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: S.M. Tanzim Hasan

ID: IT-16061

4th year 2ndsemester

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

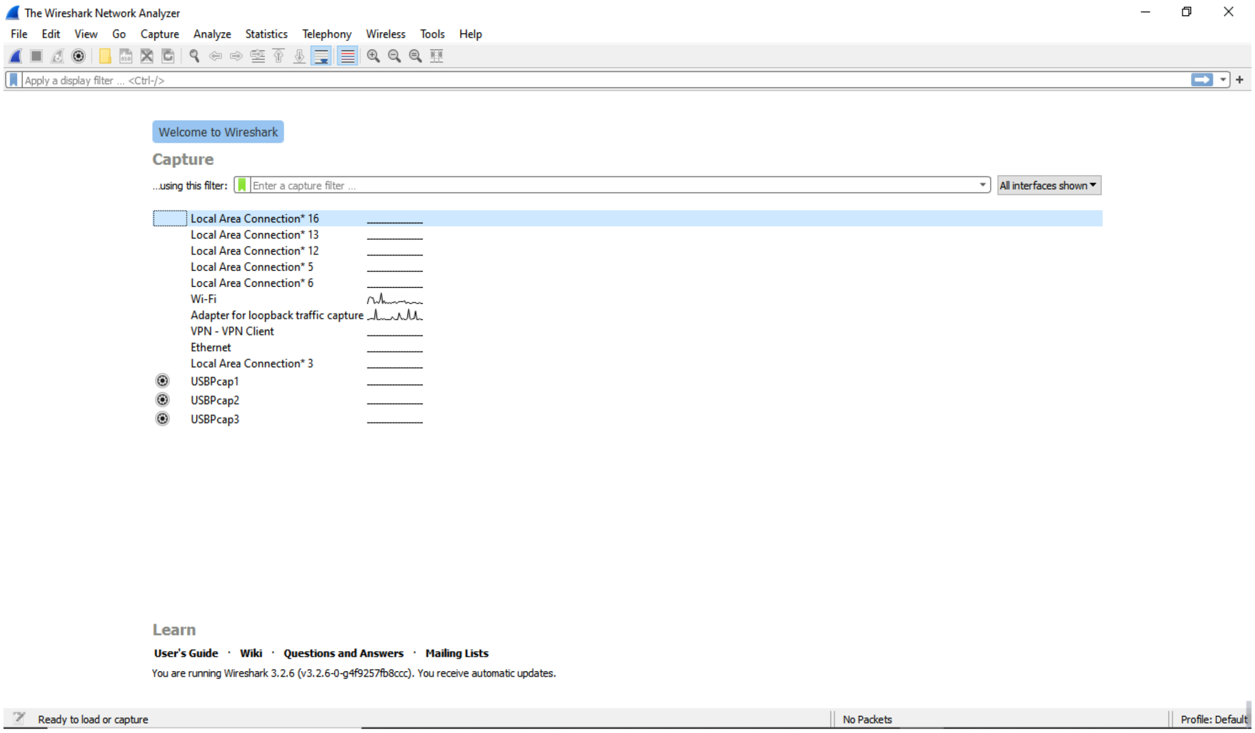
Objectives:

- 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:

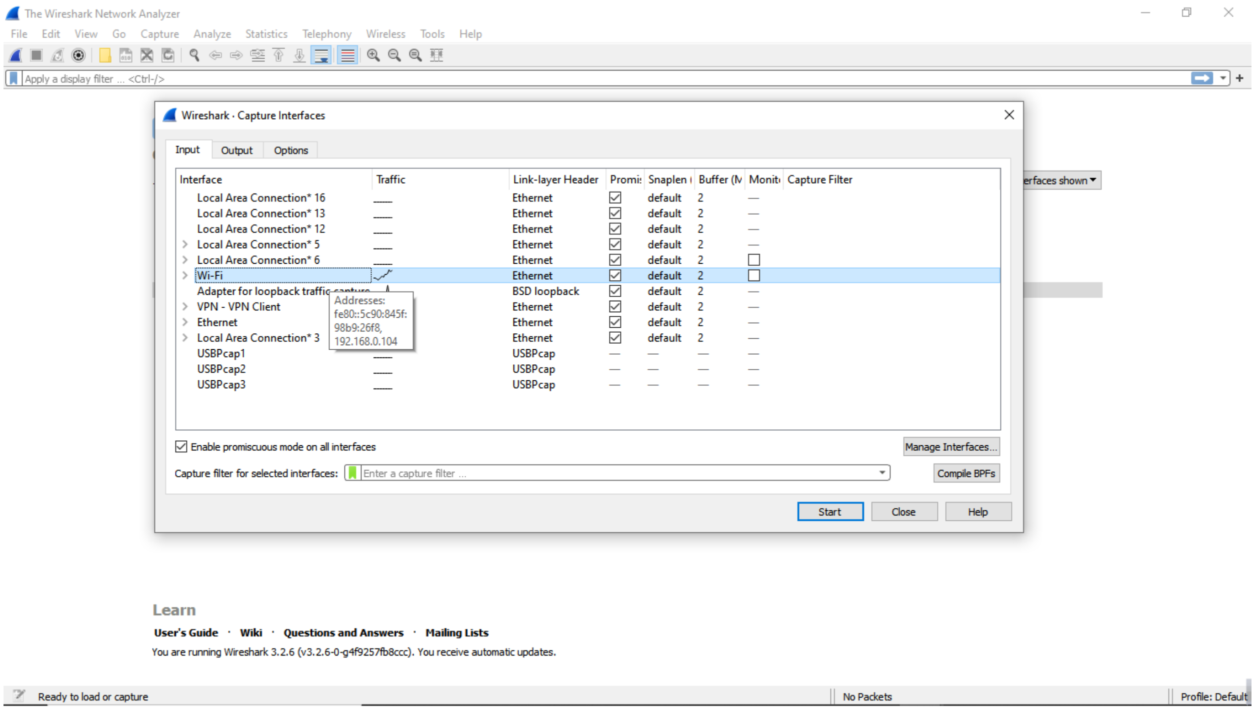
By clicking Capture menu the process of capturing will be started. It will show the available interfaces list. Then, we need to start Capturing on interface that has IP address

Capturing can be stopped by clicking on Stop the running capture button on the main toolbar.



You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.

Fig 1: Wireshark Interface List


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
erfaces shown
Manage Interfaces...
Compile BPFs
Start
Close
Help

Interface	Traffic	Link-layer Header	Promis	Snaplen	Buffer (M	Monit	Capture Filter
Local Area Connection* 16		Ethernet	☑	default	2	—	
Local Area Connection* 13		Ethernet	☑	default	2	—	
Local Area Connection* 12		Ethernet	☑	default	2	—	
Local Area Connection* 5		Ethernet	☑	default	2	—	
Local Area Connection* 6		Ethernet	☑	default	2	□	
Wi-Fi		Ethernet	☑	default	2	□	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
VPN - VPN Client		Ethernet	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	
Local Area Connection* 3		Ethernet	☑	default	2	—	
USBPcap1		USBPcap	—	—	—	—	
USBPcap2		USBPcap	—	—	—	—	
USBPcap3		USBPcap	—	—	—	—	

