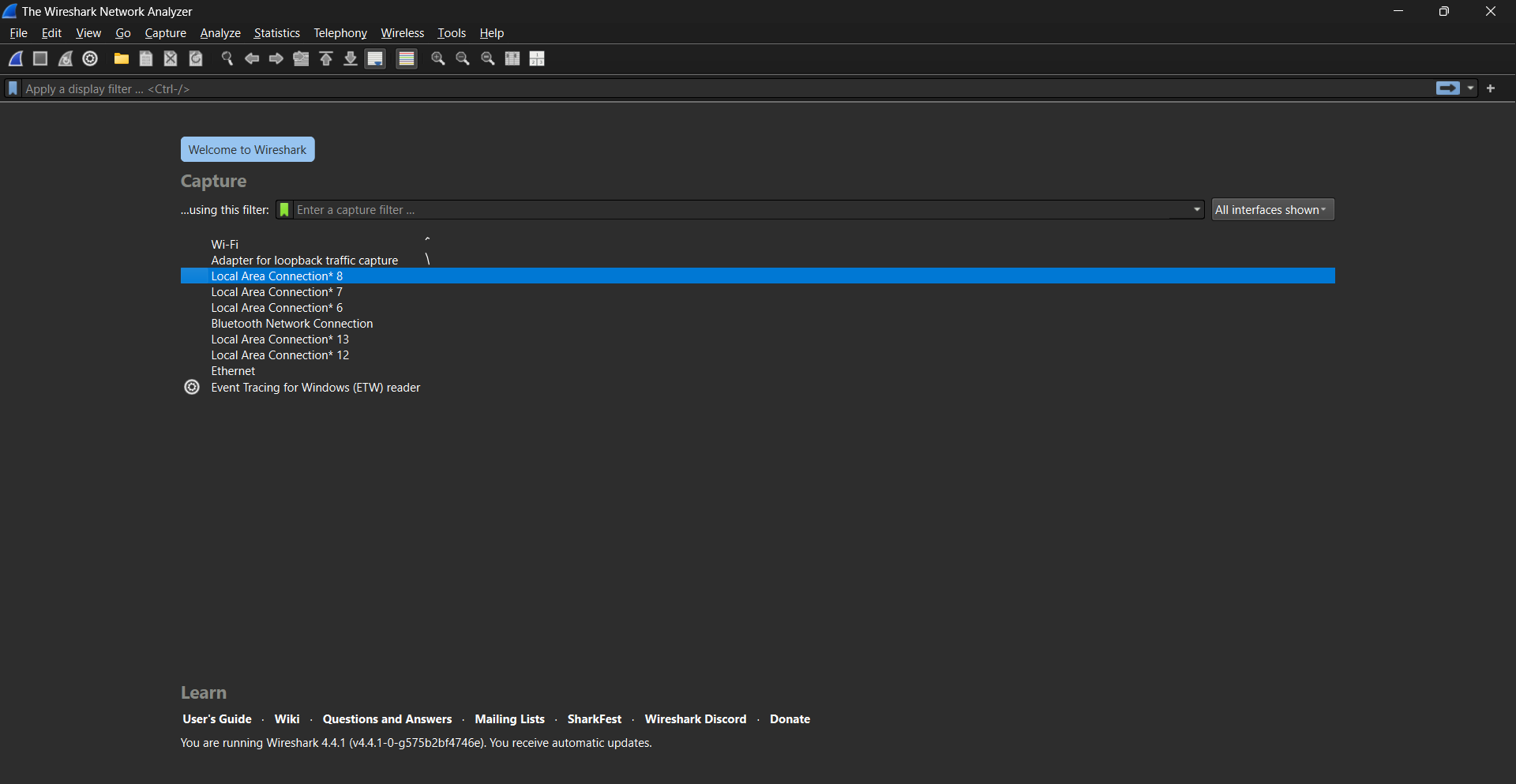
# Introduction to Computer Network – Fall24, CRN 10102

