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: Shourove Sutradhar Dip

ID: IT-16008

4th year 2nd semester

Session: 2015-2016

Dept. of ICT, MBSTU

## Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

## Experiment N0: 05

## Name of Experiment: Comparative analysis of Wired and Wireless data using Wireshark.

## Objectives:

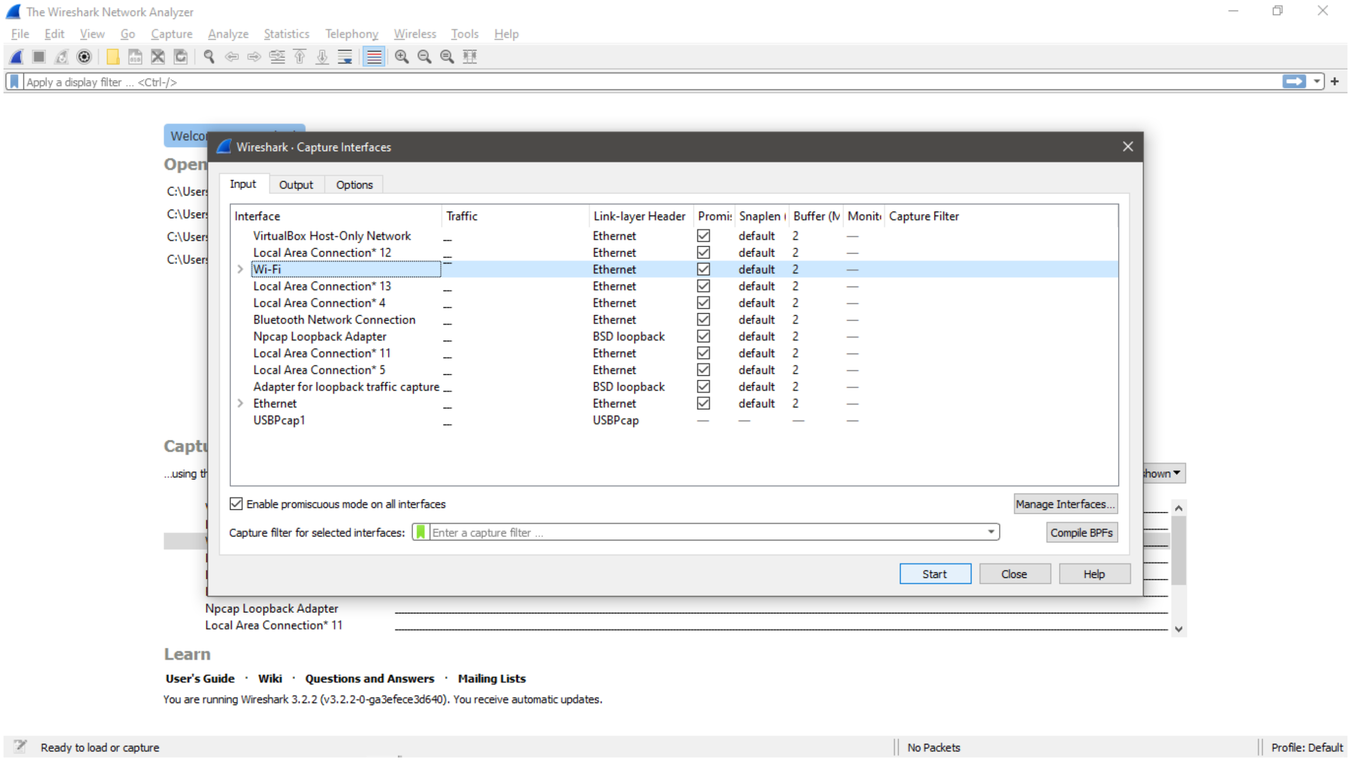
1. Learn how to analyze both wired and wireless network data.
2. Understand how different types of network data work.
3. Learn to use Wireshark to capture network packets in real time and display them in human-readable format.
4. Learn to use Wireshark for network troubleshooting and communication protocol analysis.
5. Comparing between wired and wireless network data.

## Procedures:

### Step 1- Capturing:

Packets and Protocols can be analyzed after capture. To capture, first I go to capture menu and select options. Then I start capturing on interface that has IP address.

First the starting of capturing wireless data has been shown and then the starting of wired data has been shown here.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Capture Interfaces
Input Output Options
Manage Interfaces...
Compile BPFs
Start Close Help

| Interface | Traffic | Link-layer Header | Promi: | Snaplen ( | Buffer (M | Monit | Capture Filter |
|---|---|---|---|---|---|---|---|
| VirtualBox Host-Only Network | _ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 12 | _ | Ethernet | ☑ | default | 2 | — | |
| Wi-Fi | _ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 13 | _ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 4 | _ | Ethernet | ☑ | default | 2 | — | |
| Bluetooth Network Connection | _ | Ethernet | ☑ | default | 2 | — | |
| Npcap Loopback Adapter | _ | BSD loopback | ☑ | default | 2 | — | |
| Local Area Connection* 11 | _ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 5 | _ | Ethernet | ☑ | default | 2 | — | |
| Adapter for loopback traffic capture | _ | BSD loopback | ☑ | default | 2 | — | |
| Ethernet | _ | Ethernet | ☑ | default | 2 | — | |
| USBPcap1 | _ | USBPcap | — | — | — | — | |

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Npcap Loopback Adapter
Local Area Connection* 11

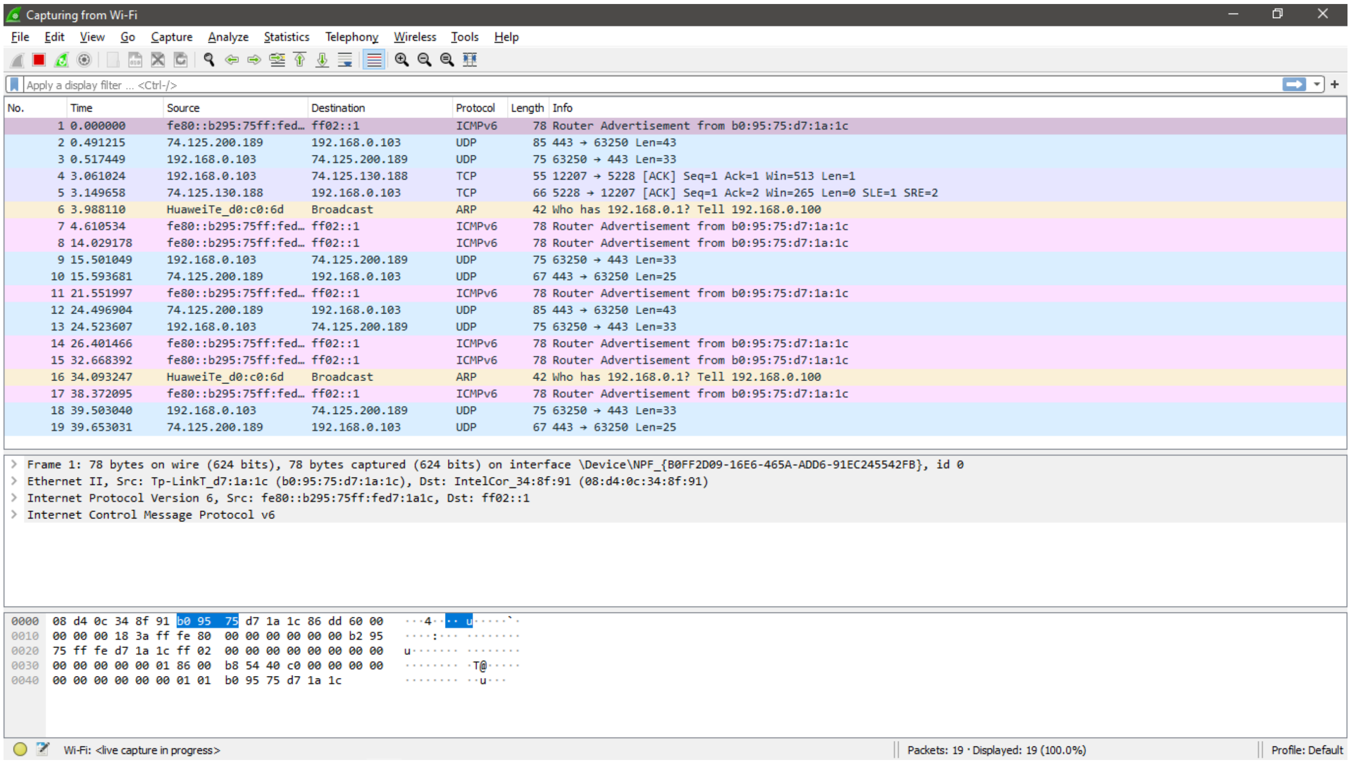
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efece3d640). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Figure-1.1: Starting to capture Wireless Network data


