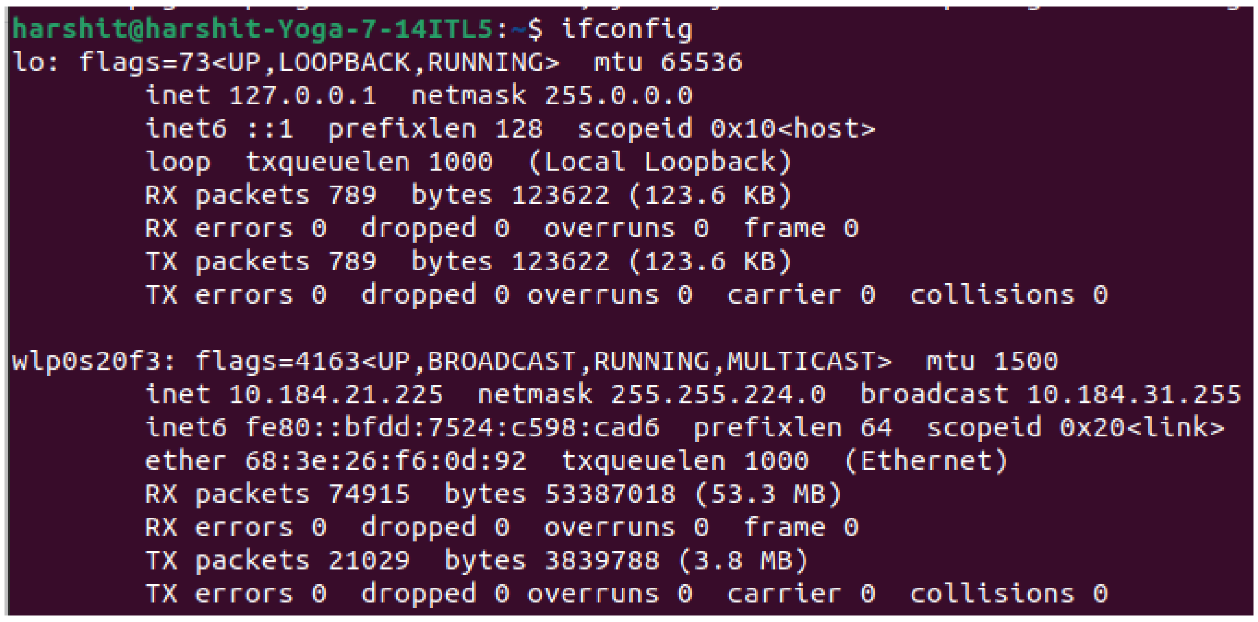
COL334 - Assignment 1 - Harshit Mawandia - 2020CS10348

Part 1 : IP address of local machine:

IP address changes on connecting to different service providers

1.

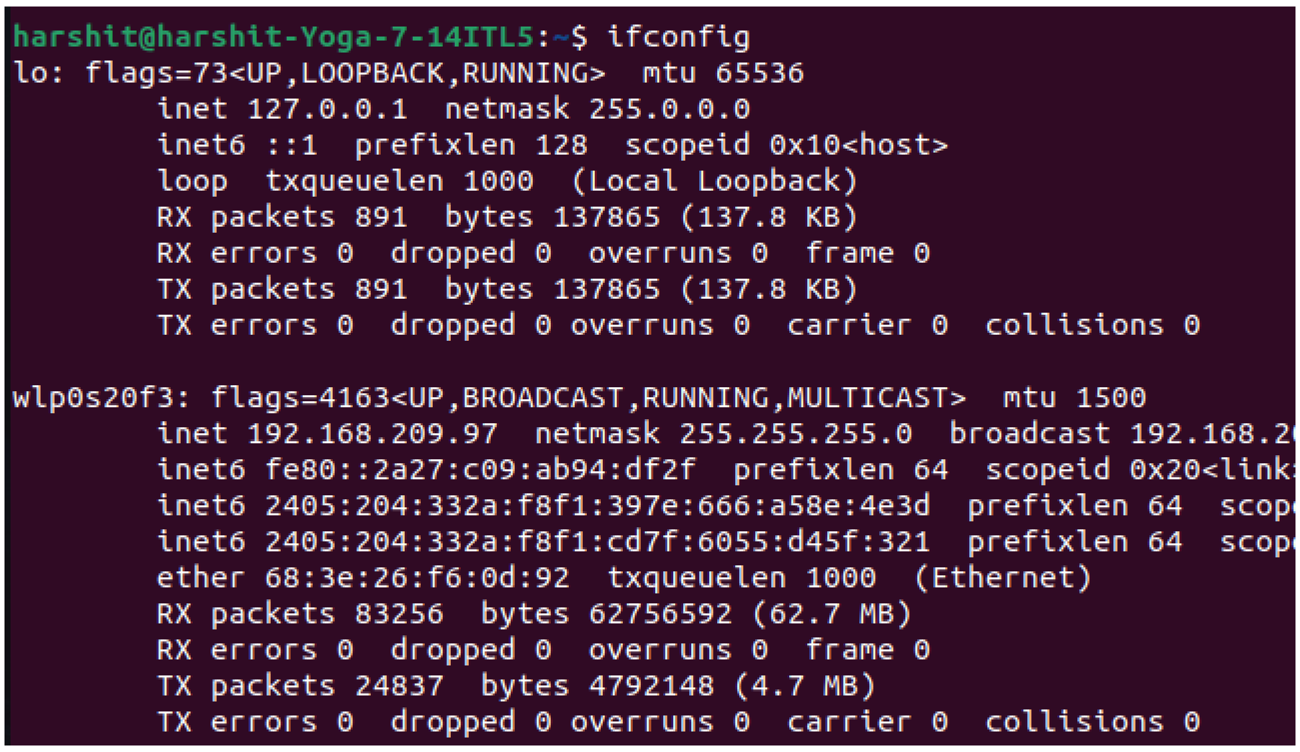
inet 10.184.21.225
inet6 fe80::bfdd:7524:c598:cad6



```
harshit@harshit-Yoga-7-14ITL5:~$ 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 789  bytes 123622 (123.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 789  bytes 123622 (123.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.184.21.225  netmask 255.255.224.0  broadcast 10.184.31.255
        inet6 fe80::bfdd:7524:c598:cad6  prefixlen 64  scopeid 0x20<link>
        ether 68:3e:26:f6:0d:92  txqueuelen 1000  (Ethernet)
        RX packets 74915  bytes 53387018 (53.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21029  bytes 3839788 (3.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.

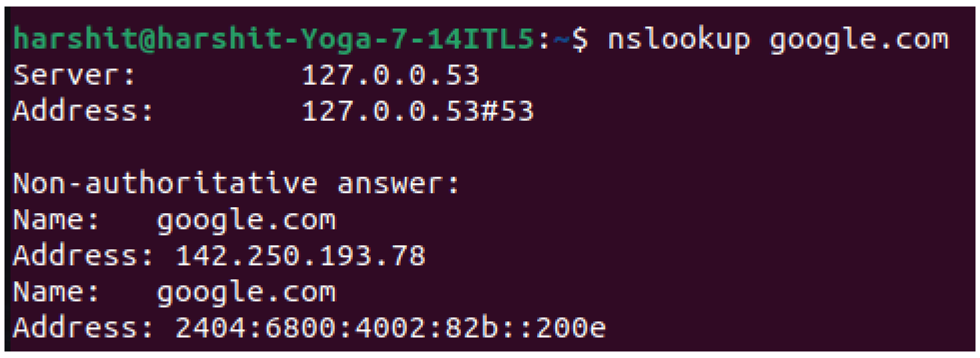
inet 192.168.209.97
inet6 fe80::2a27:c09:ab94:df2f



