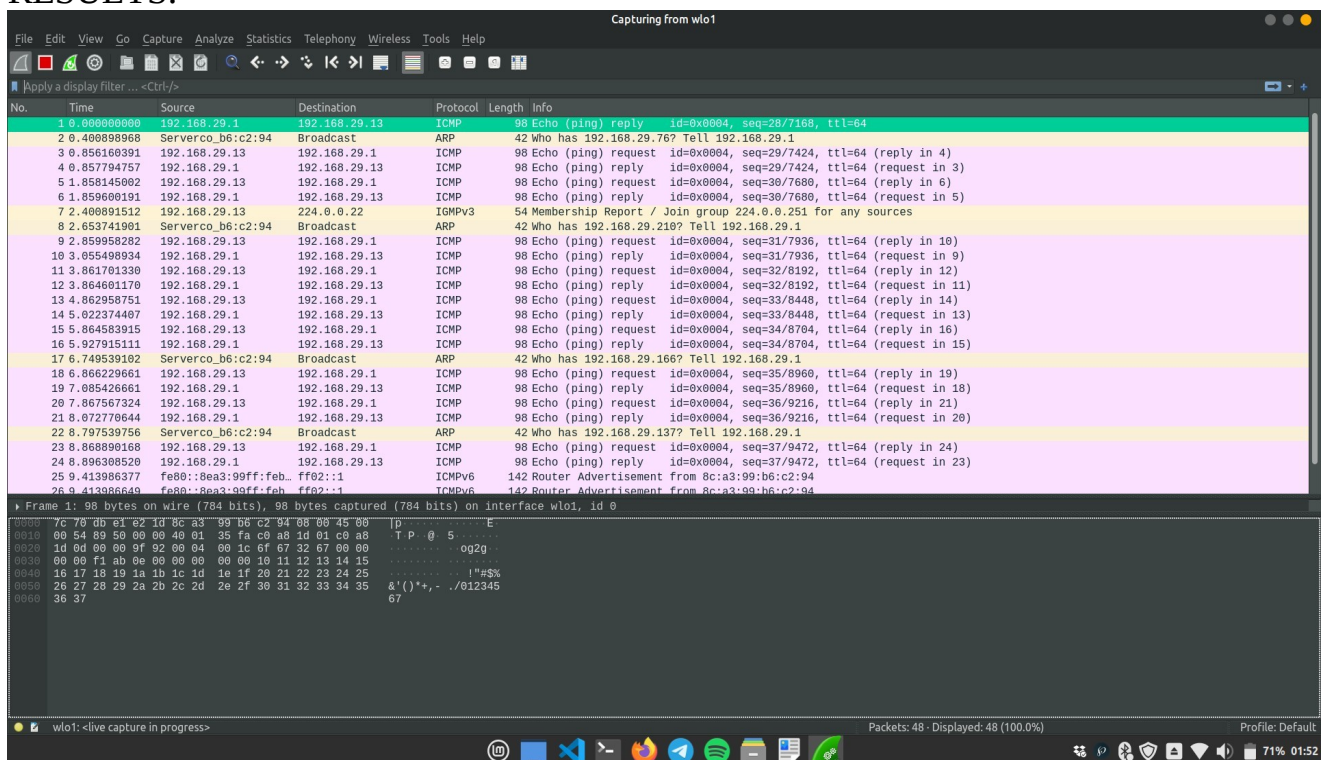


Name – Jeetesh Abrol
Roll – 002210501021
Sub - Computer Networks

Assignment no. 5
BCSE III
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

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

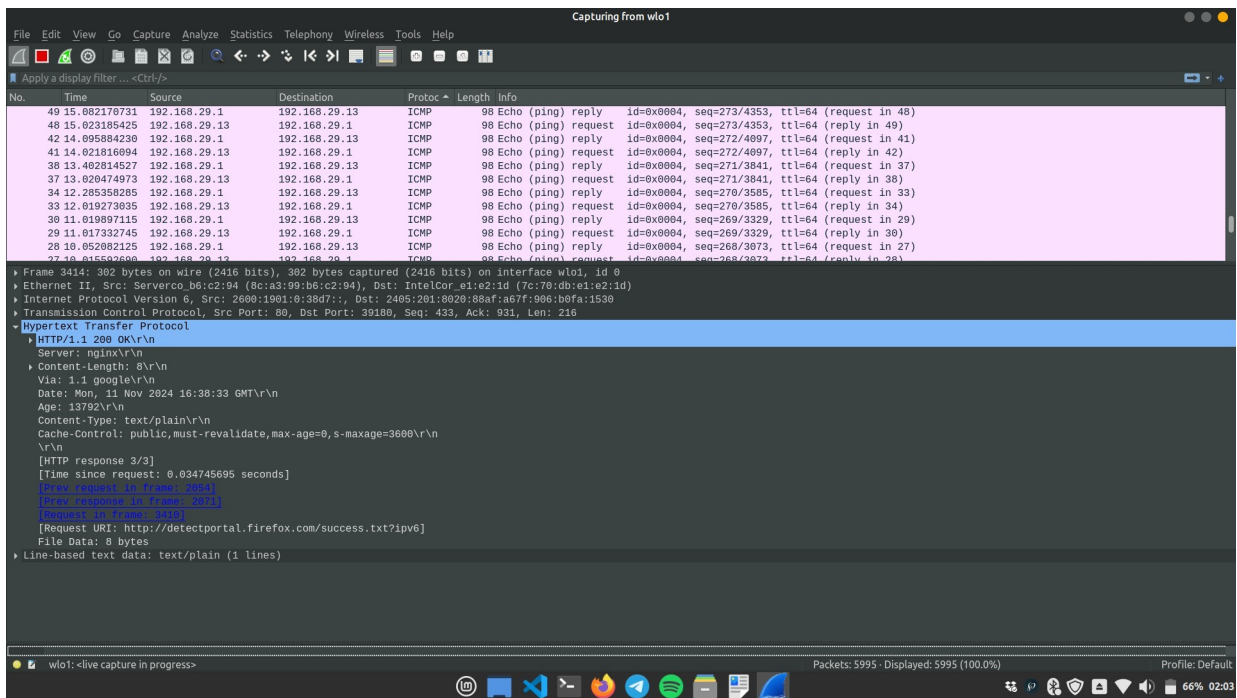
RESULTS:

The image shows the Wireshark Protocol Hierarchy Statistics window for a capture on interface wlo1. The window displays a tree view of protocols and a corresponding table of statistics.

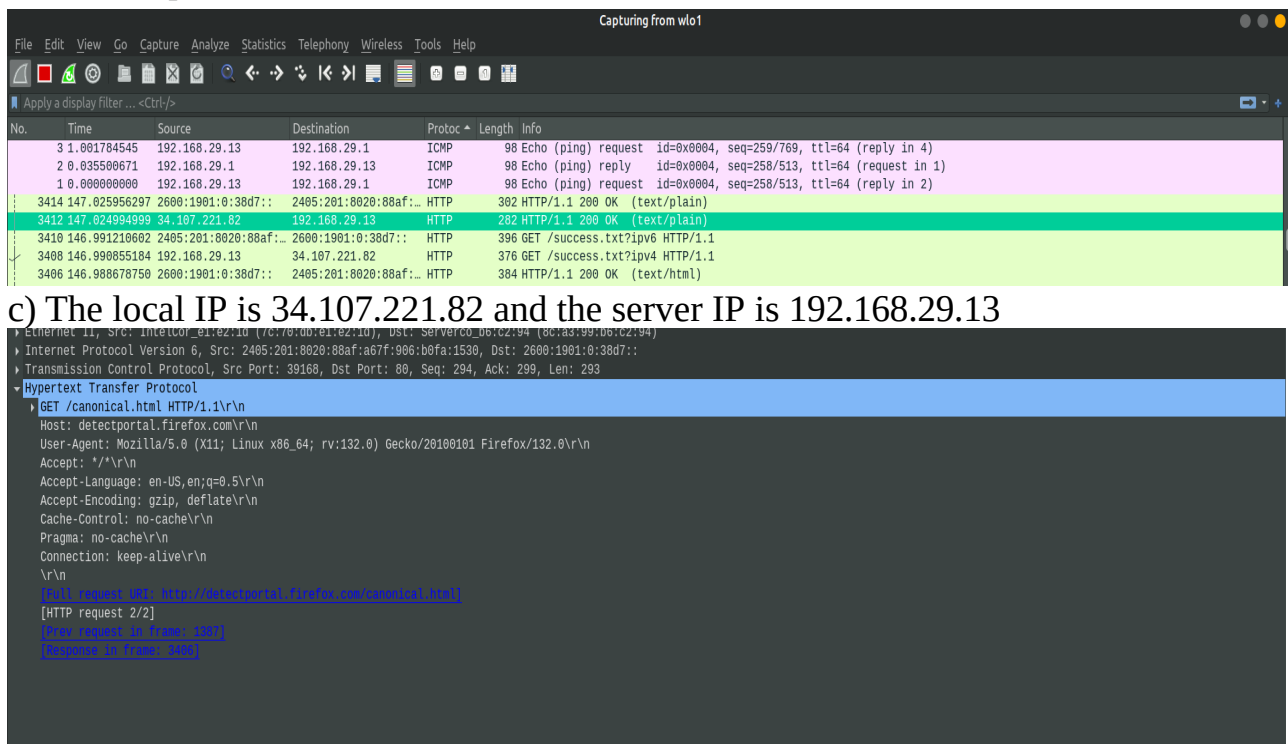
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	3963	100.0	2702821	92 k	0	0	0
Ethernet	100.0	3963	2.1	55482	1,902	0	0	0
Internet Protocol Version 6	41.9	1661	2.5	66440	2,277	0	0	0
User Datagram Protocol	6.3	251	0.1	2008	68	0	0	0
QUIC IETF	2.4	95	1.1	30147	1,033	87	24768	849
Multicast Domain Name System	0.2	6	0.0	1094	37	6	1094	37
Domain Name System	4.0	158	0.5	13633	467	158	13633	467
Transmission Control Protocol	33.7	1335	19.5	526106	18 k	787	86226	2,956
Transport Layer Security	13.2	524	18.0	486486	16 k	504	433452	14 k
Hypertext Transfer Protocol	1.1	44	0.9	24873	852	5	1516	51
Online Certificate Status Protocol	0.9	34	0.4	9945	340	34	9945	340
Line-based text data	0.1	5	0.0	204	6	5	204	6
Internet Control Message Protocol v6	1.9	75	0.2	5280	181	75	5280	181
Internet Protocol Version 4	55.2	2189	1.6	43972	1,507	0	0	0
User Datagram Protocol	2.8	112	0.0	896	30	0	0	0
QUIC IETF	2.7	107	1.7	44637	1,530	89	28829	988
NetBIOS Name Service	0.0	1	0.0	68	2	1	68	2
Multicast Domain Name System	0.1	4	0.0	638	21	4	638	21
Echo	0.1	2	0.0	2	0	2	2	0
Dropbox LAN sync Discovery Protocol	0.4	16	0.1	2128	72	16	2128	72
Transmission Control Protocol	39.3	1559	69.7	1884751	64 k	1111	658506	22 k
Transport Layer Security	13.5	534	86.5	2336675	80 k	440	853554	29 k
Hypertext Transfer Protocol	0.2	8	0.1	2962	101	3	930	31
Online Certificate Status Protocol	0.1	2	0.0	554	18	2	554	18
Line-based text data	0.1	3	0.0	24	0	3	24	0
Internet Group Management Protocol	1.2	48	0.0	624	21	48	624	21
Internet Control Message Protocol	11.9	470	1.1	30026	1,029	468	29952	1,026
Echo	0.1	2	0.0	2	0	2	2	0
Address Resolution Protocol	2.9	113	0.1	3164	108	113	3164	108

