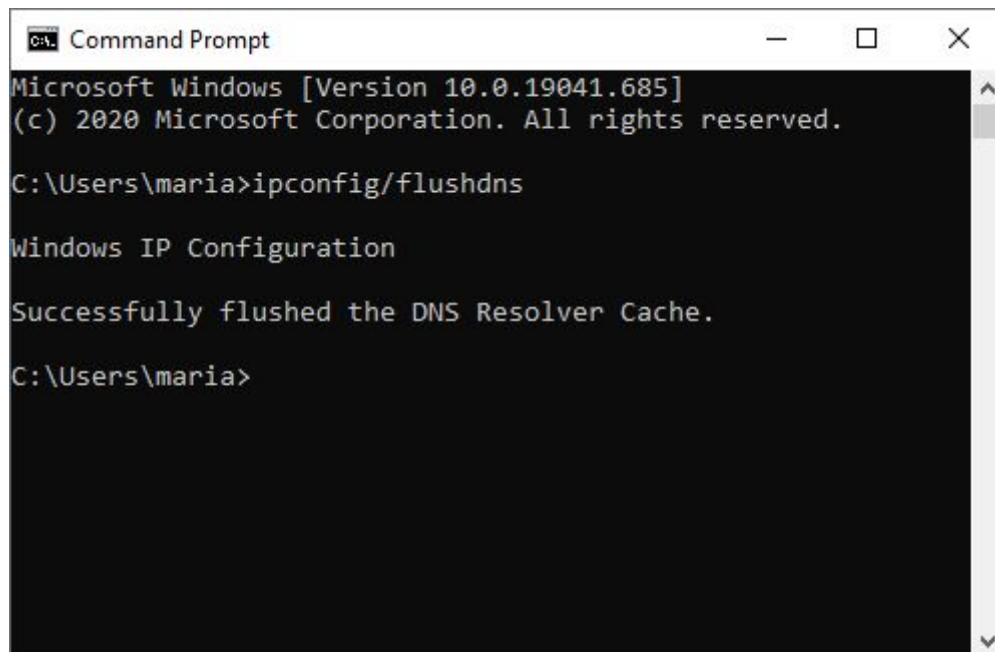


ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

2η ΕΡΓΑΣΙΑ

Σταυρουλάκη Μαρία, 3160168

ΒΗΜΑΤΑ:



```
Command Prompt
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\maria>ipconfig /flushdns

Windows IP Configuration

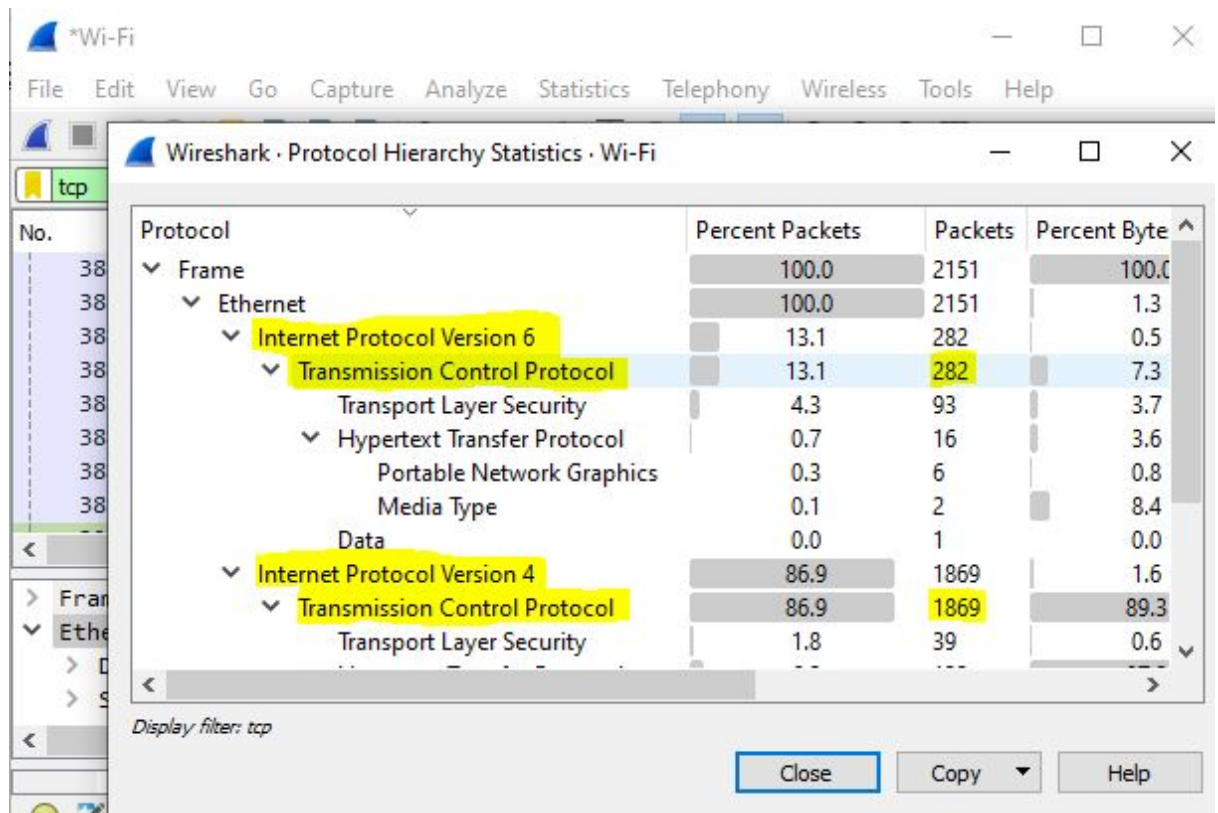
Successfully flushed the DNS Resolver Cache.

C:\Users\maria>
```

