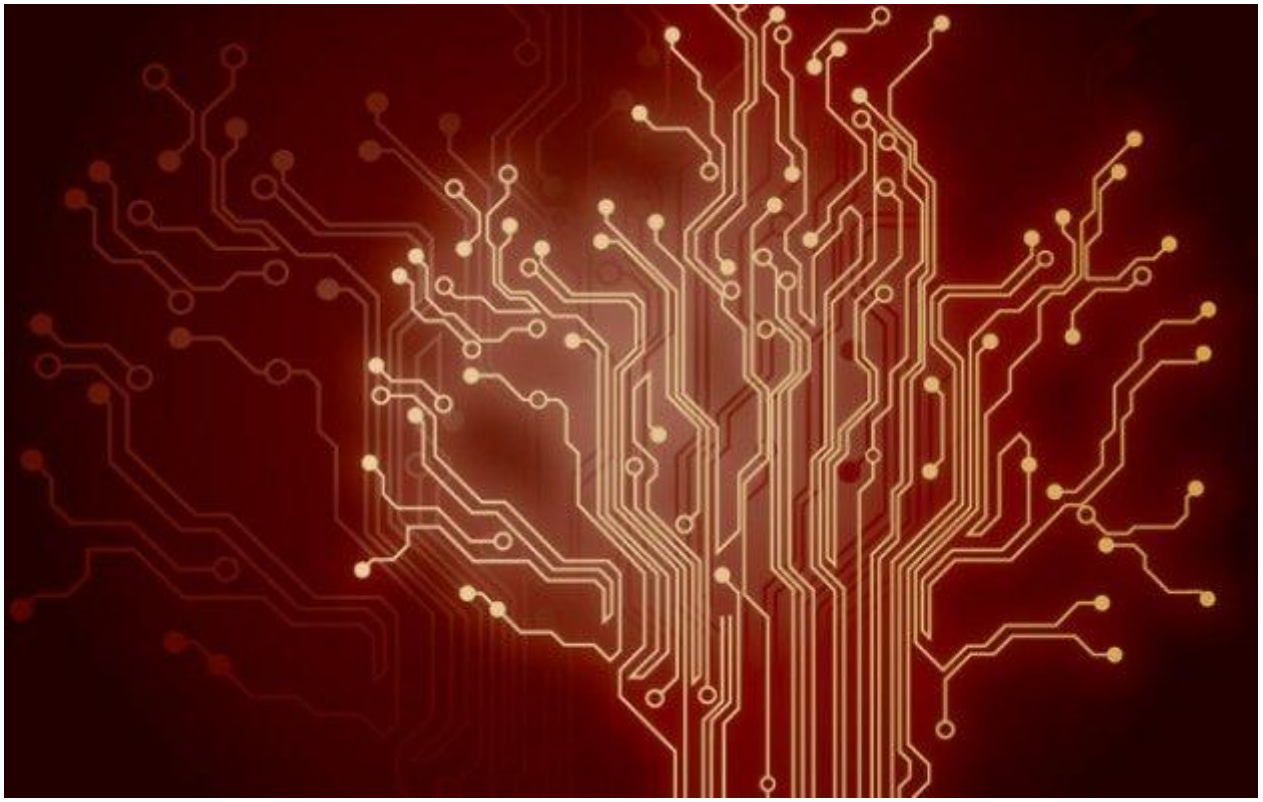
NETWORK LAB REPORT

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:

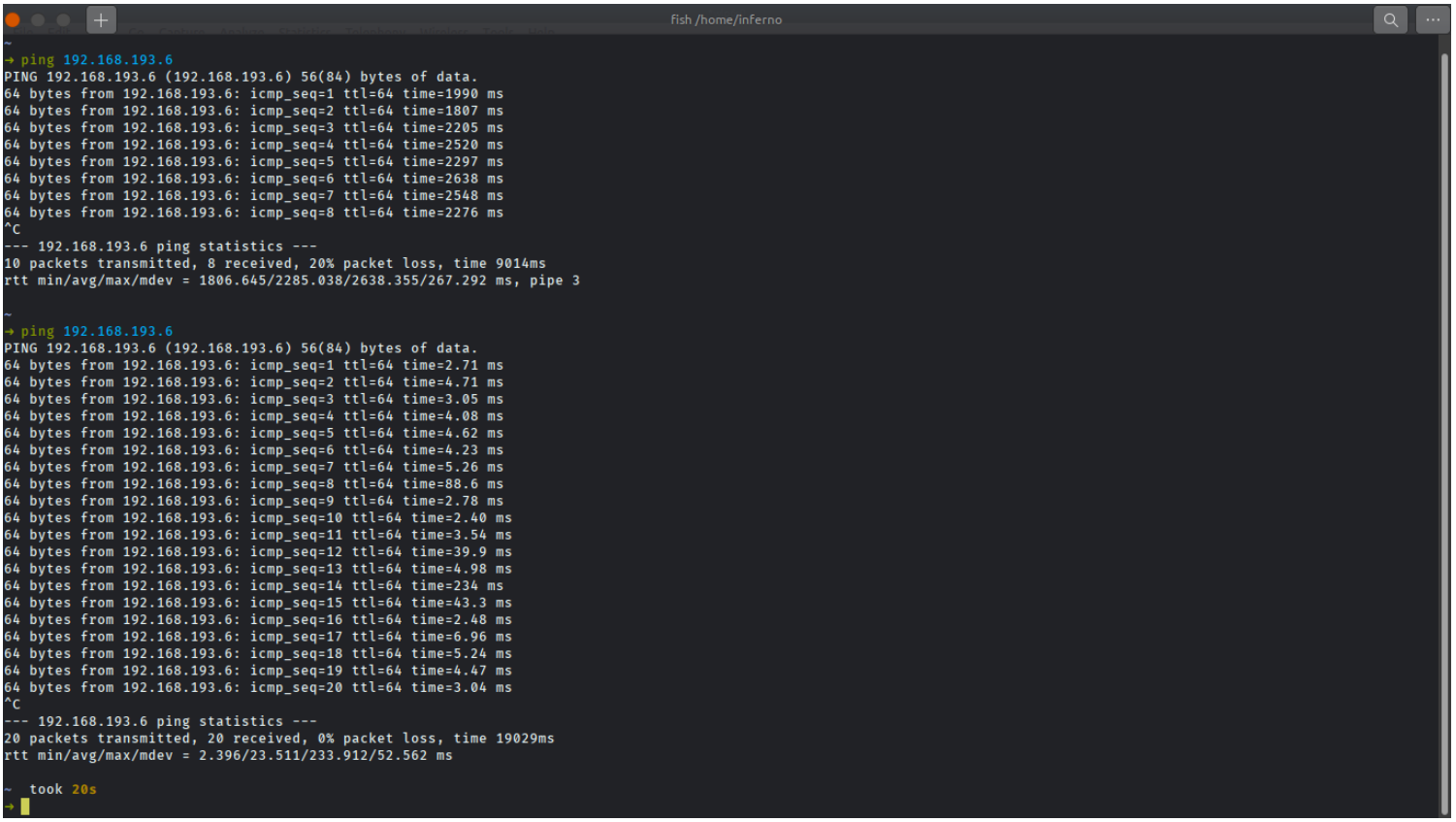
After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

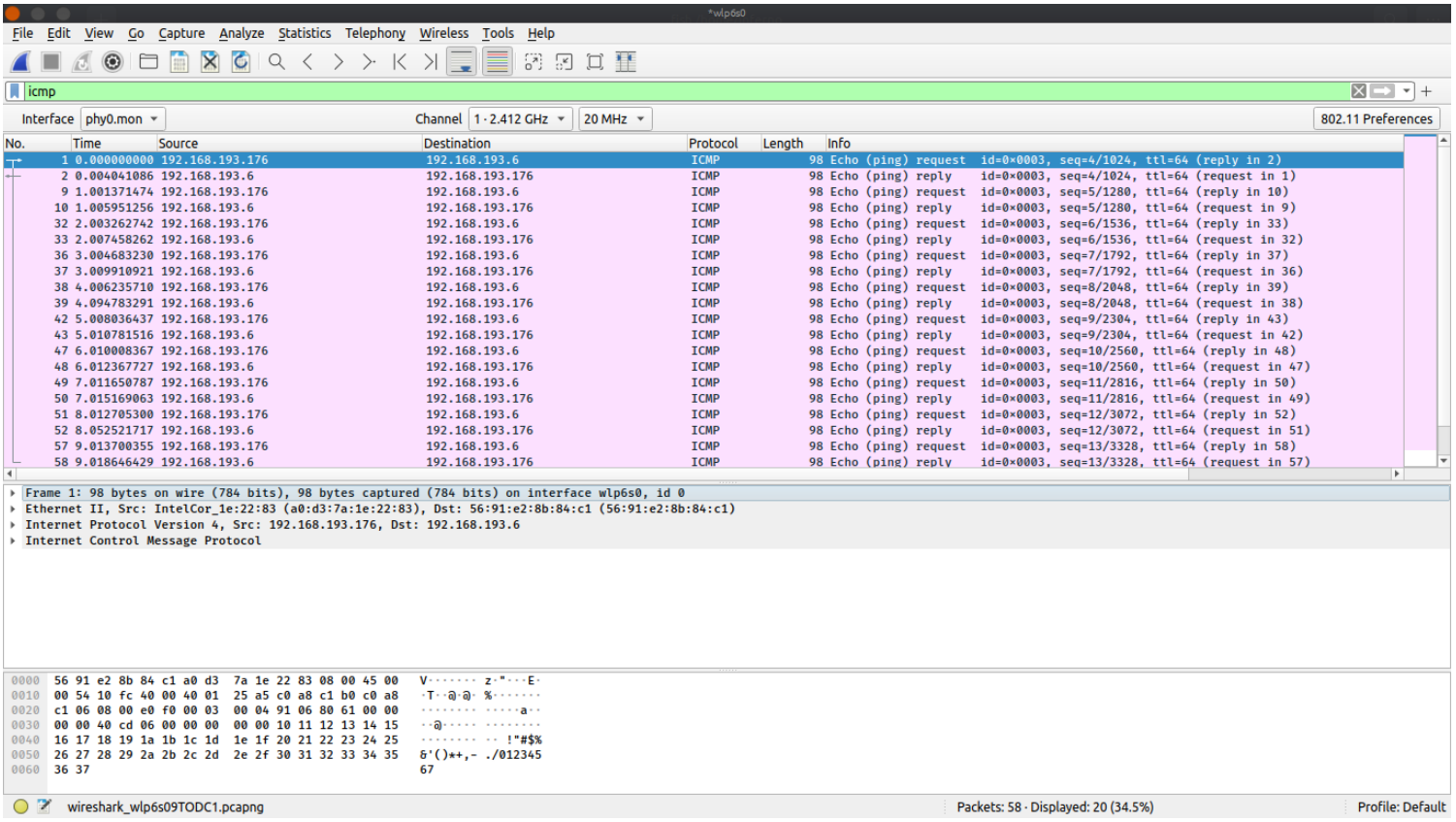
Specifications:

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

Questions and Solutions:

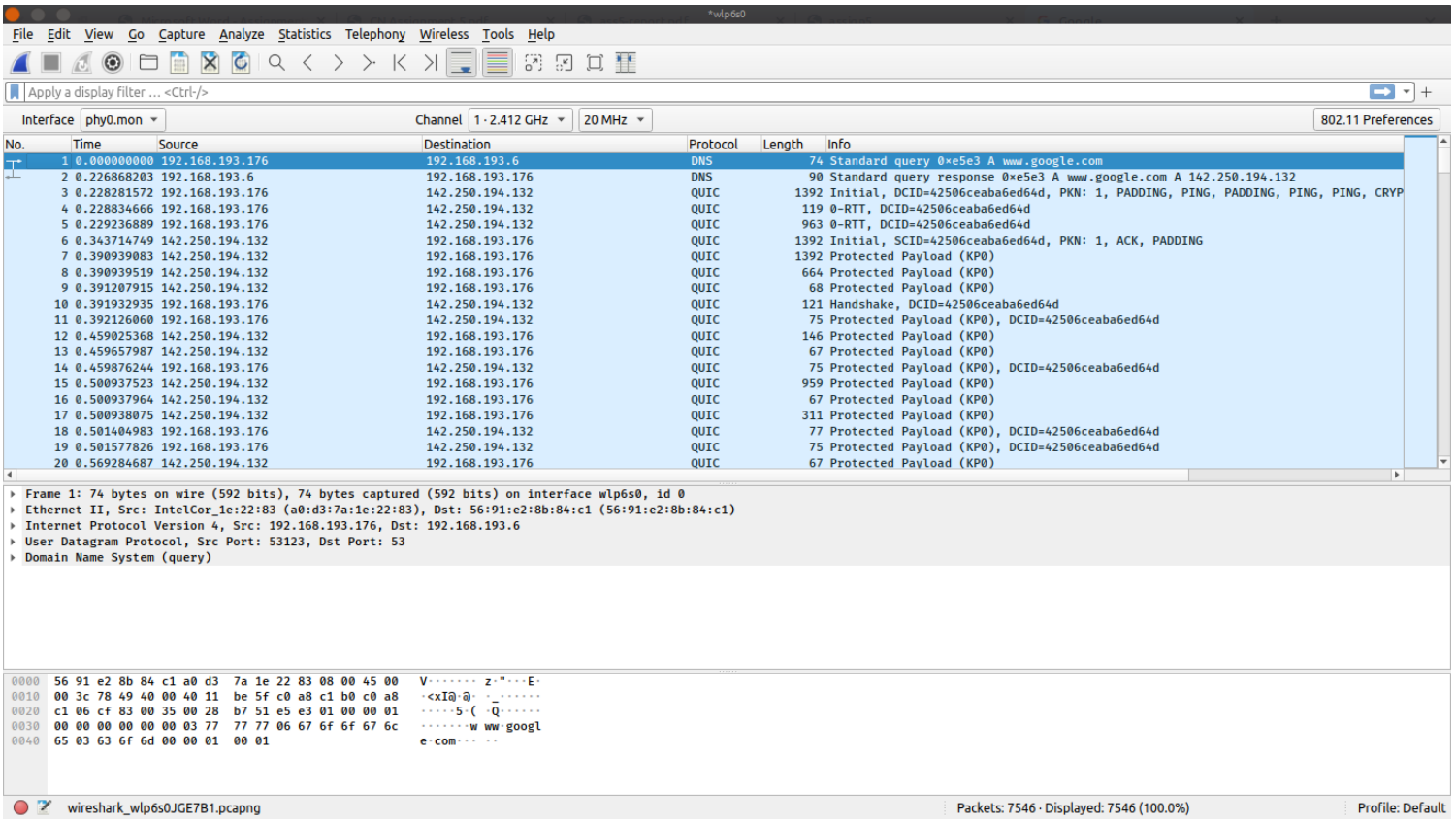
Q1. Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighbouring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

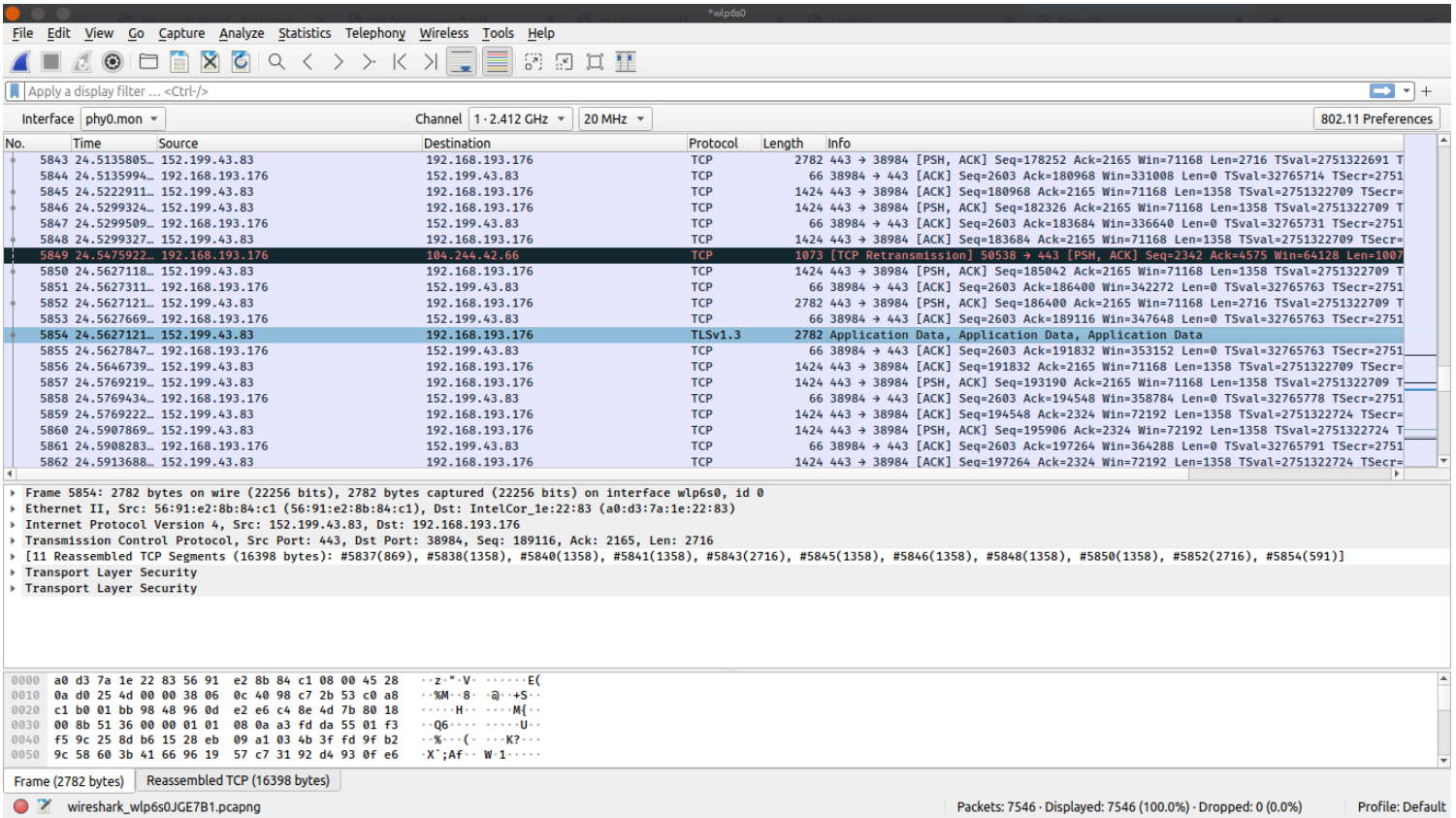




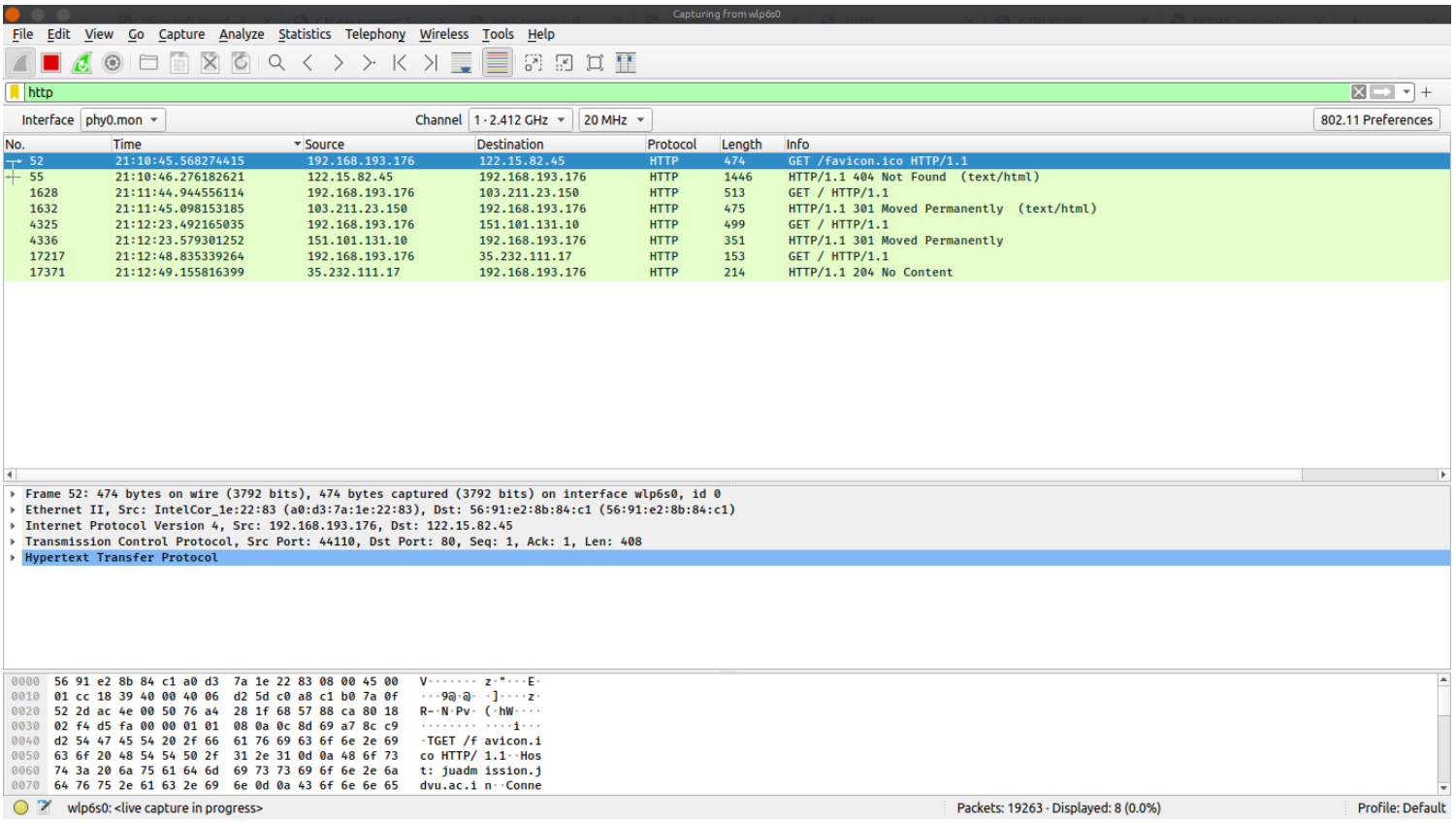
Q2. Generate some web traffic and

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



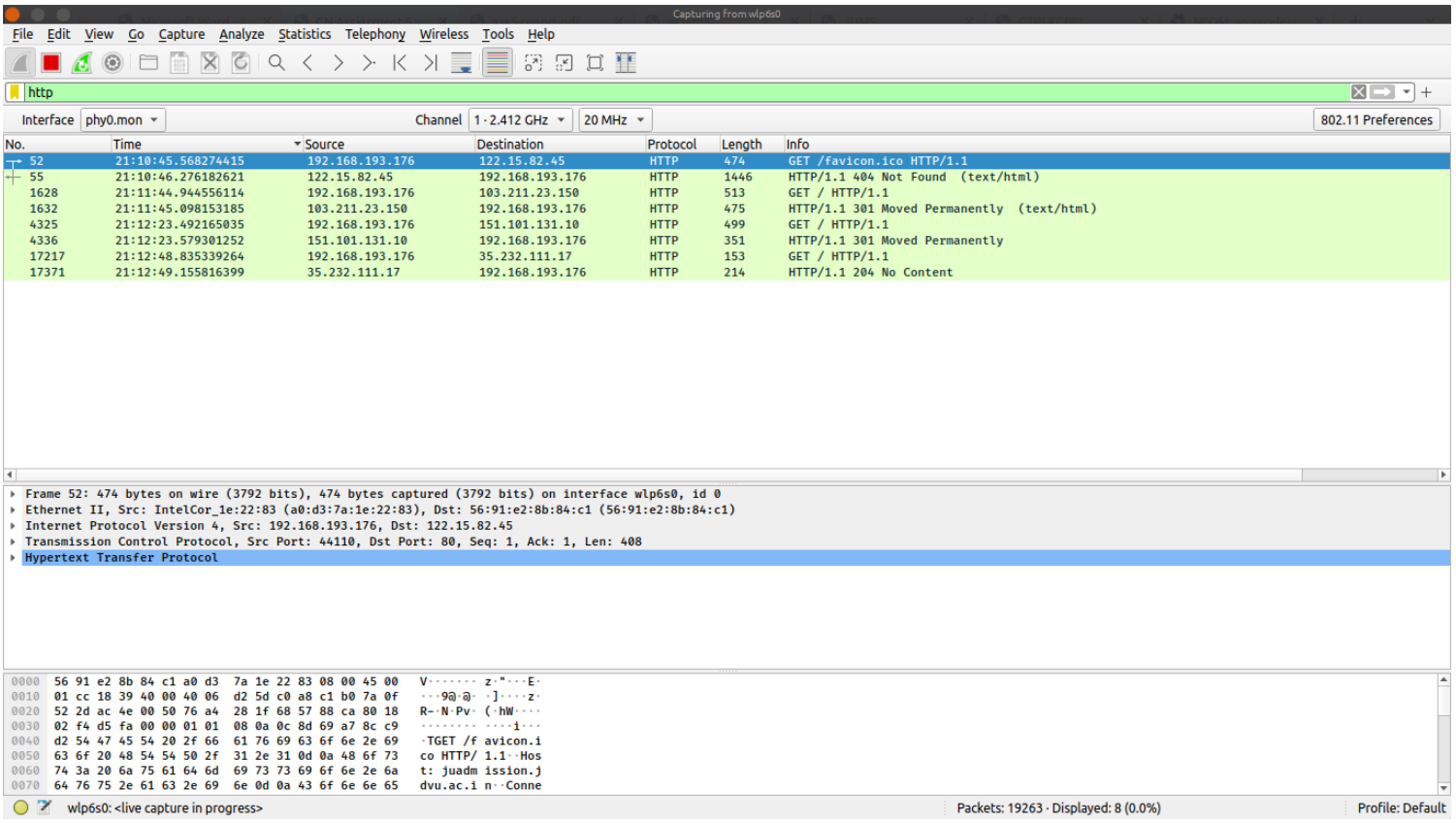


b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark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



