Ονοματεπώνυμο: Άγγελος Μητροκώτσας	Ομάδα:6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	Ημερομηνία:25/ 10/ 2021
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC: F8-63-3F-59-24-C8

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

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

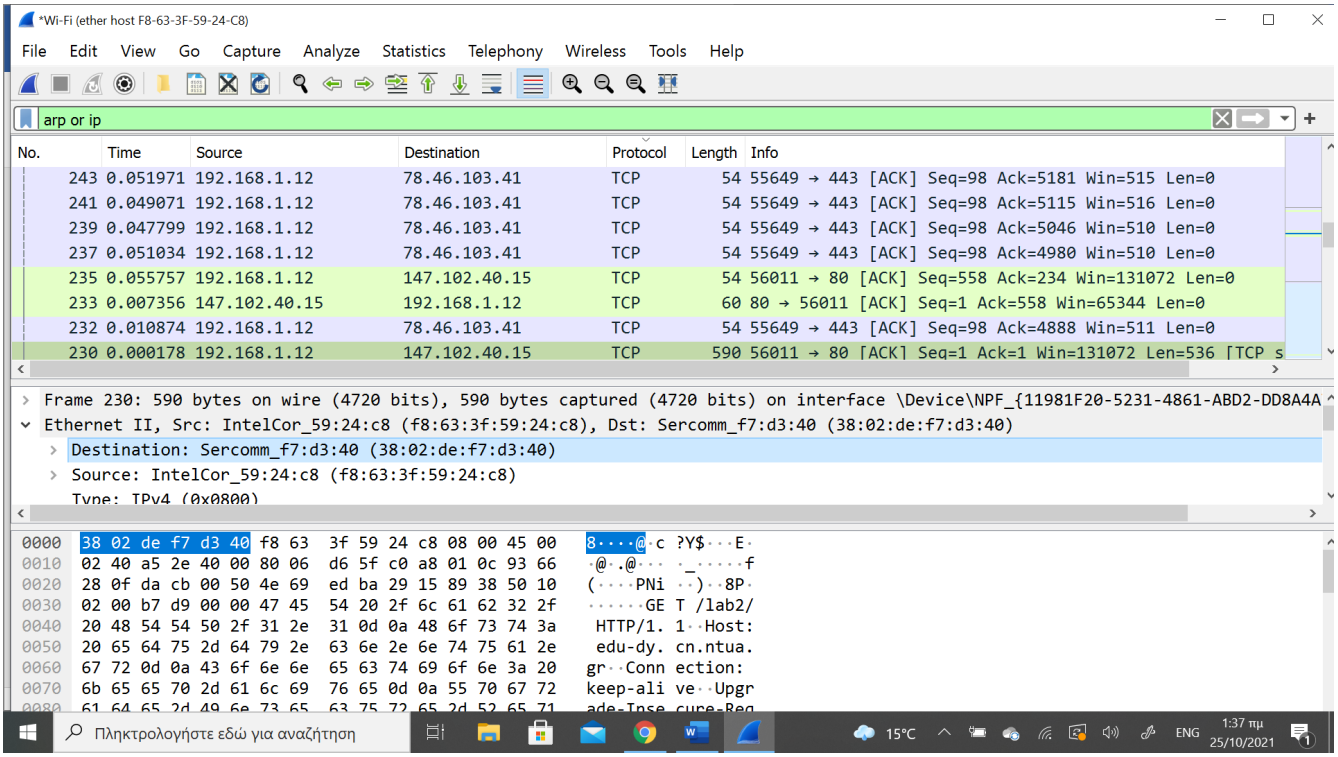
1

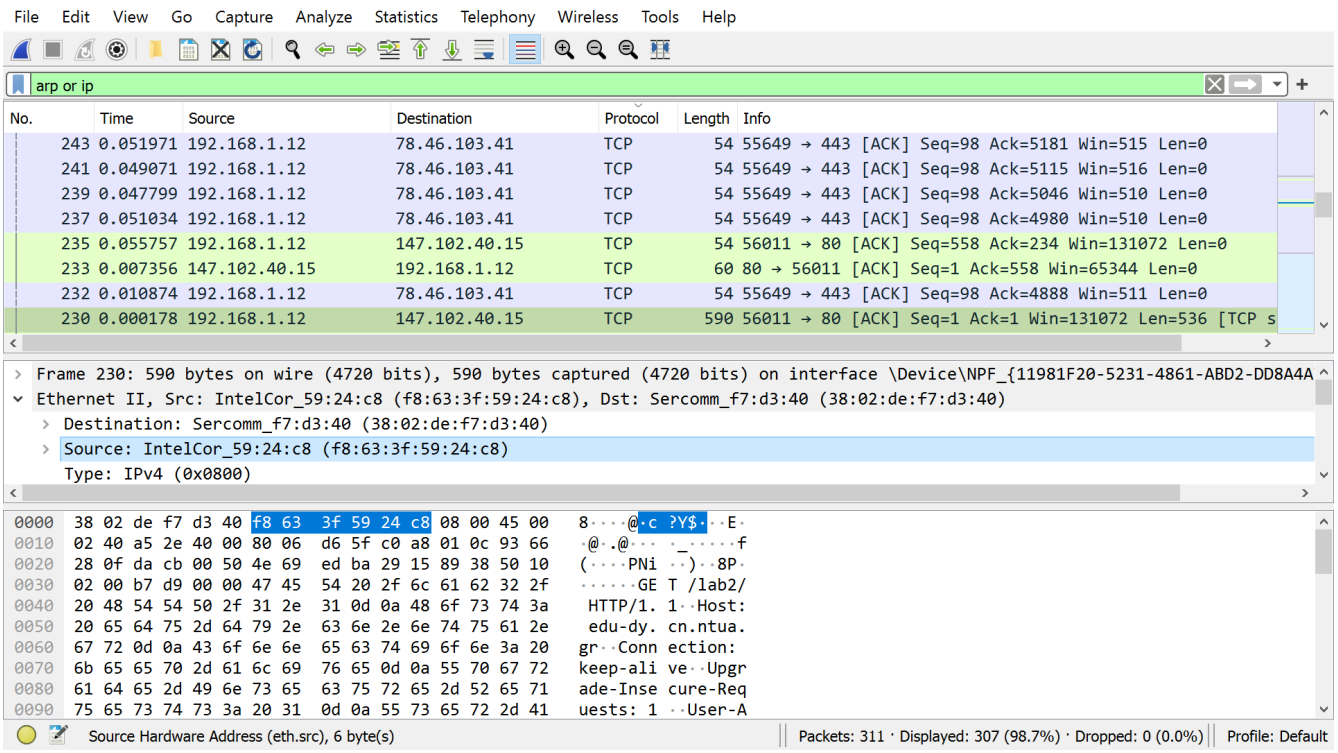
1.1 Το φιλτρο επιτρέπει την απεικονιση πρωτοκολλων μονο τύπου IP και AVR.

1.2 Destination, Source και Type.

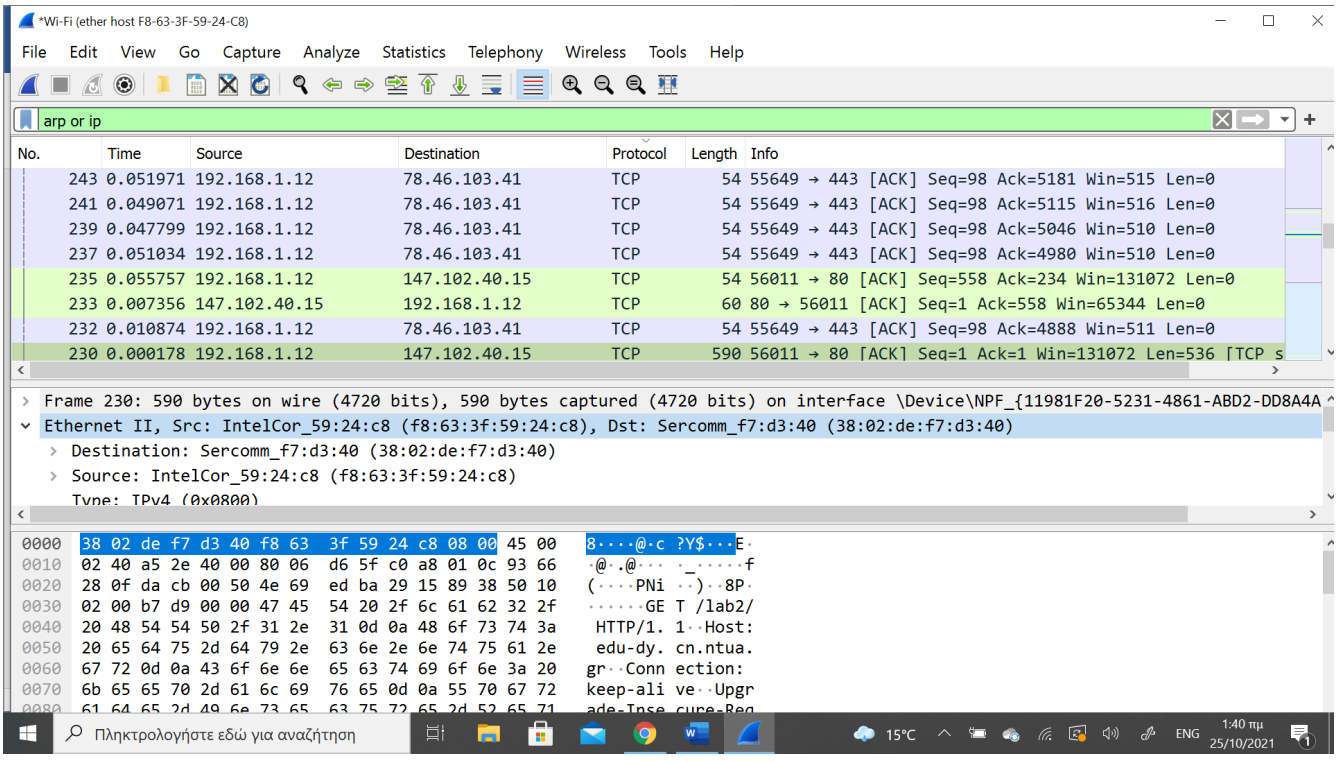
1.3 Όχι δεν υπάρχει.

