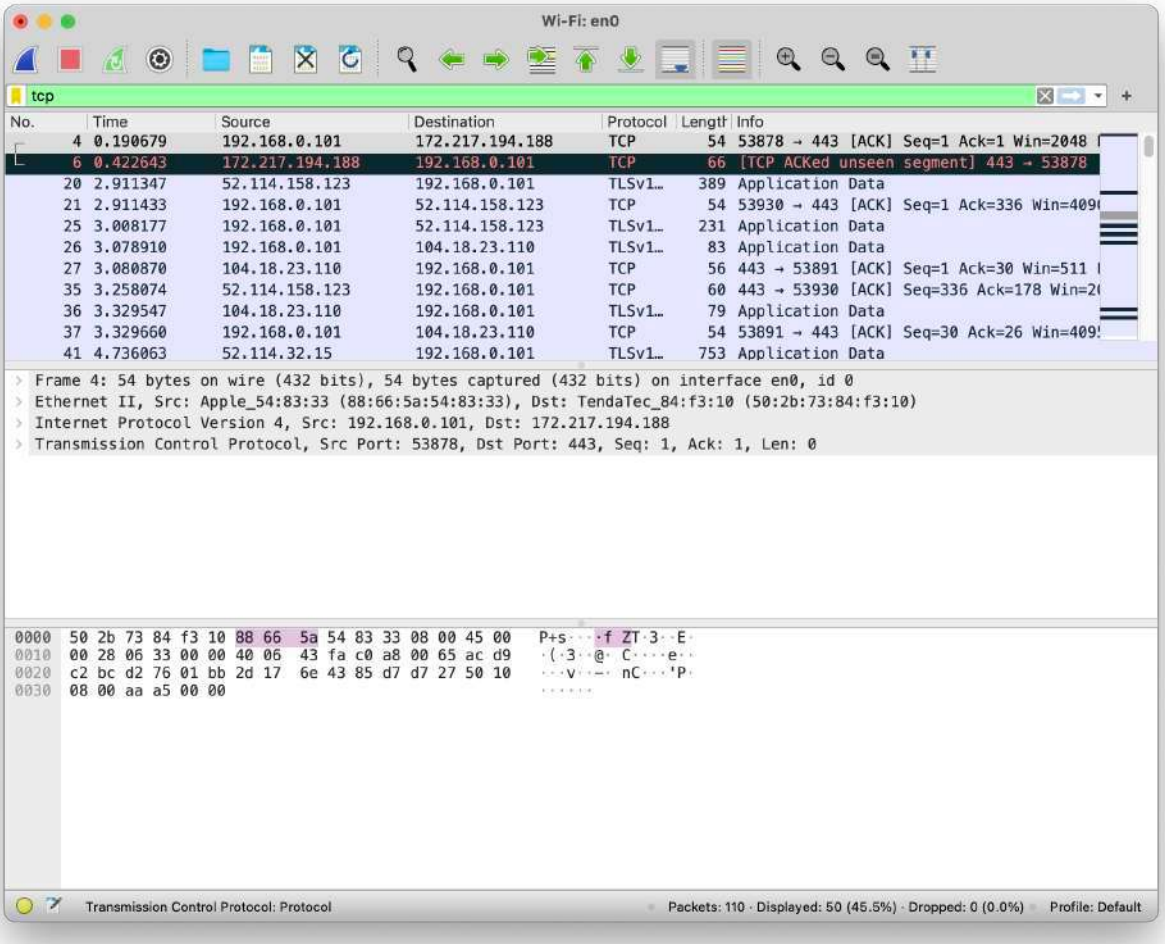
ISAA LAB ASSIGNMENT - 5

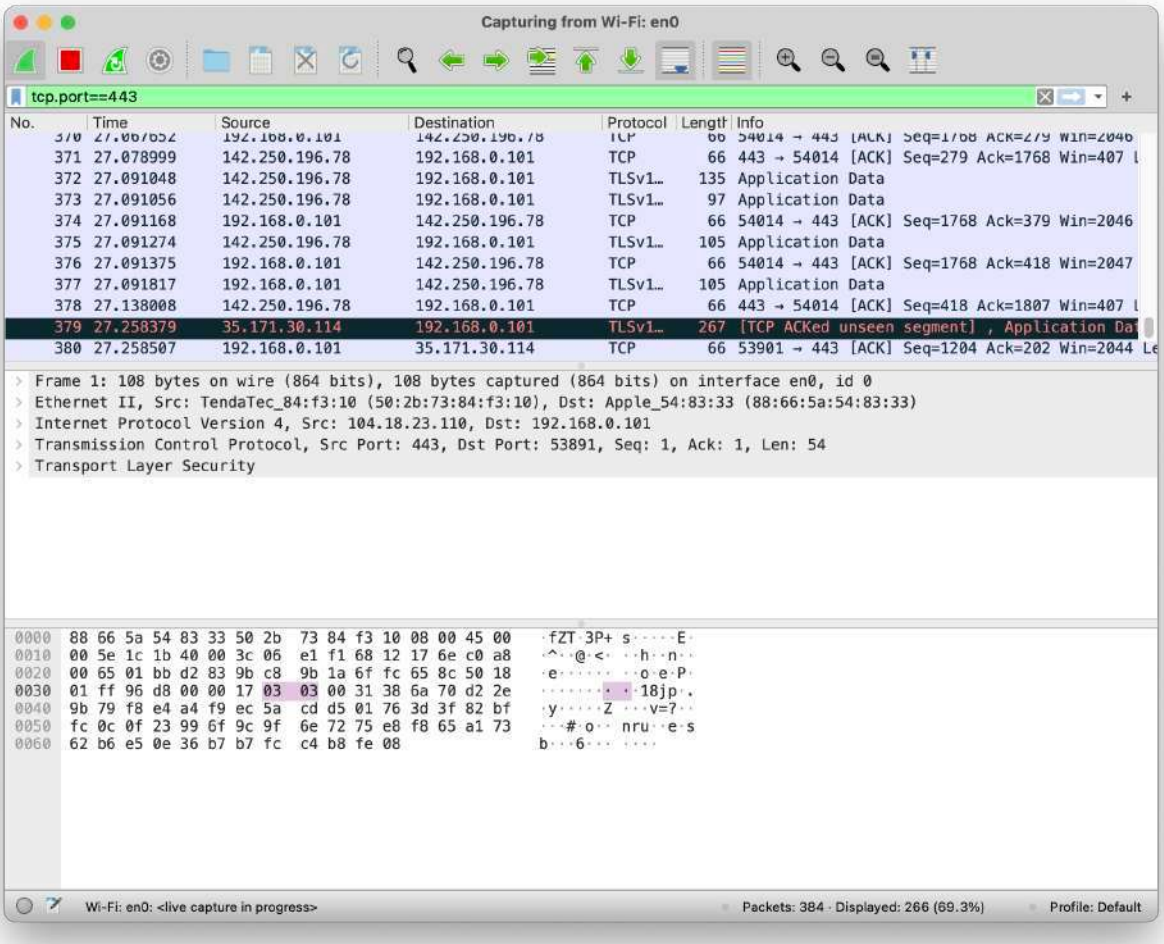
NAME	APOORVA REDDY BAGEPALLI
REGISTRATION NUMBER	19BCE2196

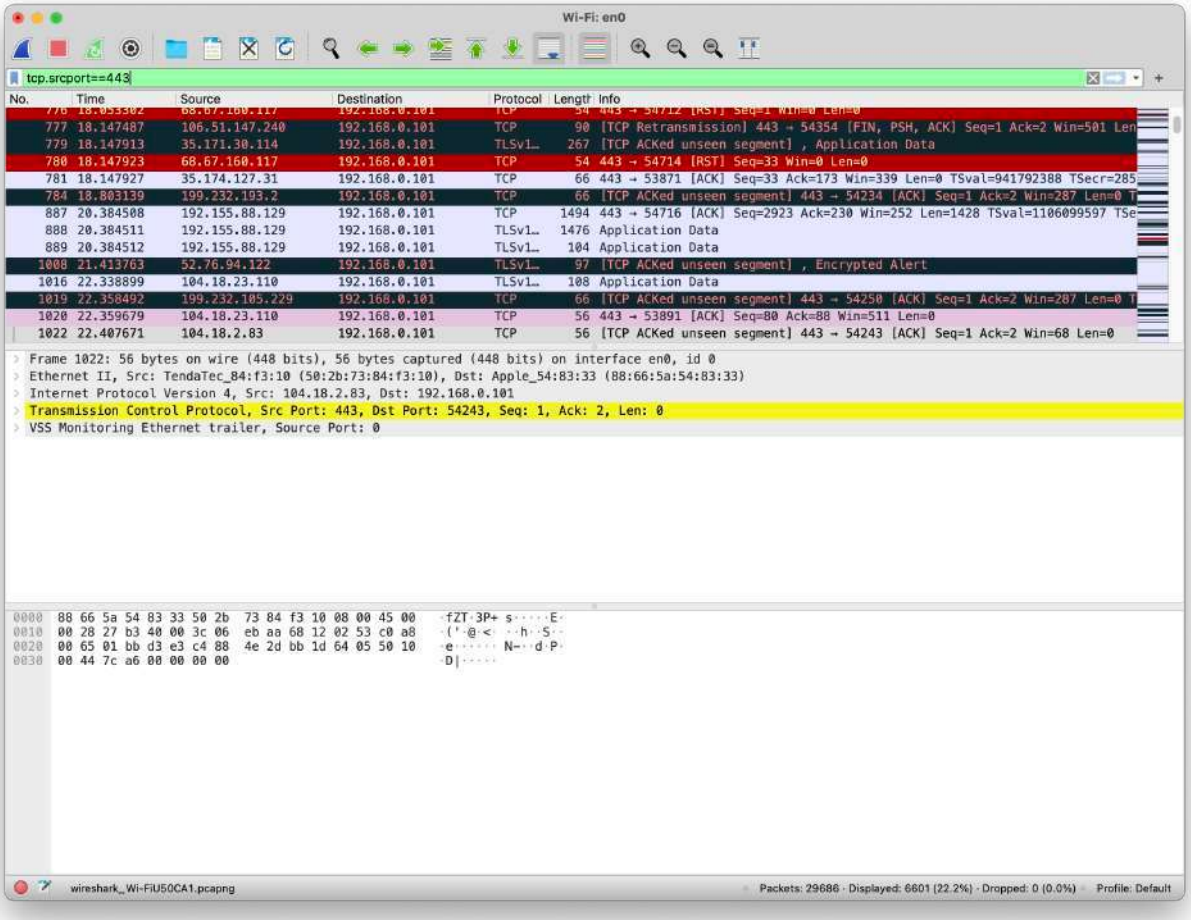
Network Packets Sniffing using WireShark

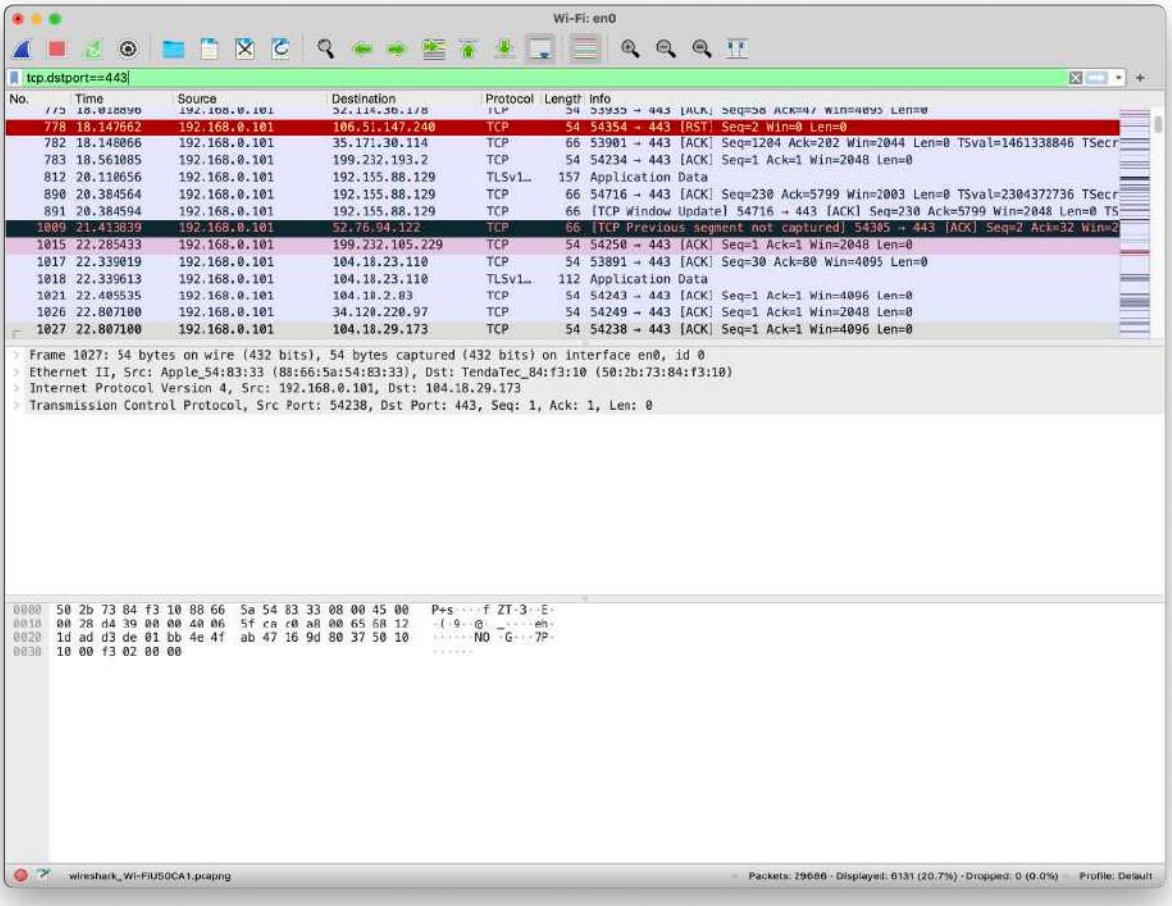
1. Filtering the packets by specifying a protocol
   - TLSv1: This protocol depends on TCP.