## Homework 3

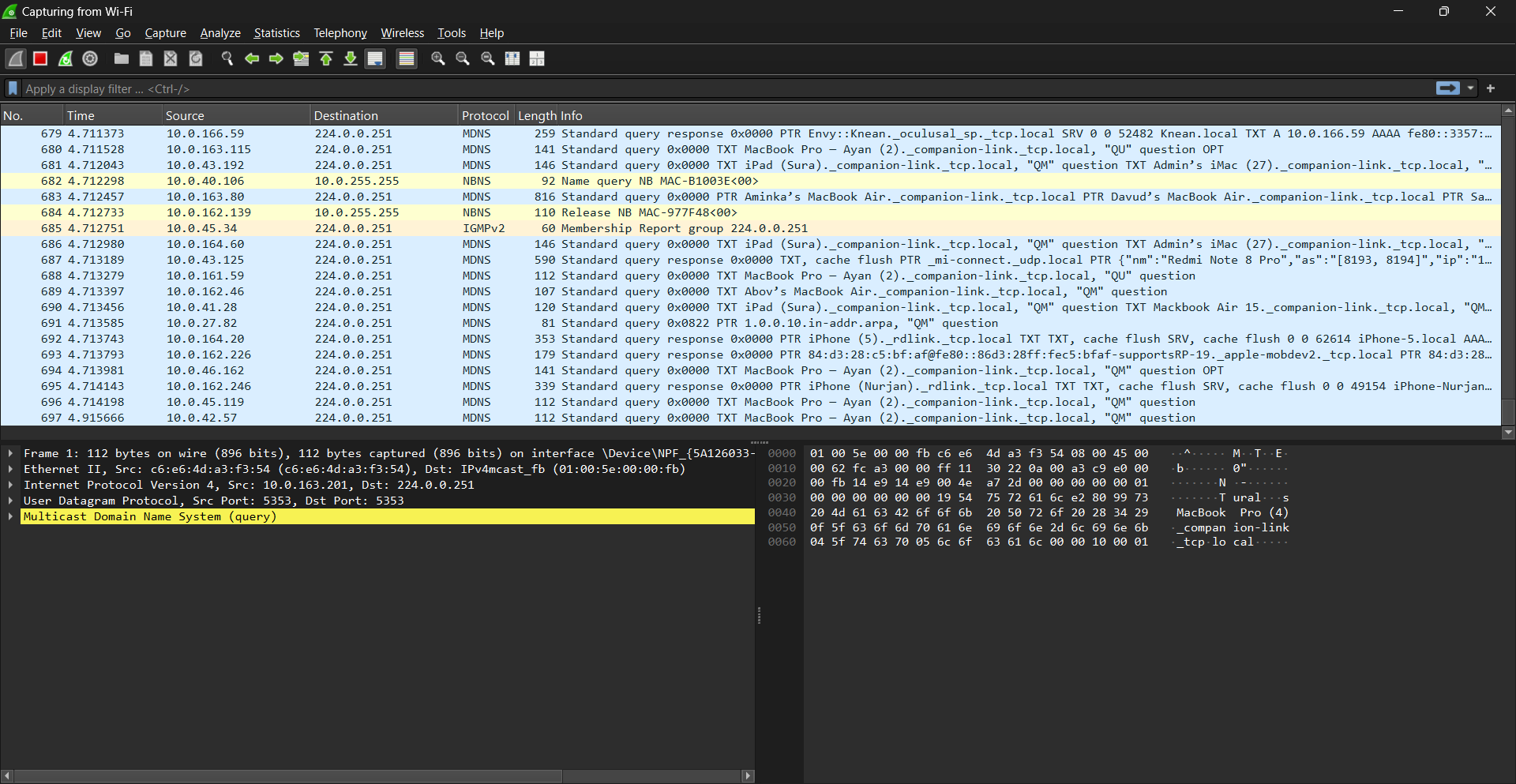
### Nilufar Babayeva

1. **Capture and Analyze Local ICMP Data in Wireshark.**

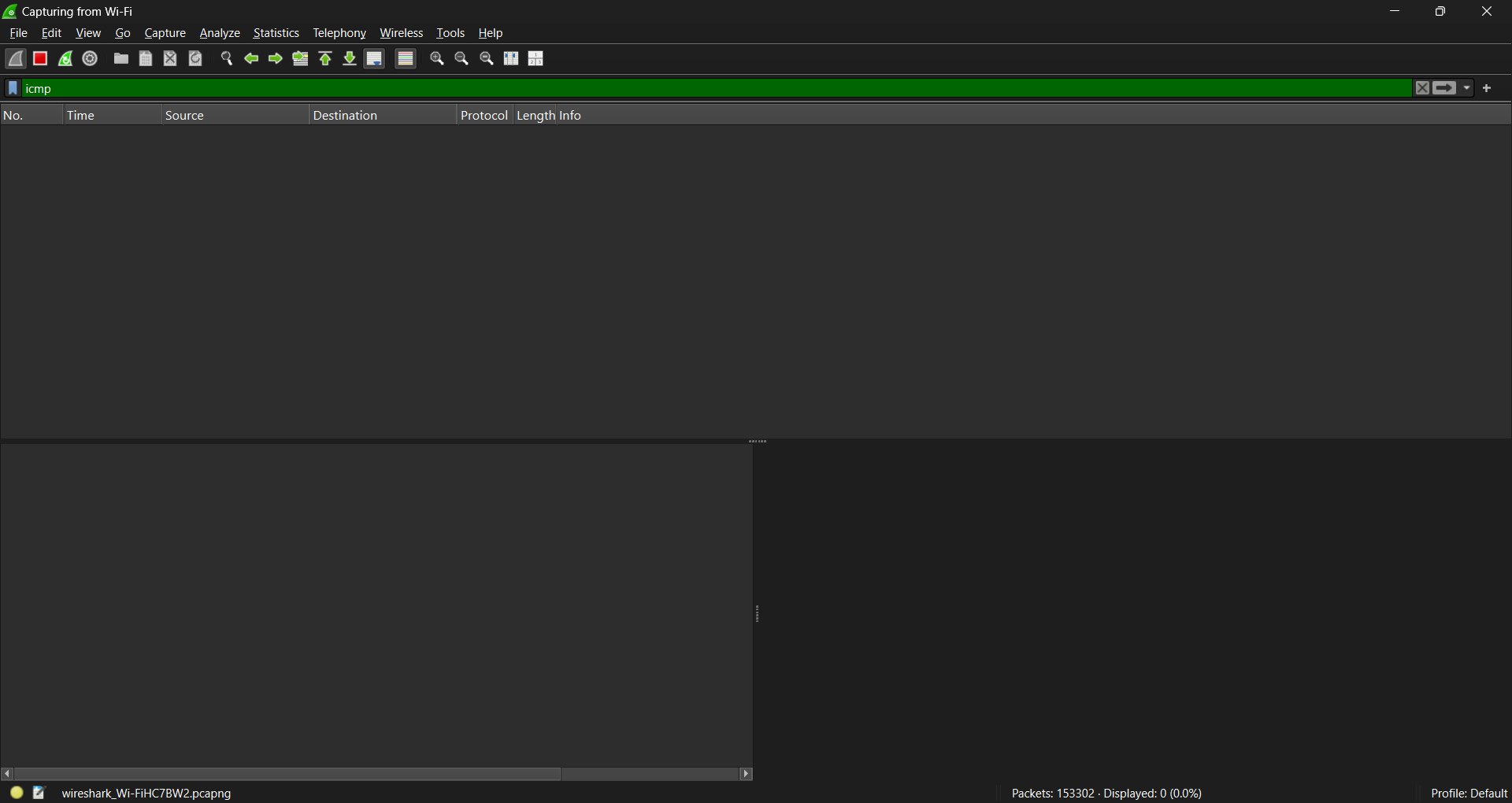
1.1 Open Wireshark app and choose the interface to work with ICMP. I selected **Wi-Fi** in the picture. Then double click the Wi-Fi to start capturing packets.



