIF, Version: GIF89a
Version: GIF89a
Screen width: 306
Screen height: 38
Global settings: (Global color table present) (7 bits per color) (8 bits per pixel)
Background color index: 0
Global color map [...]: f091957cb1b47badb2518ea573a6aa519db981aea85b9bb395c7d789b3abe747
Extension: Graphics Control
Image
Trailer (End of the GIF stream)
Compuserve GIF (image/gif), 6,660 bytes
Packets: 380 Displayed: 14 (3.7%)
Profile: Default

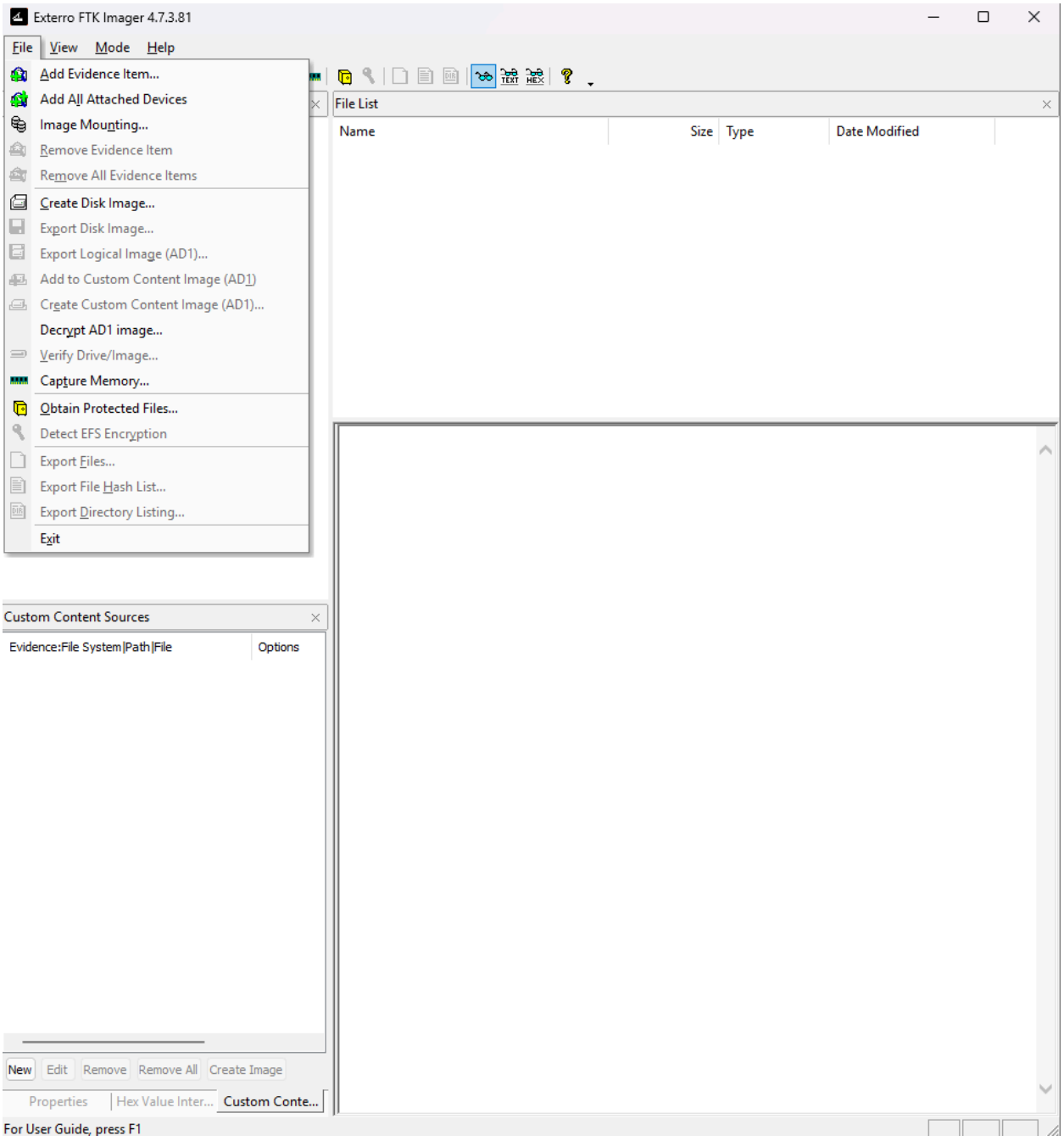

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
70 8.558589636 192.168.204.130 44.228.249.3 HTTP 404 GET /artists.php HTTP/1.1
76 8.925204594 44.228.249.3 192.168.204.130 HTTP 98 HTTP/1.1 200 OK (text/html)
78 9.000048993 192.168.204.130 44.228.249.3 HTTP 373 GET /style.css HTTP/1.1
83 9.388774987 44.228.249.3 192.168.204.130 HTTP 60 HTTP/1.1 200 OK (text/css)
86 9.389143924 192.168.204.130 44.228.249.3 HTTP 433 GET /images/logo.gif HTTP/1.1
88 9.549691712 192.168.204.130 44.228.249.3 HTTP 426 GET /favicon.ico HTTP/1.1
90 9.725913094 44.228.249.3 192.168.204.130 HTTP 6954 HTTP/1.1 200 OK (GIF89a)
92 9.885401617 44.228.249.3 192.168.204.130 HTTP 1189 HTTP/1.1 200 OK (image/x-icon)
94 11.360505325 192.168.204.130 44.228.249.3 HTTP 451 GET /login.php HTTP/1.1
98 11.704551666 44.228.249.3 192.168.204.130 HTTP 1522 HTTP/1.1 200 OK (text/html)
106 19.332365101 192.168.204.130 44.228.249.3 HTTP 578 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
110 19.807448631 44.228.249.3 192.168.204.130 HTTP 1681 HTTP/1.1 200 OK (text/html)
117 22.329681096 192.168.204.130 44.228.249.3 HTTP 686 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
121 22.791794099 44.228.249.3 192.168.204.130 HTTP 1658 HTTP/1.1 200 OK (text/html)
Frame 70: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface eth
Ethernet II, Src: VMware_a2:c5:93 (00:0c:29:a2:c5:93), Dst: VMware_f0:9f:90 (00:50:56:f0
Internet Protocol Version 4, Src: 192.168.204.130, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 58436, Dst Port: 80, Seq: 1, Ack: 1, Len: 350
Hypertext Transfer Protocol

