**Mawlana Bhashani Science and Technology University**

****



**Lab-Report**

Report No:04

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance:11.09.20

Date of Submission:18.09.20

**Submitted by Submitted To**

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Name: Amrita kamkar

ID:IT-14060

4th year 2ndsemester

Session: 2013-2014

Dept. of ICT

MBSTU.

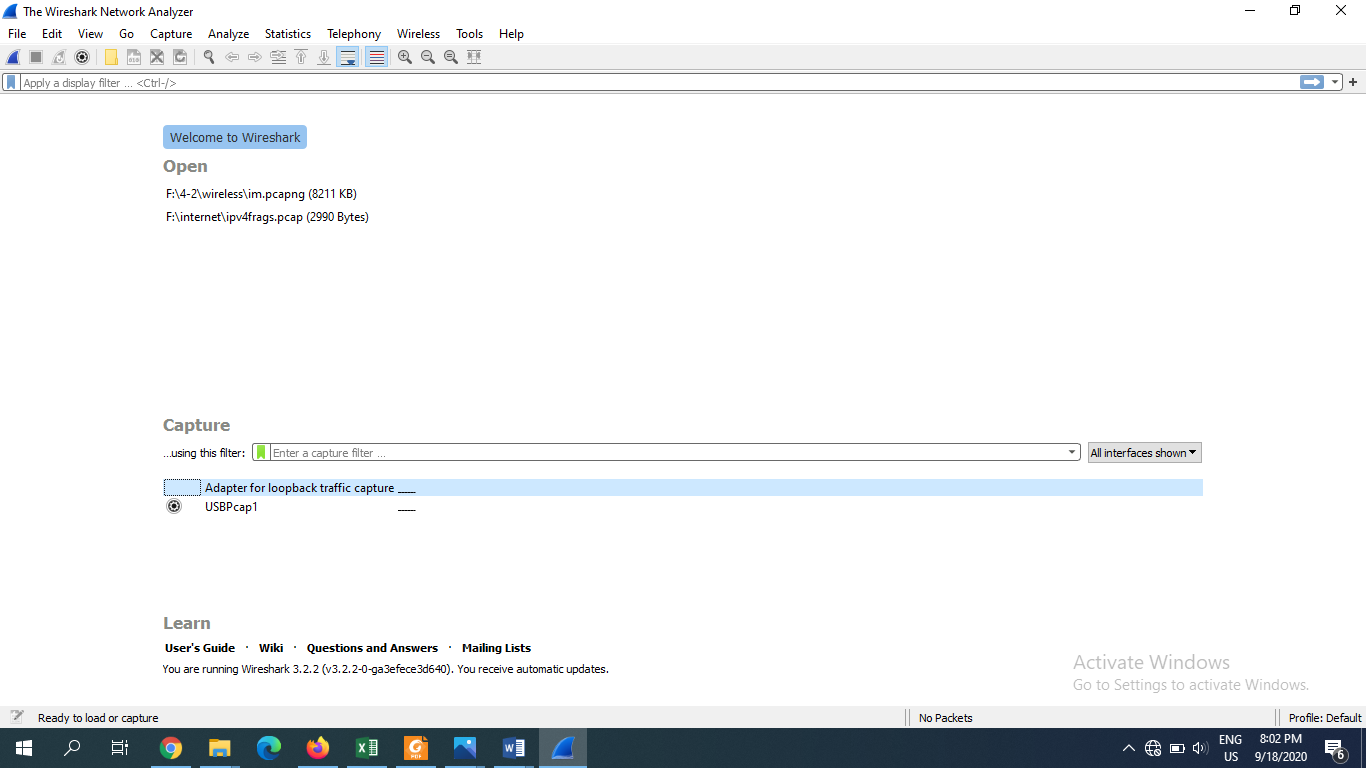
**Experiment No:04**

**Experiment Name:** Protocol Analysis with Wireshark

**Objectives:** Wireshark is a network traffic analyzer which is also an essential tool for any security professional or systems administrator. This free software lets us analyze network traffic in real time. This is one of the troubleshooting issues on our network.In this lab I am going to analyze the wireshark protocol.The capturing of traffic with specific network would be done .

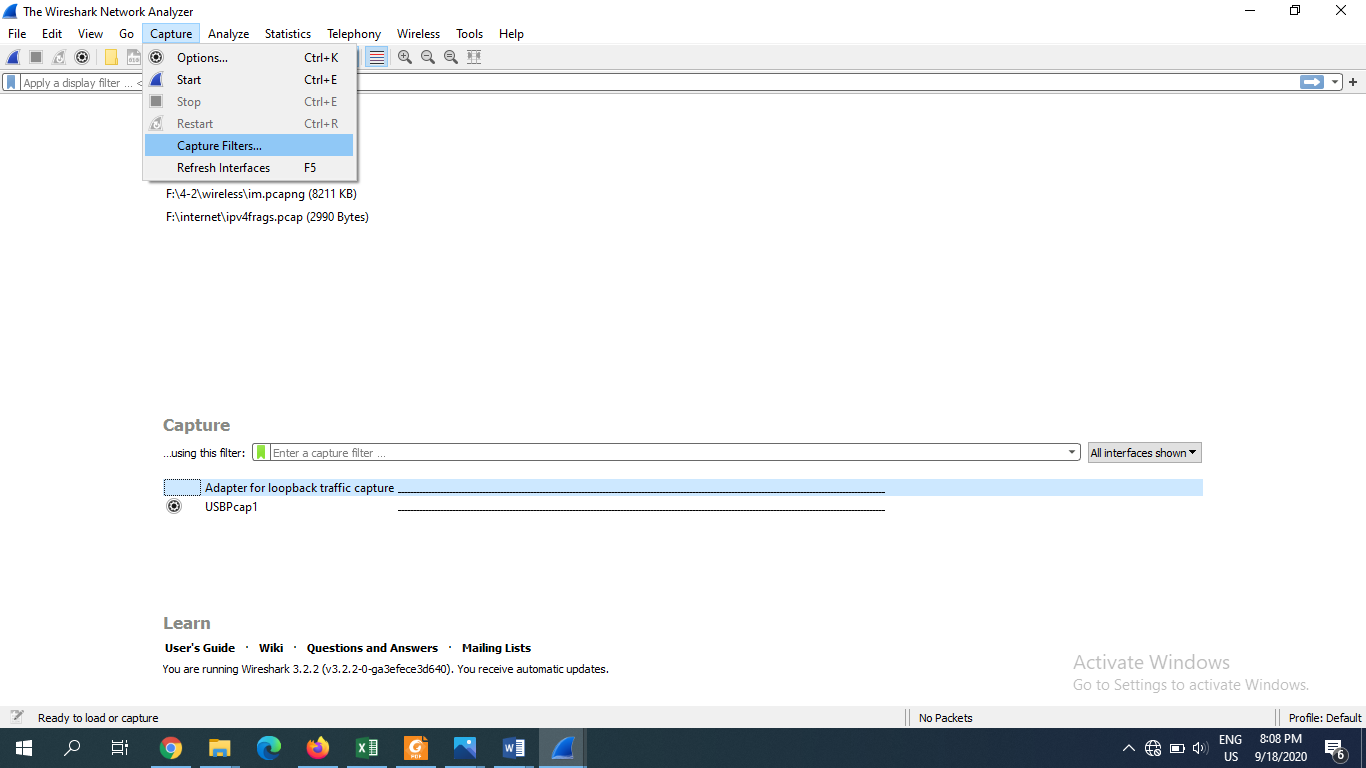
**Theoretical Explanation:** Wireshark is a network packet analyzer as a measuring device for examining what’s happening inside a cable. It can capture traffic from many different network media types including ethernet,wireless LAN,Bluetooth,USB and more. The specific media types supported may be limited by several factors, including our hardware operating system.

