**BLG433E**

**COMPUTER COMMUNICATIONS**

**HOMEWORK 2**

**“Network Analyzing with Wireshark”**

1. **Dynamic Host Configuration Protocol (DHCP)** is a protocol that assigns individual IP addresses to the hosts automatically from a block of addresses. It also gives information about subnet mask, address of a host’s first-hop router and address of a host’s local DNS server.

DHCP contains four stages for a newly arriving host. The stages are described in below:

1. **DHCP server discovery:** The newly arriving host’s task is to find DHCP server and this task is done using **DHCP discover message**. The DHCP discover message is in a UDP packet which is encapsulated with a IP datagram. The host sends the IP datagram but does not know the IP address of the server which will be connected to, so host does a broadcast with IP address 255.255.255.255 to all nodes in the subnet. Host’s assumed IP address is 0.0.0.0.
2. **DHCP server offer:** The DHCP server which receives the discover message replies client with a **DHCP offer message** with a broadcast to all nodes on the subnet, with IP broadcast address 255.255.255.255. There may exist several DHCP servers, so the client may find the most appropriate server for itself. Each DHCP offer message contains the transaction ID of the discover message, the offered IP address for the DHCP client, the network mask and amount of time for which IP address will be valid.
3. **DHCP request:** The client selectsa DHCP server and sends a **DHCP request message** to selected server.
4. **DHCP ACK:** The server responds request message of client with **DHCP ACK message** that indicates verifying requested parameters.

In Figure 1.1 and Figure 1.2, all 4 stages of DHCP can be observed which have same transaction IDs. In DHCP discover stage, the destination IP address can be observed as 255.255.255.255 because of broadcasting. The source IP address can be observed as 0.0.0.0 because the client does not have any IP address yet and its IP address is assumed as 0.0.0.0.

To observe DHCP stages from Wireshark, firstly I released my current IP address with “ipconfig /release” command. Then, to take a new IP address, I wrote “ipconfig /renew” command to the terminal. I sniffed the packets synchronously with these commands.

