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 Mahbub Islam

ID: IT-16002

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.

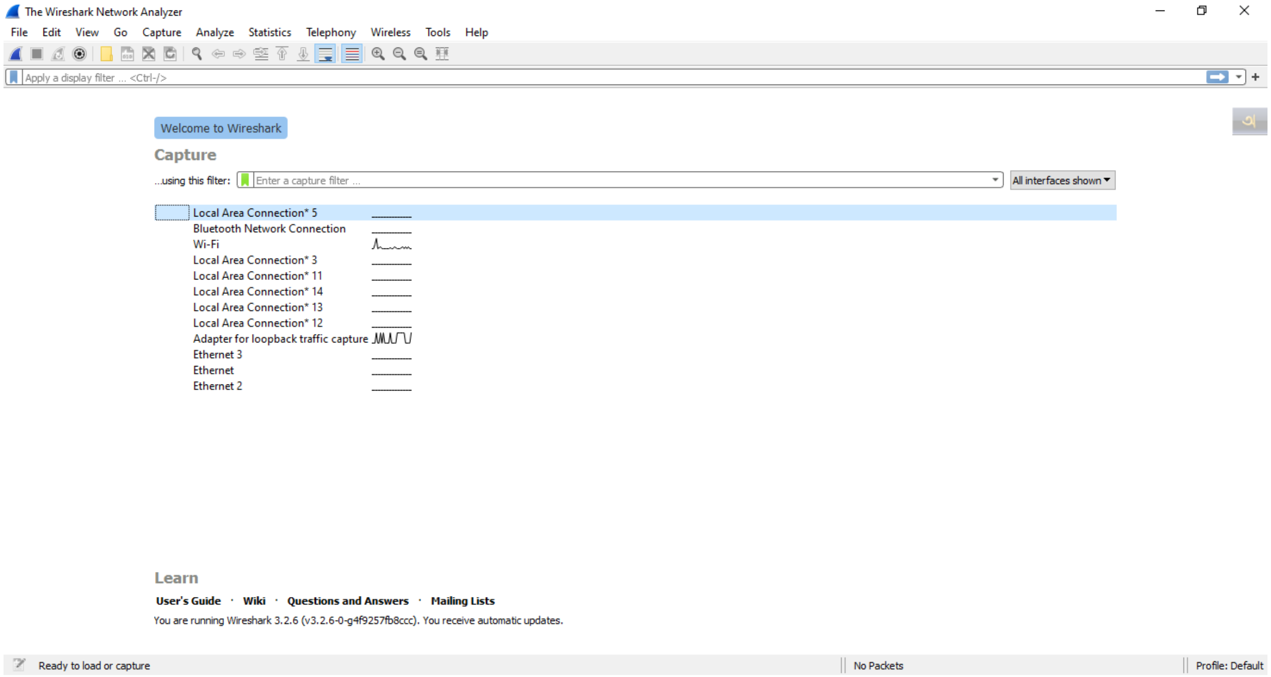
Objectives:

We will learn-

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

Procedures:

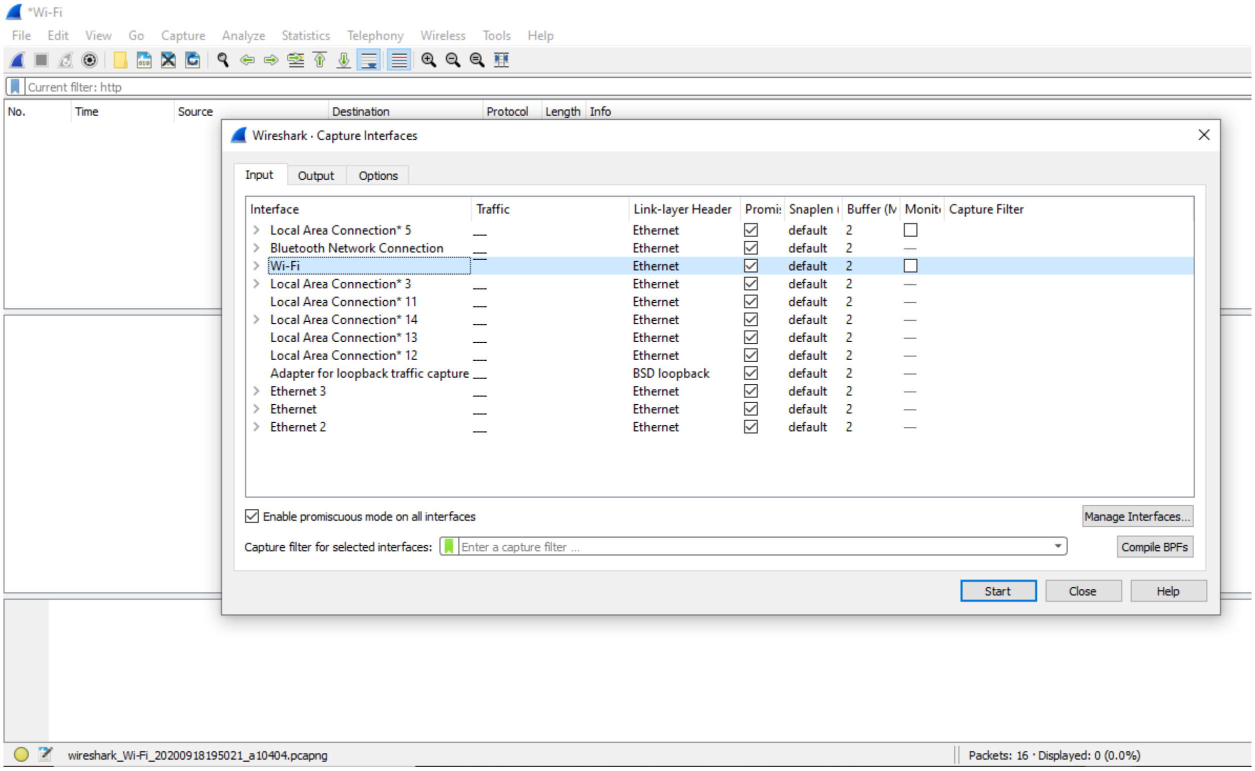
Step1: Open The Wireshark.


