COL334: Assignment 1

Monu (2020CS50432)

August 2022

Contents

1 Networking Tools

1.a Local IP Address

We can find the I.P. address of any device by command `ifconfig`. On running `ifconfig` in terminal, IP address is the inet address.

The following output is obtained on running command when connected with *My phone Hotspot*(first output) and *IITD Wi-Fi*(second output):

```
coolr@coolr-G5-5500:~$ ifconfig
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 5126  bytes 1211902 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5126  bytes 1211902 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.248.83  netmask 255.255.255.0  broadcast 192.168.248.255
        inet6 2401:4900:30c1:8a4e:3ba4:8cb2:48a4:32ed  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::e863:8258:2166:8473  prefixlen 64  scopeid 0x20<link>
        inet6 2401:4900:30c1:8a4e:3d59:7380:95f8:97e3  prefixlen 64  scopeid 0x0<global>
        ether 94:e7:0b:08:29:9c  txqueuelen 1000  (Ethernet)
        RX packets 533419  bytes 532043897 (532.0 MB)
        RX errors 0  dropped 64  overruns 0  frame 0
        TX packets 144721  bytes 60896104 (60.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

coolr@coolr-G5-5500:~$ ifconfig
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 5142  bytes 1214616 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5142  bytes 1214616 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.184.62.55  netmask 255.255.224.0  broadcast 10.184.63.255
        inet6 fe80::756e:2f57:5cb7:55e9  prefixlen 64  scopeid 0x20<link>
        ether 94:e7:0b:08:29:9c  txqueuelen 1000  (Ethernet)
        RX packets 533445  bytes 532051493 (532.0 MB)
        RX errors 0  dropped 64  overruns 0  frame 0
        TX packets 144771  bytes 60902541 (60.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1: `ifconfig` results

The first entry in the output, i.e., `lo`, is the **loopback connection** which is used to connect to ports on the same device.

The second entry, `wlp0s20f3`, is the relevant one and it contains information about the **Wi-Fi connection**.

The *IP address* for *Mobile Hotspot Connection* is the `inet` address: 127.0.0.1.

The *IP address* for *IITD Wi-Fi Connection* is the `inet` address: 10.184.62.55.

Observation: IP Address of the machine changes when it is connected to a different network.

1.b IP address for different Servers

When we run Domain name, e.g. www.google.com, then first of all our computer requests for *IP address* for www.google.com from the **DNS server**. One website can have multiple servers on

which it is running. So, it will have more than one *IP address*. To obtain the *IP address* of servers, the `nslookup` command is used. This *IP address* depends on the **DNS server** being used.

Google

Results of `nslookup www.google.com some.dns.server` are as following:

```
coolr@coolr-G5-5500:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.207.196
Name:   www.google.com
Address: 2404:6800:4007:822::2004

coolr@coolr-G5-5500:~$ nslookup www.google.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.166.228
Name:   www.google.com
Address: 2404:6800:4002:81e::2004

coolr@coolr-G5-5500:~$ nslookup www.google.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.164
Name:   www.google.com
Address: 2404:6800:4002:814::2004
```

Figure 2: `nslookup` for Google using different DNS servers

IP Addresses obtained for www.google.com from different DNS servers:

- Without specifying the DNS server gave the *IP address* as 142.250.207.196
- *IP address* is 172.217.166.228 with **Cloudfare 1.1.1.1 DNS** server.
- *IP address* is 142.250.194.164 with **Google Public DNS** server.

Facebook

Results of `nslookup www.facebook.com some.dns.server` are as following:

```
coolr@coolr-G5-5500:~$ 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:f12f:83:face:b00c:0:25de

coolr@coolr-G5-5500:~$ nslookup www.facebook.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.239.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f144:181:face:b00c:0:25de

coolr@coolr-G5-5500:~$ nslookup www.facebook.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.1.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f144:82:face:b00c:0:25de
```

Figure 3: `nslookup` for Facebook using different DNS servers

IP Addresses obtained for www.facebook.com from different DNS servers:

- Without specifying the DNS server gave the *IP address* as 157.240.16.35
- *IP address* is 157.240.239.35 with **Cloudfare 1.1.1.1 DNS** server.
- *IP address* is 157.240.1.35 with **Google Public DNS** server.

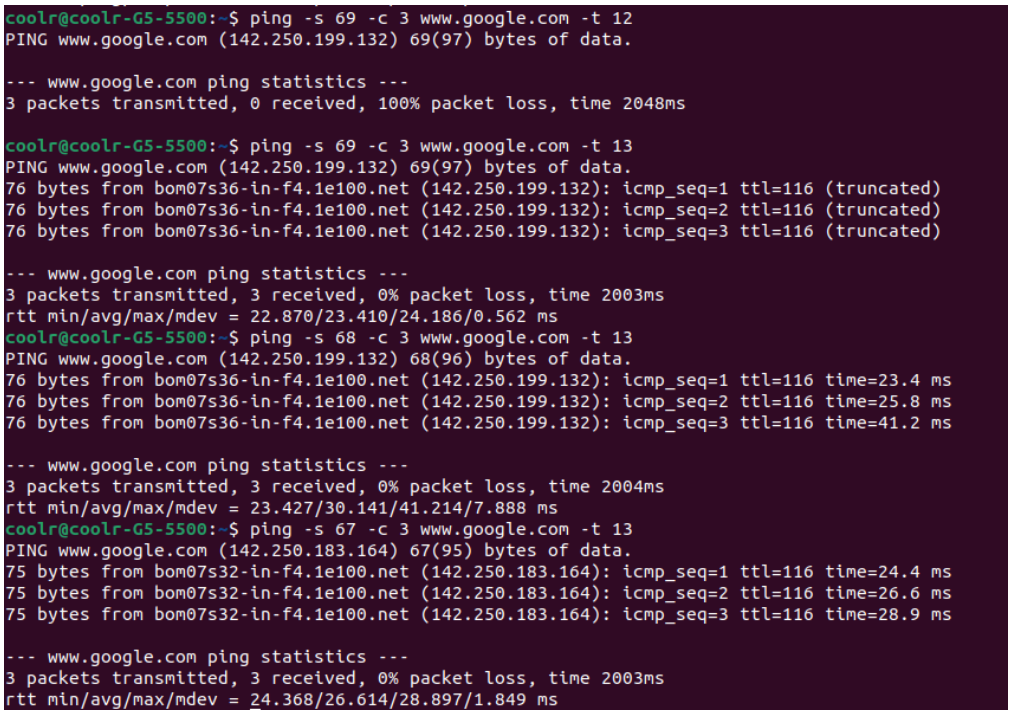
1.c Ping the different IPs

To analyse the ping values, a script was written to **binary search** on different values of *packet size* and *TTL value*.

The size of the transmitted packet is always 28 bytes larger than the size set using the `-s` command. This 28 bytes data has 8 bytes ICMP header and 20 bytes long IP header and this is the header data that has the same structure for all packets.

Observations :

- **Google** Maximum packet size (data) is 68 bytes and smallest TTL value achieved is 13. (Figure 4)
- **IITD** Maximum packet size (data) is 65507 bytes and smallest TTL value achieved is 4. (Figure 5 and Figure 6)
- **Facebook** Maximum packet size (data) is 1472 bytes and smallest TTL value achieved is 13. (Figure 7 and Figure 8)



```
coolr@coolr-G5-5500:~$ ping -s 69 -c 3 www.google.com -t 12
PING www.google.com (142.250.199.132) 69(97) bytes of data.

--- www.google.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

coolr@coolr-G5-5500:~$ ping -s 69 -c 3 www.google.com -t 13
PING www.google.com (142.250.199.132) 69(97) bytes of data.
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=1 ttl=116 (truncated)
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=2 ttl=116 (truncated)
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=3 ttl=116 (truncated)

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 22.870/23.410/24.186/0.562 ms
coolr@coolr-G5-5500:~$ ping -s 68 -c 3 www.google.com -t 13
PING www.google.com (142.250.199.132) 68(96) bytes of data.
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=1 ttl=116 time=23.4 ms
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=2 ttl=116 time=25.8 ms
76 bytes from bom07s36-in-f4.1e100.net (142.250.199.132): icmp_seq=3 ttl=116 time=41.2 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 23.427/30.141/41.214/7.888 ms
coolr@coolr-G5-5500:~$ ping -s 67 -c 3 www.google.com -t 13
PING www.google.com (142.250.183.164) 67(95) bytes of data.
75 bytes from bom07s32-in-f4.1e100.net (142.250.183.164): icmp_seq=1 ttl=116 time=24.4 ms
75 bytes from bom07s32-in-f4.1e100.net (142.250.183.164): icmp_seq=2 ttl=116 time=26.6 ms
75 bytes from bom07s32-in-f4.1e100.net (142.250.183.164): icmp_seq=3 ttl=116 time=28.9 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 24.368/26.614/28.897/1.849 ms
```

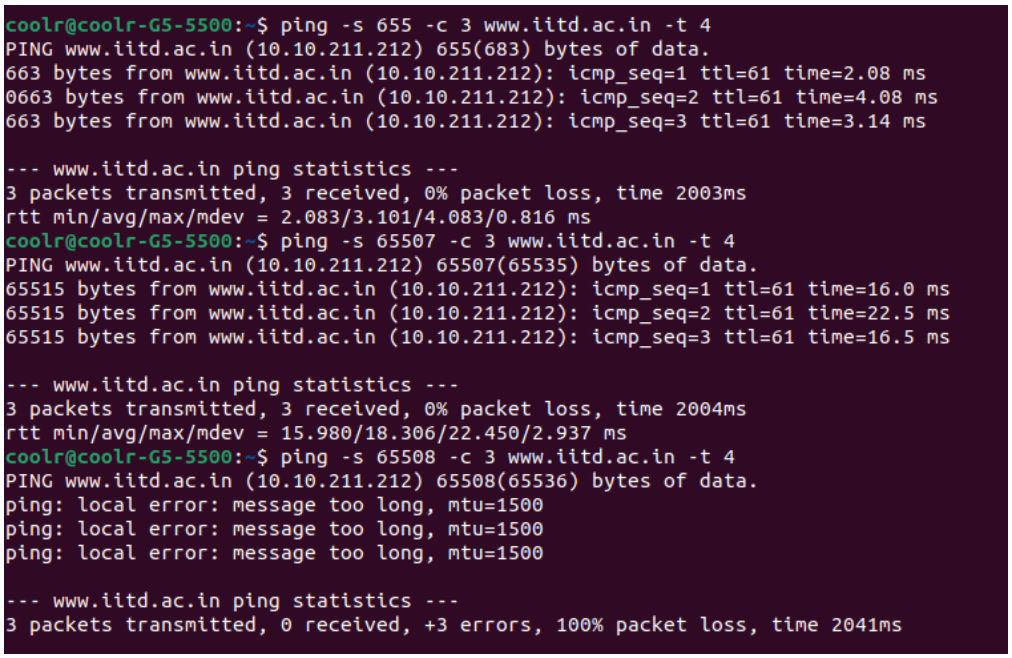
Figure 4: `ping` for Google with different packet size and ttl

```
coolr@coolr-G5-5500:~$ ping -s 655 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 655(683) bytes of data.
663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=1 ttl=61 time=2.08 ms
0663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=2 ttl=61 time=4.08 ms
663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=3 ttl=61 time=3.14 ms

