

**Mawlana Bhashani Science and Technology University**

**Lab-Report**

Report No: 05

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 Submitted To**

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Name: Mohammad Mehedy Hasan

ID:IT-16024

4th year 2ndsemester

Session: 2015-2016

Dept. of ICT

MBSTU.

**Experiment No: 05**

**Experiment Name:** **Comparative Analysis of Wired and Wireless data using Wireshark**

**Objectives:**

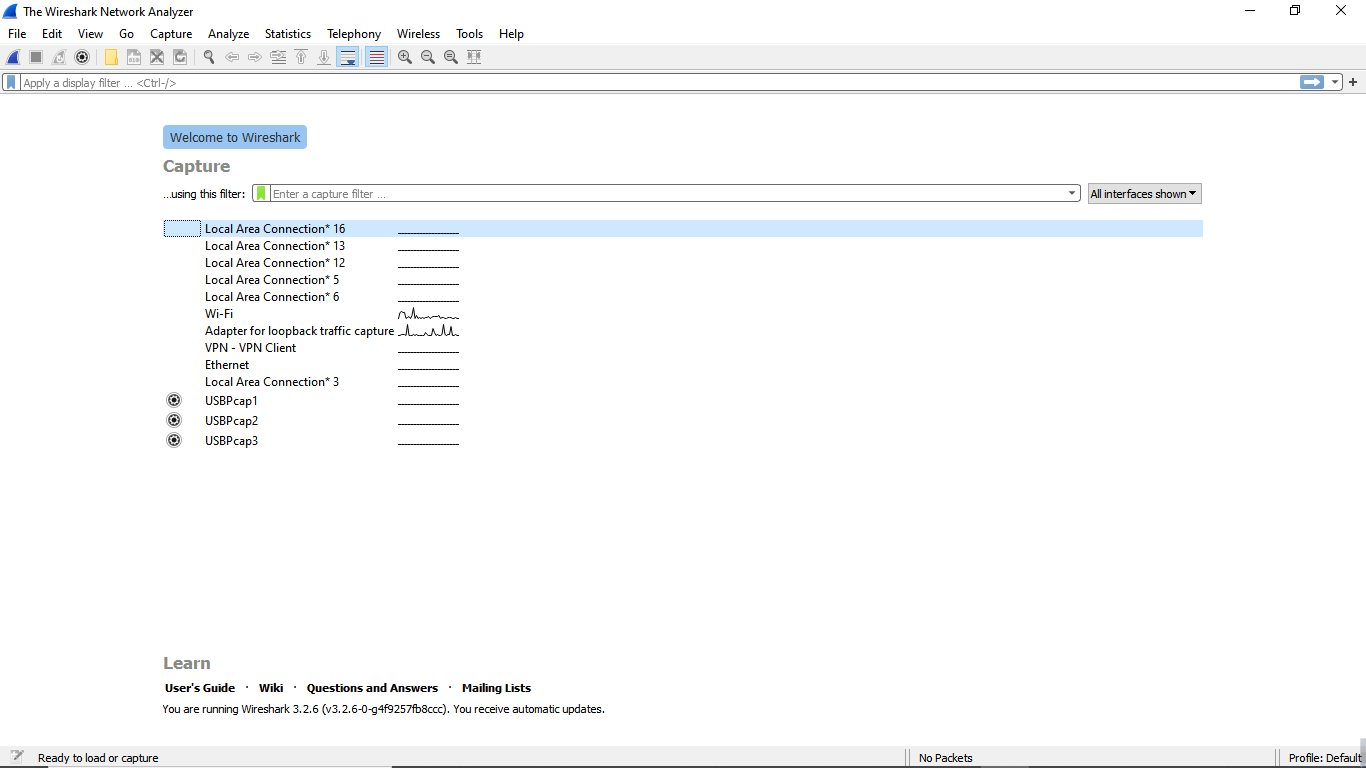
* Capture live packet data from a network interface.
* Display packets with very detailed protocol information.
* Filter packets on many criteria.
* Compare between Ethernet and wireless data packets while filtering
* Compare between Ethernet and wireless data packets in all panels
* Create various statistics.
* Compare Statistics between wired and wireless transmission

**Capturing Packets:**

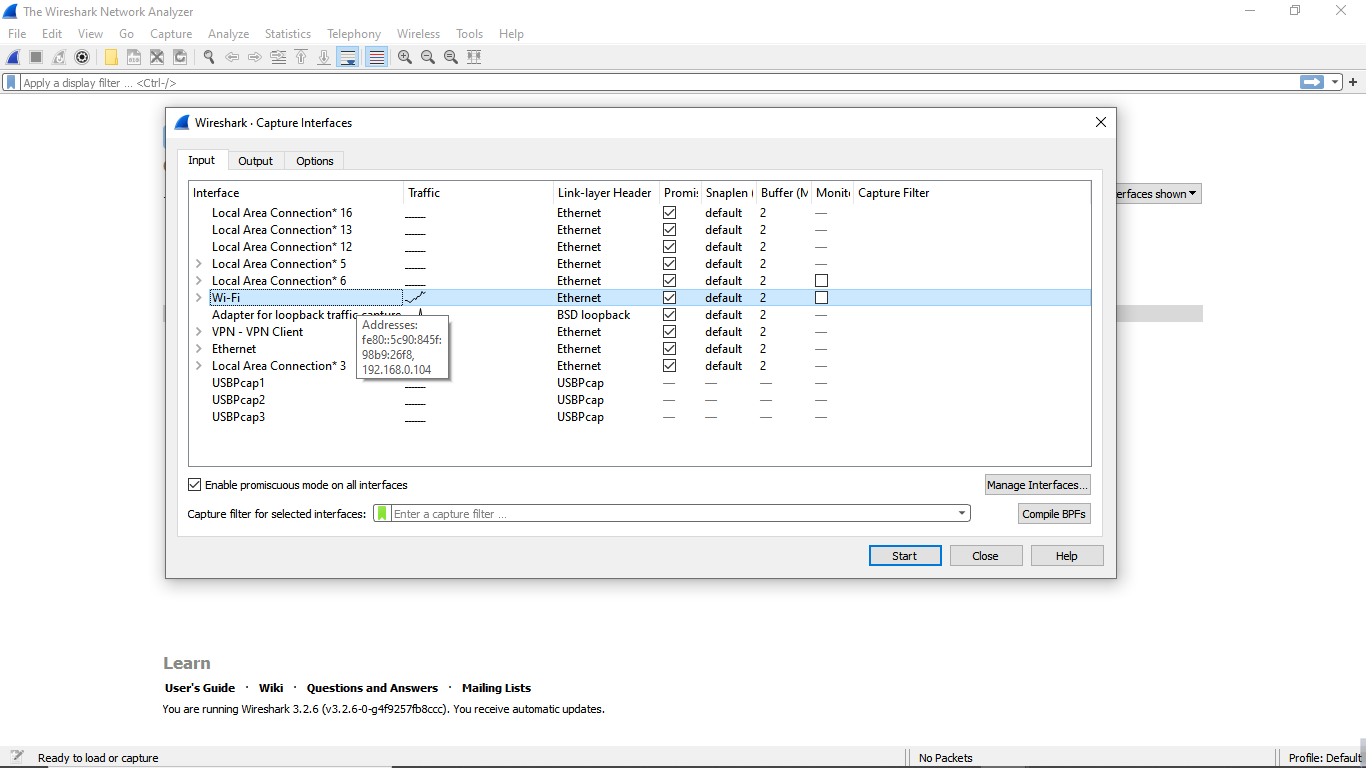
By clicking Capture menu the process of capturing will be started. It will show the available interfaces list. Then, we need to start Capturing on interface that has IP address

The packet capture will display the details of each packet as they were transmitted over the wireless LAN. Same process goes for Ethernet cable.

