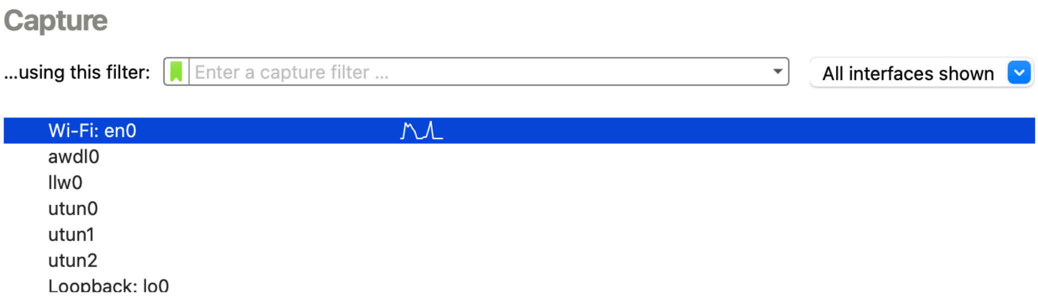
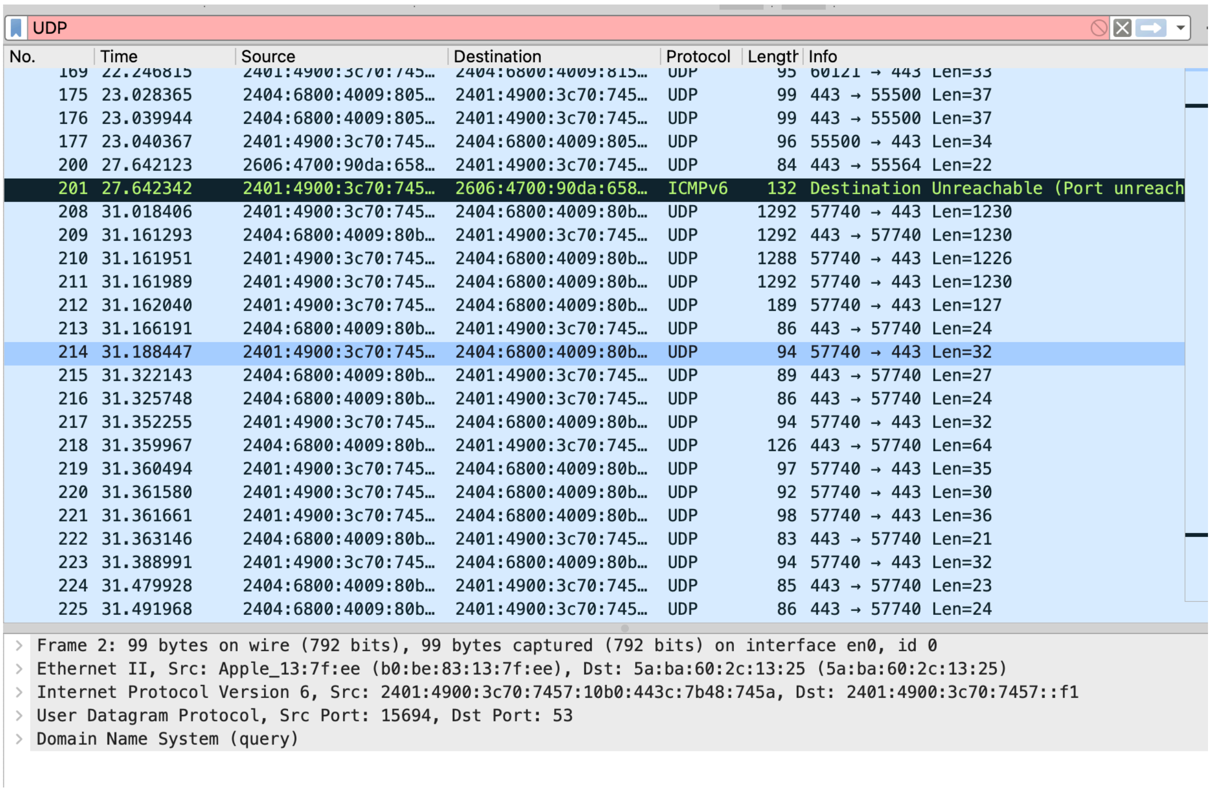
Step 1: Select Wifi/Ethernet



