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).

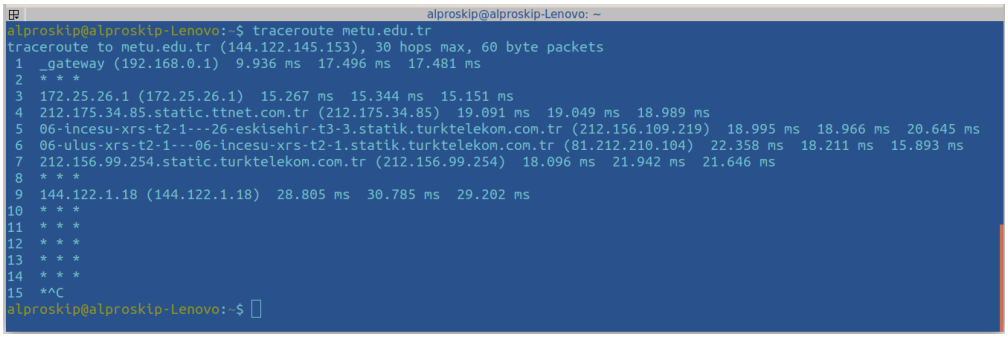

Figure 1: Question 1 - Traceroute

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.

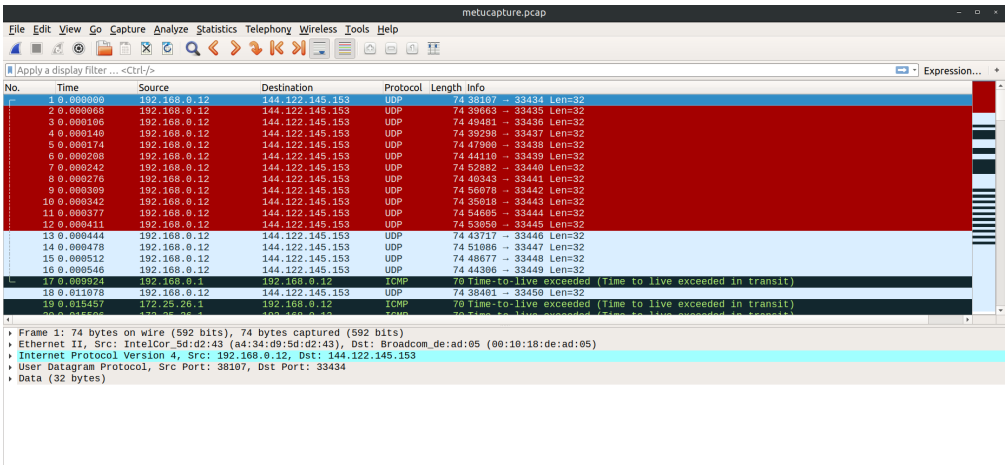

Figure 2: Question 2 - Wireshark

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

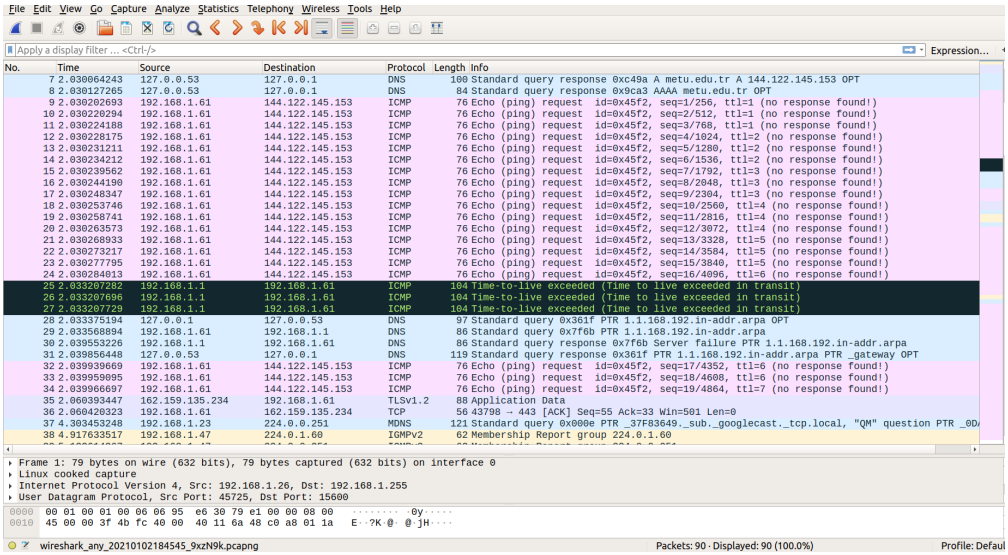

Figure 3: Question 3 - Wireshark

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 website.
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)

