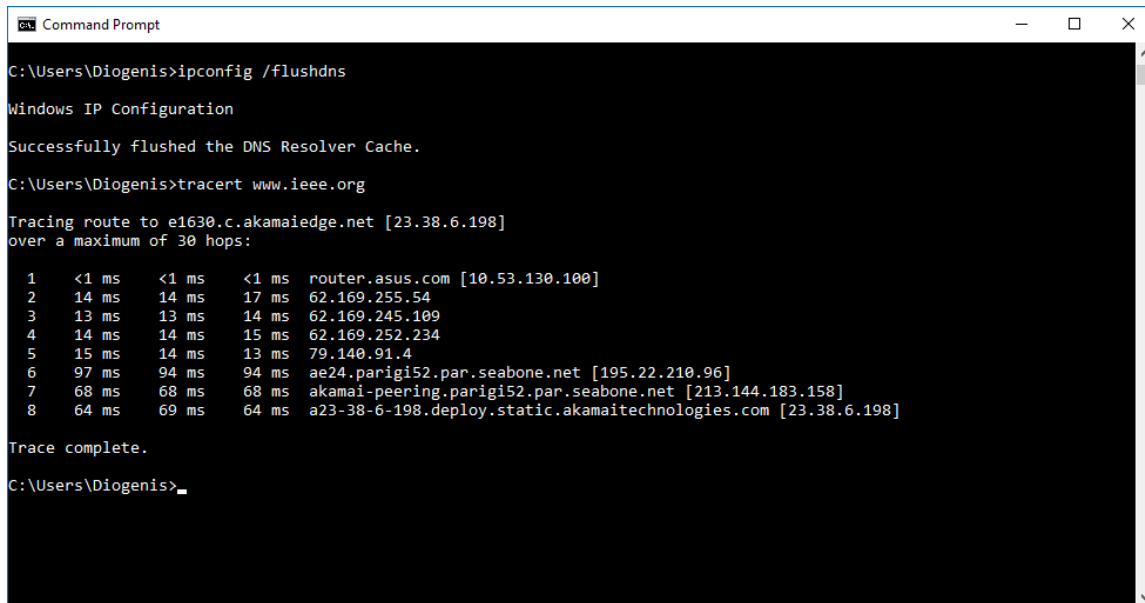


ΕΡΓΑΣΙΑ ΣΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Διογένη Τσολάκου 3170164

Α' ΜΕΡΟΣ

CMD Screenshot :



```
C:\Users\Diogenis>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Diogenis>tracert www.ietf.org

Tracing route to e1630.c.akamaiedge.net [23.38.6.198]
over a maximum of 30 hops:

  0  <1 ms  <1 ms  <1 ms  router.asus.com [10.53.130.100]
  1  14 ms  14 ms  17 ms  62.169.255.54
  2  13 ms  13 ms  14 ms  62.169.245.109
  3  14 ms  14 ms  15 ms  62.169.252.234
  4  15 ms  14 ms  13 ms  79.140.91.4
  5  97 ms  94 ms  94 ms  ae24.parigi52.par.seabone.net [195.22.210.96]
  6  68 ms  68 ms  68 ms  akamai-peering.parigi52.par.seabone.net [213.144.183.158]
  7  64 ms  69 ms  64 ms  a23-38-6-198.deploy.static.akamaitechnologies.com [23.38.6.198]

Trace complete.

C:\Users\Diogenis>
```

1) Διάρκεια : 13.941756 δευτερόλεπτα

No.	Time	Source	Destination	Protocol	Length	Info
1	13.941756	10.53.130.100	10.53.130.109	DNS	147	Standard query response 0xa998 PTR 198.6.38.23.in-addr.arpa PTR a23-38-6-198.deploy.static.akamaitechnologies.com

2)

Επίπεδο Δικτύου : UDP, ICMP, ARP, IP

Επίπεδο Εφαρμογής : DNS

3) Τα πρωτόκολλα του επιπέδου εφαρμογής χρησιμοποιούν το πρωτόκολλο UDP.

