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: Jahid Tanvir
ID: IT-15041
4th Year 2nd Semester
Session: 2014-15/2015-16
Dept. of ICT
MBSTU.

Submitted To

Nazrul Islam
Assistant Professor
Dept. of ICT
MBSTU.

Experiment No: 04

Experiment Name: Protocol Analysis with Wireshark

Objectives:

1. Live packet data capturing from a network interface.
2. Have to display packets with very detailed protocol information.
3. Filter packets on many criteria.
4. Search for packets on many criteria.
5. Colorize packet display based on filters.
6. Create various statistics.

Capture the Packets:

If we click any menu option, then it will show the available interfaces list. After clicking the menu, 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.

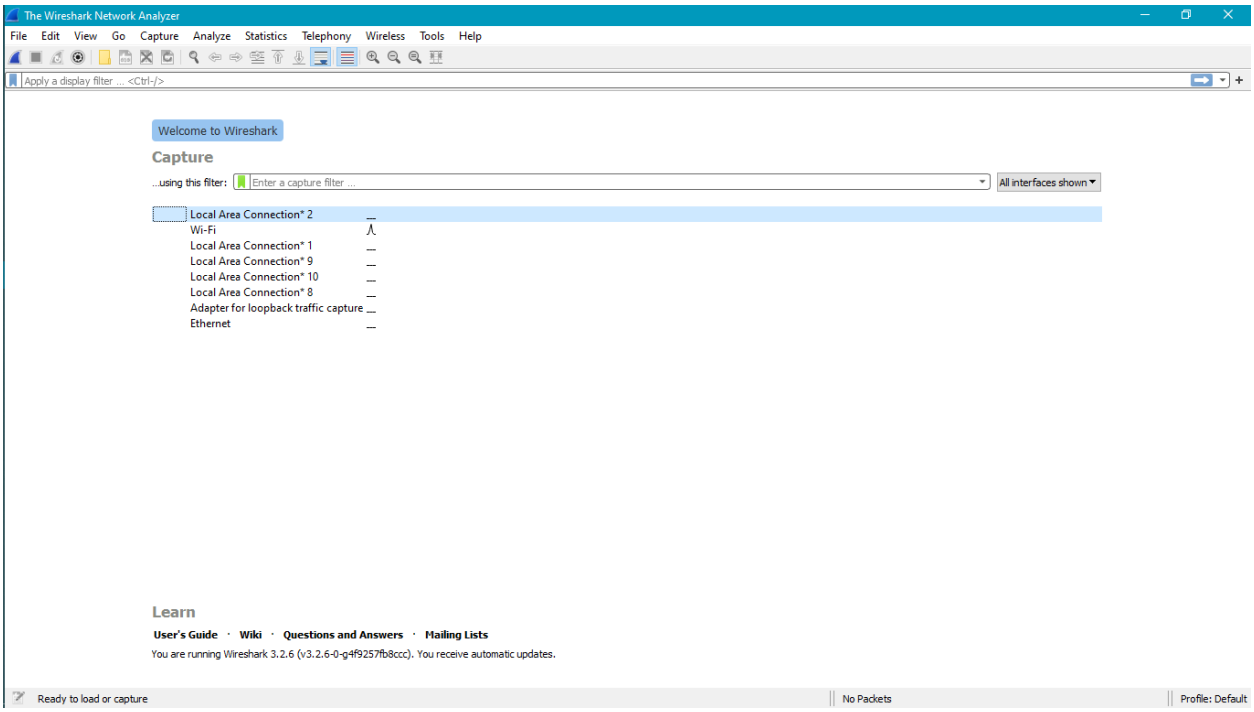

Fig-1: Wireshark interface (List of connections)