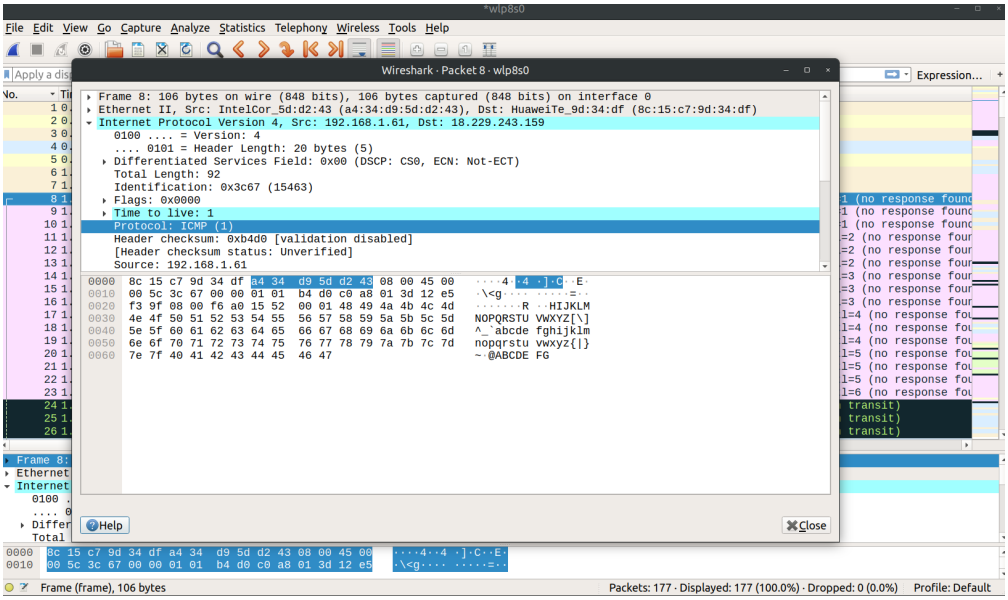

Figure 4: Question 5 - Wireshark

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.

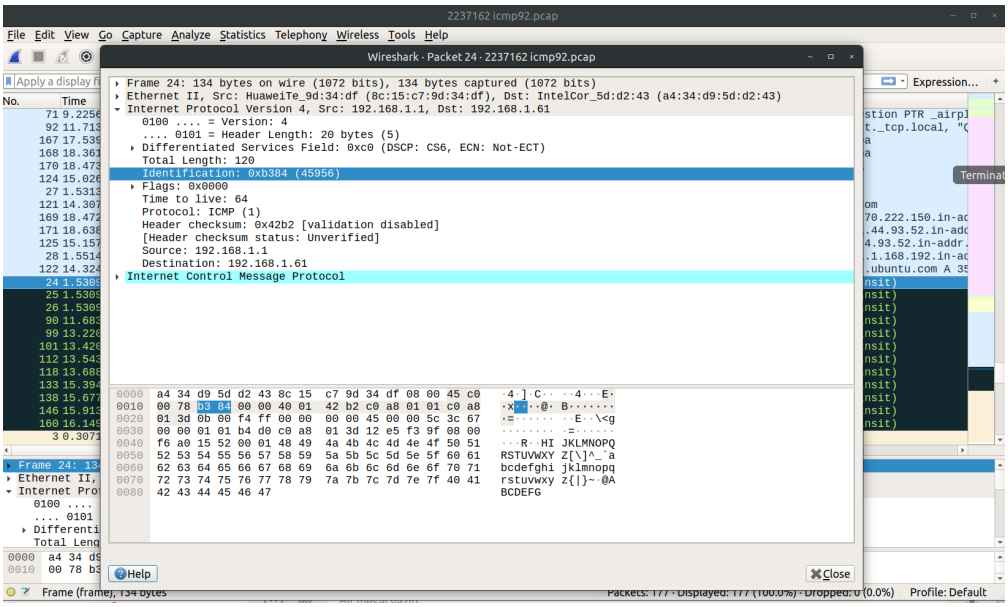

Figure 5: Question 7 - Wireshark

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.

