

<b>Όνοματεπώνυμο: Άγγελος Μητροκώτσας</b>		<b>Ομάδα: 6</b>
<b>Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2</b>		<b>Ημερομηνία: 27/ 10/ 2021</b>
<b>Διεύθυνση IP: 192.168.1.3</b>		<b>Διεύθυνση MAC: F8-63-3F-59-24-C8</b>

## Εργαστηριακή Άσκηση 6

### Πρωτόκολλο ICMP

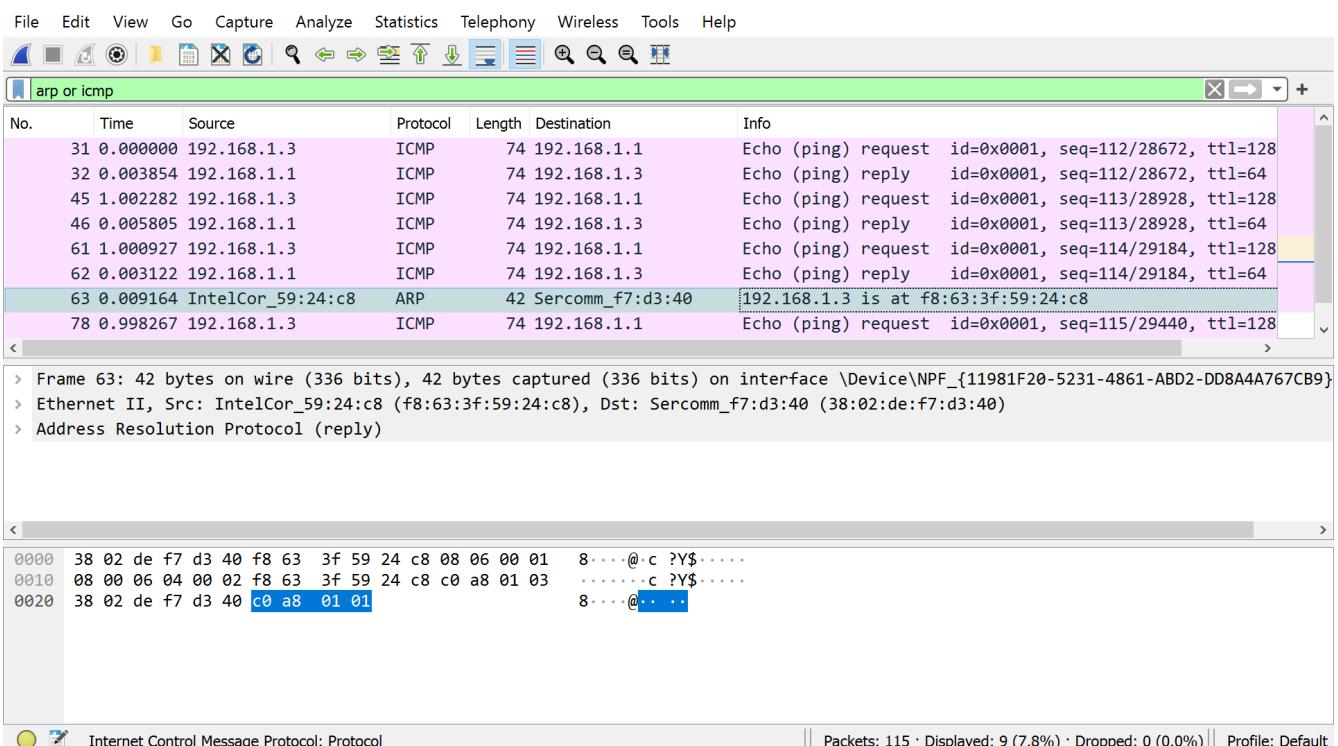
**Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.**

**1**

1.1 ether host F8-63-3F-59-24-C8

1.2 icmp or arp

1.3 Καταγράφηκαν (ένα) και σκοπός τους είναι να μετατρέπουν τις IP διευθύνσεις στις αντίστοιχες φυσικές, έτσι ώστε οι εφαρμογές να απαλλαγούν από αυτό το έργο. Στη συγκεκριμένη περίπτωση, σκοπός τους είναι να δείξουν στον υπολογιστή μας τη MAC διεύθυνση της προκαθορισμένης πύλης, στην οποία κάνουμε broadcast.