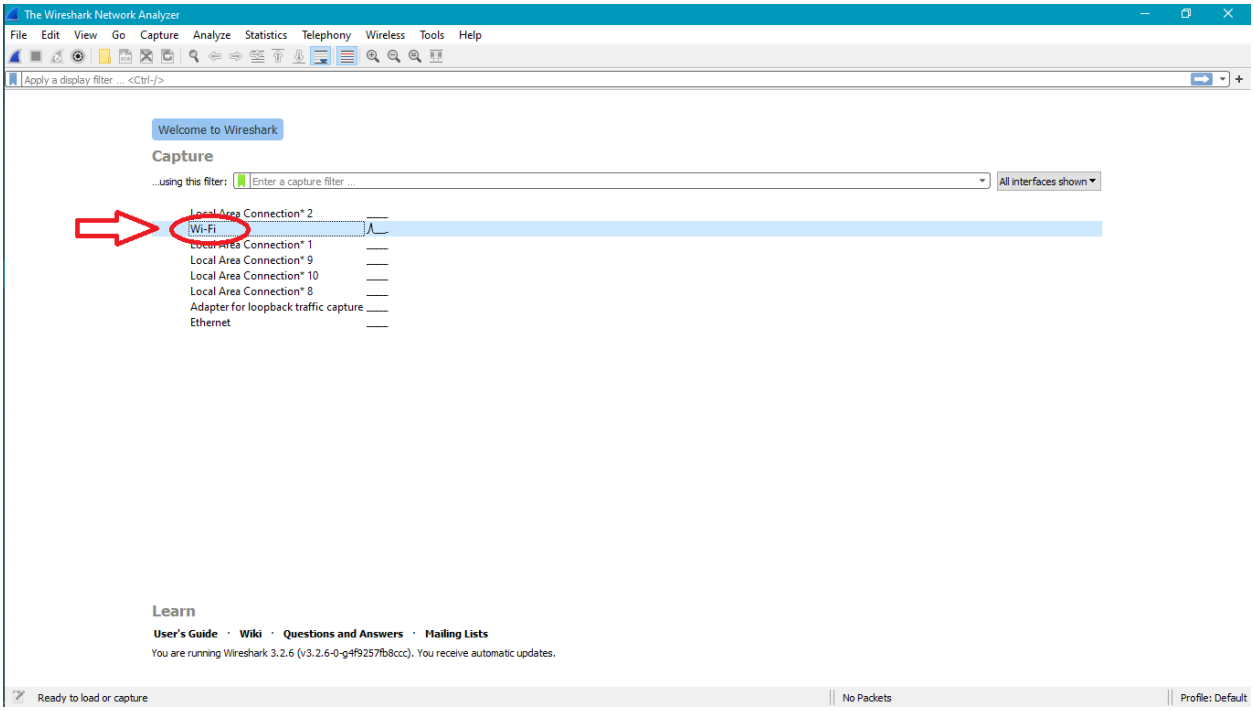

Fig-2: Start capturing interface that has IP address (WiFi)