1.4 6 bytes

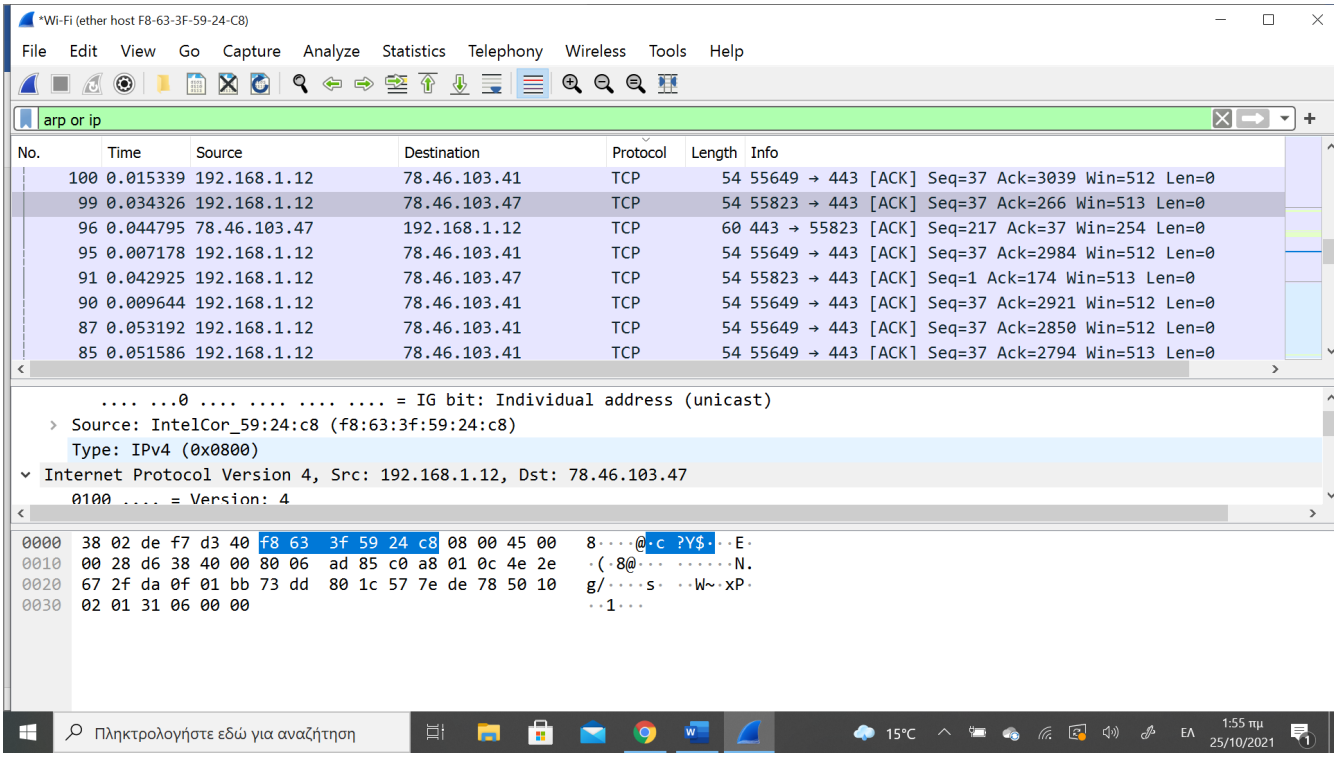




1.5 14 bytes



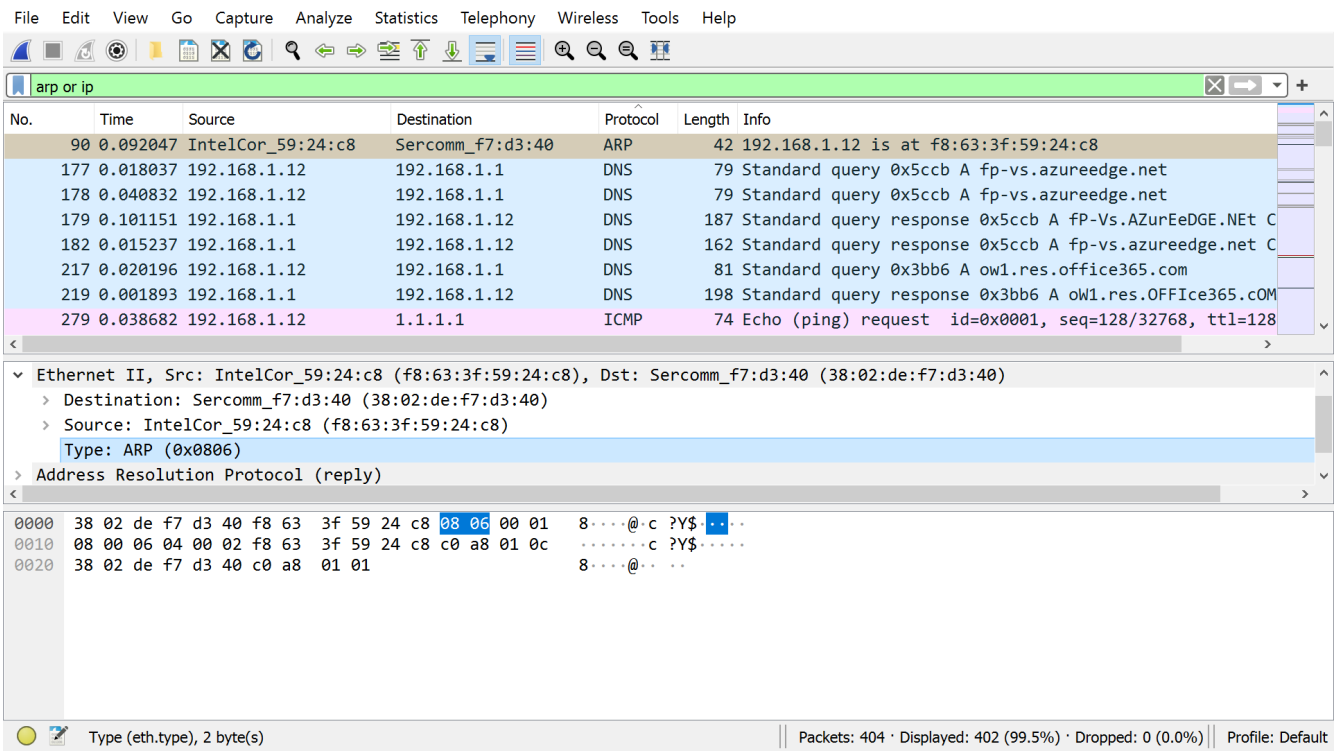
1.6 To Type.



