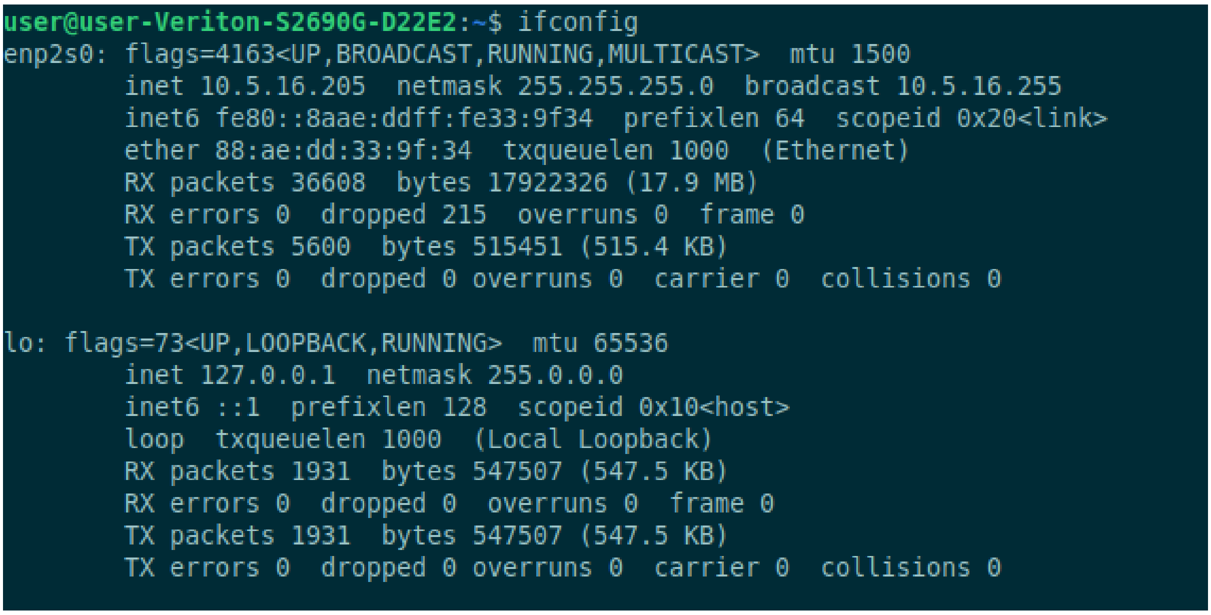
Assignment 1:
Networking Tools and Wireshark

Part 1: Networking Tools

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

IP Address: A 32-bit unique identifier that each device receives when it connects to a network. It may be public or private, and may be static (same address) or dynamic (change with time, when the device is connected again).
In general, the first 24-bits of an IP-Address give the identity of a network, and next 8-bits give the identity for the host device connected on that network. But an actual distinction between network and host identifiers is given by the Subnet Mask.

Subnet Mask: A 32-bit number in which the trailing number of 0's give the number of trailing bits in the IP-Address of the host device and the remaining bits signify network. Usually, the Subnet Mask is of the form 255.255.255.0, which is why the first 24 bits give network, and the last 8, host.



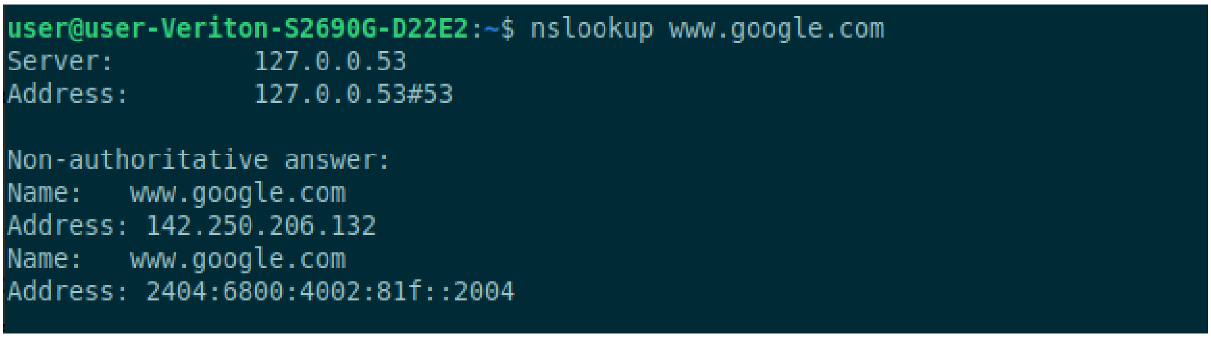
```
user@user-Veriton-S2690G-D22E2:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.5.16.205  netmask 255.255.255.0  broadcast 10.5.16.255
        inet6 fe80::8aae:ddff:fe33:9f34  prefixlen 64  scopeid 0x20<link>
        ether 88:ae:dd:33:9f:34  txqueuelen 1000  (Ethernet)
        RX packets 36608  bytes 17922326 (17.9 MB)
        RX errors 0  dropped 215  overruns 0  frame 0
        TX packets 5600  bytes 515451 (515.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1931  bytes 547507 (547.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1931  bytes 547507 (547.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

In this screenshot, we can see that, for the lab machine in use:
IP-Address: 10.5.16.205
Subnet Mask: 255.255.255.0
Network ID: 10.5.16 (Since the last 8-bits of the Subnet are 0's, they are for the host device (the lab machine), and rest give the Network ID)

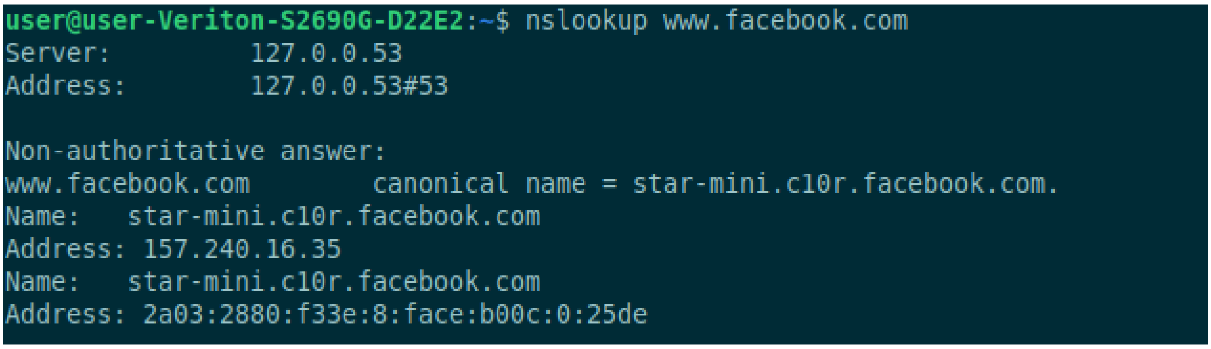
2. ***Find the IP address associated with www.google.com and www.facebook.com using nslookup.***

Nslookup: A network administration tool for **querying** the Domain Name System (DNS)

What is included in the nslookup command response?
Server: The DNS server that was used to translate the domain name into its IP-Address.
Address: The IP-Address for the DNS server along with the port number
Non-Authoritative Answer: The resolved IP-Address of the domain name entered, received from the cache memory of the DNS server (that is why it is non-authoritative).



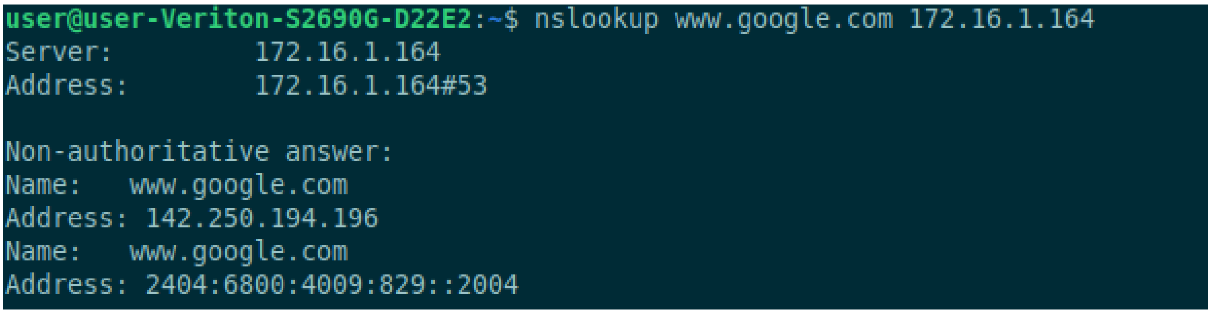
```
user@user-Veriton-S2690G-D22E2:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.206.132
Name:   www.google.com
Address: 2404:6800:4002:81f::2004
```



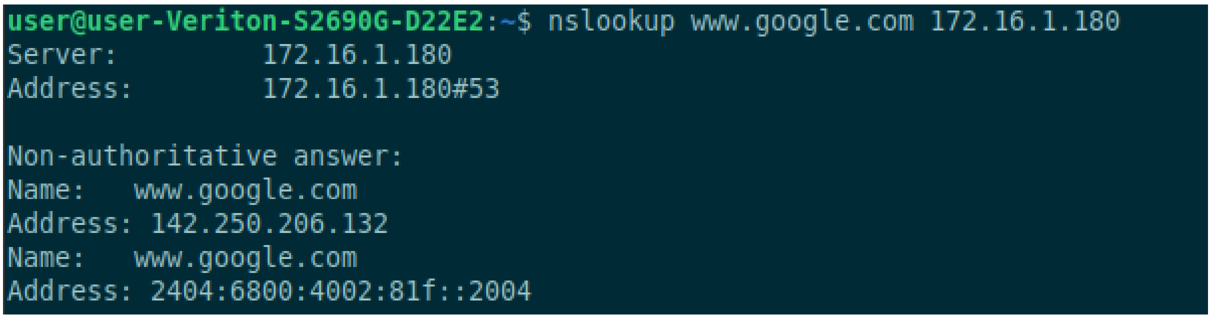
```
user@user-Veriton-S2690G-D22E2:~$ nslookup www.facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.16.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f33e:8:face:b00c:0:25de
```

Website	**IP-Address**	**DNS-Server used**	**Port Number used for DNS query**
www.google.com	142.250.206.132	127.0.0.53	53
www.facebook.com	157.240.16.35	127.0.0.53	53

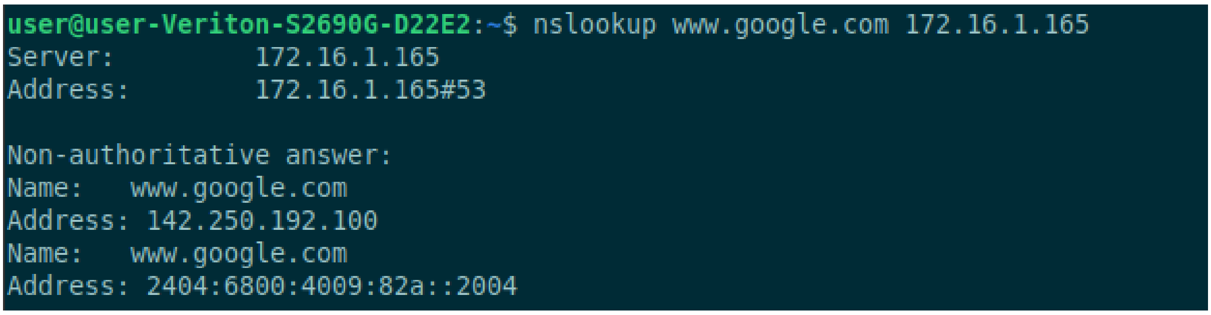
In the following part of the question, a custom IP-Address is added in the nslookup command which changes the DNS server to query. The address: 127.0.0.53 is the IP-Address that is default for the machine, but when we change them to 172.16.1.xxx, we query the respective servers.



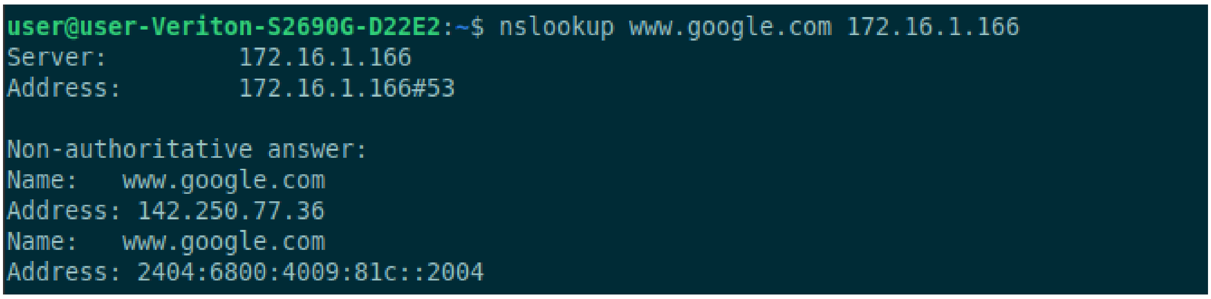
```
user@user-Veriton-S2690G-D22E2:~$ nslookup www.google.com 172.16.1.164
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.196
Name:   www.google.com
Address: 2404:6800:4009:829::2004
```



