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 Khaled Hasan Manna

ID:IT-16011

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:

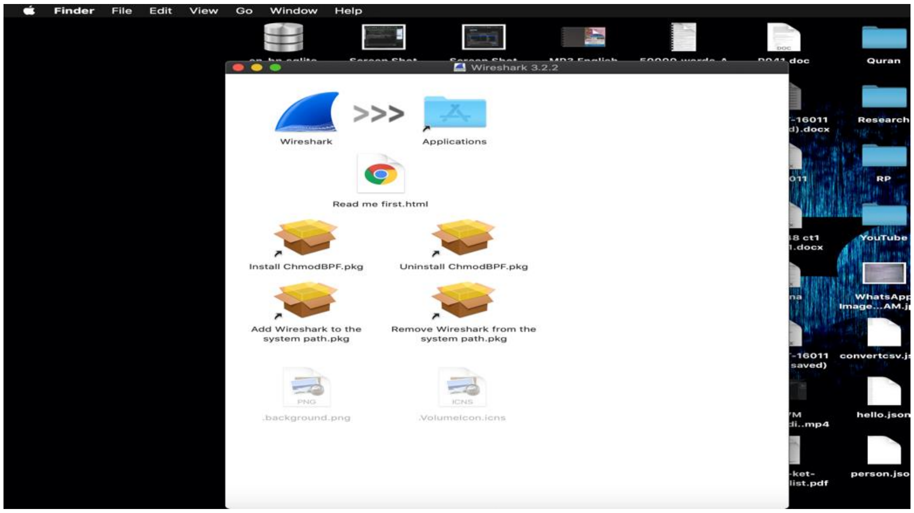
- Wireshark is a popular network analyzers
- That uses pcap library to capture network packets at different layers of the OSI model
- It is easy to install and possesses a nice GUI with many feature
- Capture live packet data from a network interface.
- Display packets with very detailed protocol information.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

## Wireshark Installation on macOS Catalina :

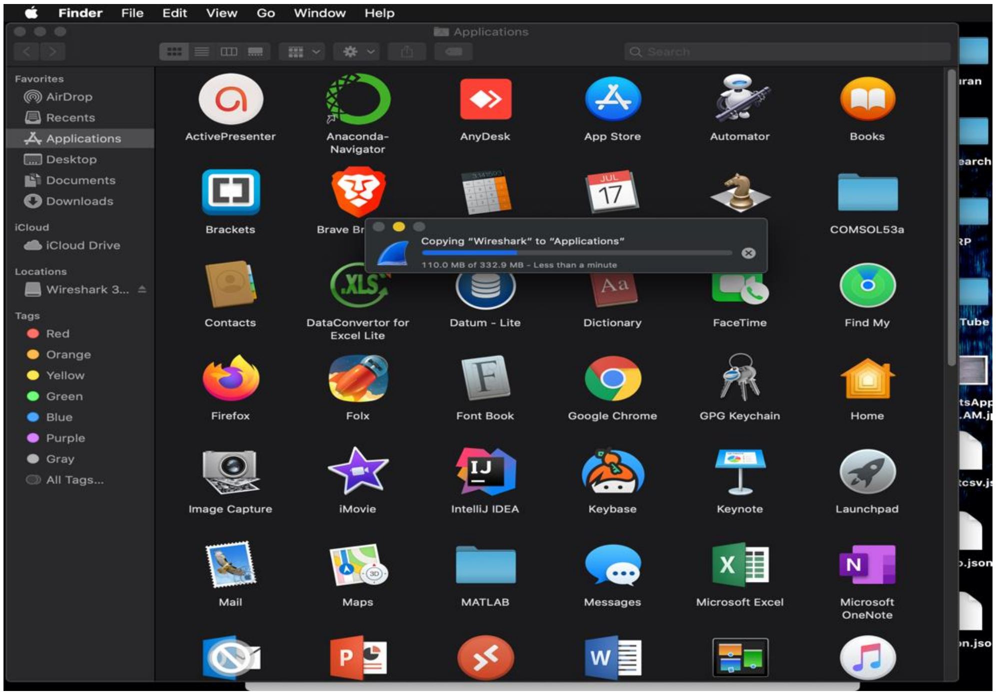
## Installation of  Wireshark requires:

- Download the relevant package
- Build the source into binary if the source is downloaded
- Install binary to their destinations
- Section 2 provide detailed installation instructions
- http://www.wireshark.org/docs/wsug_html

Download and Run Process:



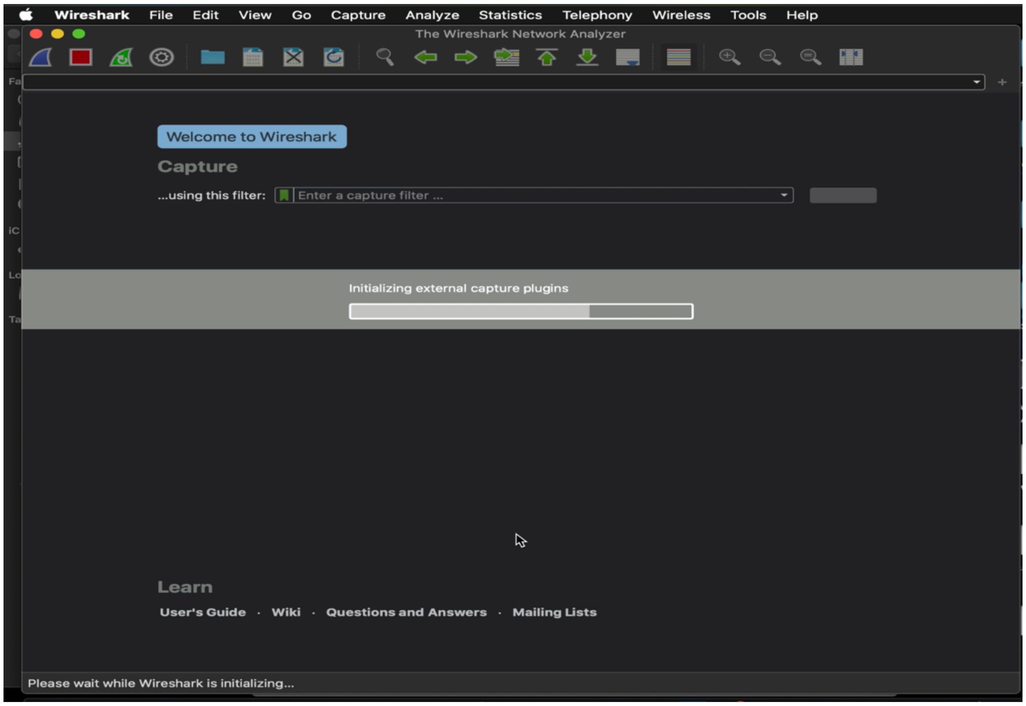
Copying to Application:



Copying “Wireshark” to “Applications”

110.0 MB of 332.9 MB - Less than a minute

Run and Open Wireshark:



Initializing external capture plugins

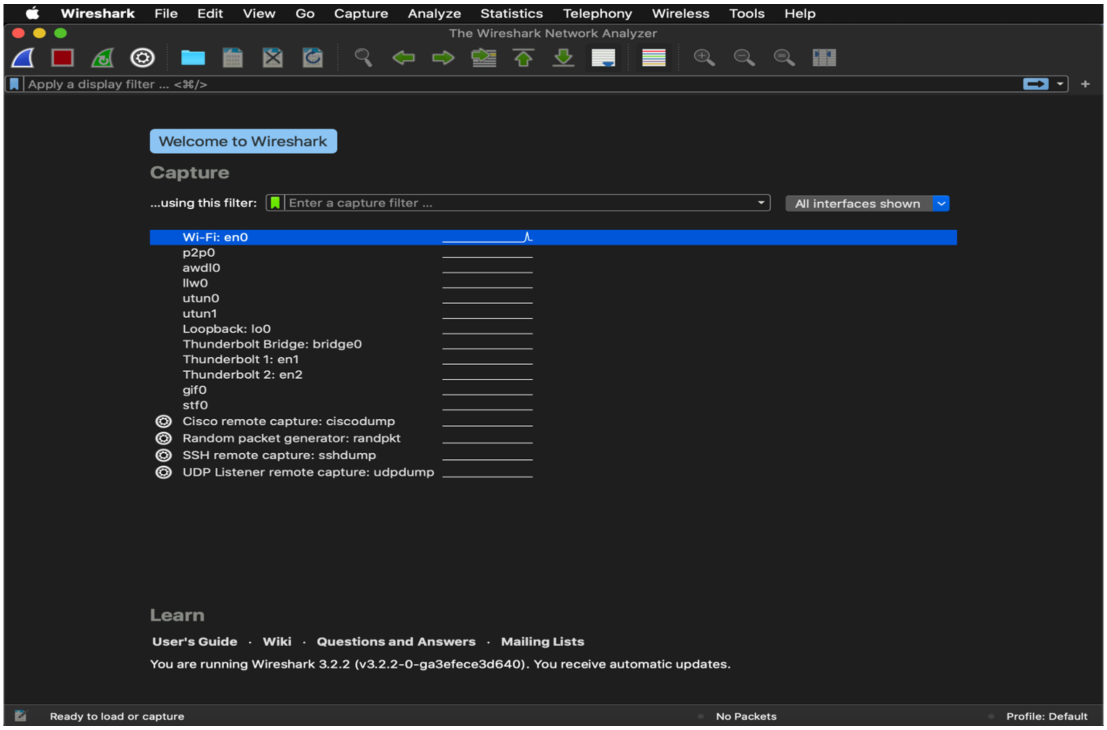
Please wait while Wireshark is initializing...

