Networks Lab
Assignment 5

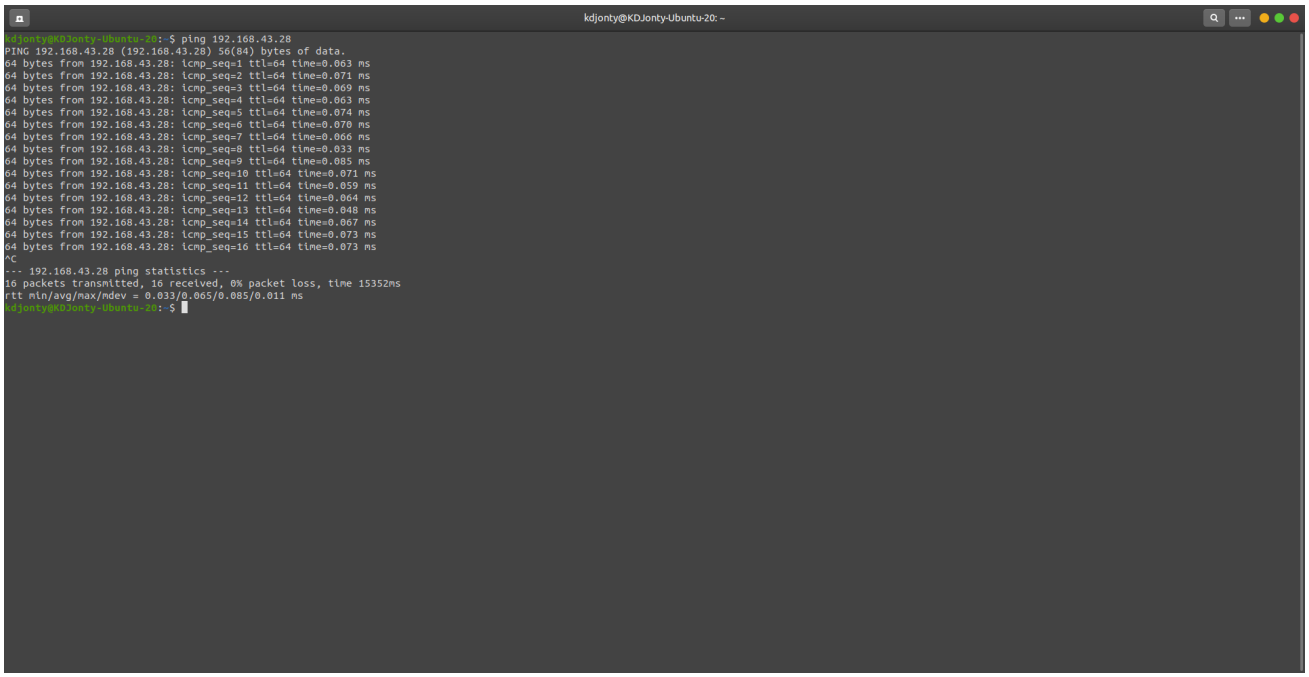
Name: Koustav Dhar Class: BCSE UG-III Group: A1 Roll: 001910501022

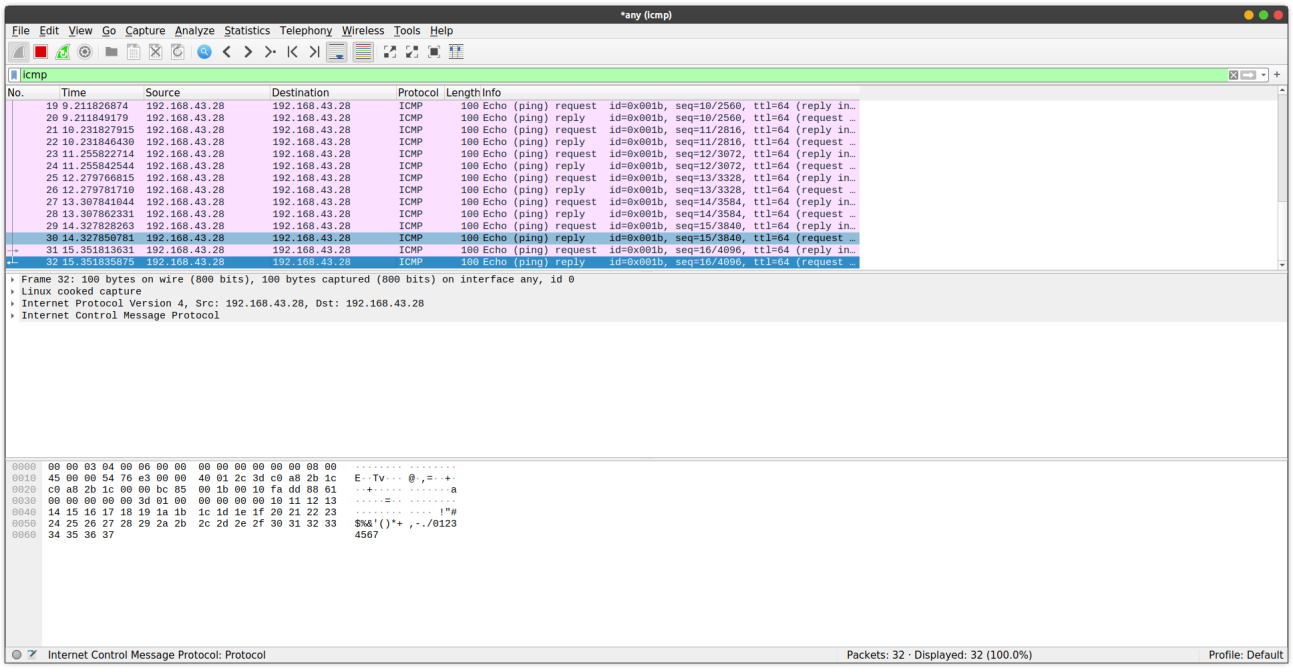
Problem Statement:

Install wireshark in the local machine and capture and analyse various packets according to the given questions.

Questions (Please take screenshots and explain)

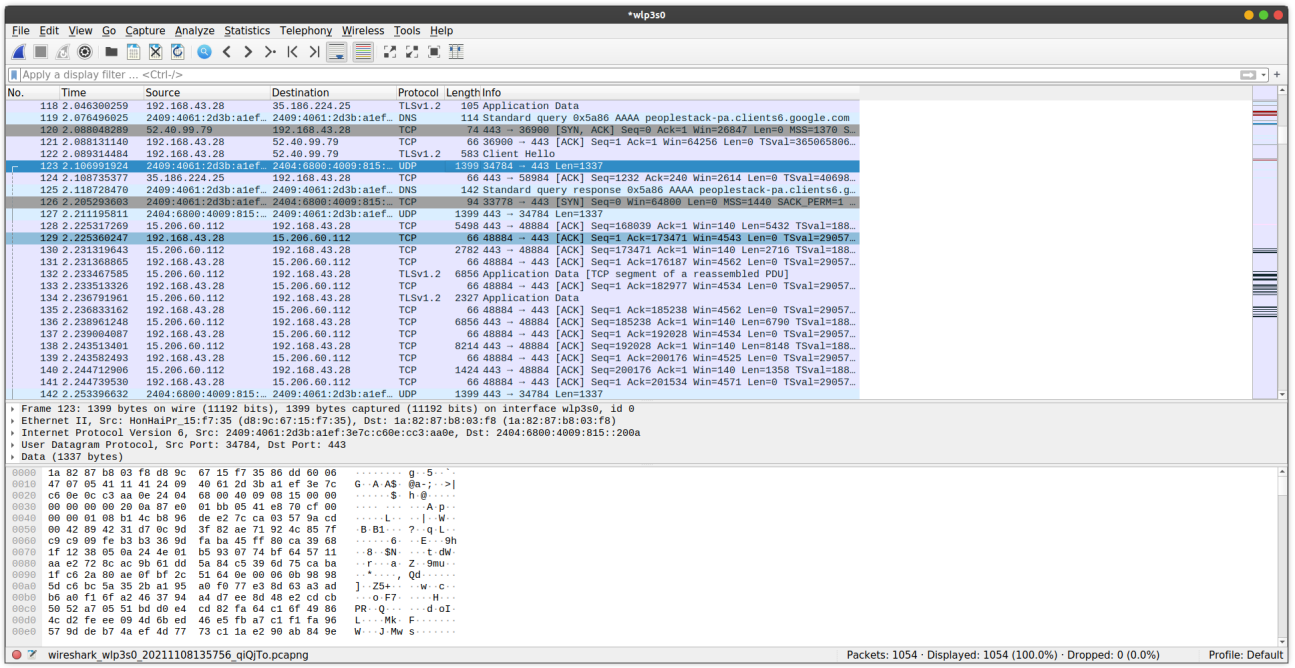
1. Generate some ICMP traffic by using the Ping command-line tool to check the connectivity of a neighboring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address and the ARP reply from the neighboring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



