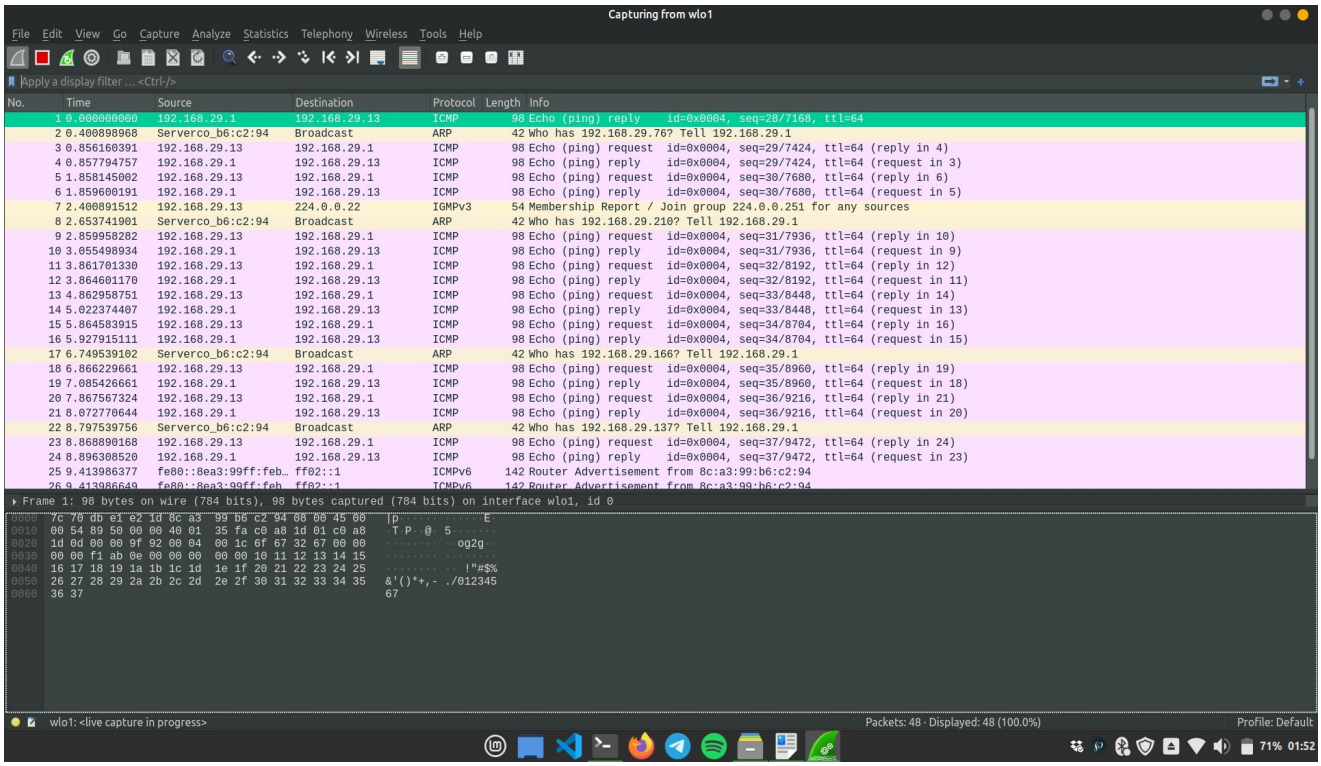
Name – Jeetesh Abrol	Assignment no. 5
Roll – 002210501021	BCSE III
Sub - Computer Networks	Group –A1

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

RESULTS:



Q2) Generate some web traffic and

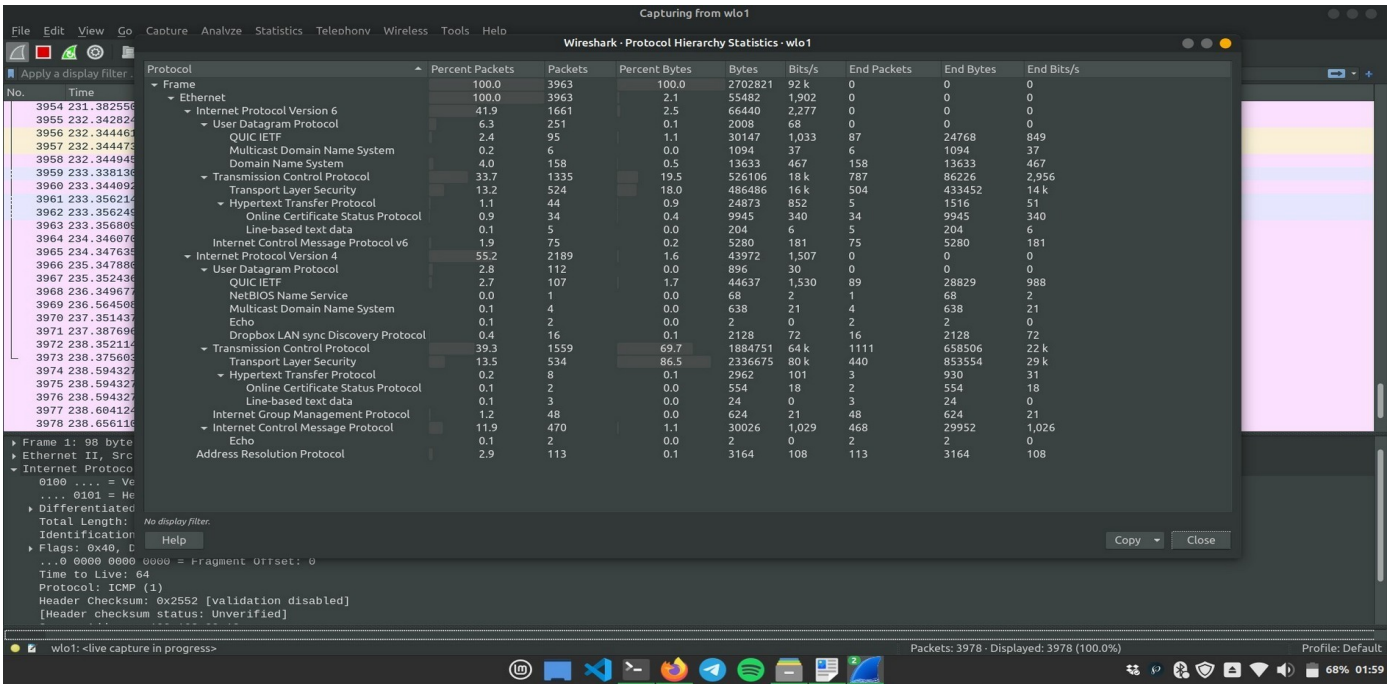
a. find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.

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

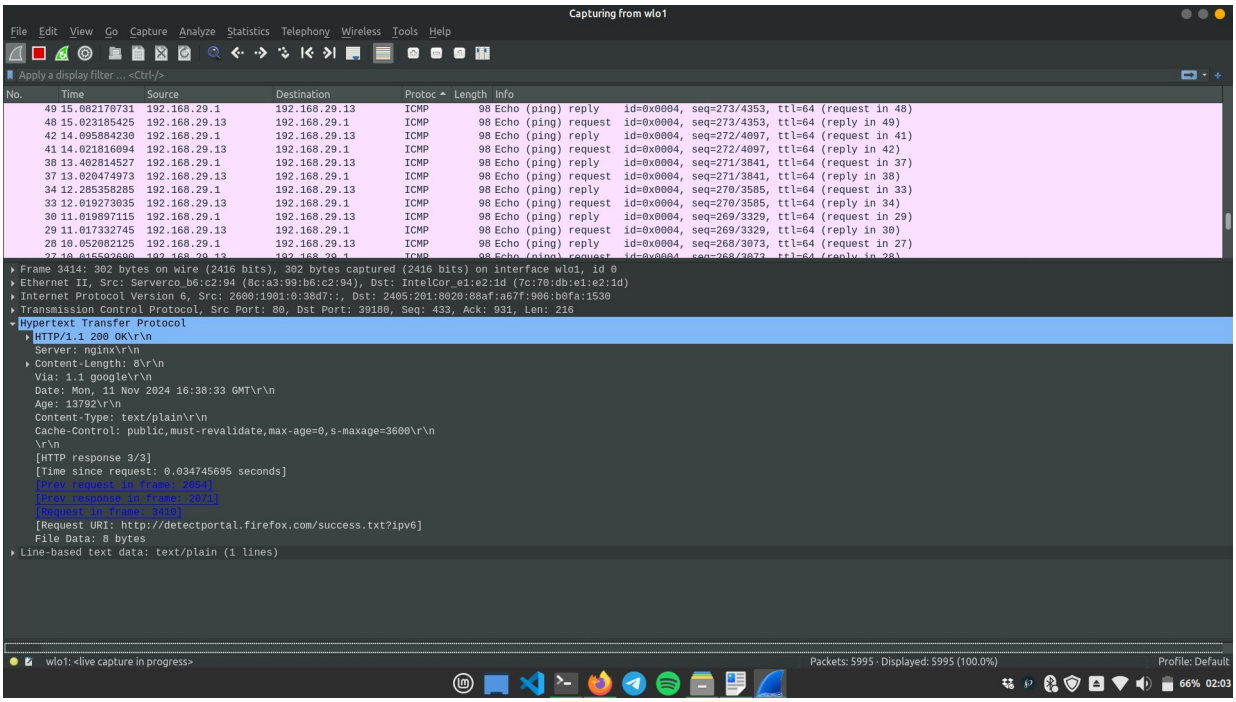
menu, then select Time Display Format, then select Time-of-day.)
c. What is the Internet address of the website? What is the Internet address of your computer?
d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand 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.

