

ASSIGNMENT - 1

- Sailaja Mudu 23110288
- Vadithya Harsha Vardhan Nayak 23110349

TASK - 1

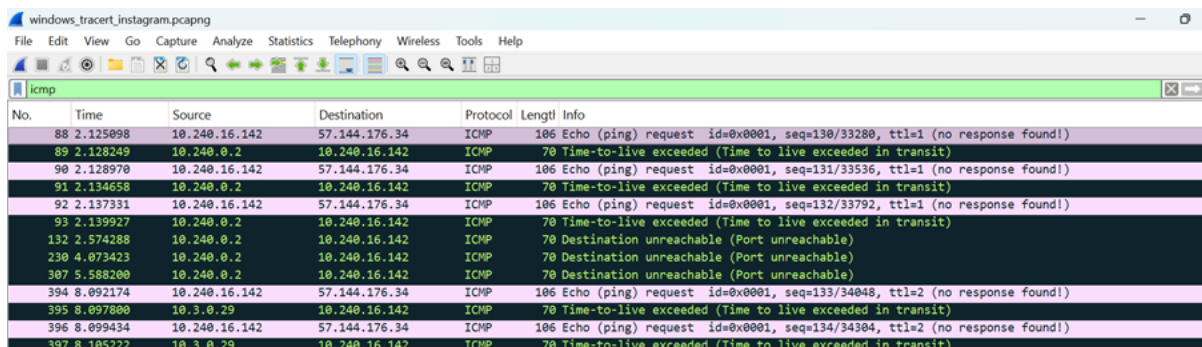
DNS Query Resolution Table”

Custom Header	Domain	Resolved IP
18041600	wikipedia.org	192.168.1.6
18041601	reddit.com	192.168.1.7
18041602	apple.com	192.168.1.8
18041603	twitter.com	192.168.1.9
18041604	yahoo.com	192.168.1.10
18041605	linkedin.com	192.168.1.6

TASK - 2

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

In Windows tracert, the tool uses ICMP Echo Request packets by default. Each hop along the path replies with ICMP Time Exceeded messages until the packet reaches the final destination, which replies with an ICMP Echo Reply. This is clearly shown in the Wireshark capture, where the protocol column displays ICMP and the Info field shows *Echo (ping) request* and *Time-to-live exceeded*



The image shows a Wireshark packet capture window titled "windows_tracert_instagram.pcapng". The packet list pane shows several ICMP packets. The first packet (No. 88) is an Echo (ping) request from 10.240.16.142 to 57.144.176.34. The second packet (No. 89) is a Time-to-live exceeded message from 10.240.16.142 to 10.240.16.142. The third packet (No. 90) is an Echo (ping) request from 10.240.16.142 to 57.144.176.34. The fourth packet (No. 91) is a Time-to-live exceeded message from 10.240.16.142 to 10.240.16.142. The fifth packet (No. 92) is an Echo (ping) request from 10.240.16.142 to 57.144.176.34. The sixth packet (No. 93) is a Time-to-live exceeded message from 10.240.16.142 to 10.240.16.142. The seventh packet (No. 132) is a Destination unreachable (Port unreachable) message from 10.240.16.142 to 10.240.16.142. The eighth packet (No. 230) is a Destination unreachable (Port unreachable) message from 10.240.16.142 to 10.240.16.142. The ninth packet (No. 307) is a Destination unreachable (Port unreachable) message from 10.240.16.142 to 10.240.16.142. The tenth packet (No. 394) is an Echo (ping) request from 10.240.16.142 to 57.144.176.34. The eleventh packet (No. 395) is a Time-to-live exceeded message from 10.3.0.29 to 10.240.16.142. The twelfth packet (No. 396) is an Echo (ping) request from 10.240.16.142 to 57.144.176.34. The thirteenth packet (No. 397) is a Time-to-live exceeded message from 10.3.0.29 to 10.240.16.142.

