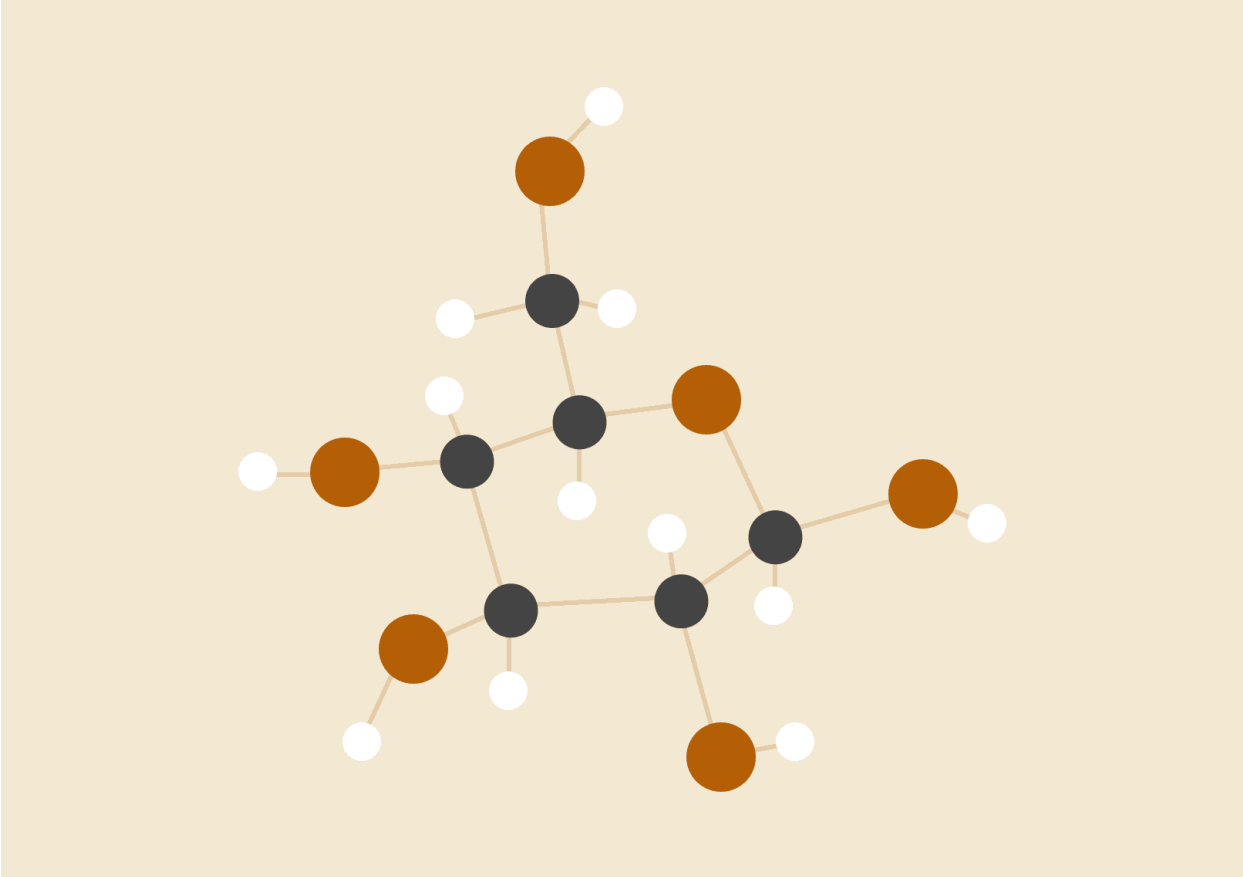
NETWORKING LAB REPORT

CLASS *BCSE III* ***SEM*** *FIFTH* ***YEAR*** *2021*



NAME Neeladri Pal

ROLL 001910501015

GROUP A1

ASSIGNMENT - 5

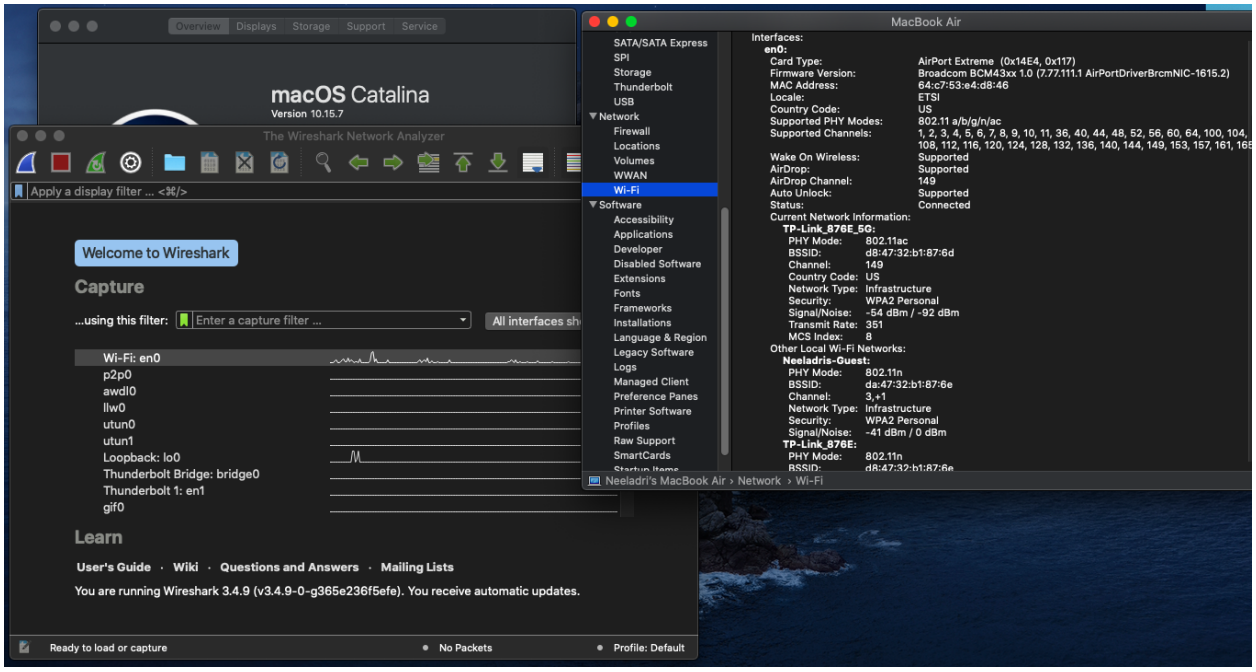
OVERVIEW

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.

OBJECTIVE

Capture and analyse packets using Wireshark.

