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: 11.09.2020

Date of Submission: 18.09.2020

Submitted by

Name: Shourove Sutradhar Dip

ID: IT-16008

4th year 2nd semester

Session: 2015-2016

Dept. of ICT, MBSTU

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment N0: 04

Name of Experiment: Protocol Analysis with Wireshark.

Objectives:

1. Learn how to analyze protocols.
2. Understand how network protocols work.
3. Learn to use Wireshark to capture network packets in real time and display them in human-readable format.
4. Learn to use Wireshark for network troubleshooting and communication protocol analysis.

Procedures:

Step 1- Capturing:

Packets and Protocols can be analyzed after capture. To capture, first I go to capture menu and select options. Then I start capturing on interface that has IP address.

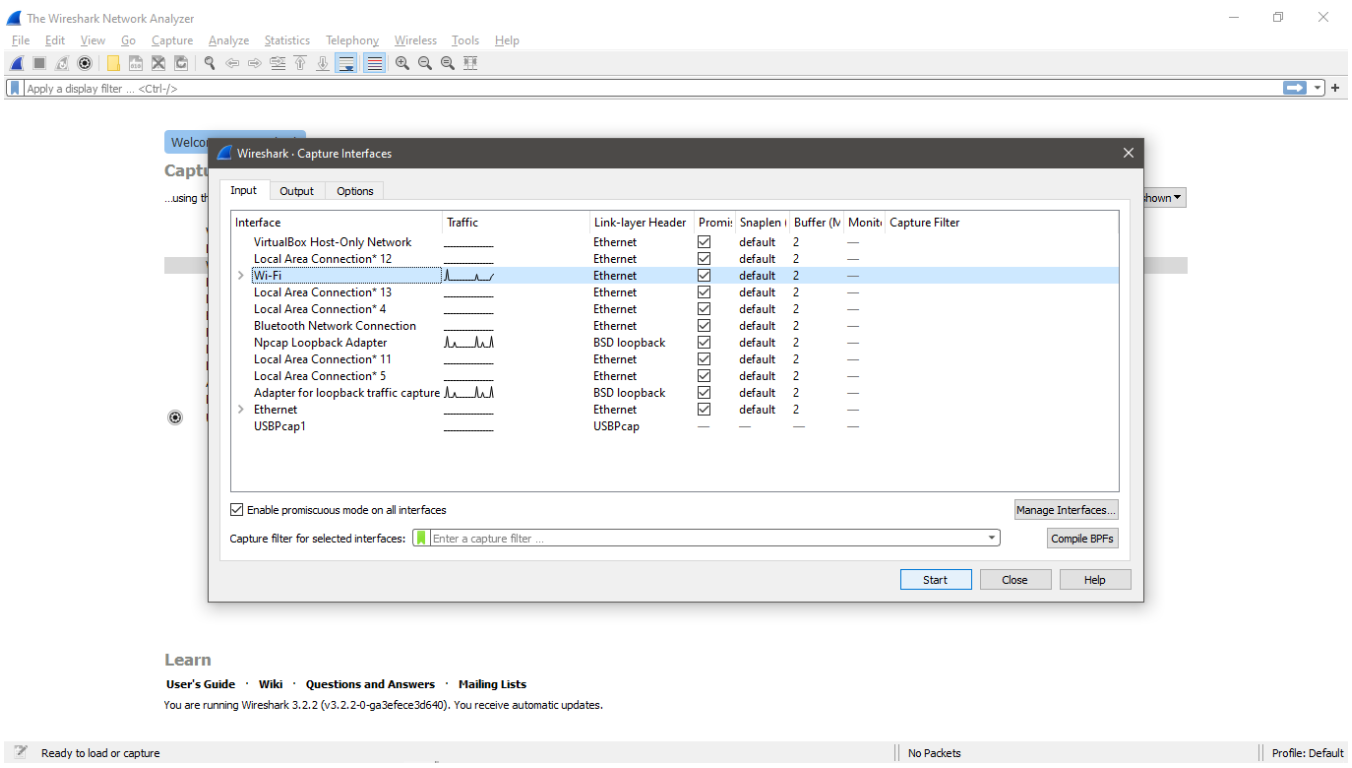

Figure-1.1: Starting Capture

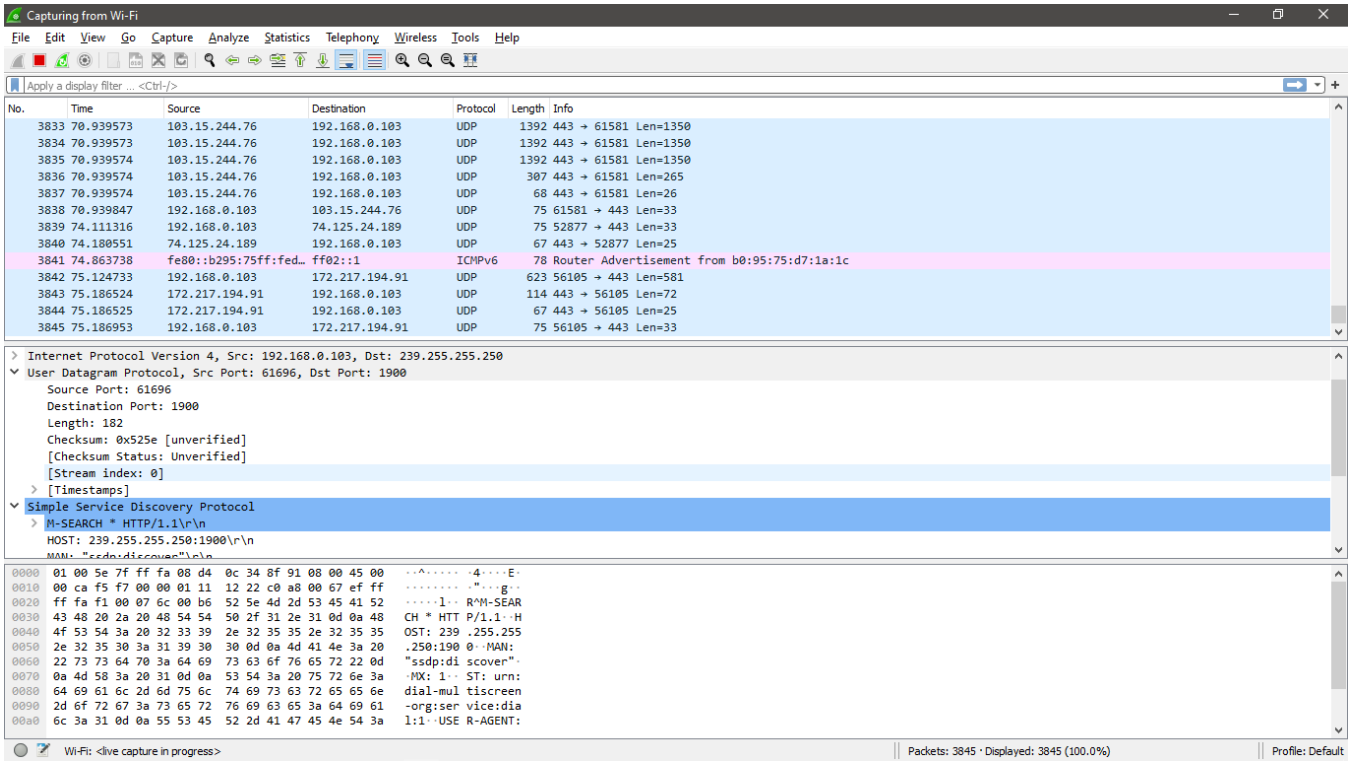

Figure-1.2: Dumped packages in main window of Wireshark

Step 2- Stopping Capture:

Capturing can be stopped by clicking on “Stop Capturing Packets” button on the main toolbar.

