

Εργασία 2 Wireshark

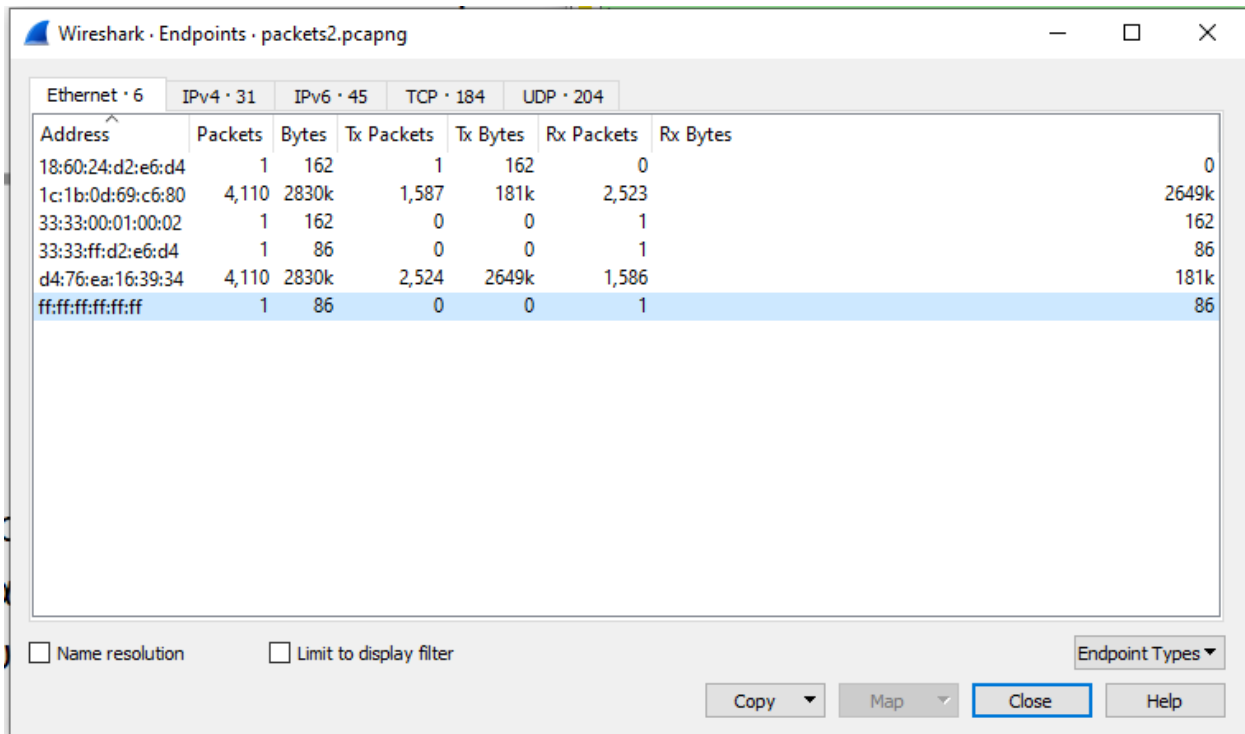
Δημήτριος Τσιομπίκας 3180223

Ερώτηση 1

Στάλθηκαν 402 πακέτα UDP και 3707 πακέτα TCP.

TCP :	<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
	Packets	4112	3707 (90.2%)	—
UDP :	<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
	Packets	4112	402 (9.8%)	—