4) Στάλθηκαν μηδέν πακέτα TCP και 61 πακέτα UDP. 18 από αυτά είναι DNS που χρησιμοποιούν UDP.

5) Τα endpoints στα οποία υπάρχει επικοινωνία Ethernet είναι δύο και είναι τα :

Wireshark - Endpoints: Ethernet

Ethernet II		IPv4		TCP		UDP		30	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
40:16:7e:62:77:38	111	13 k	77	10 k	34				1548
d0:50:99:61:44:7b	111	13 k	34	3366	77				10 k

☐ Name resolution
 ☐ Limit to display filter

Copy Filter Close Help

Endpoint Types

Windows Taskbar: Type here to search, 9:43 PM, 25-Dec-19

Το D0:50:99:61:44:7b είναι ο προσωπικός μου υπολογιστής ενώ το 40:16:7e:62:77:38 είναι το router μου.

Ethernet II, Src: AsrockIn_61:44:7b (d0:50:99:61:44:7b), Dst: AsustekC_62:77:38 (40:16:7e:62:77:38)
 > Destination: AsustekC_62:77:38 (40:16:7e:62:77:38)
 > Source: AsrockIn_61:44:7b (d0:50:99:61:44:7b)
 Type: IPv4 (0x0800)

6) Τα endpoints στα οποία υπάρχει επικοινωνία IP είναι 28 και είναι τα :

Wireshark - Endpoints - Ethernet

Ethernet II IPv4 TCP UDP 30

Address	Packets	Bytes	To Packets	To Bytes	From Packets	From Bytes	Country	City	AS Number	AS Organization
10.53.130.100	21	2197	12	1437	9	760	---	---	---	---
10.53.130.109	109	114	33	3304	76	1034	---	---	---	---
23.38.6.198	27	2862	3	318	24	2544	---	---	---	---
31.217.27.38	1	145	1	145	0	0	---	---	---	---
62.169.252.109	3	210	3	210	0	0	---	---	---	---
62.169.252.234	3	330	3	330	0	0	---	---	---	---
62.169.252.54	3	330	3	330	0	0	---	---	---	---
75.140.91.4	3	210	3	210	0	0	---	---	---	---
79.157.103.159	1	175	1	175	0	0	---	---	---	---
79.167.78.39	1	166	1	166	0	0	---	---	---	---
83.25.183.43	2	292	2	292	0	0	---	---	---	---
84.125.164.91	2	292	2	292	0	0	---	---	---	---
85.90.75.6	4	320	4	320	0	0	---	---	---	---
87.202.191.151	1	62	1	62	0	0	---	---	---	---
88.22.35.84	1	80	1	80	0	0	---	---	---	---
90.70.195.115	4	1040	4	1040	0	0	---	---	---	---
90.191.151.38	3	750	3	750	0	0	---	---	---	---
95.43.113.136	2	292	2	292	0	0	---	---	---	---
102.194.25.149	2	132	2	132	0	0	---	---	---	---
109.186.0.244	3	186	3	186	0	0	---	---	---	---
163.53.36.238	1	62	1	62	0	0	---	---	---	---
177.79.123.101	1	221	1	221	0	0	---	---	---	---
178.19.247.148	2	292	2	292	0	0	---	---	---	---
185.192.16.16	4	776	4	776	0	0	---	---	---	---
186.81.22.105	4	584	4	584	0	0	---	---	---	---
195.22.210.96	3	210	3	210	0	0	---	---	---	---
213.144.183.158	3	210	3	210	0	0	---	---	---	---
217.126.28.77	4	896	4	896	0	0	---	---	---	---

