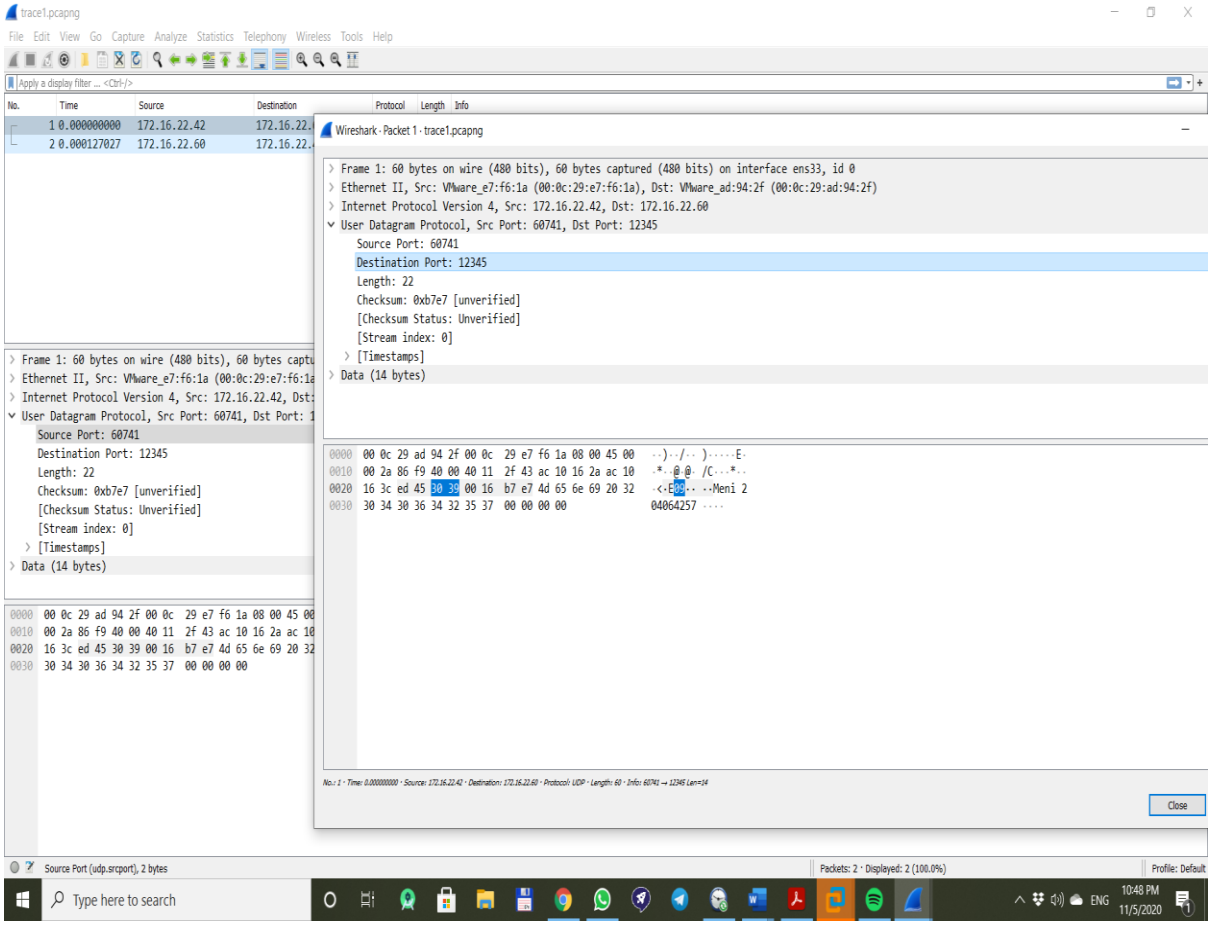
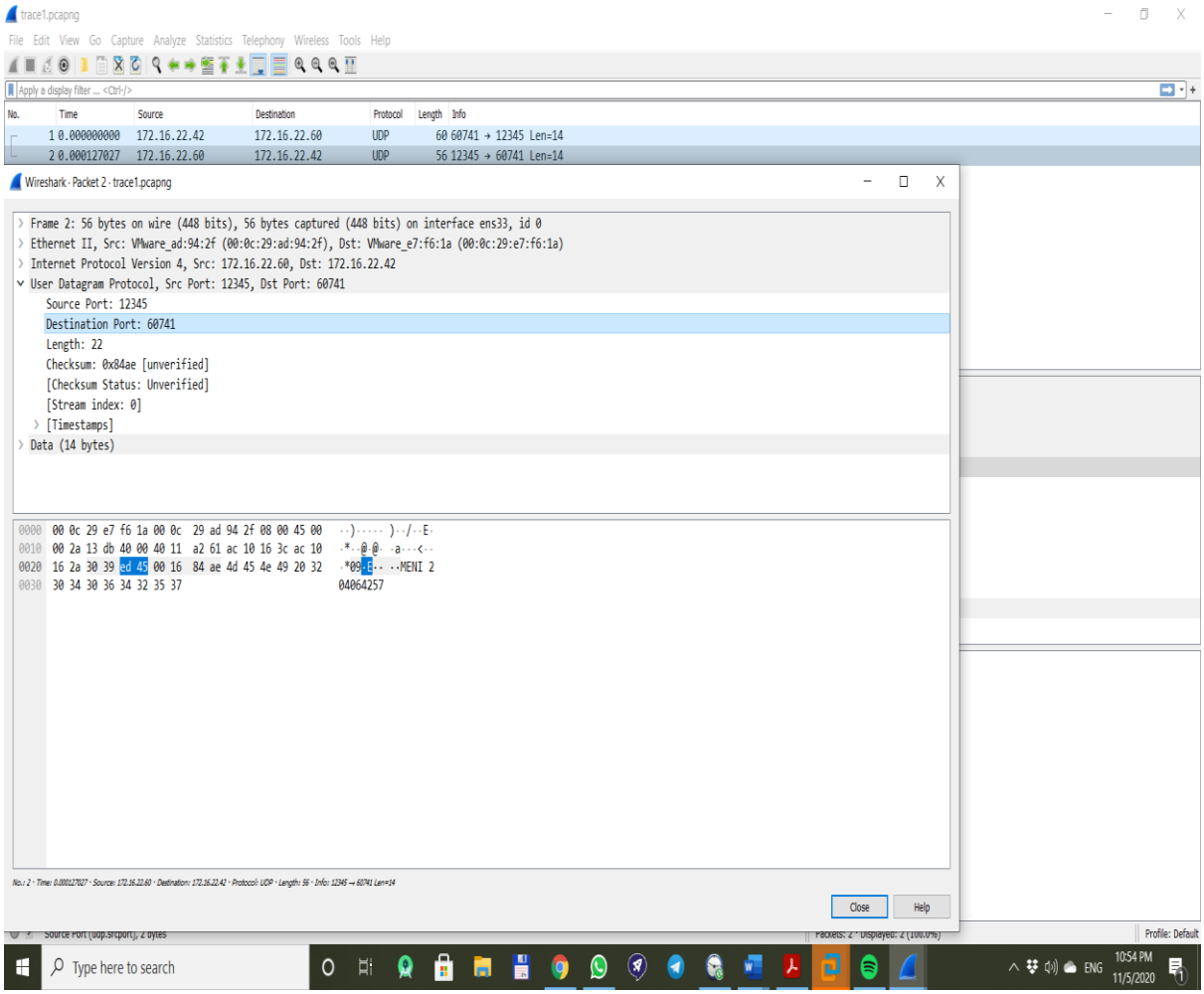
Into. To Networking – Ex. 1
Branch A:
Prerequisites : Two Virtual Machines connected to same NAT network just like Hemi showed us at the recitation – first virtual machine is with ip : 172.16.22.42 will serve as the "Client" and the second virtual machine is with ip : 172.16.22.60 will serve as the "Server"
I ran attached "Client.py" script on the "Client" machine and "Server.py" script on the "Server" machine and the results are as follows:
2. I've captured the packets via WireShark, which I ran on the "Server" machine, and filtered them with:
"(udp.port==12345 && ip.src==172.16.22.42) || ip.dst ==172.16.22.42"
(See Attached **trace1.pcapng**)
3. The Ports are specified in the following:
client.py , Line 4
the client file specifies the destination port (the port to which the server listens), which is bound to *12345* In wireshark, we can notice that the message packet (sent from client) holds a destination field which holds port 12345, as well as the destination ip which is : 172.16.22.60
Screenshot from wireshark pcap:



In the screenshot you can see that the port specification is mentioned in the "Datagram" message which is part of the "Transport" responsibility.
the dst port is : "123456" just like we configured in the "Client.py" file and the source port is some random port that the OS chose for the client machine – like expected and just like what Hemi said in the recitation

Server.py, Line 4
Same as client.py, but the server listens to the port 12345 (source instead of destination).

Screenshot from wireshark pcap(now I want to show details about the response message sent back from server to client"

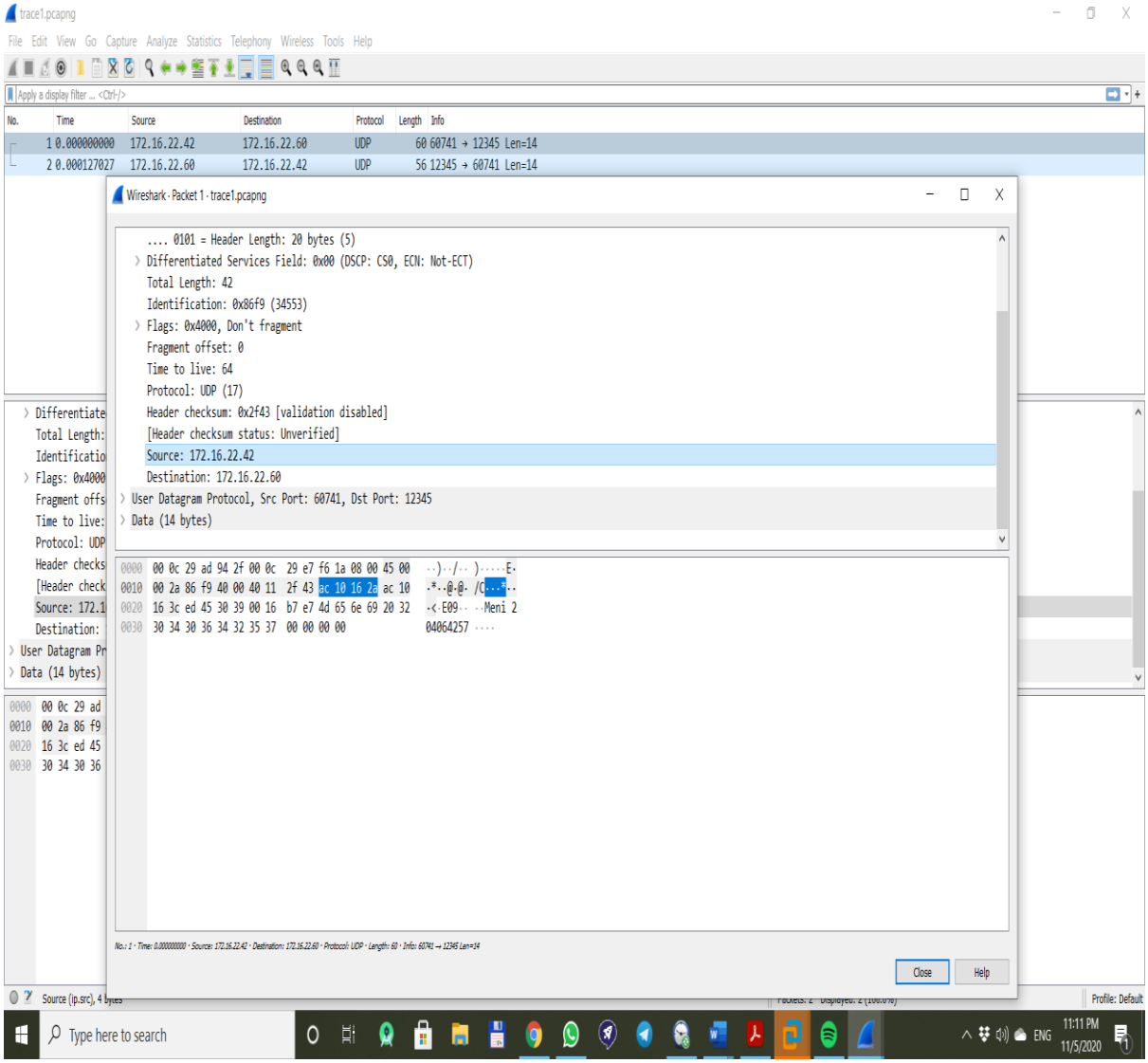


In the screenshot you can see that the port specification is mentioned in the "Datagram" message which is part of the "Transport" responsibility.
the dst port is : "60741" which is the port that the Client used during the conversation with the server and sent the original message and the source port now is the port which the server is using to listen to intercept incoming clients sockets - just like expected and just like what Hemi said in the recitation

