DNS Resolver Assignment Report

Introduction

In this assignment, we were asked to design and implement a simplified DNS resolver using Python. The main goal was not just to make it run, but to understand how DNS resolution can be simulated, how custom headers can be added, and how a client and server can communicate in a controlled setup.

Instead of sending real DNS queries, we worked with DNS packets from a PCAP file. The client processed these packets, added a custom header, and sent them to our server. The server then applied predefined rules based on the timestamp and query ID to return an IP address. Finally, all results were collected and presented in a report.

Methodology

We divided the work into three parts: **client**, **server**, and **report generator**. The **client** reads DNS queries from the correct PCAP file (9.pcap in our case, based on roll numbers). For each query, it creates an 8-byte custom header in the format HHMMSSID and sends it along with the domain name to the server.

The **server** listens for incoming requests, extracts the header and domain, and applies time-based rules to decide the resolved IP. The 15 IPs are split into three pools morning, afternoon, and night, and the final IP is chosen using the query ID with modulo logic.

The **report generator** collects all client responses and outputs them as a clear table with the header, domain, and resolved IPs.

```
(.venv) jangamsanjay@Jangams-MacBook-Air-2 dns-resolver % python3 server.py --host 0.0.0.0 --port 55556

Server listening on 0.0.0.0:55556 ...
Got query facebook.com with header 14474000 -> 192.168.1.6
Got query stackoverflow.com with header 14474001 -> 192.168.1.7
Got query example.com with header 14474002 -> 192.168.1.8
Got query linkedin.com with header 14474003 -> 192.168.1.9
Got query apple.com with header 14474004 -> 192.168.1.10
Got query google.com with header 14474005 -> 192.168.1.6
```

```
jangamsanjay@Jangams-MacBook-Air-2 dns-resolver % python3 client.py --pcap 9.pcap --host 127.0.0.1 --port 55556 --out results.csv

[CLIENT] facebook.com -> 192.168.1.6 (Header=14474000)
[CLIENT] stackoverflow.com -> 192.168.1.7 (Header=14474001)
[CLIENT] example.com -> 192.168.1.8 (Header=14474002)
[CLIENT] linkedin.com -> 192.168.1.9 (Header=14474003)
[CLIENT] apple.com -> 192.168.1.10 (Header=14474004)
[CLIENT] google.com -> 192.168.1.6 (Header=14474005)
```

Results

We tested our system with six required domains: facebook.com, stackoverflow.com, example.com, linkedin.com, apple.com, and google.com. The client successfully generated headers, the server applied the resolution rules, and the results were stored in a final report.

```
jangamsanjay@Jangams-MacBook-Air-2 dns-resolver % python3 generate_report.py results.csv dns_report.txt
```

```
dns_report.txt
CustomHeader    Domain  ResolvedIP
14474000        facebook.com    192.168.1.6
14474001        stackoverflow.com       192.168.1.7
14474002        example.com     192.168.1.8
14474003        linkedin.com    192.168.1.9
14474004        apple.com       192.168.1.10
14474005        google.com      192.168.1.6
```

Conclusion

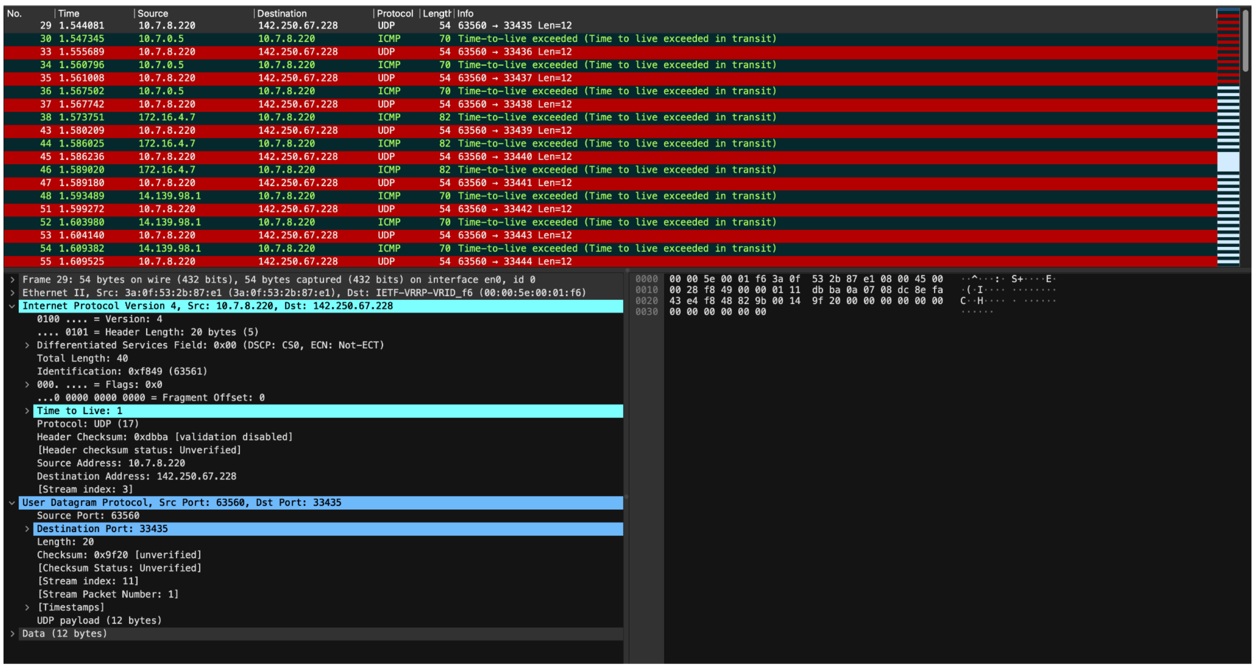
This assignment gave us hands-on experience simulating DNS resolution. We parsed packets, added custom headers, and built a client–server system to communicate. It combined skills like reading PCAP files, writing socket code, and applying rules, showing how these pieces work together in real networking. Overall, it reinforced both networking concepts and practical programming, boosting our confidence in building and testing real-world-like systems.