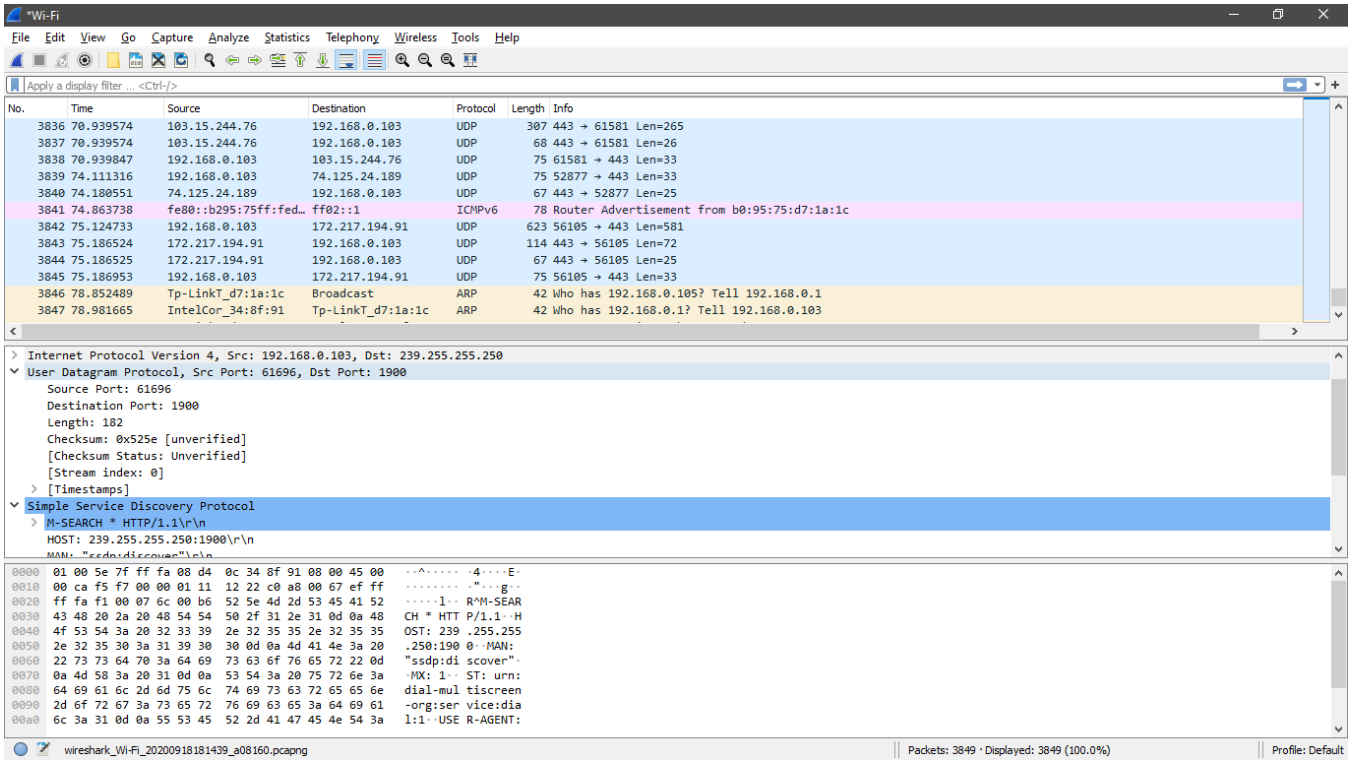

Figure-2: Stopping Capture

Step 3- Filtering:

We can filter the captures by entering the protocol name in “Apply a Display Filter” and enter.