## 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

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.

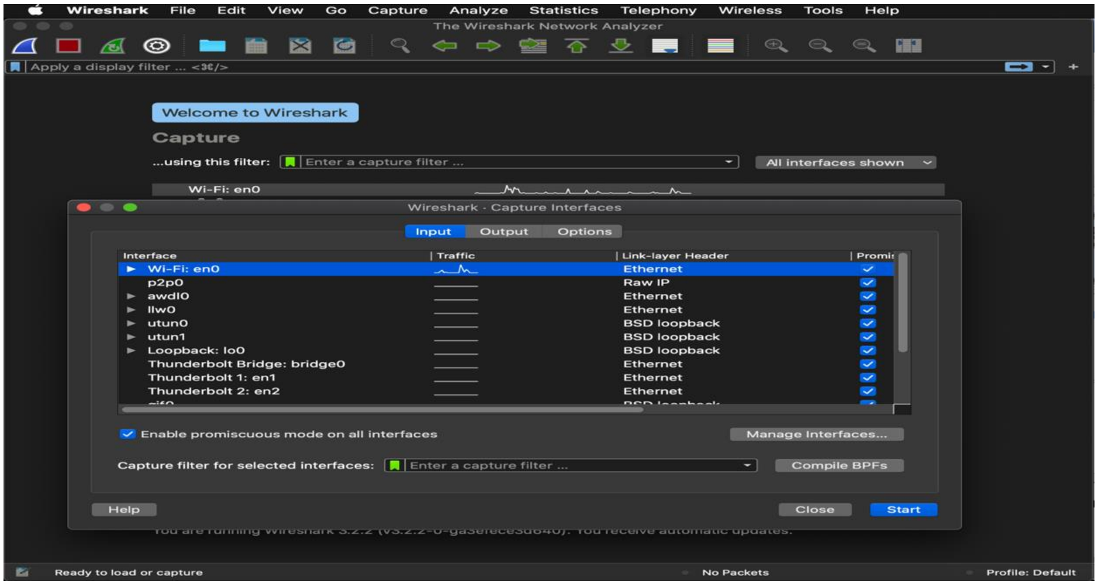

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing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

Wi-Fi: en0
p2p0
awdl0
llw0
utun0
utun1
Loopback: lo0
Thunderbolt Bridge: bridge0
Thunderbolt 1: en1
Thunderbolt 2: en2
gif0
stf0
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

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 01: Wireshark Interface List**


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wireshark · Capture Interfaces
Input
Output
Options
Manage Interfaces...
Compile BPFs
Help
Close
Start

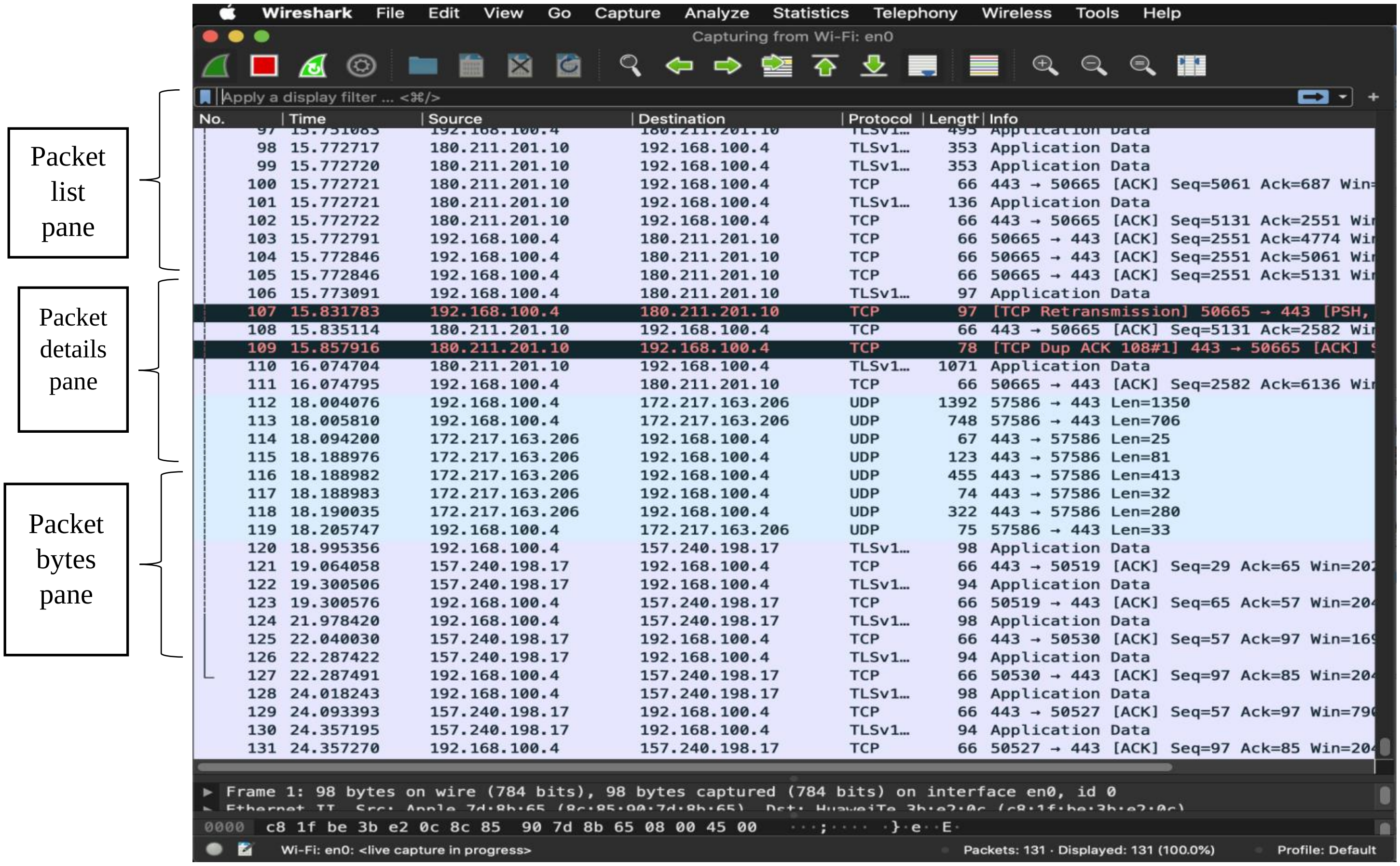
| Interface | Traffic | Link-layer Header | Promis |
|---|---|---|---|
| ► Wi-Fi: en0 | | Ethernet | ✓ |
| p2p0 | | Raw IP | ✓ |
| ► awdl0 | | Ethernet | ✓ |
| ► llw0 | | Ethernet | ✓ |
| ► utun0 | | BSD loopback | ✓ |
| ► utun1 | | BSD loopback | ✓ |
| ► Loopback: lo0 | | BSD loopback | ✓ |
| Thunderbolt Bridge: bridge0 | | Ethernet | ✓ |
| Thunderbolt 1: en1 | | Ethernet | ✓ |
| Thunderbolt 2: en2 | | Ethernet | ✓ |