1.2 You will see a view like below:



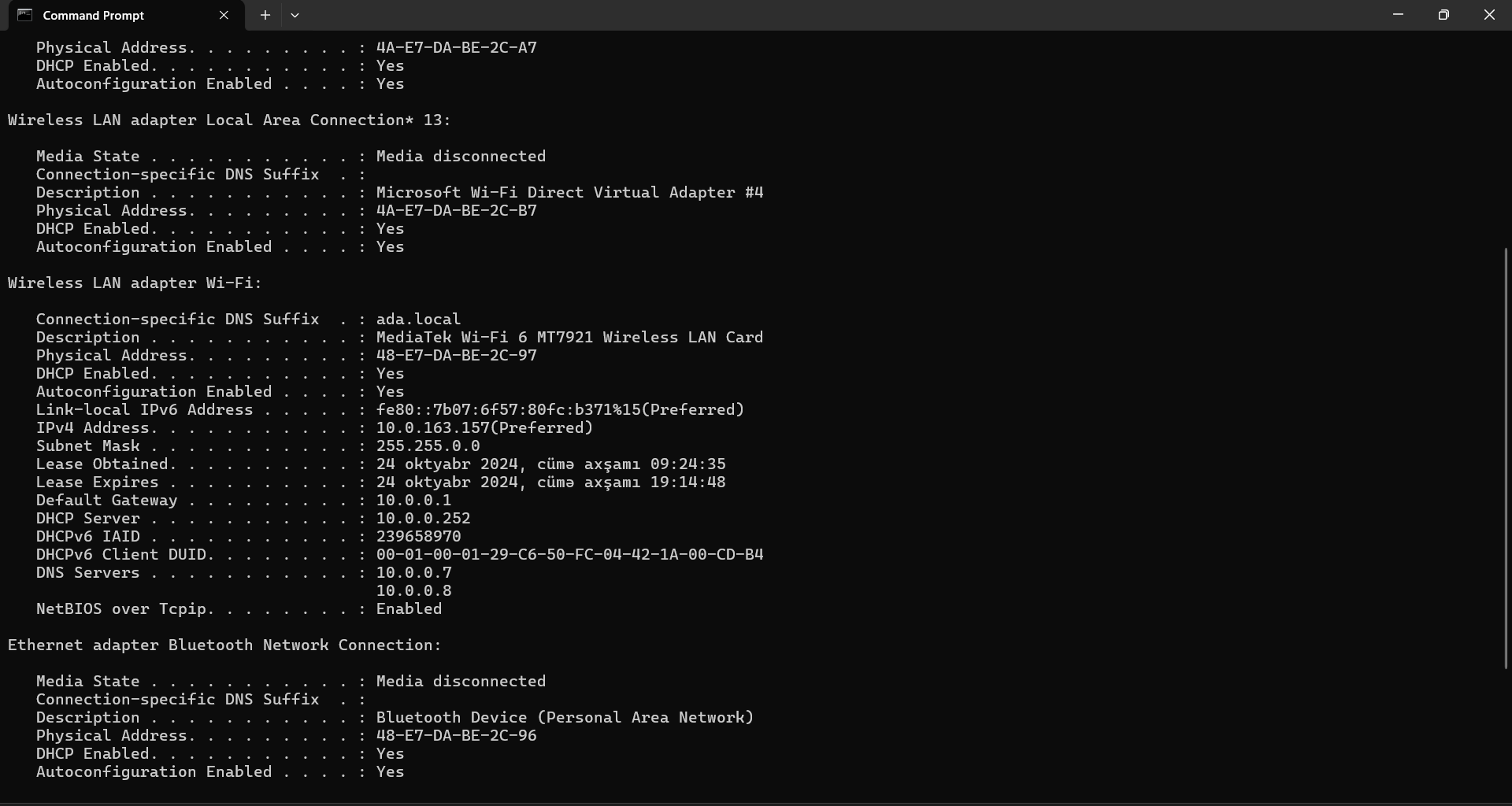
1.3 In order to capture ICMP packets, write **“icmp”** in the search bar and click arrow in the right:



1.4 Now you need to open “Command Prompt” by typing “cmd” in the Windows search bar. In order to get your IP/ MAC address type “ipconfig /all”.



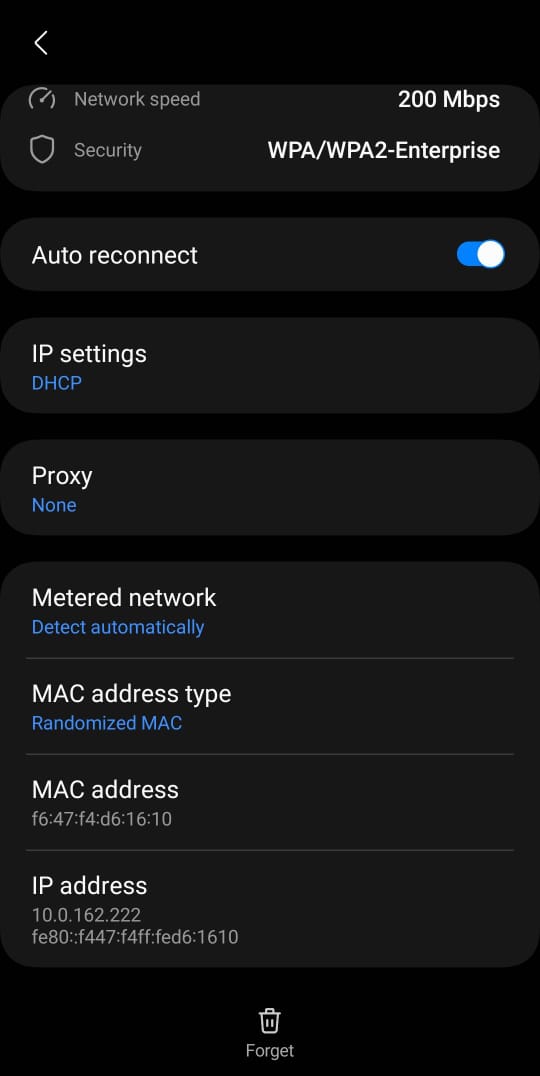
1.5 In the **“Wireless LAN adapter Wi-Fi”** bar, you will see **“Physical address”** which is MAC address and **“IPv4 Address”** which is IP address of your PC.



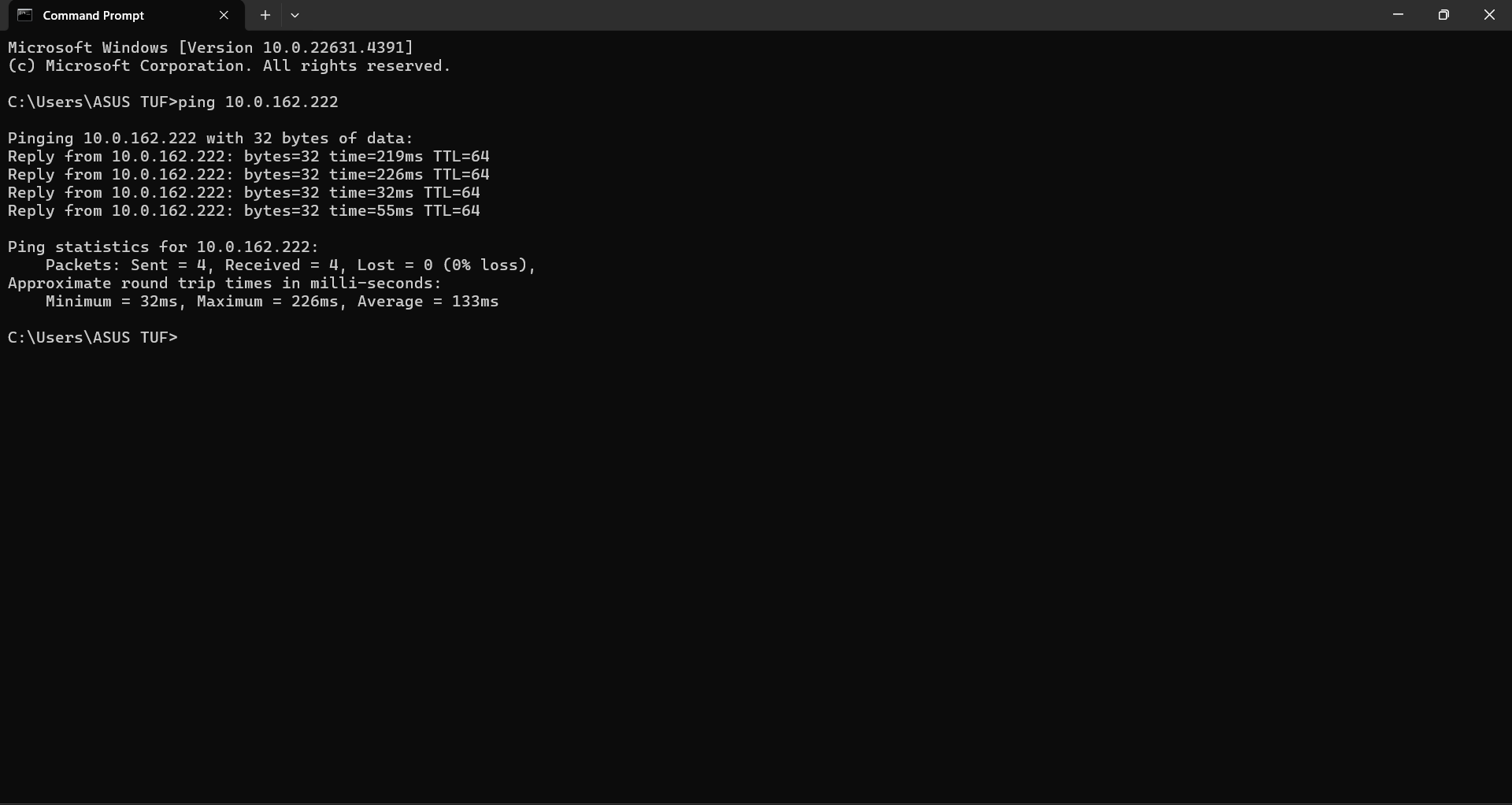
1.6 Then to be able to capture ICMP packets, we have to ping the IP address of a device. I used my phone’s IP address, since it is using the same Wi-Fi network as my PC.

