Part 1

1. Find the IP address of your machine, subnet mask, and network ID of your subnet.

Sol:

IP address = 10.145.73.75 with /17 subnet
subnet mask = 255.255.128.0
Network ID :

Ip	00001010.10010001.01001001.01001011
mask	11111111.11111111.10000000.00000000
AND	00001010.10010001.00000000.00000000

-> decimal 10.145.0.0
Network ID = 10.145.0.0

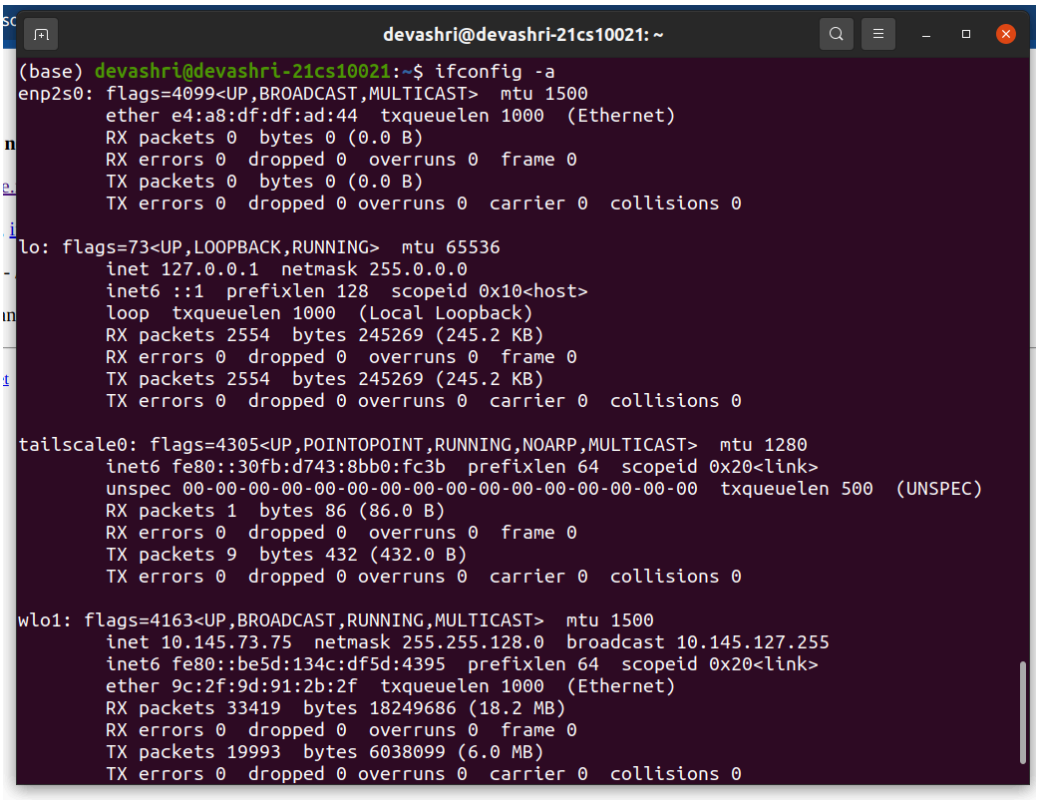


fig . 1 Showing IP, mask

2. Find the IP address associated with www.google.com and www.facebook.com using nslookup. Change the DNS server address in the nslookup command to the following four IP addresses: 172.16.1.164, 172.16.1.180, 172.16.1.165, and 172.16.1.166, and see whether the IP address of the above domain name (www.google.com) changes. If you see a change in the IP address of www.google.com, can you think of the reason behind the same?

Sol:

IP address associated with www.google.com = 142.250.192.100
IP address associated with www.facebook.com = 31.13.79.35
with default DNS server address 127.0.0.53

IP address of www.google.com with different DNS server addresses:
172.16.1.164 → 142.250.67.164
172.16.1.180 → 142.250.207.228
172.16.1.165 → 142.250.192.100
172.16.1.166 → 142.250.77.36

The IP address of google changes with change of DNS server address.

As some local DNS server is providing the IP address of the domain we requested, changing that DNS server itself will result in a change of IP address of domain coming from them.Each DNS server can return different results based on factors like caching, location, or which authoritative name server they query.

```
(base) devashri@devashri-21cs10021:~$ nslookup www.google.com 172.16.1.164
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.67.164
Name:   www.google.com
Address: 2404:6800:4009:826::2004

(base) devashri@devashri-21cs10021:~$ nslookup www.google.com 172.16.1.180
Server:         172.16.1.180
Address:        172.16.1.180#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.207.228
Name:   www.google.com
Address: 2404:6800:4002:81f::2004

(base) devashri@devashri-21cs10021:~$ nslookup www.google.com 172.16.1.165
Server:         172.16.1.165
Address:        172.16.1.165#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.100
Name:   www.google.com
Address: 2404:6800:4009:82a::2004

(base) devashri@devashri-21cs10021:~$ nslookup www.google.com 172.16.1.166
Server:         172.16.1.166
Address:        172.16.1.166#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.77.36
Name:   www.google.com
Address: 2404:6800:4009:81c::2004
```

3. Ping the IP address of one of your friend's machine IP within the software lab. Send the ping packets with different packet sizes (64, 128, 512 bytes) and timeout (100) for reporting packet loss percentage, min, avg, max, and stddev of round-trip time.

Sol:

Fig 5 below answers the above question. One observation: extra 8 bytes are getting added in ping packets, that is because of 8-byte ICMP header. Also,additionally the IP header brings 20 more bytes, resulting in 92 bytes.

```
(base) devashri@devashri-21cs10021:~$ ping 10.5.16.31 -s 64 -W 100
PING 10.5.16.31 (10.5.16.31) 64(92) bytes of data.
72 bytes from 10.5.16.31: icmp_seq=1 ttl=61 time=4.09 ms
72 bytes from 10.5.16.31: icmp_seq=2 ttl=61 time=1.66 ms
72 bytes from 10.5.16.31: icmp_seq=3 ttl=61 time=21.3 ms
72 bytes from 10.5.16.31: icmp_seq=4 ttl=61 time=2.10 ms
72 bytes from 10.5.16.31: icmp_seq=5 ttl=61 time=1.65 ms
^C
--- 10.5.16.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.654/6.153/21.269/7.610 ms
(base) devashri@devashri-21cs10021:~$ ping 10.5.16.31 -s 128 -W 100
PING 10.5.16.31 (10.5.16.31) 128(156) bytes of data.
136 bytes from 10.5.16.31: icmp_seq=1 ttl=61 time=5.64 ms
136 bytes from 10.5.16.31: icmp_seq=2 ttl=61 time=1.34 ms
136 bytes from 10.5.16.31: icmp_seq=3 ttl=61 time=2.19 ms
136 bytes from 10.5.16.31: icmp_seq=4 ttl=61 time=1.74 ms
136 bytes from 10.5.16.31: icmp_seq=5 ttl=61 time=2.43 ms
^C
--- 10.5.16.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.340/2.668/5.640/1.532 ms
(base) devashri@devashri-21cs10021:~$ ping 10.5.16.31 -s 512 -W 100
PING 10.5.16.31 (10.5.16.31) 512(540) bytes of data.
520 bytes from 10.5.16.31: icmp_seq=1 ttl=61 time=61.0 ms
520 bytes from 10.5.16.31: icmp_seq=2 ttl=61 time=3.91 ms
520 bytes from 10.5.16.31: icmp_seq=3 ttl=61 time=2.10 ms
520 bytes from 10.5.16.31: icmp_seq=4 ttl=61 time=3.03 ms
520 bytes from 10.5.16.31: icmp_seq=5 ttl=61 time=19.7 ms
^C
--- 10.5.16.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.100/17.961/61.021/22.490 ms
(base) devashri@devashri-21cs10021:~$
```

