Task 2: Traceroute Protocol Behavior

1. Objective

This report analyzes the packet-level behavior of the traceroute utility on different operating systems, as required by the assignment. We specifically:

- Compared the default probe protocols used by Windows (tracert) and Linux (traceroute).
- Captured and analyzed traffic to understand the probes and their responses.
- Explained why some hops may show * * *.
- Identified which fields change between successive probes on Linux.
- Compared intermediate vs. final hop responses.
- Explained the behavior when a firewall blocks UDP but allows ICMP.

2. Testbed & Tools

- **Host:** Ubuntu VM (interface enp0s3, source IP 10.0.2.15)
- **Additional Capture:** macOS host for the ICMP-style run.
- **Tools Used:** traceroute, tracert (Windows equivalent), tcpdump, and Wireshark.

3. Commands Used (exact; copy-paste ready)

UDP-based traceroute capture on Ubuntu (default traceroute)

```
sudo tcpdump -i enp0s3 -s 0 -w traceroute_udp.pcap icmp or udp
```

```
sudo traceroute -n -q 3 -w 3 8.8.8.8 | tee traceroute_udp_output.txt
```

(Stop the tcpdump process with Ctrl+C after traceroute ends.)

ICMP-based traceroute (equivalent to Windows tracert)

```
sudo tcpdump -i enp0s3 -s 0 -w traceroute_icmp.pcap icmp
```

```
sudo traceroute -I -n -q 3 -w 3 8.8.8.8 | tee traceroute_icmp_output.txt
```

(Stop the tcpdump process with Ctrl+C after traceroute ends.)

Extract fields with tshark

```
tshark -r traceroute_udp.pcap -Y "udp && ip.src==10.0.2.15" -T fields -e frame.number -e ip.src
```

```
-e ip.dst -e udp.dstport > udp_probes.txt

tshark -r traceroute_udp.pcap -Y "icmp" -T fields -e frame.number -e ip.src -e ip.dst -e icmp.type
-e icmp.code > icmp_responses.txt

tshark -r traceroute_icmp.pcap -Y "icmp" -T fields -e frame.number -e ip.src -e ip.dst -e
icmp.type -e icmp.code > icmp_traceroute_summary.txt
```

4. Raw Terminal Outputs (what you produced)

4.1 traceroute (UDP) partial output (Ubuntu)

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 10.0.2.2 0.709 ms 0.654 ms 0.621 ms
2 10.0.2.2 1.173 ms 1.141 ms 1.109 ms
```

4.2 tshark — UDP probe list (udp_probes.txt)

```
1 10.0.2.15 10.0.136.7 53
3 10.0.2.15 8.8.8.8 33434
4 10.0.2.15 8.8.8.8 33435
5 10.0.2.15 8.8.8.8 33436
6 10.0.2.15 8.8.8.8 33437
7 10.0.2.15 8.8.8.8 33438
8 10.0.2.15 8.8.8.8 33439
9 10.0.2.15 8.8.8.8 33440
10 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 33434
11 10.0.2.15 8.8.8.8 33441
12 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 33435
...
40 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 33449
```

4.3 tshark — ICMP responses for UDP traceroute (icmp_responses.txt)

```
10 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
12 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
13 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
24 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 3 3
25 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 3 3
27 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 3 3
```

```
...
40 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 3 3
```

4.4 tshark — ICMP traceroute capture (icmp_traceroute_summary.txt)

