

# 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 Zayed Iqbal**

**ID: IT-16038**

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.

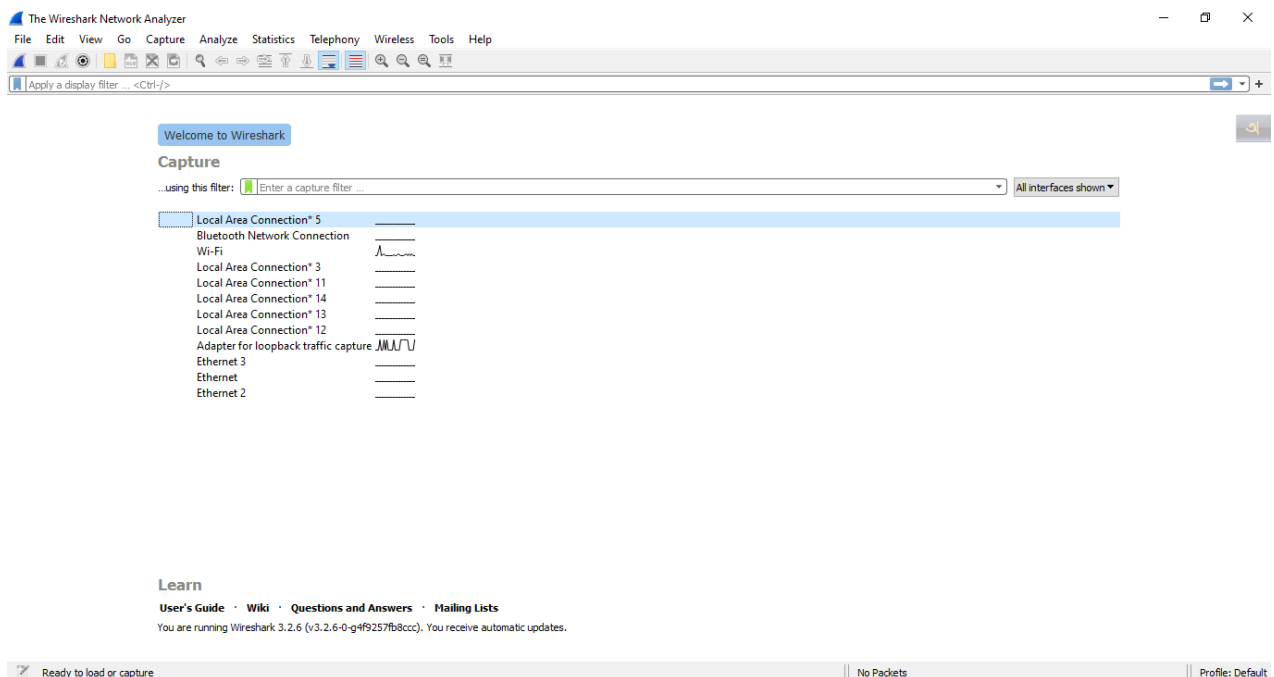
#### Objectives:

We will learn-

- How to install wireshark.
- How to analyze packets and protocols after capture.
- How to use graphs and flow diagrams in analysis.

#### Procedures:

Step1: Open The Wireshark.



