

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

No.	Time	Source	Destination	Protocol	Length	Info
56	20.287158499	fedora.local	bom12s14-in-f14.1e1...	UDP	74	55593 → 33434 Len=32
57	20.287276886	fedora.local	bom12s14-in-f14.1e1...	UDP	74	37661 → 33435 Len=32
58	20.287343234	fedora.local	bom12s14-in-f14.1e1...	UDP	74	36632 → 33436 Len=32
59	20.287391051	fedora.local	bom12s14-in-f14.1e1...	UDP	74	33936 → 33437 Len=32
60	20.287438844	fedora.local	bom12s14-in-f14.1e1...	UDP	74	33182 → 33438 Len=32
61	20.287491090	fedora.local	bom12s14-in-f14.1e1...	UDP	74	34966 → 33439 Len=32
62	20.287539422	fedora.local	bom12s14-in-f14.1e1...	UDP	74	49416 → 33440 Len=32
63	20.287584113	fedora.local	bom12s14-in-f14.1e1...	UDP	74	58774 → 33441 Len=32
64	20.287631066	fedora.local	bom12s14-in-f14.1e1...	UDP	74	59903 → 33442 Len=32
65	20.287676788	fedora.local	bom12s14-in-f14.1e1...	UDP	74	36294 → 33443 Len=32
66	20.287771982	fedora.local	bom12s14-in-f14.1e1...	UDP	74	56562 → 33444 Len=32
67	20.287826894	fedora.local	bom12s14-in-f14.1e1...	UDP	74	47409 → 33445 Len=32
68	20.287875987	fedora.local	bom12s14-in-f14.1e1...	UDP	74	41897 → 33446 Len=32
69	20.287922733	fedora.local	bom12s14-in-f14.1e1...	UDP	74	60710 → 33447 Len=32
70	20.287968349	fedora.local	bom12s14-in-f14.1e1...	UDP	74	35491 → 33448 Len=32
71	20.288014998	fedora.local	bom12s14-in-f14.1e1...	UDP	74	44326 → 33449 Len=32
72	20.289717375	10.7.0.5	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
74	20.293384317	10.7.0.5	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
75	20.293384688	10.7.0.5	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
76	20.305269825	172.16.4.7	fedora.local	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
77	20.313758813	172.16.4.7	fedora.local	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
78	20.313757338	172.16.4.7	fedora.local	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
79	20.313822262	14.139.98.1	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
80	20.313822402	14.139.98.1	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	20.313822489	14.139.98.1	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
82	20.313852345	10.117.81.253	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
83	20.313852451	10.117.81.253	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
84	20.313852597	10.117.81.253	fedora.local	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	20.315424969	10.154.8.137	fedora.local	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
86	20.315425471	10.154.8.137	fedora.local	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
87	20.315425587	10.154.8.137	fedora.local	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
88	20.321074555	10.255.239.170	fedora.local	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
93	20.710906945	fedora.local	bom12s14-in-f14.1e1...	UDP	74	51862 → 33450 Len=32
96	20.758919817	10.255.239.170	fedora.local	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
106	20.889578310	fedora.local	bom12s14-in-f14.1e1...	UDP	74	55534 → 33451 Len=32
107	20.889683344	fedora.local	bom12s14-in-f14.1e1...	UDP	74	35160 → 33452 Len=32
108	20.889781145	fedora.local	bom12s14-in-f14.1e1...	UDP	74	58481 → 33453 Len=32
109	20.889835439	fedora.local	bom12s14-in-f14.1e1...	UDP	74	58226 → 33454 Len=32

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 48.876 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) 21.791 ms 142.250.238.196 (142.250.238.196) 19.119 ms
11 142.250.209.70 (142.250.209.70) 26.836 ms 192.170.110.248 (192.170.110.248) 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

Capturing from Wi-Fi (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Cmd-/->

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=166/42496, ttl=1 (no response found!)
2	0.004558	10.240.0.2	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	0.005896	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=167/42752, ttl=1 (no response found!)
4	0.008665	10.240.0.2	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.009117	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=168/43008, ttl=1 (no response found!)
6	0.011935	10.240.0.2	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	0.453642	10.240.0.2	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
8	1.957871	10.240.0.2	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
9	1.452273	10.240.0.2	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
10	9.908735	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=169/43264, ttl=2 (no response found!)
11	9.992856	10.3.0.29	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	9.993501	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=170/43520, ttl=2 (no response found!)
13	9.996470	10.3.0.29	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	9.997610	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=171/43776, ttl=2 (no response found!)
15	0.000165	10.3.0.29	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	0.002012	10.3.0.29	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
17	7.528657	10.3.0.29	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
18	9.044268	10.3.0.29	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
19	11.555597	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=172/44032, ttl=3 (no response found!)
20	11.558925	10.3.0.5	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	11.560589	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=173/44288, ttl=3 (no response found!)
22	11.564092	10.3.0.5	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	11.565553	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=174/44544, ttl=3 (no response found!)
24	11.568626	10.3.0.5	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	11.592638	10.3.0.5	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
26	13.094471	10.3.0.5	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
27	14.594524	10.3.0.5	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)
28	17.105995	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=175/44800, ttl=4 (no response found!)
29	17.109145	172.16.4.7	10.240.24.139	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
30	17.110320	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=176/45056, ttl=4 (no response found!)
31	17.111324	172.16.4.7	10.240.24.139	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
32	17.114445	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=177/45312, ttl=4 (no response found!)
33	17.117227	172.16.4.7	10.240.24.139	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
34	22.642961	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=178/45568, ttl=5 (no response found!)
35	22.647725	14.139.98.1	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
36	22.649148	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=179/45824, ttl=5 (no response found!)
37	22.653006	14.139.98.1	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
38	22.655235	10.240.24.139	142.251.222.100	ICMP	106	Echo (ping) request id=0x0001, seq=180/46080, ttl=5 (no response found!)
39	22.659915	14.139.98.1	10.240.24.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	22.695918	14.139.98.1	10.240.24.139	ICMP	70	Destination unreachable (Port unreachable)

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 star 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 respond. 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 up to 33481. When the packet reaches the destination port or the router in its way it sends back an ICMP packet, which contains the header of the sent packet. So changing the port with each packet helps the source to match 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.