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.

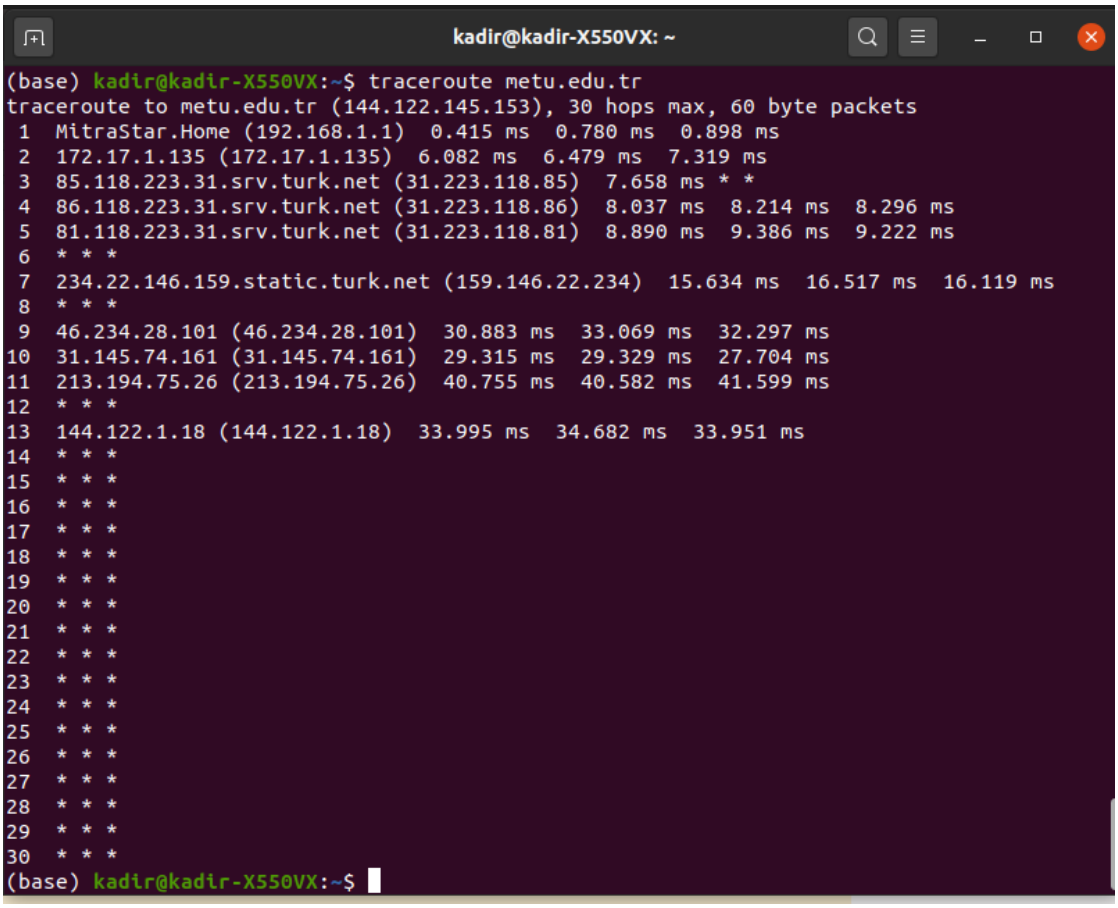

Figure 1: Traceroute output of metu.edu.tr

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

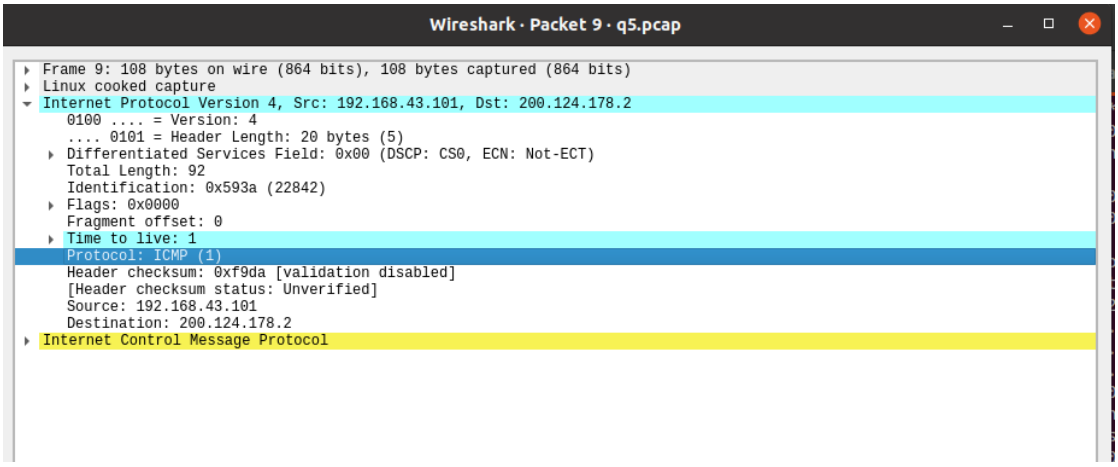

Figure 2: First ICMP packet sent by my computer

As it can seen in the higlighted 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.

