Student Information

Full Name: Ozan Akın
ID Number: 2309599

Introduction

While doing this homework I couldn't take a clean snapshot due to some packages sent from my computer. Thus, I've used a virtual machine to capture packages using Wireshark.

Question 1

No, I couldn't see the whole path to `metu.edu.tr`. I could not see that how the packages forwarded inside the METU. This is because we cannot see what happened after entering `144.122.1.18`.

```
oznakn@vbox:~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.395 ms  0.324 ms  0.293 ms
 2  192.168.1.1 (192.168.1.1)  8.583 ms  8.491 ms  8.457 ms
 3  212.156.201.28.static.turktelekom.com.tr (212.156.201.28)  17.959 ms  18.000 ms  17.981 ms
 4  81.212.105.39.static.turktelekom.com.tr (81.212.105.39)  11.041 ms  11.112 ms  12.313 ms
 5  06-siteler-t2-1---06-siteler-t3-2.statik.turktelekom.com.tr (195.175.175.49)  12.292 ms  12.594 ms  12.747 ms
 6  06-ulus-xrs-t2-1---06-siteler-t2-1.statik.turktelekom.com.tr (81.212.207.29)  12.907 ms  7.701 ms  8.199 ms
 7  212.156.99.254.static.turktelekom.com.tr (212.156.99.254)  9.370 ms  9.570 ms  9.490 ms
 8  * * *
 9  144.122.1.18 (144.122.1.18)  19.127 ms  19.339 ms  19.852 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

The output of the `traceroute`.

Question 2

The `traceroute` program uses `ICMP TIME_EXCEEDED` packets and `IP` protocol's time to live field for route tracing. Also we can see the ICMP packages in Wireshark's capture.

```
11 0.096203697   10.0.2.2        10.0.2.15       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
12 0.096203810   10.0.2.2        10.0.2.15       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
13 0.096203847   10.0.2.2        10.0.2.15       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
```

ICMP packets from Wireshark's capture.

Question 3

```
oznakn@vbox:~$ sudo traceroute metu.edu.tr -I
[sudo] password for oznakn:
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.198 ms  0.174 ms  0.169 ms
 2  192.168.1.1 (192.168.1.1)  5.303 ms  5.299 ms  5.294 ms
 3  212.156.201.28.static.turktelekom.com.tr (212.156.201.28)  13.021 ms  13.125 ms  13.370 ms
 4  81.212.105.39.static.turktelekom.com.tr (81.212.105.39)  10.330 ms  11.025 ms  11.487 ms
 5  06-siteler-t2-1---06-siteler-t3-2.statik.turktelekom.com.tr (195.175.175.49)  9.660 ms  10.263 ms  10.254 ms
 6  06-ulus-xrs-t2-1---06-siteler-t2-1.statik.turktelekom.com.tr (81.212.207.29)  10.602 ms * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

The output of the `traceroute` with `-I` flag.

When we use `-I` flag with `traceroute`, it uses `ICMP Echo (ping)` packages instead of `UDP` packages. The path is changed. The ninth entry, the one includes `144.122.1.18`, is gone. Most probably that server drops the `ICMP Echo` packages.

3	0.094500	10.0.2.15	144.122.145.153	ICMP	74	Echo (ping) request id=0x129b, seq=1/256, ttl=1 (no response found!)
4	0.094521	10.0.2.15	144.122.145.153	ICMP	74	Echo (ping) request id=0x129b, seq=2/512, ttl=1 (no response found!)
5	0.094525	10.0.2.15	144.122.145.153	ICMP	74	Echo (ping) request id=0x129b, seq=3/768, ttl=1 (no response found!)
6	0.094530	10.0.2.15	144.122.145.153	ICMP	74	Echo (ping) request id=0x129b, seq=4/1024, ttl=2 (no response found!)
7	0.094534	10.0.2.15	144.122.145.153	ICMP	74	Echo (ping) request id=0x129b, seq=5/1280, ttl=2 (no response found!)

