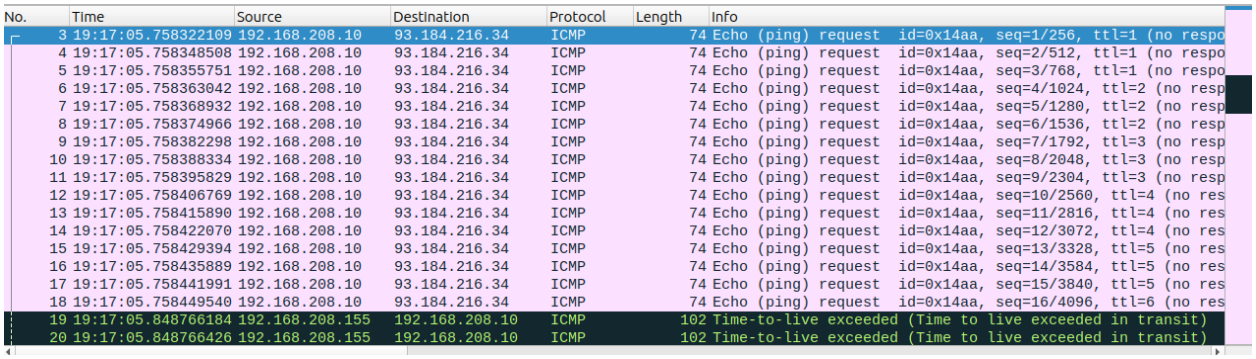
Task-1:

1)

The below snippet shows the traceroute on “**example.com”. ICMP** protocol is used to send probe packets.



No.	Time	Source	Destination	Protocol	Length	Info
3	19:17:05.758322109	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=1/256, ttl=1 (no respo
4	19:17:05.758348508	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=2/512, ttl=1 (no respo
5	19:17:05.758355751	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=3/768, ttl=1 (no respo
6	19:17:05.758363042	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=4/1024, ttl=2 (no resp
7	19:17:05.758368932	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=5/1280, ttl=2 (no resp
8	19:17:05.758374966	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=6/1536, ttl=2 (no resp
9	19:17:05.758382298	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=7/1792, ttl=3 (no resp
10	19:17:05.758388334	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=8/2048, ttl=3 (no resp
11	19:17:05.758395829	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=9/2304, ttl=3 (no resp
12	19:17:05.758406769	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=10/2560, ttl=4 (no res
13	19:17:05.758415890	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=11/2816, ttl=4 (no res
14	19:17:05.758422070	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=12/3072, ttl=4 (no res
15	19:17:05.758429394	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=13/3328, ttl=5 (no res
16	19:17:05.758435889	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=14/3584, ttl=5 (no res
17	19:17:05.758441991	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=15/3840, ttl=5 (no res
18	19:17:05.758449540	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=16/4096, ttl=6 (no res
19	19:17:05.848766184	192.168.208.155	192.168.208.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	19:17:05.848766426	192.168.208.155	192.168.208.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)

The key fields and corresponding details are as below:

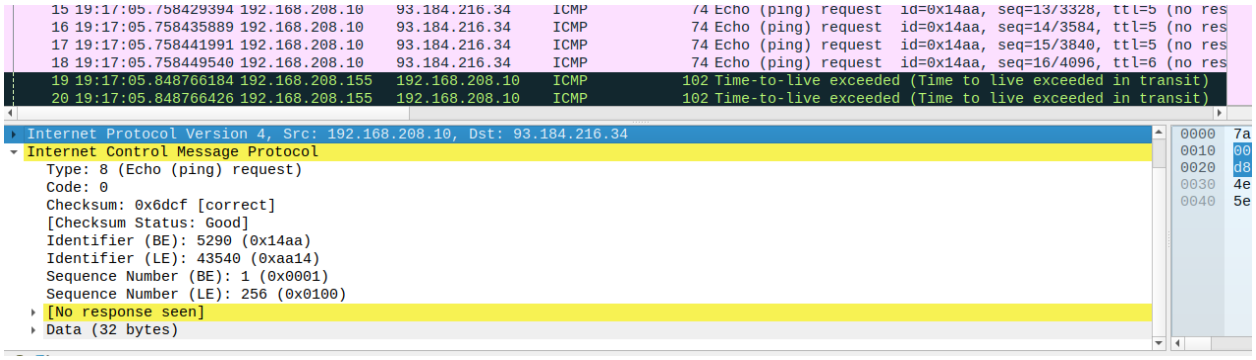
- **Source IP:** 192.168.208.10
  The IP address of the sender i.e., my system.

- **Destination IP:** 93.184.216.34
  The IP address of the destination i.e., example.com

- **Type:** 8 (Echo (ping) request) : I
- **Code:** 0
  Type 8 and code 0 shows that the selected packet is a request message.

- **Checksum:** 0x6dcf
  It shows that the calculated checksum from the ICMP header is the same as the checksum it has.

- **Identifier (Big Endian):** 5290 (0x14aa)
- **Sequence Number (Big Endian):** 1 (0x0001)
  These fields help identify individual probe packets and their order. Here, sequence number 1 shows the 1st packet. Note that these values are also provided in little endian.