Addresses:
fe80::5c90:845f:98b9:26f8,
192.168.0.104

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

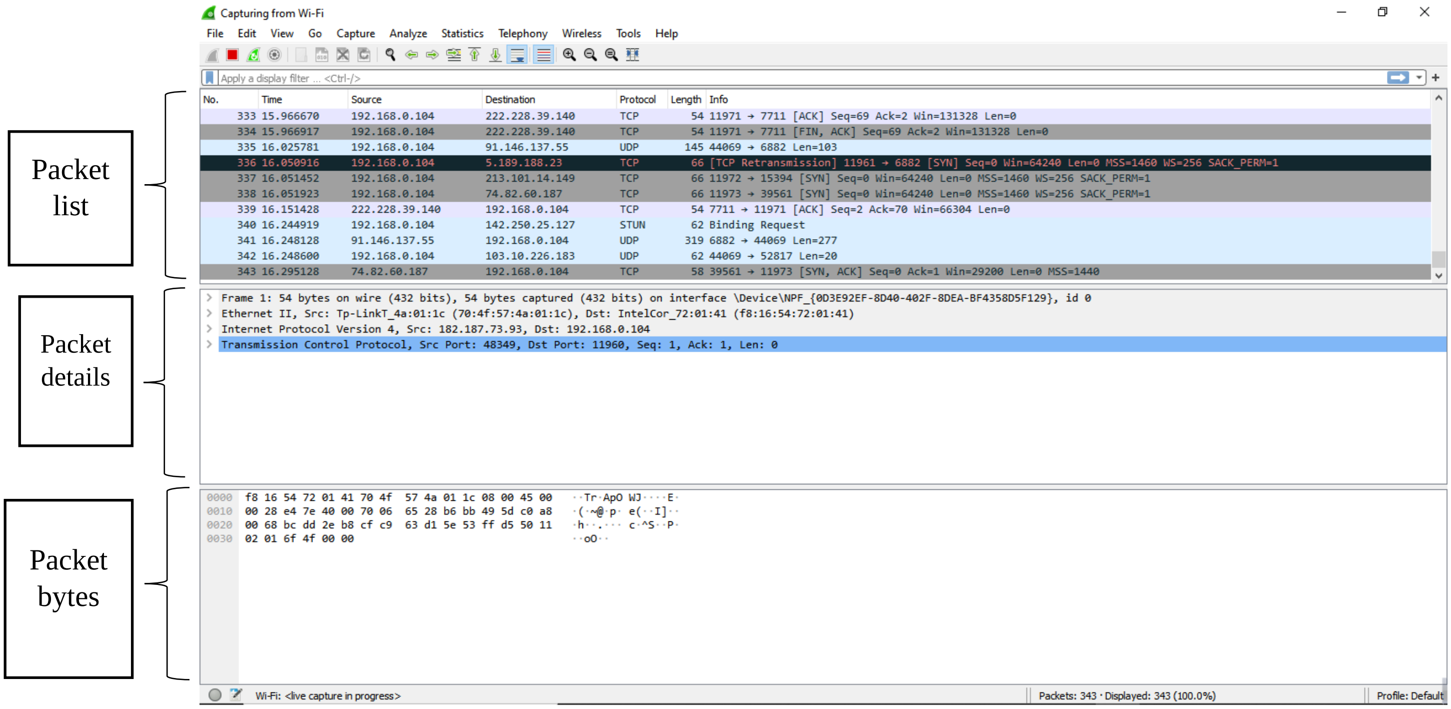
Learn

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

You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.

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

Fig 2: Capturing Interface that has IP address


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

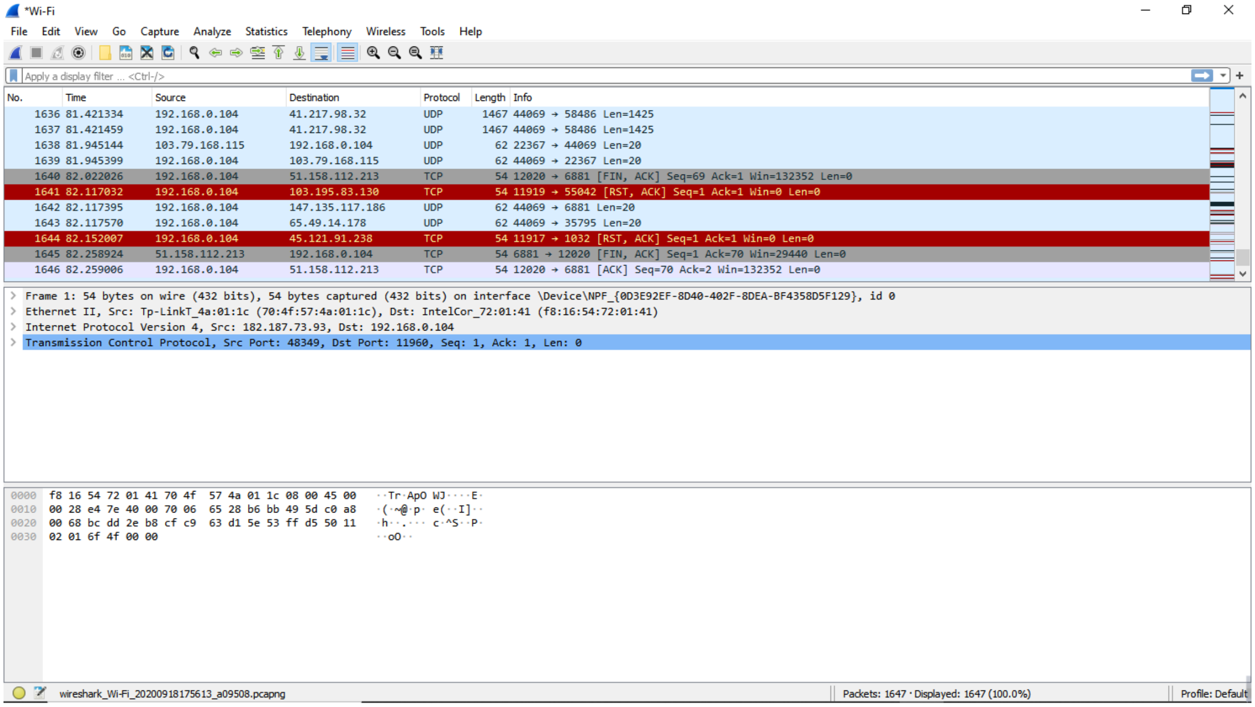
```
No.   Time        Source           Destination       Protocol  Length Info
  333 15.966670   192.168.0.104    222.228.39.140    TCP         54 11971 → 7711 [ACK] Seq=69 Ack=2 Win=131328 Len=0
  334 15.966917   192.168.0.104    222.228.39.140    TCP         54 11971 → 7711 [FIN, ACK] Seq=69 Ack=2 Win=131328 Len=0
  335 16.025781   192.168.0.104    91.146.137.55     UDP        145 44069 → 6882 Len=103
  336 16.050916   192.168.0.104    5.189.188.23      TCP         66 [TCP Retransmission] 11961 → 6882 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  337 16.051452   192.168.0.104    213.101.14.149    TCP         66 11972 → 15394 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  338 16.051923   192.168.0.104    74.82.60.187      TCP         66 11973 → 39561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  339 16.151428   222.228.39.140   192.168.0.104     TCP         54 7711 → 11971 [ACK] Seq=2 Ack=70 Win=66304 Len=0
  340 16.244919   192.168.0.104    142.250.25.127    STUN        62 Binding Request
  341 16.248128   91.146.137.55    192.168.0.104     UDP        319 6882 → 44069 Len=277
  342 16.248600   192.168.0.104    103.10.226.183    UDP         62 44069 → 52817 Len=20
  343 16.295128   74.82.60.187     192.168.0.104     TCP         58 39561 → 11973 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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
```

```
0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 28 e4 7e 40 00 70 06  65 28 b6 bb 49 5d c0 a8   ·(·~@·p· e(··I]··
0020  00 68 bc dd 2e b8 cf c9  63 d1 5e 53 ff d5 50 11   ·h··.··· c·^S··P·
0030  02 01 6f 4f 00 00                                  ··oO··
```