**Fig: Wireshark GUI (Main Window)**

## Step 2: Start capturing.

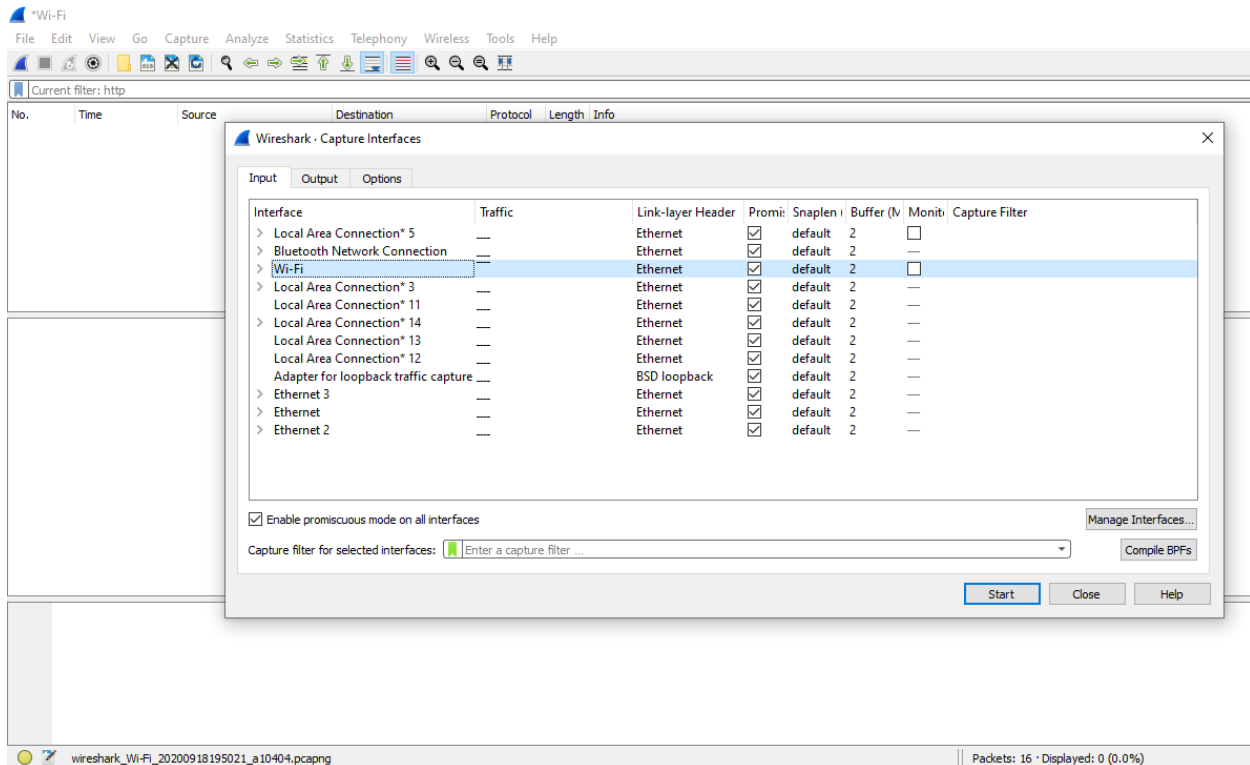


Fig : Starting capture

## Step 3: Packets are exchanging on Network Interface.

