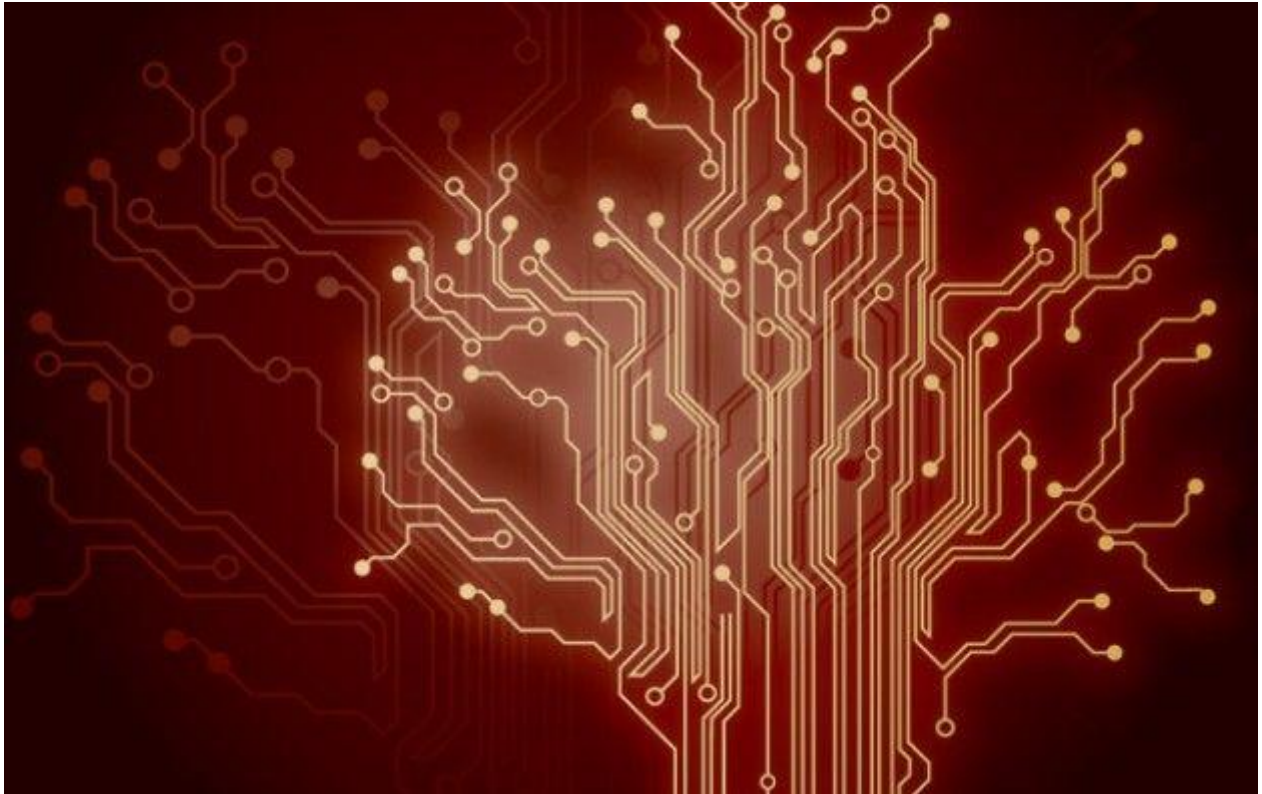


NETWORK LAB REPORT

CO5 : Packet tracer and traffic analysis with Wireshark.



Atanu Ghosh

BCSE-III (2019-2023) 5th sem, Section: A-1,

Roll: 001910501005, Date: 31/10/2021

ASSIGNMENT-5

Packet tracer and traffic analysis with Wireshark

PROBLEM STATEMENT

Overview:

Wireshark is an open-source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

The Wireshark User Guide can be found at: http://www.wireshark.org/docs/wsug_html_chunked/

Capturing Packets:

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

Specifications:

1. **OS** : Linux
2. **Distro** : Ubuntu 20.04 LTS
3. **Version** : Wireshark 3.4.8
4. **Network** : Wireless network (WIFI)

Questions and Solutions:

Q1. Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighbouring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.

```
fish /home/inferno

+ ping 192.168.193.6
PING 192.168.193.6 (192.168.193.6) 56(84) bytes of data.
64 bytes from 192.168.193.6: icmp_seq=1 ttl=64 time=1990 ms
64 bytes from 192.168.193.6: icmp_seq=2 ttl=64 time=1807 ms
64 bytes from 192.168.193.6: icmp_seq=3 ttl=64 time=2205 ms
64 bytes from 192.168.193.6: icmp_seq=4 ttl=64 time=2520 ms
64 bytes from 192.168.193.6: icmp_seq=5 ttl=64 time=2297 ms
64 bytes from 192.168.193.6: icmp_seq=6 ttl=64 time=2638 ms
64 bytes from 192.168.193.6: icmp_seq=7 ttl=64 time=2548 ms
64 bytes from 192.168.193.6: icmp_seq=8 ttl=64 time=2276 ms
^C
--- 192.168.193.6 ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9014ms
rtt min/avg/max/mdev = 1806.645/2285.038/2638.355/267.292 ms, pipe 3

+ ping 192.168.193.6
PING 192.168.193.6 (192.168.193.6) 56(84) bytes of data.
64 bytes from 192.168.193.6: icmp_seq=1 ttl=64 time=2.71 ms
64 bytes from 192.168.193.6: icmp_seq=2 ttl=64 time=4.71 ms
64 bytes from 192.168.193.6: icmp_seq=3 ttl=64 time=3.05 ms
64 bytes from 192.168.193.6: icmp_seq=4 ttl=64 time=4.08 ms
64 bytes from 192.168.193.6: icmp_seq=5 ttl=64 time=4.62 ms
64 bytes from 192.168.193.6: icmp_seq=6 ttl=64 time=4.23 ms
64 bytes from 192.168.193.6: icmp_seq=7 ttl=64 time=5.26 ms
64 bytes from 192.168.193.6: icmp_seq=8 ttl=64 time=88.6 ms
64 bytes from 192.168.193.6: icmp_seq=9 ttl=64 time=2.78 ms
64 bytes from 192.168.193.6: icmp_seq=10 ttl=64 time=2.40 ms
64 bytes from 192.168.193.6: icmp_seq=11 ttl=64 time=3.54 ms
64 bytes from 192.168.193.6: icmp_seq=12 ttl=64 time=39.9 ms
64 bytes from 192.168.193.6: icmp_seq=13 ttl=64 time=4.98 ms
64 bytes from 192.168.193.6: icmp_seq=14 ttl=64 time=234 ms
64 bytes from 192.168.193.6: icmp_seq=15 ttl=64 time=43.3 ms
64 bytes from 192.168.193.6: icmp_seq=16 ttl=64 time=2.48 ms
64 bytes from 192.168.193.6: icmp_seq=17 ttl=64 time=6.96 ms
64 bytes from 192.168.193.6: icmp_seq=18 ttl=64 time=5.24 ms
64 bytes from 192.168.193.6: icmp_seq=19 ttl=64 time=4.47 ms
64 bytes from 192.168.193.6: icmp_seq=20 ttl=64 time=3.04 ms
^C
--- 192.168.193.6 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19029ms
rtt min/avg/max/mdev = 2.396/23.511/233.912/52.562 ms

- took 20s
+ 
```

Wireshark packet capture showing ICMP ping traffic. The packet list displays 58 packets, including ARP requests and replies, and 20 ICMP echo requests and replies. The packet details pane shows the structure of the first ICMP echo request packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.193.176	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply in 2)
2	0.004041086	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=64 (request in 1)
9	1.001371474	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 10)
10	1.005951256	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=64 (request in 9)
32	2.003262742	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=6/1536, ttl=64 (reply in 33)
33	2.007458262	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=6/1536, ttl=64 (request in 32)
36	3.004683230	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=7/1792, ttl=64 (reply in 37)
37	3.009910921	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=7/1792, ttl=64 (request in 36)
38	4.006235710	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=8/2048, ttl=64 (reply in 39)
39	4.094783291	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=8/2048, ttl=64 (request in 38)
42	5.008036437	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=9/2304, ttl=64 (reply in 43)
43	5.010781516	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=9/2304, ttl=64 (request in 42)
47	6.010080367	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=10/2560, ttl=64 (reply in 48)
48	6.012367727	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=10/2560, ttl=64 (request in 47)
49	7.011650787	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=11/2816, ttl=64 (reply in 50)
50	7.015169063	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=11/2816, ttl=64 (request in 49)
51	8.012705300	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=12/3072, ttl=64 (reply in 52)
52	8.052521717	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=12/3072, ttl=64 (request in 51)
57	9.013700355	192.168.193.6	192.168.193.6	ICMP	98	Echo (ping) request id=0x0003, seq=13/3328, ttl=64 (reply in 58)
58	9.018646429	192.168.193.6	192.168.193.176	ICMP	98	Echo (ping) reply id=0x0003, seq=13/3328, ttl=64 (request in 57)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp6s0, id 0
Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
Internet Protocol Version 4, Src: 192.168.193.176, Dst: 192.168.193.6
Internet Control Message Protocol

0000 56 91 e2 8b 84 c1 a0 d3 7a 1e 22 83 08 00 45 00 V.....z....E-
0010 00 54 10 fc 40 00 40 01 25 a5 c0 a8 c1 b0 c0 a8 .T..@..%.....
0020 c1 06 08 00 e0 f0 00 03 00 04 91 06 80 61 00 00a.....
0030 00 00 40 cd 06 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 b'()*+,-./012345
0060 36 37 67

Q2. Generate some web traffic and

a. find the list of the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.

