Task-1: Capture traceroute traffic to/from one of four websites visited as part of Lab-1 using wireshark and answer the following a google doc. Feel free to include screenshots from terminal/wireshark to support your answers. [**7 Marks]**

1. What protocol is used to send probe packets? Identity key fields and comment on their values.

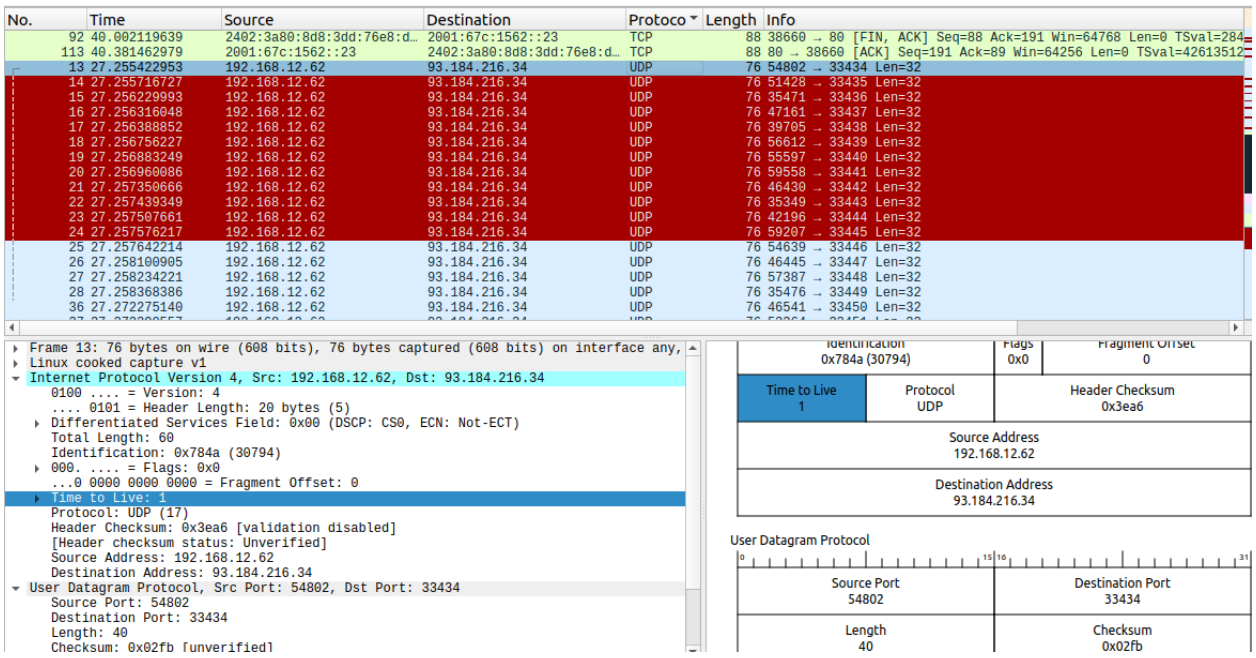
The protocol is used to send probe packets (for example.com) is UDP

Here we are going to use example.com

```
root@RajPopat:/home/raj/Desktop# traceroute example.com
traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets
 1  _gateway (192.168.12.184)  3.348 ms  3.052 ms  5.545 ms
 2  * * *
 3  * * *
 4  100.64.0.125 (100.64.0.125)  269.512 ms  269.443 ms  269.374 ms
 5  182.19.106.113 (182.19.106.113)  269.309 ms  268.857 ms  268.728 ms
 6  xe-8-3-2.mlu.cw.net (195.89.101.185)  268.591 ms  254.690 ms  340.572 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  62.115.175.71 (62.115.175.71)  290.510 ms limelight-ic-315152.ip.twelve99-cu
st.net (213.248.83.119)  304.116 ms 62.115.175.71 (62.115.175.71)  293.678 ms
12  ae-65.core1.dcb.edgecastcdn.net (152.195.64.129)  305.998 ms  305.653 ms  31
1.296 ms
13  93.184.216.34 (93.184.216.34)  356.596 ms  369.782 ms  369.595 ms
14  93.184.216.34 (93.184.216.34)  369.325 ms  369.218 ms  369.141 ms
```

```
    5 27.243451843    127.0.0.1        127.0.0.53       DNS      84 Standard query 0x5ae4 A example.com OPT
    6 27.244026168    192.168.12.62    192.168.12.184   DNS      73 Standard query 0x4268 A example.com
    7 27.244659012    127.0.0.1        127.0.0.53       DNS      84 Standard query 0x0eff AAAA example.com OPT
    8 27.245096942    192.168.12.62    192.168.12.184   DNS      73 Standard query 0xe0d0 AAAA example.com
    9 27.250071153    192.168.12.184   192.168.12.62    DNS      89 Standard query response 0x4268 A example.com A 93.184.216.34
   10 27.250714041    127.0.0.53       127.0.0.1        DNS     100 Standard query response 0x5ae4 A example.com A 93.184.216.34 (
```

First we got ip address of example.com 93.184.216.34 through DNS server



Here we can see UDP protocol is used,

Here we can see that for each hop three probe packets are sent and each of these probes the time to leave is the same.

