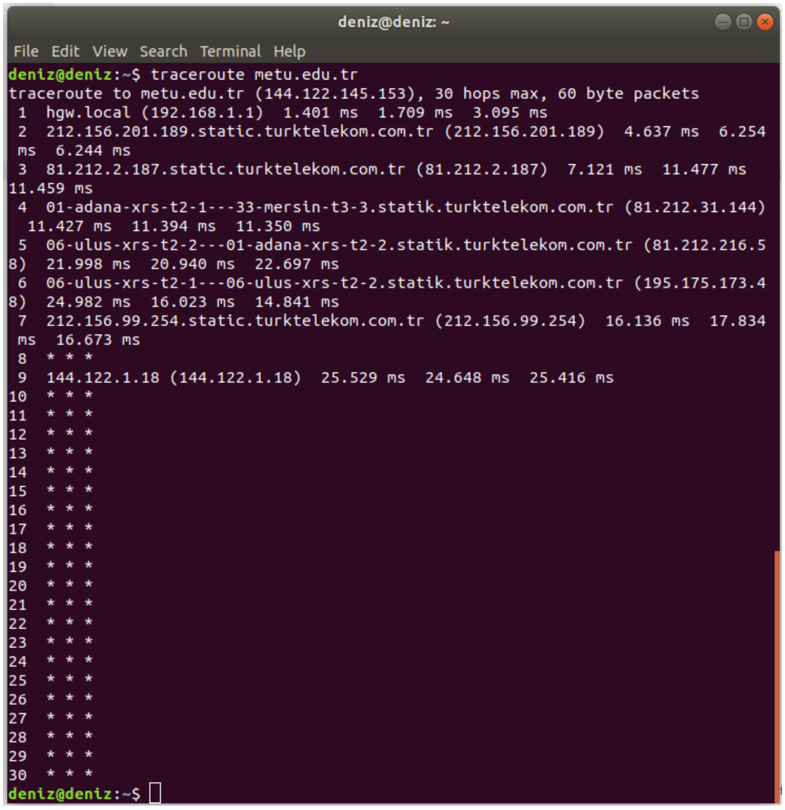
Student Information

Full Name: Deniz Polat
ID Number: 2237790

1 Question 1

As seen in Figure 1, I was not able to see the whole path. (Marked with asterisk. For instance, I cannot see the 8th hop) There might be several reasons that I cannot see some hops.

- As the type of packet might vary due to operating systems, the router's firewall settings might be blocking some type of packets.
- A router might be busy with routing packets so it might not have the resources to send out ICMP packets.
- As tracerouter show only hops having layer 3, there might be several layer 2 (or so) hops running vpn in between, which will be shown to us as one hop.
- A device might be not decrementing IP TTL field value. In such a case, that device would not show up in the path.
- Due to time limitations, a device could be responding "late". In such a case, we could not see that step of the path but asterisk instead.

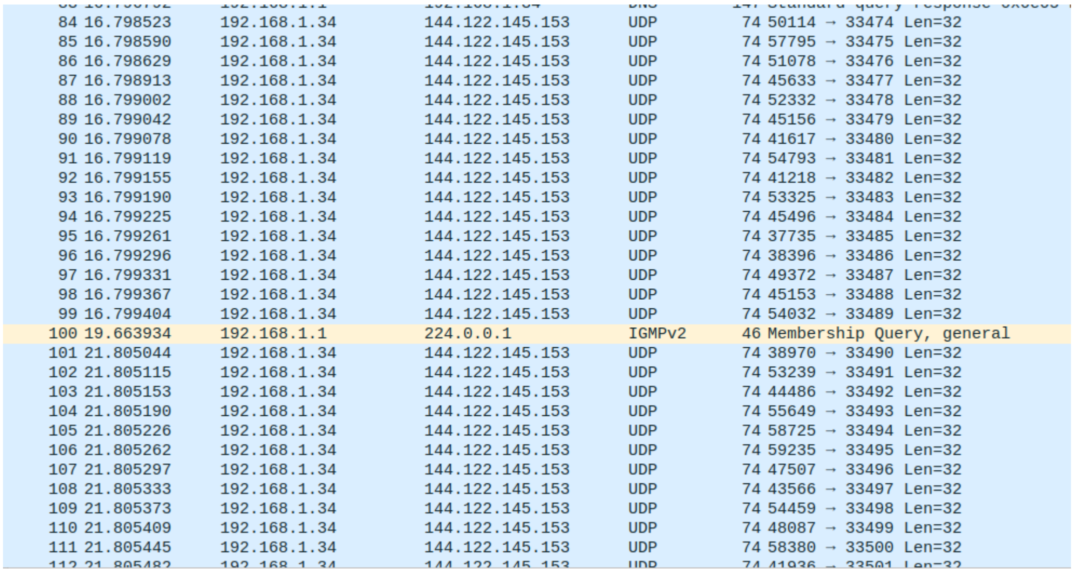


```
deniz@deniz:~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  hgw.local (192.168.1.1)  1.401 ms  1.709 ms  3.095 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  4.637 ms  6.254
 ms  6.244 ms
 3  81.212.2.187.static.turktelekom.com.tr (81.212.2.187)  7.121 ms  11.477 ms
11.459 ms
 4  01-adana-xrs-t2-1---33-mersin-t3-3.statik.turktelekom.com.tr (81.212.31.144)
  11.427 ms  11.394 ms  11.350 ms
 5  06-ulus-xrs-t2-2---01-adana-xrs-t2-2.statik.turktelekom.com.tr (81.212.216.5
8)  21.998 ms  20.940 ms  22.697 ms
 6  06-ulus-xrs-t2-1---06-ulus-xrs-t2-2.statik.turktelekom.com.tr (195.175.173.4
8)  24.982 ms  16.023 ms  14.841 ms
 7  212.156.99.254.static.turktelekom.com.tr (212.156.99.254)  16.136 ms  17.834
 ms  16.673 ms
 8  * * *
 9  144.122.1.18 (144.122.1.18)  25.529 ms  24.648 ms  25.416 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
deniz@deniz:~$ 
```

Figure 1: Output of Traceroute Program

2 Question 2

As stated in manual of tracerouter, the default method is sending probe packets as udp datagrams. It is explained in the manual as:
Probe packets are udp datagrams with so-called "unlikely" destination ports. The "unlikely" port of the first probe is 33434, then for each next probe it is incremented by one. Since the ports are expected to be unused, the destination host normally returns "icmp unreach port" as a final response. (Nobody knows what happens when some application listens for such ports, though).
We can also prove that the default mode uses udp from the capture snippet in Figure 2 (packages are sent as udp).

