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: Naznin Sultana

ID:IT-16036

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment N0: 04

Experiment Name : Protocol Analysis with Wireshark

Objective :

At the end of this activity, we will be able to:

1. Define protocol analysis.
2. Capture protocols at each TCP/IP Layer.
3. Capture, and identify a TCP connection including handshake and tear down.
4. Identify a DNS request/response session.
5. Generate and record protocol hierarchy statistics for a session.

Defining protocol analysis:

Protocol analysis describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network.

Protocol analysis can help us understand network characteristics, learn who is on a network, determine who or what is utilizing available bandwidth, identify peak network usage times, identify possible attacks or malicious activity, and find unsecured and bloated applications.

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.

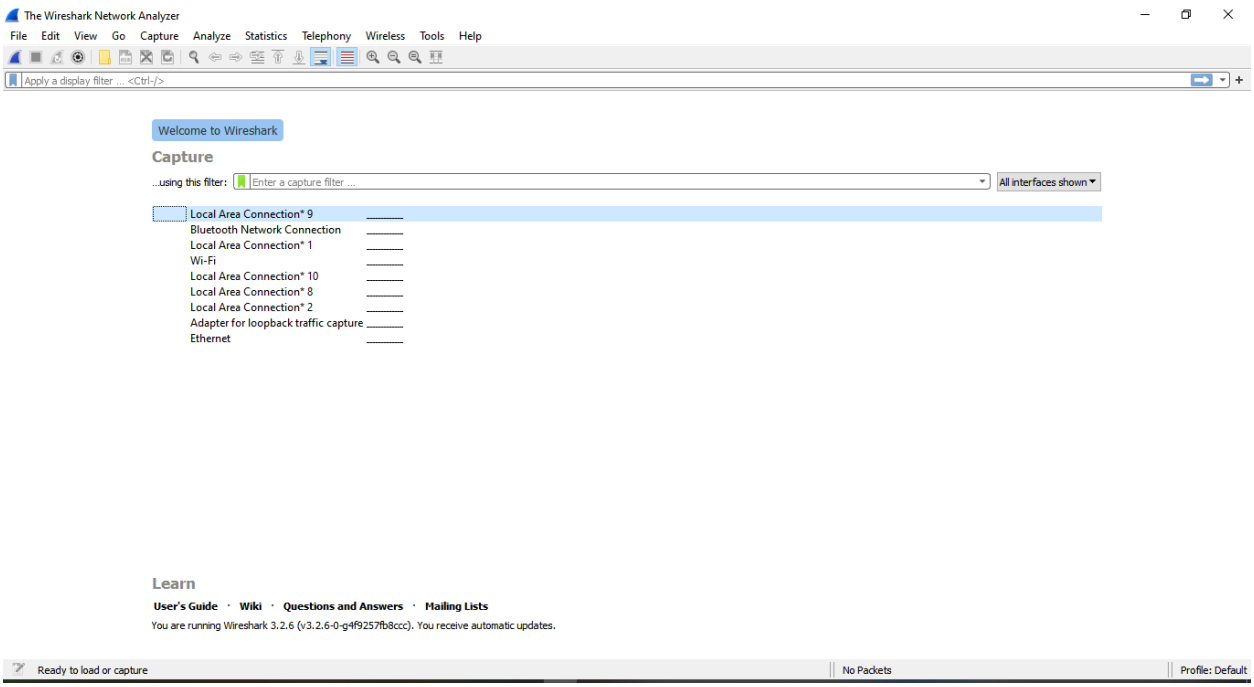

Figure 01: Wireshark Interface List

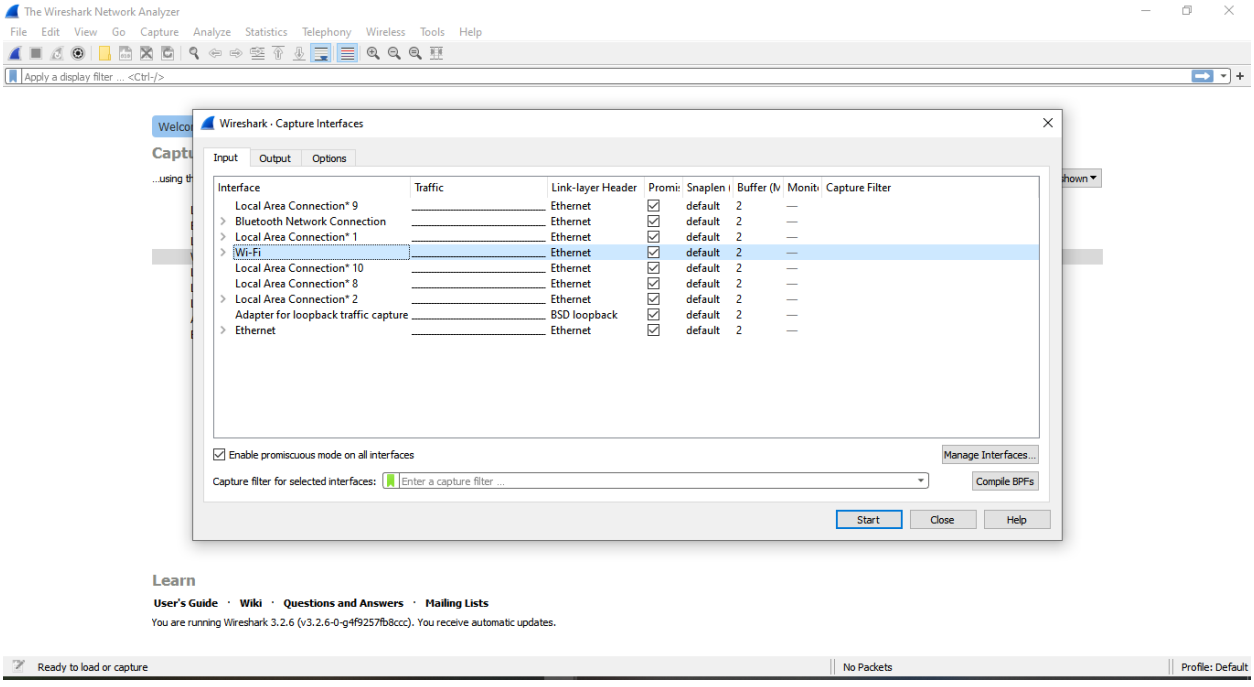

Figure 02: Start Capturing Interface that has IP address

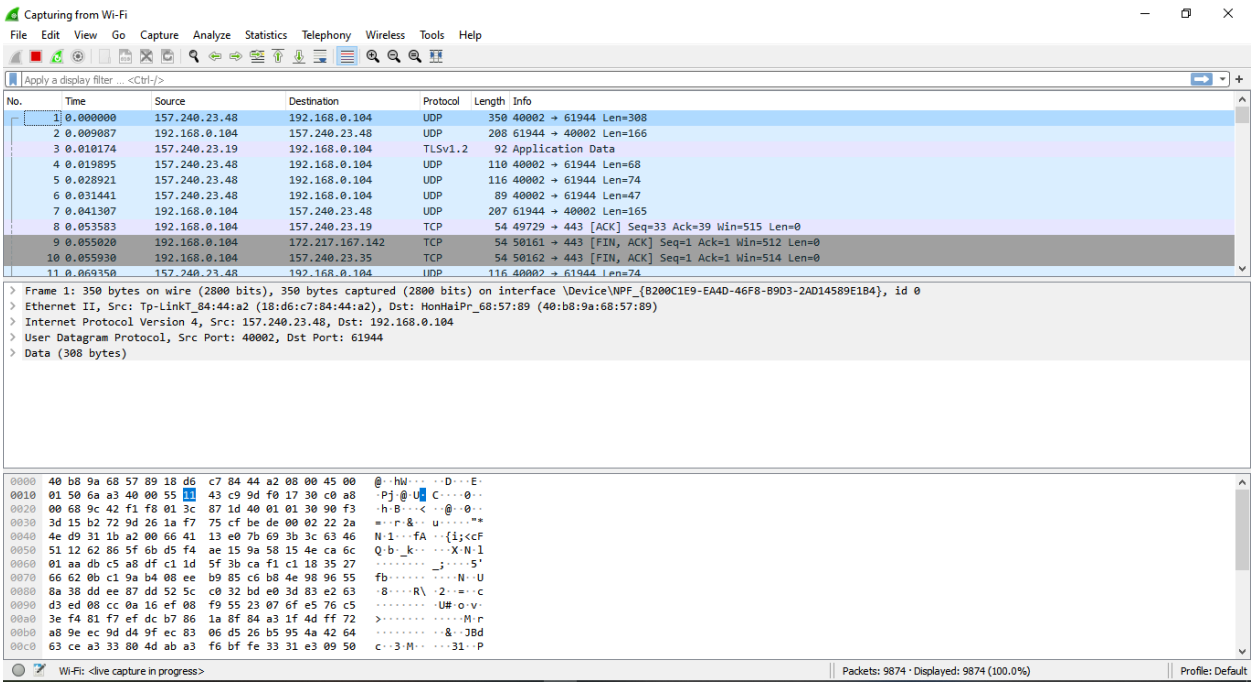

Figure 03: A sample packet capture window

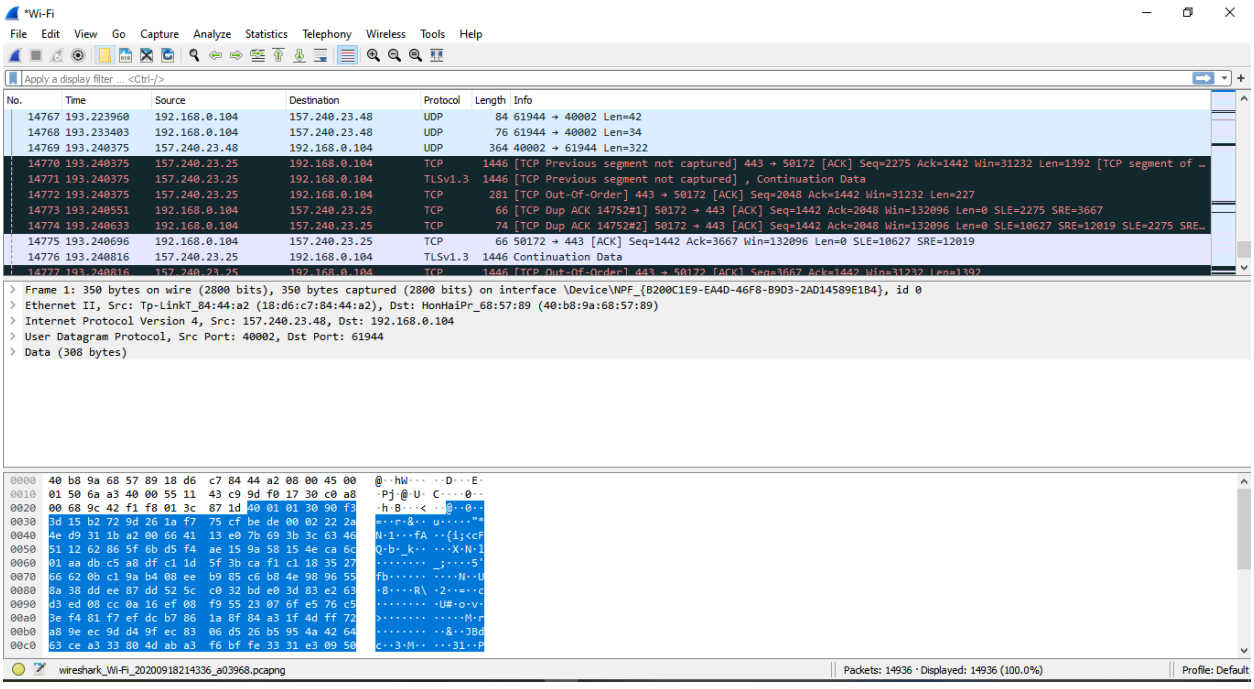

Figure 04: Stopping Capture

Filtering:

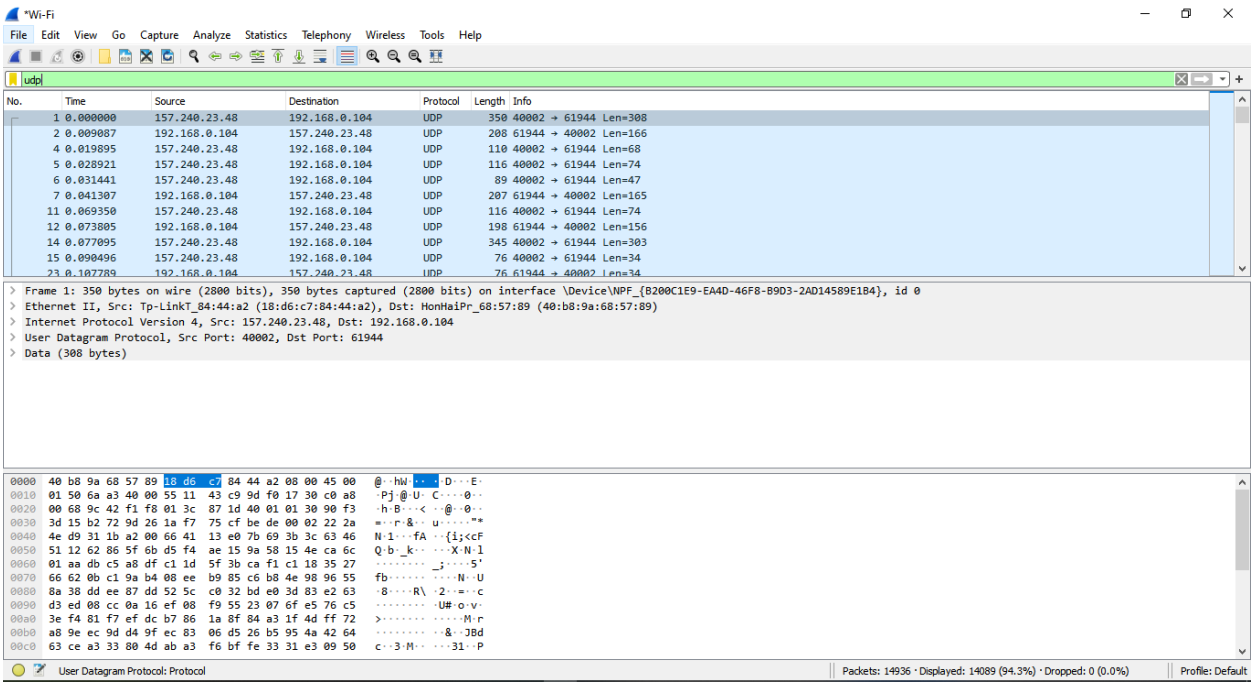

Figure 05: Filter by Protocol

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.

