Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής
Μάθημα: Δίκτυα Επικοινωνιών
Ακαδημαϊκό έτος: 2022–23
Υπεύθυνη φοιτητές: Μαρία Κονταράτου (3200078), Γεώργιος Κουμουνδούρος (3200083)

1η Εργασία

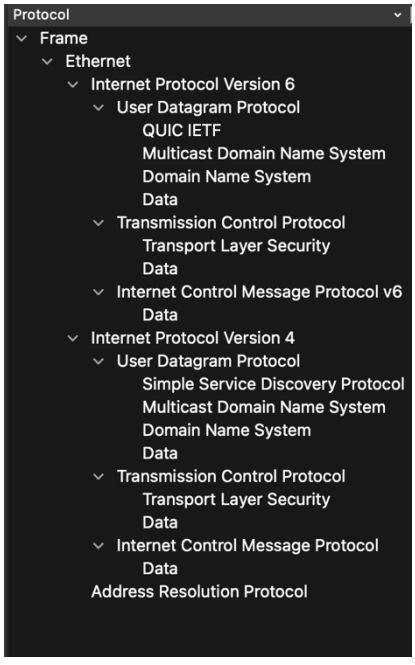
Μέρος Α΄

```
(base) maria_kontaratou@MacBook-Pro ~ % traceroute www.ieee.org
traceroute to e1630.c.akamaiedge.net (23.207.125.246), 64 hops max, 52 byte packets
 1  speedport.ip (192.168.1.1)  4.118 ms  3.891 ms  2.826 ms
 2  80.106.125.100 (80.106.125.100)  29.757 ms  19.650 ms  25.968 ms
 3  79.128.224.104 (79.128.224.104)  12.153 ms
    79.128.227.228 (79.128.227.228)  13.637 ms
    79.128.224.104 (79.128.224.104)  12.789 ms
 4  kolasr01-hu-0-0-0-0.ath.oteglobe.gr (62.75.3.9)  13.576 ms  13.584 ms  19.055 ms
 5  62.75.4.130 (62.75.4.130)  56.843 ms  57.796 ms  56.919 ms
 6  * * *
 7  ae1.3115.edge7.london1.level3.net (4.69.166.2)  65.167 ms  80.641 ms
    ae2.3215.edge7.london1.level3.net (4.69.166.6)  58.667 ms
 8  ae-15.a02.londen12.uk.bb.gin.ntt.net (129.250.9.253)  64.994 ms  57.986 ms  71.690 ms
 9  ae-0.r21.londen12.uk.bb.gin.ntt.net (129.250.3.214)  58.663 ms
    ae-0.r20.londen12.uk.bb.gin.ntt.net (129.250.3.212)  58.182 ms  58.953 ms
10  ae-7.r20.nwrknj03.us.bb.gin.ntt.net (129.250.6.147)  129.549 ms
    ae-13.r25.asbnva02.us.bb.gin.ntt.net (129.250.2.111)  133.027 ms
    ae-7.r20.nwrknj03.us.bb.gin.ntt.net (129.250.6.147)  130.920 ms
11  ae-4.r24.sttlwa01.us.bb.gin.ntt.net (129.250.6.177)  195.646 ms *
    ae-2.r25.lsanca07.us.bb.gin.ntt.net (129.250.3.189)  202.740 ms
12  ae-13.r30.tokyjp05.jp.bb.gin.ntt.net (129.250.4.143)  310.930 ms
    ae-12.r31.tokyjp05.jp.bb.gin.ntt.net (129.250.3.192)  317.899 ms  305.939 ms
13  ae-2.r01.tokyjp08.jp.bb.gin.ntt.net (129.250.6.131)  360.806 ms
    ae-3.r01.tokyjp08.jp.bb.gin.ntt.net (129.250.6.133)  309.683 ms  301.732 ms
14  ae-0.akamai.tokyjp08.jp.bb.gin.ntt.net (61.200.91.198)  450.907 ms  439.608 ms  324.042 ms
15  * * *
16  * * *
17  a23-207-125-246.deploy.static.akamaitechnologies.com (23.207.125.246)  337.285 ms  306.651 ms  291.442 ms
```

1. Η ανίχνευση διήρκησε $t_{\text{τελευταίου πακέτου ICMP}} - t_{\text{πρώτου πακέτου ICMP}}$ = 62.747564 – 1.117684 = 61.62988