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
Local Area Connection* 5
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 3
Local Area Connection* 11
Local Area Connection* 14
Local Area Connection* 13
Local Area Connection* 12
Adapter for loopback traffic capture
Ethernet 3
Ethernet
Ethernet 2
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

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

Fig: Wireshark GUI (Main Window)

Step 2: Start capturing.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Wireshark · Capture Interfaces
Input Output Options

Current filter: http

Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (M	Monit	Capture Filter
Local Area Connection* 5	__	Ethernet	☑	default	2	□	
Bluetooth Network Connection	__	Ethernet	☑	default	2	—	
Wi-Fi	__	Ethernet	☑	default	2	□	
Local Area Connection* 3	__	Ethernet	☑	default	2	—	
Local Area Connection* 11	__	Ethernet	☑	default	2	—	
Local Area Connection* 14	__	Ethernet	☑	default	2	—	
Local Area Connection* 13	__	Ethernet	☑	default	2	—	
Local Area Connection* 12	__	Ethernet	☑	default	2	—	
Adapter for loopback traffic capture	__	BSD loopback	☑	default	2	—	
Ethernet 3	__	Ethernet	☑	default	2	—	
Ethernet	__	Ethernet	☑	default	2	—	
Ethernet 2	__	Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

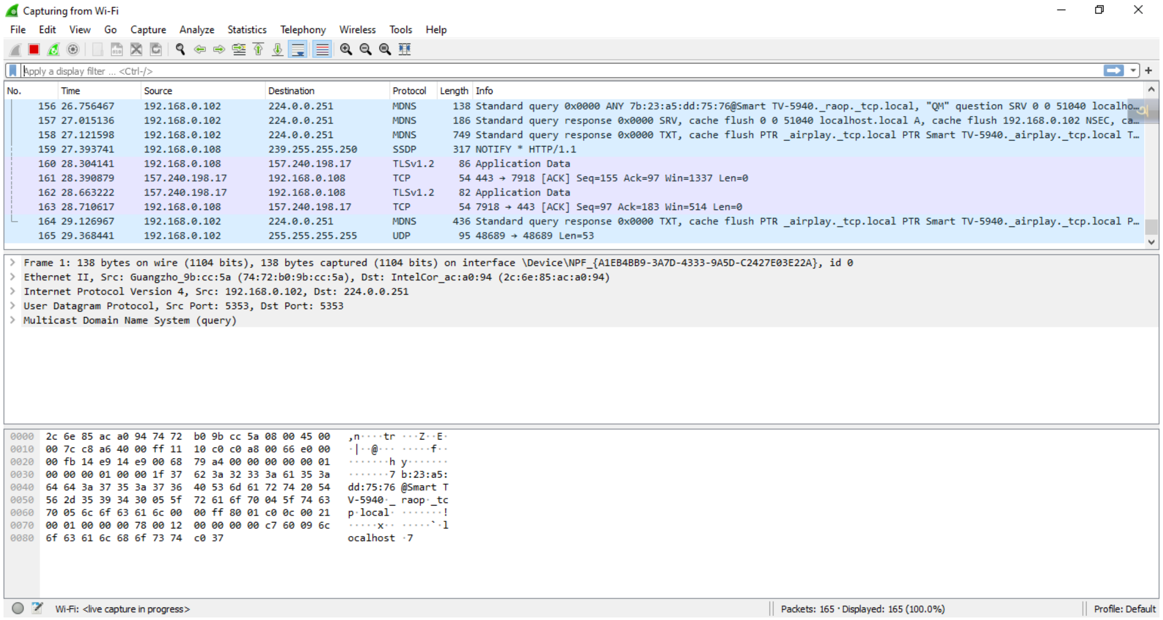
Capture filter for selected interfaces: Enter a capture filter ...

wireshark_Wi-Fi_20200918195021_a10404.pcapng

Packets: 16 · Displayed: 0 (0.0%)

Fig : Starting capture

Step 3: Packets are exchanging on Network Interface.



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
 156 26.756467   192.168.0.102   224.0.0.251      MDNS       138 Standard query 0x0000 ANY 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local, "QM" question SRV 0 0 51040 localho…
 157 27.015136   192.168.0.102   224.0.0.251      MDNS       186 Standard query response 0x0000 SRV, cache flush 0 0 51040 localhost.local A, cache flush 192.168.0.102 NSEC, ca…
 158 27.121598   192.168.0.102   224.0.0.251      MDNS       749 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Smart TV-5940._airplay._tcp.local T…
 159 27.393741   192.168.0.108   239.255.255.250  SSDP       317 NOTIFY * HTTP/1.1
 160 28.304141   192.168.0.108   157.240.198.17   TLSv1.2     86 Application Data
 161 28.390879   157.240.198.17  192.168.0.108    TCP         54 443 → 7918 [ACK] Seq=155 Ack=97 Win=1337 Len=0
 162 28.663222   157.240.198.17  192.168.0.108    TLSv1.2     82 Application Data
 163 28.710617   192.168.0.108   157.240.198.17   TCP         54 7918 → 443 [ACK] Seq=97 Ack=183 Win=514 Len=0
 164 29.126967   192.168.0.102   224.0.0.251      MDNS       436 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Smart TV-5940._airplay._tcp.local P…
 165 29.368441   192.168.0.102   255.255.255.255  UDP         95 48689 → 48689 Len=53
```