Here we can see key fields are :

Time to live: 1

Header Checksum

Source address

Destination address

Source port

Destination port

Length

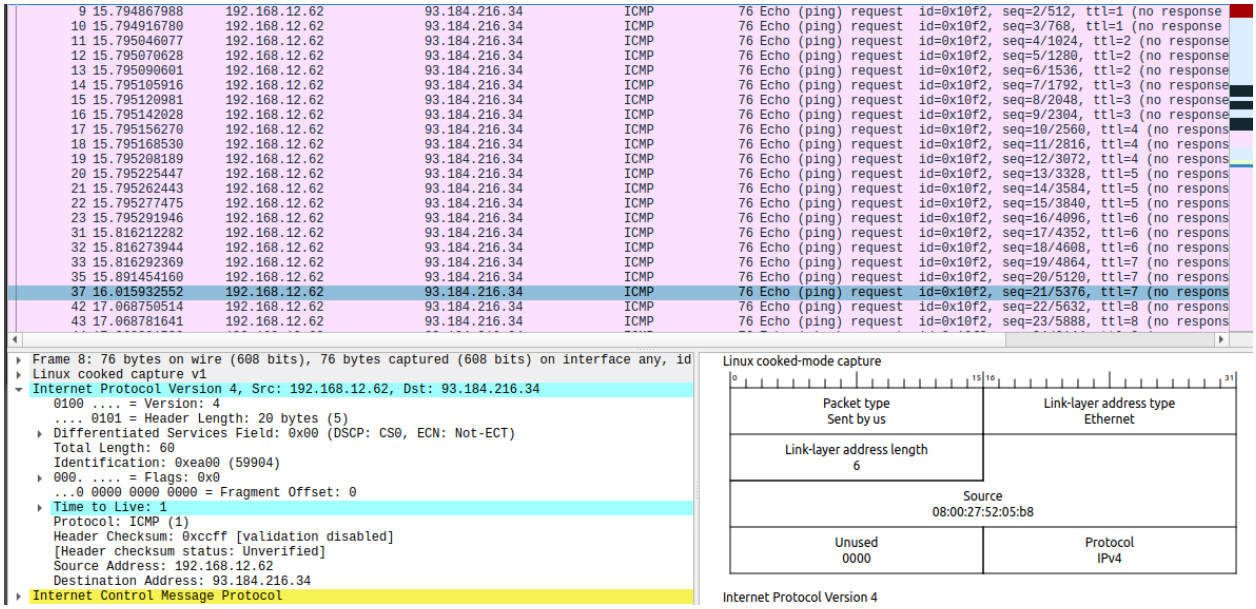
Checksum

2. Can you change the default protocol used to send probes? Demonstrate it.

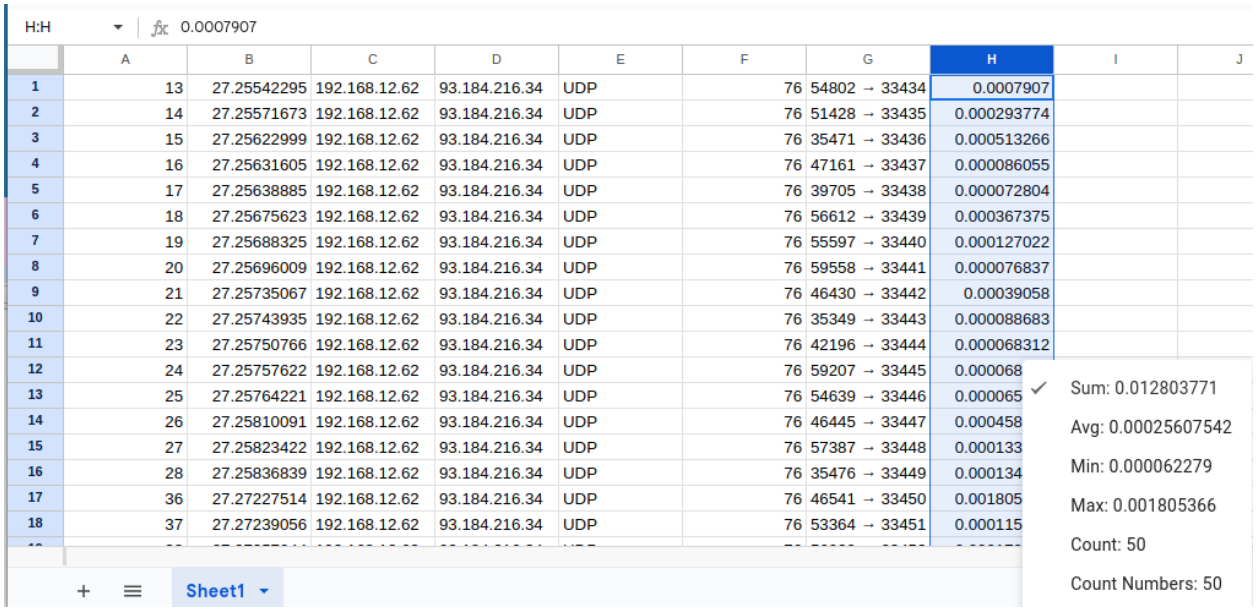
   Yes, we can change the default protocol used to send probes

   Here we are using: taceroute example.com -I to send ICMP packets

```
root@RajPopat:/home/raj/Desktop# traceroute example.com -I
traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets
 1  _gateway (192.168.12.184)  3.803 ms  7.831 ms  7.788 ms
 2  * * *
 3  * * *
 4  100.64.0.125 (100.64.0.125)  96.120 ms * *
 5  * * *
 6  xe-8-3-2.mlu.cw.net (195.89.101.185)  220.411 ms * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  62.115.175.71 (62.115.175.71)  298.264 ms * *
12  * ae-65.core1.dcb.edgecastcdn.net (152.195.64.129)  427.084 ms  320.434 ms
13  93.184.216.34 (93.184.216.34)  294.895 ms  279.916 ms  322.984 ms
root@RajPopat:/home/raj/Desktop#
```



