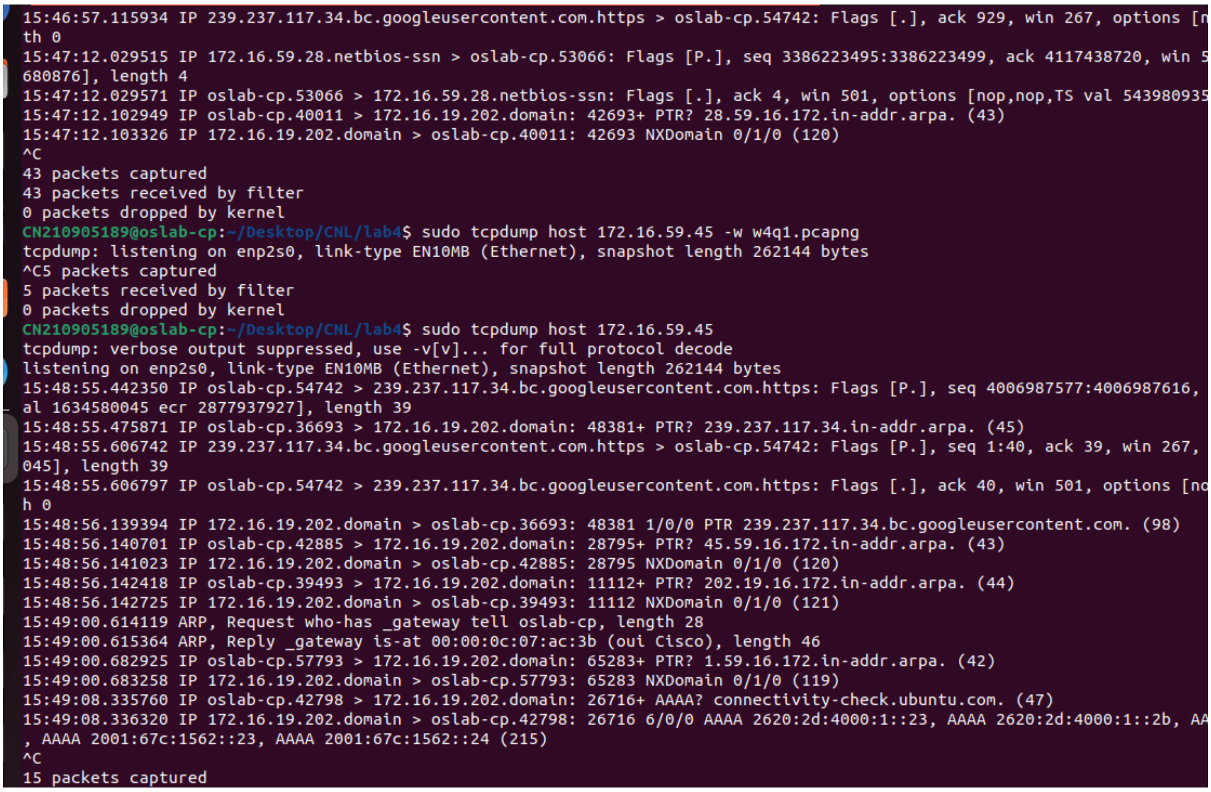
CNL LAB 4
KUSHALA SARADA A V
210905189
ROLL NO 33

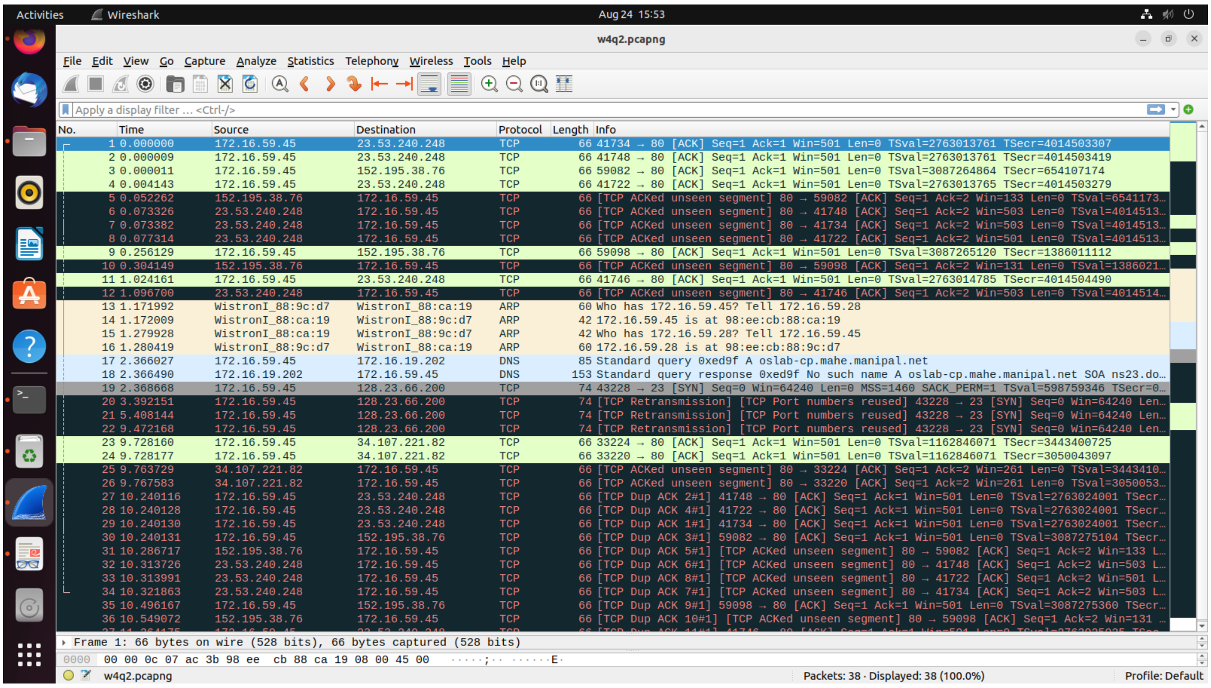
1. While tcpdump host your_host is running in one command window, run ping 127.0.0.1 from another command window. From the ping output, is the 127.0.0.1 interface on? Can you see any ICMP message sent from your host in the tcpdump output? Why?



```
15:46:57.115934 IP 239.237.117.34.bc.googleusercontent.com.https > oslab-cp.54742: Flags [.], ack 929, win 267, options [n
th 0
15:47:12.029515 IP 172.16.59.28.netbios-ssn > oslab-cp.53066: Flags [P.], seq 3386223495:3386223499, ack 4117438720, win 5
680876], length 4
15:47:12.029571 IP oslab-cp.53066 > 172.16.59.28.netbios-ssn: Flags [.], ack 4, win 501, options [nop,nop,TS val 543980935
15:47:12.102949 IP oslab-cp.40011 > 172.16.19.202.domain: 42693+ PTR? 28.59.16.172.in-addr.arpa. (43)
15:47:12.103326 IP 172.16.19.202.domain > oslab-cp.40011: 42693 NXDomain 0/1/0 (120)
^C
43 packets captured
43 packets received by filter
0 packets dropped by kernel
CN210905189@oslab-cp:~/Desktop/CNL/lab4$ sudo tcpdump host 172.16.59.45 -w w4q1.pcapng
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C5 packets captured
5 packets received by filter
0 packets dropped by kernel
CN210905189@oslab-cp:~/Desktop/CNL/lab4$ sudo tcpdump host 172.16.59.45
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:48:55.442350 IP oslab-cp.54742 > 239.237.117.34.bc.googleusercontent.com.https: Flags [P.], seq 4006987577:4006987616,