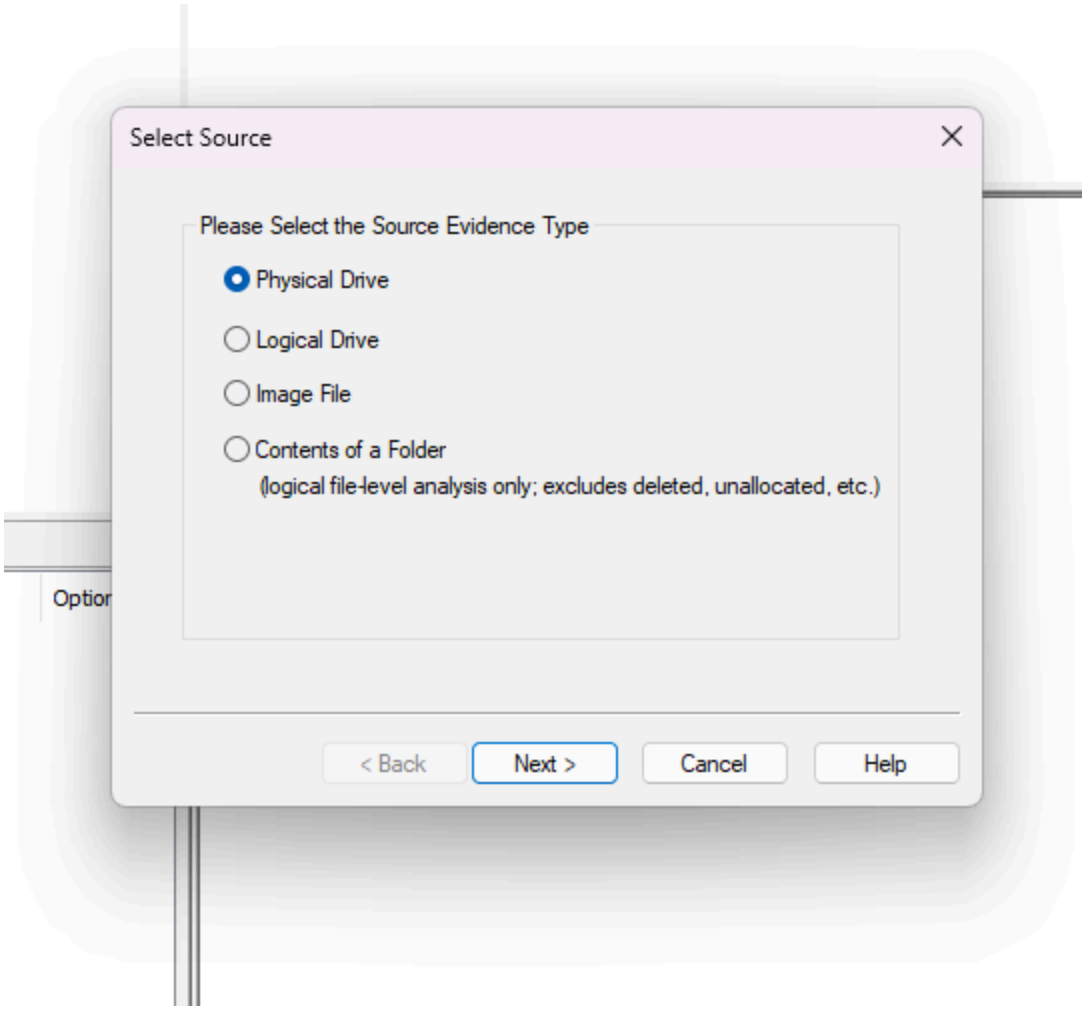

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.204.130
No. Time Source Destination Protocol Length Info
337 161.616629747 34.36.137.203 192.168.204.130 TCP 60 443 → 38812 [ACK] Seq=79 Ack=142 Win=64240 Len=0
338 161.616630008 34.36.137.203 192.168.204.130 TCP 60 443 → 38812 [ACK] Seq=79 Ack=143 Win=64239 Len=0
339 161.688446763 34.107.243.93 192.168.204.130 TCP 60 443 → 36378 [FIN, PSH, ACK] Seq=79 Ack=143 Win=64239 Len=0
340 161.688447524 34.160.144.191 192.168.204.130 TCP 60 443 → 35070 [FIN, PSH, ACK] Seq=93 Ack=171 Win=64239 Len=0
341 161.688575629 192.168.204.130 34.107.243.93 TCP 54 36378 → 443 [ACK] Seq=143 Ack=80 Win=7464 Len=0
342 161.688652089 192.168.204.130 34.160.144.191 TCP 54 35070 → 443 [ACK] Seq=171 Ack=94 Win=8924 Len=0
343 161.689113895 34.36.137.203 192.168.204.130 TCP 60 443 → 38812 [FIN, PSH, ACK] Seq=79 Ack=143 Win=64239 Len=0
344 161.689132869 192.168.204.130 34.36.137.203 TCP 54 38812 → 443 [ACK] Seq=143 Ack=80 Win=63849 Len=0
345 162.616380970 192.168.204.130 151.101.209.91 TLSv1.2 93 Application Data
346 162.616755506 192.168.204.130 151.101.209.91 TLSv1.2 78 Application Data
347 162.616892498 192.168.204.130 151.101.209.91 TCP 54 42524 → 443 [FIN, ACK] Seq=142 Ack=79 Win=65535 Len=0
348 162.616936113 151.101.209.91 192.168.204.130 TCP 60 443 → 42524 [ACK] Seq=79 Ack=118 Win=64240 Len=0
349 162.616936744 151.101.209.91 192.168.204.130 TCP 60 443 → 42524 [ACK] Seq=79 Ack=142 Win=64240 Len=0
350 162.617101576 151.101.209.91 192.168.204.130 TCP 60 443 → 42524 [ACK] Seq=79 Ack=143 Win=64239 Len=0
351 162.729771675 151.101.209.91 192.168.204.130 TLSv1.2 78 Application Data
352 162.729772377 151.101.209.91 192.168.204.130 TCP 60 443 → 42524 [FIN, PSH, ACK] Seq=103 Ack=143 Win=64239 Len=0
353 162.729835873 192.168.204.130 151.101.209.91 TCP 54 42524 → 443 [RST] Seq=143 Win=0 Len=0
354 162.729887768 192.168.204.130 151.101.209.91 TCP 54 42524 → 443 [RST] Seq=143 Win=0 Len=0
Frame 9: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0, id
Ethernet II, Src: VMware_a2:c5:93 (00:0c:29:a2:c5:93), Dst: VMware_f0:9f:90 (00:50:56:f0
Internet Protocol Version 4, Src: 192.168.204.130, Dst: 192.168.204.2
User Datagram Protocol, Src Port: 59581, Dst Port: 53
Domain Name System (query)
0000 00 50 56 f0 9f 90 00 0c 29 a2 c5 93 08 00 45 00
0010 00 41 8d c3 40 00 40 11 93 12 c0 a8 cc 82 c0 a8
0020 cc 02 e8 bd 00 35 00 2d 1a 15 64 b4 01 00 00 01
0030 00 00 00 00 00 00 05 74 65 61 6d 73 09 6d 69 63
0040 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01
wireshark_eth09GRVE3.pcapng
Packets: 354 · Displayed: 305 (86.2%)
Profile: Default