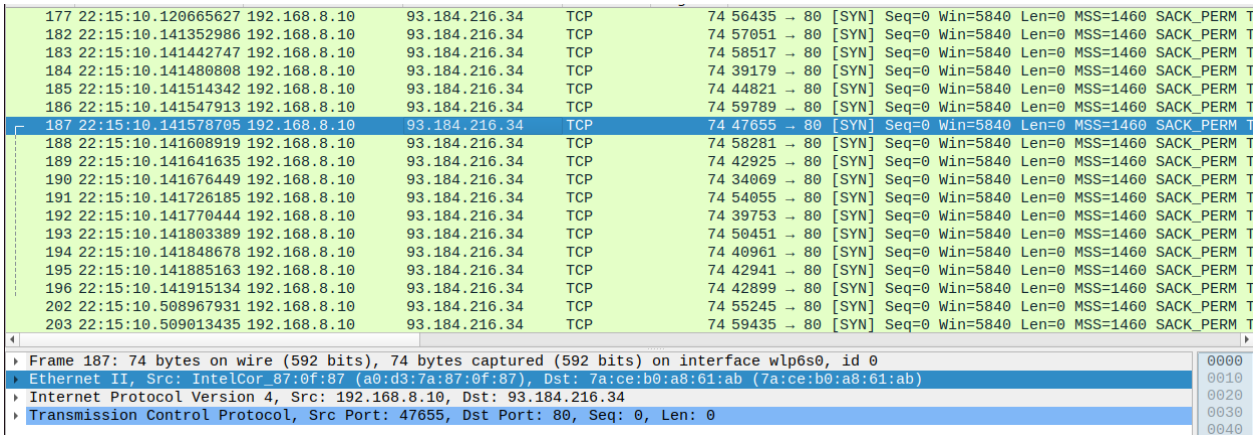


2)

Yes, we can change the default protocol used to send probes. The below command and snippets show a demonstration of it.

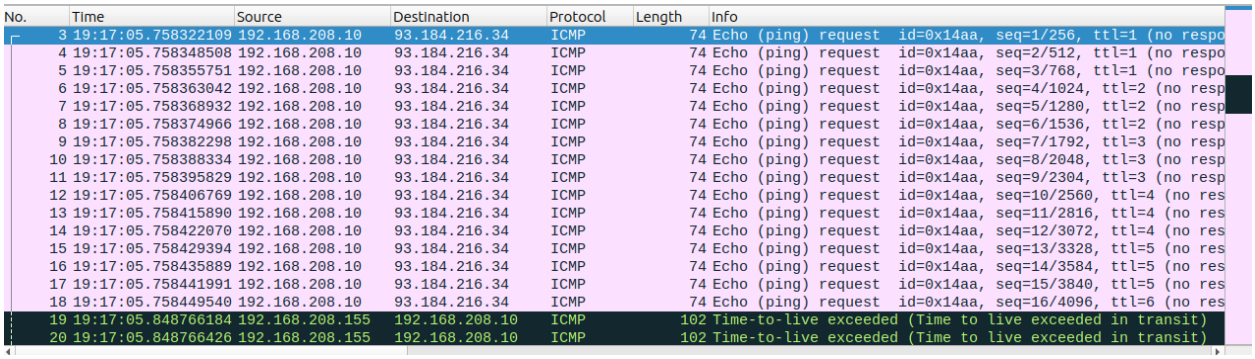
Command: traceroute -U example.com

```
akshay@akshay-Inspiron-3558:~$ sudo traceroute -T example.com
traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets
 1  _gateway (192.168.8.206)  2.904 ms  6.912 ms  6.888 ms
 2  192.168.36.15 (192.168.36.15)  158.579 ms  158.686 ms  158.797 ms
 3  192.168.34.117 (192.168.34.117)  160.667 ms  160.655 ms 192.168.34.113 (192.168.34.113)  160.641 ms
 4  192.168.48.24 (192.168.48.24)  158.332 ms  158.319 ms  158.306 ms
 5  192.168.48.33 (192.168.48.33)  160.589 ms  164.268 ms  160.563 ms
 6  125.18.92.93 (125.18.92.93)  158.254 ms  148.543 ms  148.458 ms
 7  182.79.198.125 (182.79.198.125)  163.565 ms * *
 8  * mei-b5-link.ip.twelve99.net (62.115.42.118)  200.949 ms *
 9  * * *
10  * * *
11  * * *
12  * limelight-ic-315152.ip.twelve99-cust.net (213.248.83.119)  395.412 ms 62.115.175.71 (62.115.175.71)  381.739 ms
13  ae-65.core1.dcb.edgecastcdn.net (152.195.64.129)  374.710 ms ae-66.core1.dcb.edgecastcdn.net (152.195.65.129)  381.591 m
-65.core1.dcb.edgecastcdn.net (152.195.64.129)  381.558 ms
14  93.184.216.34 (93.184.216.34)  367.338 ms  367.307 ms  367.277 ms
15  93.184.216.34 (93.184.216.34)  381.430 ms  381.487 ms  398.586 ms
akshay@akshay-Inspiron-3558:~$
```



3)

The below snippet shows the traceroute on “**example.com”.** The time between consecutive probes is calculated.