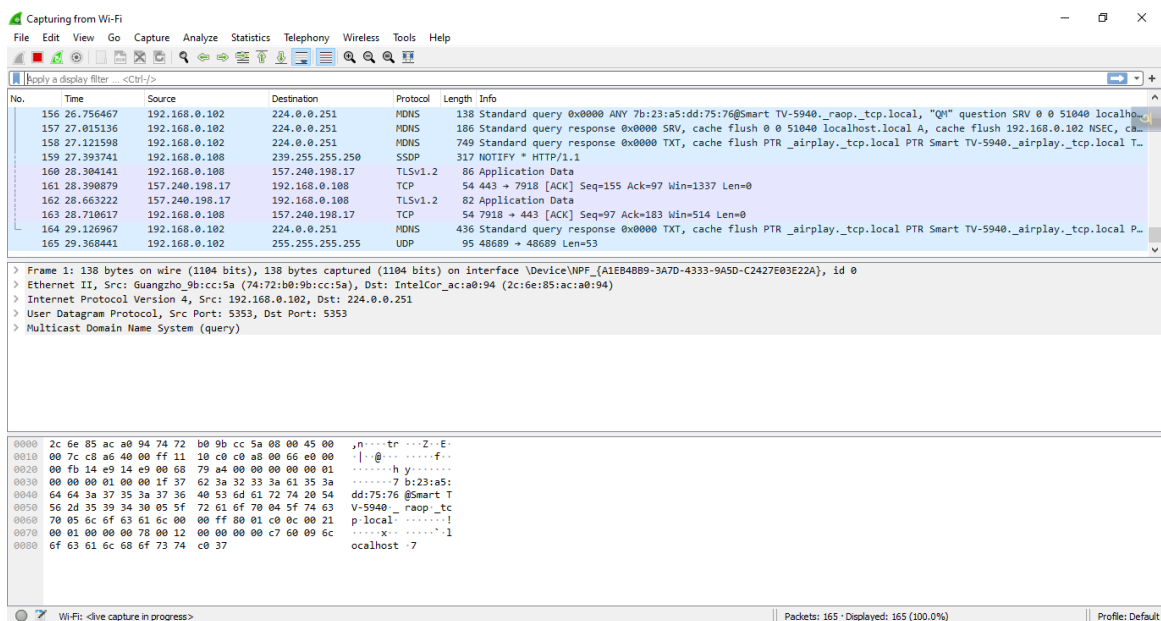


Fig: Packets are exchanging

## Step 4: Stop Capture.

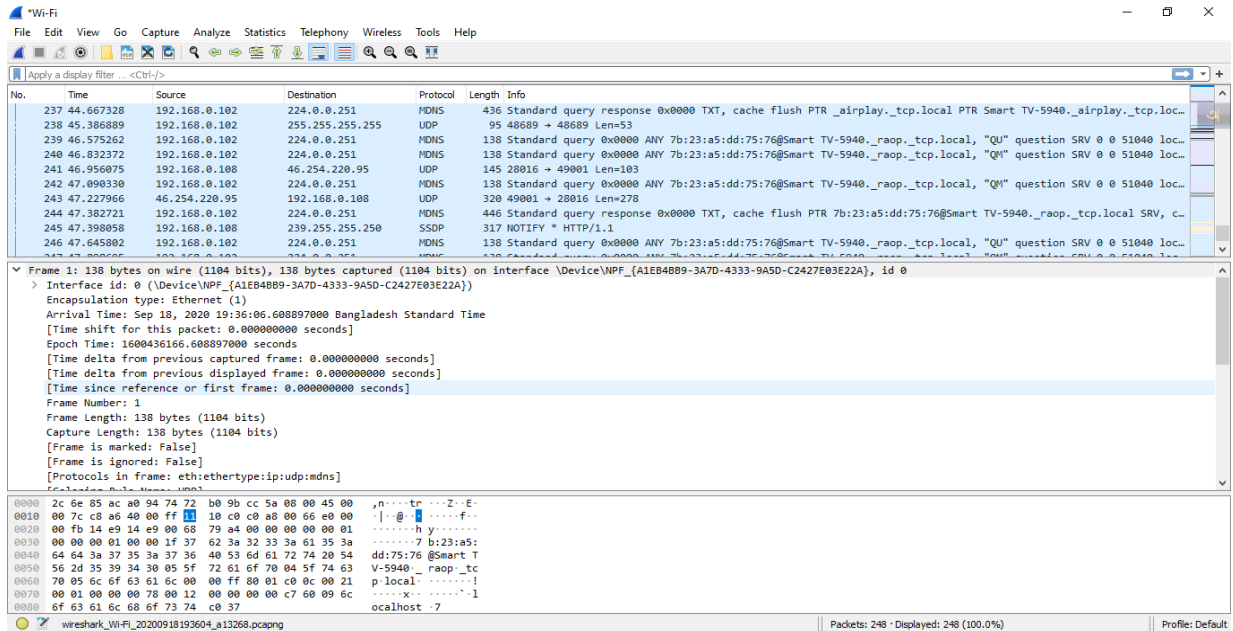


Fig: Stop capture.

