Network Assignment 5

Name: - Santanu Mandal   Roll: - 002010501102

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.

Problem Statement

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

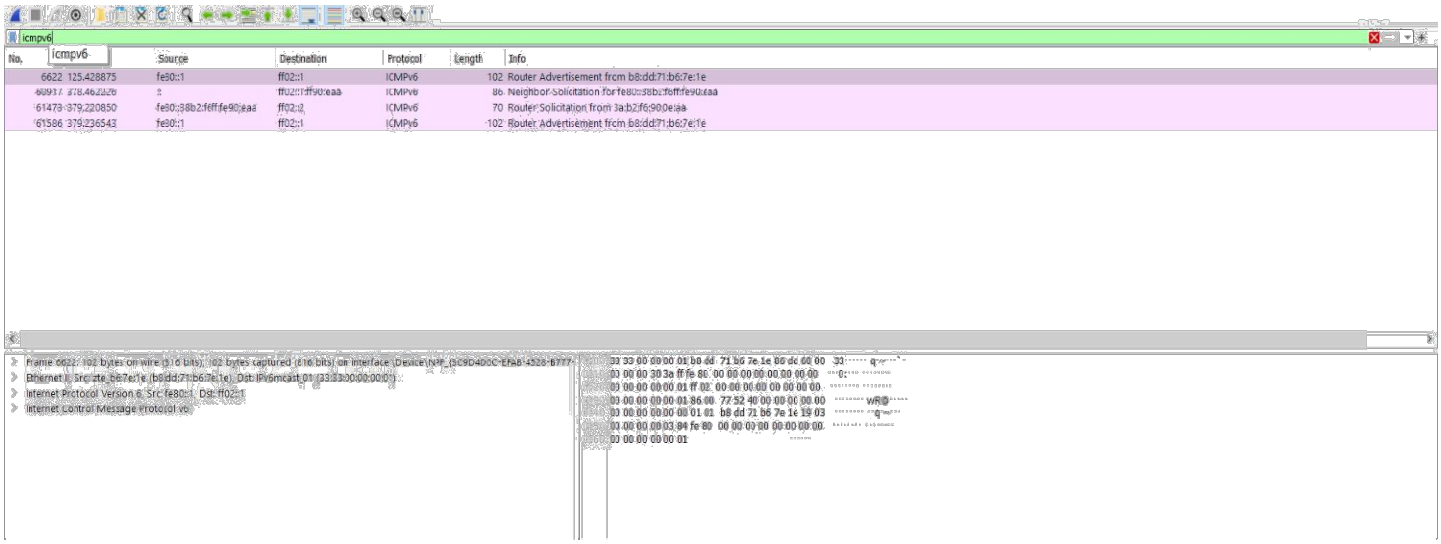
System Specifications

1. System OS Type: - Windows
2. System OS: - Ubuntu Linux 22.04
3. Wireshark: - 4.0.1
4. Network: - Wireless Network (WIFI)

Questions and Solutions

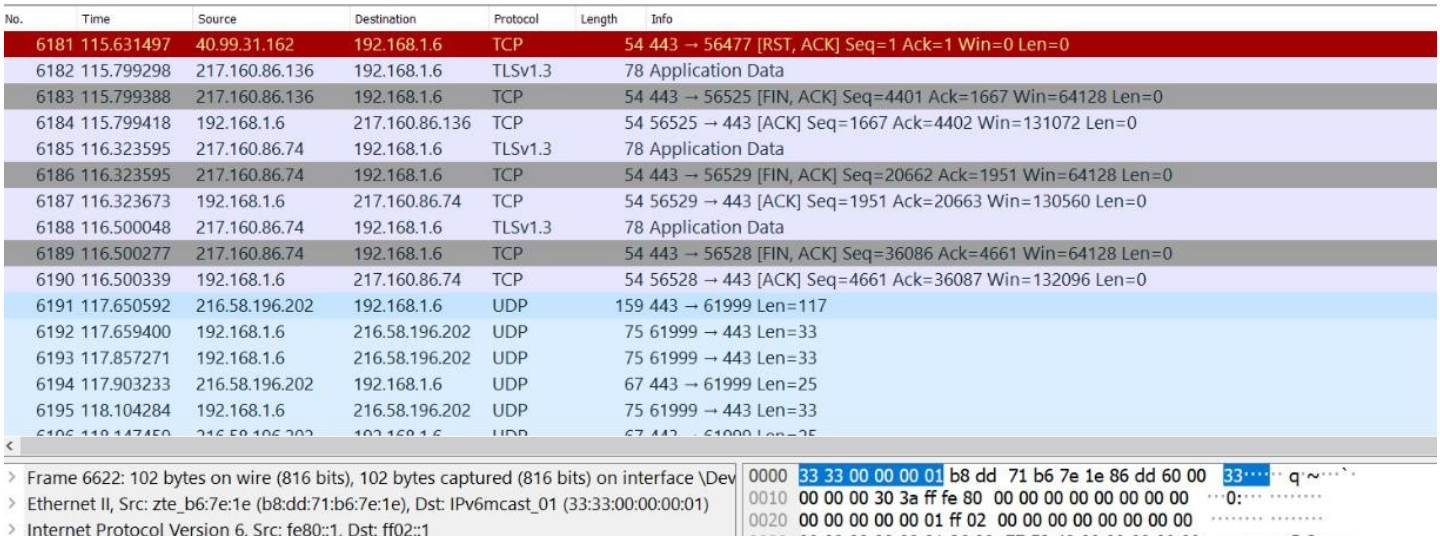
Q1. Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighbouring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

```
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
```