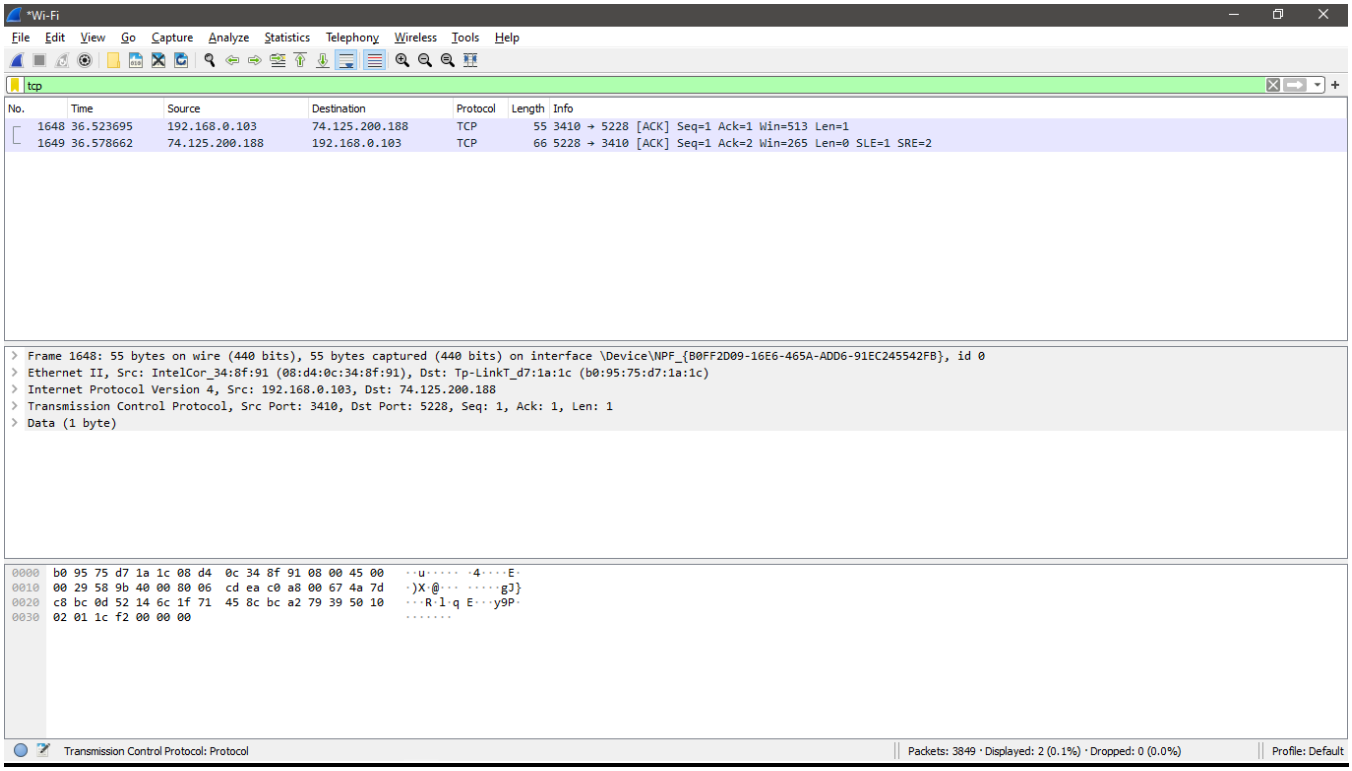

Figure-3: Filtering by TCP protocols

Step 4- Analyzing Protocols:

The analysis has to be performed manually. The given example below shows TCP segment with SYN and ACK fields set to 1.

