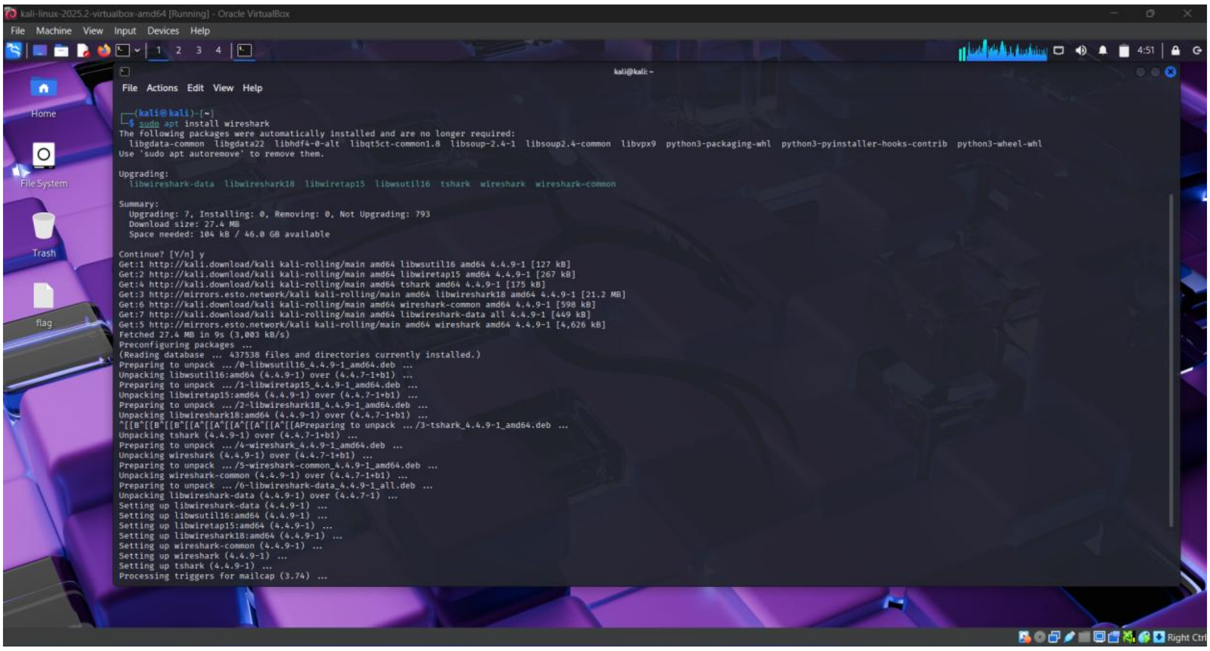
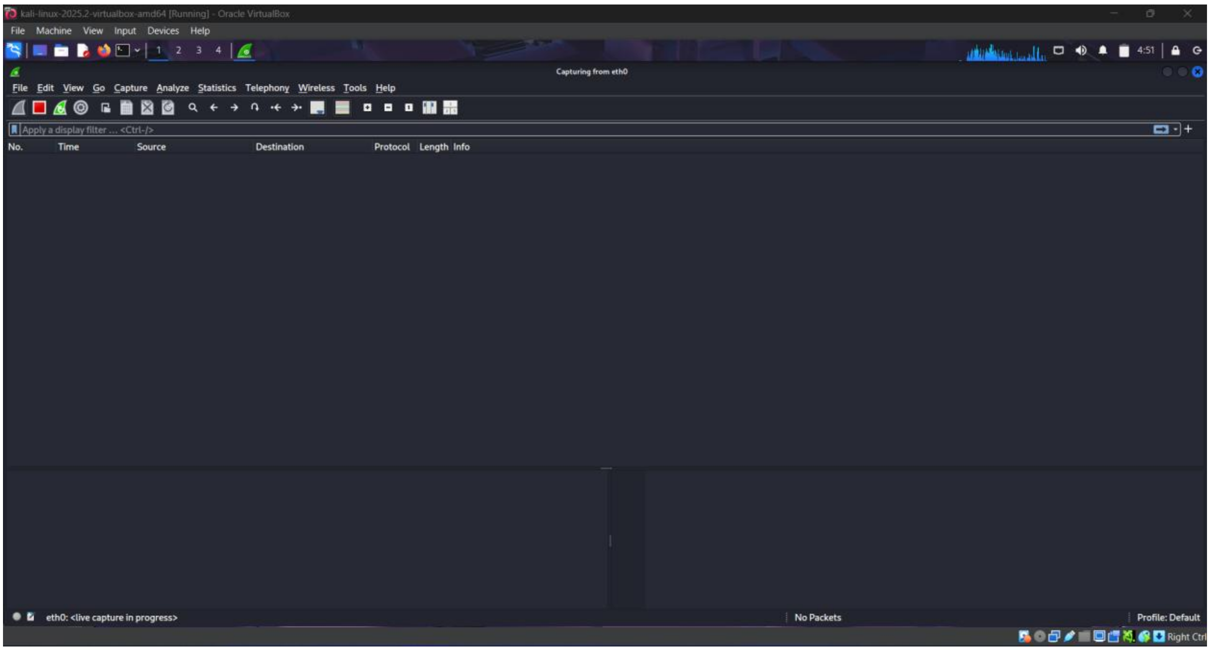
1.Insta l Wireshark.



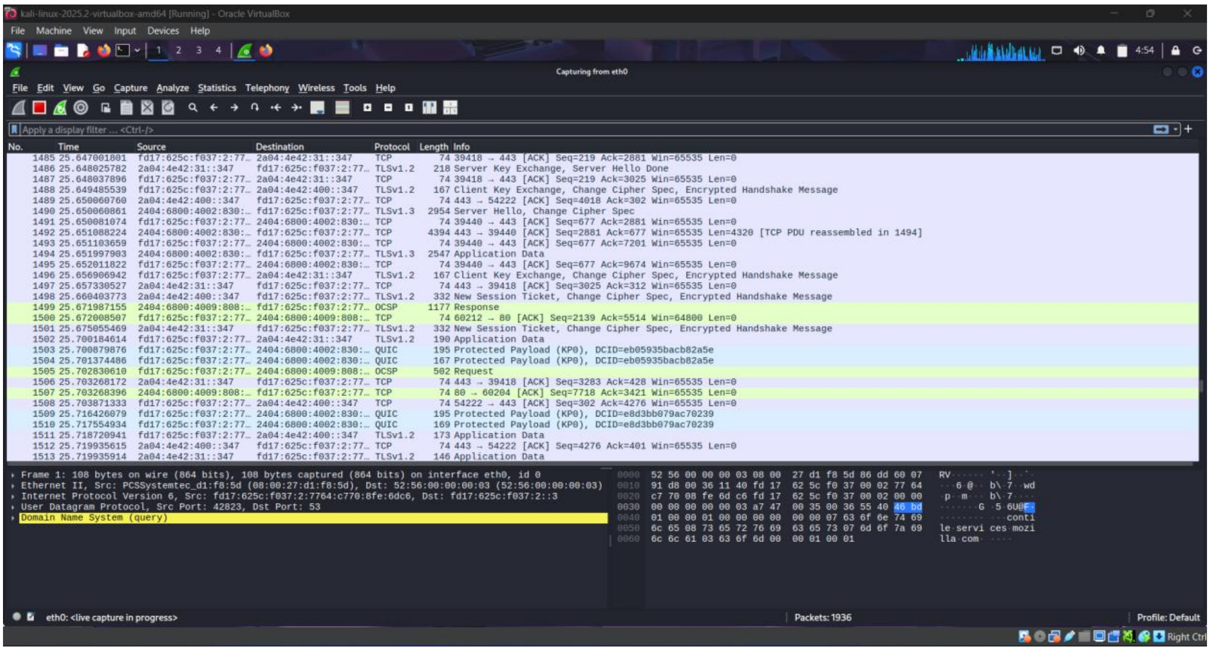
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
flag
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install wireshark
The following packages were automatically installed and are no longer required:
  libgdata-common  libgdata22  libhdf4-0-alt  libqt5ct-common1.8  libsoup-2.4-1  libsoup2.4-common  libvpx9  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libwireshark-data  libwireshark18  libwiretap15  libwsutil16  tshark  wireshark  wireshark-common