4. Run traceroute for www.google.com and print the summary. Count the number of hosts involved in the path from source to destination. Why do you see some "* * *" in the intermediate hops?

```
(base) devashri@devashri-21cs10021:~$ traceroute -4 142.250.192.100
traceroute to 142.250.192.100 (142.250.192.100), 30 hops max, 60 byte packets
 1  10.145.0.3 (10.145.0.3)  1.753 ms  1.778 ms  1.873 ms
 2  10.120.0.25 (10.120.0.25)  2.041 ms  2.040 ms  2.055 ms
 3  10.255.1.3 (10.255.1.3)  4.551 ms  4.719 ms  26.336 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  72.14.204.62 (72.14.204.62)  102.155 ms  102.119 ms 142.250.172.80 (142.250.172.80)  102.461 ms
 9  * * *
10  142.250.228.48 (142.250.228.48)  103.667 ms 142.250.61.202 (142.250.61.202)  136.755 ms 192.178.86.246 (192.178.86.246)  71.487 ms
11  142.250.208.226 (142.250.208.226)  104.160 ms 72.14.237.139 (72.14.237.139)  103.865 ms 192.178.110.244 (192.178.110.244)  105.108 ms
12  192.178.110.205 (192.178.110.205)  103.321 ms 192.178.110.107 (192.178.110.107)  78.669 ms 192.178.110.207 (192.178.110.207)  56.017 ms
13  72.14.237.139 (72.14.237.139)  49.062 ms bom12s17-in-f4.1e100.net (142.250.192.100)  56.877 ms  60.633 ms
(base) devashri@devashri-21cs10021:~$ traceroute -4 www.google.com
traceroute to www.google.com (142.250.77.36), 30 hops max, 60 byte packets
 1  10.145.0.3 (10.145.0.3)  0.799 ms  0.974 ms  1.139 ms
 2  10.120.0.25 (10.120.0.25)  1.180 ms  1.299 ms  1.411 ms
 3  10.255.1.3 (10.255.1.3)  4.388 ms  4.114 ms  4.232 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  72.14.204.62 (72.14.204.62)  110.006 ms  109.801 ms  109.628 ms
 9  * * *
10  72.14.237.10 (72.14.237.10)  104.381 ms 192.178.86.240 (192.178.86.240)  104.039 ms 172.253.77.22 (172.253.77.22)  209.360 ms
11  192.178.110.106 (192.178.110.106)  103.415 ms 192.178.110.206 (192.178.110.206)  209.379 ms 142.250.238.203 (142.250.238.203)  103.280 ms
12  142.250.226.135 (142.250.226.135)  105.015 ms bom07s26-in-f4.1e100.net (142.250.77.36)  41.058 ms 192.178.111.61 (192.178.111.61)  66.955 ms
(base) devashri@devashri-21cs10021:~$
```

Hops in 1st traceroute = 12
Hops in 2nd traceroute = 11
We see "***" in intermediate hops due to no response in traceroute timeout.
→A router is configured to ignore traceroute/ICMP packets.
→A firewall is blocking the ICMP "time exceeded" replies.
→Network congestion or any other issue causing the response to drop.

Part 2

1. Analysis of DNS Packets

a) Locate the DNS query and response messages. Is DNS using UDP or TCP in the observed packets?

Sol:

DNS is using UDP for observed packets. (shown in fig 6)

b) Check the source and destination IP address of the DNS query.

Sol:

Source: 172.16.1.166
Destination: 10.146.31.25 (my machine ip is different because wifi is different now!!)

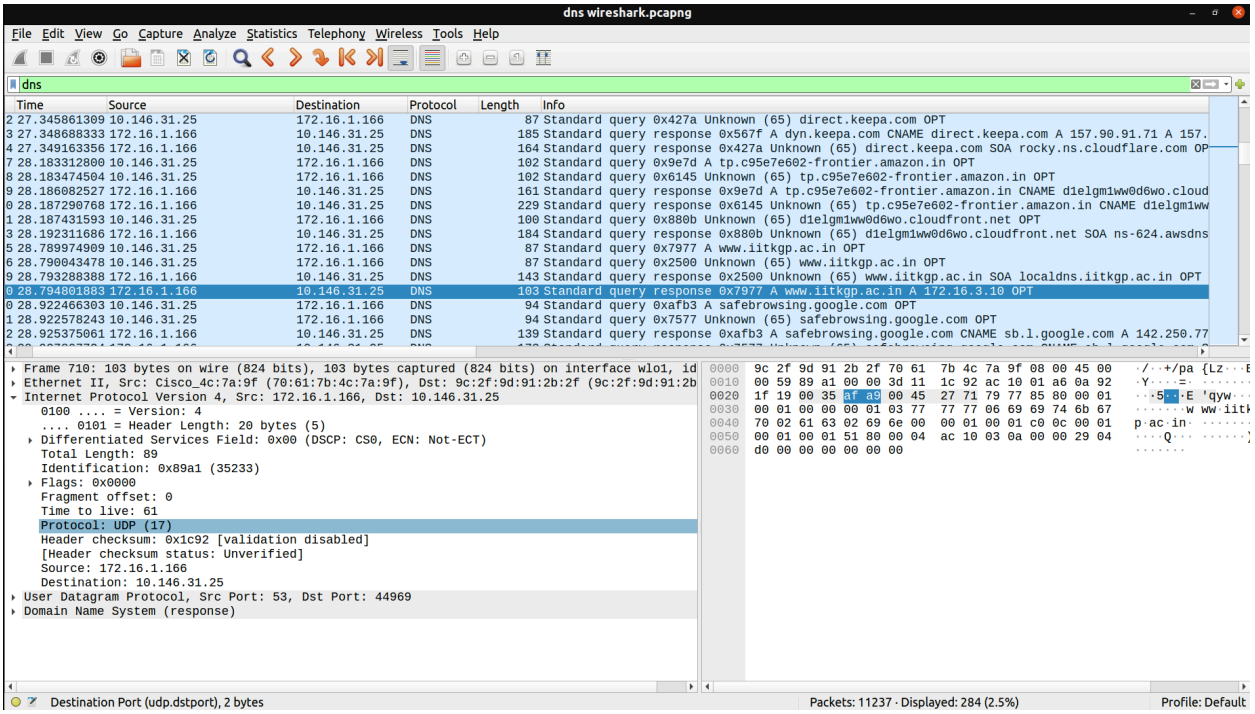


Fig 6

c) How many DNS queries are sent from your browser (host machine) to DNS Server(s) during the name-to-IP resolution?

