

# ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ



ΤΖΕΝΗ ΜΠΟΛΕΝΑ 3170117

## Α' ΜΕΡΟΣ

### Γενικές ερωτήσεις:

1. Η ανίχνευση είχε διάρκεια 35.536277 sec.

2.

Layer 2(network)	Layer 3(transport)	Layer 4(application)
ARP	TCP	DNS
ICMP	UDP	NBNS
		LLMNR
		SSDP
		TLSv1.2

Protocol

▼ Frame

▼ Ethernet

▼ Internet Protocol Version 6

▼ User Datagram Protocol

Link-local Multicast Name Resolution

▼ Internet Protocol Version 4

▼ User Datagram Protocol

Simple Service Discovery Protocol

NetBIOS Name Service

Link-local Multicast Name Resolution

Domain Name System

▼ Transmission Control Protocol

Transport Layer Security

Data

Internet Control Message Protocol

Address Resolution Protocol

3. Τα πρωτόκολλα DNS, NBNS, LLMNR, SSDP χρησιμοποιούν UDP.

Το πρωτόκολλο TLSv1.2 χρησιμοποιεί TCP.

4. Στάλθηκαν 56 UDP packets και 96 TCP packets.

Για IPv4

User Datagram Protocol	<div></div> 23.2	54	0.5
Transmission Control Protocol	<div></div> 41.2	96	75.2

Για IPv6

Internet Protocol Version 6	0.9	2
User Datagram Protocol	0.9	2
Link-local Multicast Name Resolution	0.9	2

5. Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο ethernet είναι τα εξής 7:

- 01:00:5e:00:00:fc
- 01:00:5e:7f:ff:fa
- 30:45:96:8e:fe:10
- 33:33:00:01:00:03
- 40:9f:38:fc:71:bb
- 58:d9:d5:16:f3:40
- ff:ff:ff:ff:ff:ff

Το ethernet endpoint είναι πανομοιότυπο με αυτό του ethernet's mac address.  
Αντιστοιχούν στις συσκευές που επικοινωνεί ο server.

6. Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι τα εξής 23(21 IPv4 και 2 IPv6):

- fe80:10b5:66d2:6192:711b
- ff02::1:3
- 5.56.18.138
- 10.10.17.1
- 13.107.18.11
- 40.90.22.190
- 52.114.132.73
- 52.232.216.86
- 81.95.2.185
- 104.121.152.91
- 130.117.15.162
- 142.250.13.188
- 149.14.98.9
- 154.54.59.189
- 154.54.59.233
- 172.217.23.131
- 185.89.159.17
- 192.168.0.157
- 192.168.0.157
- 204.79.197.200
- 212.73.202.130
- 224.0.0.252
- 239.255.250

Τα endpoints αυτά δεν ταυτίζονται με τα endpoints σε επίπεδο ethernet αφού του ethernet αναφέρονται σε MAC ενώ αυτά σε IP.

Ethernet · 7

IPv4 · 21

IPv6 · 2

### Ερωτήσεις σχετικά με το DNS:

7.

Οι θύρες(ports) που χρησιμοποιήθηκαν για ερώτηση από τον υπολογιστή μου προς τον DNS server είναι οι εξής:

Source port	Destination port
53680	53
60499	
55873	
55557	
53726	
54820	
61845	
62323	
64642	
58881	
52615	
52025	

Οι θύρες(ports) που χρησιμοποιήθηκαν για την απάντηση του DNS server είναι οι εξής:

Source port	Destination port
53	53680
	60499
	55873
	55557
	53726
	54820
	61845
	62323
	64642
	58881
	52615
	52025

Είναι εμφανές ότι ο DNS server χρησιμοποιεί μόνο την UDP port 53.

## 8.

Αν ένα πακέτο περιέχει απάντηση σε ερώτημα το κατανοούμε διότι το destination είναι η IP διεύθυνση μας, το src port είναι 53 και επίσης αναγράφεται Standard query response.

