ASSIGNMENT 5

Name: Imon Raj
Class: BCSE III
Roll: 002010501098
Section: A3
Subject: Computer Networks Lab Report

PROBLEM STATEMENT: **Install Wireshark in local machine and do traffic and packet analysis according to the given questions**

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

Answer:

```
PS C:\Users\hp> ping 192.168.29.27

Pinging 192.168.29.27 with 32 bytes of data:
Reply from 192.168.29.27: bytes=32 time=253ms TTL=64
Reply from 192.168.29.27: bytes=32 time=288ms TTL=64
Reply from 192.168.29.27: bytes=32 time=85ms TTL=64
Reply from 192.168.29.27: bytes=32 time=103ms TTL=64

Ping statistics for 192.168.29.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 85ms, Maximum = 288ms, Average = 182ms
PS C:\Users\hp> ping 192.168.29.27

Pinging 192.168.29.27 with 32 bytes of data:
Reply from 192.168.29.27: bytes=32 time=195ms TTL=64
Reply from 192.168.29.27: bytes=32 time=213ms TTL=64
Reply from 192.168.29.27: bytes=32 time=234ms TTL=64
Reply from 192.168.29.27: bytes=32 time=245ms TTL=64

Ping statistics for 192.168.29.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 195ms, Maximum = 245ms, Average = 221ms
```

Source	Destination	Protocol	Length	Info
AzureWav_68:10:67	b2:2a:7f:38:2b:17	ARP	42	Who has 192.168.29.27? Tell 192.168.29.243
b2:2a:7f:38:2b:17	AzureWav_68:10:67	ARP	42	192.168.29.27 is at b2:2a:7f:38:2b:17

No.	Time	Source	Destination	Protocol	Length	Info
21	0.7192…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 61)
61	0.9728…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 21)
138	1.7313…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 139)
139	2.0193…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 138)
140	2.7388…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 141)
141	2.8241…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=64 (request in 140)
142	3.7451…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 143)
143	3.8483…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=64 (request in 142)
148	5.9035…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 149)
149	6.0983…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 148)
150	6.9099…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 151)
151	7.1225…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 150)
152	7.9147…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 153)
153	8.1486…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 152)
157	8.9197…	192.168.29.243	192.168.29.27	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 161)
161	9.1645…	192.168.29.27	192.168.29.243	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 157)

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.

Ans:

192.168.29.243	136.232.79.144	HTTP	586	GET /jums_exam/misc/footer.js
136.232.79.144	192.168.29.243	HTTP	384	HTTP/1.1 200 OK (text/html)
192.168.29.243	136.232.79.144	TCP	54	2942 → 80 [ACK] Seq=1050 Ack=
85.14.245.45	192.168.29.243	TCP	66	443 → 2940 [SYN, ACK] Seq=0 A
192.168.29.243	85.14.245.45	TCP	54	2940 → 443 [ACK] Seq=1 Ack=1
192.168.29.243	136.232.79.144	TCP	54	2939 → 80 [ACK] Seq=1680 Ack=
192.168.29.243	85.14.245.45	TLSv1.3	571	Client Hello
85.14.245.45	192.168.29.243	TCP	54	443 → 2940 [ACK] Seq=1 Ack=51
85.14.245.45	192.168.29.243	TLSv1.3	298	Server Hello, Change Cipher S

The different protocols I can see are – HTTP, TCP, TLS, TLSv1.3 etc.

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.)

ans:

Time	Source	Destination	Protocol	Length	Info
12.932066	192.168.29.243	136.232.79.144	HTTP	700	GET /jums_exam/student_odd_2023
13.092242	136.232.79.144	192.168.29.243	HTTP	130	HTTP/1.1 200 OK (text/html)