Summary:
  Upgrading: 7, Installing: 0, Removing: 0, Not Upgrading: 793
  Download size: 27.4 MB
  Space needed: 104 kB / 46.0 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libwsutil16 amd64 4.4.9-1 [127 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libwiretap15 amd64 4.4.9-1 [267 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 tshark amd64 4.4.9-1 [175 kB]
Get:3 http://mirrors.esto.network/kali kali-rolling/main amd64 libwireshark18 amd64 4.4.9-1 [21.2 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 wireshark-common amd64 4.4.9-1 [598 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libwireshark-data all 4.4.9-1 [449 kB]
Get:5 http://mirrors.esto.network/kali kali-rolling/main amd64 wireshark amd64 4.4.9-1 [4,626 kB]
Fetched 27.4 MB in 9s (3,003 kB/s)
Preconfiguring packages ...
(Reading database ... 437538 files and directories currently installed.)
Preparing to unpack .../0-libwsutil16_4.4.9-1_amd64.deb ...
Unpacking libwsutil16:amd64 (4.4.9-1) over (4.4.7-1+b1) ...
Preparing to unpack .../1-libwiretap15_4.4.9-1_amd64.deb ...
Unpacking libwiretap15:amd64 (4.4.9-1) over (4.4.7-1+b1) ...
Preparing to unpack .../2-libwireshark18_4.4.9-1_amd64.deb ...
Unpacking libwireshark18:amd64 (4.4.9-1) over (4.4.7-1+b1) ...
^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[APreparing to unpack .../3-tshark_4.4.9-1_amd64.deb ...
Unpacking tshark (4.4.9-1) over (4.4.7-1+b1) ...
Preparing to unpack .../4-wireshark_4.4.9-1_amd64.deb ...
Unpacking wireshark (4.4.9-1) over (4.4.7-1+b1) ...
Preparing to unpack .../5-wireshark-common_4.4.9-1_amd64.deb ...
Unpacking wireshark-common (4.4.9-1) over (4.4.7-1+b1) ...
Preparing to unpack .../6-libwireshark-data_4.4.9-1_all.deb ...
Unpacking libwireshark-data (4.4.9-1) over (4.4.7-1) ...
Setting up libwireshark-data (4.4.9-1) ...
Setting up libwsutil16:amd64 (4.4.9-1) ...
Setting up libwiretap15:amd64 (4.4.9-1) ...
Setting up libwireshark18:amd64 (4.4.9-1) ...
Setting up wireshark-common (4.4.9-1) ...
Setting up wireshark (4.4.9-1) ...
Setting up tshark (4.4.9-1) ...
Processing triggers for mailcap (3.74) ...
```



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
eth0: <live capture in progress>
No Packets
Profile: Default
Right Ctrl

2.Start capturing on your active network interface.



```
No.  Time          Source                   Destination              Protocol Length Info
1485 25.647001801 fd17:625c:f037:2:77… 2a04:4e42:31::347      TCP        74 39418 → 443 [ACK] Seq=219 Ack=2881 Win=65535 Len=0
1486 25.648025782 2a04:4e42:31::347      fd17:625c:f037:2:77… TLSv1.2   218 Server Key Exchange, Server Hello Done
1487 25.648037896 fd17:625c:f037:2:77… 2a04:4e42:31::347      TCP        74 39418 → 443 [ACK] Seq=219 Ack=3025 Win=65535 Len=0
1488 25.649485539 fd17:625c:f037:2:77… 2a04:4e42:400::347     TLSv1.2   167 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1489 25.650060760 2a04:4e42:400::347     fd17:625c:f037:2:77… TCP        74 443 → 54222 [ACK] Seq=4018 Ack=302 Win=65535 Len=0
1490 25.650060861 2404:6800:4002:830:… fd17:625c:f037:2:77… TLSv1.3  2954 Server Hello, Change Cipher Spec
1491 25.650081074 fd17:625c:f037:2:77… 2404:6800:4002:830:… TCP        74 39440 → 443 [ACK] Seq=677 Ack=2881 Win=65535 Len=0
1492 25.651088224 2404:6800:4002:830:… fd17:625c:f037:2:77… TCP      4394 443 → 39440 [ACK] Seq=2881 Ack=677 Win=65535 Len=4320 [TCP PDU reassembled in 1494]
1493 25.651103659 fd17:625c:f037:2:77… 2404:6800:4002:830:… TCP        74 39440 → 443 [ACK] Seq=677 Ack=7201 Win=65535 Len=0
1494 25.651997903 2404:6800:4002:830:… fd17:625c:f037:2:77… TLSv1.3  2547 Application Data
1495 25.652011822 fd17:625c:f037:2:77… 2404:6800:4002:830:… TCP        74 39440 → 443 [ACK] Seq=677 Ack=9674 Win=65535 Len=0
1496 25.656906942 fd17:625c:f037:2:77… 2a04:4e42:31::347      TLSv1.2   167 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1497 25.657330527 2a04:4e42:31::347      fd17:625c:f037:2:77… TCP        74 443 → 39418 [ACK] Seq=3025 Ack=312 Win=65535 Len=0
1498 25.660403773 2a04:4e42:400::347     fd17:625c:f037:2:77… TLSv1.2   332 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1499 25.671987155 2404:6800:4009:808:… fd17:625c:f037:2:77… OCSP     1177 Response
1500 25.672008507 fd17:625c:f037:2:77… 2404:6800:4009:808:… TCP        74 60212 → 80 [ACK] Seq=2139 Ack=5514 Win=64800 Len=0
1501 25.675055469 2a04:4e42:31::347      fd17:625c:f037:2:77… TLSv1.2   332 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1502 25.700184614 fd17:625c:f037:2:77… 2a04:4e42:31::347      TLSv1.2   190 Application Data
1503 25.700879876 fd17:625c:f037:2:77… 2404:6800:4002:830:… QUIC      195 Protected Payload (KP0), DCID=eb05935bacb82a5e
1504 25.701374486 fd17:625c:f037:2:77… 2404:6800:4002:830:… QUIC      167 Protected Payload (KP0), DCID=eb05935bacb82a5e
1505 25.702830610 fd17:625c:f037:2:77… 2404:6800:4009:808:… OCSP      502 Request
1506 25.703268172 2a04:4e42:31::347      fd17:625c:f037:2:77… TCP        74 443 → 39418 [ACK] Seq=3283 Ack=428 Win=65535 Len=0
1507 25.703268396 2404:6800:4009:808:… fd17:625c:f037:2:77… TCP        74 80 → 60204 [ACK] Seq=7718 Ack=3421 Win=65535 Len=0
1508 25.703871333 fd17:625c:f037:2:77… 2a04:4e42:400::347     TCP        74 54222 → 443 [ACK] Seq=302 Ack=4276 Win=65535 Len=0
1509 25.716426079 fd17:625c:f037:2:77… 2404:6800:4002:830:… QUIC      195 Protected Payload (KP0), DCID=e8d3bb079ac70239
1510 25.717554934 fd17:625c:f037:2:77… 2404:6800:4002:830:… QUIC      169 Protected Payload (KP0), DCID=e8d3bb079ac70239
1511 25.718720941 fd17:625c:f037:2:77… 2a04:4e42:400::347     TLSv1.2   173 Application Data
1512 25.719935615 2a04:4e42:400::347     fd17:625c:f037:2:77… TCP        74 443 → 54222 [ACK] Seq=4276 Ack=401 Win=65535 Len=0
1513 25.719935914 2a04:4e42:31::347      fd17:625c:f037:2:77… TLSv1.2   146 Application Data
```

