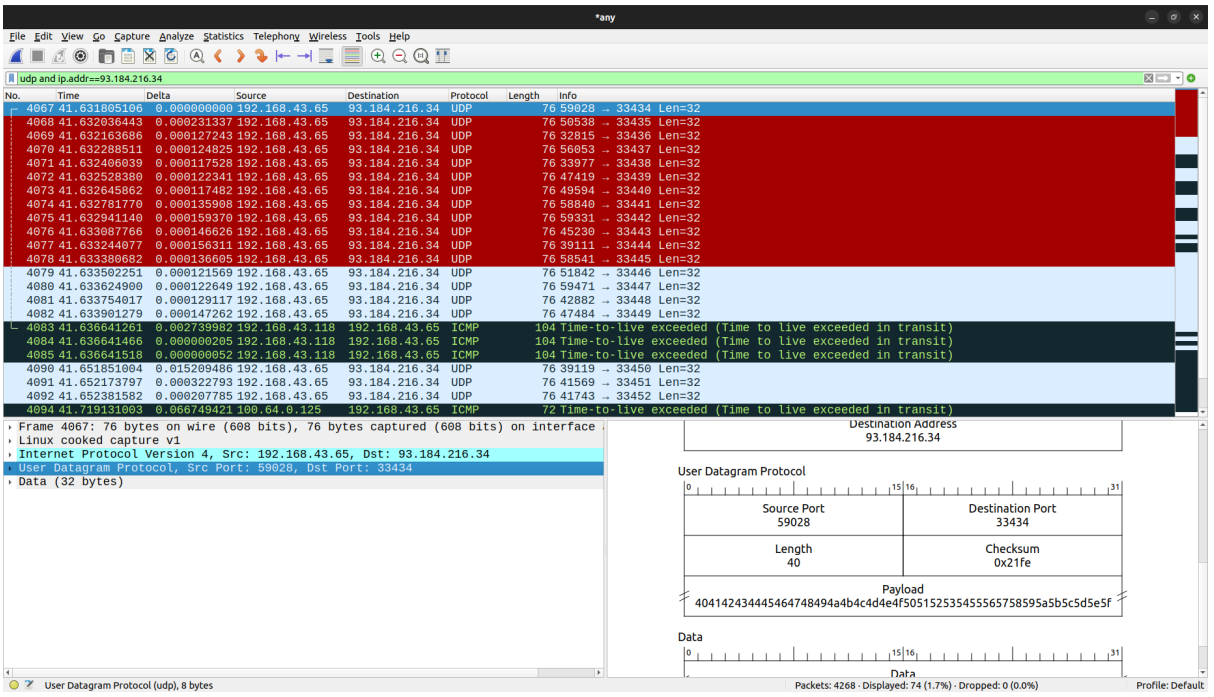
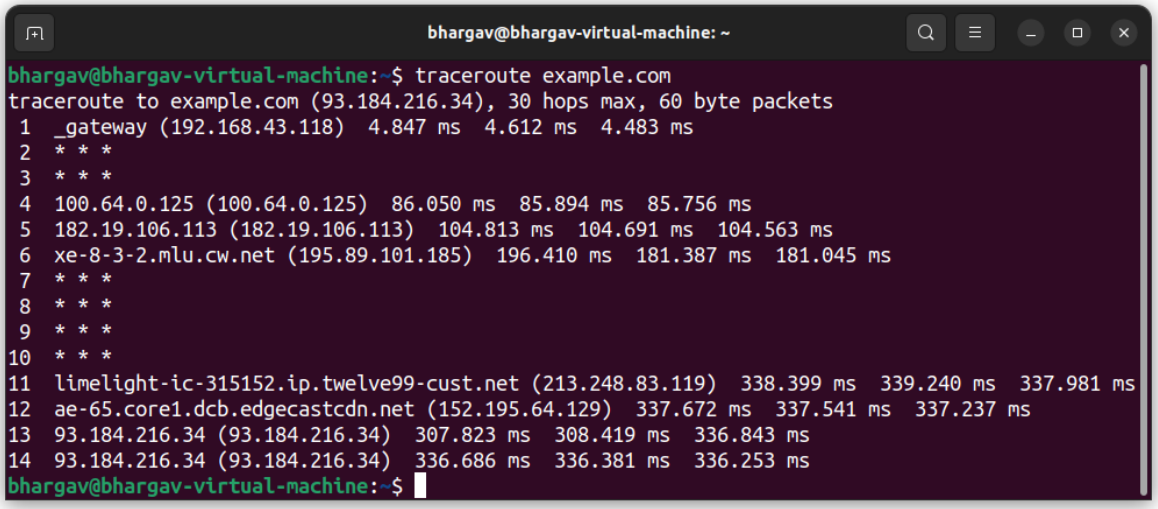
CS23Mtech11026 - Lab assignment 2