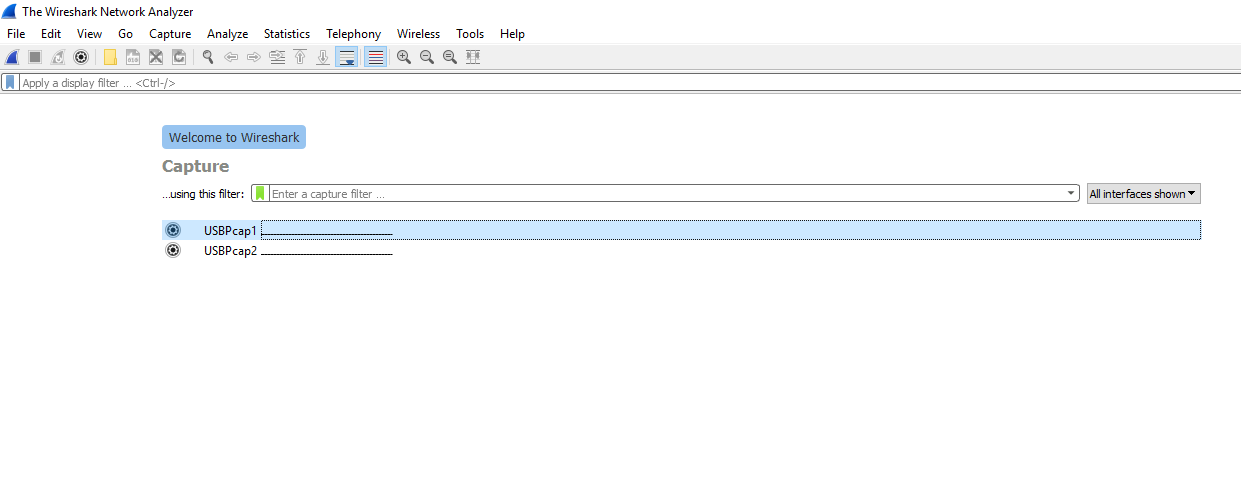
Capturing can be stopped by clicking on Stop the running capture button on the main toolbar.



