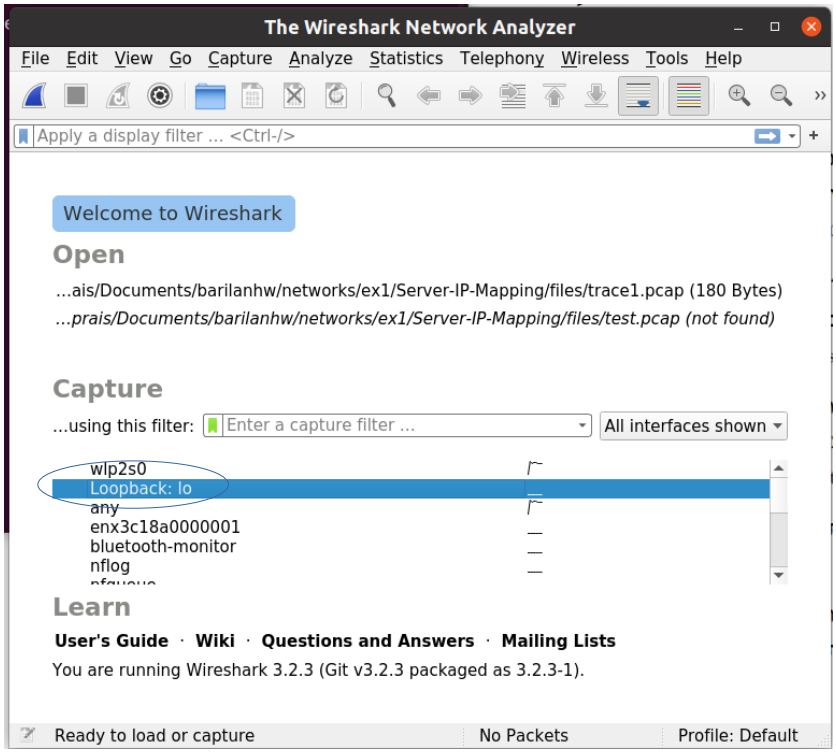
Networks - Assignment 1 Report

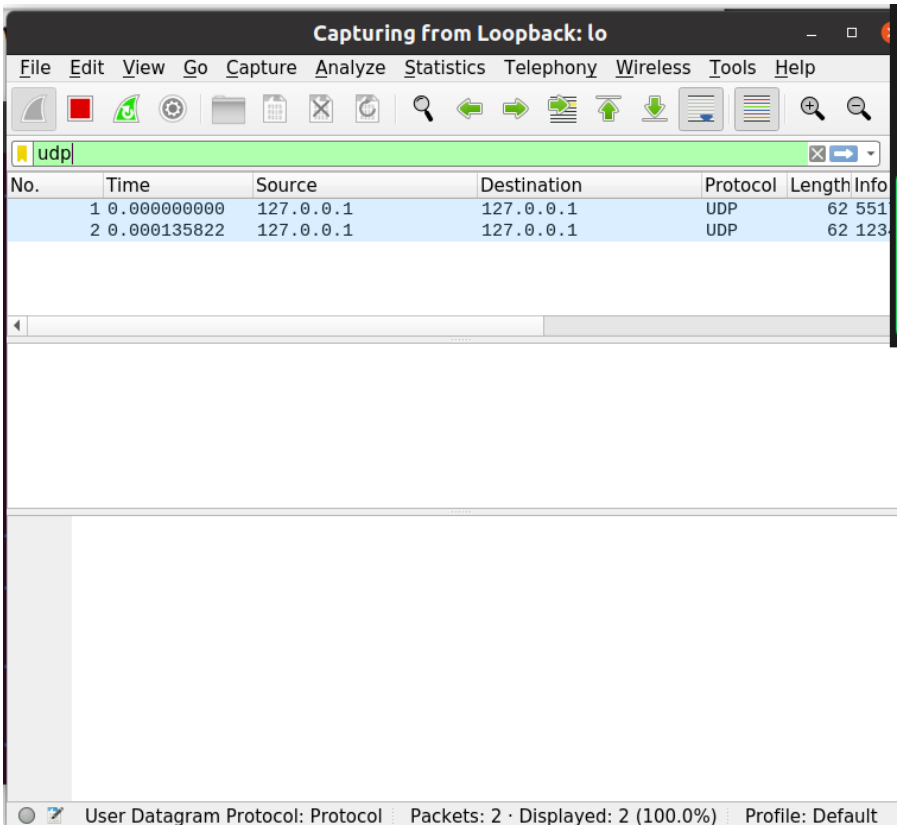
Part 1

How we Filtered the Packets

First, we opened the wireshark and got into loopback to listen to the transport in the local machine.



