
ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Εργασία-Wireshark

3160045- Καλδής Αργύριος

Εκτελώντας την εντολή **tracert** www.ieee.org στο Command Prompt έχουμε το παρακάτω αποτέλεσμα:

```
Command Prompt

> ipconfig                ... Show information
> ipconfig /all           ... Show detailed information
> ipconfig /renew         ... renew all adapters
> ipconfig /renew EL*     ... renew any connection that has its
                           name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                           eg. "Wired Ethernet Connection 1" or
                           "Wired Ethernet Connection 2"
> ipconfig /allcompartments ... Show information about all
                           compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                           compartments

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

Tracing route to e1630.c.akamaiedge.net [23.37.59.20]
over a maximum of 30 hops:

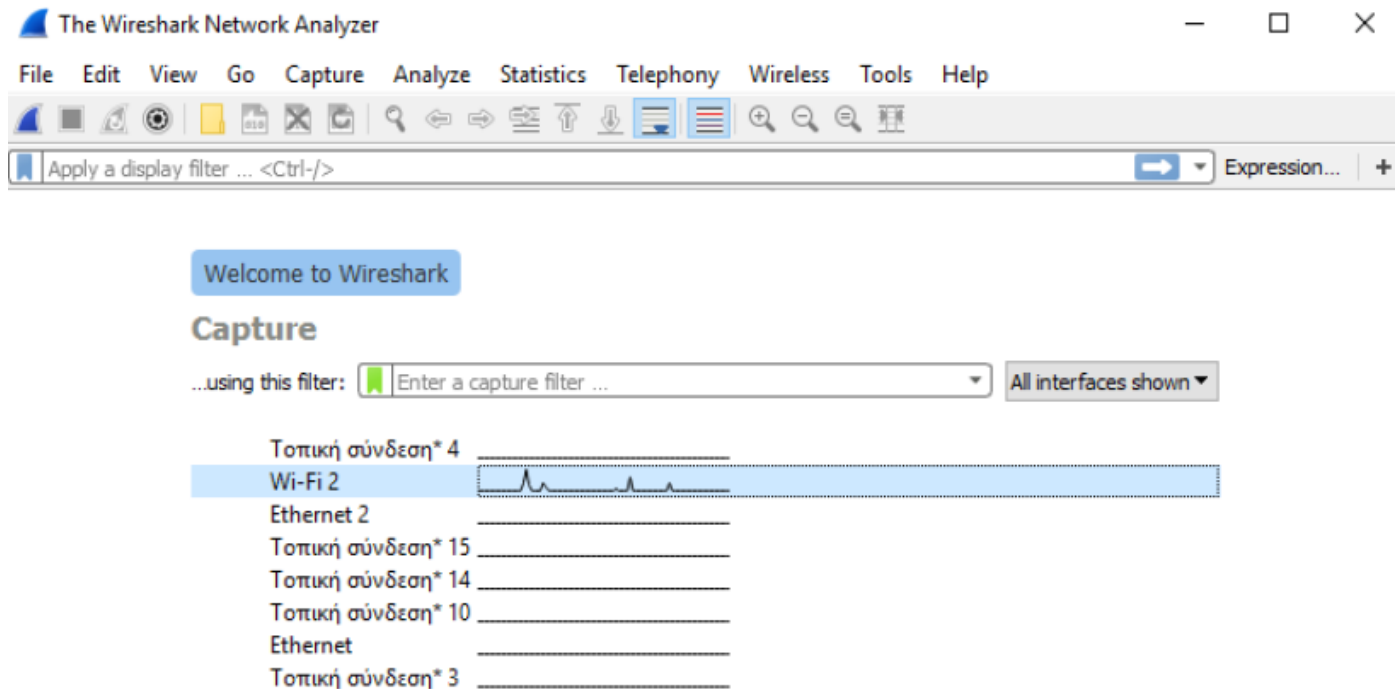
  1    2 ms    2 ms    2 ms  speedport-entry-2i.ote.gr [192.168.1.1]
  2    9 ms    7 ms    9 ms  80.106.125.100
  3    8 ms    9 ms    9 ms  79.128.250.254
  4    8 ms    8 ms   18 ms  kolasr01-hu-0-5-0-0.ath.OTEGlobe.gr [62.75.3.13]
  5   49 ms   47 ms   48 ms  62.75.6.190
  6   45 ms   47 ms   45 ms  decix-fra5.netarch.akamai.com [80.81.192.168]
  7   46 ms   46 ms   51 ms  a23-37-59-20.deploy.static.akamaitechnologies.com [23.37.59.20]

Trace complete.

C:\Users\Argy>
```

Το λειτουργικό σύστημα που χρησιμοποιείται στη παρακάτω εργασία είναι τα Windows 10 Pro 64-bit.

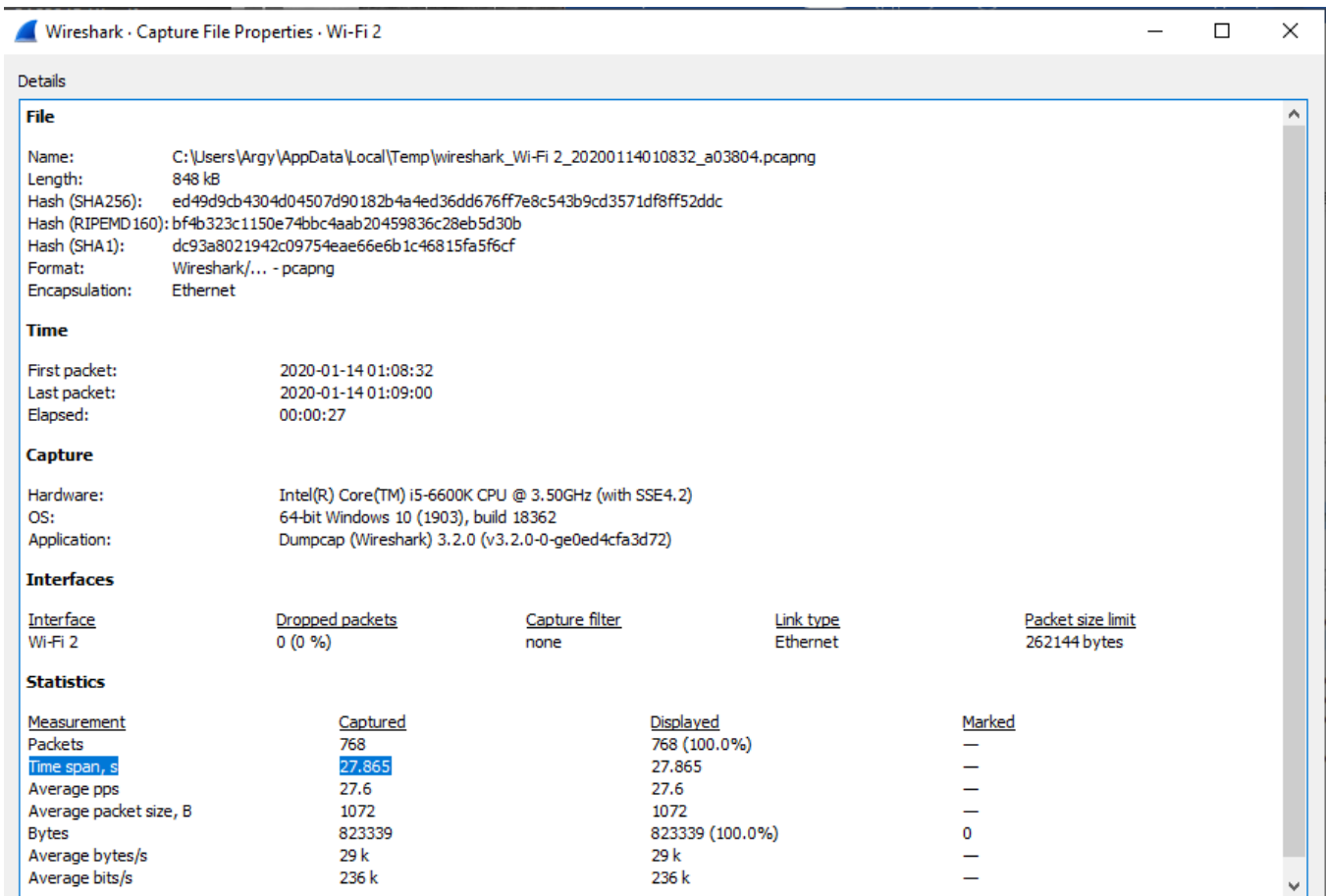
Η διαδικασία ανίχνευσης πακέτων εκτελείται στη διεπαφή Wi-Fi2 όπως φαίνεται και παρακάτω.



