

## ΕΡΓΑΣΙΑ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

### Α' ΜΕΡΟΣ

#### Εισαγωγικά:

3) Αποτέλεσμα εντολής ipconfig /flushdns στο command prompt έτσι ώστε να καθαριστεί η προσωρινή μνήμη DNS του υπολογιστή και στη συνέχεια να χρειάζεται επικοινωνία με DNS Server.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.914]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\lydia>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\lydia>
```

5) Αποτέλεσμα εντολής tracert www.ieee.org στο command prompt

```
Command Prompt
Microsoft Windows [Version 10.0.17763.914]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\lydia>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

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

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

  0  3 ms   2 ms   1 ms  192.168.2.1 [192.168.2.1]
  1  24 ms  27 ms  25 ms  10.13.255.49 [10.13.255.49]
  2  24 ms  26 ms  23 ms  62.169.245.125
  3  24 ms  32 ms  23 ms  62.169.252.118
  4  24 ms   *    23 ms  10.13.255.141 [10.13.255.141]
  5  26 ms  25 ms  25 ms  62.169.252.117
  6  26 ms  26 ms  28 ms  62.169.252.230
  7  25 ms  26 ms  56 ms  79.140.91.14
  8  77 ms  77 ms  76 ms  ae24.parigi52.par.seabone.net [195.22.210.96]
  9  77 ms  76 ms  76 ms  akamai-peering.parigi52.par.seabone.net [213.144.183.158]
 10  86 ms  76 ms  78 ms  a23-38-6-198.deploy.static.akamaitechnologies.com [23.38.6.198]

Trace complete.

C:\Users\lydia>
```

#### Γενικές Ερωτήσεις:

1) Η χρονική διάρκεια της ανίχνευσής ήταν 67.244231 msec (time τελευταίου πακέτου).

- 2) Πίνακας με τα διαφορετικά πρωτόκολλα που χρησιμοποίησε ο υπολογιστής στη χρονική διάρκεια της ανίχνευσης, διαχωρισμένα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

| Πακέτο                           | Επίπεδο που ανήκει   |
|----------------------------------|----------------------|
| TCP                              | Transfer layer       |
| ICMP                             | Internet layer       |
| ARP                              | Network access layer |
| DNS                              | Application Layer    |
| HTTP                             |                      |
| Hypertext transfer protocol HTTP |                      |
| NBNS                             |                      |
| TLSv1.2                          |                      |

- 3) Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.
- Το πρωτόκολλο επιπέδου εφαρμογής DNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
  - Το πρωτόκολλο επιπέδου εφαρμογής HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: ICMP
  - Το πρωτόκολλο επιπέδου εφαρμογής Hypertext transfer protocol HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
  - Το πρωτόκολλο επιπέδου εφαρμογής NBNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
  - Το πρωτόκολλο επιπέδου εφαρμογής TLS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: TCP

Με βοήθησε να τα εντοπίσω το παράθυρο του wireshark: statistics>protocol Hierarchy statistics

Wireshark - Protocol Hierarchy Statistics - WiFi

| Protocol                          | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s |
|-----------------------------------|-----------------|---------|---------------|-------|--------|-------------|-----------|------------|
| ▼ Frame                           | 100.0           | 185     | 100.0         | 24267 | 2887   | 0           | 0         | 0          |
| ▼ Ethernet                        | 100.0           | 185     | 10.7          | 2590  | 308    | 0           | 0         | 0          |
| ▼ Internet Protocol Version 4     | 96.8            | 179     | 14.8          | 3580  | 425    | 0           | 0         | 0          |
| ▼ User Datagram Protocol          | 23.2            | 43      | 1.4           | 344   | 40     | 0           | 0         | 0          |
| NetBIOS Name Service              | 8.1             | 15      | 3.1           | 750   | 89     | 15          | 750       | 89         |
| Domain Name System                | 15.1            | 28      | 11.3          | 2741  | 326    | 28          | 2741      | 326        |
| ▼ Transmission Control Protocol   | 30.3            | 56      | 36.2          | 8778  | 1044   | 38          | 3846      | 457        |
| Transport Layer Security          | 8.6             | 16      | 19.0          | 4606  | 547    | 16          | 4606      | 547        |
| ▼ Hypertext Transfer Protocol     | 1.1             | 2       | 12.5          | 3024  | 359    | 1           | 290       | 34         |
| Data                              | 0.5             | 1       | 10.6          | 2562  | 304    | 1           | 2734      | 325        |
| Internet Control Message Protocol | 43.2            | 80      | 21.9          | 5316  | 632    | 80          | 5316      | 632        |
| Address Resolution Protocol       | 3.2             | 6       | 0.7           | 168   | 19     | 6           | 168       | 19         |

- 4) Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Εφαρμόζοντας στο wireshark τα κατάλληλα φίλτρα και βλέποντας κάτω δεξιά το display/packets βλέπουμε ότι τα UDP πακέτα που στάλθηκαν είναι 58 ενώ τα TCP πακέτα που στάλθηκαν είναι 56. Παρακάτω φαίνεται ένα παράδειγμα με το φίλτρο udp και το displayed εμφανίζει 58.



ethernet είναι φυσικές διευθύνσεις που συνδέονται με κάρτα ασύρματης διασύνδεσης, κάρτα διασύνδεσης ethernet ή ειδική διεύθυνση MAC για broadcast(η οποία προορίζεται να ληφθεί από όλους). Τα endpoints IP είναι λογικές διευθύνσεις, στο επίπεδο δικτύου, που χρησιμοποιούνται από συσκευές που έχουν διευθύνσεις IP σε κάθε τμήμα (επίσης αποκαλούμενες VLAN) του δικτύου. Θα χρησιμοποιήσετε τα στατιστικά στοιχεία του τελικού σημείου Ethernet αν θέλουμε να δούμε τι συμβαίνει στην κάρτα διασύνδεσης (κάρτα ethernet ή wifi) ή στους δρομολογητές που είναι ο επόμενος host σε εμάς ενώ το τελικό σημείο IP, εάν θέλουμε να δούμε όλα τα δεδομένα που αναφέρονται σε μια συγκεκριμένη διεύθυνση IP με την οποία επικοινωνούμε (οποιαδήποτε συσκευή στο τοπικό δίκτυο ή στο διαδίκτυο). Άρα πρόκειται για τελείως διαφορετικά πράγματα γι' αυτό τα endpoints τους δεν ταυτίζονται.

