

## Lab:2 Assignment

### Task 1

[Ans:1]

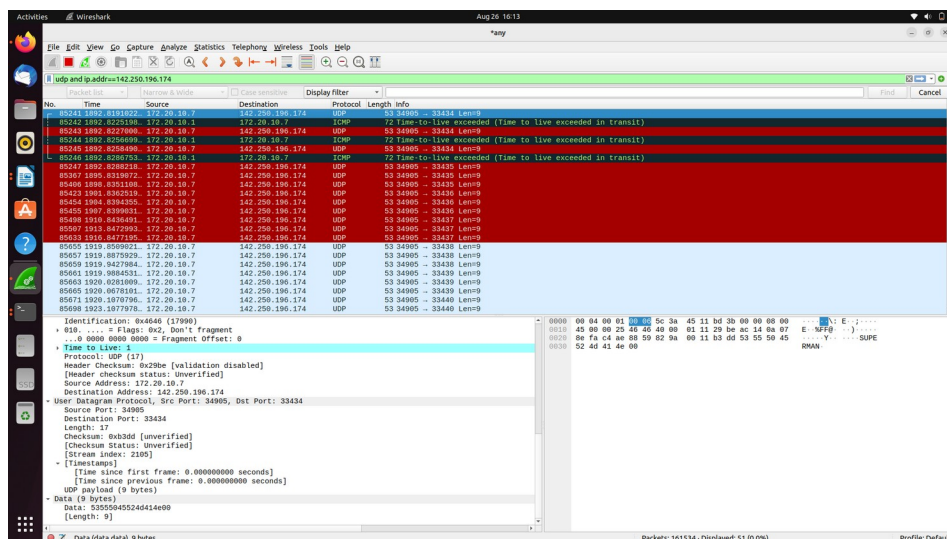
**Website:** [www.youtube.com](http://www.youtube.com)

By default UDP is used to send probe packets

Some of the key fields along with their values are as follow:

- (1) source ip address: 172.20.10.7
- (2) destination ip address: 142.250.196.174
- (3) source port: 34905
- (4) destination port: 33434
- (5) Time to Live: 1 (depending upon the probe request from the client)
- (6) UDP payload: SUPERMAN.