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.083/3.101/4.083/0.816 ms
coolr@coolr-G5-5500:~$ ping -s 65507 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 65507(65535) bytes of data.
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=1 ttl=61 time=16.0 ms
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=2 ttl=61 time=22.5 ms
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=3 ttl=61 time=16.5 ms

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 15.980/18.306/22.450/2.937 ms
coolr@coolr-G5-5500:~$ ping -s 65508 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 65508(65536) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2041ms
```

Figure 5: `ping` for IITD with different packet size

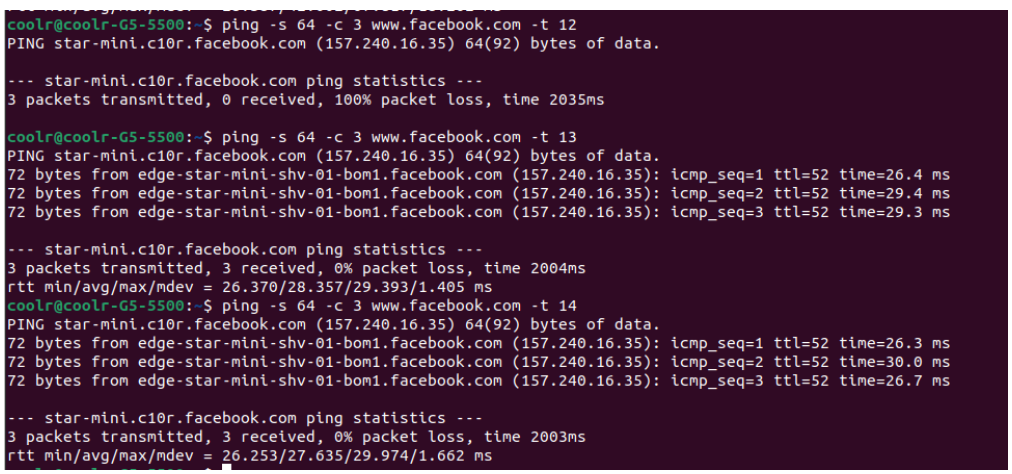
```
coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 12
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2035ms

coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 13
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=1 ttl=52 time=26.4 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=2 ttl=52 time=29.4 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=3 ttl=52 time=29.3 ms

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 26.370/28.357/29.393/1.405 ms
coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 14
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=1 ttl=52 time=26.3 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=2 ttl=52 time=30.0 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=3 ttl=52 time=26.7 ms

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 26.253/27.635/29.974/1.662 ms
```

Figure 6: `ping` for IITD with different TTL values



```
coolr@coolr-G5-5500:~$ ping -s 655 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 655(683) bytes of data.
663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=1 ttl=61 time=2.08 ms
0663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=2 ttl=61 time=4.08 ms
663 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=3 ttl=61 time=3.14 ms

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.083/3.101/4.083/0.816 ms
coolr@coolr-G5-5500:~$ ping -s 65507 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 65507(65535) bytes of data.
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=1 ttl=61 time=16.0 ms
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=2 ttl=61 time=22.5 ms
65515 bytes from www.iitd.ac.in (10.10.211.212): icmp_seq=3 ttl=61 time=16.5 ms

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 15.980/18.306/22.450/2.937 ms
coolr@coolr-G5-5500:~$ ping -s 65508 -c 3 www.iitd.ac.in -t 4
PING www.iitd.ac.in (10.10.211.212) 65508(65536) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500

--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2041ms
```

Figure 7: `ping` for Facebook with different packet size



```
coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 12
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2035ms

coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 13
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=1 ttl=52 time=26.4 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=2 ttl=52 time=29.4 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=3 ttl=52 time=29.3 ms

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 26.370/28.357/29.393/1.405 ms
coolr@coolr-G5-5500:~$ ping -s 64 -c 3 www.facebook.com -t 14
PING star-mini.c10r.facebook.com (157.240.16.35) 64(92) bytes of data.
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=1 ttl=52 time=26.3 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=2 ttl=52 time=30.0 ms
72 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=3 ttl=52 time=26.7 ms

--- star-mini.c10r.facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 26.253/27.635/29.974/1.662 ms
```

Figure 8: `ping` for Facebook with different TTL values

1.d Traceroute Responses

1.d.i With Mobile Hotspot Connection

Results of `traceroute` command when connected to Mobile Hotspot is as following:

- **IITD** Gives no response to `traceroute`. Output to `traceroute iitd.ac.in` is as following:

```
traceroute to iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.248.154  1.876ms  1.510ms  2.603ms
  2   10.50.96.4  47.288ms  29.131ms  40.236ms
```

```
 3   10.50.96.200  50.724ms  28.704ms  26.006ms
 4   *  *  *
 5   10.206.30.29  103.347ms  *  43.922ms
 6   125.23.24.17  40.822ms  21.007ms  40.795ms
 7   116.119.94.36  75.897ms  78.788ms  95.036ms
 8   49.44.129.53  75.139ms  79.720ms  63.976ms
 9   *  *  *
10   *  *  *
11   *  *  *
12   *  *  *
13   *  *  *
14   *  *  *
15   *  *  *
16   *  *  *
17   *  *  *
18   *  *  *
19   *  *  *
20   *  *  *
21   *  *  *
22   *  *  *
23   *  *  *
24   *  *  *
25   *  *  *
26   *  *  *
27   *  *  *
28   *  *  *
29   *  *  *
30   *  *  *
31   *  *  *
32   *  *  *
33   *  *  *
34   *  *  *
35   *  *  *
36   *  *  *
37   *  *  *
38   *  *  *
39   *  *  *
40   *  *  *
41   *  *  *
42   *  *  *
43   *  *  *
44   *  *  *
45   *  *  *
46   *  *  *
47   *  *  *
48   *  *  *
```

```
 49   *  *  *
 50   *  *  *
 51   *  *  *
 52   *  *  *
 53   *  *  *
 54   *  *  *
 55   *  *  *
 56   *  *  *
 57   *  *  *
 58   *  *  *
 59   *  *  *
 60   *  *  *
 61   *  *  *
 62   *  *  *
 63   *  *  *
 64   *  *  *
```

- **Google** The trace obtained was:

```
traceroute to www.google.com (142.250.194.68), 64 hops max
  1   192.168.248.154  2.517ms  1.604ms  1.641ms
  2   10.50.96.4  45.017ms  38.743ms  50.861ms
  3   10.50.96.202  34.565ms  27.000ms  37.236ms
  4   *  *  *
  5   10.206.30.157  50.258ms  *  32.246ms
  6   125.23.24.17  43.632ms  37.045ms  41.819ms
  7   74.125.51.184  37.341ms  33.727ms  29.805ms
  8   *  *  *
  9   66.249.95.74  46.708ms  40.792ms  20.227ms
 10   142.251.49.121  39.998ms  38.826ms  40.750ms
 11   142.250.194.68  46.185ms  34.291ms  89.454ms
```

- **Facebook**The trace obtained was:

```
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 64 hops max
  1   192.168.248.154  3.499ms  1.790ms  2.544ms
  2   10.50.96.4  93.376ms  16.378ms  18.755ms
  3   10.50.96.202  17.187ms  18.952ms  20.711ms
  4   *  *  *
  5   10.206.30.29  27.326ms  *  75.257ms
  6   125.23.24.17  24.640ms  18.462ms  20.100ms
  7   116.119.104.148  72.919ms  52.576ms  59.392ms
  8   157.240.67.48  42.825ms  39.329ms  40.494ms
  9   157.240.53.23  53.675ms  49.333ms  49.308ms
 10   157.240.38.169  41.798ms  40.165ms  39.560ms
 11   157.240.16.35  47.840ms  49.091ms  50.099ms
```

1.d.ii With IITD Wi-Fi Connection

Results of `traceroute` command when connected to IITD Wi-Fi is as following:

- **IITD** Running `traceroute` using *IITD VPN* was successful and gave the following trace:

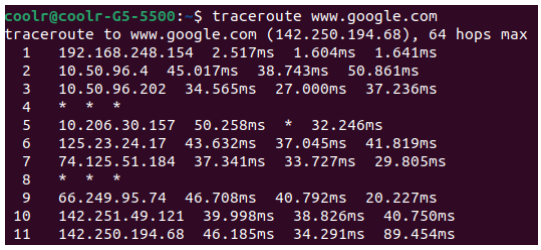
```
traceroute to iitd.ac.in (10.10.211.212), 64 hops max
  1   10.184.32.14  2.212ms  2.567ms  2.871ms
  2   10.254.236.10  2.528ms  2.928ms  2.637ms
  3   10.10.211.212  1.474ms  0.996ms  1.419ms
```

- **Google** Running `traceroute` using *IITD VPN* was not successful (No response) and gave the following trace:

```
traceroute www.google.com
traceroute to www.google.com (142.250.199.132), 64 hops max
  1   10.184.32.14  18.867ms  2.456ms  19.730ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
        .
        :

 63   *  *  *
 64   *  *  *
```

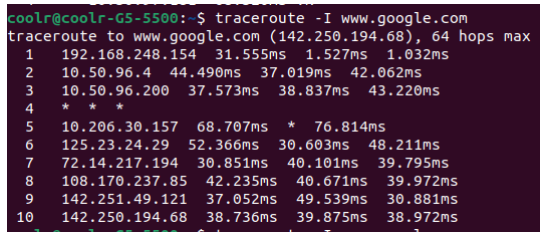
- **Facebook** Running `traceroute` using *IITD VPN* was not successful (No response) and gave the following trace:

```
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 64 hops max
  1   10.184.32.14  1.392ms  2.372ms  1.159ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
        :
        .
 64   *  *  *
```



```
coolr@coolr-G5-5500:~$ traceroute www.google.com
traceroute to www.google.com (142.250.194.68), 64 hops max
  1   192.168.248.154  2.517ms  1.604ms  1.641ms
  2   10.50.96.4  45.017ms  38.743ms  50.861ms
  3   10.50.96.202  34.565ms  27.000ms  37.236ms
  4   *  *  *
  5   10.206.30.157  50.258ms  *  32.246ms
  6   125.23.24.17  43.632ms  37.045ms  41.819ms
  7   74.125.51.184  37.341ms  33.727ms  29.805ms
  8   *  *  *
  9   66.249.95.74  46.708ms  40.792ms  20.227ms
 10   142.251.49.121  39.998ms  38.826ms  40.750ms
 11   142.250.194.68  46.185ms  34.291ms  89.454ms
```

(a) default