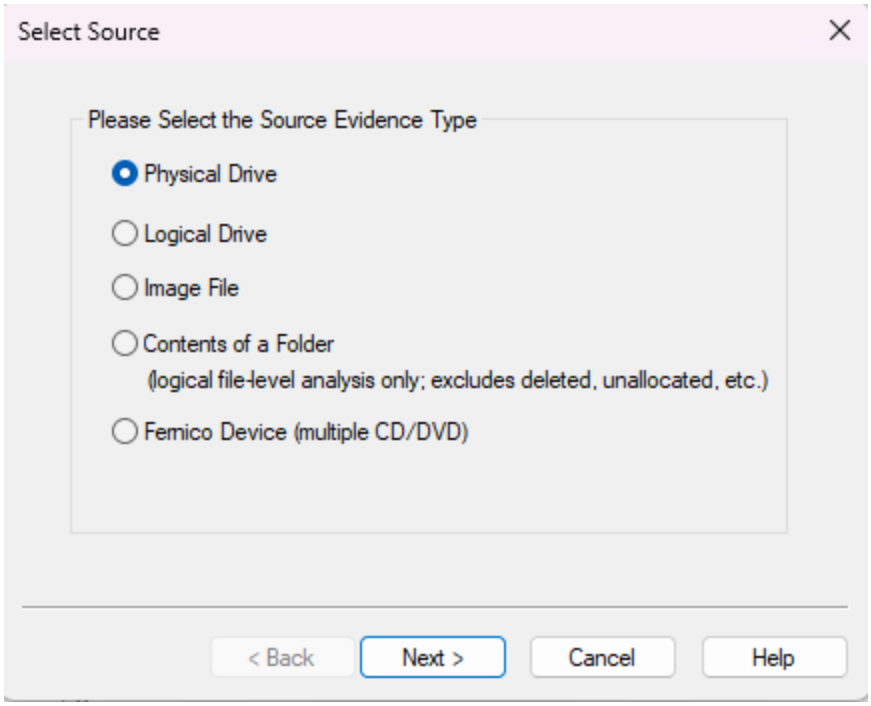

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.204.130
No. Time Source Destination Protocol Length Info
9 0.556408130 192.168.204.130 192.168.204.2 DNS 79 Standard query 0x64b4 A teams.microsoft.com
10 0.556668388 192.168.204.130 192.168.204.2 DNS 79 Standard query 0x85b0 AAAA teams.microsoft.com
11 0.593324517 192.168.204.2 192.168.204.130 DNS 257 Standard query response 0x85b0 AAAA teams.microsoft.com CNAME teams.office.com CNAME tmc-g2.tm-4.offi
12 0.593325338 192.168.204.2 192.168.204.130 DNS 233 Standard query response 0x64b4 A teams.microsoft.com CNAME teams.office.com CNAME tmc-g2.tm-4.office
13 0.594409519 192.168.204.130 52.123.128.14 TCP 74 56100 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3591016283 TSecr=0 WS=128
14 0.630484380 192.168.204.130 52.123.128.14 TCP 74 56108 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3591016319 TSecr=0 WS=128
15 0.649715903 52.123.128.14 192.168.204.130 TCP 60 443 → 56108 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16 0.649839820 192.168.204.130 52.123.128.14 TCP 54 56100 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17 0.651482114 192.168.204.130 52.123.128.14 TLSv1.3 721 Client Hello (SNI=teams.microsoft.com)
18 0.651989010 52.123.128.14 192.168.204.130 TCP 60 443 → 56100 [ACK] Seq=1 Ack=668 Win=64240 Len=0
19 0.677271917 52.123.128.14 192.168.204.130 TCP 60 443 → 56108 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
20 0.677439383 192.168.204.130 52.123.128.14 TCP 54 56108 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
21 0.679196799 192.168.204.130 52.123.128.14 TLSv1.3 721 Client Hello (SNI=teams.microsoft.com)
22 0.679744326 52.123.128.14 192.168.204.130 TCP 60 443 → 56108 [ACK] Seq=1 Ack=668 Win=64240 Len=0
23 0.707710243 52.123.128.14 192.168.204.130 TLSv1.3 1334 Server Hello, Change Cipher Spec
24 0.707711004 52.123.128.14 192.168.204.130 TLSv1.3 4797 Application Data
25 0.707832609 192.168.204.130 52.123.128.14 TCP 54 56100 → 443 [ACK] Seq=668 Ack=1281 Win=65535 Len=0
26 0.707893957 192.168.204.130 52.123.128.14 TCP 54 56100 → 443 [ACK] Seq=668 Ack=6024 Win=65535 Len=0
Frame 9: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0, id
Ethernet II, Src: VMware_a2:c5:93 (00:0c:29:a2:c5:93), Dst: VMware_f0:9f:90 (00:50:56:f0
Internet Protocol Version 4, Src: 192.168.204.130, Dst: 192.168.204.2
User Datagram Protocol, Src Port: 59581, Dst Port: 53
Domain Name System (query)
0000 00 50 56 f0 9f 90 00 0c 29 a2 c5 93 08 00 45 00
0010 00 41 8d c3 40 00 40 11 93 12 c0 a8 cc 82 c0 a8
0020 cc 02 e8 bd 00 35 00 2d 1a 15 64 b4 01 00 00 01
0030 00 00 00 00 00 00 05 74 65 61 6d 73 09 6d 69 63
0040 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01

