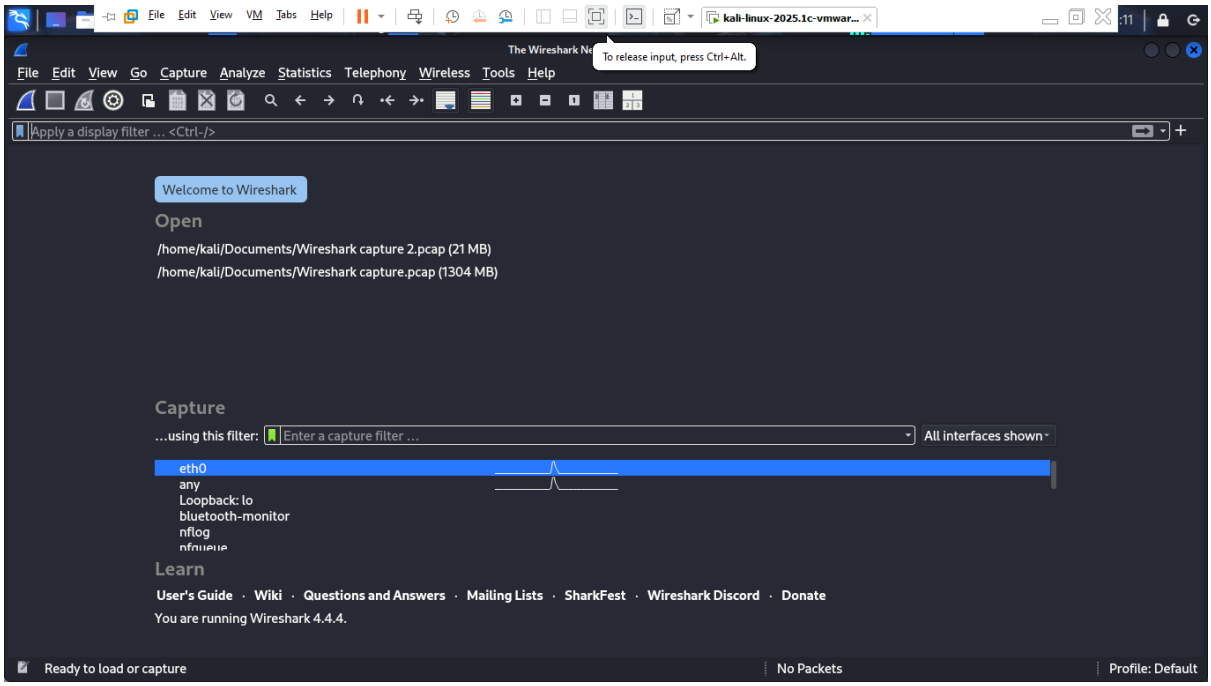
1. Install Wireshark

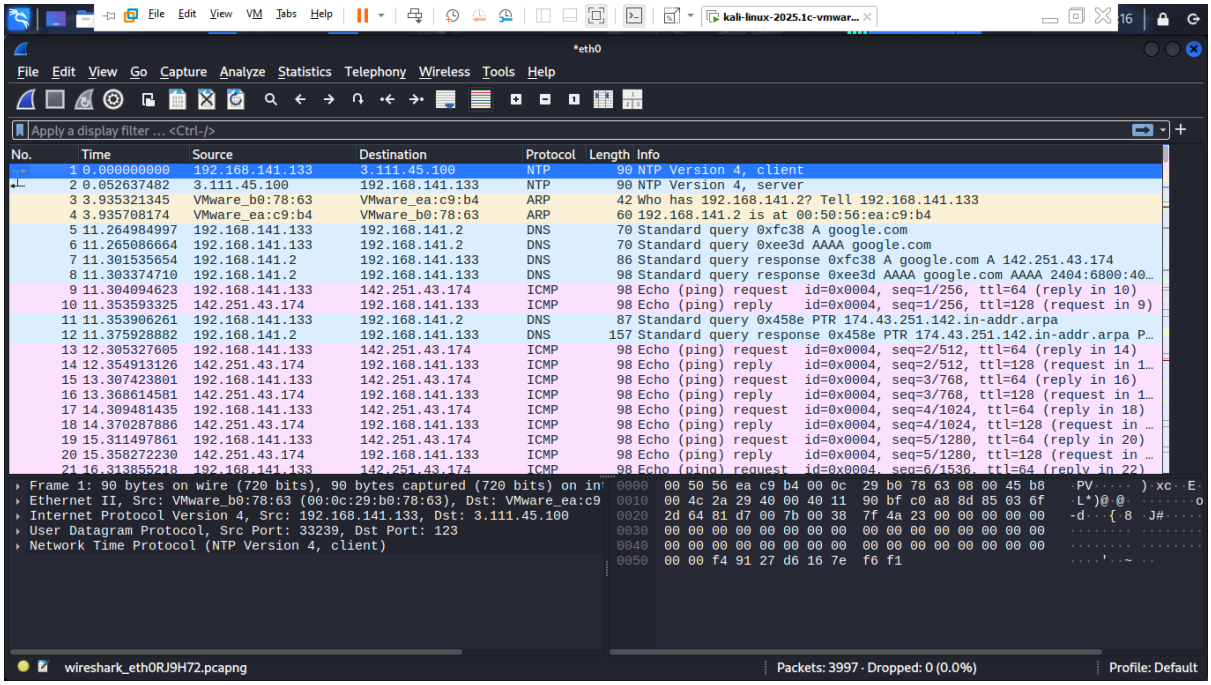
Command used : sudo apt update

sudo apt install wireshark