3. What is the typical gap (delay) between probe packets?



H:H | 0.0007907

	A	B	C	D	E	F	G	H	I	J
1	13	27.25542295	192.168.12.62	93.184.216.34	UDP	76	54802 → 33434	0.0007907		
2	14	27.25571673	192.168.12.62	93.184.216.34	UDP	76	51428 → 33435	0.000293774		
3	15	27.25622999	192.168.12.62	93.184.216.34	UDP	76	35471 → 33436	0.000513266		
4	16	27.25631605	192.168.12.62	93.184.216.34	UDP	76	47161 → 33437	0.000086055		
5	17	27.25638885	192.168.12.62	93.184.216.34	UDP	76	39705 → 33438	0.000072804		
6	18	27.25675623	192.168.12.62	93.184.216.34	UDP	76	56612 → 33439	0.000367375		
7	19	27.25688325	192.168.12.62	93.184.216.34	UDP	76	55597 → 33440	0.000127022		
8	20	27.25696009	192.168.12.62	93.184.216.34	UDP	76	59558 → 33441	0.000076837		
9	21	27.25735067	192.168.12.62	93.184.216.34	UDP	76	46430 → 33442	0.00039058		
10	22	27.25743935	192.168.12.62	93.184.216.34	UDP	76	35349 → 33443	0.000088683		
11	23	27.25750766	192.168.12.62	93.184.216.34	UDP	76	42196 → 33444	0.000068312		
12	24	27.25757622	192.168.12.62	93.184.216.34	UDP	76	59207 → 33445	0.000068		
13	25	27.25764221	192.168.12.62	93.184.216.34	UDP	76	54639 → 33446	0.000065		
14	26	27.25810091	192.168.12.62	93.184.216.34	UDP	76	46445 → 33447	0.000458		
15	27	27.25823422	192.168.12.62	93.184.216.34	UDP	76	57387 → 33448	0.000133		
16	28	27.25836839	192.168.12.62	93.184.216.34	UDP	76	35476 → 33449	0.000134		
17	36	27.27227514	192.168.12.62	93.184.216.34	UDP	76	46541 → 33450	0.001805		
18	37	27.27239056	192.168.12.62	93.184.216.34	UDP	76	53364 → 33451	0.000115		

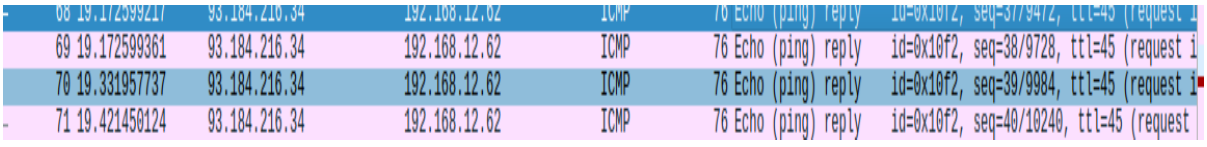
Sheet1

Sum: 0.012803771
Avg: 0.00025607542
Min: 0.000062279
Max: 0.001805366
Count: 50
Count Numbers: 50

First we add one column in wireshark delta display
Delta time: This is **the elapsed time from the previous packet to the current packet**.

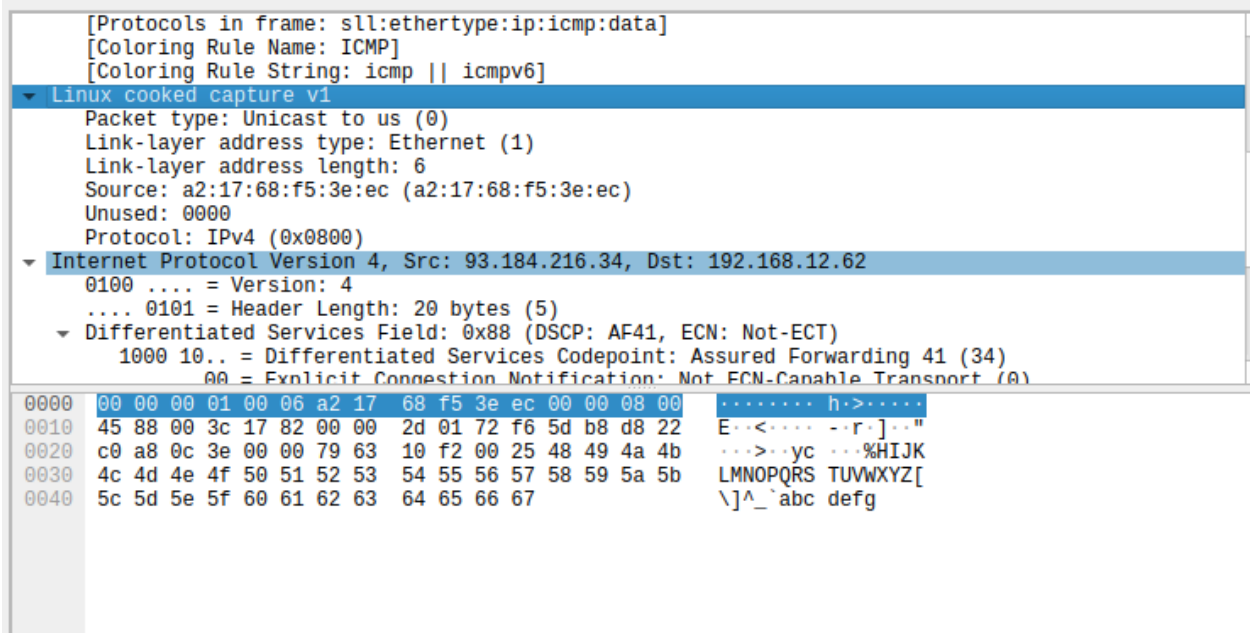
Here
We can see
Maximum gap(delay) b/w two probes is 0.00180 sec
Minimum gap(delay) b/w two probes is 0.00006227 sec
Avg is 0.0002560 sec

