CS331: Computer Networks Assignment 1

Aniket Mishra : 23110026
Zainab Kapadia : 23110373

September 15, 2025

Contents

1 DNS Resolver Results

Custom header value (HHMMSSID)	Domain name	Resolved IP address
08362900	facebook.com	192.168.1.0
08362901	stackoverflow.com	192.168.1.1
08362902	example.com	192.168.1.2
08363003	linkedin.com	192.168.1.3
08363004	apple.com	192.168.1.4
08363005	google.com	192.168.1.0

Table 1: Resolved DNS queries with custom headers

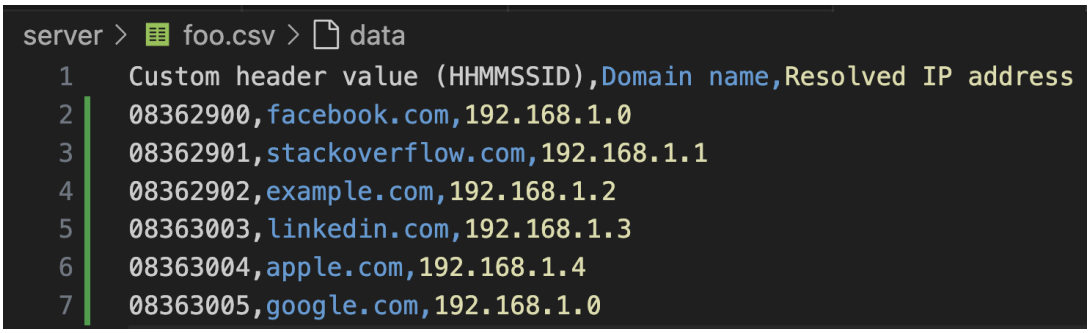


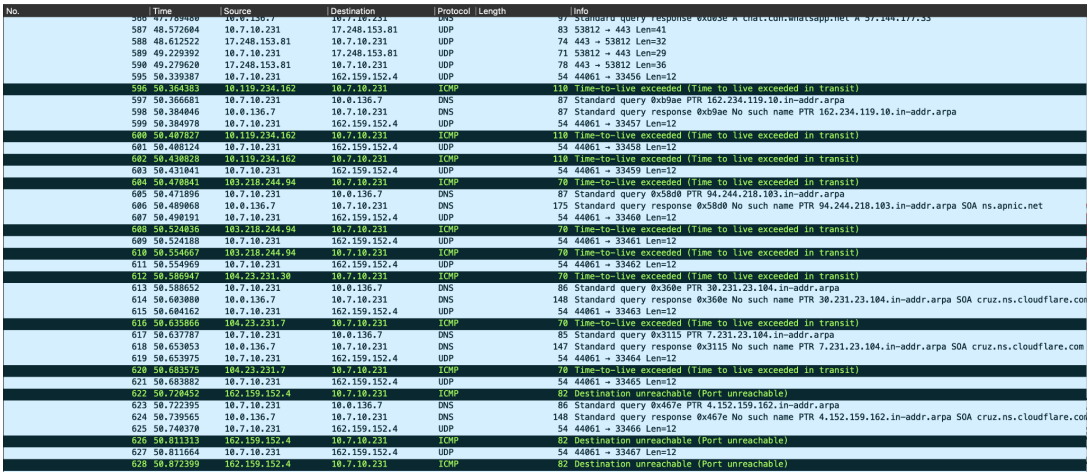
Figure 1: Screenshot of the generated CSV file (foo.csv) showing custom header, domain name, and resolved IP address for each DNS query.