The screenshot shows the Wireshark interface with the packet list pane displaying a series of DNS and QUIC packets. The packet list pane is filtered to show packets on interface 'phy0.mon'. The packet details pane shows the selected packet (No. 1) as a DNS Standard query. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.193.176	192.168.193.6	DNS	74	Standard query 0xe5e3 A www.google.com
2	0.226868203	192.168.193.6	192.168.193.176	DNS	90	Standard query response 0xe5e3 A www.google.com A 142.250.194.132
3	0.22881572	192.168.193.176	142.250.194.132	QUIC	1392	Initial, DCID=42506ceaba6ed64d, PKN: 1, PADDING, PING, PADDING, PING, CRYPT
4	0.228834666	192.168.193.176	142.250.194.132	QUIC	119	0-RTT, DCID=42506ceaba6ed64d
5	0.229236889	192.168.193.176	142.250.194.132	QUIC	963	0-RTT, DCID=42506ceaba6ed64d
6	0.343714749	142.250.194.132	192.168.193.176	QUIC	1392	Initial, SCID=42506ceaba6ed64d, PKN: 1, ACK, PADDING
7	0.390939083	142.250.194.132	192.168.193.176	QUIC	1392	Protected Payload (KP0)
8	0.390939519	142.250.194.132	192.168.193.176	QUIC	664	Protected Payload (KP0)
9	0.391207915	142.250.194.132	192.168.193.176	QUIC	68	Protected Payload (KP0)
10	0.391932935	192.168.193.176	142.250.194.132	QUIC	121	Handshake, DCID=42506ceaba6ed64d
11	0.392126060	192.168.193.176	142.250.194.132	QUIC	75	Protected Payload (KP0), DCID=42506ceaba6ed64d
12	0.459025368	142.250.194.132	192.168.193.176	QUIC	146	Protected Payload (KP0)
13	0.459657987	142.250.194.132	192.168.193.176	QUIC	67	Protected Payload (KP0)
14	0.459876244	192.168.193.176	142.250.194.132	QUIC	75	Protected Payload (KP0), DCID=42506ceaba6ed64d
15	0.500937523	142.250.194.132	192.168.193.176	QUIC	959	Protected Payload (KP0)
16	0.500937964	142.250.194.132	192.168.193.176	QUIC	67	Protected Payload (KP0)
17	0.500938075	142.250.194.132	192.168.193.176	QUIC	311	Protected Payload (KP0)
18	0.501404983	192.168.193.176	142.250.194.132	QUIC	77	Protected Payload (KP0), DCID=42506ceaba6ed64d
19	0.501577826	192.168.193.176	142.250.194.132	QUIC	75	Protected Payload (KP0), DCID=42506ceaba6ed64d
20	0.569284687	142.250.194.132	192.168.193.176	QUIC	67	Protected Payload (KP0)

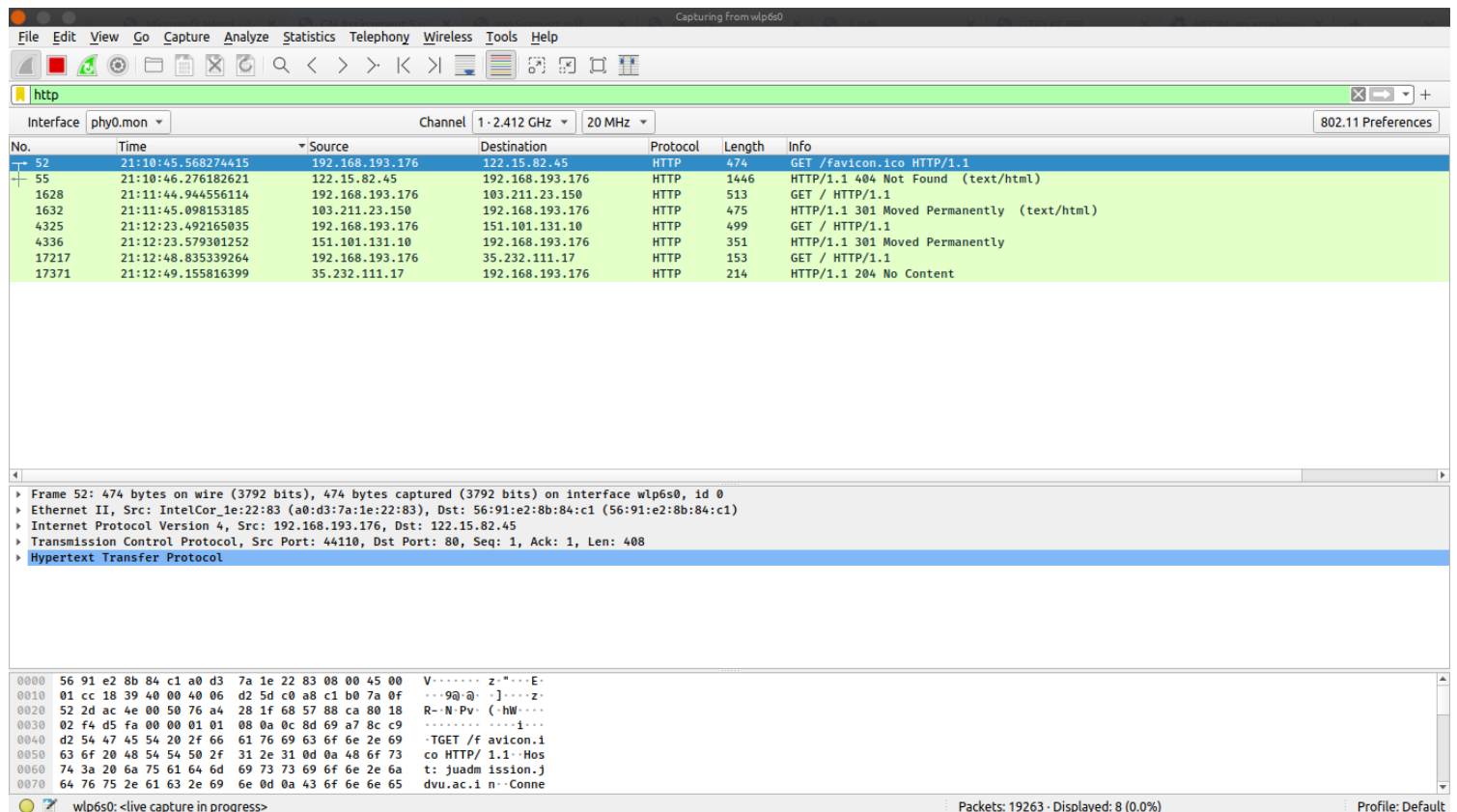
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp6s0, id 0
Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
Internet Protocol Version 4, Src: 192.168.193.176, Dst: 192.168.193.6
User Datagram Protocol, Src Port: 53123, Dst Port: 53
Domain Name System (query)

The screenshot shows the Wireshark interface with the packet list pane displaying a series of TCP and TLS packets. The packet list pane is filtered to show packets on interface 'phy0.mon'. The packet details pane shows the selected packet (No. 5849) as a TCP Retransmission. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
5843	24.5135805...	152.199.43.83	192.168.193.176	TCP	2782	443 → 38984 [PSH, ACK] Seq=178252 Ack=2165 Win=71168 Len=2716 TSval=2751322691 TSecr=2751322709
5844	24.5135994...	152.199.43.83	192.168.193.176	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=180968 Win=331008 Len=0 TSval=32765714 TSecr=2751322709
5845	24.5222911...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [ACK] Seq=180968 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5846	24.5299324...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [PSH, ACK] Seq=182326 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5847	24.5299509...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=183684 Win=336640 Len=0 TSval=32765731 TSecr=2751322709
5848	24.5299327...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [ACK] Seq=183684 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5849	24.5475922...	192.168.193.176	104.244.42.66	TCP	1073	[TCP Retransmission] 50538 → 443 [PSH, ACK] Seq=2342 Ack=4575 Win=64128 Len=1007
5850	24.5627118...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [PSH, ACK] Seq=185042 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5851	24.5627311...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=186400 Win=342272 Len=0 TSval=32765763 TSecr=2751322709
5852	24.5627121...	152.199.43.83	192.168.193.176	TCP	2782	443 → 38984 [PSH, ACK] Seq=186400 Ack=2165 Win=71168 Len=2716 TSval=2751322709 TSecr=2751322709
5853	24.5627669...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=189116 Win=347648 Len=0 TSval=32765763 TSecr=2751322709
5854	24.5627121...	152.199.43.83	192.168.193.176	TLSv1.3	2782	Application Data, Application Data, Application Data
5855	24.5627847...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=191832 Win=353152 Len=0 TSval=32765763 TSecr=2751322709
5856	24.5646739...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [ACK] Seq=191832 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5857	24.5769219...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [PSH, ACK] Seq=193190 Ack=2165 Win=71168 Len=1358 TSval=2751322709 TSecr=2751322709
5858	24.5769434...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=194548 Win=358784 Len=0 TSval=32765778 TSecr=2751322709
5859	24.5769222...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [ACK] Seq=194548 Ack=2324 Win=72192 Len=1358 TSval=2751322724 TSecr=2751322724
5860	24.5907869...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [PSH, ACK] Seq=195906 Ack=2324 Win=72192 Len=1358 TSval=2751322724 TSecr=2751322724
5861	24.5908283...	192.168.193.176	152.199.43.83	TCP	66	38984 → 443 [ACK] Seq=2603 Ack=197264 Win=364288 Len=0 TSval=32765791 TSecr=2751322724
5862	24.5913688...	152.199.43.83	192.168.193.176	TCP	1424	443 → 38984 [ACK] Seq=197264 Ack=2324 Win=72192 Len=1358 TSval=2751322724 TSecr=2751322724

Frame 5854: 2782 bytes on wire (22256 bits), 2782 bytes captured (22256 bits) on interface wlp6s0, id 0
Ethernet II, Src: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1), Dst: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)
Internet Protocol Version 4, Src: 152.199.43.83, Dst: 192.168.193.176
Transmission Control Protocol, Src Port: 443, Dst Port: 38984, Seq: 189116, Ack: 2165, Len: 2716
[11 Reassembled TCP Segments (16398 bytes): #5837(869), #5838(1358), #5840(1358), #5841(1358), #5843(2716), #5845(1358), #5846(1358), #5848(1358), #5850(1358), #5852(2716), #5854(591)]
Transport Layer Security
Transport Layer Security

b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.