```
harshit@harshit-Yoga-7-14ITL5:~$ 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 891  bytes 137865 (137.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 891  bytes 137865 (137.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.209.97  netmask 255.255.255.0  broadcast 192.168.2
        inet6 fe80::2a27:c09:ab94:df2f  prefixlen 64  scopeid 0x20<link
        inet6 2405:204:332a:f8f1:397e:666:a58e:4e3d  prefixlen 64  scop
        inet6 2405:204:332a:f8f1:cd7f:6055:d45f:321  prefixlen 64  scop
        ether 68:3e:26:f6:0d:92  txqueuelen 1000  (Ethernet)
        RX packets 83256  bytes 62756592 (62.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24837  bytes 4792148 (4.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

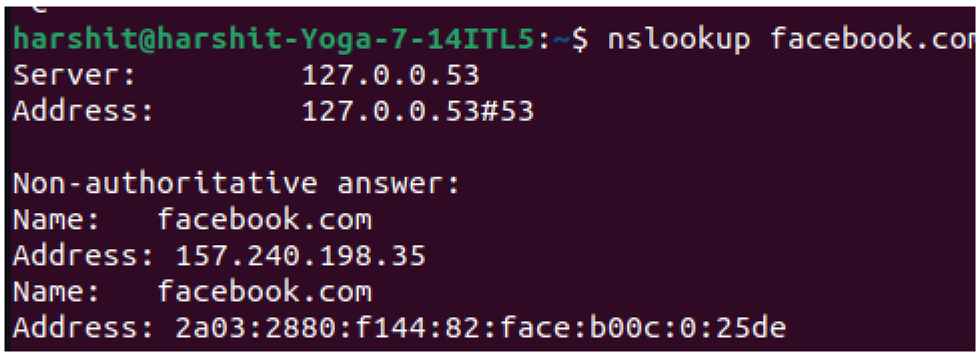
2.

a. IP of google.com



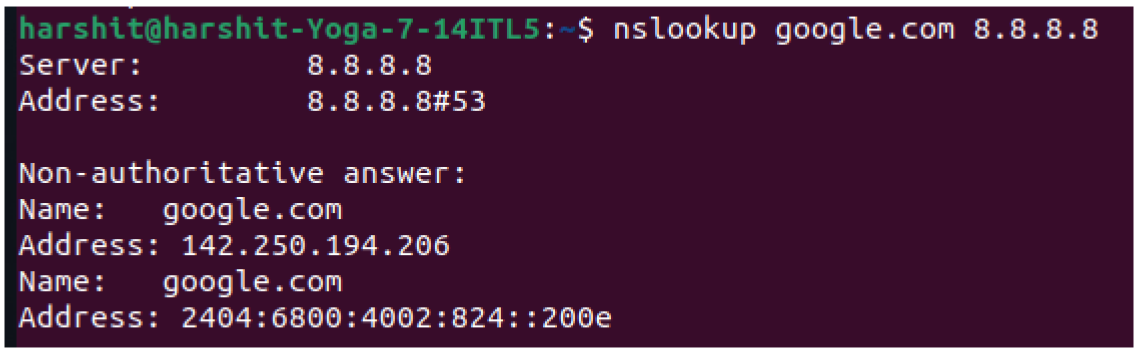
```
harshit@harshit-Yoga-7-14ITL5:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.193.78
Name:   google.com
Address: 2404:6800:4002:82b::200e
```

b. IP of facebook.com



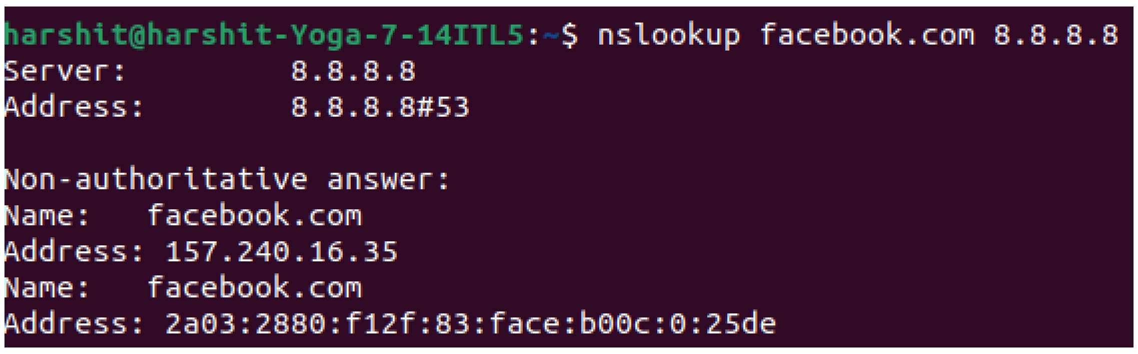
```
harshit@harshit-Yoga-7-14ITL5:~$ nslookup facebook.co
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   facebook.com
Address: 157.240.198.35
Name:   facebook.com
Address: 2a03:2880:f144:82:face:b00c:0:25de
```

c. IP of google.com from DNS 8.8.8.8



```
harshit@harshit-Yoga-7-14ITL5:~$ nslookup google.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.194.206
Name:   google.com
Address: 2404:6800:4002:824::200e
```

