Assignment-1

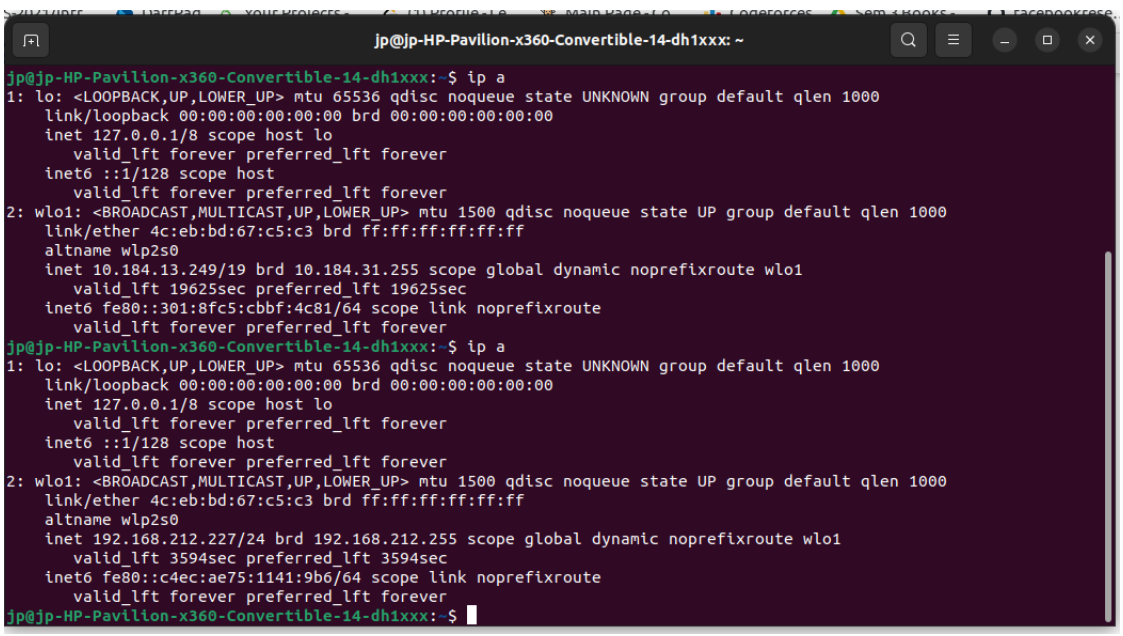
2020CS10356

August 30, 2022

1 Networking Tools :

1.1

IP address of My Machine when connected to IITD_WIFI is 10.184.13.249
IP address of My Machine when connected to my personal mobile hotspot is 192.168.212.227



1.2

IP address associated with www.google.com and www.facebook.com with local DNS server.

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.36
Name:   www.google.com
Address: 2404:6800:4009:82d::2004

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ 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

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

IP address associated with www.google.com and www.facebook.com with open DNS server(Change of DNS Server).

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.68
Name:   www.google.com
Address: 2404:6800:4002:816::2004

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ 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: 31.13.79.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

We can observe the change in IP Address

1.3

packets of size 1000 and TTL 255

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ping -s 1000 www.google.com -c 5 -t 255
PING www.google.com (142.250.206.100) 1000(1028) bytes of data.
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=1 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=2 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=3 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=4 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=5 ttl=118 (truncated)

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.995/29.112/112.858/41.908 ms
```

packets of size 1000 and TTL 150

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ping -s 1000 www.google.com -c 5 -t 150
PING www.google.com (142.250.183.36) 1000(1028) bytes of data.
76 bytes from bom12s11-in-f4.1e100.net (142.250.183.36): icmp_seq=1 ttl=117 (truncated)
76 bytes from bom12s11-in-f4.1e100.net (142.250.183.36): icmp_seq=2 ttl=117 (truncated)
76 bytes from bom12s11-in-f4.1e100.net (142.250.183.36): icmp_seq=3 ttl=117 (truncated)
76 bytes from bom12s11-in-f4.1e100.net (142.250.183.36): icmp_seq=4 ttl=117 (truncated)
76 bytes from bom12s11-in-f4.1e100.net (142.250.183.36): icmp_seq=5 ttl=117 (truncated)

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 25.852/60.692/98.934/25.980 ms
```

packets of size 500 and TTL 255

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ping -s 500 www.google.com -c 5 -t 255
PING www.google.com (142.250.206.100) 500(528) bytes of data.
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=1 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=2 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=3 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=4 ttl=118 (truncated)
76 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=5 ttl=118 (truncated)