```
user@user-Veriton-S2690G-D22E2:~$ 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: 142.250.206.132
Name:   www.google.com
Address: 2404:6800:4002:81f::2004
```



```
user@user-Veriton-S2690G-D22E2:~$ 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
```



```
user@user-Veriton-S2690G-D22E2:~$ 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
```

Now, as can be seen in the screenshots, the IP-Address for www.google.com is not the same.

According to me, this could be because of the following 3 reasons:
1. Different DNS Servers are located at different places, so are the google servers. When we query a particular DNS server to resolve the domain name, it may fetch the address of the google server in some way.

2. A DNS Server caches the address for quicker resolving. It may return that address, but it is not necessary that when we actually search www.google.com, we get the same address (because, in the meantime, probably one server may get loaded, and we may need to connect to a different google server. So even though the cache memory stores the most frequently resolved ip, real-time network traffic may change actual IPs).

3. Google may be routing the requests to different servers based on its load-balancing techniques. So, it may happen that during the time different nslookup commands were run, the DNS server may have had to send the request to a server that was not already loaded.

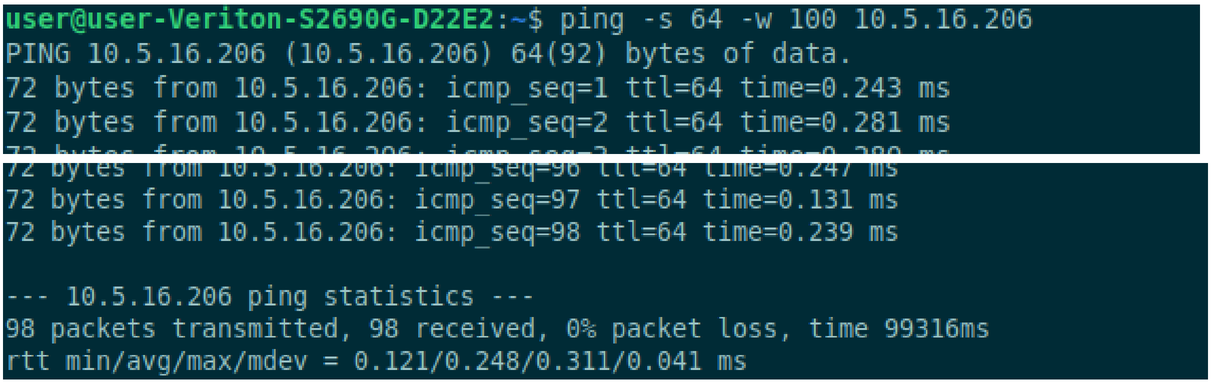
3. Ping the IP address of one of your friend's machine IP within the software lab and report the packet loss percentage, min, avg, max, and std. dev. of round-trip time.

Ping (Packet Internet Groper): is a command that allows users to test and verify the existence of connection between the host machine and the entered destination IP-Address. It also gives statistics that help in determining time taken for data to travel between the two devices.

Ping sends an **ICMP (Internet Control Message Protocol) Echo Request** to the target network interface and waits for a response (an **Echo-Reply**). This method allows to calculate RTT (Round-trip time) and also ensure that the target is available.

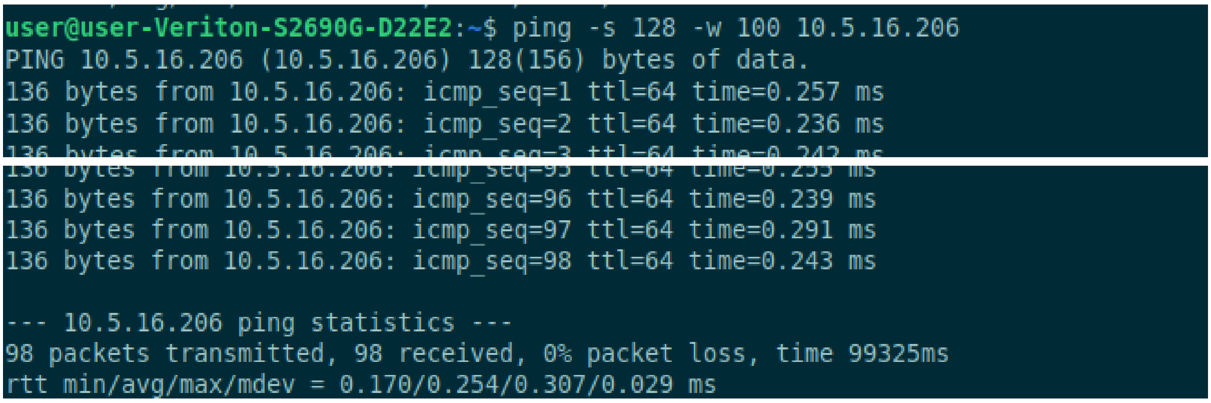
Ping Options used in the command:
-s   : custom packet size
-w : timeout (time after which Packet sending will automatically be stopped)
-W : timeout (time for which if no response is received, packet sending will be stopped)

Pinging with packet size 64 bytes:



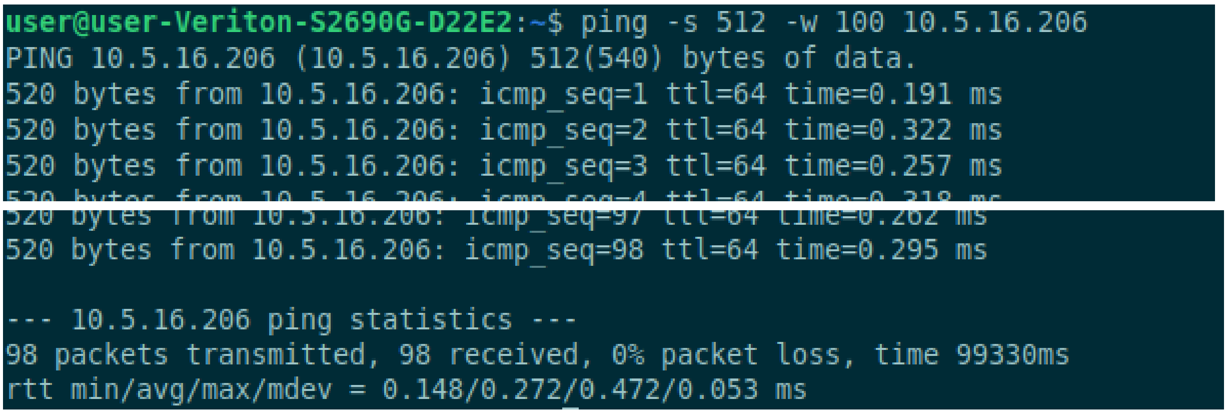
```
user@user-Veriton-S2690G-D22E2:~$ ping -s 64 -w 100 10.5.16.206
PING 10.5.16.206 (10.5.16.206) 64(92) bytes of data.
72 bytes from 10.5.16.206: icmp_seq=1 ttl=64 time=0.243 ms
72 bytes from 10.5.16.206: icmp_seq=2 ttl=64 time=0.281 ms
72 bytes from 10.5.16.206: icmp_seq=3 ttl=64 time=0.280 ms
72 bytes from 10.5.16.206: icmp_seq=96 ttl=64 time=0.247 ms
72 bytes from 10.5.16.206: icmp_seq=97 ttl=64 time=0.131 ms
72 bytes from 10.5.16.206: icmp_seq=98 ttl=64 time=0.239 ms

--- 10.5.16.206 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99316ms
rtt min/avg/max/mdev = 0.121/0.248/0.311/0.041 ms
```

Pinging with packet size 128 bytes:



```
user@user-Veriton-S2690G-D22E2:~$ ping -s 128 -w 100 10.5.16.206
PING 10.5.16.206 (10.5.16.206) 128(156) bytes of data.
136 bytes from 10.5.16.206: icmp_seq=1 ttl=64 time=0.257 ms
136 bytes from 10.5.16.206: icmp_seq=2 ttl=64 time=0.236 ms
136 bytes from 10.5.16.206: icmp_seq=3 ttl=64 time=0.242 ms
136 bytes from 10.5.16.206: icmp_seq=95 ttl=64 time=0.253 ms
136 bytes from 10.5.16.206: icmp_seq=96 ttl=64 time=0.239 ms
136 bytes from 10.5.16.206: icmp_seq=97 ttl=64 time=0.291 ms
136 bytes from 10.5.16.206: icmp_seq=98 ttl=64 time=0.243 ms