Here, in our case, wireshark is pre-installed in Kali Linux

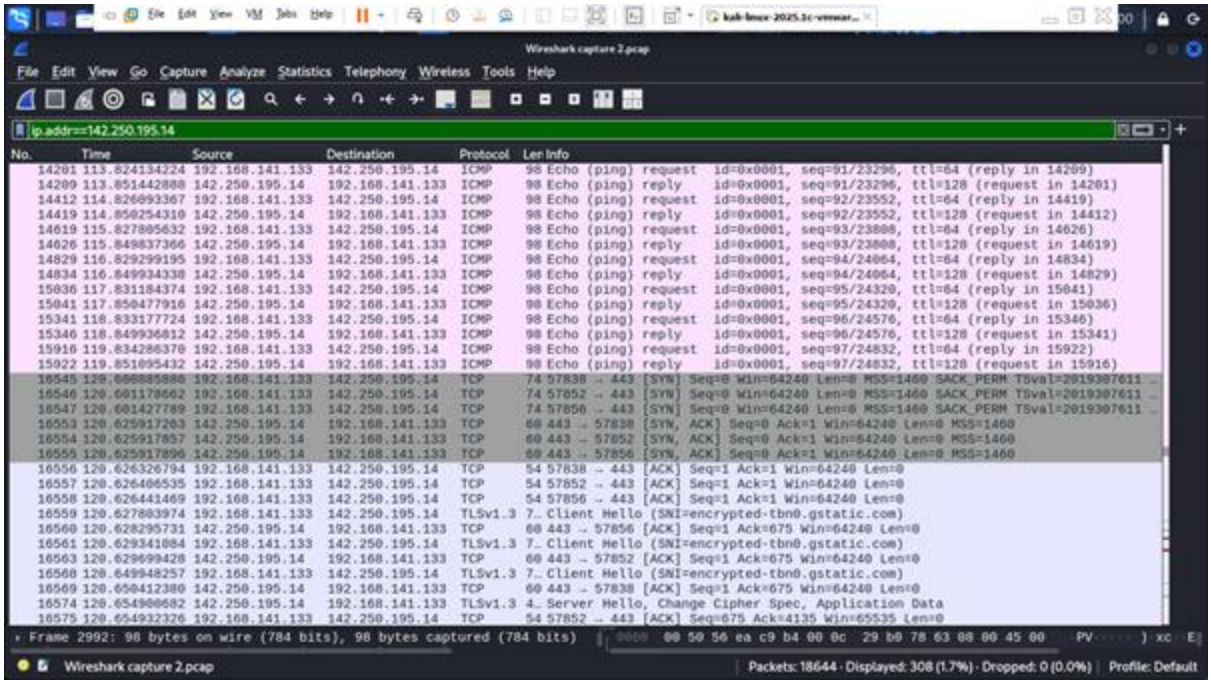
2. Start capturing on active netowrk interface



