

# 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



Name: Shamsunnahar

ID: IT-16034

4<sup>th</sup> year 2<sup>nd</sup> semester

Session: 2014-2015

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:**

Data can be captured on wired or wireless medium. 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.

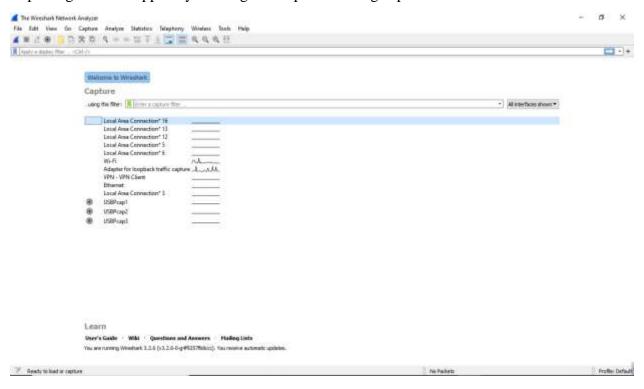


Figure 01: Wireshark Interface List

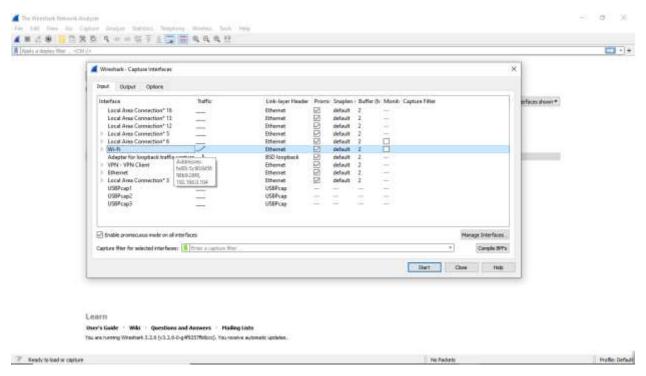


Figure 02: Start Capturing Interface that has IP address

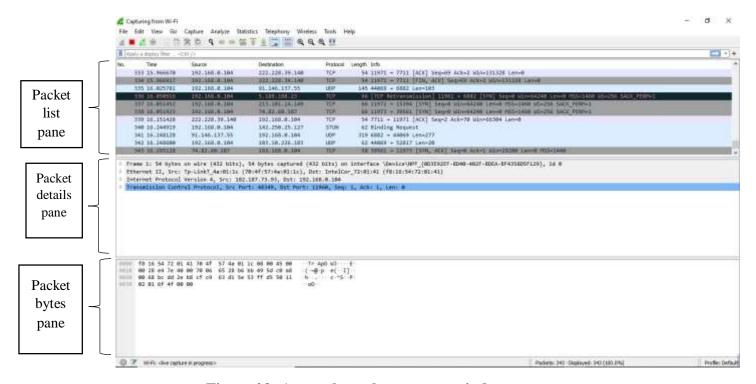


Figure 03: A sample packet capture window

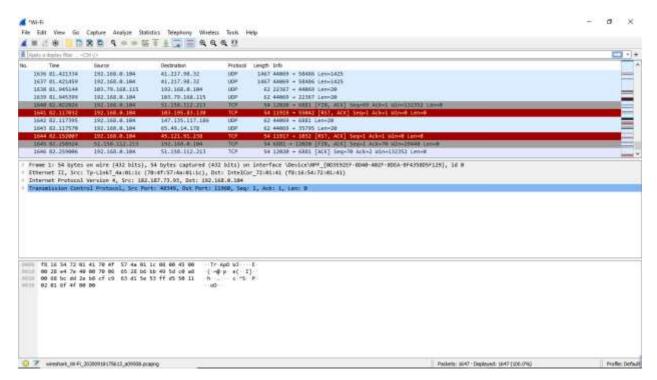


Figure 04: Stopping Capture

#### Filtering:

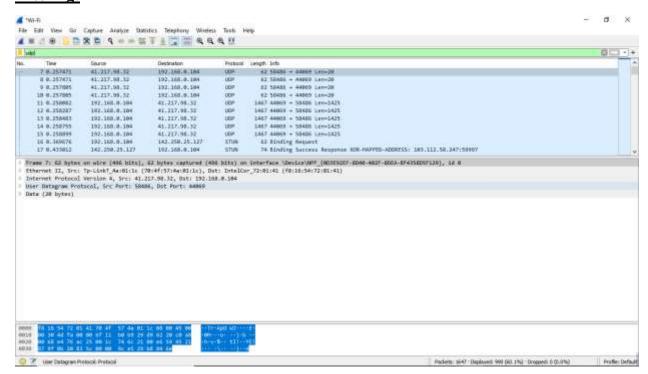


Figure 05: Filter by Protocol

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.