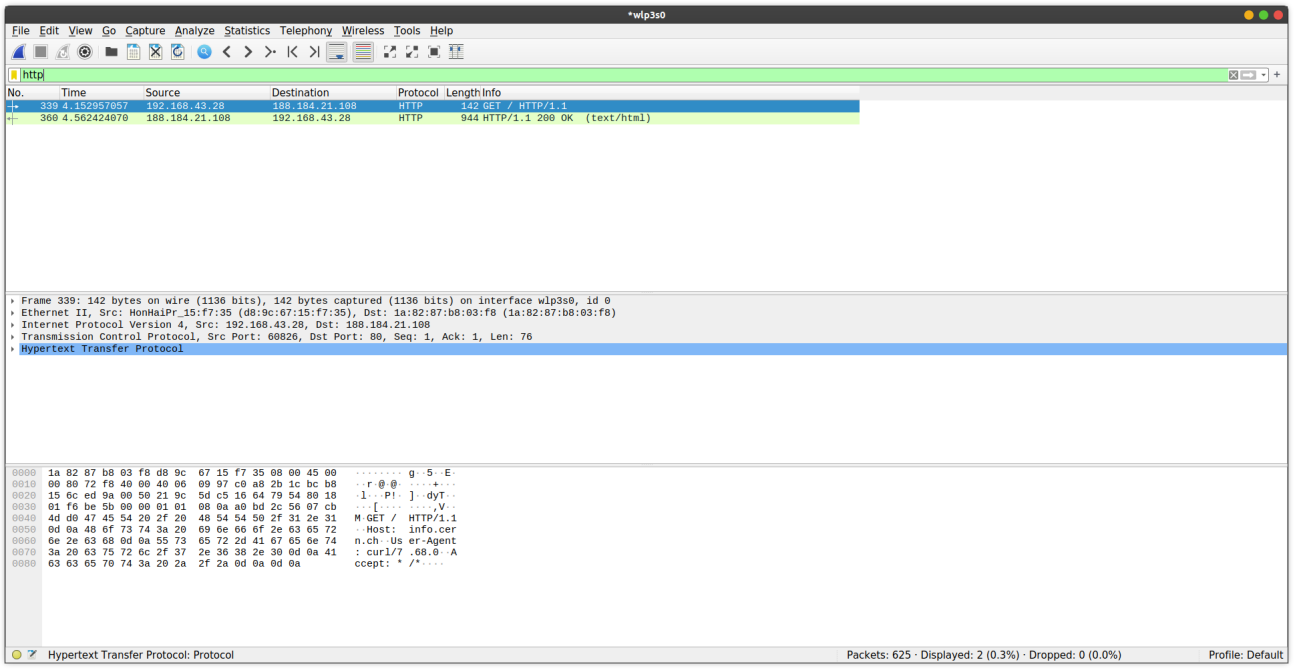


2. Generate some web traffic and

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.)



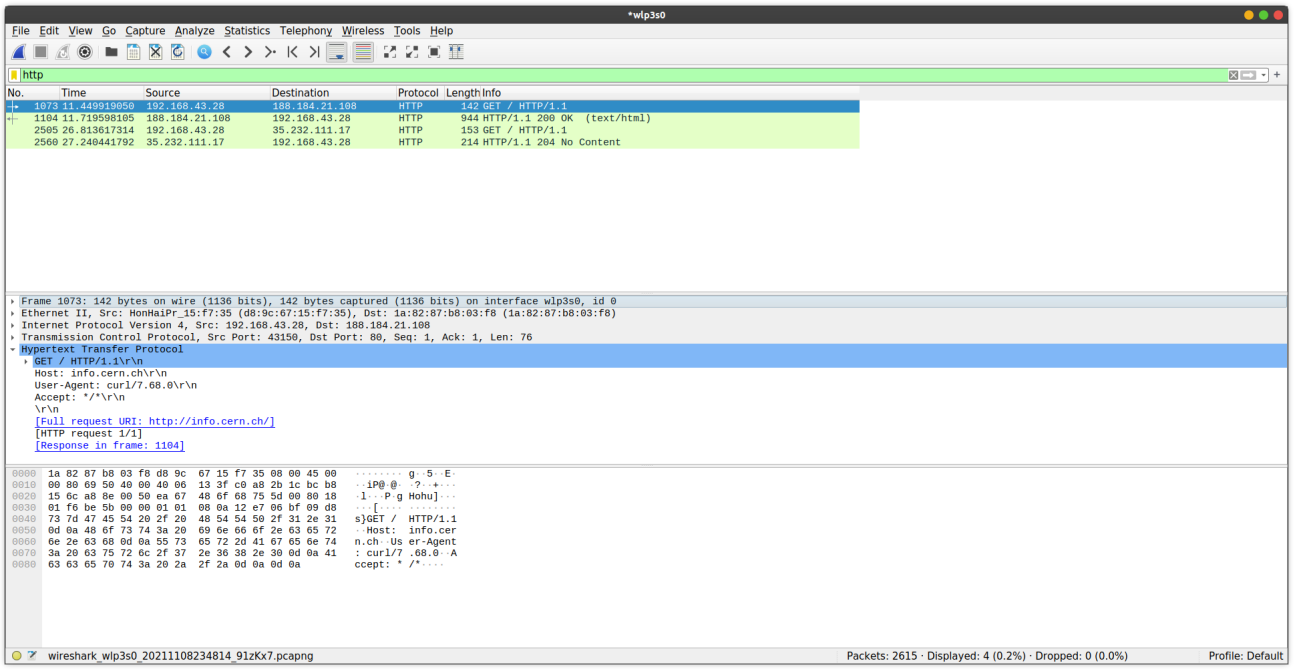
As shown in the screenshot above the GET(339) was sent at 4.152957 second and the reply OK(360) was received at 4.562424 second. Thus the delay is (4.562424-4.152957) seconds which is 409.467 milliseconds.

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 **188.184.21.108** and the

IP address of my laptop is **192.168.43.28**

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.



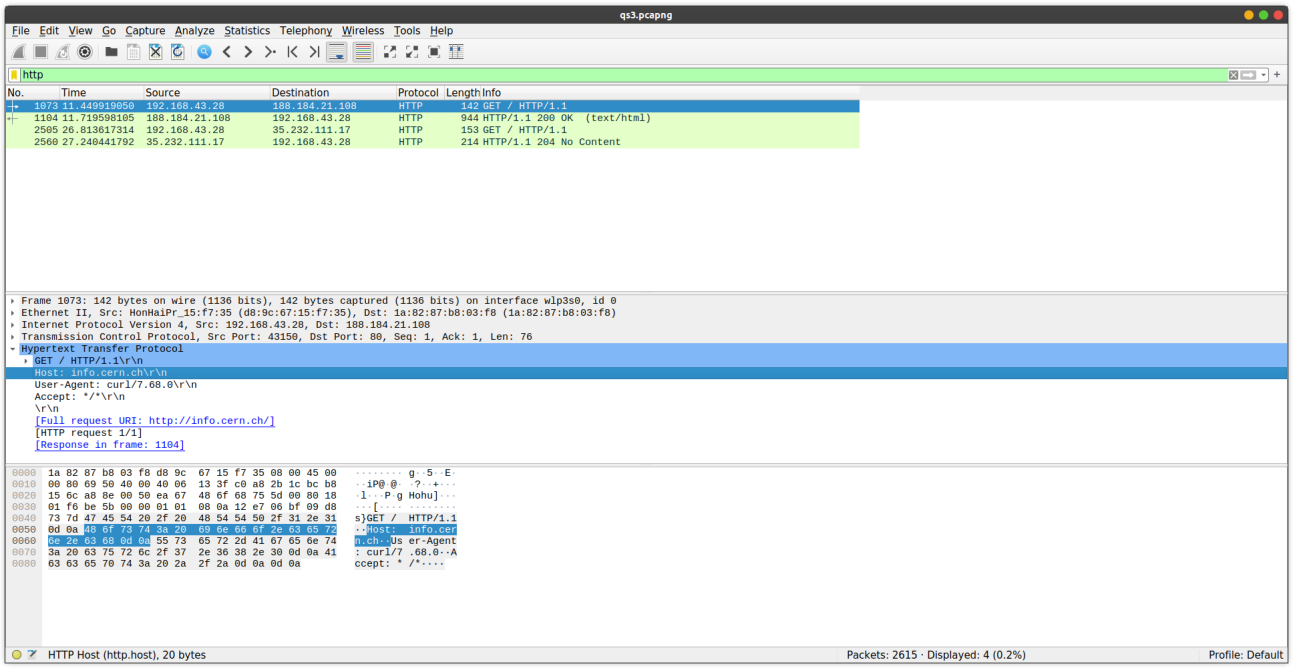
e. Find out the value of the Host from the Packet Details Panel, within the GET command.
As shown in the screenshot above, the Host is: **info.cern.ch\r\n**