Ερώτηση 2

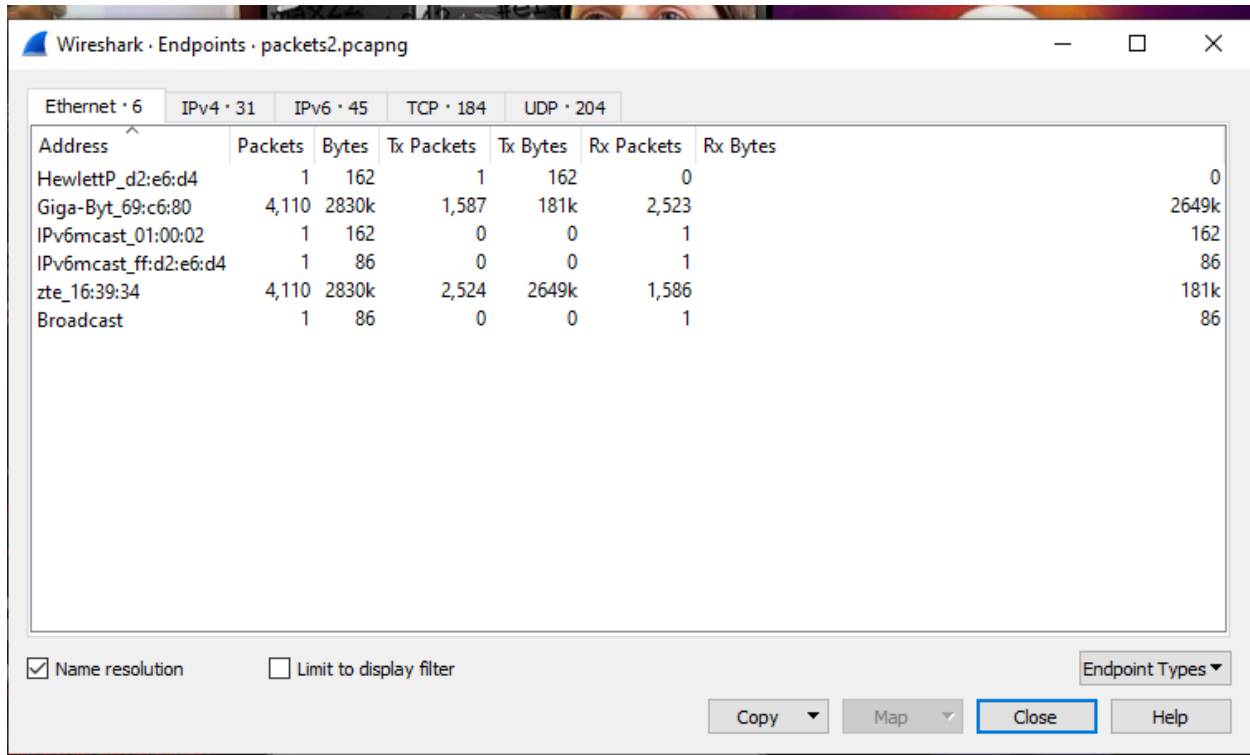


Endpoints · packets2.pcapng						
Ethernet · 6 IPv4 · 31 IPv6 · 45 TCP · 184 UDP · 204						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
18:60:24:d2:e6:d4	1	162	1	162	0	0
1c:1b:0d:69:c6:80	4,110	2830k	1,587	181k	2,523	2649k
33:33:00:01:00:02	1	162	0	0	1	162
33:33:ff:d2:e6:d4	1	86	0	0	1	86
d4:76:ea:16:39:34	4,110	2830k	2,524	2649k	1,586	181k
ff:ff:ff:ff:ff:ff	1	86	0	0	1	86

☐ Name resolution ☐ Limit to display filter Endpoint Types ▾

Copy ▾ Map ▾ Close Help

Πατώντας το Name resolution μπορούμε να δούμε μερικά ονόματα συσκευών που χρησιμοποιούν τα endpoints.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
HewlettP_d2:e6:d4	1	162	1	162	0	0
Giga-Byt_69:c6:80	4,110	2830k	1,587	181k	2,523	2649k
IPv6mcast_01:00:02	1	162	0	0	1	162
IPv6mcast_ff:d2:e6:d4	1	86	0	0	1	86
zte_16:39:34	4,110	2830k	2,524	2649k	1,586	181k
Broadcast	1	86	0	0	1	86

Πχ η πρώτη διεύθυνση χρησιμοποιείται από τον εκτυπωτή μου (μάρκας Hewlett-Packard), η 2^η χρησιμοποιείται από την μητρική μου κάρτα (μάρκας Gigabyte) και η προτελευταία χρησιμοποιείται από το modem μου (μάρκας ZTE).