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 7.164/9.814/11.142/1.385 ms
```

packets of size 500 and TTL 150

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ping -s 500 www.google.com -c 5 -t 100
PING www.google.com (142.251.42.4) 500(528) bytes of data.
76 bytes from bom12s19-in-f4.1e100.net (142.251.42.4): icmp_seq=1 ttl=117 (truncated)
76 bytes from bom12s19-in-f4.1e100.net (142.251.42.4): icmp_seq=2 ttl=117 (truncated)
76 bytes from bom12s19-in-f4.1e100.net (142.251.42.4): icmp_seq=3 ttl=117 (truncated)
76 bytes from bom12s19-in-f4.1e100.net (142.251.42.4): icmp_seq=4 ttl=117 (truncated)
76 bytes from bom12s19-in-f4.1e100.net (142.251.42.4): icmp_seq=5 ttl=117 (truncated)

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 45.332/86.214/124.176/27.075 ms
```

We can see the changes in RTT below the pictures.

1.4

Using different ISP to traceroute www.google.com and www.facebook.com.

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ traceroute www.google.com
traceroute to www.google.com (142.250.205.228), 64 hops max
  1   192.168.212.13  4.876ms  3.120ms  2.881ms
  2   192.168.59.1  191.219ms  204.581ms  192.168.27.45  204.217ms
  3   192.168.27.33  408.678ms  192.168.27.105  204.180ms  204.355ms
  4   192.168.27.111  408.719ms  122.185.39.5  204.267ms  306.432ms
  5   122.185.39.1  306.563ms  72.14.217.194  204.287ms  204.099ms
  6   72.14.217.194  408.905ms  *  268.181ms
  7   *  *  *
  8   142.251.76.196  193.987ms  204.469ms  74.125.244.195  204.515ms
  9   *  *  *
 10   108.170.225.85  183.386ms  218.335ms  *
 11   *  *  *
 12   74.125.242.145  266.639ms  142.251.60.185  204.574ms  204.385ms
 13   142.251.60.185  283.063ms  126.124ms  142.250.205.228  204.587ms
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ traceroute www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.239.35), 64 hops max
  1   192.168.212.13  4.203ms  3.076ms  2.902ms
  2   192.168.59.1  195.166ms  201.356ms  192.168.27.9  204.620ms
  3   192.168.27.21  409.352ms  192.168.27.109  204.603ms  204.626ms
  4   192.168.27.105  413.706ms  122.185.39.1  200.284ms  204.525ms
  5   122.185.39.5  423.871ms  157.240.70.152  87.833ms  102.233ms
  6   157.240.69.238  409.315ms  74.119.78.33  193.504ms  196.453ms
  7   157.240.50.169  428.707ms  157.240.39.173  207.047ms  36.711ms
  8   157.240.39.203  383.380ms  157.240.239.35  209.998ms  209.938ms
```

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 64 hops max
  1   10.184.0.14  3.877ms  2.799ms  3.177ms
  2   10.254.236.18  3.082ms  3.201ms  3.448ms
  3   10.10.211.212  6.147ms  3.127ms  3.202ms
```

All the paths are in IPv4 for www.iitd.ac.in, www.google.com ,www.facebook.com

We can make the traceroute request in tcp packets for some of the missing routers to reply.

2 DNS Task

2.1

There are total 12 DNS query and response messages.

