Samarth Sonawane 23110317
Chardiya Vanshribahen Rajeshbhai 23110074

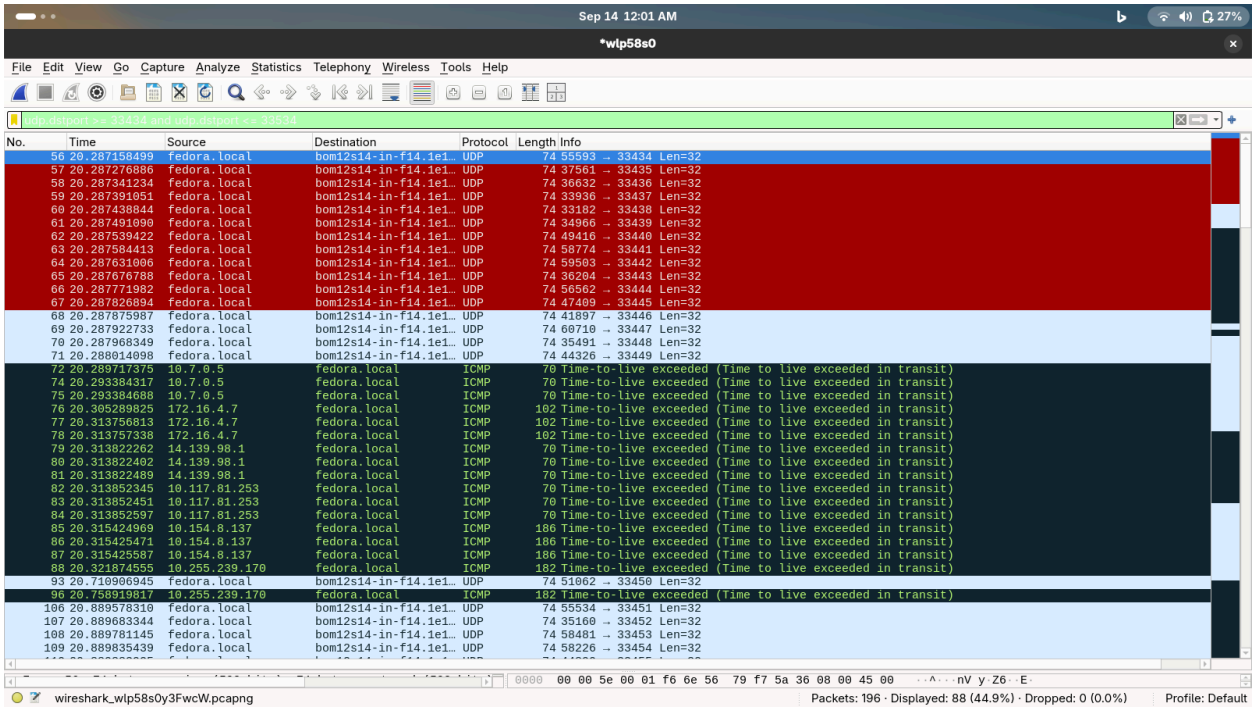
Task-1

Header Value	Domain Name	Resolved IP address
15451600	_apple-mobdev._tcp.local.	192.168.1.6
15451601	_apple-mobdev._tcp.local.	192.168.1.7
15451602	facebook.com.	192.168.1.8
15451603	stackoverflow.com.	192.168.1.9
15451604	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
15451605	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.6
15451606	example.com.	192.168.1.7
15451607	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8
15451608	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.9
15451609	linkedin.com.	192.168.1.10
15451610	_apple-mobdev._tcp.local.	192.168.1.6
15451611	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.7
15451612	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8
15451613	apple.com.	192.168.1.9
15451614	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
15451615	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.6

15451616	_apple-mobdev._tcp.local.	192.168.1.7
15451617	_apple-mobdev._tcp.local.	192.168.1.8
15451618	google.com.	192.168.1.9
15451619	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.10
15451620	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.6
15451621	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.7
15451622	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.8

Task-2

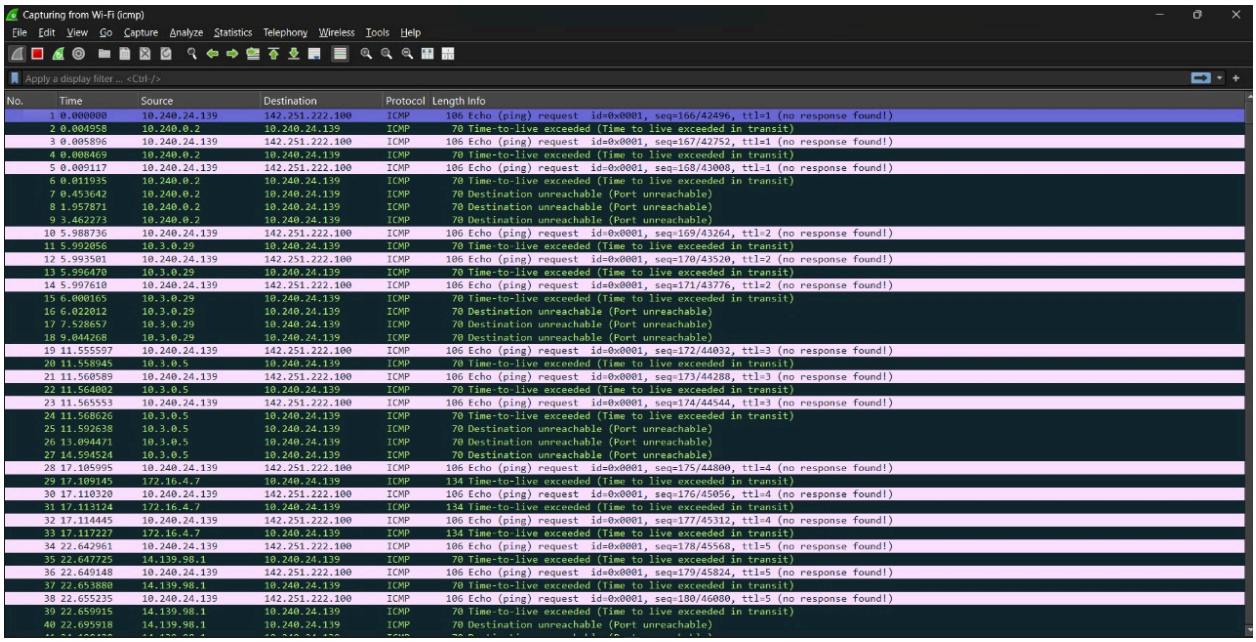
WireShark Capture of Linux for www.youtube.com