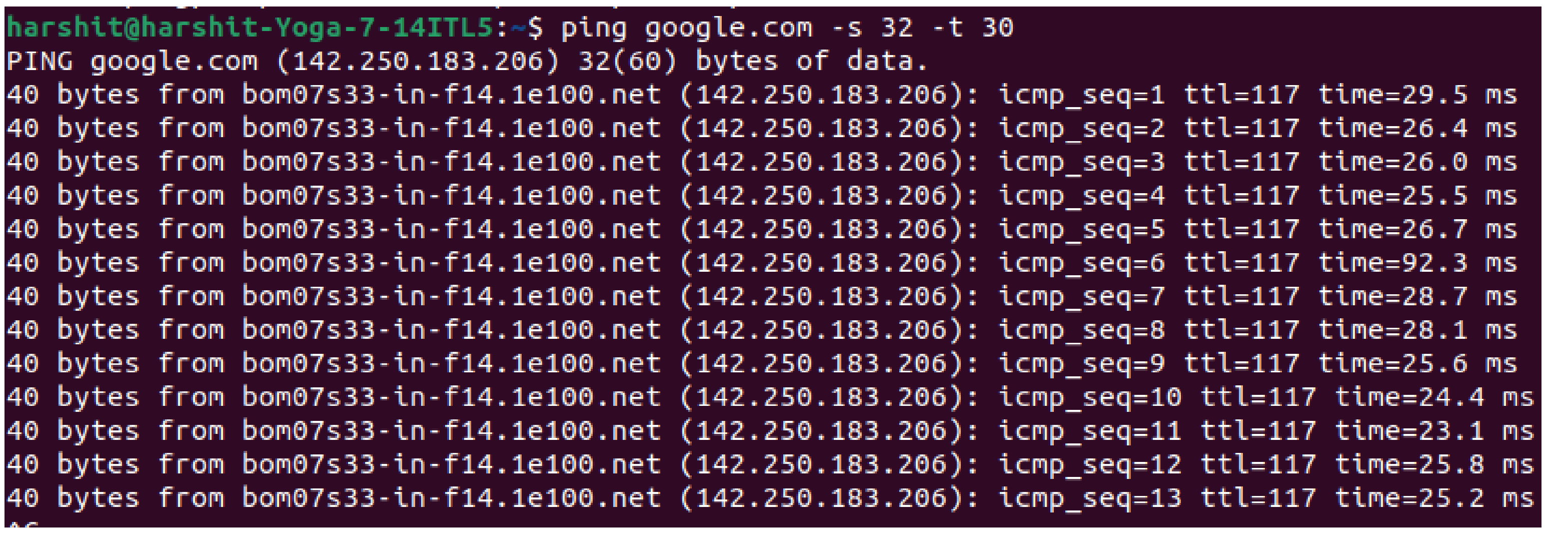
d. IP of facebook from DNS 8.8.8.8



```
harshit@harshit-Yoga-7-14ITL5:~$ nslookup facebook.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   facebook.com
Address: 157.240.16.35
Name:   facebook.com
Address: 2a03:2880:f12f:83:face:b00c:0:25de
```

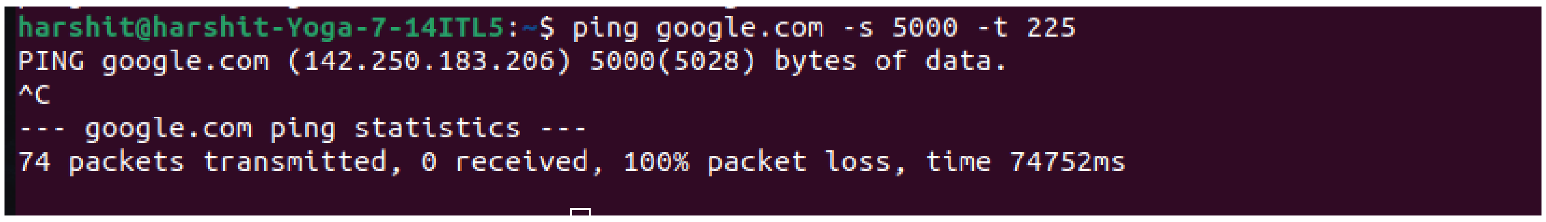
3. Pinging with different packet size and ttl

a. Size 32 & ttl 30



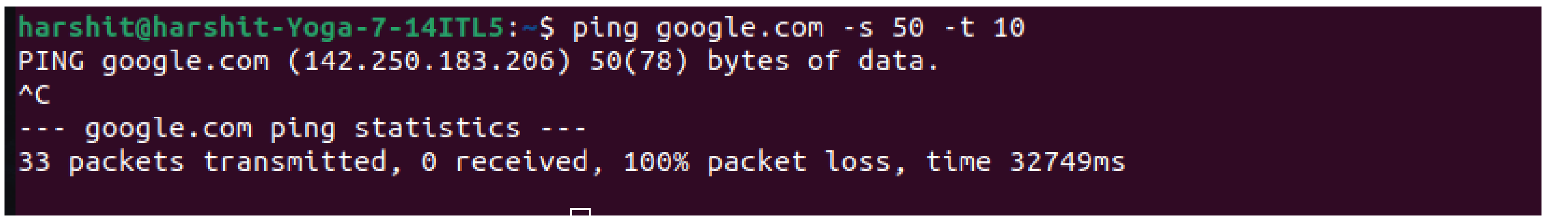
```
harshit@harshit-Yoga-7-14ITL5:~$ ping google.com -s 32 -t 30
PING google.com (142.250.183.206) 32(60) bytes of data.
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=1 ttl=117 time=29.5 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=2 ttl=117 time=26.4 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=3 ttl=117 time=26.0 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=4 ttl=117 time=25.5 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=5 ttl=117 time=26.7 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=6 ttl=117 time=92.3 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=7 ttl=117 time=28.7 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=8 ttl=117 time=28.1 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=9 ttl=117 time=25.6 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=10 ttl=117 time=24.4 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=11 ttl=117 time=23.1 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=12 ttl=117 time=25.8 ms
40 bytes from bom07s33-in-f14.1e100.net (142.250.183.206): icmp_seq=13 ttl=117 time=25.2 ms
```

b. Size 5000 & ttl 255



```
harshit@harshit-Yoga-7-14ITL5:~$ ping google.com -s 5000 -t 225
PING google.com (142.250.183.206) 5000(5028) bytes of data.
^C
--- google.com ping statistics ---
74 packets transmitted, 0 received, 100% packet loss, time 74752ms
```