☑ Enable promiscuous mode on all interfaces

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

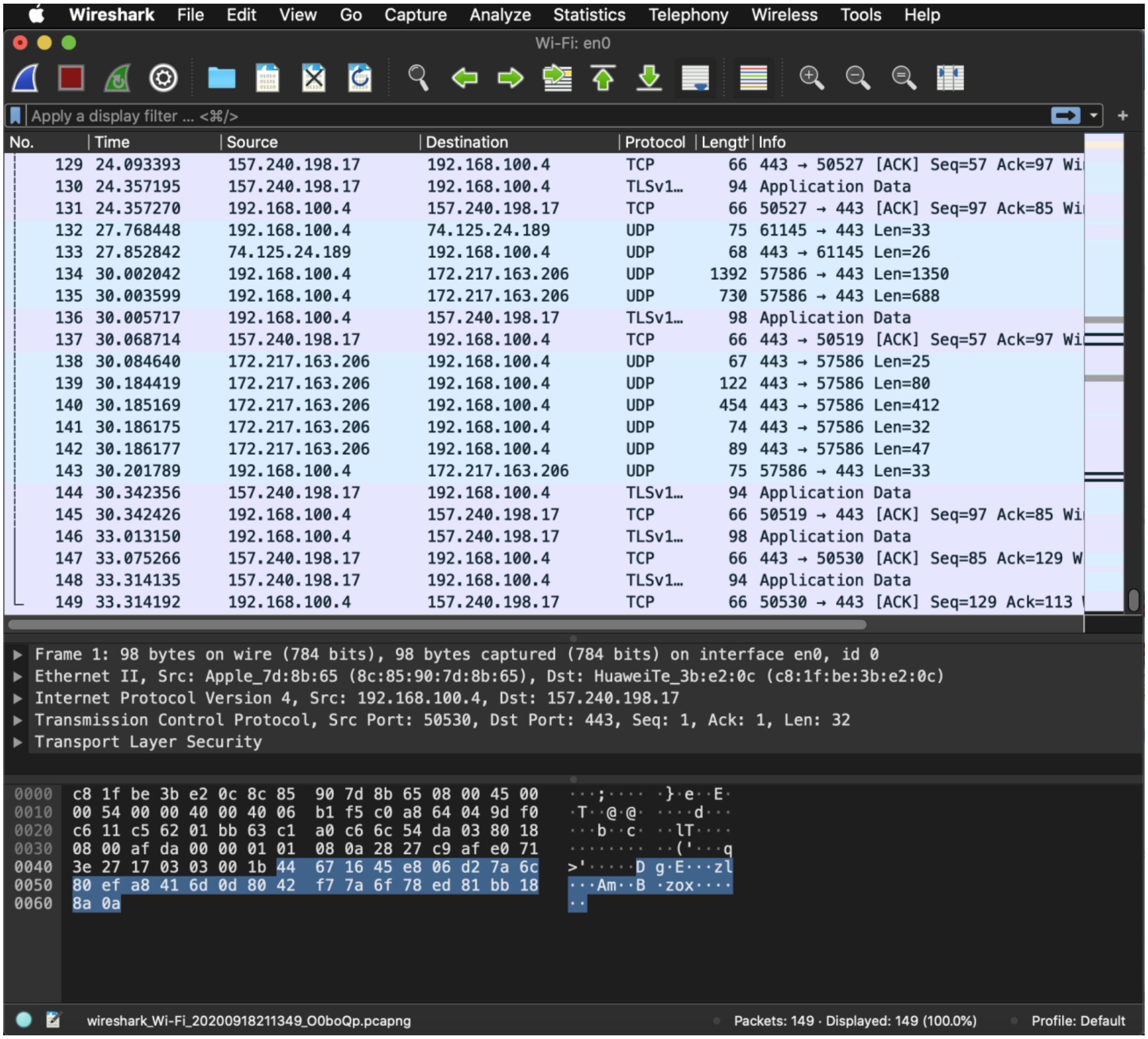
Ready to load or capture · No Packets · Profile: Default

**Figure 02: Start Capturing Interface that has IP address**



```
No.    Time       Source           Destination      Protocol  Length  Info
 97  15.751083  192.168.100.4    180.211.201.10   TLSv1…     495  Application Data
 98  15.772717  180.211.201.10   192.168.100.4    TLSv1…     353  Application Data
 99  15.772720  180.211.201.10   192.168.100.4    TLSv1…     353  Application Data
100  15.772721  180.211.201.10   192.168.100.4    TCP         66  443 → 50665 [ACK] Seq=5061 Ack=687 Win=
101  15.772721  180.211.201.10   192.168.100.4    TLSv1…     136  Application Data
102  15.772722  180.211.201.10   192.168.100.4    TCP         66  443 → 50665 [ACK] Seq=5131 Ack=2551 Wi
103  15.772791  192.168.100.4    180.211.201.10   TCP         66  50665 → 443 [ACK] Seq=2551 Ack=4774 Wi
104  15.772846  192.168.100.4    180.211.201.10   TCP         66  50665 → 443 [ACK] Seq=2551 Ack=5061 Wi
105  15.772846  192.168.100.4    180.211.201.10   TCP         66  50665 → 443 [ACK] Seq=2551 Ack=5131 Wi
106  15.773091  192.168.100.4    180.211.201.10   TLSv1…      97  Application Data
107  15.831783  192.168.100.4    180.211.201.10   TCP         97  [TCP Retransmission] 50665 → 443 [PSH,
108  15.835114  180.211.201.10   192.168.100.4    TCP         66  443 → 50665 [ACK] Seq=5131 Ack=2582 Wi
109  15.857916  180.211.201.10   192.168.100.4    TCP         78  [TCP Dup ACK 108#1] 443 → 50665 [ACK] S
110  16.074704  180.211.201.10   192.168.100.4    TLSv1…    1071  Application Data
111  16.074795  192.168.100.4    180.211.201.10   TCP         66  50665 → 443 [ACK] Seq=2582 Ack=6136 Wi
112  18.004076  192.168.100.4    172.217.163.206  UDP       1392  57586 → 443 Len=1350
113  18.005810  192.168.100.4    172.217.163.206  UDP        748  57586 → 443 Len=706
114  18.094200  172.217.163.206  192.168.100.4    UDP         67  443 → 57586 Len=25
115  18.188976  172.217.163.206  192.168.100.4    UDP        123  443 → 57586 Len=81
116  18.188982  172.217.163.206  192.168.100.4    UDP        455  443 → 57586 Len=413
117  18.188983  172.217.163.206  192.168.100.4    UDP         74  443 → 57586 Len=32
118  18.190035  172.217.163.206  192.168.100.4    UDP        322  443 → 57586 Len=280
119  18.205747  192.168.100.4    172.217.163.206  UDP         75  57586 → 443 Len=33
120  18.995356  192.168.100.4    157.240.198.17   TLSv1…      98  Application Data
121  19.064058  157.240.198.17   192.168.100.4    TCP         66  443 → 50519 [ACK] Seq=29 Ack=65 Win=20
122  19.300506  157.240.198.17   192.168.100.4    TLSv1…      94  Application Data
123  19.300576  192.168.100.4    157.240.198.17   TCP         66  50519 → 443 [ACK] Seq=65 Ack=57 Win=20
124  21.978420  192.168.100.4    157.240.198.17   TLSv1…      98  Application Data
125  22.040030  157.240.198.17   192.168.100.4    TCP         66  443 → 50530 [ACK] Seq=57 Ack=97 Win=16
126  22.287422  157.240.198.17   192.168.100.4    TLSv1…      94  Application Data
127  22.287491  192.168.100.4    157.240.198.17   TCP         66  50530 → 443 [ACK] Seq=97 Ack=85 Win=20
128  24.018243  192.168.100.4    157.240.198.17   TLSv1…      98  Application Data
129  24.093393  157.240.198.17   192.168.100.4    TCP         66  443 → 50527 [ACK] Seq=57 Ack=97 Win=79
130  24.357195  157.240.198.17   192.168.100.4    TLSv1…      94  Application Data
131  24.357270  192.168.100.4    157.240.198.17   TCP         66  50527 → 443 [ACK] Seq=97 Ack=85 Win=20

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·

Wi-Fi: en0: <live capture in progress>          Packets: 131 · Displayed: 131 (100.0%)     Profile: Default
```

**Figure 03: A sample packet capture window**



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 129 | 24.093393 | 157.240.198.17 | 192.168.100.4 | TCP | 66 | 443 → 50527 [ACK] Seq=57 Ack=97 Wi |
| 130 | 24.357195 | 157.240.198.17 | 192.168.100.4 | TLSv1… | 94 | Application Data |
| 131 | 24.357270 | 192.168.100.4 | 157.240.198.17 | TCP | 66 | 50527 → 443 [ACK] Seq=97 Ack=85 Wi |
| 132 | 27.768448 | 192.168.100.4 | 74.125.24.189 | UDP | 75 | 61145 → 443 Len=33 |
| 133 | 27.852842 | 74.125.24.189 | 192.168.100.4 | UDP | 68 | 443 → 61145 Len=26 |
| 134 | 30.002042 | 192.168.100.4 | 172.217.163.206 | UDP | 1392 | 57586 → 443 Len=1350 |
| 135 | 30.003599 | 192.168.100.4 | 172.217.163.206 | UDP | 730 | 57586 → 443 Len=688 |
| 136 | 30.005717 | 192.168.100.4 | 157.240.198.17 | TLSv1… | 98 | Application Data |
| 137 | 30.068714 | 157.240.198.17 | 192.168.100.4 | TCP | 66 | 443 → 50519 [ACK] Seq=57 Ack=97 Wi |
| 138 | 30.084640 | 172.217.163.206 | 192.168.100.4 | UDP | 67 | 443 → 57586 Len=25 |
| 139 | 30.184419 | 172.217.163.206 | 192.168.100.4 | UDP | 122 | 443 → 57586 Len=80 |
| 140 | 30.185169 | 172.217.163.206 | 192.168.100.4 | UDP | 454 | 443 → 57586 Len=412 |
| 141 | 30.186175 | 172.217.163.206 | 192.168.100.4 | UDP | 74 | 443 → 57586 Len=32 |
| 142 | 30.186177 | 172.217.163.206 | 192.168.100.4 | UDP | 89 | 443 → 57586 Len=47 |
| 143 | 30.201789 | 192.168.100.4 | 172.217.163.206 | UDP | 75 | 57586 → 443 Len=33 |
| 144 | 30.342356 | 157.240.198.17 | 192.168.100.4 | TLSv1… | 94 | Application Data |
| 145 | 30.342426 | 192.168.100.4 | 157.240.198.17 | TCP | 66 | 50519 → 443 [ACK] Seq=97 Ack=85 Wi |
| 146 | 33.013150 | 192.168.100.4 | 157.240.198.17 | TLSv1… | 98 | Application Data |
| 147 | 33.075266 | 157.240.198.17 | 192.168.100.4 | TCP | 66 | 443 → 50530 [ACK] Seq=85 Ack=129 W |
| 148 | 33.314135 | 157.240.198.17 | 192.168.100.4 | TLSv1… | 94 | Application Data |
| 149 | 33.314192 | 192.168.100.4 | 157.240.198.17 | TCP | 66 | 50530 → 443 [ACK] Seq=129 Ack=113 \ |