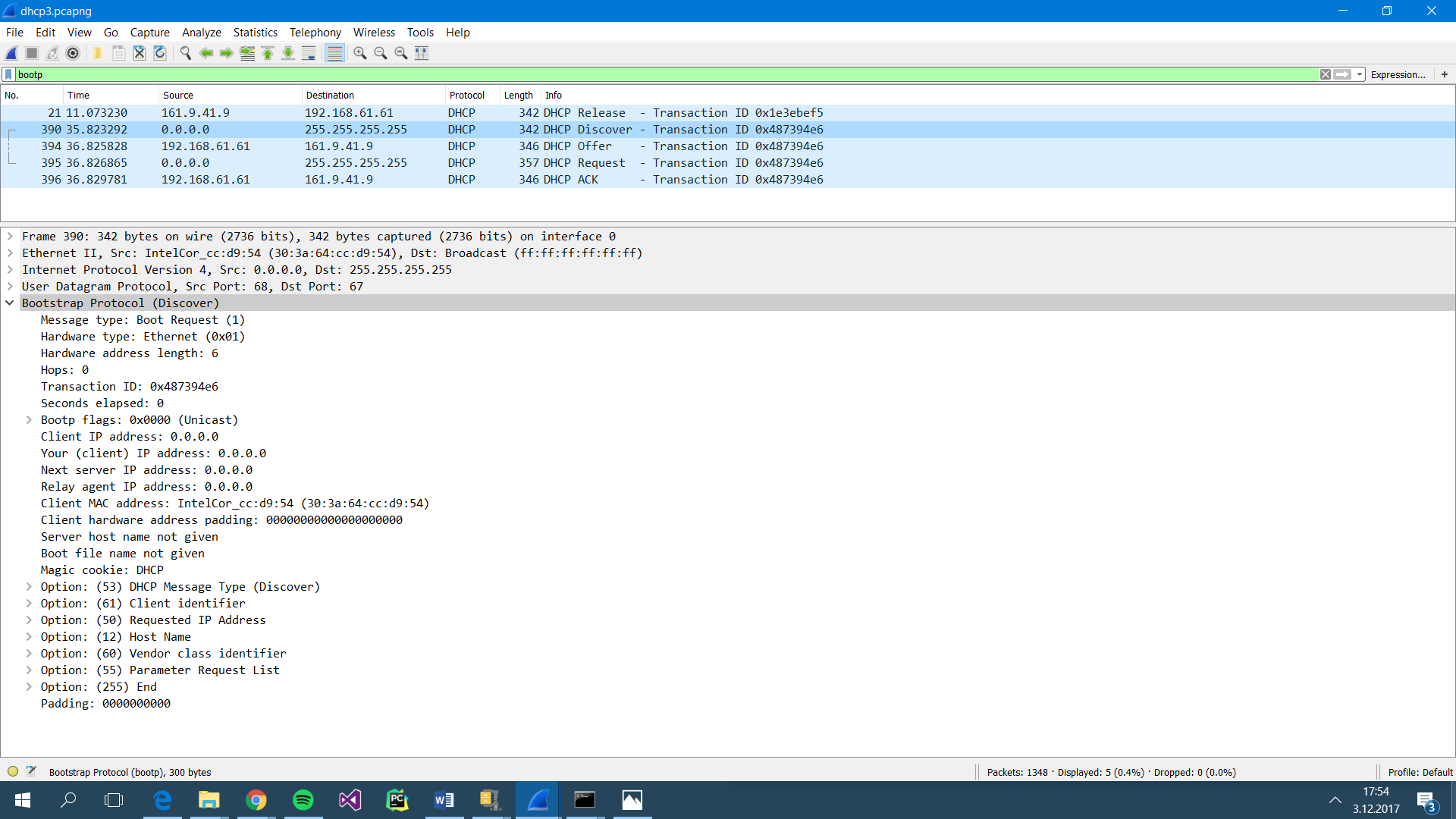


Figure 1.1: Wireshark screenshot shows DHCP stages

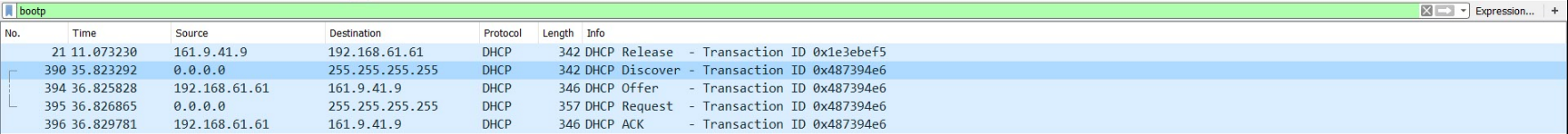


Figure 1.2: Expanded Wireshark screenshot of DHCP stages

(Stages with same Transaction IDs -last 4 rows- correspond one DHCP process.)

1. **Domain Name System (DNS)** ensures matching the IP addresses with hostnames for hosts. DNS contains the following steps:
2. Client runs the client side of the DNS application.
3. Browser extracts the hostname and passes to the client side.
4. DNS client sends a DNS query which includes hostname to the DNS server.
5. DNS client receives a response from the DNS server which includes the IP address of the host.
6. The browser takes the IP address of the host and provides a connection to the HTTP server.

