

Student Information

Full Name: Alperen Oğuz Çakmak
ID Number: 2237162

1 Question 1

As it can be seen from the Figure 1, I couldn't able to see the whole path to metu.edu.tr (144.122.145.153).

```
alproskip@alproskip-Lenovo: ~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  9.936 ms  17.496 ms  17.481 ms
 2 * * *
 3 172.25.26.1 (172.25.26.1)  15.267 ms  15.344 ms  15.151 ms
 4 212.175.34.85.static.ttnet.com.tr (212.175.34.85)  19.091 ms  19.049 ms  18.989 ms
 5 06-incesu-xrs-t2-1---26-eskisehir-t3-3.statik.turktelekom.com.tr (212.156.109.219)  18.995 ms  18.966 ms  20.645 ms
 6 06-ulus-xrs-t2-1---06-incesu-xrs-t2-1.statik.turktelekom.com.tr (81.212.210.104)  22.358 ms  18.211 ms  15.893 ms
 7 212.156.99.254.static.turktelekom.com.tr (212.156.99.254)  18.096 ms  21.942 ms  21.646 ms
 8 * * *
 9 144.122.1.18 (144.122.1.18)  28.805 ms  30.785 ms  29.202 ms
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 *^C
alproskip@alproskip-Lenovo: ~$
```

Figure 1: Question 1 - Traceroute

2 Question 2

Default method for route tracing is udp method as stated in the traceroute manual. Also in the wireshark capture(Figure 2) I can see bunch of udp packets when route tracing is stated.

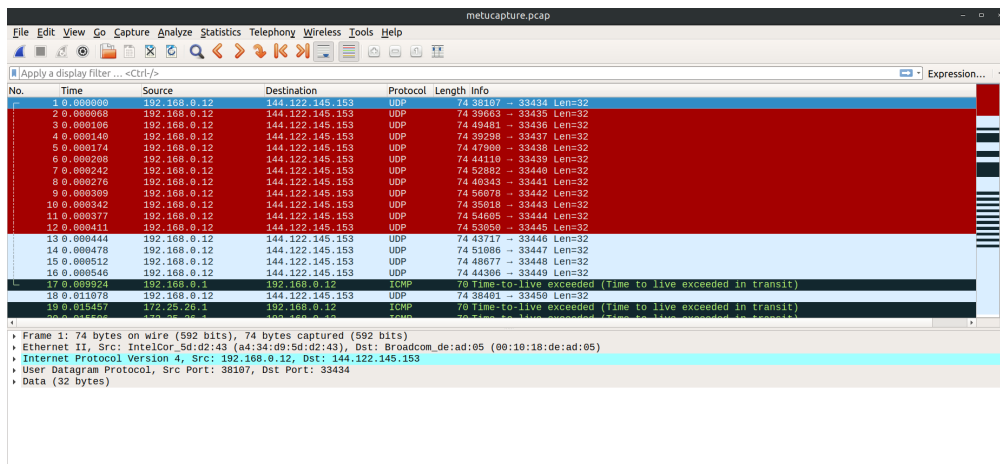
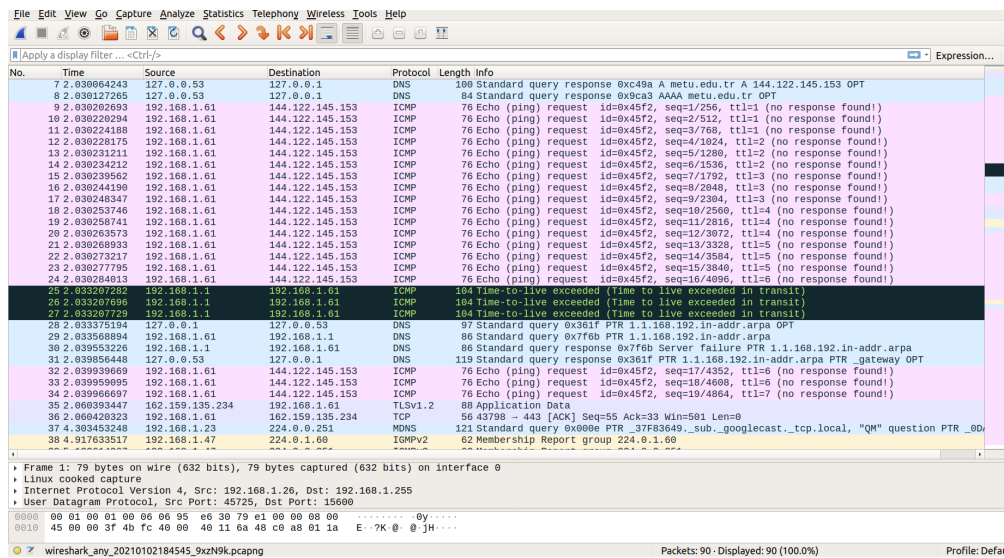


