


Task-1: DNS resolver

custom_header	domain_name	resolved_ip
9330000	_apple-mobdev._tcp.local.	192.168.1.1
9330001	_apple-mobdev._tcp.local.	192.168.1.2
9330002	linkedin.com.	192.168.1.3
9330003	wikipedia.org.	192.168.1.4
9330004	wpad.	192.168.1.5
9330005	wpad.	192.168.1.1
9330006	wpad.	192.168.1.2
9330007	wpad.	192.168.1.3
9330008	wpad.	192.168.1.4
9330009	wpad.	192.168.1.5
9330010	wpad.	192.168.1.1
9330011	wpad.	192.168.1.2
9330012	gmwnlajnl.	192.168.1.3
9330013	djoncbjcmv.	192.168.1.4
9330014	mptmkwart.	192.168.1.5
9330015	djoncbjcmv.	192.168.1.1
9330016	gmwnlajnl.	192.168.1.2
9330017	mptmkwart.	192.168.1.3
9330018	Brother MFC-7860DW._pdl-dat astream._tcp.local.	192.168.1.4
9330019	Brother MFC-7860DW._pdl-dat astream._tcp.local.	192.168.1.5
9330020	example.com.	192.168.1.1

9330021	wpad.	192.168.1.2
9330022	wpad.	192.168.1.3
9330023	wpad.	192.168.1.4

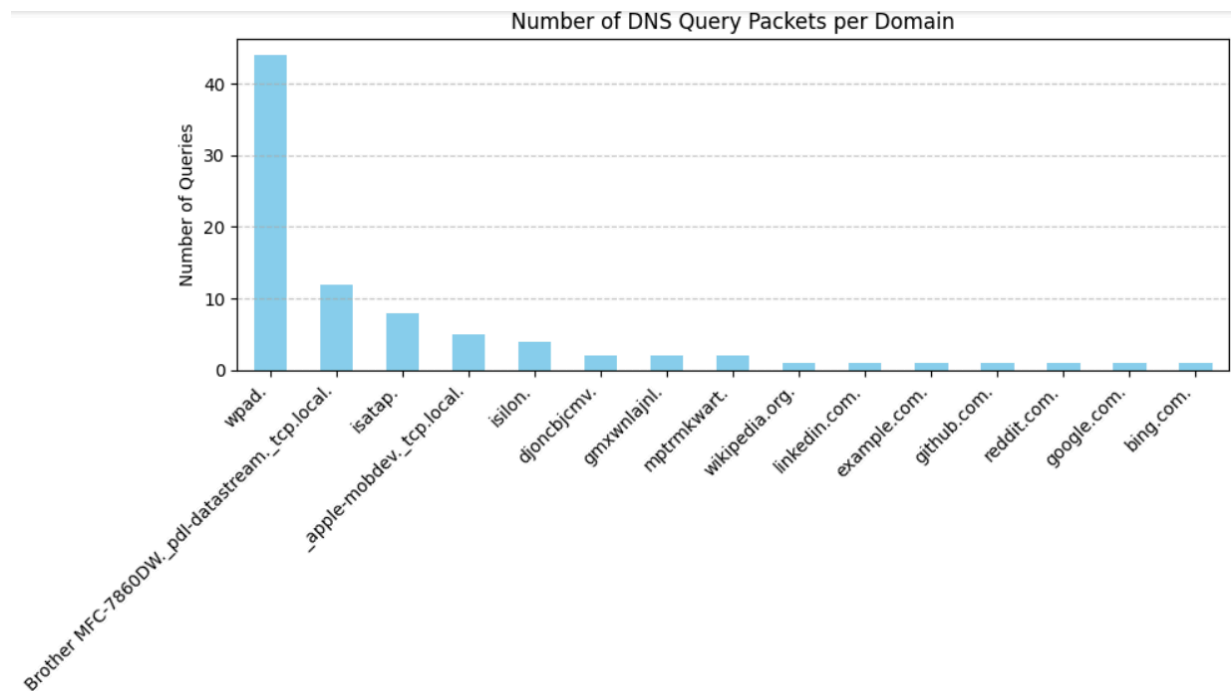
Most frequent domains



A screenshot of a terminal window with a dark background. At the top left is a window icon. The title bar reads "domain_name". The terminal displays a list of domain names and their corresponding frequencies, sorted in descending order. The domains are: wpad. (44), Brother MFC-7860DW._pdl-datastream._tcp.local. (12), isatap. (8), _apple-mobdev._tcp.local. (5), isilon. (4), djoncbjcmv. (2), gmxwnlajnl. (2), mptrmkwart. (2), wikipedia.org. (1), linkedin.com. (1), example.com. (1), github.com. (1), reddit.com. (1), google.com. (1), and bing.com. (1).