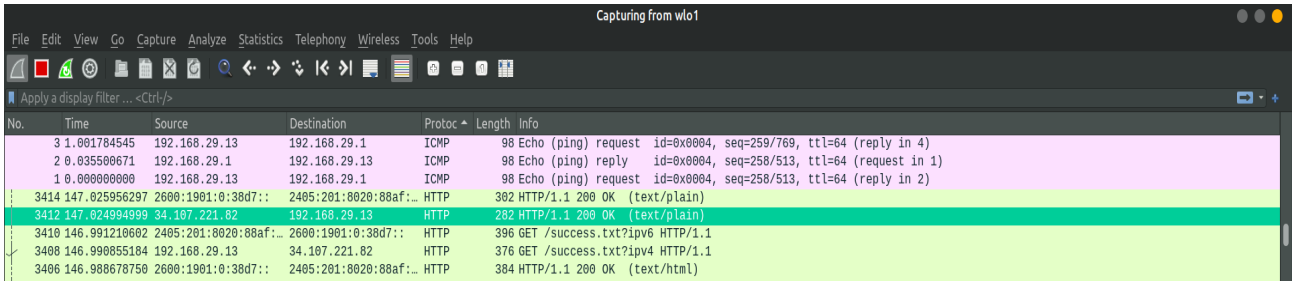
RESULTS:



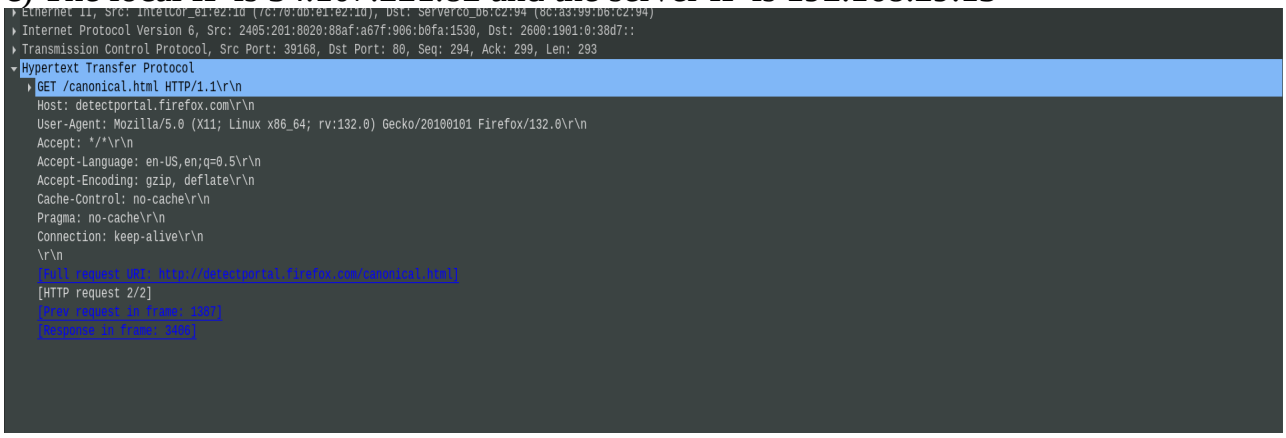
a) All the protocols that were captured are listed above.



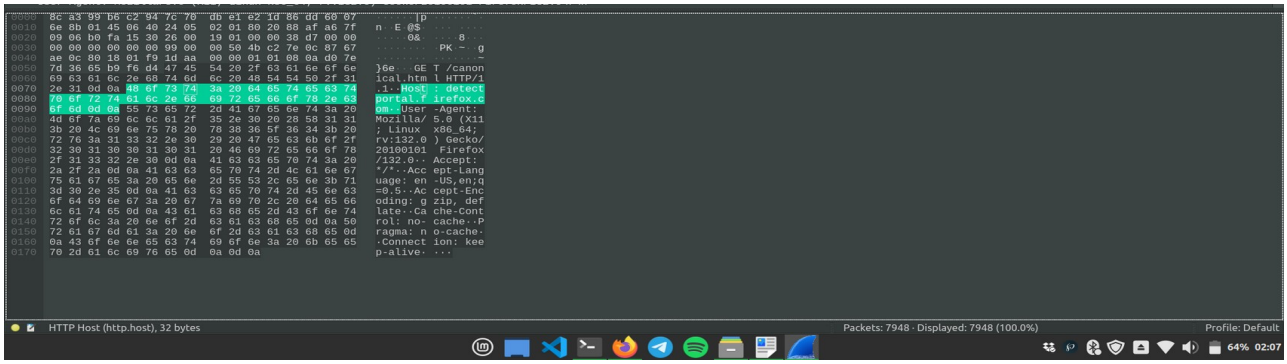
b) According to the delta time taken, it took 0.034745695 seconds approx. To get the HTTP response.