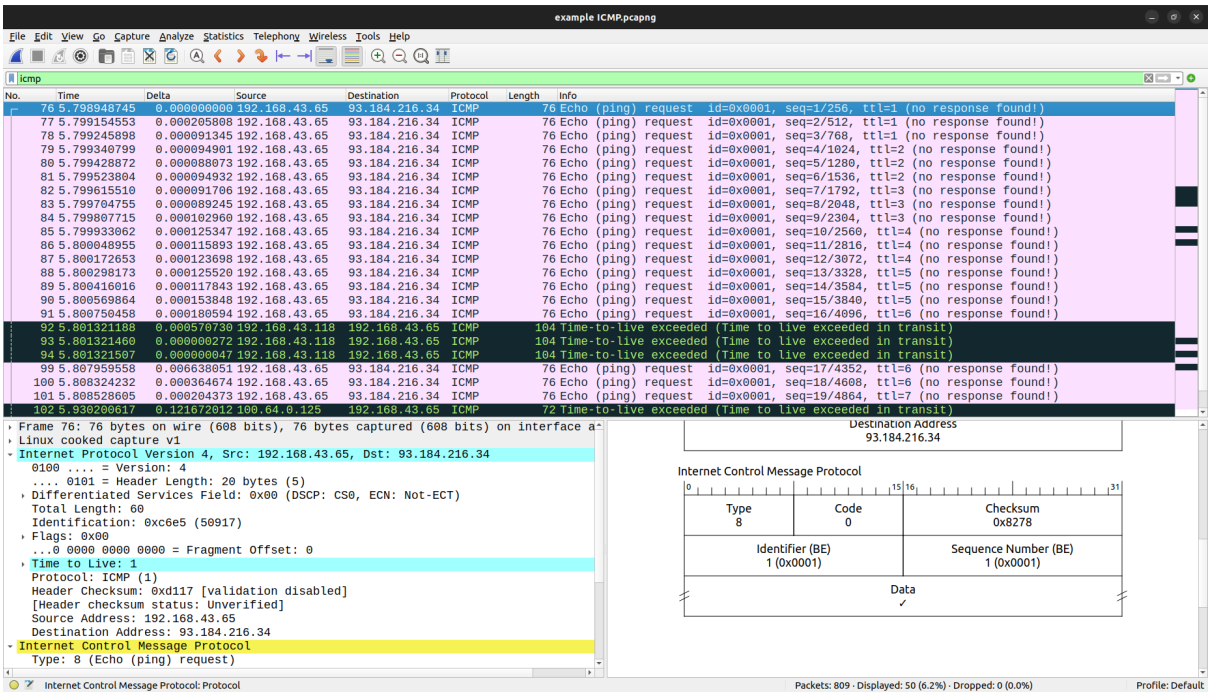
Task-1

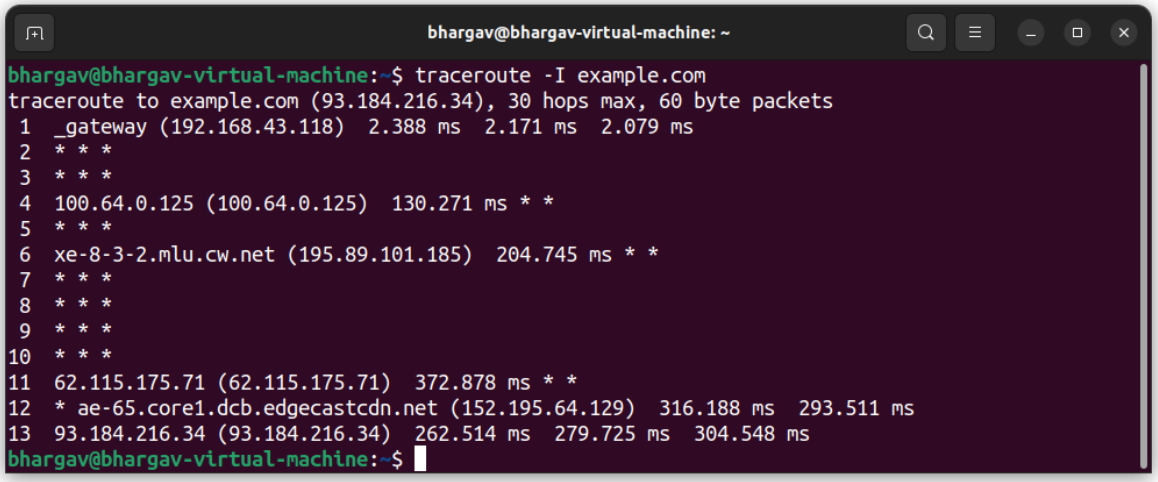
1. The protocol used to send the probe packets is UDP (Default). The key fields & their values are mentioned below.
   - Source IP = 192.168.43.65
   - Destination IP = 93.184.216.34
   - TTL = 1 (TTL 1 for the 1st probe packet, it changes depending on the probe packet you have selected.)
   - Source port = 59028
   - Destination port = 33434





2. Yes we can change the default protocol (UDP) used to send the probe packets. Here I have changed it to ICMP by using the command “traceroute -I example.com“ in Terminal. (I stands for ICMP)