☐ Name resolution ☐ Limit to display filter

Endpoint Types

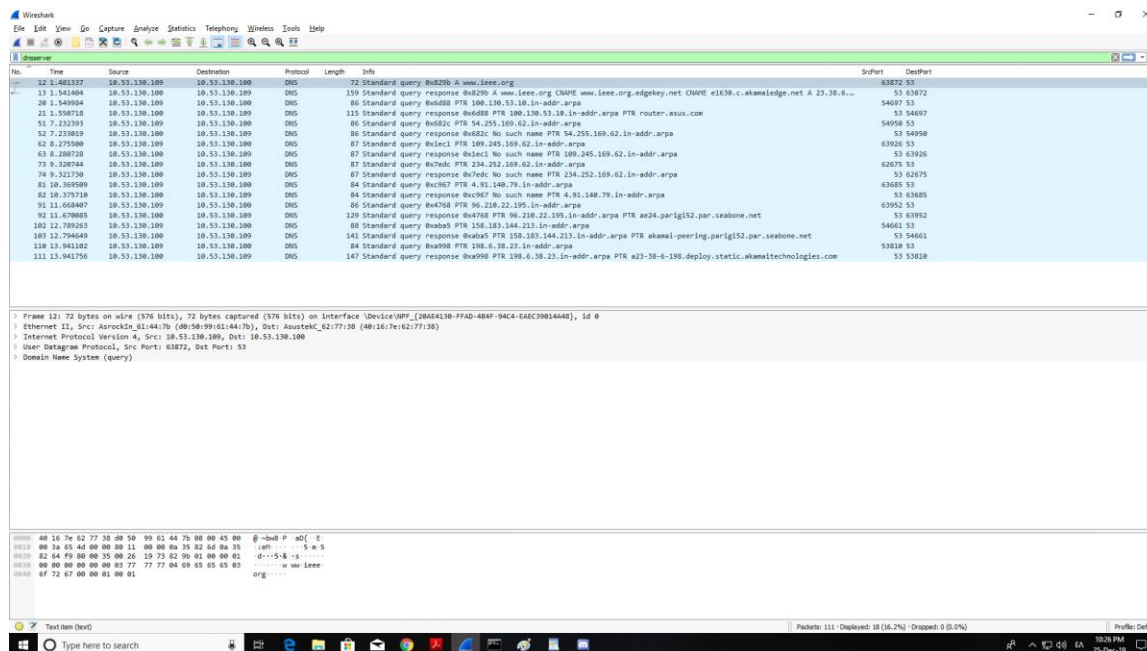
Copy Filter Close Help

Type here to search

9:58 PM 20-Dec-19

Δύο από αυτά ταυτίζονται με τα ethernet endpoints και συγκεκριμένα τα δύο πρώτα (10.53.130.100 και 10.53.130.109) οι οποίες είναι οι IP του router και PC αντίστοιχα. Τα υπόλοιπα endpoints δεν ταυτίζονται καθώς αποτελούν IPs εξωτερικών δικτύων από τα οποία περνάει ένα πακέτο στη διαδρομή του από τον υπολογιστή μου μέχρι να φτάσει στη σελίδα www.ieee.org.

7) Οι θύρες προέλευσης και προορισμού που χρησιμοποιήθηκαν από και προς τον DNS server είναι οι παρακάτω :



8) Διακρίνουμε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα από τα βελάκια που υπάρχουν αριστερά του αύξοντα αριθμού. Το δεξί βέλος υποδεικνύει request ενώ το αριστερό υποδεικνύει response. Όταν τα δύο βέλη είναι συνδεδεμένα με κάθετη συνεχόμενη γραμμή σημαίνει ότι το πακέτο της ερώτησης συνδέεται με το πακέτο της απάντησης. Π.χ. :

No.	Time	Source	Destination
12	1.481337	10.53.130.109	10.53.130.100
13	1.541404	10.53.130.100	10.53.130.109

9) Ναι, υπάρχει flag που να προσδιορίζει αν ο name server είναι authoritative. Αυτή βρίσκεται στο μεσαίο panel στο Domain Name System. Όπως φαίνεται ο server είναι authoritative για το συγκεκριμένο domain.

```

Domain Name System (response)
Transaction ID: 0x6d88
Flags: 0x8580 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... .1.. .. = Authoritative: Server is 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 by the server
.... ....0 .... = Non-authenticated data: Unacceptable
.... ....0000 = Reply code: No error (0)

