CS 331 - Computer Networks

Assignment-1

Shah Harshil Hardik (23110132), Jeet Joshi (23110148)

Task-1: DNS Resolver

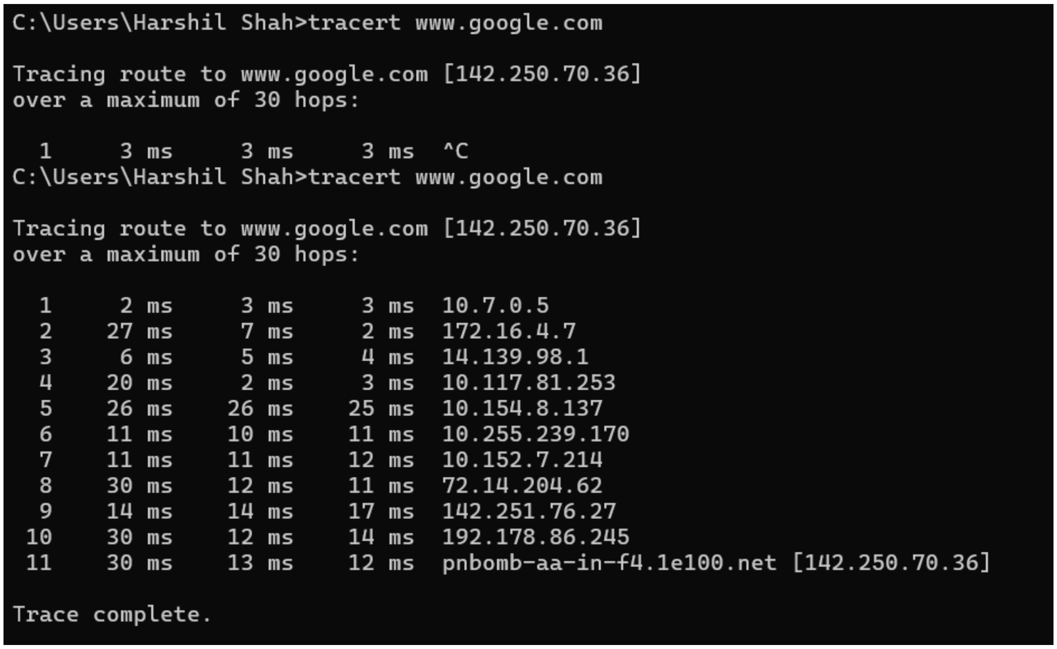
Custom Header (HHMMSSID)	Domain Name	Resolved IP Addresses
18515800	_apple-mobdev._tcp.local.	192.168.1.6
18515801	_apple-mobdev._tcp.local.	192.168.1.7
18515802	bing.com.	192.168.1.8
18515803	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.9
18515804	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
18515805	example.com.	192.168.1.6
18515906	amazon.com.	192.168.1.7
18515907	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8
18515908	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.9
18515909	yahoo.com.	192.168.1.10

18515910	_apple-mobdev._tcp.local.	192.168.1.6
18515911	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.7
18515912	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8
18520013	google.com.	192.168.1.9
18520014	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
18520015	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.6
18520016	_apple-mobdev._tcp.local.	192.168.1.7
18520017	_apple-mobdev._tcp.local.	192.168.1.8
18520018	github.com.	192.168.1.9
18520019	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
18520020	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.6
18520021	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.7
18520022	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8