2 Traceroute Protocol Behavior

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

No.	Time	Source	Destination	Protocol	Length	Info
144	5.257831	10.7.10.231	162.159.152.4	UDP	54	44061 → 33435 Len=12
145	5.260418	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
146	5.263061	10.7.10.231	10.0.136.7	DNS	81	Standard query 0xee4d PTR 5.0.7.10.in-addr.arpa
147	5.266487	10.0.136.7	10.7.10.231	DNS	81	Standard query response 0xee4d No such name PTR 5.0.7.10.in-addr.arpa
148	5.267492	10.7.10.231	162.159.152.4	UDP	54	44061 → 33436 Len=12
149	5.269942	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
150	5.270069	10.7.10.231	162.159.152.4	UDP	54	44061 → 33437 Len=12
151	5.272498	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	5.272643	10.7.10.231	162.159.152.4	UDP	54	44061 → 33438 Len=12
153	5.274785	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
154	5.275390	10.7.10.231	162.159.152.4	UDP	54	44061 → 33439 Len=12
155	5.277463	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
156	5.277518	10.7.10.231	162.159.152.4	UDP	54	44061 → 33440 Len=12
157	5.279585	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
158	5.279664	10.7.10.231	162.159.152.4	UDP	54	44061 → 33441 Len=12
159	5.283550	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
160	5.284273	10.7.10.231	162.159.152.4	UDP	54	44061 → 33442 Len=12
161	5.288031	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
162	5.288129	10.7.10.231	162.159.152.4	UDP	54	44061 → 33443 Len=12
163	5.292646	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
164	5.292765	10.7.10.231	162.159.152.4	UDP	54	44061 → 33444 Len=12
165	5.295104	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
166	5.296009	10.7.10.231	10.0.136.7	DNS	86	Standard query 0x584f PTR 253.81.117.10.in-addr.arpa
167	5.299429	10.0.136.7	10.7.10.231	DNS	86	Standard query response 0x584f No such name PTR 253.81.117.10.in-addr.arpa
168	5.299975	10.7.10.231	162.159.152.4	UDP	54	44061 → 33445 Len=12
169	5.302726	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	5.302828	10.7.10.231	162.159.152.4	UDP	54	44061 → 33446 Len=12
171	5.305085	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figure 2: Example traceroute UDP probe packets in Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
586	47.569460	10.7.10.231	162.159.152.4	UDP	97	Standard query response 0xd65e A chat.com.whatsapp.net A 57.144.177.53
587	48.572604	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
588	48.612522	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
589	49.229392	10.7.10.231	17.248.153.81	UDP	71	53812 → 443 Len=29
590	49.279620	17.248.153.81	10.7.10.231	UDP	78	443 → 53812 Len=36
595	50.339387	10.7.10.231	162.159.152.4	UDP	54	44061 → 33456 Len=12
596	50.364383	10.119.234.162	10.7.10.231	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
597	50.366681	10.7.10.231	10.0.136.7	DNS	87	Standard query 0xb9ae PTR 162.234.119.10.in-addr.arpa
598	50.384046	10.0.136.7	10.7.10.231	DNS	87	Standard query response 0xb9ae No such name PTR 162.234.119.10.in-addr.arpa
599	50.384978	10.7.10.231	162.159.152.4	UDP	54	44061 → 33457 Len=12
600	50.407827	10.119.234.162	10.7.10.231	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
601	50.408124	10.7.10.231	162.159.152.4	UDP	54	44061 → 33458 Len=12
602	50.430828	10.119.234.162	10.7.10.231	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
603	50.431041	10.7.10.231	162.159.152.4	UDP	54	44061 → 33459 Len=12
604	50.470841	103.218.244.94	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
605	50.471896	10.7.10.231	10.0.136.7	DNS	87	Standard query 0x58d0 PTR 94.244.218.103.in-addr.arpa
606	50.489068	10.0.136.7	10.7.10.231	DNS	175	Standard query response 0x58d0 No such name PTR 94.244.218.103.in-addr.arpa SOA ns.apnic.net
607	50.490191	10.7.10.231	162.159.152.4	UDP	54	44061 → 33460 Len=12
608	50.524036	103.218.244.94	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
609	50.524188	10.7.10.231	162.159.152.4	UDP	54	44061 → 33461 Len=12
610	50.554667	103.218.244.94	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
611	50.554969	10.7.10.231	162.159.152.4	UDP	54	44061 → 33462 Len=12
612	50.586947	104.23.231.30	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
613	50.586652	10.7.10.231	10.0.136.7	DNS	86	Standard query 0x360e PTR 30.231.23.104.in-addr.arpa
614	50.603080	10.0.136.7	10.7.10.231	DNS	148	Standard query response 0x360e No such name PTR 30.231.23.104.in-addr.arpa SOA cruz.ns.cloudflare.com
615	50.604162	10.7.10.231	162.159.152.4	UDP	54	44061 → 33463 Len=12
616	50.635866	104.23.231.7	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
617	50.637787	10.7.10.231	10.0.136.7	DNS	85	Standard query 0x3115 PTR 7.231.23.104.in-addr.arpa
618	50.653053	10.0.136.7	10.7.10.231	DNS	147	Standard query response 0x3115 No such name PTR 7.231.23.104.in-addr.arpa SOA cruz.ns.cloudflare.com
619	50.653975	10.7.10.231	162.159.152.4	UDP	54	44061 → 33464 Len=12
620	50.683575	104.23.231.7	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
621	50.683882	10.7.10.231	162.159.152.4	UDP	54	44061 → 33465 Len=12
622	50.720452	162.159.152.4	10.7.10.231	ICMP	82	Destination unreachable (Port unreachable)
623	50.722395	10.7.10.231	10.0.136.7	DNS	86	Standard query 0x467e PTR 4.152.159.162.in-addr.arpa
624	50.739565	10.0.136.7	10.7.10.231	DNS	148	Standard query response 0x467e No such name PTR 4.152.159.162.in-addr.arpa SOA cruz.ns.cloudflare.com
625	50.740370	10.7.10.231	162.159.152.4	UDP	54	44061 → 33466 Len=12
626	50.811313	162.159.152.4	10.7.10.231	ICMP	82	Destination unreachable (Port unreachable)
627	50.811664	10.7.10.231	162.159.152.4	UDP	54	44061 → 33467 Len=12
628	50.872399	162.159.152.4	10.7.10.231	ICMP	82	Destination unreachable (Port unreachable)

