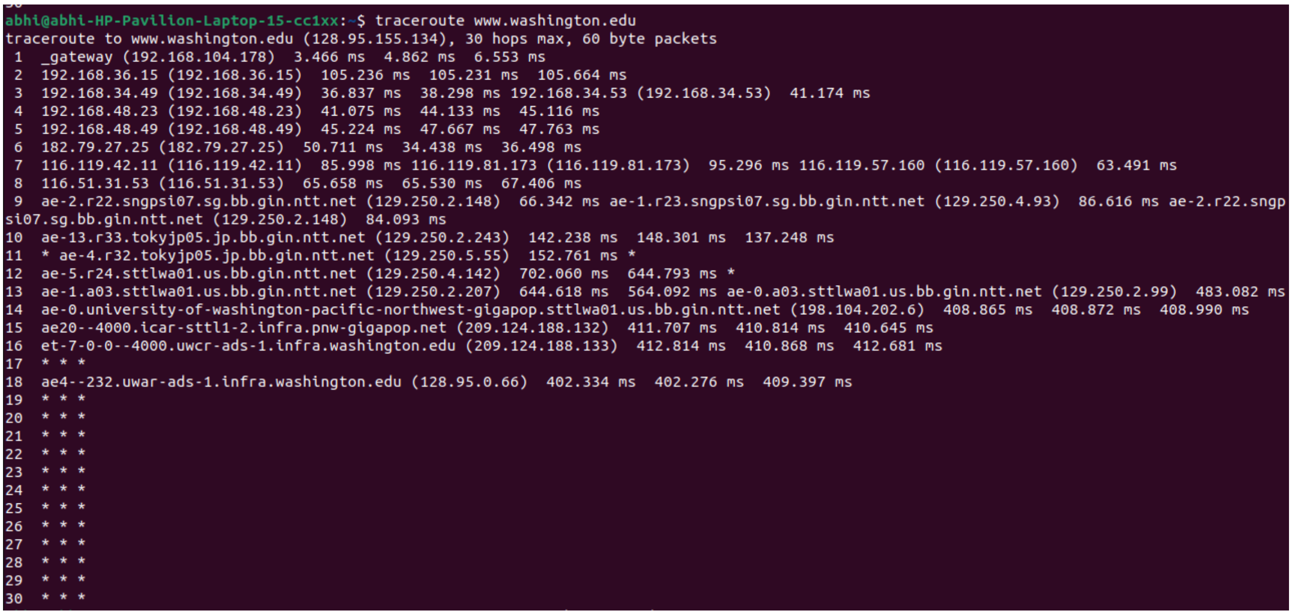
Task-1: Capture traceroute traffic to/from one of four websites visited as part of Lab-1 using wireshark and answer the following a google doc. Feel free to include screenshots from terminal/wireshark to support your answers. [**7 Marks]**

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

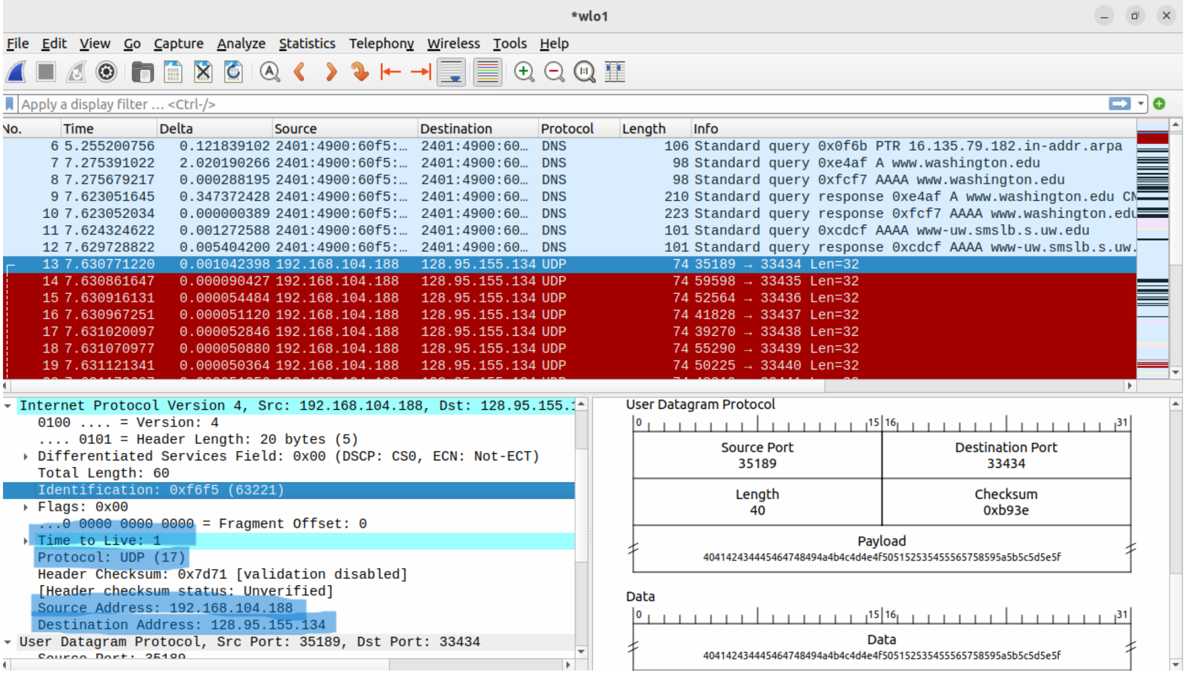
Ans: By default, UDP is used to send probe packets.

Key fields are:

1. Time to live of 1st probe: 1
2. Protocol: UDP (17)
3. Source Address: 192.168.104.188
4. Destination address: 128.95.155.134
5. Identification: 0xf6f5



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ traceroute www.washington.edu
traceroute to www.washington.edu (128.95.155.134), 30 hops max, 60 byte packets
 1  _gateway (192.168.104.178)  3.466 ms  4.862 ms  6.553 ms
 2  192.168.36.15 (192.168.36.15)  105.236 ms  105.231 ms  105.664 ms
 3  192.168.34.49 (192.168.34.49)  36.837 ms  38.298 ms 192.168.34.53 (192.168.34.53)  41.174 ms
 4  192.168.48.23 (192.168.48.23)  41.075 ms  44.133 ms  45.116 ms
 5  192.168.48.49 (192.168.48.49)  45.224 ms  47.667 ms  47.763 ms
 6  182.79.27.25 (182.79.27.25)  50.711 ms  34.438 ms  36.498 ms
 7  116.119.42.11 (116.119.42.11)  85.998 ms 116.119.81.173 (116.119.81.173)  95.296 ms 116.119.57.160 (116.119.57.160)  63.491 ms
 8  116.51.31.53 (116.51.31.53)  65.658 ms  65.530 ms  67.406 ms
 9  ae-2.r22.sngpsi07.sg.bb.gin.ntt.net (129.250.2.148)  66.342 ms ae-1.r23.sngpsi07.sg.bb.gin.ntt.net (129.250.4.93)  86.616 ms ae-2.r22.sngp
si07.sg.bb.gin.ntt.net (129.250.2.148)  84.093 ms
10  ae-13.r33.tokyjp05.jp.bb.gin.ntt.net (129.250.2.243)  142.238 ms  148.301 ms  137.248 ms
11  * ae-4.r32.tokyjp05.jp.bb.gin.ntt.net (129.250.5.55)  152.761 ms *
12  ae-5.r24.sttlwa01.us.bb.gin.ntt.net (129.250.4.142)  702.060 ms  644.793 ms *
13  ae-1.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.207)  644.618 ms  564.092 ms ae-0.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.99)  483.082 ms
14  ae-0.university-of-washington-pacific-northwest-gigapop.sttlwa01.us.bb.gin.ntt.net (198.104.202.6)  408.865 ms  408.872 ms  408.990 ms
15  ae20--4000.icar-sttl1-2.infra.pnw-gigapop.net (209.124.188.132)  411.707 ms  410.814 ms  410.645 ms
16  et-7-0-0--4000.uwcr-ads-1.infra.washington.edu (209.124.188.133)  412.814 ms  410.868 ms  412.681 ms
17  * * *
18  ae4--232.uwar-ads-1.infra.washington.edu (128.95.0.66)  402.334 ms  402.276 ms  409.397 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```