```
› Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:03 (52:56:00:00:00:03)
› Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: fd17:625c:f037:2::3
› User Datagram Protocol, Src Port: 42823, Dst Port: 53
› Domain Name System (query)
```

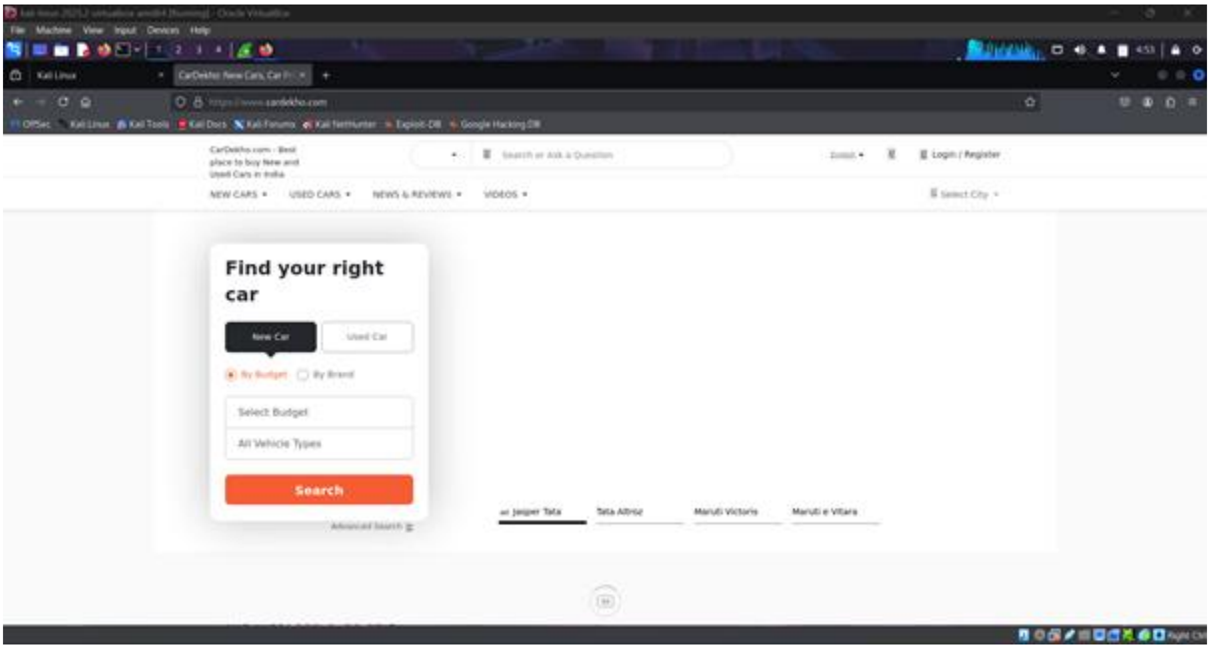
```
0000  52 56 00 00 00 03 08 00  27 d1 f8 5d 86 dd 60 07   RV······'··]··`·
0010  91 d8 00 36 11 40 fd 17  62 5c f0 37 00 02 77 64   ···6·@··b\·7··wd
0020  c7 70 08 fe 6d c6 fd 17  62 5c f0 37 00 02 00 00   ·p··m···b\·7····
0030  00 00 00 00 00 03 a7 47  00 35 00 36 55 40 46 bd   ·······G·5·6U@F·
0040  01 00 00 01 00 00 00 00  00 00 07 63 6f 6e 74 69   ···········conti
0050  6c 65 08 73 65 72 76 69  63 65 73 07 6d 6f 7a 69   le·servi ces·mozi
0060  6c 6c 61 03 63 6f 6d 00  00 01 00 01               lla·com·····
```

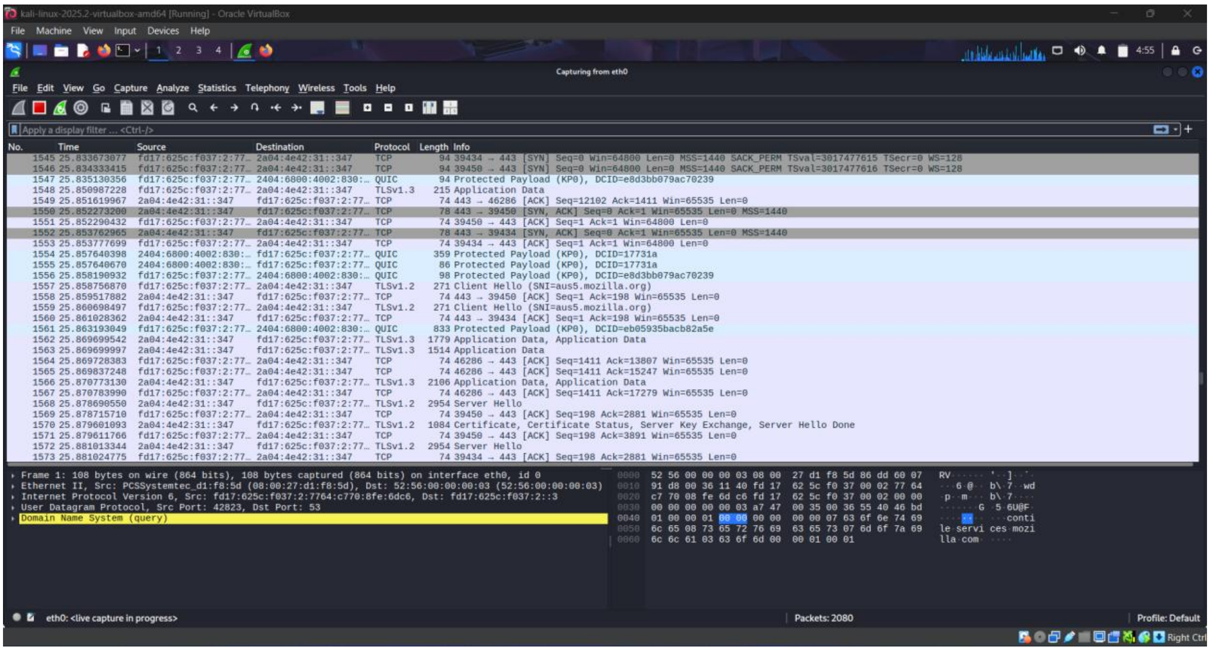
eth0: <live capture in progress>

Packets: 1936

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Profile: Default
Right Ctrl

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



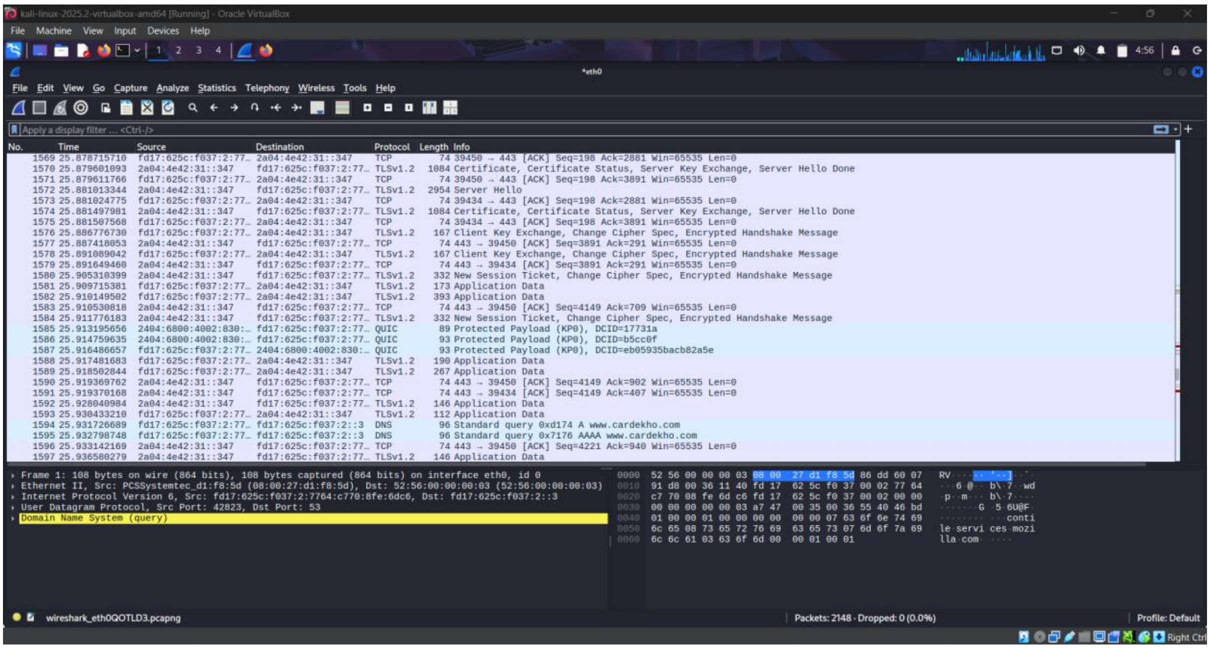

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
4:55
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Right Ctrl