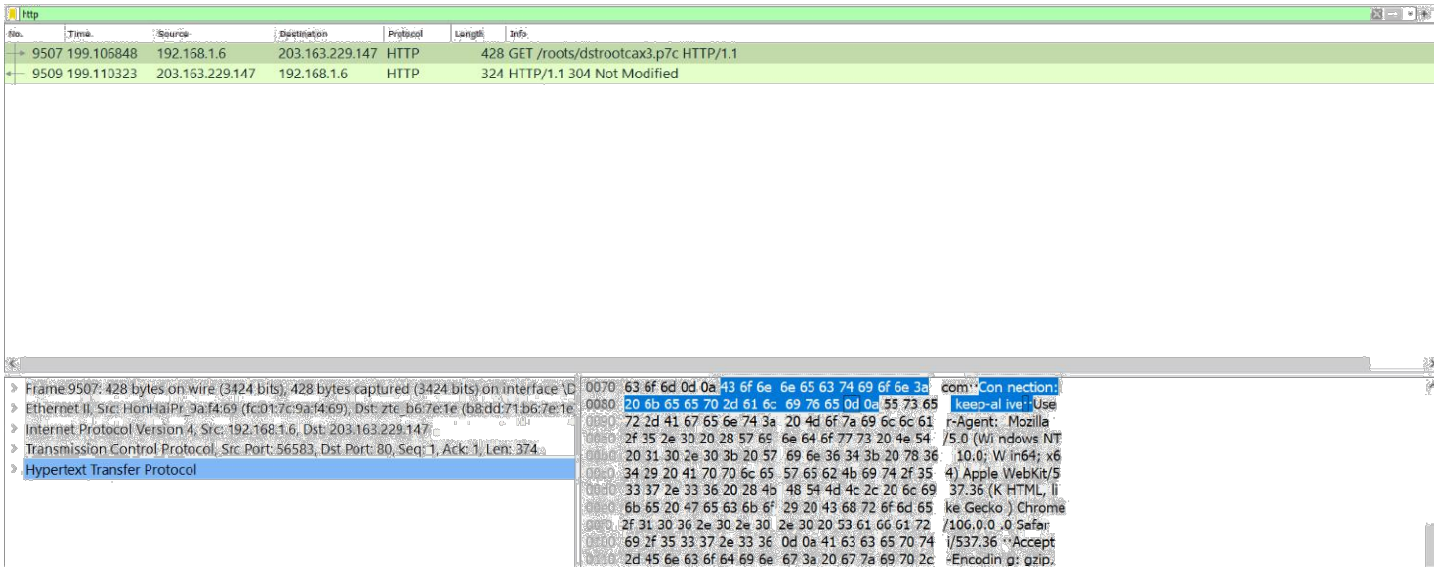
2. Generate some web traffic and

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



No.	Time	Source	Destination	Protocol	Length	Info
6181	115.631497	40.99.31.162	192.168.1.6	TCP	54	443 → 56477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6182	115.799298	217.160.86.136	192.168.1.6	TLSv1.3	78	Application Data
6183	115.799388	217.160.86.136	192.168.1.6	TCP	54	443 → 56525 [FIN, ACK] Seq=4401 Ack=1667 Win=64128 Len=0
6184	115.799418	192.168.1.6	217.160.86.136	TCP	54	56525 → 443 [ACK] Seq=1667 Ack=4402 Win=131072 Len=0
6185	116.323595	217.160.86.74	192.168.1.6	TLSv1.3	78	Application Data
6186	116.323595	217.160.86.74	192.168.1.6	TCP	54	443 → 56529 [FIN, ACK] Seq=20662 Ack=1951 Win=64128 Len=0
6187	116.323673	192.168.1.6	217.160.86.74	TCP	54	56529 → 443 [ACK] Seq=1951 Ack=20663 Win=130560 Len=0
6188	116.500048	217.160.86.74	192.168.1.6	TLSv1.3	78	Application Data
6189	116.500277	217.160.86.74	192.168.1.6	TCP	54	443 → 56528 [FIN, ACK] Seq=36086 Ack=4661 Win=64128 Len=0
6190	116.500339	192.168.1.6	217.160.86.74	TCP	54	56528 → 443 [ACK] Seq=4661 Ack=36087 Win=132096 Len=0
6191	117.650592	216.58.196.202	192.168.1.6	UDP	159	443 → 61999 Len=117
6192	117.659400	192.168.1.6	216.58.196.202	UDP	75	61999 → 443 Len=33
6193	117.857271	192.168.1.6	216.58.196.202	UDP	75	61999 → 443 Len=33
6194	117.903233	216.58.196.202	192.168.1.6	UDP	67	443 → 61999 Len=25
6195	118.104284	192.168.1.6	216.58.196.202	UDP	75	61999 → 443 Len=33

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.)

