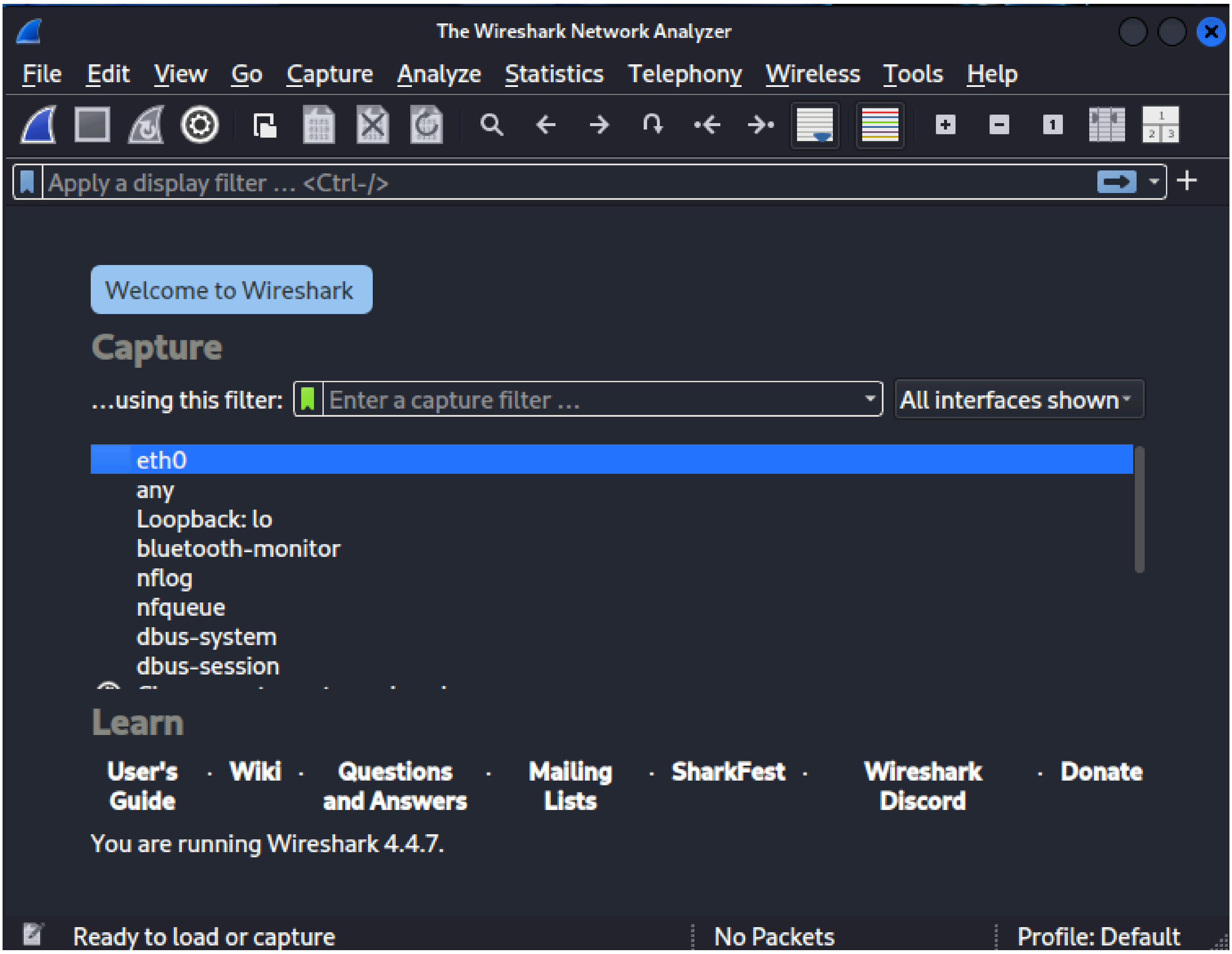
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-5:

1.Install Wireshark.