Figure 3: ICMP replies to traceroute probes showing Time Exceeded and Port Unreachable messages.

On Linux, traceroute sends **UDP (User Datagram Protocol)** packets to incrementing high ports (starting from 33435). Each probe uses a different port number, and routers reply with ICMP Time Exceeded messages when the TTL expires. The destination host replies with ICMP Port Unreachable, which signals the completion of the trace.

No.	Time	Source	Destination	Protocol	Length	Info
70	2.575826	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=145/37120, ttl=1 (no response found!)
73	2.781345	10.7.0.5	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
74	2.783891	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=146/37376, ttl=1 (no response found!)
173	6.334593	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=147/37632, ttl=1 (no response found!)
174	6.338642	10.7.0.5	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
269	9.647466	10.7.0.5	10.7.24.190	ICMP	70	Destination unreachable (Port unreachable)
357	12.301877	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=148/37888, ttl=2 (no response found!)
358	12.303788	172.16.4.7	10.7.24.190	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
359	12.306199	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=149/38144, ttl=2 (no response found!)
360	12.307966	172.16.4.7	10.7.24.190	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
361	12.309081	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=150/38400, ttl=2 (no response found!)
362	12.315149	172.16.4.7	10.7.24.190	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
434	12.780424	10.7.0.5	10.7.24.190	ICMP	70	Destination unreachable (Port unreachable)
515	17.853281	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=151/38656, ttl=3 (no response found!)
518	17.864886	14.139.98.1	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
519	17.867846	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=152/38912, ttl=3 (no response found!)
520	17.872822	14.139.98.1	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
521	17.874364	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=153/39168, ttl=3 (no response found!)
523	17.878104	14.139.98.1	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
528	17.976402	14.139.98.1	10.7.24.190	ICMP	70	Destination unreachable (Port unreachable)
530	19.460488	14.139.98.1	10.7.24.190	ICMP	70	Destination unreachable (Port unreachable)
675	20.961238	14.139.98.1	10.7.24.190	ICMP	70	Destination unreachable (Port unreachable)
709	23.473866	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=154/39424, ttl=4 (no response found!)
710	23.478525	10.117.81.253	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
711	23.482579	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=155/39680, ttl=4 (no response found!)
712	23.484854	10.117.81.253	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
713	23.488317	10.7.24.190	162.159.152.4	ICMP	106	Echo (ping) request id=0x0001, seq=156/39936, ttl=4 (no response found!)
714	23.490309	10.117.81.253	10.7.24.190	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
718	23.514157	172.16.4.7	10.7.24.190	ICMP	120	Time-to-live exceeded (Time to live exceeded in transit)

Figure 4: Windows tracert probe packets in Wireshark showing ICMP Echo Requests.

On Windows, the tracert command uses the **ICMP (Internet Control Message Protocol) Echo Request** for each probe by default. This is confirmed by inspecting the Wireshark capture, which displays the `ICMP` protocol for all outgoing tracert packets. Each router along the path replies with an ICMP Time Exceeded message, and the destination responds with an ICMP Echo Reply.

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

As can be seen from the image, we did not receive any responses for the router with IP address `10.7.10.231` for hops numbered from destination ports 33447 to 33456 (three probes per hop and three hops in total, corresponding to hops 5 to 7 in the traceroute

output). This absence of ICMP "Time-to-live exceeded" replies in the packet capture matches the *** entries in the terminal output, indicating the router did not respond to any of the traceroute probes for those TTLs.

This behavior can be reasoned due to:

- **Firewall or Security Policy Blocking Replies:** The router's firewall may block ICMP Time Exceeded or UDP error replies which prevented traceroute from receiving a response for those probes. Since we are on an institute and secure network environment, the routers might be configured not to send responses to traceroute packets, and this can be observed where all three probes go unanswered, resulting in *** in traceroute output.
- **ICMP Rate Limiting Due to Excessive Probes:** As the capture shows, traceroute sent probes starting from port 33435 up to 33446 before reaching the unresponsive sequence. This is a total of 12 sets of probes, which may trigger rate limiting or overload protection on the router. If too many probes are received in a short time interval, the router may limit the number of ICMP replies it generates, start ignoring some requests, and not respond at all for those TTLs and probes.