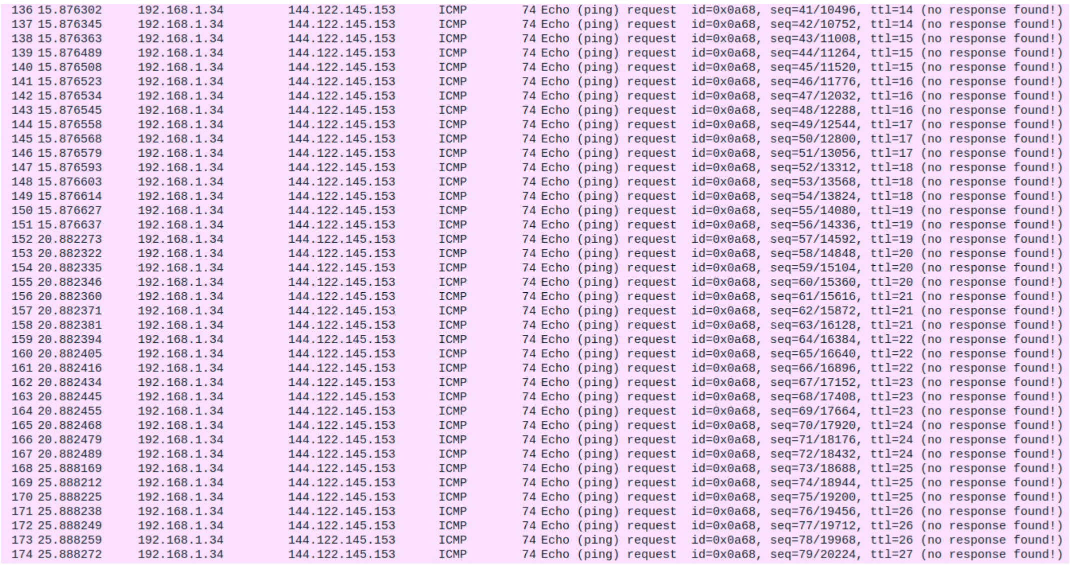


```
 84 16.798523   192.168.1.34   144.122.145.153   UDP      74 50114 → 33474 Len=32
 85 16.798590   192.168.1.34   144.122.145.153   UDP      74 57795 → 33475 Len=32
 86 16.798629   192.168.1.34   144.122.145.153   UDP      74 51078 → 33476 Len=32
 87 16.798913   192.168.1.34   144.122.145.153   UDP      74 45633 → 33477 Len=32
 88 16.799002   192.168.1.34   144.122.145.153   UDP      74 52332 → 33478 Len=32
 89 16.799042   192.168.1.34   144.122.145.153   UDP      74 45156 → 33479 Len=32
 90 16.799078   192.168.1.34   144.122.145.153   UDP      74 41617 → 33480 Len=32
 91 16.799119   192.168.1.34   144.122.145.153   UDP      74 54793 → 33481 Len=32
 92 16.799155   192.168.1.34   144.122.145.153   UDP      74 41218 → 33482 Len=32
 93 16.799190   192.168.1.34   144.122.145.153   UDP      74 53325 → 33483 Len=32
 94 16.799225   192.168.1.34   144.122.145.153   UDP      74 45496 → 33484 Len=32
 95 16.799261   192.168.1.34   144.122.145.153   UDP      74 37735 → 33485 Len=32
 96 16.799296   192.168.1.34   144.122.145.153   UDP      74 38396 → 33486 Len=32
 97 16.799331   192.168.1.34   144.122.145.153   UDP      74 49372 → 33487 Len=32
 98 16.799367   192.168.1.34   144.122.145.153   UDP      74 45153 → 33488 Len=32
 99 16.799404   192.168.1.34   144.122.145.153   UDP      74 54032 → 33489 Len=32
100 19.663934   192.168.1.1    224.0.0.1         IGMPv2   46 Membership Query, general
101 21.805044   192.168.1.34   144.122.145.153   UDP      74 38970 → 33490 Len=32
102 21.805115   192.168.1.34   144.122.145.153   UDP      74 53239 → 33491 Len=32
103 21.805153   192.168.1.34   144.122.145.153   UDP      74 44486 → 33492 Len=32
104 21.805190   192.168.1.34   144.122.145.153   UDP      74 55649 → 33493 Len=32
105 21.805226   192.168.1.34   144.122.145.153   UDP      74 58725 → 33494 Len=32
106 21.805262   192.168.1.34   144.122.145.153   UDP      74 59235 → 33495 Len=32
107 21.805297   192.168.1.34   144.122.145.153   UDP      74 47507 → 33496 Len=32
108 21.805333   192.168.1.34   144.122.145.153   UDP      74 43566 → 33497 Len=32
109 21.805373   192.168.1.34   144.122.145.153   UDP      74 54459 → 33498 Len=32
110 21.805409   192.168.1.34   144.122.145.153   UDP      74 48087 → 33499 Len=32
111 21.805445   192.168.1.34   144.122.145.153   UDP      74 58380 → 33500 Len=32
112 21.805482   192.168.1.34   144.122.145.153   UDP      74 41936 → 33501 Len=32
```