2. Filter the packets based on the port
   - tcp.port == 443
   - Tcp.dstport==443
   - tcp.srcport==443

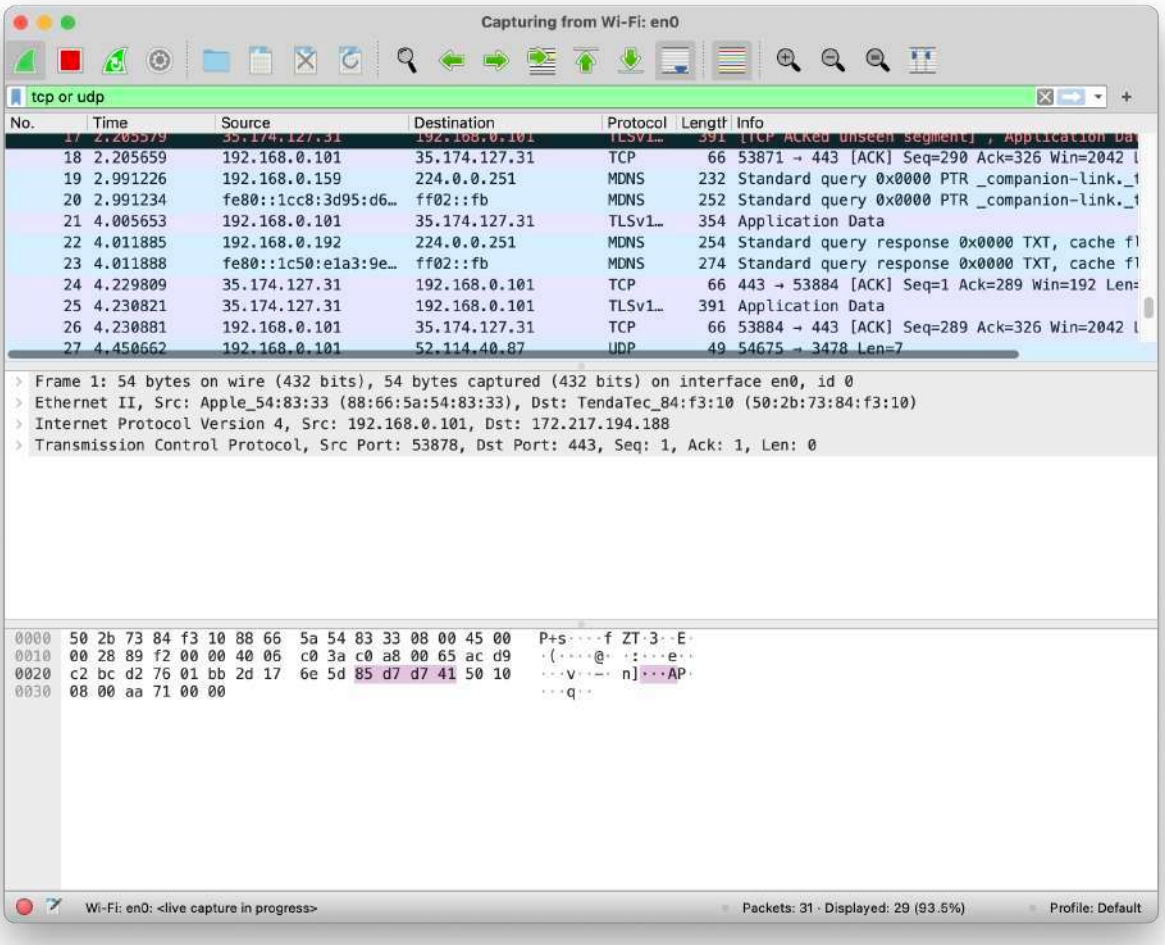


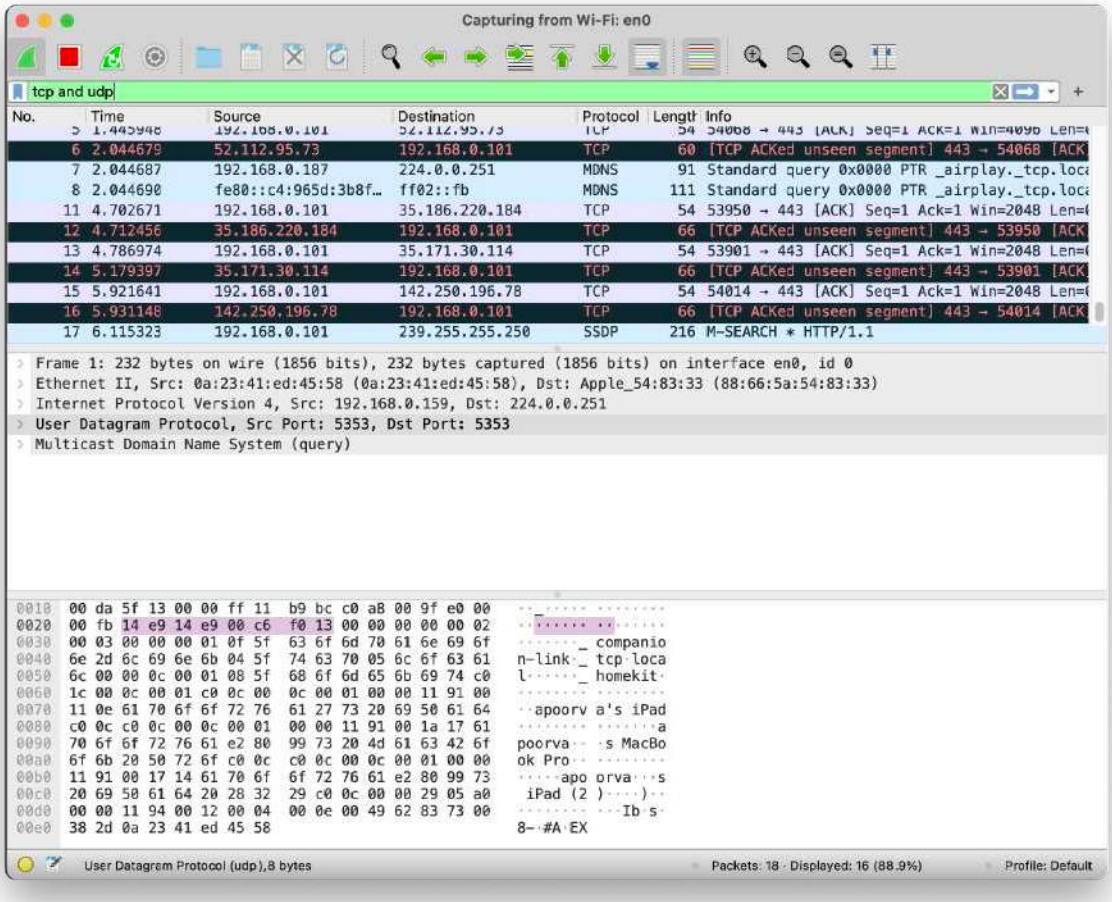

Wi-Fi: en0
tcp.srcport==443
No. Time Source Destination Protocol Length Info
776 18.053302 68.67.160.117 192.168.0.101 TCP 54 443 → 54712 [RST] Seq=1 Win=0 Len=0
777 18.147487 106.51.147.240 192.168.0.101 TCP 90 [TCP Retransmission] 443 → 54354 [FIN, PSH, ACK] Seq=1 Ack=2 Win=501 Len
779 18.147913 35.171.30.114 192.168.0.101 TLSv1... 267 [TCP ACKed unseen segment] , Application Data
780 18.147923 68.67.160.117 192.168.0.101 TCP 54 443 → 54714 [RST] Seq=33 Win=0 Len=0
781 18.147927 35.174.127.31 192.168.0.101 TCP 66 443 → 53871 [ACK] Seq=33 Ack=173 Win=339 Len=0 TSval=941792388 TSecr=285
784 18.803139 199.232.193.2 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 54234 [ACK] Seq=1 Ack=2 Win=287 Len=0 T
887 20.384508 192.155.88.129 192.168.0.101 TCP 1494 443 → 54716 [ACK] Seq=2923 Ack=230 Win=252 Len=1428 TSval=1106099597 TSe
888 20.384511 192.155.88.129 192.168.0.101 TLSv1... 1476 Application Data
889 20.384512 192.155.88.129 192.168.0.101 TLSv1... 104 Application Data
1008 21.413763 52.76.94.122 192.168.0.101 TLSv1... 97 [TCP ACKed unseen segment] , Encrypted Alert
1016 22.338899 104.18.23.110 192.168.0.101 TLSv1... 108 Application Data
1019 22.358492 199.232.105.229 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 54250 [ACK] Seq=1 Ack=2 Win=287 Len=0 T
1020 22.359679 104.18.23.110 192.168.0.101 TCP 56 443 → 53891 [ACK] Seq=80 Ack=88 Win=511 Len=0
1022 22.407671 104.18.2.83 192.168.0.101 TCP 56 [TCP ACKed unseen segment] 443 → 54243 [ACK] Seq=1 Ack=2 Win=68 Len=0
Frame 1022: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface en0, id 0
Ethernet II, Src: TendaTec_84:f3:10 (50:2b:73:84:f3:10), Dst: Apple_54:83:33 (88:66:5a:54:83:33)
Internet Protocol Version 4, Src: 104.18.2.83, Dst: 192.168.0.101
Transmission Control Protocol, Src Port: 443, Dst Port: 54243, Seq: 1, Ack: 2, Len: 0
VSS Monitoring Ethernet trailer, Source Port: 0
0000 88 66 5a 54 83 33 50 2b 73 84 f3 10 08 00 45 00 ·fZT·3P+ s·····E·
0010 00 28 27 b3 40 00 3c 06 eb aa 68 12 02 53 c0 a8 ·('·@·<· ··h··S··
0020 00 65 01 bb d3 e3 c4 88 4e 2d bb 1d 64 05 50 10 ·e····· N-··d·P·
0030 00 44 7c a6 00 00 00 00 ·D|·····
wireshark_Wi-FiU50CA1.pcapng
Packets: 29686 · Displayed: 6601 (22.2%) · Dropped: 0 (0.0%)
Profile: Default