No.	Time	Source	Destination	Protocol	Length	Info
3	19:17:05.758322109	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=1/256, ttl=1 (no respo
4	19:17:05.758348508	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=2/512, ttl=1 (no respo
5	19:17:05.758355751	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=3/768, ttl=1 (no respo
6	19:17:05.758363042	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=4/1024, ttl=2 (no resp
7	19:17:05.758368932	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=5/1280, ttl=2 (no resp
8	19:17:05.758374966	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=6/1536, ttl=2 (no resp
9	19:17:05.758382298	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=7/1792, ttl=3 (no resp
10	19:17:05.758388334	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=8/2048, ttl=3 (no resp
11	19:17:05.758395829	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=9/2304, ttl=3 (no resp
12	19:17:05.758406769	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=10/2560, ttl=4 (no res
13	19:17:05.758415890	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=11/2816, ttl=4 (no res
14	19:17:05.758422070	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=12/3072, ttl=4 (no res
15	19:17:05.758429394	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=13/3328, ttl=5 (no res
16	19:17:05.758435889	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=14/3584, ttl=5 (no res
17	19:17:05.758441991	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=15/3840, ttl=5 (no res
18	19:17:05.758449540	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=16/4096, ttl=6 (no res
19	19:17:05.848766184	192.168.208.155	192.168.208.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	19:17:05.848766426	192.168.208.155	192.168.208.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)

758348508 - 758322109 = 26399

758355751 - 758348508 = 7243

758363042 - 758355751 = 7291

758368932 - 758363042 = 5890

758374966 - 758368932 = 6034

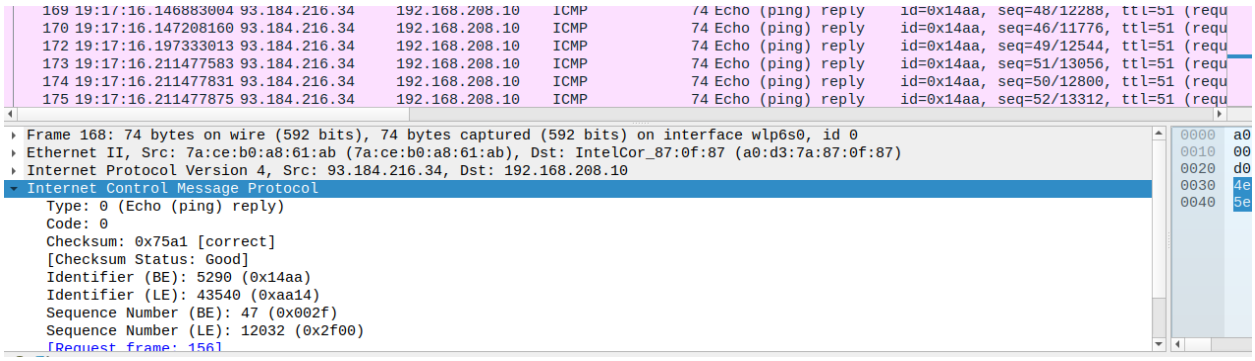
758382298 - 758374966 = 7332

758388334 - 758382298 = 6036

The typical gap (delay) between probe packets is 6000 to 7000 nano seconds.

4)

The below snippet shows the traceroute reply on “**example.com”.**



169	19:17:16.146883004	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=48/12288, ttl=51 (requ
170	19:17:16.147208160	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=46/11776, ttl=51 (requ
172	19:17:16.197333013	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=49/12544, ttl=51 (requ
173	19:17:16.211477583	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=51/13056, ttl=51 (requ
174	19:17:16.211477831	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=50/12800, ttl=51 (requ
175	19:17:16.211477875	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=52/13312, ttl=51 (requ

```
▸ Frame 168: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp6s0, id 0
▸ Ethernet II, Src: 7a:ce:b0:a8:61:ab (7a:ce:b0:a8:61:ab), Dst: IntelCor_87:0f:87 (a0:d3:7a:87:0f:87)
▸ Internet Protocol Version 4, Src: 93.184.216.34, Dst: 192.168.208.10
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x75a1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 5290 (0x14aa)
    Identifier (LE): 43540 (0xaa14)
    Sequence Number (BE): 47 (0x002f)
    Sequence Number (LE): 12032 (0x2f00)
    [Request frame: 156]
```

```
0000  a0
0010  00
0020  d0
0030  4e
0040  5e
```

The key details of the probe response are as below:

- **Source IP:** 93.184.216.34
  The IP address of the sender i.e., example.com

- **Destination IP:** 192.168.208.10
  The IP address of the destination i.e., my system.

- **Type:** 0 (Echo (ping) reply)
- **Code:** 0
  Type 0 and code 0 shows that the selected packet is a reply/response message.

- **Checksum:** 0x75a0 [correct]
  It shows that the calculated checksum from the ICMP header is the same as the checksum it has.