4. What is contained in probe responses?



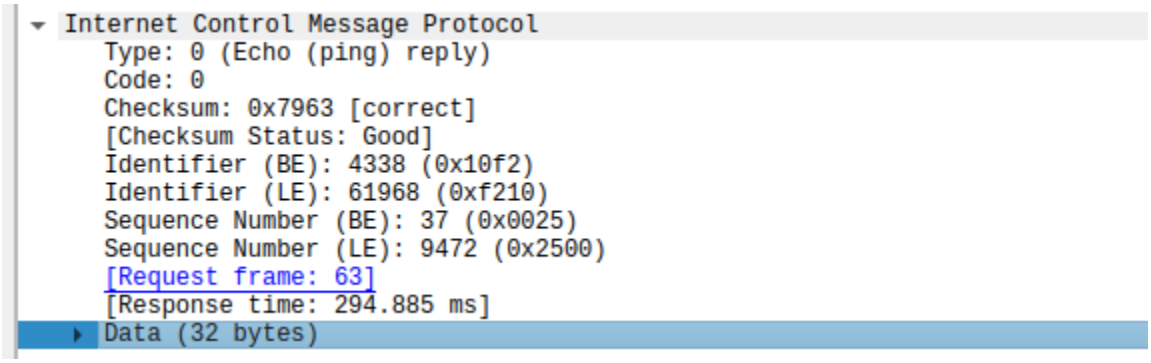
69	19.172599361	93.184.216.34	192.168.12.62	ICMP	76	Echo (ping) reply id=0x10f2, seq=38/9728, ttl=45 (request i
70	19.331957737	93.184.216.34	192.168.12.62	ICMP	76	Echo (ping) reply id=0x10f2, seq=39/9984, ttl=45 (request i
71	19.421450124	93.184.216.34	192.168.12.62	ICMP	76	Echo (ping) reply id=0x10f2, seq=40/10240, ttl=45 (request