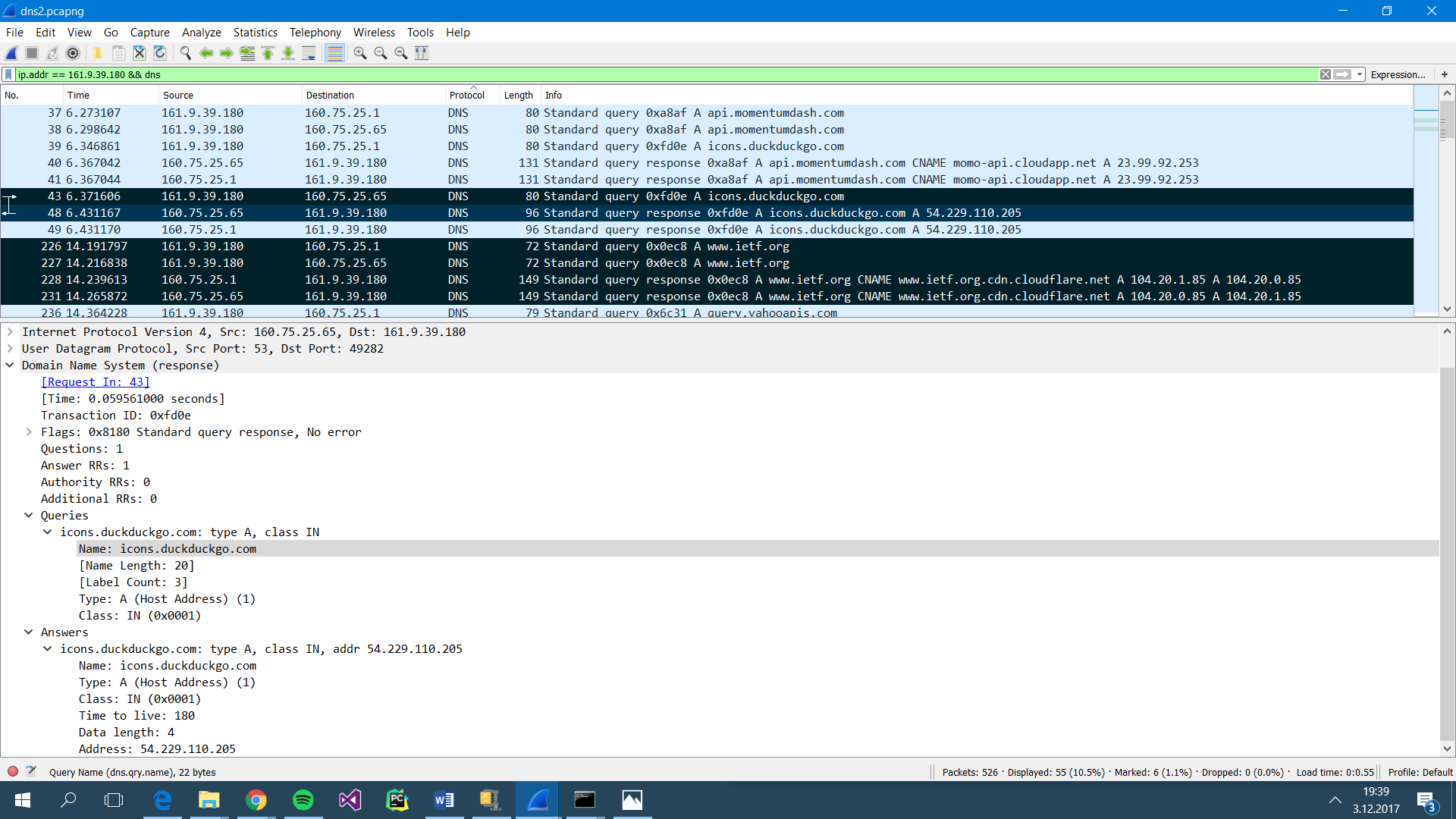
 Figure 2.1: DNS queries and query responses for new web sites

 Figure 2.2: DNS query and query response for the hostname “www.duckduckgo.com”

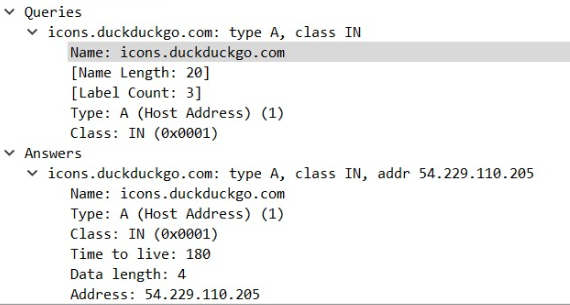


Figure 2.3: IP address of the www.duckduckgo.com is 54.229.110.205.