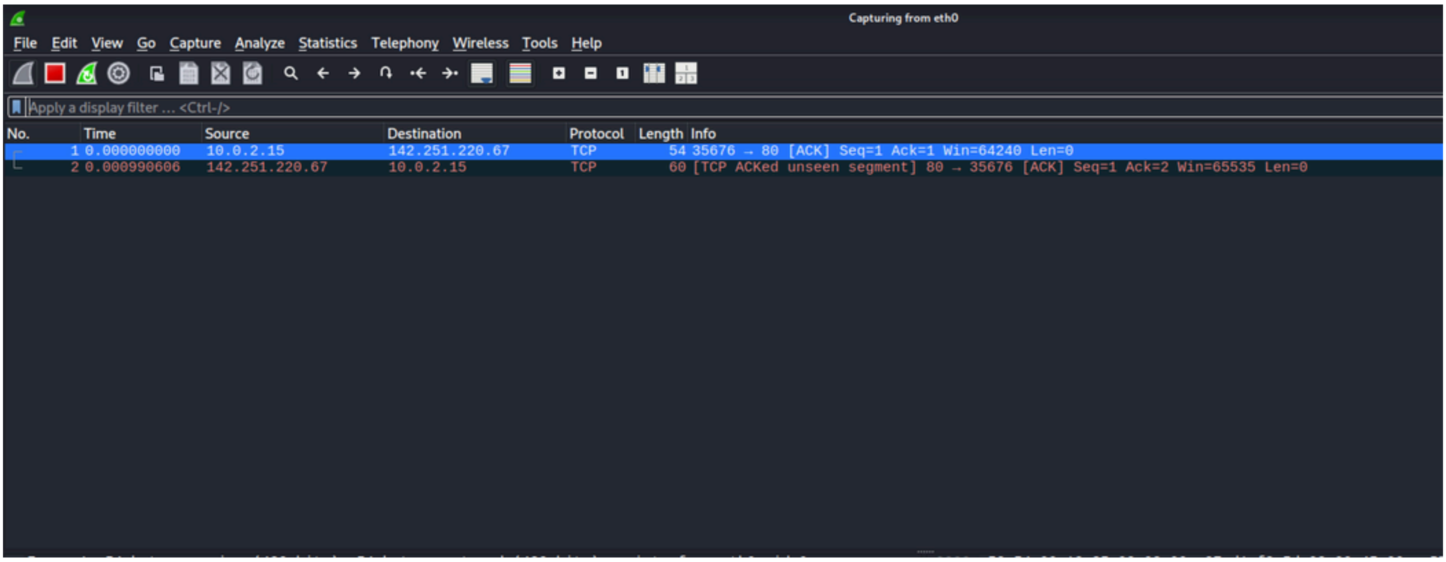
It is an inbuilt tool in the kali linux.



You are running Wireshark 4.4.7.

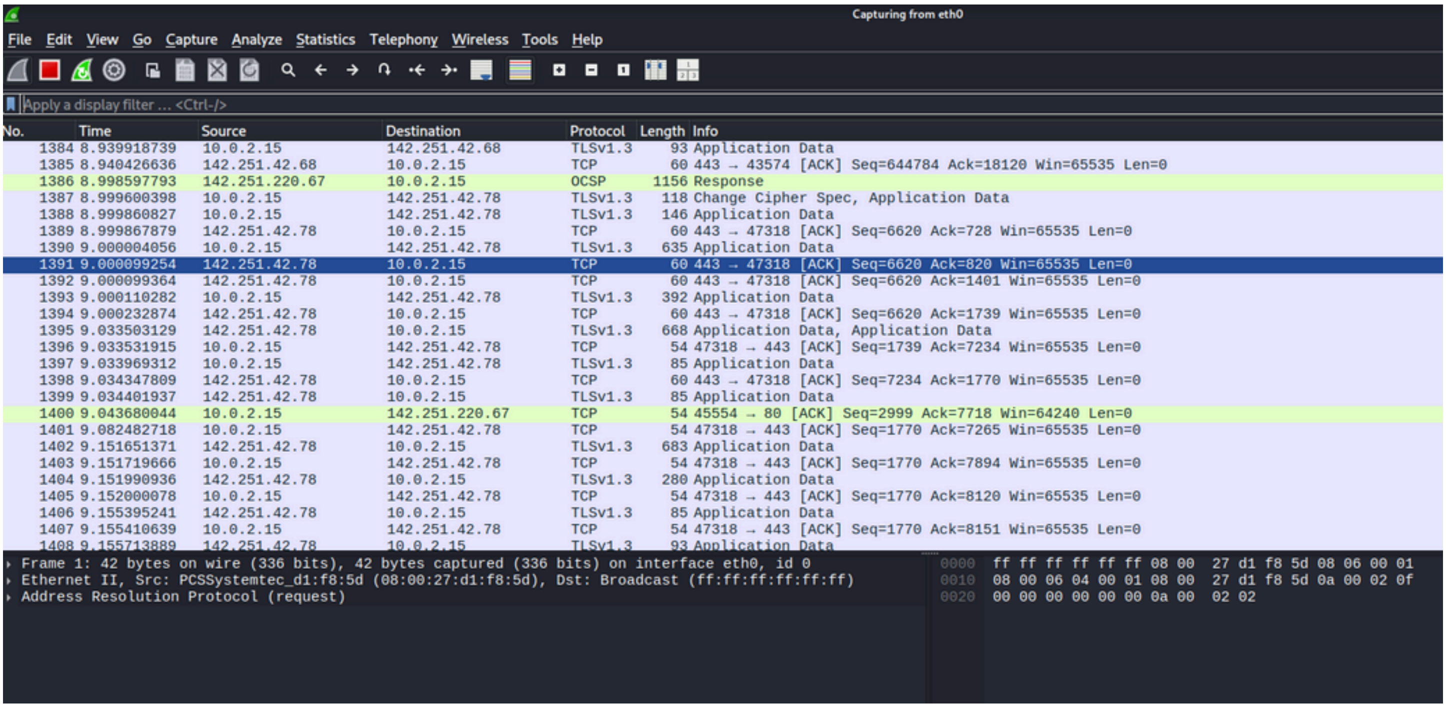
Ready to load or capture

2.Start capturing on your active network interface.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source           Destination      Protocol  Length Info
   1 0.000000000   10.0.2.15        142.251.220.67   TCP           54 35676 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   2 0.000990606   142.251.220.67   10.0.2.15        TCP           60 [TCP ACKed unseen segment] 80 → 35676 [ACK] Seq=1 Ack=2 Win=65535 Len=0
```

3.Browse a website or ping a server to generate traffic.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

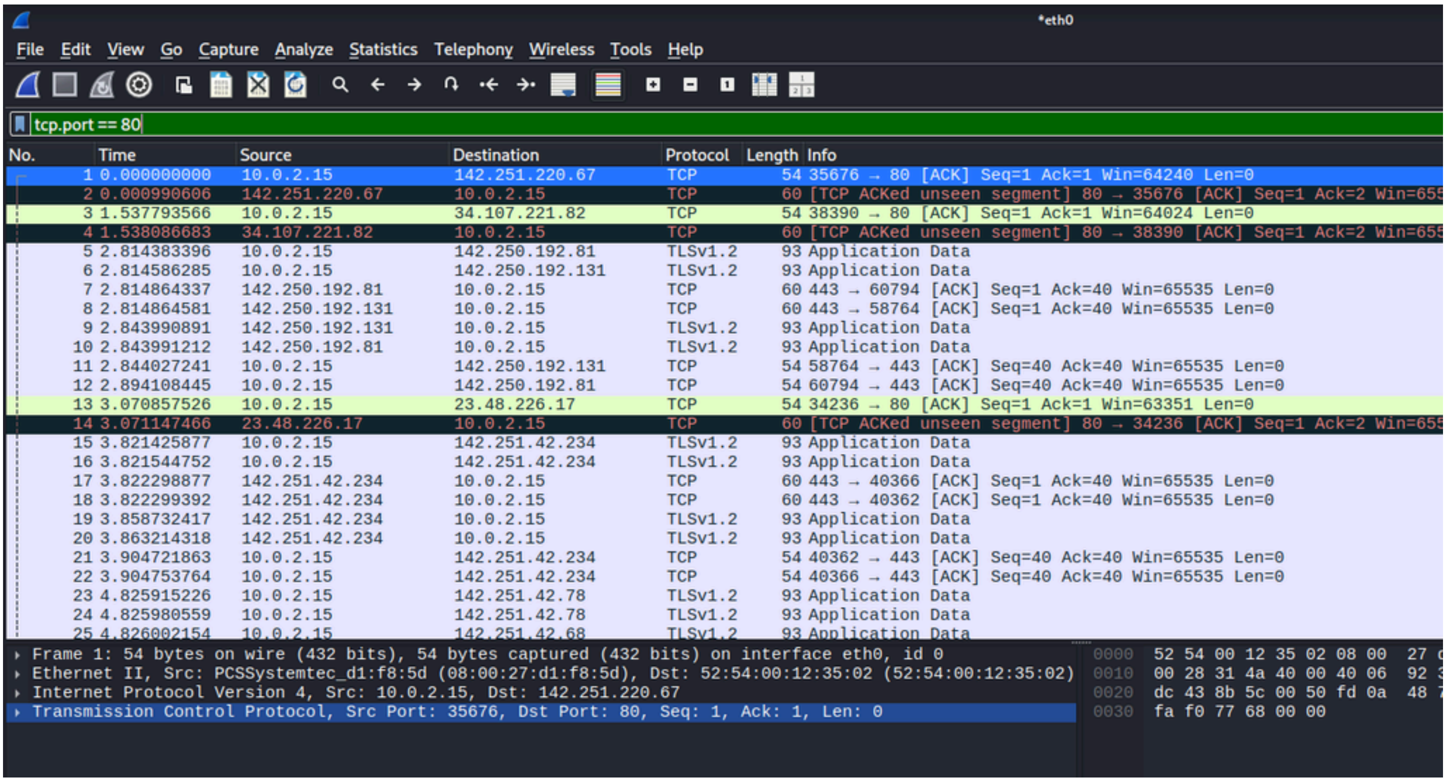
```
No.  Time          Source           Destination      Protocol  Length Info
1384 8.939918739   10.0.2.15        142.251.42.68    TLSv1.3       93 Application Data
1385 8.940426636   142.251.42.68    10.0.2.15        TCP           60 443 → 43574 [ACK] Seq=644784 Ack=18120 Win=65535 Len=0
1386 8.998597793   142.251.220.67   10.0.2.15        OCSP        1156 Response
1387 8.999600398   10.0.2.15        142.251.42.78    TLSv1.3      118 Change Cipher Spec, Application Data
