

Ελένη Τράμπαρη Λάρδα

A.M: 3180186

Εργασία: 2

1. TCP: 2688

Packets: 2723 · Displayed: 2688 (98.7%) · Dropped: 0 (0.0%)

UDP: 29

Packets: 2723 · Displayed: 29 (1.1%) · Dropped: 0 (0.0%)

2. Εδώ φαίνονται τα endpoints του Ethernet

Ethernet · 3		IPv4 · 11		IPv6 · 30		TCP · 104		UDP · 13	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
70:f8:2b:5b:b8:00	2.714	2644k	2.062	2568k	652				75k
94:3b:b1:74:de:ba	9	3659	9	3659	0				0
d0:a6:37:f0:91:53	2.723	2647k	652	75k	2.071				2572k

Κάνοντας find & select

```
> Frame 2213: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{...}
  > Ethernet II, Src: Kaonmedi_74:de:ba (94:3b:b1:74:de:ba), Dst: Apple_f0:91:53 (d0:a6:37:f0:91:53)
    > Destination: Apple_f0:91:53 (d0:a6:37:f0:91:53)
    > Source: Kaonmedi_74:de:ba (94:3b:b1:74:de:ba)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.9, Dst: 239.255.255.250
  > User Datagram Protocol, Src Port: 1900, Dst Port: 1900
  > Simple Service Discovery Protocol
```

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	—	—	

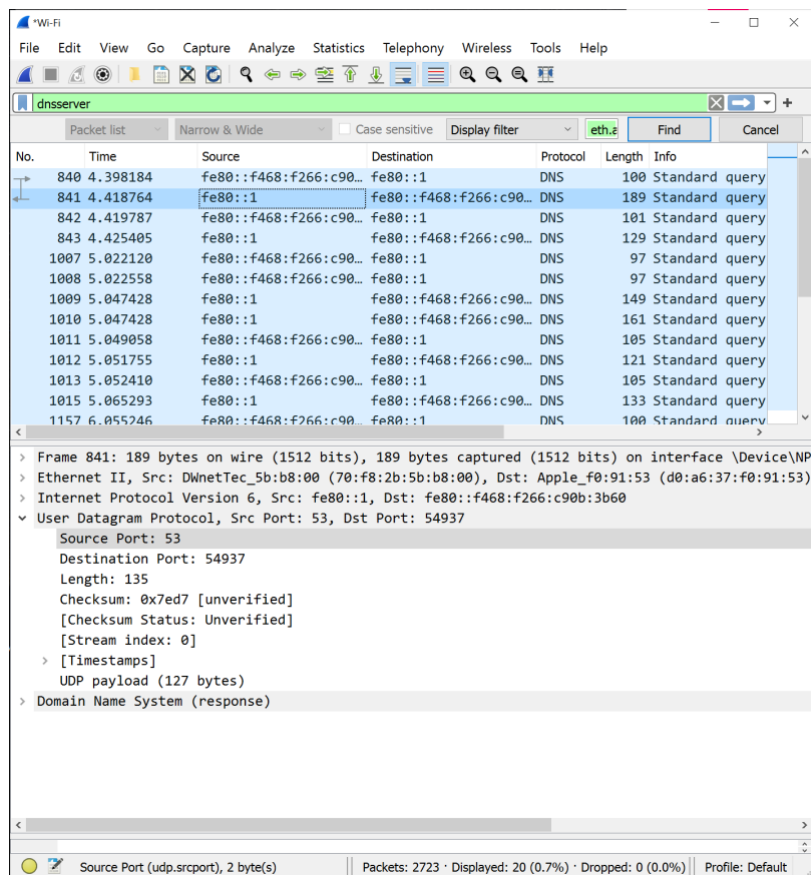
4.

Wireshark packet capture analysis of DNS traffic. The packet list shows a series of DNS queries from a source IP to a destination IP. The selected packet (No. 840) is a Standard query from Source Port 54937 to Destination Port 53. The packet details pane shows the Ethernet II, Internet Protocol Version 6, and User Datagram Protocol (UDP) layers. The UDP payload is a Domain Name System (query) packet.