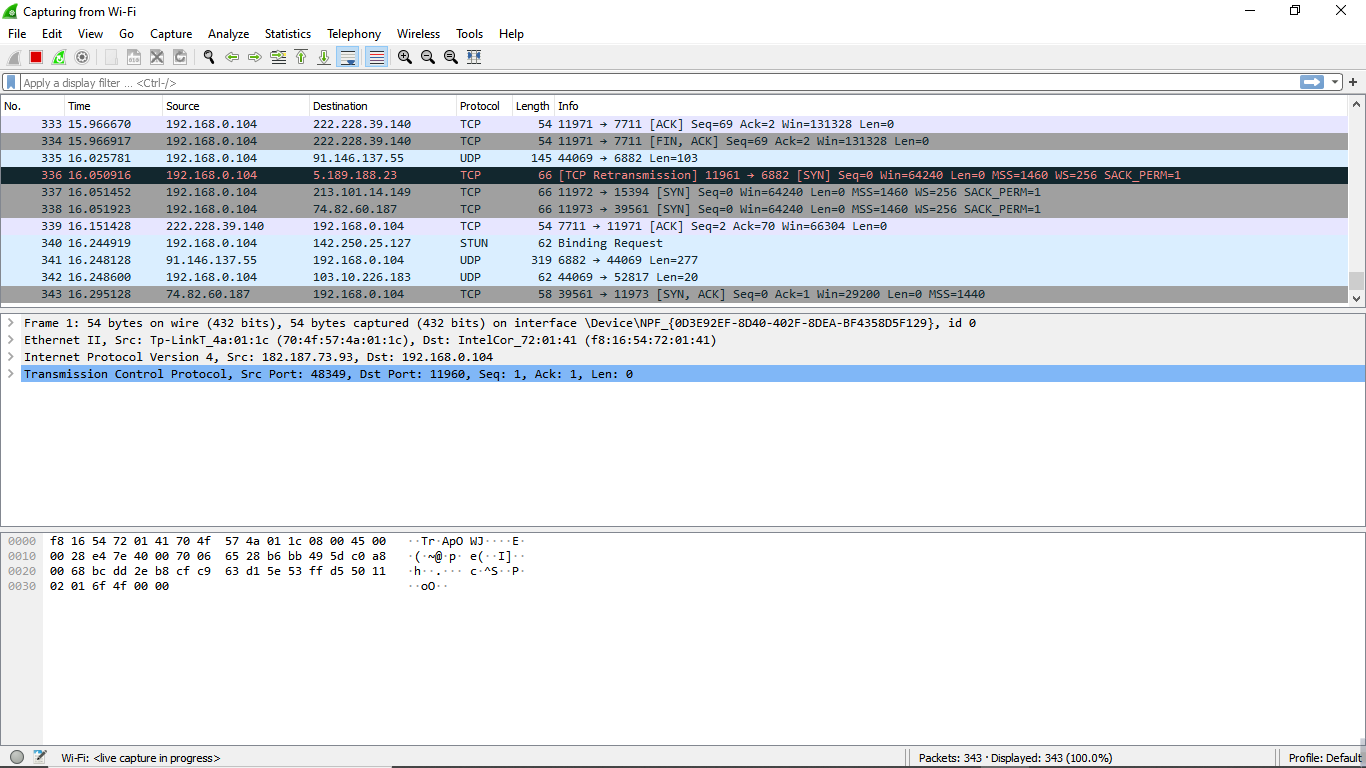
**Figure 01: Wireshark Interface List**



**Figure 02-A: Start Capturing Interface that has IP address**



**Figure 02-B: Start Capturing Interface that has for USB Tethering(Wired)**

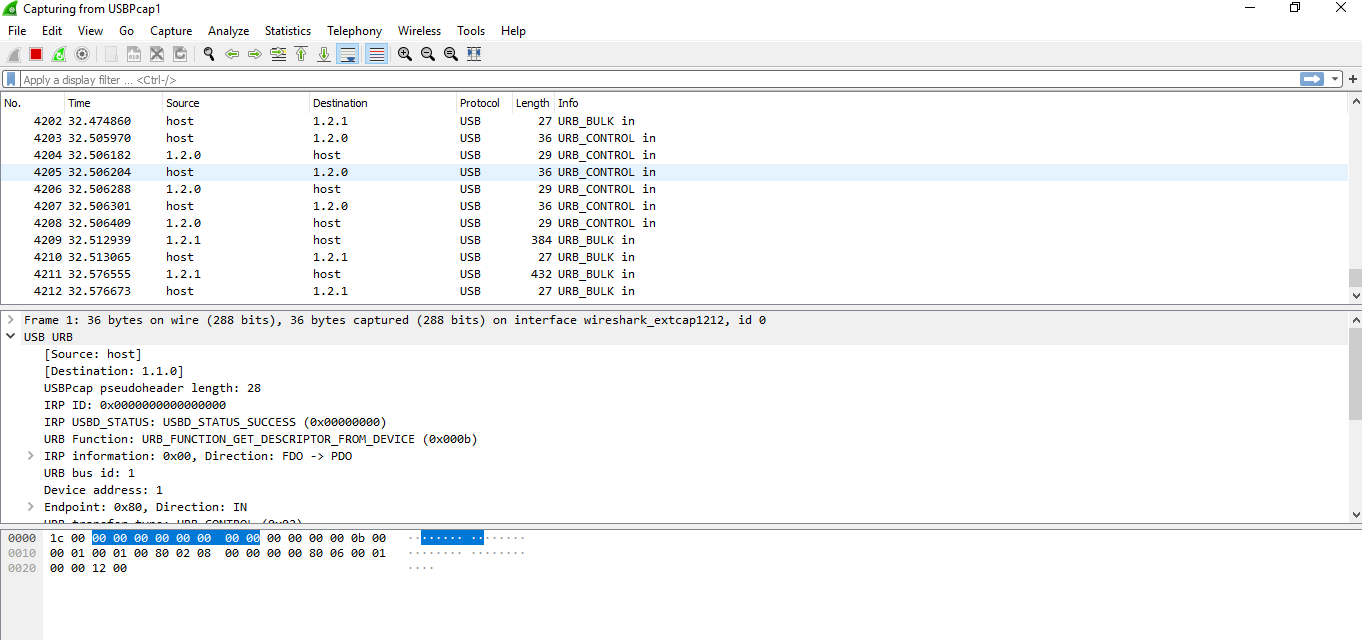


Packet bytes pane

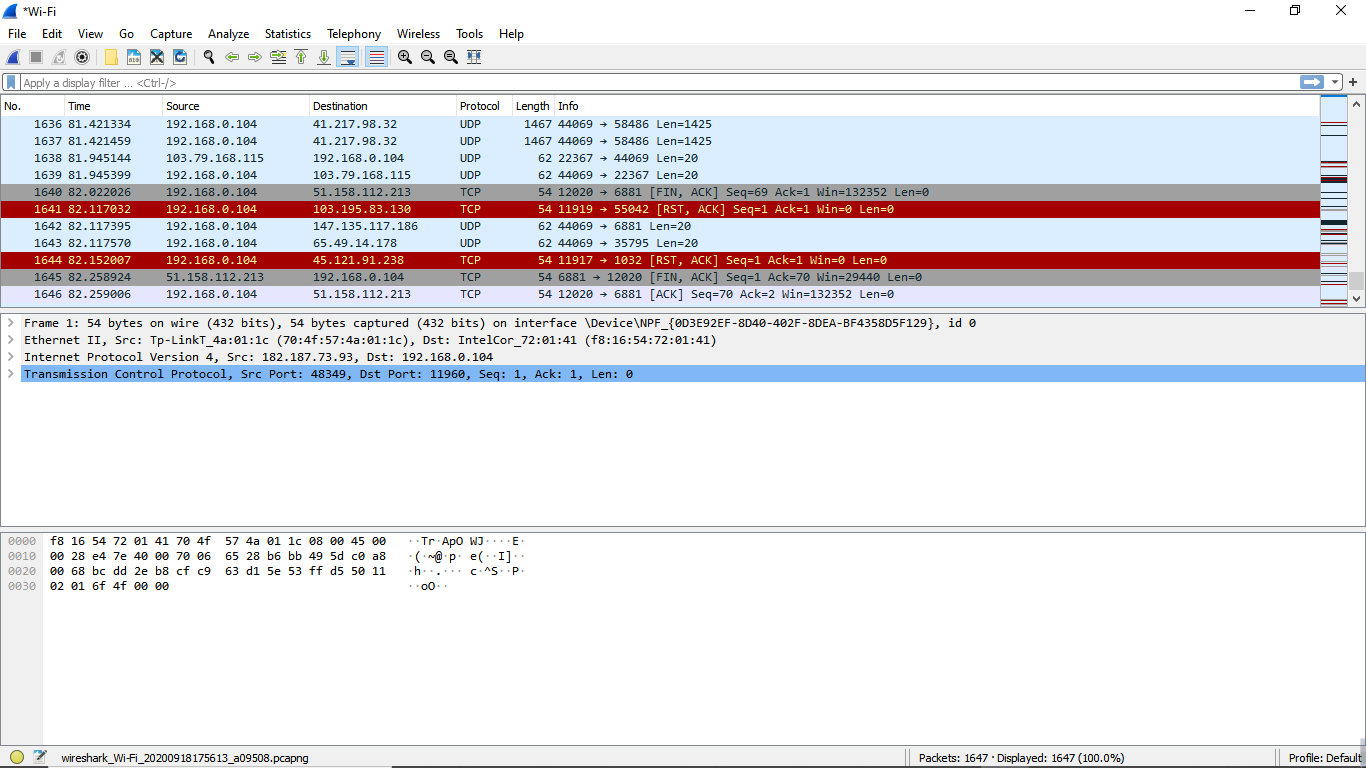
Packet details pane

Packet list pane

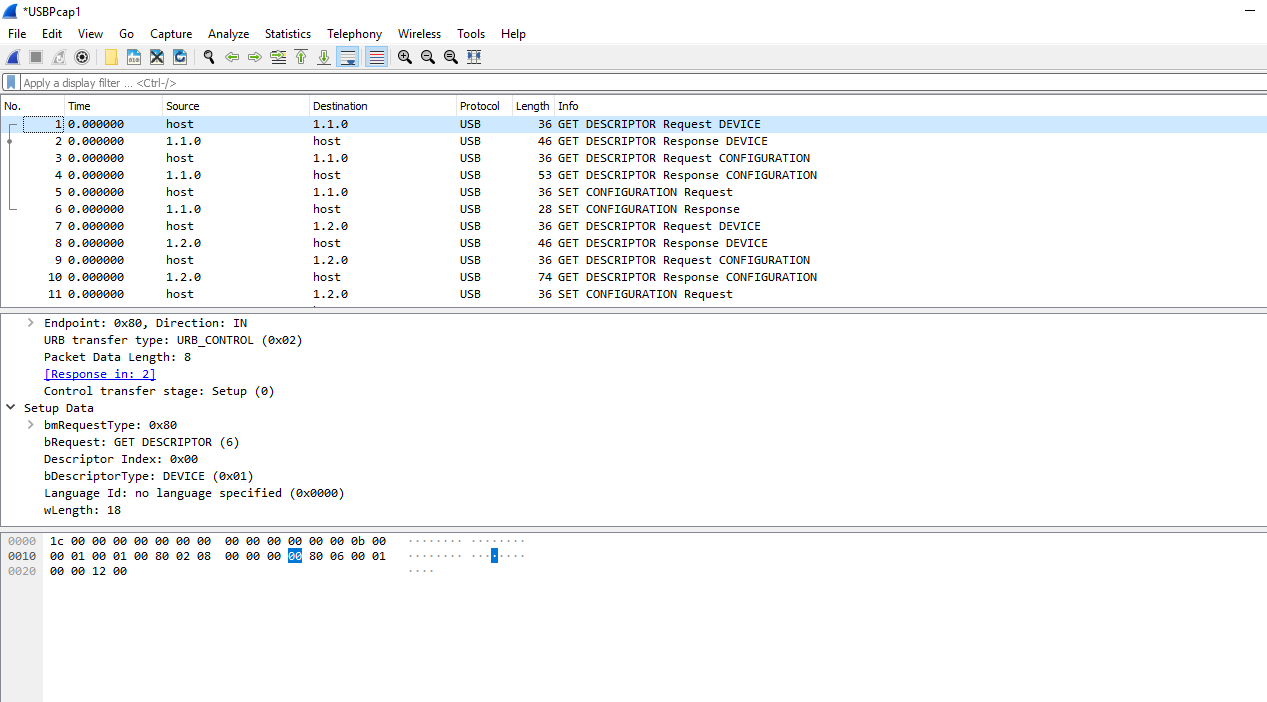
**Figure 03-A: A sample packet capture window(wireless)**