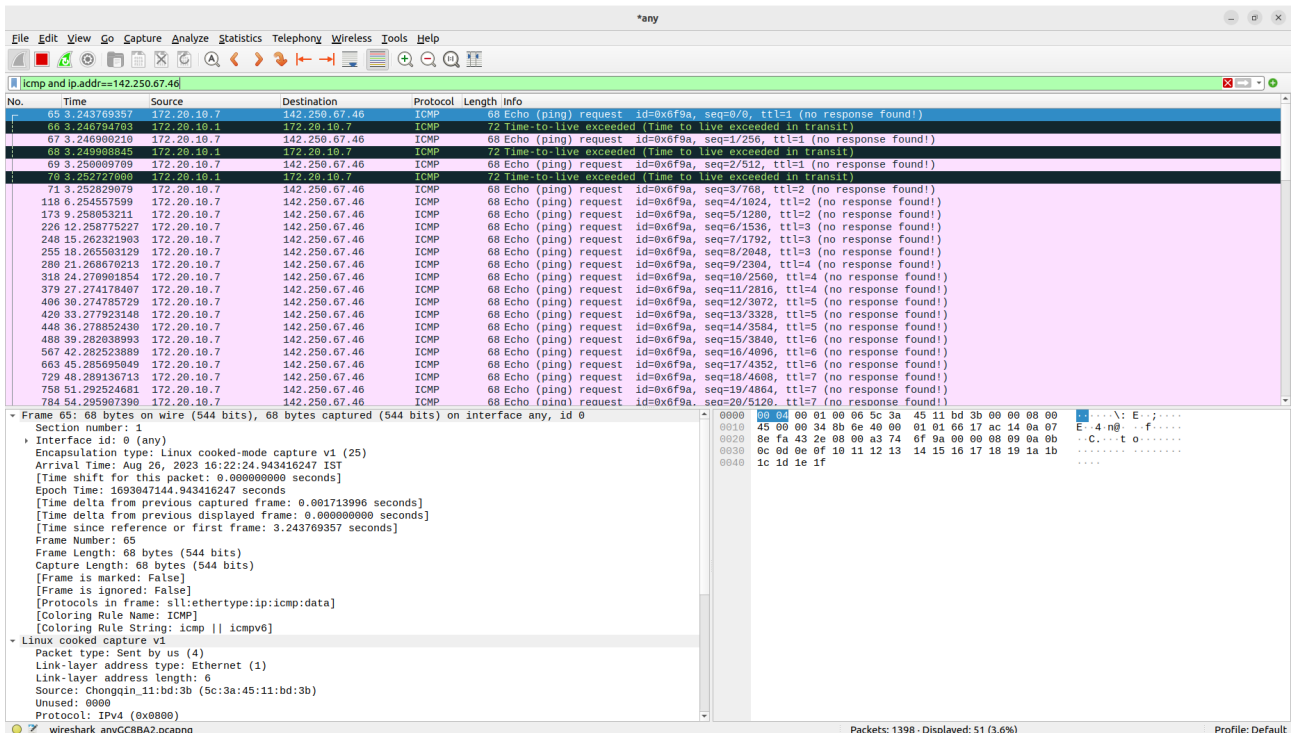
```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
60 * * *  
61 * * *  
62 * * *  
63 * * *  
64 * * *  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ traceroute www.youtube.com  
traceroute to youtube-ui.l.google.com (142.250.196.174), 64 hops max  
 1  172.20.10.1  3.498ms  3.067ms  2.884ms  
 2  * * *  
 3  * * *  
 4  * * *  
 5  172.17.185.34  36.547ms  55.079ms  45.510ms  
 6  192.168.60.228  39.512ms  39.541ms  39.193ms  
 7  * * *  
 8  * * *  
 9  74.125.51.166  93.343ms  55.724ms  59.388ms  
10  * * *  
11  142.251.77.96  96.682ms  53.472ms  59.091ms  
12  74.125.242.138  89.705ms  44.706ms  40.087ms  
13  216.239.50.22  65.228ms  60.226ms  59.758ms  
14  142.250.238.207  65.836ms  59.197ms  59.696ms  
15  142.250.196.174  66.089ms  40.076ms  64.128ms  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ ^C  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$
```



[Ans:2]

Yeah we can change the default protocol/ method used to send probe packets in traceroute. This can be made possible by using various options of traceroute commandline. -m is the one that does the work. For example to change the protocol to icmp we can use traceroute -m icmp or its shorter version i.e. traceroute -I. Similarly traceroute -m tcp or traceroute -T would send TCP packets.

```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
4 * * *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 * ^C  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ traceroute -I www.youtube.com  
traceroute to youtube-ui.l.google.com (142.250.67.46), 64 hops max  
1 172.20.10.1 3.051ms 3.033ms 2.746ms  
2 * * *  
3 * * *  
4 * * *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 * * *  
10 * * *  
11 * * *  
12 * * *  
13 * * *  
14 * * *  
15 142.250.67.46 69.686ms 119.797ms 99.811ms  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$
```



[Ans: 3]

The first the packets are send at a time gap/delay of 0.003 ms

And the remaining between packets are send at a time gap/delay of averagely 3.003 ms

The last three packets to the destination are having a time gap/delay of 0.05 ms

so average time gap/delay ~3.003ms

[Ans: 4]

The probe response in counter of probe packet's TTL reaching zero is an ICMP TTL exceeded message that contains sender's IP address, IP address of router, sequence number, some payload etc. All this information helps in calculation of round trip time and finding a path from source to destination or a host of internet.

[Ans: 5]

Mostly all the network protocol has TTL field such as UDP, ICMP, Ipv4, Ipv6 etc.

The TTL of traceroute probe packet incrementally increases every hop to hop with each of the router or hop decreasing its TTL value and when it is zero it sends the probe response packet. That is 1,2,... and so on upto hop till the destination is reached or max hop is reached whichever is smaller. Here it was till 15.

The TTL of probe response packet is default to router sending the response. Here initially the TTL was 64 for the first response and the last one had 114.

