

Σταθόπουλος Γεώργιος p3170152

## Α ΜΕΡΟΣ

Η εκτέλεση των εντολών ipconfig /flushdns και tracert [www.ieee.org](http://www.ieee.org)

```
Γραμμή εντολών
C:\Users\user>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\user>tracert www.ieee.org

Tracing route to e1630.c.akamaiedge.net [92.122.26.20]
over a maximum of 30 hops:

  1  7 ms  1 ms  1 ms  vodafone.station [192.168.2.1]
  2  16 ms 16 ms 17 ms  loopback2004.med01.dsl.hol.gr [62.38.0.170]
  3  15 ms 16 ms 15 ms  62.38.97.150
  4  15 ms 16 ms 15 ms  62.38.93.221
  5 294 ms 28 ms 18 ms  ae3-100-ucr.ata.cw.net [195.89.103.69]
  6  52 ms 61 ms 59 ms  ae4-ucr1.atm.cw.net [195.2.2.70]
  7  81 ms 71 ms 76 ms  195.2.21.57
  8  44 ms 48 ms 58 ms  195.2.27.174
  9  51 ms 50 ms 1111 ms ae2-xcr1.muc.cw.net [195.2.8.221]
 10  55 ms 53 ms 63 ms  inxs-muc.netarch.akamai.com [194.59.190.59]
 11  50 ms 51 ms 50 ms  a92-122-26-20.deploy.static.akamaitechnologies.com [92.122.26.20]

Trace complete.

C:\Users\user>
```

1) Η χρονική διάρκεια της ανίχνευσης ήταν 48.127532 δευτερόλεπτα.

No.	Time	Source	Destination	Protocol	Length	Info
269	42.977477	192.168.2.7	92.122.26.20	ICMP	106	Echo (ping) r...
270	43.027459	92.122.26.20	192.168.2.7	ICMP	106	Echo (ping) r...
271	43.028719	192.168.2.7	92.122.26.20	ICMP	106	Echo (ping) r...
272	43.039481	192.168.2.7	157.240.9.18	TLSv1.2	86	Application D...
273	43.065807	157.240.9.18	192.168.2.7	TCP	60	443 → 59767 [...]
274	43.079462	92.122.26.20	192.168.2.7	ICMP	106	Echo (ping) r...
275	43.081143	192.168.2.7	92.122.26.20	ICMP	106	Echo (ping) r...
276	43.130910	92.122.26.20	192.168.2.7	ICMP	106	Echo (ping) r...
277	43.136917	192.168.2.7	192.168.2.1	DNS	85	Standard quer...
278	43.202834	157.240.9.18	192.168.2.7	TLSv1.2	82	Application D...
279	43.202835	192.168.2.1	192.168.2.7	DNS	524	Standard quer...
280	43.211852	DwnetTec_41:e9:78	Broadcast	ARP	42	Who has 192.1...
281	43.255241	192.168.2.7	157.240.9.18	TCP	54	59767 → 443 [...]
282	43.541967	DwnetTec_41:e9:78	LiteonTe_76:08:14	ARP	42	Who has 192.1...
283	43.542018	LiteonTe_76:08:14	DwnetTec_41:e9:78	ARP	42	192.168.2.7 i...
284	45.259971	DwnetTec_41:e9:78	Broadcast	ARP	42	Who has 192.1...
285	46.283948	DwnetTec_41:e9:78	Broadcast	ARP	42	Who has 192.1...
286	47.103070	DwnetTec_41:e9:78	Broadcast	ARP	42	Who has 192.1...
287	48.127532	DwnetTec_41:e9:78	Broadcast	ARP	42	Who has 192.1...

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

> Ethernet II, Src: DwnetTec\_41:e9:78 (78:b2:13:41:e9:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