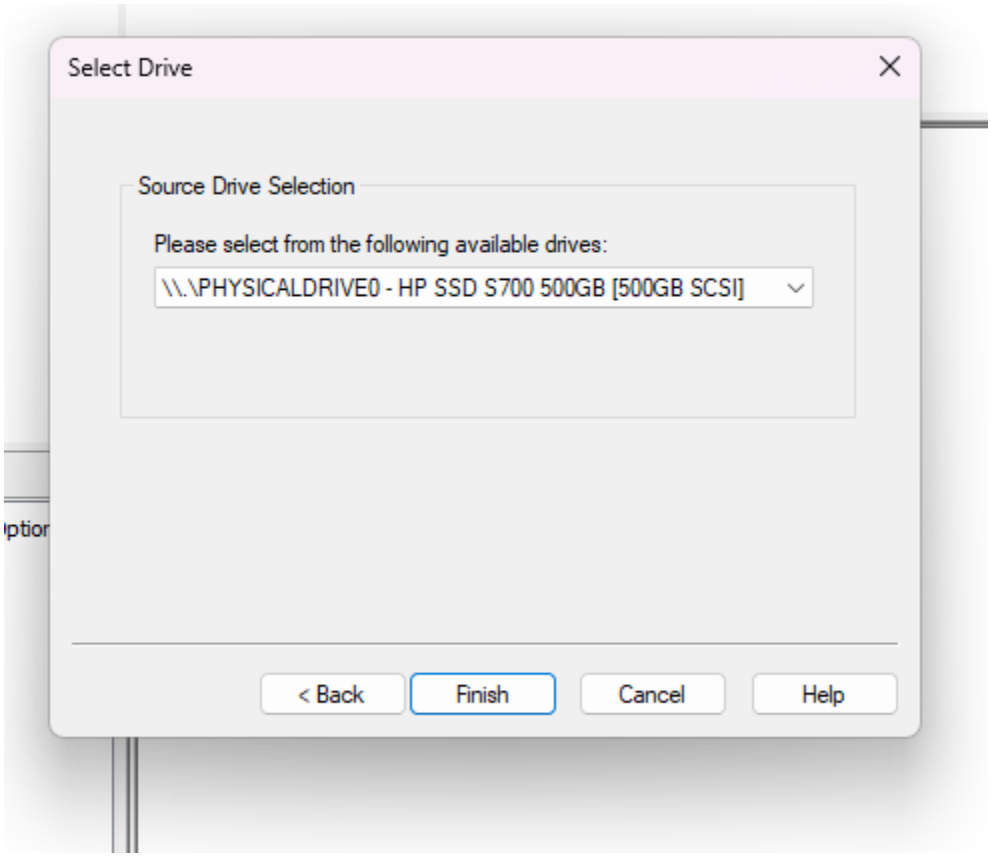

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
2:28
root@kali: /home/kali
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ echo -n "Password123" | sha256sum
008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcba0f2e6abeb3a9d601 -
┌──(kali㉿kali)-[~]
└─$ echo "008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcba0f2e6abeb3a9d601" >
hash
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 hash
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123 (?)
1g 0:00:00:00 DONE (2025-10-28 02:26) 8.333g/s 546133p/s 546133c/s 546133C/s dyesebel..sabrina7
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~]
└─$ echo -n "qwertyuiop" | sha256sum
9a900403ac313ba27a1bc81f0932652b8020dac92c234d98fa0b06bf0040ecfd -
┌──(kali㉿kali)-[~]
└─$ whoami
kali
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# whoami
root
┌──(root㉿kali)-[/home/kali]
└─#
Right Ctrl