**IP address of the DNS server is 160.75.25.65** from the Figure 2.2, because destination address of the standard query is DNS server’s IP address and source of the standard query is DNS client. After DNS query, DNS query response comes from the DNS server and its destination address is DNS client.

**IP address of the website (which has the hostname “www.duckduckgo.com”) is 54.229.110.205** from Figure 2.3. Host’s IP address is indicated at “Answers” part of the Figure 2.3.

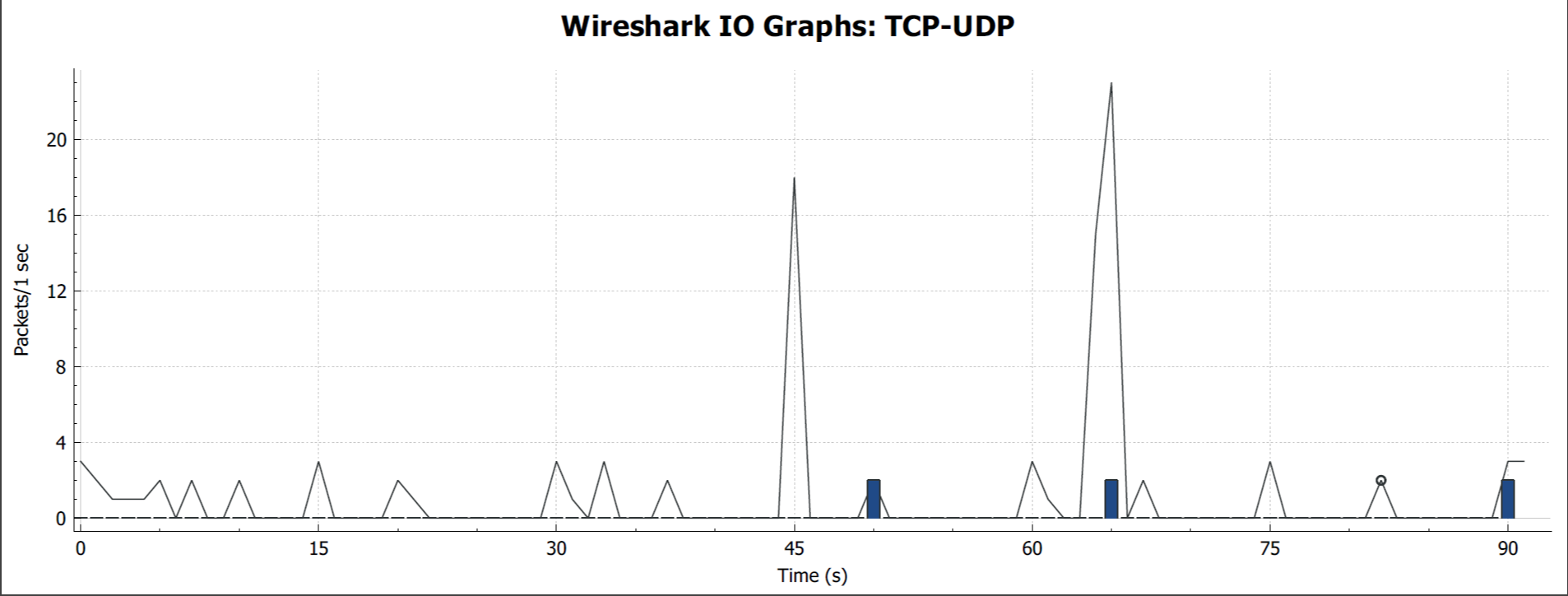
1. Bandwidth is determined as 100Mbit and in each sequence, bandwidth is increased with 100 Mbit up to 500 Mbit.

