Name: Md.Abdullah

ID : IT-17015

Lab report no: 2

Name of the lab report: Wireshark display

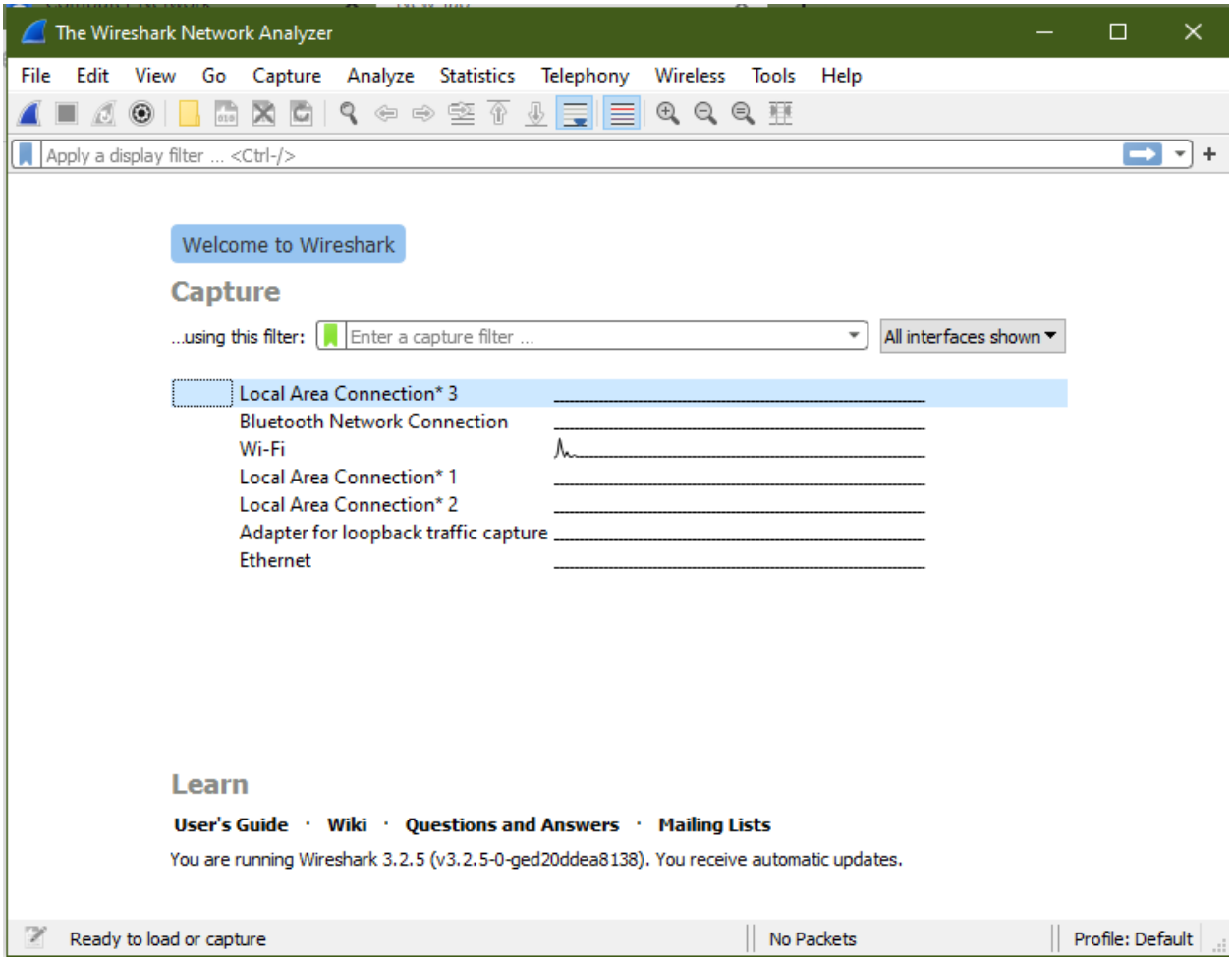
Objectives:

- To learn basic packet analysis using Wireshark

Theory:

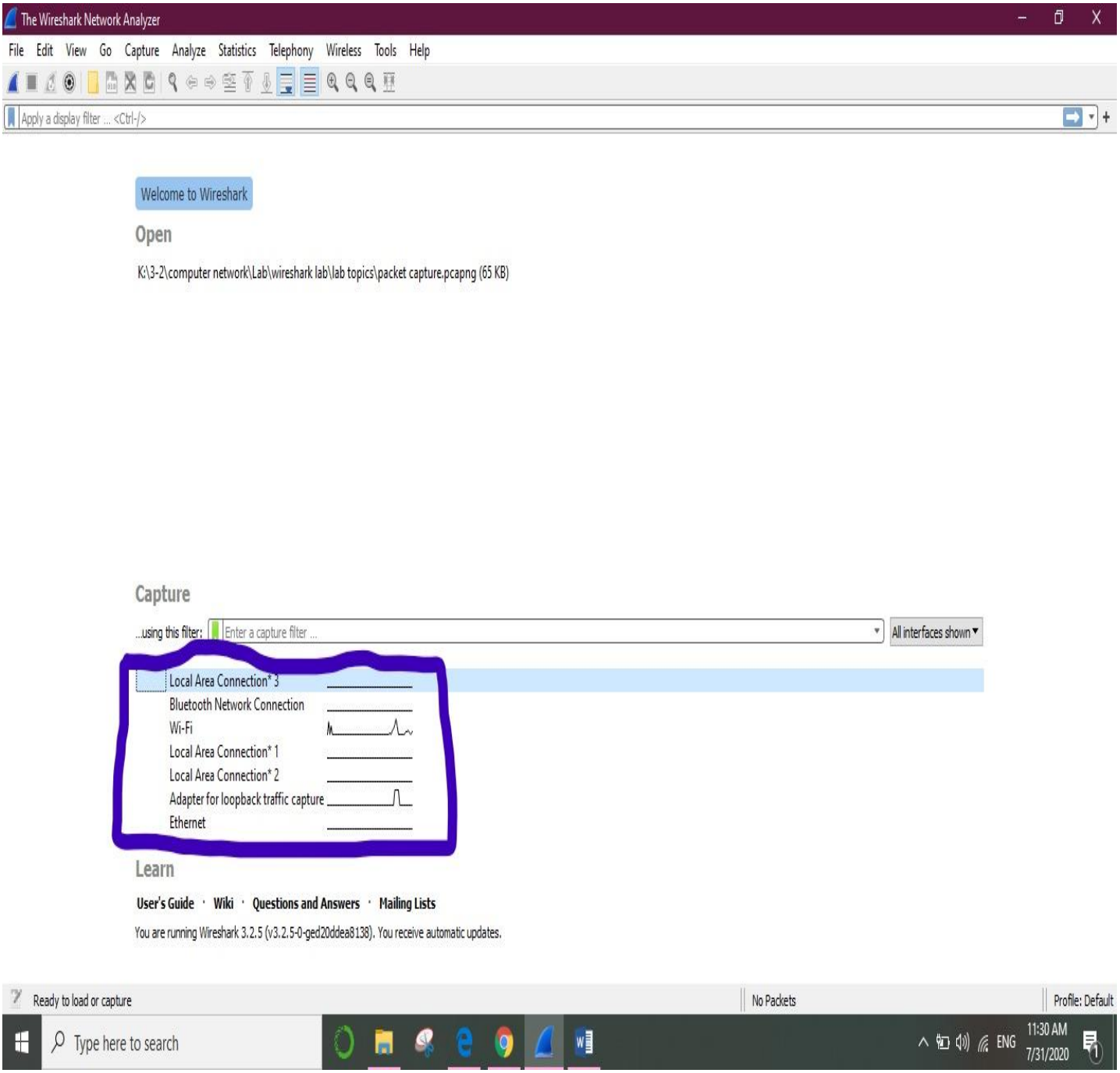
Wireshark is a free and open source network packet analyzer. It is mainly used for network troubleshooting and analysis. In this lab we will learn how to analyze the packets and to find different protocol related information from the captured packets.