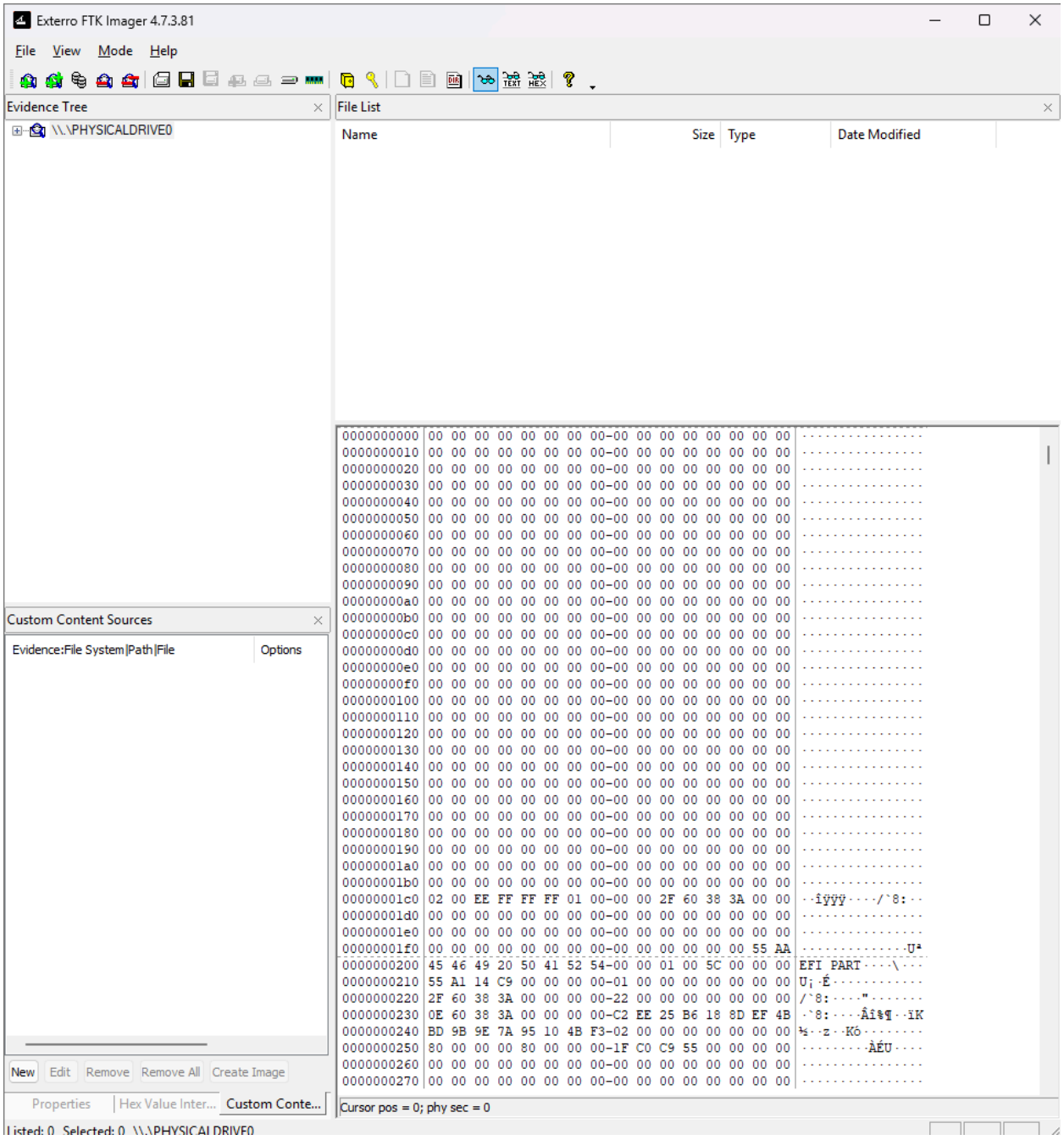

Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

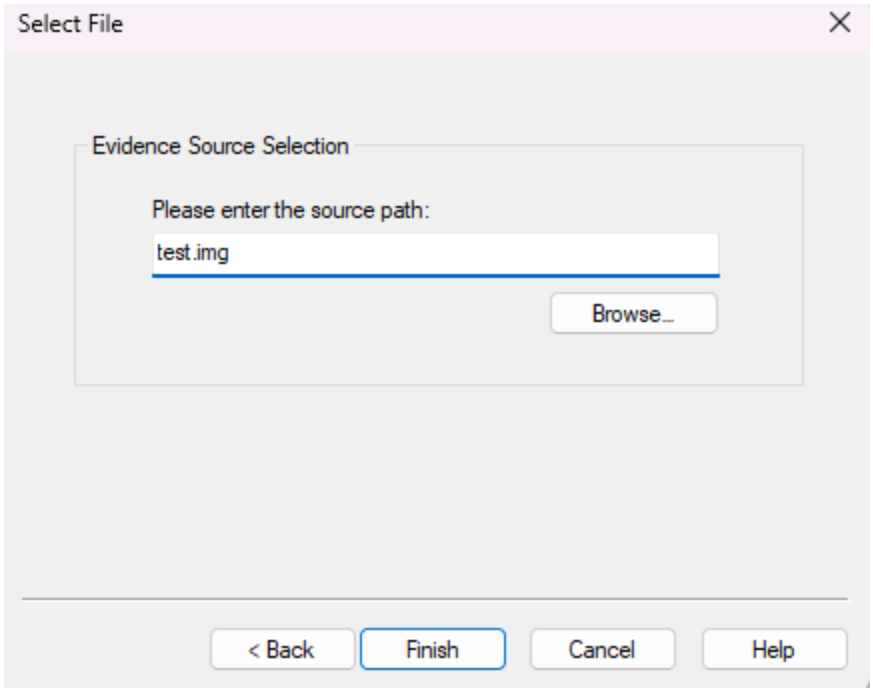

Exterro FTK Imager 4.7.3.81
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