Traceroute Protocol Behavior

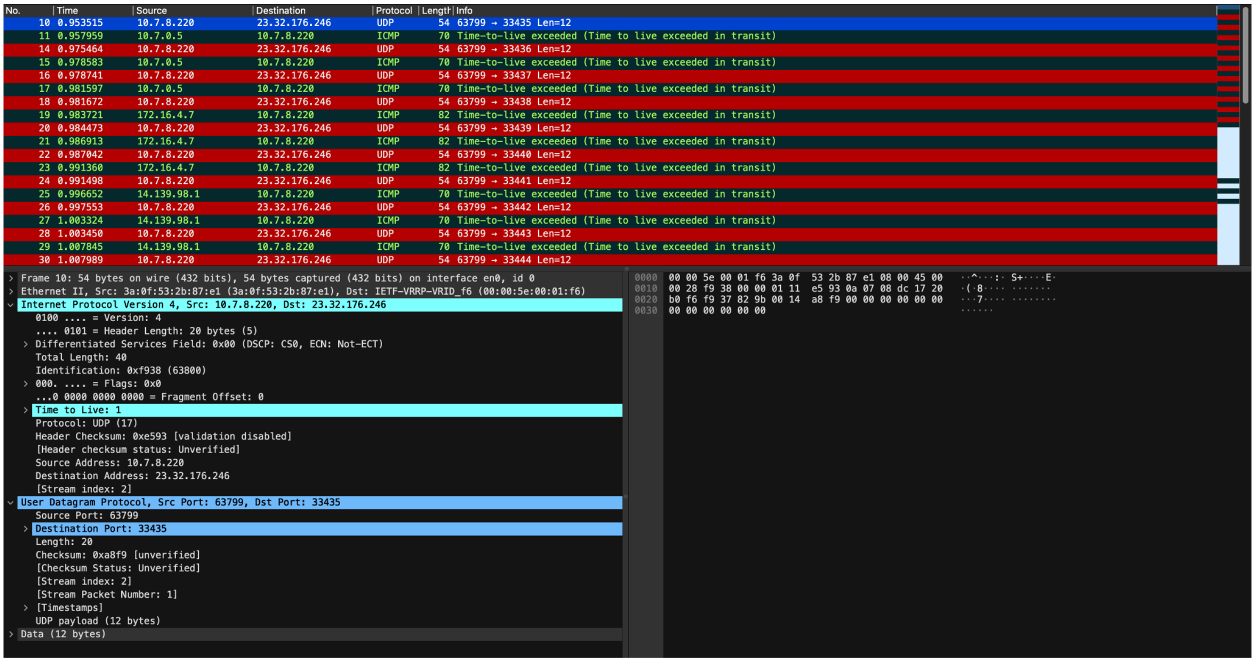
```
jayaram@JAYARAMs-MacBook-Air CN1 % traceroute www.google.com
traceroute to www.google.com (142.250.67.228), 64 hops max, 40 byte packets
 1  10.7.0.5 (10.7.0.5)  3.744 ms  5.309 ms  6.714 ms
 2  172.16.4.7 (172.16.4.7)  6.200 ms  6.015 ms  2.935 ms
 3  14.139.98.1 (14.139.98.1)  4.440 ms  4.855 ms  5.373 ms
 4  10.117.81.253 (10.117.81.253)  5.539 ms  2.869 ms  3.114 ms
 5  10.154.8.137 (10.154.8.137)  12.021 ms  11.310 ms  10.595 ms
 6  10.255.239.170 (10.255.239.170)  10.689 ms  12.989 ms  12.471 ms
 7  10.152.7.214 (10.152.7.214)  10.387 ms  10.478 ms  10.680 ms
 8  72.14.204.62 (72.14.204.62)  12.435 ms * *
 9  * * *
10  142.250.208.220 (142.250.208.220)  15.658 ms
    192.178.86.200 (192.178.86.200)  13.410 ms
    192.178.86.238 (192.178.86.238)  28.823 ms
11  216.239.58.19 (216.239.58.19)  14.157 ms  14.006 ms  13.795 ms
12  192.178.110.249 (192.178.110.249)  20.508 ms
    142.250.208.227 (142.250.208.227)  12.942 ms
    192.178.110.249 (192.178.110.249)  20.495 ms
13  216.239.58.19 (216.239.58.19)  13.728 ms  13.673 ms
    142.250.228.47 (142.250.228.47)  28.793 ms
14  bom07s24-in-f4.1e100.net (142.250.67.228)  12.545 ms  12.545 ms  12.019 ms
```