**Working Procedure for capturing Data packets:** There are some steps that to be **followed in this lab.**First of all I open the wireshark.



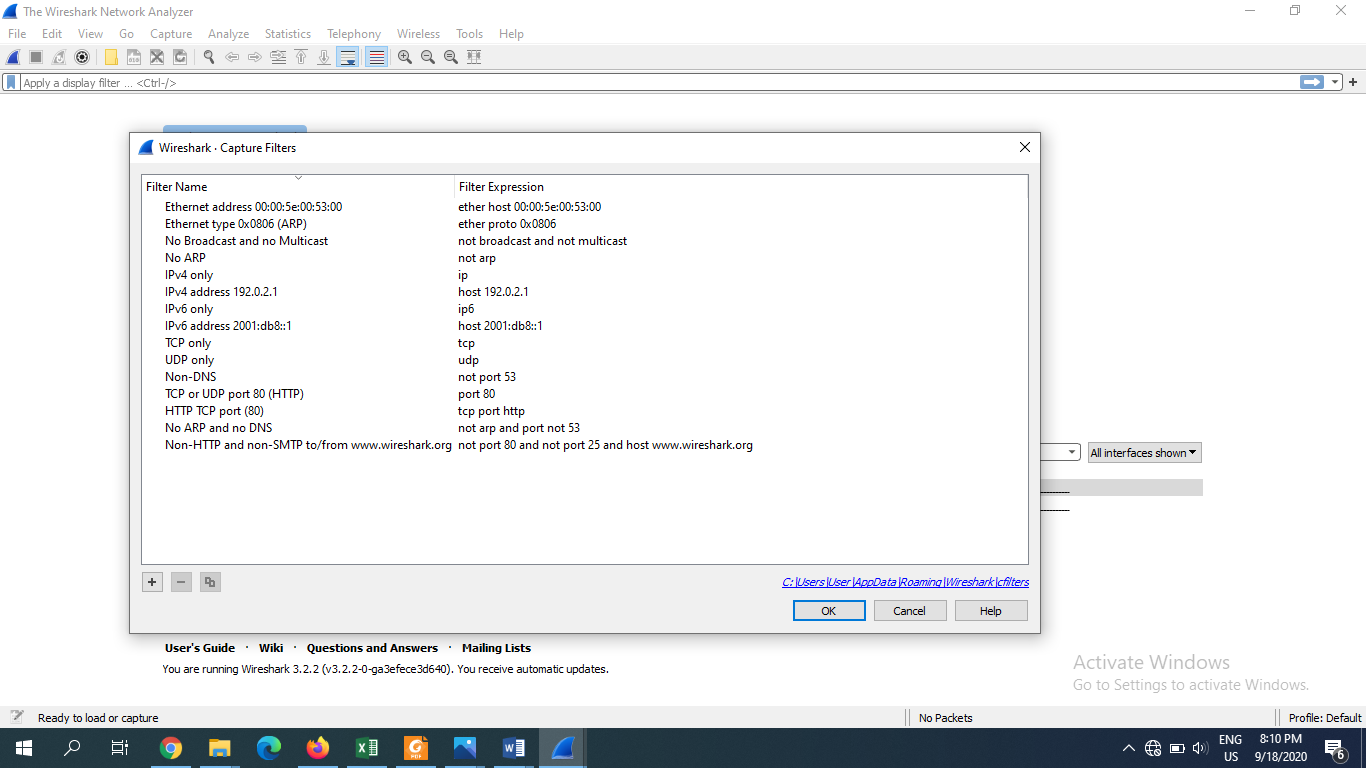
**Fig1:Openning wireshark**

Then to go to the capture and it’s capture filters.



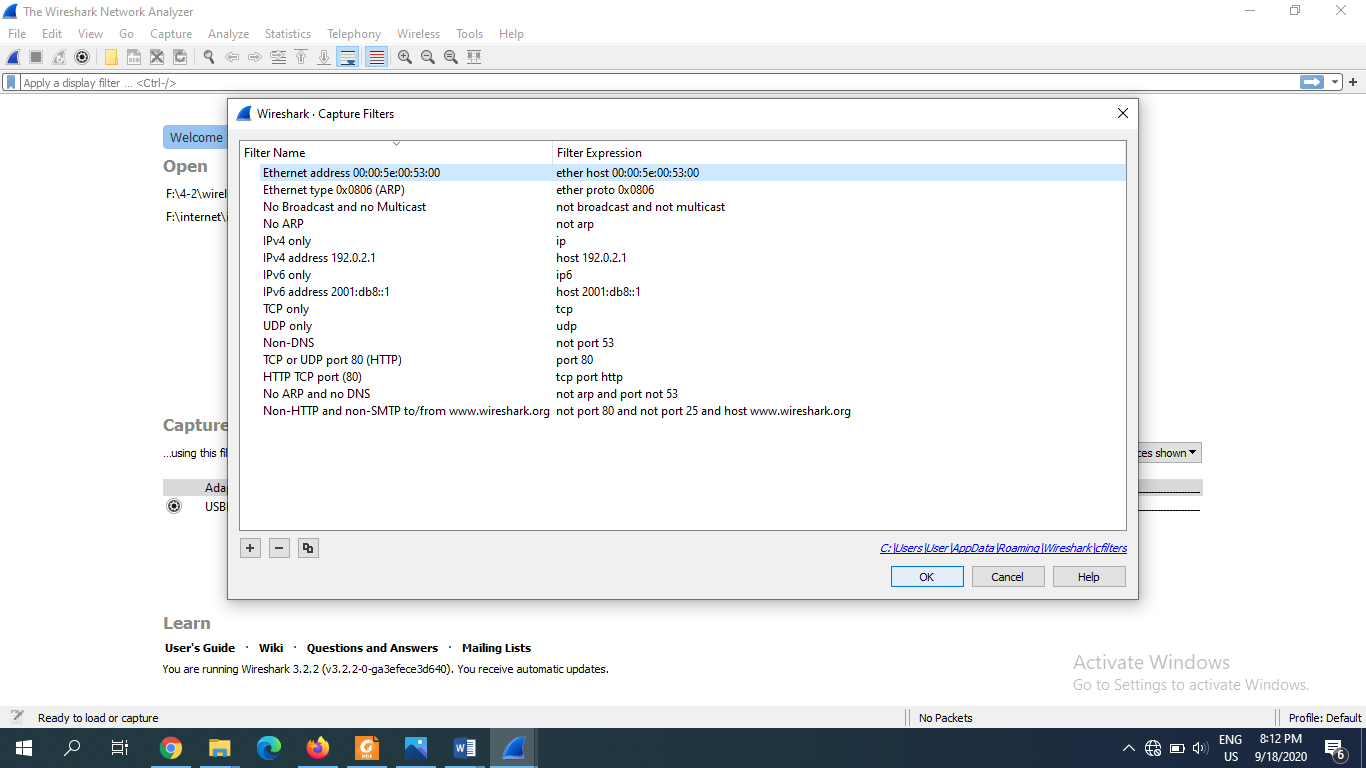
**Fig2:selecting to capture filters**

There would be some networks from where I need to select the one which has it’s IP address.