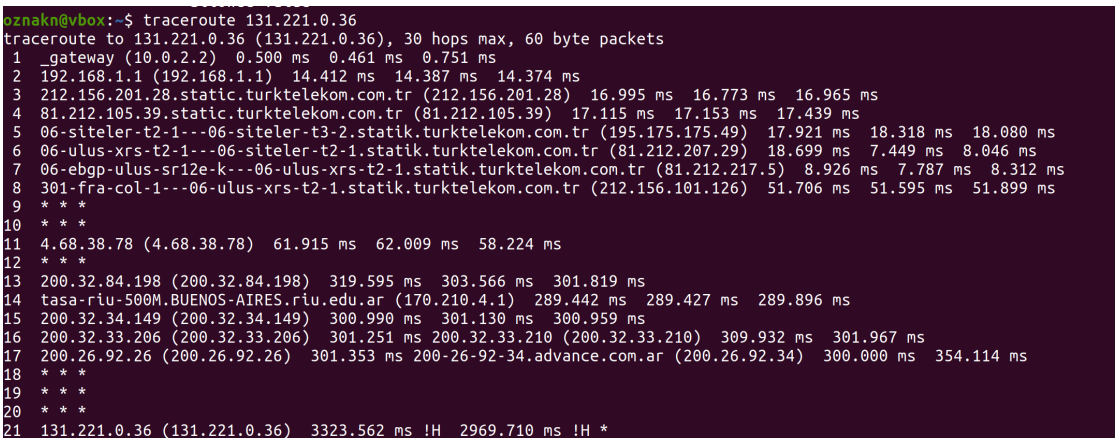
ICMP Echo (ping) packets from Wireshark's capture.

Using ICMP Echo packets with `TTL`, the routers can be traversed.

Question 4

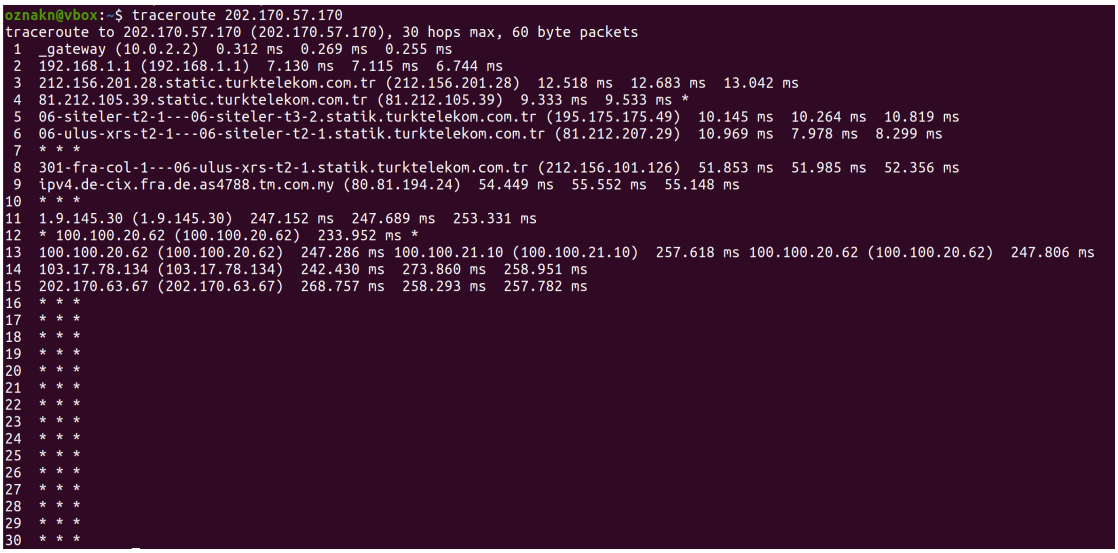
I've chose National University of Central Buenos Aires from Argentina, and Universiti Sains Malaysia from Malaysia.

The website of National University of Central Buenos Aires is `www.unicen.edu.ar` with IP `131.221.0.36`, and the website of Universiti Sains Malaysia from Malaysia is `www.usm.my with` IP `202.170.57.170`. I found these IP addresses using `dig` command.



The output of the `traceroute` for the university in Argentina.

Using `traceroute`, I managed to reach the server of the university in Argentina. However I couldn't reach the server of the the university in Malaysia.



The output of the `traceroute` for the university in Malaysia.

As seen above, I could find the IP address of the server of the university in Argentina, however I could not for the university in Malaysia.

Bonus part

I couldn't reach the university in Malaysia using `traceroute` without any flags. The last IP address shown in the `traceroute` output (`202.170.63.67`) is belongs to the same university according to `ipinfo.io`, which is a website I found that shows info about IP addresses.

I tried the following settings, `-I` for using ICMP Echo probes, and `-t 16`, and `-t 8` for settings the type of service and precedence values and all result the same as the output above. Then I tried `traceroute` with **`-UL`** for UDPLite probes, **`-D`** for UDP probes and the output was empty, all the entries were `* * *`. Lastly I used `-T` for TCP probes and then I saw the IP of the university. However in this case, there were no path to show. The output can be found below.