As shown in the screenshot above the GET(52) was sent at 21.10.45.56824415 seconds and the reply OK(55) was received at 21.10.46.26182621 seconds. Thus the delay is (46.26182621 - 45.56824415) seconds which is 693.58206 milliseconds.

c. What is the Internet address of the website? What is the Internet address of your computer?

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
52	21:10:45.568274415	192.168.193.176	122.15.82.45	HTTP	474	GET /favicon.ico HTTP/1.1
55	21:10:46.276182621	122.15.82.45	192.168.193.176	HTTP	1446	HTTP/1.1 404 Not Found (text/html)
1628	21:11:44.944556114	192.168.193.176	103.211.23.150	HTTP	513	GET / HTTP/1.1
1632	21:11:45.098153185	103.211.23.150	192.168.193.176	HTTP	475	HTTP/1.1 301 Moved Permanently (text/html)
4325	21:12:23.492165035	192.168.193.176	151.101.131.10	HTTP	499	GET / HTTP/1.1
4336	21:12:23.579301252	151.101.131.10	192.168.193.176	HTTP	351	HTTP/1.1 301 Moved Permanently
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1
17371	21:12:49.155816399	35.232.111.17	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content

The packet details pane for packet 52 shows the following structure:

- Frame 52: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface wlp6s0, id 0
- Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
- Internet Protocol Version 4, Src: 192.168.193.176, Dst: 122.15.82.45
- Transmission Control Protocol, Src Port: 44110, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 56 91 e2 8b 84 c1 a0 d3 7a 1e 22 83 08 00 45 00 V----- z-....E-
0010 01 cc 18 39 40 00 40 06 d2 5d c0 a8 c1 b0 7a 0f ...9@|@-]....z-
0020 52 2d ac 4e 00 50 76 a4 28 1f 68 57 88 ca 80 18 R--N-Pv- (hw----
0030 02 f4 d5 fa 00 00 01 01 08 0a 0c 8d 69 a7 8c c9 .....-i---
0040 d2 54 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69 -TGET /f avicon.1
0050 63 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 co HTTP/ 1.1..Mos
0060 74 3a 20 6a 75 61 64 6d 69 73 73 69 6f 6e 2e 6a t: juadm ission.j
0070 64 76 75 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65 dvu.ac.1 n--Conne
```

As shown in the screenshot above, the IP address of the website is **122.15.82.45** and the IP address of my laptop is **192.168.193.176**

d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.

Wireshark interface showing a packet capture on the http filter. The packet list shows several HTTP packets, with packet 52 selected. The packet details panel shows the expanded HTTP layer for packet 52, displaying the request line, host, user-agent, and other headers. The packet bytes panel shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
52	21:10:45.568274415	192.168.193.176	122.15.82.45	HTTP	474	GET /favicon.ico HTTP/1.1
55	21:10:46.276182621	122.15.82.45	192.168.193.176	HTTP	1446	HTTP/1.1 404 Not Found (text/html)
1628	21:11:44.944556114	192.168.193.176	103.211.23.150	HTTP	513	GET / HTTP/1.1
1632	21:11:45.098153185	103.211.23.150	192.168.193.176	HTTP	475	HTTP/1.1 301 Moved Permanently (text/html)
4325	21:12:23.492165035	192.168.193.176	151.101.131.10	HTTP	499	GET / HTTP/1.1
4336	21:12:23.579301252	151.101.131.10	192.168.193.176	HTTP	351	HTTP/1.1 301 Moved Permanently
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1
17371	21:12:49.155816399	35.232.111.17	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content
19279	21:17:48.968539876	192.168.193.176	35.224.170.84	HTTP	153	GET / HTTP/1.1
19282	21:17:50.607067084	35.224.170.84	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content

Frame 52: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface wlp6s0, id 0
Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
Internet Protocol Version 4, Src: 192.168.193.176, Dst: 122.15.82.45
Transmission Control Protocol, Src Port: 44110, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1
Host: juadmission.jdvu.ac.in
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
DNT: 1
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://juadmission.jdvu.ac.in/jums_exam/
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,bn;q=0.8
Full request URI: http://juadmission.jdvu.ac.in/favicon.ico
HTTP request 1/1
Response in frame: 55

0000 56 91 e2 8b 84 c1 a0 d3 7a 1e 22 83 08 00 45 00 V.....z...E
0010 01 cc 18 39 40 00 40 06 d2 5d c0 a8 c1 b0 7a 0f ...9@a...z
0020 52 2d ac 4e 00 50 76 a4 28 1f 68 57 88 ca 80 18 R~N~Pv~(hW...
0030 02 f4 d5 fa 00 00 01 01 08 0a 0c 8d 69 a7 8c c9i...
0040 d2 54 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69 TGET /f avicon.i
0050 63 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 co HTTP/ 1.1~Hos
0060 74 3a 20 6a 75 61 64 6d 69 73 73 69 6f 6e 2e 6a t: juadm ission.J
0070 64 76 75 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65 dvu.ac.i n~Conne

wlp6s0: <live capture in progress> Packets: 19579 · Displayed: 10 (0.1%) Profile: Default

e. Find out the value of the Host from the Packet Details Panel, within the GET command.

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list shows a GET request for /favicon.ico from 192.168.193.176 to 122.15.82.45. The packet details panel shows the following information:

- Frame 52: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface wlp6s0, id 0
- Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
- Internet Protocol Version 4, Src: 192.168.193.176, Dst: 122.15.82.45
- Transmission Control Protocol, Src Port: 44110, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
- Hypertext Transfer Protocol
 - GET /favicon.ico HTTP/1.1\r\n
 - Host: juadmission.jdvu.ac.in\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\n
 - DNT: 1\r\n
 - Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
 - Referer: http://juadmission.jdvu.ac.in/jums_exam\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en,en-US;q=0.9,bn;q=0.8\r\n
 - \r\n
 - [Full request URI: <http://juadmission.jdvu.ac.in/favicon.ico>]
 - [HTTP request 1/1]
 - [Response in frame: 55]

The packet bytes panel shows the raw data of the packet, including the Host header: `Host: juadmission.jdvu.ac.in\r\n`.

As shown in the screenshot above, the Host is : `https://juadmission.jdvu.ac.in\r\n`

Q3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.

The screenshot shows Wireshark capturing traffic on interface phy0.mon. The packet list displays several HTTP packets. Packet 52 is selected, showing a GET request for /favicon.ico from 192.168.193.176 to 192.15.82.45. The packet details pane shows the request structure, including the Host, Connection, User-Agent, DNT, Accept, and Referer headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
52	21:10:45.568274415	192.168.193.176	192.15.82.45	HTTP	474	GET /favicon.ico HTTP/1.1
55	21:10:46.276182621	122.15.82.45	192.168.193.176	HTTP	1446	HTTP/1.1 404 Not Found (text/html)
1628	21:11:44.944556114	192.168.193.176	103.211.23.150	HTTP	513	GET / HTTP/1.1
1632	21:11:45.098153185	103.211.23.150	192.168.193.176	HTTP	475	HTTP/1.1 301 Moved Permanently (text/html)
4325	21:12:23.492165035	192.168.193.176	151.101.131.10	HTTP	499	GET / HTTP/1.1
4336	21:12:23.579301252	151.101.131.10	192.168.193.176	HTTP	351	HTTP/1.1 301 Moved Permanently
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1
17371	21:12:49.155816399	35.232.111.17	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content
19279	21:17:48.968539876	192.168.193.176	35.224.170.84	HTTP	153	GET / HTTP/1.1
19282	21:17:50.607067084	35.224.170.84	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content

Packet 52 details:

- GET /favicon.ico HTTP/1.1\r\n
- Host: juadmission.jdvu.ac.in\r\n
- Connection: keep-alive\r\n
- User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\n
- DNT: 1\r\n
- Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
- Referer: http://juadmission.jdvu.ac.in/jums_exam/\r\n

Packet 52 bytes:

```
0050  63 6f 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73  co HTTP/1.1..Hos
0060  74 3a 20 6a 75 61 64 6d 69 73 73 69 6f 6e 2e 6a  t: juadmission.j
0070  64 76 75 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65  dvu.ac.in..Conne
0080  63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76  ction: keep-aliv
```

The HEX and ASCII representations of the packet are :

HEX