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

```
0000  d8 9c 67 15 f7 35 1a 82  87 b8 03 f8 86 dd 66 03   ··g··5·· ·····f·
0010  90 21 00 75 11 3d 20 01  48 60 48 64 00 06 00 00   ·!·u·=·· H`Hd····
0020  00 00 00 00 00 5a 24 09  40 61 2d 3b a1 ef 33 23   ·····Z$· @a-;··3#
0030  7f 47 fe d0 f5 dc 4b 69  e7 7e 00 75 1b 15 91 6d   ·G····Ki ·~·u···m
0040  37 d3 3d a2 d3 8b 00 00  1a 0a 82 2a 84 2d be de   7·=····· ···*·-··
0050  00 01 10 af 00 00 d8 51  8e df 27 e1 50 9a 72 e4   ·······Q ··'·P·r·
0060  3c 6c 7e 96 7e 4b 4a 8d  76 d4 a8 c8 5d 11 4f a9   <l~·~KJ· v···]·O·
0070  84 58 68 9d 5e dc b0 a8  ce fd 18 47 45 35 69 ac   ·Xh·^··· ···GE5i·
0080  e9 03 8c 5c dd 65 ba df  cc f1 24 79 19 ca 2a 3c   ···\·e·· ··$y··*<
0090  49 2e ce cf 11 8b 93 67  f8 5f 80 15 1c b5 a2 b9   I.·····g ·_·····
00a0  01 96 a5 01 5a d4 5f b1  58 64 34                 ····Z·_· Xd4
```

The left columns are hex representations and the right ones are the ASCII values of the packet content.

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

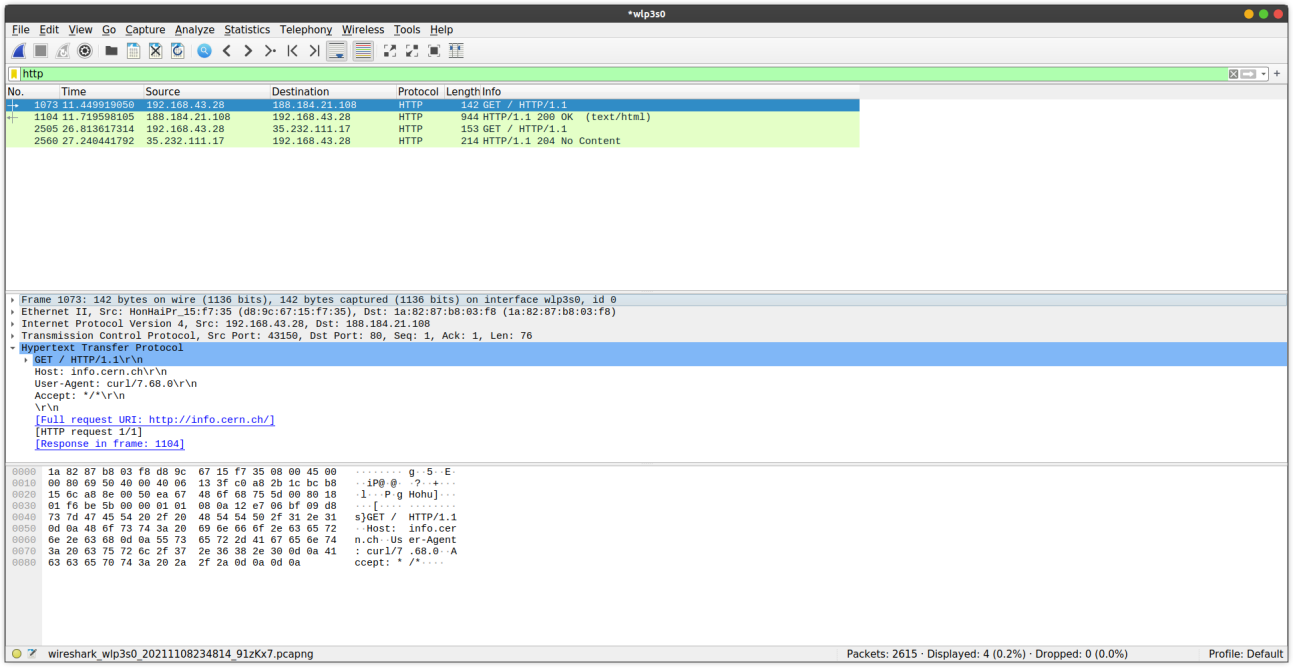


The first four bytes of the Hex value of the Host parameter from the Packet Bytes Panel are: **48 6f 73 74**

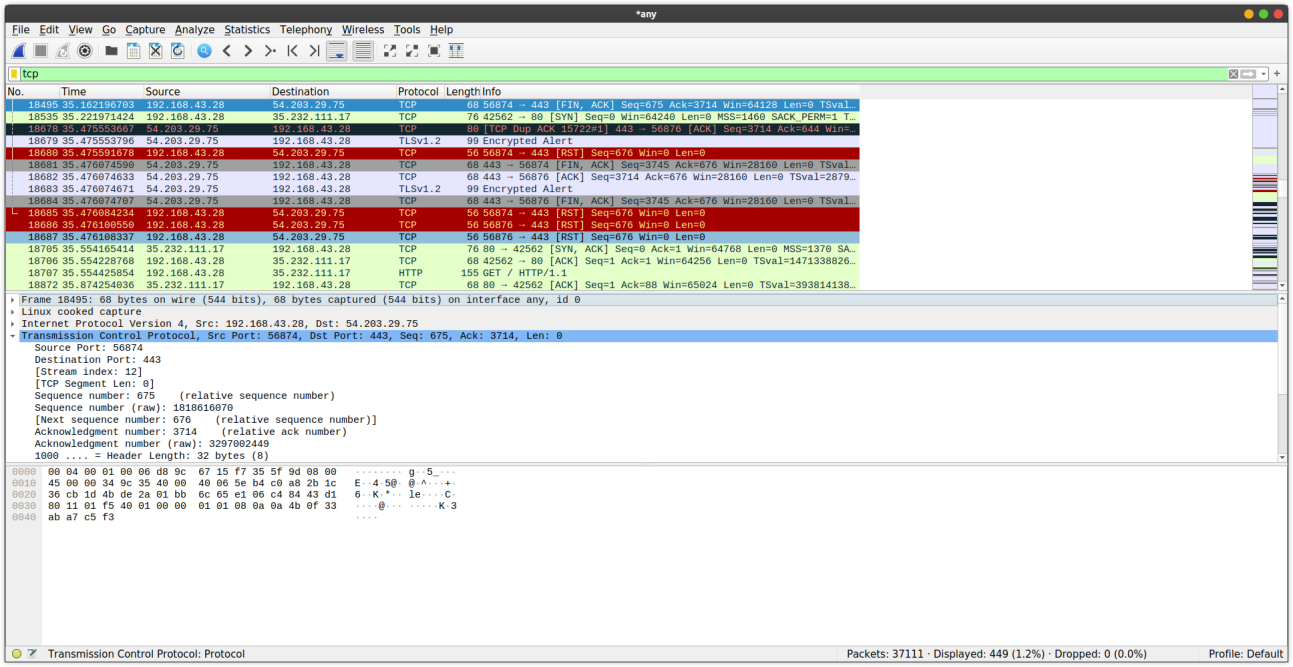
5. Filter packets with http, TCP, DNS and other protocols.

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.