```
No.     Time          Source                  Destination             Protocol  Length Info
   1545 25.833673077  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         94 39434 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3017477615 TSecr=0 WS=128
   1546 25.834333415  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         94 39450 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3017477616 TSecr=0 WS=128
   1547 25.835130356  fd17:625c:f037:2:77…   2404:6800:4002:830:…    QUIC        94 Protected Payload (KP0), DCID=e8d3bb079ac70239
   1548 25.850987228  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.3    215 Application Data
   1549 25.851619967  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 46286 [ACK] Seq=12102 Ack=1411 Win=65535 Len=0
   1550 25.852273200  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         78 443 → 39450 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
   1551 25.852290432  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39450 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0
   1552 25.853762965  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         78 443 → 39434 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
   1553 25.853777699  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39434 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0
   1554 25.857640398  2404:6800:4002:830:…   fd17:625c:f037:2:77…    QUIC       359 Protected Payload (KP0), DCID=17731a
   1555 25.857640670  2404:6800:4002:830:…   fd17:625c:f037:2:77…    QUIC        86 Protected Payload (KP0), DCID=17731a
   1556 25.858190932  fd17:625c:f037:2:77…   2404:6800:4002:830:…    QUIC        98 Protected Payload (KP0), DCID=e8d3bb079ac70239
   1557 25.858756870  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    271 Client Hello (SNI=aus5.mozilla.org)
   1558 25.859517882  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39450 [ACK] Seq=1 Ack=198 Win=65535 Len=0
   1559 25.860698497  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    271 Client Hello (SNI=aus5.mozilla.org)
   1560 25.861028362  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39434 [ACK] Seq=1 Ack=198 Win=65535 Len=0
   1561 25.863193049  fd17:625c:f037:2:77…   2404:6800:4002:830:…    QUIC       833 Protected Payload (KP0), DCID=eb05935bacb82a5e
   1562 25.869699542  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.3   1779 Application Data, Application Data
   1563 25.869699997  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.3   1514 Application Data
   1564 25.869728383  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 46286 → 443 [ACK] Seq=1411 Ack=13807 Win=65535 Len=0
   1565 25.869837248  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 46286 → 443 [ACK] Seq=1411 Ack=15247 Win=65535 Len=0
   1566 25.870773130  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.3   2106 Application Data, Application Data
   1567 25.870783990  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 46286 → 443 [ACK] Seq=1411 Ack=17279 Win=65535 Len=0
   1568 25.878690550  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   2954 Server Hello
   1569 25.878715710  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39450 → 443 [ACK] Seq=198 Ack=2881 Win=65535 Len=0
   1570 25.879601093  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   1084 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   1571 25.879611766  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39450 → 443 [ACK] Seq=198 Ack=3891 Win=65535 Len=0
   1572 25.881013344  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   2954 Server Hello
   1573 25.881024775  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39434 → 443 [ACK] Seq=198 Ack=2881 Win=65535 Len=0
```

```
▸ Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:03 (52:56:00:00:00:03)
▸ Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: fd17:625c:f037:2::3
▸ User Datagram Protocol, Src Port: 42823, Dst Port: 53
▸ Domain Name System (query)

