NAME: Debadrita Roy

CLASS: BCSE-III

GROUP: A1

ASSIGNMENT NUMBER: 5

PROBLEM STATEMENT: Packet tracer and traffic analysis with Wireshark

DEADLINE: 29th October, 2021

DATE OF SUBMISSION: 9th November, 2021

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.

SYSTEM DETAILS:

OS: 64-bit Windows 10
Wireshark version 3.4.9

QUESTIONS

1. 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 neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.

Windows command prompt:

```
C:\Users\USER19>ping 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75

Pinging 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75 with 32 bytes of data:
Reply from 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75: time=6ms
Reply from 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75: time=39ms
Reply from 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75: time=10ms
Reply from 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75: time=6ms

Ping statistics for 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 39ms, Average = 15ms

C:\Users\USER19>
```

Results in Wireshark:

icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
52	6.862420	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 (sol, ovr) is at ac:d5:64:…
81	12.740937	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	94	Echo (ping) request id=0x0001, seq=69, hop limit=128 (reply in 82)
82	12.747722	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	94	Echo (ping) reply id=0x0001, seq=69, hop limit=64 (request in 81)
83	13.750255	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	94	Echo (ping) request id=0x0001, seq=70, hop limit=128 (reply in 84)
84	13.789166	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	94	Echo (ping) reply id=0x0001, seq=70, hop limit=64 (request in 83)
89	14.766394	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	94	Echo (ping) request id=0x0001, seq=71, hop limit=128 (reply in 90)
90	14.777032	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	94	Echo (ping) reply id=0x0001, seq=71, hop limit=64 (request in 89)
136	15.780321	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	94	Echo (ping) request id=0x0001, seq=72, hop limit=128 (reply in 140)
140	15.786432	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	94	Echo (ping) reply id=0x0001, seq=72, hop limit=64 (request in 136)
190	17.466755	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75 from ac:d5:64:d6:36:9d
191	17.486876	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75 (sol, ovr) is at a2:e4:29:3…
192	17.575872	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 from a2:e4:29:3b:0b:f9
193	17.576089	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 (sol, ovr) is at ac:d5:64:…
214	20.217681	fe80::4d1e:5c22:5563:d2e8	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
217	20.229414	fe80::4d1e:5c22:5563:d2e8	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
219	20.229896	fe80::4d1e:5c22:5563:d2e8	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
221	20.230044	fe80::4d1e:5c22:5563:d2e8	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
230	20.478049	fe80::4d1e:5c22:5563:d2e8	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
245	29.049014	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 from 0e:ff:9e:60:f5:38
246	29.049128	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 (sol, ovr) is at ac:d5:64:…
388	56.141507	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 from 0e:ff:9e:60:f5:38
389	56.141620	2409:4060:2e95:dbc9:59ce:6f76:c325:b253	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 (sol, ovr) is at ac:d5:64:…
490	64.235615	fe80::cff:9eff:fe60:f538	ff02::1	ICMPv6	142	Router Advertisement from 0e:ff:9e:60:f5:38

The source ipv6 address (my machine) is 2409:4060:2e95:dbc9:59ce:6f76:c325:b253 and the ipv6 address of the neighbouring machine used is 2409:4060:2e95:dbc9:c138:4d9a:c2fa:e75.

2. Generate some web traffic and

a. find the list 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.)

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

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.

Answers:

a. List of different protocols appearing in the protocol column:

- ARP (Address Resolution Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- MDNS (multicast DNS)
- LLMNR (Link-Local Multicast Name Resolution)
- DNS (Domain Name System)
- HTTP (Hypertext Transfer Protocol)
- NBNS (NetBIOS Name Service)
- QUIC (Quick UDP Internet Connection)
- ICMPv6 (Internet Control Message Protocol version 6)
- TLSv1.2, TLSv1.3 (Transport Layer Security)
- SSDP (Simple Service Discovery Protocol)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	4.2.2.1	192.168.43.142	DNS	267	Standard query response 0x7e39 A protecti.quickheal.com CNAME PTi2-ELB-46950754.ap-south-…
2	0.010027	4.2.2.1	192.168.43.142	DNS	217	Standard query response 0xc204 AAAA protecti.quickheal.com CNAME PTi2-ELB-46950754.ap-sou…
3	0.011112	192.168.43.142	3.7.119.34	TCP	66	53779 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.011171	192.168.43.142	3.7.119.34	TCP	66	53780 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.068885	192.168.43.238	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
6	0.103652	3.7.119.34	192.168.43.142	TCP	66	80 → 53779 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1370 SACK_PERM=1 WS=256
7	0.103766	192.168.43.142	3.7.119.34	TCP	54	53779 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8	0.118226	3.7.119.34	192.168.43.142	TCP	66	80 → 53780 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1370 SACK_PERM=1 WS=256
9	0.118317	192.168.43.142	3.7.119.34	TCP	54	53780 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10	0.128436	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:82c::200a	UDP	95	61575 → 443 Len=33
11	0.128448	192.168.43.142	3.7.119.34	HTTP	911	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
12	0.128448	192.168.43.142	3.7.119.34	HTTP	903	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
13	0.143919	2404:6800:4003:c11::bd	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	UDP	88	443 → 49786 Len=26
14	0.231485	3.7.119.34	192.168.43.142	TCP	54	80 → 53779 [ACK] Seq=1 Ack=858 Win=28672 Len=0
15	0.232261	2404:6800:4002:82c::200a	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	UDP	87	443 → 61575 Len=25
16	0.241837	3.7.119.34	192.168.43.142	HTTP	578	HTTP/1.1 200 OK (text/plain)
17	0.245601	192.168.43.142	3.7.119.34	TCP	54	53779 → 80 [FIN, ACK] Seq=858 Ack=525 Win=65024 Len=0
18	0.255926	3.7.119.34	192.168.43.142	TCP	54	80 → 53780 [ACK] Seq=1 Ack=850 Win=28672 Len=0
19	0.274620	3.7.119.34	192.168.43.142	HTTP	578	HTTP/1.1 200 OK (text/plain)
20	0.275787	192.168.43.142	3.7.119.34	TCP	54	53780 → 80 [FIN, ACK] Seq=850 Ack=525 Win=65024 Len=0
21	0.324264	3.7.119.34	192.168.43.142	TCP	54	80 → 53779 [FIN, ACK] Seq=525 Ack=859 Win=28672 Len=0
22	0.324415	192.168.43.142	3.7.119.34	TCP	54	53779 → 80 [ACK] Seq=859 Ack=526 Win=65024 Len=0
23	0.358816	3.7.119.34	192.168.43.142	TCP	54	80 → 53780 [FIN, ACK] Seq=525 Ack=851 Win=28672 Len=0
24	0.358959	192.168.43.142	3.7.119.34	TCP	54	53780 → 80 [ACK] Seq=851 Ack=526 Win=65024 Len=0
25	0.472142	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:80a::200e	QUIC	1392	Initial, DCID=8199c7b62176cee2, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO,…
26	0.643734	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:82c::200a	UDP	95	61575 → 443 Len=33
27	0.659677	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:809::200e	TCP	1424	53419 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1350 [TCP segment of a reassembled PDU]
28	0.659677	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:809::200e	TLSv1.2	169	Application Data