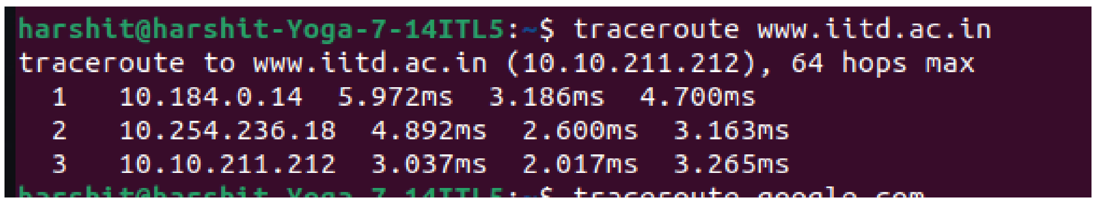
c. Size 50 & ttl 10



```
harshit@harshit-Yoga-7-14ITL5:~$ ping google.com -s 50 -t 10
PING google.com (142.250.183.206) 50(78) bytes of data.
^C
--- google.com ping statistics ---
33 packets transmitted, 0 received, 100% packet loss, time 32749ms
```

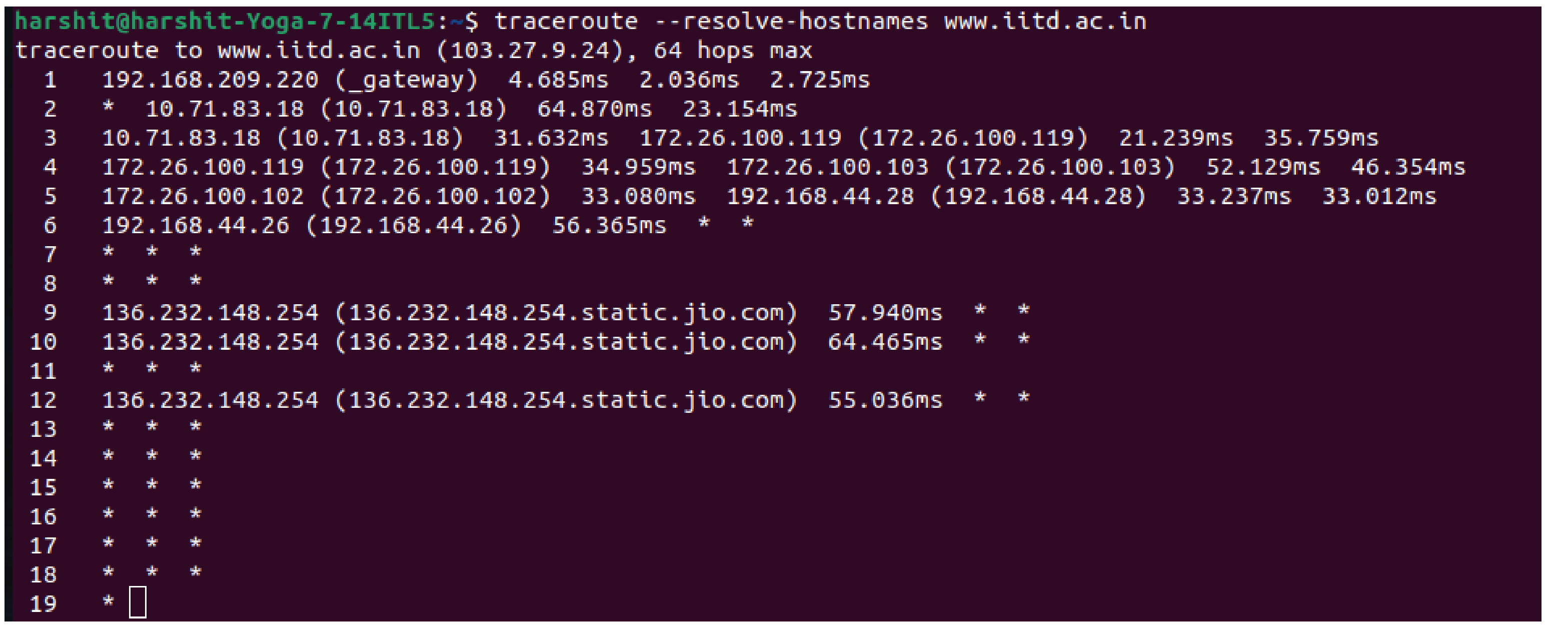
4. Traceroute to www.iitd.ac.in

a.



```
harshit@harshit-Yoga-7-14ITL5:~$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 64 hops max
  1   10.184.0.14  5.972ms  3.186ms  4.700ms
  2   10.254.236.18  4.892ms  2.600ms  3.163ms
  3   10.10.211.212  3.037ms  2.017ms  3.265ms
harshit@harshit-Yoga-7-14ITL5:~$ traceroute google.com
```

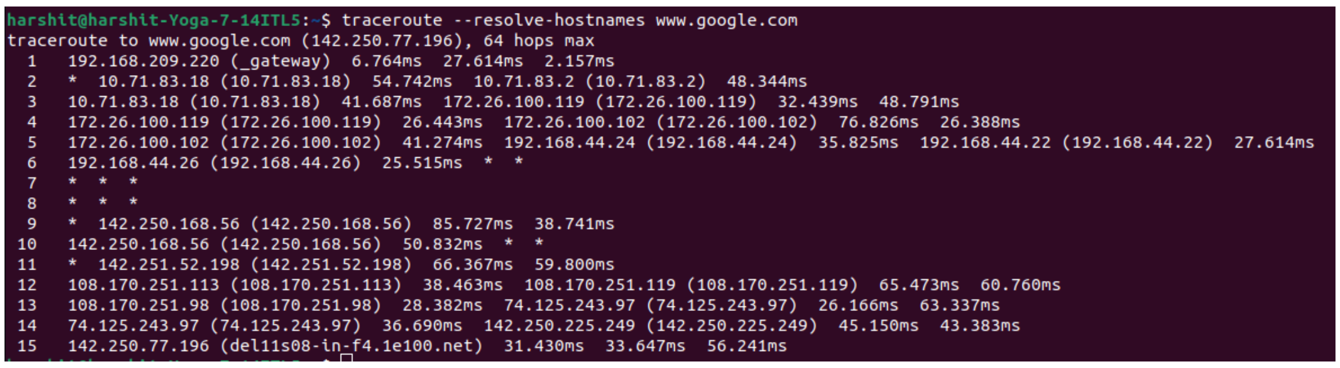
b.



```
harshit@harshit-Yoga-7-14ITL5:~$ traceroute --resolve-hostnames www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.209.220 (_gateway)  4.685ms  2.036ms  2.725ms
  2   *  10.71.83.18 (10.71.83.18)  64.870ms  23.154ms
  3   10.71.83.18 (10.71.83.18)  31.632ms  172.26.100.119 (172.26.100.119)  21.239ms  35.759ms
  4   172.26.100.119 (172.26.100.119)  34.959ms  172.26.100.103 (172.26.100.103)  52.129ms  46.354ms
  5   172.26.100.102 (172.26.100.102)  33.080ms  192.168.44.28 (192.168.44.28)  33.237ms  33.012ms
  6   192.168.44.26 (192.168.44.26)  56.365ms  *  *
  7   *  *  *
  8   *  *  *
  9   136.232.148.254 (136.232.148.254.static.jio.com)  57.940ms  *  *
 10   136.232.148.254 (136.232.148.254.static.jio.com)  64.465ms  *  *
 11   *  *  *
 12   136.232.148.254 (136.232.148.254.static.jio.com)  55.036ms  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *
```