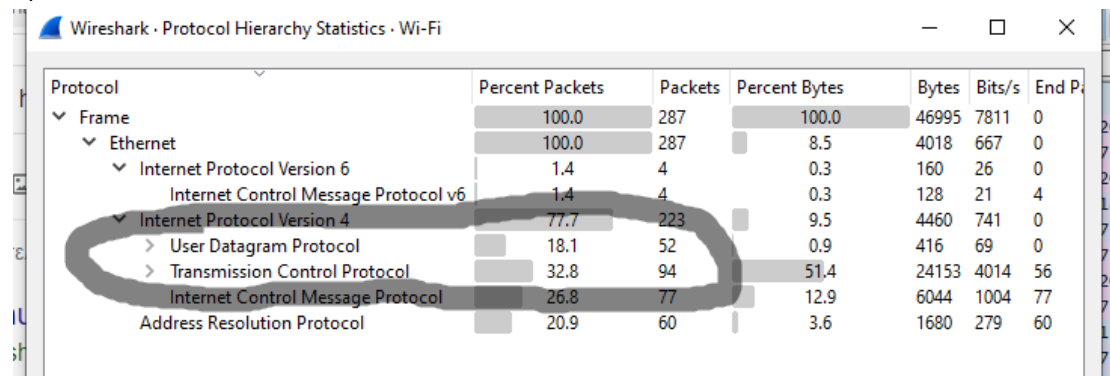
> Address Resolution Protocol (request)

2)

Επίπεδο	Πρωτόκολλο
Εφαρμογών	HTTP, DNS, NBNS, TLSv1.2
Μεταφοράς	TCP, UDP
Δικτύου	ARP, ICMP, ICMPv6, SSDP

3) Τα πρωτόκολλα DNS και NBNS χρησιμοποιούν το πρωτόκολλο UDP ενώ τα TCP και TLSv1.2 το TCP.

4)



Παρατηρούμε ότι στάλθηκαν συνολικά 52 UDP και 94 TCP πακέτα.

5)

Wireshark · Endpoints · Wi-Fi

Ethernet · 6		IPv4 · 22		IPv6 · 2		TCP · 11		UDP · 25	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
30:10:b3:76:08:14	237	44 k	119	16 k	118				
74:2f:68:e8:53:ca	8	1208	6	1036	2				
78:b2:13:41:e9:78	271	44 k	154	27 k	117				
88:83:22:ab:c7:aa	3	206	3	206	0				
ac:b5:7d:65:1a:89	5	1080	5	1080	0				
ff:ff:ff:ff:ff:ff	50	2180	0	0	50				

Τα διαφορετικά endpoints είναι 6 (αυτά που εμφανίζονται στην παραπάνω φωτογραφία).

6)

Wireshark · Endpoints · Wi-Fi

Endpoints											
Ethernet · 6   IPv4 · 22   IPv6 · 2   TCP · 11   UDP · 25											
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
40.112.91.29	35	12 k	16	7342	19	5007	—	—	—	—	
52.164.221.179	26	10 k	10	6520	16	3659	—	—	—	—	
62.38.0.170	3	330	3	330	0	0	—	—	—	—	
62.38.93.221	9	936	6	660	3	276	—	—	—	—	
62.38.97.150	8	1042	5	766	3	276	—	—	—	—	
77.234.45.63	8	2798	4	1990	4	808	—	—	—	—	
92.122.26.20	36	3816	3	318	33	3498	—	—	—	—	
108.177.127.188	2	121	1	66	1	55	—	—	—	—	
157.240.9.18	23	1974	12	962	11	1012	—	—	—	—	
192.168.2.1	32	5238	17	3992	15	1246	—	—	—	—	
192.168.2.4	5	1080	5	1080	0	0	—	—	—	—	
192.168.2.5	4	864	4	864	0	0	—	—	—	—	
192.168.2.7	212	42 k	111	16 k	101	25 k	—	—	—	—	
192.168.2.9	2	164	2	164	0	0	—	—	—	—	
194.59.190.59	3	210	3	210	0	0	—	—	—	—	
195.2.2.70	3	546	3	546	0	0	—	—	—	—	
195.2.8.221	3	210	3	210	0	0	—	—	—	—	
195.2.21.57	9	1032	6	756	3	276	—	—	—	—	
195.2.27.174	9	1032	6	756	3	276	—	—	—	—	
195.89.103.69	3	210	3	210	0	0	—	—	—	—	
239.255.255.250	9	1944	0	0	9	1944	—	—	—	—	
255.255.255.255	2	164	0	0	2	164	—	—	—	—	