> Frame 11: 911 bytes on wire (7288 bits), 911 bytes captured (7288 bits) on interface \Device\NPF_{4BB60237-4A15-4A53-9782-6CE0AB8AD924}, id 0
> Ethernet II, Src: Chongqin_d6:36:9d (ac:d5:64:d6:36:9d), Dst: 0e:ff:9e:60:f5:38 (0e:ff:9e:60:f5:38)
> Internet Protocol Version 4, Src: 192.168.43.142, Dst: 3.7.119.34

b.

7801	83.254672	192.168.43.142	15.207.154.216	HTTP	458	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
7828	83.363390	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	356	HEAD /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejgin…
7848	83.464792	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	624	HTTP/1.1 200 OK
7856	83.489189	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	428	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
7877	83.614092	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	571	HTTP/1.1 206 Partial Content
8397	87.542033	15.207.154.216	192.168.43.142	HTTP	59	HTTP/1.1 200 OK (application/text)
8456	87.857580	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8461	87.885149	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8632	88.811634	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8676	89.511158	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
9006	93.192444	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	839	HTTP/1.1 206 Partial Content
9506	97.224914	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
9643	98.272942	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	321	HTTP/1.1 206 Partial Content
9755	98.973399	192.168.43.142	15.207.154.216	HTTP	458	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
102…	102.667123	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
103…	102.946464	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	78	HTTP/1.1 206 Partial Content
109…	107.868301	192.168.43.142	120.29.198.248	HTTP	209	GET /1700/urlcat/wsaltcnf.bin HTTP/1.1
111…	109.747995	120.29.198.248	192.168.43.142	HTTP	433	HTTP/1.1 200 OK
112…	110.364012	120.29.198.248	192.168.43.142	HTTP	433	[TCP Spurious Retransmission] HTTP/1.1 200 OK
114…	111.441430	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
114…	111.552529	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	77	HTTP/1.1 206 Partial Content

Time taken from when HTTP GET was sent until the receipt of HTTP OK message

=109.747995-107.868301= 1.879694 s

c. Internet address of the destination: 120.29.198.248

Internet address of my machine : 192.168.43.142

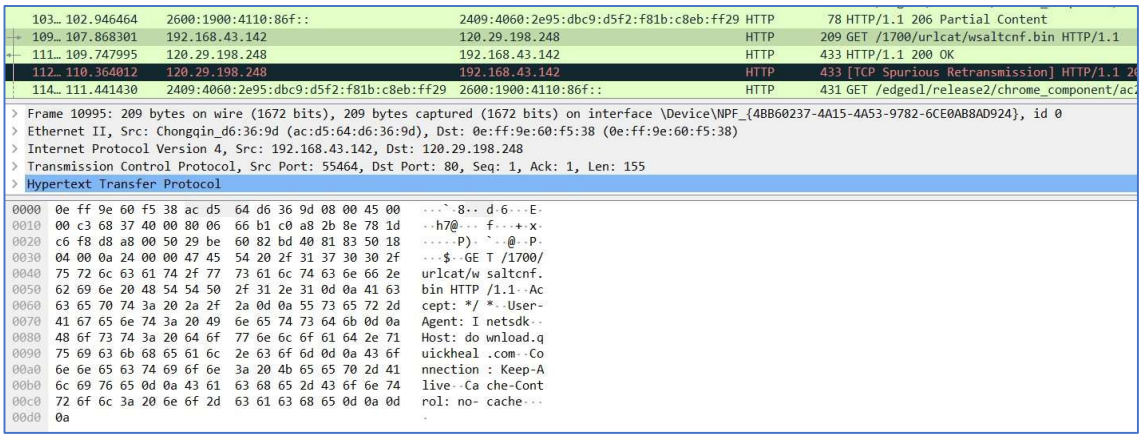
d.

9506	97.224914	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62ey
9643	98.272942	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	321	HTTP/1.1 206 Partial Content
9755	98.973399	192.168.43.142	15.207.154.216	HTTP	458	POST /URLCategorizerService/URLCategorize HTTP/1
102…	102.667123	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62ey
103…	102.946464	2600:1900:4110:86f:::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	78	HTTP/1.1 206 Partial Content
109…	107.868301	192.168.43.142	120.29.198.248	HTTP	209	GET /1700/urlcat/wsaltcnf.bin HTTP/1.1
111…	109.747995	120.29.198.248	192.168.43.142	HTTP	433	HTTP/1.1 200 OK
112…	110.364012	120.29.198.248	192.168.43.142	HTTP	433	[TCP Spurious Retransmission] HTTP/1.1 200 OK
114…	111.441430	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f:::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62ey

```
> Frame 10995: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{4BB60237-4A15-4A53-9782-6CE0AB8AD924}, id 0
> Ethernet II, Src: Chongqin_d6:36:9d (ac:d5:64:d6:36:9d), Dst: 0e:ff:9e:60:f5:38 (0e:ff:9e:60:f5:38)
> Internet Protocol Version 4, Src: 192.168.43.142, Dst: 120.29.198.248
> Transmission Control Protocol, Src Port: 55464, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
v Hypertext Transfer Protocol
  v GET /1700/urlcat/wsaltcnf.bin HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /1700/urlcat/wsaltcnf.bin HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /1700/urlcat/wsaltcnf.bin
      Request Version: HTTP/1.1
    Accept: */*\r\n
    User-Agent: Inetsdk\r\n
    Host: download.quickheal.com\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://download.quickheal.com/1700/urlcat/wsaltcnf.bin]
    [HTTP request 1/2]
    [Response in frame: 11143]
```