No.	Time	Source	Destination	Protocol	Length	Info
88	2.125098	10.240.16.142	57.144.176.34	ICMP	106	Echo (ping) request id=0x0001, seq=130/33280, ttl=1 (no response found!)
89	2.128249	10.240.16.142	10.240.16.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
90	2.128970	10.240.16.142	57.144.176.34	ICMP	106	Echo (ping) request id=0x0001, seq=131/33536, ttl=1 (no response found!)
91	2.134658	10.240.16.142	10.240.16.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
92	2.137331	10.240.16.142	57.144.176.34	ICMP	106	Echo (ping) request id=0x0001, seq=132/33792, ttl=1 (no response found!)
93	2.139927	10.240.16.142	10.240.16.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
132	2.574288	10.240.16.142	10.240.16.142	ICMP	70	Destination unreachable (Port unreachable)
230	4.073423	10.240.16.142	10.240.16.142	ICMP	70	Destination unreachable (Port unreachable)
307	5.588200	10.240.16.142	10.240.16.142	ICMP	70	Destination unreachable (Port unreachable)
394	8.092174	10.240.16.142	57.144.176.34	ICMP	106	Echo (ping) request id=0x0001, seq=133/34048, ttl=2 (no response found!)
395	8.097800	10.3.0.29	10.240.16.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
396	8.099434	10.240.16.142	57.144.176.34	ICMP	106	Echo (ping) request id=0x0001, seq=134/34304, ttl=2 (no response found!)
397	8.105222	10.3.0.29	10.240.16.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

In Linux, traceroute www.instagram.com sends UDP probe packets to high-numbered destination ports (33434–33440 in the image). The intermediate routers reply with ICMP Time Exceeded messages (seen from 10.0.2.2), showing each hop in the path. Finally, when the packets reach the destination 57.144.176.34, it would respond with an ICMP Port Unreachable, marking the completion of the trace.

	Source	Destination	Protocol	Length	Info
3	0.385702680	10.0.2.15	10.0.136.8	DNS	88 Standard query 0x81c5 A www.instagram.com OPT
4	0.386342001	10.0.2.15	10.0.136.8	DNS	88 Standard query 0xe31e AAAA www.instagram.com OPT
5	0.389345665	10.0.136.8	10.0.2.15	DNS	139 Standard query response 0x81c5 A www.instagram.com CNAME z-p42-instagram.c10r.instagram.com A
6	0.402361142	10.0.136.8	10.0.2.15	DNS	151 Standard query response 0xe31e AAAA www.instagram.com CNAME z-p42-instagram.c10r.instagram.cc
7	0.404718839	10.0.2.15	57.144.176.34	UDP	74 50339 → 33434 Len=32
8	0.404859491	10.0.2.15	57.144.176.34	UDP	74 58270 → 33435 Len=32
9	0.404926907	10.0.2.15	57.144.176.34	UDP	74 44623 → 33436 Len=32
10	0.405082698	10.0.2.15	57.144.176.34	UDP	74 58963 → 33437 Len=32
11	0.405277885	10.0.2.2	10.0.2.15	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
12	0.405303230	10.0.2.15	57.144.176.34	UDP	74 52183 → 33438 Len=32
13	0.405412829	10.0.2.15	57.144.176.34	UDP	74 43101 → 33439 Len=32
14	0.405514595	10.0.2.15	57.144.176.34	UDP	74 33984 → 33440 Len=32
15	0.405277947	10.0.2.2	10.0.2.15	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)

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

- Hop 1: _gateway (10.0.2.2) → this is your local network/VM gateway.
- Hop 2–30: All show * * *.

Here are two reasons why some hops in traceroute show * * *:

1. ICMP/UDP Filtering by Routers

- Some routers are configured to not send ICMP Time Exceeded messages or block UDP/ICMP responses altogether for security.
- This prevents traceroute from receiving a reply, so it shows * * *.