*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Delta       Source             Destination        Protocol  Length  Info
    6 5.255200756  0.121839102 2401:4900:60f5:…   2401:4900:60…     DNS          106 Standard query 0x0f6b PTR 16.135.79.182.in-addr.arpa
    7 7.275391022  2.020190266 2401:4900:60f5:…   2401:4900:60…     DNS           98 Standard query 0xe4af A www.washington.edu
    8 7.275679217  0.000288195 2401:4900:60f5:…   2401:4900:60…     DNS           98 Standard query 0xfcf7 AAAA www.washington.edu
    9 7.623051645  0.347372428 2401:4900:60f5:…   2401:4900:60…     DNS          210 Standard query response 0xe4af A www.washington.edu CN
   10 7.623052034  0.000000389 2401:4900:60f5:…   2401:4900:60…     DNS          223 Standard query response 0xfcf7 AAAA www.washington.edu
   11 7.624324622  0.001272588 2401:4900:60f5:…   2401:4900:60…     DNS          101 Standard query 0xcdcf AAAA www-uw.smslb.s.uw.edu
   12 7.629728822  0.005404200 2401:4900:60f5:…   2401:4900:60…     DNS          101 Standard query response 0xcdcf AAAA www-uw.smslb.s.uw.
   13 7.630771220  0.001042398 192.168.104.188    128.95.155.134    UDP           74 35189 → 33434 Len=32
   14 7.630861647  0.000090427 192.168.104.188    128.95.155.134    UDP           74 59598 → 33435 Len=32
   15 7.630916131  0.000054484 192.168.104.188    128.95.155.134    UDP           74 52564 → 33436 Len=32
   16 7.630967251  0.000051120 192.168.104.188    128.95.155.134    UDP           74 41828 → 33437 Len=32
   17 7.631020097  0.000052846 192.168.104.188    128.95.155.134    UDP           74 39270 → 33438 Len=32
   18 7.631070977  0.000050880 192.168.104.188    128.95.155.134    UDP           74 55290 → 33439 Len=32
   19 7.631121341  0.000050364 192.168.104.188    128.95.155.134    UDP           74 50225 → 33440 Len=32
```

```
▾ Internet Protocol Version 4, Src: 192.168.104.188, Dst: 128.95.155.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf6f5 (63221)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▸ Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x7d71 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.104.188
    Destination Address: 128.95.155.134
▾ User Datagram Protocol, Src Port: 35189, Dst Port: 33434
```

User Datagram Protocol

Source Port 35189 | Destination Port 33434

Length 40 | Checksum 0xb93e

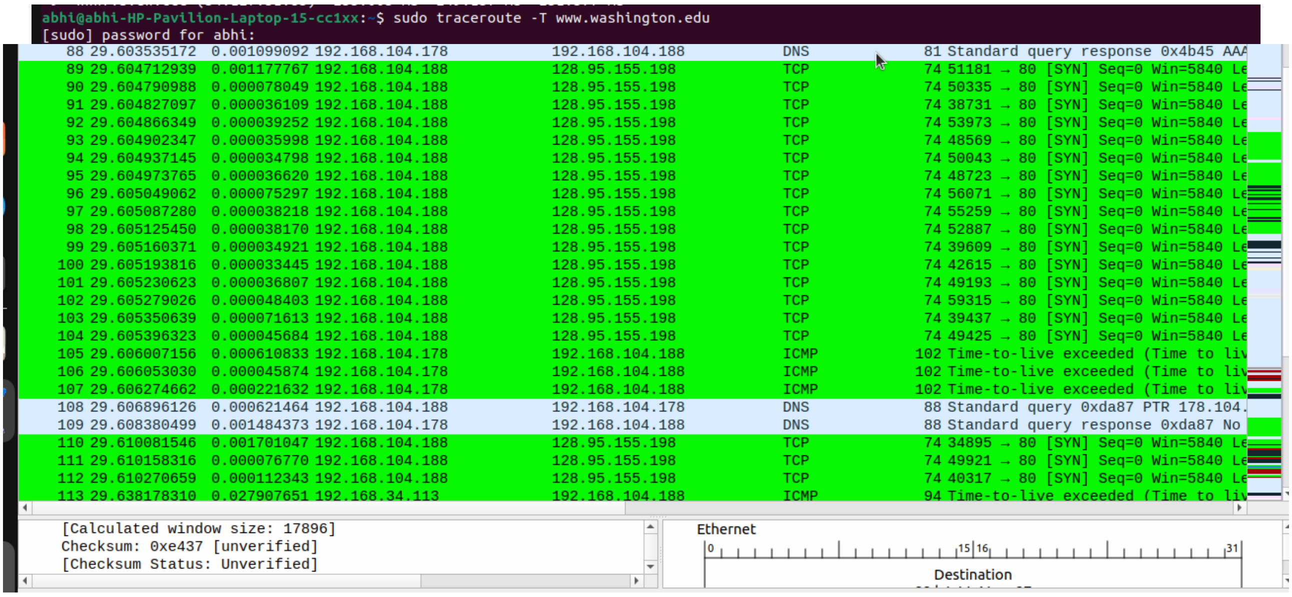
Payload 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f

Data

Data 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f

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

Ans: Yes, we can change the default protocol by specifically mentioning in traceroute command.
Here is the example of traceroute using TCP protocol



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ sudo traceroute -T www.washington.edu
[sudo] password for abhi:
```

```
   88 29.603535172  0.001099092 192.168.104.178   192.168.104.188   DNS     81 Standard query response 0x4b45 AAA
   89 29.604712939  0.001177767 192.168.104.188   128.95.155.198    TCP     74 51181 → 80 [SYN] Seq=0 Win=5840 Le
   90 29.604790988  0.000078049 192.168.104.188   128.95.155.198    TCP     74 50335 → 80 [SYN] Seq=0 Win=5840 Le
   91 29.604827097  0.000036109 192.168.104.188   128.95.155.198    TCP     74 38731 → 80 [SYN] Seq=0 Win=5840 Le
   92 29.604866349  0.000039252 192.168.104.188   128.95.155.198    TCP     74 53973 → 80 [SYN] Seq=0 Win=5840 Le
   93 29.604902347  0.000035998 192.168.104.188   128.95.155.198    TCP     74 48569 → 80 [SYN] Seq=0 Win=5840 Le
   94 29.604937145  0.000034798 192.168.104.188   128.95.155.198    TCP     74 50043 → 80 [SYN] Seq=0 Win=5840 Le
   95 29.604973765  0.000036620 192.168.104.188   128.95.155.198    TCP     74 48723 → 80 [SYN] Seq=0 Win=5840 Le
   96 29.605049062  0.000075297 192.168.104.188   128.95.155.198    TCP     74 56071 → 80 [SYN] Seq=0 Win=5840 Le
   97 29.605087280  0.000038218 192.168.104.188   128.95.155.198    TCP     74 55259 → 80 [SYN] Seq=0 Win=5840 Le
   98 29.605125450  0.000038170 192.168.104.188   128.95.155.198    TCP     74 52887 → 80 [SYN] Seq=0 Win=5840 Le
   99 29.605160371  0.000034921 192.168.104.188   128.95.155.198    TCP     74 39609 → 80 [SYN] Seq=0 Win=5840 Le
  100 29.605193816  0.000033445 192.168.104.188   128.95.155.198    TCP     74 42615 → 80 [SYN] Seq=0 Win=5840 Le
  101 29.605230623  0.000036807 192.168.104.188   128.95.155.198    TCP     74 49193 → 80 [SYN] Seq=0 Win=5840 Le
  102 29.605279026  0.000048403 192.168.104.188   128.95.155.198    TCP     74 59315 → 80 [SYN] Seq=0 Win=5840 Le
  103 29.605350639  0.000071613 192.168.104.188   128.95.155.198    TCP     74 39437 → 80 [SYN] Seq=0 Win=5840 Le
  104 29.605396323  0.000045684 192.168.104.188   128.95.155.198    TCP     74 49425 → 80 [SYN] Seq=0 Win=5840 Le
  105 29.606007156  0.000610833 192.168.104.178   192.168.104.188   ICMP   102 Time-to-live exceeded (Time to liv
  106 29.606053030  0.000045874 192.168.104.178   192.168.104.188   ICMP   102 Time-to-live exceeded (Time to liv
  107 29.606274662  0.000221632 192.168.104.178   192.168.104.188   ICMP   102 Time-to-live exceeded (Time to liv
  108 29.606896126  0.000621464 192.168.104.188   192.168.104.178   DNS     88 Standard query 0xda87 PTR 178.104.
  109 29.608380499  0.001484373 192.168.104.178   192.168.104.188   DNS     88 Standard query response 0xda87 No
  110 29.610081546  0.001701047 192.168.104.188   128.95.155.198    TCP     74 34895 → 80 [SYN] Seq=0 Win=5840 Le
  111 29.610158316  0.000076770 192.168.104.188   128.95.155.198    TCP     74 49921 → 80 [SYN] Seq=0 Win=5840 Le
  112 29.610270659  0.000112343 192.168.104.188   128.95.155.198    TCP     74 40317 → 80 [SYN] Seq=0 Win=5840 Le
  113 29.638178310  0.027907651 192.168.34.113    192.168.104.188   ICMP    94 Time-to-live exceeded (Time to liv
```

```
    [Calculated window size: 17896]
    Checksum: 0xe437 [unverified]
    [Checksum Status: Unverified]
```

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

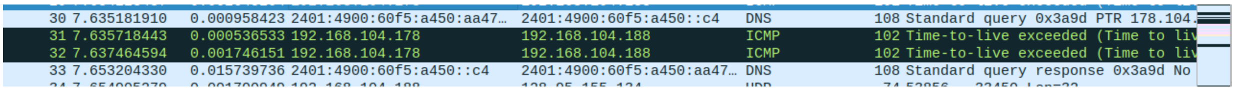
Ans: Typical gap between probe is around 35 ms

4. What is contained in probe responses?

Ans:

In UDP:

When TTL becomes 0 at router, probes come with Time to live exceeded message.

