Assignment 1

CS 331 - Computer Networks

Name 1: Mohit

Roll no: 23110207

Name 2: Tanishq Bhushan Chaudhari

Roll no: 23110329

Date of Submission: 15th September, 2025

Github Repository

Table of Contents

TASK 1 - DNS Resolver

We ran the client and server 3 different times- one in the morning, one in the afternoon and one at night.

Night

Custom header value(HHMMSSID)	Domain name	Resolved IP address
01215400	www.linkedin.com	192.168.1.11
01215401	www.reddit.com	192.168.1.12
01215402	www.facebook.com	192.168.1.13
01215403	www.bing.com	192.168.1.14
01215404	www.example.com	192.168.1.15
01215405	www.wikipedia.org	192.168.1.11
01215406	www.github.com	192.168.1.12

Morning

Custom header value(HHMMSSID)	Domain name	Resolved IP address
04210100	www.linkedin.com	192.168.1.1
04210101	www.reddit.com	192.168.1.2
04210102	www.facebook.com	192.168.1.3
04210103	www.bing.com	192.168.1.4
04210104	www.example.com	192.168.1.5
04210105	www.wikipedia.org	192.168.1.1
04210106	www.github.com	192.168.1.2

Afternoon

Custom header value(HHMMSSID)	Domain name	Resolved IP address
14222600	www.linkedin.com	192.168.1.6
14222601	www.reddit.com	192.168.1.7
14222602	www.facebook.com	192.168.1.8
14222603	www.bing.com	192.168.1.9
14222604	www.example.com	192.168.1.10
14222605	www.wikipedia.org	192.168.1.6
14222606	www.github.com	192.168.1.7

TASK 2 - Traceroute Protocol Behavior

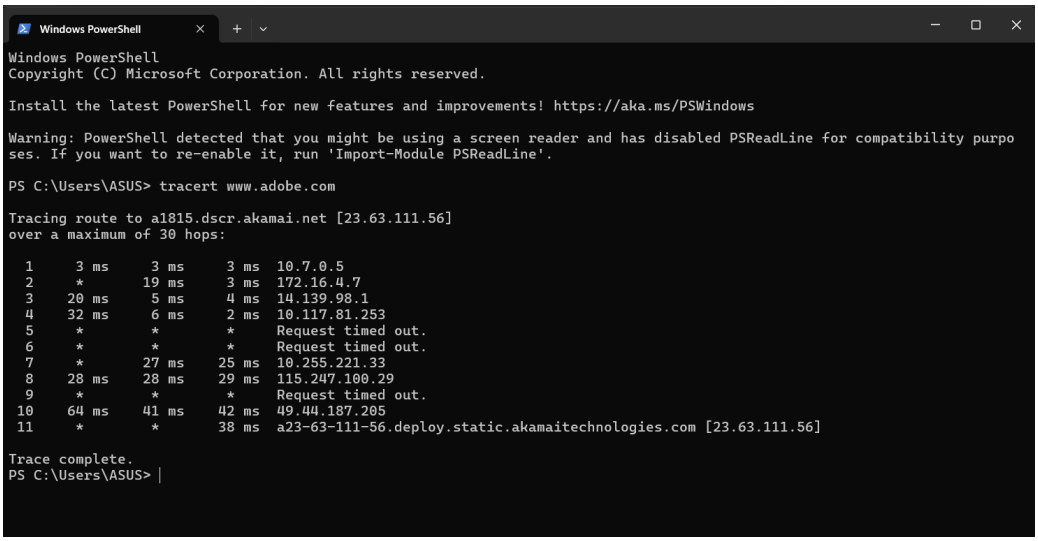
OSes Chosen: Windows and Linux

Website Traced: www.adobe.com

Purpose

The purpose of this task is to understand how the traceroute utility works in different operating systems.

Procedure

- Windows
  - Open Wireshark and select Wifi.
  - Open the terminal and run the command: tracert www.adobe.com
  - Upon completion of this tracing, stop the packet capturing and save the .pcapng file.
  - 

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

Warning: PowerShell detected that you might be using a screen reader and has disabled PSReadLine for compatibility purpo
ses. If you want to re-enable it, run 'Import-Module PSReadLine'.

PS C:\Users\ASUS> tracert www.adobe.com

Tracing route to a1815.dscr.akamai.net [23.63.111.56]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  10.7.0.5
  2     *       19 ms     3 ms  172.16.4.7
  3    20 ms     5 ms     4 ms  14.139.98.1
  4    32 ms     6 ms     2 ms  10.117.81.253
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *       27 ms    25 ms  10.255.221.33
  8    28 ms    28 ms    29 ms  115.247.100.29
  9     *        *        *     Request timed out.
 10    64 ms    41 ms    42 ms  49.44.187.205
 11     *        *       38 ms  a23-63-111-56.deploy.static.akamaitechnologies.com [23.63.111.56]

Trace complete.
PS C:\Users\ASUS>
```

- Linux
  - Open Wireshark and select wlan0.
  - Open the terminal and run the command: traceroute www.adobe.com
  - Upon completion of this tracing, stop the packet capturing and save the .pcapng file.