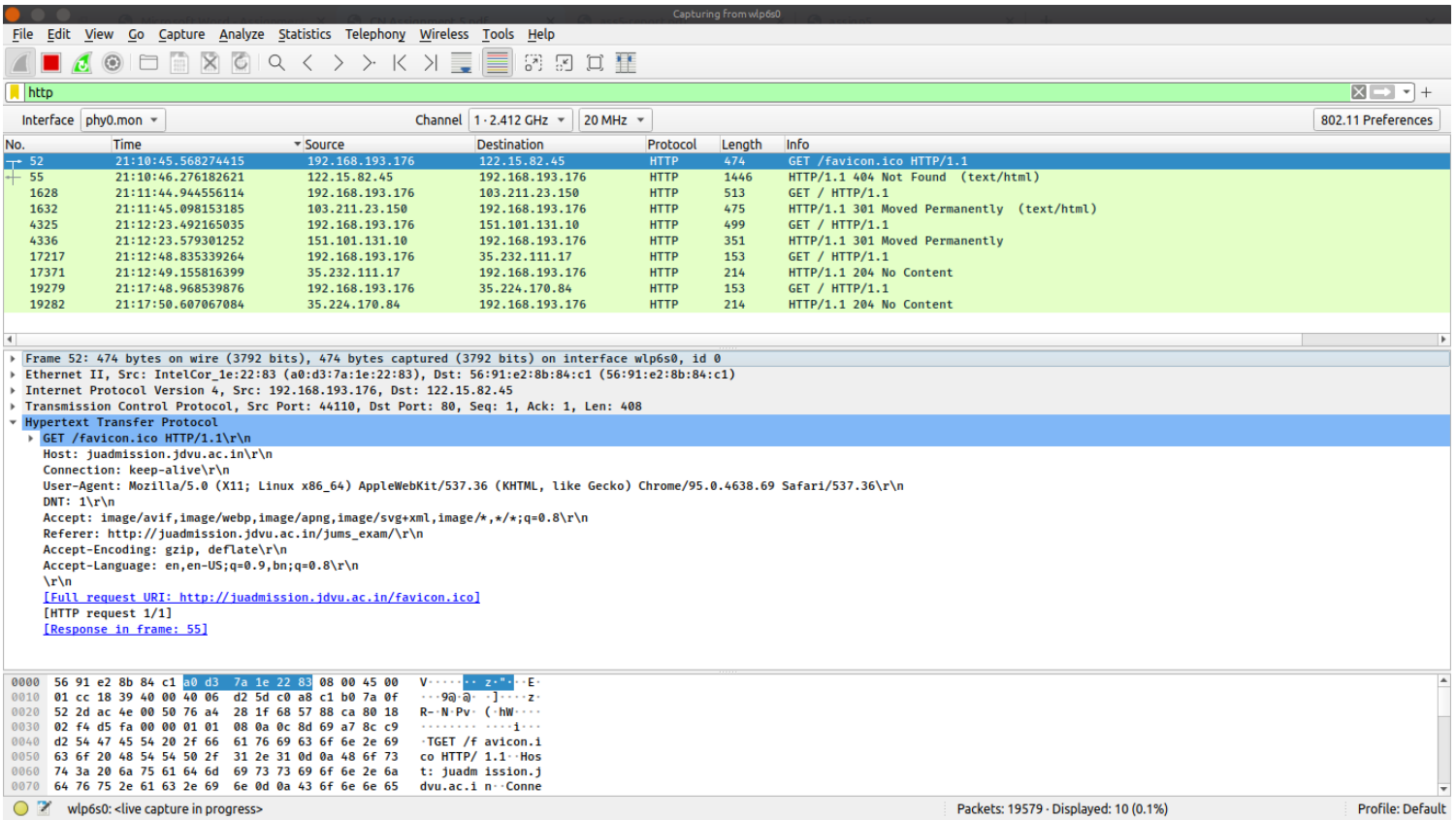
As shown in the screenshot above the GET(52) was sent at 21.10.45.56824415 seconds and the reply OK(55) was received at 21.10.46.26182621 seconds. Thus the delay is (46.26182621 - 45.56824415) seconds which is 693.58206 milliseconds.

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

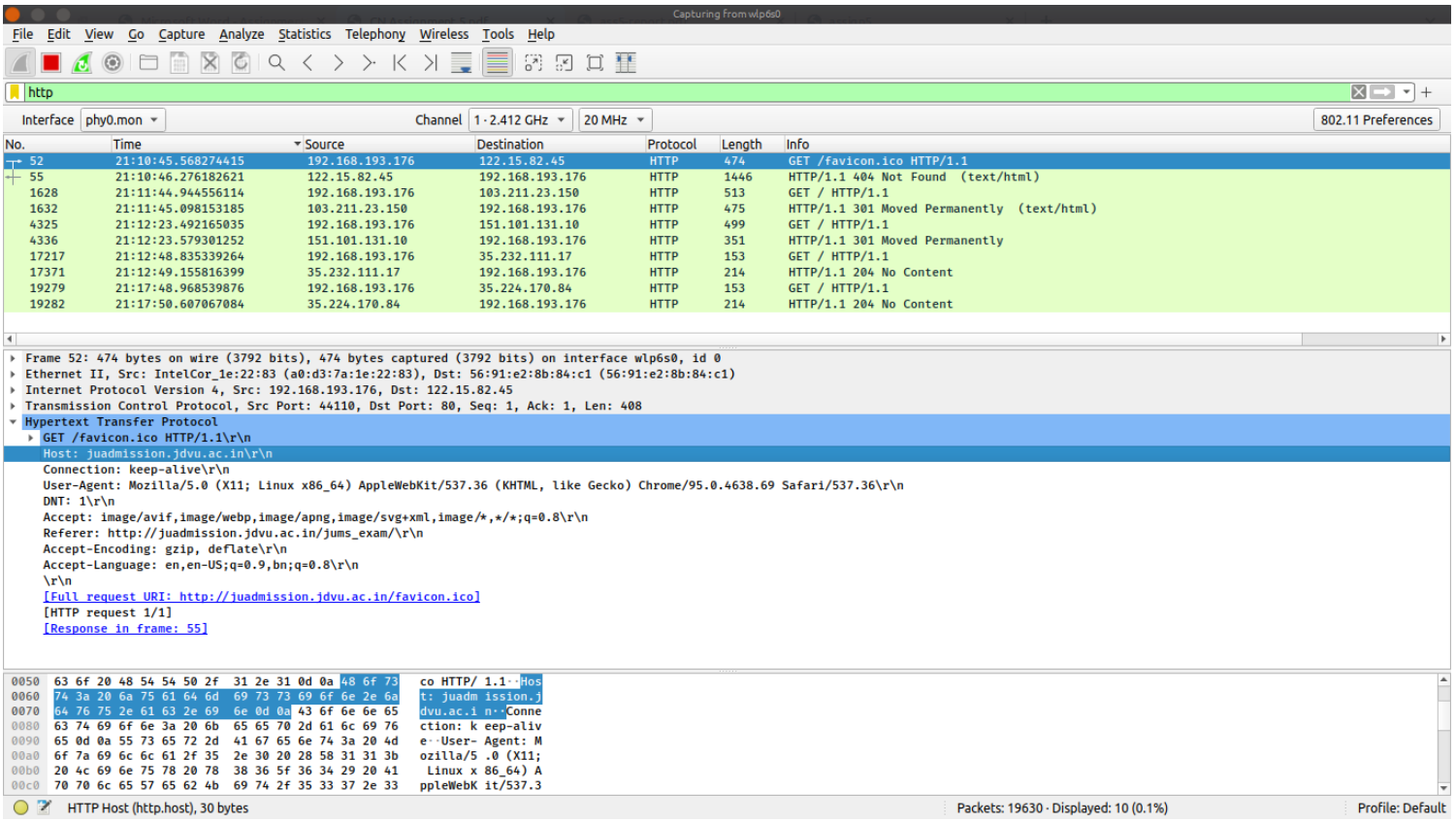


As shown in the screenshot above, the IP address of the website is **122.15.82.45** and the IP address of my laptop is **192.168.193.176**

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.

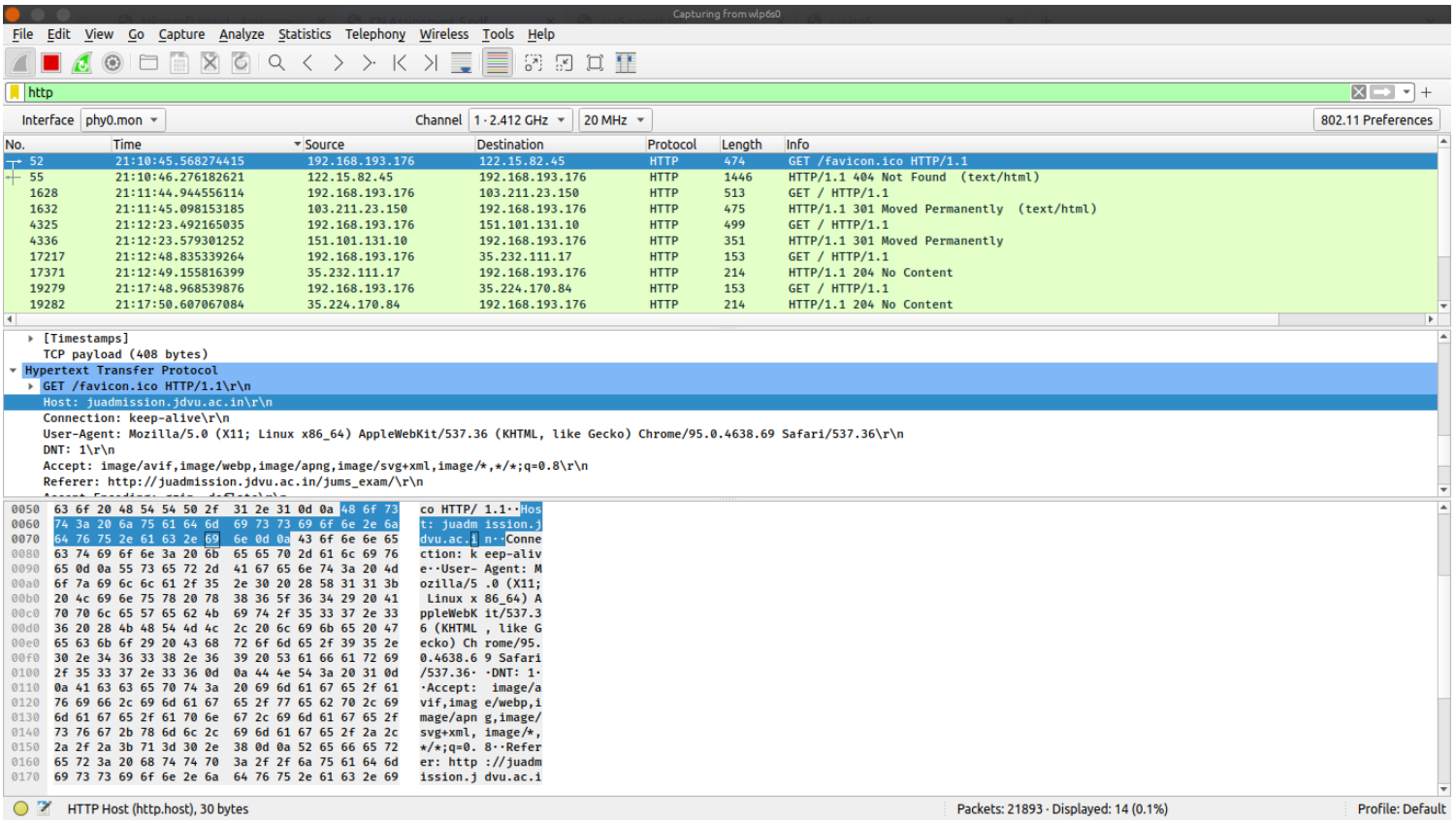


e. Find out the value of the Host from the Packet Details Panel, within the GET command.