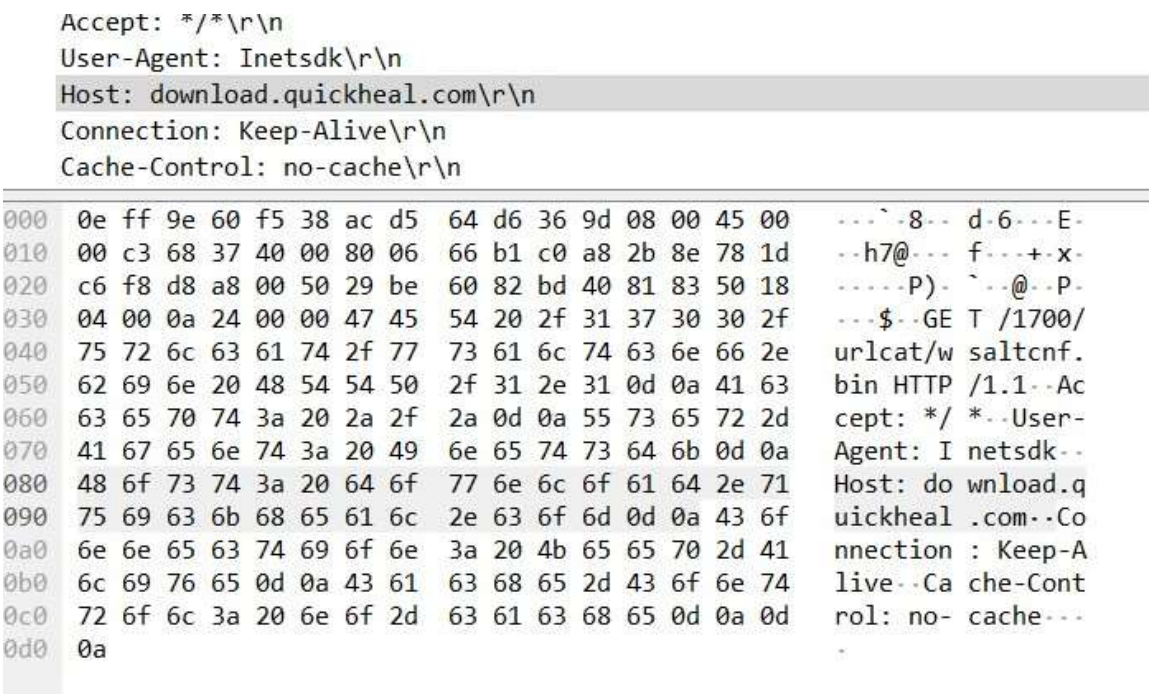
e. The value of the host is download.quickheal.com\r\n as seen in the above screenshot.

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



|-----HEX REPRESENTATION-----| |----ASCII----|

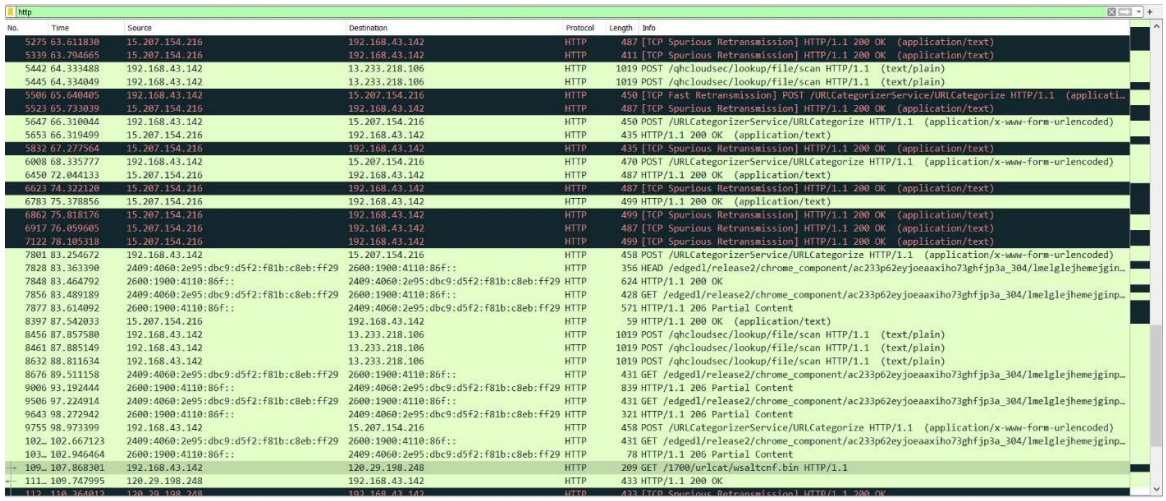
4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.



The highlighted portion of the HEX Representation of the packet is for the host parameter. The first 4 bytes are 48 6f 73 74.

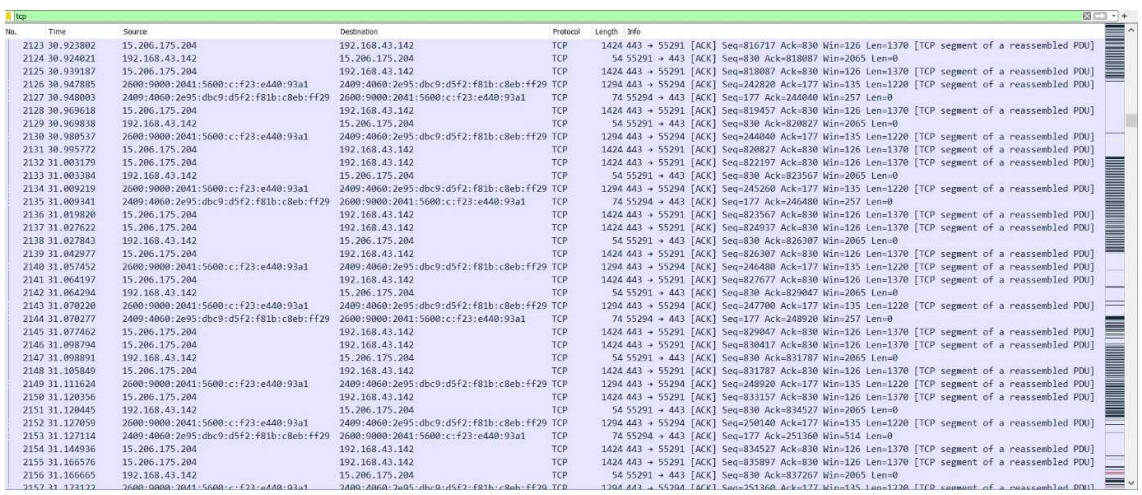
5. Filter packets with http, TCP, DNS and other protocols.