traceroute www.youtube.com

```
samarth@fedora:~/Desktop$ traceroute www.youtube.com
traceroute to www.youtube.com (142.250.192.14), 30 hops max, 60 byte packets
 1  10.7.0.5 (10.7.0.5)  2.616 ms  6.135 ms  6.059 ms
 2  172.16.4.7 (172.16.4.7)  17.912 ms  26.332 ms  26.282 ms
 3  14.139.98.1 (14.139.98.1)  26.297 ms  26.252 ms  26.205 ms
 4  10.117.81.253 (10.117.81.253)  26.190 ms  26.101 ms  26.041 ms
 5  10.154.8.137 (10.154.8.137)  27.564 ms  27.517 ms  27.470 ms
 6  10.255.239.170 (10.255.239.170)  33.874 ms  48.078 ms  13.963 ms
 7  10.152.7.214 (10.152.7.214)  13.828 ms  13.728 ms  13.668 ms
 8  72.14.204.62 (72.14.204.62)  13.614 ms *  15.180 ms
 9  * * *
10  142.250.214.110 (142.250.214.110)  15.008 ms 142.250.60.134 (142.250.60.134)  21.781 ms 142.250.238.196 (142.250.238.196)  19.119 ms
11  142.250.209.70 (142.250.209.70)  26.836 ms 192.178.110.248 (192.178.110.248)  26.739 ms 108.170.231.79 (108.170.231.79)  18.923 ms
12  192.178.110.105 (192.178.110.105)  37.467 ms bom12s14-in-f14.1e100.net (142.250.192.14)  37.355 ms  37.290 ms
samarth@fedora:~/Desktop$
```

Wireshark capture for www.google.com



tracert for www.google.com

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

Tracing route to www.google.com [142.251.222.100]
over a maximum of 30 hops:

  1     5 ms     2 ms     2 ms  10.240.0.2
  2     3 ms     3 ms     2 ms  10.3.0.29
  3     3 ms     3 ms     3 ms  10.3.0.5
  4     3 ms     3 ms     3 ms  172.16.4.7
  5     4 ms     5 ms     5 ms  14.139.98.1
  6    36 ms     3 ms     5 ms  10.117.81.253
  7    26 ms    21 ms    13 ms  10.154.8.137
  8    13 ms    10 ms    11 ms  10.255.239.170
  9    12 ms    10 ms    16 ms  10.152.7.214
 10    13 ms    14 ms    13 ms  142.250.172.80
 11    16 ms    12 ms    12 ms  142.251.76.23
 12    14 ms    13 ms    22 ms  142.251.77.97
 13    12 ms    12 ms    13 ms  pnbomb-az-in-f4.1e100.net [142.251.222.100]

Trace complete.
```

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

Ans:

Windows use ICMP to request and also gets response on ICMP.

Linux use UDP to request and gets response on ICMP.

To get these packages in wireshark on Windows we used the ICMP protocol filter, while on Linux we used udp.dstport >= 33434 and udp.dstport <= 33534, as linux traceroute uses UDP destination ports starting from 33434.

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

Ans:

`* * *` means no response was received from that hop within the timeout. In our attached screenshot, the messages that we are getting `Time-to-Live exceeded` or `Port unreachable` are explicit ICMP responses that traceroute receives showing hop is reachable.

There are two common reasons of getting ***:

1) ICMP time limit exceeded response are blocked
2) Firewall or filtering policies.(security policies that might block certain port numbers)

In some places we also got one start e.g.

```
10  72.14.204.62 (72.14.204.62)  43.283 ms *  43.165 ms
```

This shows that out of three packets sent only one didn't responded. In linux traceroute this process is repeated three times. Three stars means, three times packets were sent but no response was received.

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

Ans.

Between the successive packets, we observed that the UDP destination ports were changing, it started with 33434 and went upto 33481. When the packet reaches the destination port or the router in its way it sends back a ICMP packet, which contains the header of the sent packet. So changing the port with each packets helps the source to match with it with its response.

`traceroute` command repeats this procedure 3 times so the source actually sends 3 N packets to the destination.

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

Ans.

At intermediate hop response:

Protocol : ICMP

Info : Time-to-live exceeded (Time to live exceeded in transit)

At Destination response:

Protocol : ICMP

Info : Destination Unreachable (Port Unreachable)

The destination doesn't listen to such high-numbered UDP port. So it responds with the destination unreachable message. In this way user can identify that the destination is reached.

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

Ans.

As said above, the Linux traceroute works with the UDP packets for the requests. If the firewall blocks UDP then we will mostly see the `***` response in the output of traceroute command. But windows use tracert command which by default uses ICMP packets. They are not blocked by the firewall so we will see the normal output by tracert command.