domain_name	frequency
wpad.	44
Brother MFC-7860DW._pdl-datastream._tcp.local.	12
isatap.	8
_apple-mobdev._tcp.local.	5
isilon.	4
djoncbjcmv.	2
gmxwnlajnl.	2
mptrmkwart.	2
wikipedia.org.	1
linkedin.com.	1
example.com.	1
github.com.	1
reddit.com.	1
google.com.	1
bing.com.	1

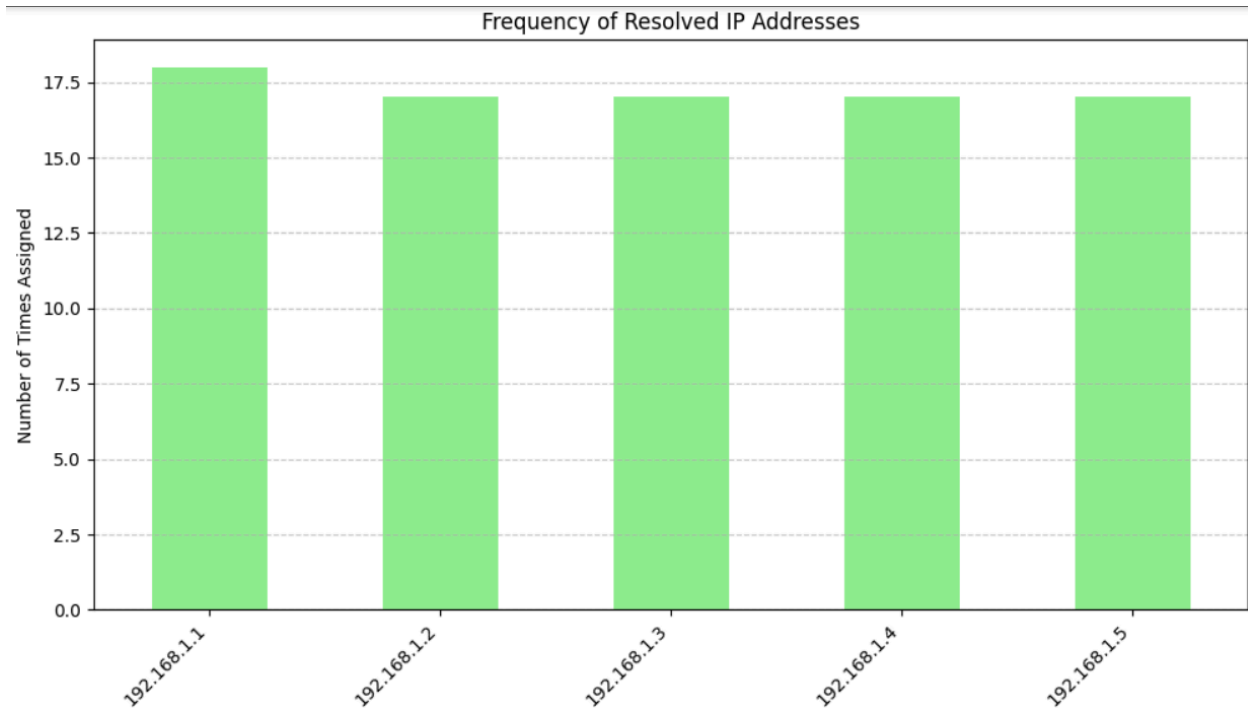
Graphical distribution of domains frequency



Resolved IPs count

count	
resolved_ip	
192.168.1.1	18
192.168.1.2	17
192.168.1.3	17
192.168.1.4	17
192.168.1.5	17

Graphical representation of Resolved IPs



Task-2: Traceroute Protocol Behavior

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

```
Tracing route to www.google.com [142.251.220.4]  
over a maximum of 30 hops:
```

