ASSIGNMENT - 1

Computer Networks

Team

Rahul Singal (23110265)

Akshat Saurin Shah (23110293)

Task 1 : DNS Resolver

Github repo: https://github.com/SRahul02/DNS-Resolver
Pcap file used: 8.pcap

DNS Query Filtering (client.py)

This file reads the pcap file, filters and gets us DNS packets. It parses them and adds a custom header to them based on the rules given. It then sends these desired packets, which we are supposed to resolve to server.py.

IP Address allotment (server.py)

This file receives the DNS packets, it then allots an IP address to the packet based on the pre set rules. It then sends back the IP allotted to each packet as a response to the client's request.

---

* We have used the "socket" library in python for creating the connection between the client and the server, which uses a server IP and a server port for creating the connection.

* We have used the "scapy" library to read the pcap file and detect the packets which are DNS packets.

* We have used the "datetime" library to access the time on the local machine on which our code is running, as that is required for creating the custom header.

* In our analysis, we found that there was no packet when the pkt[DNS].qr was set == 1, but rather 23 packets were found when pkt[DNS].qr was set ==0.

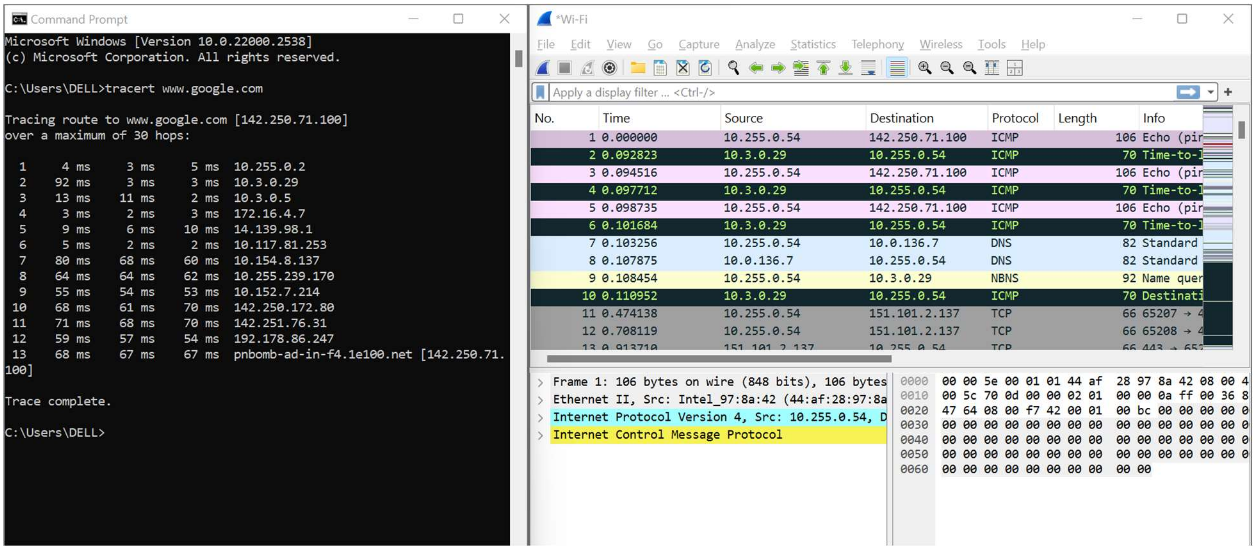
Domain Name	Custom Header	Resolved IP
_apple-mobdev._tcp.local.	22485036	192.168.1.12
_apple-mobdev._tcp.local.	22485037	192.168.1.13
github.com.	22490169	192.168.1.15
Brother MFC-7860DW._pdl-datastream._tcp.local.	22490974	192.168.1.15
Brother MFC-7860DW._pdl-datastream._tcp.local.	22490929	192.168.1.15
bing.com.	22491260	192.168.1.11
facebook.com.	22492780	192.168.1.11
Brother MFC-7860DW._pdl-datastream._tcp.local.	22493671	192.168.1.12
Brother MFC-7860DW._pdl-datastream._tcp.local.	22493669	192.168.1.15
amazon.com.	22495161	192.168.1.12
_apple-mobdev._tcp.local.	22500396	192.168.1.12
Brother MFC-7860DW._pdl-datastream._tcp.local.	22500540	192.168.1.11
Brother MFC-7860DW._pdl-datastream._tcp.local.	22500543	192.168.1.14
linkedin.com.	22502088	192.168.1.14
Brother MFC-7860DW._pdl-datastream._tcp.local.	22503749	192.168.1.15
Brother MFC-7860DW._pdl-datastream._tcp.local.	22503822	192.168.1.13
_apple-mobdev._tcp.local.	22504340	192.168.1.11
_apple-mobdev._tcp.local.	22504341	192.168.1.12
stackoverflow.com.	22505862	192.168.1.13
Brother MFC-7860DW._pdl-datastream._tcp.local.	22510769	192.168.1.15
._pdl-datastream._tcp.local.	22510761	192.168.1.12
Brother MFC-7860DW._pdl-datastream._tcp.local.	22510925	192.168.1.11
Brother MFC-7860DW._pdl-datastream._tcp.local.	22510995	192.168.1.11

Task 2 :

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

Ans. By default, Windows tracert sends ICMP Echo Request packets, whereas Linux traceroute sends UDP probes.

Windows:



```
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>tracert www.google.com

Tracing route to www.google.com [142.250.71.100]
over a maximum of 30 hops:

  1     4 ms     3 ms     5 ms  10.255.0.2
  2    92 ms     3 ms     3 ms  10.3.0.29
  3    13 ms    11 ms     2 ms  10.3.0.5
  4     3 ms     2 ms     3 ms  172.16.4.7
  5     9 ms     6 ms    10 ms  14.139.98.1
  6     5 ms     2 ms     2 ms  10.117.81.253
  7    80 ms    68 ms    60 ms  10.154.8.137
  8    64 ms    64 ms    62 ms  10.255.239.170
  9    55 ms    54 ms    53 ms  10.152.7.214
 10    68 ms    61 ms    70 ms  142.250.172.80
 11    71 ms    68 ms    70 ms  142.251.76.31
 12    59 ms    57 ms    54 ms  192.178.86.247
 13    68 ms    67 ms    67 ms  pnbomb-ad-in-f4.1e100.net [142.250.71.
100]

Trace complete.

C:\Users\DELL>
```

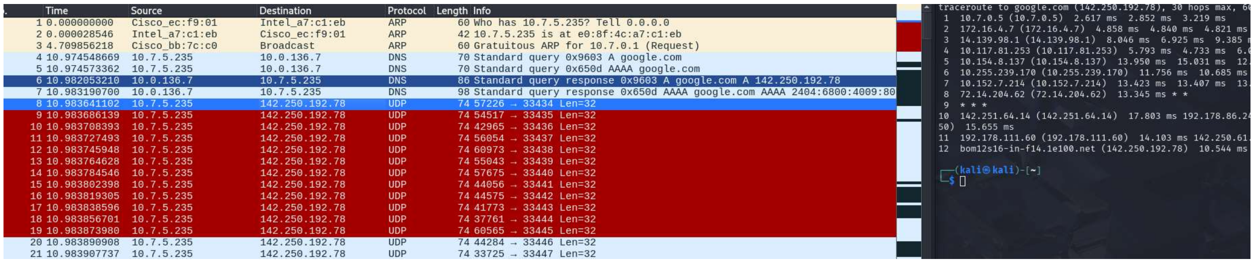
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination     Protocol  Length  Info
    1 0.000000  10.255.0.54     142.250.71.100  ICMP         106 Echo (pir
    2 0.092823  10.3.0.29       10.255.0.54     ICMP          70 Time-to-l
    3 0.094516  10.255.0.54     142.250.71.100  ICMP         106 Echo (pir
    4 0.097712  10.3.0.29       10.255.0.54     ICMP          70 Time-to-l
    5 0.098735  10.255.0.54     142.250.71.100  ICMP         106 Echo (pir
    6 0.101684  10.3.0.29       10.255.0.54     ICMP          70 Time-to-l
    7 0.103256  10.255.0.54     10.0.136.7      DNS           82 Standard
    8 0.107875  10.0.136.7      10.255.0.54     DNS           82 Standard
    9 0.108454  10.255.0.54     10.3.0.29       NBNS          92 Name quer
   10 0.110952  10.3.0.29       10.255.0.54     ICMP          70 Destinati
   11 0.474138  10.255.0.54     151.101.2.137   TCP           66 65207 → 4
   12 0.708119  10.255.0.54     151.101.2.137   TCP           66 65208 → 4
   13 0.913710  151.101.2.137   10.255.0.54     TCP           66 443 → 652
```

```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes
> Ethernet II, Src: Intel_97:8a:42 (44:af:28:97:8a
> Internet Protocol Version 4, Src: 10.255.0.54, D
> Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 01 44 af  28 97 8a 42 08 00 4
0010  00 5c 70 0d 00 00 02 01  00 00 0a ff 00 36 8
0020  47 64 08 00 f7 42 00 01  00 bc 00 00 00 00 0
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0060  00 00 00 00 00 00 00 00  00 00
```

Linux:



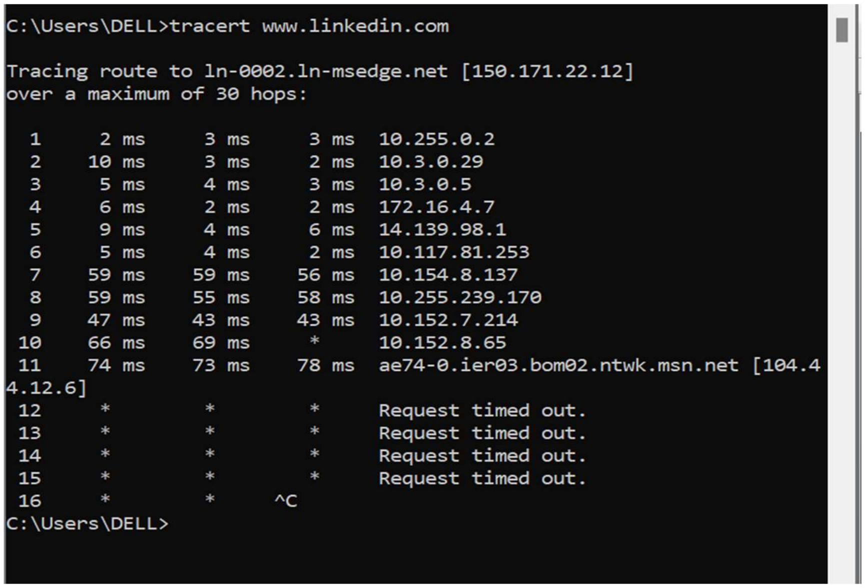
```
.    Time         Source             Destination       Protocol Length Info
   1 0.000000000  Cisco_ec:f9:01     Intel_a7:c1:eb    ARP          60 Who has 10.7.5.235? Tell 0.0.0.0
   2 0.000028546  Intel_a7:c1:eb     Cisco_ec:f9:01    ARP          42 10.7.5.235 is at e0:8f:4c:a7:c1:eb
   3 4.709856218  Cisco_bb:7c:c0     Broadcast         ARP          60 Gratuitous ARP for 10.7.0.1 (Request)
   4 10.974548669 10.7.5.235         10.0.136.7        DNS          70 Standard query 0x9603 A google.com
   5 10.974573362 10.7.5.235         10.0.136.7        DNS          70 Standard query 0x650d AAAA google.com
   6 10.982053210 10.0.136.7         10.7.5.235        DNS          86 Standard query response 0x9603 A google.com A 142.250.192.78
   7 10.983190700 10.0.136.7         10.7.5.235        DNS          98 Standard query response 0x650d AAAA google.com AAAA 2404:6800:4009:80
   8 10.983641102 10.7.5.235         142.250.192.78    UDP          74 57226 → 33434 Len=32
   9 10.983686139 10.7.5.235         142.250.192.78    UDP          74 54517 → 33435 Len=32
  10 10.983708393 10.7.5.235         142.250.192.78    UDP          74 42965 → 33436 Len=32
  11 10.983727493 10.7.5.235         142.250.192.78    UDP          74 56054 → 33437 Len=32
  12 10.983745948 10.7.5.235         142.250.192.78    UDP          74 60973 → 33438 Len=32
  13 10.983764628 10.7.5.235         142.250.192.78    UDP          74 55043 → 33439 Len=32
  14 10.983784546 10.7.5.235         142.250.192.78    UDP          74 57675 → 33440 Len=32
  15 10.983802398 10.7.5.235         142.250.192.78    UDP          74 44056 → 33441 Len=32
  16 10.983819305 10.7.5.235         142.250.192.78    UDP          74 44575 → 33442 Len=32
  17 10.983838596 10.7.5.235         142.250.192.78    UDP          74 41773 → 33443 Len=32
  18 10.983856701 10.7.5.235         142.250.192.78    UDP          74 37761 → 33444 Len=32
  19 10.983873980 10.7.5.235         142.250.192.78    UDP          74 60565 → 33445 Len=32
  20 10.983890908 10.7.5.235         142.250.192.78    UDP          74 44284 → 33446 Len=32
  21 10.983907737 10.7.5.235         142.250.192.78    UDP          74 33725 → 33447 Len=32
```

```
traceroute to google.com (142.250.192.78), 30 hops max, 60
 1  10.7.0.5 (10.7.0.5)  2.617 ms  2.852 ms  3.219 ms
 2  172.16.4.7 (172.16.4.7)  4.858 ms  4.840 ms  4.821 ms
 3  14.139.98.1 (14.139.98.1)  8.046 ms  6.925 ms  9.385 m
 4  10.117.81.253 (10.117.81.253)  5.793 ms  4.733 ms  6.0
 5  10.154.8.137 (10.154.8.137)  13.950 ms  15.031 ms  12.
 6  10.255.239.170 (10.255.239.170)  11.756 ms  10.685 ms
 7  10.152.7.214 (10.152.7.214)  13.423 ms  13.407 ms  13.
 8  72.14.204.62 (72.14.204.62)  13.345 ms * *
 9  * * *
10  142.251.64.14 (142.251.64.14)  17.803 ms 192.178.86.24
50)  15.655 ms
11  192.178.111.60 (192.178.111.60)  14.103 ms 142.250.61.
12  bom12s16-in-f14.1e100.net (142.250.192.78)  10.544 ms

┌──(kali㉿kali)-[~]
└─$ ▯
```

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

Ans. i) If the router is heavily loaded, it might drop the packets instead of responding.

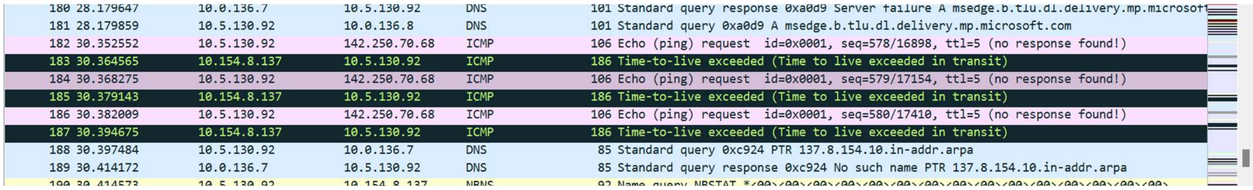
ii) The packet while reaching to its destination, maybe blocked and dropped by being encountered by a firewall at some stage and hence we did not receive the response corresponding to it.



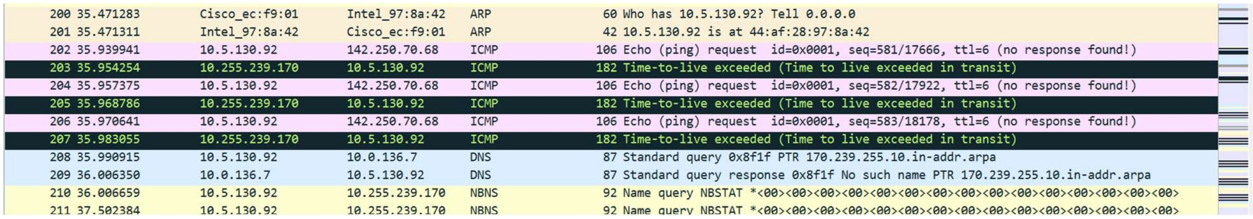
```
C:\Users\DELL>tracert www.linkedin.com

Tracing route to ln-0002.ln-msedge.net [150.171.22.12]
over a maximum of 30 hops:

  1     2 ms     3 ms     3 ms  10.255.0.2
  2    10 ms     3 ms     2 ms  10.3.0.29
  3     5 ms     4 ms     3 ms  10.3.0.5
  4     6 ms     2 ms     2 ms  172.16.4.7
  5     9 ms     4 ms     6 ms  14.139.98.1
  6     5 ms     4 ms     2 ms  10.117.81.253
  7    59 ms    59 ms    56 ms  10.154.8.137
  8    59 ms    55 ms    58 ms  10.255.239.170
  9    47 ms    43 ms    43 ms  10.152.7.214
 10    66 ms    69 ms     *     10.152.8.65
 11    74 ms    73 ms    78 ms  ae74-0.ier03.bom02.ntwk.msn.net [104.4
4.12.6]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *     ^C
C:\Users\DELL>
```

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

Ans. TTL (Time to Live) field.



```
180 28.179647    10.0.136.7       10.5.130.92      DNS     101 Standard query response 0xa0d9 Server failure A msedge.b.tlu.dl.delivery.mp.microsoft
181 28.179859    10.5.130.92      10.0.136.8       DNS     101 Standard query 0xa0d9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
182 30.352552    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=578/16898, ttl=5 (no response found!)
183 30.364565    10.154.8.137     10.5.130.92      ICMP    186 Time-to-live exceeded (Time to live exceeded in transit)
184 30.368275    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=579/17154, ttl=5 (no response found!)
185 30.379143    10.154.8.137     10.5.130.92      ICMP    186 Time-to-live exceeded (Time to live exceeded in transit)
186 30.382009    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=580/17410, ttl=5 (no response found!)
187 30.394675    10.154.8.137     10.5.130.92      ICMP    186 Time-to-live exceeded (Time to live exceeded in transit)
188 30.397484    10.5.130.92      10.0.136.7       DNS      85 Standard query 0xc924 PTR 137.8.154.10.in-addr.arpa
189 30.414172    10.0.136.7       10.5.130.92      DNS      85 Standard query response 0xc924 No such name PTR 137.8.154.10.in-addr.arpa
190 30.414573    10.5.130.92      10.154.8.137     NBNS     92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
```



```
200 35.471283    Cisco_ec:f9:01   Intel_97:8a:42   ARP      60 Who has 10.5.130.92? Tell 0.0.0.0
201 35.471311    Intel_97:8a:42   Cisco_ec:f9:01   ARP      42 10.5.130.92 is at 44:af:28:97:8a:42
202 35.939941    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=581/17666, ttl=6 (no response found!)
203 35.954254    10.255.239.170   10.5.130.92      ICMP    182 Time-to-live exceeded (Time to live exceeded in transit)
204 35.957375    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=582/17922, ttl=6 (no response found!)
205 35.968786    10.255.239.170   10.5.130.92      ICMP    182 Time-to-live exceeded (Time to live exceeded in transit)
206 35.970641    10.5.130.92      142.250.70.68    ICMP    106 Echo (ping) request  id=0x0001, seq=583/18178, ttl=6 (no response found!)
207 35.983055    10.255.239.170   10.5.130.92      ICMP    182 Time-to-live exceeded (Time to live exceeded in transit)
208 35.990915    10.5.130.92      10.0.136.7       DNS      87 Standard query 0x8f1f PTR 170.239.255.10.in-addr.arpa
209 36.006350    10.0.136.7       10.5.130.92      DNS      87 Standard query response 0x8f1f No such name PTR 170.239.255.10.in-addr.arpa
210 36.006659    10.5.130.92      10.255.239.170   NBNS     92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
211 37.502384    10.5.130.92      10.255.239.170   NBNS     92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
```

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

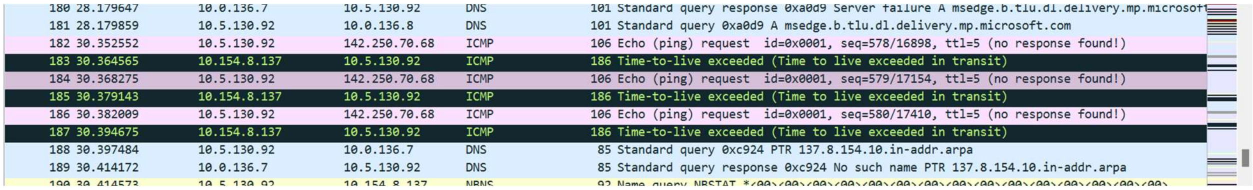
Ans.

When you run traceroute, the routers in the middle send back **"Time Exceeded"** messages because the **TTL runs out**.

When the packets finally reach the **destination**, it replies with either a **"Port Unreachable"** message (if it's the Linux UDP type) or an **"Echo Reply"** (if it's the Windows ICMP type).

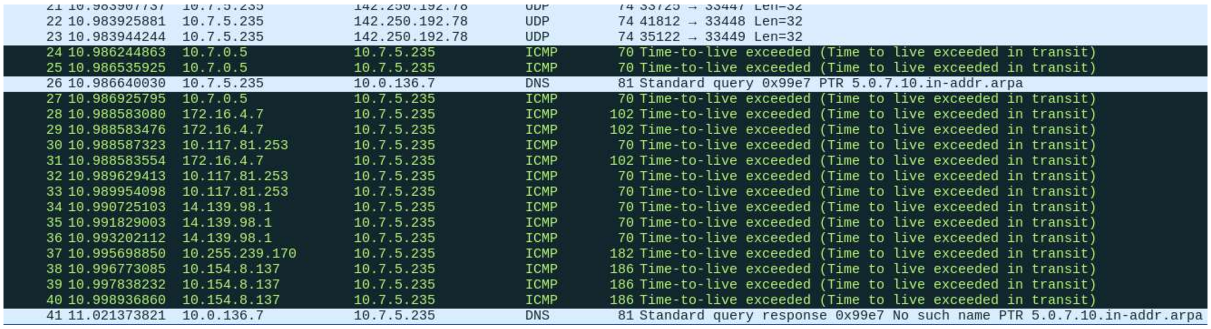
Intermediate:

Windows



```
180 28.179647   10.0.136.7     10.5.130.92    DNS    101 Standard query response 0xa0d9 Server failure A msedge.b.tlu.dl.delivery.mp.microsoft
181 28.179859   10.5.130.92    10.0.136.8     DNS    101 Standard query 0xa0d9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
182 30.352552   10.5.130.92    142.250.70.68  ICMP   106 Echo (ping) request  id=0x0001, seq=578/16898, ttl=5 (no response found!)
183 30.364565   10.154.8.137   10.5.130.92    ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
184 30.368275   10.5.130.92    142.250.70.68  ICMP   106 Echo (ping) request  id=0x0001, seq=579/17154, ttl=5 (no response found!)
185 30.379143   10.154.8.137   10.5.130.92    ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
186 30.382009   10.5.130.92    142.250.70.68  ICMP   106 Echo (ping) request  id=0x0001, seq=580/17410, ttl=5 (no response found!)
187 30.394675   10.154.8.137   10.5.130.92    ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
188 30.397484   10.5.130.92    10.0.136.7     DNS     85 Standard query 0xc924 PTR 137.8.154.10.in-addr.arpa
189 30.414172   10.0.136.7     10.5.130.92    DNS     85 Standard query response 0xc924 No such name PTR 137.8.154.10.in-addr.arpa
190 30.414573   10.5.130.92    10.154.8.137   NBNS    92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
```

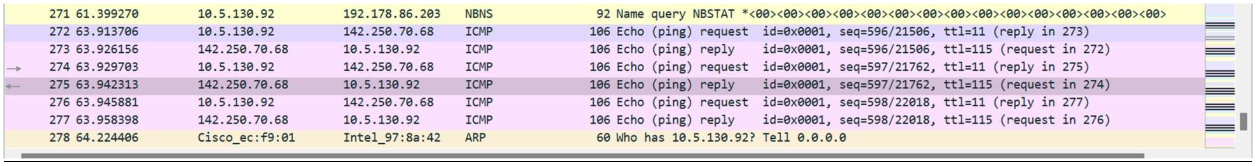
Linux



```
21 10.983907737  10.7.5.235      142.250.192.78  UDP     74 33725 → 33447 Len=32
22 10.983925881  10.7.5.235      142.250.192.78  UDP     74 41812 → 33448 Len=32
23 10.983944244  10.7.5.235      142.250.192.78  UDP     74 35122 → 33449 Len=32
24 10.986244863  10.7.0.5        10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
25 10.986535925  10.7.0.5        10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
26 10.986640030  10.7.5.235      10.0.136.7      DNS     81 Standard query 0x99e7 PTR 5.0.7.10.in-addr.arpa
27 10.986925795  10.7.0.5        10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
28 10.988583080  172.16.4.7      10.7.5.235      ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
29 10.988583476  172.16.4.7      10.7.5.235      ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
30 10.988587323  10.117.81.253   10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
31 10.988583554  172.16.4.7      10.7.5.235      ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
32 10.989629413  10.117.81.253   10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
33 10.989954098  10.117.81.253   10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
34 10.990725103  14.139.98.1     10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
35 10.991829003  14.139.98.1     10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
36 10.993202112  14.139.98.1     10.7.5.235      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
37 10.995698850  10.255.239.170  10.7.5.235      ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
38 10.996773085  10.154.8.137    10.7.5.235      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
39 10.997838232  10.154.8.137    10.7.5.235      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
40 10.998936860  10.154.8.137    10.7.5.235      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
41 11.021373821  10.0.136.7      10.7.5.235      DNS     81 Standard query response 0x99e7 No such name PTR 5.0.7.10.in-addr.arpa
```

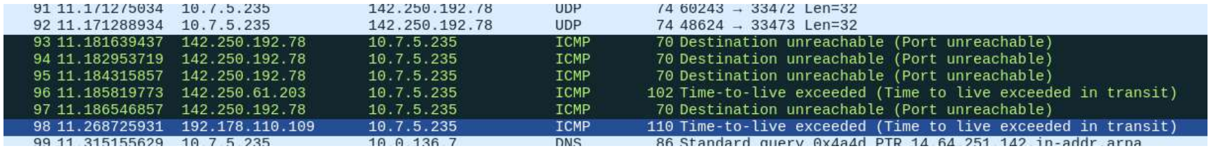
Final:

Windows



```
   271 61.399270   10.5.130.92      192.178.86.203  NBNS    92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
   272 63.913706   10.5.130.92      142.250.70.68   ICMP   106 Echo (ping) request  id=0x0001, seq=596/21506, ttl=11 (reply in 273)
   273 63.926156   142.250.70.68    10.5.130.92     ICMP   106 Echo (ping) reply    id=0x0001, seq=596/21506, ttl=115 (request in 272)
→  274 63.929703   10.5.130.92      142.250.70.68   ICMP   106 Echo (ping) request  id=0x0001, seq=597/21762, ttl=11 (reply in 275)
←  275 63.942313   142.250.70.68    10.5.130.92     ICMP   106 Echo (ping) reply    id=0x0001, seq=597/21762, ttl=115 (request in 274)
   276 63.945881   10.5.130.92      142.250.70.68   ICMP   106 Echo (ping) request  id=0x0001, seq=598/22018, ttl=11 (reply in 277)
   277 63.958398   142.250.70.68    10.5.130.92     ICMP   106 Echo (ping) reply    id=0x0001, seq=598/22018, ttl=115 (request in 276)
   278 64.224406   Cisco_ec:f9:01   Intel_97:8a:42  ARP     60 Who has 10.5.130.92? Tell 0.0.0.0
```

Linux

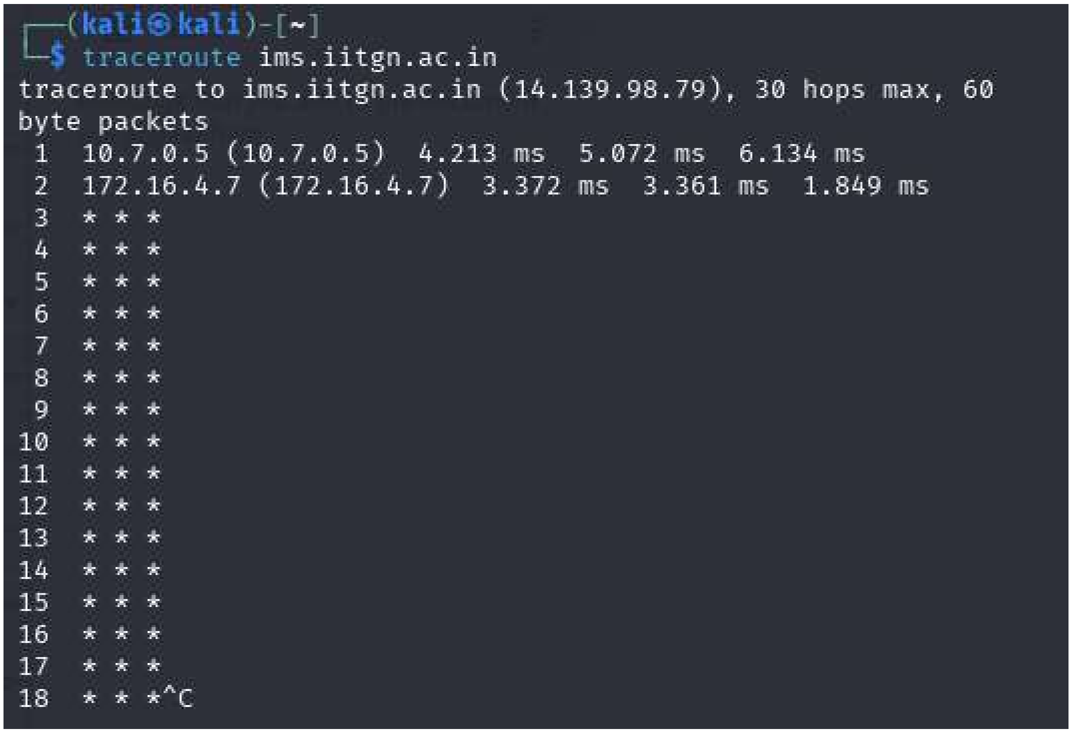


```
91 11.171275034  10.7.5.235       142.250.192.78  UDP     74 60243 → 33472 Len=32
92 11.171288934  10.7.5.235       142.250.192.78  UDP     74 48624 → 33473 Len=32
93 11.181639437  142.250.192.78   10.7.5.235      ICMP    70 Destination unreachable (Port unreachable)
94 11.182953719  142.250.192.78   10.7.5.235      ICMP    70 Destination unreachable (Port unreachable)
95 11.184315857  142.250.192.78   10.7.5.235      ICMP    70 Destination unreachable (Port unreachable)
96 11.185819773  142.250.61.203   10.7.5.235      ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
97 11.186546857  142.250.192.78   10.7.5.235      ICMP    70 Destination unreachable (Port unreachable)
98 11.268725931  192.178.110.109  10.7.5.235      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
99 11.315155629  10.7.5.235       10.0.136.7      DNS     86 Standard query 0x4a4d PTR 14.64.251.142.in-addr.arpa
```

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

Ans. If there's a firewall in the path, the **Linux traceroute (which uses UDP by default)** might stop working and just show * * * after that point, because its **UDP probes don't get any replies**.

But **Windows tracert (which uses ICMP)** would still work, since it **sends ICMP Echo Requests and gets ICMP replies back**.



```
┌──(kali㉿kali)-[~]
└─$ traceroute ims.iitgn.ac.in
traceroute to ims.iitgn.ac.in (14.139.98.79), 30 hops max, 60
byte packets
 1  10.7.0.5 (10.7.0.5)  4.213 ms  5.072 ms  6.134 ms
 2  172.16.4.7 (172.16.4.7)  3.372 ms  3.361 ms  1.849 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *^C
```