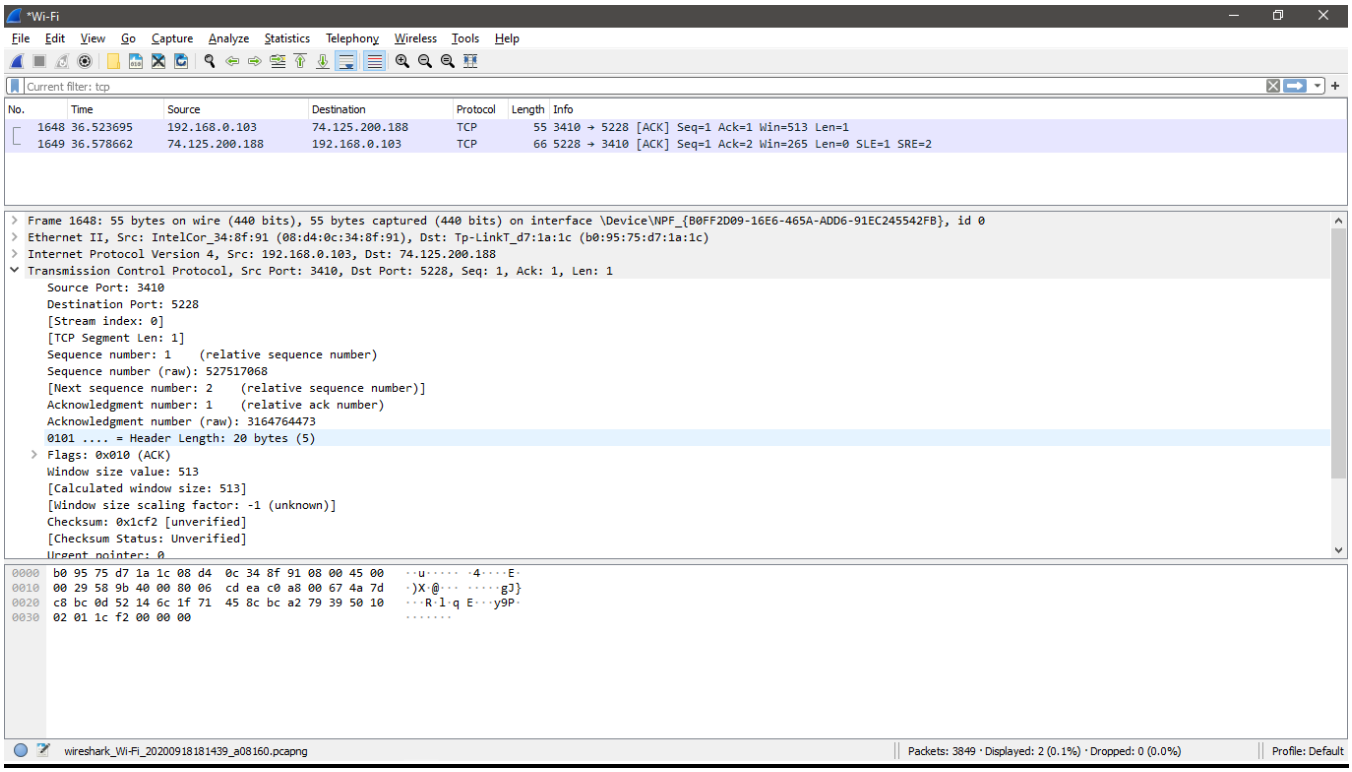

Figure-4: Analyzing TCP protocols

Step 5- Plotting a flow graph:

The Plotting can be done through the “Statistics” menu. First we select the “Statistics” menu and then go to “Flow Graph”. Then for a plotting the flow of a particular protocol, we can select an option from “Flow Type”. Here the given example below shows the “TCP Flows” has been selected as the “Flow Type”.