2. Rate Limiting or Load Handling

- Routers often prioritize forwarding traffic over replying to diagnostic packets like traceroute.
- If the router is busy or has ICMP rate-limiting enabled, it may drop or ignore the traceroute probes, leading to * * *.

```

set-lltgn-vm@set-lltgn-vm:~$ traceroute www.instagram.com
traceroute to www.instagram.com (57.144.176.34), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.564 ms  0.421 ms  0.352 ms
 2  ***
 3  ***
 4  ***
 5  ***
 6  ***
 7  ***
 8  ***
 9  ***
10  ***
11  ***
12  ***
13  ***
14  ***
15  ***
16  ***
17  ***
18  ***
19  ***
20  ***
21  ***
22  ***
23  ***
24  ***
25  ***
26  ***
27  ***
28  ***
29  ***
30  ***
set-lltgn-vm@set-lltgn-vm:~$

```

In our screenshot, after hop 1 (10.0.2.2), all other hops show * * *, likely because intermediate routers (or Instagram’s servers) are configured not to reply to traceroute probes.

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

In Linux traceroute, the field that changes between successive probes is the TTL (Time To Live) field in the IP header.

Each probe is sent with an incremented TTL value (starting from 1, then 2, 3, ...) so that each intermediate router along the path returns an ICMP *Time Exceeded* message when the TTL expires.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.404718839	10.0.2.15	57.144.176.34	UDP	74	50339 → 33434 Len=32
8	0.404859491	10.0.2.15	57.144.176.34	UDP	74	58270 → 33435 Len=32
9	0.404926907	10.0.2.15	57.144.176.34	UDP	74	44623 → 33436 Len=32
10	0.405082698	10.0.2.15	57.144.176.34	UDP	74	58963 → 33437 Len=32
11	0.405277885	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
12	0.405303230	10.0.2.15	57.144.176.34	UDP	74	52183 → 33438 Len=32
13	0.405412829	10.0.2.15	57.144.176.34	UDP	74	43101 → 33439 Len=32
14	0.405514595	10.0.2.15	57.144.176.34	UDP	74	33984 → 33440 Len=32
15	0.405277947	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
16	0.405665478	10.0.2.15	57.144.176.34	UDP	74	60524 → 33441 Len=32
17	0.405277973	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.407419024	10.0.2.15	57.144.176.34	UDP	74	50198 → 33442 Len=32
19	0.407581159	10.0.2.15	57.144.176.34	UDP	74	55618 → 33443 Len=32

The screenshot shows UDP probe packets sent to 57.144.176.34. When their TTL expired at the router 10.0.2.2, the router replied with ICMP “Time-to-live exceeded” messages. This proves that traceroute relies on incrementing the TTL value to discover each hop.

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

The responses from intermediate hops and the final hop are different, as shown in the two captures.

Intermediate hop:

No.	Time	Source	Destination	Protocol	Length	Info
7	0.404718839	10.0.2.15	57.144.176.34	UDP	74	50339 → 33434 Len=32
8	0.404859491	10.0.2.15	57.144.176.34	UDP	74	58270 → 33435 Len=32
9	0.404926907	10.0.2.15	57.144.176.34	UDP	74	44623 → 33436 Len=32
10	0.405082698	10.0.2.15	57.144.176.34	UDP	74	58963 → 33437 Len=32
11	0.405277885	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
12	0.405303230	10.0.2.15	57.144.176.34	UDP	74	52183 → 33438 Len=32
13	0.405412829	10.0.2.15	57.144.176.34	UDP	74	43101 → 33439 Len=32
14	0.405514595	10.0.2.15	57.144.176.34	UDP	74	33984 → 33440 Len=32
15	0.405277947	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
16	0.405665478	10.0.2.15	57.144.176.34	UDP	74	60524 → 33441 Len=32
17	0.405277973	10.0.2.2	10.0.2.15	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.407419024	10.0.2.15	57.144.176.34	UDP	74	50198 → 33442 Len=32
19	0.407581159	10.0.2.15	57.144.176.34	UDP	74	55818 → 33443 Len=32

In this capture, UDP probes are sent from 10.0.2.15 to the destination 57.144.176.34. At packets 11, 15, and 19, we see ICMP “Time-to-live exceeded (Time to live exceeded in transit)” messages coming back.

This indicates that at these intermediate routers, the packet’s TTL expired, and the routers replied with ICMP Time Exceeded messages, showing that the packets were dropped before reaching the final destination.

