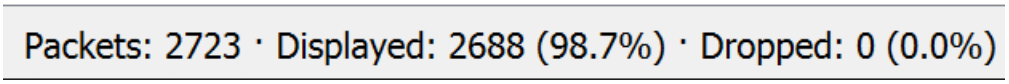
Ελένη Τράμπαρη Λάρδα

A.M: 3180186

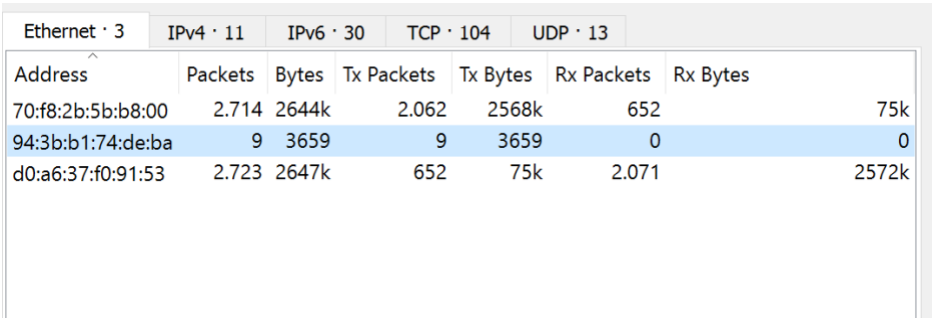
Εργασία: 2

1. TCP: 2688

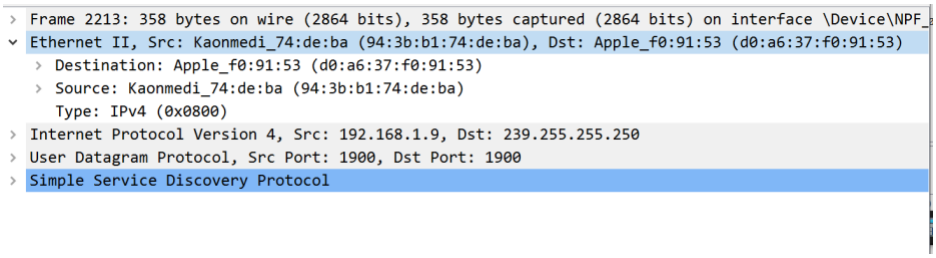


UDP: 29

2. Εδώ φαίνονται τα endpoints του Ethernet



Κάνοντας find & select



Φαίνεται το source και το destination.

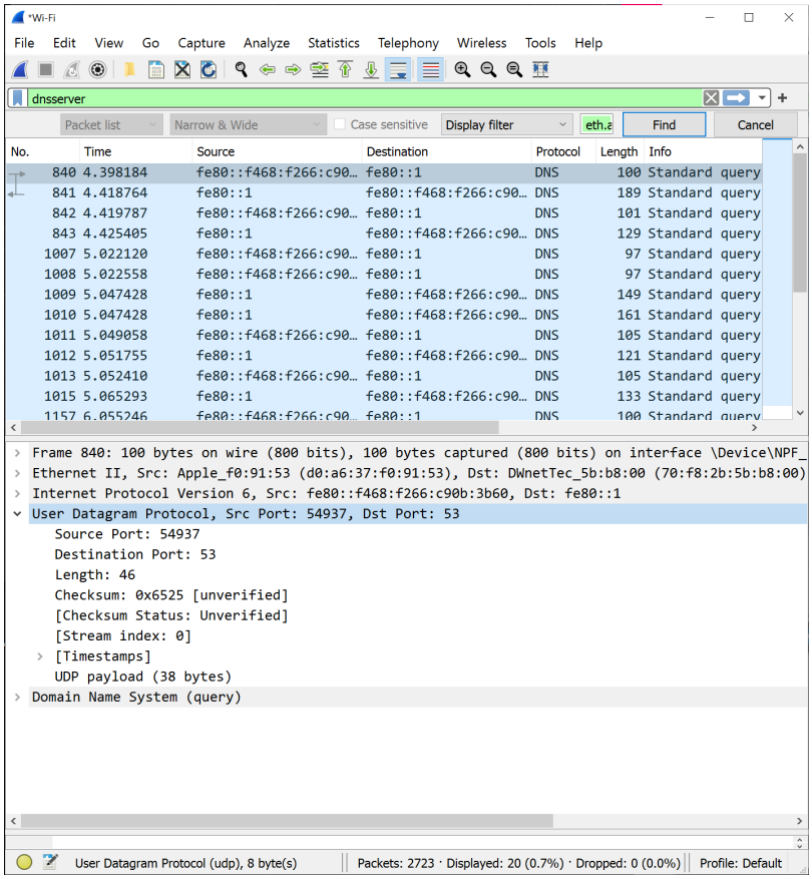
3. IPv4: network addresses
   IPv6: network addresses
   Ethernet: mac addresses

