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: Raisa Jerin Sristy

ID: IT-16056

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

LAB NO.:04

Name of Experiment: Protocol Analysis with Wireshark

Objectives:

1. To capture a data packet from interface and show the captured data in detail.
2. Filtering packets applying a display filter such as udp, ip.src etc.
3. Displaying various statistics such as flow graph.
4. Finding any specific flow graph such as TCP flow.

Procedure:

Capturing: We will to start Capturing, by clicking Capture menu and selecting an interface that has IP address from available interfaces list. The captured packet will put on the show of the details of each packet transmitted over the wireless LAN. This process can be stopped by clicking on Stop capture button.

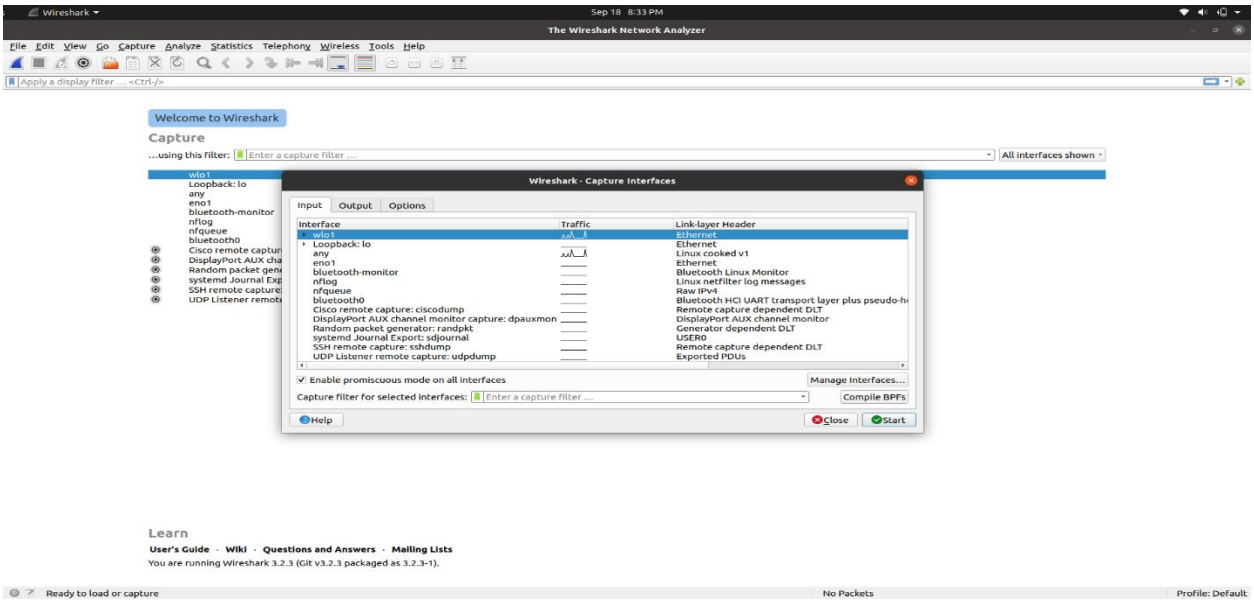

Figure: List of interfaces and start capturing that has IP address.