1.7 Τα τελευταία 2 byte (φαινεται στο στιγμιοτυπο οθονης στο 1.5)

1.8 0800 {IPv4(0x0800)}

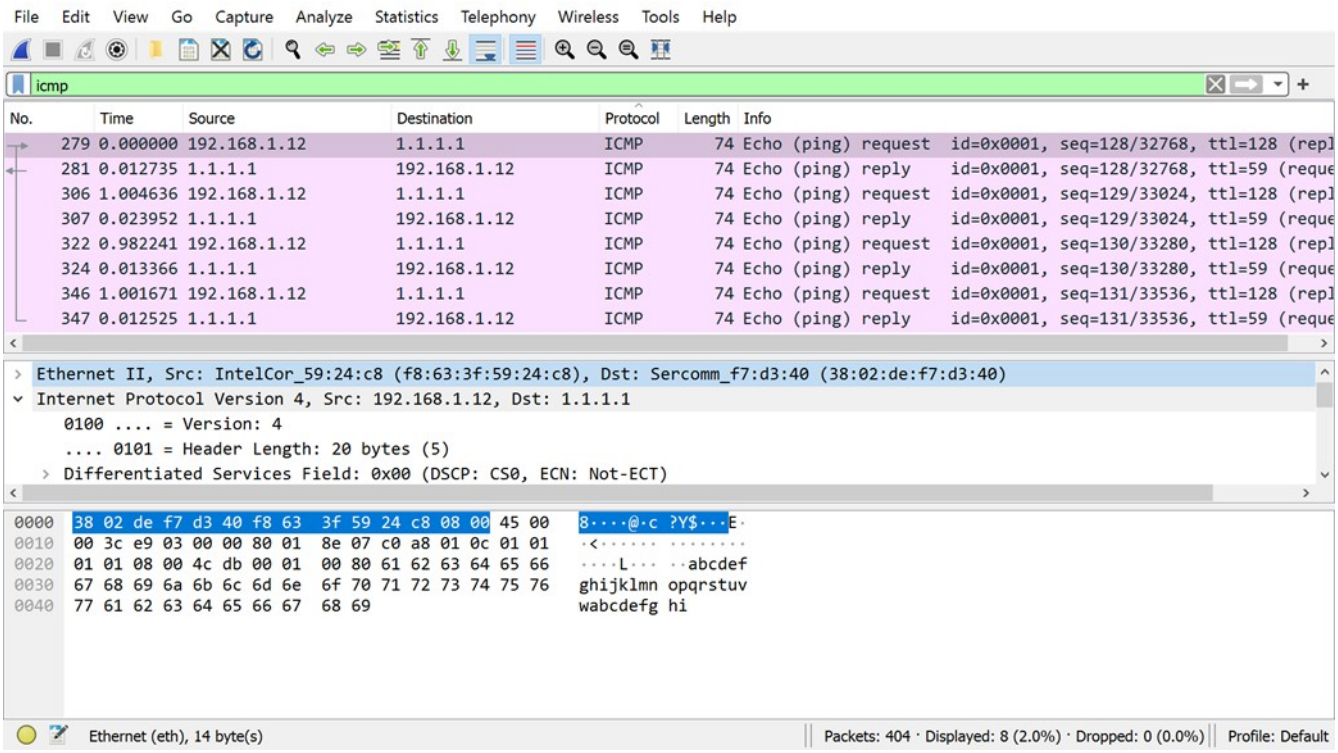
1.9 0x0806



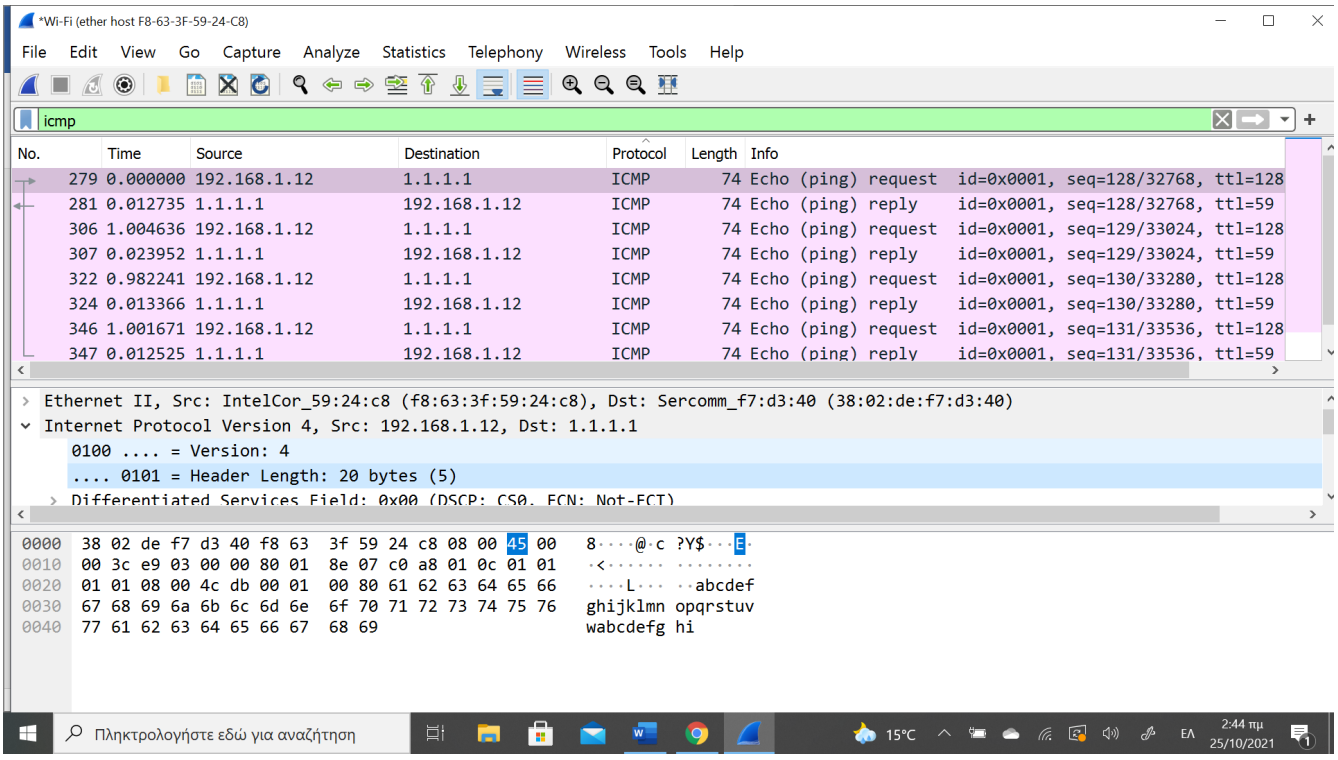
2

2.1 Το φιλτρο επιτρέπει την απεικονιση πρωτοκολλων μονο τύπου ICMP

2.2 4 bytes (όπως πριν)

