Part 2:

In this part we decided to run our server.py code twice on two separate terminals in Server's VM and client.py on terminal in Client's VM just like you guided us in the exercise.

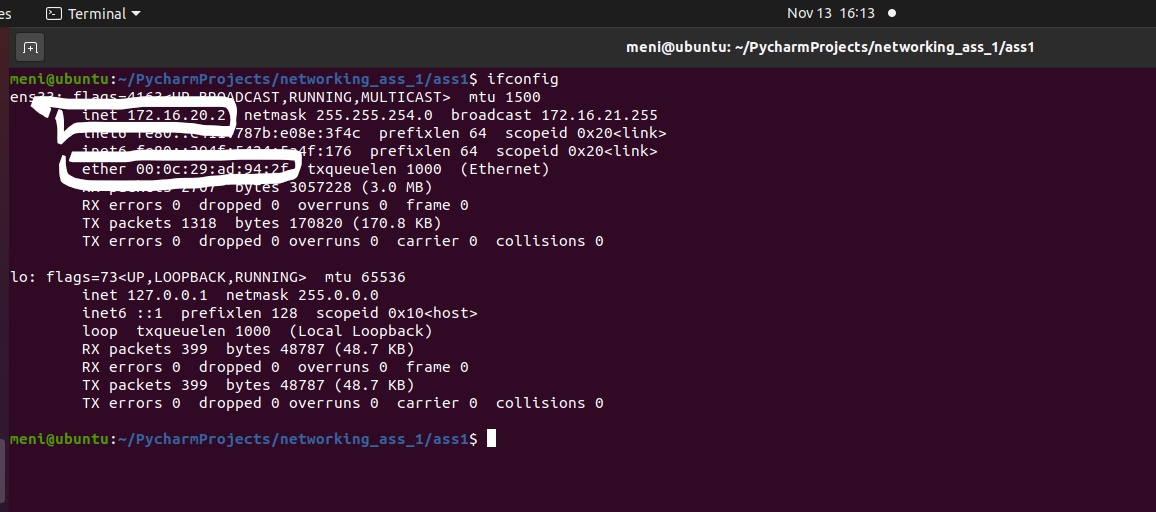
Now first lets determine the ip's and MAC's of the VM's:

Server VM:

Ip: 172.16.20.2

MAC : 00:0c:29:ad:94:2f

Print screen to show how I found these details:

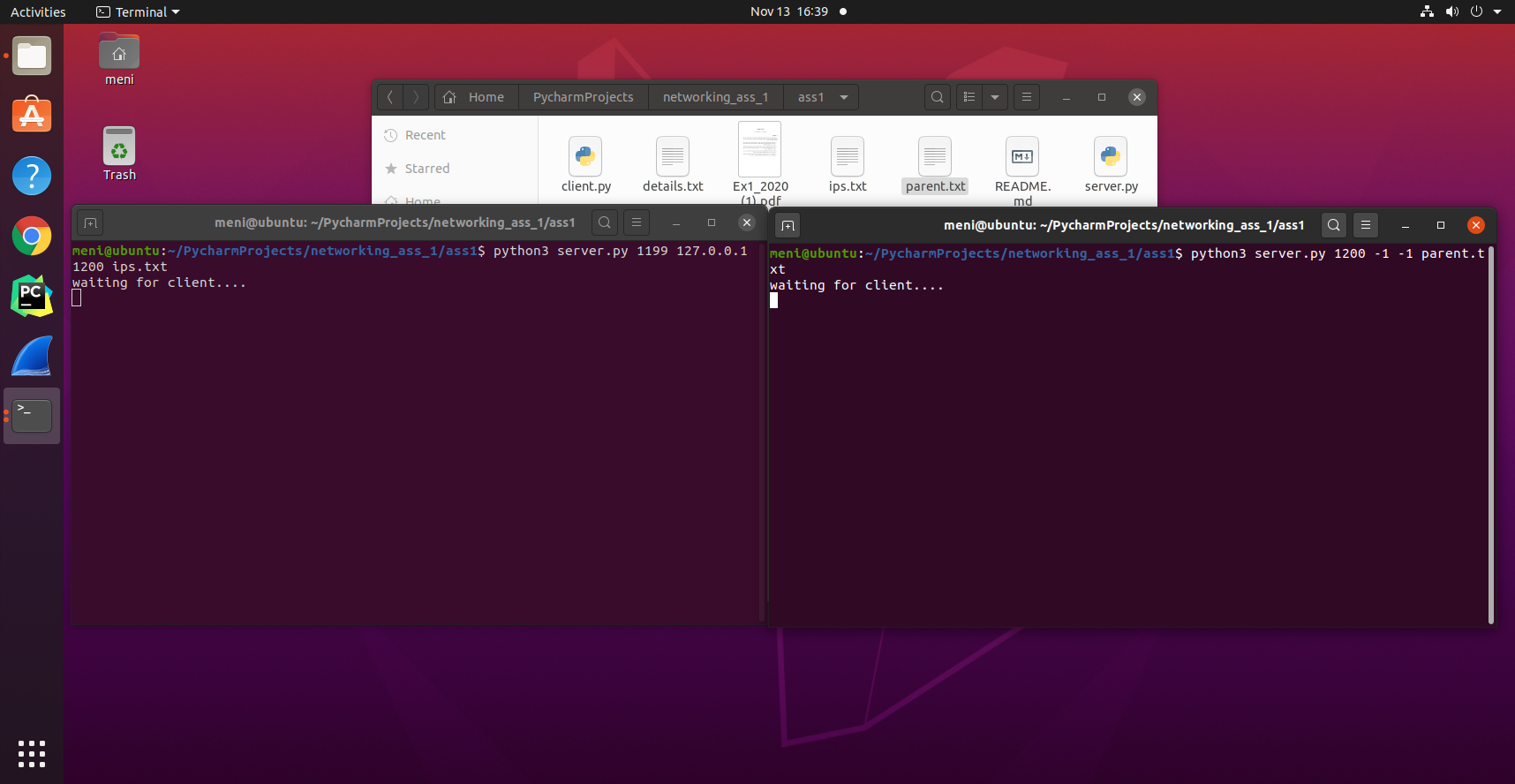


Let's run the server and its father on Server VM:

Command to run father server: python3 server.py 1200 -1 -1 parent.txt

Command to run original server: python3 server.py 1199 127.0.0.1 1200 ips.txt

Now they are working, screenshot:

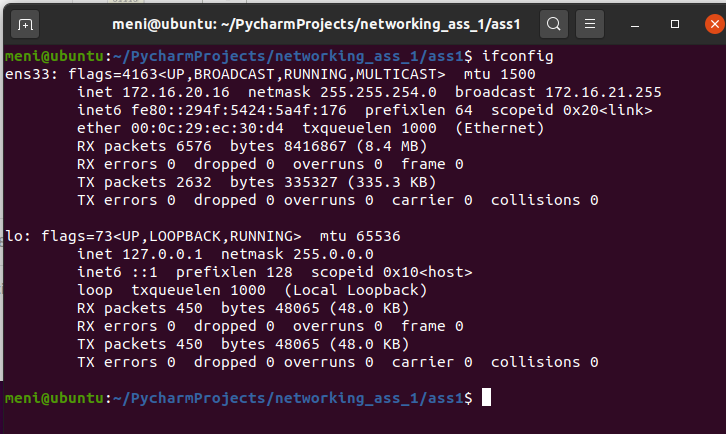


Client VM:

Ip: 172.16.20.16

MAC: 00:0c:29:ec:30:d4

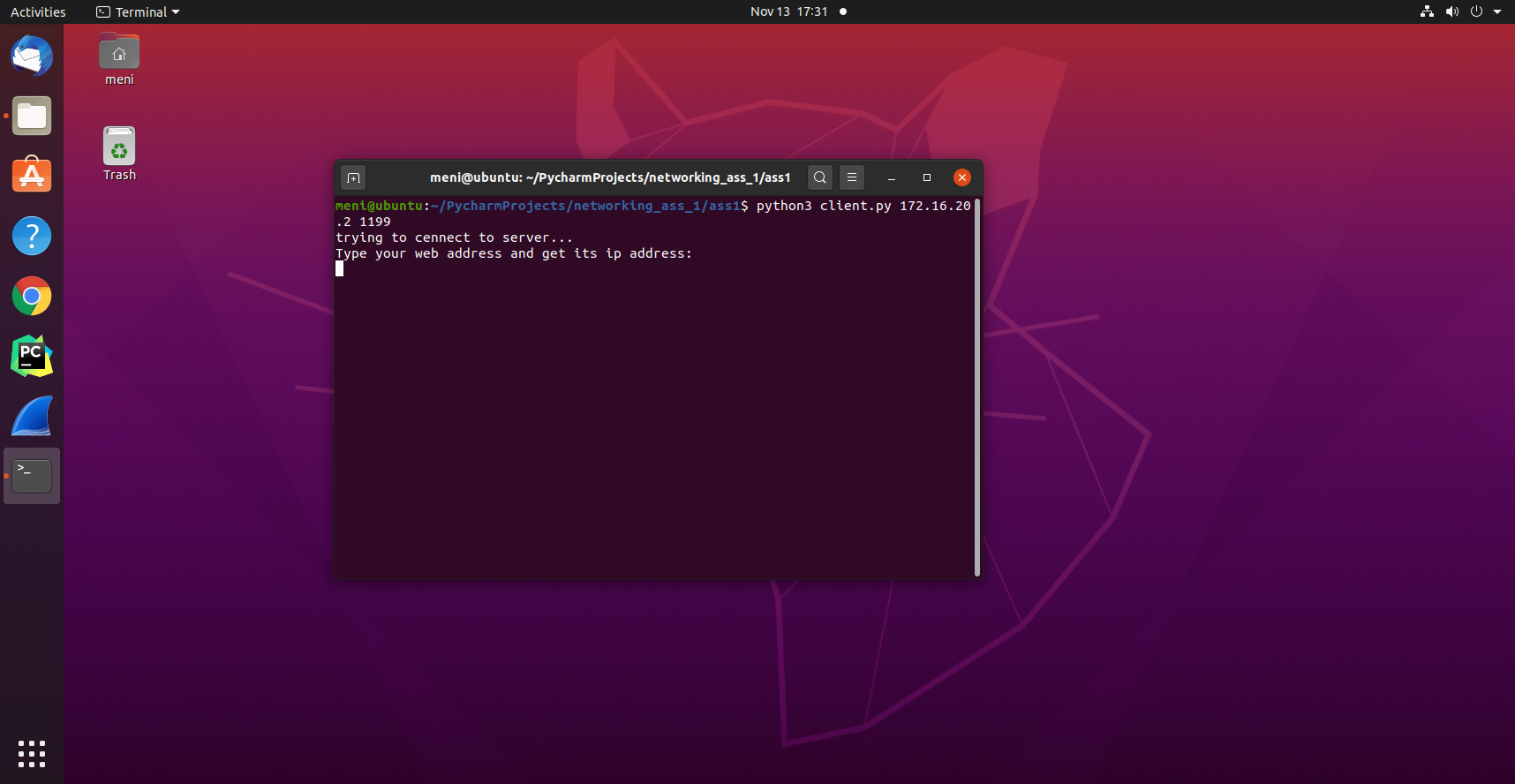
Print screen to show how I found these details:



Let's run the client on Client VM:

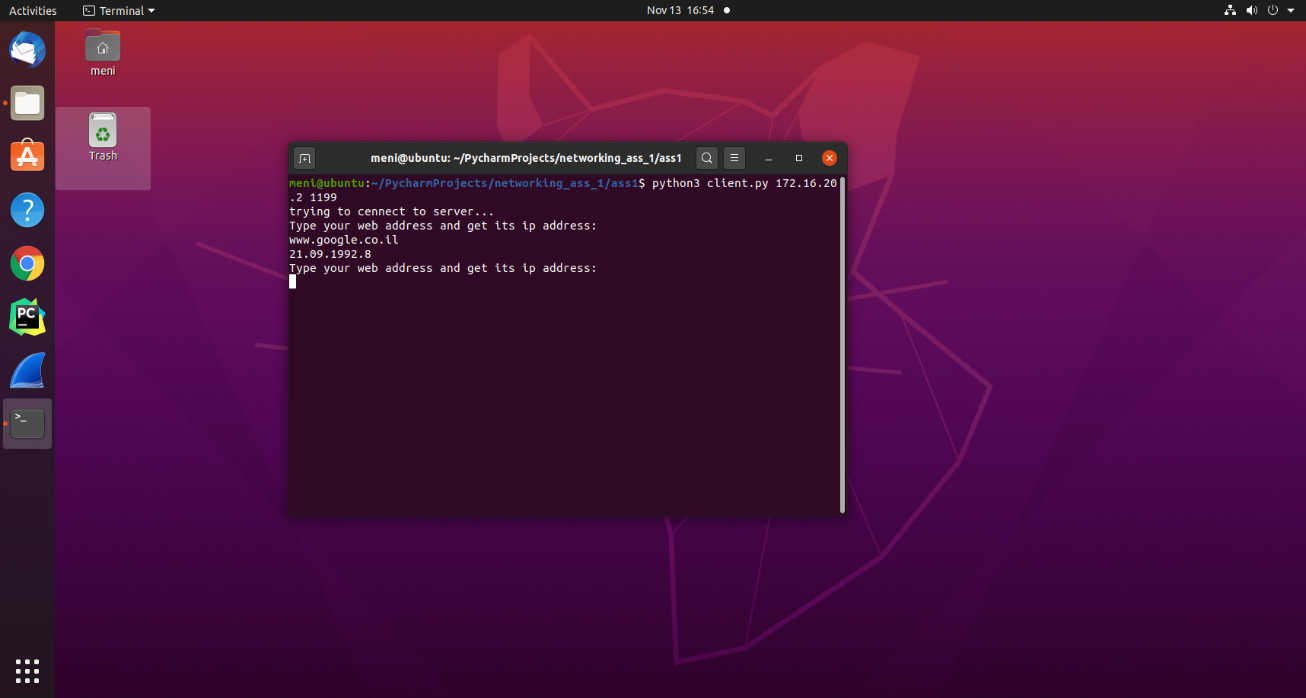
Command to run client: python3 client.py 172.16.20.2 1199

Screenshot:

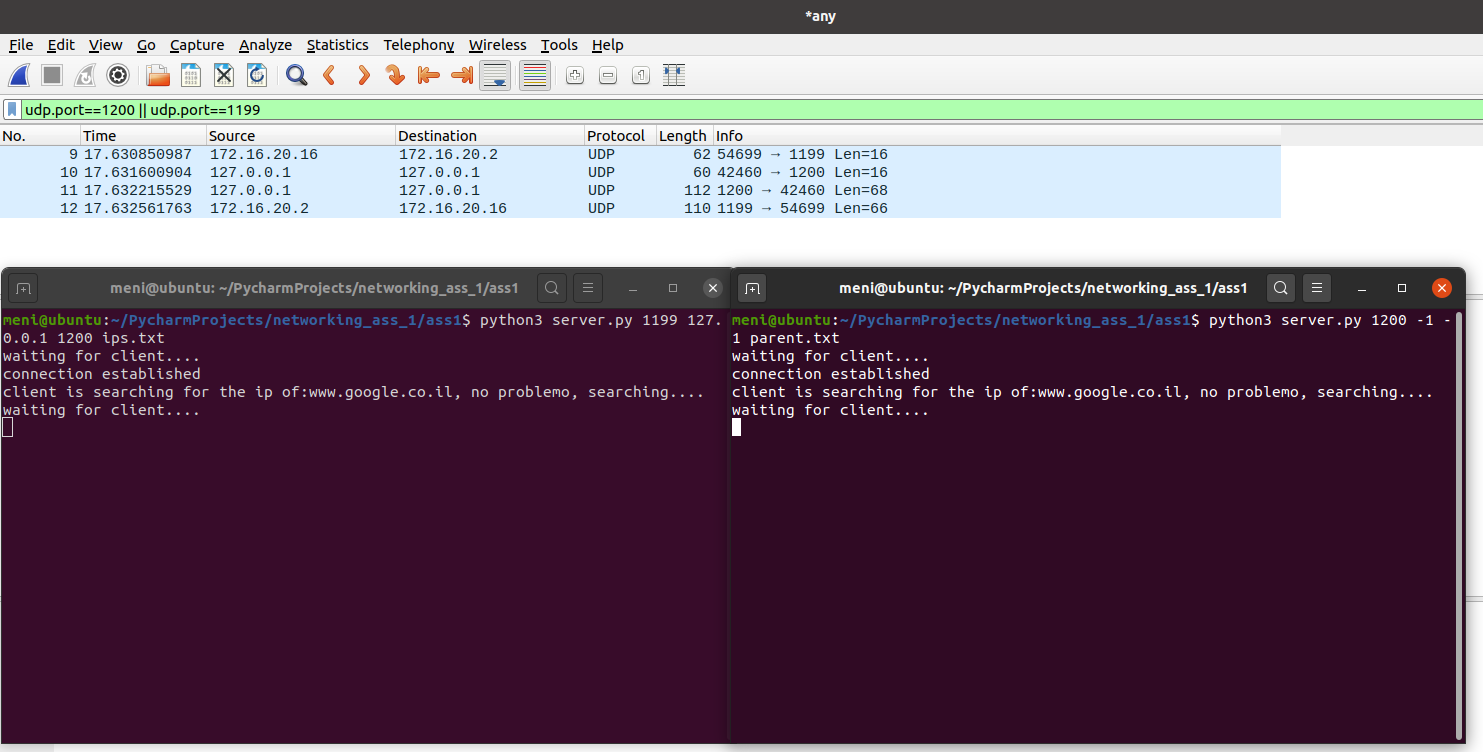


Now let's cut to the chase: try to send query to the server with an address that exists only in father server's file so the original server will have to ask for that info from the father server:

View from client:

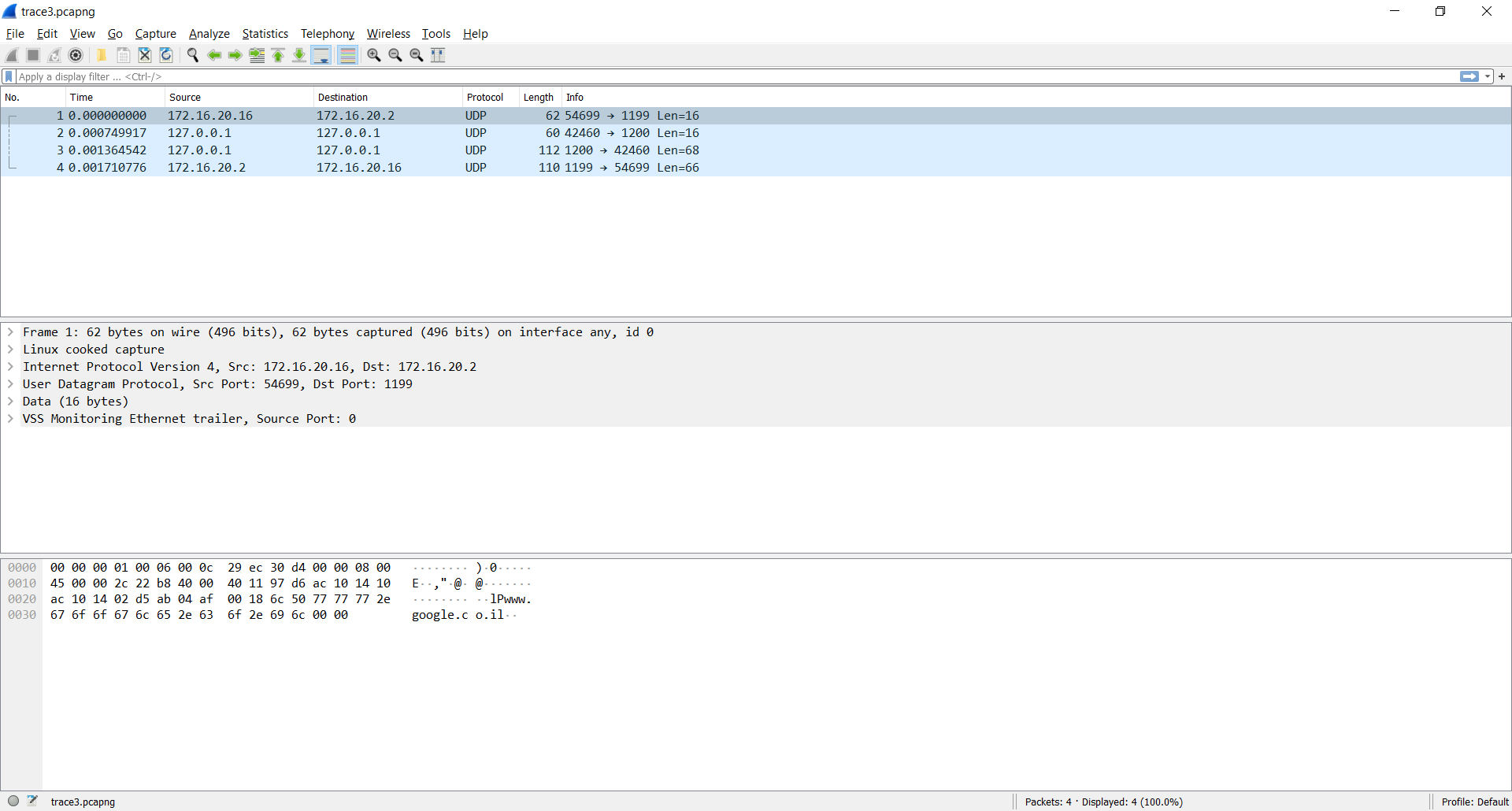


View from servers machine :



To conclude: let's see the sniffing from wireshark and analyze the data from it:

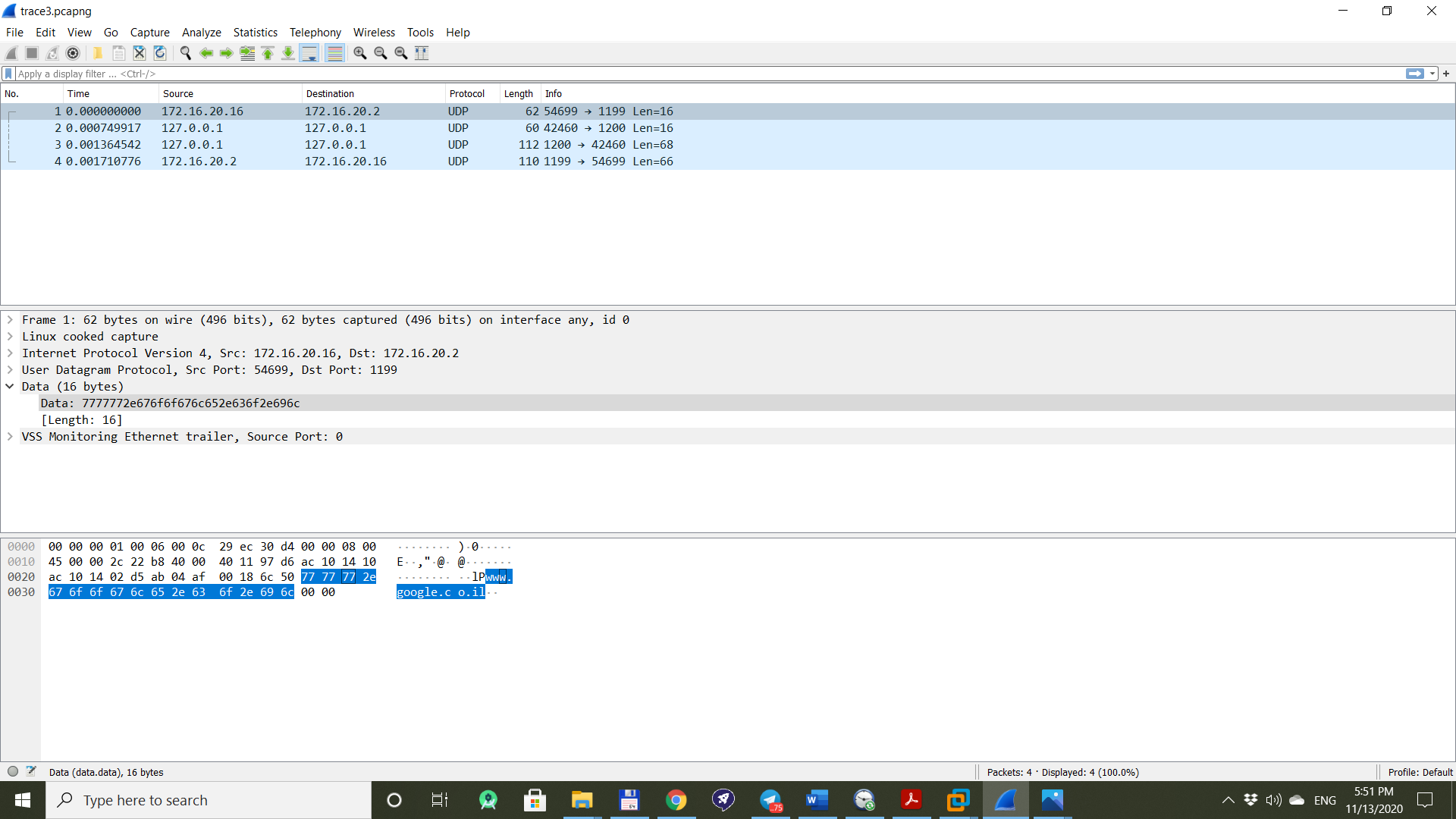
Open the trace2.pcap file:



Now I will show you how to data was sent from the client's machine to the server's machine to the destinated port – top to bottom and vice versa:

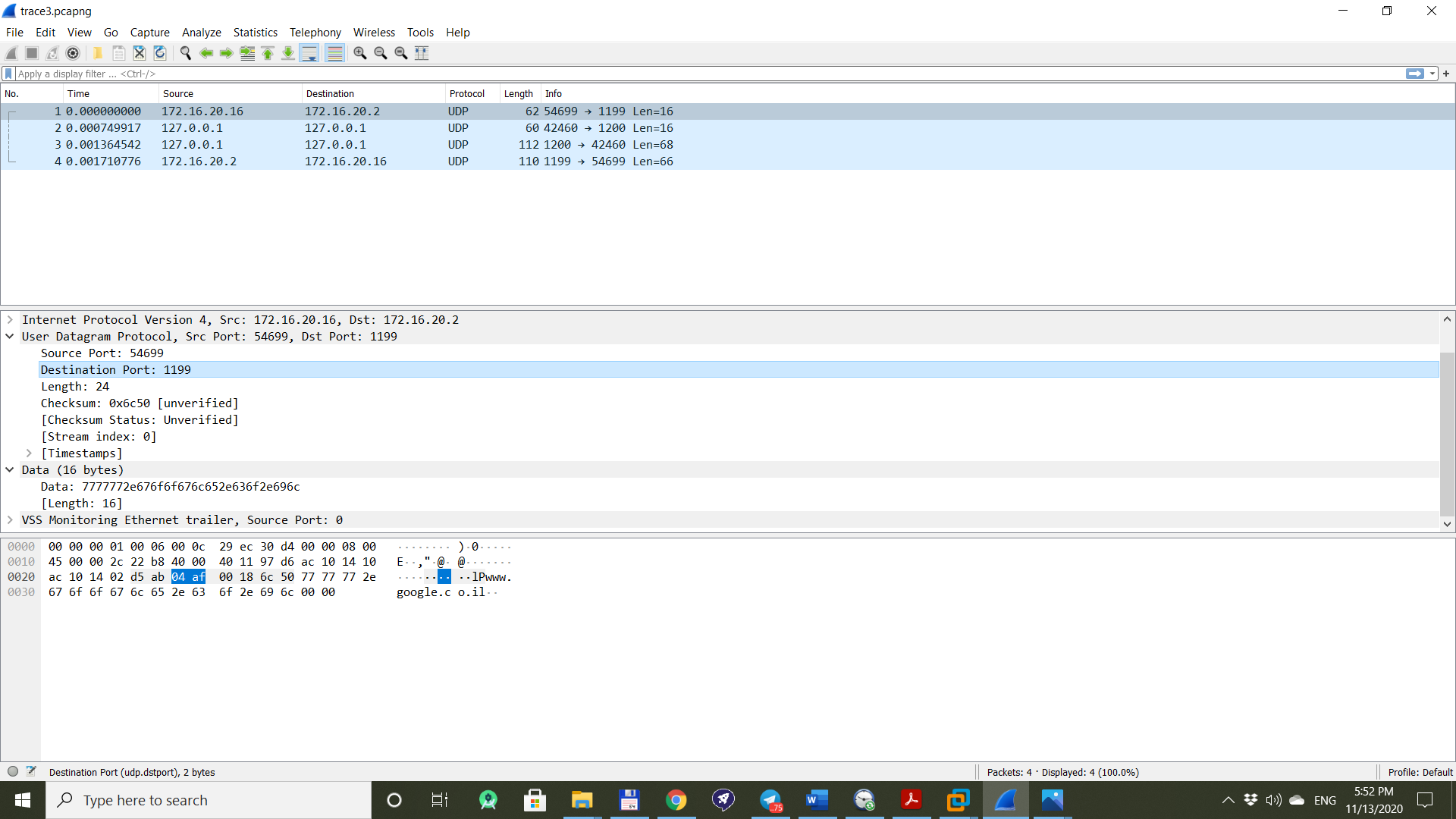
First the client sends data to the main server so I expect to see in the Application layer the data that was sent to the main server

First line indicates that socket opened between the original server and the client, at the Data tab we can see the string of the query