--- 10.5.16.206 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99325ms
rtt min/avg/max/mdev = 0.170/0.254/0.307/0.029 ms
```

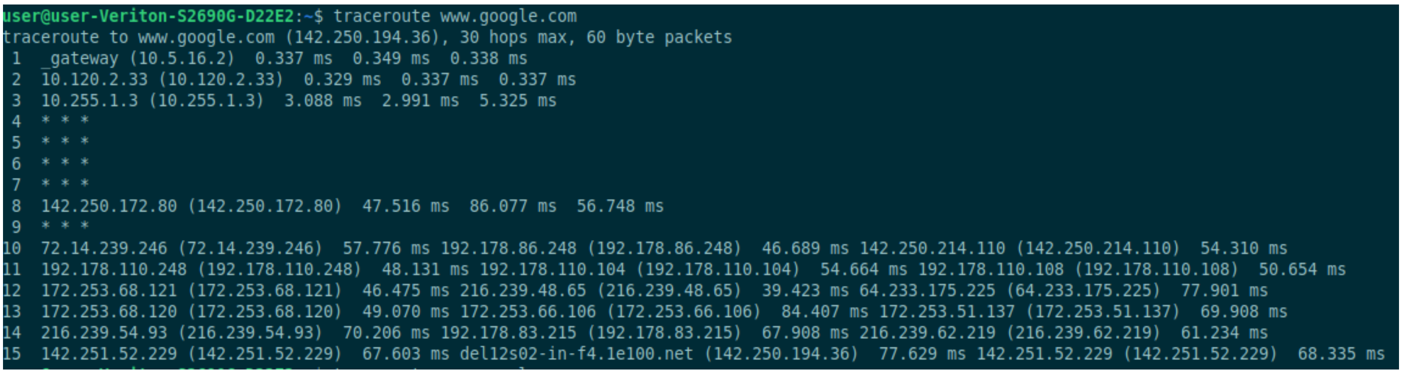
Pinging with packet size 512 bytes:



```
user@user-Veriton-S2690G-D22E2:~$ ping -s 512 -w 100 10.5.16.206
PING 10.5.16.206 (10.5.16.206) 512(540) bytes of data.
520 bytes from 10.5.16.206: icmp_seq=1 ttl=64 time=0.191 ms
520 bytes from 10.5.16.206: icmp_seq=2 ttl=64 time=0.322 ms
520 bytes from 10.5.16.206: icmp_seq=3 ttl=64 time=0.257 ms
520 bytes from 10.5.16.206: icmp_seq=4 ttl=64 time=0.318 ms
520 bytes from 10.5.16.206: icmp_seq=97 ttl=64 time=0.262 ms
520 bytes from 10.5.16.206: icmp_seq=98 ttl=64 time=0.295 ms

--- 10.5.16.206 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99330ms
rtt min/avg/max/mdev = 0.148/0.272/0.472/0.053 ms
```

Packet Size	**% Packet Loss**	**Min. RTT**	**Avg. RTT**	**Max. RTT**	**Std. Dev. RTT**
64 (+8 header)	0	0.121	0.248	0.311	0.041
128 (+8 header)	0	0.170	0254	0.307	0.029
512 (+8 header)	0	0.148	0.272	0.472	0.053

4. Run traceroute for www.google.com and print the summary.



```
user@user-Veriton-S2690G-D22E2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.194.36), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.337 ms  0.349 ms  0.338 ms
 2  10.120.2.33 (10.120.2.33)  0.329 ms  0.337 ms  0.337 ms
 3  10.255.1.3 (10.255.1.3)  3.088 ms  2.991 ms  5.325 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  142.250.172.80 (142.250.172.80)  47.516 ms  86.077 ms  56.748 ms
 9  * * *
10  72.14.239.246 (72.14.239.246)  57.776 ms 192.178.86.248 (192.178.86.248)  46.689 ms 142.250.214.110 (142.250.214.110)  54.310 ms
11  192.178.110.248 (192.178.110.248)  48.131 ms 192.178.110.104 (192.178.110.104)  54.664 ms 192.178.110.108 (192.178.110.108)  50.654 ms
12  172.253.68.121 (172.253.68.121)  46.475 ms 216.239.48.65 (216.239.48.65)  39.423 ms 64.233.175.225 (64.233.175.225)  77.901 ms
13  172.253.68.120 (172.253.68.120)  49.070 ms 172.253.66.106 (172.253.66.106)  84.407 ms 172.253.51.137 (172.253.51.137)  69.908 ms
14  216.239.54.93 (216.239.54.93)  70.206 ms 192.178.83.215 (192.178.83.215)  67.908 ms 216.239.62.219 (216.239.62.219)  61.234 ms
15  142.251.52.229 (142.251.52.229)  67.603 ms del12s02-in-f4.1e100.net (142.250.194.36)  77.629 ms 142.251.52.229 (142.251.52.229)  68.335 ms
```

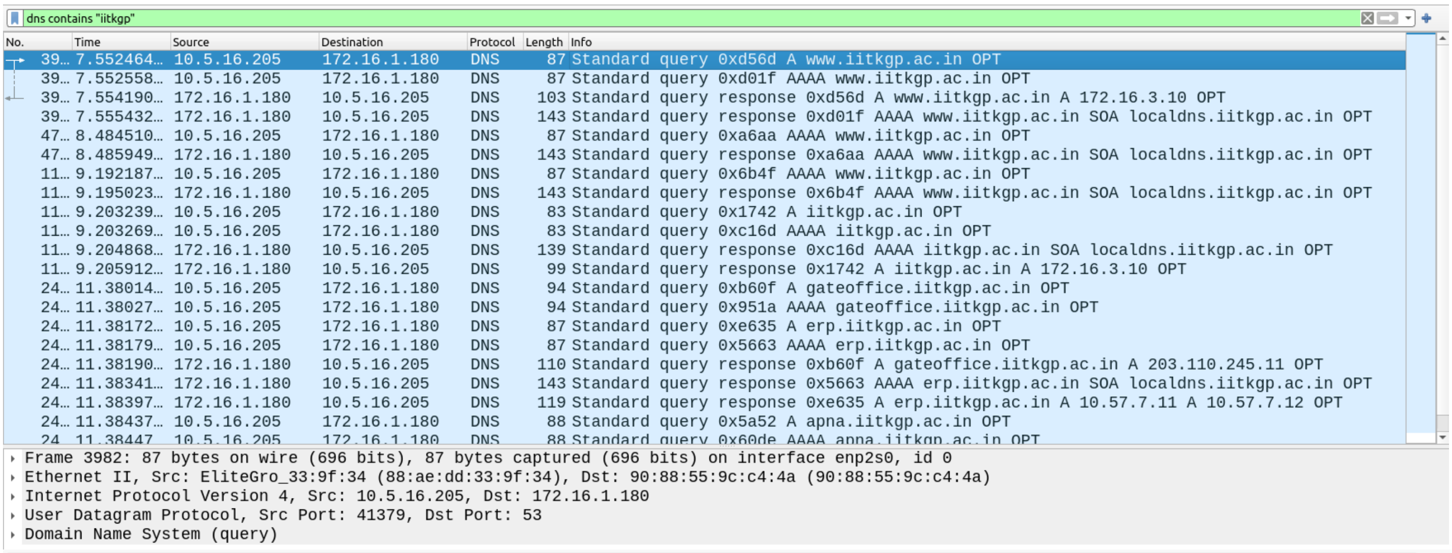
Traceroute: It is a command-line tool that shows the complete path taken by a probe packet to reach its destination. The program listens for an ICMP reply: either a “time exceeded” reply, when the packet reaches an intermediate hop (after which it sends the next set of probe packets with TTL one more than the previous one), or a “port unreachable” reply, when the packet reaches the destination or cannot connect to the router due to some issue.

Summary for traceroute for www.google.com:
Number of hops: 15
Reason for * * *: There can be 2 reasons of getting a star

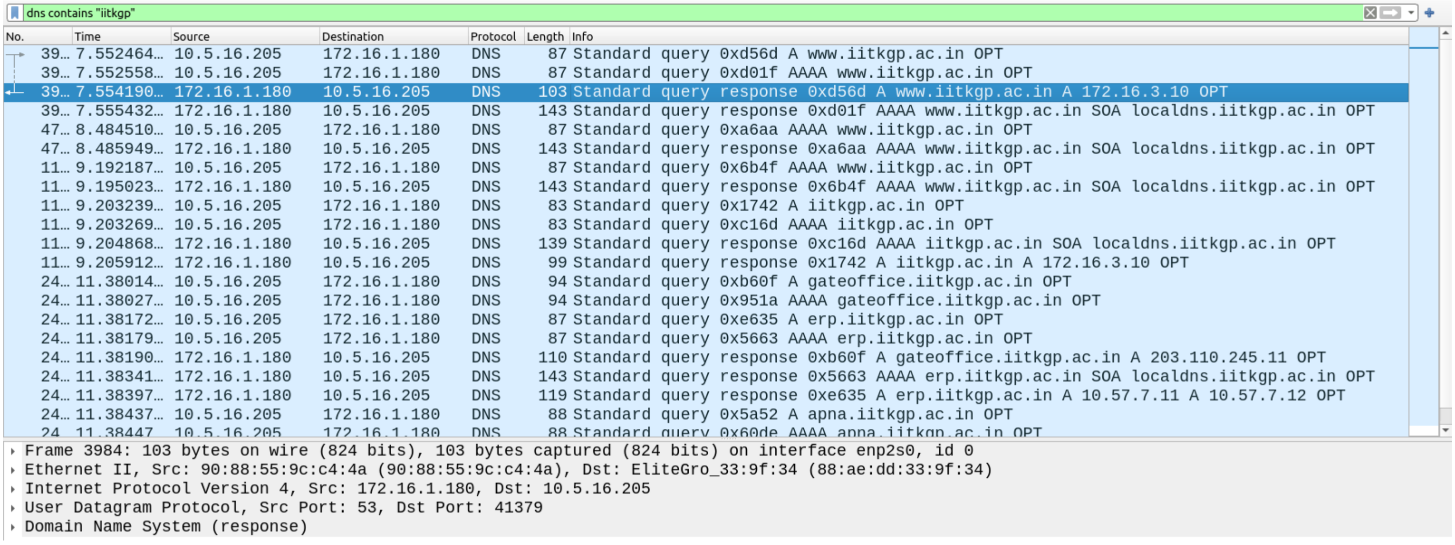
1. The intermediate router may not have been configured to reply to an ICMP or UDP packet (the type of packet that traceroute generally sends).
2. The packets were dropped due to an issue in the network.

PART 2: Packet Analysis

1. Analysis of DNS Packets: Structure and its Traffic



```
dns contains "iitkgp"

No.   Time       Source         Destination    Protocol Length Info
39…  7.552464…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xd56d A www.iitkgp.ac.in OPT
39…  7.552558…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xd01f AAAA www.iitkgp.ac.in OPT
39…  7.554190…  172.16.1.180   10.5.16.205    DNS      103 Standard query response 0xd56d A www.iitkgp.ac.in A 172.16.3.10 OPT
39…  7.555432…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0xd01f AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
47…  8.484510…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xa6aa AAAA www.iitkgp.ac.in OPT
47…  8.485949…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0xa6aa AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.192187…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0x6b4f AAAA www.iitkgp.ac.in OPT
11…  9.195023…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0x6b4f AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.203239…  10.5.16.205    172.16.1.180   DNS       83 Standard query 0x1742 A iitkgp.ac.in OPT
11…  9.203269…  10.5.16.205    172.16.1.180   DNS       83 Standard query 0xc16d AAAA iitkgp.ac.in OPT
11…  9.204868…  172.16.1.180   10.5.16.205    DNS      139 Standard query response 0xc16d AAAA iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.205912…  172.16.1.180   10.5.16.205    DNS       99 Standard query response 0x1742 A iitkgp.ac.in A 172.16.3.10 OPT
24…  11.38014…  10.5.16.205    172.16.1.180   DNS       94 Standard query 0xb60f A gateoffice.iitkgp.ac.in OPT
24…  11.38027…  10.5.16.205    172.16.1.180   DNS       94 Standard query 0x951a AAAA gateoffice.iitkgp.ac.in OPT
24…  11.38172…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xe635 A erp.iitkgp.ac.in OPT
24…  11.38179…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0x5663 AAAA erp.iitkgp.ac.in OPT
24…  11.38190…  172.16.1.180   10.5.16.205    DNS      110 Standard query response 0xb60f A gateoffice.iitkgp.ac.in A 203.110.245.11 OPT
24…  11.38341…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0x5663 AAAA erp.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
24…  11.38397…  172.16.1.180   10.5.16.205    DNS      119 Standard query response 0xe635 A erp.iitkgp.ac.in A 10.57.7.11 A 10.57.7.12 OPT
24…  11.38437…  10.5.16.205    172.16.1.180   DNS       88 Standard query 0x5a52 A apna.iitkgp.ac.in OPT
24   11.38447   10.5.16.205    172.16.1.180   DNS       88 Standard query 0x60de AAAA apna.iitkgp.ac.in OPT