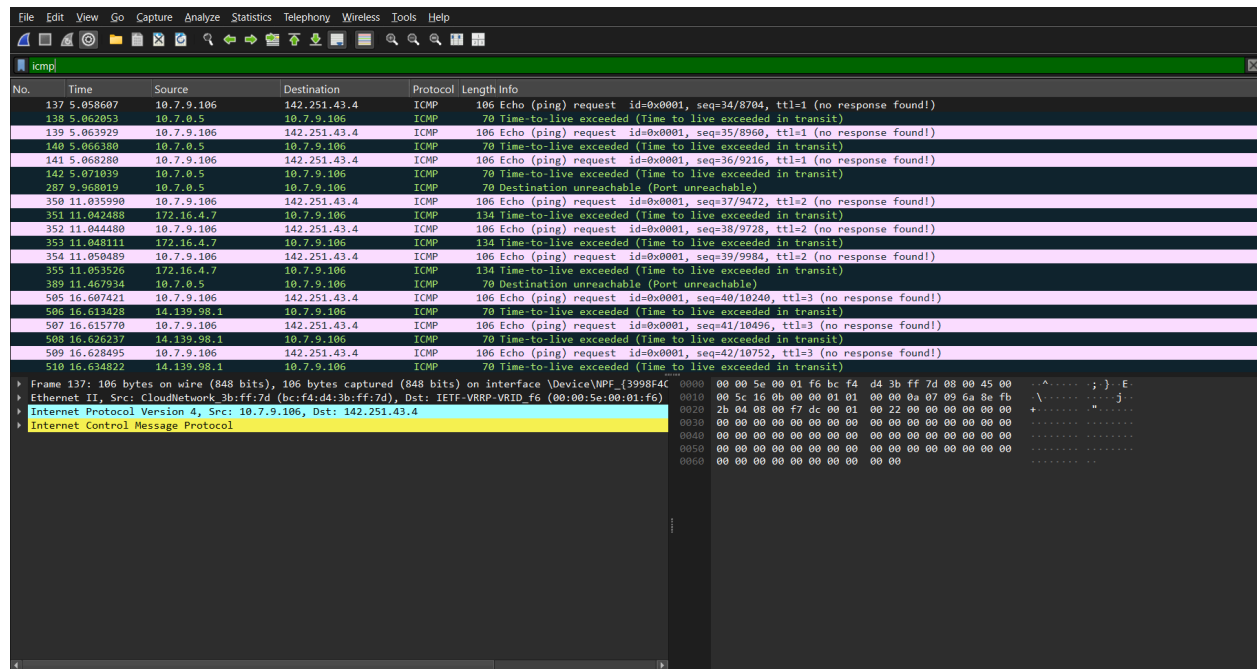
Hop	Source	Destination	Time
1	5 ms	4 ms	3 ms 10.7.0.5
2	3 ms	3 ms	2 ms 172.16.4.7
3	6 ms	5 ms	5 ms 14.139.98.1
4	4 ms	3 ms	3 ms 10.117.81.253
5	80 ms	28 ms	22 ms 10.154.8.137
6	24 ms	14 ms	11 ms 10.255.239.170
7	15 ms	11 ms	11 ms 10.152.7.214
8	14 ms	14 ms	13 ms 142.250.172.80
9	18 ms	24 ms	17 ms 142.251.76.31
10	28 ms	15 ms	15 ms 142.251.64.13
11	15 ms	13 ms	13 ms pnbomb-ay-in-f4.1e100.net [142.251.220.4]

```
Trace complete.
```

```
ayush@honormagicbook:/mnt/c/WINDOWS/system32$ traceroute www.google.com  
traceroute to www.google.com (142.250.71.100), 30 hops max, 60 byte packets  
1 Honormagicbook.mshome.net (172.20.0.1) 0.679 ms 0.913 ms 0.897 ms  
2 10.7.0.5 (10.7.0.5) 4.810 ms 4.770 ms 4.755 ms  
3 172.16.4.7 (172.16.4.7) 2.993 ms 2.979 ms 2.930 ms  
4 14.139.98.1 (14.139.98.1) 5.609 ms 5.464 ms 5.400 ms  
5 10.117.81.253 (10.117.81.253) 4.354 ms 4.334 ms 4.318 ms  
6 10.154.8.137 (10.154.8.137) 12.461 ms 11.886 ms 11.854 ms  
7 10.255.239.170 (10.255.239.170) 11.912 ms 11.864 ms 12.961 ms  
8 10.152.7.214 (10.152.7.214) 11.772 ms 11.161 ms 10.903 ms  
9 72.14.204.62 (72.14.204.62) 12.042 ms * 11.916 ms  
10 * * *  
11 142.251.77.98 (142.251.77.98) 13.163 ms 216.239.50.166 (216.239.50.166) 16.803 ms 142.251.69.44 (142.251.69.44) 14.099 ms  
12 192.178.110.104 (192.178.110.104) 12.780 ms 12.764 ms 192.178.86.247 (192.178.86.247) 13.876 ms  
13 pnbomb-ad-in-f4.1e100.net (142.250.71.100) 14.782 ms 14.764 ms 142.250.209.71 (142.250.209.71) 13.828 ms
```

