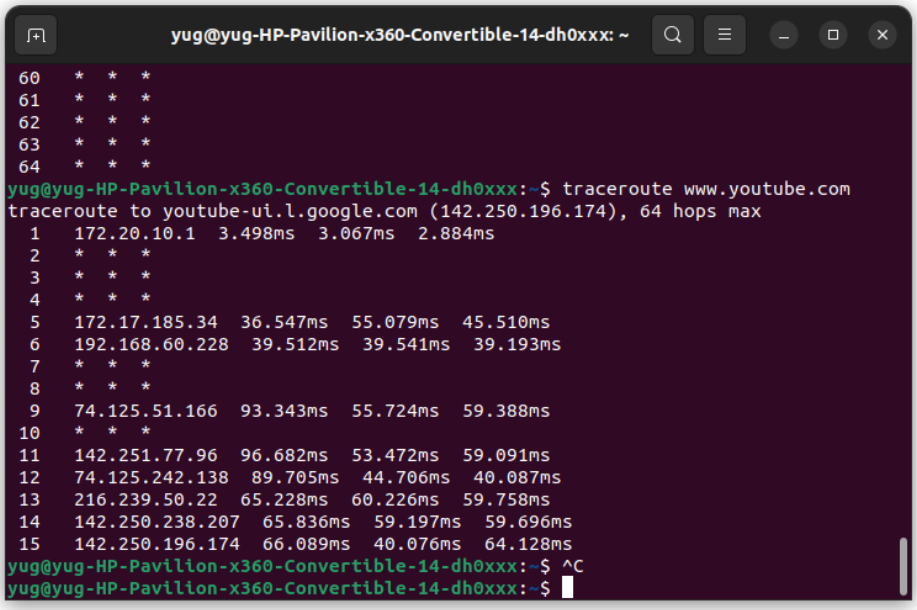
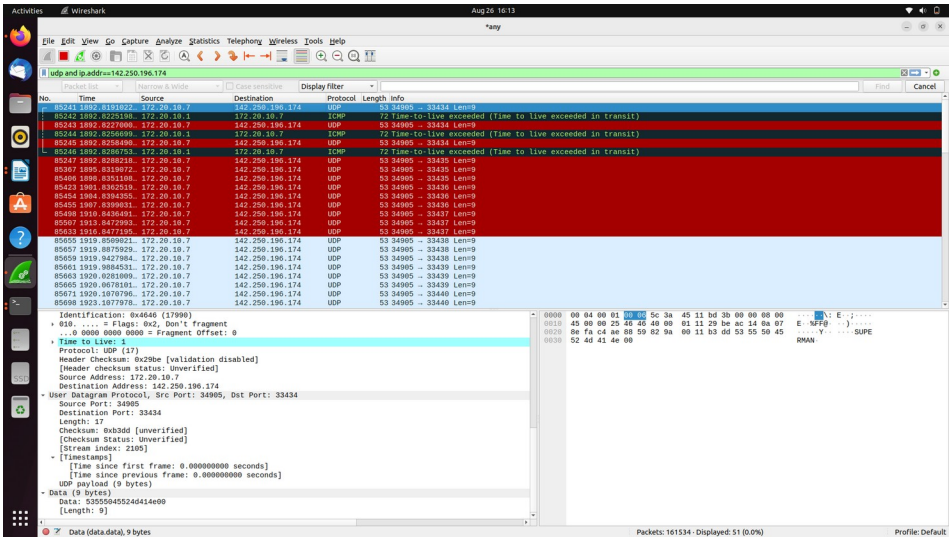
Lab:2 Assignment