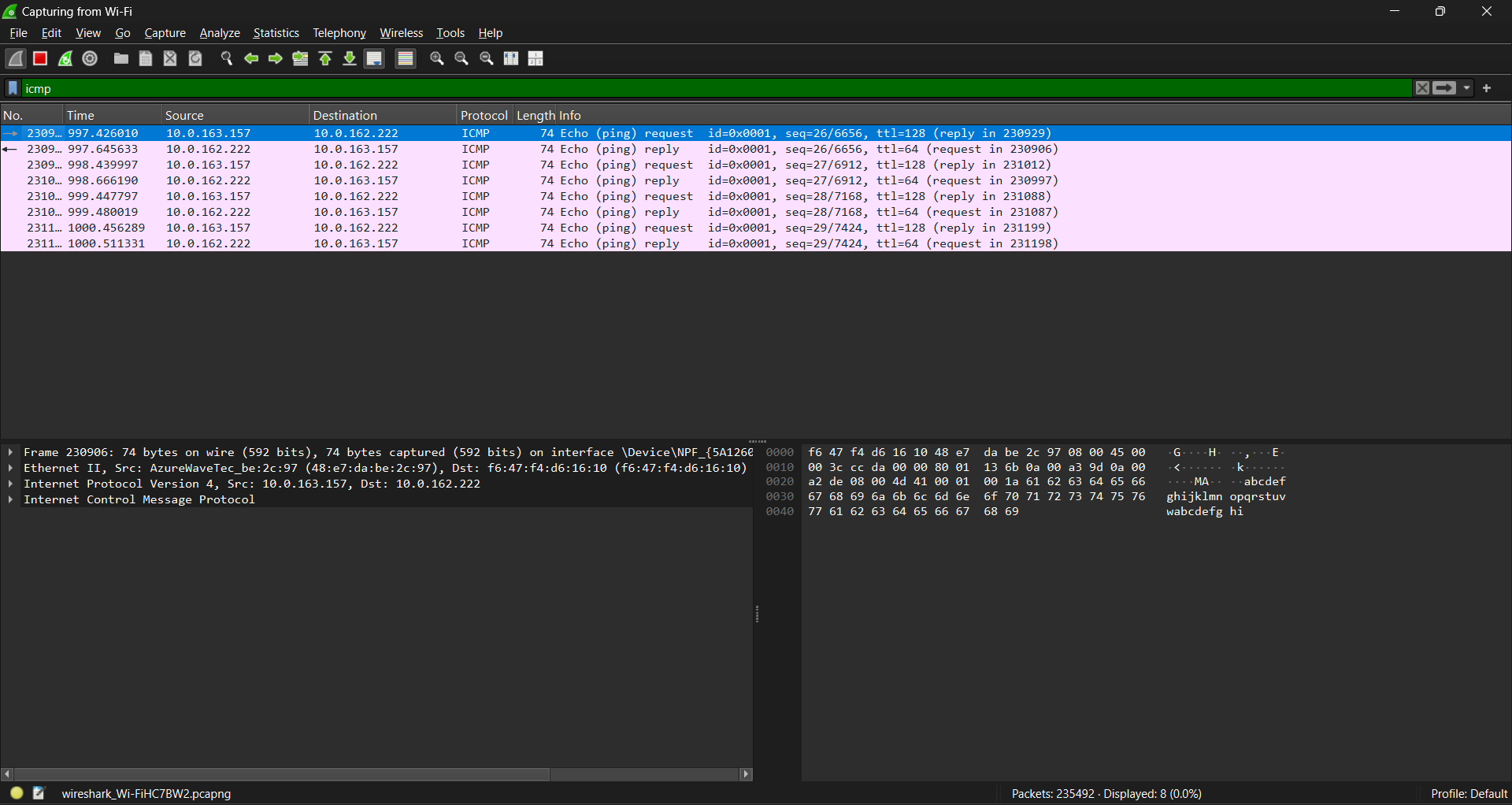
You will see “MAC address” and “IP address” below the page.

