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: Siddiqul Islam

ID:IT-16048

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No: 04

Experiment Name: Protocol Analysis with Wireshark

Objectives:

- Analyzing and count number of packets and size of packets that's are transferred.
- View the result graphically using I/O graph.
- 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.
- Compare the different protocol packets thransformation.

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.

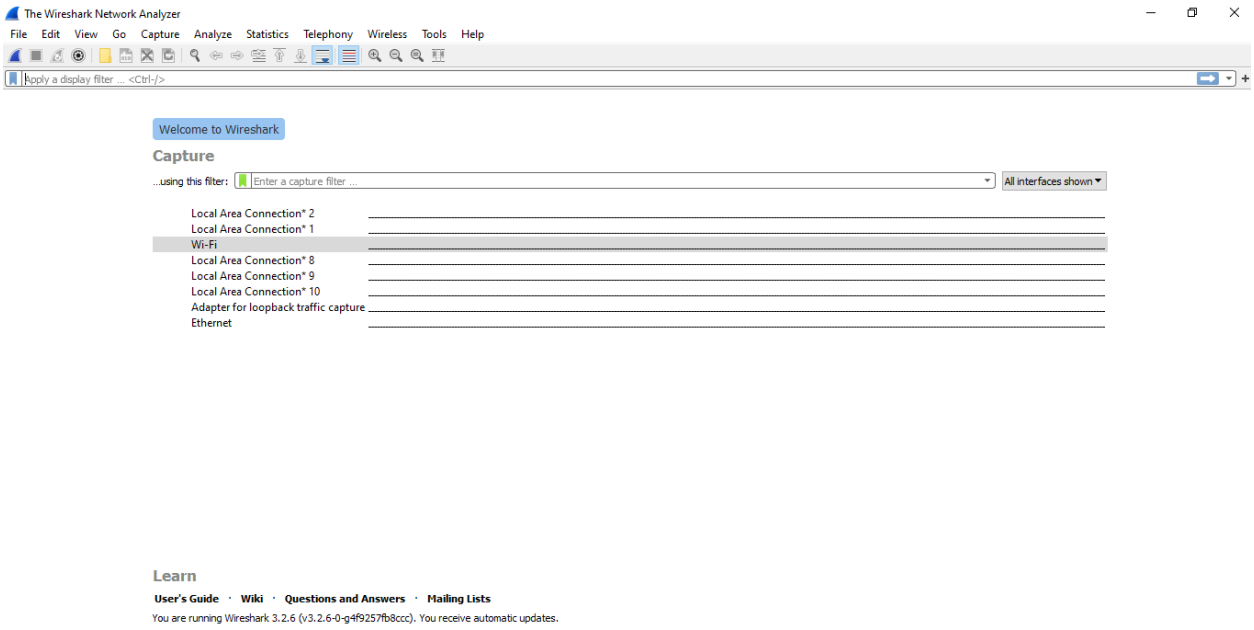


Figure 01: Wireshark Interface List

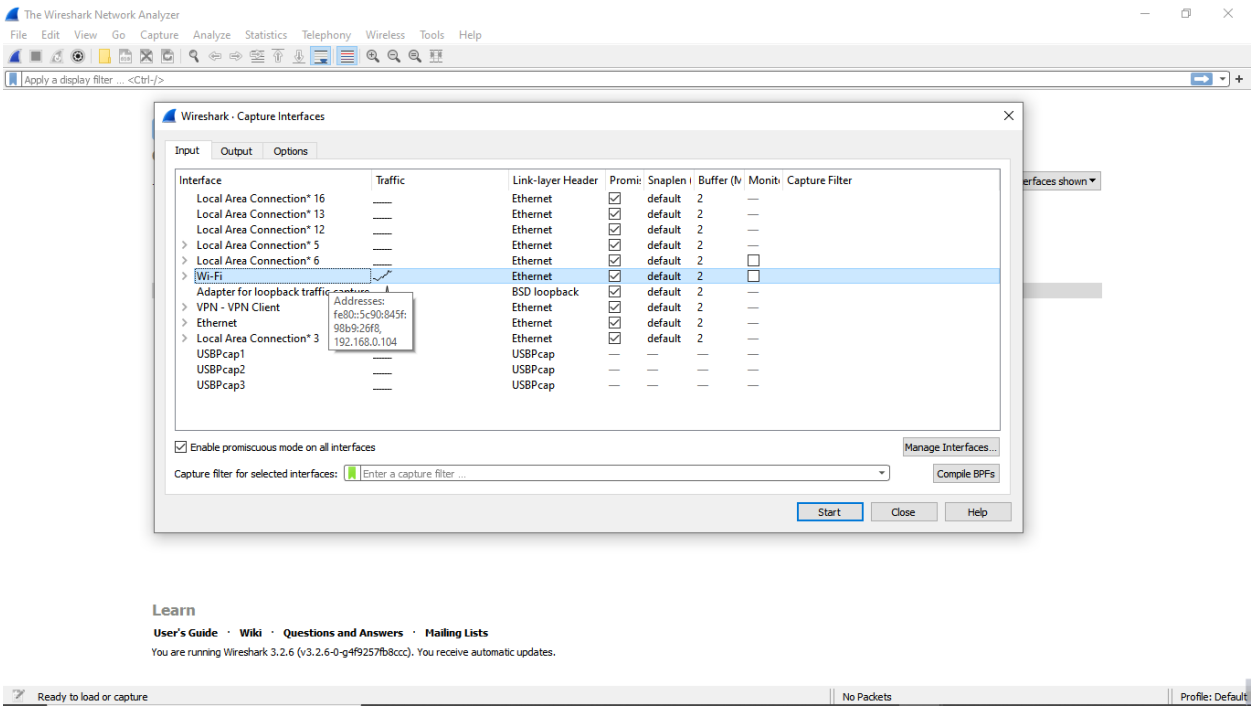


Figure 02: Start Capturing Interface that has IP address

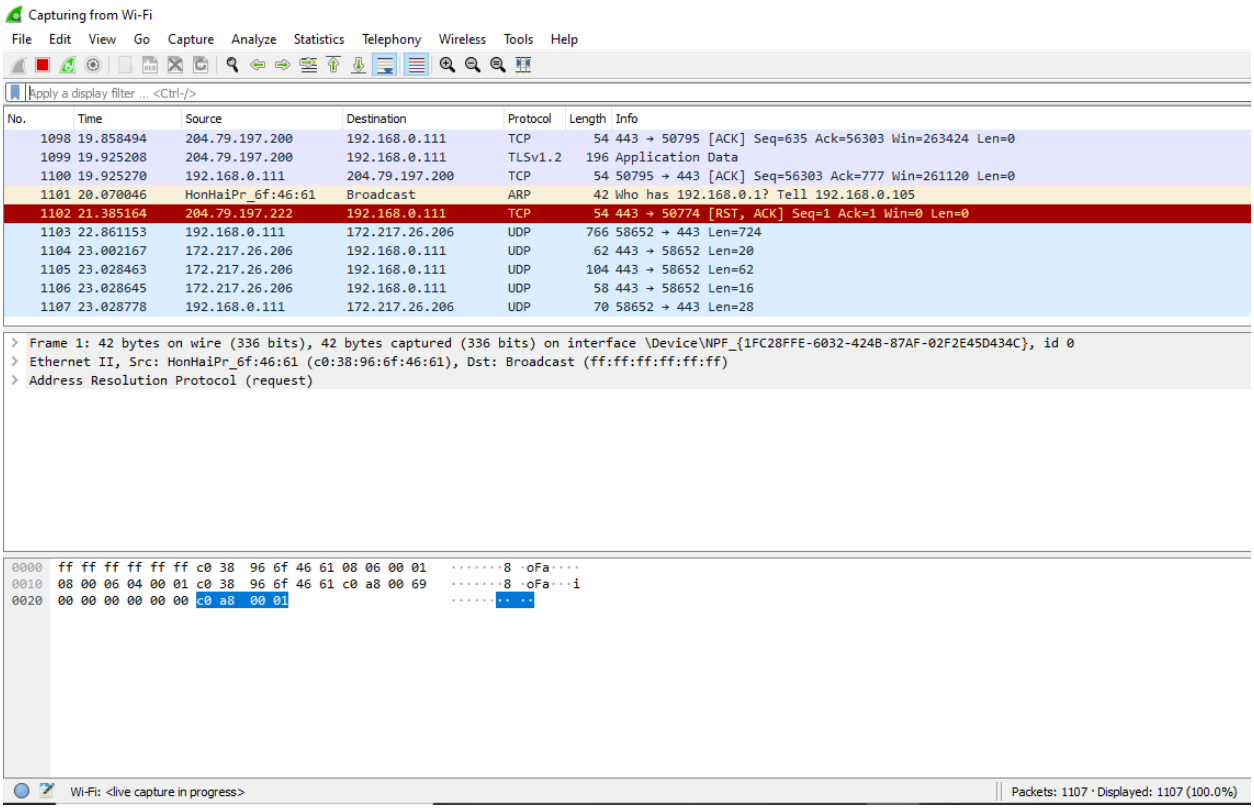


Figure 03: A sample packet capture window

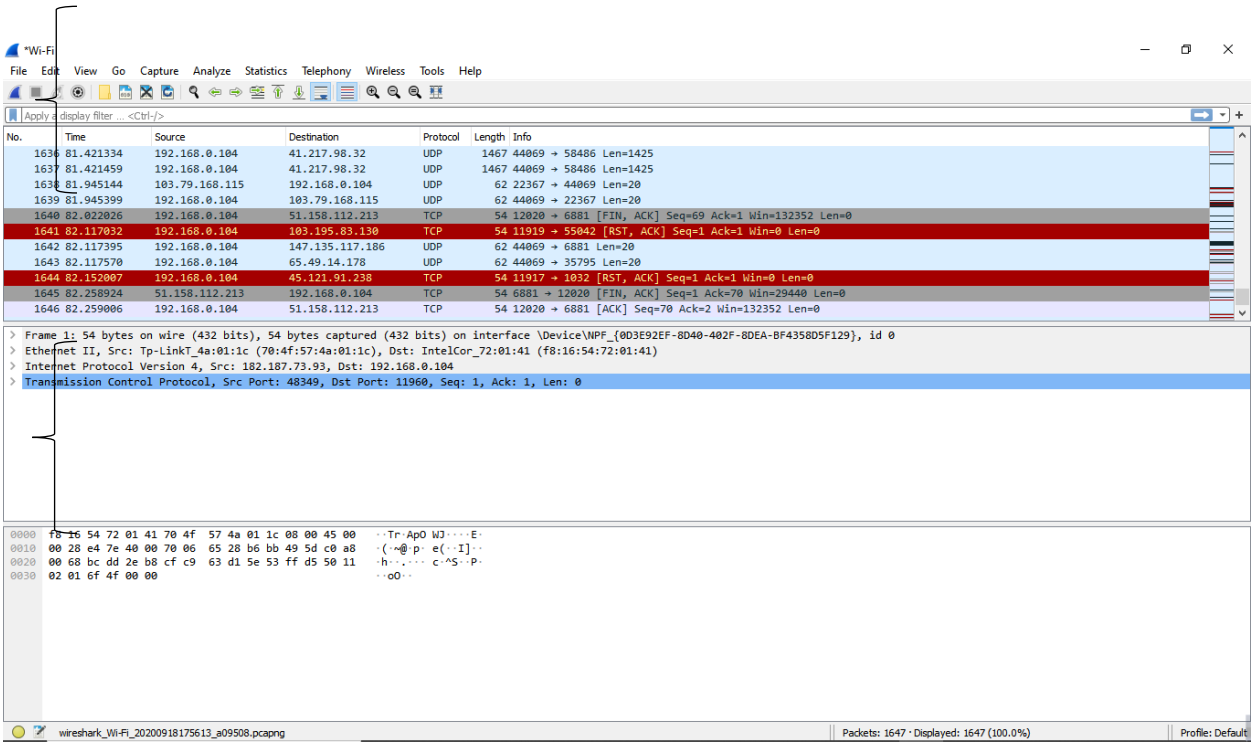
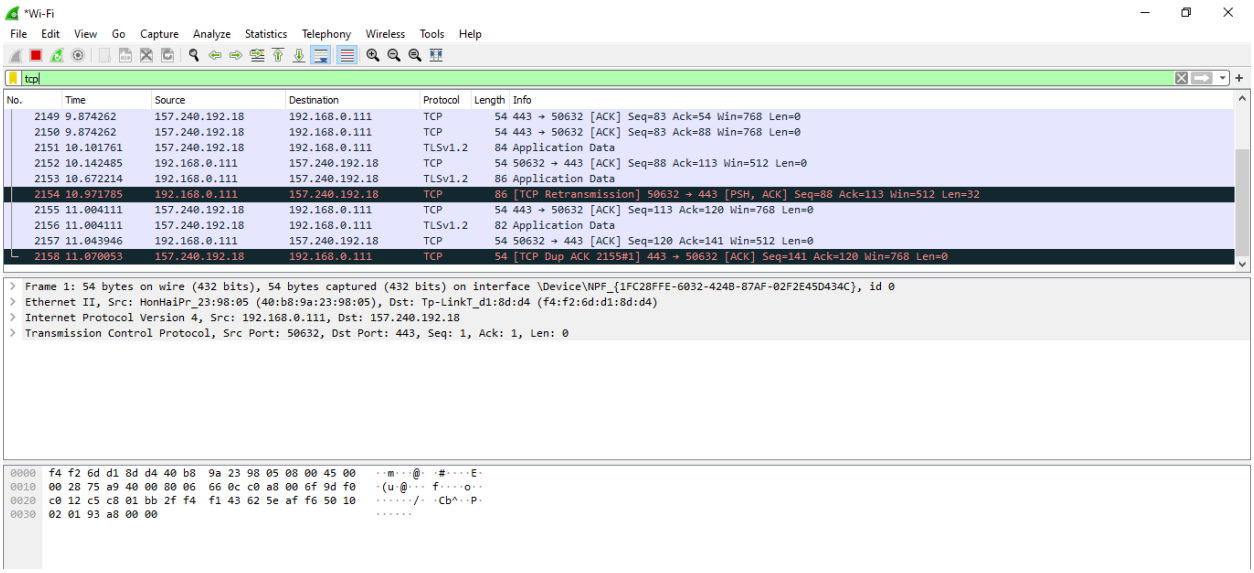