-
```
❯ traceroute www.adobe.com
traceroute to www.adobe.com (23.63.111.56), 30 hops max, 60 byte packets
 1  10.1.144.3 (10.1.144.3)  4.288 ms  4.140 ms  4.104 ms
 2  172.16.4.7 (172.16.4.7)  2.623 ms  2.593 ms  2.562 ms
 3  14.139.98.1 (14.139.98.1)  6.697 ms  6.667 ms  6.638 ms
 4  10.117.81.253 (10.117.81.253)  3.934 ms  3.871 ms  3.840 ms
 5  * * *
 6  * * *
 7  10.255.221.33 (10.255.221.33)  25.348 ms 10.255.222.33 (10.255.222.33)  24.088 ms  23.994 ms
 8  115.247.100.29 (115.247.100.29)  36.769 ms  37.845 ms  36.734 ms
 9  * * *
10  49.44.187.205 (49.44.187.205)  42.001 ms  56.950 ms  48.700 ms
11  a23-63-111-56.deploy.static.akamaitechnologies.com (23.63.111.56)  35.186 ms  34.794 ms  34.863 ms
```

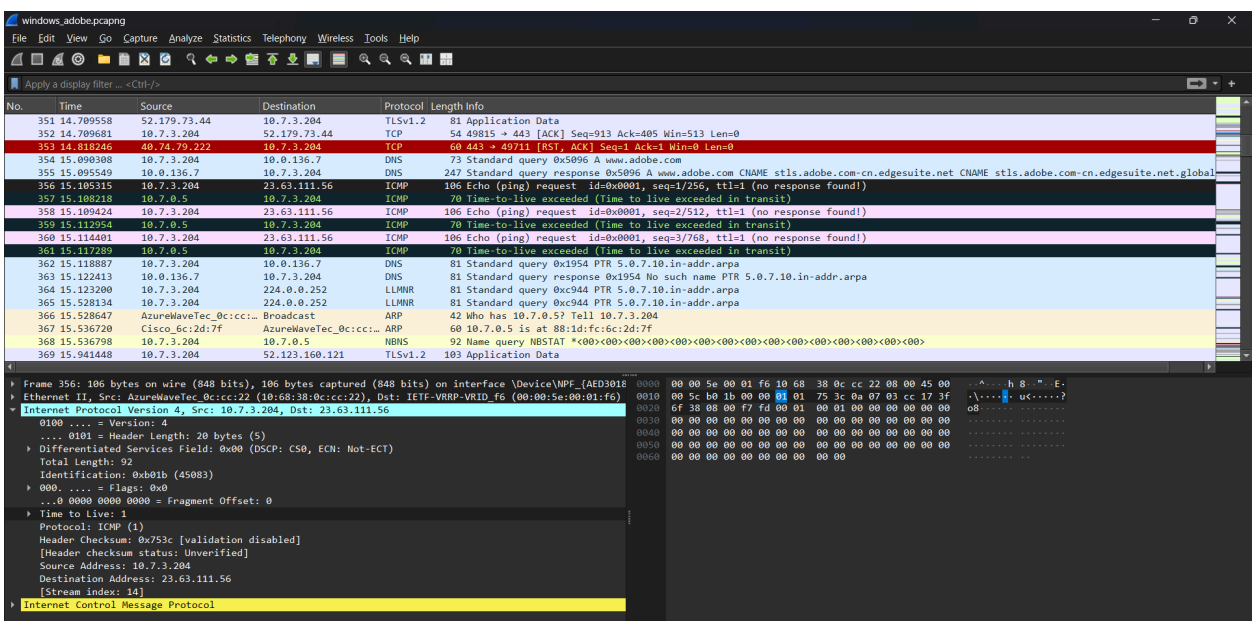
Questions

Q1.

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

Ans.

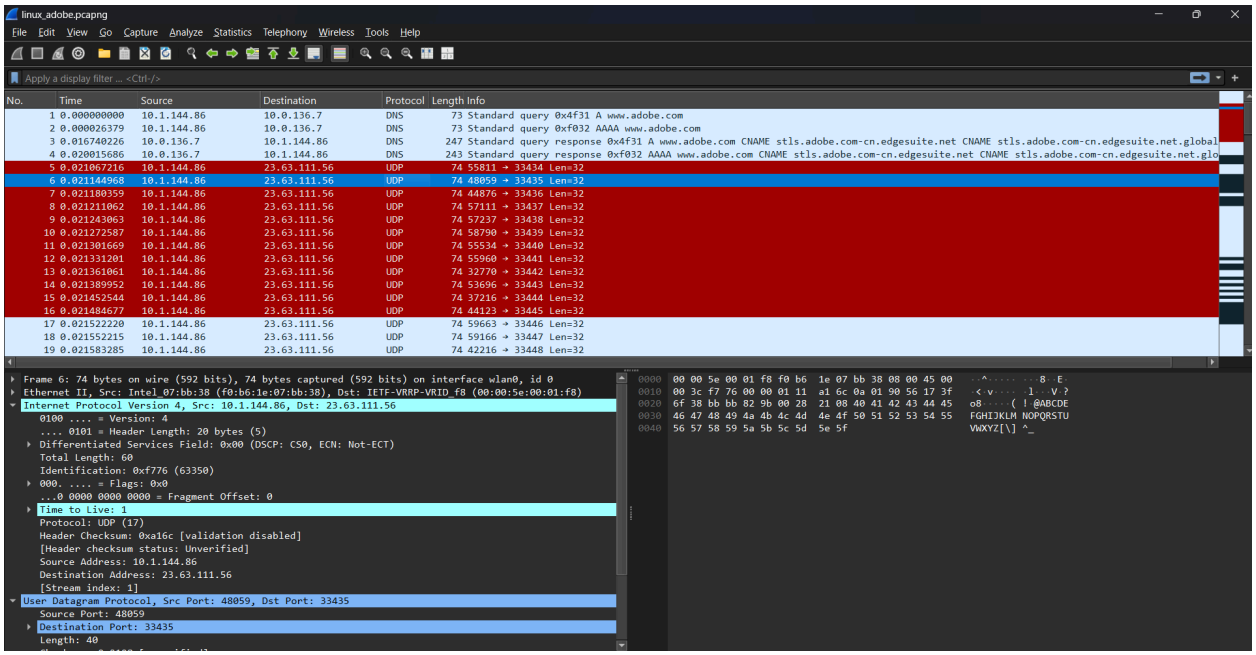
Windows tracert uses the ICMP protocol by default. I found this by looking at the packets in the pcap file and noticing that a sequence of ICMP Echo Request packets was being sent with TTL values increasing one by one, which is the typical behavior of tracert. This pattern helped me identify that these packets were generated by tracert and not just a normal ping. The following image shows the first such sequence with TTL=1(the one packet selected in black colour and the 5 packets that follow it).



