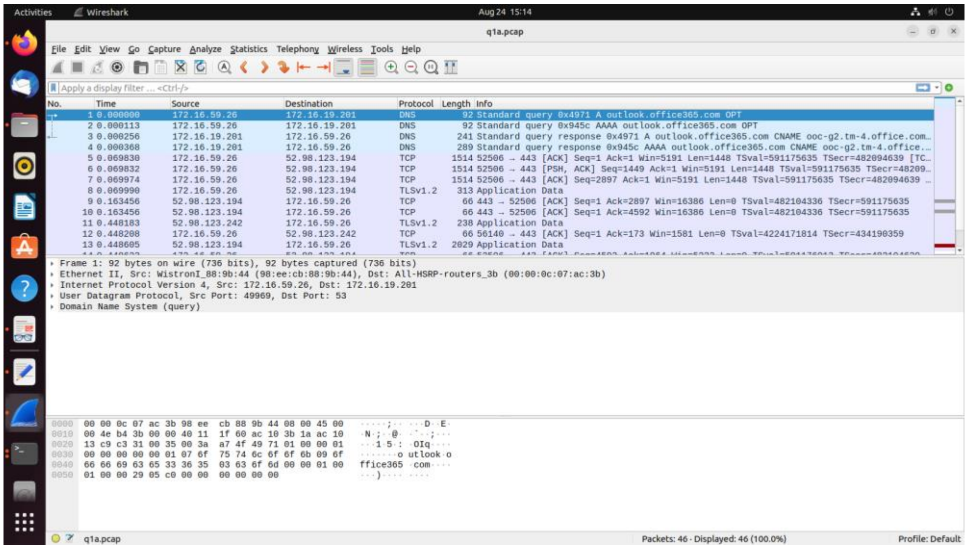
Lab 4

Q1.


Activities
Wireshark
Aug 24 15:14
q1a.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
q1a.pcap
Packets: 46 · Displayed: 46 (100.0%)
Profile: Default