Task 1

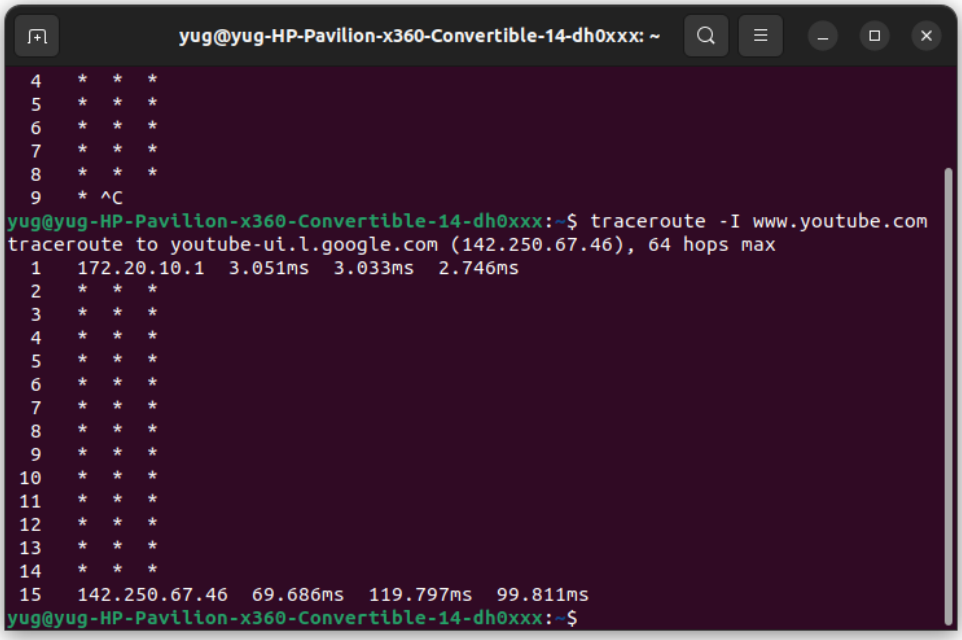
[Ans:1]
Website: www.youtube.com

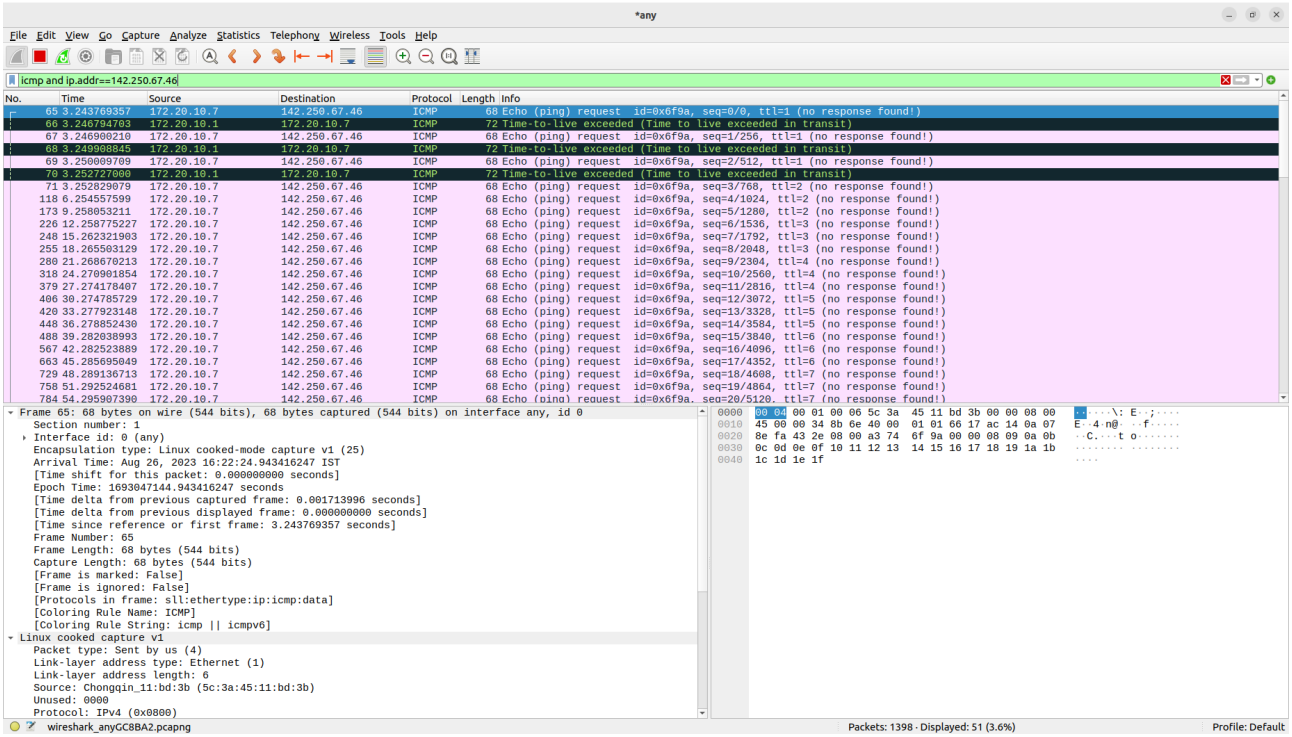
By default UDP is used to send probe packets
Some of the key fields along with their values are as follow:
(1) source ip address: 172.20.10.7
(2) destination ip address: 142.250.196.174
(3) source port: 34905
(4) destination port: 33434
(5) Time to Live: 1 (depending upon the probe request from the client)
(6) UDP payload: SUPERMAN.