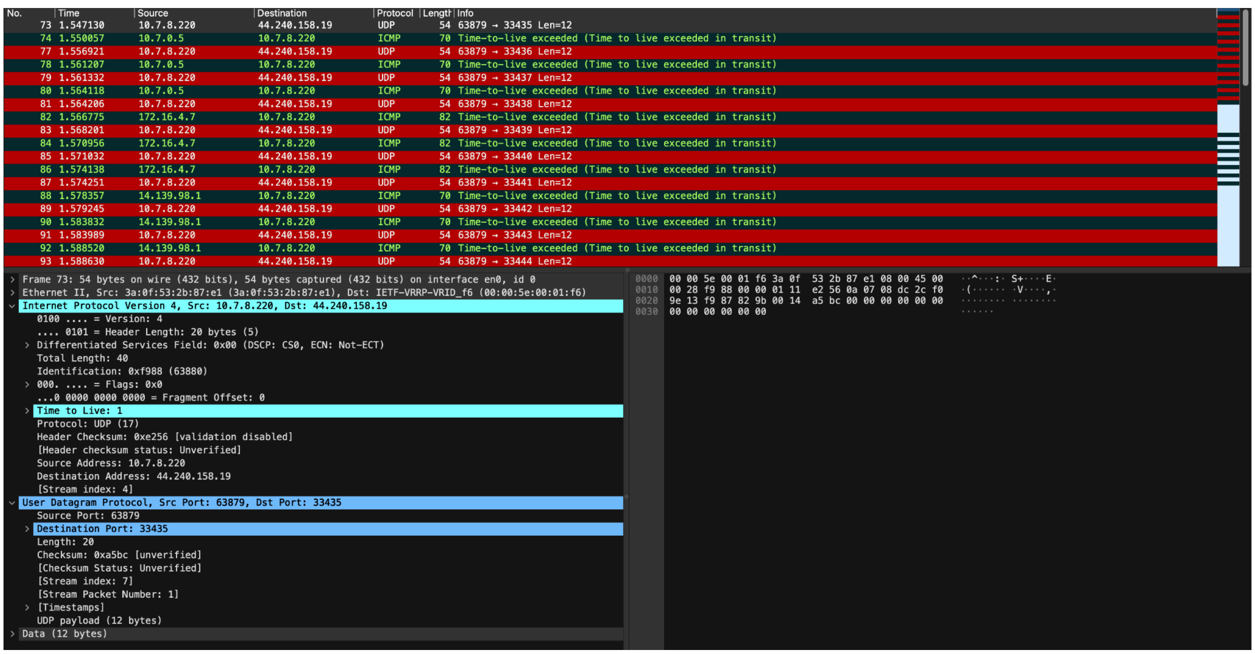
```
jayaram@JAYARAMs-MacBook-Air CN1 % traceroute www.apple.com
traceroute to e6858.dsce9.akamaiedge.net (23.32.176.246), 64 hops max, 40 byte packets
 1  10.7.0.5 (10.7.0.5)  4.887 ms  3.258 ms  2.930 ms
 2  172.16.4.7 (172.16.4.7)  2.111 ms  2.544 ms  4.443 ms
 3  14.139.98.1 (14.139.98.1)  5.252 ms  5.870 ms  4.524 ms
 4  10.117.81.253 (10.117.81.253)  5.204 ms  3.964 ms  3.098 ms
 5  * * *
 6  * * *
 7  * * *
 8  10.119.234.162 (10.119.234.162)  21.835 ms  19.259 ms  18.141 ms
 9  * * *
10  * * *
11  * * *
```