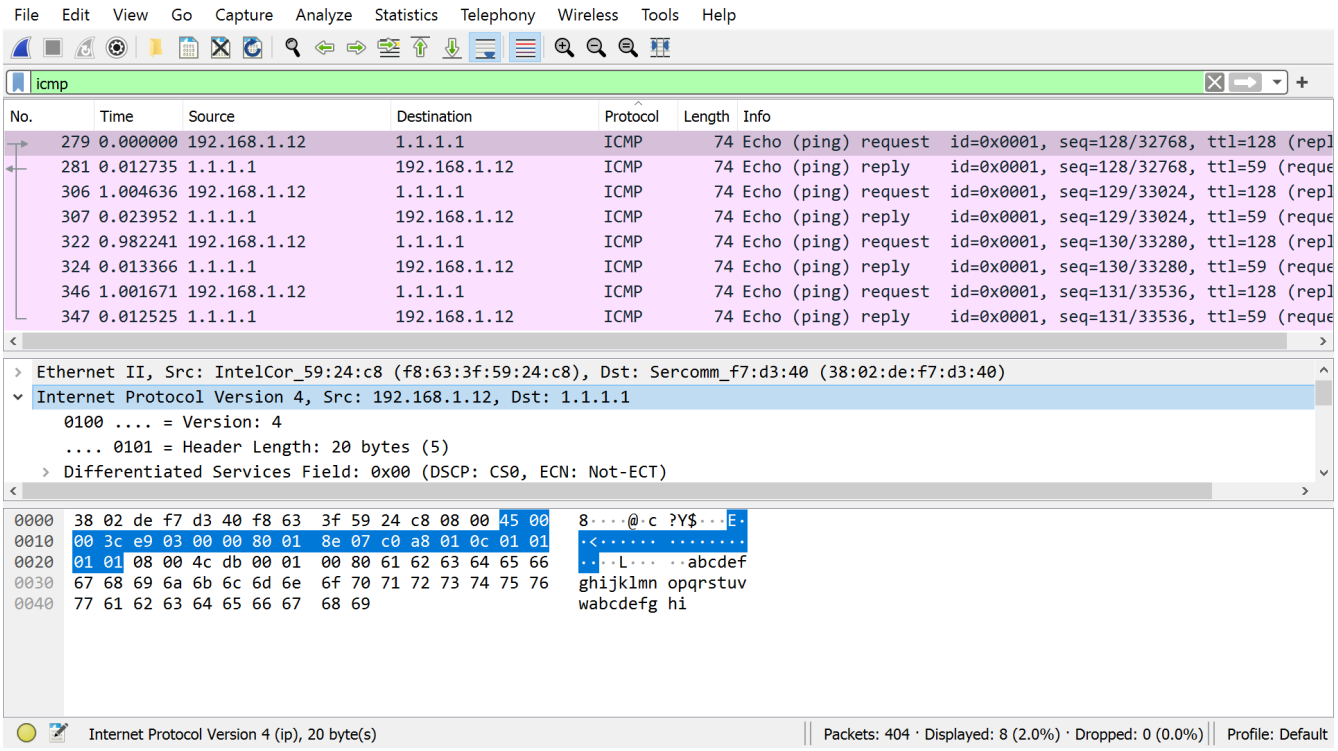


2.3 Version, Header Length



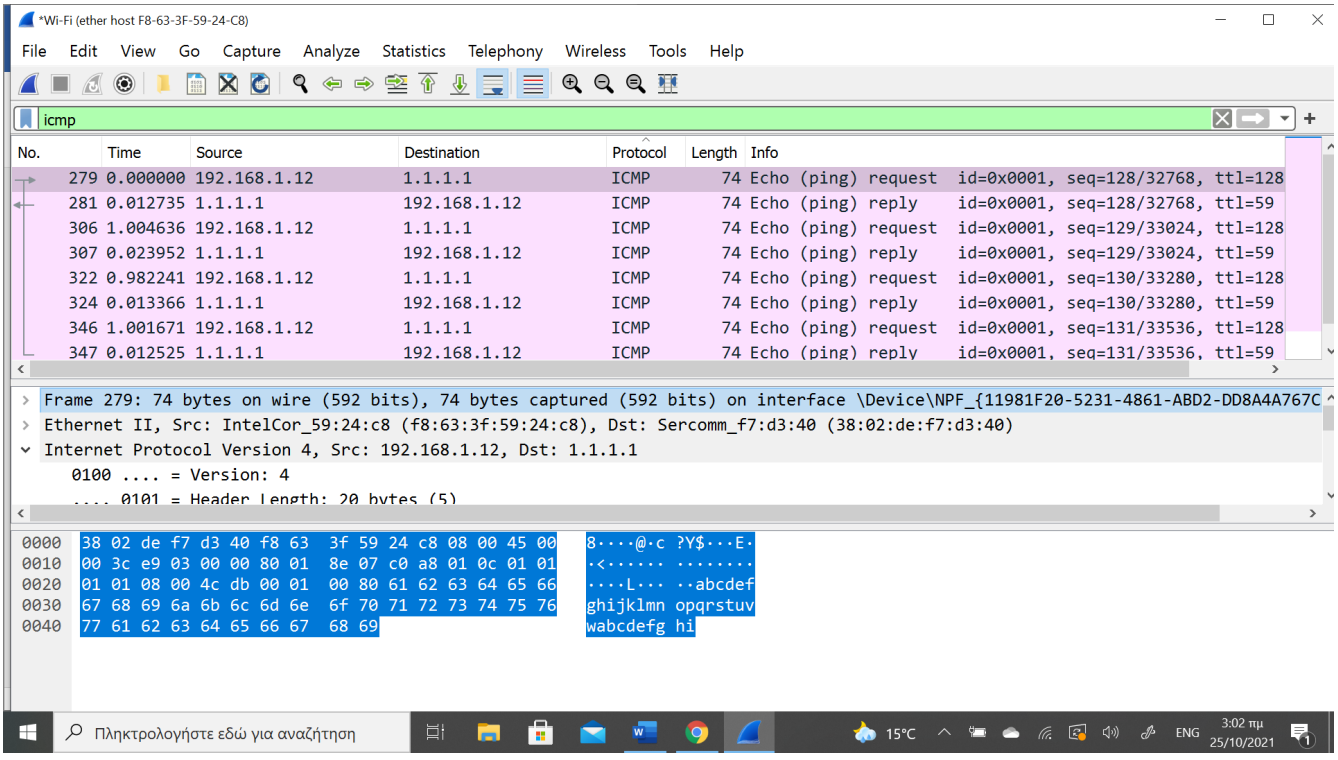
2.4 0b0100 και 0b0101 για το Version και Header Length αντιστοιχα.

2.5 20 bytes



2.6 Η τιμή του αντίστοιχου πεδίου της επικεφαλίδας IPv4είναι 5, αν το πολ/με επι 4 είναι το συνολικό μήκος της επικεφαλίδας (ή τα μετραμε και με το ματι)

2.7 74 bytes ή 592bits



2.8 Ναι υπαρχει, αυτό με την ονομασια «Length», και συμφωνει, καθως γραφει 74

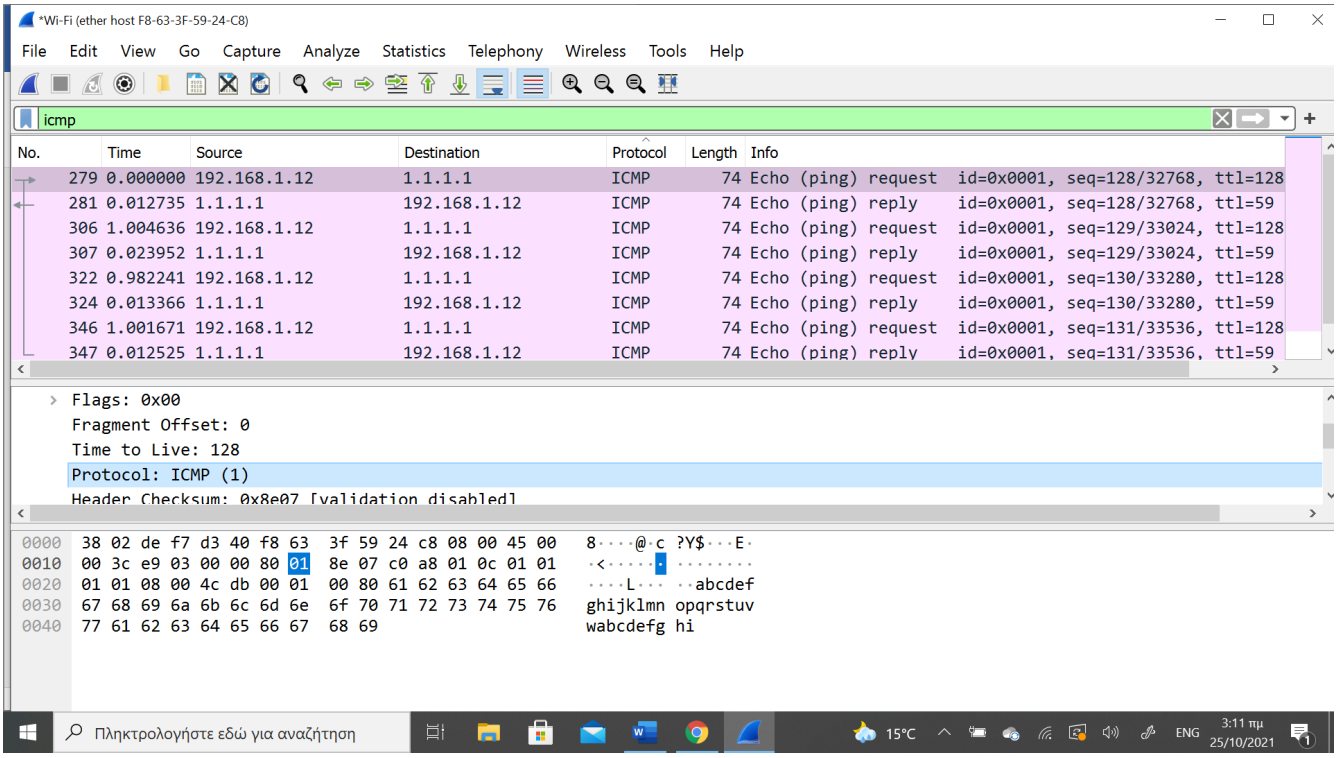
2.9 54bytes

2.10 74 -20 = 54 bytes (συνολικο μηκος – μηκος επικεφαλίδας)

2.11 Το πεδιο με ονομασια “Protocol”

