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 Habibur Rahman

ID:IT-16051

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:

1. live packet data capturing from a network interface.
2. Have to display packets with very detailed protocol information.
3. Filter packets on many criteria.
4. Search for packets on many criteria.
5. Colorize packet display based on filters.
6. Create various statistics.

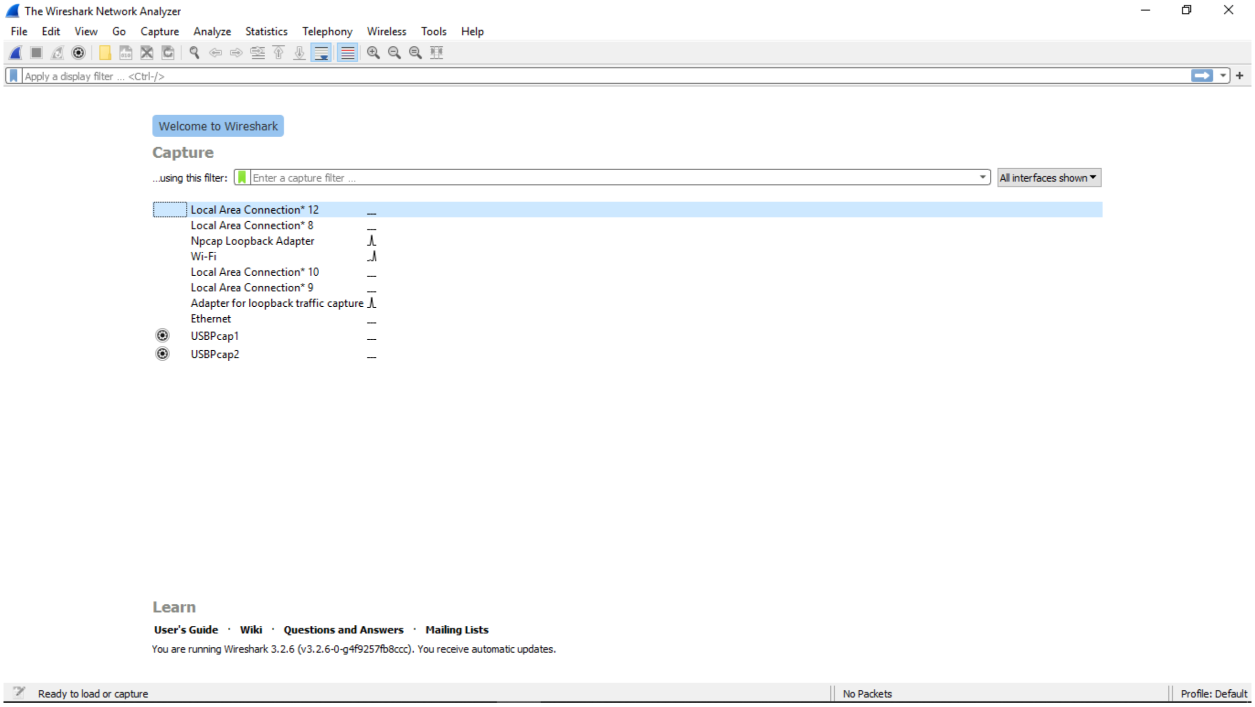
Capture the Packets:

If we click any menu option, then it will show the available interfaces list.

After clicking the menu, 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.

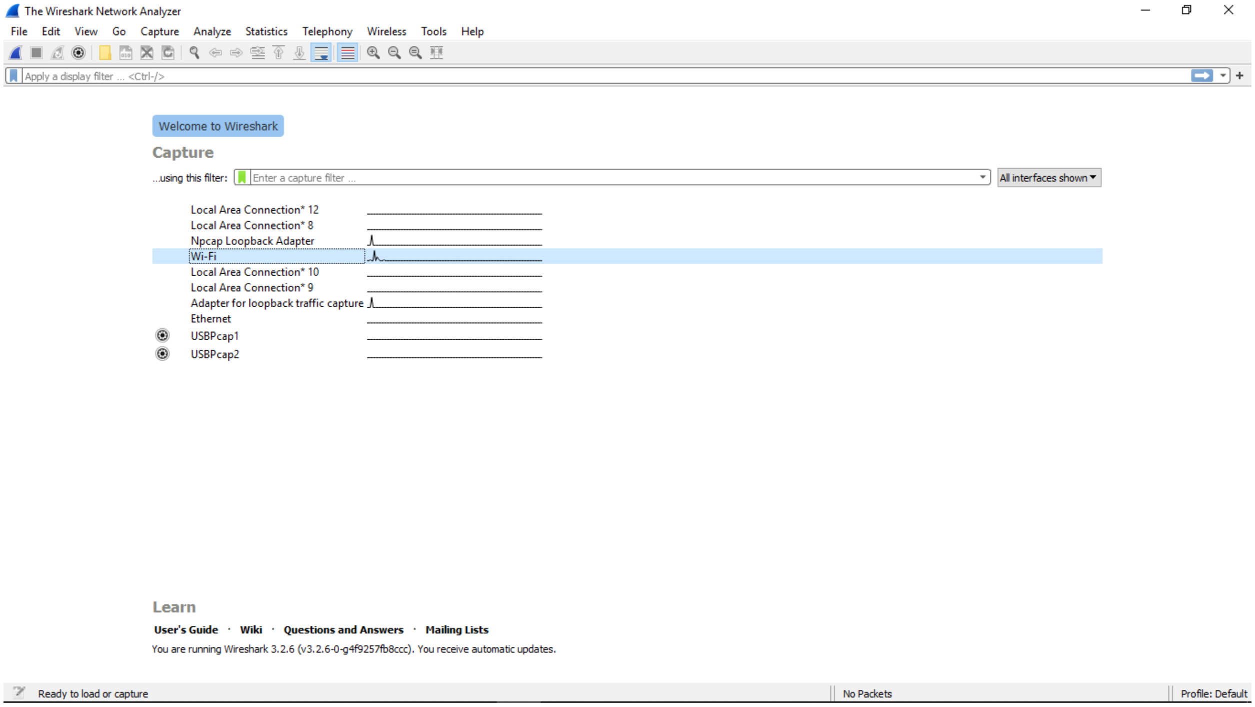

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Local Area Connection* 12
Local Area Connection* 8
Npcap Loopback Adapter
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Adapter for loopback traffic capture
Ethernet
USBPcap1
USBPcap2