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

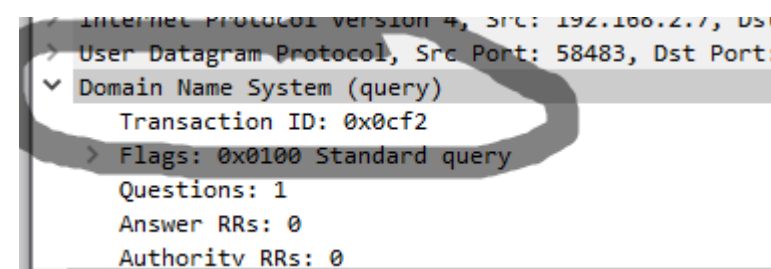
Wireshark · Endpoints · Wi-Fi

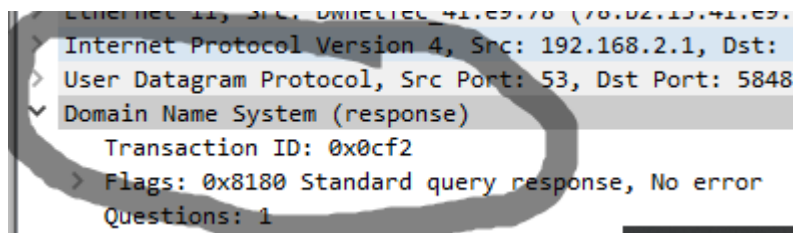
Endpoints											
Ethernet · 6   IPv4 · 22   IPv6 · 2   TCP · 11   UDP · 25											
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
fe80::d1c:9306:7522:3884	4	344	2	172	2	172	—	—	—	—	
fe80::5d83:87f:bd10:a0f4	4	344	2	172	2	172	—	—	—	—	

Έχουμε 22 IPv4 endpoints(1<sup>η</sup> φωτογραφία) και 2 IPv6(2<sup>η</sup>). Τα endpoints αυτά δεν ταυτίζονται με τα αντίστοιχα στο επίπεδο Ethernet. Αυτό συμβαίνει διότι τα endpoints κάθε επιπέδου χρησιμοποιούνται για επικοινωνία αποκλειστικά σε αυτό το επίπεδο. Επομένως δεν πρέπει να υπάρχει σύγχυση μεταξύ των ονομάτων.

7) Σε κάθε frame χρησιμοποιείται η θύρα 53 ως source ή destination port και κάποια άλλη τυχαία θύρα (π.χ. 61953,53064,...).

8)





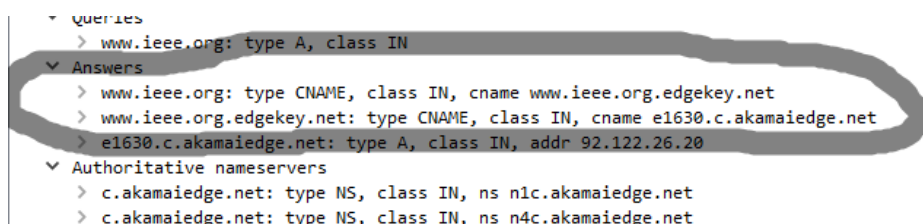
Ανάλογα με το τι υπάρχει στην παρένθεση δίπλα από το Domain Name System μπορούμε να καταλάβουμε αν πρόκειται για αίτημα προς τον DNS server (query) ή για απάντηση (response). Το πακέτο της απάντησης συνδέεται με το πακέτο της ερώτησης από το transaction ID. Η ερώτηση με την απάντηση έχουν το ίδιο ID ενώ κάποιο άλλο ζεύγος θα έχει διαφορετικό ID.

9)

```
Transaction ID: 0x0cf2
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
.... ..1 .... = Recursion desired: Do query recursively
.... ..1... .. = Recursion available: Server can do recursive queries
.... ..0.. .... = Z: reserved (0)
```

Η παραπάνω σημαία μας το προσδιορίζει. Στη συγκεκριμένη περίπτωση δεν είναι authoritative.

10)



Πρόκειται για canonical name.

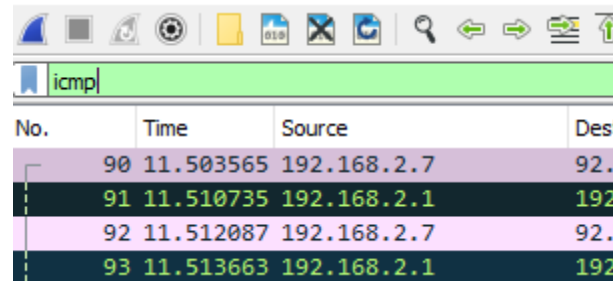
11)