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

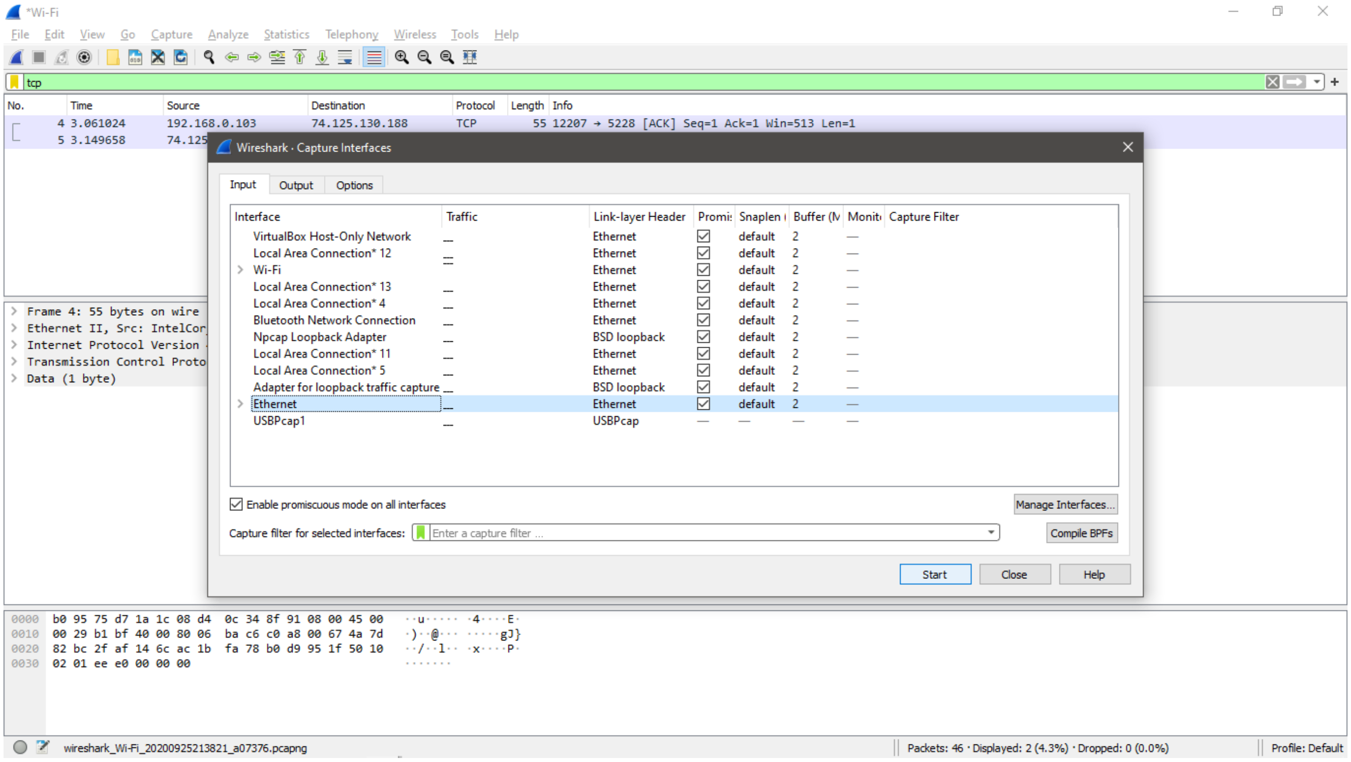
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 2 | 0.491215 | 74.125.200.189 | 192.168.0.103 | UDP | 85 | 443 → 63250 Len=43 |
| 3 | 0.517449 | 192.168.0.103 | 74.125.200.189 | UDP | 75 | 63250 → 443 Len=33 |
| 4 | 3.061024 | 192.168.0.103 | 74.125.130.188 | TCP | 55 | 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1 |
| 5 | 3.149658 | 74.125.130.188 | 192.168.0.103 | TCP | 66 | 5228 → 12207 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2 |
| 6 | 3.988110 | HuaweiTe_d0:c0:6d | Broadcast | ARP | 42 | Who has 192.168.0.1? Tell 192.168.0.100 |
| 7 | 4.610534 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 8 | 14.029178 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 9 | 15.501049 | 192.168.0.103 | 74.125.200.189 | UDP | 75 | 63250 → 443 Len=33 |
| 10 | 15.593681 | 74.125.200.189 | 192.168.0.103 | UDP | 67 | 443 → 63250 Len=25 |
| 11 | 21.551997 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 12 | 24.496904 | 74.125.200.189 | 192.168.0.103 | UDP | 85 | 443 → 63250 Len=43 |
| 13 | 24.523607 | 192.168.0.103 | 74.125.200.189 | UDP | 75 | 63250 → 443 Len=33 |
| 14 | 26.401466 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 15 | 32.668392 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 16 | 34.093247 | HuaweiTe_d0:c0:6d | Broadcast | ARP | 42 | Who has 192.168.0.1? Tell 192.168.0.100 |
| 17 | 38.372095 | fe80::b295:75ff:fed… | ff02::1 | ICMPv6 | 78 | Router Advertisement from b0:95:75:d7:1a:1c |
| 18 | 39.503040 | 192.168.0.103 | 74.125.200.189 | UDP | 75 | 63250 → 443 Len=33 |
| 19 | 39.653031 | 74.125.200.189 | 192.168.0.103 | UDP | 67 | 443 → 63250 Len=25 |

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{B0FF2D09-16E6-465A-ADD6-91EC245542FB}, id 0
> Ethernet II, Src: Tp-LinkT_d7:1a:1c (b0:95:75:d7:1a:1c), Dst: IntelCor_34:8f:91 (08:d4:0c:34:8f:91)
> Internet Protocol Version 6, Src: fe80::b295:75ff:fed7:1a1c, Dst: ff02::1
> Internet Control Message Protocol v6
```

```
0000  08 d4 0c 34 8f 91 b0 95  75 d7 1a 1c 86 dd 60 00   ···4·· ·· u·····`·
0010  00 00 00 18 3a ff fe 80  00 00 00 00 00 00 b2 95   ····:··· ········
0020  75 ff fe d7 1a 1c ff 02  00 00 00 00 00 00 00 00   u······· ········
0030  00 00 00 00 00 01 86 00  b8 54 40 c0 00 00 00 00   ········ ·T@·····
0040  00 00 00 00 00 00 01 01  b0 95 75 d7 1a 1c         ········ ··u···
```

Wi-Fi: <live capture in progress> | Packets: 19 · Displayed: 19 (100.0%) | Profile: Default

Figure-1.2: Dumped packages of Wireless Network in main window of Wireshark


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Interfaces
Input Output Options
Manage Interfaces...
Compile BPFs
Start
Close
Help

tcp

```
No.  Time      Source         Destination     Protocol Length Info
   4 3.061024  192.168.0.103  74.125.130.188  TCP         55 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
   5 3.149658  74.125
```

```
> Frame 4: 55 bytes on wire
> Ethernet II, Src: IntelCor
> Internet Protocol Version
> Transmission Control Proto
> Data (1 byte)
```

| Interface | Traffic | Link-layer Header | Promi: | Snaplen ( | Buffer (M | Monit | Capture Filter |
|---|---|---|---|---|---|---|---|
| VirtualBox Host-Only Network | __ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 12 | __ | Ethernet | ☑ | default | 2 | — | |
| > Wi-Fi | | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 13 | __ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 4 | __ | Ethernet | ☑ | default | 2 | — | |
| Bluetooth Network Connection | __ | Ethernet | ☑ | default | 2 | — | |
| Npcap Loopback Adapter | __ | BSD loopback | ☑ | default | 2 | — | |
| Local Area Connection* 11 | __ | Ethernet | ☑ | default | 2 | — | |
| Local Area Connection* 5 | __ | Ethernet | ☑ | default | 2 | — | |
| Adapter for loopback traffic capture | __ | BSD loopback | ☑ | default | 2 | — | |
| > Ethernet | __ | Ethernet | ☑ | default | 2 | — | |
| USBPcap1 | __ | USBPcap | — | — | — | — | |

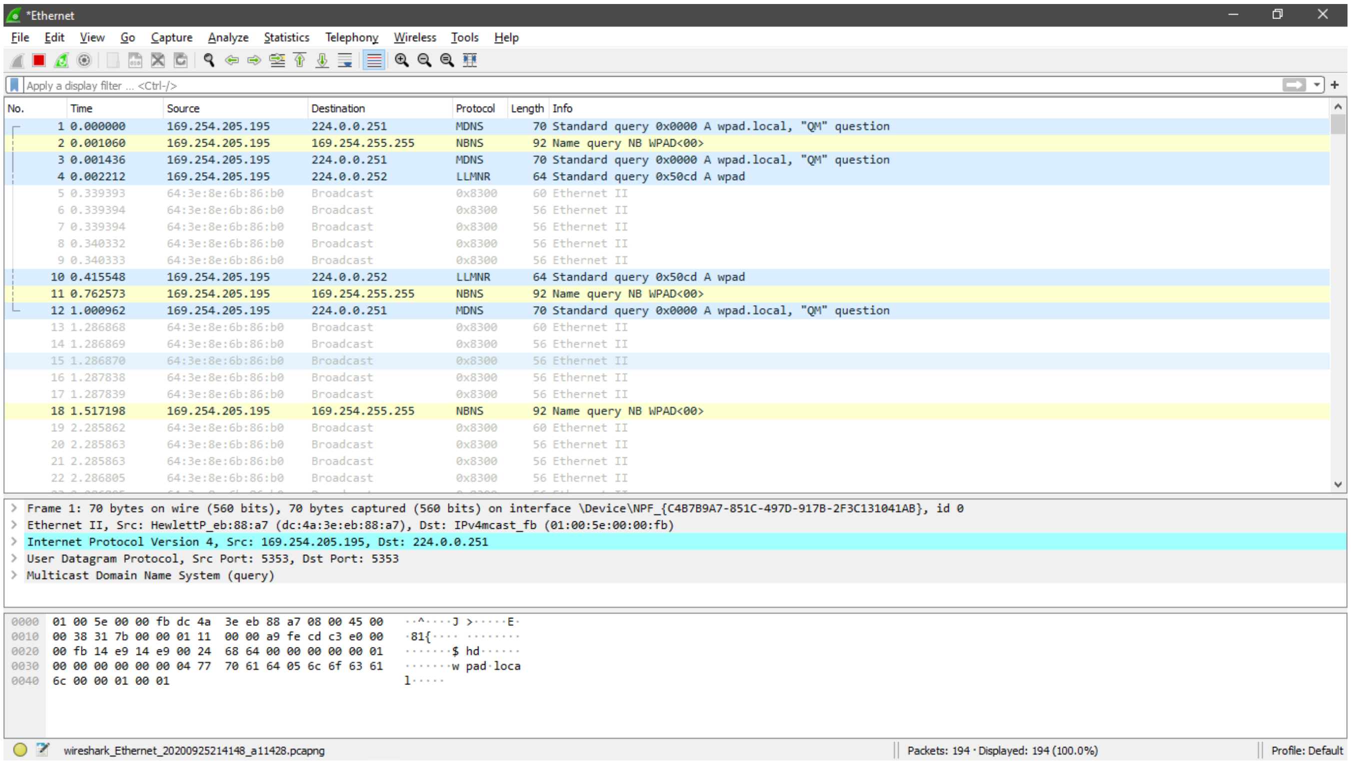
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