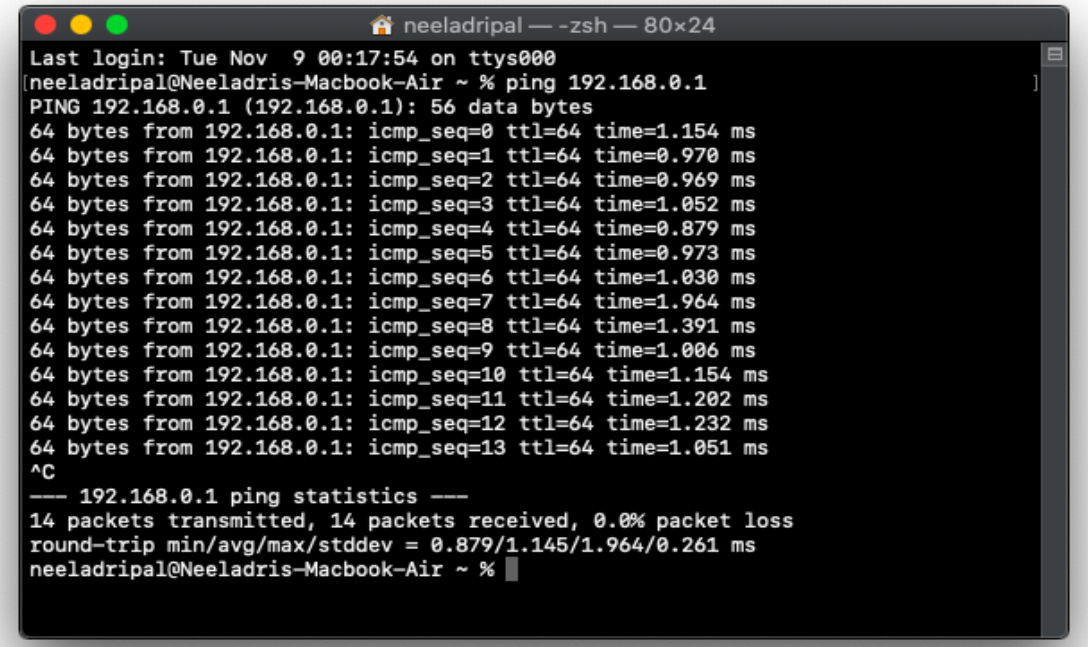
SPECIFICATIONS

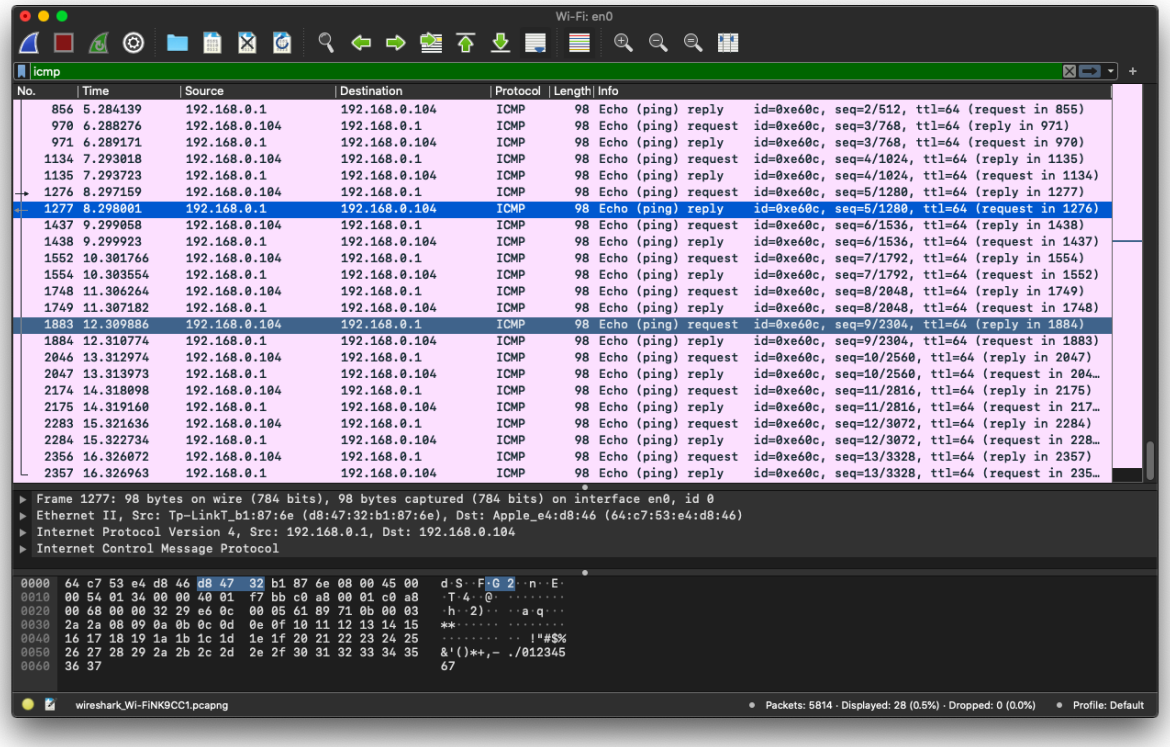


QUESTIONS AND SOLUTIONS

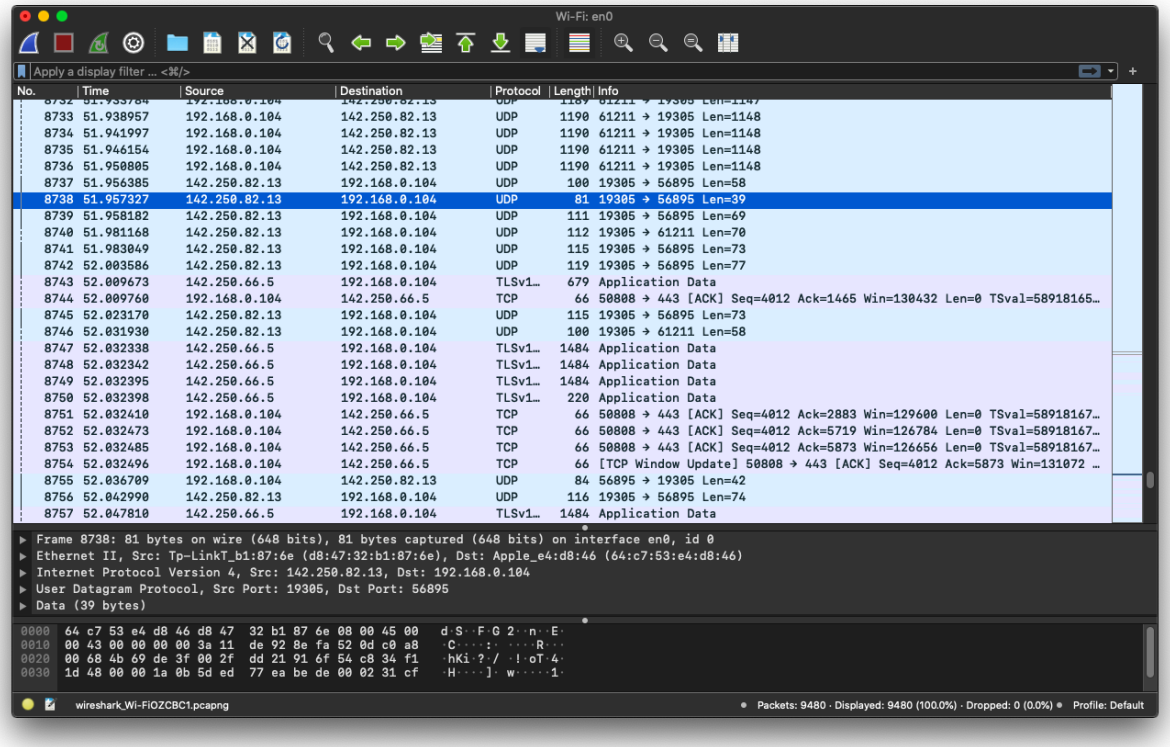
1. Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as

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.

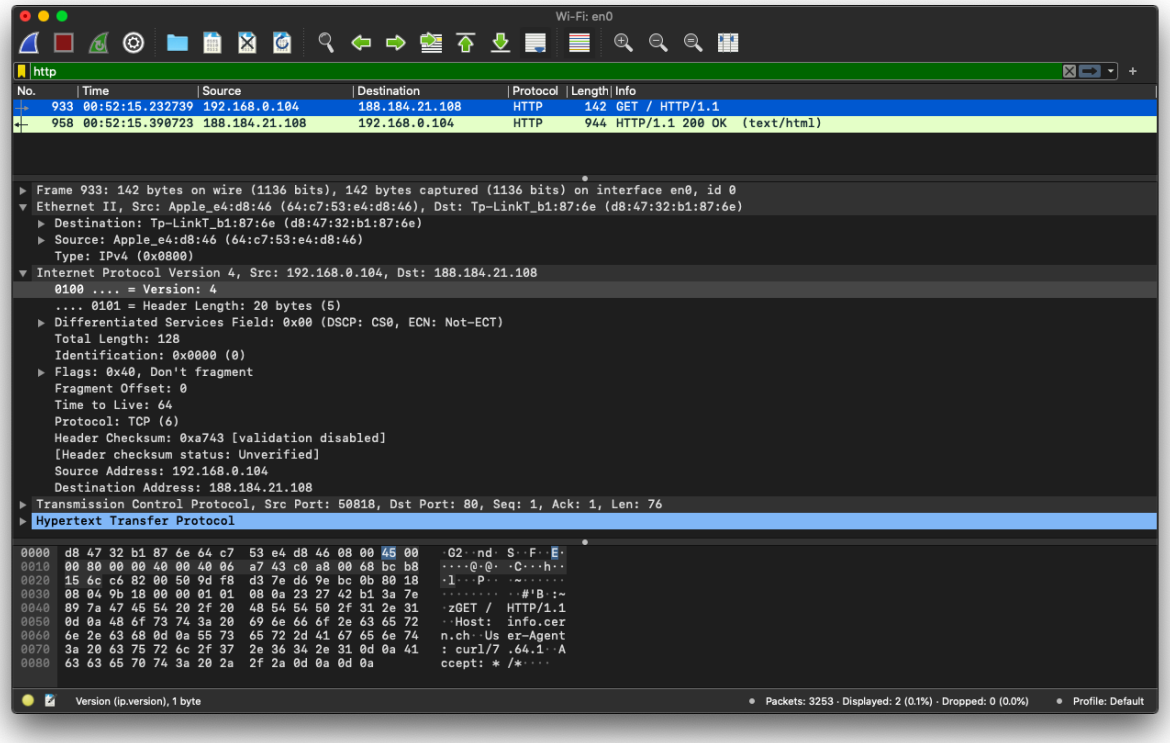




2. Generate some web traffic and
   a. find the list of the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.



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.)