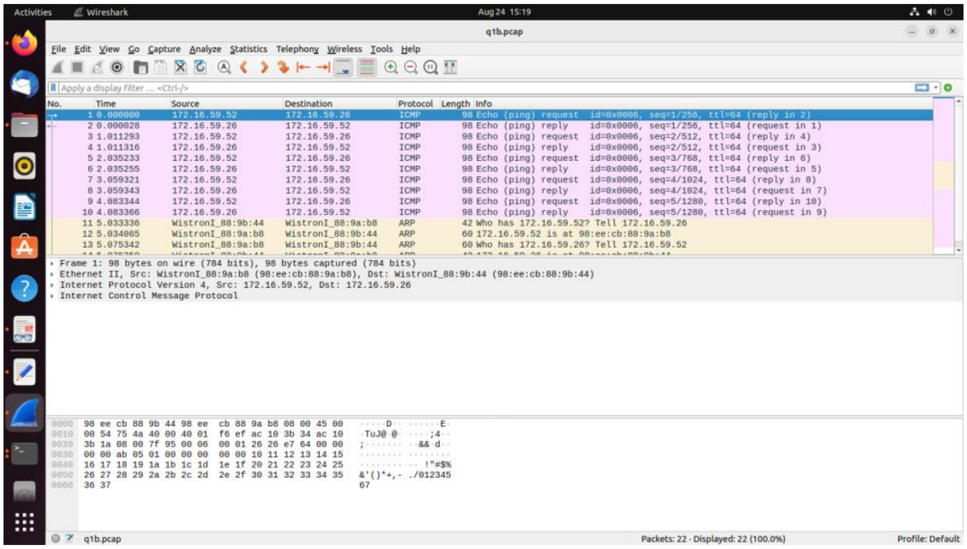
```
No.   Time      Source          Destination     Protocol Length Info
   1 0.000000  172.16.59.26    172.16.19.201   DNS        92 Standard query 0x4971 A outlook.office365.com OPT
   2 0.000113  172.16.59.26    172.16.19.201   DNS        92 Standard query 0x945c AAAA outlook.office365.com OPT
   3 0.000256  172.16.19.201   172.16.59.26    DNS       241 Standard query response 0x4971 A outlook.office365.com CNAME ooc-g2.tm-4.office.com…
   4 0.000368  172.16.19.201   172.16.59.26    DNS       289 Standard query response 0x945c AAAA outlook.office365.com CNAME ooc-g2.tm-4.office.…
   5 0.069830  172.16.59.26    52.98.123.194   TCP      1514 52506 → 443 [ACK] Seq=1 Ack=1 Win=5191 Len=1448 TSval=591175635 TSecr=482094639 [TC…
   6 0.069832  172.16.59.26    52.98.123.194   TCP      1514 52506 → 443 [PSH, ACK] Seq=1449 Ack=1 Win=5191 Len=1448 TSval=591175635 TSecr=48209…
   7 0.069974  172.16.59.26    52.98.123.194   TCP      1514 52506 → 443 [ACK] Seq=2897 Ack=1 Win=5191 Len=1448 TSval=591175635 TSecr=482094639 …
   8 0.069990  172.16.59.26    52.98.123.194   TLSv1.2   313 Application Data
   9 0.163456  52.98.123.194   172.16.59.26    TCP        66 443 → 52506 [ACK] Seq=1 Ack=2897 Win=16386 Len=0 TSval=482104336 TSecr=591175635
  10 0.163456  52.98.123.194   172.16.59.26    TCP        66 443 → 52506 [ACK] Seq=1 Ack=4592 Win=16386 Len=0 TSval=482104336 TSecr=591175635
  11 0.448183  52.98.123.242   172.16.59.26    TLSv1.2   238 Application Data
  12 0.448208  172.16.59.26    52.98.123.242   TCP        66 56140 → 443 [ACK] Seq=1 Ack=173 Win=1581 Len=0 TSval=4224171814 TSecr=434190359
  13 0.448605  52.98.123.194   172.16.59.26    TLSv1.2  2029 Application Data
```

```
› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
› Ethernet II, Src: WistronI_88:9b:44 (98:ee:cb:88:9b:44), Dst: All-HSRP-routers_3b (00:00:0c:07:ac:3b)
› Internet Protocol Version 4, Src: 172.16.59.26, Dst: 172.16.19.201
› User Datagram Protocol, Src Port: 49969, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 00 0c 07 ac 3b 98 ee  cb 88 9b 44 08 00 45 00   ·····;·· ···D··E·
0010  00 4e b4 3b 00 00 40 11  1f 60 ac 10 3b 1a ac 10   ·N·;··@· ·`··;···
0020  13 c9 c3 31 00 35 00 3a  a7 4f 49 71 01 00 00 01   ···1·5·: ·OIq····
0030  00 00 00 00 00 01 07 6f  75 74 6c 6f 6f 6b 09 6f   ·······o utlook·o
0040  66 66 69 63 65 33 36 35  03 63 6f 6d 00 00 01 00   ffice365 ·com····
0050  01 00 00 29 05 c0 00 00  00 00 00 00               ···)···· ····
```

The loopback interface (127.0.0.1) is always available and operational. It doesn't depend on external factors or network connectivity.

No, there is not any ICMP Message sent from my host but when another ip address pings me, I can see ICMP messages.