The bottom of the window shows the packet list and packet details for the selected packet (Frame 1: 98 byte). The packet details show the Ethernet II, Src, and Internet Protocol sections.

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

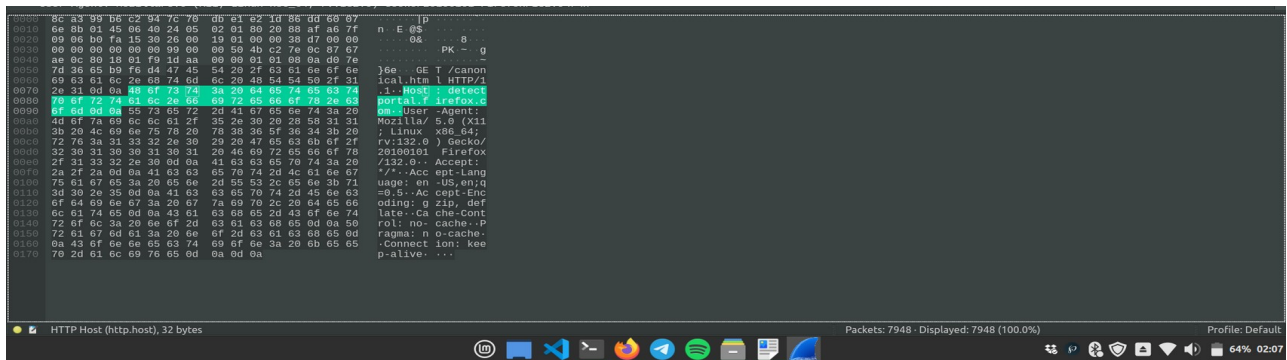


b) According to the delta time taken, it took 0.034745695 seconds approx. To get the HTTP response.



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

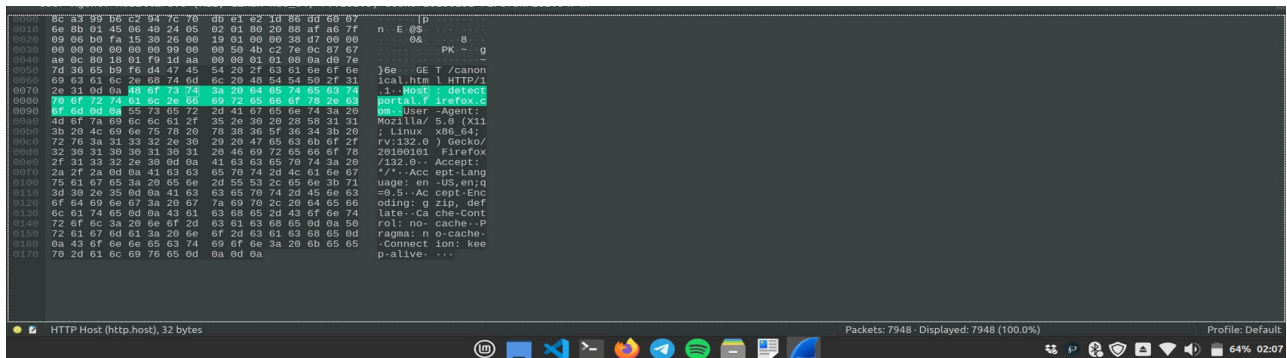
d) The above is the details of a HTTP packet



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.