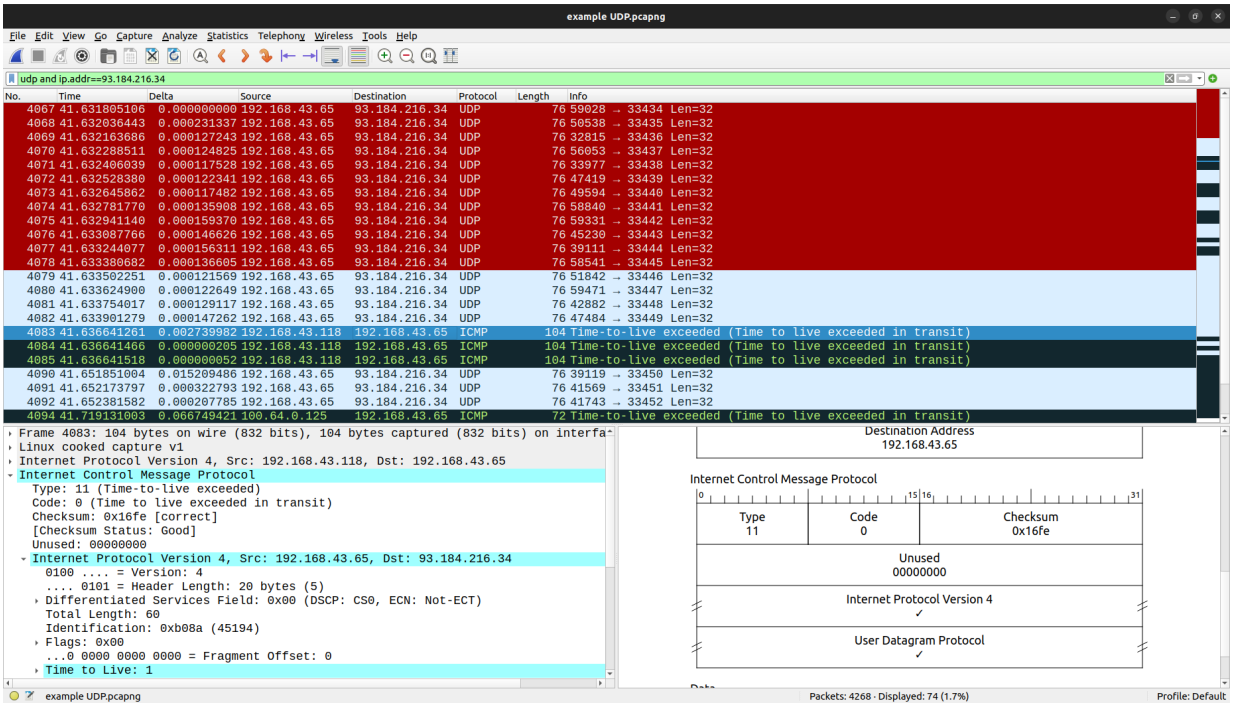


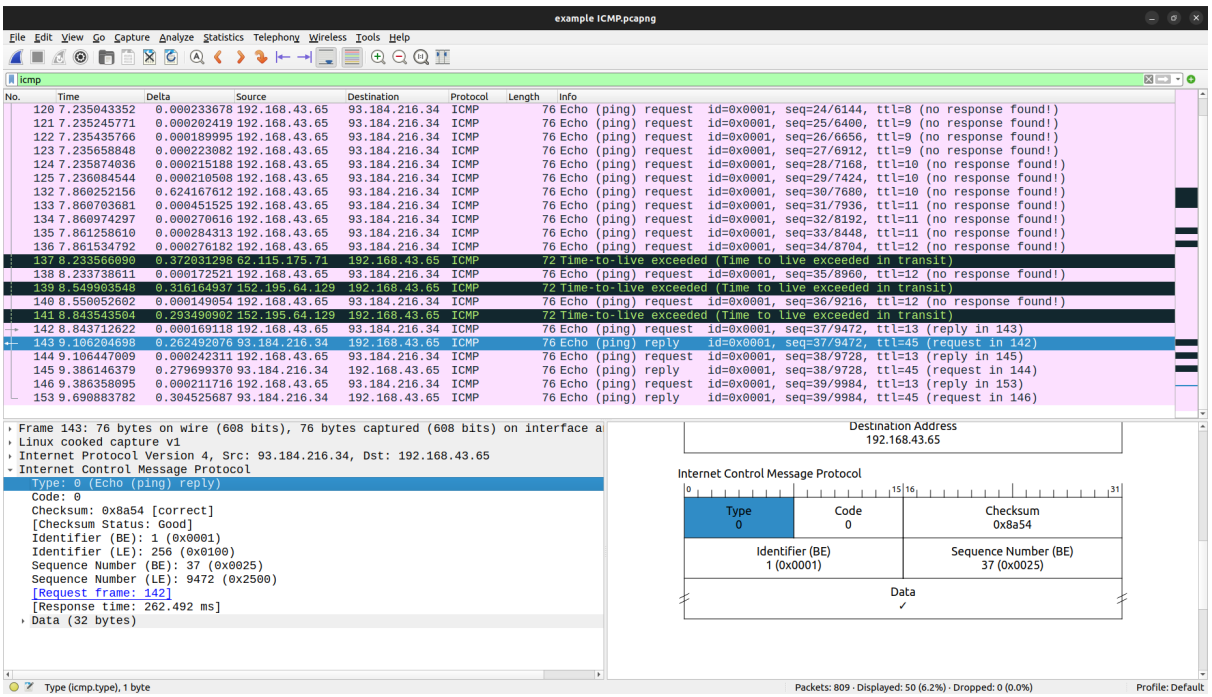


3. The Typical gap (delay) between probe packets when using UDP is 0.1374637813 sec and when using ICMP it is 0.07783870074 sec.
   (The delays given above are the average values.)

4. The response of the probe packet contains the below given fields. Also, The screenshot for the UDP and ICMP protocol used for example.com traceroute response are attached respectively.
    - Source IP address
    - Destination IP address
    - Time To live
    - Protocol used to send the probe
    - Sequence number
    - Response time

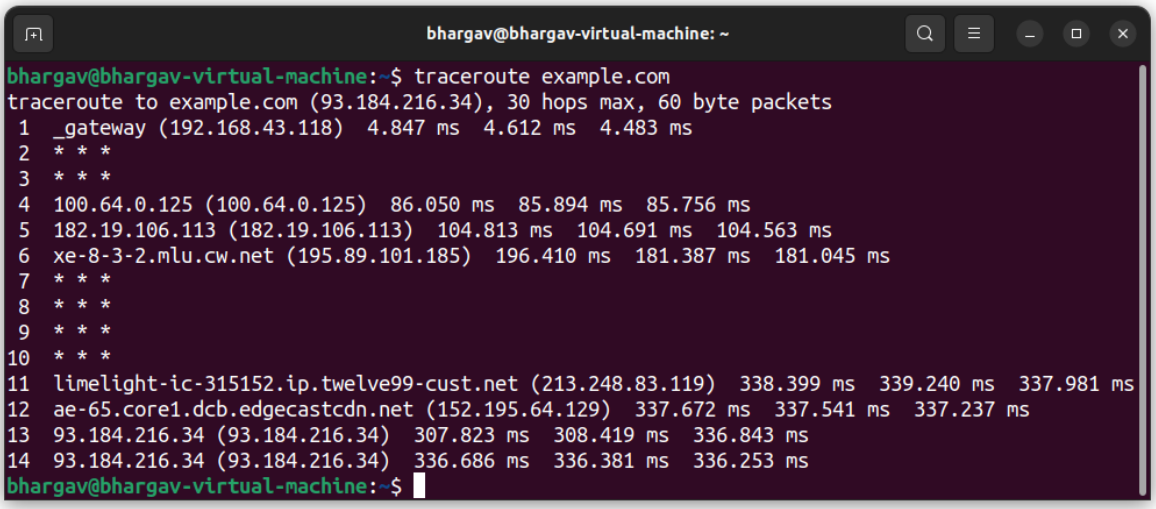
      Etc.