All the messages are send over **UDP**.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.184.16.241	10.10.2.2	DNS	85	Standard query 0x0b0d A www.google.com OPT
2	0.014569519	10.10.2.2	10.184.16.241	DNS	349	Standard query response 0x0b0d A www.google.com A 216.58.221.36 NS ns4.google.com NS ns3.google.com NS ns1.google.com NS ns…
3	0.762926232	10.184.16.241	10.10.2.2	DNS	95	Standard query 0x9449 A www.youtube-nocookie.com OPT
4	0.768546134	10.10.2.2	10.184.16.241	DNS	633	Standard query response 0x9449 A www.youtube-nocookie.com CNAME youtube-ui.l.google.com A 172.217.174.78 A 142.250.183.142 …
5	1.314970235	10.184.16.241	10.10.2.2	DNS	89	Standard query 0xda95 A www.cse.iitd.ac.in OPT
6	1.316872828	10.184.16.241	10.10.2.2	DNS	94	Standard query 0x2114 A safebrowsing.google.com OPT
7	1.318293344	10.10.2.2	10.184.16.241	DNS	283	Standard query response 0xda95 A www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in A 10.208.20.4 NS dns.cc.iitd.ernet.in NS des…
8	1.321613789	10.10.2.2	10.184.16.241	DNS	377	Standard query response 0x2114 A safebrowsing.google.com CNAME sb.l.google.com A 142.250.76.174 NS ns1.google.com NS ns4.go…
9	2.070987594	10.184.16.241	10.10.2.2	DNS	90	Standard query 0x6b9d A clients4.google.com OPT
10	2.076954557	10.10.2.2	10.184.16.241	DNS	378	Standard query response 0x6b9d A clients4.google.com CNAME clients.l.google.com A 142.250.182.174 NS ns3.google.com NS ns1.…
11	2.380281376	10.184.16.241	10.10.2.2	DNS	92	Standard query 0xdf97 A jnn-pa.googleapis.com OPT
12	2.383548138	10.10.2.2	10.184.16.241	DNS	363	Standard query response 0xdf97 A jnn-pa.googleapis.com A 172.217.174.234 NS ns3.google.com NS ns2.google.com NS ns1.google.…

The 12 DNS query and response messages

2.2

IP address of Host Machine(10.184.16.241)
IP address of IITD DNS Server (10.10.2.2)
There are total 6 queries send from Host Machine to DNS Server(s).

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4c:eb:bd:67:c5:c3 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 10.184.16.241/19 brd 10.184.31.255 scope global dynamic noprefixroute wlo1
       valid_lft 20054sec preferred_lft 20054sec
    inet6 fe80::d9ab:d7e9:c640:49a6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

Here we can see the host machine IP adrress is 10.184.16.241.

2.3

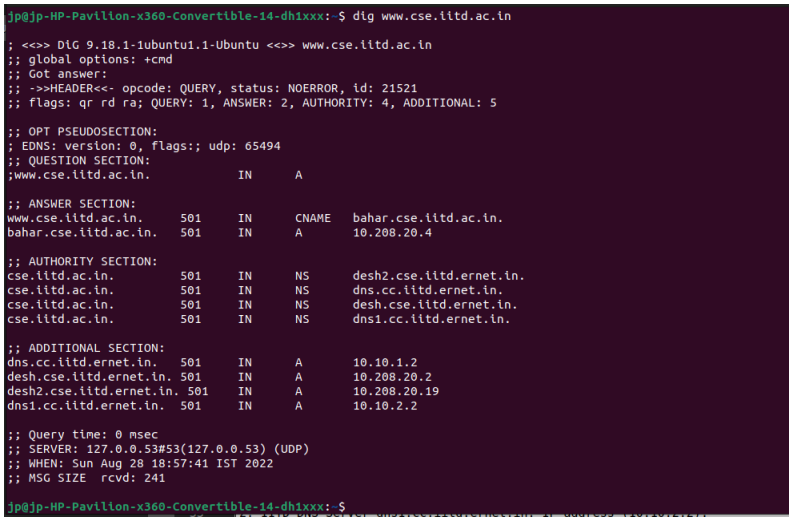
Only 1 DNS Servers are involved :
1. Local IITD DNS Server dns1.cc.iitd.ernet.in. IP address (10.10.2.2).