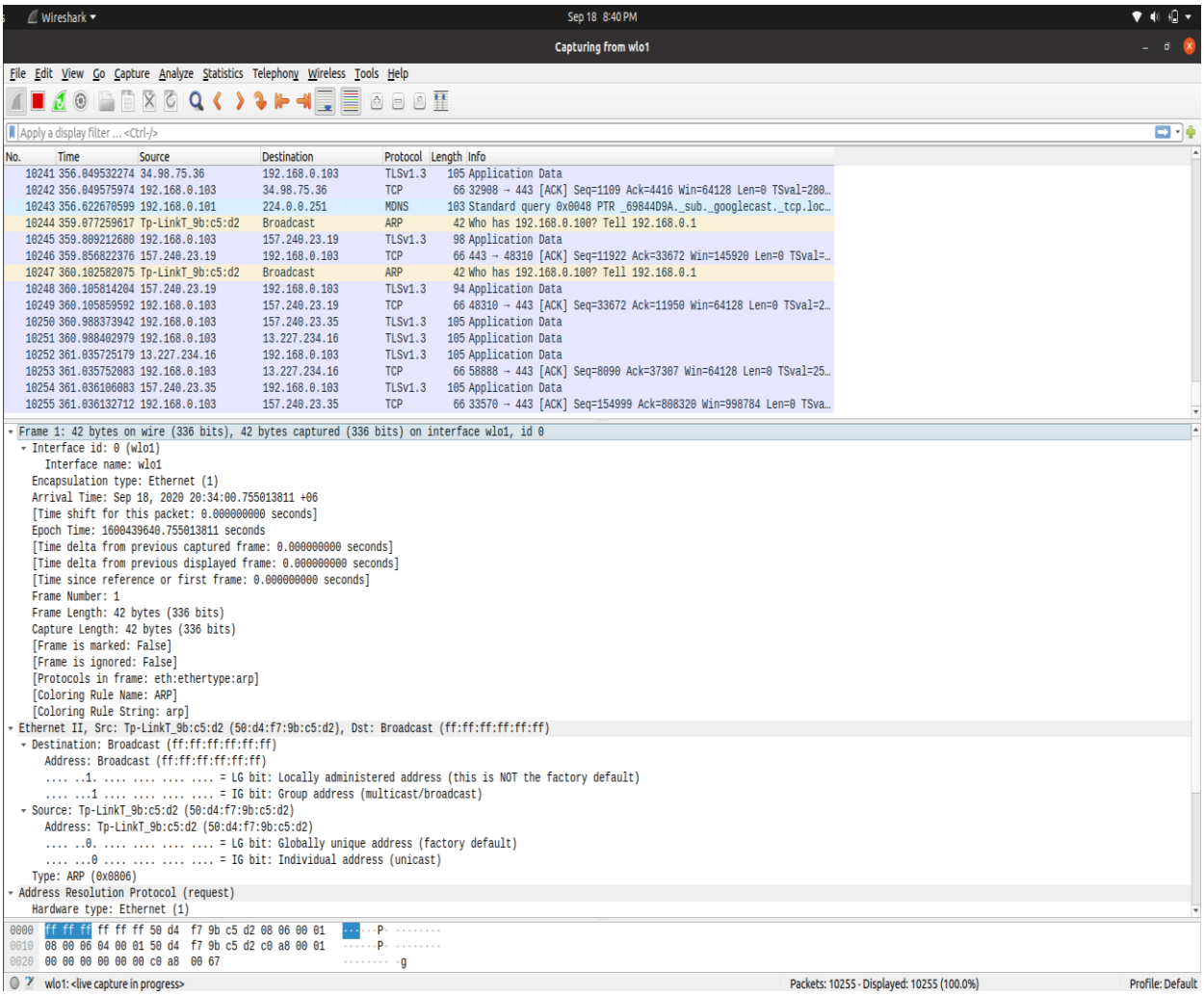

Figure: A packet capture window showing packet list panel, details panel and bytes panel.

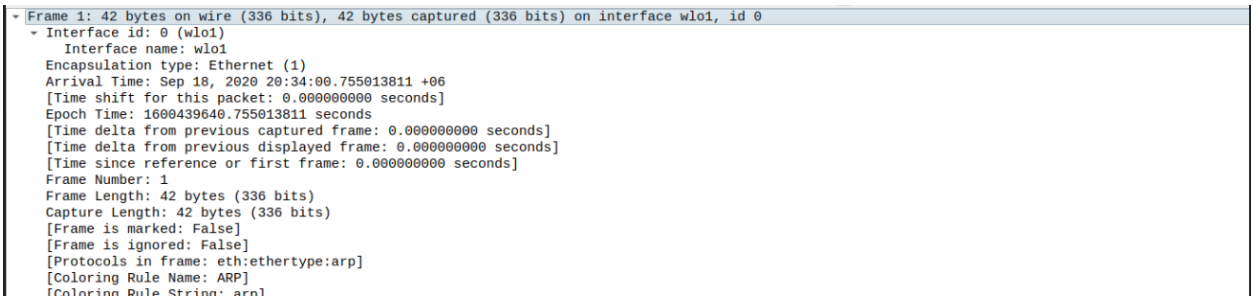

Figure: Packet Details Panel (Frame segment)

