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: Farzana Haque

ID: IT-15061

4th year 2nd semester

Session: 2014-2015

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No: 04

Experiment Name: Protocol Analysis with Wireshark

Objectives:

Wireshark is a free opensource network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis. This document uses Wireshark for the experiments, and it covers Wireshark installation, packet capturing, and protocol analysis.

To learn how to listen to local network traffic and analyze different protocols as well as learning to use some useful TCP/IP utilities.

Capturing Packets:

By clicking Capture menu the process of capturing will be started. It will show the available interfaces list. Then, we need to start Capturing on interface that has IP address

The packet capture will display the details of each packet as they were transmitted over the wireless LAN.

Capturing can be stopped by clicking on Stop the running capture button on the main toolbar.

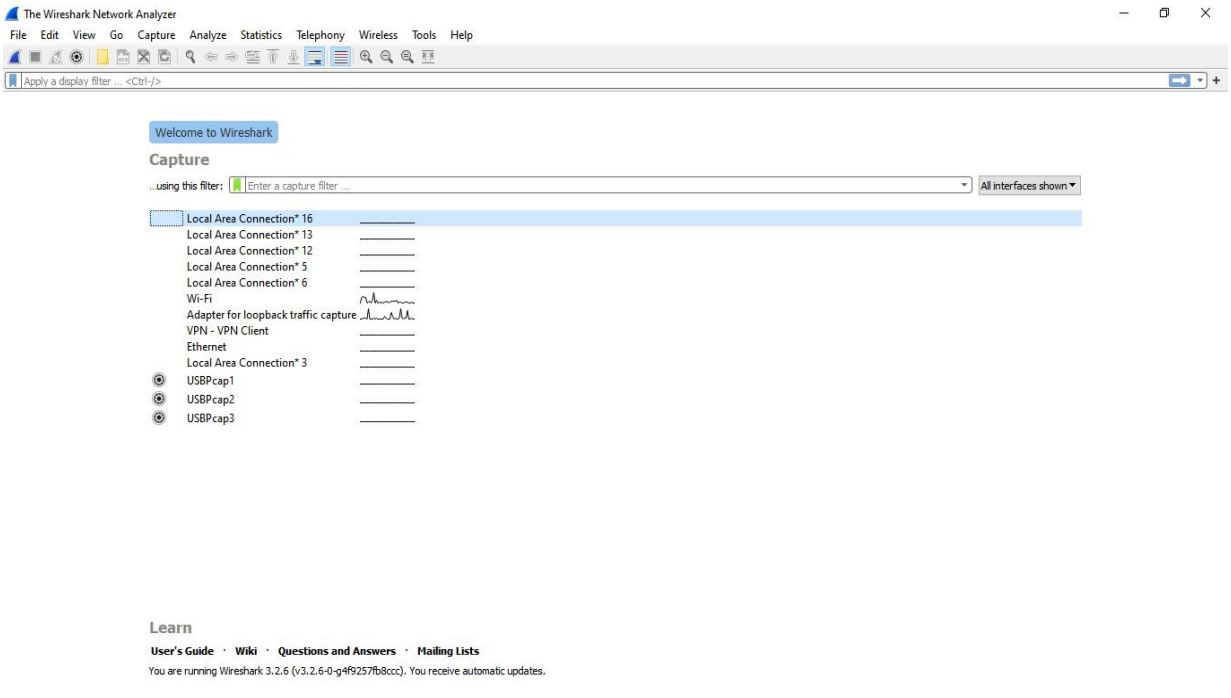