****

**Figure 03-B: A sample packet capture window for Wired Data Pack**

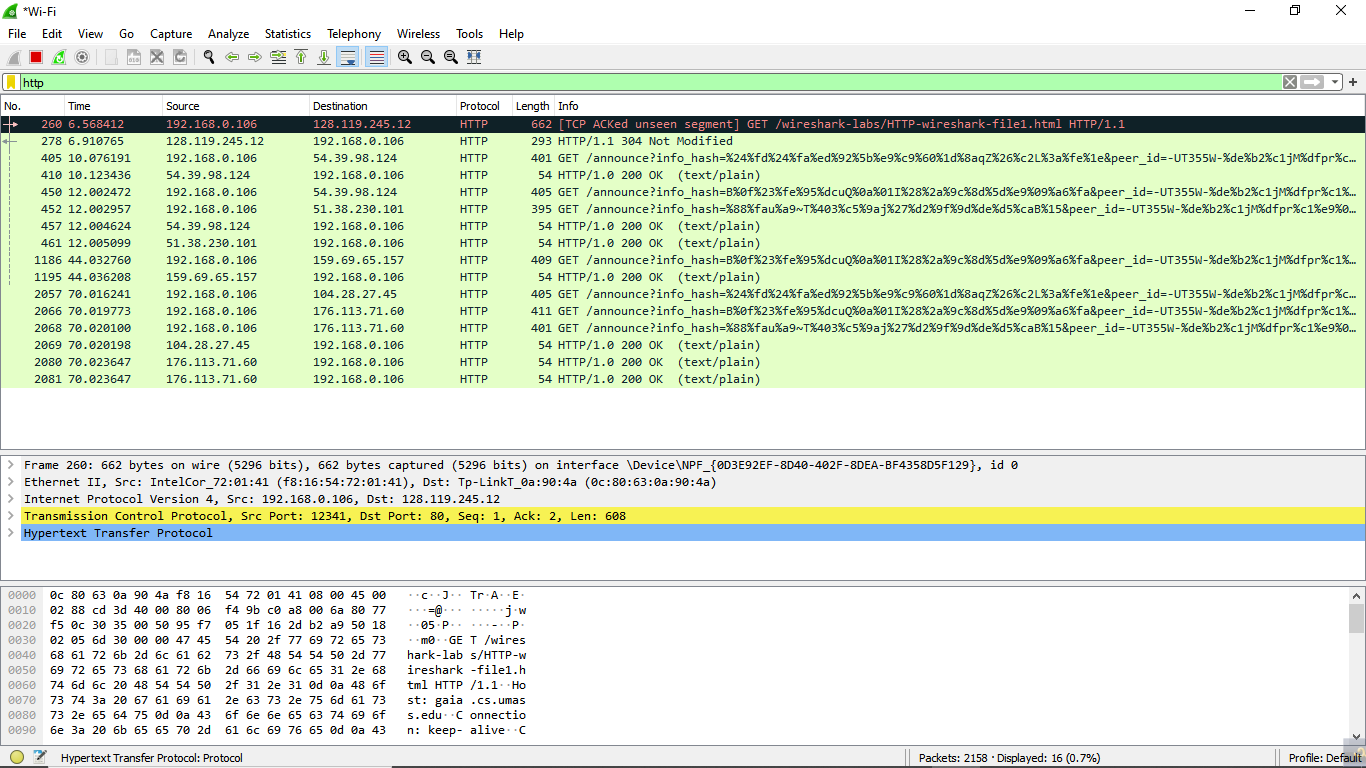


**Figure 04-A: Stopping Capture(wireless)**

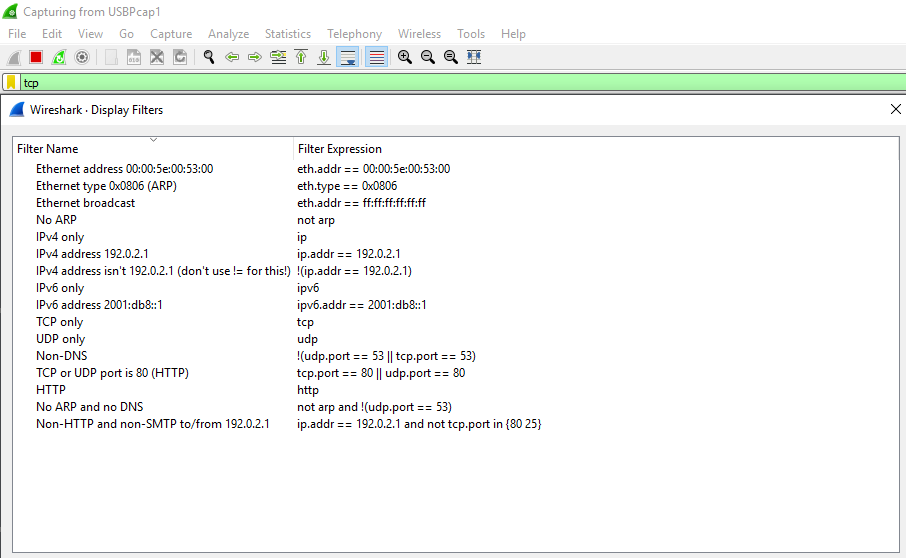
****

**Figure 04-B: Stopping Capture for Wi-Fi (Wired)**

**Filtering:**



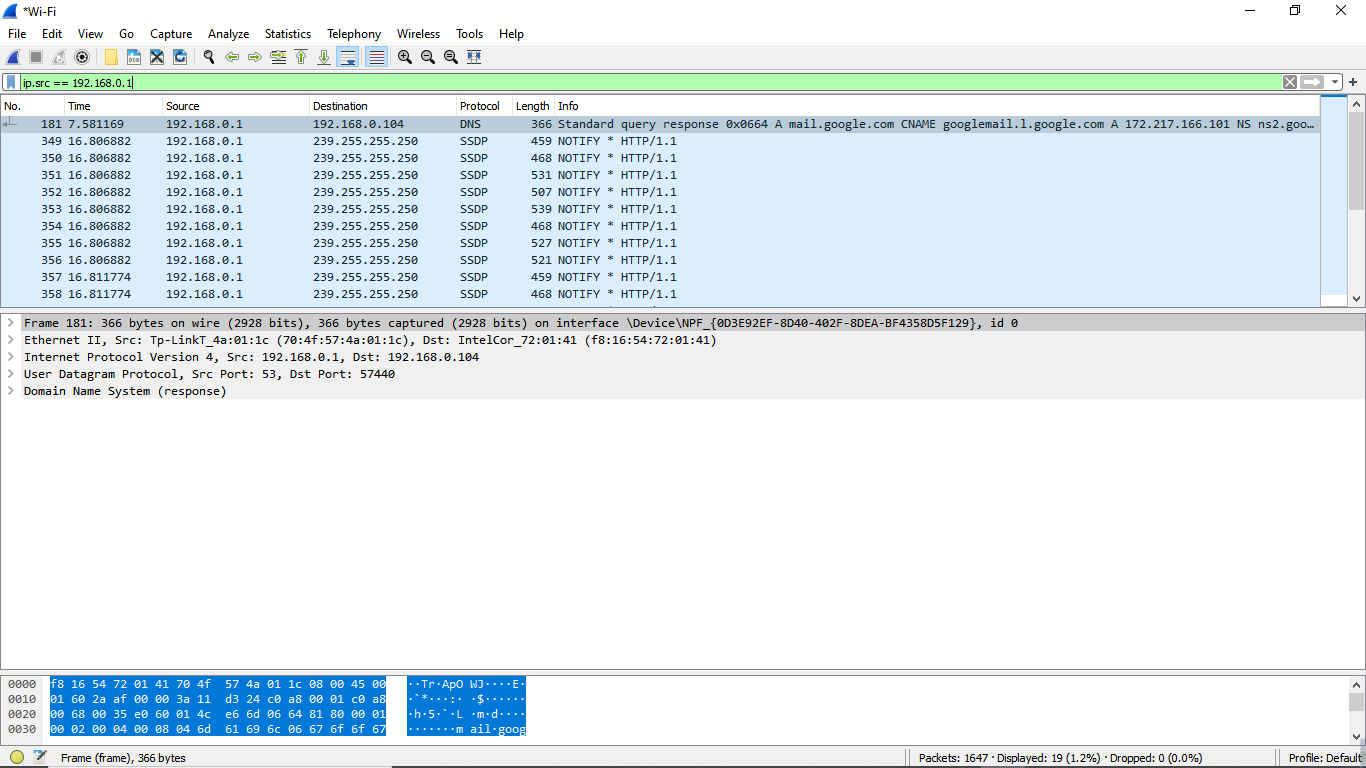
**Figure 05-A: Filter by HTTP Protocol(wireless)**

****

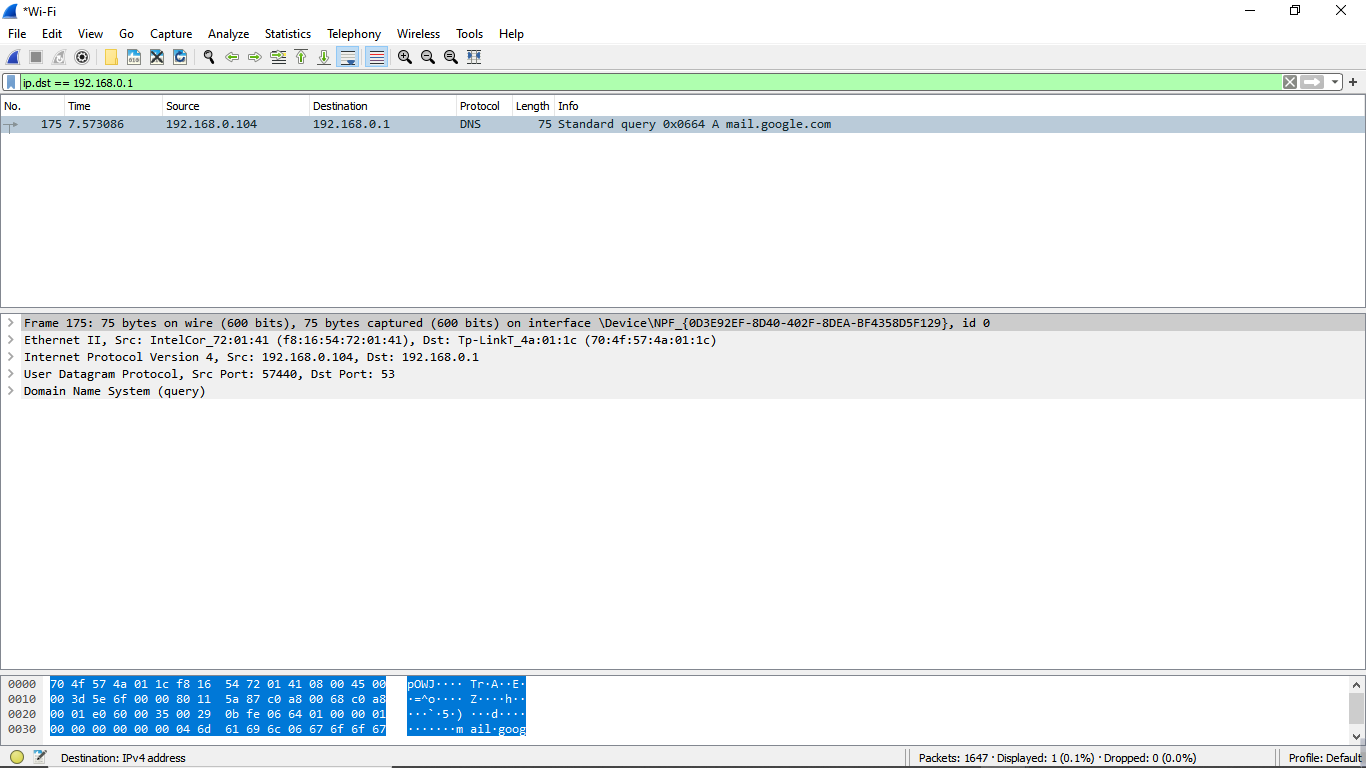
**Figure 05-B: Filter by Protocol (Wired Data Packages)**