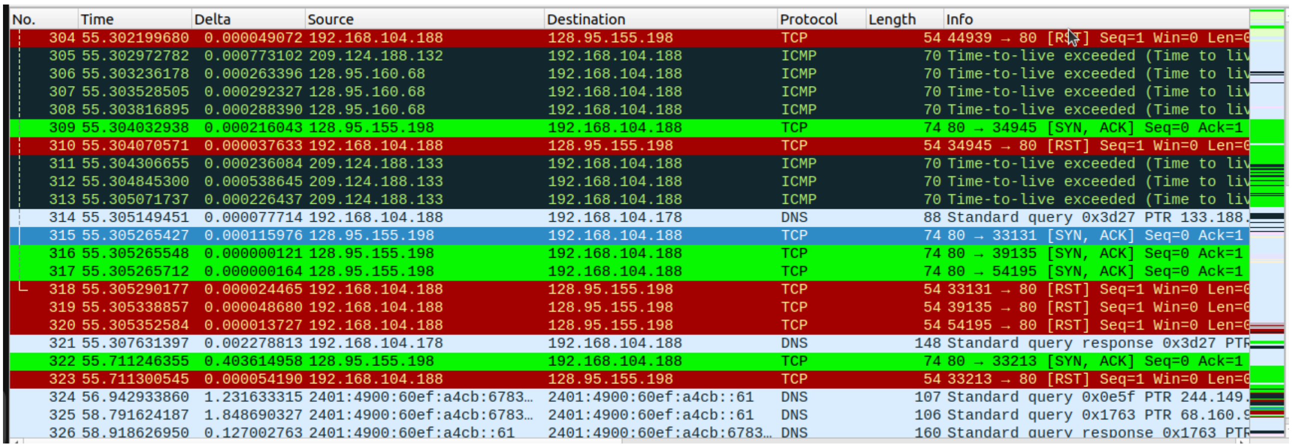


```
30 7.635181910  0.000958423 2401:4900:60f5:a450:aa47…  2401:4900:60f5:a450::c4    DNS     108 Standard query 0x3a9d PTR 178.104.
31 7.635718443  0.000536533 192.168.104.178            192.168.104.188            ICMP    102 Time-to-live exceeded (Time to liv
32 7.637464594  0.001746151 192.168.104.178            192.168.104.188            ICMP    102 Time-to-live exceeded (Time to liv
33 7.653204330  0.015739736 2401:4900:60f5:a450::c4    2401:4900:60f5:a450:aa47…  DNS     108 Standard query response 0x3a9d No
```

When probe reach the destination, the probe comes with the message as Destination port unreachable.

In TCP:

When TTL becomes 0 at router, probes come with Time to live exceeded message. Whereas, when it reaches destination, the source tries to make 3 way handshake using SYN packets with destination, which does not happen.



```
No.  Time          Delta        Source                     Destination                Protocol  Length  Info
 304 55.302199680  0.000049072 192.168.104.188            128.95.155.198             TCP        54 44939 → 80 [RST] Seq=1 Win=0 Len=0
 305 55.302972782  0.000773102 209.124.188.132            192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 306 55.303236178  0.000263396 128.95.160.68              192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 307 55.303528505  0.000292327 128.95.160.68              192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 308 55.303816895  0.000288390 128.95.160.68              192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 309 55.304032938  0.000216043 128.95.155.198             192.168.104.188            TCP        74 80 → 34945 [SYN, ACK] Seq=0 Ack=1
 310 55.304070571  0.000037633 192.168.104.188            128.95.155.198             TCP        54 34945 → 80 [RST] Seq=1 Win=0 Len=0
 311 55.304306655  0.000236084 209.124.188.133            192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 312 55.304845300  0.000538645 209.124.188.133            192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 313 55.305071737  0.000226437 209.124.188.133            192.168.104.188            ICMP       70 Time-to-live exceeded (Time to liv
 314 55.305149451  0.000077714 192.168.104.188            192.168.104.178            DNS        88 Standard query 0x3d27 PTR 133.188.
 315 55.305265427  0.000115976 128.95.155.198             192.168.104.188            TCP        74 80 → 33131 [SYN, ACK] Seq=0 Ack=1
 316 55.305265548  0.000000121 128.95.155.198             192.168.104.188            TCP        74 80 → 39135 [SYN, ACK] Seq=0 Ack=1
 317 55.305265712  0.000000164 128.95.155.198             192.168.104.188            TCP        74 80 → 54195 [SYN, ACK] Seq=0 Ack=1
 318 55.305290177  0.000024465 192.168.104.188            128.95.155.198             TCP        54 33131 → 80 [RST] Seq=1 Win=0 Len=0
 319 55.305338857  0.000048680 192.168.104.188            128.95.155.198             TCP        54 39135 → 80 [RST] Seq=1 Win=0 Len=0
 320 55.305352584  0.000013727 192.168.104.188            128.95.155.198             TCP        54 54195 → 80 [RST] Seq=1 Win=0 Len=0
 321 55.307631397  0.002278813 192.168.104.178            192.168.104.188            DNS       148 Standard query response 0x3d27 PTR
 322 55.711246355  0.403614958 128.95.155.198             192.168.104.188            TCP        74 80 → 33213 [SYN, ACK] Seq=0 Ack=1
 323 55.711300545  0.000054190 192.168.104.188            128.95.155.198             TCP        54 33213 → 80 [RST] Seq=1 Win=0 Len=0
 324 56.942933860  1.231633315 2401:4900:60ef:a4cb:6783…  2401:4900:60ef:a4cb::61    DNS       107 Standard query 0x0e5f PTR 244.149.
 325 58.791624187  1.848690327 2401:4900:60ef:a4cb:6783…  2401:4900:60ef:a4cb::61    DNS       106 Standard query 0x1763 PTR 68.160.9
 326 58.918626950  0.127002763 2401:4900:60ef:a4cb::61    2401:4900:60ef:a4cb:6783…  DNS       160 Standard query response 0x1763 PTR
```

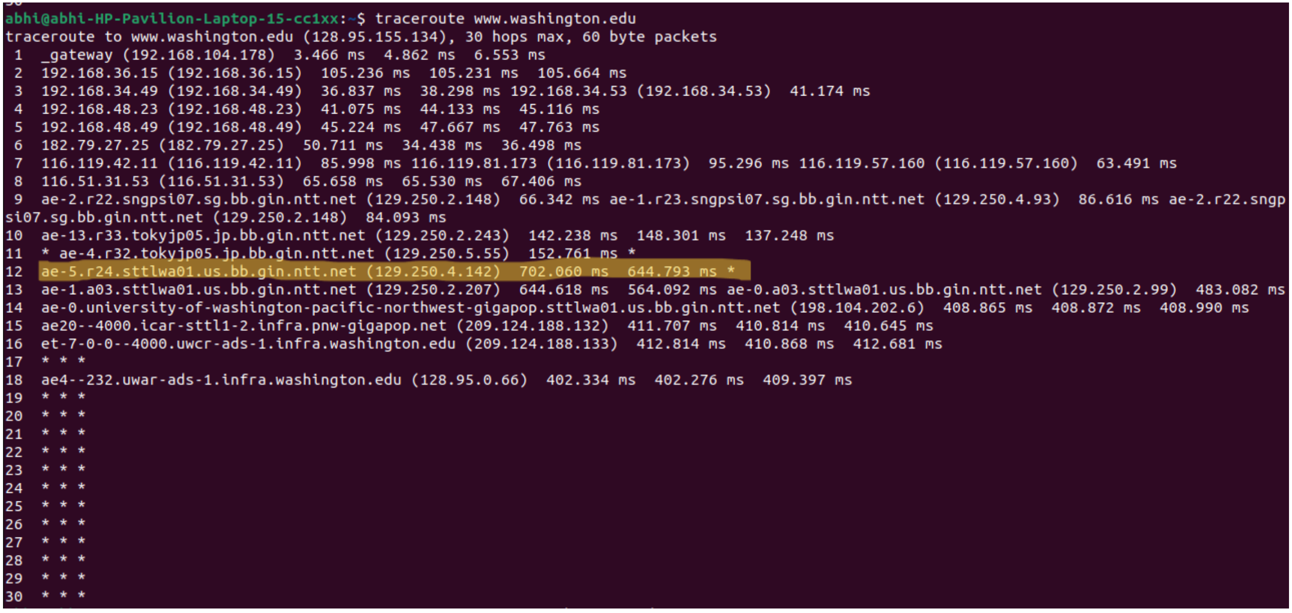
5. Which protocol has TTL field and comment on how the values of this field varied across probes and responses?