HTTP:



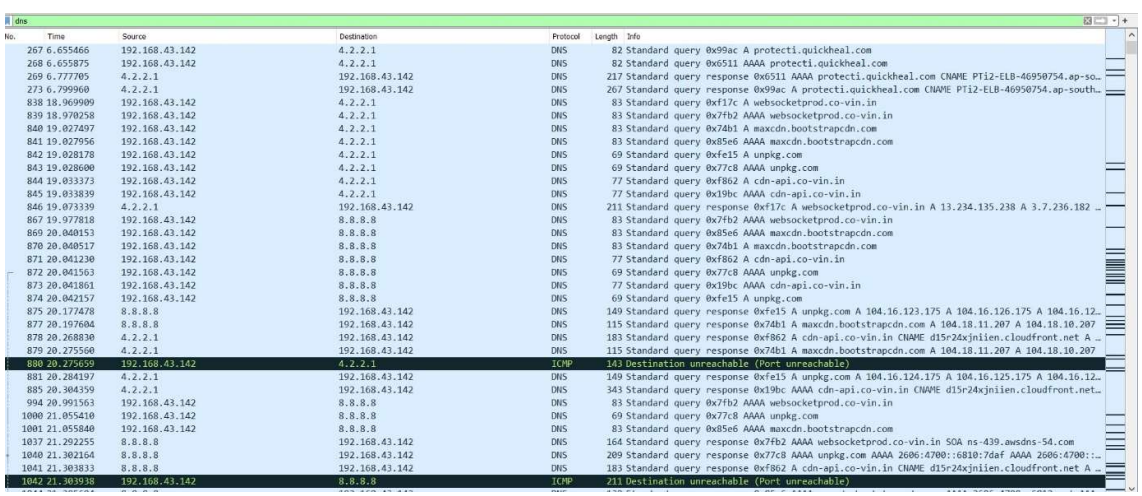
No.	Time	Source	Destination	Protocol	Length	Info
5275	63.611830	15.207.154.216	192.168.43.142	HTTP	487	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
5339	63.794665	15.207.154.216	192.168.43.142	HTTP	411	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
5442	64.333488	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
5445	64.334049	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
5506	65.640405	192.168.43.142	15.207.154.216	HTTP	450	[TCP Fast Retransmission] POST /URLCategorizerService/URLCategorize HTTP/1.1 (applicati…
5523	65.733039	15.207.154.216	192.168.43.142	HTTP	487	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
5647	66.310044	192.168.43.142	15.207.154.216	HTTP	450	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
5653	66.319499	15.207.154.216	192.168.43.142	HTTP	435	HTTP/1.1 200 OK (application/text)
5832	67.277564	15.207.154.216	192.168.43.142	HTTP	435	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
6008	68.335777	192.168.43.142	15.207.154.216	HTTP	470	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
6450	72.044133	15.207.154.216	192.168.43.142	HTTP	487	HTTP/1.1 200 OK (application/text)
6623	74.322120	15.207.154.216	192.168.43.142	HTTP	487	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
6783	75.378856	15.207.154.216	192.168.43.142	HTTP	499	HTTP/1.1 200 OK (application/text)
6862	75.818176	15.207.154.216	192.168.43.142	HTTP	499	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
6917	76.059605	15.207.154.216	192.168.43.142	HTTP	487	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
7122	78.105338	15.207.154.216	192.168.43.142	HTTP	499	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/text)
7801	83.254672	192.168.43.142	15.207.154.216	HTTP	458	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
7828	83.363390	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f::	HTTP	356	HEAD /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
7848	83.464792	2600:1900:4110:86f::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	624	HTTP/1.1 200 OK
7856	83.489189	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f::	HTTP	428	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
7877	83.614092	2600:1900:4110:86f::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	571	HTTP/1.1 206 Partial Content
8397	87.542033	15.207.154.216	192.168.43.142	HTTP	59	HTTP/1.1 200 OK (application/text)
8456	87.857580	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8461	87.885149	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8632	88.811634	192.168.43.142	13.233.218.106	HTTP	1019	POST /qhcloudsec/lookup/file/scan HTTP/1.1 (text/plain)
8676	89.511158	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
9006	93.192444	2600:1900:4110:86f::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	839	HTTP/1.1 206 Partial Content
9506	97.224914	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
9643	98.272942	2600:1900:4110:86f::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	321	HTTP/1.1 206 Partial Content
9755	98.973399	192.168.43.142	15.207.154.216	HTTP	458	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
102…	102.667123	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:1900:4110:86f::	HTTP	431	GET /edgedl/release2/chrome_component/ac233p62eyjoeaaxiho73ghfjp3a_304/lmelglejhemejginp…
103…	102.946464	2600:1900:4110:86f::	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	HTTP	78	HTTP/1.1 206 Partial Content
109…	107.868301	192.168.43.142	120.29.198.248	HTTP	209	GET /1700/urlcat/wsaltcnf.bin HTTP/1.1
111…	109.747995	120.29.198.248	192.168.43.142	HTTP	433	HTTP/1.1 200 OK

TCP:



No.	Time	Source	Destination	Protocol	Length	Info
2123	30.923802	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=816717 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2124	30.924021	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=818087 Win=2065 Len=0
2125	30.939187	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=818087 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2126	30.947885	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=242820 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2127	30.948003	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:9000:2041:5600:c:f23:e440:93a1	TCP	74	55294 → 443 [ACK] Seq=177 Ack=244040 Win=257 Len=0
2128	30.969618	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=819457 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2129	30.969618	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=820827 Win=2065 Len=0
2130	30.980537	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=244040 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2131	30.995772	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=820827 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2132	31.003179	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=822197 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2133	31.003384	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=823567 Win=2065 Len=0
2134	31.009219	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=245260 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2135	31.009341	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:9000:2041:5600:c:f23:e440:93a1	TCP	74	55294 → 443 [ACK] Seq=177 Ack=246480 Win=257 Len=0
2136	31.019820	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=823567 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2137	31.027622	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=824937 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2138	31.027843	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=826307 Win=2065 Len=0
2139	31.042977	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=826307 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2140	31.057452	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=246480 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2141	31.064197	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=827677 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2142	31.064294	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=829047 Win=2065 Len=0
2143	31.070220	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=247700 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2144	31.070277	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:9000:2041:5600:c:f23:e440:93a1	TCP	74	55294 → 443 [ACK] Seq=177 Ack=248920 Win=257 Len=0
2145	31.077462	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=829047 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2146	31.098794	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=830417 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2147	31.098891	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=831787 Win=2065 Len=0
2148	31.105849	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=831787 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2149	31.111624	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=248920 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2150	31.120356	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=833157 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2151	31.120445	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=834527 Win=2065 Len=0
2152	31.127059	2600:9000:2041:5600:c:f23:e440:93a1	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	TCP	1294	443 → 55294 [ACK] Seq=250140 Ack=177 Win=135 Len=1220 [TCP segment of a reassembled PDU]
2153	31.127114	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2600:9000:2041:5600:c:f23:e440:93a1	TCP	74	55294 → 443 [ACK] Seq=177 Ack=251360 Win=514 Len=0
2154	31.144936	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=834527 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2155	31.166576	15.206.175.204	192.168.43.142	TCP	1424	443 → 55291 [ACK] Seq=835897 Ack=830 Win=126 Len=1370 [TCP segment of a reassembled PDU]
2156	31.166665	192.168.43.142	15.206.175.204	TCP	54	55291 → 443 [ACK] Seq=830 Ack=837267 Win=2065 Len=0

DNS:



No.	Time	Source	Destination	Protocol	Length	Info
267	6.655466	192.168.43.142	4.2.2.1	DNS	82	Standard query 0x99ac A protecti.quickheal.com
268	6.655875	192.168.43.142	4.2.2.1	DNS	82	Standard query 0x6511 AAAA protecti.quickheal.com
269	6.777705	4.2.2.1	192.168.43.142	DNS	217	Standard query response 0x6511 AAAA protecti.quickheal.com CNAME PTi2-ELB-46950754.ap-so…
273	6.799960	4.2.2.1	192.168.43.142	DNS	267	Standard query response 0x99ac A protecti.quickheal.com CNAME PTi2-ELB-46950754.ap-south…
838	18.969909	192.168.43.142	4.2.2.1	DNS	83	Standard query 0xf17c A websocketprod.co-vin.in
839	18.970258	192.168.43.142	4.2.2.1	DNS	83	Standard query 0x7fb2 AAAA websocketprod.co-vin.in
840	19.027497	192.168.43.142	4.2.2.1	DNS	83	Standard query 0x74b1 A maxcdn.bootstrapcdn.com
841	19.027956	192.168.43.142	4.2.2.1	DNS	83	Standard query 0x85e6 AAAA maxcdn.bootstrapcdn.com
842	19.028178	192.168.43.142	4.2.2.1	DNS	69	Standard query 0xfe15 A unpkg.com
843	19.028600	192.168.43.142	4.2.2.1	DNS	69	Standard query 0x77c8 AAAA unpkg.com
844	19.033373	192.168.43.142	4.2.2.1	DNS	77	Standard query 0xf862 A cdn-api.co-vin.in
845	19.033839	192.168.43.142	4.2.2.1	DNS	77	Standard query 0x19bc AAAA cdn-api.co-vin.in
846	19.073339	4.2.2.1	192.168.43.142	DNS	211	Standard query response 0xf17c A websocketprod.co-vin.in A 13.234.135.238 A 3.7.236.182 …
867	19.977818	192.168.43.142	8.8.8.8	DNS	83	Standard query 0x7fb2 AAAA websocketprod.co-vin.in
869	20.040153	192.168.43.142	8.8.8.8	DNS	83	Standard query 0x85e6 AAAA maxcdn.bootstrapcdn.com
870	20.040517	192.168.43.142	8.8.8.8	DNS	83	Standard query 0x74b1 A maxcdn.bootstrapcdn.com
871	20.041230	192.168.43.142	8.8.8.8	DNS	77	Standard query 0xf862 A cdn-api.co-vin.in
872	20.041563	192.168.43.142	8.8.8.8	DNS	69	Standard query 0x77c8 AAAA unpkg.com
873	20.041861	192.168.43.142	8.8.8.8	DNS	77	Standard query 0x19bc AAAA cdn-api.co-vin.in
874	20.042157	192.168.43.142	8.8.8.8	DNS	69	Standard query 0xfe15 A unpkg.com
875	20.177478	8.8.8.8	192.168.43.142	DNS	149	Standard query response 0xfe15 A unpkg.com A 104.16.123.175 A 104.16.126.175 A 104.16.12…
877	20.197604	8.8.8.8	192.168.43.142	DNS	115	Standard query response 0x74b1 A maxcdn.bootstrapcdn.com A 104.18.11.207 A 104.18.10.207
878	20.268830	4.2.2.1	192.168.43.142	DNS	183	Standard query response 0xf862 A cdn-api.co-vin.in CNAME d15r24xjniien.cloudfront.net A …
879	20.275560	4.2.2.1	192.168.43.142	DNS	115	Standard query response 0x74b1 A maxcdn.bootstrapcdn.com A 104.18.11.207 A 104.18.10.207
880	20.275659	192.168.43.142	4.2.2.1	ICMP	143	Destination unreachable (Port unreachable)
881	20.284197	4.2.2.1	192.168.43.142	DNS	149	Standard query response 0xfe15 A unpkg.com A 104.16.124.175 A 104.16.125.175 A 104.16.12…
885	20.304359	4.2.2.1	192.168.43.142	DNS	343	Standard query response 0x19bc AAAA cdn-api.co-vin.in CNAME d15r24xjniien.cloudfront.net…
994	20.991563	192.168.43.142	8.8.8.8	DNS	83	Standard query 0x7fb2 AAAA websocketprod.co-vin.in
1000	21.055410	192.168.43.142	8.8.8.8	DNS	69	Standard query 0x77c8 AAAA unpkg.com
1001	21.055840	192.168.43.142	8.8.8.8	DNS	83	Standard query 0x85e6 AAAA maxcdn.bootstrapcdn.com
1037	21.292255	8.8.8.8	192.168.43.142	DNS	164	Standard query response 0x7fb2 AAAA websocketprod.co-vin.in SOA ns-439.awsdns-54.com
1040	21.302164	8.8.8.8	192.168.43.142	DNS	209	Standard query response 0x77c8 AAAA unpkg.com AAAA 2606:4700::6810:7daf AAAA 2606:4700::…
1041	21.303833	8.8.8.8	192.168.43.142	DNS	183	Standard query response 0xf862 A cdn-api.co-vin.in CNAME d15r24xjniien.cloudfront.net A …
1042	21.303938	192.168.43.142	8.8.8.8	ICMP	211	Destination unreachable (Port unreachable)