al 1634580045 ecr 2877937927], length 39
15:48:55.475871 IP oslab-cp.36693 > 172.16.19.202.domain: 48381+ PTR? 239.237.117.34.in-addr.arpa. (45)
15:48:55.606742 IP 239.237.117.34.bc.googleusercontent.com.https > oslab-cp.54742: Flags [P.], seq 1:40, ack 39, win 267,
045], length 39
15:48:55.606797 IP oslab-cp.54742 > 239.237.117.34.bc.googleusercontent.com.https: Flags [.], ack 40, win 501, options [no
h 0
15:48:56.139394 IP 172.16.19.202.domain > oslab-cp.36693: 48381 1/0/0 PTR 239.237.117.34.bc.googleusercontent.com. (98)
15:48:56.140701 IP oslab-cp.42885 > 172.16.19.202.domain: 28795+ PTR? 45.59.16.172.in-addr.arpa. (43)
15:48:56.141023 IP 172.16.19.202.domain > oslab-cp.42885: 28795 NXDomain 0/1/0 (120)
15:48:56.142418 IP oslab-cp.39493 > 172.16.19.202.domain: 11112+ PTR? 202.19.16.172.in-addr.arpa. (44)
15:48:56.142725 IP 172.16.19.202.domain > oslab-cp.39493: 11112 NXDomain 0/1/0 (121)
15:49:00.614119 ARP, Request who-has _gateway tell oslab-cp, length 28
15:49:00.615364 ARP, Reply _gateway is-at 00:00:0c:07:ac:3b (oui Cisco), length 46
15:49:00.682925 IP oslab-cp.57793 > 172.16.19.202.domain: 65283+ PTR? 1.59.16.172.in-addr.arpa. (42)
15:49:00.683258 IP 172.16.19.202.domain > oslab-cp.57793: 65283 NXDomain 0/1/0 (119)
15:49:08.335760 IP oslab-cp.42798 > 172.16.19.202.domain: 26716+ AAAA? connectivity-check.ubuntu.com. (47)
15:49:08.336320 IP 172.16.19.202.domain > oslab-cp.42798: 26716 6/0/0 AAAA 2620:2d:4000:1::23, AAAA 2620:2d:4000:1::2b, AA
, AAAA 2001:67c:1562::23, AAAA 2001:67c:1562::24 (215)
^C
15 packets captured
```

- Running `tcpdump host your_host` captures traffic to/from the specified IP address.
- Using `tcpdump host 127.0.0.1` captures traffic on the loopback interface.
- Loopback interface (127.0.0.1) allows local communication within a device.
- `ping 127.0.0.1` sends ICMP echo requests to test the loopback interface.
- Loopback interface is always active and integral to networking.
- With `tcpdump host 127.0.0.1` and `ping` running, ICMP traffic is captured.
- ICMP echo requests go to the loopback interface internally.
- `tcpdump` captures traffic at the network level as packets move between interfaces.
- `tcpdump` intercepts ICMP echo requests in loopback traffic.
- Capturing loopback traffic in `tcpdump` shows internal communication.
- Loopback traffic can contain system-related data, not just user data.

2. While tcpdump host your_host is running to capture traffic from your machine, execute telnet 128.238.66.200. Note there is no host with this IP address in the current configuration of the lab network. Save the tcpdump output of the first few packets for the lab report. After getting the necessary output, terminate the telnet session. From the saved tcpdump output, describe how the ARP timeout and retransmission were performed. How many attempts were made to resolve a non-existing IP address?


