**ASSIGNMENT 5**

Name: Imon Raj

Class: BCSE III

Roll: 002010501098

Section: A3

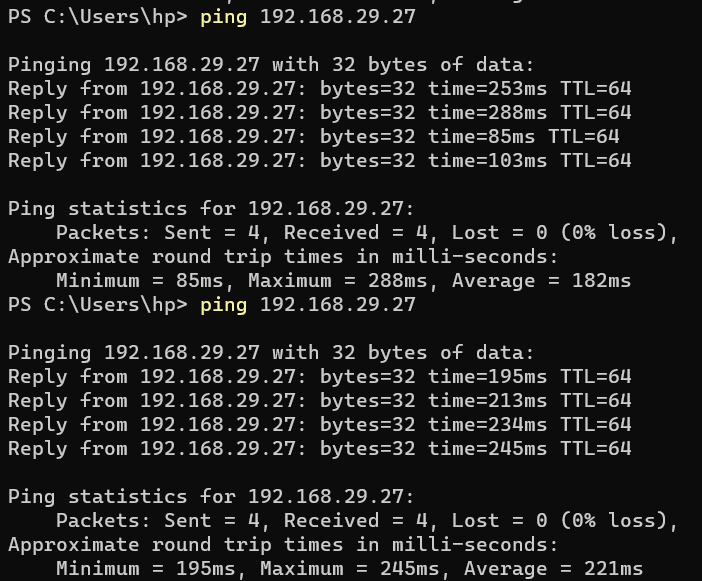
Subject: Computer Networks Lab Report

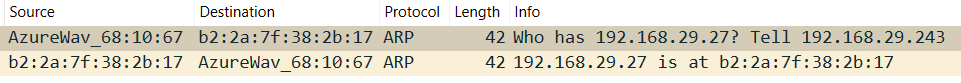
**PROBLEM STATEMENT: Install Wireshark in local machine and do traffic and packet analysis according to the given questions**