```
0000  b0 95 75 d7 1a 1c 08 d4  0c 34 8f 91 08 00 45 00   ··u····· ·4····E·
0010  00 29 b1 bf 40 00 80 06  ba c6 c0 a8 00 67 4a 7d   ·)··@··· ·····gJ}
0020  82 bc 2f af 14 6c ac 1b  fa 78 b0 d9 95 1f 50 10   ··/··l·· ·x····P·
0030  02 01 ee e0 00 00 00                               ·······
```

wireshark_Wi-Fi_20200925213821_a07376.pcapng | Packets: 46 · Displayed: 2 (4.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure-1.3: Starting to capture Wired Network data


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

```
No.  Time      Source             Destination      Protocol Length Info
   1 0.000000  169.254.205.195    224.0.0.251      MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
   2 0.001060  169.254.205.195    169.254.255.255  NBNS        92 Name query NB WPAD<00>
   3 0.001436  169.254.205.195    224.0.0.251      MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
   4 0.002212  169.254.205.195    224.0.0.252      LLMNR       64 Standard query 0x50cd A wpad
   5 0.339393  64:3e:8e:6b:86:b0  Broadcast        0x8300      60 Ethernet II
   6 0.339394  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
   7 0.339394  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
   8 0.340332  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
   9 0.340333  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  10 0.415548  169.254.205.195    224.0.0.252      LLMNR       64 Standard query 0x50cd A wpad
  11 0.762573  169.254.205.195    169.254.255.255  NBNS        92 Name query NB WPAD<00>
  12 1.000962  169.254.205.195    224.0.0.251      MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
  13 1.286868  64:3e:8e:6b:86:b0  Broadcast        0x8300      60 Ethernet II
  14 1.286869  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  15 1.286870  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  16 1.287838  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  17 1.287839  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  18 1.517198  169.254.205.195    169.254.255.255  NBNS        92 Name query NB WPAD<00>
  19 2.285862  64:3e:8e:6b:86:b0  Broadcast        0x8300      60 Ethernet II
  20 2.285863  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  21 2.285863  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
  22 2.286805  64:3e:8e:6b:86:b0  Broadcast        0x8300      56 Ethernet II
```

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{C4B7B9A7-851C-497D-917B-2F3C131041AB}, id 0
> Ethernet II, Src: HewlettP_eb:88:a7 (dc:4a:3e:eb:88:a7), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 169.254.205.195, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

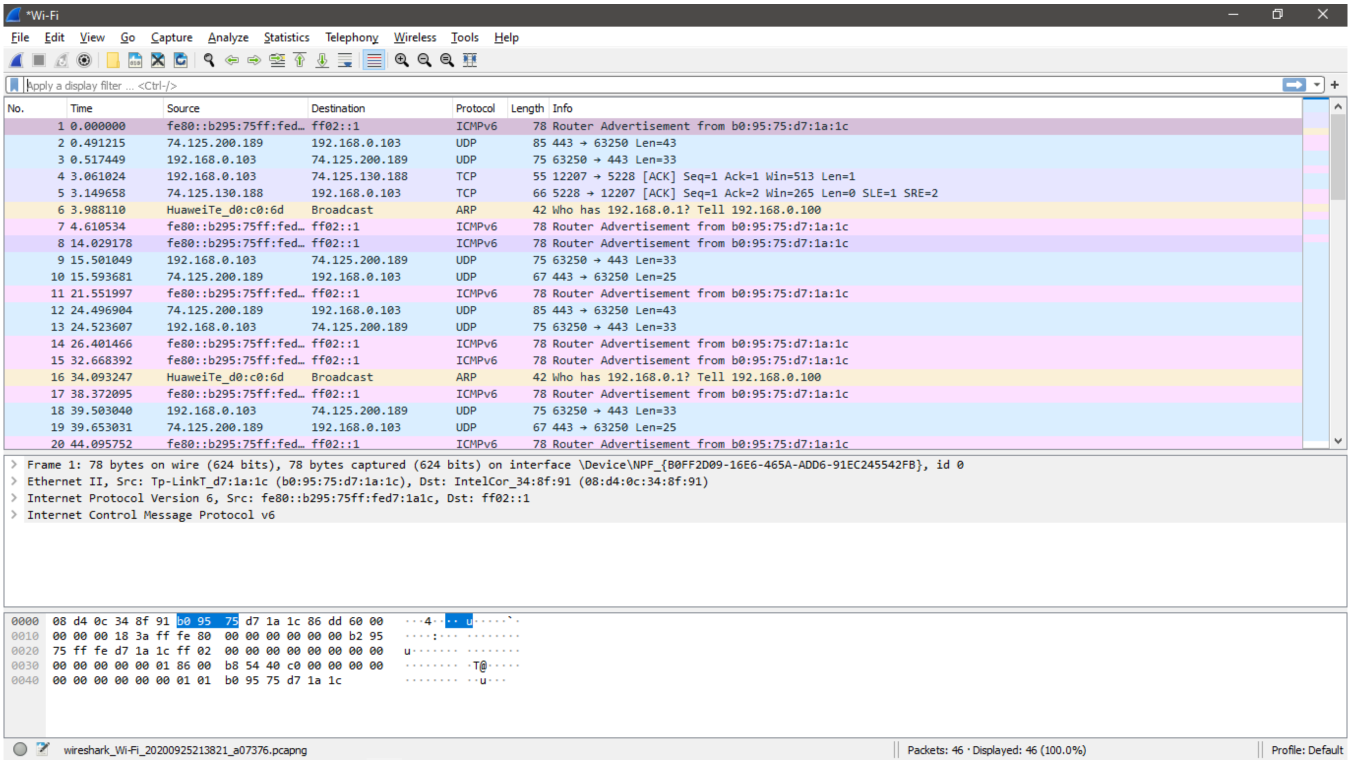
```
0000  01 00 5e 00 00 fb dc 4a  3e eb 88 a7 08 00 45 00   ··^····J >·····E·
0010  00 38 31 7b 00 00 01 11  00 00 a9 fe cd c3 e0 00   ·81{···· ········
0020  00 fb 14 e9 14 e9 00 24  68 64 00 00 00 00 00 01   ·······$ hd······
0030  00 00 00 00 00 00 04 77  70 61 64 05 6c 6f 63 61   ·······w pad·loca
0040  6c 00 00 01 00 01                                  l·····
```

wireshark_Ethernet_20200925214148_a11428.pcapng | Packets: 194 · Displayed: 194 (100.0%) | Profile: Default

Figure-1.4: Dumped packages of Wired Network in main window of Wireshark

## Step 2- Stopping Capture:

Capturing can be stopped by clicking on “Stop Capturing Packets” button on the main toolbar.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

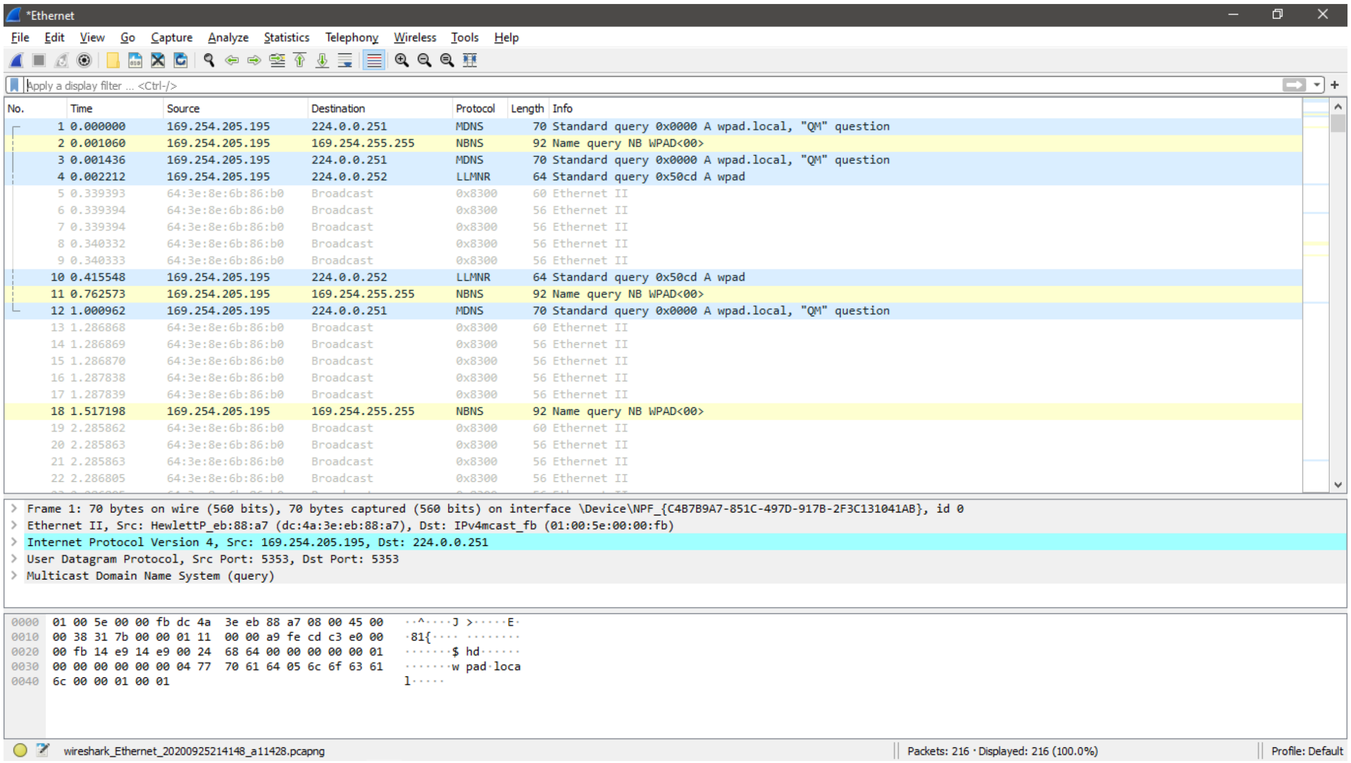
```
No.   Time       Source                Destination     Protocol Length Info
    1 0.000000   fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
    2 0.491215   74.125.200.189        192.168.0.103    UDP         85 443 → 63250 Len=43
    3 0.517449   192.168.0.103         74.125.200.189   UDP         75 63250 → 443 Len=33
    4 3.061024   192.168.0.103         74.125.130.188   TCP         55 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
    5 3.149658   74.125.130.188        192.168.0.103    TCP         66 5228 → 12207 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
    6 3.988110   HuaweiTe_d0:c0:6d     Broadcast        ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
    7 4.610534   fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
    8 14.029178  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
    9 15.501049  192.168.0.103         74.125.200.189   UDP         75 63250 → 443 Len=33
   10 15.593681  74.125.200.189        192.168.0.103    UDP         67 443 → 63250 Len=25
   11 21.551997  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
   12 24.496904  74.125.200.189        192.168.0.103    UDP         85 443 → 63250 Len=43
   13 24.523607  192.168.0.103         74.125.200.189   UDP         75 63250 → 443 Len=33
   14 26.401466  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
   15 32.668392  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
   16 34.093247  HuaweiTe_d0:c0:6d     Broadcast        ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
   17 38.372095  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
   18 39.503040  192.168.0.103         74.125.200.189   UDP         75 63250 → 443 Len=33
   19 39.653031  74.125.200.189        192.168.0.103    UDP         67 443 → 63250 Len=25
   20 44.095752  fe80::b295:75ff:fed… ff02::1          ICMPv6      78 Router Advertisement from b0:95:75:d7:1a:1c
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{B0FF2D09-16E6-465A-ADD6-91EC245542FB}, id 0
> Ethernet II, Src: Tp-LinkT_d7:1a:1c (b0:95:75:d7:1a:1c), Dst: IntelCor_34:8f:91 (08:d4:0c:34:8f:91)
> Internet Protocol Version 6, Src: fe80::b295:75ff:fed7:1a1c, Dst: ff02::1
> Internet Control Message Protocol v6
```