Activities
Wireshark
Aug 24 15:19
q1b.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
q1b.pcap
Packets: 22 · Displayed: 22 (100.0%)
Profile: Default

```
No.   Time      Source              Destination         Protocol Length Info
   1 0.000000  172.16.59.52        172.16.59.26        ICMP       98 Echo (ping) request  id=0x0006, seq=1/256, ttl=64 (reply in 2)
   2 0.000028  172.16.59.26        172.16.59.52        ICMP       98 Echo (ping) reply    id=0x0006, seq=1/256, ttl=64 (request in 1)
   3 1.011293  172.16.59.52        172.16.59.26        ICMP       98 Echo (ping) request  id=0x0006, seq=2/512, ttl=64 (reply in 4)
   4 1.011316  172.16.59.26        172.16.59.52        ICMP       98 Echo (ping) reply    id=0x0006, seq=2/512, ttl=64 (request in 3)
   5 2.035233  172.16.59.52        172.16.59.26        ICMP       98 Echo (ping) request  id=0x0006, seq=3/768, ttl=64 (reply in 6)
   6 2.035255  172.16.59.26        172.16.59.52        ICMP       98 Echo (ping) reply    id=0x0006, seq=3/768, ttl=64 (request in 5)
   7 3.059321  172.16.59.52        172.16.59.26        ICMP       98 Echo (ping) request  id=0x0006, seq=4/1024, ttl=64 (reply in 8)
   8 3.059343  172.16.59.26        172.16.59.52        ICMP       98 Echo (ping) reply    id=0x0006, seq=4/1024, ttl=64 (request in 7)
   9 4.083344  172.16.59.52        172.16.59.26        ICMP       98 Echo (ping) request  id=0x0006, seq=5/1280, ttl=64 (reply in 10)
  10 4.083366  172.16.59.26        172.16.59.52        ICMP       98 Echo (ping) reply    id=0x0006, seq=5/1280, ttl=64 (request in 9)
  11 5.033336  WistronI_88:9b:44   WistronI_88:9a:b8   ARP        42 Who has 172.16.59.52? Tell 172.16.59.26
  12 5.034065  WistronI_88:9a:b8   WistronI_88:9b:44   ARP        60 172.16.59.52 is at 98:ee:cb:88:9a:b8
  13 5.075342  WistronI_88:9a:b8   WistronI_88:9b:44   ARP        60 Who has 172.16.59.26? Tell 172.16.59.52
```

```
› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: WistronI_88:9a:b8 (98:ee:cb:88:9a:b8), Dst: WistronI_88:9b:44 (98:ee:cb:88:9b:44)
› Internet Protocol Version 4, Src: 172.16.59.52, Dst: 172.16.59.26
› Internet Control Message Protocol
```

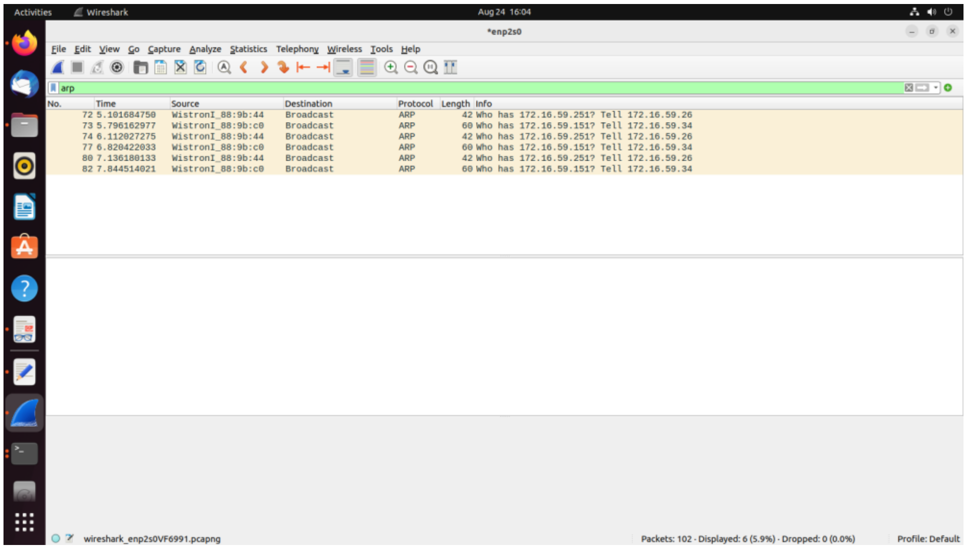
```
0000  98 ee cb 88 9b 44 98 ee  cb 88 9a b8 08 00 45 00   ·····D·· ······E·
0010  00 54 75 4a 40 00 40 01  f6 ef ac 10 3b 34 ac 10   ·TuJ@·@· ····;4··
0020  3b 1a 08 00 7f 95 00 06  00 01 26 26 e7 64 00 00   ;······· ··&&·d··
0030  00 00 ab 05 01 00 00 00  00 00 10 11 12 13 14 15   ········ ········
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   &'()*+,- ./012345
0060  36 37                                              67
```

Q2.