Απαντήσεις Γενικών Ερωτήσεων

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσής σας;

Η χρονική διάρκεια της ανίχνευσής μπορεί να βρεθεί πατώντας στη **επιλογή Statistics** - **> Capture File Properties** (ή έχοντας ένα χρονόμετρο ακριβείας στη διάθεση μας.JK) . Στη συγκεκριμένη περίπτωση η διάρκεια ήταν **27.865s**. Συγκεκριμένα η χρονική διάρκεια φαίνεται στο πεδίο Time span,s.



The screenshot shows the 'Wireshark · Capture File Properties · Wi-Fi 2' window. The 'Details' pane is active, displaying the following information:

- File**
 - Name: C:\Users\Argy\AppData\Local\Temp\wireshark_Wi-Fi 2_20200114010832_a03804.pcapng
 - Length: 848 kB
 - Hash (SHA256): ed49d9cb4304d04507d90182b4a4ed36dd676ff7e8c543b9cd3571df8ff52ddc
 - Hash (RIPEMD 160): bf4b323c1150e74bbc4aab20459836c28eb5d30b
 - Hash (SHA1): dc93a8021942c09754eae66e6b1c46815fa5f6cf
 - Format: Wireshark/... - pcapng
 - Encapsulation: Ethernet
- Time**
 - First packet: 2020-01-14 01:08:32
 - Last packet: 2020-01-14 01:09:00
 - Elapsed: 00:00:27
- Capture**
 - Hardware: Intel(R) Core(TM) i5-6600K CPU @ 3.50GHz (with SSE4.2)
 - OS: 64-bit Windows 10 (1903), build 18362
 - Application: Dumpcap (Wireshark) 3.2.0 (v3.2.0-0-ge0ed4cfa3d72)
- Interfaces**

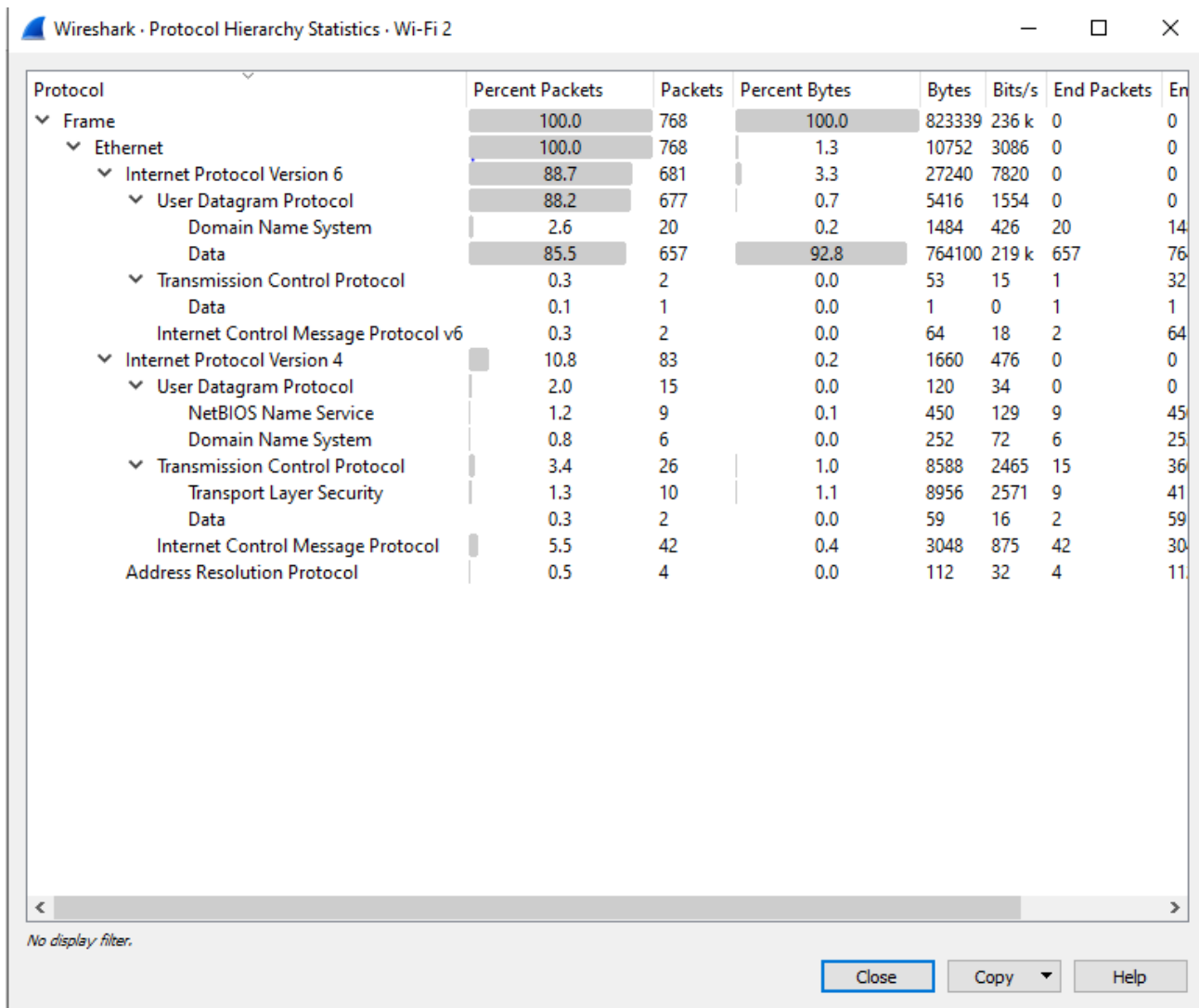
| Interface | Dropped packets | Capture filter | Link type | Packet size limit |
|-----------|-----------------|----------------|-----------|-------------------|
| Wi-Fi 2 | 0 (0 %) | none | Ethernet | 262144 bytes |
- Statistics**

| Measurement | Captured | Displayed | Marked |
|------------------------|---------------|-----------------|--------|
| Packets | 768 | 768 (100.0%) | — |
| Time span, s | 27.865 | 27.865 | — |
| Average pps | 27.6 | 27.6 | — |
| Average packet size, B | 1072 | 1072 | — |
| Bytes | 823339 | 823339 (100.0%) | 0 |
| Average bytes/s | 29 k | 29 k | — |
| Average bits/s | 236 k | 236 k | — |

2. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στη χρονική διάρκεια της ανίχνευσης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

Τα πρωτόκολλα που χρησιμοποίησε ο υπολογιστής μπορούν να βρεθούν μεταβαίνοντας στην επιλογή **Statistics -> Protocol Hierarchy**.