```
0000  08 d4 0c 34 8f 91 b0 95  75 d7 1a 1c 86 dd 60 00   ···4···· u·····`·
0010  00 00 00 18 3a ff fe 80  00 00 00 00 00 00 b2 95   ····:··· ········
0020  75 ff fe d7 1a 1c ff 02  00 00 00 00 00 00 00 00   u······· ········
0030  00 00 00 00 00 01 86 00  b8 54 40 c0 00 00 00 00   ········ ·T@·····
0040  00 00 00 00 00 00 01 01  b0 95 75 d7 1a 1c         ········ ··u···
```

wireshark_Wi-Fi_20200925213821_a07376.pcapng | Packets: 46 · Displayed: 46 (100.0%) | Profile: Default

Figure-2.1: Stopping Capture of Wireless Network



```
No.   Time       Source             Destination        Protocol  Length Info
    1 0.000000   169.254.205.195    224.0.0.251        MDNS         70 Standard query 0x0000 A wpad.local, "QM" question
    2 0.001060   169.254.205.195    169.254.255.255    NBNS         92 Name query NB WPAD<00>
    3 0.001436   169.254.205.195    224.0.0.251        MDNS         70 Standard query 0x0000 A wpad.local, "QM" question
    4 0.002212   169.254.205.195    224.0.0.252        LLMNR        64 Standard query 0x50cd A wpad
    5 0.339393   64:3e:8e:6b:86:b0  Broadcast          0x8300       60 Ethernet II
    6 0.339394   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
    7 0.339394   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
    8 0.340332   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
    9 0.340333   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   10 0.415548   169.254.205.195    224.0.0.252        LLMNR        64 Standard query 0x50cd A wpad
   11 0.762573   169.254.205.195    169.254.255.255    NBNS         92 Name query NB WPAD<00>
   12 1.000962   169.254.205.195    224.0.0.251        MDNS         70 Standard query 0x0000 A wpad.local, "QM" question
   13 1.286868   64:3e:8e:6b:86:b0  Broadcast          0x8300       60 Ethernet II
   14 1.286869   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   15 1.286870   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   16 1.287838   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   17 1.287839   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   18 1.517198   169.254.205.195    169.254.255.255    NBNS         92 Name query NB WPAD<00>
   19 2.285862   64:3e:8e:6b:86:b0  Broadcast          0x8300       60 Ethernet II
   20 2.285863   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   21 2.285863   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
   22 2.286805   64:3e:8e:6b:86:b0  Broadcast          0x8300       56 Ethernet II
```

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{C4B7B9A7-851C-497D-917B-2F3C131041AB}, id 0
> Ethernet II, Src: HewlettP_eb:88:a7 (dc:4a:3e:eb:88:a7), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 169.254.205.195, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

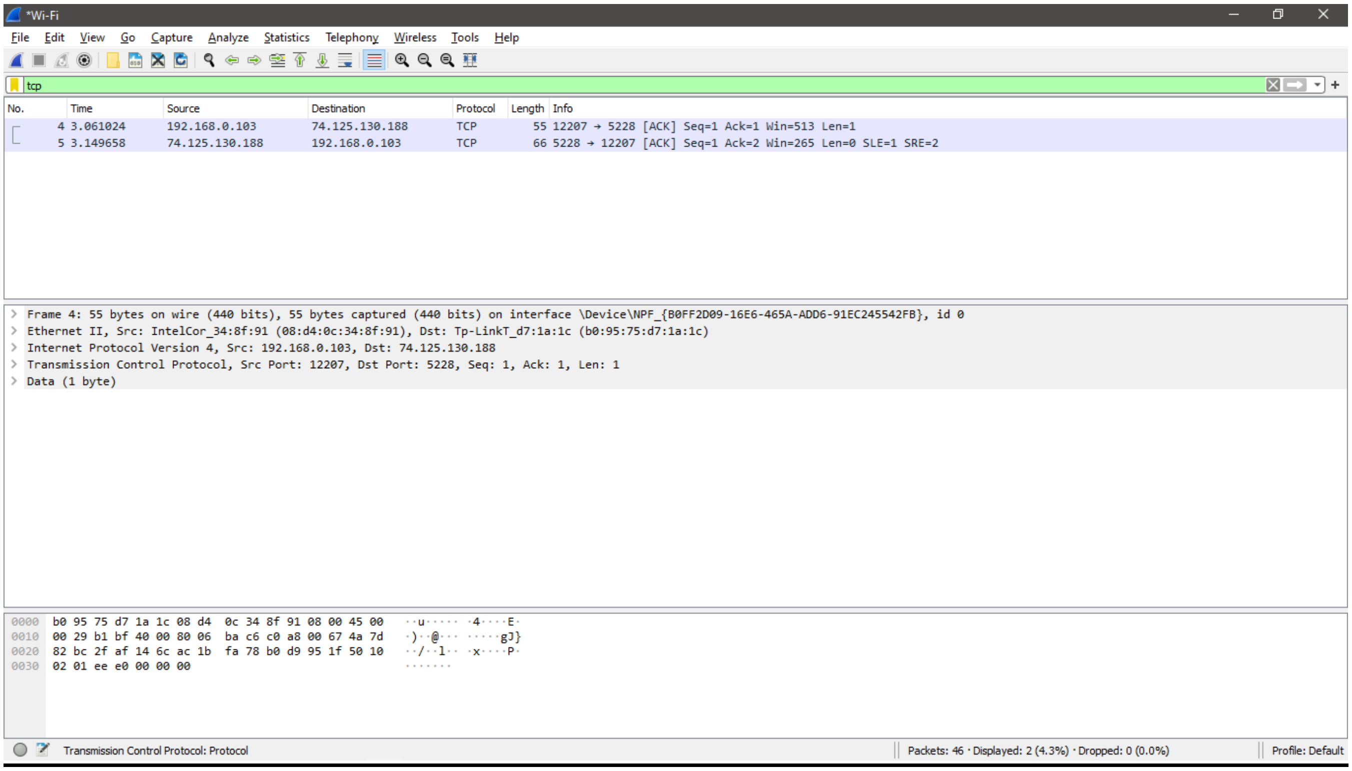
```
0000  01 00 5e 00 00 fb dc 4a  3e eb 88 a7 08 00 45 00   ··^····J >·····E·
0010  00 38 31 7b 00 00 01 11  00 00 a9 fe cd c3 e0 00   ·81{···· ········
0020  00 fb 14 e9 14 e9 00 24  68 64 00 00 00 00 00 01   ·······$ hd······
0030  00 00 00 00 00 00 04 77  70 61 64 05 6c 6f 63 61   ·······w pad·loca
0040  6c 00 00 01 00 01                                  l·····
```

wireshark_Ethernet_20200925214148_a11428.pcapng | Packets: 216 · Displayed: 216 (100.0%) | Profile: Default

Figure-2.2: Stopping Capture of Wired Network

## Step 3- Filtering:

We can filter the captures by entering the protocol name in “Apply a Display Filter” and enter.



tcp

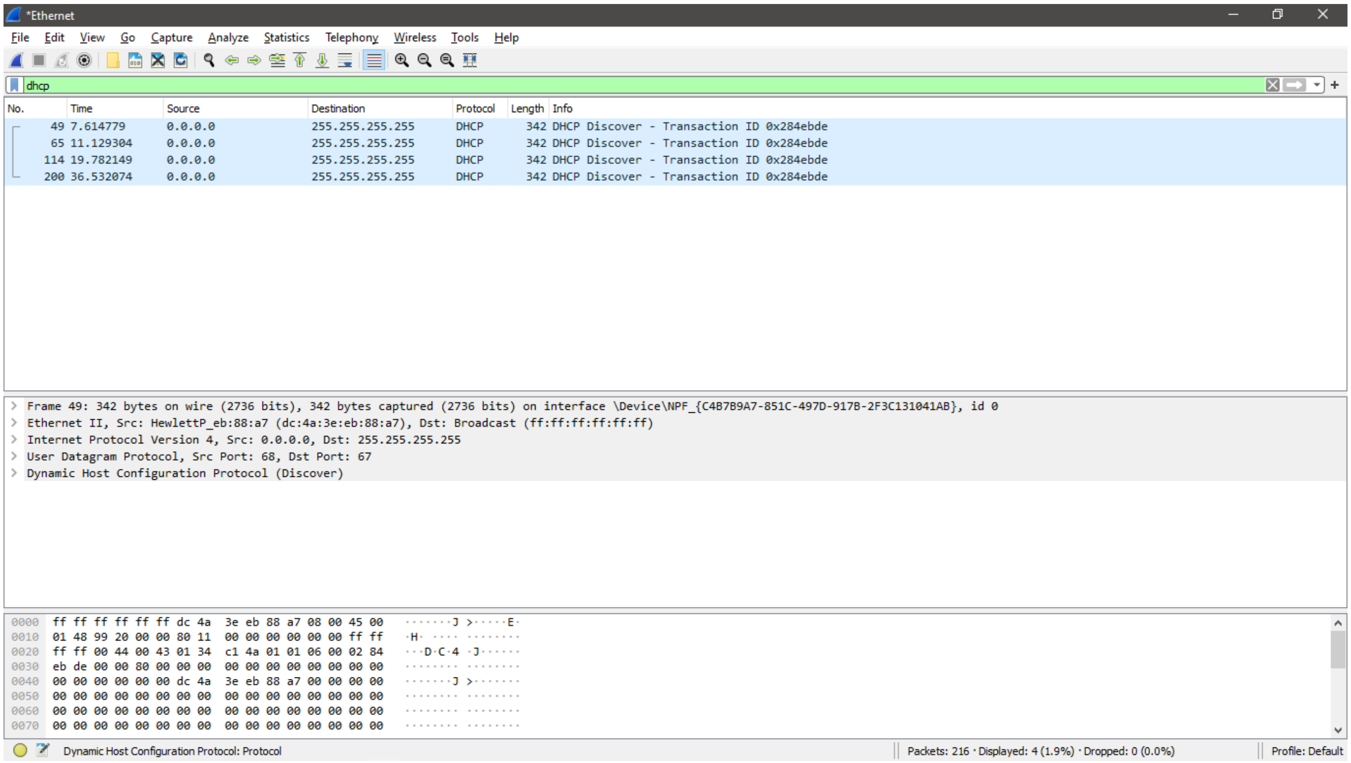
```
No.   Time       Source          Destination     Protocol  Length Info
    4 3.061024   192.168.0.103   74.125.130.188  TCP         55 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
    5 3.149658   74.125.130.188  192.168.0.103   TCP         66 5228 → 12207 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
```