Here we got probe responses in ICMP protocol

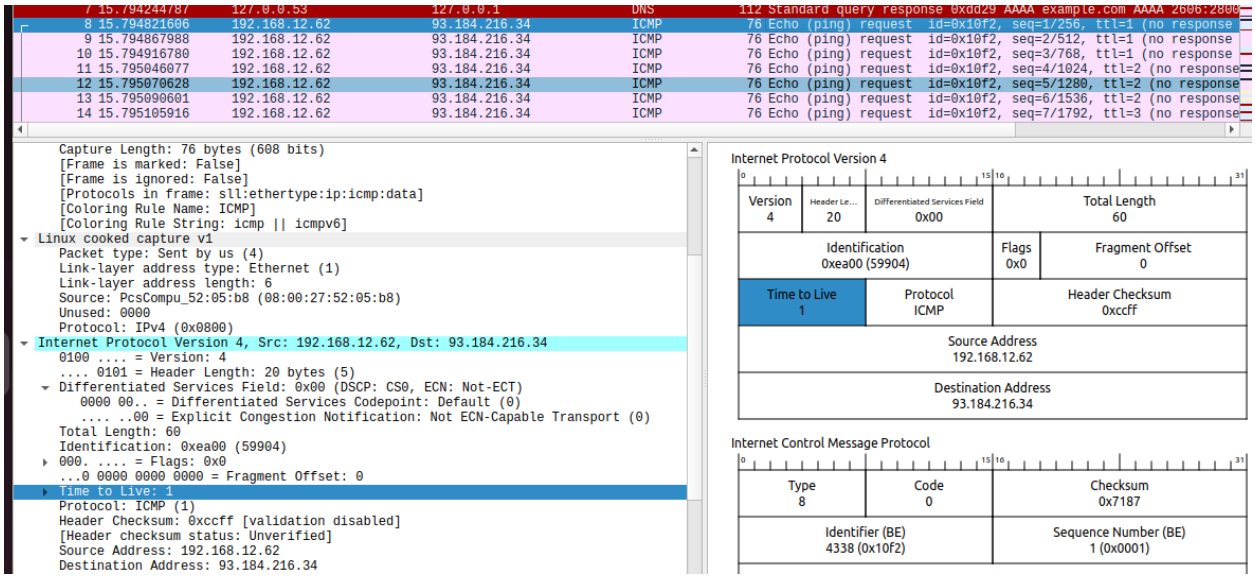


Here packet type is Unicast to us
Were in request packet type is send from us

Reply



5. Which protocol has TTL field and comment on how the values of this field varied across probes and responses?



IPV4 contain time to live

Each three probes start with time to live is 1

Then it will increase each time it pass through the hop

6. How long did it take to get the output of the traceroute session? Which is the bottleneck router?

```
root@RajPopat:/home/raj/Desktop# traceroute example.com
traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets
 1  _gateway (192.168.12.184)  3.348 ms  3.052 ms  5.545 ms
 2  * * *
 3  * * *
 4  100.64.0.125 (100.64.0.125)  269.512 ms  269.443 ms  269.374 ms
 5  182.19.106.113 (182.19.106.113)  269.309 ms  268.857 ms  268.728 ms
 6  xe-8-3-2.mlu.cw.net (195.89.101.185)  268.591 ms  254.690 ms  340.572 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  62.115.175.71 (62.115.175.71)  290.510 ms limelight-ic-315152.ip.twelve99-cu
st.net (213.248.83.119)  304.116 ms 62.115.175.71 (62.115.175.71)  293.678 ms
12  ae-65.core1.dcb.edgecastcdn.net (152.195.64.129)  305.998 ms  305.653 ms  31
1.296 ms
13  93.184.216.34 (93.184.216.34)  356.596 ms  369.782 ms  369.595 ms
14  93.184.216.34 (93.184.216.34)  369.325 ms  369.218 ms  369.141 ms
```

Here we can see that highest round trip time is 369.782 ms so from this we can say that this traceroute session definitely takes 369.782 ms

And between router 1 and router 4 time jump is around 266ms so this can be considered as bottleneck routers, but router 13 has 50ms delay so for a single router we can take it as bottleneck.

7. Do you see any stars (*) in the output? Discuss the potential reasons behind the presence of these stars in the output.

Yes i can see (*) in the output

The potential reasons behind the this could be

-Packet loss

-Congestion

-Router is not configured to response

-Protected by security measures

Task-2: Answer Task-1 Q.3, Q.5 and Q.6 using tcpdump instead of wireshark to capture traffic to/from one of the remaining three websites visited as part of Lab-1. [**3 Marks]**

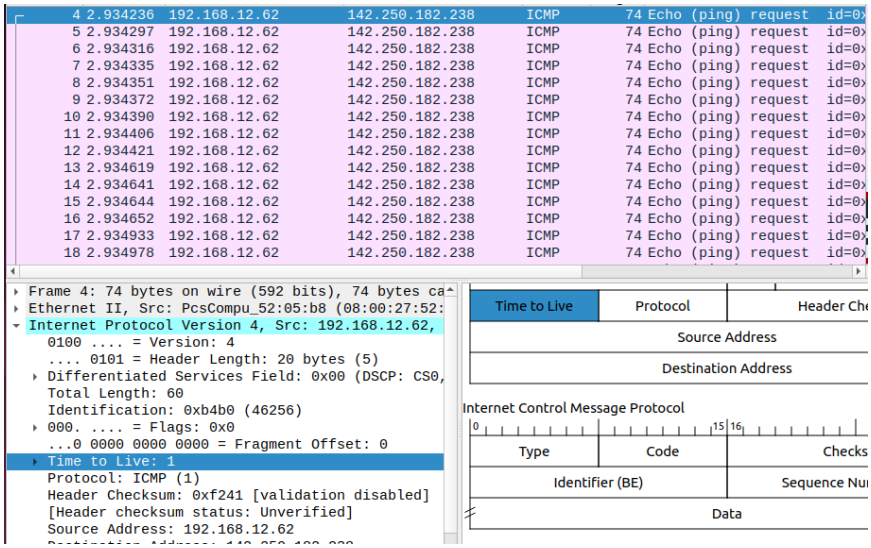
Here we are using Youtube.com

```
root@RajPopat:/home/raj/Desktop# sudo tcpdump -w 2.1.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
```

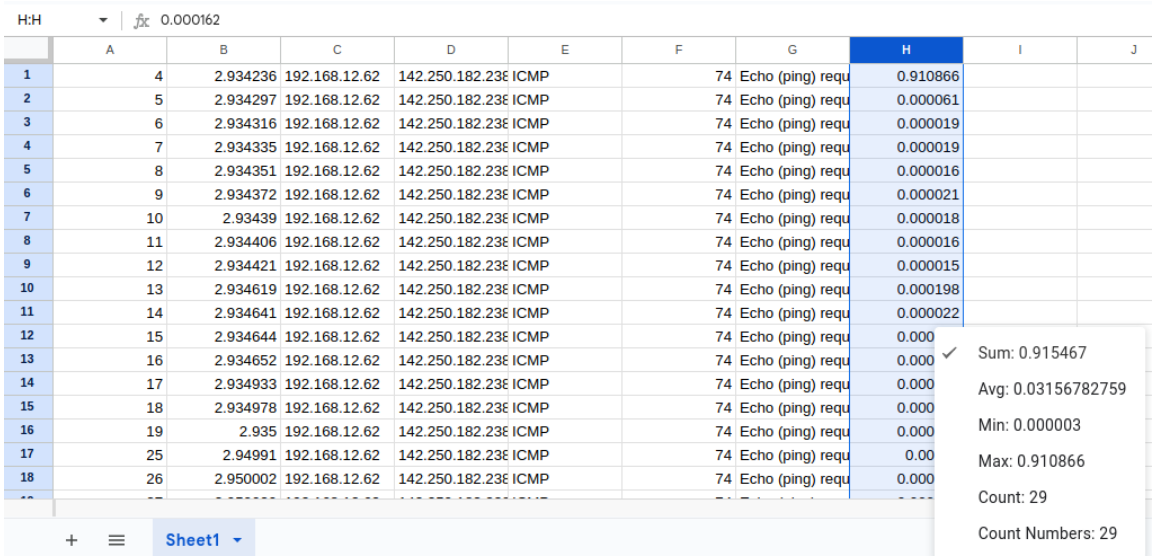
Traceroute of youtube.com

```
root@RajPopat:/home/raj/Desktop# traceroute youtube.com -I
traceroute to youtube.com (142.250.182.238), 30 hops max, 60 byte packets
 1  _gateway (192.168.12.184)  3.749 ms  3.953 ms  4.988 ms
 2  * * *
 3  * * *
 4  100.64.0.125 (100.64.0.125)  87.164 ms * *
 5  * * *
 6  * * *
 7  * * *
 8  108.170.251.124 (108.170.251.124)  95.646 ms * *
 9  * * *
10  * * *
11  108.170.248.193 (108.170.248.193)  103.002 ms * *
12  * * *
13  bom07s29-in-f14.1e100.net (142.250.182.238)  92.933 ms  79.128 ms  98.196 ms
```