1388 8.999860827   10.0.2.15        142.251.42.78    TLSv1.3      146 Application Data
1389 8.999867879   142.251.42.78    10.0.2.15        TCP           60 443 → 47318 [ACK] Seq=6620 Ack=728 Win=65535 Len=0
1390 9.000004056   10.0.2.15        142.251.42.78    TLSv1.3      635 Application Data
1391 9.000099254   142.251.42.78    10.0.2.15        TCP           60 443 → 47318 [ACK] Seq=6620 Ack=820 Win=65535 Len=0
1392 9.000099364   142.251.42.78    10.0.2.15        TCP           60 443 → 47318 [ACK] Seq=6620 Ack=1401 Win=65535 Len=0
1393 9.000110282   10.0.2.15        142.251.42.78    TLSv1.3      392 Application Data
1394 9.000232874   142.251.42.78    10.0.2.15        TCP           60 443 → 47318 [ACK] Seq=6620 Ack=1739 Win=65535 Len=0
1395 9.033503129   142.251.42.78    10.0.2.15        TLSv1.3      668 Application Data, Application Data
1396 9.033531915   10.0.2.15        142.251.42.78    TCP           54 47318 → 443 [ACK] Seq=1739 Ack=7234 Win=65535 Len=0
1397 9.033969312   10.0.2.15        142.251.42.78    TLSv1.3       85 Application Data
1398 9.034347809   142.251.42.78    10.0.2.15        TCP           60 443 → 47318 [ACK] Seq=7234 Ack=1770 Win=65535 Len=0