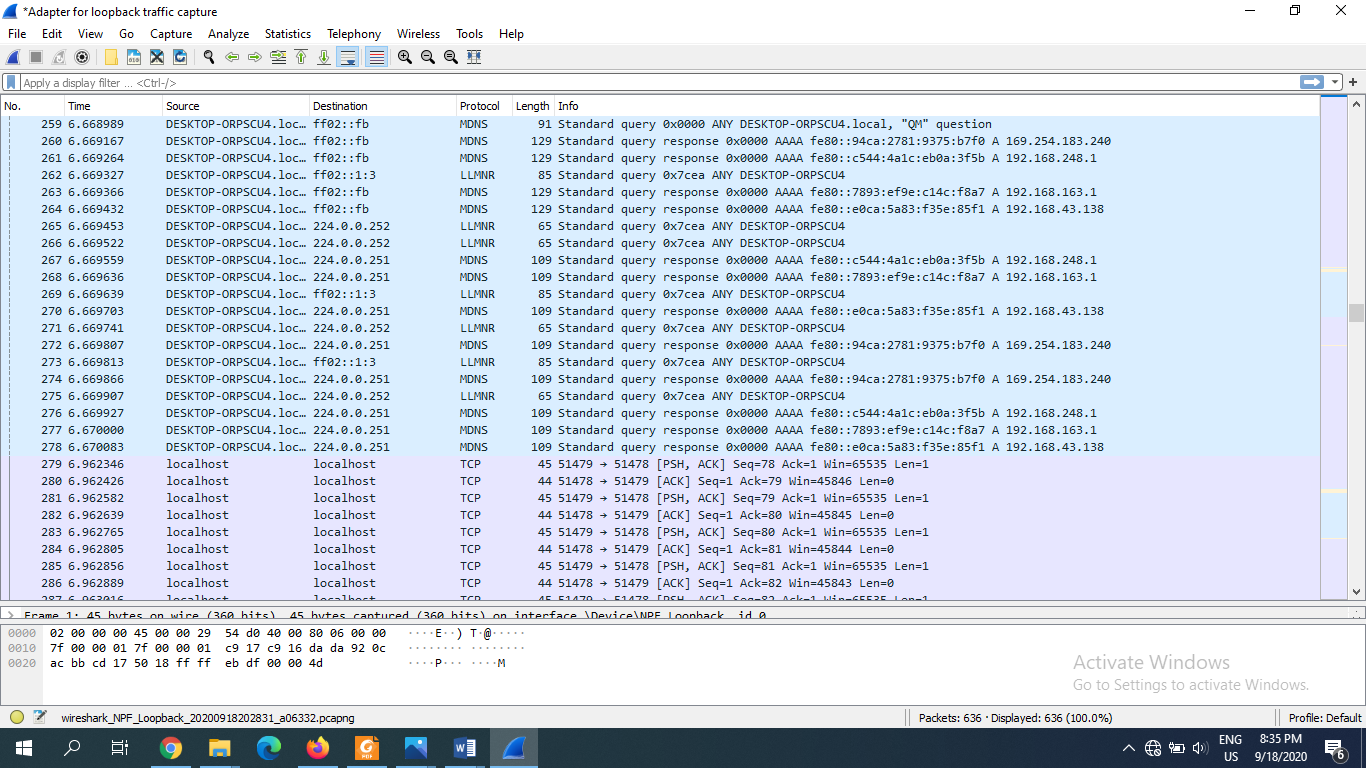
**Fig3:selecting the network**

I selected the ethernet

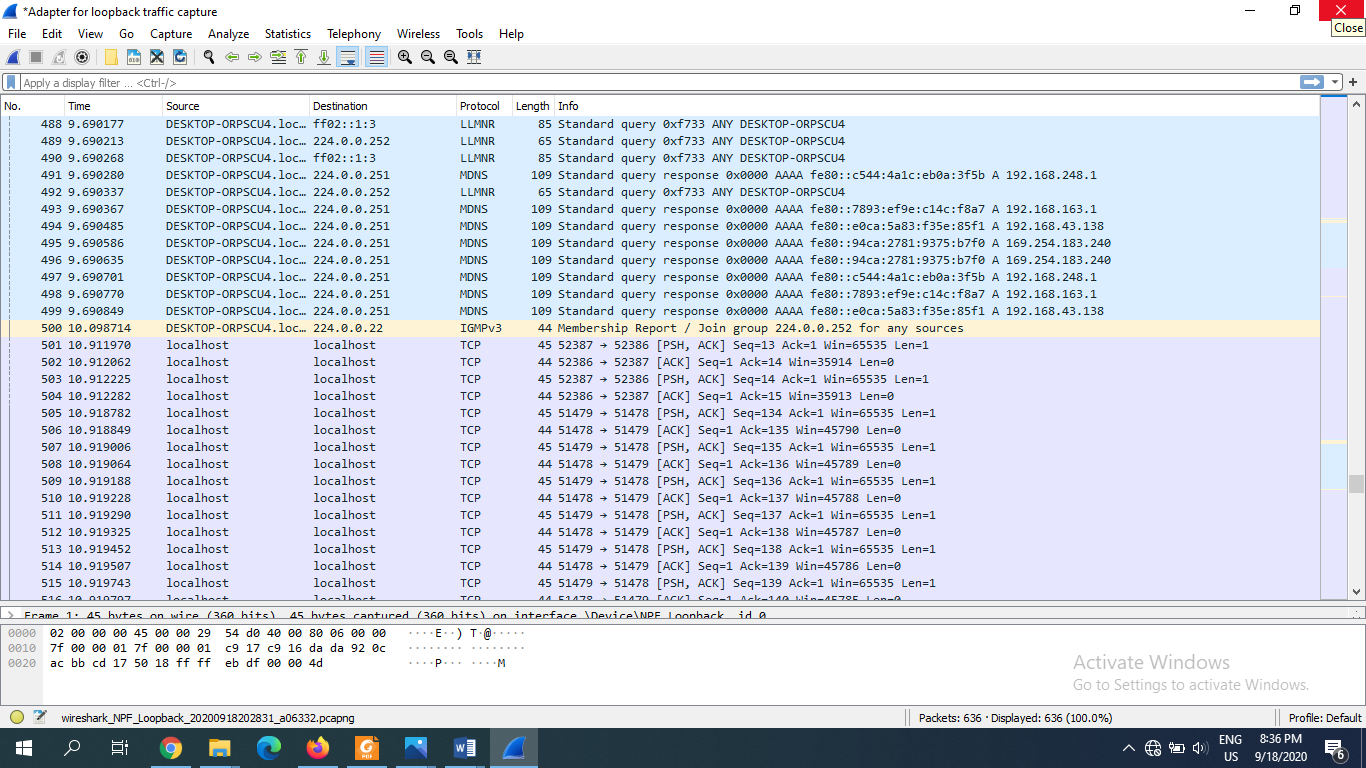


**Fig4:selecting network**

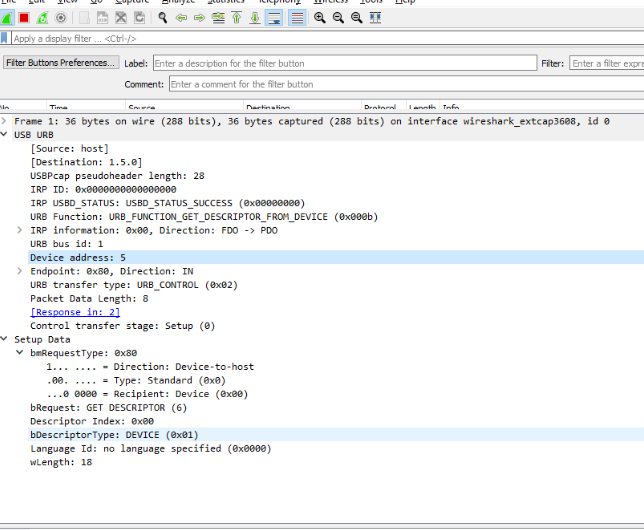
Then it’s needed to be start which would be



