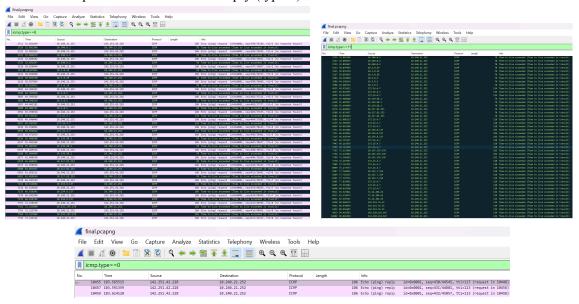
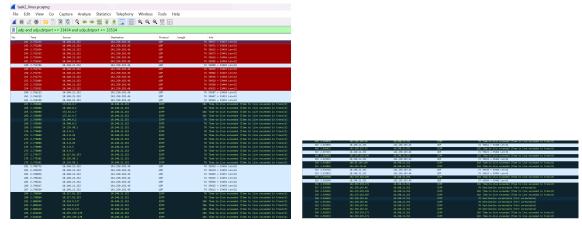
TASK-2

1. What protocol does Windows tracert use by default, and what protocol does Linux traceroute use by default?

Windows tracert uses ICMP Echo Request (ICMP type 8) by default. The probes we send are ICMP Echo Requests, intermediate routers reply with ICMP Time Exceeded (type 11), and the destination replies with ICMP Echo Reply (type 0).



Linux traceroute uses UDP by default. It sends UDP packets to very high port numbers (starting from 33434). Routers on the way reply with ICMP Time Exceeded messages when the packet's TTL runs out. When the packet finally reaches the destination, that computer replies with ICMP Port Unreachable because no program listens to those high-numbered ports.



2. Some hops in your traceroute output may show ***. Provide at least two reasons why a router might not reply.

When traceroute shows *** for a hop, no reply (no valuable ICMP Time Exceeded/ICMP Reply) arrived within the probe timeout for that TTL.

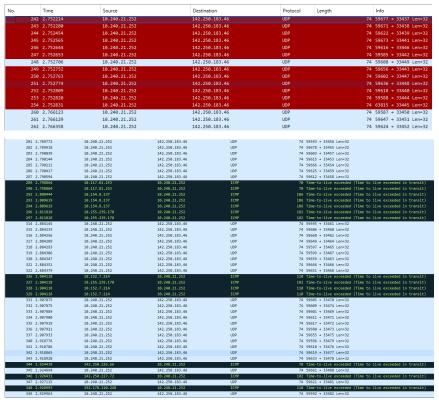
```
● heputhrisha@Thrisha:-$ traceroute go
ogle.com
traceroute to google.com (142.256.183.46), 30 hops max, 60 byte packets
1 Thrisha.mshome.net (172.21.176.1) 1.177 ms 1.157 ms 1.145 ms
2 10.240.0.2 (10.240.6.2) 17.287 ms 17.224 ms 15.997 ms
3 10.3.0.29 (10.3.0.29) 18.965 ms 18.025 ms 18.025 ms
4 10.3.0.29 (10.3.0.29) 18.965 ms 18.025 ms 18.025 ms
5 172.16.4.7 (172.16.4.7) 15.900 ms 16.890 ms 16.890 ms
5 172.16.4.7 (172.16.4.7) 15.900 ms 16.890 ms 16.890 ms
6 14.139.98.1 (14.139.98.1) 16.881 ms 13.747 ms 13.675 ms
7 10.117.81.253 (10.117.81.253) 8.947 ms 19.342 ms 19.253 ms
8 10.154.8.137 (16.154.8.137) 20.678 ms 19.652 ms 20.631 ms
9 10.255.239.170 (10.255.29).700 2.993 ms 22.991 ms 20.533 ms
10 10.152.7.214 (10.152.7.214) 20.384 ms 20.473 ms 20.378 ms
11 ***
12 ***
13 209.85.259.138 (209.85.250.138) 24.658 ms 142.251.70.56 (142.251.70.56) 24.661 ms 142.259.227.72 (142.250.227.72) 18.971 ms
14 142.259.226.66 (142.259.226.66) 16.952 ms 142.259.239.171 (142.259.239.171) 31.878 ms 192.178.110.248 (192.178.110.249) 21.248 ms
16 boml2si1-in-fi4.1e100.net (142.250.183.46) 21.059 ms 142.250.239.171 (142.250.239.371) 31.878 ms 192.178.110.249 (192.178.110.249) 21.228 ms
16 boml2si1-in-fi4.1e100.net (142.250.183.46) 21.059 ms 142.250.239.171) 31.878 ms 192.178.110.199 (192.178.110.249) 21.228 ms
```

The following are the reasons why a router might not reply:

- ICMP Filtering: Some routers are set up to block ICMP Time Exceeded messages. Since traceroute relies on these ICMP replies to identify each hop along the path, blocking them prevents traceroute from learning the router's IP address. As a result, the hop appears as *** instead of showing its actual address.
- Rate Limiting: Routers may use rate limiting, only responding to a few traceroute requests and dropping the rest. This is done to prevent overload. If our probes are dropped, traceroute will show *** even though the router is still working and forwarding traffic.
- **Security Reasons:** Some Internet Service Providers intentionally configure their routers not to respond to traceroute probes. This is done for security reasons, so outside users cannot map the internal network structure. When this happens, we will again see *** instead of the router's IP address.

3. In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?

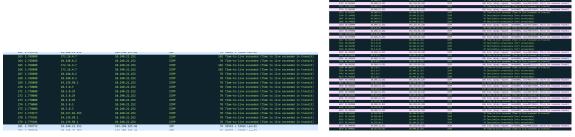
The UDP destination port changes between successive probes. Classic traceroute starts at UDP destination port 33434 and increments the destination port for each probe.



Here, from the above two pictures, in the Info column, there are entries like 59677 -> 33437, 59671 -> 33438, and so on, which show the UDP destination port (the -> 334xy value). These numbers are changing across the probe packets.

4. At the final hop, how is the response different compared to the intermediate hop?

Intermediate hops: Windows tracert and Linux traceroute at the intermediate hops see the same behavior, and the packet's TTL runs out. The router drops the packet and replies with ICMP Time Exceeded (type 11).

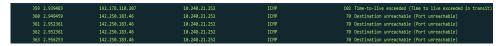


Linux Intermediate hops.

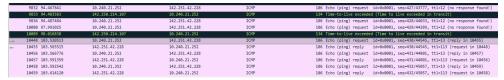
Windows Intermediate hop.

Final hop:

• In Linux traceroute, the destination usually replies with ICMP Destination Unreachable (type 3), because no program listens on the high UDP port. Traceroute recognizes this as "destination reached" and stops.



• In Windows tracert, the destination replies with an ICMP Echo Reply (type 0), since Windows sends ICMP Echo Requests.



- 5. Suppose a firewall blocks UDP traffic but allows ICMP how would this affect the results of Linux traceroute vs. Windows tracert?
 - Linux traceroute: will likely fail or be incomplete. If the firewall blocks UDP probes, those probes never reach the destination, and you will not receive the expected ICMP Destination Unreachable. We will therefore see *** for hops because the replies have not been generated or returned.
 - Windows tracert: will likely succeed, because the firewall allows ICMP. Windows tracert sends ICMP Echo Requests and expects Echo Replies. Since the firewall permits ICMP, we will receive replies, and the path will be discovered.