Ερώτηση 3

Wireshark · Endpoints · packets2.pcapng

Ethernet · 6		IPv4 · 31		IPv6 · 45		TCP · 184		UDP · 204					
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number				
2600:1901:0:38d7::	18	2431	8	1072	10	1359	—	—	—				
2600:1901:0:524d::	2	161	1	86	1	75	—	—	—				
2600:1901:1:292::	4	379	2	188	2	191	—	—	—				
2600:1901:1:64a::	2	161	1	86	1	75	—	—	—				
2600:1901:1:c36::	6	483	3	258	3	225	—	—	—				
2600:1901:1:e52::	4	379	2	188	2	191	—	—	—				
2603:1026:301:9a::2	1	74	1	74	0	0	—	—	—				
2603:1026:302:a0::2	1	74	1	74	0	0	—	—	—				
2606:2800:234:46c:e8b:1e2f:2bd:694	75	54k	48	50k	27	3407	—	—	—				
2606:4700::6810:5714	17	5111	9	3729	8	1382	—	—	—				
2620:1ec:42::132	2	148	2	148	0	0	—	—	—				
2a00:1450:4001:800::200e	54	26k	30	23k	24	3407	—	—	—				
2a00:1450:4001:801::2003	28	11k	15	9196	13	2183	—	—	—				
2a00:1450:4001:802::2001	2	161	1	86	1	75	—	—	—				
2a00:1450:4001:808::200e	19	6650	10	5184	9	1466	—	—	—				
2a00:1450:4001:80b::200a	52	18k	30	14k	22	3358	—	—	—				
2a00:1450:4001:80b::200e	213	156k	136	147k	77	9132	—	—	—				
2a00:1450:4001:814::2006	22	6136	12	4356	10	1780	—	—	—				
2a00:1450:4001:815::2016	16	5686	8	4304	8	1382	—	—	—				
2a00:1450:4001:817::2003	16	5277	8	3895	8	1382	—	—	—				
2a00:1450:4001:817::200d	25	9329	14	5836	11	3493	—	—	—				
2a00:1450:4001:819::2002	32	8341	18	6017	14	2324	—	—	—				
2a00:1450:4001:819::2003	16	5276	8	3894	8	1382	—	—	—				
2a00:1450:4001:81a::2001	18	7971	10	6589	8	1382	—	—	—				
2a00:1450:4001:81b::2004	49	16k	27	12k	22	4226	—	—	—				
2a00:1450:4001:81b::200e	1,508	1301k	988	1250k	520	50k	—	—	—				
2a00:1450:4001:821::2002	2	161	1	86	1	75	—	—	—				
2a00:1450:4001:824::200e	2	161	1	86	1	75	—	—	—				
2a00:1450:4001:825::2002	4	322	2	172	2	150	—	—	—				
2a00:1450:4001:825::2003	57	17k	28	10k	29	6821	—	—	—				
2a00:1450:4001:825::200a	20	5817	10	4277	10	1540	—	—	—				
2a00:1450:400c:c0b::9b	2	161	1	86	1	75	—	—	—				
2a02:582:a00::d4cd:7e23	2	161	1	86	1	75	—	—	—				
2a02:582:a00::d4cd:7e91	6	475	3	253	3	222	—	—	—				
2a02:587:123e:8100:a501:7625:ce50:47cf	2,424	1698k	922	112k	1,502	1585k	—	—	—				
2a02:26f0:c000:180::4106	3	222	0	0	3	222	—	—	—				
2a03:2880:f0ff:eface:b00c:0:3	44	14k	25	10k	19	3205	—	—	—				
2a03:2880:f0ff:eface:b00c:0:2	21	1968	10	886	11	1082	—	—	—				
2a04:4e42:4::760	24	1932	12	1032	12	900	—	—	—				
2a04:fa87:fffe::c000:4902	35	6470	15	3010	20	3460	—	—	—				
fe80::1	401	53k	201	33k	200	20k	—	—	—				
fe80::1a60:24ff:fed2:e6d4	1	162	1	162	0	0	—	—	—				
fe80::f437:4b95:84b4:4486	400	53k	200	20k	200	33k	—	—	—				
ff02::1:2	1	162	0	0	1	162	—	—	—				
ff02::1:ffd2:e6d4	1	86	0	0	1	86	—	—	—				