**Fig5:starting the capturing**

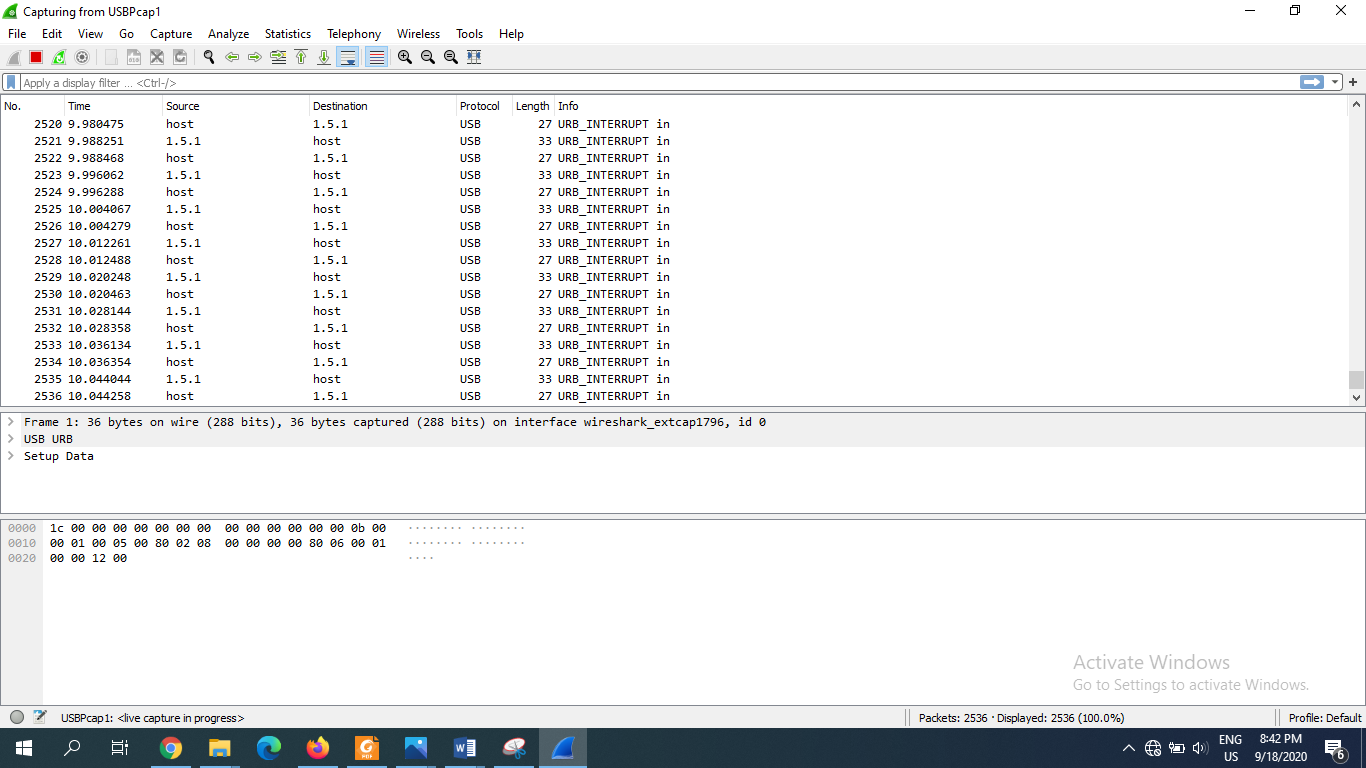


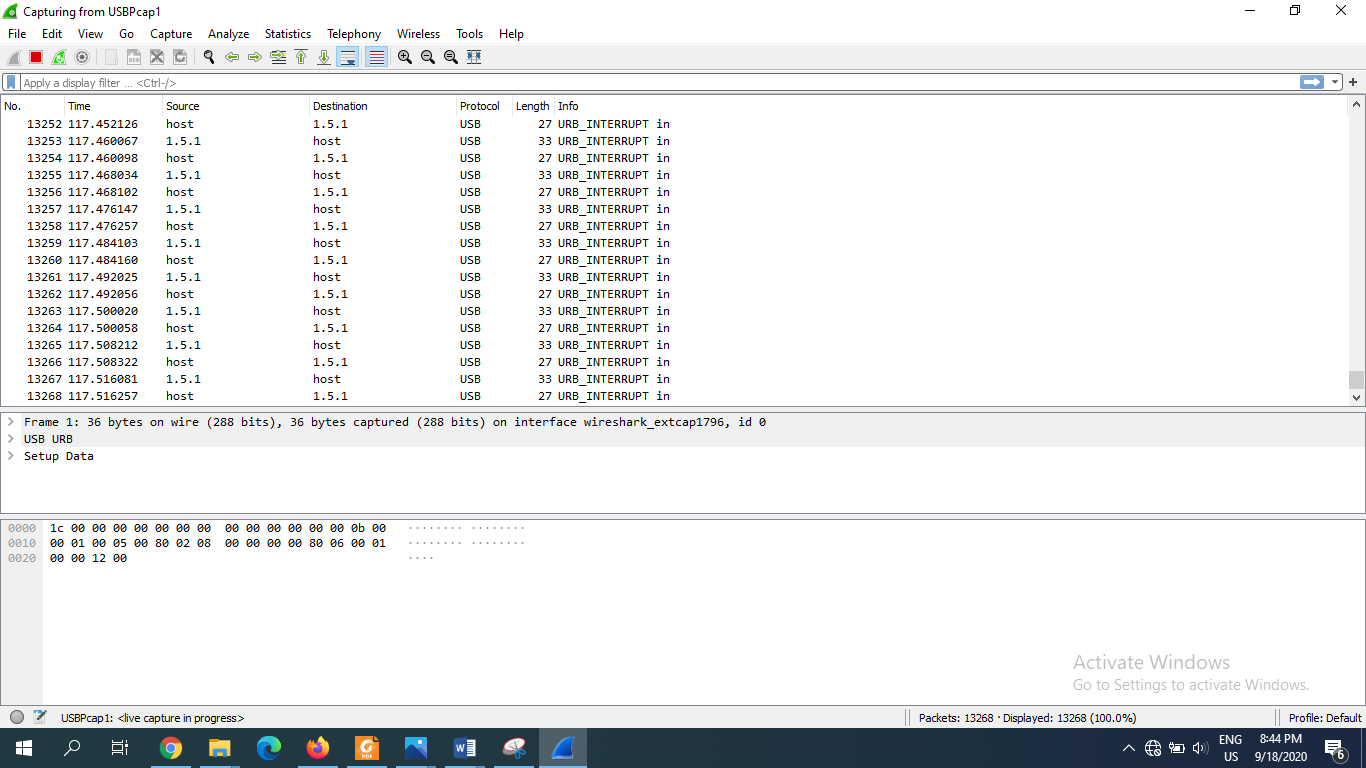
Manually performed analysis



**Fig6:Manuall analysis**