ICMPv6:

icmpv6

	Time	Source	Destination	Protocol	Length	Info
503	12.232263	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
504	12.232308	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
525	12.547551	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
526	12.547638	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
527	12.564954	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
528	12.565152	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
2719	37.965705	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
2720	37.965833	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
2771	38.478865	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
2772	38.478996	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
2826	38.923236	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
2827	38.923280	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
4109	55.253010	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:82b::2004	ICMPv6	1294	Destination Unreachable (Port unreachable)
4238	55.797611	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4002:82b::2004	ICMPv6	1294	Handshake, SCID=9103012b71551637
4527	58.345512	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2606:4700::6810:135e	ICMPv6	1294	Protected Payload (KP0)
4975	61.786540	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4009:820::2001	ICMPv6	1294	Destination Unreachable (Port unreachable)
5101	62.610268	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2606:4700::6810:135e	ICMPv6	1294	Protected Payload (KP0)
5231	63.400847	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2404:6800:4009:820::2001	ICMPv6	1294	Handshake, SCID=ac495a74b92cedaa
5270	63.559011	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	2606:4700::6810:135e	ICMPv6	1294	Destination Unreachable (Port unreachable)
5864	67.418792	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
5865	67.418826	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
5930	67.791920	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
5931	67.791948	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
5990	68.274540	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
5991	68.274594	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
6050	68.549729	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
6051	68.549762	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
6222	70.333445	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
6223	70.333482	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
6267	70.543206	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
6268	70.543230	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
6303	70.749498	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38
6304	70.749535	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	fe80::cff:9eff:fe60:f538	ICMPv6	86	Neighbor Advertisement 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 (sol, ovr) is at ac:d5:64…
6384	71.403339	fe80::cff:9eff:fe60:f538	2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29	ICMPv6	86	Neighbor Solicitation for 2409:4060:2e95:dbc9:d5f2:f81b:c8eb:ff29 from 0e:ff:9e:60:f5:38

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.

Clicking on a DNS packet and following the UDP stream,

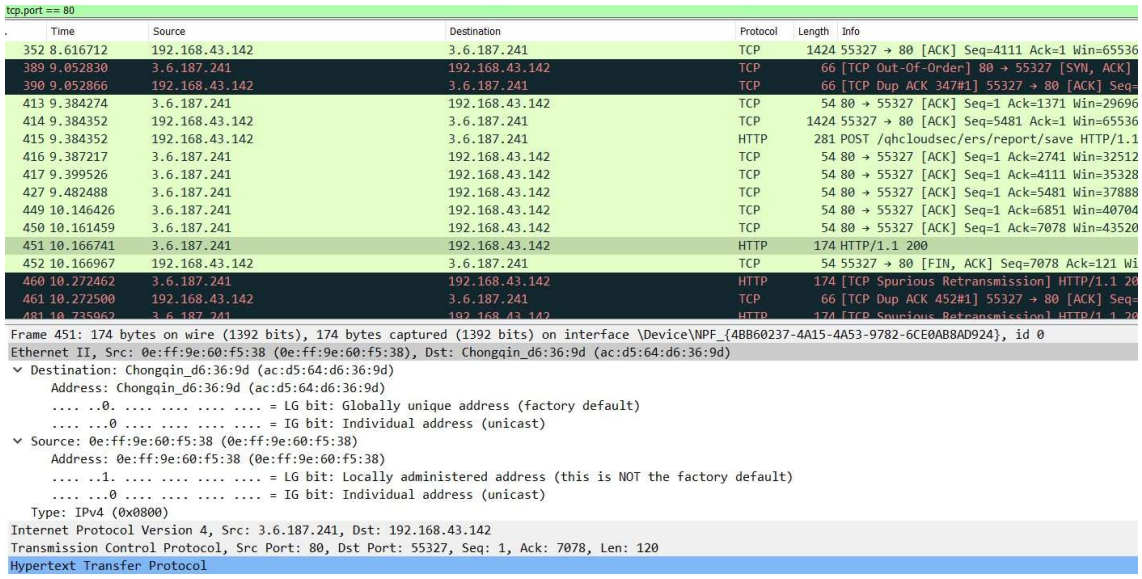
Wireshark · Follow UDP Stream (udp.stream eq 19) · Wi-Fi

```
.........
websocketprod.co-vin.in................
websocketprod.co-vin.in................
websocketprod.co-vin.in...............E.ns-439      awsdns-54.com..awsdns-hostmaster.amazon.F....... ......u...Q............
websocketprod.co-vin.in.............h.E.ns-439      awsdns-54.com..awsdns-hostmaster.amazon.F....... ......u...Q.
```

2 client pkts, 2 server pkts, 1 turn.