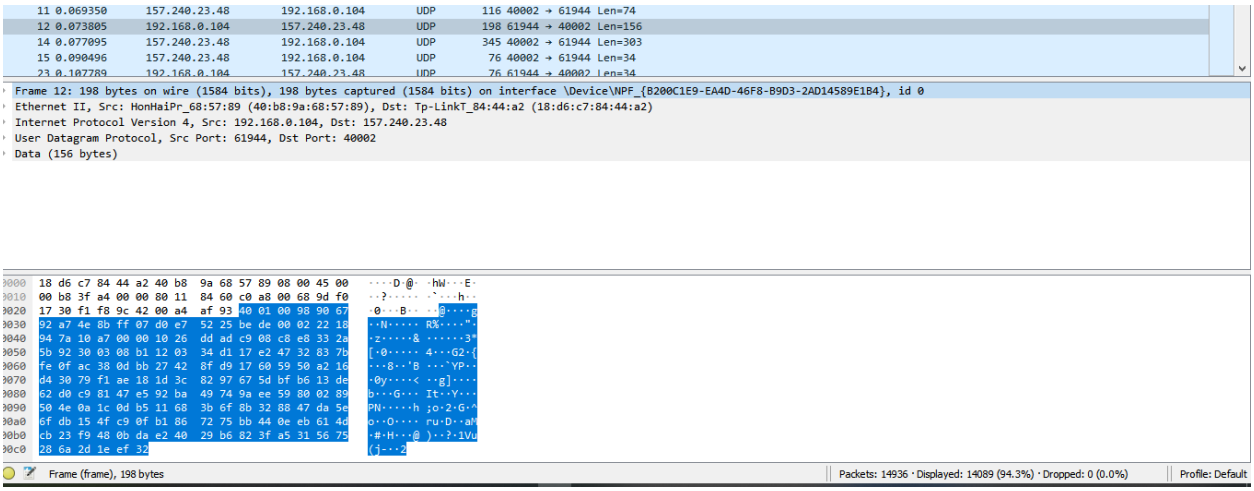

Figure 06: Packet Details Pane(Frame segment)

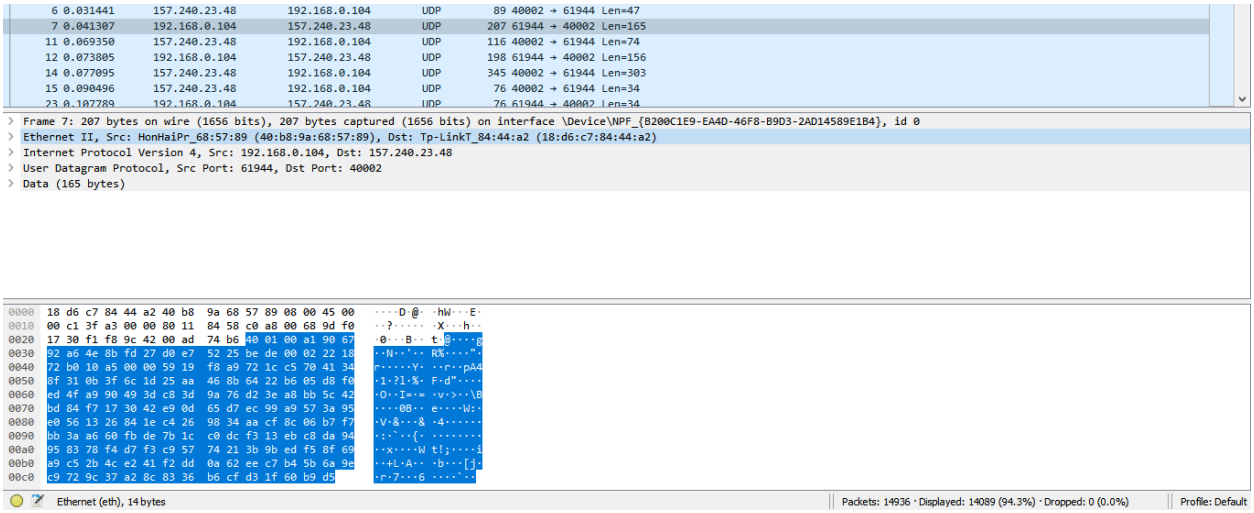

Figure 07: Packet Details Pane (Ethernet Segment)

