

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.

No.	Protocol	Source	Destination	Length	Info
6622	ICMPv6	fe80::1	ff02::1	102	Router Advertisement from b8:dd:71:b6:7e:1e
66917	ICMPv6	fe80::1	ff02::1:ffff:0:ea0	86	Neighbor-Solicitation for fe80::1:ff02::1:ffff:0:ea0
61473	ICMPv6	fe80::38b2:fe90::a8	ff02::1	70	Router-Solicitation from 3a:b2:fe:90:0:ea0
61586	ICMPv6	fe80::1	ff02::1	102	Router Advertisement from b8:dd:71:b6:7e:1e

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
6196	118.117450	216.58.196.202	192.168.1.6	UDP	67	443 → 61999 Len=25

Frame 6622: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{DC9D400C-EfA8-4528-B777} (Intel PRO/100 MT Desktop\NPF_{DC9D400C-EfA8-4528-B777})
 Ethernet II, Src: zte_b6:7e:1e (b8:dd:71:b6:7e:1e), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 Internet Protocol Version 6. Src: fe80::1. Dst: ff02::1

0000	33 33 00 00 00 01	b8 dd 71 b6 7e 1e	86 dd 60 00	33.....q~`
0010	00 00 00 30 3a ff fe 80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0.....
0020	00 00 00 00 00 01 ff 02	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

- 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.)

No.	Time	Source	Destination	Protocol	Length	Info
→	9507 199.105848	192.168.1.6	203.163.229.147	HTTP	428	GET /roots/dstrootcax3.p7c HTTP/1.1
←	9509 199.110323	203.163.229.147	192.168.1.6	HTTP	324	HTTP/1.1 304 Not Modified

> Frame 9507: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface 'D	0070 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a com*Connection:
> Ethernet II, Src: Honhai-Pr [3a:f4:69] (fc:01:7c:9a:14:69), Dst: zte_b67e:7e (bb:dd:71:b6:7e:1e)	0080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0e 55 73 65 keep-alive:Use
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147	0081 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
> Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq 1, Ack: 1, Len: 372	0082 f5 35 2e 30 20 28 57 65 6e 64 6f 77 73 20 4e 54 /5.0 (Windows NT
> Hypertext Transfer Protocol	0083 20 31 30 2e 30 2b 57 69 6e 36 34 3b 20 78 36 10.0; WIn64; x6
	0084 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) AppleWebKit/5
	0085 33 37 2e 33 36 20 28 45 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
	0086 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 65 ke Gecko) Chrome
	0087 2f 31 30 36 2e 30 20 2e 30 20 53 61 66 61 72 /106.0.0.0 Safari
	0088 69 2f 35 33 37 2e 33 36 0d 04 41 63 63 65 70 74 /537.36 ·Accept
	0089 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2e ·Encoding: gzip,

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.

No.	Time	Source	Destination	Protocol	Length	Info
→ 9507	199.106848	192.168.1.6	203.163.229.147	HTTP	428	GET /roots/dstrootcac3.p7c HTTP/1.1
← 9509	199.110323	203.163.229.147	192.168.1.6	HTTP	324	HTTP/1.1 304 Not Modified

Frame 9507: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface ^	
> Ethernet II, Src: HonHaiPr_9a:f4:69 (fc:01:7c:9a:f4:69), Dst: zte_b6:7e:1e (b8:dd:71:b6:7e:1e)	00080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 com::Connection: keep-alive Use
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147	00090 72 2d 41 67 65 66 7e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
> Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq: 1, Ack: 1, Len: 374	000a0 2f 35 2e 30 20 28 57 69 6e 64 f7 77 73 20 4e 54 5.0 (Windows NT
> Hypertext Transfer Protocol	000b0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; Win64; x64
> GET /roots/dstrootcacx3.p7c HTTP/1.1\r\n	000c0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
Host: apps.identrust.com\r\n	000d0 33 37 2e 33 36 20 28 4b 48 54 54 4d 4c 2c 20 6c 69 37.36 (KHTML, li
Connection: keep-alive\r\n	000e0 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, i/106.0.0.0 Safari	000f0 2f 31 30 36 2e 30 2e 30 2e 30 20 53 61 66 61 72 i/537.36 ..Accept
Accept-Encoding: gzip, deflate\r\n	0100 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 -Encoding: gzip, deflate ..Accept
Accept-Language: en-US,en;q=0.9,br;q=0.8\r\n	0110 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 0120 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 -Language: en-US
	0130 2d 4c 61 6e 67 51 61 67 65 3a 20 65 6e 2d 55 53

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.