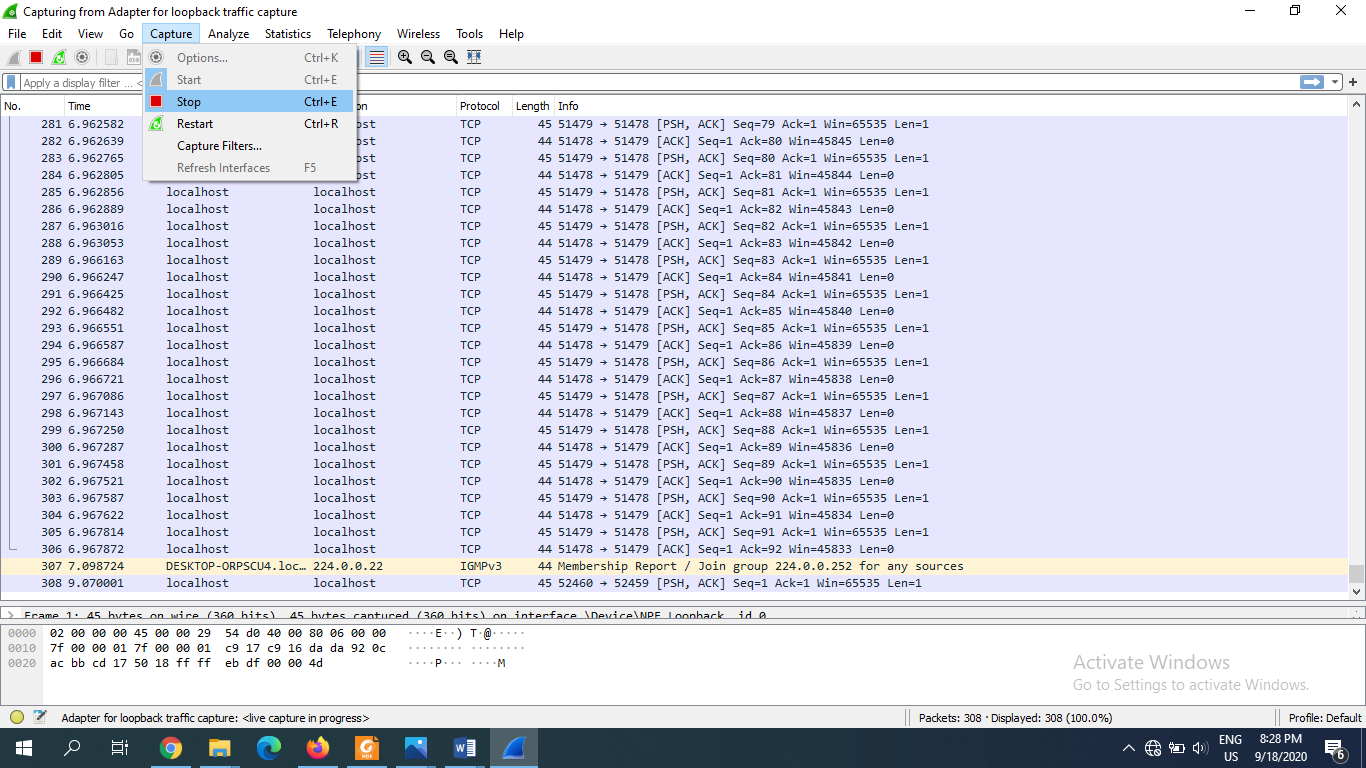
Another network that was tried is the USBP cap1.





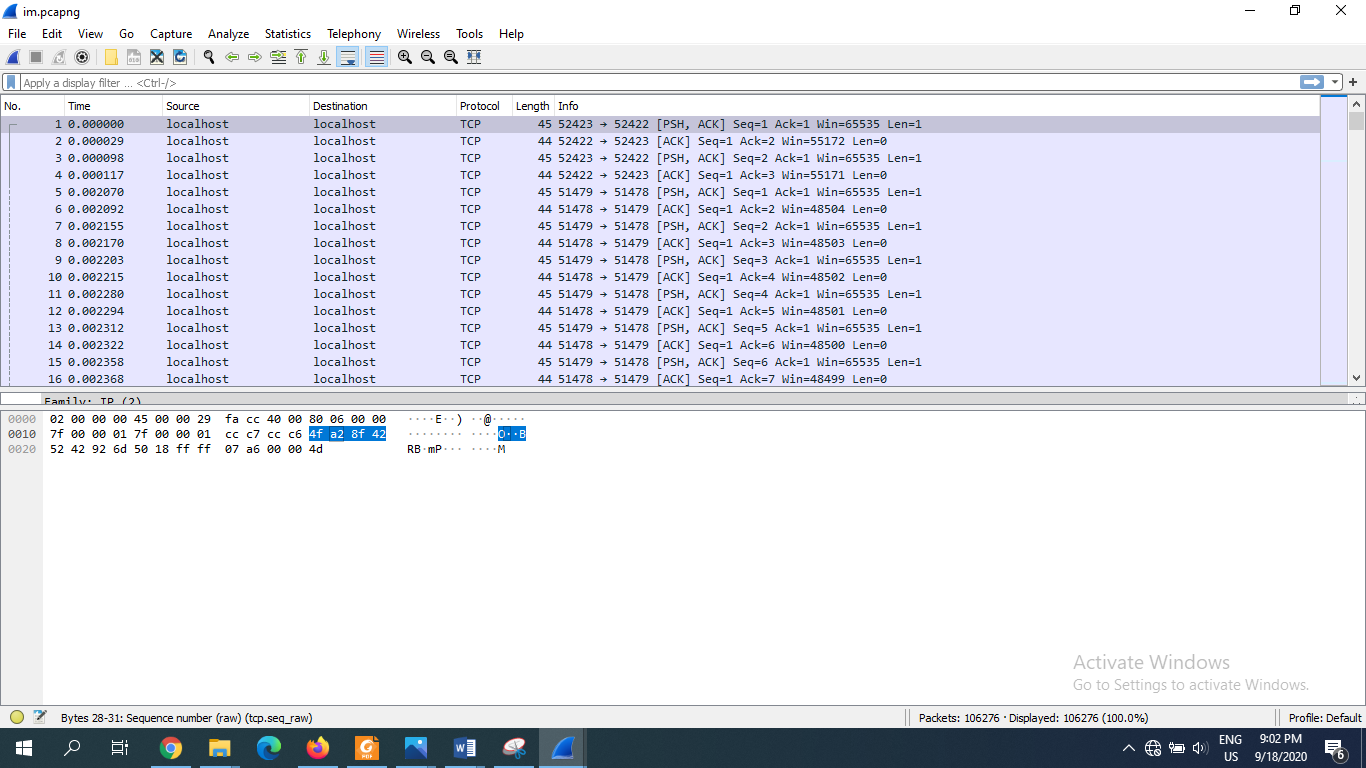
**Fig8:capturing with another network(USBP cap1)**