0000  52 56 00 00 00 03 08 00  27 d1 f8 5d 86 dd 60 07   RV······'··]··`·
0010  91 d8 00 36 11 40 fd 17  62 5c f0 37 00 02 77 64   ···6·@··b\·7··wd
0020  c7 70 08 fe 6d c6 fd 17  62 5c f0 37 00 02 00 00   ·p··m···b\·7····
0030  00 00 00 00 00 03 a7 47  00 35 00 36 55 40 46 bd   ·······G·5·6U@F·
0040  01 00 00 01 00 00 00 00  00 00 07 63 6f 6e 74 69   ···········conti
0050  6c 65 08 73 65 72 76 69  63 65 73 07 6d 6f 7a 69   le·servi ces·mozi
0060  6c 6c 61 03 63 6f 6d 00  00 01 00 01               lla·com·····
```

eth0: <live capture in progress>   Packets: 2080   Profile: Default

4.Stop capture after a minute.

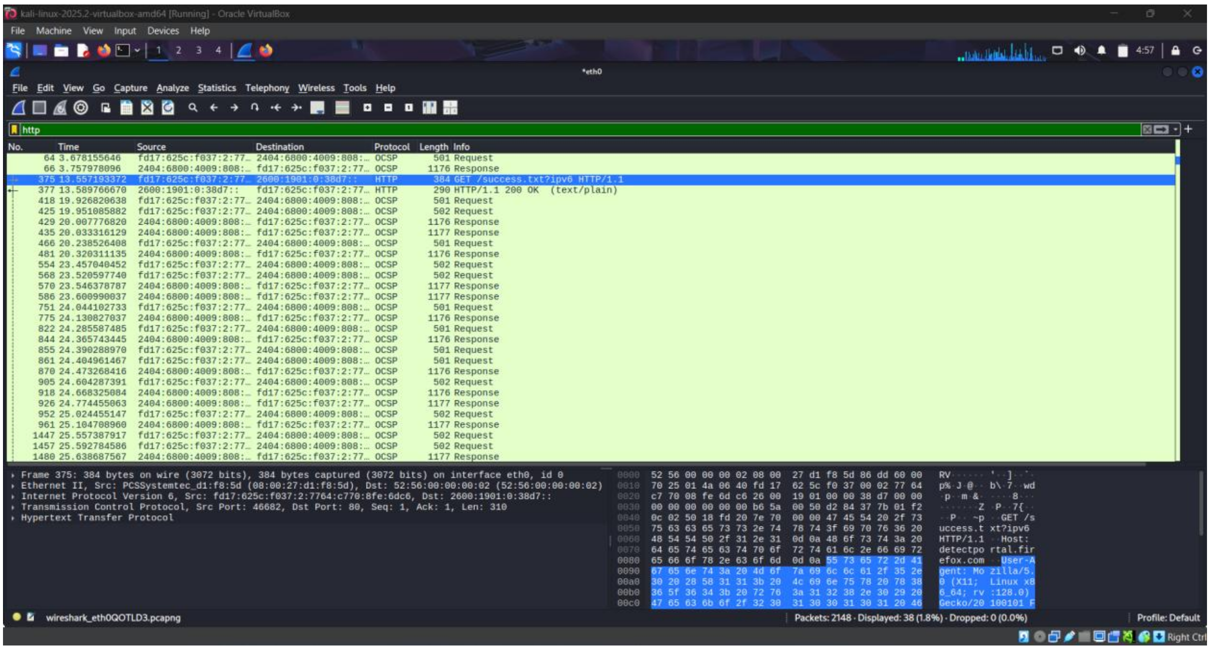

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
4:56
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Right Ctrl

```
No.     Time          Source                  Destination             Protocol  Length Info
   1569 25.878715710  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39450 → 443 [ACK] Seq=198 Ack=2881 Win=65535 Len=0
   1570 25.879601093  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   1084 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   1571 25.879611766  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39450 → 443 [ACK] Seq=198 Ack=3891 Win=65535 Len=0
   1572 25.881013344  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   2954 Server Hello
   1573 25.881024775  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39434 → 443 [ACK] Seq=198 Ack=2881 Win=65535 Len=0
   1574 25.881497981  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2   1084 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   1575 25.881507568  fd17:625c:f037:2:77…   2a04:4e42:31::347       TCP         74 39434 → 443 [ACK] Seq=198 Ack=3891 Win=65535 Len=0
   1576 25.886776730  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    167 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   1577 25.887418053  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39450 [ACK] Seq=3891 Ack=291 Win=65535 Len=0
   1578 25.891089042  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    167 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   1579 25.891649460  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39434 [ACK] Seq=3891 Ack=291 Win=65535 Len=0
   1580 25.905310399  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2    332 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   1581 25.909715381  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    173 Application Data
   1582 25.910149502  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    393 Application Data
   1583 25.910530818  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39450 [ACK] Seq=4149 Ack=709 Win=65535 Len=0
   1584 25.911776183  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2    332 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   1585 25.913195656  2404:6800:4002:830:…   fd17:625c:f037:2:77…    QUIC        89 Protected Payload (KP0), DCID=17731a
   1586 25.914759635  2404:6800:4002:830:…   fd17:625c:f037:2:77…    QUIC        93 Protected Payload (KP0), DCID=b5cc0f
   1587 25.916486657  fd17:625c:f037:2:77…   2404:6800:4002:830:…    QUIC        93 Protected Payload (KP0), DCID=eb05935bacb82a5e
   1588 25.917481683  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    190 Application Data
   1589 25.918502844  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    267 Application Data
   1590 25.919369762  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39450 [ACK] Seq=4149 Ack=902 Win=65535 Len=0
   1591 25.919370168  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39434 [ACK] Seq=4149 Ack=407 Win=65535 Len=0
   1592 25.928040984  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2    146 Application Data
   1593 25.930433210  fd17:625c:f037:2:77…   2a04:4e42:31::347       TLSv1.2    112 Application Data
   1594 25.931726689  fd17:625c:f037:2:77…   fd17:625c:f037:2::3     DNS         96 Standard query 0xd174 A www.cardekho.com
   1595 25.932798748  fd17:625c:f037:2:77…   fd17:625c:f037:2::3     DNS         96 Standard query 0x7176 AAAA www.cardekho.com
   1596 25.933142169  2a04:4e42:31::347      fd17:625c:f037:2:77…    TCP         74 443 → 39450 [ACK] Seq=4221 Ack=940 Win=65535 Len=0
   1597 25.936580279  2a04:4e42:31::347      fd17:625c:f037:2:77…    TLSv1.2    146 Application Data
```

```
▸ Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:03 (52:56:00:00:00:03)
▸ Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: fd17:625c:f037:2::3
▸ User Datagram Protocol, Src Port: 42823, Dst Port: 53
▸ Domain Name System (query)