1.4 Όνομα του πεδίου : Protocol με τιμή ICMP (1) (ή (0x01))

\*Wi-Fi (ether host F8-63-3F-59-24-C8)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or icmp

No.	Time	Source	Protocol	Length	Destination	Info
31	0.000000	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=112/28672, ttl=128
32	0.003854	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=112/28672, ttl=64
45	1.002282	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=113/28928, ttl=128
46	0.005805	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=113/28928, ttl=64
61	1.000927	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=114/29184, ttl=128
62	0.003122	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=114/29184, ttl=64
63	0.009164	IntelCor_59:24:c8	ARP	42	Sercomm_f7:d3:40	192.168.1.3 is at f8:63:3f:59:24:c8
78	0.998267	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=115/29440, ttl=128

Identification: 0x5297 (21143)  
Flags: 0x00  
Fragment Offset: 0  
Time to Live: 128  
Protocol: ICMP (1)  
Header Checksum: 0x64d5 [validation disabled]

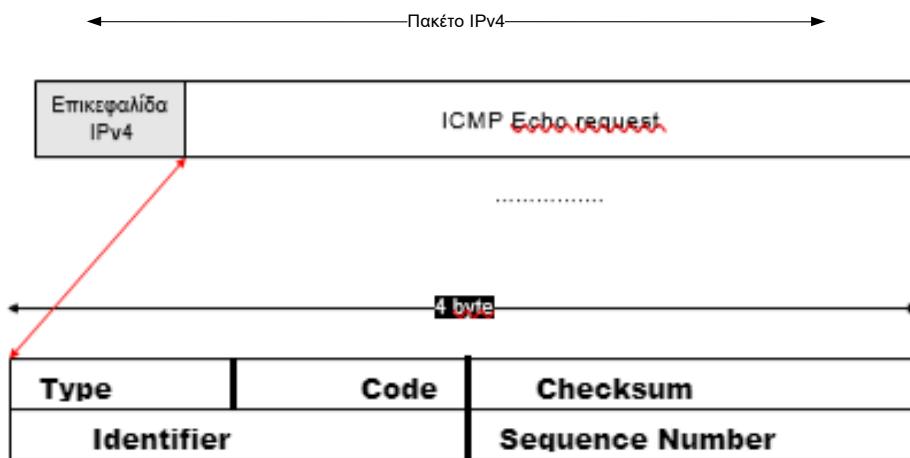
```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8.....@.c ?Y$...E.
0010 00 3c 52 97 00 00 80 01 64 d5 c0 a8 01 03 c0 a8 .<R.....d.....
0020 01 01 08 00 4c eb 00 01 00 70 61 62 63 64 65 66 ....L....pabcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

```

### 1.5 8 bytes

1.6 Type:1 byte, Code:1 byte, Checksum:2 bytes, Identifier:2 bytes, Sequence Number:2 bytes



### 1.7 Type: 8 (0x08), Code: 0 (0x00)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or icmp

No.	Time	Source	Protocol	Length	Destination	Info
31	0.000000	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=112/28672, ttl=128
32	0.003854	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=112/28672, ttl=64
45	1.002282	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=113/28928, ttl=128
46	0.005805	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=113/28928, ttl=64
61	1.000927	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=114/29184, ttl=128
62	0.003122	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=114/29184, ttl=64
63	0.009164	Intelcor_59:24:c8	ARP	42	Sercomm_f7:d3:40	192.168.1.3 is at f8:63:3f:59:24:c8
78	0.998267	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=115/29440, ttl=128

Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x4ceb [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8.....@.c ?Y$...E.
0010 00 3c 52 97 00 00 80 01 64 d5 c0 a8 01 03 c0 a8 .<R.....d.....
0020 01 01 08 00 4c eb 00 01 00 70 61 62 63 64 65 66 ....L....pabcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

```

1.8 Identifier: 1(0x001) (ιδίο σε όλα τα request), Sequence Number:113 (0x0071) (αλλάζει / ανυπόβατη κατά 1 σε κάθε request)

[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 113 (0x0071)  
Sequence Number (LE): 28928 (0x7100)  
[Response frame: 46]

0000	38 02 de f7 d3 40 f8 63	3f 59 24 c8 08 00 45 00	8...@c ?Y\$...E.
0010	00 3c 52 98 00 00 80 01	64 d4 c0 a8 01 03 c0 a8	<R.....d.....
0020	01 01 08 00 4c ea 00 01	00 71 61 62 63 64 65 66	....L...qabcdef
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67	68 69	wabdefg hi

1.9 Μήκος: 32 bytes, Περιεχόμενο: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73  
74 75 76 77 61 62 63 64 65 66 67 68 69

Sequence Number (BE): 113 (0x0071)  
Sequence Number (LE): 28928 (0x7100)  
[Response frame: 46]

▼ Data (32 bytes)  
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869  
[Length: 32]

0000	38 02 de f7 d3 40 f8 63	3f 59 24 c8 08 00 45 00	8...@c ?Y\$...E.
0010	00 3c 52 98 00 00 80 01	64 d4 c0 a8 01 03 c0 a8	<R.....d.....
0020	01 01 08 00 4c ea 00 01	00 71 61 62 63 64 65 66	....L...qabcdef
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67	68 69	wabdefg hi

1.10 Το μήκος είναι 8 bytes, ίδιο με αυτό των requests (έχουν την ίδια δομή)

1.11 Type: 0 (0x00), Code: 0 (0x00)

1.12 Το πεδίο Type, καθώς αυτό είναι που αλλάζει τιμή (8 για requests, 0 για replies). (Εξάλλου φαίνεται από το όνομά του ότι καθορίζει το είδος (ή αλλιως τον **ΤΥΠΟ**) των μηνύματος icmp )  
1.13 Identifier: 1(0x001) (ιδίο σε όλα τα replies), Sequence Number:113 (0x0071) (αλλάζει / ανυπόβατη κατά 1 σε κάθε reply)(ίδια με τις τιμές σε αυτά τα πεδία των αντίστοιχων requests)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or icmp

No.	Time	Source	Protocol	Length	Destination	Info
31	0.000000	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=112/28672, ttl=128
32	0.003854	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=112/28672, ttl=64
45	1.002282	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=113/28928, ttl=128
46	0.005805	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=113/28928, ttl=64
61	1.000927	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=114/29184, ttl=128
62	0.003122	192.168.1.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=114/29184, ttl=64
63	0.009164	IntelCor_59:24:c8	ARP	42	Sercomm_f7:d3:40	192.168.1.3 is at f8:63:3f:59:24:c8
78	0.998267	192.168.1.3	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=115/29440, ttl=128

```

Checksum: 0x54ea [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 113 (0x0071)
Sequence Number (LE): 28928 (0x7100)

```

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y$ 8. ...@..E.
0010 00 3c 88 b9 00 00 40 01 6e b3 c0 a8 01 01 c0 a8 ..<...@.n.....
0020 01 03 00 00 54 ea 00 01 00 71 61 62 63 64 65 66 ....T... .qabcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghiijklmn opqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

```

Identifier (big endian representation) (icmp.ident), 2 byte(s) | Packets: 115 · Displayed: 9 (7.8%) · Dropped: 0 (0.0%) | Profile: Default