```

10) Το όνομα www.ieee.org είναι domain name. Το canonical name του το βλέπουμε παρακάτω.

```

-----
Answers
  www.ieee.org: type CNAME, class IN, cname www.ieee.org.edgekey.net
    Name: www.ieee.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 345 (5 minutes, 45 seconds)
    Data length: 26
    CNAME: www.ieee.org.edgekey.net

```

11) Η IP που αντιστοιχεί στο www.ieee.org είναι 23.38.6.198 όπως μπορούμε να δούμε και στο tracert στο CMD αλλά και στο Wireshark.

```

Type: IN (Host Address) (1)
Class: IN (0x0001)
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.edgekey.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 345 (5 minutes, 45 seconds)
    Data length: 26
    CNAME: www.ietf.org.edgekey.net
  www.ietf.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net
    Name: www.ietf.org.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 20898 (5 hours, 48 minutes, 18 seconds)
    Data length: 21
    CNAME: e1630.c.akamaiedge.net
  e1630.c.akamaiedge.net: type A, class IN, addr 23.38.6.198
    Name: e1630.c.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 19 (19 seconds)
    Data length: 4
    Address: 23.38.6.198

```

Η IP που αντιστοιχεί στον υπολογιστή μου είναι 10.53.130.109. Αυτό το καταλαβαίνουμε επειδή το πρώτο request έχει ως source αυτή την IP αλλά και όπως έχει αναφερθεί στην ερώτηση 6.

No.	Time	Source	Destination	Protocol
12	1.481337	10.53.130.109	10.53.130.100	DNS

12) Θα γράψουμε ICMP στο filter specification tab.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
15	1.547714	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (T
16	1.548244	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
17	1.548445	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (T
18	1.548869	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
19	1.549066	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (T
45	7.182009	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
46	7.196335	62.169.255.54	10.53.130.109	ICMP	110	Time-to-live exceeded (T
47	7.197824	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
48	7.211906	62.169.255.54	10.53.130.109	ICMP	110	Time-to-live exceeded (T
49	7.213350	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
50	7.230453	62.169.255.54	10.53.130.109	ICMP	110	Time-to-live exceeded (T
55	8.231222	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
57	8.245100	62.169.245.109	10.53.130.109	ICMP	70	Time-to-live exceeded (T
58	8.245662	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
59	8.259597	62.169.245.109	10.53.130.109	ICMP	70	Time-to-live exceeded (T
60	8.260182	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
61	8.274273	62.169.245.109	10.53.130.109	ICMP	70	Time-to-live exceeded (T
67	9.272333	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
68	9.287143	62.169.252.234	10.53.130.109	ICMP	110	Time-to-live exceeded (T
69	9.288269	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=
70	9.302684	62.169.252.234	10.53.130.109	ICMP	110	Time-to-live exceeded (T

13)

α) Η διεύθυνση IP είναι 23.38.6.198

No.	Time	Source	Destination	Protocol	Length	Info
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=913/37123, ttl=1 (no response found!)
> Frame 14: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20AE4130-FFAD-4B4F-94C4-EAEC39014A48}, id 0 > Ethernet II, Src: AsrockIn_61:44:7b (d8:50:99:61:44:7b), Dst: AsustekC_62:77:38 (40:16:7e:62:77:38) > Internet Protocol Version 4, Src: 10.53.130.109, Dst: 23.38.6.198 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 92 Identification: 0x1a0f (6671) > Flags: 0x0000 ...0 0000 0000 0000 = Fragment offset: 0 > Time to live: 1 Protocol: ICMP (1) Header checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source: 10.53.130.109 Destination: 23.38.6.198						

β) Το TTL του πακέτου είναι 1.