Figure 2: Question 2 - Wireshark

3 Question 3

-I flag stands for ICMP method. ICMP and UDP are different methods. As stated in previous question, traceroute uses UDP method as default and setting the -I flag will run it on ICMP method. In the previous question there were bunch of UDP packets in the wireshark screen because it run on default method. This time, using -I flag now there is ICMP packets (Figure 3) Since these methods are different in protocols and way of handling TTLs, they give different results on both traceroute and wireshark



No.	Time	Source	Destination	Protocol	Length	Info
7	2.83064243	127.0.0.53	127.0.0.1	DNS	100	Standard query response 0xc49a A metu.edu.tr A 144.122.145.153 OPT
8	2.83027265	127.0.0.53	127.0.0.1	DNS	84	Standard query response 0xc5a3 AAAA metu.edu.tr OPT
9	2.830202693	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=1/256, ttl=1 (no response found!)
10	2.830220294	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=2/512, ttl=1 (no response found!)
11	2.830224188	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=3/768, ttl=1 (no response found!)
12	2.830228175	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=4/1024, ttl=2 (no response found!)
13	2.830231211	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=5/1280, ttl=2 (no response found!)
14	2.830234212	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=6/1536, ttl=2 (no response found!)
15	2.830235962	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=7/1792, ttl=3 (no response found!)
16	2.830244198	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=8/2048, ttl=3 (no response found!)
17	2.830248347	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=9/2304, ttl=3 (no response found!)
18	2.830253746	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=10/2560, ttl=4 (no response found!)
19	2.830258741	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=11/2816, ttl=4 (no response found!)
20	2.830263573	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=12/3072, ttl=4 (no response found!)
21	2.830268933	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=13/3328, ttl=5 (no response found!)
22	2.830273217	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=14/3584, ttl=5 (no response found!)
23	2.830277795	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=15/3840, ttl=5 (no response found!)
24	2.830284813	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=16/4096, ttl=6 (no response found!)
25	2.830297202	192.168.1.1	192.168.1.1	ICMP	104	Time-to-live exceeded (Time to live exceeded in transit)
26	2.830297696	192.168.1.1	192.168.1.1	ICMP	104	Time-to-live exceeded (Time to live exceeded in transit)
27	2.830297729	192.168.1.1	192.168.1.1	ICMP	104	Time-to-live exceeded (Time to live exceeded in transit)
28	2.833575194	127.0.0.1	127.0.0.53	DNS	97	Standard query 0x361f PTR 1.1.168.192.in-addr.arpa OPT
29	2.833568194	192.168.1.61	192.168.1.1	DNS	86	Standard query 0x7f6b PTR 1.1.168.192.in-addr.arpa
30	2.839553226	192.168.1.1	192.168.1.61	DNS	86	Standard query response 0x7f6b Server failure PTR 1.1.168.192.in-addr.arpa
31	2.839856448	127.0.0.53	127.0.0.1	DNS	119	Standard query response 0x361f PTR 1.1.168.192.in-addr.arpa PTR_gateway OPT
32	2.839939669	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=18/4608, ttl=6 (no response found!)
33	2.839959895	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=19/4864, ttl=7 (no response found!)
34	2.839966697	192.168.1.61	144.122.145.153	ICMP	76	Echo (ping) request id=0x45f2, seq=20/5120, ttl=7 (no response found!)
35	2.860393447	192.159.135.234	192.168.1.61	TLSv1.2	88	Application Data
36	2.860420323	192.168.1.61	192.159.135.234	TCP	56	43788 -> 443 [ACK] Seq=55 Ack=33 Win=501 Len=0
37	4.303453248	192.168.1.23	224.0.0.251	MDNS	121	Standard query 0x000e PTR _37F83649._sub._googlecast._tcp.local, "QM" question PTR _0D
38	4.917633517	192.168.1.47	224.0.0.160	IGMPv2	62	Membership Report group 224.0.0.160

Figure 3: Question 3 - Wireshark

4 Question 4

- 1-) Buenos Aires Institute of Technology(itba.edu.ar) - Reached to 52.93.44.63
- 2-) University of Malaysia Kelantan(umk.edu.my) - Reached to 119.110.100.165

For the university in Argentina, traceroute couldnt reach to the IP of the web-site.

For the university in Malaysia UDP method was not able to reach to the final IP address so I tried using ICMP method and it succeeded to reach to the website's IP address.

For the bonus part I tried to traceroute "Favaloro University" with UDP and ICMP methods and could not end up with the IP address of its website. However, I was able to get to the actual IP address (200.49.142.158) using -T (TCP) method. Referring to the traceroute manual, TCP is more modern than the other methods and using this method we are unlikely to get stuck to some filters on the way to the destination. Traceroute manual says UDP and ICMP methods are filtered by the firewall. I also think that reason behind this is TCP is reliable compared to the UDP and ICMP.