[Ans:6]

On average it took 56.76433 ms for the output of traceroute i.e. reaching till the destination.

The output RTT for 2,3,4 router are star(\*). And at 5<sup>th</sup> router the RTT jumped from 3ms to 46ms. So I guess any one of 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> router would be the candidate for bottleneck router.

[Ans: 7]

Yes there are appeared stars in the traceroute output. Some of the potential reasons are listed below:

- (1) no reply router
- (2) drop packet router
- (3) ICMP response from the router have a lower TTL field value

**Task: 2**  
**website:** example.com

```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
3 * * *  
^C  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ traceroute example.com  
traceroute to example.com (93.184.216.34), 64 hops max  
1 172.20.10.1 4.386ms 2.862ms 3.144ms  
2 * * *  
3 * * *  
4 * * *  
5 172.17.185.35 67.325ms 40.152ms 29.509ms  
6 192.168.60.226 41.019ms 40.002ms 40.585ms  
7 * * *  
8 * * *  
9 103.198.140.170 77.385ms 59.964ms 57.270ms  
10 49.45.4.85 278.454ms 259.810ms 254.757ms  
11 49.45.4.103 263.230ms 259.577ms 256.609ms  
12 154.54.27.117 265.294ms 260.334ms 253.477ms  
13 154.54.27.117 263.776ms 263.082ms 270.275ms  
14 38.122.147.170 270.358ms 260.284ms 254.095ms  
15 38.104.83.194 279.374ms 274.431ms 269.890ms  
16 93.184.216.34 249.941ms 260.120ms 259.620ms  
17 93.184.216.34 258.185ms 260.020ms 265.632ms  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$
```

```
Aug 26 19:47  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ sudo tcpdump host 93.184.216.34  
tcpdump: verbose output suppressed, use -v|-vv for full protocol decode  
listening on vti0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
19:45:31.017525 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33434: UDP, length 9  
19:45:31.022083 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33434: UDP, length 9  
19:45:31.025236 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33431: UDP, length 9  
19:45:31.028297 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33435: UDP, length 9  
19:45:34.031688 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33435: UDP, length 9  
19:45:37.034171 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33435: UDP, length 9  
19:45:40.037887 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33436: UDP, length 9  
19:45:43.041580 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33436: UDP, length 9  
19:45:46.045280 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33436: UDP, length 9  
19:45:49.048853 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33437: UDP, length 9  
19:45:52.052460 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33437: UDP, length 9  
19:45:55.056553 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33437: UDP, length 9  
19:45:58.057734 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33438: UDP, length 9  
19:45:58.125118 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33438: UDP, length 9  
19:45:58.165312 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33438: UDP, length 9  
19:45:58.194870 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33439: UDP, length 9  
19:45:58.235930 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33439: UDP, length 9  
19:45:58.275961 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33439: UDP, length 9  
19:45:58.316580 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33440: UDP, length 9  
19:46:01.318253 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33440: UDP, length 9  
19:46:04.321629 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33440: UDP, length 9  
19:46:07.325178 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33441: UDP, length 9  
19:46:10.328880 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33441: UDP, length 9  
19:46:13.329672 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33441: UDP, length 9  
19:46:16.333223 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33442: UDP, length 9  
19:46:16.416742 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33442: UDP, length 9  
19:46:16.478829 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33442: UDP, length 9  
19:46:16.528230 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33443: UDP, length 9  
19:46:16.806797 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33443: UDP, length 9  
19:46:17.066730 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33443: UDP, length 9  
19:46:17.321620 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33444: UDP, length 9  
19:46:17.584994 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33444: UDP, length 9  
19:46:17.844695 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33444: UDP, length 9  
19:46:18.101355 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33445: UDP, length 9  
19:46:18.368741 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33445: UDP, length 9  
19:46:18.627197 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33445: UDP, length 9  
19:46:18.880810 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33446: UDP, length 9  
19:46:19.144725 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33446: UDP, length 9  
19:46:19.407939 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33446: UDP, length 9  
19:46:19.678350 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33447: UDP, length 9  
19:46:19.948852 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33447: UDP, length 9  
19:46:20.209268 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33447: UDP, length 9  
19:46:20.463505 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33448: UDP, length 9  
19:46:20.742944 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33448: UDP, length 9  
19:46:21.017403 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33448: UDP, length 9  
19:46:21.287398 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33449: UDP, length 9  
19:46:21.537232 IP 93.184.216.34 > yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ICMP time exceeded in-transit, length 45  
19:46:21.537470 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33449: UDP, length 9  
19:46:21.797494 IP 93.184.216.34 > yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ICMP time exceeded in-transit, length 45  
19:46:21.797709 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33449: UDP, length 9  
19:46:22.057222 IP 93.184.216.34 > yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ICMP time exceeded in-transit, length 45  
19:46:22.057460 IP yug-HP-Pavilion-x360-Convertible-14-dh0xxx.42625 > 93.184.216.34.33450: UDP, length 9  
19:46:22.315553 IP 93.184.216.34 > yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ICMP 93.184.216.34 udp port 33450 unreachable, length 45
```