Wi-Fi: <live capture in progress> | Packets: 343 · Displayed: 343 (100.0%) | Profile: Default

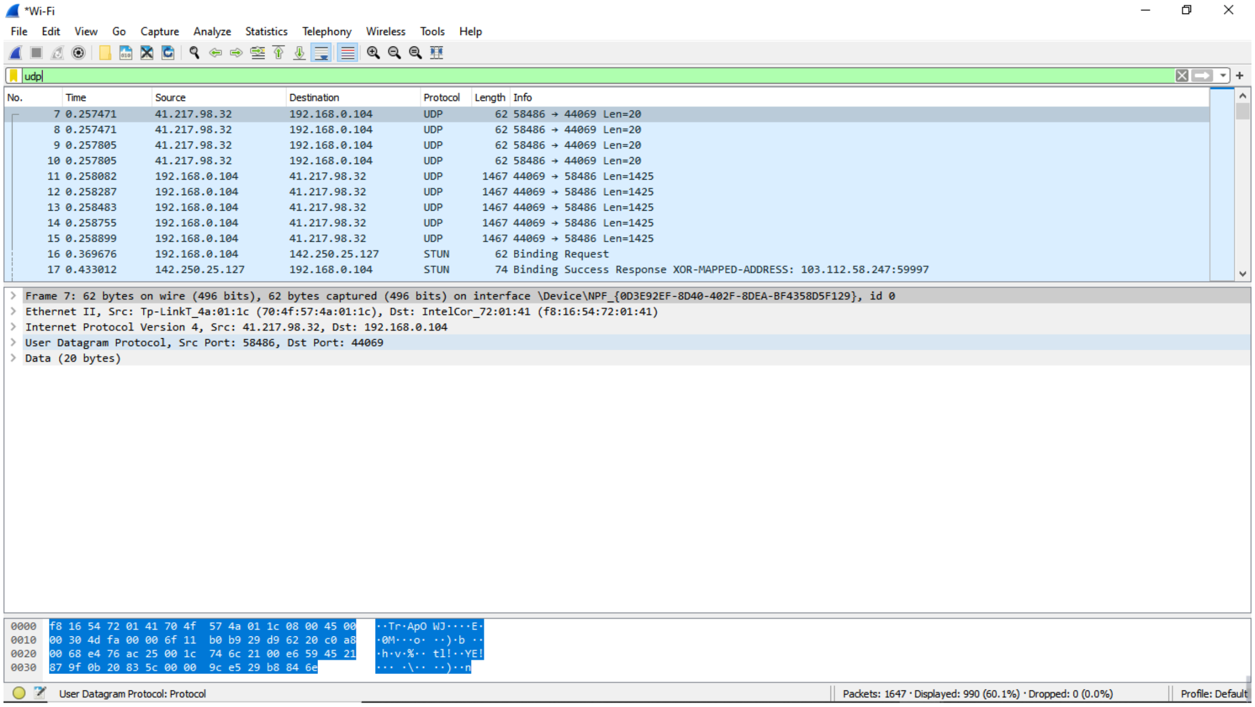
Fig 3: A sample packet capture window


*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
  1636 81.421334  192.168.0.104   41.217.98.32     UDP      1467 44069 → 58486 Len=1425
  1637 81.421459  192.168.0.104   41.217.98.32     UDP      1467 44069 → 58486 Len=1425
  1638 81.945144  103.79.168.115  192.168.0.104    UDP        62 22367 → 44069 Len=20
  1639 81.945399  192.168.0.104   103.79.168.115   UDP        62 44069 → 22367 Len=20
  1640 82.022026  192.168.0.104   51.158.112.213   TCP        54 12020 → 6881 [FIN, ACK] Seq=69 Ack=1 Win=132352 Len=0
  1641 82.117032  192.168.0.104   103.195.83.130   TCP        54 11919 → 55042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  1642 82.117395  192.168.0.104   147.135.117.186  UDP        62 44069 → 6881 Len=20
  1643 82.117570  192.168.0.104   65.49.14.178     UDP        62 44069 → 35795 Len=20
  1644 82.152007  192.168.0.104   45.121.91.238    TCP        54 11917 → 1032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  1645 82.258924  51.158.112.213  192.168.0.104    TCP        54 6881 → 12020 [FIN, ACK] Seq=1 Ack=70 Win=29440 Len=0
  1646 82.259006  192.168.0.104   51.158.112.213   TCP        54 12020 → 6881 [ACK] Seq=70 Ack=2 Win=132352 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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

0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 28 e4 7e 40 00 70 06  65 28 b6 bb 49 5d c0 a8   ·(·~@·p· e(··I]··
0020  00 68 bc dd 2e b8 cf c9  63 d1 5e 53 ff d5 50 11   ·h··.··· c·^S··P·
0030  02 01 6f 4f 00 00                                  ··oO··

wireshark_Wi-Fi_20200918175613_a09508.pcapng    Packets: 1647 · Displayed: 1647 (100.0%)    Profile: Default
```

Fig 4: Stopping Capture

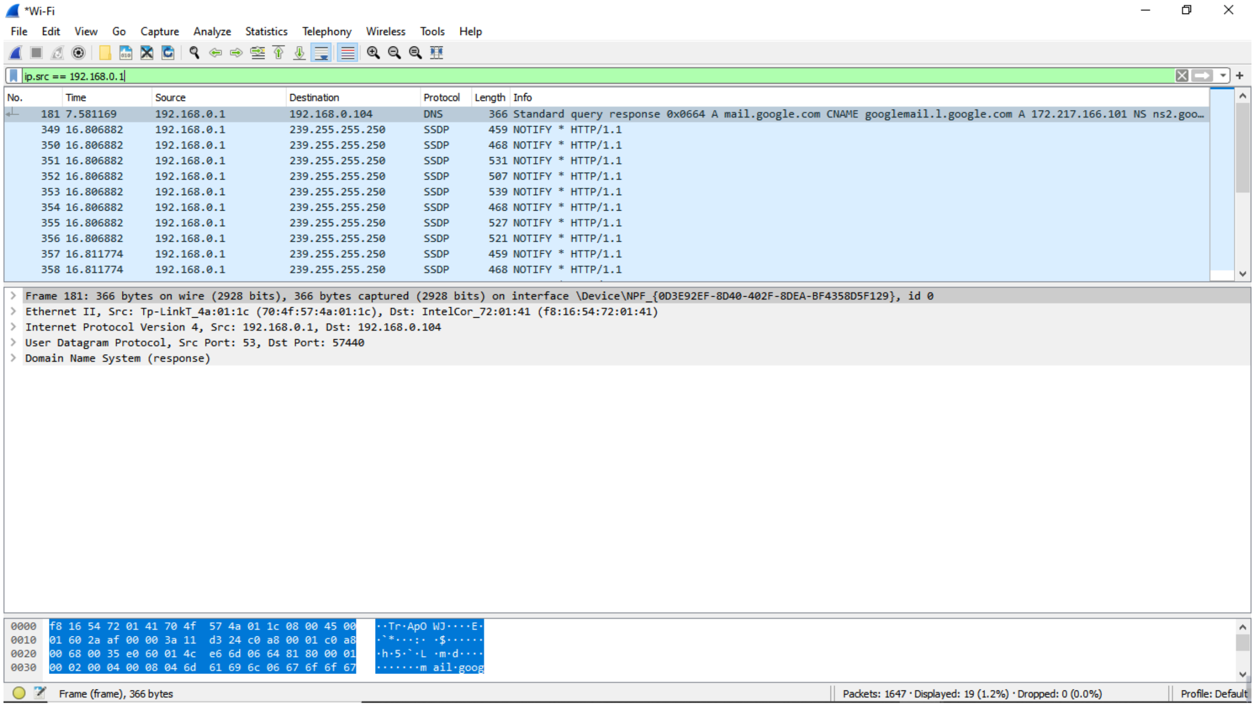
Filtering:


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