No.	Time	Source	Destination	Protocol	Length	Info
840	4.398184	fe80::f468:f266:c90...	fe80::1	DNS	100	Standard query
841	4.418764	fe80::1	fe80::f468:f266:c90...	DNS	189	Standard query
842	4.419787	fe80::f468:f266:c90...	fe80::1	DNS	101	Standard query
843	4.425405	fe80::1	fe80::f468:f266:c90...	DNS	129	Standard query
1007	5.022120	fe80::f468:f266:c90...	fe80::1	DNS	97	Standard query
1008	5.022558	fe80::f468:f266:c90...	fe80::1	DNS	97	Standard query
1009	5.047428	fe80::1	fe80::f468:f266:c90...	DNS	149	Standard query
1010	5.047428	fe80::1	fe80::f468:f266:c90...	DNS	161	Standard query
1011	5.049058	fe80::f468:f266:c90...	fe80::1	DNS	105	Standard query
1012	5.051755	fe80::1	fe80::f468:f266:c90...	DNS	121	Standard query
1013	5.052410	fe80::f468:f266:c90...	fe80::1	DNS	105	Standard query
1015	5.065293	fe80::1	fe80::f468:f266:c90...	DNS	133	Standard query
1157	6.055246	fe80::f468:f266:c90...	fe80::1	DNS	100	Standard query

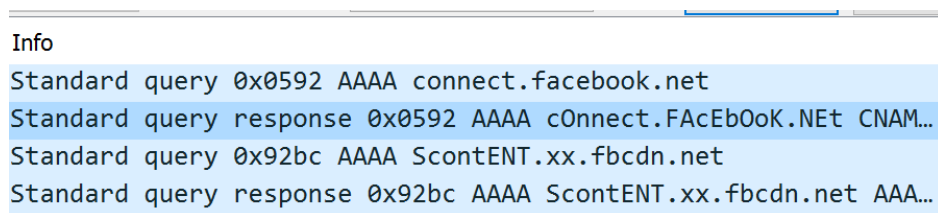
Frame 840: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_...
 Ethernet II, Src: Apple_f0:91:53 (d0:a6:37:f0:91:53), Dst: DlnetTec_5b:b8:00 (70:f8:2b:5b:b8:00)
 Internet Protocol Version 6, Src: fe80::f468:f266:c90b:3b60, Dst: fe80::1
 User Datagram Protocol, Src Port: 54937, Dst Port: 53
 Source Port: 54937
 Destination Port: 53
 Length: 46
 Checksum: 0x6525 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 0]
 [Timestamps]
 UDP payload (38 bytes)
 Domain Name System (query)

User Datagram Protocol (udp), 8 byte(s) | Packets: 2723 · Displayed: 20 (0.7%) · Dropped: 0 (0.0%) | Profile: Default



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

- 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 authenticated
 -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.