Entire conversation (326 bytes) | Show data as ASCII | Stream 19

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.



tcp.port == 80

	Time	Source	Destination	Protocol	Length	Info
352	8.616712	192.168.43.142	3.6.187.241	TCP	1424	55327 → 80 [ACK] Seq=4111 Ack=1 Win=65536
389	9.052830	3.6.187.241	192.168.43.142	TCP	66	[TCP Out-Of-Order] 80 → 55327 [SYN, ACK]
390	9.052866	192.168.43.142	3.6.187.241	TCP	66	[TCP Dup ACK 347#1] 55327 → 80 [ACK] Seq=
413	9.384274	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=1371 Win=29696
414	9.384352	192.168.43.142	3.6.187.241	TCP	1424	55327 → 80 [ACK] Seq=5481 Ack=1 Win=65536
415	9.384352	192.168.43.142	3.6.187.241	HTTP	281	POST /qhcloudsec/ers/report/save HTTP/1.1
416	9.387217	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=2741 Win=32512
417	9.399526	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=4111 Win=35328
427	9.482488	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=5481 Win=37888
449	10.146426	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=6851 Win=40704
450	10.161459	3.6.187.241	192.168.43.142	TCP	54	80 → 55327 [ACK] Seq=1 Ack=7078 Win=43520
451	10.166741	3.6.187.241	192.168.43.142	HTTP	174	HTTP/1.1 200
452	10.166967	192.168.43.142	3.6.187.241	TCP	54	55327 → 80 [FIN, ACK] Seq=7078 Ack=121 Wi
460	10.272462	3.6.187.241	192.168.43.142	HTTP	174	[TCP Spurious Retransmission] HTTP/1.1 20
461	10.272500	192.168.43.142	3.6.187.241	TCP	66	[TCP Dup ACK 452#1] 55327 → 80 [ACK] Seq=
481	10.735962	3.6.187.241	192.168.43.142	HTTP	174	[TCP Spurious Retransmission] HTTP/1.1 20

```
Frame 451: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{4BB60237-4A15-4A53-9782-6CE0AB8AD924}, id 0
Ethernet II, Src: 0e:ff:9e:60:f5:38 (0e:ff:9e:60:f5:38), Dst: Chongqin_d6:36:9d (ac:d5:64:d6:36:9d)
  Destination: Chongqin_d6:36:9d (ac:d5:64:d6:36:9d)
      Address: Chongqin_d6:36:9d (ac:d5:64:d6:36:9d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 0e:ff:9e:60:f5:38 (0e:ff:9e:60:f5:38)
      Address: 0e:ff:9e:60:f5:38 (0e:ff:9e:60:f5:38)
      .... ..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: 3.6.187.241, Dst: 192.168.43.142
Transmission Control Protocol, Src Port: 80, Dst Port: 55327, Seq: 1, Ack: 7078, Len: 120
Hypertext Transfer Protocol
```

Packet 451 is an HTTP packet coming back from the server (tcp source port ==80).

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):

Chongqing Fugui Electronics Co., Ltd

Manufacturer of the server's Network Interface Card (NIC):

MAC Address-- 0e:ff:9e:60:f5:38

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

Laptop: ac-d5-64

Server: 0e-ff-9e

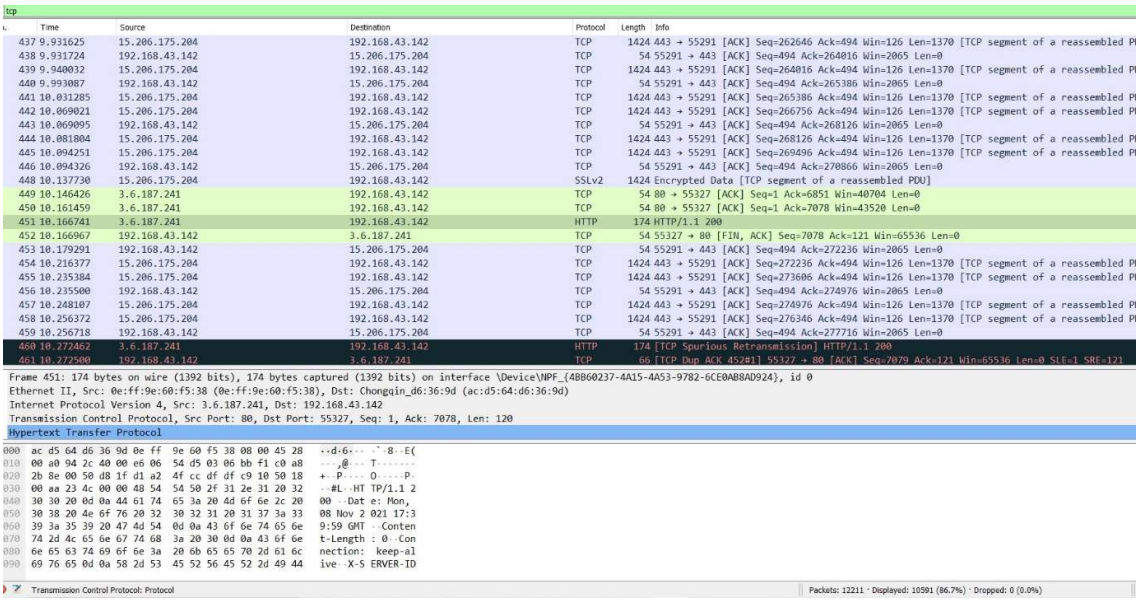
9. Find the following statistics:

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

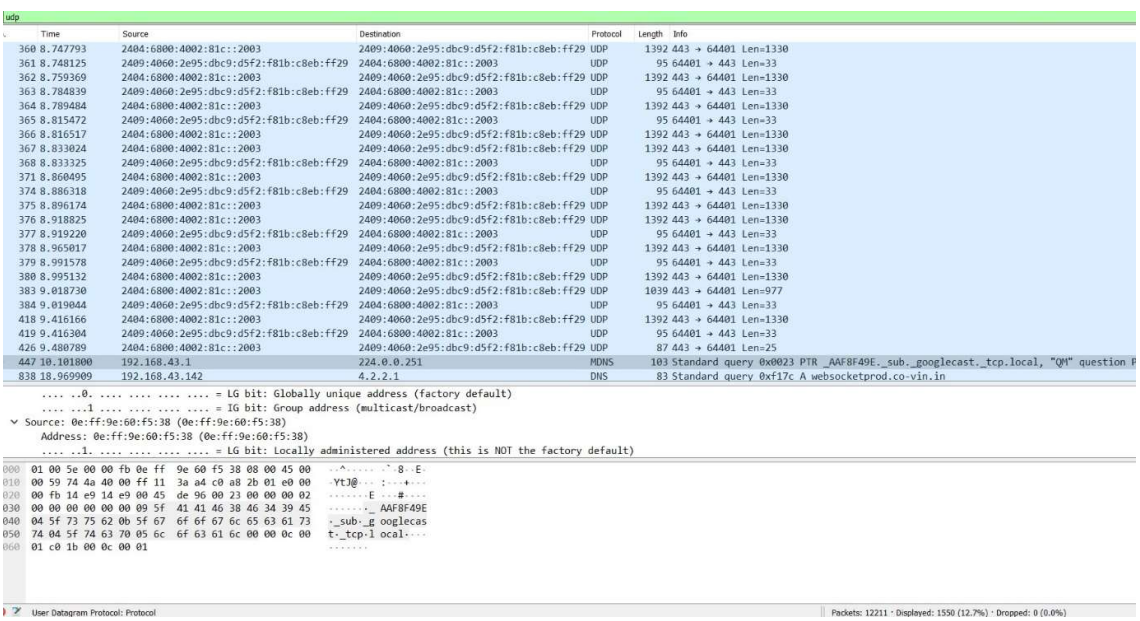
b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