Here highest RTT time we got is 103.002ms so the traceroute session will definitely take 103.002 ms to complete and we can see that b/w router 1 and router 4 difference b/w RTT is more so it is a bottleneck for the traceroute.



Here similarly IPV4 contain time to live and each probe start with time to live = 1 and increase each time to the next router



	A	B	C	D	E	F	G	H
1	4	2.934236	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.910866
2	5	2.934297	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000061
3	6	2.934316	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000019
4	7	2.934335	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000019
5	8	2.934351	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000016
6	9	2.934372	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000021
7	10	2.93439	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000018
8	11	2.934406	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000016
9	12	2.934421	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000015
10	13	2.934619	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000198
11	14	2.934641	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000022
12	15	2.934644	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000
13	16	2.934652	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000
14	17	2.934933	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000
15	18	2.934978	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000
16	19	2.935	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000
17	25	2.94991	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.00
18	26	2.950002	192.168.12.62	142.250.182.238	ICMP	74	Echo (ping) requ	0.000

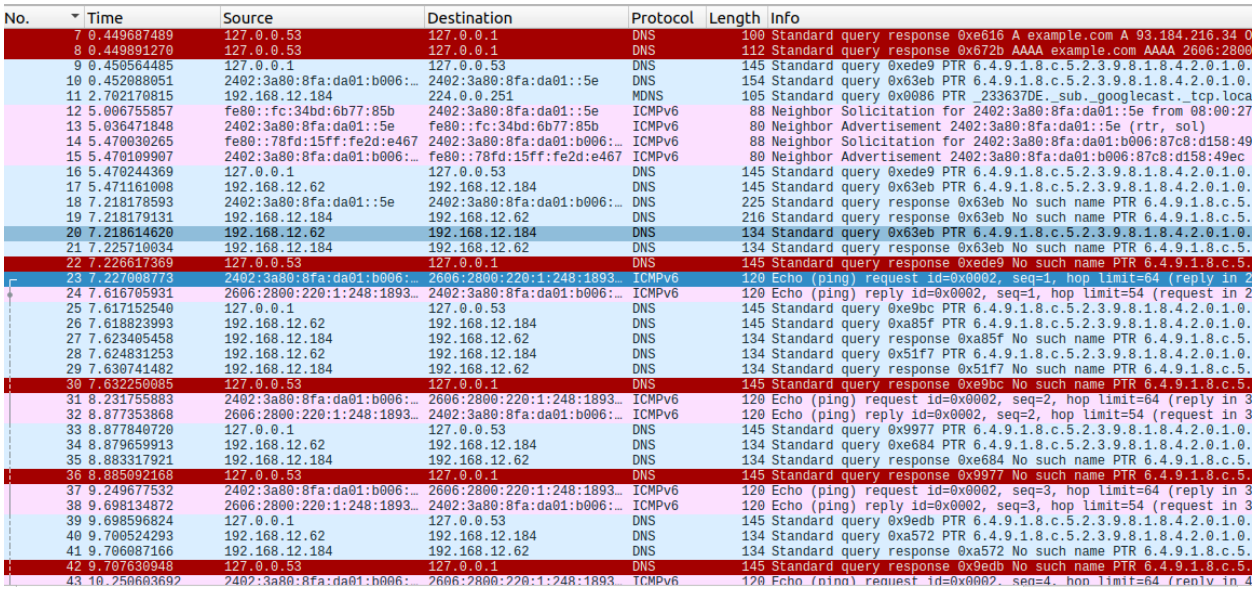
Here we can see the gap between each probe in the H column.
Were minimum is 0.000003sec maximum is 0.91066 sec and avg. is 0.031567sec

Task-3: Play with netstat or ss, ping and mtr and comment on what you see on wireshark and on terminal. [**5 Marks]**