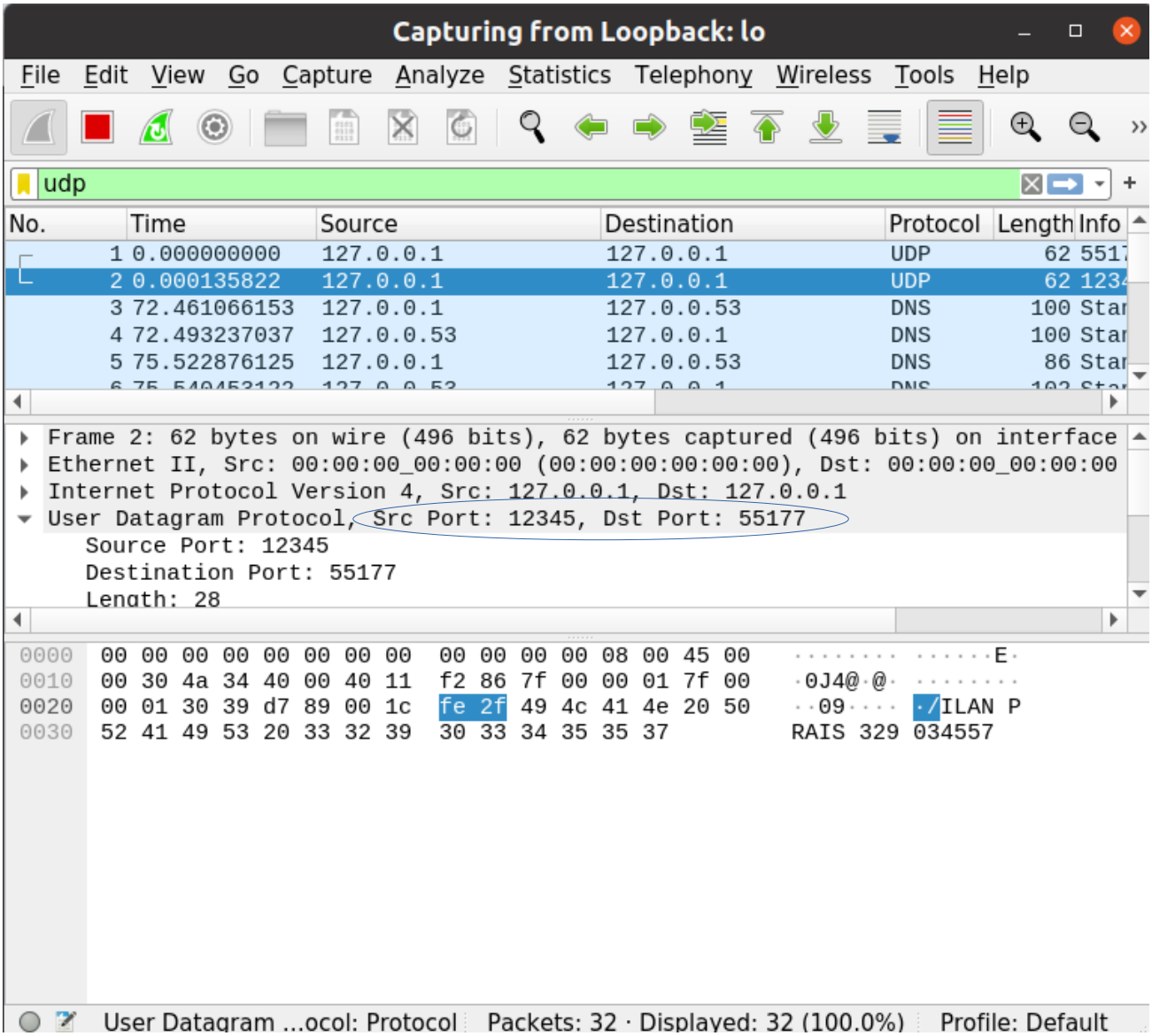
We filtered the packets according to their specific protocol, in purpose to find the UDP packets, where our packets are exist. We found two packets – the packet that the client sent to the server, and the packet that the server sent to the client.