- I see ICMP Echo Request packets going out (under Internet Control Message Protocol → Echo (ping) request).

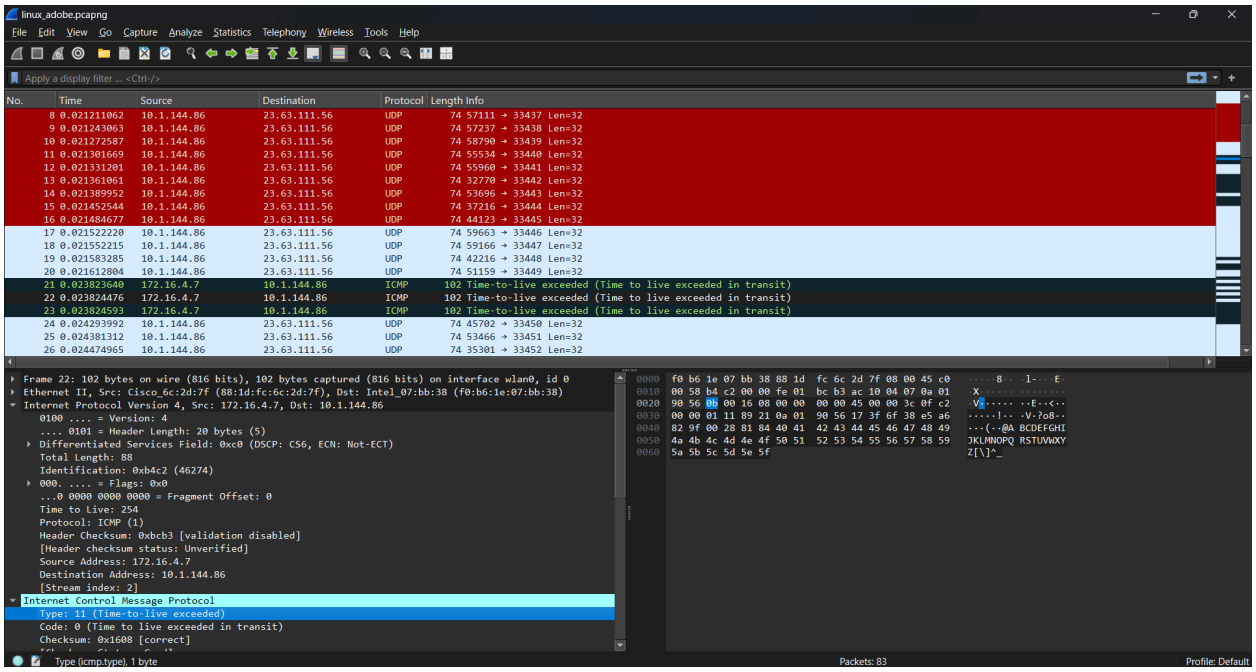
- Intermediate routers reply with ICMP (Time-to-leave exceeded) messages.
- At the final hop, the destination sends an ICMP Echo Reply.

Linux traceroute uses the UDP protocol by default. I found this by looking at the packets in the pcap file and noticing that a sequence of UDP packets was being sent to destination ports starting from 33434 and increasing with each probe, along with TTL values increasing one by one. This repeating pattern is characteristic of traceroute and helped me identify these packets as coming from the traceroute command. The following image shows the second packet with TTL=1. (Its destination port is 33435.)



- I see UDP packets going out with destination ports beginning at 33434.
- Intermediate routers reply with ICMP (Time-to-live exceeded) messages.
- At the final hop, the destination replies with an ICMP Destination Unreachable message.

The following image shows the first sequence of IMCP replies.