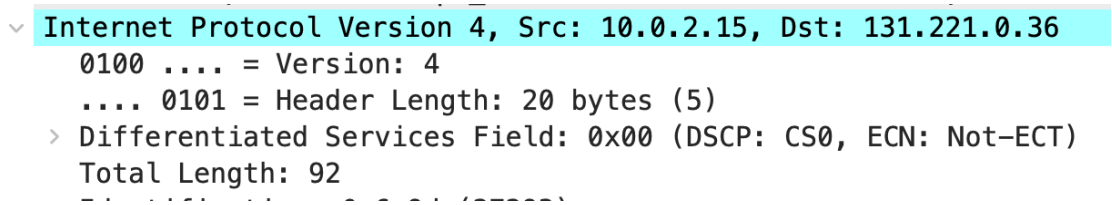
```
oznakn@vbox:~$ sudo traceroute 202.170.57.170 -T
traceroute to 202.170.57.170 (202.170.57.170), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.304 ms  0.267 ms  0.257 ms
 2  voicingconcern.net.my (202.170.57.170)  262.706 ms  264.095 ms  253.760 ms
```

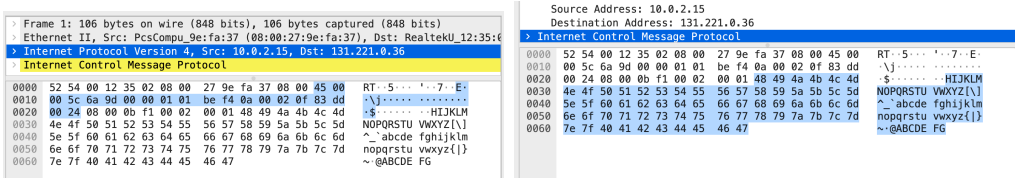
Question 5

The value of the `IPv4` protocol is `ICMP`.

Question 6

There are 20 bytes in IP header and 72 bytes in IP payload (which is a ICMP echo packet). This also satisfies the total length field in the IP header, which is 92.

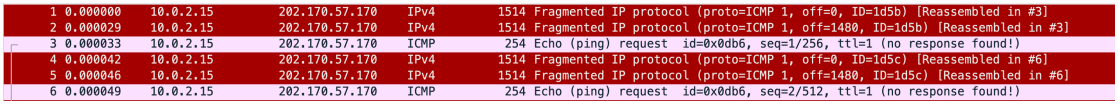




Question 7

The identification field is `0x6a9d` and the value of TTL field is `1`. And both the identification and TTL values change among the other ICMP echo packets.

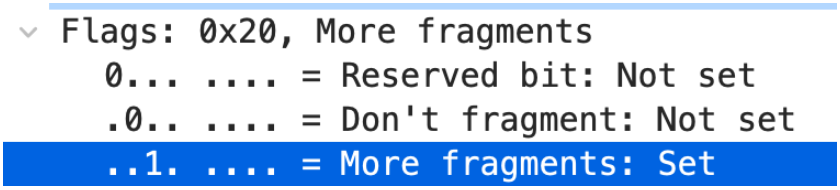
Question 8



As seen above, the packets with no 3 and 6 have been fragmented into two packets. Third packet fragmented into packets with no 1 and 2, and sixth packet fragmented into 4 and 5. Also `Reassembled in #3` and `Reassembled in #6` texts can be seen from screenshot.

Question 9

No, you cannot. There is only one flag stating that there is more fragments or not. As a result, you cannot tell how many fragments have been created by looking the packet information of the first datagram.



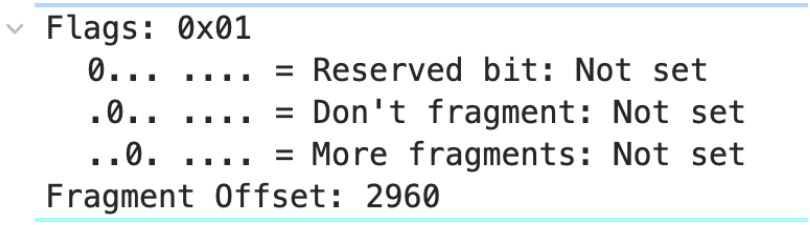
Flags of a fragmented package.

Question 10

There are two fields changes, `Fragment Offset` and `More Fragments` flag.

The `Fragment Offset` field changes for every fragment. Each offset represents the position of data inside the fragment.

The `More Fragments` flag is `1` for all fragments except the last one. For the last one, this value is 0.



The flags and `Fragment Offset` fields in the last fragment.