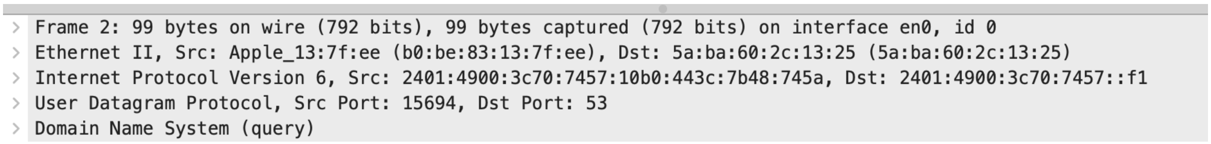
```
Wi-Fi: en0
awdl0
llw0
utun0
utun1
utun2
Loopback: lo0
```

Step 2: filter UDP packets



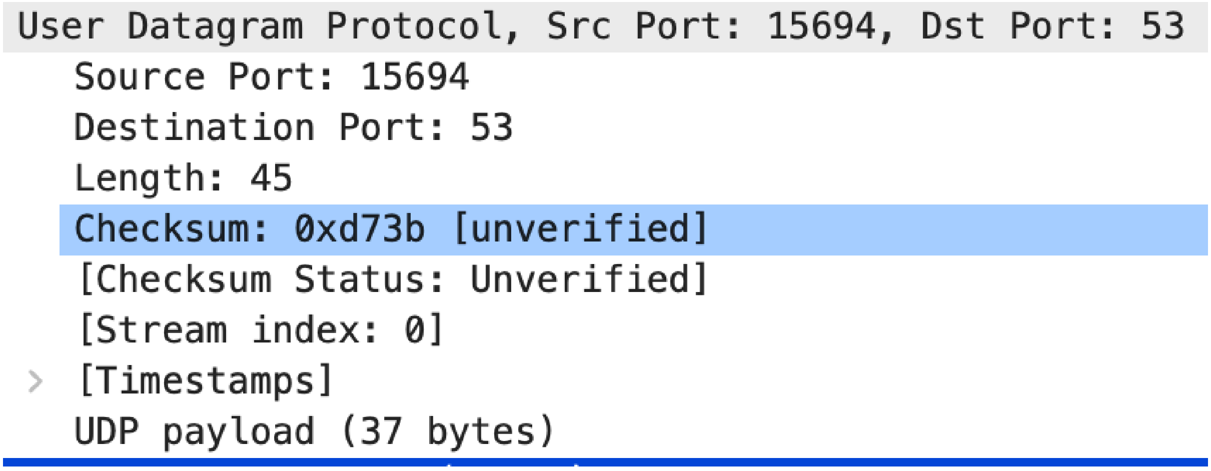
```
No.   Time        Source                 Destination            Protocol  Length Info
 169  22.246815   2401:4900:3c70:745…    2404:6800:4009:815…    UDP         95  60121 → 443 Len=33
 175  23.028365   2404:6800:4009:805…    2401:4900:3c70:745…    UDP         99  443 → 55500 Len=37
 176  23.039944   2404:6800:4009:805…    2401:4900:3c70:745…    UDP         99  443 → 55500 Len=37
 177  23.040367   2401:4900:3c70:745…    2404:6800:4009:805…    UDP         96  55500 → 443 Len=34
 200  27.642123   2606:4700:90da:658…    2401:4900:3c70:745…    UDP         84  443 → 55564 Len=22
 201  27.642342   2401:4900:3c70:745…    2606:4700:90da:658…    ICMPv6     132  Destination Unreachable (Port unreach
 208  31.018406   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP       1292  57740 → 443 Len=1230
 209  31.161293   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP       1292  443 → 57740 Len=1230
 210  31.161951   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP       1288  57740 → 443 Len=1226
 211  31.161989   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP       1292  57740 → 443 Len=1230
 212  31.162040   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP        189  57740 → 443 Len=127
 213  31.166191   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         86  443 → 57740 Len=24
 214  31.188447   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         94  57740 → 443 Len=32
 215  31.322143   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         89  443 → 57740 Len=27
 216  31.325748   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         86  443 → 57740 Len=24
 217  31.352255   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         94  57740 → 443 Len=32
 218  31.359967   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP        126  443 → 57740 Len=64
 219  31.360494   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         97  57740 → 443 Len=35
 220  31.361580   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         92  57740 → 443 Len=30
 221  31.361661   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         98  57740 → 443 Len=36
 222  31.363146   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         83  443 → 57740 Len=21
 223  31.388991   2401:4900:3c70:745…    2404:6800:4009:80b…    UDP         94  57740 → 443 Len=32
 224  31.479928   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         85  443 → 57740 Len=23
 225  31.491968   2404:6800:4009:80b…    2401:4900:3c70:745…    UDP         86  443 → 57740 Len=24

> Frame 2: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:7f:ee (b0:be:83:13:7f:ee), Dst: 5a:ba:60:2c:13:25 (5a:ba:60:2c:13:25)
> Internet Protocol Version 6, Src: 2401:4900:3c70:7457:10b0:443c:7b48:745a, Dst: 2401:4900:3c70:7457::f1
> User Datagram Protocol, Src Port: 15694, Dst Port: 53
> Domain Name System (query)
```