```
coolr@coolr-G5-5500:~$ traceroute -I www.google.com
traceroute to www.google.com (142.250.194.68), 64 hops max
  1   192.168.248.154  31.555ms  1.527ms  1.032ms
  2   10.50.96.4  44.490ms  37.019ms  42.062ms
  3   10.50.96.200  37.573ms  38.837ms  43.220ms
  4   *  *  *
  5   10.206.30.157  68.707ms  *  76.814ms
  6   125.23.24.29  52.366ms  30.603ms  48.211ms
  7   72.14.217.194  30.851ms  40.101ms  39.795ms
  8   108.170.237.85  42.235ms  40.671ms  39.972ms
  9   142.251.49.121  37.052ms  49.539ms  30.881ms
 10   142.250.194.68  38.736ms  39.875ms  38.972ms
```

(b) With -I

Figure 9: `traceroute` for Google

1.d.iii Observations And Methods to Improve Tracing

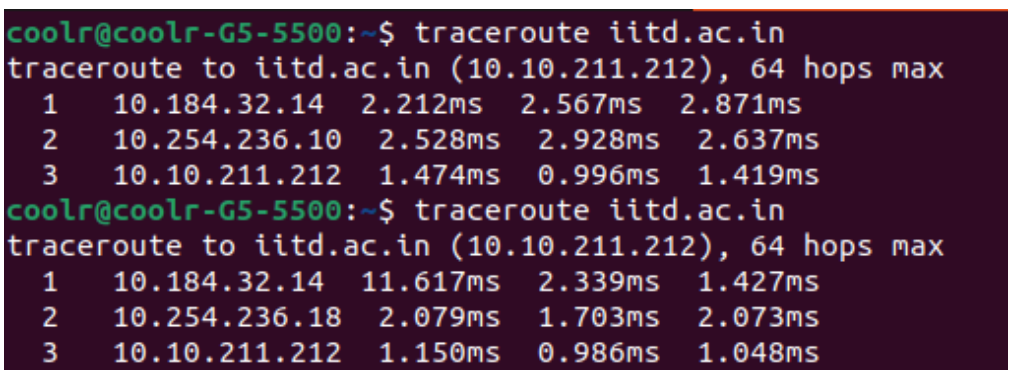
The following observations and some methods to **improve tracing** were made when running `traceroute`:

1. Three packets are pinged for each hop value to *display consistency, or a lack, in the route*

2. The router at the 8th hop value doesn't ping when using the default `traceroute` command (Figure 9(a)). `traceroute` by default uses UDP which is unreliable and hence many servers do not respond to it. To avoid this issue, -I flag can be used, which uses ICPM echo as the packet instead. See Fig. 9 for more details.

3. Different routes are followed when using different networks to access the same server.

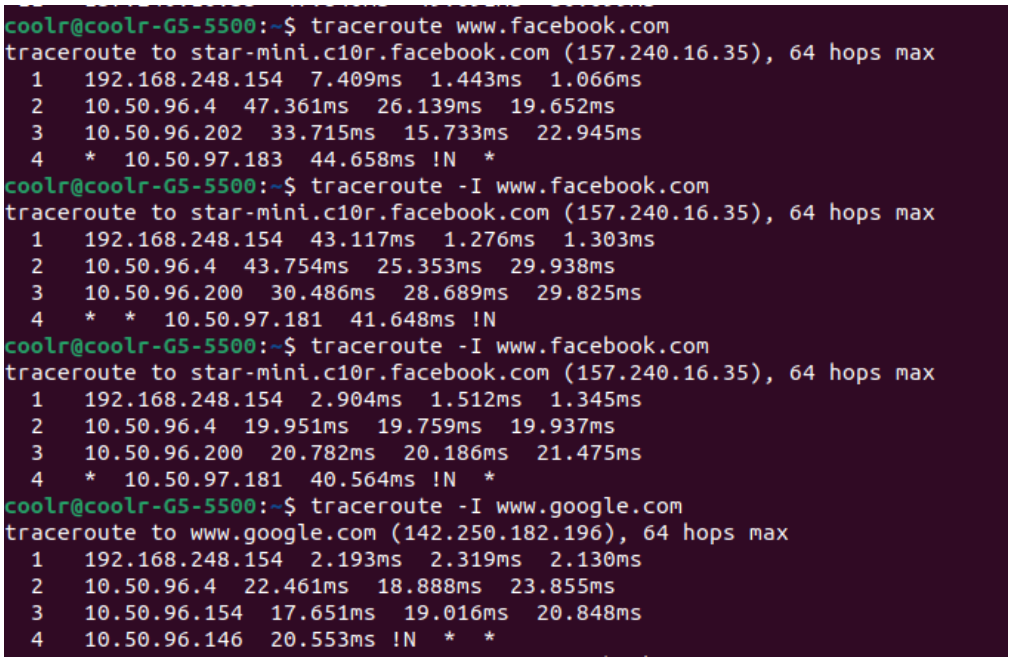
4. Different routes are followed when `traceroute` is run multiple times with same connection (Fig. 9 Fig. 10). e.g. `traceroute iitd.ac.in` with same connection has following results:



```
coolr@coolr-G5-5500:~$ traceroute iitd.ac.in
traceroute to iitd.ac.in (10.10.211.212), 64 hops max
  1   10.184.32.14  2.212ms  2.567ms  2.871ms
  2   10.254.236.10  2.528ms  2.928ms  2.637ms
  3   10.10.211.212  1.474ms  0.996ms  1.419ms
coolr@coolr-G5-5500:~$ traceroute iitd.ac.in
traceroute to iitd.ac.in (10.10.211.212), 64 hops max
  1   10.184.32.14  11.617ms  2.339ms  1.427ms
  2   10.254.236.18  2.079ms  1.703ms  2.073ms
  3   10.10.211.212  1.150ms  0.986ms  1.048ms
```

Figure 10: `traceroute` for IITD multiple times with same connection

5. When If ISP blocks packets on the path to www.iitd.ac.in then try with a different destination like www.google.com, or www.facebook.com, etc. we find the following observations:



```
coolr@coolr-G5-5500:~$ traceroute www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 64 hops max
  1   192.168.248.154  7.409ms  1.443ms  1.066ms
  2   10.50.96.4  47.361ms  26.139ms  19.652ms
  3   10.50.96.202  33.715ms  15.733ms  22.945ms
  4   *  10.50.97.183  44.658ms !N  *
coolr@coolr-G5-5500:~$ traceroute -I www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 64 hops max
  1   192.168.248.154  43.117ms  1.276ms  1.303ms
  2   10.50.96.4  43.754ms  25.353ms  29.938ms
  3   10.50.96.200  30.486ms  28.689ms  29.825ms
  4   *  *  10.50.97.181  41.648ms !N
coolr@coolr-G5-5500:~$ traceroute -I www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 64 hops max
  1   192.168.248.154  2.904ms  1.512ms  1.345ms
  2   10.50.96.4  19.951ms  19.759ms  19.937ms
  3   10.50.96.200  20.782ms  20.186ms  21.475ms
  4   *  10.50.97.181  40.564ms !N  *
coolr@coolr-G5-5500:~$ traceroute -I www.google.com
traceroute to www.google.com (142.250.182.196), 64 hops max
  1   192.168.248.154  2.193ms  2.319ms  2.130ms
  2   10.50.96.4  22.461ms  18.888ms  23.855ms
  3   10.50.96.154  17.651ms  19.016ms  20.848ms
  4   10.50.96.146  20.553ms !N  *  *
```

Figure 11: `traceroute` for Google and Facebook when `traceroute` for IITD was running

!N means Network Unreachable means that we are not able to send IP packets to the destination. (Reference: click here)

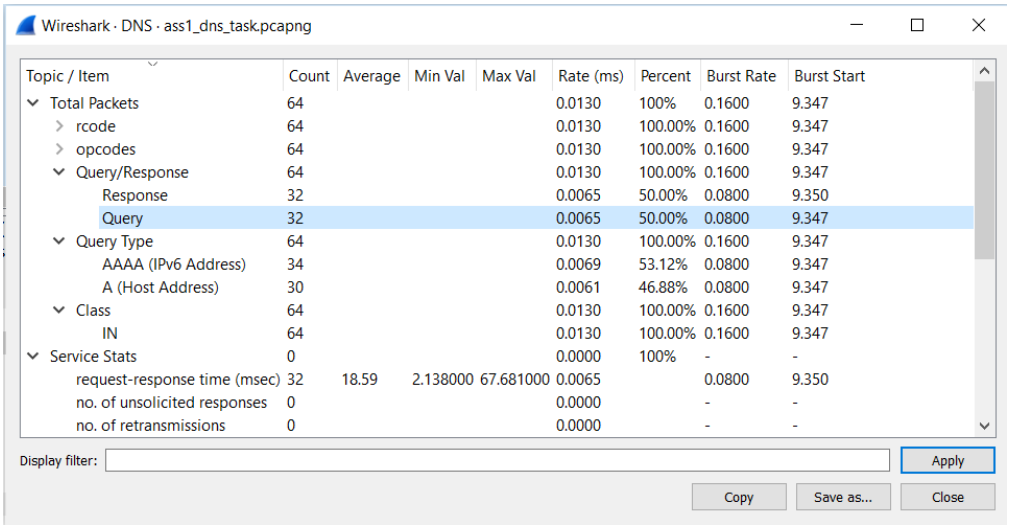
2 Packet Analysis

2.a DNS Task

My IP Address: 192.168.248.83

Using Wireshark we grab all the packets in `"ass1-dns-task.pcapng"` , while visiting CSE IITD. According to captured packets Report is as following:

1. All DNS querry and response messages are sent over UDP.
2. Total 32 querries were sent from my browser to DNS Server(s). We can get no. of DNS querries from **Statistics − DNS**. Following window will pop up:



Wireshark · DNS · ass1_dns_task.pcapng

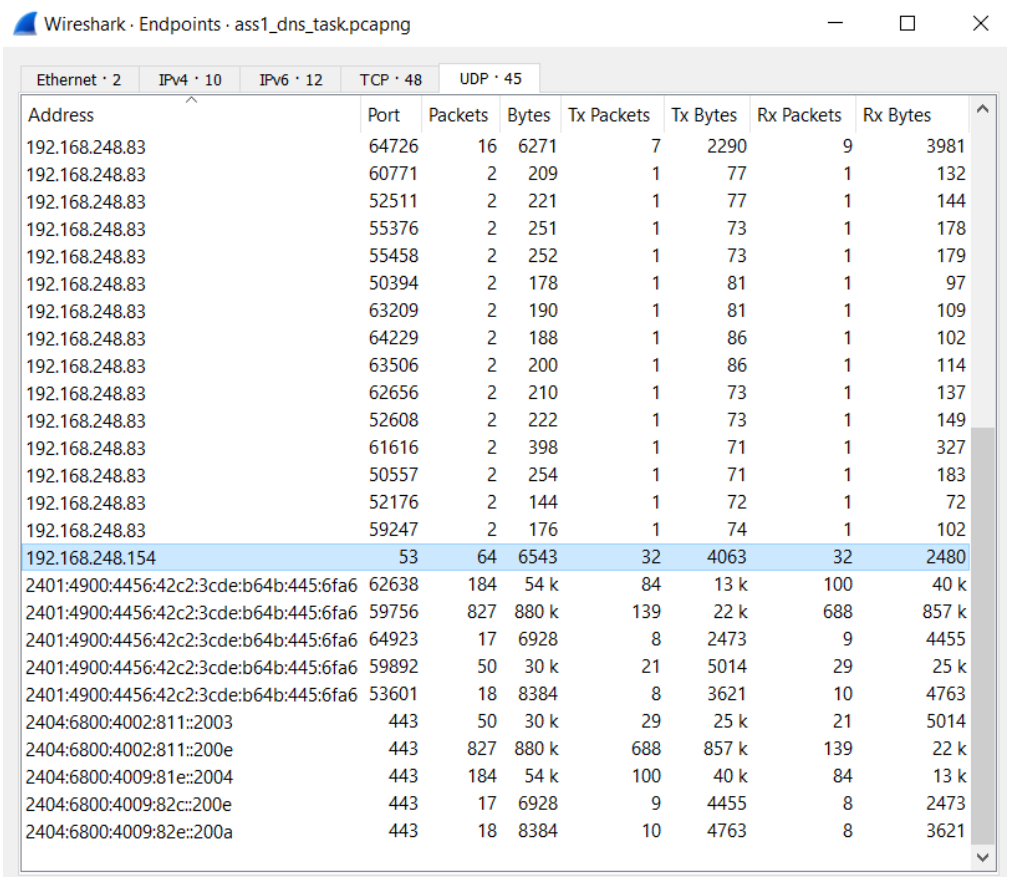
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	64				0.0130	100%	0.1600	9.347
rcode	64				0.0130	100.00%	0.1600	9.347
opcodes	64				0.0130	100.00%	0.1600	9.347
Query/Response	64				0.0130	100.00%	0.1600	9.347
Response	32				0.0065	50.00%	0.0800	9.350
Query	32				0.0065	50.00%	0.0800	9.347
Query Type	64				0.0130	100.00%	0.1600	9.347
AAAA (IPv6 Address)	34				0.0069	53.12%	0.0800	9.347
A (Host Address)	30				0.0061	46.88%	0.0800	9.347
Class	64				0.0130	100.00%	0.1600	9.347
IN	64				0.0130	100.00%	0.1600	9.347
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	32	18.59	2.138000	67.681000	0.0065		0.0800	9.350
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-

Display filter: Apply

Copy Save as... Close

Figure 12: Total DNS Querries made

3. DNS querry responses are only from port 53 and DNS uses UDP. Using these facts we can check in **Statistics – Endpoints** .



Wireshark · Endpoints · ass1_dns_task.pcapng

Ethernet · 2 | IPv4 · 10 | IPv6 · 12 | TCP · 48 | UDP · 45

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.248.83	64726	16	6271	7	2290	9	3981
192.168.248.83	60771	2	209	1	77	1	132
192.168.248.83	52511	2	221	1	77	1	144
192.168.248.83	55376	2	251	1	73	1	178
192.168.248.83	55458	2	252	1	73	1	179
192.168.248.83	50394	2	178	1	81	1	97
192.168.248.83	63209	2	190	1	81	1	109
192.168.248.83	64229	2	188	1	86	1	102
192.168.248.83	63506	2	200	1	86	1	114
192.168.248.83	62656	2	210	1	73	1	137
192.168.248.83	52608	2	222	1	73	1	149
192.168.248.83	61616	2	398	1	71	1	327
192.168.248.83	50557	2	254	1	71	1	183
192.168.248.83	52176	2	144	1	72	1	72
192.168.248.83	59247	2	176	1	74	1	102
192.168.248.154	53	64	6543	32	4063	32	2480
2401:4900:4456:42c2:3cde:b64b:445:6fa6	62638	184	54 k	84	13 k	100	40 k
2401:4900:4456:42c2:3cde:b64b:445:6fa6	59756	827	880 k	139	22 k	688	857 k
2401:4900:4456:42c2:3cde:b64b:445:6fa6	64923	17	6928	8	2473	9	4455
2401:4900:4456:42c2:3cde:b64b:445:6fa6	59892	50	30 k	21	5014	29	25 k
2401:4900:4456:42c2:3cde:b64b:445:6fa6	53601	18	8384	8	3621	10	4763
2404:6800:4002:811::2003	443	50	30 k	29	25 k	21	5014
2404:6800:4002:811::200e	443	827	880 k	688	857 k	139	22 k
2404:6800:4009:81e::2004	443	184	54 k	100	40 k	84	13 k
2404:6800:4009:82c::200e	443	17	6928	9	4455	8	2473
2404:6800:4009:82e::200a	443	18	8384	10	4763	8	3621

Figure 13: Total DNS Servers

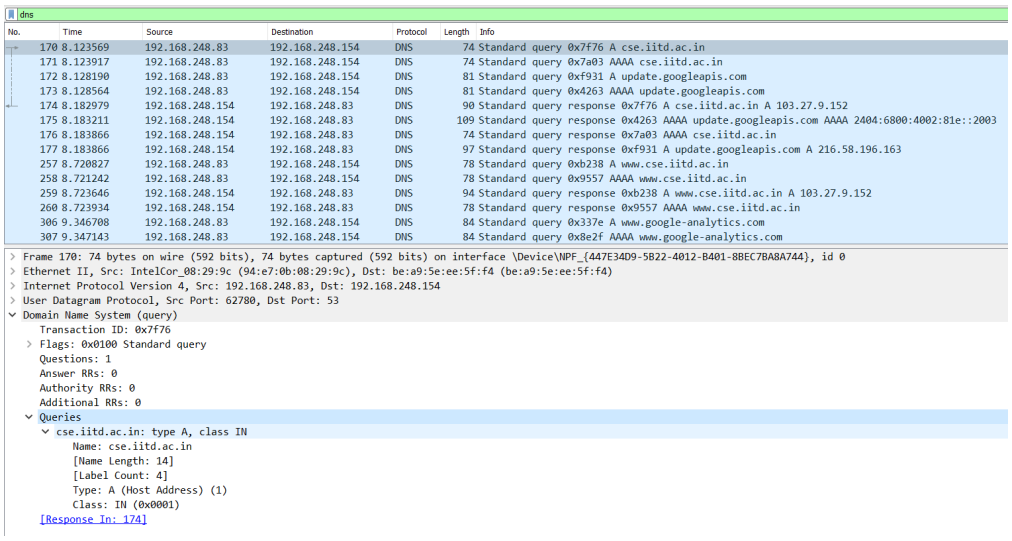
O nly One DNS server is involved in this case. (more than one is also possible.)

4. DNS Server 192.168.248.154 respond. (Figure 15)

5. DNS querry request was made with only one server. And we get one response. All servers respond in this case.

6. The resource records involved in resolving the IP address of the site:

   (a) **Querry**



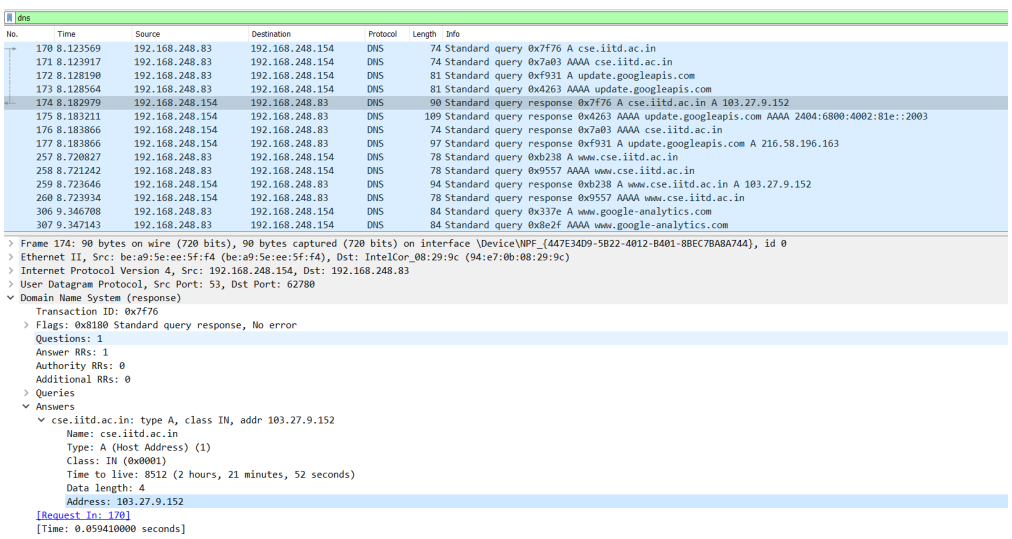
dns

No.	Time	Source	Destination	Protocol	Length	Info
170	8.123569	192.168.248.83	192.168.248.154	DNS	74	Standard query 0x7f76 A cse.iitd.ac.in
171	8.123917	192.168.248.83	192.168.248.154	DNS	74	Standard query 0x7a03 AAAA cse.iitd.ac.in
172	8.128190	192.168.248.83	192.168.248.154	DNS	81	Standard query 0xf931 A update.googleapis.com
173	8.128564	192.168.248.83	192.168.248.154	DNS	81	Standard query 0x4263 AAAA update.googleapis.com
174	8.182979	192.168.248.154	192.168.248.83	DNS	90	Standard query response 0x7f76 A cse.iitd.ac.in A 103.27.9.152
175	8.183211	192.168.248.154	192.168.248.83	DNS	109	Standard query response 0x4263 AAAA update.googleapis.com AAAA 2404:6800:4002:81e::2003
176	8.183866	192.168.248.154	192.168.248.83	DNS	74	Standard query response 0x7a03 AAAA cse.iitd.ac.in
177	8.183866	192.168.248.154	192.168.248.83	DNS	97	Standard query response 0xf931 A update.googleapis.com A 216.58.196.163
257	8.720827	192.168.248.83	192.168.248.154	DNS	78	Standard query 0xb238 A www.cse.iitd.ac.in
258	8.721242	192.168.248.83	192.168.248.154	DNS	78	Standard query 0x9557 AAAA www.cse.iitd.ac.in
259	8.723646	192.168.248.154	192.168.248.83	DNS	94	Standard query response 0xb238 A www.cse.iitd.ac.in A 103.27.9.152
260	8.723934	192.168.248.154	192.168.248.83	DNS	78	Standard query response 0x9557 AAAA www.cse.iitd.ac.in
306	9.346708	192.168.248.83	192.168.248.154	DNS	84	Standard query 0x337e A www.google-analytics.com
307	9.347143	192.168.248.83	192.168.248.154	DNS	84	Standard query 0x8e2f AAAA www.google-analytics.com

```
> Frame 170: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{447E34D9-5B22-4012-B401-8BEC7BA8A744}, id 0
> Ethernet II, Src: IntelCor_08:29:9c (94:e7:0b:08:29:9c), Dst: be:a9:5e:ee:5f:f4 (be:a9:5e:ee:5f:f4)
> Internet Protocol Version 4, Src: 192.168.248.83, Dst: 192.168.248.154
> User Datagram Protocol, Src Port: 62780, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7f76
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v cse.iitd.ac.in: type A, class IN
        Name: cse.iitd.ac.in
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 174]
```

Figure 14: DNS Querry for CSE IITD

   (b) **Response**



dns

No.	Time	Source	Destination	Protocol	Length	Info
170	8.123569	192.168.248.83	192.168.248.154	DNS	74	Standard query 0x7f76 A cse.iitd.ac.in
171	8.123917	192.168.248.83	192.168.248.154	DNS	74	Standard query 0x7a03 AAAA cse.iitd.ac.in
172	8.128190	192.168.248.83	192.168.248.154	DNS	81	Standard query 0xf931 A update.googleapis.com
173	8.128564	192.168.248.83	192.168.248.154	DNS	81	Standard query 0x4263 AAAA update.googleapis.com
174	8.182979	192.168.248.154	192.168.248.83	DNS	90	Standard query response 0x7f76 A cse.iitd.ac.in A 103.27.9.152
175	8.183211	192.168.248.154	192.168.248.83	DNS	109	Standard query response 0x4263 AAAA update.googleapis.com AAAA 2404:6800:4002:81e::2003
176	8.183866	192.168.248.154	192.168.248.83	DNS	74	Standard query response 0x7a03 AAAA cse.iitd.ac.in
177	8.183866	192.168.248.154	192.168.248.83	DNS	97	Standard query response 0xf931 A update.googleapis.com A 216.58.196.163
257	8.720827	192.168.248.83	192.168.248.154	DNS	78	Standard query 0xb238 A www.cse.iitd.ac.in
258	8.721242	192.168.248.83	192.168.248.154	DNS	78	Standard query 0x9557 AAAA www.cse.iitd.ac.in
259	8.723646	192.168.248.154	192.168.248.83	DNS	94	Standard query response 0xb238 A www.cse.iitd.ac.in A 103.27.9.152
260	8.723934	192.168.248.154	192.168.248.83	DNS	78	Standard query response 0x9557 AAAA www.cse.iitd.ac.in
306	9.346708	192.168.248.83	192.168.248.154	DNS	84	Standard query 0x337e A www.google-analytics.com
307	9.347143	192.168.248.83	192.168.248.154	DNS	84	Standard query 0x8e2f AAAA www.google-analytics.com

