

# 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: Md. Fahim Ferdous Khan

ID:IT-16018

4<sup>th</sup> year 2<sup>nd</sup>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:**

- 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.

#### **Capturing Packets:**

First off, clicking on Capture menu the capturing process will be started. It shows all available interfaces list. After that we need to start capturing an interface that has IP Address.

The packet capture will display the details of each packet as they were transmitted over the wireless LAN.

We can stop capturing by clicking on the Stop the running capture button on the main toolbar.

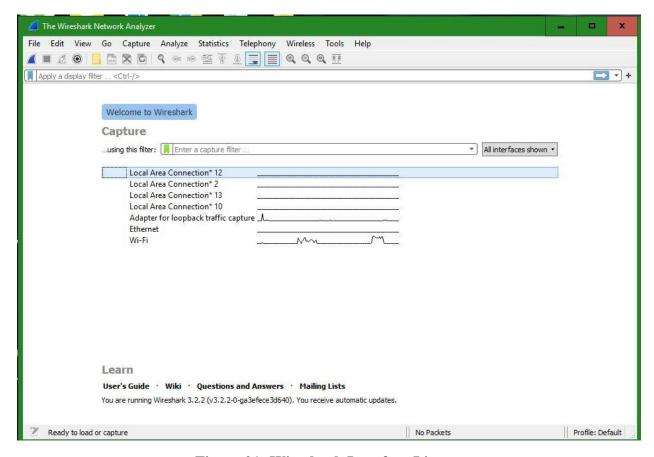


Figure 01: Wireshark Interface List

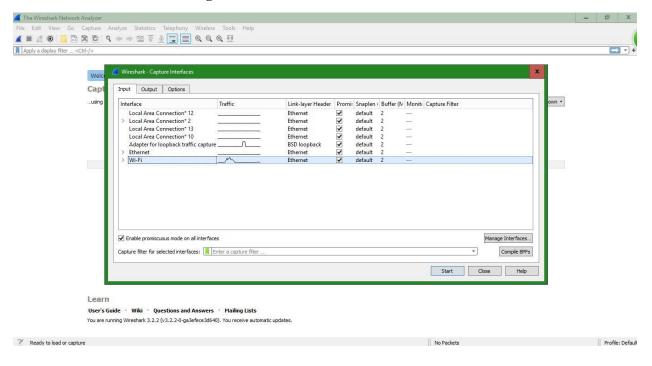


Figure 02: Start Capturing Interface that has IP address

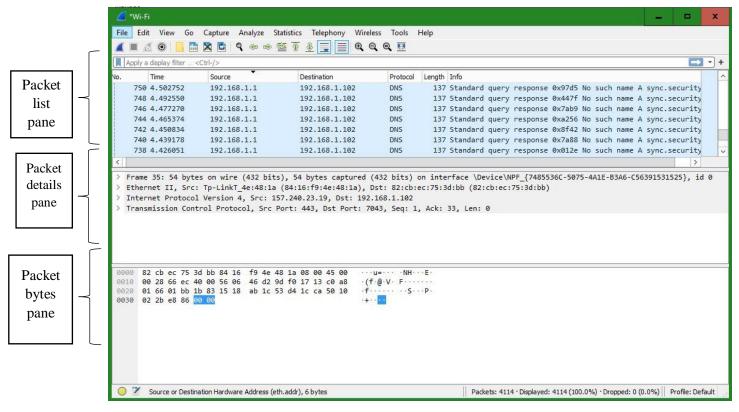


Figure 03: A sample packet capture window

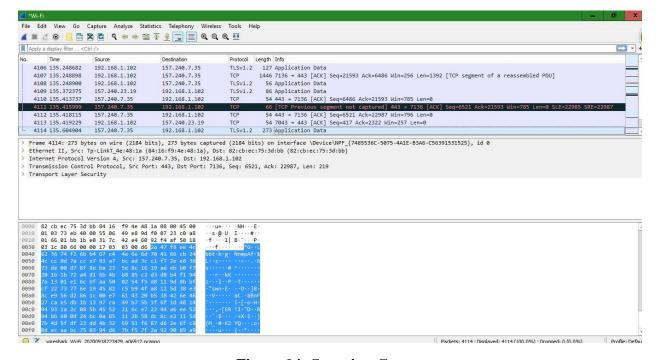


Figure 04: Stopping Capture

#### **Filtering:**

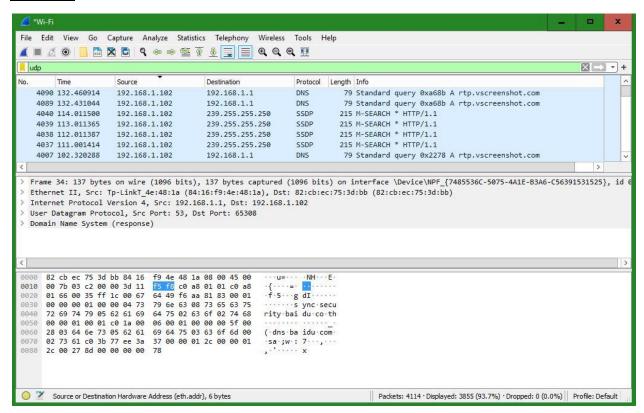


Figure 05: Filter by Protocol

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.