Step 3: Source Port ,Destination Port,Checksum and length of specific packet:



```
> Frame 2: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:7f:ee (b0:be:83:13:7f:ee), Dst: 5a:ba:60:2c:13:25 (5a:ba:60:2c:13:25)
> Internet Protocol Version 6, Src: 2401:4900:3c70:7457:10b0:443c:7b48:745a, Dst: 2401:4900:3c70:7457::f1
> User Datagram Protocol, Src Port: 15694, Dst Port: 53
> Domain Name System (query)
```

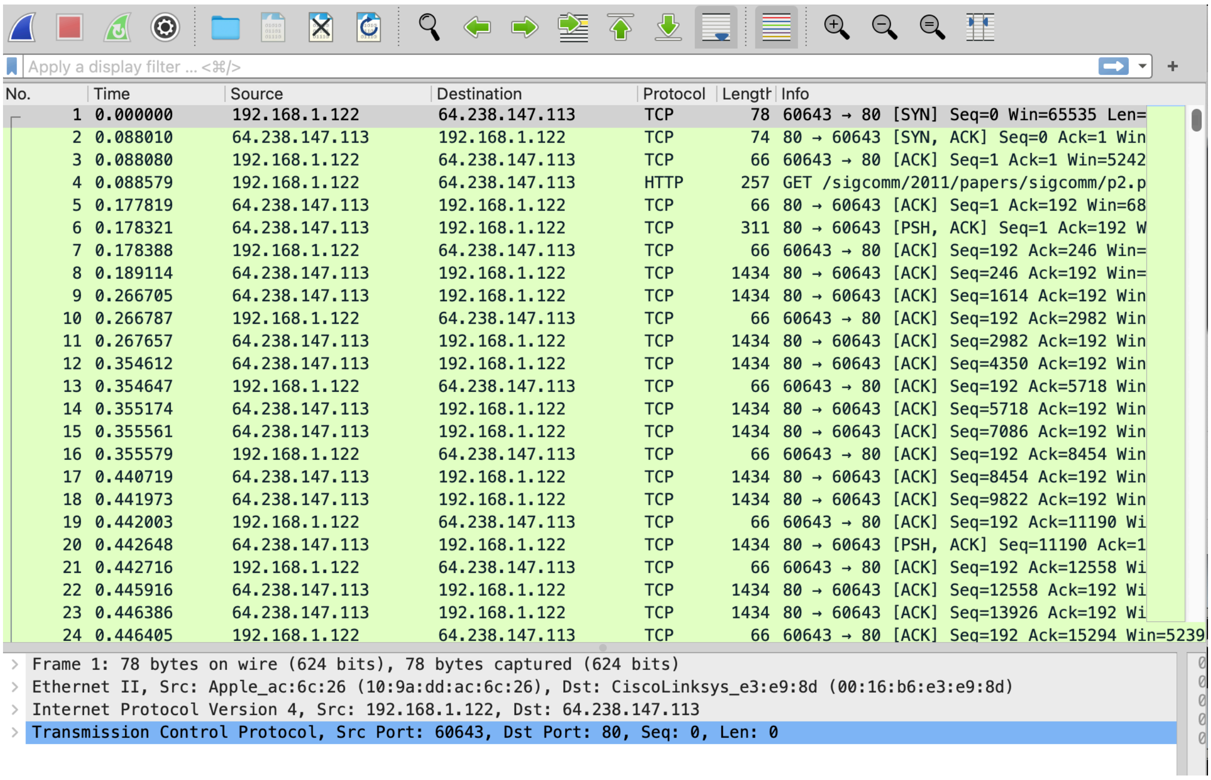
Length and Checksum:



```
User Datagram Protocol, Src Port: 15694, Dst Port: 53
    Source Port: 15694
    Destination Port: 53
    Length: 45
    Checksum: 0xd73b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (37 bytes)
```