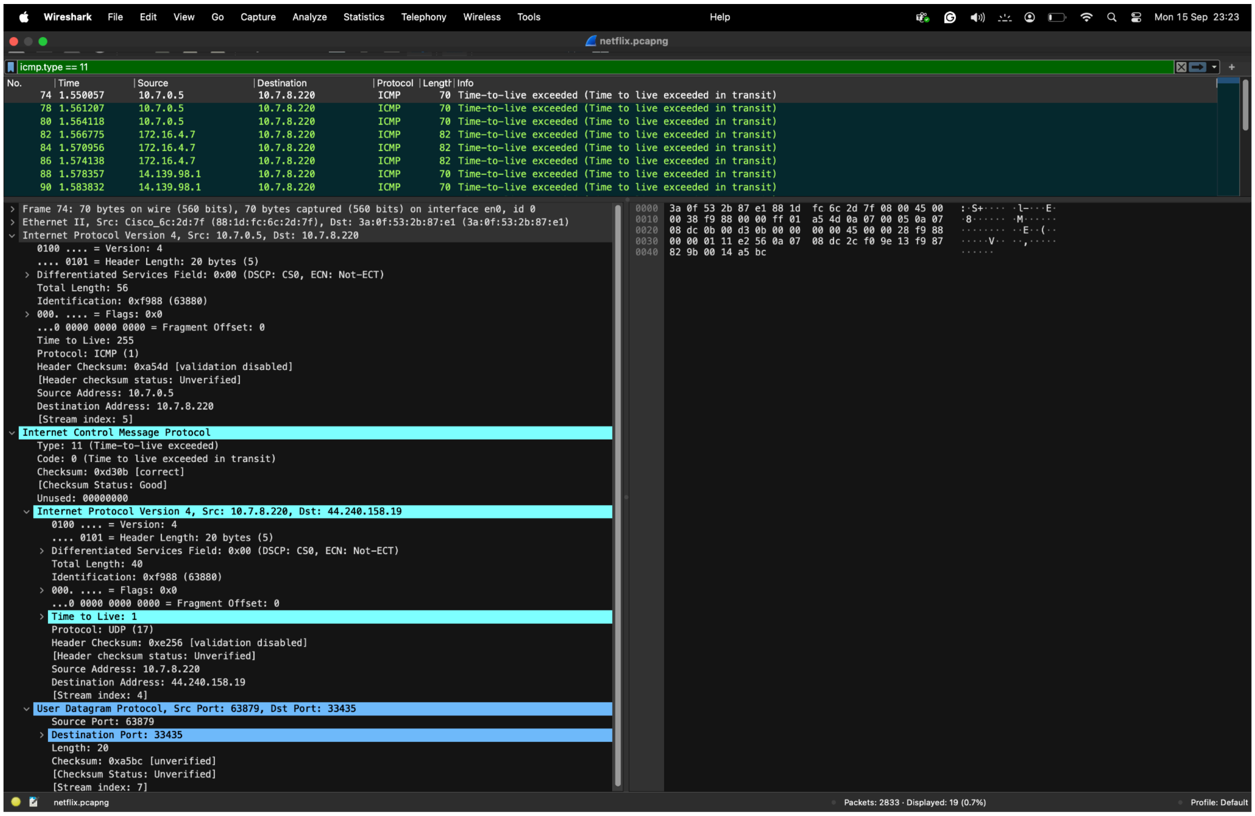
```
jayaram@JAYARAMs-MacBook-Air CN1 % traceroute www.netflix.com
traceroute: Warning: www.netflix.com has multiple addresses; using 44.240.158.19
traceroute to apiproxy-website-nlb-prod-1-bcf28d21f4bbcf2c.elb.us-west-2.amazonaws.com (44.240.158.19), 64 hops max, 40 byte packets
 1  10.7.0.5 (10.7.0.5)  3.440 ms  4.420 ms  2.864 ms
 2  172.16.4.7 (172.16.4.7)  2.700 ms  2.818 ms  3.204 ms
 3  14.139.98.1 (14.139.98.1)  4.197 ms  4.726 ms  4.638 ms
 4  10.117.81.253 (10.117.81.253)  3.152 ms  2.645 ms  3.110 ms
 5  * * *
 6  * * *
 7  10.255.222.33 (10.255.222.33)  31.111 ms  25.559 ms
    10.255.221.33 (10.255.221.33)  30.313 ms
 8  dsl-tn-085.99.246.61.airtelbroadband.in (61.246.99.85)  54.058 ms  45.156 ms  45.862 ms
 9  116.119.57.43 (116.119.57.43)  267.346 ms * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
```