ΕΡΩΤΗΣΕΙΣ:

1. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Στάλθηκαν 282 πακέτα TCP για IPv6 και 1869 για IPv4.

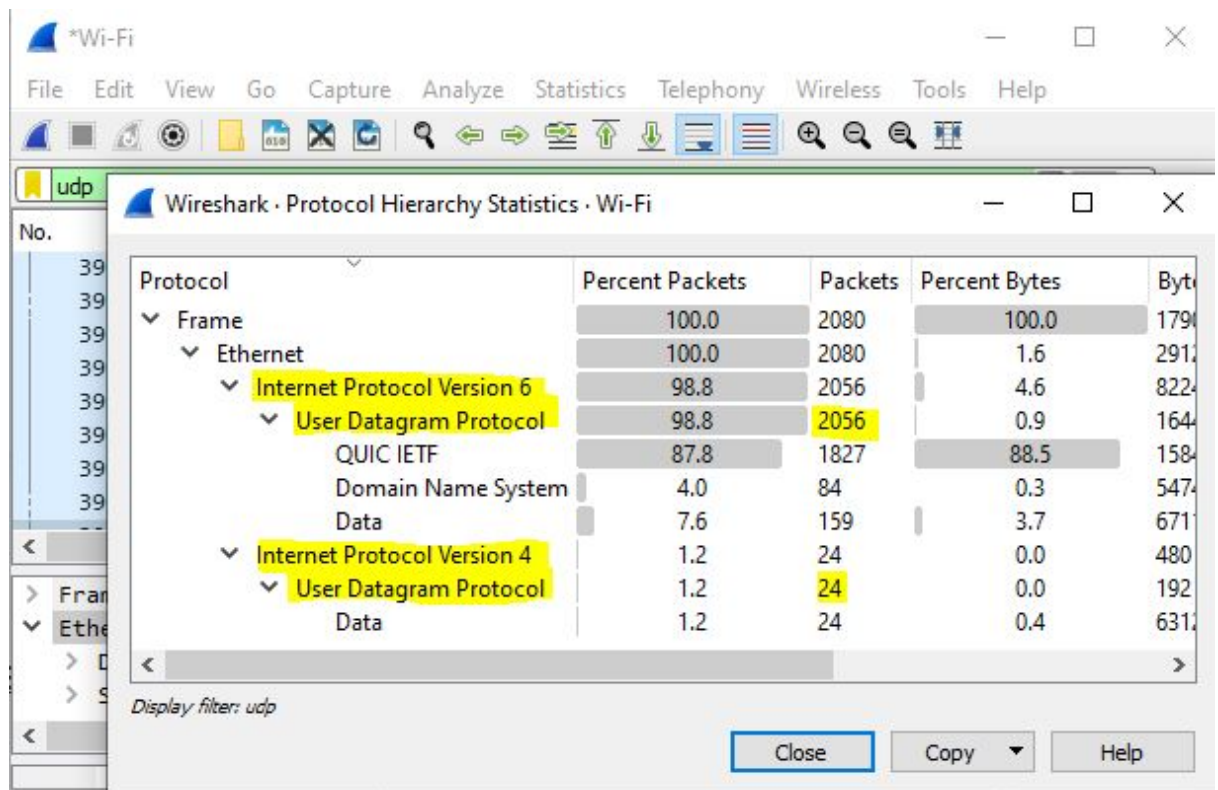


The screenshot shows the Wireshark Protocol Hierarchy Statistics window for the 'tcp' filter. The table displays the distribution of TCP packets across various protocols. The 'Packets' column shows 282 for IPv6 and 1869 for IPv4.

Protocol	Percent Packets	Packets	Percent Byte
Frame	100.0	2151	100.0
Ethernet	100.0	2151	1.3
Internet Protocol Version 6	13.1	282	0.5
Transmission Control Protocol	13.1	282	7.3
Transport Layer Security	4.3	93	3.7
Hypertext Transfer Protocol	0.7	16	3.6
Portable Network Graphics	0.3	6	0.8
Media Type	0.1	2	8.4
Data	0.0	1	0.0
Internet Protocol Version 4	86.9	1869	1.6
Transmission Control Protocol	86.9	1869	89.3
Transport Layer Security	1.8	39	0.6