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**

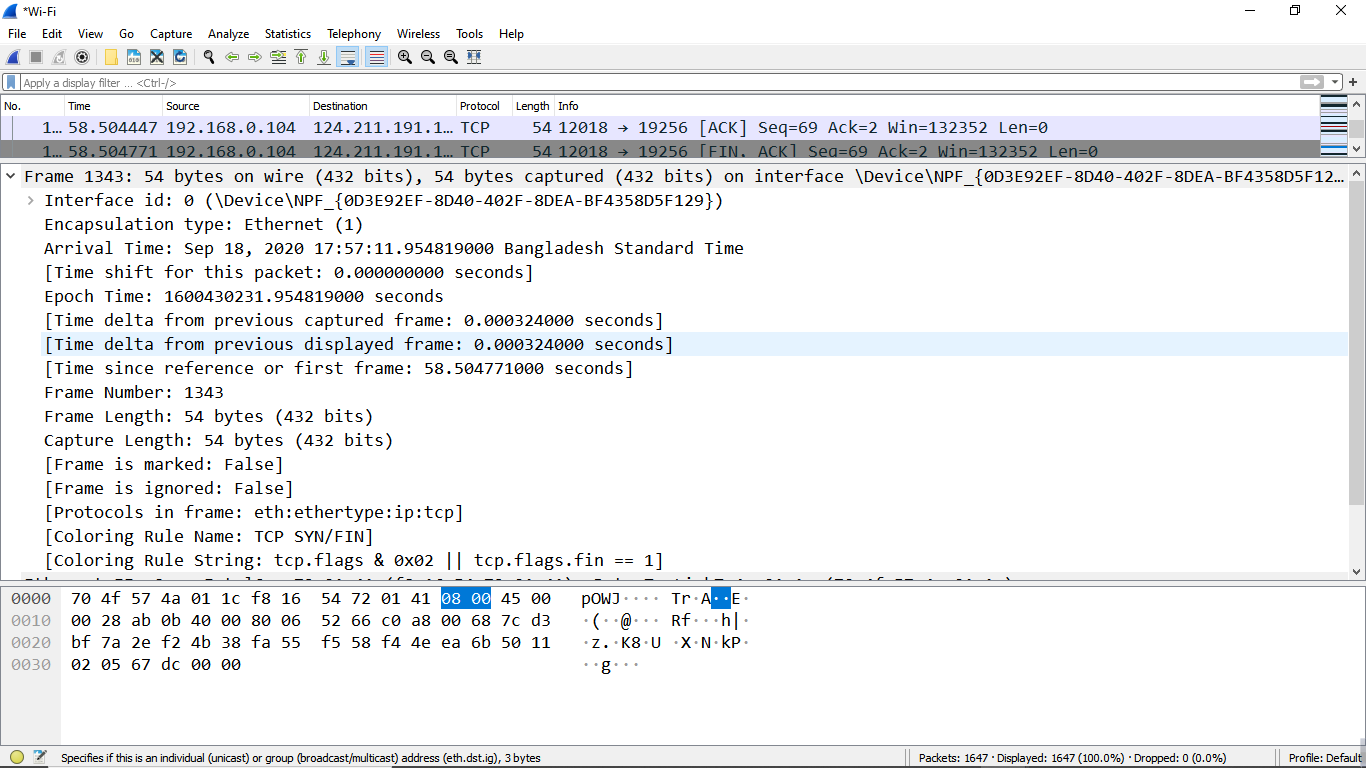


**Figure 07: Destination IP filter**

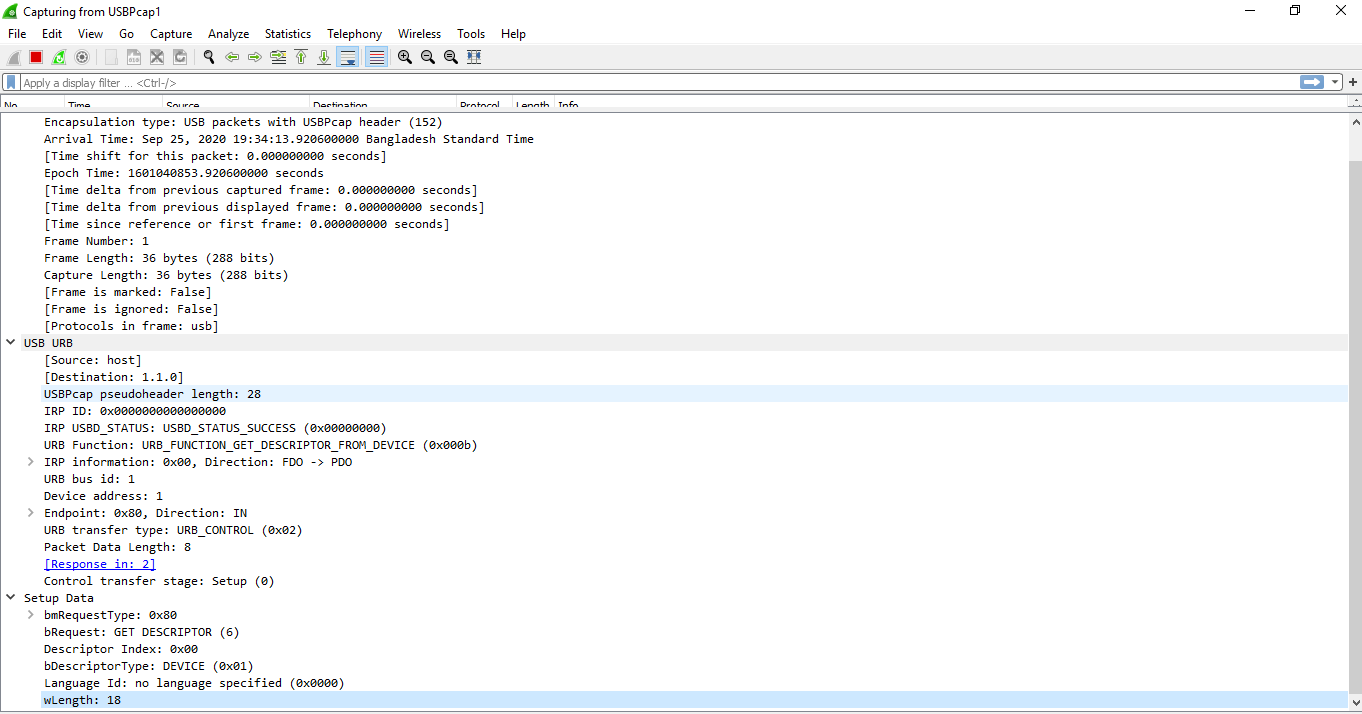
**• Packets and protocols can be analyzed after capture**