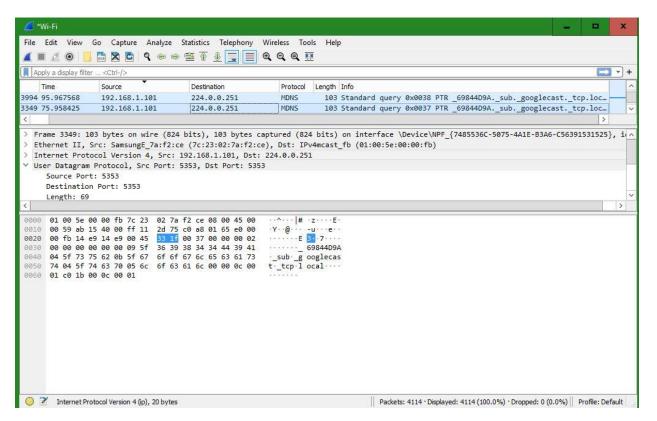


Figure 06: Source IP filter

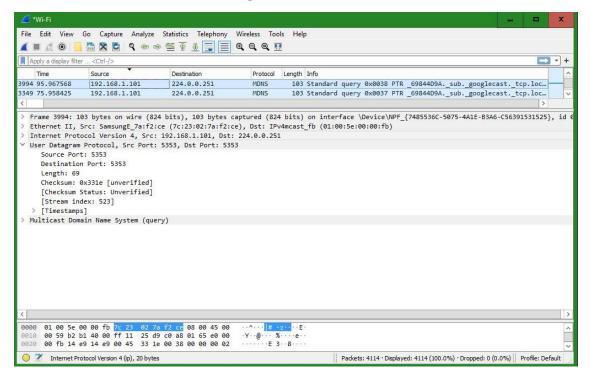


Figure 07: Destination IP filter

- 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

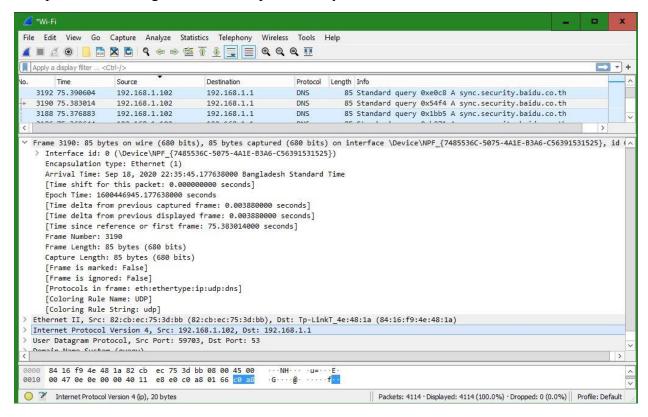


Figure 08: Packet Details Pane(Frame segment)

```
■ *Wi-Fi

                                                                                                                                           File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
                                                 Protocol Length Info
1... 58.504447 192.168.0.104 124.211.191.1... TCP 54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
1... 58.504771 192.168.0.104 124.211.191.1... TCP 54 12018 → 19256 [FIN. ACK] Seq=69 Ack=2 Win=132352 Len=0
                                                                                                                                               Frame 1343: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{@D3E92EF-8D40-402F-8DEA-BF4358D5F129...
Ethernet II, Src: IntelCor 72:01:41 (f8:16:54:72:01:41), Dst: Tp-LinkT 4a:01:1c (70:4f:57:4a:01:1c)
  v Destination: Tp-LinkT 4a:01:1c (70:4f:57:4a:01:1c)
      Address: Tp-LinkT_4a:01:1c (70:4f:57:4a:01:1c)
       ......0. .... := LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  v Source: IntelCor_72:01:41 (f8:16:54:72:01:41)
      Address: IntelCor_72:01:41 (f8:16:54:72:01:41)
      .... .0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.0.104, Dst: 124.211.191.122
  Transmission Control Protocol, Src Port: 12018, Dst Port: 19256, Seq: 69, Ack: 2, Len: 0
       70 4f 57 4a 01 1c f8 16 54 72 01 41 08 00 45 00
                                                               DOWJ · · · Tr·A··E
0010 00 28 ab 0b 40 00 80 06 52 66 c0 a8 00 68 7c d3
                                                              · ( · · @ · · · Rf · · · h | ·
 0020 bf 7a 2e f2 4b 38 fa 55 f5 58 f4 4e ea 6b 50 11
                                                              ·z.·K8·U ·X·N·kP
0030 02 05 67 dc 00 00
                                                               · · g · ·
                                                                                                 Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%) Profile: Default
O Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes
```

Figure 09: Packet Details Pane (Ethernet Segment)