Display filter: tcp

Στάλθηκαν 2056 πακέτα UDP για IPv6 και 24 για IPv4.



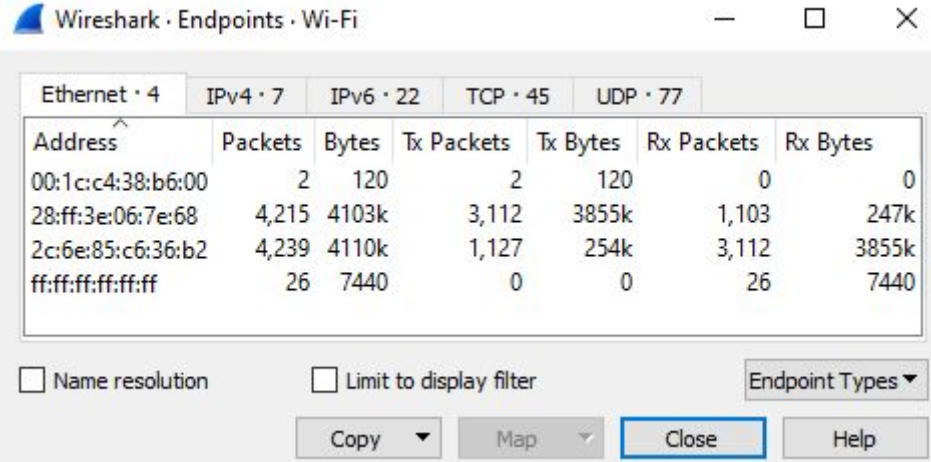
The screenshot shows the Wireshark Protocol Hierarchy Statistics window for the 'udp' filter. The table displays the distribution of UDP packets across various protocols. The 'Packets' column shows 2056 for IPv6 and 24 for IPv4.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	2080	100.0	1794
Ethernet	100.0	2080	1.6	2912
Internet Protocol Version 6	98.8	2056	4.6	8224
User Datagram Protocol	98.8	2056	0.9	1648
QUIC IETF	87.8	1827	88.5	1584
Domain Name System	4.0	84	0.3	5472
Data	7.6	159	3.7	6712
Internet Protocol Version 4	1.2	24	0.0	480
User Datagram Protocol	1.2	24	0.0	192
Data	1.2	24	0.4	6312

Display filter: udp

2. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε ποιες συσκευές αντιστοιχούν;