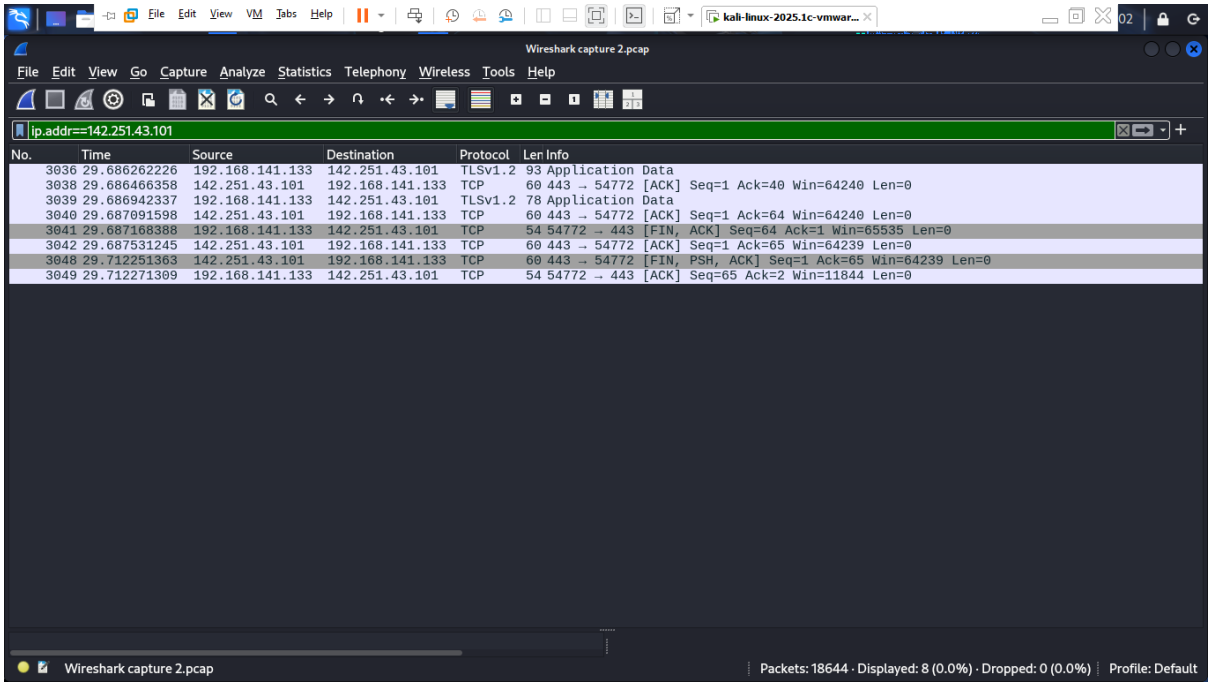


3. Browse a website or ping a website

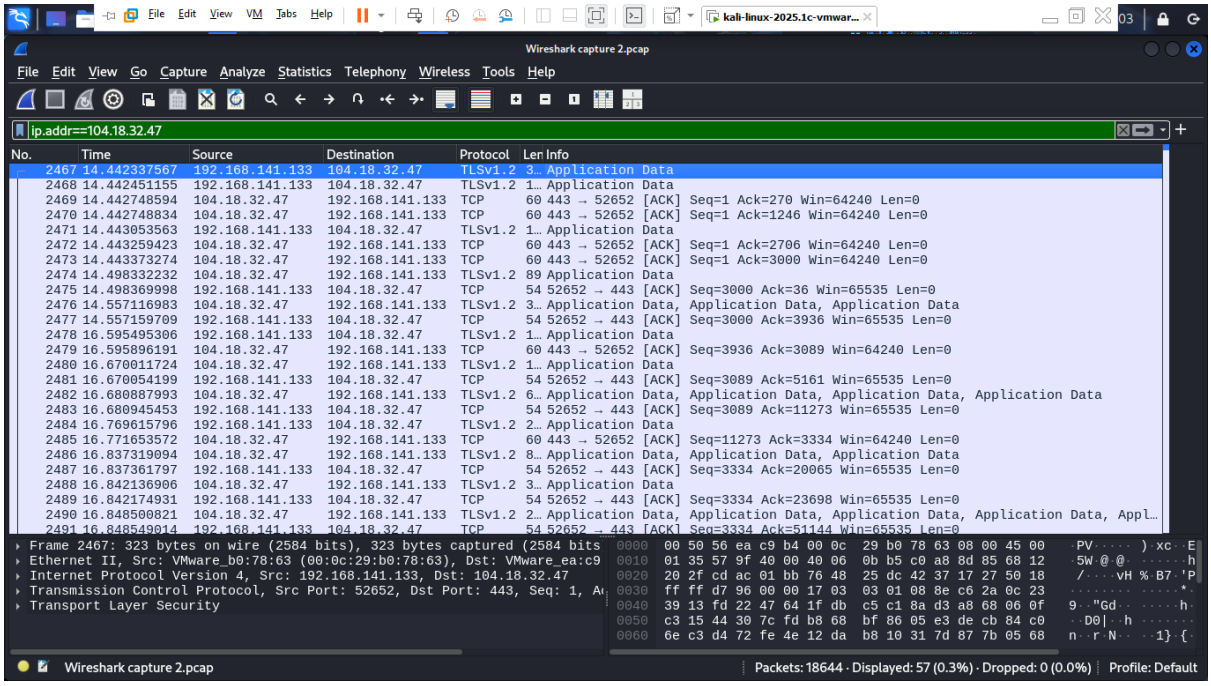
3.1 Ping request for google.com



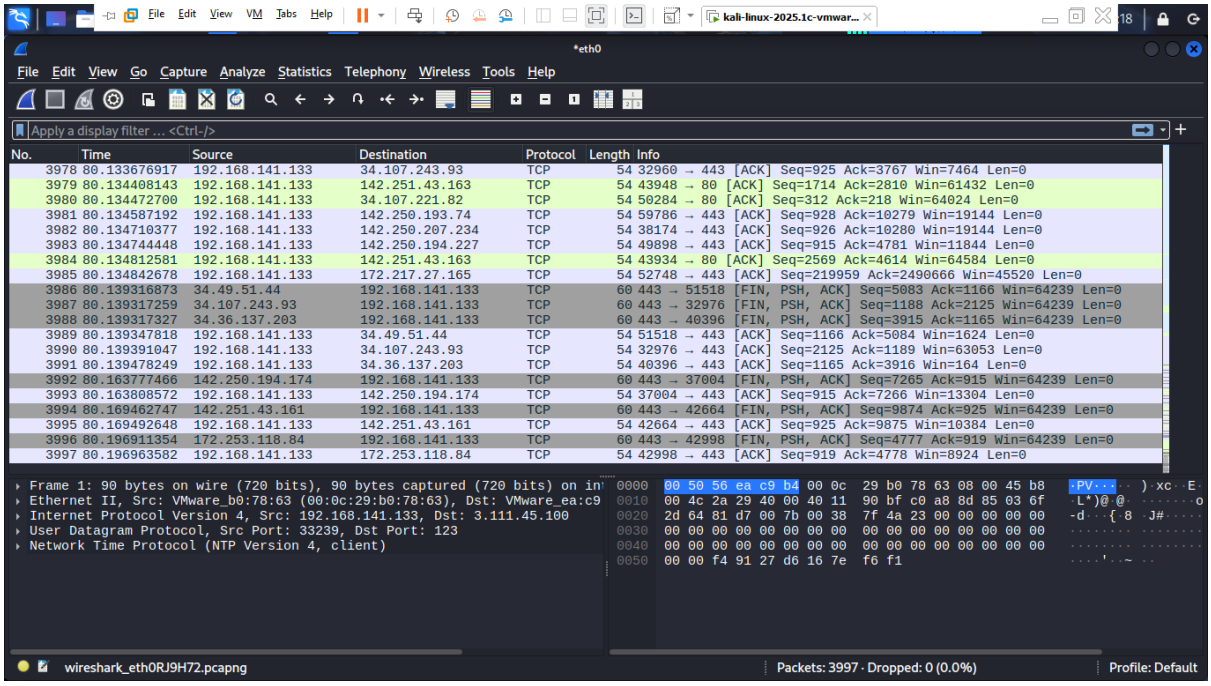
3.2 Ping request for gmail.com



3.3 Ping request for chatgpt.com

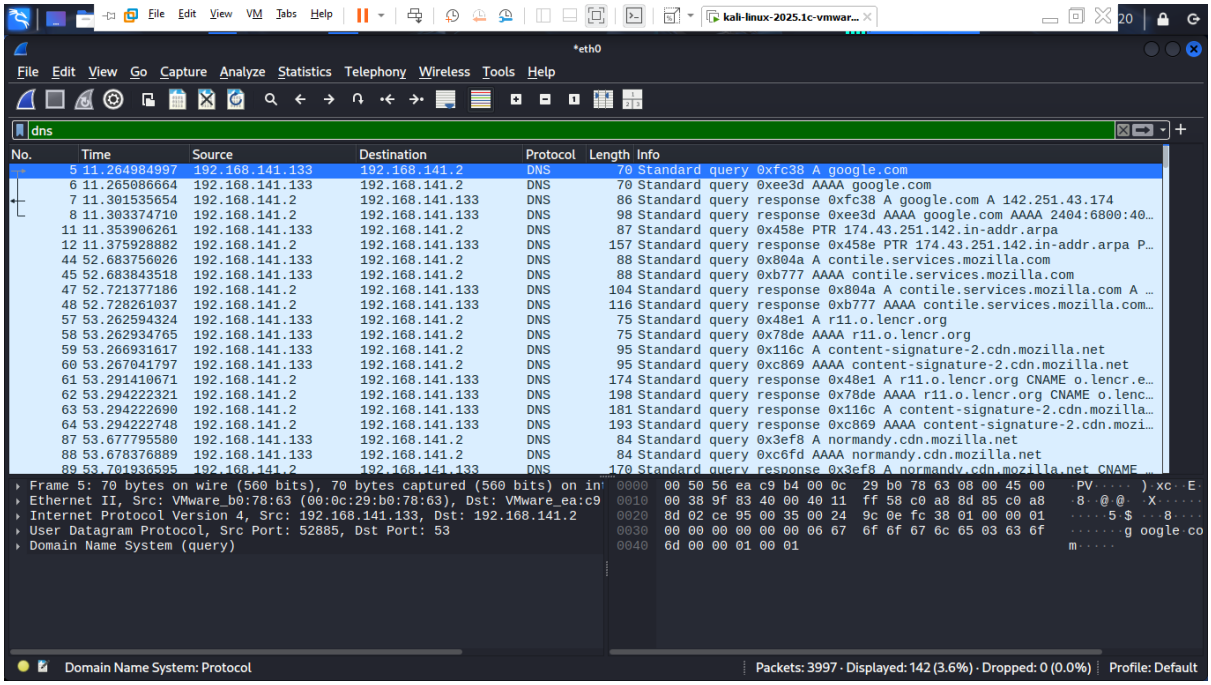


4. Stop capturing after sometime

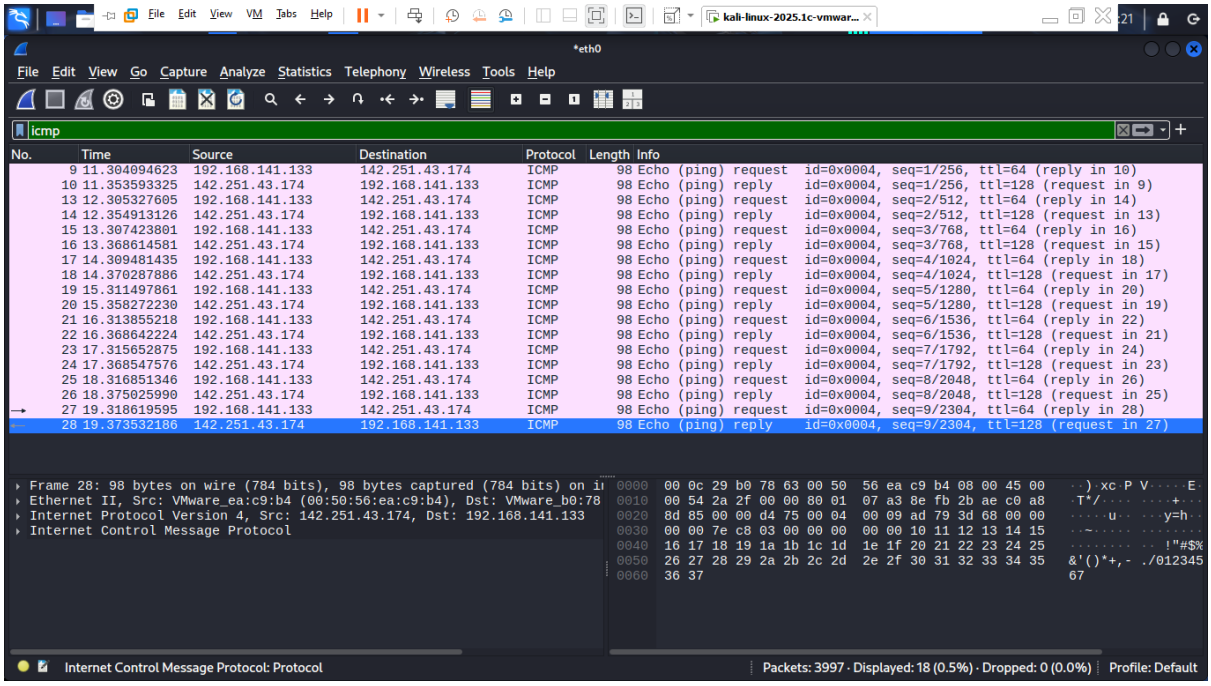


5. Filter by different protocol type

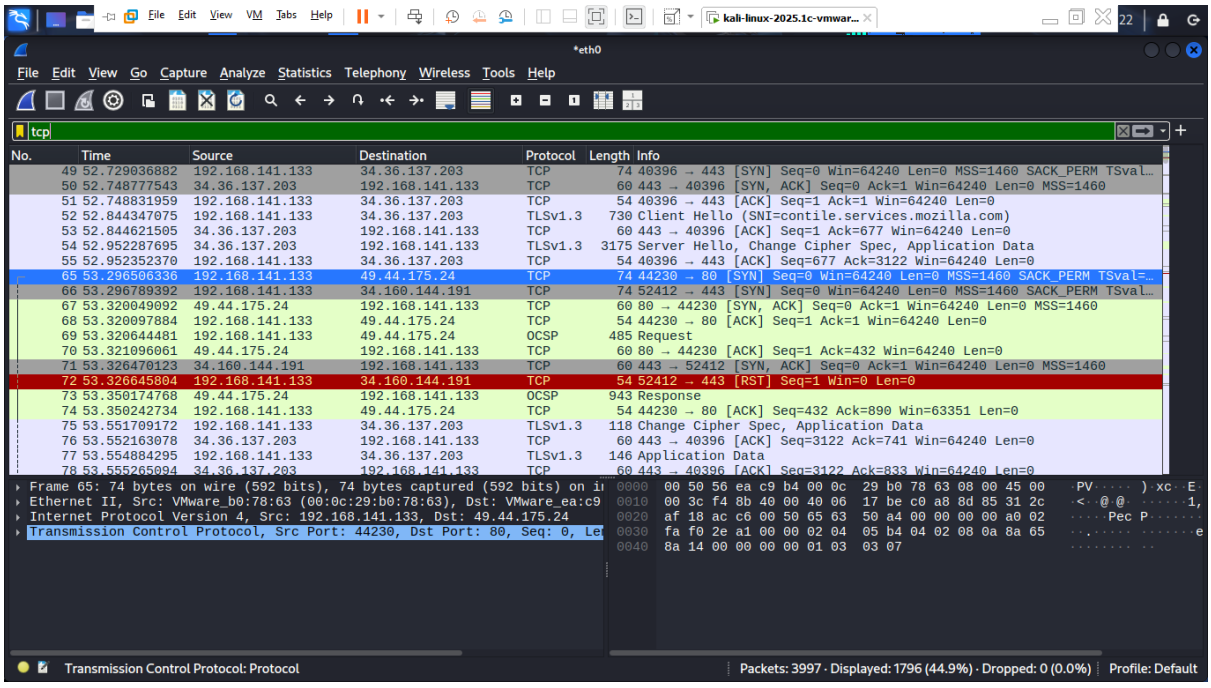
5.1 DNS



5.2 ICMP

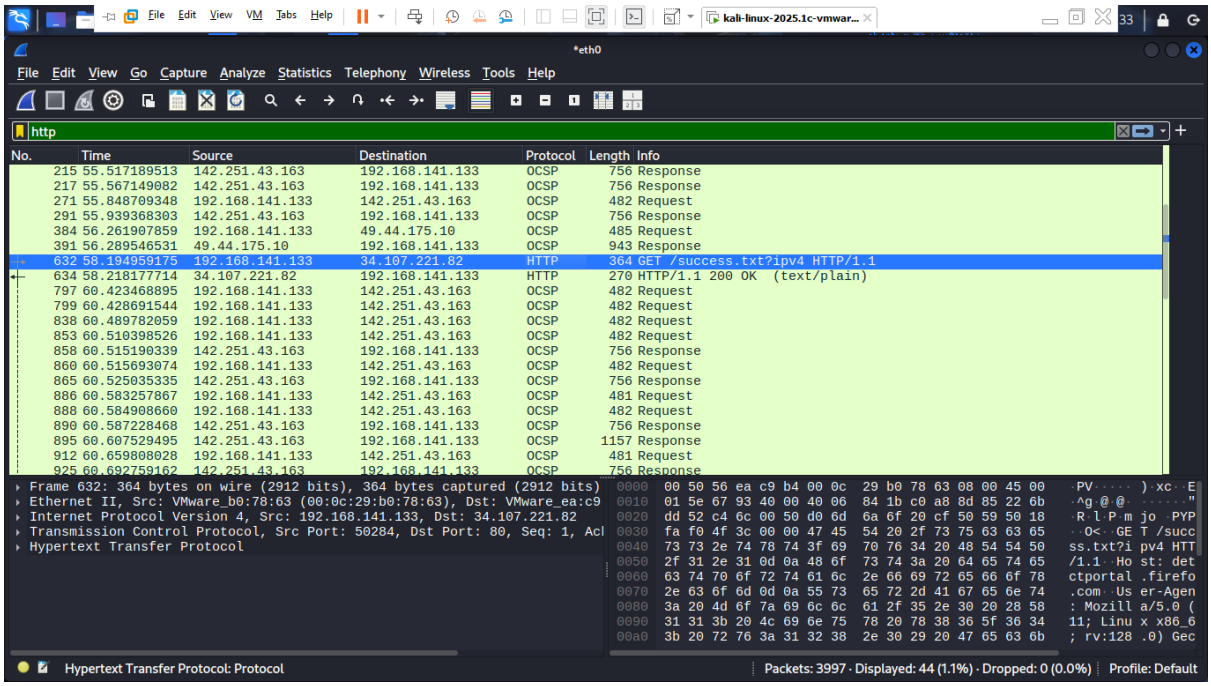

File Edit View VM Tabs Help
kali-linux-2025.1c-vmwar...
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
9 11.304094623 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 10)