2.12 Στο 10ο byte της επικεφαλιδας

2.13 0x01

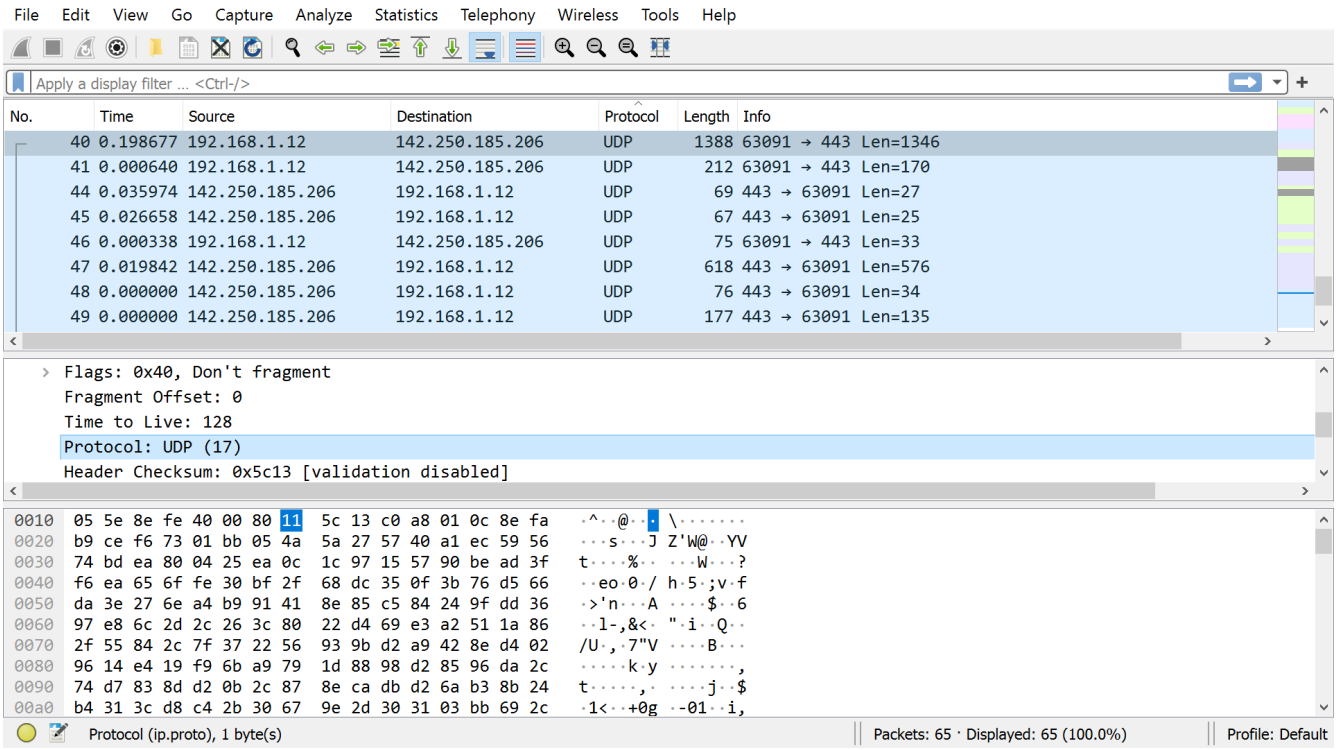

*Wi-Fi (ether host F8-63-3F-59-24-C8)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
279 0.000000 192.168.1.12 1.1.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=128/32768, ttl=128
281 0.012735 1.1.1.1 192.168.1.12 ICMP 74 Echo (ping) reply id=0x0001, seq=128/32768, ttl=59
306 1.004636 192.168.1.12 1.1.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=129/33024, ttl=128
307 0.023952 1.1.1.1 192.168.1.12 ICMP 74 Echo (ping) reply id=0x0001, seq=129/33024, ttl=59
322 0.982241 192.168.1.12 1.1.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=130/33280, ttl=128
324 0.013366 1.1.1.1 192.168.1.12 ICMP 74 Echo (ping) reply id=0x0001, seq=130/33280, ttl=59
346 1.001671 192.168.1.12 1.1.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=131/33536, ttl=128
347 0.012525 1.1.1.1 192.168.1.12 ICMP 74 Echo (ping) reply id=0x0001, seq=131/33536, ttl=59
Flags: 0x00
Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x8e07 [validation disabled]
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00
0010 00 3c e9 03 00 00 80 01 8e 07 c0 a8 01 0c 01 01
0020 01 01 08 00 4c db 00 01 00 80 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Πληκτρολογήστε εδώ για αναζήτηση
15°C
ENG
3:11 πμ
25/10/2021

3

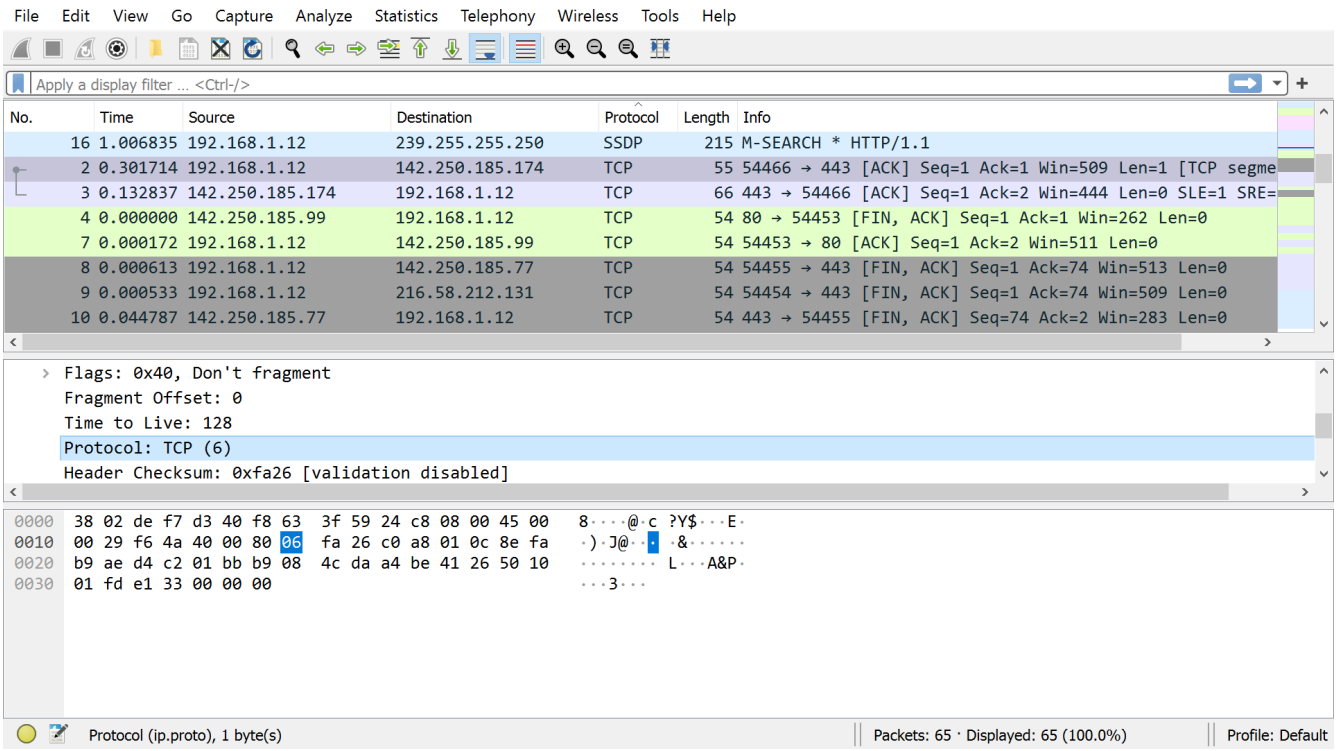
3.1 Κρατάει μόνο το σύνολο των πακέτων που είναι πρωτόκολλου UDP και εκείνα που στην επικεφαλίδα έχουν TCP type.

3.2 UDP, TCP, DNS, TLSv1.2, HTTP

3.3 Για το UDP: 17 ή 0x11

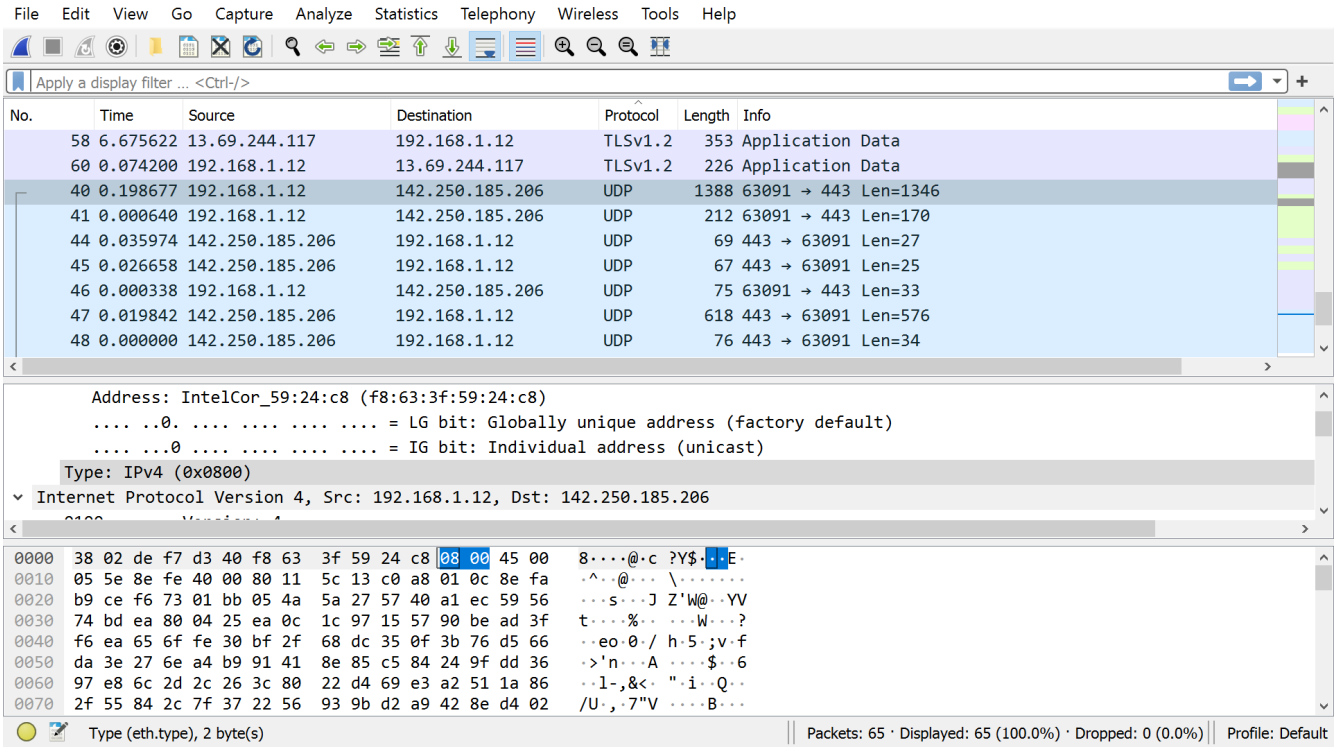


Για το TCP: 6 ή 0x06



3.4 Src Port και Dst port

3.5 8 bytes.