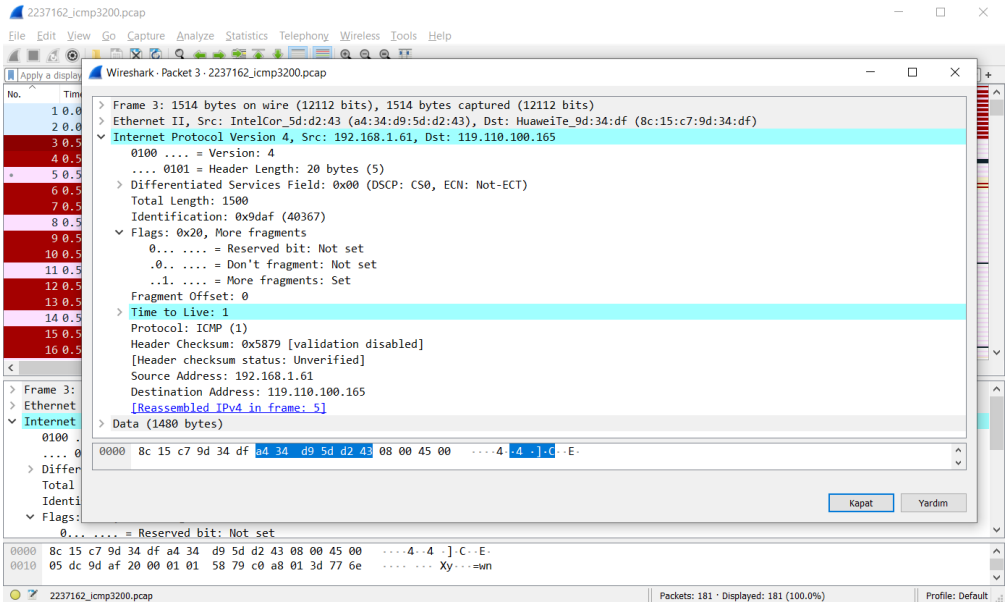

Figure 6: Question 8 - Wireshark

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.

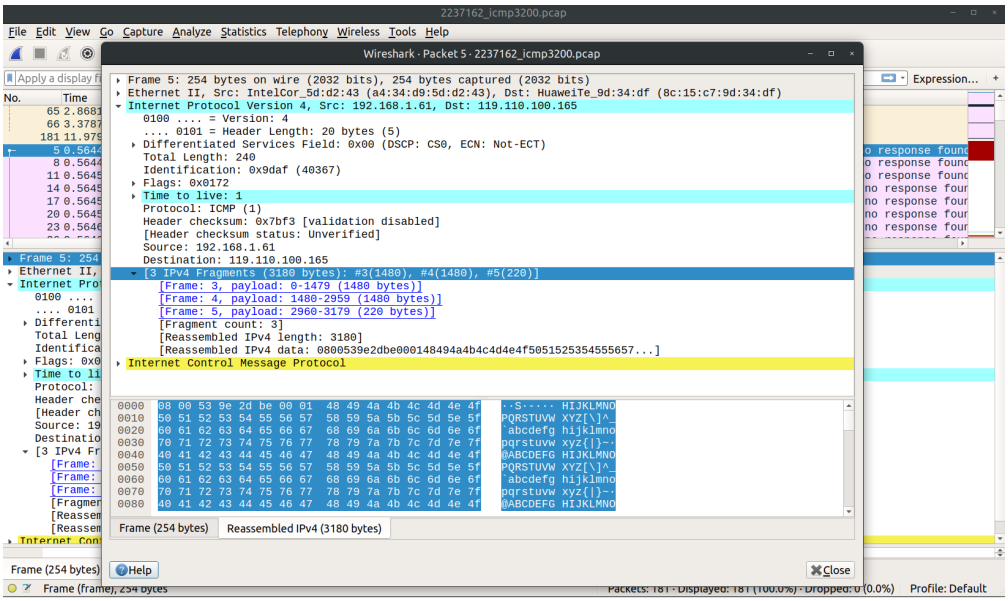

Figure 7: Question 8 - Wireshark

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.