1399 9.034401937   142.251.42.78    10.0.2.15        TLSv1.3       85 Application Data
1400 9.043680044   10.0.2.15        142.251.220.67   TCP           54 45554 → 80 [ACK] Seq=2999 Ack=7718 Win=64240 Len=0
1401 9.082482718   10.0.2.15        142.251.42.78    TCP           54 47318 → 443 [ACK] Seq=1770 Ack=7265 Win=65535 Len=0
1402 9.151651371   142.251.42.78    10.0.2.15        TLSv1.3      683 Application Data
1403 9.151719666   10.0.2.15        142.251.42.78    TCP           54 47318 → 443 [ACK] Seq=1770 Ack=7894 Win=65535 Len=0
1404 9.151990936   142.251.42.78    10.0.2.15        TLSv1.3      280 Application Data
1405 9.152000078   10.0.2.15        142.251.42.78    TCP           54 47318 → 443 [ACK] Seq=1770 Ack=8120 Win=65535 Len=0
1406 9.155395241   142.251.42.78    10.0.2.15        TLSv1.3       85 Application Data
1407 9.155410639   10.0.2.15        142.251.42.78    TCP           54 47318 → 443 [ACK] Seq=1770 Ack=8151 Win=65535 Len=0
1408 9.155713889   142.251.42.78    10.0.2.15        TLSv1.3       93 Application Data
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 d1 f8 5d 08 06 00 01
0010  08 00 06 04 00 01 08 00  27 d1 f8 5d 0a 00 02 0f
0020  00 00 00 00 00 00 0a 00  02 02
```

4.Stop capture after a minute.