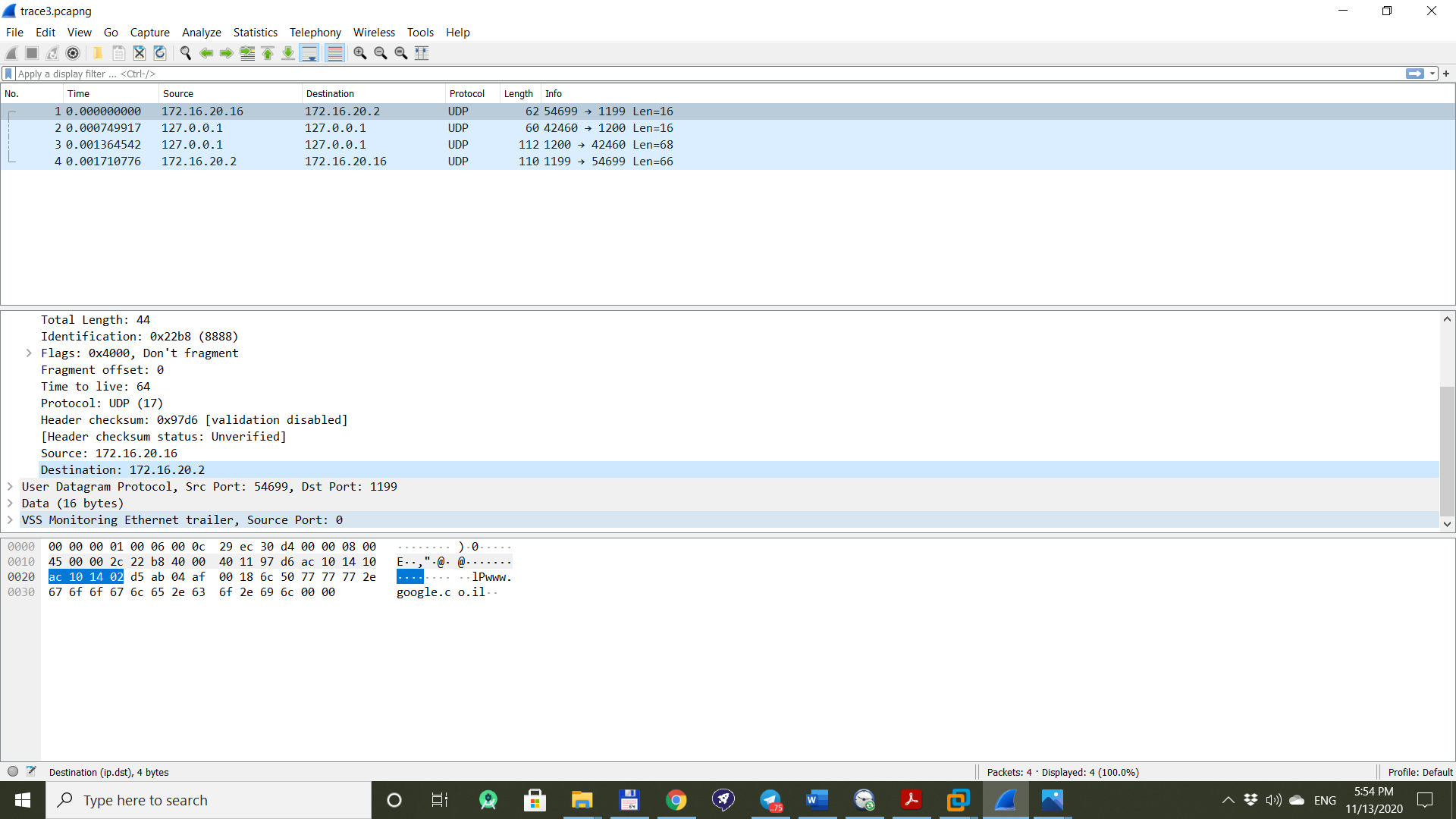
Now lets get to the lower tab – the Datagram tab which is related to the determination which network conversation protocol (TCP or UDP) is used for this conversation.

If you open the Datagram tab which is related to the transport layer you can see that the dest port is 1199 which is the port of our server program

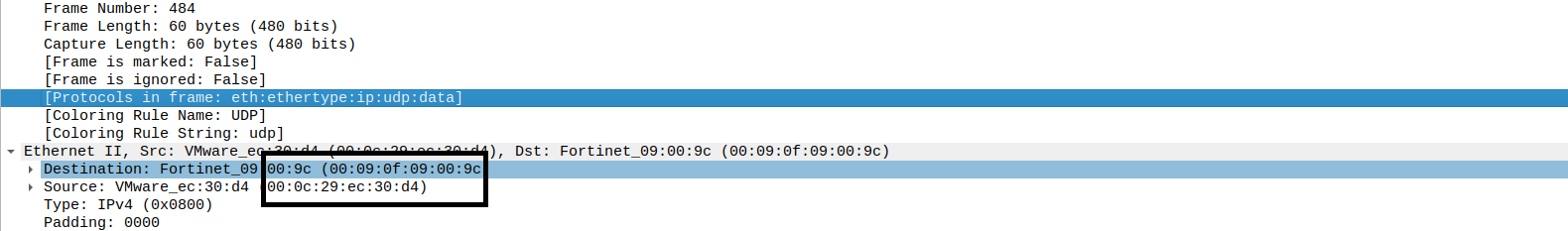


Now lets get lower to the internet tab and then we will see that the des tip is the ip of our main server machine and the source ip is the ip of the client's machine

If you open the Internet tab which is related to network layer you will see that the src ip is the ip of the client machine and the dest ip is the ip of the server machine



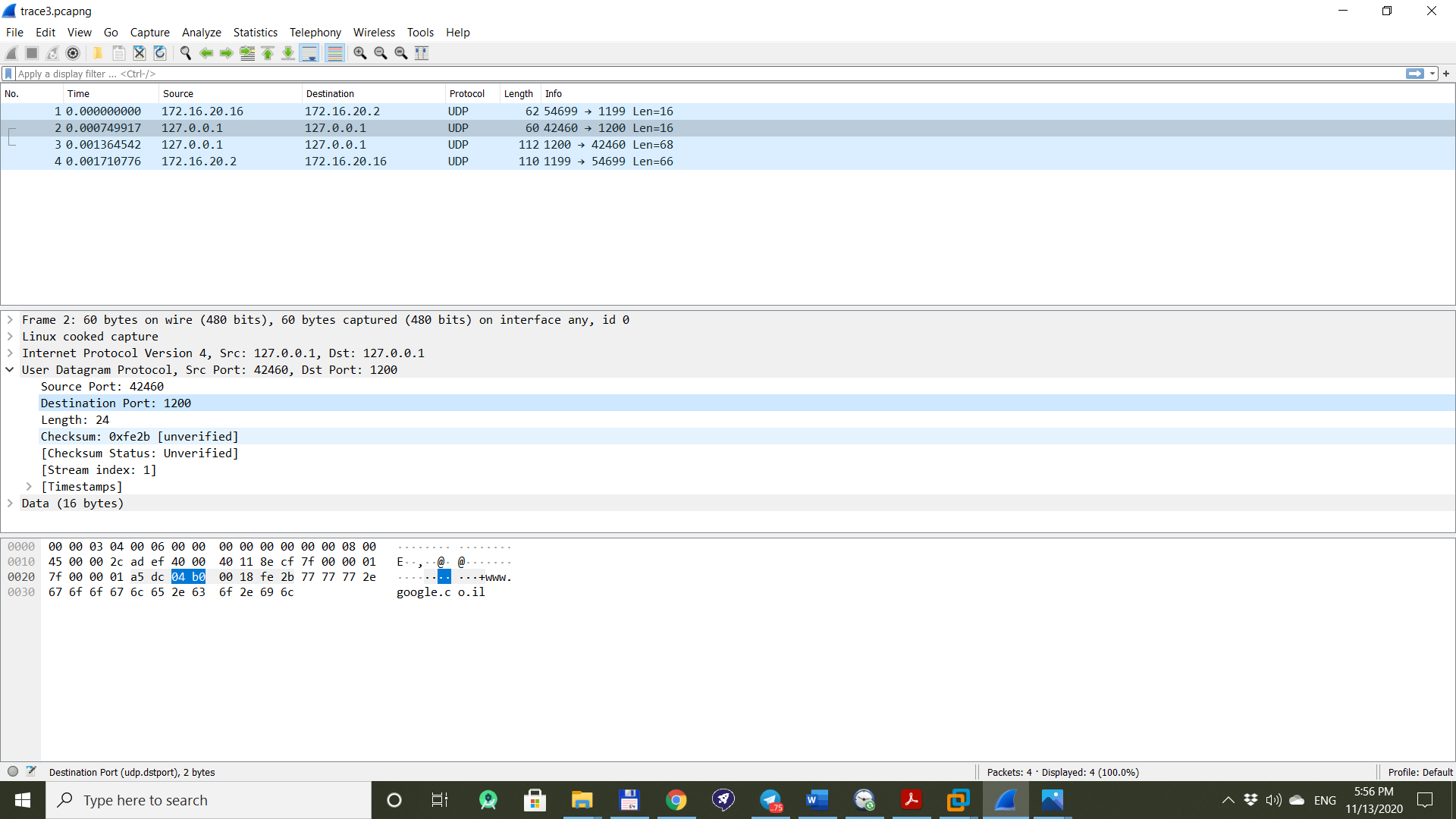
Lets get lower to the lowest layer – the data link layer where I expect to see the Mac Addresses of the source, aka the client's machine, and the dest Mac Adress, aka the main server's machine



Here we can see that the dst Mac marked is the Mac of the main server's machine and the src Mac is the Mac of the client's machine

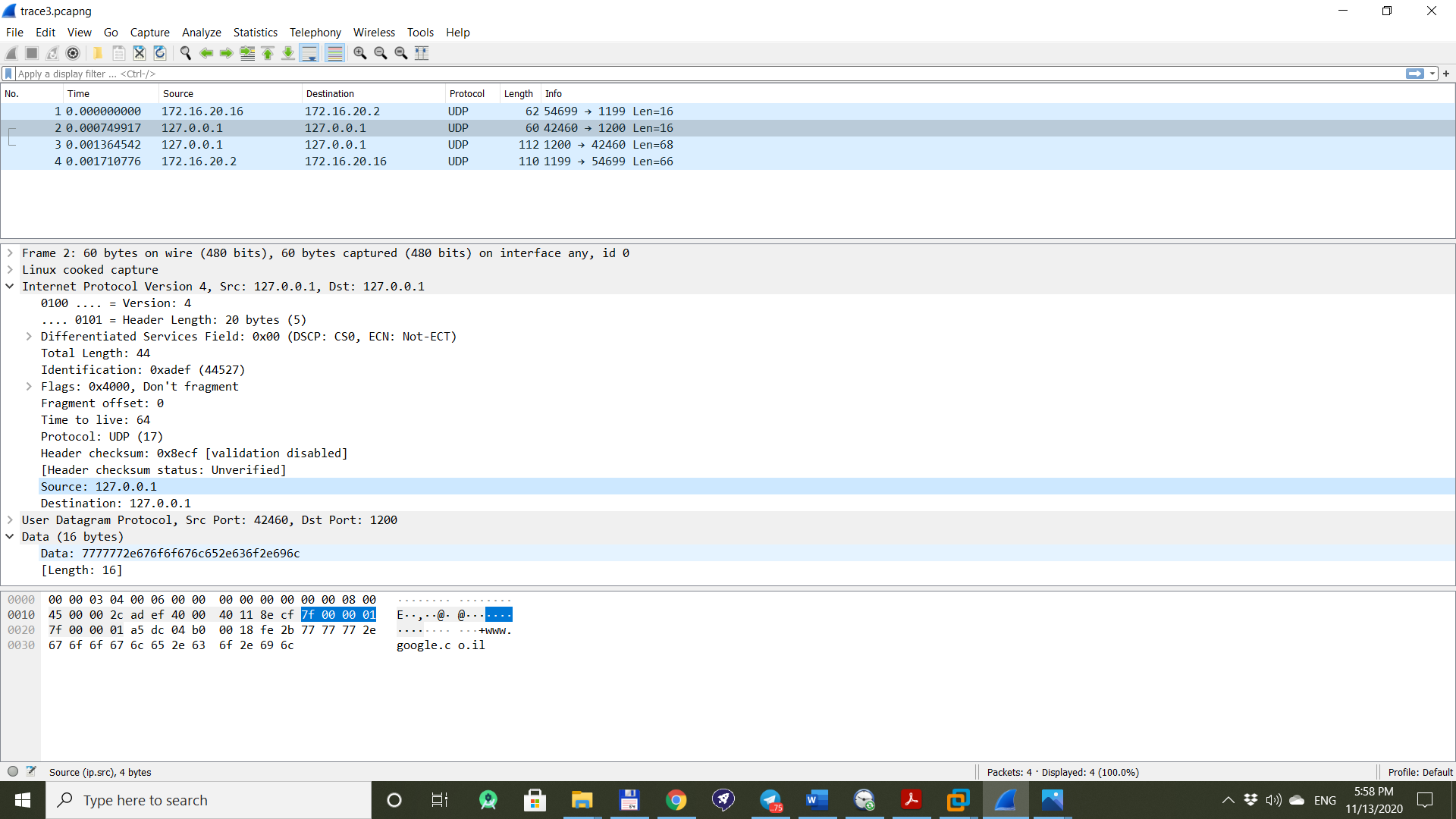
That was how the data was transferred from the client to server's machine top to bottom and vice versa, in the next records in the wireshark sniff we will see the conversation between the main server and the father server and the response sent to the client