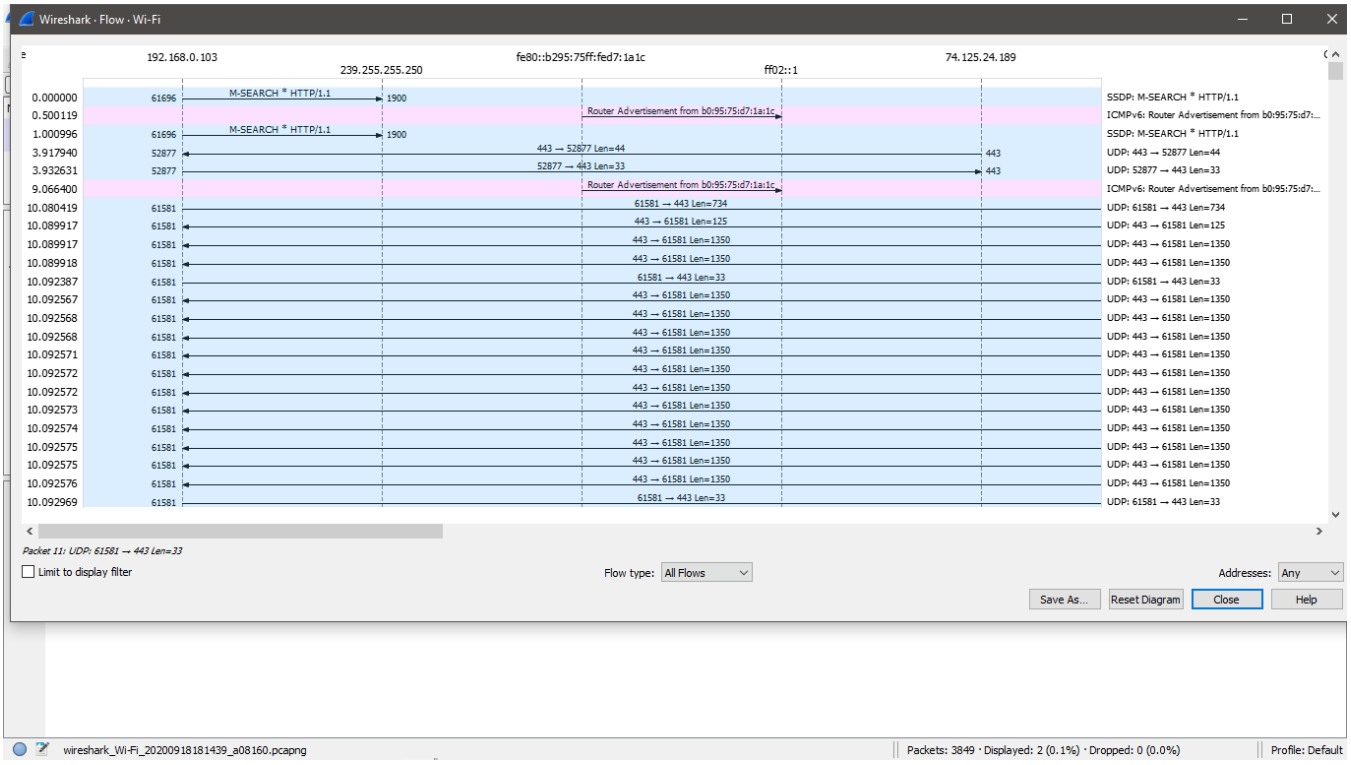

Figure-5.1: Plotting a graph for all flows

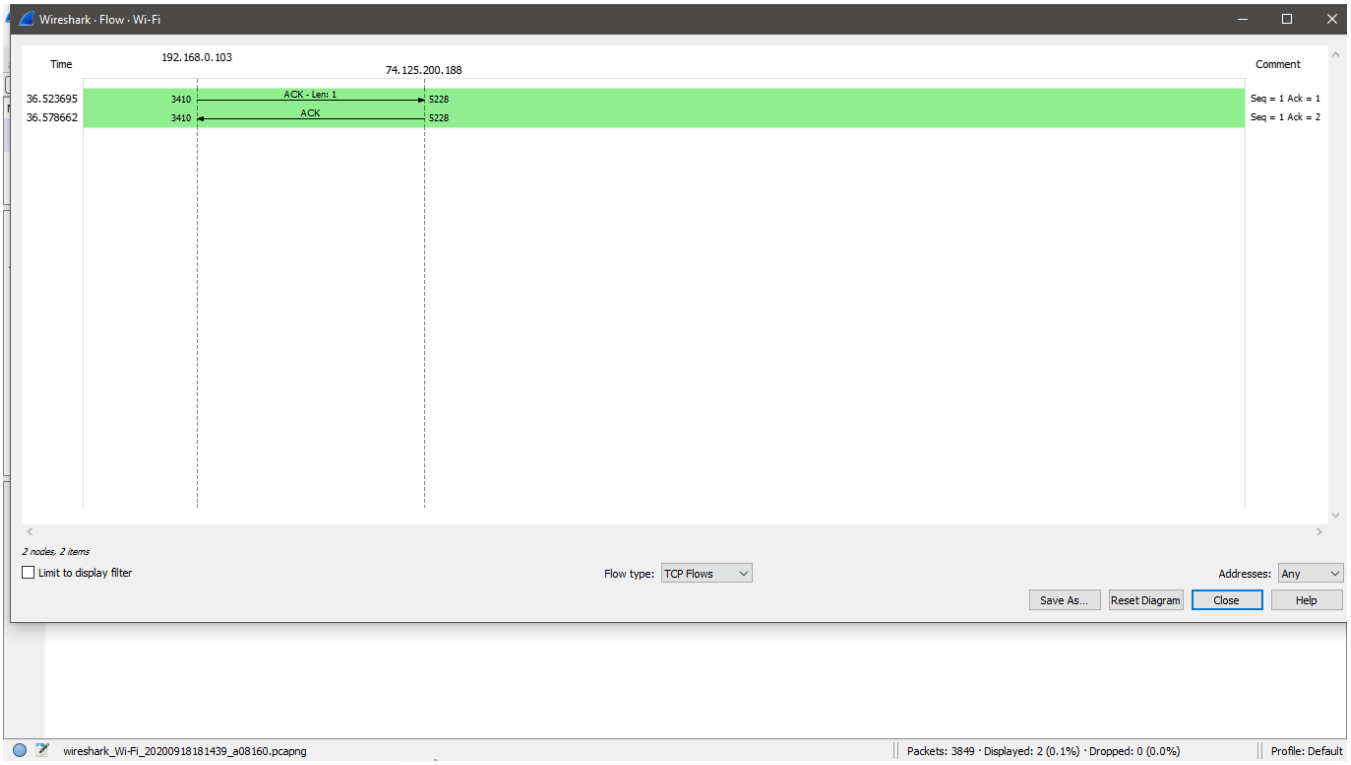

Figure-5.2: Plotting a graph for TCP flows

Conclusion:

From this lab, we've learnt how to analyze a protocol after capturing them by using Wireshark. The analysis helps us to understand how packets and protocols are transferred. The Wireshark helps us to visualize the flow of the protocols which helps us to understand the protocol flow more accurately.