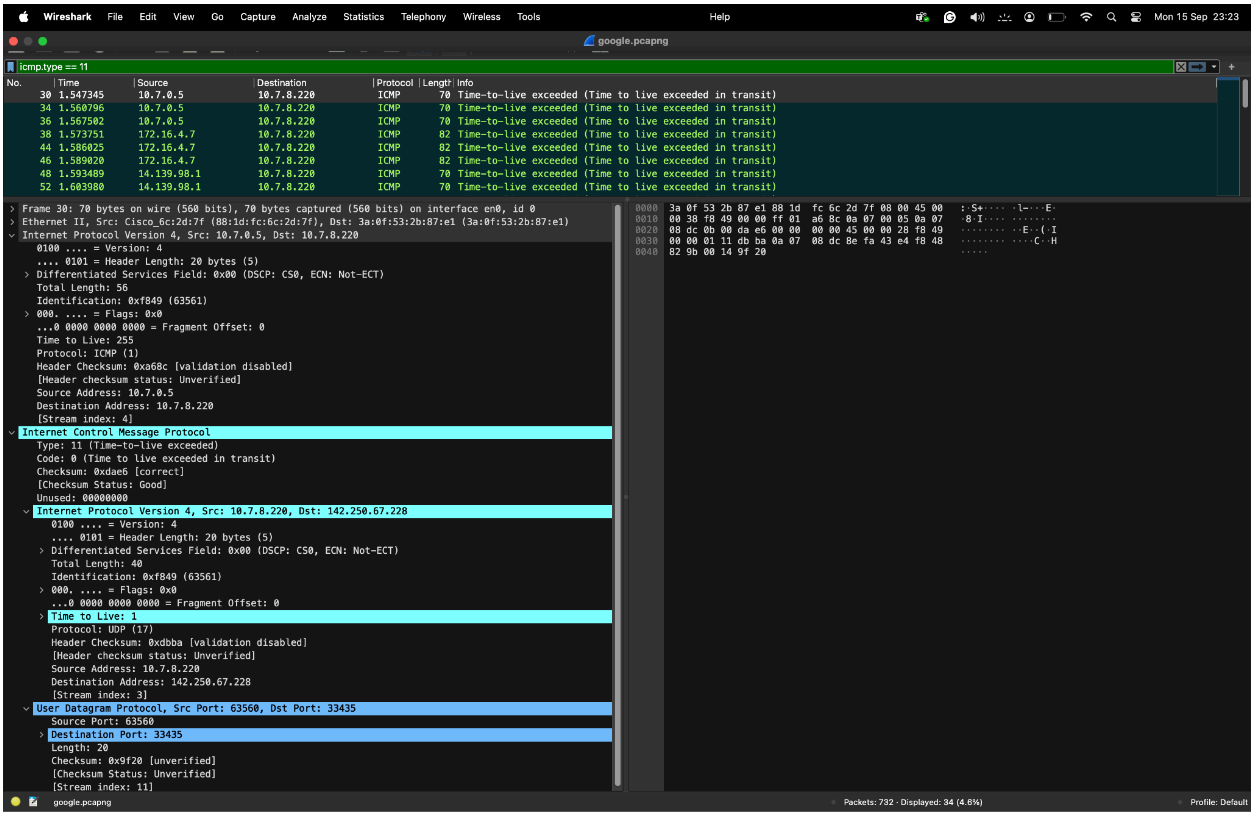
No. Time Source Destination Protocol Length Info
29 1.544081 10.7.8.220 142.250.67.228 UDP 54 63560 → 33435 Len=12
30 1.547345 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
33 1.555689 10.7.8.220 142.250.67.228 UDP 54 63560 → 33436 Len=12
34 1.560796 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
35 1.561008 10.7.8.220 142.250.67.228 UDP 54 63560 → 33437 Len=12
36 1.567502 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
37 1.567742 10.7.8.220 142.250.67.228 UDP 54 63560 → 33438 Len=12
38 1.573751 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
43 1.580209 10.7.8.220 142.250.67.228 UDP 54 63560 → 33439 Len=12
44 1.586025 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
45 1.586236 10.7.8.220 142.250.67.228 UDP 54 63560 → 33440 Len=12
46 1.589020 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
47 1.589180 10.7.8.220 142.250.67.228 UDP 54 63560 → 33441 Len=12
48 1.593489 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
51 1.599272 10.7.8.220 142.250.67.228 UDP 54 63560 → 33442 Len=12
52 1.603980 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
53 1.604140 10.7.8.220 142.250.67.228 UDP 54 63560 → 33443 Len=12
54 1.609382 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
55 1.609525 10.7.8.220 142.250.67.228 UDP 54 63560 → 33444 Len=12
Frame 29: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 142.250.67.228
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf849 (63561)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xdbba [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 142.250.67.228
[Stream index: 3]
User Datagram Protocol, Src Port: 63560, Dst Port: 33435
Source Port: 63560
Destination Port: 33435
Length: 20
Checksum: 0x9f20 [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (12 bytes)
Data (12 bytes)
0000 00 00 5e 00 01 f6 3a 0f 53 2b 87 e1 08 00 45 00
0010 00 28 f8 49 00 00 01 11 db ba 0a 07 08 dc 8e fa
0020 43 e4 f8 48 82 9b 00 14 9f 20 00 00 00 00 00 00
0030 00 00 00 00 00 00


No. Time Source Destination Protocol Length Info
10 0.953515 10.7.8.220 23.32.176.246 UDP 54 63799 → 33435 Len=12
11 0.957959 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
14 0.975464 10.7.8.220 23.32.176.246 UDP 54 63799 → 33436 Len=12
15 0.978583 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
16 0.978741 10.7.8.220 23.32.176.246 UDP 54 63799 → 33437 Len=12
17 0.981597 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
18 0.981672 10.7.8.220 23.32.176.246 UDP 54 63799 → 33438 Len=12
19 0.983721 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
20 0.984473 10.7.8.220 23.32.176.246 UDP 54 63799 → 33439 Len=12
21 0.986913 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
22 0.987042 10.7.8.220 23.32.176.246 UDP 54 63799 → 33440 Len=12
23 0.991360 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
24 0.991498 10.7.8.220 23.32.176.246 UDP 54 63799 → 33441 Len=12
25 0.996652 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
26 0.997553 10.7.8.220 23.32.176.246 UDP 54 63799 → 33442 Len=12
27 1.003324 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
28 1.003450 10.7.8.220 23.32.176.246 UDP 54 63799 → 33443 Len=12
29 1.007845 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
30 1.007989 10.7.8.220 23.32.176.246 UDP 54 63799 → 33444 Len=12
Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 23.32.176.246
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf938 (63800)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xe593 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 23.32.176.246
[Stream index: 2]
User Datagram Protocol, Src Port: 63799, Dst Port: 33435
Source Port: 63799
Destination Port: 33435
Length: 20
Checksum: 0xa8f9 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (12 bytes)
Data (12 bytes)
0000 00 00 5e 00 01 f6 3a 0f 53 2b 87 e1 08 00 45 00
0010 00 28 f9 38 00 00 01 11 e5 93 0a 07 08 dc 17 20
0020 b0 f6 f9 37 82 9b 00 14 a8 f9 00 00 00 00 00 00
0030 00 00 00 00 00 00