› Frame 3982: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface enp2s0, id 0
› Ethernet II, Src: EliteGro_33:9f:34 (88:ae:dd:33:9f:34), Dst: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a)
› Internet Protocol Version 4, Src: 10.5.16.205, Dst: 172.16.1.180
› User Datagram Protocol, Src Port: 41379, Dst Port: 53
› Domain Name System (query)
```



```
dns contains "iitkgp"

No.   Time       Source         Destination    Protocol Length Info
39…  7.552464…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xd56d A www.iitkgp.ac.in OPT
39…  7.552558…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xd01f AAAA www.iitkgp.ac.in OPT
39…  7.554190…  172.16.1.180   10.5.16.205    DNS      103 Standard query response 0xd56d A www.iitkgp.ac.in A 172.16.3.10 OPT
39…  7.555432…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0xd01f AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
47…  8.484510…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xa6aa AAAA www.iitkgp.ac.in OPT
47…  8.485949…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0xa6aa AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.192187…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0x6b4f AAAA www.iitkgp.ac.in OPT
11…  9.195023…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0x6b4f AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.203239…  10.5.16.205    172.16.1.180   DNS       83 Standard query 0x1742 A iitkgp.ac.in OPT
11…  9.203269…  10.5.16.205    172.16.1.180   DNS       83 Standard query 0xc16d AAAA iitkgp.ac.in OPT
11…  9.204868…  172.16.1.180   10.5.16.205    DNS      139 Standard query response 0xc16d AAAA iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
11…  9.205912…  172.16.1.180   10.5.16.205    DNS       99 Standard query response 0x1742 A iitkgp.ac.in A 172.16.3.10 OPT
24…  11.38014…  10.5.16.205    172.16.1.180   DNS       94 Standard query 0xb60f A gateoffice.iitkgp.ac.in OPT
24…  11.38027…  10.5.16.205    172.16.1.180   DNS       94 Standard query 0x951a AAAA gateoffice.iitkgp.ac.in OPT
24…  11.38172…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0xe635 A erp.iitkgp.ac.in OPT
24…  11.38179…  10.5.16.205    172.16.1.180   DNS       87 Standard query 0x5663 AAAA erp.iitkgp.ac.in OPT
24…  11.38190…  172.16.1.180   10.5.16.205    DNS      110 Standard query response 0xb60f A gateoffice.iitkgp.ac.in A 203.110.245.11 OPT
24…  11.38341…  172.16.1.180   10.5.16.205    DNS      143 Standard query response 0x5663 AAAA erp.iitkgp.ac.in SOA localdns.iitkgp.ac.in OPT
24…  11.38397…  172.16.1.180   10.5.16.205    DNS      119 Standard query response 0xe635 A erp.iitkgp.ac.in A 10.57.7.11 A 10.57.7.12 OPT
24…  11.38437…  10.5.16.205    172.16.1.180   DNS       88 Standard query 0x5a52 A apna.iitkgp.ac.in OPT
24   11.38447   10.5.16.205    172.16.1.180   DNS       88 Standard query 0x60de AAAA apna.iitkgp.ac.in OPT

› Frame 3984: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface enp2s0, id 0
› Ethernet II, Src: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a), Dst: EliteGro_33:9f:34 (88:ae:dd:33:9f:34)
› Internet Protocol Version 4, Src: 172.16.1.180, Dst: 10.5.16.205
› User Datagram Protocol, Src Port: 53, Dst Port: 41379
› Domain Name System (response)
```

a) The DNS query and response packets were located using the filter: **dns contains "iitkgp"**. In the second-last line of the "Packet Details" pane, we can see that the observed DNS packets use **User Datagram Protocol (UDP)**.

b) The Source IP-Address is **10.5.16.205** and the Destination IP-Address (of the DNS server) is **172.16.1.180**

c) **2 DNS queries** are sent from browser to DNS Server during the name-to-IP resolution. They are of types A and AAAA (resolving to IPv4 and IPv6 respectively).

d) The DNS Server at IP-Address 172.16.1.180 replied with the actual IP-Address.

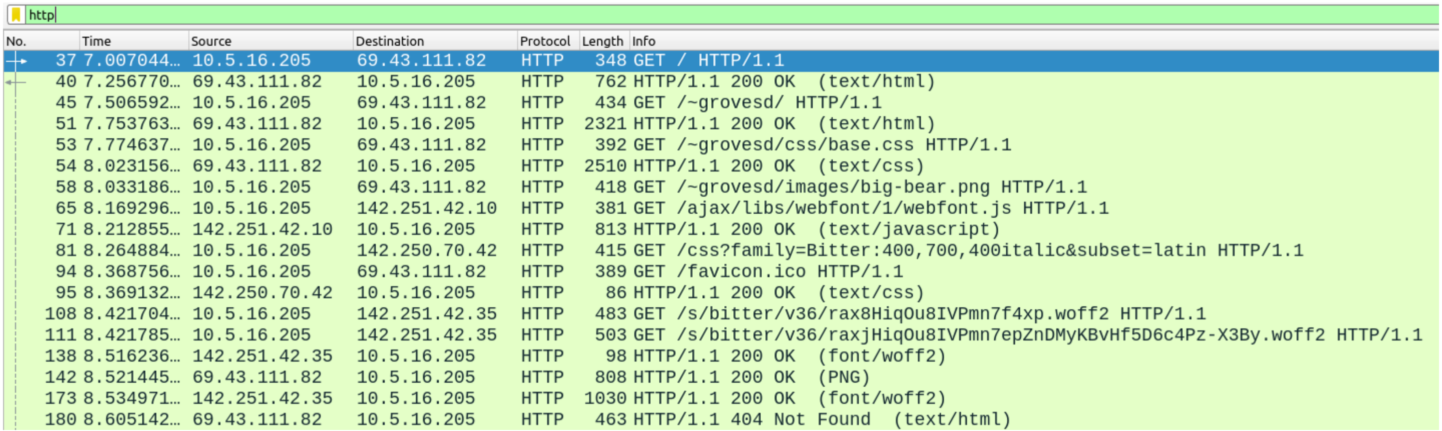
e) Only 1 server was involved in the resolution process and it responded back with the IP-Address

f) Resource Records Involved:

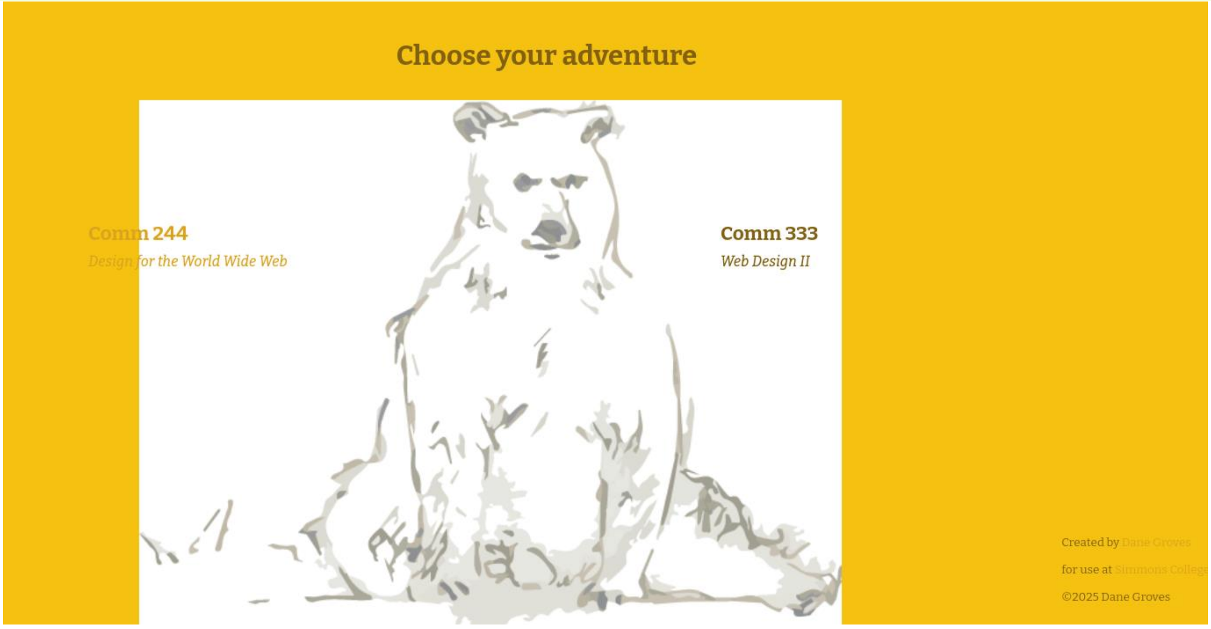
Name	www.iitkgp.ac.in
Type	A
Class	IN
TTL	86400
Data Length	4
IP-Address	172.16.3.10

2) Web Traffic (HTTP)

a) The following screenshot shows the observed HTTP packets between the client and web server. We are able to see these many packets for a single web page because to load various things on the web page, the server has to fetch them from various locations. Example: the image of the bear, different fonts, icons, etc.