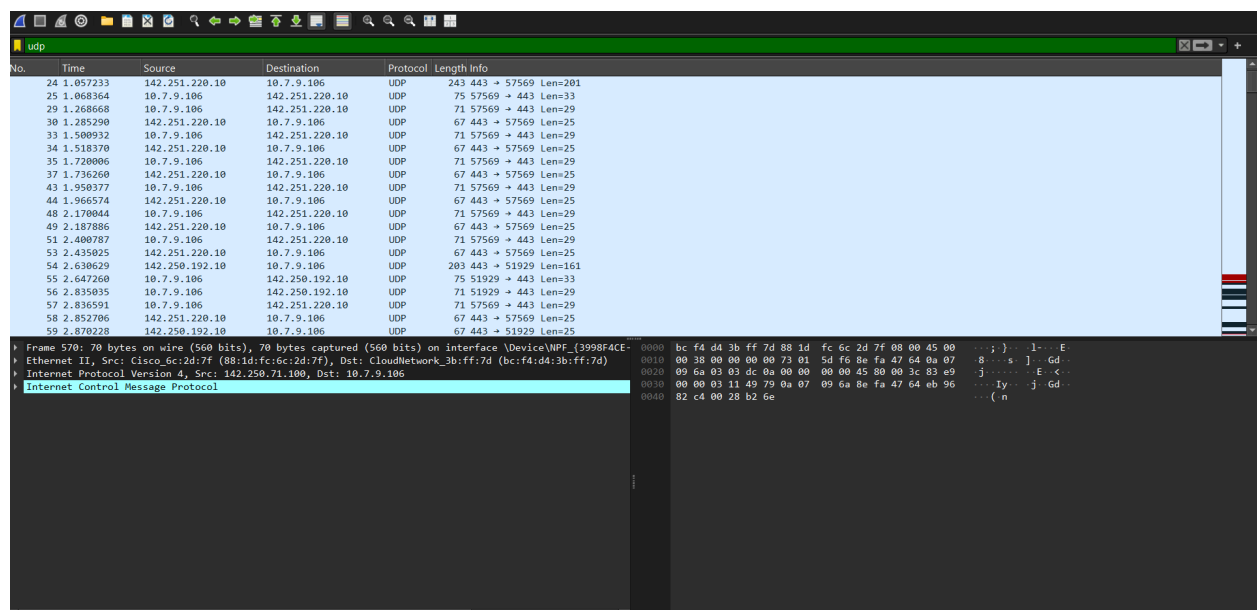
Q1. What protocol does Windows tracert use by default, and what protocol does Linux traceroute use by default ?

→ Windows tracert



No.	Time	Source	Destination	Protocol	Length	Info
137	5.058607	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=1 (no response found!)
138	5.062053	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
139	5.063929	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=1 (no response found!)
140	5.065308	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
141	5.068202	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=1 (no response found!)
142	5.071839	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
287	9.368019	10.7.0.5	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
350	11.035990	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=2 (no response found!)
351	11.042488	172.16.4.7	10.7.9.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
352	11.044480	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=2 (no response found!)
353	11.048111	172.16.4.7	10.7.9.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
354	11.050409	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=2 (no response found!)
355	11.053526	172.16.4.7	10.7.9.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
389	11.467934	10.7.0.5	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
505	16.607421	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=3 (no response found!)
506	16.613428	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
507	16.615770	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=3 (no response found!)
508	16.626237	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
509	16.628455	10.7.9.106	142.251.43.4	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=3 (no response found!)
510	16.631022	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Linux traceroute



No.	Time	Source	Destination	Protocol	Length	Info
24	1.057233	142.251.220.10	10.7.9.106	UDP	243	443 → 57569 Len=201
25	1.068364	10.7.9.106	142.251.220.10	UDP	75	57569 → 443 Len=33
29	1.268668	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
30	1.285290	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
33	1.500932	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
34	1.518370	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
35	1.728006	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
37	1.736260	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
43	1.950377	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
44	1.966574	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
48	2.170844	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
49	2.187806	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
51	2.400787	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
53	2.435025	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
54	2.630629	142.250.192.10	10.7.9.106	UDP	203	443 → 51929 Len=161
55	2.647260	10.7.9.106	142.250.192.10	UDP	75	51929 → 443 Len=33
56	2.835035	10.7.9.106	142.250.192.10	UDP	71	51929 → 443 Len=29
57	2.836591	10.7.9.106	142.251.220.10	UDP	71	57569 → 443 Len=29
58	2.852706	142.251.220.10	10.7.9.106	UDP	67	443 → 57569 Len=25
59	2.870228	142.250.192.10	10.7.9.106	UDP	67	443 → 51929 Len=25

Windows tracert uses ICMP Echo Request by default. When we put the filter icmp in wireshark we can see

- Packets labeled as Echo (ping) request
- ICMP Time Exceeded (TTL expired)
- Final Echo Reply

Linux traceroute uses UDP by default. When we put the filter as udp

- UDP packets sent from client.
- ICMP Time Exceeded.
- ICMP Destination Unreachable (Port Unreachable).

Q2. Some hops in your traceroute output may show . Provide at least two reasons why a router might not reply.

→ Some hops show *** because:

1. Firewall blocking ICMP or TTL Expired packets:
2. Rate-limiting prevents replying to every probe and drops some probs.

This is evident in Wireshark where no ICMP Time Exceeded is received for certain TTLs.

Q3. In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?

→ The UDP source port number changes in each probe packet.

Q4. At the final hop, how is the response different compared to the intermediate hop?

→ Intermediate hop sends ICMP Time Exceeded.

Final hop (destination reached) sends ICMP Destination Unreachable (Destination Unreachable Port Unreachable,).

No.	Time	Source	Destination	Protocol	Length	Info
501	33.257714	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
502	33.257714	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
504	33.257714	10.7.0.5	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
507	33.258914	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
508	33.258914	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
509	33.258914	14.139.98.1	10.7.9.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
566	33.407623	142.250.209.71	10.7.9.106	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
557	33.387530	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
558	33.387530	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
567	33.408618	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
568	33.408618	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
569	33.408618	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
570	33.409652	142.250.71.100	10.7.9.106	ICMP	70	Destination unreachable (Port unreachable)
555	33.386383	142.251.69.44	10.7.9.106	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
552	33.385111	142.251.77.98	10.7.9.106	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
492	33.256225	172.16.4.7	10.7.9.106	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
493	33.256225	172.16.4.7	10.7.9.106	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
494	33.256225	172.16.4.7	10.7.9.106	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
553	33.385111	192.178.110.104	10.7.9.106	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
554	33.385111	192.178.110.104	10.7.9.106	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Frame 492: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{3998F4C...}	0000	bc f4 d4 3b ff 7d 88 1d	fc 6c 2d 7f 08 00 45 c0	...	;	1	...	E
Ethernet II, Src: Cisco6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: CloudNetwork_3b:ff:7d (bc:f4:d4:3b:ff:7d)	0010	00 58 1f 4d 00 00 fe 01	d9 0f ac 10 04 07 0a 07	X	M
Internet Protocol Version 4, Src: 172.16.4.7, Dst: 10.7.9.106	0020	09 6a 0b 00 df 08 00 00	00 00 45 00 00 3c 84 54	j
Internet Control Message Protocol	0030	00 00 01 11 4b 8e 0a 07	09 6a 8e fa 47 64 eb 83	...	K	...	j	Gd
	0040	82 a0 00 28 b2 a5 40 41	42 43 44 45 46 47 48 49	...	@	A	BCDEFGHI	
	0050	4a 4b 4c 4d 4e 4f 50 51	52 53 54 55 56 57 58 59	J	K	L	M	N
	0060	5a 5b 5c 5d 5e 5f		Z	[\]	^

Q5. Suppose a firewall blocks UDP traffic but allows ICMP — how would this affect the results of Linux traceroute vs. Windows tracert?

→ **Windows tracert (ICMP-based)** Works normally:

ICMP Echo Requests and Replies continue without issue, it means everything is visible.

Linux traceroute (UDP-based) Will fail to get responses:

No ICMP Time Exceeded or Destination Unreachable packets returned. Shows only UDP packets going out, it means no ICMP replies received.