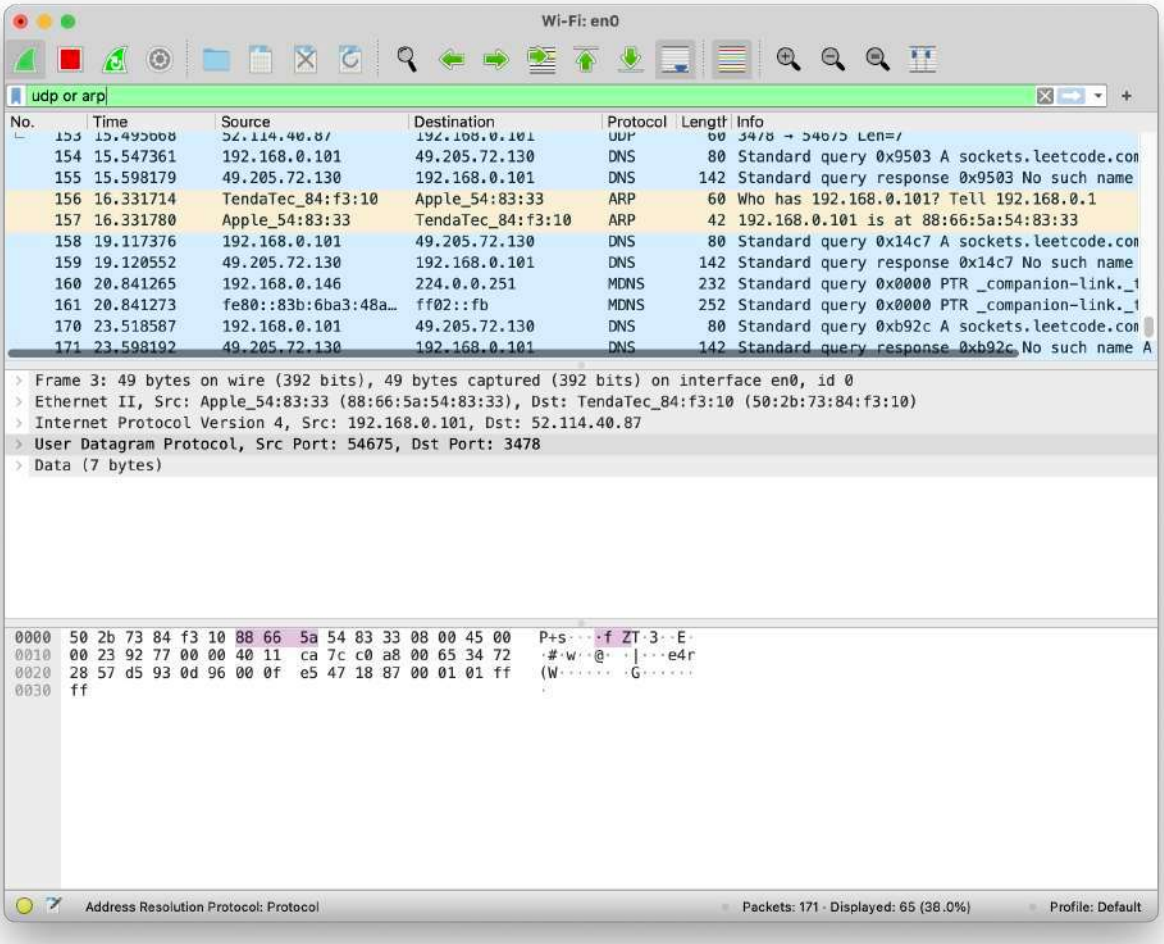

Wi-Fi: en0
tcp.dstport==443
No. Time Source Destination Protocol Length Info
778 18.147662 192.168.0.101 106.51.147.240 TCP 54 54354 → 443 [RST] Seq=2 Win=0 Len=0
782 18.148066 192.168.0.101 35.171.30.114 TCP 66 53901 → 443 [ACK] Seq=1204 Ack=202 Win=2044 Len=0 TSval=1461338846 TSecr
783 18.561085 192.168.0.101 199.232.193.2 TCP 54 54234 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
812 20.110656 192.168.0.101 192.155.88.129 TLSv1... 157 Application Data
890 20.384564 192.168.0.101 192.155.88.129 TCP 66 54716 → 443 [ACK] Seq=230 Ack=5799 Win=2003 Len=0 TSval=2304372736 TSecr
891 20.384594 192.168.0.101 192.155.88.129 TCP 66 [TCP Window Update] 54716 → 443 [ACK] Seq=230 Ack=5799 Win=2048 Len=0 TS
1009 21.413839 192.168.0.101 52.76.94.122 TCP 66 [TCP Previous segment not captured] 54305 → 443 [ACK] Seq=2 Ack=32 Win=2
1015 22.285433 192.168.0.101 199.232.105.229 TCP 54 54250 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
1017 22.339019 192.168.0.101 104.18.23.110 TCP 54 53891 → 443 [ACK] Seq=30 Ack=80 Win=4095 Len=0
1018 22.339613 192.168.0.101 104.18.23.110 TLSv1... 112 Application Data
1021 22.405535 192.168.0.101 104.18.2.83 TCP 54 54243 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
1026 22.807100 192.168.0.101 34.120.220.97 TCP 54 54249 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
1027 22.807100 192.168.0.101 104.18.29.173 TCP 54 54238 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
Frame 1027: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 104.18.29.173
Transmission Control Protocol, Src Port: 54238, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00 P+s····f ZT·3··E·
0010 00 28 d4 39 00 00 40 06 5f ca c0 a8 00 65 68 12 ·(·9··@· _····eh·
0020 1d ad d3 de 01 bb 4e 4f ab 47 16 9d 80 37 50 10 ·····NO ·G···7P·
0030 10 00 f3 02 00 00 ·····
wireshark_Wi-FiU50CA1.pcapng
Packets: 29686 · Displayed: 6131 (20.7%) · Dropped: 0 (0.0%)
Profile: Default

3. Filter results based on **or/and**

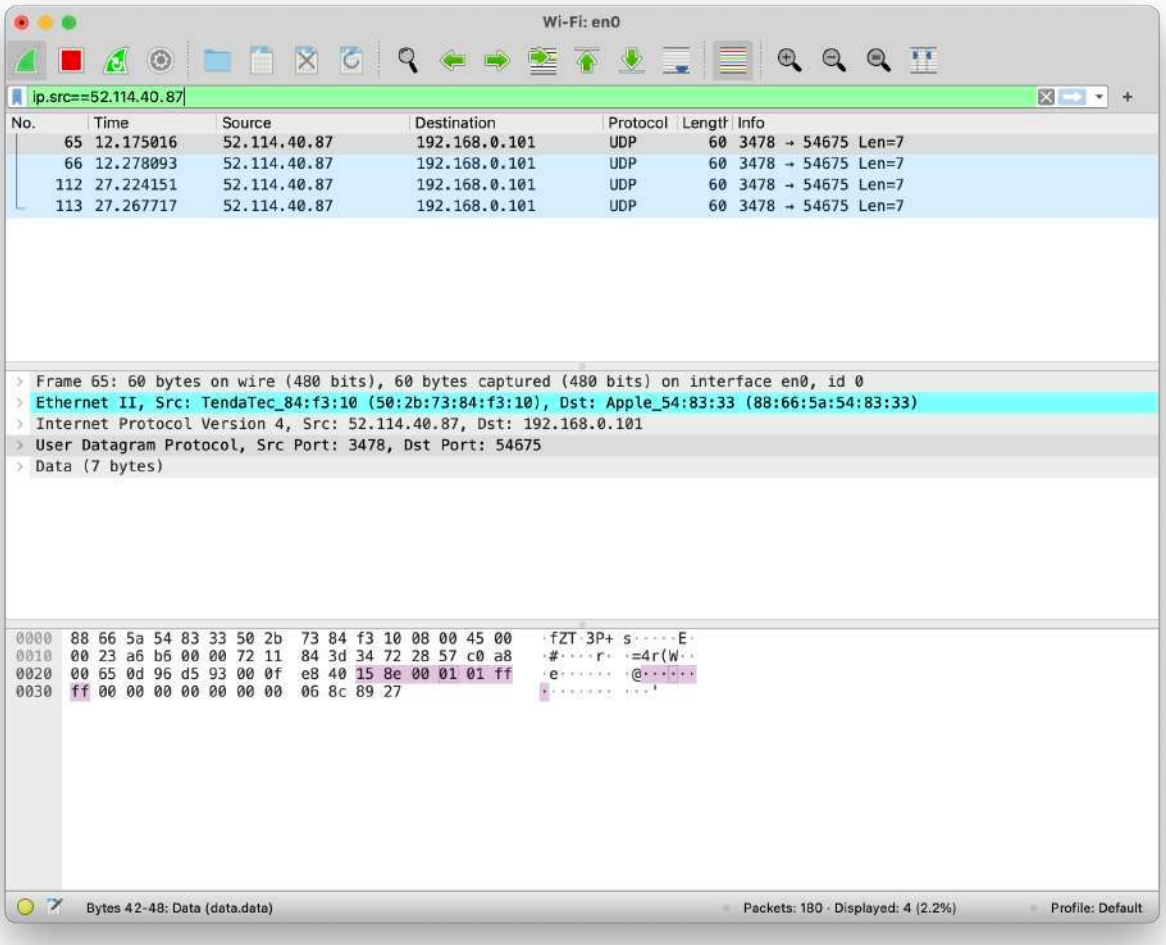
- Or : Independent
- And : Dependent
- Tcp or udp / tcp and udp / udp or arp

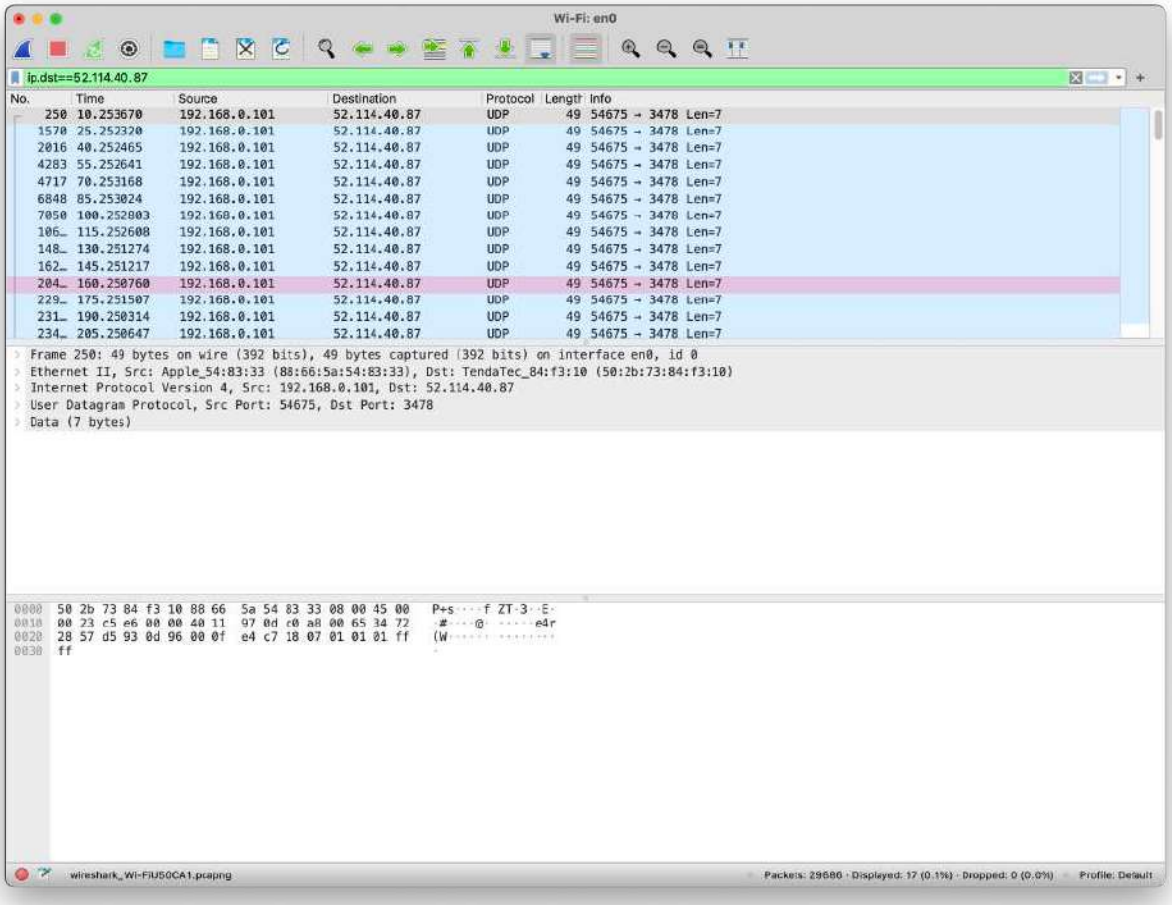



Capturing from Wi-Fi: en0
tcp and udp
No. Time Source Destination Protocol Length Info
6 2.044679 52.112.95.73 192.168.0.101 TCP 60 [TCP ACKed unseen segment] 443 → 54068 [ACK]
7 2.044687 192.168.0.187 224.0.0.251 MDNS 91 Standard query 0x0000 PTR _airplay._tcp.loca
8 2.044690 fe80::c4:965d:3b8f… ff02::fb MDNS 111 Standard query 0x0000 PTR _airplay._tcp.loca
11 4.702671 192.168.0.101 35.186.220.184 TCP 54 53950 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
12 4.712456 35.186.220.184 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 53950 [ACK]
13 4.786974 192.168.0.101 35.171.30.114 TCP 54 53901 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
14 5.179397 35.171.30.114 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 53901 [ACK]
15 5.921641 192.168.0.101 142.250.196.78 TCP 54 54014 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
16 5.931148 142.250.196.78 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 54014 [ACK]
17 6.115323 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 1: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface en0, id 0
Ethernet II, Src: 0a:23:41:ed:45:58 (0a:23:41:ed:45:58), Dst: Apple_54:83:33 (88:66:5a:54:83:33)
Internet Protocol Version 4, Src: 192.168.0.159, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
User Datagram Protocol (udp), 8 bytes
Packets: 18 · Displayed: 16 (88.9%)
Profile: Default