Πατώντας την επιλογή αυτή εμφανίζονται όλα τα πρωτόκολλα που εντοπίστηκαν στην Ανίχνευση σε ιεραρχική δομή.



Wireshark · Protocol Hierarchy Statistics · Wi-Fi 2

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes |
|--------------------------------------|-----------------|---------|---------------|--------|--------|-------------|-----------|
| ▼ Frame | 100.0 | 768 | 100.0 | 823339 | 236 k | 0 | 0 |
| ▼ Ethernet | 100.0 | 768 | 1.3 | 10752 | 3086 | 0 | 0 |
| ▼ Internet Protocol Version 6 | 88.7 | 681 | 3.3 | 27240 | 7820 | 0 | 0 |
| ▼ User Datagram Protocol | 88.2 | 677 | 0.7 | 5416 | 1554 | 0 | 0 |
| Domain Name System | 2.6 | 20 | 0.2 | 1484 | 426 | 20 | 14 |
| Data | 85.5 | 657 | 92.8 | 764100 | 219 k | 657 | 76 |
| ▼ Transmission Control Protocol | 0.3 | 2 | 0.0 | 53 | 15 | 1 | 32 |
| Data | 0.1 | 1 | 0.0 | 1 | 0 | 1 | 1 |
| Internet Control Message Protocol v6 | 0.3 | 2 | 0.0 | 64 | 18 | 2 | 64 |
| ▼ Internet Protocol Version 4 | 10.8 | 83 | 0.2 | 1660 | 476 | 0 | 0 |
| ▼ User Datagram Protocol | 2.0 | 15 | 0.0 | 120 | 34 | 0 | 0 |
| NetBIOS Name Service | 1.2 | 9 | 0.1 | 450 | 129 | 9 | 45 |
| Domain Name System | 0.8 | 6 | 0.0 | 252 | 72 | 6 | 25 |
| ▼ Transmission Control Protocol | 3.4 | 26 | 1.0 | 8588 | 2465 | 15 | 36 |
| Transport Layer Security | 1.3 | 10 | 1.1 | 8956 | 2571 | 9 | 41 |
| Data | 0.3 | 2 | 0.0 | 59 | 16 | 2 | 59 |
| Internet Control Message Protocol | 5.5 | 42 | 0.4 | 3048 | 875 | 42 | 30 |
| Address Resolution Protocol | 0.5 | 4 | 0.0 | 112 | 32 | 4 | 11 |

No display filter.

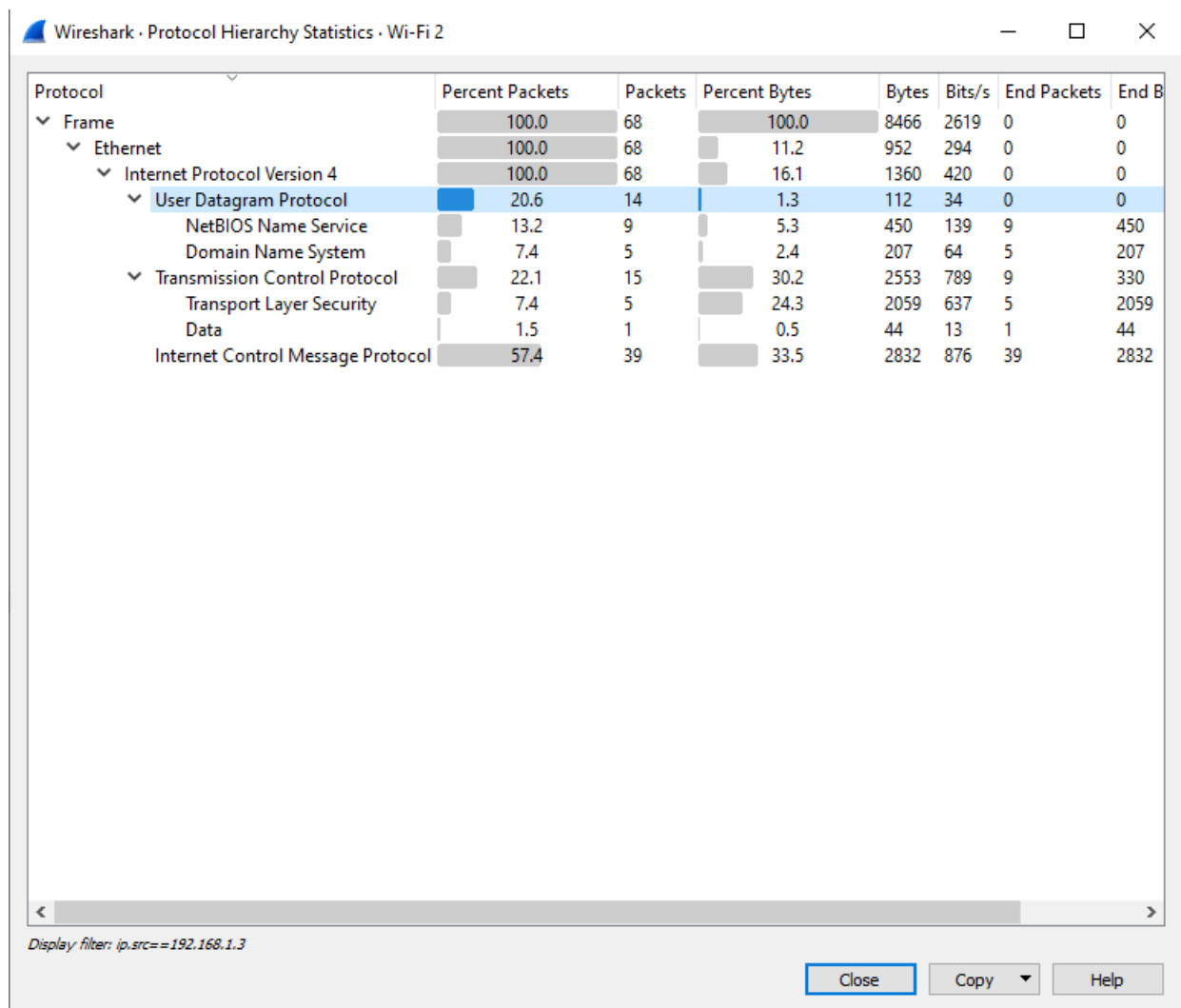
Close Copy Help

3. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

Το πρωτόκολλο DNS χρησιμοποιούν το πρωτόκολλο UDP ενώ τα υπόλοιπα πρωτόκολλα συμπεριλαμβανομένου των ICMP χρησιμοποιούν το πρωτόκολλο TCP.

4. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Εκτελώντας την εντολή `ip.src==192.168.1.3` βλέπουμε τα πακέτα που σταλθηκαν. Στη συγκεκριμένη περίπτωση είναι UDP=14 και TCP= 15.



5. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε ποιες συσκευές αντιστοιχούν;

Ο πίνακας Endpoints εμφανίζει της MAC διευθύνσεις των διαφορετικών συσκευών. Στο παρακάτω πίνακα φαίνονται η συνδέσεις και τα ονόματα τις κάθε συσκευής.

The image shows two side-by-side screenshots of the Wireshark network analysis tool. The left screenshot displays the 'Conversations' pane for 'Wi-Fi 2', showing a table of network connections. The right screenshot displays the 'Endpoints' pane for 'Wi-Fi 2', showing a table of MAC addresses and their associated traffic statistics.