Figure 01: Wireshark Interface List

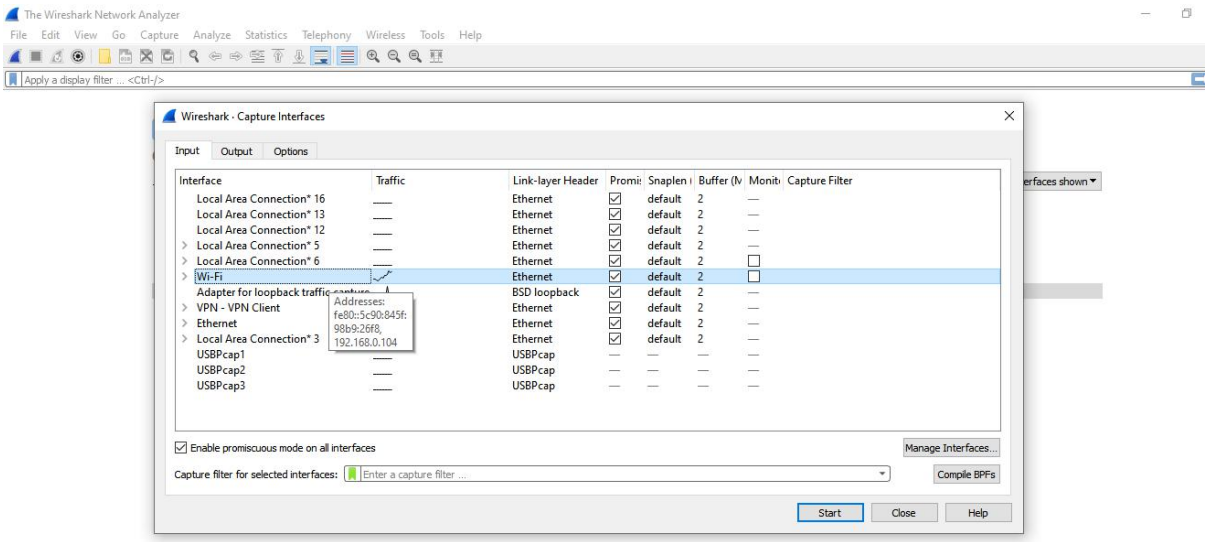

Figure 02: Start Capturing Interface that has IP address

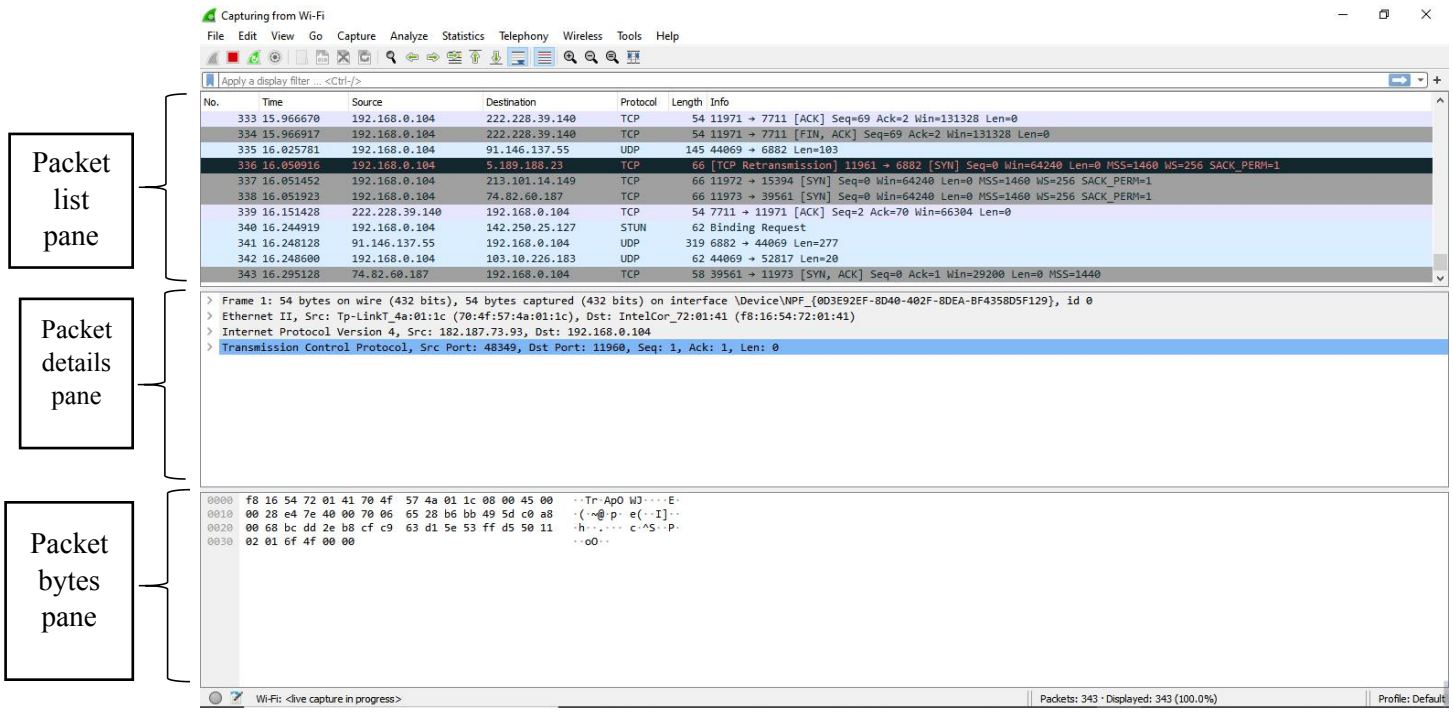

Figure 03: A sample packet capture window

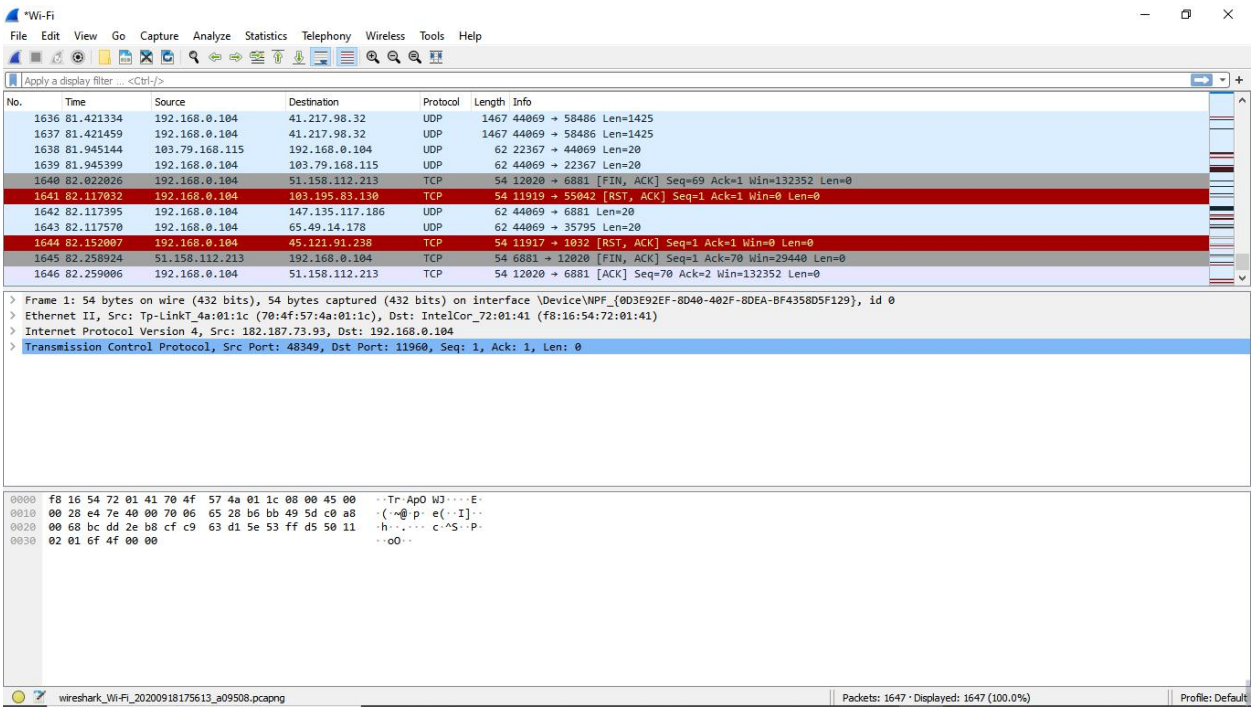

Figure 04: Stopping Capture

Filtering:

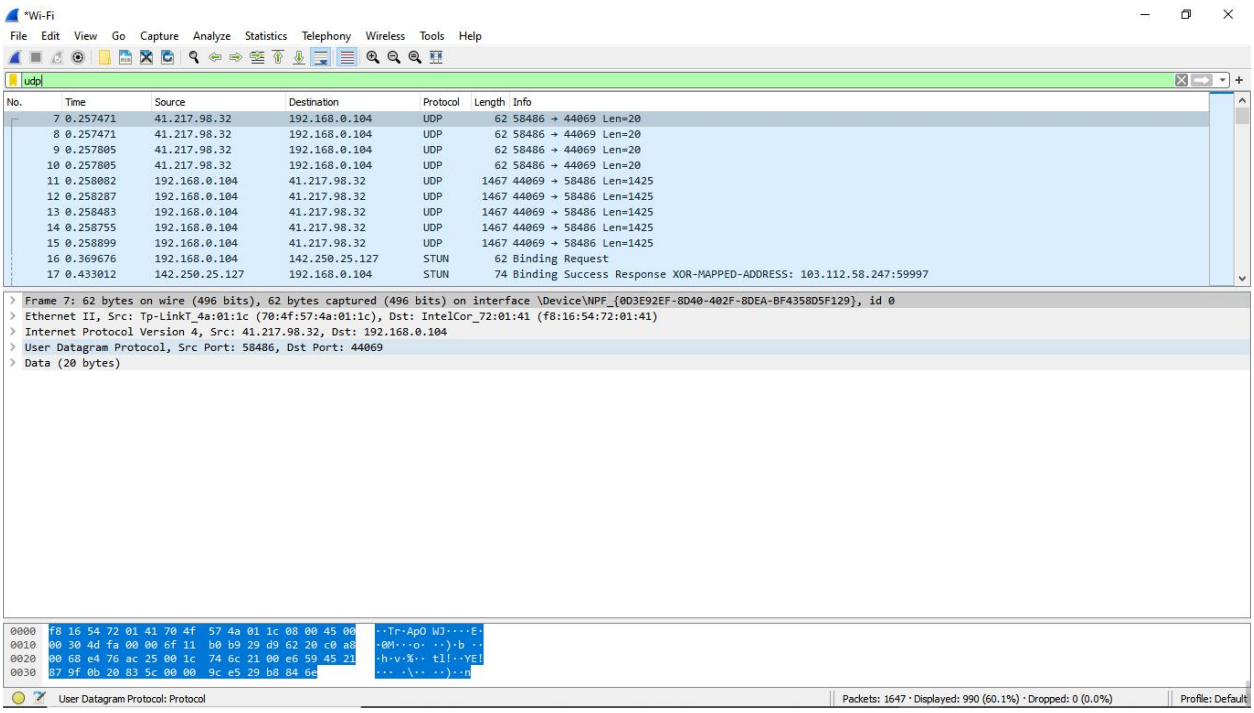

Figure 05: Filter by Protocol

A source filter can be applied to restrict the packet view in wireshark to only those packets that have source IP as mentioned in the filter.