No.	Time	Source	Destination	Protocol	Length	Info
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=913/37123, ttl=1 (no response found!)
> Frame 14: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20AE4130-FFAD-4B4F-94C4-EAEC39014A48}, id 0 > Ethernet II, Src: AsrockIn_61:44:7b (d8:50:99:61:44:7b), Dst: AsustekC_62:77:38 (40:16:7e:62:77:38) > Internet Protocol Version 4, Src: 10.53.130.109, Dst: 23.38.6.198 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 92 Identification: 0x1a0f (6671) > Flags: 0x0000 ...0 0000 0000 0000 = Fragment offset: 0 > Time to live: 1						

γ) Το μέγεθος των δεδομένων που μεταφέρει είναι 92.

No.	Time	Source	Destination	Protocol	Length	Info
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=913/37123, ttl=1 (no response found!)
> Frame 14: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20AE4130-FFAD-4B4F-94C4-EAEC39014A48}, id 0 > Ethernet II, Src: AsrockIn_61:44:7b (d0:50:99:61:44:7b), Dst: AsustekC_62:77:38 (40:16:7e:62:77:38) > Internet Protocol Version 4, Src: 10.53.130.109, Dst: 23.38.6.198 > 0100 = Version: 4 > 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) > Total Length: 92 > Identification: 0x1a0f (6671) > Flags: 0x0000 > ...0 0000 0000 0000 = Fragment offset: 0 > Time to live: 1 > Protocol: ICMP (1) > Header checksum: 0x0000 [validation disabled] > [Header checksum status: Unverified] > Source: 10.53.130.109 > Destination: 23.38.6.198						

14)

α) Η IP του destination είναι 10.53.130.109, ενώ η IP του source είναι 10.53.130.100

No.	Time	Source	Destination	Protocol	Length	Info	SrcPort	DestPort
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=913/37123, ttl=1 (no response found!)		
15	1.547714	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		

15) Οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα είναι οι : 10.53.130.100, 62.169.255.54, 62.169.255.109, 62.169.255.234, 79.140.91.4, 195.22.210.96, 213.144.183.158 . Υπάρχει αντιστοιχία με όλες τις διευθύνσεις που εμφανίζονται στο CMD κατά την εκτέλεση της tracert εκτός από την τελική IP του www.ieee.org, την 23.38.6.198