About the Port Numbers

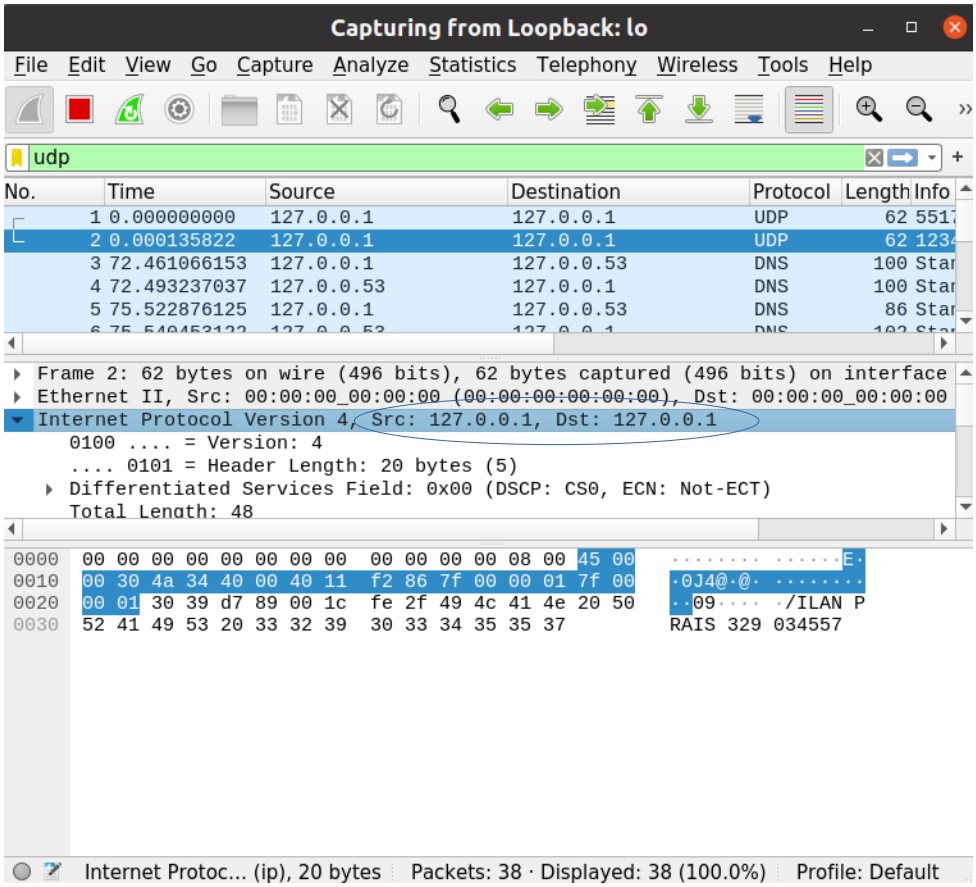
The ports are numbers that specify the actual resource in the computer the message is sent to or recieved from. For example, in client-server architecture, the server is binded to a specific port which the client knows, so when the client sends a message to the server, he sends it to the server ip address, on the server port.