Answers:

a. Out of 12211 packets captured, 10591 were TCP packets, i.e., TCP packets accounted for 86.7% of the total packets captured. HTTP (Hypertext Transfer Protocol) uses TCP.

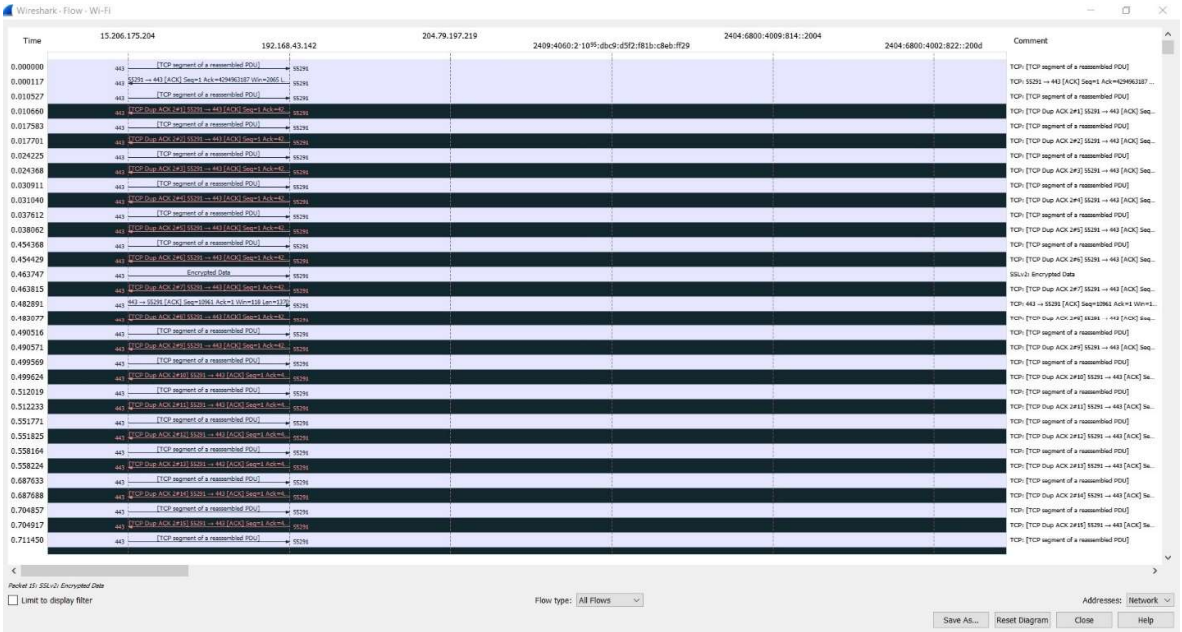


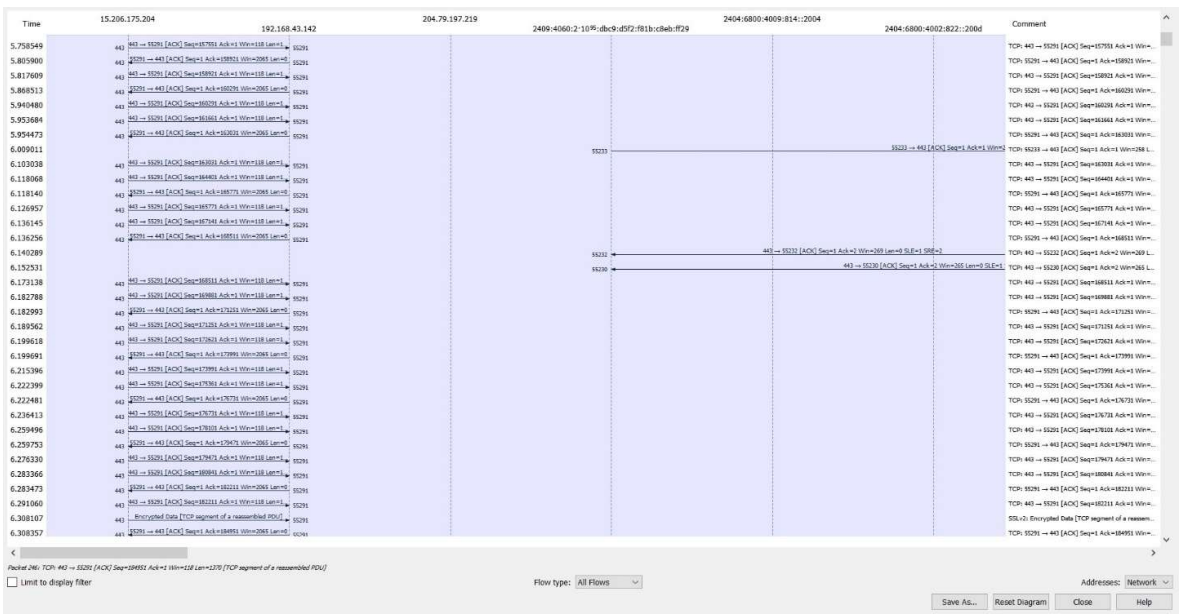
b. Out of 12211 packets captured, 1550 were UDP packets, i.e., UDP packets accounted for 12.7% of the total packets captured. SNMP (Simple Network Management Protocol) uses UDP.



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

Snippets of the graph:





COMMENTS

The assignment was interesting as it gave us a real-world idea of the packets being sent using different protocols. I liked capturing the packets at different times when I was generating different amounts of traffic and see the results. I also learnt how to use a new analysing tool, Wireshark.