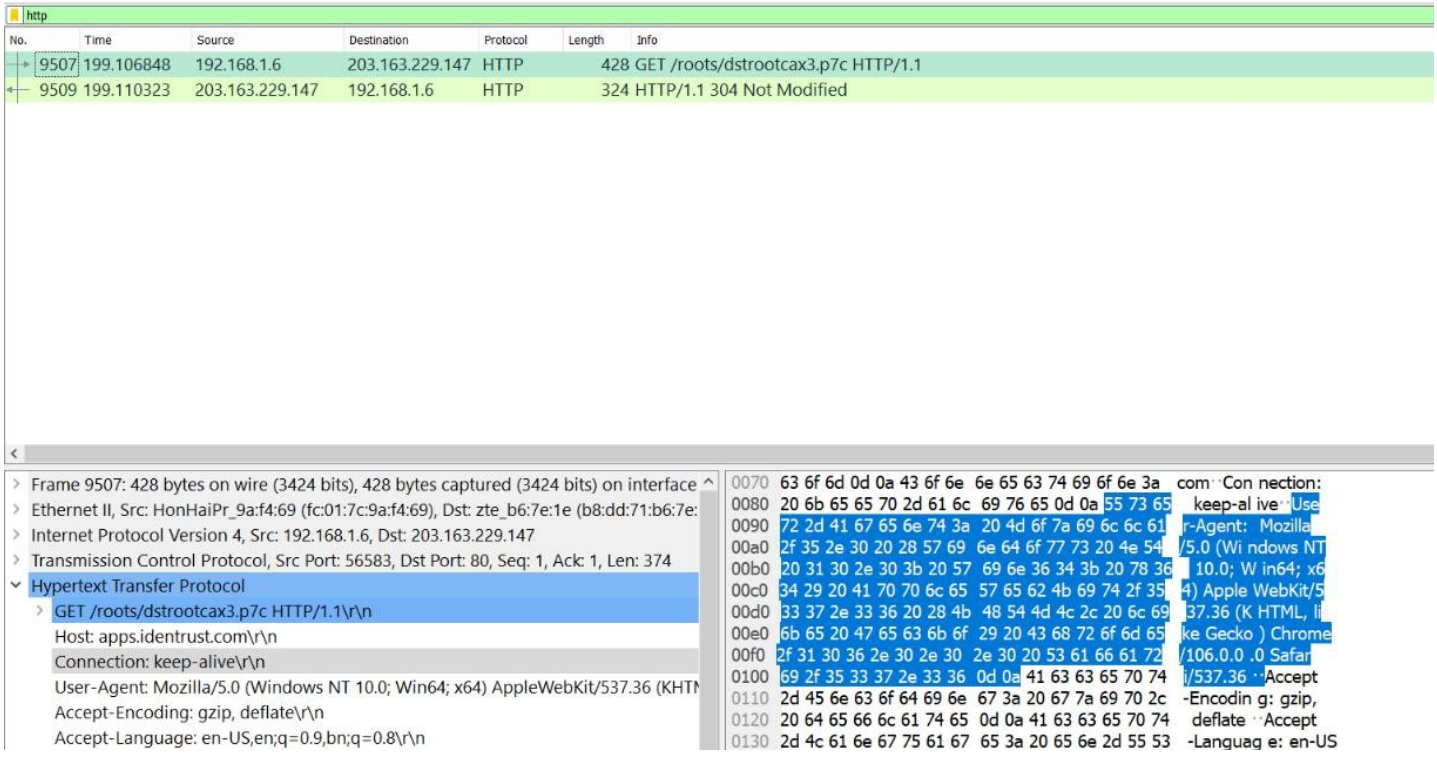


As shown in the screenshot above the GET (9507) was sent at 199.106848 and the OK was received at 199.110323 second. Thus, the total delay (199.110323-199.106848) = 0.003475 seconds.

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

From the above ss it is clearly visible that the IP address of my computer is 192.168.1.6 and the IP address of the website is 203.163.229.147.