A screenshot of a phone

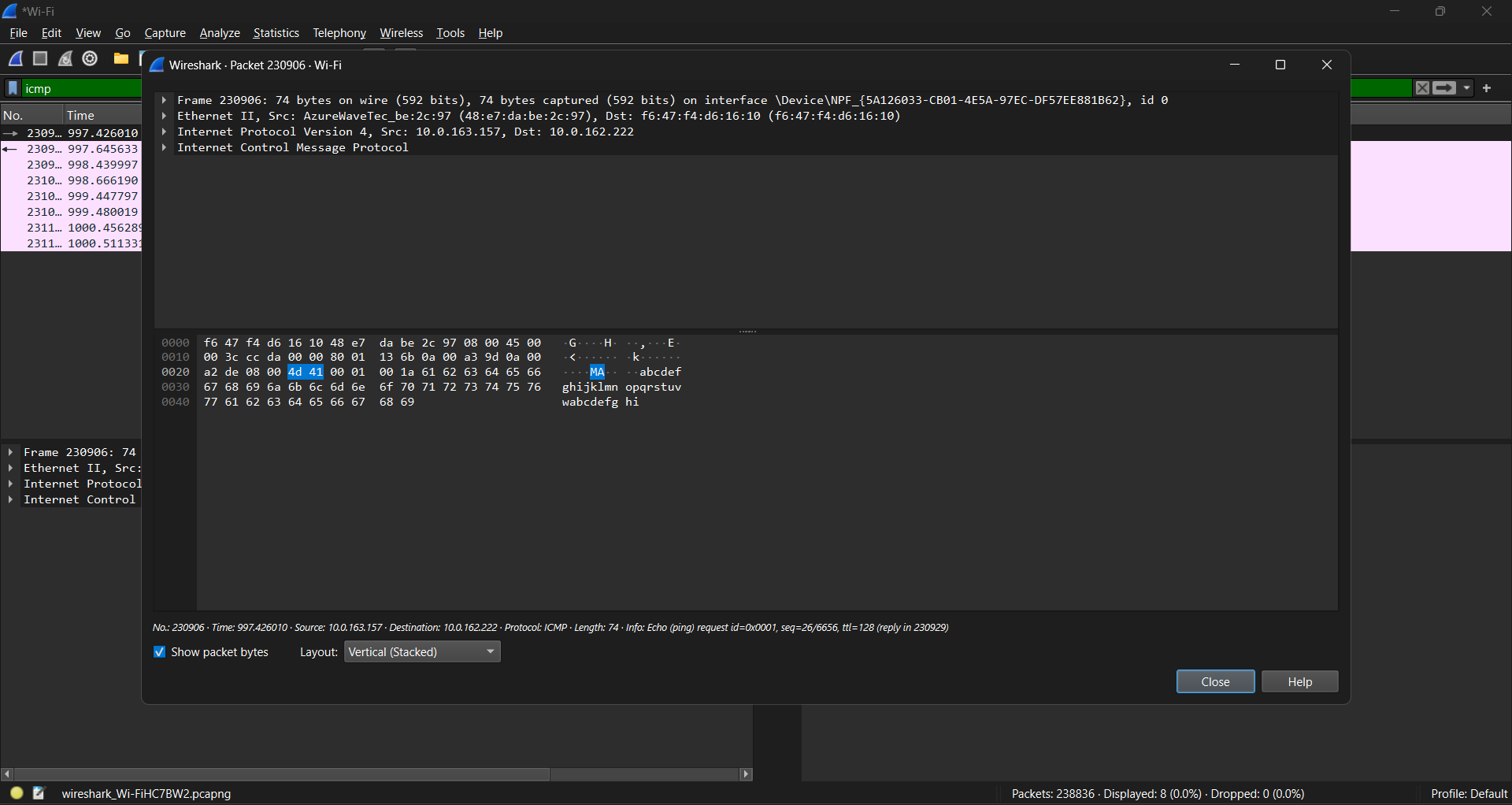
Description automatically generated

1.7. Then open CMD again and ping IP of your Wi-Fi. In my case it is ADA\_Campus.



* 1. Now we can see ICMP packets in the board. We can see that the source is my PC’s IP, and destination is the IP address that I have pinged already.

1.9.When you click on the first row, you can see that the IPs and MACs are matched.

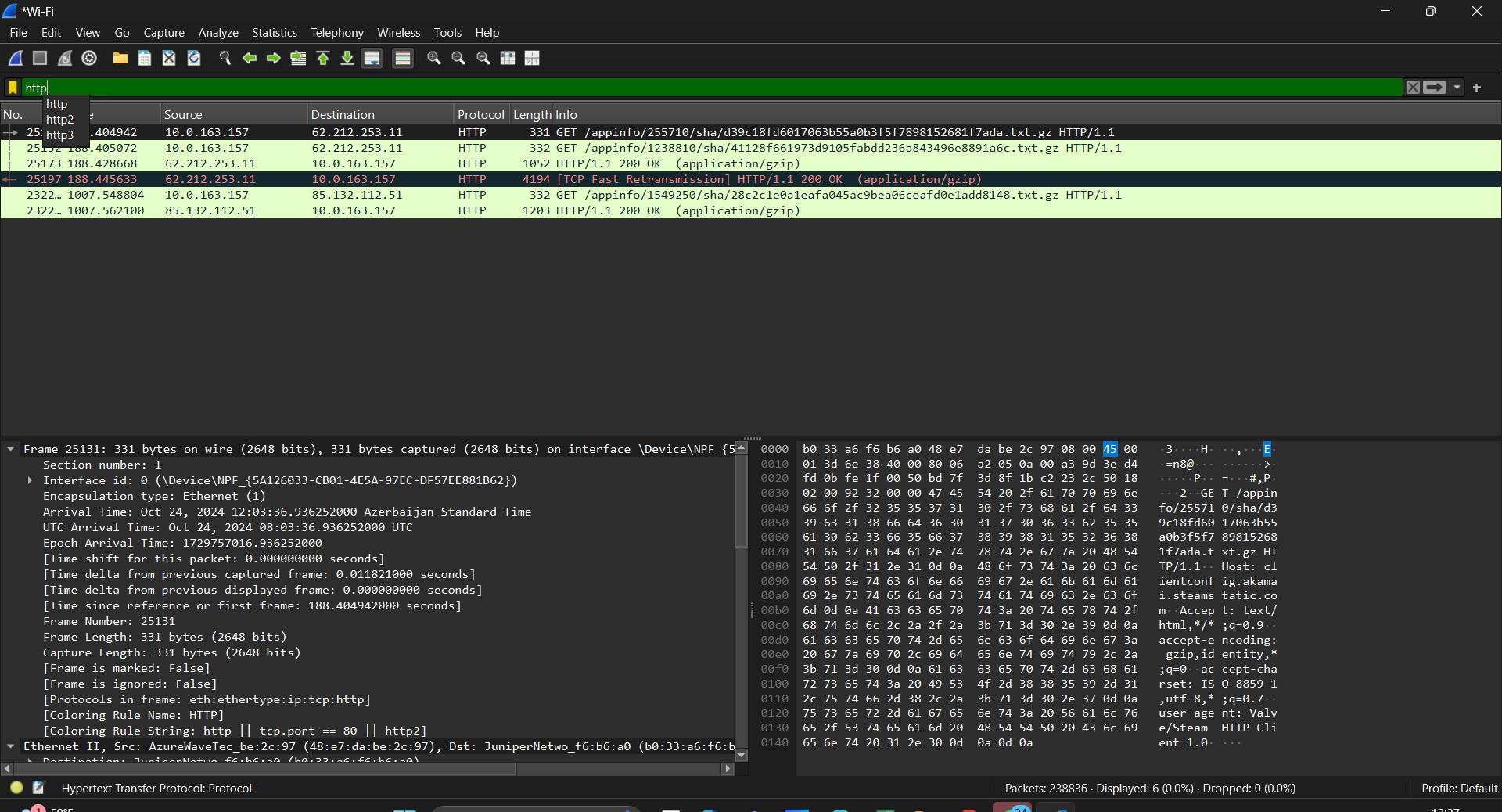


**2.0 Use WireShark to analyze the packet in http request.Highlight the SRC and DST ports and Mac Addresses.What is the source and destination ip addresses on network layer?**

2.1 Firstly, let’s find a http website. I found httparchive.org.



2.2 Now we again open Wireshark and choose the appropriate interface (my case was Wi-Fi). Instead of typing **“icmp”** write **“http”** and apply the filter.