Activities
Wireshark
Aug 24 15:53
w4q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.59.45	23.53.240.248	TCP	66	41734 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763013761 TSecr=4014503307
2	0.000009	172.16.59.45	23.53.240.248	TCP	66	41748 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763013761 TSecr=4014503419
3	0.000011	172.16.59.45	152.195.38.76	TCP	66	59082 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3087264864 TSecr=654107174
4	0.004143	172.16.59.45	23.53.240.248	TCP	66	41722 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763013765 TSecr=4014503279
5	0.052262	152.195.38.76	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 59082 [ACK] Seq=1 Ack=2 Win=133 Len=0 TSval=6541173…
6	0.073326	23.53.240.248	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 41748 [ACK] Seq=1 Ack=2 Win=503 Len=0 TSval=4014513…
7	0.073382	23.53.240.248	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 41734 [ACK] Seq=1 Ack=2 Win=503 Len=0 TSval=4014513…
8	0.077314	23.53.240.248	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 41722 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=4014513…
9	0.256129	172.16.59.45	152.195.38.76	TCP	66	59098 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3087265120 TSecr=1386011112
10	0.304149	152.195.38.76	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 59098 [ACK] Seq=1 Ack=2 Win=131 Len=0 TSval=1386021…
11	1.024161	172.16.59.45	23.53.240.248	TCP	66	41746 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763014785 TSecr=4014504490
12	1.096700	23.53.240.248	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 41746 [ACK] Seq=1 Ack=2 Win=503 Len=0 TSval=4014514…
13	1.171992	WistronI_88:9c:d7	WistronI_88:ca:19	ARP	60	Who has 172.16.59.45? Tell 172.16.59.28
14	1.172009	WistronI_88:ca:19	WistronI_88:9c:d7	ARP	42	172.16.59.45 is at 98:ee:cb:88:ca:19
15	1.279928	WistronI_88:ca:19	WistronI_88:9c:d7	ARP	42	Who has 172.16.59.28? Tell 172.16.59.45
16	1.280419	WistronI_88:9c:d7	WistronI_88:ca:19	ARP	60	172.16.59.28 is at 98:ee:cb:88:9c:d7
17	2.366027	172.16.59.45	172.16.19.202	DNS	85	Standard query 0xed9f A oslab-cp.mahe.manipal.net
18	2.366490	172.16.19.202	172.16.59.45	DNS	153	Standard query response 0xed9f No such name A oslab-cp.mahe.manipal.net SOA ns23.do…
19	2.368668	172.16.59.45	128.23.66.200	TCP	74	43228 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=598759346 TSecr=0…
20	3.392151	172.16.59.45	128.23.66.200	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 43228 → 23 [SYN] Seq=0 Win=64240 Len…
21	5.408144	172.16.59.45	128.23.66.200	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 43228 → 23 [SYN] Seq=0 Win=64240 Len…
22	9.472168	172.16.59.45	128.23.66.200	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 43228 → 23 [SYN] Seq=0 Win=64240 Len…
23	9.728160	172.16.59.45	34.107.221.82	TCP	66	33224 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1162846071 TSecr=3443400725
24	9.728177	172.16.59.45	34.107.221.82	TCP	66	33220 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1162846071 TSecr=3050043097
25	9.763729	34.107.221.82	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 33224 [ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=3443410…
26	9.767583	34.107.221.82	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 33220 [ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=3050053…
27	10.240116	172.16.59.45	23.53.240.248	TCP	66	[TCP Dup ACK 2#1] 41748 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763024001 TSecr…
28	10.240128	172.16.59.45	23.53.240.248	TCP	66	[TCP Dup ACK 4#1] 41722 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763024001 TSecr…
29	10.240130	172.16.59.45	23.53.240.248	TCP	66	[TCP Dup ACK 1#1] 41734 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2763024001 TSecr…
30	10.240131	172.16.59.45	152.195.38.76	TCP	66	[TCP Dup ACK 3#1] 59082 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3087275104 TSecr…
31	10.286717	152.195.38.76	172.16.59.45	TCP	66	[TCP Dup ACK 5#1] [TCP ACKed unseen segment] 80 → 59082 [ACK] Seq=1 Ack=2 Win=133 L…
32	10.313726	23.53.240.248	172.16.59.45	TCP	66	[TCP Dup ACK 6#1] [TCP ACKed unseen segment] 80 → 41748 [ACK] Seq=1 Ack=2 Win=503 L…
33	10.313991	23.53.240.248	172.16.59.45	TCP	66	[TCP Dup ACK 8#1] [TCP ACKed unseen segment] 80 → 41722 [ACK] Seq=1 Ack=2 Win=501 L…
34	10.321863	23.53.240.248	172.16.59.45	TCP	66	[TCP Dup ACK 7#1] [TCP ACKed unseen segment] 80 → 41734 [ACK] Seq=1 Ack=2 Win=503 L…
35	10.496167	172.16.59.45	152.195.38.76	TCP	66	[TCP Dup ACK 9#1] 59098 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3087275360 TSecr…
36	10.549072	152.195.38.76	172.16.59.45	TCP	66	[TCP Dup ACK 10#1] [TCP ACKed unseen segment] 80 → 59098 [ACK] Seq=1 Ack=2 Win=131 …

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
0000  00 00 0c 07 ac 3b 98 ee  cb 88 ca 19 08 00 45 00   ·····;·· ······E·
```

w4q2.pcapng Packets: 38 · Displayed: 38 (100.0%) Profile: Default

- ARP broadcasts IP-to-MAC address queries in local networks.