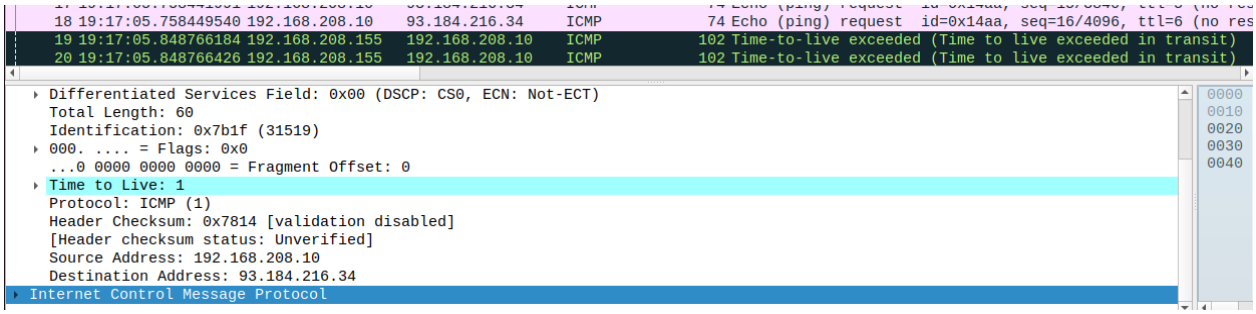
- **Identifier (Big Endian):** 5290 (0x14aa)
- **Sequence Number (Big Endian):** 1 (0x0001)
  These fields help identify individual probe packets and their order. Note that these values are also provided in little endian.

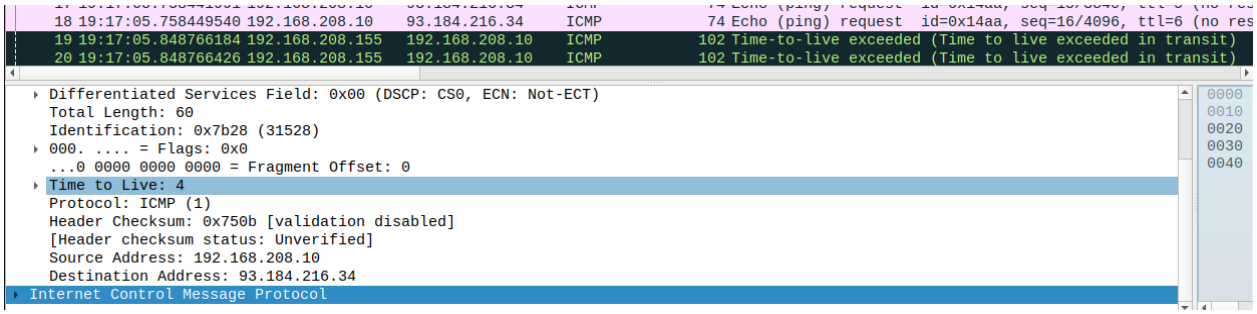
5)

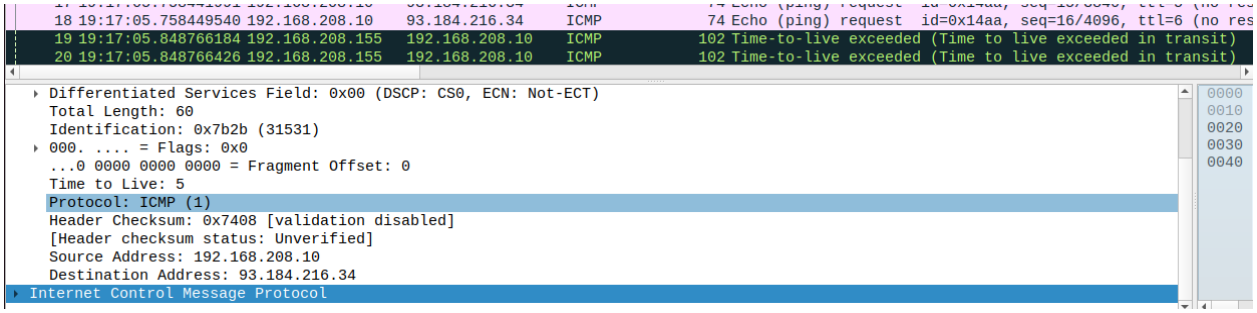
The ICMP protocol has a TTL field. The value indicates the number of hops a packet can take before being discarded

The ICMP protocol has a small TTL value for starting probes and it increases for each probe. The TTL values gradually increase as the packets traverse the network. The TTL value for each of the replies is the same.

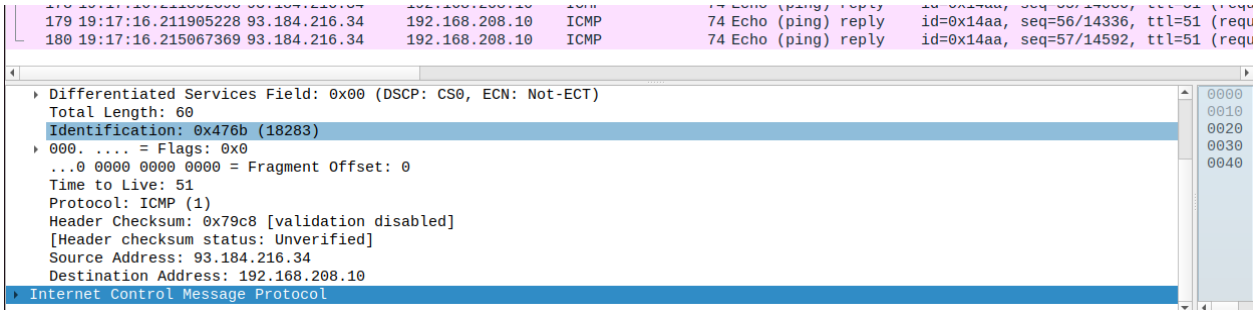
Probes:

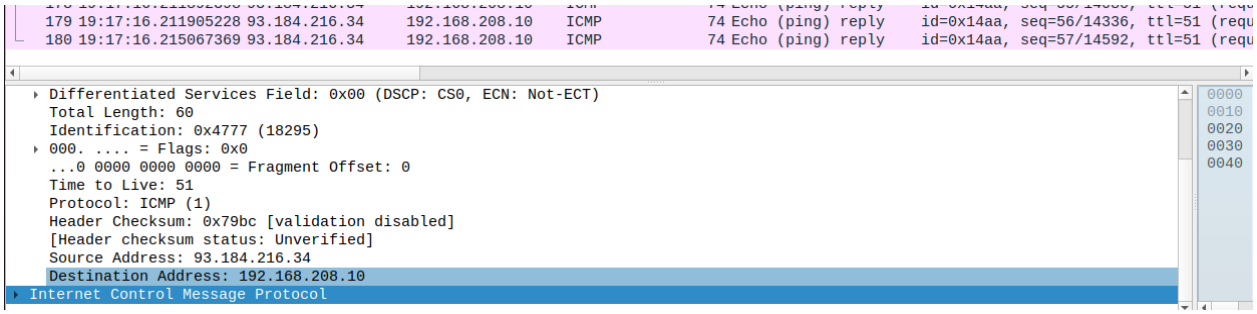






Response:

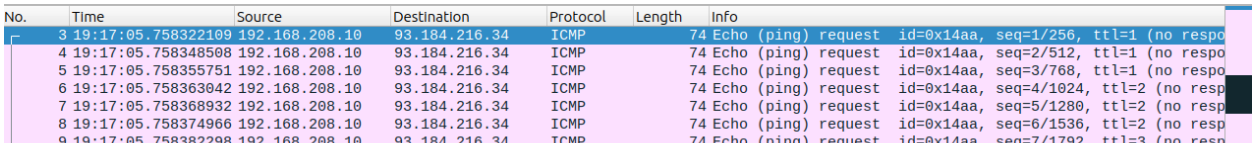




6)

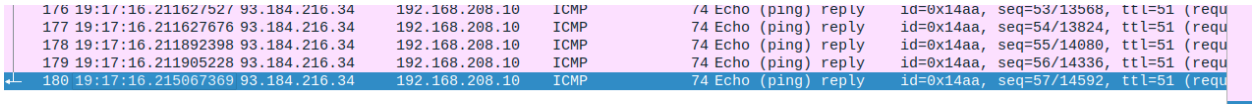
Time can be determined by comparing the timestamp of the first probe packet and the last response packet.

First probe:



No.	Time	Source	Destination	Protocol	Length	Info
3	19:17:05.758322109	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=1/256, ttl=1 (no respo
4	19:17:05.758348508	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=2/512, ttl=1 (no respo
5	19:17:05.758355751	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=3/768, ttl=1 (no respo
6	19:17:05.758363042	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=4/1024, ttl=2 (no resp
7	19:17:05.758368932	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=5/1280, ttl=2 (no resp
8	19:17:05.758374966	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=6/1536, ttl=2 (no resp
9	19:17:05.758382298	192.168.208.10	93.184.216.34	ICMP	74	Echo (ping) request id=0x14aa, seq=7/1792, ttl=3 (no resp

Last reply:



176	19:17:16.211627527	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=53/13568, ttl=51 (requ
177	19:17:16.211627676	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=54/13824, ttl=51 (requ
178	19:17:16.211892398	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=55/14080, ttl=51 (requ
179	19:17:16.211905228	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=56/14336, ttl=51 (requ
180	19:17:16.215067369	93.184.216.34	192.168.208.10	ICMP	74	Echo (ping) reply id=0x14aa, seq=57/14592, ttl=51 (requ

19:17:16.215067369 - 19:17:05.758322109 = 00:00:10.543254740

It takes approx 10 sec 543254740 nanosec to get the output of the traceroute session.
THe bottleneck router is 213.248.83.119

7)

Yes, there are stars (*) in the output. The output contains stars because no response is available from the corresponding hop and it is because of many reasons as listed below:

- Routers configured to not respond to ICMP probes
  Firewall settings
- Router/hop not working
- Packets get lost while moving from one hop to another.

Task-2:

3)

```
akshay@akshay-Inspiron-3558:~$ sudo tcpdump -i wlp6s0 -vv -nn src 128.95.155.134 or dst 128.95.155.134
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:44:37.684006 IP (tos 0x0, ttl 64, id 46112, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [S], cksum 0x83a7 (correct), seq 3155821910, win 64240, options [mss 1460,sac
kOK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.684211 IP (tos 0x0, ttl 64, id 30094, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42146 > 128.95.155.134.443: Flags [S], cksum 0x3c59 (correct), seq 552396748, win 64240, options [mss 1460,sack
OK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.884487 IP (tos 0x0, ttl 64, id 54792, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [S], cksum 0x3149 (correct), seq 4169538159, win 64240, options [mss 1460,sac
kOK,TS val 4204036923 ecr 0,nop,wscale 7], length 0
23:44:37.939964 IP (tos 0x28, ttl 48, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    128.95.155.134.443 > 192.168.8.10.42140: Flags [S.], cksum 0x4981 (correct), seq 1631662985, ack 3155821911, win 17896, opti
ons [mss 1400,sackOK,TS val 19290472 ecr 4204036722,nop,wscale 8], length 0
23:44:37.939996 IP (tos 0x0, ttl 64, id 46113, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [.], cksum 0xbb04 (correct), seq 1, ack 1, win 502, options [nop,nop,TS val 4
204036978 ecr 19290472], length 0
23:44:37.940204 IP (tos 0x0, ttl 64, id 46114, offset 0, flags [DF], proto TCP (6), length 569)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [P.], cksum 0xce24 (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS
val 4204036978 ecr 19290472], length 517
```

The typical gap (delay) between probe packets is around 205 ms.