Figure 2: A snippet of Wireshark Captures

3 Question 3

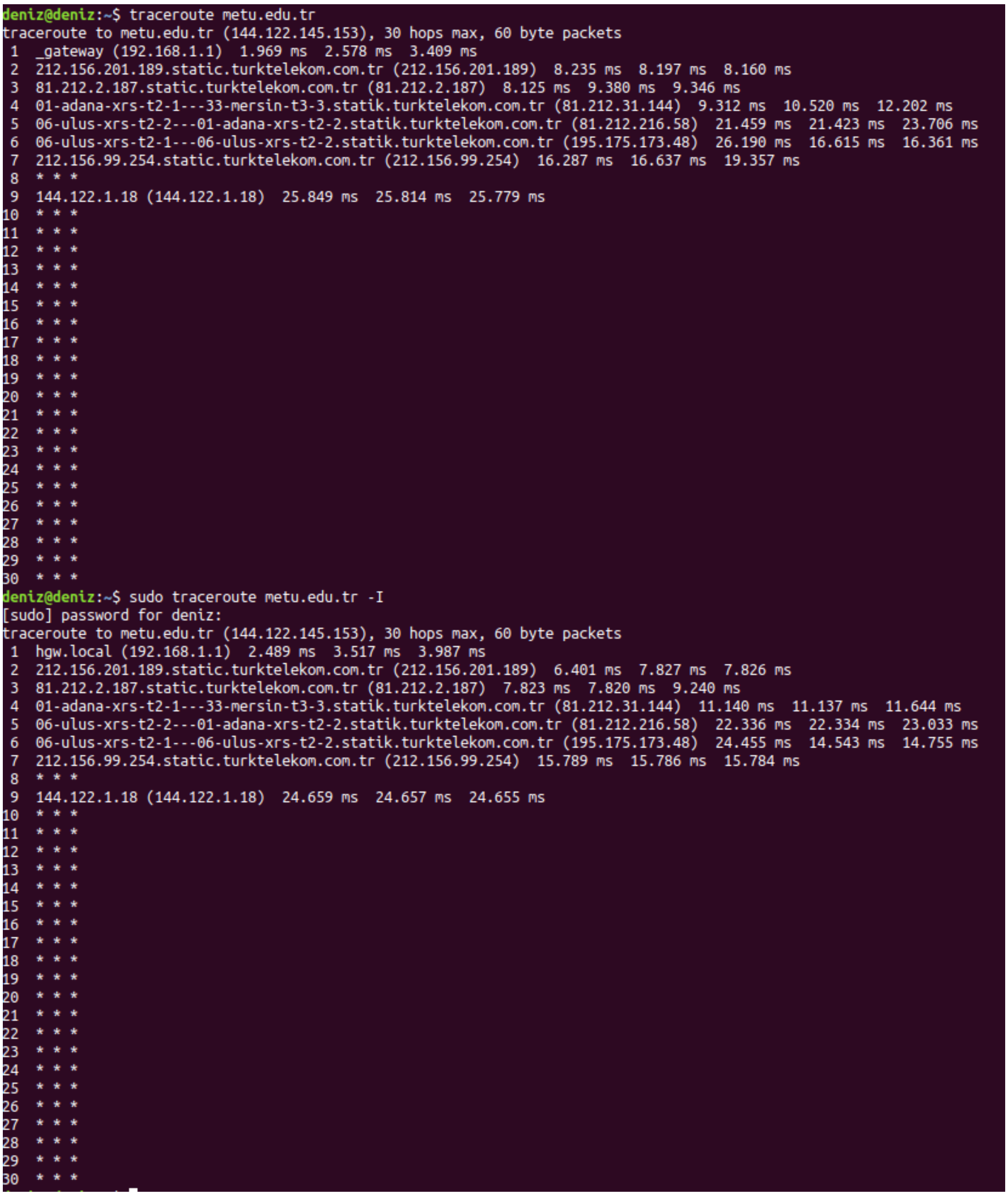
-I flag changes tracerouter method by making tracerouter use ICMP echo for probes, which can also be seen in the capture snippet given in Figure 3.



```
136 15.876302   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=41/10496, ttl=14 (no response found!)
137 15.876345   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=42/10752, ttl=14 (no response found!)
138 15.876363   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=43/11008, ttl=15 (no response found!)
139 15.876489   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=44/11264, ttl=15 (no response found!)
140 15.876508   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=45/11520, ttl=15 (no response found!)
141 15.876523   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=46/11776, ttl=16 (no response found!)
142 15.876534   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=47/12032, ttl=16 (no response found!)
143 15.876545   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=48/12288, ttl=16 (no response found!)
144 15.876558   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=49/12544, ttl=17 (no response found!)
145 15.876568   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=50/12800, ttl=17 (no response found!)
146 15.876579   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=51/13056, ttl=17 (no response found!)
147 15.876593   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=52/13312, ttl=18 (no response found!)
148 15.876603   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=53/13568, ttl=18 (no response found!)
149 15.876614   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=54/13824, ttl=18 (no response found!)
150 15.876627   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=55/14080, ttl=19 (no response found!)
151 15.876637   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=56/14336, ttl=19 (no response found!)
152 20.882273   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=57/14592, ttl=19 (no response found!)
153 20.882322   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=58/14848, ttl=20 (no response found!)
154 20.882335   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=59/15104, ttl=20 (no response found!)
155 20.882346   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=60/15360, ttl=20 (no response found!)
156 20.882360   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=61/15616, ttl=21 (no response found!)
157 20.882371   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=62/15872, ttl=21 (no response found!)
158 20.882381   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=63/16128, ttl=21 (no response found!)
159 20.882394   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=64/16384, ttl=22 (no response found!)
160 20.882405   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=65/16640, ttl=22 (no response found!)
161 20.882416   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=66/16896, ttl=22 (no response found!)
162 20.882434   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=67/17152, ttl=23 (no response found!)
163 20.882445   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=68/17408, ttl=23 (no response found!)
164 20.882455   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=69/17664, ttl=23 (no response found!)
165 20.882468   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=70/17920, ttl=24 (no response found!)
166 20.882479   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=71/18176, ttl=24 (no response found!)
167 20.882489   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=72/18432, ttl=24 (no response found!)
168 25.888169   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=73/18688, ttl=25 (no response found!)
169 25.888212   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=74/18944, ttl=25 (no response found!)
170 25.888225   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=75/19200, ttl=25 (no response found!)
171 25.888238   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=76/19456, ttl=26 (no response found!)
172 25.888249   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=77/19712, ttl=26 (no response found!)
173 25.888259   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=78/19968, ttl=26 (no response found!)
174 25.888272   192.168.1.34   144.122.145.153   ICMP   74 Echo (ping) request  id=0x0a68, seq=79/20224, ttl=27 (no response found!)
```