In the wireshark, we can see two port numbers in the packet header – the first port is the sender port on his local machine, and the second port is the reciever port on his local machine (for example, in the packet that the client sent to the server, the first port is the client port, and the second port is the server port).The port logic is in the Transport layer.

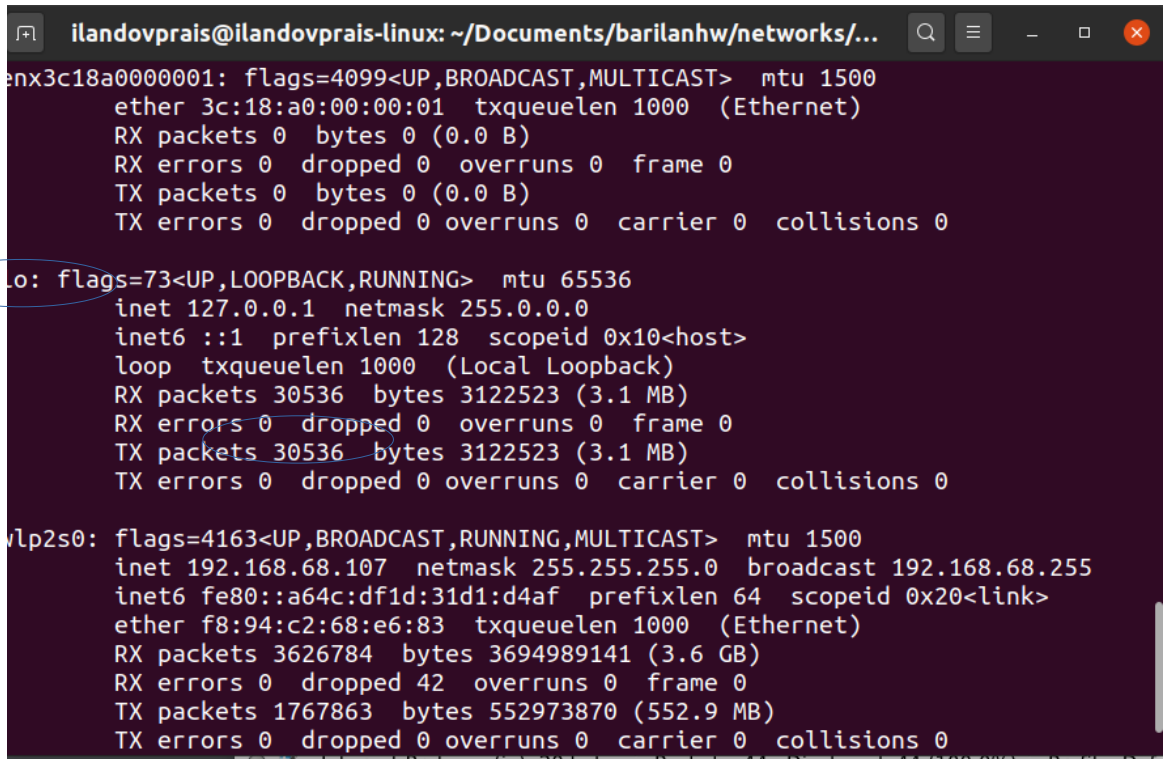


About the IP Addresses

The first ip address in the packet header is the ip address of the sender, and the second ip address is the ip address of the reciever.