Final hop:

No.	Time	Source	Destination	Protocol	Length	Info
73	15.437260002	10.0.2.15	57.144.176.34	UDP	74	41640 → 33491 Len=32
74	15.437295843	10.0.2.15	57.144.176.34	UDP	74	49529 → 33492 Len=32
75	15.437338805	10.0.2.15	57.144.176.34	UDP	74	47160 → 33493 Len=32
76	15.437377814	10.0.2.15	57.144.176.34	UDP	74	36673 → 33494 Len=32
77	15.437412661	10.0.2.15	57.144.176.34	UDP	74	39781 → 33495 Len=32
78	15.437450368	10.0.2.15	57.144.176.34	UDP	74	48134 → 33496 Len=32
79	15.437530071	10.0.2.15	57.144.176.34	UDP	74	45881 → 33497 Len=32
80	15.444126693	10.0.2.15	57.144.176.34	UDP	74	43544 → 33498 Len=32
81	15.444310558	10.0.2.15	57.144.176.34	UDP	74	35132 → 33499 Len=32
82	15.444362329	10.0.2.15	57.144.176.34	UDP	74	56055 → 33500 Len=32
83	15.464517204	fd17:625c:f037:2:f1_2620:2d:4000:1::3f	fd17:625c:f037:2:f1_2620:2d:4000:1::3f	NTP	110	NTP Version 4, client
84	15.468013783	fe80::2	fd17:625c:f037:2:f1_2620:2d:4000:1::3f	ICMPv6	158	Destination Unreachable (No route to destination)
85	20.446171195	10.0.2.15	57.144.176.34	UDP	74	50886 → 33501 Len=32

In this capture, UDP probes again go from 10.0.2.15 to the destination. At packet 84, we see an ICMPv6 “Destination Unreachable (No route to destination)” message.

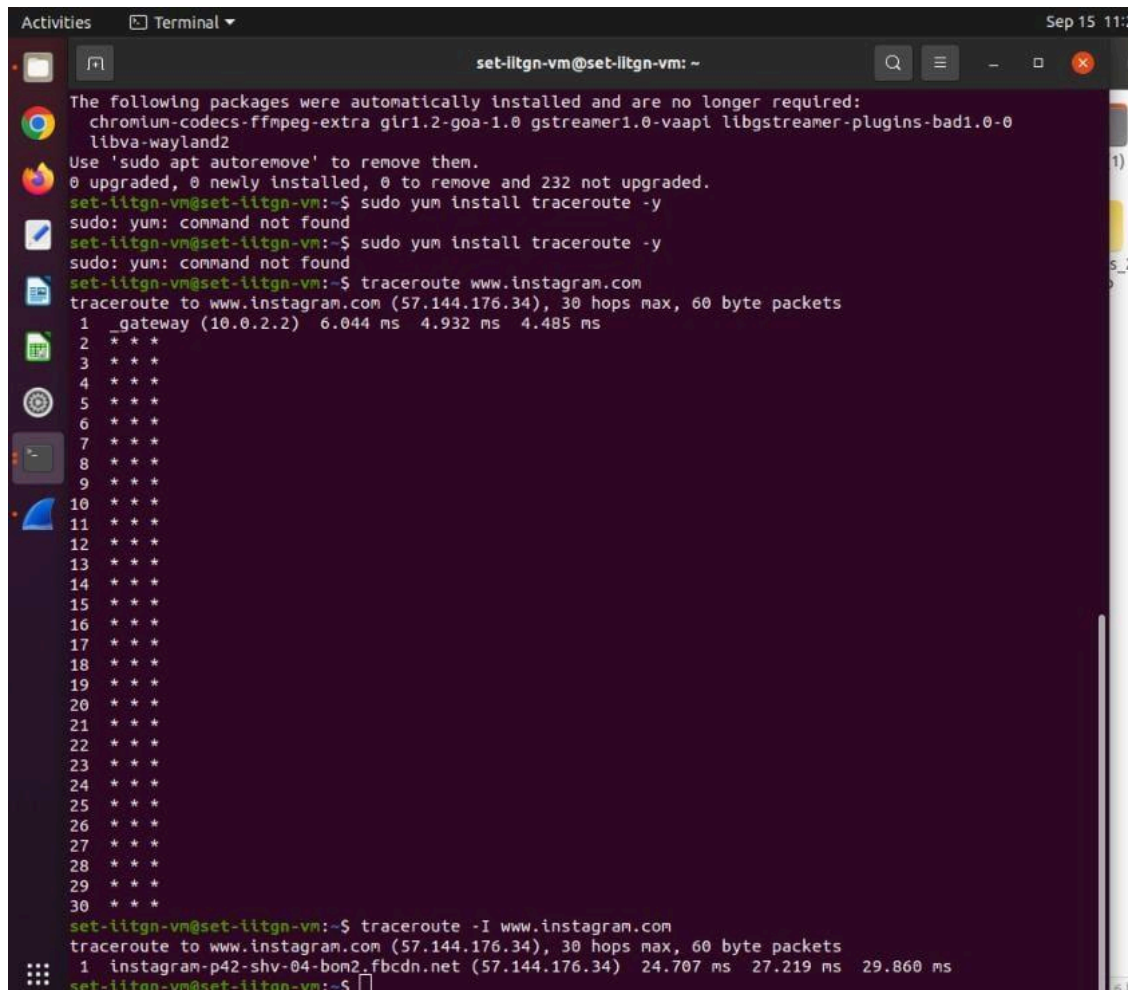
This shows that the packet reached the destination network but could not be delivered, so the final response was ICMP Destination Unreachable, instead of Time Exceeded.