Task-2: Traceroute Protocol Behaviour

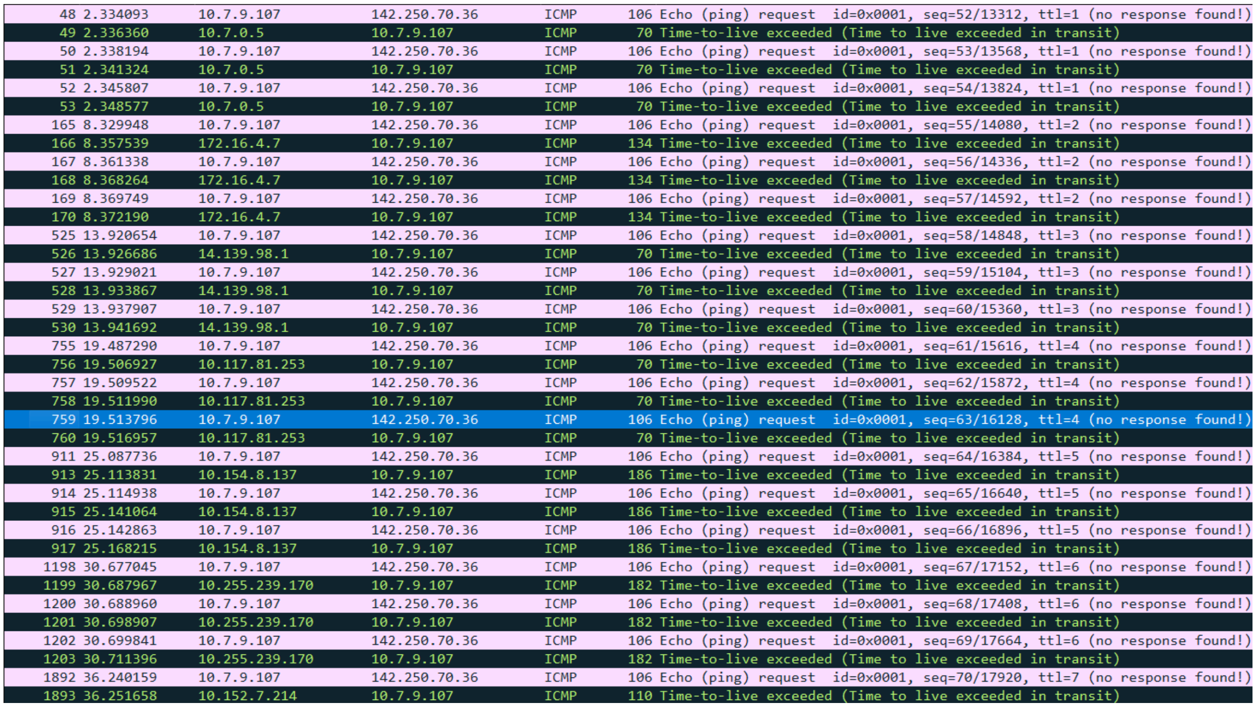
Windows:

`tracert` output for www.google.com:

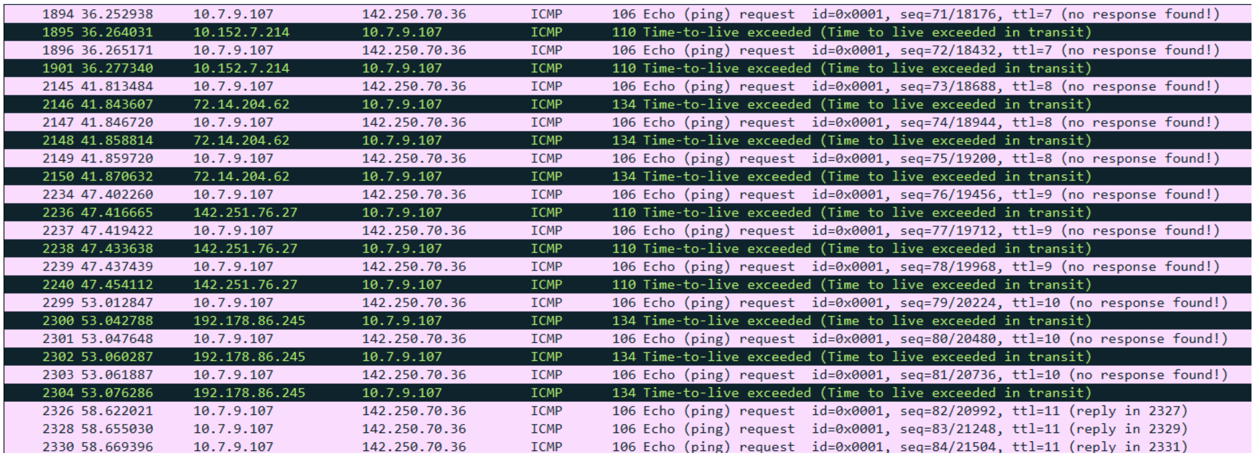


```
C:\Users\Harshil Shah>tracert www.google.com

Tracing route to www.google.com [142.250.70.36]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  ^C
C:\Users\Harshil Shah>tracert www.google.com

Tracing route to www.google.com [142.250.70.36]
over a maximum of 30 hops:

  1     2 ms     3 ms     3 ms  10.7.0.5
  2    27 ms     7 ms     2 ms  172.16.4.7
  3     6 ms     5 ms     4 ms  14.139.98.1
  4    20 ms     2 ms     3 ms  10.117.81.253
  5    26 ms    26 ms    25 ms  10.154.8.137
  6    11 ms    10 ms    11 ms  10.255.239.170
  7    11 ms    11 ms    12 ms  10.152.7.214
  8    30 ms    12 ms    11 ms  72.14.204.62
  9    14 ms    14 ms    17 ms  142.251.76.27
 10    30 ms    12 ms    14 ms  192.178.86.245
 11    30 ms    13 ms    12 ms  pnbomb-aa-in-f4.1e100.net [142.250.70.36]

Trace complete.
```