[Ans:2]
Yeah we can chnage 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 the does the work. For example to chnage the protocol to icmp we can use traceroute -m icmp or its shortern version i.e. traceroute -I. Similarly traceroute -m tcp or traceroute -T would send TCP packets.





[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

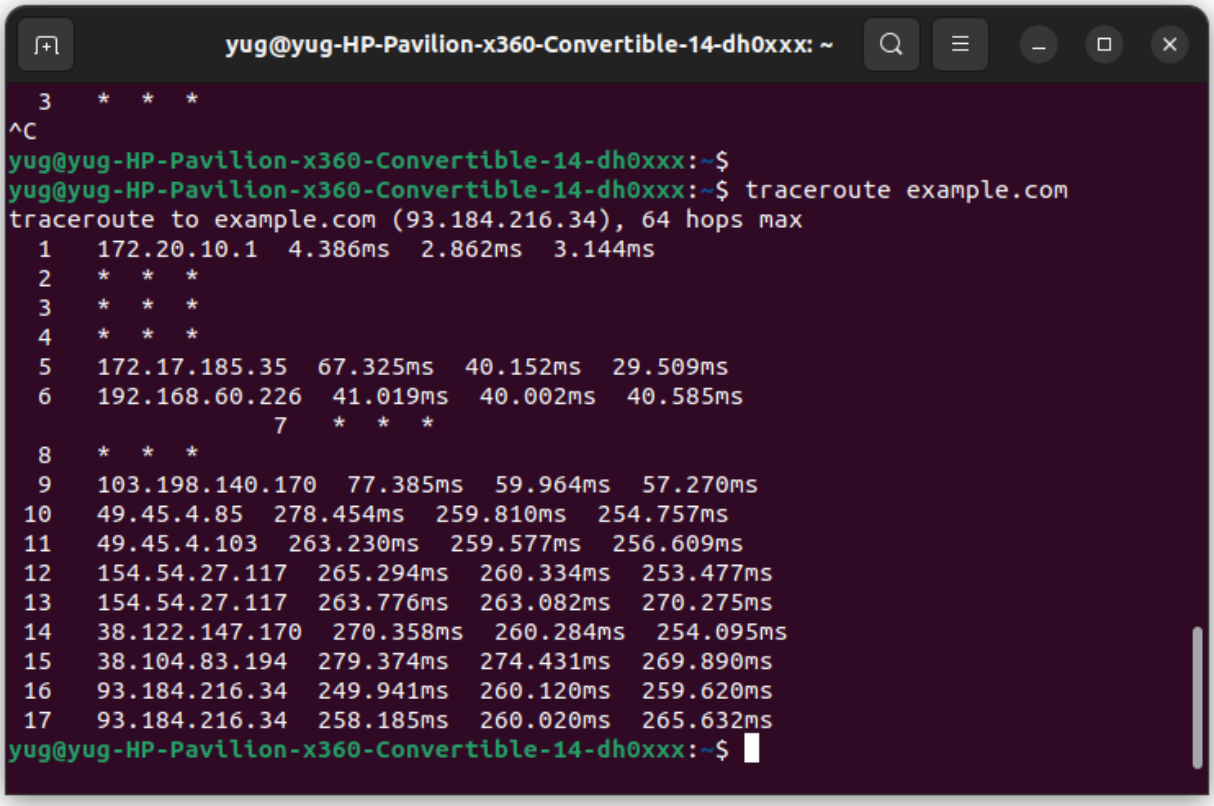
[Ans: 4]
The probe response in counter of probe packet's TTL reaching zero is an ICMP TTL exceeded message thats contains senders IP address, IP address of router, sequence number, some payload etc. All this informations helps in calculation of round trip time and finding a path from source to destination or a host of internet.