- Intermediate hops → reply with ICMP Time Exceeded (TTL expired).
- Final hop → replies with ICMP Destination Unreachable (no route to destination).

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

Linux traceroute

- By default, Linux traceroute sends UDP probes to high-numbered ports.
- If a firewall blocks UDP, then the probes will never reach the destination or intermediate hops.
- The only thing that will get back are ICMP “Time Exceeded” messages (if the firewall allows ICMP).
- Effect: Intermediate hops may still be visible (due to ICMP time exceeded), but the final hop will never reply, since the destination’s UDP response (ICMP Port Unreachable) is blocked by the firewall.
- So Linux traceroute will look like it “hangs” at the end (stars * * *), failing to resolve the last hop.



```
set-iltgn-vm@set-iltgn-vm: ~
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra glr1.2-goa-1.0 gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
libva-wayland2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
set-iltgn-vm@set-iltgn-vm:~$ sudo yum install traceroute -y
sudo: yum: command not found
set-iltgn-vm@set-iltgn-vm:~$ sudo yum install traceroute -y
sudo: yum: command not found
set-iltgn-vm@set-iltgn-vm:~$ traceroute www.instagram.com
traceroute to www.instagram.com (57.144.176.34), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  6.044 ms  4.932 ms  4.485 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
set-iltgn-vm@set-iltgn-vm:~$ traceroute -I www.instagram.com
traceroute to www.instagram.com (57.144.176.34), 30 hops max, 60 byte packets
 1 instagram-p42-shv-04-bon2.fbcdn.net (57.144.176.34)  24.707 ms  27.219 ms  29.860 ms
set-iltgn-vm@set-iltgn-vm:~$
```

On Linux, the default traceroute command uses UDP probes.

- In the first run (traceroute www.instagram.com), we see only the gateway (10.0.2.2) and then * * * for all hops.
- This happens because UDP traffic is blocked by the firewall, so no replies come back from intermediate or final hops.

When traceroute is run with the **-I** option, it switches to ICMP Echo Requests instead of UDP:

- In the second run (traceroute www.instagram.com), we immediately reach Instagram's server (57.144.176.34) successfully, since ICMP is allowed.

Windows tracert

- Windows tracert uses ICMP Echo Request packets (like ping) instead of UDP.
- If the firewall blocks only UDP but allows ICMP, then tracert will work normally, because its probes are ICMP.
- Effect: Windows tracert will successfully display the full route including the final hop.