The capturing can be stopped by clicking the stop



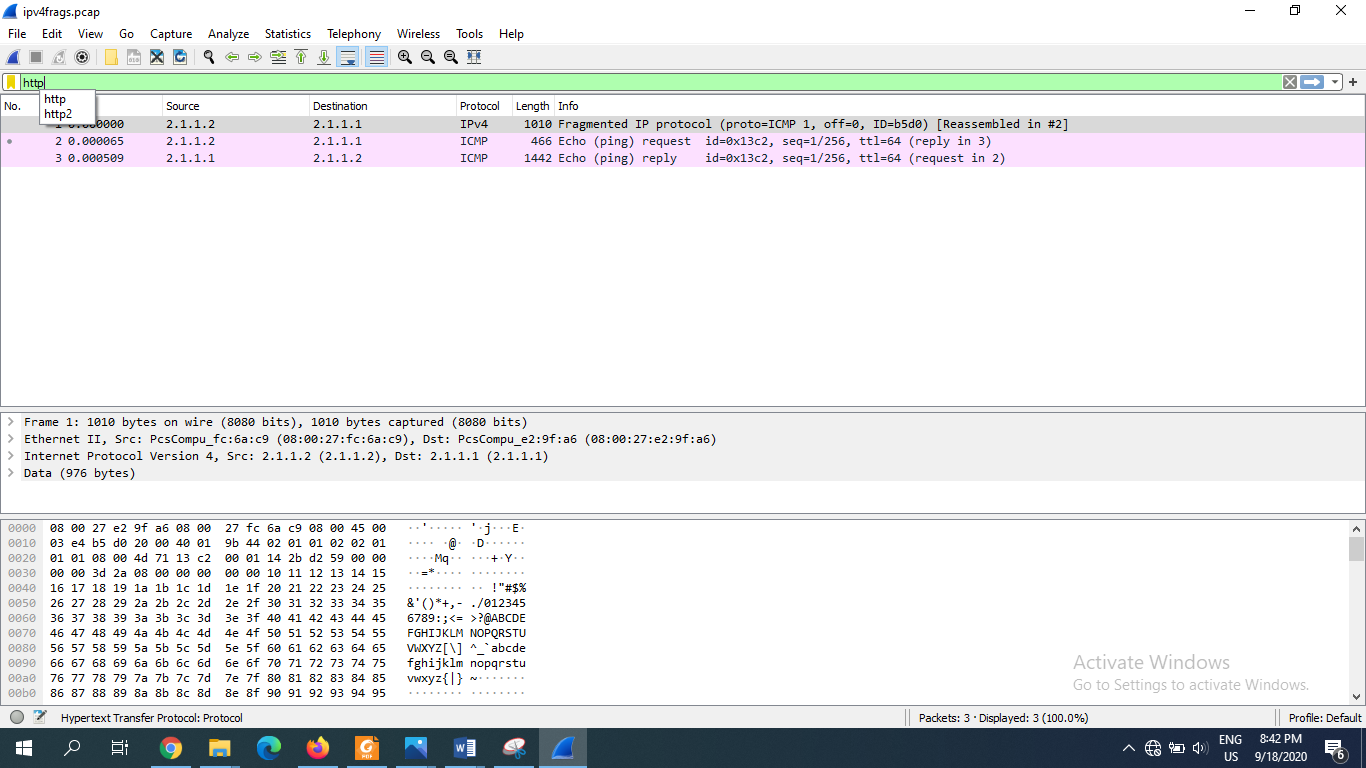
**Fig9:stopping the capture**

Packet bytes consists of Hex,ASCII and offset fields.