```
udp

No.  Time      Source          Destination     Protocol Length Info
   7 0.257471  41.217.98.32    192.168.0.104   UDP        62 58486 → 44069 Len=20
   8 0.257471  41.217.98.32    192.168.0.104   UDP        62 58486 → 44069 Len=20
   9 0.257805  41.217.98.32    192.168.0.104   UDP        62 58486 → 44069 Len=20
  10 0.257805  41.217.98.32    192.168.0.104   UDP        62 58486 → 44069 Len=20
  11 0.258082  192.168.0.104   41.217.98.32    UDP      1467 44069 → 58486 Len=1425
  12 0.258287  192.168.0.104   41.217.98.32    UDP      1467 44069 → 58486 Len=1425
  13 0.258483  192.168.0.104   41.217.98.32    UDP      1467 44069 → 58486 Len=1425
  14 0.258755  192.168.0.104   41.217.98.32    UDP      1467 44069 → 58486 Len=1425
  15 0.258899  192.168.0.104   41.217.98.32    UDP      1467 44069 → 58486 Len=1425
  16 0.369676  192.168.0.104   142.250.25.127  STUN       62 Binding Request
  17 0.433012  142.250.25.127  192.168.0.104   STUN       74 Binding Success Response XOR-MAPPED-ADDRESS: 103.112.58.247:59997

> Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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: 41.217.98.32, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 58486, Dst Port: 44069
> Data (20 bytes)

0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 30 4d fa 00 00 6f 11  b0 b9 29 d9 62 20 c0 a8   ·0M···o· ··)·b ··
0020  00 68 e4 76 ac 25 00 1c  74 6c 21 00 e6 59 45 21   ·h·v·%·· tl!··YE!
0030  87 9f 0b 20 83 5c 00 00  9c e5 29 b8 84 6e         ··· ·\·· ··)··n

User Datagram Protocol: Protocol    Packets: 1647 · Displayed: 990 (60.1%) · Dropped: 0 (0.0%)    Profile: Default
```

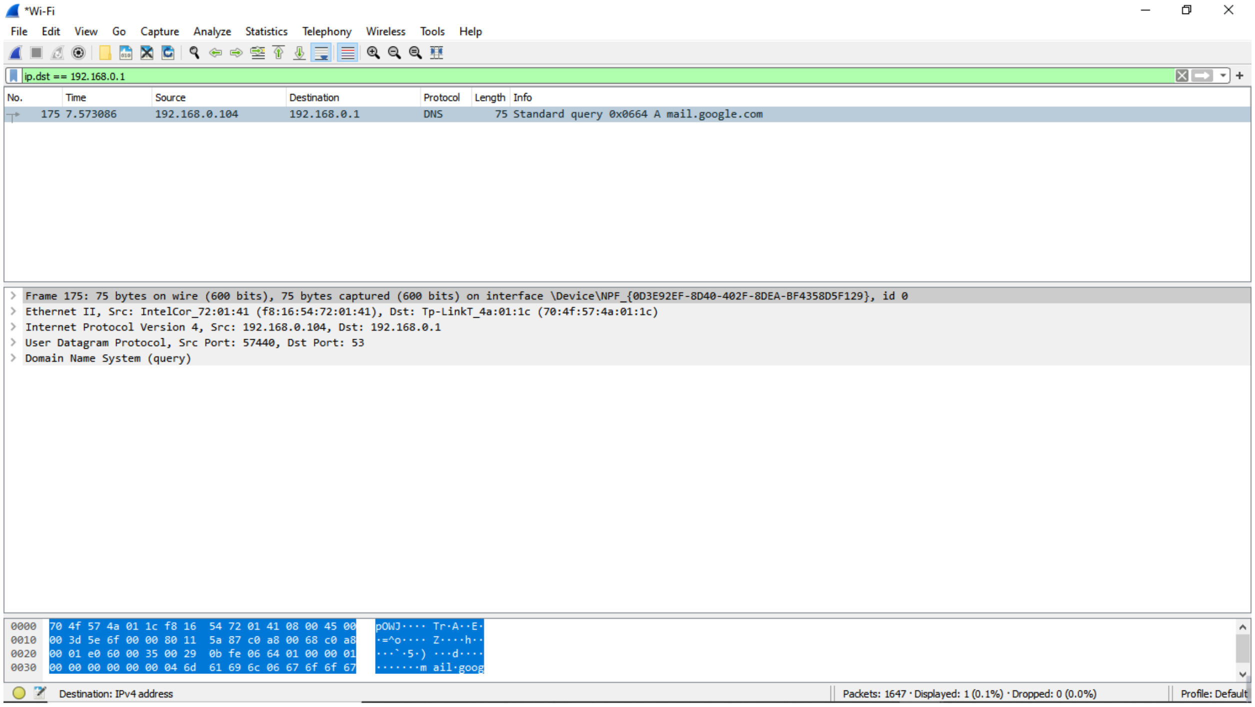
Fig 5: Filter by Protocol

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.


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

```
ip.src == 192.168.0.1

No.  Time       Source        Destination      Protocol Length Info
 181 7.581169   192.168.0.1   192.168.0.104    DNS      366 Standard query response 0x0664 A mail.google.com CNAME googlemail.l.google.com A 172.217.166.101 NS ns2.goo…
 349 16.806882  192.168.0.1   239.255.255.250  SSDP     459 NOTIFY * HTTP/1.1
 350 16.806882  192.168.0.1   239.255.255.250  SSDP     468 NOTIFY * HTTP/1.1
 351 16.806882  192.168.0.1   239.255.255.250  SSDP     531 NOTIFY * HTTP/1.1
 352 16.806882  192.168.0.1   239.255.255.250  SSDP     507 NOTIFY * HTTP/1.1
 353 16.806882  192.168.0.1   239.255.255.250  SSDP     539 NOTIFY * HTTP/1.1
 354 16.806882  192.168.0.1   239.255.255.250  SSDP     468 NOTIFY * HTTP/1.1
 355 16.806882  192.168.0.1   239.255.255.250  SSDP     527 NOTIFY * HTTP/1.1
 356 16.806882  192.168.0.1   239.255.255.250  SSDP     521 NOTIFY * HTTP/1.1
 357 16.811774  192.168.0.1   239.255.255.250  SSDP     459 NOTIFY * HTTP/1.1
 358 16.811774  192.168.0.1   239.255.255.250  SSDP     468 NOTIFY * HTTP/1.1

> Frame 181: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 57440
> Domain Name System (response)

0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  01 60 2a af 00 00 3a 11  d3 24 c0 a8 00 01 c0 a8   ·`*···:· ·$······
0020  00 68 00 35 e0 60 01 4c  e6 6d 06 64 81 80 00 01   ·h·5·`·L ·m·d····
0030  00 02 00 04 00 08 04 6d  61 69 6c 06 67 6f 6f 67   ·······m ail·goog