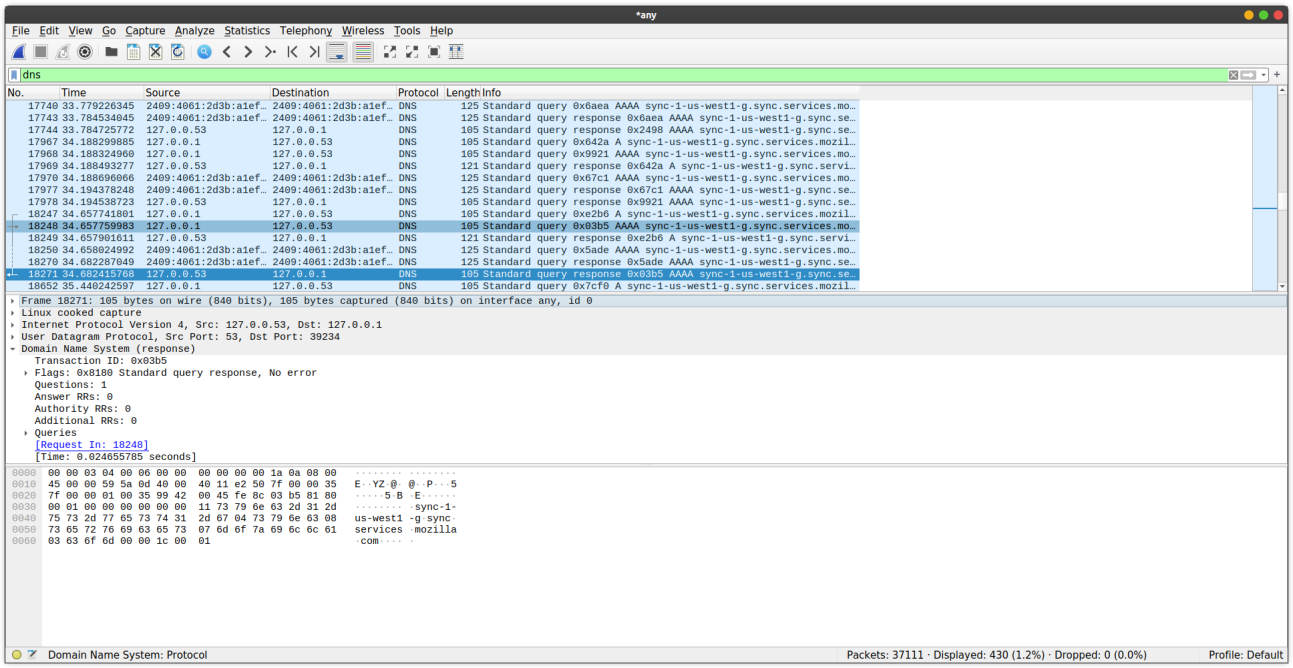
HTTP



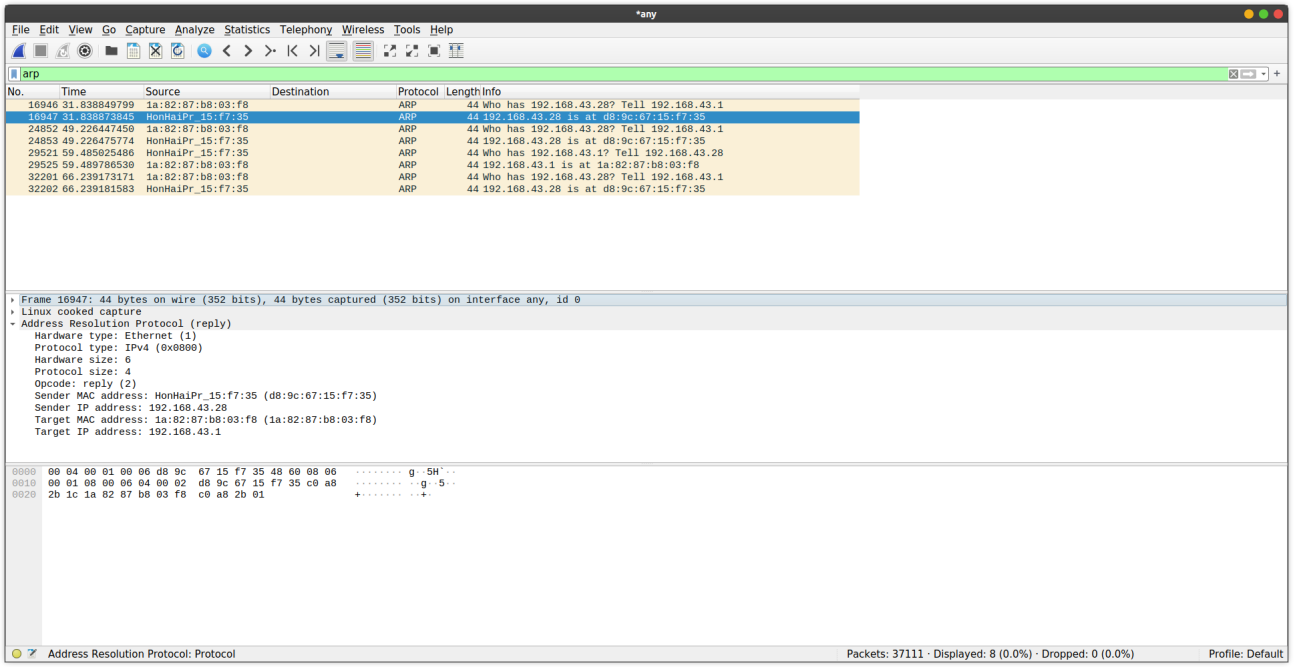
TCP


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
18495 35.162196703 192.168.43.28 54.203.29.75 TCP 68 56874 → 443 [FIN, ACK] Seq=675 Ack=3714 Win=64128 Len=0 TSval…
18535 35.221971424 192.168.43.28 35.232.111.17 TCP 76 42562 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
18678 35.475553667 54.203.29.75 192.168.43.28 TCP 80 [TCP Dup ACK 15722#1] 443 → 56876 [ACK] Seq=3714 Ack=644 Win=…
18679 35.475553796 54.203.29.75 192.168.43.28 TLSv1.2 99 Encrypted Alert
18680 35.475591678 192.168.43.28 54.203.29.75 TCP 56 56874 → 443 [RST] Seq=676 Win=0 Len=0
18681 35.476074590 54.203.29.75 192.168.43.28 TCP 68 443 → 56874 [FIN, ACK] Seq=3745 Ack=676 Win=28160 Len=0 TSval…
18682 35.476074633 54.203.29.75 192.168.43.28 TCP 68 443 → 56876 [ACK] Seq=3714 Ack=676 Win=28160 Len=0 TSval=2879…
18683 35.476074671 54.203.29.75 192.168.43.28 TLSv1.2 99 Encrypted Alert
18684 35.476074707 54.203.29.75 192.168.43.28 TCP 68 443 → 56876 [FIN, ACK] Seq=3745 Ack=676 Win=28160 Len=0 TSval…
18685 35.476084234 192.168.43.28 54.203.29.75 TCP 56 56874 → 443 [RST] Seq=676 Win=0 Len=0
18686 35.476100550 192.168.43.28 54.203.29.75 TCP 56 56876 → 443 [RST] Seq=676 Win=0 Len=0
18687 35.476108337 192.168.43.28 54.203.29.75 TCP 56 56876 → 443 [RST] Seq=676 Win=0 Len=0
18705 35.554165414 35.232.111.17 192.168.43.28 TCP 76 80 → 42562 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1370 SA…
18706 35.554228768 192.168.43.28 35.232.111.17 TCP 68 42562 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1471338826…
18707 35.554425854 192.168.43.28 35.232.111.17 HTTP 155 GET / HTTP/1.1
18872 35.874254036 35.232.111.17 192.168.43.28 TCP 68 80 → 42562 [ACK] Seq=1 Ack=88 Win=65024 Len=0 TSval=393814138…
Frame 18495: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.43.28, Dst: 54.203.29.75
Transmission Control Protocol, Src Port: 56874, Dst Port: 443, Seq: 675, Ack: 3714, Len: 0
Source Port: 56874
Destination Port: 443
[Stream index: 12]
[TCP Segment Len: 0]
Sequence number: 675 (relative sequence number)
Sequence number (raw): 1818616070
[Next sequence number: 676 (relative sequence number)]
Acknowledgment number: 3714 (relative ack number)
Acknowledgment number (raw): 3297002449
1000 .... = Header Length: 32 bytes (8)
0000 00 04 00 01 00 06 d8 9c 67 15 f7 35 5f 9d 08 00 .... g··5_···
0010 45 00 00 34 9c 35 40 00 40 06 5e b4 c0 a8 2b 1c E··4·5@· @·^···+·
0020 36 cb 1d 4b de 2a 01 bb 6c 65 e1 06 c4 84 43 d1 6··K·*·· le····C·
0030 80 11 01 f5 40 01 00 00 01 01 08 0a 0a 4b 0f 33 ····@··· ·····K·3
0040 ab a7 c5 f3 ····
Transmission Control Protocol: Protocol
Packets: 37111 · Displayed: 449 (1.2%) · Dropped: 0 (0.0%)
Profile: Default