```
> Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
> Ethernet II, Src: Guangzho_9b:cc:5a (74:72:b0:9b:cc:5a), Dst: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

```
0000  2c 6e 85 ac a0 94 74 72  b0 9b cc 5a 08 00 45 00   ,n····tr ···Z··E·
0010  00 7c c8 a6 40 00 ff 11  10 c0 c0 a8 00 66 e0 00   ·|··@··· ·····f··
0020  00 fb 14 e9 14 e9 00 68  79 a4 00 00 00 00 00 01   ·······h y·······
0030  00 00 00 01 00 00 1f 37  62 3a 32 33 3a 61 35 3a   ·······7 b:23:a5:
0040  64 64 3a 37 35 3a 37 36  40 53 6d 61 72 74 20 54   dd:75:76 @Smart T
0050  56 2d 35 39 34 30 05 5f  72 61 6f 70 04 5f 74 63   V-5940·_ raop·_tc
0060  70 05 6c 6f 63 61 6c 00  00 ff 80 01 c0 0c 00 21   p·local· ·······!
0070  00 01 00 00 00 78 00 12  00 00 00 00 c7 60 09 6c   ·····x·· ·····`·l
0080  6f 63 61 6c 68 6f 73 74  c0 37                     ocalhost ·7
```

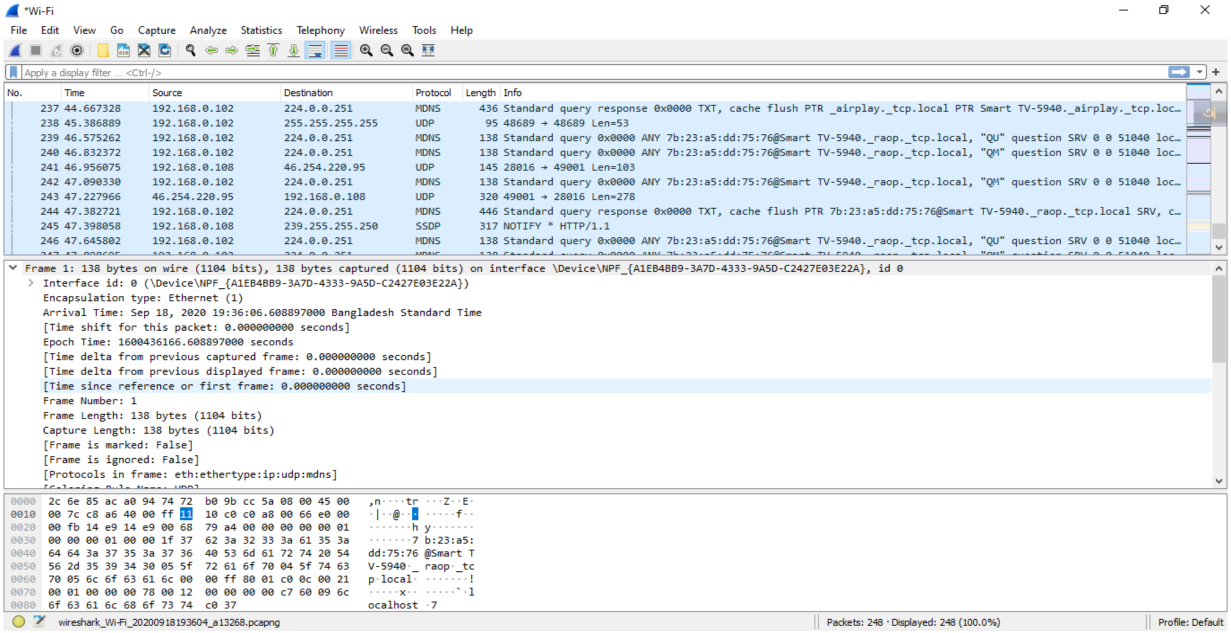
Wi-Fi: <live capture in progress>

Packets: 165 · Displayed: 165 (100.0%)

Profile: Default

Fig: Packets are exchanging

Step 4: Stop Capture.


*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
  237 44.667328  192.168.0.102   224.0.0.251      MDNS     436 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Smart TV-5940._airplay._tcp.loc…
  238 45.386889  192.168.0.102   255.255.255.255  UDP       95 48689 → 48689 Len=53
  239 46.575262  192.168.0.102   224.0.0.251      MDNS     138 Standard query 0x0000 ANY 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local, "QU" question SRV 0 0 51040 loc…
  240 46.832372  192.168.0.102   224.0.0.251      MDNS     138 Standard query 0x0000 ANY 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local, "QM" question SRV 0 0 51040 loc…
  241 46.956075  192.168.0.108   46.254.220.95    UDP      145 28016 → 49001 Len=103
  242 47.090330  192.168.0.102   224.0.0.251      MDNS     138 Standard query 0x0000 ANY 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local, "QM" question SRV 0 0 51040 loc…
  243 47.227966  46.254.220.95   192.168.0.108    UDP      320 49001 → 28016 Len=278
  244 47.382721  192.168.0.102   224.0.0.251      MDNS     446 Standard query response 0x0000 TXT, cache flush PTR 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local SRV, c…
  245 47.398058  192.168.0.108   239.255.255.250  SSDP     317 NOTIFY * HTTP/1.1
  246 47.645802  192.168.0.102   224.0.0.251      MDNS     138 Standard query 0x0000 ANY 7b:23:a5:dd:75:76@Smart TV-5940._raop._tcp.local, "QU" question SRV 0 0 51040 loc…
```

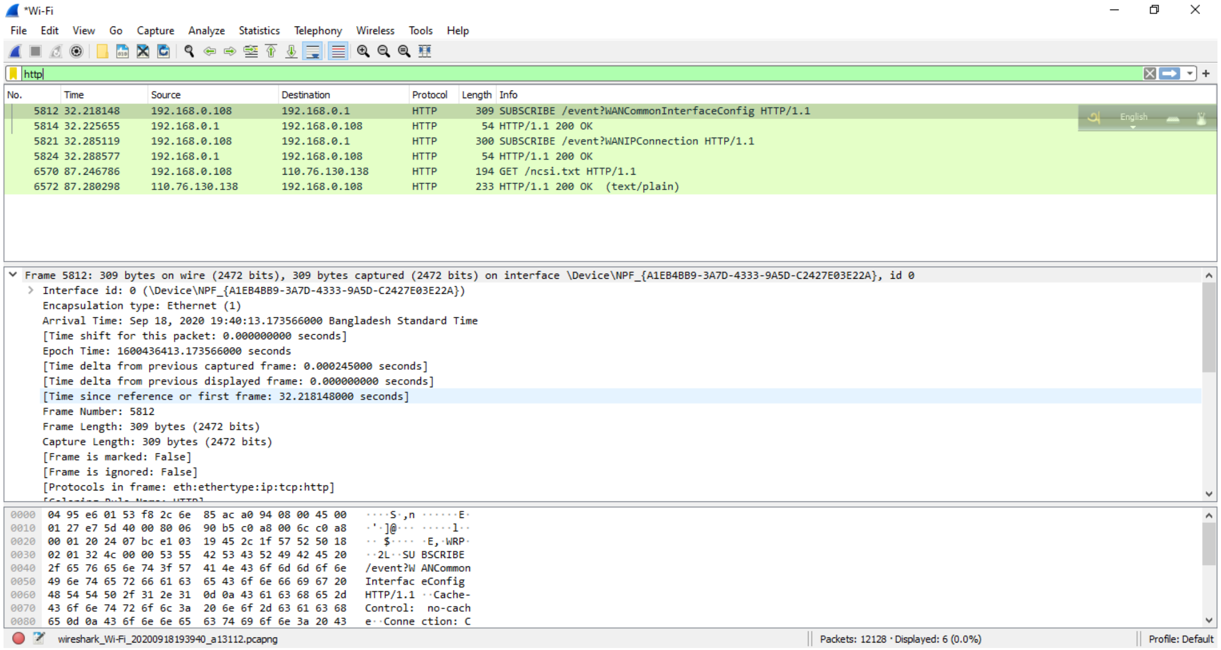
```
Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
  > Interface id: 0 (\Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 19:36:06.608897000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600436166.608897000 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: 138 bytes (1104 bits)
    Capture Length: 138 bytes (1104 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:mdns]
```

