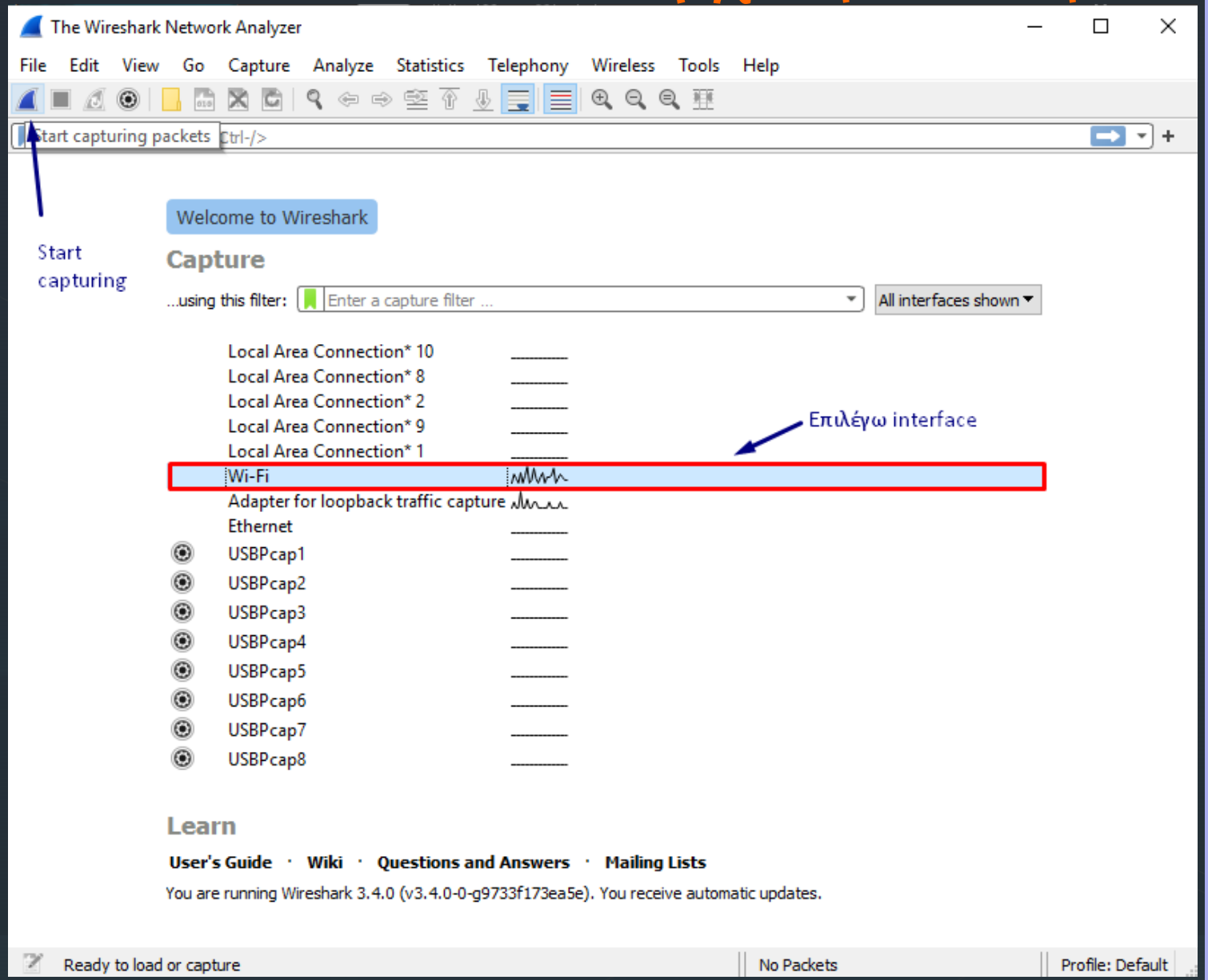
Δρ. Άννα Κεφάλα

WireShark (a network protocol analyser)

WireShark
Specifics

Αρχική οθόνη

- Click σε ένα interface για επιλογή →  start packet capture
- Menu *Capture*, *Stop* ή  → *σταματάει το* packet capture