- Unanswered ARP requests lead to retransmissions for address resolution.
- The "telnet 128.238.66.200" command triggers ARP requests.
- 2 ARP requests for 128.238.66.200 show in tcpdump without replies.
- This indicates timeout and retransmission due to unresolved IP.
- The process aims for successful resolution through multiple attempts.

3. Briefly explain the purposes of the following tcpdump expressions.
a. tcpdump udp port 520
b. tcpdump -x -s 120 ip proto 89
c. tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)
d. tcpdump -x -s 70 host ip addr1 and not ip addr2

- a. `tcpdump udp port 520`**
  - Captures UDP traffic to/from port 520.
  - Used for analyzing Routing Information Protocol (RIP) traffic.

- b. `tcpdump -x -s 120 ip proto 89`**
  - Captures IP packets with protocol number 89 (OSPF).
  - Displays packets in hexadecimal and ASCII format.
  - Limits capture to 120 bytes for examining OSPF packet contents.

- c. `tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)`
  - Captures traffic to/from `ip addr1`.
  - Includes traffic involving `ip addr2` or `ip addr3`.
  - Displays packets in hex/ASCII format.
  - Limits capture to 70 bytes for analyzing specific host communication.

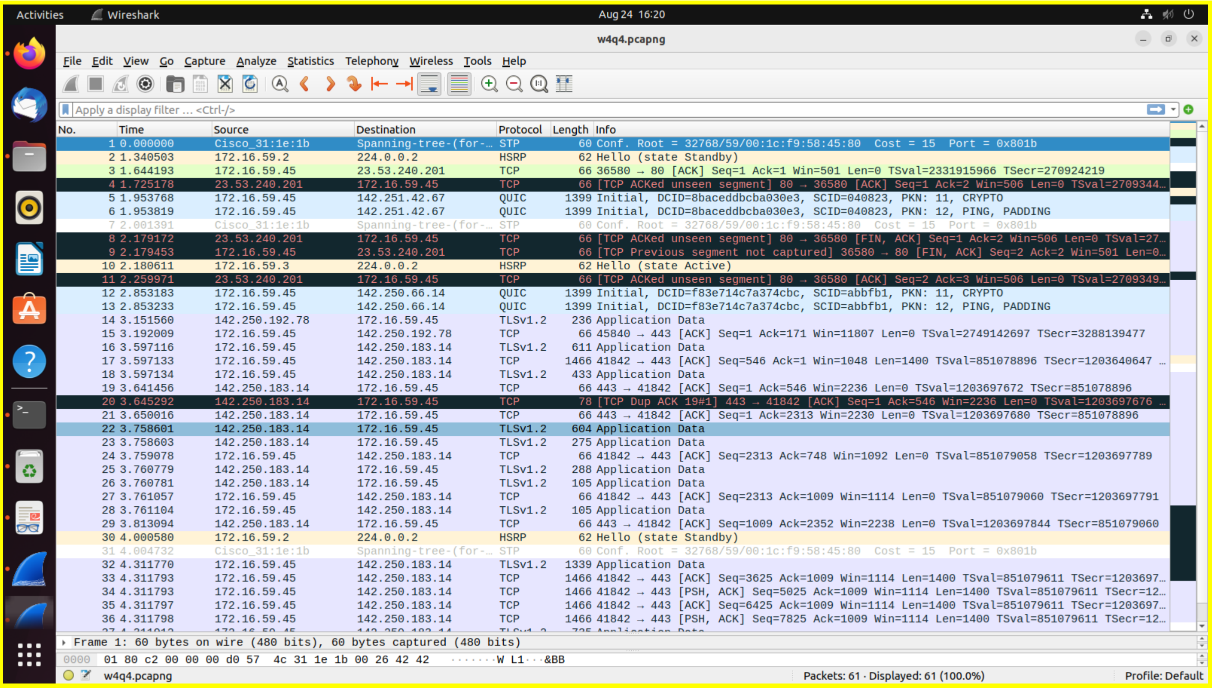
- d. `tcpdump -x -s 70 host ip addr1 and not ip addr2`
  - Captures traffic to/from `ip addr1`.