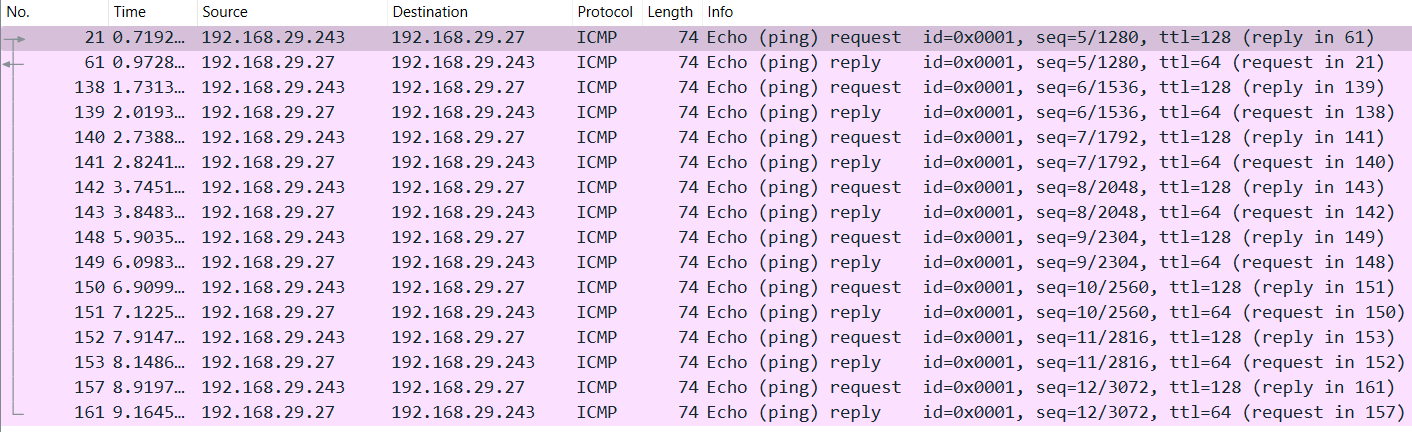
**QUESTIONS:**

**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:**

****

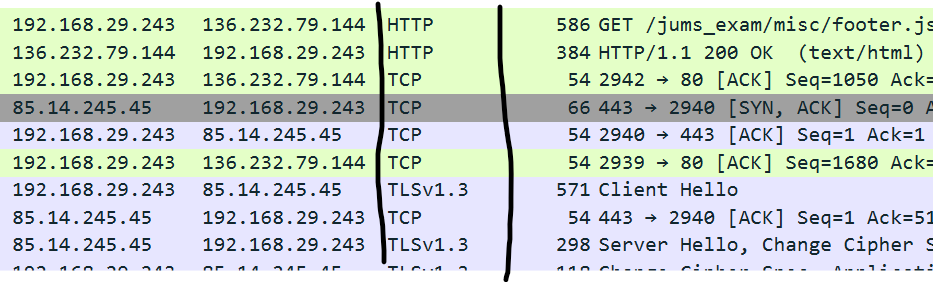




**2.) Generate some web traffic and**

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

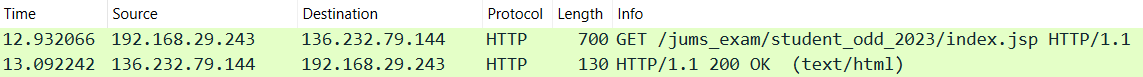