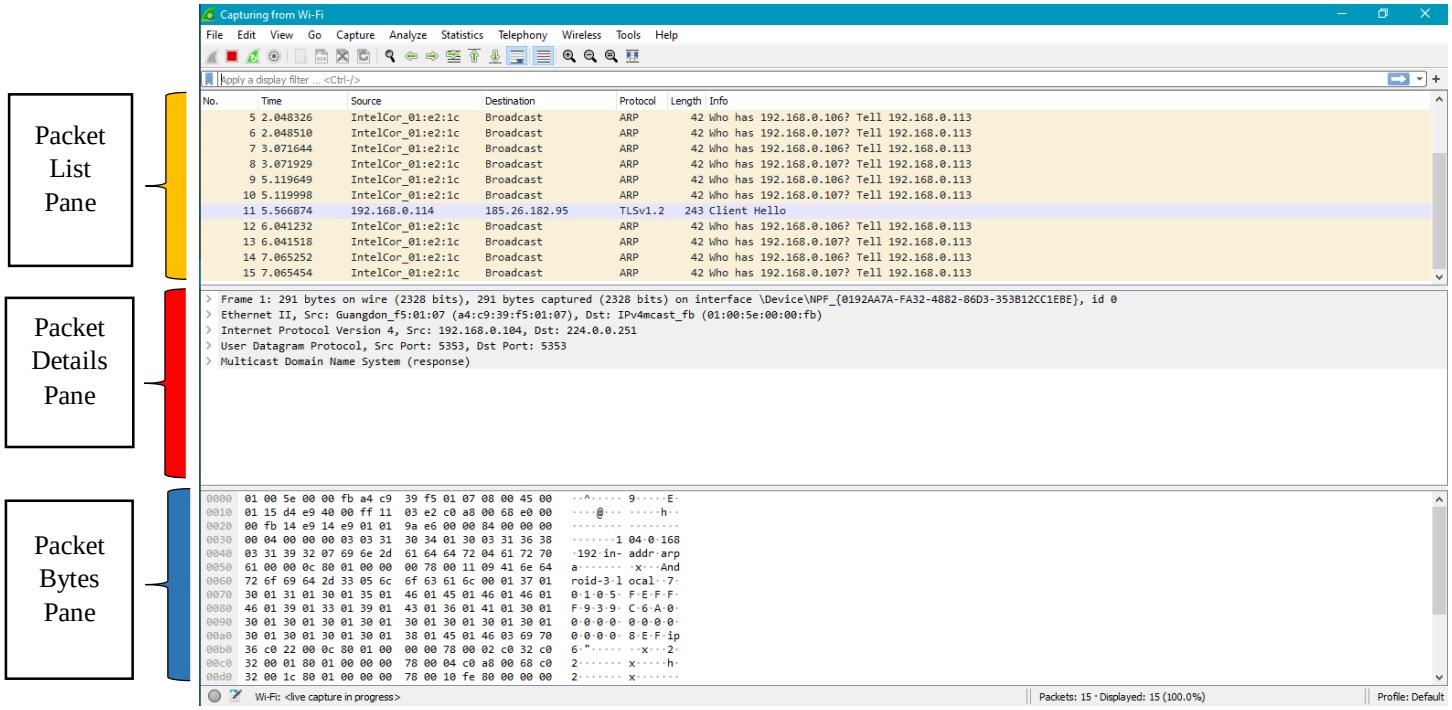

Fig-3: Sample packet capture window

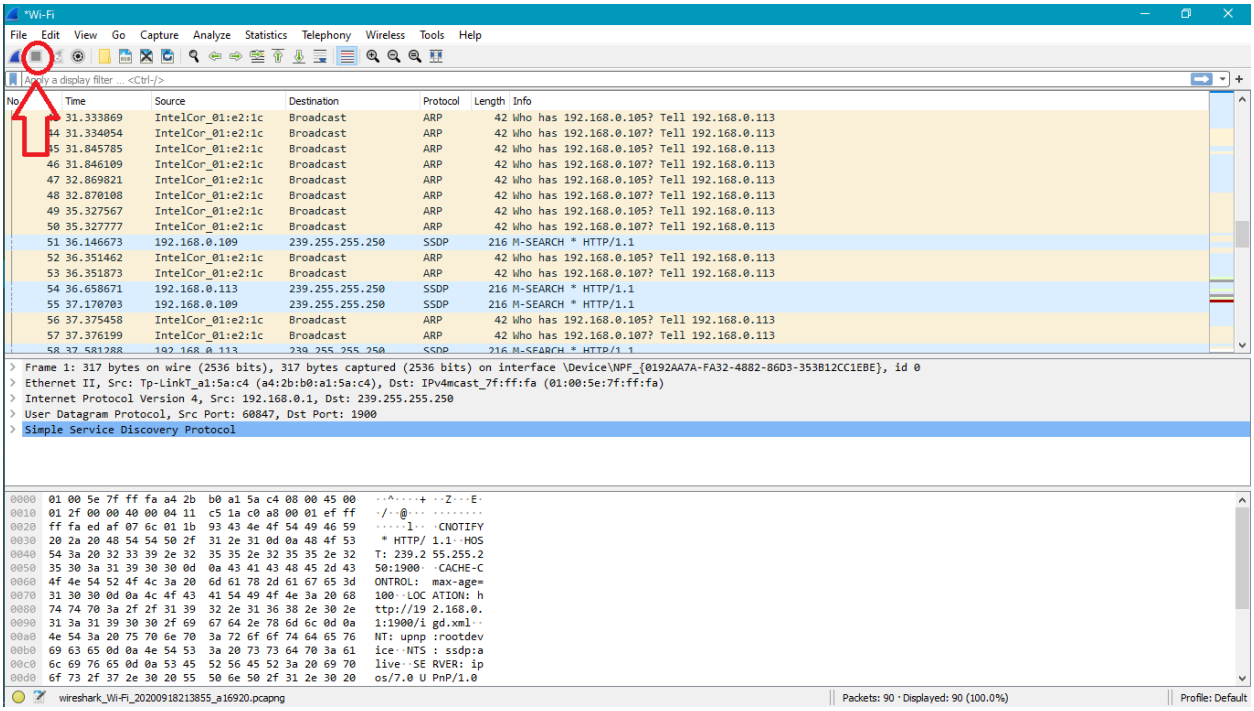

Fig-4: Stopping capturing

Filtering:

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.

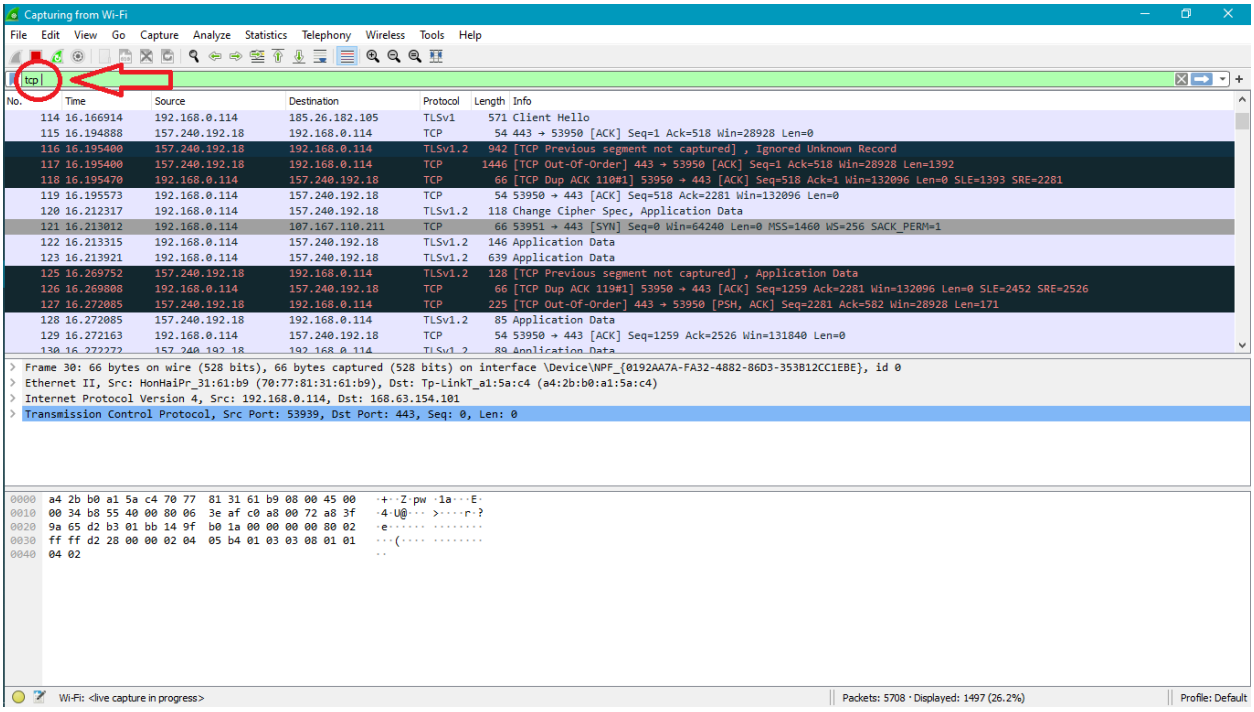

Fig-5: Filtering by Protocols (TCP/UDP)