```
0000  2c 6e 85 ac a0 94 74 72  b0 9b cc 5a 08 00 45 00   ,n····tr ···Z··E·
0010  00 7c c8 a6 40 00 ff 11  10 c0 c0 a8 00 66 e0 00   ·|··@··· ·····f··
0020  00 fb 14 e9 14 e9 00 68  79 a4 00 00 00 00 00 01   ·······h y·······
0030  00 00 00 01 00 00 1f 37  62 3a 32 33 3a 61 35 3a   ·······7 b:23:a5:
0040  64 64 3a 37 35 3a 37 36  40 53 6d 61 72 74 20 54   dd:75:76 @Smart T
0050  56 2d 35 39 34 30 05 5f  72 61 6f 70 04 5f 74 63   V-5940·_ raop·_tc
0060  70 05 6c 6f 63 61 6c 00  00 ff 80 01 c0 0c 00 21   p·local· ·······!
0070  00 01 00 00 00 78 00 12  00 00 00 00 c7 60 09 6c   ·····x·· ·····`·l
0080  6f 63 61 6c 68 6f 73 74  c0 37                     ocalhost ·7
```

```
wireshark_Wi-Fi_20200918193604_a13268.pcapng    Packets: 248 · Displayed: 248 (100.0%)    Profile: Default
```

Fig: Stop capture.

Step 5: Filter by entering the protocol http.


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

```
http
```

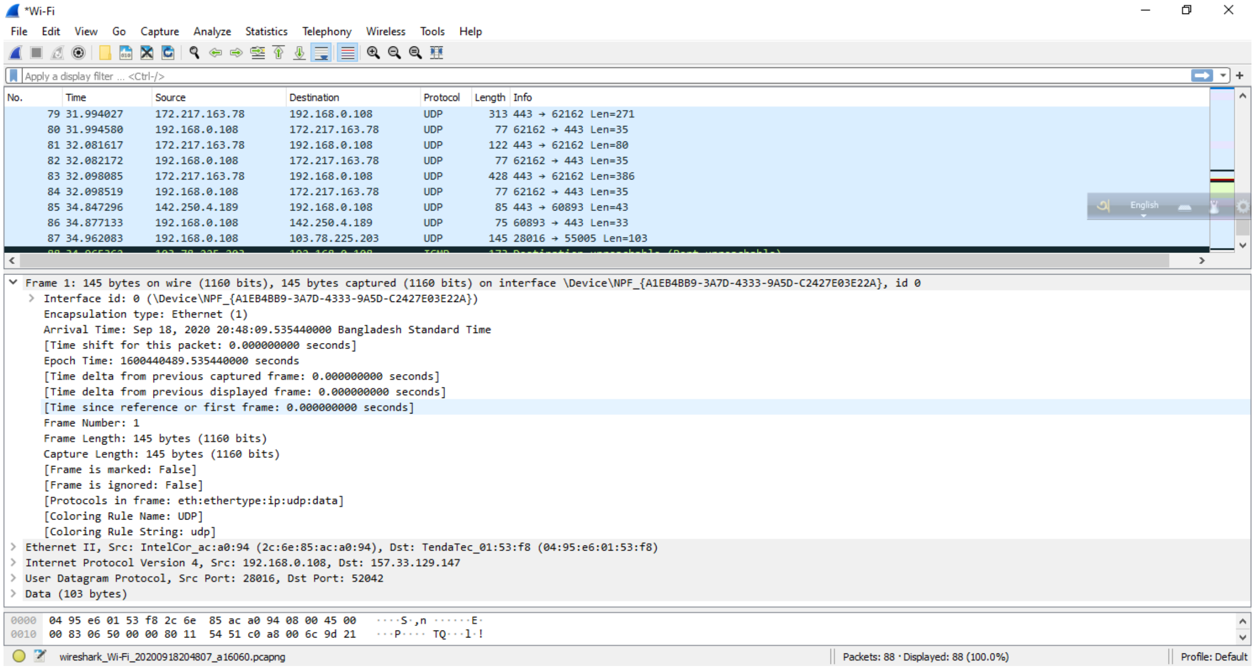
```
No.   Time       Source          Destination      Protocol Length Info
 5812 32.218148  192.168.0.108   192.168.0.1      HTTP     309 SUBSCRIBE /event?WANCommonInterfaceConfig HTTP/1.1
 5814 32.225655  192.168.0.1     192.168.0.108    HTTP      54 HTTP/1.1 200 OK
 5821 32.285119  192.168.0.108   192.168.0.1      HTTP     300 SUBSCRIBE /event?WANIPConnection HTTP/1.1
 5824 32.288577  192.168.0.1     192.168.0.108    HTTP      54 HTTP/1.1 200 OK
 6570 87.246786  192.168.0.108   110.76.130.138   HTTP     194 GET /ncsi.txt HTTP/1.1
 6572 87.280298  110.76.130.138  192.168.0.108    HTTP     233 HTTP/1.1 200 OK  (text/plain)
```