ISP blocked the route to iitd.ac.in

c.



```
harshit@harshit-Yoga-7-14ITL5:~$ traceroute --resolve-hostnames www.google.com
traceroute to www.google.com (142.250.77.196), 64 hops max
  1   192.168.209.220 (_gateway)  6.764ms  27.614ms  2.157ms
  2   *  10.71.83.18 (10.71.83.18)  54.742ms  10.71.83.2 (10.71.83.2)  48.344ms
  3   10.71.83.18 (10.71.83.18)  41.687ms  172.26.100.119 (172.26.100.119)  32.439ms  48.791ms
  4   172.26.100.119 (172.26.100.119)  26.443ms  172.26.100.102 (172.26.100.102)  76.826ms  26.388ms
  5   172.26.100.102 (172.26.100.102)  41.274ms  192.168.44.24 (192.168.44.24)  35.825ms  192.168.44.22 (192.168.44.22)  27.614ms
  6   192.168.44.26 (192.168.44.26)  25.515ms  *  *
  7   *  *  *
  8   *  *  *
  9   *  142.250.168.56 (142.250.168.56)  85.727ms  38.741ms
 10   142.250.168.56 (142.250.168.56)  50.832ms  *  *
 11   *  142.251.52.198 (142.251.52.198)  66.367ms  59.800ms
 12   108.170.251.113 (108.170.251.113)  38.463ms  108.170.251.119 (108.170.251.119)  65.473ms  60.760ms
 13   108.170.251.98 (108.170.251.98)  28.382ms  74.125.243.97 (74.125.243.97)  26.166ms  63.337ms
 14   74.125.243.97 (74.125.243.97)  36.690ms  142.250.225.249 (142.250.225.249)  45.150ms  43.383ms
 15   142.250.77.196 (del11s08-in-f4.1e100.net)  31.430ms  33.647ms  56.241ms
```

Traceroute to google.com

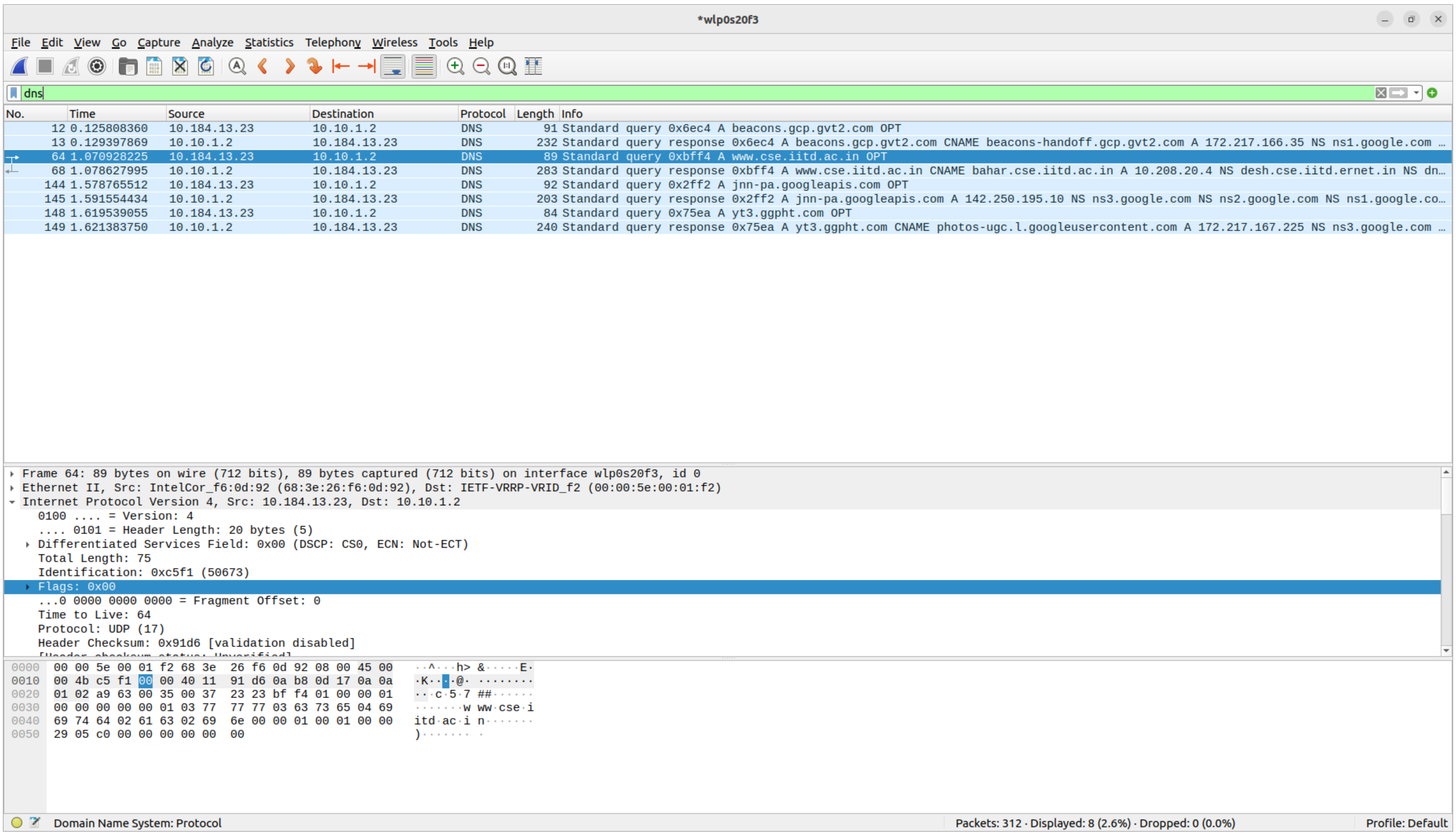
We can force traceroute to use IPv4 by using -4 flag

We can also use the -w tag to increase waiting time for a response or we can send a smaller data packet.