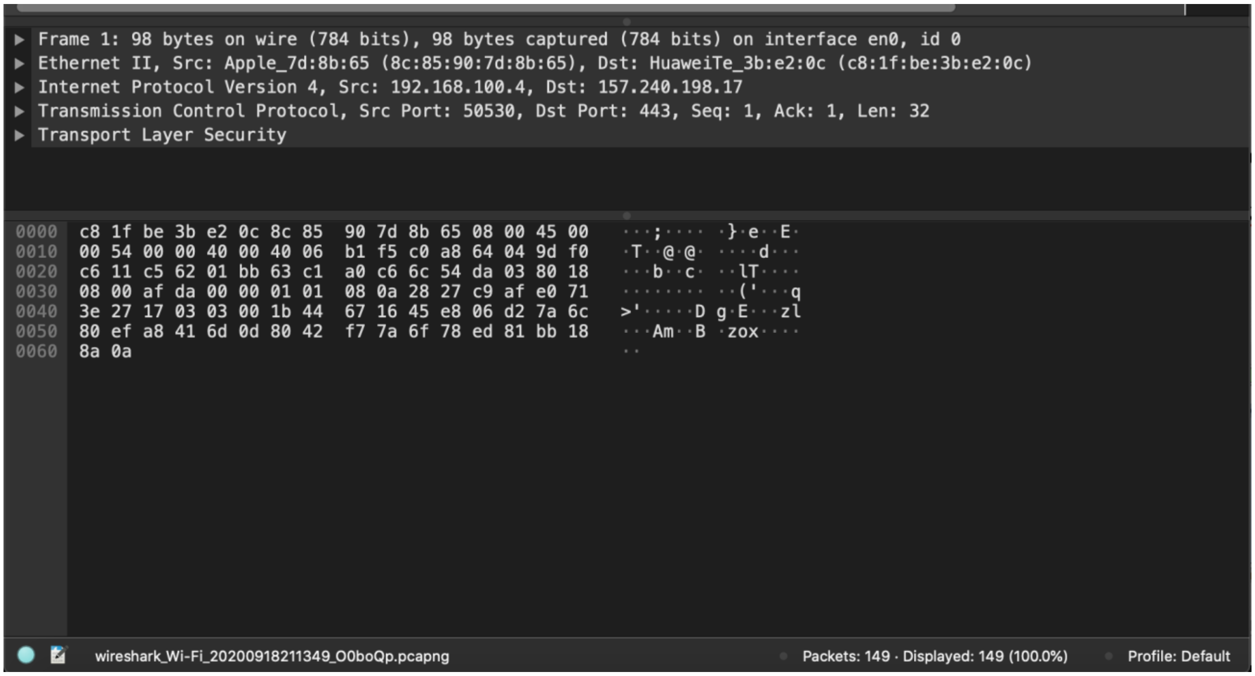
```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17
▶ Transmission Control Protocol, Src Port: 50530, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
▶ Transport Layer Security
```

```
0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 62 01 bb 63 c1  a0 c6 6c 54 da 03 80 18   ···b··c·  ··lT····
0030  08 00 af da 00 00 01 01  08 0a 28 27 c9 af e0 71   ········  ··('···q
0040  3e 27 17 03 03 00 1b 44  67 16 45 e8 06 d2 7a 6c   >'·····D  g·E···zl
0050  80 ef a8 41 6d 0d 80 42  f7 7a 6f 78 ed 81 bb 18   ···Am··B  ·zox····
0060  8a 0a                                              ··
```

wireshark_Wi-Fi_20200918211349_O0boQp.pcapng     Packets: 149 · Displayed: 149 (100.0%)     Profile: Default

**Figure 04: Stopping Capture**

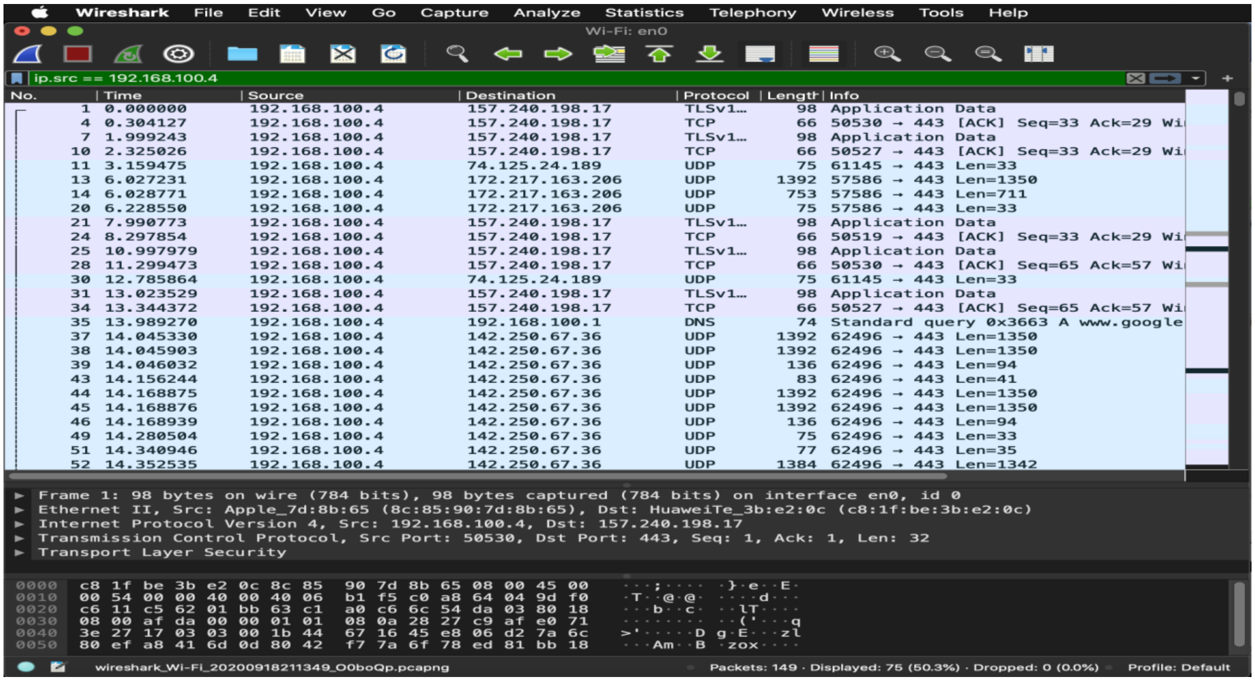
## Filtering:



```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17
▶ Transmission Control Protocol, Src Port: 50530, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
▶ Transport Layer Security

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 62 01 bb 63 c1  a0 c6 6c 54 da 03 80 18   ···b··c·  ··lT····
0030  08 00 af da 00 00 01 01  08 0a 28 27 c9 af e0 71   ········  ··('···q
0040  3e 27 17 03 03 00 1b 44  67 16 45 e8 06 d2 7a 6c   >'·····D g·E···zl
0050  80 ef a8 41 6d 0d 80 42  f7 7a 6f 78 ed 81 bb 18   ···Am··B ·zox····
0060  8a 0a                                              ··

wireshark_Wi-Fi_20200918211349_O0boQp.pcapng     Packets: 149 · Displayed: 149 (100.0%)     Profile: Default
```