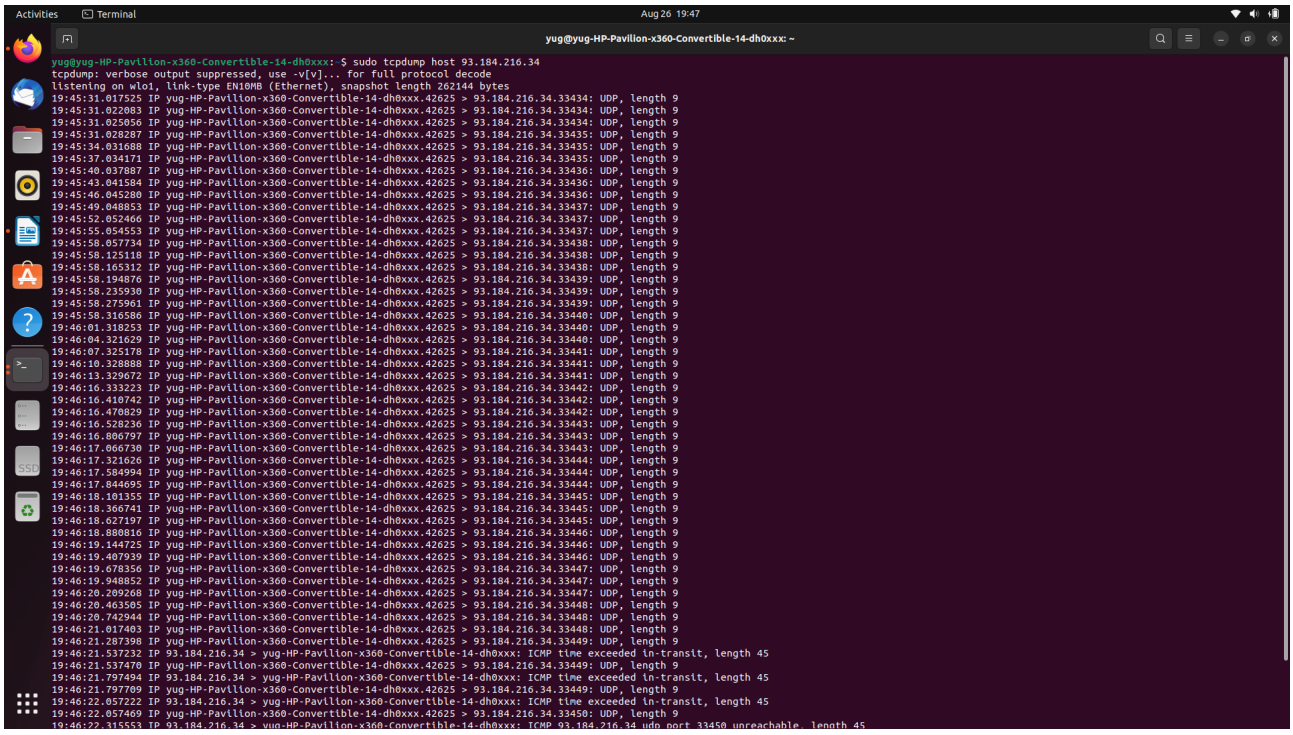
[Ans: 5]
Mostly all the network protocol has TTL field such as UDP, ICMP, Ipv4, Ipv6 etc.
The TTL of traceroute probe packet incremently increases evry hop to hop with each of the router or hop decreasing its TTL value and when it its zero its send the probe respone packet. That is 1,2,... and so on 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 initiallay the TTL was 64 for the first response and the 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^{th} router the RTT jumped from 3ms to 46ms. So i guess anyone of 2^{nd}, 3^{rd} and 4^{th} router would be the cadidate for bottleneck router.

[Ans: 7]
Yes there are apperared 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