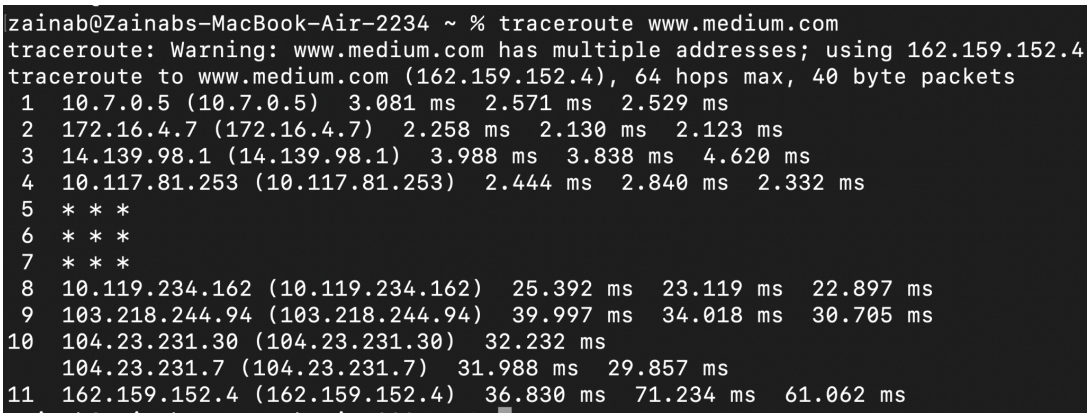


Figure 5: Traceroute output showing non-responsive hops as ***.