```
http
No.  Time        Source          Destination     Protocol Length Info
  37 7.007044…   10.5.16.205     69.43.111.82    HTTP      348 GET / HTTP/1.1
  40 7.256770…   69.43.111.82    10.5.16.205     HTTP      762 HTTP/1.1 200 OK  (text/html)
  45 7.506592…   10.5.16.205     69.43.111.82    HTTP      434 GET /~grovesd/ HTTP/1.1
  51 7.753763…   69.43.111.82    10.5.16.205     HTTP     2321 HTTP/1.1 200 OK  (text/html)
  53 7.774637…   10.5.16.205     69.43.111.82    HTTP      392 GET /~grovesd/css/base.css HTTP/1.1
  54 8.023156…   69.43.111.82    10.5.16.205     HTTP     2510 HTTP/1.1 200 OK  (text/css)
  58 8.033186…   10.5.16.205     69.43.111.82    HTTP      418 GET /~grovesd/images/big-bear.png HTTP/1.1
  65 8.169296…   10.5.16.205     142.251.42.10   HTTP      381 GET /ajax/libs/webfont/1/webfont.js HTTP/1.1
  71 8.212855…   142.251.42.10   10.5.16.205     HTTP      813 HTTP/1.1 200 OK  (text/javascript)
  81 8.264884…   10.5.16.205     142.250.70.42   HTTP      415 GET /css?family=Bitter:400,700,400italic&subset=latin HTTP/1.1
  94 8.368756…   10.5.16.205     69.43.111.82    HTTP      389 GET /favicon.ico HTTP/1.1
  95 8.369132…   142.250.70.42   10.5.16.205     HTTP       86 HTTP/1.1 200 OK  (text/css)
 108 8.421704…   10.5.16.205     142.251.42.35   HTTP      483 GET /s/bitter/v36/rax8HiqOu8IVPmn7f4xp.woff2 HTTP/1.1
 111 8.421785…   10.5.16.205     142.251.42.35   HTTP      503 GET /s/bitter/v36/raxjHiqOu8IVPmn7epZnDMyKBvHf5D6c4Pz-X3By.woff2 HTTP/1.1
 138 8.516236…   142.251.42.35   10.5.16.205     HTTP       98 HTTP/1.1 200 OK  (font/woff2)
 142 8.521445…   69.43.111.82    10.5.16.205     HTTP      808 HTTP/1.1 200 OK  (PNG)
 173 8.534971…   142.251.42.35   10.5.16.205     HTTP     1030 HTTP/1.1 200 OK  (font/woff2)
 180 8.605142…   69.43.111.82    10.5.16.205     HTTP      463 HTTP/1.1 404 Not Found  (text/html)
```



Choose your adventure

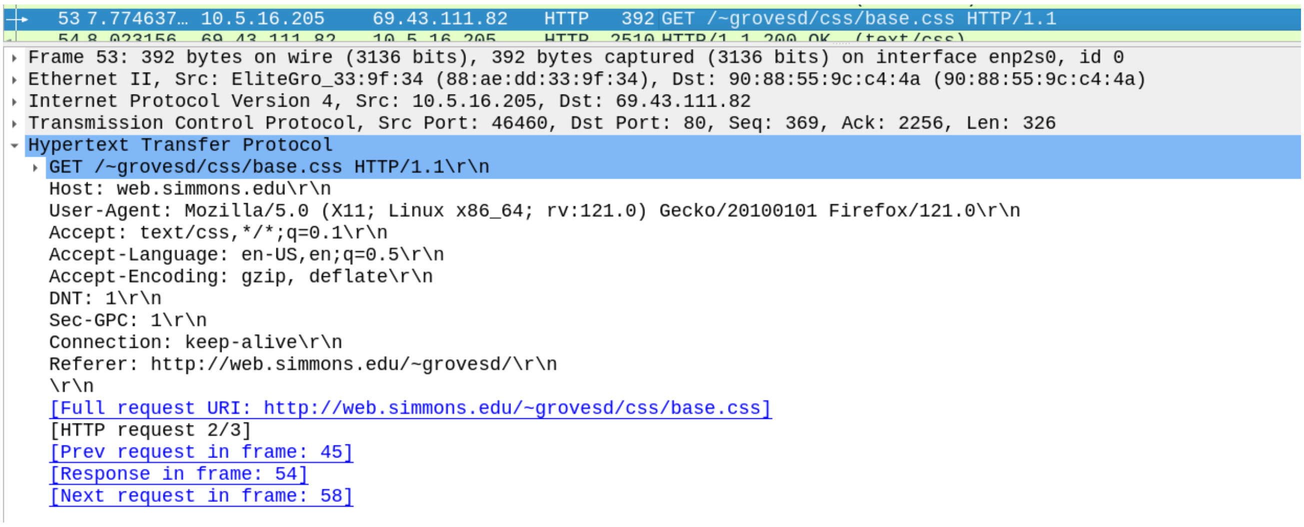
Comm 244
Design for the World Wide Web

Comm 333
Web Design II

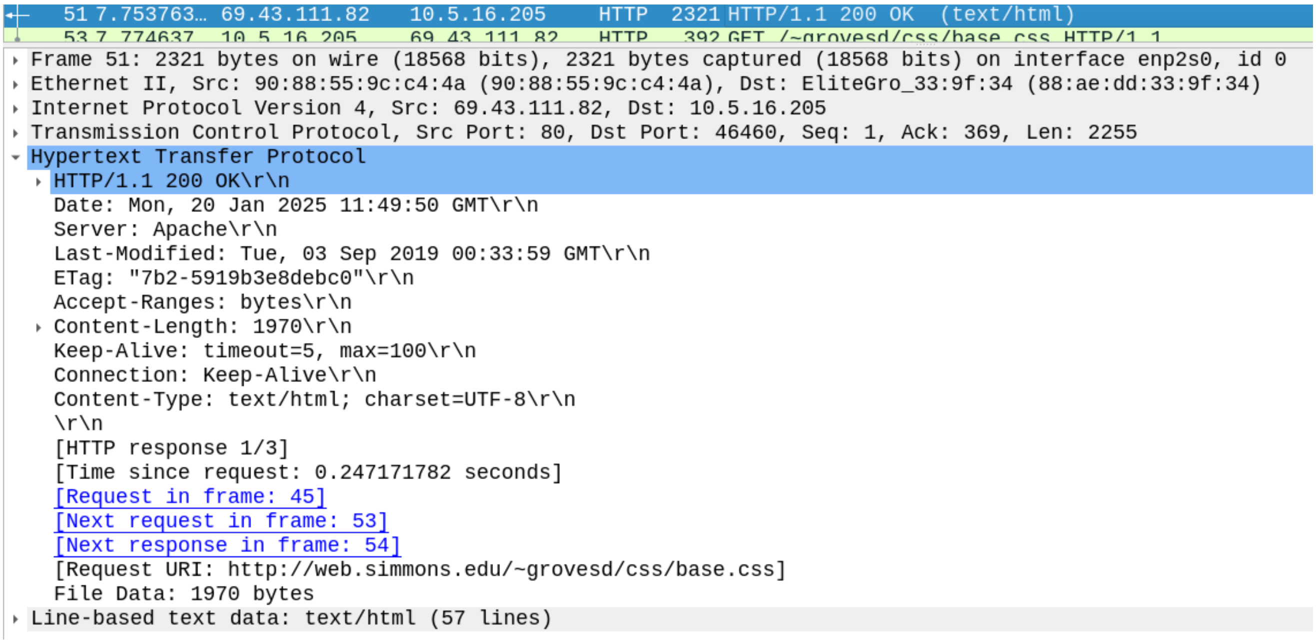
Created by Dane Groves
for use at Simmons College
©2025 Dane Groves

b) In the above screenshot, the Info having "GET" type is the request packer, and the info having "HTTP" type is the response packet.
Different headers for request and response are (most common ones)

REQUEST	RESPONSE
User-Agent	Server
Accept	Last-Modified
Accept-Encoding	Accept-Ranges
Accept-Language	Content-Type
Connection	Request-URI
Referer	Keep-Alive



```
53 7.774637… 10.5.16.205     69.43.111.82    HTTP   392 GET /~grovesd/css/base.css HTTP/1.1
54 8.023156… 69.43.111.82    10.5.16.205     HTTP  2510 HTTP/1.1 200 OK  (text/css)
Frame 53: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface enp2s0, id 0
Ethernet II, Src: EliteGro_33:9f:34 (88:ae:dd:33:9f:34), Dst: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a)
Internet Protocol Version 4, Src: 10.5.16.205, Dst: 69.43.111.82
Transmission Control Protocol, Src Port: 46460, Dst Port: 80, Seq: 369, Ack: 2256, Len: 326
Hypertext Transfer Protocol
  GET /~grovesd/css/base.css HTTP/1.1\r\n
  Host: web.simmons.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
  Accept: text/css,*/*;q=0.1\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Referer: http://web.simmons.edu/~grovesd/\r\n
  \r\n
  [Full request URI: http://web.simmons.edu/~grovesd/css/base.css]
  [HTTP request 2/3]
  [Prev request in frame: 45]
  [Response in frame: 54]
  [Next request in frame: 58]
```

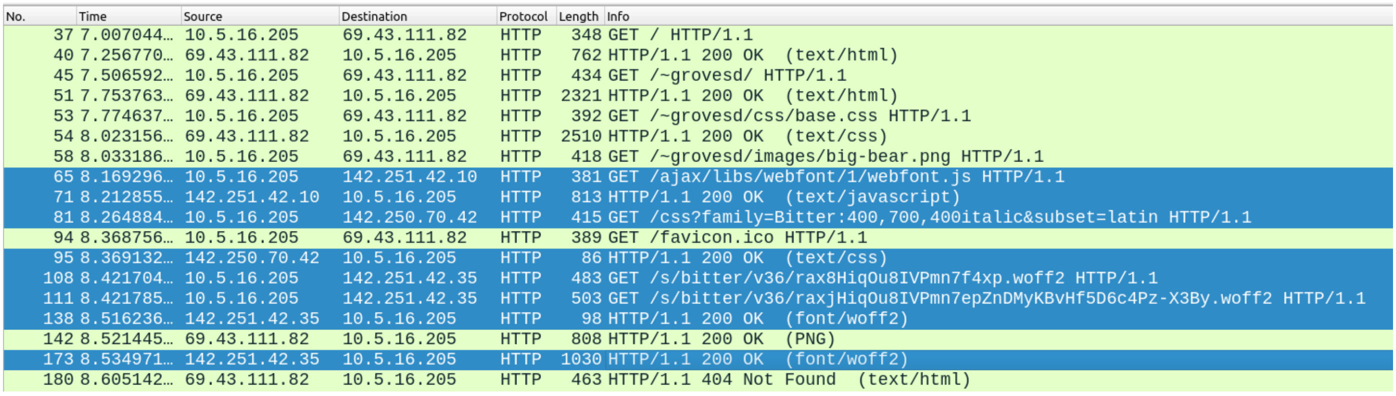