108	12.583115	192.168.2.7	192.168.2.1	DNS
109	12.605368	192.168.2.1	192.168.2.7	DNS

Στην παραπάνω εικόνα βλέπουμε ένα ζεύγος ερώτησης/απάντησης προς/από τον DNS server. Στην ερώτηση η source address είναι η 192.168.2.7 ενώ η destination address η 192.168.2.1. Στην απάντηση οι διευθύνσεις είναι αντίστροφα. Από αυτό συμπεραίνουμε ότι

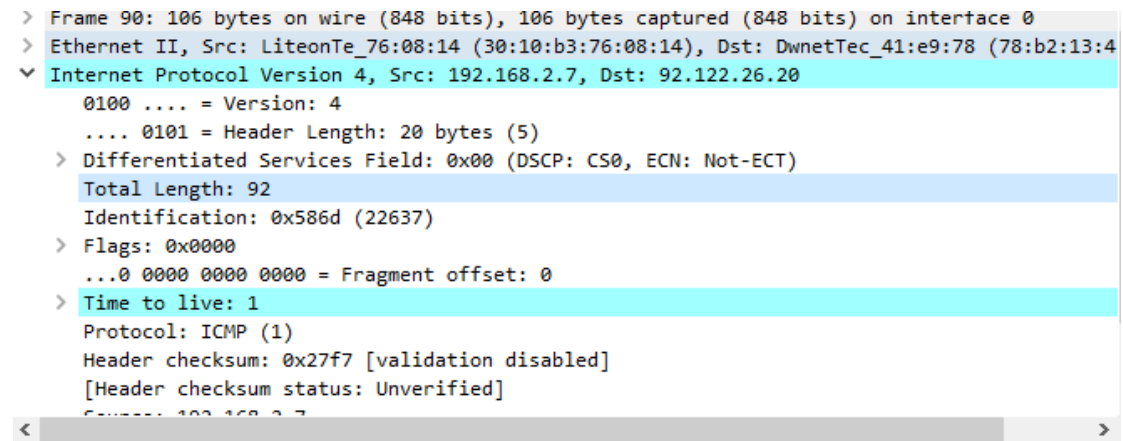
η IP διεύθυνση που αντιστοιχεί στον [www.ietf.org](http://www.ietf.org) είναι η 192.168.2.1 ενώ η άλλη είναι η δικιά μας.

12) Πληκτρολογώντας ICMP στο πεδίο φιλτραρίσματος.

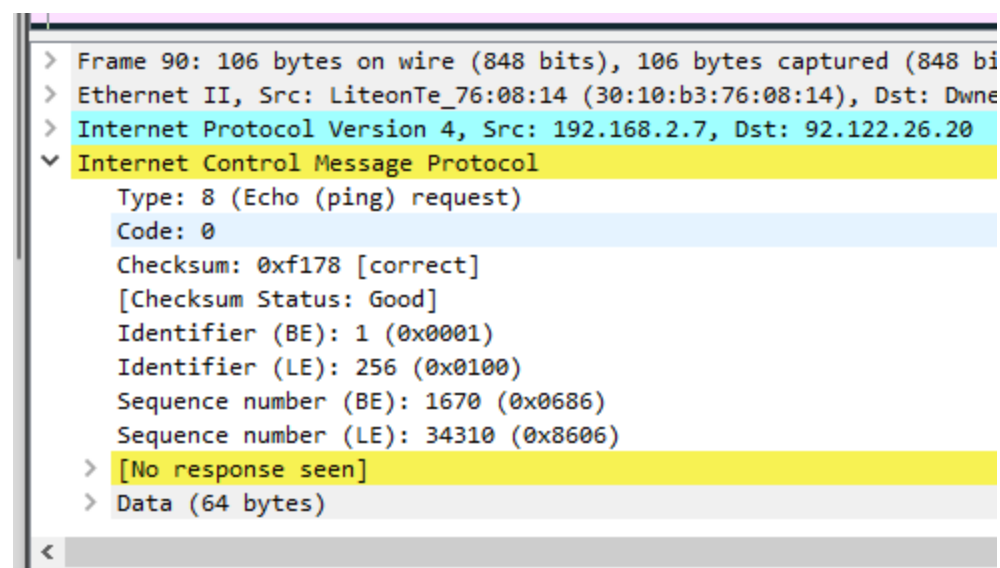


No.	Time	Source	Destination
90	11.503565	192.168.2.7	92.122.26.20
91	11.510735	192.168.2.1	92.122.26.20
92	11.512087	192.168.2.7	92.122.26.20
93	11.513663	192.168.2.1	92.122.26.20