Wireshark · Endpoints · WiFi

Ethernet · 2IPv4 · 24IPv6TCP · 23UDP · 21

| Address        | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number | AS Organization |
|----------------|---------|-------|------------|----------|------------|----------|---------|------|-----------|-----------------|
| 5.45.58.39     | 8       | 436   | 4          | 216      | 4          | 220      | —       | —    | —         | —               |
| 10.13.255.49   | 3       | 330   | 3          | 330      | 0          | 0        | —       | —    | —         | —               |
| 10.13.255.141  | 2       | 140   | 2          | 140      | 0          | 0        | —       | —    | —         | —               |
| 13.107.18.254  | 1       | 54    | 1          | 54       | 0          | 0        | —       | —    | —         | —               |
| 13.107.42.254  | 1       | 54    | 1          | 54       | 0          | 0        | —       | —    | —         | —               |
| 13.107.246.254 | 1       | 54    | 1          | 54       | 0          | 0        | —       | —    | —         | —               |
| 23.38.6.198    | 36      | 3816  | 3          | 318      | 33         | 3498     | —       | —    | —         | —               |
| 40.69.223.198  | 22      | 5478  | 10         | 3588     | 12         | 1890     | —       | —    | —         | —               |
| 40.90.22.192   | 3       | 162   | 1          | 54       | 2          | 108      | —       | —    | —         | —               |
| 51.105.249.228 | 6       | 664   | 2          | 360      | 4          | 304      | —       | —    | —         | —               |
| 62.169.245.125 | 6       | 834   | 3          | 558      | 3          | 276      | —       | —    | —         | —               |
| 62.169.245.133 | 3       | 330   | 3          | 330      | 0          | 0        | —       | —    | —         | —               |
| 62.169.252.117 | 12      | 906   | 9          | 630      | 3          | 276      | —       | —    | —         | —               |
| 62.169.252.118 | 6       | 606   | 3          | 330      | 3          | 276      | —       | —    | —         | —               |
| 62.169.252.230 | 9       | 936   | 6          | 660      | 3          | 276      | —       | —    | —         | —               |
| 77.234.45.60   | 6       | 3348  | 4          | 2950     | 2          | 398      | —       | —    | —         | —               |
| 79.140.91.14   | 9       | 696   | 6          | 420      | 3          | 276      | —       | —    | —         | —               |
| 93.184.221.240 | 3       | 162   | 1          | 54       | 2          | 108      | —       | —    | —         | —               |
| 152.199.19.161 | 2       | 108   | 1          | 54       | 1          | 54       | —       | —    | —         | —               |

☐ Name resolution☐ Limit to display filter

Endpoint Types ▾

Copy ▾

Map ▾

Close

Help

#### Ερωτήσεις σχετικά με το DNS:

- 7) Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.

WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

| No. | Time      | Source      | Destination | Protocol |
|-----|-----------|-------------|-------------|----------|
| 1   | 0.000000  | 192.168.2.3 | 192.168.2.1 | DNS      |
| 2   | 0.003138  | 192.168.2.1 | 192.168.2.3 | DNS      |
| 14  | 24.056305 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 15  | 24.084951 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 22  | 24.110451 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 23  | 24.113667 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 30  | 25.215015 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 31  | 25.218151 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 38  | 26.289274 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 39  | 26.584097 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 44  | 28.192783 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 45  | 28.199250 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 82  | 32.172142 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 83  | 32.584452 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 95  | 41.647581 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 96  | 41.654773 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 103 | 42.734727 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 104 | 43.585233 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 119 | 49.161824 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 122 | 49.584580 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 144 | 55.191333 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 145 | 55.584627 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 162 | 61.270070 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 163 | 61.330405 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 170 | 62.504032 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 171 | 62.533796 | 192.168.2.1 | 192.168.2.3 | DNS      |
| 178 | 63.718982 | 192.168.2.3 | 192.168.2.1 | DNS      |
| 179 | 63.807028 | 192.168.2.1 | 192.168.2.3 | DNS      |

> Frame 2: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)

|      |                         |                         |                |
|------|-------------------------|-------------------------|----------------|
| 0000 | 48 5f 99 92 6d f5 34 4d | ea 87 50 24 08 00 45 00 | H_..m.4M..P\$. |
| 0010 | 00 5a 00 00 40 00 40 11 | b5 3e c0 a8 02 01 c0 a8 | -Z..@.@.->...  |

- 8) Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

Το πακέτο μια απάντησης με το πακέτο της ερώτησης συνδέονται με το transaction ID . Οι αιτήσεις έχουν το ίδιο Id Με τις αντίστοιχες απαντήσεις τους. (Όταν περνάς το ποντίκι πάνω στο αίτημα δείχνει ένα εξερχόμενο και ένα εισερχόμενο βελάκι στα αριστερά).

Wireshark capture of DNS traffic. The packet list shows a query and response for www.ieee.org. The packet details pane shows the response structure with flags set to 0x8180.