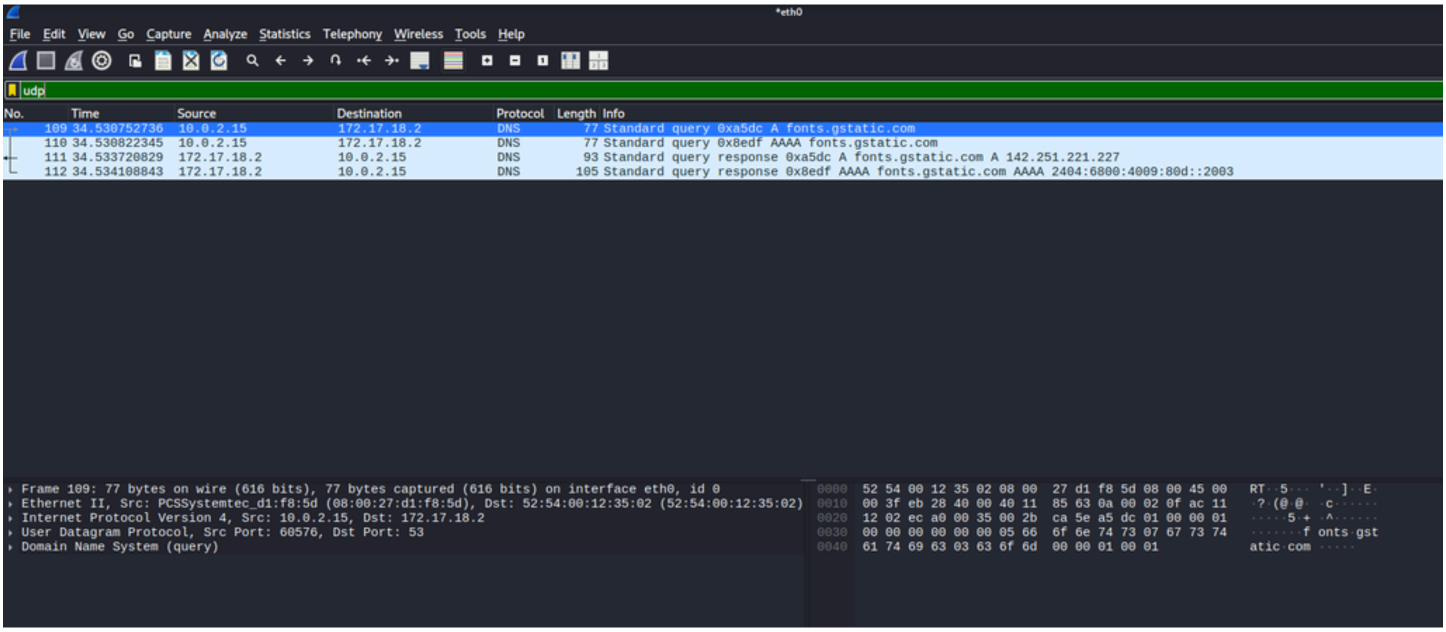
5.Filter captured packets by protocol.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80

```
No.  Time         Source           Destination      Protocol Length Info
   1 0.000000000  10.0.2.15        142.251.220.67   TCP      54 35676 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   2 0.000990606  142.251.220.67   10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 35676 [ACK] Seq=1 Ack=2 Win=655
   3 1.537793566  10.0.2.15        34.107.221.82    TCP      54 38390 → 80 [ACK] Seq=1 Ack=1 Win=64024 Len=0
   4 1.538086683  34.107.221.82    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 38390 [ACK] Seq=1 Ack=2 Win=655
   5 2.814383396  10.0.2.15        142.250.192.81   TLSv1.2  93 Application Data
   6 2.814586285  10.0.2.15        142.250.192.131  TLSv1.2  93 Application Data
   7 2.814864337  142.250.192.81   10.0.2.15        TCP      60 443 → 60794 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   8 2.814864581  142.250.192.131  10.0.2.15        TCP      60 443 → 58764 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   9 2.843990891  142.250.192.131  10.0.2.15        TLSv1.2  93 Application Data
  10 2.843991212  142.250.192.81   10.0.2.15        TLSv1.2  93 Application Data
  11 2.844027241  10.0.2.15        142.250.192.131  TCP      54 58764 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
  12 2.894108445  10.0.2.15        142.250.192.81   TCP      54 60794 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
  13 3.070857526  10.0.2.15        23.48.226.17     TCP      54 34236 → 80 [ACK] Seq=1 Ack=1 Win=63351 Len=0
  14 3.071147466  23.48.226.17     10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 34236 [ACK] Seq=1 Ack=2 Win=655
  15 3.821425877  10.0.2.15        142.251.42.234   TLSv1.2  93 Application Data
  16 3.821544752  10.0.2.15        142.251.42.234   TLSv1.2  93 Application Data
  17 3.822298877  142.251.42.234   10.0.2.15        TCP      60 443 → 40366 [ACK] Seq=1 Ack=40 Win=65535 Len=0
  18 3.822299392  142.251.42.234   10.0.2.15        TCP      60 443 → 40362 [ACK] Seq=1 Ack=40 Win=65535 Len=0
  19 3.858732417  142.251.42.234   10.0.2.15        TLSv1.2  93 Application Data