PING

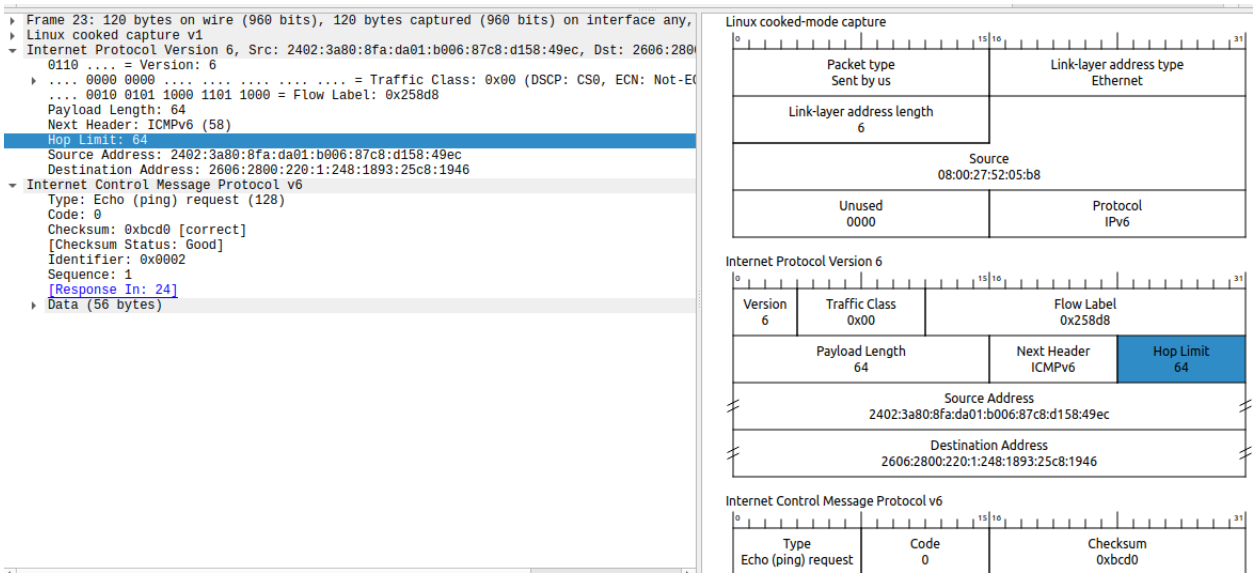
Ping example.com

```
root@RajPopat:/home/raj/Desktop# ping example.com
PING example.com(2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25
c8:1946)) 56 data bytes
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=1 ttl=54 time=390 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=2 ttl=54 time=646 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=3 ttl=54 time=449 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=4 ttl=54 time=388 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=5 ttl=54 time=460 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=6 ttl=54 time=483 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=7 ttl=54 time=730 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=8 ttl=54 time=549 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=9 ttl=54 time=343 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
1946): icmp_seq=10 ttl=54 time=358 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:
```



No.	Time	Source	Destination	Protocol	Length	Info
7	0.449687489	127.0.0.53	127.0.0.1	DNS	100	Standard query response 0xe616 A example.com A 93.184.216.34 C
8	0.449891270	127.0.0.53	127.0.0.1	DNS	112	Standard query response 0x672b AAAA example.com AAAA 2606:2800
9	0.450564485	127.0.0.1	127.0.0.53	DNS	145	Standard query 0xede9 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
10	0.452088051	2402:3a80:8fa:da01:b006:…	2402:3a80:8fa:da01::5e	DNS	154	Standard query 0x63eb PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
11	2.702170815	192.168.12.184	224.0.0.251	MDNS	105	Standard query 0x0086 PTR _233637DE._sub._googlecast._tcp.loca
12	5.006755857	fe80::fc:34bd:6b77:85b	2402:3a80:8fa:da01::5e	ICMPv6	88	Neighbor Solicitation for 2402:3a80:8fa:da01::5e from 08:00:27
13	5.036471848	2402:3a80:8fa:da01::5e	fe80::fc:34bd:6b77:85b	ICMPv6	80	Neighbor Advertisement 2402:3a80:8fa:da01::5e (rtr, sol)
14	5.470030265	fe80::78fd:15ff:fe2d:e467	2402:3a80:8fa:da01:b006:…	ICMPv6	88	Neighbor Solicitation for 2402:3a80:8fa:da01:b006:87c8:d158:49
15	5.470109907	2402:3a80:8fa:da01:b006:…	fe80::78fd:15ff:fe2d:e467	ICMPv6	80	Neighbor Advertisement 2402:3a80:8fa:da01:b006:87c8:d158:49ec
16	5.470244369	127.0.0.1	127.0.0.53	DNS	145	Standard query 0xede9 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
17	5.471161008	192.168.12.62	192.168.12.184	DNS	145	Standard query 0x63eb PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
18	7.218178593	2402:3a80:8fa:da01::5e	2402:3a80:8fa:da01:b006:…	DNS	225	Standard query response 0x63eb No such name PTR 6.4.9.1.8.c.5.
19	7.218179131	192.168.12.184	192.168.12.62	DNS	216	Standard query response 0x63eb No such name PTR 6.4.9.1.8.c.5.
20	7.218614620	192.168.12.62	192.168.12.184	DNS	134	Standard query 0x63eb PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
21	7.225710034	192.168.12.184	192.168.12.62	DNS	134	Standard query response 0x63eb No such name PTR 6.4.9.1.8.c.5.
22	7.226617369	127.0.0.53	127.0.0.1	DNS	145	Standard query response 0xede9 No such name PTR 6.4.9.1.8.c.5.
23	7.227008773	2402:3a80:8fa:da01:b006:…	2606:2800:220:1:248:1893…	ICMPv6	120	Echo (ping) request id=0x0002, seq=1, hop limit=64 (reply in 2
24	7.616705931	2606:2800:220:1:248:1893…	2402:3a80:8fa:da01:b006:…	ICMPv6	120	Echo (ping) reply id=0x0002, seq=1, hop limit=54 (request in 2
25	7.617152540	127.0.0.1	127.0.0.53	DNS	145	Standard query 0xe9bc PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
26	7.618823993	192.168.12.62	192.168.12.184	DNS	145	Standard query 0xa85f PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
27	7.623405458	192.168.12.184	192.168.12.62	DNS	134	Standard query response 0xa85f No such name PTR 6.4.9.1.8.c.5.
28	7.624831253	192.168.12.62	192.168.12.184	DNS	134	Standard query 0x51f7 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
29	7.630741482	192.168.12.184	192.168.12.62	DNS	134	Standard query response 0x51f7 No such name PTR 6.4.9.1.8.c.5.
30	7.632250085	127.0.0.53	127.0.0.1	DNS	145	Standard query response 0xe9bc No such name PTR 6.4.9.1.8.c.5.
31	8.231755883	2402:3a80:8fa:da01:b006:…	2606:2800:220:1:248:1893…	ICMPv6	120	Echo (ping) request id=0x0002, seq=2, hop limit=64 (reply in 3
32	8.877353868	2606:2800:220:1:248:1893…	2402:3a80:8fa:da01:b006:…	ICMPv6	120	Echo (ping) reply id=0x0002, seq=2, hop limit=54 (request in 3
33	8.877840720	127.0.0.1	127.0.0.53	DNS	145	Standard query 0x9977 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
34	8.879659913	192.168.12.62	192.168.12.184	DNS	134	Standard query 0xe684 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
35	8.883317921	192.168.12.184	192.168.12.62	DNS	134	Standard query response 0xe684 No such name PTR 6.4.9.1.8.c.5.
36	8.885092168	127.0.0.53	127.0.0.1	DNS	145	Standard query response 0x9977 No such name PTR 6.4.9.1.8.c.5.
37	9.249677532	2402:3a80:8fa:da01:b006:…	2606:2800:220:1:248:1893…	ICMPv6	120	Echo (ping) request id=0x0002, seq=3, hop limit=64 (reply in 3
38	9.698134872	2606:2800:220:1:248:1893…	2402:3a80:8fa:da01:b006:…	ICMPv6	120	Echo (ping) reply id=0x0002, seq=3, hop limit=54 (request in 3
39	9.698596824	127.0.0.1	127.0.0.53	DNS	145	Standard query 0x9edb PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
40	9.700524293	192.168.12.62	192.168.12.184	DNS	134	Standard query 0xa572 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.1.0.
41	9.706087166	192.168.12.184	192.168.12.62	DNS	134	Standard query response 0xa572 No such name PTR 6.4.9.1.8.c.5.
42	9.707630948	127.0.0.53	127.0.0.1	DNS	145	Standard query response 0x9edb No such name PTR 6.4.9.1.8.c.5.
43	10.250603692	2402:3a80:8fa:da01:b006:…	2606:2800:220:1:248:1893…	ICMPv6	120	Echo (ping) request id=0x0002, seq=4, hop limit=64 (reply in 4