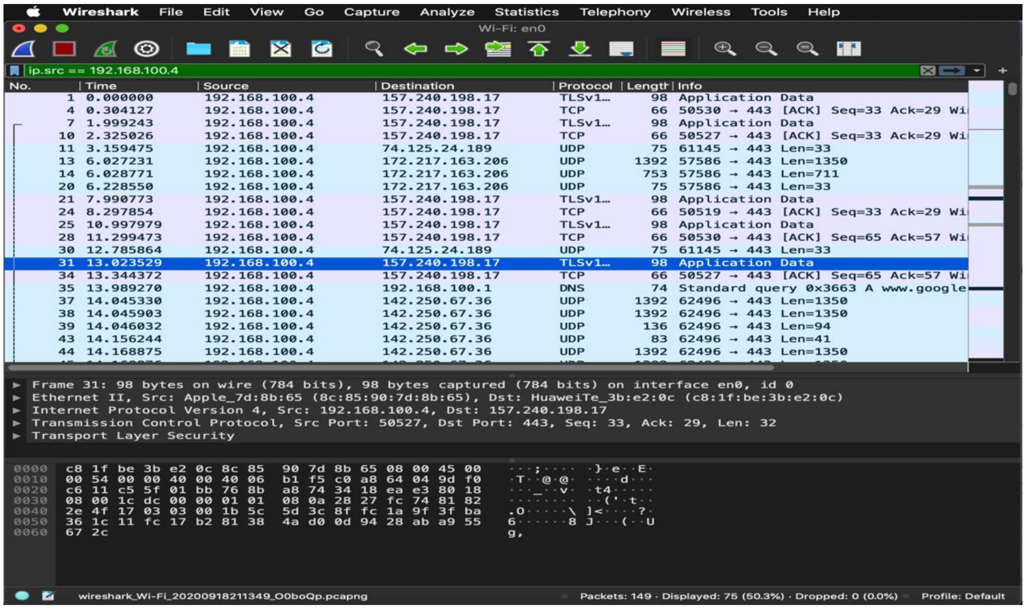
**Figure 05: Filter by Protocol**

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.



```
ip.src == 192.168.100.4

No.   Time        Source           Destination       Protocol  Length  Info
   1  0.000000    192.168.100.4    157.240.198.17    TLSv1…        98  Application Data
   4  0.304127    192.168.100.4    157.240.198.17    TCP           66  50530 → 443 [ACK] Seq=33 Ack=29 Wi
   7  1.999243    192.168.100.4    157.240.198.17    TLSv1…        98  Application Data
  10  2.325026    192.168.100.4    157.240.198.17    TCP           66  50527 → 443 [ACK] Seq=33 Ack=29 Wi
  11  3.159475    192.168.100.4    74.125.24.189     UDP           75  61145 → 443 Len=33
  13  6.027231    192.168.100.4    172.217.163.206   UDP         1392  57586 → 443 Len=1350
  14  6.028771    192.168.100.4    172.217.163.206   UDP          753  57586 → 443 Len=711
  20  6.228550    192.168.100.4    172.217.163.206   UDP           75  57586 → 443 Len=33
  21  7.990773    192.168.100.4    157.240.198.17    TLSv1…        98  Application Data
  24  8.297854    192.168.100.4    157.240.198.17    TCP           66  50519 → 443 [ACK] Seq=33 Ack=29 Wi
  25  10.997979   192.168.100.4    157.240.198.17    TLSv1…        98  Application Data
  28  11.299473   192.168.100.4    157.240.198.17    TCP           66  50530 → 443 [ACK] Seq=65 Ack=57 Wi
  30  12.785864   192.168.100.4    74.125.24.189     UDP           75  61145 → 443 Len=33
  31  13.023529   192.168.100.4    157.240.198.17    TLSv1…        98  Application Data
  34  13.344372   192.168.100.4    157.240.198.17    TCP           66  50527 → 443 [ACK] Seq=65 Ack=57 Wi
  35  13.989270   192.168.100.4    192.168.100.1     DNS           74  Standard query 0x3663 A www.google
  37  14.045330   192.168.100.4    142.250.67.36     UDP         1392  62496 → 443 Len=1350
  38  14.045903   192.168.100.4    142.250.67.36     UDP         1392  62496 → 443 Len=1350
  39  14.046032   192.168.100.4    142.250.67.36     UDP          136  62496 → 443 Len=94
  43  14.156244   192.168.100.4    142.250.67.36     UDP           83  62496 → 443 Len=41
  44  14.168875   192.168.100.4    142.250.67.36     UDP         1392  62496 → 443 Len=1350
  45  14.168876   192.168.100.4    142.250.67.36     UDP         1392  62496 → 443 Len=1350
  46  14.168939   192.168.100.4    142.250.67.36     UDP          136  62496 → 443 Len=94
  49  14.280504   192.168.100.4    142.250.67.36     UDP           75  62496 → 443 Len=33
  51  14.340946   192.168.100.4    142.250.67.36     UDP           77  62496 → 443 Len=35
  52  14.352535   192.168.100.4    142.250.67.36     UDP         1384  62496 → 443 Len=1342

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17
▶ Transmission Control Protocol, Src Port: 50530, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
▶ Transport Layer Security

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 62 01 bb 63 c1  a0 c6 6c 54 da 03 80 18   ···b··c·  ··lT····
0030  08 00 af da 00 00 01 01  08 0a 28 27 c9 af e0 71   ········  ··('···q
0040  3e 27 17 03 03 00 1b 44  67 16 45 e8 06 d2 7a 6c   >'·····D g·E···zl
0050  80 ef a8 41 6d 0d 80 42  f7 7a 6f 78 ed 81 bb 18   ···Am··B ·zox····

wireshark_Wi-Fi_20200918211349_O0boQp.pcapng     Packets: 149 · Displayed: 75 (50.3%) · Dropped: 0 (0.0%)     Profile: Default
```

**Figure 06: Source IP filter**


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wi-Fi: en0

```
ip.src == 192.168.100.4
```

```
No.  Time       Source          Destination      Protocol Length Info
  1  0.000000   192.168.100.4   157.240.198.17   TLSv1…     98  Application Data
  4  0.304127   192.168.100.4   157.240.198.17   TCP        66  50530 → 443 [ACK] Seq=33 Ack=29 Wi
  7  1.999243   192.168.100.4   157.240.198.17   TLSv1…     98  Application Data
 10  2.325026   192.168.100.4   157.240.198.17   TCP        66  50527 → 443 [ACK] Seq=33 Ack=29 Wi
 11  3.159475   192.168.100.4   74.125.24.189    UDP        75  61145 → 443 Len=33
 13  6.027231   192.168.100.4   172.217.163.206  UDP      1392  57586 → 443 Len=1350
 14  6.028771   192.168.100.4   172.217.163.206  UDP       753  57586 → 443 Len=711
 20  6.228550   192.168.100.4   172.217.163.206  UDP        75  57586 → 443 Len=33
 21  7.990773   192.168.100.4   157.240.198.17   TLSv1…     98  Application Data
 24  8.297854   192.168.100.4   157.240.198.17   TCP        66  50519 → 443 [ACK] Seq=33 Ack=29 Wi
 25  10.997979  192.168.100.4   157.240.198.17   TLSv1…     98  Application Data
 28  11.299473  192.168.100.4   157.240.198.17   TCP        66  50530 → 443 [ACK] Seq=65 Ack=57 Wi
 30  12.785864  192.168.100.4   74.125.24.189    UDP        75  61145 → 443 Len=33
 31  13.023529  192.168.100.4   157.240.198.17   TLSv1…     98  Application Data
 34  13.344372  192.168.100.4   157.240.198.17   TCP        66  50527 → 443 [ACK] Seq=65 Ack=57 Wi
 35  13.989270  192.168.100.4   192.168.100.1    DNS        74  Standard query 0x3663 A www.google
 37  14.045330  192.168.100.4   142.250.67.36    UDP      1392  62496 → 443 Len=1350
 38  14.045903  192.168.100.4   142.250.67.36    UDP      1392  62496 → 443 Len=1350
 39  14.046032  192.168.100.4   142.250.67.36    UDP       136  62496 → 443 Len=94
 43  14.156244  192.168.100.4   142.250.67.36    UDP        83  62496 → 443 Len=41
 44  14.168875  192.168.100.4   142.250.67.36    UDP      1392  62496 → 443 Len=1350
```