```
1 10.0.2.15 8.8.8.8 8 0
2 10.0.2.15 8.8.8.8 8 0
3 10.0.2.15 8.8.8.8 8 0
...
10 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11,8 0,0
...
85 8.8.8.8 10.0.2.15 0 0
86 8.8.8.8 10.0.2.15 0 0
89 8.8.8.8 10.0.2.15 0 0
90 8.8.8.8 10.0.2.15 0 0
...
100 8.8.8.8 10.0.2.15 0 0
```

4.5 traceroute -I (ICMP) output (Ubuntu)

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 10.0.2.2 0.647 ms 0.574 ms 0.547 ms
2 10.0.177.2 2.027 ms 1.999 ms 1.973 ms
3 10.3.0.37 1.945 ms 1.921 ms 1.894 ms
4 10.3.0.5 1.866 ms 1.897 ms 1.883 ms
5 172.16.4.7 1.753 ms 1.785 ms 1.759 ms
6 14.139.98.1 6.353 ms 6.242 ms 6.214 ms
7 10.117.81.253 3.590 ms 2.007 ms 1.972 ms
8 10.154.8.137 10.646 ms 11.231 ms 11.205 ms
9 10.255.239.170 18.419 ms 18.374 ms 18.860 ms
10 10.152.7.214 8.601 ms 8.667 ms 9.758 ms
11 142.250.172.80 13.214 ms 12.223 ms 14.488 ms
12 74.125.37.7 19.628 ms 19.272 ms 19.399 ms
13 216.239.54.85 11.496 ms 11.555 ms 11.561 ms
14 8.8.8.8 9.754 ms 9.721 ms 9.940 ms
```

4.6 macOS traceroute excerpt

```
traceroute to [www.google.com](https://www.google.com) (142.250.71.100), 64 hops max, 40
byte packets
```

```
1 10.240.0.2 (10.240.0.2) 6.021 ms 5.217 ms 5.500 ms
...
10 72.14.204.62 (72.14.204.62) 14.861 ms * 14.375 ms
11 * * *
12 142.251.64.8 (142.251.64.8) 16.625 ms ...
...
14 pnbomb-ad-in-f4.1e100.net (142.250.71.100) 18.184 ms 17.979 ms ...
```

5. Analysis & Mapping of Evidence → Questions

Q1 — Which protocols do Windows tracert and Linux traceroute use by default?

Answer:

- Windows tracert uses **ICMP Echo Requests** (ICMP type 8) by default.
- Linux traceroute (default) uses **UDP** probes to high-numbered destination ports (starting at 33434).

Evidence:

- Our captures confirm this. The **udp_probes.txt** output shows UDP probes to ports 33434, 33435, etc.
- The **icmp_traceroute_summary.txt** output and macOS capture show ICMP Echo Requests (type 8) and Echo Replies (type 0).

Q2 — Why might a router show * * * (no reply)?

Short Answer: * * * indicates no reply was received within the probe timeout. Possible reasons include:

1. **ICMP/Probe Filtering:** A router or firewall is configured to block ICMP Time Exceeded/Echo messages or to drop UDP probes.
2. **Rate Limiting/Prioritization:** Routers may deprioritize or drop low-priority control messages, such as traceroute probes, under heavy network load.

Evidence:

- The macOS terminal output shows hop 11 as * * *, a clear example of a router not responding.

Q3 — In Linux traceroute, which field changes between successive probes?

Answer: The **UDP destination port** changes. It increments starting at 33434. This allows traceroute to match incoming ICMP replies to the corresponding probe.

Evidence:

- The **udp_probes.txt** output shows successive destination ports: 33434, 33435, 33436, and so on.

Q4 — How is the final hop response different from intermediate hops?

Answer:

- **Intermediate Hops:** Routers whose TTL expired respond with **ICMP Time Exceeded** (type 11, code 0).
- **Final Hop** (for Linux UDP probes): The destination receives the UDP probe and, since the destination port is unused, responds with **ICMP Destination Unreachable — Port Unreachable** (type 3, code 3).
- **Final Hop** (for ICMP probes / Windows tracert): The destination responds with **ICMP Echo Reply** (type 0).

Evidence:

- The **icmp_responses.txt** output shows both Type 11 (Time Exceeded) and Type 3, Code 3 (Port Unreachable) messages from the destination.
- The **icmp_traceroute_summary.txt** output shows Echo Reply (type 0) from the destination 8.8.8.8.

Q5 — Firewall blocks UDP but allows ICMP — compare Linux traceroute vs. Windows tracert

Comparative Explanation:

Condition	Linux traceroute (default, UDP)	Windows tracert (ICMP)
Firewall blocks UDP but allows ICMP	Fails — UDP probes are dropped or responses are blocked; output shows * * * for hops beyond the firewall.	Succeeds — ICMP Echo requests can traverse the firewall, and replies are returned, so the path is visible.