```
> Frame 174: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{447E34D9-5B22-4012-B401-8BEC7BA8A744}, id 0
> Ethernet II, Src: be:a9:5e:ee:5f:f4 (be:a9:5e:ee:5f:f4), Dst: IntelCor_08:29:9c (94:e7:0b:08:29:9c)
> Internet Protocol Version 4, Src: 192.168.248.154, Dst: 192.168.248.83
> User Datagram Protocol, Src Port: 53, Dst Port: 62780
v Domain Name System (response)
    Transaction ID: 0x7f76
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v cse.iitd.ac.in: type A, class IN, addr 103.27.9.152
        Name: cse.iitd.ac.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 8512 (2 hours, 21 minutes, 52 seconds)
        Data length: 4
        Address: 103.27.9.152
    [Request In: 170]
    [Time: 0.059410000 seconds]
```

Figure 15: DNS Querry Response for CSE IITD

   (c) Details as recieved in Response (Zoom in to Figure 15).

```
cse.iitd.ac.in: type A, class IN, addr 103.27.9.152
    Name: cse.iitd.ac.in
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 8512 (2 hours, 21 minutes, 52 seconds)
    Data length: 4
    Address: 103.27.9.152
```

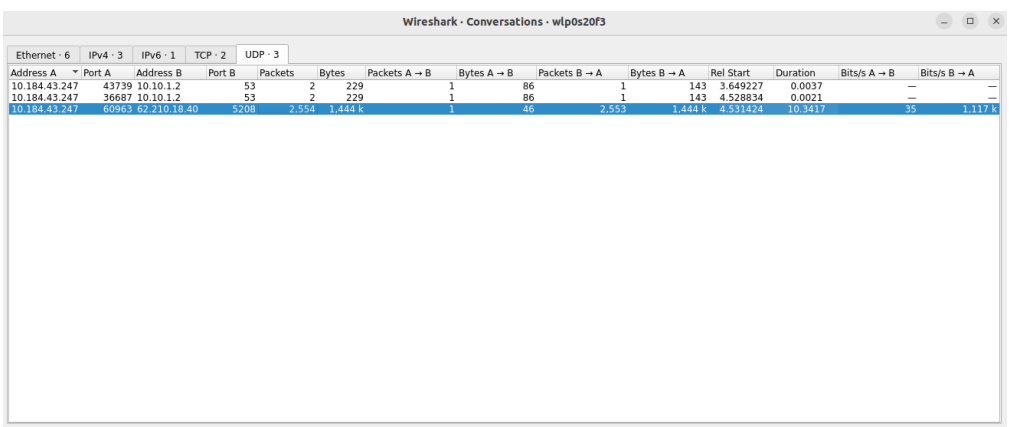
Figure 16: Details for IP Address, Name , Type, TTL etc. for CSE IITD

2.b Iperf Task

My machine's IP Address during packet capturing: 10.184.43.247

P acket Captured during `iperf3 -u -t 10 -c ping.online.net -p 5208 -R` are in file `ass1-iperf-task.pca`
Answer to asked questions:

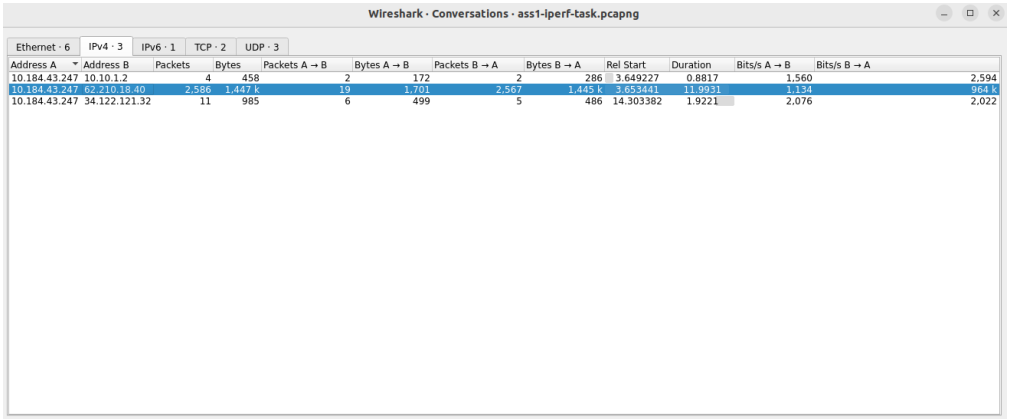
1. Only one packet was transferred from the iperf3 client(my machine) and destination server. Check this from **Statistics – Conversation**. A popup will come to the screen as shown in Figure 17.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.184.43.247	43739	10.10.1.2	53	2	229	1	86	1	143	3.649227	0.0037	—	—
10.184.43.247	36687	10.10.1.2	53	2	229	1	86	1	143	4.528834	0.0021	—	—
10.184.43.247	60963	62.210.18.40	5208	2,554	1,444 k	1	46	2,553	1,444 k	4.531424	10.3417	35	1,117 k

Figure 17: Packet transfer from client(A here) to server(B here)

2. Client: 10.184.43.247 (A) (My device) Server: 62.210.18.40 (B) For analyzing packet transfer go to **Statistis – Conversations** Open IPv4 tab.



Wireshark · Conversations · ass1-iperf-task.pcapng

Ethernet · 6 | IPv4 · 3 | IPv6 · 1 | TCP · 2 | UDP · 3

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.184.43.247	10.10.1.2	4	458	2	172	2	286	3.649227	0.8817	1,560	2,594
10.184.43.247	62.210.18.40	2,586	1,447 k	19	1,701	2,567	1,445 k	3.653441	11.9931	1,134	964 k
10.184.43.247	34.122.121.32	11	985	6	499	5	486	14.303382	1.9221	2,076	2,022

Figure 18: Conversations IPv4 tab

By observations, B -¿ A packet transfer is maximum. From B to A:

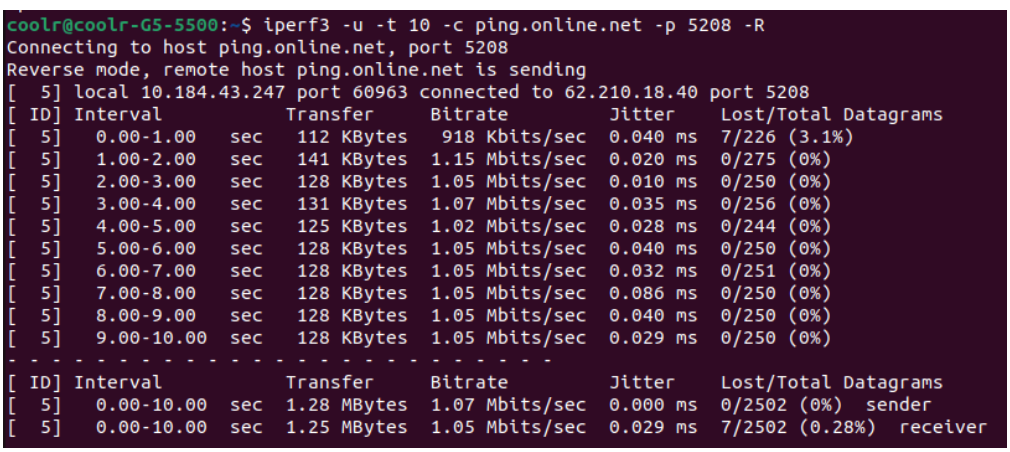
$$Total\ Data\ Transfer = 1,445\ k\ bytes$$

$$Total\ Packets\ transferred = 2567$$

$$Average\ Packet\ Size = \frac{Total\ Data\ Transfer}{Total\ Packets\ transferred}$$

$$Average\ Packet\ Size \approx 563\ bytes$$

3. The throughput (bytes transferred per unit time) from terminal = 1.05 Mbits/sec.