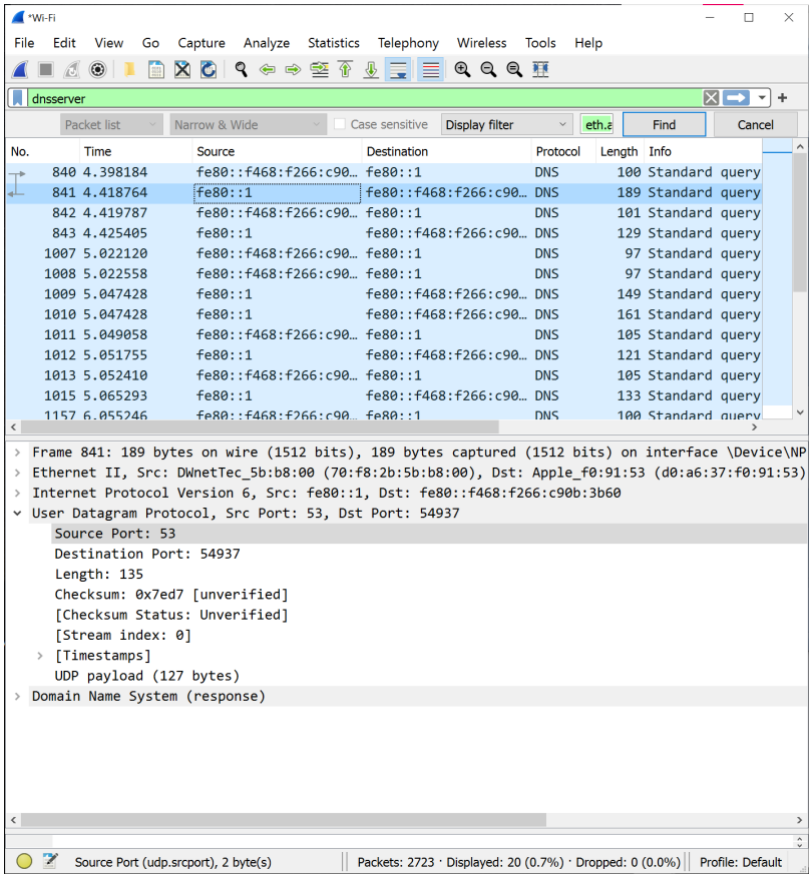
   Τα IP είναι επιπέδου 3, ενώ το Ethernet είναι επιπέδου 1,2.

Ethernet · 3 | IPv4 · 11 | IPv6 · 30 | TCP · 104 | UDP · 13

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City
13.107.6.254	1	54	1	54	0	0	—	—
34.107.221.82	3	162	1	54	2	108	—	—
52.114.75.85	31	10k	15	7267	16	3715	—	—
84.53.156.184	3	162	1	54	2	108	—	—
93.184.220.29	13	721	5	288	8	433	—	—
104.244.42.136	8	1744	4	684	4	1060	—	—
192.168.1.8	1.707	1979k	341	33k	1.366	1946k	—	—
192.168.1.9	9	3659	9	3659	0	0	—	—
195.201.241.83	1.631	1963k	1.330	1936k	301	26k	—	—
195.251.255.206	17	2848	9	1228	8	1620	—	—
239.255.255.250	9	3659	0	0	9	3659	—	—