```
Frame 5812: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
  > Interface id: 0 (\Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 19:40:13.173566000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600436413.173566000 seconds
    [Time delta from previous captured frame: 0.000245000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 32.218148000 seconds]
    Frame Number: 5812
    Frame Length: 309 bytes (2472 bits)
    Capture Length: 309 bytes (2472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
```

```
0000  04 95 e6 01 53 f8 2c 6e  85 ac a0 94 08 00 45 00   ····S·,n ······E·
0010  01 27 e7 5d 40 00 80 06  90 b5 c0 a8 00 6c c0 a8   ·'·]@··· ·····l··
0020  00 01 20 24 07 bc e1 03  19 45 2c 1f 57 52 50 18   ·· $···· ·E,·WRP·
0030  02 01 32 4c 00 00 53 55  42 53 43 52 49 42 45 20   ··2L··SU BSCRIBE 
0040  2f 65 76 65 6e 74 3f 57  41 4e 43 6f 6d 6d 6f 6e   /event?W ANCommon
0050  49 6e 74 65 72 66 61 63  65 43 6f 6e 66 69 67 20   Interfac eConfig 
0060  48 54 54 50 2f 31 2e 31  0d 0a 43 61 63 68 65 2d   HTTP/1.1 ··Cache-
0070  43 6f 6e 74 72 6f 6c 3a  20 6e 6f 2d 63 61 63 68   Control:  no-cach
0080  65 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 43   e··Conne ction: C
```

```
wireshark_Wi-Fi_20200918193940_a13112.pcapng    Packets: 12128 · Displayed: 6 (0.0%)    Profile: Default
```

Fig: http filtering

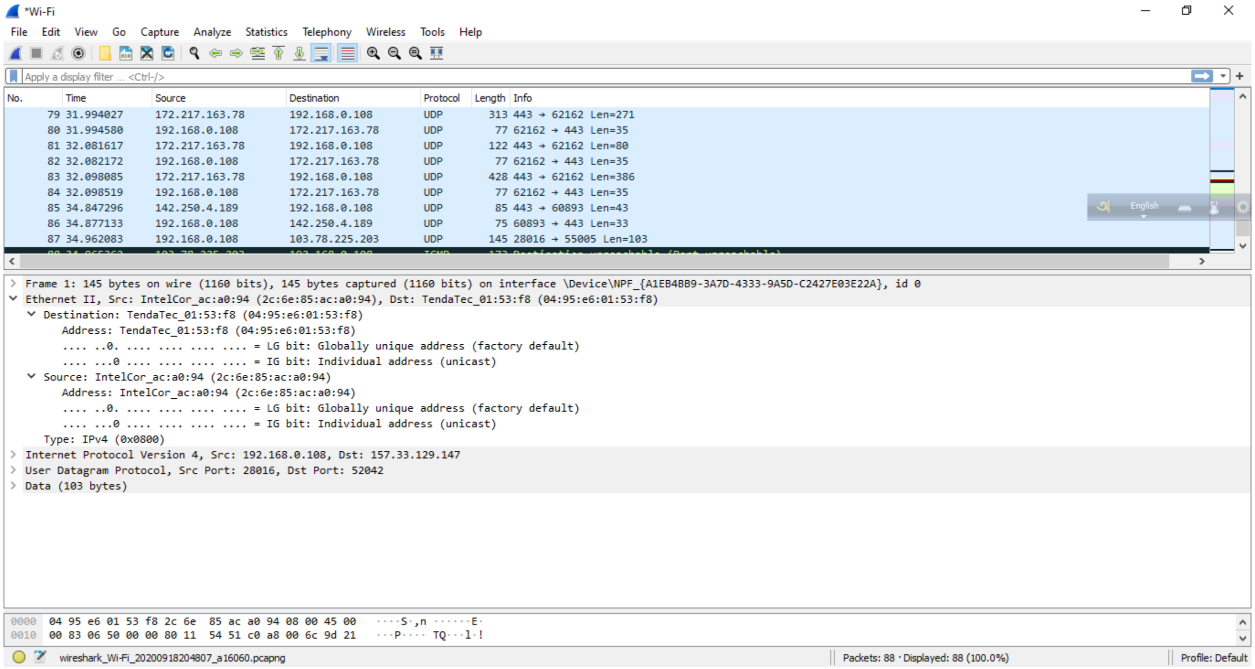

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_Wi-Fi_20200918204807_a16060.pcapng
Packets: 88 · Displayed: 88 (100.0%)
Profile: Default

```
No.     Time        Source           Destination      Protocol  Length Info
     79 31.994027   172.217.163.78   192.168.0.108    UDP        313 443 → 62162 Len=271
     80 31.994580   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     81 32.081617   172.217.163.78   192.168.0.108    UDP        122 443 → 62162 Len=80
     82 32.082172   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     83 32.098085   172.217.163.78   192.168.0.108    UDP        428 443 → 62162 Len=386
     84 32.098519   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     85 34.847296   142.250.4.189    192.168.0.108    UDP         85 443 → 60893 Len=43
     86 34.877133   192.168.0.108    142.250.4.189    UDP         75 60893 → 443 Len=33
     87 34.962083   192.168.0.108    103.78.225.203   UDP        145 28016 → 55005 Len=103
```