```
coolr@coolr-G5-5500:~$ iperf3 -u -t 10 -c ping.online.net -p 5208 -R
Connecting to host ping.online.net, port 5208
Reverse mode, remote host ping.online.net is sending
[  5] local 10.184.43.247 port 60963 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec   112 KBytes   918 Kbits/sec  0.040 ms  7/226 (3.1%)
[  5]   1.00-2.00   sec   141 KBytes  1.15 Mbits/sec  0.020 ms  0/275 (0%)
[  5]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec  0.010 ms  0/250 (0%)
[  5]   3.00-4.00   sec   131 KBytes  1.07 Mbits/sec  0.035 ms  0/256 (0%)
[  5]   4.00-5.00   sec   125 KBytes  1.02 Mbits/sec  0.028 ms  0/244 (0%)
[  5]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec  0.040 ms  0/250 (0%)
[  5]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec  0.032 ms  0/251 (0%)
[  5]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec  0.086 ms  0/250 (0%)
[  5]   8.00-9.00   sec   128 KBytes  1.05 Mbits/sec  0.040 ms  0/250 (0%)
[  5]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec  0.029 ms  0/250 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.00  sec  1.28 MBytes  1.07 Mbits/sec  0.000 ms  0/2502 (0%)  sender
[  5]   0.00-10.00  sec  1.25 MBytes  1.05 Mbits/sec  0.029 ms  7/2502 (0.28%)  receiver
```

Figure 19: Terminal Output on `iperf3 -u -t 10 -c ping.online.net -p 5208 -R` command

The throughput (bytes transferred per unit time) from Wireshark = 1117 k Bits/sec.($\approx 1.12 Mbits/sec) Thereisadifferenceofapprox 0.07 Mbits/sec.$

2.c HTTP Task

Answers:

1. HTTP packets: 2.(Figure 20) HTTP2 packets: 10.(Figure 21)

Wireshark · Packet Counter · http2-h2c.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	2				0.0033	100%	0.0100	0.000
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	1				0.0017	50.00%	0.0100	0.600
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	1				0.0017	100.00%	0.0100	0.600
101 Switching Protocols	1				0.0017	100.00%	0.0100	0.600
HTTP Request Packets	1				0.0017	50.00%	0.0100	0.000
GET	1				0.0017	100.00%	0.0100	0.000

Figure 20: HTTP packet counts `Settings -- HTTP`

Wireshark · HTTP2 · http2-h2c.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP2	10				0.0316	100%	0.0700	0.600
Type	10				0.0316	100.00%	0.0700	0.600
WINDOW_UPDATE	1				0.0032	10.00%	0.0100	0.601
SETTINGS	4				0.0126	40.00%	0.0300	0.600
HEADERS	3				0.0095	30.00%	0.0200	0.601
DATA	2				0.0063	20.00%	0.0100	0.601

Figure 21: HTTP2 packet counts `Settings -- HTTP2`

2. First object is fetched at frame 6. HTTP/2 packets are exchanged between client and server here before the first object is fetched: 5 packets.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.2	139.162.123.134	HTTP	244	GET /robots.txt HTTP/1.1
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3	0.600465	10.9.0.2	139.162.123.134	HTTP2	90	Magic
4	0.600541	10.9.0.2	139.162.123.134	HTTP2	93	SETTINGS[0]
5	0.600575	10.9.0.2	139.162.123.134	HTTP2	75	SETTINGS[0]
6	0.600596	139.162.123.134	10.9.0.2	HTTP2	342	HEADERS[1]: 200 OK, DATA[1] (text/plain)
7	0.600603	10.9.0.2	139.162.123.134	HTTP2	79	WINDOW_UPDATE[0]
8	0.601307	10.9.0.2	139.162.123.134	HTTP2	115	HEADERS[3]: GET /humans.txt
9	0.912304	139.162.123.134	10.9.0.2	HTTP2	75	SETTINGS[0]
10	0.916413	139.162.123.134	10.9.0.2	HTTP2	156	HEADERS[3]: 404 Not Found, DATA[3] (text/plain)

Figure 22: packets in `http2-h2c.pcap`

3. Main difference observed in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets:

(a) HTTP2 uses header compression. That's why HTTP2 headers are smaller than HTTP headers.

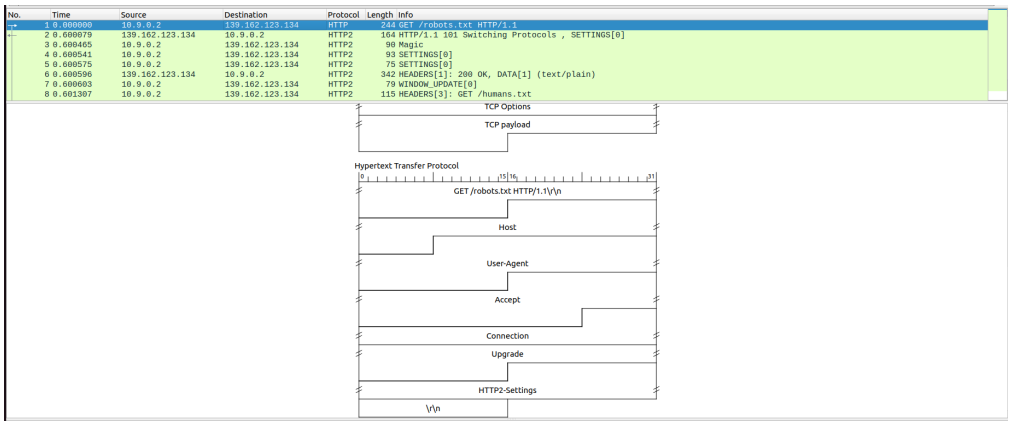


Figure 23: HTTP Header

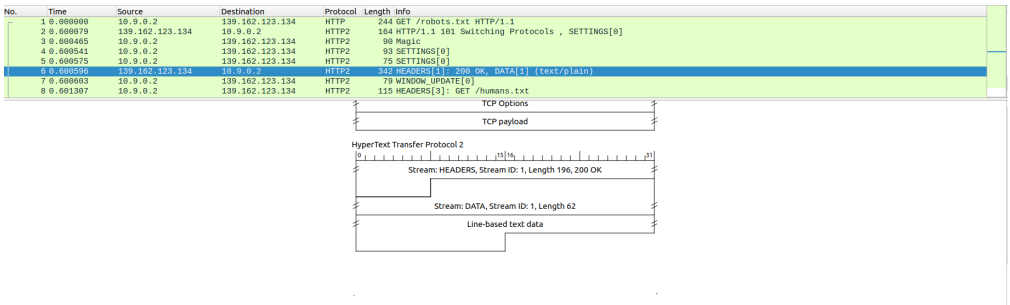


Figure 24: HTTP2 Header

(b) HTTP2 headers had an attribute **stream** that is not present in HTTP.

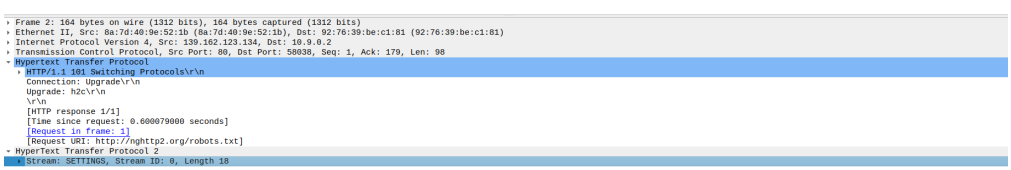
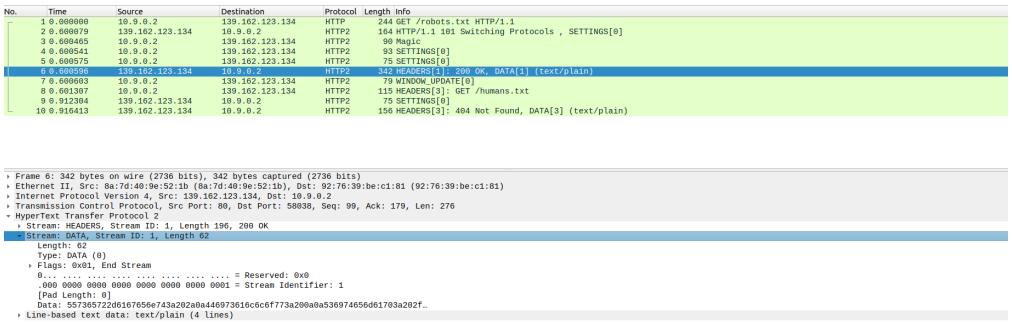


Figure 25

(c) Frame 6 is a push response from the server(pushing data that is not requested). One HTTP2 response header from the server doesn't have an http2 request. but in the HTTP response header, there is always a request made before it.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.2	139.162.123.134	HTTP	244	GET /robots.txt HTTP/1.1
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3	0.600465	10.9.0.2	139.162.123.134	HTTP2	90	Magic
4	0.600541	10.9.0.2	139.162.123.134	HTTP2	93	SETTINGS[0]
5	0.600575	10.9.0.2	139.162.123.134	HTTP2	75	SETTINGS[0]
6	0.600596	139.162.123.134	10.9.0.2	HTTP2	342	HEADERS[1]: 200 OK, DATA[1] (text/plain)
7	0.600603	10.9.0.2	139.162.123.134	HTTP2	79	WINDOW_UPDATE[0]
8	0.601307	10.9.0.2	139.162.123.134	HTTP2	115	HEADERS[3]: GET /humans.txt
9	0.912304	139.162.123.134	10.9.0.2	HTTP2	75	SETTINGS[0]
10	0.916413	139.162.123.134	10.9.0.2	HTTP2	156	HEADERS[3]: 404 Not Found, DATA[3] (text/plain)

```
▸ Frame 6: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
▸ Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 50038, Seq: 99, Ack: 179, Len: 276
▾ HyperText Transfer Protocol 2
  ▸ Stream: HEADERS, Stream ID: 1, Length 196, 200 OK
  ▾ Stream: DATA, Stream ID: 1, Length 62
      Length: 62
      Type: DATA (0)
    ▸ Flags: 0x01, End Stream
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0001 = Stream Identifier: 1
      [Pad Length: 0]
      Data: 557365722d6167656e743a202a0a446973616c6c6f773a200a0a536974656d61703a202f…
  ▸ Line-based text data: text/plain (4 lines)
```

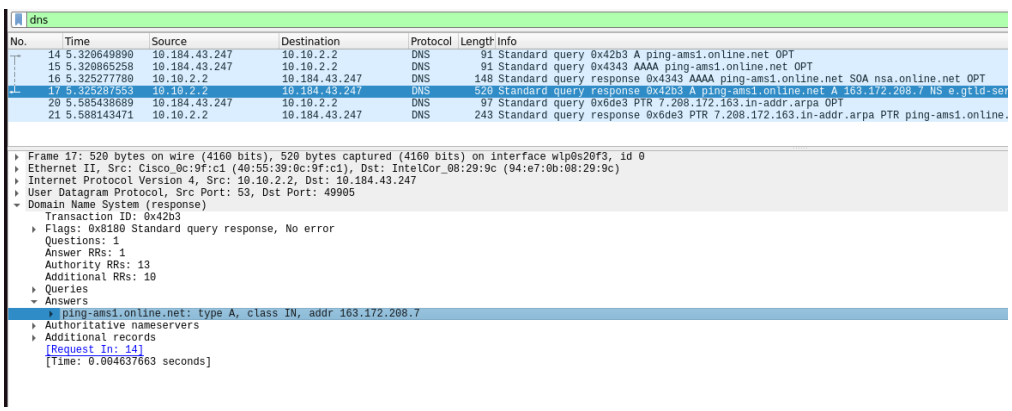
Figure 26: HTTP2 push

2.d PING Task

I made a ping request with packet sizes 1000 and 2500. The question asked for a ping request with packet size 2500 but server is not responding with this packet size so I also ping with -s 1000.

1. After running command `ping -s 1000 ping-ams1.online.net -c 5` on the terminal and capturing packets in Wireshark. Observations are as follows:

   (a) IP Address for ping-ams1.online.net : **163.172.208.7**. (Obtained from the response of DNS see figure 27)



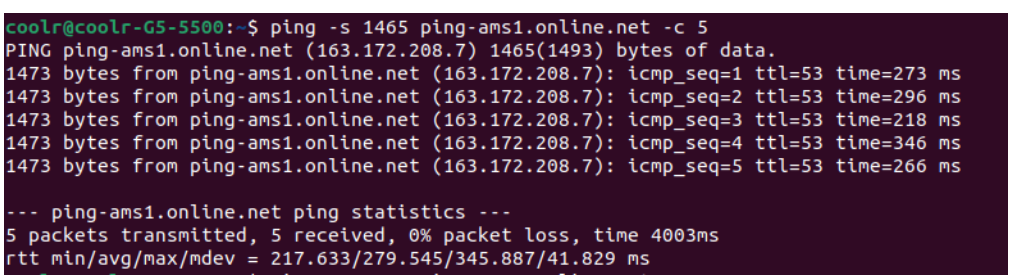
dns

No.	Time	Source	Destination	Protocol	Length	Info
14	5.320649890	10.184.43.247	10.10.2.2	DNS	91	Standard query 0x42b3 A ping-ams1.online.net OPT
15	5.320865258	10.184.43.247	10.10.2.2	DNS	91	Standard query 0x4343 AAAA ping-ams1.online.net OPT
16	5.325277780	10.10.2.2	10.184.43.247	DNS	148	Standard query response 0x4343 AAAA ping-ams1.online.net SOA nsa.online.net OPT
17	5.325287553	10.10.2.2	10.184.43.247	DNS	520	Standard query response 0x42b3 A ping-ams1.online.net A 163.172.208.7 NS e.gtld-ser
20	5.585438689	10.184.43.247	10.10.2.2	DNS	97	Standard query 0x6de3 PTR 7.208.172.163.in-addr.arpa OPT
21	5.588143471	10.10.2.2	10.184.43.247	DNS	243	Standard query response 0x6de3 PTR 7.208.172.163.in-addr.arpa PTR ping-ams1.online.