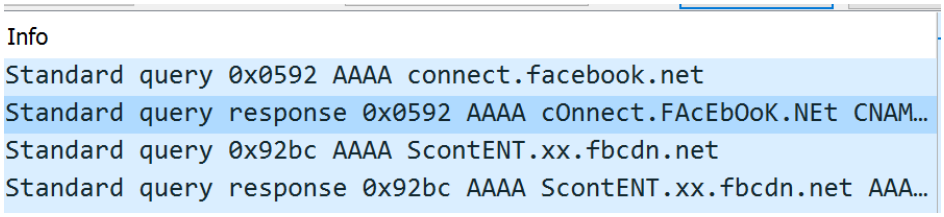
4.





Παρατηρούμε ότι το server port είναι 53 και ανάλογα με το request & reply αλλάζουν τα destination ή τα source αντίστοιχα.

5. Μέσω του info, φαίνεται ποιο είναι request και ποιο reply.



Η σύνδεση των πακέτων φαίνεται από το queries εκεί που λέει response in & request in αντίστοιχα.

```
Domain Name System (response)
    Transaction ID: 0x0592
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 840]
    [Time: 0.020580000 seconds]
```

```
Domain Name System (query)
    Transaction ID: 0x0592
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 841]
```

6.

```
Domain Name System (response)
    Transaction ID: 0x92bc
  > Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticat
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
```

Ο server δεν είναι authorized.

7. Το όνομα www.book4book.gr είναι CN (canonical name)
με IP address: 195.201.241.83

8.

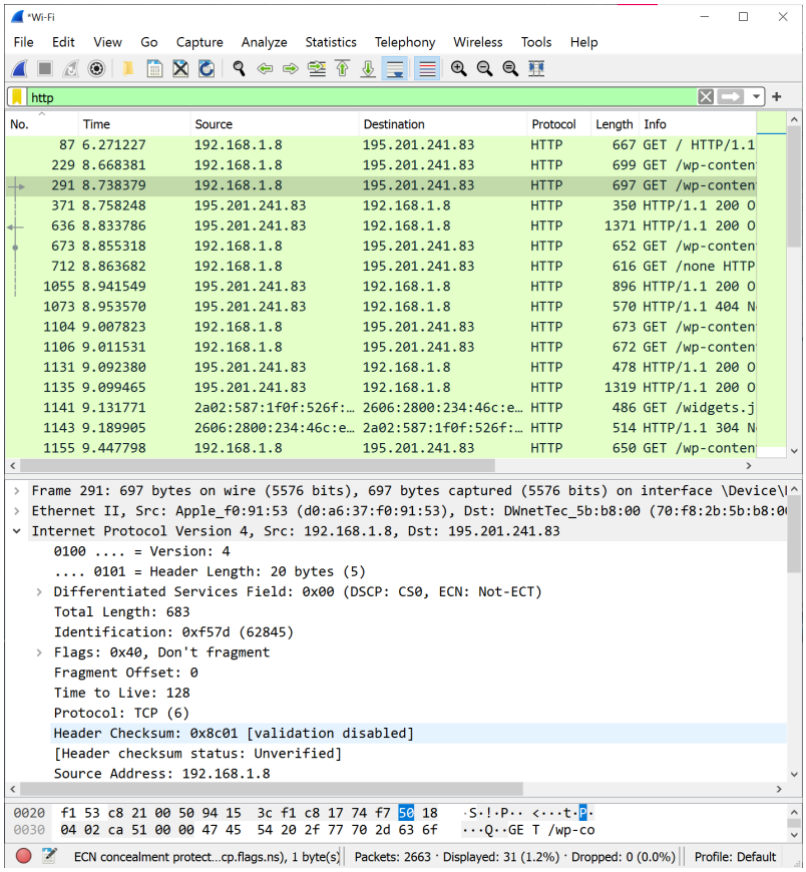
```
TCP      86 51239 → 80 [SYN] Seq=0 Win=64440 Len=0 MSS=1432 WS=256 SACK_P…
TCP      86 80 → 51239 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SA…
TCP      74 51239 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
```