<u>Running Wireshark:</u>

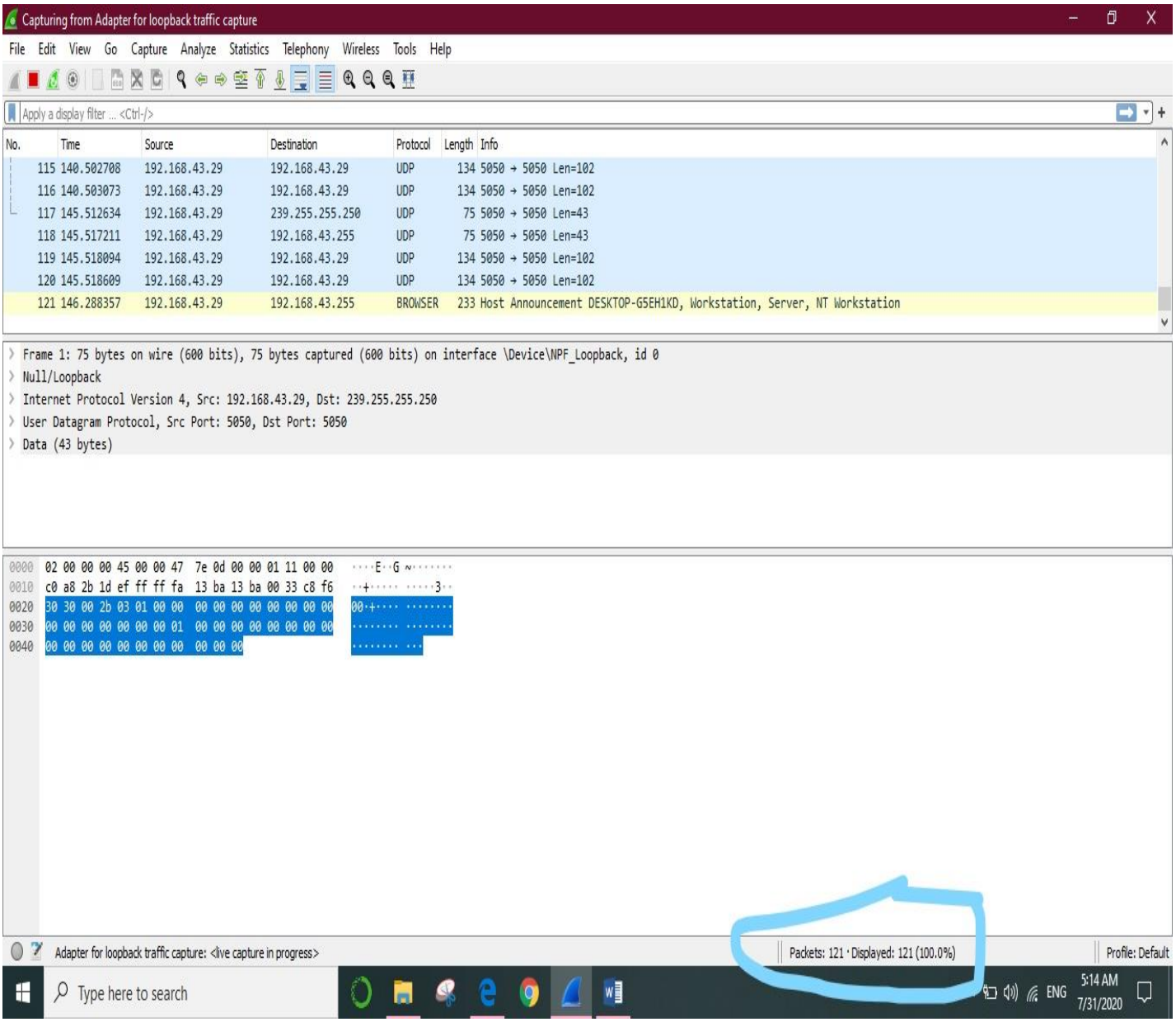


Capturing packet:

First we need to double click on the interfaces shown in below figure marked by blue color.