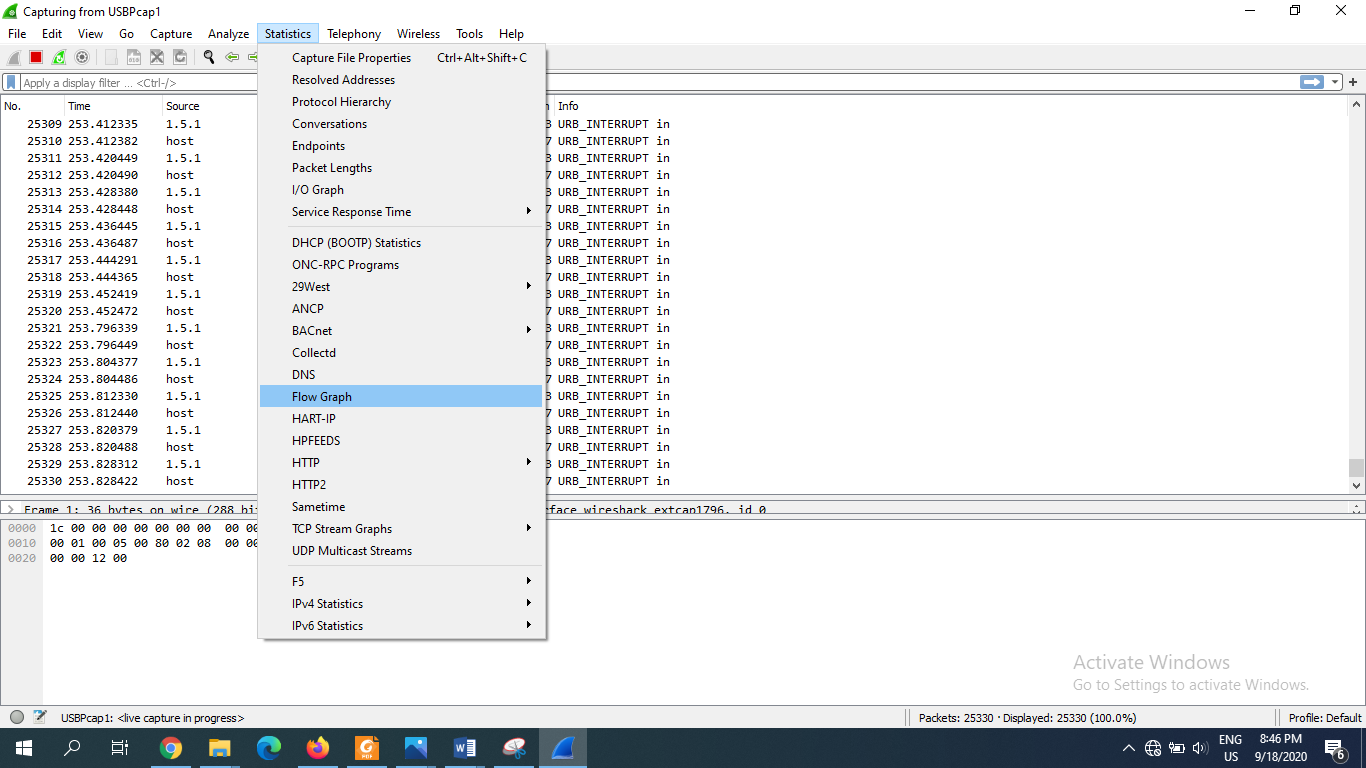
**Fig10:consisted data packet fields**

The packet details pane is

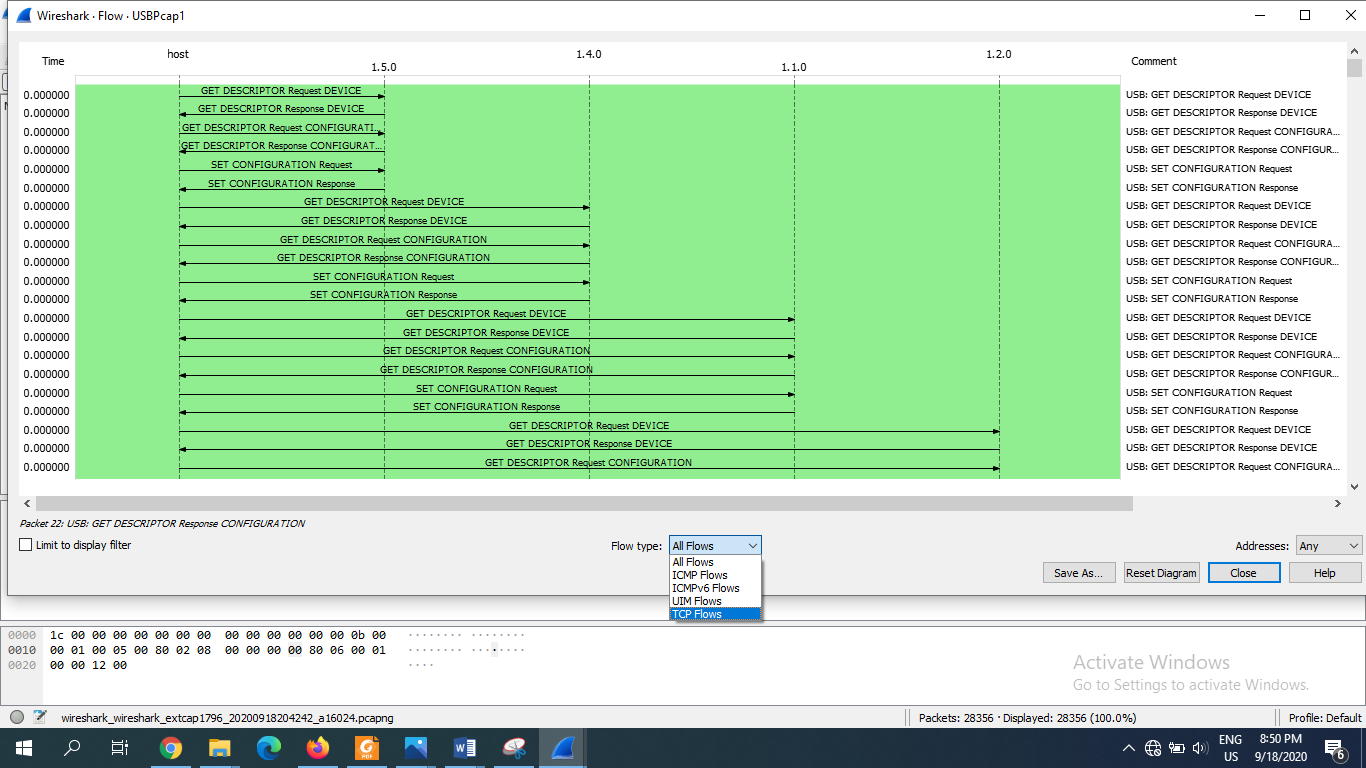


**Fig11:packet details for pane segment**

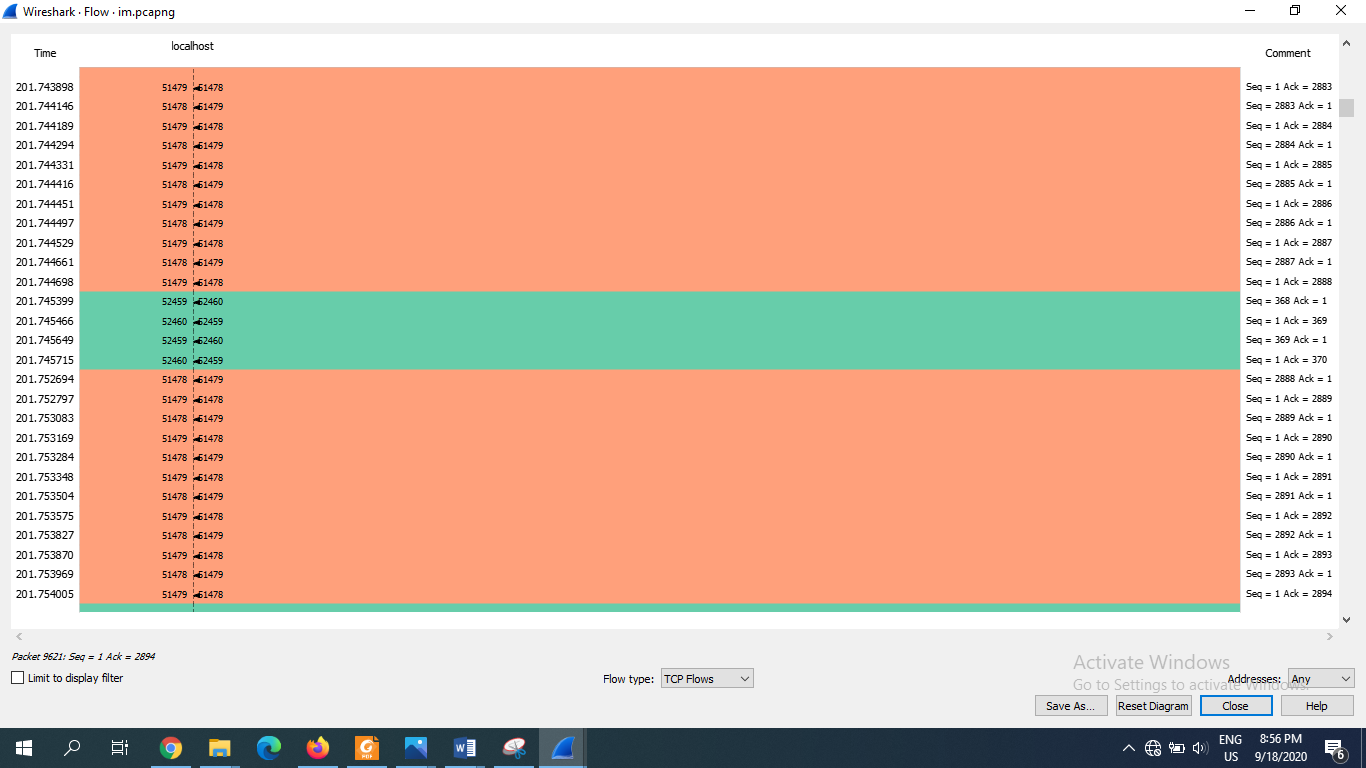
To see the traffic flow, the flow graph option in statistics is then needed to select.