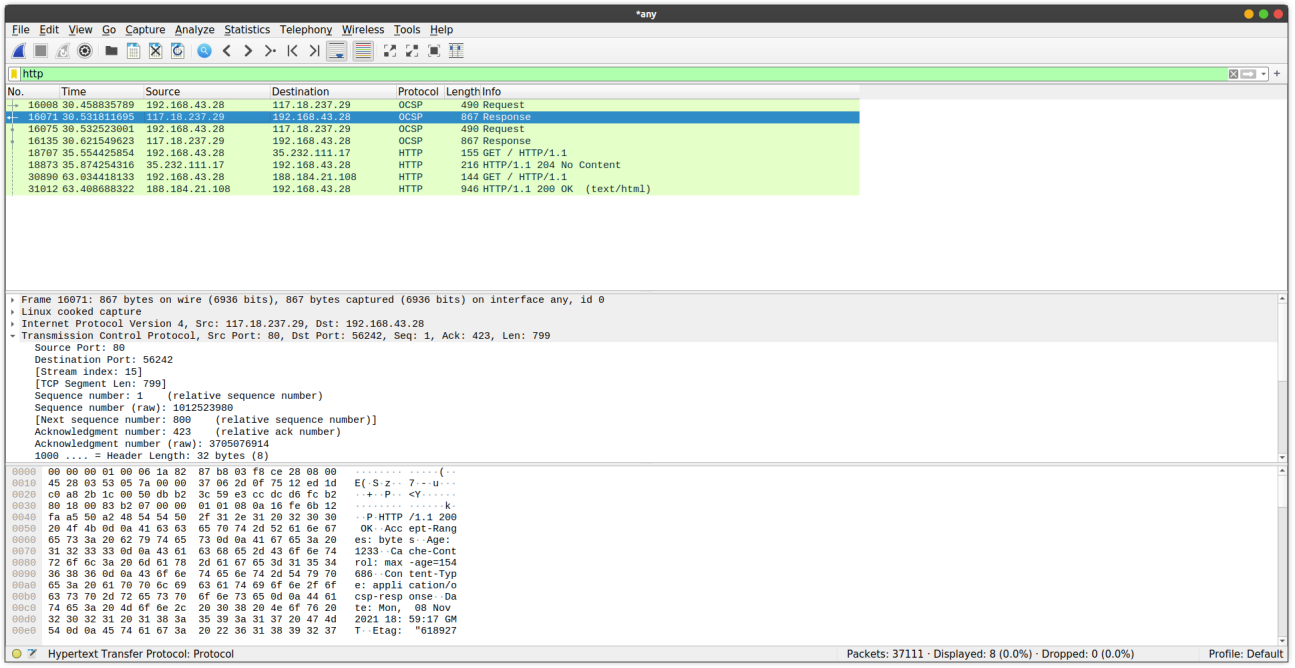
DNS


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
17740 33.779226345 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query 0x6aea AAAA sync-1-us-west1-g.sync.services.mo…
17743 33.784534045 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query response 0x6aea AAAA sync-1-us-west1-g.sync.se…
17744 33.784725772 127.0.0.53 127.0.0.1 DNS 105 Standard query response 0x2498 AAAA sync-1-us-west1-g.sync.se…
17967 34.188299885 127.0.0.1 127.0.0.53 DNS 105 Standard query 0x642a A sync-1-us-west1-g.sync.services.mozil…
17968 34.188324960 127.0.0.1 127.0.0.53 DNS 105 Standard query 0x9921 AAAA sync-1-us-west1-g.sync.services.mo…
17969 34.188493277 127.0.0.53 127.0.0.1 DNS 121 Standard query response 0x642a A sync-1-us-west1-g.sync.servi…
17970 34.188696066 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query 0x67c1 AAAA sync-1-us-west1-g.sync.services.mo…
17977 34.194378248 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query response 0x67c1 AAAA sync-1-us-west1-g.sync.se…
17978 34.194538723 127.0.0.53 127.0.0.1 DNS 105 Standard query response 0x9921 AAAA sync-1-us-west1-g.sync.se…
18247 34.657741801 127.0.0.1 127.0.0.53 DNS 105 Standard query 0xe2b6 A sync-1-us-west1-g.sync.services.mozil…
18248 34.657759983 127.0.0.1 127.0.0.53 DNS 105 Standard query 0x03b5 AAAA sync-1-us-west1-g.sync.services.mo…
18249 34.657901611 127.0.0.53 127.0.0.1 DNS 121 Standard query response 0xe2b6 A sync-1-us-west1-g.sync.servi…
18250 34.658024992 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query 0x5ade AAAA sync-1-us-west1-g.sync.services.mo…
18270 34.682287049 2409:4061:2d3b:a1ef… 2409:4061:2d3b:a1ef… DNS 125 Standard query response 0x5ade AAAA sync-1-us-west1-g.sync.se…
18271 34.682415768 127.0.0.53 127.0.0.1 DNS 105 Standard query response 0x03b5 AAAA sync-1-us-west1-g.sync.se…
18652 35.440242597 127.0.0.1 127.0.0.53 DNS 105 Standard query 0x7cf0 A sync-1-us-west1-g.sync.services.mozil…
Frame 18271: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 53, Dst Port: 39234
Domain Name System (response)
Transaction ID: 0x03b5
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Request In: 18248]
[Time: 0.024655785 seconds]
0000 00 00 03 04 00 06 00 00 00 00 00 1a 0a 08 00 ....
0010 45 00 00 59 5a 0d 40 00 40 11 e2 50 7f 00 00 35 E··YZ·@· @··P···5
0020 7f 00 00 01 00 35 99 42 00 45 fe 8c 03 b5 81 80 ·····5·B ·E·····
0030 00 01 00 00 00 00 00 00 11 73 79 6e 63 2d 31 2d ········ ·sync-1-
0040 75 73 2d 77 65 73 74 31 2d 67 04 73 79 6e 63 08 us-west1 -g·sync·
0050 73 65 72 76 69 63 65 73 07 6d 6f 7a 69 6c 6c 61 services ·mozilla
0060 03 63 6f 6d 00 00 1c 00 01 ·com···· ·
Domain Name System: Protocol
Packets: 37111 · Displayed: 430 (1.2%) · Dropped: 0 (0.0%)
Profile: Default