00:1c:c4:38:b6:00
 28:ff:3e:06:7e:68
 2c:6e:85:c6:36:b2
 ff:ff:ff:ff:ff



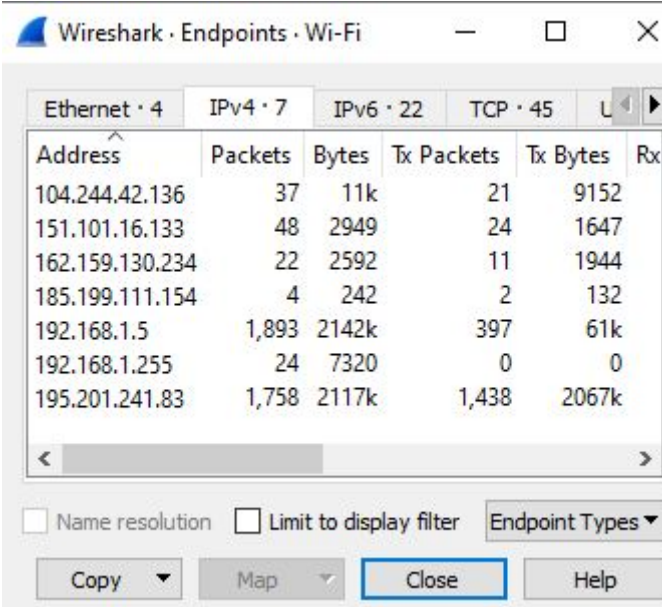
Wireshark · Endpoints · Wi-Fi

Ethernet · 4		IPv4 · 7		IPv6 · 22		TCP · 45		UDP · 77	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
00:1c:c4:38:b6:00	2	120	2	120	0	0			
28:ff:3e:06:7e:68	4,215	4103k	3,112	3855k	1,103	247k			
2c:6e:85:c6:36:b2	4,239	4110k	1,127	254k	3,112	3855k			
ff:ff:ff:ff:ff	26	7440	0	0	26	7440			

☐ Name resolution
 ☐ Limit to display filter
 Endpoint Types ▼
 Copy ▼ Map ▼ Close Help

3. Πόσα και ποια είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγήστε γιατί συμβαίνει αυτό.

IPv4:

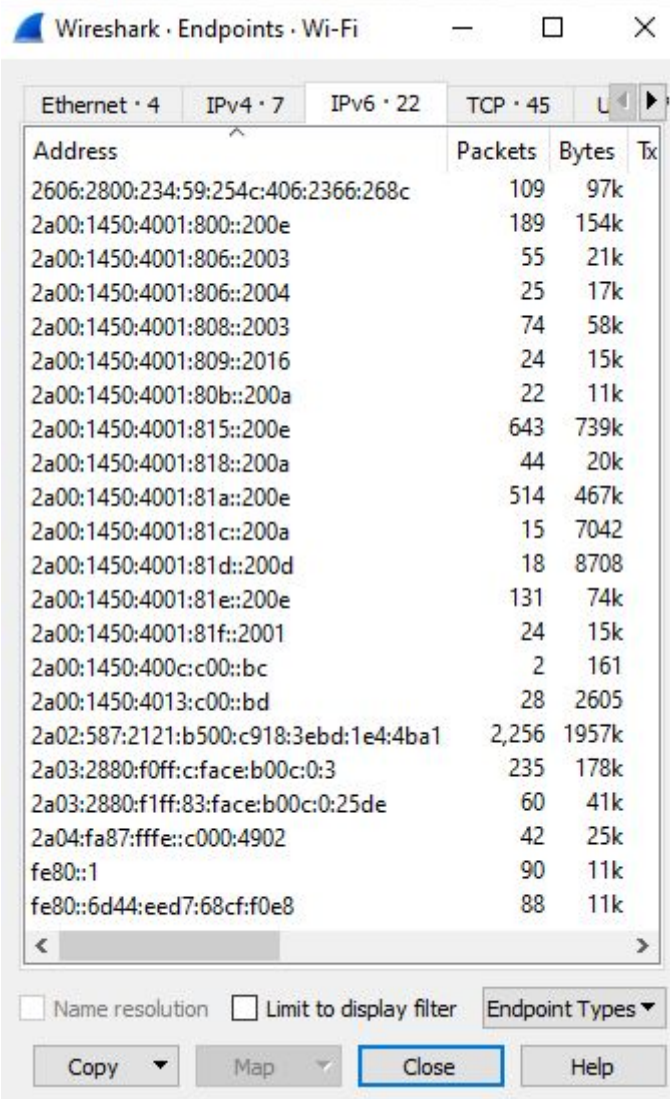


Wireshark · Endpoints · Wi-Fi

Ethernet · 4		IPv4 · 7		IPv6 · 22		TCP · 45		UDP · 77	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
104.244.42.136	37	11k	21	9152					
151.101.16.133	48	2949	24	1647					
162.159.130.234	22	2592	11	1944					
185.199.111.154	4	242	2	132					
192.168.1.5	1,893	2142k	397	61k					
192.168.1.255	24	7320	0	0					
195.201.241.83	1,758	2117k	1,438	2067k					