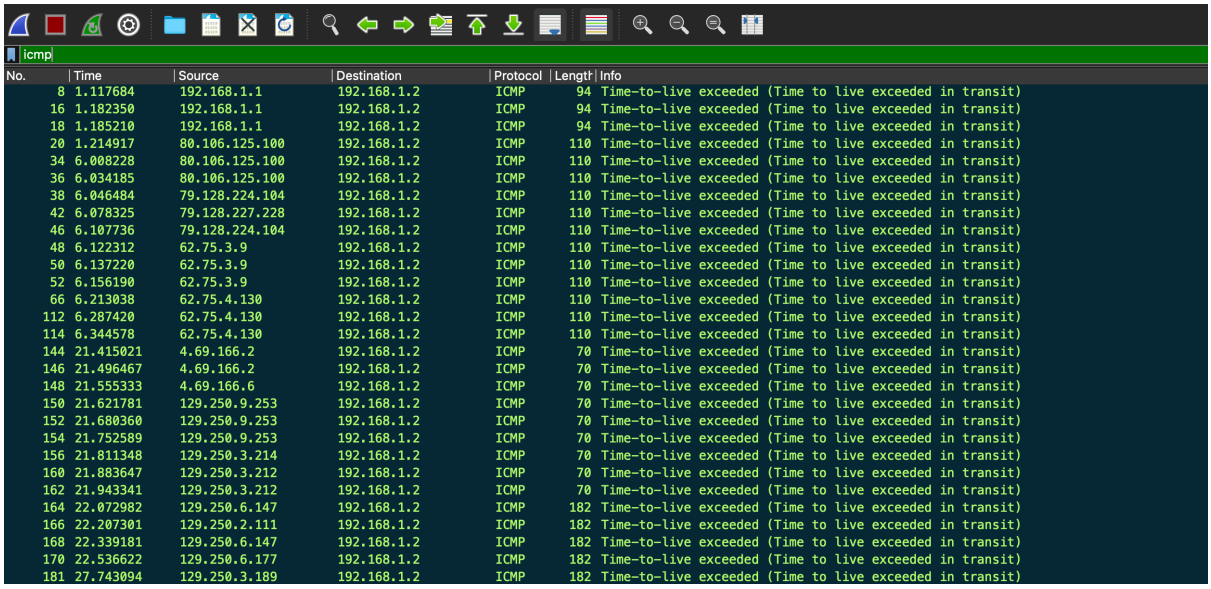
2.

Επίπεδο δικτύου	Επίπεδο Μεταφοράς	Επίπεδο Εφαρμογής
ARP	TCP	DNS
ICMPv6	UPD	TLSv1.2
	QUIC IETF	SSDP
		MDNS



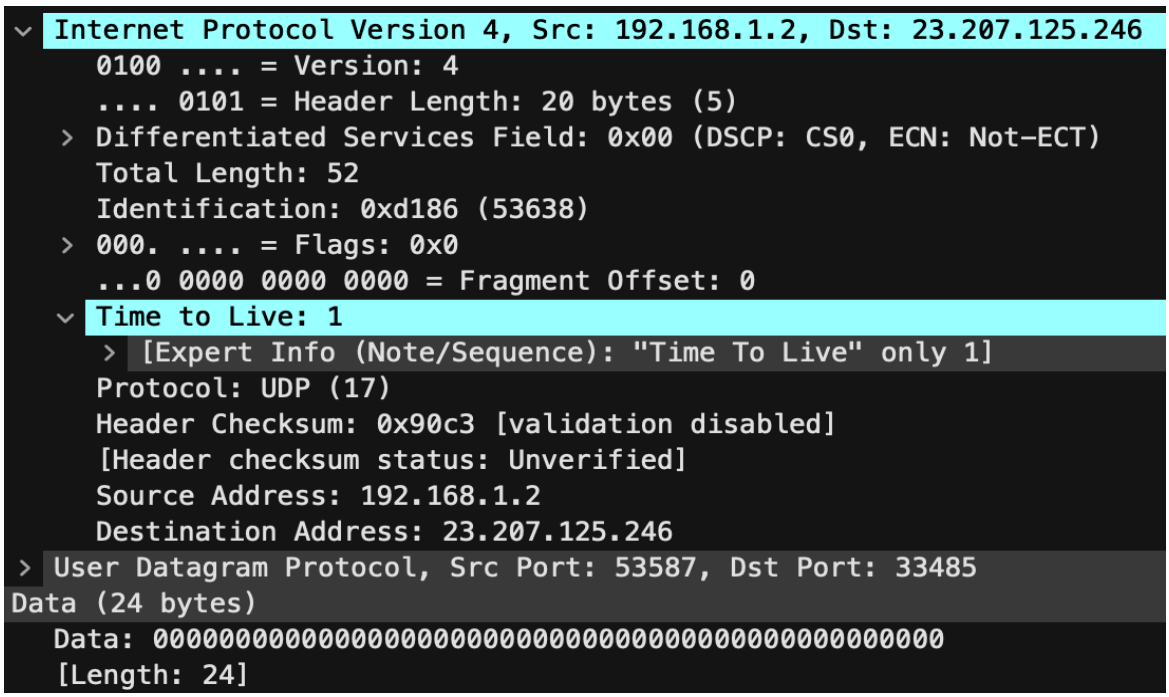
3. Τα DNS, SSDP, MDNS χρησιμοποιούν UPD ενώ το TLSv1.2 χρησιμοποιεί TCP