Sol: 2 DNS queries are sent from the host machine to the dns server. (shown below fig7).
Used filter "dns.flags.response==0 and dns.qry.name contains iitkgp.ac.in"
dns.flags.response==0 for queries from source (my host) to destination.
dns.qry.name to filter domain name.

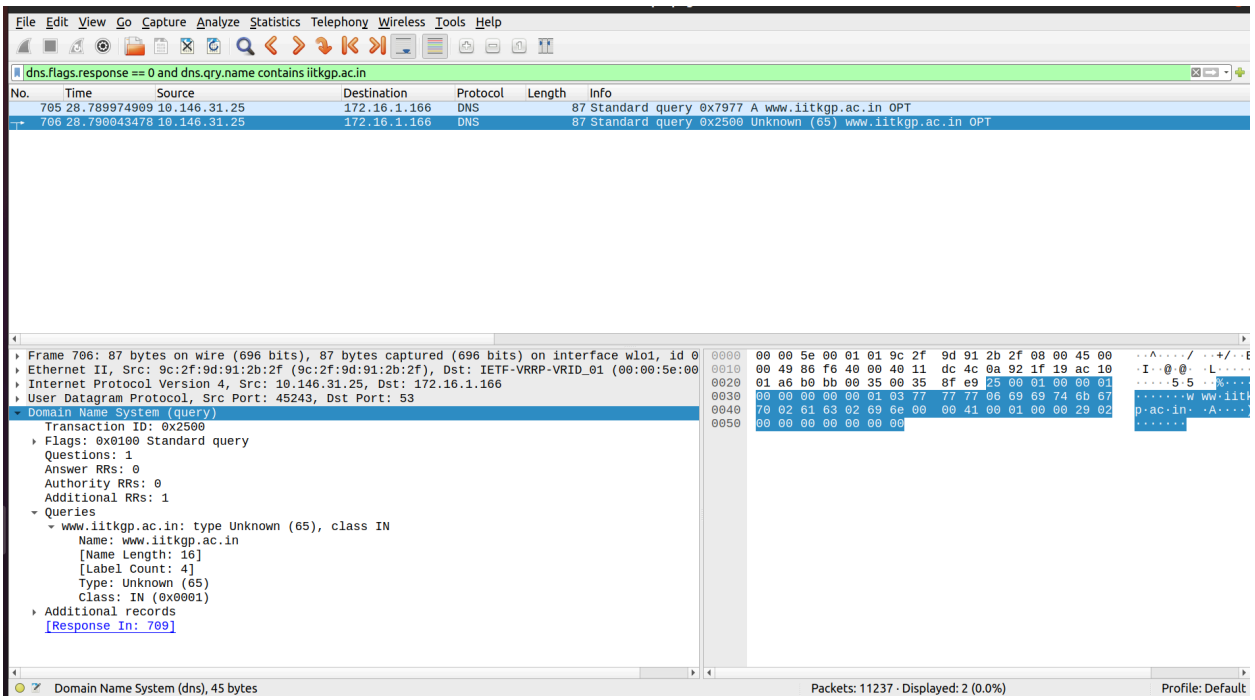


Fig 7

d) Which DNS Server replies with actual IP Address(es).

Sol:

source IP of DNS server that responds IP of www.iitkgp.ac.in : 172.16.1.166

IP Address of domain www.iitkgp.ac.in provided : 172.16.3.10 as shown in fig 8

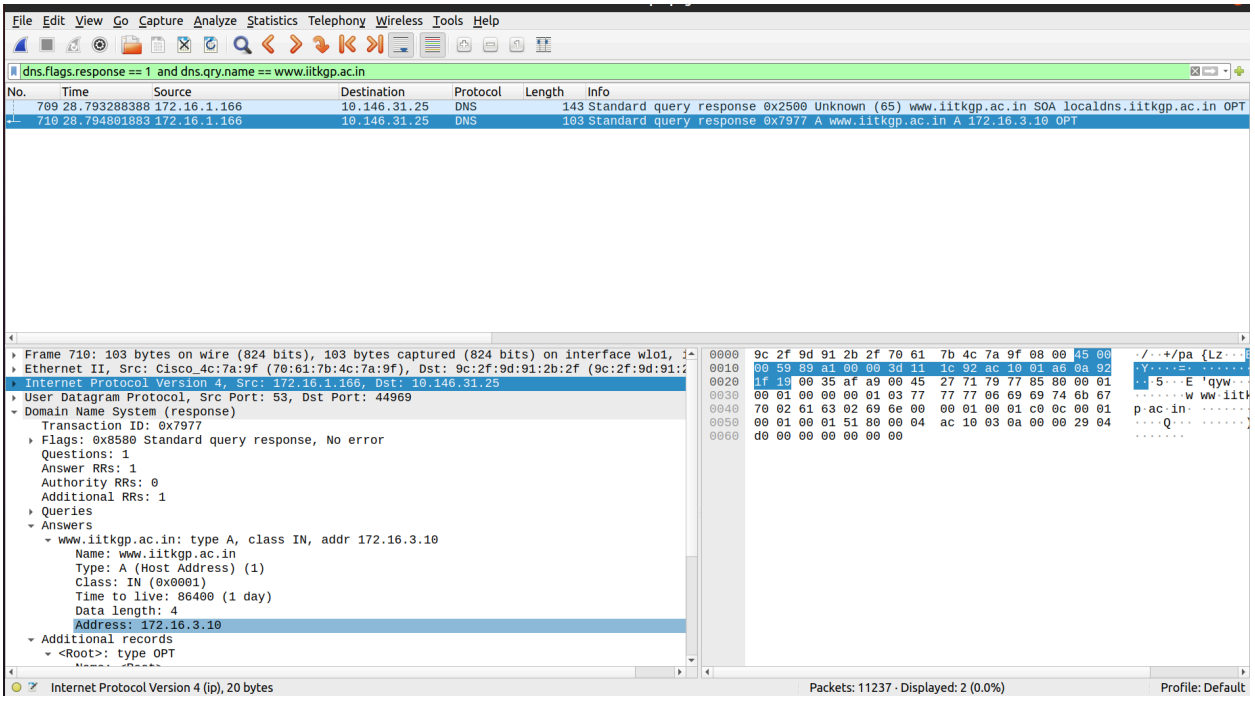


Fig 8

e) How many DNS servers are involved? Do all DNS servers respond?

Sol:

Only one DNS server (172.16.1.166) was involved in responding.