```
51 7.753763… 69.43.111.82    10.5.16.205     HTTP  2321 HTTP/1.1 200 OK  (text/html)
53 7.774637  10.5.16.205     69.43.111.82    HTTP   392 GET /~grovesd/css/base.css HTTP/1.1
Frame 51: 2321 bytes on wire (18568 bits), 2321 bytes captured (18568 bits) on interface enp2s0, id 0
Ethernet II, Src: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a), Dst: EliteGro_33:9f:34 (88:ae:dd:33:9f:34)
Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.5.16.205
Transmission Control Protocol, Src Port: 80, Dst Port: 46460, Seq: 1, Ack: 369, Len: 2255
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 20 Jan 2025 11:49:50 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Tue, 03 Sep 2019 00:33:59 GMT\r\n
  ETag: "7b2-5919b3e8debc0"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 1970\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/3]
  [Time since request: 0.247171782 seconds]
  [Request in frame: 45]
  [Next request in frame: 53]
  [Next response in frame: 54]
  [Request URI: http://web.simmons.edu/~grovesd/css/base.css]
  File Data: 1970 bytes
Line-based text data: text/html (57 lines)
```

c) In total **18 HTTP packets** are exchanged to load the entire webpage. However

10 packets are exchanged between client and server (69.43.111.42)

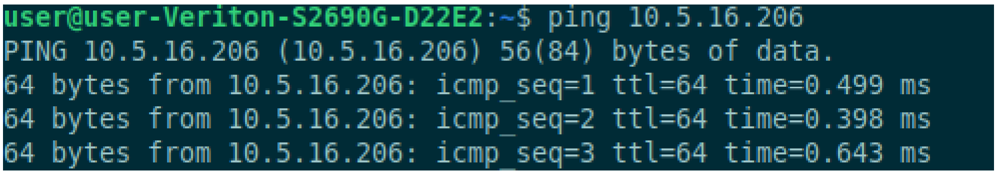
8 packets are exchanged between client and external servers to get some css, fonts, etc. (142.251.42.10, 142.250.70.42, 142.251.42.35)



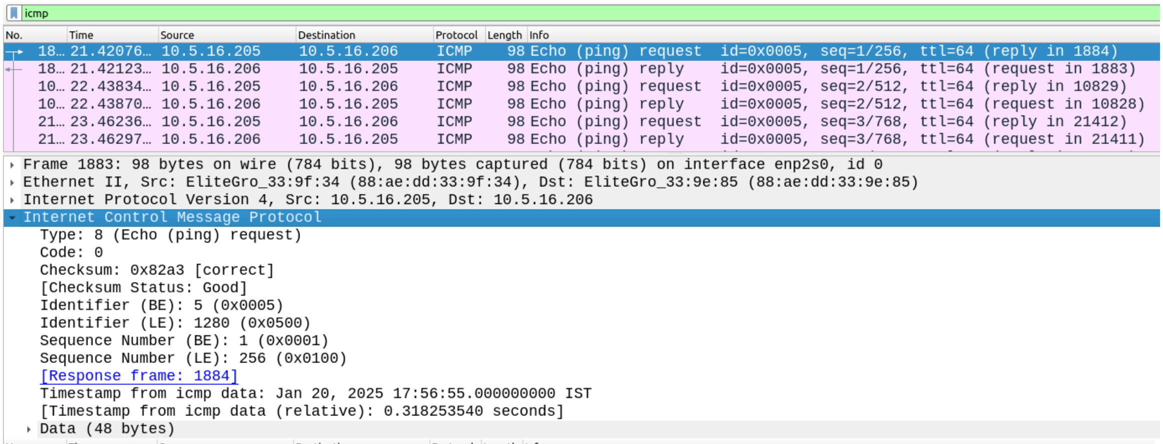
No.	Time	Source	Destination	Protocol	Length	Info
37	7.007044…	10.5.16.205	69.43.111.82	HTTP	348	GET / HTTP/1.1
40	7.256770…	69.43.111.82	10.5.16.205	HTTP	762	HTTP/1.1 200 OK (text/html)
45	7.506592…	10.5.16.205	69.43.111.82	HTTP	434	GET /~grovesd/ HTTP/1.1
51	7.753763…	69.43.111.82	10.5.16.205	HTTP	2321	HTTP/1.1 200 OK (text/html)
53	7.774637…	10.5.16.205	69.43.111.82	HTTP	392	GET /~grovesd/css/base.css HTTP/1.1
54	8.023156…	69.43.111.82	10.5.16.205	HTTP	2510	HTTP/1.1 200 OK (text/css)
58	8.033186…	10.5.16.205	69.43.111.82	HTTP	418	GET /~grovesd/images/big-bear.png HTTP/1.1
65	8.169296…	10.5.16.205	142.251.42.10	HTTP	381	GET /ajax/libs/webfont/1/webfont.js HTTP/1.1
71	8.212855…	142.251.42.10	10.5.16.205	HTTP	813	HTTP/1.1 200 OK (text/javascript)
81	8.264884…	10.5.16.205	142.250.70.42	HTTP	415	GET /css?family=Bitter:400,700,400italic&subset=latin HTTP/1.1
94	8.368756…	10.5.16.205	69.43.111.82	HTTP	389	GET /favicon.ico HTTP/1.1
95	8.369132…	142.250.70.42	10.5.16.205	HTTP	86	HTTP/1.1 200 OK (text/css)
108	8.421704…	10.5.16.205	142.251.42.35	HTTP	483	GET /s/bitter/v36/rax8HiqOu8IVPmn7f4xp.woff2 HTTP/1.1
111	8.421785…	10.5.16.205	142.251.42.35	HTTP	503	GET /s/bitter/v36/raxjHiqOu8IVPmn7epZnDMyKBvHf5D6c4Pz-X3By.woff2 HTTP/1.1
138	8.516236…	142.251.42.35	10.5.16.205	HTTP	98	HTTP/1.1 200 OK (font/woff2)
142	8.521445…	69.43.111.82	10.5.16.205	HTTP	808	HTTP/1.1 200 OK (PNG)
173	8.534971…	142.251.42.35	10.5.16.205	HTTP	1030	HTTP/1.1 200 OK (font/woff2)
180	8.605142…	69.43.111.82	10.5.16.205	HTTP	463	HTTP/1.1 404 Not Found (text/html)

3) ICMP Traffic (ping/traceroute)

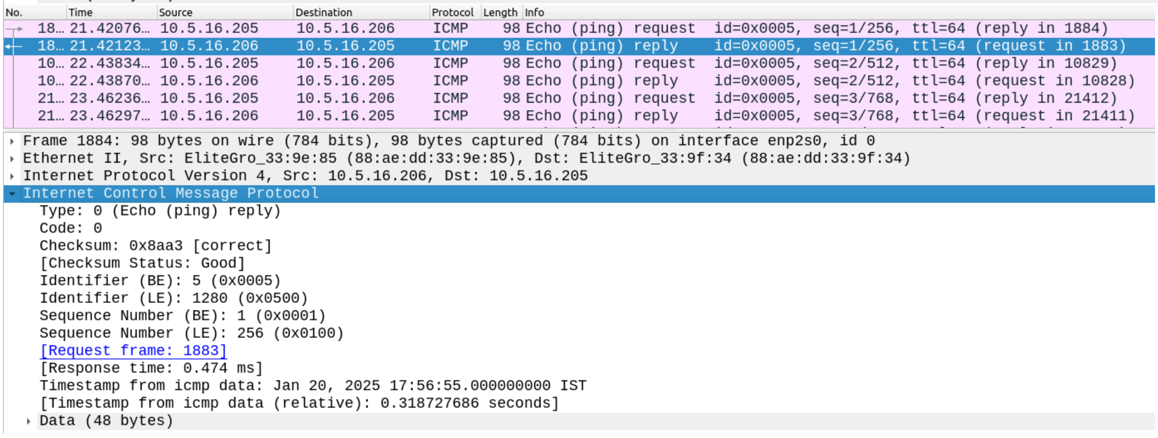
a) Pinging friend’s machine (10.5.16.206)



```
user@user-Veriton-S2690G-D22E2:~$ ping 10.5.16.206
PING 10.5.16.206 (10.5.16.206) 56(84) bytes of data.
64 bytes from 10.5.16.206: icmp_seq=1 ttl=64 time=0.499 ms
64 bytes from 10.5.16.206: icmp_seq=2 ttl=64 time=0.398 ms
64 bytes from 10.5.16.206: icmp_seq=3 ttl=64 time=0.643 ms
```



```
icmp
No.   Time        Source       Destination  Protocol Length Info
18…  21.42076…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=1/256, ttl=64 (reply in 1884)
18…  21.42123…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=1/256, ttl=64 (request in 1883)
10…  22.43834…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=2/512, ttl=64 (reply in 10829)
10…  22.43870…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=2/512, ttl=64 (request in 10828)
21…  23.46236…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=3/768, ttl=64 (reply in 21412)
21…  23.46297…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=3/768, ttl=64 (request in 21411)
▸ Frame 1883: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp2s0, id 0
▸ Ethernet II, Src: EliteGro_33:9f:34 (88:ae:dd:33:9f:34), Dst: EliteGro_33:9e:85 (88:ae:dd:33:9e:85)
▸ Internet Protocol Version 4, Src: 10.5.16.205, Dst: 10.5.16.206
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x82a3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 5 (0x0005)
    Identifier (LE): 1280 (0x0500)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 1884]
    Timestamp from icmp data: Jan 20, 2025 17:56:55.000000000 IST
    [Timestamp from icmp data (relative): 0.318253540 seconds]
  ▸ Data (48 bytes)
```