c) The local IP is 34.107.221.82 and the server IP is 192.168.29.13

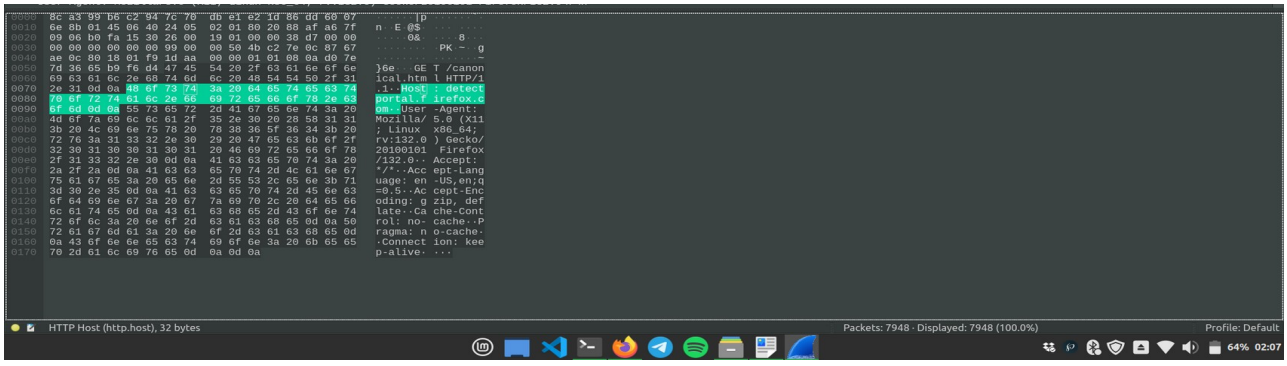


d) The above is the details of a HTTP packet



e) The value of Host as shown above is: testphp.vulnweb.com

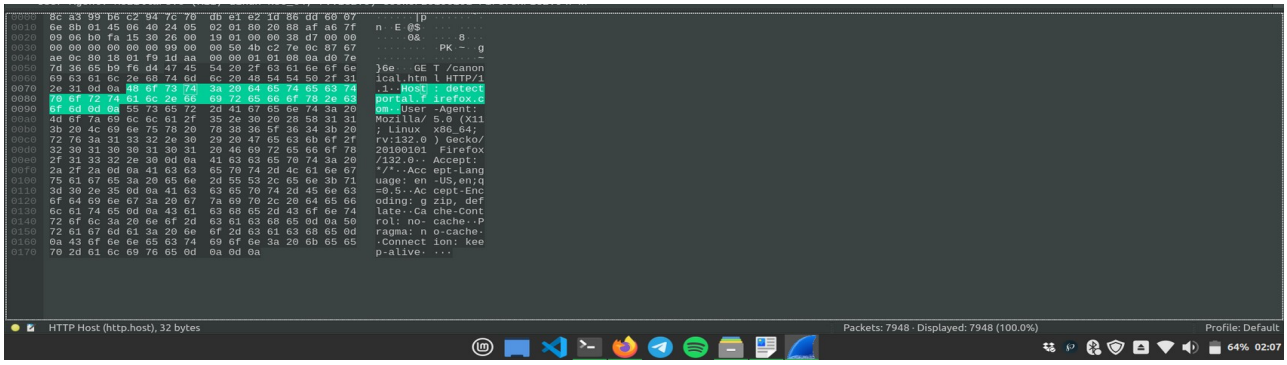
Q3)Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.
RESULTS:



The above picture clearly shows the hex and ASCII representation of the packet in Packet Bytes panel.

Q4) Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.

RESULTS:

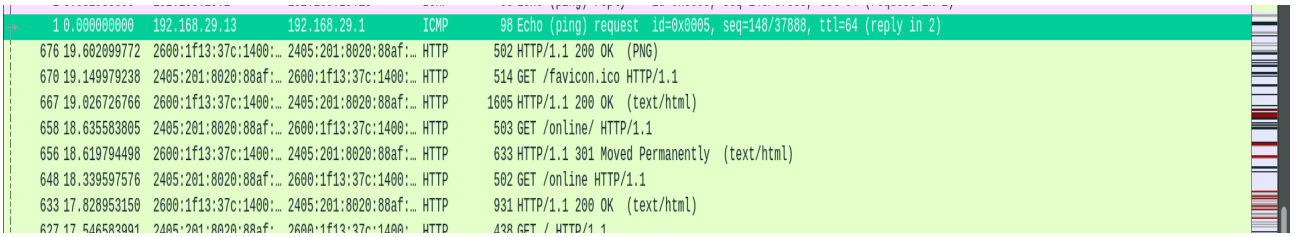


Ans: The first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel are: 48 6f 73 74