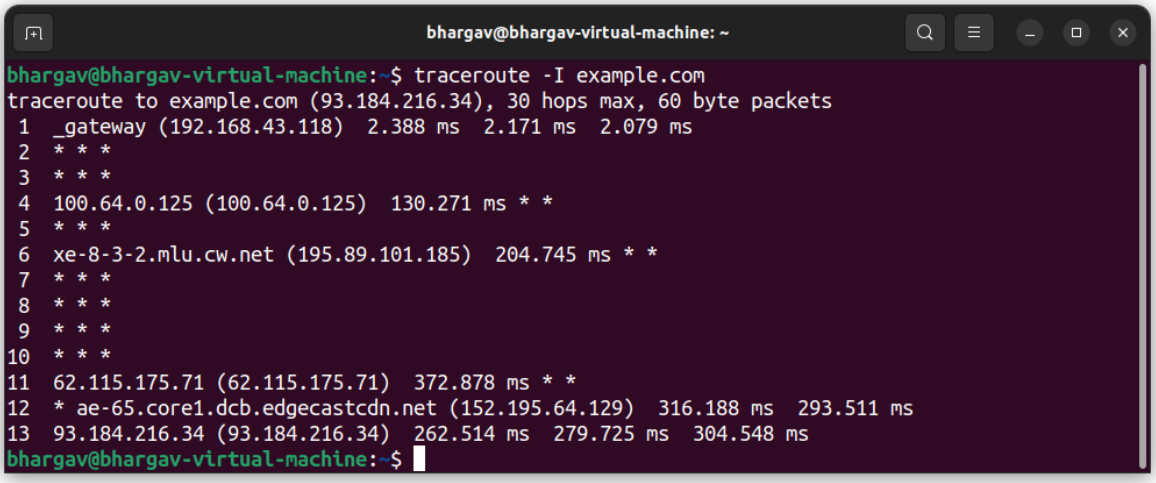


5. The Internet Protocol (IP) contains the Time to live field (TTL). The value of the TTL field is changing according to the probe sent by the host. The TTL is increasing by 1 after every probe until we reach the destination. When the Time to live exceeded transit the value of TTL field in the response are random like 64, 251, 245 etc.

6. Using UDP protocol the total time for the traceroute session is 336.253 ms and the bottleneck router is the 10th router.



And by using ICMP protocol the total time for the traceroute session is 304.548 ms and the bottleneck router is the 8th router.



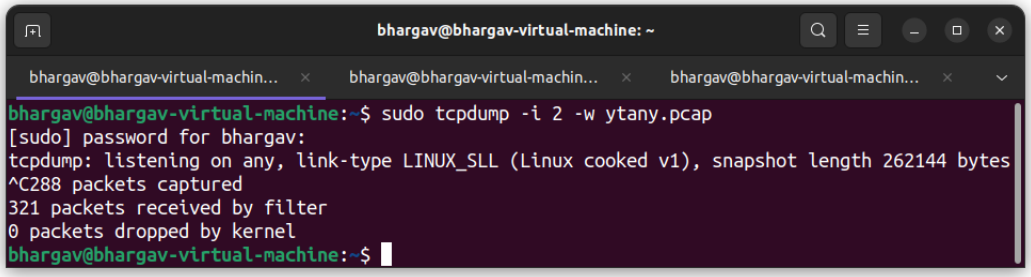
The bottleneck router is found from the wireshark by having the delta time column and by finding the highest gap between the probe packet. Then by finding the TTL of that highest gap probe packet. That would be the no. of the router which is the bottleneck.

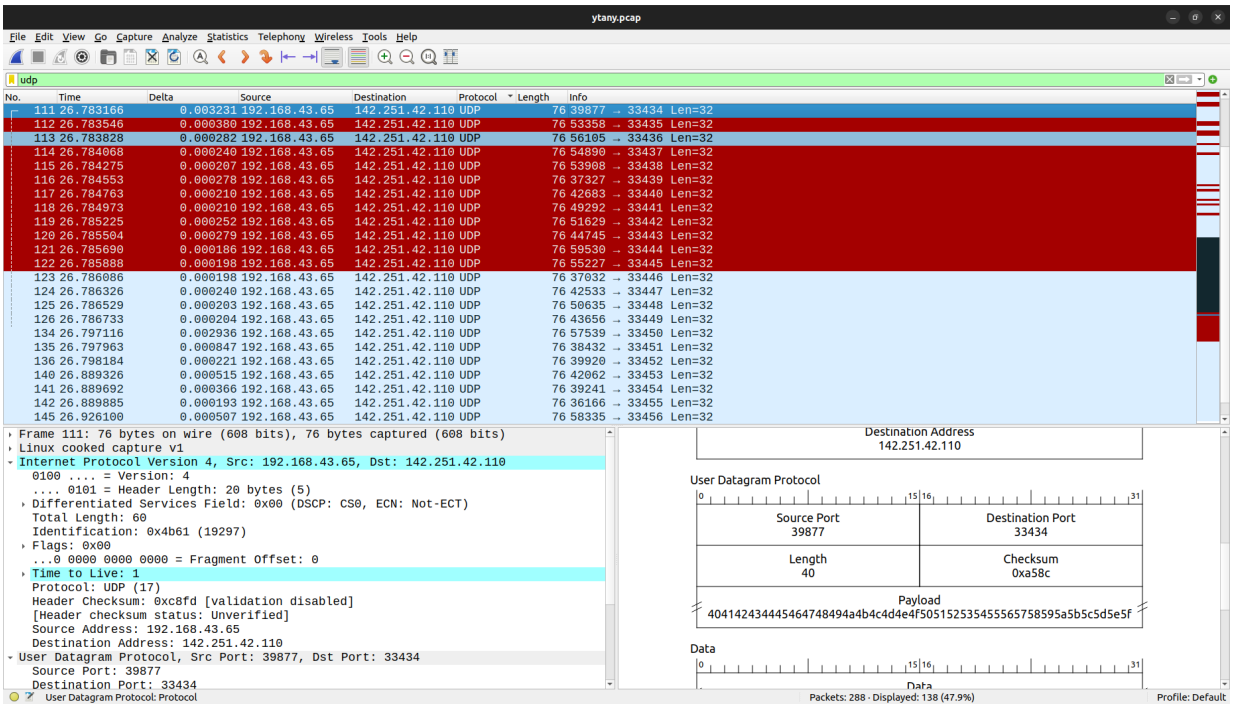
7. Yes there are “*” in the traceroute session done for example.com using UDP and ICMP protocols. The potential reason for “*” to appear are (1) Destination Unreachable (2) Time to live exceeds the transit. Also there are many more reason for “*” to appear as if some router has a personal preference not to respond to certain probes coming from the particular host.