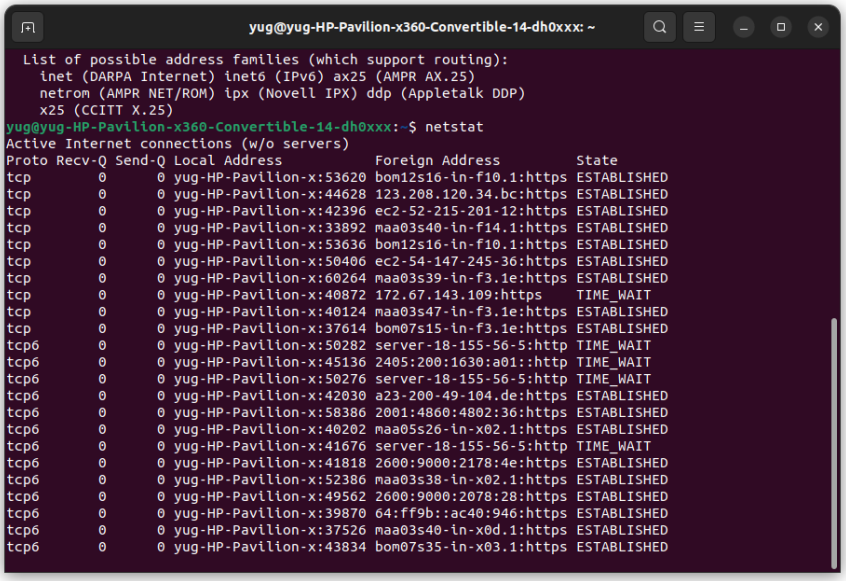
[Ans: Q3]
Average gap between probe packets: 0.98510611538462 ms

[Ans: Q5]
UDP: {1,2.....,18}
ICMP: 51

[Ans: Q6]
Time: 278.223 ms
Bottleneck router: 10^{th} router as the jump is from ~70 ms to ~260 ms