## Step 5: Filter by entering the protocol http.

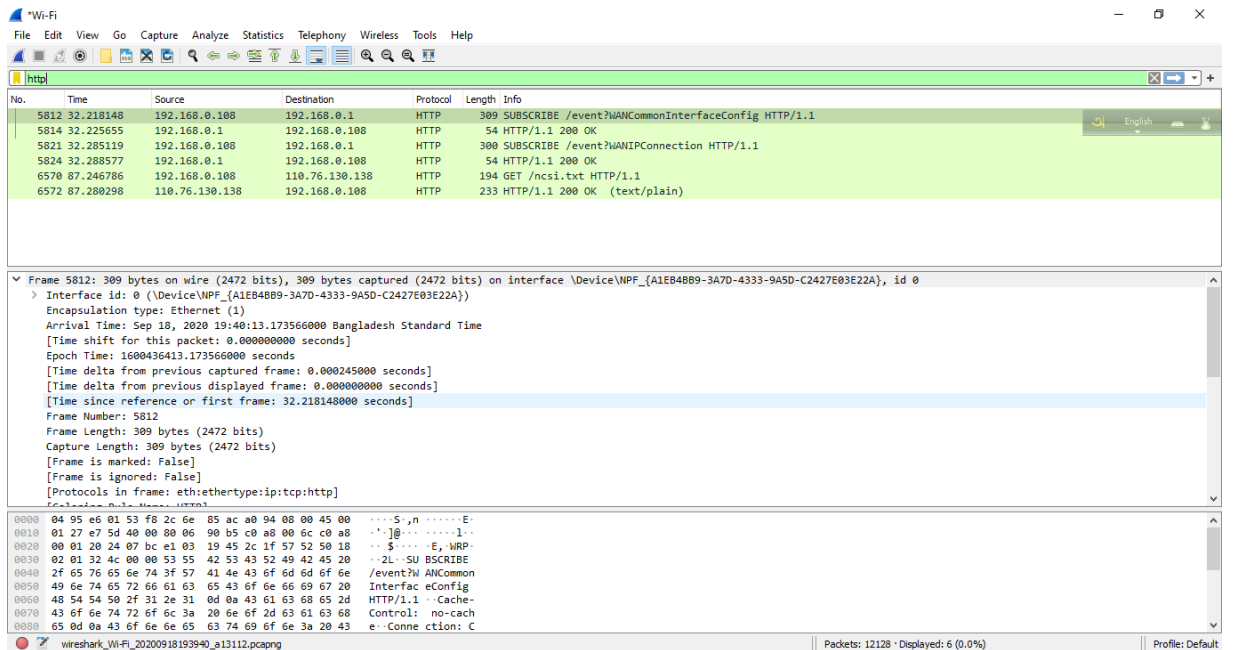


Fig: http filtering



```

> Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
> Ethernet II, Src: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94), Dst: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
▼ Internet Protocol Version 4, Src: 192.168.0.108, Dst: 157.33.129.147
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 131
    Identification: 0x0650 (1616)
    > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x5451 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.108
    Destination: 157.33.129.147
> User Datagram Protocol, Src Port: 28016, Dst Port: 52042
> Data (103 bytes)

