Onur Can ÜNAL
2095966

WIRESHARK ASSIGNMENT 3

1. Traceroute sent 17 ICMP echo requests. TTL fields of these packets are incremented by 1 from one packet to another in order.
2. The numbers of TTL-exceeded responses are 23, 24, 26, 27, 28, 35, 36, 37, 38, 39. The source IP addresses of those responses are 192.168.1.1, 10.36.250.65, 10.38.219.5, 10.40.141.51, 176.40.126.1, 195.219.50.50, 195.219.50.165, 4.69.163.22, 5.23.8.21, 212.162.24.214, respectively.
The output of the traceroute command that I typed was:

```
traceroute to www.twitch.tv (151.101.14.167), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  11.952 ms
 2  host-176-40-126-1.reverse.superonline.net (176.40.126.1)  17.417 ms
 3  10.36.250.65 (10.36.250.65)  12.409 ms
 4  10.40.141.51 (10.40.141.51)  16.623 ms
 5  10.38.219.5 (10.38.219.5)  12.817 ms
 6  ix-ae-6-0.tcore1.it6-ankara.as6453.net (5.23.8.21)  52.687 ms
 7  if-ae-37-3.tcore1.fr0-frankfurt.as6453.net (195.219.50.165)  52.622 ms
 8  195.219.50.50 (195.219.50.50)  52.586 ms
 9  ae-2-3207.edge5.Frankfurt1.Level3.net (4.69.163.22)  52.611 ms
10  212.162.24.214 (212.162.24.214)  54.249 ms
11  151.101.14.167 (151.101.14.167)  50.894 ms
```

The matching between TTL-exceeded responses and the order of the output as, No. 23 packet with 1, No. 24 with 3, No. 26 with 5, No. 27 with 4, No. 28 with 2, No. 35 with 8, No. 36 with 7, No. 37 with 9, No. 38 with 6, No. 39 with 10.
3. Traceroute finds out the route to the destination with the help of the TTL fields in the IP header. There are routers between the source and the destination. The first packet that is sent from the source starts with TTL value 1. When a router receives that packet and forwards it, the TTL value is decreased by 1. If the TTL value becomes zero, the packet is ignored, and the router responds back to source with a TTL exceeded message. In our traceroute example for www.twitch.tv, there are 11 hops that can be seen from the answer 2. Thus, since TTL values are decreased by 1 for each route, the packet with the TTL value of less than 11 cannot reach the destination, they are ignored. By this way, we know that the destination is reachable from the source host. I run the traceroute command a few times again, I observed that there were different routes. This is because there is congestion control on the network, and so the hops on the path can change, and the packet from source to destination can follow different paths.
4. The IP header length and total packet length of the DNS query response with type A record for hbostann.com are 20 bytes and 74 bytes respectively.
5. The value of the Protocol field in the IP header for UDP communication is 17, and the value of the Protocol field in the IP header for ICMP communication is 1.
6. Yes, the IP datagram has been fragmented, and 4 fragments are used. Because datagram is big in size, and it cannot be sent in one packet, so it has been fragmented into 4 fragments.