3.6 Ναι, υπάρχει (φαίνεται στο παραπάνω στιγμιότυπο οθόνης).

3.7 Το βρίσκουμε στο 13ο byte της επικεφαλιδας

3.8 Αντίστοιχο πεδίο δεν υπαρχει. Το συνολικό μήκος προκύπτει από άθροισμα των IPv4 Header Length και TCP Header Length

3.9 Το Destination Port.

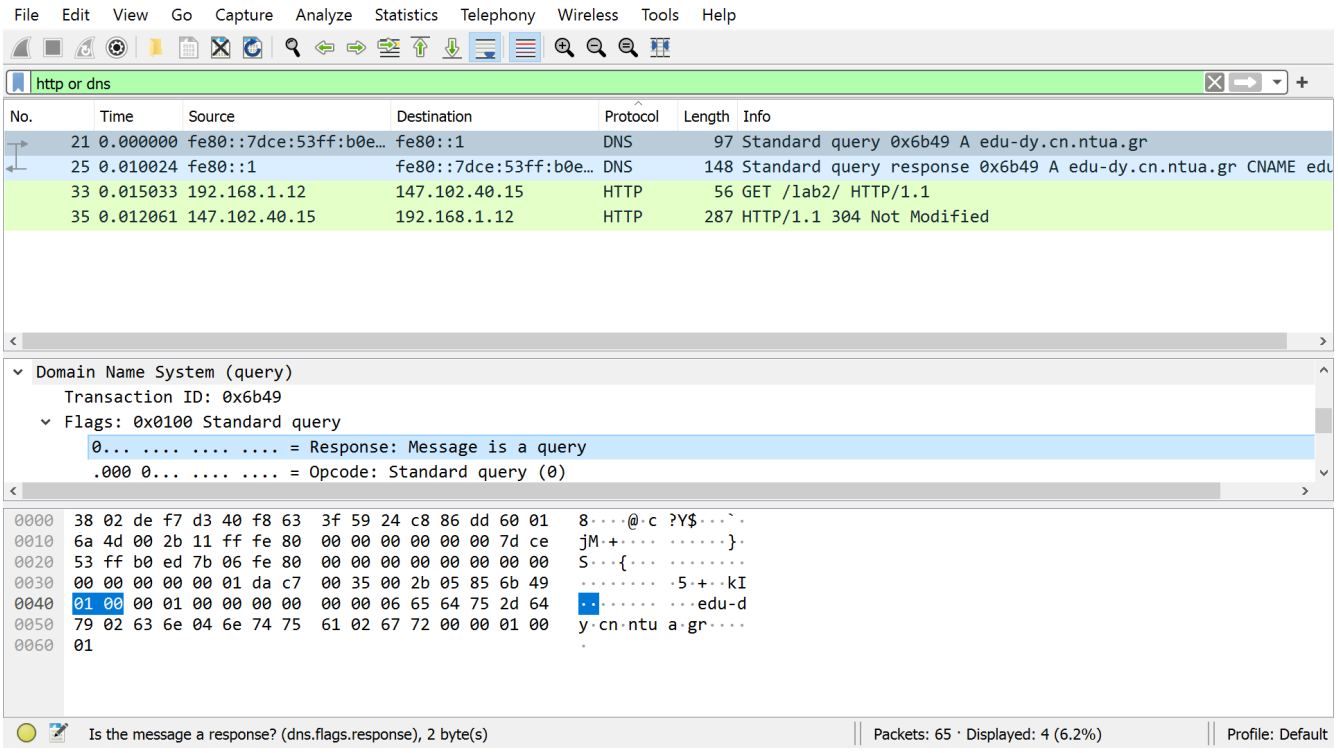
3.10 SSDP, ICMPv6, ARP

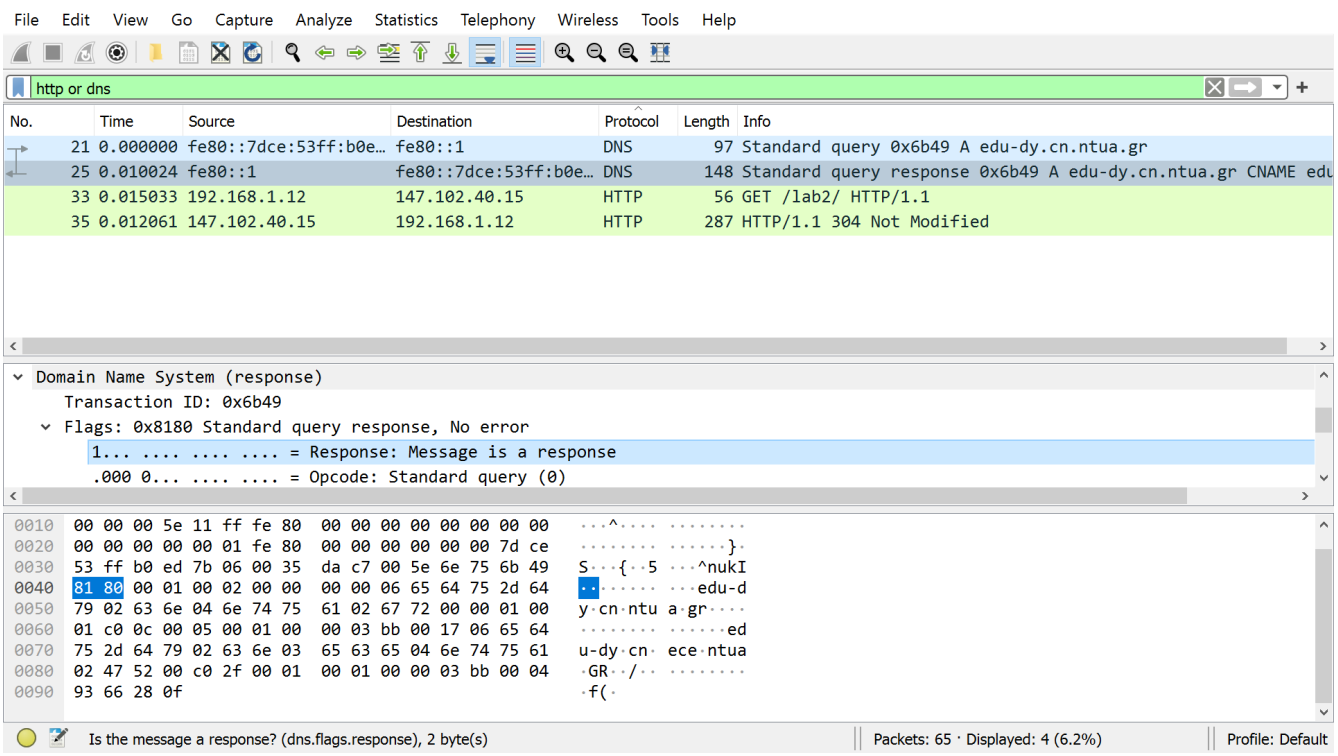
4

4.1 Το UDP.

4.2 Το TCP.