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

Figure a: Wireshark Interface List


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
Local Area Connection* 12
Local Area Connection* 8
Npcap Loopback Adapter
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Adapter for loopback traffic capture
Ethernet
USBPcap1
USBPcap2
```

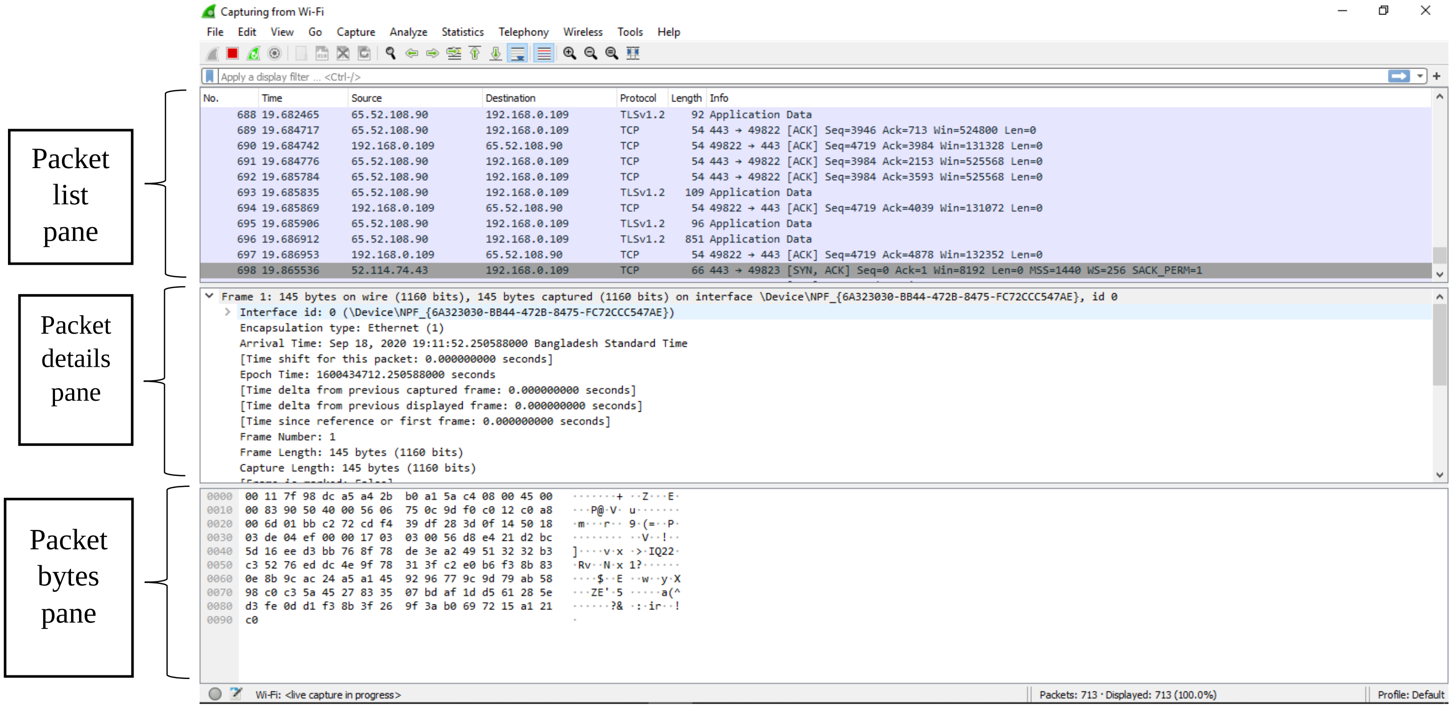
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default

Figure b: Start Capturing Interface that has IP address


Packet list pane
Packet details pane
Packet bytes pane
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
 688 19.682465   65.52.108.90   192.168.0.109  TLSv1.2    92 Application Data
 689 19.684717   65.52.108.90   192.168.0.109  TCP        54 443 → 49822 [ACK] Seq=3946 Ack=713 Win=524800 Len=0
 690 19.684742   192.168.0.109  65.52.108.90   TCP        54 49822 → 443 [ACK] Seq=4719 Ack=3984 Win=131328 Len=0
 691 19.684776   65.52.108.90   192.168.0.109  TCP        54 443 → 49822 [ACK] Seq=3984 Ack=2153 Win=525568 Len=0
 692 19.685784   65.52.108.90   192.168.0.109  TCP        54 443 → 49822 [ACK] Seq=3984 Ack=3593 Win=525568 Len=0
 693 19.685835   65.52.108.90   192.168.0.109  TLSv1.2   109 Application Data
 694 19.685869   192.168.0.109  65.52.108.90   TCP        54 49822 → 443 [ACK] Seq=4719 Ack=4039 Win=131072 Len=0
 695 19.685906   65.52.108.90   192.168.0.109  TLSv1.2    96 Application Data
 696 19.686912   65.52.108.90   192.168.0.109  TLSv1.2   851 Application Data
 697 19.686953   192.168.0.109  65.52.108.90   TCP        54 49822 → 443 [ACK] Seq=4719 Ack=4878 Win=132352 Len=0
 698 19.865536   52.114.74.43   192.168.0.109  TCP        66 443 → 49823 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
```

```
v Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE}, id 0
  > Interface id: 0 (\Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 19:11:52.250588000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600434712.250588000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 145 bytes (1160 bits)
    Capture Length: 145 bytes (1160 bits)
```

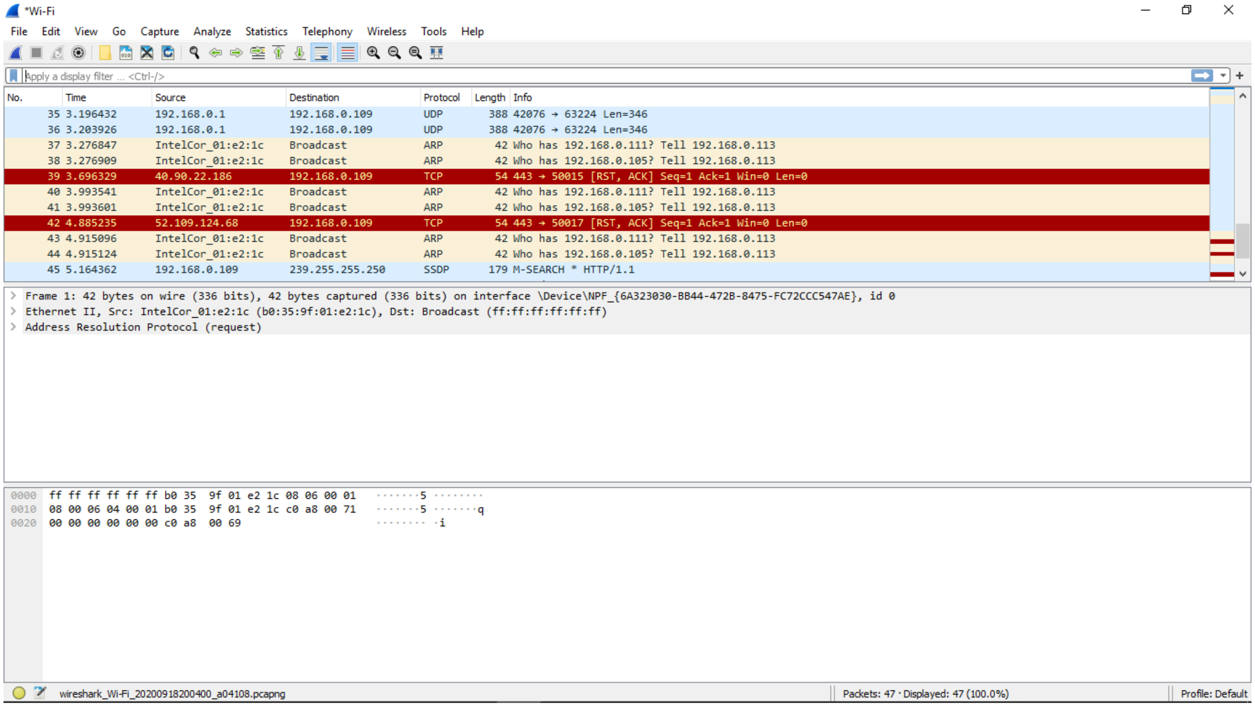
```
0000  00 11 7f 98 dc a5 a4 2b  b0 a1 5a c4 08 00 45 00   ·······+ ··Z···E·
0010  00 83 90 50 40 00 56 06  75 0c 9d f0 c0 12 c0 a8   ···P@·V· u·······
0020  00 6d 01 bb c2 72 cd f4  39 df 28 3d 0f 14 50 18   ·m···r·· 9·(=··P·
0030  03 de 04 ef 00 00 17 03  03 00 56 d8 e4 21 d2 bc   ········ ··V··!··
0040  5d 16 ee d3 bb 76 8f 78  de 3e a2 49 51 32 32 b3   ]····v·x ·>·IQ22·
0050  c3 52 76 ed dc 4e 9f 78  31 3f c2 e0 b6 f3 8b 83   ·Rv··N·x 1?······
0060  0e 8b 9c ac 24 a5 a1 45  92 96 77 9c 9d 79 ab 58   ····$··E ··w··y·X
0070  98 c0 c3 5a 45 27 83 35  07 bd af 1d d5 61 28 5e   ···ZE'·5 ·····a(^
0080  d3 fe 0d d1 f3 8b 3f 26  9f 3a b0 69 72 15 a1 21   ······?& ·:·ir··!
0090  c0                                                 ·
```