Frame (frame), 366 bytes        Packets: 1647 · Displayed: 19 (1.2%) · Dropped: 0 (0.0%)        Profile: Default
```

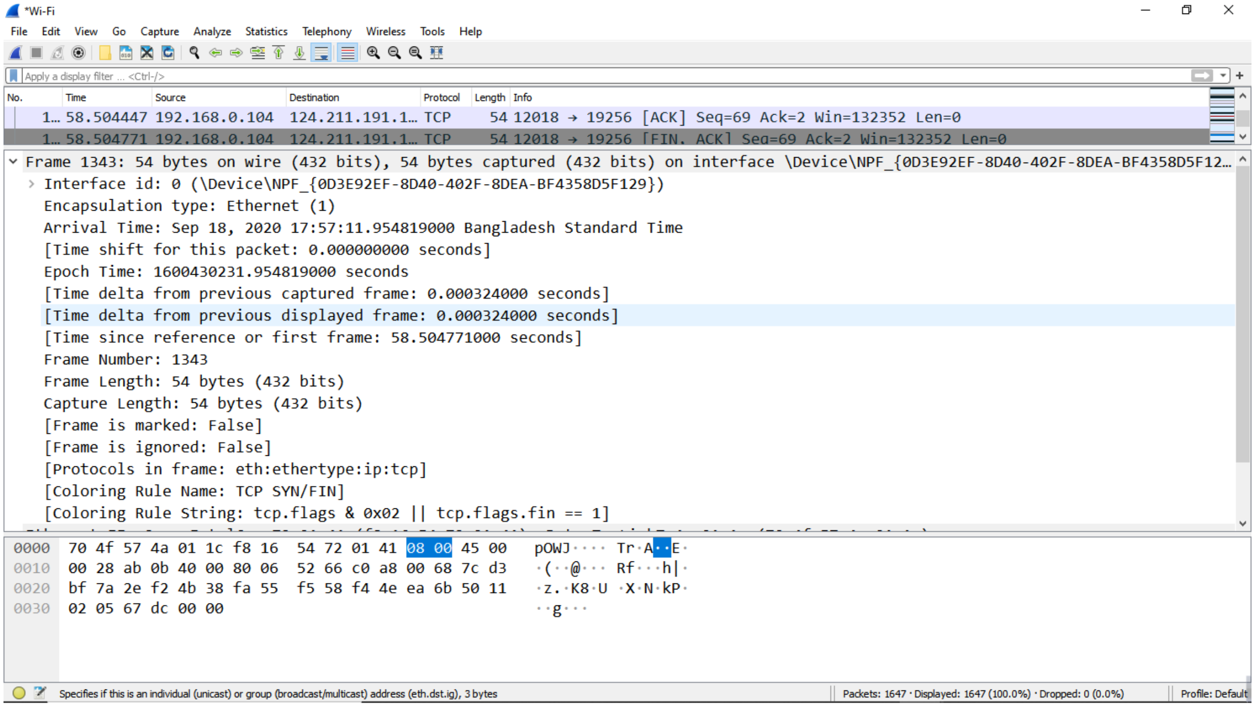
Fig 6: Source IP filter


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

```
ip.dst == 192.168.0.1

No.  Time       Source          Destination    Protocol Length Info
 175 7.573086   192.168.0.104   192.168.0.1    DNS       75 Standard query 0x0664 A mail.google.com

> Frame 175: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 57440, Dst Port: 53
> Domain Name System (query)

0000  70 4f 57 4a 01 1c f8 16  54 72 01 41 08 00 45 00   pOWJ···· Tr·A··E·
0010  00 3d 5e 6f 00 00 80 11  5a 87 c0 a8 00 68 c0 a8   ·=^o···· Z····h··
0020  00 01 e0 60 00 35 00 29  0b fe 06 64 01 00 00 01   ···`·5·) ···d····
0030  00 00 00 00 00 00 04 6d  61 69 6c 06 67 6f 6f 67   ·······m ail·goog

Destination: IPv4 address        Packets: 1647 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%)        Profile: Default
```

Fig 7: 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**



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

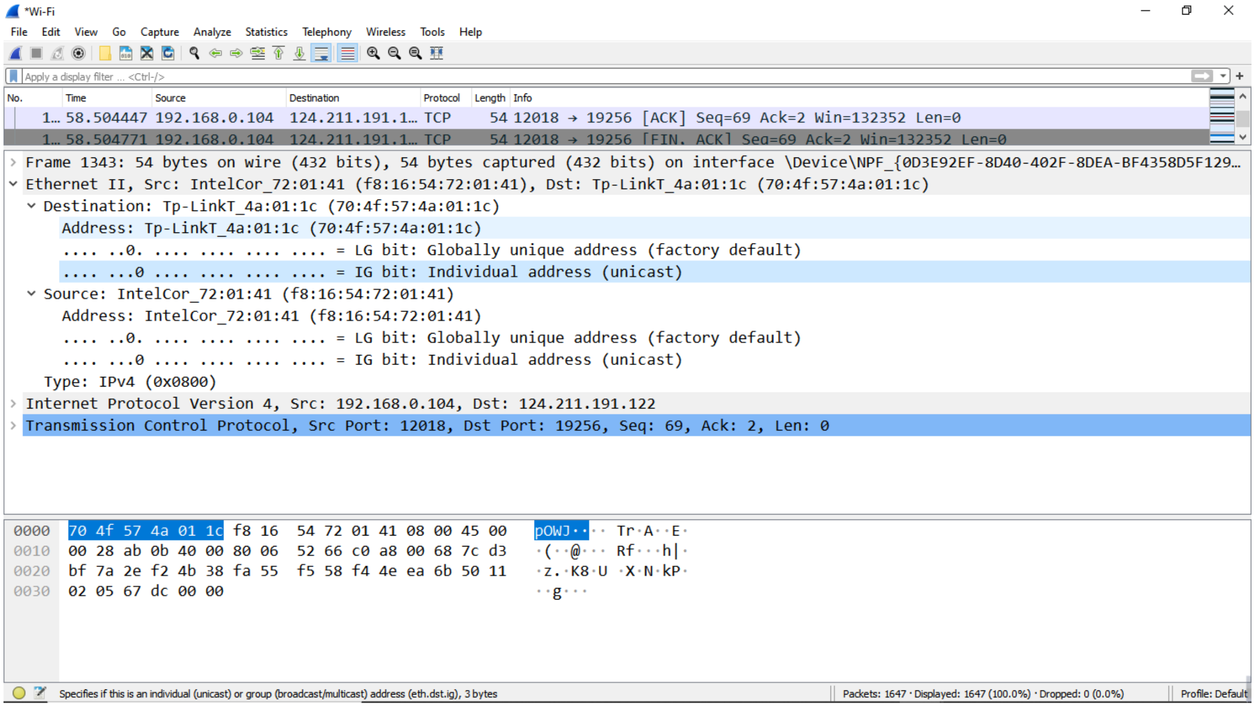
```
No.   Time      Source        Destination     Protocol Length Info
 1… 58.504447 192.168.0.104 124.211.191.1… TCP      54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
 1… 58.504771 192.168.0.104 124.211.191.1… TCP      54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0
```

```
˅ Frame 1343: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F12…
  › Interface id: 0 (\Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 17:57:11.954819000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600430231.954819000 seconds
    [Time delta from previous captured frame: 0.000324000 seconds]
    [Time delta from previous displayed frame: 0.000324000 seconds]
    [Time since reference or first frame: 58.504771000 seconds]
    Frame Number: 1343
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP SYN/FIN]
    [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
```