Wireshark:



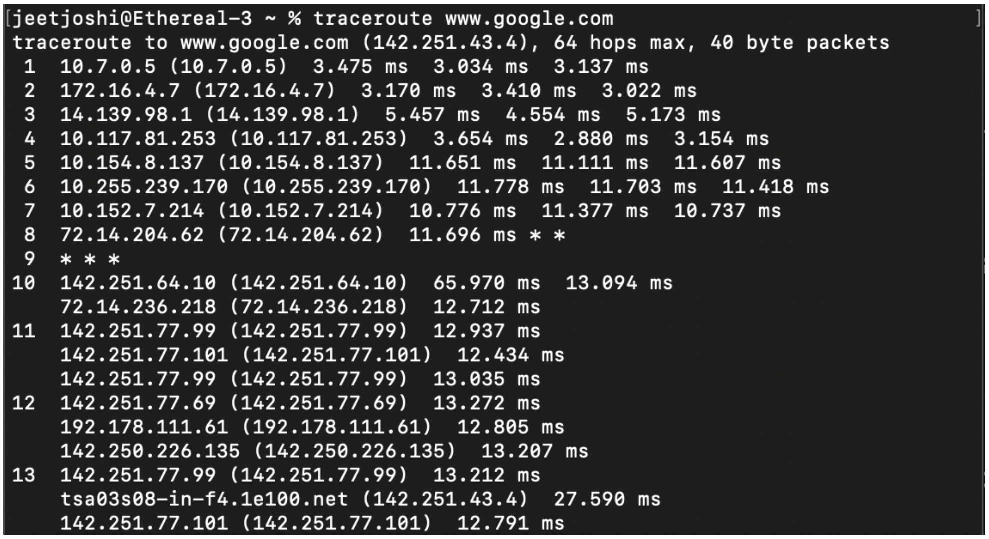
```
  48 2.334093    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=52/13312, ttl=1 (no response found!)
  49 2.336360    10.7.0.5        10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  50 2.338194    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=53/13568, ttl=1 (no response found!)
  51 2.341324    10.7.0.5        10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  52 2.345807    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=54/13824, ttl=1 (no response found!)
  53 2.348577    10.7.0.5        10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 165 8.329948    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=55/14080, ttl=2 (no response found!)
 166 8.357539    172.16.4.7      10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
 167 8.361338    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=56/14336, ttl=2 (no response found!)
 168 8.368264    172.16.4.7      10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
 169 8.369749    10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=57/14592, ttl=2 (no response found!)
 170 8.372190    172.16.4.7      10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
 525 13.920654   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=58/14848, ttl=3 (no response found!)
 526 13.926686   14.139.98.1     10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 527 13.929021   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=59/15104, ttl=3 (no response found!)
 528 13.933867   14.139.98.1     10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 529 13.937907   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=60/15360, ttl=3 (no response found!)
 530 13.941692   14.139.98.1     10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 755 19.487290   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=61/15616, ttl=4 (no response found!)
 756 19.506927   10.117.81.253   10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 757 19.509522   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=62/15872, ttl=4 (no response found!)
 758 19.511990   10.117.81.253   10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 759 19.513796   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=63/16128, ttl=4 (no response found!)
 760 19.516957   10.117.81.253   10.7.9.107      ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
 911 25.087736   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=64/16384, ttl=5 (no response found!)
 913 25.113831   10.154.8.137    10.7.9.107      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
 914 25.114938   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=65/16640, ttl=5 (no response found!)
 915 25.141064   10.154.8.137    10.7.9.107      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
 916 25.142863   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=66/16896, ttl=5 (no response found!)
 917 25.168215   10.154.8.137    10.7.9.107      ICMP   186 Time-to-live exceeded (Time to live exceeded in transit)
1198 30.677045   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=67/17152, ttl=6 (no response found!)
1199 30.687967   10.255.239.170  10.7.9.107      ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
1200 30.688960   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=68/17408, ttl=6 (no response found!)
1201 30.698907   10.255.239.170  10.7.9.107      ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
1202 30.699841   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=69/17664, ttl=6 (no response found!)
1203 30.711396   10.255.239.170  10.7.9.107      ICMP   182 Time-to-live exceeded (Time to live exceeded in transit)
1892 36.240159   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=70/17920, ttl=7 (no response found!)
1893 36.251658   10.152.7.214    10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
```



```
1894 36.252938   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=71/18176, ttl=7 (no response found!)
1895 36.264031   10.152.7.214    10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
1896 36.265171   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=72/18432, ttl=7 (no response found!)
1901 36.277340   10.152.7.214    10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
2145 41.813484   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=73/18688, ttl=8 (no response found!)
2146 41.843607   72.14.204.62    10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2147 41.846720   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=74/18944, ttl=8 (no response found!)
2148 41.858814   72.14.204.62    10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2149 41.859720   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=75/19200, ttl=8 (no response found!)
2150 41.870632   72.14.204.62    10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2234 47.402260   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=76/19456, ttl=9 (no response found!)
2236 47.416665   142.251.76.27   10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
2237 47.419422   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=77/19712, ttl=9 (no response found!)
2238 47.433638   142.251.76.27   10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
2239 47.437439   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=78/19968, ttl=9 (no response found!)
2240 47.454112   142.251.76.27   10.7.9.107      ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
2299 53.012847   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=79/20224, ttl=10 (no response found!)
2300 53.042788   192.178.86.245  10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2301 53.047648   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=80/20480, ttl=10 (no response found!)
2302 53.060287   192.178.86.245  10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2303 53.061887   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=81/20736, ttl=10 (no response found!)
2304 53.076286   192.178.86.245  10.7.9.107      ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
2326 58.622021   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=82/20992, ttl=11 (reply in 2327)
2328 58.655030   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=83/21248, ttl=11 (reply in 2329)
2330 58.669396   10.7.9.107      142.250.70.36   ICMP   106 Echo (ping) request  id=0x0001, seq=84/21504, ttl=11 (reply in 2331)
```