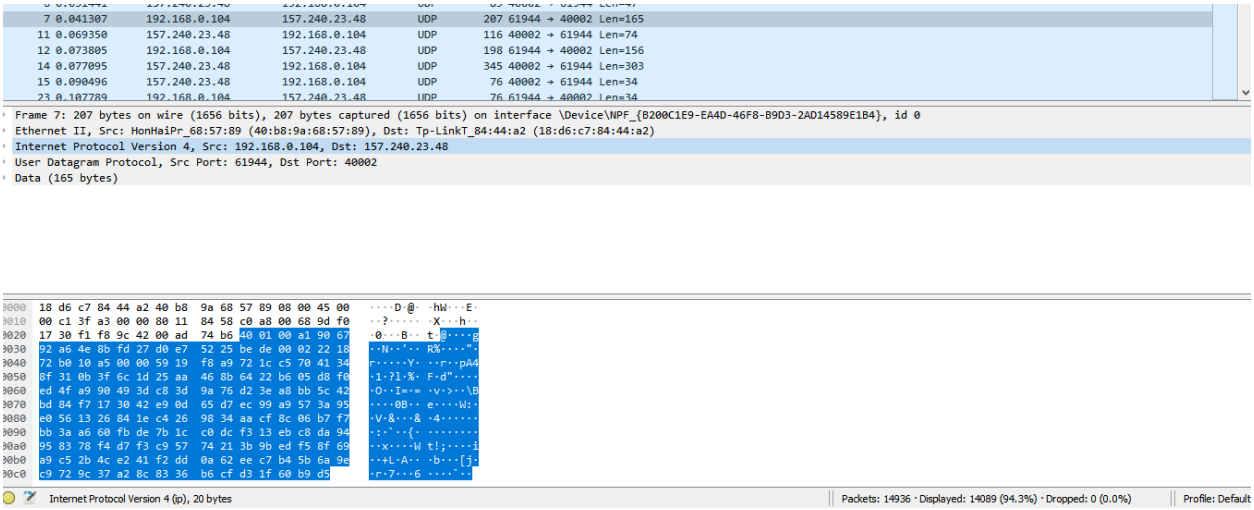

Figure 8: Packet Details Pane(IP segment)

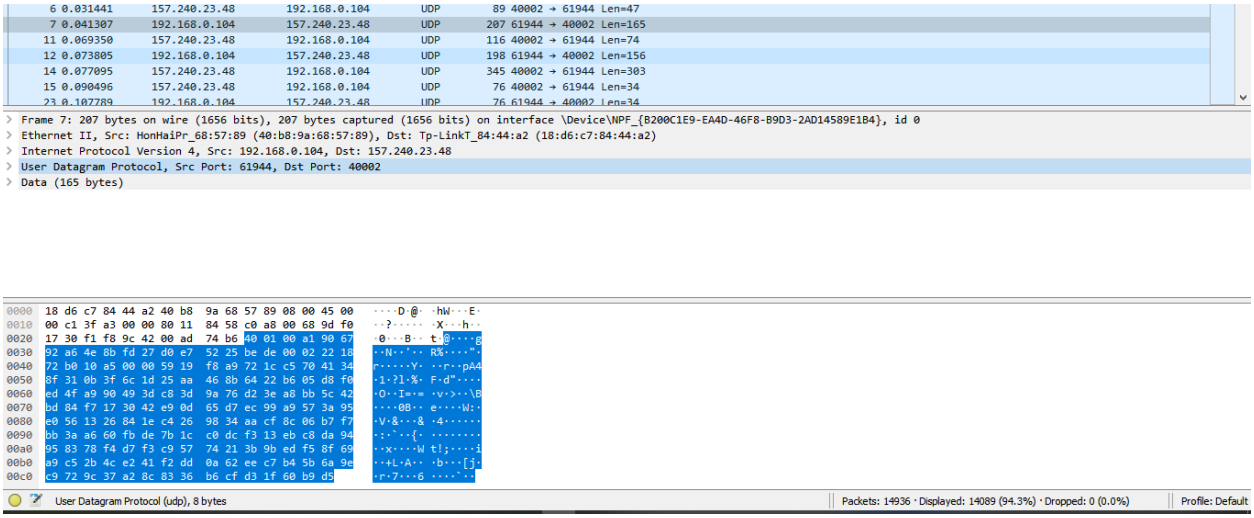

Figure 9: Packet Details Pane (TCP Segment)