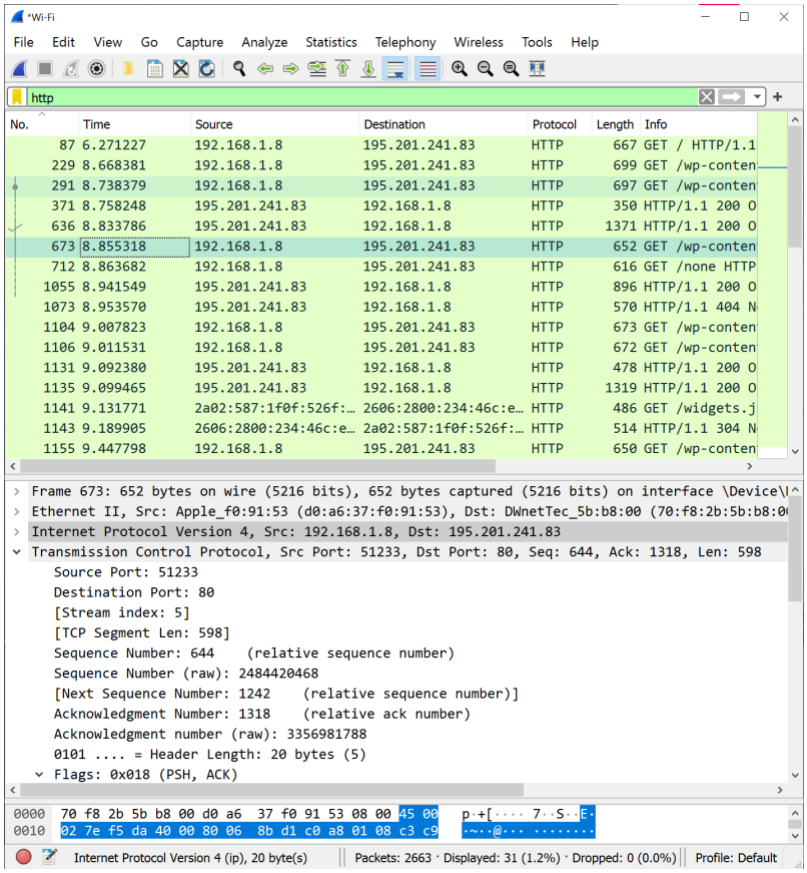
Βήμα 1: Ο client δημιουργεί μια σύνδεση με τον server. Στέλνει segment TCP SYN και πληροφορεί τον server για τον client .

Βήμα 2: Ο server απαντά στο πελάτη στέλνοντας TCP SYN-ACK.

Βήμα 3: Ο client απαντά με TCP ACK, όπου δείχνει ότι έχει αποδεχθεί τη σύνδεση.

9.





Source: 80
Destination: 51233 (etc)

Το port είναι 80 και ανάλογα με το request & reply αλλάζουν τα destination ή τα source αντίστοιχα.

Το http χρησιμοποιεί τα TCP όπως φαίνεται και από το πρώτο screenshot στο σημείο internet protocol (protocol).

10. Τα http get είναι 16 (από τα 31)

IP διευθύνσεις: 195.201.241.83

Source	Destination	Protocol	Length	Info
192.168.1.8	195.201.241.83	HTTP	667	GET / HTTP/1.1
192.168.1.8	195.201.241.83	HTTP	699	GET /wp-content/plugins/sitepre
192.168.1.8	195.201.241.83	HTTP	697	GET /wp-content/plugins/jquery-

11. Ο browser μας τρέχει σε HTTP/1.1 έκδοση

    Ο server τρέχει σε HTTP/1.1 έκδοση

    Το λογισμικό web server που τρέχει ο server που απάντησε για το book4book είναι Mozilla/5.0.