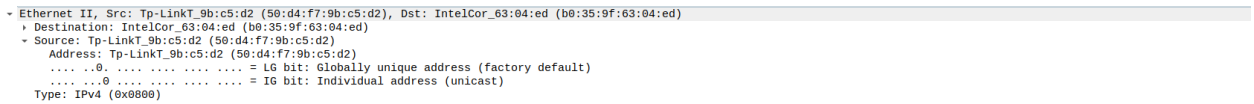

Figure: Packet Details Panel (Ethernet segment)

```
Internet Protocol Version 4, Src: 209.85.229.155, Dst: 192.168.0.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xce94 (52884)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 58
    Protocol: TCP (6)
    Header checksum: 0x3a2f [validation disabled]
    [Header checksum status: Unverified]
    Source: 209.85.229.155
    Destination: 192.168.0.103
Transmission Control Protocol, Src Port: 443, Dst Port: 42886, Seq: 1, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 42886
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 1744720126
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 4039947558
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 2712
    [Calculated window size: 2712]
```

Figure: Packet Details Panel (TCP segment)

```
0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 28 e4 7e 40 00 70 06  65 28 b6 bb 49 5d c0 a8   ·(·~@·p· e(··I]··
0020  00 68 bc dd 2e b8 cf c9  63 d1 5e 53 ff d5 50 11   ·h·.···· c·^S··P·
0030  02 01 6f 4f 00 00                                 ··oO··
```

Figure: Packet bytes panel.

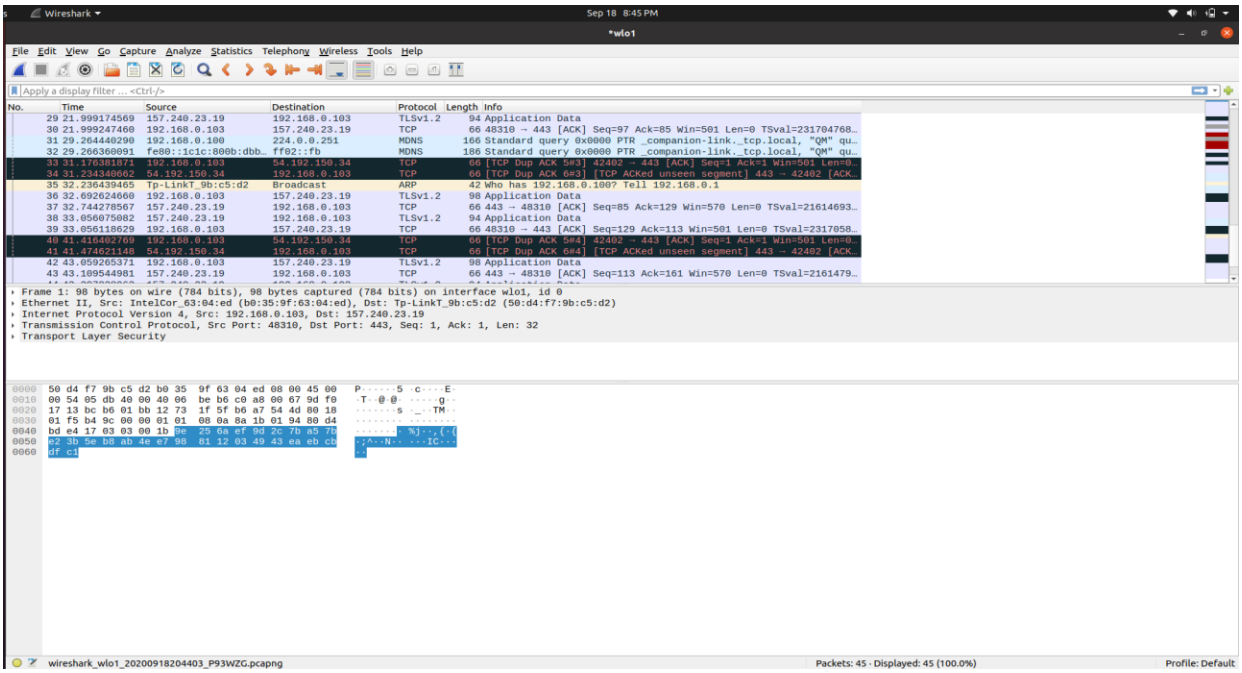

Figure: Stopping Capture.