I used this command to clear arp cache first: sudo ip -s -s neigh flush all

Then I gave this command to the terminal: ping 172.16.59.251 -c 1 –b

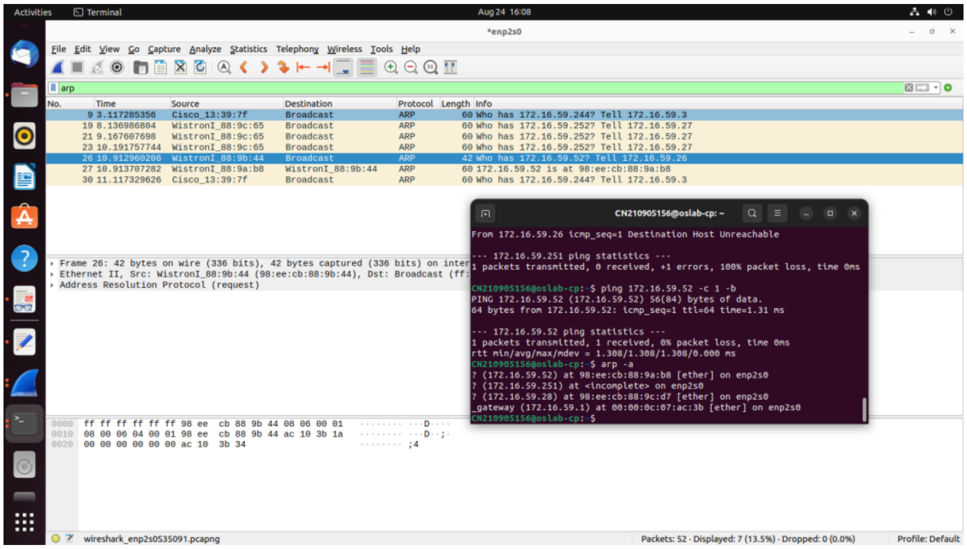
Even though, I transmitted only 1 packet. But as the ip address is non existent so it's mac address wasn't found and it was retransmitted twice. Hence, in total 3 attempts were made.


Activities
Wireshark
Aug 24 16:04
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp
No.    Time          Source               Destination   Protocol  Length  Info
    72 5.101684750   WistronI_88:9b:44    Broadcast     ARP           42 Who has 172.16.59.251? Tell 172.16.59.26
    73 5.796162977   WistronI_88:9b:c0    Broadcast     ARP           60 Who has 172.16.59.151? Tell 172.16.59.34
    74 6.112027275   WistronI_88:9b:44    Broadcast     ARP           42 Who has 172.16.59.251? Tell 172.16.59.26
    77 6.820422033   WistronI_88:9b:c0    Broadcast     ARP           60 Who has 172.16.59.151? Tell 172.16.59.34
    80 7.136180133   WistronI_88:9b:44    Broadcast     ARP           42 Who has 172.16.59.251? Tell 172.16.59.26
    82 7.844514021   WistronI_88:9b:c0    Broadcast     ARP           60 Who has 172.16.59.151? Tell 172.16.59.34

wireshark_enp2s0VF6991.pcapng        Packets: 102 · Displayed: 6 (5.9%) · Dropped: 0 (0.0%)        Profile: Default
```

Now, when I pinged a local known ip address, I am able to see it's mac address after just 1 attempt.


Activities
Terminal
Aug 24 16:08
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
CN210905156@oslab-cp: ~

```
arp
No.    Time          Source               Destination          Protocol  Length  Info
     9 3.117285356   Cisco_13:39:7f       Broadcast            ARP           60 Who has 172.16.59.244? Tell 172.16.59.3
    19 8.136986804   WistronI_88:9c:65    Broadcast            ARP           60 Who has 172.16.59.252? Tell 172.16.59.27
    21 9.167607698   WistronI_88:9c:65    Broadcast            ARP           60 Who has 172.16.59.252? Tell 172.16.59.27
    23 10.191757744  WistronI_88:9c:65    Broadcast            ARP           60 Who has 172.16.59.252? Tell 172.16.59.27
    26 10.912960206  WistronI_88:9b:44    Broadcast            ARP           42 Who has 172.16.59.52? Tell 172.16.59.26
    27 10.913707282  WistronI_88:9a:b8    WistronI_88:9b:44    ARP           60 172.16.59.52 is at 98:ee:cb:88:9a:b8
    30 11.117329626  Cisco_13:39:7f       Broadcast            ARP           60 Who has 172.16.59.244? Tell 172.16.59.3