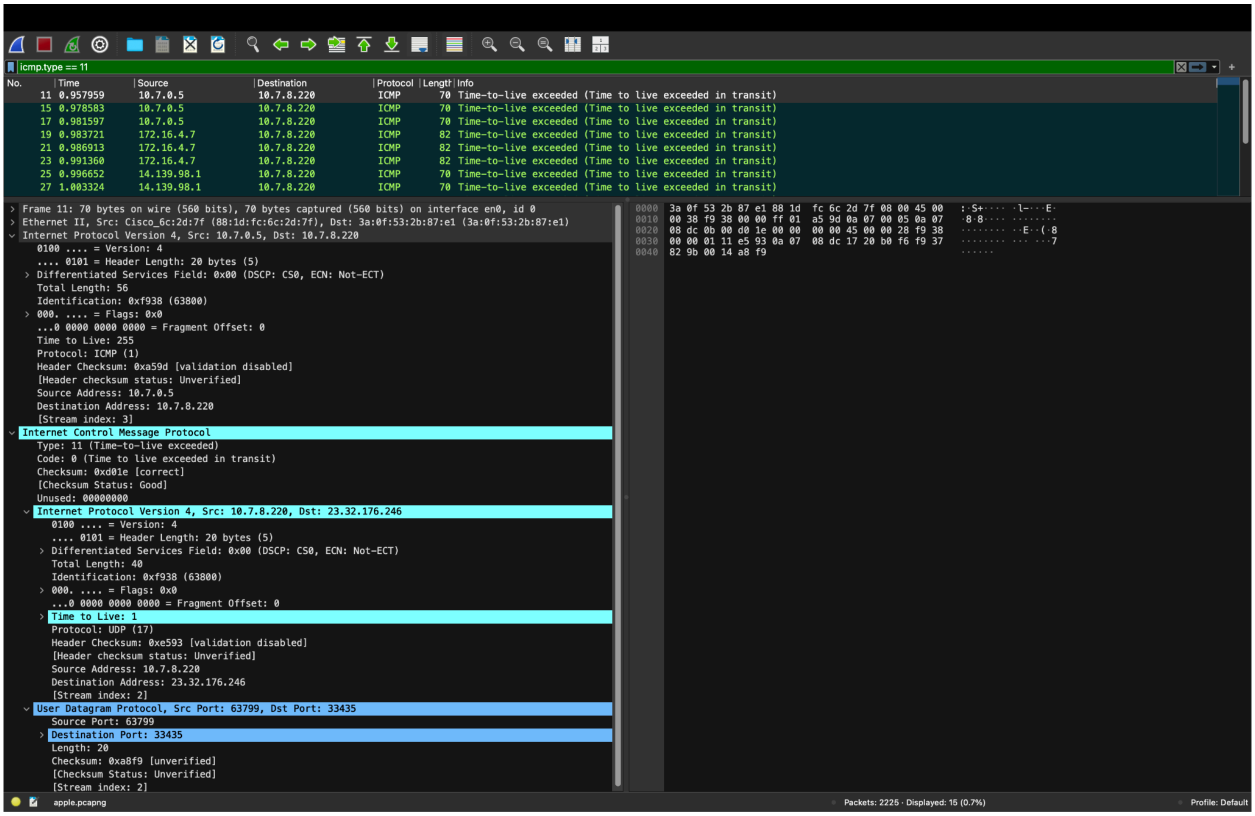

No. Time Source Destination Protocol Length Info
73 1.547130 10.7.8.220 44.240.158.19 UDP 54 63879 → 33435 Len=12
74 1.550057 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
77 1.556921 10.7.8.220 44.240.158.19 UDP 54 63879 → 33436 Len=12
78 1.561207 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
79 1.561332 10.7.8.220 44.240.158.19 UDP 54 63879 → 33437 Len=12
80 1.564118 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
81 1.564206 10.7.8.220 44.240.158.19 UDP 54 63879 → 33438 Len=12
82 1.566775 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
83 1.568201 10.7.8.220 44.240.158.19 UDP 54 63879 → 33439 Len=12
84 1.570956 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
85 1.571032 10.7.8.220 44.240.158.19 UDP 54 63879 → 33440 Len=12
86 1.574138 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
87 1.574251 10.7.8.220 44.240.158.19 UDP 54 63879 → 33441 Len=12
88 1.578357 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
89 1.579245 10.7.8.220 44.240.158.19 UDP 54 63879 → 33442 Len=12
90 1.583832 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
91 1.583989 10.7.8.220 44.240.158.19 UDP 54 63879 → 33443 Len=12
92 1.588520 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
93 1.588630 10.7.8.220 44.240.158.19 UDP 54 63879 → 33444 Len=12
Frame 73: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1), Dst: IETF-VRRP-VRID_f6 (00:00:5e:00:01:f6)
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 44.240.158.19
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf988 (63880)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xe256 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 44.240.158.19
[Stream index: 4]
User Datagram Protocol, Src Port: 63879, Dst Port: 33435
Source Port: 63879
Destination Port: 33435
Length: 20
Checksum: 0xa5bc [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (12 bytes)
Data (12 bytes)
0000 00 00 5e 00 01 f6 3a 0f 53 2b 87 e1 08 00 45 00
0010 00 28 f9 88 00 00 01 11 e2 56 0a 07 08 dc 2c f0
0020 9e 13 f9 87 82 9b 00 14 a5 bc 00 00 00 00 00 00
0030 00 00 00 00 00 00