Task - 2 Traceroute session for www.youtube.com

T1 - Q3

By “sudo tcpdump -i 2 -w ytany.pcap” we are using tcpdump instead of wireshark and storing the frames in ytany.pcap file. Here “-i 2” means we are selecting the “any” interface. The typical gap (delay) between the probe packets using tcpdump is 0.0004600444444 sec



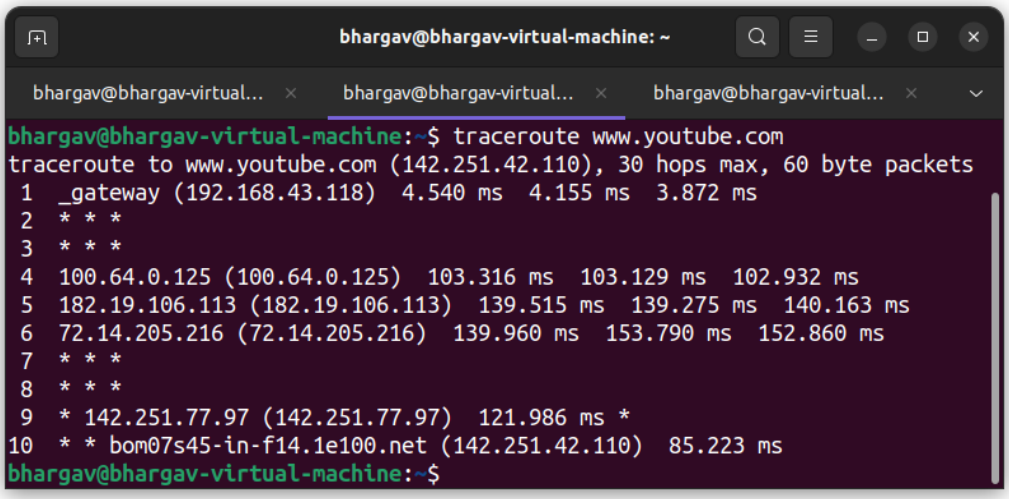


T1 - Q5

The Internet protocol (IP) version 4 has the Time to live field (TTL). The value of TTL for the first probe packet is 1 and then by increasing it by 1 until we reach the destination. For the packets in which the time to live exceeded or destination unreachable have different values.

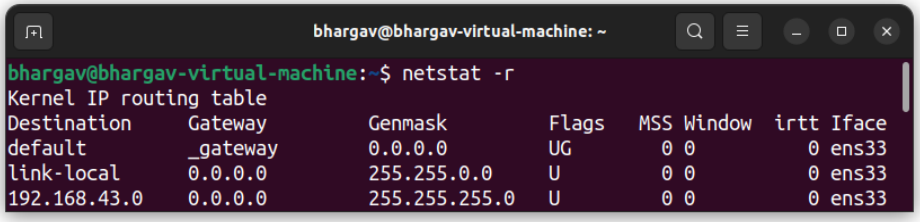
T1 - Q6

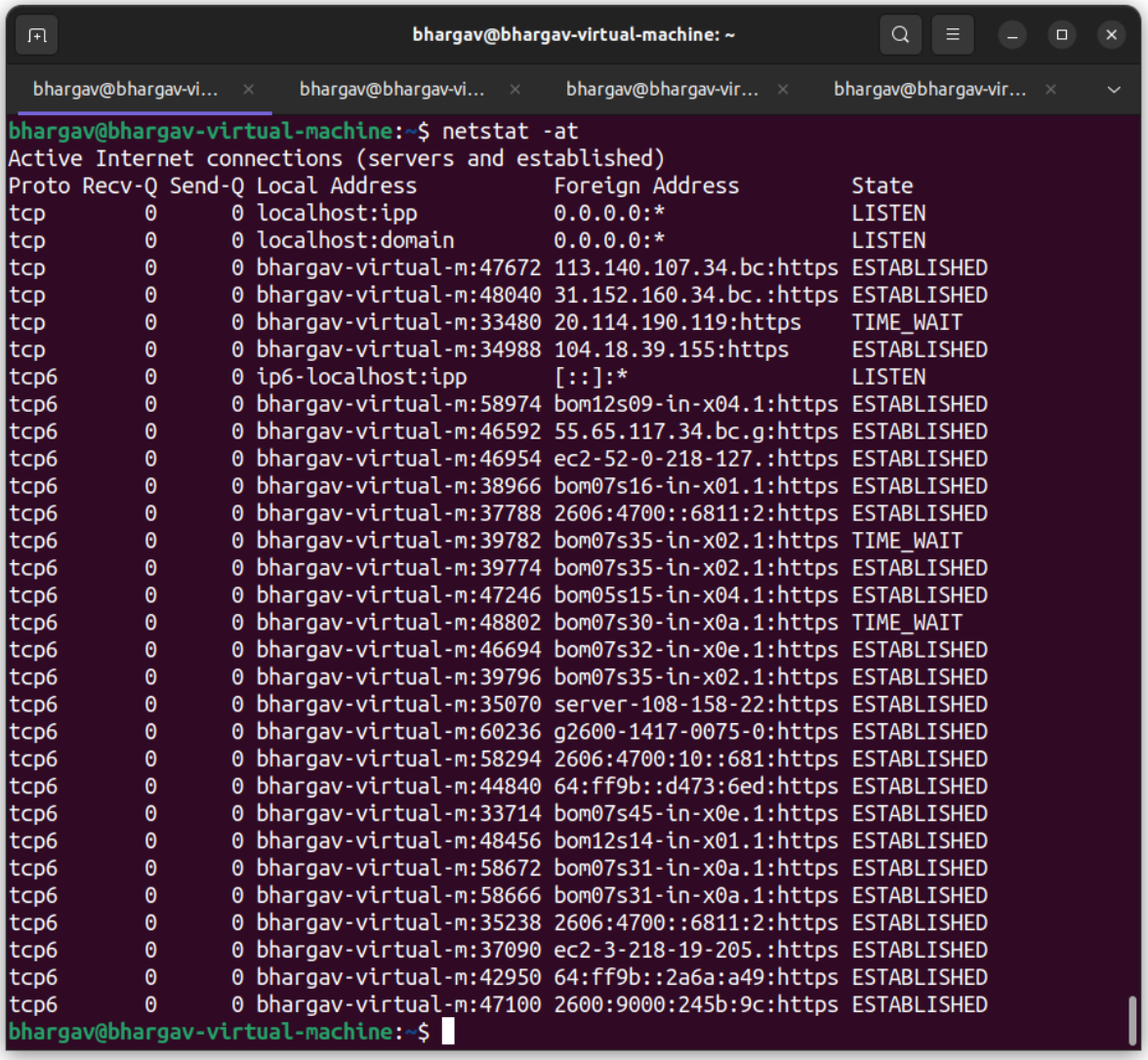
The total time required for the traceroute session is 85.223 ms.
The bottleneck router is the 2nd router.