2.4

The DNS Server dns1.cc.iitd.ernet.in replies with
actual IP Address(10.10.2.2)

2.5

No not all DNS Servers responded only 1 responded out of 4 DNS Servers of IITD.



```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ dig www.cse.iitd.ac.in

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.cse.iitd.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21521
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.cse.iitd.ac.in.            IN      A

;; ANSWER SECTION:
www.cse.iitd.ac.in.     501     IN      CNAME   bahar.cse.iitd.ac.in.
bahar.cse.iitd.ac.in.   501     IN      A       10.208.20.4

;; AUTHORITY SECTION:
cse.iitd.ac.in.         501     IN      NS      desh2.cse.iitd.ernet.in.
cse.iitd.ac.in.         501     IN      NS      dns.cc.iitd.ernet.in.
cse.iitd.ac.in.         501     IN      NS      desh.cse.iitd.ernet.in.
cse.iitd.ac.in.         501     IN      NS      dns1.cc.iitd.ernet.in.

;; ADDITIONAL SECTION:
dns.cc.iitd.ernet.in.   501     IN      A       10.10.1.2
desh.cse.iitd.ernet.in. 501     IN      A       10.208.20.2
desh2.cse.iitd.ernet.in. 501    IN      A       10.208.20.19
dns1.cc.iitd.ernet.in.  501     IN      A       10.10.2.2

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Aug 28 18:57:41 IST 2022
;; MSG SIZE  rcvd: 241

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

We can see here there are 4 IITD DNS Server's. and out of them only 10.10.2.2 is resopnded.

2.6

List of resources and records involved in resolving the IP Address of the site :

resource	A www.google.com OPT
value/address	10.10.2.2
type	A
length of packet	85 bytes
Time to live(TTL)	64

resource	A www.google.com A 216.58.221.36 NS ns3.google.com
value/address	10.184.16.241
type	A ,class IN
length of packet	349 bytes
Time to live(TTL)	62

resource	A ,class IN
value/address	10.10.2.2
type	A Standard query , IPv4
length of packet	95 bytes
Time to live(TTL)	64

resource	A www.youtube.com-nocookie.com CNAME youtube-ui.l.google.com
value/address	10.10.2.2
type	A ,class IN
length of packet	633 bytes
Time to live(TTL)	62

resource	A www.cse.iitd.ac.in OPT
value/address	10.10.2.2
type	A , class IN
length of packet	89 bytes
Time to live(TTL)	64

resource	A safebrowsing.google.com OPT
value/address	10.10.2.2
type	A , class IN
length of packet	94 bytes
Time to live(TTL)	64

resource	A www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in
value/address	10.10.2.2
type	A , class IN
length of packet	288 bytes
Time to live(TTL)	62

resource	A safebrowsing.google.com CNAME sb.l.google.com
value/address	10.10.2.2
type	A , class IN
length of packet	377 bytes
Time to live(TTL)	62

resource	A clients.google.com OPT
value/address	10.10.2.2
type	A , class IN
length of packet	90 bytes
Time to live(TTL)	64

resource	A clients4.google.com CNAME clients.l.google.com
value/address	10.10.2.2
type	A , class IN
length of packet	378 bytes
Time to live(TTL)	62

resource	A jnn-pa.googleapis.com OPT
value/address	10.10.2.2
type	A , class IN
length of packet	92 bytes
Time to live(TTL)	64

resource	A jnn-pa.googleapis.com A 172.217.174.234 NS ns3.google.com
value/address	10.10.2.2
type	A , class IN
length of packet	363 bytes
Time to live(TTL)	62

1

2

3 Iperf Task :

3.1

There are 2529 UDP packets exchanged between iperf3 client and remote server in this communication.

These packets are shared with wireshark file 2020CS10356_iperf.pcap.png

3.2

The server with IP Address 62.210.18.40 (ping.online.net) is sending Bulk data to local reciever with IP address with IP address 10.184.28.108.

The average size of Packet Sent is 566 Bytes

3.3

Throughput Calculation :

Throughtput = $\frac{AverageDatatransfered}{AverageTimeTaken}$

Average size of packets = 566

Number of packets 2529

Time taken for all the packets = 10.238183687

Total Data Transfered = Number of packets × Average size of packets.

Total Data Transfered = 1431414 bytes.

$$\text{Throughput} = \frac{1431414}{10.238183687}$$
$$\text{Throughput} = 139.81132 \text{ kbps.}$$

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.184.28.108	62.210.18.40	UDP	46	60715 → 5208 Len=4
2	0.196565821	62.210.18.40	10.184.28.108	UDP	46	5208 → 60715 Len=4
3	0.196565906	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
4	0.301583452	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
5	0.301583591	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
6	0.301583609	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
7	0.301583627	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
8	0.301583646	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
9	0.301583664	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
10	0.301583682	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
11	0.301583701	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
12	0.301598995	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
13	0.301599014	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
14	0.301599031	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
15	0.301599055	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
16	0.301599073	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
17	0.301599092	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
18	0.301599111	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
19	0.301599130	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
20	0.301610345	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524
21	0.301610363	62.210.18.40	10.184.28.108	UDP	566	5208 → 60715 Len=524