```
0000  70 4f 57 4a 01 1c f8 16  54 72 01 41 08 00 45 00   pOWJ····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···
```

```
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes    Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig 8: Packet Details Pane (Frame segment)



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

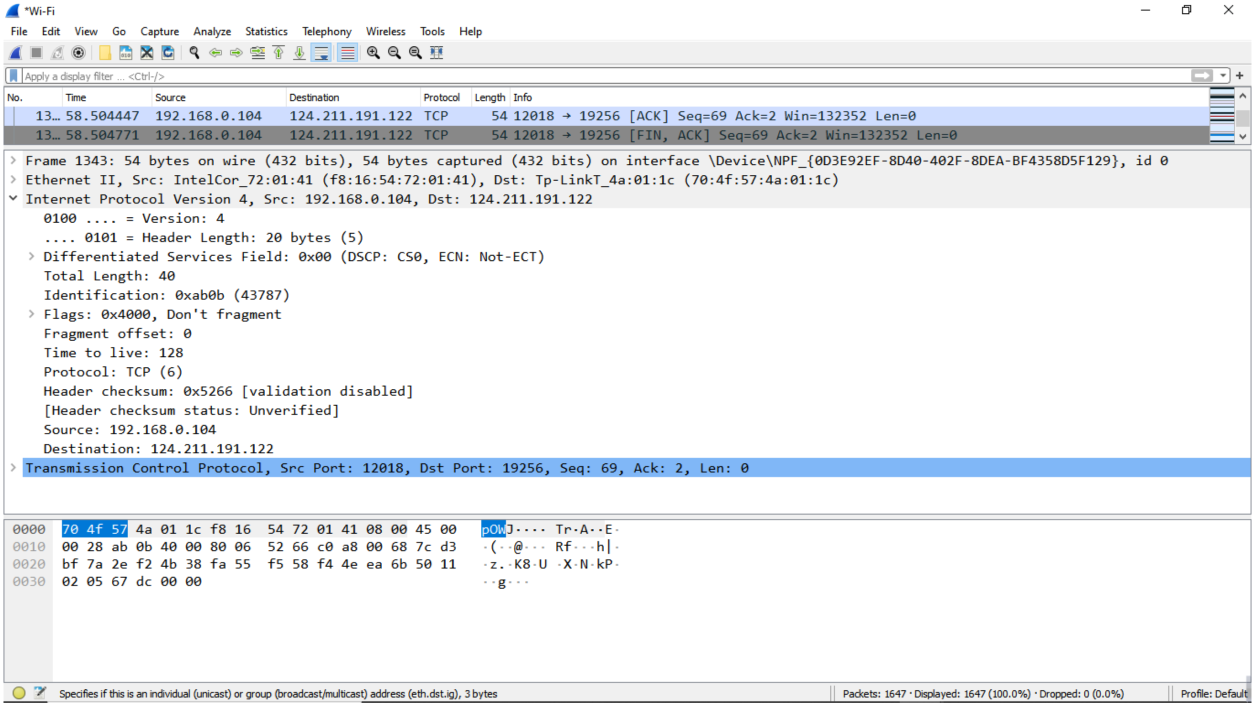
```
No.   Time      Source        Destination     Protocol Length Info
 1… 58.504447 192.168.0.104 124.211.191.1… TCP      54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
 1… 58.504771 192.168.0.104 124.211.191.1… TCP      54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0
```

```
› Frame 1343: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-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)
  ˅ 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)
  ˅ 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
```

```
0000  70 4f 57 4a 01 1c f8 16  54 72 01 41 08 00 45 00   pOWJ····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···
```

```
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes    Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig 9: Packet Details Pane (Ethernet Segment)


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

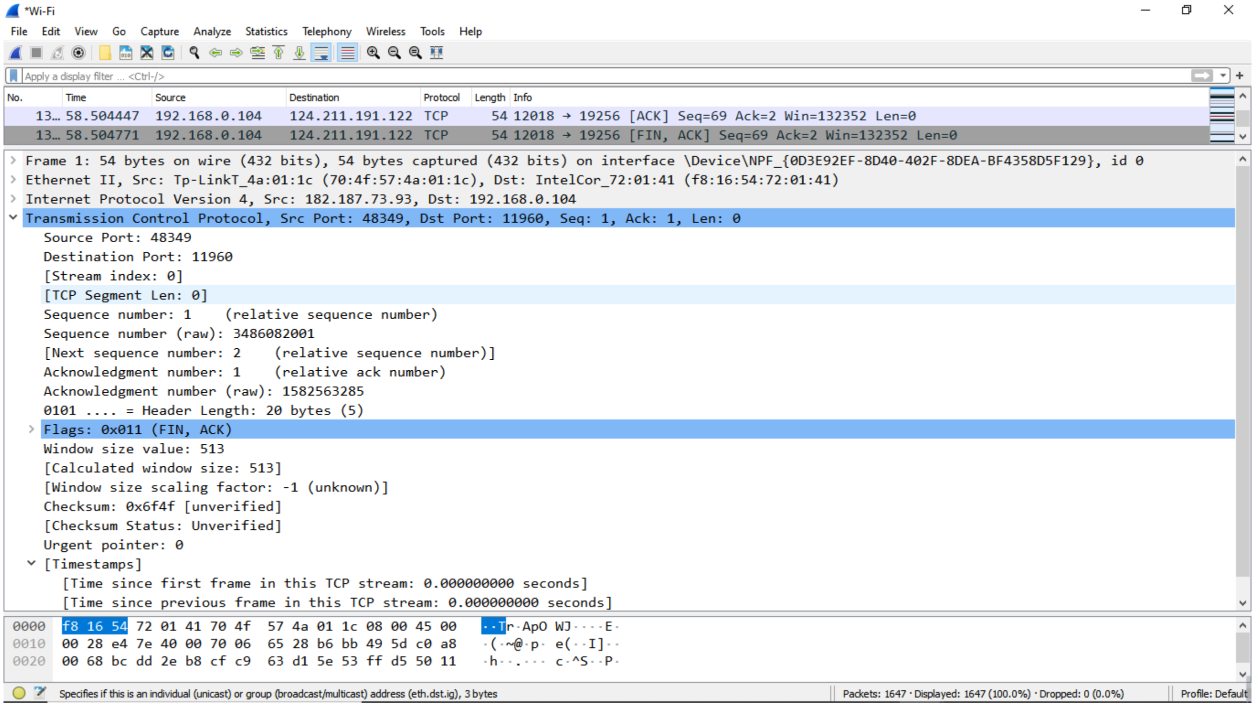
```
No.   Time        Source          Destination      Protocol Length Info
13… 58.504447  192.168.0.104   124.211.191.122  TCP      54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
13… 58.504771  192.168.0.104   124.211.191.122  TCP      54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0
```

```
> Frame 1343: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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 Internet Protocol Version 4, Src: 192.168.0.104, Dst: 124.211.191.122
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xab0b (43787)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x5266 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.104
    Destination: 124.211.191.122
> Transmission Control Protocol, Src Port: 12018, Dst Port: 19256, Seq: 69, Ack: 2, Len: 0
```

```
0000  70 4f 57 4a 01 1c f8 16  54 72 01 41 08 00 45 00   pOWJ···· 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···
```