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|-------------------|------------------|---------|-------|---------------|-------------|---------------|-------------|
| 18:d6:c7:18:02:2f | 50:78:b3:cefb:46 | 768 | 823 k | 142 | 16 k | 626 | 806 k |

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|-------------------|---------|-------|------------|----------|------------|----------|
| 18:d6:c7:18:02:2f | 768 | 823 k | 142 | 16 k | 626 | 806 k |
| 50:78:b3:cefb:46 | 768 | 823 k | 626 | 806 k | 142 | 16 k |

6. Πόσα και ποια είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγήστε γιατί συμβαίνει αυτό.

Οι διευθύνσεις IPv4 που εντοπίστηκαν κατά την ανίχνευση ήταν 13 δηλαδή 11 περισσότερα από τα Ethernet. Αυτό οφείλεται στο γεγονός ότι το κάθε επίπεδο δικτύου επικοινωνεί με κόμβους του διαδικτύου ενώ το επίπεδο σύνδεσης δεδομένων με κόμβους στους οποίους ο υπολογιστής συνδέεται άμεσα.

Τα μόνα endpoint που ταυτίζονται είναι οι διεύθυνσης του υπολογιστή.

| Wireshark · Endpoints · Wi-Fi 2 | | | | | | | | | |
|---------------------------------|---------|-----------|------------|----------|------------|----------|--|----------|-------|
| Ethernet · 2 | | IPv4 · 13 | | IPv6 · 6 | | TCP · 12 | | UDP · 22 | |
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | | | |
| 18:d6:c7:18:02:2f | 768 | 823 k | 142 | 16 k | 626 | | | | 806 k |
| 50:78:b3:ce:fb:46 | 768 | 823 k | 626 | 806 k | 142 | | | | 16 k |

| Wireshark · Endpoints · Wi-Fi 2 | | | | | | | | | |
|---------------------------------|---------|-----------|------------|----------|------------|----------|---------|----------|-----------|
| Ethernet · 2 | | IPv4 · 13 | | IPv6 · 6 | | TCP · 12 | | UDP · 22 | |
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number |
| 23.37.59.20 | 24 | 2544 | 3 | 318 | 21 | 2226 | — | — | — |
| 34.194.76.214 | 2 | 139 | 0 | 0 | 2 | 139 | — | — | — |
| 34.199.158.228 | 3 | 534 | 1 | 288 | 2 | 246 | — | — | — |
| 34.225.107.124 | 2 | 139 | 0 | 0 | 2 | 139 | — | — | — |
| 52.5.92.97 | 16 | 8439 | 8 | 5998 | 8 | 2441 | — | — | — |
| 62.75.3.13 | 3 | 330 | 3 | 330 | 0 | 0 | — | — | — |
| 62.75.6.190 | 6 | 606 | 3 | 330 | 3 | 276 | — | — | — |
| 67.229.60.114 | 3 | 221 | 2 | 123 | 1 | 98 | — | — | — |
| 79.128.250.254 | 6 | 606 | 3 | 330 | 3 | 276 | — | — | — |
| 80.81.192.168 | 3 | 210 | 3 | 210 | 0 | 0 | — | — | — |
| 80.106.125.100 | 6 | 606 | 3 | 330 | 3 | 276 | — | — | — |
| 192.168.1.1 | 9 | 906 | 4 | 489 | 5 | 417 | — | — | — |
| 192.168.1.3 | 83 | 15 k | 50 | 6534 | 33 | 8746 | — | — | — |

Ερωτήσεις σχετικά με το DNS.

- 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.

Εφαρμόζοντας την εντολή `dns.qry.name == "www.ieee.org"` βρίσκουμε τον αποστολέα και τον παραλήπτη.

*Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name=="www.ietf.org"

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|---|
| 207 | 1.703611 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x4c18 A www.ietf.org |
| 208 | 1.703770 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x51f3 AAAA www.ietf.org |
| 209 | 1.714487 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 179 | Standard query response 0x4c18 A www.ietf.org CNAME www.ietf.org |
| 210 | 1.734660 | 192.168.1.3 | 192.168.1.1 | DNS | 72 | Standard query 0x51f3 AAAA www.ietf.org |
| 211 | 1.757307 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 224 | Standard query response 0x51f3 AAAA www.ietf.org CNAME www.ietf.org |

< >

> Frame 211: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF_{A2FCB102-B16C-458A-8FFC-DFCB7EAE888}

> Ethernet II, Src: Zte_ce:fb:46 (50:78:b3:ce:fb:46), Dst: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f)

> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::c188:53b4:3e61:94d7

> User Datagram Protocol, Src Port: 53, Dst Port: 59440

Source Port: 53

Destination Port: 59440

Length: 170

Checksum: 0xb611 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

> [Timestamps]

> Domain Name System (response)

< >

Κατά την αποστολή η UDP Θύρα είναι η 59440 , και η θύρα παραλαβής είναι η 53. Η απάντηση περιέχει τις θύρες αποστολής και παραλαβής αντεστραμμένες όπως φαίνεται και στη παραπάνω εικόνα.

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;

*Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name=="www.ietf.org"

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|---|
| 207 | 1.703611 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x4c18 A www.ietf.org |
| 208 | 1.703770 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x51f3 AAAA www.ietf.org |
| 209 | 1.714487 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 179 | Standard query response 0x4c18 A www.ietf.org CNAME www.ietf.org |
| 210 | 1.734660 | 192.168.1.3 | 192.168.1.1 | DNS | 72 | Standard query 0x51f3 AAAA www.ietf.org |
| 211 | 1.757307 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 224 | Standard query response 0x51f3 AAAA www.ietf.org CNAME www.ietf.org |

< >

> Frame 207: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{A2FCB102-B16C-458A-8FFC-DFCB7EAE888F},
 > Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_ce:fb:46 (50:78:b3:ce:fb:46)
 > Internet Protocol Version 6, Src: fe80::c188:53b4:3e61:94d7, Dst: fe80::1
 > User Datagram Protocol, Src Port: 55397, Dst Port: 53
 > Domain Name System (query)
 > Transaction ID: 0x4c18
 > Flags: 0x0100 Standard query
 > Questions: 1
 > Answer RRs: 0
 > Authority RRs: 0
 > Additional RRs: 0
 > Queries
 > [Response In: 209]

Η διάκριση μεταξύ ενός πακέτου αιτήματος και ενός απάντησης σε ερώτημα θα μπορούσε να διακριθεί από το πεδίο κάτω απ το Queries (Παραπάνω εικόνα) όπου εάν είναι αίτημα τότε αναγράφεται "Response In: __" Ενώ αν είναι απάντηση τότε είναι " Request In: __".

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

Στη συγκεκριμένη περίπτωση ο server δεν είναι authoritative όπως φαίνεται στη παρακάτω εικόνα.

The image shows a Wireshark capture of DNS traffic. The packet list pane at the top shows five packets. Packet 209 is selected, showing a DNS response from 192.168.1.3 to fe80::1. The packet details pane below shows the structure of the DNS response, including flags indicating it is a standard query response and not authoritative.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|---|
| 207 | 1.703611 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x4c18 A www.ieee.org |
| 208 | 1.703770 | fe80::c188:53b4:3e6... | fe80::1 | DNS | 92 | Standard query 0x51f3 AAAA www.ieee.org |
| 209 | 1.714487 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 179 | Standard query response 0x4c18 A www.ieee.org CNAME www.i |
| 210 | 1.734660 | 192.168.1.3 | 192.168.1.1 | DNS | 72 | Standard query 0x51f3 AAAA www.ieee.org |
| 211 | 1.757307 | fe80::1 | fe80::c188:53b4:3e6... | DNS | 224 | Standard query response 0x51f3 AAAA www.ieee.org CNAME ww |

Packet 209 details:

- User Datagram Protocol, Src Port: 53, Dst Port: 55397
- Domain Name System (response)
 - Transaction ID: 0x4c18
 - 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

10. Το όνομα www.ieee.org είναι domain name ή πρόκειται για canonical name;

Όπως φαίνεται στη πανω εικόνα στα info της απάντησης , μετά την διεύθυνση www.ieee.org υπάρχει η λέξη CNAME που σημαίνει ότι το ονομα είναι canonical και όχι domain.

11. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.ieee.org; Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;

Το ip του υπολογιστη μας είναι το **192.168.1.3**
Και του www.ieee.org είναι το 23.37.59.20

```
Select Command Prompt
Wireless LAN adapter Τοπική σύνδεση* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Τοπική σύνδεση* 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2a02:587:200b:2900:c188:53b4:3e61:94d7
Temporary IPv6 Address. . . . . : 2a02:587:200b:2900:c1d7:792f:da8f:b623
Link-local IPv6 Address . . . . . : fe80::c188:53b4:3e61:94d7%18
IPv4 Address. . . . . : 192.168.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%18
                          192.168.1.1

C:\Users\Argy>

Select Command Prompt
"Wired Ethernet 2"
> ipconfig /allcompartments ... Show information about all
> ipconfig /allcompartments /all ... Show detailed information about all compartments

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

Tracing route to e1630.c.akamaiedge.net [23.37.59.20]
over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms    speedport-entry-2i.ote.gr [192.168.1.1]
  2    9 ms    7 ms    9 ms    80.106.125.100
  3    8 ms    9 ms    9 ms    79.128.250.254
  4    8 ms    8 ms    18 ms   kolasr01-hu-0-5-0-0.ath.OTEGlobe.gr [62.75.3.13]
  5   49 ms   47 ms   48 ms   62.75.6.190
  6   45 ms   47 ms   45 ms   decix-fra5.netarch.akamai.com [80.81.192.168]
  7   46 ms   46 ms   51 ms   a23-37-59-20.deploy.static.akamaitechnologies.com [23.37.59.20]

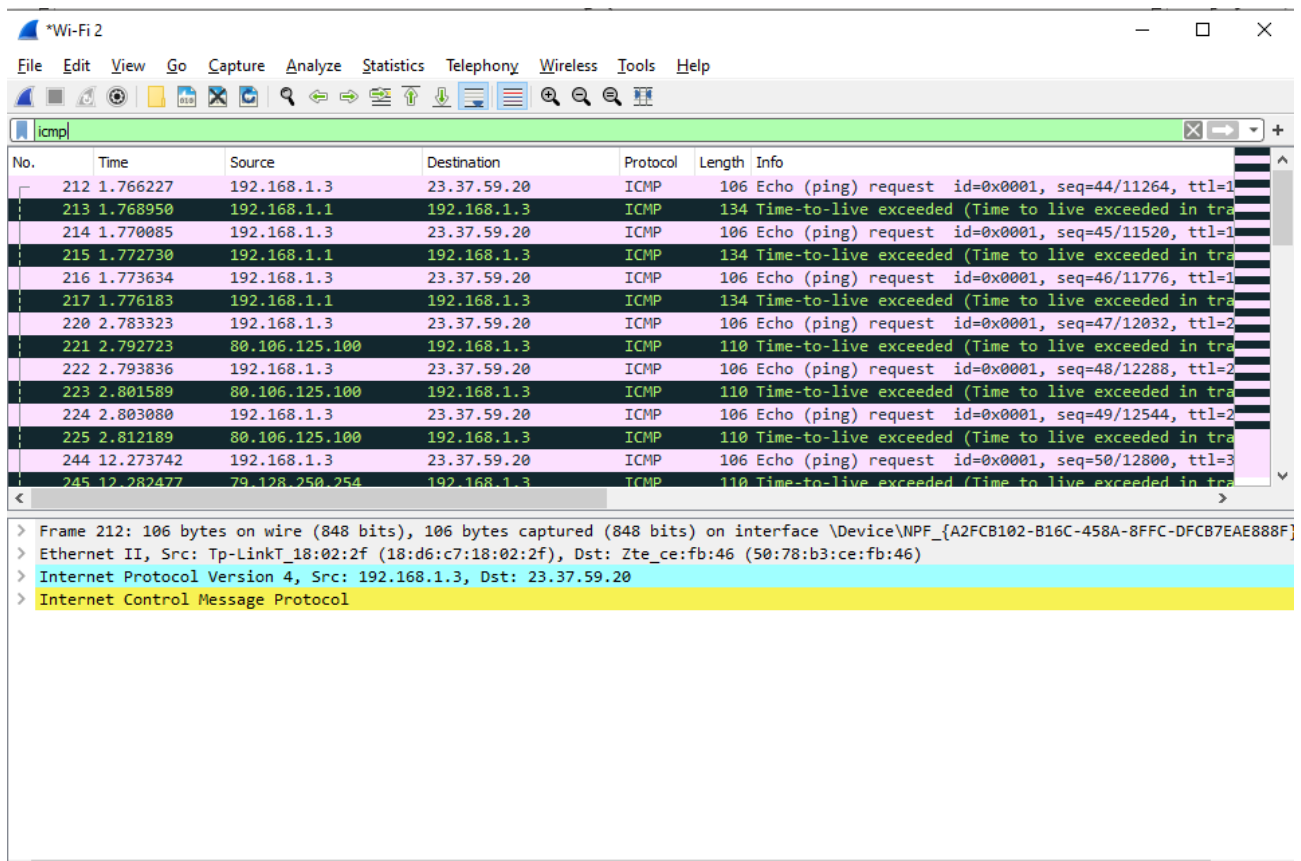
Trace complete.

C:\Users\Argy>
```

Ερωτήσεις σχετικά με το ICMP.

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

Εκτελούμε την εντολή `icmp` στο πλαίσιο.



13. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.

- Ποια είναι η IP διεύθυνση του destination;
- Πόσο είναι το time-to-live του πακέτου (ή το hop limit αν στο δίκτυο του provider τρέχει η IPv6 και όχι η IPv4 έκδοση του πρωτοκόλλου IP);
- Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;

a) Η IP διεύθυνση του destination όπως φαίνεται και στη παραπάνω εικόνα είναι η: 23.37.59.20

b) Κάνοντας κλικ στο πεδίο Internet Protocol Version 4 μπορούμε να βρούμε το πεδίο Time to live όπου στη συγκεκριμένη περίπτωση είναι 1.

The image shows a Wireshark capture of ICMP Echo (ping) requests and Time-to-live exceeded responses. The packet list shows multiple requests from 192.168.1.3 to 23.37.59.20 and corresponding 'Time-to-live exceeded' responses from 23.37.59.20 to 192.168.1.1. The packet details for the selected ICMP packet show a TTL of 1 and a source of 192.168.1.3.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|-------------|----------|--------|---|
| 212 | 1.766227 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=44/11264, ttl=1 |
| 213 | 1.768950 | 192.168.1.1 | 192.168.1.3 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in tra |
| 214 | 1.770085 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=45/11520, ttl=1 |
| 215 | 1.772730 | 192.168.1.1 | 192.168.1.3 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in tra |
| 216 | 1.773634 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=46/11776, ttl=1 |
| 217 | 1.776183 | 192.168.1.1 | 192.168.1.3 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in tra |
| 220 | 2.783323 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=47/12032, ttl=2 |
| 221 | 2.792723 | 80.106.125.100 | 192.168.1.3 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in tra |
| 222 | 2.793836 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=48/12288, ttl=2 |
| 223 | 2.801589 | 80.106.125.100 | 192.168.1.3 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in tra |
| 224 | 2.803080 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=49/12544, ttl=2 |
| 225 | 2.812189 | 80.106.125.100 | 192.168.1.3 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in tra |
| 244 | 12.273742 | 192.168.1.3 | 23.37.59.20 | ICMP | 106 | Echo (ping) request id=0x0001, seq=50/12800, ttl=3 |
| 245 | 12.282477 | 79.128.250.254 | 192.168.1.3 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in tra |

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 92
 Identification: 0x554b (21835)
 > Flags: 0x0000
 ...0 0000 0000 0000 = Fragment offset: 0
 > Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x5072 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.3
 Destination: 23.37.59.20
 > Internet Control Message Protocol

0000 50 78 b3 ce fb 46 18 d6 c7 18 02 2f 08 00 45 00 Px...F...../..E.
 0010 00 5c 55 4b 00 00 01 01 50 72 c0 a8 01 03 17 25 ..\UK.... Pr....%
 0020 3b 14 08 00 f7 d2 00 01 00 2c 00 00 00 00 00 00 ;.....,.....