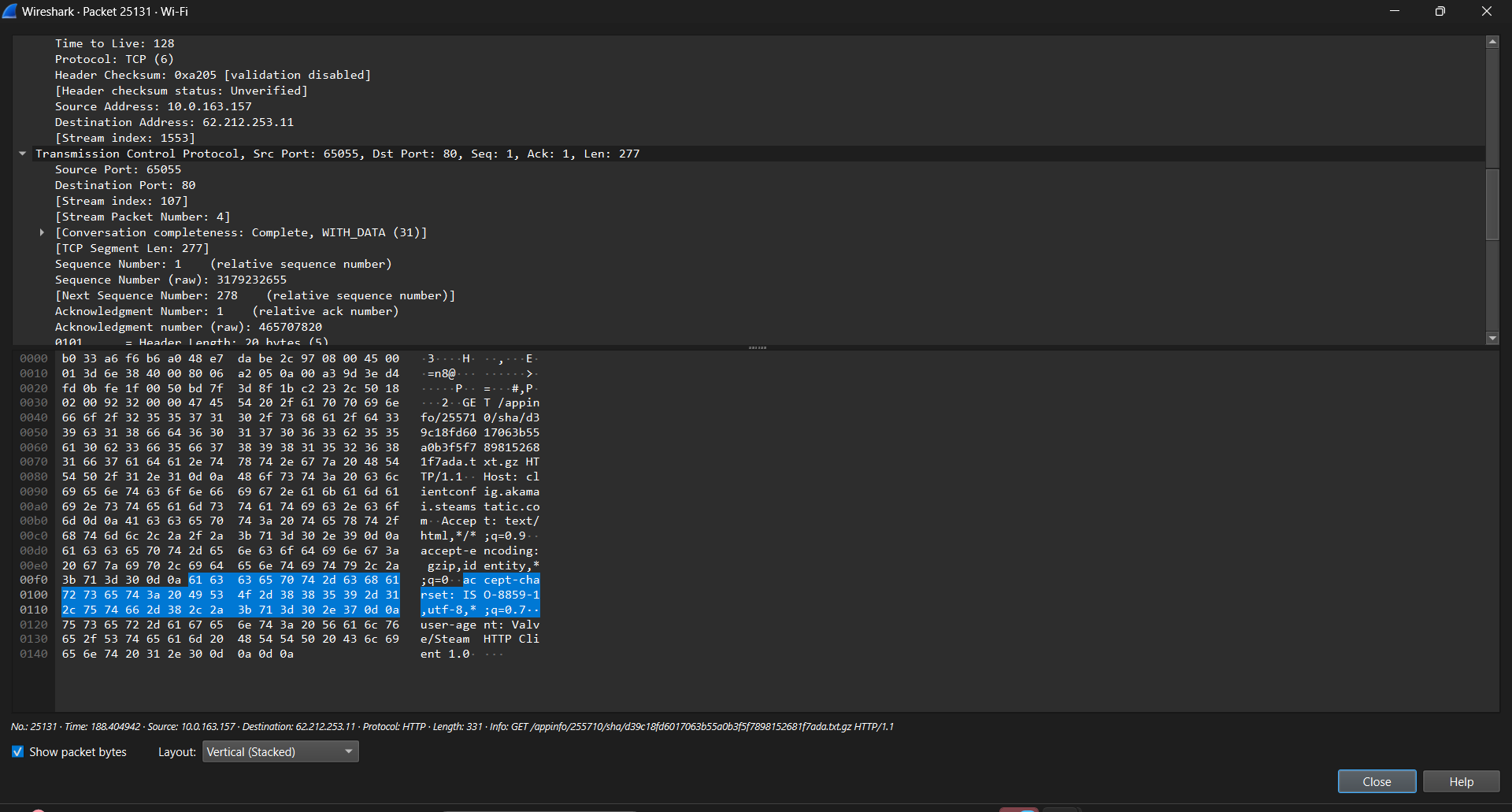


2.3 To observe the **http** traffic we have to choose a packet that contains **GET**.

A screenshot of a computer

Description automatically generated

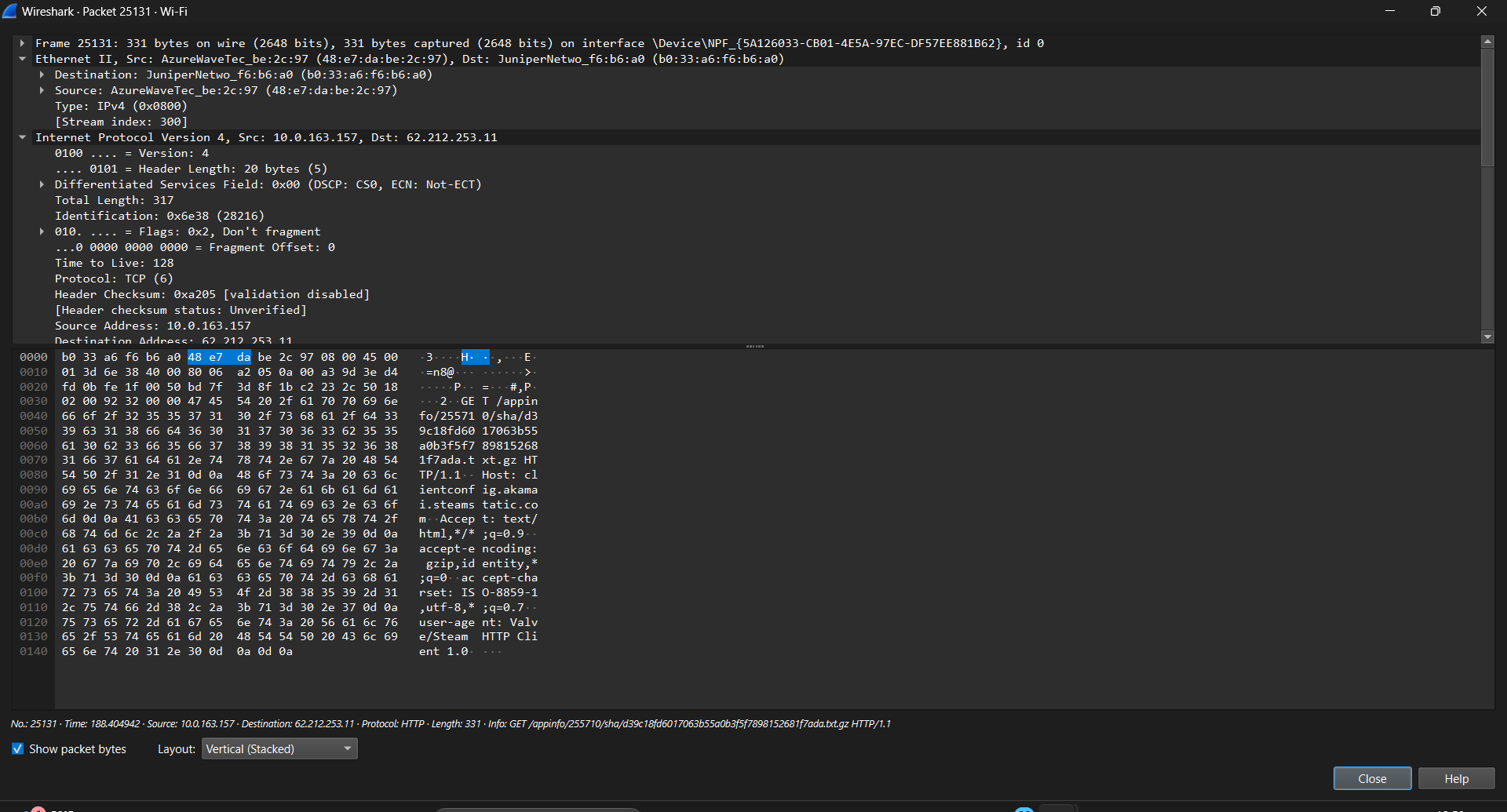
2.4 These are source and destination ports.