▸ Frame 26: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on inter
▸ Ethernet II, Src: WistronI_88:9b:44 (98:ee:cb:88:9b:44), Dst: Broadcast (ff:
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 98 ee  cb 88 9b 44 08 06 00 01   ········ ···D····
0010  08 00 06 04 00 01 98 ee  cb 88 9b 44 ac 10 3b 1a   ········ ···D··;·
0020  00 00 00 00 00 00 ac 10  3b 34                     ········ ;4

wireshark_enp2s0535091.pcapng        Packets: 52 · Displayed: 7 (13.5%) · Dropped: 0 (0.0%)        Profile: Default
```

```
From 172.16.59.26 icmp_seq=1 Destination Host Unreachable

--- 172.16.59.251 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

CN210905156@oslab-cp:~$ ping 172.16.59.52 -c 1 -b
PING 172.16.59.52 (172.16.59.52) 56(84) bytes of data.
64 bytes from 172.16.59.52: icmp_seq=1 ttl=64 time=1.31 ms

--- 172.16.59.52 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.308/1.308/1.308/0.000 ms
CN210905156@oslab-cp:~$ arp -a
? (172.16.59.52) at 98:ee:cb:88:9a:b8 [ether] on enp2s0
? (172.16.59.251) at <incomplete> on enp2s0
? (172.16.59.28) at 98:ee:cb:88:9c:d7 [ether] on enp2s0
_gateway (172.16.59.1) at 00:00:0c:07:ac:3b [ether] on enp2s0
CN210905156@oslab-cp:~$
```

Q3.

a. `tcpdump udp port 520`: This expression captures network traffic that uses the UDP protocol and is sent to or from port 520. Port 520 is commonly associated with the Routing Information Protocol (RIP), which is used in routing tables on routers.

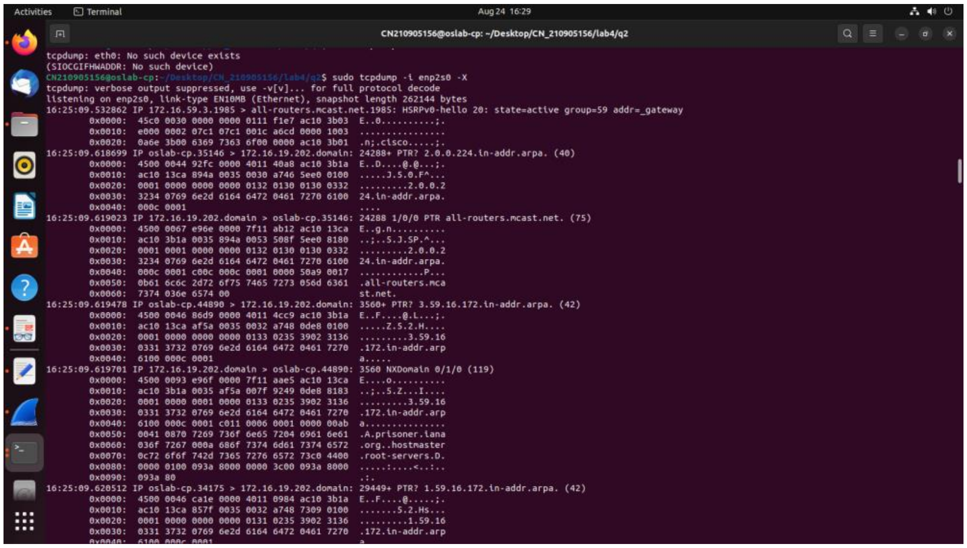
b. `tcpdump -x -s 120 ip proto 89`: This expression captures IP packets (IPv4) with protocol number 89. Protocol number 89 corresponds to the OSPF (Open Shortest Path First) protocol, which is used for dynamic routing in IP networks. The `-x` option prints the packet data in hexadecimal and ASCII formats, and the `-s 120` option sets the snap length to 120 bytes, limiting the amount of data captured per packet.

c. `tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)`: This expression captures packets sent to or from the host with IP address `ip addr1`. Additionally, it includes packets sent to or from either `ip addr2` or `ip addr3`. The `-x` option displays packet data in hexadecimal and ASCII formats, and the `-s 70` option sets the snap length to 70 bytes.

d. `tcpdump -x -s 70 host ip addr1 and not ip addr2`: This expression captures packets sent to or from the host with IP address `ip addr1`. However, it excludes packets sent to or from `ip addr2`. The `-x` option displays packet data in hexadecimal and ASCII formats, and the `-s 70` option sets the snap length to 70 bytes.

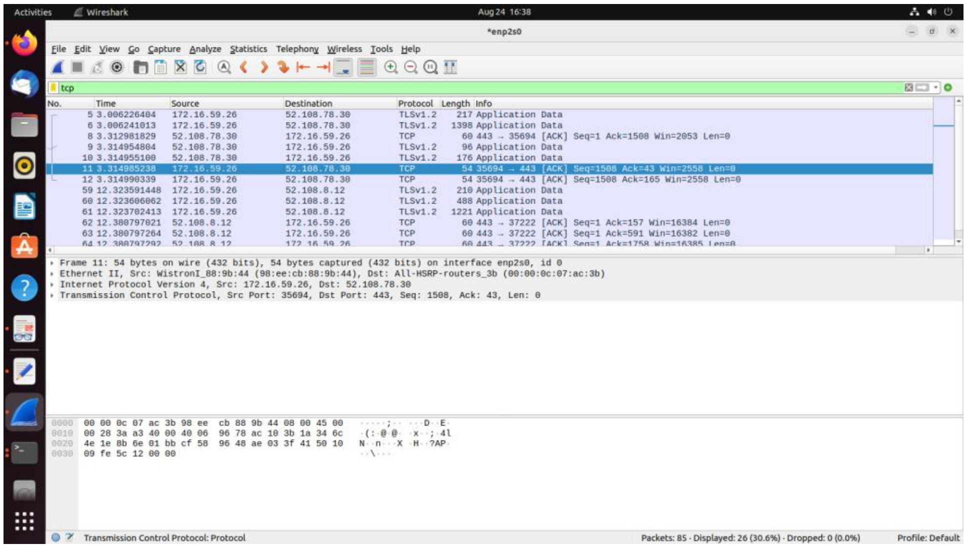
Q4.

tcpdump command to dump network traffic: sudo tcpdump -i enp2s0 –X