| No. | Time      | Source      | Destination | Protocol | Length | Info  |
|-----|-----------|-------------|-------------|----------|--------|---|
| 1   | 0.000000  | 192.168.2.3 | 192.168.2.1 | DNS      | 88     | Standard query 0x0dcb A fcmconnection.googleapis.com  |
| 2   | 0.003138  | 192.168.2.1 | 192.168.2.3 | DNS      | 104    | Standard query response 0x0dcb A fcmconnection.googleapis.com A 216.58.206.202  |
| 14  | 24.056305 | 192.168.2.3 | 192.168.2.1 | DNS      | 72     | Standard query 0x20f5 A www.ieee.org  |
| 15  | 24.084951 | 192.168.2.1 | 192.168.2.3 | DNS      | 459    | Standard query response 0x20f5 A www.ieee.org CNAME www.ieee.org.edgekey.net CNAME e1630.c.akamaiedge.net A 23.38.6.198 NS n2c... |
| 22  | 24.110451 | 192.168.2.3 | 192.168.2.1 | DNS      | 84     | Standard query 0xb506 PTR 1.2.168.192.in-addr.arpa  |
| 23  | 24.113667 | 192.168.2.1 | 192.168.2.3 | DNS      | 109    | Standard query response 0xb506 PTR 1.2.168.192.in-addr.arpa PTR 192.168.2.1   |
| 30  | 25.215015 | 192.168.2.3 | 192.168.2.1 | DNS      | 85     | Standard query 0x7e4d PTR 49.255.13.10.in-addr.arpa   |
| 31  | 25.218151 | 192.168.2.1 | 192.168.2.3 | DNS      | 111    | Standard query response 0x7e4d PTR 49.255.13.10.in-addr.arpa PTR 10.13.255.49   |
| 38  | 26.289274 | 192.168.2.3 | 192.168.2.1 | DNS      | 87     | Standard query 0x440e PTR 125.245.169.62.in-addr.arpa   |
| 39  | 26.584097 | 192.168.2.1 | 192.168.2.3 | DNS      | 147    | Standard query response 0x440e No such name PTR 125.245.169.62.in-addr.arpa SOA pri.authdns.ripe.net                              |
| 44  | 28.192783 | 192.168.2.3 | 192.168.2.1 | DNS      | 97     | Standard query 0x2ea9 A array610.prod.do.dsp.mp.microsoft.com   |
| 45  | 28.199250 | 192.168.2.1 | 192.168.2.3 | DNS      | 113    | Standard query response 0x2ea9 A array610.prod.do.dsp.mp.microsoft.com A 40.69.223.198  |
| 82  | 32.172142 | 192.168.2.3 | 192.168.2.1 | DNS      | 87     | Standard query 0xa5b3 PTR 118.252.169.62.in-addr.arpa   |
| 83  | 32.584452 | 192.168.2.1 | 192.168.2.3 | DNS      | 147    | Standard query response 0xa5b3 No such name PTR 118.252.169.62.in-addr.arpa SOA pri.authdns.ripe.net                              |

Source Port: 53  
Destination Port: 64094  
Length: 425  
Checksum: 0xe9c4 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 1]  
[Timestamps]  
[Time since first frame: 0.028646000 seconds]  
[Time since previous frame: 0.028646000 seconds]  
Domain Name System (response)  
Transaction ID: 0x20f5  
Flags: 0x8180 Standard query response. No error

- 9) Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει για το www.ieee.org είναι authoritative για το συγκεκριμένο domain; Είναι ο name server που μας έχει απαντήσει authoritative για το συγκεκριμένο domain;

Υπάρχει σημαία flag που προσδιορίζει αν ο name server είναι authoritative στο συγκεκριμένο domain και μάλιστα στο παράδειγμά μας ο server που μας έχει απαντήσει δεν είναι (server is not an authoritative for domain).

Wireshark interface showing DNS traffic. The packet list shows a series of DNS queries and responses. The selected packet (No. 15) is a Standard query response from 192.168.2.1 to 192.168.2.3, transaction ID 0x20f5. The packet details show the response flags and the answer section.

| No. | Time      | Source      | Destination | Protocol | Length | Info  |
|-----|-----------|-------------|-------------|----------|--------|---|
| 1   | 0.000000  | 192.168.2.3 | 192.168.2.1 | DNS      | 88     | Standard query 0x0dcb A fcmconnection.googleapis.com  |
| 2   | 0.003138  | 192.168.2.1 | 192.168.2.3 | DNS      | 104    | Standard query response 0x0dcb A fcmconnection.googleapis.com A 216.58.206.202  |
| 14  | 24.056305 | 192.168.2.3 | 192.168.2.1 | DNS      | 72     | Standard query 0x20f5 A www.ietf.org  |
| 15  | 24.084951 | 192.168.2.1 | 192.168.2.3 | DNS      | 459    | Standard query response 0x20f5 A www.ietf.org CNAME www.ietf.org.edgekey.net CNAME e1630.c.akamaiedge.net A 23.38.6.198 NS n2c... |
| 22  | 24.110451 | 192.168.2.3 | 192.168.2.1 | DNS      | 84     | Standard query 0xb506 PTR 1.2.168.192.in-addr.arpa  |
| 23  | 24.113667 | 192.168.2.1 | 192.168.2.3 | DNS      | 109    | Standard query response 0xb506 PTR 1.2.168.192.in-addr.arpa PTR 192.168.2.1   |
| 30  | 25.215015 | 192.168.2.3 | 192.168.2.1 | DNS      | 85     | Standard query 0x7e4d PTR 49.255.13.10.in-addr.arpa   |
| 31  | 25.218151 | 192.168.2.1 | 192.168.2.3 | DNS      | 111    | Standard query response 0x7e4d PTR 49.255.13.10.in-addr.arpa PTR 10.13.255.49   |
| 38  | 26.289274 | 192.168.2.3 | 192.168.2.1 | DNS      | 87     | Standard query 0x440e PTR 125.245.169.62.in-addr.arpa   |
| 39  | 26.584097 | 192.168.2.1 | 192.168.2.3 | DNS      | 147    | Standard query response 0x440e No such name PTR 125.245.169.62.in-addr.arpa SOA pri.authdns.ripe.net                              |
| 44  | 28.192783 | 192.168.2.3 | 192.168.2.1 | DNS      | 97     | Standard query 0x2ea9 A array610.prod.do.dsp.mp.microsoft.com   |
| 45  | 28.199250 | 192.168.2.1 | 192.168.2.3 | DNS      | 113    | Standard query response 0x2ea9 A array610.prod.do.dsp.mp.microsoft.com A 40.69.223.198  |
| 82  | 32.172142 | 192.168.2.3 | 192.168.2.1 | DNS      | 87     | Standard query 0xa5b3 PTR 118.252.169.62.in-addr.arpa   |
| 83  | 32.584452 | 192.168.2.1 | 192.168.2.3 | DNS      | 147    | Standard query response 0xa5b3 No such name PTR 118.252.169.62.in-addr.arpa SOA pri.authdns.ripe.net                              |

Transaction ID: 0x20f5

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)
- .... .... .0.. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
- .... .... ...0 .... = Non-authenticated data: Unacceptable
- .... .... .... 0000 = Reply code: No error (0)

Questions: 1  
Answer RRs: 3  
Authority RRs: 8  
Additional RRs: 0

10) Ένα domain name είναι η διεύθυνση όπου οι internet users μπορούν να έχουν πρόσβαση στον ιστότοπό μας. Ένα domain name χρησιμοποιείται για την εύρεση και αναγνώριση υπολογιστών στο Διαδίκτυο. Οι υπολογιστές χρησιμοποιούν διευθύνσεις IP, οι οποίες είναι μια σειρά αριθμών. Ωστόσο, είναι δύσκολο για τους ανθρώπους να θυμούνται τις σειρές αριθμών. Εξαιτίας αυτού, τα ονόματα τομέα αναπτύχθηκαν και χρησιμοποιήθηκαν για τον εντοπισμό οντοτήτων στο Διαδίκτυο αντί για τη χρήση διευθύνσεων IP.