```
▸ Frame 17: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface wlp0s20f3, id 0
▸ Ethernet II, Src: Cisco_0c:9f:c1 (40:55:39:0c:9f:c1), Dst: IntelCor_08:29:9c (94:e7:0b:08:29:9c)
▸ Internet Protocol Version 4, Src: 10.10.2.2, Dst: 10.184.43.247
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49905
▾ Domain Name System (response)
    Transaction ID: 0x42b3
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 13
    Additional RRs: 10
  ▸ Queries
  ▾ Answers
    ▸ ping-ams1.online.net: type A, class IN, addr 163.172.208.7
  ▸ Authoritative nameservers
  ▸ Additional records
    [Request In: 14]
    [Time: 0.004637663 seconds]
```

Figure 27: DNS response for IP Address of ping-ams1.online.net

   (b) Terminal Response:

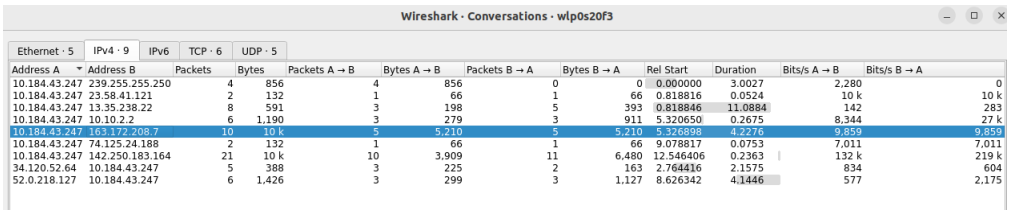


```
coolr@coolr-G5-5500:~$ ping -s 1465 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7) 1465(1493) bytes of data.
1473 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=1 ttl=53 time=273 ms
1473 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=2 ttl=53 time=296 ms
1473 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=3 ttl=53 time=218 ms
1473 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=4 ttl=53 time=346 ms
1473 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=5 ttl=53 time=266 ms

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 217.633/279.545/345.887/41.829 ms
```

Figure 28: Terminal for ping on ping-ams1.online.net Details

Answer for Questions asked:

(a) Total 5 packets are transferred from my host to destination ping-ams1.online.net (IP Address : **163.172.208.7**). And 5 packets are transferred from ping-ams1.online.net to my host(IP address: 10.184.43.247). (Figure 28)



Wireshark · Conversations · wlp0s20f3

Ethernet · 5 | IPv4 · 9 | IPv6 | TCP · 6 | UDP · 5

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.184.43.247	239.255.255.250	4	856	4	856	0	0	0.000000	3.0027	2,280	0
10.184.43.247	23.58.41.121	2	132	1	66	1	66	0.818816	0.0524	10 k	10 k
10.184.43.247	13.35.238.22	8	591	3	198	5	393	0.818846	11.0884	142	283
10.184.43.247	10.10.2.2	6	1,190	3	279	3	911	5.320650	0.2675	8,344	27 k
10.184.43.247	163.172.208.7	10	10 k	5	5,210	5	5,210	5.326898	4.2276	9,859	9,859
10.184.43.247	74.125.24.188	2	132	1	66	1	66	9.078817	0.0753	7,011	7,011
10.184.43.247	142.250.183.164	21	10 k	10	3,909	11	6,480	12.546406	0.2363	132 k	219 k
34.120.52.64	10.184.43.247	5	388	3	225	2	163	2.764416	2.1575	834	604
52.0.218.127	10.184.43.247	6	1,426	3	299	3	1,127	8.626342	4.1446	577	2,175

Figure 29: Packet transferred between my host and ping-ams1.online.net Details

(b)

$$Size\ of\ ping\ request = \frac{Total\ data\ transferred}{Total\ ping\ requests}$$

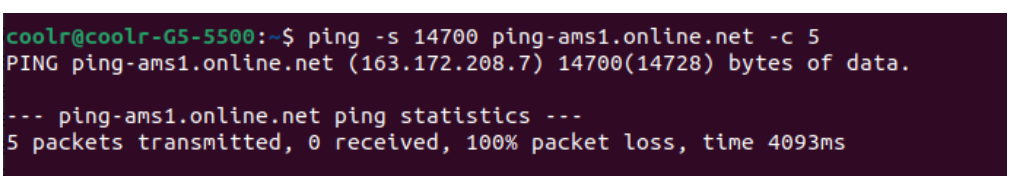
$$Size\ of\ ping\ request = \frac{5210}{5}$$

$$Size\ of\ ping\ request = 1042\ bytes$$

(c) None of the ping packets is fragmented in this case.

ping	Request fragmented	Response fragmented	sending time	packet size	Ping Response	Response Size	Data Size
1	No	No	5.326	1042	5.584	1042	992
2	No	No	6.328	1042	6.524	1042	992
3	No	No	7.329	1042	7.569	1042	992
4	No	No	8.330	1042	8.614	1042	992
5	No	No	9.331	1042	9.554	1042	992

2. After running command `ping -s 2500 ping-ams1.online.net -c 5` on the terminal and capturing packets in Wireshark.No response from the server for our ping. Output of terminal is as follow:

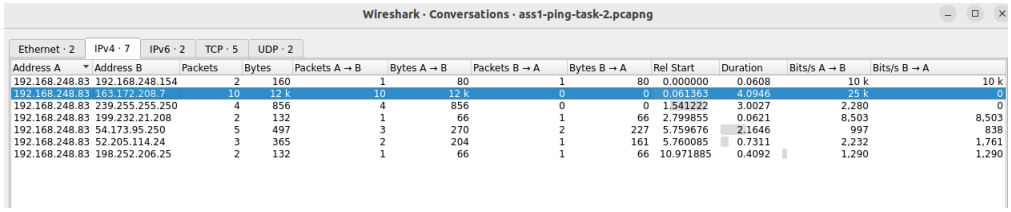


```
coolr@coolr-G5-5500:~$ ping -s 14700 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7) 14700(14728) bytes of data.