Figure 3: A snippet of Wireshark Captures with -I flag

As seen in Figure 4, although I could not observe any changes in my path (I think, the reason why I observe the same path for both options is that metu.edu.tr has blocked both udp and icmp), the reason of a possible change in path might be that router or internal devices might be filtering or blocking icmp echo / udp requests.



```
deniz@deniz:~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  1.969 ms  2.578 ms  3.409 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  8.235 ms  8.197 ms  8.160 ms
 3  81.212.2.187.static.turktelekom.com.tr (81.212.2.187)  8.125 ms  9.380 ms  9.346 ms
 4  01-adana-xrs-t2-1---33-mersin-t3-3.statik.turktelekom.com.tr (81.212.31.144)  9.312 ms  10.520 ms  12.202 ms
 5  06-ulus-xrs-t2-2---01-adana-xrs-t2-2.statik.turktelekom.com.tr (81.212.216.58)  21.459 ms  21.423 ms  23.706 ms
 6  06-ulus-xrs-t2-1---06-ulus-xrs-t2-2.statik.turktelekom.com.tr (195.175.173.48)  26.190 ms  16.615 ms  16.361 ms
 7  212.156.99.254.static.turktelekom.com.tr (212.156.99.254)  16.287 ms  16.637 ms  19.357 ms
 8  * * *
 9  144.122.1.18 (144.122.1.18)  25.849 ms  25.814 ms  25.779 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
deniz@deniz:~$ sudo traceroute metu.edu.tr -I
[sudo] password for deniz:
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  hgw.local (192.168.1.1)  2.489 ms  3.517 ms  3.987 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  6.401 ms  7.827 ms  7.826 ms
 3  81.212.2.187.static.turktelekom.com.tr (81.212.2.187)  7.823 ms  7.820 ms  9.240 ms
 4  01-adana-xrs-t2-1---33-mersin-t3-3.statik.turktelekom.com.tr (81.212.31.144)  11.140 ms  11.137 ms  11.644 ms
 5  06-ulus-xrs-t2-2---01-adana-xrs-t2-2.statik.turktelekom.com.tr (81.212.216.58)  22.336 ms  22.334 ms  23.033 ms
 6  06-ulus-xrs-t2-1---06-ulus-xrs-t2-2.statik.turktelekom.com.tr (195.175.173.48)  24.455 ms  14.543 ms  14.755 ms
 7  212.156.99.254.static.turktelekom.com.tr (212.156.99.254)  15.789 ms  15.786 ms  15.784 ms
 8  * * *
 9  144.122.1.18 (144.122.1.18)  24.659 ms  24.657 ms  24.655 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 4: Comparison of Default and ICMP Mode

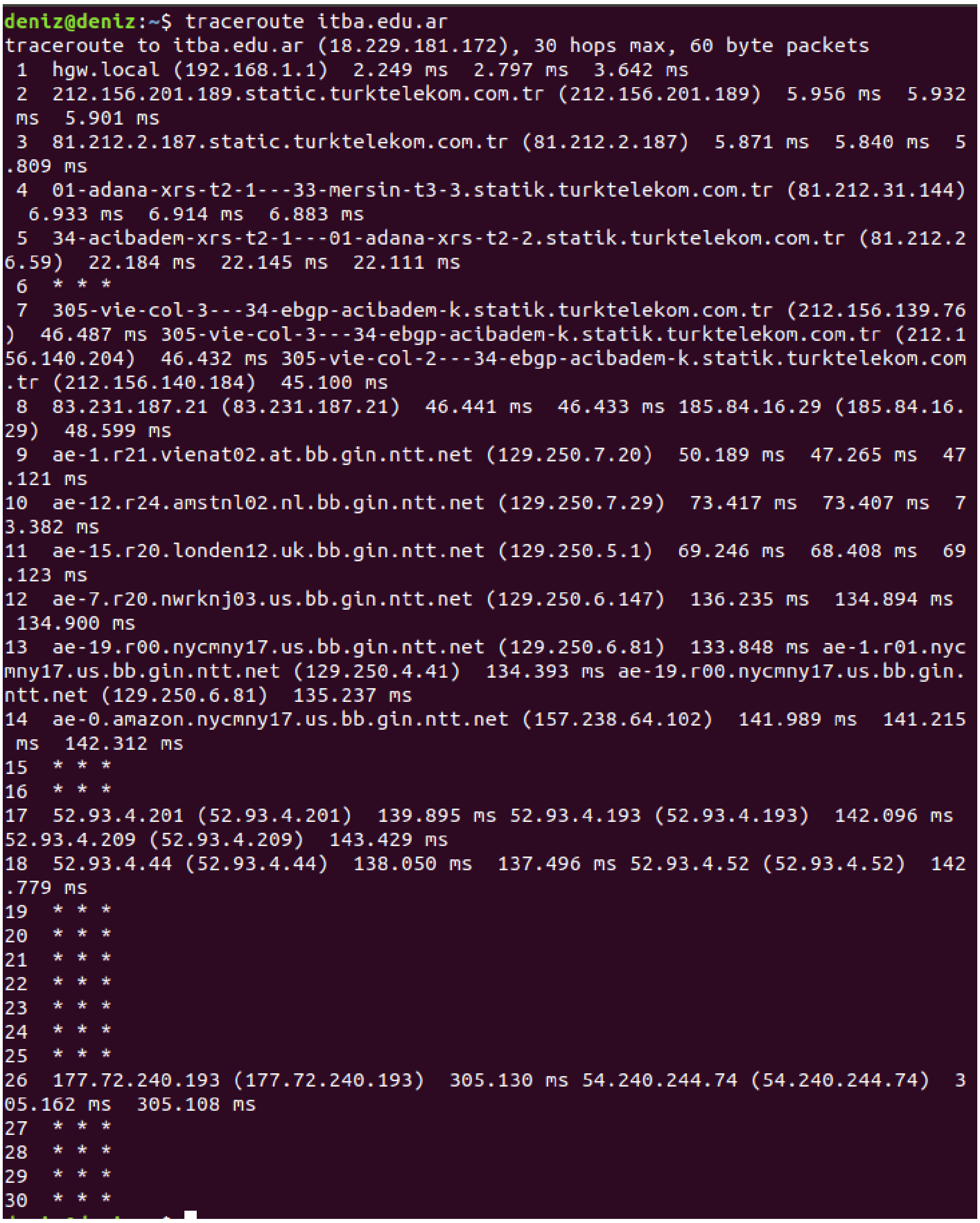
4 Question 4

The university that I have chosen from Argentina is Universidad Nacional de Quilmes, which has the website unq.edu.ar (207.248.74.50)

The university that I have chosen from Malaysia is Universiti Putra Malaysia, which has the website upm.edu.my (211.25.98.234)

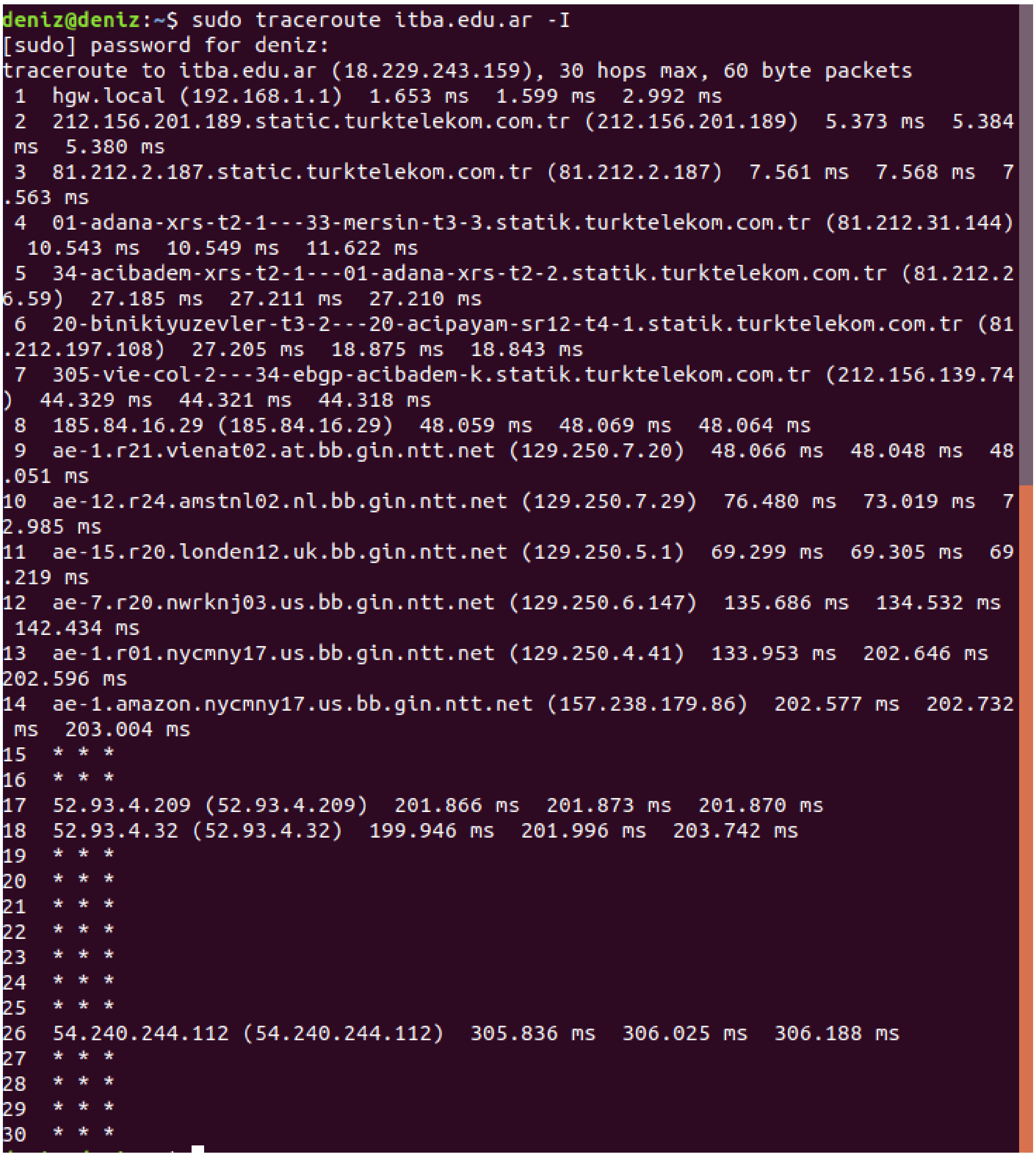
4.1 Bonus

As seen in Figure 5 & 6, I could not reach the itba.edu.ar website using given traceroute commands.