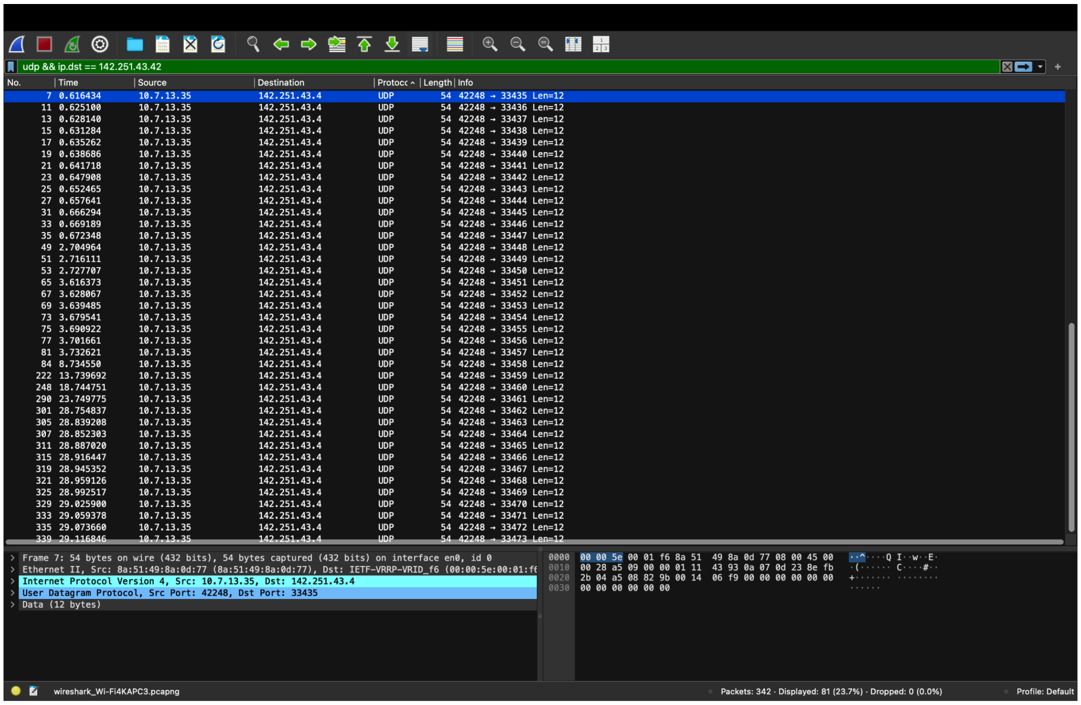
MacOS:

`traceroute` output for www.google.com:



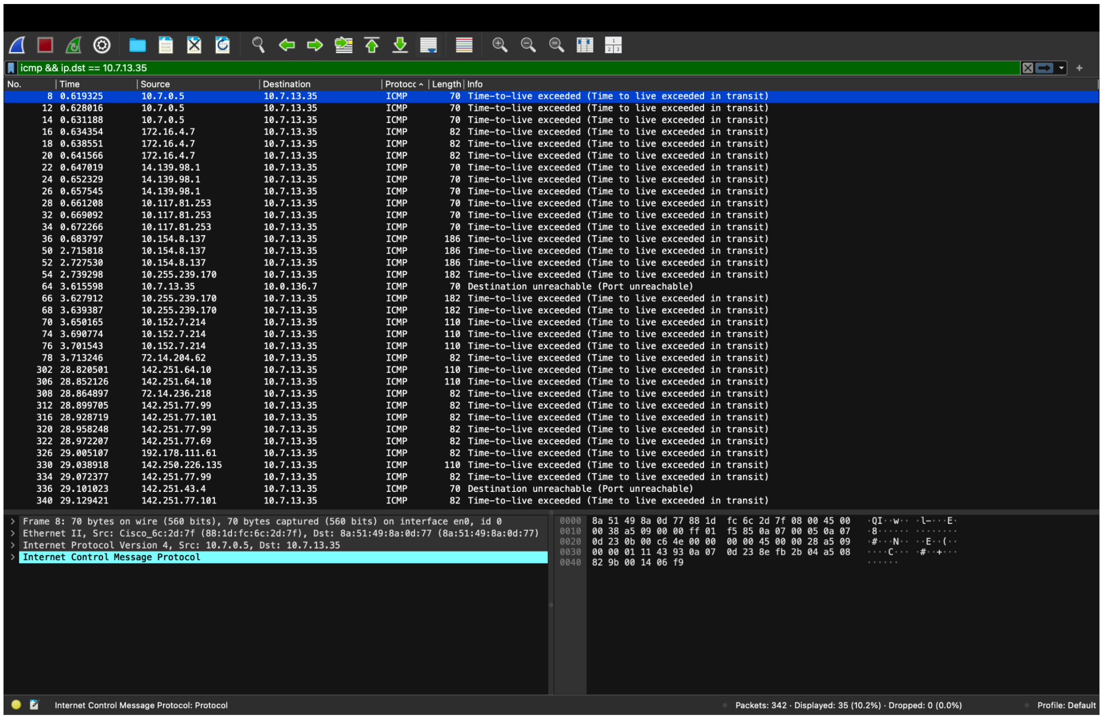
```
[jeetjoshi@Ethereal-3 ~ % traceroute www.google.com                              ]
 traceroute to www.google.com (142.251.43.4), 64 hops max, 40 byte packets
  1  10.7.0.5 (10.7.0.5)  3.475 ms  3.034 ms  3.137 ms
  2  172.16.4.7 (172.16.4.7)  3.170 ms  3.410 ms  3.022 ms
  3  14.139.98.1 (14.139.98.1)  5.457 ms  4.554 ms  5.173 ms
  4  10.117.81.253 (10.117.81.253)  3.654 ms  2.880 ms  3.154 ms
  5  10.154.8.137 (10.154.8.137)  11.651 ms  11.111 ms  11.607 ms
  6  10.255.239.170 (10.255.239.170)  11.778 ms  11.703 ms  11.418 ms
  7  10.152.7.214 (10.152.7.214)  10.776 ms  11.377 ms  10.737 ms
  8  72.14.204.62 (72.14.204.62)  11.696 ms * *
  9  * * *
 10  142.251.64.10 (142.251.64.10)  65.970 ms  13.094 ms
     72.14.236.218 (72.14.236.218)  12.712 ms
 11  142.251.77.99 (142.251.77.99)  12.937 ms
     142.251.77.101 (142.251.77.101)  12.434 ms
     142.251.77.99 (142.251.77.99)  13.035 ms
 12  142.251.77.69 (142.251.77.69)  13.272 ms
     192.178.111.61 (192.178.111.61)  12.805 ms
     142.250.226.135 (142.250.226.135)  13.207 ms
 13  142.251.77.99 (142.251.77.99)  13.212 ms
     tsa03s08-in-f4.1e100.net (142.251.43.4)  27.590 ms
     142.251.77.101 (142.251.77.101)  12.791 ms
```

