Ονοματεπώνυμο: Άγγελος Μητροκώτσας		Ομάδα:6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2		Ημερομηνία: 31 /10/ 2021
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC: F8-63-3F-59-24-C8	

Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 Η εντολή arp -a

1.2 Με την εντολή arp -d *

1.3 Με την εντολη ipconfig /all,

IPv4 Address. . . . . : 192.168.1.12(Preferred)

DNS Servers . . . . . : fe80::1%3

192.168.1.1

192.168.1.1

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-91G20CF
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home

Wireless LAN adapter Τοπική σύνδεση* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : F8-63-3F-59-24-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Τοπική σύνδεση* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : FA-63-3F-59-24-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-63-3F-59-24-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Temporary IPv6 Address. . . . . . : 2a02:587:2103:db95:bd93:2779:92af:f3a4(Preferred)
   Temporary IPv6 Address. . . . . . : 2a02:587:2103:db95:fd28:957f:56f7:3fbb(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c161:5c8:9f00:b45b%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Σάββατο, 30 Οκτωβρίου 2021 3:49:12 μμ
   Lease Expires . . . . . . . . . . : Δευτέρα, 1 Νοεμβρίου 2021 1:06:48 μμ
   Default Gateway . . . . . . . . . : fe80::1%3
                                       192.168.1.1
```

```
   DNS Suffix Search List. . . . . : home

Wireless LAN adapter Τοπική σύνδεση* 1:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . : F8-63-3F-59-24-C9
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Τοπική σύνδεση* 2:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . : FA-63-3F-59-24-C8
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . : F8-63-3F-59-24-C8
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:bd93:2779:92af:f3a4(Preferred)
   Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:fd28:957f:56f7:3fbb(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c161:5c8:9f00:b45b%3(Preferred)
   IPv4 Address. . . . . : 192.168.1.12(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Lease Obtained. . . . . : Σάββατο, 30 Οκτωβρίου 2021 3:49:12 μμ
   Lease Expires . . . . . : Δευτέρα, 1 Νοεμβρίου 2021 1:06:48 μμ
   Default Gateway . . . . . : fe80::1%3
                               192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . : 66609983
   DHCPv6 Client DUID. . . . . : 00-01-00-01-27-47-6E-E2-F8-63-3F-59-24-C8
   DNS Servers . . . . . : fe80::1%3
                               192.168.1.1
                               192.168.1.1
   NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>
```

1.4

```
C:\Windows\system32>arp -a

Interface: 192.168.1.12 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           38-02-de-f7-d3-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>
```

1.5 Τα DNS resolves εκτελούνται από την προκαθορισμένη πυλη. Υπάρχει η διεύθυνση της προκαθορισμένης πύλης (default gateway) και οχι του DNS εξυπηρετητη (όπως φαίνεται στο αποτέλεσμα της ipconfig /all πανω, ταυτιζονται οι 2 διευθύνσεις).

1.6 C:\Windows\system32>arp -d *

C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

```
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 4ms
```

1.7 C:\Windows\system32>arp -a

```
Interface: 192.168.1.12 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           38-02-de-f7-d3-40     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Παρατηρώ ότι υπάρχουν λιγότερες διευθύνσεις στον πινακα