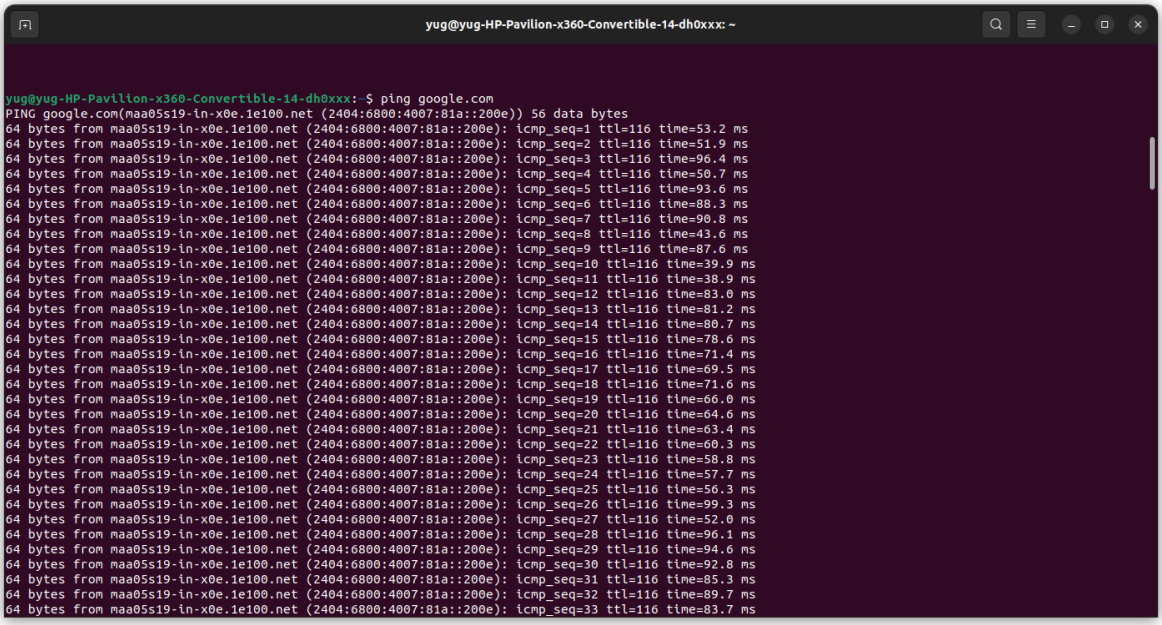
Task: 3

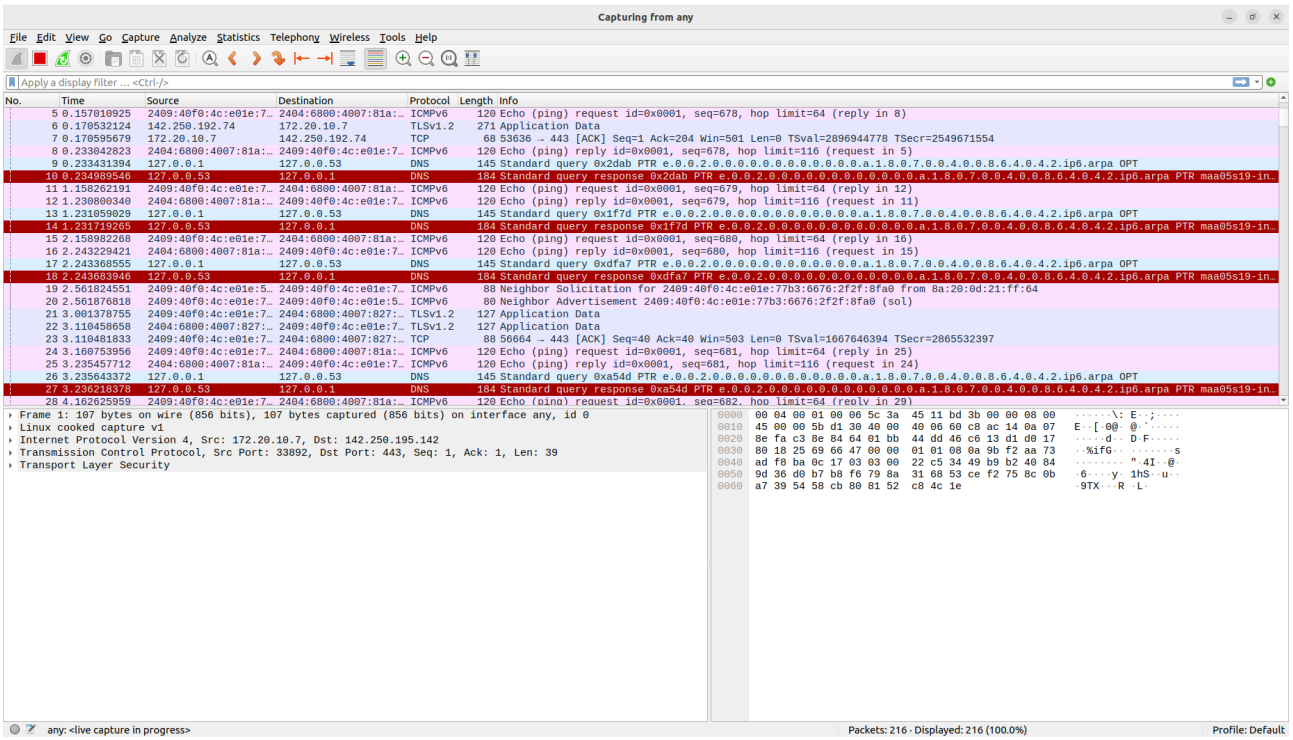
Netstat: netstat command is used to display networking statistics that includes netwrok connection, interface statistics, routing table etc As such there is no direct effect of running netstat command on wireshark



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

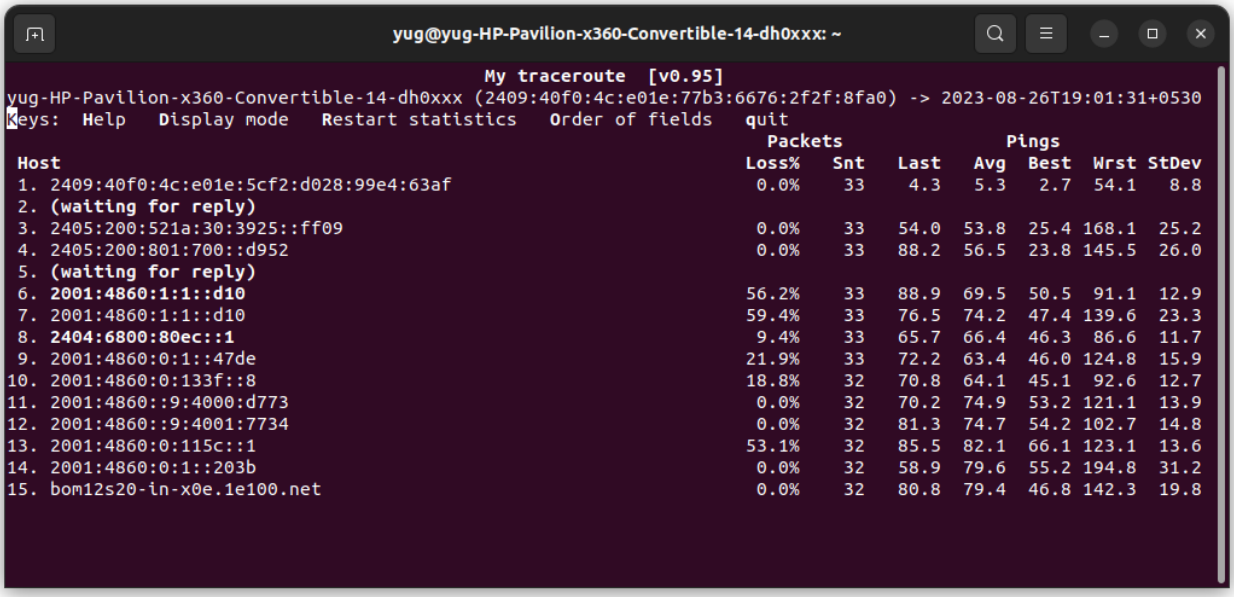
When ping command was hit in terminal then corresponding to each of the request to the another host or server on internet an ICMPv6 request and reply packet was captured from source to destination and destination to source respectively.