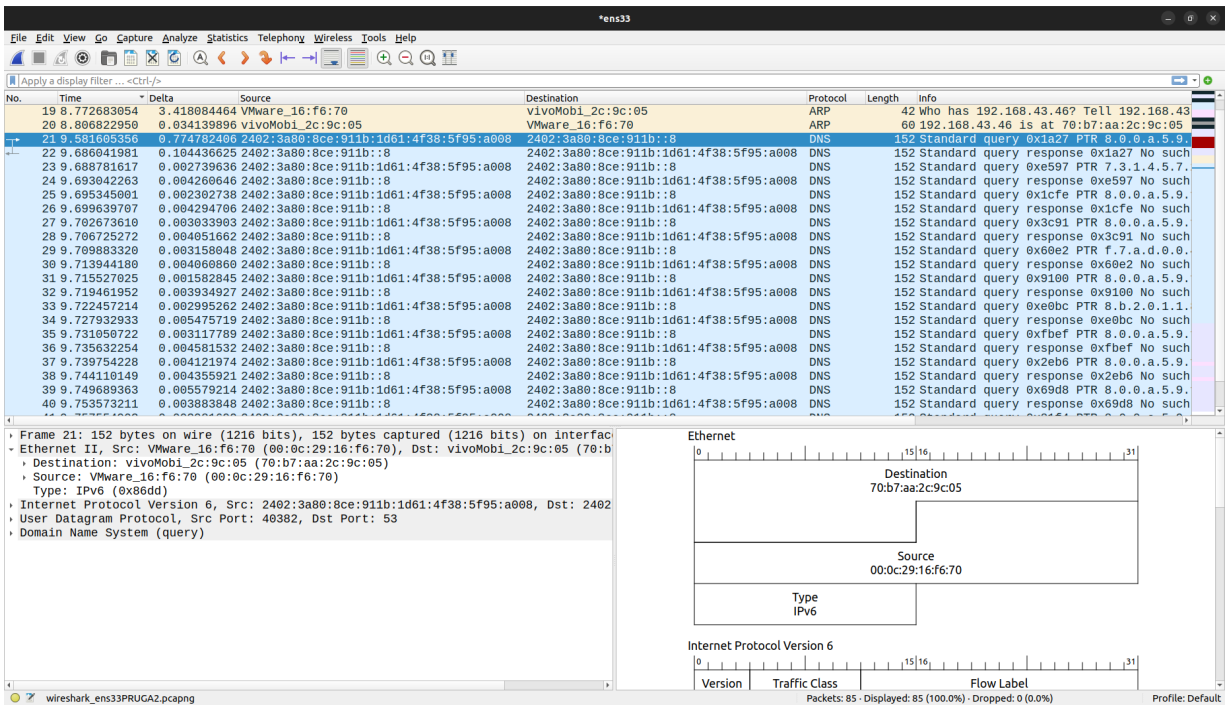


Task - 3

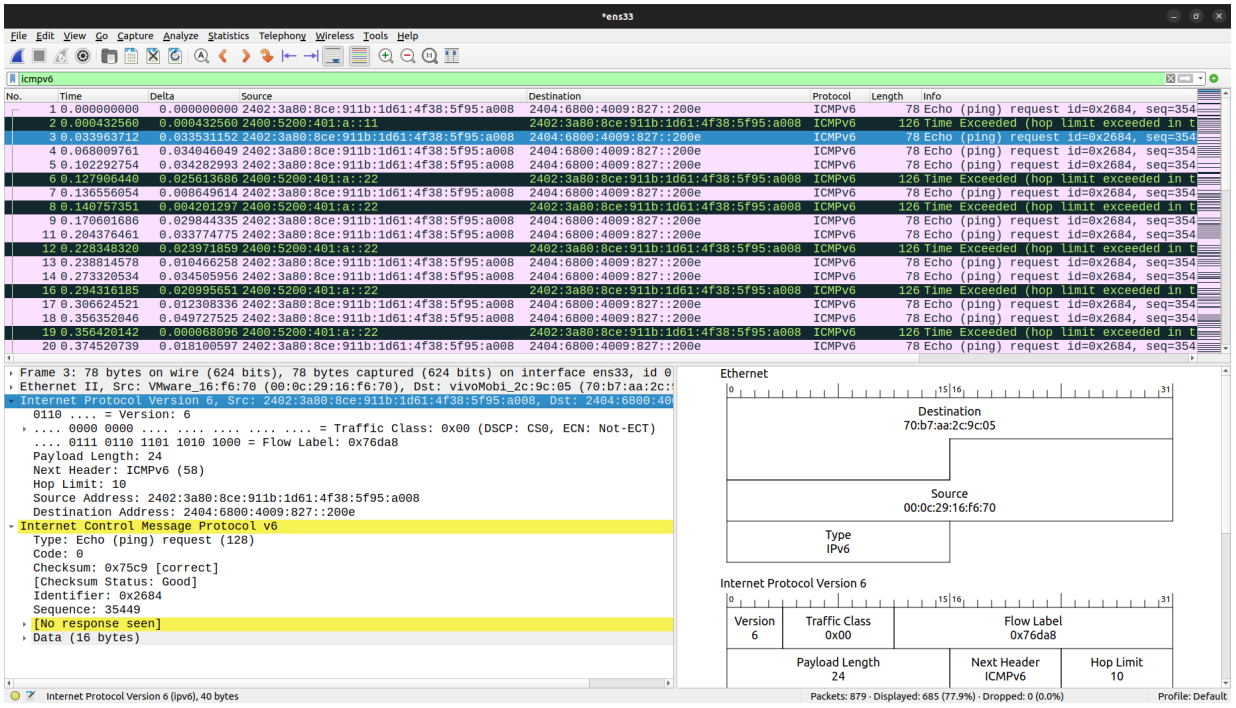
The netstat is used to have statistics about our network like how many TCP connection, UDP connections there are with our computer. Using “netstat -at” shows the all tcp connection similarly for UPD it is “netstat -au”.
As i have internet connection with my mobile “vivo” then when i enter the command “netstat -at” in the terminal and then side by side I have wireshark running with that interface. So the no. of TCP connections show to me in the terminal which are requested by my mobile’s internet connection DNS server and their responses show to me that you have those many TCP connections. The screenshot for the terminal and wireshark are shown below.
The ss is the same as the netstat just it is faster than netstat. We can also have the command for getting the routing table “netstat -r”