Wireshark:



```
udp && ip.dst == 142.251.43.42

No.  Time       Source       Destination    Protocol Length Info
  7  0.616434   10.7.13.35   142.251.43.4   UDP      54  42248 → 33435 Len=12
 11  0.625100   10.7.13.35   142.251.43.4   UDP      54  42248 → 33436 Len=12
 13  0.628140   10.7.13.35   142.251.43.4   UDP      54  42248 → 33437 Len=12
 15  0.631284   10.7.13.35   142.251.43.4   UDP      54  42248 → 33438 Len=12
 17  0.635262   10.7.13.35   142.251.43.4   UDP      54  42248 → 33439 Len=12
 19  0.638686   10.7.13.35   142.251.43.4   UDP      54  42248 → 33440 Len=12
 21  0.641718   10.7.13.35   142.251.43.4   UDP      54  42248 → 33441 Len=12
 23  0.647908   10.7.13.35   142.251.43.4   UDP      54  42248 → 33442 Len=12
 25  0.652465   10.7.13.35   142.251.43.4   UDP      54  42248 → 33443 Len=12
 27  0.657641   10.7.13.35   142.251.43.4   UDP      54  42248 → 33444 Len=12
 31  0.666294   10.7.13.35   142.251.43.4   UDP      54  42248 → 33445 Len=12
 33  0.669189   10.7.13.35   142.251.43.4   UDP      54  42248 → 33446 Len=12
 35  0.672348   10.7.13.35   142.251.43.4   UDP      54  42248 → 33447 Len=12
 49  2.704964   10.7.13.35   142.251.43.4   UDP      54  42248 → 33448 Len=12
 51  2.716111   10.7.13.35   142.251.43.4   UDP      54  42248 → 33449 Len=12
 53  2.727707   10.7.13.35   142.251.43.4   UDP      54  42248 → 33450 Len=12
 65  3.616373   10.7.13.35   142.251.43.4   UDP      54  42248 → 33451 Len=12
 67  3.628067   10.7.13.35   142.251.43.4   UDP      54  42248 → 33452 Len=12
 69  3.639485   10.7.13.35   142.251.43.4   UDP      54  42248 → 33453 Len=12
 73  3.679541   10.7.13.35   142.251.43.4   UDP      54  42248 → 33454 Len=12
 75  3.690922   10.7.13.35   142.251.43.4   UDP      54  42248 → 33455 Len=12
 77  3.701661   10.7.13.35   142.251.43.4   UDP      54  42248 → 33456 Len=12
 81  3.732621   10.7.13.35   142.251.43.4   UDP      54  42248 → 33457 Len=12
 84  8.734550   10.7.13.35   142.251.43.4   UDP      54  42248 → 33458 Len=12
222  13.739692  10.7.13.35   142.251.43.4   UDP      54  42248 → 33459 Len=12
248  18.744751  10.7.13.35   142.251.43.4   UDP      54  42248 → 33460 Len=12
290  23.749775  10.7.13.35   142.251.43.4   UDP      54  42248 → 33461 Len=12
301  28.754837  10.7.13.35   142.251.43.4   UDP      54  42248 → 33462 Len=12
305  28.839208  10.7.13.35   142.251.43.4   UDP      54  42248 → 33463 Len=12
307  28.852303  10.7.13.35   142.251.43.4   UDP      54  42248 → 33464 Len=12
311  28.887020  10.7.13.35   142.251.43.4   UDP      54  42248 → 33465 Len=12
315  28.916447  10.7.13.35   142.251.43.4   UDP      54  42248 → 33466 Len=12
319  28.945352  10.7.13.35   142.251.43.4   UDP      54  42248 → 33467 Len=12
321  28.959126  10.7.13.35   142.251.43.4   UDP      54  42248 → 33468 Len=12
325  28.992517  10.7.13.35   142.251.43.4   UDP      54  42248 → 33469 Len=12
329  29.025900  10.7.13.35   142.251.43.4   UDP      54  42248 → 33470 Len=12
333  29.059378  10.7.13.35   142.251.43.4   UDP      54  42248 → 33471 Len=12
335  29.073660  10.7.13.35   142.251.43.4   UDP      54  42248 → 33472 Len=12
339  29.116846  10.7.13.35   142.251.43.4   UDP      54  42248 → 33473 Len=12

> Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
> Ethernet II, Src: 8a:51:49:8a:0d:77 (8a:51:49:8a:0d:77), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6
> Internet Protocol Version 4, Src: 10.7.13.35, Dst: 142.251.43.4
> User Datagram Protocol, Src Port: 42248, Dst Port: 33435
> Data (12 bytes)

0000  00 00 5e 00 01 f6 8a 51  49 8a 0d 77 08 00 45 00   ··^····Q I··w··E·
0010  00 28 a5 09 00 00 01 11  43 93 0a 07 0d 23 8e fb   ·(······ C····#··
0020  2b 04 a5 08 82 9b 00 14  06 f9 00 00 00 00 00 00   +······· ········
0030  00 00 00 00 00 00                                  ······

wireshark_Wi-Fi4KAPC3.pcapng          Packets: 342 · Displayed: 81 (23.7%) · Dropped: 0 (0.0%)          Profile: Default
```