Yes, all servers are responding. (ie., only 1 server in this case) see fig 9 and details ↓

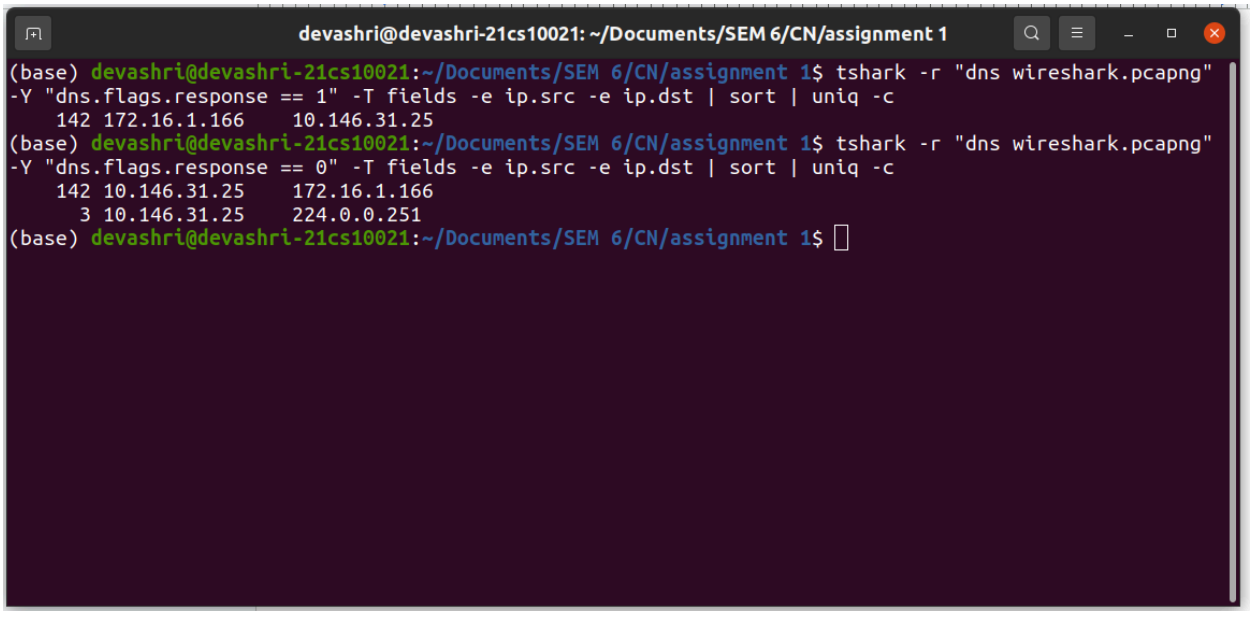


fig 9

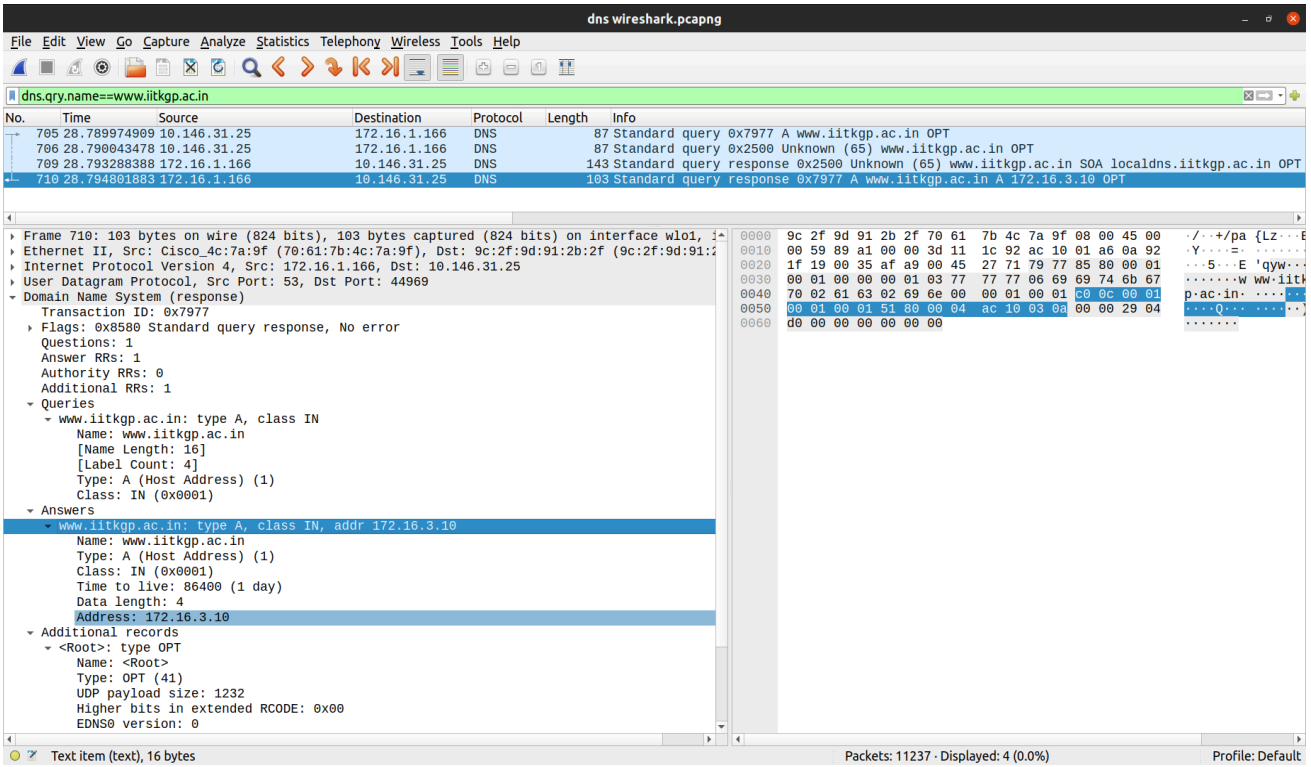
tshark -r "dns wireshark.pcapng" → Reads the pcapng file
-Y "dns.flags.response == 1" → Filters only DNS response packets.
-T fields -e ip.src -e ip.dst → Extracts source and destination IP addresses (i.e.,DNS servers).
sort | uniq -c → Sorts and counts the unique DNS server IPs.

f) Clearly list the resource records involved in resolving the site's IP address, mentioning Name, Type, Class, TTL, Data length, and resolved IP address appropriately in the complete resolving process of this DNS conversation, including query/queries and response/answer(s).