Packet length: 500B

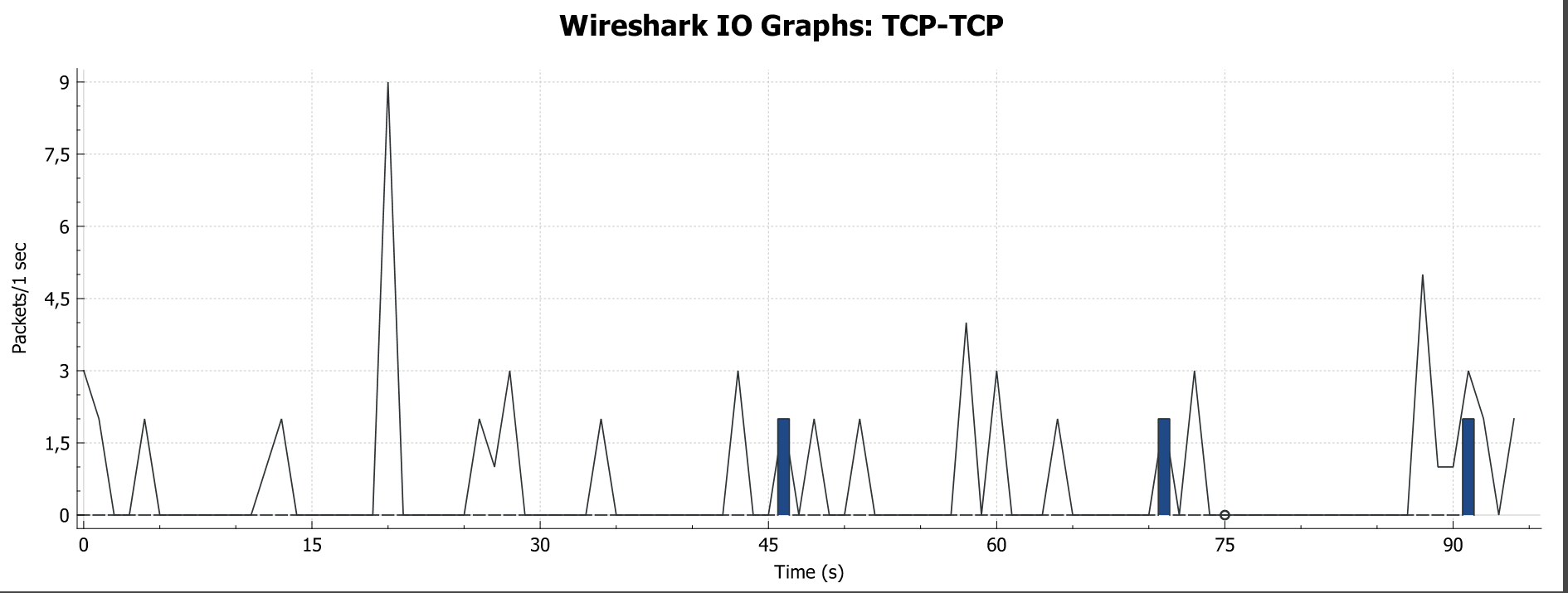
Number of generated packets per flow: 100M

For each analysis, 2 servers and 2 clients are generated with iperf3 and I/O graphs are observed with Wireshark.

**Analysis 1:**



**Analysis 2:**



* Packet header is larger in TCP (192 bit) than in UDP (64 bit). Because of that, in Analysis 1, the generated packets are less.

