

# 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`.

```
oznkn@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.

110.096203697	10.0.2.2	10.0.2.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)
120.096203810	10.0.2.2	10.0.2.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)
130.096203847	10.0.2.2	10.0.2.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)

ICMP packets from Wireshark's capture.

## Question 3

```
oznakh@vbox:~$ sudo traceroute metu.edu.tr -I
[sudo] password for oznakh:
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](http://www.unicen.edu.ar) with IP 131.221.0.36, and the website of Universiti Sains Malaysia from Malaysia is [www.usm.my](http://www.usm.my) with IP 202.170.57.170. I found these IP addresses using `dig` command.

```

oznakh@vbox:~$ traceroute 131.221.0.36
traceroute to 131.221.0.36 (131.221.0.36), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2) 0.500 ms 0.461 ms 0.751 ms
 2 192.168.1.1 (192.168.1.1) 14.412 ms 14.387 ms 14.374 ms
 3 212.156.201.28.static.turktelekom.com.tr (212.156.201.28) 16.995 ms 16.773 ms 16.965 ms
 4 81.212.105.39.static.turktelekom.com.tr (81.212.105.39) 17.115 ms 17.153 ms 17.439 ms
 5 06-siteler-t2-1---06-siteler-t3-2.statik.turktelekom.com.tr (195.175.175.49) 17.921 ms 18.318 ms 18.080 ms
 6 06-ulus-xrs-t2-1---06-siteler-t2-1.statik.turktelekom.com.tr (81.212.207.29) 18.699 ms 7.449 ms 8.046 ms
 7 06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-1.statik.turktelekom.com.tr (81.212.217.5) 8.926 ms 7.787 ms 8.312 ms
 8 301-fra-col-1---06-ulus-xrs-t2-1.statik.turktelekom.com.tr (212.156.101.126) 51.706 ms 51.595 ms 51.899 ms
 9 * * *
10 * * *
11 4.68.38.78 (4.68.38.78) 61.915 ms 62.009 ms 58.224 ms
12 * * *
13 200.32.84.198 (200.32.84.198) 319.595 ms 303.566 ms 301.819 ms
14 tasa-riu-500M.BUENOS-AIRES.riu.edu.ar (170.210.4.1) 289.442 ms 289.427 ms 289.896 ms
15 200.32.34.149 (200.32.34.149) 300.990 ms 301.130 ms 300.959 ms
16 200.32.33.206 (200.32.33.206) 301.251 ms 200.32.33.210 (200.32.33.210) 309.932 ms 301.967 ms
17 200.26.92.26 (200.26.92.26) 301.353 ms 200-26-92-34.advance.com.ar (200.26.92.34) 300.000 ms 354.114 ms
18 * * *
19 * * *
20 * * *
21 131.221.0.36 (131.221.0.36) 3323.562 ms !H 2969.710 ms !H *

```

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.

```

oznakh@vbox:~$ traceroute 202.170.57.170
traceroute to 202.170.57.170 (202.170.57.170), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2) 0.312 ms 0.269 ms 0.255 ms
 2 192.168.1.1 (192.168.1.1) 7.130 ms 7.115 ms 6.744 ms
 3 212.156.201.28.static.turktelekom.com.tr (212.156.201.28) 12.518 ms 12.683 ms 13.042 ms
 4 81.212.105.39.static.turktelekom.com.tr (81.212.105.39) 9.333 ms 9.533 ms *
 5 06-siteler-t2-1---06-siteler-t3-2.statik.turktelekom.com.tr (195.175.175.49) 10.145 ms 10.264 ms 10.819 ms
 6 06-ulus-xrs-t2-1---06-siteler-t2-1.statik.turktelekom.com.tr (81.212.207.29) 10.969 ms 7.978 ms 8.299 ms
 7 * * *
 8 301-fra-col-1---06-ulus-xrs-t2-1.statik.turktelekom.com.tr (212.156.101.126) 51.853 ms 51.985 ms 52.356 ms
 9 ipv4.de-cix.fra.de.as4788.tm.com.ny (80.81.194.24) 54.449 ms 55.552 ms 55.148 ms
10 * * *
11 1.9.145.30 (1.9.145.30) 247.152 ms 247.689 ms 253.331 ms
12 * 100.100.20.62 (100.100.20.62) 233.952 ms *
13 100.100.20.62 (100.100.20.62) 247.286 ms 100.100.21.10 (100.100.21.10) 257.618 ms 100.100.20.62 (100.100.20.62) 247.806 ms
14 103.17.78.134 (103.17.78.134) 242.430 ms 273.860 ms 258.951 ms
15 202.170.63.67 (202.170.63.67) 268.757 ms 258.293 ms 257.782 ms
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

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](http://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.

```
oznahn@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.

Protocol: ICMP (1)

## 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.

- ✓ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 131.221.0.36
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 92

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0 > Ethernet II, Src: PcsCompu_9e:fa:37 (08:00:27:9e:fa:37), Dst: RealtekU_12:35:66 (08:00:27:12:35:66) > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 131.221.0.36 > Internet Control Message Protocol		Source Address: 10.0.2.15 Destination Address: 131.221.0.36 > Internet Control Message Protocol	
0000	52 54 00 12 35 02 00 00	27 9e fa 37 08 00 45 00	RT - 5... ..7..E
0010	00 5c 6a 9d 00 00 01 01	be f4 0a 00 02 0f 83 dd	^J.....
0020	00 24 08 00 0b f1 00 02	00 01 48 49 4a 4b 4c 4d	\$. ....HIJKLM
0030	4e 4f 50 51 52 53 54 55	56 57 58 59 5a 5b 5c 5d	NOPQRSTU VWXYZ[\]
0040	5e 5f 60 61 62 63 64 65	66 67 68 69 6a 6b 6c 6d	^_ abcde fghijklm
0050	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqrstu vwxyz{ }
0060	7e 7f 40 41 42 43 44 45	46 47	~@ABCDE FG

## 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

1	0.000000	10.0.2.15	202.170.57.170	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=1d5b) [Reassembled in #3]
2	0.000029	10.0.2.15	202.170.57.170	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=1d5b) [Reassembled in #3]
3	0.000033	10.0.2.15	202.170.57.170	ICMP	254	Echo (ping) request id=0x0db6, seq=1/256, ttl=1 (no response found!)
4	0.000042	10.0.2.15	202.170.57.170	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=1d5c) [Reassembled in #6]
5	0.000046	10.0.2.15	202.170.57.170	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=1d5c) [Reassembled in #6]
6	0.000049	10.0.2.15	202.170.57.170	ICMP	254	Echo (ping) request id=0x0db6, seq=2/512, ttl=1 (no response found!)

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: 0x20, More fragments
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
```

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.

```
✓ Flags: 0x01
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment Offset: 2960
```

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