```
No.   Time        Source       Destination  Protocol Length Info
18…  21.42076…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=1/256, ttl=64 (reply in 1884)
18…  21.42123…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=1/256, ttl=64 (request in 1883)
10…  22.43834…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=2/512, ttl=64 (reply in 10829)
10…  22.43870…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=2/512, ttl=64 (request in 10828)
21…  23.46236…  10.5.16.205  10.5.16.206  ICMP     98 Echo (ping) request  id=0x0005, seq=3/768, ttl=64 (reply in 21412)
21…  23.46297…  10.5.16.206  10.5.16.205  ICMP     98 Echo (ping) reply    id=0x0005, seq=3/768, ttl=64 (request in 21411)
▸ Frame 1884: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp2s0, id 0
▸ Ethernet II, Src: EliteGro_33:9e:85 (88:ae:dd:33:9e:85), Dst: EliteGro_33:9f:34 (88:ae:dd:33:9f:34)
▸ Internet Protocol Version 4, Src: 10.5.16.206, Dst: 10.5.16.205
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8aa3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 5 (0x0005)
    Identifier (LE): 1280 (0x0500)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 1883]
    [Response time: 0.474 ms]
    Timestamp from icmp data: Jan 20, 2025 17:56:55.000000000 IST
    [Timestamp from icmp data (relative): 0.318727686 seconds]
  ▸ Data (48 bytes)
```

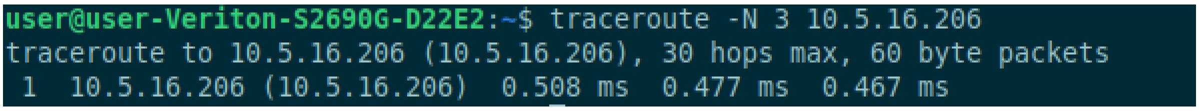
From Wireshark:

Request Source: 10.5.16.205	Reply Source: 10.5.16.206
Request Destination: 10.5.16.206	Reply Destination: 10.5.16.205

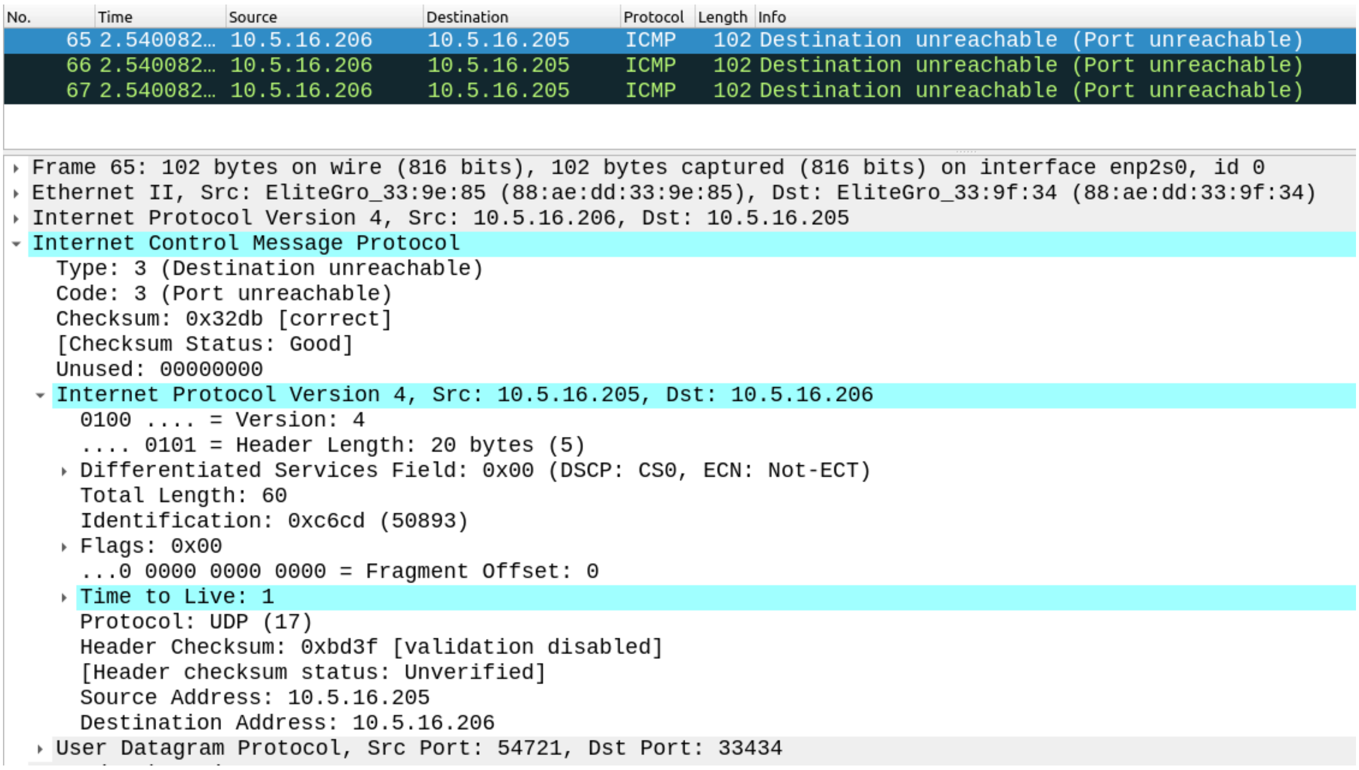
a) Tracerouting probe packet sent to friend’s machine (10.5.16.206)

As discussed in the report earlier, traceroute sends out ICMP probe packets with an increasing number of TTL (in groups of 3 by default).

Now, the command shown in the first screenshot uses an **option “-N”** which sets the number of concurrent packets sent for probing. By default this value is 16 (to speed up the process of tracerouting), because of which running without this option gives 6 packets in Wireshark (3 having TTL=1 and 3 having TTL=2).

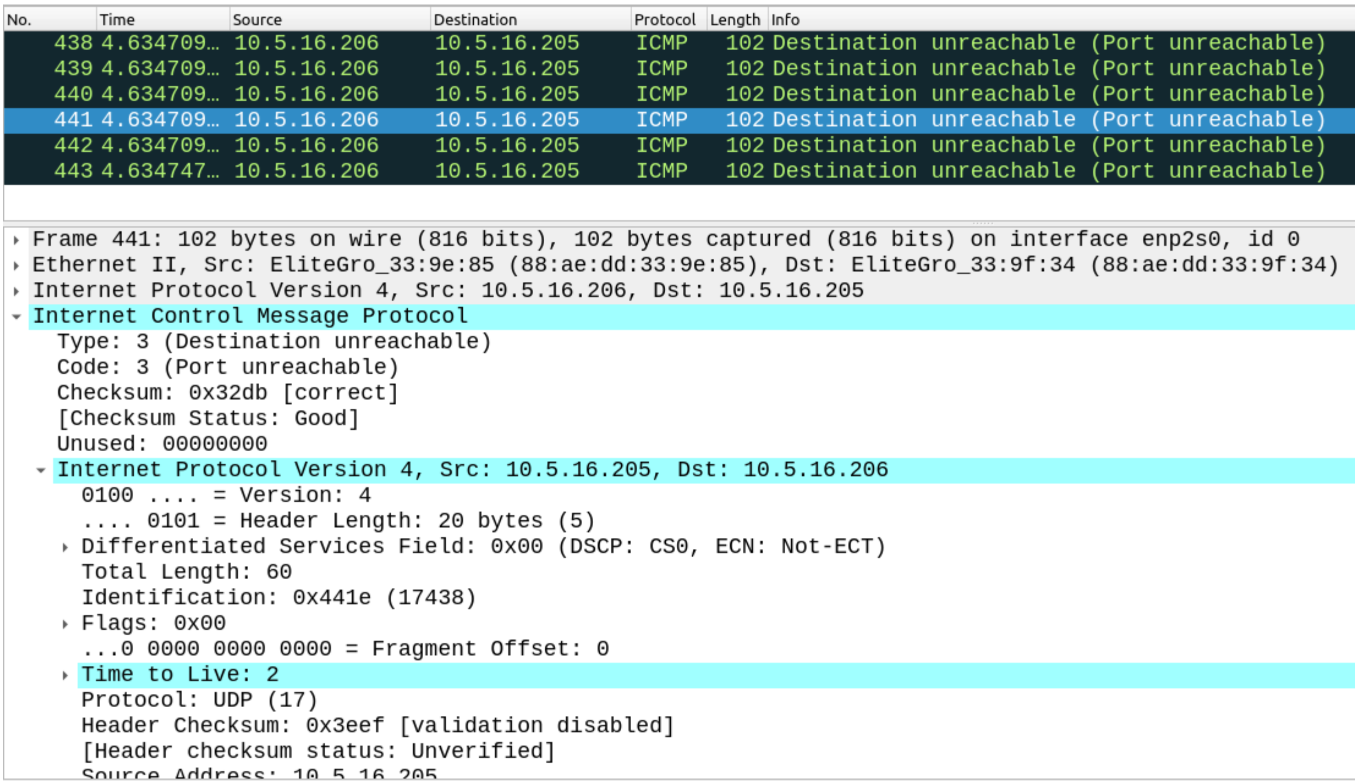


```
user@user-Veriton-S2690G-D22E2:~$ traceroute -N 3 10.5.16.206
traceroute to 10.5.16.206 (10.5.16.206), 30 hops max, 60 byte packets
 1  10.5.16.206 (10.5.16.206)  0.508 ms  0.477 ms  0.467 ms
```



```
No.  Time          Source         Destination    Protocol Length Info
  65 2.540082…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
  66 2.540082…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
  67 2.540082…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)

› Frame 65: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp2s0, id 0
› Ethernet II, Src: EliteGro_33:9e:85 (88:ae:dd:33:9e:85), Dst: EliteGro_33:9f:34 (88:ae:dd:33:9f:34)
› Internet Protocol Version 4, Src: 10.5.16.206, Dst: 10.5.16.205
⌄ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x32db [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ⌄ Internet Protocol Version 4, Src: 10.5.16.205, Dst: 10.5.16.206
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
      Identification: 0xc6cd (50893)
    › Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
    › Time to Live: 1
      Protocol: UDP (17)
      Header Checksum: 0xbd3f [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.5.16.205
      Destination Address: 10.5.16.206
  › User Datagram Protocol, Src Port: 54721, Dst Port: 33434
```

<u>Without “-N 3”</u>

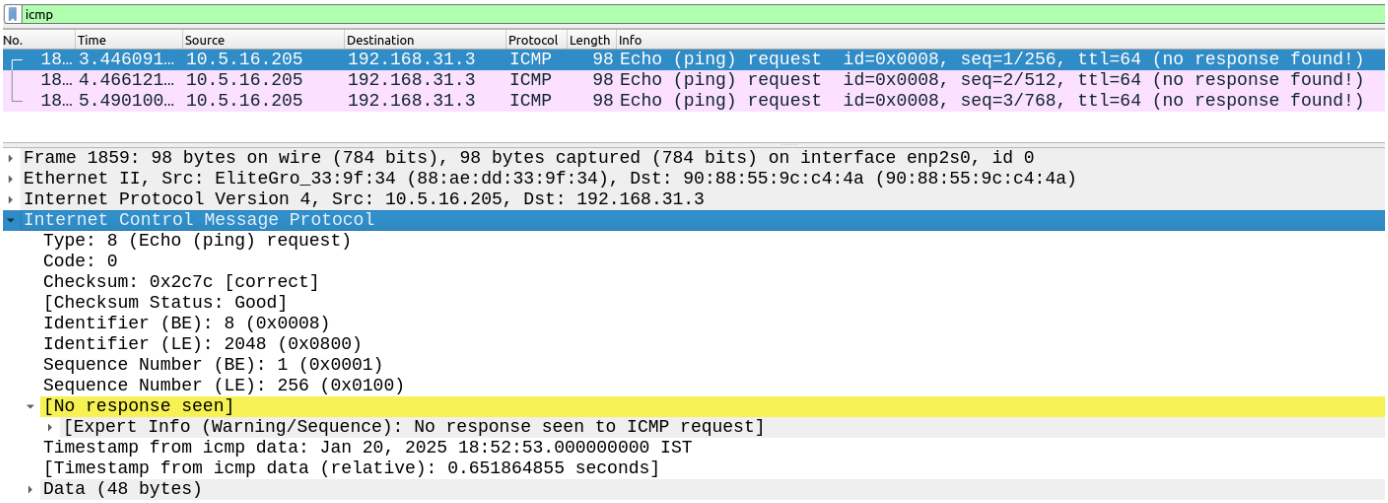


```
No.  Time          Source         Destination    Protocol Length Info
 438 4.634709…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
 439 4.634709…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
 440 4.634709…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
 441 4.634709…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
 442 4.634709…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)
 443 4.634747…  10.5.16.206    10.5.16.205    ICMP     102 Destination unreachable (Port unreachable)

› Frame 441: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp2s0, id 0
› Ethernet II, Src: EliteGro_33:9e:85 (88:ae:dd:33:9e:85), Dst: EliteGro_33:9f:34 (88:ae:dd:33:9f:34)
› Internet Protocol Version 4, Src: 10.5.16.206, Dst: 10.5.16.205
⌄ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x32db [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ⌄ Internet Protocol Version 4, Src: 10.5.16.205, Dst: 10.5.16.206
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
      Identification: 0x441e (17438)
    › Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
    › Time to Live: 2
      Protocol: UDP (17)
      Header Checksum: 0x3eef [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.5.16.205
```

We can see that the source and destination are reversed in this case (from user PoV). The reason is that traceroute sends a UDP package to the routers, but the routers return an ICMP response. This is why the source/destination are opposite.

b) Pinging an unreachable server (192.168.31.3)

None of the packets were received (100% packet loss) and an ICMP request could not find any response (otherwise a “Response-frame” field appears which tells the frame number of the response packet (can refer the earlier ping screenshots)



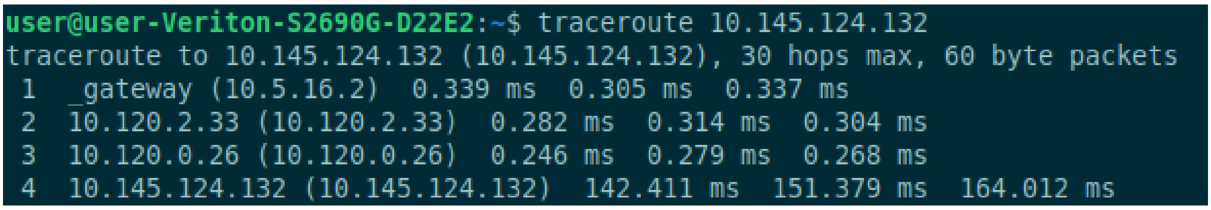
```
icmp
No.     Time        Source        Destination    Protocol Length Info
 18…  3.446091…  10.5.16.205   192.168.31.3   ICMP     98 Echo (ping) request  id=0x0008, seq=1/256, ttl=64 (no response found!)
 18…  4.466121…  10.5.16.205   192.168.31.3   ICMP     98 Echo (ping) request  id=0x0008, seq=2/512, ttl=64 (no response found!)
 18…  5.490100…  10.5.16.205   192.168.31.3   ICMP     98 Echo (ping) request  id=0x0008, seq=3/768, ttl=64 (no response found!)

