Task 2: Network Path Analysis using Traceroute and Tracert

Your Name Your Partner's Name

September 15, 2025

Objective

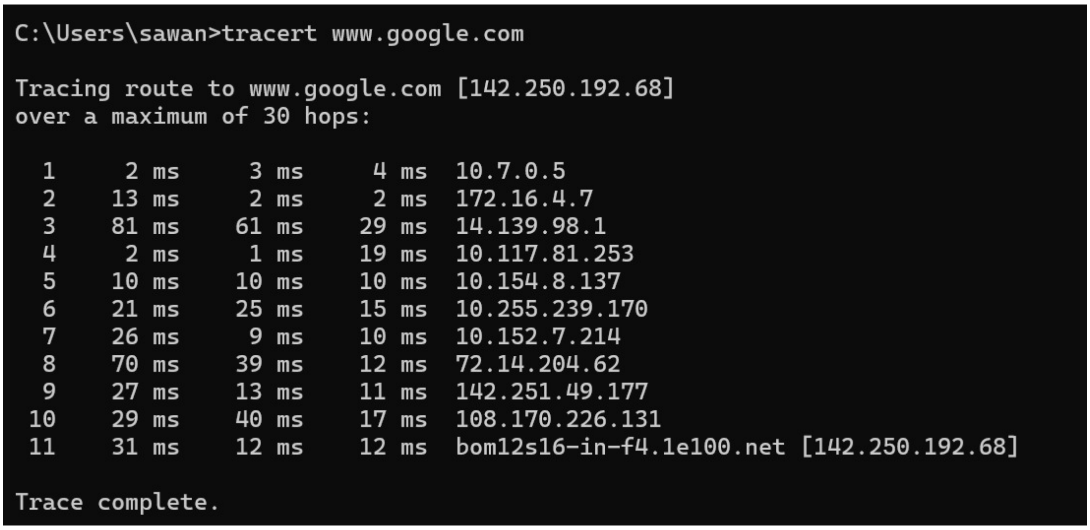
The objective of this task is to analyze the path taken by packets to a remote host using `tracert` (Windows) and `traceroute` (Linux/macOS). We will examine the intermediate hops, final hop responses, and compare protocol behavior based on captured network traffic.

Methodology

To understand the underlying mechanisms of the traceroute utilities, experiments were conducted on both Windows and macOS. The network traffic for each was captured to analyze the protocols used.

Windows (`tracert` – ICMP based)

The `tracert www.google.com` command was executed on Windows. The output in Figure 1 shows the successful trace to the destination. Wireshark captures (Figures 2 and 3) confirm that `tracert` uses the ICMP protocol.



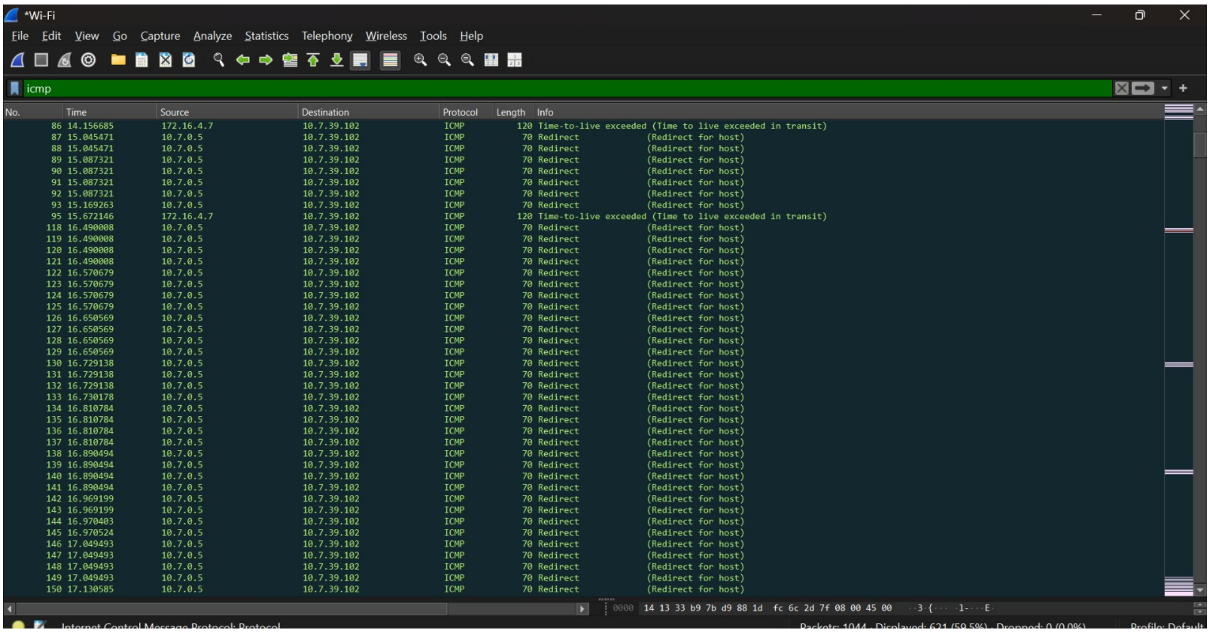
```
C:\Users\sawan>tracert www.google.com

Tracing route to www.google.com [142.250.192.68]
over a maximum of 30 hops:

  1     2 ms     3 ms     4 ms  10.7.0.5
  2    13 ms     2 ms     2 ms  172.16.4.7
  3    81 ms    61 ms    29 ms  14.139.98.1
  4     2 ms     1 ms    19 ms  10.117.81.253
  5    10 ms    10 ms    10 ms  10.154.8.137
  6    21 ms    25 ms    15 ms  10.255.239.170
  7    26 ms     9 ms    10 ms  10.152.7.214
  8    70 ms    39 ms    12 ms  72.14.204.62
  9    27 ms    13 ms    11 ms  142.251.49.177
 10    29 ms    40 ms    17 ms  108.170.226.131
 11    31 ms    12 ms    12 ms  bom12s16-in-f4.1e100.net [142.250.192.68]

Trace complete.
```