4. Γράφουμε στο filter ICMP ώστε να εμφανιστούν μόνο τα πακέτα που αφορούν το πρωτόκολλο.


icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	1.117684	192.168.1.1	192.168.1.2	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
16	1.182350	192.168.1.1	192.168.1.2	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
18	1.185210	192.168.1.1	192.168.1.2	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
20	1.214917	80.106.125.100	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
34	6.008228	80.106.125.100	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
36	6.034185	80.106.125.100	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
38	6.046484	79.128.224.104	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
42	6.078325	79.128.227.228	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
46	6.107736	79.128.224.104	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
48	6.122312	62.75.3.9	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
50	6.137220	62.75.3.9	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
52	6.156190	62.75.3.9	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
66	6.213038	62.75.4.130	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
112	6.287420	62.75.4.130	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
114	6.344578	62.75.4.130	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
144	21.415021	4.69.166.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
146	21.496467	4.69.166.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
148	21.555333	4.69.166.6	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
150	21.621781	129.250.9.253	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	21.680360	129.250.9.253	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
154	21.752589	129.250.9.253	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
156	21.811348	129.250.3.214	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
160	21.883647	129.250.3.212	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
162	21.943341	129.250.3.212	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
164	22.072982	129.250.6.147	192.168.1.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
166	22.207301	129.250.2.111	192.168.1.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
168	22.339181	129.250.6.147	192.168.1.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
170	22.536622	129.250.6.177	192.168.1.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
181	27.743094	129.250.3.189	192.168.1.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

5.



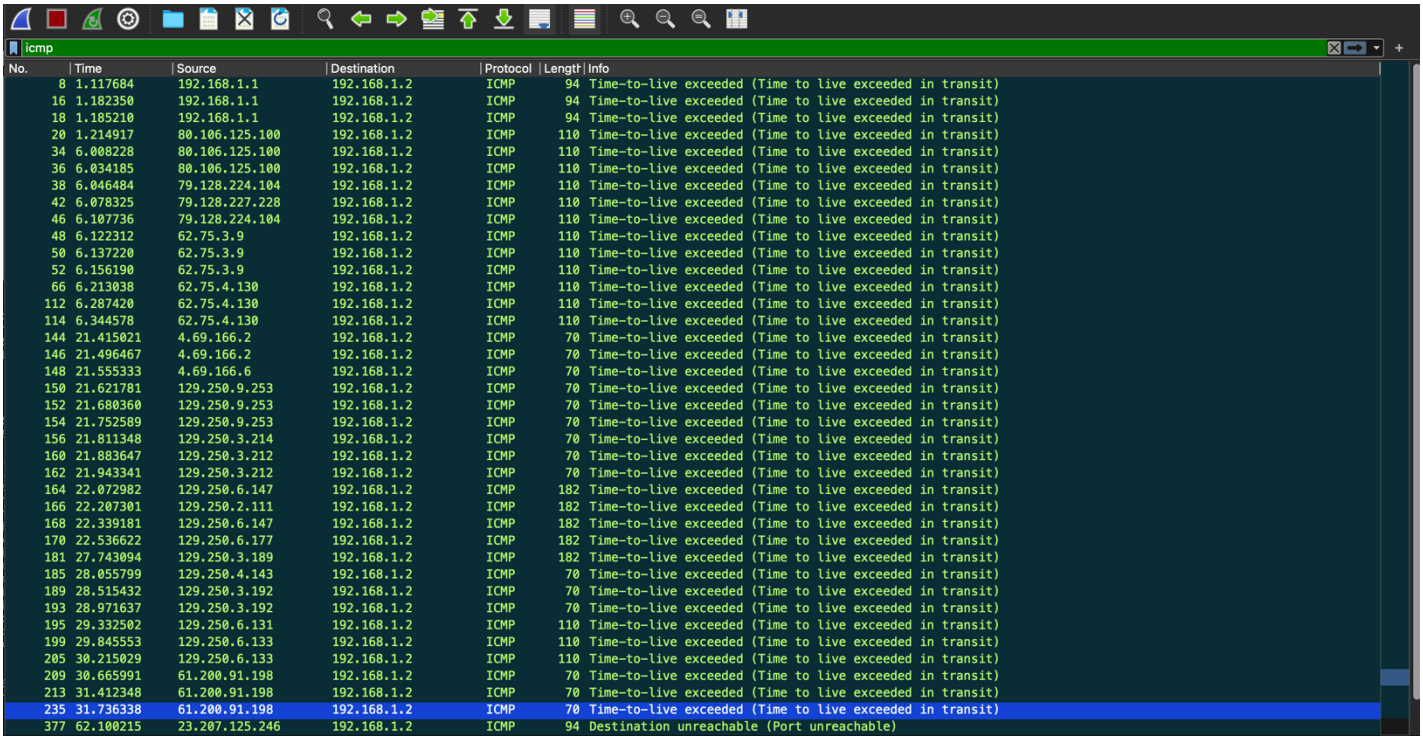
a. 23.207.125.246
b. 1
c. Total length: 52 bytes, data length: 24 bytes