```

**Fig: Packet Details Pane (IP segment)**

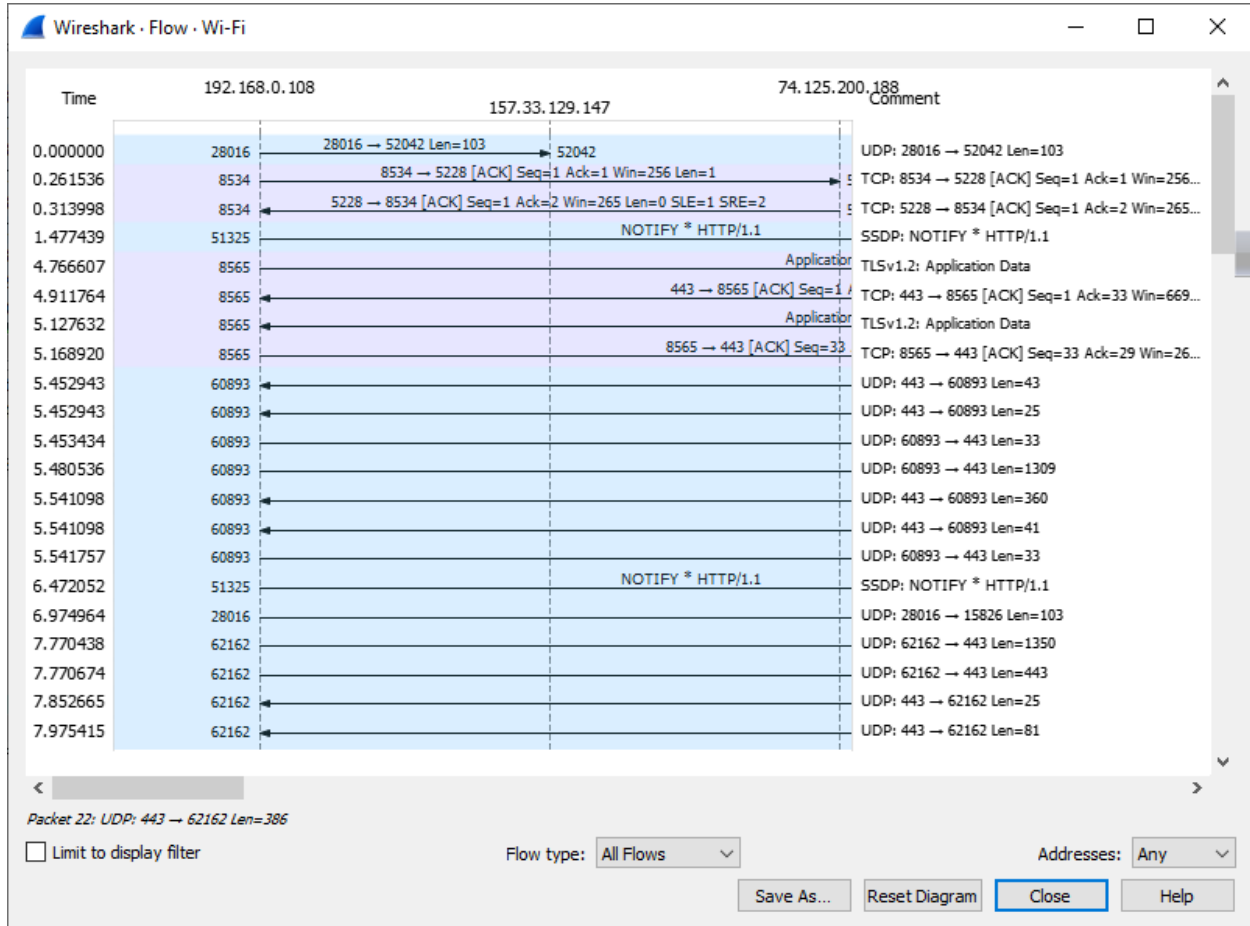
```

> Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
> Ethernet II, Src: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94), Dst: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 157.33.129.147
▼ User Datagram Protocol, Src Port: 28016, Dst Port: 52042
    Source Port: 28016
    Destination Port: 52042
    Length: 111
    Checksum: 0x0225 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    ▼ [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
▼ Data (103 bytes)