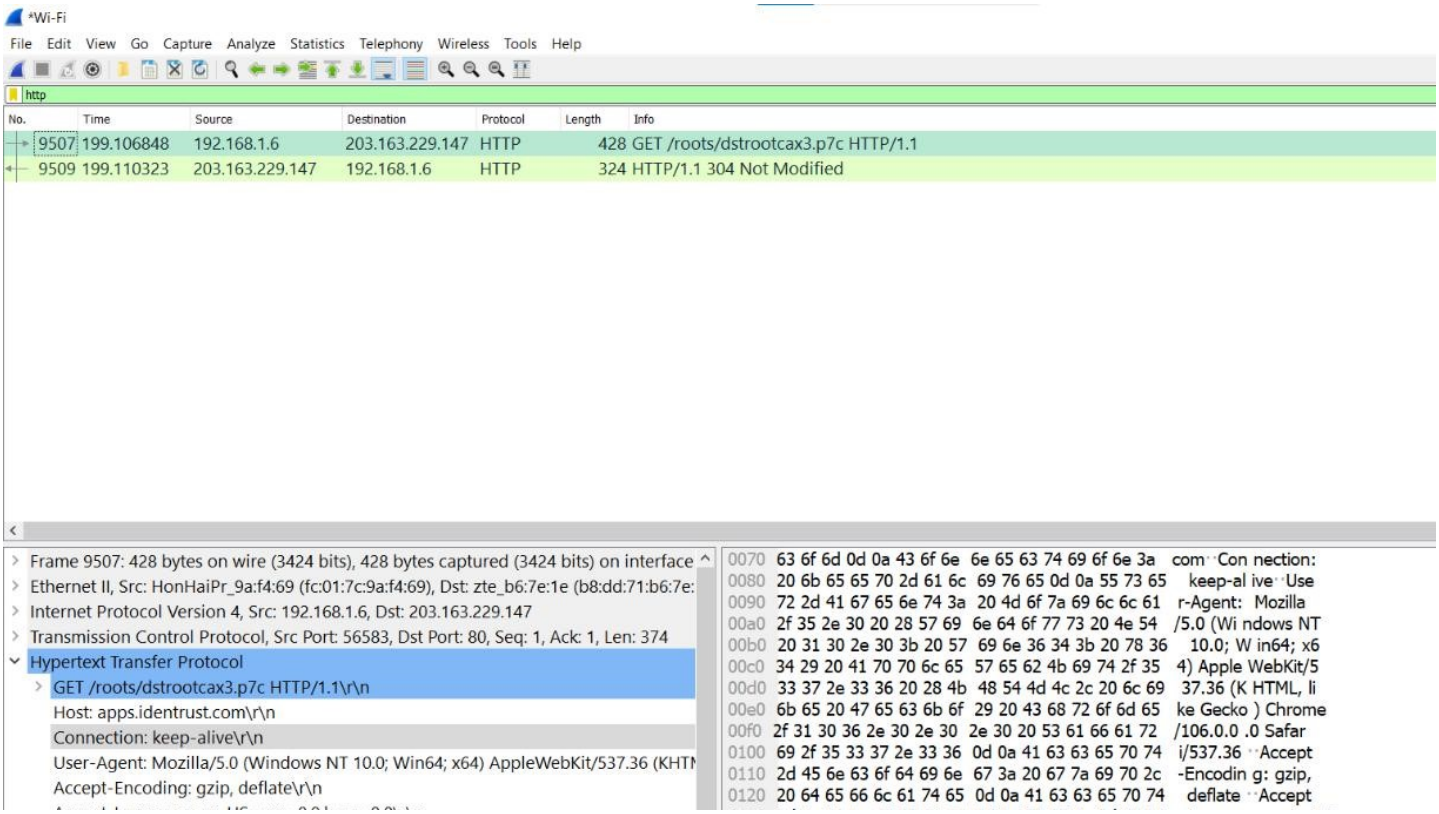
d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.



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

The above screenshot shows that the host's name is aps.identrust.com

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

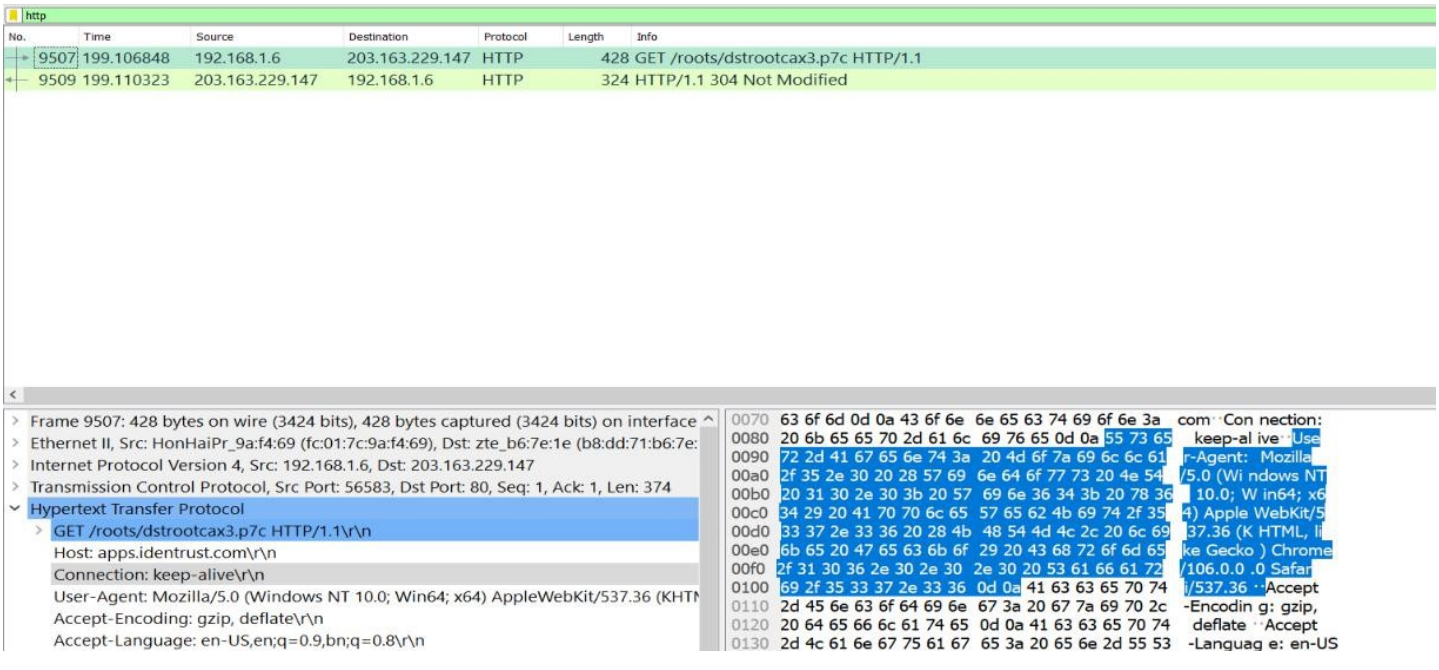


4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.

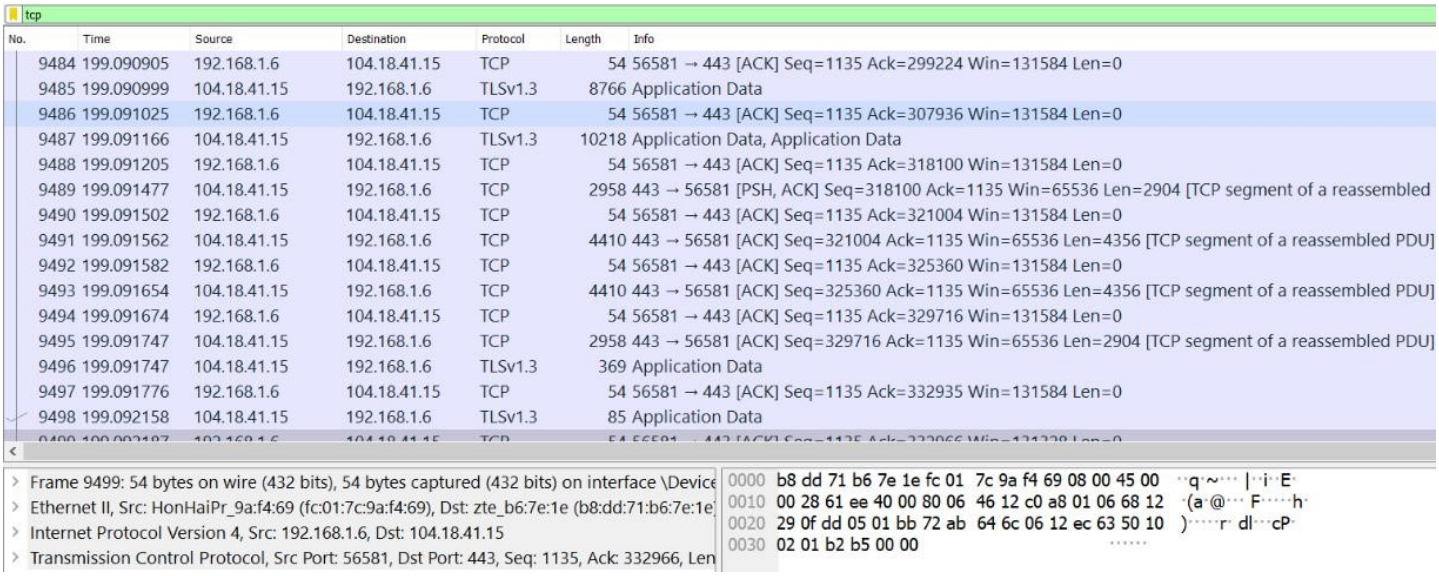
From the above screen shot it is visible that the first four bytes of the Host parameter from the packet's byte panel are: 49 66 2d 4d

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

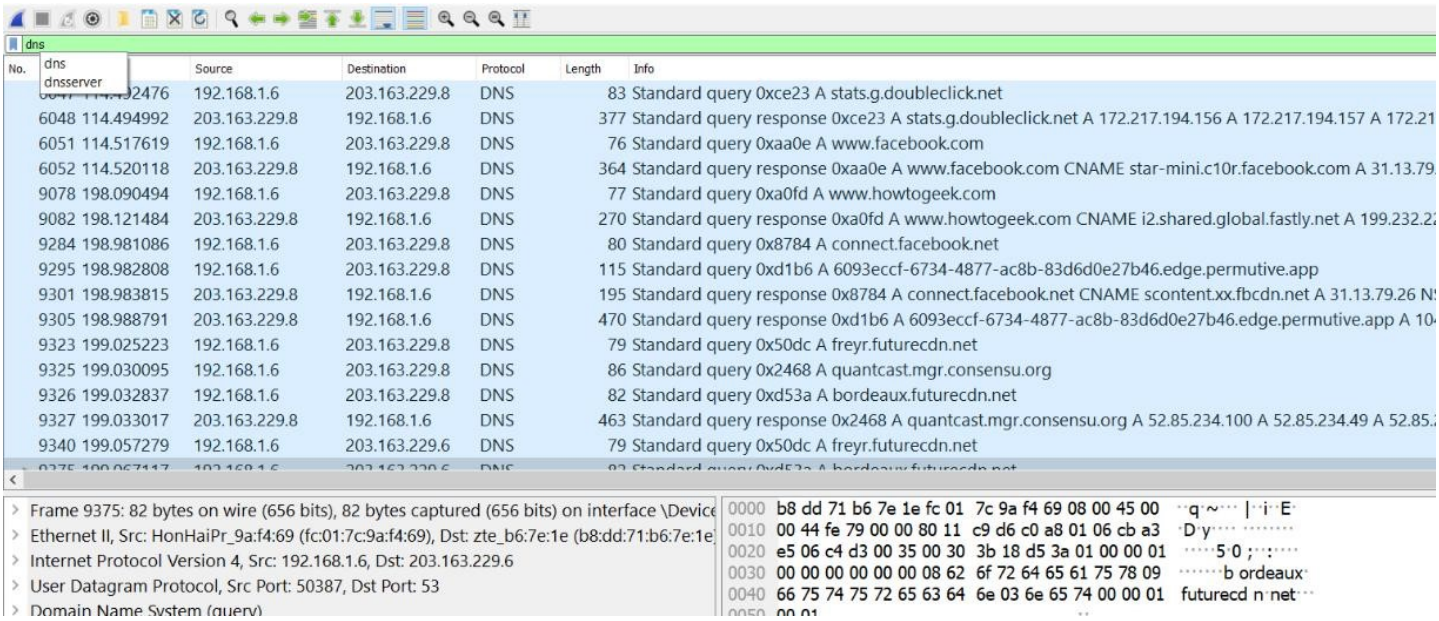
http:



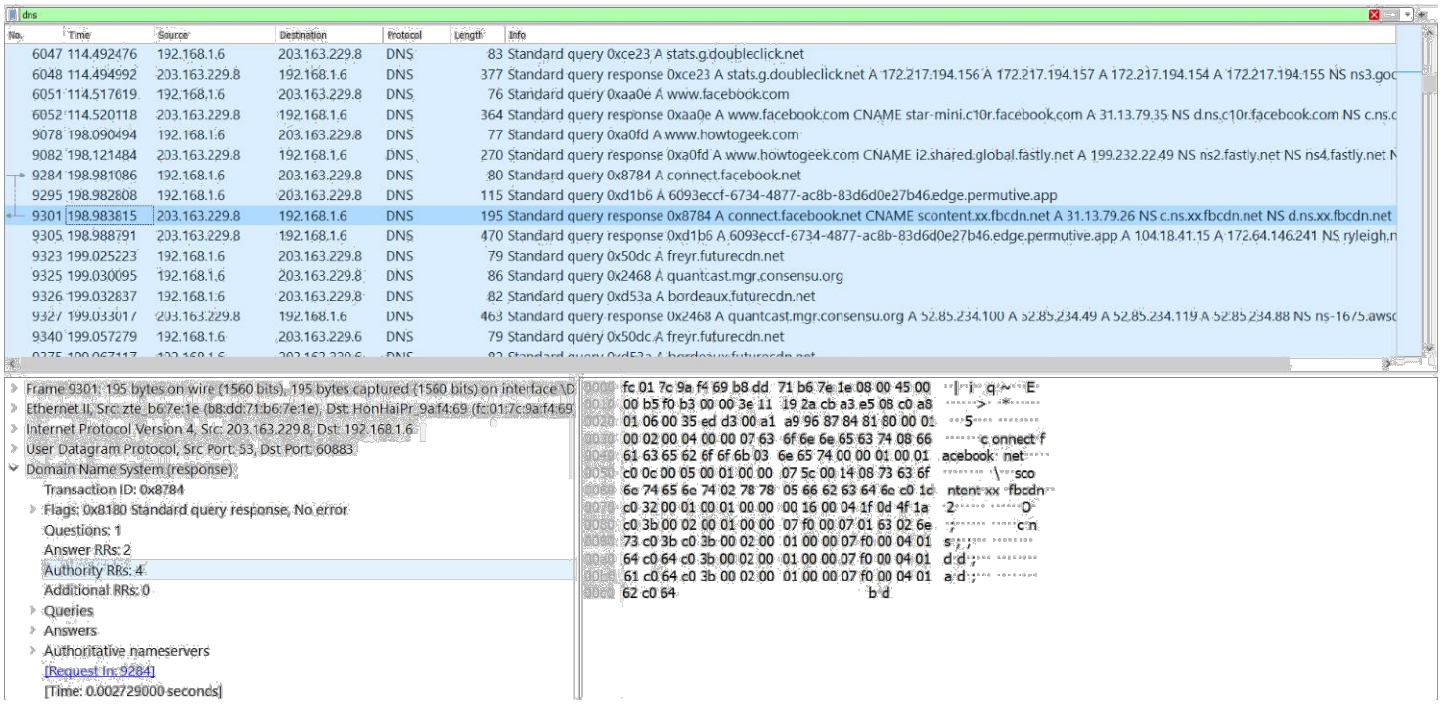
TCP:



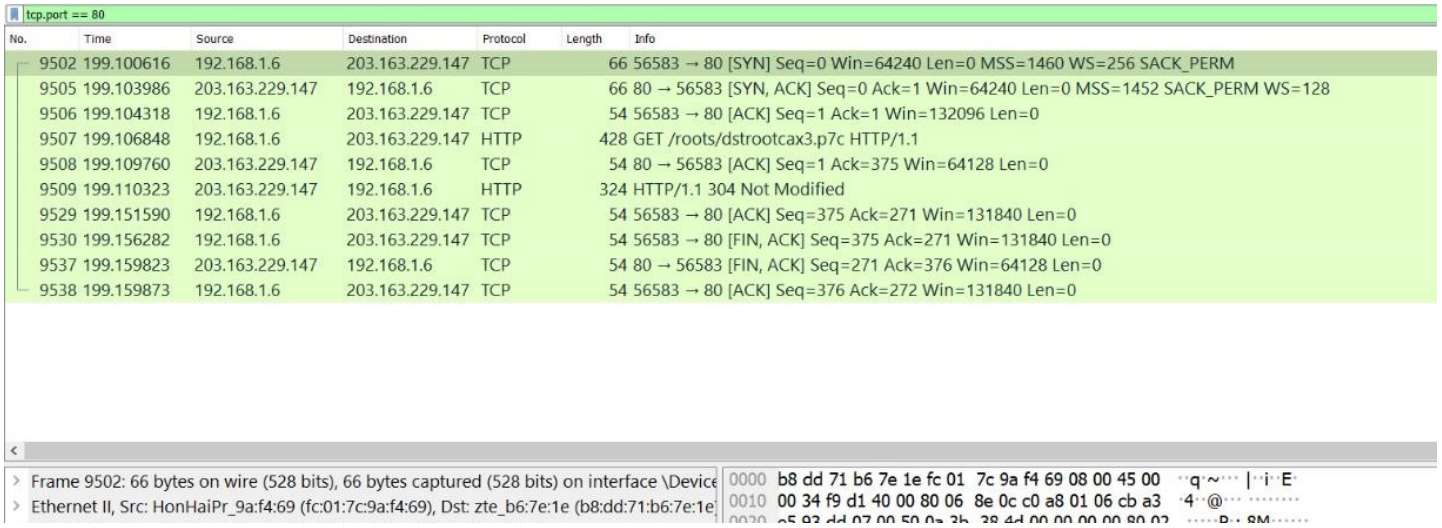
DNS:



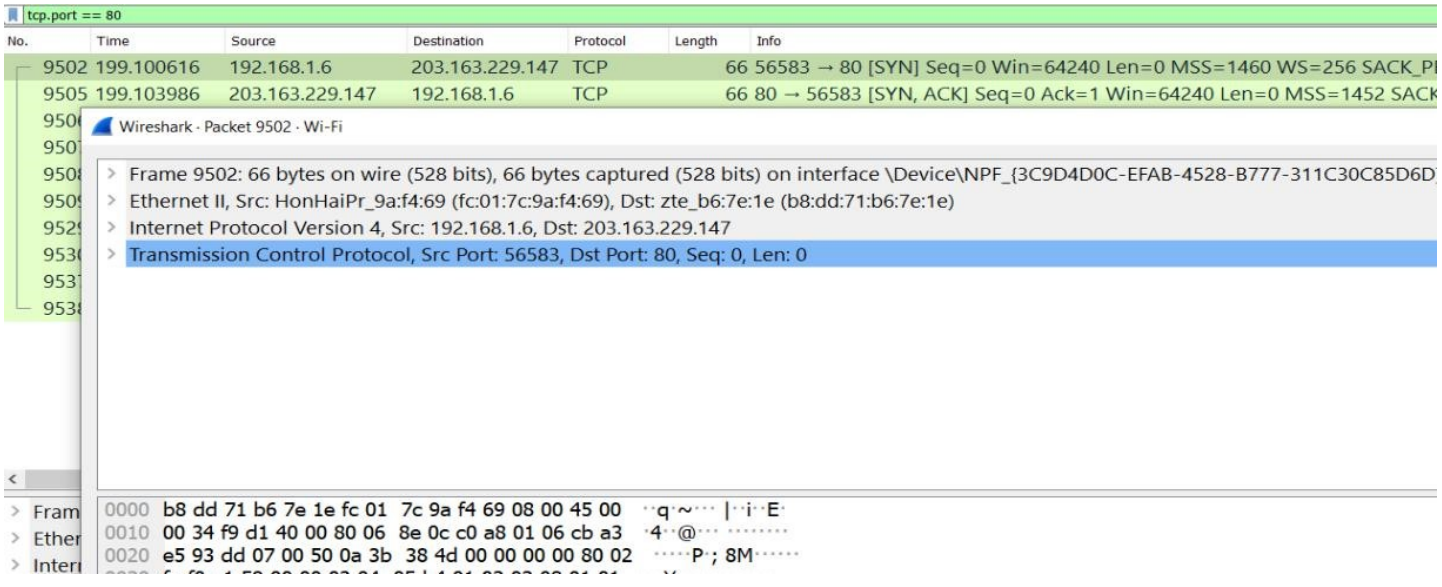
On selecting the packet of dns protocol, and on selecting follow UDP Stream for this packet, the following results are obtained.



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.



On expanding packet number 9502 in the Packet Details Panel, the following results are obtained.



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

Ethernet II, Src: HonHaiPr_9a:f4:69 (fc:01:7c:9a:f4:69), Dst: zte_b6:7e:1e (b8:dd:71:b6:7e:1e)

Manufacturer's NIC: - zte_b6:7e:1e (b8:dd:71:b6:7e:1e)

server's NIC :- HonHaipr_9a:f4:69 (fc:01:7c:9a:f4:69)

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

For Laptop's Manufacturer: - b8:dd:71:b6:7e:1e

For server's Manufacturer: - fc:01:7c:9a:f4:69 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?