10 11.353593325 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=1/256, ttl=128 (request in 9)
13 12.305327605 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 14)
14 12.354913126 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=2/512, ttl=128 (request in 13)
15 13.307423801 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 16)
16 13.368614581 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=3/768, ttl=128 (request in 15)
17 14.309481435 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (reply in 18)
18 14.370287886 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=4/1024, ttl=128 (request in 17)
19 15.311497861 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=5/1280, ttl=64 (reply in 20)
20 15.358272230 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=5/1280, ttl=128 (request in 19)
21 16.313855218 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=6/1536, ttl=64 (reply in 22)
22 16.368642224 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=6/1536, ttl=128 (request in 21)
23 17.315652875 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=7/1792, ttl=64 (reply in 24)
24 17.368547576 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=7/1792, ttl=128 (request in 23)
25 18.316851346 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=8/2048, ttl=64 (reply in 26)
26 18.375025990 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=8/2048, ttl=128 (request in 25)
27 19.318619595 192.168.141.133 142.251.43.174 ICMP 98 Echo (ping) request id=0x0004, seq=9/2304, ttl=64 (reply in 28)
28 19.373532186 142.251.43.174 192.168.141.133 ICMP 98 Echo (ping) reply id=0x0004, seq=9/2304, ttl=128 (request in 27)
Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on i
Ethernet II, Src: VMware_ea:c9:b4 (00:50:56:ea:c9:b4), Dst: VMware_b0:78
Internet Protocol Version 4, Src: 142.251.43.174, Dst: 192.168.141.133
Internet Control Message Protocol
0000 00 0c 29 b0 78 63 00 50 56 ea c9 b4 08 00 45 00
0010 00 54 2a 2f 00 00 80 01 07 a3 8e fb 2b ae c0 a8
0020 8d 85 00 00 d4 75 00 04 00 09 ad 79 3d 68 00 00
0030 00 00 7e c8 03 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37
Internet Control Message Protocol: Protocol
Packets: 3997 · Displayed: 18 (0.5%) · Dropped: 0 (0.0%)
Profile: Default