  - Excludes communication involving `ip addr2`.
  - Displays packets in hex/ASCII format.
  - Limits capture to 70 bytes for focused host analysis.

4. Basic packet decoding

1) Write a tcpdump command to dump network traffic from an Ethernet connection to the screen in human readable output format. Perform the following operation and write down the observations.

a) Capture all the traffic of maximum snap length of 65,535 bytes and provide the hexadecimal and ASCII decodes of all the traffic in each packet.

b) Find the IP addresses, IP packet length, TCP port numbers, TCP flags, etc. by using the reference chart to locate those fields on the hexadecimal dump.


Activities
Wireshark
Aug 24 16:20
w4q4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_31:1e:1b	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/59/00:1c:f9:58:45:80 Cost = 15 Port = 0x801b
2	1.340503	172.16.59.2	224.0.0.2	HSRP	62	Hello (state Standby)
3	1.644193	172.16.59.45	23.53.240.201	TCP	66	36580 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2331915966 TSecr=270924219
4	1.725178	23.53.240.201	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 36580 [ACK] Seq=1 Ack=2 Win=506 Len=0 TSval=2709344…
5	1.953768	172.16.59.45	142.251.42.67	QUIC	1399	Initial, DCID=8baceddbcba030e3, SCID=040823, PKN: 11, CRYPTO
6	1.953819	172.16.59.45	142.251.42.67	QUIC	1399	Initial, DCID=8baceddbcba030e3, SCID=040823, PKN: 12, PING, PADDING
7	2.001391	Cisco_31:1e:1b	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/59/00:1c:f9:58:45:80 Cost = 15 Port = 0x801b
8	2.179172	23.53.240.201	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 36580 [FIN, ACK] Seq=1 Ack=2 Win=506 Len=0 TSval=27…
9	2.179453	172.16.59.45	23.53.240.201	TCP	66	[TCP Previous segment not captured] 36580 → 80 [FIN, ACK] Seq=2 Ack=2 Win=501 Len=0…
10	2.180611	172.16.59.3	224.0.0.2	HSRP	62	Hello (state Active)
11	2.259971	23.53.240.201	172.16.59.45	TCP	66	[TCP ACKed unseen segment] 80 → 36580 [ACK] Seq=2 Ack=3 Win=506 Len=0 TSval=2709349…
12	2.853183	172.16.59.45	142.250.66.14	QUIC	1399	Initial, DCID=f83e714c7a374cbc, SCID=abbfb1, PKN: 11, CRYPTO
13	2.853233	172.16.59.45	142.250.66.14	QUIC	1399	Initial, DCID=f83e714c7a374cbc, SCID=abbfb1, PKN: 12, PING, PADDING
14	3.151560	142.250.192.78	172.16.59.45	TLSv1.2	236	Application Data
15	3.192009	172.16.59.45	142.250.192.78	TCP	66	45840 → 443 [ACK] Seq=1 Ack=171 Win=11807 Len=0 TSval=2749142697 TSecr=3288139477
16	3.597116	172.16.59.45	142.250.183.14	TLSv1.2	611	Application Data
