Zeynep Erdoğan - 2171577

# Wireshark Assignment 3

**Q1:** There are 17 ICMP echo requests traceroute send, TTL fields of these packets changes incrementally one by one.

**Q2:** Source IP's are the same with the output of the traceroute command but not in the same order. The order depends on the timestamps in the output of the traceroute command. If the timestamp is bigger, it is captured later.

| Number | Source IP |
|---|---|
| 51 | 10.70.0.2 |
| 53 | 144.122.2.1 |
| 54 | 144.122.171.1 |
| 55 | 193.140.85.137 |
| 56 | 213.194.75.25 |
| 57 | 31.145.74.162 |
| 58 | 46.234.28.57 |
| 59 | 144.122.1.21 |
| 60 | 195.2.23.129 |
| 61 | 195.2.27.149 |
| 62 | 195.2.16.1 |
| 72 | 23.235.41.162 |

**Q3:** The traceroute uses TLL exceeded responses to find out the route to destination. In each router TLL is decremented by one and if it reduces to 0 in any of the router, it sends a TLL exceeded response to host. With that response host can identify address of that router so traceroute makes use of that. First it sets TLL to one to find out the first router packet goes, then it sets TLL to two to find out the second router and it goes on until packet reaches the destination.

This route is not always the same even if you run traceroute from same location/network. Because this path depends on the routers it is passed through and router can make a different decision each time depending on the traffic among the routers. Also destination server may have different IP's so each time packets may go to different one.

**Q4:** IP Header Length is 20 and Total Length is 85.

**Q5:** The value of Protocol field in IP header for UDP communication is 17 and for ICMP communication is 1.

**Q6:**IP datagram been fragmented and there are 4 fragments because the maximum transmission unit is smaller than the IP datagram length. In my case, total length is 5008 bytes and each fragment carry 1480 bytes, 1480 bytes, 1480 bytes and 568 bytes respectively.