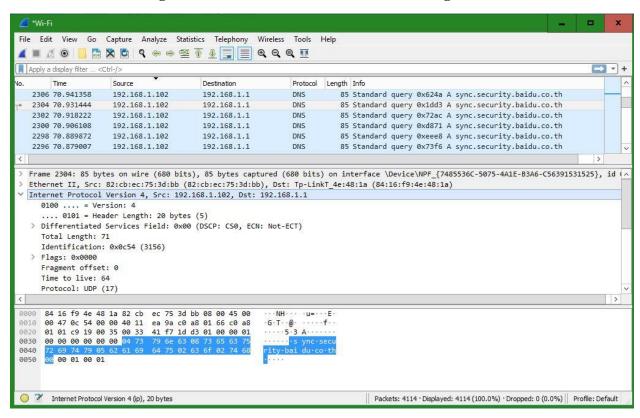


Figure 10: Packet Details Pane(IP segment)

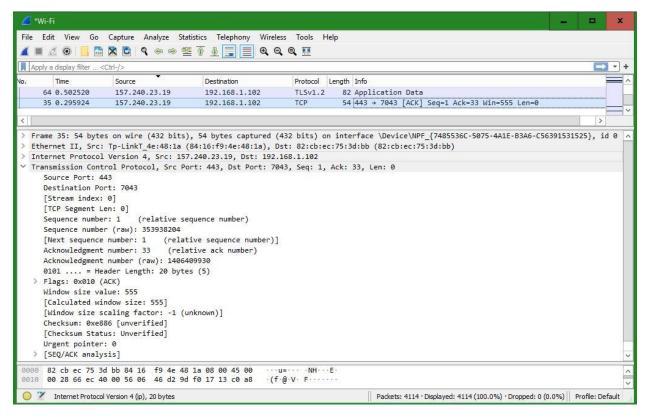


Figure 11: Packet Details Pane (TCP Segment)

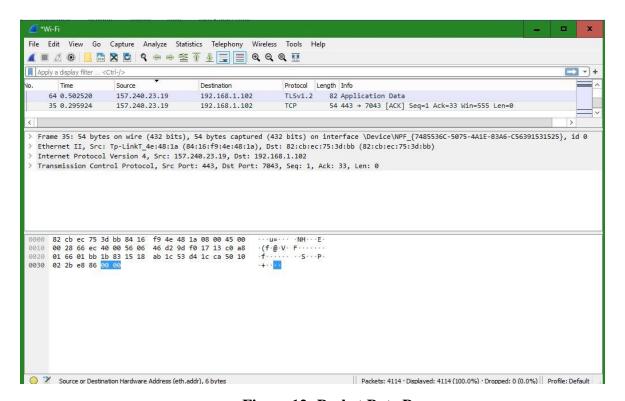


Figure 12: Packet Byte Pane

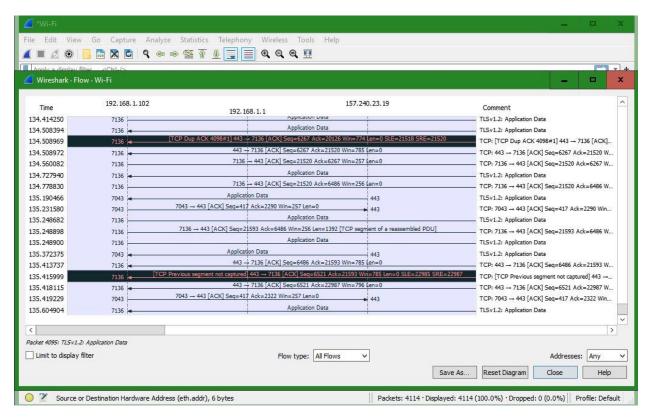


Figure 13: Statistics- Flow Graph(All Flows)

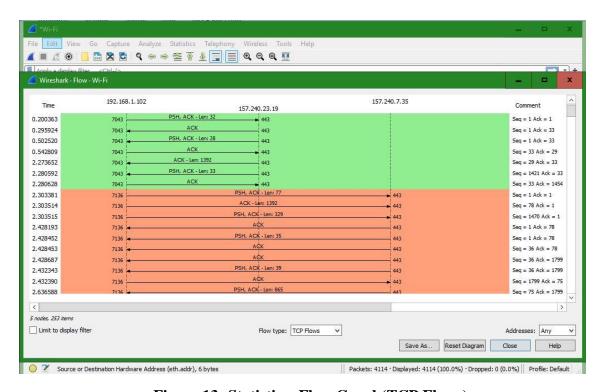


Figure 13: Statistics- Flow Graph(TCP Flows)

### **Conclusion:**

So,By Wireshark we can easily Capture live packet data from a network interface. We showed all Wireshark interface lists. Packet details are showed specifically such as IP segment, TCP segment.

The TCP Stream Throughput graph have shown us the throughput from one TCP stream, in one direction, based on the selected packet. Statistics flow graph are shown with TCP flows.