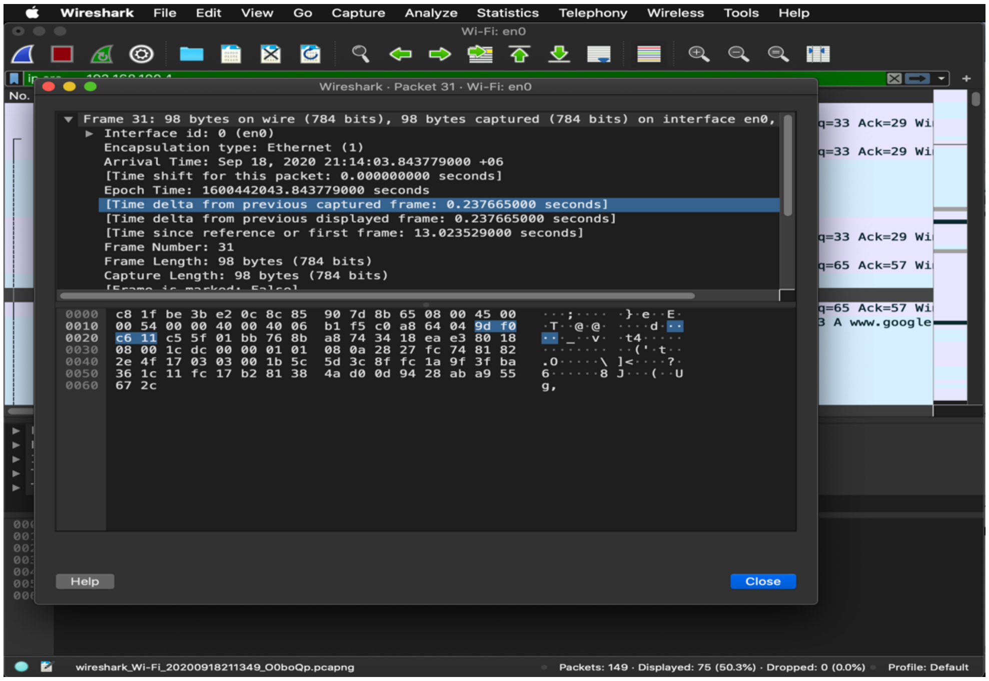
```
▶ Frame 31: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17
▶ Transmission Control Protocol, Src Port: 50527, Dst Port: 443, Seq: 33, Ack: 29, Len: 32
▶ Transport Layer Security
```

```
0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 5f 01 bb 76 8b  a8 74 34 18 ea e3 80 18   ···_··v·  ·t4·····
0030  08 00 1c dc 00 00 01 01  08 0a 28 27 fc 74 81 82   ········  ··('·t··
0040  2e 4f 17 03 03 00 1b 5c  5d 3c 8f fc 1a 9f 3f ba   .O·····\  ]<····?·
0050  36 1c 11 fc 17 b2 81 38  4a d0 0d 94 28 ab a9 55   6······8  J···(··U
0060  67 2c                                              g,
```

```
wireshark_Wi-Fi_20200918211349_O0boQp.pcapng    Packets: 149 · Displayed: 75 (50.3%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 07: 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**

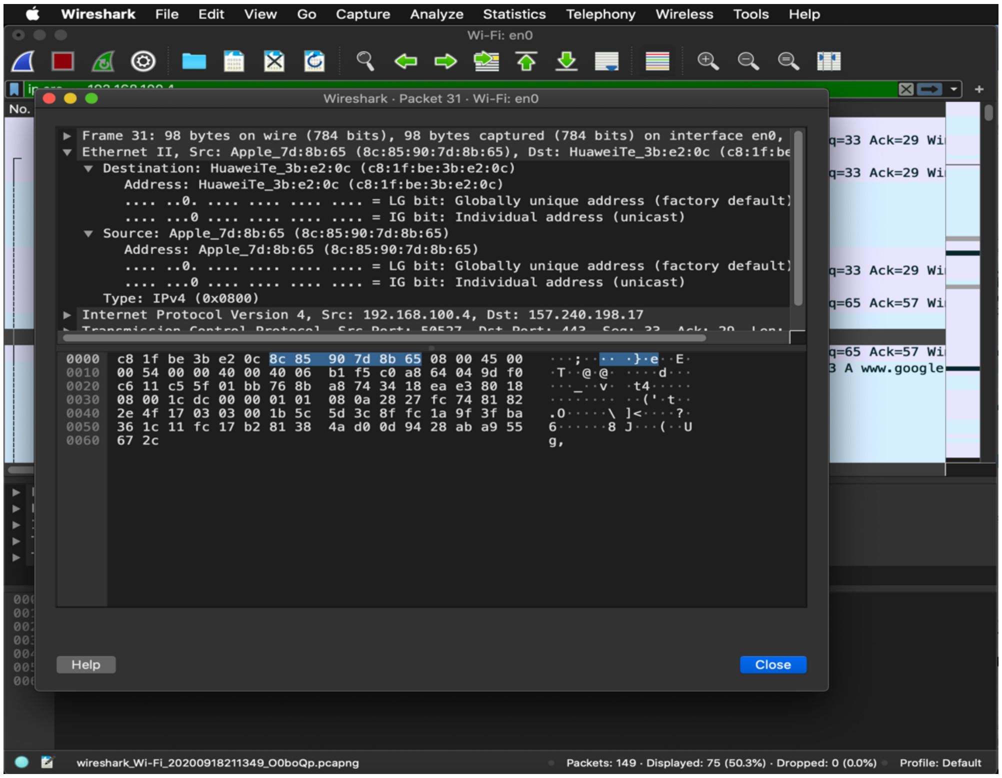

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wi-Fi: en0
Wireshark · Packet 31 · Wi-Fi: en0
Help
Close

```
▼ Frame 31: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0,
  ▶ Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 21:14:03.843779000 +06
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600442043.843779000 seconds
    [Time delta from previous captured frame: 0.237665000 seconds]
    [Time delta from previous displayed frame: 0.237665000 seconds]
    [Time since reference or first frame: 13.023529000 seconds]
    Frame Number: 31
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
```

```
0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 5f 01 bb 76 8b  a8 74 34 18 ea e3 80 18   ···_··v·  ·t4·····
0030  08 00 1c dc 00 00 01 01  08 0a 28 27 fc 74 81 82   ········  ··('·t··
0040  2e 4f 17 03 03 00 1b 5c  5d 3c 8f fc 1a 9f 3f ba   .O·····\  ]<····?·
0050  36 1c 11 fc 17 b2 81 38  4a d0 0d 94 28 ab a9 55   6······8  J···(··U
0060  67 2c                                              g,
```

```
wireshark_Wi-Fi_20200918211349_O0boQp.pcapng    Packets: 149 · Displayed: 75 (50.3%) · Dropped: 0 (0.0%)    Profile: Default
```

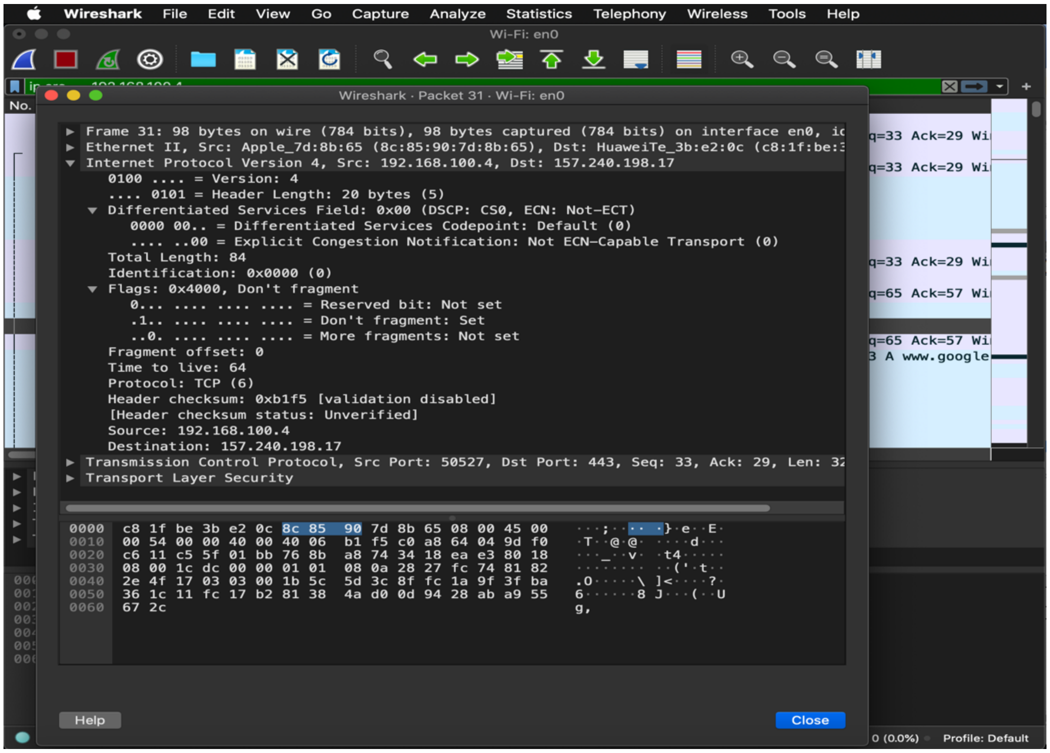
Figure 08: Packet Details Pane(Frame segment)



```
▶ Frame 31: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0,
▼ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be
  ▼ Destination: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
      Address: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: Apple_7d:8b:65 (8c:85:90:7d:8b:65)
      Address: Apple_7d:8b:65 (8c:85:90:7d:8b:65)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;··· ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@· ····d···
0020  c6 11 c5 5f 01 bb 76 8b  a8 74 34 18 ea e3 80 18   ···_··v· ·t4·····
0030  08 00 1c dc 00 00 01 01  08 0a 28 27 fc 74 81 82   ········ ··('·t··
0040  2e 4f 17 03 03 00 1b 5c  5d 3c 8f fc 1a 9f 3f ba   .O·····\ ]<····?·
0050  36 1c 11 fc 17 b2 81 38  4a d0 0d 94 28 ab a9 55   6······8 J···(··U
0060  67 2c                                              g,
```

wireshark_Wi-Fi_20200918211349_O0boQp.pcapng · Packets: 149 · Displayed: 75 (50.3%) · Dropped: 0 (0.0%) · Profile: Default

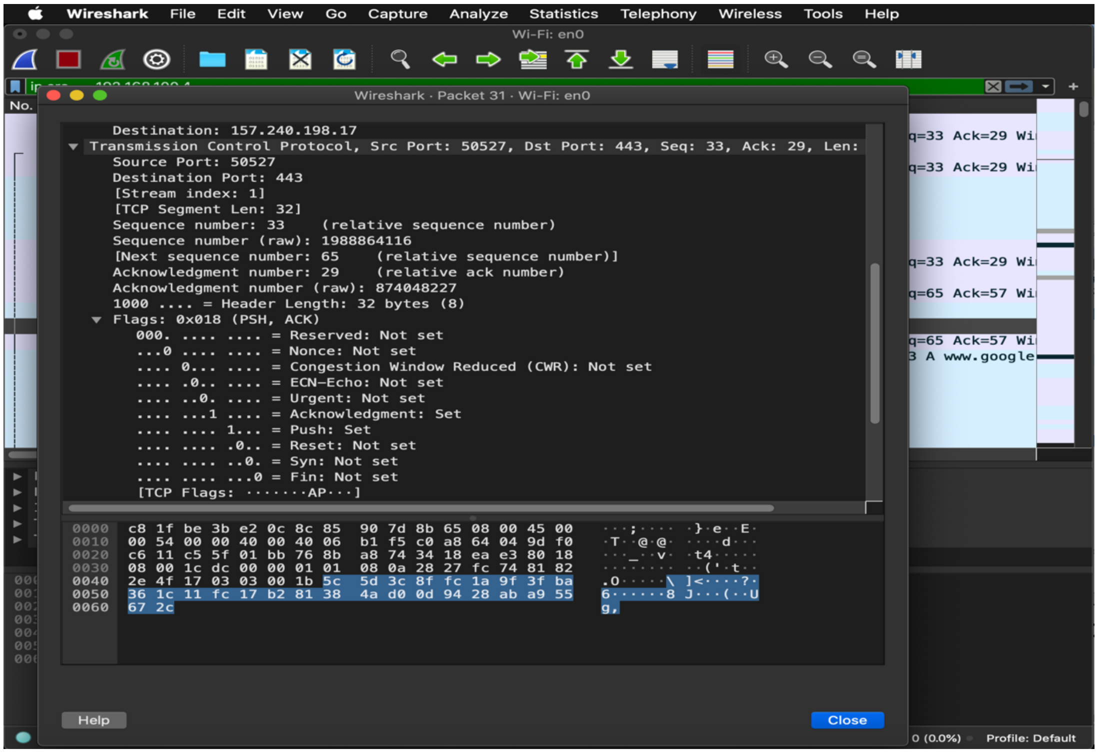
Figure 09: Packet Details Pane (Ethernet Segment)