```
Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
  Interface id: 0 (\Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 18, 2020 20:48:09.535440000 Bangladesh Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1600440489.535440000 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)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:data]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94), Dst: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 157.33.129.147
User Datagram Protocol, Src Port: 28016, Dst Port: 52042
Data (103 bytes)
```

```
0000  04 95 e6 01 53 f8 2c 6e  85 ac a0 94 08 00 45 00   ····S·,n ······E·
0010  00 83 06 50 00 00 80 11  54 51 c0 a8 00 6c 9d 21   ···P···· TQ···l·!
```

Fig: Packet Details Pane (Frame segment)

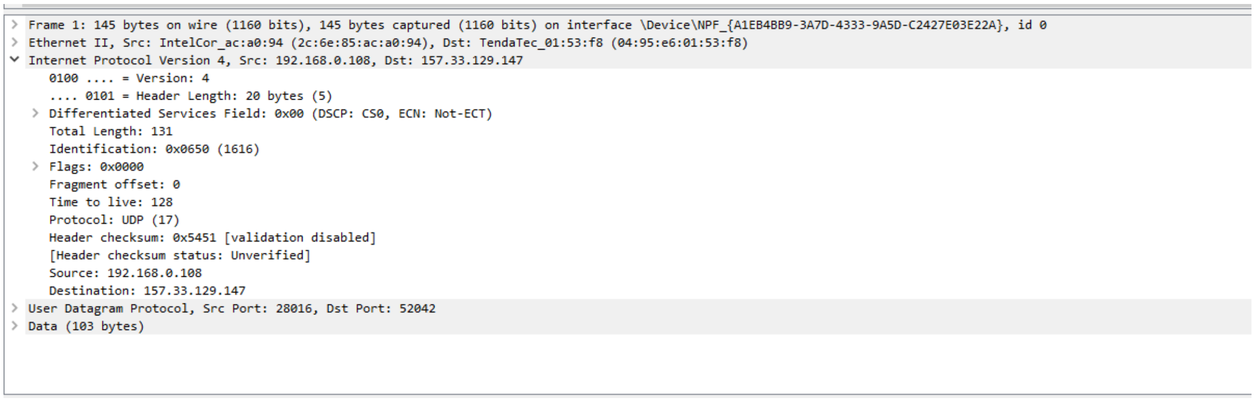

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_Wi-Fi_20200918204807_a16060.pcapng
Packets: 88 · Displayed: 88 (100.0%)
Profile: Default

```
No.     Time        Source           Destination      Protocol  Length Info
     79 31.994027   172.217.163.78   192.168.0.108    UDP        313 443 → 62162 Len=271
     80 31.994580   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     81 32.081617   172.217.163.78   192.168.0.108    UDP        122 443 → 62162 Len=80
     82 32.082172   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     83 32.098085   172.217.163.78   192.168.0.108    UDP        428 443 → 62162 Len=386
     84 32.098519   192.168.0.108    172.217.163.78   UDP         77 62162 → 443 Len=35
     85 34.847296   142.250.4.189    192.168.0.108    UDP         85 443 → 60893 Len=43
     86 34.877133   192.168.0.108    142.250.4.189    UDP         75 60893 → 443 Len=33
     87 34.962083   192.168.0.108    103.78.225.203   UDP        145 28016 → 55005 Len=103
```