```
deniz@deniz:~$ traceroute itba.edu.ar
traceroute to itba.edu.ar (18.229.181.172), 30 hops max, 60 byte packets
 1  hgw.local (192.168.1.1)  2.249 ms  2.797 ms  3.642 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  5.956 ms  5.932
 ms  5.901 ms
 3  81.212.2.187.static.turktelekom.com.tr (81.212.2.187)  5.871 ms  5.840 ms  5
.809 ms
 4  01-adana-xrs-t2-1---33-mersin-t3-3.statik.turktelekom.com.tr (81.212.31.144)
  6.933 ms  6.914 ms  6.883 ms
 5  34-acibadem-xrs-t2-1---01-adana-xrs-t2-2.statik.turktelekom.com.tr (81.212.2
6.59)  22.184 ms  22.145 ms  22.111 ms
 6  * * *
 7  305-vie-col-3---34-ebgp-acibadem-k.statik.turktelekom.com.tr (212.156.139.76
)  46.487 ms 305-vie-col-3---34-ebgp-acibadem-k.statik.turktelekom.com.tr (212.1
56.140.204)  46.432 ms 305-vie-col-2---34-ebgp-acibadem-k.statik.turktelekom.com
.tr (212.156.140.184)  45.100 ms
 8  83.231.187.21 (83.231.187.21)  46.441 ms  46.433 ms 185.84.16.29 (185.84.16.
29)  48.599 ms
 9  ae-1.r21.vienat02.at.bb.gin.ntt.net (129.250.7.20)  50.189 ms  47.265 ms  47
.121 ms
10  ae-12.r24.amstnl02.nl.bb.gin.ntt.net (129.250.7.29)  73.417 ms  73.407 ms  7
3.382 ms
11  ae-15.r20.londen12.uk.bb.gin.ntt.net (129.250.5.1)  69.246 ms  68.408 ms  69
.123 ms
12  ae-7.r20.nwrknj03.us.bb.gin.ntt.net (129.250.6.147)  136.235 ms  134.894 ms
 134.900 ms
13  ae-19.r00.nycmny17.us.bb.gin.ntt.net (129.250.6.81)  133.848 ms ae-1.r01.nyc
mny17.us.bb.gin.ntt.net (129.250.4.41)  134.393 ms ae-19.r00.nycmny17.us.bb.gin.
ntt.net (129.250.6.81)  135.237 ms
14  ae-0.amazon.nycmny17.us.bb.gin.ntt.net (157.238.64.102)  141.989 ms  141.215
 ms  142.312 ms
15  * * *
16  * * *
17  52.93.4.201 (52.93.4.201)  139.895 ms 52.93.4.193 (52.93.4.193)  142.096 ms
52.93.4.209 (52.93.4.209)  143.429 ms
18  52.93.4.44 (52.93.4.44)  138.050 ms  137.496 ms 52.93.4.52 (52.93.4.52)  142
.779 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  177.72.240.193 (177.72.240.193)  305.130 ms 54.240.244.74 (54.240.244.74)  3
05.162 ms  305.108 ms
27  * * *
28  * * *
29  * * *
30  * * *
```

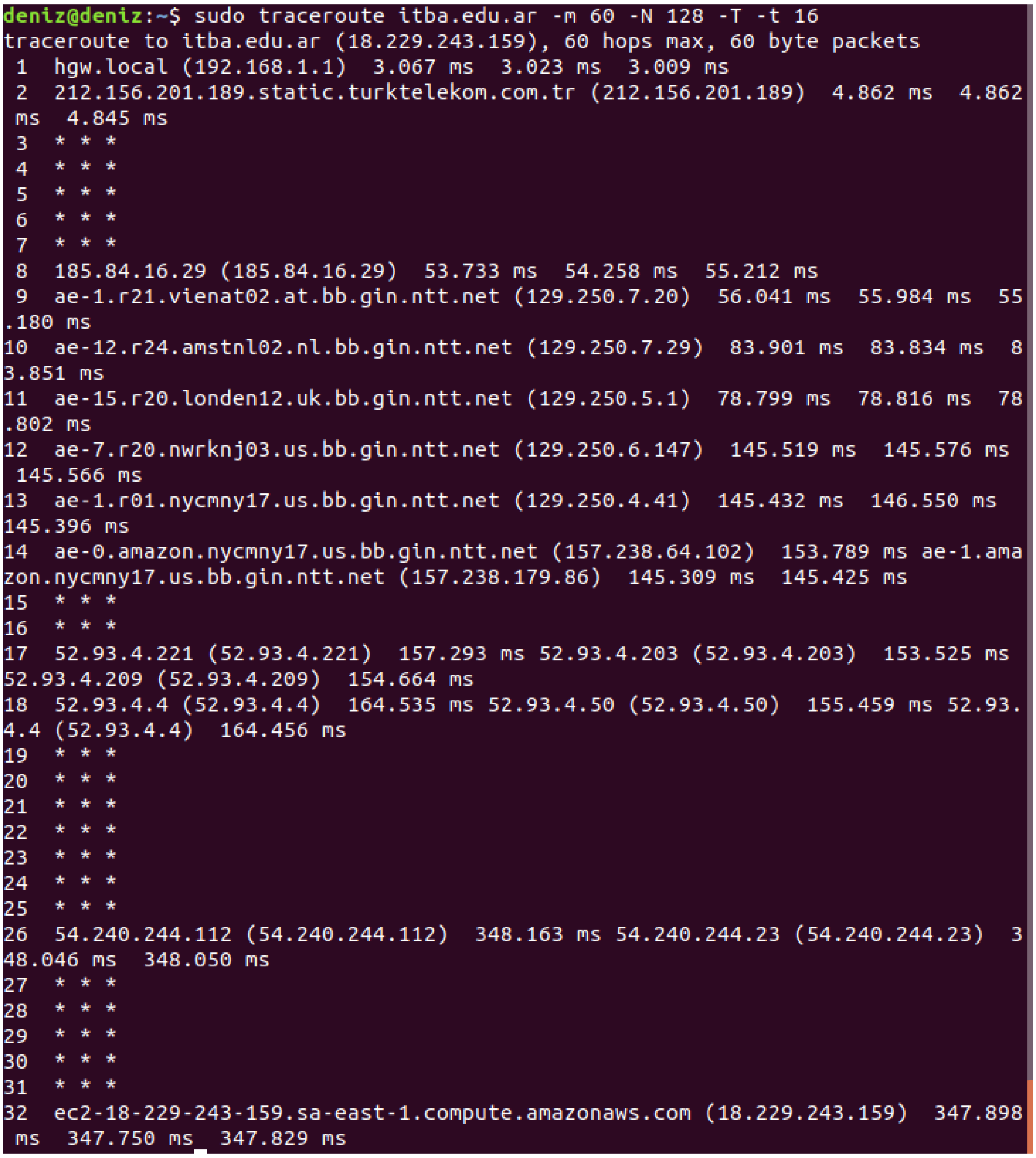
Figure 5: tranceroute itba.edu.ar