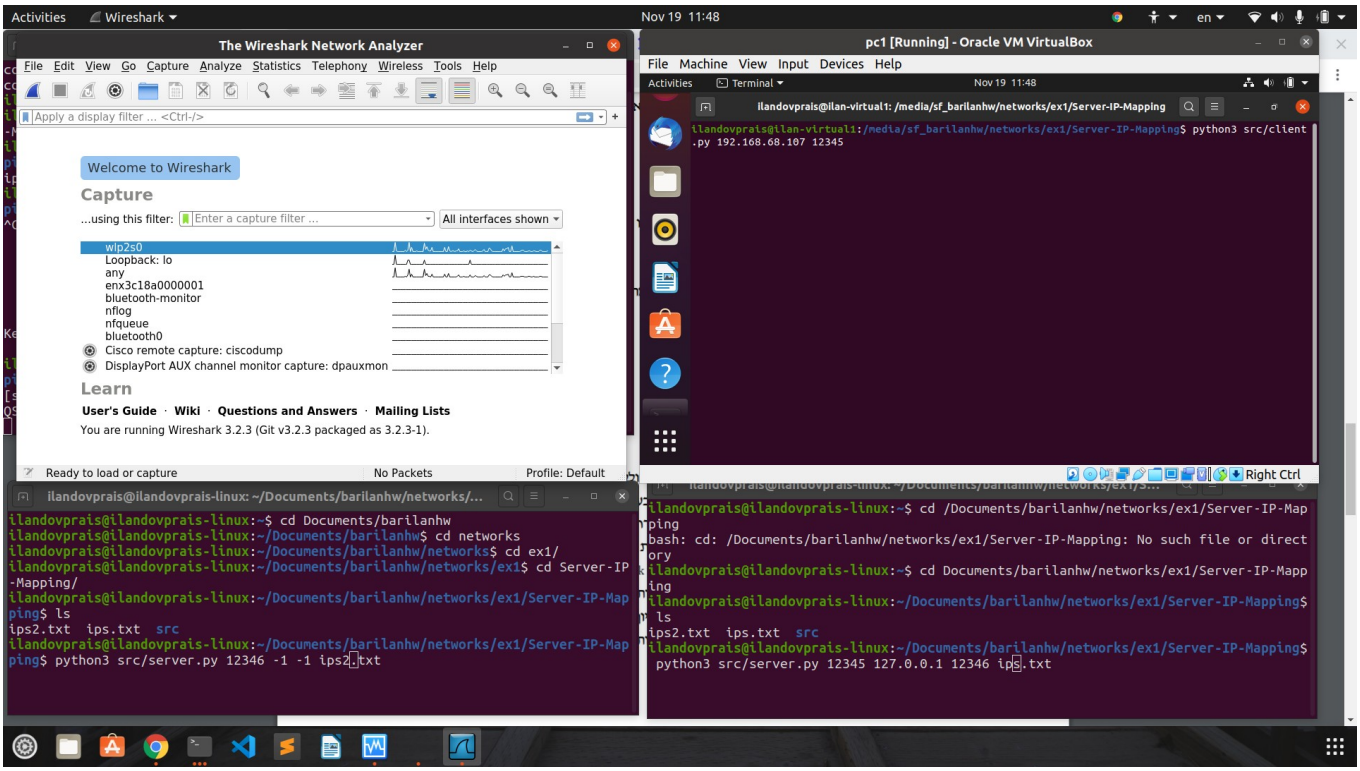
As we can see, the ip addresses in the packet header are similar to the ip addresses of the local machine, that we found using the ifconfing command.