<

>

☐ Name resolution

☐ Limit to display filter

Endpoint Types ▾

Copy ▾

Map ▾

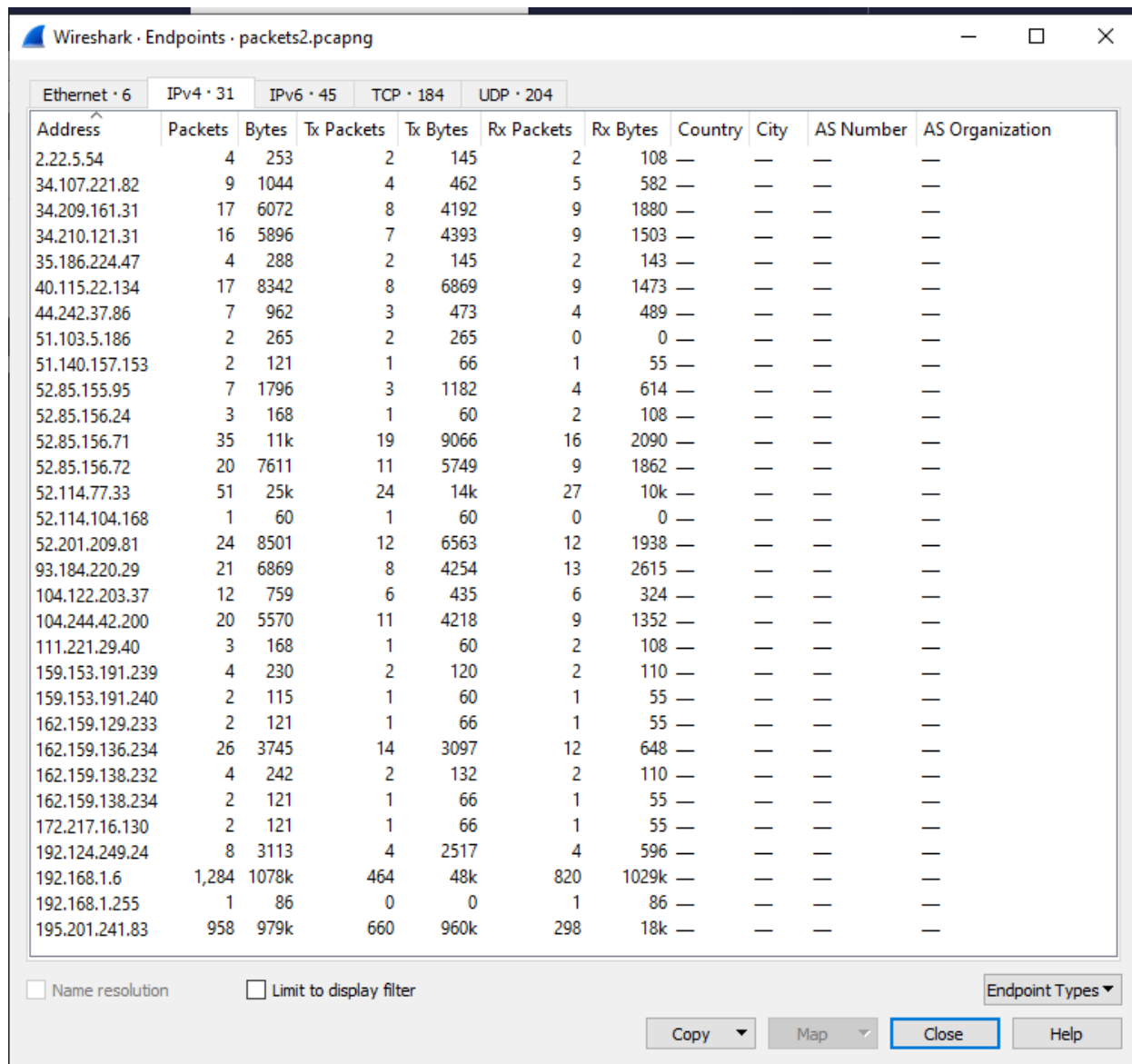
Close

Help

Έχουμε 45 endpoints που επικοινωνούν σε επίπεδο IP . Μετράω τα IPv6 καθώς αυτά χρησιμοποιεί ο υπολογιστής μου. Δεν έχουν κάποια

σχέση με τα endpoints στο ethernet επίπεδο και αυτό γιατί τα ethernet endpoints επικοινωνούν με τις συσκευές που είναι συνδεδεμένες με το ethernet (Local,physical addresses) ενώ τα IP endpoints επικοινωνούν με άλλες IP Addresses (δικές μου ή άλλες , private networks, public networks κλπ).

Και τέλος τα IPv4 Endpoints (31):