Wi-Fi: <live capture in progress>

Packets: 713 · Displayed: 713 (100.0%)

Profile: Default

Figure c: A sample packet capture window



```
No.    Time       Source             Destination       Protocol Length Info
    35 3.196432   192.168.0.1        192.168.0.109     UDP       388 42076 → 63224 Len=346
    36 3.203926   192.168.0.1        192.168.0.109     UDP       388 42076 → 63224 Len=346
    37 3.276847   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.111? Tell 192.168.0.113
    38 3.276909   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
    39 3.696329   40.90.22.186       192.168.0.109     TCP        54 443 → 50015 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    40 3.993541   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.111? Tell 192.168.0.113
    41 3.993601   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
    42 4.885235   52.109.124.68      192.168.0.109     TCP        54 443 → 50017 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    43 4.915096   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.111? Tell 192.168.0.113
    44 4.915124   IntelCor_01:e2:1c  Broadcast         ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
    45 5.164362   192.168.0.109      239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
```

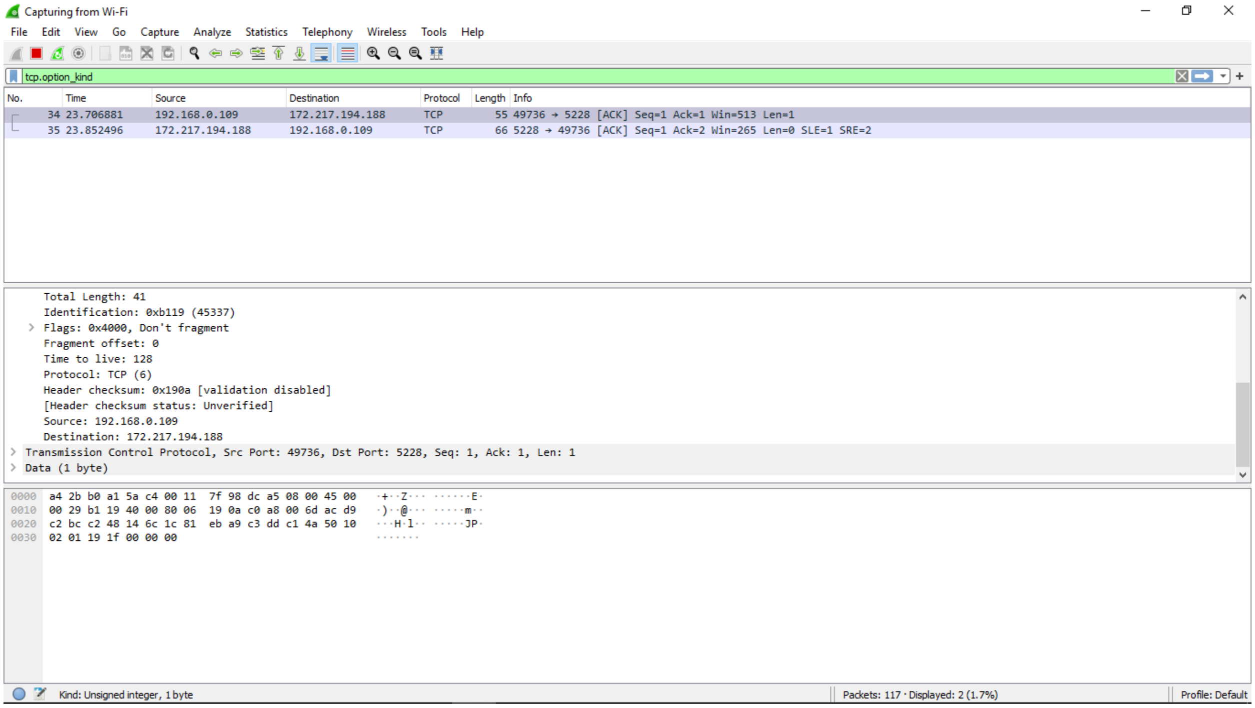
```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE}, id 0
> Ethernet II, Src: IntelCor_01:e2:1c (b0:35:9f:01:e2:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff b0 35  9f 01 e2 1c 08 06 00 01   ·······5 ········
0010  08 00 06 04 00 01 b0 35  9f 01 e2 1c c0 a8 00 71   ·······5 ·······q
0020  00 00 00 00 00 00 c0 a8  00 69                     ········ ·i
```

```
wireshark_Wi-Fi_20200918200400_a04108.pcapng     Packets: 47 · Displayed: 47 (100.0%)     Profile: Default
```

Figure d: Stopping Capture

Filtering:



```
tcp.option_kind
```

```
No.    Time        Source            Destination       Protocol Length Info
    34 23.706881   192.168.0.109     172.217.194.188   TCP        55 49736 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
    35 23.852496   172.217.194.188   192.168.0.109     TCP        66 5228 → 49736 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
```

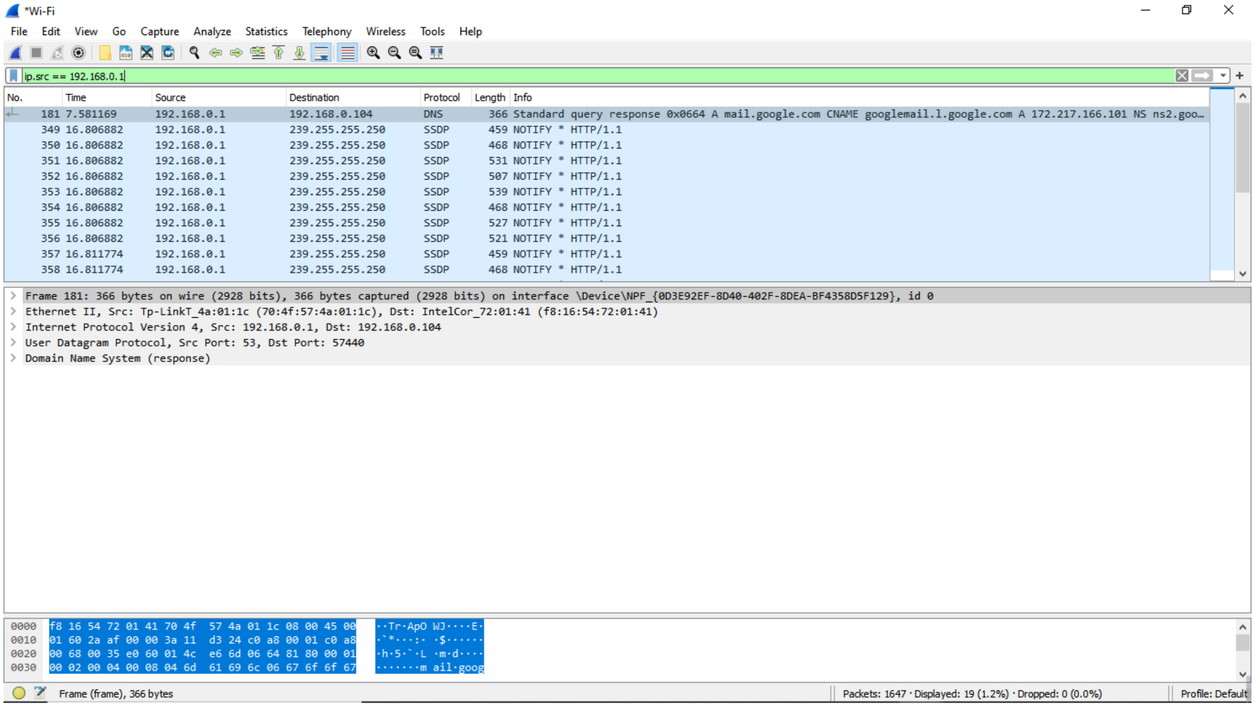
```
    Total Length: 41
    Identification: 0xb119 (45337)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x190a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.109
    Destination: 172.217.194.188
> Transmission Control Protocol, Src Port: 49736, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  a4 2b b0 a1 5a c4 00 11  7f 98 dc a5 08 00 45 00   ·+··Z··· ······E·
0010  00 29 b1 19 40 00 80 06  19 0a c0 a8 00 6d ac d9   ·)··@··· ·····m··
0020  c2 bc c2 48 14 6c 1c 81  eb a9 c3 dd c1 4a 50 10   ···H·l·· ·····JP·
0030  02 01 19 1f 00 00 00                               ·······
```

```
Kind: Unsigned integer, 1 byte     Packets: 117 · Displayed: 2 (1.7%)     Profile: Default
```