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.157
User Datagram Protocol, Src Port: 53, Dst Port: 60449
Domain Name System (response)
```

Αν το πακέτο περιέχει αίτημα προς τον DNS server τότε γίνεται κατανοητό επειδή το src είναι η IP διεύθυνση μας, το dst port είναι 53 και αναγράφεται απλώς Standard query.

```
Internet Protocol Version 4, Src: 192.168.0.157, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 60449, Dst Port: 53
Domain Name System (query)
```

Το πακέτο ερώτησης με το πακέτο απάντησης συνδέονται μέσω του src port στην ερώτηση και dst port στην απάντηση, όπως βλέπουμε και στις παραπάνω δύο εικόνες.

## 9. Υπάρχει flag

Flags: 0x8183 Standard query response, No such name

και μας λέει ότι ο server που μας έχει απαντήσει δεν είναι authoritative για το συγκεκριμένο domain.

Authoritative: Server is not an authority for domain

10. Το [www.ieee.org](http://www.ieee.org) είναι canonical name, το domain name είναι το ieee.org.

11. Η IP διεύθυνση που αντιστοιχεί στον [www.ieee.org](http://www.ieee.org) είναι: 104.121.152.91

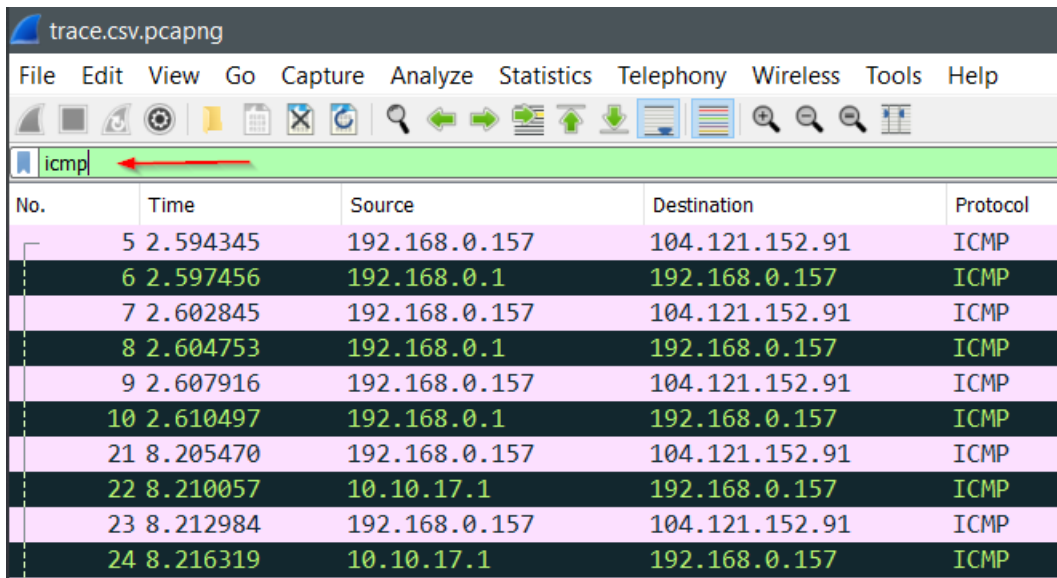
```
C:\Users\JennyB>tracert www.ieee.org