The screenshot shows the Wireshark interface with two captured HTTP packets. The first packet (No. 9507) is highlighted and expanded in the details and bytes panes. The bytes pane displays the raw hex and ASCII data for the selected packet, which corresponds to a GET request for "/roots/dstrootcax3.p7c". The ASCII pane shows the decoded HTTP headers and body.

No.	Time	Source	Destination	Protocol	Length	Info
+ 9507	199.106848	192.168.1.6	203.163.229.147	HTTP	428	GET /roots/dstrootcax3.p7c HTTP/1.1
- 9509	199.110323	203.163.229.147	192.168.1.6	HTTP	324	HTTP/1.1 304 Not Modified

```

Frame 9507: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface ^ 
Ethernet II, Src: HonHaiPr_9a:f4:69 (fc:01:7c:9a:f4:69), Dst: zte_b6:7e:1e (b8:dd:71:b6:7e:1)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147
Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq: 1, Ack: 1, Len: 374
Hypertext Transfer Protocol
    > GET /roots/dstrootcax3.p7c HTTP/1.1\r\n
        Host: apps.identrust.com\r\n
        Connection: keep-alive\r\n
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
        Accept-Encoding: gzip, deflate\r\n

```

0070	63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a	com 'Con nection:
0080	20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65	keep-al ive' Use
0090	72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61	r-Agent: Mozilla
00a0	0a 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54	/5.0 (Wi ndows NT
00b0	0b 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36	10.0; W in64; x6
00c0	0c 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35	4) Apple WebKit/5
00d0	0d 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69	37.36 (K HTML, li
00e0	0e 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65	ke Gecko) Chrome
00f0	0f 2f 31 30 36 2e 30 2e 30 2e 30 20 53 61 66 61 72	/106.0.0.0 Safar
0100	10 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74	i/537.36 ..Accept
0110	11 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c	-Encodin g: gzip,
0120	12 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74	deflate ..Accept

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:

The screenshot shows the Wireshark interface with two captured HTTP packets. The first packet (No. 9507) is highlighted and expanded in the details and bytes panes. The bytes pane displays the raw hex and ASCII data for the selected packet, which corresponds to a GET request for "/roots/dstrootcax3.p7c". The ASCII pane shows the decoded HTTP headers and body.

No.	Time	Source	Destination	Protocol	Length	Info
+ 9507	199.106848	192.168.1.6	203.163.229.147	HTTP	428	GET /roots/dstrootcax3.p7c HTTP/1.1
- 9509	199.110323	203.163.229.147	192.168.1.6	HTTP	324	HTTP/1.1 304 Not Modified

```

Frame 9507: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface ^ 
Ethernet II, Src: HonHaiPr_9a:f4:69 (fc:01:7c:9a:f4:69), Dst: zte_b6:7e:1e (b8:dd:71:b6:7e:1)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147
Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq: 1, Ack: 1, Len: 374
Hypertext Transfer Protocol
    > GET /roots/dstrootcax3.p7c HTTP/1.1\r\n
        Host: apps.identrust.com\r\n
        Connection: keep-alive\r\n
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n

```

0070	63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a	com 'Con nection:
0080	20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65	keep-al ive' Use
0090	72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61	r-Agent: Mozilla
00a0	0a 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54	/5.0 (Wi ndows NT
00b0	0b 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36	10.0; W in64; x6
00c0	0c 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35	4) Apple WebKit/5
00d0	0d 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69	37.36 (K HTML, li
00e0	0e 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65	ke Gecko) Chrome
00f0	0f 2f 31 30 36 2e 30 2e 30 2e 30 20 53 61 66 61 72	/106.0.0.0 Safar
0100	10 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74	i/537.36 ..Accept
0110	11 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c	-Encodin g: gzip,
0120	12 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74	deflate ..Accept
0130	13 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53	-Langug e: en-US

TCP:

No.	Time	Source	Destination	Protocol	Length	Info
9484 199.090905	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=299224 Win=131584 Len=0	
9485 199.090999	104.18.41.15	192.168.1.6	TLSv1.3	8766	Application Data	
9486 199.091025	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=307936 Win=131584 Len=0	
9487 199.091166	104.18.41.15	192.168.1.6	TLSv1.3	10218	Application Data, Application Data	
9488 199.091205	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=318100 Win=131584 Len=0	
9489 199.091477	104.18.41.15	192.168.1.6	TCP	2958	443 → 56581 [PSH, ACK] Seq=318100 Ack=1135 Win=65536 Len=2904 [TCP segment of a reassembled PDU]	
9490 199.091502	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=321004 Win=131584 Len=0	
9491 199.091562	104.18.41.15	192.168.1.6	TCP	4410	443 → 56581 [ACK] Seq=321004 Ack=1135 Win=65536 Len=4356 [TCP segment of a reassembled PDU]	
9492 199.091582	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=325360 Win=131584 Len=0	
9493 199.091654	104.18.41.15	192.168.1.6	TCP	4410	443 → 56581 [ACK] Seq=325360 Ack=1135 Win=65536 Len=4356 [TCP segment of a reassembled PDU]	
9494 199.091674	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=329716 Win=131584 Len=0	
9495 199.091747	104.18.41.15	192.168.1.6	TCP	2958	443 → 56581 [ACK] Seq=329716 Ack=1135 Win=65536 Len=2904 [TCP segment of a reassembled PDU]	
9496 199.091747	104.18.41.15	192.168.1.6	TLSv1.3	369	Application Data	
9497 199.091776	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=332935 Win=131584 Len=0	
9498 199.092158	104.18.41.15	192.168.1.6	TLSv1.3	85	Application Data	
0400 199.092187	192.168.1.6	104.18.41.15	TCP	54	56581 → 443 [ACK] Seq=1135 Ack=332966 Win=131584 Len=0	

DNS:

No.	dns	Source	Destination	Protocol	Length	Info
0000 114.492476	dnsserver	192.168.1.6	203.163.229.8	DNS	83	Standard query 0xce23 A stats.g.doubleclick.net
0048 114.494992		203.163.229.8	192.168.1.6	DNS	377	Standard query response 0xce23 A stats.g.doubleclick.net A 172.217.194.156 A 172.217.194.157 A 172.21
0051 114.517619		192.168.1.6	203.163.229.8	DNS	76	Standard query 0xaa0e A www.facebook.com
0052 114.520118		203.163.229.8	192.168.1.6	DNS	364	Standard query response 0xaa0e A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.79.
0078 198.090494		192.168.1.6	203.163.229.8	DNS	77	Standard query 0xa0fd A www.howtogeek.com
0082 198.121484		203.163.229.8	192.168.1.6	DNS	270	Standard query response 0xa0fd A www.howtogeek.com CNAME i2.shared.global.fastly.net A 199.232.2
0284 198.981086		192.168.1.6	203.163.229.8	DNS	80	Standard query 0x8784 A connect.facebook.net
0295 198.982808		192.168.1.6	203.163.229.8	DNS	115	Standard query 0xd1b6 A 6093eccf-6734-4877-ac8b-83d6d0e27b46.edge.permutive.app
0301 198.983815		203.163.229.8	192.168.1.6	DNS	195	Standard query response 0x8784 A connect.facebook.net CNAME scontent.xx.fbcdn.net A 31.13.79.26 N
0305 198.988791		203.163.229.8	192.168.1.6	DNS	470	Standard query response 0xd1b6 A 6093eccf-6734-4877-ac8b-83d6d0e27b46.edge.permutive.app A 10-
0323 199.025223		192.168.1.6	203.163.229.8	DNS	79	Standard query 0x50dc A freyr.futurecdn.net
0325 199.030095		192.168.1.6	203.163.229.8	DNS	86	Standard query 0x2468 A quantcast.mgr.consenso.org
0326 199.032837		192.168.1.6	203.163.229.8	DNS	82	Standard query 0xd53a A bordeaux.futurecdn.net
0327 199.033017		203.163.229.8	192.168.1.6	DNS	463	Standard query response 0x2468 A quantcast.mgr.consenso.org A 52.85.234.100 A 52.85.234.49 A 52.85.
0340 199.057279		192.168.1.6	203.163.229.6	DNS	79	Standard query 0x50dc A freyr.futurecdn.net
0375 199.067117		192.168.1.6	203.163.229.6	DNS	82	Standard query 0xd53a A bordeaux.futurecdn.net