Ans: IPV4 has TTL field. It defines the number of hops packet can take before reaching destination. Its value is decreased by 1 at each router.
Initially, while sending the probes, its value is set to 1. At first router it is decreased to 0 and an ICMP packet is sent to source with message as Time to Live exceeded. Again a packet is sent by source with TTL value 2, Which becomes 0 after passing 2 routers (if destination is not reached within 2 hops).
Source keeps on increasing the value of TTL until the destination is reached. At destination, the source reply by sending Destination port unreachable message if the sending protocol is UDP.

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

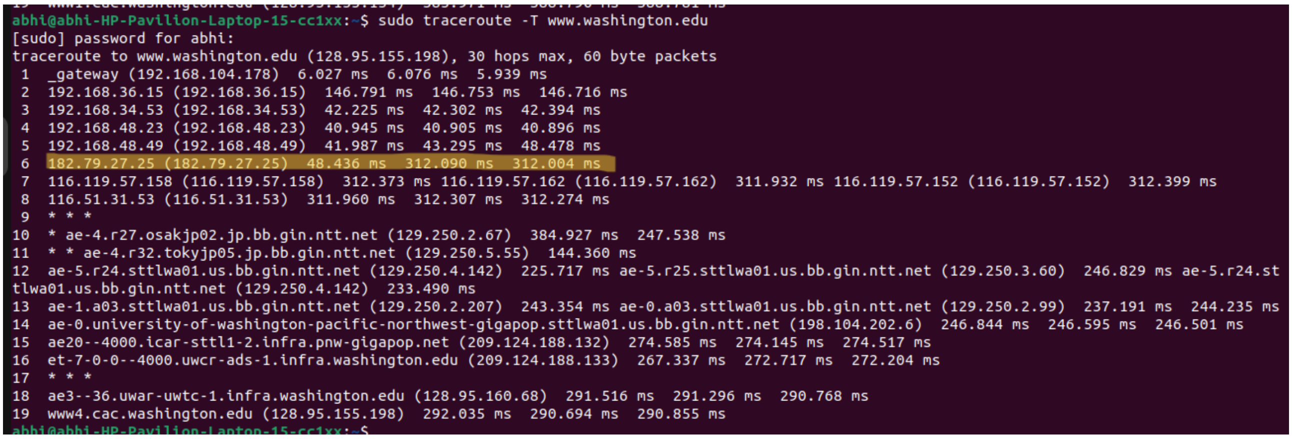
Ans: The output of the traceroute session took near around 30 sec in both tcp and udp protocol.

In case of udp the bottleneck router was ae-5.r24.sttlwa01.us.bb.gin.ntt.net (129.250.4.142).



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ traceroute www.washington.edu
traceroute to www.washington.edu (128.95.155.134), 30 hops max, 60 byte packets
 1  _gateway (192.168.104.178)  3.466 ms  4.862 ms  6.553 ms
 2  192.168.36.15 (192.168.36.15)  105.236 ms  105.231 ms  105.664 ms
 3  192.168.34.49 (192.168.34.49)  36.837 ms  38.298 ms 192.168.34.53 (192.168.34.53)  41.174 ms
 4  192.168.48.23 (192.168.48.23)  41.075 ms  44.133 ms  45.116 ms
 5  192.168.48.49 (192.168.48.49)  45.224 ms  47.667 ms  47.763 ms
 6  182.79.27.25 (182.79.27.25)  50.711 ms  34.438 ms  36.498 ms
 7  116.119.42.11 (116.119.42.11)  85.998 ms 116.119.81.173 (116.119.81.173)  95.296 ms 116.119.57.160 (116.119.57.160)  63.491 ms
 8  116.51.31.53 (116.51.31.53)  65.658 ms  65.530 ms  67.406 ms
 9  ae-2.r22.sngpsi07.sg.bb.gin.ntt.net (129.250.2.148)  66.342 ms ae-1.r23.sngpsi07.sg.bb.gin.ntt.net (129.250.4.93)  86.616 ms ae-2.r22.sngp
si07.sg.bb.gin.ntt.net (129.250.2.148)  84.093 ms
10  ae-13.r33.tokyjp05.jp.bb.gin.ntt.net (129.250.2.243)  142.238 ms  148.301 ms  137.248 ms
11  * ae-4.r32.tokyjp05.jp.bb.gin.ntt.net (129.250.5.55)  152.761 ms *
12  ae-5.r24.sttlwa01.us.bb.gin.ntt.net (129.250.4.142)  702.060 ms  644.793 ms *
13  ae-1.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.207)  644.618 ms  564.092 ms ae-0.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.99)  483.082 ms
14  ae-0.university-of-washington-pacific-northwest-gigapop.sttlwa01.us.bb.gin.ntt.net (198.104.202.6)  408.865 ms  408.872 ms  408.990 ms
15  ae20--4000.icar-sttl1-2.infra.pnw-gigapop.net (209.124.188.132)  411.707 ms  410.814 ms  410.645 ms
16  et-7-0-0--4000.uwcr-ads-1.infra.washington.edu (209.124.188.133)  412.814 ms  410.868 ms  412.681 ms
17  * * *
18  ae4--232.uwar-ads-1.infra.washington.edu (128.95.0.66)  402.334 ms  402.276 ms  409.397 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