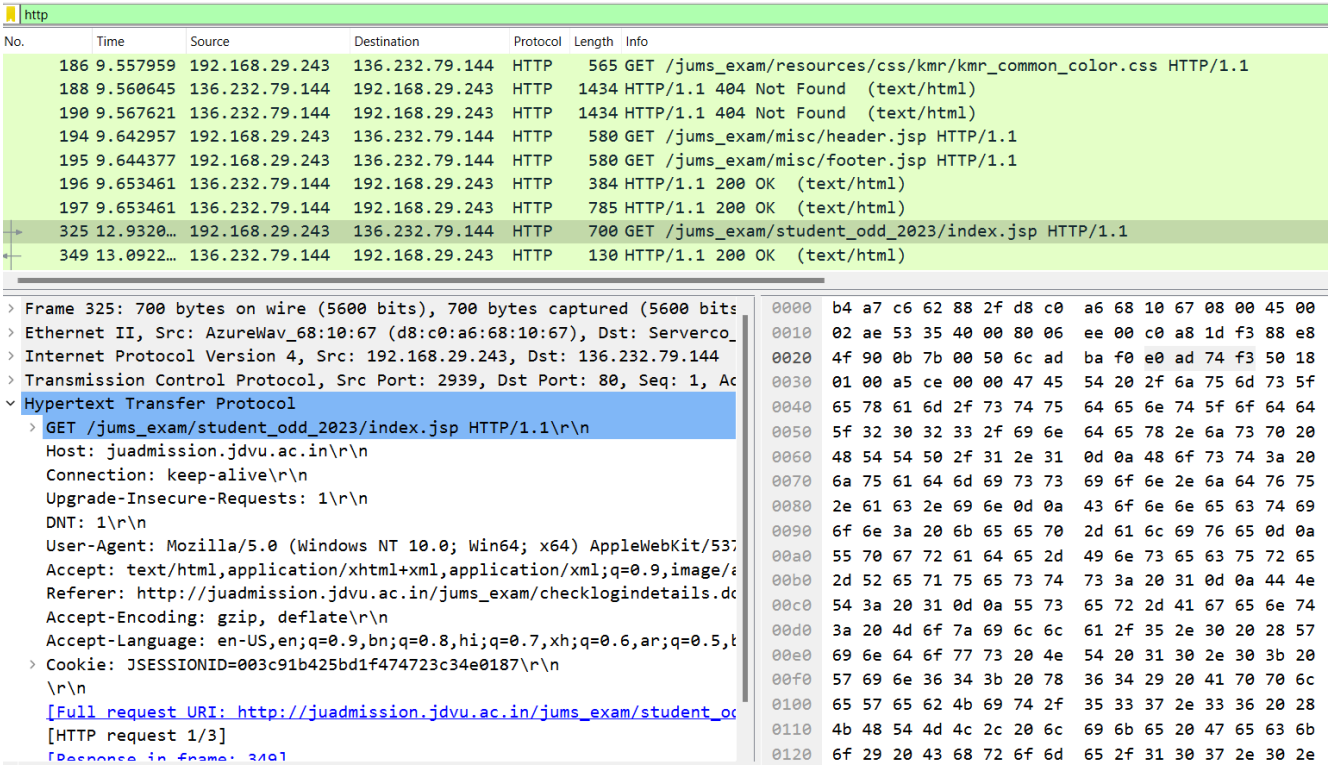
As we can see, that GET message was sent in time 12.932066 and OK response was received in time 13.092242. So the time taken is – (13.092242-12.932066) = 0.160176 seconds.

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

Ans: From the previous screenshot, we can see that the internet(IP) address of the website is – 136.232.79.144 and IP address of my computer is – 192.168.29.243.

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.

Ans:



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

Ans: The value of host from the previous screenshot is – juadmission.jdvu.ac.in

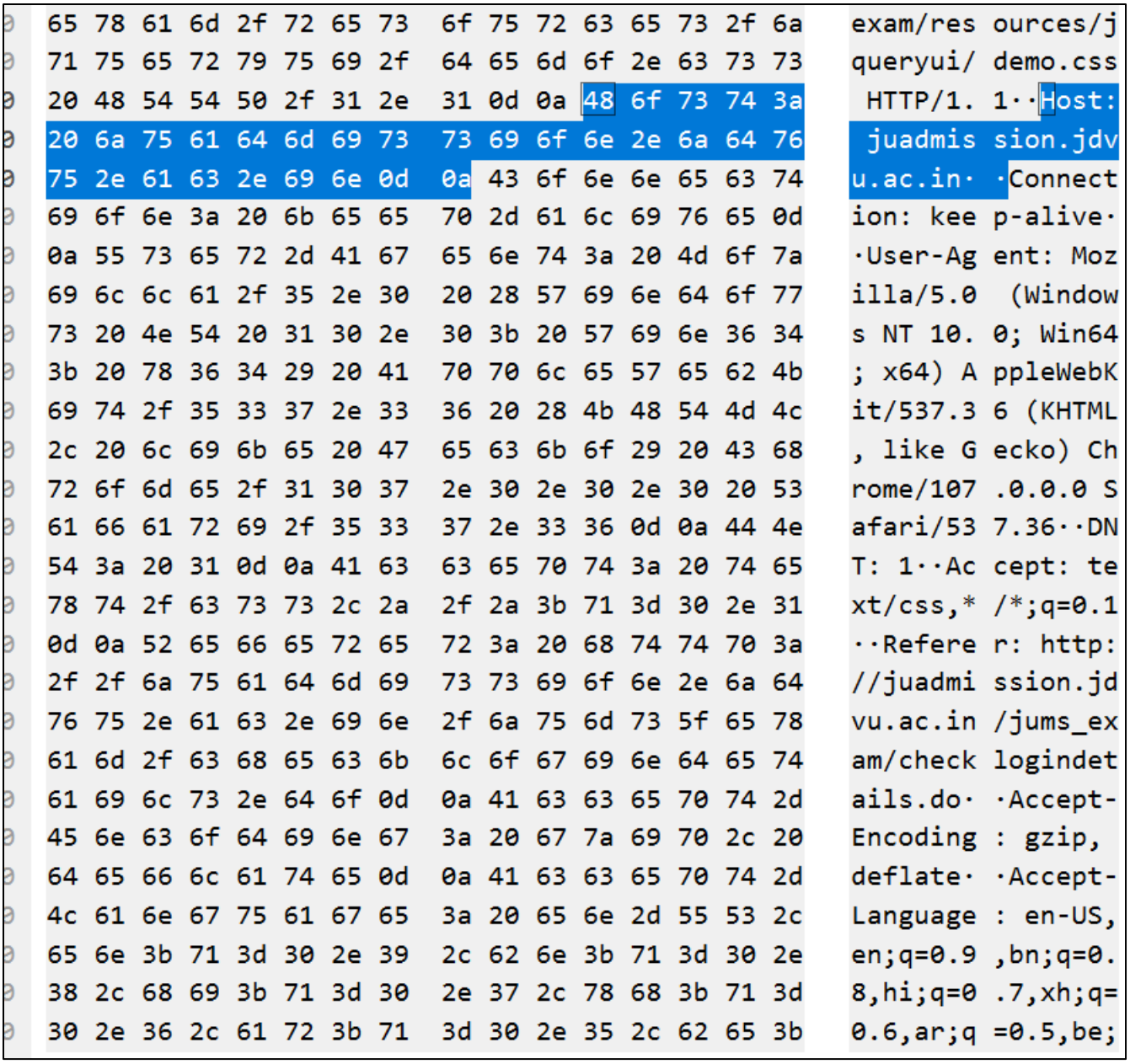
3.) Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel

ANS:

```
b4 a7 c6 62 88 2f d8 c0  a6 68 10 67 08 00 45 00   ···b·/·· ·h·g··E·
02 1c 53 1f 40 00 80 06  ee a8 c0 a8 1d f3 88 e8   ··S·@··· ········
4f 90 0b 71 00 50 e5 bb  21 09 cb 66 80 f3 50 18   O··q·P·· !··f··P·
01 00 33 27 00 00 47 45  54 20 2f 6a 75 6d 73 5f   ··3'··GE T /jums_
65 78 61 6d 2f 72 65 73  6f 75 72 63 65 73 2f 6a   exam/res ources/j
71 75 65 72 79 75 69 2f  64 65 6d 6f 2e 63 73 73   queryui/ demo.css
20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
20 6a 75 61 64 6d 69 73  73 69 6f 6e 2e 6a 64 76    juadmis sion.jdv
75 2e 61 63 2e 69 6e 0d  0a 43 6f 6e 6e 65 63 74   u.ac.in· ·Connect
69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
72 6f 6d 65 2f 31 30 37  2e 30 2e 30 2e 30 20 53   rome/107 .0.0.0 S
61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 44 4e   afari/53 7.36··DN
54 3a 20 31 0d 0a 41 63  63 65 70 74 3a 20 74 65   T: 1··Ac cept: te
78 74 2f 63 73 73 2c 2a  2f 2a 3b 71 3d 30 2e 31   xt/css,* /*;q=0.1
0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: http:
2f 2f 6a 75 61 64 6d 69  73 73 69 6f 6e 2e 6a 64   //juadmi ssion.jd
76 75 2e 61 63 2e 69 6e  2f 6a 75 6d 73 5f 65 78   vu.ac.in /jums_ex
61 6d 2f 63 68 65 63 6b  6c 6f 67 69 6e 64 65 74   am/check logindet
61 69 6c 73 2e 64 6f 0d  0a 41 63 63 65 70 74 2d   ails.do· ·Accept-
45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
```