**Ans:**

****

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:**

****

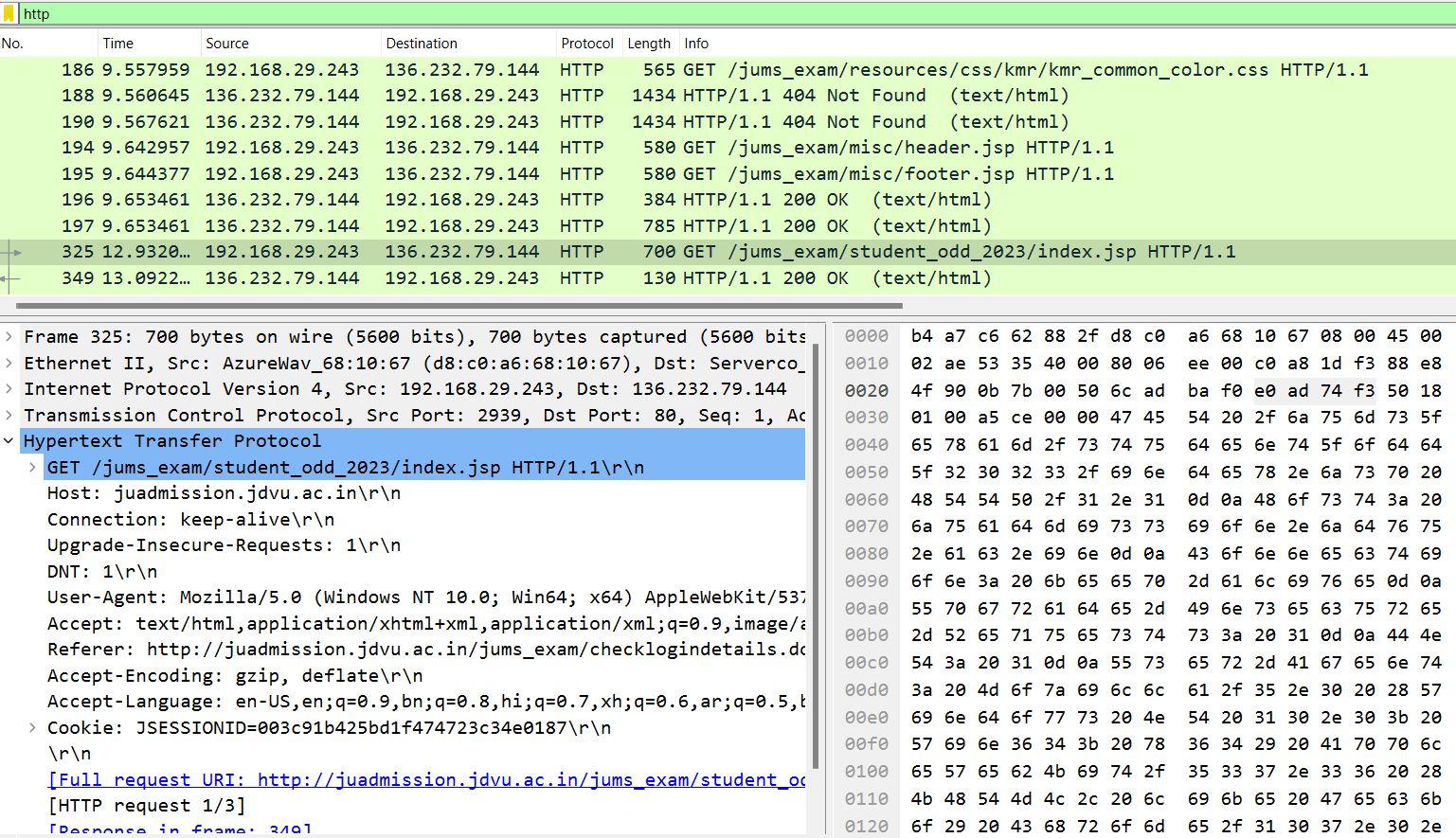
As we can see, that GET message was sent in time 12.932066 and OK response was received in time 13.092242. So the time taken is – (13.092242-12.932066) = 0.160176 seconds.