Figure 1: Output of the `tracert www.google.com` command on Windows.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

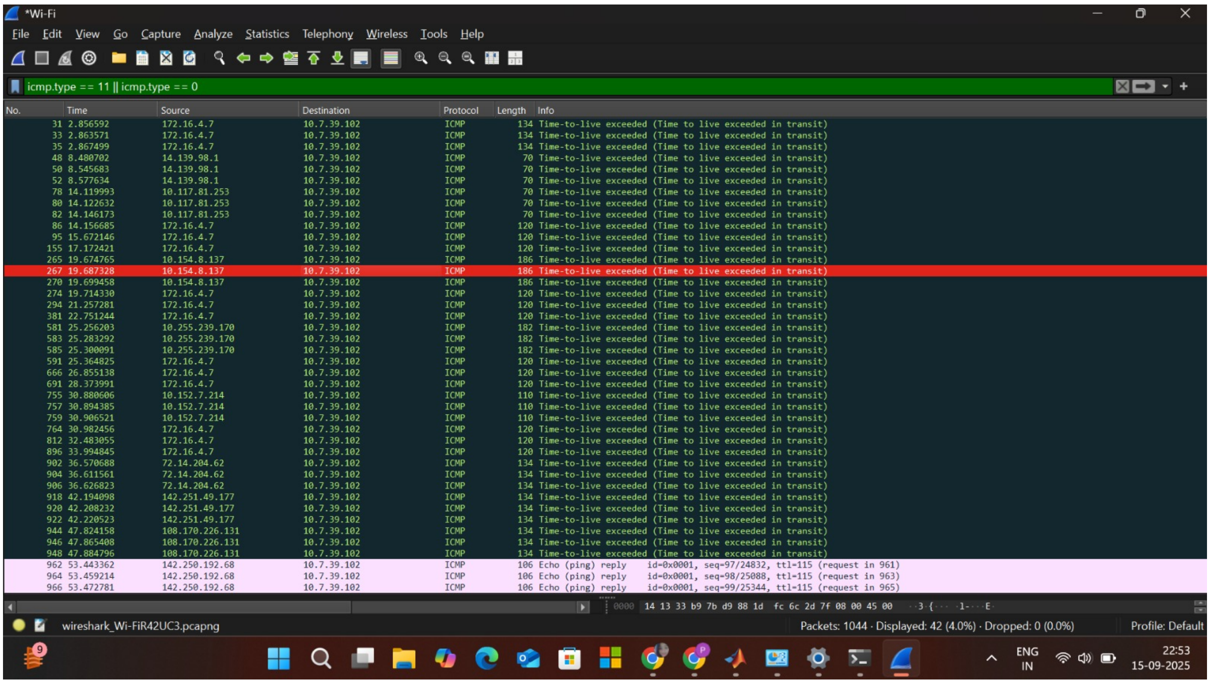
```
icmp
```

```
No.     Time       Source        Destination    Protocol  Length  Info
     86 14.156685  172.16.4.7    10.7.39.102    ICMP       120 Time-to-live exceeded (Time to live exceeded in transit)
     87 15.045471  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     88 15.045471  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     89 15.087321  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     90 15.087321  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     91 15.087321  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     92 15.087321  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     93 15.169263  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
     95 15.672146  172.16.4.7    10.7.39.102    ICMP       120 Time-to-live exceeded (Time to live exceeded in transit)
    118 16.490008  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    119 16.490008  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    120 16.490008  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    121 16.490008  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    122 16.570679  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    123 16.570679  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    124 16.570679  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    125 16.570679  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    126 16.650569  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    127 16.650569  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    128 16.650569  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    129 16.650569  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    130 16.729138  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    131 16.729138  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    132 16.729138  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    133 16.730178  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    134 16.810784  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    135 16.810784  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    136 16.810784  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    137 16.810784  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    138 16.890494  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    139 16.890494  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    140 16.890494  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    141 16.890494  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    142 16.969199  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    143 16.969199  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    144 16.970403  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    145 16.970524  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    146 17.049493  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    147 17.049493  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    148 17.049493  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    149 17.049493  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
    150 17.130585  10.7.0.5      10.7.39.102    ICMP        70 Redirect             (Redirect for host)
```

```
0000  14 13 33 b9 7b d9 88 1d  fc 6c 2d 7f 08 00 45 00   ··3·{··· ·l-···E·
```

```
Internet Control Message Protocol: Protocol     Packets: 1044 · Displayed: 621 (59.5%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 2: Wireshark capture showing the various ICMP packets generated by `tracert`.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wireshark_Wi-FiR42UC3.pcapng
Profile: Default
ENG IN
22:53
15-09-2025