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.

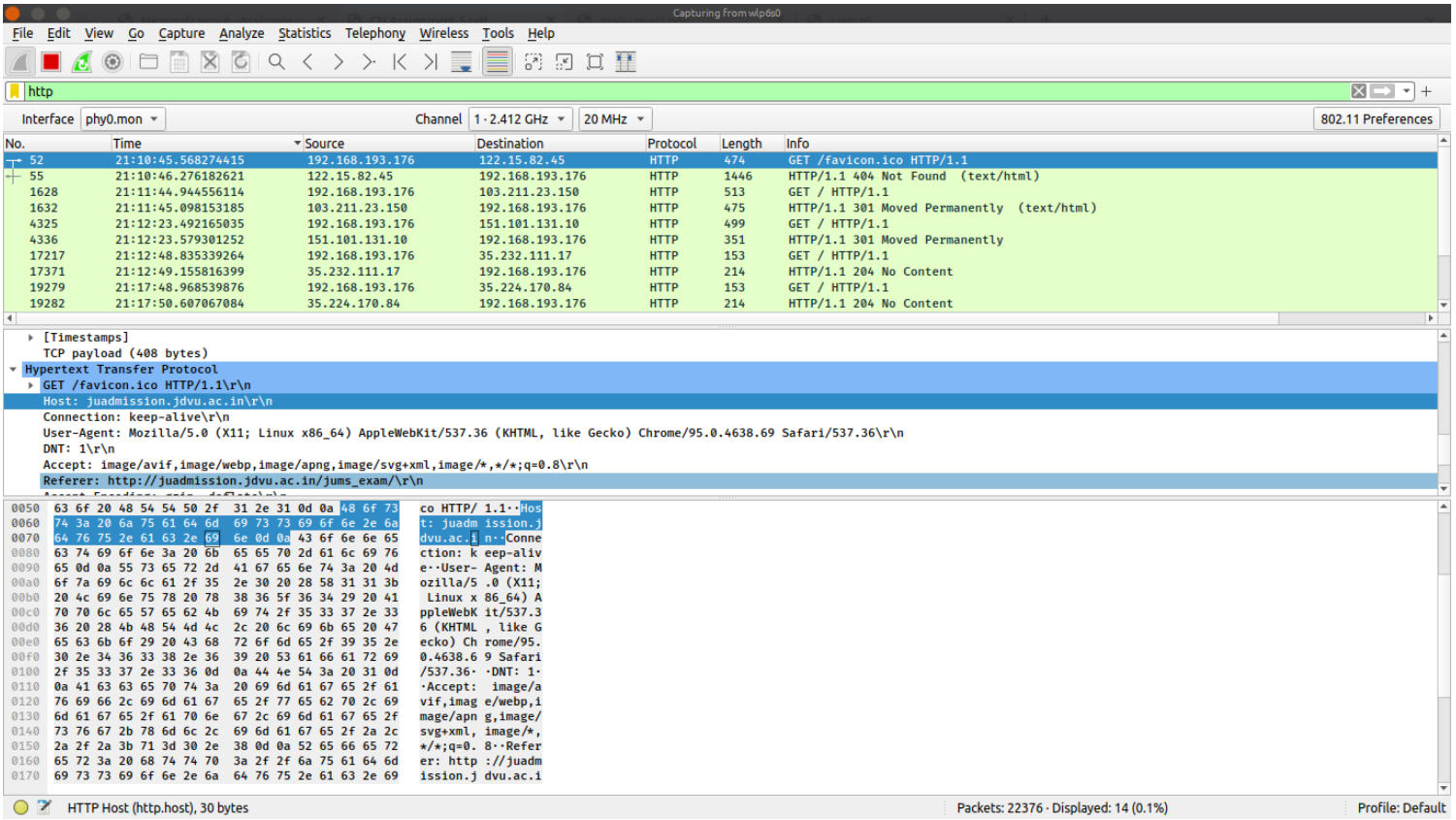


The **HEX** and **ASCII** representations of the packet are :

HEX	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 /favicon.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: 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

```
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....
```

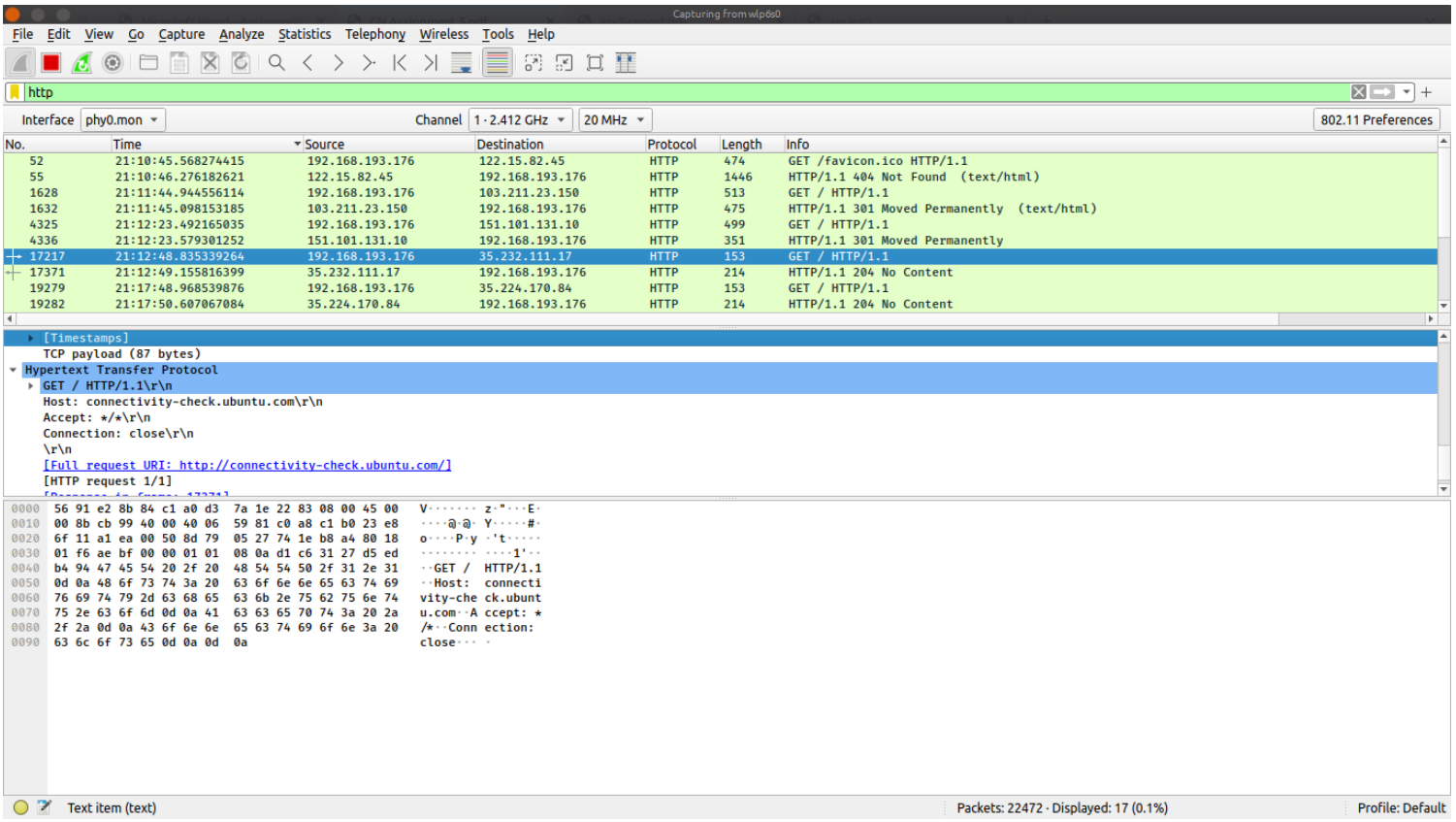
Q4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel



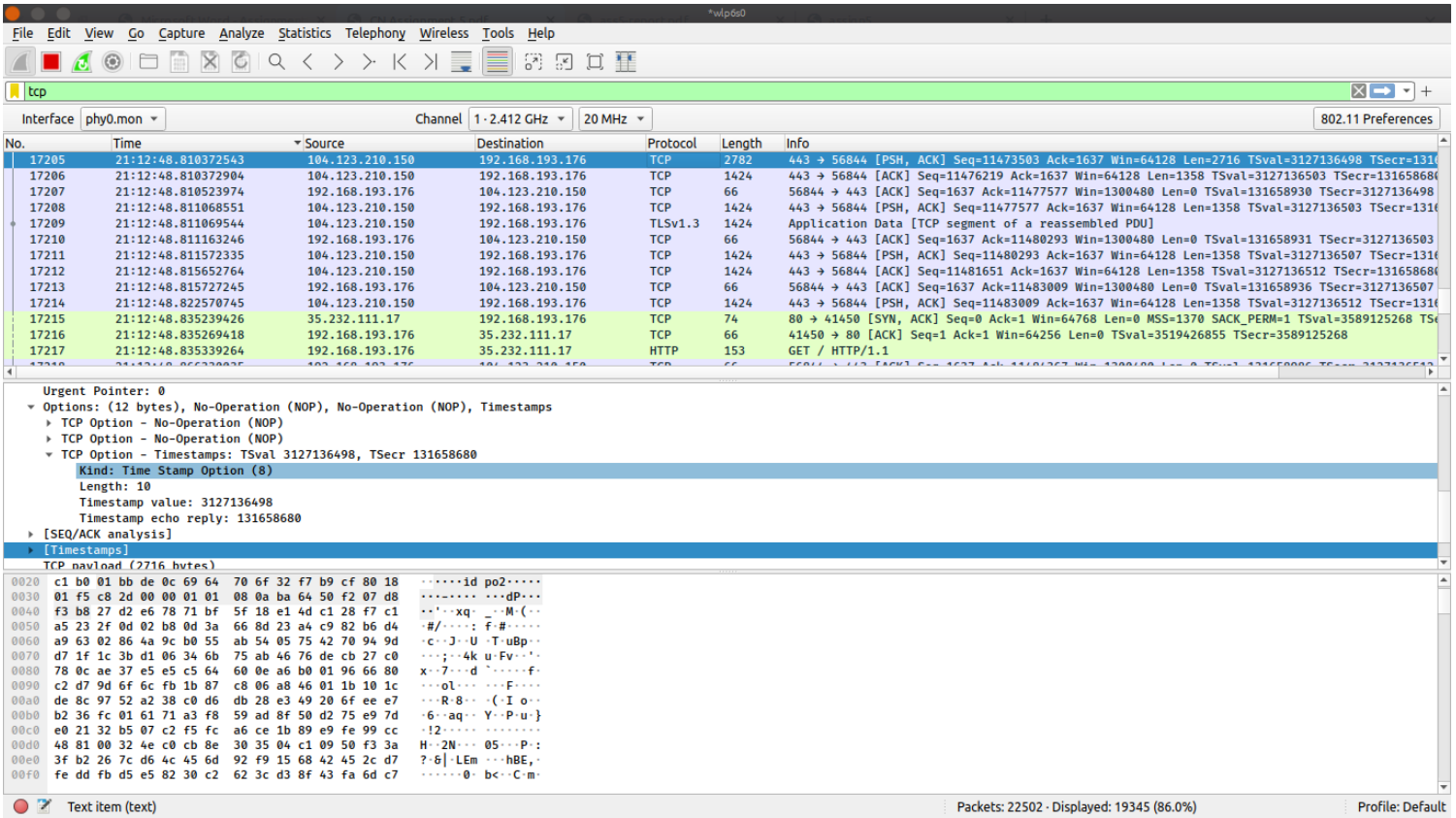
The first four bytes of the Hex value of the Host parameter from the Packet Bytes Panel are : **48 6f 73 74**

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.