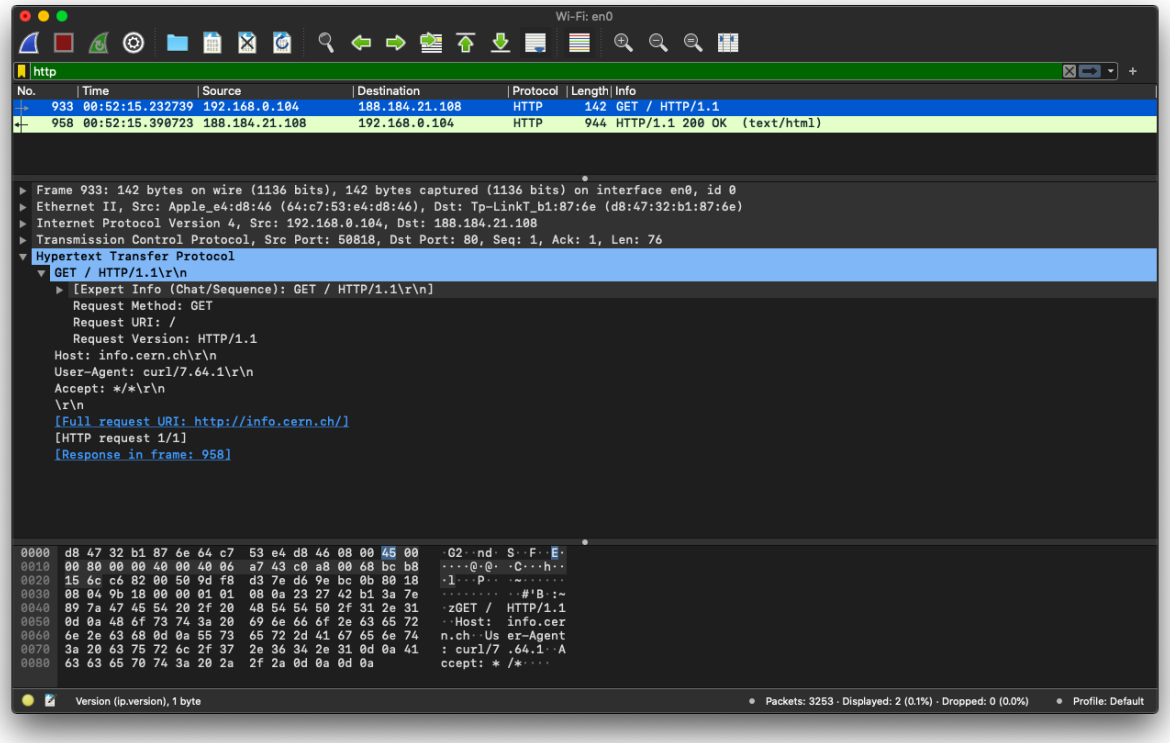


HTTP GET message sent at 00:52:15.232739 and HTTP OK reply was received at 00:52:15.390723 . Delay = 00:52:15.390723 - 00:52:15.232739 = 0.157984 seconds

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

The IP address of the website is 188.184.21.108 and that of my computer is 192.168.0.104.

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.

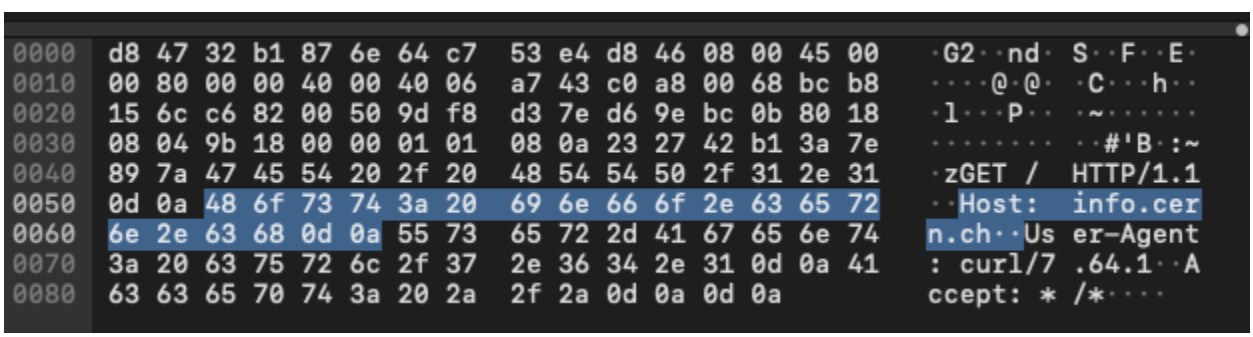


e. Find out the value of the Host from the Packet Details Panel, within the GET command.

Host name - info.cern.ch\r\n

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

HEX ASCII

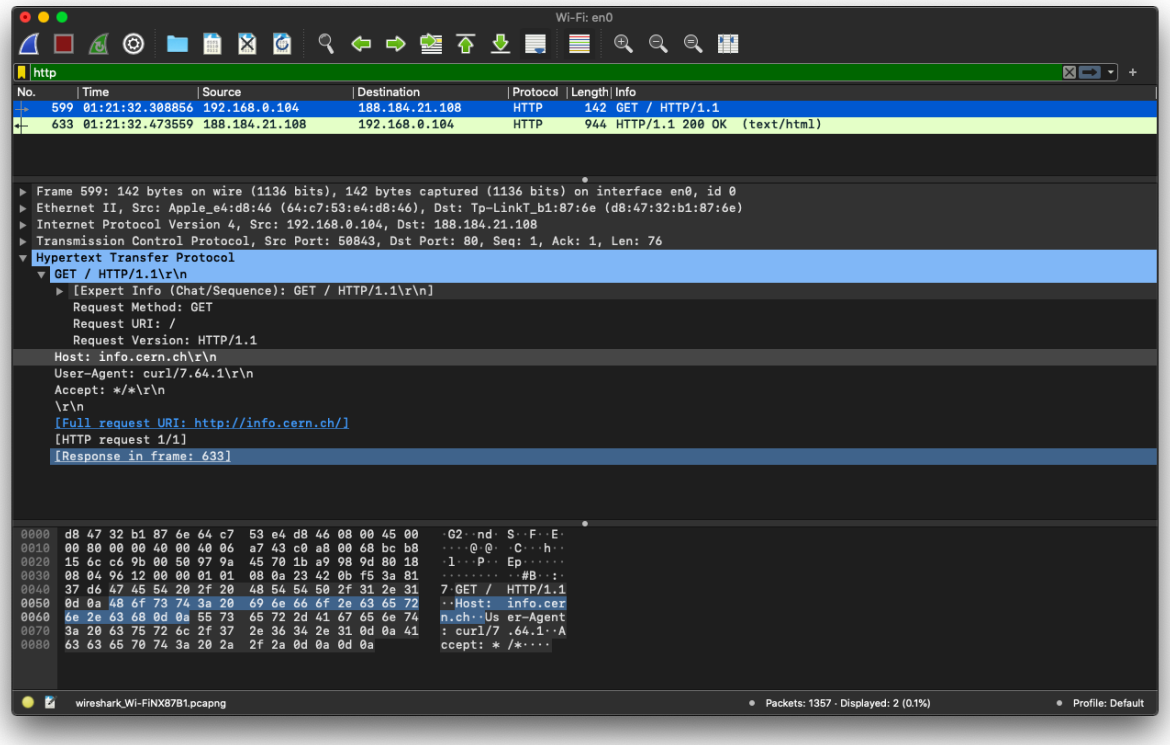


4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.

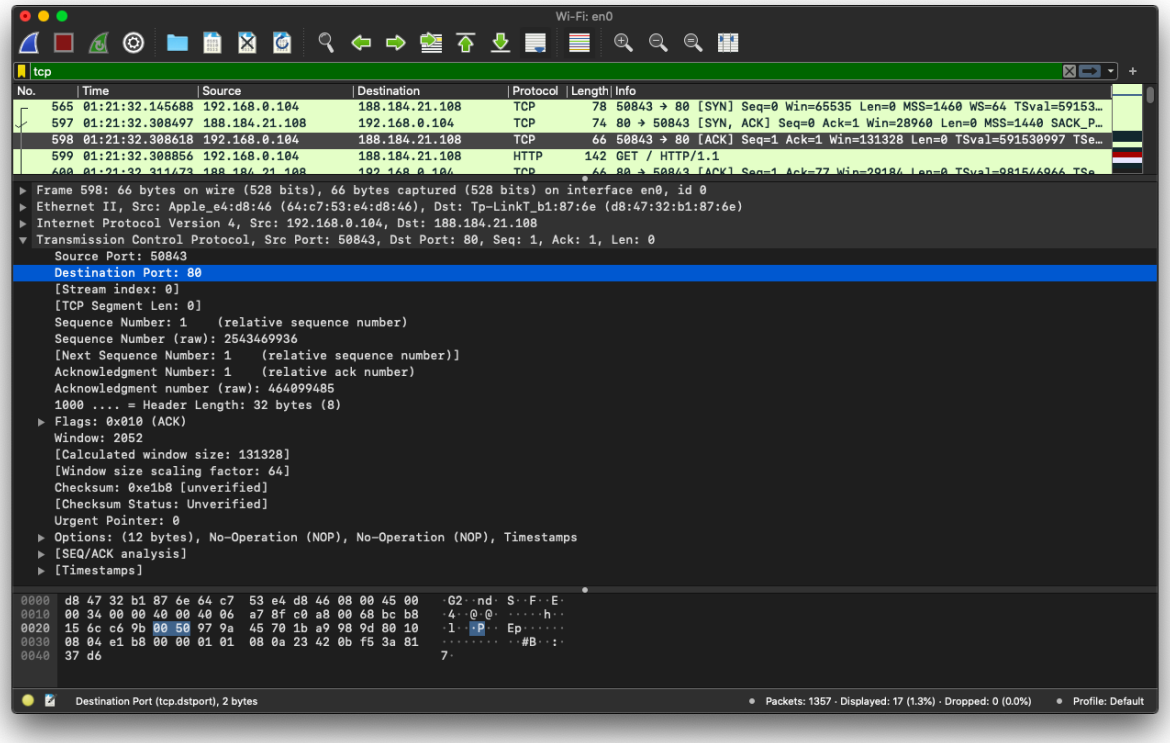
First 4 bytes are 48 6f 73 74

5. 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.