Figure 04: Stopping Capture

Filtering:



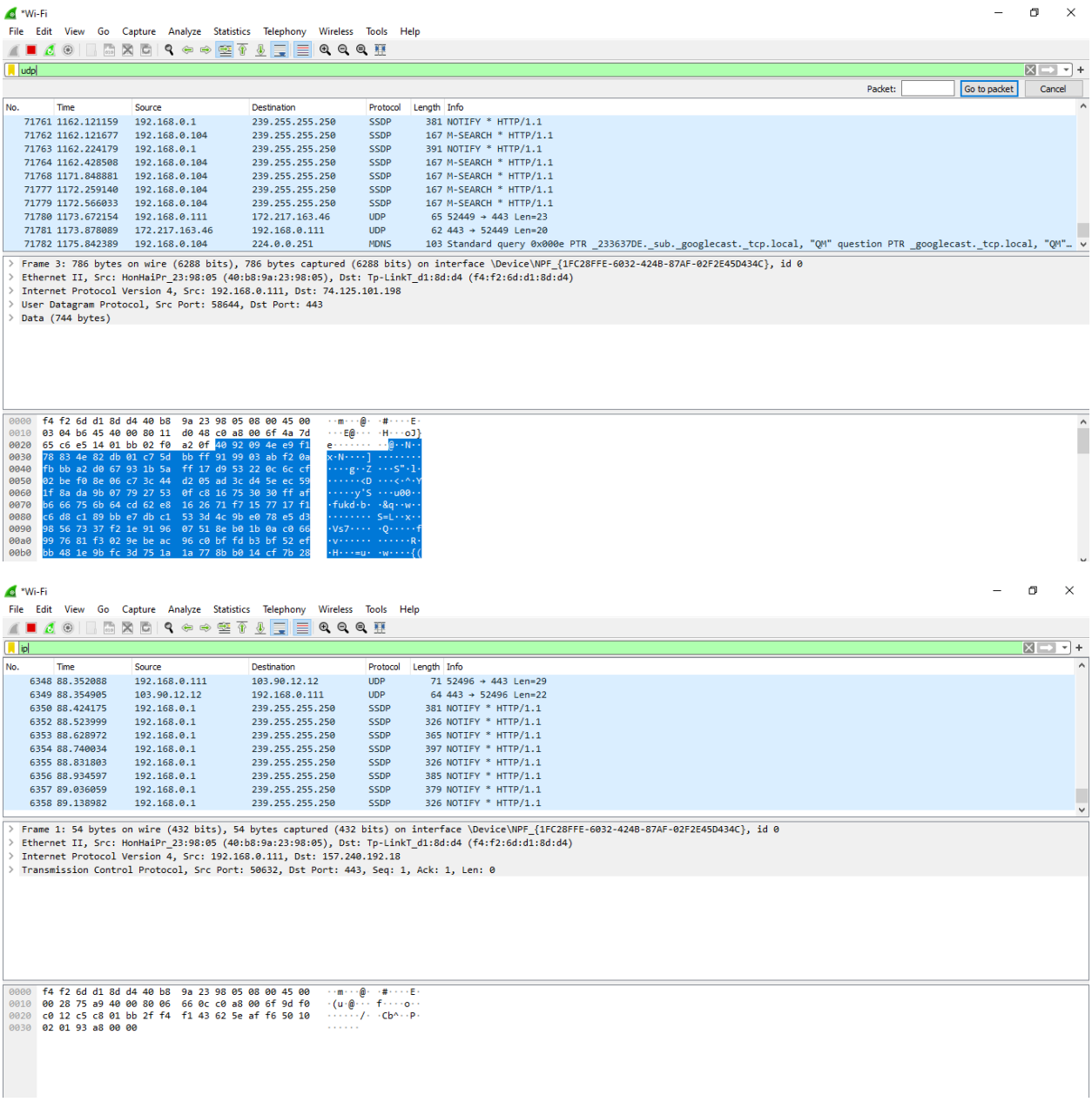


Figure 05: Filter by Protocol

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.