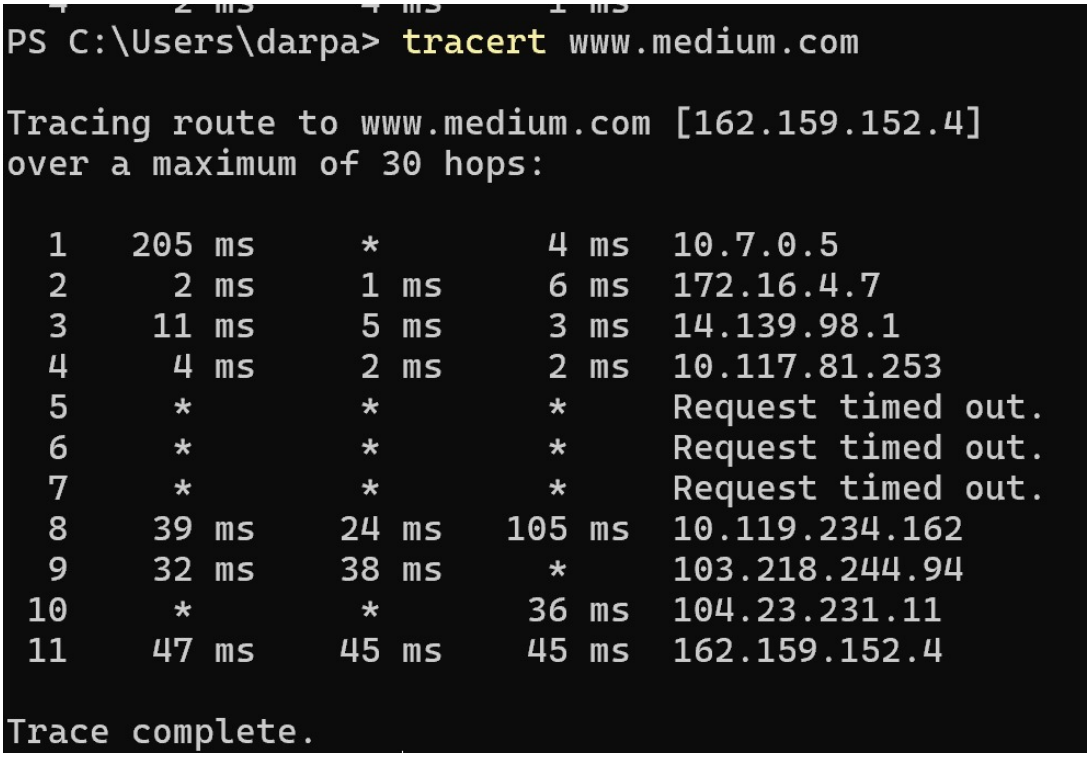
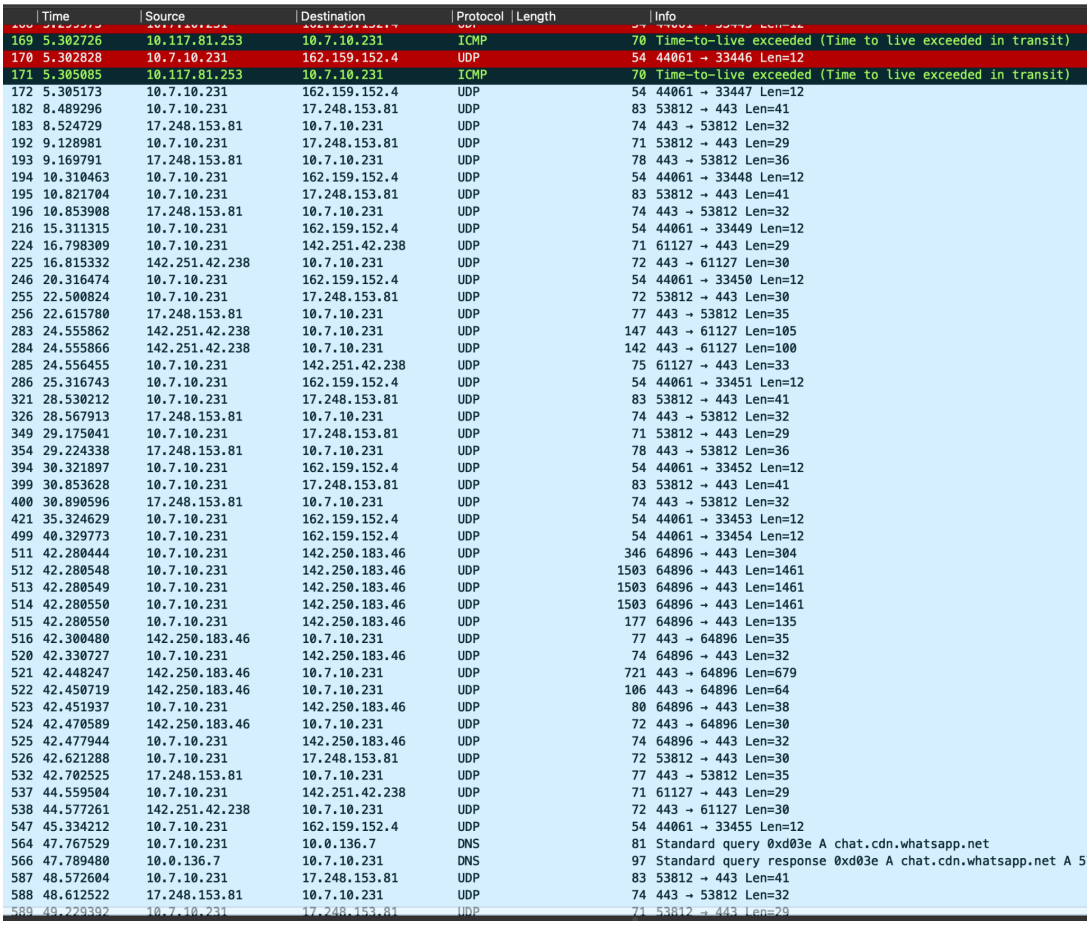


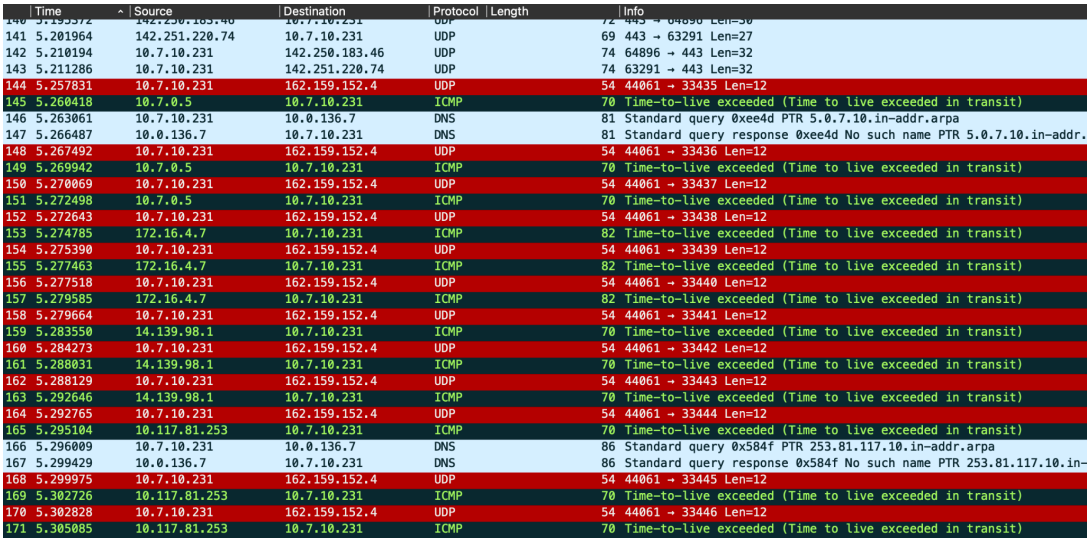
Figure 6: Windows tracert command output showing hop responses and non-responses.