**• Individual fields in protocols can be easily seen**

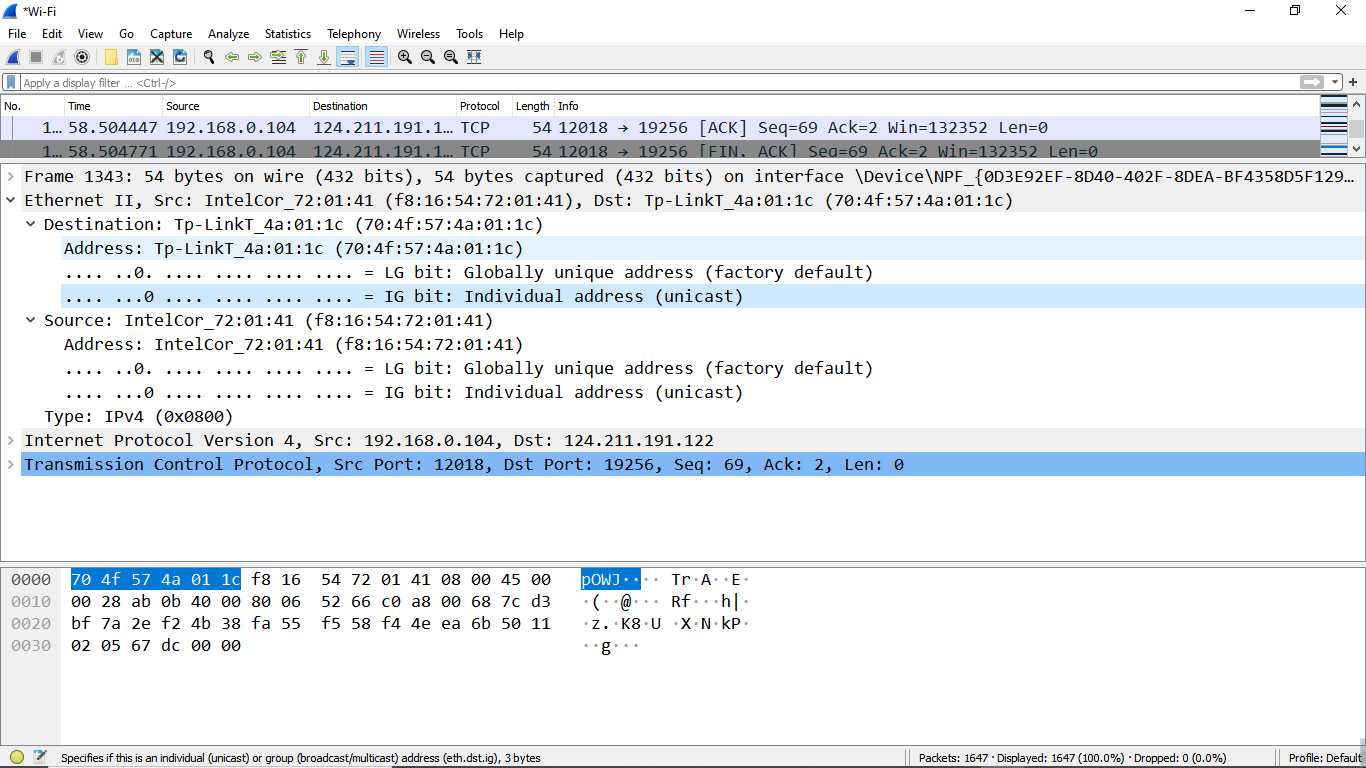
**• Graphs and flow diagrams can be helpful in analysis**



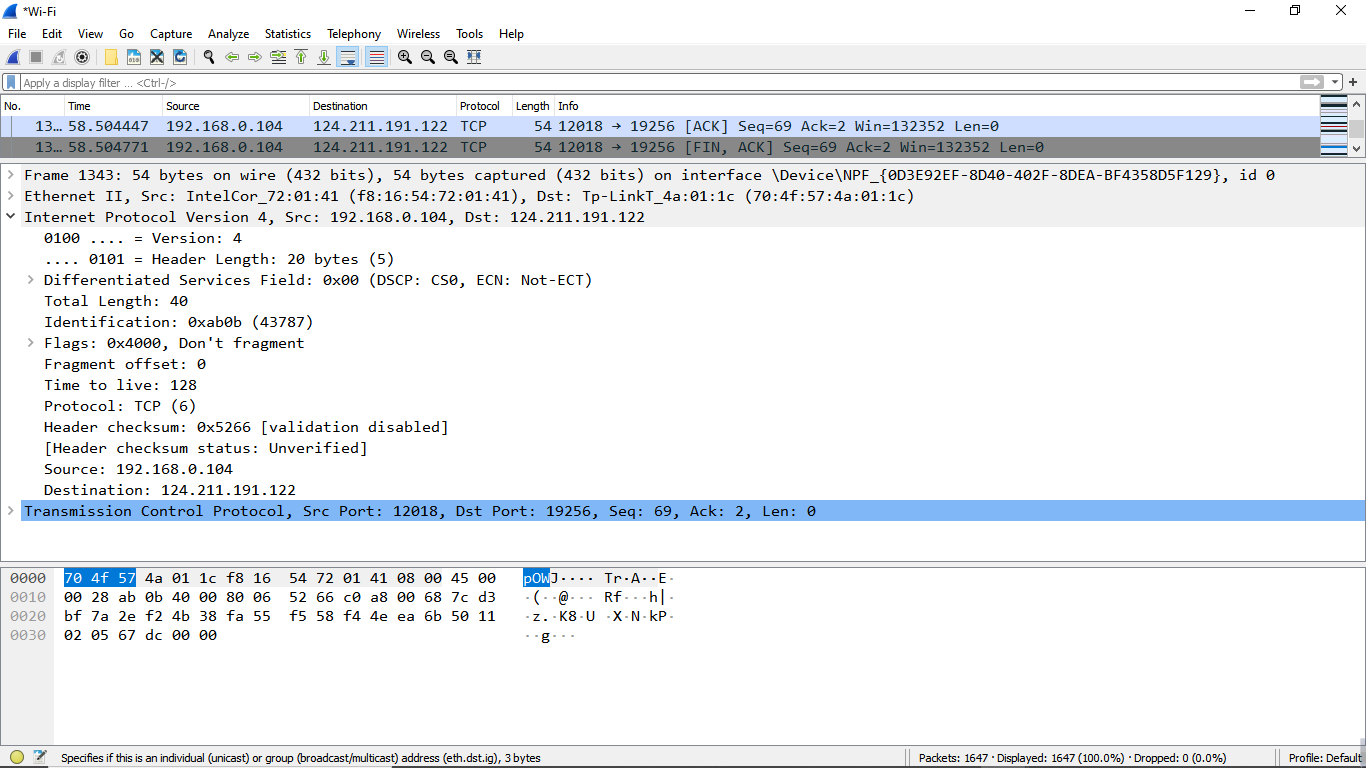
**Figure 08-A: Packet Details Pane(Frame segment) in wireless**