Figure e: 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

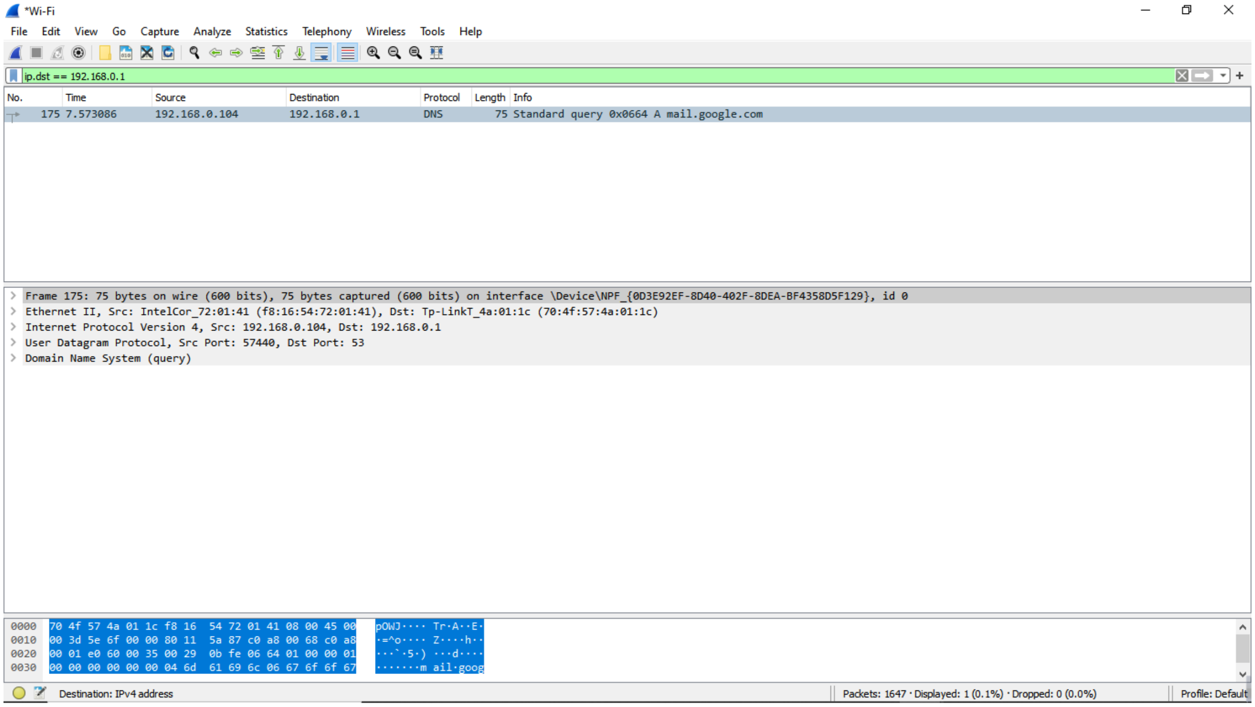
```
No.     Time        Source          Destination       Protocol  Length  Info
    181 7.581169    192.168.0.1     192.168.0.104     DNS          366 Standard query response 0x0664 A mail.google.com CNAME googlemail.l.google.com A 172.217.166.101 NS ns2.goo…
    349 16.806882   192.168.0.1     239.255.255.250   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

Figure f: 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
```

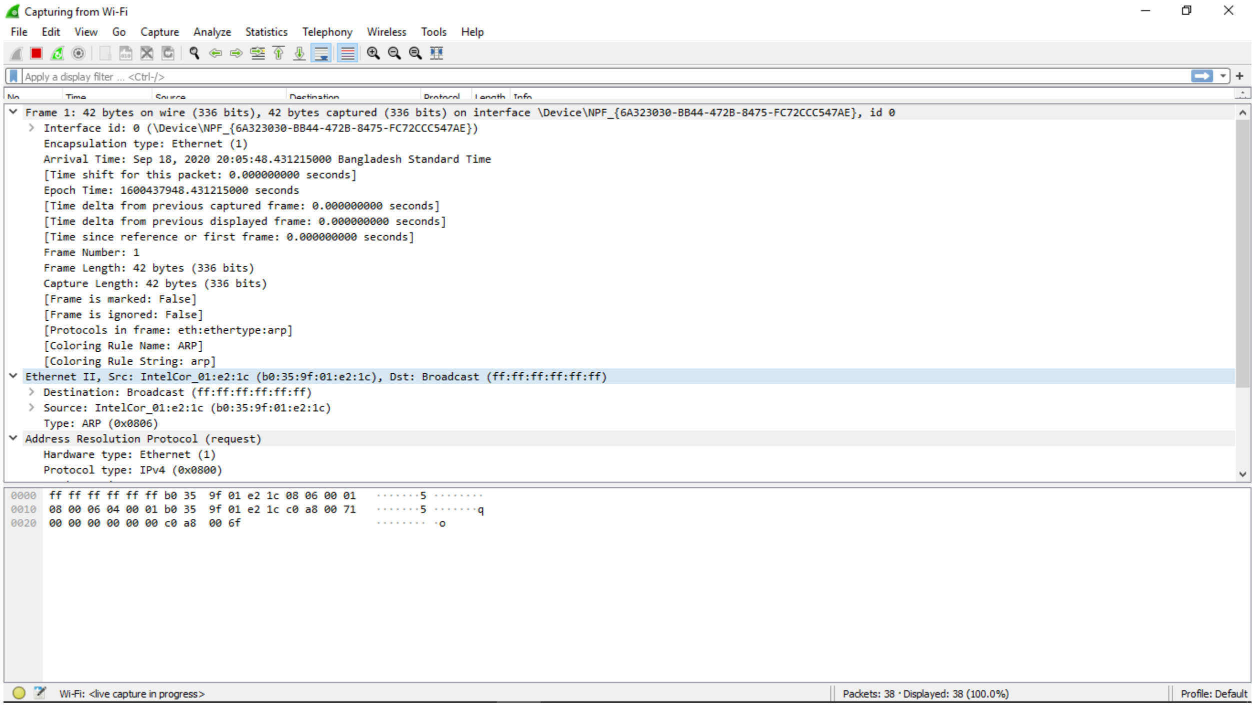
```
> Frame 175: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0D3E92EF-8D40-402F-8DEA-BF4358D5F129}, id 0
> Ethernet II, Src: IntelCor_72:01:41 (f8:16:54:72:01:41), Dst: Tp-LinkT_4a:01:1c (70:4f:57:4a:01:1c)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 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

Figure g: 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**

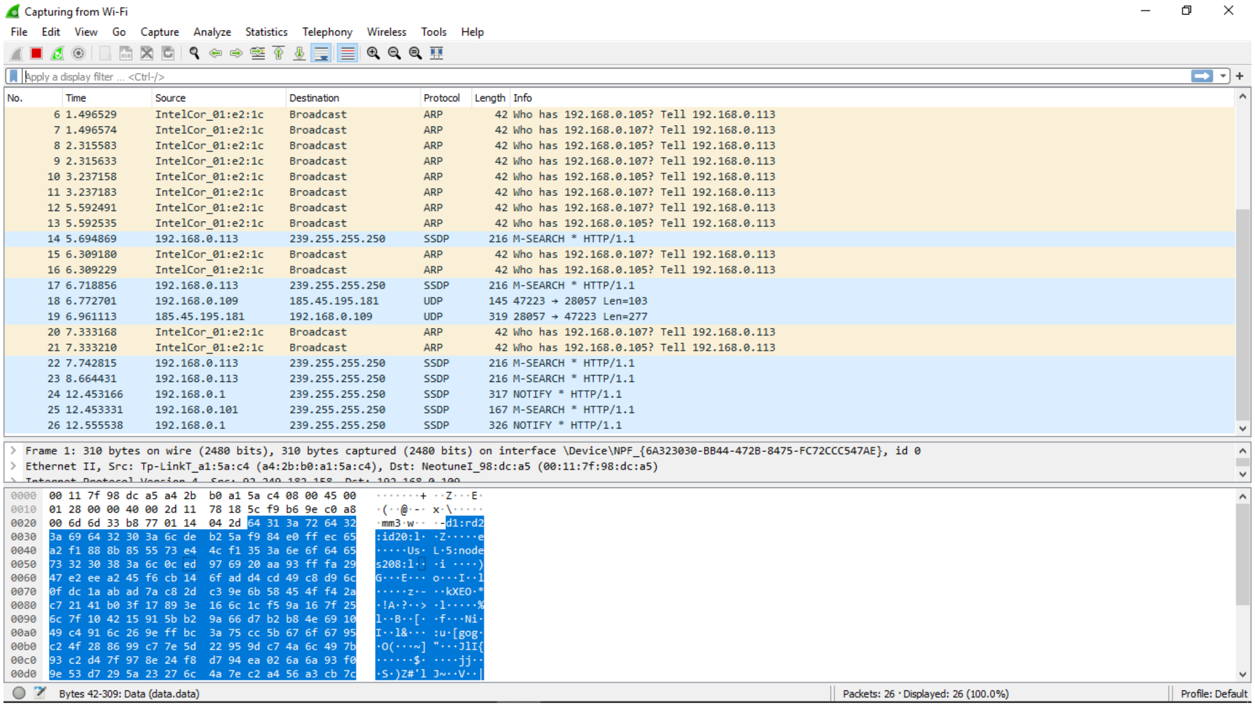

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE}, id 0
  > Interface id: 0 (\Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 20:05:48.431215000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600437948.431215000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: IntelCor_01:e2:1c (b0:35:9f:01:e2:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_01:e2:1c (b0:35:9f:01:e2:1c)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
```

```
0000  ff ff ff ff ff ff b0 35  9f 01 e2 1c 08 06 00 01   ·······5 ········
0010  08 00 06 04 00 01 b0 35  9f 01 e2 1c c0 a8 00 71   ·······5 ·······q
0020  00 00 00 00 00 00 c0 a8  00 6f                     ········ ·o
```