```
deniz@deniz:~$ sudo traceroute itba.edu.ar -I
[sudo] password for deniz:
traceroute to itba.edu.ar (18.229.243.159), 30 hops max, 60 byte packets
 1  hgw.local (192.168.1.1)  1.653 ms  1.599 ms  2.992 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  5.373 ms  5.384
 ms  5.380 ms
 3  81.212.2.187.static.turktelekom.com.tr (81.212.2.187)  7.561 ms  7.568 ms  7
.563 ms
 4  01-adana-xrs-t2-1---33-mersin-t3-3.statik.turktelekom.com.tr (81.212.31.144)
  10.543 ms  10.549 ms  11.622 ms
 5  34-acibadem-xrs-t2-1---01-adana-xrs-t2-2.statik.turktelekom.com.tr (81.212.2
6.59)  27.185 ms  27.211 ms  27.210 ms
 6  20-binikiyuzevler-t3-2---20-acipayam-sr12-t4-1.statik.turktelekom.com.tr (81
.212.197.108)  27.205 ms  18.875 ms  18.843 ms
 7  305-vie-col-2---34-ebgp-acibadem-k.statik.turktelekom.com.tr (212.156.139.74
)  44.329 ms  44.321 ms  44.318 ms
 8  185.84.16.29 (185.84.16.29)  48.059 ms  48.069 ms  48.064 ms
 9  ae-1.r21.vienat02.at.bb.gin.ntt.net (129.250.7.20)  48.066 ms  48.048 ms  48
.051 ms
10  ae-12.r24.amstnl02.nl.bb.gin.ntt.net (129.250.7.29)  76.480 ms  73.019 ms  7
2.985 ms
11  ae-15.r20.londen12.uk.bb.gin.ntt.net (129.250.5.1)  69.299 ms  69.305 ms  69
.219 ms
12  ae-7.r20.nwrknj03.us.bb.gin.ntt.net (129.250.6.147)  135.686 ms  134.532 ms
 142.434 ms
13  ae-1.r01.nycmny17.us.bb.gin.ntt.net (129.250.4.41)  133.953 ms  202.646 ms
202.596 ms
14  ae-1.amazon.nycmny17.us.bb.gin.ntt.net (157.238.179.86)  202.577 ms  202.732
 ms  203.004 ms
15  * * *
16  * * *
17  52.93.4.209 (52.93.4.209)  201.866 ms  201.873 ms  201.870 ms
18  52.93.4.32 (52.93.4.32)  199.946 ms  201.996 ms  203.742 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  54.240.244.112 (54.240.244.112)  305.836 ms  306.025 ms  306.188 ms
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 6: tranceroute itba.edu.ar -I

Yet, as seen in Figure 7, I could reach the desired destination by using other options.