Frame 1859: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp2s0, id 0
Ethernet II, Src: EliteGro_33:9f:34 (88:ae:dd:33:9f:34), Dst: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a)
Internet Protocol Version 4, Src: 10.5.16.205, Dst: 192.168.31.3
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2c7c [correct]
    [Checksum Status: Good]
    Identifier (BE): 8 (0x0008)
    Identifier (LE): 2048 (0x0800)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [No response seen]
      [Expert Info (Warning/Sequence): No response seen to ICMP request]
    Timestamp from icmp data: Jan 20, 2025 18:52:53.000000000 IST
    [Timestamp from icmp data (relative): 0.651864855 seconds]
  Data (48 bytes)
```

c) Tracerouting reachable and unreachable hosts:
Reachable: 10.145.124.132
Unreachable: 192.168.31.3

Tracerouting works as follows:
For every set of 3 packets, the TTL is set as 1, 2 and so on in increasing order. When a packet reaches an intermediate router, the TTL value decreases by 1. If the value becomes 0, the router sends back an ICMP TTL exceeded response, otherwise sends the packet to the next router.

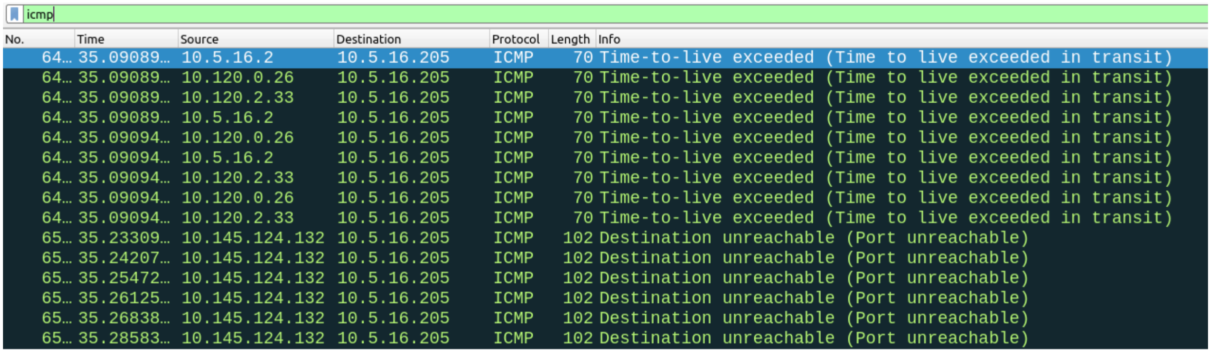
If the packet reaches the destination, as discussed before, the ICMP Destination Unreachable response is returned. The time calculations are done with the use of the ICMP responses.
By default, a packet can have a maximum TTL of 30 (meaning it can visit up to 30 routers until the destination).

<u>Reachable:</u>



```
user@user-Veriton-S2690G-D22E2:~$ traceroute 10.145.124.132
traceroute to 10.145.124.132 (10.145.124.132), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.339 ms  0.305 ms  0.337 ms
 2  10.120.2.33 (10.120.2.33)  0.282 ms  0.314 ms  0.304 ms
 3  10.120.0.26 (10.120.0.26)  0.246 ms  0.279 ms  0.268 ms
 4  10.145.124.132 (10.145.124.132)  142.411 ms  151.379 ms  164.012 ms
```

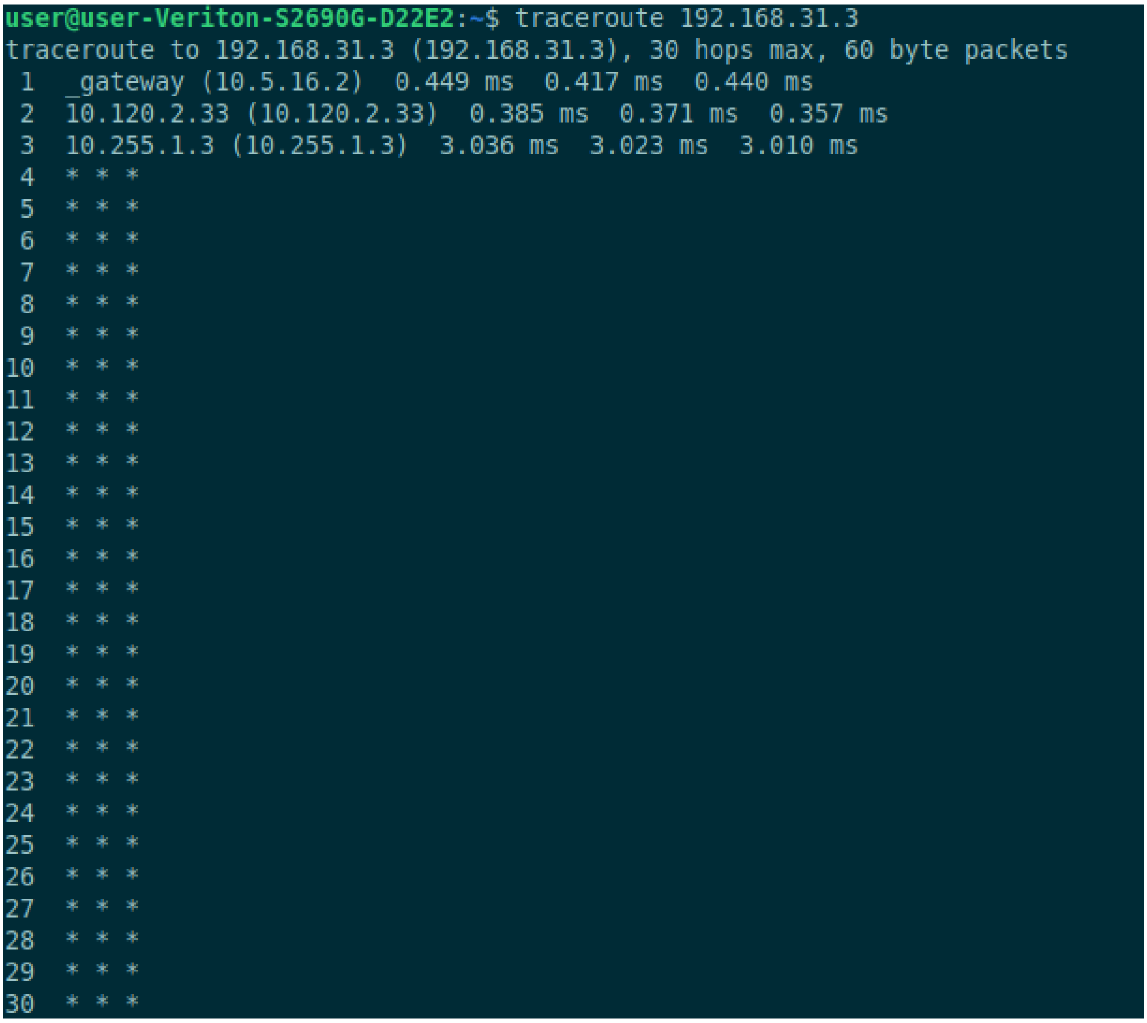
The reachable destination was reached in 4 hops. Which means the first 9 packets should return ICMP TTL Exceeded and the next 3 should return Destination Unreachable.



```
icmp
No.     Time        Source           Destination   Protocol Length Info
 64…  35.09089…  10.5.16.2        10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09089…  10.120.0.26      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09089…  10.120.2.33      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09089…  10.5.16.2        10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09094…  10.120.0.26      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09094…  10.5.16.2        10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09094…  10.120.2.33      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09094…  10.120.0.26      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 64…  35.09094…  10.120.2.33      10.5.16.205   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 65…  35.23309…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
 65…  35.24207…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
 65…  35.25472…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
 65…  35.26125…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
 65…  35.26838…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
 65…  35.28583…  10.145.124.132   10.5.16.205   ICMP     102 Destination unreachable (Port unreachable)
```

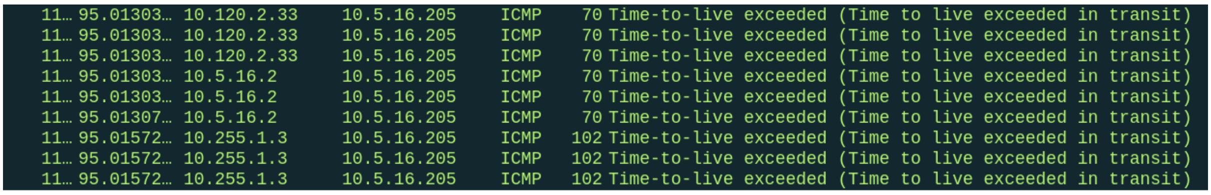
This is verified in the Wireshark packet list. However, we see 3 more packets with ICMP Destination Unreachable because of the reason mentioned in part 3.a (16 default concurrent packets).

Unreachable:



```
user@user-Veriton-S2690G-D22E2:~$ traceroute 192.168.31.3
traceroute to 192.168.31.3 (192.168.31.3), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.449 ms  0.417 ms  0.440 ms
 2  10.120.2.33 (10.120.2.33)  0.385 ms  0.371 ms  0.357 ms
 3  10.255.1.3 (10.255.1.3)  3.036 ms  3.023 ms  3.010 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

In this case, we can see that the probe packets tried to connect to the server, but after 3 intermediate routers, it could not find any router to connect to.



```
   11… 95.01303… 10.120.2.33    10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01303… 10.120.2.33    10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01303… 10.120.2.33    10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01303… 10.5.16.2      10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01303… 10.5.16.2      10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01307… 10.5.16.2      10.5.16.205    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01572… 10.255.1.3     10.5.16.205    ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01572… 10.255.1.3     10.5.16.205    ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
   11… 95.01572… 10.255.1.3     10.5.16.205    ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
```

This is why, after 9 packets, there are no other packets because there was no response.