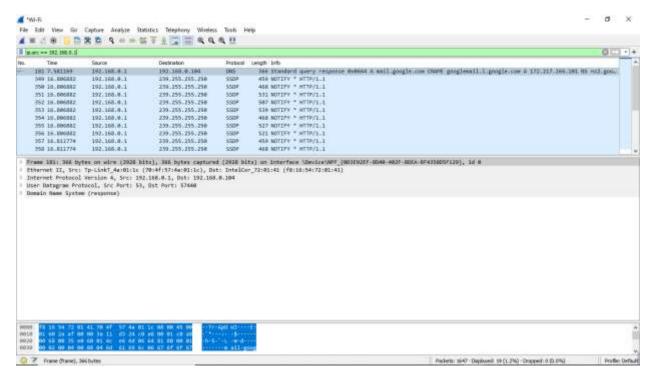
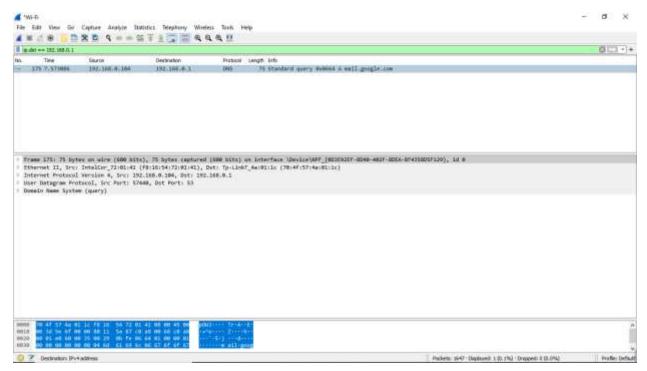


Figure 06: Source IP filter



#### 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

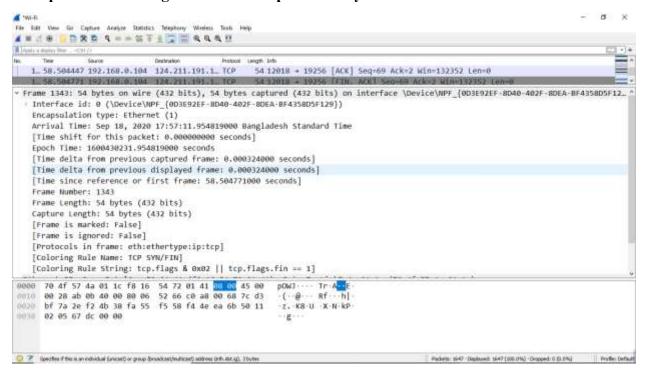


Figure 08: Packet Details Pane (Frame segment)

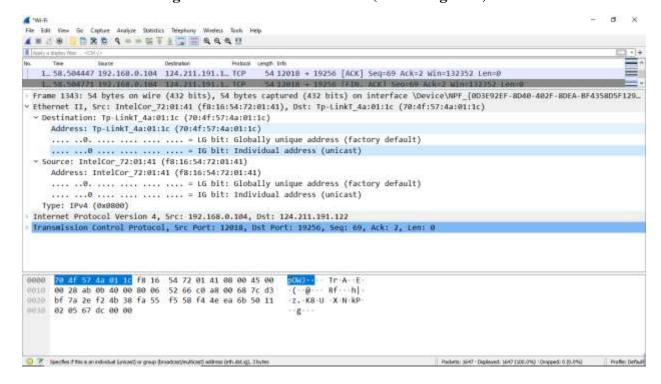


Figure 09: Packet Details Pane (Ethernet Segment)

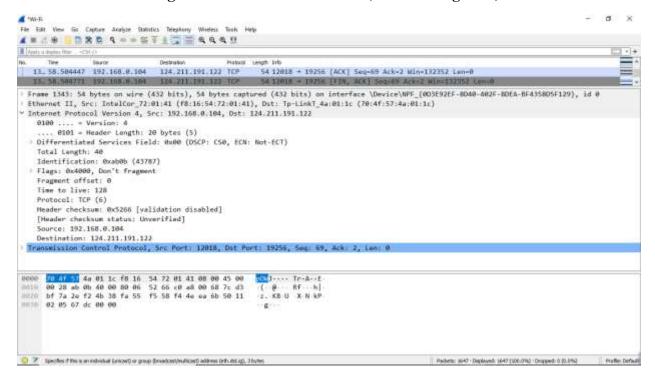


Figure 10: Packet Details Pane (IP segment)