```
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes | Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%) | Profile: Default
```

Fig 10: Packet Details Pane (IP segment)


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

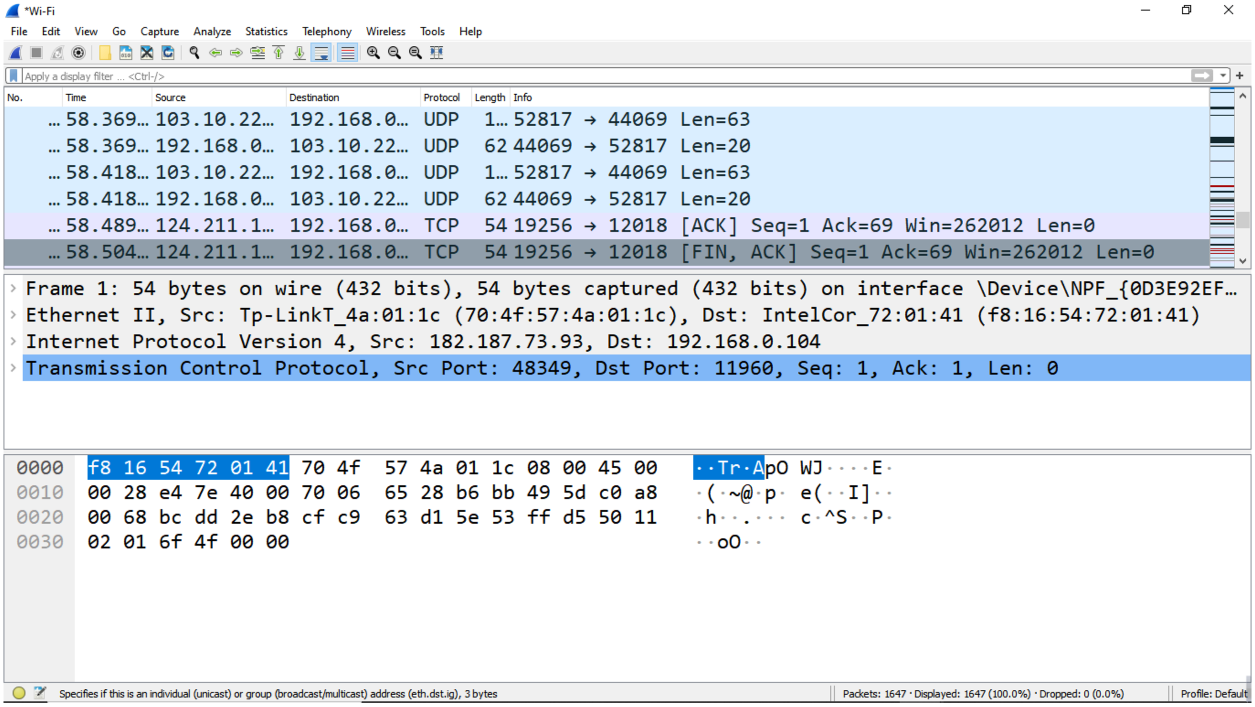
```
No.   Time        Source          Destination      Protocol Length Info
13… 58.504447  192.168.0.104   124.211.191.122  TCP      54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
13… 58.504771  192.168.0.104   124.211.191.122  TCP      54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> 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
v Transmission Control Protocol, Src Port: 48349, Dst Port: 11960, Seq: 1, Ack: 1, Len: 0
    Source Port: 48349
    Destination Port: 11960
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3486082001
    [Next sequence number: 2    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1582563285
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window size value: 513
    [Calculated window size: 513]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x6f4f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds]
      [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

```
0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 28 e4 7e 40 00 70 06  65 28 b6 bb 49 5d c0 a8   ·(·~@·p· e(··I]··
0020  00 68 bc dd 2e b8 cf c9  63 d1 5e 53 ff d5 50 11   ·h···.·· c·^S··P·
```

```
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes | Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%) | Profile: Default
```

Fig 11: Packet Details Pane (TCP Segment)


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

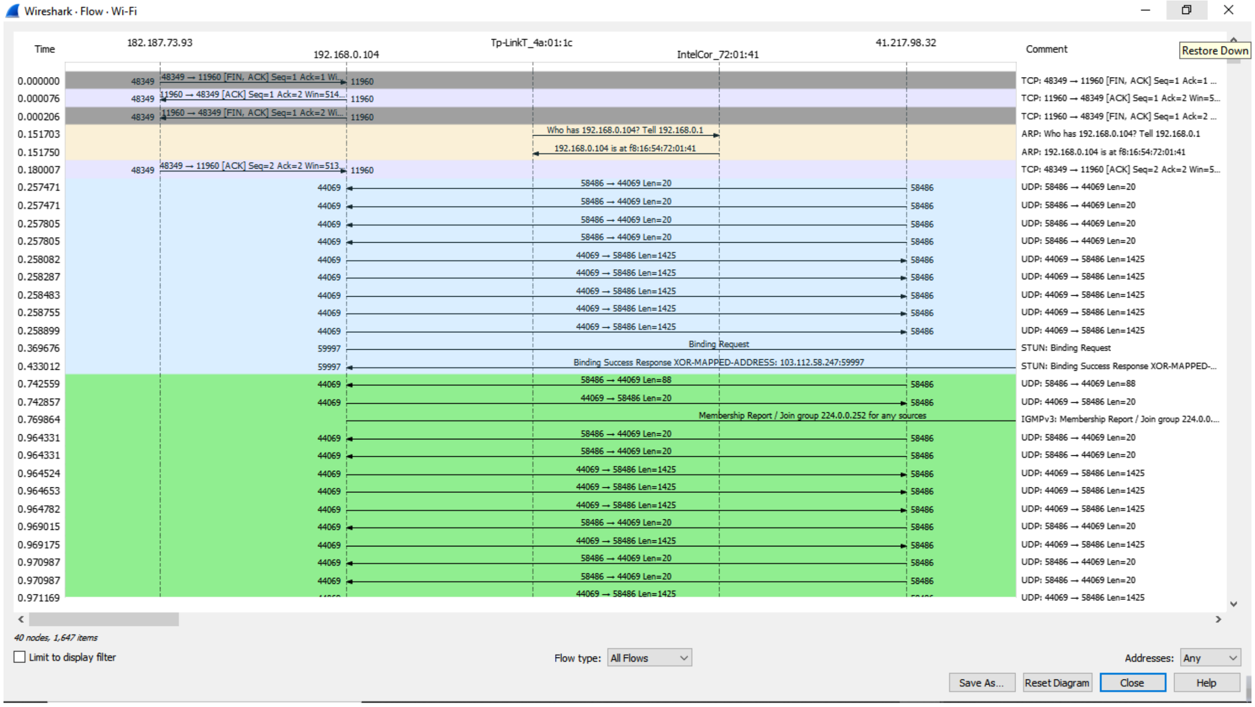
```
No.   Time        Source         Destination    Protocol  Length  Info
…     58.369…     103.10.22…     192.168.0…     UDP       1…      52817 → 44069 Len=63
…     58.369…     192.168.0…     103.10.22…     UDP       62      44069 → 52817 Len=20
…     58.418…     103.10.22…     192.168.0…     UDP       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
```

```
0000  f8 16 54 72 01 41 70 4f  57 4a 01 1c 08 00 45 00   ··Tr·ApO WJ····E·
0010  00 28 e4 7e 40 00 70 06  65 28 b6 bb 49 5d c0 a8   ·(·~@·p· e(··I]··
0020  00 68 bc dd 2e b8 cf c9  63 d1 5e 53 ff d5 50 11   ·h··.··· c·^S··P·
0030  02 01 6f 4f 00 00                                  ··oO··
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes | Packets: 1647 · Displayed: 1647 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig 12: Packet Byte Pane