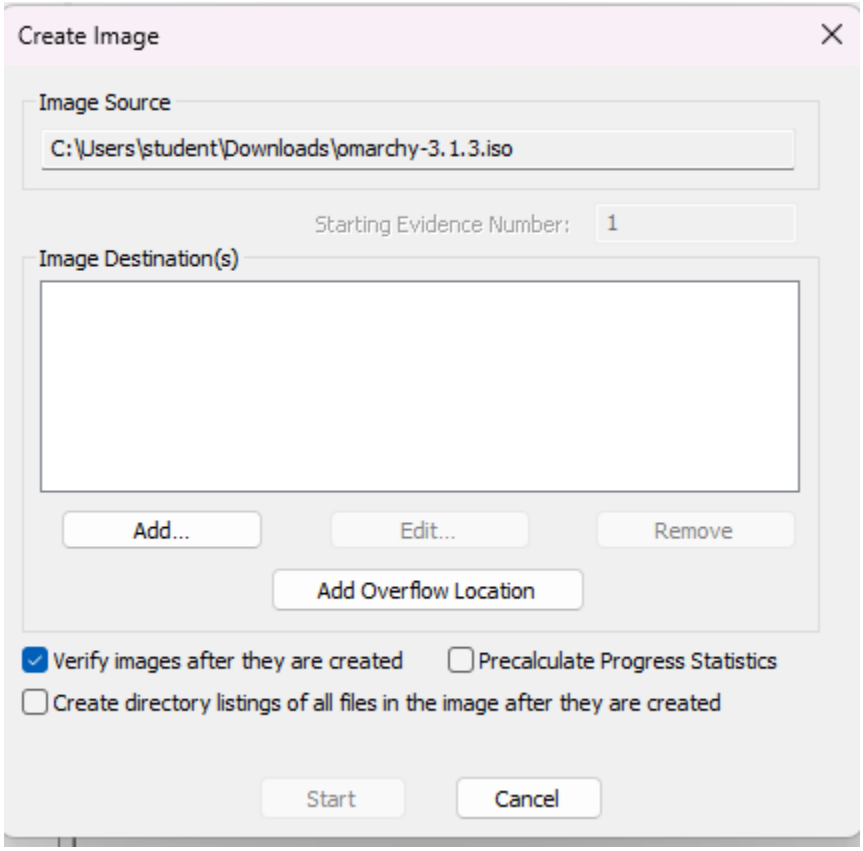

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help

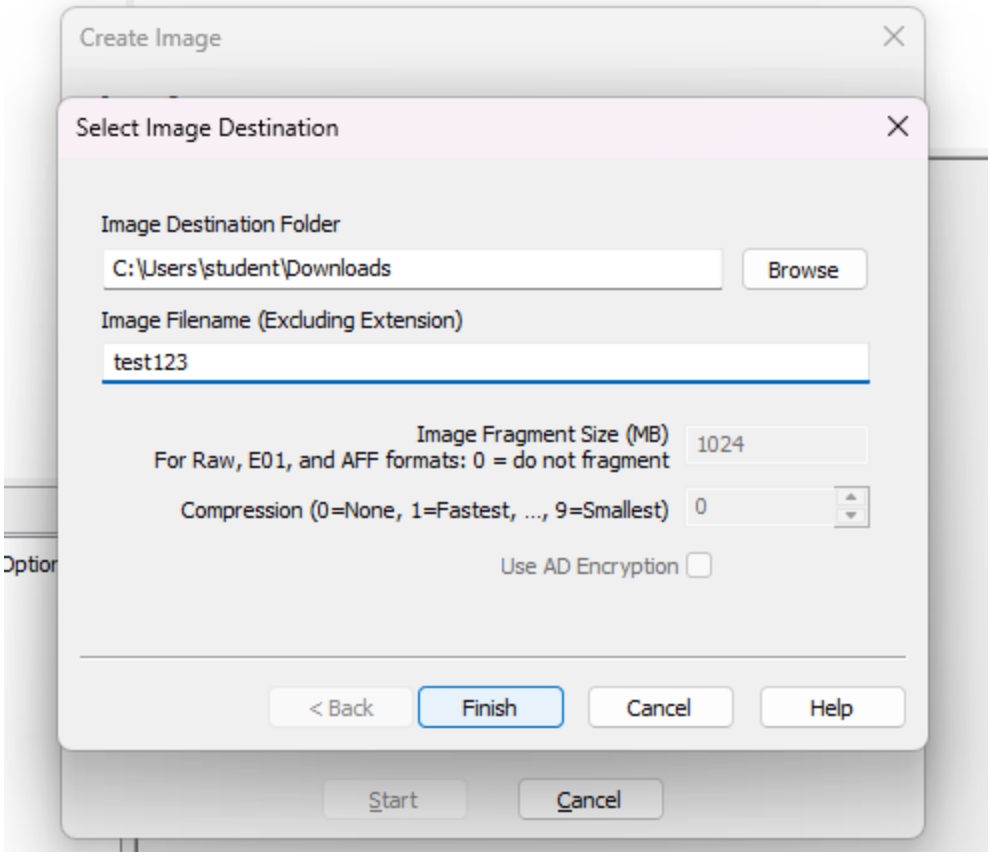

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

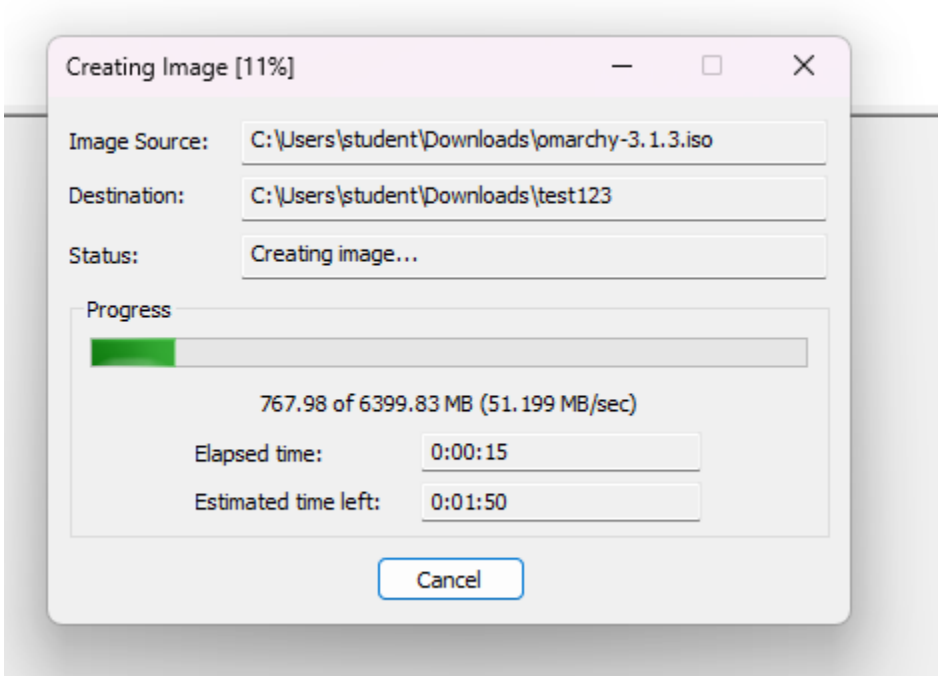

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - HP SSD S700 500GB [500GB SCSI]
< Back
Finish
Cancel
Help