5)

The ICMP protocol has a TTL field. The value indicates the number of hops a packet can take before being discarded

The ICMP protocol has a fixed value for each probe and its response.


```
akshay@akshay-Inspiron-3558:~$ sudo tcpdump -i wlp6s0 -vv -nn src 128.95.155.134 or dst 128.95.155.134
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:44:37.684006 IP (tos 0x0, ttl 64, id 46112, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [S], cksum 0x83a7 (correct), seq 3155821910, win 64240, options [mss 1460,sac
kOK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.684211 IP (tos 0x0, ttl 64, id 30094, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42146 > 128.95.155.134.443: Flags [S], cksum 0x3c59 (correct), seq 552396748, win 64240, options [mss 1460,sack
OK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.884487 IP (tos 0x0, ttl 64, id 54792, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [S], cksum 0x3149 (correct), seq 4169538159, win 64240, options [mss 1460,sac
kOK,TS val 4204036923 ecr 0,nop,wscale 7], length 0
23:44:37.939964 IP (tos 0x28, ttl 48, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    128.95.155.134.443 > 192.168.8.10.42140: Flags [S.], cksum 0x4981 (correct), seq 1631662985, ack 3155821911, win 17896, opti
ons [mss 1400,sackOK,TS val 19290472 ecr 4204036722,nop,wscale 8], length 0
23:44:37.939996 IP (tos 0x0, ttl 64, id 46113, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [.], cksum 0xbb04 (correct), seq 1, ack 1, win 502, options [nop,nop,TS val 4
204036978 ecr 19290472], length 0
23:44:37.940204 IP (tos 0x0, ttl 64, id 46114, offset 0, flags [DF], proto TCP (6), length 569)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [P.], cksum 0xce24 (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS
val 4204036978 ecr 19290472], length 517
```


6)

Time can be determined by comparing the timestamp of the first probe packet and the last response packet.

```
akshay@akshay-Inspiron-3558:~$ sudo tcpdump -i wlp6s0 -vv -nn src 128.95.155.134 or dst 128.95.155.134
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:44:37.684006 IP (tos 0x0, ttl 64, id 46112, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [S], cksum 0x83a7 (correct), seq 3155821910, win 64240, options [mss 1460,sac
kOK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.684211 IP (tos 0x0, ttl 64, id 30094, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42146 > 128.95.155.134.443: Flags [S], cksum 0x3c59 (correct), seq 552396748, win 64240, options [mss 1460,sack
OK,TS val 4204036722 ecr 0,nop,wscale 7], length 0
23:44:37.884487 IP (tos 0x0, ttl 64, id 54792, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [S], cksum 0x3149 (correct), seq 4169538159, win 64240, options [mss 1460,sac
kOK,TS val 4204036923 ecr 0,nop,wscale 7], length 0
23:44:37.939964 IP (tos 0x28, ttl 48, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    128.95.155.134.443 > 192.168.8.10.42140: Flags [S.], cksum 0x4981 (correct), seq 1631662985, ack 3155821911, win 17896, opti
ons [mss 1400,sackOK,TS val 19290472 ecr 4204036722,nop,wscale 8], length 0
23:44:37.939996 IP (tos 0x0, ttl 64, id 46113, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [.], cksum 0xbb04 (correct), seq 1, ack 1, win 502, options [nop,nop,TS val 4
204036978 ecr 19290472], length 0
23:44:37.940204 IP (tos 0x0, ttl 64, id 46114, offset 0, flags [DF], proto TCP (6), length 569)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [P.], cksum 0xce24 (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS
val 4204036978 ecr 19290472], length 517
```

```
23:44:49.199683 IP (tos 0x0, ttl 64, id 54801, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [.], cksum 0x5d30 (correct), seq 644, ack 5724, win 500, options [nop,nop,TS
val 4204048238 ecr 19301700], length 0
23:44:49.199792 IP (tos 0x28, ttl 49, id 65117, offset 0, flags [DF], proto TCP (6), length 83)
    128.95.155.134.443 > 192.168.8.10.42156: Flags [P.], cksum 0xe5bb (correct), seq 5724:5755, ack 644, win 75, options [nop,no
p,TS val 19301700 ecr 4204038246], length 31
23:44:49.199802 IP (tos 0x0, ttl 64, id 54802, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [.], cksum 0x5d10 (correct), seq 644, ack 5755, win 501, options [nop,nop,TS
val 4204048238 ecr 19301700], length 0
23:44:49.199910 IP (tos 0x28, ttl 48, id 65118, offset 0, flags [DF], proto TCP (6), length 52)
    128.95.155.134.443 > 192.168.8.10.42156: Flags [F.], cksum 0x85c1 (correct), seq 5755, ack 644, win 75, options [nop,nop,TS
val 19301700 ecr 4204038246], length 0
23:44:49.243437 IP (tos 0x0, ttl 64, id 54803, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42156 > 128.95.155.134.443: Flags [.], cksum 0x5ce3 (correct), seq 644, ack 5756, win 501, options [nop,nop,TS
val 4204048282 ecr 19301700], length 0
23:44:49.243464 IP (tos 0x0, ttl 64, id 46123, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42140 > 128.95.155.134.443: Flags [.], cksum 0x4481 (correct), seq 1984, ack 5849, win 501, options [nop,nop,TS
 val 4204048282 ecr 19301677], length 0
23:44:49.243474 IP (tos 0x0, ttl 64, id 30105, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.8.10.42146 > 128.95.155.134.443: Flags [.], cksum 0xad42 (correct), seq 644, ack 5756, win 501, options [nop,nop,TS
```