17	3.597133	172.16.59.45	142.250.183.14	TCP	1466	41842 → 443 [ACK] Seq=546 Ack=1 Win=1048 Len=1400 TSval=851078896 TSecr=1203640647 …
18	3.597134	172.16.59.45	142.250.183.14	TLSv1.2	433	Application Data
19	3.641456	142.250.183.14	172.16.59.45	TCP	66	443 → 41842 [ACK] Seq=1 Ack=546 Win=2236 Len=0 TSval=1203697672 TSecr=851078896
20	3.645292	142.250.183.14	172.16.59.45	TCP	78	[TCP Dup ACK 19#1] 443 → 41842 [ACK] Seq=1 Ack=546 Win=2236 Len=0 TSval=1203697676 …
21	3.650016	142.250.183.14	172.16.59.45	TCP	66	443 → 41842 [ACK] Seq=1 Ack=2313 Win=2230 Len=0 TSval=1203697680 TSecr=851078896
22	3.758601	142.250.183.14	172.16.59.45	TLSv1.2	604	Application Data
23	3.758603	142.250.183.14	172.16.59.45	TLSv1.2	275	Application Data
24	3.759078	172.16.59.45	142.250.183.14	TCP	66	41842 → 443 [ACK] Seq=2313 Ack=748 Win=1092 Len=0 TSval=851079058 TSecr=1203697789
25	3.760779	142.250.183.14	172.16.59.45	TLSv1.2	288	Application Data
26	3.760781	142.250.183.14	172.16.59.45	TLSv1.2	105	Application Data
27	3.761057	172.16.59.45	142.250.183.14	TCP	66	41842 → 443 [ACK] Seq=2313 Ack=1009 Win=1114 Len=0 TSval=851079060 TSecr=1203697791
28	3.761104	172.16.59.45	142.250.183.14	TLSv1.2	105	Application Data
29	3.813094	142.250.183.14	172.16.59.45	TCP	66	443 → 41842 [ACK] Seq=1009 Ack=2352 Win=2238 Len=0 TSval=1203697844 TSecr=851079060
30	4.000580	172.16.59.2	224.0.0.2	HSRP	62	Hello (state Standby)
31	4.004732	Cisco_31:1e:1b	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/59/00:1c:f9:58:45:80 Cost = 15 Port = 0x801b
32	4.311770	172.16.59.45	142.250.183.14	TLSv1.2	1339	Application Data
33	4.311793	172.16.59.45	142.250.183.14	TCP	1466	41842 → 443 [ACK] Seq=3625 Ack=1009 Win=1114 Len=1400 TSval=851079611 TSecr=1203697…
34	4.311793	172.16.59.45	142.250.183.14	TCP	1466	41842 → 443 [PSH, ACK] Seq=5025 Ack=1009 Win=1114 Len=1400 TSval=851079611 TSecr=12…
35	4.311797	172.16.59.45	142.250.183.14	TCP	1466	41842 → 443 [ACK] Seq=6425 Ack=1009 Win=1114 Len=1400 TSval=851079611 TSecr=1203697…
36	4.311798	172.16.59.45	142.250.183.14	TCP	1466	41842 → 443 [PSH, ACK] Seq=7825 Ack=1009 Win=1114 Len=1400 TSval=851079611 TSecr=12…

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
0000  01 80 c2 00 00 00 d0 57  4c 31 1e 1b 00 26 42 42   ·······W L1···&BB
```

-i enp2s0 specifies the interface to capture traffic from.

● -XX tells tcpdump to display the packet data in both hexadecimal and ASCII formats.

sudo tcpdump -i enp2s0 -XX -w w4q4.pcapng