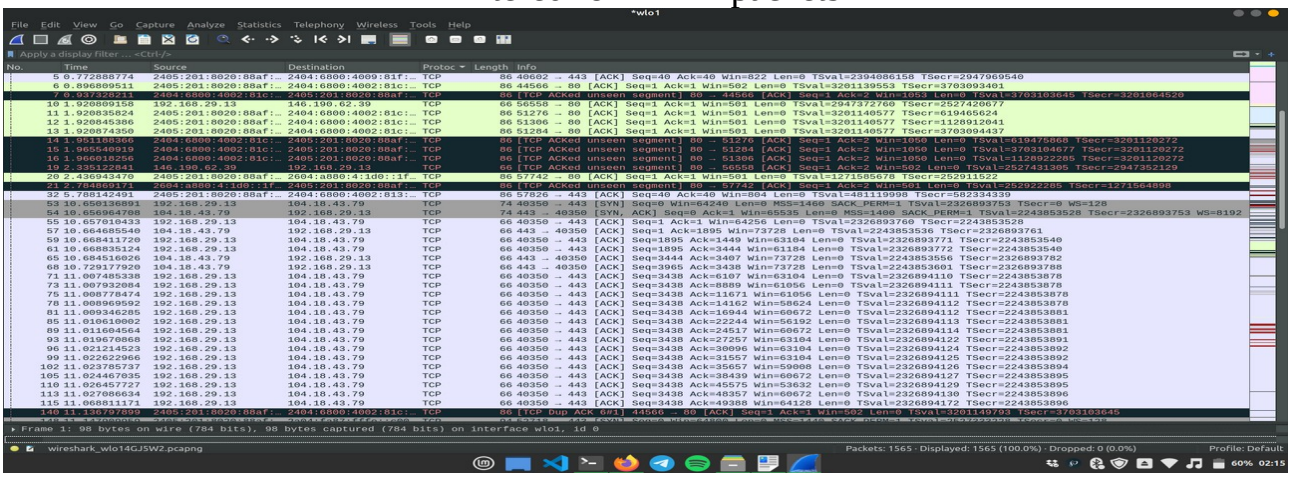
Q5) Filter packets with http, TCP, DNS and other protocols.

RESULTS:

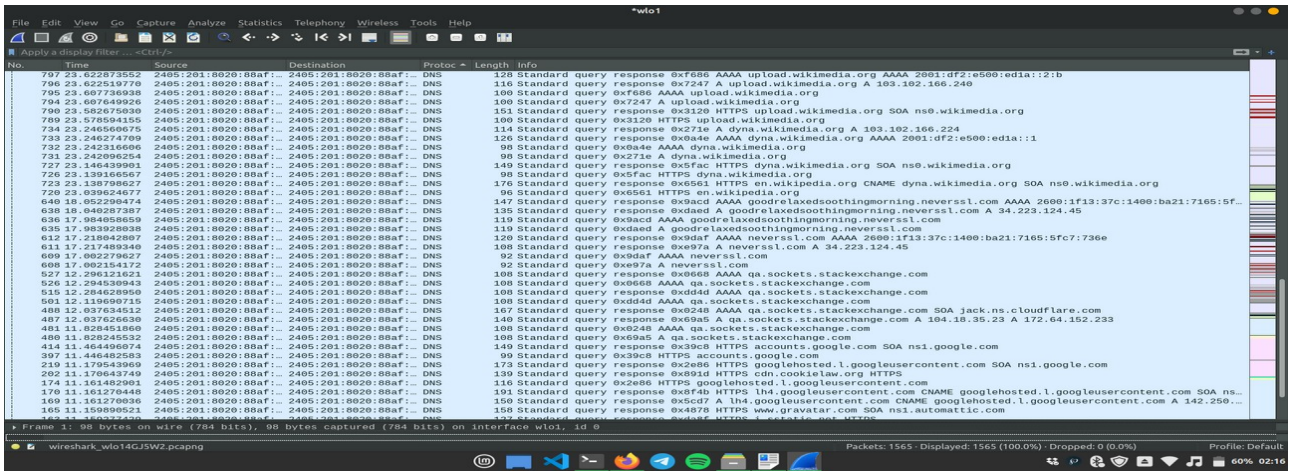
]