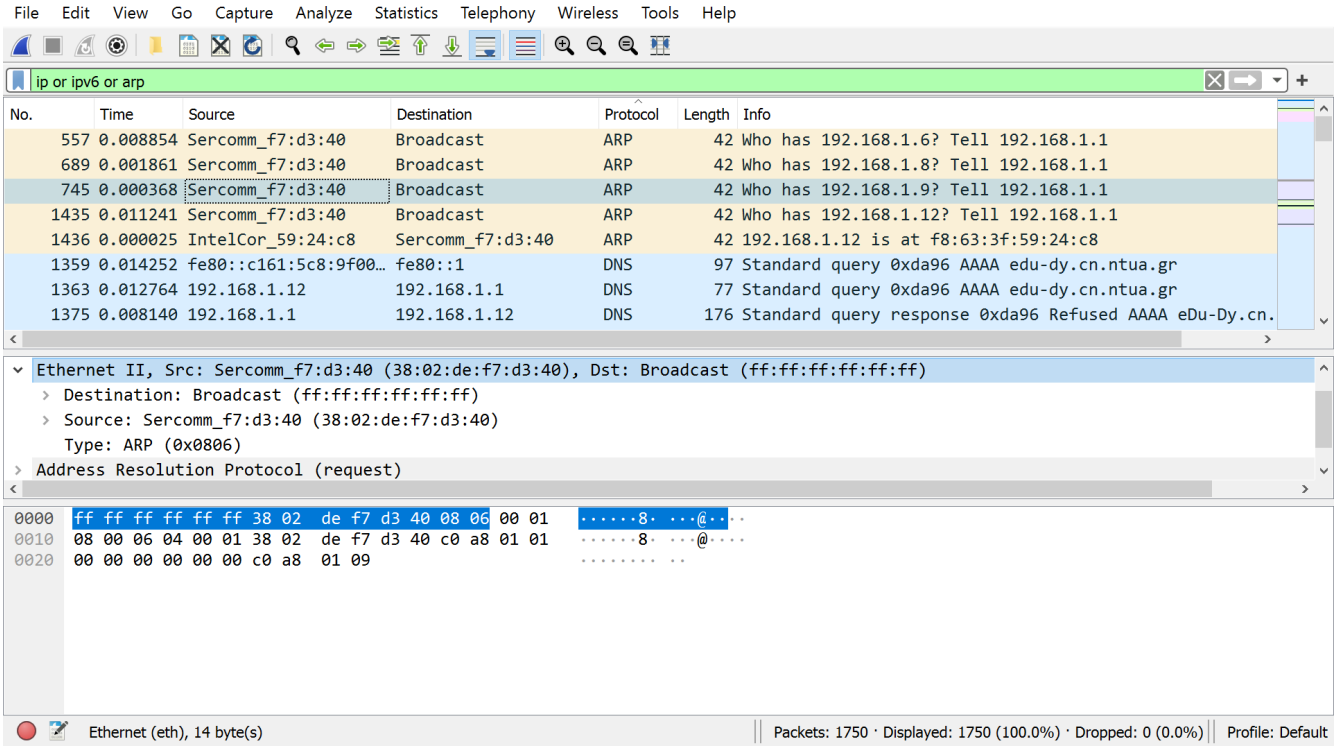
1.8

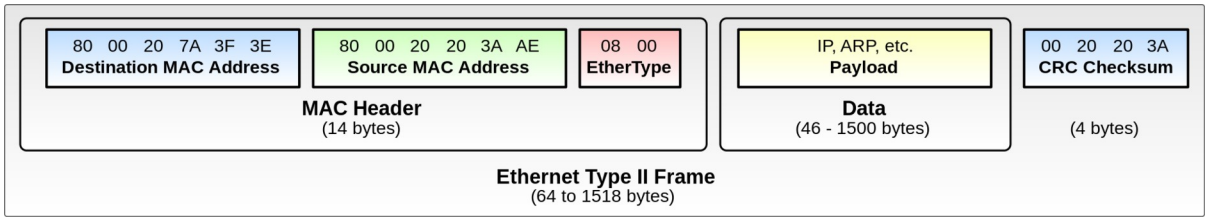
```
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>arp -d *

C:\Windows\system32>arp -a

Interface: 192.168.1.12 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           38-02-de-f7-d3-40     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

1.9 Όχι, είναι σε διαφορετικό υποδικτυο

Άσκηση 2

2.1 Το πεδία Source, Destination και Type





2.2 Το προοιμιο δεν καταγραφεται από το wireshark γιατι δεν είναι μέρος του πλαισιου ethernet. (Τα πρώτα 56 bit του προοιμίου είναι εναλλαγές του 1 και του 0 για να επιτευχθεί συγχρονισμός. Χρησιμεύουν ώστε τα ηλεκτρονικά στοιχεία να προλάβουν να ανιχνεύσουν την ύπαρξη σήματος και να αρχίσουν να διαβάζουν προτού αρχίσει η μετάδοση του πλαισίου. Τα επόμενα 8 bit είναι και υποδεικνύουν την αρχή του πλαισίου)

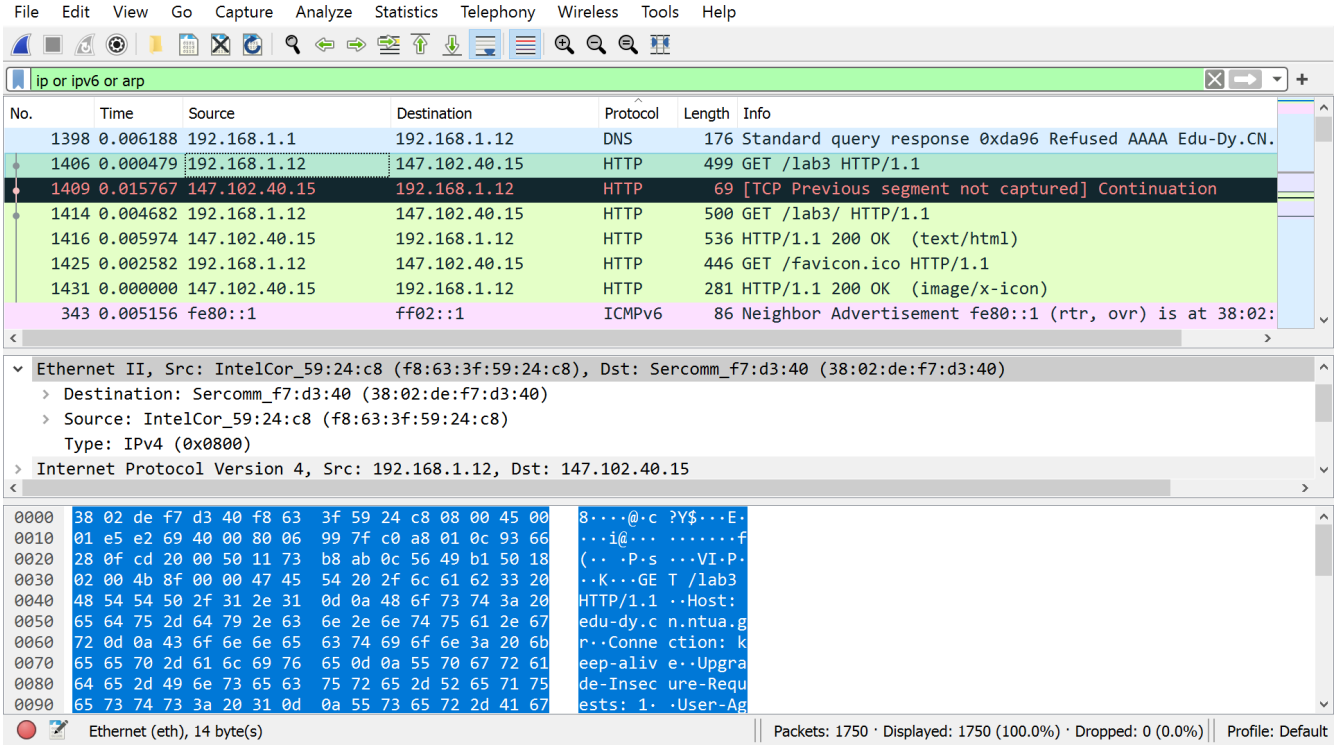
2.3 Το wireshark δεν μπορει να καταγραψει πακέτα τύπου CRC. Γι' αυτό ευθύνεται το λειτουργικό μας σύστημα καθώς και οι βιβλιοθήκες που χρησιμοποιεί η εφαρμογή, οι οποίες χρειάζονται μετατροπές για να το πετύχουν

2.4 0x0800
2.5 0x0806

2.6 0x86dd

2.7 f8:63:3f:59:24:c8

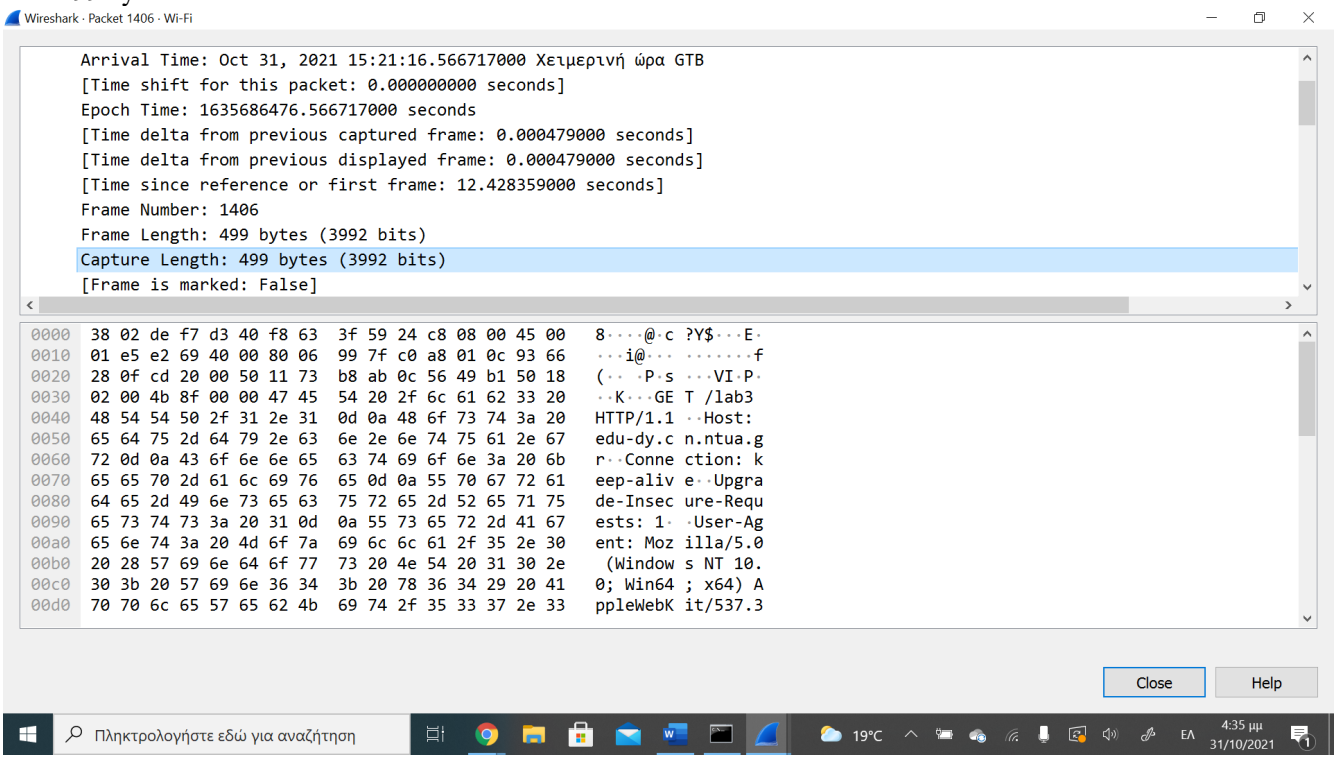
2.8 38:02:de:f7:d3:40



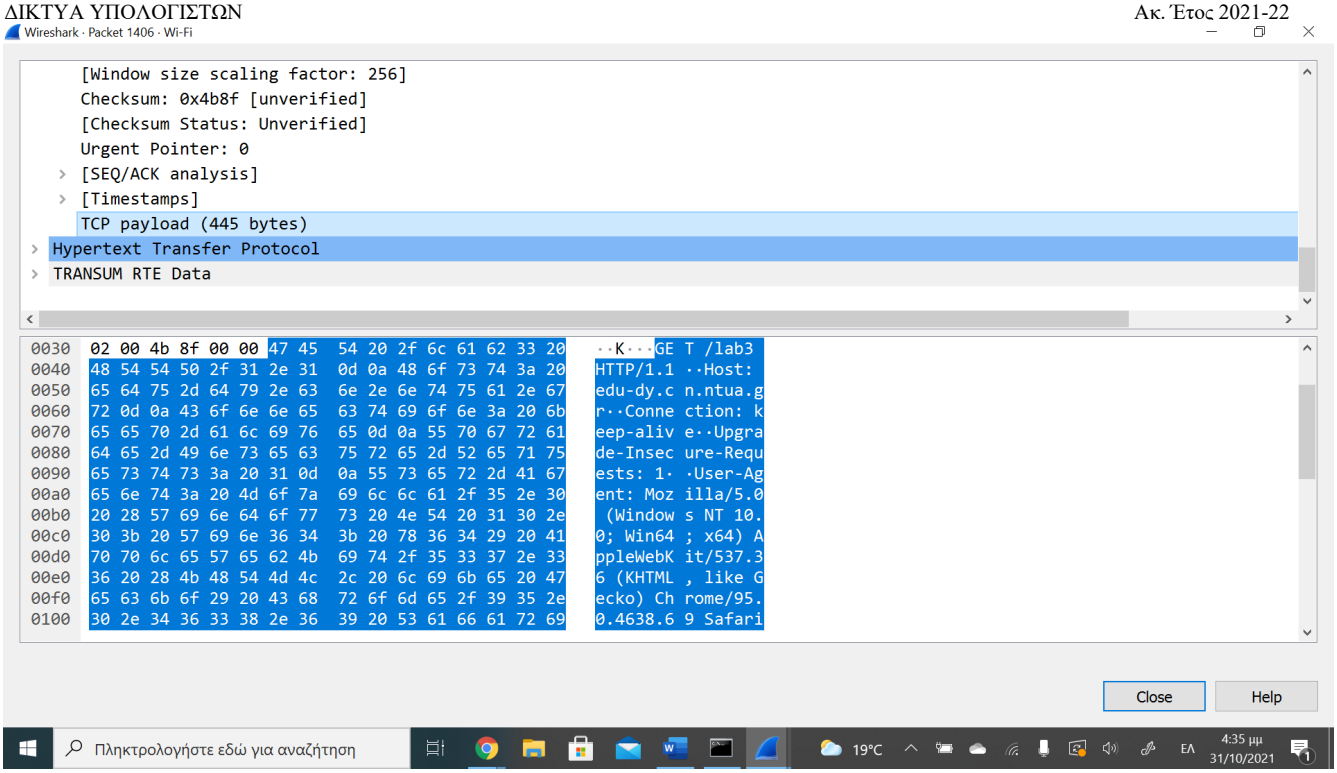
2.9 Όχι