	Time	Source	Destination	Protocol	Length	Info
169	5.302726	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	5.302828	10.7.10.231	162.159.152.4	UDP	54	44061 → 33446 Len=12
171	5.305085	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
172	5.305173	10.7.10.231	162.159.152.4	UDP	54	44061 → 33447 Len=12
182	8.489296	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
183	8.524729	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
192	9.128981	10.7.10.231	17.248.153.81	UDP	71	53812 → 443 Len=29
193	9.169791	17.248.153.81	10.7.10.231	UDP	78	443 → 53812 Len=36
194	10.310463	10.7.10.231	162.159.152.4	UDP	54	44061 → 33448 Len=12
195	10.821704	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
196	10.853908	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
216	15.311315	10.7.10.231	162.159.152.4	UDP	54	44061 → 33449 Len=12
224	16.798309	10.7.10.231	142.251.42.238	UDP	71	61127 → 443 Len=29
225	16.815332	142.251.42.238	10.7.10.231	UDP	72	443 → 61127 Len=30
246	20.316474	10.7.10.231	162.159.152.4	UDP	54	44061 → 33450 Len=12
255	22.500824	10.7.10.231	17.248.153.81	UDP	72	53812 → 443 Len=30
256	22.615780	17.248.153.81	10.7.10.231	UDP	77	443 → 53812 Len=35
283	24.555862	142.251.42.238	10.7.10.231	UDP	147	443 → 61127 Len=105
284	24.555866	142.251.42.238	10.7.10.231	UDP	142	443 → 61127 Len=100
285	24.556455	10.7.10.231	142.251.42.238	UDP	75	61127 → 443 Len=33
286	25.316743	10.7.10.231	162.159.152.4	UDP	54	44061 → 33451 Len=12
321	28.530212	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
326	28.567913	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
349	29.175041	10.7.10.231	17.248.153.81	UDP	71	53812 → 443 Len=29
354	29.224338	17.248.153.81	10.7.10.231	UDP	78	443 → 53812 Len=36
394	30.321897	10.7.10.231	162.159.152.4	UDP	54	44061 → 33452 Len=12
399	30.853628	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
400	30.890596	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
421	35.324629	10.7.10.231	162.159.152.4	UDP	54	44061 → 33453 Len=12
499	40.329773	10.7.10.231	162.159.152.4	UDP	54	44061 → 33454 Len=12
511	42.280444	10.7.10.231	142.250.183.46	UDP	346	64896 → 443 Len=304
512	42.280548	10.7.10.231	142.250.183.46	UDP	1503	64896 → 443 Len=1461
513	42.280549	10.7.10.231	142.250.183.46	UDP	1503	64896 → 443 Len=1461
514	42.280550	10.7.10.231	142.250.183.46	UDP	1503	64896 → 443 Len=1461
515	42.280550	10.7.10.231	142.250.183.46	UDP	177	64896 → 443 Len=135
516	42.300480	142.250.183.46	10.7.10.231	UDP	77	443 → 64896 Len=35
520	42.330727	10.7.10.231	142.250.183.46	UDP	74	64896 → 443 Len=32
521	42.448247	142.250.183.46	10.7.10.231	UDP	721	443 → 64896 Len=679
522	42.450719	142.250.183.46	10.7.10.231	UDP	106	443 → 64896 Len=64
523	42.451937	10.7.10.231	142.250.183.46	UDP	80	64896 → 443 Len=38
524	42.470589	142.250.183.46	10.7.10.231	UDP	72	443 → 64896 Len=30
525	42.477944	10.7.10.231	142.250.183.46	UDP	74	64896 → 443 Len=32
526	42.621288	10.7.10.231	17.248.153.81	UDP	72	53812 → 443 Len=30
532	42.702525	17.248.153.81	10.7.10.231	UDP	77	443 → 53812 Len=35
537	44.559504	10.7.10.231	142.251.42.238	UDP	71	61127 → 443 Len=29
538	44.577261	142.251.42.238	10.7.10.231	UDP	72	443 → 61127 Len=30
547	45.334212	10.7.10.231	162.159.152.4	UDP	54	44061 → 33455 Len=12
564	47.767529	10.7.10.231	10.0.136.7	DNS	81	Standard query 0xd03e A chat.cdn.whatsapp.net
566	47.789480	10.0.136.7	10.7.10.231	DNS	97	Standard query response 0xd03e A chat.cdn.whatsapp.net A 5
587	48.572604	10.7.10.231	17.248.153.81	UDP	83	53812 → 443 Len=41
588	48.612522	17.248.153.81	10.7.10.231	UDP	74	443 → 53812 Len=32
589	49.229392	10.7.10.231	17.248.153.81	UDP	71	53812 → 443 Len=29