13)



```
> Frame 90: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: LiteonTe_76:08:14 (30:10:b3:76:08:14), Dst: DwnetTec_41:e9:78 (78:b2:13:4
▼ Internet Protocol Version 4, Src: 192.168.2.7, Dst: 92.122.26.20
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 92
        Identification: 0x586d (22637)
    > Flags: 0x0000
        ...0 0000 0000 0000 = Fragment offset: 0
    > Time to live: 1
        Protocol: ICMP (1)
        Header checksum: 0x27f7 [validation disabled]
        [Header checksum status: Unverified]
        Source: 192.168.2.7
```



```
> Frame 90: 106 bytes on wire (848 bits), 106 bytes captured (848 bi
> Ethernet II, Src: LiteonTe_76:08:14 (30:10:b3:76:08:14), Dst: Dwnet
> Internet Protocol Version 4, Src: 192.168.2.7, Dst: 92.122.26.20
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf178 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1670 (0x0686)
    Sequence number (LE): 34310 (0x8606)
    > [No response seen]
    > Data (64 bytes)
```

a) Η destination IP είναι η 92.122.26.20.

b) Το time-to-live του πακέτου είναι 1.

c) Το συνολικό μέγεθος είναι 92 bytes. Το μέγεθος της κεφαλίδας είναι 20 bytes. Άρα το μέγεθος των δεδομένων είναι 72 bytes.

14)

```
> Frame 91: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
> Ethernet II, Src: DwnetTec_41:e9:78 (78:b2:13:41:e9:78), Dst: LiteonTe_76:08:14 (30:10:b:
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.7
  ✓ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ✓ Internet Protocol Version 4, Src: 192.168.2.7, Dst: 92.122.26.20
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ✓ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
```

Η destination IP είναι 192.168.2.7 ενώ η source address 192.168.2.1

15) Οι διευθύνσεις είναι οι ακόλουθες:

192.168.2.1

62.38.0.170

62.38.97.150

62.38.93.221

195.89.103.69

195.2.2.70

195.2.21.57

195.2.27.174

195.2.8.221

194.59.190.59

```

Tracing route to e1630.c.akamaiedge.net [92.122.26.20]
over a maximum of 30 hops:

  1    7 ms    1 ms    1 ms    vodafone.station [192.168.2.1]
  2   16 ms   16 ms   17 ms   loopback2004.med01.dsl.hol.gr [62.38.0.170]
  3   15 ms   16 ms   15 ms   62.38.97.150
  4   15 ms   16 ms   15 ms   62.38.93.221
  5  294 ms   28 ms   18 ms   ae3-100-ucr.ata.cw.net [195.89.103.69]
  6   52 ms   61 ms   59 ms   ae4-ucr1.atm.cw.net [195.2.2.70]
  7   81 ms   71 ms   76 ms   195.2.21.57
  8   44 ms   48 ms   58 ms   195.2.27.174
  9   51 ms   50 ms  1111 ms  ae2-xcr1.muc.cw.net [195.2.8.221]
 10   55 ms   53 ms   63 ms   inxs-muc.netarch.akamai.com [194.59.190.59]
 11   50 ms   51 ms   50 ms   a92-122-26-20.deploy.static.akamaitechnologies.com [92.122.26.20]

```

Παρατηρούμε ότι όλες οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα υπάρχουν στο cmd. Επίσης παρατηρούμε ότι η τελευταία διεύθυνση που εμφανίζεται στο cmd (92.122.26.20) δεν υπάρχει ως source IP διεύθυνση πακέτου που μεταφέρει ICMP Time Exceeded μήνυμα.

## B ΜΕΡΟΣ

1)

```

> Frame 644: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0
> Ethernet II, Src: LiteonTe_76:08:14 (30:10:b3:76:08:14), Dst: DwnetTec_41:e9:78 (78:b2:13:41)
> Internet Protocol Version 4, Src: 192.168.2.7, Dst: 194.177.214.44
> Transmission Control Protocol, Src Port: 62108, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
  Hypertext Transfer Protocol
    > GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v 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)
      Accept: */*\r\n
      Referer: http://www.ekt.gr/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: el-GR,el;q=0.9\r\n
      \r\n
      [Full request URI: http://www.ekt.gr/sites/ekt-site/libraries/tablesorter/jquery.metadata.js?q2yx7v]
      [HTTP request 1/1]

```

Στη φωτογραφία βλέπουμε ένα πακέτο που περιλαμβάνει HTTP GET αίτημα. Host είναι ο [www.ekt.gr](http://www.ekt.gr). Αυτό στέλνεται από τον υπολογιστή μας στην διεύθυνση του ekt, άρα η IP διεύθυνση που αντιστοιχεί στον [www.ekt.gr](http://www.ekt.gr) είναι η 194.177.214.44 (dest).