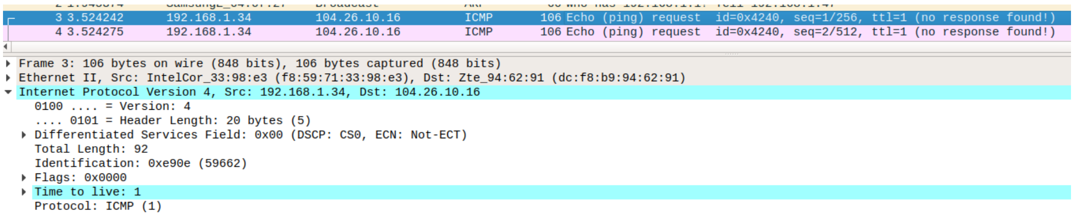
```
deniz@deniz:~$ sudo traceroute itba.edu.ar -m 60 -N 128 -T -t 16
traceroute to itba.edu.ar (18.229.243.159), 60 hops max, 60 byte packets
 1  hgw.local (192.168.1.1)  3.067 ms  3.023 ms  3.009 ms
 2  212.156.201.189.static.turktelekom.com.tr (212.156.201.189)  4.862 ms  4.862
 ms  4.845 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  185.84.16.29 (185.84.16.29)  53.733 ms  54.258 ms  55.212 ms
 9  ae-1.r21.vienat02.at.bb.gin.ntt.net (129.250.7.20)  56.041 ms  55.984 ms  55
.180 ms
10  ae-12.r24.amstnl02.nl.bb.gin.ntt.net (129.250.7.29)  83.901 ms  83.834 ms  8
3.851 ms
11  ae-15.r20.londen12.uk.bb.gin.ntt.net (129.250.5.1)  78.799 ms  78.816 ms  78
.802 ms
12  ae-7.r20.nwrknj03.us.bb.gin.ntt.net (129.250.6.147)  145.519 ms  145.576 ms
 145.566 ms
13  ae-1.r01.nycmny17.us.bb.gin.ntt.net (129.250.4.41)  145.432 ms  146.550 ms
145.396 ms
14  ae-0.amazon.nycmny17.us.bb.gin.ntt.net (157.238.64.102)  153.789 ms ae-1.ama
zon.nycmny17.us.bb.gin.ntt.net (157.238.179.86)  145.309 ms  145.425 ms
15  * * *
16  * * *
17  52.93.4.221 (52.93.4.221)  157.293 ms 52.93.4.203 (52.93.4.203)  153.525 ms
52.93.4.209 (52.93.4.209)  154.664 ms
18  52.93.4.4 (52.93.4.4)  164.535 ms 52.93.4.50 (52.93.4.50)  155.459 ms 52.93.
4.4 (52.93.4.4)  164.456 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  54.240.244.112 (54.240.244.112)  348.163 ms 54.240.244.23 (54.240.244.23)  3
48.046 ms  348.050 ms
27  * * *
28  * * *
29  * * *
30  * * *
31  * * *
32  ec2-18-229-243-159.sa-east-1.compute.amazonaws.com (18.229.243.159)  347.898
 ms  347.750 ms  347.829 ms
```

Figure 7: sudo traceroute itba.edu.ar -m 60 -N 128 -T -t 16

I obtained the required result by trying different options. From everything that I tried, incluing failures, I assume itba.edu.ar disabled both icmp and udp packets but not tcp, thats why it worked with -T flag.
I added -m 60 to see more hops and -N 128 to speed up process. With -t 16, I set type of service value to 16 (low delay).

5 Question 5

As seen in last line in Figure 8, protocol value of first sent ICMP packet is 1 (As Protocol is ICMP(1))



```
   3 3.524242   192.168.1.34   104.26.10.16   ICMP   106 Echo (ping) request  id=0x4240, seq=1/256, ttl=1 (no response found!)
   4 3.524275   192.168.1.34   104.26.10.16   ICMP   106 Echo (ping) request  id=0x4240, seq=2/512, ttl=1 (no response found!)

▸ Frame 3: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
▸ Ethernet II, Src: IntelCor_33:98:e3 (f8:59:71:33:98:e3), Dst: Zte_94:62:91 (dc:f8:b9:94:62:91)
▾ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 104.26.10.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xe90e (59662)
  ▸ Flags: 0x0000
  ▸ Time to live: 1
    Protocol: ICMP (1)
```

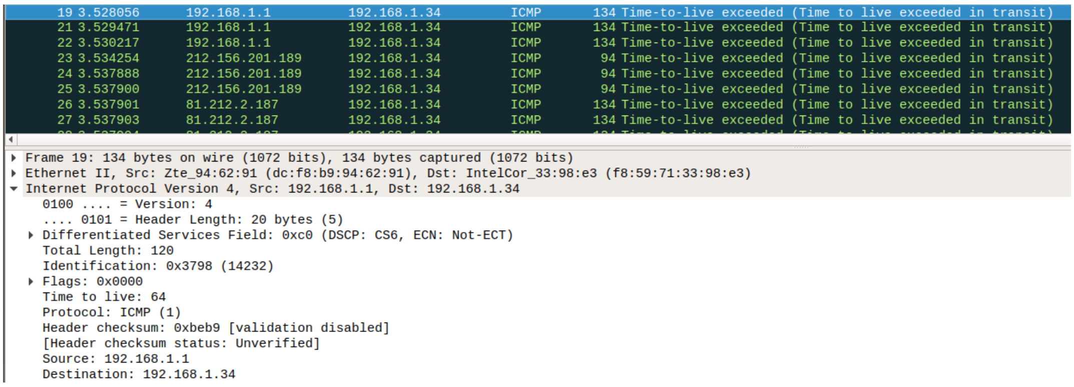
Figure 8: First sent ICMP Packet Header

6 Question 6

Again, as seen in Figure 8, length of IP header is 20 bytes. Since total length is 92 bytes and 20 of them is header, payload of datagram is 92 - 20 = 72 bytes.

7 Question 7

According to Figure 9, the value of identification field is 0x3798 in hex (14232 in decimal) and the value of TTL field is 64. For same source-destination couples, both identification and ttl values are same. Nevertheless, when source or destination changes, both of these two values also change. All source-destination couples occur 3 times in the list, which I assume by looking at terminal results, traceroute sends 3 packages to take average of trip time.