In case of tcp the bottleneck router was 182.79.27.25



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ sudo traceroute -T www.washington.edu
[sudo] password for abhi:
traceroute to www.washington.edu (128.95.155.198), 30 hops max, 60 byte packets
 1  _gateway (192.168.104.178)  6.027 ms  6.076 ms  5.939 ms
 2  192.168.36.15 (192.168.36.15)  146.791 ms  146.753 ms  146.716 ms
 3  192.168.34.53 (192.168.34.53)  42.225 ms  42.302 ms  42.394 ms
 4  192.168.48.23 (192.168.48.23)  40.945 ms  40.905 ms  40.896 ms
 5  192.168.48.49 (192.168.48.49)  41.987 ms  43.295 ms  48.478 ms
 6  182.79.27.25 (182.79.27.25)  48.436 ms  312.090 ms  312.004 ms
 7  116.119.57.158 (116.119.57.158)  312.373 ms 116.119.57.162 (116.119.57.162)  311.932 ms 116.119.57.152 (116.119.57.152)  312.399 ms
 8  116.51.31.53 (116.51.31.53)  311.960 ms  312.307 ms  312.274 ms
 9  * * *
10  * ae-4.r27.osakjp02.jp.bb.gin.ntt.net (129.250.2.67)  384.927 ms  247.538 ms
11  * * ae-4.r32.tokyjp05.jp.bb.gin.ntt.net (129.250.5.55)  144.360 ms
12  ae-5.r24.sttlwa01.us.bb.gin.ntt.net (129.250.4.142)  225.717 ms ae-5.r25.sttlwa01.us.bb.gin.ntt.net (129.250.3.60)  246.829 ms ae-5.r24.st
tlwa01.us.bb.gin.ntt.net (129.250.4.142)  233.490 ms
13  ae-1.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.207)  243.354 ms ae-0.a03.sttlwa01.us.bb.gin.ntt.net (129.250.2.99)  237.191 ms  244.235 ms
14  ae-0.university-of-washington-pacific-northwest-gigapop.sttlwa01.us.bb.gin.ntt.net (198.104.202.6)  246.844 ms  246.595 ms  246.501 ms
15  ae20--4000.icar-sttl1-2.infra.pnw-gigapop.net (209.124.188.132)  274.585 ms  274.145 ms  274.517 ms
16  et-7-0-0--4000.uwcr-ads-1.infra.washington.edu (209.124.188.133)  267.337 ms  272.717 ms  272.204 ms
17  * * *
18  ae3--36.uwar-uwtc-1.infra.washington.edu (128.95.160.68)  291.516 ms  291.296 ms  290.768 ms
19  www4.cac.washington.edu (128.95.155.198)  292.035 ms  290.694 ms  290.855 ms
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$
```

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

Ans: Yes, Stars can be seen in middle as well as at the end of traceroute results.

Stars that comes in middle can come when the router does not accept icmp packets and does not want to reveal its identity or it can happen that the router buffer is full and it discarded the udp/icmp packet.

Similarly, stars at the end can come because the destination does not accept icmp packets due to security reasons.

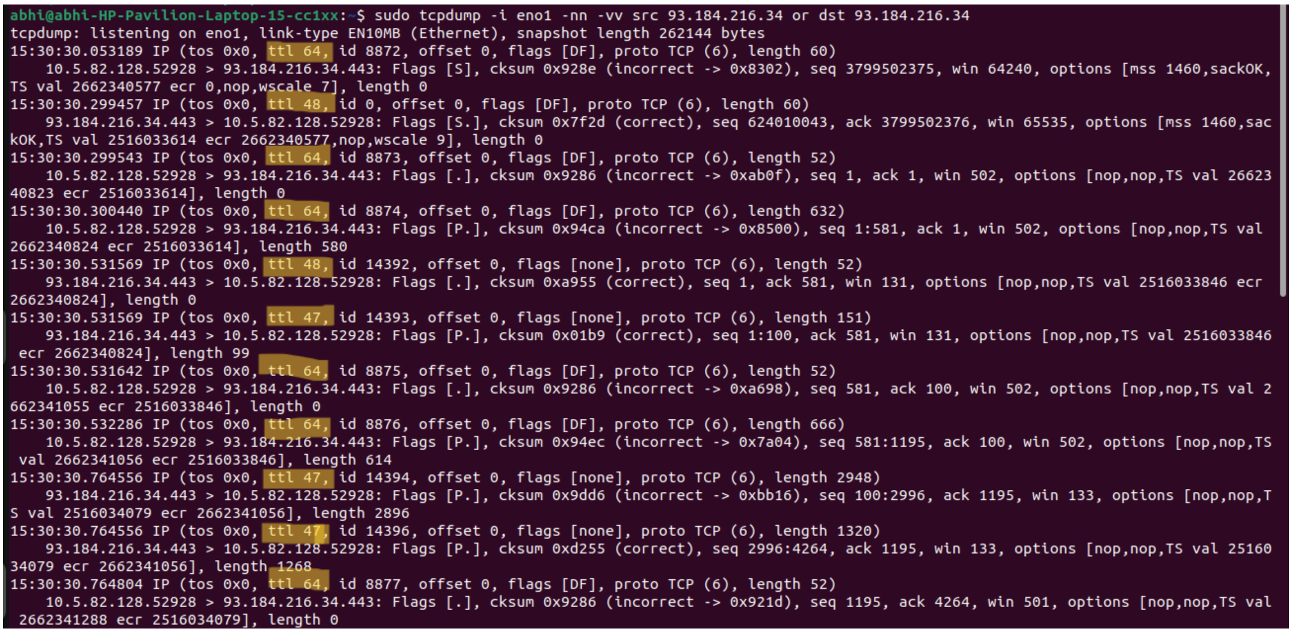
Task-2: Answer Task-1 Q.3, Q.5 and Q.6 using tcpdump instead of wireshark to capture traffic to/from one of the remaining three websites visited as part of Lab-1. [**3 Marks]**

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

Ans: Typical delay between probe packets is 0.3 sec.

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

Ans: IPV4 has TTL field. It defines the number of hops packet can take before reaching destination. Its value is decreased by 1 at each router.
From client side, the ttl value remain 64 for each packets, whereas from host side it changes between 47 and 48.



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ sudo tcpdump -i eno1 -nn -vv src 93.184.216.34 or dst 93.184.216.34
tcpdump: listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:30:30.053189 IP (tos 0x0, ttl 64, id 8872, offset 0, flags [DF], proto TCP (6), length 60)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [S], cksum 0x928e (incorrect -> 0x8302), seq 3799502375, win 64240, options [mss 1460,sackOK,
TS val 2662340577 ecr 0,nop,wscale 7], length 0
15:30:30.299457 IP (tos 0x0, ttl 48, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    93.184.216.34.443 > 10.5.82.128.52928: Flags [S.], cksum 0x7f2d (correct), seq 624010043, ack 3799502376, win 65535, options [mss 1460,sac
kOK,TS val 2516033614 ecr 2662340577,nop,wscale 9], length 0
15:30:30.299543 IP (tos 0x0, ttl 64, id 8873, offset 0, flags [DF], proto TCP (6), length 52)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [.], cksum 0x9286 (incorrect -> 0xab0f), seq 1, ack 1, win 502, options [nop,nop,TS val 26623
40823 ecr 2516033614], length 0
15:30:30.300440 IP (tos 0x0, ttl 64, id 8874, offset 0, flags [DF], proto TCP (6), length 632)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [P.], cksum 0x94ca (incorrect -> 0x8500), seq 1:581, ack 1, win 502, options [nop,nop,TS val
2662340824 ecr 2516033614], length 580
15:30:30.531569 IP (tos 0x0, ttl 48, id 14392, offset 0, flags [none], proto TCP (6), length 52)
    93.184.216.34.443 > 10.5.82.128.52928: Flags [.], cksum 0xa955 (correct), seq 1, ack 581, win 131, options [nop,nop,TS val 2516033846 ecr
2662340824], length 0
15:30:30.531569 IP (tos 0x0, ttl 47, id 14393, offset 0, flags [none], proto TCP (6), length 151)
    93.184.216.34.443 > 10.5.82.128.52928: Flags [P.], cksum 0x01b9 (correct), seq 1:100, ack 581, win 131, options [nop,nop,TS val 2516033846
 ecr 2662340824], length 99
15:30:30.531642 IP (tos 0x0, ttl 64, id 8875, offset 0, flags [DF], proto TCP (6), length 52)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [.], cksum 0x9286 (incorrect -> 0xa698), seq 581, ack 100, win 502, options [nop,nop,TS val 2
662341055 ecr 2516033846], length 0
15:30:30.532286 IP (tos 0x0, ttl 64, id 8876, offset 0, flags [DF], proto TCP (6), length 666)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [P.], cksum 0x94ec (incorrect -> 0x7a04), seq 581:1195, ack 100, win 502, options [nop,nop,TS
 val 2662341056 ecr 2516033846], length 614
15:30:30.764556 IP (tos 0x0, ttl 47, id 14394, offset 0, flags [none], proto TCP (6), length 2948)
    93.184.216.34.443 > 10.5.82.128.52928: Flags [P.], cksum 0x9dd6 (incorrect -> 0xbb16), seq 100:2996, ack 1195, win 133, options [nop,nop,T
S val 2516034079 ecr 2662341056], length 2896
15:30:30.764556 IP (tos 0x0, ttl 47, id 14396, offset 0, flags [none], proto TCP (6), length 1320)
    93.184.216.34.443 > 10.5.82.128.52928: Flags [P.], cksum 0xd255 (correct), seq 2996:4264, ack 1195, win 133, options [nop,nop,TS val 25160
34079 ecr 2662341056], length 1268
15:30:30.764804 IP (tos 0x0, ttl 64, id 8877, offset 0, flags [DF], proto TCP (6), length 52)
    10.5.82.128.52928 > 93.184.216.34.443: Flags [.], cksum 0x9286 (incorrect -> 0x921d), seq 1195, ack 4264, win 501, options [nop,nop,TS val
 2662341288 ecr 2516034079], length 0
```

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

Ans: The output of the tcpdump session took near around 1 sec
We cannot find bottleneck router using tcpdump.

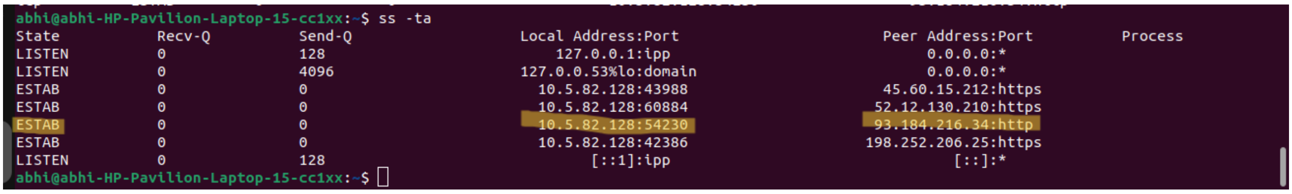
Task-3: Play with netstat or ss, ping and mtr and comment on what you see on wireshark and on terminal. [**5 Marks]**

Ans:

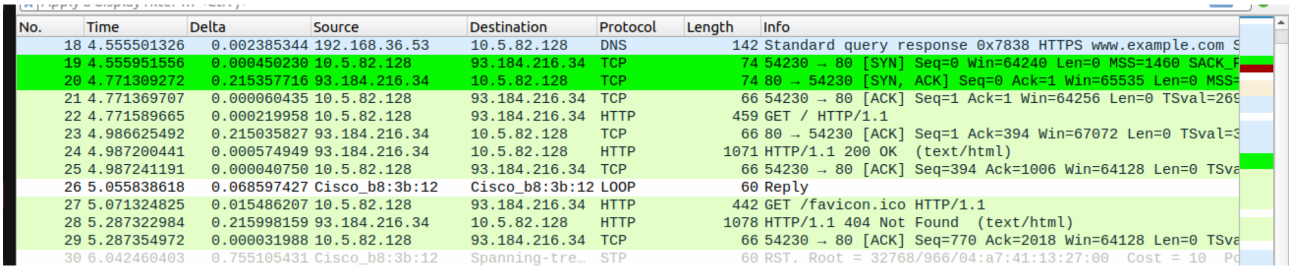
1. SS

When we open www.example.com, with the help of ss command, we can see that a tcp socket connection is established between source and destination.