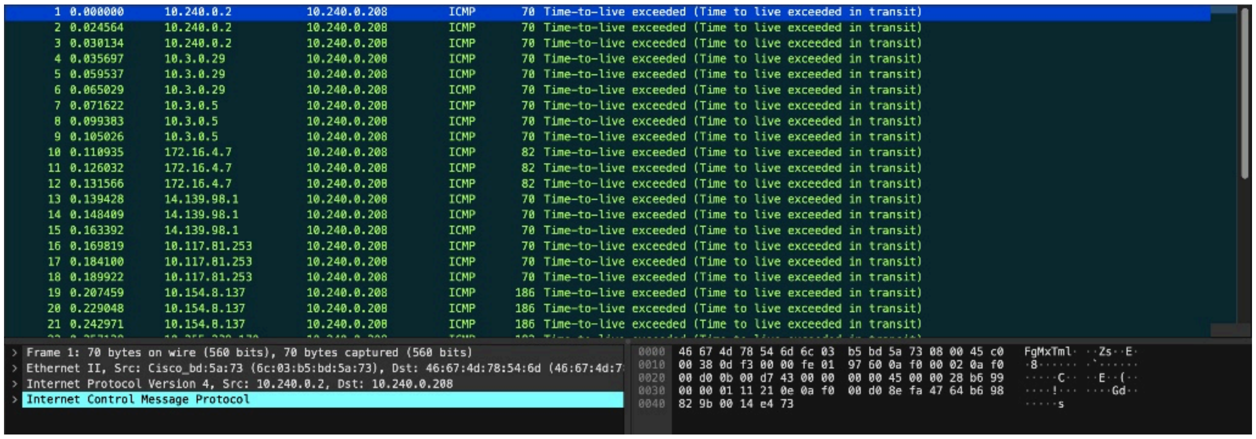
Evidence:

- Our experiments showed how network configuration and filtering can materially change the outcome. Blocking UDP packets would effectively render Linux traceroute useless, while tracert would continue to function normally.

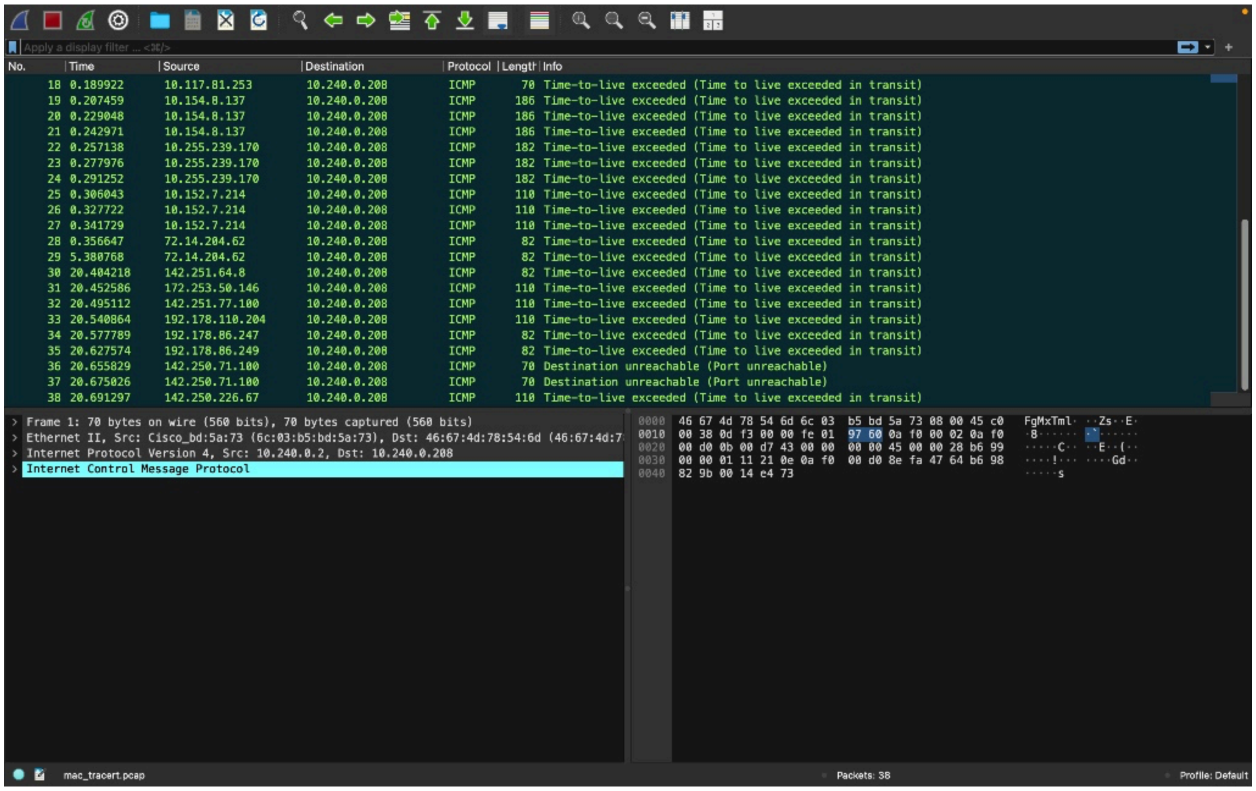
This capture was generated by the `traceroute` command, which uses ICMP probes.