UDP probes going out



icmp && ip.dst == 10.7.13.35

```
No.   Time       Source           Destination   Protocol Length Info
  8 0.619325    10.7.0.5         10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 12 0.628016    10.7.0.5         10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 14 0.631188    10.7.0.5         10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 16 0.634354    172.16.4.7       10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
 18 0.638551    172.16.4.7       10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
 20 0.641566    172.16.4.7       10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
 22 0.647019    14.139.98.1      10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 24 0.652329    14.139.98.1      10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 26 0.657545    14.139.98.1      10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 28 0.661208    10.117.81.253    10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 32 0.669092    10.117.81.253    10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 34 0.672266    10.117.81.253    10.7.13.35    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 36 0.683797    10.154.8.137     10.7.13.35    ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
 50 2.715818    10.154.8.137     10.7.13.35    ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
 52 2.727530    10.154.8.137     10.7.13.35    ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
 54 2.739298    10.255.239.170   10.7.13.35    ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
 64 3.615598    10.7.13.35       10.0.136.7    ICMP      70 Destination unreachable (Port unreachable)
 66 3.627912    10.255.239.170   10.7.13.35    ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
 68 3.639387    10.255.239.170   10.7.13.35    ICMP     182 Time-to-live exceeded (Time to live exceeded in transit)
 70 3.650165    10.152.7.214     10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 74 3.690774    10.152.7.214     10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 76 3.701543    10.152.7.214     10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 78 3.713246    72.14.204.62     10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
302 28.820501   142.251.64.10    10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
306 28.852126   142.251.64.10    10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
308 28.864897   72.14.236.218    10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
312 28.899705   142.251.77.99    10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
316 28.928719   142.251.77.101   10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
320 28.958248   142.251.77.99    10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
322 28.972207   142.251.77.69    10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
326 29.005107   192.178.111.61   10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
330 29.038918   142.250.226.135  10.7.13.35    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
334 29.072377   142.251.77.99    10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
336 29.101023   142.251.43.4     10.7.13.35    ICMP      70 Destination unreachable (Port unreachable)
340 29.129421   142.251.77.101   10.7.13.35    ICMP      82 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 8: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_6c:2d:7f (88:1d:fc:6c:2d:7f), Dst: 8a:51:49:8a:0d:77 (8a:51:49:8a:0d:77)
> Internet Protocol Version 4, Src: 10.7.0.5, Dst: 10.7.13.35
> Internet Control Message Protocol
```

```
0000  8a 51 49 8a 0d 77 88 1d  fc 6c 2d 7f 08 00 45 00   ·QI··w·· ·l-···E·
0010  00 38 a5 09 00 00 ff 01  f5 85 0a 07 00 05 0a 07   ·8······ ········
0020  0d 23 0b 00 c6 4e 00 00  00 00 45 00 00 28 a5 09   ·#···N·· ··E··(··
0030  00 00 01 11 43 93 0a 07  0d 23 8e fb 2b 04 a5 08   ····C··· ·#··+···
0040  82 9b 00 14 06 f9                                  ······
```