0000  52 56 00 00 00 03 08 00  27 d1 f8 5d 86 dd 60 07   RV······'··]··`·
0010  91 d8 00 36 11 40 fd 17  62 5c f0 37 00 02 77 64   ···6·@··b\·7··wd
0020  c7 70 08 fe 6d c6 fd 17  62 5c f0 37 00 02 00 00   ·p··m···b\·7····
0030  00 00 00 00 00 03 a7 47  00 35 00 36 55 40 46 bd   ·······G·5·6U@F·
0040  01 00 00 01 00 00 00 00  00 00 07 63 6f 6e 74 69   ···········conti
0050  6c 65 08 73 65 72 76 69  63 65 73 07 6d 6f 7a 69   le·servi ces·mozi
0060  6c 6c 61 03 63 6f 6d 00  00 01 00 01               lla·com·····
```

wireshark_eth0QOTLD3.pcapng   Packets: 2148 · Dropped: 0 (0.0%)   Profile: Default

5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:57
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

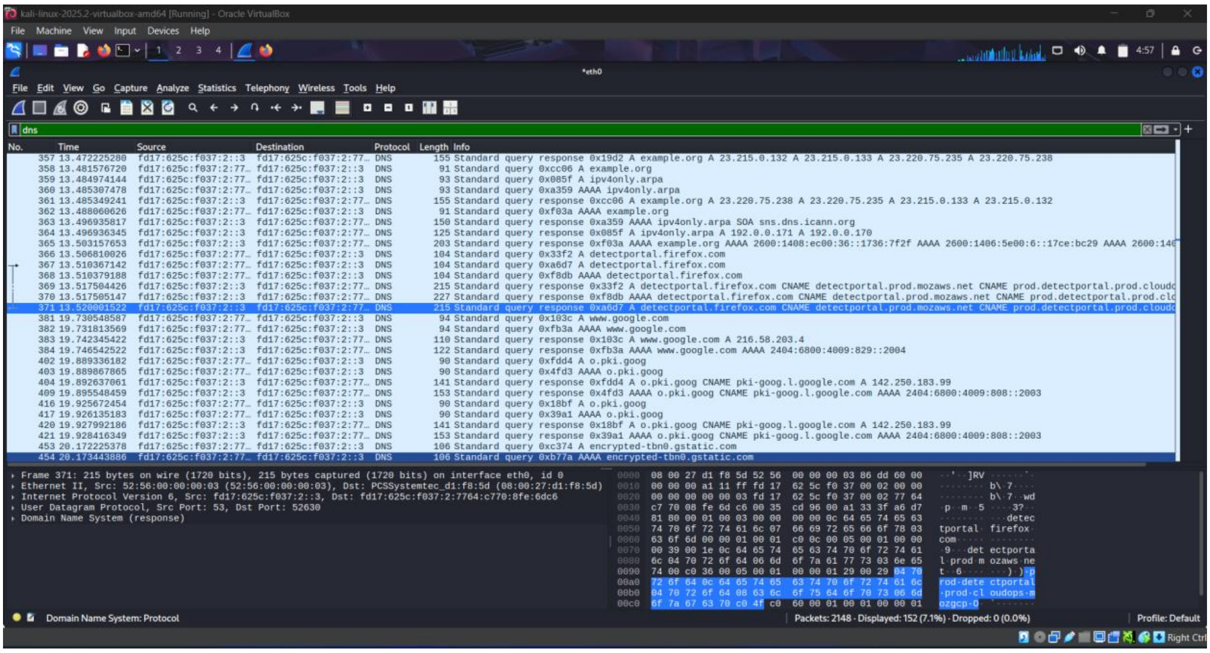
```
http
```

```
No.  Time          Source                 Destination            Protocol Length Info
  64 3.678155646   fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
  66 3.757978096   2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 375 13.557193372  fd17:625c:f037:2:77…  2600:1901:0:38d7::     HTTP      384 GET /success.txt?ipv6 HTTP/1.1
 377 13.589766670  2600:1901:0:38d7::     fd17:625c:f037:2:77…  HTTP      290 HTTP/1.1 200 OK  (text/plain)
 418 19.926820638  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 425 19.951085882  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
 429 20.007776820  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 435 20.033316129  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
 466 20.238526408  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 481 20.320311135  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 554 23.457040452  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
 568 23.520597740  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
 570 23.546378787  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
 586 23.600990037  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
 751 24.044102733  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 775 24.130827037  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 822 24.285587485  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 844 24.365743445  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 855 24.390288970  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 861 24.404961467  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      501 Request
 870 24.473268416  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 905 24.604287391  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
 918 24.668325084  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1176 Response
 926 24.774455063  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
 952 25.024455147  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
 961 25.104708960  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
1447 25.557387917  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
1457 25.592784586  fd17:625c:f037:2:77…  2404:6800:4009:808:…  OCSP      502 Request
1480 25.638687567  2404:6800:4009:808:…  fd17:625c:f037:2:77…  OCSP     1177 Response
```

```
› Frame 375: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)
› Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: 2600:1901:0:38d7::
› Transmission Control Protocol, Src Port: 46682, Dst Port: 80, Seq: 1, Ack: 1, Len: 310
› Hypertext Transfer Protocol
```

```
0000  52 56 00 00 00 02 08 00  27 d1 f8 5d 86 dd 60 00   RV······ '··]··`·
0010  70 25 01 4a 06 40 fd 17  62 5c f0 37 00 02 77 64   p%·J·@·· b\·7··wd
0020  c7 70 08 fe 6d c6 26 00  19 01 00 00 38 d7 00 00   ·p··m·&· ····8···
0030  00 00 00 00 00 00 b6 5a  00 50 d2 84 37 7b 01 f2   ·······Z ·P··7{··
0040  0c 02 50 18 fd 20 7e 70  00 00 47 45 54 20 2f 73   ··P·· ~p ··GET /s
0050  75 63 63 65 73 73 2e 74  78 74 3f 69 70 76 36 20   uccess.t xt?ipv6 
0060  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0070  64 65 74 65 63 74 70 6f  72 74 61 6c 2e 66 69 72   detectpo rtal.fir
0080  65 66 6f 78 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   efox.com ··User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00a0  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
00b0  36 5f 36 34 3b 20 72 76  3a 31 32 38 2e 30 29 20   6_64; rv :128.0) 
00c0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
```

wireshark_eth0QOTLD3.pcapng   Packets: 2148 · Displayed: 38 (1.8%) · Dropped: 0 (0.0%)   Profile: Default


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:57
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

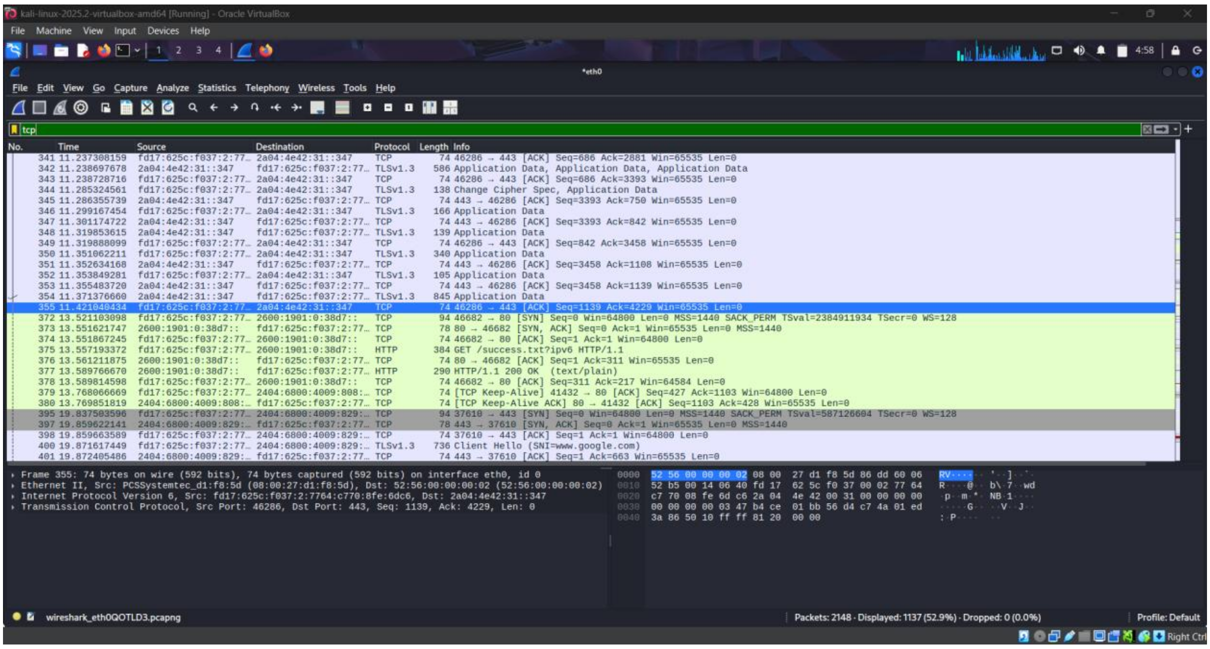
```
dns
```