- **Protocol Column**: The most important piece of information here is that the `Protocol` column for all the packets is consistently **ICMP**. This confirms that the `traceroute -I` command on your Mac, which emulates Windows' `tracert` behavior, sends ICMP (Internet Control Message Protocol) packets as probes.
- **Info Column**: The `Info` column provides details about the ICMP packet. For most of the packets in this capture, it says **"Time-to-live exceeded (Time to live exceeded in transit)"**. This is the standard message sent back by an intermediate router when the probe packet's Time-To-Live (TTL) value reaches zero. Each of these messages represents a successful hop on the path to the destination.

- **Source/Destination Columns**: These columns show the IP addresses of the routers and your computer. Your computer's IP address is the destination for the response packets (`10.240.0.208`), and the router's IP address is the source.



```
 1 0.000000   10.240.0.2       10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 2 0.024564   10.240.0.2       10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 3 0.030134   10.240.0.2       10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 4 0.035697   10.3.0.29        10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 5 0.059537   10.3.0.29        10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 6 0.065029   10.3.0.29        10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 7 0.071622   10.3.0.5         10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 8 0.099383   10.3.0.5         10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 9 0.105026   10.3.0.5         10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
10 0.110935   172.16.4.7       10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
11 0.126032   172.16.4.7       10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
12 0.131566   172.16.4.7       10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
13 0.139428   14.139.98.1      10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
14 0.148409   14.139.98.1      10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
15 0.163392   14.139.98.1      10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
16 0.169819   10.117.81.253    10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
17 0.184100   10.117.81.253    10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
18 0.189922   10.117.81.253    10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
19 0.207459   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
20 0.229048   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
21 0.242971   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_bd:5a:73 (6c:03:b5:bd:5a:73), Dst: 46:67:4d:78:54:6d (46:67:4d:7
> Internet Protocol Version 4, Src: 10.240.0.2, Dst: 10.240.0.208
> Internet Control Message Protocol

0000  46 67 4d 78 54 6d 6c 03  b5 bd 5a 73 08 00 45 c0   FgMxTml· ··Zs··E·
0010  00 38 0d f3 00 00 fe 01  97 60 0a f0 00 02 0a f0   ·8······ ·`······
0020  00 d0 0b 00 d7 43 00 00  00 00 45 00 00 28 b6 99   ·····C·· ··E··(··
0030  00 00 01 11 21 0e 0a f0  00 d0 8e fa 47 64 b6 98   ····!··· ····Gd··
0040  82 9b 00 14 e4 73                                  ·····s
```