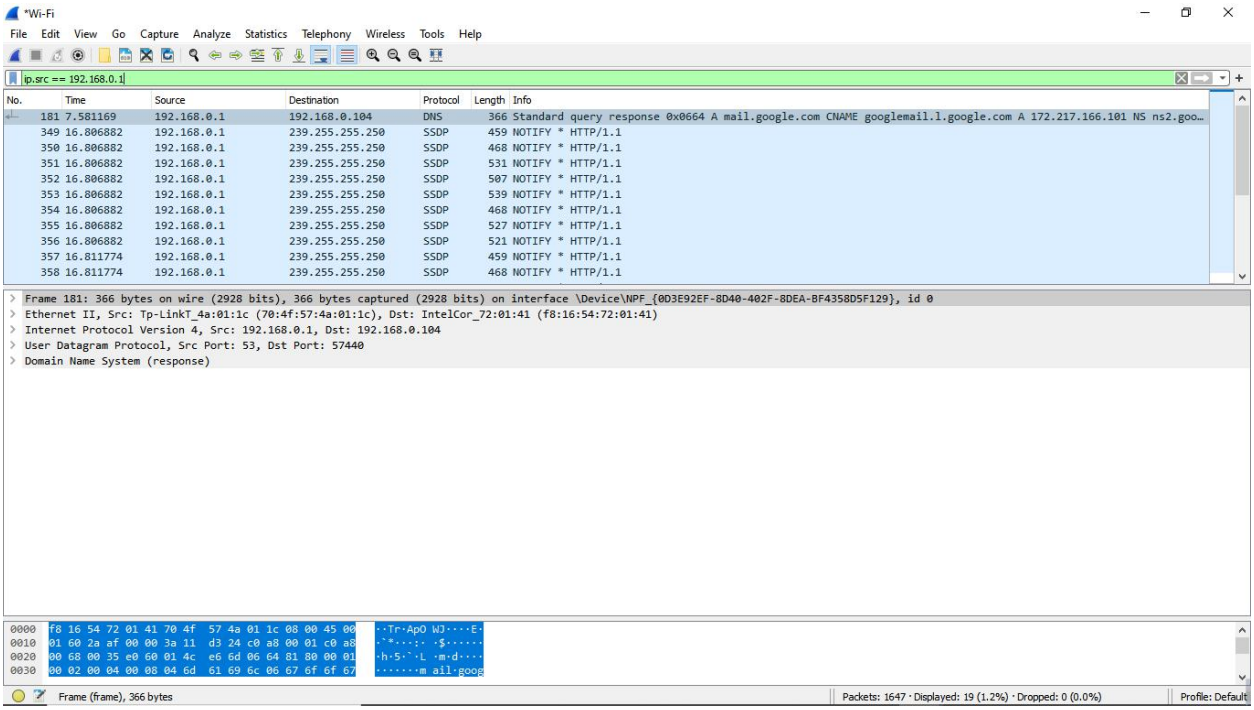

Figure 06: Source IP filter

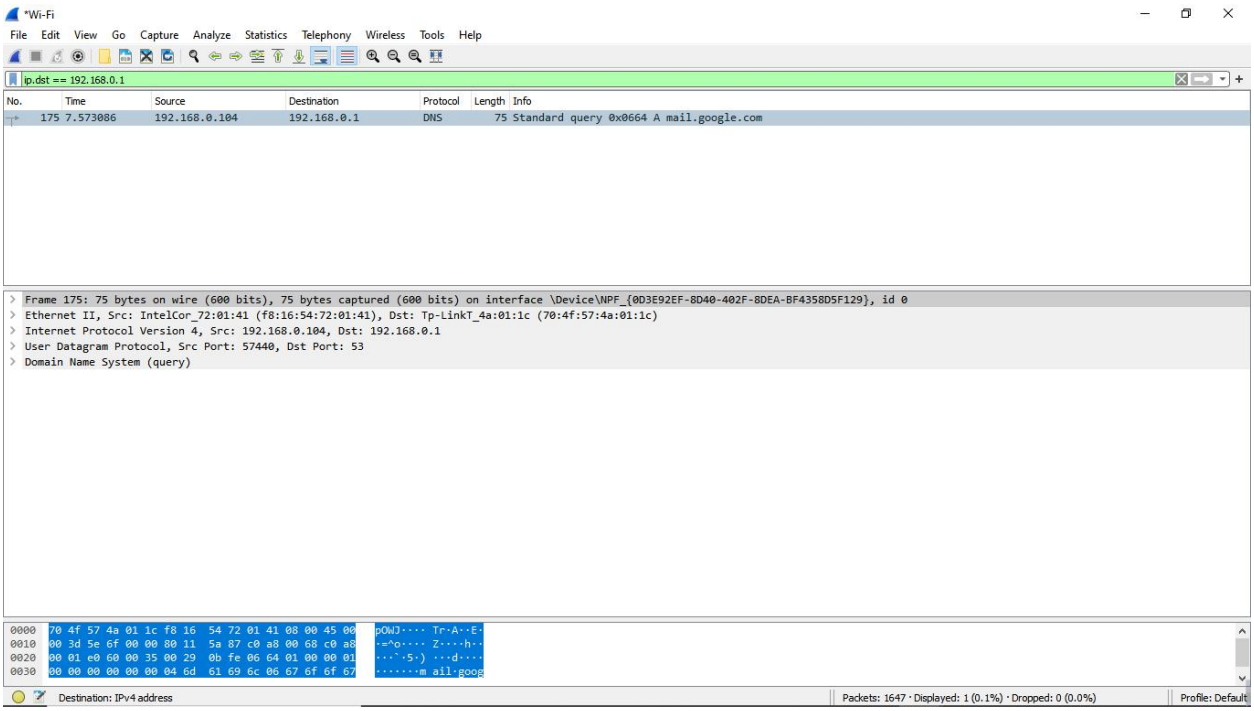

Figure 07: Destination IP filter

• Packets and protocols can be analyzed after capture

• Individual fields in protocols can be easily seen