```
Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{A1EB4BB9-3A7D-4333-9A5D-C2427E03E22A}, id 0
Ethernet II, Src: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94), Dst: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
  Destination: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
    Address: TendaTec_01:53:f8 (04:95:e6:01:53:f8)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94)
    Address: IntelCor_ac:a0:94 (2c:6e:85:ac:a0:94)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 157.33.129.147
User Datagram Protocol, Src Port: 28016, Dst Port: 52042
Data (103 bytes)
```

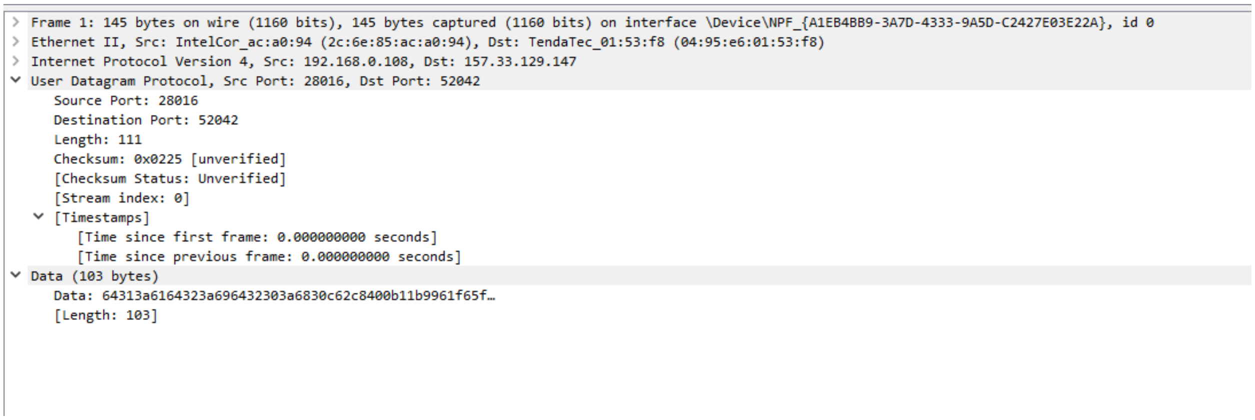
```
0000  04 95 e6 01 53 f8 2c 6e  85 ac a0 94 08 00 45 00   ····S·,n ······E·
0010  00 83 06 50 00 00 80 11  54 51 c0 a8 00 6c 9d 21   ···P···· TQ···l·!
```

Fig: Packet Details Pane (Ethernet segment)



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

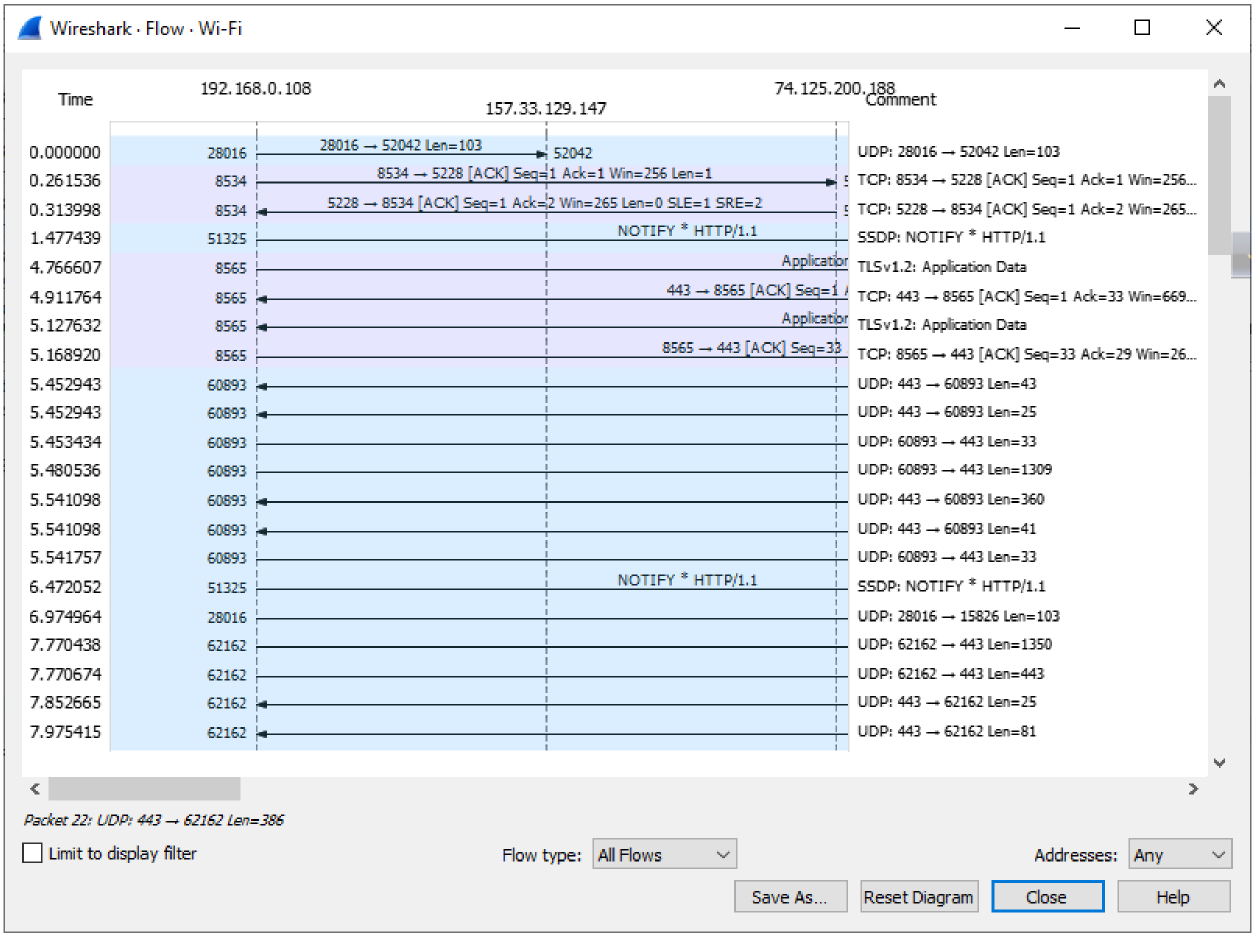
Fig: Packet Details Pane (IP segment)



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

Fig: Packet Details Pane (UDP segment)

Step 6: TCP plots and flowgraph



```
Time        192.168.0.108          157.33.129.147          74.125.200.188   Comment