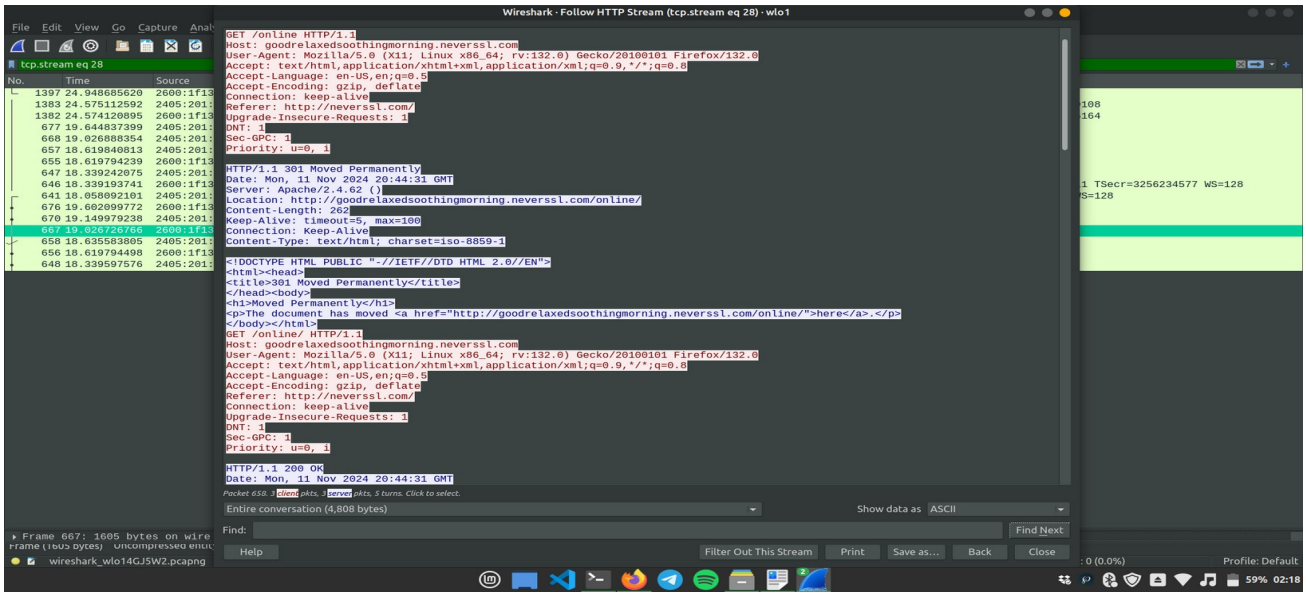
Filtered for HTTP packets



Filtered for TCP packets



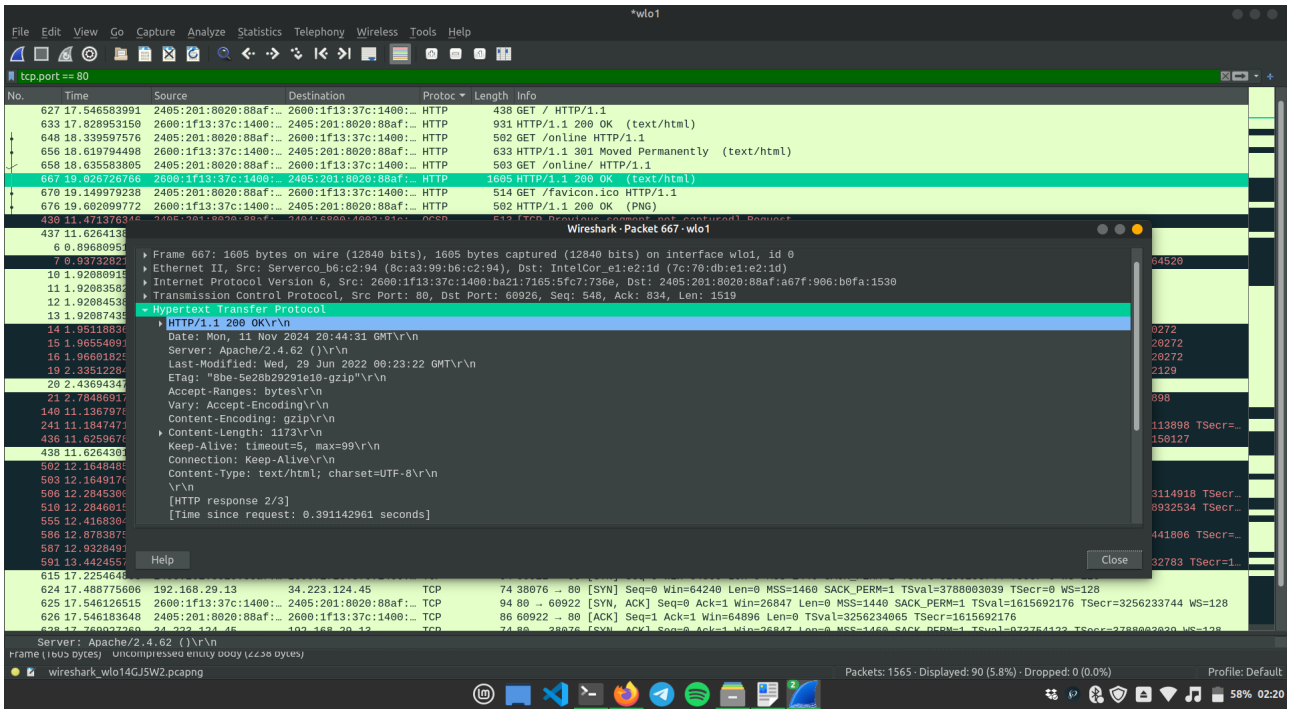
Filtered for DNS packets



Followed HTTP stream

Q6) 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.