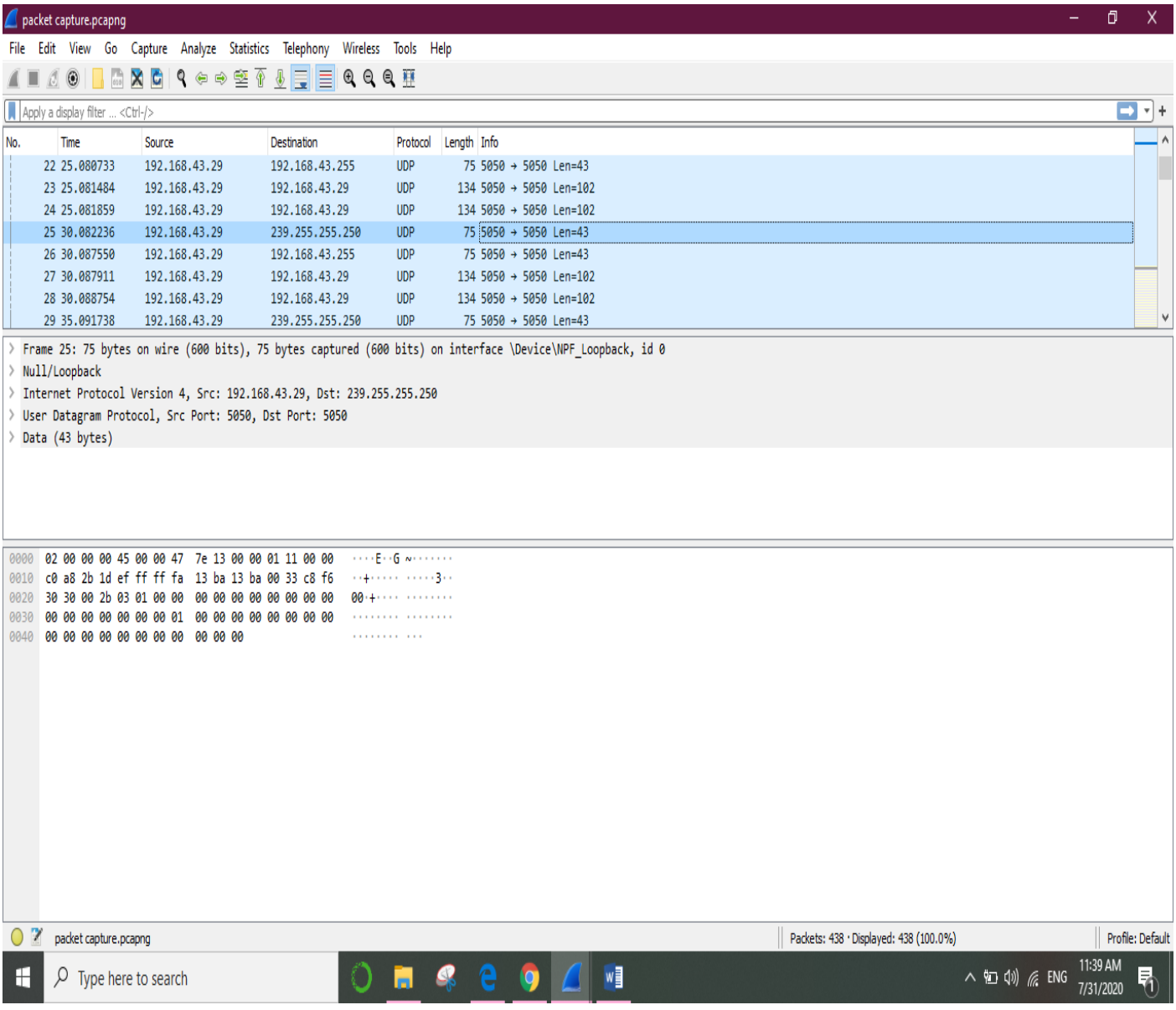


After double click on any of the item Wireshark is now capturing all packets being sent/received from/by your computer. Here total 121 packet are captured and it will continued.