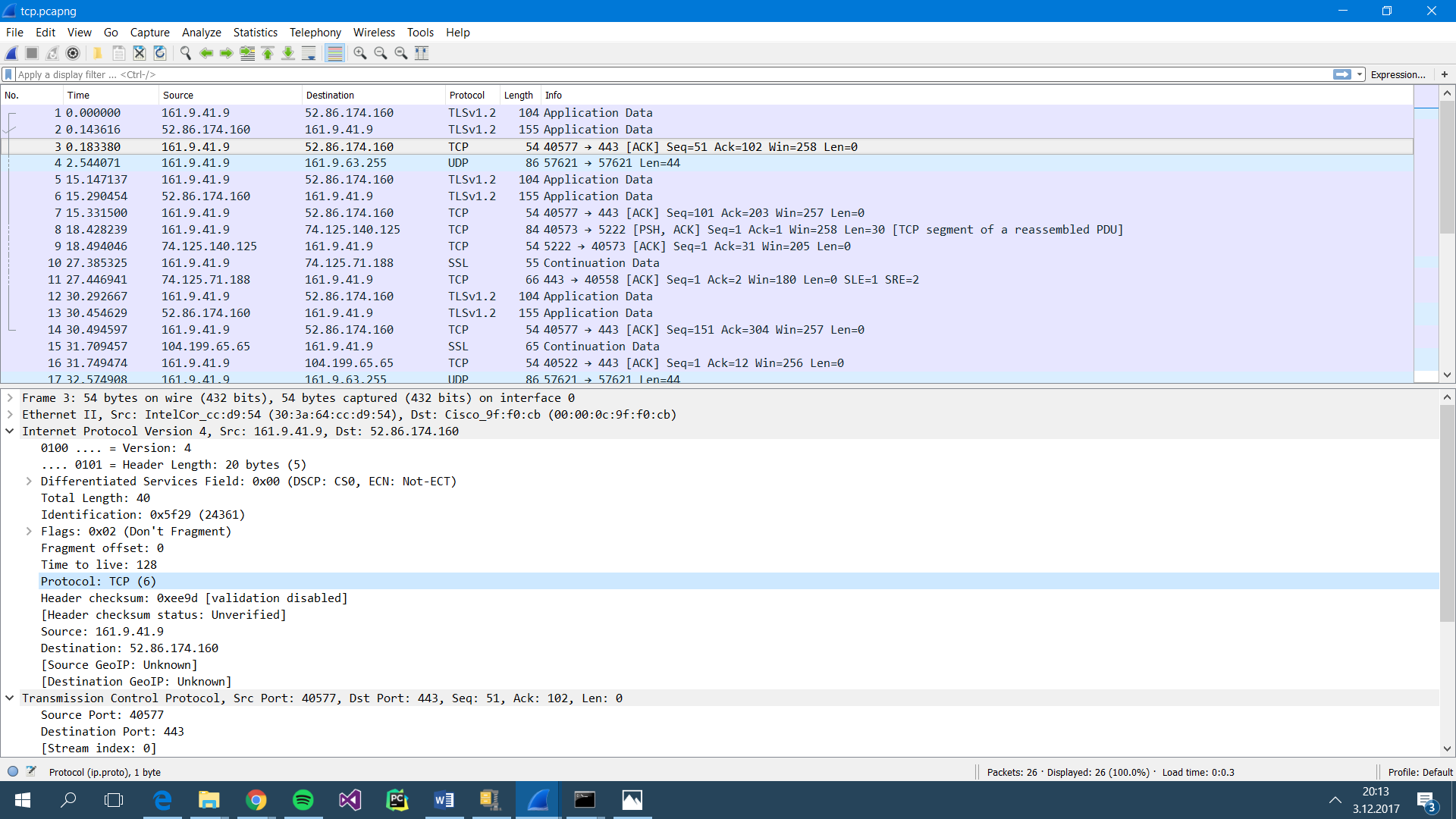


Figure 3.1: Protocol number of TCP is 6 as shown in Wireshark capture.