Wi-Fi: <live capture in progress>   Packets: 38 · Displayed: 38 (100.0%)   Profile: Default

Figure h: Packet Details Pane(Frame segment)


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

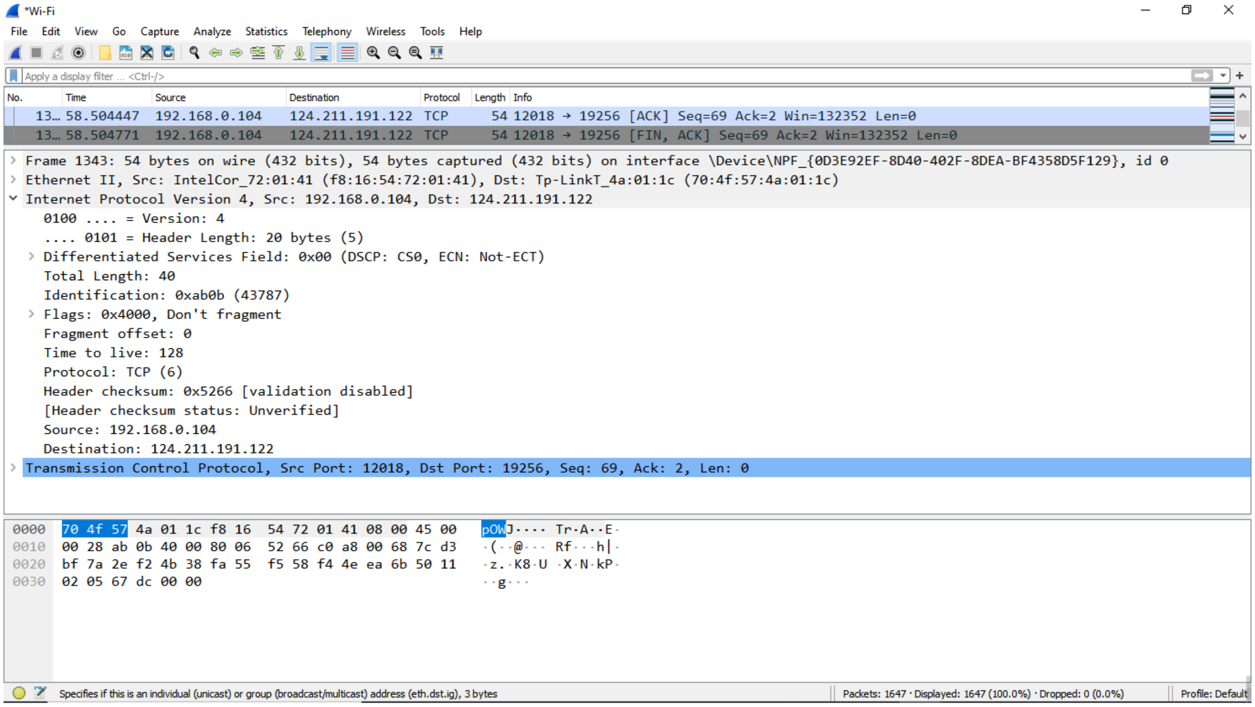
```
No.  Time       Source             Destination      Protocol Length Info
   6 1.496529   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
   7 1.496574   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
   8 2.315583   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
   9 2.315633   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
  10 3.237158   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
  11 3.237183   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
  12 5.592491   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
  13 5.592535   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
  14 5.694869   192.168.0.113      239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  15 6.309180   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
  16 6.309229   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
  17 6.718856   192.168.0.113      239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  18 6.772701   192.168.0.109      185.45.195.181   UDP       145 47223 → 28057 Len=103
  19 6.961113   185.45.195.181     192.168.0.109    UDP       319 28057 → 47223 Len=277
  20 7.333168   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.107? Tell 192.168.0.113
  21 7.333210   IntelCor_01:e2:1c  Broadcast        ARP        42 Who has 192.168.0.105? Tell 192.168.0.113
  22 7.742815   192.168.0.113      239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  23 8.664431   192.168.0.113      239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  24 12.453166  192.168.0.1        239.255.255.250  SSDP      317 NOTIFY * HTTP/1.1
  25 12.453331  192.168.0.101      239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
  26 12.555538  192.168.0.1        239.255.255.250  SSDP      326 NOTIFY * HTTP/1.1
```

```
> Frame 1: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface \Device\NPF_{6A323030-BB44-472B-8475-FC72CCC547AE}, id 0
> Ethernet II, Src: Tp-LinkT_a1:5a:c4 (a4:2b:b0:a1:5a:c4), Dst: NeotuneI_98:dc:a5 (00:11:7f:98:dc:a5)
> Internet Protocol Version 4, Src: 92.240.182.158, Dst: 192.168.0.109
```

```
0000  00 11 7f 98 dc a5 a4 2b  b0 a1 5a c4 08 00 45 00   ·······+ ··Z···E·
0010  01 28 00 00 40 00 2d 11  78 18 5c f9 b6 9e c0 a8   ·(··@·-· x·\·····
0020  00 6d 6d 33 b8 77 01 14  04 2d 64 31 3a 72 64 32   ·mm3·w·· ·-d1:rd2
0030  3a 69 64 32 30 3a 6c de  b2 5a f9 84 e0 ff ec 65   :id20:l· ·Z·····e
0040  a2 f1 88 8b 85 55 73 e4  4c f1 35 3a 6e 6f 64 65   ·····Us· L·5:node
0050  73 32 30 38 3a 6c 0c ed  97 69 20 aa 93 ff fa 29   s208:l·· ·i ····)
0060  47 e2 ee a2 45 f6 cb 14  6f ad d4 cd 49 c8 d9 6c   G···E··· o···I··l
0070  0f dc 1a ab ad 7a c8 2d  c3 9e 6b 58 45 4f f4 2a   ·····z·- ··kXEO·*
0080  c7 21 41 b0 3f 17 89 3e  16 6c 1c f5 9a 16 7f 25   ·!A·?··> ·l·····%
0090  6c 7f 10 42 15 91 5b b2  9a 66 d7 b2 b8 4e 69 10   l··B··[· ·f···Ni·
00a0  49 c4 91 6c 26 9e ff bc  3a 75 cc 5b 67 6f 67 95   I··l&··· :u·[gog·
00b0  c2 4f 28 86 99 c7 7e 5d  22 95 9d c7 4a 6c 49 7b   ·O(···~] "···JlI{
00c0  93 c2 d4 7f 97 8e 24 f8  d7 94 ea 02 6a 6a 93 f0   ······$· ····jj··
00d0  9e 53 d7 29 5a 23 27 6c  4a 7e c2 a4 56 a3 cb 7c   ·S·)Z#'l J~··V··|
```