****

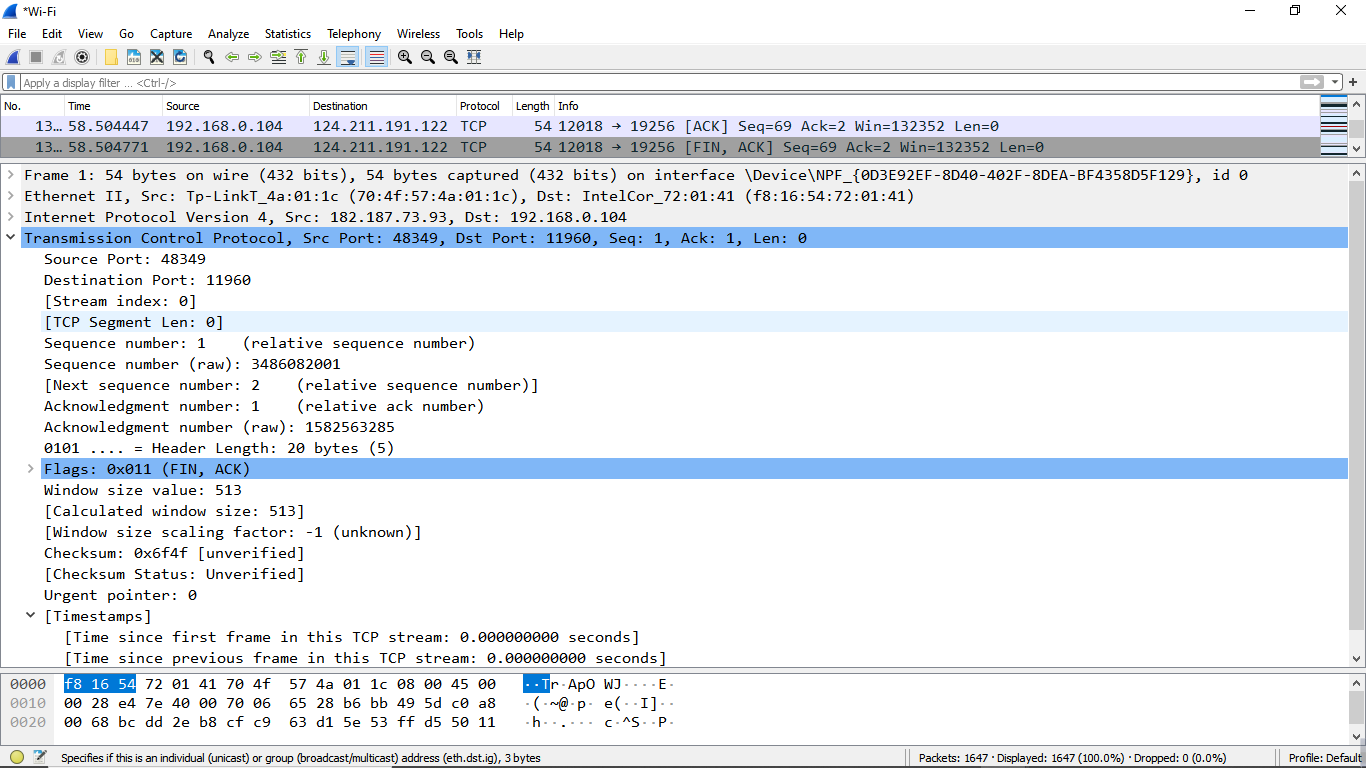
**Figure 08-B: Packet Details Pane (Frame segment) for Wired Data Packages.**



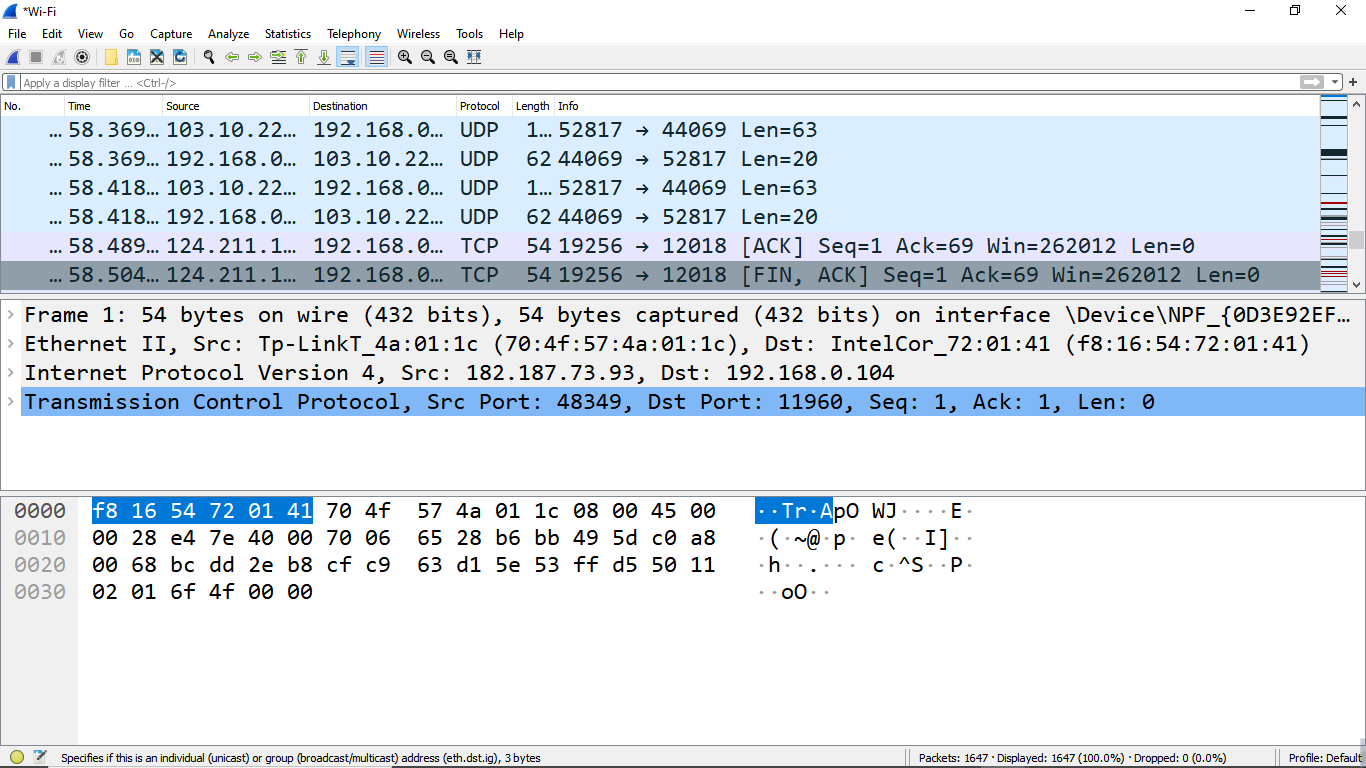
**Figure 09: Packet Details Pane (Ethernet Segment)-wireless**



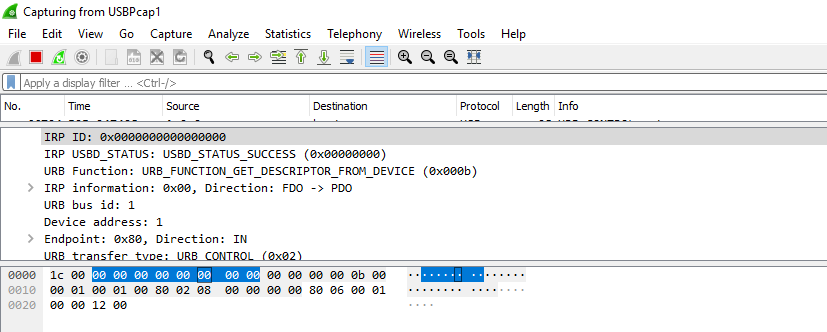
**Figure 10: Packet Details Pane(IP segment)-wireless**



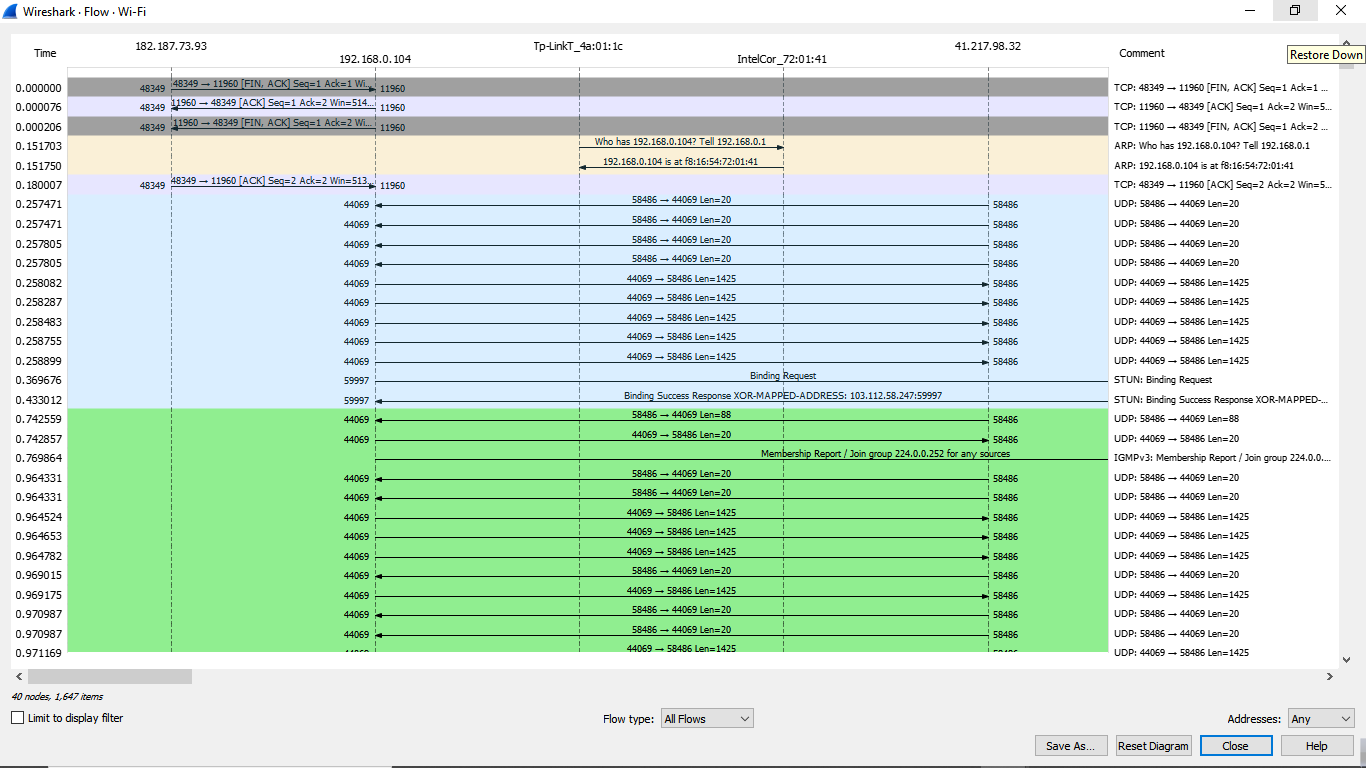
**Figure 11: Packet Details Pane (TCP Segment)-wireless**