  20 3.863214318  142.251.42.234   10.0.2.15        TLSv1.2  93 Application Data
  21 3.904721863  10.0.2.15        142.251.42.234   TCP      54 40362 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
  22 3.904753764  10.0.2.15        142.251.42.234   TCP      54 40366 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
  23 4.825915226  10.0.2.15        142.251.42.78    TLSv1.2  93 Application Data
  24 4.825980559  10.0.2.15        142.251.42.78    TLSv1.2  93 Application Data
  25 4.826002154  10.0.2.15        142.251.42.68    TLSv1.2  93 Application Data
```

```
› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.220.67
› Transmission Control Protocol, Src Port: 35676, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

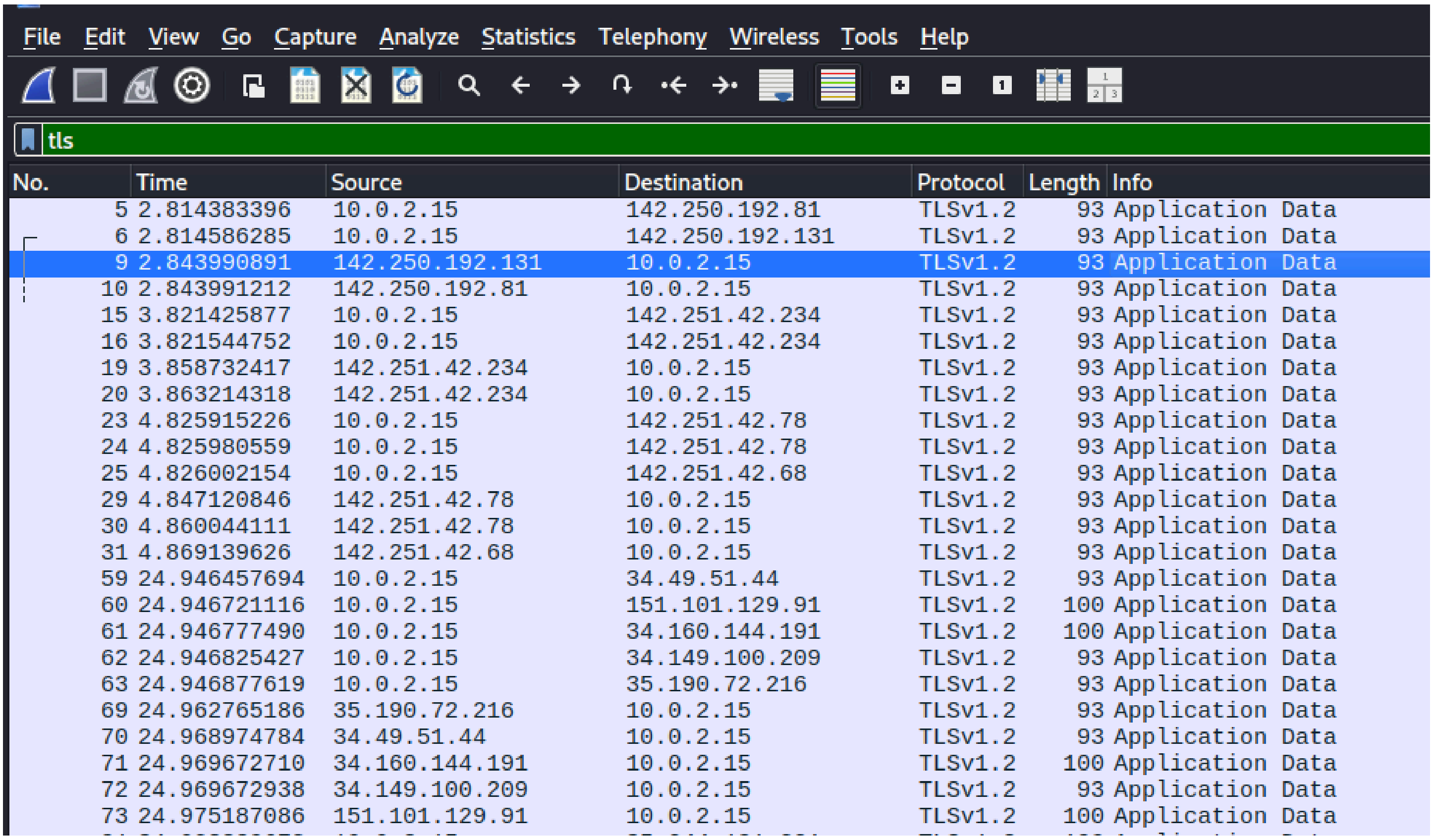
```
0000  52 54 00 12 35 02 08 00  27 c
0010  00 28 31 4a 40 00 40 06  92 3
0020  dc 43 8b 5c 00 50 fd 0a  48 7
0030  fa f0 77 68 00 00
```


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.  Time          Source        Destination   Protocol Length Info
 109 34.530752736  10.0.2.15     172.17.18.2   DNS       77 Standard query 0xa5dc A fonts.gstatic.com
 110 34.530822345  10.0.2.15     172.17.18.2   DNS       77 Standard query 0x8edf AAAA fonts.gstatic.com
 111 34.533720829  172.17.18.2   10.0.2.15     DNS       93 Standard query response 0xa5dc A fonts.gstatic.com A 142.251.221.227
 112 34.534108843  172.17.18.2   10.0.2.15     DNS      105 Standard query response 0x8edf AAAA fonts.gstatic.com AAAA 2404:6800:4009:80d::2003
```

```
› Frame 109: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.17.18.2
› User Datagram Protocol, Src Port: 60576, Dst Port: 53
› Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 d1 f8 5d 08 00 45 00   RT··5··· '··]··E·
0010  00 3f eb 28 40 00 40 11  85 63 0a 00 02 0f ac 11   ·?·(@·@· ·c······
0020  12 02 ec a0 00 35 00 2b  ca 5e a5 dc 01 00 00 01   ·····5·+ ·^······
0030  00 00 00 00 00 00 05 66  6f 6e 74 73 07 67 73 74   ·······f onts·gst
0040  61 74 69 63 03 63 6f 6d  00 00 01 00 01            atic·com ·····
```



```
tls
```

```
No.   Time           Source            Destination       Protocol  Length Info