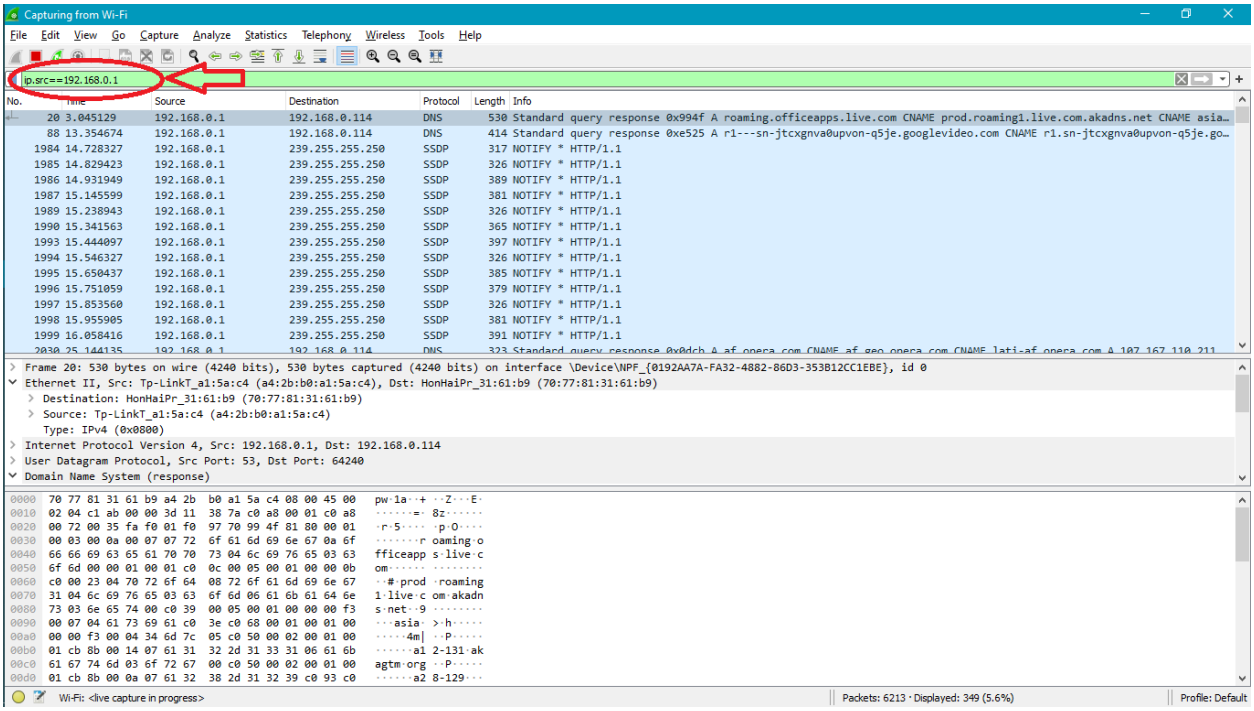

Fig-6: Source IP filtering

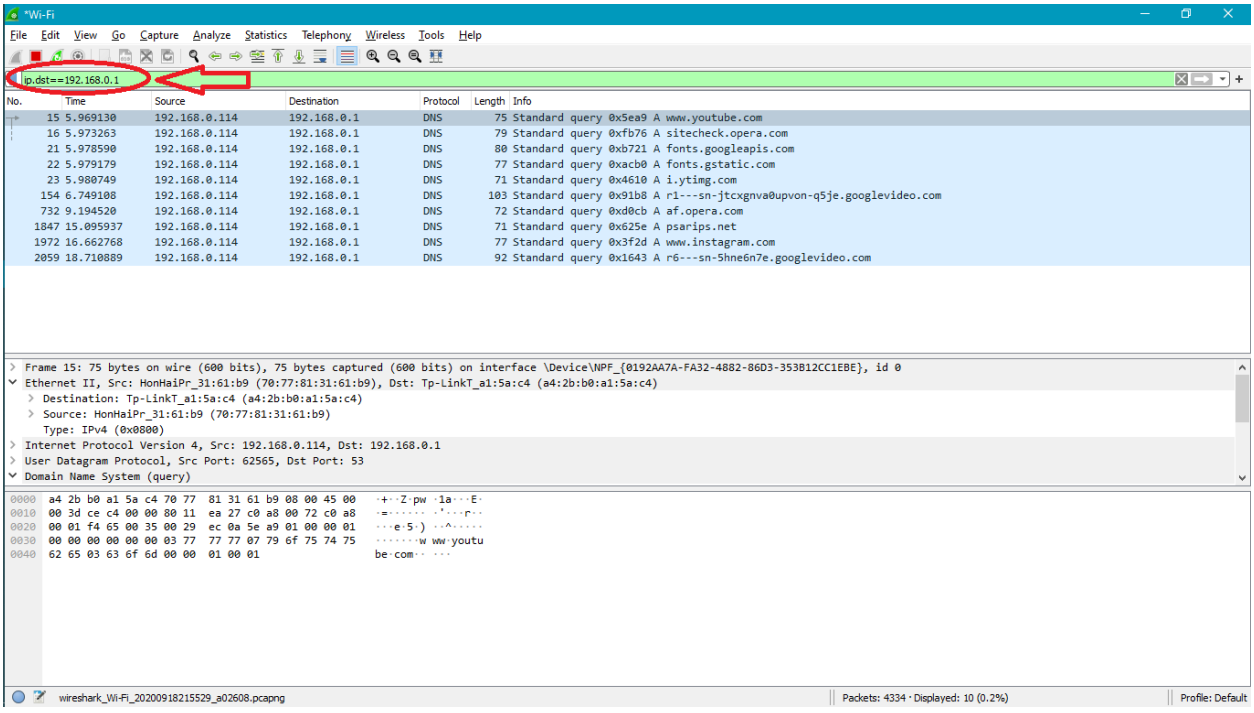

Fig-7: Destination IP filtering

Analyzing:

- 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

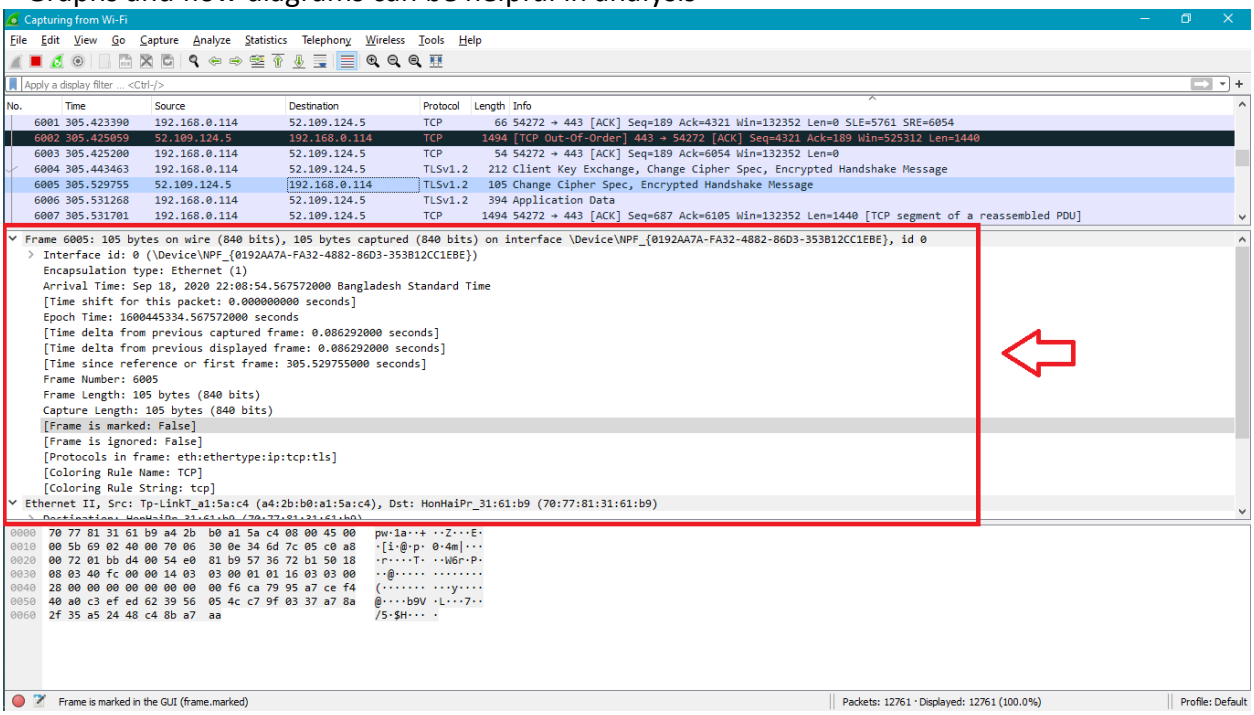

Fig-8: Packet Details Pane (Frame segment)