```
Time       Comment
0.000000   TCP: 48349 → 11960 [FIN, ACK] Seq=1 Ack=1 ...
0.000076   TCP: 11960 → 48349 [ACK] Seq=1 Ack=2 Win=5...
0.000206   TCP: 11960 → 48349 [FIN, ACK] Seq=1 Ack=2 ...
0.151703   ARP: Who has 192.168.0.104? Tell 192.168.0.1
0.151750   ARP: 192.168.0.104 is at f8:16:54:72:01:41
0.180007   TCP: 48349 → 11960 [ACK] Seq=2 Ack=2 Win=5...
0.257471   UDP: 58486 → 44069 Len=20
0.257471   UDP: 58486 → 44069 Len=20
0.257805   UDP: 58486 → 44069 Len=20
0.257805   UDP: 58486 → 44069 Len=20
0.258082   UDP: 44069 → 58486 Len=1425
0.258287   UDP: 44069 → 58486 Len=1425
0.258483   UDP: 44069 → 58486 Len=1425
0.258755   UDP: 44069 → 58486 Len=1425
0.258899   UDP: 44069 → 58486 Len=1425
0.369676   STUN: Binding Request
0.433012   STUN: Binding Success Response XOR-MAPPED-...
0.742559   UDP: 58486 → 44069 Len=88
0.742857   UDP: 44069 → 58486 Len=20
0.769864   IGMPv3: Membership Report / Join group 224.0.0....
0.964331   UDP: 58486 → 44069 Len=20
0.964331   UDP: 58486 → 44069 Len=20
0.964524   UDP: 44069 → 58486 Len=1425
0.964653   UDP: 44069 → 58486 Len=1425
0.964782   UDP: 44069 → 58486 Len=1425
0.969015   UDP: 58486 → 44069 Len=20
0.969175   UDP: 44069 → 58486 Len=1425
0.970987   UDP: 58486 → 44069 Len=20
0.970987   UDP: 58486 → 44069 Len=20
0.971169   UDP: 44069 → 58486 Len=1425
```

Binding Success Response XOR-MAPPED-ADDRESS: 103.112.58.247:59997

Membership Report / Join group 224.0.0.252 for any sources

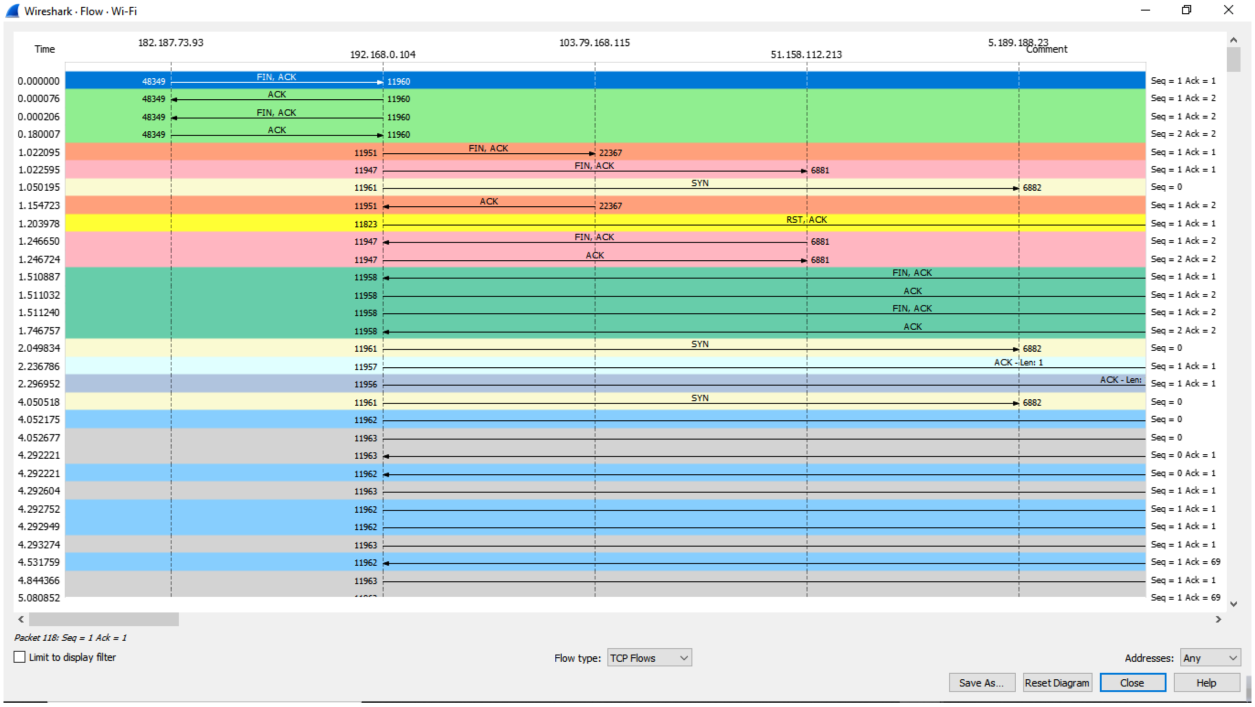
40 nodes, 1,647 items

□ Limit to display filter

Flow type: All Flows

Addresses: Any

Fig 13: Statistics- Flow Graph(All Flows)



Time	182.187.73.93	192.168.0.104	103.79.168.115	51.158.112.213	5.189.188.23		Comment
0.000000	48349	11960				FIN, ACK	Seq = 1 Ack = 1
0.000076	48349	11960				ACK	Seq = 1 Ack = 2
0.000206	48349	11960				FIN, ACK	Seq = 1 Ack = 2
0.180007	48349	11960				ACK	Seq = 2 Ack = 2
1.022095		11951	22367			FIN, ACK	Seq = 1 Ack = 1
1.022595		11947		6881		FIN, ACK	Seq = 1 Ack = 1
1.050195		11961			6882	SYN	Seq = 0
1.154723		11951	22367			ACK	Seq = 1 Ack = 2
1.203978		11823				RST, ACK	Seq = 1 Ack = 1
1.246650		11947		6881		FIN, ACK	Seq = 1 Ack = 2
1.246724		11947		6881		ACK	Seq = 2 Ack = 2
1.510887		11958				FIN, ACK	Seq = 1 Ack = 1
1.511032		11958				ACK	Seq = 1 Ack = 2
1.511240		11958				FIN, ACK	Seq = 1 Ack = 2
1.746757		11958				ACK	Seq = 2 Ack = 2
2.049834		11961			6882	SYN	Seq = 0
2.236786		11957				ACK - Len: 1	Seq = 1 Ack = 1
2.296952		11956				ACK - Len:	Seq = 1 Ack = 1
4.050518		11961			6882	SYN	Seq = 0
4.052175		11962					Seq = 0
4.052677		11963					Seq = 0
4.292221		11963					Seq = 0 Ack = 1
4.292221		11962					Seq = 0 Ack = 1
4.292604		11963					Seq = 1 Ack = 1
4.292752		11962					Seq = 1 Ack = 1
4.292949		11962					Seq = 1 Ack = 1
4.293274		11963					Seq = 1 Ack = 1
4.531759		11962					Seq = 1 Ack = 69
4.844366		11963					Seq = 1 Ack = 1
5.080852							Seq = 1 Ack = 69

Packet 118: Seq = 1 Ack = 1

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

Fig 13: Statistics- Flow Graph (TCP Flows)

Conclusion:

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.