2.5 And let’s look at MAC addresses

A screenshot of a computer

Description automatically generated

2.6 And let’s look at IP addresses

2.7 Lastly, it is crucial to ensure that the IP address found in the captured packets matches the IP address of the target website (10.0.162.222). You can verify the website's IP address by using the `ping` command in the command prompt, which will query the domain name and return the associated IP address for confirmation.



**3.Analyze DNS packages using WireShark and nslookup tool.**

3.1. First, in order to observe DNS packets, I texted DNS and applied the filter.

A screenshot of a computer

Description automatically generated

3.2 As it is shown I have chosen [www.shazam.com](http://www.shazam.com) and then checked nslookup from <https://www.cloudns.net/nslookup-tool>.

A screenshot of a computer

Description automatically generated

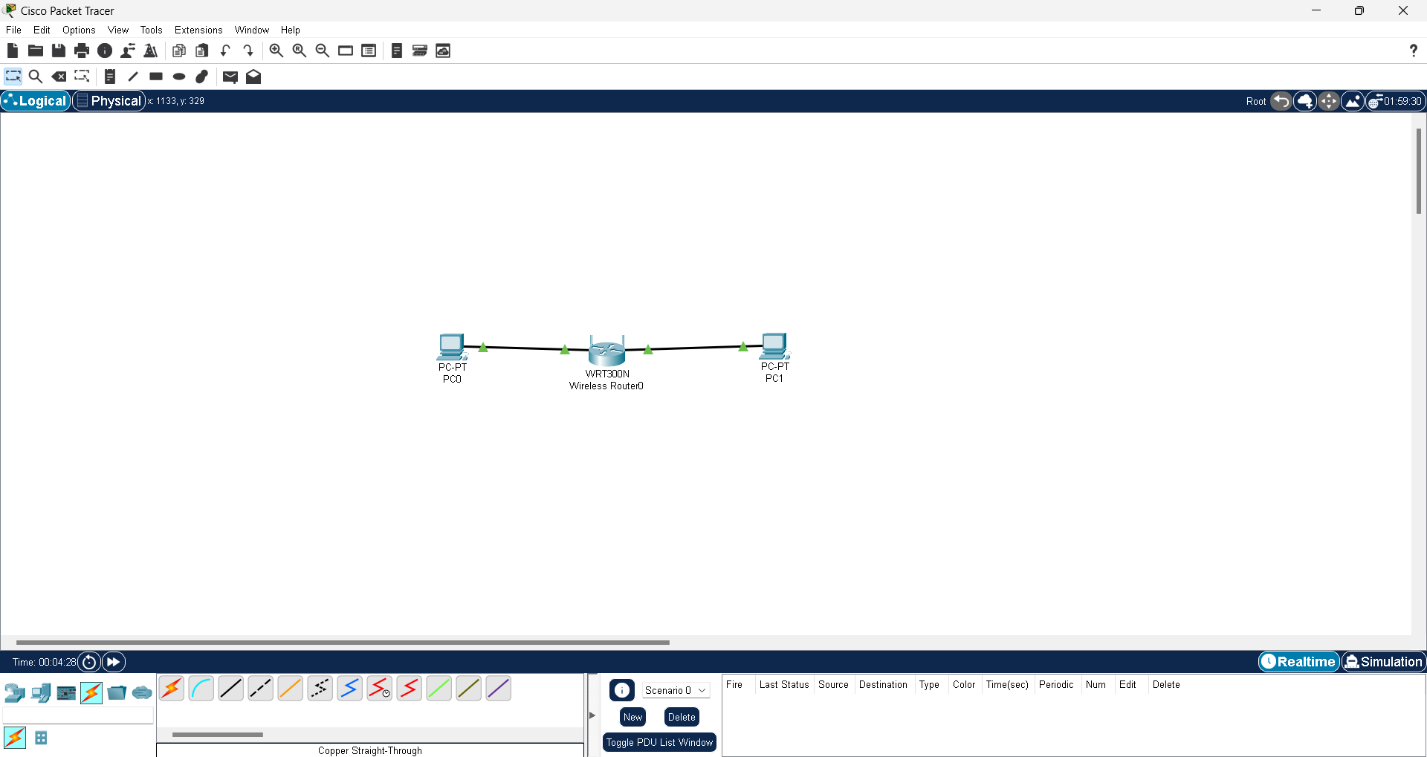
3.3 We get the answer as how it was in Wireshark. We have verified the accuracy of the data related to DNS information.