2.10 Η διευθυνση αυτου του ιστότοπου είναι σε διαφορετικό δίκτυο από το τοπικό μου δίκτυο. Η παραπανω MAC διεύθυνση ανήκει στην προκαθορισμένη πύλη (default gateway), γιατί μεσω αυτής στέλνονται τα πακέτα και γίνεται η επικοινωνια.

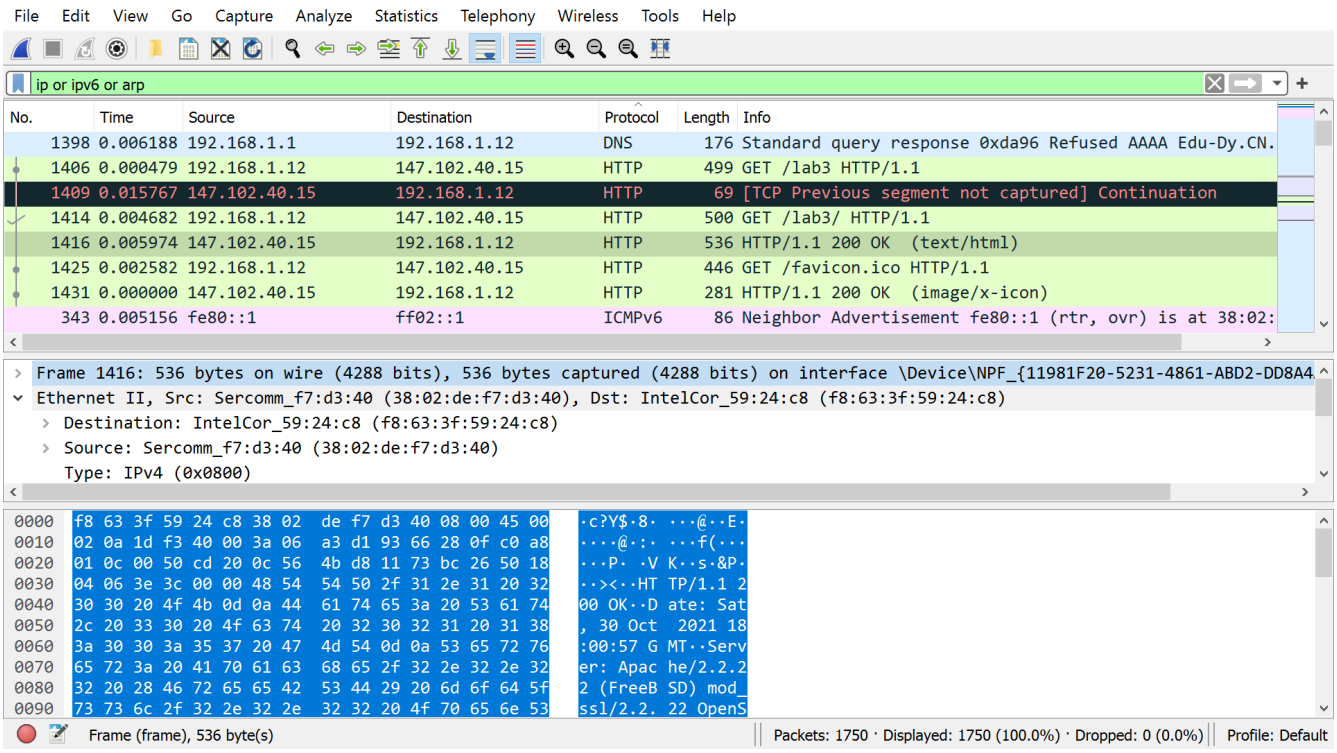
2.11 499 bytes



2.12 499 – TCP payload = 44bytes



2.13 38:02:de:f7:d3:40



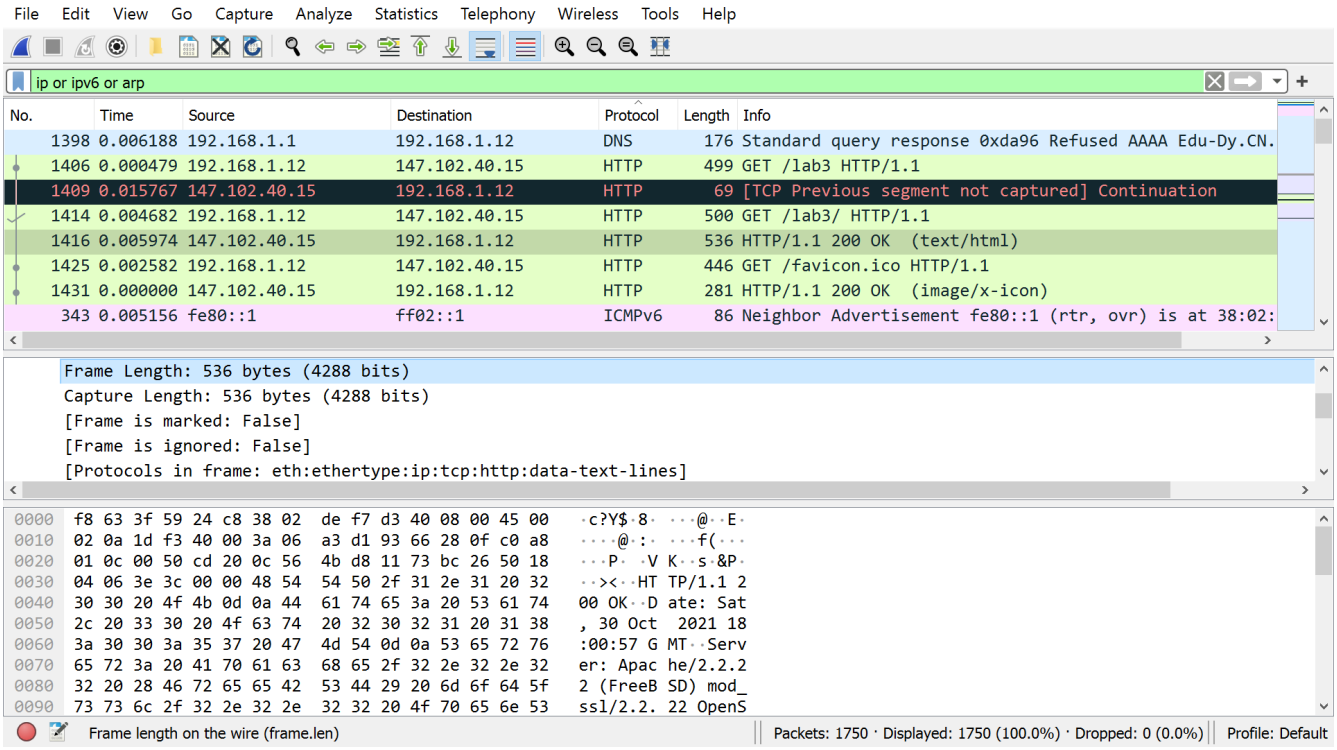
2.14 Όχι

2.15 Στο router του δικτύου στο οποίο βρίσκομαι.

2.16 f8:63:3f:59:24:c8

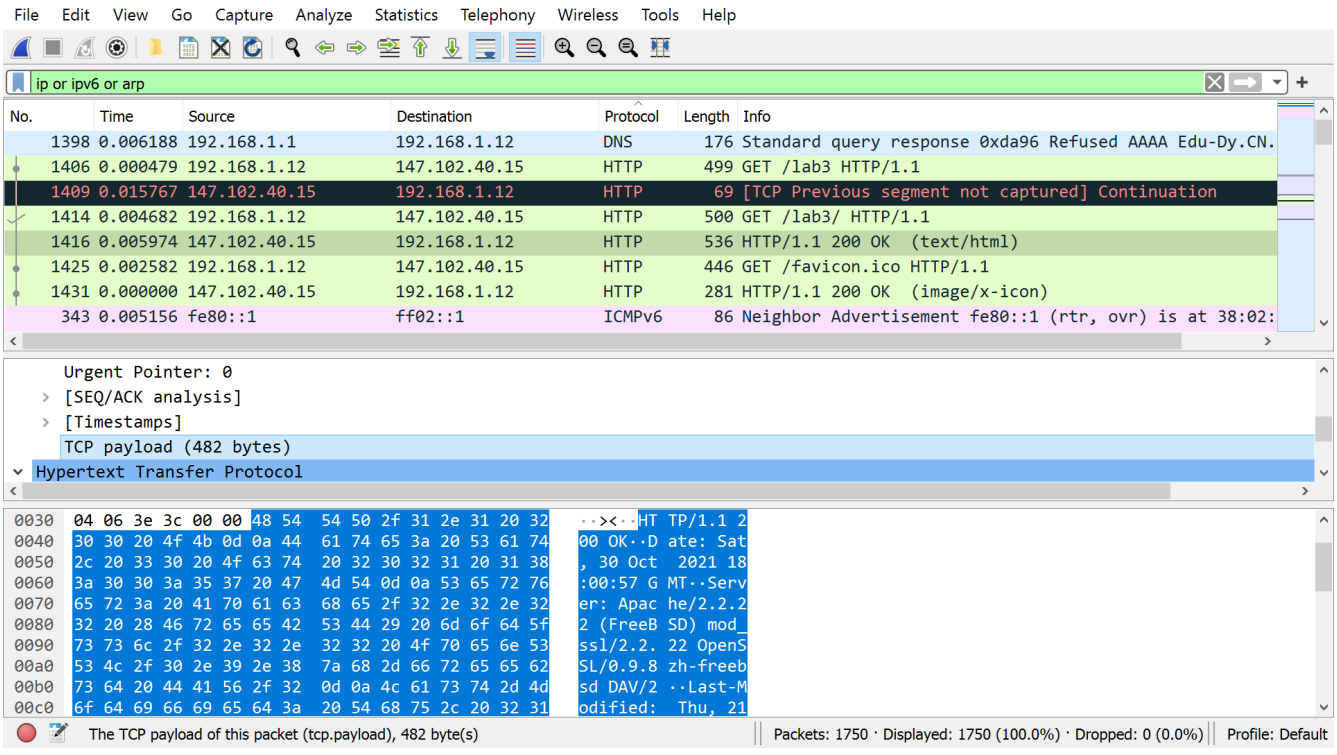
2.17 Ανήκει στον δικό μου υπολογιστή

2.18 536 bytes



2.19

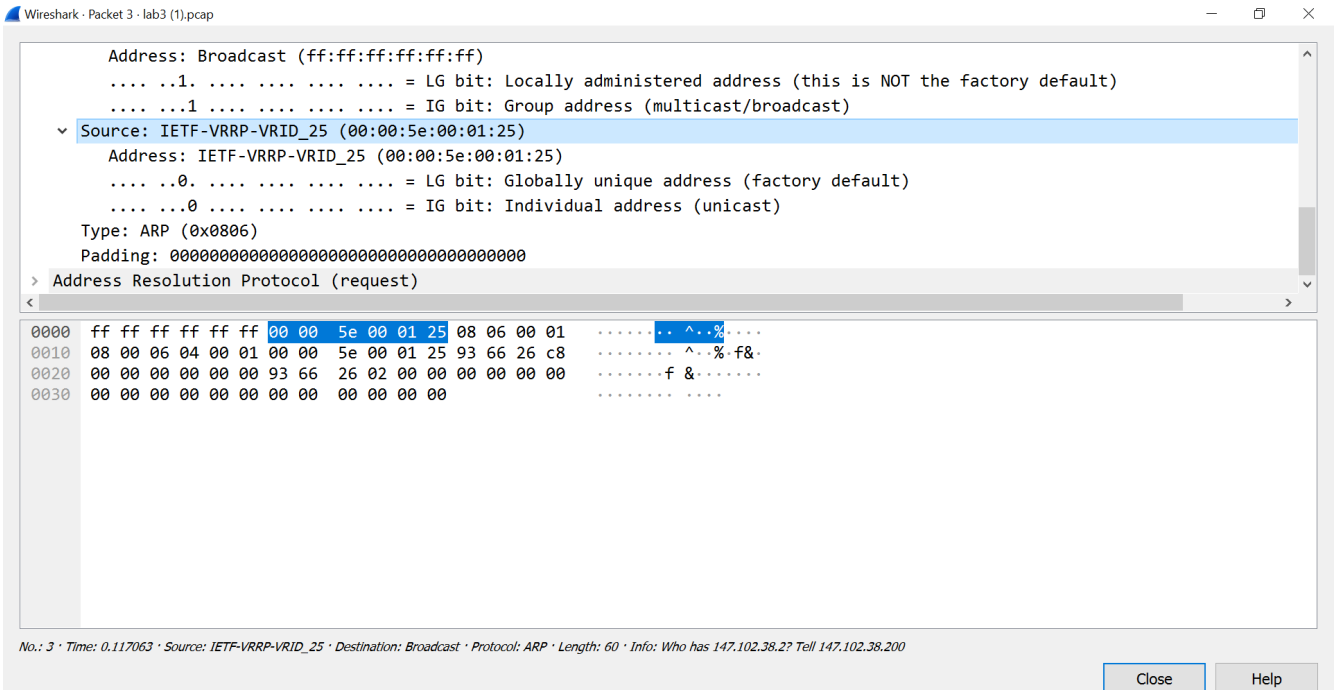
536 – 482 = 54bytes



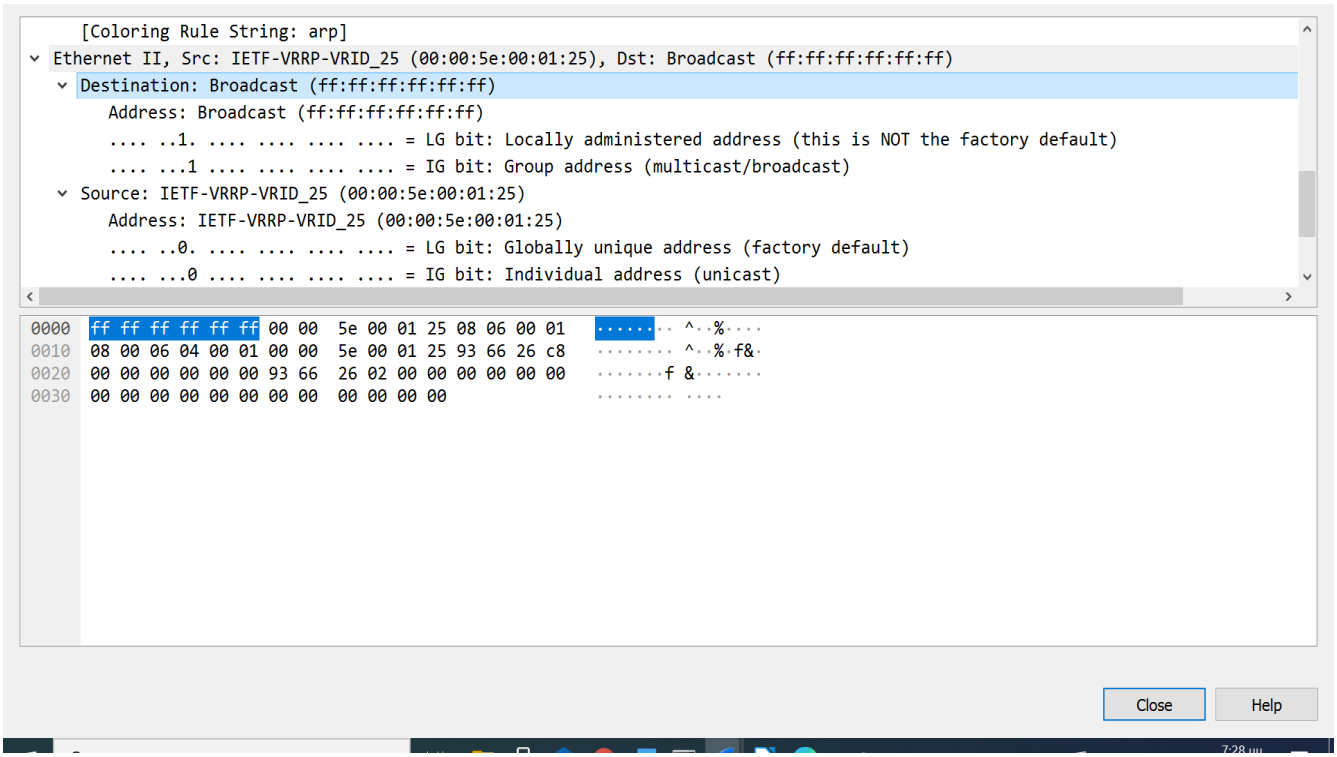
Άσκηση 3

(χρησιμοποίησα το αρχείο που κατέβασα)

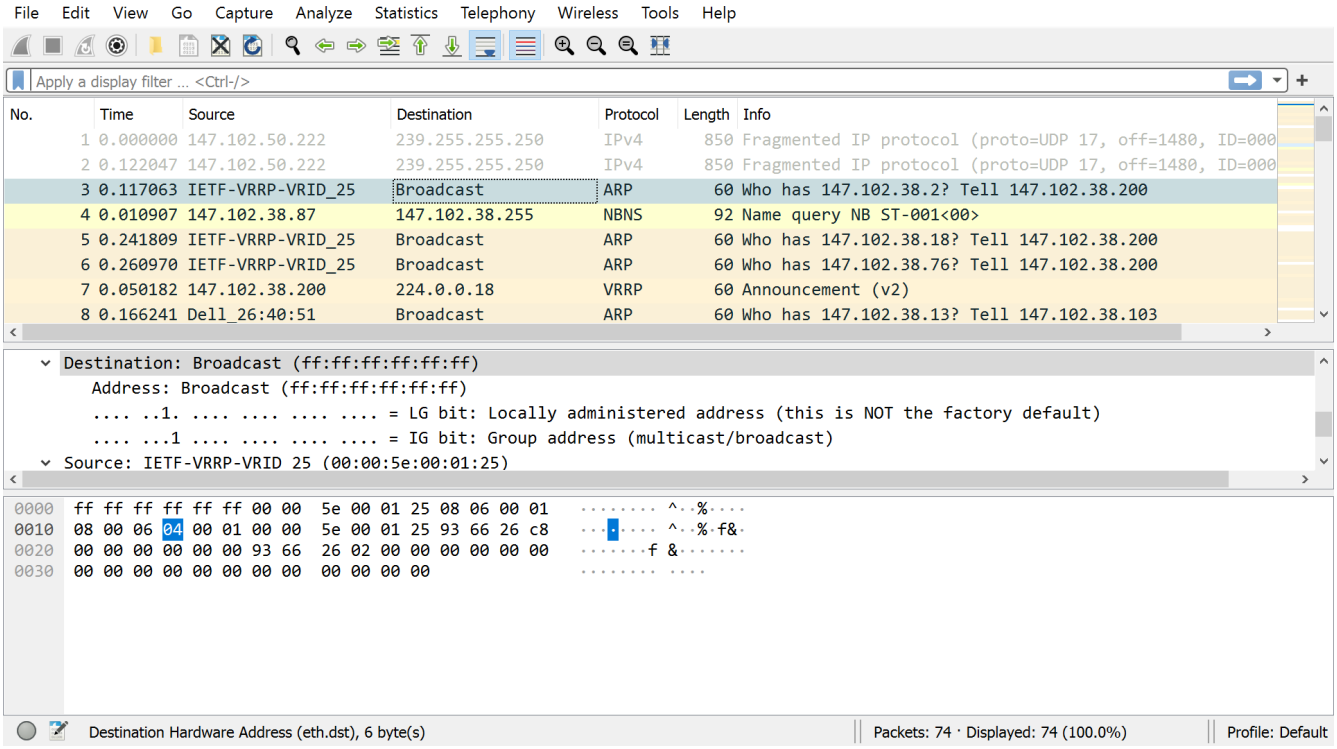
3.1 Το 2ο byte είναι 0 άρα καταγράψαμε **μοναδικές** διευθύνσεις MAC πηγής και το 2ο LSB είναι 0 άρα καταγράψαμε **ατομικές** διευθύνσεις MAC πηγής.



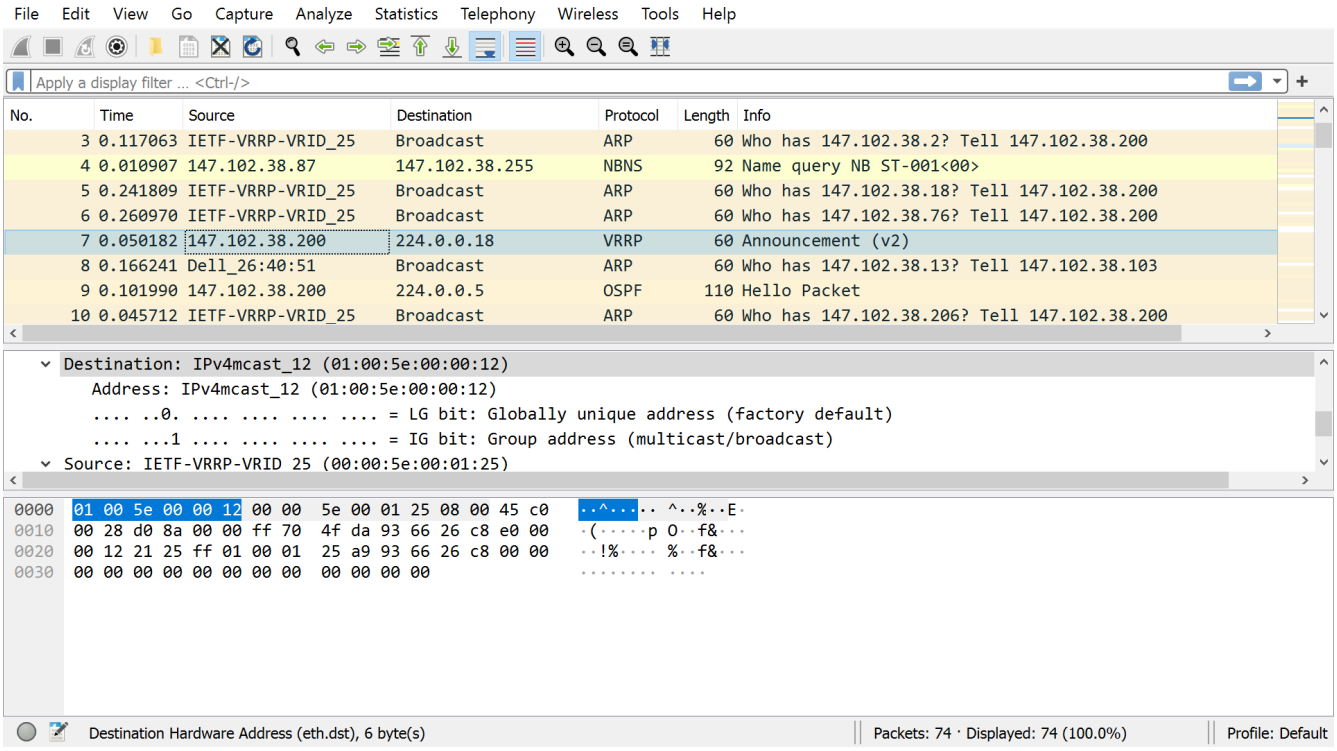
3.2 Το 2ο byte είναι 1 άρα καταγράψαμε **τοπικές** διευθύνσεις MAC προορισμού (κάποιες) και το 2ο LSB είναι 1 άρα καταγράψαμε **ομαδικές** διευθύνσεις MAC προορισμού.



Πρόκειται βασικα για broadcasting, καθώς οι διευθύνσεις MAC προορισμού αποτελούνται μόνο από 1 (το γράφει κιολας)



(Υπάρχει και μοναδική και ομαδική διεύθυνση MAC προορισμού σε κάποια πλαίσια:

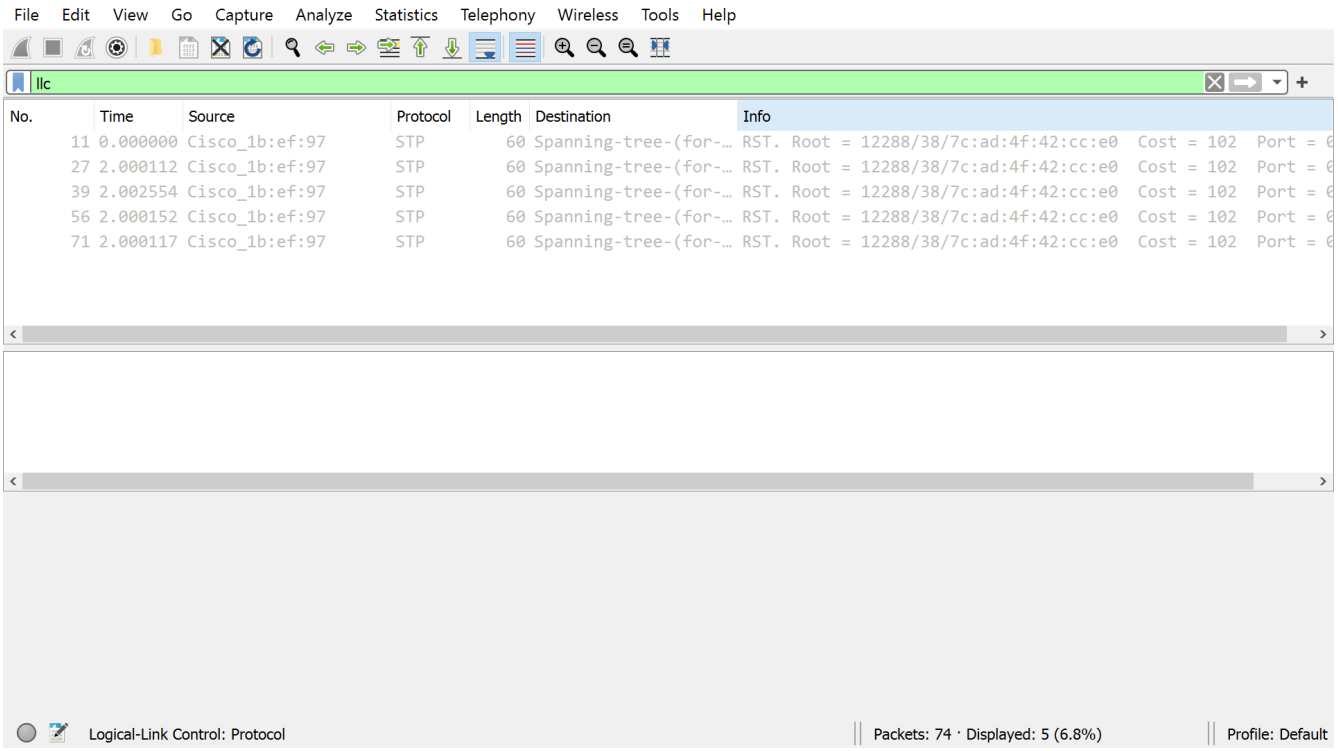


)

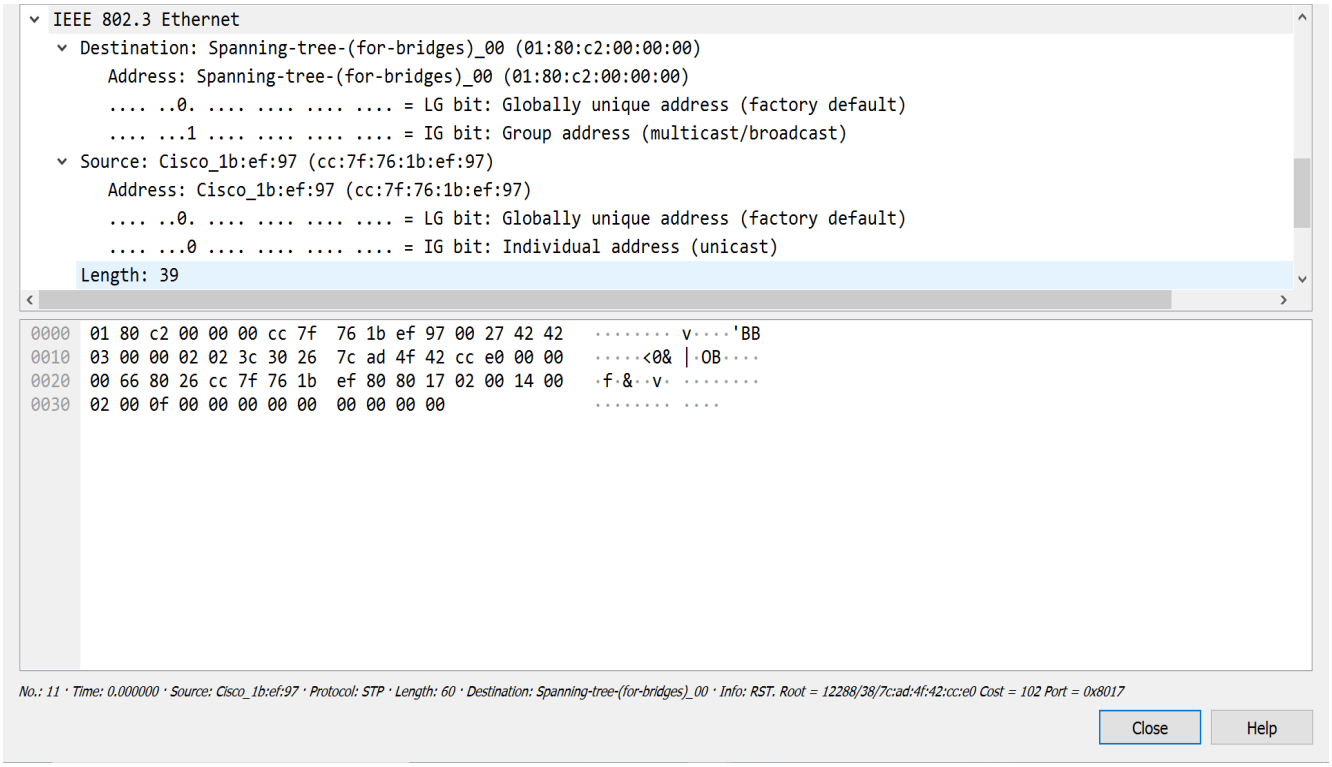
3.3 Εμφανίζεται στο LSB του 1ου byte (1ο απ'τα αριστερά)

3.4 Προορισμού: ff:ff:ff:ff:ff, Πηγής: 00:00:5e:00:01:25

3.5 Παραμένουν πλαίσια με πρωτόκολλο STP:

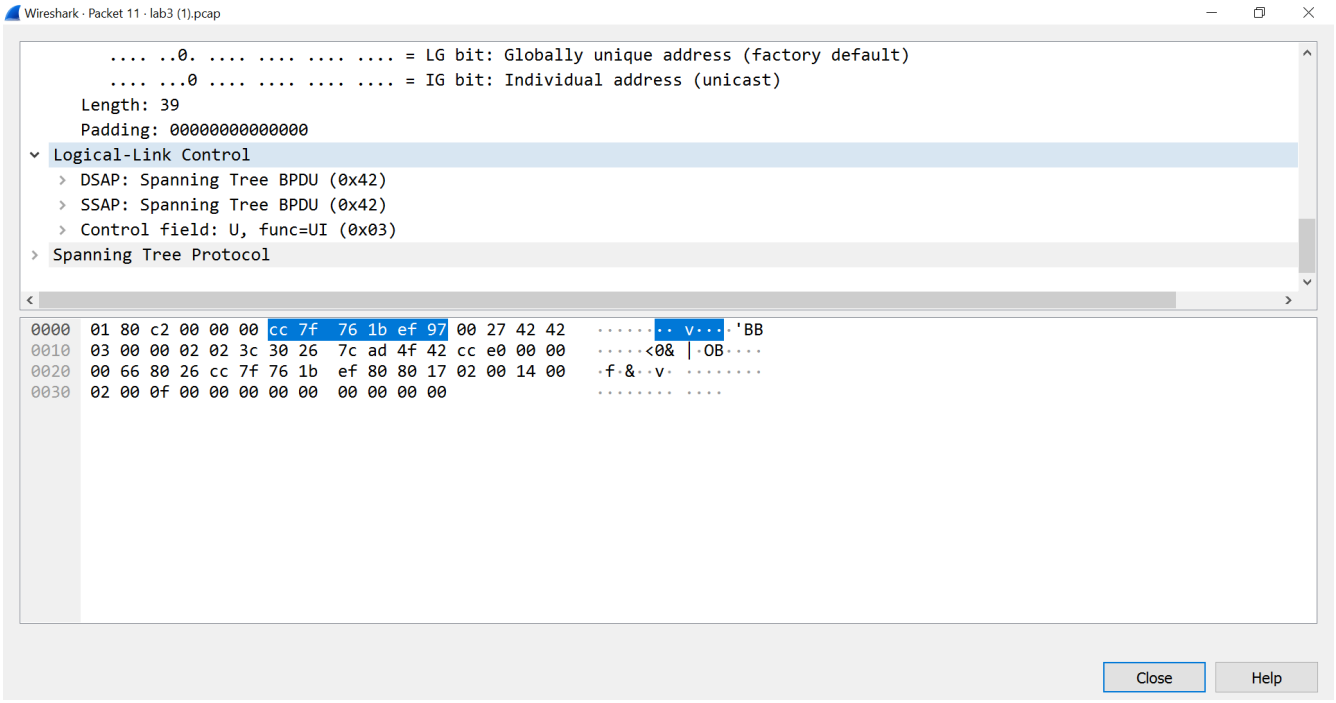


3.6 Δηλώνει το μήκος των δεδομένων (είναι το πεδίο length)

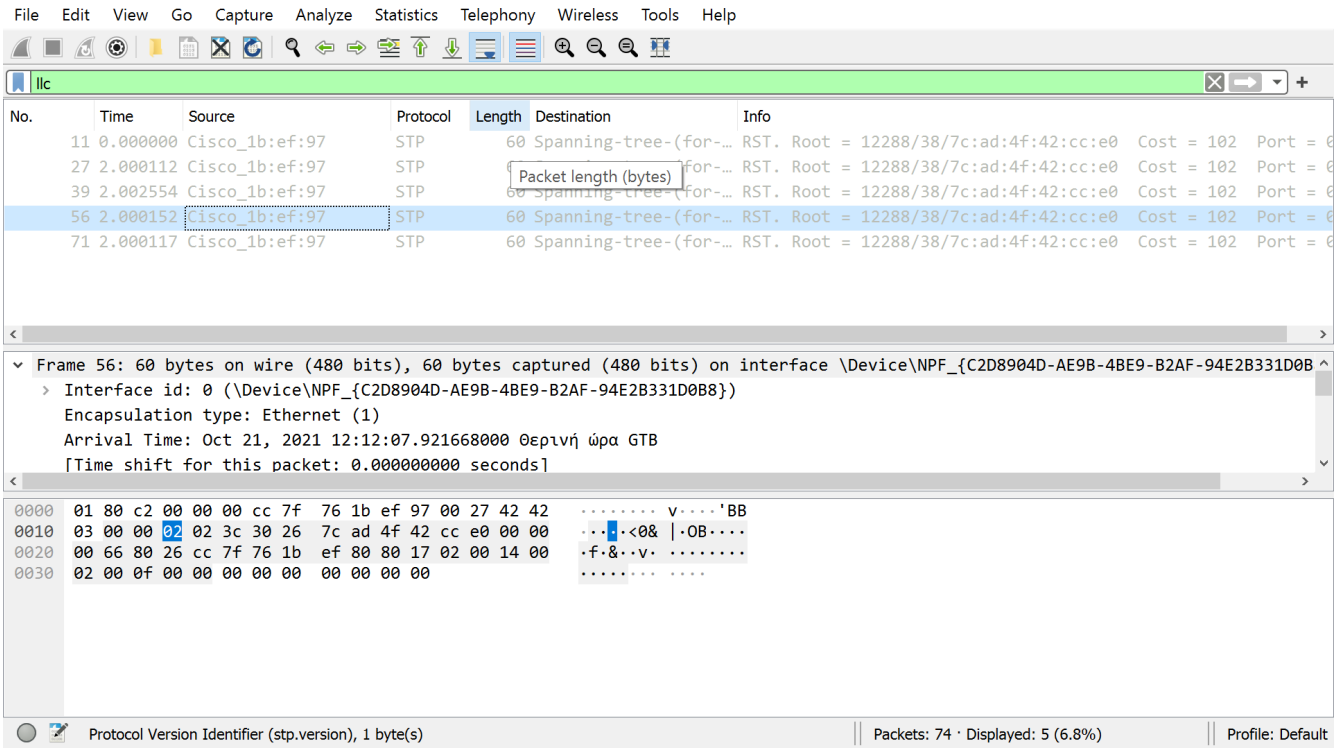


3.7 Το πεδίο Type έχει τιμή <=1500 για τα πλαίσια Ethernet IEEE802.3 ενώ για τα πλαίσια Ethernet II έχει την τιμή 1536.

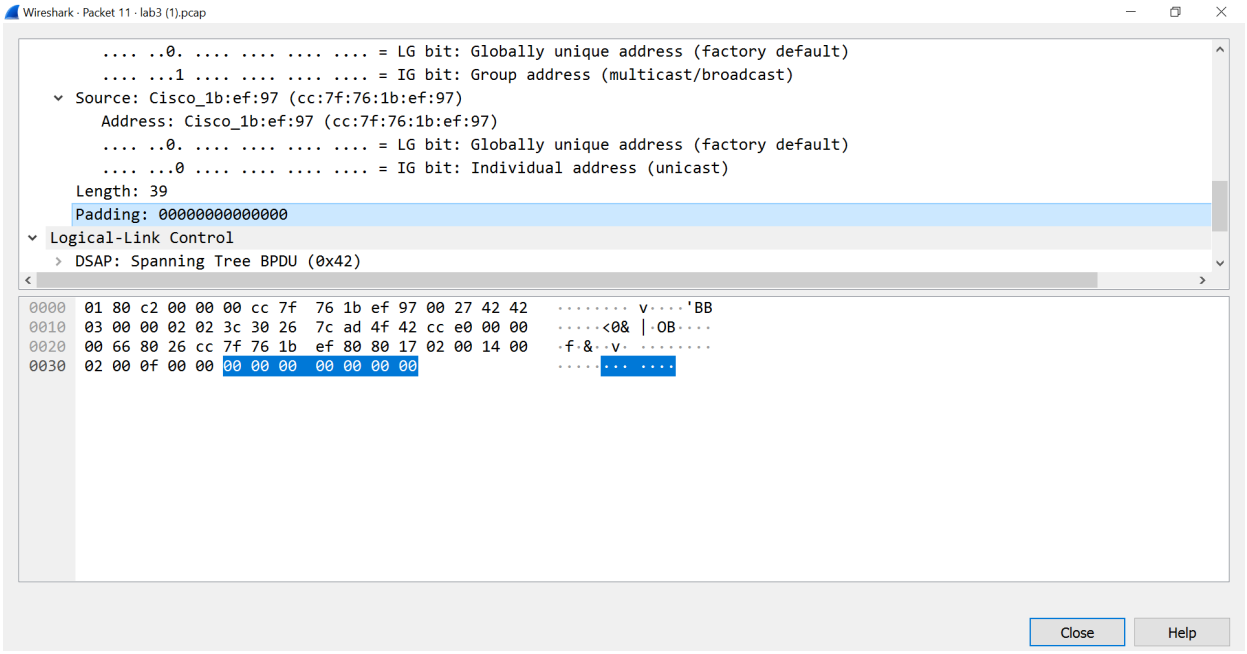
3.8 Μέγεθος: 3 byte. Περιέχει τα πεδία DSAP, SSAP, Control field



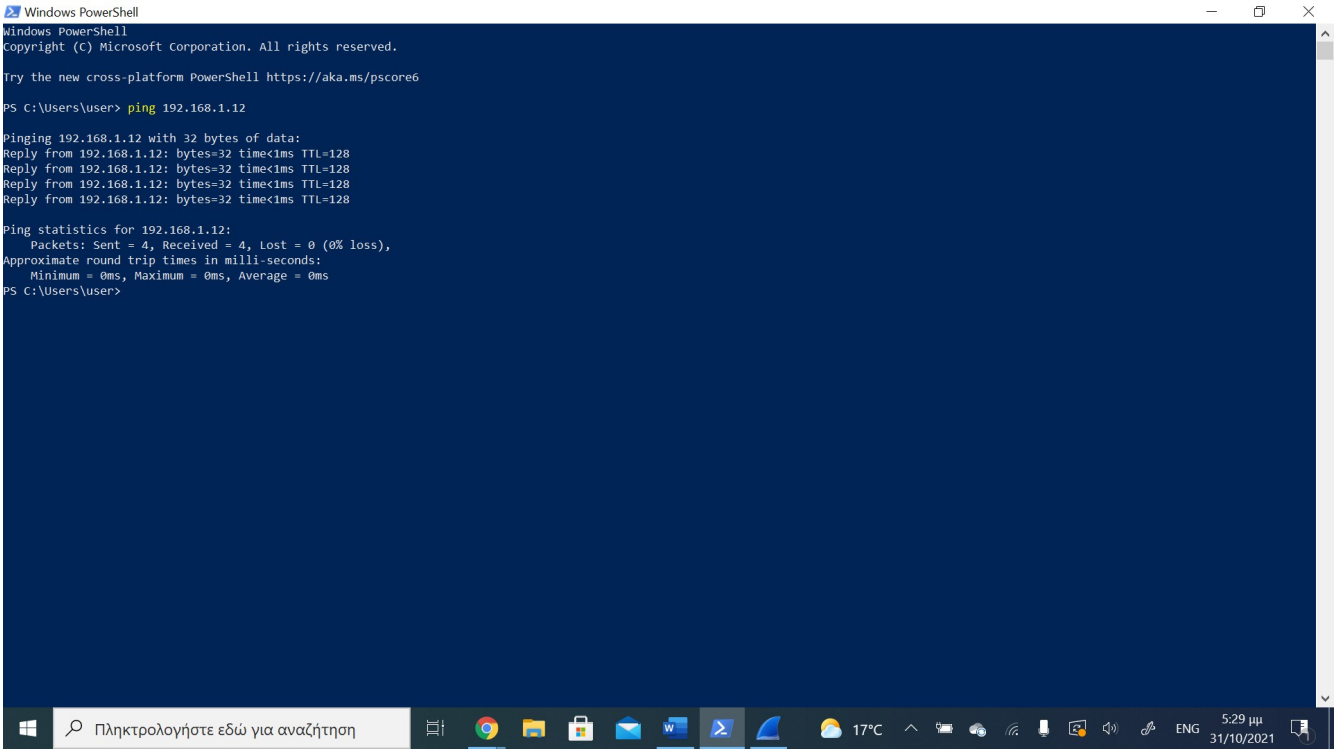
3.9 Μεταφέρου δεδομένα πρωτοκόλλου STP και όλα έχουν μέγεθος 60 bytes



3.10 7 bytes



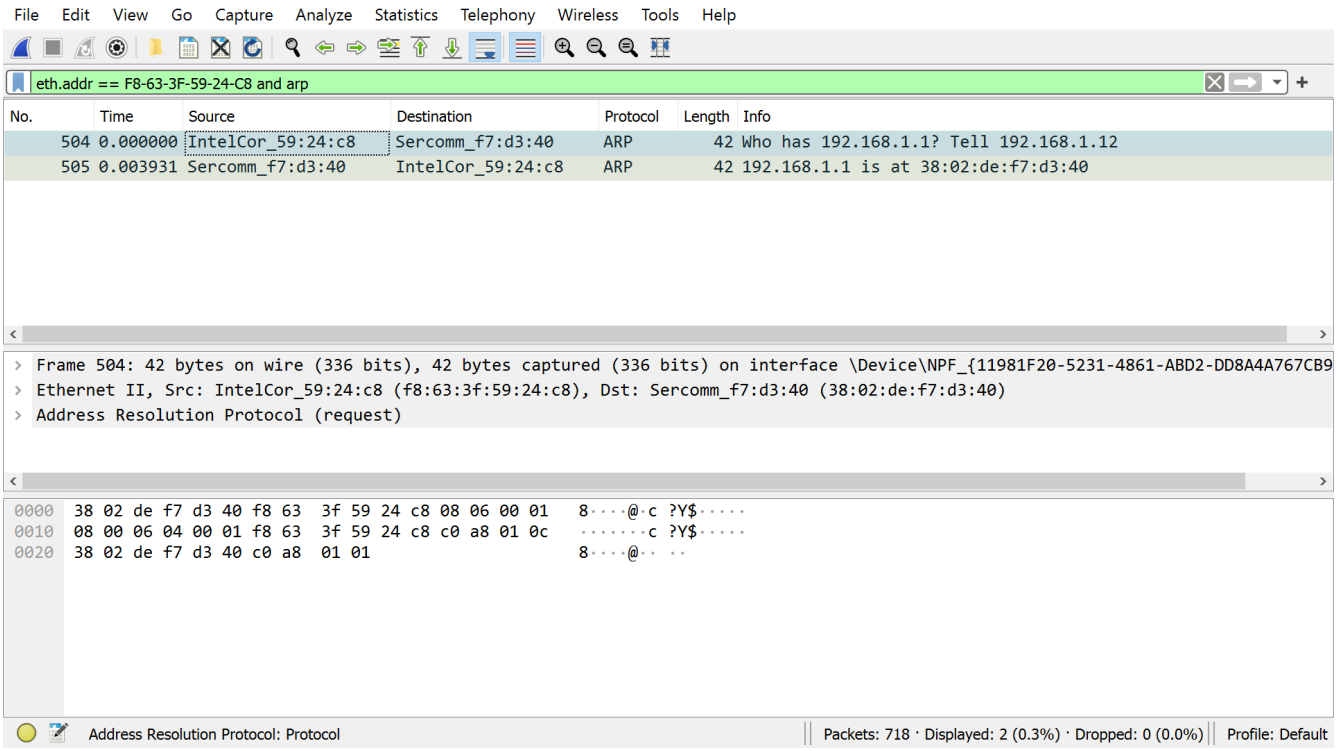
Άσκηση 4



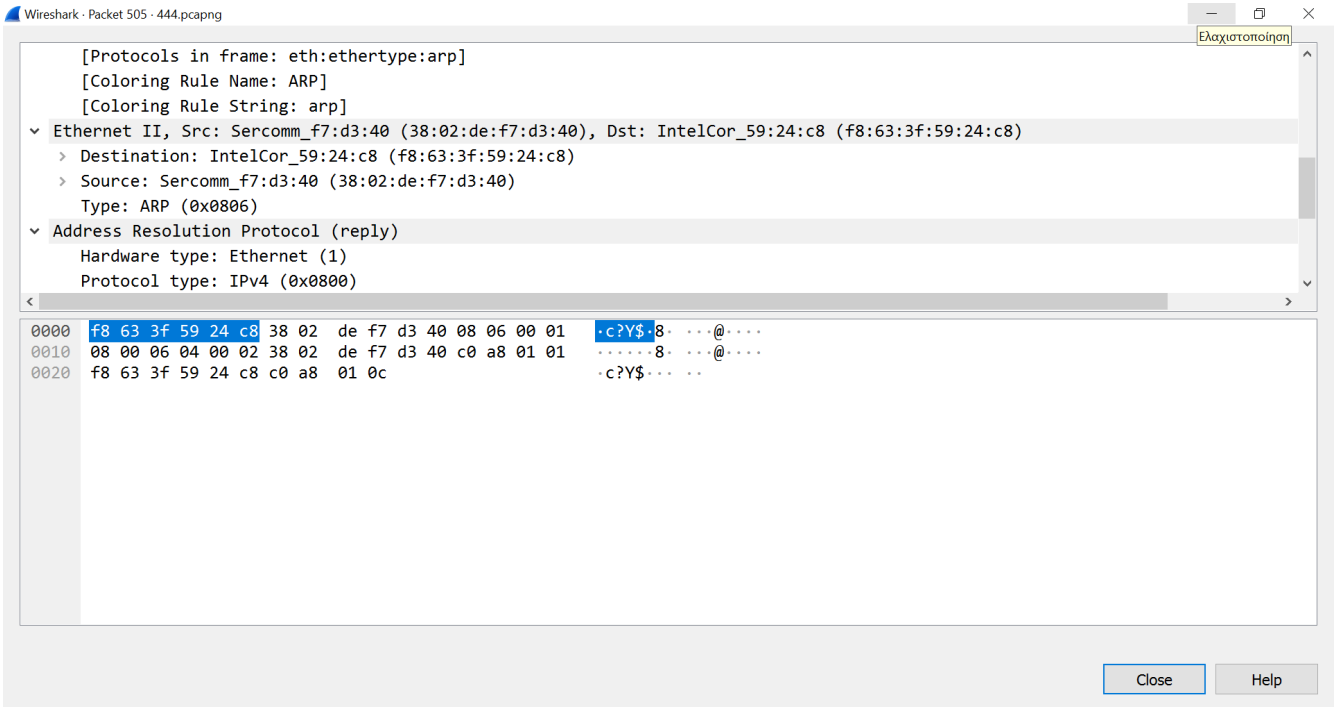
4.1 Απεικονίζει όλα τα πλαίσια που έχουν destination ή source την MAC address που έβαλα στο φίλτρο.

4.2 Απεικονίζει μονο τα πακέτα με πρωτόκολλο ARP που έχουν destination ή source την MAC address που έβαλα στο φίλτρο

4.3 Δύο


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eth.addr == F8-63-3F-59-24-C8 and arp
No. Time Source Destination Protocol Length Info
504 0.000000 IntelCor_59:24:c8 Sercomm_f7:d3:40 ARP 42 Who has 192.168.1.1? Tell 192.168.1.12