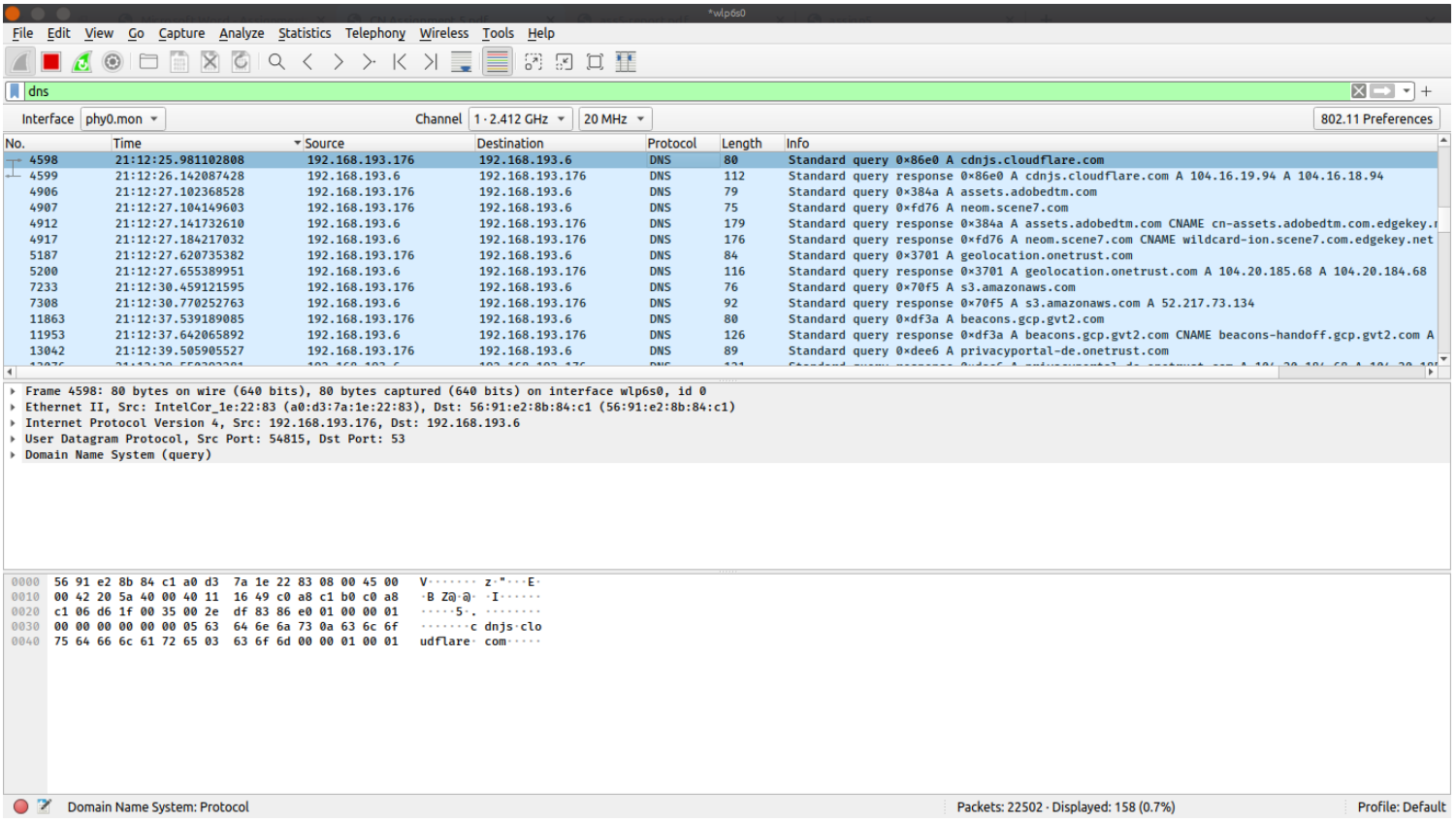
HTTP:



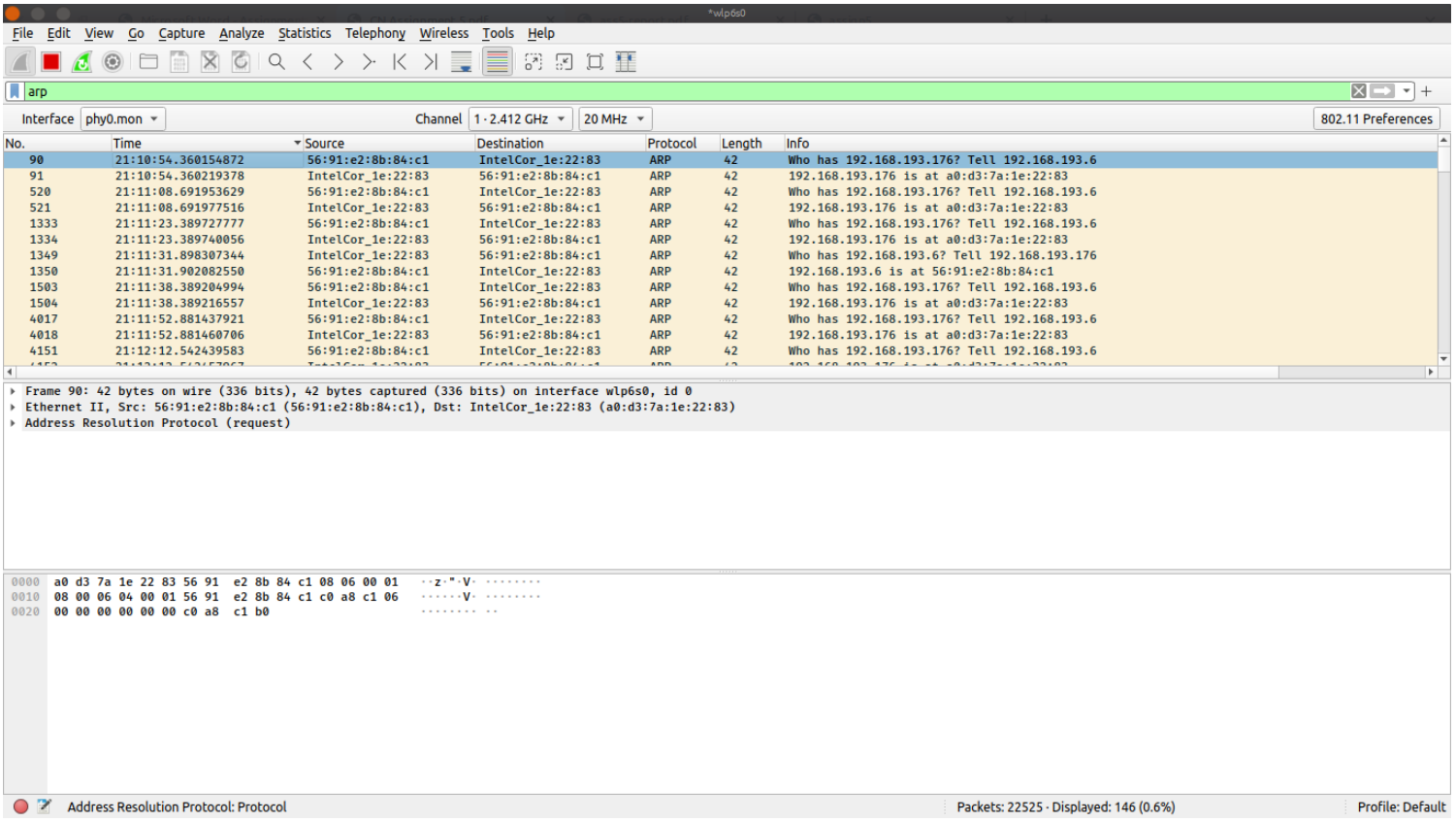
TCP:



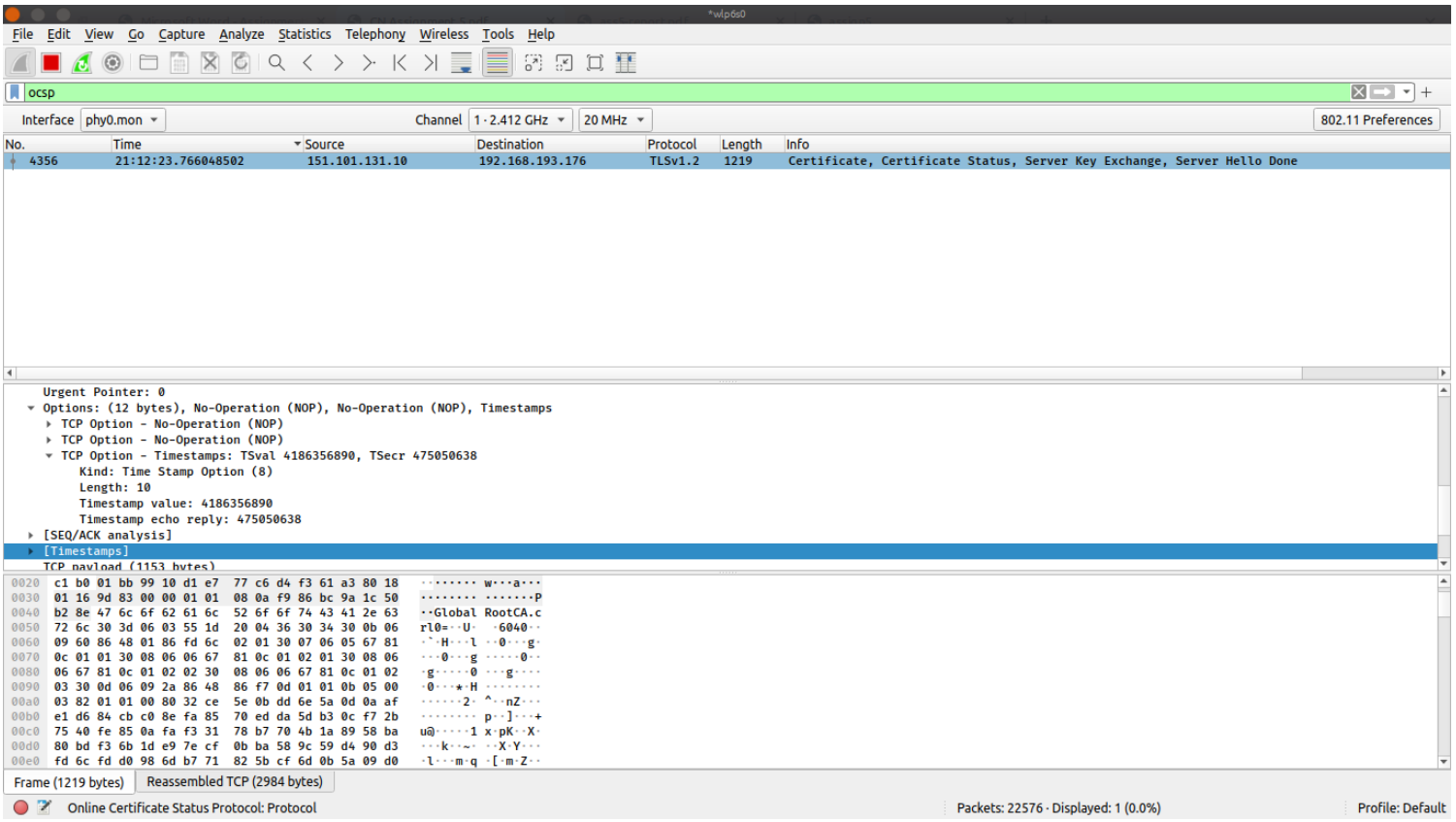
DNS:


*wlp6s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
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.
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
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)
0000 56 91 e2 8b 84 c1 a0 d3 7a 1e 22 83 08 00 45 00 V····· z·"···E·
0010 00 42 20 5a 40 00 40 11 16 49 c0 a8 c1 b0 c0 a8 ·B Z@·@· ·I····
0020 c1 06 d6 1f 00 35 00 2e df 83 86 e0 01 00 00 01 ·····5·. ·····
0030 00 00 00 00 00 00 05 63 64 6e 6a 73 0a 63 6c 6f ·····c dnjs·clo
0040 75 64 66 6c 61 72 65 03 63 6f 6d 00 00 01 00 01 udflare· com·····
Domain Name System: Protocol
Packets: 22502 · Displayed: 158 (0.7%)
Profile: Default

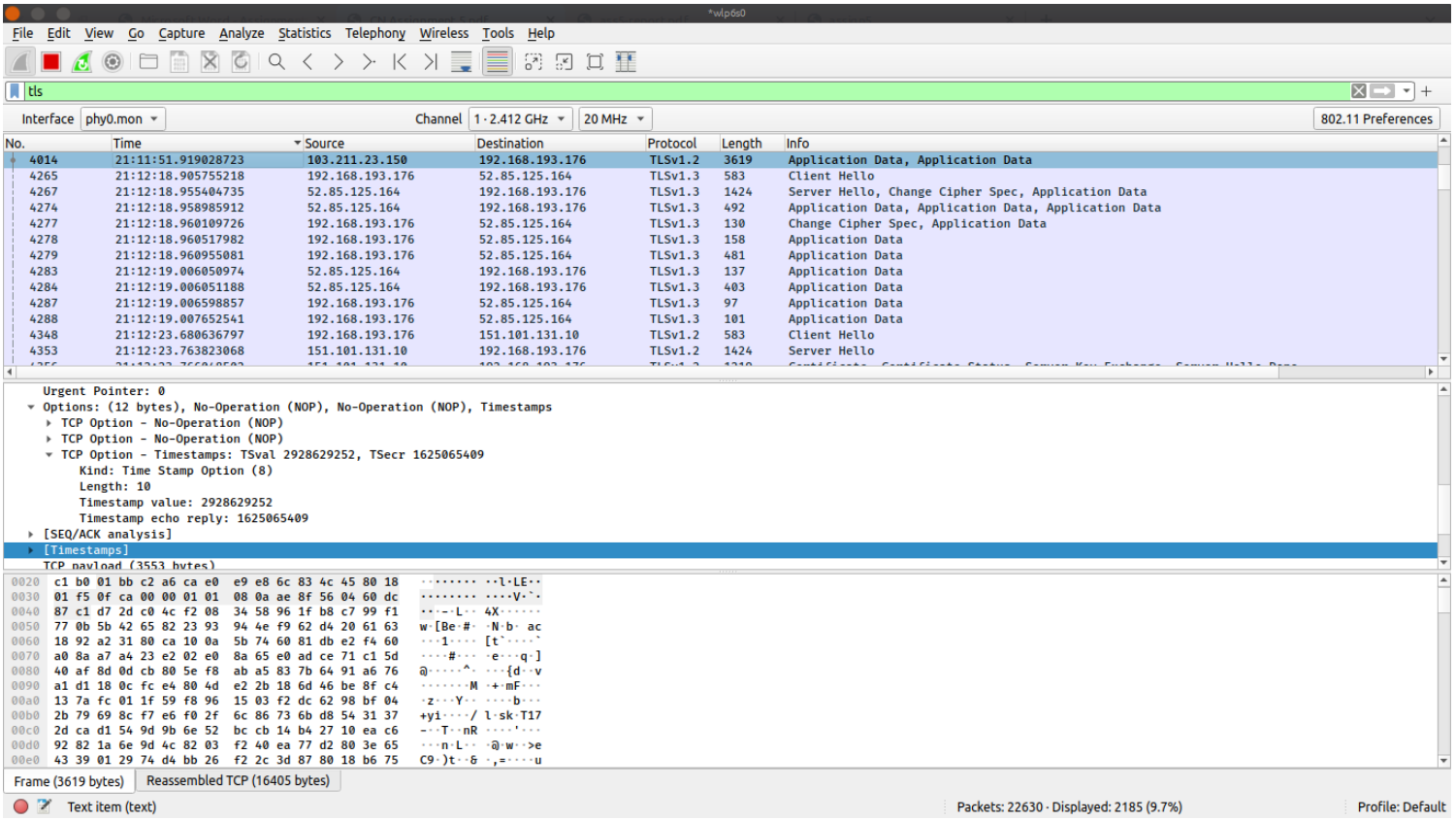
ARP:


*wlp6s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
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)
0000 a0 d3 7a 1e 22 83 56 91 e2 8b 84 c1 08 06 00 01 ··z·"·V· ····
0010 08 00 06 04 00 01 56 91 e2 8b 84 c1 c0 a8 c1 06 ·····V· ····
0020 00 00 00 00 00 00 c0 a8 c1 b0 ····· ··
Address Resolution Protocol: Protocol
Packets: 22525 · Displayed: 146 (0.6%)
Profile: Default

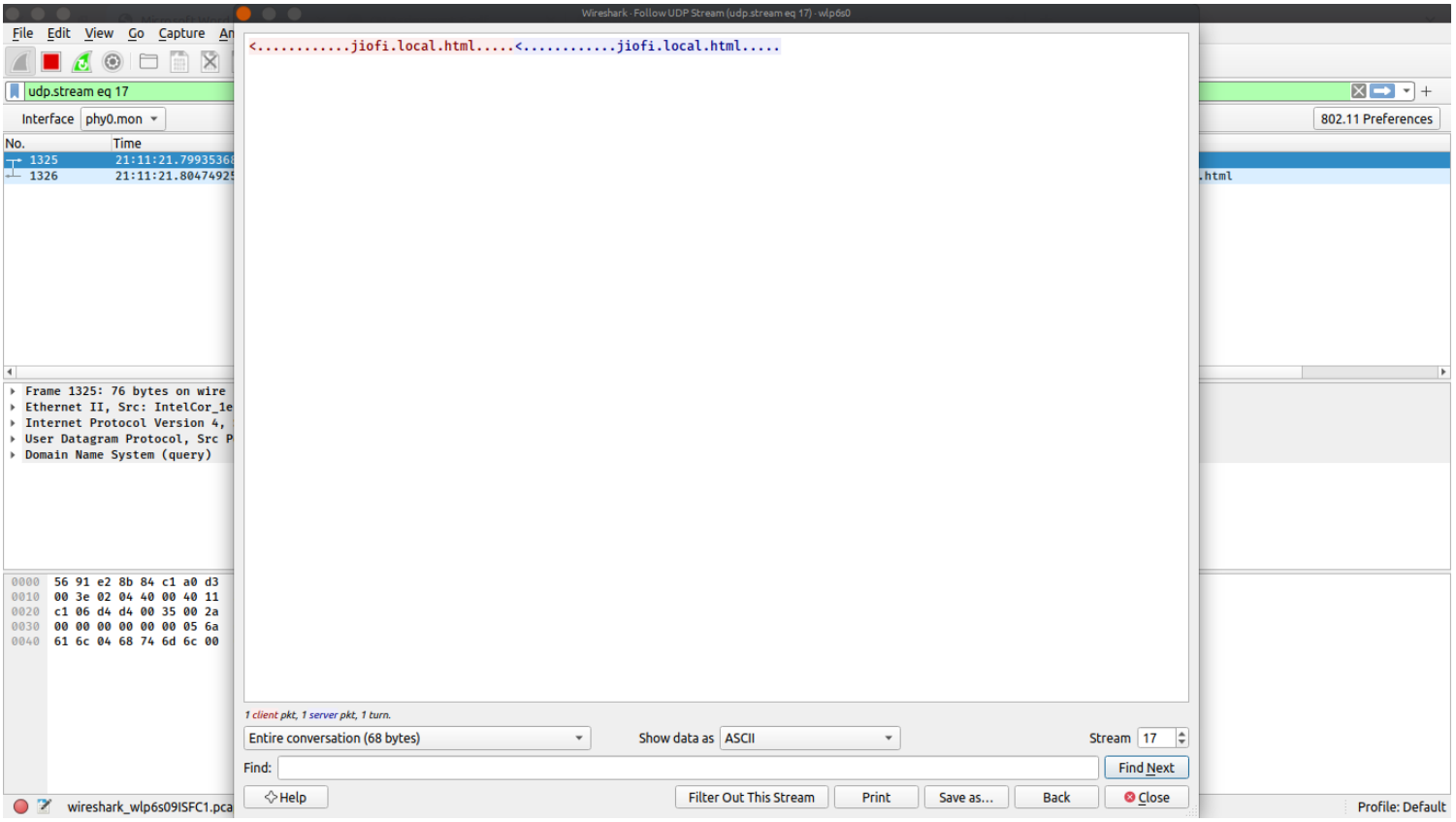
OCSP:

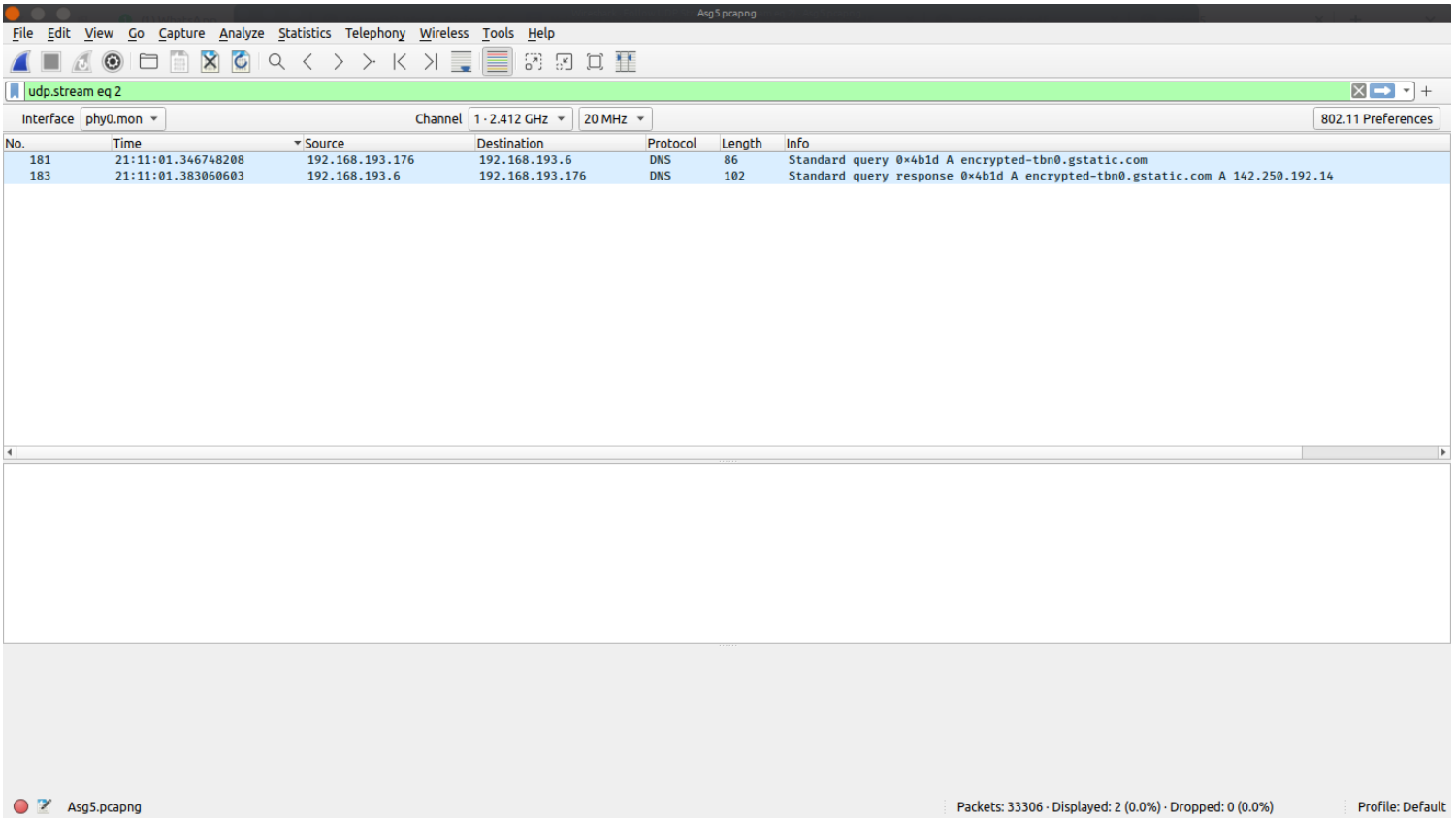

*wlp6s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ocsp
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
4356 21:12:23.766048502 151.101.131.10 192.168.193.176 TLSv1.2 1219 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
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)
0020 c1 b0 01 bb 99 10 d1 e7 77 c6 d4 f3 61 a3 80 18
0030 01 16 9d 83 00 00 01 01 08 0a f9 86 bc 9a 1c 50
0040 b2 8e 47 6c 6f 62 61 6c 52 6f 6f 74 43 41 2e 63
0050 72 6c 30 3d 06 03 55 1d 20 04 36 30 34 30 0b 06
0060 09 60 86 48 01 86 fd 6c 02 01 30 07 06 05 67 81
0070 0c 01 01 30 08 06 06 67 81 0c 01 02 01 30 08 06
0080 06 67 81 0c 01 02 02 30 08 06 06 67 81 0c 01 02
0090 03 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00
00a0 03 82 01 01 00 80 32 ce 5e 0b dd 6e 5a 0d 0a af
00b0 e1 d6 84 cb c0 8e fa 85 70 ed da 5d b3 0c f7 2b
00c0 75 40 fe 85 0a fa f3 31 78 b7 70 4b 1a 89 58 ba
00d0 80 bd f3 6b 1d e9 7e cf 0b ba 58 9c 59 d4 90 d3
00e0 fd 6c fd d0 98 6d b7 71 82 5b cf 6d 0b 5a 09 d0
Frame (1219 bytes)
Reassembled TCP (2984 bytes)
Online Certificate Status Protocol: Protocol
Packets: 22576 · Displayed: 1 (0.0%)
Profile: Default