```
> Frame 4: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B0FF2D09-16E6-465A-ADD6-91EC245542FB}, id 0
> Ethernet II, Src: IntelCor_34:8f:91 (08:d4:0c:34:8f:91), Dst: Tp-LinkT_d7:1a:1c (b0:95:75:d7:1a:1c)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 74.125.130.188
> Transmission Control Protocol, Src Port: 12207, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  b0 95 75 d7 1a 1c 08 d4  0c 34 8f 91 08 00 45 00   ··u····· ·4····E·
0010  00 29 b1 bf 40 00 80 06  ba c6 c0 a8 00 67 4a 7d   ·)··@··· ·····gJ}
0020  82 bc 2f af 14 6c ac 1b  fa 78 b0 d9 95 1f 50 10   ··/··l·· ·x····P·
0030  02 01 ee e0 00 00 00                               ·······
```

Transmission Control Protocol: Protocol | Packets: 46 · Displayed: 2 (4.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure-3.1: Filtering by TCP protocols of Wireless Network data



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

```
No.   Time       Source    Destination      Protocol  Length Info
   49 7.614779   0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x284ebde
   65 11.129304  0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x284ebde
  114 19.782149  0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x284ebde
  200 36.532074  0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x284ebde
```

```
> Frame 49: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{C4B7B9A7-851C-497D-917B-2F3C131041AB}, id 0
> Ethernet II, Src: HewlettP_eb:88:a7 (dc:4a:3e:eb:88:a7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

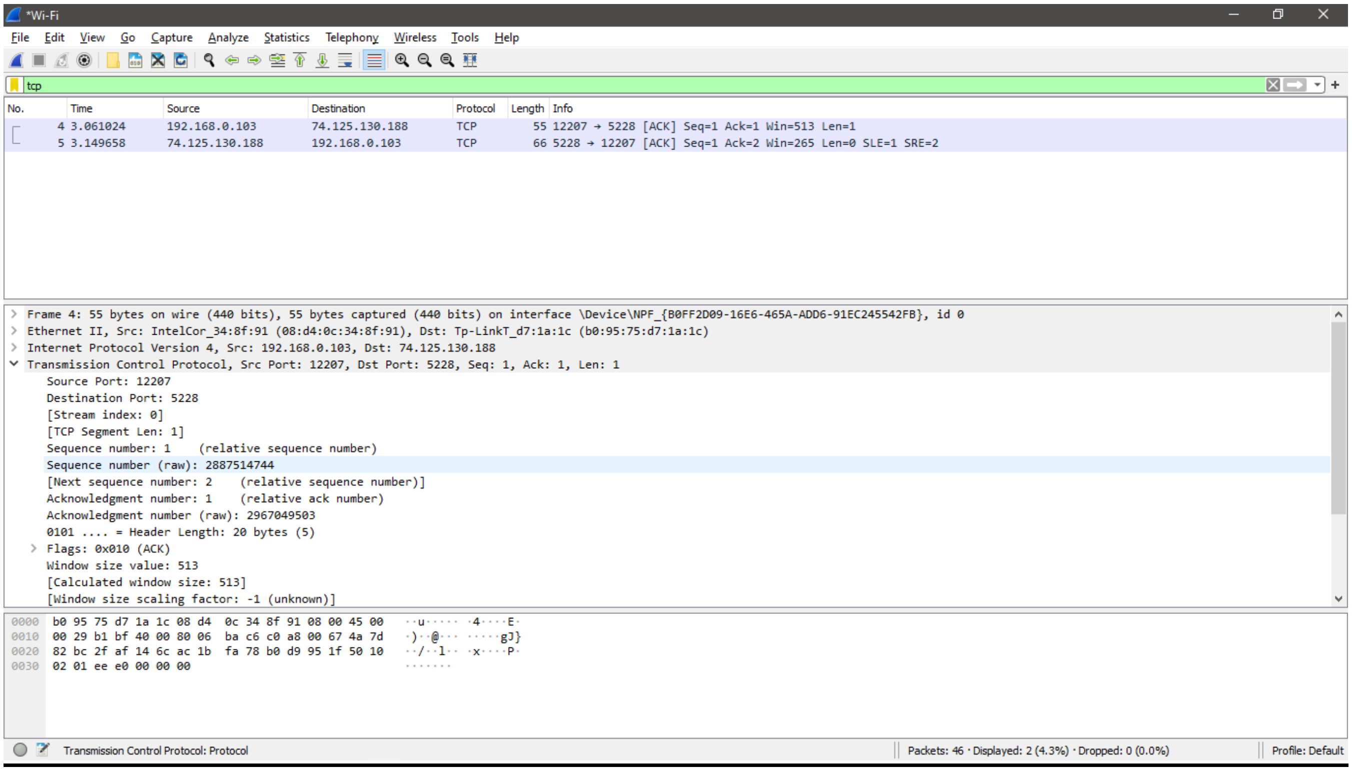
```
0000  ff ff ff ff ff ff dc 4a  3e eb 88 a7 08 00 45 00   ·······J >·····E·
0010  01 48 99 20 00 00 80 11  00 00 00 00 00 00 ff ff   ·H· ···· ········
0020  ff ff 00 44 00 43 01 34  c1 4a 01 01 06 00 02 84   ···D·C·4 ·J······
0030  eb de 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 dc 4a  3e eb 88 a7 00 00 00 00   ·······J >·······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Dynamic Host Configuration Protocol: Protocol | Packets: 216 · Displayed: 4 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

Figure-3.2: Filtering by DHCP protocols of Wired Network data

## Step 4- Analyzing Protocols:

The analysis has to be performed manually. The given example below shows TCP segment with SYN and ACK fields set to 1.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

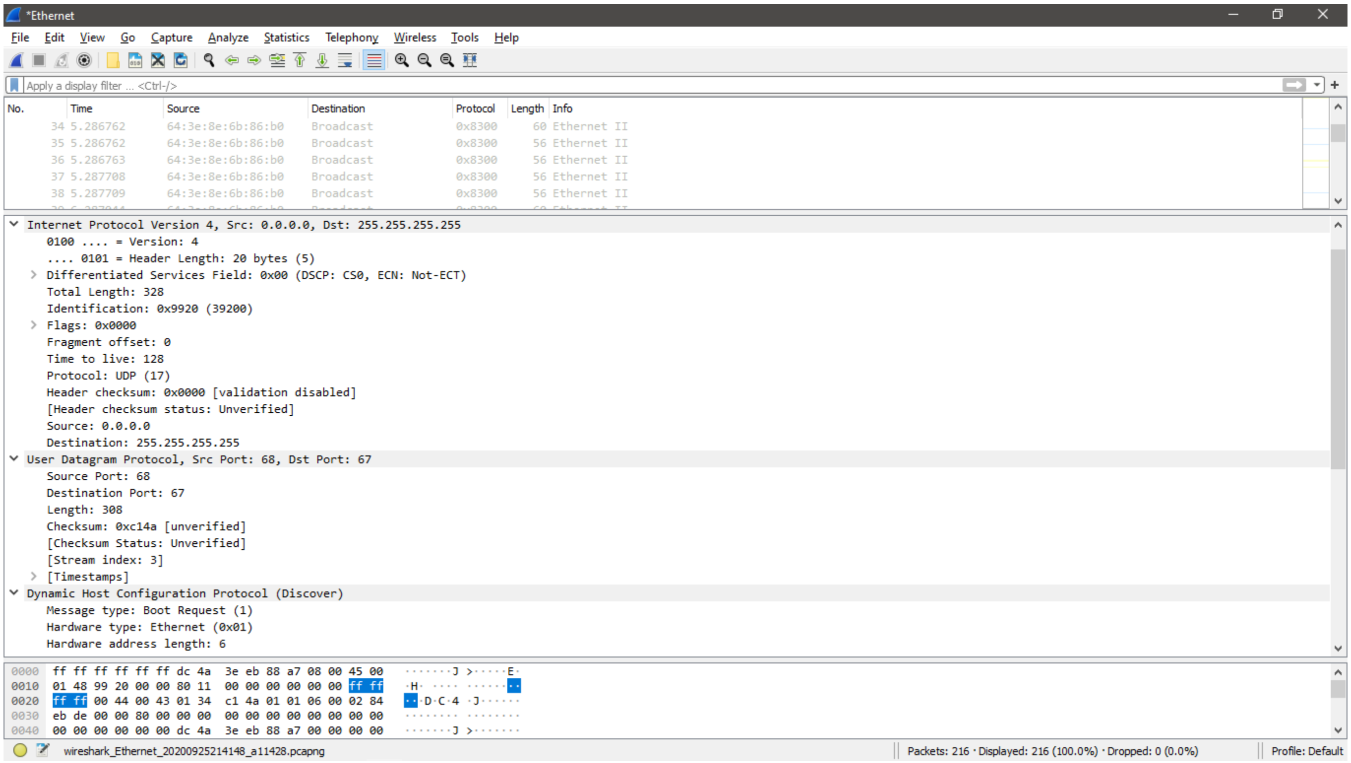
```
tcp