Wireshark · Endpoints · packets2.pcapng

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
2.22.5.54	4	253	2	145	2	108	—	—	—	—
34.107.221.82	9	1044	4	462	5	582	—	—	—	—
34.209.161.31	17	6072	8	4192	9	1880	—	—	—	—
34.210.121.31	16	5896	7	4393	9	1503	—	—	—	—
35.186.224.47	4	288	2	145	2	143	—	—	—	—
40.115.22.134	17	8342	8	6869	9	1473	—	—	—	—
44.242.37.86	7	962	3	473	4	489	—	—	—	—
51.103.5.186	2	265	2	265	0	0	—	—	—	—
51.140.157.153	2	121	1	66	1	55	—	—	—	—
52.85.155.95	7	1796	3	1182	4	614	—	—	—	—
52.85.156.24	3	168	1	60	2	108	—	—	—	—
52.85.156.71	35	11k	19	9066	16	2090	—	—	—	—
52.85.156.72	20	7611	11	5749	9	1862	—	—	—	—
52.114.77.33	51	25k	24	14k	27	10k	—	—	—	—
52.114.104.168	1	60	1	60	0	0	—	—	—	—
52.201.209.81	24	8501	12	6563	12	1938	—	—	—	—
93.184.220.29	21	6869	8	4254	13	2615	—	—	—	—
104.122.203.37	12	759	6	435	6	324	—	—	—	—
104.244.42.200	20	5570	11	4218	9	1352	—	—	—	—
111.221.29.40	3	168	1	60	2	108	—	—	—	—
159.153.191.239	4	230	2	120	2	110	—	—	—	—
159.153.191.240	2	115	1	60	1	55	—	—	—	—
162.159.129.233	2	121	1	66	1	55	—	—	—	—
162.159.136.234	26	3745	14	3097	12	648	—	—	—	—
162.159.138.232	4	242	2	132	2	110	—	—	—	—
162.159.138.234	2	121	1	66	1	55	—	—	—	—
172.217.16.130	2	121	1	66	1	55	—	—	—	—
192.124.249.24	8	3113	4	2517	4	596	—	—	—	—
192.168.1.6	1,284	1078k	464	48k	820	1029k	—	—	—	—
192.168.1.255	1	86	0	0	1	86	—	—	—	—
195.201.241.83	958	979k	660	960k	298	18k	—	—	—	—

☐ Name resolution ☐ Limit to display filter Endpoint Types ▾

Copy ▾ Map ▾ Close Help

Ερώτηση 4

Destination	Protocol	Length	Info
fe80::1	DNS	96	Standard query 0x1e34 A www.book4book.gr
fe80::f437:4b95:84b...	DNS	126	Standard query response 0x1e34 A www.book4book.gr CNAME book4...

Εδώ έχουμε μια ερωταπόκριση της ιστοσελίδας www.book4book.gr

Source και destination port ερώτησης :

Source Port: 53516
Destination Port: 53

Source και destination port απάντησης :

Source Port: 53
Destination Port: 53516

Ερώτηση 5

Το διακρίνουμε από το tab Info που λέει standard query (για ερώτηση) και standard query RESPONSE (για απάντηση). Τα πακέτα απάντησης και ερώτησης συνδέονται με τα source και destination ports.

Ερώτηση 6

Στην συγκεκριμένη επερώτηση ναι υπάρχει Flag και συγκεκριμένα στο response :

▼ 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

Το name server αυτής της ερωταπόκρισης ΔΕΝ είναι authoritative.

.... .0.. = Authoritative: Server is not an authority for domain
Truncated: Message is not truncated

Ερώτηση 7

```
> www.book4book.gr: type CNAME, class IN, cname book4book.gr
```

Από εδώ συμπεραίνουμε ότι το www.book4book.gr είναι canonical name για το book4book.gr.

```
> book4book.gr: type A, class IN, addr 195.201.241.83
```

Ακριβώς από κάτω παρουσιάζεται η διεύθυνση IP της ιστοσελίδας που είναι η 195.201.241.83.

Ερώτηση 8

Πρώτο πακέτο (SYN)

192.168.1.6	195.201.241.83	TCP	62 50105 → 80 [SYN] Seq=0 Win=64240 Len=0
-------------	----------------	-----	---

Δεύτερο πακέτο (SYN/ACK)

192.168.1.6	195.201.241.83	TCP	62 80 → 50105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1
-------------	----------------	-----	---

Τρίτο πακέτο (ACK)

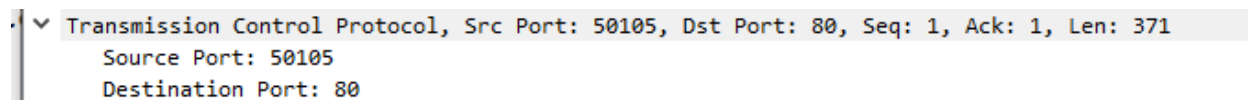
192.168.1.6	195.201.241.83	TCP	54 50105 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
-------------	----------------	-----	---

Εδώ η χειραψία 3 βημάτων συμβαίνει ως εξής : Αρχικά στέλνει ο Υπολογιστής σήμα (το SYN) στον εξυπηρετητή της ιστοσελίδας book4book , η book4book στέλνει στον υπολογιστή μου δικό της σήμα και σήμα αναγνώρισης (SYN,ACK) και τέλος ο υπολογιστής μου στέλνει σήμα αναγνώρισης (ACK) στον book4book server για να τον ενημερώσει ότι λάβαμε τα πακέτα.