505 0.003931 Sercomm_f7:d3:40 IntelCor_59:24:c8 ARP 42 192.168.1.1 is at 38:02:de:f7:d3:40
Frame 504: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB9
Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Address Resolution Protocol (request)
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c
0020 38 02 de f7 d3 40 c0 a8 01 01
Address Resolution Protocol: Protocol
Packets: 718 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%)
Profile: Default

4..4



4.5

Hardware Type: Ethernet(1) :3 bytes

Hardware Size: 6 : 1 byte

Protocol Type: 2 bytes

Protocol Size: 4 : 1 byte

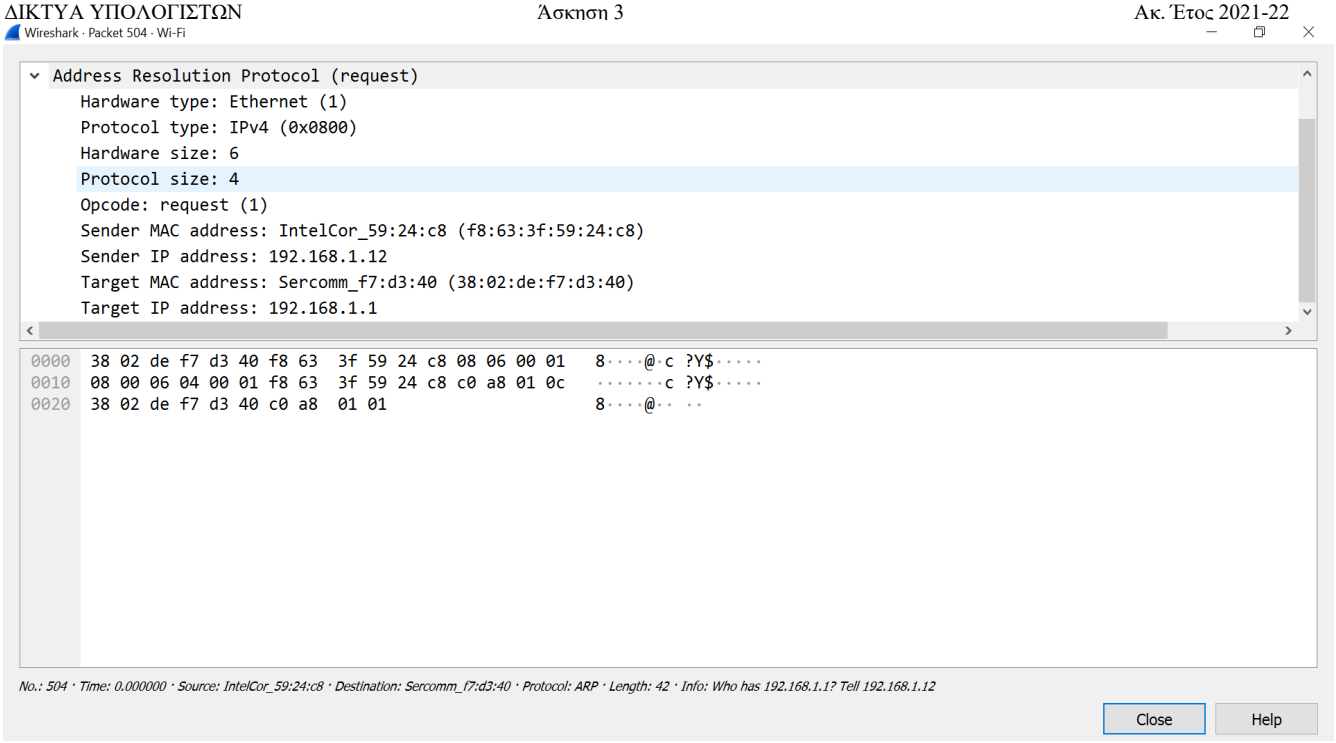
Opcode: request(1) : 2 bytes

Sender MAC Address: 6 bytes

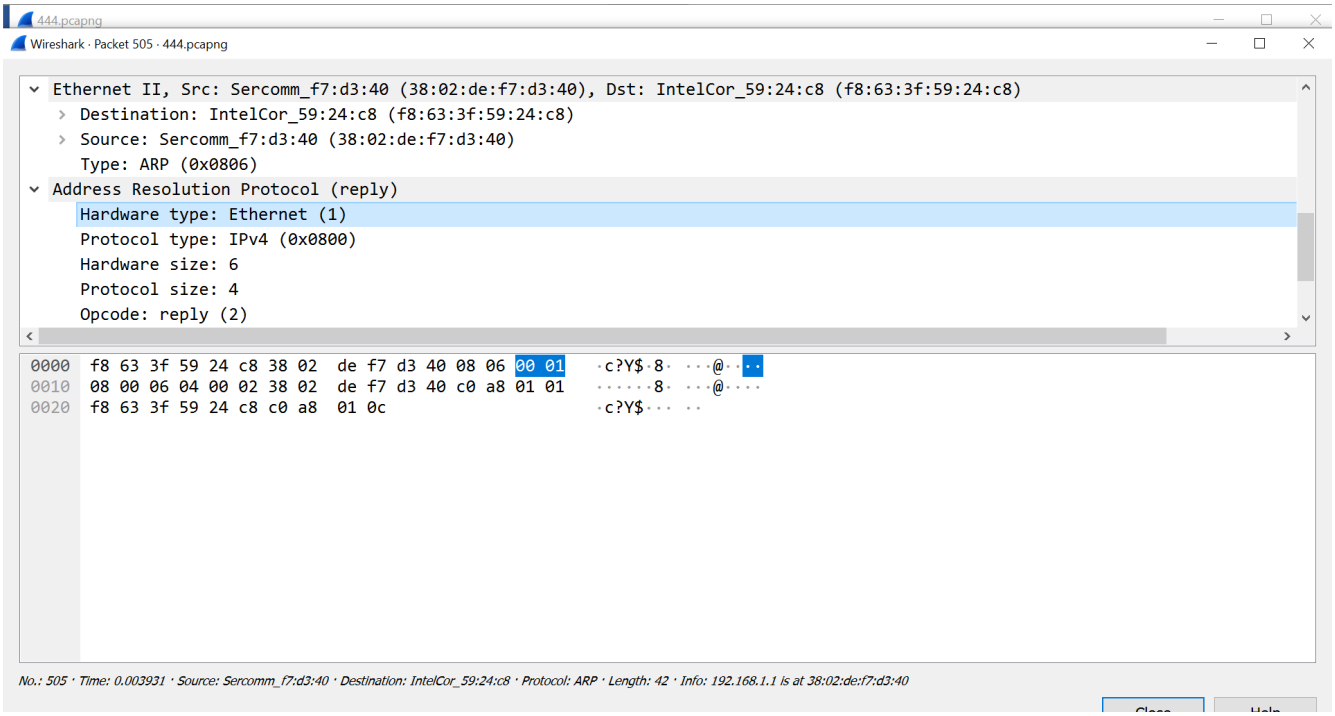
Target MAC Address: 6 bytes

Sender IP Address: 4 bytes

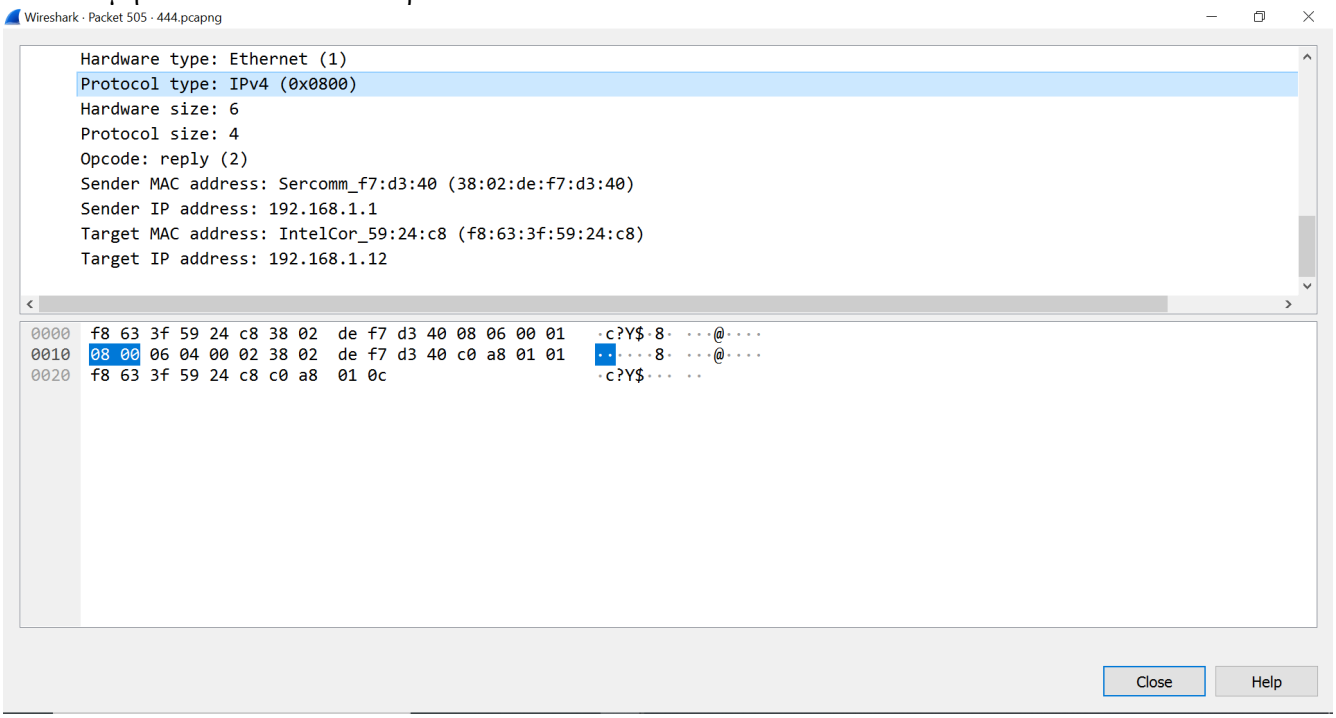
Target IP Address: 4 bytes



4.6 Τιμή: 0001 . Υποδεικνύει ότι η μεταφορά του πλαισίου γίνεται μεσω Ethernet.



4.7 Τιμή: 0800. Υποδεικνύε:ι πρωτόκολλο IPv4.

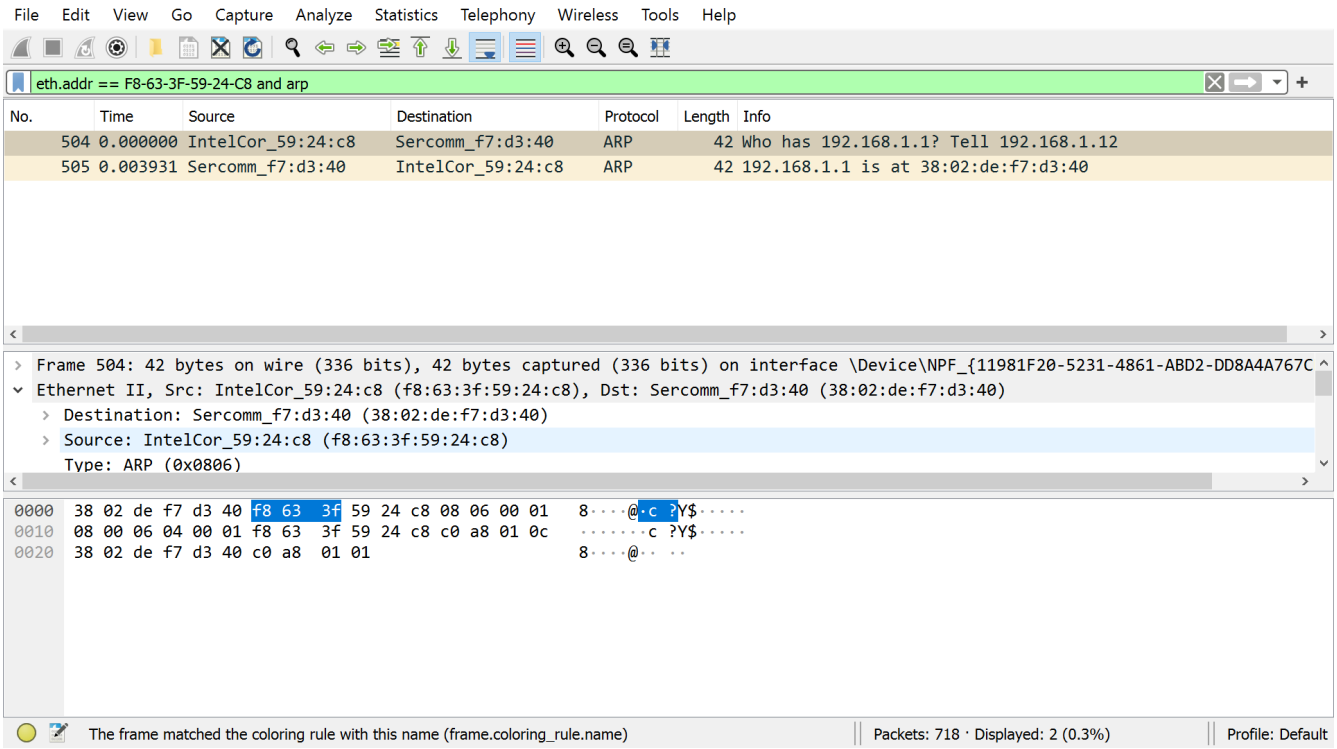


4.8 Εχουν ίδιο μήκος (2 bytes) και η τιμή του Protocol Type (η 16δική) αντιστοιχεί σε κάποιο EtherType

4.9 Δηλώνει το μέγεθος της διεύθυνσης του πρωτόκολλου IPv4, το οποιο είναι 4 bytes

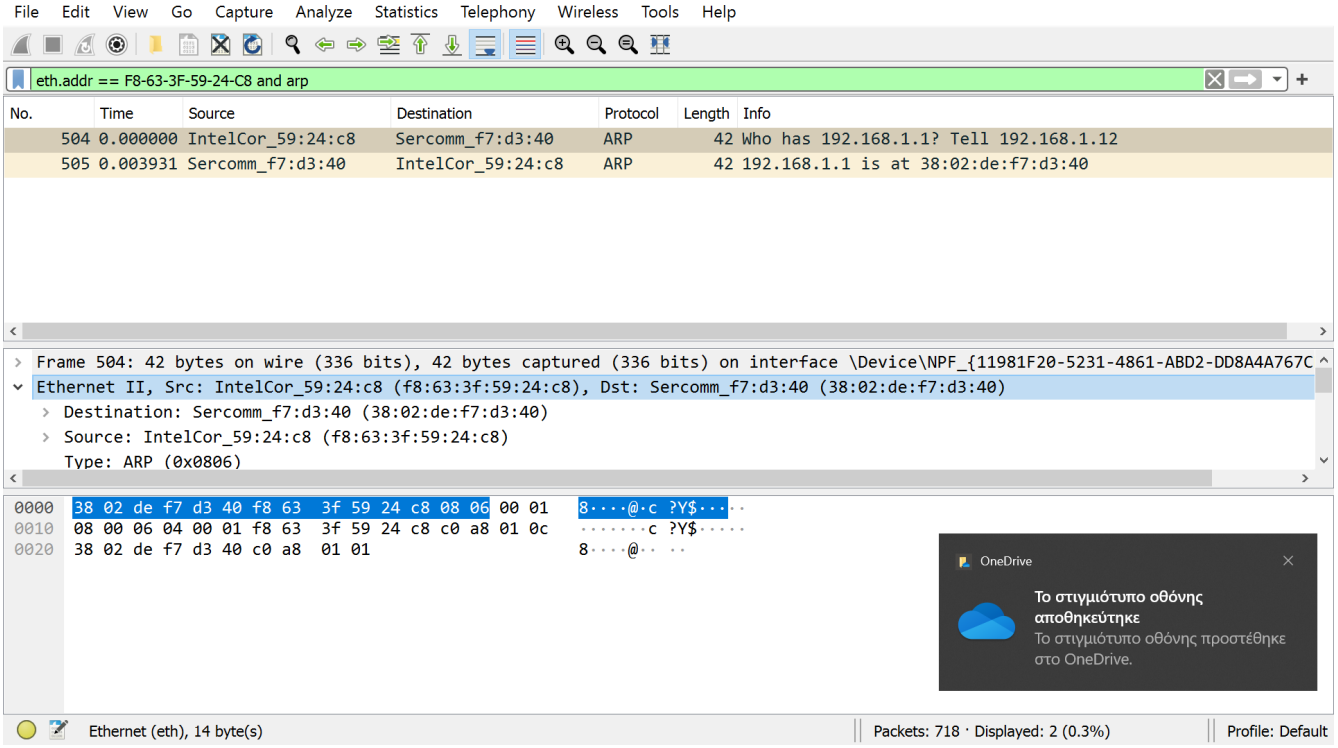