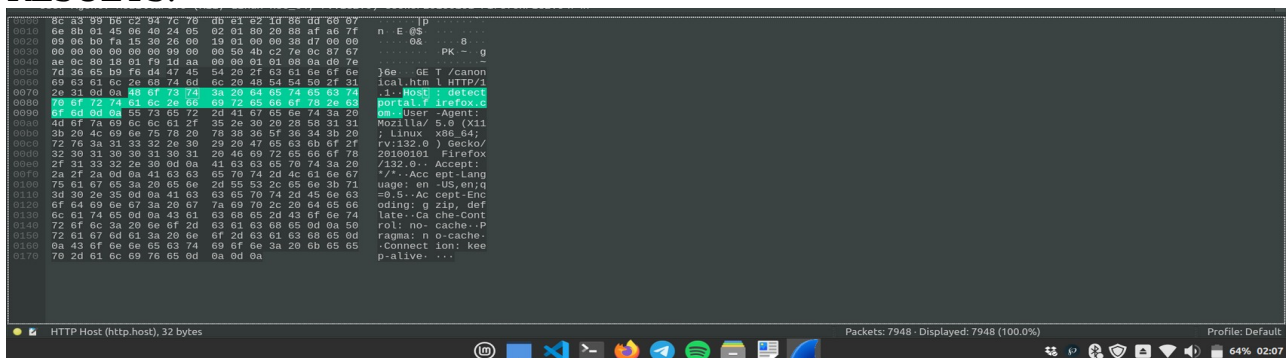
RESULTS:



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:

1	0.800000000	192.168.29.13	192.168.29.1	TCP	98 Echo (ping) request id=0x0905, seq=148/37888, ttl=64 (reply in 2)
676	19.602899772	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	502 HTTP/1.1 200 OK (PNG)
678	19.149979238	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	514 GET /favicon.ico HTTP/1.1
667	19.026726766	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	1605 HTTP/1.1 200 OK (text/html)
658	18.635583805	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	503 GET /online/ HTTP/1.1
656	18.619794498	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	633 HTTP/2.1 301 Moved Permanently (text/html)
648	18.339597576	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	502 GET /online HTTP/1.1
633	17.828953150	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	931 HTTP/1.1 200 OK (text/html)
627	17.516583001	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	438 GET / HTTP/1.1