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

Wireshark - dns

No.	Time	Source	Destination	Protocol	Length	Info
6047	114.492476	192.168.1.6	203.163.229.8	DNS	83	Standard query 0x2e23 A stats.g.doubleclick.net
6048	114.494992	203.163.229.8	192.168.1.6	DNS	377	Standard query response 0x2e23 A stats.g.doubleclick.net A 172.217.194.156 & 172.217.194.157 A 172.217.194.154 A 172.217.194.155 NS ns3.google.com
6051	114.517619	192.168.1.6	203.163.229.8	DNS	76	Standard query 0xa0e A www.facebook.com
6052	114.520118	203.163.229.8	192.168.1.6	DNS	364	Standard query response 0xa0e A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.79.35 NS dns.c10r.facebook.com NS c.nse.facebook.com
9078	198.090494	192.168.1.6	203.163.229.8	DNS	77	Standard query 0xa0fd A www.howtogeek.com
9082	198.121484	203.163.229.8	192.168.1.6	DNS	270	Standard query response 0xa0fd A www.howtogeek.com CNAME i2.shared.global.fastly.net A 199.232.22.49 NS ns2.fastly.net NS ns4.fastly.net N
9284	198.981086	192.168.1.6	203.163.229.8	DNS	80	Standard query 0x8784 A connect.facebook.net
9295	198.982608	192.168.1.6	203.163.229.8	DNS	115	Standard query 0xd1b6 A 6093eccf-6734-4877-ac8b-83d6d0e27b46.edge.permutive.app
9301	198.983615	203.163.229.8	192.168.1.6	DNS	195	Standard query response 0x8784 A connect.facebook.net CNAME scontent.xx.fbcdn.net A 31.13.79.26 NS c.ns.xx.fbcdn.net NS d.ns.xx.fbcdn.net
9305	198.988791	203.163.229.8	192.168.1.6	DNS	470	Standard query response 0xd1b6 A 6093eccf-6734-4877-ac8b-83d6d0e27b46.edge.permutive.app A 104.18.41.15 A 172.64.146.241 NS rleigh.net
9323	199.025223	192.168.1.6	203.163.229.8	DNS	79	Standard query 0x50dc A freyr.futurecdn.net
9325	199.030095	192.168.1.6	203.163.229.8	DNS	86	Standard query 0x2468 A quantcast.mgr.consu.org
9326	199.032637	192.168.1.6	203.163.229.8	DNS	82	Standard query 0x53a A bordeaux.futurecdn.net
9327	199.033017	203.163.229.8	192.168.1.6	DNS	463	Standard query response 0x2468 A quantcast.mgr.consu.org A 52.85.234.100 A 52.85.234.49 A 52.85.234.119 A 52.85.234.88 NS ns-16/5.awso.net
9340	199.057279	192.168.1.6	203.163.229.6	DNS	79	Standard query 0x50dc A freyr.futurecdn.net
9375	199.067117	192.168.1.6	203.163.229.6	DNS	92	Standard query 0x50dc A headersfuturecdn.net

Frame 9301: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface \Device\NPF_{3C9D4D0C-EFAB-4528-B777-311C30C85D6D

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

Internet Protocol Version 4, Src: 203.163.229.8, Dst: 192.168.1.6

User Datagram Protocol, Src Port: 53, Dst Port: 60883

Domain Name System (resolved):

- Transaction ID: 0x8784
- Flags: 0x8100 Standard query response, No error
- Questions: 1
- Answer RRs: 2
- Authority RRs: 4
- Additional RRs: 0

Queries:

Answers:

Authoritative nameservers

[Request In: #284]

[Time: 0.002729000 seconds]

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

No.	Time	Source	Destination	Protocol	Length	Info
9502	199.100616	192.168.1.6	203.163.229.147	TCP	66	56583 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9505	199.103986	203.163.229.147	192.168.1.6	TCP	66	80 → 56583 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
9506	199.104318	192.168.1.6	203.163.229.147	TCP	54	56583 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
9507	199.106848	192.168.1.6	203.163.229.147	HTTP	428	GET /roots/dstrootcax3.p7c HTTP/1.1
9508	199.109760	203.163.229.147	192.168.1.6	TCP	54	80 → 56583 [ACK] Seq=1 Ack=375 Win=64128 Len=0
9509	199.110323	203.163.229.147	192.168.1.6	HTTP	324	HTTP/1.1 304 Not Modified
9529	199.151590	192.168.1.6	203.163.229.147	TCP	54	56583 → 80 [ACK] Seq=375 Ack=271 Win=131840 Len=0
9530	199.156282	192.168.1.6	203.163.229.147	TCP	54	56583 → 80 [FIN, ACK] Seq=375 Ack=271 Win=131840 Len=0
9537	199.159823	203.163.229.147	192.168.1.6	TCP	54	80 → 56583 [FIN, ACK] Seq=271 Ack=376 Win=64128 Len=0
9538	199.159873	192.168.1.6	203.163.229.147	TCP	54	56583 → 80 [ACK] Seq=376 Ack=272 Win=131840 Len=0

Frame 9502: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3C9D4D0C-EFAB-4528-B777-311C30C85D6D

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

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

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
9502	199.100616	192.168.1.6	203.163.229.147	TCP	66	56583 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9505	199.103986	203.163.229.147	192.168.1.6	TCP	66	80 → 56583 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM

Wireshark - Packet 9502 - Wi-Fi

Frame 9502: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3C9D4D0C-EFAB-4528-B777-311C30C85D6D

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

Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147

Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq: 0, Len: 0

Frame 9502: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3C9D4D0C-EFAB-4528-B777-311C30C85D6D

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

Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.163.229.147

Transmission Control Protocol, Src Port: 56583, Dst Port: 80, Seq: 0, Len: 0

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

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?

