

1)

ημοποιήθηκαν από το HTTP πρωτόκολλο. Ποιο πρωτόκολλο επιπέδου μεταφοράς

2)

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:80:c2:00:00:00	7	420	0	0	7	420
10:78:d2:95:a3:c3	1.307	1142k	468	57k	839	1085k
28:ff:3e:29:51:2c	1.306	1142k	839	1085k	467	57k
f4:f2:6d:b0:85:cb	7	420	7	420	0	0
ff:ff:ff:ff:ff:ff	1	42	0	0	1	42

Το 2ο είναι η MAC address του pc

Το 3ο είναι η MAC address του router

3)

4)

The image shows a Wireshark packet capture window titled '\*Ethernet'. The packet list pane displays several DNS packets. Packet 12 is highlighted with a red box. The packet details pane shows the structure of this packet, with the Source Port (54255) and Destination Port (53) also highlighted with red boxes.

No.	Time	Source	Destination	Protocol	Length	Info
11	3.785412	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	96	Standard query 0x0320 A www.book4book.gr
12	3.785703	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	96	Standard query 0x61bf AAAA www.book4book.gr
13	3.787063	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	112	Standard query response 0x0320 A www.book4book.gr A
14	3.891530	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	164	Standard query response 0x61bf AAAA www.book4book.gr
985	7.285822	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	95	Standard query 0x1538 A www.youtube.com
986	7.285886	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	95	Standard query 0x14fb AAAA www.youtube.com
987	7.287994	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	255	Standard query response 0x1538 A www.youtube.com A 1
988	7.305407	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	241	Standard query response 0x14fb AAAA www.youtube.com
1038	8.123890	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	99	Standard query 0x287c A maps.googleapis.com
1039	8.124406	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	99	Standard query 0x881b AAAA maps.googleapis.com
1040	8.142594	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	115	Standard query response 0x287c A maps.googleapis.com
1041	8.144764	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	143	Standard query response 0x881b AAAA maps.googleapis.com
1076	8.938701	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	95	Standard query 0x7a7a A apis.google.com
1077	8.939152	fe80::b0d9:8bf5:2b2...	fe80::1	DNS	95	Standard query 0x8cf7 AAAA apis.google.com
1079	8.957604	fe80::1	fe80::b0d9:8bf5:2b2...	DNS	132	Standard query response 0x7a7a A apis.google.com CNA

Frame 12: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NPF\_{81BE2529-437A-48B6-94F5-B1B66F8C4F1D}, Ethernet II, Src: Elitegro\_95:a3:c3 (10:78:d2:95:a3:c3), Dst: zte\_29:51:2c (28:ff:3e:29:51:2c)

Internet Protocol Version 6, Src: fe80::b0d9:8bf5:2b29:7d1, Dst: fe80::1

User Datagram Protocol, Src Port: 54255, Dst Port: 53

- Source Port: 54255
- Destination Port: 53
- Length: 42
- Checksum: 0xd07 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 1]
- [Timestamps]
- UDP payload (34 bytes)
- Domain Name System (query)

5)

The top screenshot shows a list of DNS traffic in Wireshark. The table below represents the data shown in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
11	3.785412	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	96	Standard query 0x0320 A www.book4book.gr
12	3.785703	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	96	Standard query 0x61bf AAAA www.book4book.gr
13	3.787063	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	112	Standard query response 0x0320 A www.book4book.gr
14	3.891530	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	164	Standard query response 0x61bf AAAA www.book4book.gr
985	7.285822	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x1538 A www.youtube.com
986	7.285886	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x14fb AAAA www.youtube.com
987	7.287994	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	255	Standard query response 0x1538 A www.youtube.com
988	7.305407	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	241	Standard query response 0x14fb AAAA www.youtube.com
1038	8.123890	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	99	Standard query 0x287c A maps.googleapis.com
1039	8.124406	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	99	Standard query 0x881b AAAA maps.googleapis.com
1040	8.142594	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	115	Standard query response 0x287c A maps.googleapis.com
1041	8.144764	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	143	Standard query response 0x881b AAAA maps.googleapis.com
1076	8.938701	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x7a7a A apis.google.com
1077	8.939152	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x8cf7 AAAA apis.google.com
1079	8.957604	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	132	Standard query response 0x7a7a A apis.google.com

The detailed view of Frame 11 shows:

```

> Frame 11: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NPF_{81BE2529-437A-48B6-94F5-B1B66F8C4F1D},
> Ethernet II, Src: Elitagro_95:a3:c3 (10:78:d2:95:a3:c3), Dst: zte_29:51:2c (28:ff:3e:29:51:2c)
> Internet Protocol Version 6, Src: fe80::b0d9:8bf5:2b29:7d1, Dst: fe80::1
> User Datagram Protocol, Src Port: 55943, Dst Port: 53
  Source Port: 55943
  Destination Port: 53
  Length: 42
  Checksum: 0x6d07 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
  UDP payload (34 bytes)
  Domain Name System (query)

```

The bottom screenshot shows a similar list of DNS traffic, with a detailed view of a response for 'www.book4book.gr'.