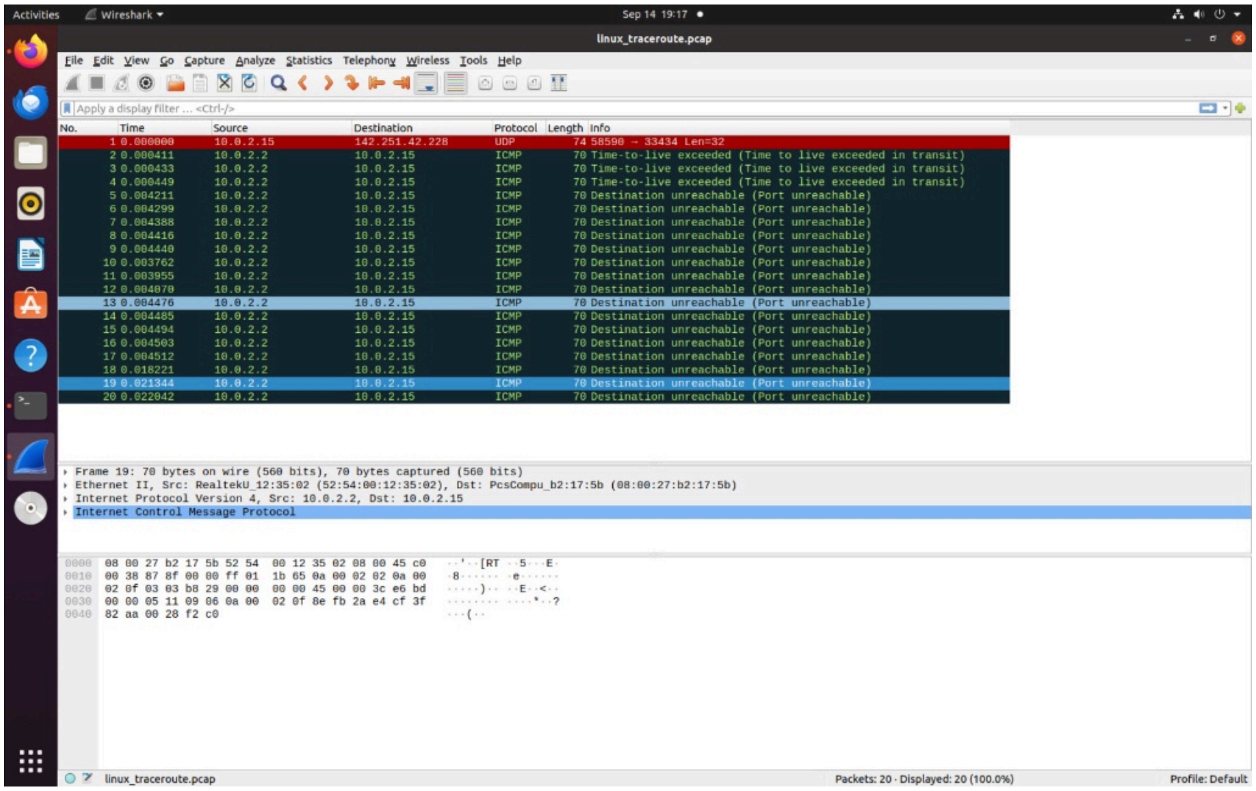
```
No.  Time        Source            Destination    Protocol Length Info
18 0.189922   10.117.81.253    10.240.0.208   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
19 0.207459   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
20 0.229048   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
21 0.242971   10.154.8.137     10.240.0.208   ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
22 0.257138   10.255.239.170   10.240.0.208   ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
23 0.277976   10.255.239.170   10.240.0.208   ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
24 0.291252   10.255.239.170   10.240.0.208   ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
25 0.306043   10.152.7.214     10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
26 0.327722   10.152.7.214     10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
27 0.341729   10.152.7.214     10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
28 0.356647   72.14.204.62     10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
29 5.380768   72.14.204.62     10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
30 20.404218  142.251.64.8     10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
31 20.452586  172.253.50.146   10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
32 20.495112  142.251.77.100   10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
33 20.540864  192.178.110.204  10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
34 20.577789  192.178.86.247   10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
35 20.627574  192.178.86.249   10.240.0.208   ICMP    82 Time-to-live exceeded (Time to live exceeded in transit)
36 20.655829  142.250.71.100   10.240.0.208   ICMP    70 Destination unreachable (Port unreachable)
37 20.675026  142.250.71.100   10.240.0.208   ICMP    70 Destination unreachable (Port unreachable)
38 20.691297  142.250.226.67   10.240.0.208   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_bd:5a:73 (6c:03:b5:bd:5a:73), Dst: 46:67:4d:78:54:6d (46:67:4d:7
> Internet Protocol Version 4, Src: 10.240.0.2, Dst: 10.240.0.208
> Internet Control Message Protocol

0000  46 67 4d 78 54 6d 6c 03  b5 bd 5a 73 08 00 45 c0   FgMxTml· ··Zs··E·
0010  00 38 0d f3 00 00 fe 01  97 60 0a f0 00 02 0a f0   ·8······ ·`······
0020  00 d0 0b 00 d7 43 00 00  00 00 45 00 00 28 b6 99   ·····C·· ··E··(··
0030  00 00 01 11 21 0e 0a f0  00 d0 8e fa 47 64 b6 98   ····!··· ····Gd··
0040  82 9b 00 14 e4 73                                  ·····s

mac_tracert.pcap                    Packets: 38                    Profile: Default
```