#### 1.14 Είναι αυτά στο 1.8

1.15 Βοηθούν στο ταίριασμα των requests και των replies ένα προς ένα (στην αντιστοίχιση τους). Για να αντιστοιχηθούν ένα προς ένα τα replies στα πακέτα που έστειλα, έχουν το ίδιο Identifier και τους αντίστοιχους αύξοντες Sequence Numbers με τα requests τα οποία απαντούν. (Τα requests που στέλνω με την εντολή ping έχουν τον ίδιο identifier και ο sequence number αυξάνεται κατά 1 όσο μεταδίδω νέα πακέτα request)

1.16 32 bytes, το περιεχόμενο είναι ουσιαστικά αύξουσα ακολουθία αριθμών, ξεκινώντας από τον αριθμό  $01100001 = 6*16+1 = 97$

#### 1.17 Οχι

1.18 Κάθε αποτέλεσμα που εμφανίζει η εντολή ping είναι πληροφορία ενός πακέτου ICMP που στέλνει

1.19 ping <ip> -n 1

1.20 Εστειλα 3 ARP πακέτα και η ping τύπωσε Destination host unreachable

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp or arp

No.	Time	Source	Protocol	Length	Destination	Info
234	0.000000	IntelCor_59:24:c8	ARP	42	Broadcast	Who has 192.168.1.8? Tell 192.168.1.3
248	0.822285	IntelCor_59:24:c8	ARP	42	Broadcast	Who has 192.168.1.8? Tell 192.168.1.3
266	0.999425	IntelCor_59:24:c8	ARP	42	Broadcast	Who has 192.168.1.8? Tell 192.168.1.3

```

Frame 234: 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: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000 ff ff ff ff ff f8 63 3f 59 24 c8 08 06 00 01 .....c ?Y$.....
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 03 .....c ?Y$.....
0020 00 00 00 00 00 00 c0 a8 01 08 ..... ...

```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ping 192.168.1.8 -n 1
Pinging 192.168.1.8 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.1.8:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
PS C:\Windows\system32>
```

## 1.21 κάθε 1 δευτερόλεπτο

1.22 Κανένα (ίσως επρεπε να βγάλει ένα που λέει destination not reachable)

1.23 Για να φτάσει το κάθε icmp πακέτο στον προορισμό του πρέπει να ξέρει την MAC διεύθυνσή του (βλ 1.3 τον σκοπό των πακέτων πρωτοκόλλου arp). Αφού για τα πρώτα 3 broadcasts δεν έλαβε απάντηση ώστε να μάθει την MAC address του προορισμού και να στείλει τα icmp πακέτα, η εντολή υποθέτει ότι δεν γίνεται να φτάσει στον host που της δωσαμε.

## 2

### 2.1 Μετα την εντολή:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> ping 147.102.7.1

Pinging 147.102.7.1 with 32 bytes of data:
Reply from 147.102.7.1: bytes=32 time=15ms TTL=57
Reply from 147.102.7.1: bytes=32 time=13ms TTL=57
Reply from 147.102.7.1: bytes=32 time=13ms TTL=57
Reply from 147.102.7.1: bytes=32 time=13ms TTL=57

Ping statistics for 147.102.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 15ms, Average = 13ms
PS C:\Windows\system32> arp -a

Interface: 192.168.1.3 --- 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
PS C:\Windows\system32>
```

No.	Time	Source	Protocol	Length	Destination	Info
42	0.000000	192.168.1.3	ICMP	74	147.102.7.1	Echo (ping) request id=0x0001, seq=145/37120, ttl=128 (replicated)
43	0.015750	147.102.7.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=145/37120, ttl=57 (replicated)
55	0.998150	192.168.1.3	ICMP	74	147.102.7.1	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (replicated)
56	0.013363	147.102.7.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=146/37376, ttl=57 (replicated)
69	0.995619	192.168.1.3	ICMP	74	147.102.7.1	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (replicated)
70	0.013366	147.102.7.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=147/37632, ttl=57 (replicated)
89	0.991553	192.168.1.3	ICMP	74	147.102.7.1	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (replicated)
90	0.013522	147.102.7.1	ICMP	74	192.168.1.3	Echo (ping) reply id=0x0001, seq=148/37888, ttl=57 (replicated)
120	2.111268	IntelCor_59:24:c8	ARP	42	Sercomm_f7:d3:40	192.168.1.3 is at f8:63:3f:59:24:c8