No.	Time	Source	Destination	Protocol	Length	Info
11	3.785412	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	96	Standard query 0x0320 A www.book4book.gr
12	3.785703	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	96	Standard query 0x61bf AAAA www.book4book.gr
13	3.787063	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	112	Standard query response 0x0320 A www.book4book.gr
14	3.891530	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	164	Standard query response 0x61bf AAAA www.book4book.gr
985	7.285822	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x1538 A www.youtube.com
986	7.285886	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x14fb AAAA www.youtube.com
987	7.287994	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	255	Standard query response 0x1538 A www.youtube.com
988	7.305407	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	241	Standard query response 0x14fb AAAA www.youtube.com
1038	8.123890	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	99	Standard query 0x287c A maps.googleapis.com
1039	8.124406	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	99	Standard query 0x881b AAAA maps.googleapis.com
1040	8.142594	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	115	Standard query response 0x287c A maps.googleapis.com
1041	8.144764	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	143	Standard query response 0x881b AAAA maps.googleapis.com
1076	8.938701	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x7a7a A apis.google.com
1077	8.939152	fe80::b0d9:8bf5:2b29:7d1	fe80::1	DNS	95	Standard query 0x8cf7 AAAA apis.google.com
1079	8.957604	fe80::1	fe80::b0d9:8bf5:2b29:7d1	DNS	132	Standard query response 0x7a7a A apis.google.com

The detailed view of Frame 13 shows:

```

> Frame 13: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{81BE2529-437A-48B6-94F5-B1B66F8C4F1D},
> Ethernet II, Src: zte_29:51:2c (28:ff:3e:29:51:2c), Dst: Elitagro_95:a3:c3 (10:78:d2:95:a3:c3)
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b0d9:8bf5:2b29:7d1
> User Datagram Protocol, Src Port: 53, Dst Port: 55943
  Source Port: 53
  Destination Port: 55943
  Length: 58
  Checksum: 0x0b9b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
  UDP payload (50 bytes)
  Domain Name System (response)

```

Το διακρίνουμε γιατί στο info μας λέει standard query response

Το πακέτο συνδέεται επειδή βλέπουμε ότι αντιστρέφονται τα destination και source port. Επομένως καταλαβαίνουμε ότι αναφέρονται στο ίδιο πακέτο.

6)





Για να γίνει η χειραψία 3 βημάτων πρέπει να υπάρχει σταθερή συνδεση .Η σύνδεση πρέπει να είναι full duplex και οι δυο μεριές πρέπει να συγχρονίζονται (syn) και να γνωρίζονται(ack).Για να γίνει η ανταλλαγή των flags, γίνονται σε 3 βήματα SYN, SYN-ACK, and ACK

9)

9)

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
18	3.970295	192.168.1.9	195.201.241.83	HTTP	595	GET / HTTP/1.1
71	5.773520	192.168.1.9	195.201.241.83	HTTP	564	GET /wp-content/plugins/jquery-vertical-accordion-menu/sk
253	5.859443	195.201.241.83	192.168.1.9	HTTP	1371	HTTP/1.1 200 OK (text/css)
403	5.952866	192.168.1.9	195.201.241.83	HTTP	519	GET /none HTTP/1.1
962	6.056028	195.201.241.83	192.168.1.9	HTTP	569	HTTP/1.1 404 Not Found (text/html)
979	6.058605	195.201.241.83	192.168.1.9	HTTP	904	HTTP/1.1 200 OK (text/html)
1072	8.834089	192.168.1.9	195.201.241.83	HTTP	503	GET /r HTTP/1.1
1074	8.908676	195.201.241.83	192.168.1.9	HTTP	570	HTTP/1.1 404 Not Found (text/html)
1141	10.370223	2a02:587:2d06:7700::...	2606:2800:234:59:254c:406:2...	HTTP	420	GET /widgets.js?_=1608463723050 HTTP/1.1
1179	10.480983	2606:2800:234:59:25...	2a02:587:2d06:7700:49a1:de7...	HTTP	1271	HTTP/1.1 200 OK (application/javascript)
2	0.737853	52.109.88.177	192.168.1.9	TCP	60	443 → 62032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2.185434	2a02:587:2d06:7700::...	2620:1ec:a92::156	TCP	75	61984 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment
7	2.228351	2620:1ec:a92::156	2a02:587:2d06:7700:49a1:de7...	TCP	86	443 → 61984 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
8	2.728690	13.105.66.144	192.168.1.9	TCP	60	443 → 62035 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	3.763413	40.126.1.129	192.168.1.9	TCP	60	443 → 62037 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	3.782280	2a02:587:2d06:7700::...	2606:2800:234:59:254c:406:2...	TCP	74	61978 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	3.893769	192.168.1.9	195.201.241.83	TCP	66	62065 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S
16	3.952393	195.201.241.83	192.168.1.9	TCP	66	80 → 62065 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=145
17	3.952590	192.168.1.9	195.201.241.83	TCP	54	62065 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
20	4.029989	195.201.241.83	192.168.1.9	TCP	60	80 → 62065 [ACK] Seq=1 Ack=542 Win=30336 Len=0
23	5.657795	195.201.241.83	192.168.1.9	TCP	1506	80 → 62065 [ACK] Seq=1 Ack=542 Win=30336 Len=1452 [TCP se
24	5.658066	195.201.241.83	192.168.1.9	TCP	1506	80 → 62065 [ACK] Seq=1453 Ack=542 Win=30336 Len=1452 [TCP se
25	5.658130	192.168.1.9	195.201.241.83	TCP	54	62065 → 80 [ACK] Seq=542 Ack=2905 Win=132096 Len=0