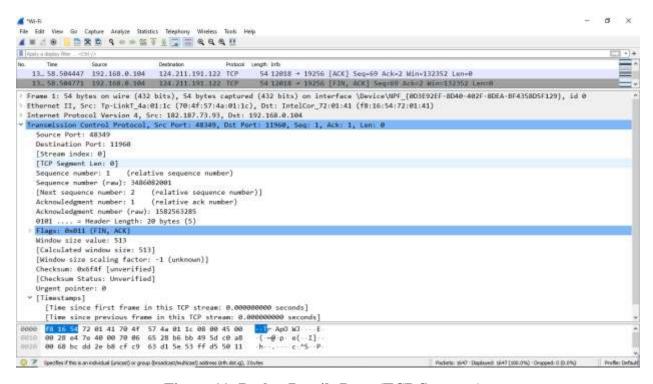


Figure 11: Packet Details Pane (TCP Segment)

```
- s ×
₫ 'Wi-Fi
File Edit View Go Copture Analyze Statistics Telephony Wireless Took Help
ARIBERT STATE
   ... 58.369... 103.10.22... 192.168.0... UDP 1... 52817 + 44069 Len=63
   ... 58.369... 192.168.0... 103.10.22... UDP 62 44069 + 52817 Len=20
   ... 58.418... 103.10.22... 192.168.0... UDP 1... 52817 + 44069 Len=63
   ... 58.418... 192.168.0... 103.10.22... UDP 62.44069 → 52817 Len=20
    ...58.489...124.211.1... 192.168.0... TCP 54 19256 → 12018 [ACK] Seq=1 Ack=69 Win=262012 Len=0
   ...58.504...124.211.1...192.168.0...TCP 54.19256 → 12018 [FIN, ACK] Seq=1 Ack=69 Win=262012 Len=0
 Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF...
 Ethernet II, Src: Tp-LinkT_4a:01:1c (70:4f:57:4a:01:1c), Dst: IntelCor_72:01:41 (f8:16:54:72:01:41)
 Internet Protocol Version 4, Src: 182.187.73.93, Dst: 192.168.0.104
 Transmission Control Protocol, Src Port: 48349, Dst Port: 11960, Seq: 1, Ack: 1, Len: 0
       f8 16 54 72 01 41 70 4f
 0000
                                   57 4a 01 1c 08 00 45 00
                                                                 Tr-ApO WJ----E
       00 28 e4 7e 40 00 70 06
                                   65 28 b6 bb 49 5d c0 a8
0010
                                                                -(-~@-p-e(--I]--
8020 00 68 bc dd 2e b8 cf c9 63 d1 5e 53 ff d5 50 11
                                                                0030 02 01 6f 4f 00 00
                                                                --00--
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (rdv.list.ig), 3 bytes.
                                                                             Politets: 3647 - Displayed: 1647 (100.0%) - Onsped: 0.00.0% Profile: Default
```

Figure 12: Packet Byte Pane



Figure 13: Statistics- Flow Graph (All Flows)

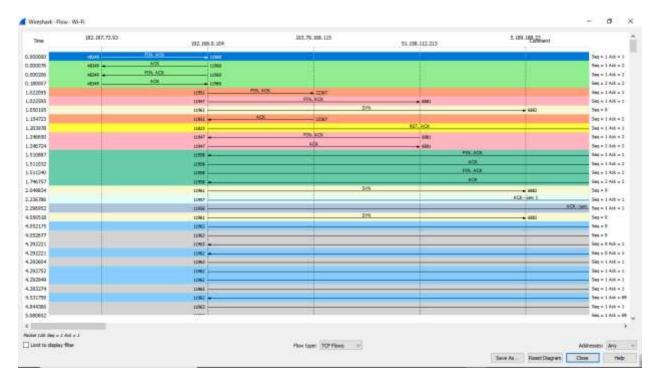


Figure 13: Statistics- Flow Graph (TCP Flows)

#### **Conclusion:**

Wireshark is a network protocol analyzer which captures network packets and displays packet data in details. After downloading and installing Wireshark we can easily Capture live packet data from a network interface using Wireshark. We have applied filter to monitor particular traffic. The TCP Stream Throughput graph have shown us the throughput from one TCP stream, in one direction, based on the selected packet.