> Frame 42: 74 bytes on wire (592 bits), 74 bytes captured (592 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)  
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 147.102.7.1  
> Internet Control Message Protocol

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$...E.  
0010 00 3c cf fc 00 00 80 01 0e b2 c0 a8 01 03 93 66 <..... .f  
0020 07 01 08 00 4c ca 00 01 00 91 61 62 63 64 65 66 ...L... abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghiijklmn opqrstuvwxyz  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Address Resolution Protocol: Protocol || Packets: 310 · Displayed: 9 (2.9%) · Dropped: 0 (0.0%) || Profile: Default

2.2 Source: f8:63:3f:59:24:c8, Destination: 38:02:de:f7:d3:40

2.3 Source: 192.168.1.3, Destination: 147.102.7.1

2.4 H 38:02:de:f7:d3:40 στην 147.102.7.1 και η f8:63:3f:59:24:c8 στην 192.168.1.3 (source στην source και destination στην destination προφανως)

## 2.5 val

2.6 Η ping στέλνει πακέτα σε εξωτερικό δίκτυο μέσω της προκαθορισμένης πύλης, την οποία έχω αποθηκευμένη στον arp πίνακα (βλ. και 1.3)

## 2.7 icmp.type == 0

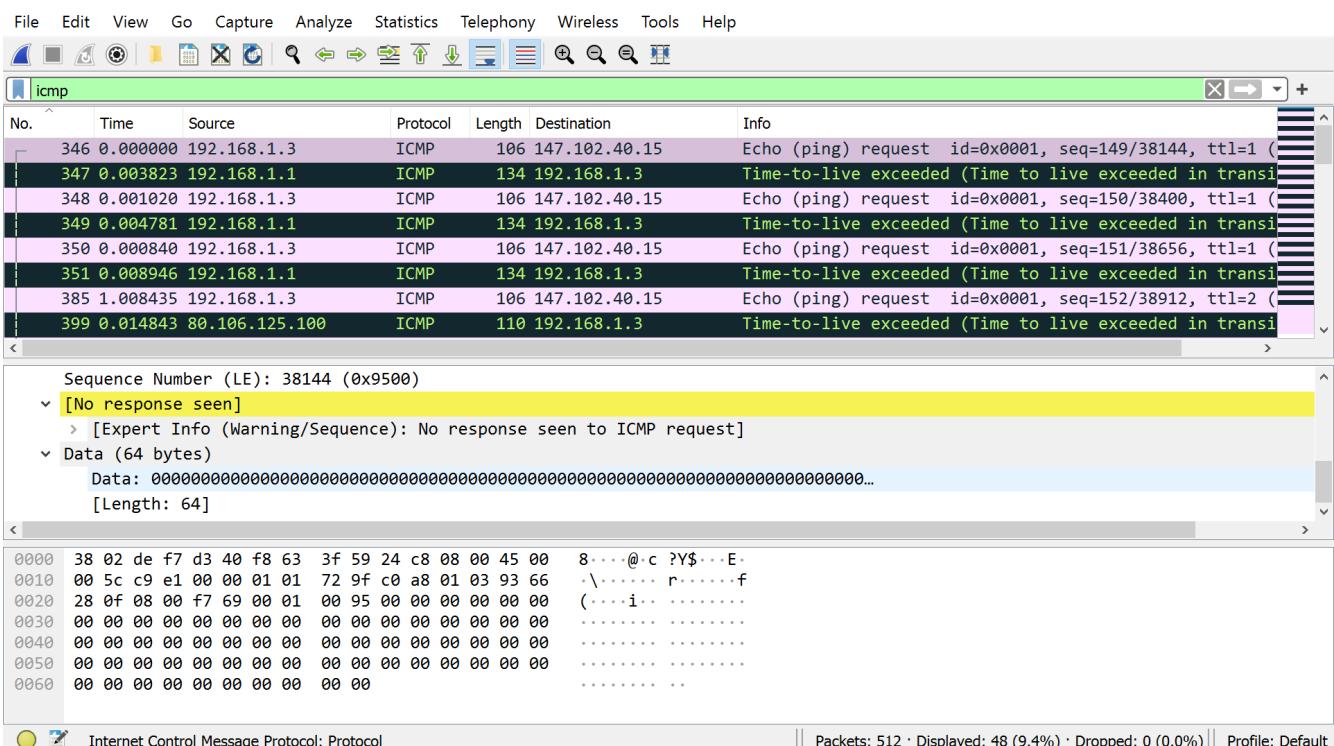
2.8 TTL = 57. Βλέπω ότι η τιμή σε όλα τα πακέτα είναι TTL = 57. Επίσης γνωρίζω ότι η προκαθορισμένη (default) τιμή TTL = 64. Οπότε αν υποθέσουμε ότι έχει αυτή την τιμή τότε το 57 που βλέπουμε υποδεικνύει ότι έγιναν 8 hops (κόμβους) μέχρι να φτάσει το πακέτο σε μένα (επιβεβαιώνεται τρέχοντας την tracert)