6. a. IP_{source}: 192.168.1.1
b. IP_{source}: 192.168.1.2

7.

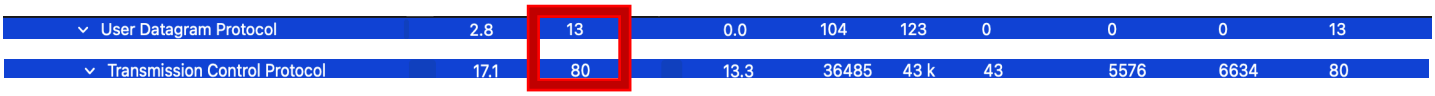
- 192.168.1.1
- 80.106.125.100
- 79.128.224.104
- 79.128.227.228
- 79.128.224.104
- 62.75.3.9
- 62.75.4.130
- 4.69.166.2
- 4.69.166.6
- 129.250.9.253
- 129.250.3.212
- 129.250.3.214
- 129.250.6.147
- 129.250.6.177
- 129.250.3.189
- 129.250.4.143
- 129.250.3.192
- 129.250.6.131
- 129.250.6.133
- 61.200.91.198

Παρατηρούμε ότι οι διευθύνσεις είναι ίδιες εκτός του τελευταίου IP address στο cmd που είναι ουσιαστικά το Echo reply



Μέρος Β΄

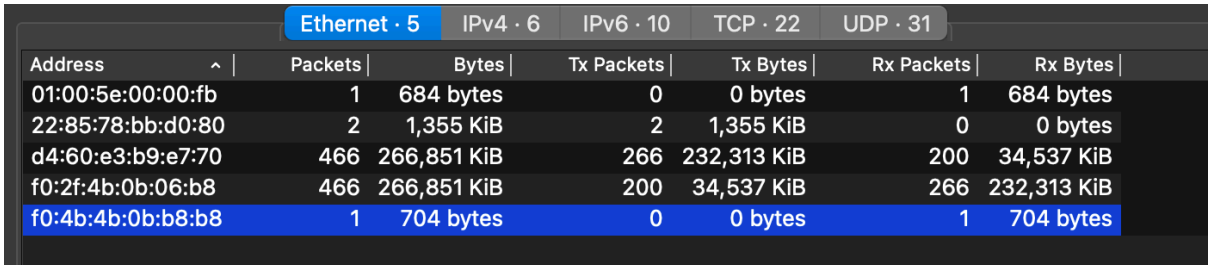
1. Έχουμε 13 πακέτα UPD και 80 πακέτα TCP



2.

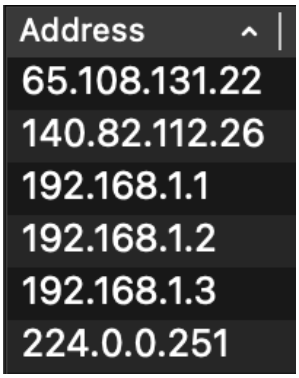
- 01:00:5e:00:00:fb
- 22:85:78:bb:d0:80
- d4:60:e3:b9:e7:70
- f0:2f:4b:0b:06:b8
- f0:4b:4b:0b:b8:b8

Το ethernet endpoint είναι ίδιας φύσης με το mac address του ethernet και τα endpoints αντιστοιχούν σε συσκευές που επικοινωνεί ο server.