• Graphs and flow diagrams can be helpful in analysis

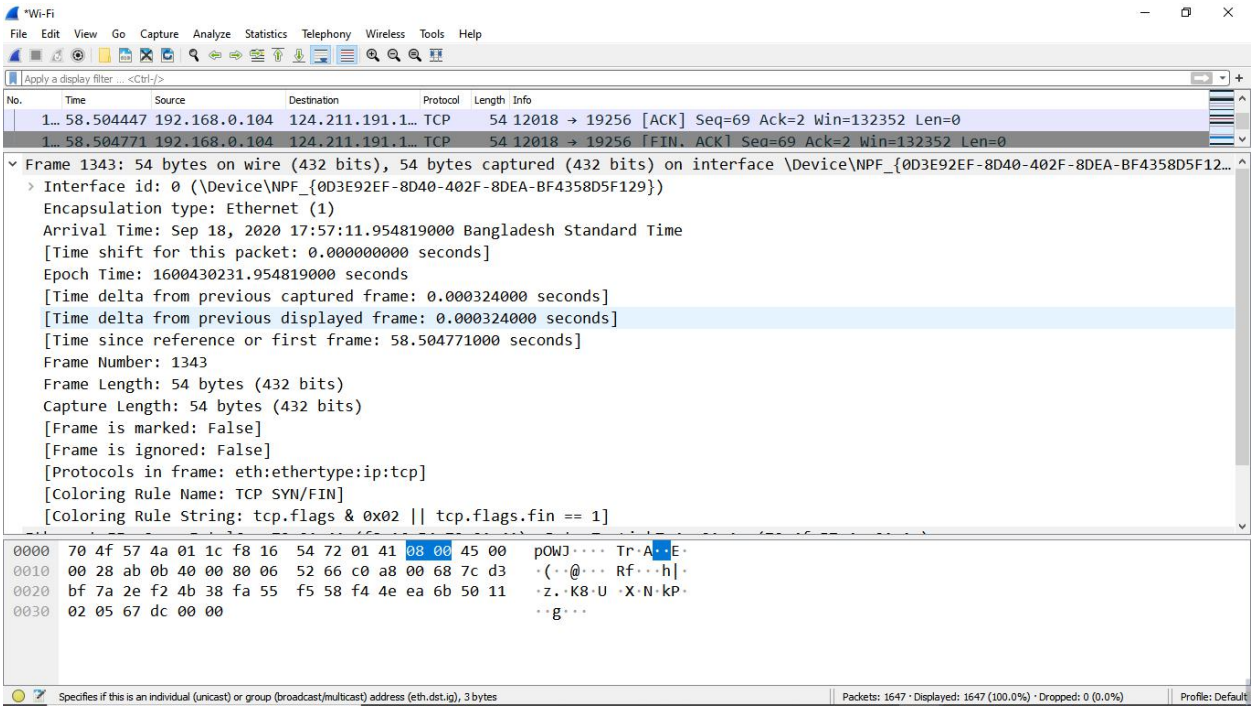

Figure 08: Packet Details Pane(Frame segment)

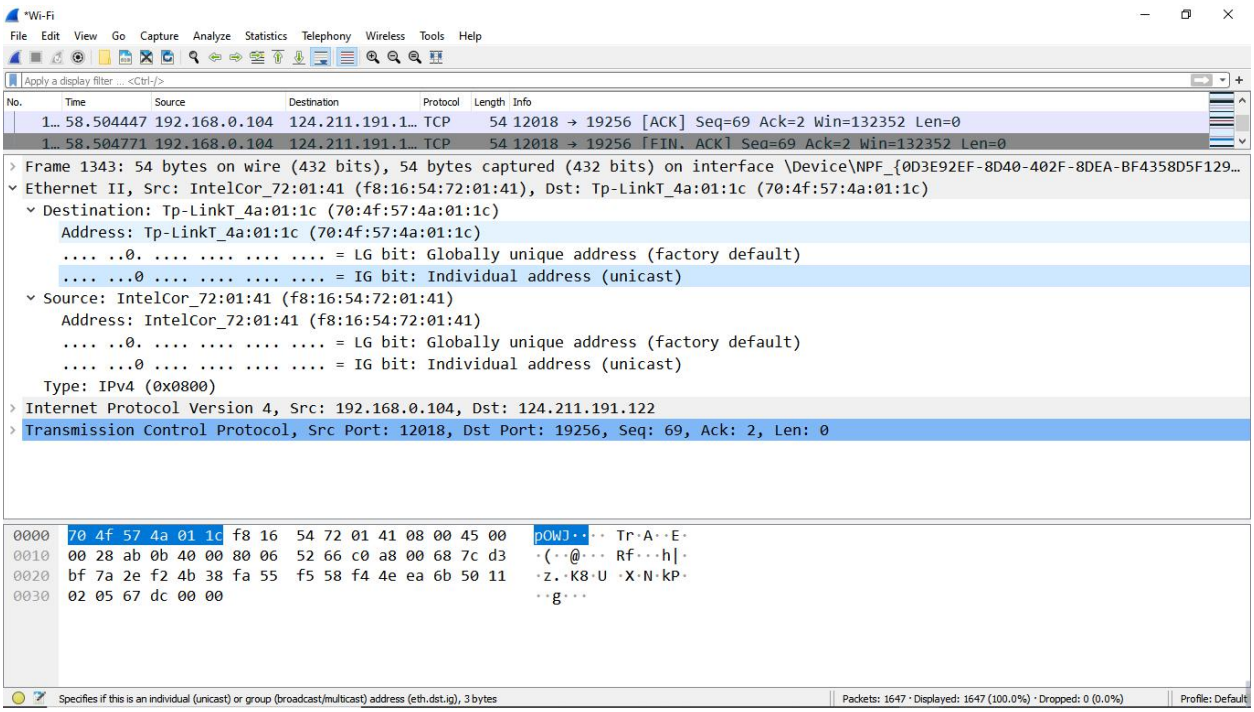

Figure 09: Packet Details Pane (Ethernet Segment)