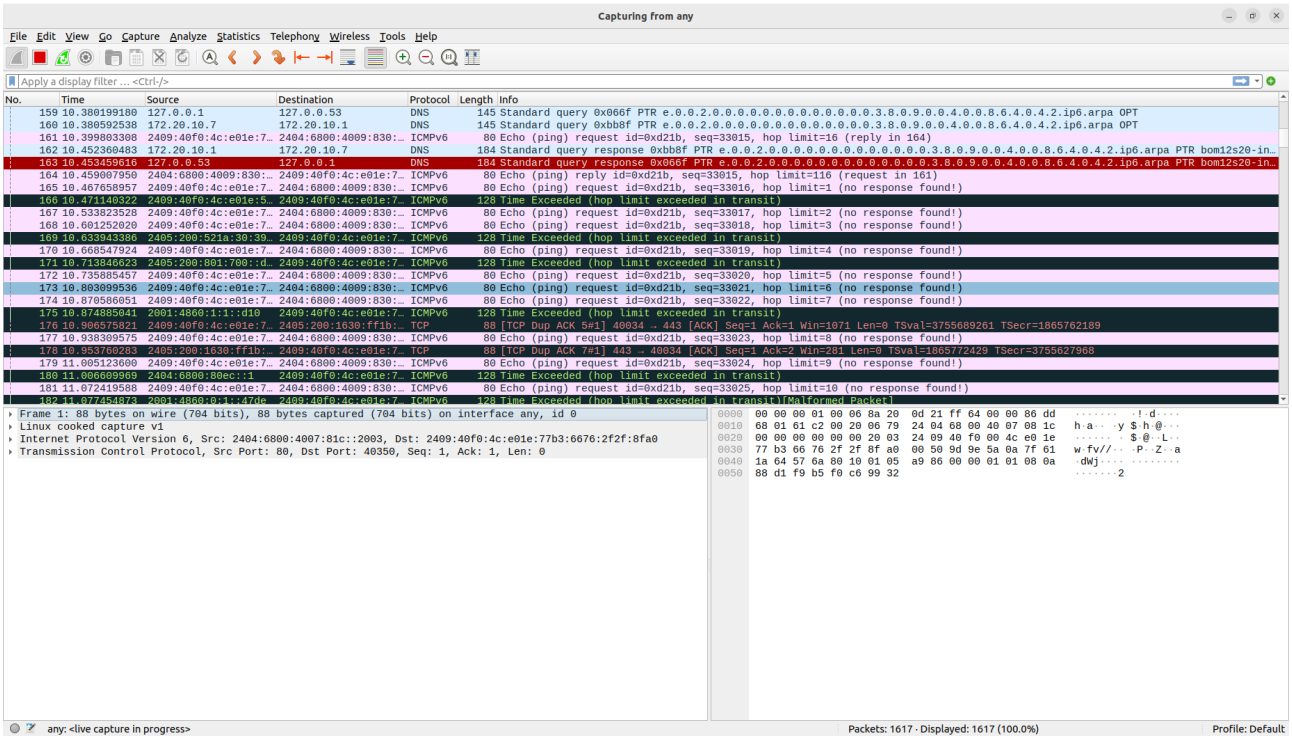




Pink color shows echo ping request and reply

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





Pink color shows echo ping request and reply as a part of mtr request that ultimately translates to traceroute so basically each of the pick entry in above image is a ping echo for each traceroute entry