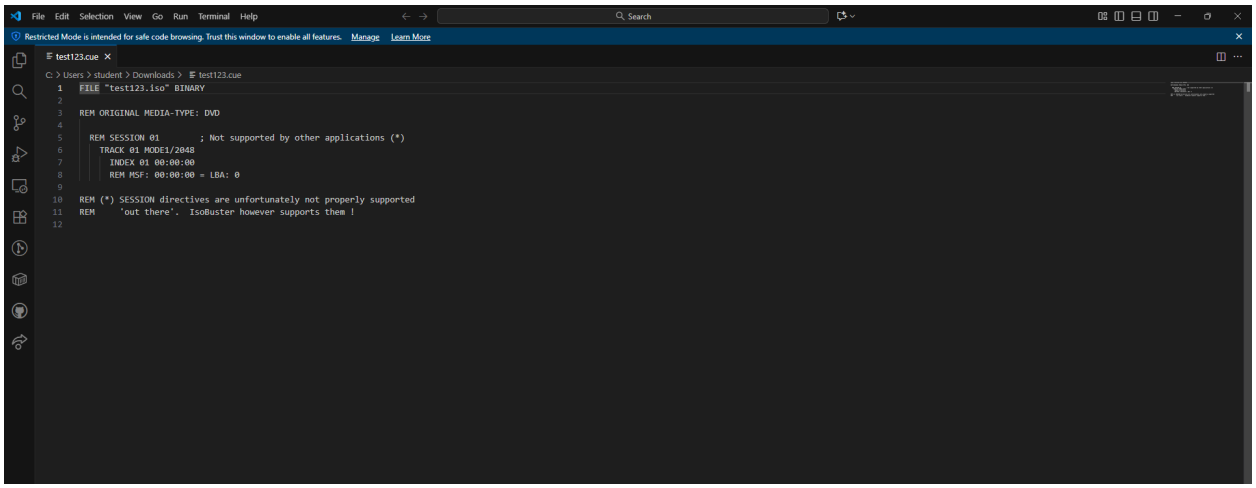

Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

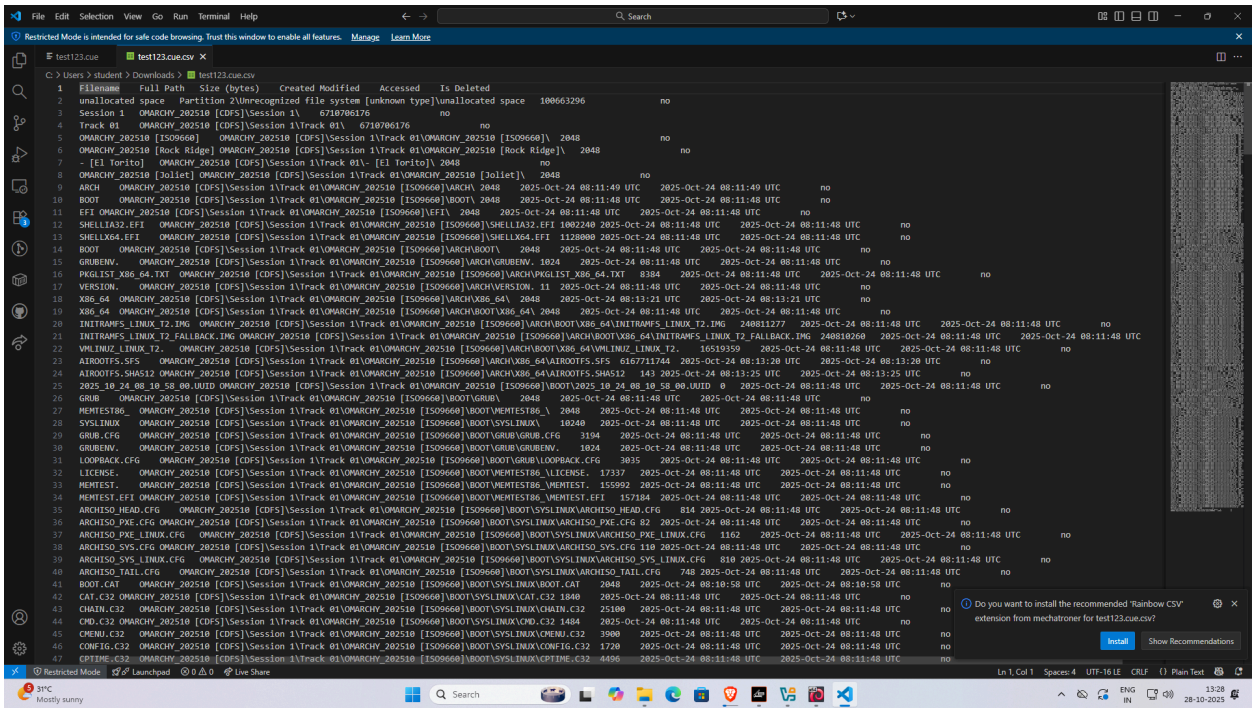

Select File
Evidence Source Selection
Please enter the source path:
test.img
Browse...
< Back
Finish
Cancel
Help

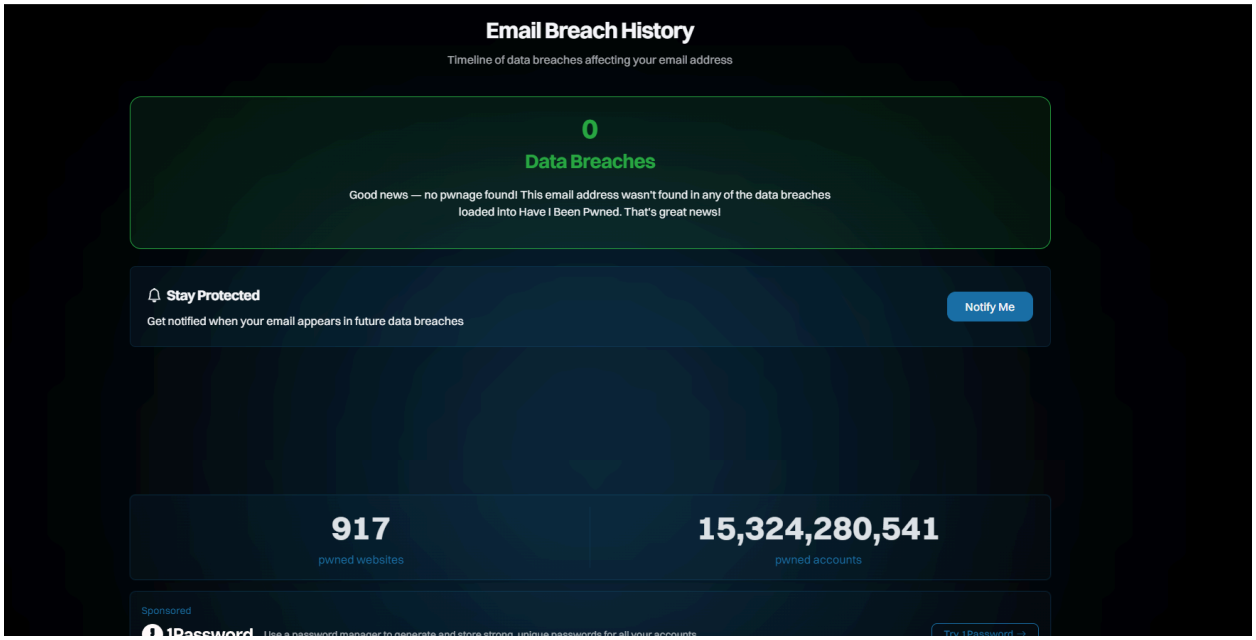

Create Image
Image Source
C:\Users\student\Downloads\omarchy-3.1.3.iso
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Create Image
Select Image Destination
Image Destination Folder
C:\Users\student\Downloads
Browse
Image Filename (Excluding Extension)
test123
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1024
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Back
Finish
Cancel
Help
Start
Cancel