And in wireshark we can see that tcp 3-way handshake is completed between source and destination.



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ ss -ta
State          Recv-Q          Send-Q                   Local Address:Port                   Peer Address:Port          Process
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                        10.5.82.128:43988                    45.60.15.212:https
ESTAB          0               0                        10.5.82.128:60884                   52.12.130.210:https
ESTAB          0               0                        10.5.82.128:54230                   93.184.216.34:http
ESTAB          0               0                        10.5.82.128:42386                  198.252.206.25:https
LISTEN         0               128                              [::1]:ipp                            [::]:*
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$
```



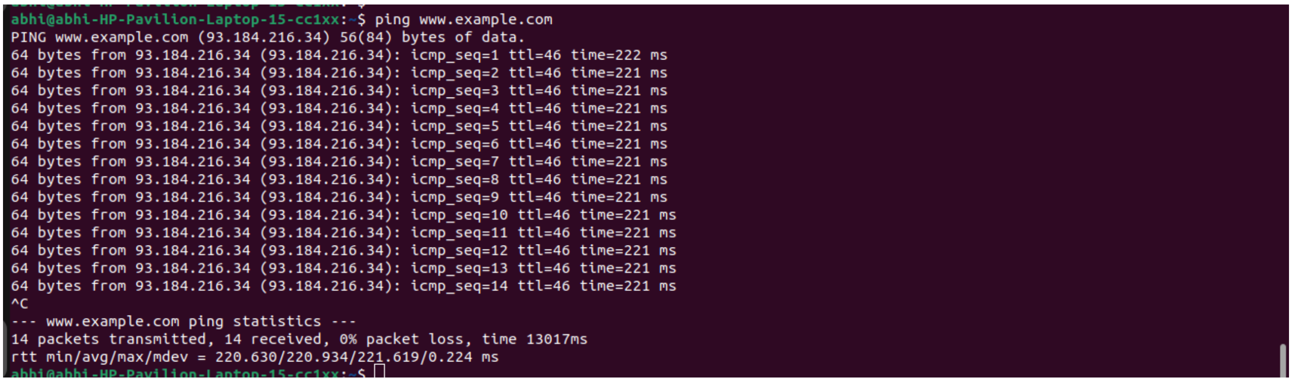
```
No.    Time        Delta       Source          Destination     Protocol Length Info
    18 4.555501326 0.002385344 192.168.36.53   10.5.82.128     DNS         142 Standard query response 0x7838 HTTPS www.example.com S
    19 4.555951556 0.000450230 10.5.82.128     93.184.216.34   TCP          74 54230 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
    20 4.771309272 0.215357716 93.184.216.34   10.5.82.128     TCP          74 80 → 54230 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
    21 4.771369707 0.000060435 10.5.82.128     93.184.216.34   TCP          66 54230 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=269
    22 4.771589665 0.000219958 10.5.82.128     93.184.216.34   HTTP        459 GET / HTTP/1.1
    23 4.986625492 0.215035827 93.184.216.34   10.5.82.128     TCP          66 80 → 54230 [ACK] Seq=1 Ack=394 Win=67072 Len=0 TSval=3
    24 4.987200441 0.000574949 93.184.216.34   10.5.82.128     HTTP       1071 HTTP/1.1 200 OK  (text/html)
    25 4.987241191 0.000040750 10.5.82.128     93.184.216.34   TCP          66 54230 → 80 [ACK] Seq=394 Ack=1006 Win=64128 Len=0 TSva
    26 5.055838618 0.068597427 Cisco_b8:3b:12  Cisco_b8:3b:12  LOOP         60 Reply
    27 5.071324825 0.015486207 10.5.82.128     93.184.216.34   HTTP        442 GET /favicon.ico HTTP/1.1
    28 5.287322984 0.215998159 93.184.216.34   10.5.82.128     HTTP       1078 HTTP/1.1 404 Not Found  (text/html)
    29 5.287354972 0.000031988 10.5.82.128     93.184.216.34   TCP          66 54230 → 80 [ACK] Seq=770 Ack=2018 Win=64128 Len=0 TSva
    30 6.042460403 0.755105431 Cisco_b8:3b:12  Spanning-tre…   STP          60 RST. Root = 32768/966/04:a7:41:13:27:00  Cost = 10  Po
```

2. Ping

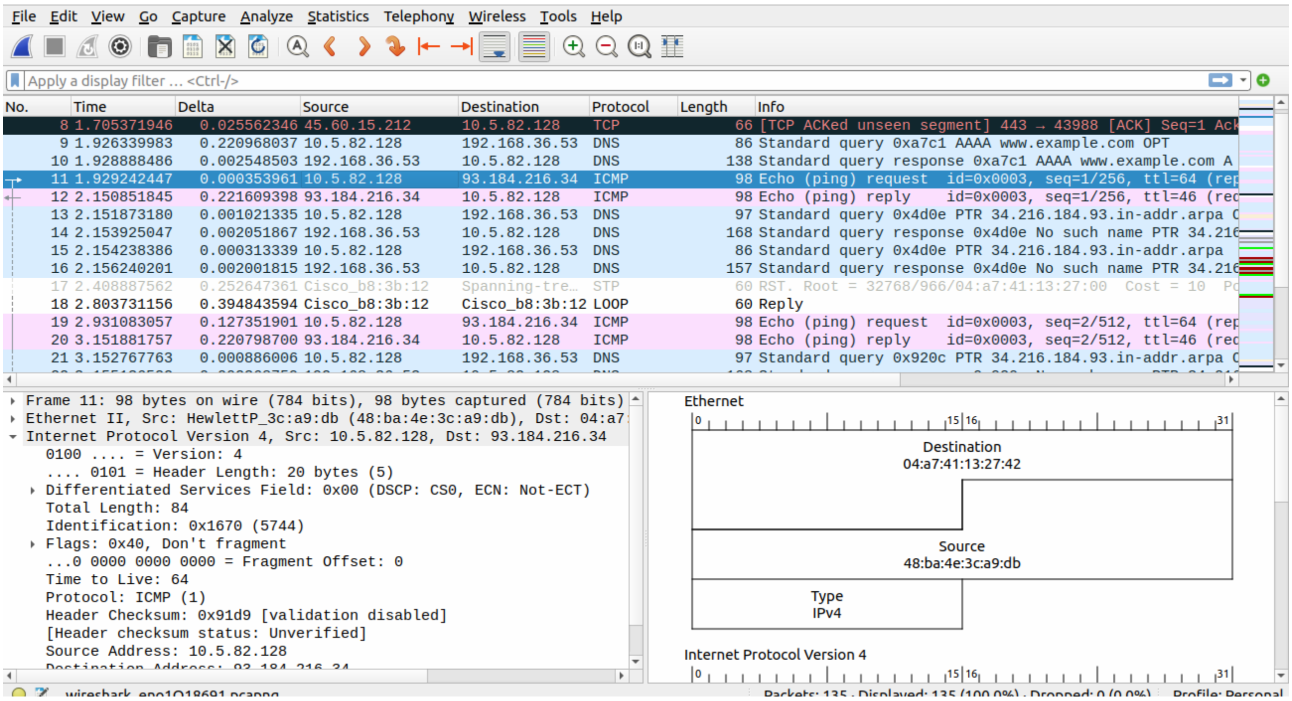
Ping continuosly sends ICMP packets to www.example.com to check connectivity of the packet.

On terminal we can see the ip address of the host, sequence number of icmp packet, TTL and round trip time of packets.

Similarly, on wireshark we can see that ICMP packets are sent and received.



```
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=1 ttl=46 time=222 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=2 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=3 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=4 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=5 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=6 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=7 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=8 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=9 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=10 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=11 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=12 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=13 ttl=46 time=221 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=14 ttl=46 time=221 ms
^C
--- www.example.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13017ms
rtt min/avg/max/mdev = 220.630/220.934/221.619/0.224 ms
abhi@abhi-HP-Pavilion-Laptop-15-cc1xx:~$
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Ethernet
0
15
16
31
Destination
04:a7:41:13:27:42
Source
48:ba:4e:3c:a9:db
Type
IPv4
Internet Protocol Version 4
0
15
16
31