```
tcpdump: eth0: No such device exists
(SIOCGIFHWADDR: No such device)
CN210905156@oslab-cp:~/Desktop/CN_210905156/lab4/q2$ sudo tcpdump -i enp2s0 -X
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:25:09.532862 IP 172.16.59.3.1985 > all-routers.mcast.net.1985: HSRPv0-hello 20: state=active group=59 addr=_gateway
        0x0000:  45c0 0030 0000 0000 0111 f1e7 ac10 3b03  E..0..........;.
        0x0010:  e000 0002 07c1 07c1 001c a6cd 0000 1003  ................
        0x0020:  0a6e 3b00 6369 7363 6f00 0000 ac10 3b01  .n;.cisco.....;.
16:25:09.618699 IP oslab-cp.35146 > 172.16.19.202.domain: 24288+ PTR? 2.0.0.224.in-addr.arpa. (40)
        0x0000:  4500 0044 92fc 0000 4011 40a8 ac10 3b1a  E..D....@.@...;.
        0x0010:  ac10 13ca 894a 0035 0030 a746 5ee0 0100  .....J.5.0.F^...
        0x0020:  0001 0000 0000 0000 0132 0130 0130 0332  .........2.0.0.2
        0x0030:  3234 0769 6e2d 6164 6472 0461 7270 6100  24.in-addr.arpa.
        0x0040:  000c 0001                                ....
16:25:09.619023 IP 172.16.19.202.domain > oslab-cp.35146: 24288 1/0/0 PTR all-routers.mcast.net. (75)
        0x0000:  4500 0067 e96e 0000 7f11 ab12 ac10 13ca  E..g.n..........
        0x0010:  ac10 3b1a 0035 894a 0053 508f 5ee0 8180  ..;..5.J.SP.^...
        0x0020:  0001 0001 0000 0000 0132 0130 0130 0332  .........2.0.0.2
        0x0030:  3234 0769 6e2d 6164 6472 0461 7270 6100  24.in-addr.arpa.
        0x0040:  000c 0001 c00c 000c 0001 0000 50a9 0017  ............P...
        0x0050:  0b61 6c6c 2d72 6f75 7465 7273 056d 6361  .all-routers.mca
        0x0060:  7374 036e 6574 00                        st.net.
16:25:09.619478 IP oslab-cp.44890 > 172.16.19.202.domain: 3560+ PTR? 3.59.16.172.in-addr.arpa. (42)
        0x0000:  4500 0046 86d9 0000 4011 4cc9 ac10 3b1a  E..F....@.L...;.
        0x0010:  ac10 13ca af5a 0035 0032 a748 0de8 0100  .....Z.5.2.H....
        0x0020:  0001 0000 0000 0000 0133 0235 3902 3136  .........3.59.16
        0x0030:  0331 3732 0769 6e2d 6164 6472 0461 7270  .172.in-addr.arp
        0x0040:  6100 000c 0001                           a.....
16:25:09.619701 IP 172.16.19.202.domain > oslab-cp.44890: 3560 NXDomain 0/1/0 (119)
        0x0000:  4500 0093 e96f 0000 7f11 aae5 ac10 13ca  E....o..........
        0x0010:  ac10 3b1a 0035 af5a 007f 9249 0de8 8183  ..;..5.Z...I....
        0x0020:  0001 0000 0001 0000 0133 0235 3902 3136  .........3.59.16
        0x0030:  0331 3732 0769 6e2d 6164 6472 0461 7270  .172.in-addr.arp
        0x0040:  6100 000c 0001 c011 0006 0001 0000 00ab  a...............
        0x0050:  0041 0870 7269 736f 6e65 7204 6961 6e61  .A.prisoner.iana
        0x0060:  036f 7267 000a 686f 7374 6d61 7374 6572  .org..hostmaster