Sol:

Queries
www.iitkgp.ac.in: type A, class IN
Name: www.iitkgp.ac.in
[Name Length: 16]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
www.iitkgp.ac.in: type A, class IN, addr 172.16.3.10
Name: www.iitkgp.ac.in
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 86400 (1 day)
Data length: 4
Address: 172.16.3.10



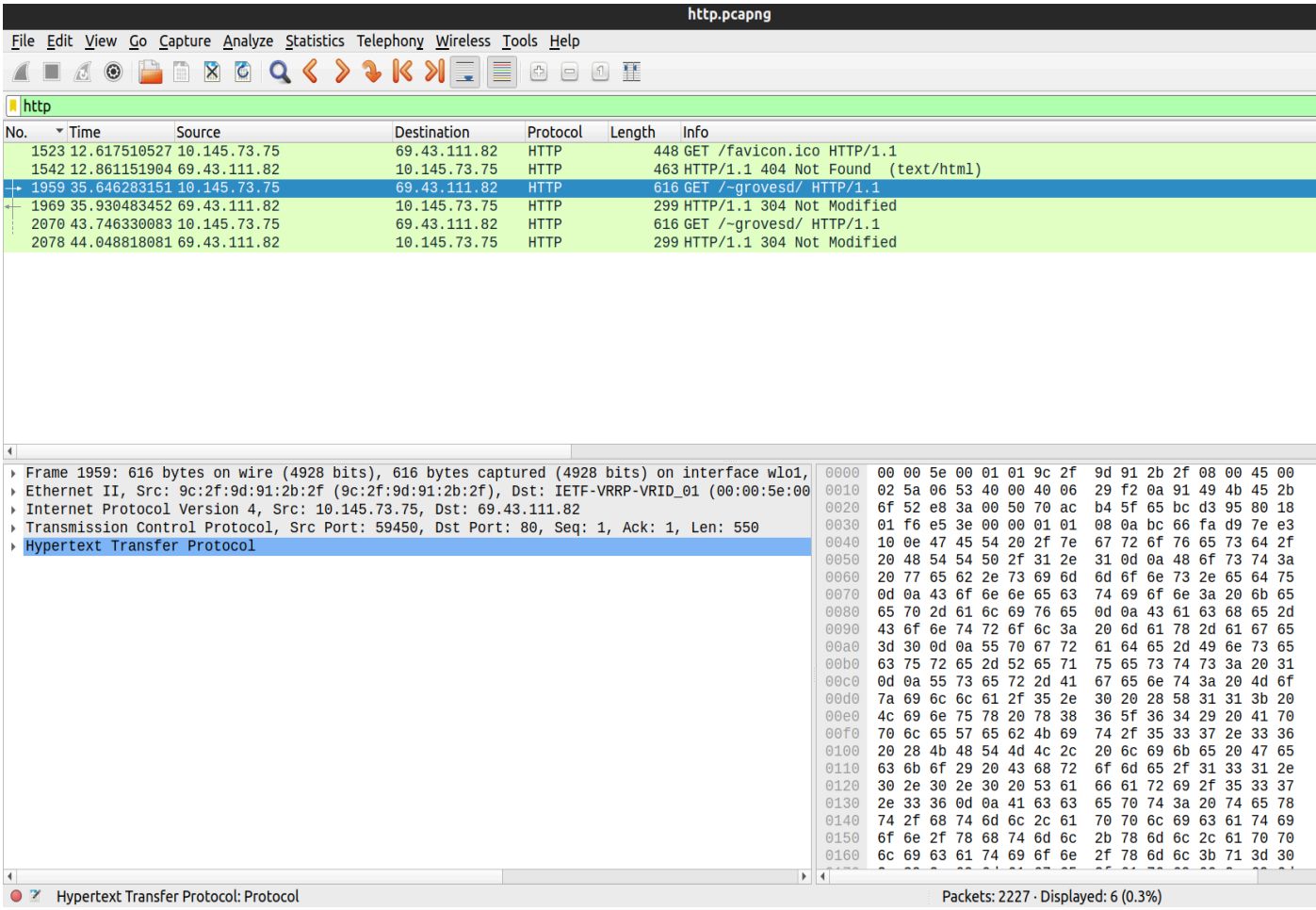
2. Web Traffic (HTTP)

a) Filter the HTTP packets and observe traffic between the client and the web server.

Sol:

Local machine: 10.145.73.75 -client

IP address : 69.43.111.82 -web server



ASSIGNMENT 1: Networking Tools and Wireshark

b) Check the header of the HTTP packet and try to identify the HTTP request and response.

Sol:

Request:

Hypertext Transfer Protocol

GET /~grovesd/ HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /~grovesd/ HTTP/1.1\r\n]

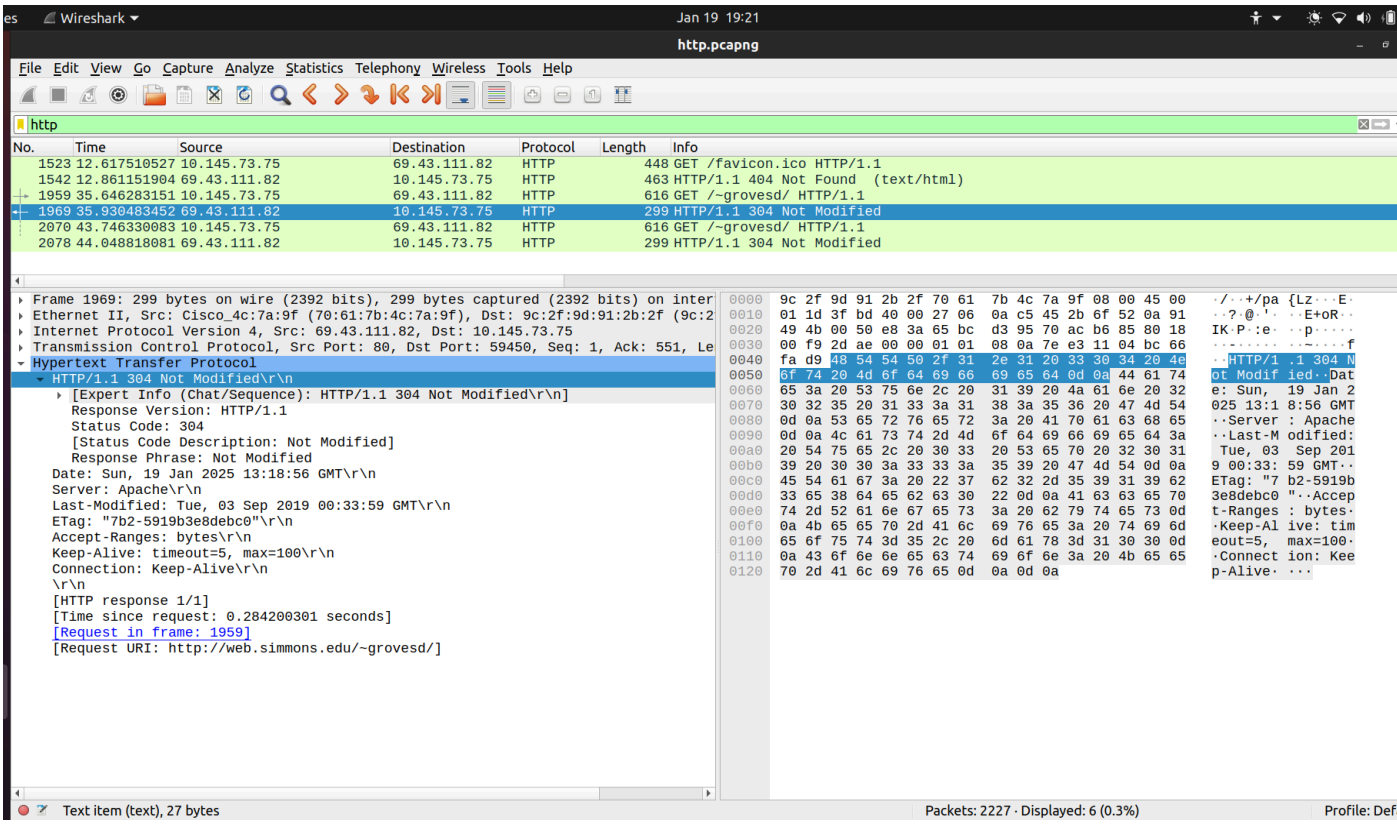
Request Method: GET

Request URI: /~grovesd/

Request Version: HTTP/1.1

Host: web.simmons.edu\r\n

Connection: keep-alive\r\n



Response:

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

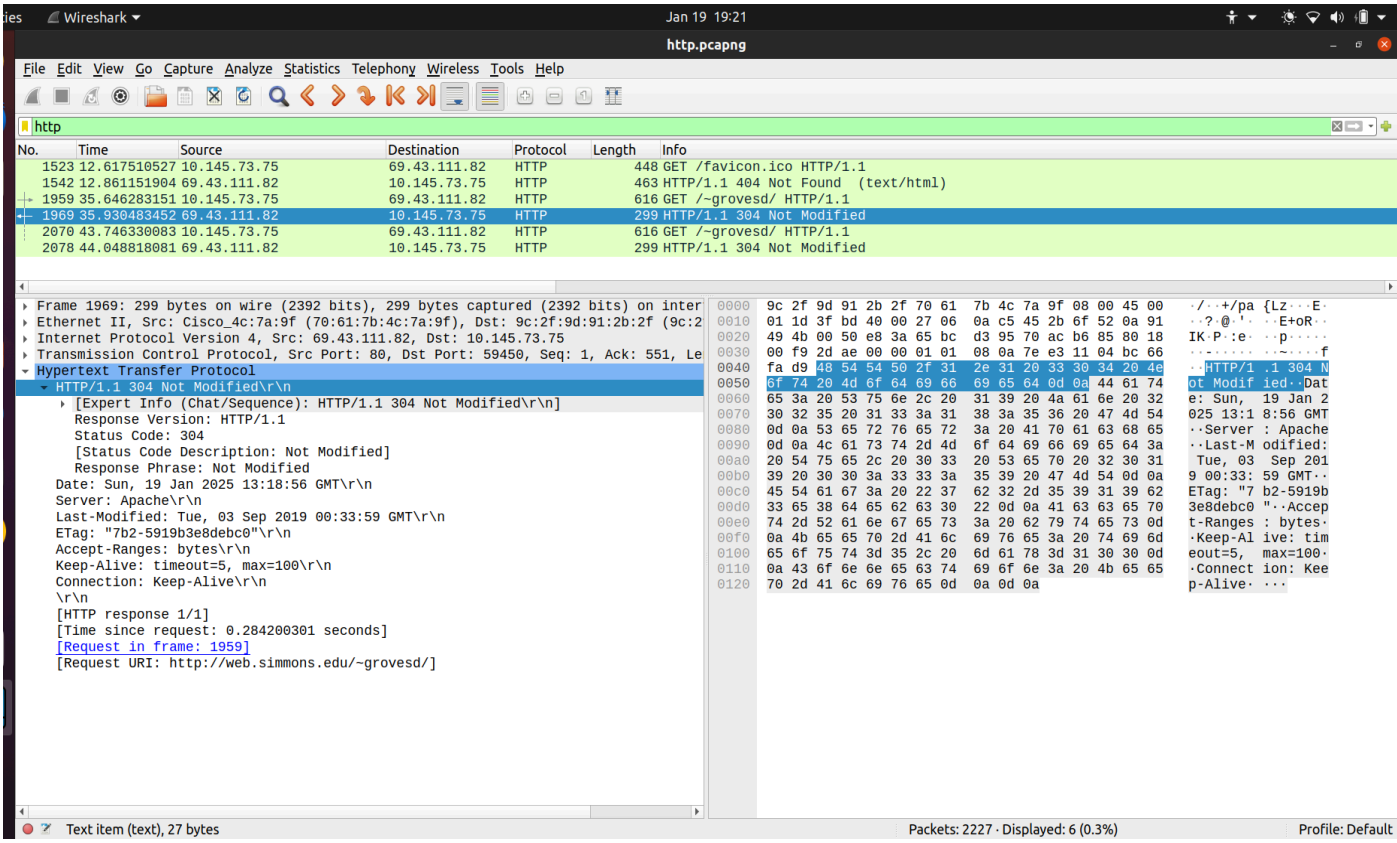
Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

ASSIGNMENT 1: Networking Tools and Wireshark

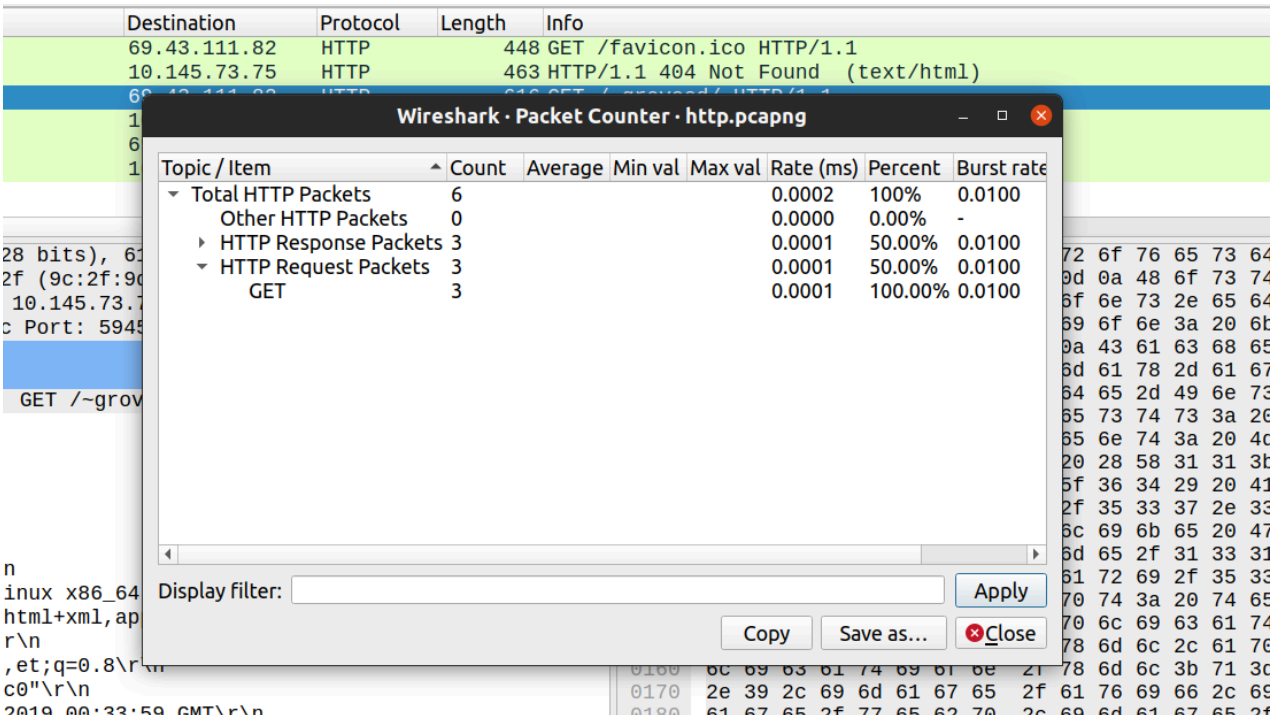


c) How many HTTP packets are exchanged between client and server to load an entire web page?