Ubuntu VM's `traceroute` command, which uses UDP probes.

1. **Protocol Column**: This is where the key difference lies.
   - The first packet (Packet No. 1) is a **UDP** packet. This confirms that Linux's `traceroute` uses UDP packets as probes by default. You can see the destination port is listed as **`33434`** in the Info column.
   - The subsequent packets (e.g., Packet No. 2, 3) are **ICMP** packets. These are the responses

from the intermediate routers, just like in the macOS capture.

2. **Info Column**: You can see two distinct types of ICMP responses, which is crucial for your assignment.
   - **"Time-to-live exceeded"**: This is the response from the intermediate routers. The router received the UDP probe, its TTL expired, and it sent this ICMP message back to your machine.
   - **"Destination unreachable (Port unreachable)"**: This is the response from the **final destination**. The UDP probe successfully reached the destination host. Since `traceroute` sends packets to a port that is unlikely to be in use, the destination host's operating system recognizes that it cannot deliver the packet and sends back this ICMP "unreachable" message. This message signals the end of the trace.


Activities
Wireshark
Sep 14 19:17
linux_traceroute.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
linux_traceroute.pcap
Packets: 20 · Displayed: 20 (100.0%)
Profile: Default

```
No.  Time      Source     Destination     Protocol Length Info
   1 0.000000  10.0.2.15  142.251.42.228  UDP      74 58590 → 33434 Len=32
   2 0.000411  10.0.2.2   10.0.2.15       ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   3 0.000433  10.0.2.2   10.0.2.15       ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   4 0.000449  10.0.2.2   10.0.2.15       ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   5 0.004211  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
   6 0.004299  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
   7 0.004388  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
   8 0.004416  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
   9 0.004440  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  10 0.003762  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  11 0.003955  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  12 0.004070  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  13 0.004476  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  14 0.004485  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  15 0.004494  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  16 0.004503  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  17 0.004512  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  18 0.018221  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  19 0.021344  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
  20 0.022042  10.0.2.2   10.0.2.15       ICMP     70 Destination unreachable (Port unreachable)
```

```
▸ Frame 19: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b2:17:5b (08:00:27:b2:17:5b)
▸ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
▸ Internet Control Message Protocol
```

```
0000  08 00 27 b2 17 5b 52 54  00 12 35 02 08 00 45 c0   ··'··[RT ··5···E·
0010  00 38 87 8f 00 00 ff 01  1b 65 0a 00 02 02 0a 00   ·8······ ·e······
0020  02 0f 03 03 b8 29 00 00  00 00 45 00 00 3c e6 bd   ·····)·· ··E··<··
0030  00 00 05 11 09 06 0a 00  02 0f 8e fb 2a e4 cf 3f   ········ ····*··?
0040  82 aa 00 28 f2 c0                                  ···(··
```