TLS:


*wlp6s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
4014 21:11:51.919028723 103.211.23.150 192.168.193.176 TLSv1.2 3619 Application Data, Application Data
4265 21:12:18.905755218 192.168.193.176 52.85.125.164 TLSv1.3 583 Client Hello
4267 21:12:18.955404735 52.85.125.164 192.168.193.176 TLSv1.3 1424 Server Hello, Change Cipher Spec, Application Data
4274 21:12:18.958985912 52.85.125.164 192.168.193.176 TLSv1.3 492 Application Data, Application Data, Application Data
4277 21:12:18.960109726 192.168.193.176 52.85.125.164 TLSv1.3 130 Change Cipher Spec, Application Data
4278 21:12:18.960517982 192.168.193.176 52.85.125.164 TLSv1.3 158 Application Data
4279 21:12:18.960955081 192.168.193.176 52.85.125.164 TLSv1.3 481 Application Data
4283 21:12:19.006050974 52.85.125.164 192.168.193.176 TLSv1.3 137 Application Data
4284 21:12:19.006051188 52.85.125.164 192.168.193.176 TLSv1.3 403 Application Data
4287 21:12:19.006598857 192.168.193.176 52.85.125.164 TLSv1.3 97 Application Data
4288 21:12:19.007652541 192.168.193.176 52.85.125.164 TLSv1.3 101 Application Data
4348 21:12:23.680636797 192.168.193.176 151.101.131.10 TLSv1.2 583 Client Hello
4353 21:12:23.763823068 151.101.131.10 192.168.193.176 TLSv1.2 1424 Server 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)
0020 c1 b0 01 bb c2 a6 ca e0 e9 e8 6c 83 4c 45 80 18
0030 01 f5 0f ca 00 00 01 01 08 0a ae 8f 56 04 60 dc
0040 87 c1 d7 2d c0 4c f2 08 34 58 96 1f b8 c7 99 f1
0050 77 0b 5b 42 65 82 23 93 94 4e f9 62 d4 20 61 63
0060 18 92 a2 31 80 ca 10 0a 5b 74 60 81 db e2 f4 60
0070 a0 8a a7 a4 23 e2 02 e0 8a 65 e0 ad ce 71 c1 5d
0080 40 af 8d 0d cb 80 5e f8 ab a5 83 7b 64 91 a6 76
0090 a1 d1 18 0c fc e4 80 4d e2 2b 18 6d 46 be 8f c4
00a0 13 7a fc 01 1f 59 f8 96 15 03 f2 dc 62 98 bf 04
00b0 2b 79 69 8c f7 e6 f0 2f 6c 86 73 6b d8 54 31 37
00c0 2d ca d1 54 9d 9b 6e 52 bc cb 14 b4 27 10 ea c6
00d0 92 82 1a 6e 9d 4c 82 03 f2 40 ea 77 d2 80 3e 65
00e0 43 39 01 29 74 d4 bb 26 f2 2c 3d 87 80 18 b6 75
Frame (3619 bytes)
Reassembled TCP (16405 bytes)
Text item (text)
Packets: 22630 · Displayed: 2185 (9.7%)
Profile: Default

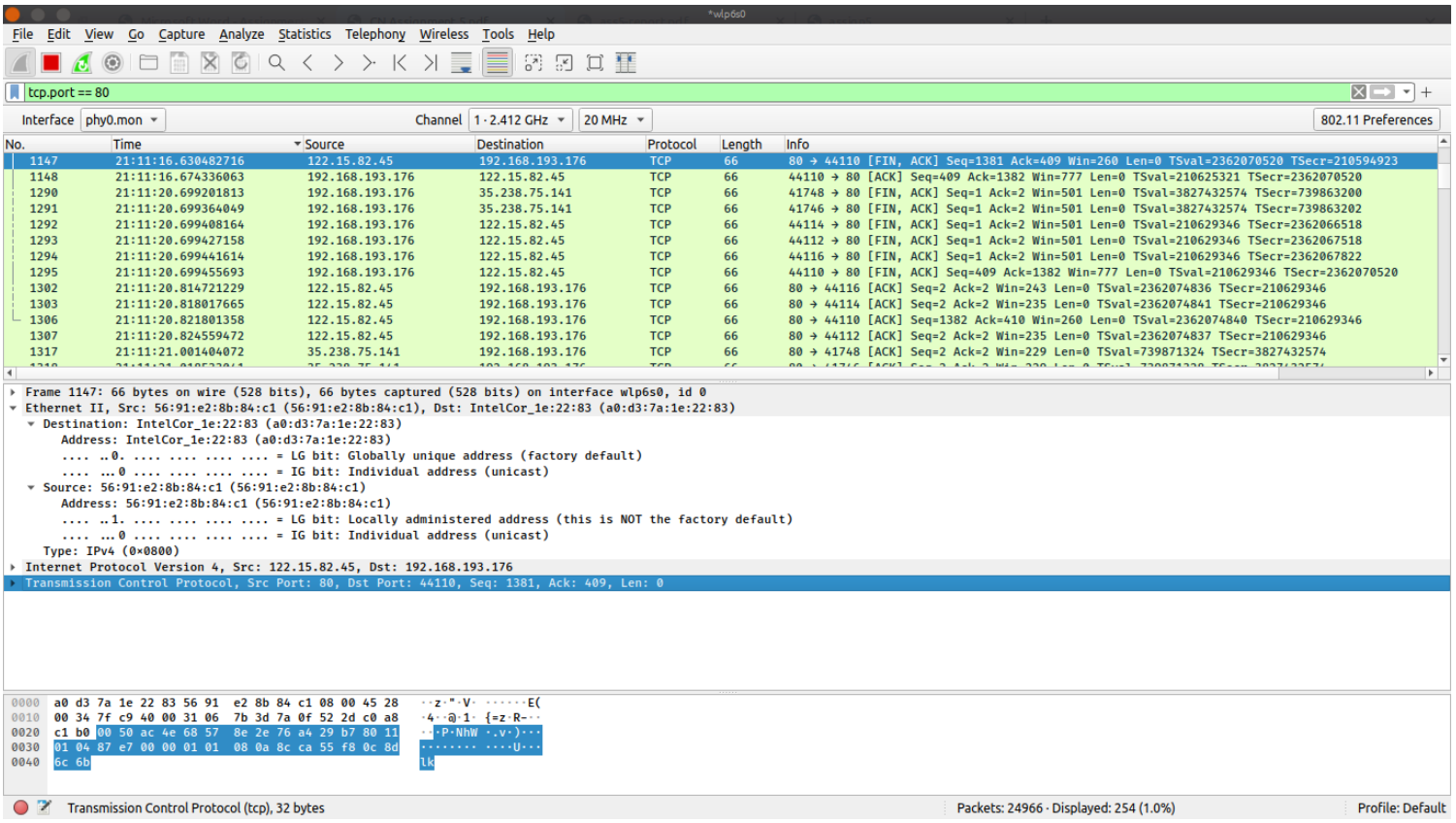
a. Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow.





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:



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**

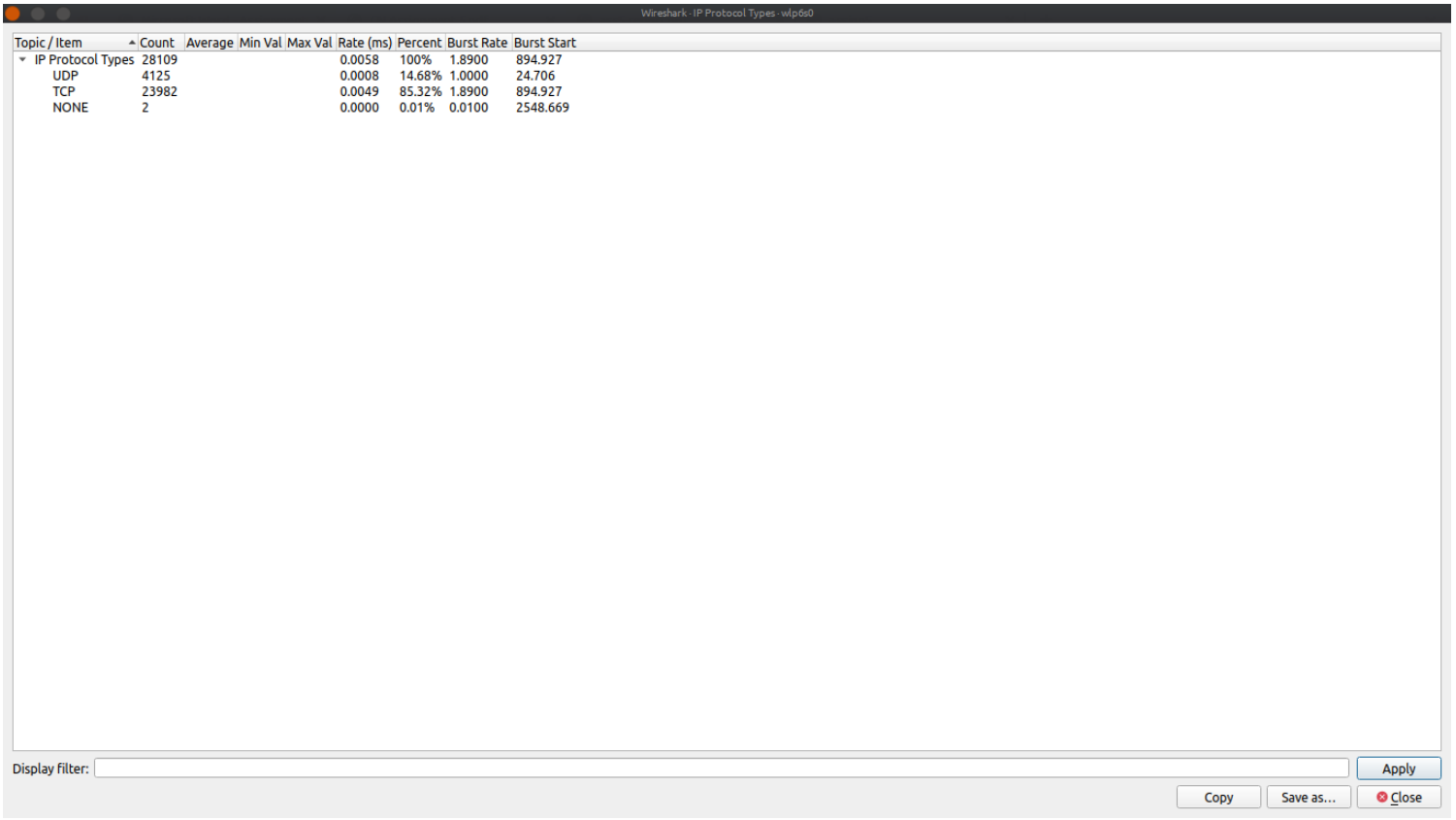
For server's manufacturer : **56:91:e2:8b:84:c1**