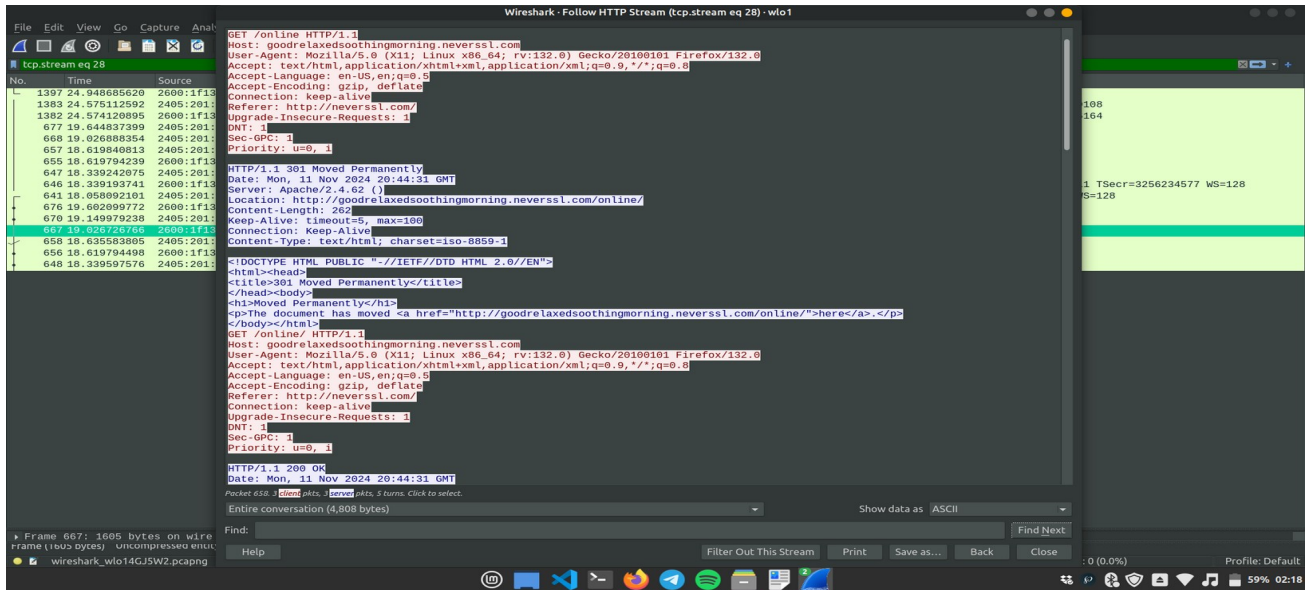
Filtered for HTTP packets

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000000	192.168.29.13	192.168.29.1	TCP	98	Echo (ping) request id=0x0905, seq=148/37888, ttl=64 (reply in 2)
676	19.602899772	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	502	HTTP/1.1 200 OK (PNG)
678	19.149979238	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	514	GET /favicon.ico HTTP/1.1
667	19.026726766	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	1605	HTTP/1.1 200 OK (text/html)
658	18.635583805	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	503	GET /online/ HTTP/1.1
656	18.619794498	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	633	HTTP/2.1 301 Moved Permanently (text/html)
648	18.339597576	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	502	GET /online HTTP/1.1
633	17.828953150	2600:1f13:37c:1400::	2405:201:8020:88af::	HTTP	931	HTTP/1.1 200 OK (text/html)
627	17.516583001	2405:201:8020:88af::	2600:1f13:37c:1400::	HTTP	438	GET / HTTP/1.1

Filtered for TCP packets

No.	Time	Source	Destination	Protocol	Length	Info
797	23.622073552	2405:201:8020:88af::	2405:201:8020:88af::	DNS	128	Standard query response 0x6f86 AAAA upload.wikimedia.org AAAA 2001:df2:e500:ed1a:12:b
796	23.622519170	2405:201:8020:88af::	2405:201:8020:88af::	DNS	136	Standard query response 0x7247 A upload.wikimedia.org A 103.102.166.240
795	23.607736038	2405:201:8020:88af::	2405:201:8020:88af::	DNS	109	Standard query 0x6f86 AAAA upload.wikimedia.org
794	23.607649926	2405:201:8020:88af::	2405:201:8020:88af::	DNS	109	Standard query 0x7247 A upload.wikimedia.org
793	23.502675038	2405:201:8020:88af::	2405:201:8020:88af::	DNS	151	Standard query response 0x3128 HTTPS upload.wikimedia.org SOA ns0.wikimedia.org
789	23.578594155	2405:201:8020:88af::	2405:201:8020:88af::	DNS	109	Standard query 0x3128 HTTPS upload.wikimedia.org
734	23.246560676	2405:201:8020:88af::	2405:201:8020:88af::	DNS	114	Standard query response 0x271e A dyna.wikimedia.org A 103.102.166.224
733	23.246274709	2405:201:8020:88af::	2405:201:8020:88af::	DNS	126	Standard query response 0xa04e AAAA dyna.wikimedia.org AAAA 2001:df2:e500:ed1a:1
732	23.242316686	2405:201:8020:88af::	2405:201:8020:88af::	DNS	98	Standard query 0xa04e AAAA dyna.wikimedia.org
731	23.242096254	2405:201:8020:88af::	2405:201:8020:88af::	DNS	98	Standard query 0x271e A dyna.wikimedia.org
727	23.146439903	2405:201:8020:88af::	2405:201:8020:88af::	DNS	149	Standard query response 0x5fac HTTPS dyna.wikimedia.org SOA ns0.wikimedia.org
726	23.139166567	2405:201:8020:88af::	2405:201:8020:88af::	DNS	98	Standard query 0x5fac HTTPS dyna.wikimedia.org
723	23.138798627	2405:201:8020:88af::	2405:201:8020:88af::	DNS	176	Standard query response 0x6581 HTTPS en.wikipedia.org CNAME dyna.wikimedia.org SOA ns0.wikimedia.org
726	23.039624677	2405:201:8020:88af::	2405:201:8020:88af::	DNS	98	Standard query 0x6581 HTTPS en.wikipedia.org
646	18.065229474	2405:201:8020:88af::	2405:201:8020:88af::	DNS	147	Standard query response 0xa9ad AAAA googlerelaxedsoothingmorning.neverssl.com AAAA 2001:df2:e500:ed1a:1
638	18.048287387	2405:201:8020:88af::	2405:201:8020:88af::	DNS	135	Standard query response 0xa9ad AAAA googlerelaxedsoothingmorning.neverssl.com AAAA 2001:df2:e500:ed1a:1
635	17.983028938	2405:201:8020:88af::	2405:201:8020:88af::	DNS	119	Standard query 0xa9ad AAAA googlerelaxedsoothingmorning.neverssl.com
612	17.218642807	2405:201:8020:88af::	2405:201:8020:88af::	DNS	129	Standard query response 0x9daa A googlerelaxedsoothingmorning.neverssl.com
611	17.217489340	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x9daa A googlerelaxedsoothingmorning.neverssl.com
608	17.002278627	2405:201:8020:88af::	2405:201:8020:88af::	DNS	92	Standard query 0x9daa A googlerelaxedsoothingmorning.neverssl.com
608	17.002154172	2405:201:8020:88af::	2405:201:8020:88af::	DNS	92	Standard query 0x9daa A googlerelaxedsoothingmorning.neverssl.com
527	12.296121621	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0668 AAAA qa.sockets.stackexchange.com
526	12.294530943	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0668 AAAA qa.sockets.stackexchange.com
515	12.284628950	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0668 AAAA qa.sockets.stackexchange.com
501	11.198907735	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0668 AAAA qa.sockets.stackexchange.com
488	12.037634512	2405:201:8020:88af::	2405:201:8020:88af::	DNS	167	Standard query response 0x0248 AAAA qa.sockets.stackexchange.com SOA ns0.cloudflare.com
487	12.037626538	2405:201:8020:88af::	2405:201:8020:88af::	DNS	140	Standard query response 0x0248 AAAA qa.sockets.stackexchange.com SOA ns0.cloudflare.com
481	11.828451860	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0248 AAAA qa.sockets.stackexchange.com
480	11.828245532	2405:201:8020:88af::	2405:201:8020:88af::	DNS	108	Standard query response 0x0248 AAAA qa.sockets.stackexchange.com
414	11.464496974	2405:201:8020:88af::	2405:201:8020:88af::	DNS	149	Standard query response 0x30c8 HTTPS accounts.google.com SOA ns1.google.com
397	11.446482583	2405:201:8020:88af::	2405:201:8020:88af::	DNS	99	Standard query response 0x30c8 HTTPS accounts.google.com
310	11.170543060	2405:201:8020:88af::	2405:201:8020:88af::	DNS	173	Standard query response 0x2686 HTTPS googlehosted.l.googleusercontent.com SOA ns1.google.com
292	11.170643749	2405:201:8020:88af::	2405:201:8020:88af::	DNS	139	Standard query response 0x2686 HTTPS googlehosted.l.googleusercontent.com
174	11.161482903	2405:201:8020:88af::	2405:201:8020:88af::	DNS	116	Standard query response 0x2686 HTTPS googlehosted.l.googleusercontent.com
170	11.161270448	2405:201:8020:88af::	2405:201:8020:88af::	DNS	193	Standard query response 0x2686 HTTPS googlehosted.l.googleusercontent.com
169	11.161270638	2405:201:8020:88af::	2405:201:8020:88af::	DNS	150	Standard query response 0x2686 HTTPS googlehosted.l.googleusercontent.com
165	11.159890521	2405:201:8020:88af::	2405:201:8020:88af::	DNS	158	Standard query response 0x4878 HTTPS www.gravatar.com SOA ns1.automattic.com