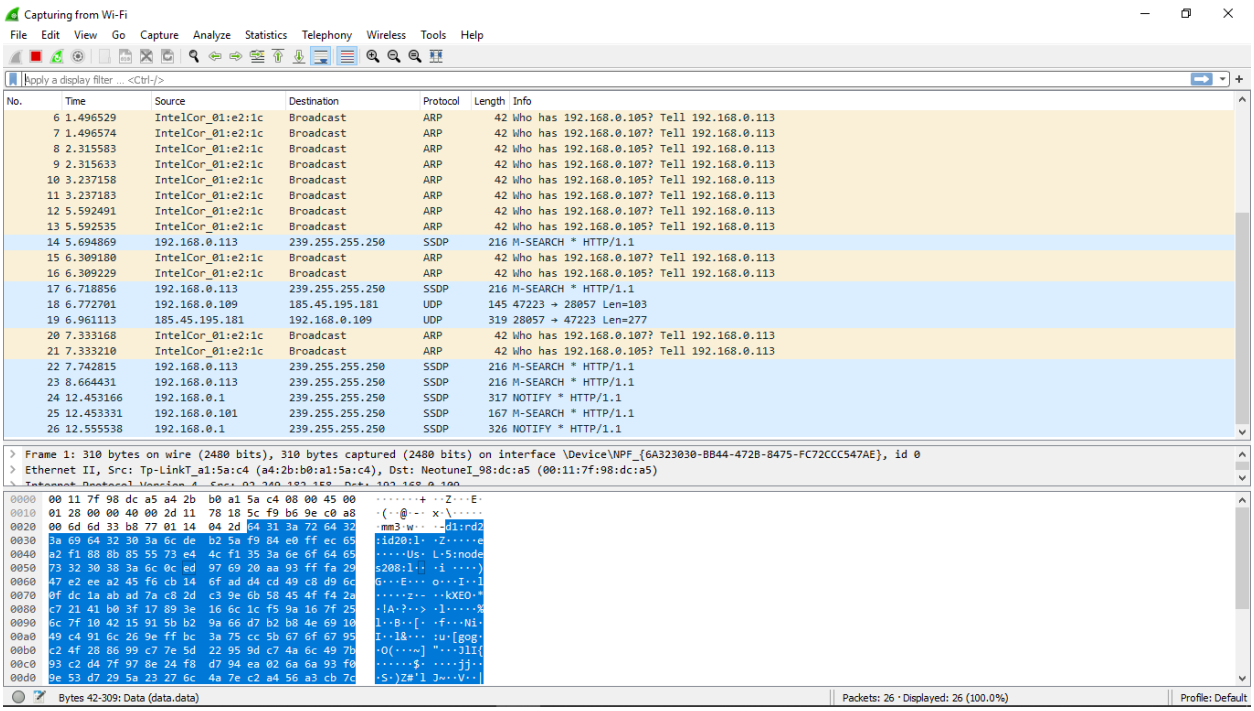

Fig-9: Packet Details Pane (Ethernet Segment)

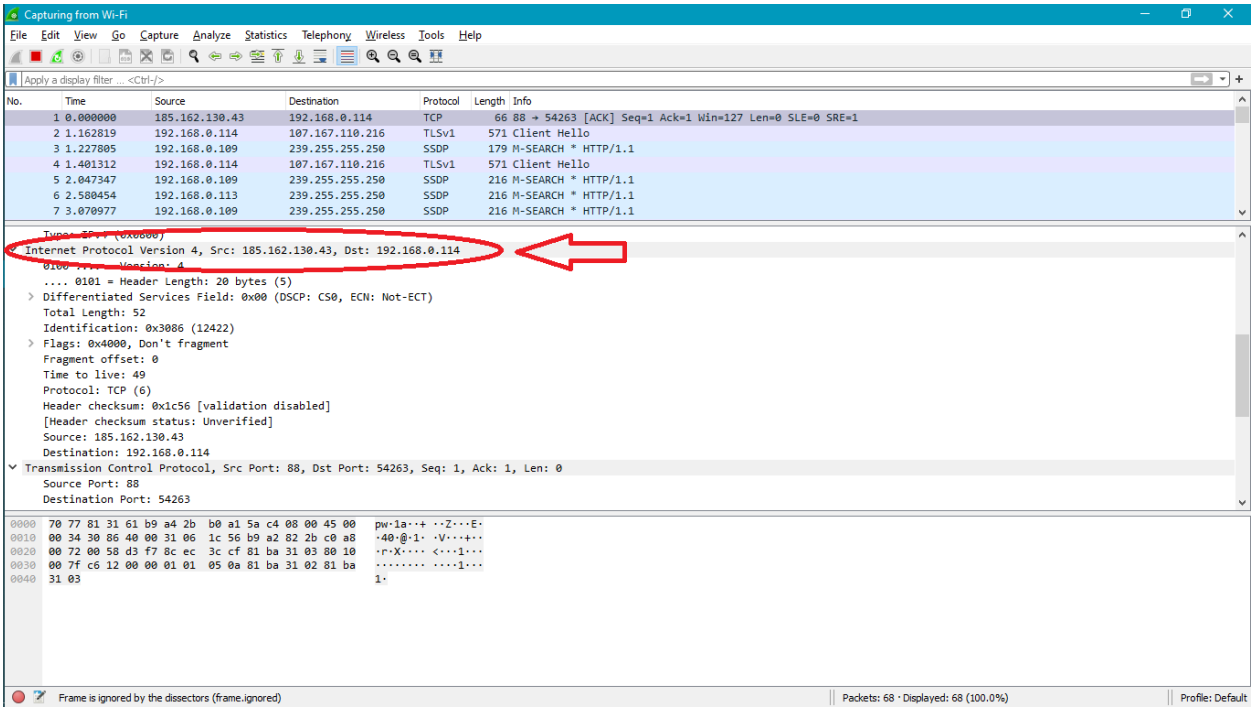

Fig-10: Packet Details Pane (IP segment)