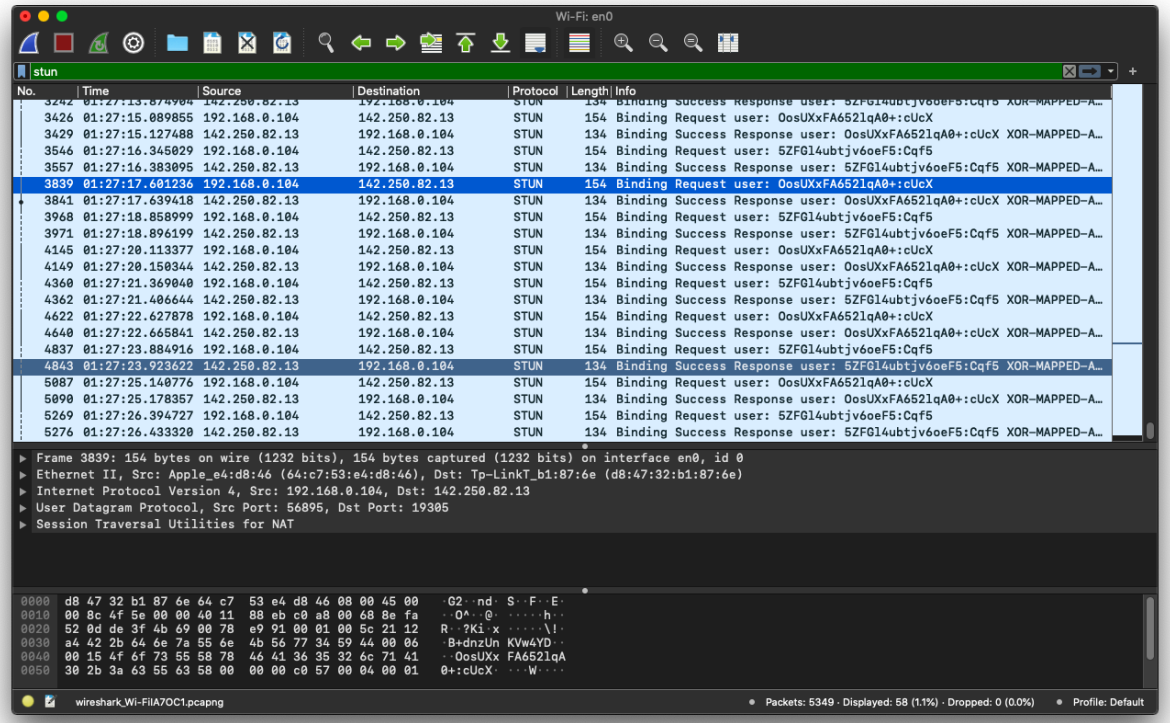
HTTP:



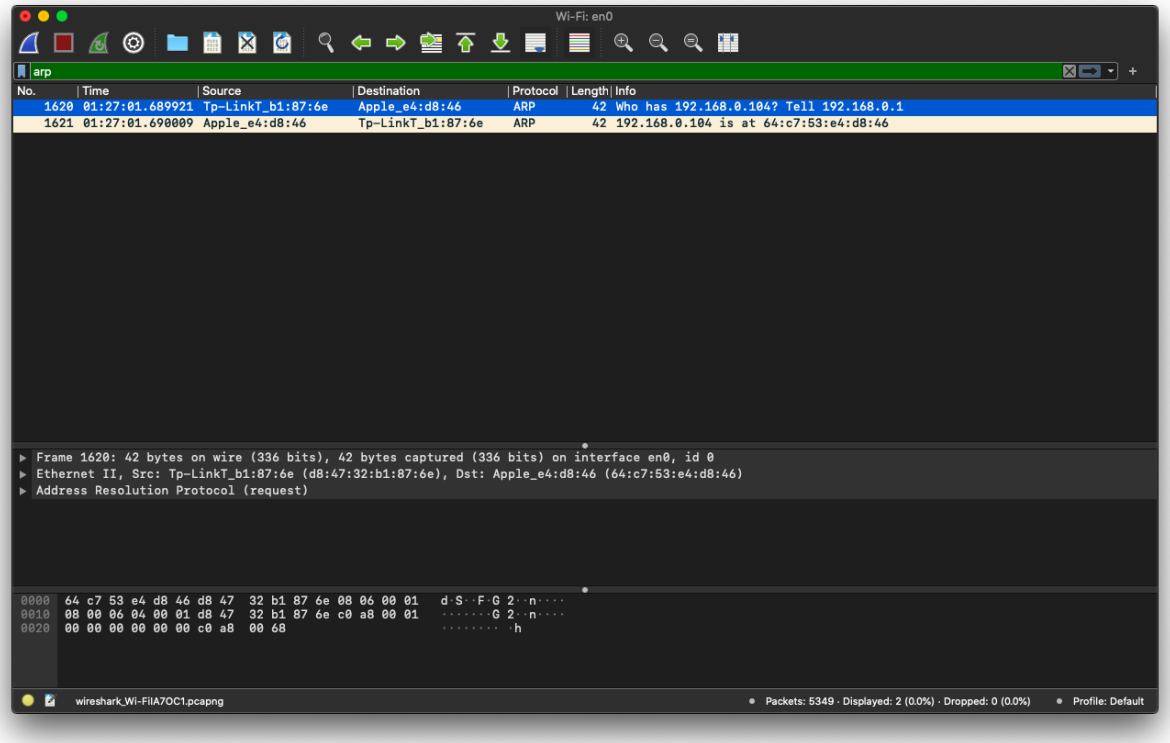
TCP:


Wi-Fi: en0
tcp
No. Time Source Destination Protocol Length Info
565 01:21:32.145688 192.168.0.104 188.184.21.108 TCP 78 50843 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=59153…
597 01:21:32.308497 188.184.21.108 192.168.0.104 TCP 74 80 → 50843 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_P…
598 01:21:32.308618 192.168.0.104 188.184.21.108 TCP 66 50843 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=591530997 TSe…
599 01:21:32.308856 192.168.0.104 188.184.21.108 HTTP 142 GET / HTTP/1.1
Frame 598: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
Ethernet II, Src: Apple_e4:d8:46 (64:c7:53:e4:d8:46), Dst: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
Transmission Control Protocol, Src Port: 50843, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 50843
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2543469936
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 464099485
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 2052
[Calculated window size: 131328]
[Window size scaling factor: 64]
Checksum: 0xe1b8 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
Destination Port (tcp.dstport), 2 bytes
Packets: 1357 · Displayed: 17 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

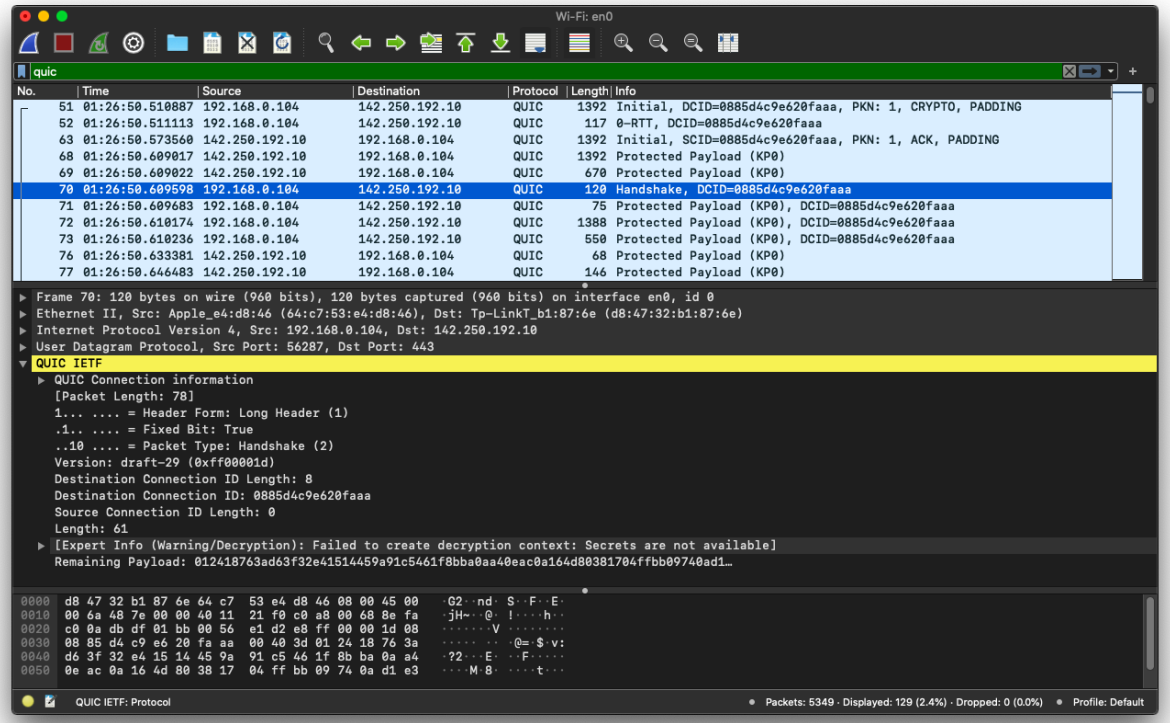
STUN:


Wi-Fi: en0
stun
No. Time Source Destination Protocol Length Info
3426 01:27:15.089855 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: OosUXxFA6521qA0+:cUcX
3429 01:27:15.127488 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: OosUXxFA6521qA0+:cUcX XOR-MAPPED-A…
3546 01:27:16.345029 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: 5ZFGl4ubtjv6oeF5:Cqf5
3557 01:27:16.383095 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: 5ZFGl4ubtjv6oeF5:Cqf5 XOR-MAPPED-A…
3839 01:27:17.601236 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: OosUXxFA6521qA0+:cUcX
3841 01:27:17.639418 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: OosUXxFA6521qA0+:cUcX XOR-MAPPED-A…
3968 01:27:18.858999 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: 5ZFGl4ubtjv6oeF5:Cqf5
3971 01:27:18.896199 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: 5ZFGl4ubtjv6oeF5:Cqf5 XOR-MAPPED-A…
4145 01:27:20.113377 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: OosUXxFA6521qA0+:cUcX
4149 01:27:20.150344 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: OosUXxFA6521qA0+:cUcX XOR-MAPPED-A…
4360 01:27:21.369040 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: 5ZFGl4ubtjv6oeF5:Cqf5
4362 01:27:21.406644 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: 5ZFGl4ubtjv6oeF5:Cqf5 XOR-MAPPED-A…
4622 01:27:22.627878 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: OosUXxFA6521qA0+:cUcX
4640 01:27:22.665841 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: OosUXxFA6521qA0+:cUcX XOR-MAPPED-A…
4837 01:27:23.884916 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: 5ZFGl4ubtjv6oeF5:Cqf5
4843 01:27:23.923622 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: 5ZFGl4ubtjv6oeF5:Cqf5 XOR-MAPPED-A…
5087 01:27:25.140776 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: OosUXxFA6521qA0+:cUcX
5090 01:27:25.178357 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: OosUXxFA6521qA0+:cUcX XOR-MAPPED-A…
5269 01:27:26.394727 192.168.0.104 142.250.82.13 STUN 154 Binding Request user: 5ZFGl4ubtjv6oeF5:Cqf5
5276 01:27:26.433320 142.250.82.13 192.168.0.104 STUN 134 Binding Success Response user: 5ZFGl4ubtjv6oeF5:Cqf5 XOR-MAPPED-A…
Frame 3839: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface en0, id 0
Ethernet II, Src: Apple_e4:d8:46 (64:c7:53:e4:d8:46), Dst: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 142.250.82.13
User Datagram Protocol, Src Port: 56895, Dst Port: 19305
Session Traversal Utilities for NAT
wireshark_Wi-FiIA7OC1.pcapng
Packets: 5349 · Displayed: 58 (1.1%) · Dropped: 0 (0.0%)
Profile: Default

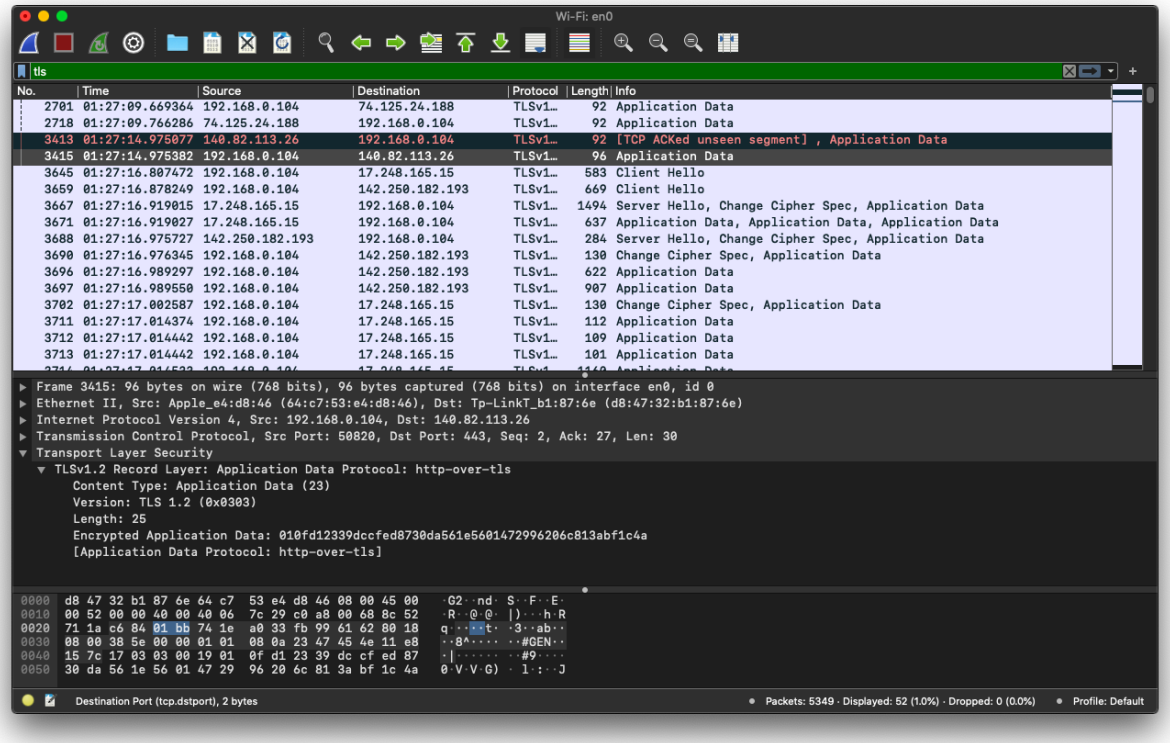
ARP:


Wi-Fi: en0
arp
No. Time Source Destination Protocol Length Info
1620 01:27:01.689921 Tp-LinkT_b1:87:6e Apple_e4:d8:46 ARP 42 Who has 192.168.0.104? Tell 192.168.0.1
1621 01:27:01.690009 Apple_e4:d8:46 Tp-LinkT_b1:87:6e ARP 42 192.168.0.104 is at 64:c7:53:e4:d8:46
Frame 1620: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e), Dst: Apple_e4:d8:46 (64:c7:53:e4:d8:46)
Address Resolution Protocol (request)
0000 64 c7 53 e4 d8 46 d8 47 32 b1 87 6e 08 06 00 01
0010 08 00 06 04 00 01 d8 47 32 b1 87 6e c0 a8 00 01
0020 00 00 00 00 00 00 c0 a8 00 68
wireshark_Wi-FiIA7OC1.pcapng
Packets: 5349 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

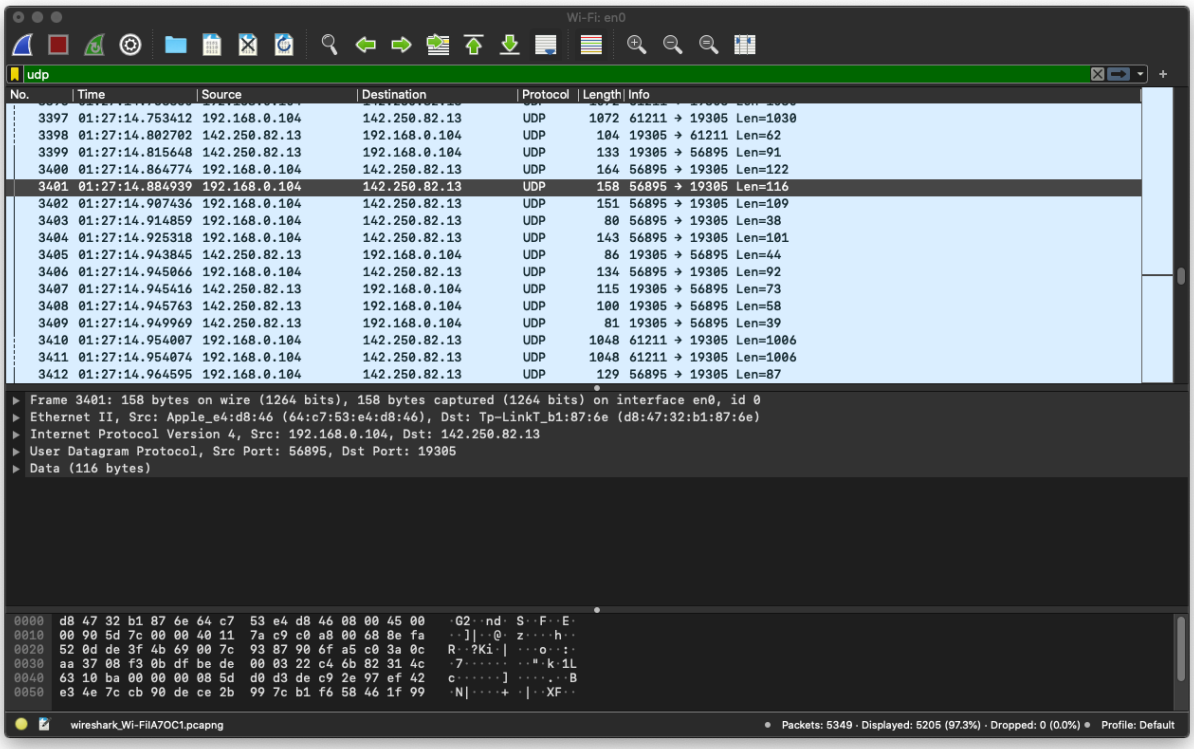
QUIC:

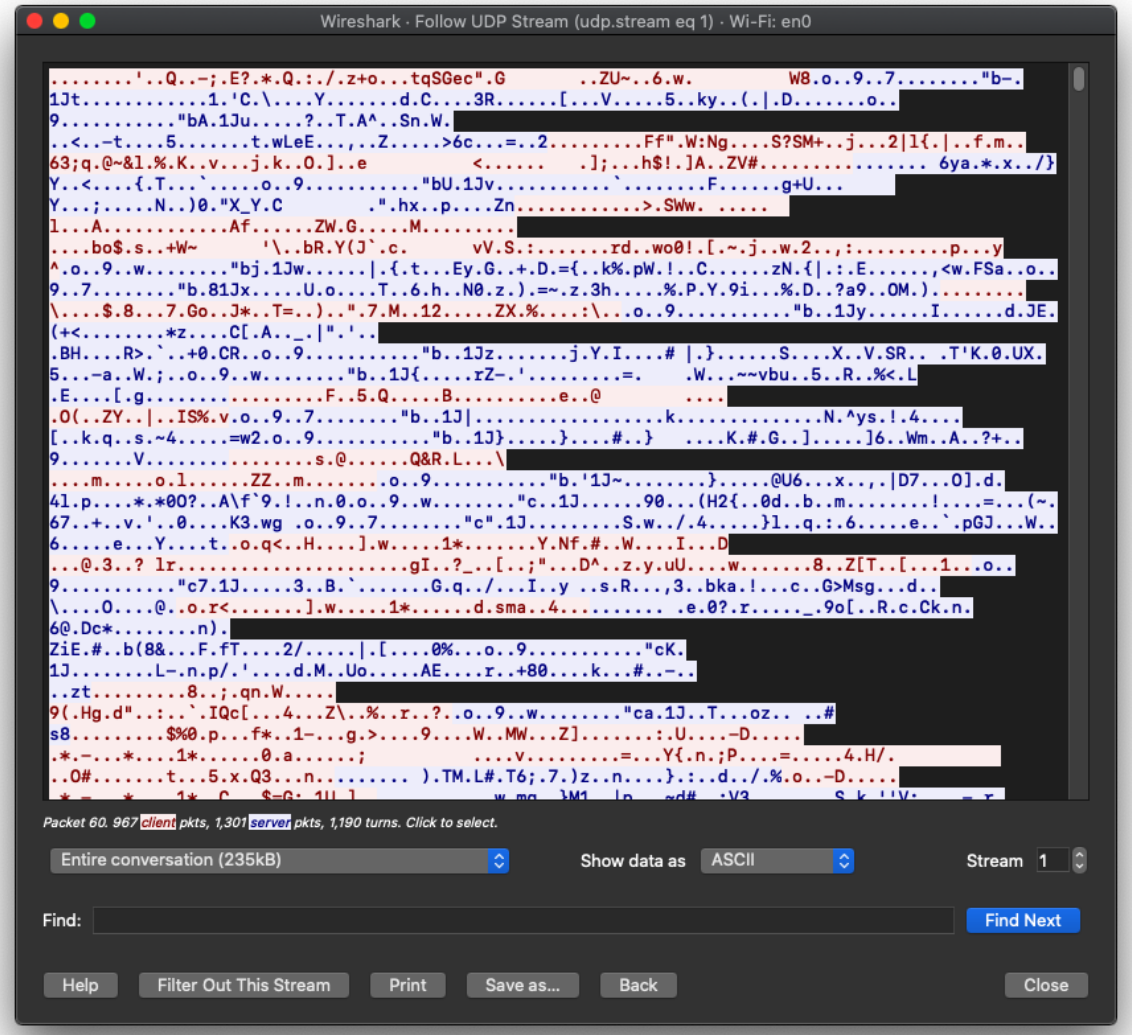

Wi-Fi: en0
quic
No. Time Source Destination Protocol Length Info
51 01:26:50.510887 192.168.0.104 142.250.192.10 QUIC 1392 Initial, DCID=0885d4c9e620faaa, PKN: 1, CRYPTO, PADDING
52 01:26:50.511113 192.168.0.104 142.250.192.10 QUIC 117 0-RTT, DCID=0885d4c9e620faaa
63 01:26:50.573560 142.250.192.10 192.168.0.104 QUIC 1392 Initial, SCID=0885d4c9e620faaa, PKN: 1, ACK, PADDING
68 01:26:50.609017 142.250.192.10 192.168.0.104 QUIC 1392 Protected Payload (KP0)
69 01:26:50.609022 142.250.192.10 192.168.0.104 QUIC 670 Protected Payload (KP0)
70 01:26:50.609598 192.168.0.104 142.250.192.10 QUIC 120 Handshake, DCID=0885d4c9e620faaa
71 01:26:50.609683 192.168.0.104 142.250.192.10 QUIC 75 Protected Payload (KP0), DCID=0885d4c9e620faaa
72 01:26:50.610174 192.168.0.104 142.250.192.10 QUIC 1388 Protected Payload (KP0), DCID=0885d4c9e620faaa
73 01:26:50.610236 192.168.0.104 142.250.192.10 QUIC 550 Protected Payload (KP0), DCID=0885d4c9e620faaa
76 01:26:50.633381 142.250.192.10 192.168.0.104 QUIC 68 Protected Payload (KP0)
77 01:26:50.646483 142.250.192.10 192.168.0.104 QUIC 146 Protected Payload (KP0)
Frame 70: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface en0, id 0
Ethernet II, Src: Apple_e4:d8:46 (64:c7:53:e4:d8:46), Dst: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 142.250.192.10
User Datagram Protocol, Src Port: 56287, Dst Port: 443
QUIC IETF
QUIC Connection information
[Packet Length: 78]
1... .... = Header Form: Long Header (1)
.1.. .... = Fixed Bit: True
..10 .... = Packet Type: Handshake (2)
Version: draft-29 (0xff00001d)
Destination Connection ID Length: 8
Destination Connection ID: 0885d4c9e620faaa
Source Connection ID Length: 0
Length: 61
[Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
Remaining Payload: 012418763ad63f32e41514459a91c5461f8bba0aa40eac0a164d80381704ffbb09740ad1…
0000 d8 47 32 b1 87 6e 64 c7 53 e4 d8 46 08 00 45 00
0010 00 6a 48 7e 00 00 40 11 21 f0 c0 a8 00 68 8e fa
0020 c0 0a db df 01 bb 00 56 e1 d2 e8 ff 00 00 1d 08
0030 08 85 d4 c9 e6 20 fa aa 00 40 3d 01 24 18 76 3a
0040 d6 3f 32 e4 15 14 45 9a 91 c5 46 1f 8b ba 0a a4
0050 0e ac 0a 16 4d 80 38 17 04 ff bb 09 74 0a d1 e3
QUIC IETF: Protocol
Packets: 5349 · Displayed: 129 (2.4%) · Dropped: 0 (0.0%)
Profile: Default

TLS:

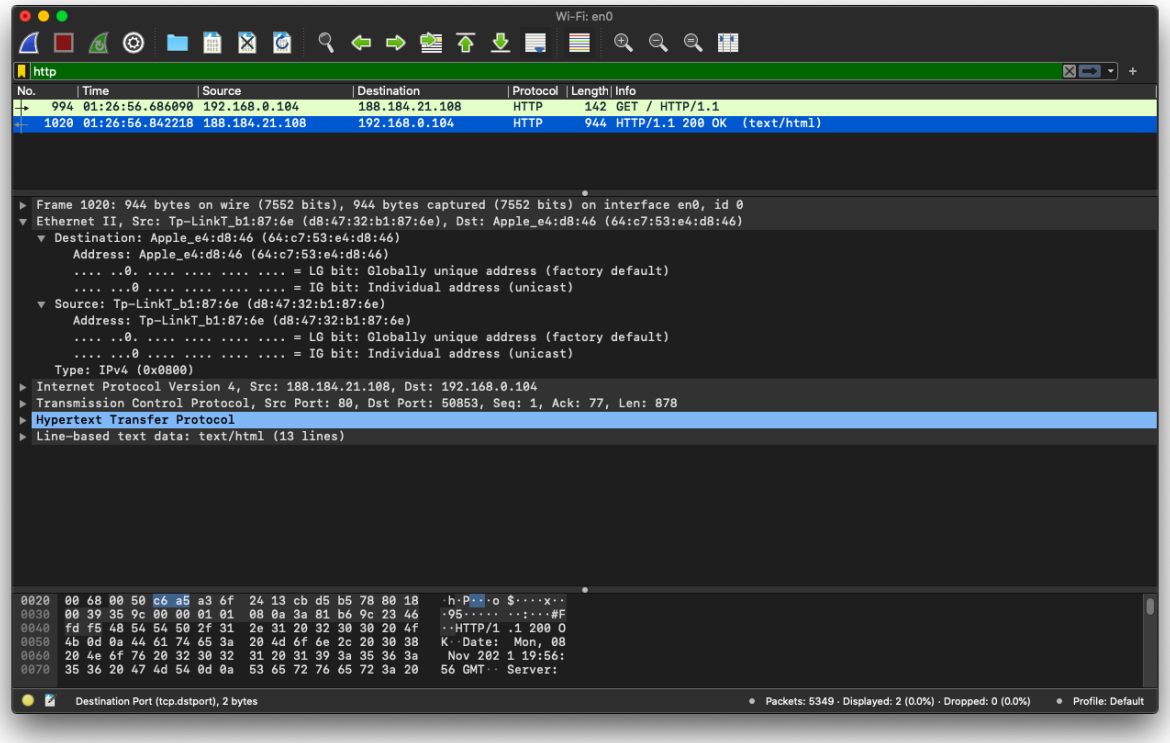

Wi-Fi: en0
tls
No. Time Source Destination Protocol Length Info
2701 01:27:09.669364 192.168.0.104 74.125.24.188 TLSv1… 92 Application Data
2718 01:27:09.766286 74.125.24.188 192.168.0.104 TLSv1… 92 Application Data
3413 01:27:14.975077 140.82.113.26 192.168.0.104 TLSv1… 92 [TCP ACKed unseen segment] , Application Data
3415 01:27:14.975382 192.168.0.104 140.82.113.26 TLSv1… 96 Application Data
3645 01:27:16.807472 192.168.0.104 17.248.165.15 TLSv1… 583 Client Hello
3659 01:27:16.878249 192.168.0.104 142.250.182.193 TLSv1… 669 Client Hello
3667 01:27:16.919015 17.248.165.15 192.168.0.104 TLSv1… 1494 Server Hello, Change Cipher Spec, Application Data
3671 01:27:16.919027 17.248.165.15 192.168.0.104 TLSv1… 637 Application Data, Application Data, Application Data
3688 01:27:16.975727 142.250.182.193 192.168.0.104 TLSv1… 284 Server Hello, Change Cipher Spec, Application Data
3690 01:27:16.976345 192.168.0.104 142.250.182.193 TLSv1… 130 Change Cipher Spec, Application Data
3696 01:27:16.989297 192.168.0.104 142.250.182.193 TLSv1… 622 Application Data
3697 01:27:16.989550 192.168.0.104 142.250.182.193 TLSv1… 907 Application Data
3702 01:27:17.002587 192.168.0.104 17.248.165.15 TLSv1… 130 Change Cipher Spec, Application Data
3711 01:27:17.014374 192.168.0.104 17.248.165.15 TLSv1… 112 Application Data
3712 01:27:17.014442 192.168.0.104 17.248.165.15 TLSv1… 109 Application Data
3713 01:27:17.014442 192.168.0.104 17.248.165.15 TLSv1… 101 Application Data
Frame 3415: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface en0, id 0
Ethernet II, Src: Apple_e4:d8:46 (64:c7:53:e4:d8:46), Dst: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 140.82.113.26
Transmission Control Protocol, Src Port: 50820, Dst Port: 443, Seq: 2, Ack: 27, Len: 30
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 25
Encrypted Application Data: 010fd12339dccfed8730da561e5601472996206c813abf1c4a
[Application Data Protocol: http-over-tls]
0000 d8 47 32 b1 87 6e 64 c7 53 e4 d8 46 08 00 45 00
0010 00 52 00 00 40 00 40 06 7c 29 c0 a8 00 68 8c 52
0020 71 1a c6 84 01 bb 74 1e a0 33 fb 99 61 62 80 18
0030 08 00 38 5e 00 00 01 01 08 0a 23 47 45 4e 11 e8
0040 15 7c 17 03 03 00 19 01 0f d1 23 39 dc cf ed 87
0050 30 da 56 1e 56 01 47 29 96 20 6c 81 3a bf 1c 4a
Destination Port (tcp.dstport), 2 bytes
Packets: 5349 · Displayed: 52 (1.0%) · Dropped: 0 (0.0%)
Profile: Default

UDP:


Wi-Fi: en0
udp
No. Time Source Destination Protocol Length Info
3397 01:27:14.753412 192.168.0.104 142.250.82.13 UDP 1072 61211 → 19305 Len=1030
3398 01:27:14.802702 142.250.82.13 192.168.0.104 UDP 104 19305 → 61211 Len=62
3399 01:27:14.815648 142.250.82.13 192.168.0.104 UDP 133 19305 → 56895 Len=91
3400 01:27:14.864774 192.168.0.104 142.250.82.13 UDP 164 56895 → 19305 Len=122
3401 01:27:14.884939 192.168.0.104 142.250.82.13 UDP 158 56895 → 19305 Len=116
3402 01:27:14.907436 192.168.0.104 142.250.82.13 UDP 151 56895 → 19305 Len=109
3403 01:27:14.914859 192.168.0.104 142.250.82.13 UDP 80 56895 → 19305 Len=38
3404 01:27:14.925318 192.168.0.104 142.250.82.13 UDP 143 56895 → 19305 Len=101
3405 01:27:14.943845 142.250.82.13 192.168.0.104 UDP 86 19305 → 56895 Len=44
3406 01:27:14.945066 192.168.0.104 142.250.82.13 UDP 134 56895 → 19305 Len=92
3407 01:27:14.945416 142.250.82.13 192.168.0.104 UDP 115 19305 → 56895 Len=73
3408 01:27:14.945763 142.250.82.13 192.168.0.104 UDP 100 19305 → 56895 Len=58
3409 01:27:14.949969 142.250.82.13 192.168.0.104 UDP 81 19305 → 56895 Len=39
3410 01:27:14.954007 192.168.0.104 142.250.82.13 UDP 1048 61211 → 19305 Len=1006
3411 01:27:14.954074 192.168.0.104 142.250.82.13 UDP 1048 61211 → 19305 Len=1006
3412 01:27:14.964595 192.168.0.104 142.250.82.13 UDP 129 56895 → 19305 Len=87
Frame 3401: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface en0, id 0
Ethernet II, Src: Apple_e4:d8:46 (64:c7:53:e4:d8:46), Dst: Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 142.250.82.13
User Datagram Protocol, Src Port: 56895, Dst Port: 19305
Data (116 bytes)
0000 d8 47 32 b1 87 6e 64 c7 53 e4 d8 46 08 00 45 00
0010 00 90 5d 7c 00 00 40 11 7a c9 c0 a8 00 68 8e fa
0020 52 0d de 3f 4b 69 00 7c 93 87 90 6f a5 c0 3a 0c
0030 aa 37 08 f3 0b df be de 00 03 22 c4 6b 82 31 4c
0040 63 10 ba 00 00 00 08 5d d0 d3 de c9 2e 97 ef 42
0050 e3 4e 7c cb 90 de ce 2b 99 7c b1 f6 58 46 1f 99
wireshark_Wi-FilA7OC1.pcapng
Packets: 5349 · Displayed: 5205 (97.3%) · Dropped: 0 (0.0%)
Profile: Default



6. 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.