Q9. Find the following statistics:

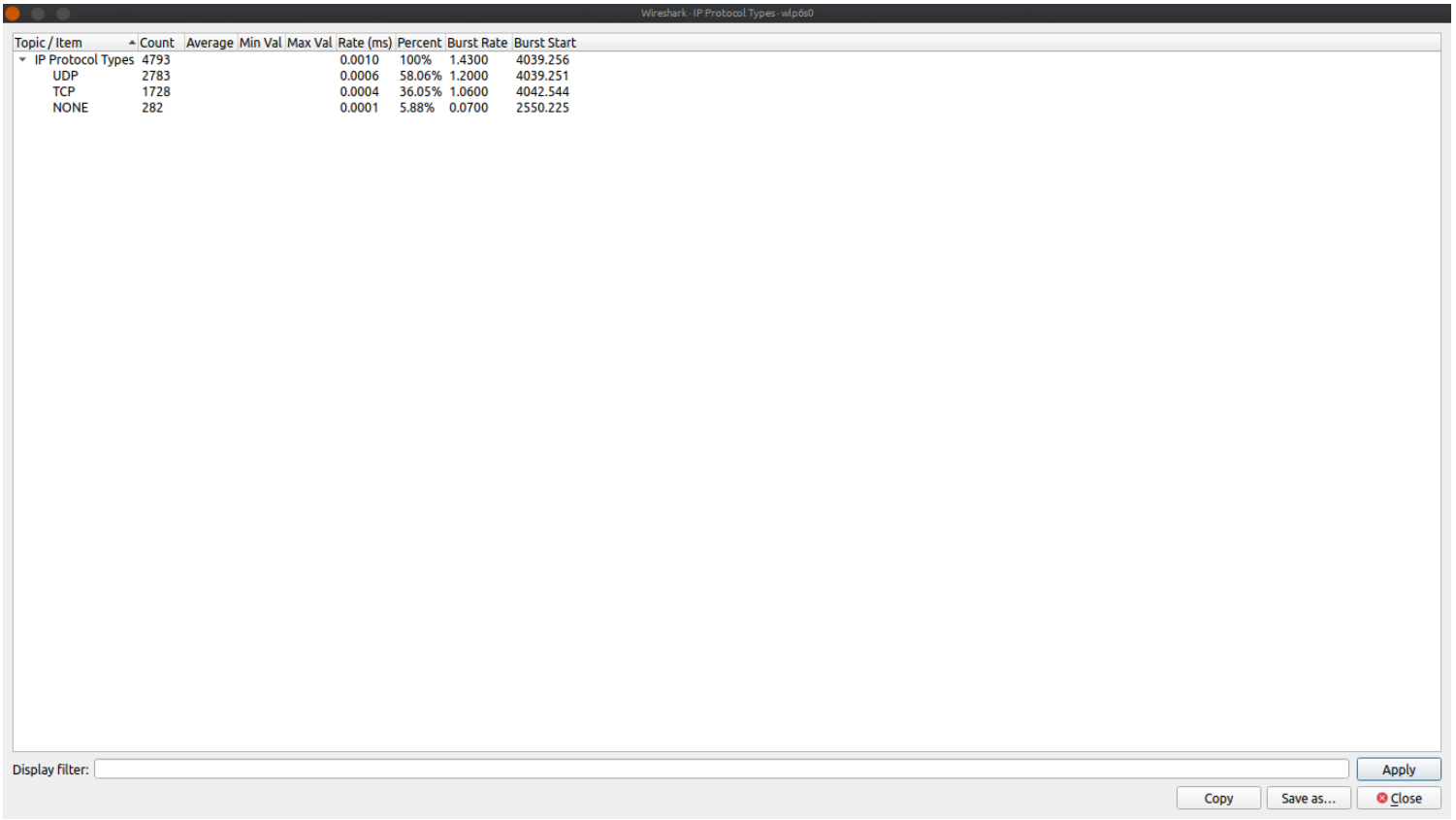
a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?

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 IPv6 statistics of the packet capture:



Higher level protocols which use **TCP**:

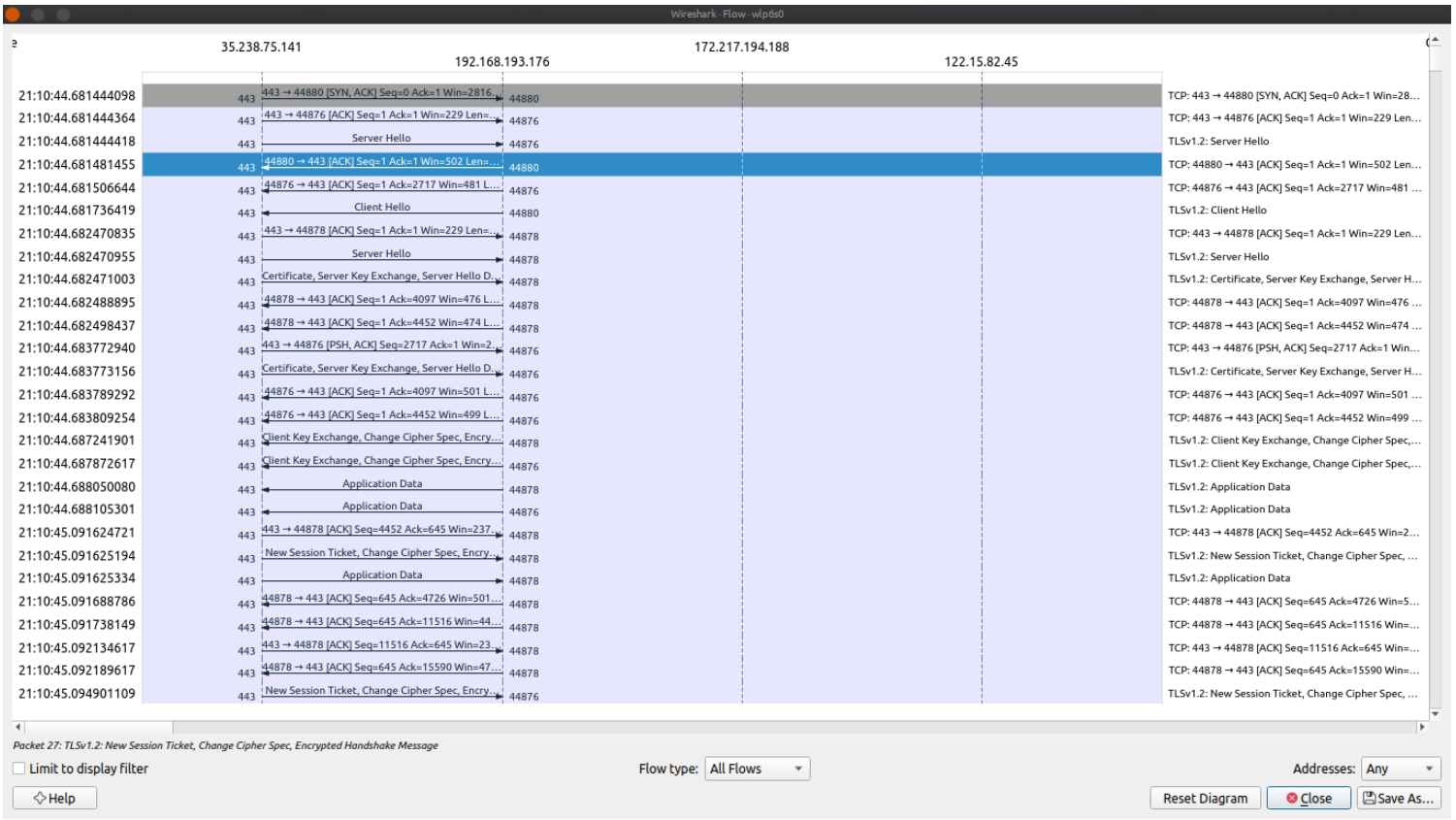
1. **HTTPS** - HyperText Transfer Protocol Secure
2. **FTP** - File Transfer Protocol

Higher level protocols which use **UDP**:

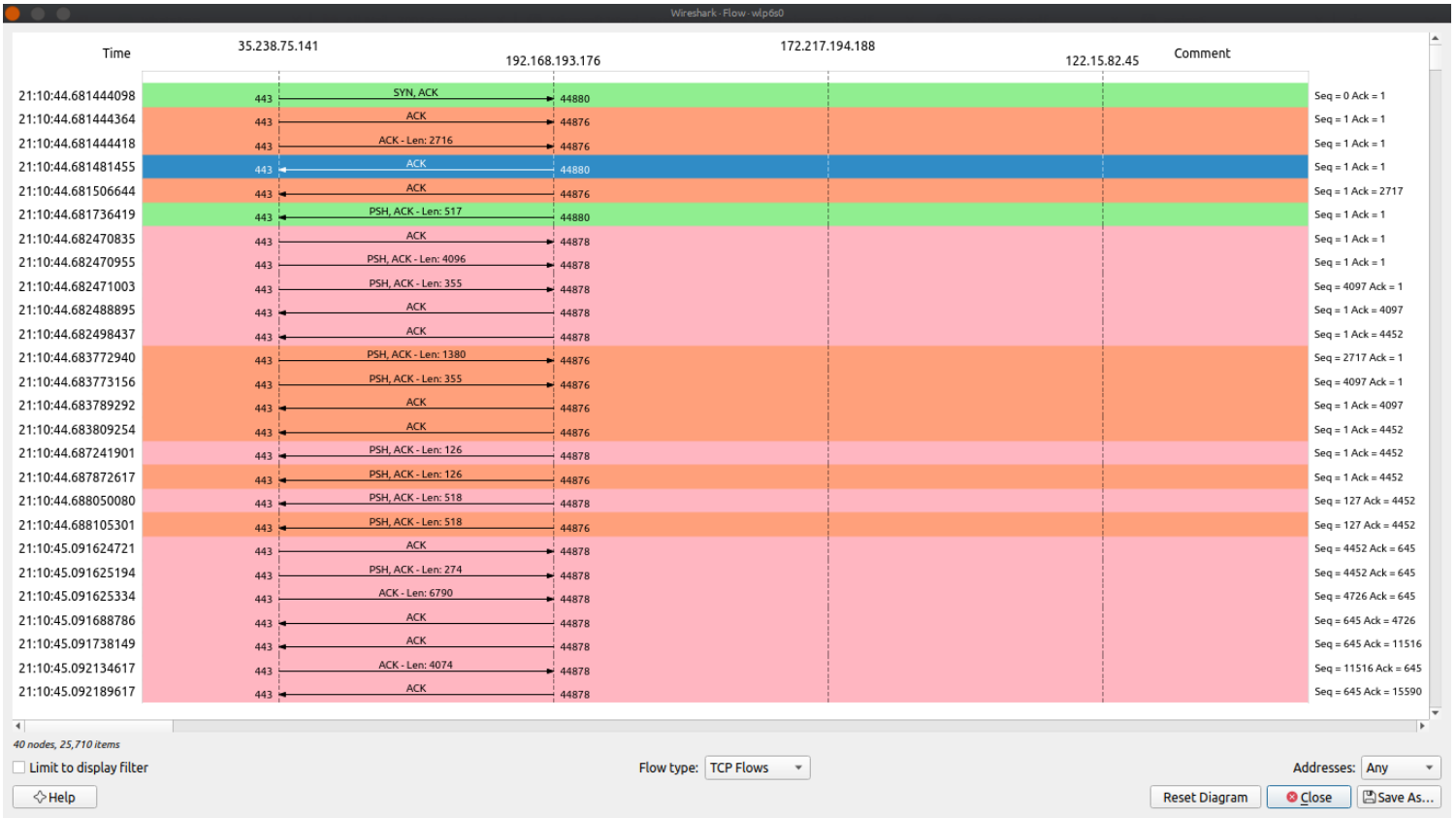
1. **SNMP** - Simple Network Management Protocol
2. **RIP** - Routing Information Protocol

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:



COMMENTS

This was a very interesting and unique assignment. It led me to learn using a new utility tool Wireshark. The packets were captured and analysed as per the requirements and helped me get a clear knowledge about how the protocols work in the real world.