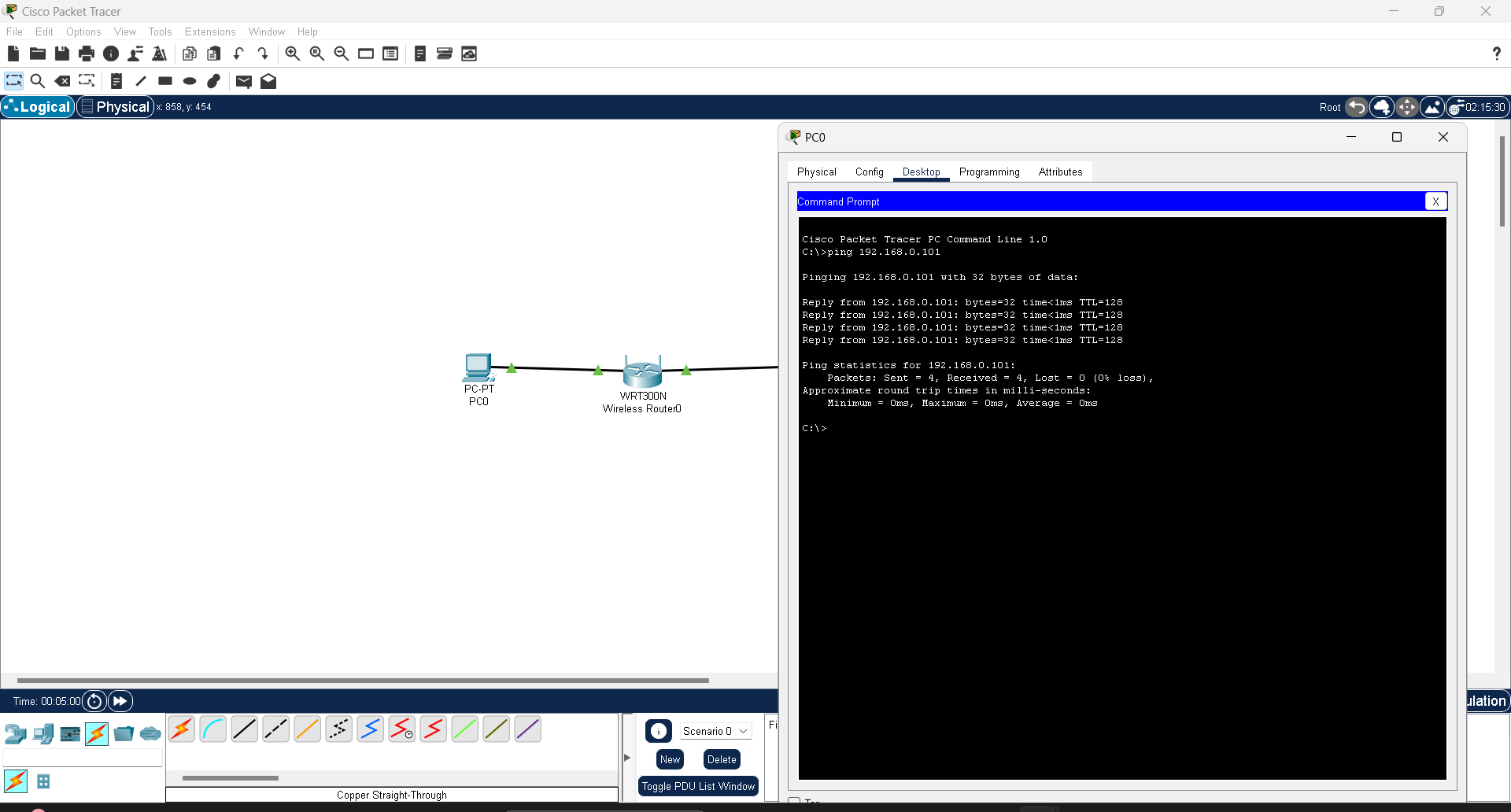
A screenshot of a computer

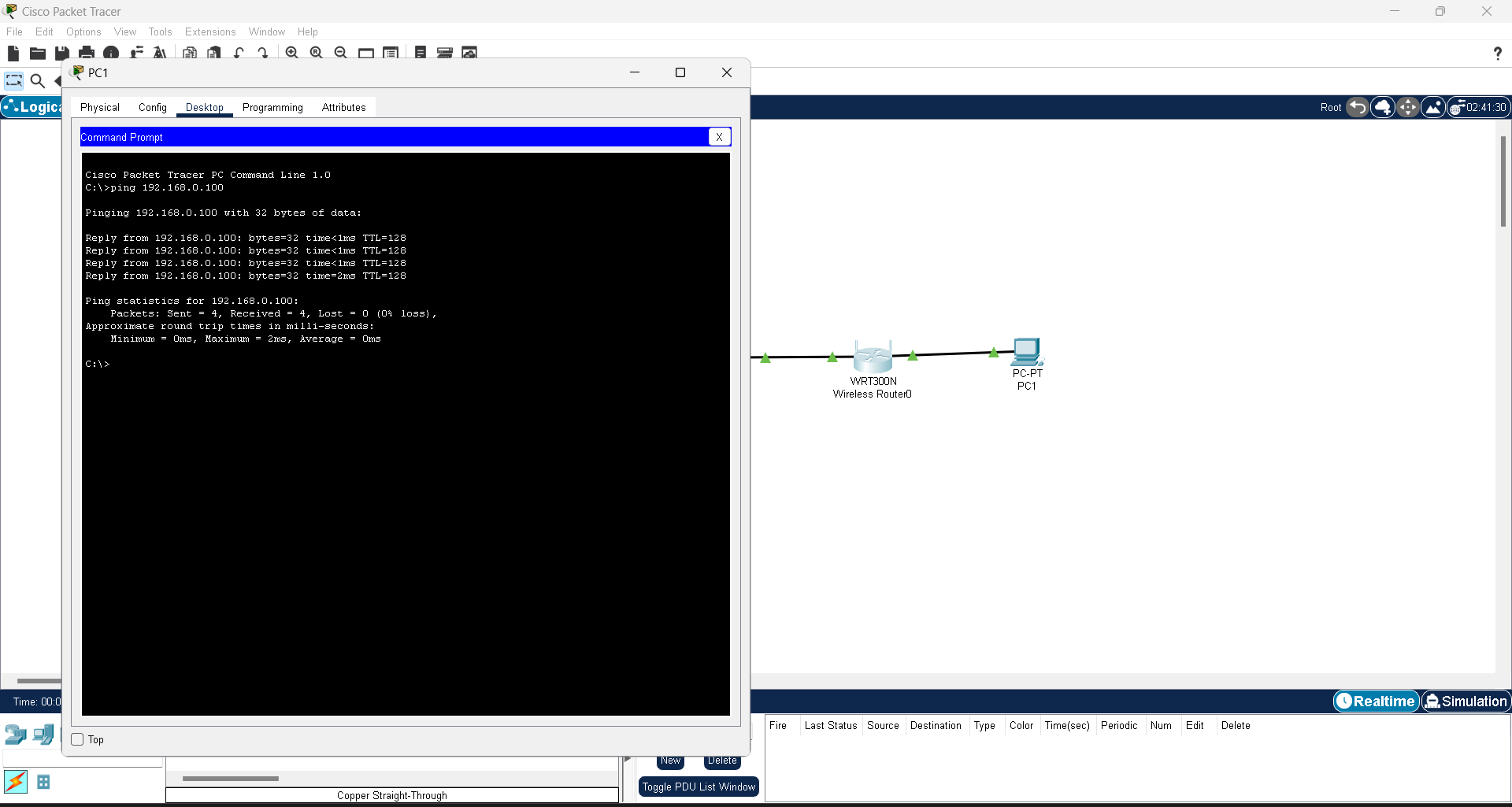
Description automatically generated

**4. Create a small network (use your imagination) and simulate an OSI layer. Screenshot each layer how the request goes through each OSI layers.**

4.1. Small network that I created.



4.2. Then I pinged each end device.



4.3. Lastly, these are the OSI layers of my small network