Ερώτηση 9

237 7.881029	192.168.1.6	195.201.241.83	HTTP	425 GET / HTTP/1.1
--------------	-------------	----------------	------	--------------------

Εδώ είναι το πρώτο packet HTTP που στάλθηκε στην book4book και τα source ,destination ports :



Το HTTP χρησιμοποιεί κυρίως το TCP αλλά με προσαρμογές μπορεί να χρησιμοποιήσει και UDP. Εδώ χρησιμοποιεί το TCP.

Ερώτηση 10

No.	Time	Source	Destination	Protocol	Length	Info
115	7.273623	2a02:587:123e:8100::...	2600:1901:0:38d7::...	HTTP	372	GET /success.txt HTTP/1.1
164	7.407228	192.168.1.6	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
167	7.411605	2a02:587:123e:8100::...	2600:1901:0:38d7::...	HTTP	377	GET /success.txt?ipv6 HTTP/1.1
237	7.881029	192.168.1.6	195.201.241.83	HTTP	425	/ HTTP/1.1
385	10.346574	192.168.1.6	195.201.241.83	HTTP	475	GET /wp-content/plugins/wp-bannerize/css/wpBannerizeStyle...
388	10.373800	192.168.1.6	195.201.241.83	HTTP	493	GET /wp-content/plugins/jquery-vertical-accordion-menu/sk...
577	10.541850	192.168.1.6	195.201.241.83	HTTP	412	/none HTTP/1.1
1343	11.399994	192.168.1.6	195.201.241.83	HTTP	469	GET /wp-content/plugins/wp-bannerize/js/wpBannerizeFronter...
1353	11.434035	192.168.1.6	195.201.241.83	HTTP	467	GET /wp-content/plugins/slick-social-share-buttons/js/ga...
1356	11.440799	2a02:587:123e:8100::...	2a04:fa87:fffe::c00...	HTTP	462	GET /avatar/5d6a6fdd605dec93c34d10dc969ecd1a?d=monsterid&
1361	11.449853	2a02:587:123e:8100::...	2a04:fa87:fffe::c00...	HTTP	462	GET /avatar/acd3ca1da0dd44f725654010d67bf99c?d=monsterid&
1362	11.449954	2a02:587:123e:8100::...	2a04:fa87:fffe::c00...	HTTP	462	GET /avatar/0f972f97081c92b88774b6a23e4c1b67?d=monsterid&
1367	11.451295	2a02:587:123e:8100::...	2a04:fa87:fffe::c00...	HTTP	462	GET /avatar/0fc54678f1530ccee809f64e8c298739?d=monsterid&
1368	11.451372	2a02:587:123e:8100::...	2a04:fa87:fffe::c00...	HTTP	462	GET /avatar/71b807e6b1c052f31b7d9f7dff57e6ea?d=monsterid&
1467	11.656470	192.168.1.6	195.201.241.83	HTTP	458	/r HTTP/1.1
4028	16.792479	2a02:587:123e:8100::...	2606:2800:234:46c:e...	HTTP	375	GET /widgets.js?_=1608717978363 HTTP/1.1
4073	16.905547	2606:2800:234:46c:e...	2a02:587:123e:8100::...	HTTP	1241	HTTP/1.1 200 OK (application/javascript)

Displayed
17 (0.4%)

Περιείχε 17 HTTP GET Packets.

Οι IP Διευθύνσεις ήταν οι εξής :

2600:1901:0:38d7::

34.107.221.82

195.201.241.83 (IP του book4book)

2a04:fa87:fffe::c000:4902

2606:2800:234:46c:e8b:1e2f:2bd:694

2a02:587:123e:8100:a501:7625:ce50:47cf

Ερώτηση 11

425 GET / HTTP/1.1

Ο browser μου χρησιμοποιεί HTTP 1.1

294	0.454000	95.104.220.29	192.168.1.6	662	response
441	10.421762	195.201.241.83	192.168.1.6	662	HTTP/1.1 200 OK (text/css)

Ο server λοιπόν του book4book έχει ΚΑΙ αυτός έκδοση HTTP 1.1

Server: Apache/2.4.18

Και εδώ βλέπουμε ότι ο web server του book4book χρησιμοποιεί Apache HTTP Server software.