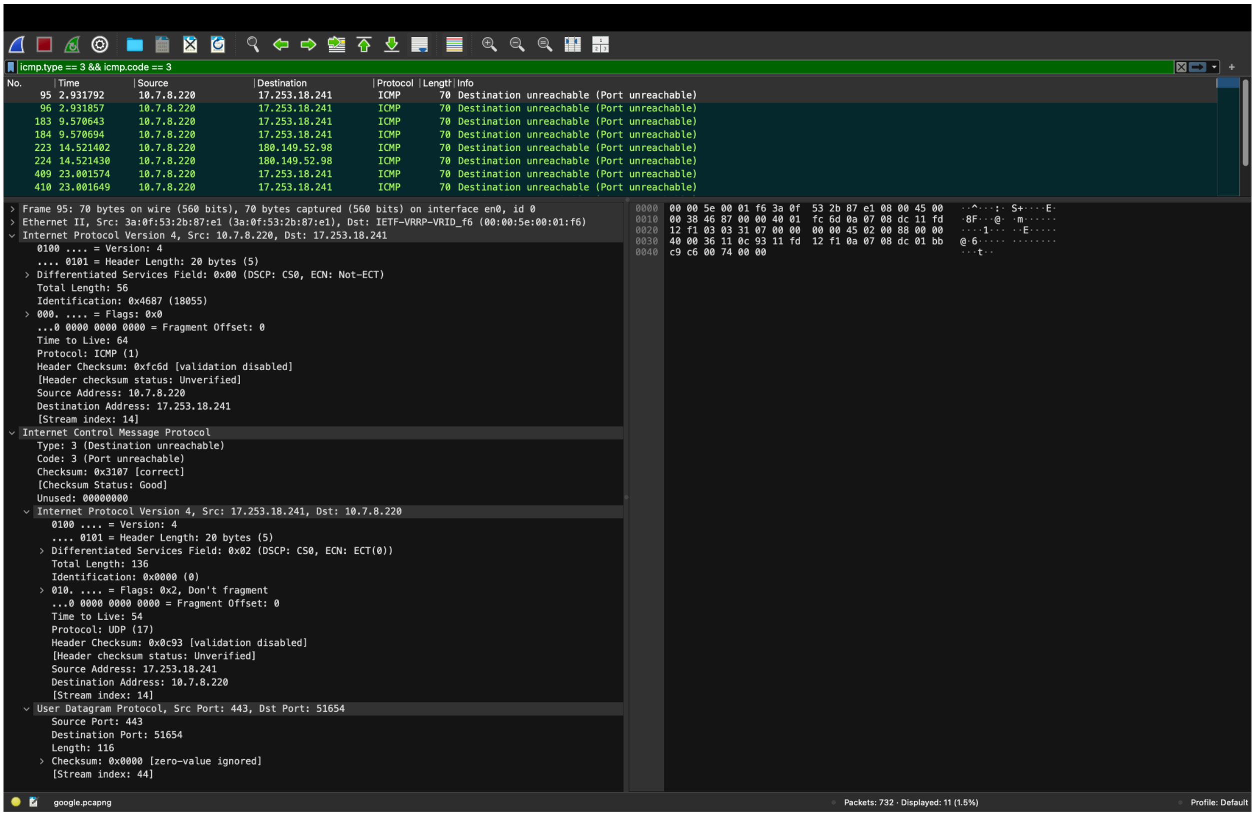


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mon 15 Sep 23:23
netflix.pcapng
icmp.type == 11
No. Time Source Destination Protocol Length Info
74 1.550057 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
78 1.561207 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
80 1.564118 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
82 1.566775 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
84 1.570956 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
86 1.574138 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
88 1.578357 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
90 1.583832 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 74: 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: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1)
Internet Protocol Version 4, Src: 10.7.0.5, Dst: 10.7.8.220
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0xf988 (63880)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xa54d [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.0.5
Destination Address: 10.7.8.220
[Stream index: 5]
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd30b [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 44.240.158.19
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf988 (63880)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xe256 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 44.240.158.19
[Stream index: 4]
User Datagram Protocol, Src Port: 63879, Dst Port: 33435
Source Port: 63879
Destination Port: 33435
Length: 20
Checksum: 0xa5bc [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
0000 3a 0f 53 2b 87 e1 88 1d fc 6c 2d 7f 08 00 45 00
0010 00 38 f9 88 00 00 ff 01 a5 4d 0a 07 00 05 0a 07
0020 08 dc 0b 00 d3 0b 00 00 00 00 45 00 00 28 f9 88
0030 00 00 01 11 e2 56 0a 07 08 dc 2c f0 9e 13 f9 87
0040 82 9b 00 14 a5 bc
netflix.pcapng
Packets: 2833 · Displayed: 19 (0.7%)
Profile: Default



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mon 15 Sep 23:23
google.pcapng
icmp.type == 11
No. Time Source Destination Protocol Length Info
30 1.547345 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
34 1.560796 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
36 1.567502 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
38 1.573751 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
44 1.586025 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
46 1.589020 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
48 1.593489 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
52 1.603980 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 30: 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: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1)
Internet Protocol Version 4, Src: 10.7.0.5, Dst: 10.7.8.220
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0xf849 (63561)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xa68c [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.0.5
Destination Address: 10.7.8.220
[Stream index: 4]
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xdae6 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 142.250.67.228
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf849 (63561)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xdbba [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 142.250.67.228
[Stream index: 3]
User Datagram Protocol, Src Port: 63560, Dst Port: 33435
Source Port: 63560
Destination Port: 33435
Length: 20
Checksum: 0x9f20 [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