Figure 7: Wireshark capture showing UDP probes to 10.7.10.231 for hops 5, 6, and 7 (ports 33447–33456) with no corresponding ICMP reply packets.

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



	Time	Source	Destination	Protocol	Length	Info
141	5.201964	142.251.220.74	10.7.10.231	UDP	69	443 → 63291 Len=27
142	5.210194	10.7.10.231	142.250.183.46	UDP	74	64896 → 443 Len=32
143	5.211286	10.7.10.231	142.251.220.74	UDP	74	63291 → 443 Len=32
144	5.257831	10.7.10.231	162.159.152.4	UDP	54	44061 → 33435 Len=12
145	5.260418	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
146	5.263061	10.7.10.231	10.0.136.7	DNS	81	Standard query 0xee4d PTR 5.0.7.10.in-addr.arpa
147	5.266487	10.0.136.7	10.7.10.231	DNS	81	Standard query response 0xee4d No such name PTR 5.0.7.10.in-addr.
148	5.267492	10.7.10.231	162.159.152.4	UDP	54	44061 → 33436 Len=12
149	5.269942	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
150	5.270069	10.7.10.231	162.159.152.4	UDP	54	44061 → 33437 Len=12
151	5.272498	10.7.0.5	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	5.272643	10.7.10.231	162.159.152.4	UDP	54	44061 → 33438 Len=12
153	5.274785	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
154	5.275390	10.7.10.231	162.159.152.4	UDP	54	44061 → 33439 Len=12
155	5.277463	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
156	5.277518	10.7.10.231	162.159.152.4	UDP	54	44061 → 33440 Len=12
157	5.279585	172.16.4.7	10.7.10.231	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
158	5.279664	10.7.10.231	162.159.152.4	UDP	54	44061 → 33441 Len=12
159	5.283550	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
160	5.284273	10.7.10.231	162.159.152.4	UDP	54	44061 → 33442 Len=12
161	5.288031	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
162	5.288129	10.7.10.231	162.159.152.4	UDP	54	44061 → 33443 Len=12
163	5.292646	14.139.98.1	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
164	5.292765	10.7.10.231	162.159.152.4	UDP	54	44061 → 33444 Len=12
165	5.295104	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
166	5.296009	10.7.10.231	10.0.136.7	DNS	86	Standard query 0x584f PTR 253.81.117.10.in-addr.arpa
167	5.299429	10.0.136.7	10.7.10.231	DNS	86	Standard query response 0x584f No such name PTR 253.81.117.10.in-
168	5.299975	10.7.10.231	162.159.152.4	UDP	54	44061 → 33445 Len=12
169	5.302726	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	5.302828	10.7.10.231	162.159.152.4	UDP	54	44061 → 33446 Len=12
171	5.305085	10.117.81.253	10.7.10.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figure 8: Wireshark capture showing incrementing destination UDP ports.

In Linux traceroute, the destination UDP port number in the probe packets changes between successive probes sent to the destination.

As can be seen from the terminal output, the very first probe was sent to the router with IP address `10.7.0.5`, showing response times of 3.081 ms, 2.571 ms, and 2.529 ms for the three probes. This directly corresponds to the Wireshark output, where rows 144, 148, and 150 also reference `10.7.0.5` as the destination, with all field values except the destination UDP port number remaining the same. In each successive probe, the destination port is incremented by one which is clearly visible in the Info field of these Wireshark rows (e.g., destination ports 33435, 33436, 33437). Thus, in Linux traceroute, the field in the probe packets that changes between successive probes sent to the destination is the destination UDP port number, while the other packet fields (source IP, destination IP, protocol type) remain constant for each hop.

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

In Linux traceroute, the response from an intermediate hop is an ICMP "Time-to-live exceeded" message, which is generated when the TTL of the probe packet expires at a router along the path. While, the response from the final hop (the destination) is an ICMP "Destination unreachable (Port unreachable)" message, indicating that the UDP probe reached the destination but targeted a closed port. This difference is clearly visible in my Wireshark captures, where intermediate routers reply with Time Exceeded message and the destination host replies with Destination Unreachable, Port Unreachable message.