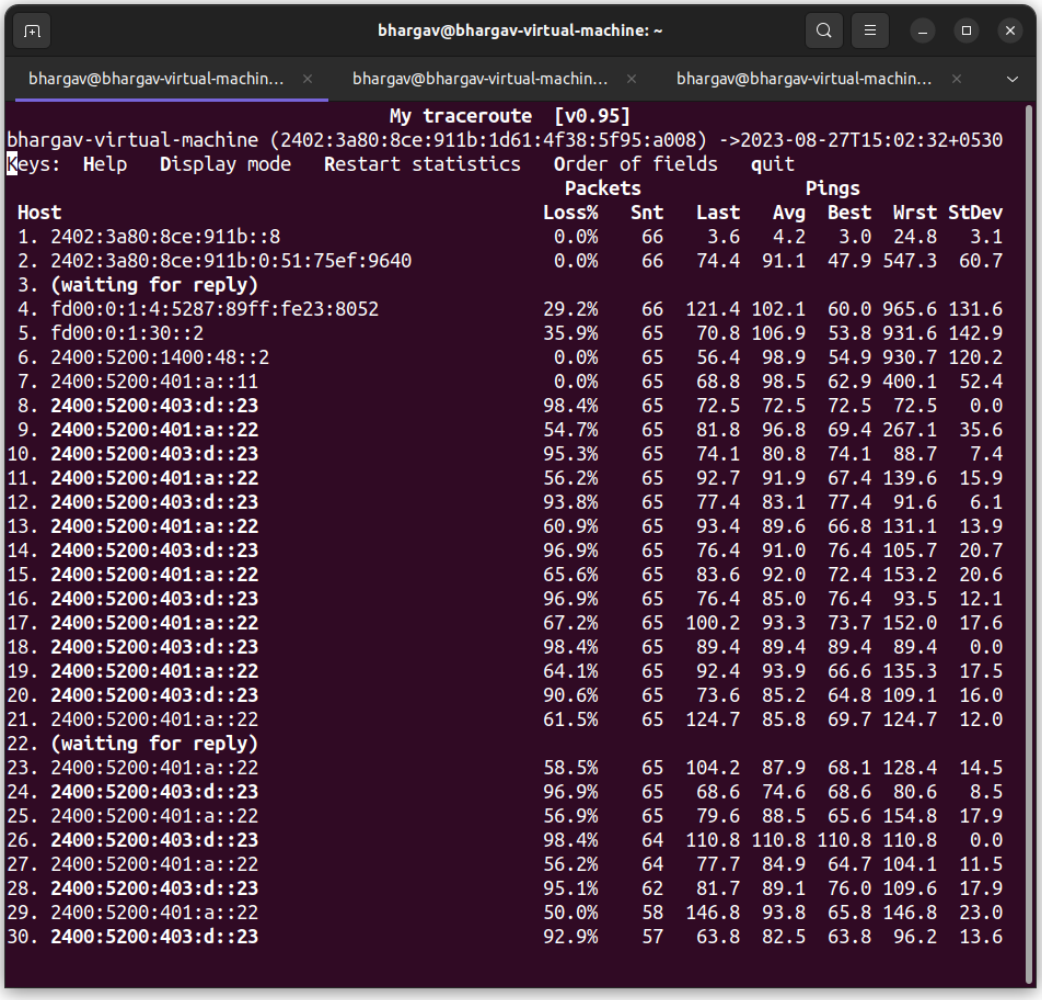



bhargav@bhargav-virtual-machine: ~
bhargav@bhargav-vi...
bhargav@bhargav-vi...
bhargav@bhargav-vir...
bhargav@bhargav-vir...
bhargav@bhargav-virtual-machine:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 localhost:ipp 0.0.0.0:* LISTEN
tcp 0 0 localhost:domain 0.0.0.0:* LISTEN
tcp 0 0 bhargav-virtual-m:47672 113.140.107.34.bc:https ESTABLISHED
tcp 0 0 bhargav-virtual-m:48040 31.152.160.34.bc.:https ESTABLISHED
tcp 0 0 bhargav-virtual-m:33480 20.114.190.119:https TIME_WAIT
tcp 0 0 bhargav-virtual-m:34988 104.18.39.155:https ESTABLISHED
tcp6 0 0 ip6-localhost:ipp [::]:* LISTEN
tcp6 0 0 bhargav-virtual-m:58974 bom12s09-in-x04.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:46592 55.65.117.34.bc.g:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:46954 ec2-52-0-218-127.:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:38966 bom07s16-in-x01.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:37788 2606:4700::6811:2:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:39782 bom07s35-in-x02.1:https TIME_WAIT
tcp6 0 0 bhargav-virtual-m:39774 bom07s35-in-x02.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:47246 bom05s15-in-x04.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:48802 bom07s30-in-x0a.1:https TIME_WAIT
tcp6 0 0 bhargav-virtual-m:46694 bom07s32-in-x0e.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:39796 bom07s35-in-x02.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:35070 server-108-158-22:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:60236 g2600-1417-0075-0:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:58294 2606:4700:10::681:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:44840 64:ff9b::d473:6ed:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:33714 bom07s45-in-x0e.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:48456 bom12s14-in-x01.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:58672 bom07s31-in-x0a.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:58666 bom07s31-in-x0a.1:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:35238 2606:4700::6811:2:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:37090 ec2-3-218-19-205.:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:42950 64:ff9b::2a6a:a49:https ESTABLISHED
tcp6 0 0 bhargav-virtual-m:47100 2600:9000:245b:9c:https ESTABLISHED
bhargav@bhargav-virtual-machine:~$

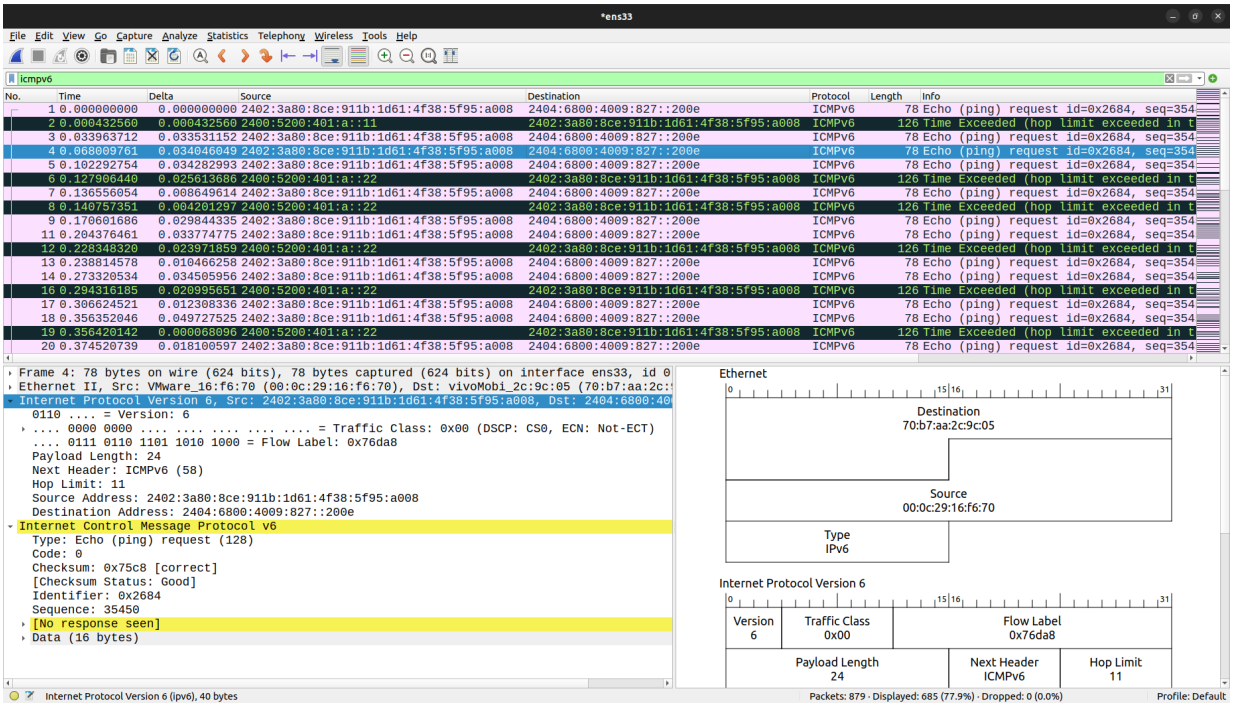

*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Delta Source Destination Protocol Length Info
19 8.772683054 3.418084464 VMware_16:f6:70 vivoMobi_2c:9c:05 ARP 42 Who has 192.168.43.46? Tell 192.168.43
20 8.806822950 0.034139896 vivoMobi_2c:9c:05 VMware_16:f6:70 ARP 60 192.168.43.46 is at 70:b7:aa:2c:9c:05
21 9.581605356 0.774782406 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x1a27 PTR 8.0.0.a.5.9.
22 9.686041981 0.104436625 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x1a27 No such
23 9.688781617 0.002739636 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0xe597 PTR 7.3.1.4.5.7.
24 9.693042263 0.004260646 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0xe597 No such
25 9.695345001 0.002302738 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x1cfe PTR 8.0.0.a.5.9.
26 9.699639707 0.004294706 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x1cfe No such
27 9.702673610 0.003033903 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x3c91 PTR 8.0.0.a.5.9.
28 9.706725272 0.004051662 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x3c91 No such
29 9.709883320 0.003158048 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x60e2 PTR f.7.a.d.0.0.
30 9.713944180 0.004060860 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x60e2 No such
31 9.715527025 0.001582845 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x9100 PTR 8.0.0.a.5.9.
32 9.719461952 0.003934927 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x9100 No such
33 9.722457214 0.002995262 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0xe0bc PTR 8.b.2.0.1.1.
34 9.727932933 0.005475719 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0xe0bc No such
35 9.731050722 0.003117789 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0xfbef PTR 8.0.0.a.5.9.
36 9.735632254 0.004581532 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0xfbef No such
37 9.739754228 0.004121974 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x2eb6 PTR 8.0.0.a.5.9.
38 9.744110149 0.004355921 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x2eb6 No such
39 9.749689363 0.005579214 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 2402:3a80:8ce:911b::8 DNS 152 Standard query 0x69d8 PTR 8.0.0.a.5.9.
40 9.753573211 0.003883848 2402:3a80:8ce:911b::8 2402:3a80:8ce:911b:1d61:4f38:5f95:a008 DNS 152 Standard query response 0x69d8 No such
Frame 21: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interfac
Ethernet II, Src: VMware_16:f6:70 (00:0c:29:16:f6:70), Dst: vivoMobi_2c:9c:05 (70:b
Destination: vivoMobi_2c:9c:05 (70:b7:aa:2c:9c:05)
Source: VMware_16:f6:70 (00:0c:29:16:f6:70)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2402:3a80:8ce:911b:1d61:4f38:5f95:a008, Dst: 2402
User Datagram Protocol, Src Port: 40382, Dst Port: 53
Domain Name System (query)
Ethernet
Destination
70:b7:aa:2c:9c:05
Source
00:0c:29:16:f6:70
Type
IPv6
Internet Protocol Version 6
Version
Traffic Class
Flow Label
wireshark_ens33PRUGA2.pcapng
Packets: 85 · Displayed: 85 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

- Now using mtr for the youtube.com in the terminal we can see the live statistics for the loss, pings for the last packet, for average packet etc.





While using the mtr it is not sending the extra 2 packets like the traceroutes does and that can be seen in the wireshark that one packet has Time to live = 10 then just next packet will have TTL = 11. Here as i have demonstrated this mtr it is using the ICMP version 6.
The below given image has the Hop limit = 11 while the above image which is just the above probe is having hop limit = 10.



Entering the ping command for the youtube.com it has the time exceeded response. As using my mobile network it is able to reach the destination within certain probes hence it is showing the hop limit exceeded.