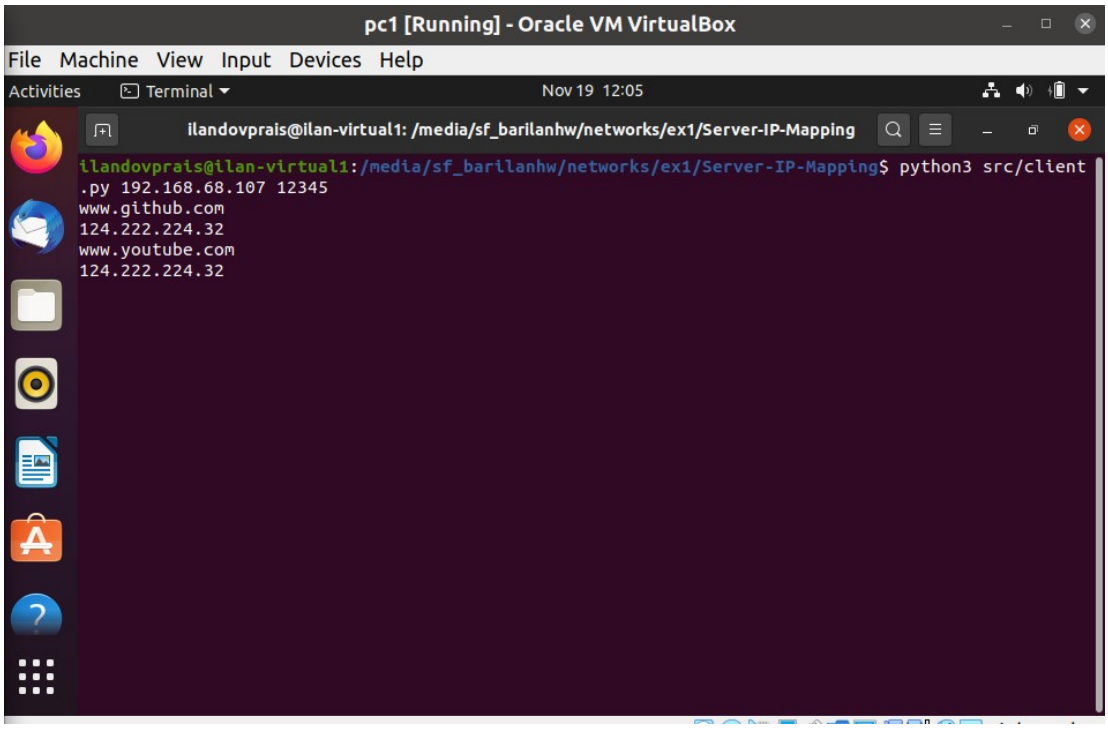
Part 2

Running the servers and the client

First, we opened 2 termials in the host computer, 1 terminal for each server, and also started the virtual machine. Then we opened the parent server on 1 terminal, the child server on the other and the client on the virtual machine. We used ifconfig to find the ip adress of the server so the client could connect to it. Then we opened wireshark.