Packet Analysis

Task 1 - DNS Task

1. The DNS query is sent over UDP



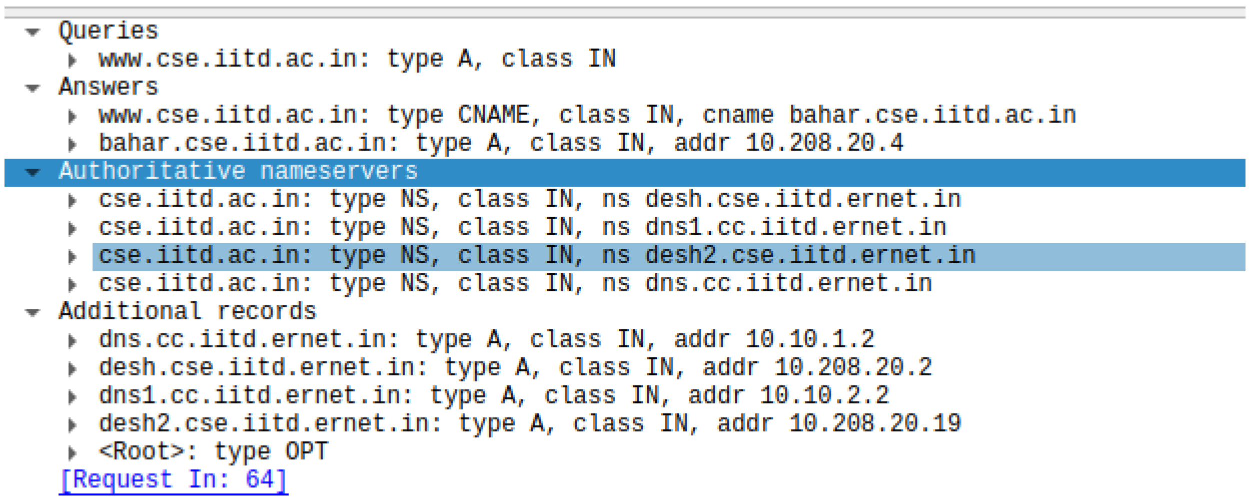
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
No.    Time          Source          Destination     Protocol Length Info
    12 0.125808360   10.184.13.23    10.10.1.2       DNS       91 Standard query 0x6ec4 A beacons.gcp.gvt2.com OPT
    13 0.129397869   10.10.1.2       10.184.13.23    DNS      232 Standard query response 0x6ec4 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.166.35 NS ns1.google.com …
    64 1.070928225   10.184.13.23    10.10.1.2       DNS       89 Standard query 0xbff4 A www.cse.iitd.ac.in OPT
    68 1.078627995   10.10.1.2       10.184.13.23    DNS      283 Standard query response 0xbff4 A www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in A 10.208.20.4 NS desh.cse.iitd.ernet.in NS dn…
   144 1.578765512   10.184.13.23    10.10.1.2       DNS       92 Standard query 0x2ff2 A jnn-pa.googleapis.com OPT
   145 1.591554434   10.10.1.2       10.184.13.23    DNS      203 Standard query response 0x2ff2 A jnn-pa.googleapis.com A 142.250.195.10 NS ns3.google.com NS ns2.google.com NS ns1.google.co…
   148 1.619539055   10.184.13.23    10.10.1.2       DNS       84 Standard query 0x75ea A yt3.ggpht.com OPT
   149 1.621383750   10.10.1.2       10.184.13.23    DNS      240 Standard query response 0x75ea A yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com A 172.217.167.225 NS ns3.google.com …

Frame 64: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: IntelCor_f6:0d:92 (68:3e:26:f6:0d:92), Dst: IETF-VRRP-VRID_f2 (00:00:5e:00:01:f2)
Internet Protocol Version 4, Src: 10.184.13.23, Dst: 10.10.1.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 75
    Identification: 0xc5f1 (50673)
  Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x91d6 [validation disabled]
    [Header checksum status: Unverified]

0000  00 00 5e 00 01 f2 68 3e  26 f6 0d 92 08 00 45 00   ··^···h> &·····E·
0010  00 4b c5 f1 00 00 40 11  91 d6 0a b8 0d 17 0a 0a   ·K····@· ········
0020  01 02 a9 63 00 35 00 37  23 23 bf f4 01 00 00 01   ···c·5·7 ##······
0030  00 00 00 00 00 01 03 77  77 77 03 63 73 65 04 69   ·······w ww·cse·i
0040  69 74 64 02 61 63 02 69  6e 00 00 01 00 01 00 00   itd·ac·i n·······
0050  29 05 c0 00 00 00 00 00  00                        )······· ·
```

Domain Name System: Protocol
Packets: 312 · Displayed: 8 (2.6%) · Dropped: 0 (0.0%)
Profile: Default

2. 8 queries are sent from host to the DNS server

3. There is 2 Answer RR, while there are 4 Authority RRs and 5 Additional RRs.