Source: Elitegro\_95:a3:c3 (10:78:d2:95:a3:c3)  
Address: Elitegro\_95:a3:c3 (10:78:d2:95:a3:c3)  
.....0..... = LG bit: Globally unique address (factory default)  
.....0..... = IG bit: Individual address (unicast)  
Type: IPv4 (0x0000)  
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 195.201.241.83  
Transmission Control Protocol, Src Port: 62065, Dst Port: 80, Seq: 1, Ack: 1, Len: 541  
Source Port: 62065  
Destination Port: 80  
[Stream Index: 5]  
[TCP Segment Len: 541]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 2702122138  
[Next Sequence Number: 542 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 1151930919

10)

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
18	3.970295	192.168.1.9	195.201.241.83	HTTP	595	GET / HTTP/1.1
71	5.773520	192.168.1.9	195.201.241.83	HTTP	564	GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.
253	5.859443	195.201.241.83	192.168.1.9	HTTP	1371	HTTP/1.1 200 OK (text/css)
403	5.952866	192.168.1.9	195.201.241.83	HTTP	519	GET /none HTTP/1.1
962	6.056028	195.201.241.83	192.168.1.9	HTTP	569	HTTP/1.1 404 Not Found (text/html)
979	6.058605	195.201.241.83	192.168.1.9	HTTP	904	HTTP/1.1 200 OK (text/html)
1072	8.834089	192.168.1.9	195.201.241.83	HTTP	503	GET /r HTTP/1.1
1074	8.908676	195.201.241.83	192.168.1.9	HTTP	570	HTTP/1.1 404 Not Found (text/html)
1141	10.370223	2a02:587:2d06:7700::...	2606:2800:234:59:254c:406:2...	HTTP	420	GET /widgets.js?_=1608463723050 HTTP/1.1
1179	10.480983	2606:2800:234:59:25...	2a02:587:2d06:7700:49a1:de7...	HTTP	1271	HTTP/1.1 200 OK (application/javascript)
2	0.737853	52.109.88.177	192.168.1.9	TCP	60	443 → 62032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2.185434	2a02:587:2d06:7700::...	2620:1ec:a92::156	TCP	75	61984 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of
7	2.228351	2620:1ec:a92::156	2a02:587:2d06:7700:49a1:de7...	TCP	86	443 → 61984 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
8	2.728690	13.105.66.144	192.168.1.9	TCP	60	443 → 62035 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	3.763413	40.126.1.129	192.168.1.9	TCP	60	443 → 62037 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	3.782280	2a02:587:2d06:7700::...	2606:2800:234:59:254c:406:2...	TCP	74	61978 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	3.893769	192.168.1.9	195.201.241.83	TCP	66	62065 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
16	3.952393	195.201.241.83	192.168.1.9	TCP	66	80 → 62065 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 S
17	3.952590	192.168.1.9	195.201.241.83	TCP	54	62065 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
20	4.029989	195.201.241.83	192.168.1.9	TCP	60	80 → 62065 [ACK] Seq=1 Ack=542 Win=30336 Len=0
23	5.657795	195.201.241.83	192.168.1.9	TCP	1506	80 → 62065 [ACK] Seq=1 Ack=542 Win=30336 Len=1452 [TCP segme
24	5.658066	195.201.241.83	192.168.1.9	TCP	1506	80 → 62065 [ACK] Seq=1453 Ack=542 Win=30336 Len=1452 [TCP se
25	5.658130	192.168.1.9	195.201.241.83	TCP	54	62065 → 80 [ACK] Seq=542 Ack=2905 Win=132096 Len=0

Source: Elitegro\_95:a3:c3 (10:78:d2:95:a3:c3)

Έστειλα 3 get στο book4book.gr(195.201.241.83)

11)Τρέχω την έκδοση HTTP 1.1 όπως και ο σερβερ. Ο σερβερ λειτουργεί με apache