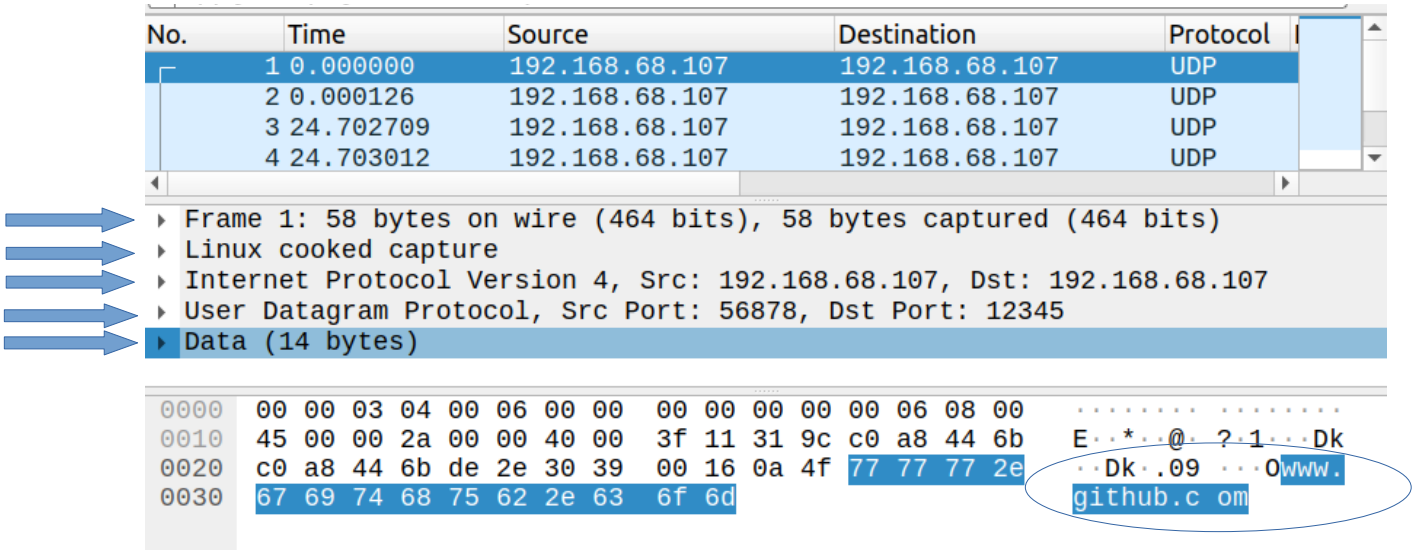


We opened the server and ran the client. First, we gave it the input “www.github.com” which the child server knows, so the ip was returned. Afterwards, the client requested the ip of “www.youtube.com”, which the child does not have,but the parent does so the child requested it from his father and returned it to the client.



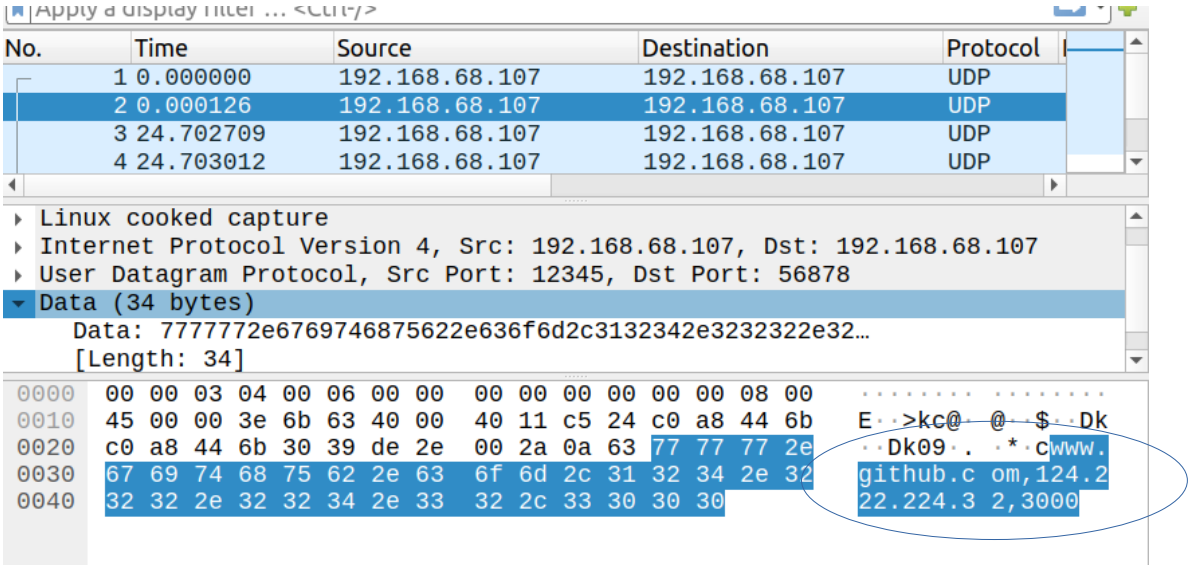
Capturing the packets in Wireshark

while running the servers and the client, we sniffed the packages using wireshark. Let's look at the first request: "www.github.com" -> "124.222.224.32"