```
No.  Time          Source                 Destination            Protocol Length Info
 357 13.472225280  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       155 Standard query response 0x19d2 A example.org A 23.215.0.132 A 23.215.0.133 A 23.220.75.235 A 23.220.75.238
 358 13.481576720  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        91 Standard query 0xcc06 A example.org
 359 13.484974144  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        93 Standard query 0x085f A ipv4only.arpa
 360 13.485307478  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        93 Standard query 0xa359 AAAA ipv4only.arpa
 361 13.485349241  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       155 Standard query response 0xcc06 A example.org A 23.220.75.238 A 23.220.75.235 A 23.215.0.133 A 23.215.0.132
 362 13.488060626  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        91 Standard query 0xf03a AAAA example.org
 363 13.496935817  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       150 Standard query response 0xa359 AAAA ipv4only.arpa SOA sns.dns.icann.org
 364 13.496936345  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       125 Standard query response 0x085f A ipv4only.arpa A 192.0.0.171 A 192.0.0.170
 365 13.503157653  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       203 Standard query response 0xf03a AAAA example.org AAAA 2600:1408:ec00:36::1736:7f2f AAAA 2600:1406:5e00:6::17ce:bc29 AAAA 2600:14(
 366 13.506810026  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS       104 Standard query 0x33f2 A detectportal.firefox.com
 367 13.510367142  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS       104 Standard query 0xa6d7 A detectportal.firefox.com
 368 13.510379188  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS       104 Standard query 0xf8db AAAA detectportal.firefox.com
 369 13.517504426  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       215 Standard query response 0x33f2 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudo
 370 13.517505147  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       227 Standard query response 0xf8db AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.clo
 371 13.520001522  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       215 Standard query response 0xa6d7 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudo
 381 19.730548587  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        94 Standard query 0x103c A www.google.com
 382 19.731813569  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        94 Standard query 0xfb3a AAAA www.google.com
 383 19.742345422  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       110 Standard query response 0x103c A www.google.com A 216.58.203.4
 384 19.746542522  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       122 Standard query response 0xfb3a AAAA www.google.com AAAA 2404:6800:4009:829::2004
 402 19.889336182  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        90 Standard query 0xfdd4 A o.pki.goog
 403 19.889867865  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        90 Standard query 0x4fd3 AAAA o.pki.goog
 404 19.892637061  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       141 Standard query response 0xfdd4 A o.pki.goog CNAME pki-goog.l.google.com A 142.250.183.99
 409 19.895548459  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       153 Standard query response 0x4fd3 AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4009:808::2003
 416 19.925672454  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        90 Standard query 0x18bf A o.pki.goog
 417 19.926135183  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS        90 Standard query 0x39a1 AAAA o.pki.goog
 420 19.927992186  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       141 Standard query response 0x18bf A o.pki.goog CNAME pki-goog.l.google.com A 142.250.183.99
 421 19.928416349  fd17:625c:f037:2::3    fd17:625c:f037:2:77…  DNS       153 Standard query response 0x39a1 AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4009:808::2003
 453 20.172225378  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS       106 Standard query 0xc374 A encrypted-tbn0.gstatic.com
 454 20.173443886  fd17:625c:f037:2:77…  fd17:625c:f037:2::3    DNS       106 Standard query 0xb77a AAAA encrypted-tbn0.gstatic.com
```

```
› Frame 371: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, id 0
› Ethernet II, Src: 52:56:00:00:00:03 (52:56:00:00:00:03), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
› Internet Protocol Version 6, Src: fd17:625c:f037:2::3, Dst: fd17:625c:f037:2:7764:c770:8fe:6dc6
› User Datagram Protocol, Src Port: 53, Dst Port: 52630
› Domain Name System (response)
```

```
0000  08 00 27 d1 f8 5d 52 56  00 00 00 03 86 dd 60 00   ··'··]RV ······`·
0010  00 00 00 a1 11 ff fd 17  62 5c f0 37 00 02 00 00   ········ b\·7····
0020  00 00 00 00 00 03 fd 17  62 5c f0 37 00 02 77 64   ········ b\·7··wd
0030  c7 70 08 fe 6d c6 00 35  cd 96 00 a1 33 3f a6 d7   ·p··m··5 ····3?··
0040  81 80 00 01 00 03 00 00  00 00 0c 64 65 74 65 63   ········ ···detec
0050  74 70 6f 72 74 61 6c 07  66 69 72 65 66 6f 78 03   tportal· firefox·
0060  63 6f 6d 00 00 01 00 01  c0 0c 00 05 00 01 00 00   com····· ········
0070  00 39 00 1e 0c 64 65 74  65 63 74 70 6f 72 74 61   ·9···det ectporta
0080  6c 04 70 72 6f 64 06 6d  6f 7a 61 77 73 03 6e 65   l·prod·m ozaws·ne
0090  74 00 c0 36 00 05 00 01  00 00 01 29 00 29 04 70   t··6···· ···)·)·p
00a0  72 6f 64 0c 64 65 74 65  63 74 70 6f 72 74 61 6c   rod·dete ctportal
00b0  04 70 72 6f 64 08 63 6c  6f 75 64 6f 70 73 06 6d   ·prod·cl oudops·m
00c0  6f 7a 67 63 70 c0 4f c0  60 00 01 00 01 00 00 01   ozgcp·O· `·······
```

Domain Name System: Protocol   Packets: 2148 · Displayed: 152 (7.1%) · Dropped: 0 (0.0%)   Profile: Default


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:58
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

tcp

