

# 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: 18.09.2020

Date of Submission: 25.09.2020

### **Submitted by**

Name: Raisa Jerin Sristy

ID:IT-16056

 $4^{th}$  year  $2^{nd}$ semester

Session: 2015-2016

Dept. of ICT

MBSTU.

### **Submitted To**

Nazrul Islam

**Assistant Professor** 

Dept. of ICT

MBSTU.

### **LAB NO.:05**

## <u>Name of Experiment:</u> Comparative Analysis of Wired and Wireless data using Wireshark <u>Objectives:</u>

- 1. To capture a wired data packet from interface and comparing the analysis with wireless data packet.
- 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 start Capturing, by clicking Capture menu and selecting two interface that one has wireless data packet and another is wired data packet. The captured packet will put on the show of the details of each packet transmitted over the wireless LAN and Ethernet. This process can be stopped by clicking on Stop capture button.

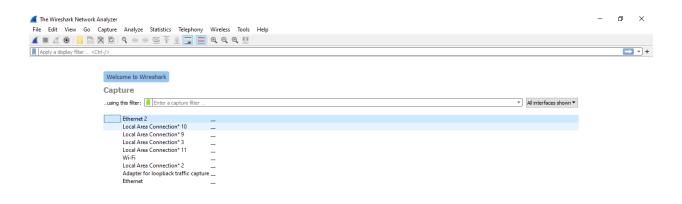


Figure: Wireshark Interface List

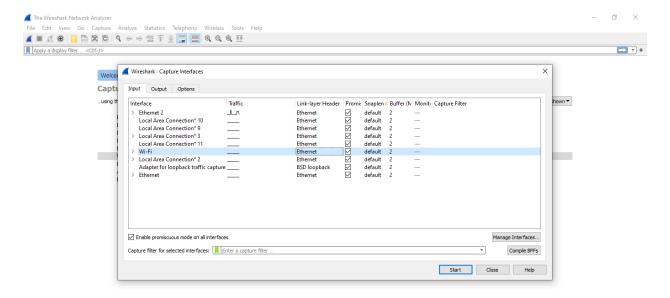


Figure: Start Capturing Interface for Wireless data packets (WiFi)

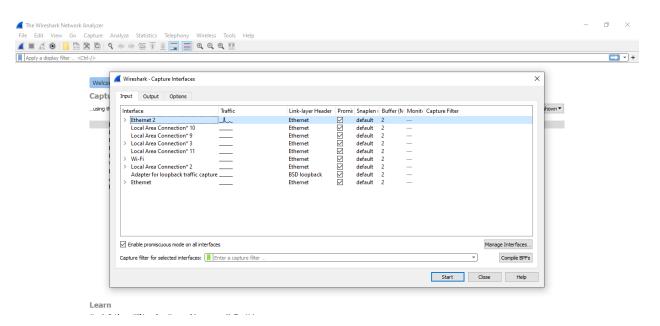


Figure: Start Capturing Interface for Wired data packets (Ethernet 2)