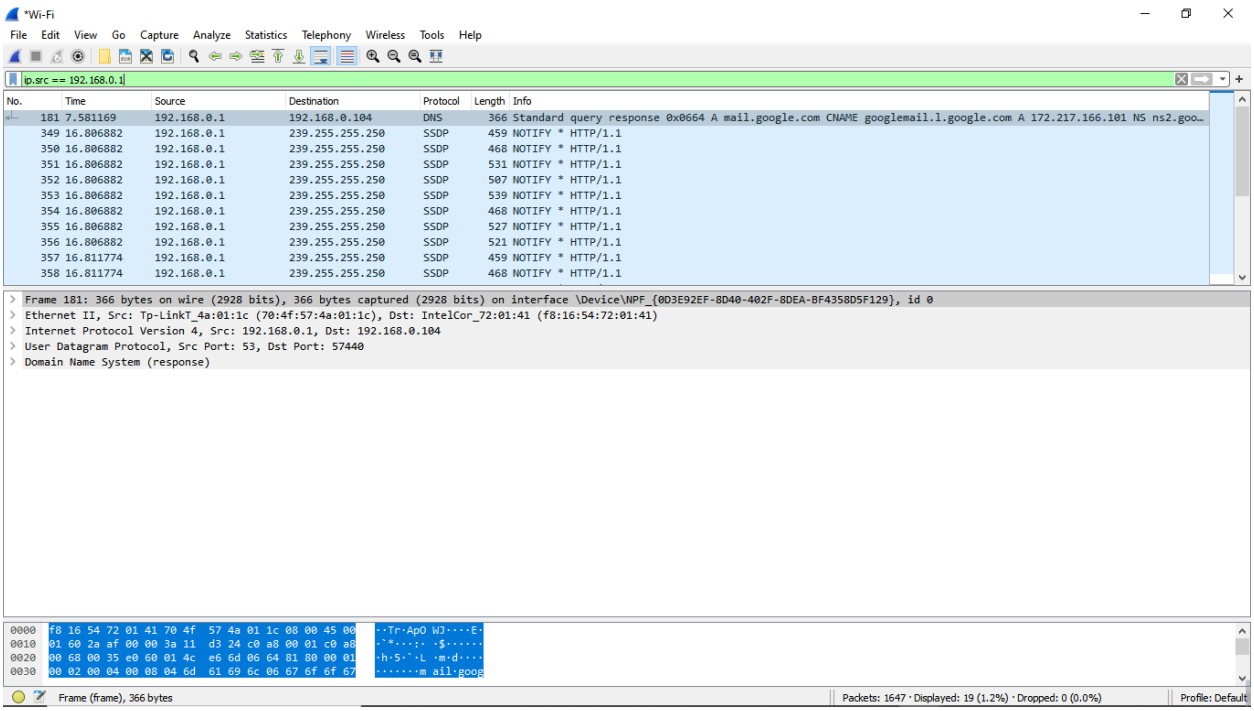


Figure 06: Source IP filter

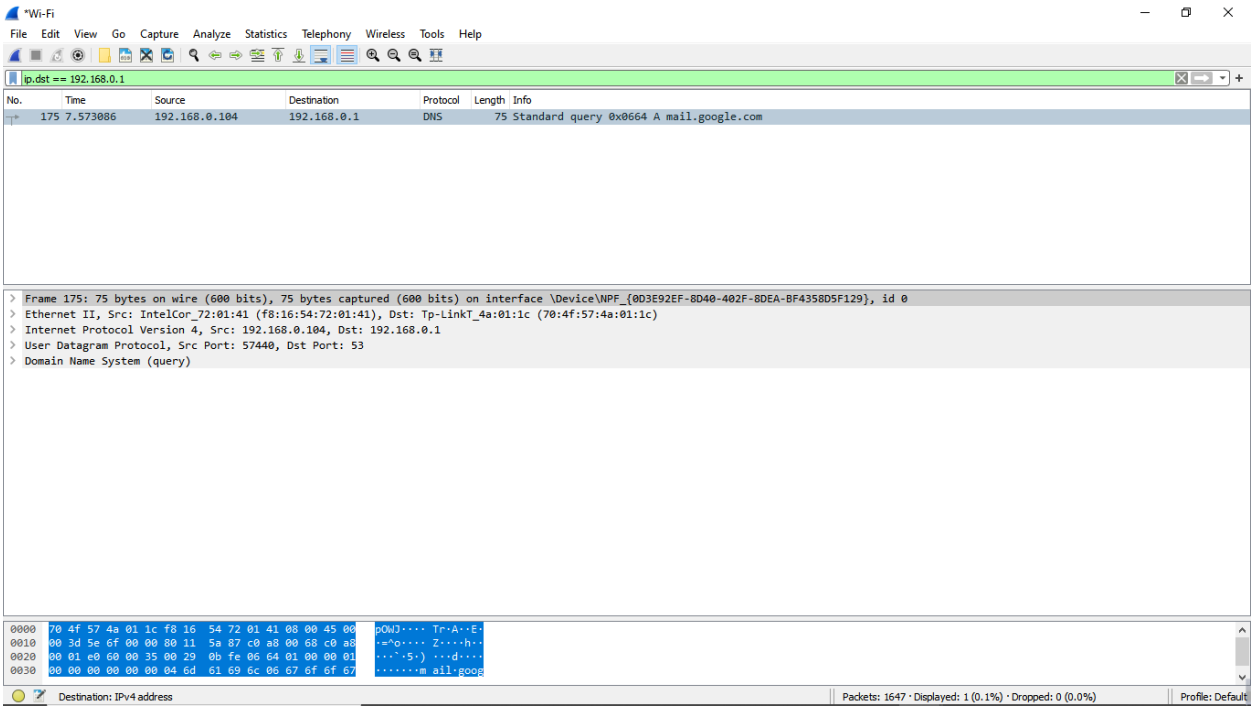


Figure 07: Destination IP filter

- **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**

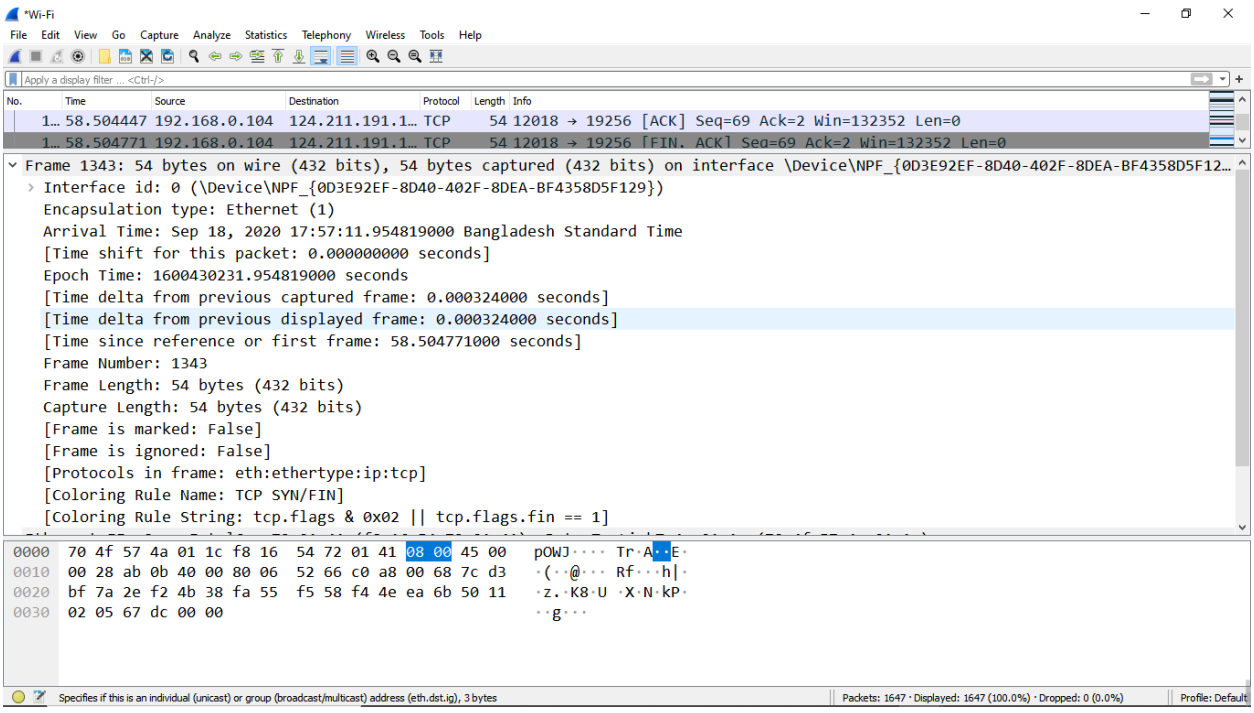


Figure 08: Packet Details Pane(Frame segment)