No.   Time       Source          Destination     Protocol Length Info
    4 3.061024   192.168.0.103   74.125.130.188  TCP          55 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
    5 3.149658   74.125.130.188  192.168.0.103   TCP          66 5228 → 12207 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
```

```
> Frame 4: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B0FF2D09-16E6-465A-ADD6-91EC245542FB}, id 0
> Ethernet II, Src: IntelCor_34:8f:91 (08:d4:0c:34:8f:91), Dst: Tp-LinkT_d7:1a:1c (b0:95:75:d7:1a:1c)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 74.125.130.188
v Transmission Control Protocol, Src Port: 12207, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
     Source Port: 12207
     Destination Port: 5228
     [Stream index: 0]
     [TCP Segment Len: 1]
     Sequence number: 1    (relative sequence number)
     Sequence number (raw): 2887514744
     [Next sequence number: 2    (relative sequence number)]
     Acknowledgment number: 1    (relative ack number)
     Acknowledgment number (raw): 2967049503
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x010 (ACK)
     Window size value: 513
     [Calculated window size: 513]
     [Window size scaling factor: -1 (unknown)]
```

```
0000  b0 95 75 d7 1a 1c 08 d4  0c 34 8f 91 08 00 45 00   ··u····· ·4····E·
0010  00 29 b1 bf 40 00 80 06  ba c6 c0 a8 00 67 4a 7d   ·)··@··· ·····gJ}
0020  82 bc 2f af 14 6c ac 1b  fa 78 b0 d9 95 1f 50 10   ··/··l·· ·x····P·
0030  02 01 ee e0 00 00 00                               ·······
```

Transmission Control Protocol: Protocol | Packets: 46 · Displayed: 2 (4.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure-4.1: Analyzing TCP protocols from Wireless Network Data


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time        Source              Destination   Protocol  Length Info
     34 5.286762    64:3e:8e:6b:86:b0   Broadcast     0x8300        60 Ethernet II
     35 5.286762    64:3e:8e:6b:86:b0   Broadcast     0x8300        56 Ethernet II
     36 5.286763    64:3e:8e:6b:86:b0   Broadcast     0x8300        56 Ethernet II
     37 5.287708    64:3e:8e:6b:86:b0   Broadcast     0x8300        56 Ethernet II
     38 5.287709    64:3e:8e:6b:86:b0   Broadcast     0x8300        56 Ethernet II
```

```
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 328
     Identification: 0x9920 (39200)
   > Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source: 0.0.0.0
     Destination: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
     Source Port: 68
     Destination Port: 67
     Length: 308
     Checksum: 0xc14a [unverified]
     [Checksum Status: Unverified]
     [Stream index: 3]
   > [Timestamps]
v Dynamic Host Configuration Protocol (Discover)
     Message type: Boot Request (1)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
```

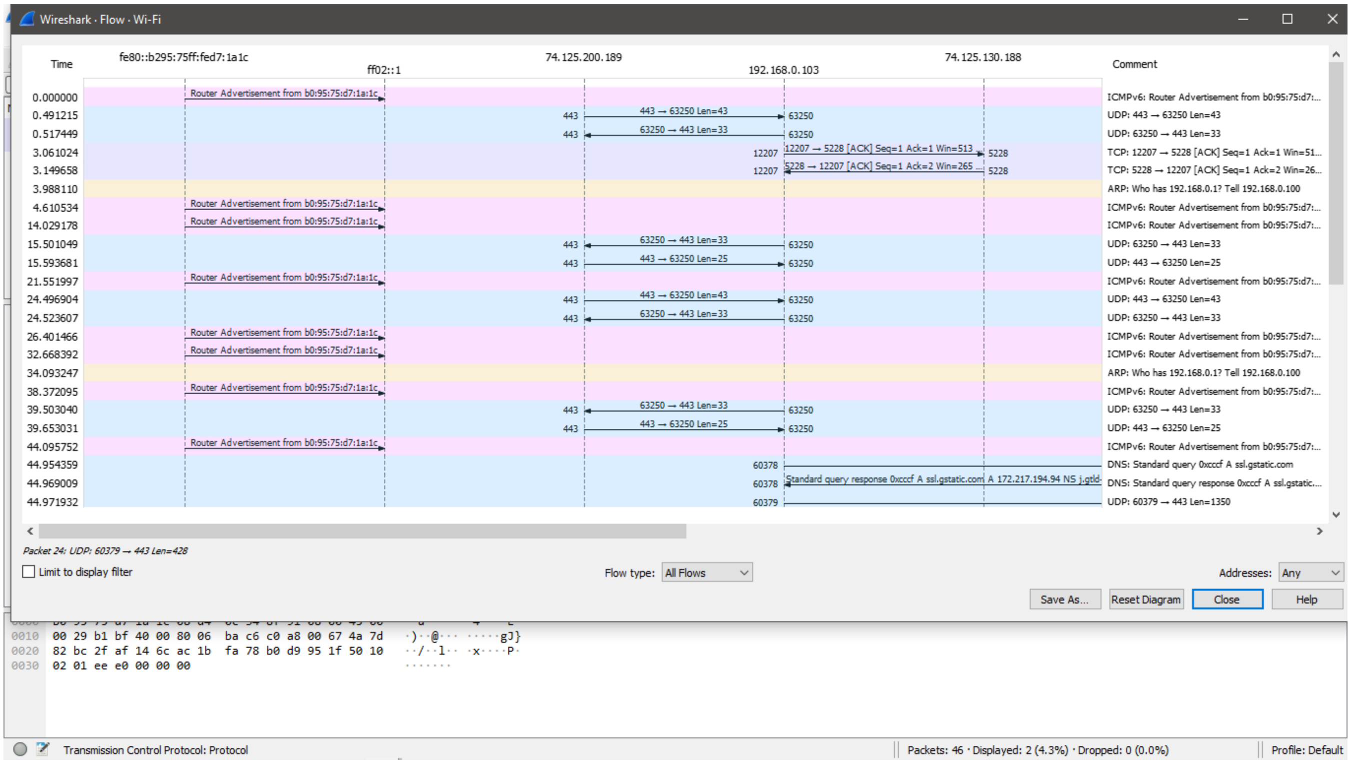
```
0000  ff ff ff ff ff ff dc 4a  3e eb 88 a7 08 00 45 00   ·······J >·····E·
0010  01 48 99 20 00 00 80 11  00 00 00 00 00 00 ff ff   ·H· ···· ········
0020  ff ff 00 44 00 43 01 34  c1 4a 01 01 06 00 02 84   ···D·C·4 ·J······
0030  eb de 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 dc 4a  3e eb 88 a7 00 00 00 00   ·······J >·······
```

wireshark_Ethernet_20200925214148_a11428.pcapng | Packets: 216 · Displayed: 216 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure-4.2: Analyzing different protocols from Wired Network Data

