Student Information

Full Name: Abdulkadir Pamukçu

ID Number: 2237774

1 Question 1

I can not see the whole path to the metu.edu.tr. The last meaningful output is 144.122.1.18 and metu.edu.tr's address is 144.122.145.153. After that output gives "***" until it reaches the max hop count which is 30.

```
kadir@kadir-X550VX: ~
(base) kadir@kadir-X550VX:~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets

1 MitraStar.Home (192.168.1.1) 0.415 ms 0.780 ms 0.898 ms

2 172.17.1.135 (172.17.1.135) 6.082 ms 6.479 ms 7.319 ms

3 85.118.223.31.srv.turk.net (31.223.118.85) 7.658 ms * *

4 86.118.223.31.srv.turk.net (31.223.118.86) 8.037 ms 8.214 ms 8.296
      81.118.223.31.srv.turk.net (31.223.118.81) 8.890 ms 9.386 ms
 б
      234.22.146.159.static.turk.net (159.146.22.234) 15.634 ms 16.517 ms 16.119 ms
     46.234.28.101 (46.234.28.101)
31.145.74.161 (31.145.74.161)
                                                      30.883 ms
                                                                        33.069 ms
                                                                                         32.297 ms
                                                      29.315 ms
                                                                        29.329 ms
                                                                                         27.704 ms
      213.194.75.26 (213.194.75.26)
                                                      40.755 ms
                                                                       40.582 ms
12
13
      144.122.1.18 (144.122.1.18) 33.995 ms 34.682 ms 33.951 ms
14
15
16
17
18
19
20
21
22
24
25
27
28
30
(base) kadir@kadir-X550VX:~$
```

Figure 1: Traceroute output of metu.edu.tr

2 Question 2

As it can be seen from protocol bar in Wireshark capture and as in the traceroute manual, the default method of route tracing is UDP.

3 Question 3

When I use -I flag while using traceroute and capturing with Wireshark O noticed in Wireshark there is lots ICMP packets instead of UDP ones like in the previous capture without the -I flag. And in manual of traceroute it says "Use ICMP ECHO for probes".

So using -I flag make traceroute use different method, namely ICMP. Thus time makes both traceroute and wireshark outputs to be different than the other ones.

4 Question 4

Argentina:

University: National University of Northwestern Buenos Aires Website: unnoba.edu.ar

IP address: 200.124.178.2

Malaysia:

University: University of Malaya Website: um.edu.my IP address: 52.187.23.205

4.1 Bonus

I could not reach um.edu.my with traceroute in normal tryings.

When i read the manual of traceroute i saw traceroute -T option and description was: Use TCP SYN for probes

I knew TCP is a more reliable way of transferring. So i gave a try and i actually reached the university website's IP address 52.187.23.205

After i found this and researched about it and i found why.

As we know traceroute use udp protocol as default and if there is any filter or firewall then most probably any udp ports will be blocked or filtered, with using -T as an argument we are using TCP protocol so we are only using the allowed protocol and ports. In that way we can reach the university's website with traceroute.

5 Question 5

```
Wireshark · Packet 9 · q5.pcap

Frame 9: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
Linux cooked capture

Internet Protocol Version 4, Src: 192.168.43.101, Dst: 200.124.178.2

0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
bifferentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x593a (22842)
Flags: 0x0000
Fragment offset: 0
Filme to live: 1
Protocol: ICMP (1)
Header checksum: 0xf9da [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.43.101
Destination: 200.124.178.2
Internet Control Message Protocol
```

Figure 2: First ICMP packet sent by my computer

As it can seen in the highlighted protocol from the figure, IPv4 protocol is ICMP(Internet Control Message Protocol).

6 Question 6

As it can be seen from figure 2, header length is 20 bytes and total length is 92 bytes.

In order the find payload we need to find non-header bytes. Since header length is 20 bytes and total length 92 bytes.

Payload length is 92-20=72 bytes.

7 Question 7

The value in the Identification field is 0xad96 (44438) and the value in TTL field is 125.

After looking at the other TTL exceeded packets I observed that Identification field always increments by 1. Also TTL fields is changing but I could not find any pattern.

8 Question 8

By looking at the packet information that is given in figure 3 I can tell that this datagram has been fragmented since in flags section More fragmented flag is set. This tells that the datagram has been fragmented.

```
Wireshark · Packet 20 · any
Frame 20: 1516 bytes on wire (12128 bits), 1516 bytes captured (12128 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.43.101, Dst: 52.187.23.205
   0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x9963 (39267)
   Flags: 0x2000, More fragments
       0.... Not set
       .0.. .... = Don't fragment: Not set
    Fragment offset: 0
   Time to live: 1
Protocol: ICMP (1)
    Header checksum: 0xc228 [validation disabled]
[Header checksum status: Unverified]
    Šource: 192.168.43.101
   Destination: 52.187.23.205
Reassembled IPv4 in frame: 22
Data (1480 bytes)
```

Figure 3: First ICMP Echo request sent from my machine

9 Question 9

```
Wireshark Packet 20 any

Frame 20: 1516 bytes on wire (12128 bits), 1516 bytes captured (12128 bits) on interface any, id 0

Link Layer address type: 1
Link Layer address type: 1
Link Layer address length: 6
Source: LiteonTe_45:fb:2f (94:e9:79:45:fb:2f)
Unused: 0000
Protocol: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.43.101, Dst: 52.187.23.205
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x9903 (39267)
Flags: 0x2000, More fragments
0... = Reserved bit: Not set
0... = Bon't fragment: Not set
1... = More fragment: Not set
1... = More fragments: Set
Fragment offset: 0
Fine to live: 1
Protocol: ICMP (1)
Header checksum: 0xc228 [validation disabled]
[Header checksum: 0xc228 [validation disabled]
[Header checksum: 0xc228 [validation disabled]
Source: 192.168.43.101
Destination: 52.187.23.205
Reassembled TPV4 in frame: 22

Data (1480 bytes)
```

Figure 4: Highlighted resassambled IPv4 in frame

When I looked at highlighted part in the given figure, it says Reassembled IPv4 in frame: 22 what I understand from here is this packet, the 20th packet, is actually part of 22th packet but since the original packet is fragmented this packet came as 20th packet.

With this approach and knowing the 20th packet is the first packet arrived I was able to tell this is the first fragment of 22th packet and 21th packet is also a fragment of 22th packet.

So I can tell that 3 fragments created by the fragmentation.

10 Question 10

There are 4 fields that are changing between fragments, these are:

- Total Length
- Flags
- Fragment offset
- Header checksum