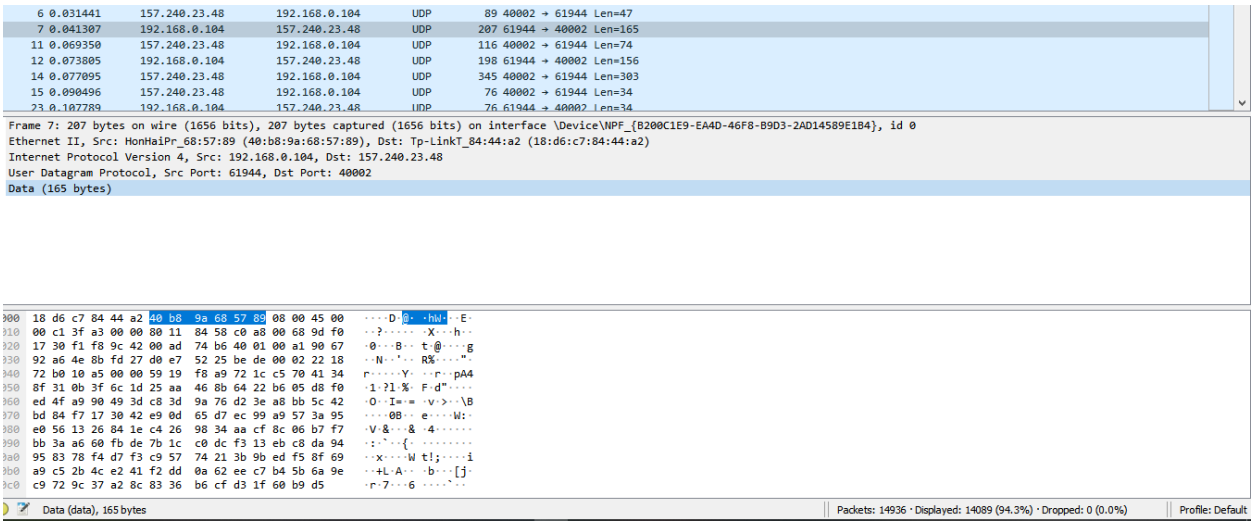

Figure 10: Packet Byte Pane

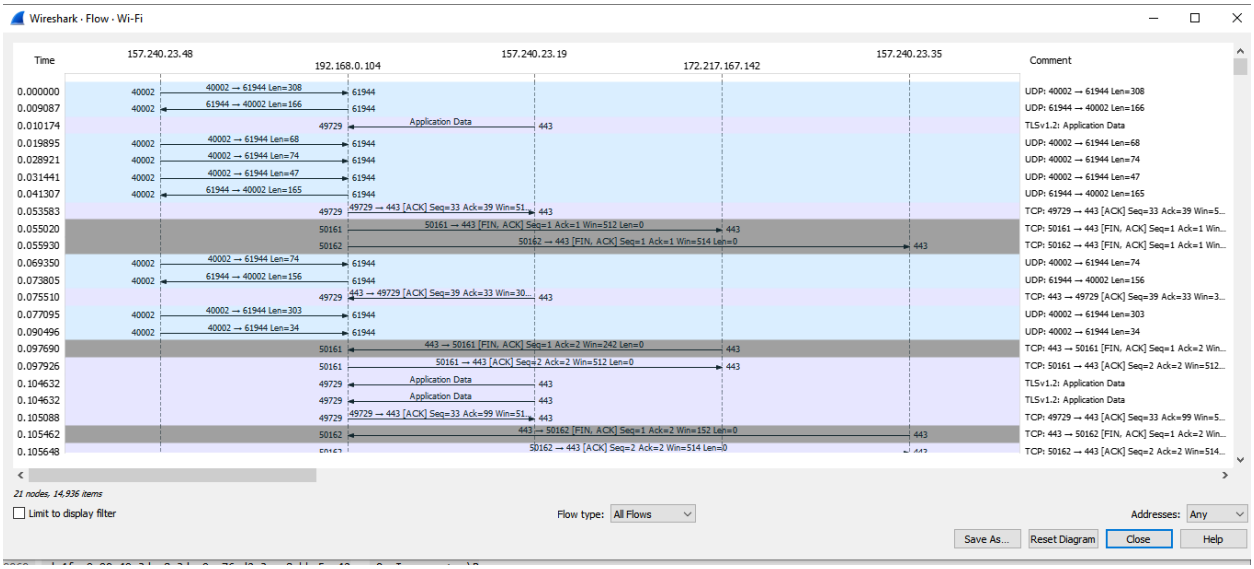

Figure 11: Statistics- Flow Graph(All Flows)

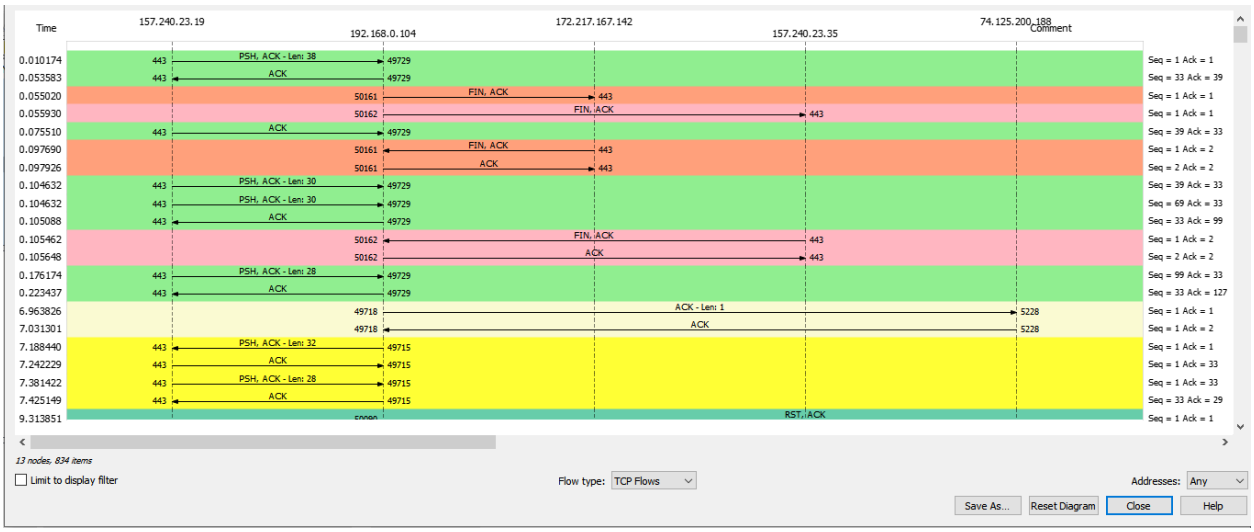

Figure 12: Statistics- Flow Graph(TCP Flows)

Conclusion: In this lab, We have applied filter to monitor particular traffic.The TCP Stream throughput graph helps us by giving the throughput from one TCP stream, in one direction, based on the selected packet.For this we first start captured data with wireshark. After that we indentify a tcp connection including handshake and also indentify a DNS request. At last we generate the protocol hierarchy statistics for this session. We have learned about protocol analysis with wireshark.