Bytes 42-309: Data (data.data)   Packets: 26 · Displayed: 26 (100.0%)   Profile: Default

Figure i: Packet Details Pane (Ethernet Segment)


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

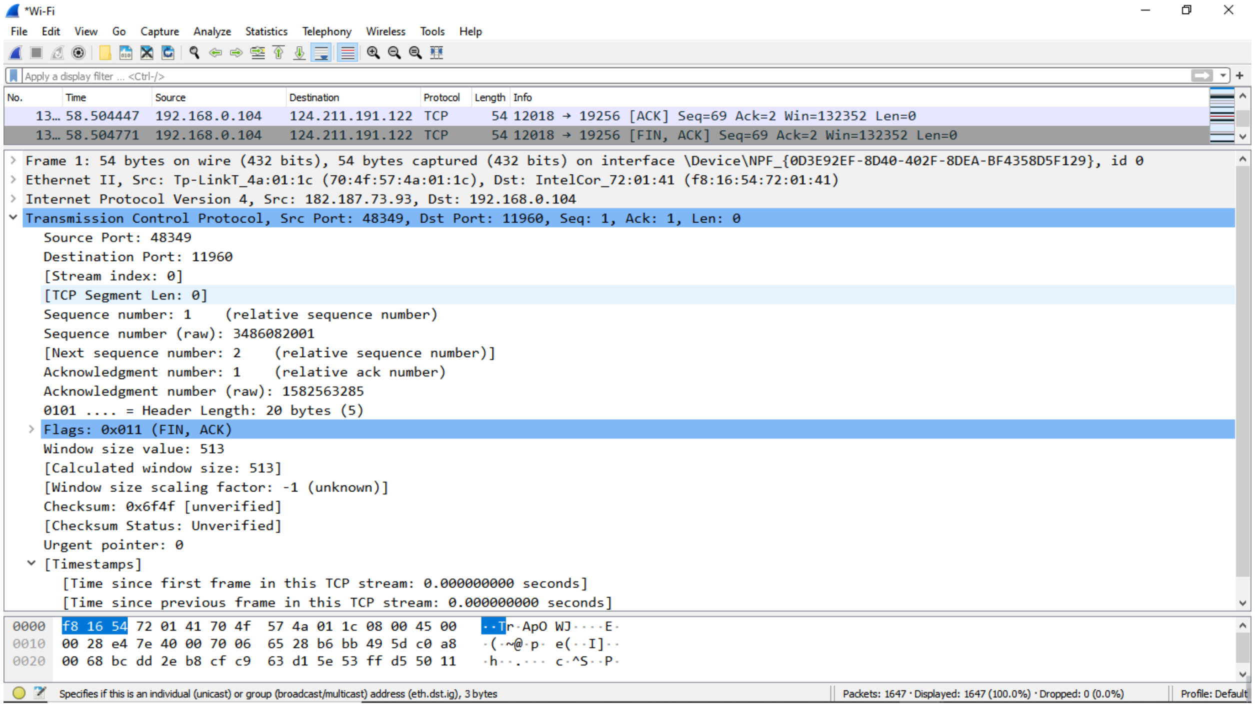
```
No.     Time        Source         Destination      Protocol  Length  Info
13…  58.504447  192.168.0.104  124.211.191.122  TCP     54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
13…  58.504771  192.168.0.104  124.211.191.122  TCP     54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0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

```
> 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

Figure j: Packet Details Pane(IP segment)


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

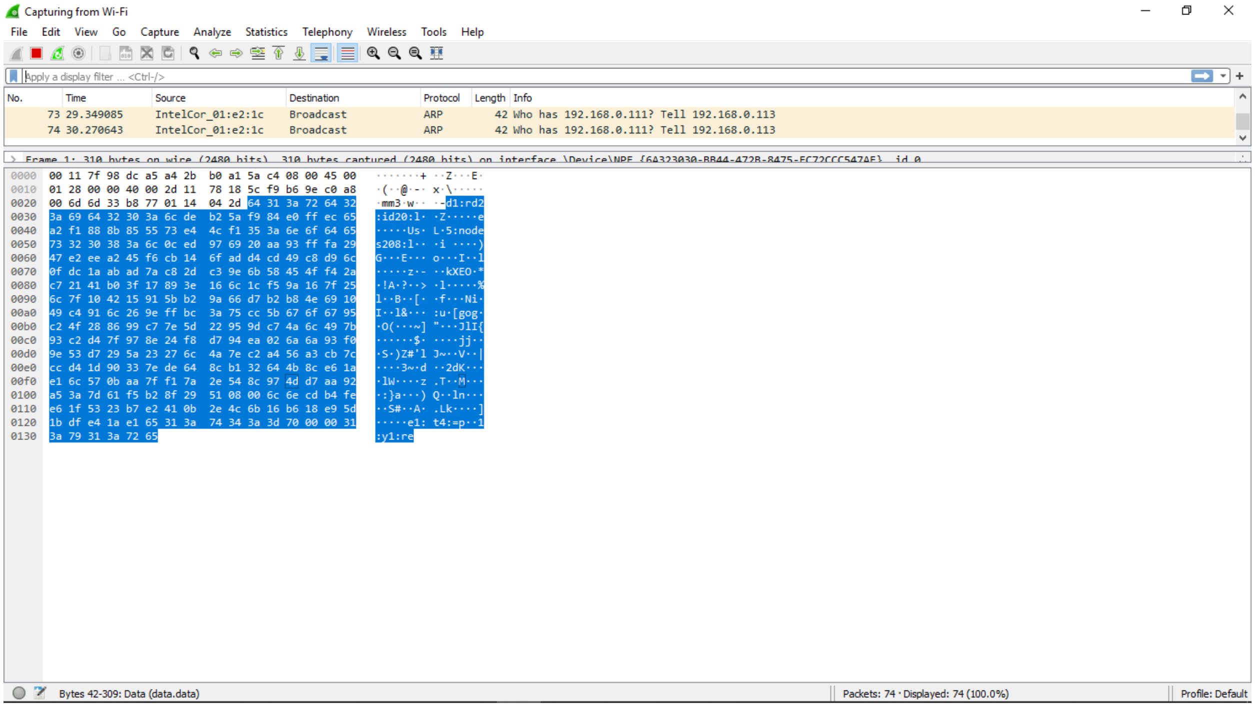
```
No.     Time        Source         Destination      Protocol  Length  Info
13…  58.504447  192.168.0.104  124.211.191.122  TCP     54 12018 → 19256 [ACK] Seq=69 Ack=2 Win=132352 Len=0
13…  58.504771  192.168.0.104  124.211.191.122  TCP     54 12018 → 19256 [FIN, ACK] Seq=69 Ack=2 Win=132352 Len=0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