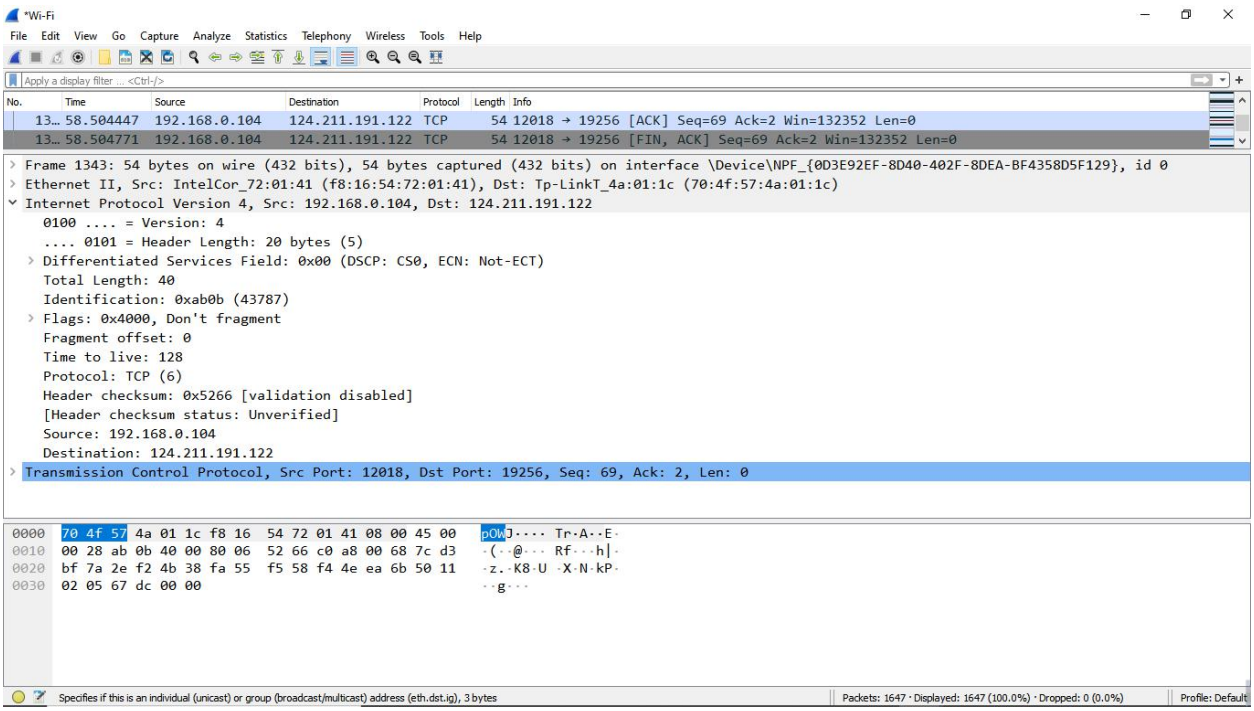

Figure 10: Packet Details Pane(IP segment)