```
▸ Frame 4: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface wlo1, id 0
▸ Ethernet II, Src: Cisco_19:a5:41 (84:78:ac:19:a5:41), Dst: Chongqin_67:c5:c3 (4c:eb:bd:67:c5:c3)
▸ Internet Protocol Version 4, Src: 62.210.18.40, Dst: 10.184.28.108
▸ User Datagram Protocol, Src Port: 5208, Dst Port: 60715
▸ Data (524 bytes)
```

while, that from iperf3 terminal we get that,
Throughput = 126kbps.
while , that from capture file properties it is 141.43.

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx: ~
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ resolvectl flush-caches
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ resolvectl flush-caches
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ 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 10.184.28.108 port 60715 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec   128 KBytes  1.05 Mbits/sec  0.948 ms  0/251 (0%)
[  5]   1.00-2.00   sec   128 KBytes  1.05 Mbits/sec  0.196 ms  0/250 (0%)
[  5]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec  0.106 ms  0/250 (0%)
[  5]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  0.245 ms  0/250 (0%)
[  5]   4.00-5.00   sec   128 KBytes  1.05 Mbits/sec  0.089 ms  0/250 (0%)
[  5]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec  0.017 ms  0/250 (0%)
[  5]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec  0.012 ms  0/251 (0%)
[  5]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec  0.060 ms  0/250 (0%)
[  5]   8.00-9.00   sec   128 KBytes  1.05 Mbits/sec  0.130 ms  0/250 (0%)
[  5]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec  0.055 ms  0/250 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.00  sec  1.26 MBytes  1.06 Mbits/sec  0.000 ms  0/2502 (0%)  sender
[  5]   0.00-10.00  sec  1.25 MBytes  1.05 Mbits/sec  0.055 ms  0/2502 (0%)  receiver

iperf Done.
```

Here , We can observe that there is significant difference in throughput,

wireshark shows more throughput than iperf3 terminal.
This is because iperf captures the payload data rate , i.e. the actual useful user-data sent inside packets.
Wireshark captures all data and overheads,including user-data, plus packet headers around the user data, and frame headers around the packets.

4 HTTP Task :

4.1

There are 2 HTTP/1.1 and 9 HTTP/2 packets are present(when filtered).
while it is shown 10 HTTP/2 in the statastics this is because
Out of which packet 2 HTTP/1.1 is switching protocol. which is counted on both HTTP/1.1 and HTTP/2
Packet 6 has two header types of HTTP/1.1 and HTTP/2.

4.2

There are 6 HTTP/2 packets are exchanged between client and server before the first object is fetched.
Out of which 1 packet is Switching protocol. and considered as HTTP/2

4.3

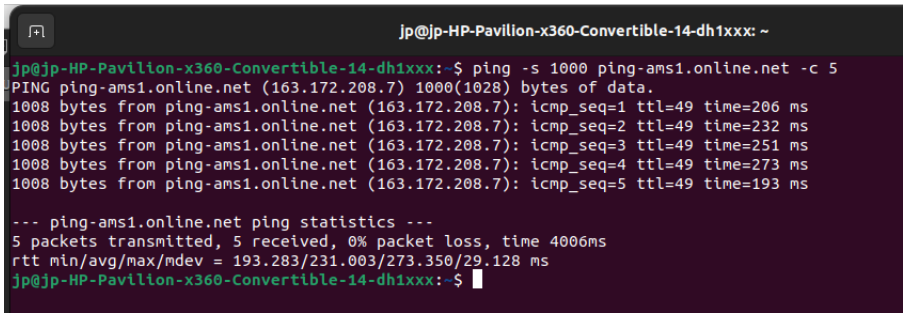
The differnce between Headers of HTTP/1.1 and HTTP/2 in the packets is
The Headers of HTTP/1.1 are textual format ie., common language.
While that of headers of HTTP/2 packets are binary framing layer.