        0x0070:  0c72 6f6f 742d 7365 7276 6572 73c0 4400  .root-servers.D.
        0x0080:  0000 0100 093a 8000 0000 3c00 093a 8000  .....:....<..:..
        0x0090:  093a 80                                  .:.
16:25:09.620512 IP oslab-cp.34175 > 172.16.19.202.domain: 29449+ PTR? 1.59.16.172.in-addr.arpa. (42)
        0x0000:  4500 0046 ca1e 0000 4011 0984 ac10 3b1a  E..F....@.....;.
        0x0010:  ac10 13ca 857f 0035 0032 a748 7309 0100  .......5.2.Hs...
        0x0020:  0001 0000 0000 0000 0131 0235 3902 3136  .........1.59.16
        0x0030:  0331 3732 0769 6e2d 6164 6472 0461 7270  .172.in-addr.arp
        0x0040:  6100 000c 0001                           a
```

a)
sudo tcpdump -s 65535 -xa -w q4.pcap


Activities
Wireshark
Aug 24 16:38
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time          Source          Destination     Protocol  Length Info
   5 3.006226404   172.16.59.26    52.108.78.30    TLSv1.2    217 Application Data
   6 3.006241013   172.16.59.26    52.108.78.30    TLSv1.2   1398 Application Data
   8 3.312981829   52.108.78.30    172.16.59.26    TCP         60 443 → 35694 [ACK] Seq=1 Ack=1508 Win=2053 Len=0
   9 3.314954804   52.108.78.30    172.16.59.26    TLSv1.2     96 Application Data
  10 3.314955100   52.108.78.30    172.16.59.26    TLSv1.2    176 Application Data
  11 3.314985238   172.16.59.26    52.108.78.30    TCP         54 35694 → 443 [ACK] Seq=1508 Ack=43 Win=2558 Len=0
  12 3.314990339   172.16.59.26    52.108.78.30    TCP         54 35694 → 443 [ACK] Seq=1508 Ack=165 Win=2558 Len=0
  59 12.323591448  172.16.59.26    52.108.8.12     TLSv1.2    210 Application Data
  60 12.323606062  172.16.59.26    52.108.8.12     TLSv1.2    488 Application Data
  61 12.323702413  172.16.59.26    52.108.8.12     TLSv1.2   1221 Application Data
  62 12.380797021  52.108.8.12     172.16.59.26    TCP         60 443 → 37222 [ACK] Seq=1 Ack=157 Win=16384 Len=0
  63 12.380797264  52.108.8.12     172.16.59.26    TCP         60 443 → 37222 [ACK] Seq=1 Ack=591 Win=16382 Len=0
  64 12.380797292  52.108.8.12     172.16.59.26    TCP         60 443 → 37222 [ACK] Seq=1 Ack=1758 Win=16385 Len=0

› Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp2s0, id 0
› Ethernet II, Src: WistronI_88:9b:44 (98:ee:cb:88:9b:44), Dst: All-HSRP-routers_3b (00:00:0c:07:ac:3b)
› Internet Protocol Version 4, Src: 172.16.59.26, Dst: 52.108.78.30
› Transmission Control Protocol, Src Port: 35694, Dst Port: 443, Seq: 1508, Ack: 43, Len: 0

0000  00 00 0c 07 ac 3b 98 ee  cb 88 9b 44 08 00 45 00   ·····;·· ···D··E·
0010  00 28 3a a3 40 00 40 06  96 78 ac 10 3b 1a 34 6c   ·(:·@·@· ·x··;·4l
0020  4e 1e 8b 6e 01 bb cf 58  96 48 ae 03 3f 41 50 10   N··n···X ·H··?AP·
0030  09 fe 5c 12 00 00                                  ··\···
```