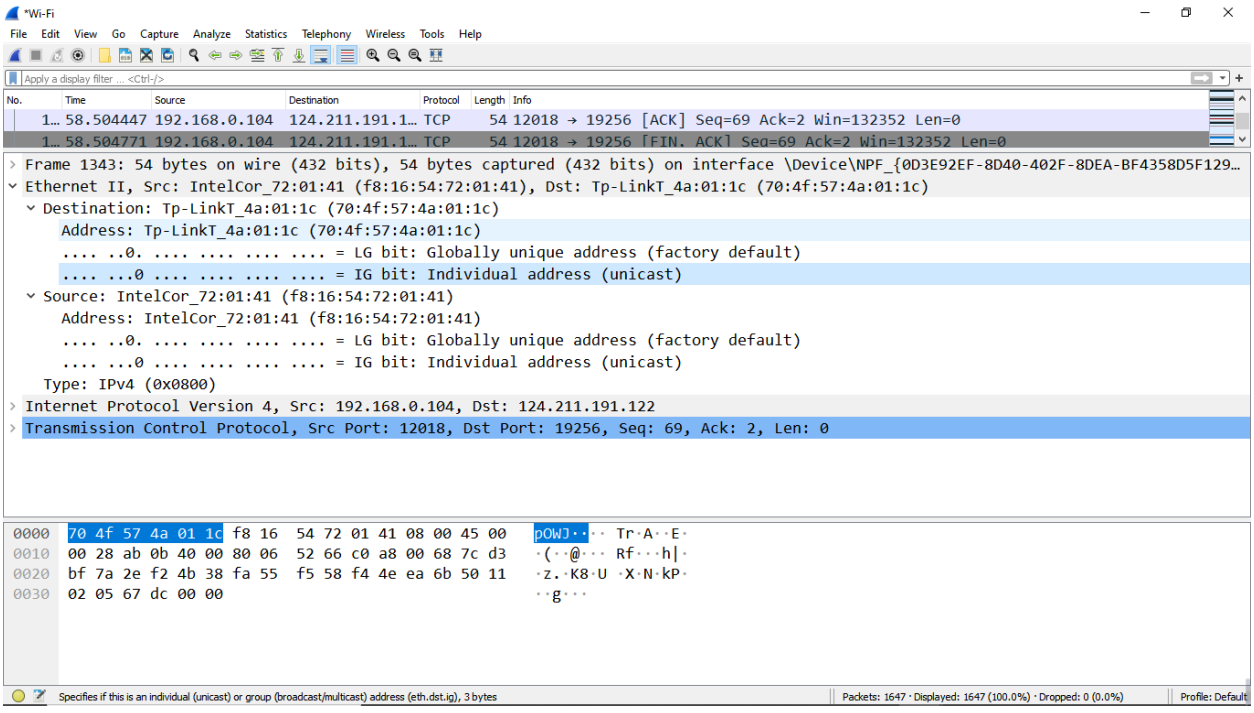
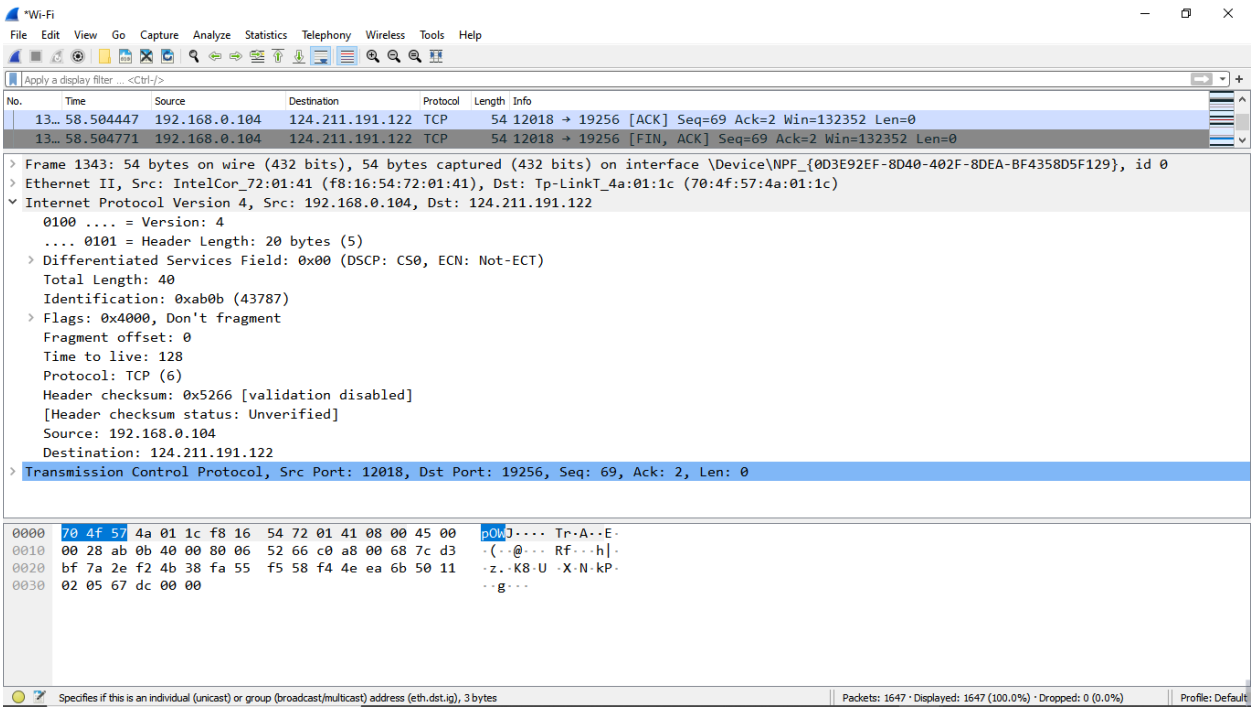


Figure 09: Packet Details Pane (Ethernet Segment)