**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:**

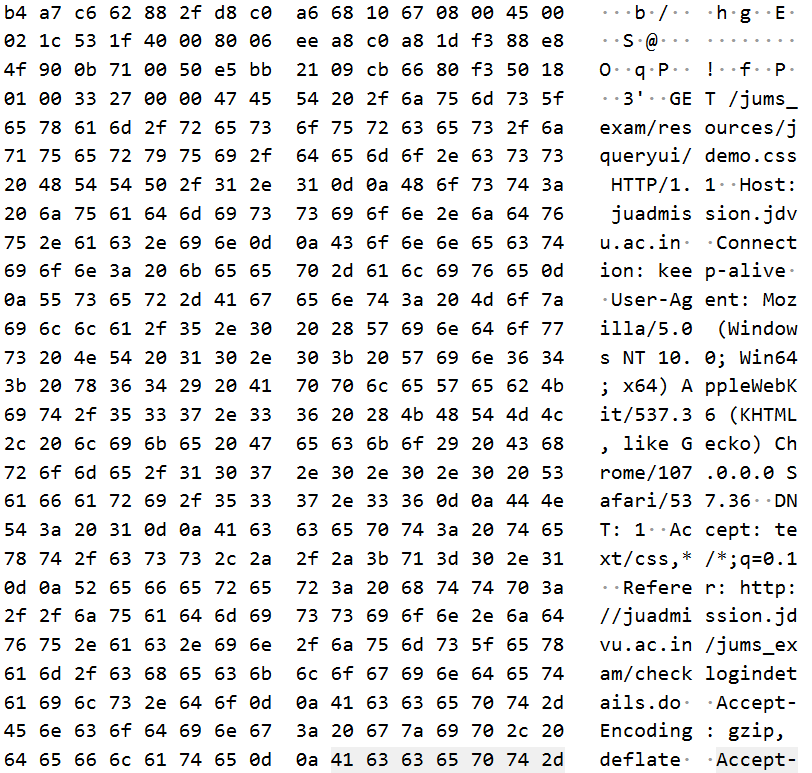
****

**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

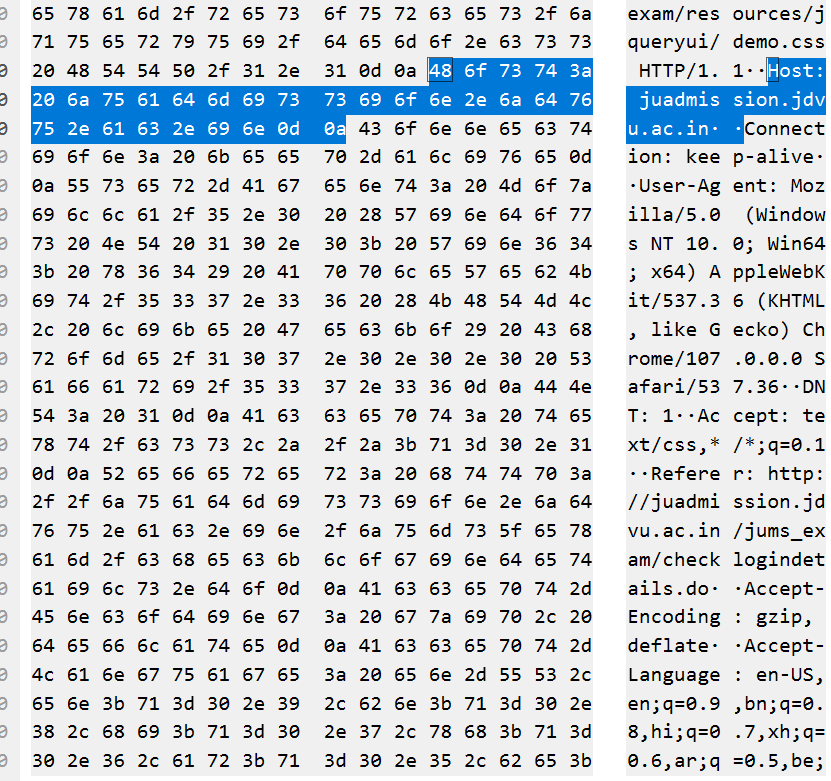
**3.) Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel**

**ANS:**



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

**Ans:**

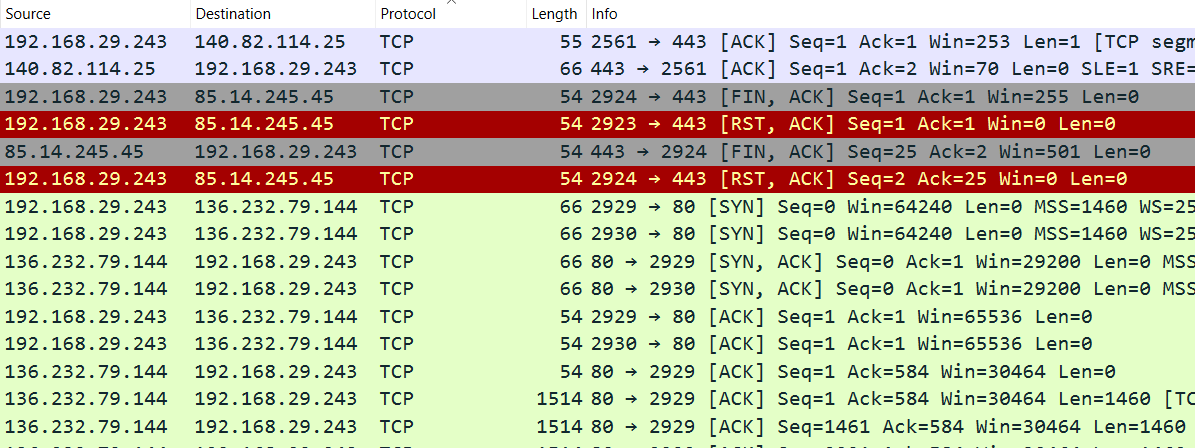
****

As we can see first four bytes of the Hex value of the Host parameter is: 48 6f 73 74