595	50.339387	10.7.10.231	162.159.152.4	UDP	54 44061 → 33456 Len=12
596	50.364383	10.119.234.162	10.7.10.231	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
597	50.366681	10.7.10.231	10.0.136.7	DNS	87 Standard query 0xb9ae PTR 162.234.119.10.in-addr.arpa
598	50.384046	10.0.136.7	10.7.10.231	DNS	87 Standard query response 0xb9ae No such name PTR 162.234.119
599	50.384978	10.7.10.231	162.159.152.4	UDP	54 44061 → 33457 Len=12
600	50.407827	10.119.234.162	10.7.10.231	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
601	50.408124	10.7.10.231	162.159.152.4	UDP	54 44061 → 33458 Len=12
602	50.430828	10.119.234.162	10.7.10.231	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
603	50.431041	10.7.10.231	162.159.152.4	UDP	54 44061 → 33459 Len=12
604	50.470841	103.218.244.94	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
605	50.471896	10.7.10.231	10.0.136.7	DNS	87 Standard query 0x58d0 PTR 94.244.218.103.in-addr.arpa
606	50.489068	10.0.136.7	10.7.10.231	DNS	175 Standard query response 0x58d0 No such name PTR 94.244.218.
607	50.490191	10.7.10.231	162.159.152.4	UDP	54 44061 → 33460 Len=12
608	50.524036	103.218.244.94	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
609	50.524188	10.7.10.231	162.159.152.4	UDP	54 44061 → 33461 Len=12
610	50.554667	103.218.244.94	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
611	50.554969	10.7.10.231	162.159.152.4	UDP	54 44061 → 33462 Len=12
612	50.586947	104.23.231.30	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
613	50.588652	10.7.10.231	10.0.136.7	DNS	86 Standard query 0x360e PTR 30.231.23.104.in-addr.arpa
614	50.603080	10.0.136.7	10.7.10.231	DNS	148 Standard query response 0x360e No such name PTR 30.231.23.1
615	50.604162	10.7.10.231	162.159.152.4	UDP	54 44061 → 33463 Len=12
616	50.635866	104.23.231.7	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
617	50.637787	10.7.10.231	10.0.136.7	DNS	85 Standard query 0x3115 PTR 7.231.23.104.in-addr.arpa
618	50.653053	10.0.136.7	10.7.10.231	DNS	147 Standard query response 0x3115 No such name PTR 7.231.23.10
619	50.653975	10.7.10.231	162.159.152.4	UDP	54 44061 → 33464 Len=12
620	50.683575	104.23.231.7	10.7.10.231	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
621	50.683882	10.7.10.231	162.159.152.4	UDP	54 44061 → 33465 Len=12
622	50.720452	162.159.152.4	10.7.10.231	ICMP	82 Destination unreachable (Port unreachable)
623	50.722395	10.7.10.231	10.0.136.7	DNS	86 Standard query 0x467e PTR 4.152.159.162.in-addr.arpa
624	50.739565	10.0.136.7	10.7.10.231	DNS	148 Standard query response 0x467e No such name PTR 4.152.159.1
625	50.740370	10.7.10.231	162.159.152.4	UDP	54 44061 → 33466 Len=12
626	50.811313	162.159.152.4	10.7.10.231	ICMP	82 Destination unreachable (Port unreachable)
627	50.811664	10.7.10.231	162.159.152.4	UDP	54 44061 → 33467 Len=12
628	50.872399	162.159.152.4	10.7.10.231	ICMP	82 Destination unreachable (Port unreachable)
629	50.895828	10.7.10.231	17.248.153.81	UDP	83 53812 → 443 Len=41
630	50.933982	17.248.153.81	10.7.10.231	UDP	74 443 → 53812 Len=32

Figure 9: ICMP Time Exceeded replies from intermediate routers and ICMP Port Unreachable from final destination.

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

If a firewall blocks UDP traffic but allows ICMP, it will significantly impact Linux traceroute and Windows tracert differently:

- Linux traceroute by default sends UDP probe packets to high-numbered ports. The firewall blocking UDP probes means Linux traceroute probes do not reach the destination or intermediate routers, resulting in many hops showing no response (***) as was seen in the above outputs.
- Windows tracert uses ICMP Echo Request probes by default, which the firewall allows. Therefore, Windows tracert will generally complete the trace successfully because ICMP messages pass through, and routers or the destination can reply.

Thus, in this scenario, Windows tracert will function correctly, while Linux traceroute's output will be limited or show timeouts due to the UDP blockage.