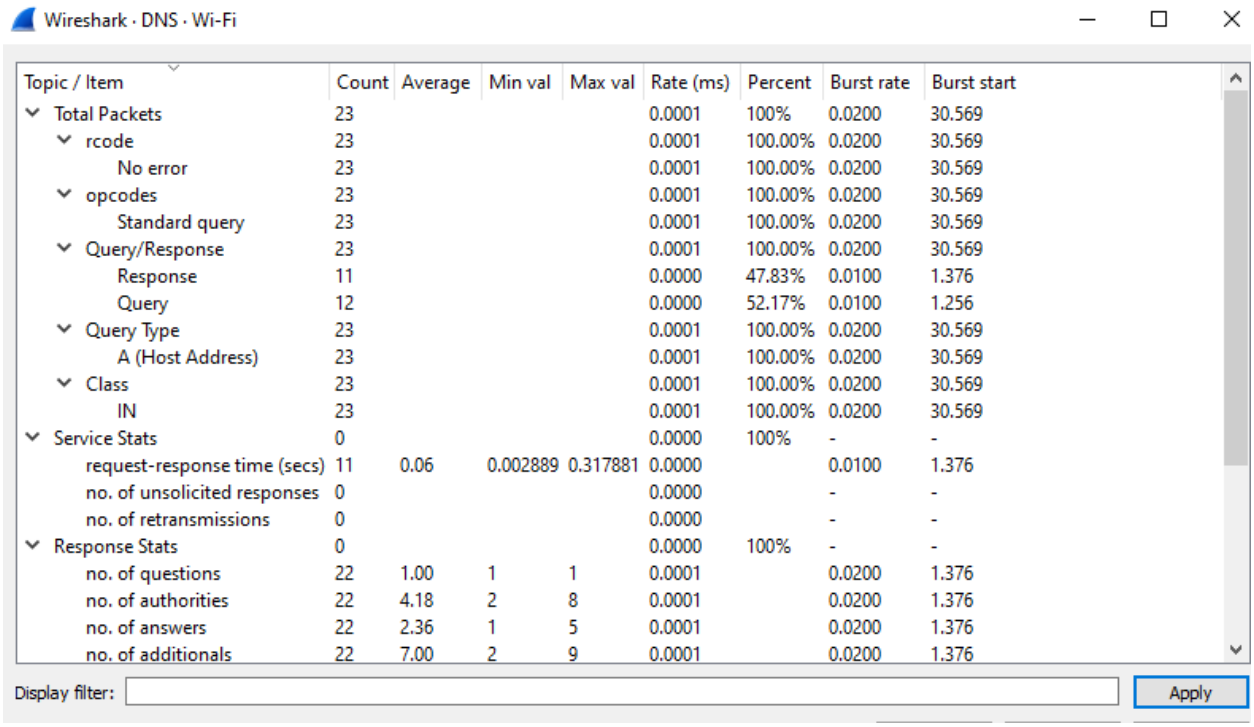


Figure 10: Packet Details Pane(IP segment)

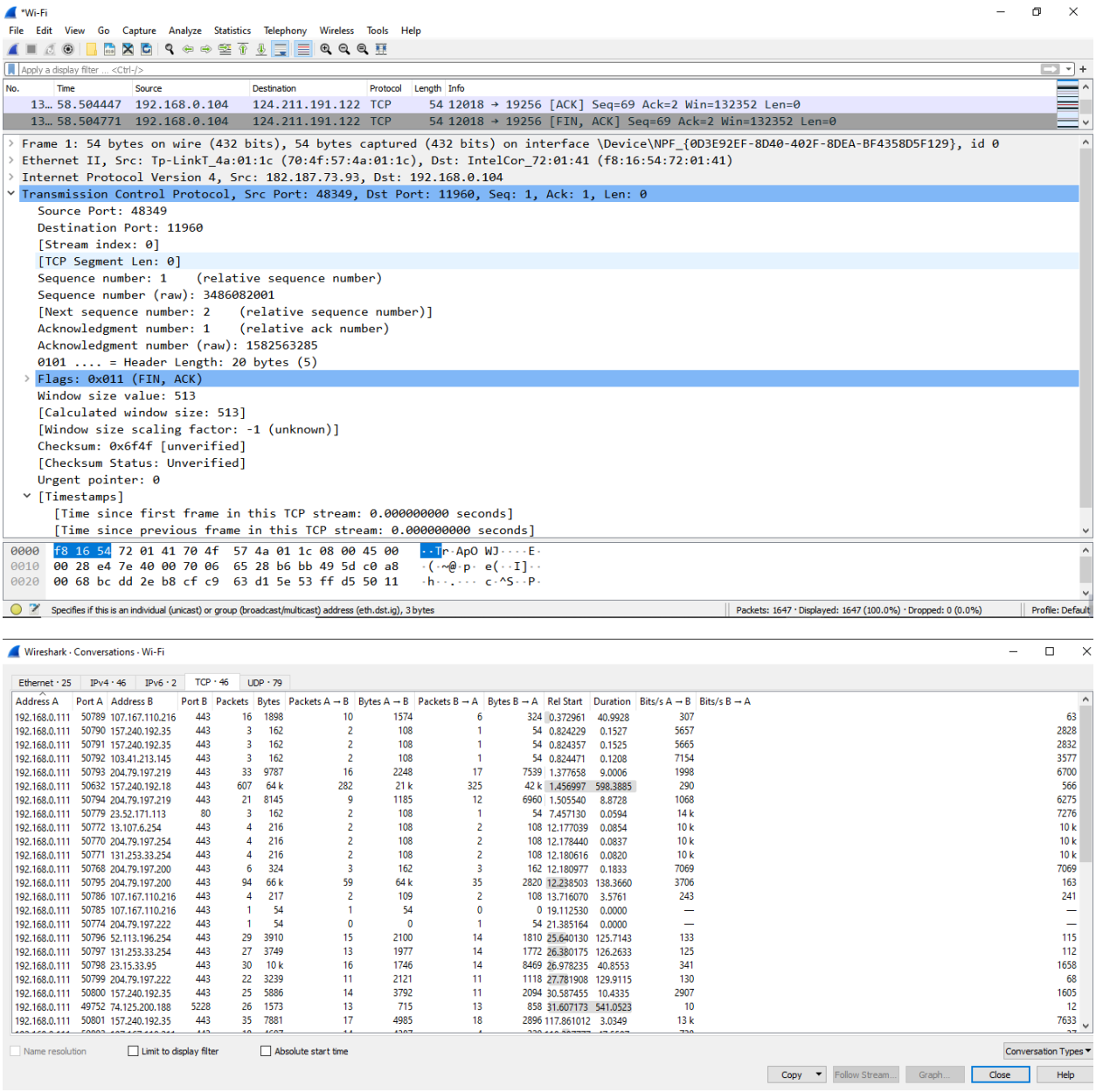


Figure 11: Packet Details Pane (TCP Segment)