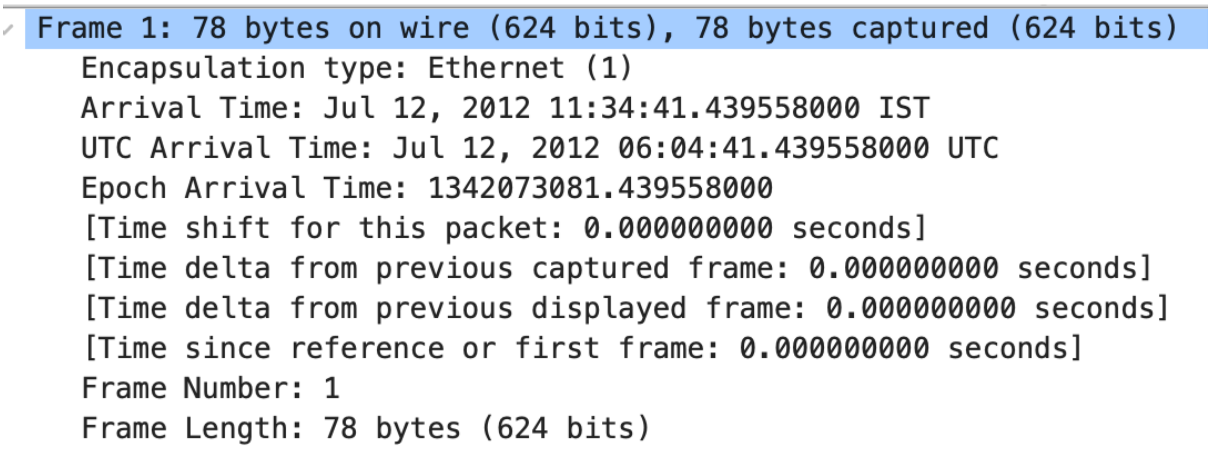
Lab Exercise – TCP

Step 1: Open the Trace:



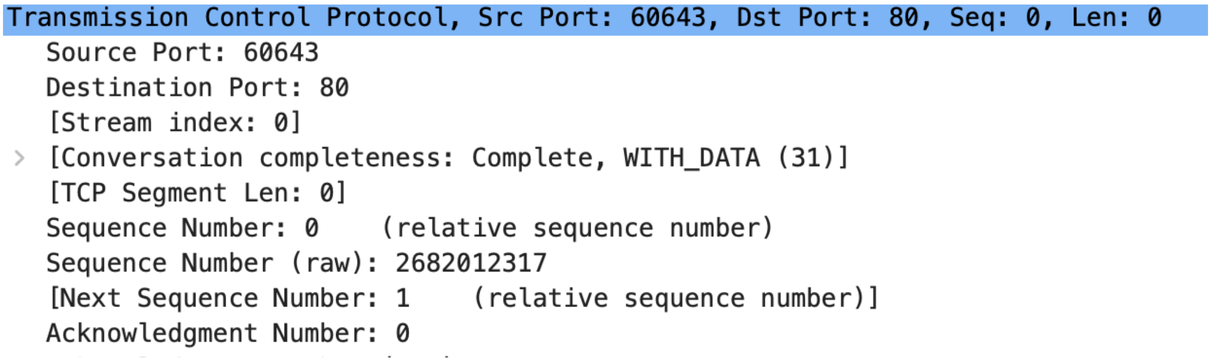
```
No.  Time      Source          Destination     Protocol Length Info
  1 0.000000   192.168.1.122   64.238.147.113  TCP        78 60643 → 80 [SYN] Seq=0 Win=65535 Len=
  2 0.088010   64.238.147.113  192.168.1.122   TCP        74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win
  3 0.088080   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=1 Ack=1 Win=5242
  4 0.088579   192.168.1.122   64.238.147.113  HTTP      257 GET /sigcomm/2011/papers/sigcomm/p2.p
  5 0.177819   64.238.147.113  192.168.1.122   TCP        66 80 → 60643 [ACK] Seq=1 Ack=192 Win=68
  6 0.178321   64.238.147.113  192.168.1.122   TCP       311 80 → 60643 [PSH, ACK] Seq=1 Ack=192 W
  7 0.178388   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=246 Win=
  8 0.189114   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=246 Ack=192 Win=
  9 0.266705   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=1614 Ack=192 Win
 10 0.266787   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=2982 Win
 11 0.267657   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=2982 Ack=192 Win
 12 0.354612   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=4350 Ack=192 Win
 13 0.354647   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=5718 Win
 14 0.355174   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=5718 Ack=192 Win
 15 0.355561   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=7086 Ack=192 Win
 16 0.355579   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=8454 Win
 17 0.440719   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=8454 Ack=192 Win
 18 0.441973   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=9822 Ack=192 Win
 19 0.442003   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=11190 Wi
 20 0.442648   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [PSH, ACK] Seq=11190 Ack=1
 21 0.442716   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=12558 Wi
 22 0.445916   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=12558 Ack=192 Wi
 23 0.446386   64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=13926 Ack=192 Wi
 24 0.446405   192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=15294 Win=5239

> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: CiscoLinksys_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
> Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 0, Len: 0
```