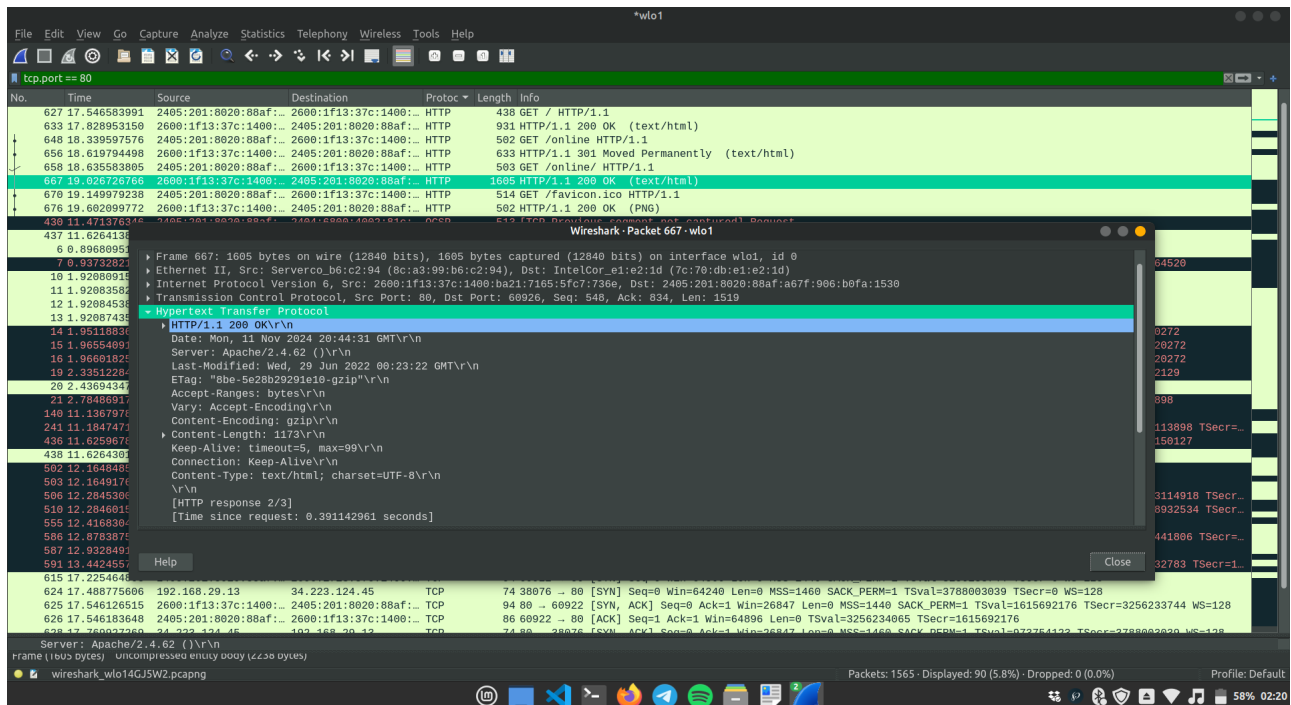
Filtered for DNS packets



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.