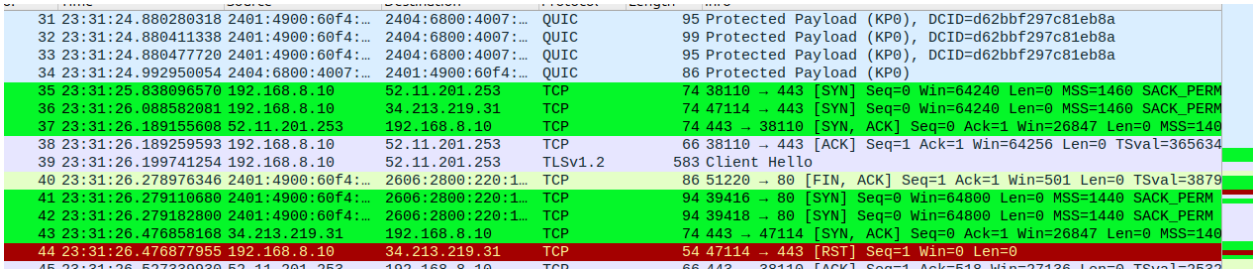
It takes around 1.5 second to get the output of the traceroute session. We cannot find the router info in tcpdump hence not able to find bottleneck router.

Task-3:

SS:

Here, the ss command in terminal shows the socket connection, whereas the wireshark is used to show the http connection as shown in the snippet below.

```
akshay@akshay-Inspiron-3558:~$ ss -ta
State      Recv-Q Send-Q                    Local Address:Port                     Peer Address:Port
Process
LISTEN     0      4096                         127.0.0.54:domain                        0.0.0.0:*

LISTEN     0      128                          127.0.0.1:ipp                            0.0.0.0:*

LISTEN     0      4096                      127.0.0.53%lo:domain                        0.0.0.0:*

ESTAB      0      0                         192.168.8.10:45842                   74.125.24.188:https

ESTAB      0      0                         192.168.8.10:45858                   74.125.24.188:https

ESTAB      0      0                         192.168.8.10:55576                   52.11.201.253:https

LISTEN     0      128                             [::1]:ipp                               [::]:*
```



PING:

The ping command is used for testing of the network by sending requests and waiting for reply. In the terminal has less information as compared to the information available in the wireshark.

The command prompt mentions only ICMP sequence to which we can understand it uses ICMP protocol. The wireshark specifically mentions it uses ICMPv6 protocol.

Also, the wireshark has details of request and reply for each ping.

```
akshay@akshay-Inspiron-3558:~$ ping -c 10 www.example.com
PING www.example.com(2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946)) 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=49 time=544 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=2 ttl=49 time=363 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=3 ttl=49 time=696 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=4 ttl=49 time=656 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=5 ttl=49 time=949 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=6 ttl=49 time=277 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=7 ttl=49 time=493 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=8 ttl=49 time=723 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=9 ttl=49 time=547 ms
64 bytes from 2606:2800:220:1:248:1893:25c8:1946 (2606:2800:220:1:248:1893:25c8:1946): icmp_seq=10 ttl=49 time=454 ms

--- www.example.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9000ms
rtt min/avg/max/mdev = 277.028/570.170/948.822/184.306 ms
```