Tracing route to e1630.c.akamaiedge.net [104.121.152.91]
over a maximum of 30 hops:
```

Η IP διεύθυνση που αντιστοιχεί στον υπολογιστή μου είναι: 192.168.0.157

### Ερωτήσεις σχετικά με το ICMP:

**12.** Στο filter γράφουμε icmp για να δούμε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP



The screenshot shows the Wireshark interface with a packet capture filter 'icmp' applied. The packet list shows 12 packets, all of which are ICMP. The first packet (No. 5) is an Echo (ping) request from 192.168.0.157 to 104.121.152.91. The subsequent packets (Nos. 6-12) are Echo replies from 104.121.152.91 to 192.168.0.157. The packet details pane shows the selected packet (No. 5) with its structure: Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) request.

No.	Time	Source	Destination	Protocol
5	2.594345	192.168.0.157	104.121.152.91	ICMP
6	2.597456	192.168.0.1	192.168.0.157	ICMP
7	2.602845	192.168.0.157	104.121.152.91	ICMP
8	2.604753	192.168.0.1	192.168.0.157	ICMP
9	2.607916	192.168.0.157	104.121.152.91	ICMP
10	2.610497	192.168.0.1	192.168.0.157	ICMP
21	8.205470	192.168.0.157	104.121.152.91	ICMP
22	8.210057	10.10.17.1	192.168.0.157	ICMP
23	8.212984	192.168.0.157	104.121.152.91	ICMP
24	8.216319	10.10.17.1	192.168.0.157	ICMP

**13.**

**a.** IP διεύθυνση του destination είναι: 104.121.152.91

Internet Protocol Version 4, Src: 192.168.0.157, Dst: 104.121.152.91

**b.** Το time-to-live του πακέτου είναι: 1

Time to live: 1

**c.** Total length: 92bytes(20 για το IP header και 8 για ICMP header και 64 για data)

Data length: 64 bytes

Internet Protocol Version 4, Src: 192.168.0.157, Dst: 104.121.152.91

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 92  
Identification: 0xdca8 (56488)  
> Flags: 0x0000  
...0 0000 0000 0000 = Fragment offset: 0  
> Time to live: 1  
Protocol: ICMP (1)  
Header checksum: 0x1adf [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.0.157  
Destination: 104.121.152.91

#### Internet Control Message Protocol

Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xf7a2 [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence number (BE): 92 (0x005c)  
Sequence number (LE): 23552 (0x5c00)  
> [No response seen]  
✓ Data (64 bytes)  
Data: 00...  
[Length: 64]

14.

a. IP διεύθυνση του source: 192.168.0.1

IP διεύθυνση του destination: 192.168.0.157

6 2.597456	192.168.0.1	192.168.0.157	ICMP	134 Time-to-live exceeded
------------	-------------	---------------	------	---------------------------

15. Οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα είναι οι εξής:

- 192.168.0.1
- 10.10.17.1
- 185.89.159.17
- 149.14.98.9
- 154.54.59.233
- 154.54.59.189
- 130.117.15.162
- 212.73.202.130
- 81.95.2.185
- 5.56.18.138

```
C:\Users\JennyB>tracert www.ietf.org

Tracing route to e1630.c.akamaiedge.net [104.121.152.91]
over a maximum of 30 hops:

  1    3 ms    2 ms    2 ms  192.168.0.1
  2    4 ms    3 ms    3 ms  10.10.17.1
  3   10 ms    9 ms   12 ms  185.89.159.17
  4    7 ms    8 ms    8 ms  be5298.rcr51.tia01.atlas.cogentco.com [149.14.98.9]
  5   18 ms   18 ms   19 ms  be2024.ccr51.beg03.atlas.cogentco.com [154.54.59.233]
  6   29 ms   30 ms   29 ms  be3464.ccr52.vie01.atlas.cogentco.com [154.54.59.189]
  7   29 ms   29 ms   28 ms  level3.vie01.atlas.cogentco.com [130.117.15.162]
  8   35 ms   31 ms   29 ms  212.73.202.130
  9   56 ms   46 ms   53 ms  ae4-2028.muc20.core-backbone.com [81.95.2.185]
 10  48 ms   50 ms   46 ms  core-backbone.akamai.com [5.56.18.138]
 11  40 ms   40 ms   40 ms  a104-121-152-91.deploy.static.akamaitechnologies.com [104.121.152.91]