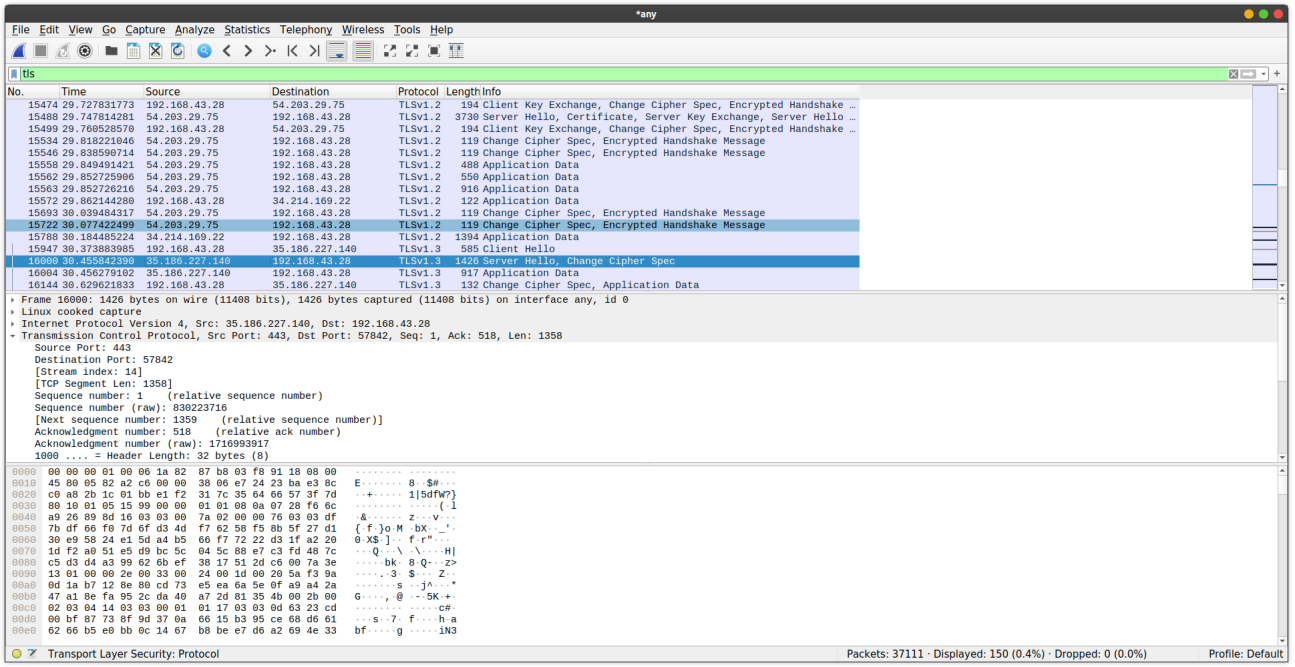
ARP


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
16946 31.838849799 1a:82:87:b8:03:f8 ARP 44 Who has 192.168.43.28? Tell 192.168.43.1
16947 31.838873845 HonHaiPr_15:f7:35 ARP 44 192.168.43.28 is at d8:9c:67:15:f7:35
24852 49.226447450 1a:82:87:b8:03:f8 ARP 44 Who has 192.168.43.28? Tell 192.168.43.1
24853 49.226475774 HonHaiPr_15:f7:35 ARP 44 192.168.43.28 is at d8:9c:67:15:f7:35
29521 59.485025486 HonHaiPr_15:f7:35 ARP 44 Who has 192.168.43.1? Tell 192.168.43.28
29525 59.489786530 1a:82:87:b8:03:f8 ARP 44 192.168.43.1 is at 1a:82:87:b8:03:f8
32201 66.239173171 1a:82:87:b8:03:f8 ARP 44 Who has 192.168.43.28? Tell 192.168.43.1
32202 66.239181583 HonHaiPr_15:f7:35 ARP 44 192.168.43.28 is at d8:9c:67:15:f7:35
Frame 16947: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
Linux cooked capture
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HonHaiPr_15:f7:35 (d8:9c:67:15:f7:35)
Sender IP address: 192.168.43.28
Target MAC address: 1a:82:87:b8:03:f8 (1a:82:87:b8:03:f8)
Target IP address: 192.168.43.1
0000 00 04 00 01 00 06 d8 9c 67 15 f7 35 48 60 08 06
0010 00 01 08 00 06 04 00 02 d8 9c 67 15 f7 35 c0 a8
0020 2b 1c 1a 82 87 b8 03 f8 c0 a8 2b 01
Address Resolution Protocol: Protocol
Packets: 37111 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

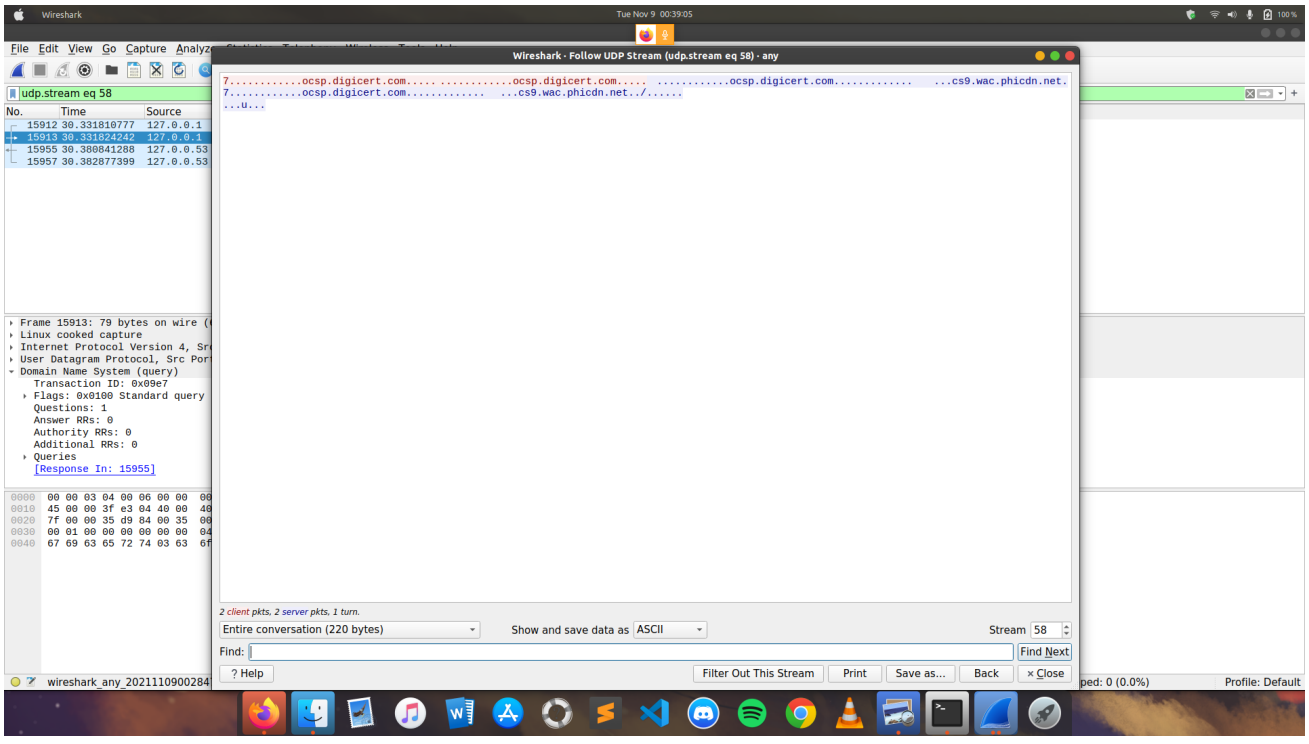
OSCP


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
16008 30.458835789 192.168.43.28 117.18.237.29 OCSP 490 Request
16071 30.531811695 117.18.237.29 192.168.43.28 OCSP 867 Response
16075 30.532523001 192.168.43.28 117.18.237.29 OCSP 490 Request
16135 30.621549623 117.18.237.29 192.168.43.28 OCSP 867 Response
18707 35.554425854 192.168.43.28 35.232.111.17 HTTP 155 GET / HTTP/1.1
18873 35.874254316 35.232.111.17 192.168.43.28 HTTP 216 HTTP/1.1 204 No Content
30890 63.034418133 192.168.43.28 188.184.21.108 HTTP 144 GET / HTTP/1.1
31012 63.408688322 188.184.21.108 192.168.43.28 HTTP 946 HTTP/1.1 200 OK (text/html)
Frame 16071: 867 bytes on wire (6936 bits), 867 bytes captured (6936 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 117.18.237.29, Dst: 192.168.43.28
Transmission Control Protocol, Src Port: 80, Dst Port: 56242, Seq: 1, Ack: 423, Len: 799
Source Port: 80
Destination Port: 56242
[Stream index: 15]
[TCP Segment Len: 799]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 1012523980
[Next sequence number: 800 (relative sequence number)]
Acknowledgment number: 423 (relative ack number)
Acknowledgment number (raw): 3705076914
1000 .... = Header Length: 32 bytes (8)
0000 00 00 00 01 00 06 1a 82 87 b8 03 f8 ce 28 08 00
0010 45 28 03 53 05 7a 00 00 37 06 2d 0f 75 12 ed 1d
0020 c0 a8 2b 1c 00 50 db b2 3c 59 e3 cc dc d6 fc b2
0030 80 18 00 83 b2 07 00 00 01 01 08 0a 16 fe 6b 12
0040 fa a5 50 a2 48 54 54 50 2f 31 2e 31 20 32 30 30
0050 20 4f 4b 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67
0060 65 73 3a 20 62 79 74 65 73 0d 0a 41 67 65 3a 20
0070 31 32 33 33 0d 0a 43 61 63 68 65 2d 43 6f 6e 74
0080 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 31 35 34
0090 36 38 36 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70
00a0 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f
00b0 63 73 70 2d 72 65 73 70 6f 6e 73 65 0d 0a 44 61
00c0 74 65 3a 20 4d 6f 6e 2c 20 30 38 20 4e 6f 76 20
00d0 32 30 32 31 20 31 38 3a 35 39 3a 31 37 20 47 4d
00e0 54 0d 0a 45 74 61 67 3a 20 22 36 31 38 39 32 37
Hypertext Transfer Protocol: Protocol
Packets: 37111 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