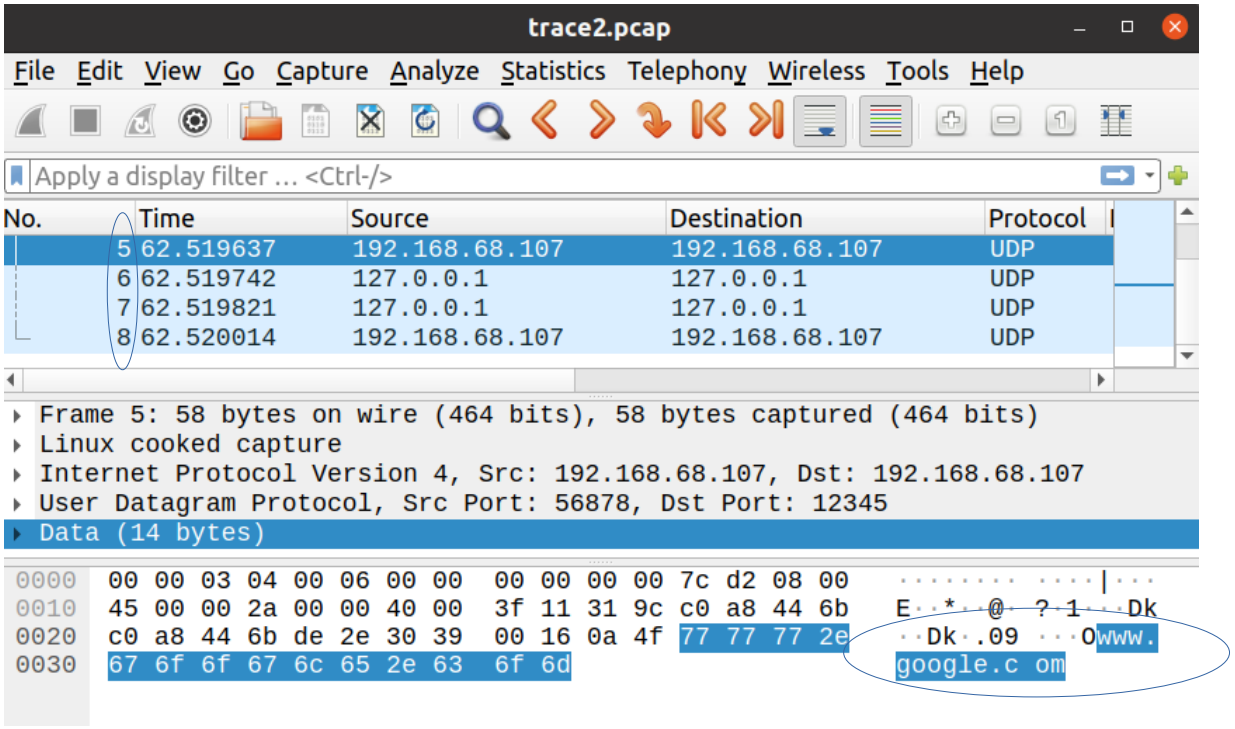
As we can see, "www.github.com" appears in the data in the application layer. In the transport layer, we can see that udp protocol was used, and the packet was sent from port 56878 on the virtual machine client to port 12345 on the server. In the network layer, we can see ipv4 is used, and that the package was sent from the virtual machine with ip 192.168.68.107 to the server, 192.168.68.107 (they have the same ip because the vm uses the host network).In the data link layer the mac is specified, and in the physical layer we can see that 58 bytes were sent in total.

Similarly, we captured the server's respond:



The packet is similer to the previous one, however this time the src and dest port and ip are swapped, and the message is the domain with it's ip and ttl.

Next, we captures the second request – where the server had to request the ip from his parent server



As we can see, this time there are 4 packets – the client request, the child server request, the parent response, and then the chid server response.

(packet 5) The client request was sent from ip 192.168.68.107 port 56878 to the child server, at 192.168.68.107 port 12345.

(packet 6) The child server did not have the requested ip in it's ips.txt file, so it requested the ip from his parent server- and as they are on the same machine, the request was sent from and to ip 127.0.0.1 (but different ports).

(packet 7) The parent server had the requested ip, so it sent it to the child server, again at ip 127.0.0.1.

(packet 8) Finally, the child server had the requested ip so it sent it to the client.