Filtering: Filtering can be done applying a display filter (such as udp, IP source filter, IP destination filter etc.).

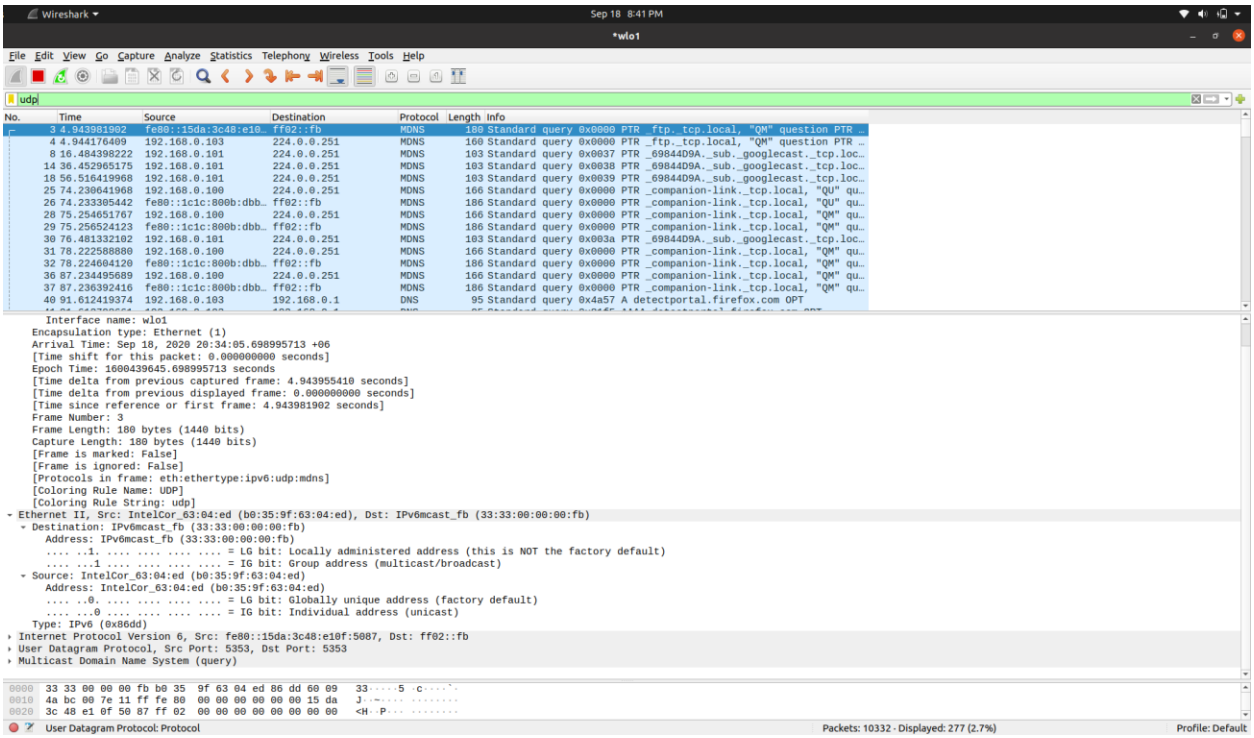

Figure: Filtering by protocol

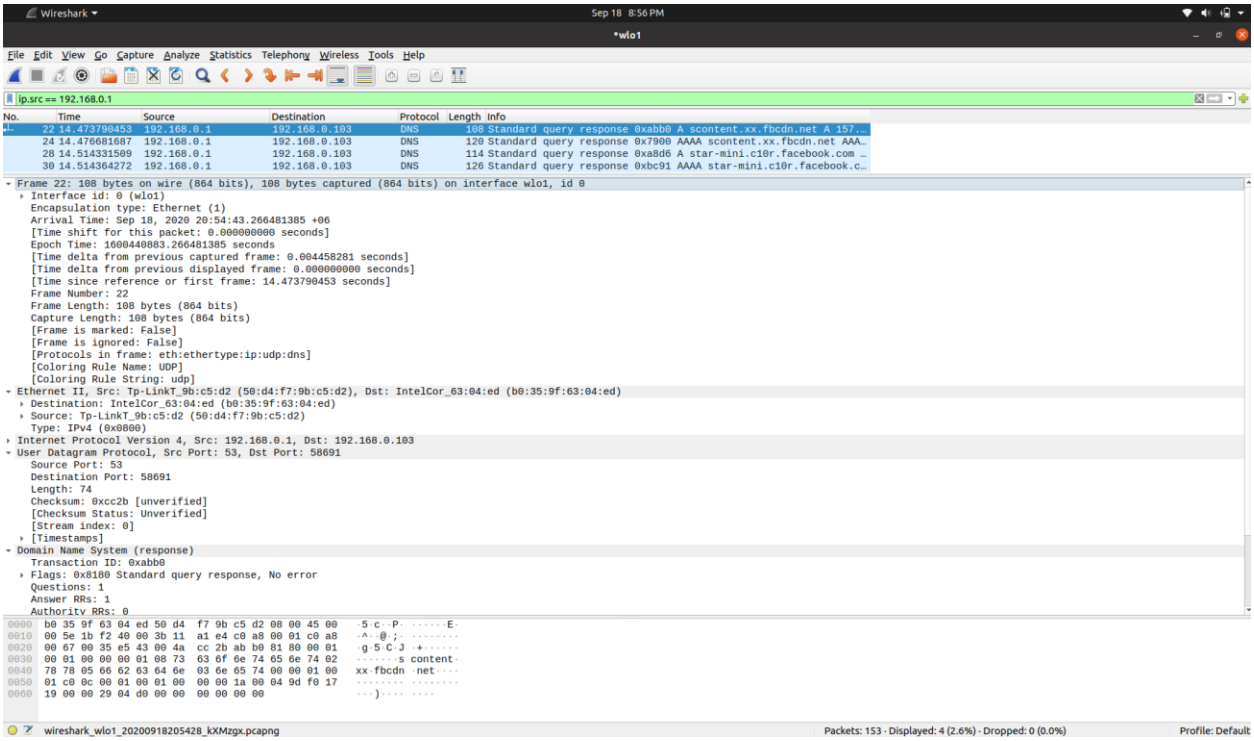

Figure: IP source filter.