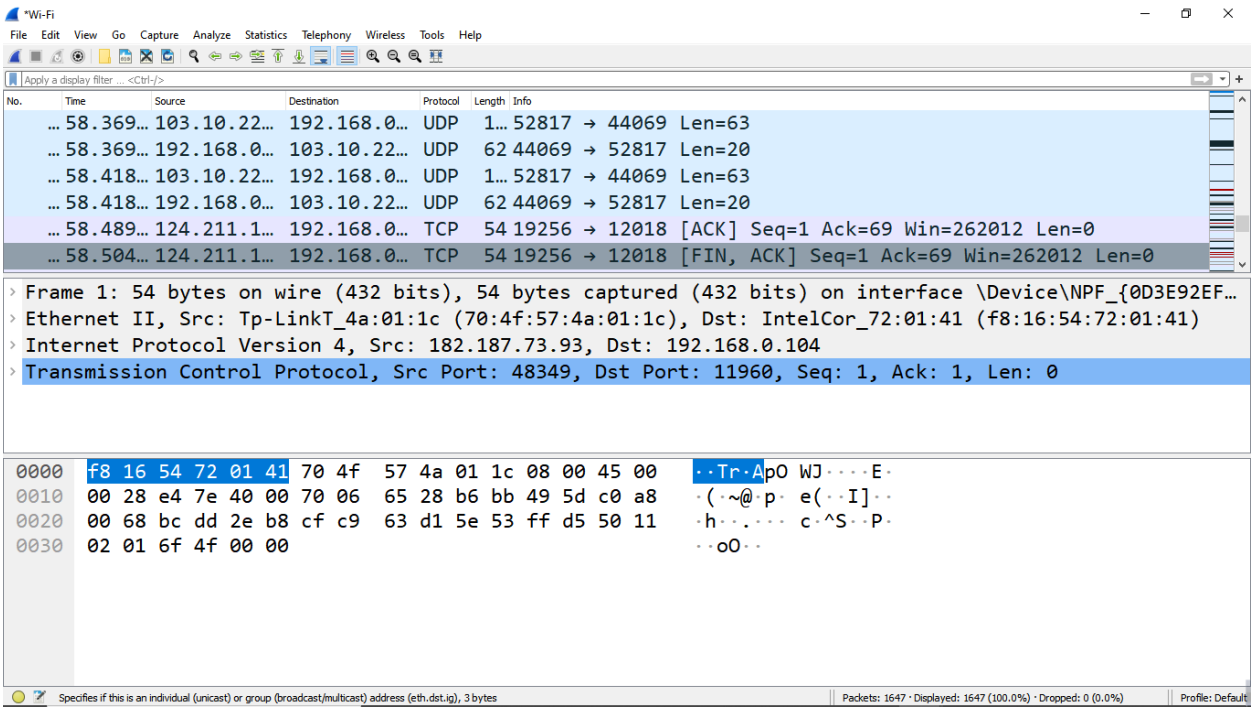


Figure 12: Packet Byte Pane

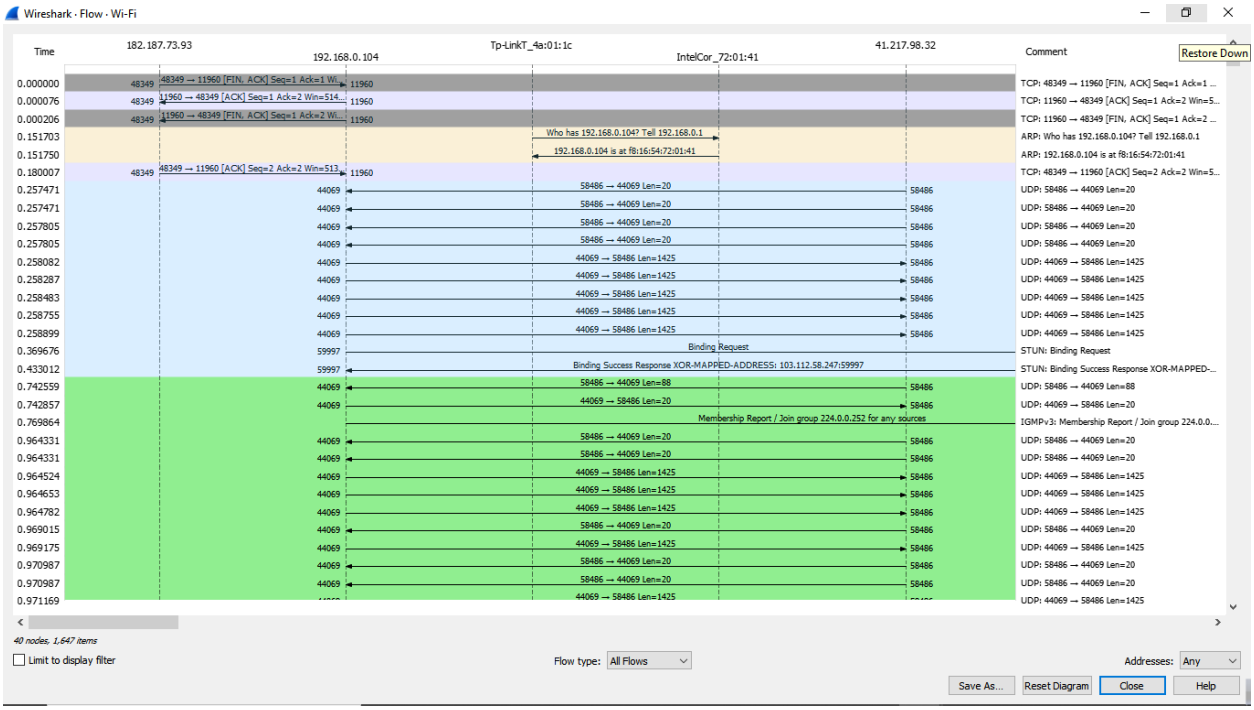
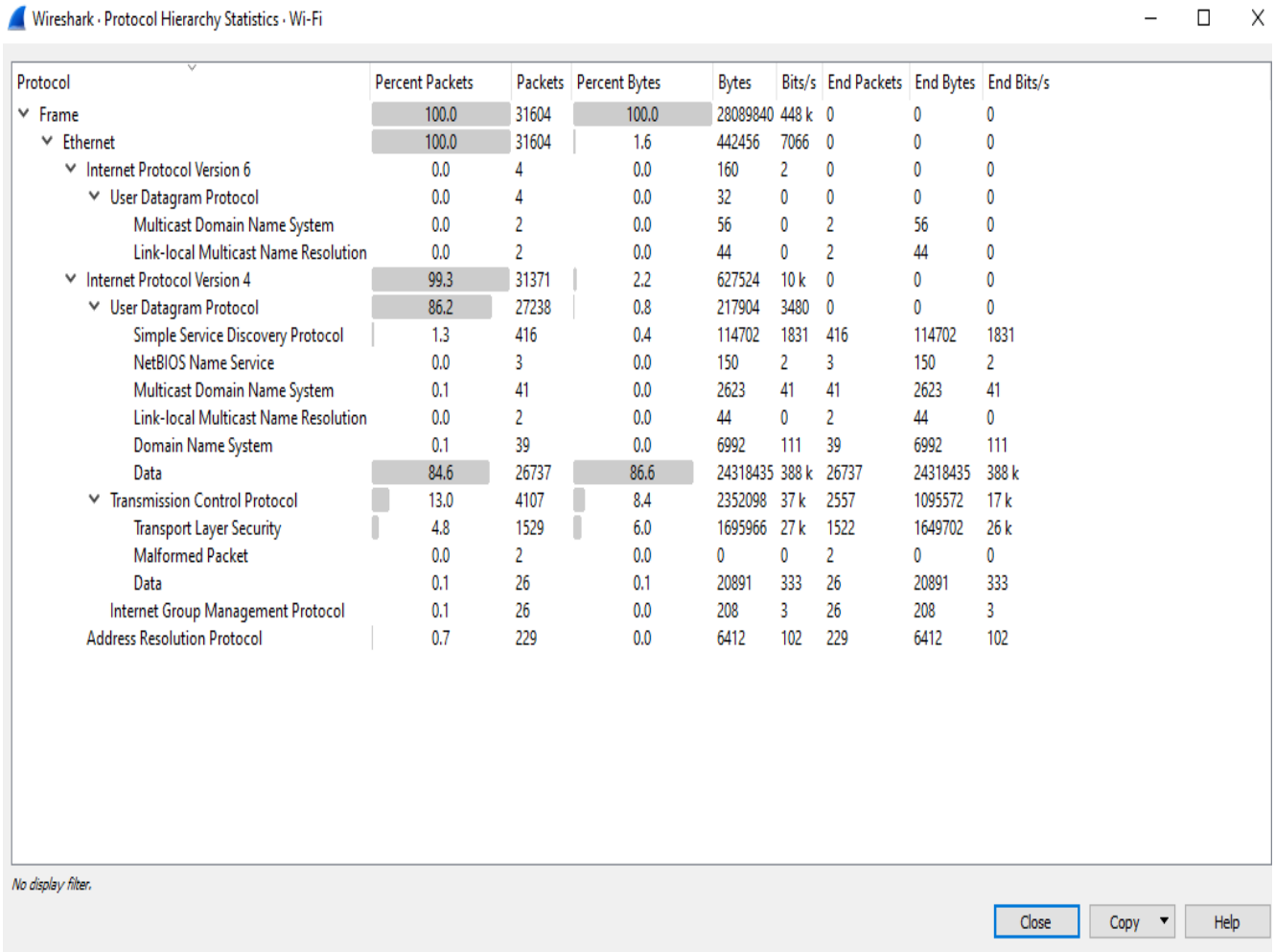


Figure 13: Statistics- Flow Graph(All Flows)


Wireshark · Protocol Hierarchy Statistics · Wi-Fi
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
Frame 100.0 31604 100.0 28089840 448 k 0 0 0
Ethernet 100.0 31604 1.6 442456 7066 0 0 0
Internet Protocol Version 6 0.0 4 0.0 160 2 0 0 0
User Datagram Protocol 0.0 4 0.0 32 0 0 0 0
Multicast Domain Name System 0.0 2 0.0 56 0 2 56 0
Link-local Multicast Name Resolution 0.0 2 0.0 44 0 2 44 0
Internet Protocol Version 4 99.3 31371 2.2 627524 10 k 0 0 0
User Datagram Protocol 86.2 27238 0.8 217904 3480 0 0 0
Simple Service Discovery Protocol 1.3 416 0.4 114702 1831 416 114702 1831
NetBIOS Name Service 0.0 3 0.0 150 2 3 150 2
Multicast Domain Name System 0.1 41 0.0 2623 41 41 2623 41
Link-local Multicast Name Resolution 0.0 2 0.0 44 0 2 44 0
Domain Name System 0.1 39 0.0 6992 111 39 6992 111
Data 84.6 26737 86.6 24318435 388 k 26737 24318435 388 k
Transmission Control Protocol 13.0 4107 8.4 2352098 37 k 2557 1095572 17 k
Transport Layer Security 4.8 1529 6.0 1695966 27 k 1522 1649702 26 k
Malformed Packet 0.0 2 0.0 0 0 2 0 0
Data 0.1 26 0.1 20891 333 26 20891 333
Internet Group Management Protocol 0.1 26 0.0 208 3 26 208 3
Address Resolution Protocol 0.7 229 0.0 6412 102 229 6412 102
No display filter.
Close
Copy
Help

***

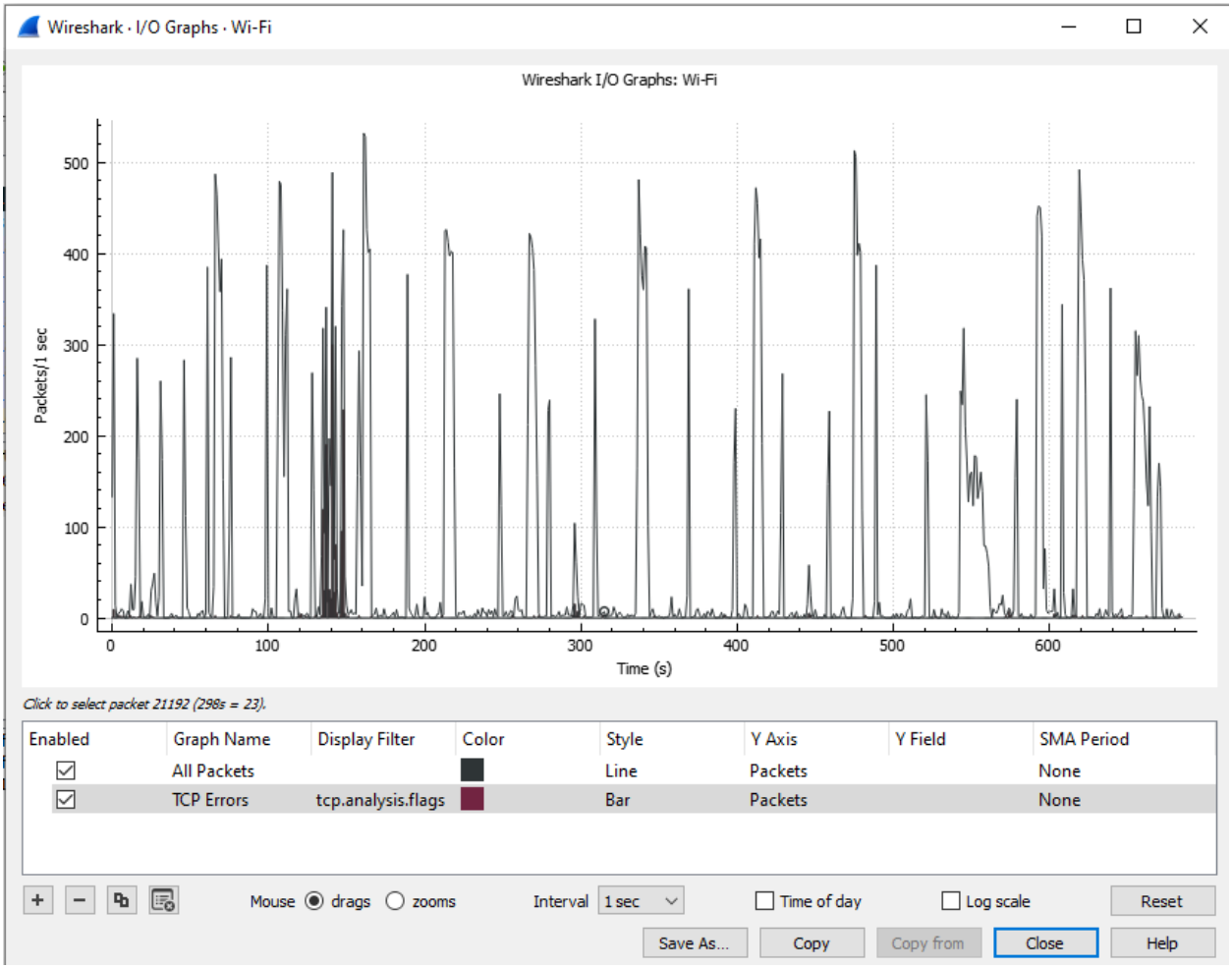


Figure 13: Statistics I/O- Flow Graph*

Conclusion:

After performing this experiment we come to know that by downloading and installing Wireshark, we can easily Capture live packet data from different network interface using Wireshark.. We have applied filter to monitor particular traffic and protocol. Besides that there are many more option such that view, filter, capture, statistics, telephone, wireless using this amazing Wireshark network analyzer.