## Step 5- Plotting a flow graph:

The Plotting can be done through the “Statistics” menu. First we select the “Statistics” menu and then go to “Flow Graph”. Then for a plotting the flow of a particular protocol, we can select an option from “Flow Type”. Here the given example below shows the “TCP Flows” has been selected as the “Flow Type”.



| Time | fe80::b295:75ff:fed7:1a1c → ff02::1 | 74.125.200.189 ↔ 192.168.0.103 ↔ 74.125.130.188 | Comment |
|---|---|---|---|
| 0.000000 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 0.491215 | | 443 443 → 63250 Len=43 63250 | UDP: 443 → 63250 Len=43 |
| 0.517449 | | 443 63250 → 443 Len=33 63250 | UDP: 63250 → 443 Len=33 |
| 3.061024 | | 12207 12207 → 5228 [ACK] Seq=1 Ack=1 Win=513 ... 5228 | TCP: 12207 → 5228 [ACK] Seq=1 Ack=1 Win=51... |
| 3.149658 | | 12207 5228 → 12207 [ACK] Seq=1 Ack=2 Win=265 ... 5228 | TCP: 5228 → 12207 [ACK] Seq=1 Ack=2 Win=26... |
| 3.988110 | | | ARP: Who has 192.168.0.1? Tell 192.168.0.100 |
| 4.610534 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 14.029178 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 15.501049 | | 443 63250 → 443 Len=33 63250 | UDP: 63250 → 443 Len=33 |
| 15.593681 | | 443 443 → 63250 Len=25 63250 | UDP: 443 → 63250 Len=25 |
| 21.551997 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 24.496904 | | 443 443 → 63250 Len=43 63250 | UDP: 443 → 63250 Len=43 |
| 24.523607 | | 443 63250 → 443 Len=33 63250 | UDP: 63250 → 443 Len=33 |
| 26.401466 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 32.668392 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 34.093247 | | | ARP: Who has 192.168.0.1? Tell 192.168.0.100 |
| 38.372095 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 39.503040 | | 443 63250 → 443 Len=33 63250 | UDP: 63250 → 443 Len=33 |
| 39.653031 | | 443 443 → 63250 Len=25 63250 | UDP: 443 → 63250 Len=25 |
| 44.095752 | Router Advertisement from b0:95:75:d7:1a:1c | | ICMPv6: Router Advertisement from b0:95:75:d7:... |
| 44.954359 | | 60378 | DNS: Standard query 0xcccf A ssl.gstatic.com |
| 44.969009 | | 60378 Standard query response 0xcccf A ssl.gstatic.com A 172.217.194.94 NS j.gtld- | DNS: Standard query response 0xcccf A ssl.gstatic.... |
| 44.971932 | | 60379 | UDP: 60379 → 443 Len=1350 |

*Packet 24: UDP: 60379 → 443 Len=428*

☐ Limit to display filter

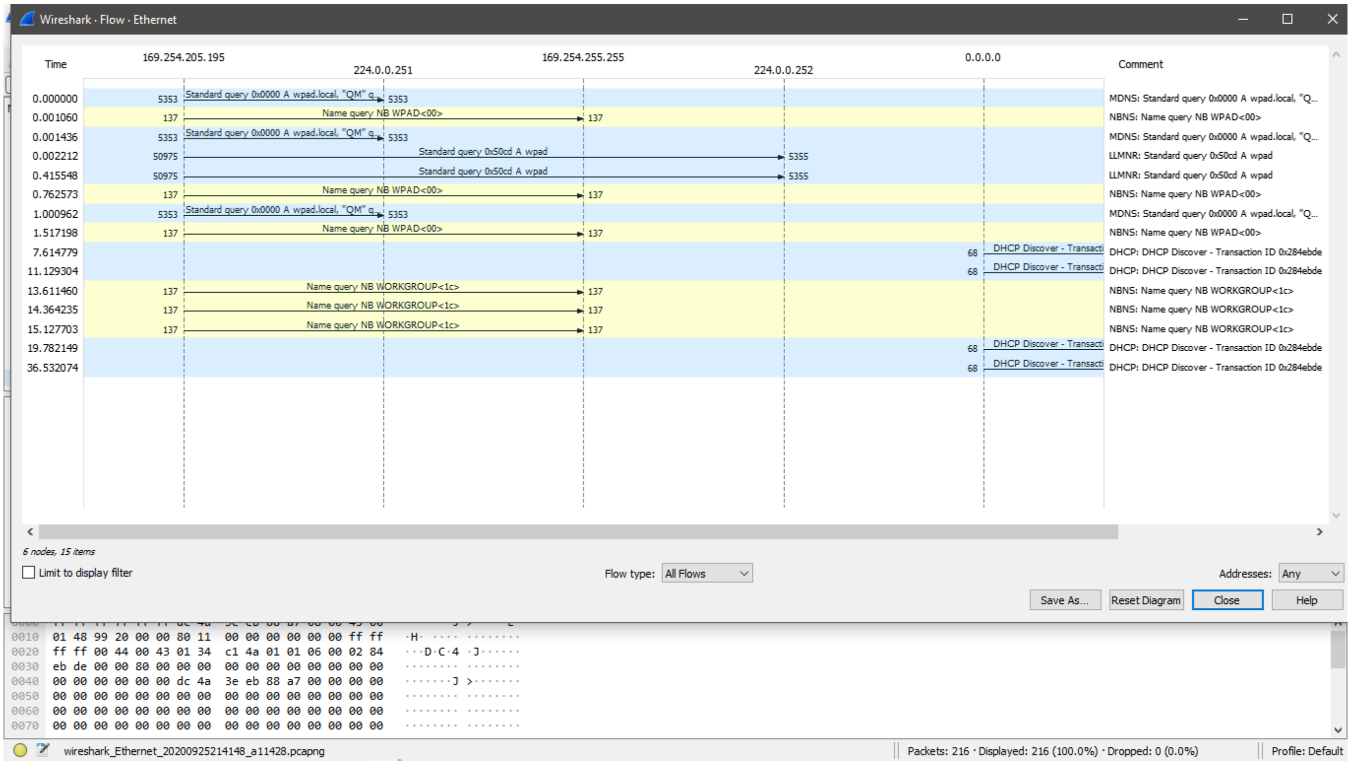
Flow type: All Flows

Addresses: Any

```
0010  00 29 b1 bf 40 00 80 06  ba c6 c0 a8 00 67 4a 7d   ·)··@··· ·····gJ}
0020  82 bc 2f af 14 6c ac 1b  fa 78 b0 d9 95 1f 50 10   ··/··l·· ·x····P·
0030  02 01 ee e0 00 00 00                               ·······
```

Transmission Control Protocol: Protocol | Packets: 46 · Displayed: 2 (4.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure-5.1: Plotting a graph for all flows of Wireless Network Data