Transmission Control Protocol: Protocol
Packets: 85 · Displayed: 26 (30.6%) · Dropped: 0 (0.0%)
Profile: Default

b)

IP address:

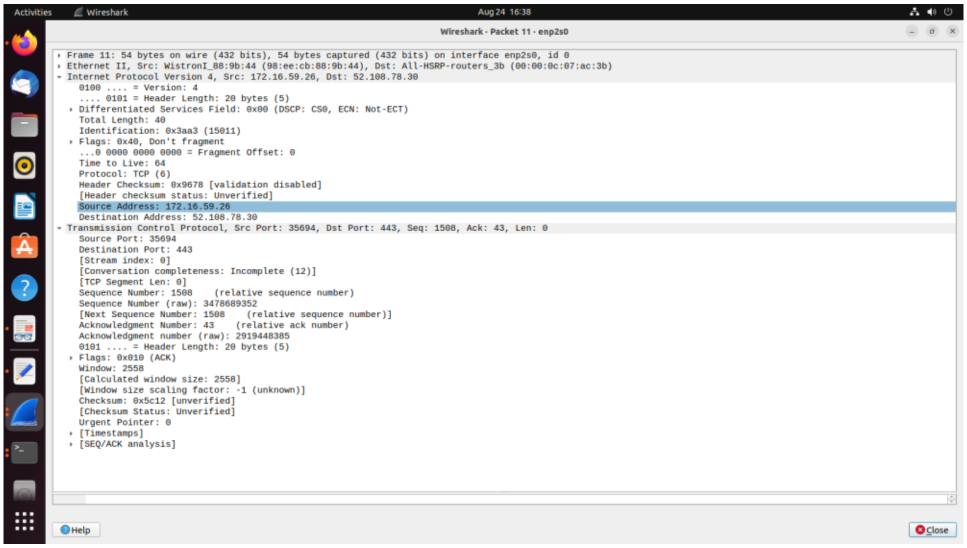
Source Address: 172.16.59.26

Destination Address: 52.108.78.30

Packet length = TCP Segment Len =0

Transmission Control Protocol, Src Port: 35694, Dst Port: 443

Flags: 0x010 (ACK)



```
› Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp2s0, id 0
› Ethernet II, Src: WistronI_88:9b:44 (98:ee:cb:88:9b:44), Dst: All-HSRP-routers_3b (00:00:0c:07:ac:3b)
˅ Internet Protocol Version 4, Src: 172.16.59.26, Dst: 52.108.78.30
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x3aa3 (15011)
  › Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9678 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.59.26
    Destination Address: 52.108.78.30
˅ Transmission Control Protocol, Src Port: 35694, Dst Port: 443, Seq: 1508, Ack: 43, Len: 0
    Source Port: 35694
    Destination Port: 443
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 1508    (relative sequence number)
    Sequence Number (raw): 3478689352
    [Next Sequence Number: 1508    (relative sequence number)]
    Acknowledgment Number: 43    (relative ack number)
    Acknowledgment number (raw): 2919448385
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x010 (ACK)
    Window: 2558
    [Calculated window size: 2558]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5c12 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
  › [SEQ/ACK analysis]
```