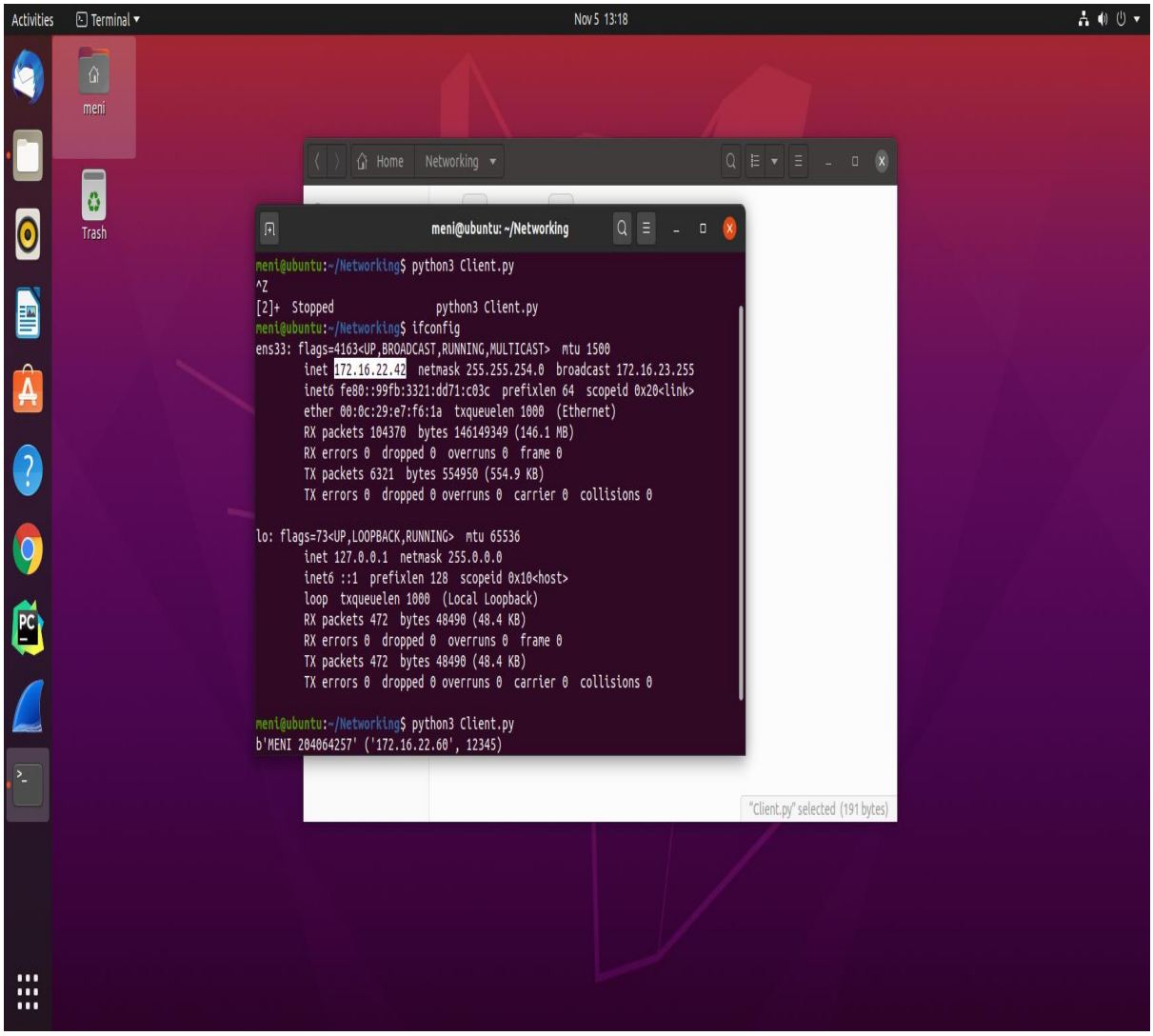
The Port is part of UDP in the Trasport (4th) layer of the OSI model.

4. In this part I need to demonstrate how the ip address is used

o.k, lets see the relevant packet from the sniff of the conversation between the server and the client:



We can see that the information about the source and dst ip addresses are shown at the packet tab from the sniff : the ip address is used in the "Network" layer in order to guide the router to the recipient of the message which, in our case is the server. So we can see that the source ip addr is the ip addr of the client. Lets run "ifconfig" command in terminal of the "Client" machine and prove you that:



So we see that the NAT network name is "ens33" and the server machine also connected to that network.

Here you have the proof the client's ip addr is "172.16.22.42" which is shown in the wireshark sniff