```
0000  56 91 e2 8b 84 c1 a0 d3 7a 1e 22 83 08 00
0010  01 cc 18 39 40 00 40 06 d2 5d c0 a8 c1 b0 7a 0f
0020  52 2d ac 4e 00 50 76 a4 28 1f 68 57 88 ca 80 18
0030  02 f4 d5 fa 00 00 01 01 08 0a 0c 8d 69 a7 8c c9
0040  d2 54 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69
0050  63 6f 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73
0060  74 3a 20 6a 75 61 64 6d 69 73 73 69 6f 6e 2e 6a
0070  64 76 75 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65
0080  63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76
```

ASCII

```
45 00  V.....z."...E.
...9@.@...]....z.
R-.N.Pv.(.hW....
.....i...
.TGET /favicon.i
co HTTP/1.1..Hos
t: juadmission.j
dvu.ac.in..Conne
ction: keep-aliv
```

0090	65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	e..User-Agent: M
00a0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b	ozilla/5.0 (X11;
00b0	20 4c 69 6e 75 78 20 78 38 36 5f 36 34 29 20 41	Linux x86_64) A
00c0	70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33	ppleWebKit/537.3
00d0	36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47	6 (KHTML, like G
00e0	65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 39 35 2e	ecko) Chrome/95.
00f0	30 2e 34 36 33 38 2e 36 39 20 53 61 66 61 72 69	0.4638.69 Safari
0100	2f 35 33 37 2e 33 36 0d 0a 44 4e 54 3a 20 31 0d	/537.36..DNT: 1.
0110	0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 61	.Accept: image/a
0120	76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69	vif,image/webp,i
0130	6d 61 67 65 2f 61 70 6e 67 2c 69 6d 61 67 65 2f	mage/apng,image/
0140	73 76 67 2b 78 6d 6c 2c 69 6d 61 67 65 2f 2a 2c	svg+xml,image/*,
0150	2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72	*/*;q=0.8..Refer
0160	65 72 3a 20 68 74 74 70 3a 2f 2f 6a 75 61 64 6d	er: http://juadm
0170	69 73 73 69 6f 6e 2e 6a 64 76 75 2e 61 63 2e 69	ission.jdvu.ac.i
0180	6e 2f 6a 75 6d 73 5f 65 78 61 6d 2f 0d 0a 41 63	n/jums_exam/..Ac
0190	63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67	cept-Encoding: g
01a0	7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63	zip, deflate..Ac
01b0	63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65	cept-Language: e
01c0	6e 2c 65 6e 2d 55 53 3b 71 3d 30 2e 39 2c 62 6e	n,en-US;q=0.9,bn
01d0	3b 71 3d 30 2e 38 0d 0a 0d 0a	;q=0.8....

Q4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list shows a GET request to /favicon.ico. The packet details show the Host header as juadmission.jdvu.ac.in. The packet bytes panel shows the raw hex and ASCII data of the packet, with the Host header value highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
52	21:10:45.568274415	192.168.193.176	122.15.82.45	HTTP	474	GET /favicon.ico HTTP/1.1
55	21:10:46.276182621	122.15.82.45	192.168.193.176	HTTP	1446	HTTP/1.1 404 Not Found (text/html)
1628	21:11:44.944556114	192.168.193.176	103.211.23.150	HTTP	513	GET / HTTP/1.1
1632	21:11:45.098153185	103.211.23.150	192.168.193.176	HTTP	475	HTTP/1.1 301 Moved Permanently (text/html)
4325	21:12:23.492165035	192.168.193.176	151.101.131.10	HTTP	499	GET / HTTP/1.1
4336	21:12:23.579301252	151.101.131.10	192.168.193.176	HTTP	351	HTTP/1.1 301 Moved Permanently
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1
17371	21:12:49.155816399	35.232.111.17	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content
19279	21:17:48.968539876	192.168.193.176	35.224.170.84	HTTP	153	GET / HTTP/1.1
19282	21:17:50.607067084	35.224.170.84	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content

Packet 52 details:

- GET /favicon.ico HTTP/1.1\r\n
- Host: juadmission.jdvu.ac.in\r\n
- Connection: keep-alive\r\n
- User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\n
- DNT: 1\r\n
- Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
- Referer: http://juadmission.jdvu.ac.in/jums_exam/\r\n

Packet 52 bytes:

```
0050  63 6f 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73  co HTTP/ 1.1..Mos
0060  74 3a 20 6a 75 61 64 6d 69 73 73 69 6f 6e 2e 6a  t: juadm ission,j
0070  64 75 75 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65  dvu.ac.i n..Conne
0080  63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76  ction: k eep-aliv
0090  65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  e..User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b  ozilla/5 .0 (X11;
00b0  20 4c 69 6e 75 78 20 78 38 36 5f 36 3a 29 20 41  Linux x 86_64) A
00c0  70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33  ppleWebK it/537.3
00d0  36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47  6 (KHTML , like G
00e0  65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 39 35 2e  ecko) Ch rome/95.
00f0  30 2e 34 36 33 38 2e 36 39 20 53 61 66 61 72 69  0.4638.6 9 Safari
0100  2f 35 33 37 2e 33 36 0d 0a 44 4e 54 3a 20 31 0d  /537.36. DNT: 1
0110  0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 61  .Accept: image/a
0120  76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69  vif,imag e/webp,i
0130  6d 61 67 65 2f 61 70 6e 67 2c 69 6d 61 67 65 2f  mage/apn g,image/
0140  73 76 67 2b 78 6d 6c 2c 69 6d 61 67 65 2f 2a 2c  svg+xml, image/*,
0150  2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72  /*;q=0. 8..Refer
0160  65 72 3a 20 68 74 74 70 3a 2f 2f 6a 75 61 64 6d  er: http ://juadm
0170  69 73 73 69 6f 6e 2e 6a 64 76 75 2e 61 63 2e 69  ission.j dvu.ac.i
```

The first four bytes of the Hex value of the Host parameter from the Packet Bytes Panel are : **48 6f 73 74**

Q5. Filter packets with http, TCP, DNS and other protocols. Find out what those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button. Click on follow.

HTTP:

Wireshark interface showing a capture of HTTP traffic. The packet list displays several HTTP GET requests. Packet 17217 is selected, showing the full request for `http://connectivity-check.ubuntu.com/`. The packet details pane shows the Hypertext Transfer Protocol section with the full request URI and the HTTP request line. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
52	21:10:45.568274415	192.168.193.176	122.15.82.45	HTTP	474	GET /favicon.ico HTTP/1.1
55	21:10:46.276182621	122.15.82.45	192.168.193.176	HTTP	1446	HTTP/1.1 404 Not Found (text/html)
1628	21:11:44.944556114	192.168.193.176	103.211.23.150	HTTP	513	GET / HTTP/1.1
1632	21:11:45.098153185	103.211.23.150	192.168.193.176	HTTP	475	HTTP/1.1 301 Moved Permanently (text/html)
4325	21:12:23.492165035	192.168.193.176	151.101.131.10	HTTP	499	GET / HTTP/1.1
4336	21:12:23.579301252	151.101.131.10	192.168.193.176	HTTP	351	HTTP/1.1 301 Moved Permanently
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1
17371	21:12:49.155816399	35.232.111.17	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content
19279	21:17:48.968539876	192.168.193.176	35.224.170.84	HTTP	153	GET / HTTP/1.1
19282	21:17:50.607067084	35.224.170.84	192.168.193.176	HTTP	214	HTTP/1.1 204 No Content

TCP:

Wireshark interface showing a capture of TCP traffic. The packet list displays several TCP segments. Packet 17217 is selected, showing the SYN segment for the connection to 35.232.111.17. The packet details pane shows the TCP segment structure, including the sequence number and the SYN flag. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
17205	21:12:48.810372543	104.123.210.150	192.168.193.176	TCP	2782	443 → 56844 [PSH, ACK] Seq=11473503 Ack=1637 Win=64128 Len=2716 TSval=3127136498 TSecr=131658680
17206	21:12:48.810372904	104.123.210.150	192.168.193.176	TCP	1424	443 → 56844 [ACK] Seq=11476219 Ack=1637 Win=64128 Len=1358 TSval=3127136503 TSecr=131658680
17207	21:12:48.810523974	192.168.193.176	104.123.210.150	TCP	66	56844 → 443 [ACK] Seq=1637 Ack=11477577 Win=1300480 Len=0 TSval=131658930 TSecr=3127136498
17208	21:12:48.811068551	104.123.210.150	192.168.193.176	TCP	1424	443 → 56844 [PSH, ACK] Seq=11477577 Ack=1637 Win=64128 Len=1358 TSval=3127136503 TSecr=131658680