Ένα canonical name είναι το σωστά δηλωμένο όνομα κεντρικού υπολογιστή ενός διακομιστή υπολογιστή ή δικτύου. Ένα CNAME καθορίζει ένα ψευδώνυμο για μια κανονική εγγραφή ονόματος κεντρικού υπολογιστή σε μια βάση δεδομένων του συστήματος ονομάτων τομέα (DNS). Κατά τον προγραμματισμό, ο όρος "canonical" σημαίνει "σύμφωνα με τους κανόνες". Το DNS είναι η τυπική μέθοδος καθορισμού των τοποθεσιών των τοποθεσιών στο Διαδίκτυο, ιδιαίτερα στις τοποθεσίες Web. Άρα το όνομα [www.ieee.org](http://www.ieee.org) είναι canonical name.

The image shows a Wireshark capture of a DNS transaction. The packet list pane displays several DNS packets. The selected packet is a Standard query response (ID: 0x20f5) from 192.168.2.1 to 192.168.2.3, containing the answer for the query. The packet details pane shows the Domain Name System (response) structure, including the transaction ID, flags, questions, answer RRs, and the specific answer for the query: www.ieee.org. The answer is a CNAME record pointing to www.ieee.org.edgekey.net, which in turn points to e1630.c.akamaiedge.net, an A record with IP address 23.38.6.198.

| No. | Time      | Source      | Destination | Protocol | Length | Info  |
|-----|-----------|-------------|-------------|----------|--------|---|
| 1   | 0.000000  | 192.168.2.3 | 192.168.2.1 | DNS      | 88     | Standard query 0x0dcb A fcmconnection.googleapis.com  |
| 2   | 0.003138  | 192.168.2.1 | 192.168.2.3 | DNS      | 104    | Standard query response 0x0dcb A fcmconnection.googleapis.com A 216.58.206.202  |
| 14  | 24.056305 | 192.168.2.3 | 192.168.2.1 | DNS      | 72     | Standard query 0x20f5 A www.ieee.org  |
| 15  | 24.084951 | 192.168.2.1 | 192.168.2.3 | DNS      | 459    | Standard query response 0x20f5 A www.ieee.org CNAME www.ieee.org.edgekey.net CNAME e1630.c.akamaiedge.net A 23.38.6.198 NS n2c... |

Domain Name System (response)  
Transaction ID: 0x20f5  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 3  
Authority RRs: 8  
Additional RRs: 9  
Queries  
Answers  
www.ieee.org: type CNAME, class IN, cname www.ieee.org.edgekey.net  
www.ieee.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net  
e1630.c.akamaiedge.net: type A, class IN, addr 23.38.6.198  
Authoritative nameservers  
Additional records

- 11) Ποια είναι η IP διεύθυνση που αντιστοιχεί στον [www.ieee.org](http://www.ieee.org); Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;  
Η IP διεύθυνση που αντιστοιχεί στον [www.ieee.org](http://www.ieee.org) είναι η 23.98.6.198  
Η IP διεύθυνση που αντιστοιχεί στον δικό μου υπολογιστή είναι η 192.168.2.3

This image shows the same Wireshark capture as above, but with the packet details pane expanded to show the full structure of the DNS response. The 'Answers' section is expanded, showing the CNAME record for www.ieee.org pointing to www.ieee.org.edgekey.net, which points to e1630.c.akamaiedge.net, an A record with IP address 23.38.6.198. The 'Additional records' section is also expanded, showing the SOA record for the domain.