Creating Image [11%]
Image Source:
C:\Users\student\Downloads\omarchy-3.1.3.iso
Destination:
C:\Users\student\Downloads\test123
Status:
Creating image...
Progress
767.98 of 6399.83 MB (51.199 MB/sec)
Elapsed time:
0:00:15
Estimated time left:
0:01:50
Cancel


File Edit Selection View Go Run Terminal Help
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
test123.cue
Users > student > Downloads > test123.cue
FILE "test123.iso" BINARY
REM ORIGINAL MEDIA-TYPE: DVD
REM SESSION 01 ; Not supported by other applications (*)
TRACK 01 MODE1/2048
INDEX 01 00:00:00
REM MSF: 00:00:00 = LBA: 0
REM (*) SESSION directives are unfortunately not properly supported
REM 'out there'. IsoBuster however supports them !


File Edit Selection View Go Run Terminal Help
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
test123.cue
test123.cue.csv
Users > student > Downloads > test123.cue.csv
Filename Full Path Size (bytes) Created Modified Accessed Is Deleted
unallocated space Partition 2\Unrecognized file system [unknown type]\unallocated space 100663296 no
Session 1 OMARCHY_202510 [CDFS]\Session 1\ 6710706176 no
Track 01 OMARCHY_202510 [CDFS]\Session 1\Track 01\ 6710706176 no
OMARCHY_202510 [ISO9660] OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ 2048 no
OMARCHY_202510 [Rock Ridge] OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [Rock Ridge]\ 2048 no
- [El Torito] OMARCHY_202510 [CDFS]\Session 1\Track 01\- [El Torito]\ 2048 no
OMARCHY_202510 [Joliet] OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [Joliet]\ 2048 no
ARCH OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\ 2048 2025-Oct-24 08:11:49 UTC 2025-Oct-24 08:11:49 UTC no
BOOT OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
EFI OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\EFI\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
SHELLIA32.EFI OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\SHELLIA32.EFI 1002240 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
SHELLX64.EFI OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\SHELLX64.EFI 1128000 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
BOOT OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\BOOT\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
GRUBENV. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\GRUBENV. 1024 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
PKGLIST_X86_64.TXT OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\PKGLIST_X86_64.TXT 8384 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
VERSION. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\VERSION. 11 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
X86_64 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\X86_64\ 2048 2025-Oct-24 08:13:21 UTC 2025-Oct-24 08:13:21 UTC no
X86_64 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\BOOT\X86_64\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
INITRAMFS_LINUX_T2.IMG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\BOOT\X86_64\INITRAMFS_LINUX_T2.IMG 240811277 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
INITRAMFS_LINUX_T2_FALLBACK.IMG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\BOOT\X86_64\INITRAMFS_LINUX_T2_FALLBACK.IMG 240810260 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC
VMLINUZ_LINUX_T2. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\BOOT\X86_64\VMLINUZ_LINUX_T2. 16519359 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
AIROOTFS.SFS OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\X86_64\AIROOTFS.SFS 6167711744 2025-Oct-24 08:13:20 UTC 2025-Oct-24 08:13:20 UTC no
AIROOTFS.SHA512 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\ARCH\X86_64\AIROOTFS.SHA512 143 2025-Oct-24 08:13:25 UTC 2025-Oct-24 08:13:25 UTC no
2025_10_24_08_10_58_00.UUID OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\2025_10_24_08_10_58_00.UUID 0 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
GRUB OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\GRUB\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
MEMTEST86_ OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\MEMTEST86_\ 2048 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
SYSLINUX OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ 10240 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
GRUB.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\GRUB\GRUB.CFG 3194 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
GRUBENV. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\GRUB\GRUBENV. 1024 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
LOOPBACK.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\GRUB\LOOPBACK.CFG 3035 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
LICENSE. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\MEMTEST86_\LICENSE. 17337 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
MEMTEST. OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\MEMTEST86_\MEMTEST. 155992 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
MEMTEST.EFI OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\MEMTEST86_\MEMTEST.EFI 157184 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_HEAD.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_HEAD.CFG 814 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_PXE.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_PXE.CFG 82 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_PXE_LINUX.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_PXE_LINUX.CFG 1162 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_SYS.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_SYS.CFG 110 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_SYS_LINUX.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_SYS_LINUX.CFG 810 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
ARCHISO_TAIL.CFG OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\ARCHISO_TAIL.CFG 748 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
BOOT.CAT OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\BOOT.CAT 2048 2025-Oct-24 08:10:58 UTC 2025-Oct-24 08:10:58 UTC no
CAT.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CAT.C32 1840 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
CHAIN.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CHAIN.C32 25100 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
CMD.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CMD.C32 1484 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
CMENU.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CMENU.C32 3900 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
CONFIG.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CONFIG.C32 1720 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
CPTIME.C32 OMARCHY_202510 [CDFS]\Session 1\Track 01\OMARCHY_202510 [ISO9660]\BOOT\SYSLINUX\CPTIME.C32 4496 2025-Oct-24 08:11:48 UTC 2025-Oct-24 08:11:48 UTC no
Do you want to install the recommended 'Rainbow CSV' extension from mechatroner for test123.cue.csv?
Install
Show Recommendations
Restricted Mode
Launchpad
Live Share
Ln 1, Col 1
Spaces: 4
UTF-16 LE
CRLF
Plain Text
31°C
Mostly sunny
Search
ENG
IN
13:28
28-10-2025



12.7 Conclusion:

Understanding how to geolocate IP addresses aids in identifying the physical location relevant to cyber incidents, which is essential for pinpointing suspects or compromised systems.

Analyzing email headers reveals detailed information about the route and authenticity of emails, helping to detect phishing, spoofing, or unauthorized access.

Recovering browser search history provides crucial insights into user intent, digital footprints, and evidence of potential malicious activities or information gathering.

Collectively, these methods empower forensic investigators to construct a comprehensive timeline and narrative of cyber events, supporting accurate incident resolution and legal proceedings.

Effective use of these techniques is vital to maintaining cybersecurity and supporting law enforcement efforts in today’s cloud-centric digital environment.