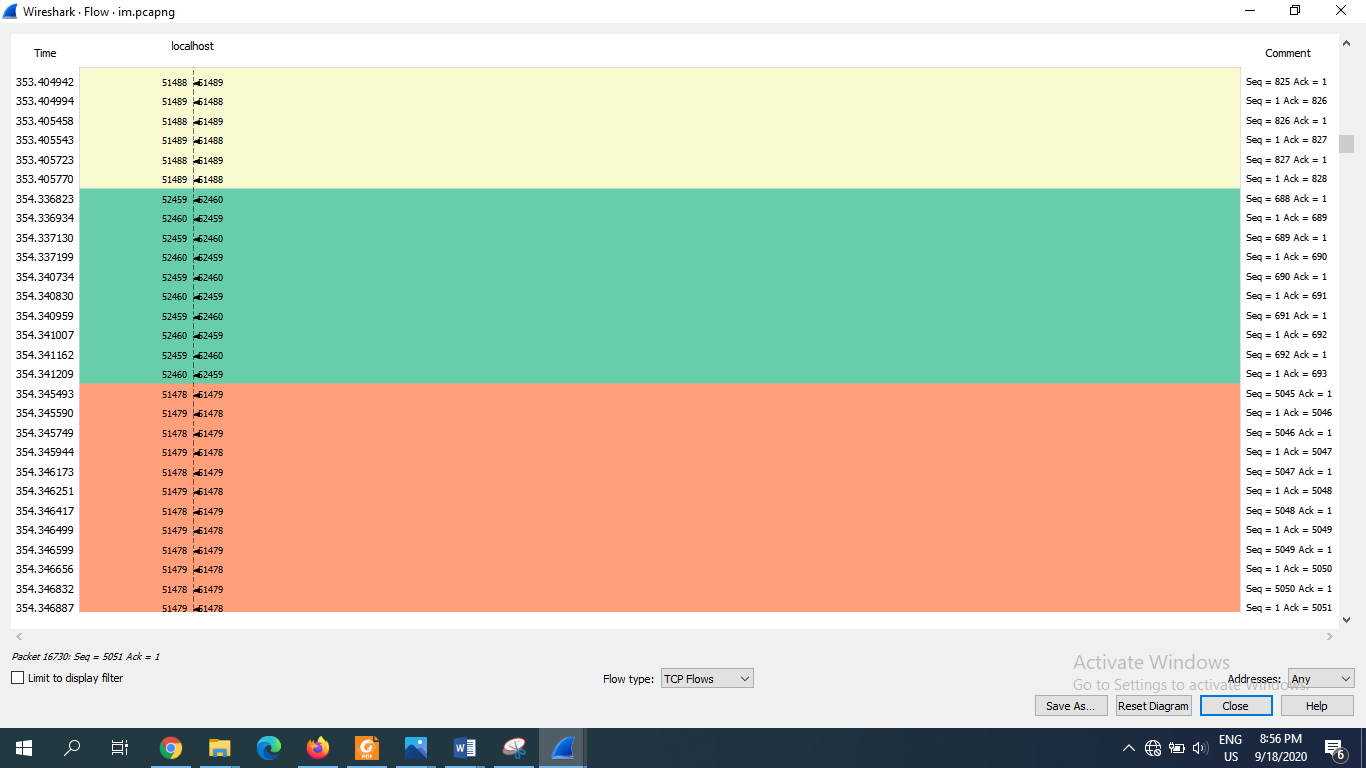
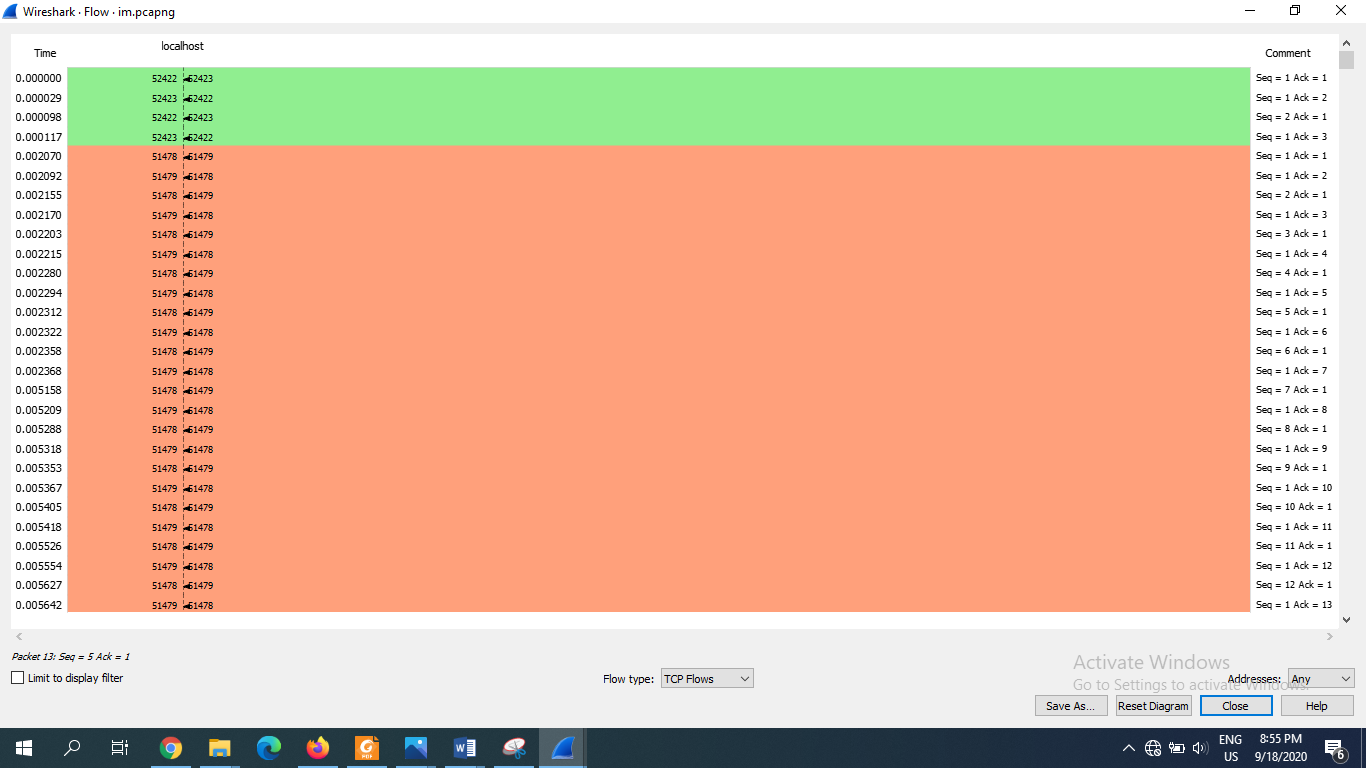


Then the TCP flow is changed from all flow.



The TCP flows are





**Fig12: Graph of TCP flow statistics**

**Discussion:** This lab, required some steps to be followed after installing the free software wireshark. Which is a traffic analyzer tool.Through the steps the capturing and analysis of traffic was done.After the capture the traffic flow was also elaborated.