Internet Control Message Protocol: Protocol | Packets: 768 · Displayed: 42 (5.5%) · Dropped: 0 (0.0%) | Profile: Default

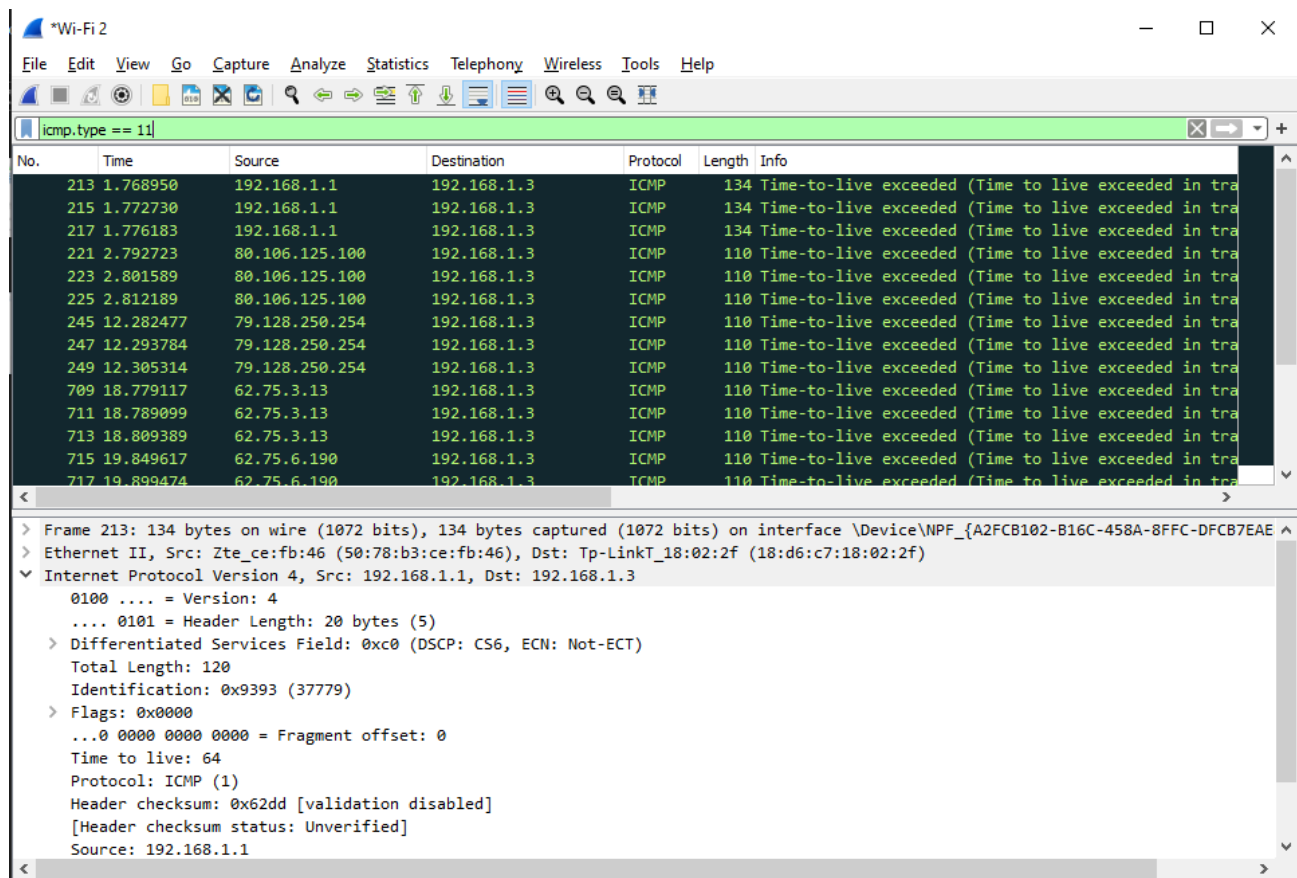
c) Το μέγεθος των δεδομένων είναι $92-20=72$.

14. . Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded.

Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του Source;

Εφαρμόζω την εντολή `icmp.type == 11` και μου εμφανίζει τη λίστα με όλα τα ICMP Time Exceeded.

Όπως φαίνεται και στη παρακάτω εικόνα το ip του **Source** είναι: **192.168.1.1** Και του **destination** είναι: **192.168.1.3**.

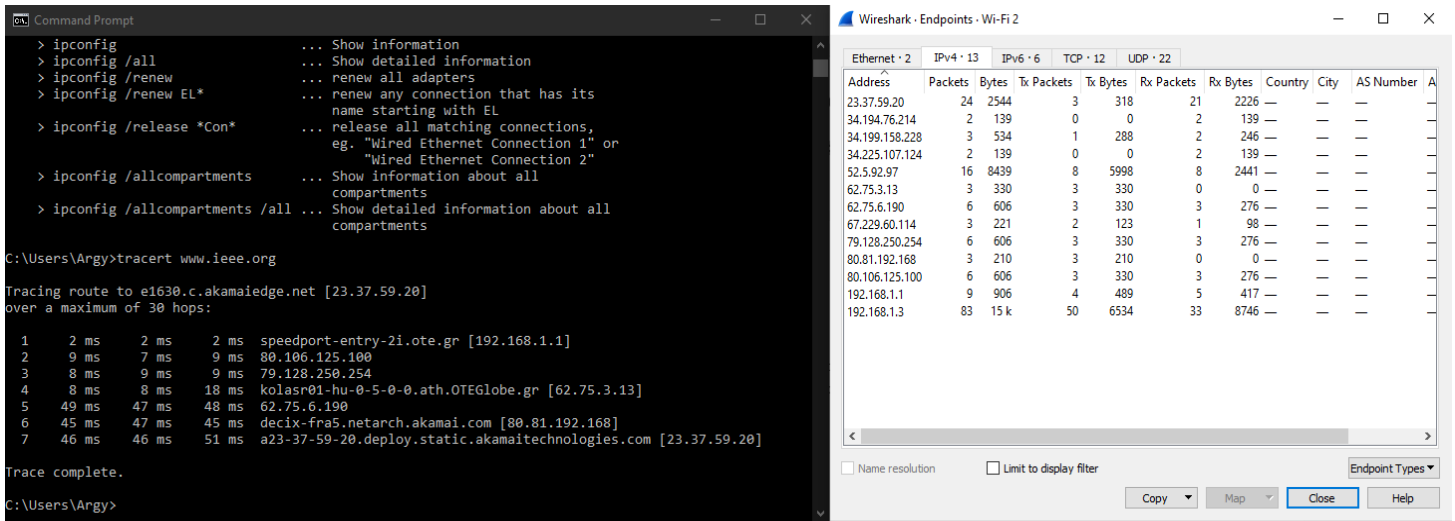


15. Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα.

Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής `tracert` στο `command prompt` παράθυρο;

Εφαρμόζω το φίλτρο `icmp` όπου θα μου εμφανίσει όλα τα `Icmp` πακέτα `Echo Request` και `Time exceeded`.

Ανοίγοντας τα endpoints για IPV4 παρατηρούμε ότι υπάρχει αντιστοιχία μεταξύ των source IP και της εντολής `tracert` στο `cmd`.



Μέρος Β

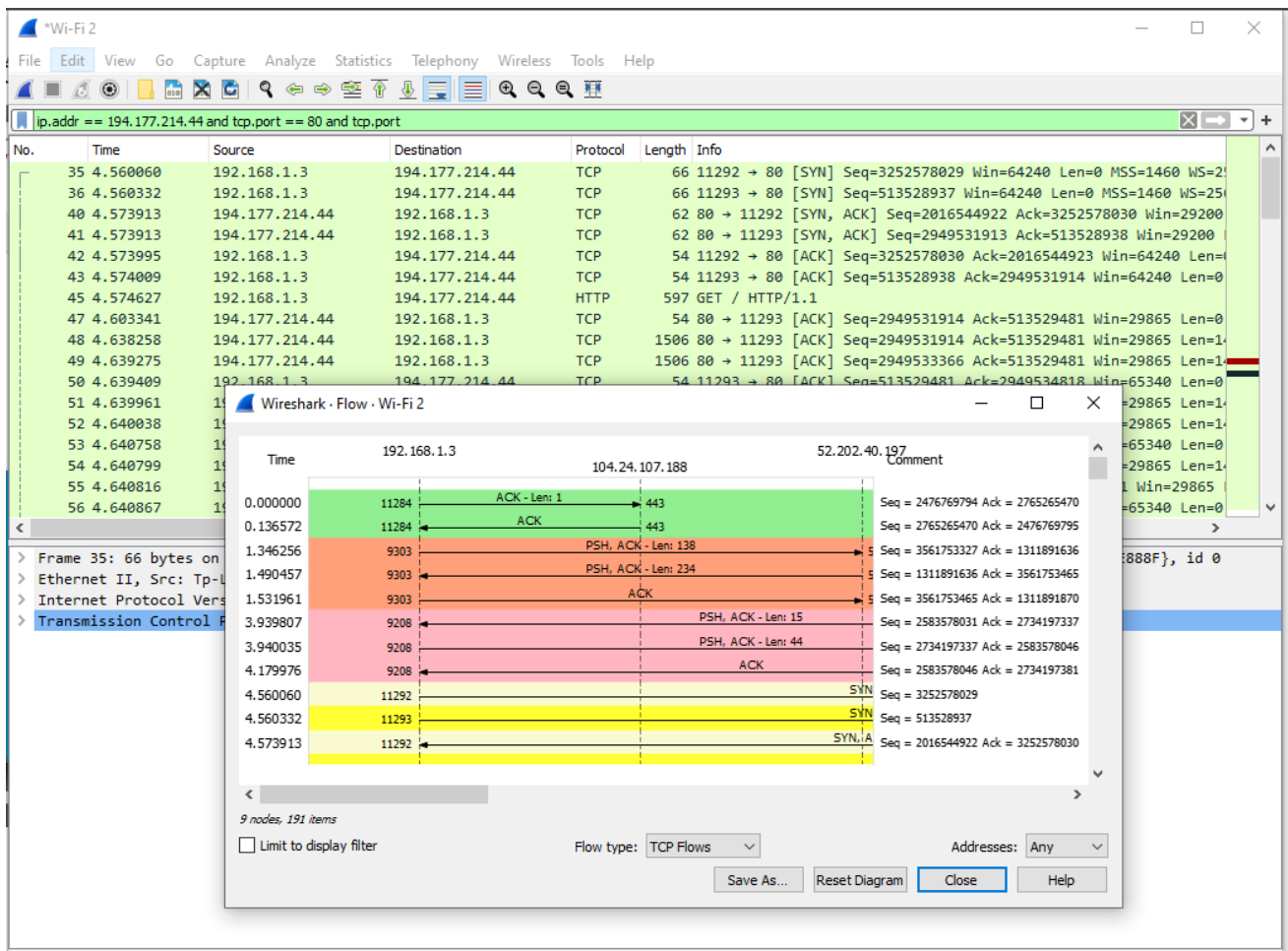
1. Ποία είναι η IP διεύθυνση που αντιστοιχεί στον www.ekt.gr;

Η διεύθυνση που αντιστοιχεί στον www.ekt.gr είναι **194.177.214.44**.

2. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το 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.

Για να πραγματοποιήσω την ανάλυση απενεργοποιώ αρχικά την επιλογή **Relative sequence numbers** από τις ρυθμίσεις του πρωτοκόλλου TCP επιλέγοντας **Edit → Preferences** από το μενού και μεταβαίνοντας στην καρτέλα **Protocols → TCP**.

Στην συνέχεια εφαρμόζω το φίλτρο **ip.addr == 194.177.214.44 and tcp.port == 80 and tcp.port** συγκεκριμένη σύνδεση στον server. Τα τρία πρώτα πακέτα στην λίστα πραγματοποιούν τη χειραψία τριών βημάτων για την εγκαθίδρυση της σύνδεσης. Τέλος επιλέγω **Statistics → Flow Graph** από το μενού, και στο νέο παράθυρο επιλέγω **TCP Flows** στο Flow Type πεδίο. Το νέο παράθυρο δίνει μία πιο συνοπτική εικόνα της χειραψίας.



3. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο.

Εφαρμόζω το πρωτόκολλο **http**. Στην συνέχεια επιλέγω **Statistics → Conversations → TCP** από το μενού και ενεργοποιώ την επιλογή **Limit to display filter**.

Στο HTTP πρωτόκολλο οι TCP θύρα του destination είναι η 80 ενώ η θύρα του source είναι η 11342. Ο αριθμός το TCP θυρών που χρησιμοποιήθηκαν από τον client είναι σχετικός του αριθμού των αρχείων που σχετίζονται με την Ιστοσελίδα και των αριθμώ των συνδέσεων που χρειαστήκαν μέχρι τα αρχεία να μεταφερθούν επιτυχώς.

The screenshot shows a Wireshark capture of HTTP traffic. The main packet list displays several GET requests to 194.177.214.44. A 'Conversations' window is open, showing a summary of the traffic between 192.168.1.3 and 194.177.214.44.