☐ Name resolution
 ☐ Limit to display filter
 Endpoint Types ▼
 Copy ▼ Map ▼ Close Help

IPv6:



The screenshot shows the 'Endpoints' window in Wireshark for the 'Wi-Fi' interface. It displays a list of IPv6 addresses and their corresponding packet and byte counts. The window has tabs for 'Ethernet', 'IPv4', 'IPv6', and 'TCP'. The 'IPv6' tab is selected, showing 22 endpoints. The table below represents the data shown in the window.

Address	Packets	Bytes
2606:2800:234:59:254c:406:2366:268c	109	97k
2a00:1450:4001:800::200e	189	154k
2a00:1450:4001:806::2003	55	21k
2a00:1450:4001:806::2004	25	17k
2a00:1450:4001:808::2003	74	58k
2a00:1450:4001:809::2016	24	15k
2a00:1450:4001:80b::200a	22	11k
2a00:1450:4001:815::200e	643	739k
2a00:1450:4001:818::200a	44	20k
2a00:1450:4001:81a::200e	514	467k
2a00:1450:4001:81c::200a	15	7042
2a00:1450:4001:81d::200d	18	8708
2a00:1450:4001:81e::200e	131	74k
2a00:1450:4001:81f::2001	24	15k
2a00:1450:400c:c00::bc	2	161
2a00:1450:4013:c00::bd	28	2605
2a02:587:2121:b500:c918:3ebd:1e4:4ba1	2,256	1957k
2a03:2880:f0ff:c:face:b00c:0:3	235	178k
2a03:2880:f1ff:83:face:b00c:0:25de	60	41k
2a04:fa87:fffe::c000:4902	42	25k
fe80::1	90	11k
fe80::6d44:eed7:68cf:f0e8	88	11k

Τα endpoints δεν ταυτίζονται καθώς για το ethernet αντιστοιχούν σε διευθύνσεις MAC, ενώ για IPv4 και IPv6 σε διευθύνσεις ip.

4. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.

Οι θύρες που χρησιμοποιήθηκαν για την ερώτηση του DNS είναι οι εξής:

Source: 53699, 55564, 63644, 56484, 61148, 57584, 64750, 599947, 58528, 61047, 56525, 56489, 65368, 65314, 63556, 62617,..., 56847

Destination: 53 (για όλες)

Οι θύρες που χρησιμοποιήθηκαν για την απάντηση του DNS είναι οι εξής:

Source: 53 (για όλες)

Destination: 53699, 55564, 56484, 63644, 61148, 57584, 64750, 59947,

58528, 61047, 56489, 56525, 65368, 65314,..., 56847

5. Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

Μπορούμε να διακρίνουμε αν ένα πακέτο περιέχει αίτημα ερώτησης προς τον DNS server όταν το destination port είναι 53 και απάντηση όταν το source port είναι 53. Επίσης στη στήλη info του wireshark χαρακτηρίζεται ως standard query και standard query response αντίστοιχα.