0000 3a 0f 53 2b 87 e1 88 1d fc 6c 2d 7f 08 00 45 00
0010 00 38 f8 49 00 00 ff 01 a6 8c 0a 07 00 05 0a 07
0020 08 dc 0b 00 da e6 00 00 00 00 45 00 00 28 f8 49
0030 00 00 01 11 db ba 0a 07 08 dc 8e fa 43 e4 f8 48
0040 82 9b 00 14 9f 20
google.pcapng
Packets: 732 · Displayed: 34 (4.6%)
Profile: Default


icmp.type == 11
No. Time Source Destination Protocol Length Info
11 0.957959 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
15 0.978583 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
17 0.981597 10.7.0.5 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
19 0.983721 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
21 0.986913 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
23 0.991360 172.16.4.7 10.7.8.220 ICMP 82 Time-to-live exceeded (Time to live exceeded in transit)
25 0.996652 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
27 1.003324 14.139.98.1 10.7.8.220 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 11: 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: 3a:0f:53:2b:87:e1 (3a:0f:53:2b:87:e1)
Internet Protocol Version 4, Src: 10.7.0.5, Dst: 10.7.8.220
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0xf938 (63800)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xa59d [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.0.5
Destination Address: 10.7.8.220
[Stream index: 3]
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd01e [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 10.7.8.220, Dst: 23.32.176.246
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf938 (63800)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xe593 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.7.8.220
Destination Address: 23.32.176.246
[Stream index: 2]
User Datagram Protocol, Src Port: 63799, Dst Port: 33435
Source Port: 63799
Destination Port: 33435
Length: 20
Checksum: 0xa8f9 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
0000 3a 0f 53 2b 87 e1 88 1d fc 6c 2d 7f 08 00 45 00
0010 00 38 f9 38 00 00 ff 01 a5 9d 0a 07 00 05 0a 07
0020 08 dc 0b 00 d0 1e 00 00 00 00 45 00 00 28 f9 38
0030 00 00 01 11 e5 93 0a 07 08 dc 17 20 b0 f6 f9 37
0040 82 9b 00 14 a8 f9
apple.pcapng
Packets: 2225 · Displayed: 15 (0.7%)
Profile: Default



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

On my Mac, running traceroute used UDP packets by default to trace the path to the destination. Windows tracert normally uses ICMP packets, but I only performed the experiment on Mac.

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

Sometimes, traceroute shows *** for certain hops. This can happen because:

- The router at that hop is configured **not to reply** to traceroute packets.
- There is **network congestion or packet loss** causing the probe to be dropped.

3. In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?
In Mac/Linux traceroute, the **UDP destination port number** changes for each probe sent to the destination. This helps distinguish between the responses of successive probes.

4. At the final hop, how is the response different compared to the intermediate hop?
Intermediate hops: Respond with **TTL expired** messages to indicate the packet was dropped.

Final hop: Responds with a **port unreachable** message (because the UDP port is closed), confirming that the destination host has been reached.

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 packets but allows ICMP:

- Mac/Linux traceroute (which uses UDP) may fail to receive replies at some hops, showing ***.
- Windows tracert (which uses ICMP) would still work normally because ICMP is allowed.