```
Queries
    www.cse.iitd.ac.in: type A, class IN
Answers
    www.cse.iitd.ac.in: type CNAME, class IN, cname bahar.cse.iitd.ac.in
    bahar.cse.iitd.ac.in: type A, class IN, addr 10.208.20.4
Authoritative nameservers
    cse.iitd.ac.in: type NS, class IN, ns desh.cse.iitd.ernet.in
    cse.iitd.ac.in: type NS, class IN, ns dns1.cc.iitd.ernet.in
    cse.iitd.ac.in: type NS, class IN, ns desh2.cse.iitd.ernet.in
    cse.iitd.ac.in: type NS, class IN, ns dns.cc.iitd.ernet.in
Additional records
    dns.cc.iitd.ernet.in: type A, class IN, addr 10.10.1.2
    desh.cse.iitd.ernet.in: type A, class IN, addr 10.208.20.2
    dns1.cc.iitd.ernet.in: type A, class IN, addr 10.10.2.2
    desh2.cse.iitd.ernet.in: type A, class IN, addr 10.208.20.19
    <Root>: type OPT
[Request In: 64]
```

4. bahar.cse.iitd.ac.in(10.208.20.4) replies with IP addresses. Some additional RRs also reply with IP addresses:
    a. Name: dns.cc.iitd.ernet.in, Address:10.10.1.2
    b. Name: desh.cse.iitd.ernet.in, Address: 10.208.20.2
    c. Name: dns1.cc.iitd.ernet.in, Address: 10.10.2.2
    d. Name: desh2.cse.iitd.ernet.in, Address: 10.208.20.19

5. No, all DNS servers do not respond.

6.

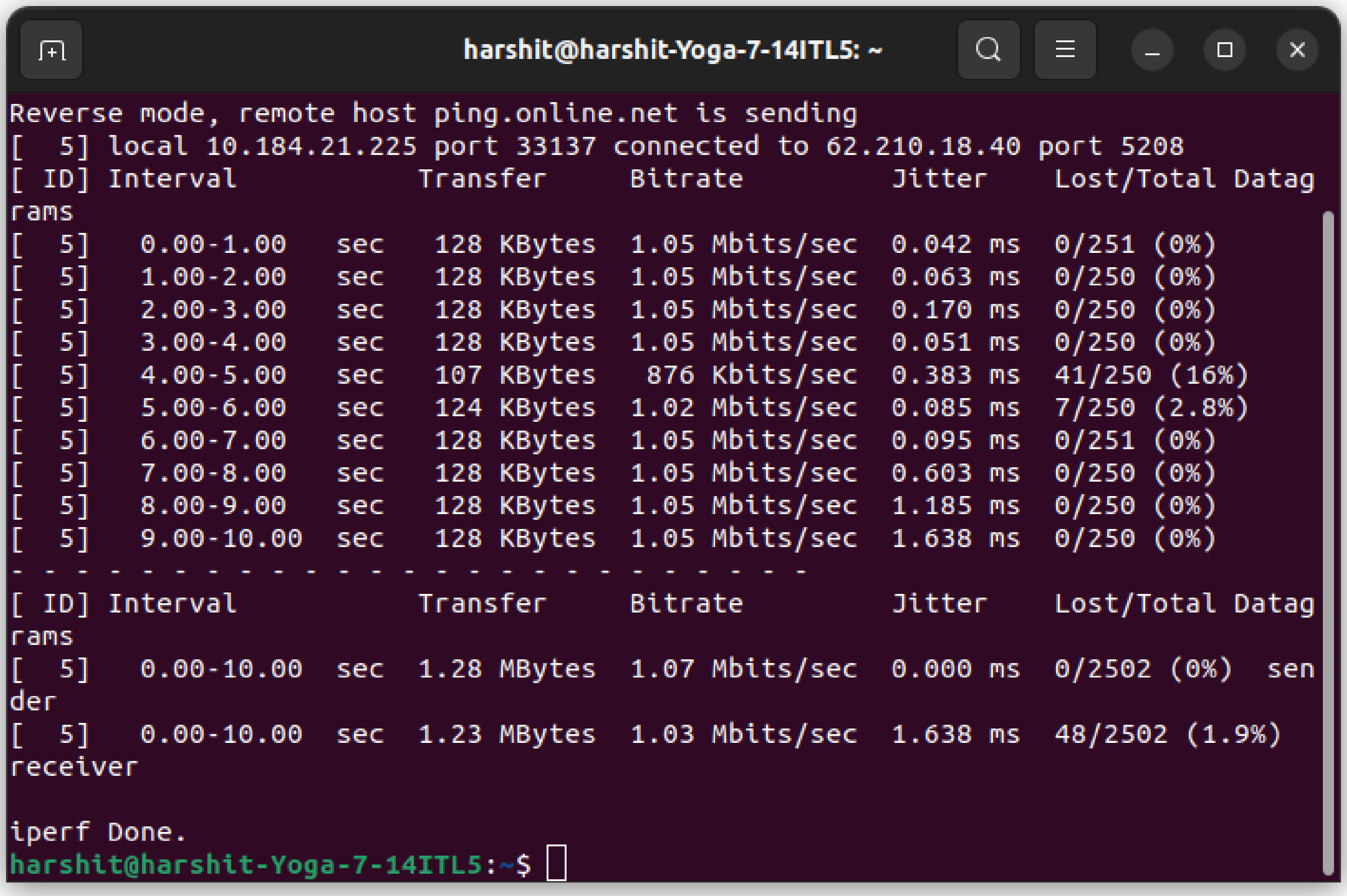
Domain Name	IP address	TTL	Query/Answer	Type	Value
www.cse.iitd.ac.in			Query	A	www.cse.iitd.ac.in
www.cse.iitd.ac.in		3600	Answer	CNAME	www.cse.iitd.ac.in
www.cse.iitd.ac.in	10.208.20.4	3600	Answer	A	bahar.cse.iitd.ac.in
www.cse.iitd.ac.in	10.10.1.2	3600	Answer	NS	dns.cc.iitd.ernet.in

www.cse.iitd.ac.in	10.208.20.2	3600	Answer	NS	desh.cse.iitd.ernet.in
www.cse.iitd.ac.in	10.10.2.2	3600	Answer	NS	dns1.cc.iitd.ernet.in
www.cse.iitd.ac.in	10.208.20.19	3600	Answer	NS	desh2.cse.iitd.ernet.in

Task 2 - Iperf Task

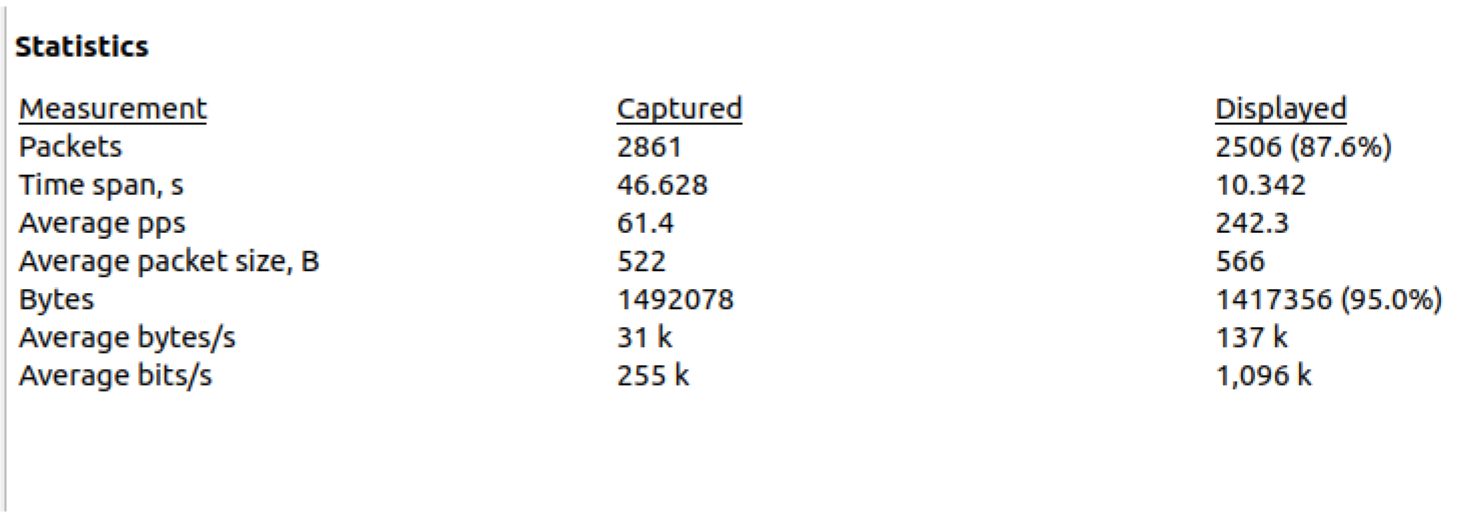
1. 2506 UDP packets
2. Remote server 62.210.18.40 is sending bulk data to the local client 10.184.21.225. Average size of the packet is 566 Bytes.
3. 2504 packets of size 566 bytes each starting from time 16.767 sec to time 26.910 sec, which gives 566*2504/(26.91-16.767) = 139728 bytes/sec = 136.45 kB/sec = 0.133 mB/sec = 1.06 mbits/sec

   We can verify by the iperf terminal