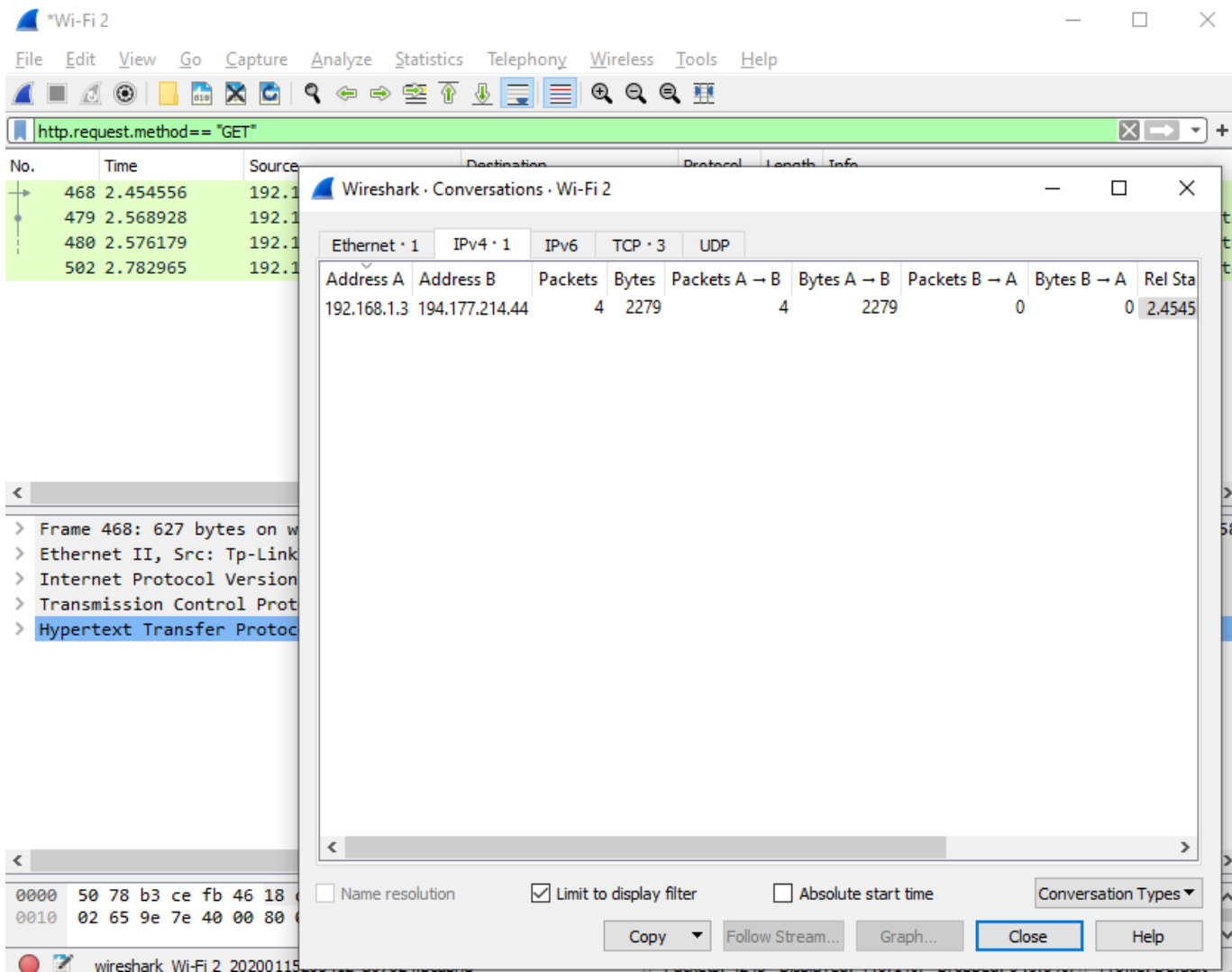
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 468 | 2.454556 | 192.168.1.3 | 194.177.214.44 | HTTP | 627 | GET / HTTP/1.1 |
| 477 | 2.525131 | 194.177.214.44 | 192.168.1.3 | HTTP | 338 | HTTP/1.1 304 Not Modified |
| 479 | 2.568928 | 192.168.1.3 | 194.177.214.44 | HTTP | 536 | GET /sites/ekt-site/libraries/tablesorter/jquery.metadata |
| 480 | 2.576179 | 192.168.1.3 | 194.177.214.44 | HTTP | 558 | GET /sites/ekt-site/libraries/tablesorter/addons/pager/jc |
| 489 | 2.747865 | 194.177.214.44 | 192.168.1.3 | HTTP | 59 | HTTP/1.1 404 Not Found (text/html) |
| 494 | 2.754537 | 194.177.214.44 | 192.168.1.3 | HTTP | 256 | HTTP/1.1 404 Not Found (text/html) |
| 502 | 2.782965 | 192.168.1.3 | 194.177.214.44 | HTTP | 558 | GET /sites/ekt-site/libraries/tablesorter/addons/pager/jc |
| 728 | 3.035606 | 194.177.214.44 | 192.168.1.3 | HTTP | 263 | HTTP/1.1 404 Not Found (text/html) |

| Ethernet · 1 | | IPv4 · 1 | | TCP · 3 | | UDP | | | |
|--------------|--------|----------------|--------|---------|-------|---------------|-------------|---------------|-------|
| Address A | Port A | Address B | Port B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes |
| 192.168.1.3 | 11342 | 194.177.214.44 | 80 | 4 | 1757 | 2 | 1163 | 2 | |
| 192.168.1.3 | 11343 | 194.177.214.44 | 80 | 2 | 617 | 1 | 558 | 1 | |
| 192.168.1.3 | 11344 | 194.177.214.44 | 80 | 2 | 821 | 1 | 558 | 1 | |

4. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;

Εφαρμόζω το φίλτρο **http.request.method == "GET"**. Στην συνέχεια επιλέγω **Statistics → Conversations → IPv4** από το μενού και ενεργοποιώ την επιλογή **Limit to display filter**.

Συνολικά στάλθηκαν 4 HTTP Get Requests, τα οποία απευθύνονται στην διεύθυνση 194.177.214.44.



5. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server;

Ο server όπως και ο client τρέχουν την έκδοση HTTP 1.1 όπως φαίνεται και στη παρακάτω εικόνα.

*Wi-Fi 2

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 468 | 2.454556 | 192.168.1.3 | 194.177.214.44 | HTTP | 627 | GET / HTTP/1.1 |
| 477 | 2.525131 | 194.177.214.44 | 192.168.1.3 | HTTP | 338 | HTTP/1.1 304 Not Modified |
| 479 | 2.568928 | 192.168.1.3 | 194.177.214.44 | HTTP | 536 | GET /sites/ekt-site/libraries/tablesorte |
| 480 | 2.576179 | 192.168.1.3 | 194.177.214.44 | HTTP | 558 | GET /sites/ekt-site/libraries/tablesorte |
| 489 | 2.747865 | 194.177.214.44 | 192.168.1.3 | HTTP | 59 | HTTP/1.1 404 Not Found (text/html) |
| 494 | 2.754537 | 194.177.214.44 | 192.168.1.3 | HTTP | 256 | HTTP/1.1 404 Not Found (text/html) |
| 502 | 2.782965 | 192.168.1.3 | 194.177.214.44 | HTTP | 558 | GET /sites/ekt-site/libraries/tablesorte |
| 728 | 3.035606 | 194.177.214.44 | 192.168.1.3 | HTTP | 263 | HTTP/1.1 404 Not Found (text/html) |

> Frame 477: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits) on interface \Device\NPF_{A2FCB102-B16C-4
> Ethernet II, Src: Zte_ce:fb:46 (50:78:b3:ce:fb:46), Dst: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f)
> Internet Protocol Version 4, Src: 194.177.214.44, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 11342, Seq: 303121939, Ack: 2723165378, Len: 284
Hypertext Transfer Protocol
> HTTP/1.1 304 Not Modified\r\n
Date: Wed, 15 Jan 2020 18:54:16 GMT\r\n
Server: Apache/2.4.6 (CentOS)\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=15, max=100\r\n
Etag: "1579111418-1"\r\n
Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
Cache-Control: public, max-age=43200\r\n

0000 18 d6 c7 18 02 2f 50 78 b3 ce fb 46 00 00 45 00/Px ...F..E.
0010 01 44 66 a2 40 00 39 06 7f 88 c2 b1 d6 2c c0 a8 .Df.@.9.,..

Hypertext Transfer Protocol: Protocol
Packets: 4243 · Displayed: 8 (0.2%) · Dropped: 0 (0.0%)
Profile: Default