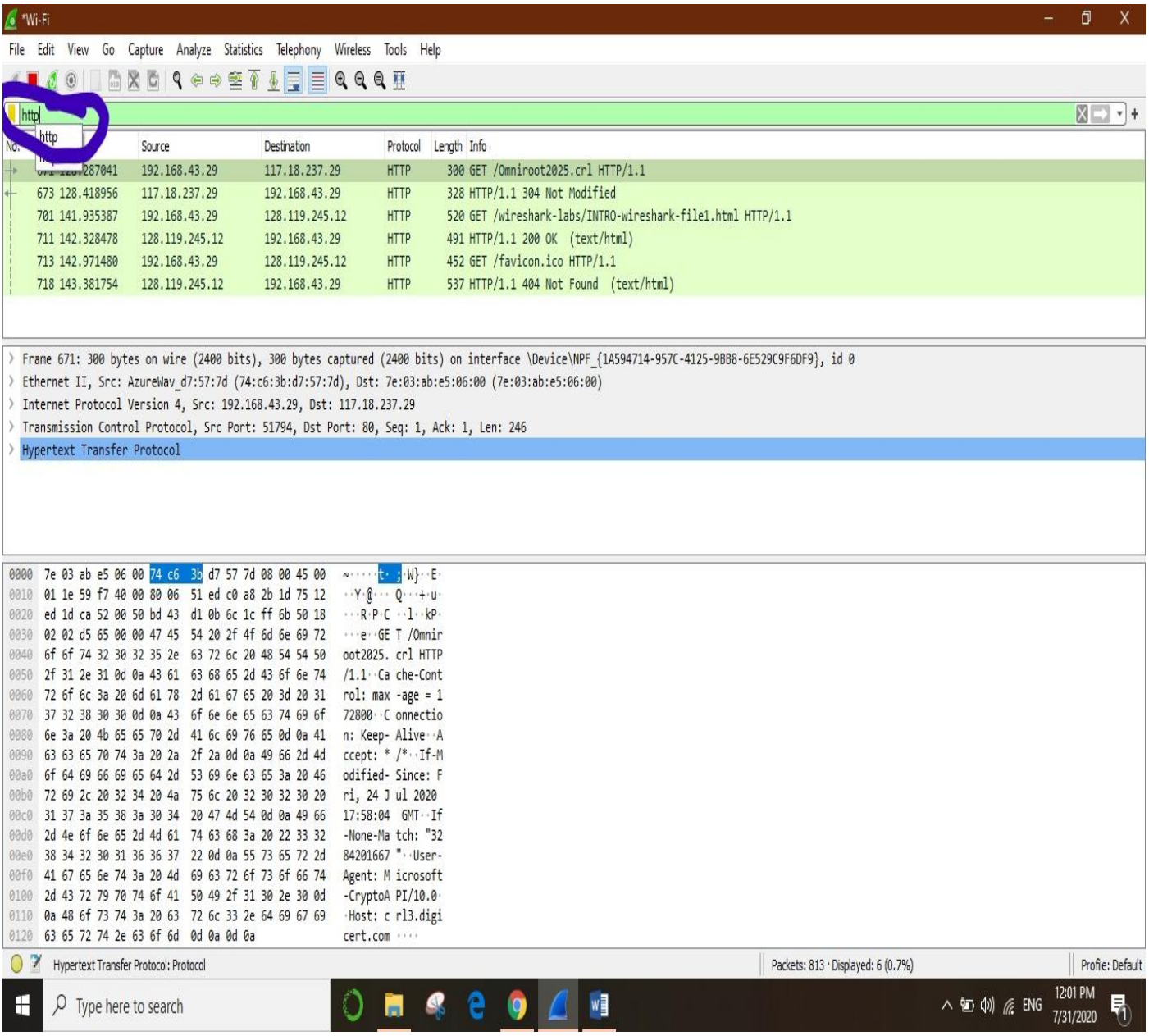


List of packet that are captured:

Here the name of the file is packet capture.pcpng.