4.10 Δηλώνει το μέγεθος της διεύθυνσης MAC, το οποίο είναι 6 bytes.

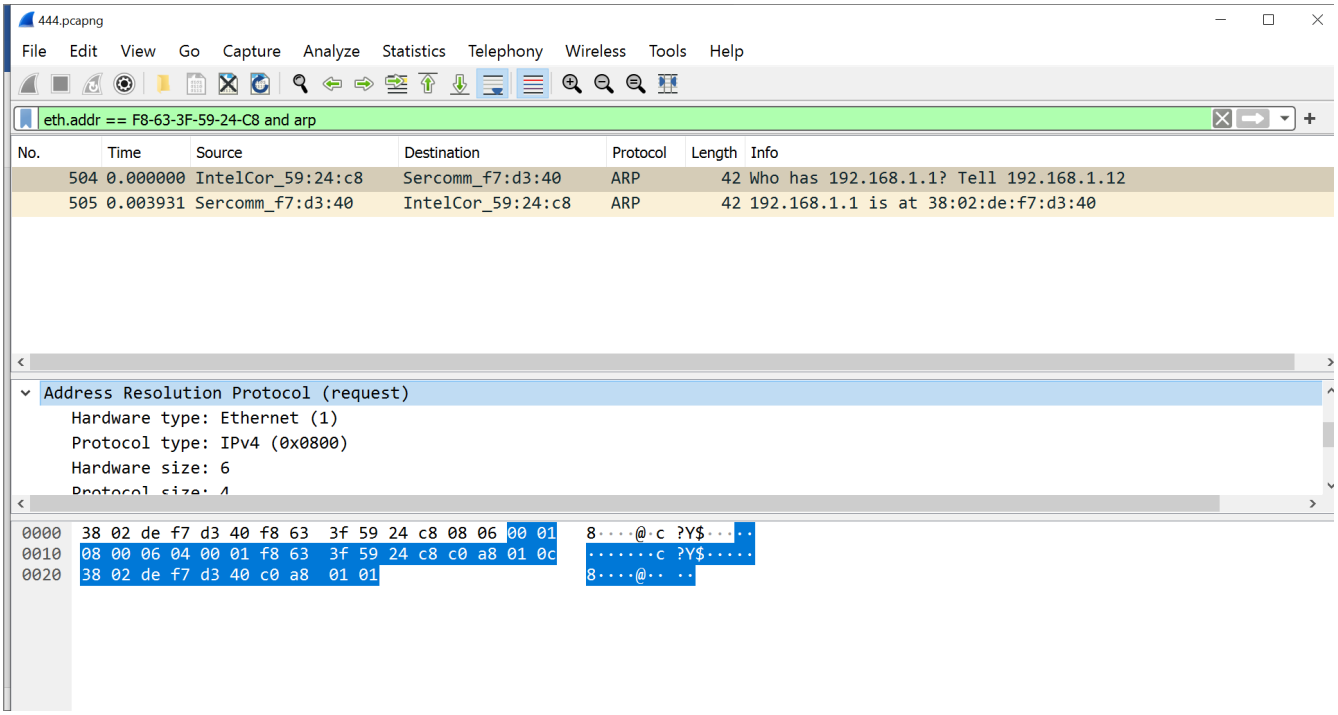
4.11 Ανήκει στον υπολογιστή μου



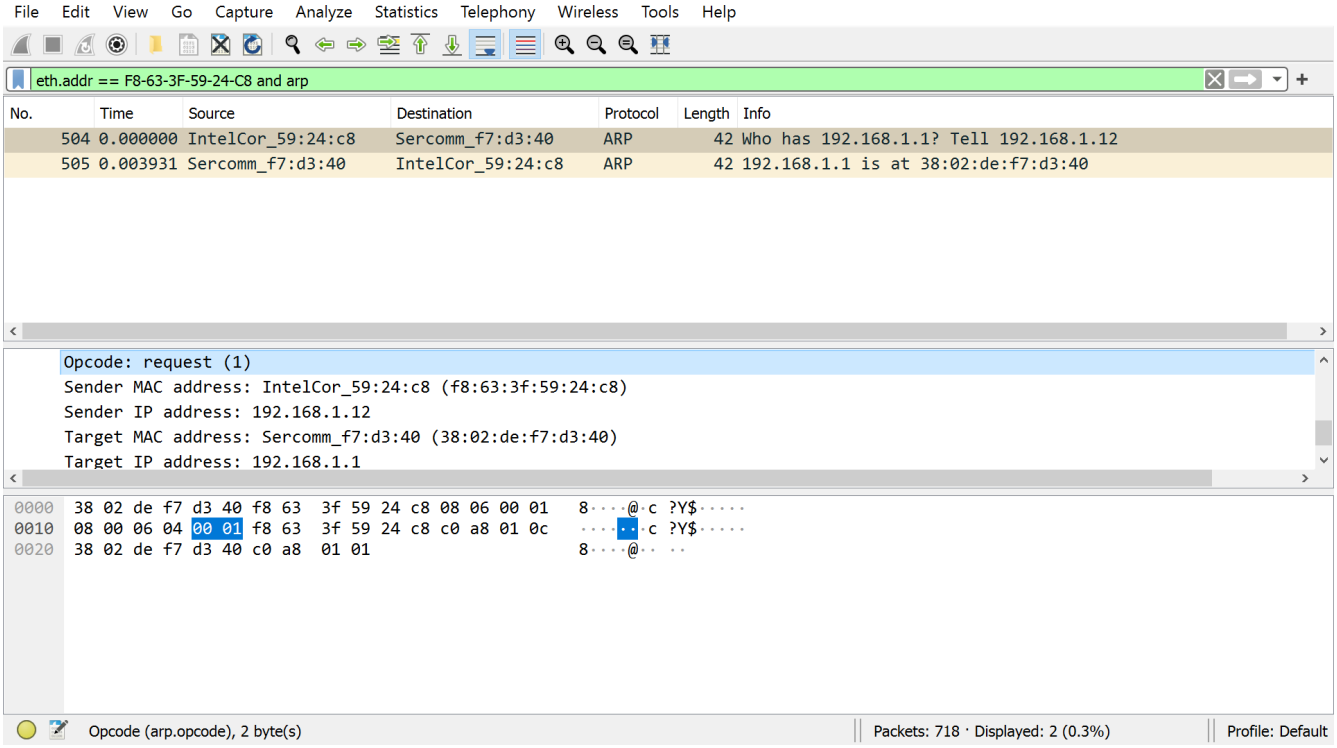
4.12 38:02:de:f8:09:a0 (κανονικά δεν την γνωρίζουμε ως τοτε, και αυτος είναι εξάλλου και ο λόγος που στέλνουμε το ARP request)

4.13 Μέγεθος ARP: 28 bytes, Μέγεθος Ethernet: 42 bytes επειδή έχει ενθυλακώσει το ARP


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eth.addr == F8-63-3F-59-24-C8 and arp
No. Time Source Destination Protocol Length Info
504 0.000000 IntelCor_59:24:c8 Sercomm_f7:d3:40 ARP 42 Who has 192.168.1.1? Tell 192.168.1.12
505 0.003931 Sercomm_f7:d3:40 IntelCor_59:24:c8 ARP 42 192.168.1.1 is at 38:02:de:f7:d3:40
Frame 504: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767C
Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Destination: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Source: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
Type: ARP (0x0806)
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c
0020 38 02 de f7 d3 40 c0 a8 01 01
OneDrive
Το στιγμιότυπο οθόνης αποθηκεύτηκε
Το στιγμιότυπο οθόνης προστέθηκε στο OneDrive.
Ethernet (eth), 14 byte(s)
Packets: 718 · Displayed: 2 (0.3%)
Profile: Default

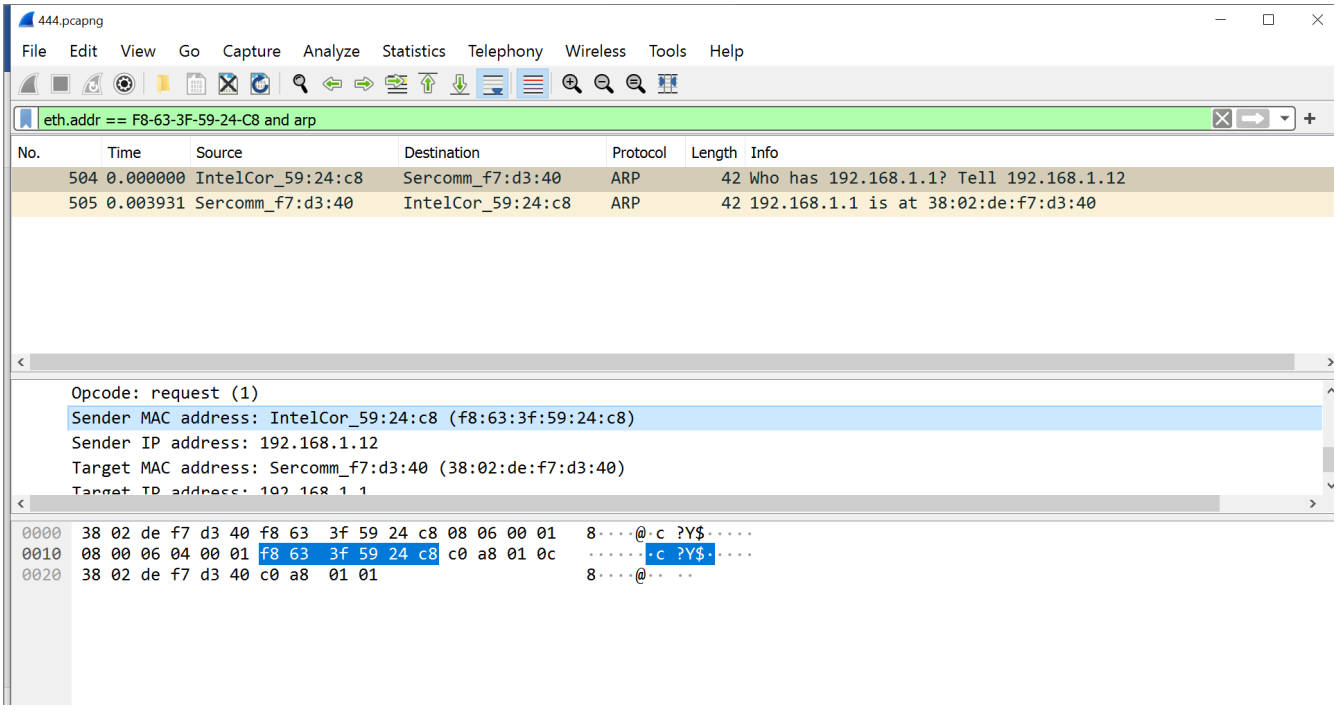