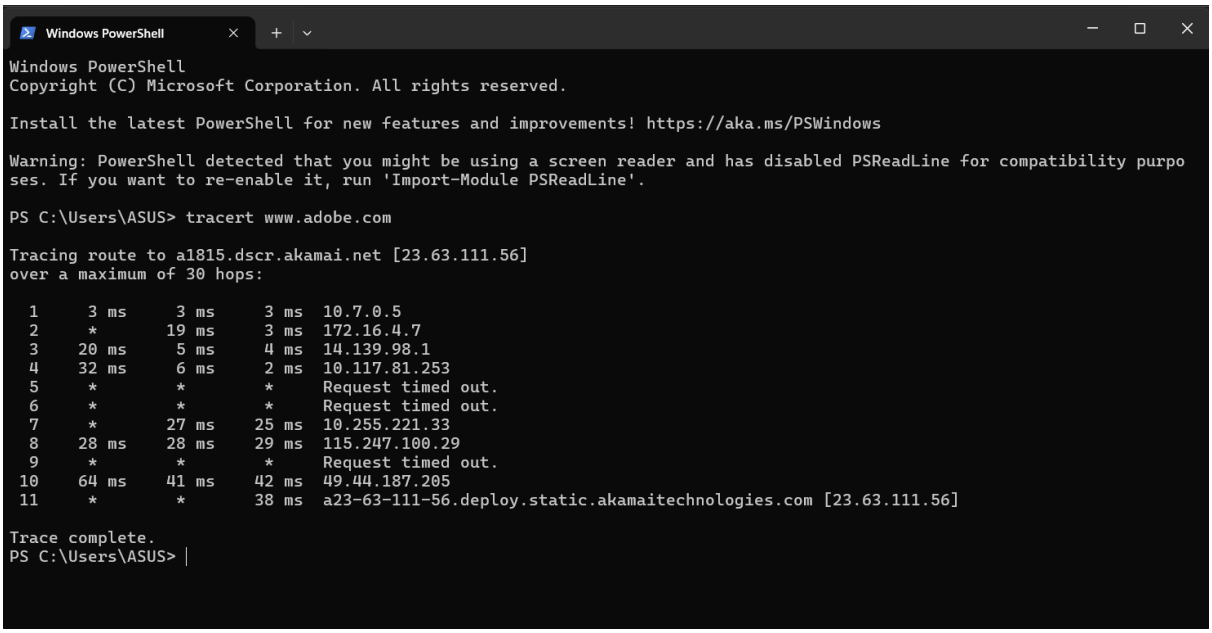


Q2

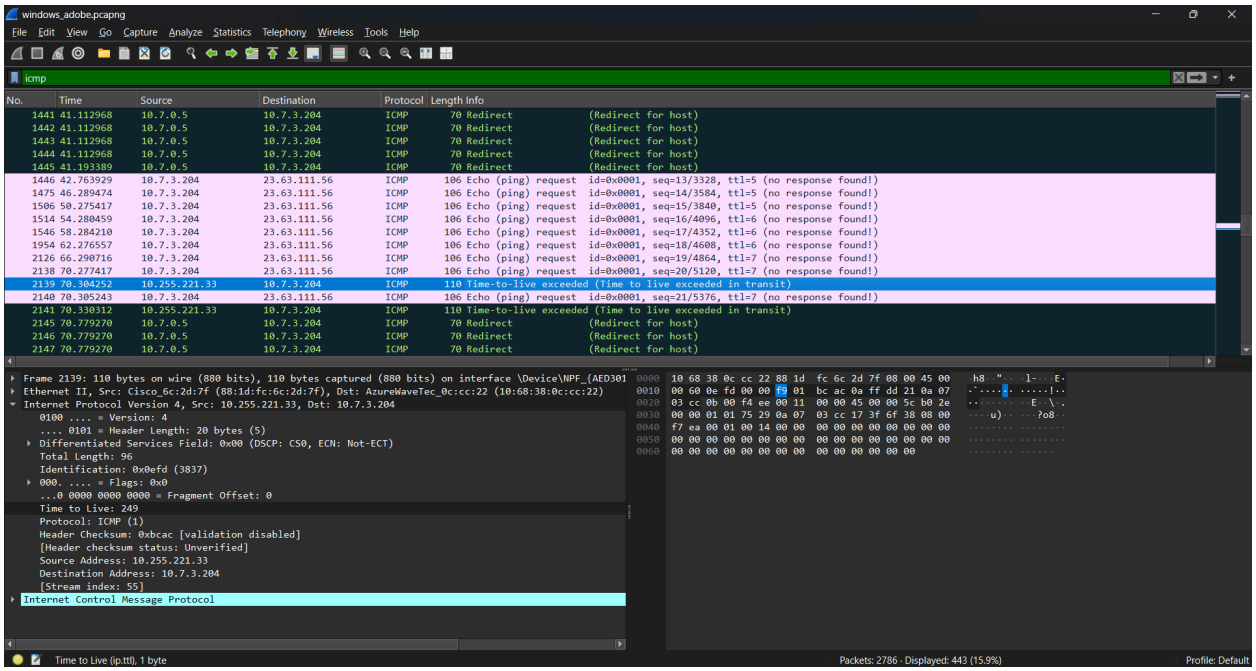
Some hops in your traceroute output may show ***. Provide at least two reasons why a router might not reply.

Ans.

The terminal on both Linux and Windows showed *** for hops 5, 6 and 9 while tracing packets.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

Warning: PowerShell detected that you might be using a screen reader and has disabled PSReadLine for compatibility purpo
ses. If you want to re-enable it, run 'Import-Module PSReadLine'.

PS C:\Users\ASUS> tracert www.adobe.com

Tracing route to a1815.dscr.akamai.net [23.63.111.56]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  10.7.0.5
  2     *       19 ms     3 ms  172.16.4.7
  3    20 ms     5 ms     4 ms  14.139.98.1
  4    32 ms     6 ms     2 ms  10.117.81.253
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *       27 ms    25 ms  10.255.221.33
  8    28 ms    28 ms    29 ms  115.247.100.29
  9     *        *        *     Request timed out.
 10    64 ms    41 ms    42 ms  49.44.187.205
 11     *        *       38 ms  a23-63-111-56.deploy.static.akamaitechnologies.com [23.63.111.56]

Trace complete.
PS C:\Users\ASUS>
```