```
▶ Frame 31: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, ic
▶ Ethernet II, Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3
▼ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 157.240.198.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x0000 (0)
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xb1f5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.100.4
    Destination: 157.240.198.17
▶ Transmission Control Protocol, Src Port: 50527, Dst Port: 443, Seq: 33, Ack: 29, Len: 32
▶ Transport Layer Security

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;··· ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@· ····d···
0020  c6 11 c5 5f 01 bb 76 8b  a8 74 34 18 ea e3 80 18   ···_··v· ·t4·····
0030  08 00 1c dc 00 00 01 01  08 0a 28 27 fc 74 81 82   ········ ··('·t··
0040  2e 4f 17 03 03 00 1b 5c  5d 3c 8f fc 1a 9f 3f ba   .O·····\ ]<····?·
0050  36 1c 11 fc 17 b2 81 38  4a d0 0d 94 28 ab a9 55   6······8 J···(··U
0060  67 2c                                              g,
```

0 (0.0%) · Profile: Default

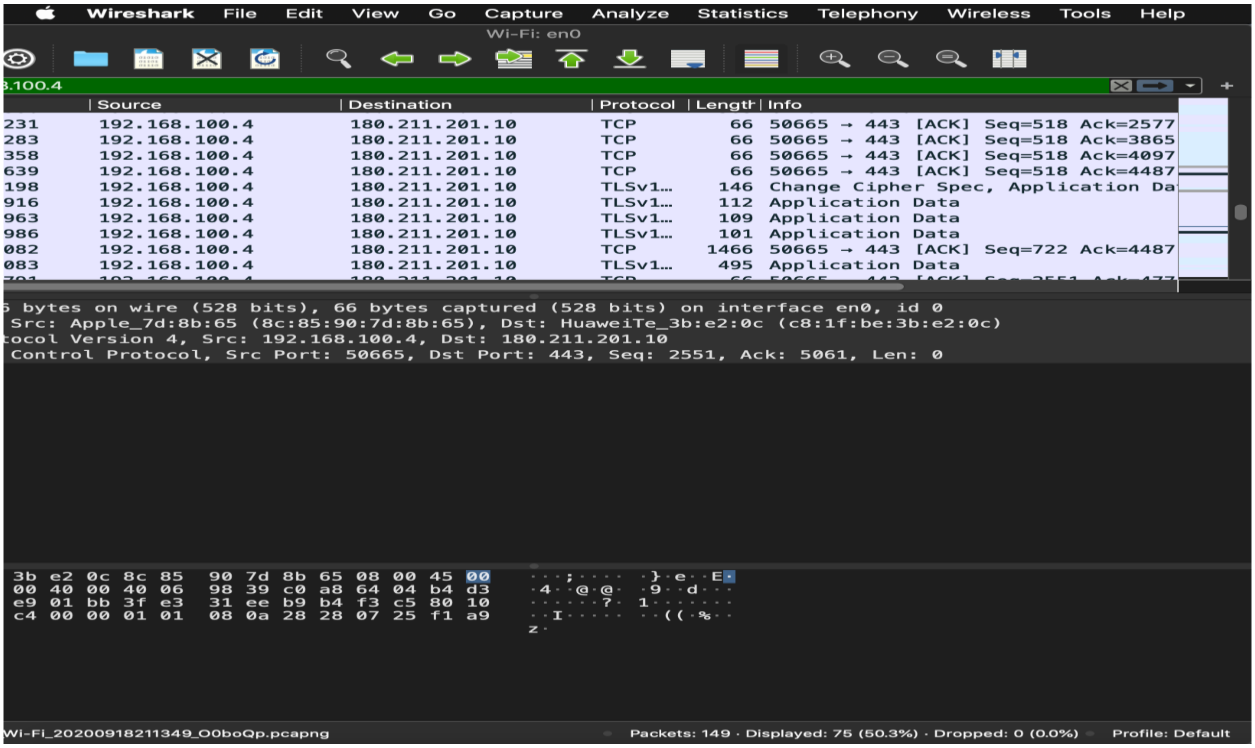
Figure 10: Packet Details Pane(IP segment)



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wi-Fi: en0
Wireshark · Packet 31 · Wi-Fi: en0
Help
Close

```
      Destination: 157.240.198.17
  ▼ Transmission Control Protocol, Src Port: 50527, Dst Port: 443, Seq: 33, Ack: 29, Len:
      Source Port: 50527
      Destination Port: 443
      [Stream index: 1]
      [TCP Segment Len: 32]
      Sequence number: 33    (relative sequence number)
      Sequence number (raw): 1988864116
      [Next sequence number: 65    (relative sequence number)]
      Acknowledgment number: 29    (relative ack number)
      Acknowledgment number (raw): 874048227
      1000 .... = Header Length: 32 bytes (8)
    ▼ Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]

0000  c8 1f be 3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
0010  00 54 00 00 40 00 40 06  b1 f5 c0 a8 64 04 9d f0   ·T··@·@·  ····d···
0020  c6 11 c5 5f 01 bb 76 8b  a8 74 34 18 ea e3 80 18   ···_··v·  ·t4·····
0030  08 00 1c dc 00 00 01 01  08 0a 28 27 fc 74 81 82   ········  ··('·t··
0040  2e 4f 17 03 03 00 1b 5c  5d 3c 8f fc 1a 9f 3f ba   .O·····\ ]<····?·
0050  36 1c 11 fc 17 b2 81 38  4a d0 0d 94 28 ab a9 55   6······8 J···(··U
0060  67 2c                                              g,
```

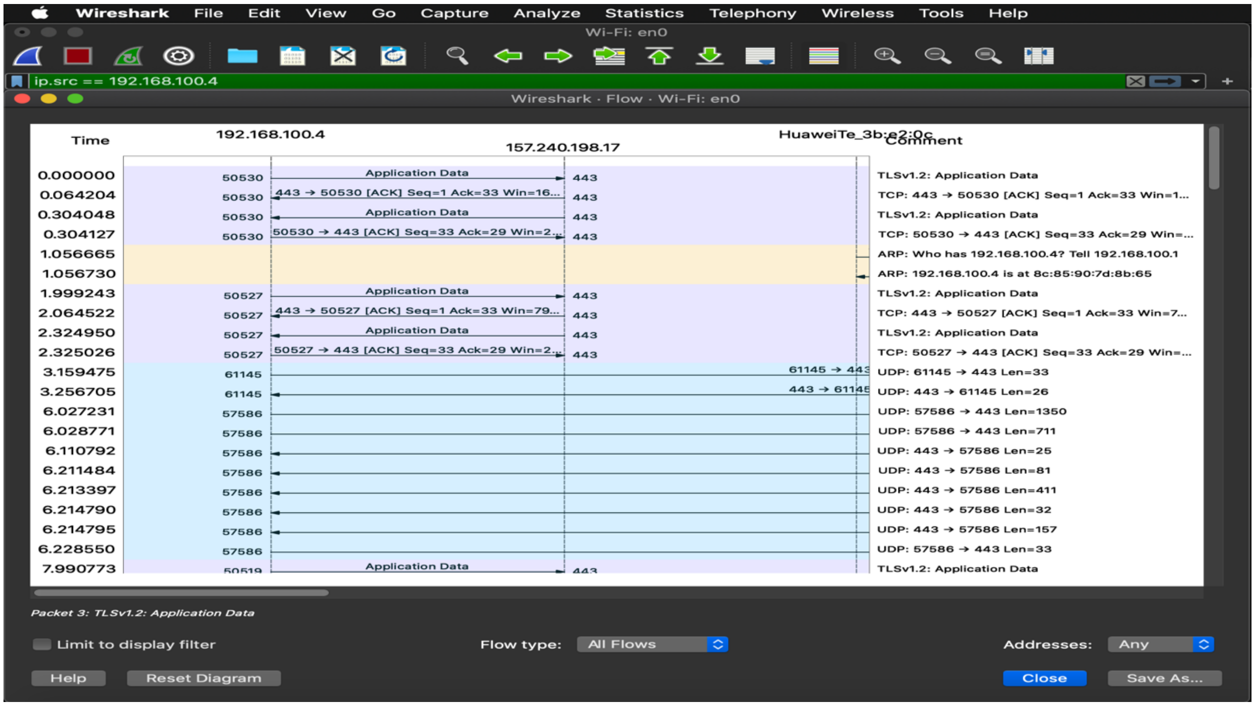
Figure 11: Packet Details Pane (TCP Segment)



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wi-Fi: en0
3.100.4