444.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eth.addr == F8-63-3F-59-24-C8 and arp
No. Time Source Destination Protocol Length Info
504 0.000000 IntelCor_59:24:c8 Sercomm_f7:d3:40 ARP 42 Who has 192.168.1.1? Tell 192.168.1.12
505 0.003931 Sercomm_f7:d3:40 IntelCor_59:24:c8 ARP 42 192.168.1.1 is at 38:02:de:f7:d3:40
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c
0020 38 02 de f7 d3 40 c0 a8 01 01

4.14 20 bytes

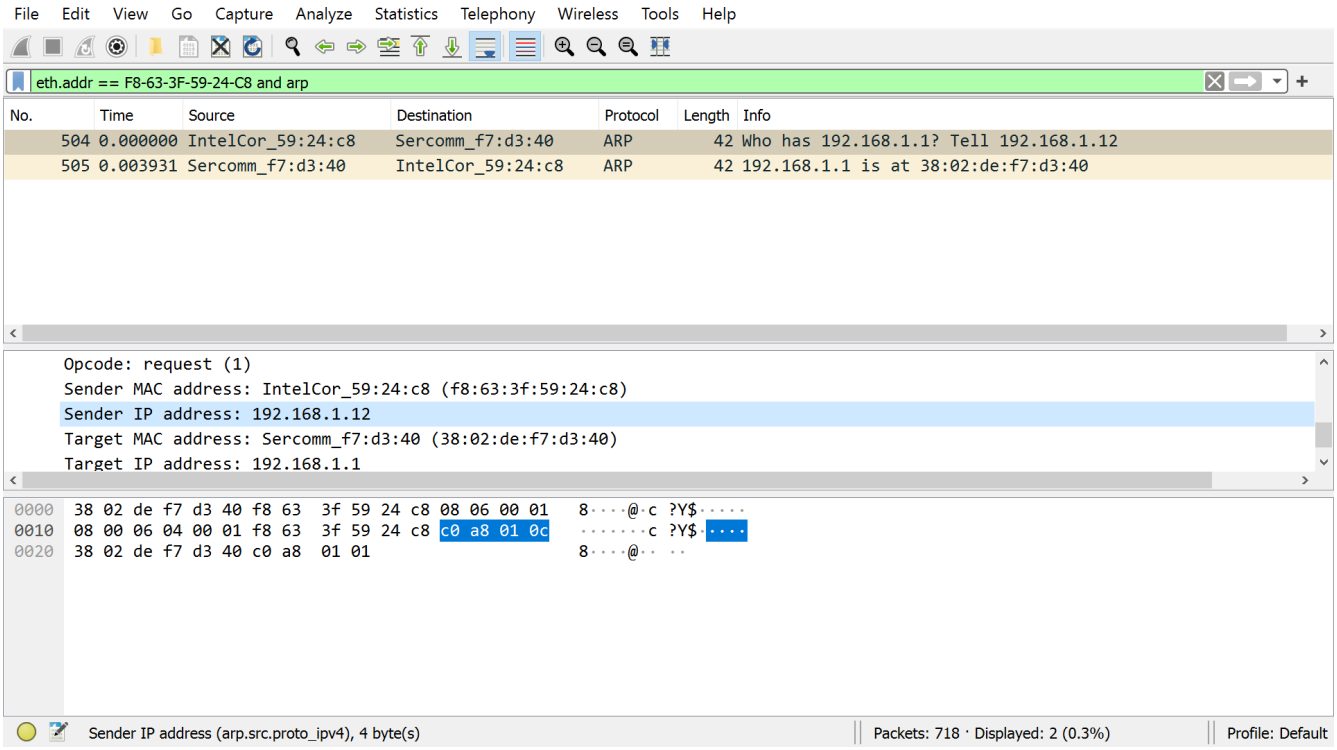


4.15 Είναι 0001 όπως φαίνεται και στο παραπάνω στιγμιότυπο οθόνης

4.16 Στο Sender MAC address



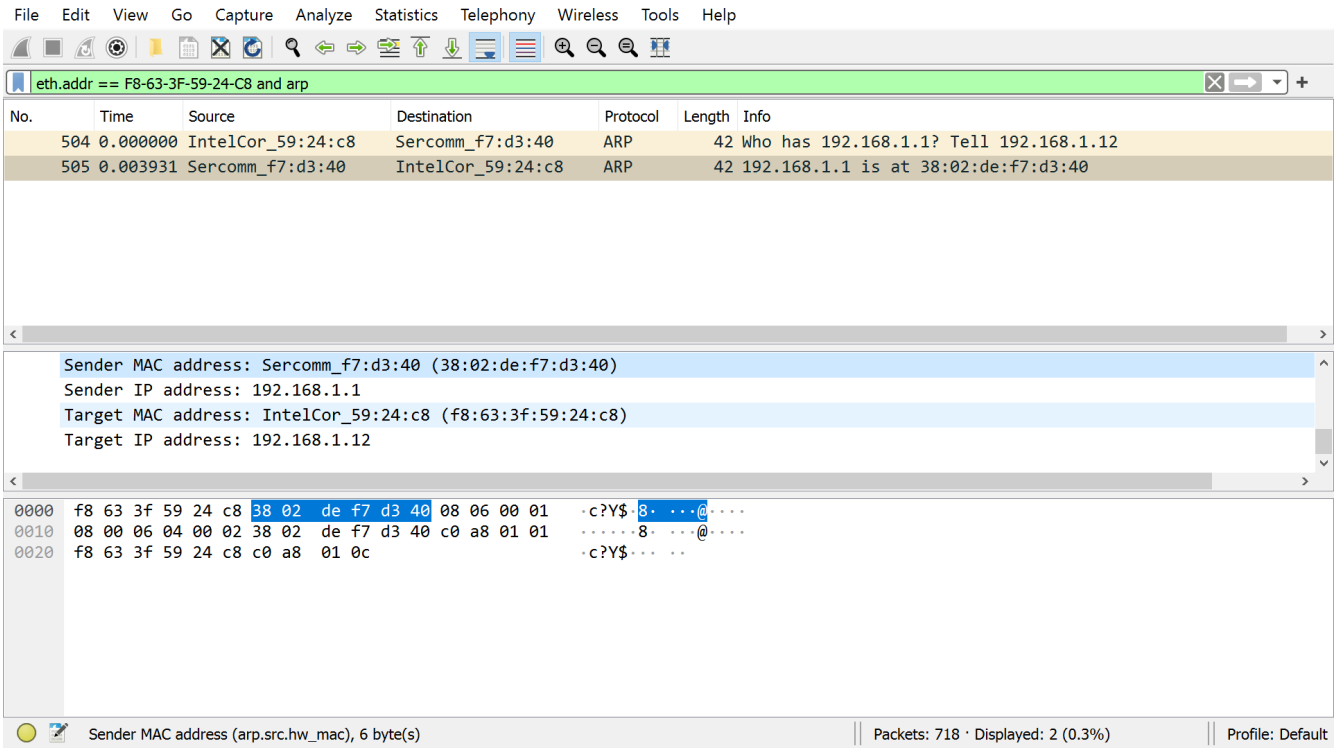
4.17 Στο Sender IP address



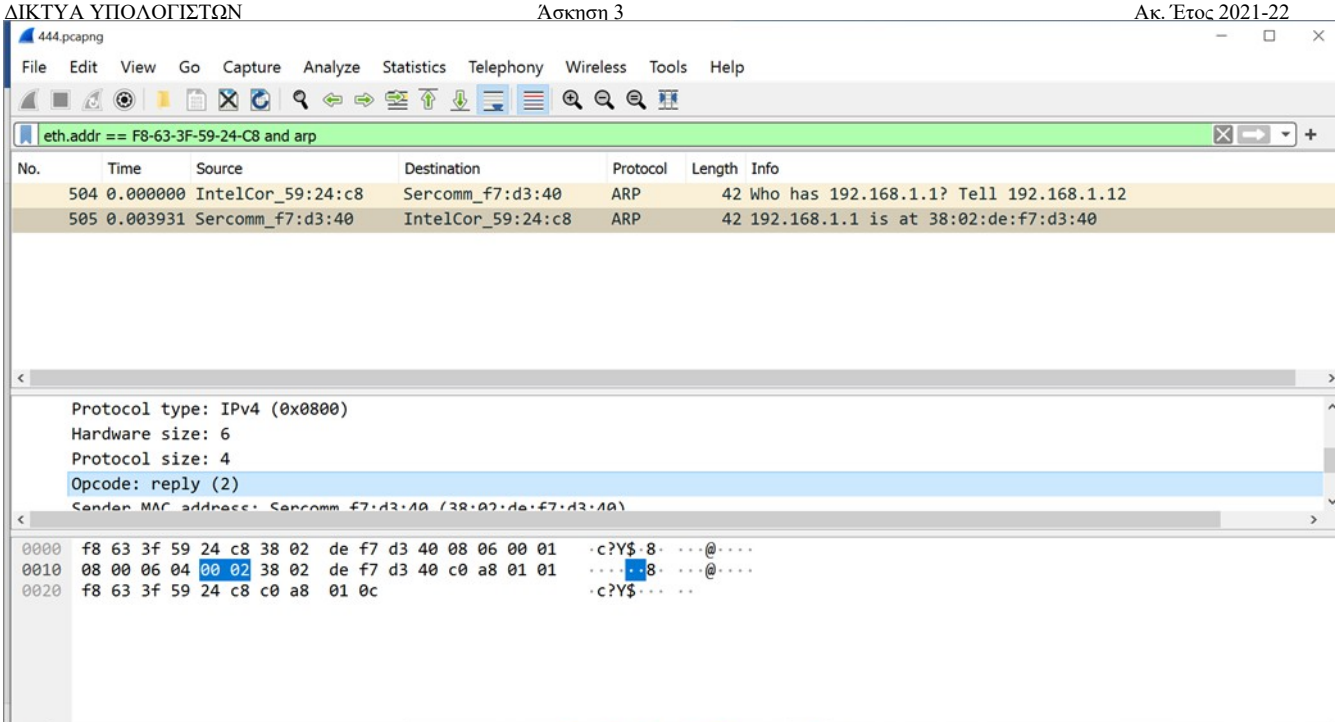
4.18 Στο πεδίο Target IP address (φαίνεται στα παραπάνω στιγμιότυπα οθόνης)

4.19 Είναι το πεδίο Target MAC address και η τιμή που θα έπρεπε να περιέχει είναι 00:00:00:00 καθώς δεν την ξέρουμε. (εδώ περιέχει την τιμή της ζητούμενης διεύθυνσης MAC σαν να την έχει ήδη βρει)

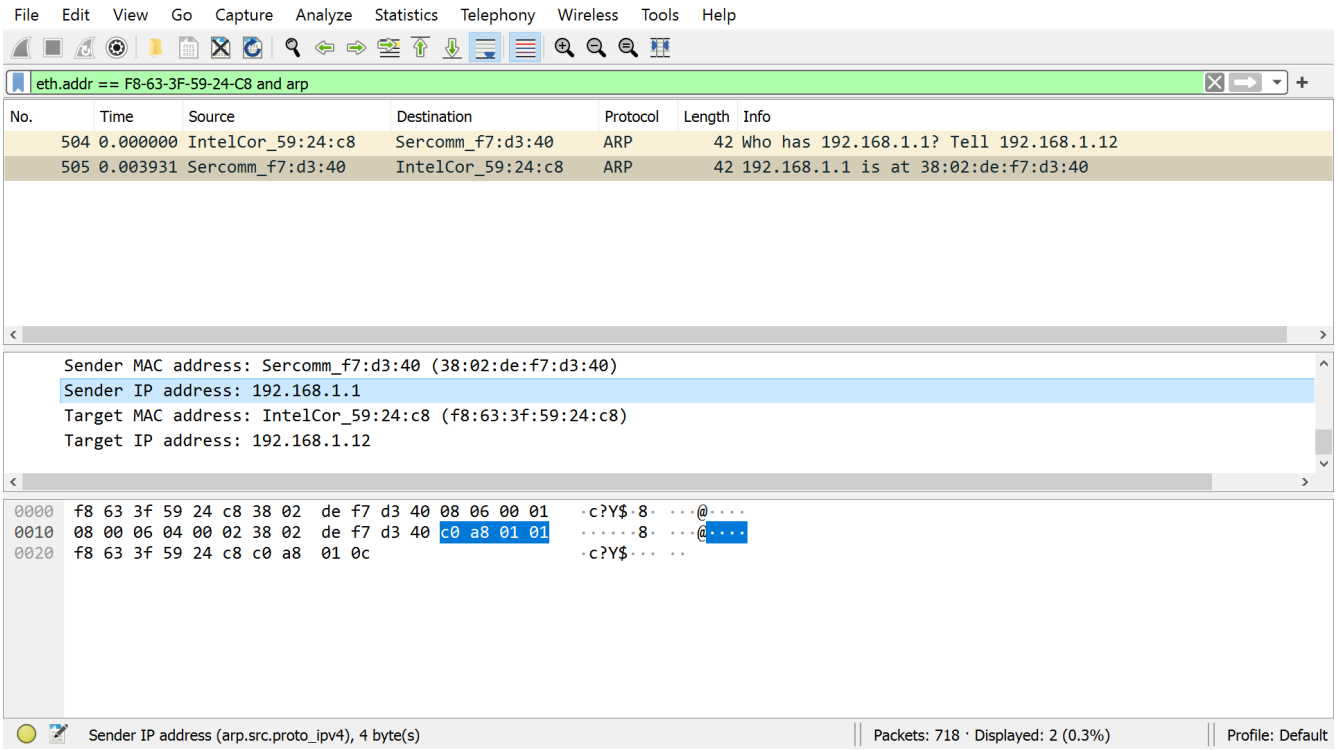
4.20 Η διεύθυνση MAC του αποστολέα είναι αυτή του router μου και η διεύθυνση MAC του παραλήπτη είναι του λαπτοπ μου.



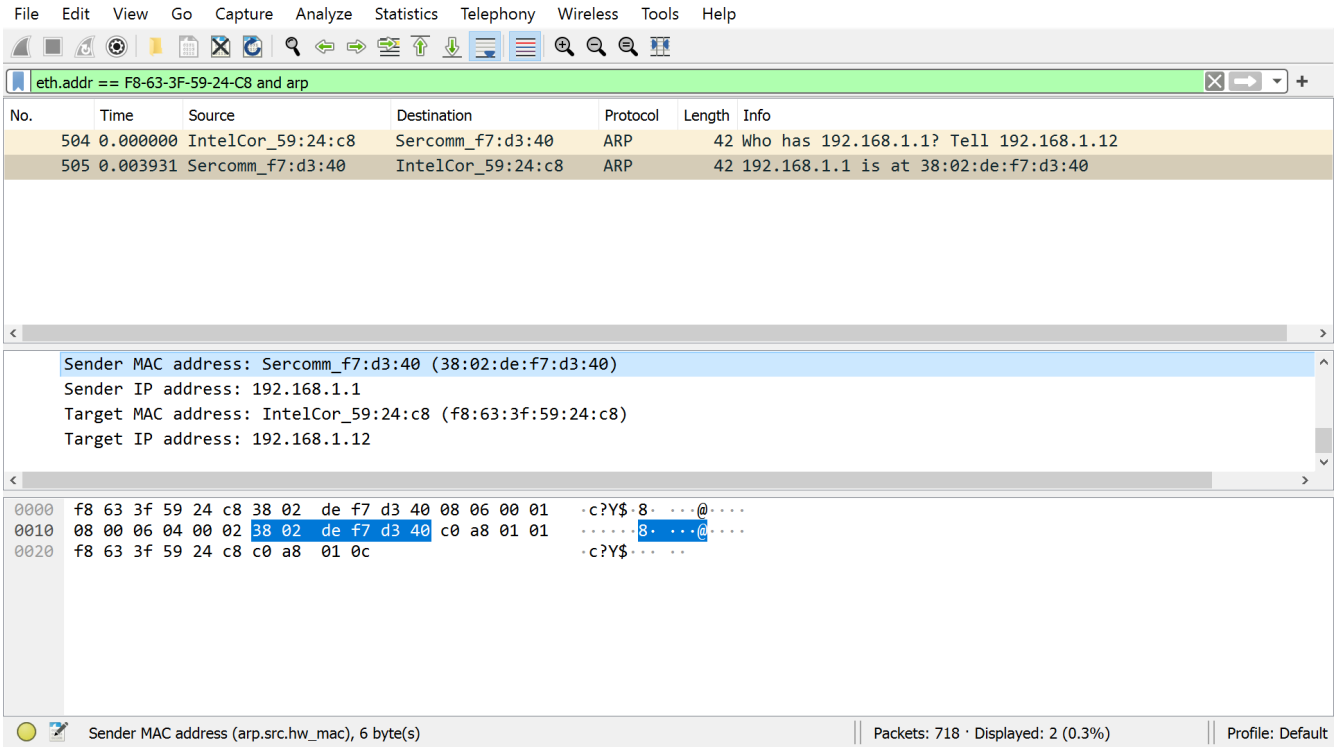
4.21 Η τιμή είναι 0002



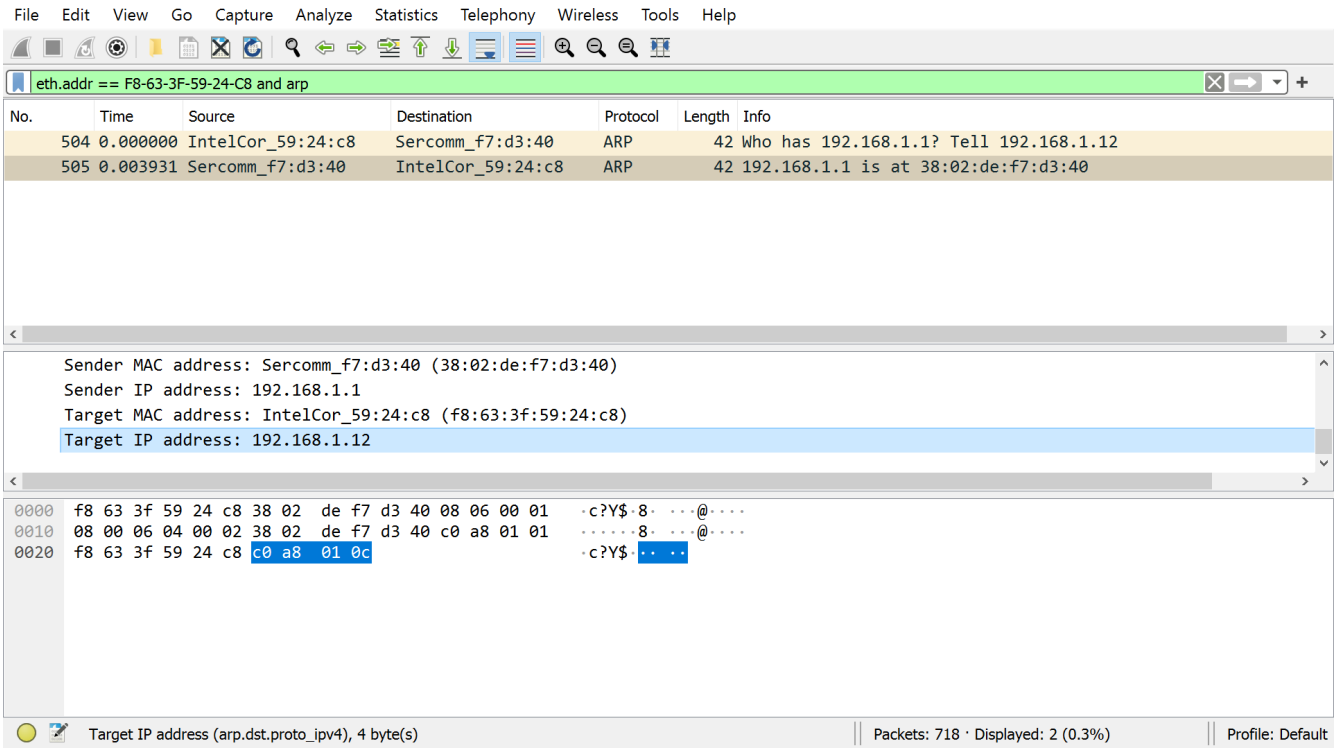
4.22 Στο πεδίο Sender IP address



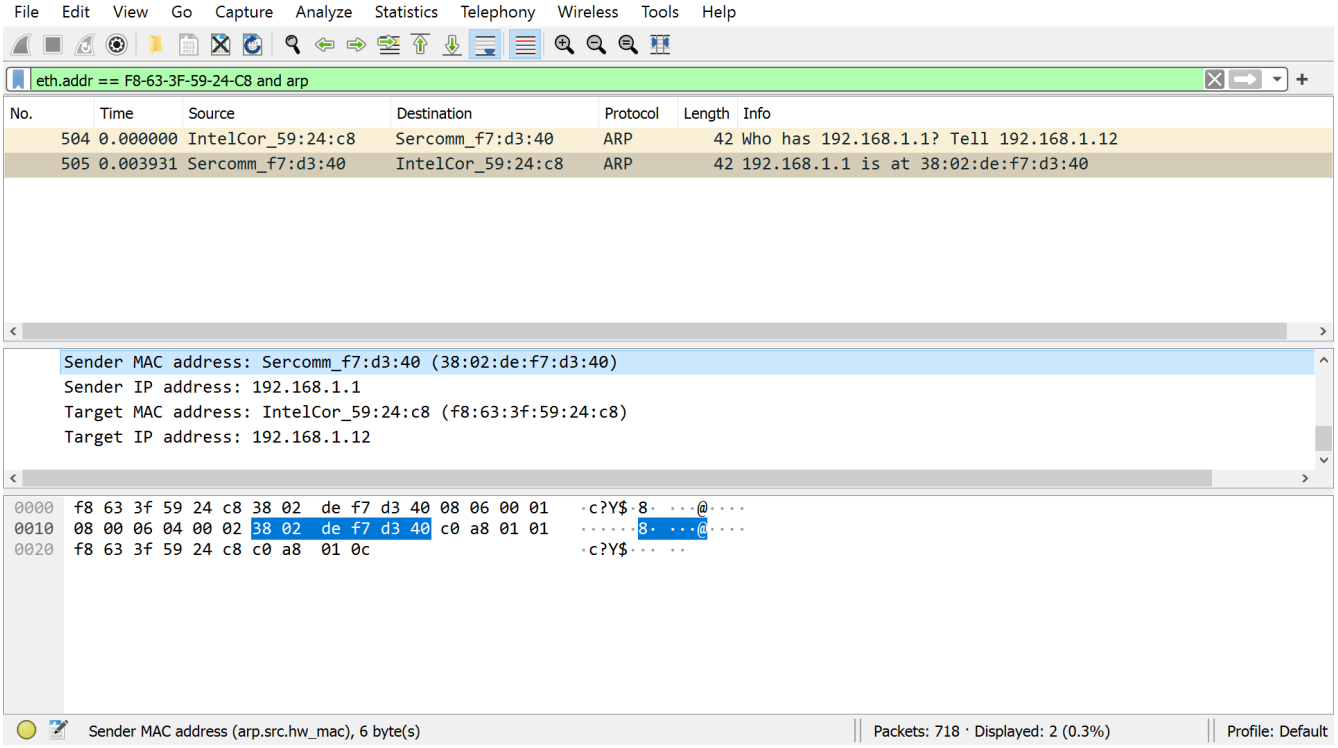