Trace complete.
```

Παρατηρούμε ότι τα 10 πρώτα IP's στο cmd με τα την εκτέλεση της εντολής tracert είναι ίδια με αυτά που βρήκαμε και στο wireshark. Το τελευταίο IP source που βλέπουμε στο cmd αναφέρεται στο τελευταίο Echo reply.

145	32.074366	104.121.152.91	192.168.0.157	ICMP	106	Echo (ping) reply
-----	-----------	----------------	---------------	------	-----	-------------------

Αυτό που κάνει η εντολή tracert είναι να τυπώνει μια διατεταγμένη λίστα με τους ενδιάμεσους δρομολογητές που επιστρέφουν ICMP "time exceeded".



## Β' ΜΕΡΟΣ

1. Η IP διεύθυνση που αντιστοιχεί στον [www.ekt.gr](http://www.ekt.gr) είναι: 194.177.214.44

2. Με το 3-way-handshake υλοποιείται η εγκαθίδρυση της σύνδεσης. Υπάρχουν τρία βήματα:

- I. **(SYN)** Ο πελάτης(εμείς) θέλει να εγκαθίδρυση σύνδεση με τον server, του στέλνει ένα segment με SYN. Το SYN δηλώνει με ποιόν αριθμό ξεκινάει τα segments του. Με την αποστολή αυτή δηλώνει ότι είναι πολύ πιθανό να ξεκινήσει επικοινωνία με τον server.
- II. **(SYN, ACK)** ο server απαντάει στο αίτημα του πελάτη με ένα σετ από SYN-ACK signal bits. Το ACK(acknowledgement) δηλώνει την απάντηση στο segment που ο χρήστης έστειλε και το SYN δηλώνει τον αριθμό με τον οποίο ο server θα ξεκινάει τα segments του.
- III. **(ACK)** Ο πελάτης τώρα αναγνωρίζει το response από τον server και πλέον εγκαθιδρύεται μια secure/reliable σύνδεση μεταξύ τους για μεταφορά data.

tcp							
No.	Time	Time to live	Source	Destination	Protocol	Length	Info
3	0.021695	128	192.168.0.157	37.228.108.133	TCP	66	62070 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.151555	48	37.228.108.133	192.168.0.157	TCP	58	443 → 62070 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440
5	0.151645	128	192.168.0.157	37.228.108.133	TCP	54	62070 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

i. Παρατηρούμε ότι το sequence number που στέλνει ο πελάτης είναι Initialized, είναι το SYN που στέλνεται στον server. Επίσης αν πάμε στα flags θα δούμε ότι το SYN:set. Από αυτό γίνεται κατανοητό ότι είμαστε στο πρώτο Part του 3-way-hanshaking.

```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{8C2B4595-1BD3-4AED-BC14-C94D757D963E}, id 0
> Ethernet II, Src: Azurewav_fc:71:bb (40:9f:38:fc:71:bb), Dst: TendaTec_16:f3:40 (58:d9:d5:16:f3:40)
> Internet Protocol Version 4, Src: 192.168.0.157, Dst: 37.228.108.133
v Transmission Control Protocol, Src Port: 62070, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 62070
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 3001653511
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
v Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... ..... 0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....S.]
  Window size value: 64240
  [Calculated window size: 64240]
  Checksum: 0xe04d [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
> [Timestamps]
```

ii. Παρατηρούμε ότι το sequence number που στέλνει ο server είναι Initialized, είναι το SYN που στέλνεται στον πελάτη για να ξέρει με ποιόν αριθμό θα ξεκινάνε τα segments του ο server. Και το acknowledgement number έχει value και δηλώνει response προς το αίτημα του πελάτη. Επίσης αν πάμε στα flags θα δούμε ότι το SYN:set και το ACK: set. Από αυτό γίνεται κατανοητό ότι είμαστε στο δεύτερο part του 3-way-hanshaking.