    Data: 64313a6164323a696432303a6830c62c8400b11b9961f65f...
    [Length: 103]

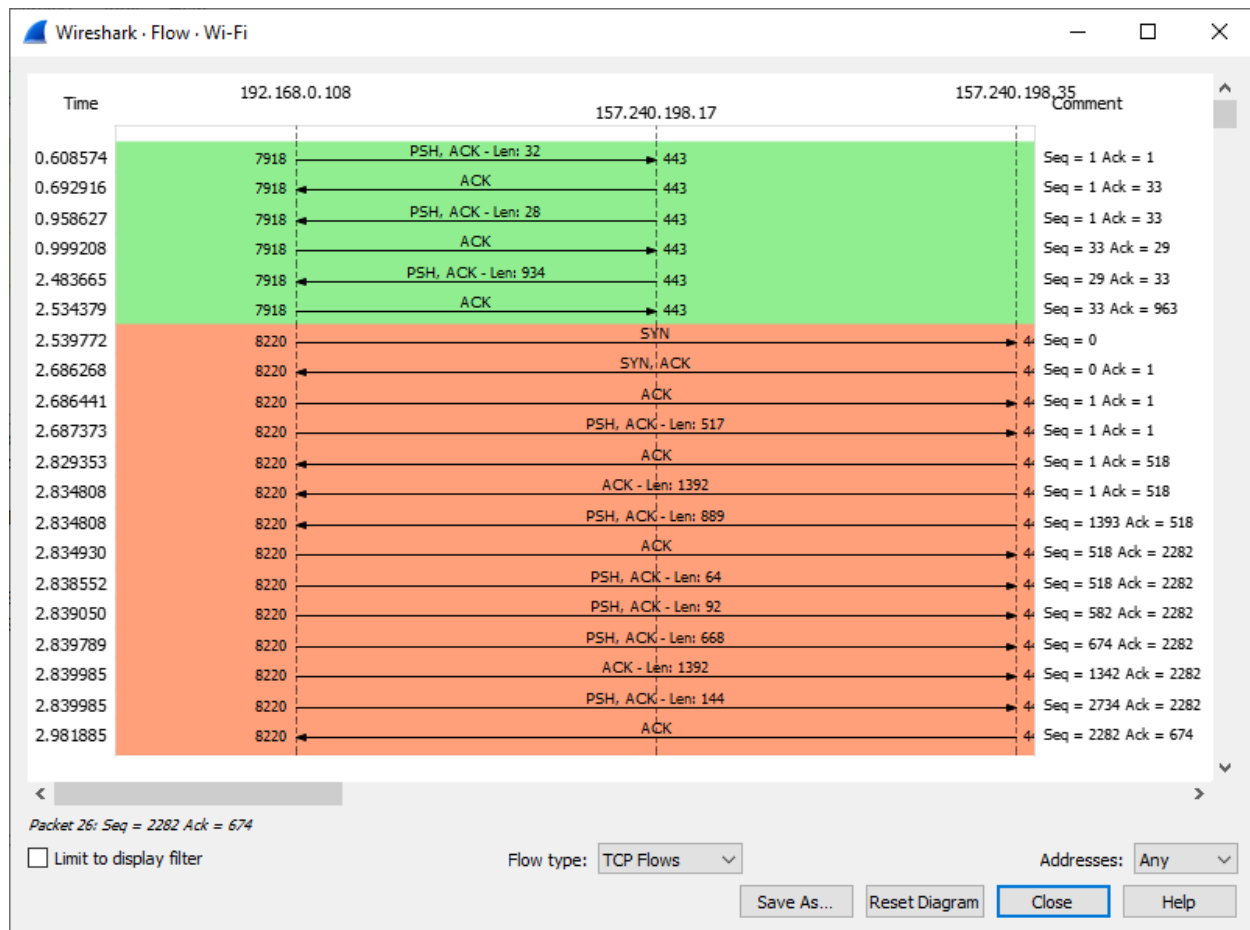
```

**Fig: Packet Details Pane (UDP segment)**

## Step 6: TCP plots and flowgraph



**Fig: Flowgraph(all flows)**



**Fig: TCP flowgraph**

**Discussion:** From the lab we can learn about packet and protocol analysis. Through wireshark live traffic can be captured. Data can be captured on wired and wireless media. Numerous protocols can be capture and analyze by wireshark. We can see the packets exchanging in detail. We use filtering when a lot of packets are exchanging.