5.3 TCP

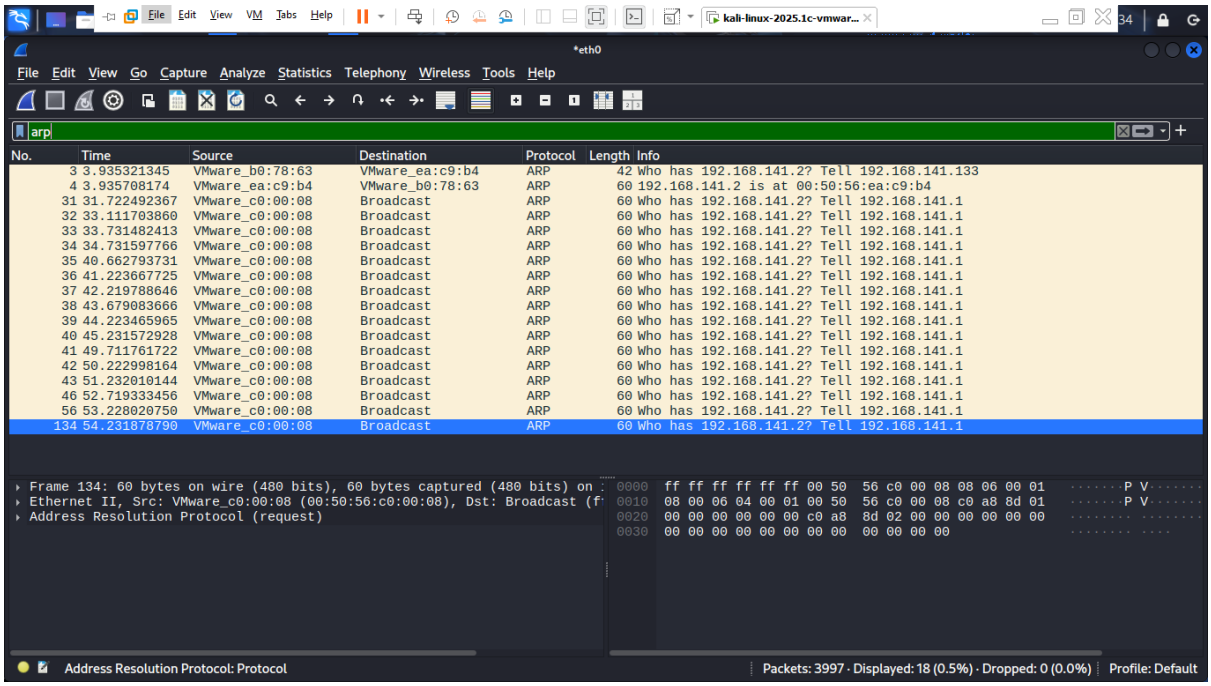

File Edit View VM Tabs Help
kali-linux-2025.1c-vmwar...
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
49 52.729036882 192.168.141.133 34.36.137.203 TCP 74 40396 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval…
50 52.748777543 34.36.137.203 192.168.141.133 TCP 60 443 → 40396 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
51 52.748831959 192.168.141.133 34.36.137.203 TCP 54 40396 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
52 52.844347075 192.168.141.133 34.36.137.203 TLSv1.3 730 Client Hello (SNI=contile.services.mozilla.com)
53 52.844621505 34.36.137.203 192.168.141.133 TCP 60 443 → 40396 [ACK] Seq=1 Ack=677 Win=64240 Len=0
54 52.952287695 34.36.137.203 192.168.141.133 TLSv1.3 3175 Server Hello, Change Cipher Spec, Application Data
55 52.952352370 192.168.141.133 34.36.137.203 TCP 54 40396 → 443 [ACK] Seq=677 Ack=3122 Win=64240 Len=0
65 53.296506336 192.168.141.133 49.44.175.24 TCP 74 44230 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=…
66 53.296789392 192.168.141.133 34.160.144.191 TCP 74 52412 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval…
67 53.320049092 49.44.175.24 192.168.141.133 TCP 60 80 → 44230 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
68 53.320097884 192.168.141.133 49.44.175.24 TCP 54 44230 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
69 53.320644481 192.168.141.133 49.44.175.24 OCSP 485 Request
70 53.321096061 49.44.175.24 192.168.141.133 TCP 60 80 → 44230 [ACK] Seq=1 Ack=432 Win=64240 Len=0
71 53.326470123 34.160.144.191 192.168.141.133 TCP 60 443 → 52412 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
72 53.326645804 192.168.141.133 34.160.144.191 TCP 54 52412 → 443 [RST] Seq=1 Win=0 Len=0
73 53.350174768 49.44.175.24 192.168.141.133 OCSP 943 Response
74 53.350242734 192.168.141.133 49.44.175.24 TCP 54 44230 → 80 [ACK] Seq=432 Ack=890 Win=63351 Len=0
75 53.551709172 192.168.141.133 34.36.137.203 TLSv1.3 118 Change Cipher Spec, Application Data
76 53.552163078 34.36.137.203 192.168.141.133 TCP 60 443 → 40396 [ACK] Seq=3122 Ack=741 Win=64240 Len=0
77 53.554884295 192.168.141.133 34.36.137.203 TLSv1.3 146 Application Data
78 53.555265094 34.36.137.203 192.168.141.133 TCP 60 443 → 40396 [ACK] Seq=3122 Ack=833 Win=64240 Len=0
Frame 65: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
Ethernet II, Src: VMware_b0:78:63 (00:0c:29:b0:78:63), Dst: VMware_ea:c9
Internet Protocol Version 4, Src: 192.168.141.133, Dst: 49.44.175.24
Transmission Control Protocol, Src Port: 44230, Dst Port: 80, Seq: 0, Le
0000 00 50 56 ea c9 b4 00 0c 29 b0 78 63 08 00 45 00
0010 00 3c f4 8b 40 00 40 06 17 be c0 a8 8d 85 31 2c
0020 af 18 ac c6 00 50 65 63 50 a4 00 00 00 00 a0 02
0030 fa f0 2e a1 00 00 02 04 05 b4 04 02 08 0a 8a 65
0040 8a 14 00 00 00 00 01 03 03 07
Transmission Control Protocol: Protocol
Packets: 3997 · Displayed: 1796 (44.9%) · Dropped: 0 (0.0%)
Profile: Default