exercise.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

icmp

No.	Time	Source	Destination	Protocol	Length	Info	SrcPort	DestPort
14	1.547477	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=913/37123, ttl=1 (no response found!)		
15	1.547714	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
16	1.548214	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=914/37129, ttl=1 (no response found!)		
17	1.548455	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
18	1.548809	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=915/37135, ttl=1 (no response found!)		
19	1.549099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
20	1.549399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=916/37141, ttl=1 (no response found!)		
21	1.549699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
22	1.549999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=917/37147, ttl=1 (no response found!)		
23	1.550299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
24	1.550599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=918/37153, ttl=1 (no response found!)		
25	1.550899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
26	1.551199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=919/37159, ttl=1 (no response found!)		
27	1.551499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
28	1.551799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=920/37165, ttl=1 (no response found!)		
29	1.552099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
30	1.552399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=921/37171, ttl=1 (no response found!)		
31	1.552699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
32	1.552999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=922/37177, ttl=1 (no response found!)		
33	1.553299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
34	1.553599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=923/37183, ttl=1 (no response found!)		
35	1.553899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
36	1.554199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=924/37189, ttl=1 (no response found!)		
37	1.554499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
38	1.554799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=925/37195, ttl=1 (no response found!)		
39	1.555099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
40	1.555399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=926/37201, ttl=1 (no response found!)		
41	1.555699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
42	1.555999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=927/37207, ttl=1 (no response found!)		
43	1.556299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
44	1.556599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=928/37213, ttl=1 (no response found!)		
45	1.556899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
46	1.557199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=929/37219, ttl=1 (no response found!)		
47	1.557499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
48	1.557799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=930/37225, ttl=1 (no response found!)		
49	1.558099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
50	1.558399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=931/37231, ttl=1 (no response found!)		
51	1.558699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
52	1.558999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=932/37237, ttl=1 (no response found!)		
53	1.559299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
54	1.559599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=933/37243, ttl=1 (no response found!)		
55	1.559899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
56	1.560199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=934/37249, ttl=1 (no response found!)		
57	1.560499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
58	1.560799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=935/37255, ttl=1 (no response found!)		
59	1.561099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
60	1.561399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=936/37261, ttl=1 (no response found!)		
61	1.561699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
62	1.561999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=937/37267, ttl=1 (no response found!)		
63	1.562299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
64	1.562599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=938/37273, ttl=1 (no response found!)		
65	1.562899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
66	1.563199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=939/37279, ttl=1 (no response found!)		
67	1.563499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
68	1.563799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=940/37285, ttl=1 (no response found!)		
69	1.564099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
70	1.564399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=941/37291, ttl=1 (no response found!)		
71	1.564699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
72	1.564999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=942/37297, ttl=1 (no response found!)		
73	1.565299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
74	1.565599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=943/37303, ttl=1 (no response found!)		
75	1.565899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
76	1.566199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=944/37309, ttl=1 (no response found!)		
77	1.566499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
78	1.566799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=945/37315, ttl=1 (no response found!)		
79	1.567099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
80	1.567399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=946/37321, ttl=1 (no response found!)		
81	1.567699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
82	1.567999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=947/37327, ttl=1 (no response found!)		
83	1.568299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
84	1.568599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=948/37333, ttl=1 (no response found!)		
85	1.568899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
86	1.569199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=949/37339, ttl=1 (no response found!)		
87	1.569499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
88	1.569799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=950/37345, ttl=1 (no response found!)		
89	1.570099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
90	1.570399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=951/37351, ttl=1 (no response found!)		
91	1.570699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
92	1.570999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=952/37357, ttl=1 (no response found!)		
93	1.571299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
94	1.571599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=953/37363, ttl=1 (no response found!)		
95	1.571899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
96	1.572199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=954/37369, ttl=1 (no response found!)		
97	1.572499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
98	1.572799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=955/37375, ttl=1 (no response found!)		
99	1.573099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
100	1.573399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=956/37381, ttl=1 (no response found!)		
101	1.573699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
102	1.573999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=957/37387, ttl=1 (no response found!)		
103	1.574299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
104	1.574599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=958/37393, ttl=1 (no response found!)		
105	1.574899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
106	1.575199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=959/37399, ttl=1 (no response found!)		
107	1.575499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
108	1.575799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=960/37405, ttl=1 (no response found!)		
109	1.576099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
110	1.576399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=961/37411, ttl=1 (no response found!)		
111	1.576699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
112	1.576999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=962/37417, ttl=1 (no response found!)		
113	1.577299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
114	1.577599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=963/37423, ttl=1 (no response found!)		
115	1.577899	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
116	1.578199	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=964/37429, ttl=1 (no response found!)		
117	1.578499	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
118	1.578799	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=965/37435, ttl=1 (no response found!)		
119	1.579099	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
120	1.579399	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=966/37441, ttl=1 (no response found!)		
121	1.579699	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
122	1.579999	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=967/37447, ttl=1 (no response found!)		
123	1.580299	10.53.130.100	10.53.130.109	ICMP	134	Time-to-live exceeded (time to live exceeded in transit)		
124	1.580599	10.53.130.109	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=968/37453, ttl=1 (no response found!)		
125	1.580899	10.53.130.100	10.53.130					

```
Command Prompt

C:\Users\Diogenis>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Diogenis>tracert www.ietf.org

Tracing route to e1630.c.akamaiedge.net [23.38.6.198]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  router.asus.com [10.53.130.100]
  2  14 ms  14 ms  17 ms  62.169.255.54
  3  13 ms  13 ms  14 ms  62.169.245.109
  4  14 ms  14 ms  15 ms  62.169.252.234
  5  15 ms  14 ms  13 ms  79.140.91.4
  6  97 ms  94 ms  94 ms  ae24.parigi52.par.seabone.net [195.22.210.96]
  7  68 ms  68 ms  68 ms  akamai-peering.parigi52.par.seabone.net [213.144.183.158]
  8  64 ms  69 ms  64 ms  a23-38-6-198.deploy.static.akamaitechnologies.com [23.38.6.198]

Trace complete.

C:\Users\Diogenis>_
```