5 Question 5

Protocol fields value: ICMP (1)

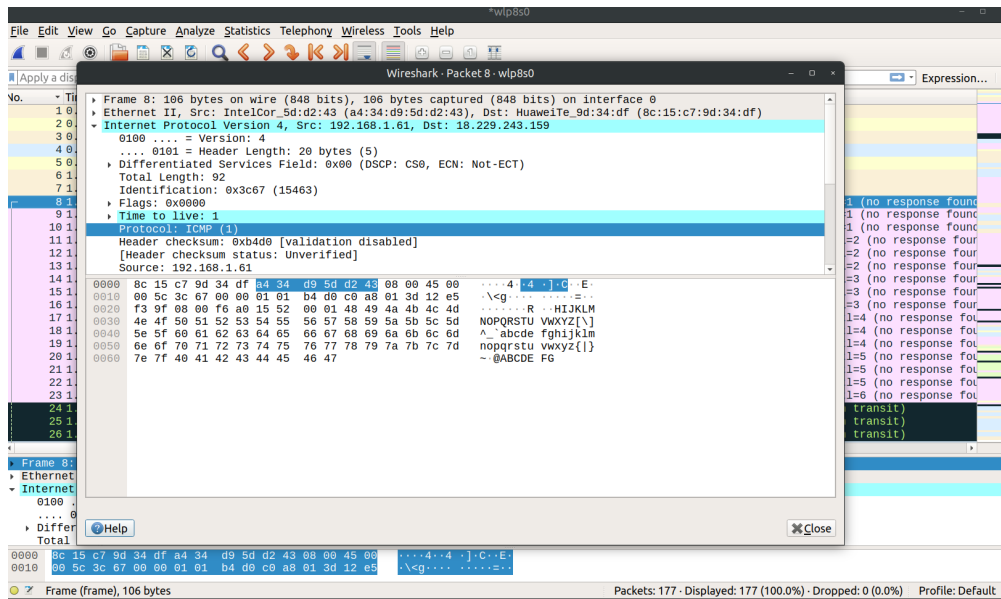


Figure 4: Question 5 - Wireshark

6 Question 6

20 bytes are in IP header as it is stated in IPv4 section. And it also says total length is 92 bytes and 20 of the is header so payload is 72 bytes.

7 Question 7

As it can be seen from the Figure 5, identification value is 45956 (0xb384) and TTL is 64. And this value changes for different TTL-exceeded packets.

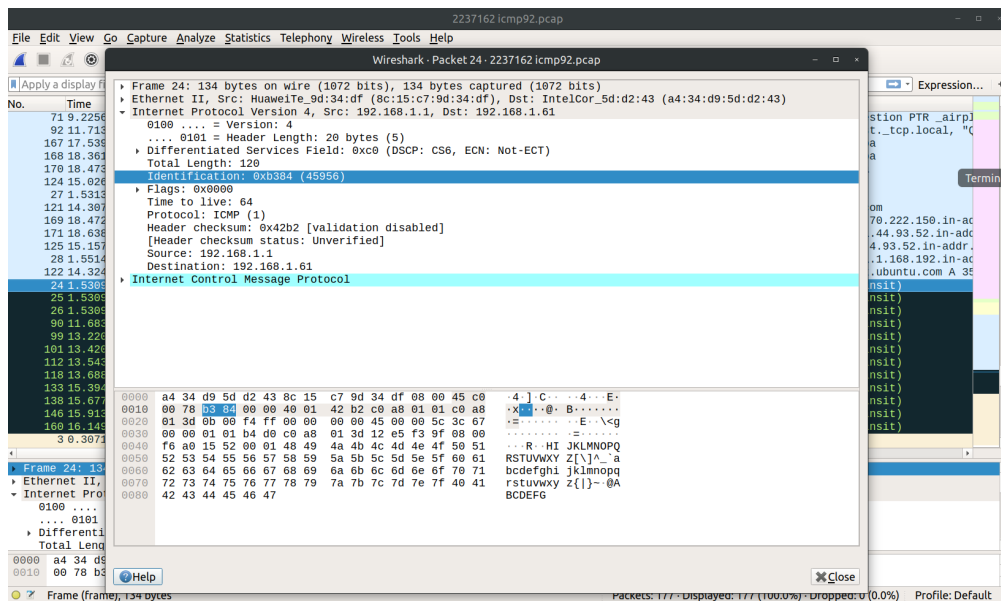


Figure 5: Question 7 - Wireshark

8 Question 8

For this homework I used ubuntu to capture and traceroute but after that I decided to change this questions figure and took another screenshot of pcap from windows. My laptop has 2 operating systems, even though this questions figure is taken from windows it is also my own laptop.