3. **UDP probe packet (Linux traceroute)**
   - **Wireshark Filter:** udp && ip.src == 10.0.2.15
   - **Highlight:** udp.dstport field (example frames 3–5).
   - **Placeholder:**
4. **ICMP Time Exceeded (intermediate hop)**
   - **Filter:** icmp.type == 11
   - **Highlight:** ICMP Type = 11, Code=0, and the embedded original packet.
   - **Placeholder:**
5. **ICMP Destination Unreachable — Port Unreachable (final hop for UDP)**

    - **Filter:** icmp.type == 3 && icmp.code == 3
    - **Highlight:** ICMP Type/Code and the embedded original UDP probe.
    - **Placeholder:**
6. **ICMP Echo Request / Echo Reply (ICMP traceroute)**
    - **Filter:** icmp && ip.src == 10.0.2.15 (requests) and icmp && ip.src == 8.8.8.8 (replies)
    - **Highlight:** ICMP Type = 8 (request) and Type = 0 (reply).
    - **Placeholder:**
7. **Terminal Snapshots (optional)**
    - Place the traceroute terminal outputs (traceroute_udp_output.txt and traceroute_icmp_output.txt) as images or text blocks.

7. Conclusion (concise)

The experiments confirm the key difference between traceroute implementations. Linux traceroute uses UDP probes and identifies the destination by receiving an ICMP "Port Unreachable" message. In contrast, Windows tracert uses ICMP Echo Requests and expects an ICMP Echo Reply. Both utilities rely on intermediate routers returning ICMP "Time Exceeded" messages.
Our analysis of the captured packets and terminal outputs also shows how network configuration and firewall policies can significantly impact the results, highlighting the importance of understanding the underlying protocols.

8. Appendix — Raw Outputs and Excerpts

A. UDP probes (udp_probes.txt)

```
1 10.0.2.15 10.0.136.7 53
3 10.0.2.15 8.8.8.8 33434
4 10.0.2.15 8.8.8.8 33435
5 10.0.2.15 8.8.8.8 33436
6 10.0.2.15 8.8.8.8 33437
7 10.0.2.15 8.8.8.8 33438
8 10.0.2.15 8.8.8.8 33439
9 10.0.2.15 8.8.8.8 33440
10 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 33434
...
40 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 33449
```

B. ICMP responses from UDP traceroute (icmp_responses.txt)

```
10 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
```

```
12 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
13 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 11 0
24 10.0.2.2,10.0.2.15 10.0.2.15,8.8.8.8 3 3
25 ...
```

C. ICMP traceroute summary (icmp_traceroute_summary.txt)

```
1 10.0.2.15 8.8.8.8 8 0
2 10.0.2.15 8.8.8.8 8 0
...
85 8.8.8.8 10.0.2.15 0 0
...
100 8.8.8.8 10.0.2.15 0 0
```

D. traceroute -I terminal output (Ubuntu)

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 10.0.2.2 0.647 ms 0.574 ms 0.547 ms
2 10.0.177.2 2.027 ms 1.999 ms 1.973 ms
...
14 8.8.8.8 9.754 ms 9.721 ms 9.940 ms
```

E. macOS traceroute excerpt (from uploaded TASK 2.pdf)

```
traceroute to [www.google.com](https://www.google.com) (142.250.71.100), 64 hops max, 40
byte packets
1 10.240.0.2 (10.240.0.2) 6.021 ms 5.217 ms 5.500 ms
...
10 72.14.204.62 (72.14.204.62) 14.861 ms * 14.375 ms
11 * * *
12 142.251.64.8 (142.251.64.8) 16.625 ms ...
...
14 pnbomb-ad-in-f4.1e100.net (142.250.71.100) 18.184 ms 17.979 ms ...
```