Sol:

6 HTTP packets are exchanged between client and server to load an entire web page.

Also shown in fig below:



3. ICMP Traffic (Ping/Traceroute)

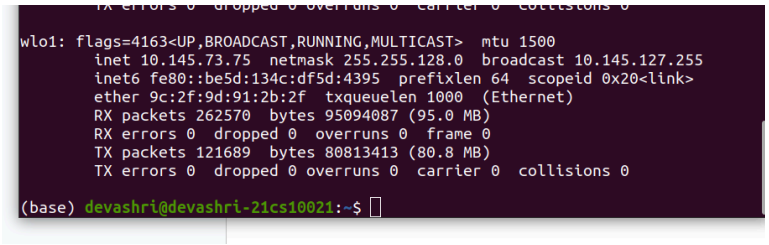
a) Run ‘ping’ and ‘traceroute’ commands to initiate ICMP traffic for your friend's machine and capture it through Wireshark. Inspect & crosscheck the Source and Destination IP address of captured ICMP packets.

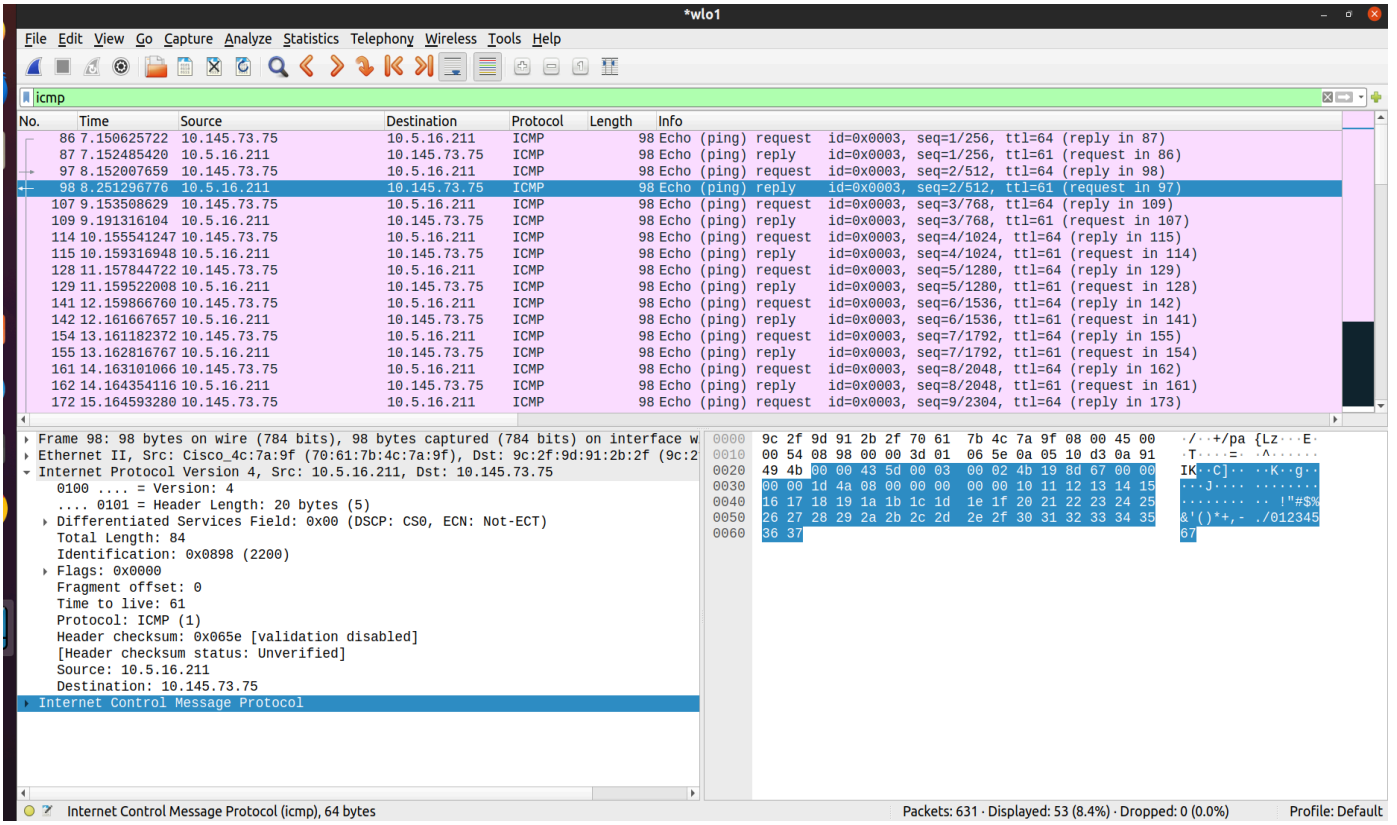
Sol:

Source IP = 10.145.73.75

Destination IP = 10.5.16.211

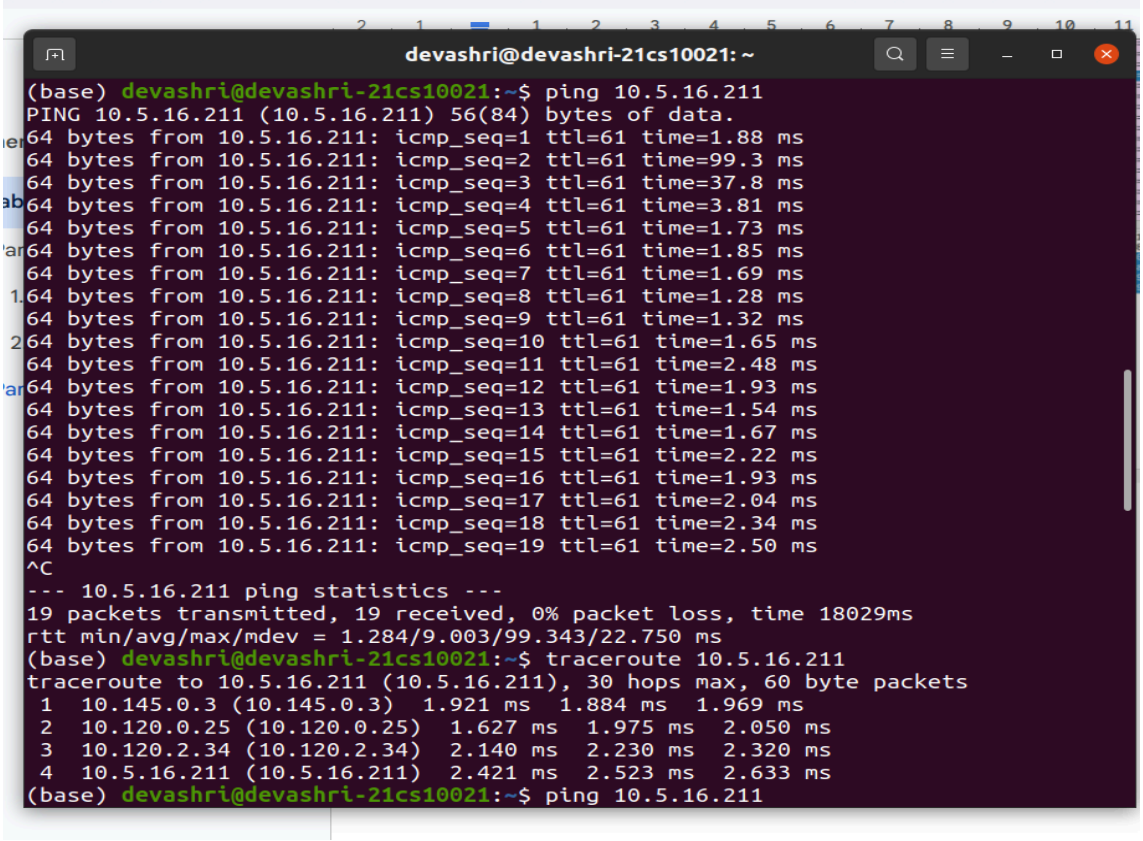
crosschecked from terminal as well as wireshark, in figs below.





Request and reply between local host and friend’s machine.

ASSIGNMENT 1: Networking Tools and Wireshark



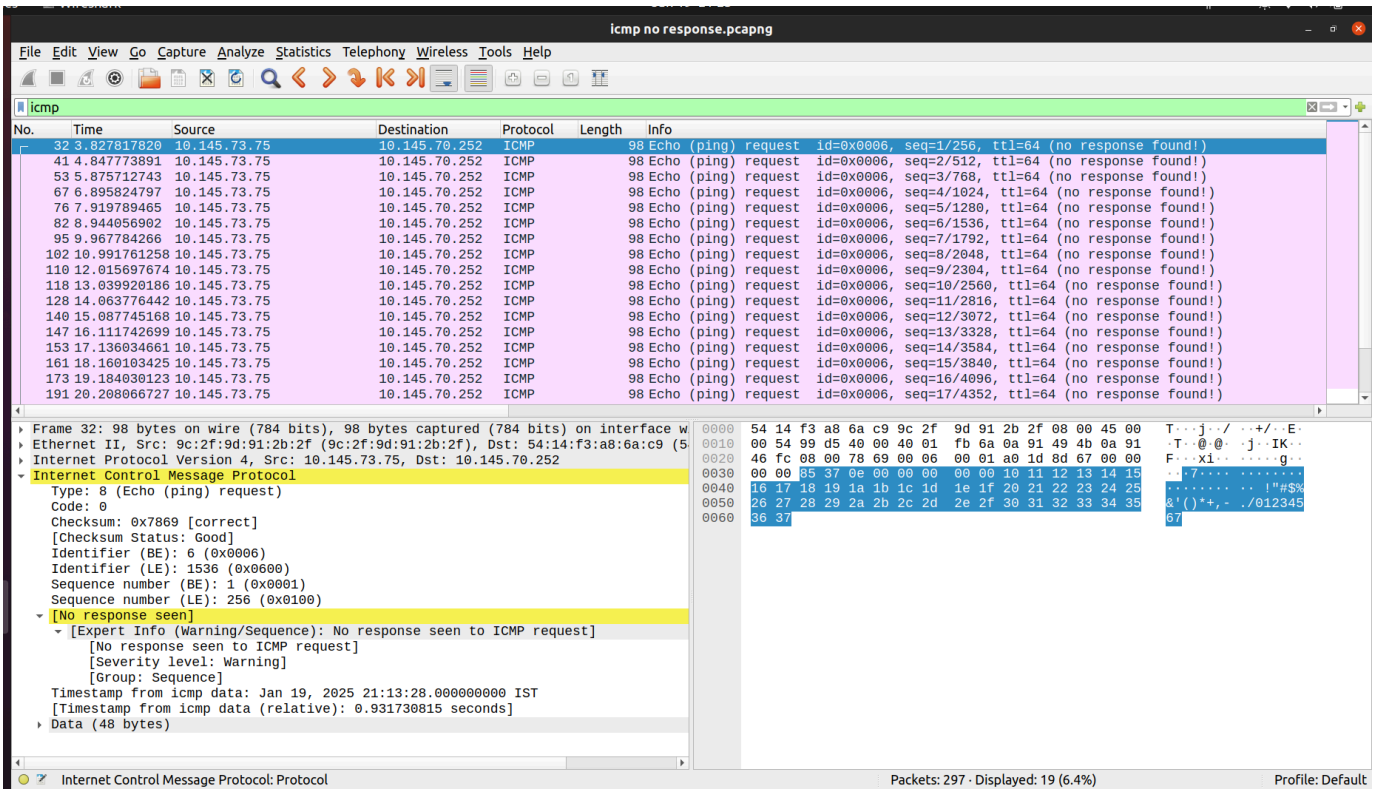
b) Send a ping to an unreachable host (e.g., a host with IP 192.168.31.3 does not exist in the IIT KGP network) and analyze ICMP no-response packets.
Sol:

Source IP: 10.145.73.75
Destination IP: 10.145.70.252
Destination was a windows laptop on the same network but with firewall on. We could only ping it when its firewall was off.

ICMP Packet Details:
Type: 8 (Echo Request)
Code: 0 (indicating a standard ping request)
Sequence Number: Incremented with each request.

Expert Info in Wireshark:
"No response seen to ICMP request."
This indicates that the host did not reply with an ICMP Echo Reply (Type 0).

ASSIGNMENT 1: Networking Tools and Wireshark



c) Perform a 'traceroute' operation for both reachable and unreachable hosts and prepare a brief report of your observation using Wireshark.

Sol:

Traceroute for reachable host:
It connects with an intermediate server with limited TTL and hops on next till it reaches the destination IP. ICMP **"Time-to-live exceeded"** messages show packets reaching routers along the route.

Traceroute for unreachable host:
ICMP **"Destination Unreachable (Port Unreachable)"** shows that the host exists but is not accepting connections. Also in terminal it shows ***, ***, ***, *** on screen as it does not get reply from destination host.

- If **TTL exceeded messages are returned**, it means:
  The packet is successfully **hopping through routers** towards the destination.
  The network path is **functioning properly**.
- If the host were **completely unreachable**, we would expect:
  No response at all or
  ICMP "Destination Unreachable" messages early in the path.

ASSIGNMENT 1: Networking Tools and Wireshark