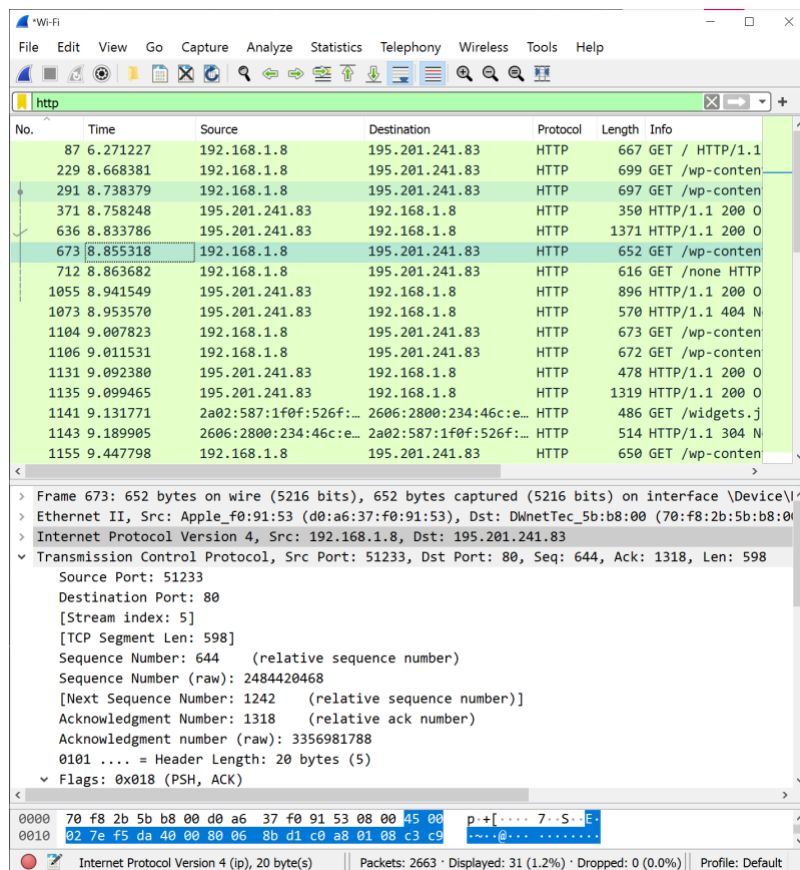
Βήμα 3: Ο client απαντά με TCP ACK, όπου δείχνει ότι έχει αποδεχθεί τη σύνδεση.

9.

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a series of HTTP packets. The selected packet is a GET request from 192.168.1.8 to 195.201.241.83. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) header. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
87	6.271227	192.168.1.8	195.201.241.83	HTTP	667	GET / HTTP/1.1
229	8.668381	192.168.1.8	195.201.241.83	HTTP	699	GET /wp-content
291	8.738379	192.168.1.8	195.201.241.83	HTTP	697	GET /wp-content
371	8.758248	195.201.241.83	192.168.1.8	HTTP	350	HTTP/1.1 200 O
636	8.833786	195.201.241.83	192.168.1.8	HTTP	1371	HTTP/1.1 200 O
673	8.855318	192.168.1.8	195.201.241.83	HTTP	652	GET /wp-content
712	8.863682	192.168.1.8	195.201.241.83	HTTP	616	GET /none HTTP
1055	8.941549	195.201.241.83	192.168.1.8	HTTP	896	HTTP/1.1 200 O
1073	8.953570	195.201.241.83	192.168.1.8	HTTP	570	HTTP/1.1 404 N
1104	9.007823	192.168.1.8	195.201.241.83	HTTP	673	GET /wp-content
1106	9.011531	192.168.1.8	195.201.241.83	HTTP	672	GET /wp-content
1131	9.092380	195.201.241.83	192.168.1.8	HTTP	478	HTTP/1.1 200 O
1135	9.099465	195.201.241.83	192.168.1.8	HTTP	1319	HTTP/1.1 200 O
1141	9.131771	2a02:587:1f0f:526f::...	2606:2800:234:46c:e...	HTTP	486	GET /widgets.j
1143	9.189905	2606:2800:234:46c:e...	2a02:587:1f0f:526f::...	HTTP	514	HTTP/1.1 304 N
1155	9.447798	192.168.1.8	195.201.241.83	HTTP	650	GET /wp-content

Frame 291: 697 bytes on wire (5576 bits), 697 bytes captured (5576 bits) on interface \Device\NPF...
Ethernet II, Src: Apple_f0:91:53 (d0:a6:37:f0:91:53), Dst: Dwnetec_5b:b8:00 (70:f8:2b:5b:b8:00)
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 195.201.241.83
Hypertext Transfer Protocol
GET /wp-content/ HTTP/1.1
Host: 195.201.241.83
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100603 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: max-age=0
Connection: keep-alive
Cookie: ...
DNT: 1
Referer: http://192.168.1.8/



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.

```
▼ Hypertext Transfer Protocol
  > GET /wp-content/uploads/2012/04/favicon.ico HTTP/1.1\r\n
    Host: www.book4book.gr\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\
```