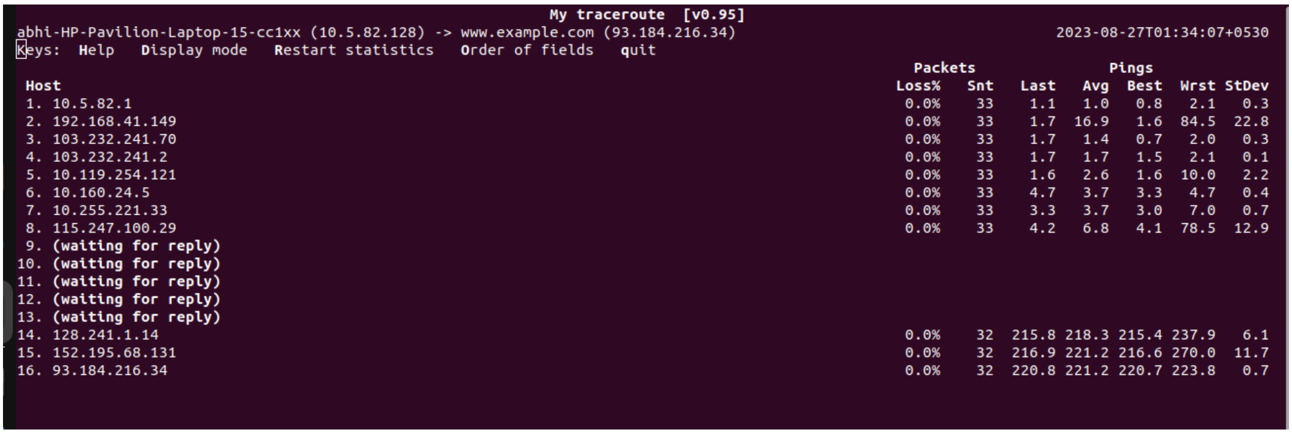
```
No.   Time         Delta       Source          Destination     Protocol Length Info
    8 1.705371946  0.025562346 45.60.15.212    10.5.82.128     TCP       66 [TCP ACKed unseen segment] 443 → 43988 [ACK] Seq=1 Ack
    9 1.926339983  0.220968037 10.5.82.128     192.168.36.53   DNS       86 Standard query 0xa7c1 AAAA www.example.com OPT
   10 1.928888486  0.002548503 192.168.36.53   10.5.82.128     DNS      138 Standard query response 0xa7c1 AAAA www.example.com A
   11 1.929242447  0.000353961 10.5.82.128     93.184.216.34   ICMP      98 Echo (ping) request  id=0x0003, seq=1/256, ttl=64 (rep
   12 2.150851845  0.221609398 93.184.216.34   10.5.82.128     ICMP      98 Echo (ping) reply    id=0x0003, seq=1/256, ttl=46 (rec
   13 2.151873180  0.001021335 10.5.82.128     192.168.36.53   DNS       97 Standard query 0x4d0e PTR 34.216.184.93.in-addr.arpa C
   14 2.153925047  0.002051867 192.168.36.53   10.5.82.128     DNS      168 Standard query response 0x4d0e No such name PTR 34.216
   15 2.154238386  0.000313339 10.5.82.128     192.168.36.53   DNS       86 Standard query 0x4d0e PTR 34.216.184.93.in-addr.arpa
   16 2.156240201  0.002001815 192.168.36.53   10.5.82.128     DNS      157 Standard query response 0x4d0e No such name PTR 34.216
   17 2.408887562  0.252647361 Cisco_b8:3b:12  Spanning-tre…   STP       60 RST. Root = 32768/966/04:a7:41:13:27:00  Cost = 10  Po
   18 2.803731156  0.394843594 Cisco_b8:3b:12  Cisco_b8:3b:12  LOOP      60 Reply
   19 2.931083057  0.127351901 10.5.82.128     93.184.216.34   ICMP      98 Echo (ping) request  id=0x0003, seq=2/512, ttl=64 (rep
   20 3.151881757  0.220798700 93.184.216.34   10.5.82.128     ICMP      98 Echo (ping) reply    id=0x0003, seq=2/512, ttl=46 (rec
   21 3.152767763  0.000886006 10.5.82.128     192.168.36.53   DNS       97 Standard query 0x920c PTR 34.216.184.93.in-addr.arpa C
```

```
▸ Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: HewlettP_3c:a9:db (48:ba:4e:3c:a9:db), Dst: 04:a7
▾ Internet Protocol Version 4, Src: 10.5.82.128, Dst: 93.184.216.34
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x1670 (5744)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x91d9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.5.82.128
```

3. mtr

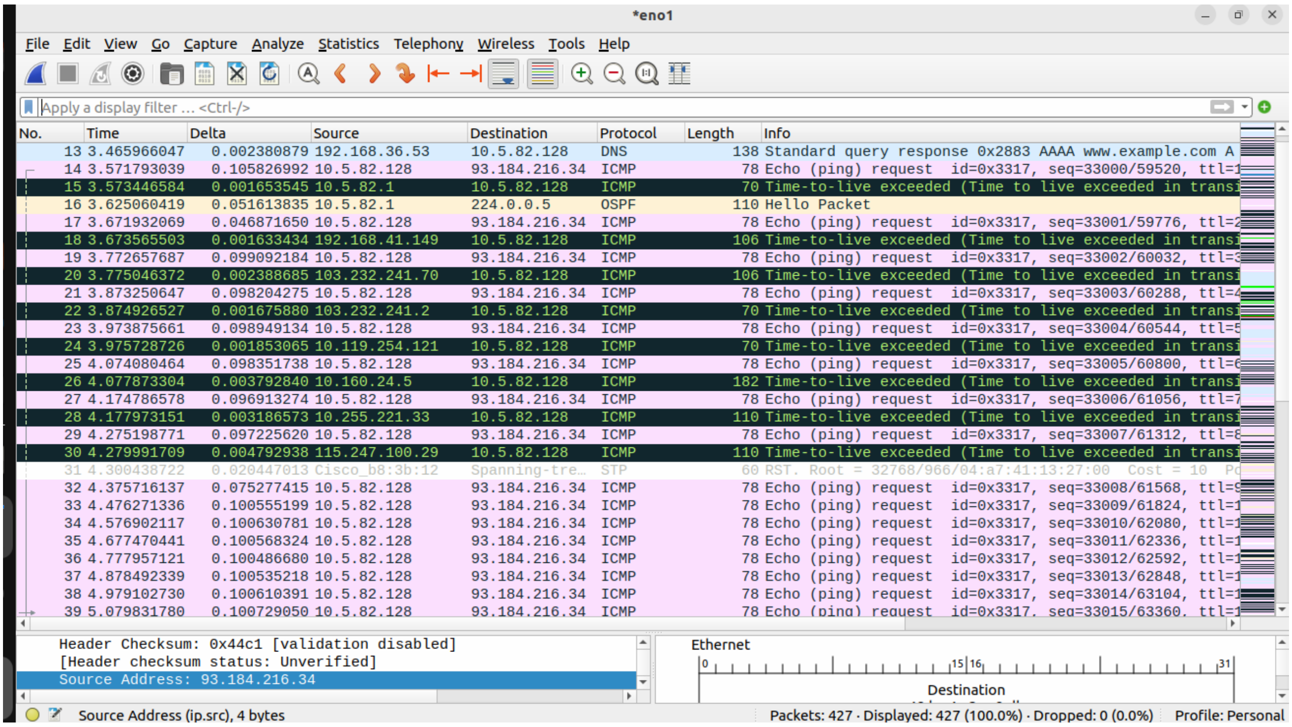
mtr is combination of both traceroute and ping. Therefore, on terminal we can clearly see the path the packets are taking and how much time it is taking. As it also uses ping, we can see that ICMP packets are continuosly sent and mtr gives us a report which gives values like percentage of packets lost, how many packets are sent, best, average, worst RTT time taken by the packets.

In this case we can see that loss % is 0, and best RTT is 220.7ms and worst RTT is 220.8ms.



```
                                          My traceroute  [v0.95]
abhi-HP-Pavilion-Laptop-15-cc1xx (10.5.82.128) -> www.example.com (93.184.216.34)          2023-08-27T01:34:07+0530
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                  Packets               Pings
 Host                                                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.5.82.1                                                    0.0%    33    1.1   1.0   0.8   2.1   0.3
 2. 192.168.41.149                                               0.0%    33    1.7  16.9   1.6  84.5  22.8
 3. 103.232.241.70                                               0.0%    33    1.7   1.4   0.7   2.0   0.3
 4. 103.232.241.2                                                0.0%    33    1.7   1.7   1.5   2.1   0.1
 5. 10.119.254.121                                               0.0%    33    1.6   2.6   1.6  10.0   2.2
 6. 10.160.24.5                                                  0.0%    33    4.7   3.7   3.3   4.7   0.4
 7. 10.255.221.33                                                0.0%    33    3.3   3.7   3.0   7.0   0.7
 8. 115.247.100.29                                               0.0%    33    4.2   6.8   4.1  78.5  12.9
 9. (waiting for reply)
10. (waiting for reply)
11. (waiting for reply)
12. (waiting for reply)
13. (waiting for reply)
14. 128.241.1.14                                                 0.0%    32  215.8 218.3 215.4 237.9   6.1
15. 152.195.68.131                                               0.0%    32  216.9 221.2 216.6 270.0  11.7
16. 93.184.216.34                                                0.0%    32  220.8 221.2 220.7 223.8   0.7
```