TLS

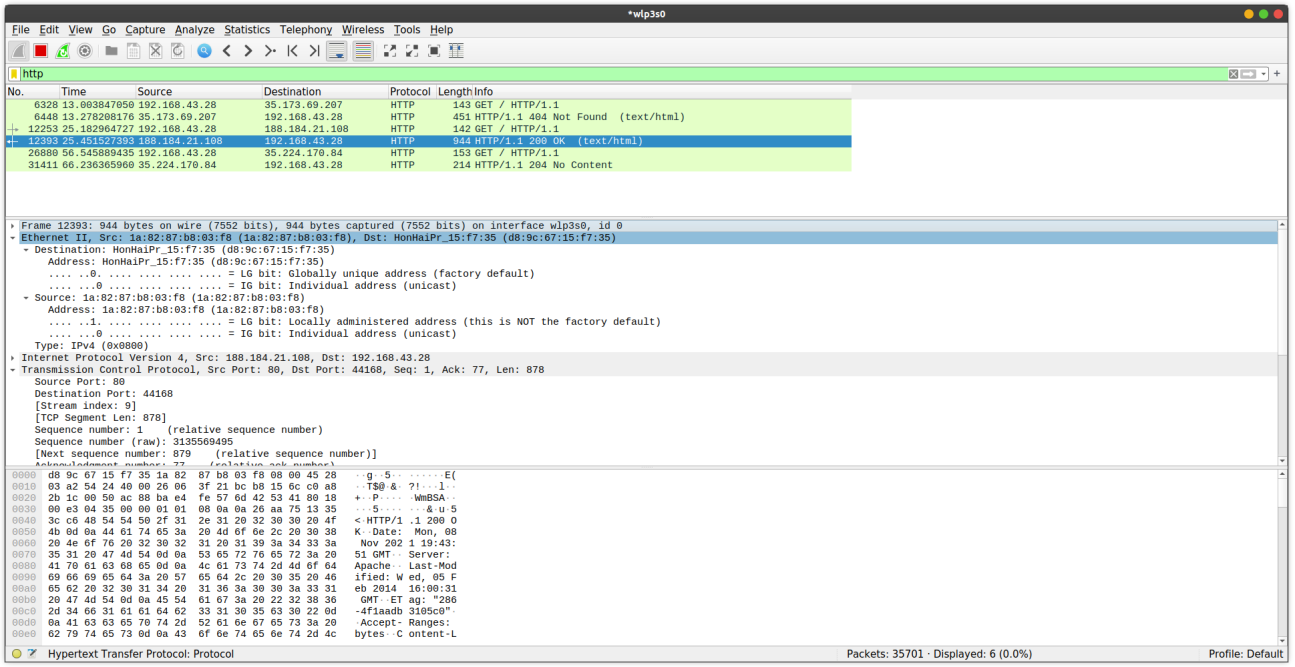


On selecting a packet of DNS protocol, and on selecting follow UDP Stream for this paket, the following result was obtained:



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.



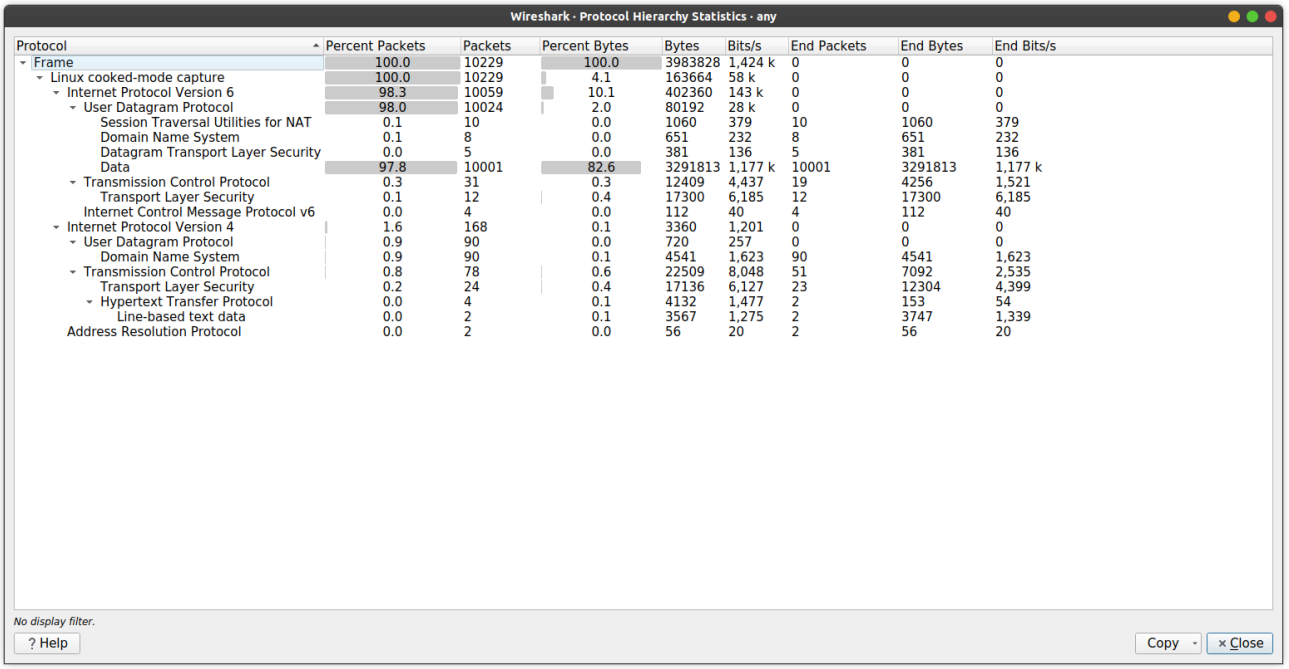
7. What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?

Manufacturer of my Laptop's Network Interface Card (NIC) is:
1a:82:87:b8:03:f8 (1a:82:87:b8:03:f8)

Manufacturer of the Server's Network Interface Card (NIC) is:
HonHaiPr_15:f7:35 (d8:9c:67:15:f7:35)

8. What are the Hex values (shown in the raw bytes panel) of the two NICS Manufacturers OUIs?
For my Laptop's manufacturer: **1a:82:87:b8:03:f8**
For server's manufacturer: **d8:9c:67:15:f7:35**

9. Find the following statistics:



Protocol Hierarchy Statistics

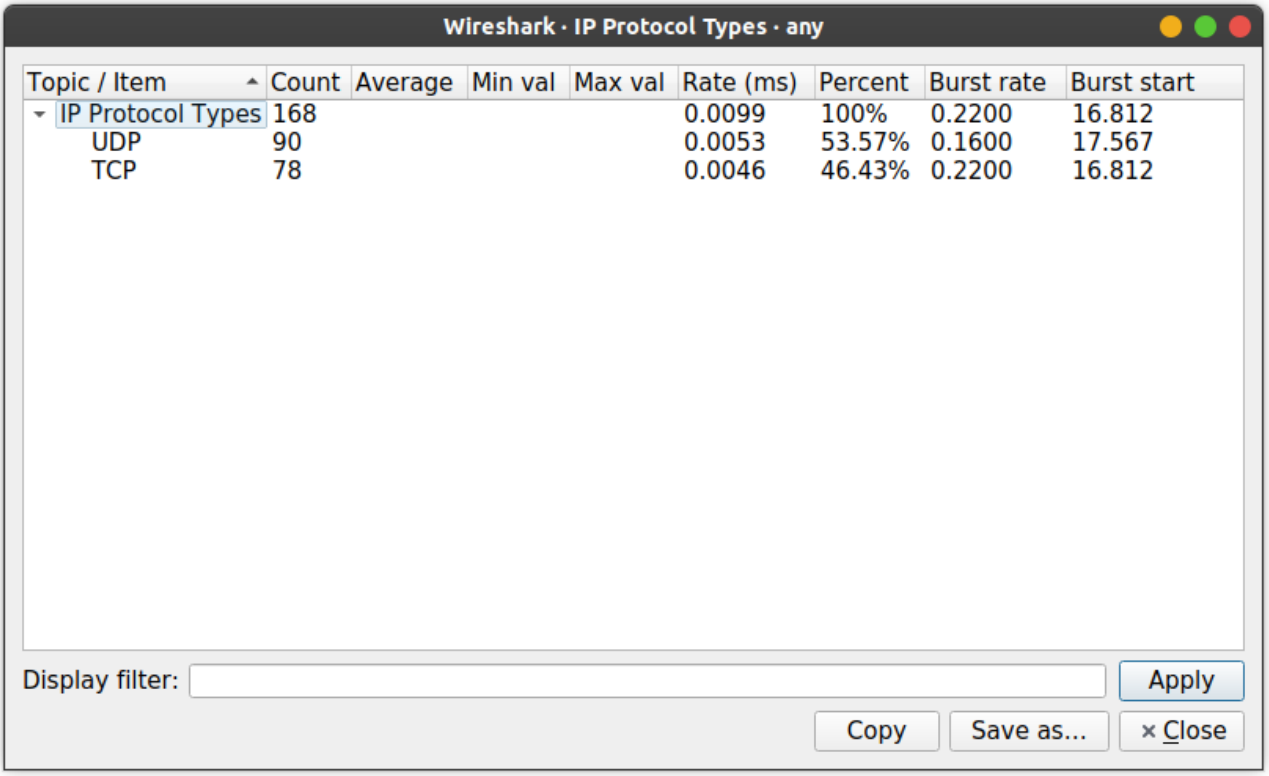
a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?