4.23 Sender MAC address



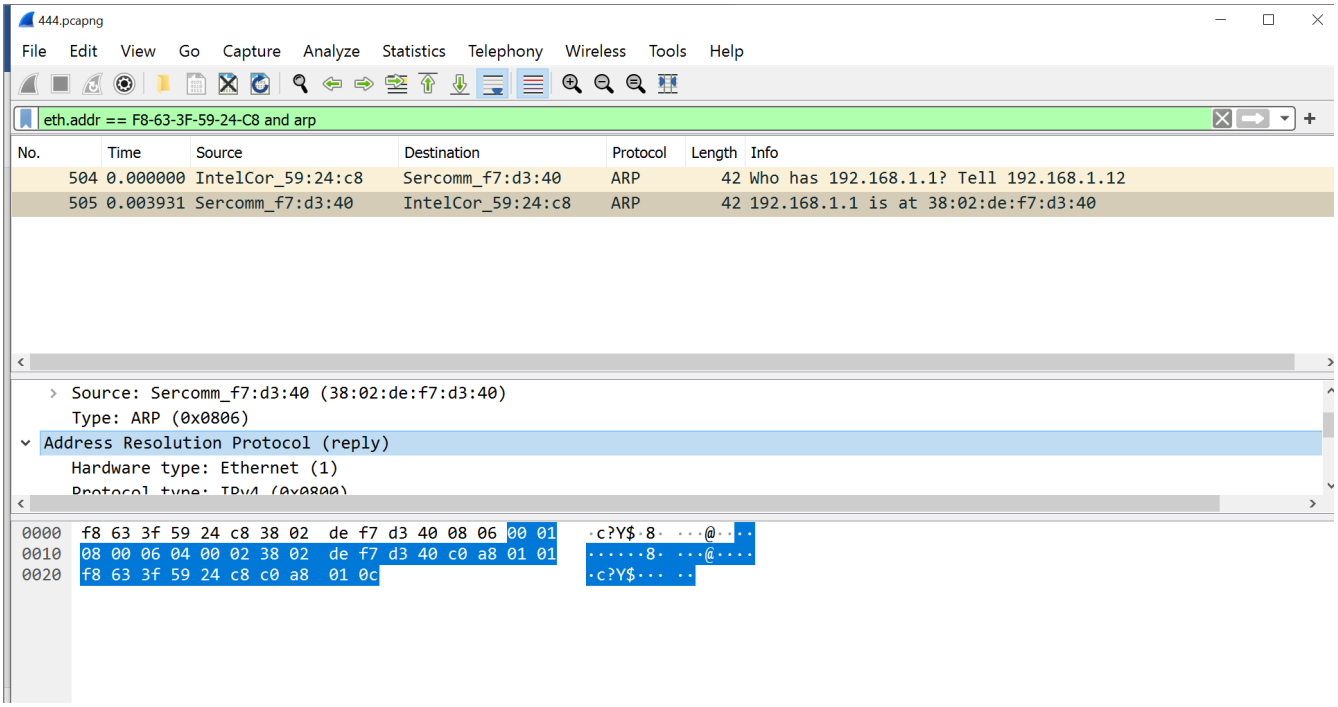
4.24 Target IP address

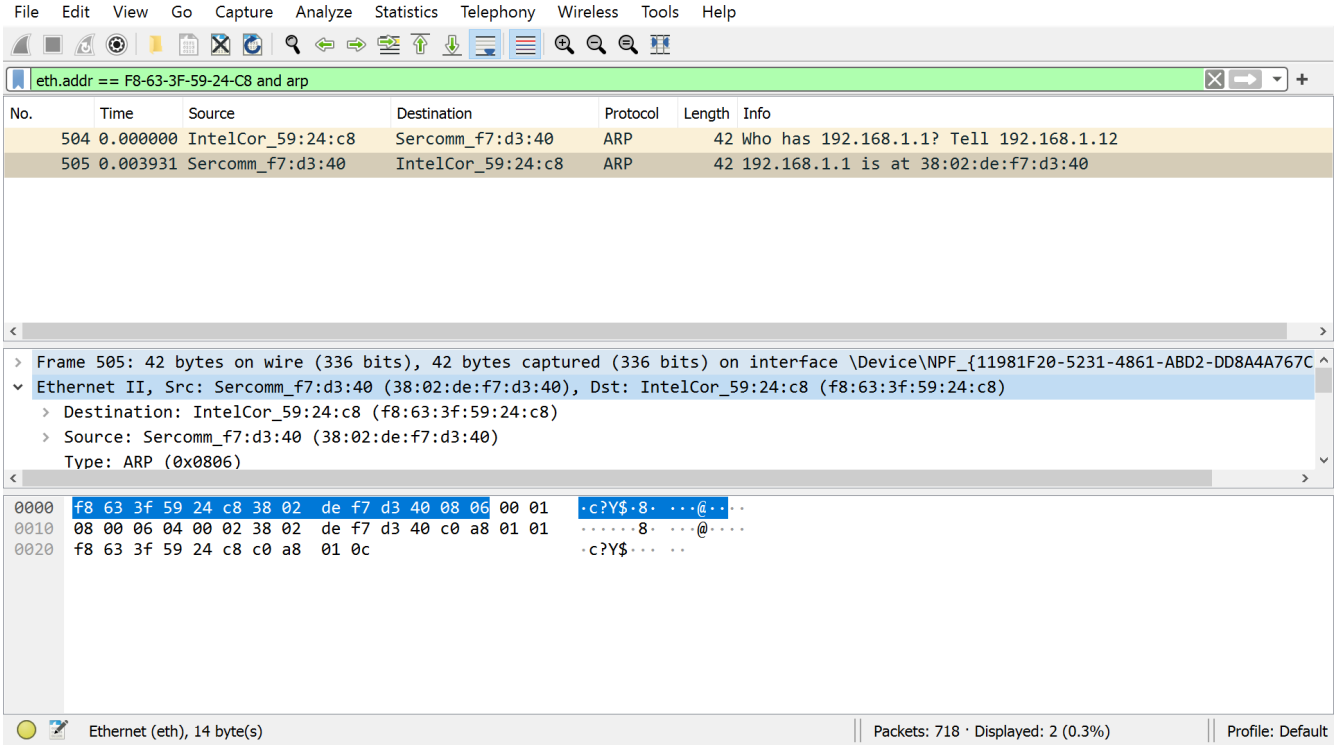


4.25 Στο πεδίο Sender MAC address.



4.26 Μέγεθος ARP reply: 28 bytes, Μέγεθος Ethernet: 42 bytes, όπως πριν





4.27 Ναι, αφού συνδέομαι από Wi-Fi (ασύρματα) δεν καταγραφεται (και ούτε βλέπω) το padding που φτάνει εως 64 bytes

4.28 (Θεωρητικά) Το wireshark θα καταγράφει τα πακέτα πριν φτάσουν στο στρώμα ζεύξης όπου και θα αποκτήσουν το απαραίτητο padding μέχρι τα 64 bytes που είναι το ελάχιστο μέγεθος για το πλαισιο ethernet. Στην απάντηση όπου το padding έχει γίνει από τον αποστολέα θα είναι φαίνεται στο wireshark. Φυσικά εγώ βλέπω ίδια τα μεγέθη

4.29 Το πεδίο Opcode

4.30 Στο ARP request (θεωρητικά) το πεδίο Target MAC address έχει την τιμή 00:00:00:00:00:00 καθώς δεν το γνωρίζουμε (γι αυτό εξάλλου στέλνουμε το request). Στο reply αυτή η τιμή προφανώς θα αντικατασταθεί από την MAC address της συσκευής που ψάχναμε. Επίσης το request το στέλνουμε «ανοικτά» (broadcast) ενώ το reply στέλνεται προς συγκεκριμένο παραλήπτη.

4.31 Θα έθετε σε κίνδυνο τα δεδομένα όλων των χρηστών του δικτύου, καθως θα έστελναν πλαίσια στον κακόβουλο υπολογιστή, και αυτός θα μπορεί να ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από κάποιον/ους φιλικό/ούς χρήστη/ες.