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4093ms
```

Figure 30: Terminal for ping on ping-ams1.online.net Details

Answer to asked questions:

(a) Total 10 packets are transferred from my host to destination ping-ams1.online.net (IP Address : **163.172.208.7**). And 0 packets received from ping-ams1.online.net to my host(IP address: 10.184.43.247). (Figure 29)



Wireshark · Conversations · ass1-ping-task-2.pcapng

Ethernet · 2 | IPv4 · 7 | IPv6 · 2 | TCP · 5 | UDP · 2

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.248.83	192.168.248.154	2	160	1	80	1	80	0.000000	0.0608	10 k	10 k
192.168.248.83	163.172.208.7	10	12 k	10	12 k	0	0	0.001153	4.0016	25 k	0
192.168.248.83	239.255.255.250	4	856	4	856	0	0	1.541222	3.0027	2,280	0
192.168.248.83	199.232.21.208	2	132	1	66	1	66	2.799855	0.0621	8,503	8,503
192.168.248.83	54.173.95.250	5	497	3	270	2	227	5.759676	2.1646	997	838
192.168.248.83	52.205.114.24	3	365	2	204	1	161	5.760085	0.7311	2,232	1,761
192.168.248.83	198.252.206.25	2	132	1	66	1	66	10.971885	0.4092	1,290	1,290

Figure 31: Packet transferred between my host and ping-ams1.online.net Details

(b)

$$Size\ of\ ping\ request = \frac{Total\ data\ transferred}{Total\ ping\ requests}$$

$$Size\ of\ ping\ request = \frac{12430}{5}$$

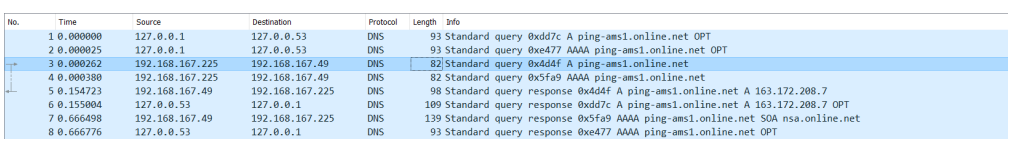
$$Size\ of\ ping\ request = 2586\ bytes$$

(c) Every packet is fragmented into 2 fragments in this case. But no response from the ping-ams1.online.net.

ping	frag.	no. of fragments	fragment No.	sending time	packet size	Any Response
1	Yes	2	1	0.000000	1514	No
1	Yes	2	2	0.000026	1062	No
2	Yes	2	1	1.022569	1514	No
2	Yes	2	2	1.022600	1062	No
3	Yes	2	1	2.050512	1514	No
3	Yes	2	2	2.050544	1062	No
4	Yes	2	1	3.070491	1514	No
4	Yes	2	2	3.070504	1062	No
5	Yes	2	1	4.094589	1514	No
5	Yes	2	2	4.096208	1062	No

2.e Traceroute Task

Command Run in Terminal : `traceroute -q 5 ping-ams1.online.net 1000` File Name:
As obtained from dns querry IP address of ping-asm1.online.net = 163.172.208.7.

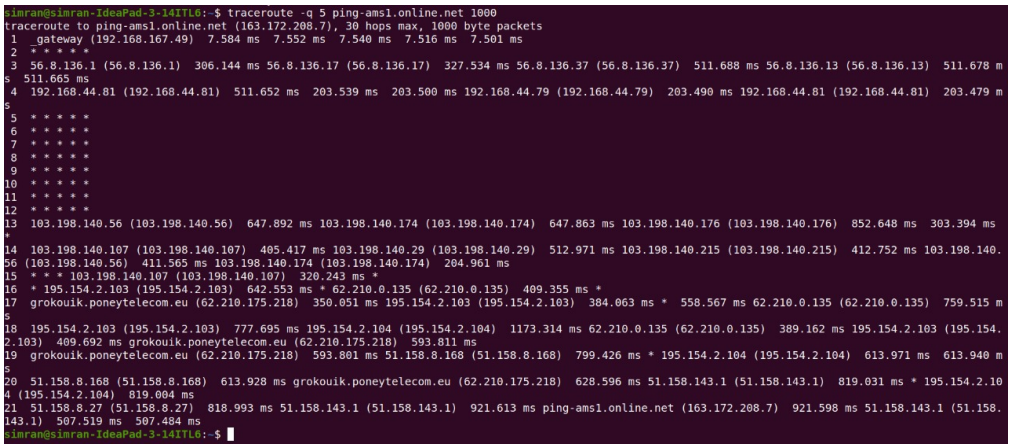


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.53	DNS	93	Standard query 0xdd7c A ping-ams1.online.net OPT
2	0.000025	127.0.0.1	127.0.0.53	DNS	93	Standard query 0xe477 AAAA ping-ams1.online.net OPT
3	0.000262	192.168.167.225	192.168.167.49	DNS	82	Standard query 0x4d4f A ping-ams1.online.net
4	0.000380	192.168.167.225	192.168.167.49	DNS	82	Standard query 0x5fa9 AAAA ping-ams1.online.net
5	0.154723	192.168.167.49	192.168.167.225	DNS	98	Standard query response 0x4d4f A ping-ams1.online.net A 163.172.208.7
6	0.155004	127.0.0.53	127.0.0.1	DNS	109	Standard query response 0xdd7c A ping-ams1.online.net A 163.172.208.7 OPT
7	0.666498	192.168.167.49	192.168.167.225	DNS	139	Standard query response 0x5fa9 AAAA ping-ams1.online.net SOA nsa.online.net
8	0.666776	127.0.0.53	127.0.0.1	DNS	93	Standard query response 0xe477 AAAA ping-ams1.online.net OPT

Figure 32: DNS querry and response of ip-address of ping-asm1.online.net

Answers:

1. 21 hops. As seen from terminal output. (see figure below)



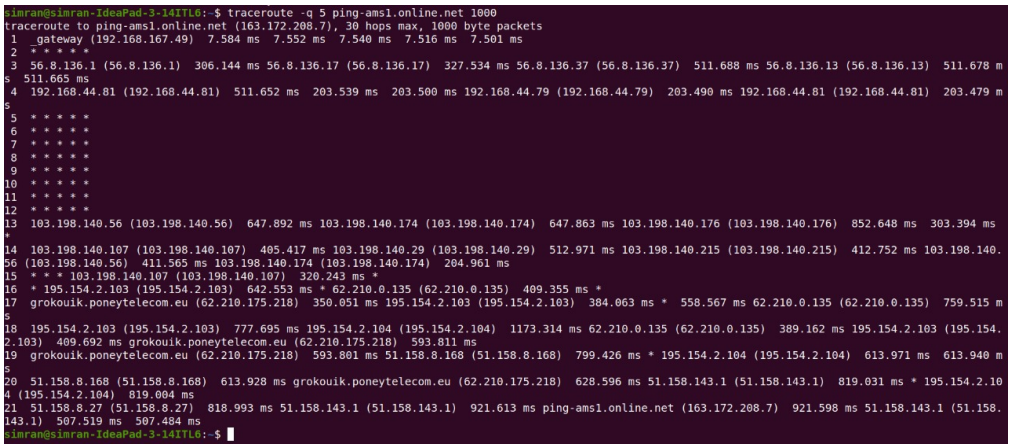
```
simran@simran-IdeaPad-3-14ITL6:~$ traceroute -q 5 ping-ams1.online.net 1000
traceroute to ping-ams1.online.net (163.172.208.7), 30 hops max, 1000 byte packets
 1  _gateway (192.168.167.49)  7.584 ms  7.552 ms  7.540 ms  7.516 ms  7.501 ms
 2  * * * * *
 3  56.8.136.1 (56.8.136.1)  306.144 ms 56.8.136.17 (56.8.136.17)  327.534 ms 56.8.136.37 (56.8.136.37)  511.688 ms 56.8.136.13 (56.8.136.13)  511.678 m
s  511.665 ms
 4  192.168.44.81 (192.168.44.81)  511.652 ms  203.539 ms  203.500 ms 192.168.44.79 (192.168.44.79)  203.490 ms 192.168.44.81 (192.168.44.81)  203.479 m
s
 5  * * * * *
 6  * * * * *
 7  * * * * *
 8  * * * * *
 9  * * * * *
10  * * * * *
11  * * * * *
12  * * * * *
13  103.198.140.56 (103.198.140.56)  647.892 ms 103.198.140.174 (103.198.140.174)  647.863 ms 103.198.140.176 (103.198.140.176)  852.648 ms  303.394 ms
*
14  103.198.140.107 (103.198.140.107)  405.417 ms 103.198.140.29 (103.198.140.29)  512.971 ms 103.198.140.215 (103.198.140.215)  412.752 ms 103.198.140.
56 (103.198.140.56)  411.565 ms 103.198.140.174 (103.198.140.174)  204.961 ms
15  * * * 103.198.140.107 (103.198.140.107)  320.243 ms *
16  * 195.154.2.103 (195.154.2.103)  642.553 ms * 62.210.0.135 (62.210.0.135)  409.355 ms *
17  grokouik.poneytelecom.eu (62.210.175.218)  350.051 ms 195.154.2.103 (195.154.2.103)  384.063 ms *  558.567 ms 62.210.0.135 (62.210.0.135)  759.515 m
s
18  195.154.2.103 (195.154.2.103)  777.695 ms 195.154.2.104 (195.154.2.104)  1173.314 ms 62.210.0.135 (62.210.0.135)  389.162 ms 195.154.2.103 (195.154.
2.103)  409.692 ms grokouik.poneytelecom.eu (62.210.175.218)  593.811 ms
19  grokouik.poneytelecom.eu (62.210.175.218)  593.801 ms 51.158.8.168 (51.158.8.168)  799.426 ms * 195.154.2.104 (195.154.2.104)  613.971 ms  613.940 m
s
20  51.158.8.168 (51.158.8.168)  613.928 ms grokouik.poneytelecom.eu (62.210.175.218)  628.596 ms 51.158.143.1 (51.158.143.1)  819.031 ms * 195.154.2.10
4 (195.154.2.104)  819.004 ms
21  51.158.8.27 (51.158.8.27)  818.993 ms 51.158.143.1 (51.158.143.1)  921.613 ms ping-ams1.online.net (163.172.208.7)  921.598 ms 51.158.143.1 (51.158.
143.1)  507.519 ms  507.484 ms
simran@simran-IdeaPad-3-14ITL6:~$
```

Figure 33: Terminal output on running `traceroute -q 5 ping-ams1.online.net 1000`

2. Filter: `ip.addr==163.172.208.7`. Total packets: 162 packet are exchanged in this traceroute communication. Packets sent from client to remote machine (server/router)(ip.src==192.168.167.225): 109. Packets sent from the remote machine (hop/server/router) to the local client(ip.dst==192.168.167.225): 53

   Client IP Adress: 192.168.167.225

server/host IP address	packets sent from client to server	packets sent from server to client
51.158.8.27	0	1
51.158.8.168	0	2
51.158.143.1	0	5
51.158.143.3	0	2
56.8.136.1	0	1
56.8.136.13	0	2
56.8.136.17	0	1
56.8.136.37	0	1
62.210.0.135	0	3
62.210.175.218	0	4
103.198.140.29	0	1
103.198.140.56	0	2
103.198.140.107	0	2
103.198.140.174	0	2
103.198.140.176	0	2
103.198.140.215	0	1
163.172.208.7	109	2
192.168.44.79	0	1
192.168.44.81	0	4
192.168.167.49	0	5
195.154.2.103	0	5
195.154.2.104	0	4



```
simran@simran-IdeaPad-3-14ITL6:~$ traceroute -q 5 ping-ams1.online.net 1000
traceroute to ping-ams1.online.net (163.172.208.7), 30 hops max, 1000 byte packets
 1  _gateway (192.168.167.49)  7.584 ms  7.552 ms  7.540 ms  7.516 ms  7.501 ms
 2  * * * * *
 3  56.8.136.1 (56.8.136.1)  306.144 ms 56.8.136.17 (56.8.136.17)  327.534 ms 56.8.136.37 (56.8.136.37)  511.688 ms 56.8.136.13 (56.8.136.13)  511.678 m
s  511.665 ms
 4  192.168.44.81 (192.168.44.81)  511.652 ms  203.539 ms  203.500 ms 192.168.44.79 (192.168.44.79)  203.490 ms 192.168.44.81 (192.168.44.81)  203.479 m
s
 5  * * * * *
 6  * * * * *
 7  * * * * *
 8  * * * * *
 9  * * * * *
10  * * * * *
11  * * * * *
12  * * * * *
13  103.198.140.56 (103.198.140.56)  647.892 ms 103.198.140.174 (103.198.140.174)  647.863 ms 103.198.140.176 (103.198.140.176)  852.648 ms  303.394 ms
*
14  103.198.140.107 (103.198.140.107)  405.417 ms 103.198.140.29 (103.198.140.29)  512.971 ms 103.198.140.215 (103.198.140.215)  412.752 ms 103.198.140.
56 (103.198.140.56)  411.565 ms 103.198.140.174 (103.198.140.174)  204.961 ms
15  * * * 103.198.140.107 (103.198.140.107)  320.243 ms *
16  * 195.154.2.103 (195.154.2.103)  642.553 ms * 62.210.0.135 (62.210.0.135)  409.355 ms *
17  grokouik.poneytelecom.eu (62.210.175.218)  350.051 ms 195.154.2.103 (195.154.2.103)  384.063 ms *  558.567 ms 62.210.0.135 (62.210.0.135)  759.515 m
s
18  195.154.2.103 (195.154.2.103)  777.695 ms 195.154.2.104 (195.154.2.104)  1173.314 ms 62.210.0.135 (62.210.0.135)  389.162 ms 195.154.2.103 (195.154.
2.103)  409.692 ms grokouik.poneytelecom.eu (62.210.175.218)  593.811 ms
19  grokouik.poneytelecom.eu (62.210.175.218)  593.801 ms 51.158.8.168 (51.158.8.168)  799.426 ms * 195.154.2.104 (195.154.2.104)  613.971 ms  613.940 m
s
20  51.158.8.168 (51.158.8.168)  613.928 ms grokouik.poneytelecom.eu (62.210.175.218)  628.596 ms 51.158.143.1 (51.158.143.1)  819.031 ms * 195.154.2.10
4 (195.154.2.104)  819.004 ms
21  51.158.8.27 (51.158.8.27)  818.993 ms 51.158.143.1 (51.158.143.1)  921.613 ms ping-ams1.online.net (163.172.208.7)  921.598 ms 51.158.143.1 (51.158.
143.1)  507.519 ms  507.484 ms
simran@simran-IdeaPad-3-14ITL6:~$
```

Figure 34: Conversation of filtered data with filter `ip.dst==192.168.167.225`

3. (a) **Fields that changes:** Destination Port No. , Src Port No. , Time to live , Checksum(decription key), etc.

   (b) **Field that doesn't change:** Size of datagram, destination IP address, Data carried by datagram , IP protocol used(IPv4 and UDP are used in this case) etc.

   (c) **Size of datagram** must remain same because in commandline we had fixed packet size to 1000. **Destination IP Address** must also remain same because destination ip can't change in between. Once we get destination IP address from dns querry, we send all packets for same destination. **Client address** will also remain same.

   (d) **Time to live** must change to trace the route and it must increase every time. Because when datagram is sent from one router to another it's ttl value is decreased by 1. If ttl became 0 then icmp error message is sent to the client and packet is dropped.Let path from client to destination is **client − router1 − router2 − router 3 − destination**. If we want to trace route then first we sent packet with **ttl=1** and get error message from router1 , next time we send packet with **ttl=2** and get error message from router 2 and so on. For tracing the route we should start with **ttl=1** and increase it by 1 every time until we reach destination.

   (e) Checksum will be obviously different for every datagram as it is used for decription of data.

```
Internet Protocol Version 4, Src: 192.168.167.225, Dst: 163.172.208.7
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1000
    Identification: 0x6898 (26776)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 2
        [Expert Info (Note/Sequence): "Time To Live" only 2]
    Protocol: UDP (17)
    Header Checksum: 0x702f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.167.225
    Destination Address: 163.172.208.7
User Datagram Protocol, Src Port: 55982, Dst Port: 33439
    Source Port: 55982
    Destination Port: 33439
        [Expert Info (Chat/Sequence): Possible traceroute: hop #2, attempt #2]
    Length: 980
    Checksum: 0x4a61 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (972 bytes)
Data (972 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f60616263…
    [Length: 972]
```

Figure 35: Datagram (Highlighted with **Green:** field that don't change,Highlighted with **Blue:** field that change)