Frame Length:



```
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 12, 2012 11:34:41.439558000 IST
    UTC Arrival Time: Jul 12, 2012 06:04:41.439558000 UTC
    Epoch Arrival Time: 1342073081.439558000
    [Time shift for this packet: 0.000000000 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: 78 bytes (624 bits)
```

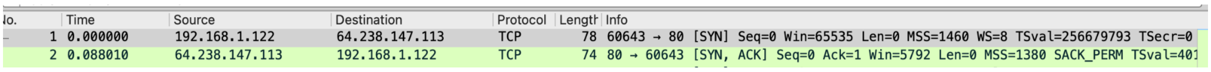
TCP Port:



```
Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2682012317
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
```

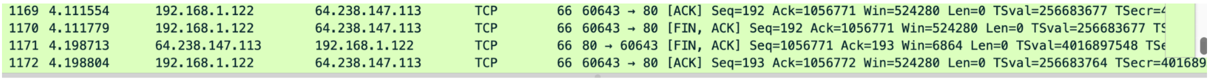
Step 2: ThreeWay Handshake:

1.Sending SYN and Receiving ACK for starting the connection:



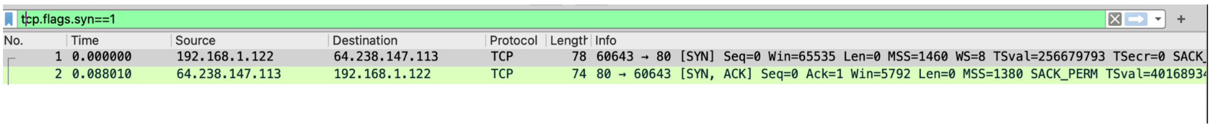
```
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    192.168.1.122    64.238.147.113   TCP       78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=256679793 TSecr=0
    2 0.088010    64.238.147.113   192.168.1.122    TCP       74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM TSval=401
```

2.Closing the Connection with FYN and Acknowledging it:



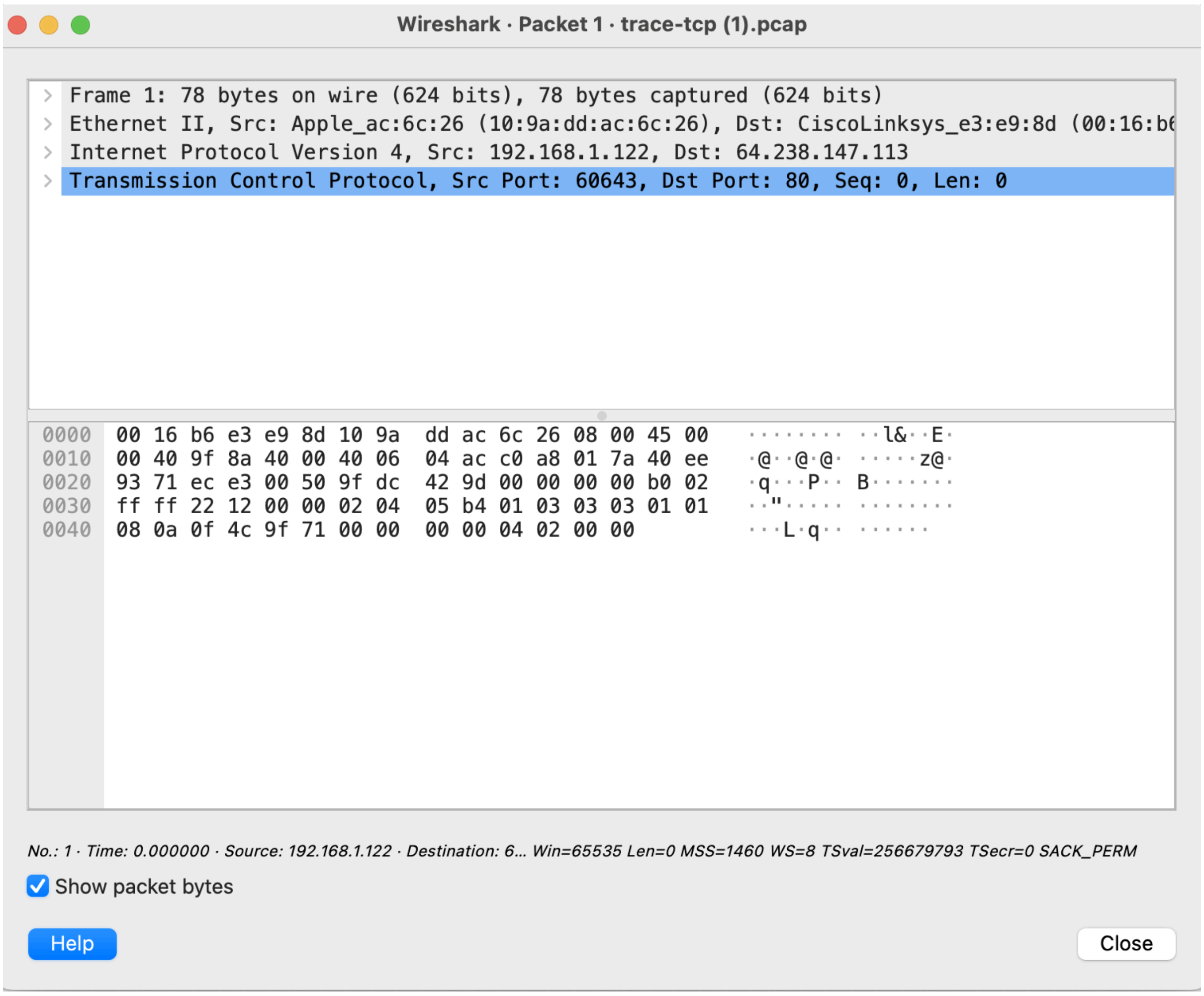
```
1169 4.111554    192.168.1.122    64.238.147.113   TCP    66 60643 → 80 [ACK] Seq=192 Ack=1056771 Win=524280 Len=0 TSval=256683677 TSecr=4
1170 4.111779    192.168.1.122    64.238.147.113   TCP    66 60643 → 80 [FIN, ACK] Seq=192 Ack=1056771 Win=524280 Len=0 TSval=256683677 TS
1171 4.198713    64.238.147.113   192.168.1.122    TCP    66 80 → 60643 [FIN, ACK] Seq=1056771 Ack=193 Win=6864 Len=0 TSval=4016897548 TSe
1172 4.198804    192.168.1.122    64.238.147.113   TCP    66 60643 → 80 [ACK] Seq=193 Ack=1056772 Win=524280 Len=0 TSval=256683764 TSecr=401689
```

Step 3: We can search syn packets with this command as well: tcp.flags.syn==1



```
tcp.flags.syn==1
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    192.168.1.122    64.238.147.113   TCP       78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=256679793 TSecr=0 SACK_
    2 0.088010    64.238.147.113   192.168.1.122    TCP       74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM TSval=40168934
```

Step 4: On clicking on syn request , we get:



Wireshark · Packet 1 · trace-tcp (1).pcap

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: CiscoLinksys_e3:e9:8d (00:16:b6
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
> Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 0, Len: 0
```

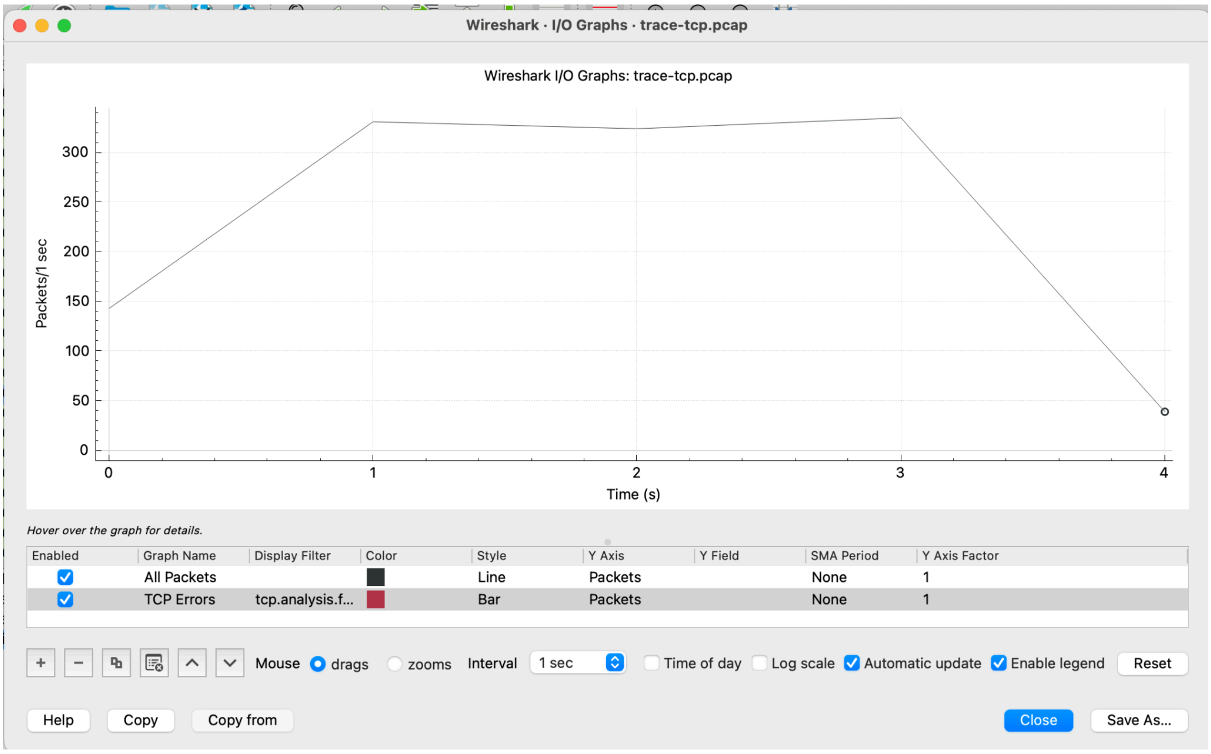
```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ········ ··l&··E·
0010  00 40 9f 8a 40 00 40 06  04 ac c0 a8 01 7a 40 ee   ·@··@·@· ·····z@·
0020  93 71 ec e3 00 50 9f dc  42 9d 00 00 00 00 b0 02   ·q···P·· B·······
0030  ff ff 22 12 00 00 02 04  05 b4 01 03 03 03 01 01   ··"····· ········
0040  08 0a 0f 4c 9f 71 00 00  00 00 04 02 00 00        ···L·q·· ······
```

No.: 1 · Time: 0.000000 · Source: 192.168.1.122 · Destination: 6… Win=65535 Len=0 MSS=1460 WS=8 TSval=256679793 TSecr=0 SACK_PERM

☑ Show packet bytes

TCP Data Transfer:

IO Graph :



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Packets		None	1
☑	TCP Errors	tcp.analysis.f...	🟥	Bar	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic update ☑ Enable legend