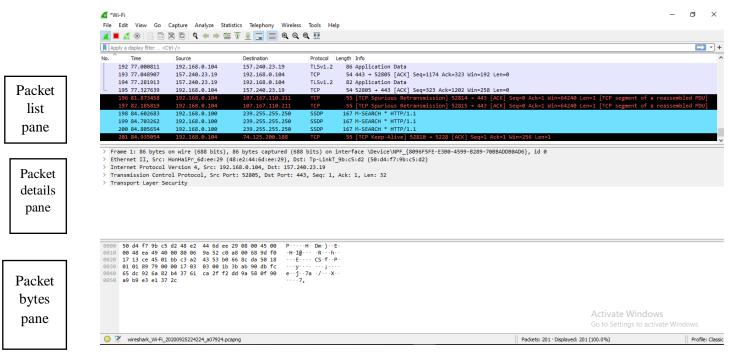


Figure: A sample packet capture window for Wireless Data Packets

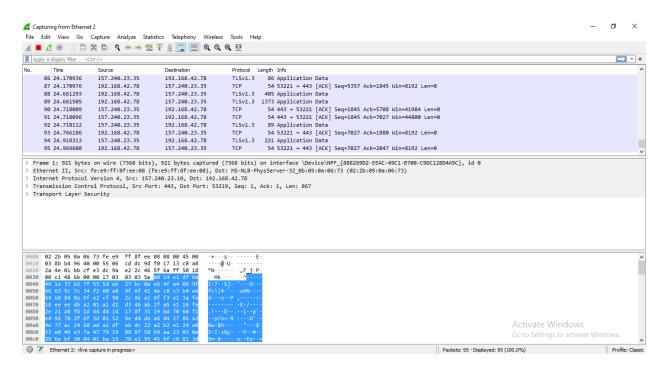


Figure: A sample packet capture window for Wired Data Pack

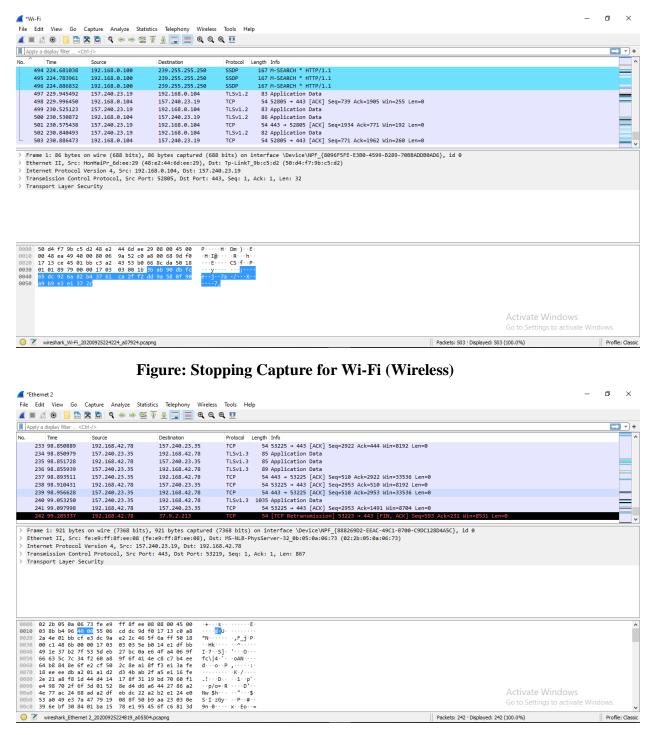


Figure: Stopping Capture for Wi-Fi (Wired)