```
> 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

Figure k: Packet Details Pane (TCP Segment)

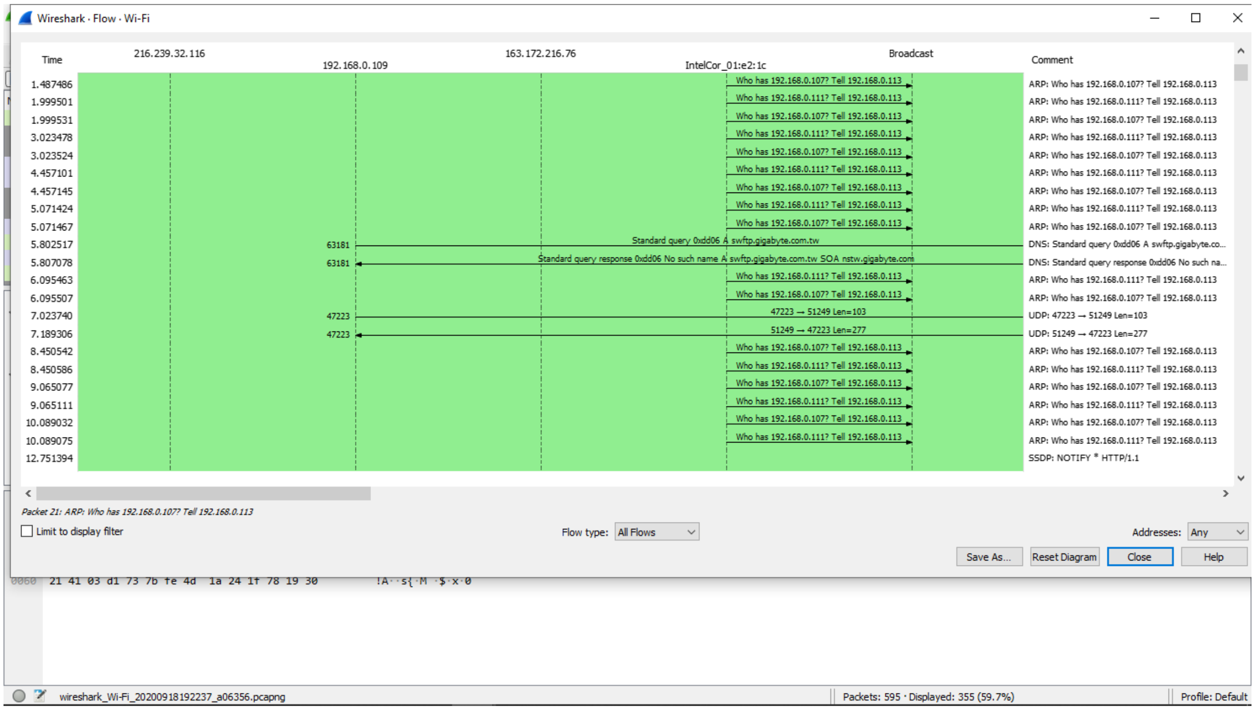

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
73	29.349085	IntelCor_01:e2:1c	Broadcast	ARP	42	Who has 192.168.0.111? Tell 192.168.0.113
74	30.270643	IntelCor_01:e2:1c	Broadcast	ARP	42	Who has 192.168.0.111? Tell 192.168.0.113

```
> Frame 1: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface \Device\NPF_{6A323030-BB44-472B-8475-EC72CCC547AE}, id 0
0000  00 11 7f 98 dc a5 a4 2b  b0 a1 5a c4 08 00 45 00   ·······+ ··Z···E·
0010  01 28 00 00 40 00 2d 11  78 18 5c f9 b6 9e c0 a8   ·(··@·-· x·\·····
0020  00 6d 6d 33 b8 77 01 14  04 2d 64 31 3a 72 64 32   ·mm3·w·· ·-d1:rd2
0030  3a 69 64 32 30 3a 6c de  b2 5a f9 84 e0 ff ec 65   :id20:l· ·Z·····e
0040  a2 f1 88 8b 85 55 73 e4  4c f1 35 3a 6e 6f 64 65   ·····Us· L·5:node
0050  73 32 30 38 3a 6c 0c ed  97 69 20 aa 93 ff fa 29   s208:l·· ·i ····)
0060  47 e2 ee a2 45 f6 cb 14  6f ad d4 cd 49 c8 d9 6c   G···E··· o···I··l
0070  0f dc 1a ab ad 7a c8 2d  c3 9e 6b 58 45 4f f4 2a   ·····z·- ··kXEO·*
0080  c7 21 41 b0 3f 17 89 3e  16 6c 1c f5 9a 16 7f 25   ·!A·?··> ·l·····%
0090  6c 7f 10 42 15 91 5b b2  9a 66 d7 b2 b8 4e 69 10   l··B··[· ·f···Ni·
00a0  49 c4 91 6c 26 9e ff bc  3a 75 cc 5b 67 6f 67 95   I··l&··· :u·[gog·
00b0  c2 4f 28 86 99 c7 7e 5d  22 95 9d c7 4a 6c 49 7b   ·O(···~] "···JlI{
00c0  93 c2 d4 7f 97 8e 24 f8  d7 94 ea 02 6a 6a 93 f0   ······$· ····jj··
00d0  9e 53 d7 29 5a 23 27 6c  4a 7e c2 a4 56 a3 cb 7c   ·S·)Z#'l J~··V··|
00e0  cc d4 1d 90 33 7e de 64  8c b1 32 64 4b 8c e6 1a   ····3~·d ··2dK···
00f0  e1 6c 57 0b aa 7f f1 7a  2e 54 8c 97 4d d7 aa 92   ·lW····z .T··M···
0100  a5 3a 7d 61 f5 b2 8f 29  51 08 00 6c 6e cd b4 fe   ·:}a···) Q··ln···
0110  e6 1f 53 23 b7 e2 41 0b  2e 4c 6b 16 b6 18 e9 5d   ··S#··A· .Lk····]
0120  1b df e4 1a e1 65 31 3a  74 34 3a 3d 70 00 00 31   ·····e1: t4:=p··1
0130  3a 79 31 3a 72 65                                  :y1:re
```

Bytes 42-309: Data (data.data)
Packets: 74 · Displayed: 74 (100.0%)
Profile: Default