6. Identify at least 3 different protocols

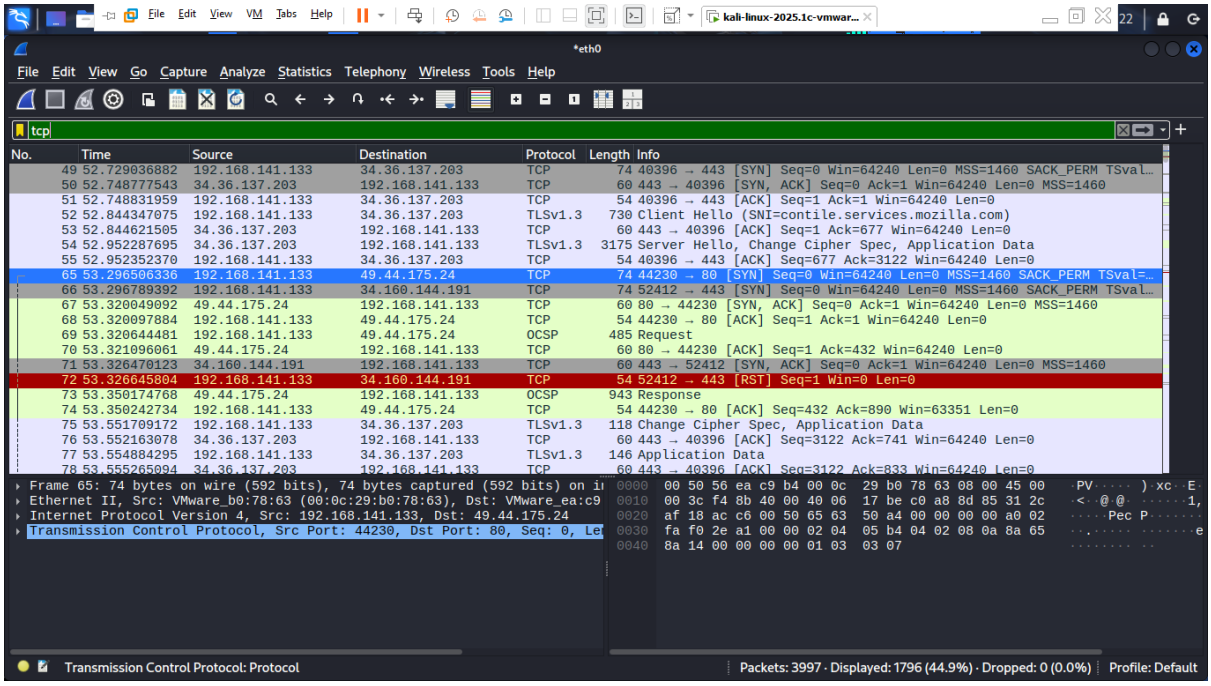
6.1 HTTP



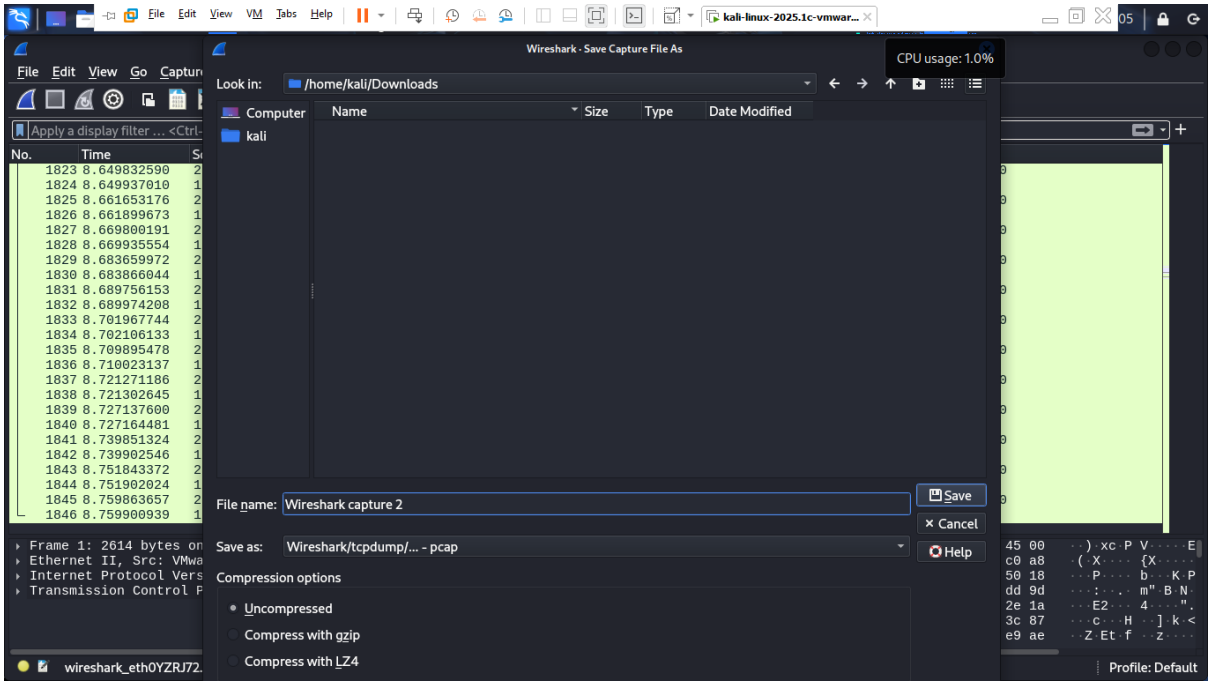
6.2 ARP



6.3 TCP



7. Exporting the packet capture as .pcap file



8. Summarize your findings and packet details.

- The Wireshark capture session successfully demonstrated the process of monitoring network activity on a Linux system.
- The capture included essential steps such as installing Wireshark, initiating a live capture on an active network interface, and generating traffic by pinging well-known websites like Google, Gmail, and ChatGPT. During the session, traffic was filtered based on protocol types such as DNS, ICMP, and TCP to observe how each behaves in a typical communication flow.
- Further inspection of the packet capture revealed additional network protocols like HTTPS and ARP, providing a broader view of the network interactions occurring during the session.
- The exercise culminated with the export of the capture into a .pcap file, offering a practical understanding of traffic analysis, protocol behaviour, and packet structure for network troubleshooting and educational purposes.