B' ΜΕΡΟΣ

1) Η IP διεύθυνση που αντιστοιχεί στο www.ekt.gr είναι 194.177.214.44

```
28 3.554303 10.53.130.109 194.177.214.44 HTTP 536 GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?2yx7v HTTP/1.1 62768 80

Source: 10.53.130.109
Destination: 194.177.214.44
Transmission Control Protocol, Src Port: 62768, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Source Port: 62768
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 482]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 3066923616
[Next sequence number: 483 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 2881789515
0101 ... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x277d [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (482 bytes)
> Hypertext Transfer Protocol
> GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?2yx7v HTTP/1.1\r\n
Host: www.ekt.gr\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36\r\n
Accept: */*\r\n
Referer: http://www.ekt.gr/\r\n
Accept-encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,el;q=0.7\r\n
Cookie: _ga=G41.2.1703163466.1577468828; _gid=G41.2.997758616.1577468828; _gat=1\r\n
\r\n
[Full request URI: http://www.ekt.gr/sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?2yx7v]
[HTTP request 1/1]
[Response in frame: 67]
```

2) Τα πακέτα που μας απασχολούν για την χειραψία τριών βημάτων είναι τα 20, 24, 26. Ο υπολογιστής μου στέλνει ένα μήνυμα συγχρονισμού στο σύστημα (SYN) με αριθμό sequence μηδέν. Το σύστημα απαντάει με ένα μήνυμα συγχρονισμού και αναγνώρισης (SYN-ACK) με αριθμό sequence μηδέν και αριθμό αναγνώρισης (Ack) 1, δηλαδή κατά ένα μεγαλύτερο από τον αριθμό sequence. Τέλος, ο υπολογιστής μου στέλνει μήνυμα αναγνώρισης με αριθμό sequence 1 και αριθμό αναγνώρισης 1.

tcp && p.addr == 194.177.214.44									
No.	Time	Source	Destination	Protocol	Length	Info	SrcPort	DestPort	
20	3.535705	10.53.130.109	194.177.214.44	TCP	66	62768 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		62768 80	
21	3.535887	10.53.130.109	194.177.214.44	TCP	66	62769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		62769 80	
24	3.535758	194.177.214.44	10.53.130.109	TCP	62	80 → 62768 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1	80	62768	
25	3.553759	194.177.214.44	10.53.130.109	TCP	62	80 → 62769 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1	80	62769	
26	3.553871	10.53.130.109	194.177.214.44	TCP	54	62768 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0		62768 80	
27	3.553894	10.53.130.109	194.177.214.44	TCP	54	62769 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0		62769 80	

3) Οι θύρες προέλευσης που χρησιμοποίησε το πρωτόκολλο HTTP είναι οι : 62768, 62769, 80. Οι ίδιες χρησιμοποιήθηκαν από το πρωτόκολλο ως θύρες προορισμού.

http									
No.	Time	Source	Destination	Protocol	Length	Info	SrcPort	DestPort	
28	3.554303	10.53.130.109	194.177.214.44	HTTP	536	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?q2yx7v HTTP/1.1		62768 80	
29	3.554437	10.53.130.109	194.177.214.44	HTTP	514	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v HTTP/1.1		62769 80	
67	3.671679	194.177.214.44	10.53.130.109	HTTP	759	HTTP/1.1 404 Not Found (text/html)	80	62768	
70	3.684944	194.177.214.44	10.53.130.109	HTTP	751	HTTP/1.1 404 Not Found (text/html)	80	62769	
204	5.680814	10.53.130.109	194.177.214.44	HTTP	532	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v HTTP/1.1		62769 80	
206	5.718725	194.177.214.44	10.53.130.109	HTTP	750	HTTP/1.1 404 Not Found (text/html)	80	62769	
207	5.729439	10.53.130.109	194.177.214.44	HTTP	554	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?q2yx7v HTTP/1.1		62769 80	
211	5.856404	194.177.214.44	10.53.130.109	HTTP	60	HTTP/1.1 404 Not Found (text/html)	80	62769	
228	6.894187	10.53.130.109	194.177.214.44	HTTP	546	GET /sites/ekt-site/themes/ekt/images/ekt.ico HTTP/1.1		62769 80	
238	6.922696	194.177.214.44	10.53.130.109	HTTP	393	HTTP/1.1 200 OK (image/x-icon)	80	62769	