Figure L: Packet Byte Pane



```
Time        Comment
1.487486    ARP: Who has 192.168.0.107? Tell 192.168.0.113
1.999501    ARP: Who has 192.168.0.111? Tell 192.168.0.113
1.999531    ARP: Who has 192.168.0.107? Tell 192.168.0.113
3.023478    ARP: Who has 192.168.0.111? Tell 192.168.0.113
3.023524    ARP: Who has 192.168.0.107? Tell 192.168.0.113
4.457101    ARP: Who has 192.168.0.111? Tell 192.168.0.113
4.457145    ARP: Who has 192.168.0.107? Tell 192.168.0.113
5.071424    ARP: Who has 192.168.0.111? Tell 192.168.0.113
5.071467    ARP: Who has 192.168.0.107? Tell 192.168.0.113
5.802517    DNS: Standard query 0xdd06 A swftp.gigabyte.co...
5.807078    DNS: Standard query response 0xdd06 No such na...
6.095463    ARP: Who has 192.168.0.111? Tell 192.168.0.113
6.095507    ARP: Who has 192.168.0.107? Tell 192.168.0.113
7.023740    UDP: 47223 → 51249 Len=103
7.189306    UDP: 51249 → 47223 Len=277
8.450542    ARP: Who has 192.168.0.107? Tell 192.168.0.113
8.450586    ARP: Who has 192.168.0.111? Tell 192.168.0.113
9.065077    ARP: Who has 192.168.0.107? Tell 192.168.0.113
9.065111    ARP: Who has 192.168.0.111? Tell 192.168.0.113
10.089032   ARP: Who has 192.168.0.107? Tell 192.168.0.113
10.089075   ARP: Who has 192.168.0.111? Tell 192.168.0.113
12.751394   SSDP: NOTIFY * HTTP/1.1
```

Standard query 0xdd06 A swftp.gigabyte.com.tw
Standard query response 0xdd06 No such name A swftp.gigabyte.com.tw SOA nstw.gigabyte.com
47223 → 51249 Len=103
51249 → 47223 Len=277

Packet 21: ARP: Who has 192.168.0.107? Tell 192.168.0.113

☐ Limit to display filter

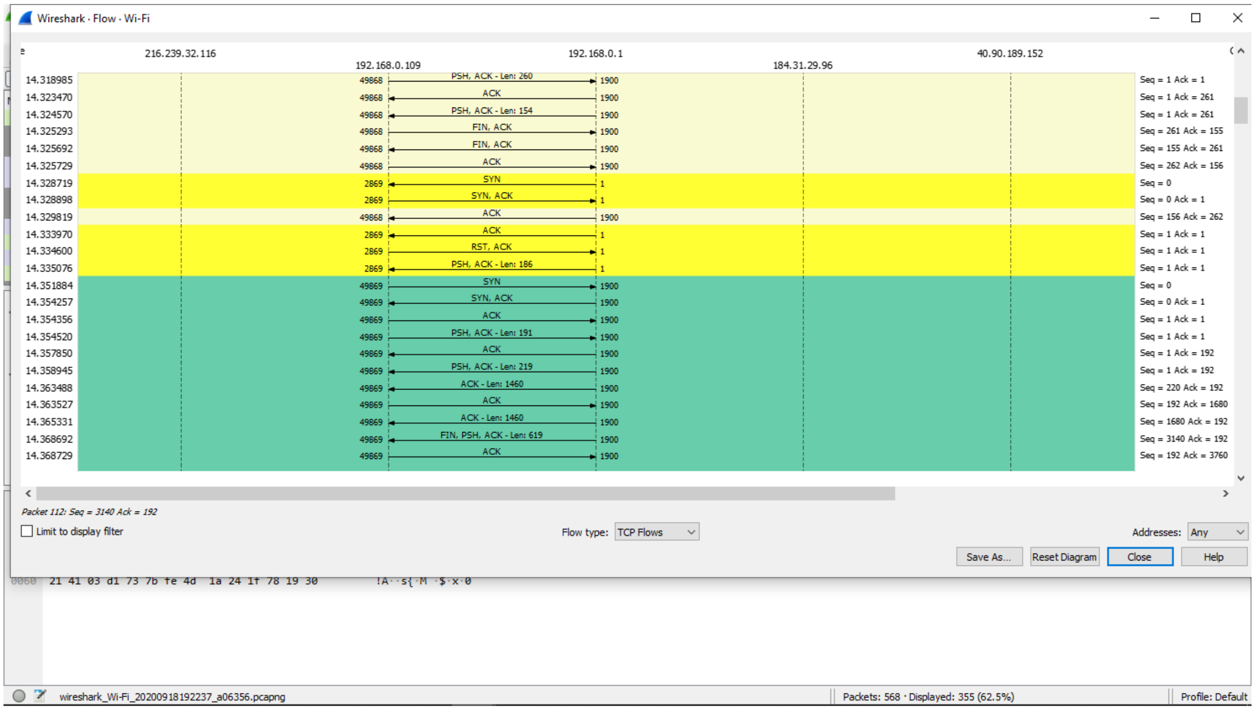
Flow type: All Flows

Addresses: Any

```
0060  21 41 03 d1 73 7b fe 4d  1a 24 1f 78 19 30   !A··s{·M ·$·x·0
```

wireshark_Wi-Fi_20200918192237_a06356.pcapng
Packets: 595 · Displayed: 355 (59.7%)
Profile: Default

Figure m: Statistics- Flow Graph(All Flows)



```
            216.239.32.116                          192.168.0.1                          40.90.189.152
                              192.168.0.109                          184.31.29.96
14.318985   49868 ──PSH, ACK - Len: 260──→ 1900      Seq = 1 Ack = 1
14.323470   49868 ←─────────ACK─────────── 1900      Seq = 1 Ack = 261
14.324570   49868 ←─PSH, ACK - Len: 154─── 1900      Seq = 1 Ack = 261
14.325293   49868 ───────FIN, ACK────────→ 1900      Seq = 261 Ack = 155
14.325692   49868 ←──────FIN, ACK───────── 1900      Seq = 155 Ack = 261
14.325729   49868 ──────────ACK──────────→ 1900      Seq = 262 Ack = 156
14.328719    2869 ←─────────SYN─────────── 1         Seq = 0
14.328898    2869 ───────SYN, ACK────────→ 1         Seq = 0 Ack = 1
14.329819   49868 ←─────────ACK─────────── 1900      Seq = 156 Ack = 262
14.333970    2869 ←─────────ACK─────────── 1         Seq = 1 Ack = 1
14.334600    2869 ───────RST, ACK────────→ 1         Seq = 1 Ack = 1
14.335076    2869 ←─PSH, ACK - Len: 186─── 1         Seq = 1 Ack = 1
14.351884   49869 ──────────SYN──────────→ 1900      Seq = 0
14.354257   49869 ←───────SYN, ACK──────── 1900      Seq = 0 Ack = 1
14.354356   49869 ──────────ACK──────────→ 1900      Seq = 1 Ack = 1
14.354520   49869 ──PSH, ACK - Len: 191──→ 1900      Seq = 1 Ack = 1
14.357850   49869 ←─────────ACK─────────── 1900      Seq = 1 Ack = 192
14.358945   49869 ←─PSH, ACK - Len: 219─── 1900      Seq = 1 Ack = 192
14.363488   49869 ←───ACK - Len: 1460───── 1900      Seq = 220 Ack = 192
14.363527   49869 ──────────ACK──────────→ 1900      Seq = 192 Ack = 1680
14.365331   49869 ←───ACK - Len: 1460───── 1900      Seq = 1680 Ack = 192
14.368692   49869 ←FIN, PSH, ACK - Len: 619 1900     Seq = 3140 Ack = 192
14.368729   49869 ──────────ACK──────────→ 1900      Seq = 192 Ack = 3760
```

Packet 112: Seq = 3140 Ack = 192

☐ Limit to display filter   Flow type: TCP Flows   Addresses: Any

```
0060  21 41 03 d1 73 7b fe 4d  1a 24 1f 78 19 30        !A··s{·M ·$·x·0
```

wireshark_Wi-Fi_20200918192237_a06356.pcapng   Packets: 568 · Displayed: 355 (62.5%)   Profile: Default

Figure n: Statistics- Flow Graph(TCP Flows)

Conclusion:

All we need to do just download the Wireshark exe fie form the source and install it to the computer. We captured the network and run it. The Transfer Control Protocol through the graph have shown us the desired output.