Internet Control Message Protocol: Protocol

Packets: 342 · Displayed: 35 (10.2%) · Dropped: 0 (0.0%)

Profile: Default

ICMP replies coming back

Observations:

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

- Windows uses the ICMP (Internet Control Message Protocol) by default for tracert for both request and response. For analysis in wireshark, we can filter these packets using the filter command: `icmp && ip.dst == <destination-ip>` (here 142.250.70.36). This would give all the packets which use ICMP protocol and are directed towards the IP of the destination.
- Linux/MacOS traceroute uses UDP (User Datagram Protocol) protocol for sending requests and ICMP protocol for receiving response. For analysis in wireshark, we can filter these packets using the filter command `udp && ip.dst == <destination-ip>`(here 142.251.43.4) for the packets sent as request and `icmp && ip.dst == <host-ip>` (here 10.7.13.35) for the packets received as response from the server.

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

- * in the traceroute output indicates that no response is received from that hop within the time limit. * * * means that all the three probes that were sent in that hop didn’t send any response back within the time limit.
- The reasons why a router might not reply are:
    a. Configuration: Routers may have a rate limit on the ICMP response or has a prioritization for the actual service requests which may lead to routers ignoring the traceroute requests.
    b. Firewall or Filtering policies: Firewalls along the path may be configured to drop certain types of traffic, such as the high-numbered UDP ports used by Linux/macOS traceroute or even ICMP replies themselves. This is often a deliberate security measure to prevent network probing or scanning.

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

- In Linux traceroute, the destination port for UDP changes between successive probes. It usually starts with the port 33434, and is incremented on every hop. This is done so that the ICMP responses received from the server can be matched to the correct sending probe by matching the destination port. Without changing the destination port, traceroute would not be able to distinguish between replies corresponding to different probes, especially since multiple probes are sent per TTL value.

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

- For the intermediate hops, the response received is of type **Time-To-Live exceeded**. When a probe packet's TTL reaches 0 at an intermediate router, the router discards the packet and sends a reply TTL exceeded.
- At the final hop, the response received is of type **destination unreachable**. This indicates the traceroute that it has reached its destination.

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, Windows tracert would remain unaffected as it uses only ICMP protocol for both request and response. But, Linux/MacOS traceroute uses UDP for sending the requests and ICMP for receiving the response. So, the requests sent by the Linux/MacOS traceroute would be dropped by the firewall before reaching the router. So, traceroute will not receive any responses also. Hence, it would show `* * *` for every hop till the maximum number of hops allowed.
- But Linux/MacOS also provides a flag `-I` in the traceroute, which then uses the ICMP protocol for sending the request probes also. In that case, there would be no effect of the firewall.