| No. | Time      | Source      | Destination | Protocol | Length | Info  |
|-----|-----------|-------------|-------------|----------|--------|---|
| 1   | 0.000000  | 192.168.2.3 | 192.168.2.1 | DNS      | 88     | Standard query 0x0dcb A fcmconnection.googleapis.com  |
| 2   | 0.003138  | 192.168.2.1 | 192.168.2.3 | DNS      | 104    | Standard query response 0x0dcb A fcmconnection.googleapis.com A 216.58.206.202  |
| 14  | 24.056305 | 192.168.2.3 | 192.168.2.1 | DNS      | 72     | Standard query 0x20f5 A www.ieee.org  |
| 15  | 24.084951 | 192.168.2.1 | 192.168.2.3 | DNS      | 459    | Standard query response 0x20f5 A www.ieee.org CNAME www.ieee.org.edgekey.net CNAME e1630.c.akamaiedge.net A 23.38.6.198 NS n2c... |

CNAME: www.ieee.org.edgekey.net  
www.ieee.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net  
Name: www.ieee.org.edgekey.net  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 965 (16 minutes, 5 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  
Authoritative nameservers



```

Select Command Prompt

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : B0-0C-D1-F1-50-E6
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : CA-5F-99-92-6D-F5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Realtek RTL8821CE 802.11ac PCIe Adapter
    Physical Address. . . . . : 48-5F-99-92-6D-F5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::791d:fb54:2e16:9cd%7(Preferred)
    IPv4 Address. . . . . : 192.168.2.3(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 08 January 2020 12:51:24
    Lease Expires . . . . . : 10 January 2020 12:18:49
    Default Gateway . . . . . : 192.168.2.1
    DHCP Server . . . . . : 192.168.2.1
    DHCPv6 IAID . . . . . : 105406361
    DHCPv6 Client DUID. . . . . : 00-01-00-01-24-14-61-75-B0-0C-D1-F1-50-E6
    DNS Servers . . . . . : 192.168.2.1
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 48-5F-99-92-6D-F6
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

```

## Ερωτήσεις σχετικά με το ICMP:

12) Πως θα δείτε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;

Θα βάλω στα φίλτρα το φίλτρο ICMP

μερος A.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

| No. | Time      | Source         | Destination | Protocol | Length | Info   |
|-----|-----------|----------------|-------------|----------|--------|--|
| 16  | 24.099079 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1567/7942, ttl=1 (no response found!) |
| 17  | 24.101844 | 192.168.2.1    | 192.168.2.3 | ICMP     | 134    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 18  | 24.102970 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1568/8198, ttl=1 (no response found!) |
| 19  | 24.105214 | 192.168.2.1    | 192.168.2.3 | ICMP     | 134    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 20  | 24.106167 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1569/8454, ttl=1 (no response found!) |
| 21  | 24.107908 | 192.168.2.1    | 192.168.2.3 | ICMP     | 134    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 24  | 25.131114 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1570/8710, ttl=2 (no response found!) |
| 25  | 25.154966 | 10.13.255.49   | 192.168.2.3 | ICMP     | 110    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 26  | 25.156350 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1571/8966, ttl=2 (no response found!) |
| 27  | 25.183822 | 10.13.255.49   | 192.168.2.3 | ICMP     | 110    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 28  | 25.186187 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1572/9222, ttl=2 (no response found!) |
| 29  | 25.210881 | 10.13.255.49   | 192.168.2.3 | ICMP     | 110    | Time-to-live exceeded (Time to live exceeded in transit)                 |
| 32  | 26.209574 | 192.168.2.3    | 23.38.6.198 | ICMP     | 106    | Echo (ping) request id=0x0001, seq=1573/9478, ttl=3 (no response found!) |
| 33  | 26.232696 | 62.160.245.125 | 192.168.2.3 | ICMP     | 186    | Time-to-live exceeded (Time to live exceeded in transit)                 |

> Frame 24: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface Device\NPF\_{3F93E3E8-9A67-4B48-913D-F871FB40EBE4}, id 0

> Ethernet II, Src: CloudNet\_92:6d:f5 (48:5f:99:92:6d:f5), Dst: Zte\_87:50:24 (34:4d:ea:87:50:24)

> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 23.38.6.198

> Internet Control Message Protocol

c) Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει =64 Bytes

IP διεύθυνση του Source: 192.168.2.1

15) Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο;

Υπάρχει αντιστοιχία των source ID διευθύνσεων των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt. Και συγκεκριμένα παρατηρώ πως το command prompt περιέχει τις ίδιες διευθύνσεις με το source IP απλά στο wireshark εμφανίζονται διπλότυπα ενώ στο tracert είναι μοναδικές οι διευθύνσεις.

μερος A.pcapng

File Edit View Go Capture Analyze Statistics



icmp.type == 11

| No. | Time      | Source         |
|-----|-----------|----------------|
| 17  | 24.101844 | 192.168.2.1    |
| 19  | 24.105214 | 192.168.2.1    |
| 21  | 24.107908 | 192.168.2.1    |
| 25  | 25.154966 | 10.13.255.49   |
| 27  | 25.183822 | 10.13.255.49   |
| 29  | 25.210881 | 10.13.255.49   |
| 33  | 26.233696 | 62.169.245.125 |
| 35  | 26.261200 | 62.169.245.125 |
| 37  | 26.285860 | 62.169.245.125 |
| 77  | 32.110685 | 62.169.252.118 |
| 79  | 32.144377 | 62.169.252.118 |
| 81  | 32.169147 | 62.169.252.118 |
| 91  | 38.096455 | 10.13.255.141  |

μερος A.pcapng

File Edit View Go Capture Analyze Statistics



icmp.type == 11

| No. | Time      | Source          |
|-----|-----------|-----------------|
| 91  | 38.096455 | 10.13.255.141   |
| 94  | 41.644483 | 10.13.255.141   |
| 98  | 42.678323 | 62.169.252.117  |
| 100 | 42.705015 | 62.169.252.117  |
| 102 | 42.731653 | 62.169.252.117  |
| 114 | 49.101945 | 62.169.252.230  |
| 116 | 49.129256 | 62.169.252.230  |
| 118 | 49.158787 | 62.169.252.230  |
| 139 | 55.103394 | 79.140.91.14    |
| 141 | 55.130715 | 79.140.91.14    |
| 143 | 55.188146 | 79.140.91.14    |
| 157 | 61.109951 | 195.22.210.96   |
| 159 | 61.188327 | 195.22.210.96   |
| 159 | 61.188327 | 195.22.210.96   |
| 161 | 61.266502 | 195.22.210.96   |
| 165 | 62.344607 | 213.144.183.158 |
| 167 | 62.422132 | 213.144.183.158 |
| 169 | 62.500229 | 213.144.183.158 |

## B' ΜΕΡΟΣ

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

Wireshark capture showing DNS traffic. The selected packet is a DNS query response from 192.168.2.1 to 192.168.2.3, containing the IP address 194.177.214.44 for www.ekt.gr.