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

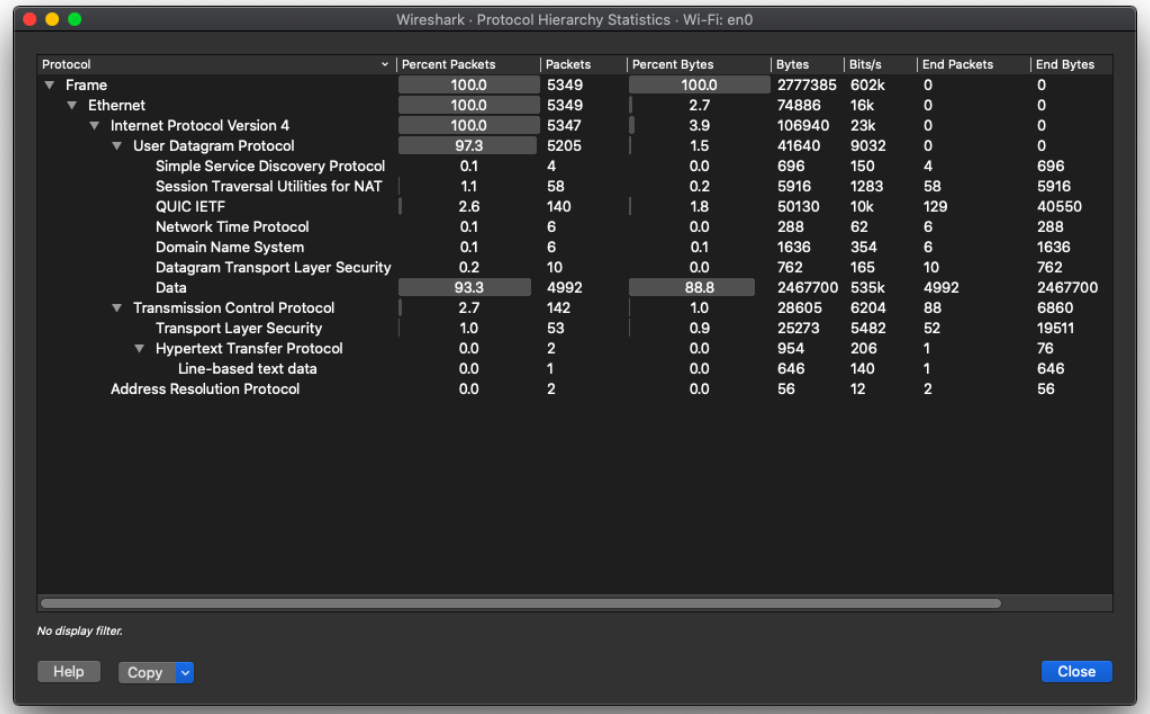
Manufacturer of my PC's NIC - Apple_e4:d8:46 (64:c7:53:e4:d8:46)

Manufacturer of server's NIC - Tp-LinkT_b1:87:6e (d8:47:32:b1:87:6e)

8. What are the Hex values (shown in the raw bytes panel) of the two NICS Manufacturers OUIs?

HEX value of my PC's NIC - 64:c7:53:e4:d8:46, server's NIC - d8:47:32:b1:87:6e

9. Find the following statistics:



Wireshark · Protocol Hierarchy Statistics · Wi-Fi: en0

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	5349	100.0	2777385	602k	0	0
Ethernet	100.0	5349	2.7	74886	16k	0	0
Internet Protocol Version 4	100.0	5347	3.9	106940	23k	0	0
User Datagram Protocol	97.3	5205	1.5	41640	9032	0	0
Simple Service Discovery Protocol	0.1	4	0.0	696	150	4	696
Session Traversal Utilities for NAT	1.1	58	0.2	5916	1283	58	5916
QUIC IETF	2.6	140	1.8	50130	10k	129	40550
Network Time Protocol	0.1	6	0.0	288	62	6	288
Domain Name System	0.1	6	0.1	1636	354	6	1636
Datagram Transport Layer Security	0.2	10	0.0	762	165	10	762
Data	93.3	4992	88.8	2467700	535k	4992	2467700
Transmission Control Protocol	2.7	142	1.0	28605	6204	88	6860
Transport Layer Security	1.0	53	0.9	25273	5482	52	19511
Hypertext Transfer Protocol	0.0	2	0.0	954	206	1	76
Line-based text data	0.0	1	0.0	646	140	1	646
Address Resolution Protocol	0.0	2	0.0	56	12	2	56

No display filter.

Help Copy Close

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

   2.7 percent of packets are TCP

   Higher level protocols using TCP -

   a) HTTPS - HyperText Transfer Protocol Secure
   b) FTP - File Transfer Protocol

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

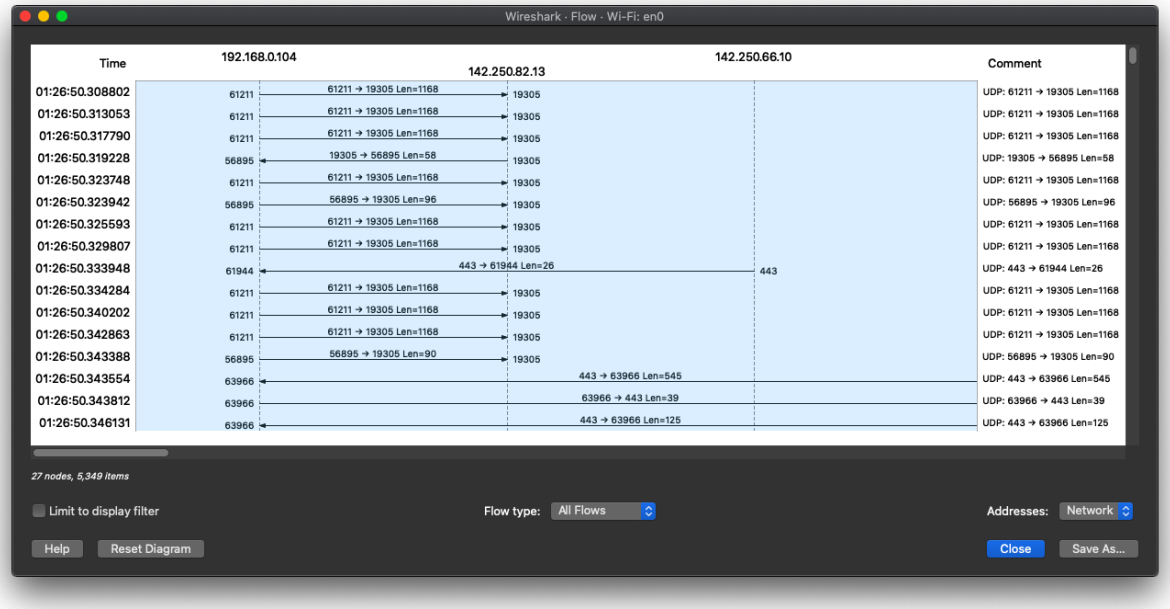
   97.3 percent of packets are UDP

   Higher level protocols using UDP :

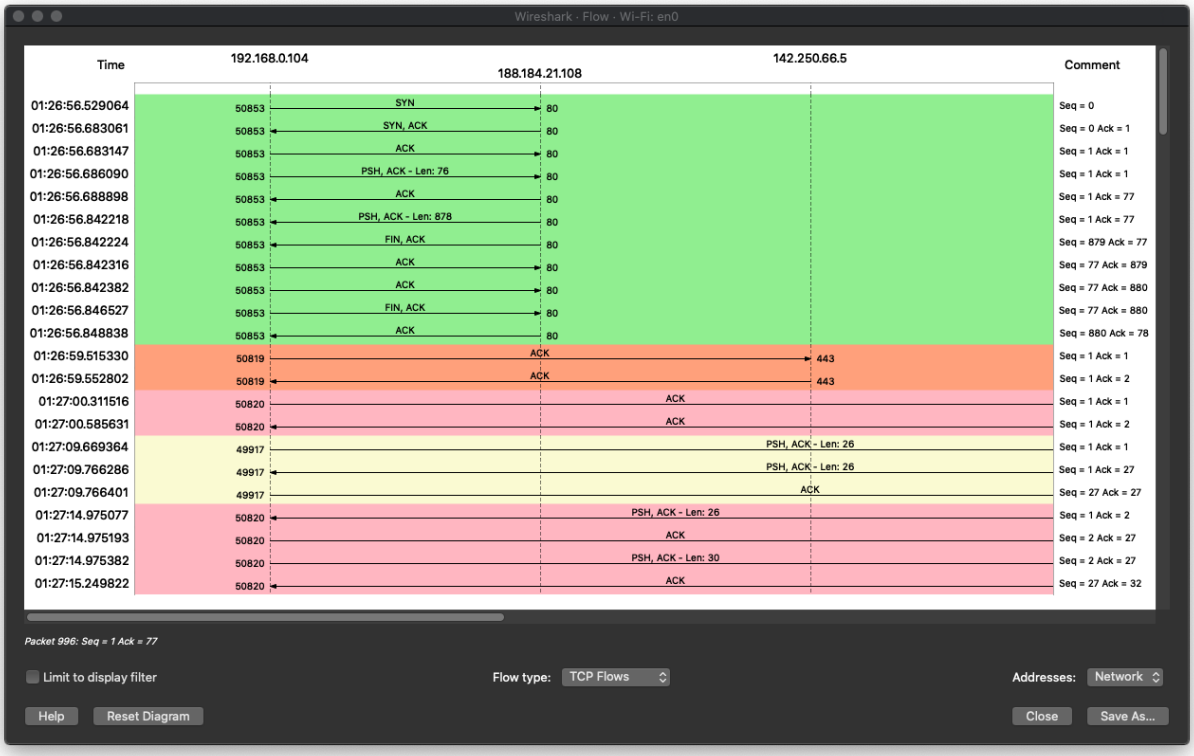
   a) SNMP - Simple Network Management Protocol
   b) RIP - Routing Information Protocol

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

Graph for general Flow and Network source -



Graph for TCP flow and network source -



COMMENTS

The assignment helps to get a real world scenario of how packets are transmitted over the network using a tool called Wireshark.