Looking at the .pcapng, I see the probe packets going out, but no ICMP reply comes back for those hops. The routers were not faulty because later probes reached their destination, which was confirmed by their replies.

Possible reasons:

- Some routers/firewalls block or drop ICMP/UDP responses, so the probes never return and traceroute shows *.
- Routers may rate-limit ICMP replies or be configured not to send TTL-expired responses, which also leads to *.

Since hops 5, 6, and 9 dropped in both Windows and Linux, the most likely reason is suppression or blocking at those routers.

Q3

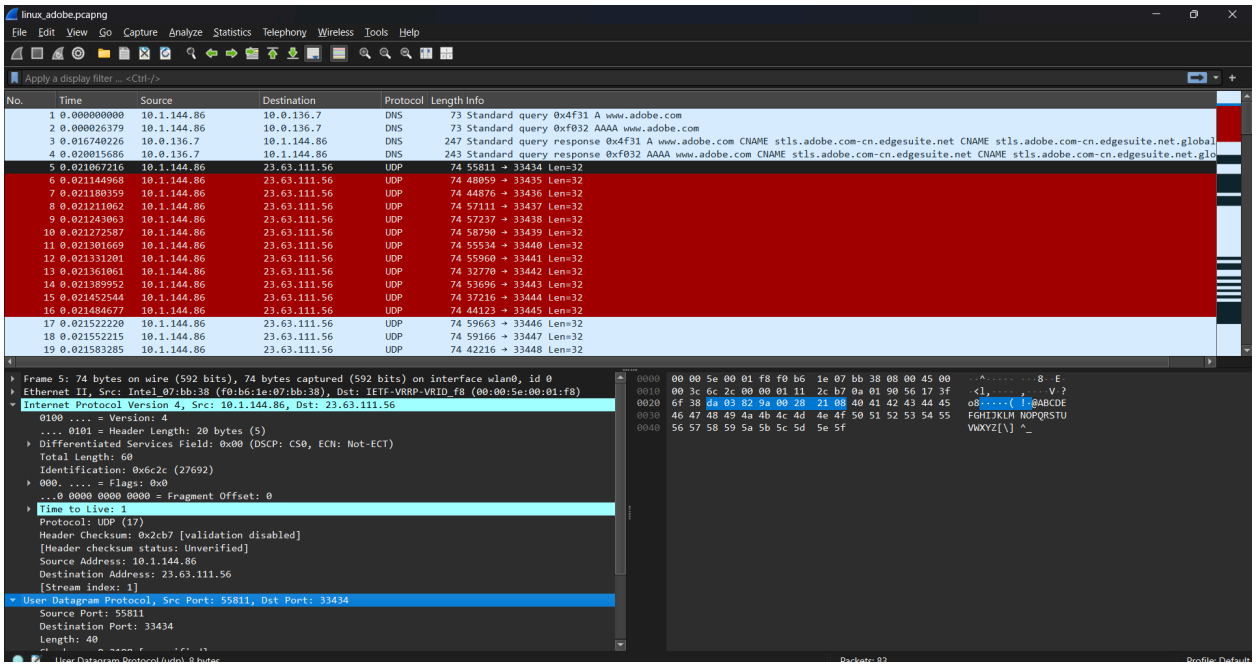
In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?