| No.  | Time      | Source      | Destination | Protocol | Length | Info  |
|------|-----------|-------------|-------------|----------|--------|---|
| 1080 | 8.040104  | 192.168.2.1 | 192.168.2.3 | DNS      | 360    | Standard query response 0xd463 A apis.google.com CNAME plus.l.google.com A 172.217.169.142 NS ns1.google.com NS ns4.google.com... |
| 1189 | 8.490059  | 192.168.2.3 | 192.168.2.1 | DNS      | 79     | Standard query 0xfa6e A adservice.google.gr   |
| 1190 | 8.490680  | 192.168.2.3 | 192.168.2.1 | DNS      | 91     | Standard query 0x7905 A browser.pipe.aria.microsoft.com   |
| 1191 | 8.519001  | 192.168.2.1 | 192.168.2.3 | DNS      | 393    | Standard query response 0xfa6e A adservice.google.gr CNAME pagead46.l.doubleclick.net A 172.217.169.194 NS ns3.google.com NS n... |
| 1192 | 8.520992  | 192.168.2.1 | 192.168.2.3 | DNS      | 528    | Standard query response 0x7905 A browser.pipe.aria.microsoft.com CNAME prd.col.aria.browser.skypedata.akadns.net CNAME pipe.sk... |
| 1302 | 12.373975 | 192.168.2.3 | 192.168.2.1 | DNS      | 70     | Standard query 0xe3b6 A www.ekt.gr  |
| 1303 | 12.378566 | 192.168.2.1 | 192.168.2.3 | DNS      | 86     | Standard query response 0xe3b6 A www.ekt.gr A 194.177.214.44  |
| 1564 | 12.985983 | 192.168.2.3 | 192.168.2.1 | DNS      | 80     | Standard query 0xa315 A platform.twitter.com  |
| 1566 | 12.990175 | 192.168.2.1 | 192.168.2.3 | DNS      | 96     | Standard query response 0xa315 A platform.twitter.com A 192.229.233.25  |
| 1575 | 13.010766 | 192.168.2.3 | 192.168.2.1 | DNS      | 80     | Standard query 0x498f A fonts.googleapis.com  |
| 1596 | 13.050071 | 192.168.2.1 | 192.168.2.3 | DNS      | 351    | Standard query response 0x498f A fonts.googleapis.com A 172.217.169.202 NS ns3.google.com NS ns4.google.com NS ns1.google.com ... |
| 2994 | 14.386341 | 192.168.2.3 | 192.168.2.1 | DNS      | 84     | Standard query 0xbae4 A www.google-analytics.com  |
| 3030 | 14.413459 | 192.168.2.1 | 192.168.2.3 | DNS      | 392    | Standard query response 0xbae4 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 172.217.169.174 NS ns1.goo... |
| 3101 | 14.464200 | 192.168.2.3 | 192.168.2.1 | DNS      | 77     | Standard query 0x5b02 A fonts.gstatic.com   |

Ethernet II, Src: Zte\_87:50:24 (34:4d:ea:87:50:24), Dst: CloudNet\_92:6d:f5 (48:5f:99:92:6d:f5)  
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.3  
User Datagram Protocol, Src Port: 53, Dst Port: 65456  
Domain Name System (response)  
Transaction ID: 0xe3b6  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0  
Queries  
Answers  
www.ekt.gr: type A, class IN, addr 194.177.214.44  
[Request In: 1302]  
[Time: 0.004591000 seconds]

2) Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το [www.ekt.gr](http://www.ekt.gr) υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

Εφαρμόζω το φίλτρο tcp.port == 80

Wireshark capture showing TCP traffic filtered by tcp.port == 80. The selected packet is a TCP SYN segment from 192.168.2.3 to 194.177.214.44.

| No.  | Time      | Source         | Destination    | Protocol | Length | Info  |
|------|-----------|----------------|----------------|----------|--------|---|
| 63   | 5.437405  | 192.168.2.3    | 216.58.212.3   | TCP      | 66     | [TCP Dup ACK 55#1] 61595 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0 SLE=0 SRE=1      |
| 72   | 5.848482  | 216.58.212.3   | 192.168.2.3    | TCP      | 54     | 80 → 61596 [ACK] Seq=1 Ack=384 Win=61952 Len=0                                    |
| 77   | 5.849583  | 192.168.2.3    | 216.58.212.3   | TCP      | 54     | 61596 → 80 [ACK] Seq=384 Ack=591 Win=261376 Len=0                                 |
| 1318 | 12.383210 | 192.168.2.3    | 194.177.214.44 | TCP      | 66     | 61617 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 1319 | 12.383214 | 192.168.2.3    | 194.177.214.44 | TCP      | 66     | 61618 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 1348 | 12.614573 | 194.177.214.44 | 192.168.2.3    | TCP      | 62     | 80 → 61617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1            |
| 1349 | 12.614573 | 194.177.214.44 | 192.168.2.3    | TCP      | 62     | 80 → 61618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1            |
| 1351 | 12.615376 | 192.168.2.3    | 194.177.214.44 | TCP      | 54     | 61617 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                                      |
| 1352 | 12.615527 | 192.168.2.3    | 194.177.214.44 | TCP      | 54     | 61618 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                                      |
| 1374 | 12.768412 | 194.177.214.44 | 192.168.2.3    | TCP      | 54     | 80 → 61617 [ACK] Seq=1 Ack=381 Win=30016 Len=0                                    |
| 1375 | 12.768413 | 194.177.214.44 | 192.168.2.3    | TCP      | 1506   | 80 → 61617 [ACK] Seq=1 Ack=381 Win=30016 Len=1452 [TCP segment of a reassembled P |
| 1376 | 12.768414 | 194.177.214.44 | 192.168.2.3    | TCP      | 1506   | 80 → 61617 [ACK] Seq=1453 Ack=381 Win=30016 Len=1452 [TCP segment of a reassemble |
| 1377 | 12.768418 | 194.177.214.44 | 192.168.2.3    | TCP      | 1506   | 80 → 61617 [ACK] Seq=2905 Ack=381 Win=30016 Len=1452 [TCP segment of a reassemble |

Η σειρά εμφάνισης των πακέτων που ανταλλάσσονται μεταξύ του υπολογιστή μου και του συστήματος που φιλοξενεί το [www.ekt.gr](http://www.ekt.gr) και υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων πρέπει να εμφανίζονται με συγκεκριμένη σειρά όπως στο screen. Πρώτα εμφανίζεται το [SYN] έπειτα το [SYN,ACK] και τέλος το [ACK].

