CS 331: COMPUTER NETWORKS ASSIGNMENT 1

Team Members:
Kushal Mehta - 23110205
Vedant Sharan - 23110354

Date:
15th September, 2025

GitHub Link:
https://github.com/KushalMehta17/CS-331_Computer_Networks_Assign-1

Task-1: DNS Resolver

The file structure, file description and instructions for usage are all elaborated in the **README.md** file of the submitted GitHub Repository. Please go through the same. For the results and explanation, please refer below.

Final Table Output (printed in the terminal after running) for the file **9.pcap** :

Afternoon Routing:

Custom Header	Domain	Resolved IP
17251100	www.twitter.com.	192.168.1.6
17251101	www.example.com.	192.168.1.7
17251102	www.netflix.com.	192.168.1.8
17251103	www.linkedin.com.	192.168.1.9
17251104	www.reddit.com.	192.168.1.10
17251105	www.openai.com.	192.168.1.6

Explanation:

The header

- `17251100` is parsed as hour = 17, which falls in the **afternoon (12:00–19:59)** slot with `ip_pool_start = 5`. The session ID is `00`, so `00 % 5 = 0`. Adding this to the pool start index gives `5 + 0 = 5`, which corresponds to the IP at index 5, i.e., **192.168.1.6**
- Similarly, we parsed all other DNS Queries.

Night Routing:

Custom Header	Domain	Resolved IP
22513700	www.twitter.com.	192.168.1.11
22513701	www.example.com.	192.168.1.12
22513702	www.netflix.com.	192.168.1.13
22513703	www.linkedin.com.	192.168.1.14
22513704	www.reddit.com.	192.168.1.15
22513705	www.openai.com.	192.168.1.11

Explanation:

The header

- `22513700` is parsed as hour = 22, which falls in the **night** slot with `ip_pool_start = 10`. The session ID is `00`, so `00 % 5 = 0`. Adding this to the pool start index gives `10 + 0 = 10`, which corresponds to the IP at index 10, i.e., **192.168.1.11**
- Similarly, we parsed all other DNS Queries.

Task-2: Traceroute Protocol Behaviour

For this we used www.youtube.com.

Below are the windows tracert and linux traceroute screenshots.

```
(base) PS C:\Users\vedan> tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.251.220.14]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  10.7.0.5
  2     3 ms     3 ms     2 ms  172.16.4.7
  3     4 ms     4 ms     4 ms  14.139.98.1
  4     2 ms     1 ms     2 ms  10.117.81.253
  5    12 ms    11 ms    11 ms  10.154.8.137
  6    12 ms    10 ms    13 ms  10.255.239.170
  7    12 ms    11 ms    11 ms  10.152.7.214
  8    12 ms    11 ms    12 ms  72.14.204.62
  9    28 ms    20 ms    20 ms  142.251.76.33
 10    34 ms    12 ms    26 ms  142.251.64.13
 11    13 ms    13 ms    14 ms  pnbomb-ay-in-f14.1e100.net [142.251.220.14]
```

```
(base) vedant@LENOVO:~$ traceroute www.youtube.com
traceroute to www.youtube.com (142.250.183.46), 30 hops max, 60 byte packets
 1  LENOVO.mshome.net (172.28.32.1)  0.899 ms  0.868 ms  0.854 ms
 2  10.7.0.5 (10.7.0.5)  16.342 ms  16.328 ms  16.315 ms
 3  172.16.4.7 (172.16.4.7)  15.671 ms  15.659 ms  15.642 ms
 4  14.139.98.1 (14.139.98.1)  18.107 ms  18.096 ms  18.085 ms
 5  10.117.81.253 (10.117.81.253)  16.220 ms  16.208 ms  16.196 ms
 6  10.154.8.137 (10.154.8.137)  25.795 ms  24.365 ms  24.342 ms
 7  10.255.239.170 (10.255.239.170)  24.324 ms  22.145 ms  22.118 ms
 8  10.152.7.214 (10.152.7.214)  22.398 ms  26.526 ms  26.492 ms
 9  * 72.14.204.62 (72.14.204.62)  26.407 ms  26.394 ms
10  * * *
11  142.250.235.8 (142.250.235.8)  19.038 ms 142.250.214.98 (142.250.214.98)  27.922 ms 216.239.58.18 (216.239.58.18)  14.051 ms
12  142.250.239.171 (142.250.239.171)  28.700 ms 192.178.110.248 (192.178.110.248)  18.322 ms 142.250.209.70 (142.250.209.70)  14.050 ms
13  192.178.110.199 (192.178.110.199)  15.421 ms 192.178.110.207 (192.178.110.207)  15.335 ms bom12s11-in-f14.1e100.net (142.250.183.46)  15.779 ms
```

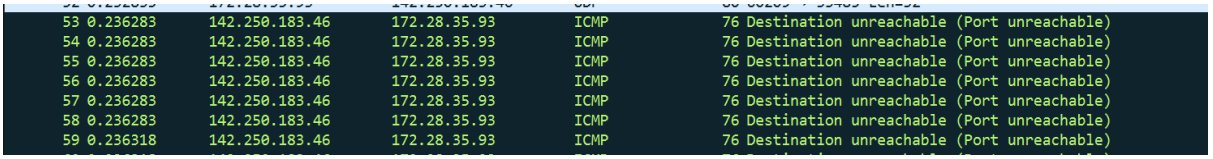
Q1.What protocol does Windows tracert use by default, and what protocol does Linux traceroute use by default?

Windows tracert uses ICMP Echo Request probes by default. Each probe is an ICMP Echo Request; intermediate routers reply with ICMP Time Exceeded, and the destination replies with ICMP Echo Reply.

No.	Time	Source	Destination	Protocol	Length	Info
10	4.375528	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=1/256, ttl=1 (no response found!)
11	4.377785	10.7.0.5	10.7.14.227	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	4.378967	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=2/512, ttl=1 (no response found!)
13	4.381410	10.7.0.5	10.7.14.227	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	4.382367	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=3/768, ttl=1 (no response found!)
15	4.384079	10.7.0.5	10.7.14.227	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
36	10.388863	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=4/1024, ttl=2 (no response found!)
37	10.391563	172.16.4.7	10.7.14.227	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
38	10.393117	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=5/1280, ttl=2 (no response found!)
1407	55.167155	142.251.64.13	10.7.14.227	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1420	60.762617	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=11 (reply in 1421)
1422	60.777908	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=11 (reply in 1423)
1424	60.793568	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=11 (reply in 1425)

Linux traceroute uses UDP probes by default. It sends UDP datagrams to high-numbered destination ports and the final destination typically replies with ICMP Destination Unreachable — Port Unreachable.

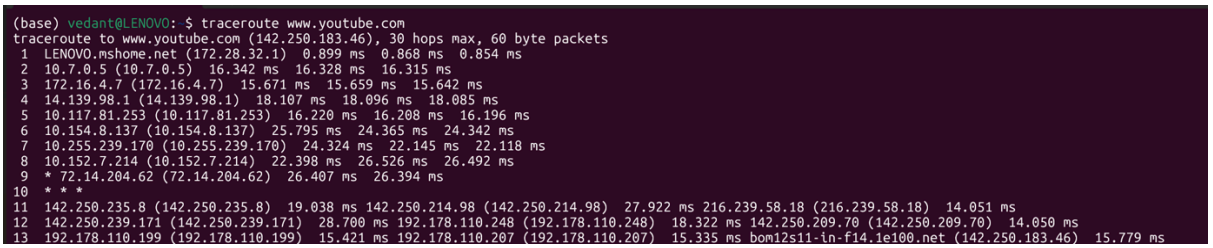
No.	Time	Source	Destination	Protocol	Length	Info
13	0.000169	172.28.35.93	142.250.183.46	UDP	80	45146 → 33446 Len=32
14	0.000181	172.28.35.93	142.250.183.46	UDP	80	55159 → 33447 Len=32
15	0.000195	172.28.35.93	142.250.183.46	UDP	80	57783 → 33448 Len=32
16	0.000207	172.28.35.93	142.250.183.46	UDP	80	45777 → 33449 Len=32
17	0.006266	172.28.35.93	142.250.183.46	UDP	80	40283 → 33450 Len=32
18	0.006281	172.28.35.93	142.250.183.46	UDP	80	59358 → 33451 Len=32
19	0.006290	172.28.35.93	142.250.183.46	UDP	80	58230 → 33452 Len=32



53	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
54	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
55	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
56	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
57	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
58	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
59	0.236318	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)

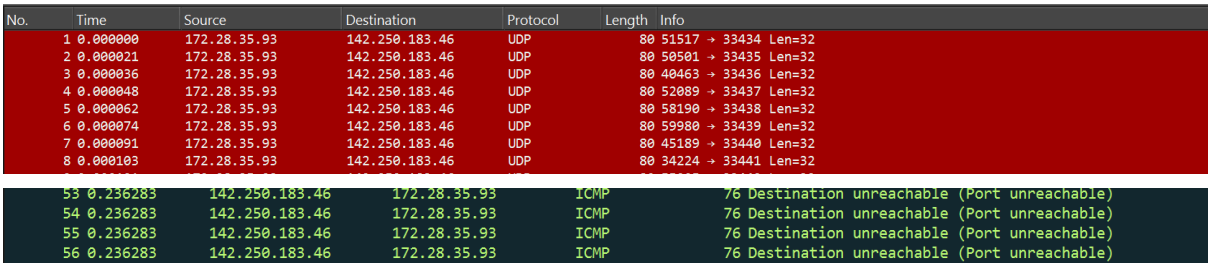
Q2.Some hops show *. Provide at least two reasons why a router might not reply.**
ICMP/Ttl-exceeded messages are filtered or disabled — many routers or firewall policies drop or block ICMP Time Exceeded messages for security reasons. If the router forwards the packet but does not generate ICMP TTL-exceeded replies, traceroute shows * * *.

Rate limiting of ICMP on routers — routers often limit the rate at which they send ICMP replies; when the limit is hit, some probes get no reply and appear as *.



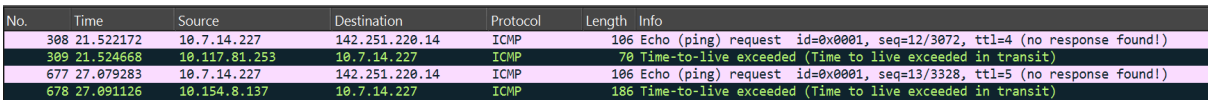
```
(base) vedant@LENOVO: $ traceroute www.youtube.com
traceroute to www.youtube.com (142.250.183.46), 30 hops max, 60 byte packets
 1  LENOVO.mshome.net (172.28.32.1)  0.899 ms  0.868 ms  0.854 ms
 2  10.7.0.5 (10.7.0.5)  16.342 ms  16.328 ms  16.315 ms
 3  172.16.4.7 (172.16.4.7)  15.671 ms  15.659 ms  15.642 ms
 4  14.139.98.1 (14.139.98.1)  18.107 ms  18.096 ms  18.085 ms
 5  10.117.81.253 (10.117.81.253)  16.220 ms  16.208 ms  16.196 ms
 6  10.154.8.137 (10.154.8.137)  25.795 ms  24.365 ms  24.342 ms
 7  10.255.239.170 (10.255.239.170)  24.324 ms  22.145 ms  22.118 ms
 8  10.152.7.214 (10.152.7.214)  22.398 ms  26.526 ms  26.492 ms
 9  * 72.14.204.62 (72.14.204.62)  26.407 ms  26.394 ms
10  * * *
11  142.250.235.8 (142.250.235.8)  19.038 ms 142.250.214.98 (142.250.214.98)  27.922 ms 216.239.58.18 (216.239.58.18)  14.051 ms
12  142.250.239.171 (142.250.239.171)  28.700 ms 192.178.110.248 (192.178.110.248)  18.322 ms 142.250.209.70 (142.250.209.70)  14.050 ms
13  192.178.110.199 (192.178.110.199)  15.421 ms 192.178.110.207 (192.178.110.207)  15.335 ms bom12s11-in-f14.1e100.net (142.250.183.46)  15.779 ms
```

Q3.In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?
UDP destination port. The default Linux traceroute sends UDP datagrams to consecutive high-numbered destination ports (typically starting at 33434 and incrementing). This incrementing destination port is how traceroute distinguishes multiple probes and matches ICMP replies back to the original probe. The same can be seen in the figure below:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.35.93	142.250.183.46	UDP	80	51517 → 33434 Len=32
2	0.000021	172.28.35.93	142.250.183.46	UDP	80	50501 → 33435 Len=32
3	0.000036	172.28.35.93	142.250.183.46	UDP	80	40463 → 33436 Len=32
4	0.000048	172.28.35.93	142.250.183.46	UDP	80	52089 → 33437 Len=32
5	0.000062	172.28.35.93	142.250.183.46	UDP	80	58190 → 33438 Len=32
6	0.000074	172.28.35.93	142.250.183.46	UDP	80	59980 → 33439 Len=32
7	0.000091	172.28.35.93	142.250.183.46	UDP	80	45189 → 33440 Len=32
8	0.000103	172.28.35.93	142.250.183.46	UDP	80	34224 → 33441 Len=32
53	0.236283	142.250.183.46	172.28.35.93	ICMP	76	Destination unreachable (Port unreachable)
54	0.236283	142.250.183.46	172.28.35.93	ICMP	76	Destination unreachable (Port unreachable)
55	0.236283	142.250.183.46	172.28.35.93	ICMP	76	Destination unreachable (Port unreachable)
56	0.236283	142.250.183.46	172.28.35.93	ICMP	76	Destination unreachable (Port unreachable)

Q4.At the final hop, how is the response different compared to the intermediate hop?
Intermediate hop: Routers to which the packet's TTL becomes zero reply with ICMP Time Exceeded. These identify the intermediate router and allow traceroute to list that hop.



No.	Time	Source	Destination	Protocol	Length	Info
308	21.522172	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=4 (no response found!)
309	21.524668	10.117.81.253	10.7.14.227	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
677	27.079283	10.7.14.227	142.251.220.14	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=5 (no response found!)
678	27.091126	10.154.8.137	10.7.14.227	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)

Final hop (Linux UDP default): When the UDP probe finally reaches the destination, there is typically no process listening on the high UDP port used. The destination therefore replies with ICMP Destination Unreachable — Port Unreachable. This indicates you reached the target.

53	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)
54	0.236283	142.250.183.46	172.28.35.93	ICMP	76 Destination unreachable (Port unreachable)

Windows tracert final hop: If using ICMP Echo requests, the final hop replies with ICMP Echo Reply rather than Destination Unreachable.

1420	60.762617	10.7.14.227	142.251.220.14	ICMP	106 Echo (ping) request id=0x0001, seq=31/7936, ttl=11 (reply in 1421)
1422	60.777908	10.7.14.227	142.251.220.14	ICMP	106 Echo (ping) request id=0x0001, seq=32/8192, ttl=11 (reply in 1423)
1424	60.793568	10.7.14.227	142.251.220.14	ICMP	106 Echo (ping) request id=0x0001, seq=33/8448, ttl=11 (reply in 1425)

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

Linux traceroute (default UDP): If a firewall on the path (or on the destination) blocks UDP, the UDP probes will be dropped or blocked and will not elicit ICMP Time Exceeded or Port Unreachable replies. As a result, traceroute will show * * * (timeouts) for those hops and likely fail to reach the destination.

Windows tracert (ICMP): Since it uses ICMP Echo probes, if the firewall allows ICMP then tracert will succeed and show the path. The firewall permitting ICMP means intermediate routers and final host can reply with ICMP Time Exceeded / Echo Replies, so tracert output will be normal.