First ICMP echo request is packet number 5, which has the information of its fragments as 3, 4 and 5 (Figure 7), so now we inspect the packet number 3 which is the first fragment of this datagram. In the Figure 6 it can be seen that there is Flags section, looking at the last flag, "More Fragments", we can see that it is set which indicates that more fragments will follow. This implies that this datagram is fragmented.

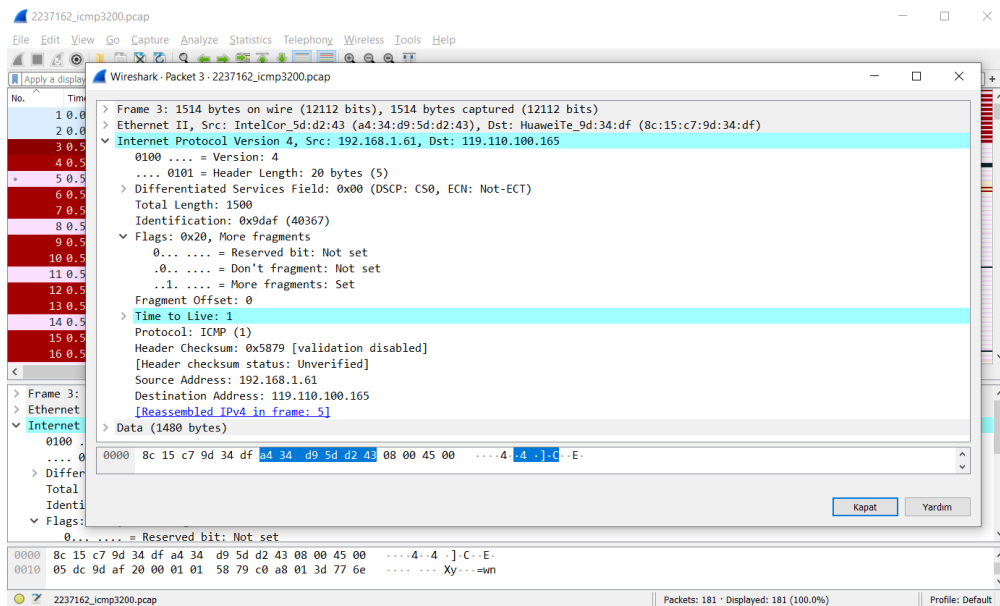


Figure 6: Question 8 - Wireshark

9 Question 9

It can be seen from the Figure 7 that there is 3 fragments created by this fragmentation and relevant part is highlighted.

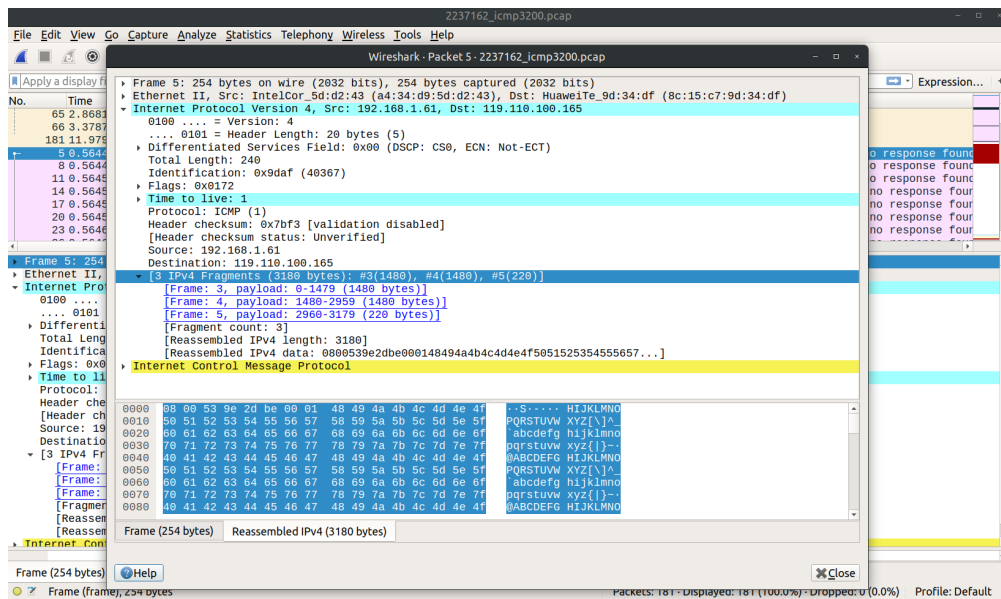


Figure 7: Question 8 - Wireshark

10 Question 10

For different fragments, several fields are changed. These fields are:

Flags are different in last fragments.

Total length is different for last fragments.

Header checksum is different for all fragments.

Fragment offset is different for all fragments.