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

Ans:



```
65 78 61 6d 2f 72 65 73  6f 75 72 63 65 73 2f 6a   exam/res ources/j
71 75 65 72 79 75 69 2f  64 65 6d 6f 2e 63 73 73   queryui/ demo.css
20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
20 6a 75 61 64 6d 69 73  73 69 6f 6e 2e 6a 64 76   juadmis sion.jdv
75 2e 61 63 2e 69 6e 0d  0a 43 6f 6e 6e 65 63 74   u.ac.in· ·Connect
69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
72 6f 6d 65 2f 31 30 37  2e 30 2e 30 2e 30 20 53   rome/107 .0.0.0 S
61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 44 4e   afari/53 7.36··DN
54 3a 20 31 0d 0a 41 63  63 65 70 74 3a 20 74 65   T: 1··Ac cept: te
78 74 2f 63 73 73 2c 2a  2f 2a 3b 71 3d 30 2e 31   xt/css,* /*;q=0.1
0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: http:
2f 2f 6a 75 61 64 6d 69  73 73 69 6f 6e 2e 6a 64   //juadmi ssion.jd
76 75 2e 61 63 2e 69 6e  2f 6a 75 6d 73 5f 65 78   vu.ac.in /jums_ex
61 6d 2f 63 68 65 63 6b  6c 6f 67 69 6e 64 65 74   am/check logindet
61 69 6c 73 2e 64 6f 0d  0a 41 63 63 65 70 74 2d   ails.do· ·Accept-
45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
65 6e 3b 71 3d 30 2e 39  2c 62 6e 3b 71 3d 30 2e   en;q=0.9 ,bn;q=0.
38 2c 68 69 3b 71 3d 30  2e 37 2c 78 68 3b 71 3d   8,hi;q=0 .7,xh;q=
30 2e 36 2c 61 72 3b 71  3d 30 2e 35 2c 62 65 3b   0.6,ar;q =0.5,be;
```

As we can see first four bytes of the Hex value of the Host parameter is: 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

Ans:

TCP:

Source	Destination	Protocol	Length	Info
192.168.29.243	140.82.114.25	TCP	55	2561 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segm
140.82.114.25	192.168.29.243	TCP	66	443 → 2561 [ACK] Seq=1 Ack=2 Win=70 Len=0 SLE=1 SRE=
192.168.29.243	85.14.245.45	TCP	54	2924 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
192.168.29.243	85.14.245.45	TCP	54	2923 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85.14.245.45	192.168.29.243	TCP	54	443 → 2924 [FIN, ACK] Seq=25 Ack=2 Win=501 Len=0
192.168.29.243	85.14.245.45	TCP	54	2924 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
192.168.29.243	136.232.79.144	TCP	66	2929 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
192.168.29.243	136.232.79.144	TCP	66	2930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
136.232.79.144	192.168.29.243	TCP	66	80 → 2929 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
136.232.79.144	192.168.29.243	TCP	66	80 → 2930 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
192.168.29.243	136.232.79.144	TCP	54	2929 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.29.243	136.232.79.144	TCP	54	2930 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
136.232.79.144	192.168.29.243	TCP	54	80 → 2929 [ACK] Seq=1 Ack=584 Win=30464 Len=0
136.232.79.144	192.168.29.243	TCP	1514	80 → 2929 [ACK] Seq=1 Ack=584 Win=30464 Len=1460 [TC
136.232.79.144	192.168.29.243	TCP	1514	80 → 2929 [ACK] Seq=1461 Ack=584 Win=30464 Len=1460

DNS:

Source	Destination	Protocol	Length	Info
2405:201:8012:…	2405:201:8012:…	DNS	91	Standard query 0xbac4 A cssdeck.com
2405:201:8012:…	2405:201:8012:…	DNS	91	Standard query 0x6383 AAAA cssdeck.com
2405:201:8012:…	2405:201:8012:…	DNS	91	Standard query 0x188a HTTPS cssdeck.com
2405:201:8012:…	2405:201:8012:…	DNS	123	Standard query response 0xbac4 A cssdeck.com A 172.67.162.
2405:201:8012:…	2405:201:8012:…	DNS	119	Standard query response 0x6383 AAAA cssdeck.com AAAA 2606:
2405:201:8012:…	2405:201:8012:…	DNS	142	Standard query response 0x188a HTTPS cssdeck.com HTTPS
2405:201:8012:…	2405:201:8012:…	DNS	98	Standard query 0x4ae8 A www.jaduniv.edu.in
2405:201:8012:…	2405:201:8012:…	DNS	98	Standard query 0xdb05 AAAA www.jaduniv.edu.in
2405:201:8012:…	2405:201:8012:…	DNS	98	Standard query 0x0e9c HTTPS www.jaduniv.edu.in
2405:201:8012:…	2405:201:8012:…	DNS	114	Standard query response 0x4ae8 A www.jaduniv.edu.in A 136.
2405:201:8012:…	2405:201:8012:…	DNS	169	Standard query response 0xdb05 AAAA www.jaduniv.edu.in SOA
2405:201:8012:…	2405:201:8012:…	DNS	169	Standard query response 0x0e9c HTTPS www.jaduniv.edu.in SO
2405:201:8012:…	2405:201:8012:…	DNS	109	Standard query 0xaf2e A d27xxe7juh1us6.cloudfront.net
2405:201:8012:…	2405:201:8012:…	DNS	109	Standard query 0xe864 AAAA d27xxe7juh1us6.cloudfront.net
2405:201:8012:…	2405:201:8012:…	DNS	109	Standard query 0x76f8 HTTPS d27xxe7juh1us6.cloudfront.net
2405:201:8012:…	2405:201:8012:…	DNS	189	Standard query response 0xe864 AAAA d27xxe7juh1us6.cloudfr
2405:201:8012:…	2405:201:8012:…	DNS	189	Standard query response 0x76f8 HTTPS d27xxe7juh1us6.cloudf
2405:201:8012:…	2405:201:8012:…	DNS	173	Standard query response 0xaf2e A d27xxe7juh1us6.cloudfront

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 in the Packet Details Panel, the following results are obtained.

```
Frame 67: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface
  Section number: 1
> Interface id: 0 (\Device\NPF_{A1D23659-979B-4254-9862-F6ECA398591B})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 19, 2022 19:37:12.088244000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1668866832.088244000 seconds
  [Time delta from previous captured frame: 0.001353000 seconds]
  [Time delta from previous displayed frame: 0.034173000 seconds]
  [Time since reference or first frame: 4.026843000 seconds]
  Frame Number: 67
  Frame Length: 521 bytes (4168 bits)
  Capture Length: 521 bytes (4168 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

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

Ans:

```
> Destination: Serverco_62:88:2f (b4:a7:c6:62:88:2f)
> Source: AzureWav_68:10:67 (d8:c0:a6:68:10:67)
```

Manufacturer's NIC: AzureWav_68:10:67 (d8:c0:a6:68:10:67)

Server's NIC: Serverco_62:88:2f (b4:a7:c6:62:88:2f)

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

Ans:

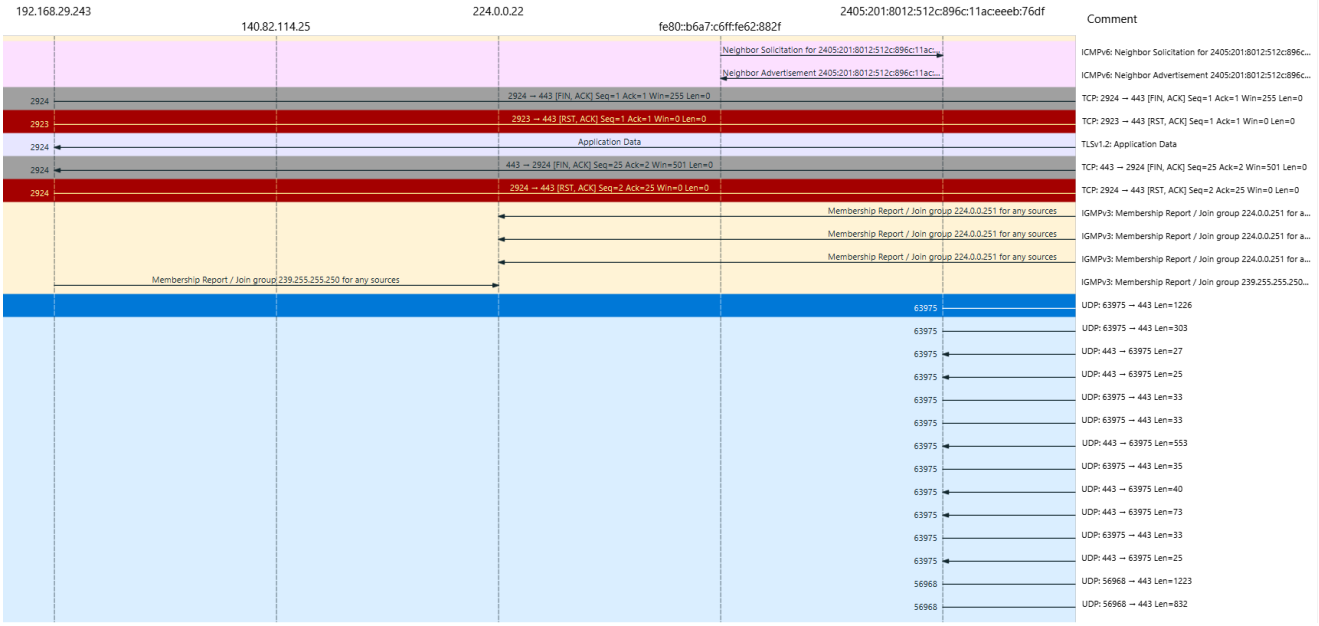
For Laptop's Manufacturer :- d8:c0:a6:68:10:67

For server's Manufacturer :- b4:a7:c6:62:88:2f

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

Ans:

Graph Obtained from General Flow and network source option of flow graphs:


192.168.29.243
140.82.114.25
224.0.0.22
fe80::b6a7:c6ff:fe62:882f
2405:201:8012:512c:896c:11ac:eeeb:76df
Comment
Neighbor Solicitation for 2405:201:8012:512c:896c:11ac...
Neighbor Advertisement 2405:201:8012:512c:896c:11ac...
2924 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
2923 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Application Data
443 → 2924 [FIN, ACK] Seq=25 Ack=2 Win=501 Len=0
2924 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
Membership Report / Join group 224.0.0.251 for any sources
Membership Report / Join group 224.0.0.251 for any sources
Membership Report / Join group 224.0.0.251 for any sources
Membership Report / Join group 239.255.255.250 for any sources
2924
2923
2924
2924
2924
63975
63975
63975
63975
63975
63975
63975
63975
63975
63975
63975
63975
56968
56968
ICMPv6: Neighbor Solicitation for 2405:201:8012:512c:896c...
ICMPv6: Neighbor Advertisement 2405:201:8012:512c:896c...
TCP: 2924 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
TCP: 2923 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TLSv1.2: Application Data
TCP: 443 → 2924 [FIN, ACK] Seq=25 Ack=2 Win=501 Len=0
TCP: 2924 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
IGMPv3: Membership Report / Join group 224.0.0.251 for a...
IGMPv3: Membership Report / Join group 224.0.0.251 for a...
IGMPv3: Membership Report / Join group 224.0.0.251 for a...
IGMPv3: Membership Report / Join group 239.255.255.250...
UDP: 63975 → 443 Len=1226
UDP: 63975 → 443 Len=303
UDP: 443 → 63975 Len=27
UDP: 443 → 63975 Len=25
UDP: 63975 → 443 Len=33
UDP: 63975 → 443 Len=33
UDP: 443 → 63975 Len=553
UDP: 63975 → 443 Len=35
UDP: 443 → 63975 Len=40
UDP: 443 → 63975 Len=73
UDP: 63975 → 443 Len=33
UDP: 443 → 63975 Len=25
UDP: 56968 → 443 Len=1223
UDP: 56968 → 443 Len=832