[Ans: Q3]

Average gap between probe packets: 0.98510611538462 ms

[Ans: Q5]

UDP: {1,2.....,18}

ICMP: 51

[Ans: Q6]

Time: 278.223 ms

Bottleneck router: 10<sup>th</sup> router as the jump is from ~70 ms to ~260 ms

### Task: 3

**Netstat:** netstat command is used to display networking statistics that includes network connection, interface statistics, routing table etc. As such there is no direct effect of running netstat command on Wireshark.

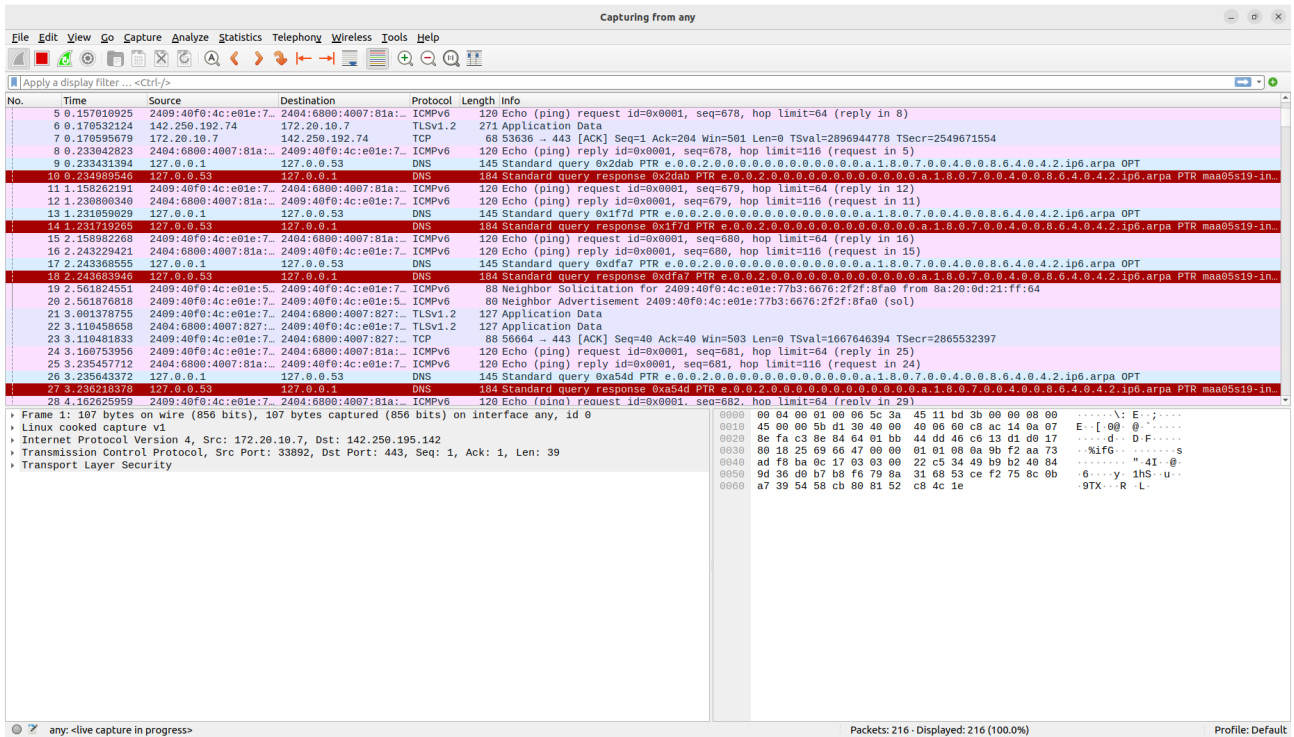
```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
List of possible address families (which support routing):  
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)  
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)  
x25 (CCITT X.25)  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~$ netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 yug-HP-Pavilion-x:53620 bom12s16-ln-f10.1:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:44628 123.208.120.34:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:42396 ec2-52-215-201-12:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:33892 maa03s40-ln-f14.1:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:53636 bom12s16-ln-f10.1:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:50406 ec2-54-147-245-30:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:60264 maa03s39-ln-f3.1e:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:40872 172.67.143.109:https TIME_WAIT  
tcp        0      0 yug-HP-Pavilion-x:40124 maa03s47-ln-f3.1e:https ESTABLISHED  
tcp        0      0 yug-HP-Pavilion-x:37614 bom07s15-ln-f3.1e:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:50282 server-18-155-56-5:http TIME_WAIT  
tcp6       0      0 yug-HP-Pavilion-x:45136 2405:200:1630:a01:htp TIME_WAIT  
tcp6       0      0 yug-HP-Pavilion-x:50276 server-18-155-56-5:http TIME_WAIT  
tcp6       0      0 yug-HP-Pavilion-x:42030 a23-200-49-104.de:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:58386 2001:4860:4802:36:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:40202 maa05s26-ln-x02.1:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:41676 server-18-155-56-5:http TIME_WAIT  
tcp6       0      0 yug-HP-Pavilion-x:41818 2600:9000:2178:4e:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:52386 maa03s38-ln-x02.1:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:49562 2600:9000:2078:28:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:39870 64:ff9b:ac40:946:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:37526 maa03s40-ln-x0d.1:https ESTABLISHED  
tcp6       0      0 yug-HP-Pavilion-x:43834 bom07s35-ln-x03.1:https ESTABLISHED
```