4) Ο browser έστειλε πέντε πακέτα που περιείχαν αίτημα HTTP GET και στάλθηκαν προς την IP διεύθυνση της ιστοσελίδας : 194.177.214.44

http									
No.	Time	Source	Destination	Protocol	Length	Info	SrcPort	DestPort	
28	3.554303	10.53.130.109	194.177.214.44	HTTP	536	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?q2yx7v HTTP/1.1		62768 80	
29	3.554437	10.53.130.109	194.177.214.44	HTTP	514	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v HTTP/1.1		62769 80	
67	3.671679	194.177.214.44	10.53.130.109	HTTP	759	HTTP/1.1 404 Not Found (text/html)	80	62768	
70	3.684944	194.177.214.44	10.53.130.109	HTTP	751	HTTP/1.1 404 Not Found (text/html)	80	62769	
204	5.680814	10.53.130.109	194.177.214.44	HTTP	532	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v HTTP/1.1		62769 80	
206	5.718725	194.177.214.44	10.53.130.109	HTTP	750	HTTP/1.1 404 Not Found (text/html)	80	62769	
207	5.729439	10.53.130.109	194.177.214.44	HTTP	554	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?q2yx7v HTTP/1.1		62769 80	
211	5.856404	194.177.214.44	10.53.130.109	HTTP	60	HTTP/1.1 404 Not Found (text/html)	80	62769	
228	6.894187	10.53.130.109	194.177.214.44	HTTP	546	GET /sites/ekt-site/themes/ekt/images/ekt.ico HTTP/1.1		62769 80	
238	6.922696	194.177.214.44	10.53.130.109	HTTP	393	HTTP/1.1 200 OK (image/x-icon)	80	62769	

5) Ο browser τρέχει την έκδοση 1.1 του HTTP.

228	6.894187	10.53.130.109	194.177.214.44	HTTP	546	GET /sites/ekt-site/themes/ekt/images/ekt.ico HTTP/1.1	62769	80
238	6.922696	194.177.214.44	10.53.130.109	HTTP	393	HTTP/1.1 200 OK (image/x-icon)	80	62769

```

> Frame 228: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{20A84130-FFAD-4B4F-94CA-EAEC39014A48}, id 0
> Ethernet II, Src: AsrockIn_61:44:7b (d8:5b:99:61:44:7b), Dst: AsustekC_62:77:38 (40:16:7e:62:77:38)
> Internet Protocol Version 4, Src: 10.53.130.109, Dst: 194.177.214.44
> Transmission Control Protocol, Src Port: 62769, Dst Port: 80, Seq: 1439, Ack: 2098, Len: 492
> Hypertext Transfer Protocol
  GET /sites/ekt-site/themes/ekt/images/ekt.ico HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /sites/ekt-site/themes/ekt/images/ekt.ico HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /sites/ekt-site/themes/ekt/images/ekt.ico
    Request Version: HTTP/1.1
    Host: www.ekt.gr\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36\r\n
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://www.ekt.gr/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,el;q=0.7\r\n
    Cookie: _ga=G41.2.1703163466.1577468828; _gid=G41.2.997758616.1577468828; _gat=1; has_js=1\r\n
    dnt: 1\r\n
    \r\n
    [Full request URI: http://www.ekt.gr/sites/ekt-site/themes/ekt/images/ekt.ico]
    [HTTP request 4/4]
    [Prev request in frame: 207]
    [Response in frame: 238]

```

Ο server τρέχει την έκδοση 1.1 του HTTP.