5 Ping Task :

Task was performed on a small packet size like:
ping -s 1000 ping-ams1.online.net -c 5

5.1

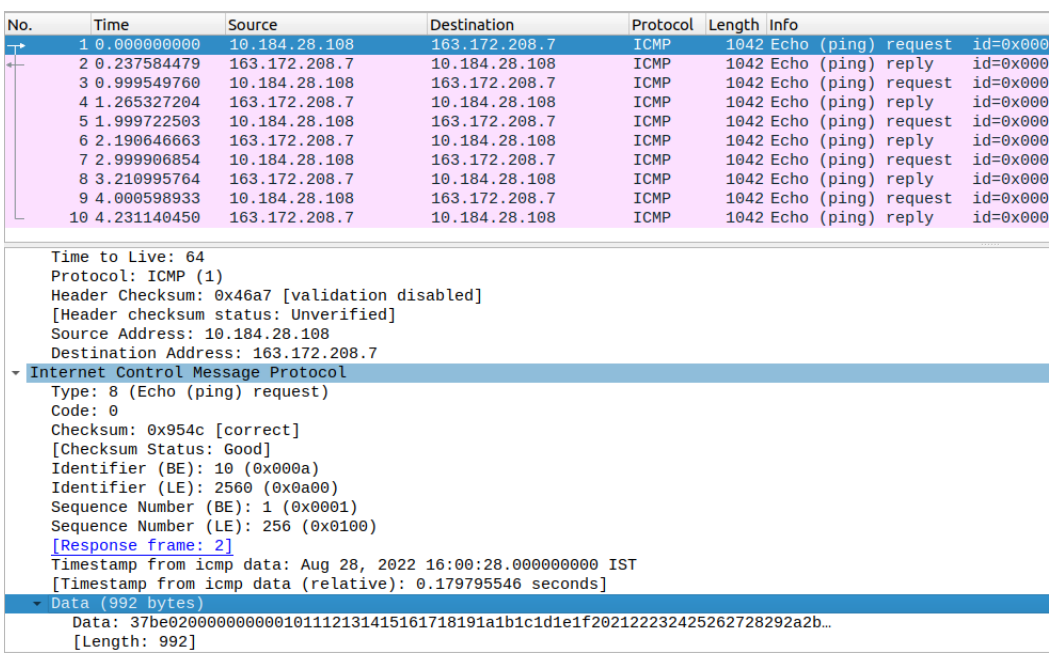
A total of 10 IP packets are exchanged between host and remote server representing ping-ams1.online.net.



```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx: ~
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ ping -s 1000 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7) 1000(1028) bytes of data.
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=1 ttl=49 time=206 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=2 ttl=49 time=232 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=3 ttl=49 time=251 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=4 ttl=49 time=273 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=5 ttl=49 time=193 ms

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 193.283/231.003/273.350/29.128 ms
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

5.2

The packet size of each ping request sent from host to remote server is **1042 bytes**.
while that of size of data in each packet is **992 bytes**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.184.28.108	163.172.208.7	ICMP	1042	Echo (ping) request id=0x000
2	0.237584479	163.172.208.7	10.184.28.108	ICMP	1042	Echo (ping) reply id=0x000
3	0.999549760	10.184.28.108	163.172.208.7	ICMP	1042	Echo (ping) request id=0x000
4	1.265327204	163.172.208.7	10.184.28.108	ICMP	1042	Echo (ping) reply id=0x000
5	1.999722503	10.184.28.108	163.172.208.7	ICMP	1042	Echo (ping) request id=0x000
6	2.190646663	163.172.208.7	10.184.28.108	ICMP	1042	Echo (ping) reply id=0x000
7	2.999906854	10.184.28.108	163.172.208.7	ICMP	1042	Echo (ping) request id=0x000
8	3.210995764	163.172.208.7	10.184.28.108	ICMP	1042	Echo (ping) reply id=0x000
9	4.000598933	10.184.28.108	163.172.208.7	ICMP	1042	Echo (ping) request id=0x000
10	4.231140450	163.172.208.7	10.184.28.108	ICMP	1042	Echo (ping) reply id=0x000