## 2.9 Εμφανίζονται ICMP Echo(ping) Request (Type: 8 (0x08))

2.10 Θεμελιώδης διαφορά είναι ότι στην περίπτωση του τοπικού μου δικτύου τα πακέτα ICMP δεν έφυγαν ποτέ, αφού δεν είχαν τη MAC διεύθυνση της συσκευής (του προορισμού τους) για να συμπληρωθεί η επικεφαλίδα Ethernet. Αντίθετα, αφού τα πακέτα σε εξωτερικά υποδίκτυα δρομολογούνται μέσω της προκαθορισμένης πυλης, έχουμε τη MAC διεύθυνση του προορισμού και αφού δεν γνωρίζουμε αν οι διευθύνσεις IPv4 αντιστοιχούν σε ενεργό κόμβο, τα πακέτα φεύγουν.

3

3.1 Μήκος: 64 bytes, Περιεχόμενο: μηδενικά.



3.2 Το μήκος όταν εκανα ping ήταν 32 bytes, τώρα είναι διπλασιο, και με ping το περιεχόμενο ήταν διαφορετικό (αύξοντες αριθμοί)

### 3.3 Time-to-live exceeded (Time to live exceeded in transit)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

Time	Source	Protocol	Length	Destination	Info
0.000000	192.168.1.3	ICMP	106	147.102.40.15	Echo (ping) request id=0x0001, seq=149/38144, ttl=1 (no resp...)
0.003823	192.168.1.1	ICMP	134	192.168.1.3	Time-to-live exceeded (Time to live exceeded in transit)
0.001020	192.168.1.3	ICMP	106	147.102.40.15	Echo (ping) request id=0x0001, seq=150/38400, ttl=1 (no resp...)
0.004781	192.168.1.1	ICMP	134	192.168.1.3	Time-to-live exceeded (Time to live exceeded in transit)
0.000840	192.168.1.3	ICMP	106	147.102.40.15	Echo (ping) request id=0x0001, seq=151/38656, ttl=1 (no resp...)
0.008946	192.168.1.1	ICMP	134	192.168.1.3	Time-to-live exceeded (Time to live exceeded in transit)
1.008435	192.168.1.3	ICMP	106	147.102.40.15	Echo (ping) request id=0x0001, seq=152/38912, ttl=2 (no resp...)
0.014843	80.106.125.100	ICMP	110	192.168.1.3	Time-to-live exceeded (Time to live exceeded in transit)

Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xf769 [unverified] [in ICMP error packet]  
[Checksum Status: Unverified]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 c0 .c?Y\$ 8 .@. E.  
0010 00 78 ba 34 00 00 40 01 3c 3c c0 a8 01 01 c0 a8 .x. 4 .@. <<....  
0020 01 03 0b 00 f4 ff 00 00 00 00 45 00 00 5c c9 e1 ..... .E .\..  
0030 00 00 01 01 72 9f c0 a8 01 03 93 66 28 0f 08 00 ..... r . .f(...  
0040 f7 69 00 01 00 95 00 00 00 00 00 00 00 00 00 00 00 .i.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Internet Control Message Protocol: Protocol | Packets: 512 · Displayed: 48 (9.4%) · Dropped: 0 (0.0%) | Profile: Default

### 3.4 Type: 11 (0x0b) (Time-to-live exceeded), Code:0 (Time to live exceeded in transit) (0x00)

\*Wi-Fi (host 192.168.1.3)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

Wireshark - Packet 347 · Wi-Fi (host 192.168.1.3)

No.	Time
346 0.0	
347 0.0	
348 0.0	
349 0.0	
350 0.0	
351 0.0	
385 1.0	
399 0.0	

> Frame 347: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF\_{^}

> Ethernet II, Src: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40), Dst: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3

> Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)  
Code: 0 (Time to live exceeded in transit)  
Checksum: 0xffff [correct]

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 c0 .c?Y\$ 8 .@. E.  
0010 00 78 ba 34 00 00 40 01 3c 3c c0 a8 01 01 c0 a8 .x. 4 .@. <<....  
0020 01 03 0b 00 f4 ff 00 00 00 00 45 00 00 5c c9 e1 ..... .E .\..  
0030 00 00 01 01 72 9f c0 a8 01 03 93 66 28 0f 08 00 ..... r . .f(...  
0040 f7 69 00 01 00 95 00 00 00 00 00 00 00 00 00 00 00 .i.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

### 3.5 Checksum: 2 bytes και Unused: 4 bytes

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3

> Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)  
Code: 0 (Time to live exceeded in transit)  
Checksum: 0xffff [correct]  
[Checksum Status: Good]  
Unused: 00000000

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 c0 .c?Y\$ 8 .@. E.  
0010 00 78 ba 34 00 00 40 01 3c 3c c0 a8 01 01 c0 a8 .x. 4 .@. <<....  
0020 01 03 0b 00 f4 ff 00 00 00 00 45 00 00 5c c9 e1 ..... .E .\..  
0030 00 00 01 01 72 9f c0 a8 01 03 93 66 28 0f 08 00 ..... r . .f(...  
0040 f7 69 00 01 00 95 00 00 00 00 00 00 00 00 00 00 00 .i.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

### 3.6 68 bytes

3.7 Το περιεχόμενο του μυνήματος λάθους είναι η επικεφαλίδα IPv4 του ληφθέντος ICMP request μυνήματος στον κόμβο και τα πρώτα 8 bytes του ICMP request μυνήματος που έλαβε. Κάποιοι από τους κόμβους επιστρέφουν και 40 bytes από το περιεχόμενο του ICMP request

## 4

### 4.1 1500, 1492, 1006, 576, 552, 544

```

Windows PowerShell

Pinging 147.102.40.15 with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\user> ping -n 1 -l 1492 147.102.40.15 -f

Pinging 147.102.40.15 with 1492 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\user> ping -n 1 -l 1006 147.102.40.15 -f

Pinging 147.102.40.15 with 1006 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\user> ping -n 1 -l 576 147.102.40.15 -f

Pinging 147.102.40.15 with 576 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\user> ping -n 1 -l 552 147.102.40.15 -f

Pinging 147.102.40.15 with 552 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\user> ping -n 1 -l 544 147.102.40.15 -f

Pinging 147.102.40.15 with 544 bytes of data:
Reply from 147.102.40.15: bytes=544 time=18ms TTL=57

Ping statistics for 147.102.40.15:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 18ms, Maximum = 18ms, Average = 18ms
PS C:\Users\user>