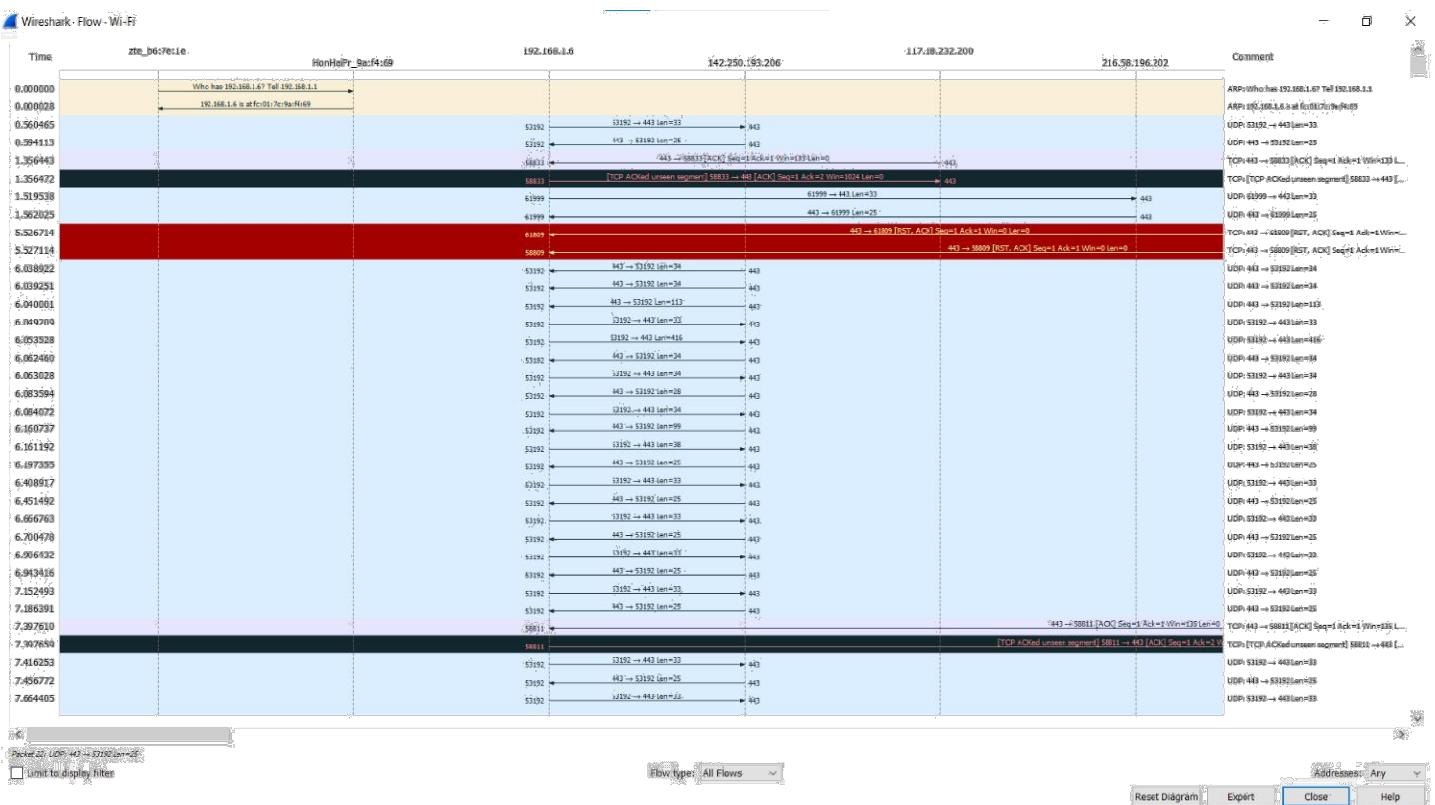
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
▼ All Addresses	54978				0.1224	100%	10.0800
89.207.22.140	24				0.0001	0.04%	0.0800
89.207.22.137	25				0.0001	0.05%	0.1200
89.187.162.136	93				0.0002	0.17%	0.3100
85.114.159.118	19				0.0000	0.03%	0.0700
82.145.213.8	24				0.0001	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.