Move on to the next line in wireshark sniff – we can see that the original server didn’t know the ip address of the given query so he goes to his father in order to get more info from it so in the Datagram tab we can see that the dest port is the port of the father server:



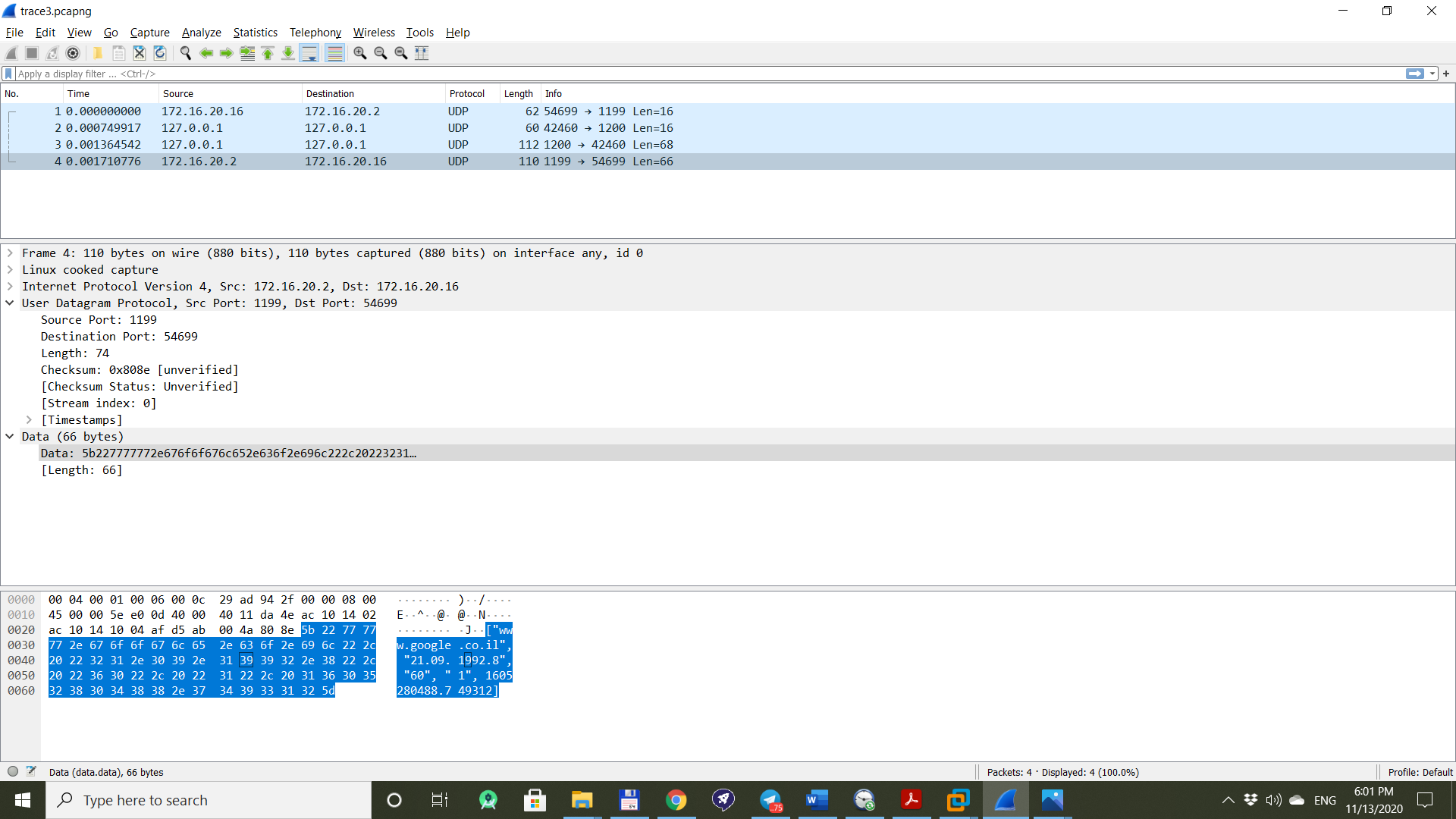
\*the source port is some random that the OS on the Server VM gave the original server program after it asked to open new socket to the father server

In the Internet tab we can see that the src ip and des tip is the same: 127.0.0.1 – meaning that we work on the local machine :



Finally, lets take a look at the last line which is the data sent from the server to the client:

Screenshot from the last line in the Data tab:



Above we can see that the data sent back to the client was the full details about the address of [www.google.co.il](http://www.google.co.il) which is its web address,ip address and TTL.

We can conclude that the ip address of [www.google.co.il](http://www.google.co.il) is "21.09.1992.8" , and TTL is 60s.