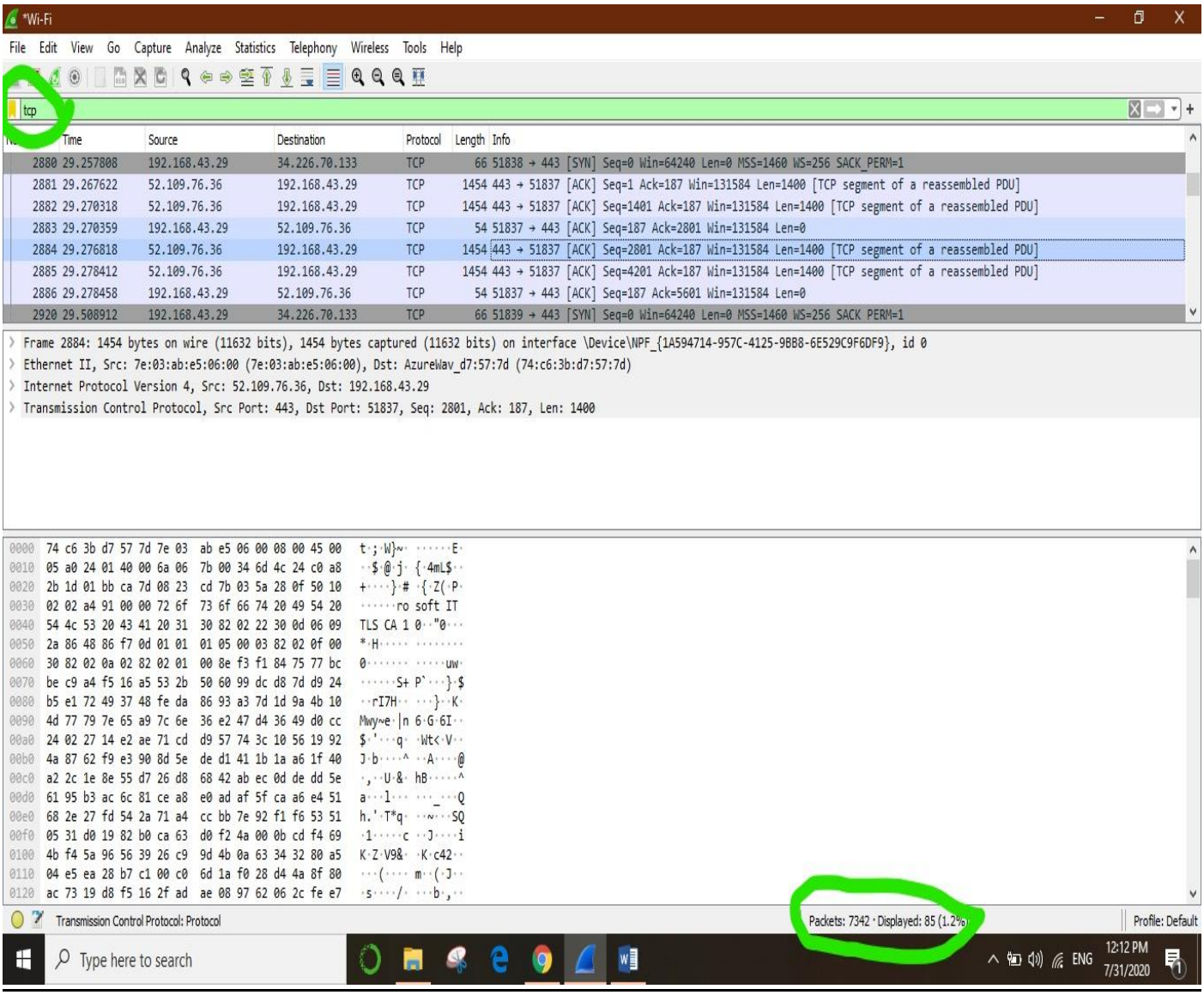


Capturing a packet set and received by HTTP:



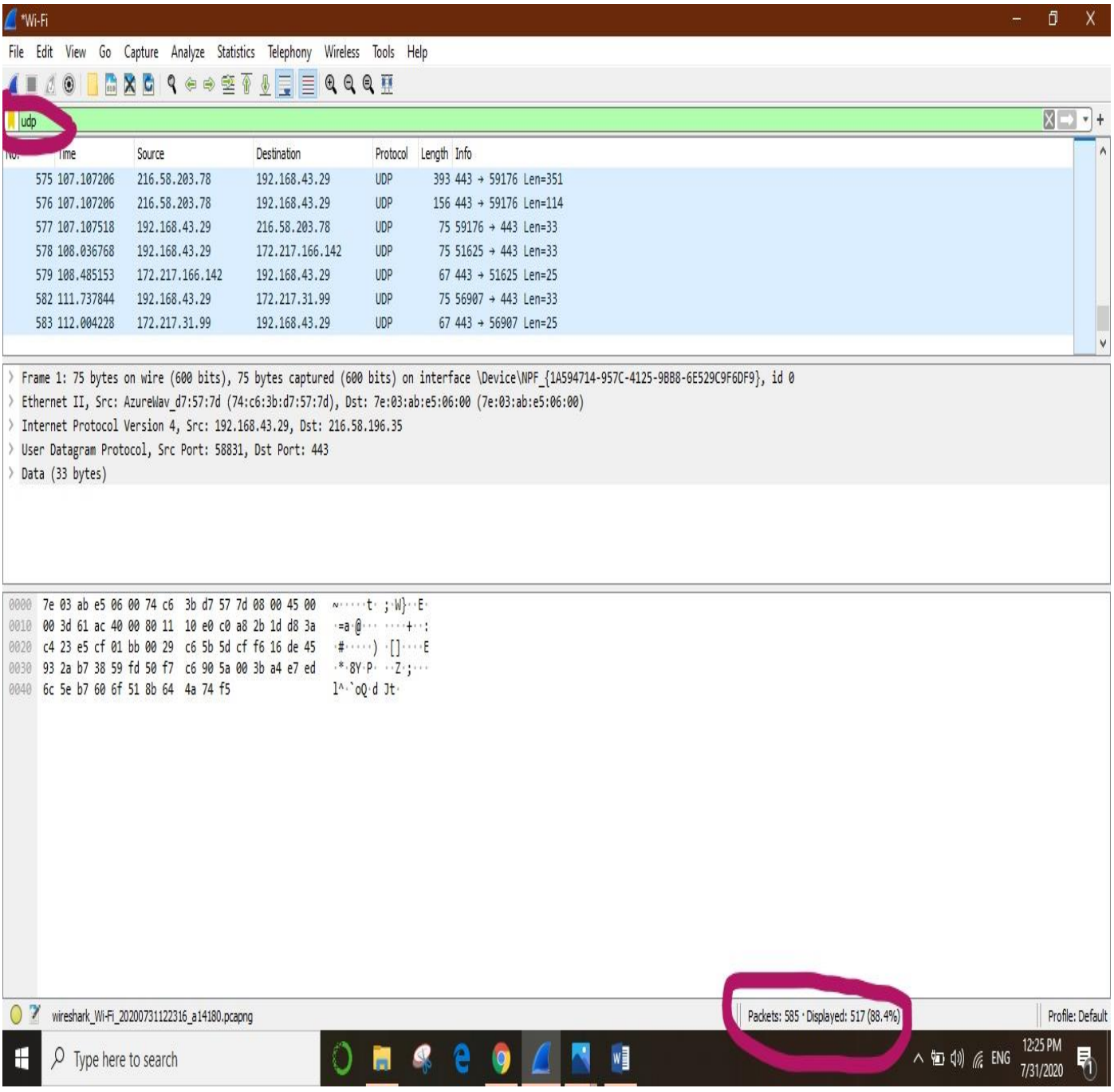
TCP packet capture:

Here we show that total number of packet captured are 7342 but displayed 85 because there are 85 TCP packet are send or received.



UDP packet capture:

Here we show that total number of packet captured are 585 but displayed 85 because there are 517 TCP packet are send or received.



Discussion:

This was an interesting lab. I learned many things from this lab. This lab helps me to understand the basic of wireshark display such as how to use wireshark display, how to capture different types packets such as tcp, udp etc. I also learn how to filter a packet using wireshark. I can successfully capture different types of packets as screenshot given above.