```
     | Source           | Destination       | Protocol | Length | Info
231    192.168.100.4      180.211.201.10      TCP          66  50665 → 443 [ACK] Seq=518 Ack=2577
283    192.168.100.4      180.211.201.10      TCP          66  50665 → 443 [ACK] Seq=518 Ack=3865
358    192.168.100.4      180.211.201.10      TCP          66  50665 → 443 [ACK] Seq=518 Ack=4097
639    192.168.100.4      180.211.201.10      TCP          66  50665 → 443 [ACK] Seq=518 Ack=4487
198    192.168.100.4      180.211.201.10      TLSv1…      146  Change Cipher Spec, Application Da
916    192.168.100.4      180.211.201.10      TLSv1…      112  Application Data
963    192.168.100.4      180.211.201.10      TLSv1…      109  Application Data
986    192.168.100.4      180.211.201.10      TLSv1…      101  Application Data
082    192.168.100.4      180.211.201.10      TCP        1466  50665 → 443 [ACK] Seq=722 Ack=4487
083    192.168.100.4      180.211.201.10      TLSv1…      495  Application Data

5 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
 Src: Apple_7d:8b:65 (8c:85:90:7d:8b:65), Dst: HuaweiTe_3b:e2:0c (c8:1f:be:3b:e2:0c)
tocol Version 4, Src: 192.168.100.4, Dst: 180.211.201.10
 Control Protocol, Src Port: 50665, Dst Port: 443, Seq: 2551, Ack: 5061, Len: 0

3b e2 0c 8c 85  90 7d 8b 65 08 00 45 00   ···;····  ·}·e··E·
00 40 00 40 06  98 39 c0 a8 64 04 b4 d3   ·4··@·@·  ·9··d···
e9 01 bb 3f e3  31 ee b9 b4 f3 c5 80 10   ·······?·  1·······
c4 00 00 01 01  08 0a 28 28 07 25 f1 a9   ··I·····  ··((·%··
                                          z·

Wi-Fi_20200918211349_O0boQp.pcapng   Packets: 149 · Displayed: 75 (50.3%) · Dropped: 0 (0.0%)   Profile: Default
```

Figure 12: Packet Byte Pane



ip.src == 192.168.100.4

```
Time        192.168.100.4                                              HuaweiTe_3b:e2:0c  Comment
                               157.240.198.17
0.000000    50530        Application Data                443              TLSv1.2: Application Data
0.064204    50530  443 → 50530 [ACK] Seq=1 Ack=33 Win=16...  443          TCP: 443 → 50530 [ACK] Seq=1 Ack=33 Win=1...
0.304048    50530        Application Data                443              TLSv1.2: Application Data
0.304127    50530  50530 → 443 [ACK] Seq=33 Ack=29 Win=2...  443          TCP: 50530 → 443 [ACK] Seq=33 Ack=29 Win=...
1.056665                                                                  ARP: Who has 192.168.100.4? Tell 192.168.100.1
1.056730                                                                  ARP: 192.168.100.4 is at 8c:85:90:7d:8b:65
1.999243    50527        Application Data                443              TLSv1.2: Application Data
2.064522    50527  443 → 50527 [ACK] Seq=1 Ack=33 Win=79...  443          TCP: 443 → 50527 [ACK] Seq=1 Ack=33 Win=7...
2.324950    50527        Application Data                443              TLSv1.2: Application Data
2.325026    50527  50527 → 443 [ACK] Seq=33 Ack=29 Win=2...  443          TCP: 50527 → 443 [ACK] Seq=33 Ack=29 Win=...
3.159475    61145                                   61145 → 443           UDP: 61145 → 443 Len=33
3.256705    61145                                   443 → 61145           UDP: 443 → 61145 Len=26
6.027231    57586                                                         UDP: 57586 → 443 Len=1350
6.028771    57586                                                         UDP: 57586 → 443 Len=711
6.110792    57586                                                         UDP: 443 → 57586 Len=25
6.211484    57586                                                         UDP: 443 → 57586 Len=81
6.213397    57586                                                         UDP: 443 → 57586 Len=411
6.214790    57586                                                         UDP: 443 → 57586 Len=32
6.214795    57586                                                         UDP: 443 → 57586 Len=157
6.228550    57586                                                         UDP: 57586 → 443 Len=33
7.990773    50519        Application Data                443              TLSv1.2: Application Data
```

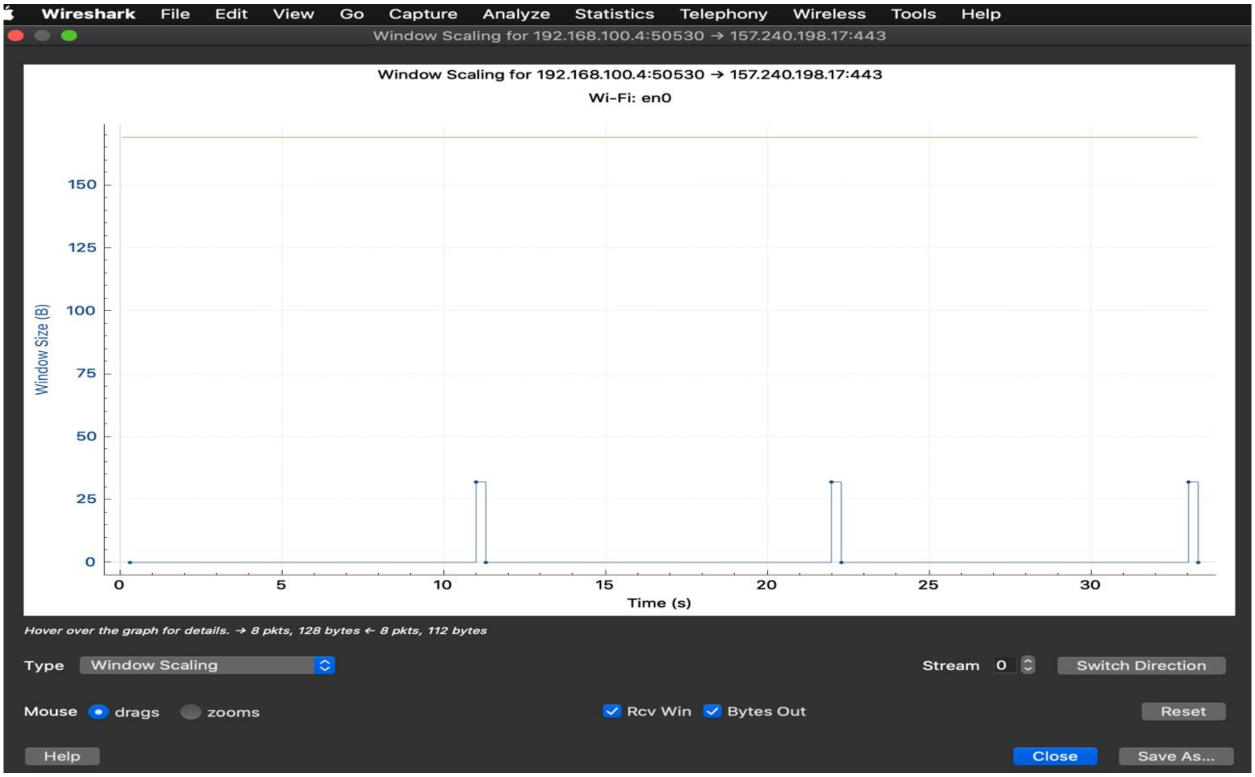
*Packet 3: TLSv1.2: Application Data*

□ Limit to display filter

Flow type: All Flows

Addresses: Any

## Figure 13: Statistics- Flow Graph(All Flows)



*Hover over the graph for details. → 8 pkts, 128 bytes ← 8 pkts, 112 bytes*

Type Window Scaling

Stream 0

Mouse ● drags ○ zooms

☑ Rcv Win ☑ Bytes Out

## Figure 13: Statistics- Flow Graph(TCP Window Scalling)

## Conclusion:

Wireshark is a popular network analyses that uses pcap library to capture network packets at different layers of the OSI model.

Network administrators use it to troubleshoot network problems. Network security engineers use it to examine security problems.QA engineers use it to verify network applications. Developers use it to debug protocol implementations.