Capture & analysis

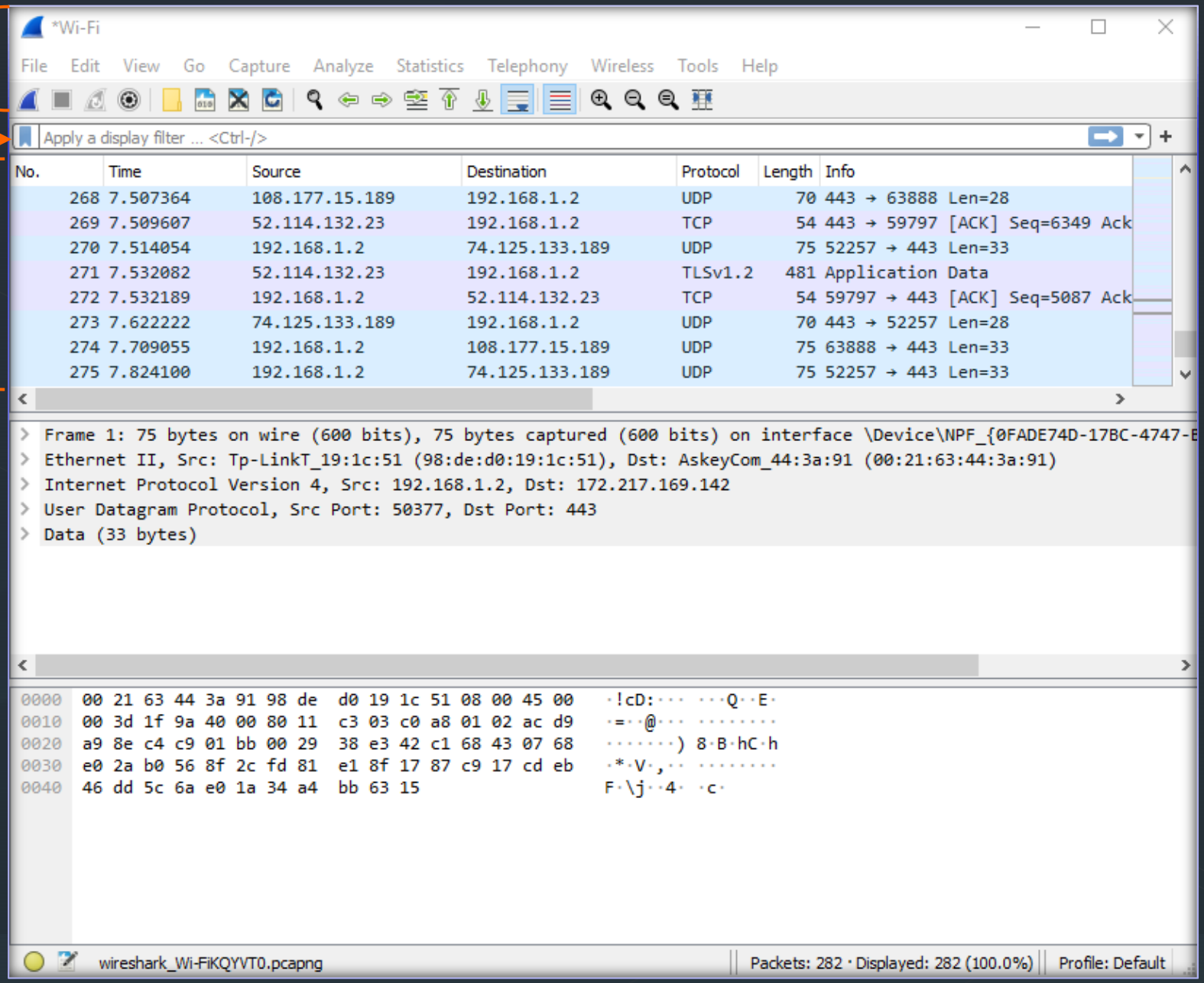
menus εντολών

προσδιορισμός φίλτρου

λίστα με captured πακέτα

λεπτομέρειες επικεφαλίδων επιλεγμένου πακέτου

δεδομένα πακέτου σε HEX και ASCII μορφή



Capture & analysis

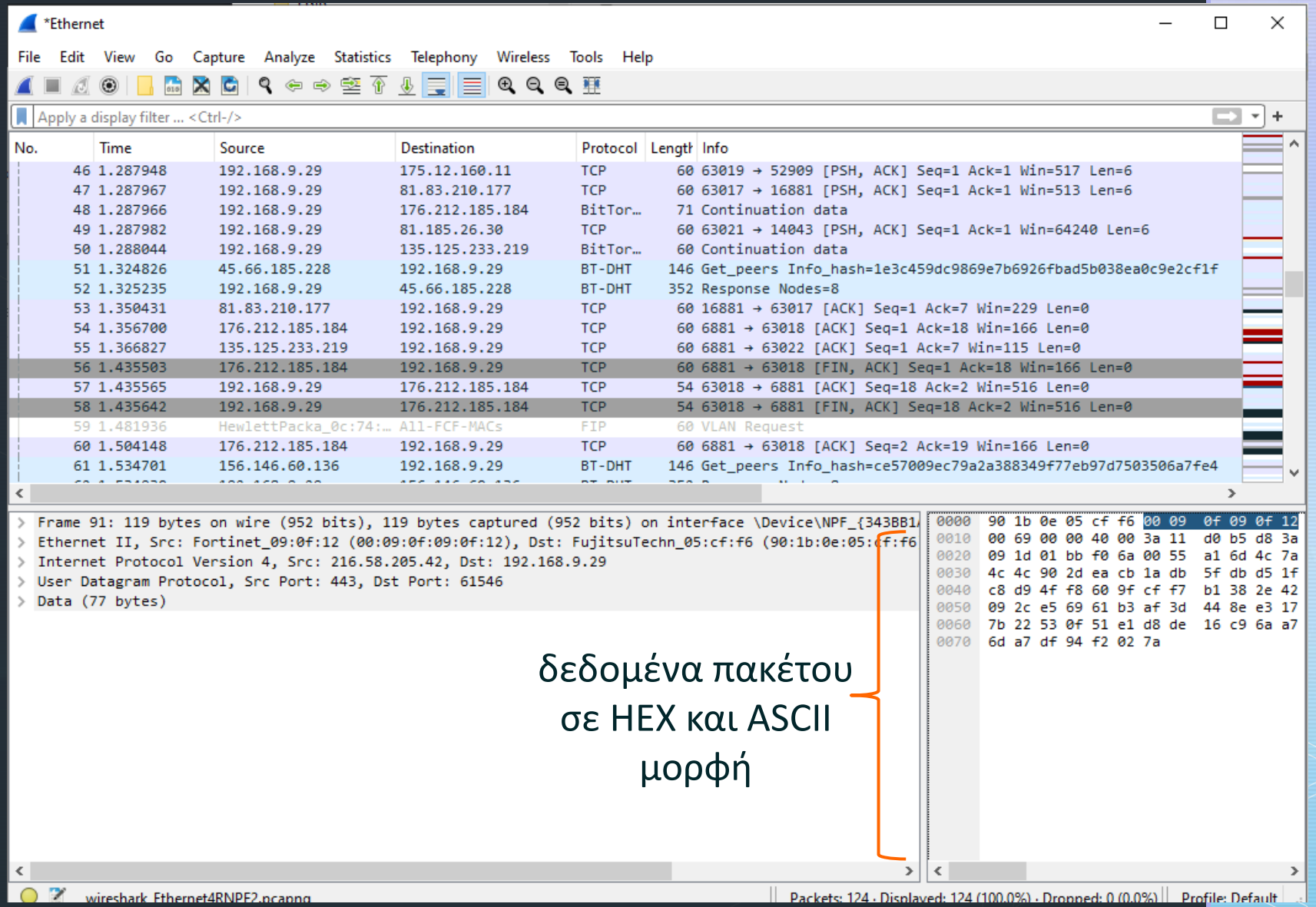
menus εντολών

προσδιορισμός φίλτρου

λίστα με captured πακέτα

λεπτομέρειες επικεφαλίδων επιλεγμένου πακέτου

δεδομένα πακέτου σε HEX και ASCII μορφή

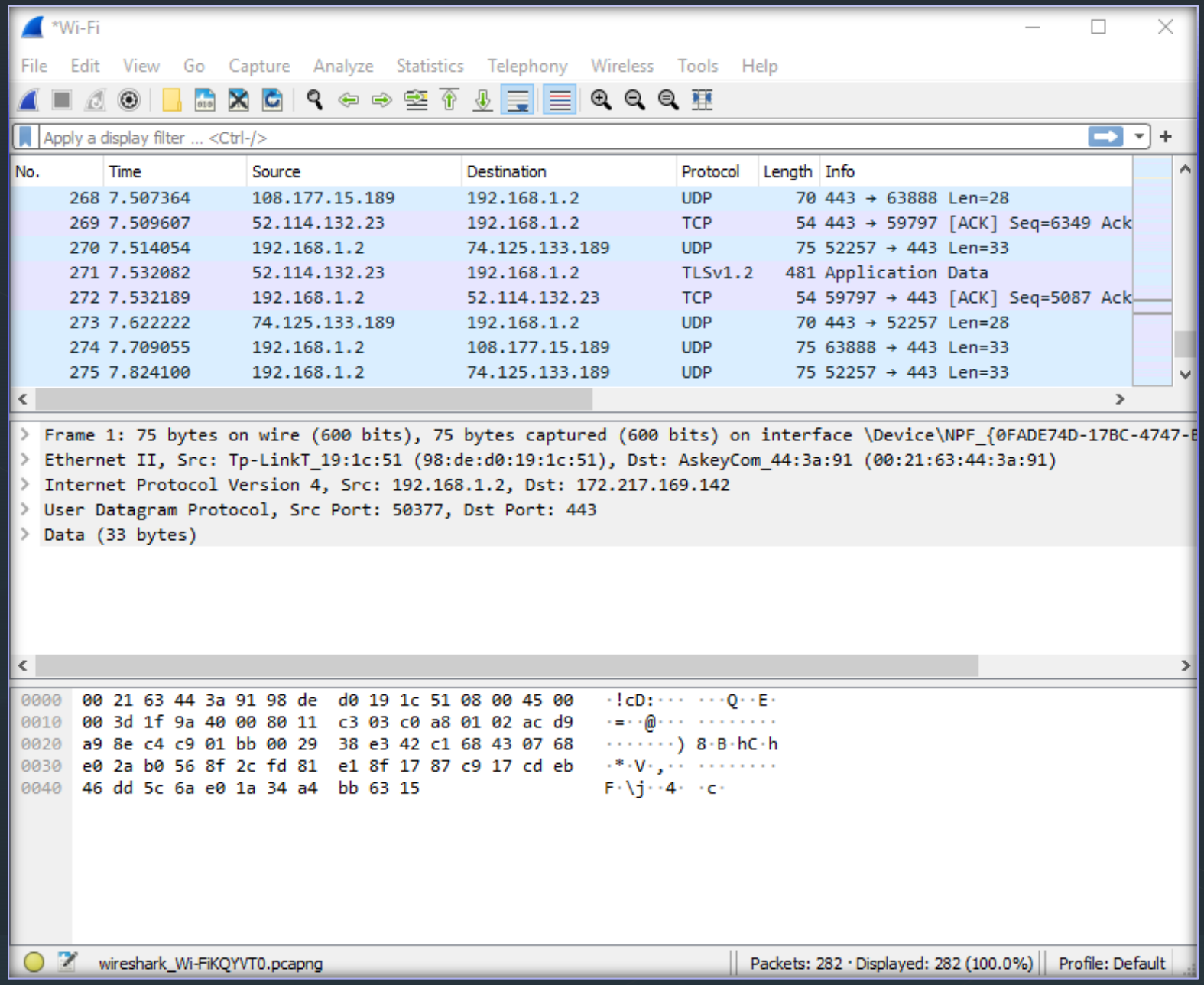


Packet Listing

- Packet number (σειρά με την οποία γίνεται το capturing)
- Time elapsed (ο χρόνος που έχει περάσει από την αρχή της ανίχνευσης)
- Source/destination addresses (IP ή Ethernet)
- Protocol type (top level: TCP, UDP, http, ssl, …)
- Length
- Protocol-specific information

Inside a packet

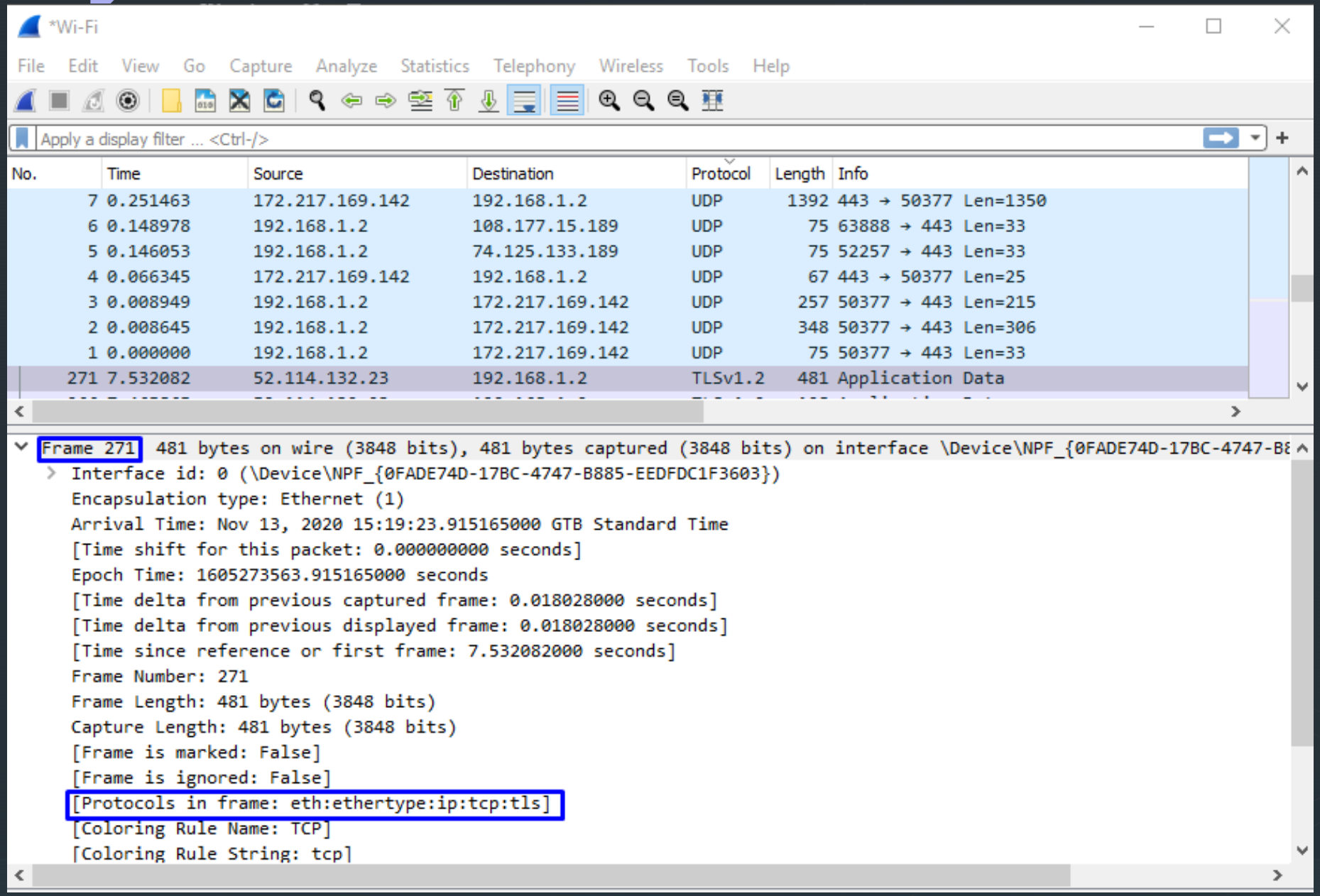
διαφορετικά πρωτόκολλα ενσωματώνονται μέσα σε ένα πακέτο



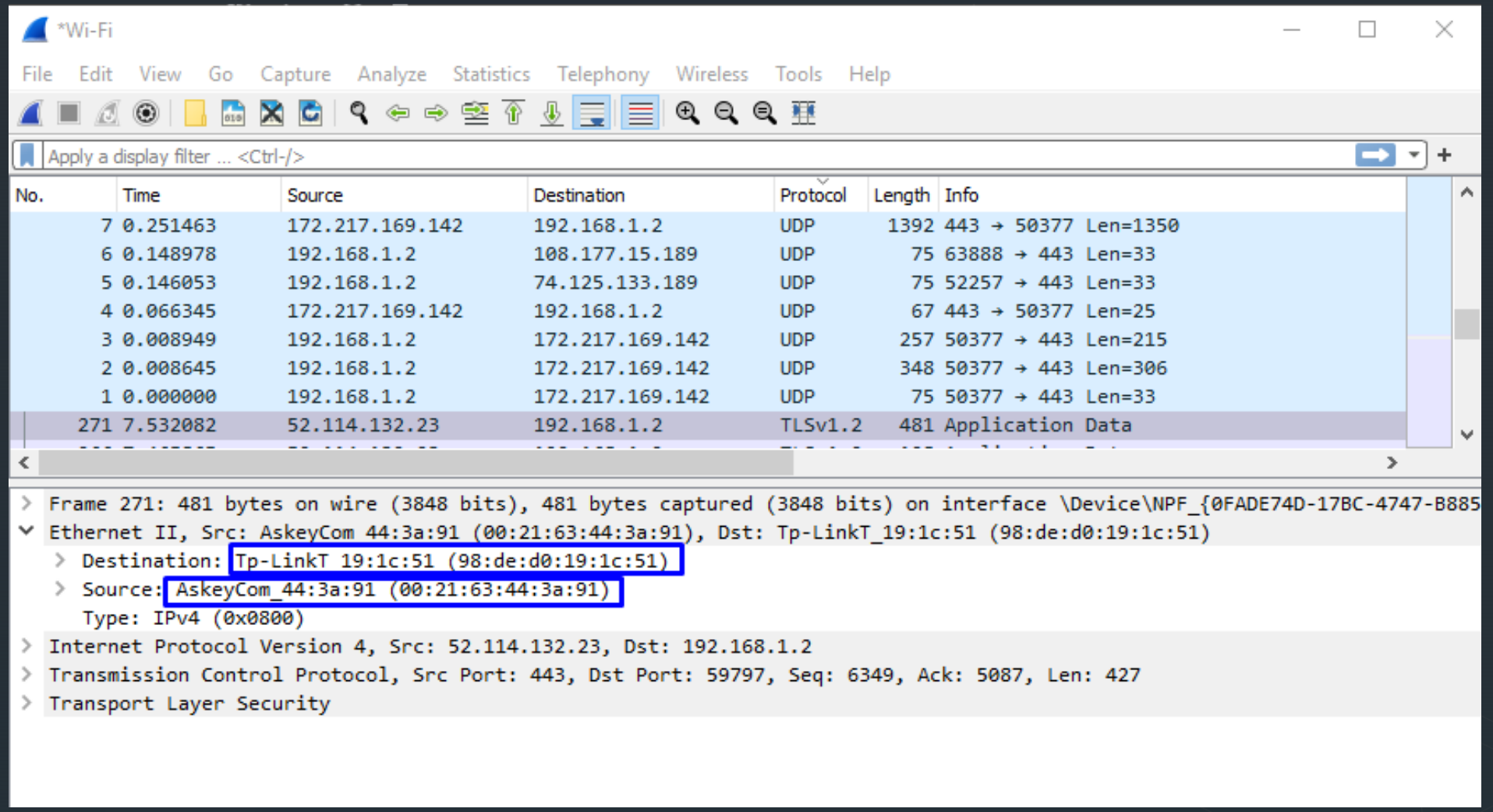
Packet-fields/headers details (για επιλεγμένο πακέτο)