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

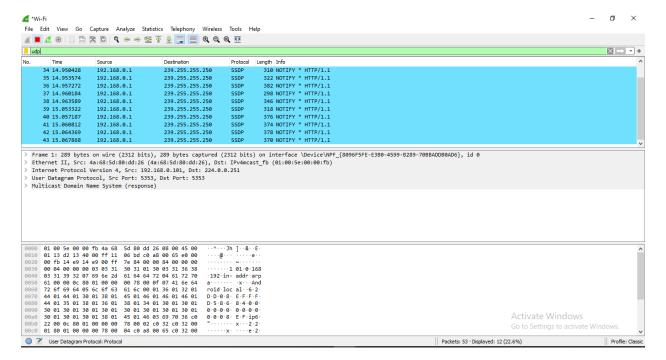


Figure: Filter by Protocol Wireless Data Packets

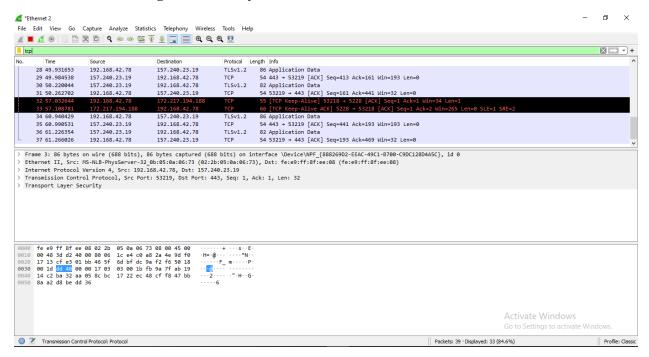


Figure: Filter by Protocol Wired Data Packets

```
Prame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{88826902-EEAC-49C1-8700-C90C12804ASC}, id 0

> Interface id: 0 (\Device\NPF_{18826902-EEAC-49C1-8700-C90C12804ASC})
Encapsulation type: Ethernet (1)
Arrival Time: sep 25, 2020 22:53:31.248737000 Bangladesh Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1601052751.248737000 seconds
[Time delta from previous captured frame: 3.935316000 seconds]
[Time delta from previous captured frame: 5.935363000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.0000000000 seconds]
[Time since reference or first frame: 5.935363000 seconds]
Frame Number: 3
Frame Length: 86 bytes (688 bits)
Capture Length: 86 bytes (688 bits)
[Frame is ignored: False]
[Fr
```

Figure: Packet Details Pane (Frame segment) for Wired Data Packets.

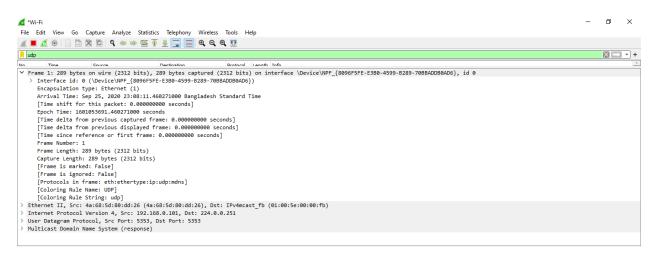


Figure: Packet Details Pane (Frame segment) for Wireless Data Packets.



Figure: Packet Byte Pane for Wired data packet (USB Tethering)

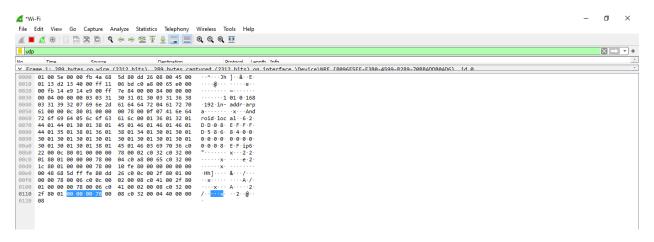


Figure 07-B: Packet Byte Pane (For Wi-Fi)



Figure 08-A: Statistics- Flow Graph -All Flows for Wi-Fi (Wireless Data Packages)

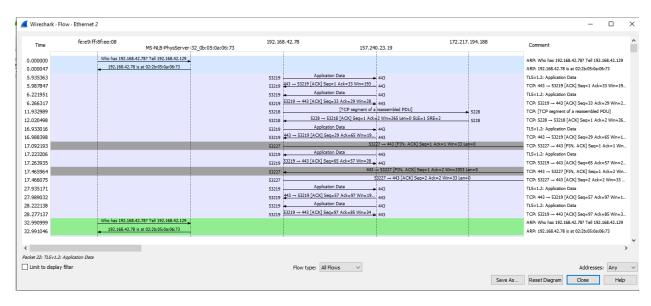


Figure 08-B: Statistics- Flow Graph -All Flows for Ethernet2(Wired Data Packages)

### **Conclusion:**

Here in this experiment, using Wireshark live packet data from a network interface can be captured easily whether it is wired or wireless. Applying a display filter particular traffic can be monitored in both cases. Wired network is much more efficient than wireless network. Because wired data packages transfer rate are very much faster than wireless.

All tasks have been done perfectly.