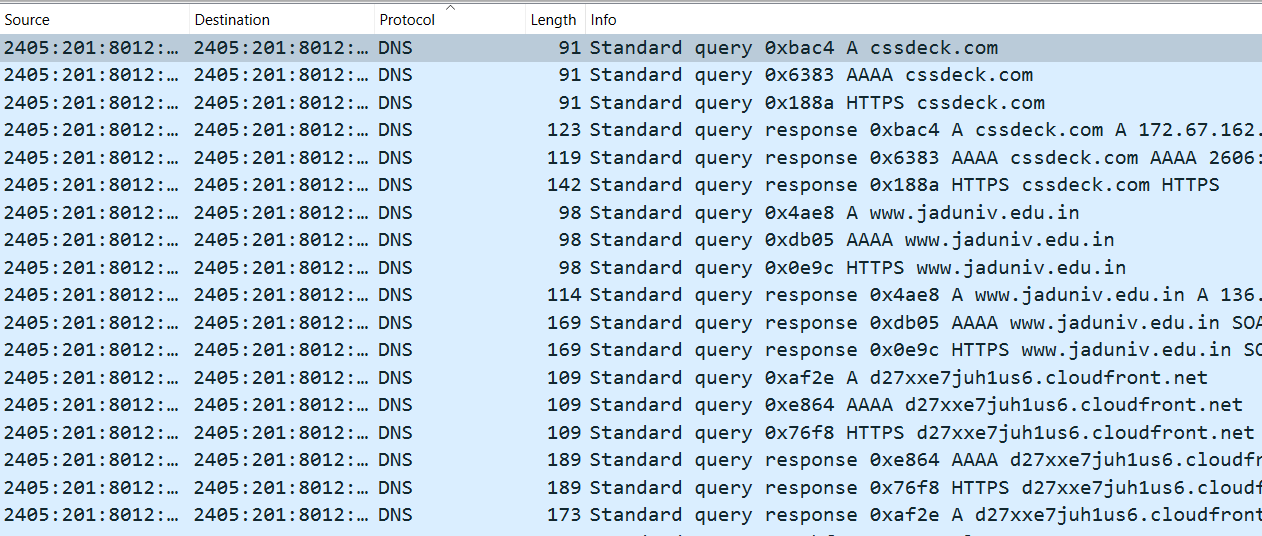
**5. Filter packets with http, TCP, DNS and other protocols. a. Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow**

**Ans:**

**TCP:**

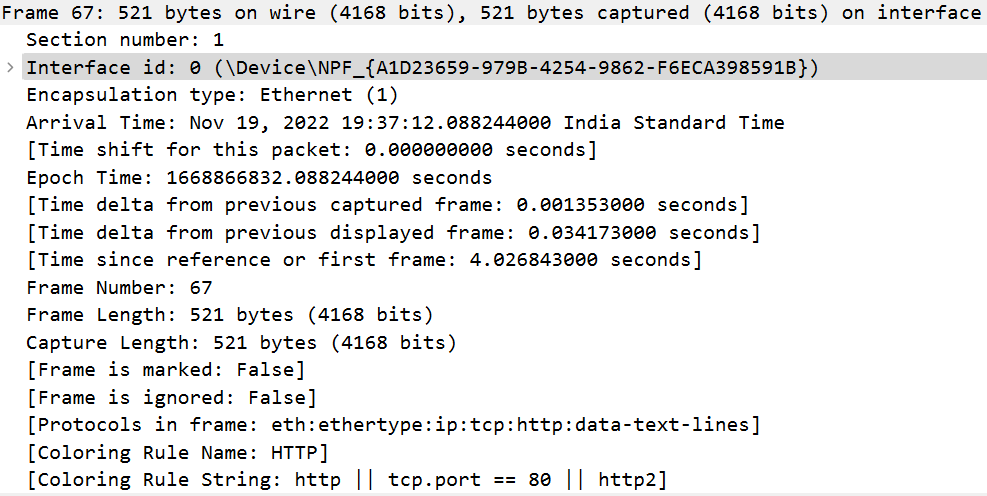
****

**DNS:**

****

**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.



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

**Ans:**

****

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:

