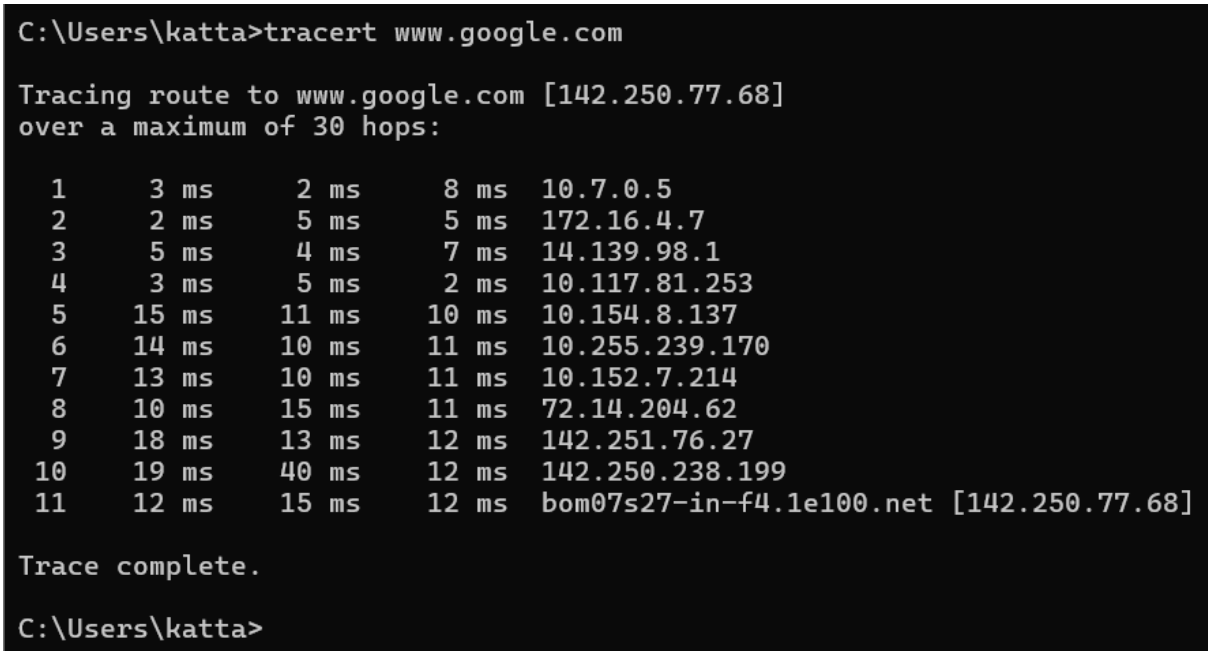
Task-2: Traceroute Protocol Behavior

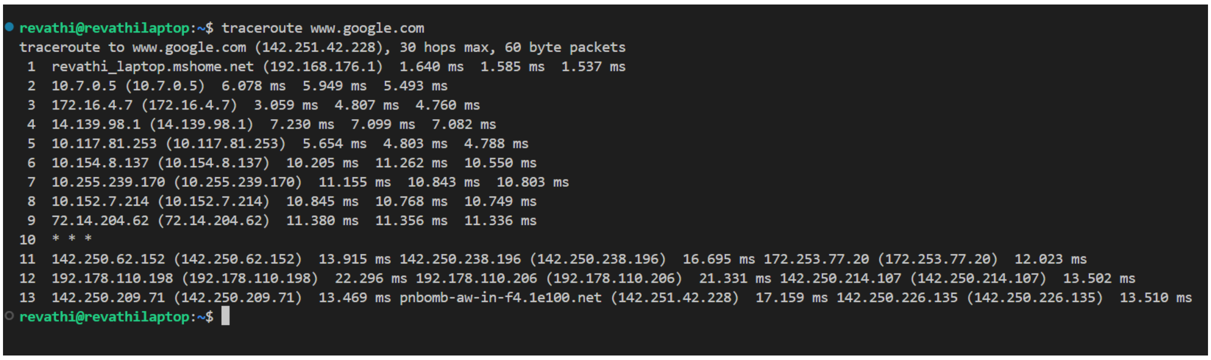
1. Run the following commands to trace the route to a given destination (e.g., www.google.com):

a. On Windows: tracert www.google.com



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

Tracing route to www.google.com [142.250.77.68]
over a maximum of 30 hops:

  1     3 ms     2 ms     8 ms  10.7.0.5
  2     2 ms     5 ms     5 ms  172.16.4.7
  3     5 ms     4 ms     7 ms  14.139.98.1
  4     3 ms     5 ms     2 ms  10.117.81.253
  5    15 ms    11 ms    10 ms  10.154.8.137
  6    14 ms    10 ms    11 ms  10.255.239.170
  7    13 ms    10 ms    11 ms  10.152.7.214
  8    10 ms    15 ms    11 ms  72.14.204.62
  9    18 ms    13 ms    12 ms  142.251.76.27
 10    19 ms    40 ms    12 ms  142.250.238.199
 11    12 ms    15 ms    12 ms  bom07s27-in-f4.1e100.net [142.250.77.68]

Trace complete.

C:\Users\katta>
```

b. On Linux: traceroute www.google.com



```
revathi@revathilaptop:~$ traceroute www.google.com
traceroute to www.google.com (142.251.42.228), 30 hops max, 60 byte packets
 1  revathi_laptop.mshome.net (192.168.176.1)  1.640 ms  1.585 ms  1.537 ms
 2  10.7.0.5 (10.7.0.5)  6.078 ms  5.949 ms  5.493 ms
 3  172.16.4.7 (172.16.4.7)  3.059 ms  4.807 ms  4.760 ms
 4  14.139.98.1 (14.139.98.1)  7.230 ms  7.099 ms  7.082 ms
 5  10.117.81.253 (10.117.81.253)  5.654 ms  4.803 ms  4.788 ms
 6  10.154.8.137 (10.154.8.137)  10.205 ms  11.262 ms  10.550 ms
 7  10.255.239.170 (10.255.239.170)  11.155 ms  10.843 ms  10.803 ms
 8  10.152.7.214 (10.152.7.214)  10.845 ms  10.768 ms  10.749 ms
 9  72.14.204.62 (72.14.204.62)  11.380 ms  11.356 ms  11.336 ms
10  * * *
11  142.250.62.152 (142.250.62.152)  13.915 ms 142.250.238.196 (142.250.238.196)  16.695 ms 172.253.77.20 (172.253.77.20)  12.023 ms
12  192.178.110.198 (192.178.110.198)  22.296 ms 192.178.110.206 (192.178.110.206)  21.331 ms 142.250.214.107 (142.250.214.107)  13.502 ms
13  142.250.209.71 (142.250.209.71)  13.469 ms pnbomb-aw-in-f4.1e100.net (142.251.42.228)  17.159 ms 142.250.226.135 (142.250.226.135)  13.510 ms
revathi@revathilaptop:~$
```

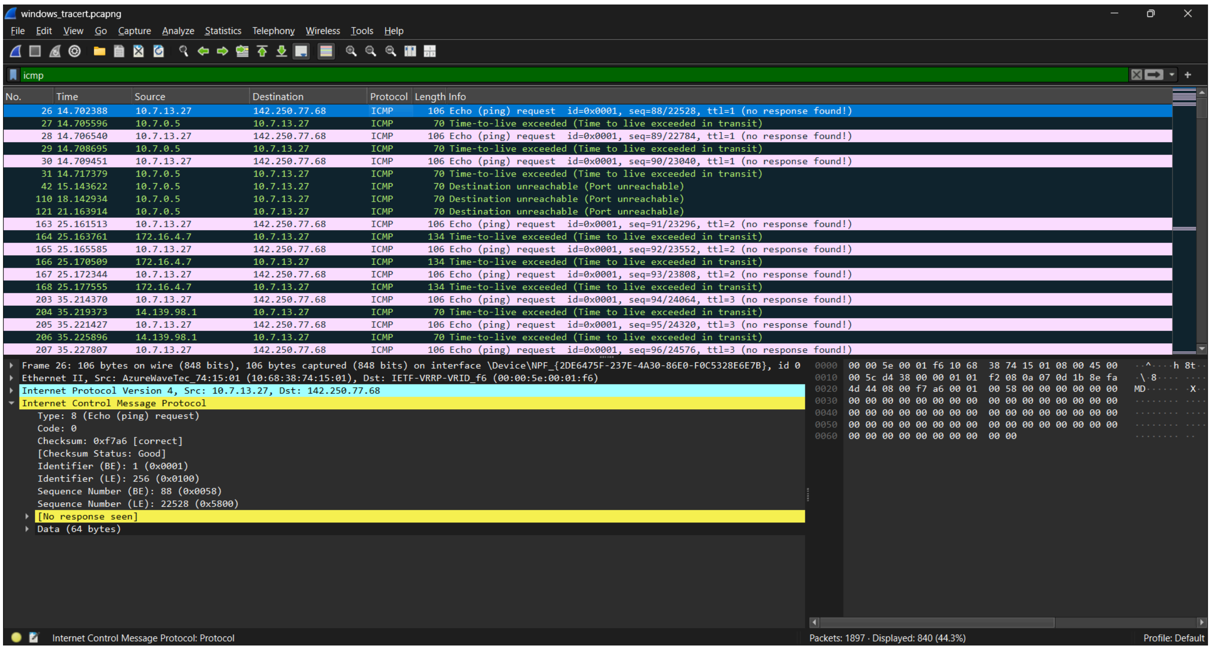
2. Capture the network traffic during both executions using Wireshark or tcpdump.

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

a. On Windows: tracert www.google.com

Windows tracert uses the **ICMP protocol** by default. It sends ICMP Echo Request packets (Type 8) toward the destination. Intermediate routers reply with ICMP Time Exceeded (Type 11) messages when TTL expires, and the final destination replies with an ICMP Echo Reply (Type 0). Applying the filter icmp in Wireshark shows outgoing ICMP Echo Request packets and incoming ICMP Time Exceeded / Echo Reply packets.

ICMP Echo Request packets (Type 8)



```
No.    Time       Source         Destination    Protocol Length Info
    26 14.702388  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=88/22528, ttl=1 (no response found!)
    27 14.705596  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    28 14.706540  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=89/22784, ttl=1 (no response found!)
    29 14.708695  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    30 14.709451  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=90/23040, ttl=1 (no response found!)
    31 14.717379  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    42 15.143622  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   110 18.142934  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   121 21.163914  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   163 25.161513  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=2 (no response found!)
   164 25.163761  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   165 25.165585  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=2 (no response found!)
   166 25.170509  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   167 25.172344  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=2 (no response found!)
   168 25.177555  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   203 35.214370  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=94/24064, ttl=3 (no response found!)
   204 35.219373  14.139.98.1    10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   205 35.221427  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=95/24320, ttl=3 (no response found!)
   206 35.225896  14.139.98.1    10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   207 35.227807  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=96/24576, ttl=3 (no response found!)
```

```
> Frame 26: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
> Ethernet II, Src: AzureWaveTec_74:15:01 (10:68:38:74:15:01), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
> Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.250.77.68
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7a6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 88 (0x0058)
    Sequence Number (LE): 22528 (0x5800)
  > [No response seen]
  > Data (64 bytes)
```

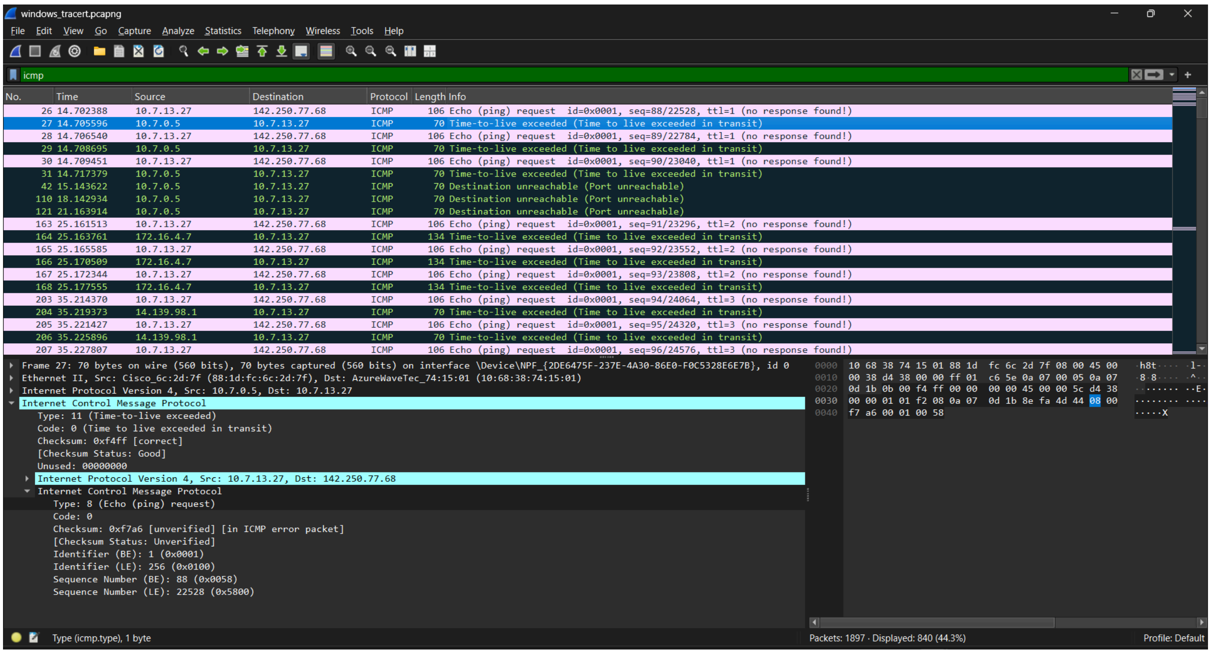
```
0000  00 00 5e 00 01 f6 10 68  38 74 15 01 08 00 45 00   ··^····h 8t····E·
0010  00 5c d4 38 00 00 01 01  f2 08 0a 07 0d 1b 8e fa   ·\·8···· ········
0020  4d 44 08 00 f7 a6 00 01  00 58 00 00 00 00 00 00   MD······ ·X······
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Internet Control Message Protocol: Protocol

Packets: 1897 · Displayed: 840 (44.3%)

Profile: Default

Intermediate routers reply with ICMP Time Exceeded (Type 11) messages when TTL expires



```
No.    Time       Source         Destination    Protocol Length Info
    26 14.702388  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=88/22528, ttl=1 (no response found!)
    27 14.705596  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    28 14.706540  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=89/22784, ttl=1 (no response found!)
    29 14.708695  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    30 14.709451  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=90/23040, ttl=1 (no response found!)
    31 14.717379  10.7.0.5       10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    42 15.143622  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   110 18.142934  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   121 21.163914  10.7.0.5       10.7.13.27     ICMP      70 Destination unreachable (Port unreachable)
   163 25.161513  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=2 (no response found!)
   164 25.163761  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   165 25.165585  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=2 (no response found!)
   166 25.170509  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   167 25.172344  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=2 (no response found!)
   168 25.177555  172.16.4.7     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   203 35.214370  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=94/24064, ttl=3 (no response found!)
   204 35.219373  14.139.98.1    10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   205 35.221427  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=95/24320, ttl=3 (no response found!)
   206 35.225896  14.139.98.1    10.7.13.27     ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   207 35.227807  10.7.13.27     142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=96/24576, ttl=3 (no response found!)
```

```
> Frame 27: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
> Ethernet II, Src: Cisco_6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: AzureWaveTec_74:15:01 (10:68:38:74:15:01)
> Internet Protocol Version 4, Src: 10.7.0.5, Dst: 10.7.13.27
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.250.77.68
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7a6 [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 88 (0x0058)
      Sequence Number (LE): 22528 (0x5800)
```

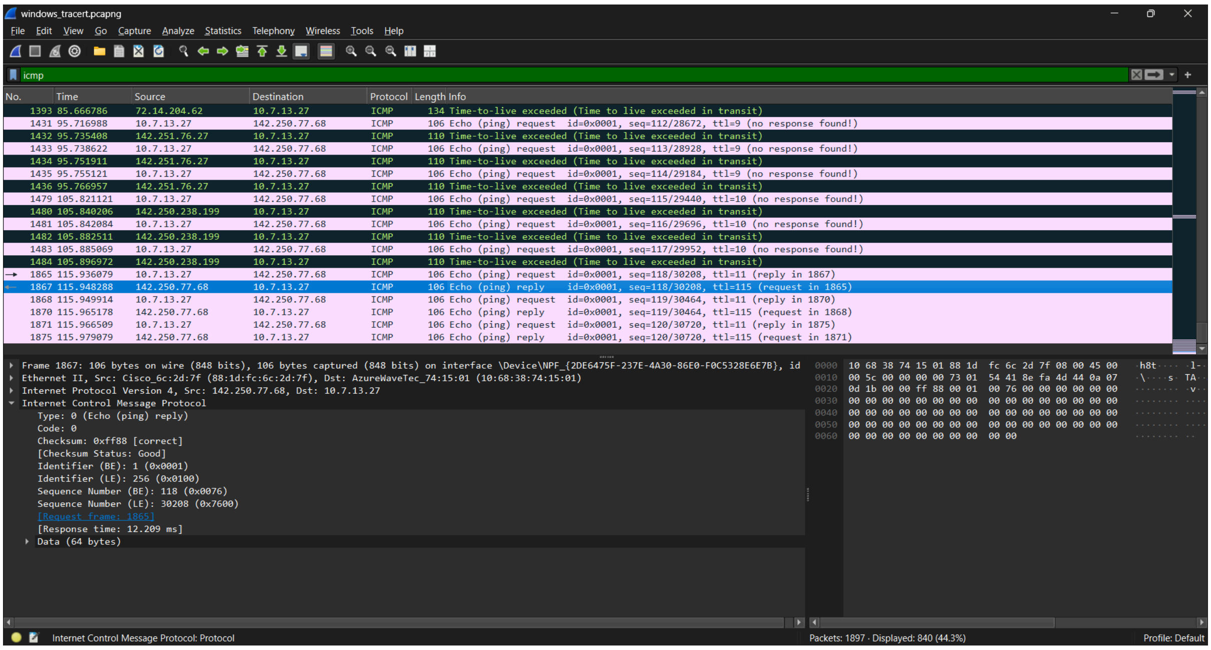
```
0000  10 68 38 74 15 01 88 1d  fc 6c 2d 7f 08 00 45 00   ·h8t···· ·l-···E·
0010  00 38 d4 38 00 00 ff 01  c6 5e 0a 07 00 05 0a 07   ·8·8···· ·^······
0020  0d 1b 0b 00 f4 ff 00 00  00 00 45 00 00 5c d4 38   ········ ··E··\·8
0030  00 00 01 01 f2 08 0a 07  0d 1b 8e fa 4d 44 08 00   ········ ····MD··
0040  f7 a6 00 01 00 58                                  ·····X
```

Type (icmp.type), 1 byte

Packets: 1897 · Displayed: 840 (44.3%)

Profile: Default

Final destination replies with an ICMP Echo Reply (Type 0)


windows_tracert.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
```

```
No.  Time        Source           Destination    Protocol Length Info
1393 85.666786   72.14.204.62     10.7.13.27     ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
1431 95.716988   10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=112/28672, ttl=9 (no response found!)
1432 95.735408   142.251.76.27    10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1433 95.738622   10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=113/28928, ttl=9 (no response found!)
1434 95.751911   142.251.76.27    10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1435 95.755121   10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=114/29184, ttl=9 (no response found!)
1436 95.766957   142.251.76.27    10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1479 105.821121  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=115/29440, ttl=10 (no response found!)
1480 105.840206  142.250.238.199  10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1481 105.842084  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=116/29696, ttl=10 (no response found!)
1482 105.882511  142.250.238.199  10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1483 105.885069  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=117/29952, ttl=10 (no response found!)
1484 105.896972  142.250.238.199  10.7.13.27     ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
1865 115.936079  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=118/30208, ttl=11 (reply in 1867)
1867 115.948288  142.250.77.68    10.7.13.27     ICMP     106 Echo (ping) reply    id=0x0001, seq=118/30208, ttl=115 (request in 1865)
1868 115.949914  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=119/30464, ttl=11 (reply in 1870)
1870 115.965178  142.250.77.68    10.7.13.27     ICMP     106 Echo (ping) reply    id=0x0001, seq=119/30464, ttl=115 (request in 1868)
1871 115.966509  10.7.13.27       142.250.77.68  ICMP     106 Echo (ping) request  id=0x0001, seq=120/30720, ttl=11 (reply in 1875)
1875 115.979079  142.250.77.68    10.7.13.27     ICMP     106 Echo (ping) reply    id=0x0001, seq=120/30720, ttl=115 (request in 1871)
```

```
Frame 1867: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id
Ethernet II, Src: Cisco_6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: AzureWaveTec_74:15:01 (10:68:38:74:15:01)
Internet Protocol Version 4, Src: 142.250.77.68, Dst: 10.7.13.27
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff88 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 118 (0x0076)
    Sequence Number (LE): 30208 (0x7600)
    [Request frame: 1865]
    [Response time: 12.209 ms]
    Data (64 bytes)
```

```
0000  10 68 38 74 15 01 88 1d  fc 6c 2d 7f 08 00 45 00   ·h8t····  ·l-···E·
0010  00 5c 00 00 00 00 73 01  54 41 8e fa 4d 44 0a 07   ·\····s·  TA··MD··
0020  0d 1b 00 00 ff 88 00 01  00 76 00 00 00 00 00 00   ········  ·v······
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0060  00 00 00 00 00 00 00 00  00 00                     ········  ··
```

Internet Control Message Protocol: Protocol

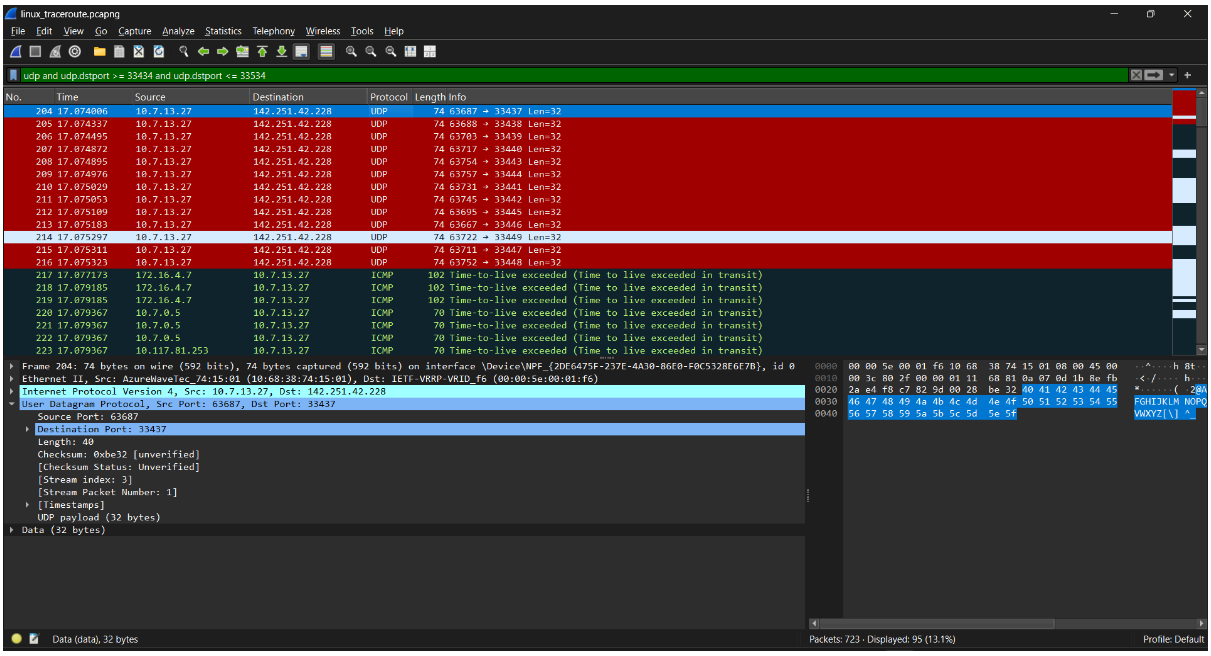
Packets: 1897 · Displayed: 840 (44.3%)

Profile: Default

b. On Linux: traceroute www.google.com

Linux traceroute uses the **UDP protocol** by default. It sends UDP datagrams to high-numbered destination ports (starting at 33434). Intermediate routers reply with ICMP Time Exceeded (Type 11) messages when TTL expires, and the final destination responds with ICMP Port Unreachable (Type 3, Code 3) since those ports are closed. In Wireshark, the filter “udp and udp. dstport >= 33434 and udp .dstport <= 33534” shows the UDP probes with destination ports 33434, 33435, etc.

UDP datagrams to high-numbered destination ports (starting at >33434)


linux_traceroute.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp and udp.dstport >= 33434 and udp.dstport <= 33534
```

```
No. Time        Source          Destination     Protocol Length Info
204 17.074006   10.7.13.27      142.251.42.228  UDP       74 63687 → 33437 Len=32
205 17.074337   10.7.13.27      142.251.42.228  UDP       74 63688 → 33438 Len=32
206 17.074495   10.7.13.27      142.251.42.228  UDP       74 63703 → 33439 Len=32
207 17.074872   10.7.13.27      142.251.42.228  UDP       74 63717 → 33440 Len=32
208 17.074895   10.7.13.27      142.251.42.228  UDP       74 63754 → 33443 Len=32
209 17.074976   10.7.13.27      142.251.42.228  UDP       74 63757 → 33444 Len=32
210 17.075029   10.7.13.27      142.251.42.228  UDP       74 63731 → 33441 Len=32
211 17.075053   10.7.13.27      142.251.42.228  UDP       74 63745 → 33442 Len=32
212 17.075109   10.7.13.27      142.251.42.228  UDP       74 63695 → 33445 Len=32
213 17.075183   10.7.13.27      142.251.42.228  UDP       74 63667 → 33446 Len=32
214 17.075297   10.7.13.27      142.251.42.228  UDP       74 63722 → 33449 Len=32
215 17.075311   10.7.13.27      142.251.42.228  UDP       74 63711 → 33447 Len=32
216 17.075323   10.7.13.27      142.251.42.228  UDP       74 63752 → 33448 Len=32
217 17.077173   172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
218 17.079185   172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
219 17.079185   172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
220 17.079367   10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
221 17.079367   10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
222 17.079367   10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
223 17.079367   10.117.81.253   10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
Frame 204: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
Ethernet II, Src: AzureWaveTec_74:15:01 (10:68:38:74:15:01), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.251.42.228
User Datagram Protocol, Src Port: 63687, Dst Port: 33437
    Source Port: 63687
    Destination Port: 33437
    Length: 40
    Checksum: 0xbe32 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (32 bytes)
Data (32 bytes)
```

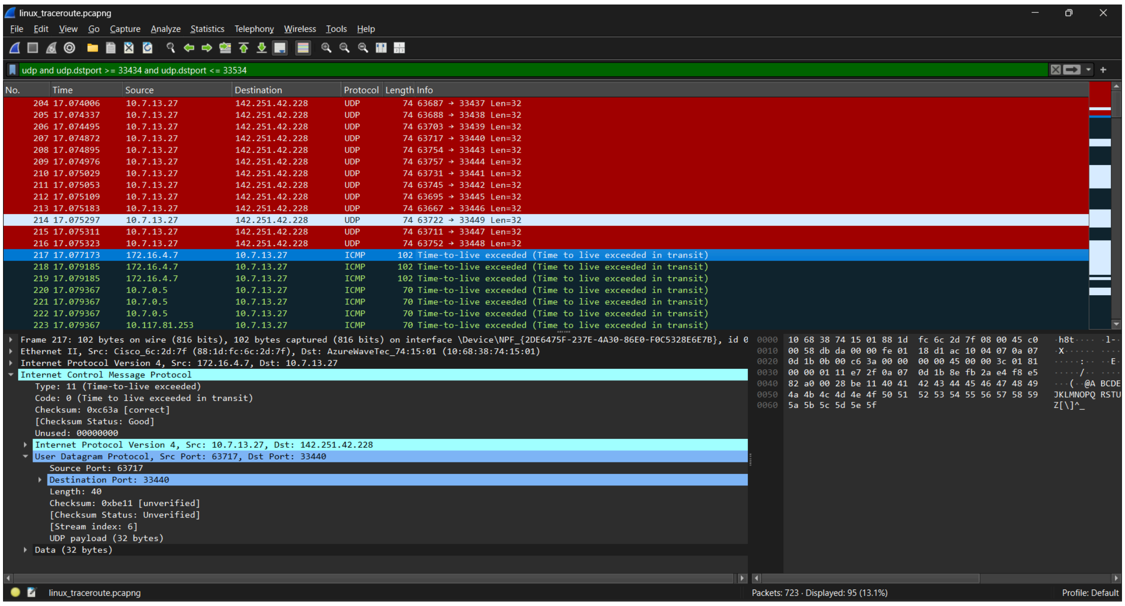
```
0000  00 00 5e 00 01 f6 10 68  38 74 15 01 08 00 45 00   ··^····h 8t····E·
0010  00 3c 80 2f 00 00 01 11  68 81 0a 07 0d 1b 8e fb   ·<·/···· h·······
0020  2a e4 f8 c7 82 9d 00 28  be 32 40 41 42 43 44 45   *······( ·2@ABCDE
0030  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM NOPQRSTU
0040  56 57 58 59 5a 5b 5c 5d  5e 5f                     VWXYZ[\] ^_
```

Data (data), 32 bytes

Packets: 723 · Displayed: 95 (13.1%)

Profile: Default

Intermediate routers reply with ICMP Time Exceeded (Type 11) messages when TTL expires


linux_traceroute.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

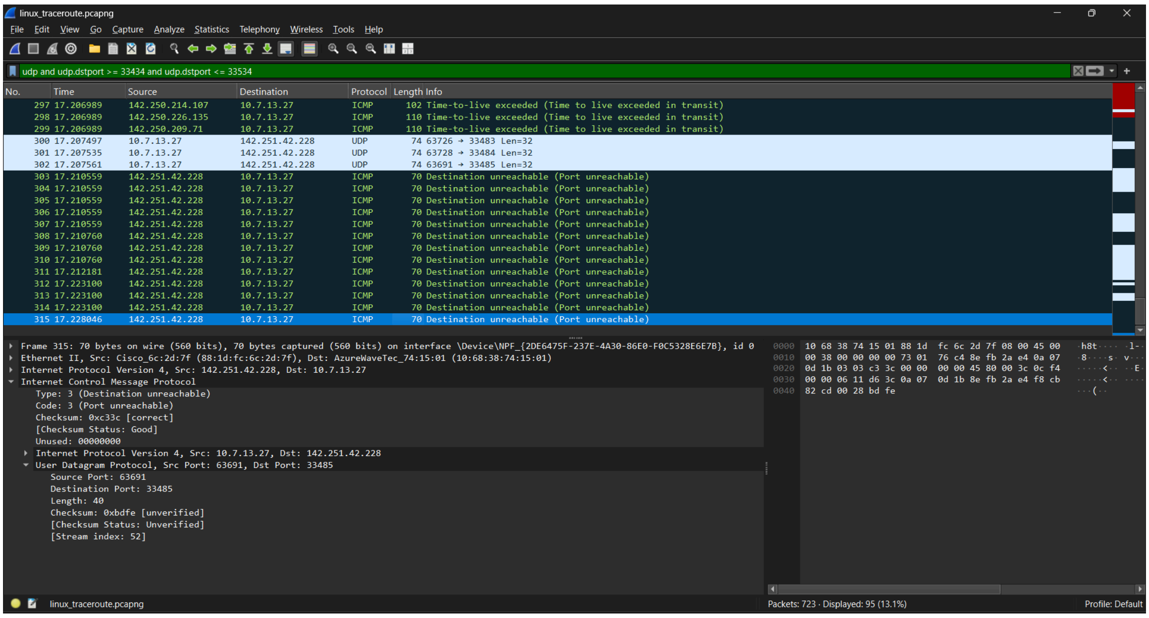
```
udp and udp.dstport >= 33434 and udp.dstport <= 33534

No.  Time       Source          Destination     Protocol Length Info
 204 17.074006  10.7.13.27      142.251.42.228  UDP       74 63687 → 33437 Len=32
 205 17.074337  10.7.13.27      142.251.42.228  UDP       74 63688 → 33438 Len=32
 206 17.074495  10.7.13.27      142.251.42.228  UDP       74 63703 → 33439 Len=32
 207 17.074872  10.7.13.27      142.251.42.228  UDP       74 63717 → 33440 Len=32
 208 17.074895  10.7.13.27      142.251.42.228  UDP       74 63754 → 33443 Len=32
 209 17.074976  10.7.13.27      142.251.42.228  UDP       74 63757 → 33444 Len=32
 210 17.075029  10.7.13.27      142.251.42.228  UDP       74 63731 → 33441 Len=32
 211 17.075053  10.7.13.27      142.251.42.228  UDP       74 63745 → 33442 Len=32
 212 17.075109  10.7.13.27      142.251.42.228  UDP       74 63695 → 33445 Len=32
 213 17.075183  10.7.13.27      142.251.42.228  UDP       74 63667 → 33446 Len=32
 214 17.075297  10.7.13.27      142.251.42.228  UDP       74 63722 → 33449 Len=32
 215 17.075311  10.7.13.27      142.251.42.228  UDP       74 63711 → 33447 Len=32
 216 17.075323  10.7.13.27      142.251.42.228  UDP       74 63752 → 33448 Len=32
 217 17.077173  172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 218 17.079185  172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 219 17.079185  172.16.4.7      10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 220 17.079367  10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 221 17.079367  10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 222 17.079367  10.7.0.5        10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 223 17.079367  10.117.81.253   10.7.13.27      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 217: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
> Ethernet II, Src: Cisco_6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: AzureWaveTec_74:15:01 (10:68:38:74:15:01)
> Internet Protocol Version 4, Src: 172.16.4.7, Dst: 10.7.13.27
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xc63a [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.251.42.228
  v User Datagram Protocol, Src Port: 63717, Dst Port: 33440
      Source Port: 63717
    > Destination Port: 33440
      Length: 40
      Checksum: 0xbe11 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 6]
      UDP payload (32 bytes)
  > Data (32 bytes)
```

```
0000  10 68 38 74 15 01 88 1d  fc 6c 2d 7f 08 00 45 c0   ·h8t····  ·l-···E·
0010  00 58 db da 00 00 fe 01  18 d1 ac 10 04 07 0a 07   ·X······  ········
0020  0d 1b 0b 00 c6 3a 00 00  00 00 45 00 00 3c 01 81   ·····:··  ··E··<··
0030  00 00 01 11 e7 2f 0a 07  0d 1b 8e fb 2a e4 f8 e5   ·····/··  ····*···
0040  82 a0 00 28 be 11 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   JKLMNOPQ  RSTUVWXY
0060  5a 5b 5c 5d 5e 5f                                  Z[\]^_
```

linux_traceroute.pcapng   Packets: 723 · Displayed: 95 (13.1%)   Profile: Default

Final destination responds with ICMP Port Unreachable (Type 3, Code 3)


linux_traceroute.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

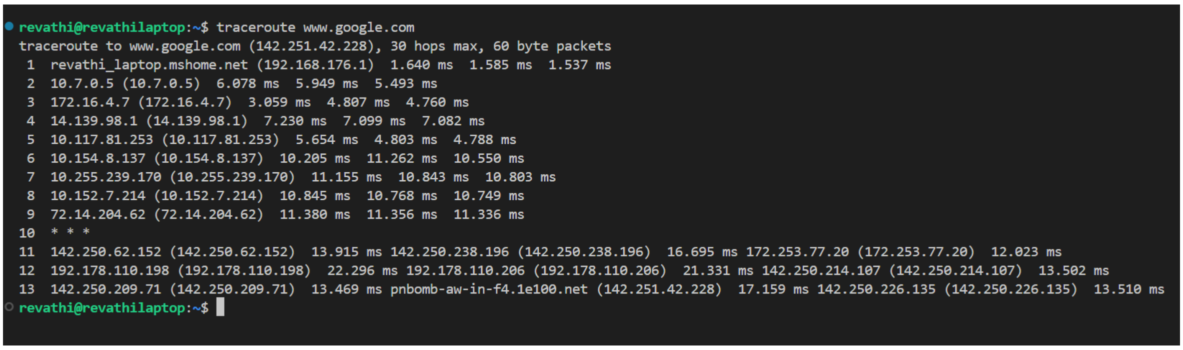
```
udp and udp.dstport >= 33434 and udp.dstport <= 33534

No.  Time       Source          Destination     Protocol Length Info
 297 17.206989  142.250.214.107 10.7.13.27      ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 298 17.206989  142.250.226.135 10.7.13.27      ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 299 17.206989  142.250.209.71  10.7.13.27      ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 300 17.207497  10.7.13.27      142.251.42.228  UDP       74 63726 → 33483 Len=32
 301 17.207535  10.7.13.27      142.251.42.228  UDP       74 63728 → 33484 Len=32
 302 17.207561  10.7.13.27      142.251.42.228  UDP       74 63691 → 33485 Len=32
 303 17.210559  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 304 17.210559  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 305 17.210559  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 306 17.210559  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 307 17.210559  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 308 17.210760  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 309 17.210760  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 310 17.210760  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 311 17.212181  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 312 17.223100  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 313 17.223100  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 314 17.223100  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
 315 17.228046  142.251.42.228  10.7.13.27      ICMP      70 Destination unreachable (Port unreachable)
```

```
> Frame 315: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
> Ethernet II, Src: Cisco_6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: AzureWaveTec_74:15:01 (10:68:38:74:15:01)
> Internet Protocol Version 4, Src: 142.251.42.228, Dst: 10.7.13.27
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xc33c [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.251.42.228
  v User Datagram Protocol, Src Port: 63691, Dst Port: 33485
      Source Port: 63691
      Destination Port: 33485
      Length: 40
      Checksum: 0xbdfe [unverified]
      [Checksum Status: Unverified]
      [Stream index: 52]
```

```
0000  10 68 38 74 15 01 88 1d  fc 6c 2d 7f 08 00 45 00   ·h8t····  ·l-···E·
0010  00 38 00 00 00 00 73 01  76 c4 8e fb 2a e4 0a 07   ·8····s·  v···*···
0020  0d 1b 03 03 c3 3c 00 00  00 00 45 80 00 3c 0c f4   ·····<··  ··E··<··
0030  00 00 06 11 d6 3c 0a 07  0d 1b 8e fb 2a e4 f8 cb   ·····<··  ····*···
0040  82 cd 00 28 bd fe                                  ···(··
```

linux_traceroute.pcapng   Packets: 723 · Displayed: 95 (13.1%)   Profile: Default

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



```
revathi@revathilaptop:~$ traceroute www.google.com
traceroute to www.google.com (142.251.42.228), 30 hops max, 60 byte packets
 1  revathi_laptop.mshome.net (192.168.176.1)  1.640 ms  1.585 ms  1.537 ms
 2  10.7.0.5 (10.7.0.5)  6.078 ms  5.949 ms  5.493 ms
 3  172.16.4.7 (172.16.4.7)  3.059 ms  4.807 ms  4.760 ms
 4  14.139.98.1 (14.139.98.1)  7.230 ms  7.099 ms  7.082 ms
 5  10.117.81.253 (10.117.81.253)  5.654 ms  4.803 ms  4.788 ms
 6  10.154.8.137 (10.154.8.137)  10.205 ms  11.262 ms  10.550 ms
 7  10.255.239.170 (10.255.239.170)  11.155 ms  10.843 ms  10.803 ms
 8  10.152.7.214 (10.152.7.214)  10.845 ms  10.768 ms  10.749 ms
 9  72.14.204.62 (72.14.204.62)  11.380 ms  11.356 ms  11.336 ms
10  * * *
11  142.250.62.152 (142.250.62.152)  13.915 ms 142.250.238.196 (142.250.238.196)  16.695 ms 172.253.77.20 (172.253.77.20)  12.023 ms
12  192.178.110.198 (192.178.110.198)  22.296 ms 192.178.110.206 (192.178.110.206)  21.331 ms 142.250.214.107 (142.250.214.107)  13.502 ms
13  142.250.209.71 (142.250.209.71)  13.469 ms pnbomb-aw-in-f4.1e100.net (142.251.42.228)  17.159 ms 142.250.226.135 (142.250.226.135)  13.510 ms
revathi@revathilaptop:~$
```

I spotted the *** at hop 10 while using traceroute. That means your probes timed out because no ICMP response was received. Based on networking fundamentals and traceroute behavior, these might be the reasons:

ICMP Replies Are Blocked by Firewall/ACL: Many routers (especially in ISP backbones or within Google's network) are configured to drop or rate-limit ICMP responses for security and performance reasons. So even though packets pass through, the router does not send back the expected ICMP *Time Exceeded* message.

Router is Busy or Deprioritizes TTL-Expired Responses: Routers prioritize forwarding actual traffic over generating ICMP error messages. The router may not generate an ICMP reply if it is heavily loaded. Traceroute probes are low-priority control traffic, so routers often ignore them to conserve resources.

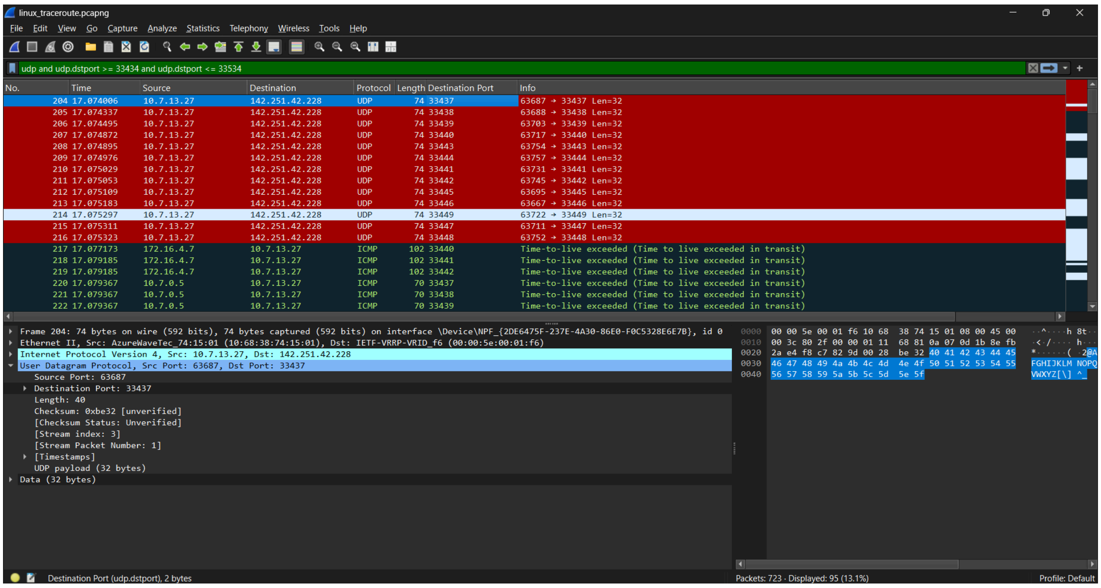
In addition to firewalls blocking ICMP and routers deprioritizing responses, some routers may apply ICMP rate-limiting (to avoid DoS attacks), or the reply may be lost due to asymmetric routing. This also results in *** in traceroute output.