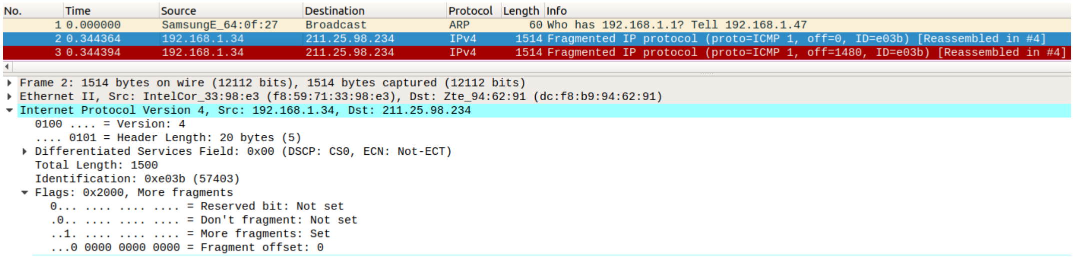
```
  19 3.528056   192.168.1.1      192.168.1.34   ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
  21 3.529471   192.168.1.1      192.168.1.34   ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
  22 3.530217   192.168.1.1      192.168.1.34   ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
  23 3.534254   212.156.201.189  192.168.1.34   ICMP    94 Time-to-live exceeded (Time to live exceeded in transit)
  24 3.537888   212.156.201.189  192.168.1.34   ICMP    94 Time-to-live exceeded (Time to live exceeded in transit)
  25 3.537900   212.156.201.189  192.168.1.34   ICMP    94 Time-to-live exceeded (Time to live exceeded in transit)
  26 3.537901   81.212.2.187     192.168.1.34   ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
  27 3.537903   81.212.2.187     192.168.1.34   ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)

▸ Frame 19: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
▸ Ethernet II, Src: Zte_94:62:91 (dc:f8:b9:94:62:91), Dst: IntelCor_33:98:e3 (f8:59:71:33:98:e3)
▾ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.34
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x3798 (14232)
  ▸ Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xbeb9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.34
```

Figure 9: Topmost ”TTL Exceeded” Reported Packet Header

8 Question 8

By looking at Figure 10, as the more fragments flag bit is set and don’t fragment bit is not set, we can say that the datagram is fragmented.



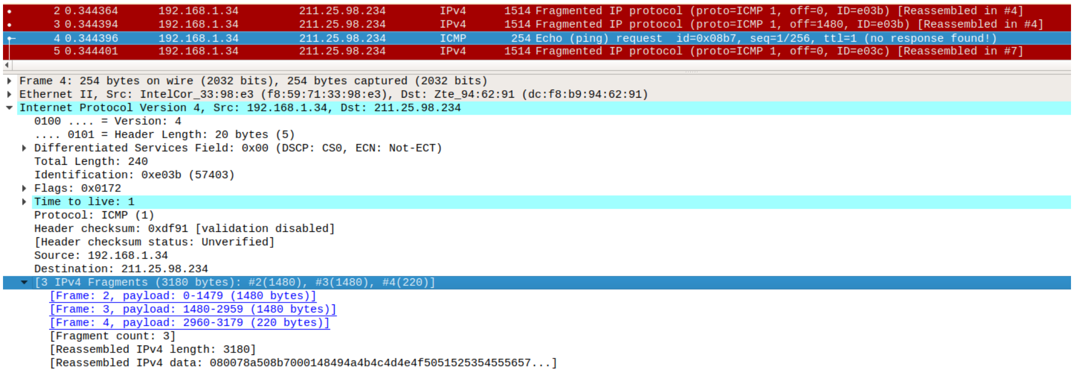
```
No.  Time        Source              Destination     Protocol  Length  Info
   1 0.000000    SamsungE_64:0f:27   Broadcast       ARP           60 Who has 192.168.1.1? Tell 192.168.1.47
   2 0.344364    192.168.1.34        211.25.98.234   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e03b) [Reassembled in #4]
   3 0.344394    192.168.1.34        211.25.98.234   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=e03b) [Reassembled in #4]

▸ Frame 2: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▸ Ethernet II, Src: IntelCor_33:98:e3 (f8:59:71:33:98:e3), Dst: Zte_94:62:91 (dc:f8:b9:94:62:91)
▾ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 211.25.98.234
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xe03b (57403)
  ▾ Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
      ...0 0000 0000 0000 = Fragment offset: 0
```

Figure 10: First Fragment Header

9 Question 9

Again, by looking at Figure 10, we know that first fragment's total size is 1500 and header size is 20, which tells us that payload of that fragment is 1480 bytes. On the other hand, as we indicated that the packet size will be 3200 when running traceroute command, we can easily calculate that there should be 3 fragments with sizes 1480, 1480 and 220 (+20 for header = 3200). We could also ensure it by looking at Figure 11, which states that there are 3 IPv4 fragments and gives the sizes same as we expected.



```
•    2 0.344364    192.168.1.34    211.25.98.234   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e03b) [Reassembled in #4]
•    3 0.344394    192.168.1.34    211.25.98.234   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=e03b) [Reassembled in #4]
     4 0.344396    192.168.1.34    211.25.98.234   ICMP     254 Echo (ping) request  id=0x08b7, seq=1/256, ttl=1 (no response found!)
     5 0.344401    192.168.1.34    211.25.98.234   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e03c) [Reassembled in #7]

▸ Frame 4: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits)
▸ Ethernet II, Src: IntelCor_33:98:e3 (f8:59:71:33:98:e3), Dst: Zte_94:62:91 (dc:f8:b9:94:62:91)
▾ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 211.25.98.234
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 240
    Identification: 0xe03b (57403)
  ▸ Flags: 0x0172
  ▸ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xdf91 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.34
    Destination: 211.25.98.234
  ▾ [3 IPv4 Fragments (3180 bytes): #2(1480), #3(1480), #4(220)]
      [Frame: 2, payload: 0-1479 (1480 bytes)]
      [Frame: 3, payload: 1480-2959 (1480 bytes)]
      [Frame: 4, payload: 2960-3179 (220 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3180]
      [Reassembled IPv4 data: 080078a508b7000148494a4b4c4d4e4f5051525354555657...]
```

Figure 11: Number of Fragments

10 Question 10

Even within the same packet, as 1st and 2nd fragments has more fragments flag set, the last fragment has "not set" for that flag. Similarly, total length is 1500 for first 2 fragments and 240 for the last one. Fragment offset and checksum values are also changed in each fragment.
Between all packets, TTL and identification is changed (incremented by 1 for every package). Changes within the same package are also valid for different packages, for sure.