- Ethernet frame (επίπεδο σύνδεσης δεδομένων)
- IP datagram (επίπεδο δικτύου)
- TCP/UDP segment (επίπεδο μεταφοράς)
- Upper layer protocol (επίπεδο εφαρμογής)

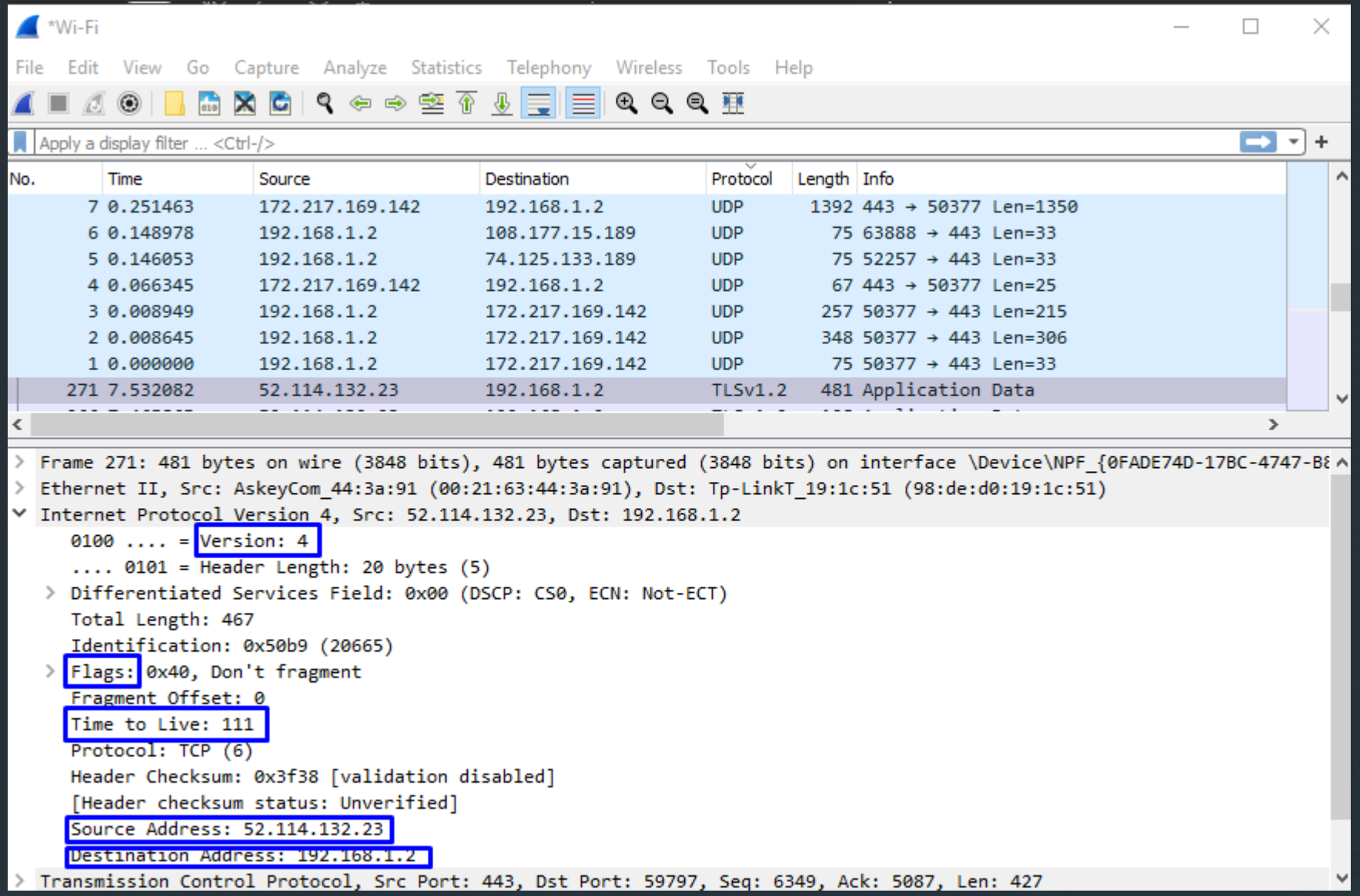
Frame


*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
7 0.251463 172.217.169.142 192.168.1.2 UDP 1392 443 → 50377 Len=1350
6 0.148978 192.168.1.2 108.177.15.189 UDP 75 63888 → 443 Len=33
5 0.146053 192.168.1.2 74.125.133.189 UDP 75 52257 → 443 Len=33
4 0.066345 172.217.169.142 192.168.1.2 UDP 67 443 → 50377 Len=25
3 0.008949 192.168.1.2 172.217.169.142 UDP 257 50377 → 443 Len=215
2 0.008645 192.168.1.2 172.217.169.142 UDP 348 50377 → 443 Len=306
1 0.000000 192.168.1.2 172.217.169.142 UDP 75 50377 → 443 Len=33
271 7.532082 52.114.132.23 192.168.1.2 TLSv1.2 481 Application Data
Frame 271: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-B8
Interface id: 0 (\Device\NPF_{0FADE74D-17BC-4747-B885-EEDFDC1F3603})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 13, 2020 15:19:23.915165000 GTB Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1605273563.915165000 seconds
[Time delta from previous captured frame: 0.018028000 seconds]
[Time delta from previous displayed frame: 0.018028000 seconds]
[Time since reference or first frame: 7.532082000 seconds]
Frame Number: 271
Frame Length: 481 bytes (3848 bits)
Capture Length: 481 bytes (3848 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:tls]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]

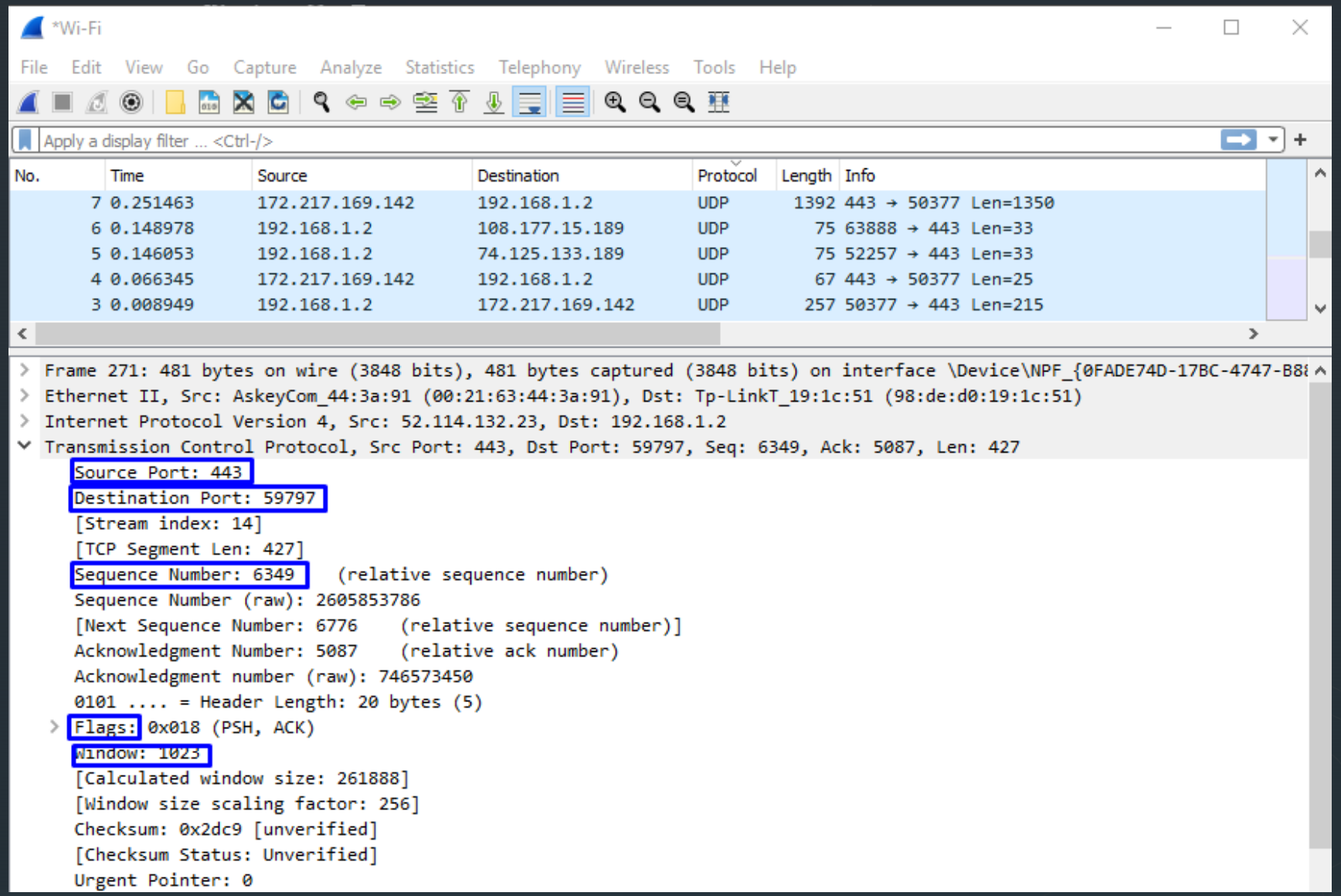
Ethernet


*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
7 0.251463 172.217.169.142 192.168.1.2 UDP 1392 443 → 50377 Len=1350
6 0.148978 192.168.1.2 108.177.15.189 UDP 75 63888 → 443 Len=33
5 0.146053 192.168.1.2 74.125.133.189 UDP 75 52257 → 443 Len=33
4 0.066345 172.217.169.142 192.168.1.2 UDP 67 443 → 50377 Len=25
3 0.008949 192.168.1.2 172.217.169.142 UDP 257 50377 → 443 Len=215
2 0.008645 192.168.1.2 172.217.169.142 UDP 348 50377 → 443 Len=306
1 0.000000 192.168.1.2 172.217.169.142 UDP 75 50377 → 443 Len=33
271 7.532082 52.114.132.23 192.168.1.2 TLSv1.2 481 Application Data
Frame 271: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-B885
Ethernet II, Src: AskeyCom 44:3a:91 (00:21:63:44:3a:91), Dst: Tp-LinkT 19:1c:51 (98:de:d0:19:1c:51)
Destination: Tp-LinkT 19:1c:51 (98:de:d0:19:1c:51)
Source: AskeyCom 44:3a:91 (00:21:63:44:3a:91)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 52.114.132.23, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 443, Dst Port: 59797, Seq: 6349, Ack: 5087, Len: 427
Transport Layer Security

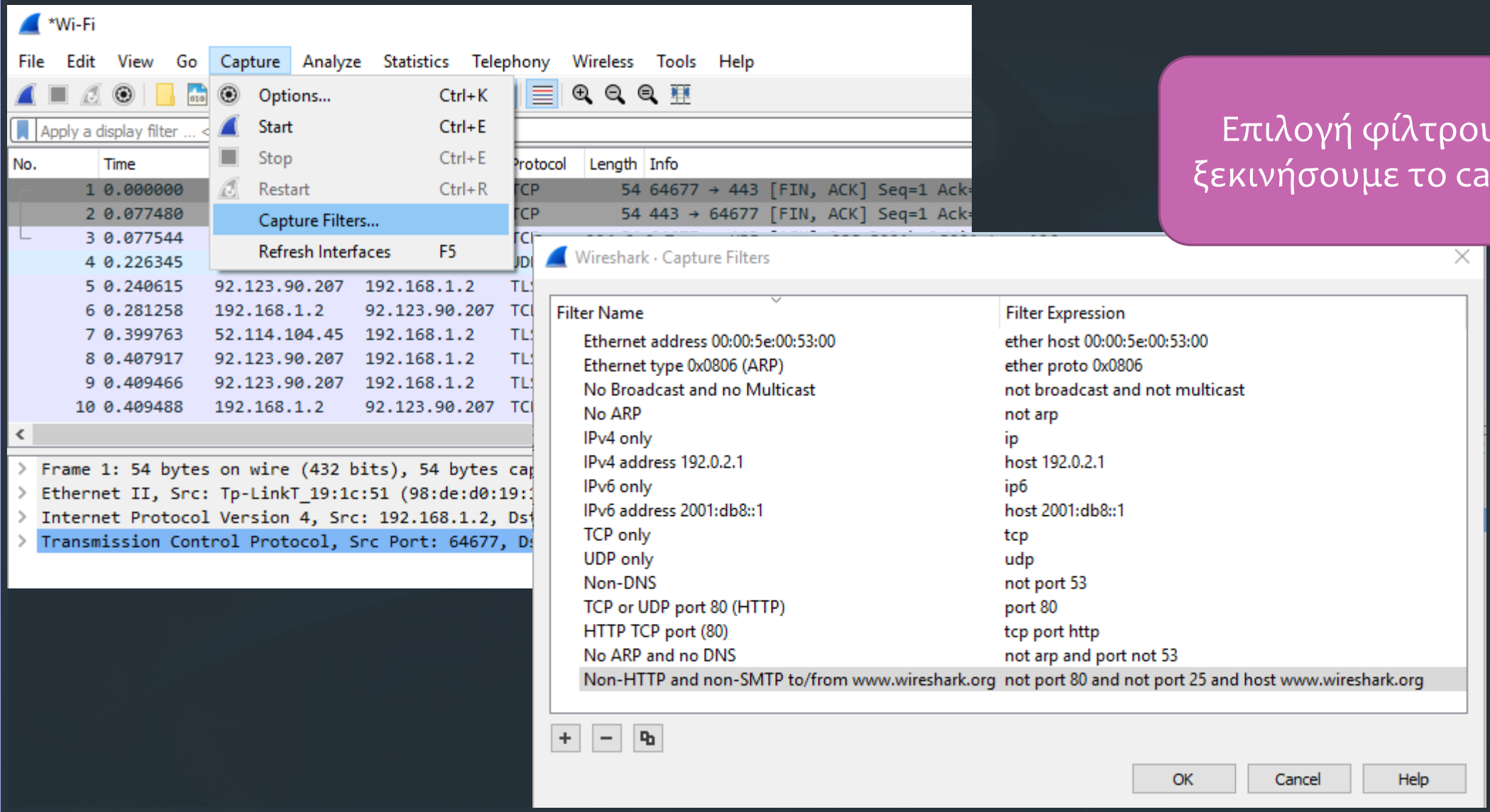
Internet Protocol (ver4)



Transmission Control Protocol

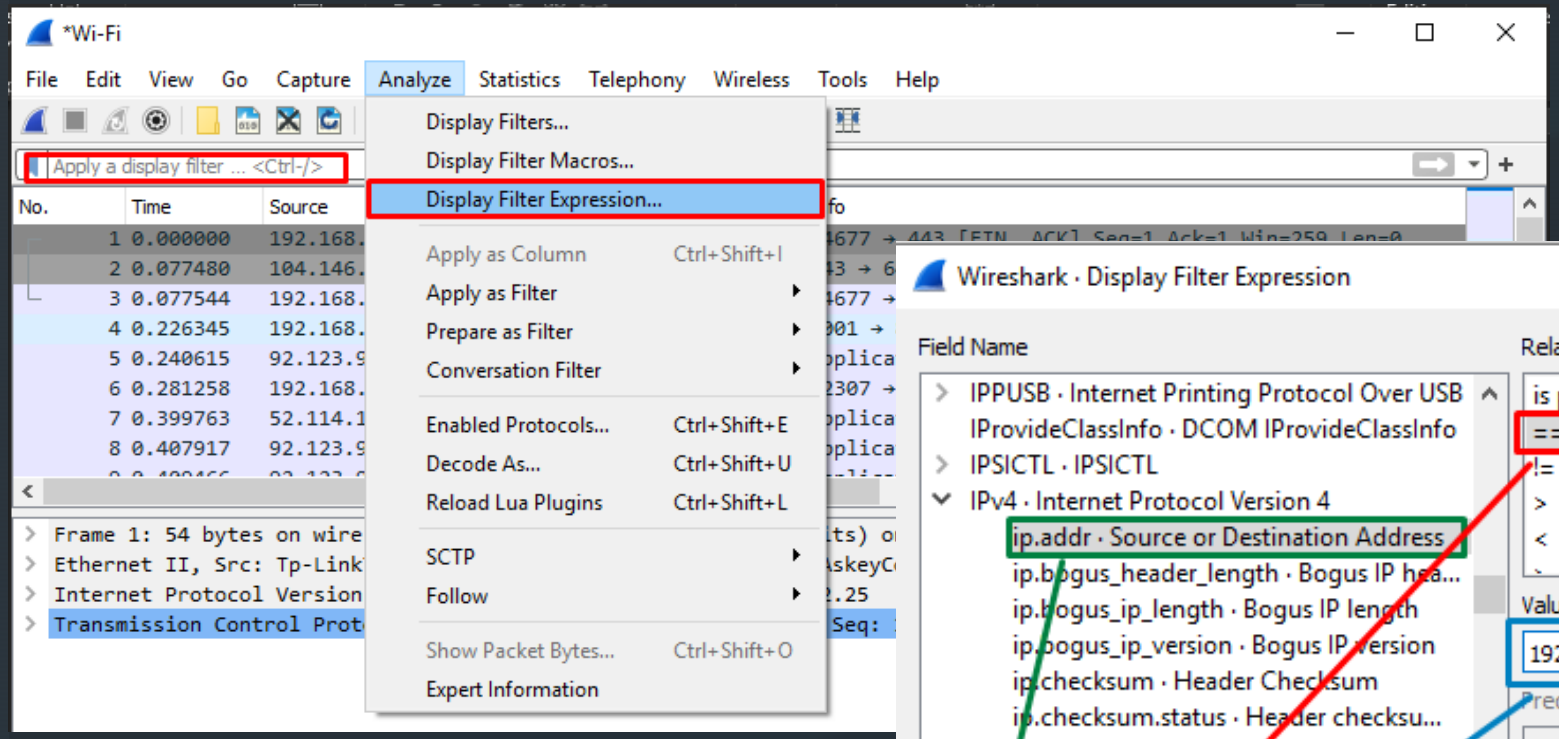


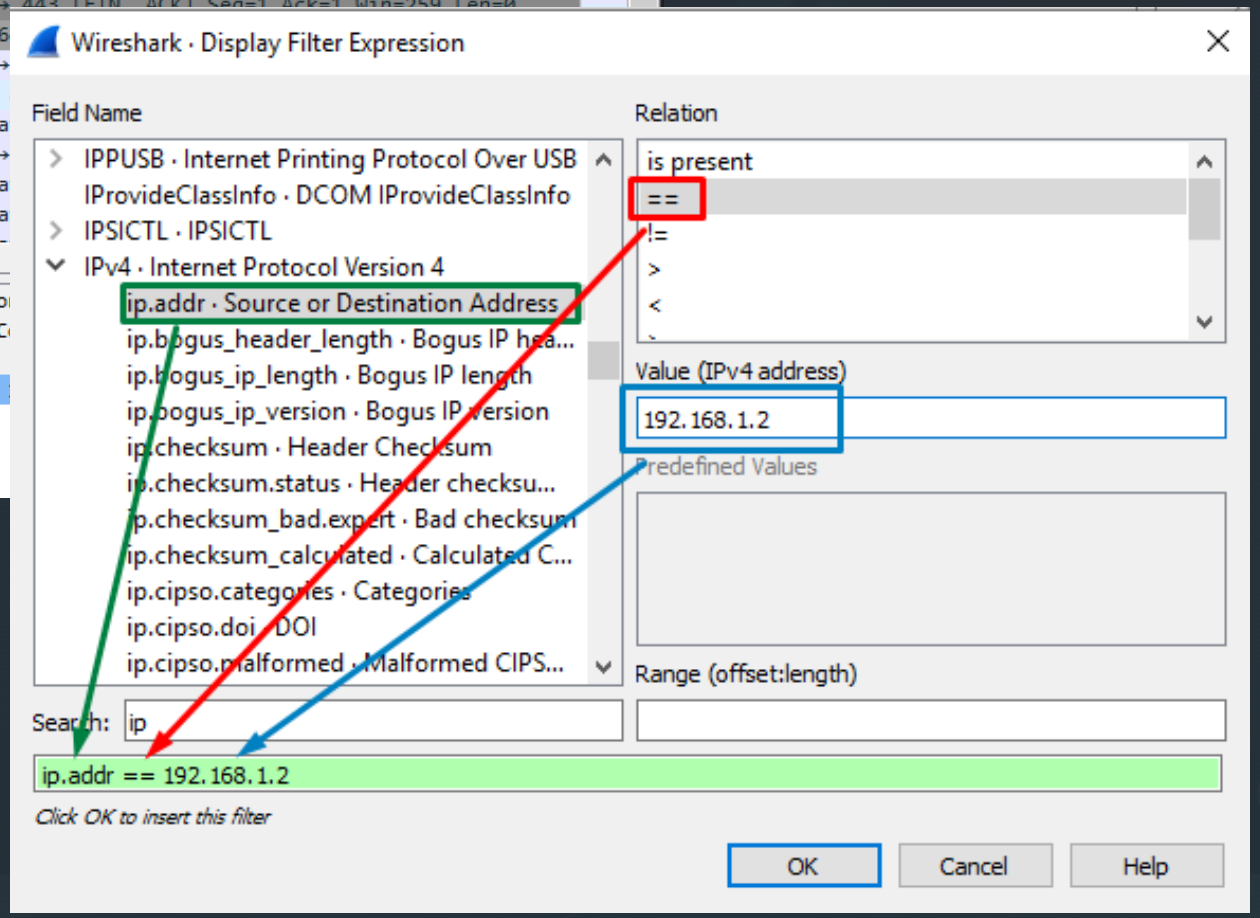
Filtering packets | while capturing (ποια πακέτα γίνονται captured)



Επιλογή φίλτρου πριν ξεκινήσουμε το capturing

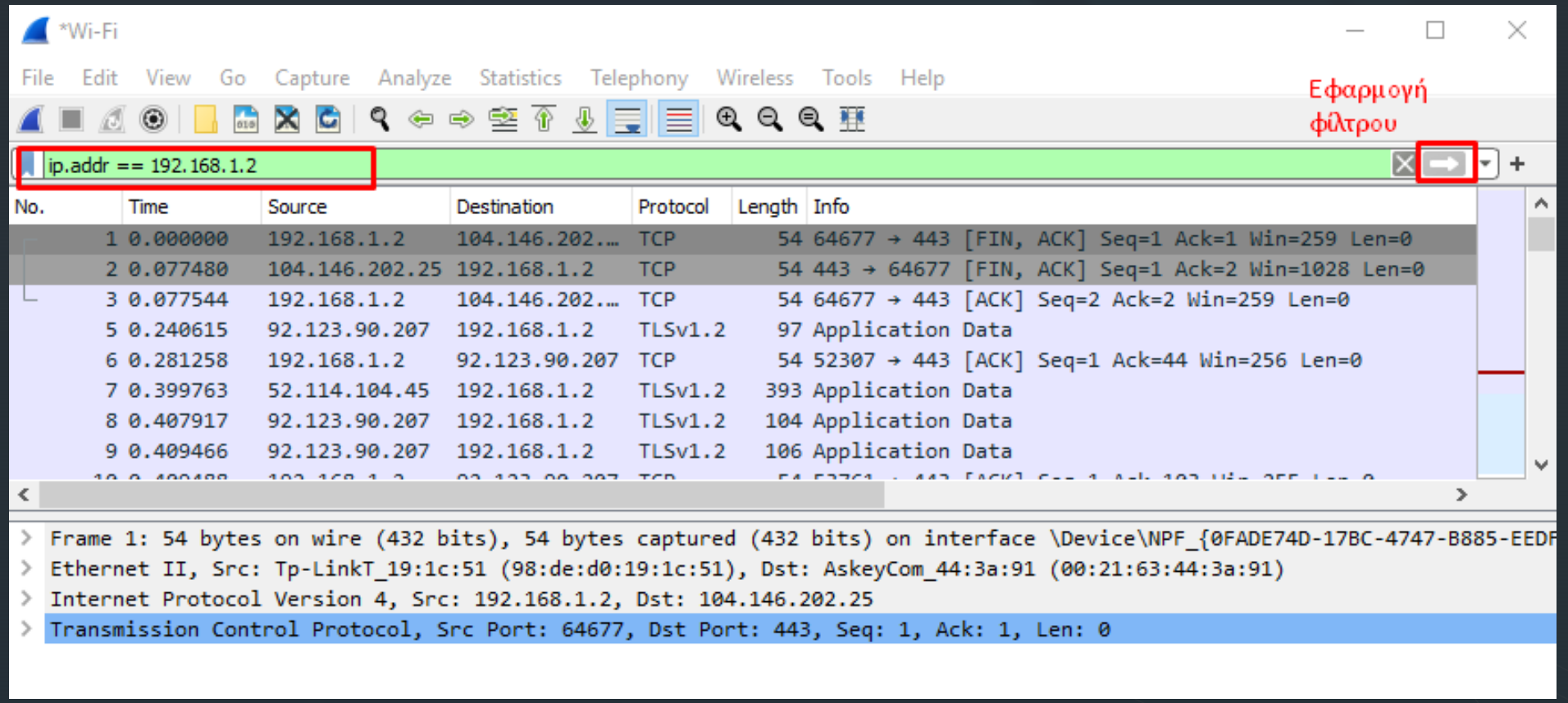
Filtering packets | while analyzing (ποια captured πακέτα εμφανίζονται)





Field Name: all supported protocols headers fields

Filtering packets | while analyzing (εφαρμογή του φίλτρου)



Παραδείγματα φίλτρων

- Κίνηση μόνο από/προς την IP διεύθυνση: 104.146.202.25

```
ip.host == "104.146.202.25"
```

- Κίνηση από/προς ένα εύρος (range) IP διευθύνσεων

```
ip.addr==192.168.0.0/16
```

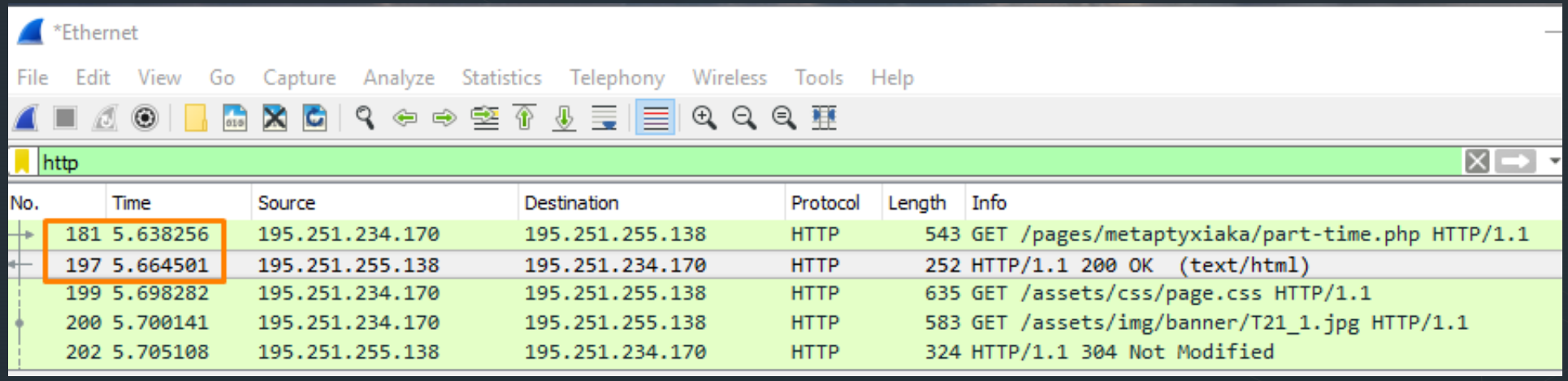
- HTTP κίνηση (well known port: 80, tcp)

```
tcp.port==80
```

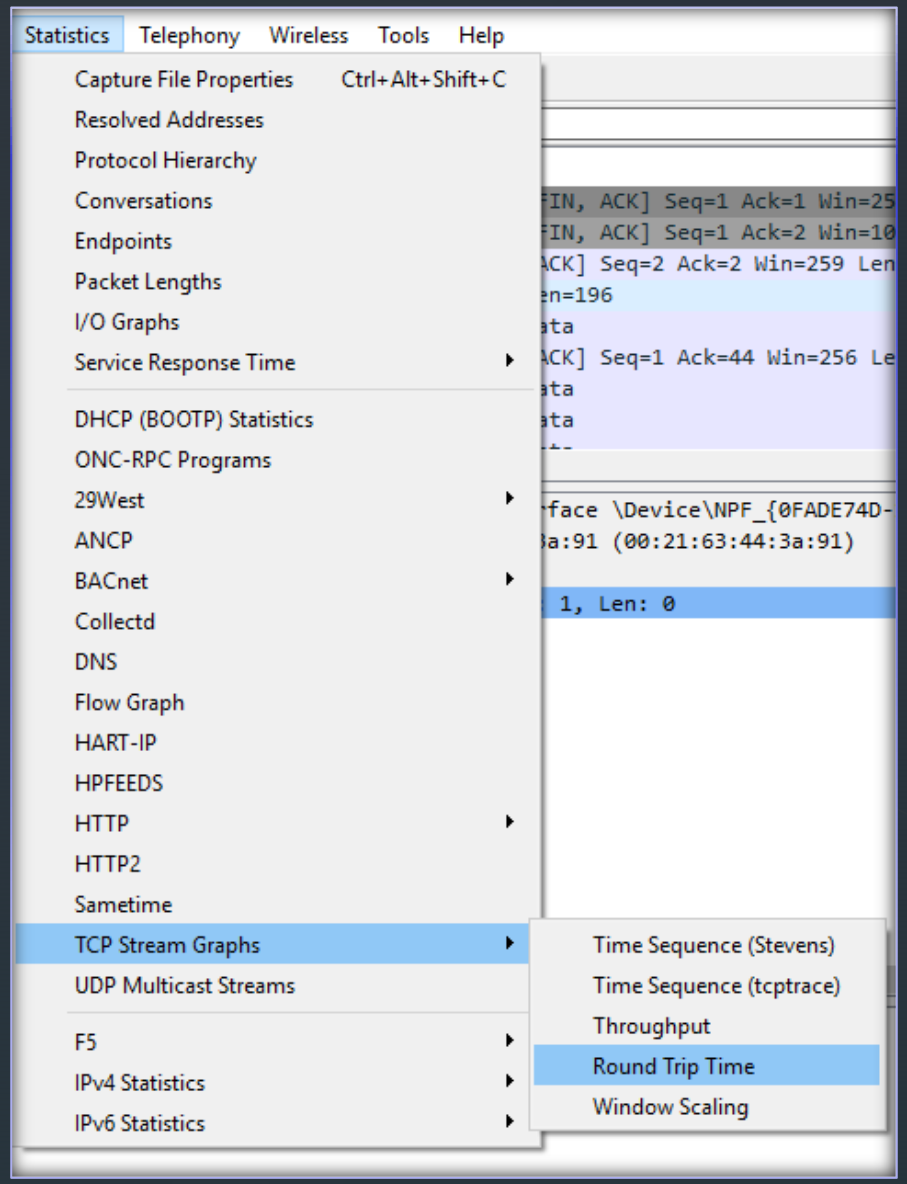
- Capturing filters: https://gitlab.com/wireshark/wireshark/-/wikis/CaptureFilters
- Displaying filter: https://gitlab.com/wireshark/wireshark/-/wikis/DisplayFilters

Τι μπορεί να κάνει το WireShark

- Ανάλυση της λειτουργίας ενός πρωτοκόλλου
- Απλό παράδειγμα: ποιο είναι το RTT (Round Trip Time) ενός HTTP request?
  - Time του GET message (No 181)
  - Time του response message (No 197)

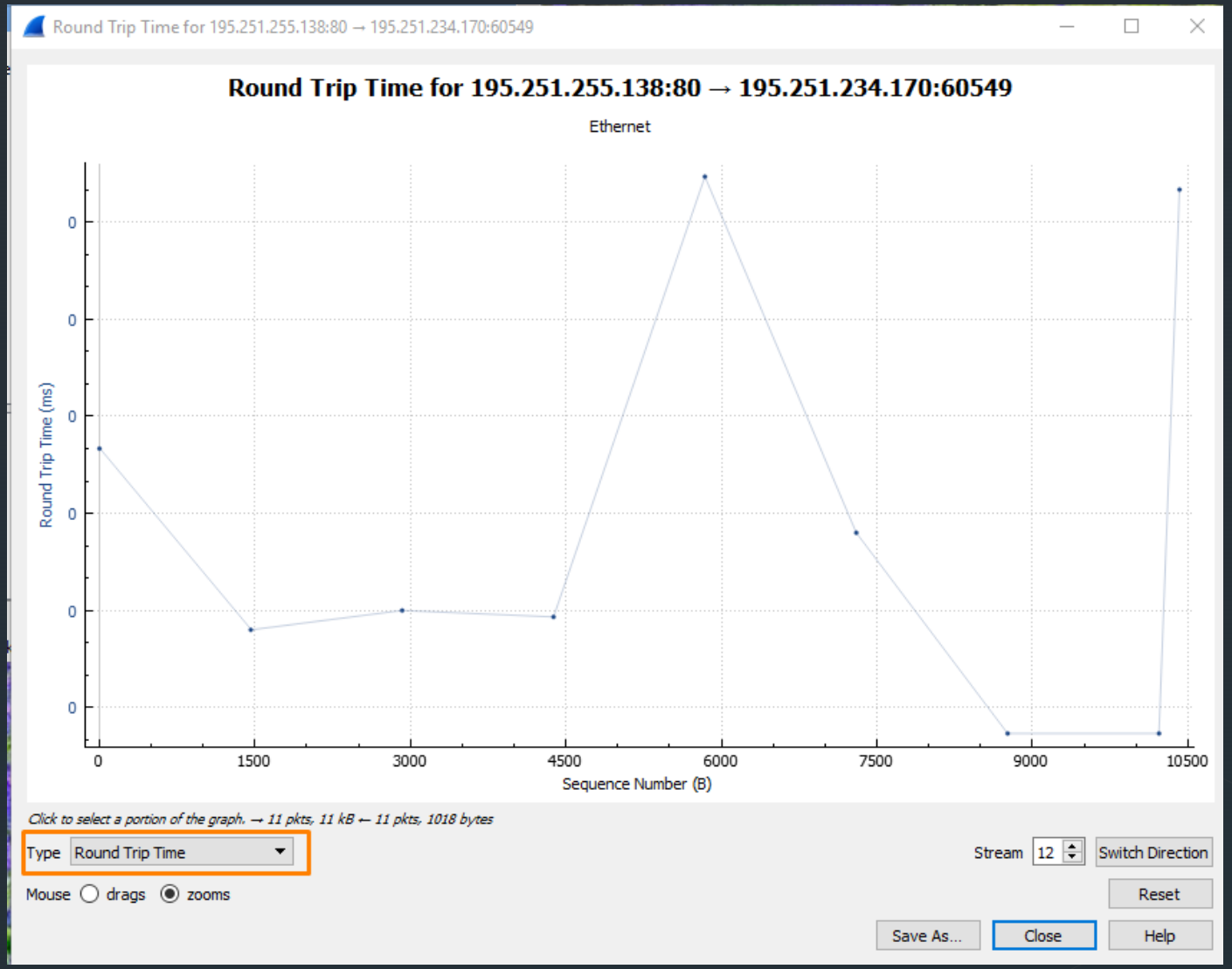


Τι μπορεί να κάνει το WireShark (2)

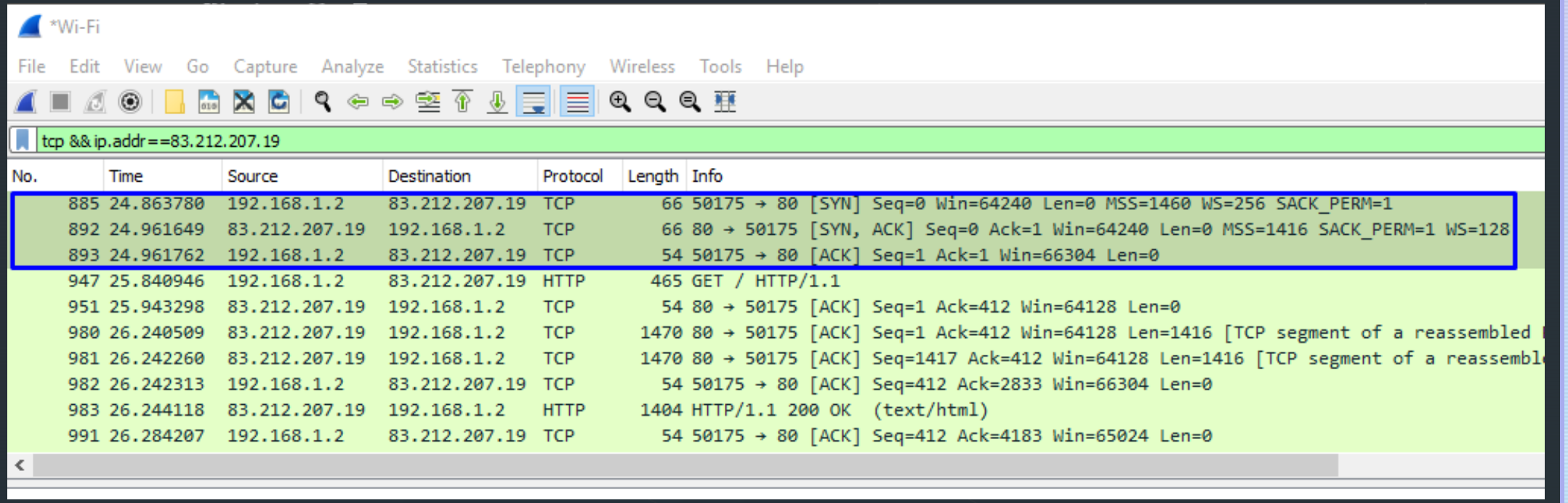


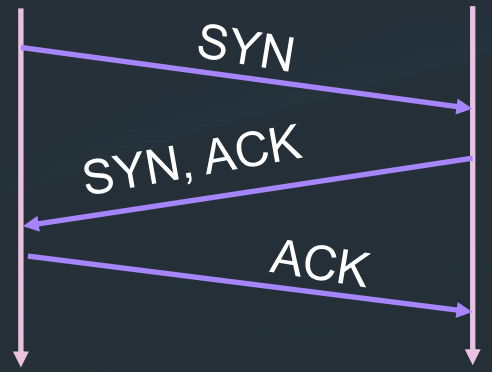
- Πιο πολύπλοκο παράδειγμα: ποιο είναι το RTT ενός TCP segment?
  - το TCP στέλνει πολλά segments μέχρι να ληφθεί επιβεβαίωση (ACK)
  - Δεν είναι εύκολο να βρει κανείς ποια μηνύματα σχετίζονται
  - Το WireShark μπορεί να το κάνει (Statistics | TCP streams graph)

RTT for TCP stream

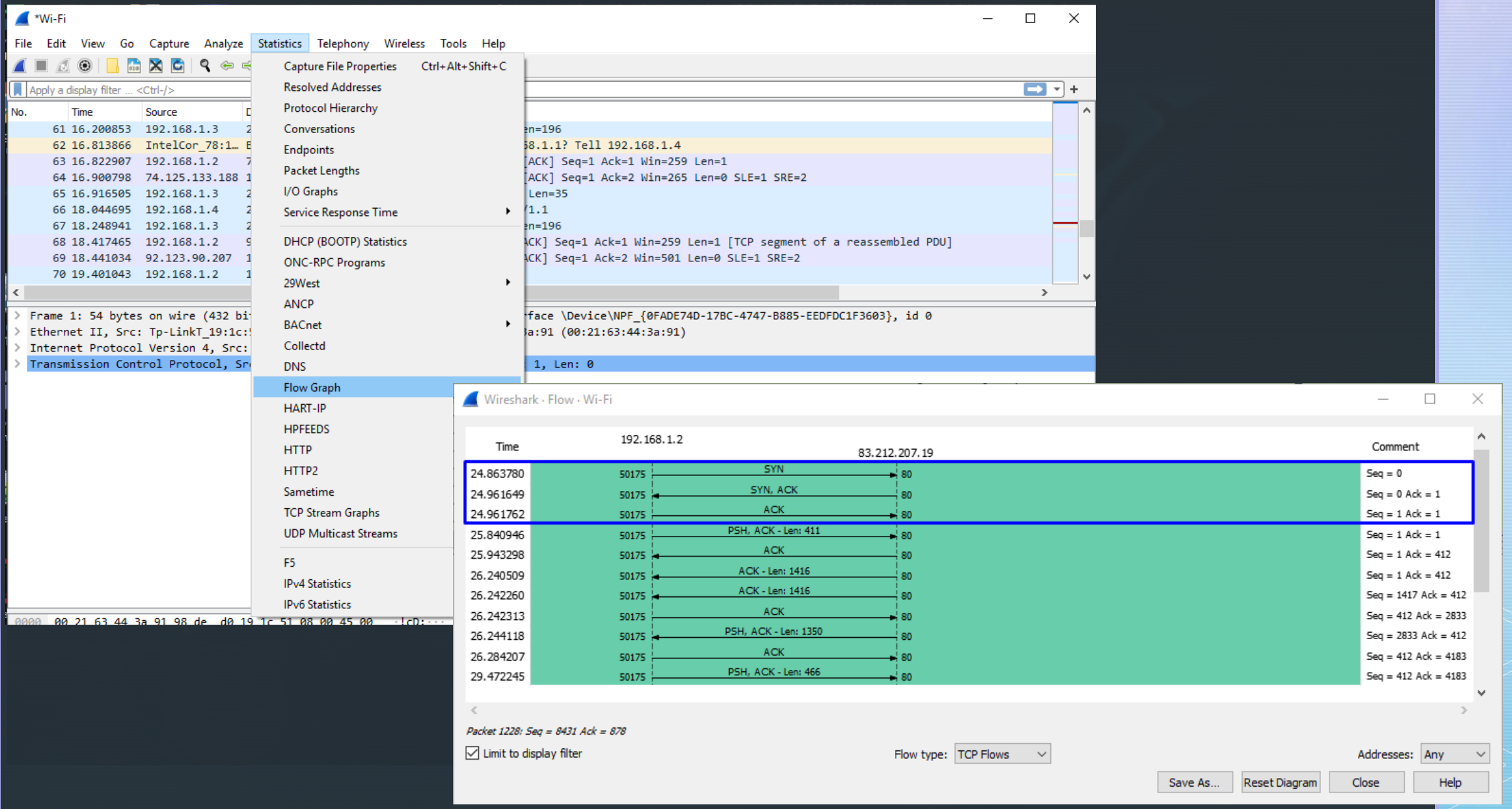


TCP 3-way Handshake

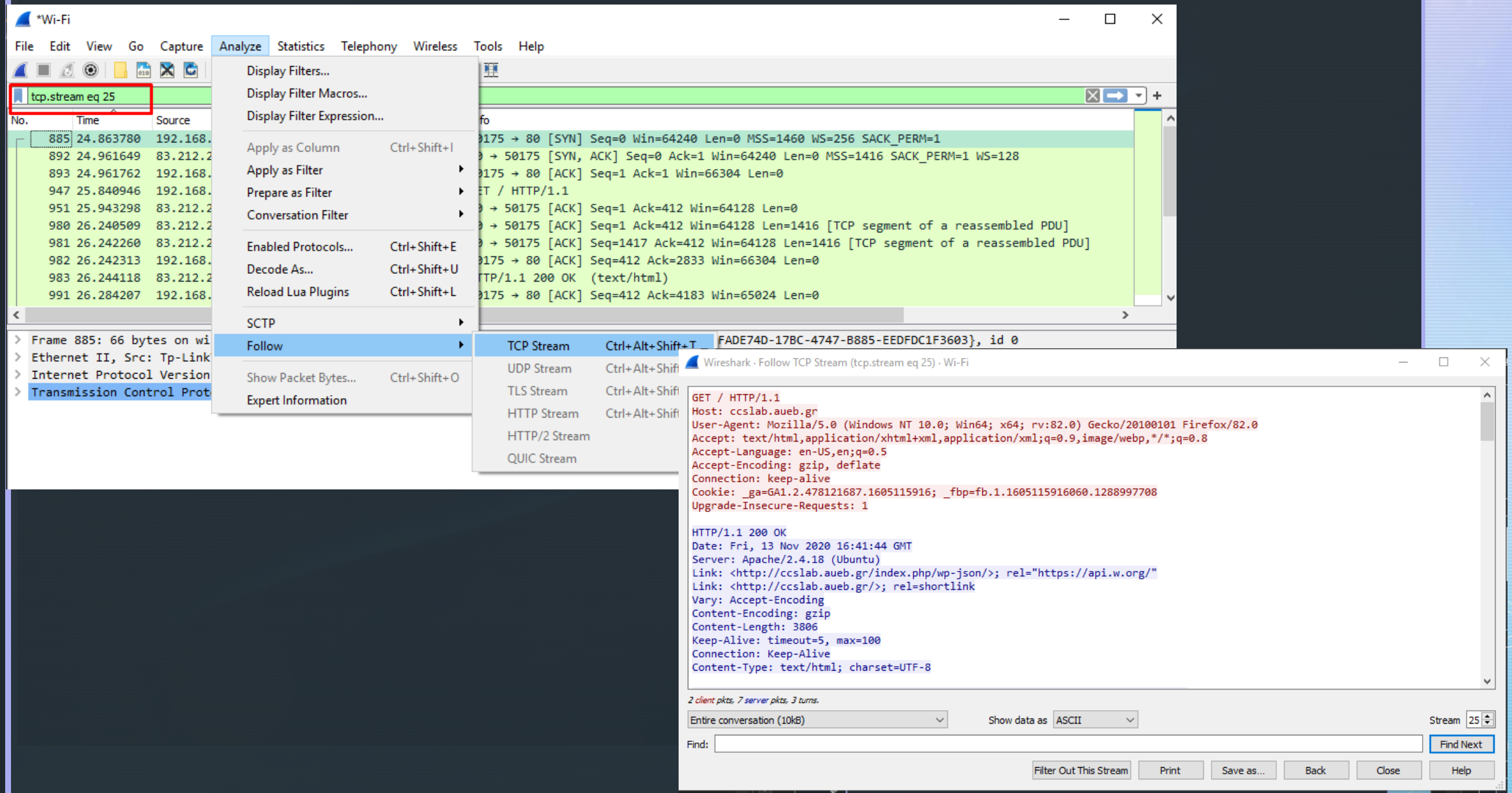




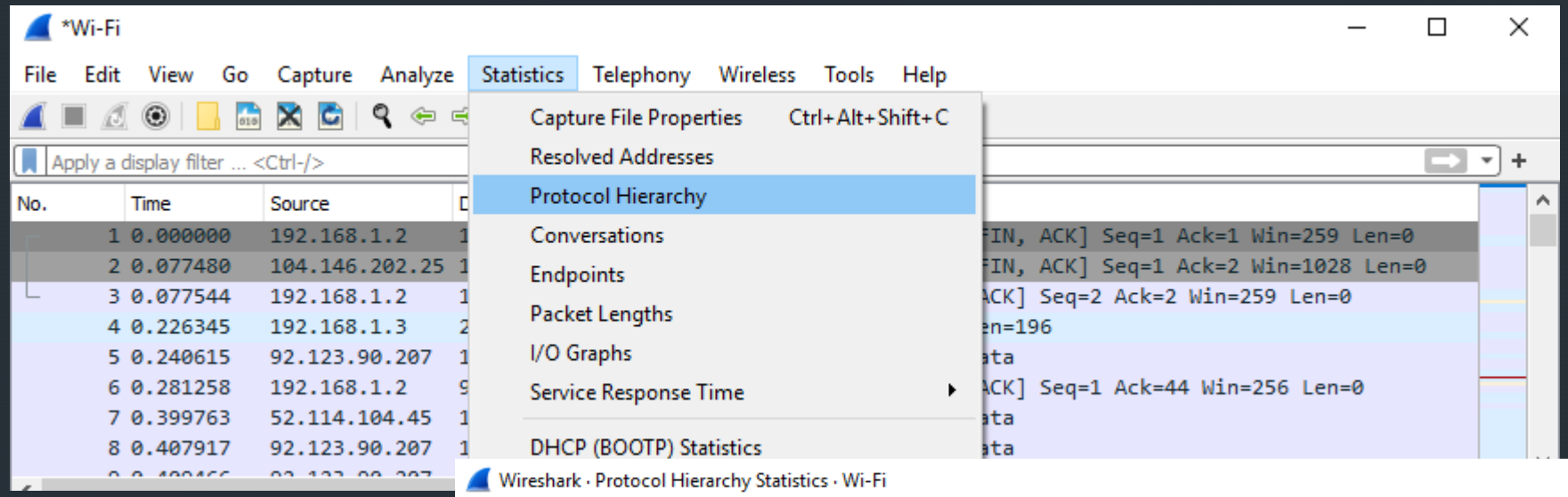
Statistics | Flow Graph

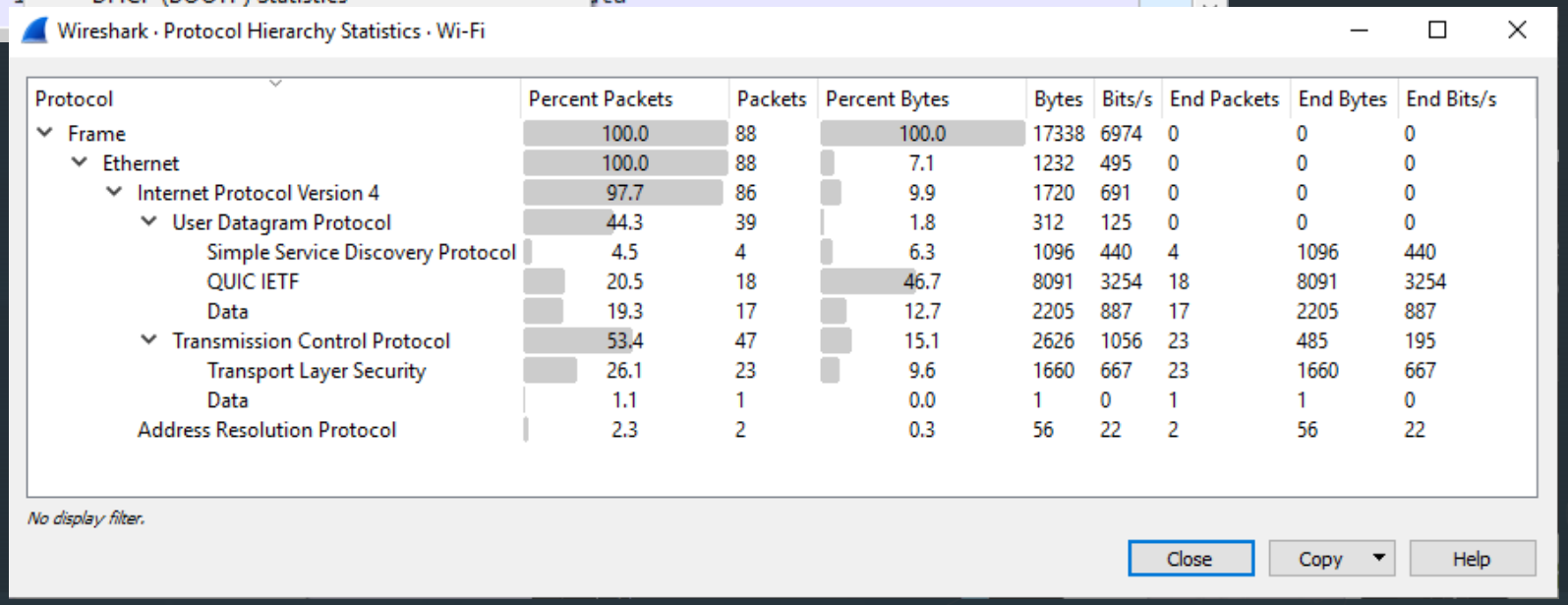


Analyze | Follow TCP stream

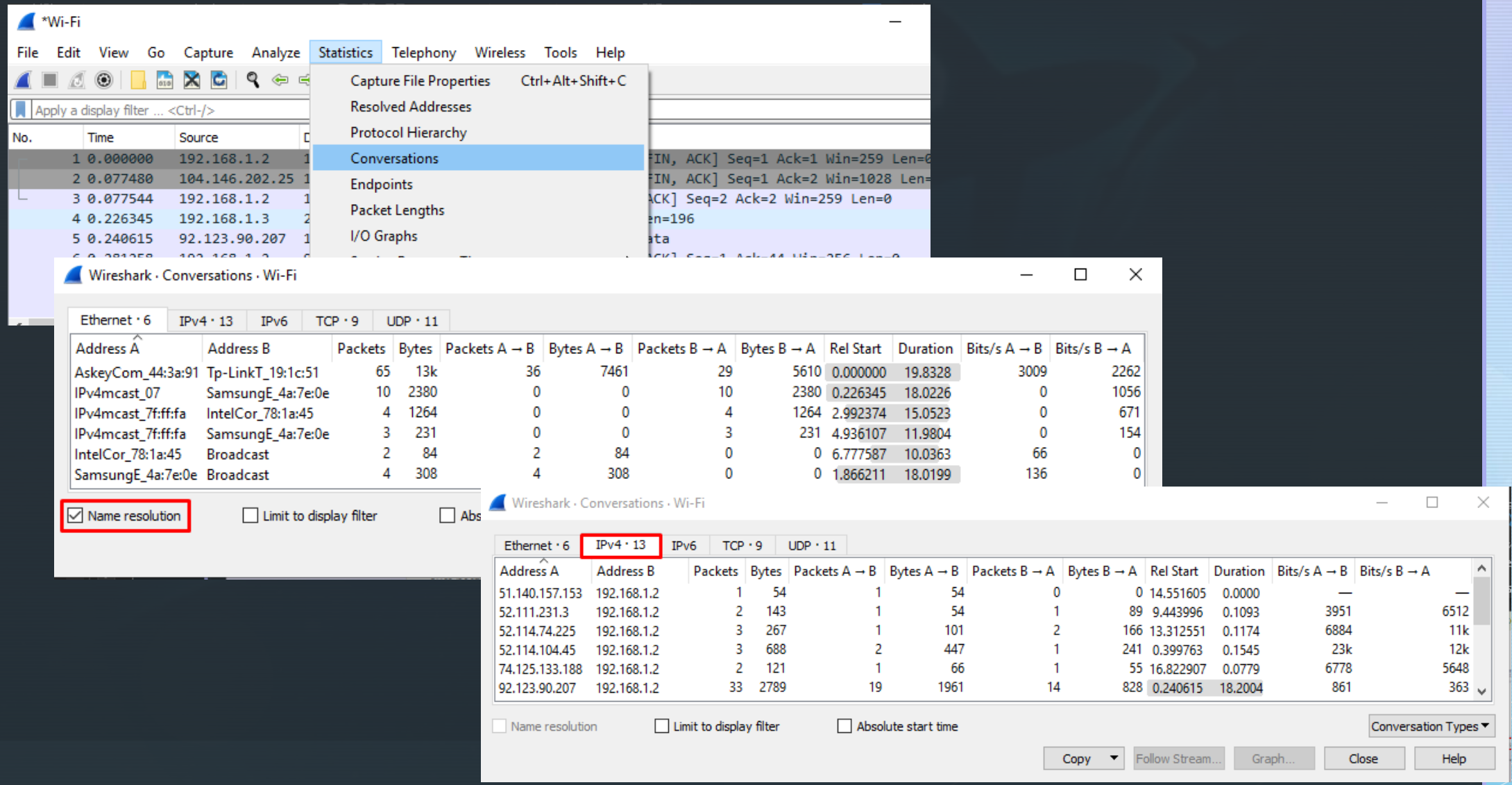


Statistics | Protocol Hierarchy

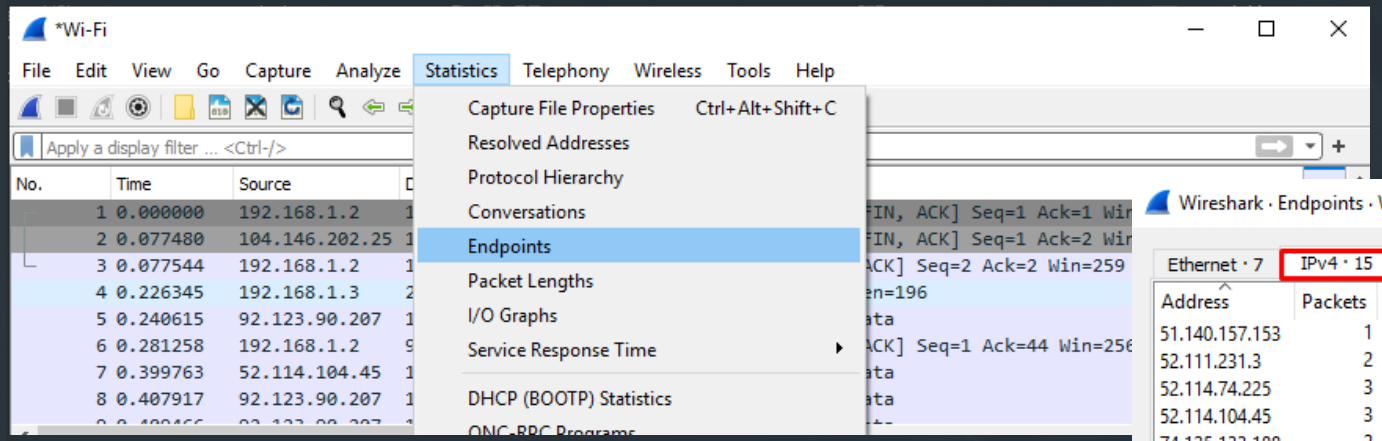


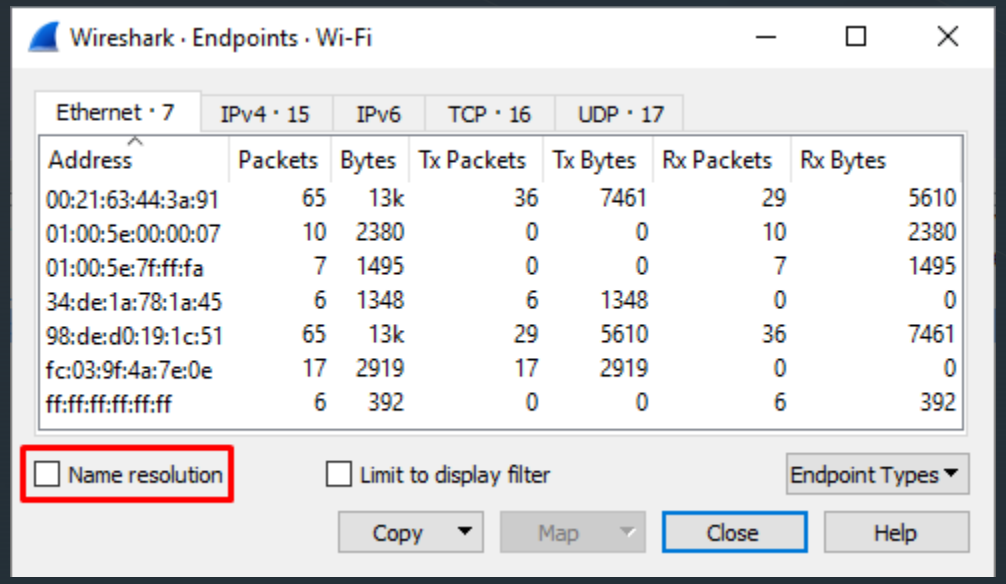


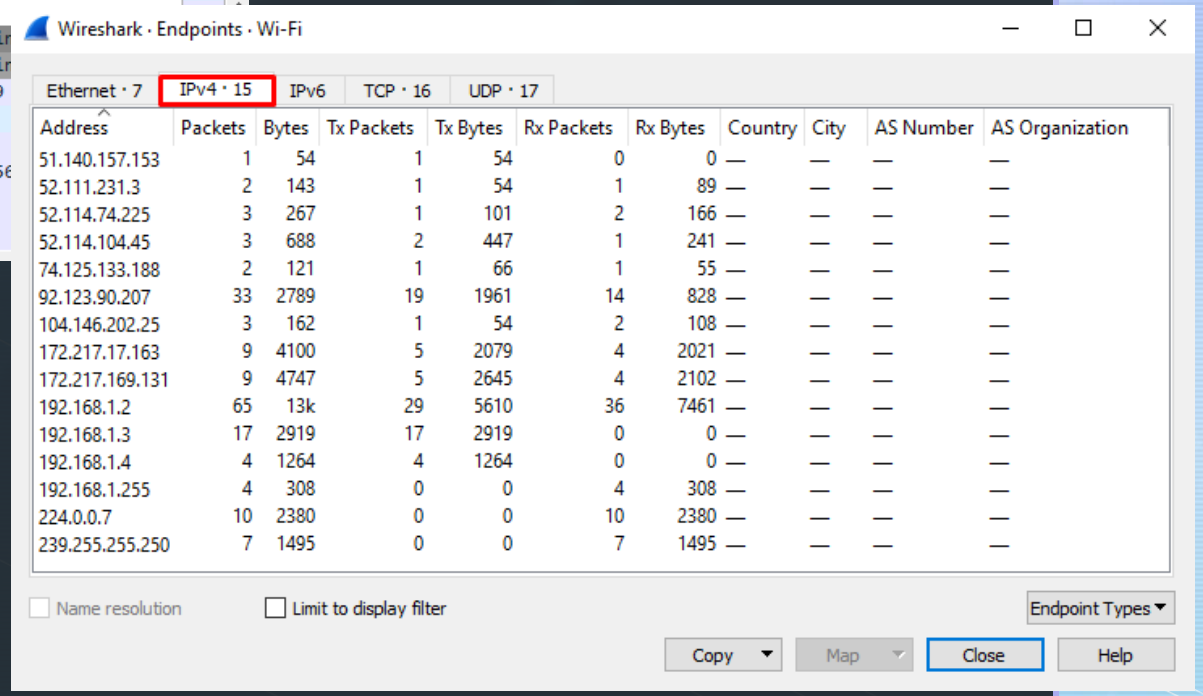
Statistics | Conversations



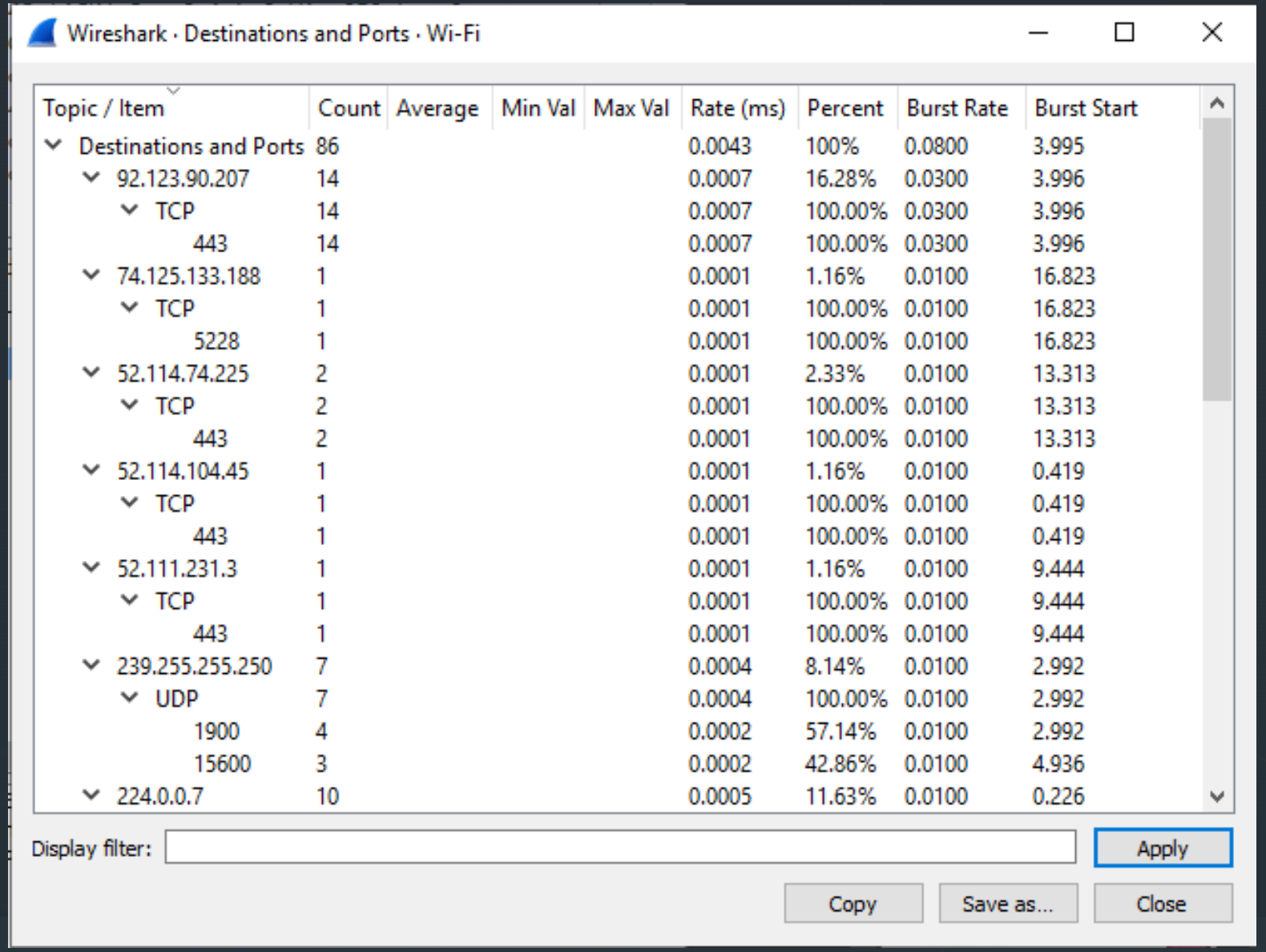
Statistics | Endpoints







Statistics | IPv4 Statistics | Destinations & Ports



Wireshark | Color Coding (while listing packets)

Color in Wireshark	Packet Type
Light purple	TCP
Light blue	UDP
Black	Packets with errors
Light green	HTTP traffic
Light yellow	Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS
Dark yellow	Routing
Dark gray	TCP SYN, FIN and ACK traffic