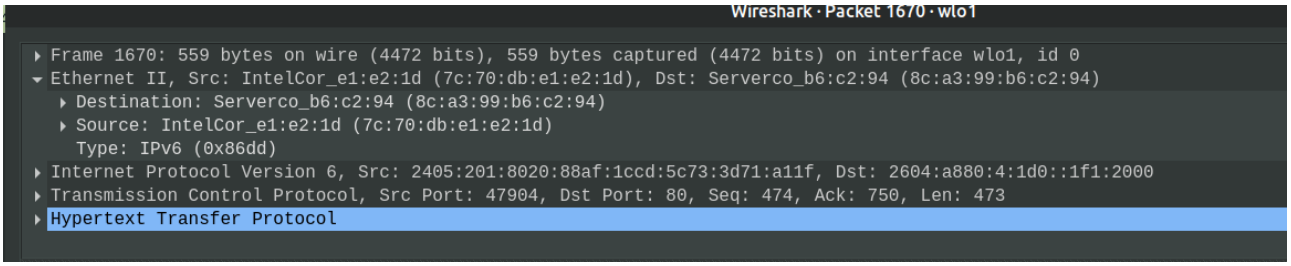
RESULTS:



The above images shows the Ethernet layer in the Packet details.

Q7) What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?

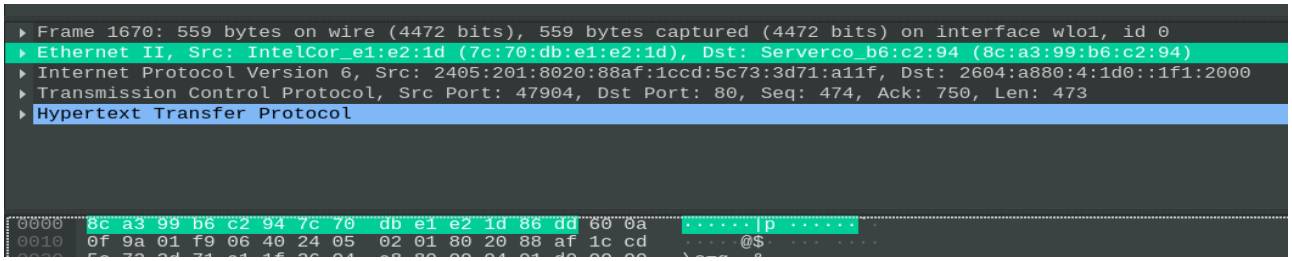
Ans-



So according to the details, my PC's Network Interface Card (NIC) has the manufacturer: IntelCor.
And the server's Network Interface Card (NIC) has the manufacturer: ServerCo.

Q8) What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?

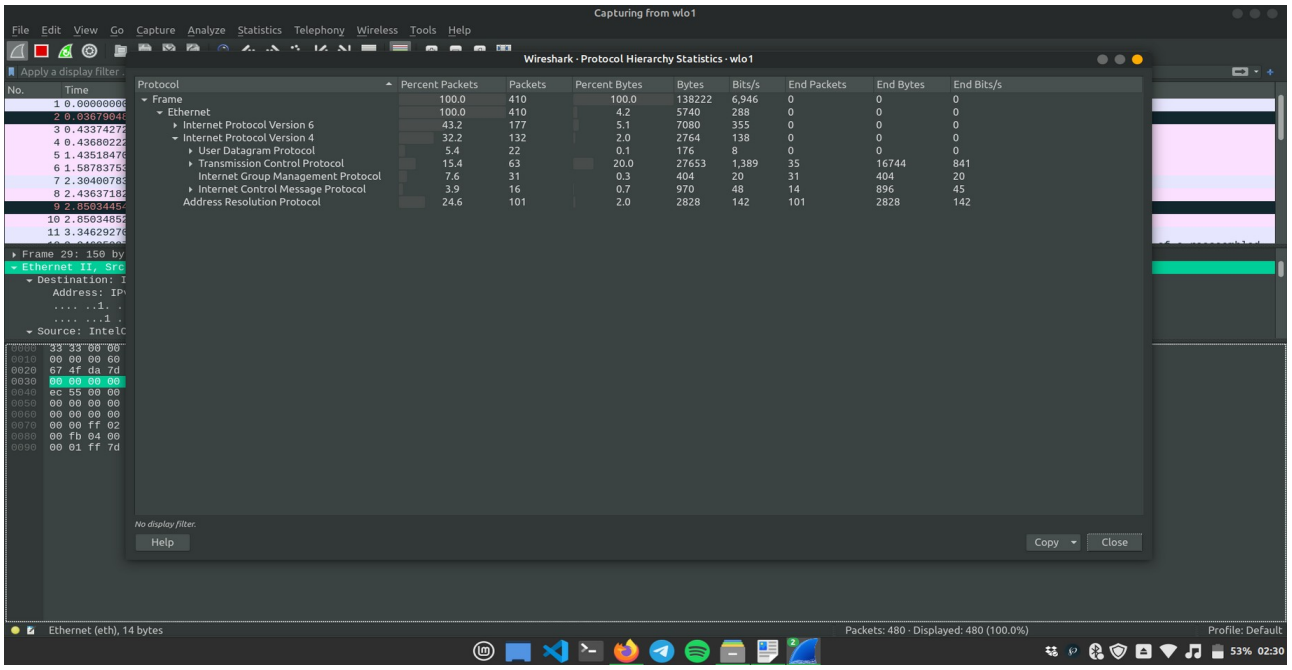
RESULTS:



Ans: The hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs are: 8c a3 99 b6 c2 94 (my NIC raw bytes) and 7c 70 db e1 e2 1d 86 dd (server NIC)

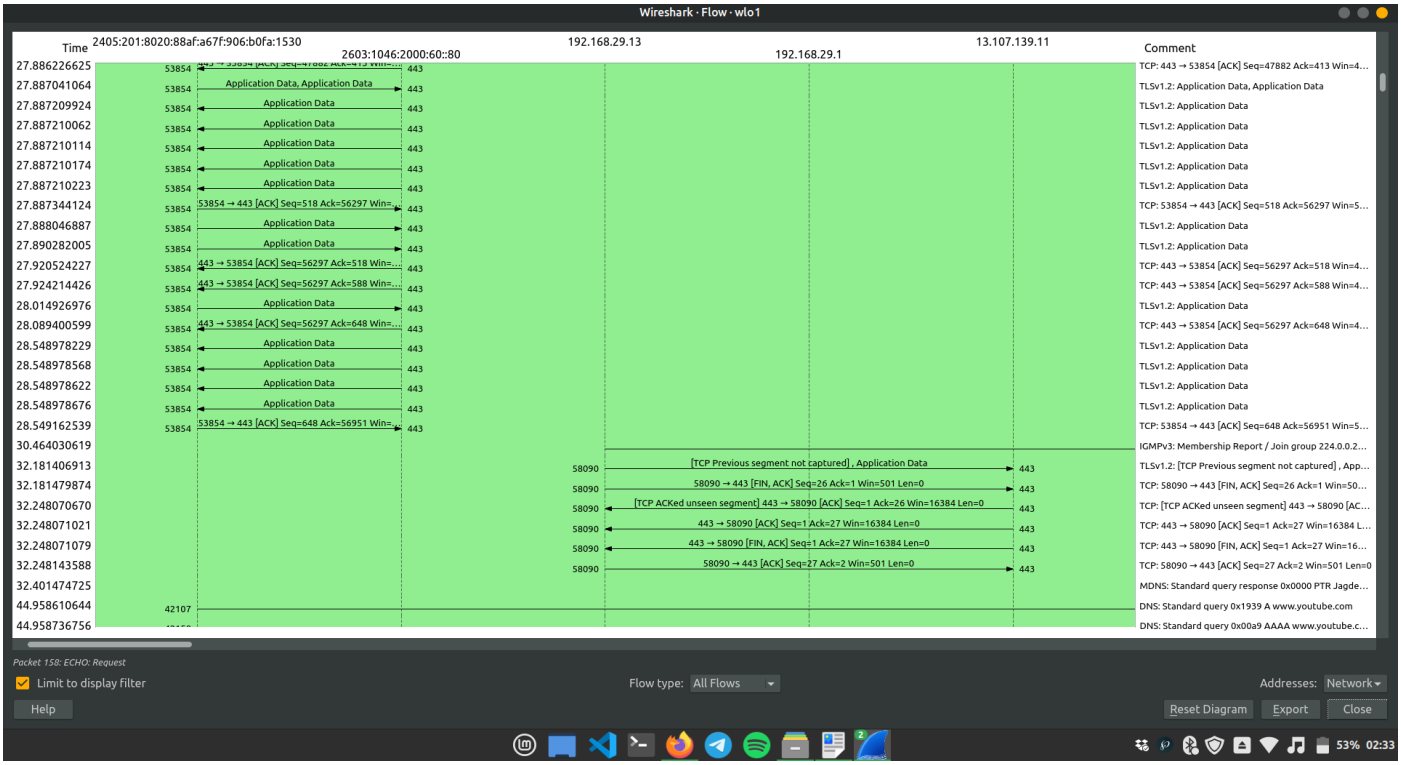
Q9) Find the following statistics:
a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?
b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

RESULTS:



Ans: a) From the above statistics, the percentage of TCP packets is 15.4%
A protocol that uses TCP is HTTP.
b) The percentage of UDP packets is 5.4%. A protocol that uses UDP is DNS.

Q10)Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.



Shown as mentioned in question