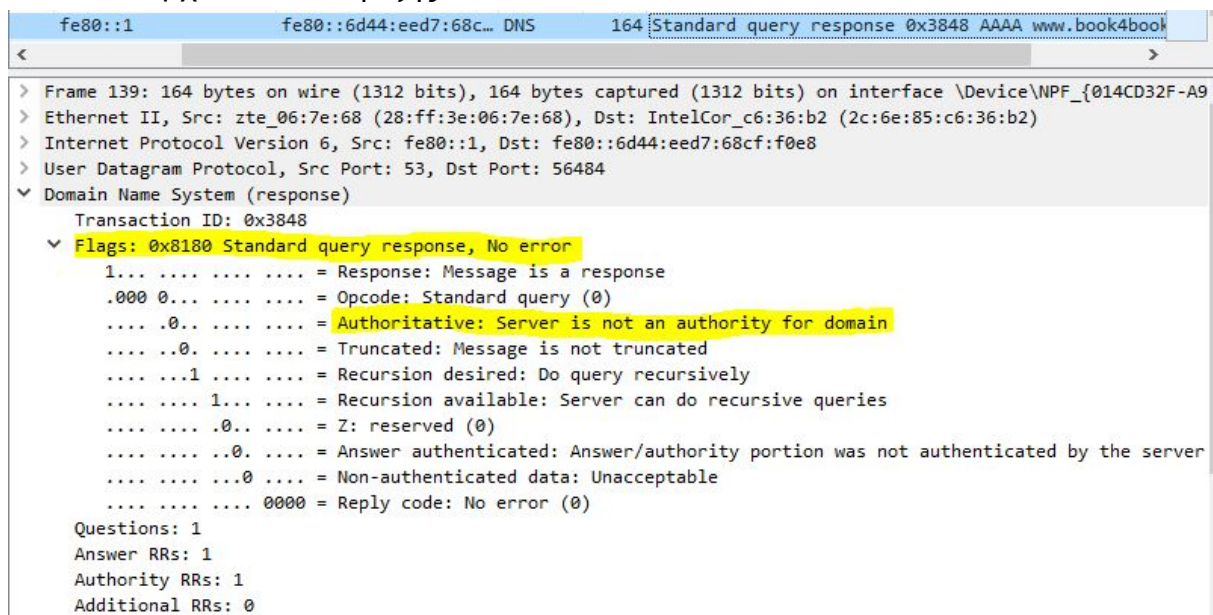
Standard query 0x3848 AAAA www.book4book.gr

Standard query response 0x3848 AAAA www.book4book.gr CNAME book4book.gr SO...

Ο τρόπος σύνδεσης γίνεται μέσω του ίδιου port που δίνεται ως destination port για την ερώτηση και ως source port για την απάντηση.

6. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει είναι authoritative για το συγκεκριμένο domain; Ο name server που μας έχει απαντήσει είναι authoritative για το συγκεκριμένο domain;

Υπάρχει και είναι η εξής:



Ο name server δεν είναι authoritative για το συγκεκριμένο domain.

7. Το όνομα www.book4book.gr είναι domain ή canonical name; Ποια είναι η IP διεύθυνση που αντιστοιχεί στο www.book4book.gr;

Το www.book4book.gr είναι canonical name και η ip που του αντιστοιχεί είναι [195.201.241.83].

```
✓ www.book4book.gr: type CNAME, class IN, cname book4book.gr
  Name: www.book4book.gr
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 2
  CNAME: book4book.gr
```

```
C:\Users\maria>tracert www.book4book.gr

Tracing route to book4book.gr [195.201.241.83]
over a maximum of 30 hops:
```

8. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.book4book.gr υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

Βήμα Πρώτο:

Ο Client στέλνει στον Server ένα μήνυμα SYN που περιέχει μία ακολουθία επιλεγμένων αριθμών με την οποία θα ξεκινάνε τα segments του.

Βήμα Δεύτερο:

Ο Server απαντάει στέλνοντας στον Client ένα μήνυμα SYNACK, το οποίο σηματοδοτεί ότι είναι έτοιμος για σύνδεση. Το μήνυμα αυτό περιέχει την απάντηση του Server, ACK (acknowledgement) και τον αριθμό με τον οποίο θα ξεκινάει τα segments του (SYN).

Βήμα Τρίτο:

Ο Client αναγνωρίζει την απάντηση του Server (ACK - acknowledgement) και εγκαθιδρύεται η σύνδεση.

9. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο. Ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιεί το HTTP;

GET:

Source port: 50883, 50885, 50886, 50887, 50888, 50889

Destination port: 80

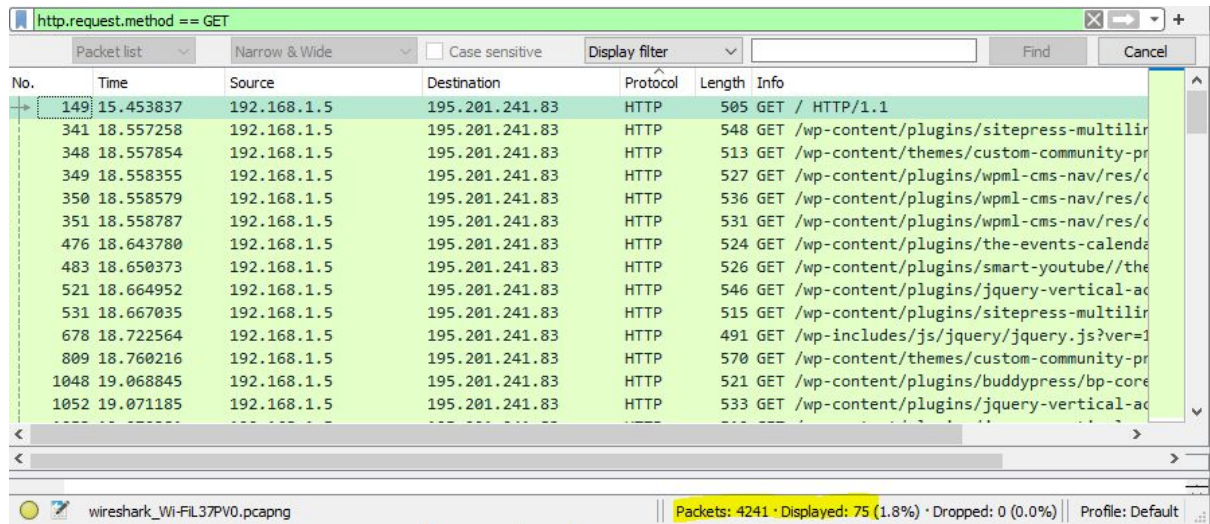
Απάντηση:

Source port: 80

Destination port: 50883, 50885, 50886, 50887, 50888, 50889

10. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;

Στάλθηκαν 4241 πακέτα στην IP διεύθυνση [195.201.241.83], η οποία αντιστοιχεί στο www.book4book.gr.



No.	Time	Source	Destination	Protocol	Length	Info
149	15.453837	192.168.1.5	195.201.241.83	HTTP	505	GET / HTTP/1.1
341	18.557258	192.168.1.5	195.201.241.83	HTTP	548	GET /wp-content/plugins/sitepress-multilir
348	18.557854	192.168.1.5	195.201.241.83	HTTP	513	GET /wp-content/themes/custom-community-pr
349	18.558355	192.168.1.5	195.201.241.83	HTTP	527	GET /wp-content/plugins/wpml-cms-nav/res/c
350	18.558579	192.168.1.5	195.201.241.83	HTTP	536	GET /wp-content/plugins/wpml-cms-nav/res/c
351	18.558787	192.168.1.5	195.201.241.83	HTTP	531	GET /wp-content/plugins/wpml-cms-nav/res/c
476	18.643780	192.168.1.5	195.201.241.83	HTTP	524	GET /wp-content/plugins/the-events-calenda
483	18.650373	192.168.1.5	195.201.241.83	HTTP	526	GET /wp-content/plugins/smart-youtube//the
521	18.664952	192.168.1.5	195.201.241.83	HTTP	546	GET /wp-content/plugins/jquery-vertical-ac
531	18.667035	192.168.1.5	195.201.241.83	HTTP	515	GET /wp-content/plugins/sitepress-multilir
678	18.722564	192.168.1.5	195.201.241.83	HTTP	491	GET /wp-includes/js/jquery/jquery.js?ver=1
809	18.760216	192.168.1.5	195.201.241.83	HTTP	570	GET /wp-content/themes/custom-community-pr
1048	19.068845	192.168.1.5	195.201.241.83	HTTP	521	GET /wp-content/plugins/buddypress/bp-core
1052	19.071185	192.168.1.5	195.201.241.83	HTTP	533	GET /wp-content/plugins/jquery-vertical-ac

11. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server; Ποιο λογισμικό web server «τρέχει» ο server που σας απάντησε για το site www.book4book.gr;

Ο browser μου τρέχει την έκδοση HTTP/1.1

```
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.book4book.gr\r\n
    Connection: keep-alive\r\n
```

Ο Server τρέχει την έκδοση HTTP/1.1 και το software Apache.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 12 Dec 2020 10:52:03 GMT\r\n
    Server: Apache\r\n
```