17209	21:12:48.811069544	104.123.210.150	192.168.193.176	TLSv1.3	1424	Application Data [TCP segment of a reassembled PDU]
17210	21:12:48.811163246	192.168.193.176	104.123.210.150	TCP	66	56844 → 443 [ACK] Seq=1637 Ack=11480293 Win=1300480 Len=0 TSval=131658931 TSecr=3127136503
17211	21:12:48.811572335	104.123.210.150	192.168.193.176	TCP	1424	443 → 56844 [PSH, ACK] Seq=11480293 Ack=1637 Win=64128 Len=1358 TSval=3127136507 TSecr=131658680
17212	21:12:48.815652764	104.123.210.150	192.168.193.176	TCP	1424	443 → 56844 [ACK] Seq=11481651 Ack=1637 Win=64128 Len=1358 TSval=3127136512 TSecr=131658680
17213	21:12:48.815727245	192.168.193.176	104.123.210.150	TCP	66	56844 → 443 [ACK] Seq=1637 Ack=11483009 Win=1300480 Len=0 TSval=131658936 TSecr=3127136507
17214	21:12:48.822570745	104.123.210.150	192.168.193.176	TCP	1424	443 → 56844 [PSH, ACK] Seq=11483009 Ack=1637 Win=64128 Len=1358 TSval=3127136512 TSecr=131658680
17215	21:12:48.835239426	35.232.111.17	192.168.193.176	TCP	74	80 → 41450 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1370 SACK_PERM=1 TSval=3589125268 TSecr=0
17216	21:12:48.835269418	192.168.193.176	35.232.111.17	TCP	66	41450 → 80 [ACK] Seq=1 Ack=1 Win=0 TSval=3519426855 TSecr=3589125268
17217	21:12:48.835339264	192.168.193.176	35.232.111.17	HTTP	153	GET / HTTP/1.1

DNS:

Wireshark capture of DNS traffic on interface phy0.mon. The packet list shows a query for cdnjs.cloudflare.com. The packet details pane shows the structure of the DNS query packet.

No.	Time	Source	Destination	Protocol	Length	Info
4598	21:12:25.981102808	192.168.193.176	192.168.193.6	DNS	80	Standard query 0x86e0 A cdnjs.cloudflare.com
4599	21:12:26.142087428	192.168.193.6	192.168.193.176	DNS	112	Standard query response 0x86e0 A cdnjs.cloudflare.com A 104.16.19.94 A 104.16.18.94
4906	21:12:27.102368528	192.168.193.176	192.168.193.6	DNS	79	Standard query 0x384a A assets.adobedtm.com
4907	21:12:27.104149603	192.168.193.176	192.168.193.6	DNS	75	Standard query 0xfd76 A neom.scene7.com
4912	21:12:27.141732610	192.168.193.6	192.168.193.176	DNS	179	Standard query response 0x384a A assets.adobedtm.com CNAME cn-assets.adobedtm.com.edgekey.net
4917	21:12:27.184217032	192.168.193.6	192.168.193.176	DNS	176	Standard query response 0xfd76 A neom.scene7.com CNAME wildcard-ion.scene7.com.edgekey.net
5187	21:12:27.620735382	192.168.193.176	192.168.193.6	DNS	84	Standard query 0x3701 A geolocation.onetrust.com
5200	21:12:27.655389951	192.168.193.6	192.168.193.176	DNS	116	Standard query response 0x3701 A geolocation.onetrust.com A 104.20.185.68 A 104.20.184.68
7233	21:12:30.459121595	192.168.193.176	192.168.193.6	DNS	76	Standard query 0x70f5 A s3.amazonaws.com
7308	21:12:30.770252763	192.168.193.6	192.168.193.176	DNS	92	Standard query response 0x70f5 A s3.amazonaws.com A 52.217.73.134
11863	21:12:37.539189085	192.168.193.176	192.168.193.6	DNS	80	Standard query 0xdf3a A beacons.gcp.gvt2.com
11953	21:12:37.642065892	192.168.193.6	192.168.193.176	DNS	126	Standard query response 0xdf3a A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 104.20.185.68 A 104.20.184.68
13042	21:12:39.505905527	192.168.193.176	192.168.193.6	DNS	89	Standard query 0xdee6 A privacyportal-de.onetrust.com

Frame 4598: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface wlp6s0, id 0
Ethernet II, Src: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83), Dst: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
Internet Protocol Version 4, Src: 192.168.193.176, Dst: 192.168.193.6
User Datagram Protocol, Src Port: 54815, Dst Port: 53
Domain Name System (query)

Domain Name System: Protocol Packets: 22502 - Displayed: 158 (0.7%) Profile: Default

ARP:

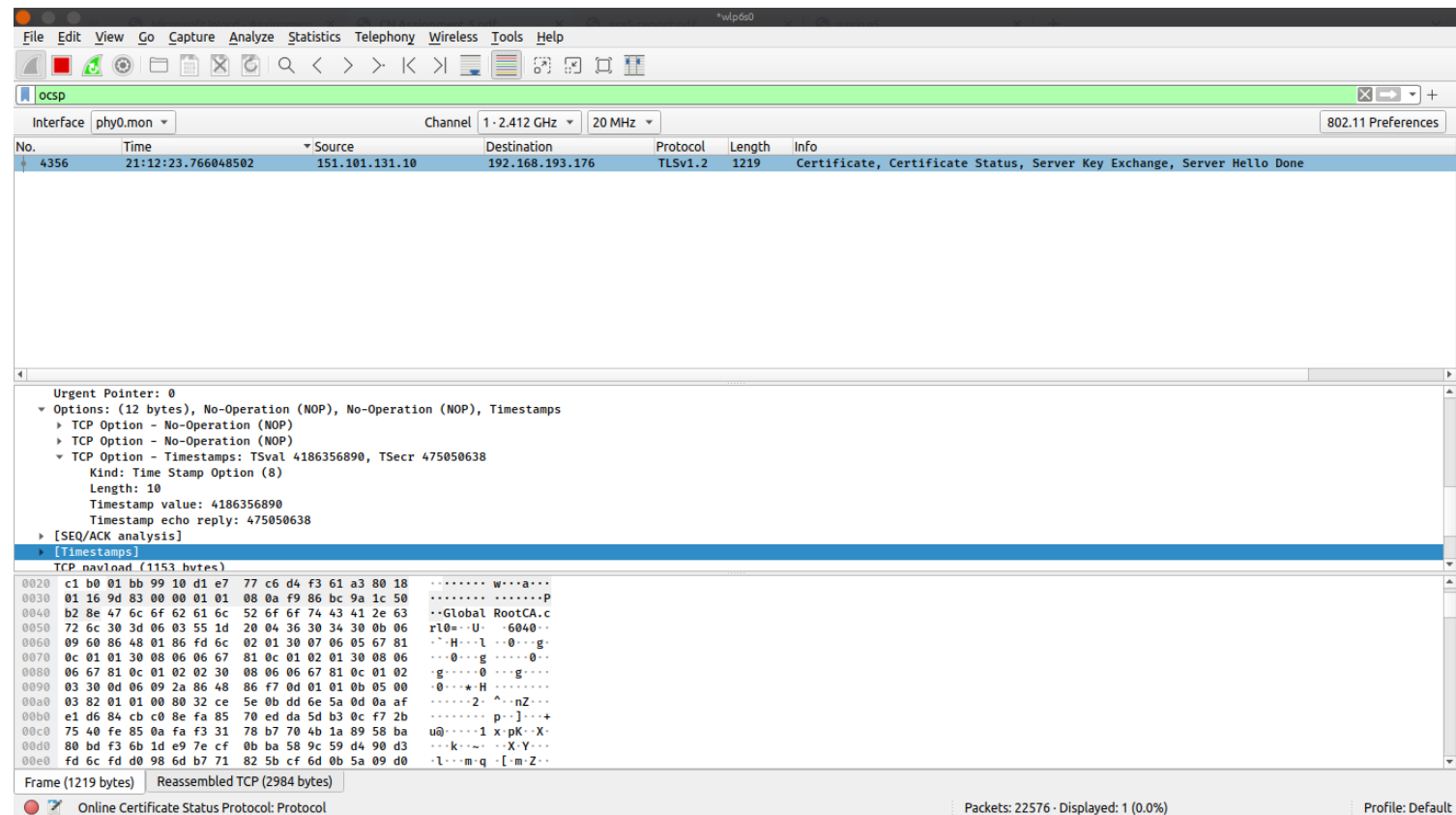
Wireshark capture of ARP traffic on interface phy0.mon. The packet list shows a request for 192.168.193.176. The packet details pane shows the structure of the ARP request packet.

No.	Time	Source	Destination	Protocol	Length	Info