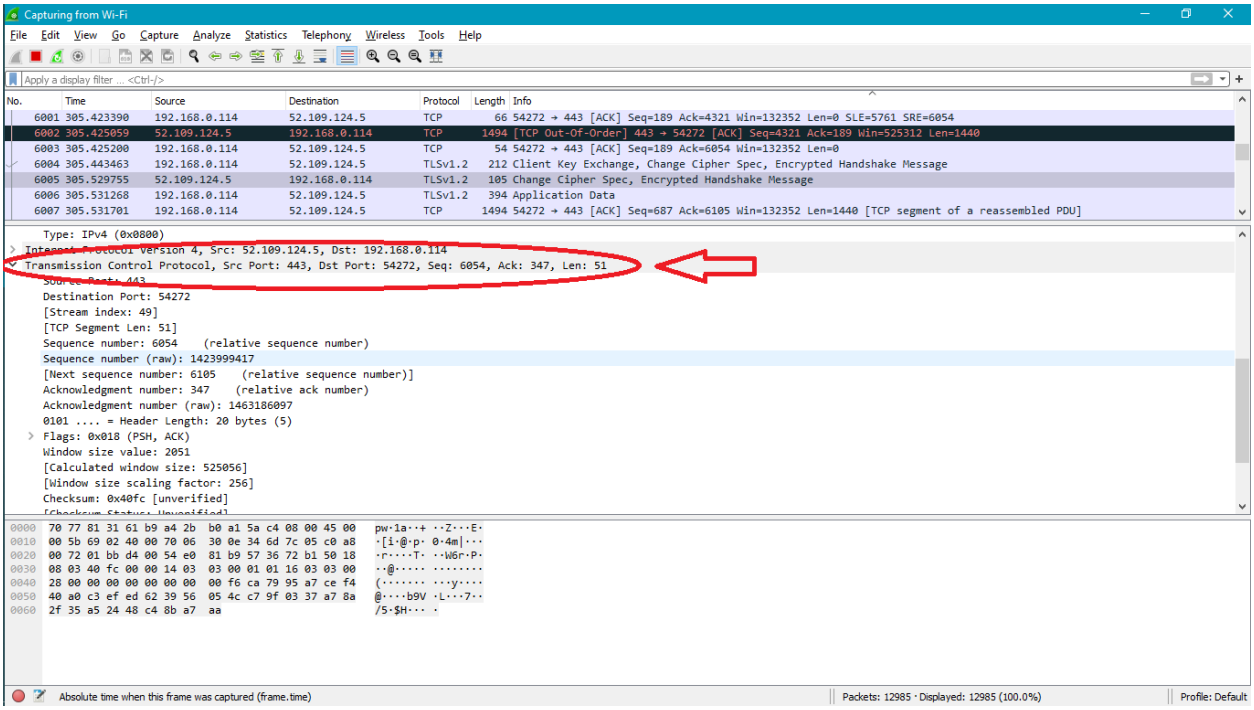

Fig-11: Packet Details Pane (TCP Segment)