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

In Linux traceroute (default UDP mode), the **UDP destination port** field changes between successive probes. Traceroute starts with a base port (by default,≥33434) and increments it (33435, 33436, …) for each probe.

- This ensures that when the destination host receives the probe, it replies with an **ICMP Destination Unreachable — Port Unreachable** message (since no application listens to those high-numbered ports).
- Routers along the path generate **ICMP Time Exceeded** messages when the TTL expires, and the unique destination port allows traceroute to correctly match each ICMP reply to the probe that triggered it.
- Note: the **TTL value** increases per hop, whereas the **UDP destination port** changes between probes. This combination lets traceroute discover intermediate hops and correlate replies with the right probe packet.

In the screenshot below, I added the UDP.dstport column in Wireshark, showing how the UDP destination port increments across multiple probes.



udp and udp.dstport >= 33434 and udp.dstport <= 33534

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
204	17.074006	10.7.13.27	142.251.42.228	UDP	74	33437	63687 → 33437 Len=32
205	17.074337	10.7.13.27	142.251.42.228	UDP	74	33438	63688 → 33438 Len=32
206	17.074495	10.7.13.27	142.251.42.228	UDP	74	33439	63703 → 33439 Len=32
207	17.074872	10.7.13.27	142.251.42.228	UDP	74	33440	63717 → 33440 Len=32
208	17.074895	10.7.13.27	142.251.42.228	UDP	74	33443	63754 → 33443 Len=32
209	17.074976	10.7.13.27	142.251.42.228	UDP	74	33444	63757 → 33444 Len=32
210	17.075029	10.7.13.27	142.251.42.228	UDP	74	33441	63731 → 33441 Len=32
211	17.075053	10.7.13.27	142.251.42.228	UDP	74	33442	63745 → 33442 Len=32
212	17.075109	10.7.13.27	142.251.42.228	UDP	74	33445	63695 → 33445 Len=32
213	17.075183	10.7.13.27	142.251.42.228	UDP	74	33446	63667 → 33446 Len=32
214	17.075297	10.7.13.27	142.251.42.228	UDP	74	33449	63722 → 33449 Len=32
215	17.075311	10.7.13.27	142.251.42.228	UDP	74	33447	63711 → 33447 Len=32
216	17.075323	10.7.13.27	142.251.42.228	UDP	74	33448	63752 → 33448 Len=32
217	17.077173	172.16.4.7	10.7.13.27	ICMP	102	33440	Time-to-live exceeded (Time to live exceeded in transit)
218	17.079185	172.16.4.7	10.7.13.27	ICMP	102	33441	Time-to-live exceeded (Time to live exceeded in transit)
219	17.079185	172.16.4.7	10.7.13.27	ICMP	102	33442	Time-to-live exceeded (Time to live exceeded in transit)
220	17.079367	10.7.0.5	10.7.13.27	ICMP	70	33437	Time-to-live exceeded (Time to live exceeded in transit)
221	17.079367	10.7.0.5	10.7.13.27	ICMP	70	33438	Time-to-live exceeded (Time to live exceeded in transit)
222	17.079367	10.7.0.5	10.7.13.27	ICMP	70	33439	Time-to-live exceeded (Time to live exceeded in transit)

```
Frame 204: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2DE6475F-237E-4A30-86E0-F0C5328E6E7B}, id 0
Ethernet II, Src: AzureWaveTec_74:15:01 (10:68:38:74:15:01), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
Internet Protocol Version 4, Src: 10.7.13.27, Dst: 142.251.42.228
User Datagram Protocol, Src Port: 63687, Dst Port: 33437
    Source Port: 63687
    Destination Port: 33437
    Length: 40
    Checksum: 0xbe32 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (32 bytes)
Data (32 bytes)
```

```
0000  00 00 5e 00 01 f6 10 68  38 74 15 01 08 00 45 00   ··^····h 8t····E·
0010  00 3c 80 2f 00 00 01 11  68 81 0a 07 0d 1b 8e fb   ·<·/···· h·······
0020  2a e4 f8 c7 82 9d 00 28  be 32 40 41 42 43 44 45   *······( ·2@ABCDE
0030  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM NOPQRSTU
0040  56 57 58 59 5a 5b 5c 5d  5e 5f                     VWXYZ[\] ^_
```

Destination Port (udp.dstport), 2 bytes

Packets: 723 · Displayed: 95 (13.1%)

Profile: Default

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

- **Intermediate hops:** Routers send ICMP Time Exceeded (Type 11, Code 0) when a probe's TTL reaches zero. This indicates the probe expired before reaching the destination. In Wireshark, filter with icmp. Type == 11 and show one packet with ICMP Time Exceeded (Screenshot added in Q1).
- **Final hop (Linux traceroute, UDP probes):** Destination host sends ICMP Destination Unreachable — Port Unreachable (Type 3, Code 3) because the UDP probe reaches the host but is sent to a high, unused port. Filter ICMP.type == 3 && icmp.code == 3, highlight the packet, and show source IP = final hop (Screenshot added in Q1).
- **Final hop (Windows tracert, ICMP probes):** Destination host sends ICMP Echo Reply (Type 0), since Windows sends ICMP Echo Requests. Filter ICMP.type == 0 and show Echo Reply from the final hop (Screenshot added in Q1).

5. 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 mode): If the firewall blocks UDP traffic, the UDP probes from traceroute will be dropped. Intermediate routers may still generate **ICMP Time Exceeded (Type 11)** messages so that the first few hops can appear. However, the final destination will not send the expected **ICMP Port Unreachable (Type 3, Code 3)** reply.

Result: traceroute output shows *** for the later hops and fails to resolve the destination. In Wireshark, filtering with ICMP.type == 3 && icmp.code == 3 confirms no Port Unreachable messages.

Windows tracert (ICMP mode): Since Windows tracert uses **ICMP Echo Requests** (Type 8) by default, and ICMP is allowed through the firewall, it still works normally. The final destination responds with an **ICMP Echo Reply** (Type 0).

Result: tracert completes successfully. In Wireshark, filtering with ICMP.type == 0 shows the Echo Reply packet (as seen in the Q1 screenshots where tracert generated Echo Requests and got Echo Replies).