90	21:10:54.360154872	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6
91	21:10:54.360219378	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	192.168.193.176 is at a0:d3:7a:1e:22:83
520	21:11:08.691953629	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6
521	21:11:08.691977516	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	192.168.193.176 is at a0:d3:7a:1e:22:83
1333	21:11:23.389727777	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6
1334	21:11:23.389740056	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	192.168.193.176 is at a0:d3:7a:1e:22:83
1349	21:11:31.898307344	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	Who has 192.168.193.6? Tell 192.168.193.176
1350	21:11:31.902082550	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	192.168.193.6 is at 56:91:e2:8b:84:c1
1503	21:11:38.389204994	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6
1504	21:11:38.389216557	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	192.168.193.176 is at a0:d3:7a:1e:22:83
4017	21:11:52.881437921	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6
4018	21:11:52.881460706	IntelCor_1e:22:83	56:91:e2:8b:84:c1	ARP	42	192.168.193.176 is at a0:d3:7a:1e:22:83
4151	21:12:12.542439583	56:91:e2:8b:84:c1	IntelCor_1e:22:83	ARP	42	Who has 192.168.193.176? Tell 192.168.193.6

Frame 90: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp6s0, id 0
Ethernet II, Src: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1), Dst: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)
Address Resolution Protocol (request)

Address Resolution Protocol: Protocol Packets: 22525 - Displayed: 146 (0.6%) Profile: Default

OCSF:

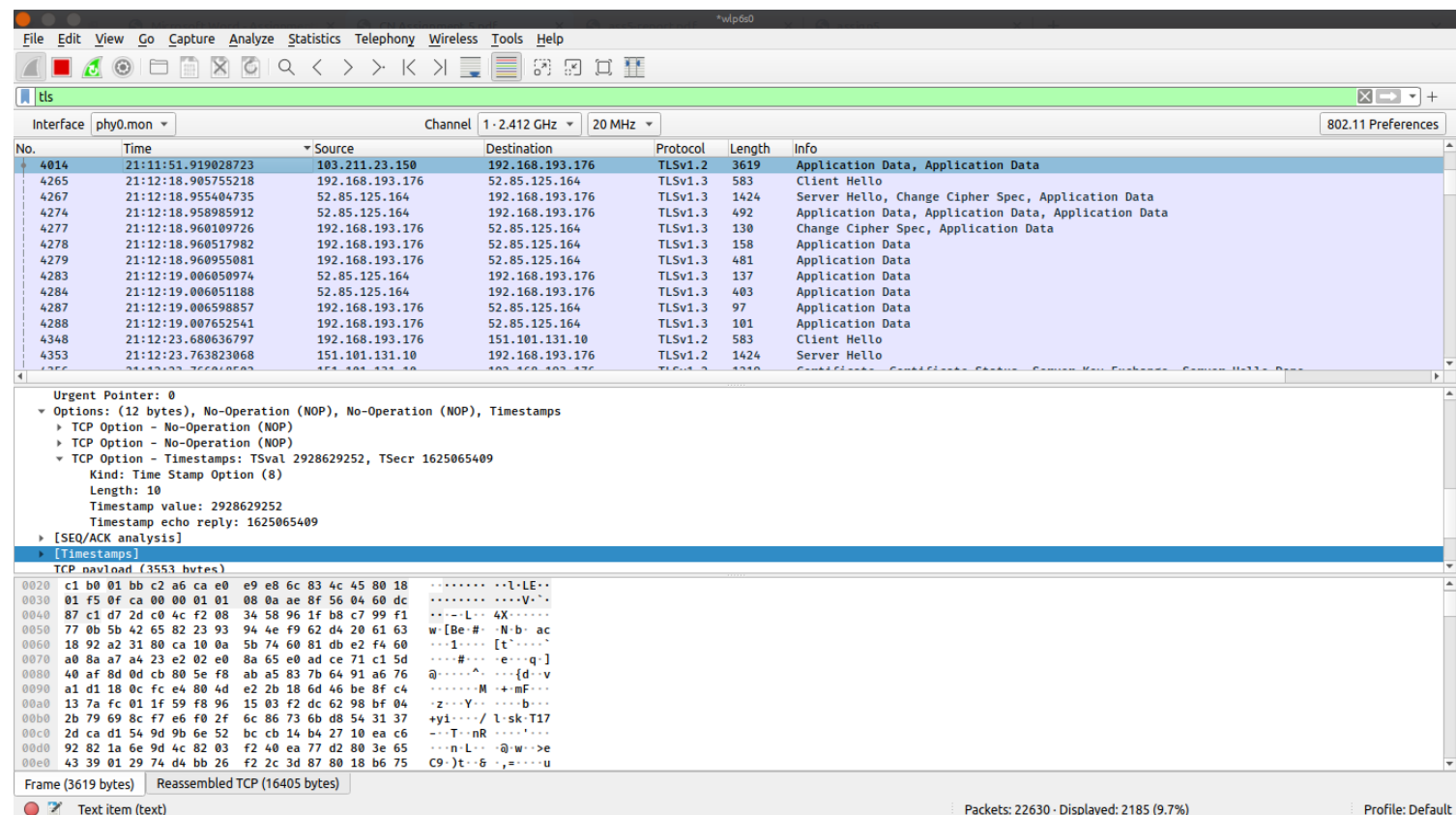


The image shows a Wireshark capture of an OCSF (Online Certificate Status Protocol) packet. The packet list shows a single packet of length 1219 bytes, protocol TLSv1.2, destination 192.168.193.176. The packet details pane shows the following structure:

- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - TCP Option - No-Operation (NOP)
 - TCP Option - No-Operation (NOP)
 - TCP Option - Timestamps: TSval 4186356890, TSecr 475050638
 - Kind: Time Stamp Option (8)
 - Length: 10
 - Timestamp value: 4186356890
 - Timestamp echo reply: 475050638
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (1153 bytes)

The packet bytes pane shows the raw data of the packet, including the TLS header and the OCSF payload. The status bar at the bottom indicates that the packet is part of a reassembled TCP stream (2984 bytes) and that the Online Certificate Status Protocol is the protocol being analyzed.

TLS:

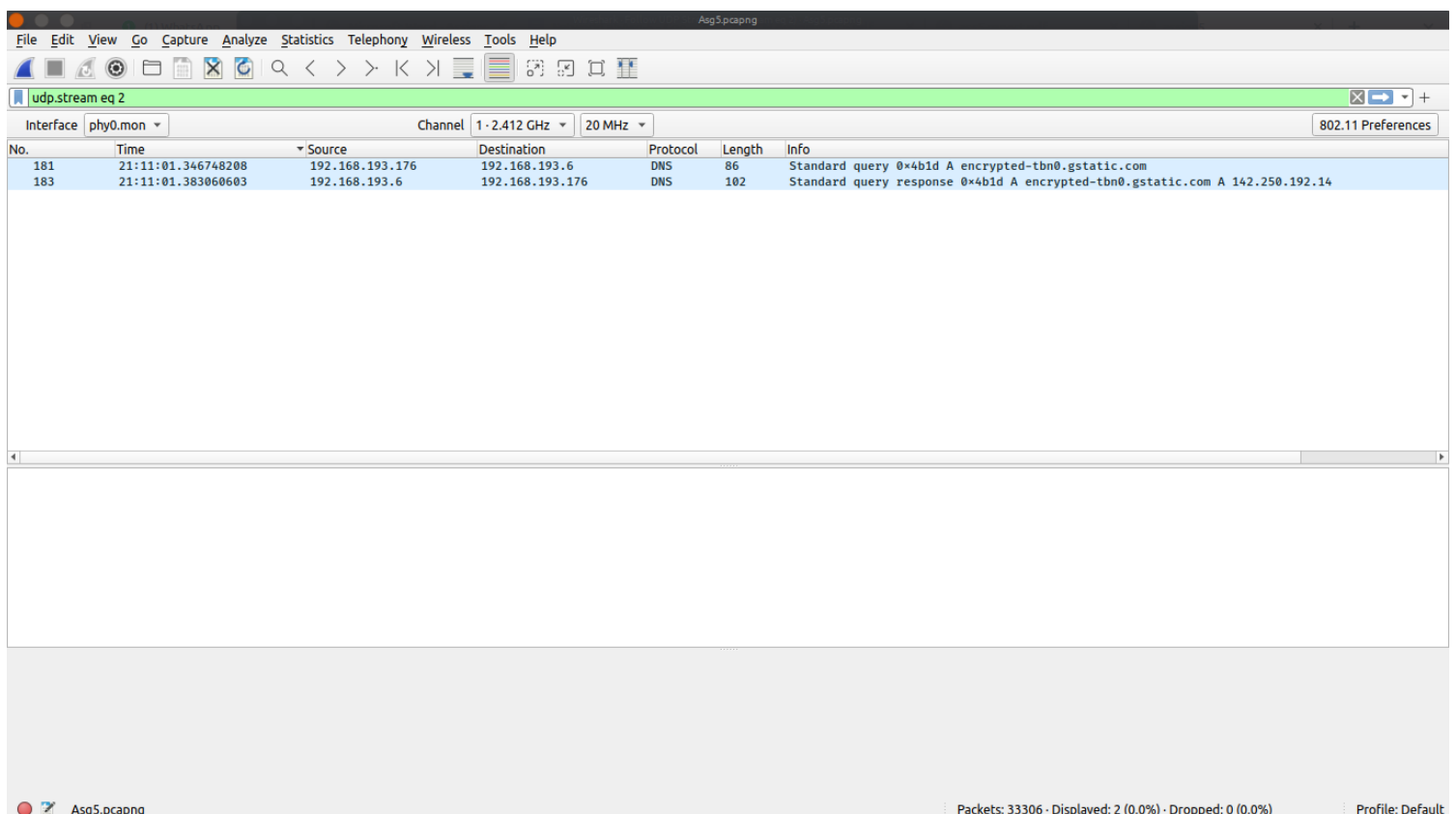
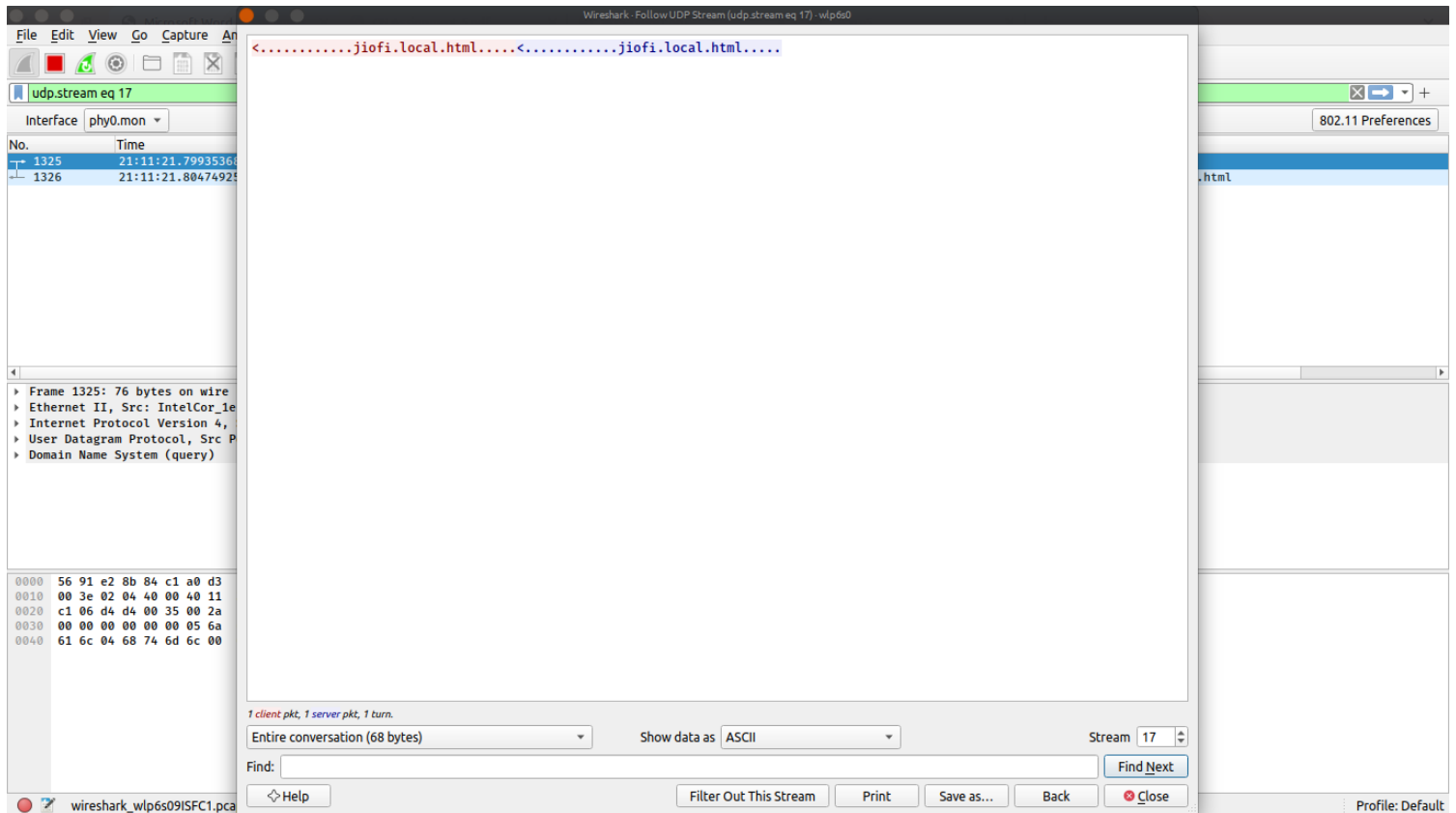


The image shows a Wireshark capture of a TLS session. The packet list shows a sequence of packets, including Client Hello, Server Hello, Change Cipher Spec, and Application Data. The packet details pane shows the following structure for the first packet (Client Hello):

- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - TCP Option - No-Operation (NOP)
 - TCP Option - No-Operation (NOP)
 - TCP Option - Timestamps: TSval 2928629252, TSecr 1625065409
 - Kind: Time Stamp Option (8)
 - Length: 10
 - Timestamp value: 2928629252
 - Timestamp echo reply: 1625065409
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (3553 bytes)

The packet bytes pane shows the raw data of the packet, including the TLS header and the Client Hello payload. The status bar at the bottom indicates that the packet is part of a reassembled TCP stream (16405 bytes) and that the Text item (text) is the protocol being analyzed.

a. Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow.



Q6. Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.

On expanding Ethernet layer of packet 1147 in the Packet Details Panel, the following result is obtained:

The screenshot shows the Wireshark interface with the packet list, packet details, and raw bytes panels. The packet list shows a TCP packet from 192.168.193.176 to 122.15.82.45. The packet details show the Ethernet II layer expanded, displaying the source and destination MAC addresses. The raw bytes panel shows the hexadecimal and ASCII representation of the packet data.

No.	Time	Source	Destination	Protocol	Length	Info
1147	21:11:16.630482716	122.15.82.45	192.168.193.176	TCP	66	80 → 44110 [FIN, ACK] Seq=1381 Ack=409 Win=260 Len=0 TSval=2362070520 TSecr=210594923

Frame 1147: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp6s0, id 0
Ethernet II, Src: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1), Dst: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)
Destination: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)
Address: IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)
... 0 ... = LG bit: Globally unique address (factory default)
... 0 ... = IG bit: Individual address (unicast)
Source: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
Address: 56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)
... 1 ... = LG bit: Locally administered address (this is NOT the factory default)
... 0 ... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 122.15.82.45, Dst: 192.168.193.176
Transmission Control Protocol, Src Port: 80, Dst Port: 44110, Seq: 1381, Ack: 409, Len: 0

0000 a0 d3 7a 1e 22 83 56 91 e2 8b 84 c1 08 00 45 28 --z"-V-E(
0010 00 34 7f c9 40 00 31 06 7b 3d 7a 0f 52 2d c0 a8 -4-@!- {=z R--
0020 c1 b0 00 50 ac 4e 68 57 8e 2e 76 a4 29 b7 80 11 -P-NHW .v-)...
0030 01 04 87 e7 00 00 01 01 08 0a 8c ca 55 f8 0c 8dU...
0040 6c 6b lk

Q7. What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?

The manufacturer of my Laptop's Network Interface Card (NIC) is :

IntelCor_1e:22:83 (a0:d3:7a:1e:22:83)

The manufacturer of the server's Network Interface Card (NIC) is :

56:91:e2:8b:84:c1 (56:91:e2:8b:84:c1)

Q8. What are the Hex values (shown the raw bytes panel) of the two NICs Manufacturers OUIs?

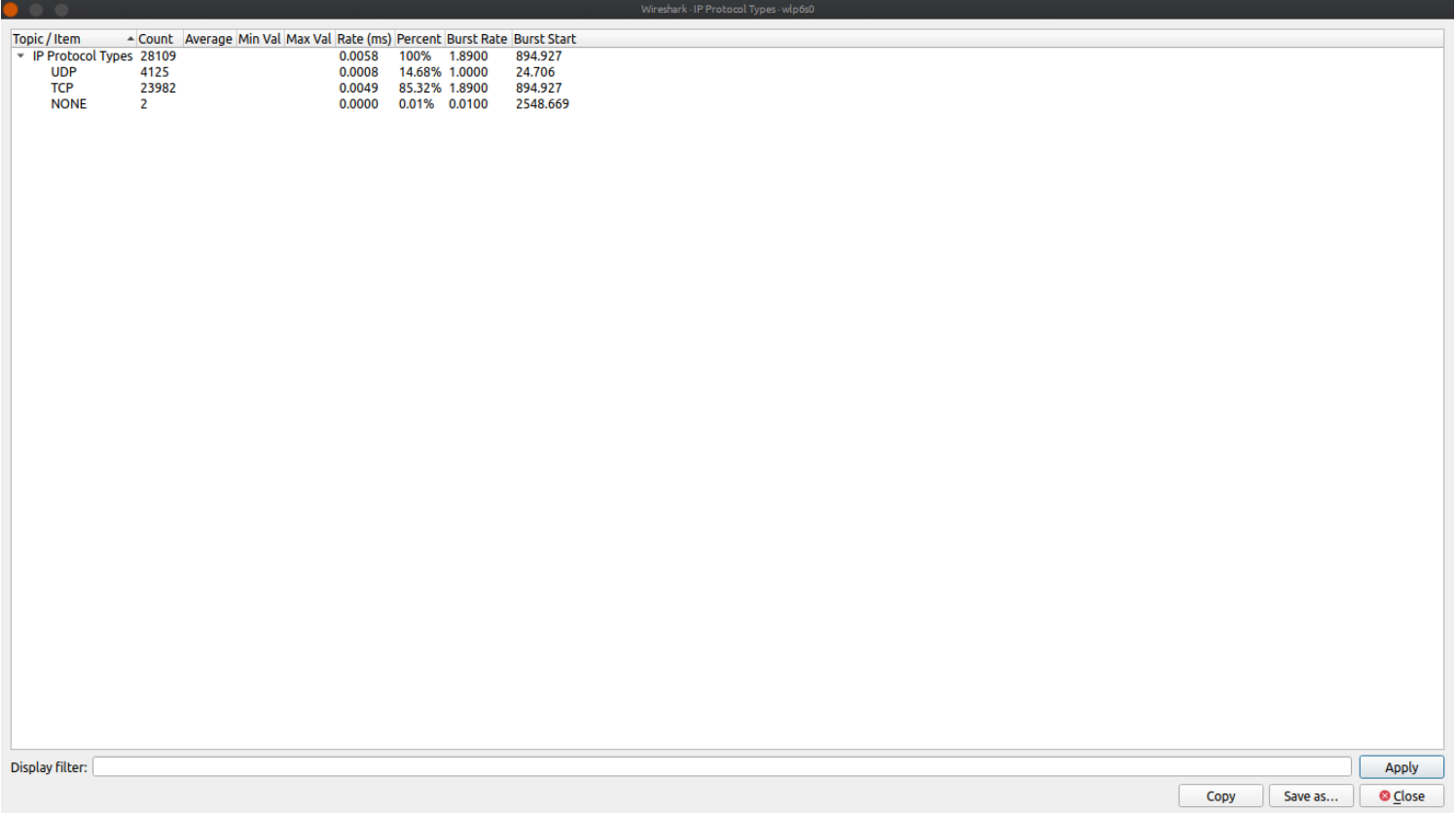
For my Laptop's manufacturer : **a0:d3:7a:1e:22:83**

For server's manufacturer : **56:91:e2:8b:84:c1**

Q9. Find the following statistics:

- a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?**
- b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?**

The IPv4 statistics of the packet capture:

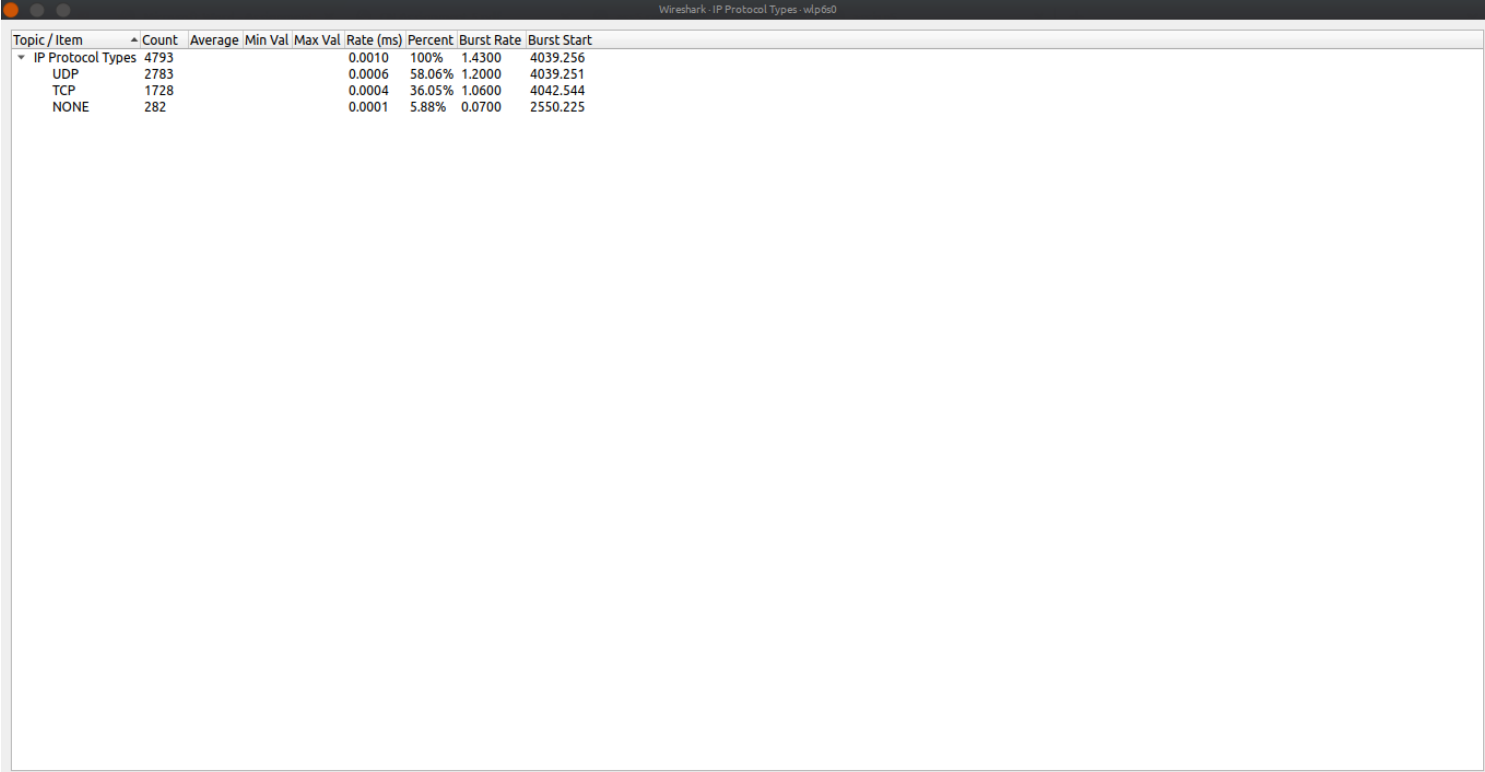


The image shows a Wireshark window titled "Wireshark - IP Protocol Types - wlp60". It displays a table of statistics for IP Protocol Types. The table has columns: Topic / Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst Start. The data is as follows:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IP Protocol Types	28109				0.0058	100%	1.8900	894.927
UDP	4125				0.0008	14.68%	1.0000	24.706
TCP	23982				0.0049	85.32%	1.8900	894.927
NONE	2				0.0000	0.01%	0.0100	2548.669

At the bottom of the window, there is a "Display filter:" field and three buttons: "Copy", "Save as...", and "Close".

The IPv6 statistics of the packet capture:



The image shows a Wireshark window titled "Wireshark - IP Protocol Types - wlp6s0". It displays a table of statistics for IP Protocol Types. The table has columns for Topic/Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst Start. The data is as follows:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IP Protocol Types	4793				0.0010	100%	1.4300	4039.256
UDP	2783				0.0006	58.06%	1.2000	4039.251
TCP	1728				0.0004	36.05%	1.0600	4042.544
NONE	282				0.0001	5.88%	0.0700	2550.225

At the bottom of the window, there is a "Display filter:" field, an "Apply" button, and "Copy", "Save as...", and "Close" buttons.

Higher level protocols which use **TCP**:

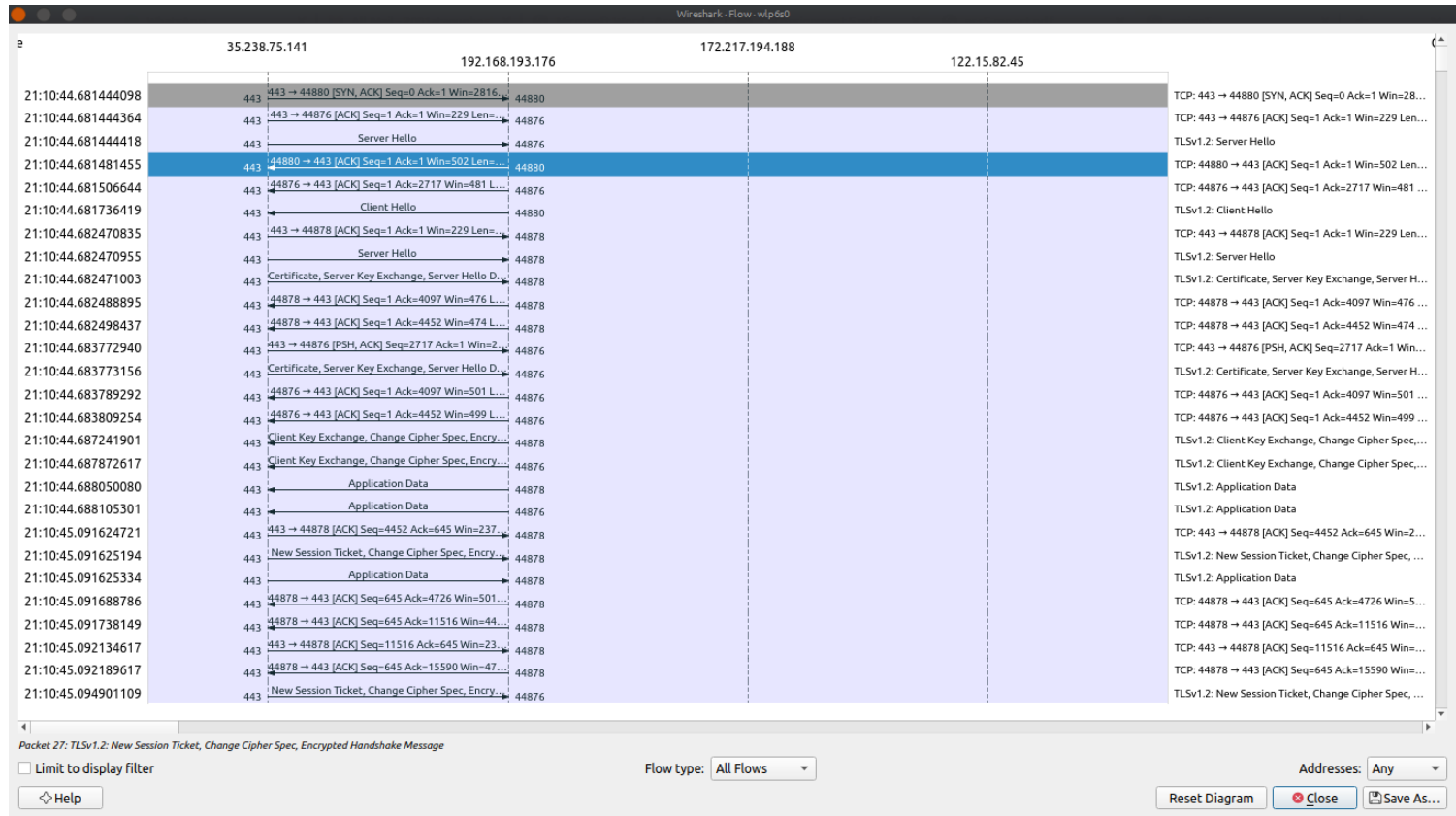
1. **HTTPS** - HyperText Transfer Protocol Secure
2. **FTP** - File Transfer Protocol

Higher level protocols which use **UDP**:

1. **SNMP** - Simple Network Management Protocol
2. **RIP** - Routing Information Protocol

Q10. Find the traffic flow. Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.

For general flow :



For TCP flow:

