



Δρ. Άννα Κεφάλια

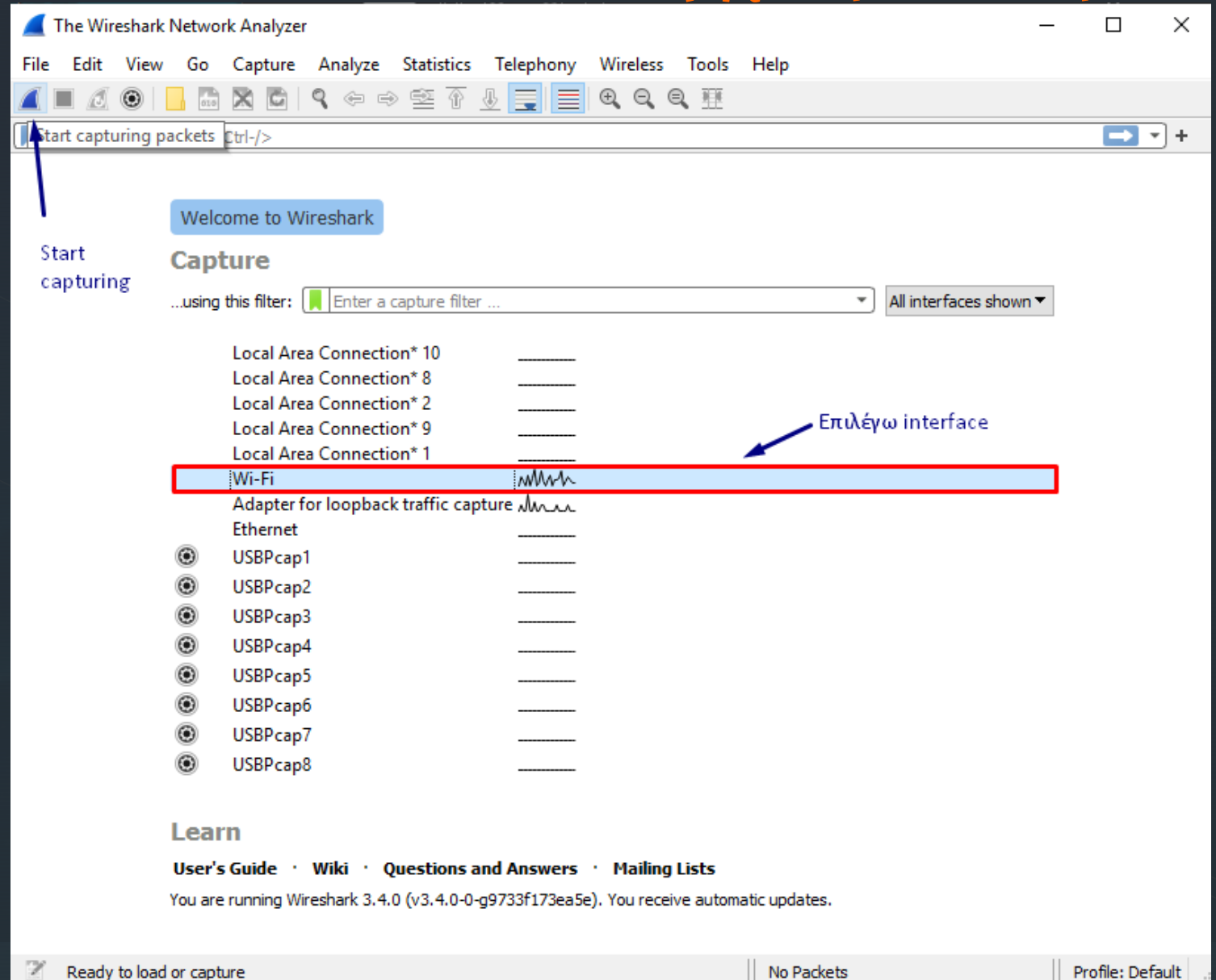
WireShark
(a network protocol analyser)

WireShark Specifics



Αρχική οθόνη

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



menus εντολών

προσδιορισμός φίλτρου

λίστα με captured
πακέτα

λεπτομέρειες
επιλεγμένου
πακέτου

δεδομένα πακέτου
σε HEX και ASCII
μορφή

*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
268	7.507364	108.177.15.189	192.168.1.2	UDP	70	443 → 63888 Len=28
269	7.509607	52.114.132.23	192.168.1.2	TCP	54	443 → 59797 [ACK] Seq=6349 Ack
270	7.514054	192.168.1.2	74.125.133.189	UDP	75	52257 → 443 Len=33
271	7.532082	52.114.132.23	192.168.1.2	TLSv1.2	481	Application Data
272	7.532189	192.168.1.2	52.114.132.23	TCP	54	59797 → 443 [ACK] Seq=5087 Ack
273	7.622222	74.125.133.189	192.168.1.2	UDP	70	443 → 52257 Len=28
274	7.709055	192.168.1.2	108.177.15.189	UDP	75	63888 → 443 Len=33
275	7.824100	192.168.1.2	74.125.133.189	UDP	75	52257 → 443 Len=33

> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-E...}

> Ethernet II, Src: Tp-LinkT_19:1c:51 (98:de:d0:19:1c:51), Dst: AskeyCom_44:3a:91 (00:21:63:44:3a:91)

> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 172.217.169.142

> User Datagram Protocol, Src Port: 50377, Dst Port: 443

> Data (33 bytes)

```

0000  00 21 63 44 3a 91 98 de d0 19 1c 51 08 00 45 00  ·!cD:··· ···Q··E·
0010  00 3d 1f 9a 40 00 80 11 c3 03 c0 a8 01 02 ac d9  ···@··· ········
0020  a9 8e c4 c9 01 bb 00 29 38 e3 42 c1 68 43 07 68  ······) 8·B·hC·h
0030  e0 2a b0 56 8f 2c fd 81 e1 8f 17 87 c9 17 cd eb  ·*·V·,·· ········
0040  46 dd 5c 6a e0 1a 34 a4 bb 63 15                F·\j···4· ·c·
  
```

wireshark_Wi-FIKQYVT0.pcapng | Packets: 282 · Displayed: 282 (100.0%) | Profile: Default

menus εντολών

προσδιορισμός φίλτρου

λίστα με captured
πακέτα

λεπτομέρειες
επικεφαλίδων
επιλεγμένου
πακέτου

The screenshot shows the Wireshark interface with the following components:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Filter Bar:** Apply a display filter ... <Ctrl-/>
- Packet List:** A table with columns: No., Time, Source, Destination, Protocol, Length, Info.

No.	Time	Source	Destination	Protocol	Length	Info
46	1.287948	192.168.9.29	175.12.160.11	TCP	60	63019 → 52909 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=6
47	1.287967	192.168.9.29	81.83.210.177	TCP	60	63017 → 16881 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=6
48	1.287966	192.168.9.29	176.212.185.184	BitTor...	71	Continuation data
49	1.287982	192.168.9.29	81.185.26.30	TCP	60	63021 → 14043 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=6
50	1.288044	192.168.9.29	135.125.233.219	BitTor...	60	Continuation data
51	1.324826	45.66.185.228	192.168.9.29	BT-DHT	146	Get_peers Info_hash=1e3c459dc9869e7b6926fbad5b038ea0c9e2cf1f
52	1.325235	192.168.9.29	45.66.185.228	BT-DHT	352	Response Nodes=8
53	1.350431	81.83.210.177	192.168.9.29	TCP	60	16881 → 63017 [ACK] Seq=1 Ack=7 Win=229 Len=0
54	1.356700	176.212.185.184	192.168.9.29	TCP	60	6881 → 63018 [ACK] Seq=1 Ack=18 Win=166 Len=0
55	1.366827	135.125.233.219	192.168.9.29	TCP	60	6881 → 63022 [ACK] Seq=1 Ack=7 Win=115 Len=0
56	1.435503	176.212.185.184	192.168.9.29	TCP	60	6881 → 63018 [FIN, ACK] Seq=1 Ack=18 Win=166 Len=0
57	1.435565	192.168.9.29	176.212.185.184	TCP	54	63018 → 6881 [ACK] Seq=18 Ack=2 Win=516 Len=0
58	1.435642	192.168.9.29	176.212.185.184	TCP	54	63018 → 6881 [FIN, ACK] Seq=18 Ack=2 Win=516 Len=0
59	1.481936	HewlettPacka_0c:74:...	All-FCF-MACs	FIP	60	VLAN Request
60	1.504148	176.212.185.184	192.168.9.29	TCP	60	6881 → 63018 [ACK] Seq=2 Ack=19 Win=166 Len=0
61	1.534701	156.146.60.136	192.168.9.29	BT-DHT	146	Get_peers Info_hash=ce57009ec79a2a388349f77eb97d7503506a7fe4
- Packet Details:**
 - > Frame 91: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{343BB1...}
 - > Ethernet II, Src: Fortinet_09:0f:12 (00:09:0f:09:0f:12), Dst: FujitsuTechn_05:cf:f6 (90:1b:0e:05:cf:f6)
 - > Internet Protocol Version 4, Src: 216.58.205.42, Dst: 192.168.9.29
 - > User Datagram Protocol, Src Port: 443, Dst Port: 61546
 - > Data (77 bytes)
- Packet Bytes:**

```

0000  90 1b 0e 05 cf f6 00 09 0f 09 0f 12
0010  00 69 00 00 40 00 3a 11 d0 b5 d8 3a
0020  09 1d 01 bb f0 6a 00 55 a1 6d 4c 7a
0030  4c 4c 90 2d ea cb 1a db 5f db d5 1f
0040  c8 d9 4f f8 60 9f cf f7 b1 38 2e 42
0050  09 2c e5 69 61 b3 af 3d 44 8e e3 17
0060  7b 22 53 0f 51 e1 d8 de 16 c9 6a a7
0070  6d a7 df 94 f2 02 7a

```

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

διαφορετικά
πρωτόκολλα
ενσωματώνονται
μέσα σε ένα πακέτο



No.	Time	Source	Destination	Protocol	Length	Info
268	7.507364	108.177.15.189	192.168.1.2	UDP	70	443 → 63888 Len=28
269	7.509607	52.114.132.23	192.168.1.2	TCP	54	443 → 59797 [ACK] Seq=6349 Ack
270	7.514054	192.168.1.2	74.125.133.189	UDP	75	52257 → 443 Len=33
271	7.532082	52.114.132.23	192.168.1.2	TLSv1.2	481	Application Data
272	7.532189	192.168.1.2	52.114.132.23	TCP	54	59797 → 443 [ACK] Seq=5087 Ack
273	7.622222	74.125.133.189	192.168.1.2	UDP	70	443 → 52257 Len=28
274	7.709055	192.168.1.2	108.177.15.189	UDP	75	63888 → 443 Len=33
275	7.824100	192.168.1.2	74.125.133.189	UDP	75	52257 → 443 Len=33

> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-E...
 > Ethernet II, Src: Tp-LinkT_19:1c:51 (98:de:d0:19:1c:51), Dst: AskeyCom_44:3a:91 (00:21:63:44:3a:91)
 > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 172.217.169.142
 > User Datagram Protocol, Src Port: 50377, Dst Port: 443
 > Data (33 bytes)

```

0000  00 21 63 44 3a 91 98 de d0 19 1c 51 08 00 45 00  ·!cD:··· ···Q··E·
0010  00 3d 1f 9a 40 00 80 11 c3 03 c0 a8 01 02 ac d9  ·=··@··· ········
0020  a9 8e c4 c9 01 bb 00 29 38 e3 42 c1 68 43 07 68  ······) 8·B·hC·h
0030  e0 2a b0 56 8f 2c fd 81 e1 8f 17 87 c9 17 cd eb  ·*·V··· ········
0040  46 dd 5c 6a e0 1a 34 a4 bb 63 15                F·\j··4· ·c·
  
```

wireshark_Wi-FiKQYVT0.pcapng | Packets: 282 · Displayed: 282 (100.0%) | Profile: Default

▶ 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)

The image shows a Wireshark network traffic capture window. The top part displays a list of captured packets. The bottom part shows a detailed view of a selected frame (Frame 271).

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-EEDFDC1F3603}

- > 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]

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (No. 271) is a TLSv1.2 packet. The detailed view below shows the following structure:

- 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)

Wireshark interface showing network traffic capture. The packet list pane displays several packets, with packet 271 selected. The packet details pane shows the structure of the selected packet, which is an Internet Protocol Version 4 packet.

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

Packet 271 details:

- Frame 271: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-B8...}
- 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)
- Internet Protocol Version 4, Src: 52.114.132.23, Dst: 192.168.1.2
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 467
 - Identification: 0x50b9 (20665)
 - Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 111
 - Protocol: TCP (6)
 - Header Checksum: 0x3f38 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 52.114.132.23
 - Destination Address: 192.168.1.2
 - Transmission Control Protocol, Src Port: 443, Dst Port: 59797, Seq: 6349, Ack: 5087, Len: 427

Transmission Control Protocol

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The main pane displays a list of captured packets. Packet 3 is selected, and its details pane is expanded to show the Transmission Control Protocol (TCP) segment. Several fields in the details pane are highlighted with blue boxes.

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

Details of the selected packet (No. 3):

- Frame 271: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-B88}
- 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)
- 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
 - Source Port: 443
 - Destination Port: 59797
 - [Stream index: 14]
 - [TCP Segment Len: 427]
 - Sequence Number: 6349 (relative sequence number)
 - Sequence Number (raw): 2605853786
 - [Next Sequence Number: 6776 (relative sequence number)]
 - Acknowledgment Number: 5087 (relative ack number)
 - Acknowledgment number (raw): 746573450
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window: 1023
 - [Calculated window size: 261888]
 - [Window size scaling factor: 256]
 - Checksum: 0x2dc9 [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0

Filtering packets | while capturing (ποια πακέτα γίνονται captured)

Επιλογή φίλτρου πριν
ξεκινήσουμε το capturing

The screenshot shows the Wireshark interface with the 'Capture Filters...' dialog box open. The dialog box contains a list of filter expressions and their corresponding filter names. The filter expressions are:

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

The dialog box also includes buttons for '+', '-', and 'Reset' at the bottom left, and 'OK', 'Cancel', and 'Help' at the bottom right.

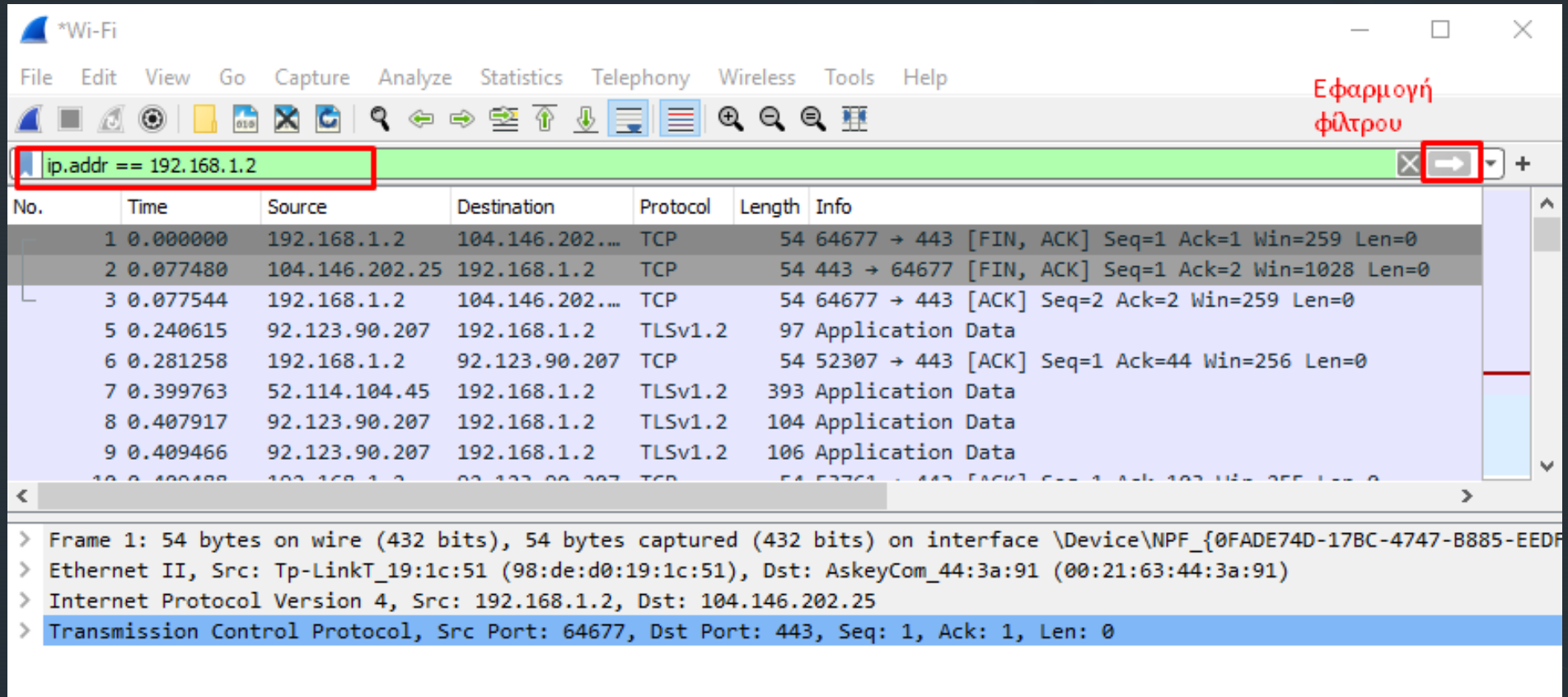
Filtering packets | while analyzing (ποια captured πακέτα εμφανίζονται)

The screenshot shows the Wireshark interface with the 'Display Filter Expression' dialog box open. The dialog box contains the following information:

- Field Name:** A list of fields is shown, with 'ip.addr · Source or Destination Address' selected and highlighted in green.
- Relation:** The relation '==' is selected and highlighted in red.
- Value (IPv4 address):** The value '192.168.1.2' is entered in the text box and highlighted in blue.
- Predefined Values:** An empty list box for predefined values.
- Range (offset:length):** An empty text box for range specification.
- Search:** The search term 'ip' is entered in the search box.
- Result:** The final filter expression 'ip.addr == 192.168.1.2' is displayed in a green box at the bottom of the dialog.

Below the dialog box, a purple callout box contains the text: "Field Name: all supported protocols headers fields".

Filtering packets | while analyzing (εφαρμογή του φίλτρου)



The screenshot shows the Wireshark interface with the filter `ip.addr == 192.168.1.2` applied. The filter is highlighted in green, and a red box highlights the filter text and a red arrow pointing to the filter icon. The packet list shows several packets, and the packet details pane shows the structure of the first packet.

Εφαρμογή φίλτρου

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	104.146.202.25	TCP	54	64677 → 443 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0
2	0.077480	104.146.202.25	192.168.1.2	TCP	54	443 → 64677 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
3	0.077544	192.168.1.2	104.146.202.25	TCP	54	64677 → 443 [ACK] Seq=2 Ack=2 Win=259 Len=0
5	0.240615	92.123.90.207	192.168.1.2	TLSv1.2	97	Application Data
6	0.281258	192.168.1.2	92.123.90.207	TCP	54	52307 → 443 [ACK] Seq=1 Ack=44 Win=256 Len=0
7	0.399763	52.114.104.45	192.168.1.2	TLSv1.2	393	Application Data
8	0.407917	92.123.90.207	192.168.1.2	TLSv1.2	104	Application Data
9	0.409466	92.123.90.207	192.168.1.2	TLSv1.2	106	Application Data
10	0.409488	192.168.1.2	92.123.90.207	TCP	54	52307 → 443 [ACK] Seq=1 Ack=103 Win=256 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0FADE74D-17BC-4747-B885-EEDF...}

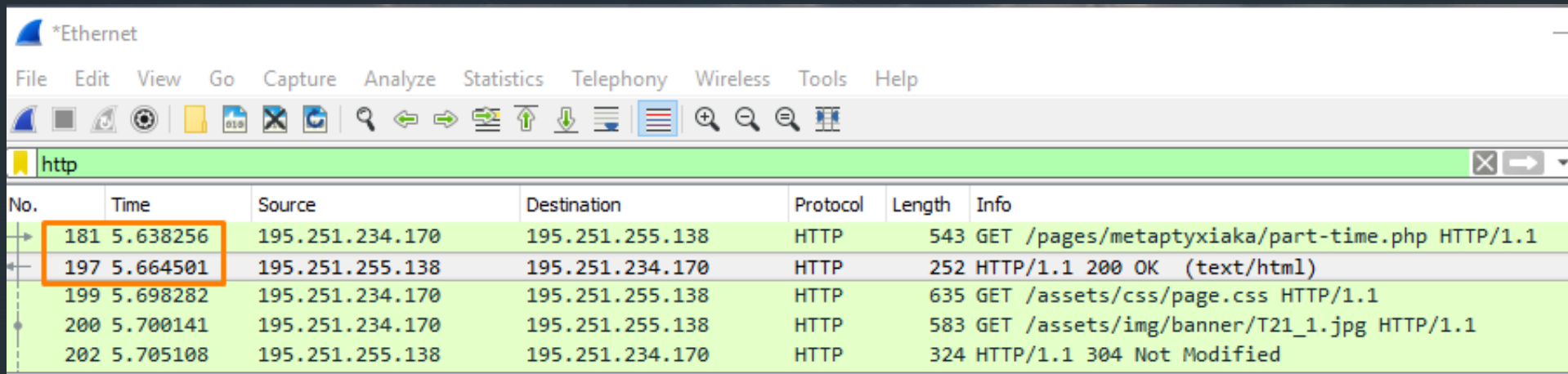
- Ethernet II, Src: Tp-LinkT_19:1c:51 (98:de:d0:19:1c:51), Dst: AskeyCom_44:3a:91 (00:21:63:44:3a:91)
- Internet Protocol Version 4, Src: 192.168.1.2, Dst: 104.146.202.25
- Transmission Control Protocol, Src Port: 64677, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

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>

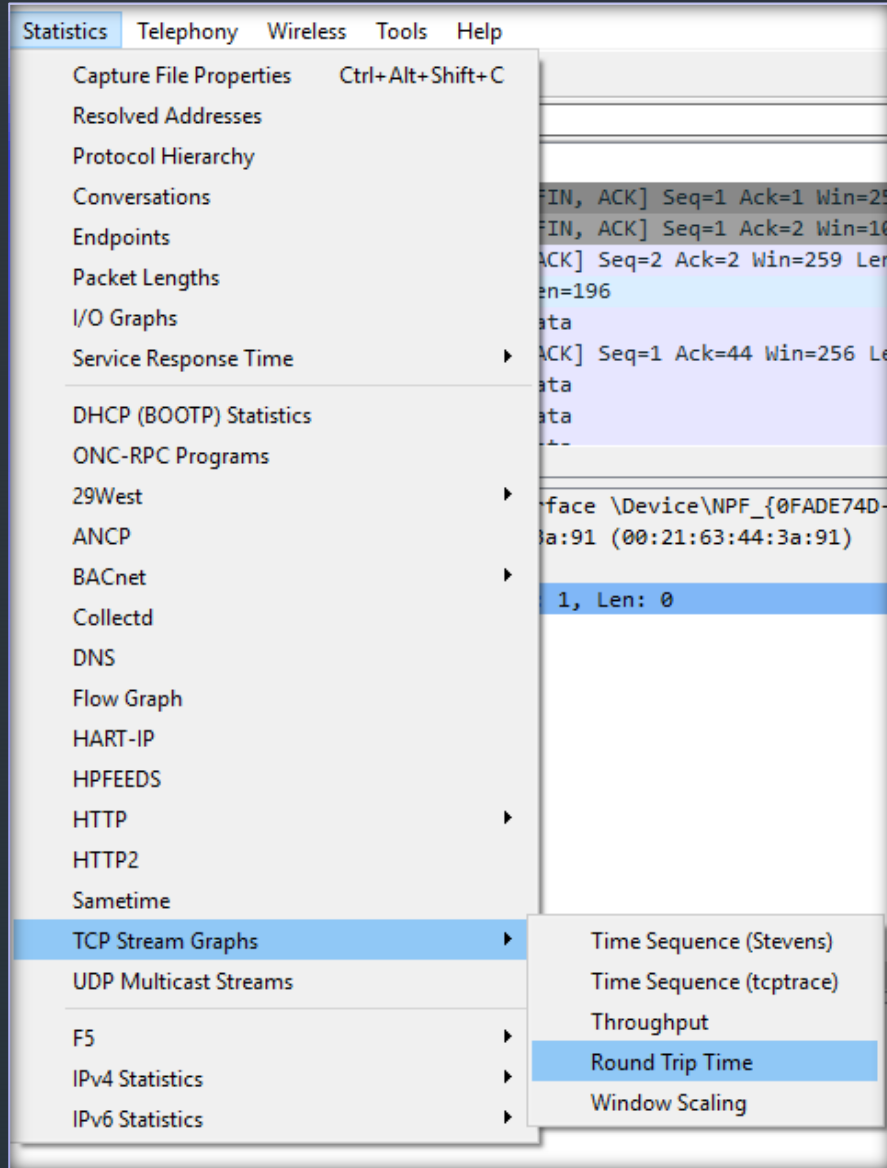
Τι μπορεί να κάνει το Wireshark

- 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)



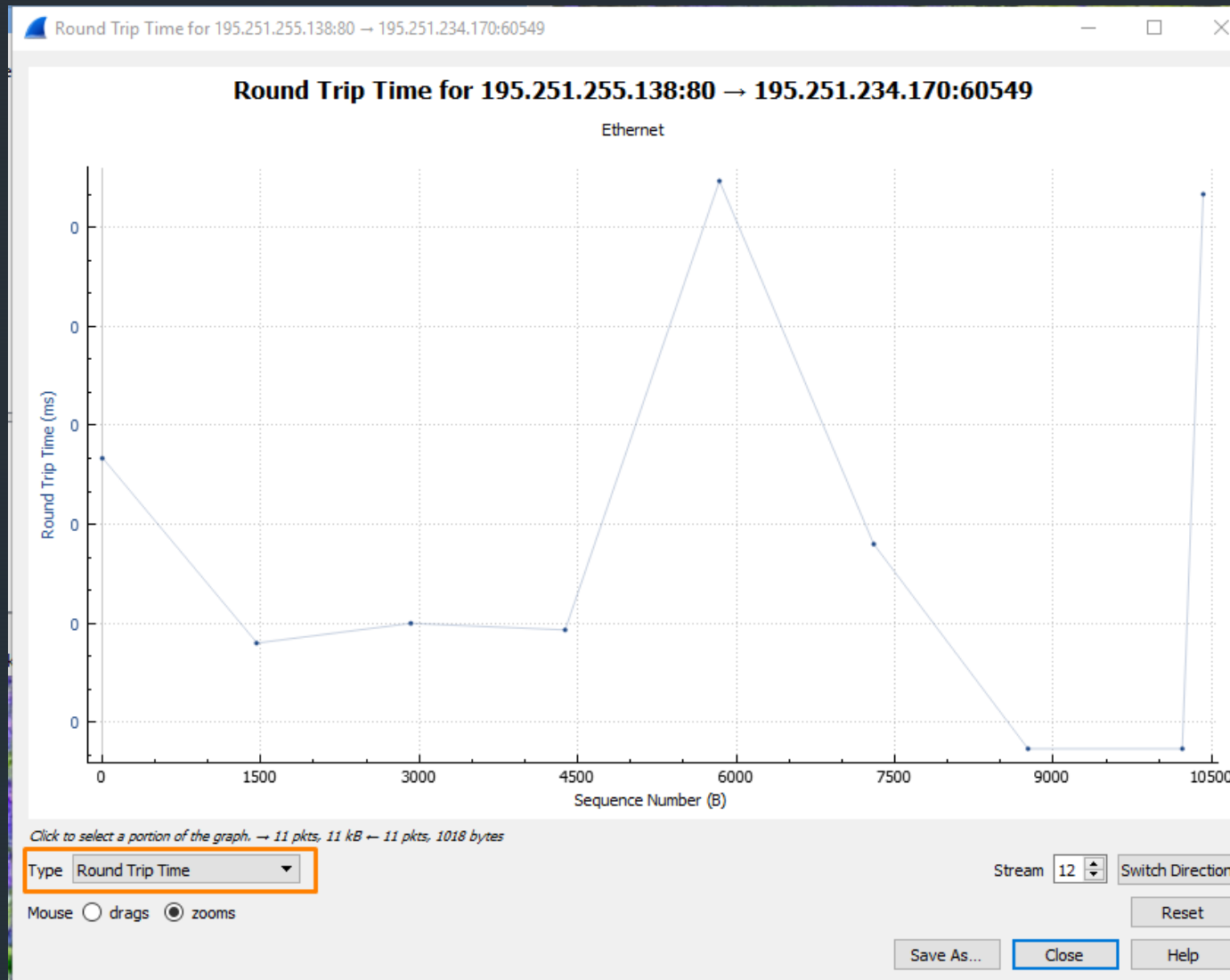
No.	Time	Source	Destination	Protocol	Length	Info
181	5.638256	195.251.234.170	195.251.255.138	HTTP	543	GET /pages/metaptyxiaka/part-time.php HTTP/1.1
197	5.664501	195.251.255.138	195.251.234.170	HTTP	252	HTTP/1.1 200 OK (text/html)
199	5.698282	195.251.234.170	195.251.255.138	HTTP	635	GET /assets/css/page.css HTTP/1.1
200	5.700141	195.251.234.170	195.251.255.138	HTTP	583	GET /assets/img/banner/T21_1.jpg HTTP/1.1
202	5.705108	195.251.255.138	195.251.234.170	HTTP	324	HTTP/1.1 304 Not Modified

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



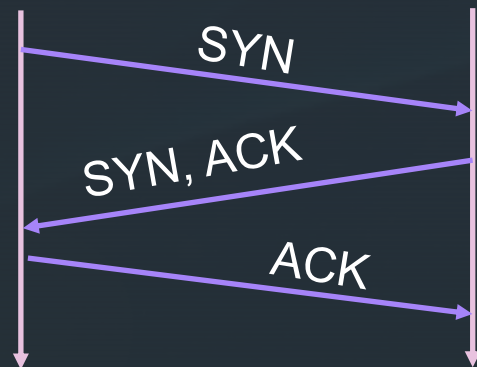
TCP 3-way Handshake

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && ip.addr==83.212.207.19

No.	Time	Source	Destination	Protocol	Length	Info
885	24.863780	192.168.1.2	83.212.207.19	TCP	66	50175 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
892	24.961649	83.212.207.19	192.168.1.2	TCP	66	80 → 50175 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1416 SACK_PERM=1 WS=128
893	24.961762	192.168.1.2	83.212.207.19	TCP	54	50175 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
947	25.840946	192.168.1.2	83.212.207.19	HTTP	465	GET / HTTP/1.1
951	25.943298	83.212.207.19	192.168.1.2	TCP	54	80 → 50175 [ACK] Seq=1 Ack=412 Win=64128 Len=0
980	26.240509	83.212.207.19	192.168.1.2	TCP	1470	80 → 50175 [ACK] Seq=1 Ack=412 Win=64128 Len=1416 [TCP segment of a reassembled
981	26.242260	83.212.207.19	192.168.1.2	TCP	1470	80 → 50175 [ACK] Seq=1417 Ack=412 Win=64128 Len=1416 [TCP segment of a reassembl
982	26.242313	192.168.1.2	83.212.207.19	TCP	54	50175 → 80 [ACK] Seq=412 Ack=2833 Win=66304 Len=0
983	26.244118	83.212.207.19	192.168.1.2	HTTP	1404	HTTP/1.1 200 OK (text/html)
991	26.284207	192.168.1.2	83.212.207.19	TCP	54	50175 → 80 [ACK] Seq=412 Ack=4183 Win=65024 Len=0



Statistics | Flow Graph

The screenshot displays the Wireshark interface with the Statistics menu open. The menu items include: Capture File Properties, Resolved Addresses, Protocol Hierarchy, Conversations, Endpoints, Packet Lengths, I/O Graphs, Service Response Time, DHCP (BOOTP) Statistics, ONC-RPC Programs, 29West, ANCP, BACnet, Collectd, DNS, Flow Graph, HART-IP, HPFEEDS, HTTP, HTTP2, Sametime, TCP Stream Graphs, UDP Multicast Streams, F5, IPv4 Statistics, and IPv6 Statistics. The Flow Graph window is also visible, showing a sequence of TCP flows between 192.168.1.2 and 83.212.207.19.

Flow Graph Data:

Time	Source	Destination	Flow Type	Comment
24.863780	50175	80	SYN	Seq = 0
24.961649	50175	80	SYN, ACK	Seq = 0 Ack = 1
24.961762	50175	80	ACK	Seq = 1 Ack = 1
25.840946	50175	80	PSH, ACK - Len: 411	Seq = 1 Ack = 1
25.943298	50175	80	ACK	Seq = 1 Ack = 412
26.240509	50175	80	ACK - Len: 1416	Seq = 1 Ack = 412
26.242260	50175	80	ACK - Len: 1416	Seq = 1417 Ack = 412
26.242313	50175	80	ACK	Seq = 412 Ack = 2833
26.244118	50175	80	PSH, ACK - Len: 1350	Seq = 2833 Ack = 412
26.284207	50175	80	ACK	Seq = 412 Ack = 4183
29.472245	50175	80	PSH, ACK - Len: 466	Seq = 412 Ack = 4183

Packet 1228: Seq = 8431 Ack = 878

Flow type: TCP Flows

Addresses: Any

Buttons: Save As..., Reset Diagram, Close, Help

Analyze | Follow TCP stream

Wireshark interface showing a packet capture on Wi-Fi. The filter applied is `tcp.stream eq 25`. The packet list shows several packets, with packet 885 selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The 'Follow' menu is open, and 'TCP Stream' is selected.

No.	Time	Source	Destination	Protocol	Length	Info
885	24.863780	192.168.1.1	192.168.1.100	TCP	60	50175 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
892	24.961649	83.212.2.1	192.168.1.100	TCP	60	50175 → 50175 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1416 SACK_PERM=1 WS=128
893	24.961762	192.168.1.1	83.212.2.1	TCP	60	50175 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
947	25.840946	192.168.1.1	83.212.2.1	HTTP	1416	GET / HTTP/1.1
951	25.943298	83.212.2.1	192.168.1.1	TCP	60	50175 → 50175 [ACK] Seq=1 Ack=412 Win=64128 Len=0
980	26.240509	83.212.2.1	192.168.1.1	TCP	1416	50175 → 50175 [ACK] Seq=1 Ack=412 Win=64128 Len=1416 [TCP segment of a reassembled PDU]
981	26.242260	83.212.2.1	192.168.1.1	TCP	1416	50175 → 50175 [ACK] Seq=1417 Ack=412 Win=64128 Len=1416 [TCP segment of a reassembled PDU]
982	26.242313	192.168.1.1	83.212.2.1	TCP	60	50175 → 80 [ACK] Seq=412 Ack=2833 Win=66304 Len=0
983	26.244118	83.212.2.1	192.168.1.1	HTTP	200	200 OK (text/html)
991	26.284207	192.168.1.1	83.212.2.1	TCP	60	50175 → 80 [ACK] Seq=412 Ack=4183 Win=65024 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 25) · Wi-Fi

```

GET / HTTP/1.1
Host: ccslab.aueb.gr
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: _ga=GA1.2.478121687.1605115916; _fbp=fb.1.1605115916060.1288997708
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 13 Nov 2020 16:41:44 GMT
Server: Apache/2.4.18 (Ubuntu)
Link: <http://ccslab.aueb.gr/index.php/wp-json/>; rel="https://api.w.org/"
Link: <http://ccslab.aueb.gr/>; rel=shortlink
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3806
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
  
```

2 client pkts, 7 server pkts, 3 turns.

Entire conversation (10kB) Show data as ASCII Stream 25

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Statistics | Protocol Hierarchy

The screenshot shows the Wireshark interface with the 'Statistics' menu open and 'Protocol Hierarchy' selected. The main packet list shows several packets with their respective times and source addresses. The Protocol Hierarchy Statistics window provides a detailed breakdown of the captured traffic.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	88	100.0	17338	6974	0	0	0
Ethernet	100.0	88	7.1	1232	495	0	0	0
Internet Protocol Version 4	97.7	86	9.9	1720	691	0	0	0
User Datagram Protocol	44.3	39	1.8	312	125	0	0	0
Simple Service Discovery Protocol	4.5	4	6.3	1096	440	4	1096	440
QUIC IETF	20.5	18	46.7	8091	3254	18	8091	3254
Data	19.3	17	12.7	2205	887	17	2205	887
Transmission Control Protocol	53.4	47	15.1	2626	1056	23	485	195
Transport Layer Security	26.1	23	9.6	1660	667	23	1660	667
Data	1.1	1	0.0	1	0	1	1	0
Address Resolution Protocol	2.3	2	0.3	56	22	2	56	22

No display filter.

Close Copy Help

Statistics | Conversations

The screenshot shows the Wireshark interface with the **Statistics** menu open, highlighting the **Conversations** option. Below it, the **Conversations** window is displayed, showing a table of network conversations. The window has tabs for different protocols: Ethernet (6), IPv4 (13), IPv6, TCP (9), and UDP (11). The **IPv4** tab is selected, and the **Name resolution** checkbox is checked.

The main table in the **Conversations** window (IPv4 tab) shows the following data:

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
AskeyCom_44:3a:91	Tp-LinkT_19:1c:51	65	13k	36	7461	29	5610	0.000000	19.8328	3009	2262
IPv4mcast_07	SamsungE_4a:7e:0e	10	2380	0	0	10	2380	0.226345	18.0226	0	1056
IPv4mcast_7f:ff:fa	IntelCor_78:1a:45	4	1264	0	0	4	1264	2.992374	15.0523	0	671
IPv4mcast_7f:ff:fa	SamsungE_4a:7e:0e	3	231	0	0	3	231	4.936107	11.9804	0	154
IntelCor_78:1a:45	Broadcast	2	84	2	84	0	0	6.777587	10.0363	66	0
SamsungE_4a:7e:0e	Broadcast	4	308	4	308	0	0	1.866211	18.0199	136	0

Below this table, the **Name resolution** checkbox is checked, and the **Limit to display filter** checkbox is unchecked. The **IPv4** tab is highlighted in the top navigation bar.

A second **Conversations** window is shown below, with the **IPv4** tab selected. The **Name resolution** checkbox is unchecked, and the **Absolute start time** checkbox is also unchecked. The table below shows a different set of conversations:

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
51.140.157.153	192.168.1.2	1	54	1	54	0	0	14.551605	0.0000	—	—
52.111.231.3	192.168.1.2	2	143	1	54	1	89	9.443996	0.1093	3951	6512
52.114.74.225	192.168.1.2	3	267	1	101	2	166	13.312551	0.1174	6884	11k
52.114.104.45	192.168.1.2	3	688	2	447	1	241	0.399763	0.1545	23k	12k
74.125.133.188	192.168.1.2	2	121	1	66	1	55	16.822907	0.0779	6778	5648
92.123.90.207	192.168.1.2	33	2789	19	1961	14	828	0.240615	18.2004	861	363

At the bottom of the second window, there are buttons for **Copy**, **Follow Stream...**, **Graph...**, **Close**, and **Help**.

Statistics | Endpoints

The main Wireshark window shows a packet capture on interface 'Wi-Fi'. The 'Statistics' menu is open, and 'Endpoints' is highlighted. The main pane shows a list of packets with columns for No., Time, and Source.

The 'Wireshark · Endpoints · Wi-Fi' window shows the 'IPv4 · 15' tab selected. It displays a table of IP addresses and their associated statistics.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
51.140.157.153	1	54	1	54	0	0	—	—	—	—
52.111.231.3	2	143	1	54	1	89	—	—	—	—
52.114.74.225	3	267	1	101	2	166	—	—	—	—
52.114.104.45	3	688	2	447	1	241	—	—	—	—
74.125.133.188	2	121	1	66	1	55	—	—	—	—
92.123.90.207	33	2789	19	1961	14	828	—	—	—	—
104.146.202.25	3	162	1	54	2	108	—	—	—	—
172.217.17.163	9	4100	5	2079	4	2021	—	—	—	—
172.217.169.131	9	4747	5	2645	4	2102	—	—	—	—
192.168.1.2	65	13k	29	5610	36	7461	—	—	—	—
192.168.1.3	17	2919	17	2919	0	0	—	—	—	—
192.168.1.4	4	1264	4	1264	0	0	—	—	—	—
192.168.1.255	4	308	0	0	4	308	—	—	—	—
224.0.0.7	10	2380	0	0	10	2380	—	—	—	—
239.255.255.250	7	1495	0	0	7	1495	—	—	—	—

The 'Wireshark · Endpoints · Wi-Fi' window shows the 'Ethernet · 7' tab selected. It displays a table of MAC addresses and their associated statistics.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:21:63:44:3a:91	65	13k	36	7461	29	5610
01:00:5e:00:00:07	10	2380	0	0	10	2380
01:00:5e:7f:ff:fa	7	1495	0	0	7	1495
34:de:1a:78:1a:45	6	1348	6	1348	0	0
98:de:d0:19:1c:51	65	13k	29	5610	36	7461
fc:03:9f:4a:7e:0e	17	2919	17	2919	0	0
ff:ff:ff:ff:ff:ff	6	392	0	0	6	392

Statistics | IPv4 Statistics | Destinations & Ports

Wireshark · Destinations and Ports · Wi-Fi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Destinations and Ports	86				0.0043	100%	0.0800	3.995
▼ 92.123.90.207	14				0.0007	16.28%	0.0300	3.996
▼ TCP	14				0.0007	100.00%	0.0300	3.996
443	14				0.0007	100.00%	0.0300	3.996
▼ 74.125.133.188	1				0.0001	1.16%	0.0100	16.823
▼ TCP	1				0.0001	100.00%	0.0100	16.823
5228	1				0.0001	100.00%	0.0100	16.823
▼ 52.114.74.225	2				0.0001	2.33%	0.0100	13.313
▼ TCP	2				0.0001	100.00%	0.0100	13.313
443	2				0.0001	100.00%	0.0100	13.313
▼ 52.114.104.45	1				0.0001	1.16%	0.0100	0.419
▼ TCP	1				0.0001	100.00%	0.0100	0.419
443	1				0.0001	100.00%	0.0100	0.419
▼ 52.111.231.3	1				0.0001	1.16%	0.0100	9.444
▼ TCP	1				0.0001	100.00%	0.0100	9.444
443	1				0.0001	100.00%	0.0100	9.444
▼ 239.255.255.250	7				0.0004	8.14%	0.0100	2.992
▼ UDP	7				0.0004	100.00%	0.0100	2.992
1900	4				0.0002	57.14%	0.0100	2.992
15600	3				0.0002	42.86%	0.0100	4.936
▼ 224.0.0.7	10				0.0005	11.63%	0.0100	0.226

Display filter:

Apply Copy Save as... Close

▶ 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