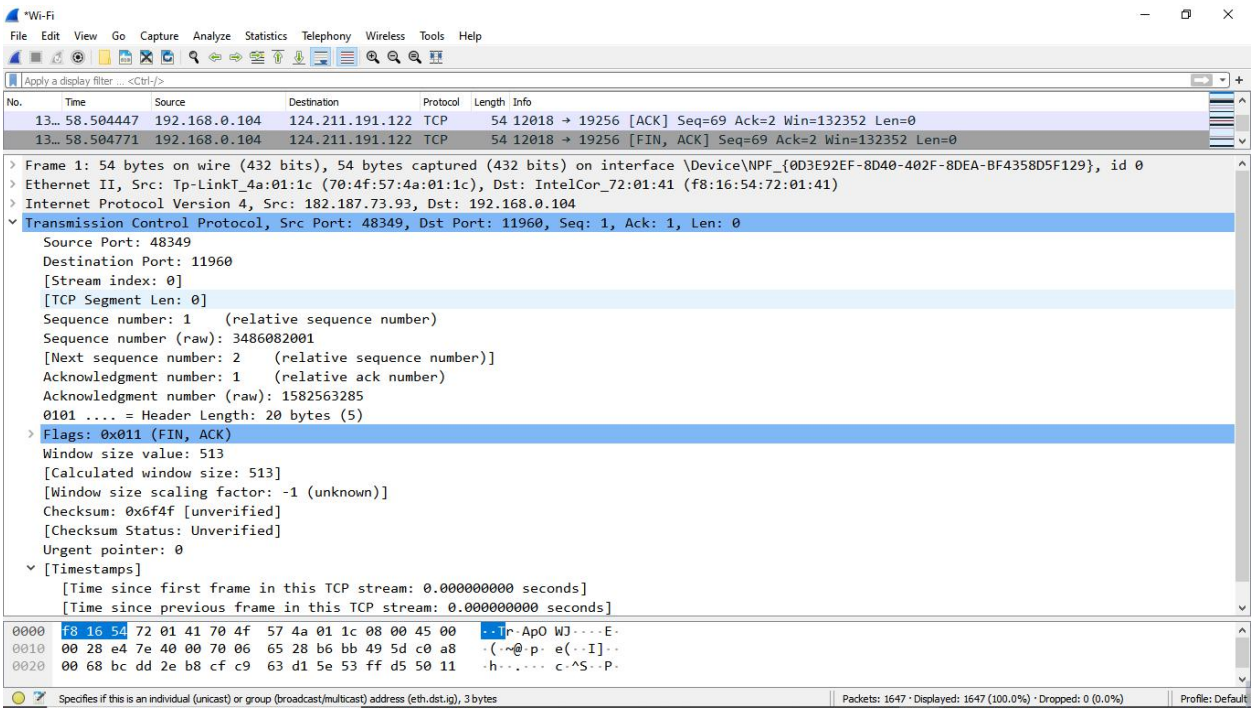

Figure 11: Packet Details Pane (TCP Segment)