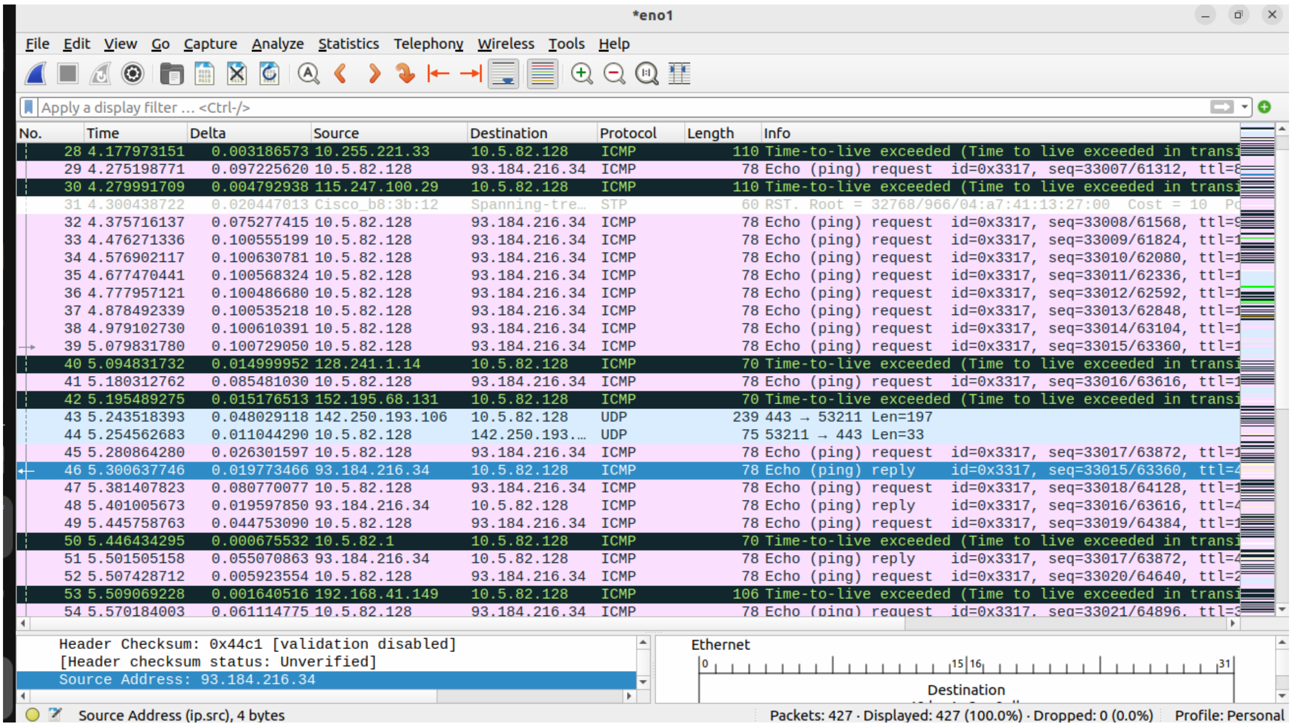
On wireshark, we can see that ICMP packets are sent continuously by increasing TTL values and we can see the response Time to live exceeded wherenever ttl is becoming 0 at any router and we can see ping reply on reaching destination



```
No.  Time        Delta       Source          Destination    Protocol Length Info
  13 3.465966047 0.002380879 192.168.36.53   10.5.82.128    DNS         138 Standard query response 0x2883 AAAA www.example.com A
  14 3.571793039 0.105826992 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33000/59520, ttl=1
  15 3.573446584 0.001653545 10.5.82.1       10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  16 3.625060419 0.051613835 10.5.82.1       224.0.0.5      OSPF        110 Hello Packet
  17 3.671932069 0.046871650 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33001/59776, ttl=2
  18 3.673565503 0.001633434 192.168.41.149  10.5.82.128    ICMP        106 Time-to-live exceeded (Time to live exceeded in transi
  19 3.772657687 0.099092184 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33002/60032, ttl=3
  20 3.775046372 0.002388685 103.232.241.70  10.5.82.128    ICMP        106 Time-to-live exceeded (Time to live exceeded in transi
  21 3.873250647 0.098204275 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33003/60288, ttl=4
  22 3.874926527 0.001675880 103.232.241.2   10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  23 3.973875661 0.098949134 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33004/60544, ttl=5
  24 3.975728726 0.001853065 10.119.254.121  10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  25 4.074080464 0.098351738 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33005/60800, ttl=6
  26 4.077873304 0.003792840 10.160.24.5     10.5.82.128    ICMP        182 Time-to-live exceeded (Time to live exceeded in transi
  27 4.174786578 0.096913274 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33006/61056, ttl=7
  28 4.177973151 0.003186573 10.255.221.33   10.5.82.128    ICMP        110 Time-to-live exceeded (Time to live exceeded in transi
  29 4.275198771 0.097225620 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33007/61312, ttl=8
  30 4.279991709 0.004792938 115.247.100.29  10.5.82.128    ICMP        110 Time-to-live exceeded (Time to live exceeded in transi
  31 4.300438722 0.020447013 Cisco_b8:3b:12  Spanning-tre…  STP          60 RST. Root = 32768/966/04:a7:41:13:27:00  Cost = 10  Po
  32 4.375716137 0.075277415 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33008/61568, ttl=9
  33 4.476271336 0.100555199 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33009/61824, ttl=1
  34 4.576902117 0.100630781 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33010/62080, ttl=1
  35 4.677470441 0.100568324 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33011/62336, ttl=1
  36 4.777957121 0.100486680 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33012/62592, ttl=1
  37 4.878492339 0.100535218 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33013/62848, ttl=1
  38 4.979102730 0.100610391 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33014/63104, ttl=1
  39 5.079831780 0.100729050 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33015/63360, ttl=1
```

```
    Header Checksum: 0x44c1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 93.184.216.34
```

```
Source Address (ip.src), 4 bytes        Packets: 427 · Displayed: 427 (100.0%) · Dropped: 0 (0.0%)    Profile: Personal
```



```
No.  Time        Delta       Source          Destination    Protocol Length Info
  28 4.177973151 0.003186573 10.255.221.33   10.5.82.128    ICMP        110 Time-to-live exceeded (Time to live exceeded in transi
  29 4.275198771 0.097225620 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33007/61312, ttl=8
  30 4.279991709 0.004792938 115.247.100.29  10.5.82.128    ICMP        110 Time-to-live exceeded (Time to live exceeded in transi
  31 4.300438722 0.020447013 Cisco_b8:3b:12  Spanning-tre…  STP          60 RST. Root = 32768/966/04:a7:41:13:27:00  Cost = 10  Po
  32 4.375716137 0.075277415 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33008/61568, ttl=9
  33 4.476271336 0.100555199 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33009/61824, ttl=1
  34 4.576902117 0.100630781 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33010/62080, ttl=1
  35 4.677470441 0.100568324 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33011/62336, ttl=1
  36 4.777957121 0.100486680 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33012/62592, ttl=1
  37 4.878492339 0.100535218 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33013/62848, ttl=1
  38 4.979102730 0.100610391 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33014/63104, ttl=1
  39 5.079831780 0.100729050 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33015/63360, ttl=1
  40 5.094831732 0.014999952 128.241.1.14    10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  41 5.180312762 0.085481030 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33016/63616, ttl=1
  42 5.195489275 0.015176513 152.195.68.131  10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  43 5.243518393 0.048029118 142.250.193.106 10.5.82.128    UDP         239 443 → 53211 Len=197
  44 5.254562683 0.011044290 10.5.82.128     142.250.193.…  UDP          75 53211 → 443 Len=33
  45 5.280864280 0.026301597 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33017/63872, ttl=1
  46 5.300637746 0.019773466 93.184.216.34   10.5.82.128    ICMP         78 Echo (ping) reply    id=0x3317, seq=33015/63360, ttl=4
  47 5.381407823 0.080770077 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33018/64128, ttl=1
  48 5.401005673 0.019597850 93.184.216.34   10.5.82.128    ICMP         78 Echo (ping) reply    id=0x3317, seq=33016/63616, ttl=4
  49 5.445758763 0.044753090 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33019/64384, ttl=1
  50 5.446434295 0.000675532 10.5.82.1       10.5.82.128    ICMP         70 Time-to-live exceeded (Time to live exceeded in transi
  51 5.501505158 0.055070863 93.184.216.34   10.5.82.128    ICMP         78 Echo (ping) reply    id=0x3317, seq=33017/63872, ttl=4
  52 5.507428712 0.005923554 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33020/64640, ttl=2
  53 5.509069228 0.001640516 192.168.41.149  10.5.82.128    ICMP        106 Time-to-live exceeded (Time to live exceeded in transi
  54 5.570184003 0.061114775 10.5.82.128     93.184.216.34  ICMP         78 Echo (ping) request  id=0x3317, seq=33021/64896, ttl=3
```

```
    Header Checksum: 0x44c1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 93.184.216.34
```

```
Source Address (ip.src), 4 bytes        Packets: 427 · Displayed: 427 (100.0%) · Dropped: 0 (0.0%)    Profile: Personal
```