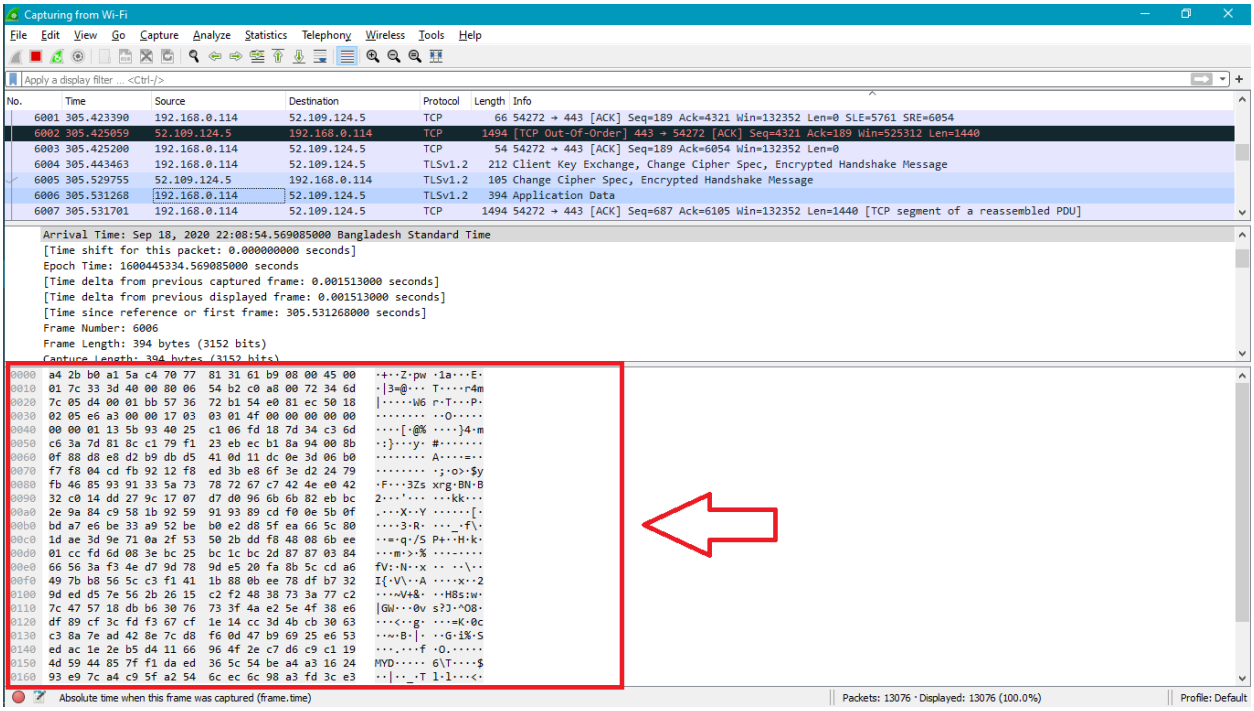

Fig-12: Packet Byte Pane

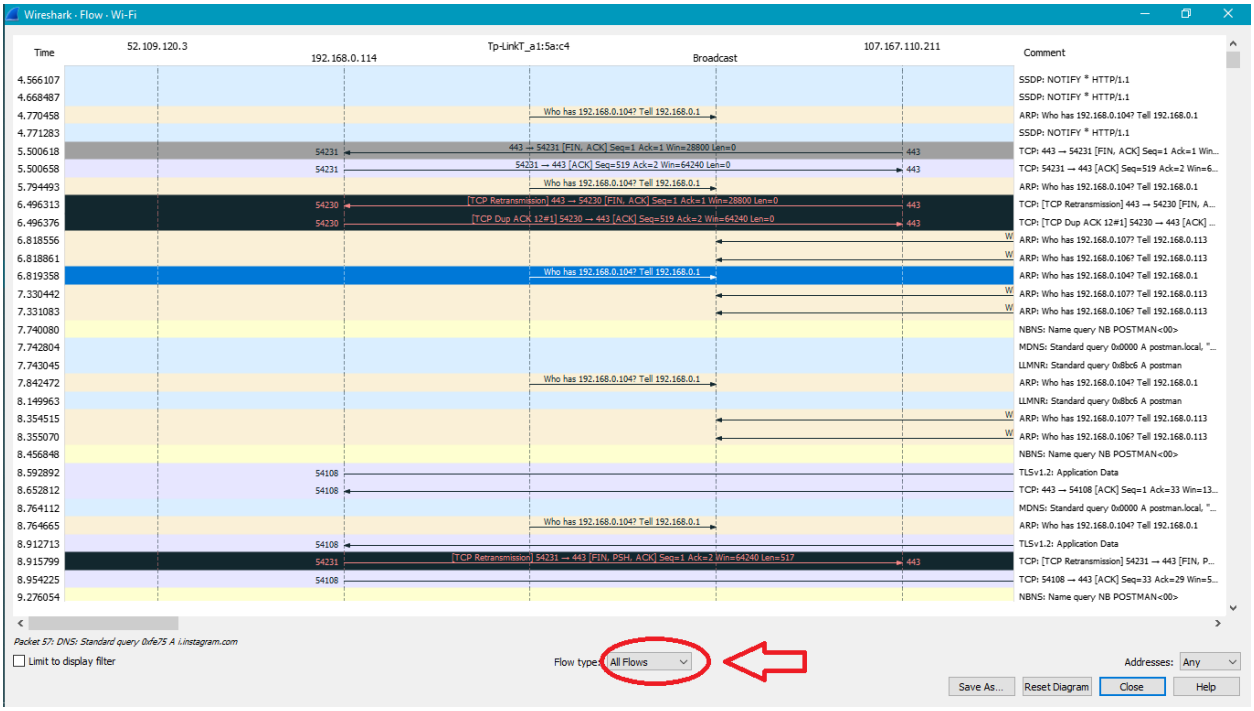

Fig-13: Statistics-Flow Graph: All Flows

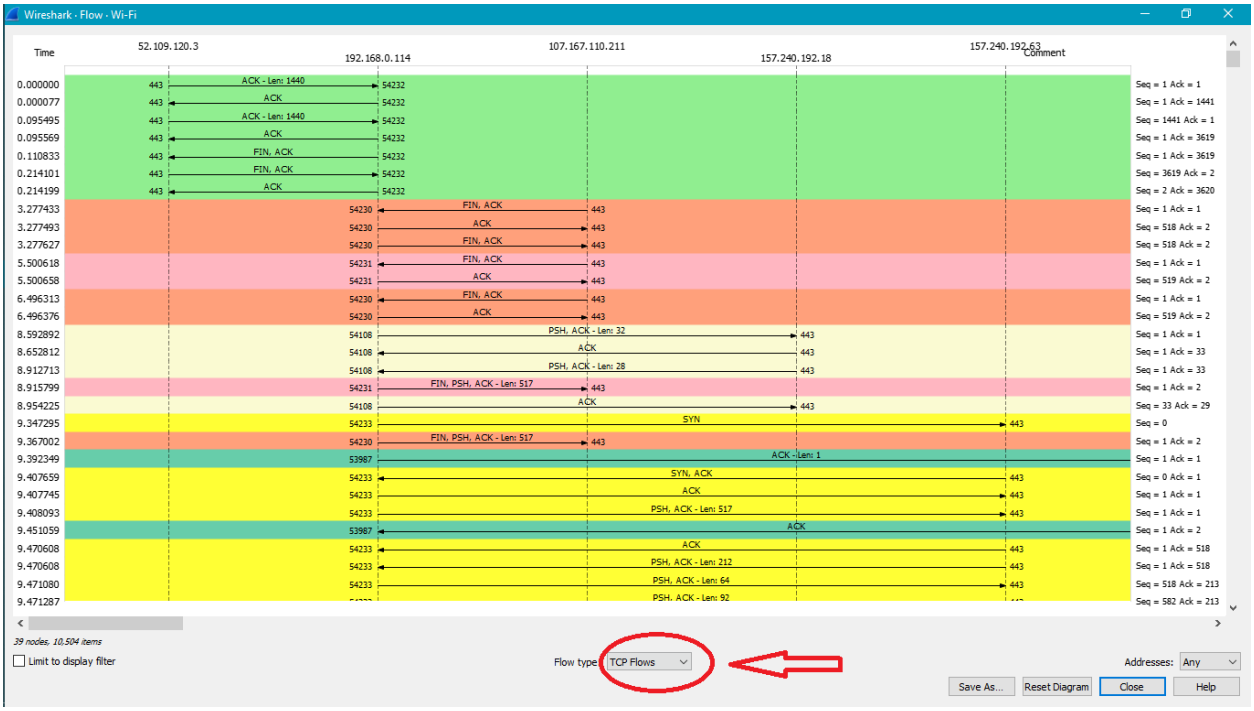

Fig-14: Statistics- Flow Graph: TCP Flows

Conclusion:

All we need to do just download the Wireshark.exe fie from the source and install it to the computer. We run it and captured the network. The Transfer Control Protocol (TCP) through the graph have shown us the desired output.

- o -