Για να δημιουργηθεί μία σύνδεση TCP από έναν υπολογιστή (πελάτη) σε έναν άλλο (διακομιστής) θα πρέπει να ακολουθηθούν τα βήματα που καθορίζονται στο πρωτόκολλο TCP. Συγκεκριμένα θα πρέπει οι δύο υπολογιστές να εμπλακούν σε μία διαδικασία που ονομάζεται τριμερής χειραψία, η οποία περιληπτικά έχει ως εξής:

1. Ο πελάτης (client) ζητά την δημιουργία μίας σύνδεσης στέλνοντας έναν πακέτο TCP SYN στον διακομιστή (server). Το όνομα του πακέτου προέρχεται από την λέξη *synchronize* που σημαίνει συγχρονισμός.
2. Ο διακομιστής απαντά στην αίτηση του πελάτη στέλνοντάς του ένα πακέτο TCP SYN-ACK, από την αγγλική λέξη *acknowledge* που σημαίνει αναγνώριση, αποδοχή.
3. Ο πελάτης απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός την σύνδεση.

Μετά το πέρας αυτών των τριών βημάτων, η σύνδεση TCP έχει εγκαθιδρυθεί και μπορούν να αποσταλούν δεδομένα προς και από τους δύο υπολογιστές

Η διαδικασία της χειραψίας τριών βημάτων πρέπει να έχει τα εξής χαρακτηριστικά :

Acknowledge number [ACK] = Sequence number [SYN, ACK]

Acknowledge number [SYN, ACK] = Sequence number [SYN]

- 3) Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο. Συνολικά έχω 230 πακέτα με φίλτρο http. Παρατηρώ πως κατά την επικοινωνία οι source ports γίνονται destination ports και το αντίθετο.

Ενδεικτικά:

| Source ports | Destination ports |
|--------------|-------------------|
| 61593        | 80                |
| 80           | 61593             |
| 61596        | 80                |
| 80           | 61596             |
| 61617        | 80                |
| 80           | 61617             |
| ...          | ...               |

μερος B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No.  | Time      | Source          | Destination     | Protocol | Length | Info   |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 30   | 4.042375  | 192.168.2.3     | 172.217.169.195 | HTTP     | 433    | GET / HTTP/1.1   |
| 32   | 4.525010  | 172.217.169.195 | 192.168.2.3     | HTTP     | 580    | HTTP/1.1 301 Moved Permanently (text/html)   |
| 64   | 5.461105  | 192.168.2.3     | 216.58.212.3    | HTTP     | 437    | GET / HTTP/1.1   |
| 76   | 5.849296  | 216.58.212.3    | 192.168.2.3     | HTTP     | 644    | HTTP/1.1 302 Found (text/html)   |
| 1354 | 12.617280 | 192.168.2.3     | 194.177.214.44  | HTTP     | 434    | GET / HTTP/1.1   |
| 1395 | 12.797099 | 194.177.214.44  | 192.168.2.3     | HTTP     | 155    | HTTP/1.1 200 OK (text/html)  |
| 1398 | 12.808378 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_bI168Ghk-1JLv0tKtEjgN4Lpjnn1sYDyRuvb7EQ0rLc.css HTTP/1.1 |
| 1401 | 12.817278 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_xE-rWrJf-fncB6ztZfd2huxagxu4W0-qwma6Xer30m4.css HTTP/1.1 |
| 1408 | 12.825037 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_RB9Xcn1mzDe6urw6Cx0SM8Uqx_9cEkJ4T679PqnEqqI.css HTTP/1.1 |
| 1409 | 12.826870 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_pkDSqtLbuzkTYVXT3fILlWSPE0EHcsjALx_gZX1g6kA.css HTTP/1.1 |
| 1414 | 12.856162 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_MeXNqsgksWlMe63FfAOFVcGc0FL1noZ0biXB2069spU.css HTTP/1.1 |
| 1418 | 12.857982 | 192.168.2.3     | 194.177.214.44  | HTTP     | 395    | GET /misc/jquery.js?v=1.4.4 HTTP/1.1   |
| 1425 | 12.858250 | 194.177.214.44  | 192.168.2.3     | HTTP     | 970    | HTTP/1.1 200 OK (text/css)   |
| 1429 | 12.858255 | 194.177.214.44  | 192.168.2.3     | HTTP     | 1254   | HTTP/1.1 200 OK (text/css)   |

> Frame 30: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF\_{3F93E3E8-9A67-4B48-913D-F871FB40EBE4}, id 0

> Ethernet II, Src: CloudNet\_92:6d:f5 (48:5f:99:92:6d:f5), Dst: Zte\_87:50:24 (34:4d:ea:87:50:24)

> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 172.217.169.195

✓ Transmission Control Protocol, Src Port: 61593, Dst Port: 80, Seq: 1, Ack: 1, Len: 379

Source Port: 61593

Destination Port: 80

[Stream index: 3]

[TCP Segment Len: 379]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3960309100



4) Τα πακέτα που περιείχαν HTTP GET αίτημα που έστειλε ο browser μου είναι: 100

Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;

Παρατηρώ ότι οι IP destination διευθύνσεις επαναλαμβάνονται και συνολικά έχω 5 μοναδικές (Για διευκόλυνση ταξινομώ τα πακέτα στο Wireshark με βάσει τις στήλες που μου εμφανίζει ανά πακέτο)..