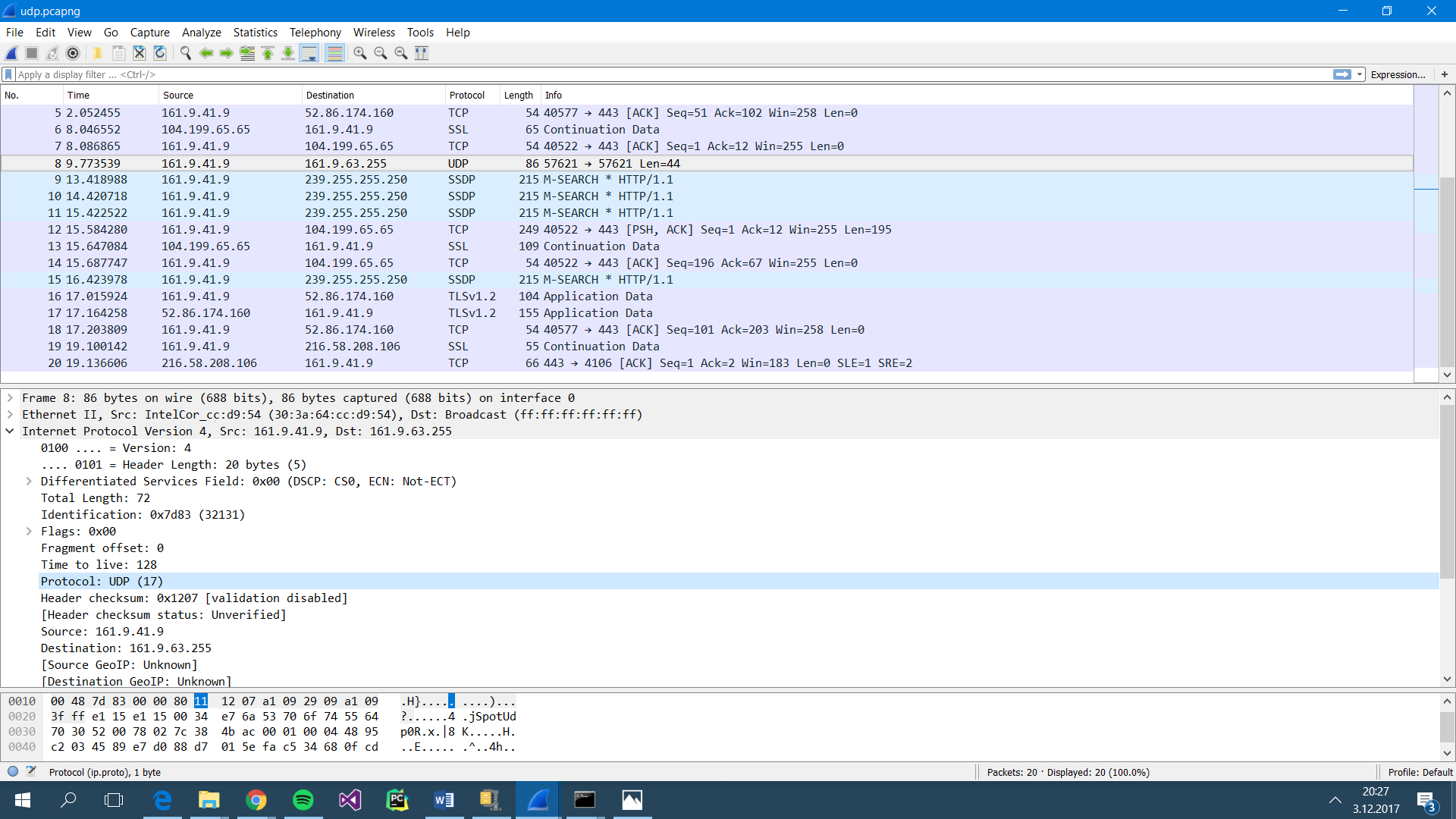


Figure 3.2: Protocol number of UDP is 17 as shown in Wireshark capture.