156	22:42:39.442288852	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=1, hop limit=64 (reply
157	22:42:39.986675283	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=1, hop limit=49 (request
158	22:42:39.987217385	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0x9108 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
159	22:42:39.994186919	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0x9108 No such name PTR 6.4.9.1.8.
160	22:42:40.442257542	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=2, hop limit=64 (reply
161	22:42:40.804961568	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=2, hop limit=49 (request
162	22:42:40.805543727	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0x84c9 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
163	22:42:40.811750072	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0x84c9 No such name PTR 6.4.9.1.8.
164	22:42:41.443000884	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=3, hop limit=64 (reply
165	22:42:42.139429403	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=3, hop limit=49 (request
166	22:42:42.139994677	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0x9390 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
167	22:42:42.147412516	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0x9390 No such name PTR 6.4.9.1.8.
168	22:42:42.443317895	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=4, hop limit=64 (reply
169	22:42:43.099467181	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=4, hop limit=49 (request
170	22:42:43.100001380	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0xba36 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
171	22:42:43.106940824	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0xba36 No such name PTR 6.4.9.1.8.
172	22:42:43.442825103	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=5, hop limit=64 (reply
173	22:42:44.391624242	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=5, hop limit=49 (request
174	22:42:44.392185693	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0xda39 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
175	22:42:44.397090848	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0xda39 No such name PTR 6.4.9.1.8.
176	22:42:44.442763991	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=6, hop limit=64 (reply
177	22:42:44.449544932	fe80::78ce:b0ff…	2401:4900:60f4:…	ICMPv6	86	Neighbor Solicitation for 2401:4900:60f4:44b9:4b6c:34ac:9f
178	22:42:44.449576132	2401:4900:60f4:…	fe80::78ce:b0ff…	ICMPv6	78	Neighbor Advertisement 2401:4900:60f4:44b9:4b6c:34ac:9fdb:
179	22:42:44.656572223	fe80::6ee4:9373…	2401:4900:60f4:…	ICMPv6	86	Neighbor Solicitation for 2401:4900:60f4:44b9::b4 from a0:
180	22:42:44.719748100	2401:4900:60f4:…	fe80::6ee4:9373…	ICMPv6	78	Neighbor Advertisement 2401:4900:60f4:44b9::b4 (rtr, sol)
181	22:42:44.719748406	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	118	Echo (ping) reply id=0x3c6e, seq=6, hop limit=49 (request
182	22:42:44.721047580	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query 0xa745 PTR 6.4.9.1.8.c.5.2.3.9.8.1.8.4.2.0.
183	22:42:44.726381772	2401:4900:60f4:…	2401:4900:60f4:…	DNS	152	Standard query response 0xa745 No such name PTR 6.4.9.1.8.
184	22:42:45.443635872	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	118	Echo (ping) request id=0x3c6e, seq=7, hop limit=64 (reply

MTR:

The MTR command combines both ping and traceroute and provides information about the packet loss. The terminal provides a crisp table showing packet loss and required details, but has less information as compared to the information available in the wireshark.

The command prompt does not provide all the details of protocols used. The wireshark specifically mentions it uses ICMPv6 protocol.

Also, the wireshark has details of request and reply for each ping.

```
akshay@akshay-Inspiron-3558:~$ mtr -c 10 -r www.example.com
Start: 2023-08-27T23:02:50+0530
HOST: akshay-Inspiron-3558        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 2401:4900:60f4:44b9::b4    0.0%    10   18.8  17.4   2.7  57.0  20.6
  2.|-- ???                      100.0    10    0.0   0.0   0.0   0.0   0.0
  3.|-- 2401:4900:d0:4600::249     0.0%    10   66.7  69.1  37.9 148.4  39.3
  4.|-- 2404:a800:3a00:201::a9     0.0%    10   44.3  73.0  44.3 136.3  29.5
  5.|-- 2404:a800::158             0.0%    10  292.2 267.2 242.0 303.0  20.6
  6.|-- ???                      100.0    10    0.0   0.0   0.0   0.0   0.0
  7.|-- eqix.ny9.edgecast.com      0.0%    10  278.7 300.5 274.7 375.0  29.2
  8.|-- ae-71.core1.nyb.edgecastc  0.0%    10  333.2 298.1 274.9 344.9  24.1
  9.|-- 2606:2800:220:1:248:1893:  0.0%    10  422.7 308.2 278.2 422.7  43.6
akshay@akshay-Inspiron-3558:~$
```

No.	TIme	Source	Destination	Protocol	Length	Info
10	23:02:51.199233170	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33001, hop limit=2 (no
11	23:02:51.299432520	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33002, hop limit=3 (no
12	23:02:51.358342329	2401:4900:d0:46…	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
13	23:02:51.399462613	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33003, hop limit=4 (no
14	23:02:51.499704923	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33004, hop limit=5 (no
15	23:02:51.535679913	2404:a800:3a00:…	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
16	23:02:51.600015154	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33005, hop limit=6 (no
17	23:02:51.700364092	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33006, hop limit=7 (no
18	23:02:51.759175367	2404:a800::158	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
19	23:02:51.800462278	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33007, hop limit=8 (no
20	23:02:51.900780053	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33008, hop limit=9 (rep
21	23:02:52.001100516	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33009, hop limit=10 (no
22	23:02:52.075196571	2001:504:f::1:5…	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
23	23:02:52.075196809	2606:2800:4263:…	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
24	23:02:52.101026803	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33010, hop limit=11 (re
25	23:02:52.180494505	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	78	Echo (ping) reply id=0x2856, seq=33008, hop limit=48 (requ
26	23:02:52.201194379	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33011, hop limit=12 (re
27	23:02:52.313500316	2401:4900:60f4:…	2606:2800:220:1…	ICMPv6	78	Echo (ping) request id=0x2856, seq=33012, hop limit=1 (no
28	23:02:52.370359002	2401:4900:60f4:…	2401:4900:60f4:…	ICMPv6	126	Time Exceeded (hop limit exceeded in transit)
29	23:02:52.382140894	2606:2800:220:1…	2401:4900:60f4:…	ICMPv6	78	Echo (ping) reply id=0x2856, seq=33010, hop limit=48 (requ