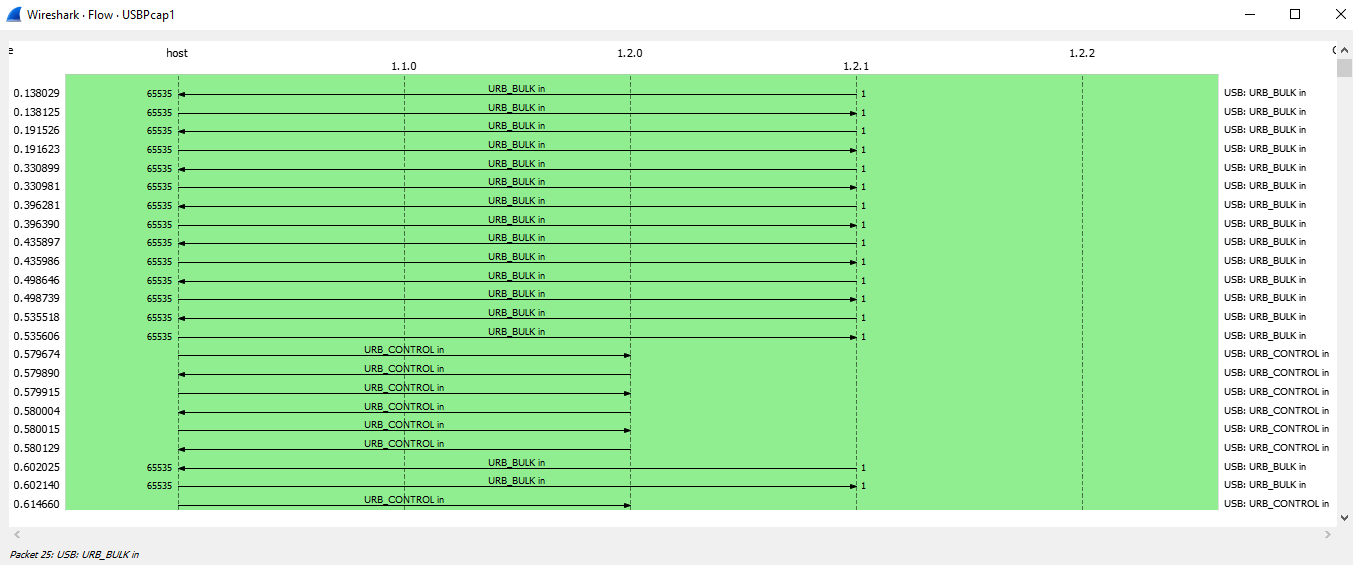
**Figure 12-A: Packet Byte Pane(wireless)**

****

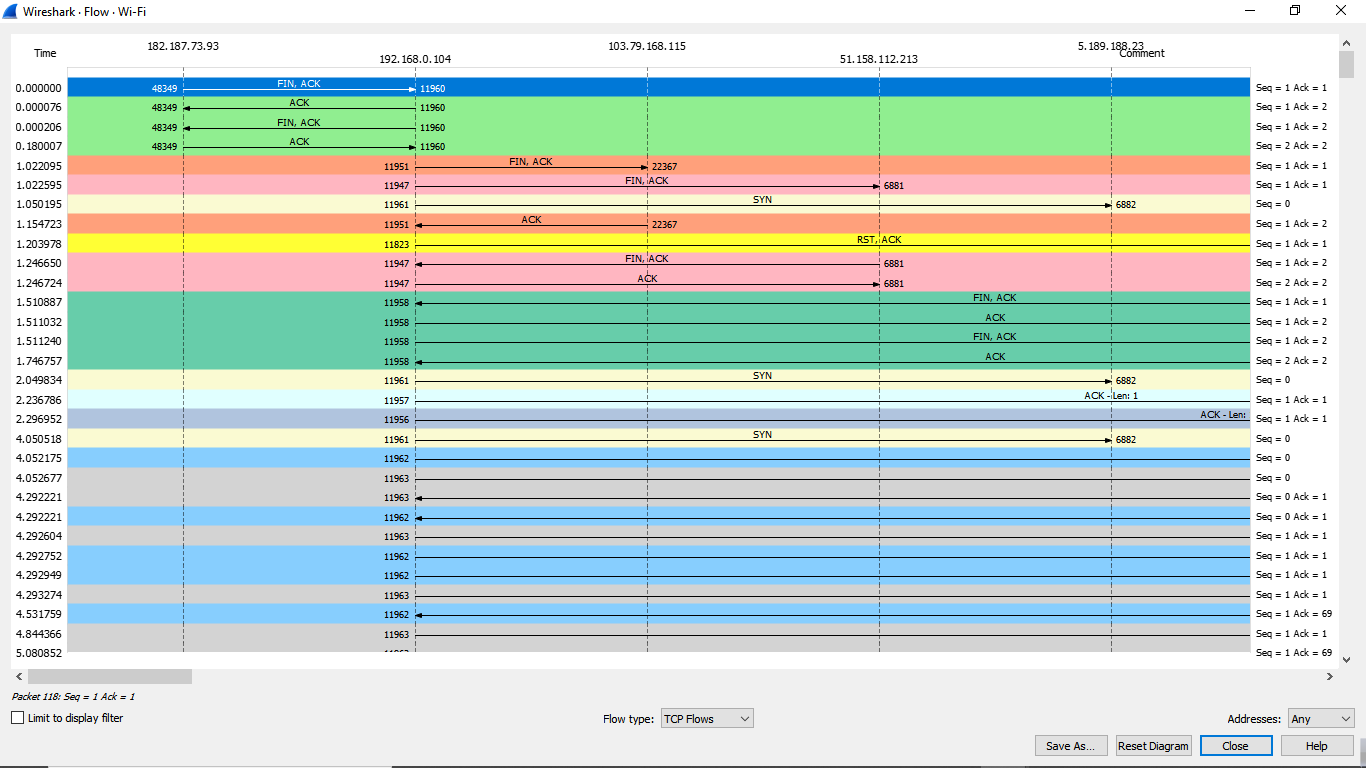
**Figure 12-B: Packet Byte Pane for Wireless (USB Tethering)**



**Figure 13: Statistics- Flow Graph(All Flows)- Wireless**

****

**Figure 13-A: Statistics- Flow Graph -All Flows for Wi-Fi (Wired Data Packages)**



**Figure 13-B: Statistics- Flow Graph(TCP Flows)-wireless**

**Conclusion:**

By using wireshark both wired and wireless data transmission can be captured very easily. We can capture the transmission in wired connection in multiple ways, but wireshark made it simple for the user. So whenever we need to troubleshoot any problem or analysis of any kind of protocol transmission we can use wireshark very conveniently. There we can see the data transmission flow is little bit faster and more secure in wired connection than the wireless. The statistical flow graph also covers the comparison between all flows in the network.