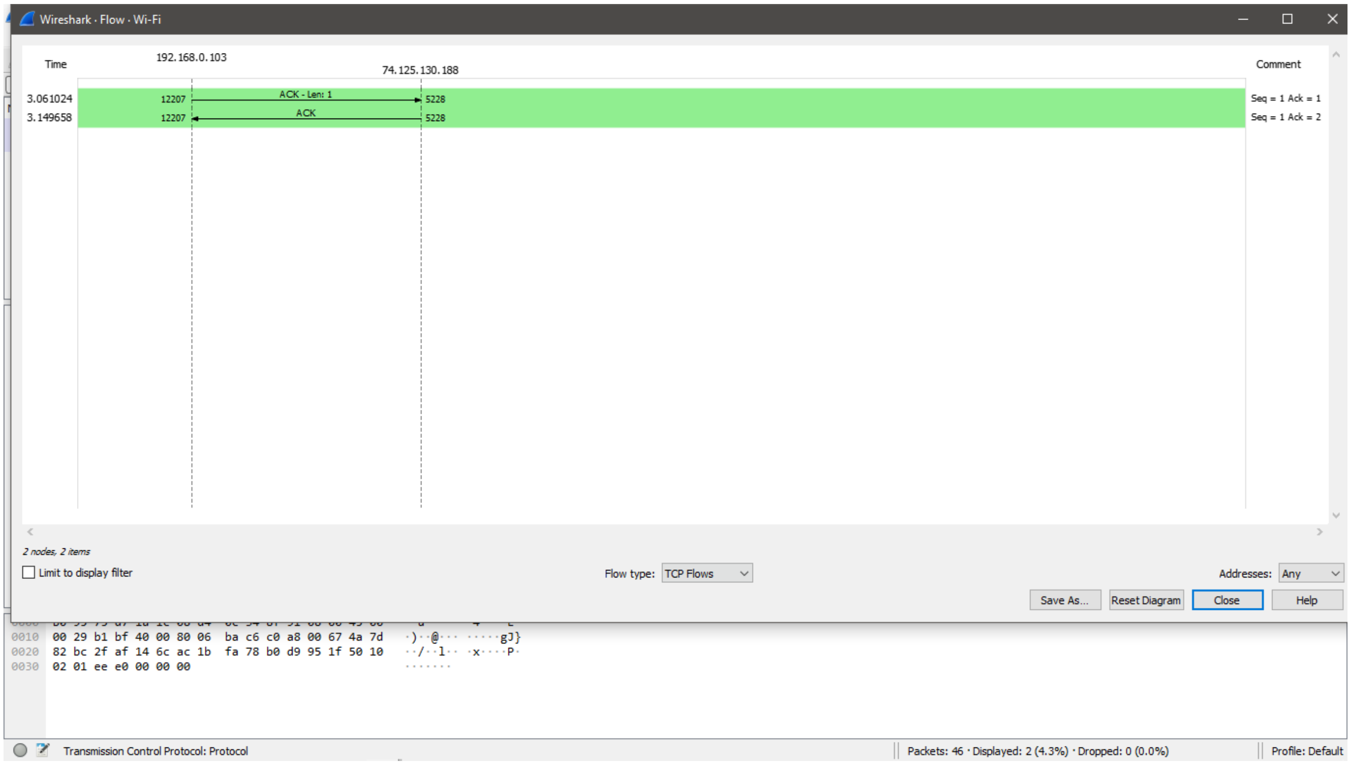


```
Time       169.254.205.195   224.0.0.251   169.254.255.255   224.0.0.252   0.0.0.0   Comment

0.000000   5353  Standard query 0x0000 A wpad.local, "QM" q... 5353          MDNS: Standard query 0x0000 A wpad.local, "Q...
0.001060   137   Name query NB WPAD<00>                          137           NBNS: Name query NB WPAD<00>
0.001436   5353  Standard query 0x0000 A wpad.local, "QM" q... 5353          MDNS: Standard query 0x0000 A wpad.local, "Q...
0.002212   50975 Standard query 0x50cd A wpad                    5355          LLMNR: Standard query 0x50cd A wpad
0.415548   50975 Standard query 0x50cd A wpad                    5355          LLMNR: Standard query 0x50cd A wpad
0.762573   137   Name query NB WPAD<00>                          137           NBNS: Name query NB WPAD<00>
1.000962   5353  Standard query 0x0000 A wpad.local, "QM" q... 5353          MDNS: Standard query 0x0000 A wpad.local, "Q...
1.517198   137   Name query NB WPAD<00>                          137           NBNS: Name query NB WPAD<00>
7.614779   68    DHCP Discover - Transacti                                     DHCP: DHCP Discover - Transaction ID 0x284ebde
11.129304  68    DHCP Discover - Transacti                                     DHCP: DHCP Discover - Transaction ID 0x284ebde
13.611460  137   Name query NB WORKGROUP<1c>                     137           NBNS: Name query NB WORKGROUP<1c>
14.364235  137   Name query NB WORKGROUP<1c>                     137           NBNS: Name query NB WORKGROUP<1c>
15.127703  137   Name query NB WORKGROUP<1c>                     137           NBNS: Name query NB WORKGROUP<1c>
19.782149  68    DHCP Discover - Transacti                                     DHCP: DHCP Discover - Transaction ID 0x284ebde
36.532074  68    DHCP Discover - Transacti                                     DHCP: DHCP Discover - Transaction ID 0x284ebde
```

```
0010  01 48 99 20 00 00 80 11  00 00 00 00 00 00 ff ff   ·H· ···· ········
0020  ff ff 00 44 00 43 01 34  c1 4a 01 01 06 00 02 84   ···D·C·4 ·J······
0030  eb de 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 dc 4a  3e eb 88 a7 00 00 00 00   ·······J >·······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

```
wireshark_Ethernet_20200925214148_a11428.pcapng    Packets: 216 · Displayed: 216 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure-5.2: Plotting a graph for all flows of Wired Network Data



*2 nodes, 2 items*

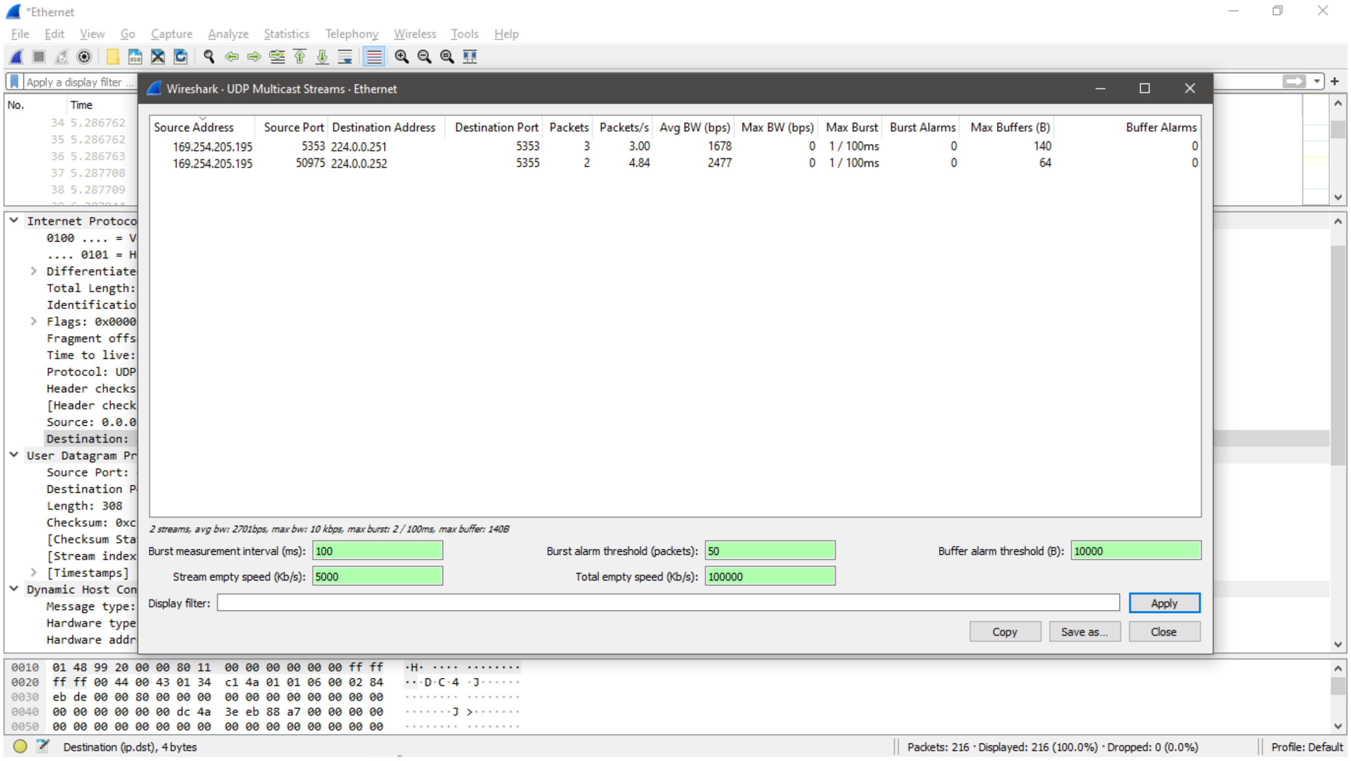
□ Limit to display filter

```
0010  00 29 b1 bf 40 00 80 06  ba c6 c0 a8 00 67 4a 7d   ·)··@··· ·····gJ}
0020  82 bc 2f af 14 6c ac 1b  fa 78 b0 d9 95 1f 50 10   ··/··l·· ·x····P·
0030  02 01 ee e0 00 00 00                               ·······
```

Transmission Control Protocol: Protocol

Packets: 46 · Displayed: 2 (4.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure-5.3: Plotting a graph for TCP flows of Wireless Network data



```
No.   Time
   34 5.286762
   35 5.286762
   36 5.286763
   37 5.287708
   38 5.287709
```

```
v Internet Protoco
    0100 .... = V
    .... 0101 = H
  > Differentiate
    Total Length:
    Identificatio
  > Flags: 0x0000
    Fragment offs
    Time to live:
    Protocol: UDP
    Header checks
    [Header check
    Source: 0.0.0
    Destination:
v User Datagram Pr
    Source Port:
    Destination P
    Length: 308
    Checksum: 0xc
    [Checksum Sta
    [Stream index
  > [Timestamps]
v Dynamic Host Con
    Message type:
    Hardware type
    Hardware addr
```

| Source Address | Source Port | Destination Address | Destination Port | Packets | Packets/s | Avg BW (bps) | Max BW (bps) | Max Burst | Burst Alarms | Max Buffers (B) | Buffer Alarms |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 169.254.205.195 | 5353 | 224.0.0.251 | 5353 | 3 | 3.00 | 1678 | 0 | 1 / 100ms | 0 | 140 | 0 |
| 169.254.205.195 | 50975 | 224.0.0.252 | 5355 | 2 | 4.84 | 2477 | 0 | 1 / 100ms | 0 | 64 | 0 |

*2 streams, avg bw: 2701bps, max bw: 10 kbps, max burst: 2 / 100ms, max buffer: 140B*

Burst measurement interval (ms): 100
Burst alarm threshold (packets): 50
Buffer alarm threshold (B): 10000
Stream empty speed (Kb/s): 5000
Total empty speed (Kb/s): 100000
Display filter:

```
0010  01 48 99 20 00 00 80 11  00 00 00 00 00 00 ff ff   ·H· ···· ········
0020  ff ff 00 44 00 43 01 34  c1 4a 01 01 06 00 02 84   ··D·C·4 ·J······
0030  eb de 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 dc 4a  3e eb 88 a7 00 00 00 00   ·······J >·······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Destination (ip.dst), 4 bytes

Packets: 216 · Displayed: 216 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure-5.4: Plotting a graph for UDP Multicast Streams of Wired Network data

## **Conclusion**:

From this lab, we’ve learnt how to compare between wired and wireless network data protocols after capturing them by using Wireshark. The comparative analysis helps us to understand how packets and protocols of wired and wireless networks are transferred. The Wireshark helps us to visualize the flow of the protocols which helps us to understand the protocol flow more accurately.