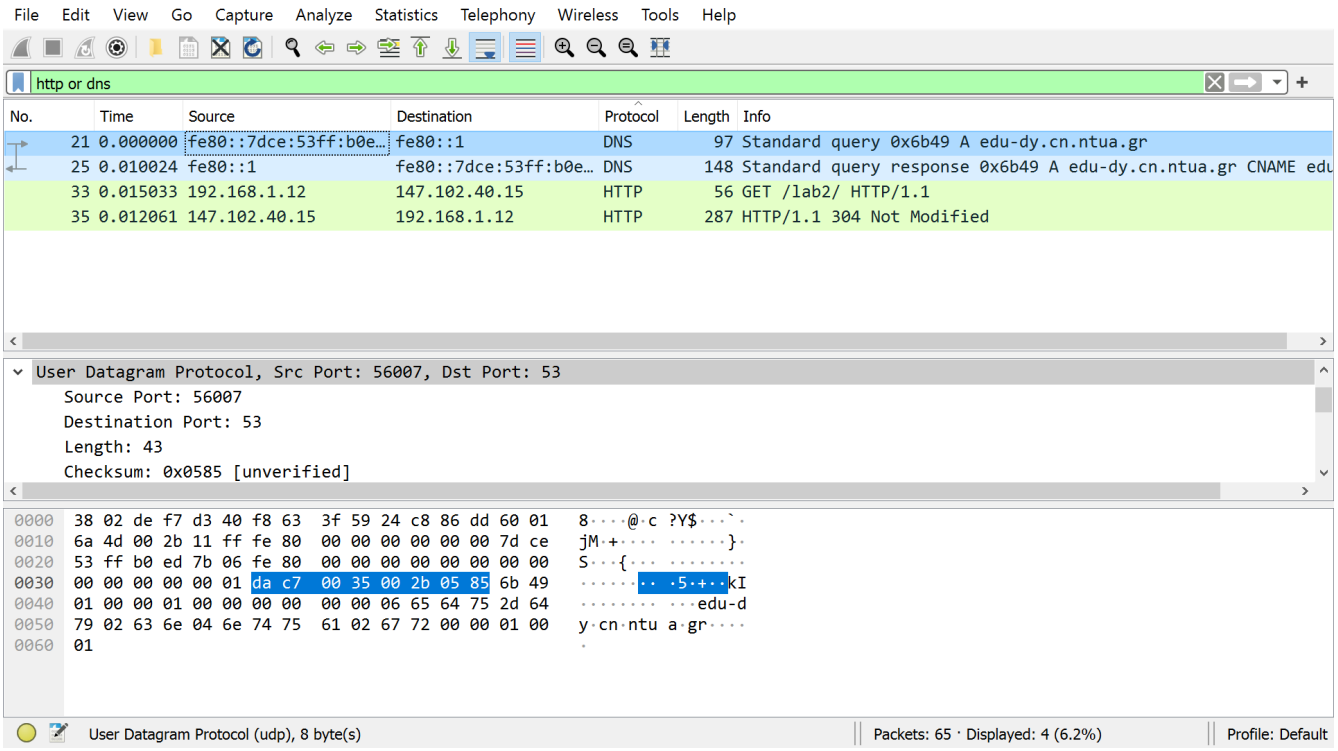
4.3 Το καθοριζει το 1ο bit του flag (σημαιας) και έχει τιμή 0 όταν είναι query και 1 όταν ειναι response.





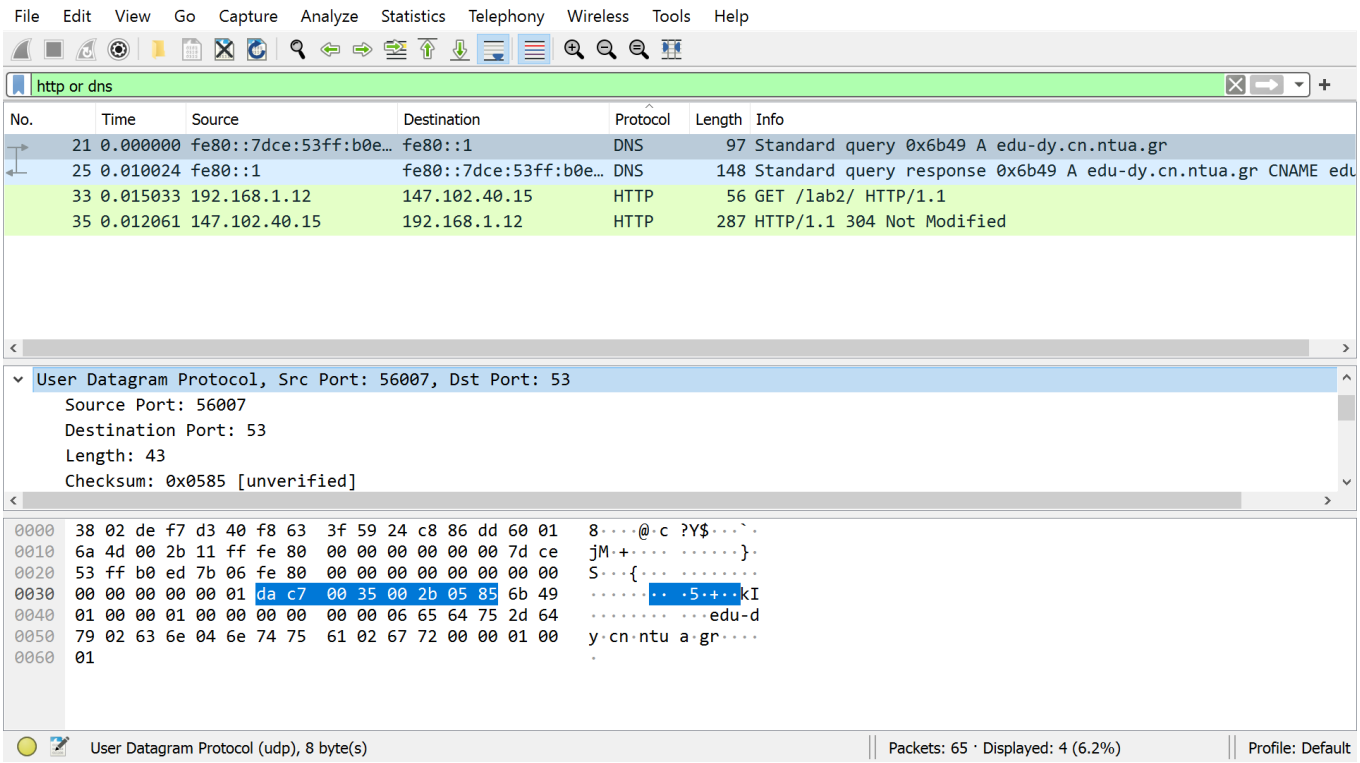
4.4 56007

4.5 53



4.6 53

4.7 56007

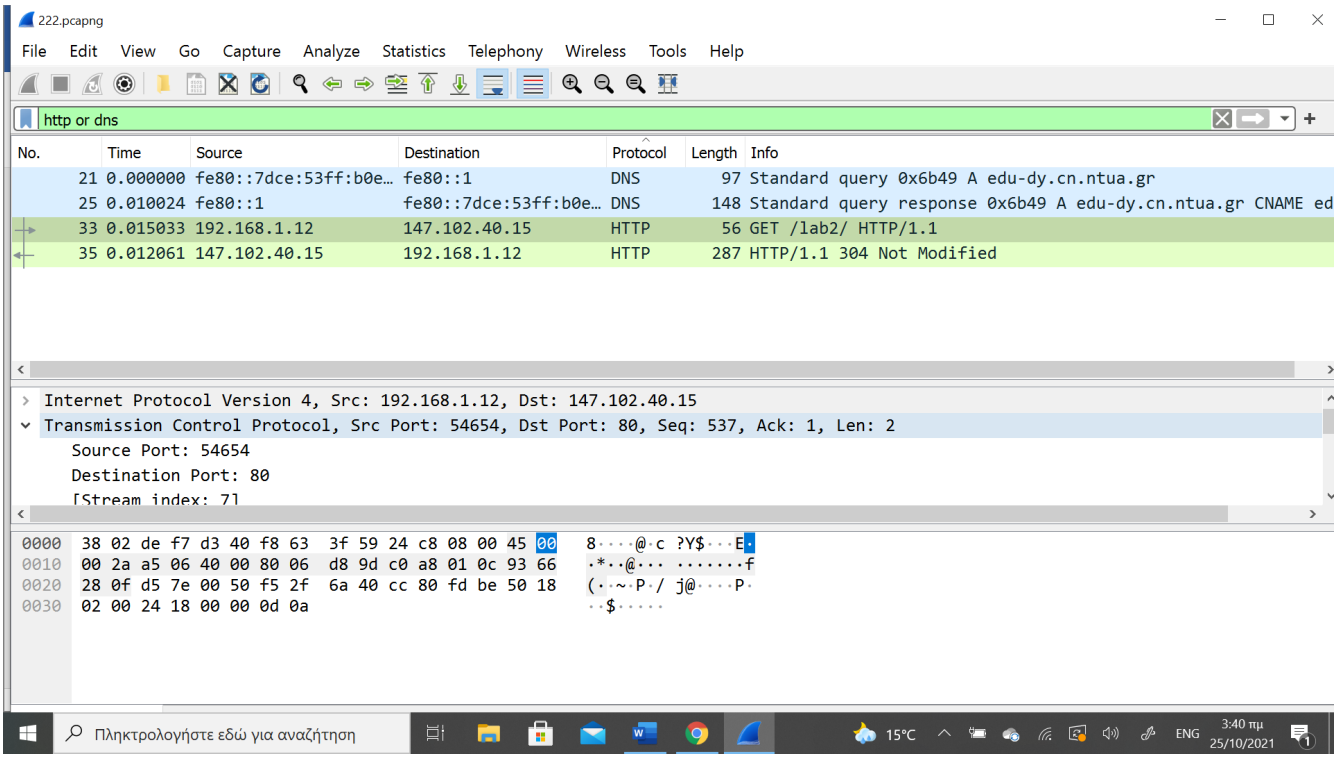


4.8 Είναι οι ίδιες.