```
icmp.type == 11 || icmp.type == 0
```

```
No.  Time       Source           Destination   Protocol Length Info
 31 2.856592   172.16.4.7       10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 33 2.863571   172.16.4.7       10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 35 2.867499   172.16.4.7       10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 48 8.480702   14.139.98.1      10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 50 8.545683   14.139.98.1      10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 52 8.577634   14.139.98.1      10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 78 14.119993  10.117.81.253    10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 80 14.122632  10.117.81.253    10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 82 14.146173  10.117.81.253    10.7.39.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 86 14.156685  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
 95 15.672146  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
155 17.172421  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
265 19.674765  10.154.8.137     10.7.39.102   ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
267 19.687328  10.154.8.137     10.7.39.102   ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
270 19.699458  10.154.8.137     10.7.39.102   ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
274 19.714330  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
294 21.257281  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
381 22.751244  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
581 25.256203  10.255.239.170   10.7.39.102   ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
583 25.283292  10.255.239.170   10.7.39.102   ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
585 25.300091  10.255.239.170   10.7.39.102   ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
591 25.364825  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
666 26.855138  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
691 28.373991  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
755 30.880606  10.152.7.214     10.7.39.102   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
757 30.894385  10.152.7.214     10.7.39.102   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
759 30.906521  10.152.7.214     10.7.39.102   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
764 30.982456  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
812 32.483055  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
896 33.994845  172.16.4.7       10.7.39.102   ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
902 36.570688  72.14.204.62     10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
904 36.611561  72.14.204.62     10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
906 36.626823  72.14.204.62     10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
918 42.194098  142.251.49.177   10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
920 42.208232  142.251.49.177   10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
922 42.220523  142.251.49.177   10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
944 47.824158  108.170.226.131  10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
946 47.865408  108.170.226.131  10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
948 47.884796  108.170.226.131  10.7.39.102   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
962 53.443362  142.250.192.68   10.7.39.102   ICMP     106 Echo (ping) reply    id=0x0001, seq=97/24832, ttl=115 (request in 961)
964 53.459214  142.250.192.68   10.7.39.102   ICMP     106 Echo (ping) reply    id=0x0001, seq=98/25088, ttl=115 (request in 963)
966 53.472781  142.250.192.68   10.7.39.102   ICMP     106 Echo (ping) reply    id=0x0001, seq=99/25344, ttl=115 (request in 965)

0000  14 13 33 b9 7b d9 88 1d  fc 6c 2d 7f 08 00 45 00

Packets: 1044 · Displayed: 42 (4.0%) · Dropped: 0 (0.0%)
```

Figure 3: Filtered Wireshark capture highlighting the final ICMP Echo Reply (bottom packet) from the destination, which is different from the intermediate "Time-to-live exceeded" responses.

macOS (traceroute – UDP based)

The `traceroute www.google.com` command was executed on macOS, and the traffic was captured using `tcpdump`. The command output is shown below, followed by the corresponding packet capture.

Traceroute Command Output:

```
traceroute to www.google.com (216.58.203.4), 64 hops max, 40 byte packets
 1  10.7.0.5 (10.7.0.5)  4.529 ms  3.718 ms  3.772 ms
 2  172.16.4.7 (172.16.4.7)  3.841 ms  3.521 ms  3.228 ms
 3  14.139.98.1 (14.139.98.1)  5.281 ms  5.321 ms  5.182 ms
 4  10.117.81.253 (10.117.81.253)  16.463 ms  3.935 ms  3.693 ms
 5  10.154.8.137 (10.154.8.137)  12.214 ms  11.907 ms  11.876 ms
 6  10.255.239.170 (10.255.239.170)  13.410 ms  11.888 ms  11.877 ms
 7  10.152.7.214 (10.152.7.214)  12.171 ms  15.959 ms  13.713 ms
 8  72.14.204.62 (72.14.204.62)  12.172 ms * *
 9  * * *
10  142.250.228.48 (142.250.228.48)  26.352 ms
    216.239.58.18 (216.239.58.18)  13.912 ms
    192.178.86.238 (192.178.86.238)  29.365 ms
11  142.250.226.134 (142.250.226.134)  13.885 ms  13.686 ms  14.401 ms
12  bom12s04-in-f4.1e100.net (216.58.203.4)  12.268 ms  12.472 ms  12.551 ms
```

Tcpdump Packet Capture Analysis: The `tcpdump` output below provides clear evidence of the UDP-based approach on macOS.

- **Intermediate Hop Probes:** For each intermediate hop (e.g., lines starting with `23:16:36`), we can see an `ICMP time exceeded in-transit` message. This is the router's response when it receives a UDP packet with a TTL of 1. Inside this ICMP message, the original UDP probe packet is quoted.
- **Final Hop Probe:** The final packet in the trace (timestamp `23:17:02.194677`) shows the destination server `216.58.203.4` responding with an `ICMP 216.58.203.4 udp port 33468 unreachable` message. This confirms that the traceroute has reached its destination.

```
23:16:36.560938 IP ... 10.7.0.5 > 10.7.44.10: ICMP time exceeded in-transit...
    10.7.44.10.56667 > 216.58.203.4.33435: UDP, length 12
...
23:17:02.194677 IP ... 216.58.203.4 > 10.7.44.10: ICMP 216.58.203.4 udp port 33468 unreachable...
    10.7.44.10.56667 > 216.58.203.4.33468: UDP, length 12
```

Results Summary

OS	**Command**	**Intermediate Hops**	**Final Hop**
Windows	`tracert www.google.com`	ICMP Time Exceeded	ICMP Echo Reply
Linux/macOS	`traceroute www.google.com`	ICMP Time Exceeded	ICMP Port Unreachable

Table 1: Summary of Tracert and Traceroute Behavior

Questions and Answers

Q1: What protocol does Windows tracert use by default, and what protocol does Linux/macOS traceroute use by default?
As shown in the Wireshark and `tcpdump` captures, Windows `tracert` uses **ICMP** Echo Request packets. In contrast, the default behavior for Linux/macOS `traceroute` is to use **UDP** probes sent to high-numbered ports.

Q2: Some hops in your traceroute output may show * * *. Provide at least two reasons why a router might not reply.
A router might not reply for several reasons, leading to a timeout (* * *):

- **Firewall Configuration:** The router or a firewall in front of it may be configured to block incoming probes or outgoing ICMP "Time Exceeded" messages for security reasons.
- **Low Priority of ICMP:** Routers prioritize their primary task of forwarding traffic. Generating ICMP error messages is a low-priority task that may be ignored if the router is experiencing high traffic loads.

Q3: In Linux/macOS traceroute, which field in the probe packets changes between successive probes sent to the destination?
In Linux/macOS `traceroute`, the **Time-to-Live (TTL)** field in the IP header of the outgoing UDP probe packets is incremented by one for each successive hop. It starts with TTL=1 for the first hop, TTL=2 for the second, and so on. The destination UDP port also typically increments for each probe.

Q4: At the final hop, how is the response different compared to the intermediate hop?
The responses are fundamentally different and signal the end of the trace, as evidenced by the packet captures:

- **Intermediate Hops:** All intermediate routers respond with an **ICMP "Time-to-live exceeded"** message when the packet's TTL value drops to zero.
- **Final Hop:** The final destination responds differently. On Windows, it sends an **ICMP "Echo reply"**. As seen in the `tcpdump` output, on macOS it sends an **ICMP "Destination unreachable (Port unreachable)"** message because it receives a UDP packet on a port it isn't listening on.

Q5: Suppose a firewall blocks UDP traffic but allows ICMP — how would this affect the results of Linux/macOS traceroute vs. Windows tracert?
This scenario would have drastically different outcomes for the two utilities:

- **Linux/macOS `traceroute`:** It would **fail**. The outgoing UDP probe packets would be blocked by the firewall. The command would time out at every hop, resulting in an output of only * * *.
- **Windows `tracert`:** It would **succeed**. Since it uses ICMP packets for its probes and the firewall allows ICMP, the trace would complete normally.