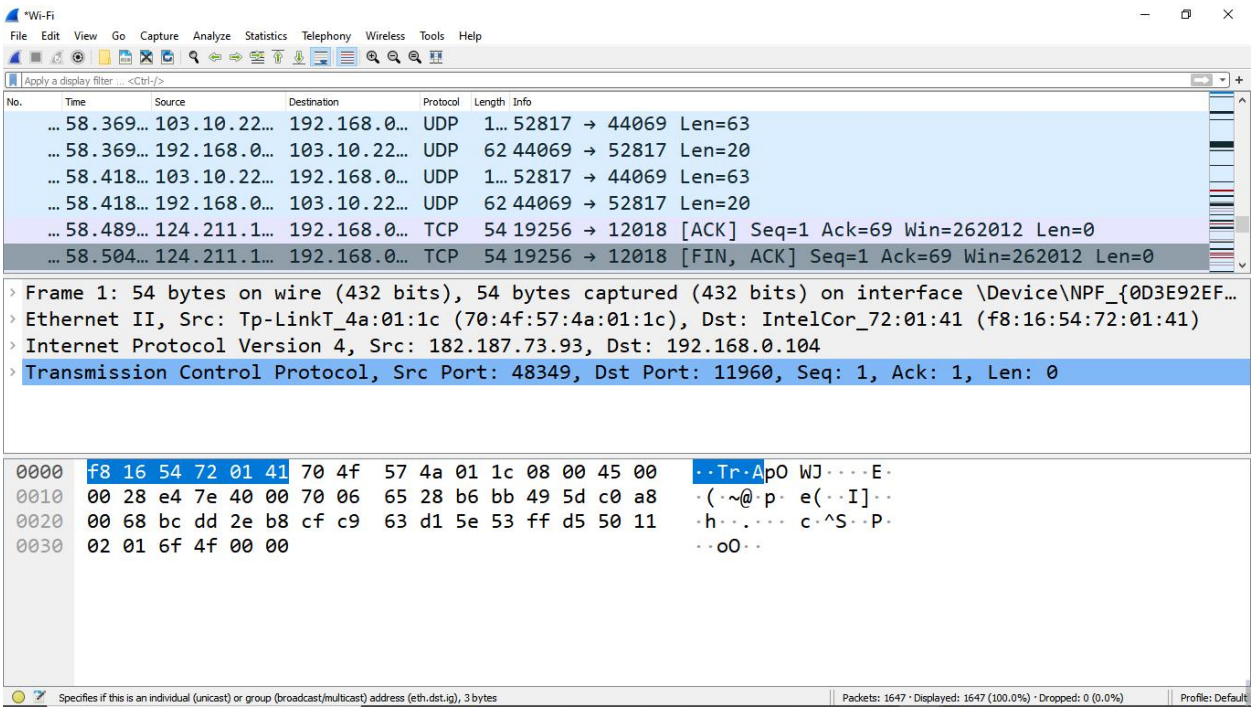

Figure 12: Packet Byte Pane

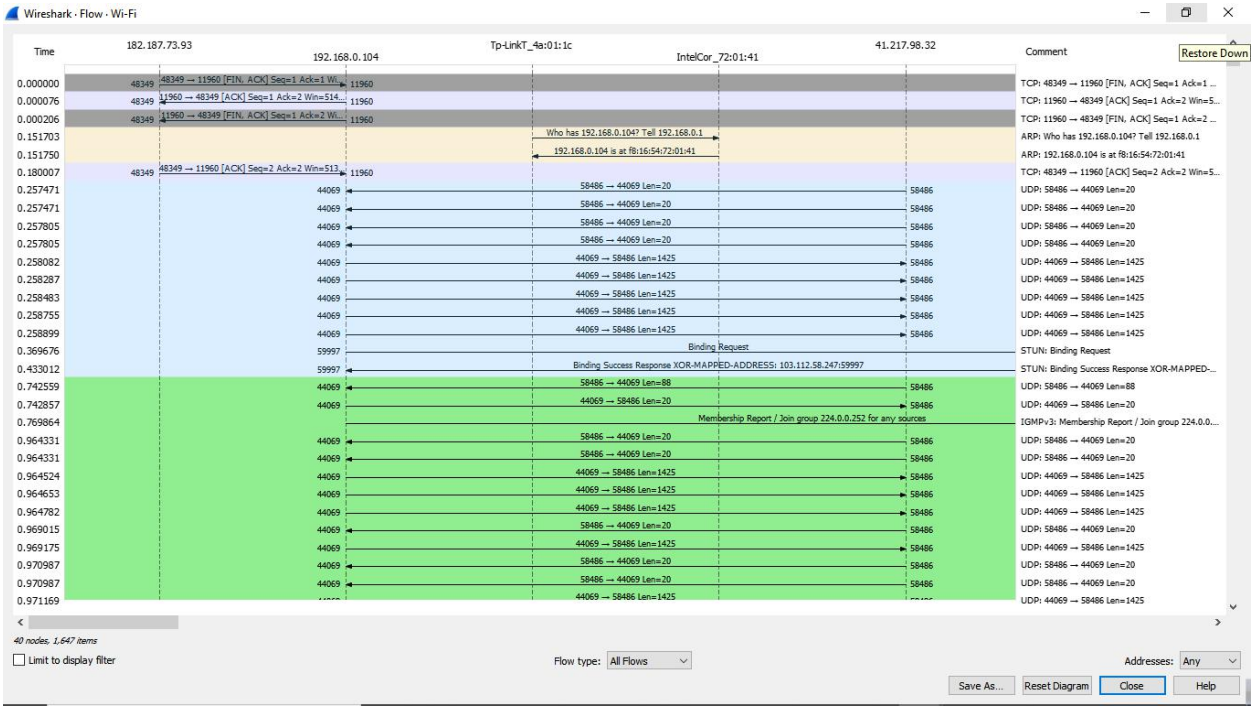

Figure 13: Statistics- Flow Graph(All Flows)

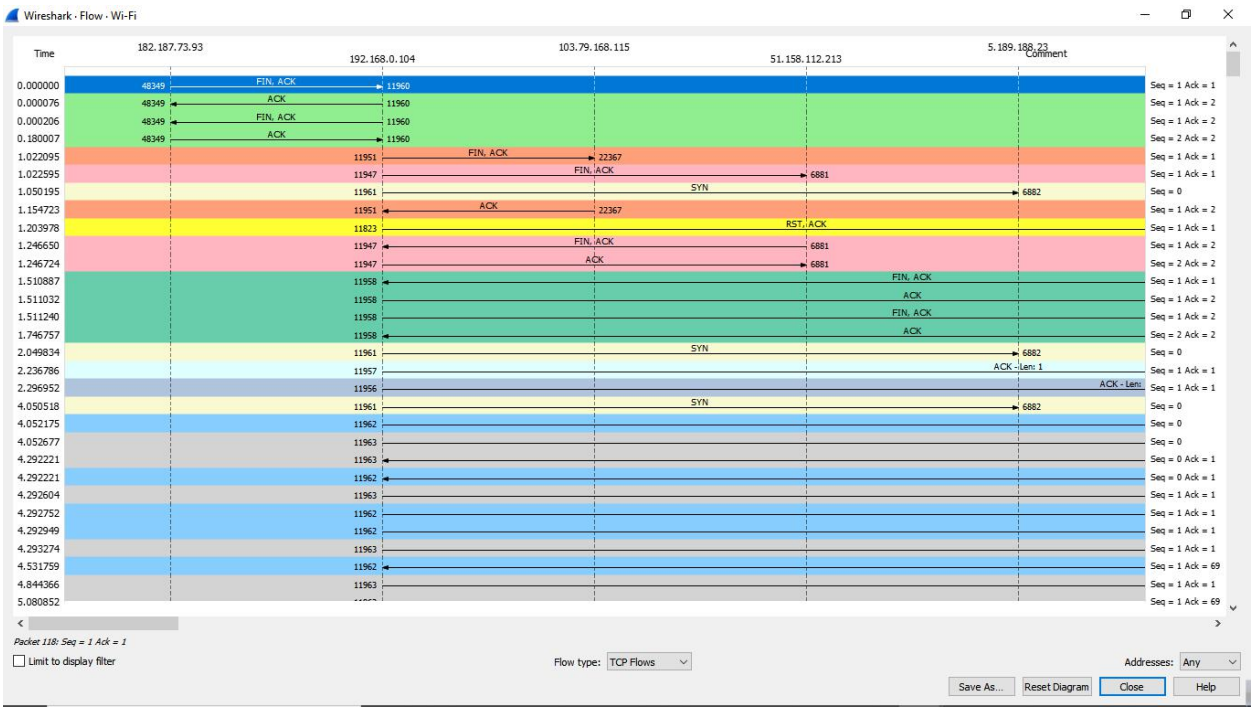

Figure 13: Statistics- Flow Graph(TCP Flows)

Conclusion:

By using Wireshark we can perform the following actions-
Capture live packet data from a network interface, Display packets with very detailed protocol information, Filter packets on many criteria, Search for packets on many criteria, Colorize packet display based on filters, Create various statistics.

So after downloading and installing Wireshark we can easily Capture live packet data from a network interface using Wireshark. We have applied filter to monitor particular traffic. The TCP Stream Throughput graph have shown us the throughput from one TCP stream, in one direction, based on the selected packet.