Higher level protocols which use TCP :
1. HTTPS - HyperText Transfer Protocol Secure
2. FTP - File Transfer Protocol

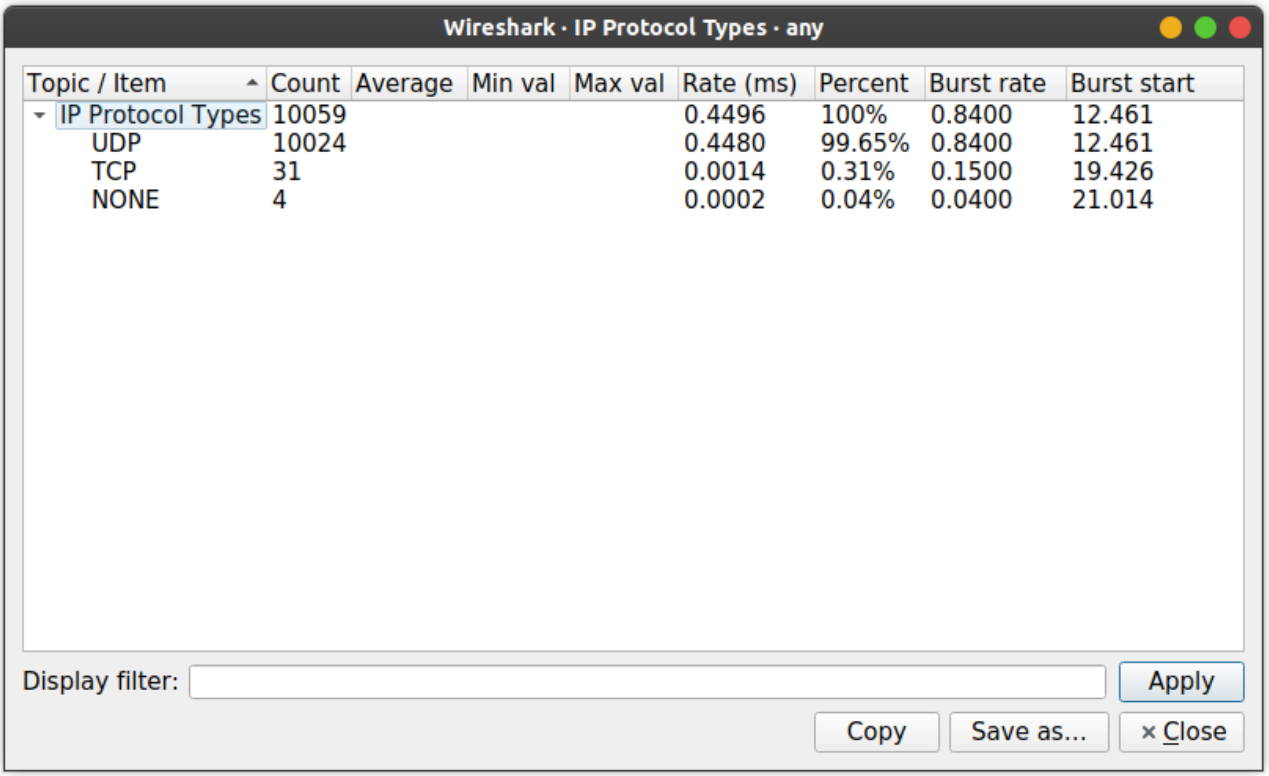
b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

Higher level protocols which use UDP :
1. SNMP - Simple Network Management Protocol
2. RIP - Routing Information Protocol

The IPv4 statistics of the packet capture:

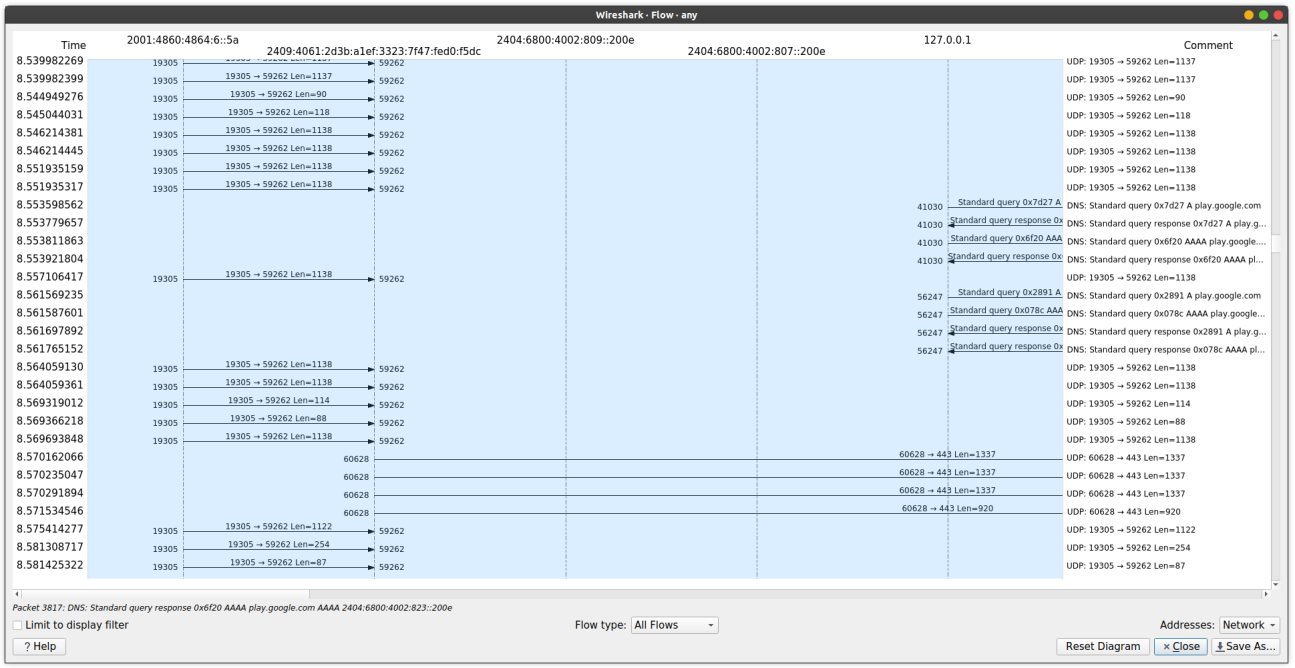


The IPv6 statistics of the packet capture:

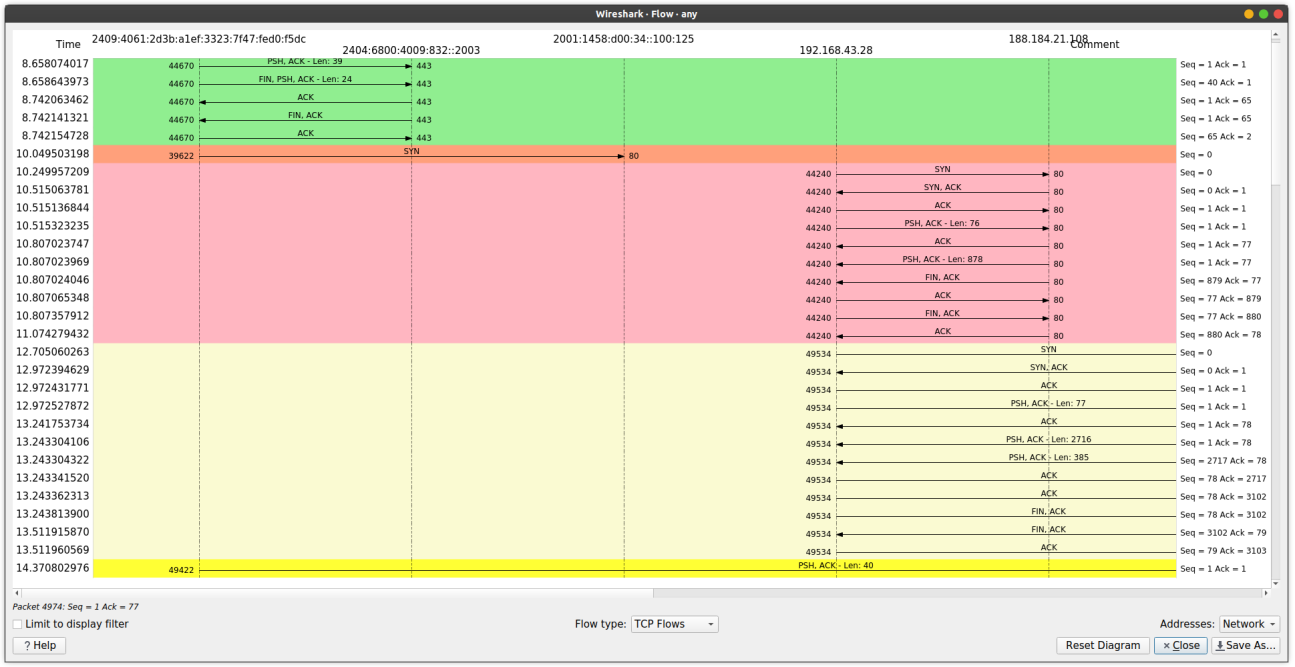


10. Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.

Graph obtained for General Flow and Network Source Options:



Graph obtained for TCP Flow and Network Source Options:



Comments:

This was a unique assignment with a new tool Wireshark. The packets were captured and analysed and helped me get a clear knowledge about how protocols work in the real world.