```
Reverse mode, remote host ping.online.net is sending
[  5] local 10.184.21.225 port 33137 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datag
rams
[  5]   0.00-1.00   sec   128 KBytes  1.05 Mbits/sec  0.042 ms  0/251 (0%)
[  5]   1.00-2.00   sec   128 KBytes  1.05 Mbits/sec  0.063 ms  0/250 (0%)
[  5]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec  0.170 ms  0/250 (0%)
[  5]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  0.051 ms  0/250 (0%)
[  5]   4.00-5.00   sec   107 KBytes   876 Kbits/sec  0.383 ms  41/250 (16%)
[  5]   5.00-6.00   sec   124 KBytes  1.02 Mbits/sec  0.085 ms  7/250 (2.8%)
[  5]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec  0.095 ms  0/251 (0%)
[  5]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec  0.603 ms  0/250 (0%)
[  5]   8.00-9.00   sec   128 KBytes  1.05 Mbits/sec  1.185 ms  0/250 (0%)
[  5]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec  1.638 ms  0/250 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datag
rams
[  5]   0.00-10.00  sec  1.28 MBytes  1.07 Mbits/sec  0.000 ms  0/2502 (0%)  sen
der
[  5]   0.00-10.00  sec  1.23 MBytes  1.03 Mbits/sec  1.638 ms  48/2502 (1.9%)
receiver

iperf Done.
harshit@harshit-Yoga-7-14ITL5:~$ 
```

By Capture files properties:



Statistics

Measurement	Captured	Displayed
Packets	2861	2506 (87.6%)
Time span, s	46.628	10.342
Average pps	61.4	242.3
Average packet size, B	522	566
Bytes	1492078	1417356 (95.0%)
Average bytes/s	31 k	137 k
Average bits/s	255 k	1,096 k

There is a very small difference in the result between the calculated value and the values by iperf Terminal and the Capture file properties on wireshark which may be due to the fact that some packets are lost, which can be seen on the iperf terminal, which gives us a larger calculated value. Also, header files have some size which do not appear on the iperf terminal.

Task 3 - HTTP Task

1. No. of HTTP/2 packets - 9
   No. of HTTP/1.1 packets - 1
2. 4
3. HTTP/1.1 uses textual format while HTTP/2 works by using a binary protocol and stream with an id.

Task 4 - Ping Task

1. 15 IP packets are exchanged in the communication between your host(10.184.22.243) and the remote server representing ping-ams1.online.net(163.172.208.7). 10 of them are IPv4 packets while 5 are ICMP.
2. Each IPv4 packet is of size 1514 Bytes out of which data is 1480 Bytes while ICMP is of 532 Bytes each. The IPv4 packets are fragmented and the total size of each ping sent is 3528 bytes as seen in the PING terminal. The total length of Ping request as seen on wireshark is 3492 Bytes each.
3.

No.	source	dest	size	fragmented	fragment part no	time taken to send	Response
1	10.184.22.243	163.172.208.7	1480	Yes	1/3	0.000023256	
2	10.184.22.243	163.172.208.7	1480	Yes	2/3	0.000003545	
3	10.184.22.243	163.172.208.7	532	No	3/3	1.019716509	No Response Recieved
4	10.184.22.243	163.172.208.7	1480	Yes	1/3	0.000025516	
5	10.184.22.243	163.172.208.7	1480	Yes	2/3	0.000003448	
6	10.184.22.243	163.172.208.7	532	No	3/3	1.02405715	No Response Recieved
7	10.184.22.243	163.172.208.7	1480	Yes	1/3	0.000025191	
8	10.184.22.243	163.172.208.7	1480	Yes	2/3	0.000003964	
9	10.184.22.243	163.172.208.7	532	No	3/3	1.023903677	No Response Recieved
10	10.184.22.243	163.172.208.7	1480	Yes	1/3	0.000025568	
11	10.184.22.243	163.172.208.7	1480	Yes	2/3	0.000004302	
12	10.184.22.243	163.172.208.7	532	No	3/3	1.023816042	No Response Recieved
13	10.184.22.243	163.172.208.7	1480	Yes	1/3	0.000014844	
14	10.184.22.243	163.172.208.7	1480	Yes	2/3	0.000001195	
15	10.184.22.243	163.172.208.7	532	No	3/3	0.671656611	No Response Received

Task 5 - Traceroute task

1. 22 hops are involved in finding the route to this ping-ams1.online.net
2. Total 256 packets are exchanged between source and destination which are of type udp or icmp.
   a. From the client (192.168.209.97), 160 packets are sent.
   b. From the remote server, 96 packets are sent to the client(192.168.209.97)

   Attached the link to **tabulated data.** Click the underlined text to view.
   https://docs.google.com/spreadsheets/d/1hNB59f5_rMGWRKg1GYY_V_ByTvqMj5yRp7FjxfyGlpE/edit?usp=sharing
   Link in case the hyperlink doesn't work.

3. The fields that always change are Header Checksum and Identification and stream index. Source and Destination ports also always changes.
   Length, Source and Destination Address always remains same.
   Header Checksum and Identification and stream index must change.
   Source and Destination Address must remain same