0.000000    28016   28016 → 52042 Len=103   52042                         UDP: 28016 → 52042 Len=103
0.261536    8534    8534 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1           TCP: 8534 → 5228 [ACK] Seq=1 Ack=1 Win=256…
0.313998    8534    5228 → 8534 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2   TCP: 5228 → 8534 [ACK] Seq=1 Ack=2 Win=265…
1.477439    51325                          NOTIFY * HTTP/1.1              SSDP: NOTIFY * HTTP/1.1
4.766607    8565                                     Applicatior          TLSv1.2: Application Data
4.911764    8565                          443 → 8565 [ACK] Seq=1 /        TCP: 443 → 8565 [ACK] Seq=1 Ack=33 Win=669…
5.127632    8565                                     Applicatior          TLSv1.2: Application Data
5.168920    8565                          8565 → 443 [ACK] Seq=33         TCP: 8565 → 443 [ACK] Seq=33 Ack=29 Win=26…
5.452943    60893                                                         UDP: 443 → 60893 Len=43
5.452943    60893                                                         UDP: 443 → 60893 Len=25
5.453434    60893                                                         UDP: 60893 → 443 Len=33
5.480536    60893                                                         UDP: 60893 → 443 Len=1309
5.541098    60893                                                         UDP: 443 → 60893 Len=360
5.541098    60893                                                         UDP: 443 → 60893 Len=41
5.541757    60893                                                         UDP: 60893 → 443 Len=33
6.472052    51325                          NOTIFY * HTTP/1.1              SSDP: NOTIFY * HTTP/1.1
6.974964    28016                                                         UDP: 28016 → 15826 Len=103
7.770438    62162                                                         UDP: 62162 → 443 Len=1350
7.770674    62162                                                         UDP: 62162 → 443 Len=443
7.852665    62162                                                         UDP: 443 → 62162 Len=25
7.975415    62162                                                         UDP: 443 → 62162 Len=81
```

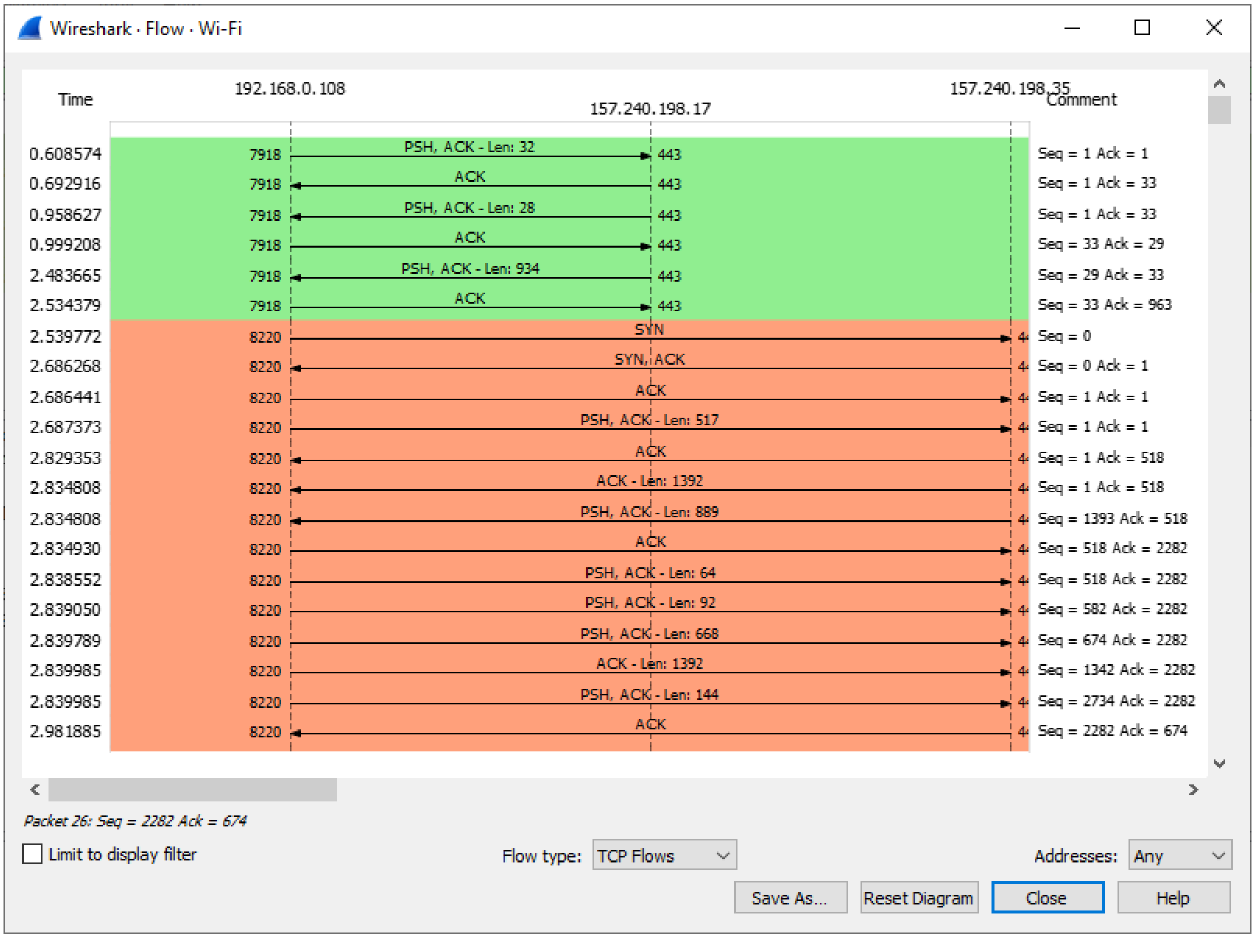
Packet 22: UDP: 443 → 62162 Len=386

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

Fig: Flowgraph(all flows)



Time	192.168.0.108		157.240.198.17 / 157.240.198.35	Comment
0.608574	7918	PSH, ACK - Len: 32 →	443	Seq = 1 Ack = 1
0.692916	7918	← ACK	443	Seq = 1 Ack = 33
0.958627	7918	← PSH, ACK - Len: 28	443	Seq = 1 Ack = 33
0.999208	7918	ACK →	443	Seq = 33 Ack = 29
2.483665	7918	← PSH, ACK - Len: 934	443	Seq = 29 Ack = 33
2.534379	7918	ACK →	443	Seq = 33 Ack = 963
2.539772	8220	SYN →	44	Seq = 0
2.686268	8220	← SYN, ACK	44	Seq = 0 Ack = 1
2.686441	8220	ACK →	44	Seq = 1 Ack = 1
2.687373	8220	PSH, ACK - Len: 517 →	44	Seq = 1 Ack = 1
2.829353	8220	← ACK	44	Seq = 1 Ack = 518
2.834808	8220	← ACK - Len: 1392	44	Seq = 1 Ack = 518
2.834808	8220	← PSH, ACK - Len: 889	44	Seq = 1393 Ack = 518
2.834930	8220	ACK →	44	Seq = 518 Ack = 2282
2.838552	8220	PSH, ACK - Len: 64 →	44	Seq = 518 Ack = 2282
2.839050	8220	PSH, ACK - Len: 92 →	44	Seq = 582 Ack = 2282
2.839789	8220	PSH, ACK - Len: 668 →	44	Seq = 674 Ack = 2282
2.839985	8220	ACK - Len: 1392 →	44	Seq = 1342 Ack = 2282
2.839985	8220	PSH, ACK - Len: 144 →	44	Seq = 2734 Ack = 2282
2.981885	8220	← ACK	44	Seq = 2282 Ack = 674

Packet 26: Seq = 2282 Ack = 674

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

Fig: TCP flowgraph

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