Ans.

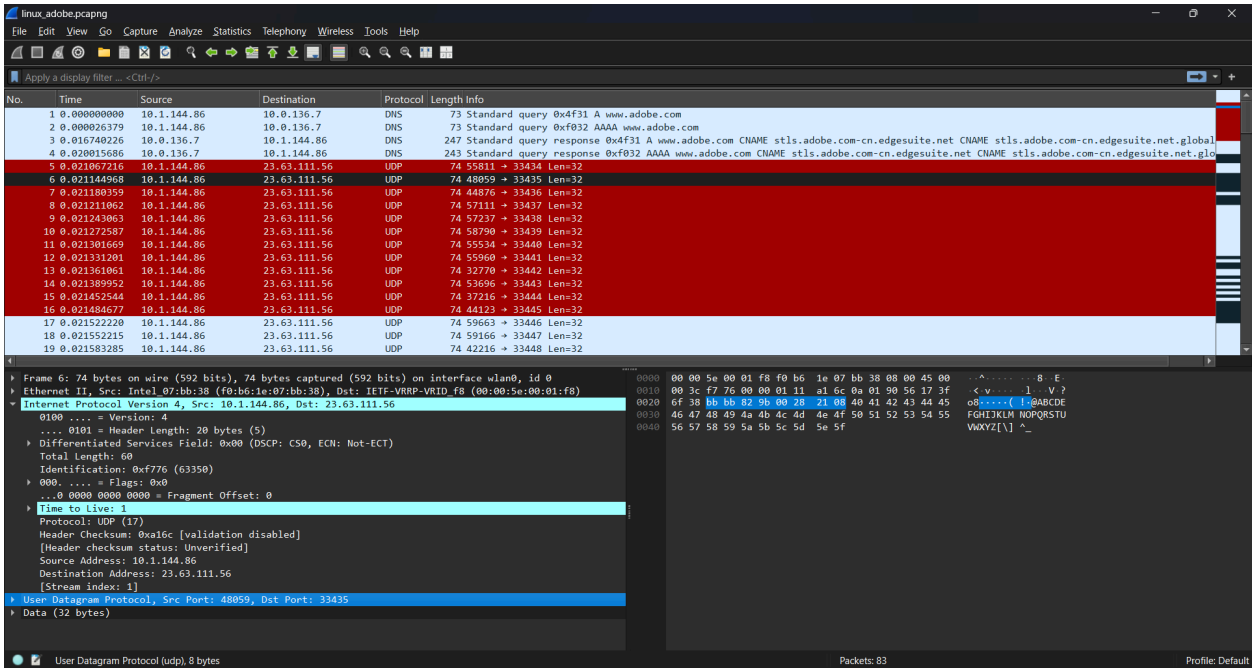
In Linux traceroute, I noticed mainly three fields that change between consecutive probes:

- Time to Live: It started from 1 and kept increasing in groups of 3 as traceroute sends 3 probes for each hop.
- Destination port: Starting from 33434, it kept increasing by 1 in each consecutive probe.
- Source port: It keeps changing in each hop, but I don’t see any pattern in it.