4.9 Η θύρα 53

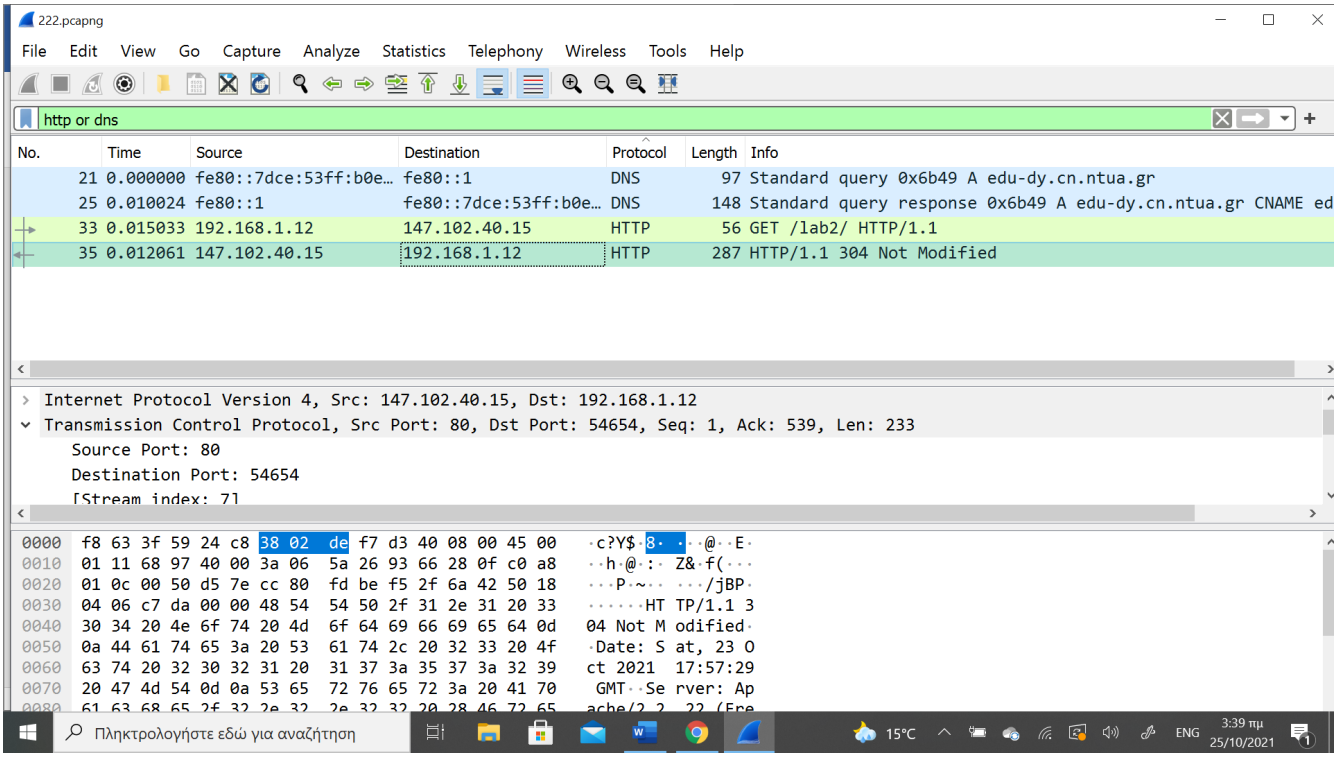
4.10 Η θύρα 80 (Destination)

4.11 Η 54654 (Source)



4.12 Η θύρα 80 (Source)

4.13 Η 54654 (Destination)

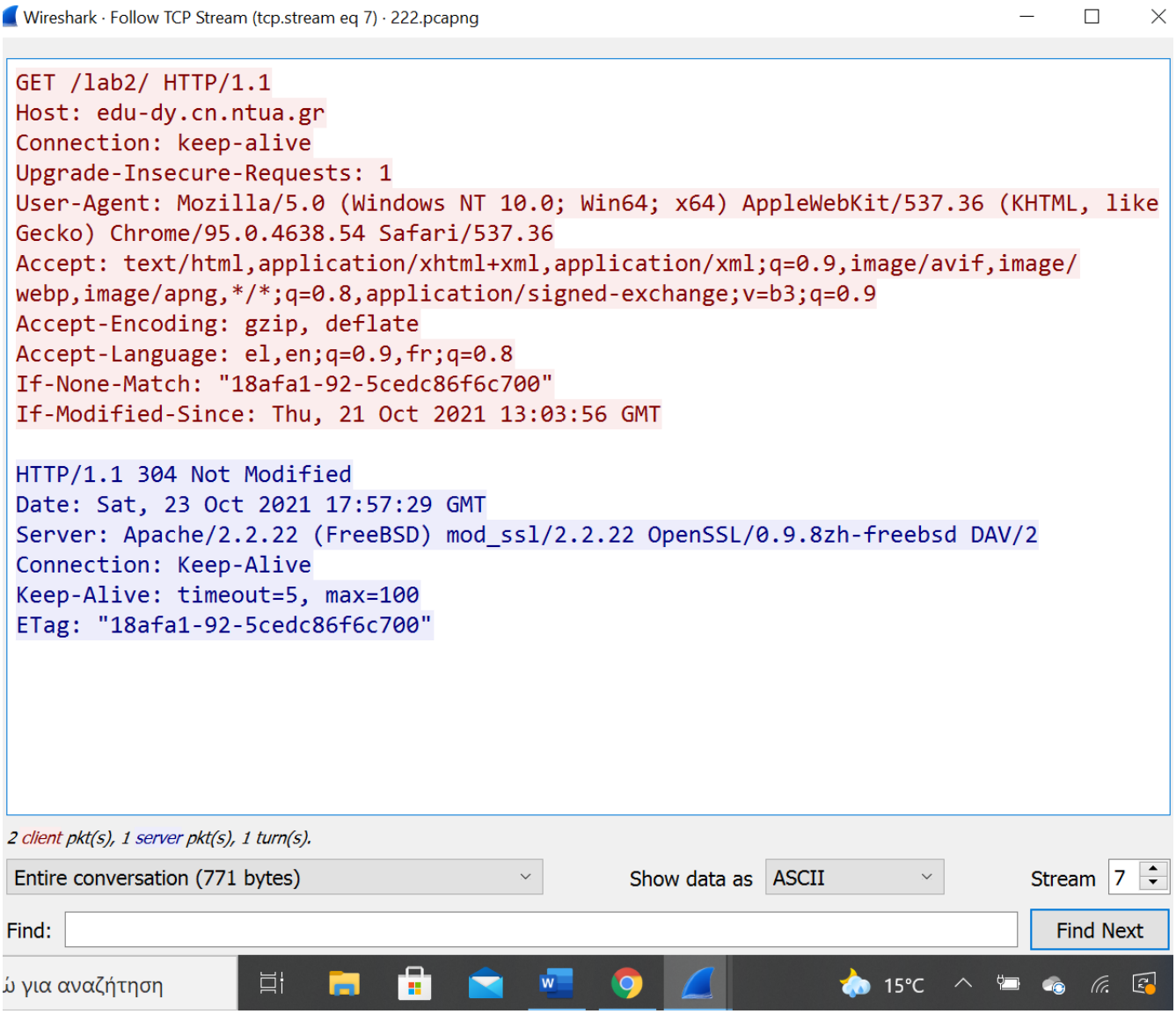


4.14 Η θύρα 80

4.15 Είναι οι ίδες θύρες

4.16 GET /lab2/ HTTP/1.1

4.17 HTTP/1.1 304 Not Modified



4.18 Με την εντολή ipconfig /flushdns καθαρίζουμε την DNS cache. Την 1η φορά που επισκεπτόμαστε μια ιστοσελιδα ναι μεν χρειάζεται η διαδικασία να γίνουν DNS queries πριν τη ληψη του πακέτου GET, αλλά θα χρειαστεί μονο μία φορά και τις υπόλοιπες φορες δεν θα χρειαστεί γιατι το αποτέλεσμα θα υπάρχει αποθηκευμένο στη μνήμη cache. Η εντολή χρειαζόταν για να δουμε αυτή τη μοναδική φορά που θα συμβεί ,τι περιέχουν τα πακέτα,τι ερωτήσεις κάνουν και σε ποιες διευθύνσεις και θύρες κάνουν ερωτήσεις κλπ