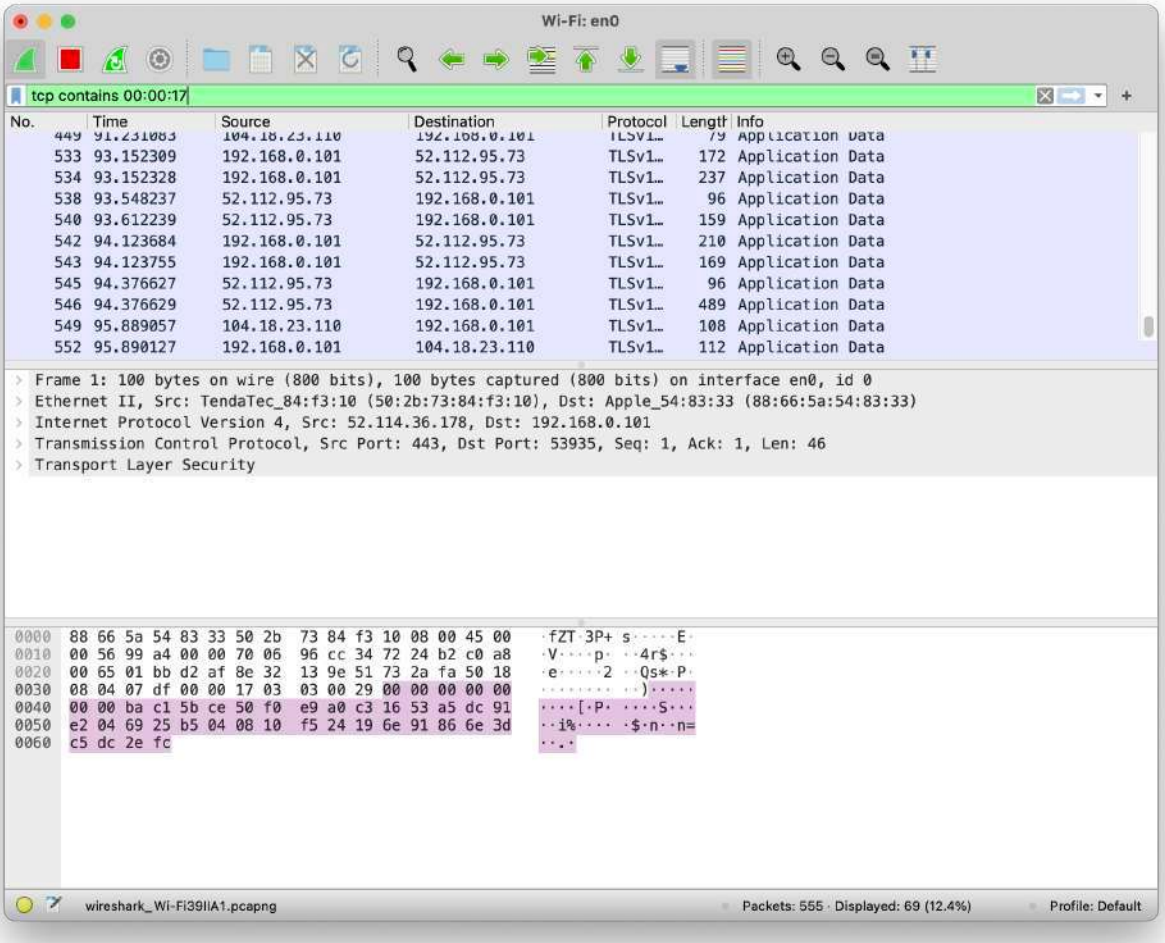

Wi-Fi: en0
udp or arp
No. Time Source Destination Protocol Length Info
154 15.547361 192.168.0.101 49.205.72.130 DNS 80 Standard query 0x9503 A sockets.leetcode.com
155 15.598179 49.205.72.130 192.168.0.101 DNS 142 Standard query response 0x9503 No such name
156 16.331714 TendaTec_84:f3:10 Apple_54:83:33 ARP 60 Who has 192.168.0.101? Tell 192.168.0.1
157 16.331780 Apple_54:83:33 TendaTec_84:f3:10 ARP 42 192.168.0.101 is at 88:66:5a:54:83:33
158 19.117376 192.168.0.101 49.205.72.130 DNS 80 Standard query 0x14c7 A sockets.leetcode.com
159 19.120552 49.205.72.130 192.168.0.101 DNS 142 Standard query response 0x14c7 No such name
160 20.841265 192.168.0.146 224.0.0.251 MDNS 232 Standard query 0x0000 PTR _companion-link._t
161 20.841273 fe80::83b:6ba3:48a… ff02::fb MDNS 252 Standard query 0x0000 PTR _companion-link._t
170 23.518587 192.168.0.101 49.205.72.130 DNS 80 Standard query 0xb92c A sockets.leetcode.com
171 23.598192 49.205.72.130 192.168.0.101 DNS 142 Standard query response 0xb92c No such name A
Frame 3: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.114.40.87
User Datagram Protocol, Src Port: 54675, Dst Port: 3478
Data (7 bytes)
Address Resolution Protocol: Protocol
Packets: 171 · Displayed: 65 (38.0%)
Profile: Default

4. Filter results based on Ip addresses
   - ip.src==52.114.40.87
   - Ip.dst==52.114.40.87

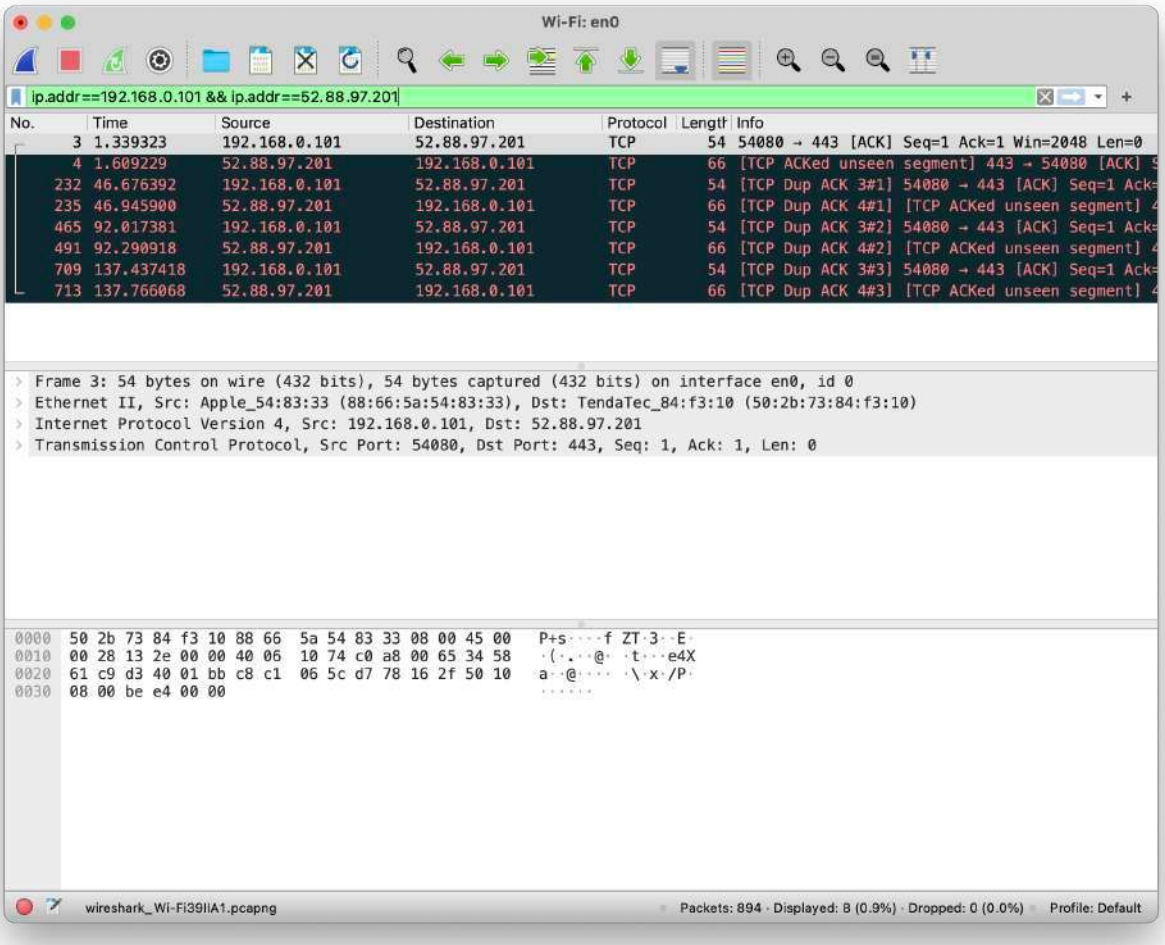


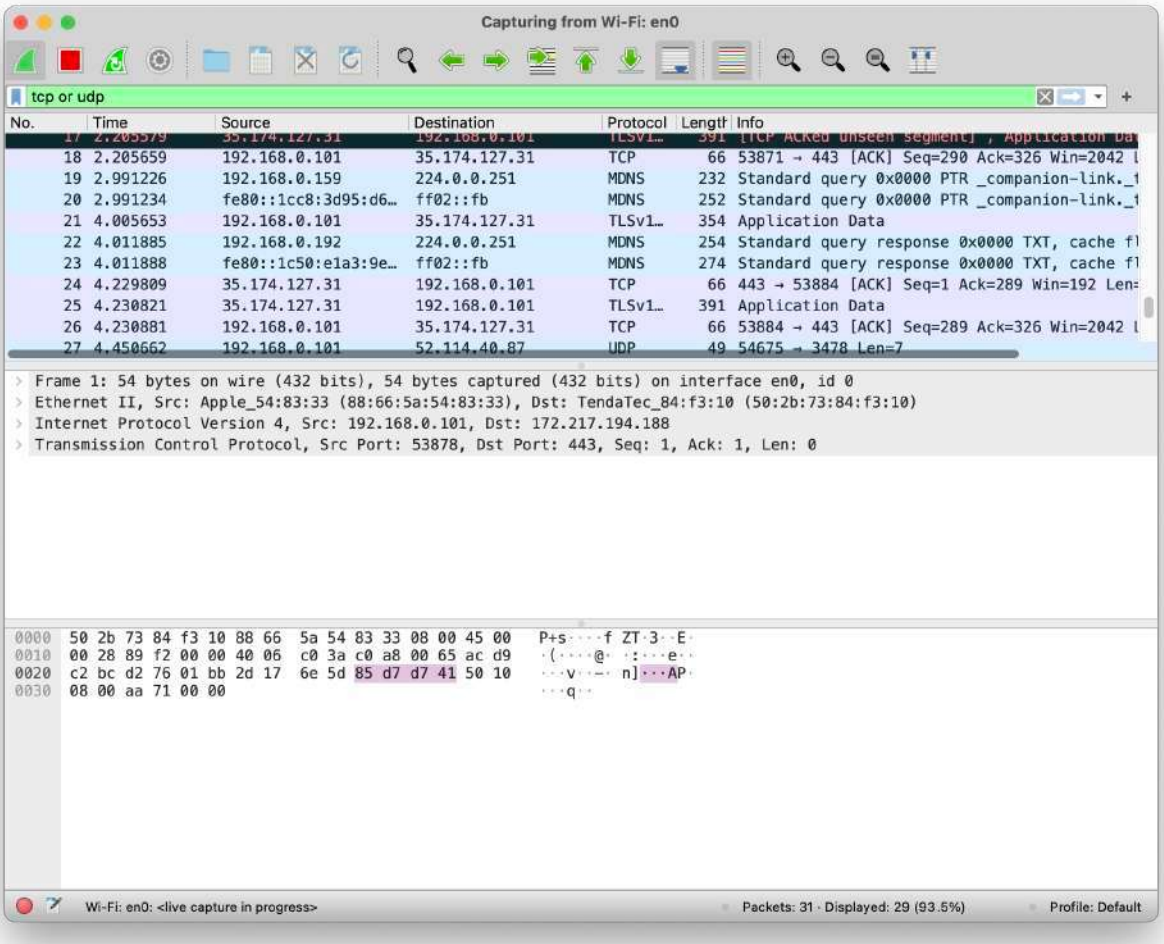

Wi-Fi: en0
ip.dst==52.114.40.87
No. Time Source Destination Protocol Length Info
250 10.253670 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
1570 25.252320 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
2016 40.252465 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
4283 55.252641 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
4717 70.253168 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
6848 85.253024 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
7050 100.252803 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
106… 115.252608 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
148… 130.251274 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
162… 145.251217 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
204… 160.250760 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
229… 175.251507 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
231… 190.250314 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
234… 205.250647 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
Frame 250: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.114.40.87
User Datagram Protocol, Src Port: 54675, Dst Port: 3478
Data (7 bytes)
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 23 c5 e6 00 00 40 11 97 0d c0 a8 00 65 34 72
0020 28 57 d5 93 0d 96 00 0f e4 c7 18 07 01 01 01 ff
0030 ff
wireshark_Wi-FIU50CA1.pcapng
Packets: 29680 · Displayed: 17 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

5. Filter results based on the byte sequence
   - Tcp contains 00:00:17

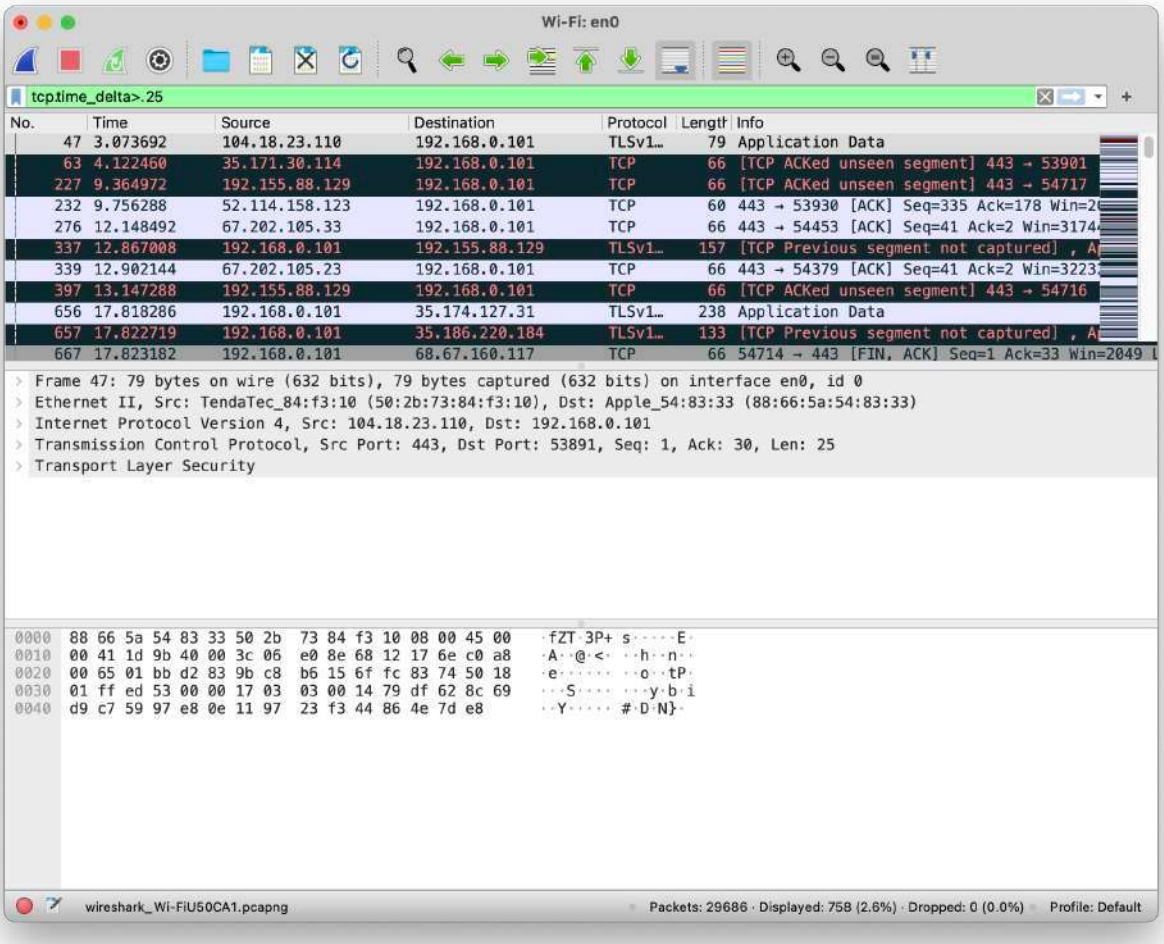


6. Filter result based on two IP addresses
   - ip.addr==192.168.0.101 && ip.addr==52.88.97.201
   - (ip.addr==192.168.0.101 or ip.addr==49.205.72.130) and(ip.addr==142.250.195.100 or ip.addr==142.250.77.110)

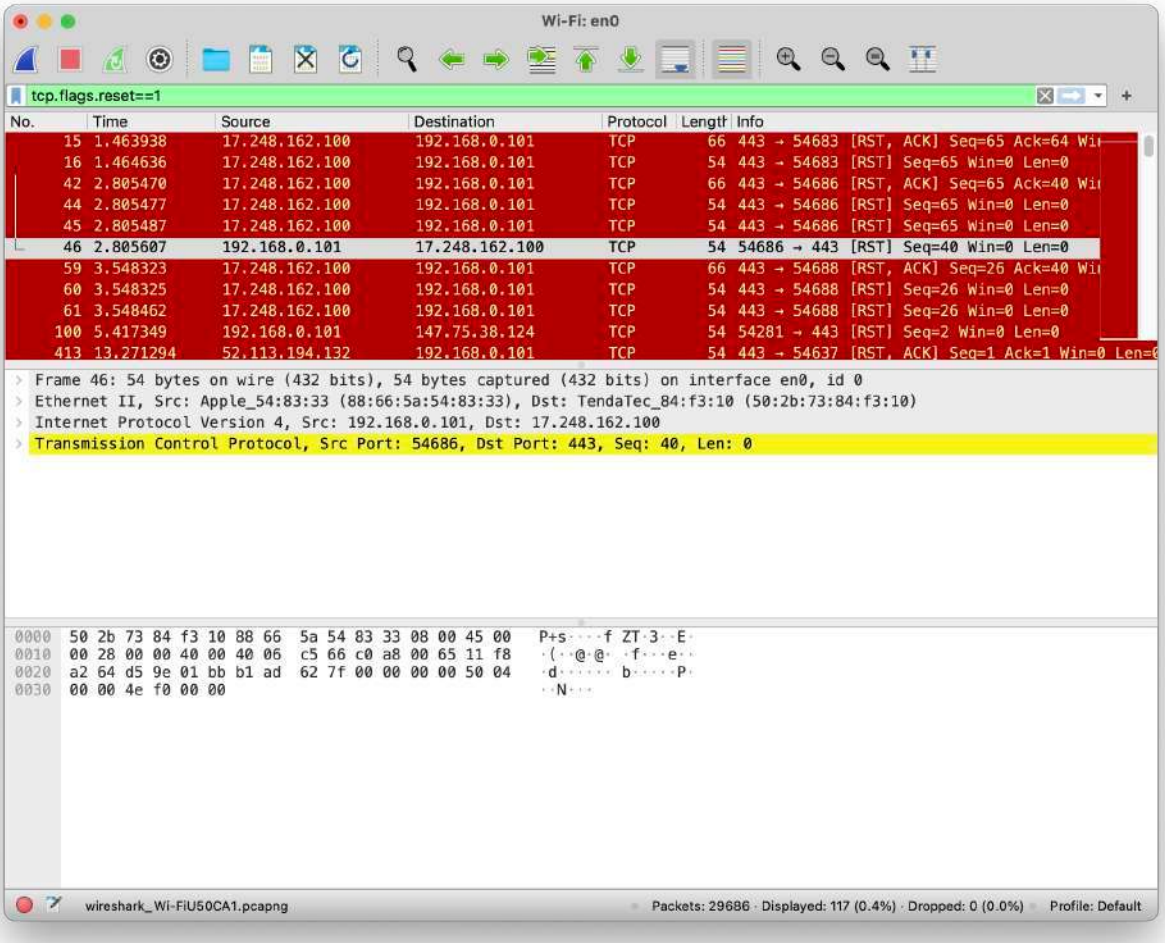


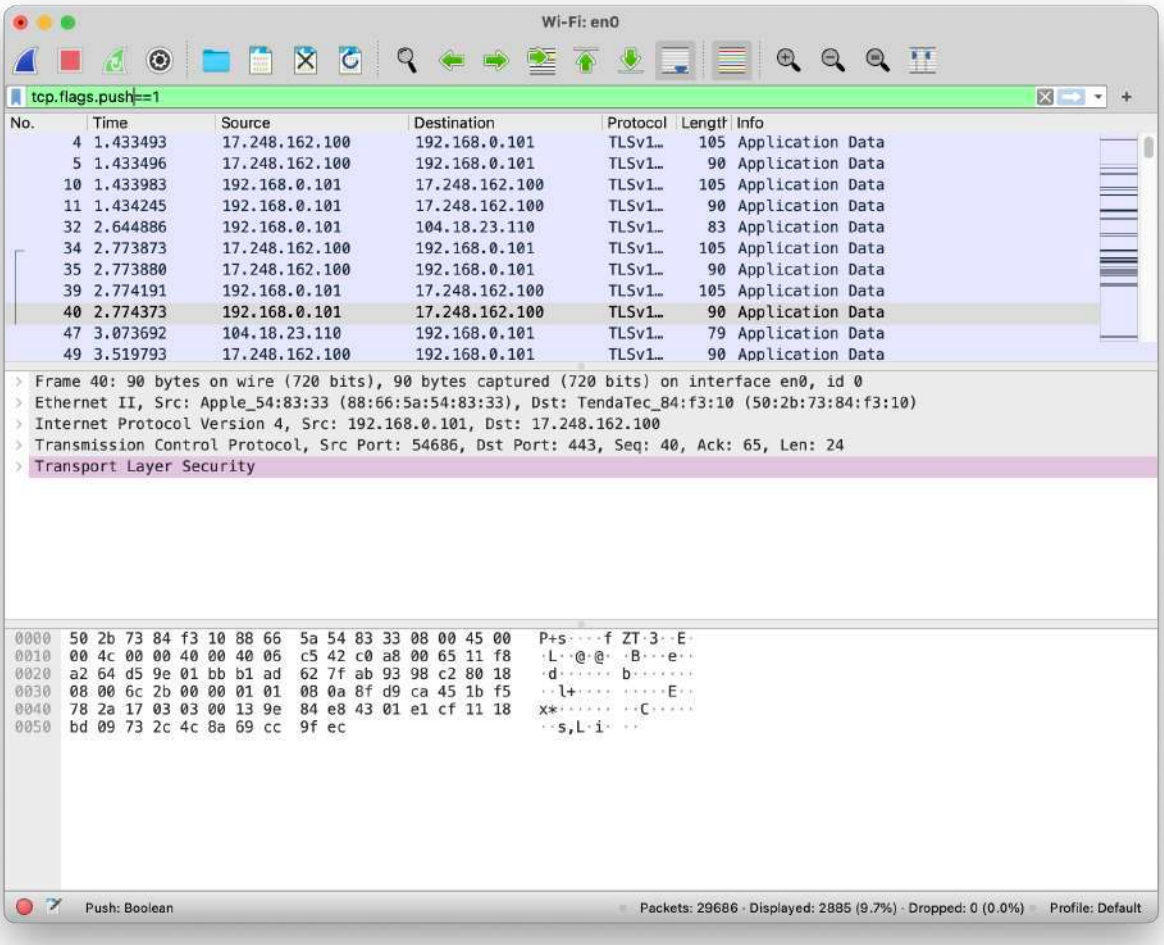

Capturing from Wi-Fi: en0
tcp or udp
No. Time Source Destination Protocol Length Info
17 2.205579 35.174.127.31 192.168.0.101 TLSv1… 591 [TCP ACKed unseen segment] , Application Da
18 2.205659 192.168.0.101 35.174.127.31 TCP 66 53871 → 443 [ACK] Seq=290 Ack=326 Win=2042 L
19 2.991226 192.168.0.159 224.0.0.251 MDNS 232 Standard query 0x0000 PTR _companion-link._t
20 2.991234 fe80::1cc8:3d95:d6… ff02::fb MDNS 252 Standard query 0x0000 PTR _companion-link._t
21 4.005653 192.168.0.101 35.174.127.31 TLSv1… 354 Application Data
22 4.011885 192.168.0.192 224.0.0.251 MDNS 254 Standard query response 0x0000 TXT, cache fl
23 4.011888 fe80::1c50:e1a3:9e… ff02::fb MDNS 274 Standard query response 0x0000 TXT, cache fl
24 4.229809 35.174.127.31 192.168.0.101 TCP 66 443 → 53884 [ACK] Seq=1 Ack=289 Win=192 Len=
25 4.230821 35.174.127.31 192.168.0.101 TLSv1… 391 Application Data
26 4.230881 192.168.0.101 35.174.127.31 TCP 66 53884 → 443 [ACK] Seq=289 Ack=326 Win=2042 L
27 4.450662 192.168.0.101 52.114.40.87 UDP 49 54675 → 3478 Len=7
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 172.217.194.188
Transmission Control Protocol, Src Port: 53878, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 28 89 f2 00 00 40 06 c0 3a c0 a8 00 65 ac d9
0020 c2 bc d2 76 01 bb 2d 17 6e 5d 85 d7 d7 41 50 10
0030 08 00 aa 71 00 00
Wi-Fi: en0: <live capture in progress>
Packets: 31 · Displayed: 29 (93.5%)
Profile: Default

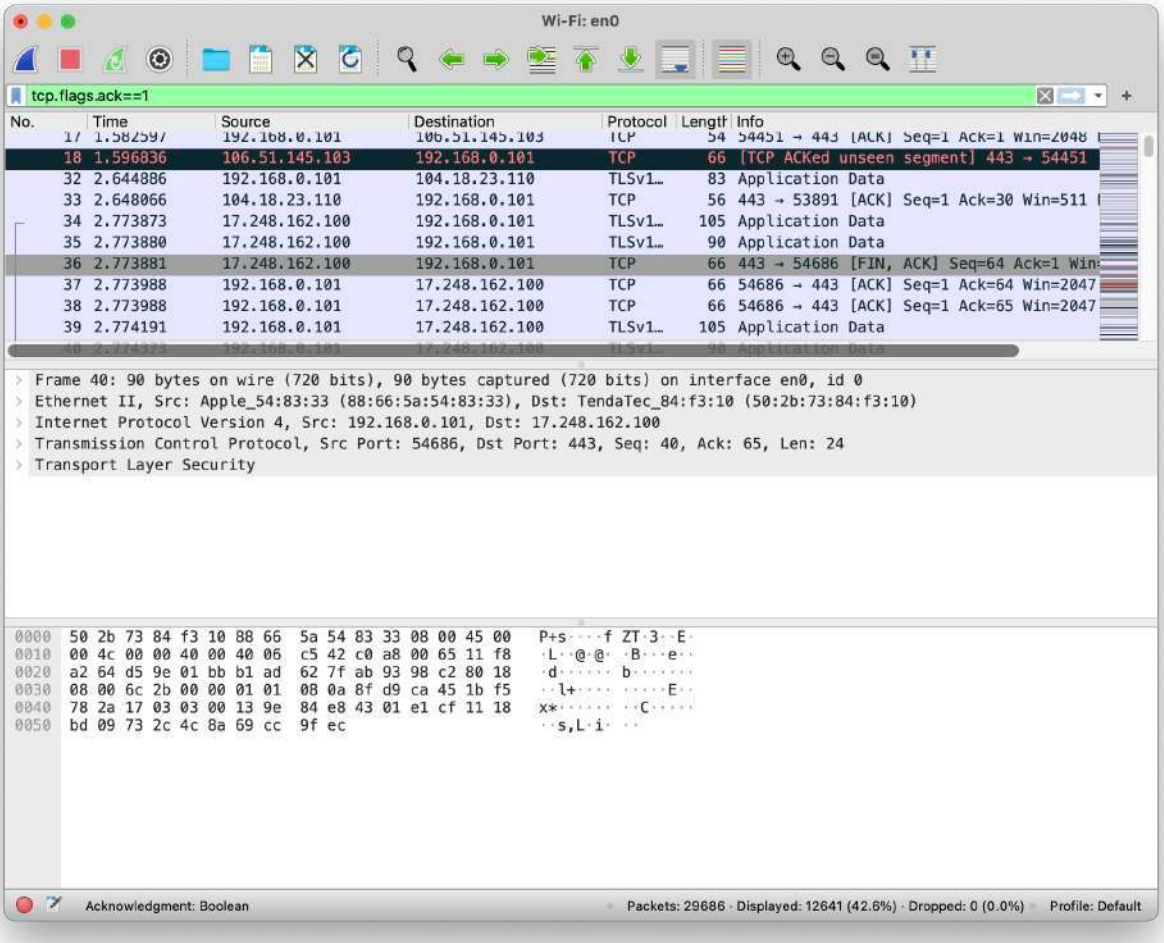
7. Filter the results based on timestamp
   - tcp.time_delta>.25

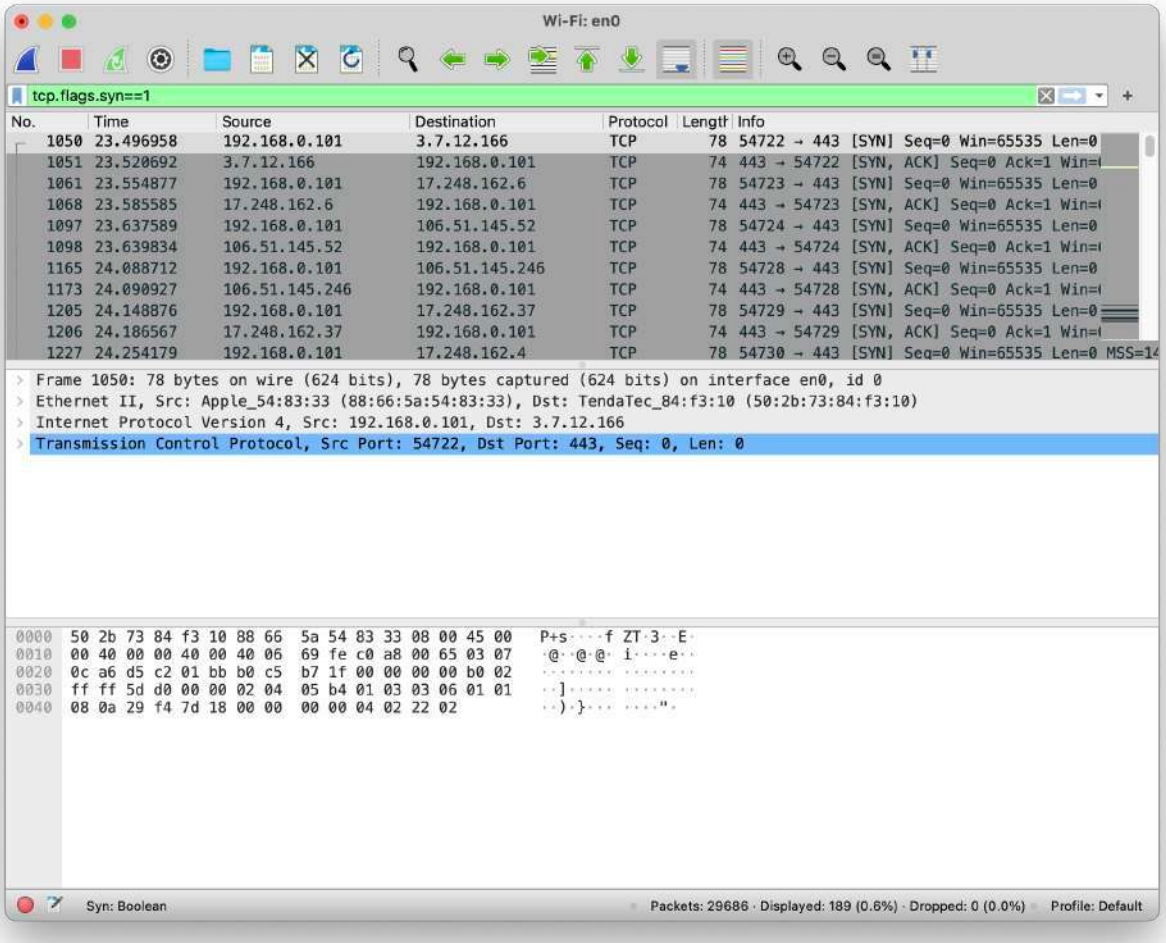


8. Filter the results based on the flags
   - tcp.flags.reset==1
   - tcp.flags.push==1
   - tcp.flags.ack==1
   - tcp.flags.syn==1

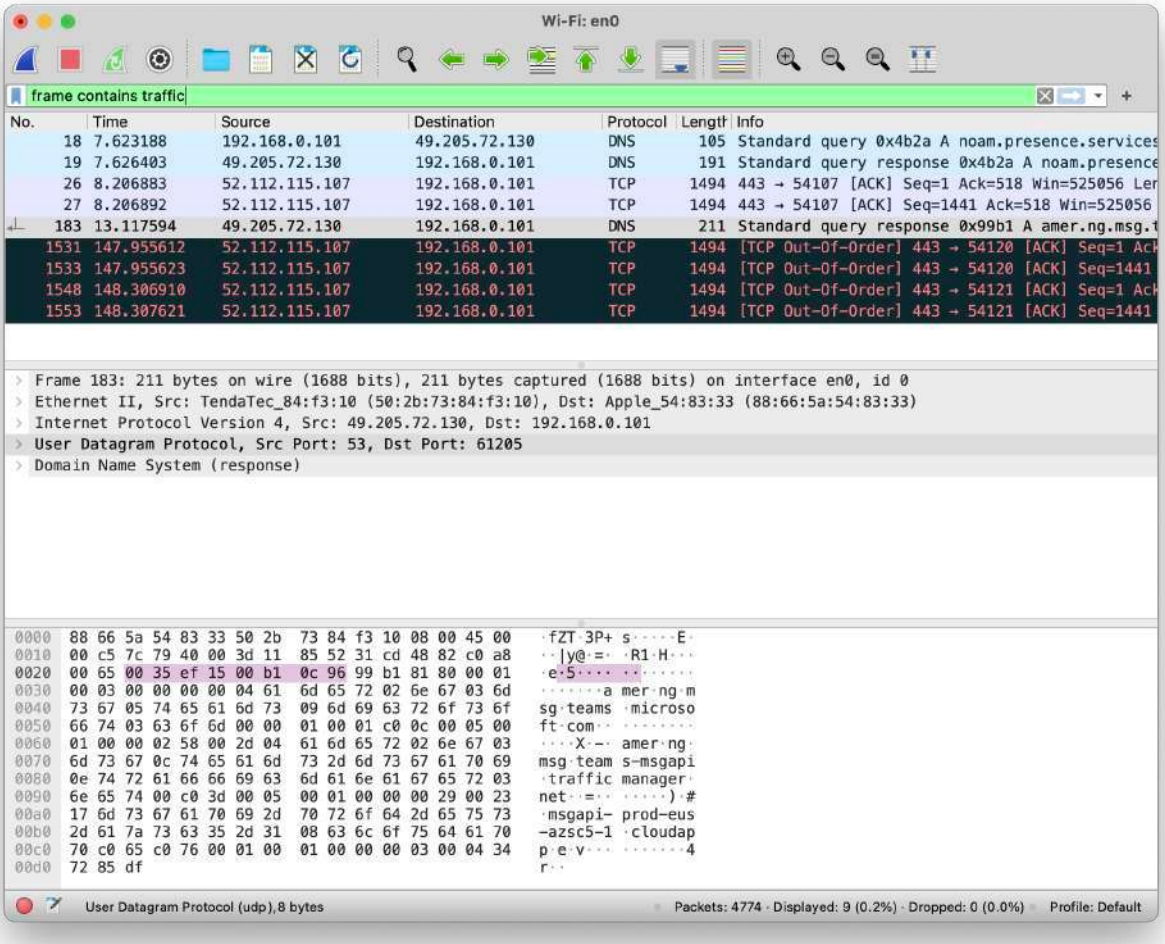



Wi-Fi: en0
tcp.flags.push==1
No. Time Source Destination Protocol Length Info
4 1.433493 17.248.162.100 192.168.0.101 TLSv1… 105 Application Data
5 1.433496 17.248.162.100 192.168.0.101 TLSv1… 90 Application Data
10 1.433983 192.168.0.101 17.248.162.100 TLSv1… 105 Application Data
11 1.434245 192.168.0.101 17.248.162.100 TLSv1… 90 Application Data
32 2.644886 192.168.0.101 104.18.23.110 TLSv1… 83 Application Data
34 2.773873 17.248.162.100 192.168.0.101 TLSv1… 105 Application Data
35 2.773880 17.248.162.100 192.168.0.101 TLSv1… 90 Application Data
39 2.774191 192.168.0.101 17.248.162.100 TLSv1… 105 Application Data
40 2.774373 192.168.0.101 17.248.162.100 TLSv1… 90 Application Data
47 3.073692 104.18.23.110 192.168.0.101 TLSv1… 79 Application Data
49 3.519793 17.248.162.100 192.168.0.101 TLSv1… 90 Application Data
Frame 40: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 17.248.162.100
Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 40, Ack: 65, Len: 24
Transport Layer Security
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 4c 00 00 40 00 40 06 c5 42 c0 a8 00 65 11 f8
0020 a2 64 d5 9e 01 bb b1 ad 62 7f ab 93 98 c2 80 18
0030 08 00 6c 2b 00 00 01 01 08 0a 8f d9 ca 45 1b f5
0040 78 2a 17 03 03 00 13 9e 84 e8 43 01 e1 cf 11 18
0050 bd 09 73 2c 4c 8a 69 cc 9f ec
Push: Boolean
Packets: 29686 · Displayed: 2885 (9.7%) · Dropped: 0 (0.0%)
Profile: Default

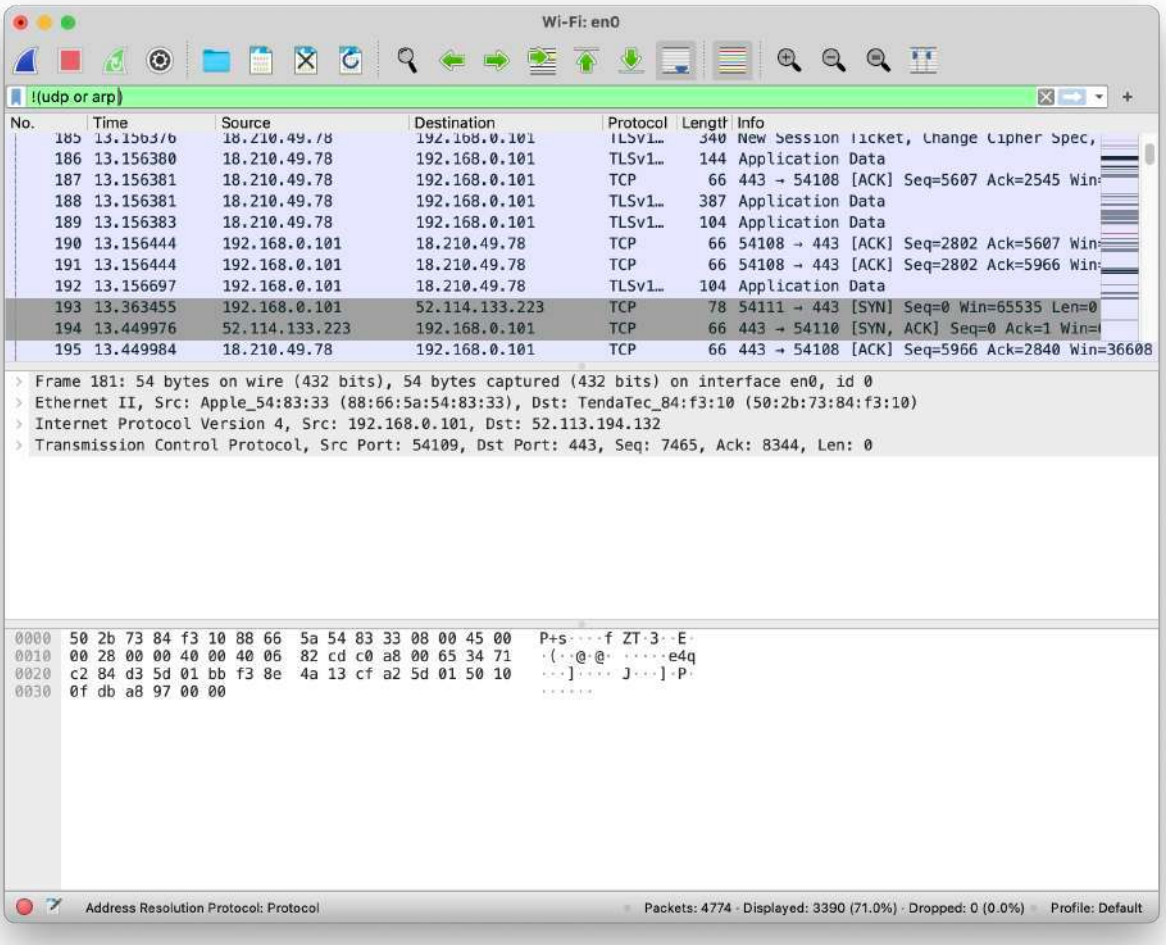

Wi-Fi: en0
tcp.flags.ack==1
No. Time Source Destination Protocol Length Info
18 1.596836 106.51.145.103 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 54451
32 2.644886 192.168.0.101 104.18.23.110 TLSv1… 83 Application Data
33 2.648066 104.18.23.110 192.168.0.101 TCP 56 443 → 53891 [ACK] Seq=1 Ack=30 Win=511
34 2.773873 17.248.162.100 192.168.0.101 TLSv1… 105 Application Data
35 2.773880 17.248.162.100 192.168.0.101 TLSv1… 90 Application Data
36 2.773881 17.248.162.100 192.168.0.101 TCP 66 443 → 54686 [FIN, ACK] Seq=64 Ack=1
37 2.773988 192.168.0.101 17.248.162.100 TCP 66 54686 → 443 [ACK] Seq=1 Ack=64 Win=2047
38 2.773988 192.168.0.101 17.248.162.100 TCP 66 54686 → 443 [ACK] Seq=1 Ack=65 Win=2047
39 2.774191 192.168.0.101 17.248.162.100 TLSv1… 105 Application Data
Frame 40: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 17.248.162.100
Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 40, Ack: 65, Len: 24
Transport Layer Security
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 4c 00 00 40 00 40 06 c5 42 c0 a8 00 65 11 f8
0020 a2 64 d5 9e 01 bb b1 ad 62 7f ab 93 98 c2 80 18
0030 08 00 6c 2b 00 00 01 01 08 0a 8f d9 ca 45 1b f5
0040 78 2a 17 03 03 00 13 9e 84 e8 43 01 e1 cf 11 18
0050 bd 09 73 2c 4c 8a 69 cc 9f ec
Acknowledgment: Boolean
Packets: 29686 · Displayed: 12641 (42.6%) · Dropped: 0 (0.0%)
Profile: Default

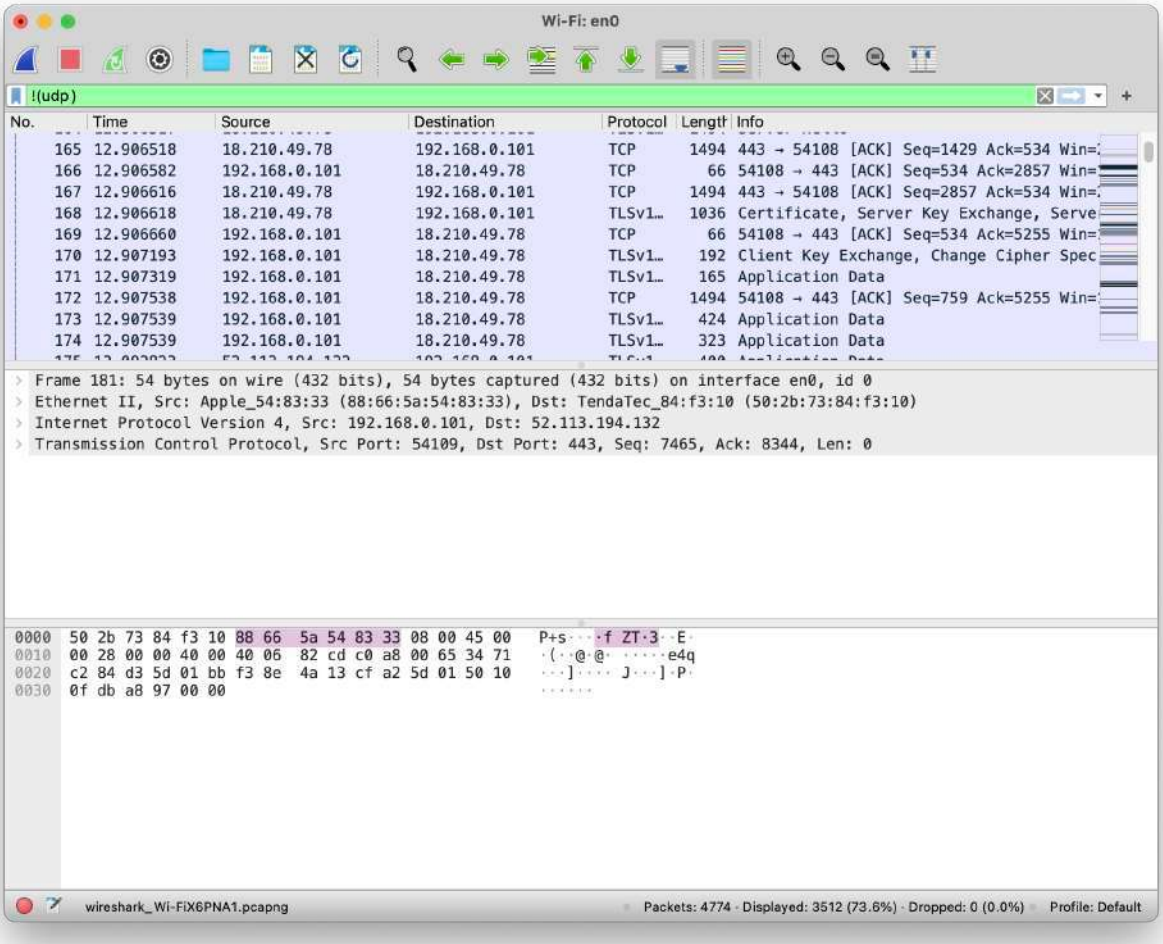

Wi-Fi: en0
tcp.flags.syn==1
No. Time Source Destination Protocol Lengtl Info
1050 23.496958 192.168.0.101 3.7.12.166 TCP 78 54722 → 443 [SYN] Seq=0 Win=65535 Len=0
1051 23.520692 3.7.12.166 192.168.0.101 TCP 74 443 → 54722 [SYN, ACK] Seq=0 Ack=1 Win=
1061 23.554877 192.168.0.101 17.248.162.6 TCP 78 54723 → 443 [SYN] Seq=0 Win=65535 Len=0
1068 23.585585 17.248.162.6 192.168.0.101 TCP 74 443 → 54723 [SYN, ACK] Seq=0 Ack=1 Win=
1097 23.637589 192.168.0.101 106.51.145.52 TCP 78 54724 → 443 [SYN] Seq=0 Win=65535 Len=0
1098 23.639834 106.51.145.52 192.168.0.101 TCP 74 443 → 54724 [SYN, ACK] Seq=0 Ack=1 Win=
1165 24.088712 192.168.0.101 106.51.145.246 TCP 78 54728 → 443 [SYN] Seq=0 Win=65535 Len=0
1173 24.090927 106.51.145.246 192.168.0.101 TCP 74 443 → 54728 [SYN, ACK] Seq=0 Ack=1 Win=
1205 24.148876 192.168.0.101 17.248.162.37 TCP 78 54729 → 443 [SYN] Seq=0 Win=65535 Len=0
1206 24.186567 17.248.162.37 192.168.0.101 TCP 74 443 → 54729 [SYN, ACK] Seq=0 Ack=1 Win=
1227 24.254179 192.168.0.101 17.248.162.4 TCP 78 54730 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=14
Frame 1050: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 3.7.12.166
Transmission Control Protocol, Src Port: 54722, Dst Port: 443, Seq: 0, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 40 00 00 40 00 40 06 69 fe c0 a8 00 65 03 07
0020 0c a6 d5 c2 01 bb b0 c5 b7 1f 00 00 00 00 b0 02
0030 ff ff 5d d0 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a 29 f4 7d 18 00 00 00 00 04 02 22 02
Syn: Boolean
Packets: 29686 · Displayed: 189 (0.6%) · Dropped: 0 (0.0%)
Profile: Default

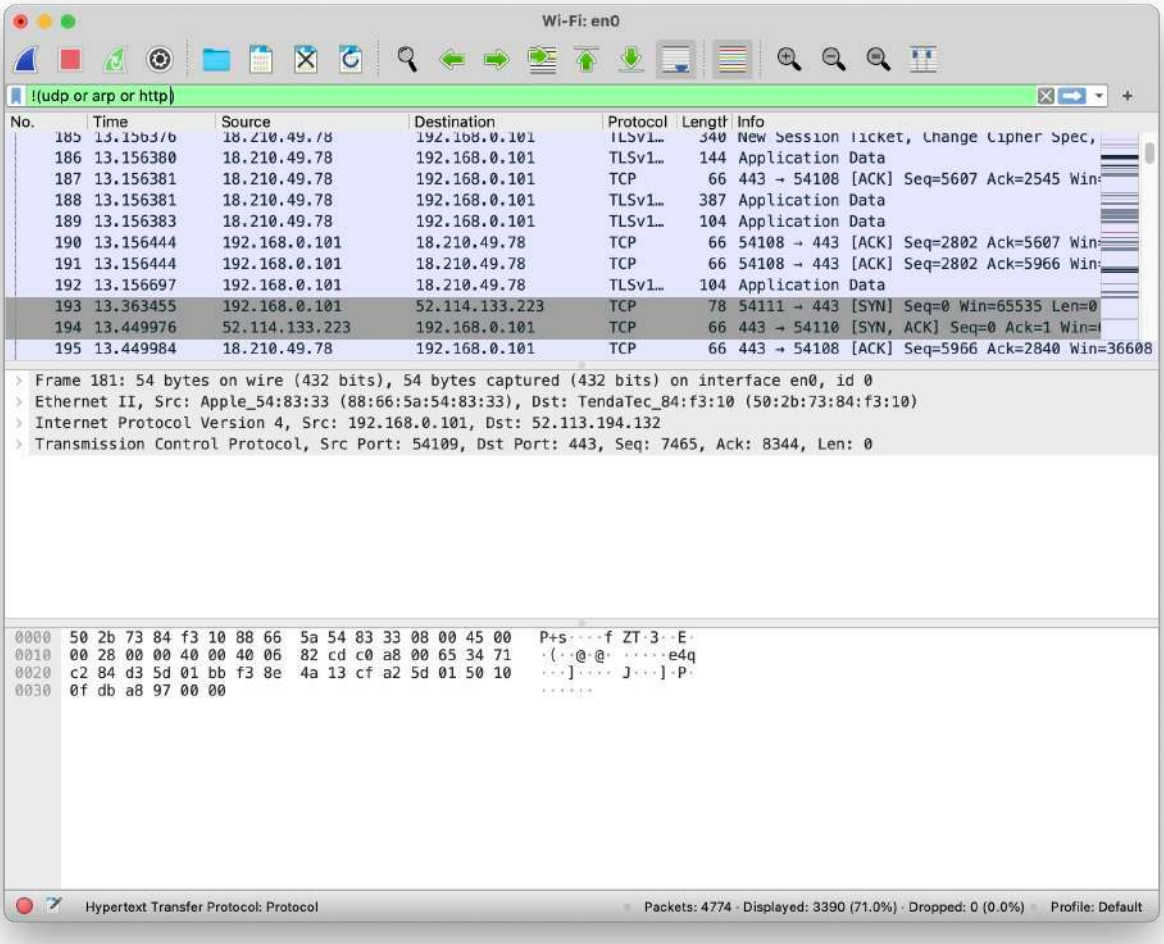
9. Traffic
   - frame contains traffic



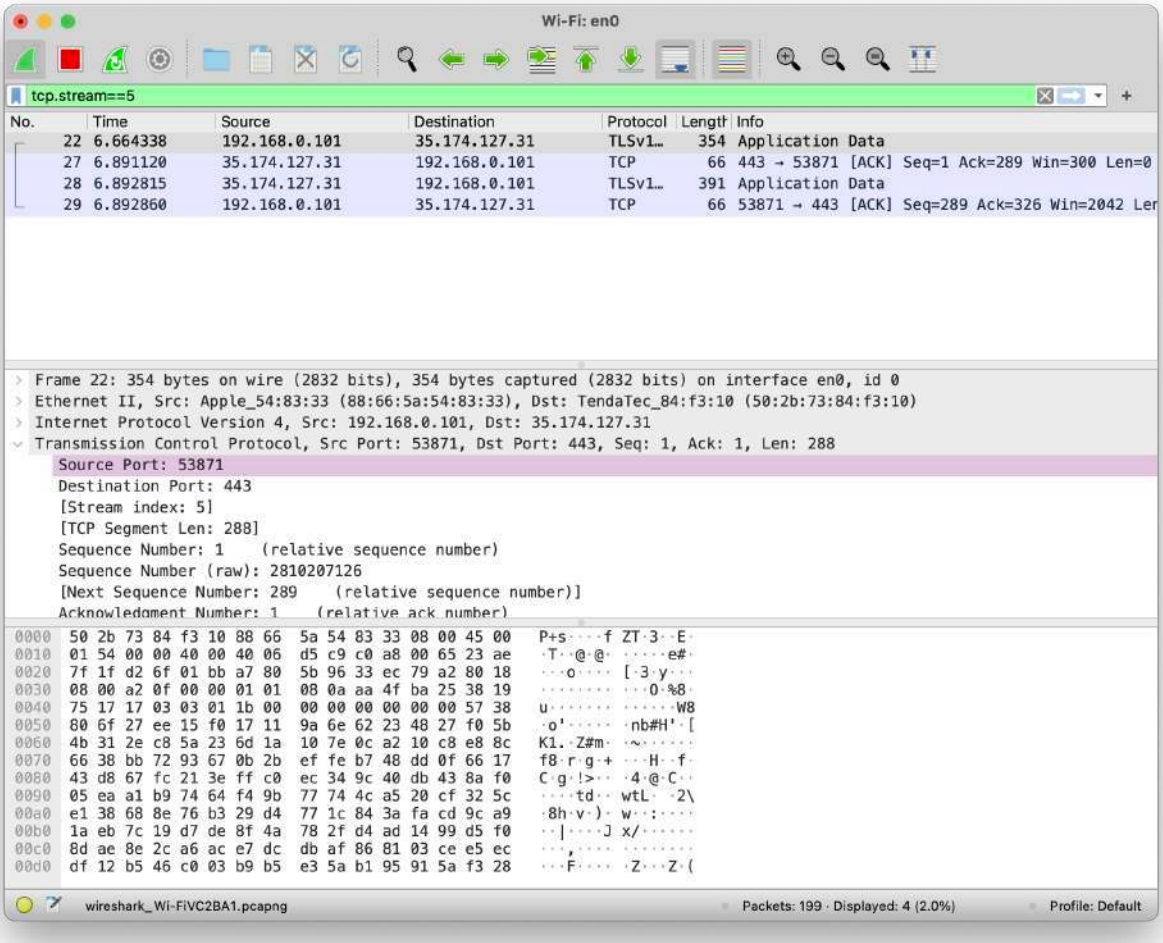
10. Filter based on NOT
    - !(udp or arp or http) / !(udp) / !(udp or arp)



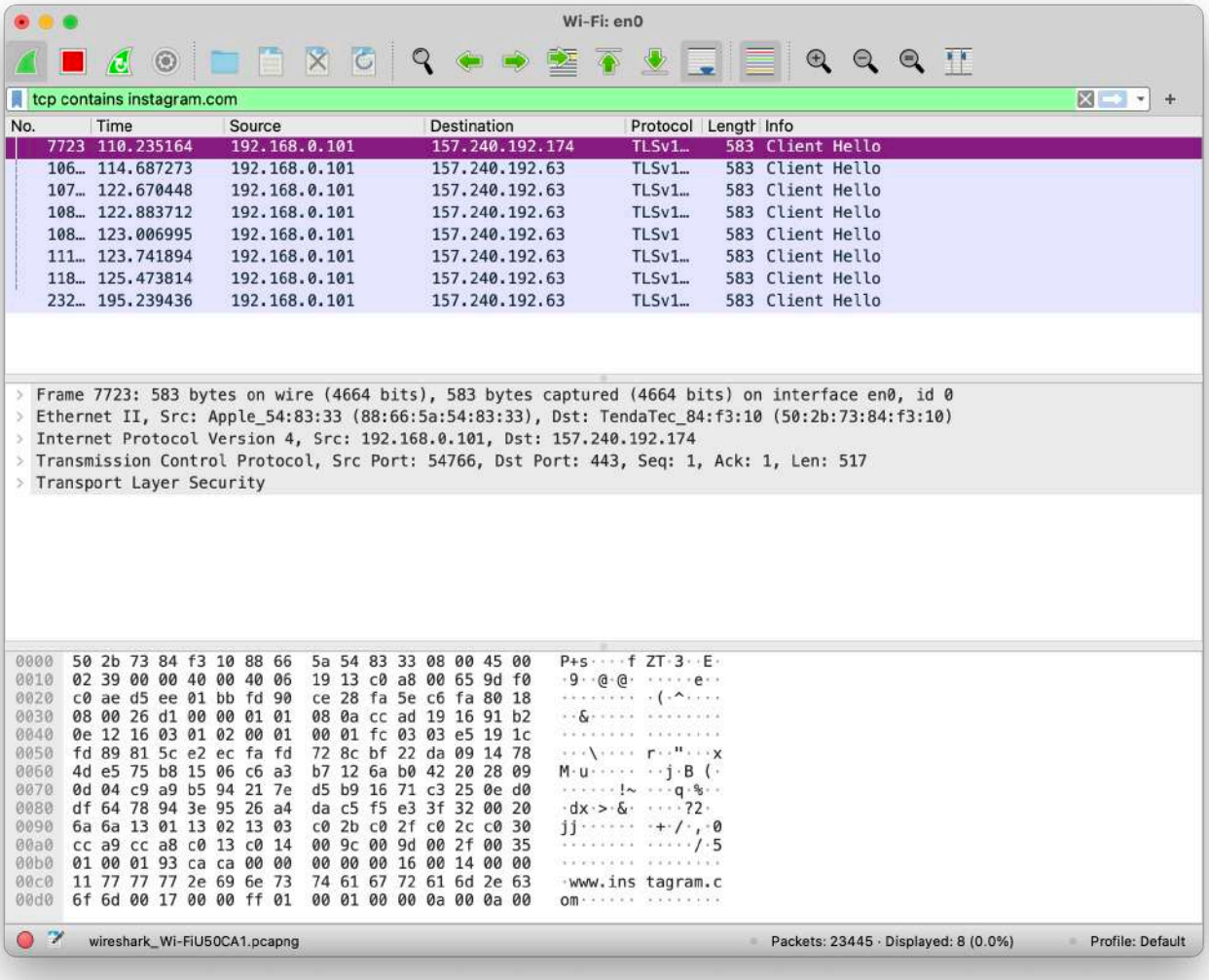

Wi-Fi: en0
!(udp)
No. Time Source Destination Protocol Length Info
165 12.906518 18.210.49.78 192.168.0.101 TCP 1494 443 → 54108 [ACK] Seq=1429 Ack=534 Win=
166 12.906582 192.168.0.101 18.210.49.78 TCP 66 54108 → 443 [ACK] Seq=534 Ack=2857 Win=
167 12.906616 18.210.49.78 192.168.0.101 TCP 1494 443 → 54108 [ACK] Seq=2857 Ack=534 Win=
168 12.906618 18.210.49.78 192.168.0.101 TLSv1… 1036 Certificate, Server Key Exchange, Serve
169 12.906660 192.168.0.101 18.210.49.78 TCP 66 54108 → 443 [ACK] Seq=534 Ack=5255 Win=
170 12.907193 192.168.0.101 18.210.49.78 TLSv1… 192 Client Key Exchange, Change Cipher Spec
171 12.907319 192.168.0.101 18.210.49.78 TLSv1… 165 Application Data
172 12.907538 192.168.0.101 18.210.49.78 TCP 1494 54108 → 443 [ACK] Seq=759 Ack=5255 Win=
173 12.907539 192.168.0.101 18.210.49.78 TLSv1… 424 Application Data
174 12.907539 192.168.0.101 18.210.49.78 TLSv1… 323 Application Data
Frame 181: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.113.194.132
Transmission Control Protocol, Src Port: 54109, Dst Port: 443, Seq: 7465, Ack: 8344, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 28 00 00 40 00 40 06 82 cd c0 a8 00 65 34 71
0020 c2 84 d3 5d 01 bb f3 8e 4a 13 cf a2 5d 01 50 10
0030 0f db a8 97 00 00
wireshark_Wi-FiX6PNA1.pcapng
Packets: 4774 · Displayed: 3512 (73.6%) · Dropped: 0 (0.0%)
Profile: Default


Wi-Fi: en0
!(udp or arp or http)
No. Time Source Destination Protocol Length Info
186 13.156380 18.210.49.78 192.168.0.101 TLSv1… 144 Application Data
187 13.156381 18.210.49.78 192.168.0.101 TCP 66 443 → 54108 [ACK] Seq=5607 Ack=2545 Win=
188 13.156381 18.210.49.78 192.168.0.101 TLSv1… 387 Application Data
189 13.156383 18.210.49.78 192.168.0.101 TLSv1… 104 Application Data
190 13.156444 192.168.0.101 18.210.49.78 TCP 66 54108 → 443 [ACK] Seq=2802 Ack=5607 Win=
191 13.156444 192.168.0.101 18.210.49.78 TCP 66 54108 → 443 [ACK] Seq=2802 Ack=5966 Win=
192 13.156697 192.168.0.101 18.210.49.78 TLSv1… 104 Application Data
193 13.363455 192.168.0.101 52.114.133.223 TCP 78 54111 → 443 [SYN] Seq=0 Win=65535 Len=0
194 13.449976 52.114.133.223 192.168.0.101 TCP 66 443 → 54110 [SYN, ACK] Seq=0 Ack=1 Win=
195 13.449984 18.210.49.78 192.168.0.101 TCP 66 443 → 54108 [ACK] Seq=5966 Ack=2840 Win=36608
Frame 181: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.113.194.132
Transmission Control Protocol, Src Port: 54109, Dst Port: 443, Seq: 7465, Ack: 8344, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 28 00 00 40 00 40 06 82 cd c0 a8 00 65 34 71
0020 c2 84 d3 5d 01 bb f3 8e 4a 13 cf a2 5d 01 50 10
0030 0f db a8 97 00 00
Hypertext Transfer Protocol: Protocol
Packets: 4774 · Displayed: 3390 (71.0%) · Dropped: 0 (0.0%)
Profile: Default

11. Filter based on the stream number
    - tcp.stream==5



12. Filter based on the website
    - tcp contains instagram.com



13. Filter the packets based on retransmission and duplicate acks
    - tcp analysis.flags