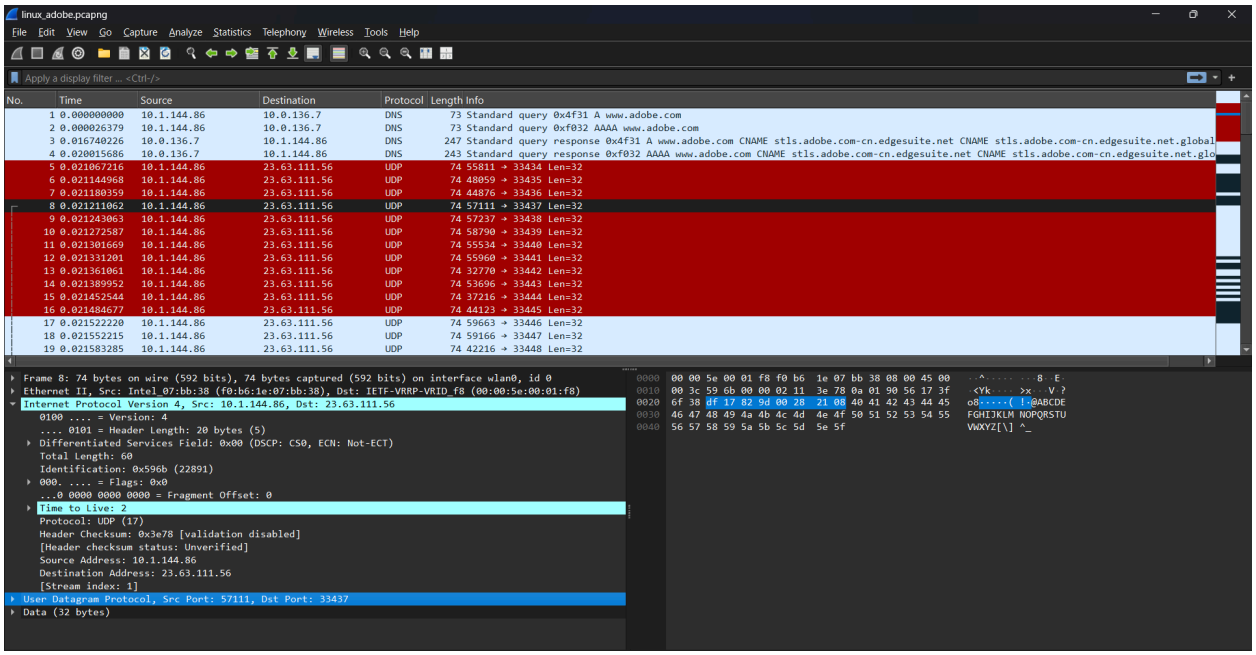
Hop1- probe1:



Hop1 - probe2:



Hop2 - probe1:



Q4

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

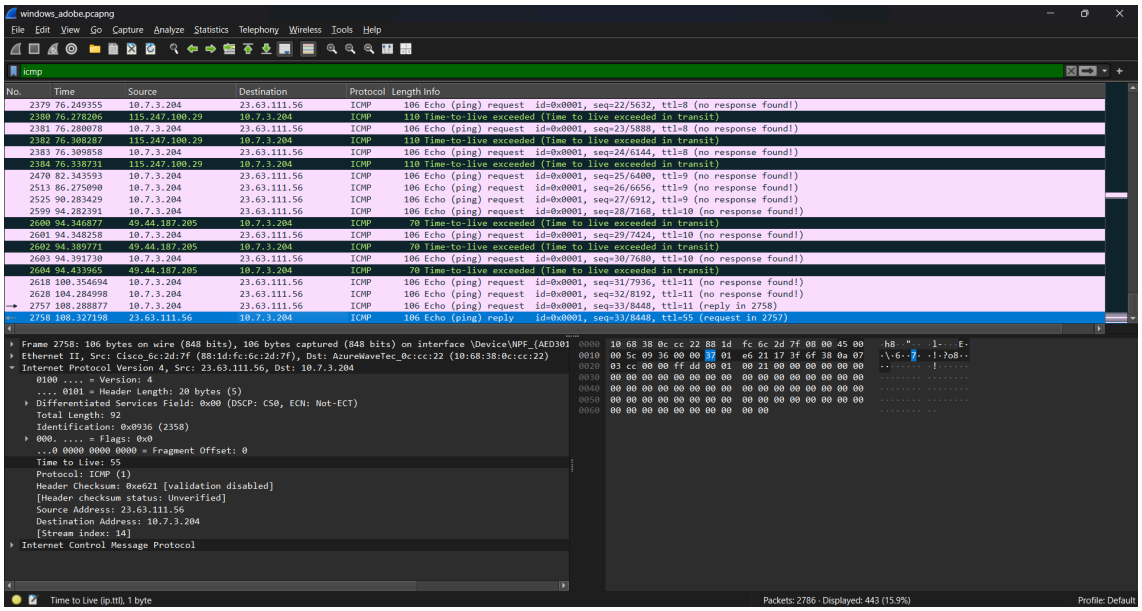
Ans.

Windows:

- Intermediate hop: We get a Time-to-live exceeded ICMP message for each probe of the intermediate hop. (Type:11, Code:0)