    5 2.814383396    10.0.2.15         142.250.192.81    TLSv1.2     93 Application Data
    6 2.814586285    10.0.2.15         142.250.192.131   TLSv1.2     93 Application Data
    9 2.843990891    142.250.192.131   10.0.2.15         TLSv1.2     93 Application Data
   10 2.843991212    142.250.192.81    10.0.2.15         TLSv1.2     93 Application Data
   15 3.821425877    10.0.2.15         142.251.42.234    TLSv1.2     93 Application Data
   16 3.821544752    10.0.2.15         142.251.42.234    TLSv1.2     93 Application Data
   19 3.858732417    142.251.42.234    10.0.2.15         TLSv1.2     93 Application Data
   20 3.863214318    142.251.42.234    10.0.2.15         TLSv1.2     93 Application Data
   23 4.825915226    10.0.2.15         142.251.42.78     TLSv1.2     93 Application Data
   24 4.825980559    10.0.2.15         142.251.42.78     TLSv1.2     93 Application Data
   25 4.826002154    10.0.2.15         142.251.42.68     TLSv1.2     93 Application Data
   29 4.847120846    142.251.42.78     10.0.2.15         TLSv1.2     93 Application Data
   30 4.860044111    142.251.42.78     10.0.2.15         TLSv1.2     93 Application Data
   31 4.869139626    142.251.42.68     10.0.2.15         TLSv1.2     93 Application Data
   59 24.946457694   10.0.2.15         34.49.51.44       TLSv1.2     93 Application Data
   60 24.946721116   10.0.2.15         151.101.129.91    TLSv1.2    100 Application Data
   61 24.946777490   10.0.2.15         34.160.144.191    TLSv1.2    100 Application Data
   62 24.946825427   10.0.2.15         34.149.100.209    TLSv1.2     93 Application Data
   63 24.946877619   10.0.2.15         35.190.72.216     TLSv1.2     93 Application Data
   69 24.962765186   35.190.72.216     10.0.2.15         TLSv1.2     93 Application Data
   70 24.968974784   34.49.51.44       10.0.2.15         TLSv1.2     93 Application Data
   71 24.969672710   34.160.144.191    10.0.2.15         TLSv1.2    100 Application Data
   72 24.969672938   34.149.100.209    10.0.2.15         TLSv1.2     93 Application Data
   73 24.975187086   151.101.129.91    10.0.2.15         TLSv1.2    100 Application Data
```

6.Identify at least 3 different protocols in the capture.