It is sending an ICMP Echo request message to target host and wait for reply , it is used to measure the round-trip time b/w two host.



It uses IPV6 protocol and instead of TTL it has a Hop limit.

NETSTAT

Netstat -at : to list all tcp ports

```
root@RajPopat:/home/raj/Desktop# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
root@RajPopat:/home/raj/Desktop#
```

Netstat -au : to list all udp ports

```
root@RajPopat:/home/raj/Desktop# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:35557           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:46292              [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

netsat -ie : to display extended information on the interfaces

```
root@RajPopat:/home/raj/Desktop# netstat -ie
Kernel Interface table
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::fc:34bd:6b77:85b  prefixlen 64  scopeid 0x20<link>
        inet6 2402:3a80:8fa:da01:c80f:9d24:794a:2d4f  prefixlen 64  scopeid 0x0<
global>
        inet6 2402:3a80:8fa:da01:b006:87c8:d158:49ec  prefixlen 64  scopeid 0x0<
global>
        ether 08:00:27:52:05:b8  txqueuelen 1000  (Ethernet)
        RX packets 135105  bytes 52245212 (52.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 115838  bytes 69002747 (69.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 70850  bytes 6509584 (6.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 70850  bytes 6509584 (6.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

MTR

mtr example.com

```
                             My traceroute  [v0.95]
RajPopat (2402:3a80:8fa:da01:b006:87c8:d158:49ec) -> ex2023-08-27T22:32:17+0530
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                  Packets               Pings
 Host                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 2402:3a80:8fa:da01::5e       0.0%     5   29.3  19.5   4.8  51.5  20.6
 2. 2402:3a80:8fa:da01:0:43:c8a0:e40  0.0%     5   93.5 100.4  63.7 200.2  56.9
 3. (waiting for reply)
 4. fd00:0:1:4:5287:89ff:fe23:8052    0.0%     5   68.8  78.8  64.2 110.0  19.3
 5. fd00:0:1:30::2                    0.0%     5   71.7  76.0  53.8 108.7  20.8
 6. 2400:5200:1400:48::2              0.0%     5   81.8  88.3  60.3 115.8  20.6
 7. 2404:a800:3a00:1::1ee             0.0%     5  113.9 127.4  93.9 168.8  31.9
 8. (waiting for reply)
 9. 2403:e800:fd32:1001::            66.7%     4  348.4 348.4 348.4 348.4   0.0
10. 2403:e800:fd31:1011::1            0.0%     4  363.9 337.5 287.6 363.9  34.8
11. 2403:e800:fd04:1002::            25.0%     4  315.3 327.0 315.3 349.1  19.2
12. ec-eqix1-lax-10g.edgecastcdn.net 25.0%     4  310.0 350.1 310.0 372.6  34.8
13. ae-85.core1.oxr.edgecastcdn.net  33.3%     4  337.0 320.8 304.5 337.0  23.0
14. 2606:2800:220:1:248:1893:25c8:19  0.0%     4  319.0 321.8 299.0 349.8  20.9
```

It is a combination of ping and traceroute, it provides real-time information about the path that packets take from my pc to a destination host.

On wireshark