**Ping:** Packet Internet Groper command is used to check the network connectivity between host and server.

When ping command was hit in terminal then corresponding to each of the request to the another host or server on internet an ICMPv6 request and reply packet was captured from source to destination and destination to source respectively.

```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~  
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx: ~$ ping google.com  
PING google.com(maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e)) 56 data bytes  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=1 ttl=116 time=53.2 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=2 ttl=116 time=51.9 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=3 ttl=116 time=96.4 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=4 ttl=116 time=50.7 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=5 ttl=116 time=93.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=6 ttl=116 time=88.3 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=7 ttl=116 time=90.8 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=8 ttl=116 time=43.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=9 ttl=116 time=87.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=10 ttl=116 time=39.9 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=11 ttl=116 time=38.9 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=12 ttl=116 time=83.0 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=13 ttl=116 time=81.2 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=14 ttl=116 time=80.7 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=15 ttl=116 time=78.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=16 ttl=116 time=71.4 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=17 ttl=116 time=69.5 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=18 ttl=116 time=71.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=19 ttl=116 time=66.0 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=20 ttl=116 time=64.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=21 ttl=116 time=63.4 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=22 ttl=116 time=60.3 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=23 ttl=116 time=58.8 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=24 ttl=116 time=57.7 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=25 ttl=116 time=56.3 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=26 ttl=116 time=99.3 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=27 ttl=116 time=52.0 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=28 ttl=116 time=96.1 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=29 ttl=116 time=94.6 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=30 ttl=116 time=92.8 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=31 ttl=116 time=85.3 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=32 ttl=116 time=89.7 ms  
64 bytes from maa05s19-ln-x0e.1e100.net (2404:6800:4007:81a::200e): icmp_seq=33 ttl=116 time=83.7 ms
```





*Pink color shows echo ping request and reply*

**Mtr:** mtr command is a network diagnostic tool that combines ping and traceroute commands. So basically it performs ping for each of the entries in traceroute output.