- 172.217.169.195
- 172.217.169.202
- 192.229.233.50
- 194.177.214.44
- 216.28.212.3

μερος B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == GET

| No.  | Time      | Source      | Destination     | Protocol | Length | Info  |
|------|-----------|-------------|-----------------|----------|--------|---|
| 30   | 4.042375  | 192.168.2.3 | 172.217.169.195 | HTTP     | 433    | GET / HTTP/1.1  |
| 3248 | 14.576718 | 192.168.2.3 | 172.217.169.195 | HTTP     | 452    | GET /s/opensans/v17/mem8YaGs126MiZpBA-UfVZ0b.woff2 HTTP/1.1   |
| 3249 | 14.577111 | 192.168.2.3 | 172.217.169.195 | HTTP     | 456    | GET /s/opensans/v17/mem5YaGs126MiZpBA-UN7rgOUuuhp.woff2 HTTP/1.1  |
| 3250 | 14.577113 | 192.168.2.3 | 172.217.169.195 | HTTP     | 456    | GET /s/opensans/v17/mem5YaGs126MiZpBA-UNirkOUuuhp.woff2 HTTP/1.1  |
| 3260 | 14.581426 | 192.168.2.3 | 172.217.169.195 | HTTP     | 455    | GET /s/opensans/v17/mem8YaGs126MiZpBA-UfVp0bbck.woff2 HTTP/1.1  |
| 3283 | 14.594164 | 192.168.2.3 | 172.217.169.195 | HTTP     | 459    | GET /s/opensans/v17/mem5YaGs126MiZpBA-UN7rgOUehp0qc.woff2 HTTP/1.1  |
| 3295 | 14.602563 | 192.168.2.3 | 172.217.169.195 | HTTP     | 459    | GET /s/opensans/v17/mem5YaGs126MiZpBA-UNirkOUehp0qc.woff2 HTTP/1.1  |
| 1630 | 13.095328 | 192.168.2.3 | 172.217.169.202 | HTTP     | 493    | GET /css?family=Open+Sans:300italic,400italic,600italic,700italic,400,600,700,300&subset=latin,greek HTTP/1.1 |
| 6000 | 16.620845 | 192.168.2.3 | 192.229.233.50  | HTTP     | 421    | GET /emoji/v2/72x72/1f1ea-1f1fa.png HTTP/1.1  |
| 1354 | 12.617280 | 192.168.2.3 | 194.177.214.44  | HTTP     | 434    | GET / HTTP/1.1  |
| 1398 | 12.808378 | 192.168.2.3 | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_bI168Ghk-1JLv0tKtEjgN4LpjnnlsYDyRuvb7EQ0rLc.css HTTP/1.1                    |
| 1401 | 12.817278 | 192.168.2.3 | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4W0-qwma6Xer30m4.css HTTP/1.1                    |
| 1408 | 12.825037 | 192.168.2.3 | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_RB9Xcn1mzDe6urw6Cx0SM8Uqx_9cEkJ4T679PqnEqqI.css HTTP/1.1                    |
| 1409 | 12.826870 | 192.168.2.3 | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_pkDSqtLbuzkTYVXT3FiLlWSPE0EHcsjALx_gZX1g6kA.css HTTP/1.1                    |

> Frame 30: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF\_{3F93E3E8-9A67-4B48-913D-F871FB40EBE4}, id 0

> Ethernet II, Src: CloudNet\_92:6d:f5 (48:5f:99:92:6d:f5), Dst: Zte\_87:50:24 (34:4d:ea:87:50:24)

> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 172.217.169.195

> Transmission Control Protocol, Src Port: 61593, Dst Port: 80, Seq: 1, Ack: 1, Len: 379

> Hypertext Transfer Protocol

Φαίνεται και στο screen πως η διεύθυνση 172.217.169.195 για παράδειγμα πως επαναλαμβάνεται πολλές φορές. Οι μοναδικές distinct destination addresses είναι οι παραπάνω.

5) Ο browser μου τρέχει την έκδοση HTTP 1.1  
Ο server Τρέχει την έκδοση 1.1

\*WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

| No.  | Time      | Source          | Destination     | Protocol | Length | Info   |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 30   | 4.042375  | 192.168.2.3     | 172.217.169.195 | HTTP     | 433    | GET / HTTP/1.1   |
| 32   | 4.525010  | 172.217.169.195 | 192.168.2.3     | HTTP     | 580    | HTTP/1.1 301 Moved Permanently (text/html)   |
| 64   | 5.461105  | 192.168.2.3     | 216.58.212.3    | HTTP     | 437    | GET / HTTP/1.1   |
| 76   | 5.849296  | 216.58.212.3    | 192.168.2.3     | HTTP     | 644    | HTTP/1.1 302 Found (text/html)   |
| 1354 | 12.617280 | 192.168.2.3     | 194.177.214.44  | HTTP     | 434    | GET / HTTP/1.1   |
| 1395 | 12.797099 | 194.177.214.44  | 192.168.2.3     | HTTP     | 155    | HTTP/1.1 200 OK (text/html)  |
| 1398 | 12.808378 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_bI168Ghk-1JLv0tKtEjgN4LpjnnlsYDyRuvb7EQ0rLc.css HTTP/1.1 |
| 1401 | 12.817278 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4W0-qwma6Xer30m4.css HTTP/1.1 |
| 1408 | 12.825037 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_RB9Xcn1mzDe6urw6Cx0SM8Uqx_9cEkJ4T679PqnEqqI.css HTTP/1.1 |
| 1409 | 12.826870 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_pkDSqtLbuzkTYVXT3FiLlWSPE0EHcsjALx_gZX1g6kA.css HTTP/1.1 |
| 1414 | 12.856162 | 192.168.2.3     | 194.177.214.44  | HTTP     | 464    | GET /sites/ekt-site/files/css/css_MeXNqsgksWlMe63FfA0FVcGc0FLnoZ0biXB2069spU.css HTTP/1.1  |
| 1418 | 12.857982 | 192.168.2.3     | 194.177.214.44  | HTTP     | 395    | GET /misc/jquery.js?v=1.4.4 HTTP/1.1   |
| 1425 | 12.858250 | 194.177.214.44  | 192.168.2.3     | HTTP     | 970    | HTTP/1.1 200 OK (text/css)   |
| 1429 | 12.858255 | 194.177.214.44  | 192.168.2.3     | HTTP     | 1254   | HTTP/1.1 200 OK (text/css)   |

> Frame 30: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF\_{3F93E3E8-9A67-4B48-913D-F871FB40EBE4}, id 0

> Ethernet II, Src: CloudNet\_92:6d:f5 (48:5f:99:92:6d:f5), Dst: Zte\_87:50:24 (34:4d:ea:87:50:24)

> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 172.217.169.195

> Transmission Control Protocol, Src Port: 61593, Dst Port: 80, Seq: 1, Ack: 1, Len: 379

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: en-GB,en;q=0.7,el;q=0.3\r\n

Upgrade-Insecure-Requests: 1\r\n