```
No.  Time          Source                  Destination             Protocol Length Info
 341 11.237308159  fd17:625c:f037:2:77…    2a04:4e42:31::347       TCP        74 46286 → 443 [ACK] Seq=686 Ack=2881 Win=65535 Len=0
 342 11.238697678  2a04:4e42:31::347       fd17:625c:f037:2:77…    TLSv1.3   586 Application Data, Application Data, Application Data
 343 11.238728716  fd17:625c:f037:2:77…    2a04:4e42:31::347       TCP        74 46286 → 443 [ACK] Seq=686 Ack=3393 Win=65535 Len=0
 344 11.285324561  fd17:625c:f037:2:77…    2a04:4e42:31::347       TLSv1.3   138 Change Cipher Spec, Application Data
 345 11.286355739  2a04:4e42:31::347       fd17:625c:f037:2:77…    TCP        74 443 → 46286 [ACK] Seq=3393 Ack=750 Win=65535 Len=0
 346 11.299167454  fd17:625c:f037:2:77…    2a04:4e42:31::347       TLSv1.3   166 Application Data
 347 11.301174722  2a04:4e42:31::347       fd17:625c:f037:2:77…    TCP        74 443 → 46286 [ACK] Seq=3393 Ack=842 Win=65535 Len=0
 348 11.319853615  2a04:4e42:31::347       fd17:625c:f037:2:77…    TLSv1.3   139 Application Data
 349 11.319888099  fd17:625c:f037:2:77…    2a04:4e42:31::347       TCP        74 46286 → 443 [ACK] Seq=842 Ack=3458 Win=65535 Len=0
 350 11.351062211  fd17:625c:f037:2:77…    2a04:4e42:31::347       TLSv1.3   340 Application Data
 351 11.352634168  2a04:4e42:31::347       fd17:625c:f037:2:77…    TCP        74 443 → 46286 [ACK] Seq=3458 Ack=1108 Win=65535 Len=0
 352 11.353849281  fd17:625c:f037:2:77…    2a04:4e42:31::347       TLSv1.3   105 Application Data
 353 11.355483720  2a04:4e42:31::347       fd17:625c:f037:2:77…    TCP        74 443 → 46286 [ACK] Seq=3458 Ack=1139 Win=65535 Len=0
 354 11.371376660  2a04:4e42:31::347       fd17:625c:f037:2:77…    TLSv1.3   845 Application Data
 355 11.421040434  fd17:625c:f037:2:77…    2a04:4e42:31::347       TCP        74 46286 → 443 [ACK] Seq=1139 Ack=4229 Win=65535 Len=0
 372 13.521103098  fd17:625c:f037:2:77…    2600:1901:0:38d7::      TCP        94 46682 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=2384911934 TSecr=0 WS=128
 373 13.551621747  2600:1901:0:38d7::      fd17:625c:f037:2:77…    TCP        78 80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
 374 13.551867245  fd17:625c:f037:2:77…    2600:1901:0:38d7::      TCP        74 46682 → 80 [ACK] Seq=1 Ack=1 Win=64800 Len=0
 375 13.557193372  fd17:625c:f037:2:77…    2600:1901:0:38d7::      HTTP      384 GET /success.txt?ipv6 HTTP/1.1
 376 13.561211875  2600:1901:0:38d7::      fd17:625c:f037:2:77…    TCP        74 80 → 46682 [ACK] Seq=1 Ack=311 Win=65535 Len=0
 377 13.589766670  2600:1901:0:38d7::      fd17:625c:f037:2:77…    HTTP      290 HTTP/1.1 200 OK  (text/plain)
 378 13.589814598  fd17:625c:f037:2:77…    2600:1901:0:38d7::      TCP        74 46682 → 80 [ACK] Seq=311 Ack=217 Win=64584 Len=0
 379 13.768066669  fd17:625c:f037:2:77…    2404:6800:4009:808:…    TCP        74 [TCP Keep-Alive] 41432 → 80 [ACK] Seq=427 Ack=1103 Win=64800 Len=0
 380 13.769851819  2404:6800:4009:808:…    fd17:625c:f037:2:77…    TCP        74 [TCP Keep-Alive ACK] 80 → 41432 [ACK] Seq=1103 Ack=428 Win=65535 Len=0
 395 19.837503596  fd17:625c:f037:2:77…    2404:6800:4009:829:…    TCP        94 37610 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=587126604 TSecr=0 WS=128
 397 19.859622141  2404:6800:4009:829:…    fd17:625c:f037:2:77…    TCP        78 443 → 37610 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
 398 19.859663589  fd17:625c:f037:2:77…    2404:6800:4009:829:…    TCP        74 37610 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0
 400 19.871617449  fd17:625c:f037:2:77…    2404:6800:4009:829:…    TLSv1.3   736 Client Hello (SNI=www.google.com)
 401 19.872405486  2404:6800:4009:829:…    fd17:625c:f037:2:77…    TCP        74 443 → 37610 [ACK] Seq=1 Ack=663 Win=65535 Len=0
```

```
▸ Frame 355: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)
▸ Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: 2a04:4e42:31::347
▸ Transmission Control Protocol, Src Port: 46286, Dst Port: 443, Seq: 1139, Ack: 4229, Len: 0
```

```
0000  52 56 00 00 00 02 08 00  27 d1 f8 5d 86 dd 60 06   RV······'··]··`·
0010  52 b5 00 14 06 40 fd 17  62 5c f0 37 00 02 77 64   R····@··b\·7··wd
0020  c7 70 08 fe 6d c6 2a 04  4e 42 00 31 00 00 00 00   ·p··m·*·NB·1····
0030  00 00 00 00 03 47 b4 ce  01 bb 56 d4 c7 4a 01 ed   ·····G····V··J··
0040  3a 86 50 10 ff ff 81 20  00 00                     :·P·······
```

wireshark_eth0QOTLD3.pcapng | Packets: 2148 · Displayed: 1137 (52.9%) · Dropped: 0 (0.0%) | Profile: Default

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

DNS:-dns to find lookups for website names (Domain Name System).

HTTP:-http to find unencrypted web traffic (Hypertext Transfer Protocol).

TCP :-(Transmission Control Protocol) packets in Wireshark, you use a simple filter expression. The goal is to isolate the packets that belong to TCP conversations, often looking for the handshake (SYN, SYN/ACK, ACK) that establishes a connection.

7.Export the capture as a .pcap file.

- **Attached in the GitHub file name** My_Web_Capture.pcap

8.Summarize your findings and packet details

- **DNS** (Domain Name System) dns Used to translate a human-readable domain name (e.g., https://www.google.com/url?sa=E&source=gmail&q=google.com) into an IP address. **Query:** Standard query 0x5243 A google.com. **Response:** Standard query response 0x5243 A 142.250.72.100
- **2. ICMP** (Internet Control Message Protocol) icmp Used for network diagnostics, specifically the `ping` command. It reports errors and provides information about the network layer. **Request:** Echo (ping) request (Type 8, Code 0). **Reply:** Echo (ping) reply (Type 0, Code 0) from the server.
- **3. TCP** (Transmission Control Protocol) tcp A connection-oriented protocol used to establish reliable connections, often as the foundation for HTTP/HTTPS. **Three-Way Handshake:** Observed SYN→SYN/ACK→ACK packets between my computer's IP and a web server's IP, establishing a session.
- **2. HTTP** `http` **Application data** for web browsing. Sits directly above TCP.**GET** request (Client → Server) and **200 OK** response (Server → Client), showing plaintext data like `Host` and `User-Agent`.