```
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x46a7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.184.28.108
    Destination Address: 163.172.208.7
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x954c [correct]
    [Checksum Status: Good]
    Identifier (BE): 10 (0x000a)
    Identifier (LE): 2560 (0x0a00)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 2]
    Timestamp from icmp data: Aug 28, 2022 16:00:28.000000000 IST
    [Timestamp from icmp data (relative): 0.179795546 seconds]
    Data (992 bytes)
      Data: 37be020000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 992]
```

```
jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$ nslookup ping-ams1.online.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ping-ams1.online.net
Address: 163.172.208.7

jp@jp-HP-Pavilion-x360-Convertible-14-dh1xxx:~$
```

5.3

seq	Sent Time	Fragmented or not	length	actual data length
1	0.00000	No	1042	992
2	0.99954	No	1042	992
3	1.99972	No	1042	992
4	2.99990	No	1042	992
5	4.00059	No	1042	992

seq	Response time	Fragmented or not	length	actual data length
1	0.23758	No	1042	992
2	1.26532	No	1042	992
3	2.19064	No	1042	992
4	3.21099	No	1042	992
5	4.23114	No	1042	992

6 Traceroute Task :

6.1

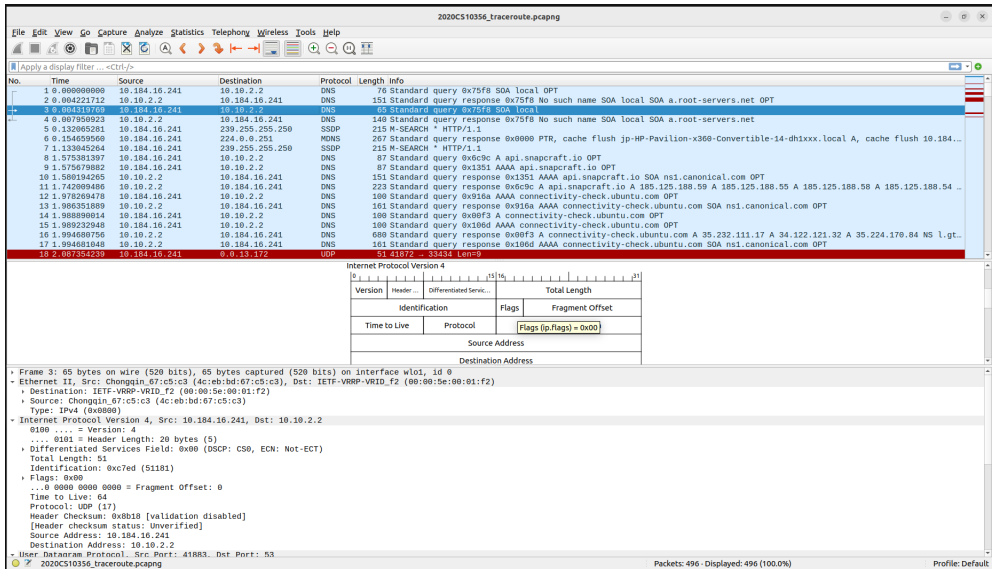
18 hops are involved in finding the route to this ping-ams1.online.net

```
C:\Users\jayap>tracert ping-ams1.online.net

Tracing route to ping-ams1.online.net [163.172.208.7]
over a maximum of 30 hops:

  1    17 ms     3 ms     4 ms  10.184.0.14
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18   231 ms   169 ms   236 ms  ping-ams1.online.net [163.172.208.7]

Trace complete.
```

6.2

There are a total of 1199 IP packets are exchanged in the communication to get the final tracerote of ping-ams1.online.net.

packet route	Number of packets
client to remote machine(router/server)	595
remote machine(hop/server/router) to local client	169
remote machine(client/hop/router) to server(ping-ams1.online.net)	320



The fields that change from one datagram to other are :

Identification

Time to Live (TTL)

Header Checksum

The fields that are constant from one datagram to other are :

IPv4 Version

header length

source IP

Differentiated Services Field

Fields that should not change due to :

Version - since we are using IPv4 for all packets.

header length - since all are UDP Packets.

source IP - sending from same source.

Differentiated Services Field - Since all packets use same type of service class.

Fields that should change due to :

Identification - since IP packets must have different ID's

Time to live (TTL) - since When a data packet reaches a hop (such as a router) on the way to the destination device,

the TTL value is decreased by 1.

Header Checksum - since Header changes its checksum also changes.