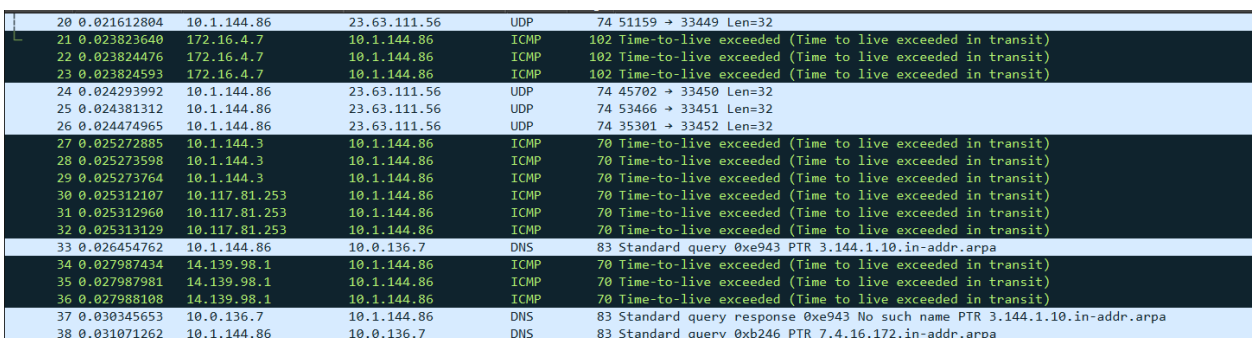
681	30.767394	10.7.3.204	23.63.111.56	ICMP	106	Echo (ping) request id=0x0001, seq=7/1792, ttl=3 (no response found!)
682	30.787827	14.139.98.1	10.7.3.204	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
683	30.789207	10.7.3.204	23.63.111.56	ICMP	106	Echo (ping) request id=0x0001, seq=8/2048, ttl=3 (no response found!)
684	30.794206	14.139.98.1	10.7.3.204	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
685	30.795256	10.7.3.204	23.63.111.56	ICMP	106	Echo (ping) request id=0x0001, seq=9/2304, ttl=3 (no response found!)
686	30.799146	14.139.98.1	10.7.3.204	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

- Final hop: We get an ICMP - Echo (ping) reply message for each of the final hop probes. But in my case, only one probe led to a reply, as for the other two probes, my terminal printed *. (Type:0, Code:0)

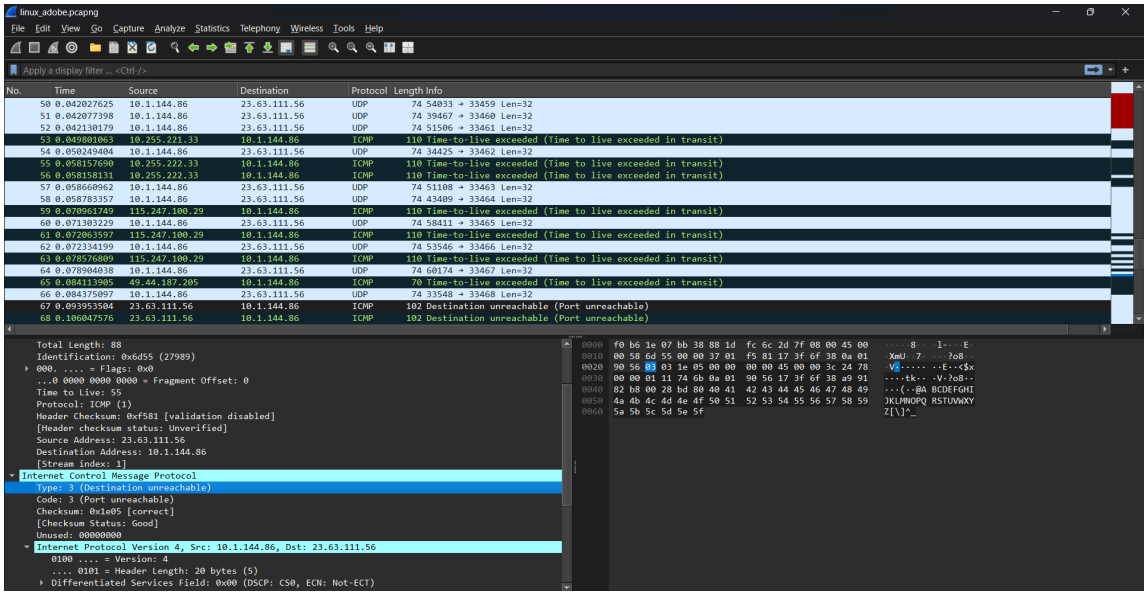


Linux:

- Intermediate hop: This is similar to the Windows tracert, as we get an ICMP Time-to-live exceeded message when TTL becomes 0. (Type:11, Code:0)



- Final hop: For this, we get an ICMP Destination Unreachable message because the packet reaches before the TTL expires, but the host has no application listening on that port. (Type:3, Code:3)



Q5

Suppose a firewall blocks UDP traffic but allows ICMP — how would this affect the results of Linux traceroute vs. Windows tracert?

Ans.

Windows

- As Windows tracert uses ICMP probes, it will act normally as expected.

Linux

- As Linuc tracroute uses UDP probes, there will be some abnormalities.
- Probes act normally up to the hop just before the firewall.
- From this hop onwards, the UDP probes would be dropped by the firewall. So, they never reach their destination, nor do their TTLs expire, leading to no ICMP reply.
- Traceroute probably shows *** for these packets because no reply is received.
- The blocked packets may generate an ICMP Destination Unreachable message, or the firewall may silently drop them.

References

- Superuser
- Stack Exchange