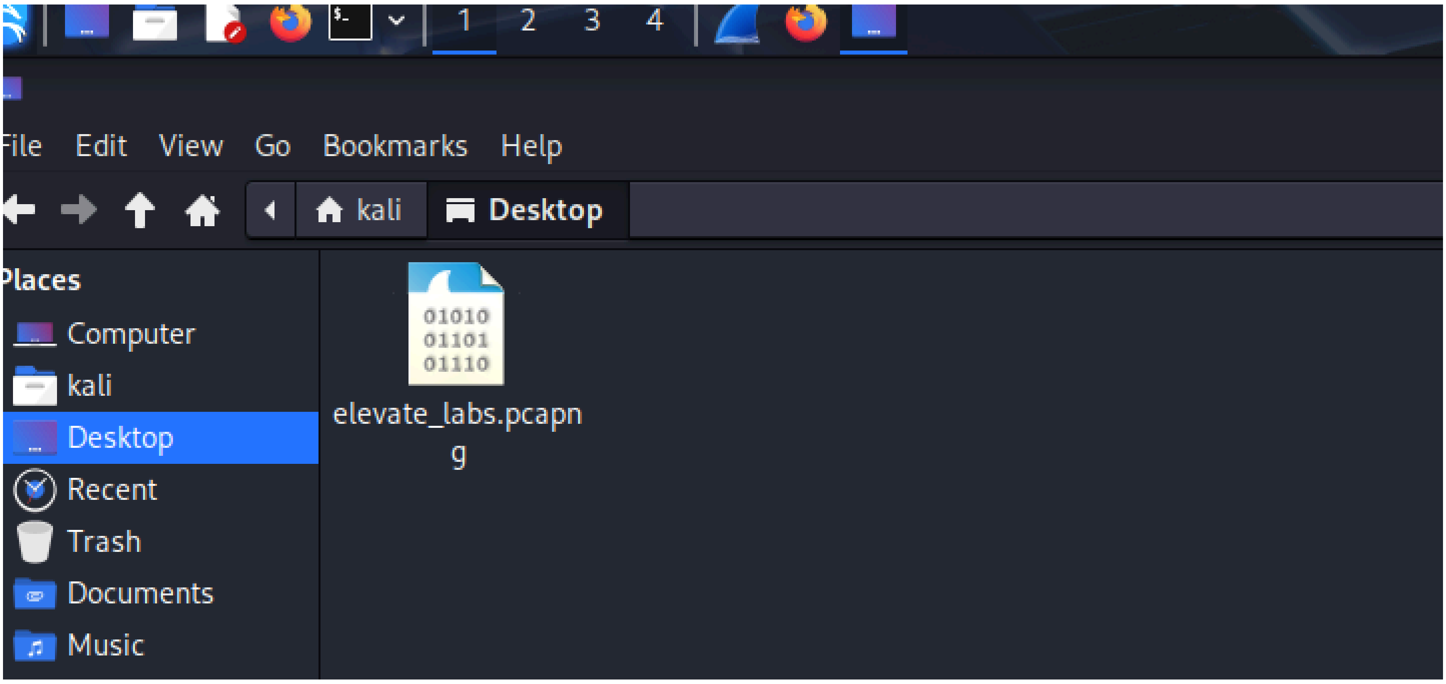
→ TCP

→ UDP

→ TLS

7.Export the capture as a .pcap file.

saved the file as elevate_labs.pcap



elevate_labs.pcapng

8.Summarize your findings and packet details.

The Wireshark packet capture analysis displays a network session featuring TCP, TLSv1.2, and Application Data packets, with communication between a local source IP and an external destination IP, suggesting a secure data exchange, possibly related to web or application traffic. Packet sizes vary from a few dozen to over a hundred bytes, with many including sequence and acknowledgment numbers, some indicating control packets with no data payload. A highlighted packet details a TCP segment with specific source and destination ports, a sequence number, an acknowledgment number, and a modest data payload, utilizing TLSv1.2 for encryption, indicative of a typical secure session with a combination of control and data transmissions.