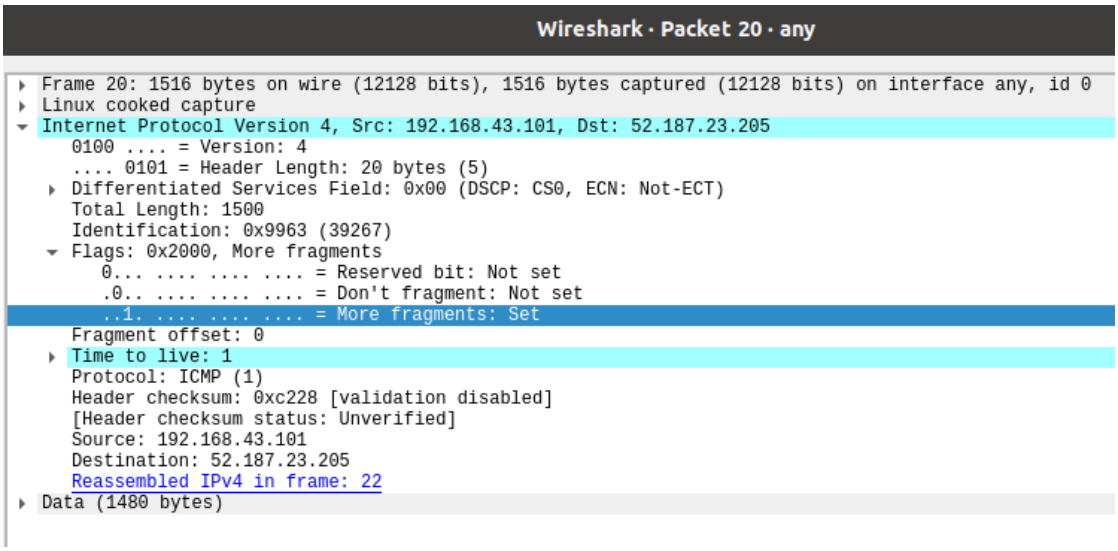

Figure 3: First ICMP Echo request sent from my machine

9 Question 9

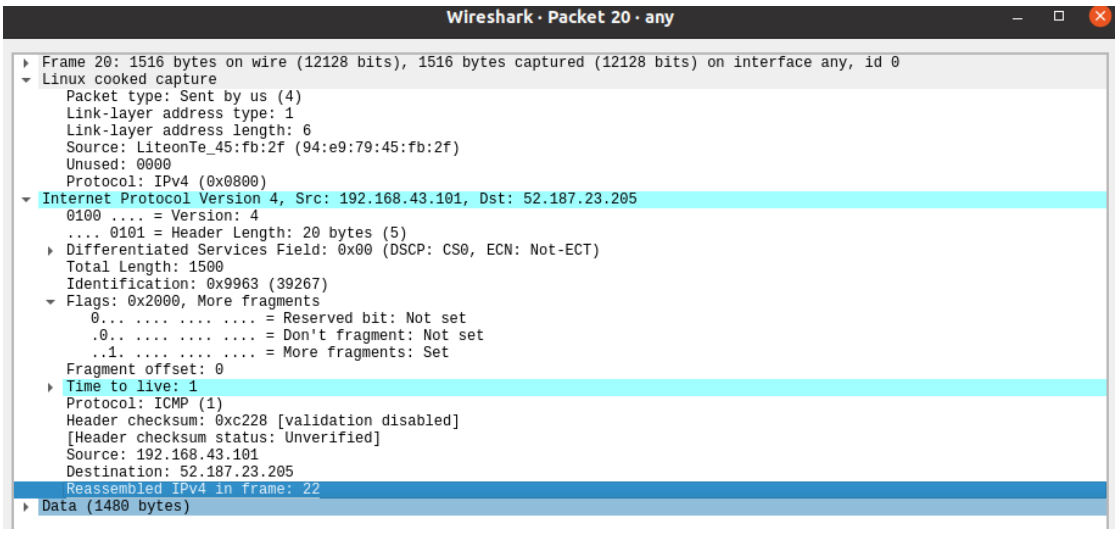

Figure 4: Highlighted resassambled IPv4 in frame

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