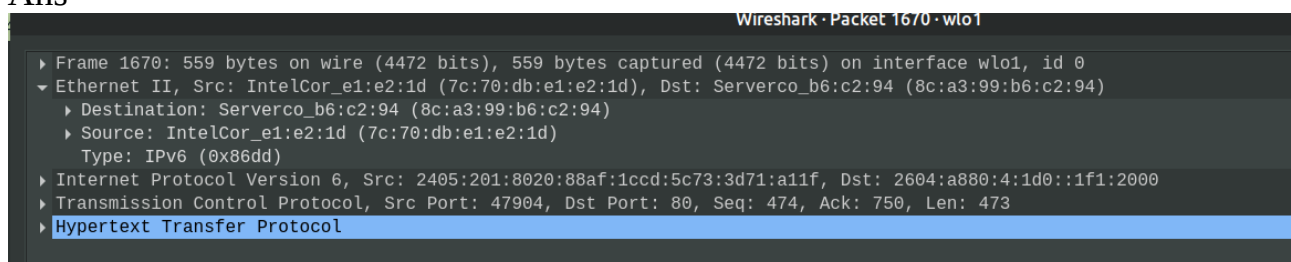
RESULTS:



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-

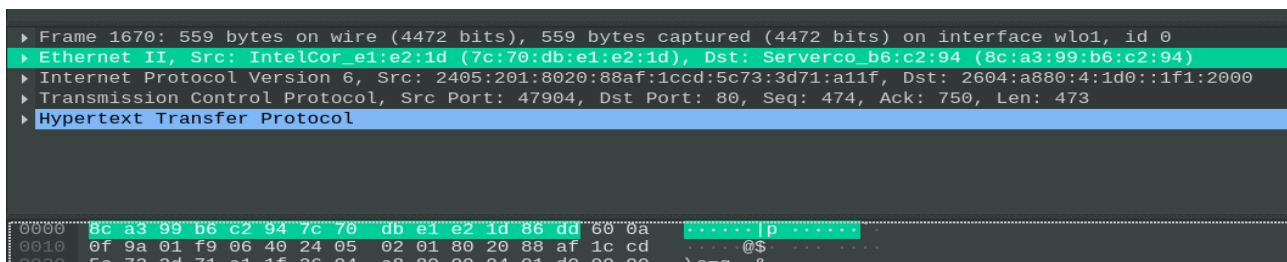


So according to the details, my PC's Network Interface Card (NIC) has the manufacturer: IntelCor.

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:

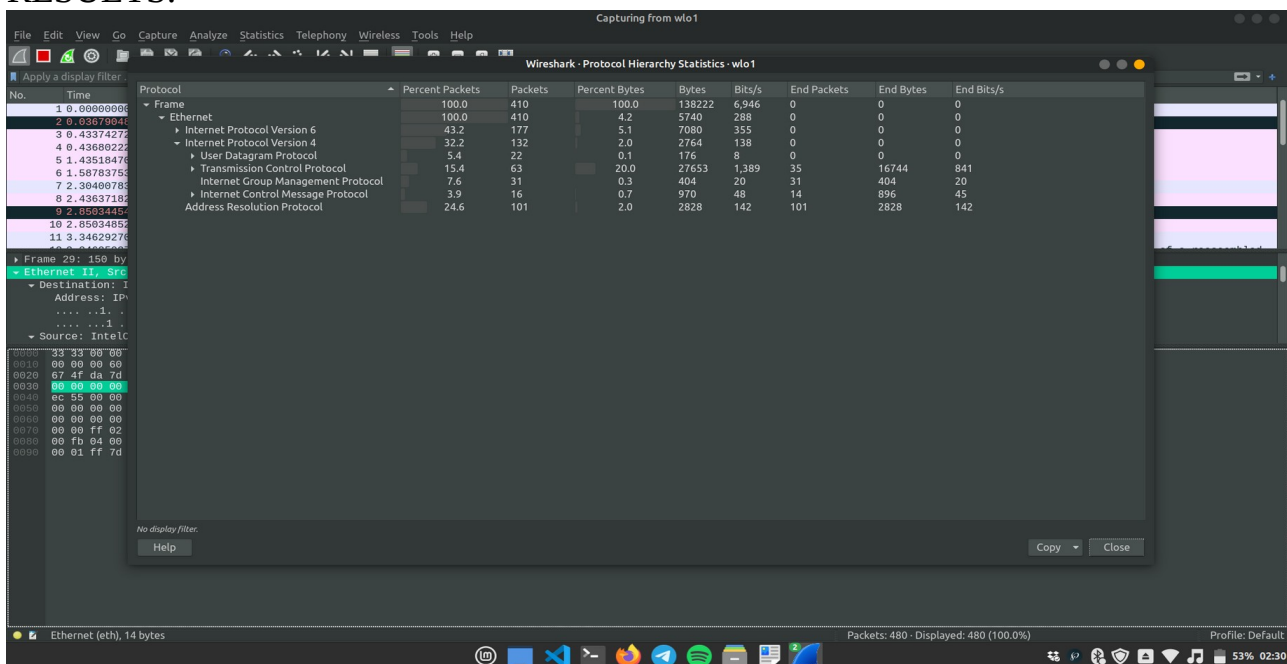


Ans: The hex values (shown the raw bytes panel) of the two NICs Manufacturers OUIs are: 8c a3 99 b6 c2 94 (my NIC raw bytes) and 7c 70 db e1 e2 1d 86 dd (server NIC)

Q9) Find the following statistics:

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

RESULTS:

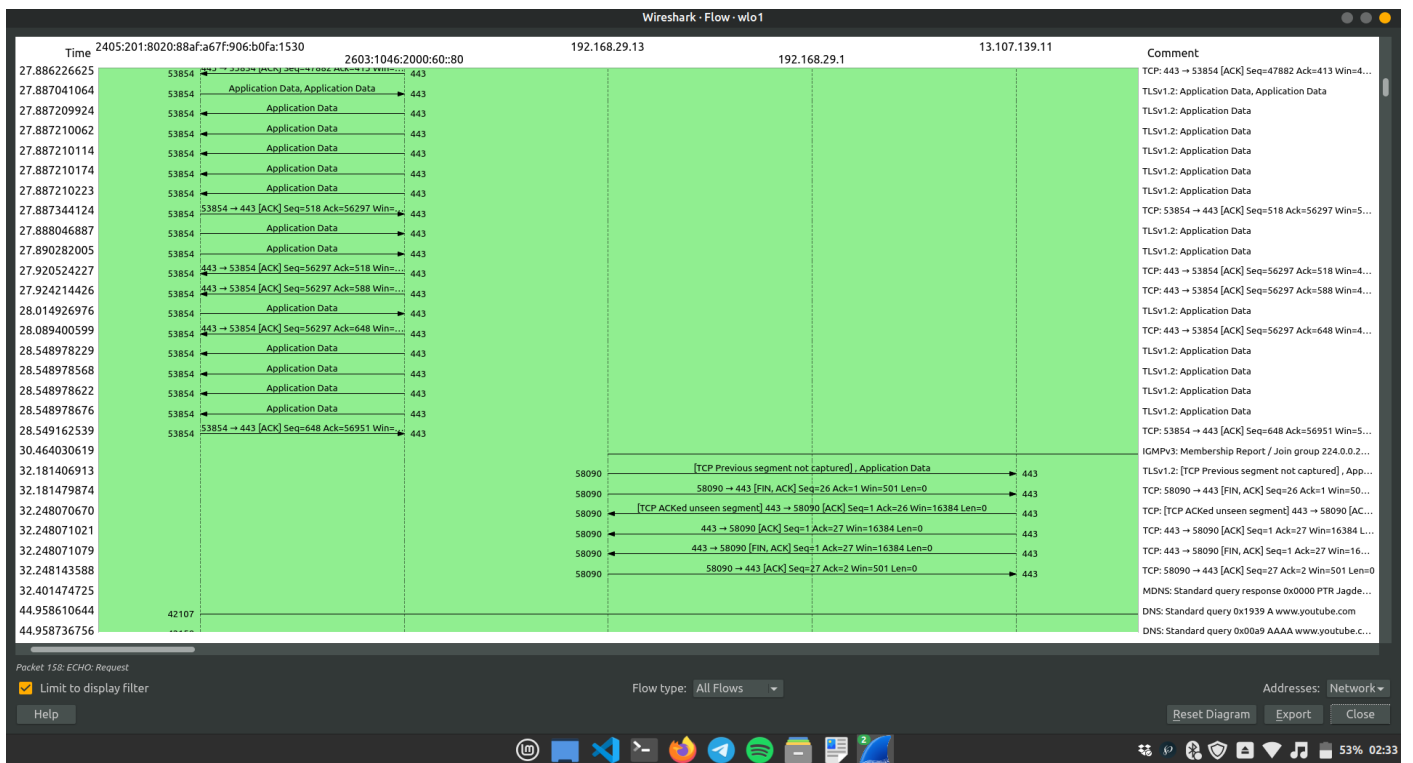


Ans: a) From the above statistics, the percentage of TCP packets is 15.4%

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