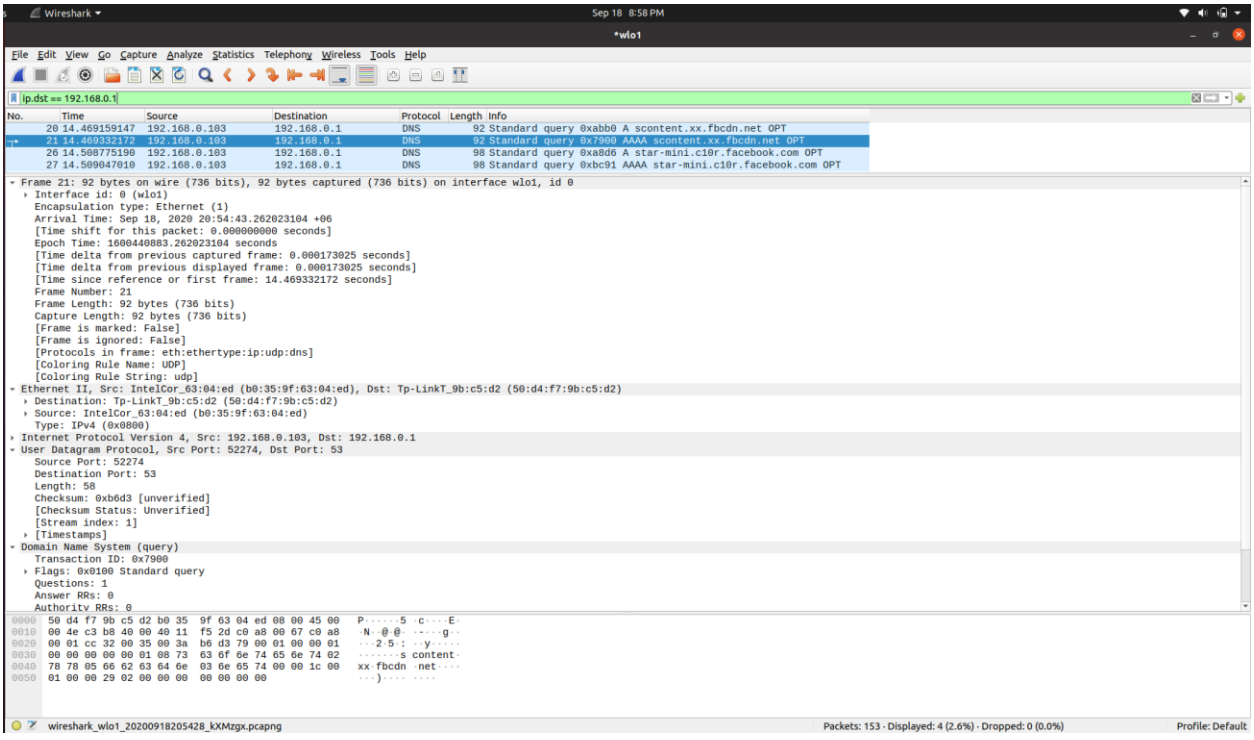

Figure: IP destination filter.

Statistics: Creating various statistics with flow graph can be helpful for better understanding the analysis**.**

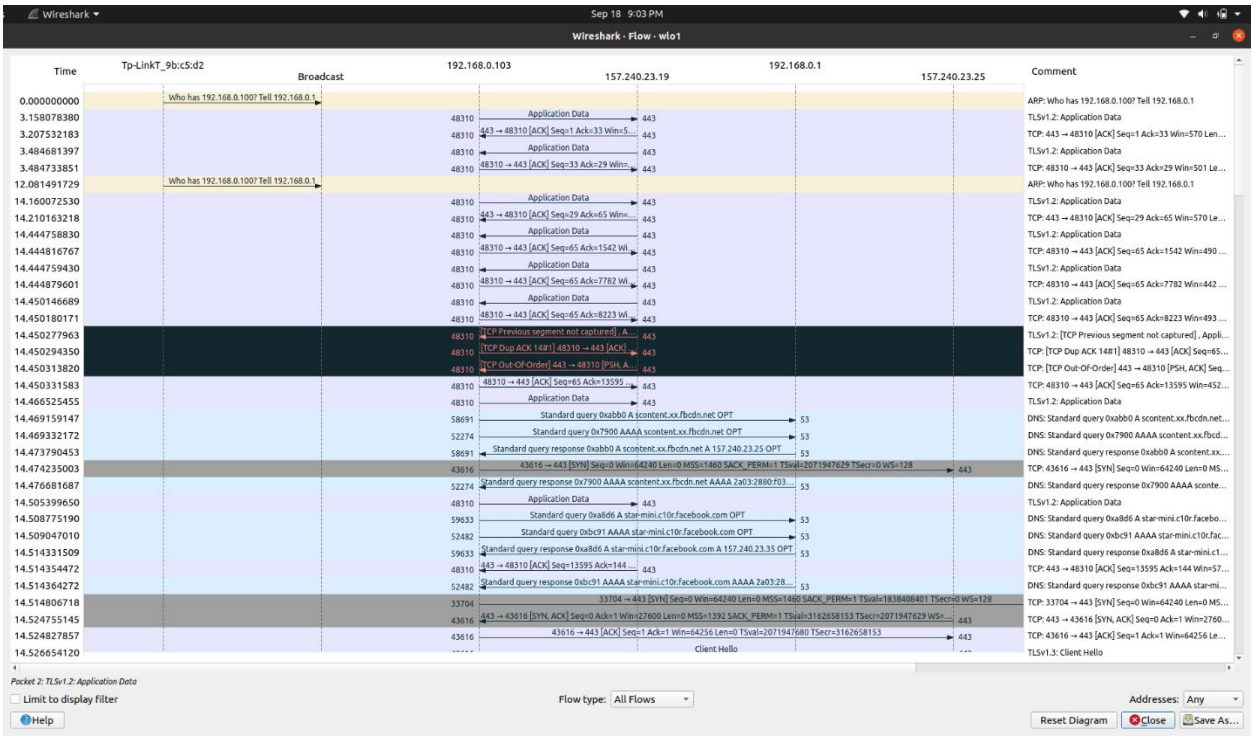

Figure: Statistics- Flow Graph (All Flows)

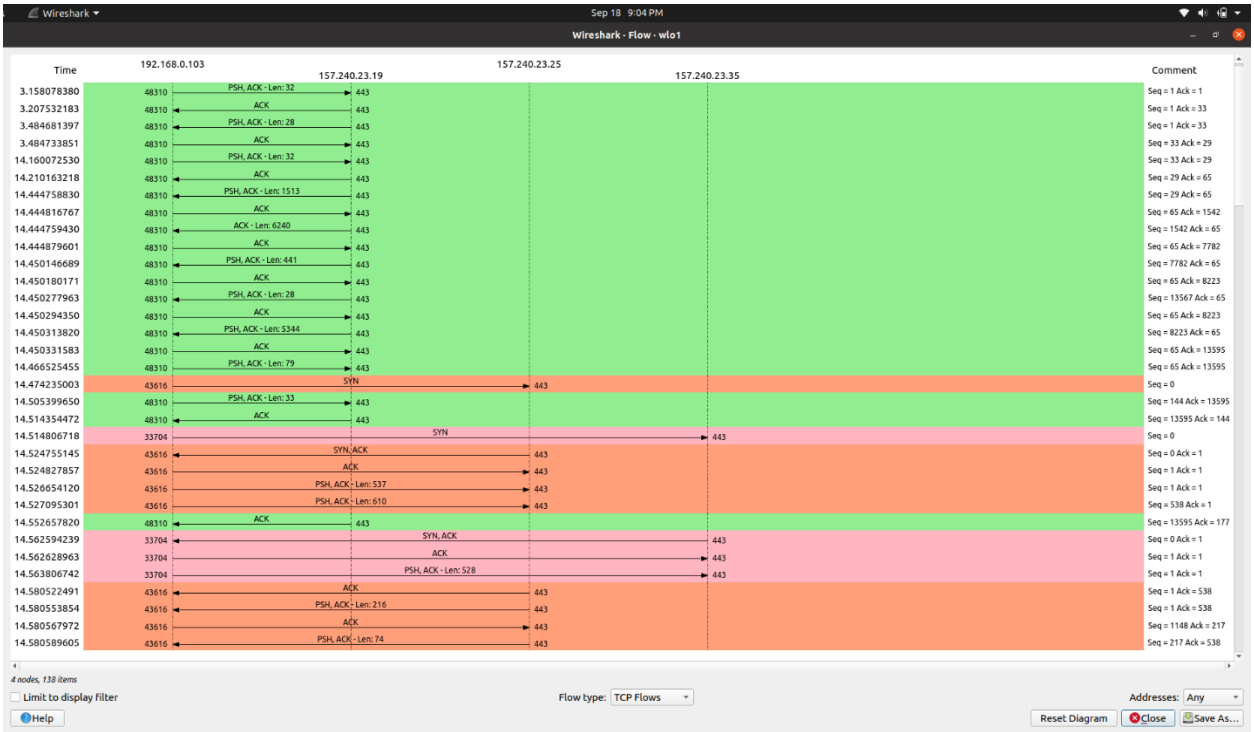

Figure: Statistics- Flow Graph (TCP Flow)

Conclusion:

Here in this experiment, using Wireshark live packet data from a network interface can be captured easily. Applying a display filter particular traffic can be monitored. The flow graph of TCP flow exhibit the throughput from one TCP flow, in one way. All tasks have been done perfectly.