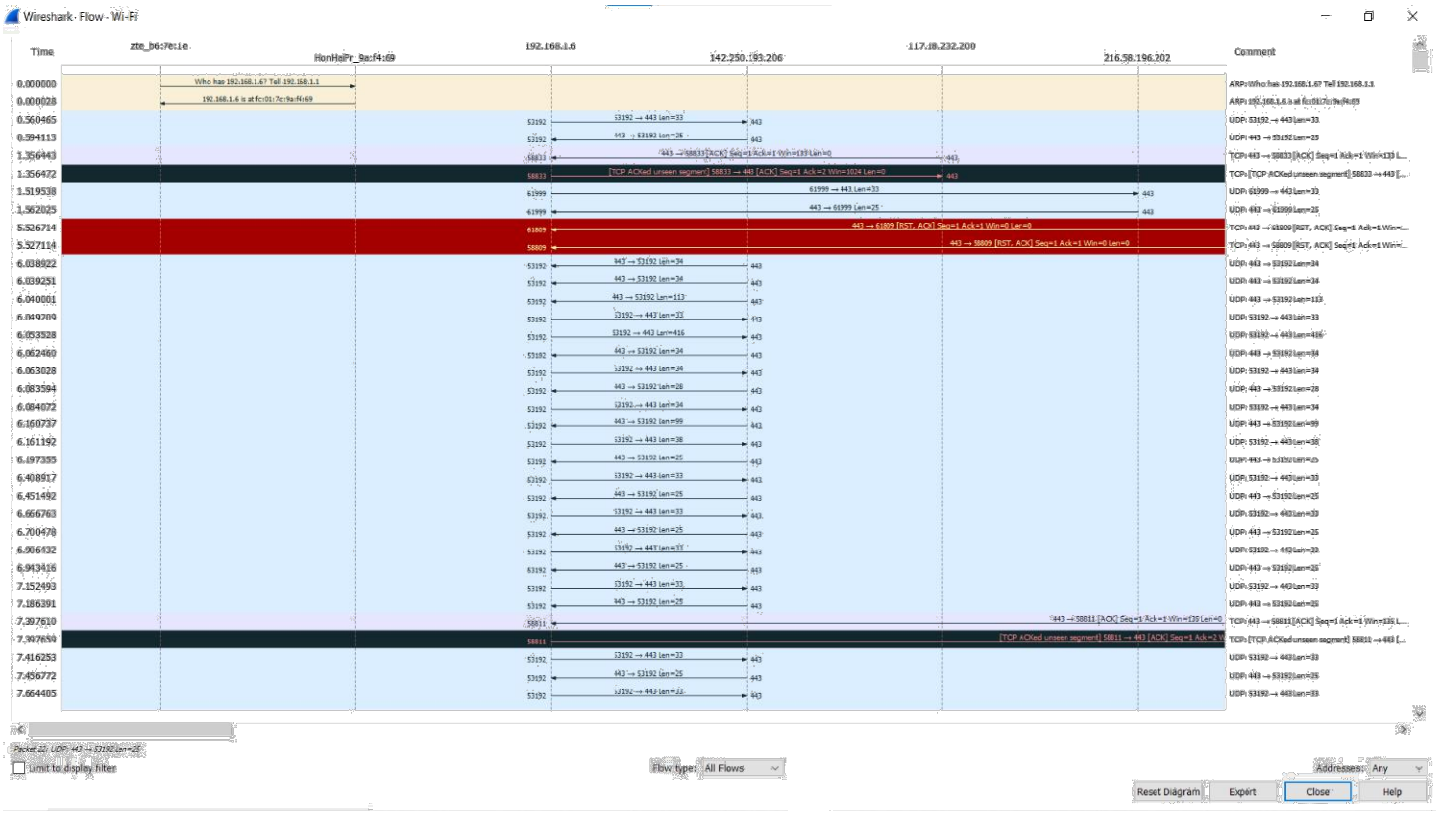
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
All Addresses	54978				0.1224	100%	10.0800
89.207.22.140	24				0.0001	0.04%	0.0800
89.207.22.137	25				0.0001	0.05%	0.1200
89.187.162.136	93				0.0002	0.17%	0.3100
85.114.159.118	19				0.0000	0.03%	0.0700
82.145.213.8	24				0.0001	0.04%	0.0600
80.77.87.216	163				0.0004	0.30%	0.1600
8.43.72.98	83				0.0002	0.15%	0.0900
8.2.111.124	331				0.0007	0.60%	0.2000
8.2.111.121	70				0.0002	0.13%	0.1300
8.2.110.134	40				0.0001	0.07%	0.1300
77.245.57.81	18				0.0000	0.03%	0.0700
77.245.57.72	19				0.0000	0.03%	0.0700

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

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
IP Protocol Types	6				0.0000	100%	0.0200
UDP	2				0.0000	33.33%	0.0100
NONE	4				0.0000	66.67%	0.0200

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 from General Flow and network source option of flow graphs:



Comments:

The entire assignment focuses on discovering the utility of the tool Wireshark. It helped in tracing and analysing packets and packet transfer respectively. Also helped to understand how packet transfer takes place following protocols like TCP, UDP, ARP etc. Looking forward to learning more tools like this.