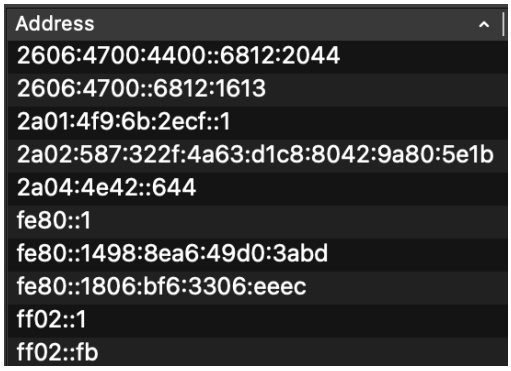


3.

Endpoints IPv4 (6)



Endpoints IPv6 (10)



Σε επίπεδο IP έχουμε συνολικά 16 endpoints, τα οποία δεν ταυτίζονται με εκείνα του ethernet καθώς τα μεν αναφέρονται σε IP ενώ τα δε σε MAC addresses

4. Από υπολογιστή σε DNS server για ερώτηση, όπου port A: source port και port B: destination port

Port A	Port B
15468	53
16707	53
17894	53
18139	53
33836	53
35796	53
37372	53
42535	53
42840	53
44765	53
51288	53
52296	53
52753	53
55287	53
56605	53
60575	53
60698	53
63123	53
64656	53
5353	5353
49816	53
50106	53
57007	53
58425	53
58606	53
63376	53
5353	5353

Οι θύρες για απάντηση του DNS server είναι αντεστραμμένες δηλαδή port B: source port και port A: destination port

5.
Αν το πακέτο έχει απάντηση σε ερώτημα τότε το destination είναι η IP, το source port 53 και αναγράφεται response.

```
Frame 7: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
Ethernet II, Src: Apple_0b:06:b8 (f0:2f:4b:0b:06:b8), Dst: Sercomm_b9:e7:70 (d4:60:e3:b9:e7:70)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 35796, Dst Port: 53
Domain Name System (query)
```

Αν το πακέτο έχει αίτημα στον DNS server τότε το source είναι η IP, το destination port 53 και αναγράφεται query.

```
Frame 268: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
Ethernet II, Src: Apple_0b:06:b8 (f0:2f:4b:0b:06:b8), Dst: Sercomm_b9:e7:70 (d4:60:e3:b9:e7:70)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 64656, Dst Port: 53
Domain Name System (query)
```

Το πακέτο ερώτησης και απάντησης συνδέονται μέσω του source port στην ερώτηση και destination port στην απάντηση.

6.
Υπάρχει flag, που μας ορίζει αν ο server που μας έχει απαντήσει δεν είναι authoritative για το εκάστοτε domain.

```
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
```

Ο Name Server δεν είναι authoritative άρα.

7.
Είναι alias ενώ το domain name είναι openoffice.org και η IP του είναι 65.108.131.22

8.

18	0.385379	192.168.1.2	65.108.131.22	TCP	78 53259 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2607483991 TSecr=0 SACK_PERM
19	0.471868	65.108.131.22	192.168.1.2	TCP	74 443 → 53259 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1452 SACK_PERM TSval=2038056950 TSecr=2607483991 WS…
20	0.472067	192.168.1.2	65.108.131.22	TCP	66 53259 → 443 [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=2607484078 TSecr=2038056950

(α) [SYN] Ο πελάτης θέλει να συνδεθεί με server και στέλνει μέσω SYN ένα segment . Το SYN δείχνει με ποιο αριθμό γίνεται έναρξη segments
(β) [SYN,ACK] Ο server απαντά στον πελάτη μέσω SYN, ACK. Το SYN δείχνει με ποιον αριθμό γίνεται έναρξη segments από τον server ενώ το ACK δείχνει την απάντηση στο αρχικά σταλμένο segment από τον πελάτη.
(γ) [ACK] Ο πελάτης αναγνωρίζει το response και ουσιαστικά εγκαθιδρύεται ως μια secure connection μεταξύ τους για την εκάστοτε μεταφορά δεδομένων.

9.

Source port	Destination port
53259	443
53260	443
53266	443
53267	443
53268	443
53269	443
63289	80

10.
Στάλθηκε ένα HTTP GET request

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
50	0.675074	2a02:587:322f:4a63…	2606:4700:4400::68…	HTTP	440	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQ
61	0.759908	2606:4700:4400::68…	2a02:587:322f:4a63…	OCSP	1100	Response