2)

TIME	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
456	6.884385	192.168.2.7	194.177.214.44	TCP	66	62108 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
457	6.885124	192.168.2.7	194.177.214.44	TCP	66	62109 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
458	6.901210	194.177.214.44	192.168.2.7	TCP	62	80 → 62108 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1416 SACK_PERM=1
459	6.901211	194.177.214.44	192.168.2.7	TCP	62	80 → 62109 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1416 SACK_PERM=1
460	6.901911	192.168.2.7	194.177.214.44	TCP	54	62108 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
461	6.902129	192.168.2.7	194.177.214.44	TCP	54	62109 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Στο πρώτο βήμα ο υπολογιστής μας θέλει να ξεκινήσει μία σύνδεση με το σύστημα που φιλοξενεί το [www.ekt.gr](http://www.ekt.gr). Για τον λόγο αυτό στέλνει ένα τμήμα με SYN το οποίο ενημερώνει τον server ότι επιθυμούμε να ξεκινήσουμε επικοινωνία μαζί του καθώς επίσης και με ποιον αριθμό σειράς θα ξεκινάμε τα τμήματα.

Στο δεύτερο βήμα ο server μας απαντάει με ένα SYN-ACK σήμα. Το ACK δηλώνει ότι έλαβε το αντίστοιχο τμήμα ενώ το SYN δηλώνει με ποιον αριθμό σειράς θα ξεκινάνε τα τμήματα.

Τέλος, στο 3<sup>ο</sup> βήμα ο πελάτης γνωρίζει την απάντηση του server και εγκαθιδρύουν μία σύνδεση πάνω από την οποία θα σταλούν τα δεδομένα.

3) Χρησιμοποιούνται οι θύρες: 80 (παγκόσμιος ιστός,http) καθώς επίσης και οι 62108,62109,62110.

4)

No.	Time	Source	Destination	Protocol	Length	Info
480	7.199051	192.168.2.7	138.197.59.141	HTTP	392	GET /api/adcheck?url...
494	7.355944	138.197.59.141	192.168.2.7	HTTP	264	HTTP/1.1 200 OK (te...
644	9.128202	192.168.2.7	194.177.214.44	HTTP	411	GET /sites/ekt-site/...
645	9.137348	192.168.2.7	194.177.214.44	HTTP	433	GET /sites/ekt-site/...
651	9.263196	194.177.214.44	192.168.2.7	HTTP	756	HTTP/1.1 404 Not Fou...
652	9.276840	194.177.214.44	192.168.2.7	HTTP	759	HTTP/1.1 404 Not Fou...
940	12.432289	192.168.2.7	194.177.214.44	HTTP	429	GET /sites/ekt-site/...
953	12.564543	194.177.214.44	192.168.2.7	HTTP	60	HTTP/1.1 404 Not Fou...
955	12.594231	192.168.2.7	194.177.214.44	HTTP	451	GET /sites/ekt-site/...
958	12.724709	194.177.214.44	192.168.2.7	HTTP	60	HTTP/1.1 404 Not Fou...

Έστειλε 5 πακέτα. Οι IP διευθύνσεις προς τις οποίες στάλθηκαν είναι: 138.197.59.141 και 194.177.214.44.

5).

```
> Internet Protocol Version 4, Src: 192.168.2.7, Dst: 194.177.214.44
> Transmission Control Protocol, Src Port: 60591, Dst Port: 80
  > Hypertext Transfer Protocol
    > GET / HTTP/1.1\r\n
      Host: www.ekt.gr\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
      Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
  > [13 Reassembled TCP Segments (16057 bytes): #446(1416)]
  > Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Fri, 03 Jan 2020 14:48:40 GMT\r\n
      Server: Apache/2.4.6 (CentOS)\r\n
      Content-Type: text/html; charset=utf-8\r\n
```

Browser και server τρέχουν την έκδοση 1.1.