```
> Frame 4: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{8C2B4595-1BD3-4AED-BC14-C94D757D963E}, id 0
> Ethernet II, Src: TendaTec_16:f3:40 (58:d9:d5:16:f3:40), Dst: Azurewav_fc:71:bb (40:9f:38:fc:71:bb)
> Internet Protocol Version 4, Src: 37.228.108.133, Dst: 192.168.0.157
v Transmission Control Protocol, Src Port: 443, Dst Port: 62070, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 62070
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 3001375723
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 3001653512
  0110 .... = Header Length: 24 bytes (6)
v Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
> .... .... .1. = Syn: Set
  .... .... ..0 = Fin: Not set
  [TCP Flags: .....A..S.]
  Window size value: 29200
  [Calculated window size: 29200]
  Checksum: 0x8376 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> Options: (4 bytes), Maximum segment size
> [SEQ/ACK analysis]
> [Timestamps]
```

iii. Παρατηρούμε ότι το sequence number είναι ίδιο με το αρχικό που έστειλε ο πελάτης(δλδ είναι αυτό με το οποίο αναγνωρίζεται ότι το segment είναι δικό του). Και το acknowledgement number έχει value και δηλώνει response του πελάτη στον server(δλδ είναι το ok για την εγκαθίδρυση της σύνδεσης). Επίσης αν πάμε στα flags θα δούμε ότι το ACK: set. Από αυτό γίνεται κατανοητό ότι είμαστε στο τρίτο και τελευταίο part του 3-way-hanshaking.

```
> Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8C2B4595-1BD3-4AED-BC14-C94D757D963E}, id 0
> Ethernet II, Src: Azurewav_fc:71:bb (40:9f:38:fc:71:bb), Dst: TendaTec_16:f3:40 (58:d9:d5:16:f3:40)
> Internet Protocol Version 4, Src: 192.168.0.157, Dst: 37.228.108.133
v Transmission Control Protocol, Src Port: 62070, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 62070
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 3001653512
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 3001375724
  0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... = Push: Not set
    .... ....0.. = Reset: Not set
    .... .... .0. = Syn: Not set
    .... .... ..0 = Fin: Not set
    [TCP Flags: .....A....]
  Window size value: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x123f [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

3.

Για GET

Source port	Destination port
62073	80
62072	

!GET

Source port	Destination port
80	62073
	62072

Παρατηρούμε ότι ο server χρησιμοποιεί το port 80, ενώ ο πελάτης(εμείς) τα ports 62073 και 62072. Στένουμε αίτημα μέσω των ports 62073, 62072 και λαμβάνουμε response μέσω αυτών. Ο server στέλνει response μέσω του port 80 και λαμβάνει request μέσω του ίδιου port. Το 80 είναι το default port για το HTTP protocol και χειρίζεται όλα τα request και responds(είναι η τοποθεσία που βρίσκονται οι HTTP servers).

4. Ο browser έστειλε τέσσερα HTTP GET request. Τα μηνύματα αυτά στάλθηκαν στην IP διεύθυνση του [www.ekt.gr](http://www.ekt.gr) που είναι: 194.177.214.44

No.	Time	Time to live	Source	Destination	Protocol	Length	Info
107	2.846851	128	192.168.0.157	194.177.214.44	HTTP	615	GET / HTTP/1.1
120	3.167490	128	192.168.0.157	194.177.214.44	HTTP	546	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter-pager.js?2yx7v HTTP/1.1
121	3.168039	128	192.168.0.157	194.177.214.44	HTTP	524	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?2yx7v HTTP/1.1
132	4.086226	128	192.168.0.157	194.177.214.44	HTTP	556	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter-pager.js?2yx7v HTTP/1.1

5.

Η έκδοση του HTTP που τρέχει ο browser μου είναι: HTTP/1.1

▼ Hypertext Transfer Protocol  
    > GET / HTTP/1.1\r\n

Η έκδοση του HTTP που τρέχει ο server είναι: HTTP/1.1

▼ Hypertext Transfer Protocol  
    > HTTP/1.1 200 OK\r\n