```

### 4.2 Όχι, τα βλεπω μονο στο powershell

### 4.3 Κανονικά έπρεπε να τα παράγει το router μου

### 4.4 Type: 3 (0x03), Code: 4 (0x04) (βρήκα στο google ότι είναι ετσι)

4.5 To Code: 4 δηλώνει ότι χρειαζόταν θρυμματισμός, ενώ η τιμή του πεδίου Next-Hop MTU είναι 1492.

4.6 Περιέχει 22 φορες τους δεκαεξαδικούς αριθμούς από 61 ως 77 (97 ως 120 στο 10δικο) και άλλα 14 bytes στο τέλος, 61-6e (τα νούμερα αυτά αντιστοιχούν σε λατινικού αλφαριθμητικού ASCII τιμές)

4.7 1492 bytes

4.8 Δεν απαντά για τις τιμές: 1500, 1492, 1006, 576, 552.

4.9 H 544

4.10 Το MTU που εμφανίζεται είναι ενός ενδιάμεσου κόμβου. Με την εντολή

tracert -4 147.102.40.15 βρίσκω το μονοπάτι που ακολουθήθηκε, στέλνω Echo Requests σε έναν έναν από τους ενδιάμεσους κόμβους και παρατηρώ ότι πάντα σταματάει η μετάδοση του πακέτου προτού φτάσω στον κόμβο προορισμού και πιο συγκεκριμένα, στον κόμβο grnet-2.gr-ix.gr [176.126.38.31]

4.11 Επειδή ο κόμβος που παρήγαγε το μήνυμα μαλλον έβαλε στα δεδομένα όλη την πληροφορία που έλαβε και έτσι ξεπέρασε το MTU σε κάποιο από τους κόμβους επιστροφής(αφού δεν είναι αυταραίτητα οι ίδιοι κόμβοι με αυτούς που περνάει όταν πηγαίνει ως εκεί)

4.12 Από την εντολή παράγονται 2 θραύσματα. Το μέγεθος του πακέτου συνολικά είναι 1514 Bytes, τα 14 Bytes είναι του Ethernet II, ενώ τα 20 προέρχονται από την επικεφαλίδα του IPv4 και τα υπόλοιπα 1480 αποτελούν τα δεδομένα. Προφανώς, οι τιμές είναι διάφορες του 1492 (λογικό να μην είναι η ίδια τιμή, αλλιώς δεν θα απαιτούταν θρυμματισμός).

## 5

5.1 ip host <ip> (το ip είναι το 147.102.40.15)

5.2 nslookup <ip> edu-dy.cn.ntua.gr (το ip είναι το 147.102.40.15)

5.3

 Windows PowerShell

```
PS C:\Users\user> nslookup 147.102.40.15 edu-dy.cn.ntua.gr
```

```
>>
```

```
DNS request timed out.
```

```
    timeout was 2 seconds.
```

```
Server: Unknown
```

```
Address: 147.102.40.15
```

```
DNS request timed out.
```

```
    timeout was 2 seconds.
```

```
*** Request to Unknown timed-out
```

```
PS C:\Users\user> ■
```

Το νόημά της είναι το Destination Unreachable που βλέπω και στο wireshark, δηλαδή θέλει να μας δείξει ότι η διεύθυνση του DNS δεν ακούει την συγκεκριμένη θύρα(port)

## 5.4 Ναι

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 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)  
 Internet Protocol Version 4, Src: 192.168.1.3, Dst: 147.102.40.15  
 User Datagram Protocol, Src Port: 49257, Dst Port: 53  
 Domain Name System (query)  
 TRANSUM RTE Data

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.3	DNS	86	147.102.40.15	Standard query 0x0001 PTR 15.40.102.147.in-addr.arpa
2	0.012660	147.102.40.15	ICMP	70	192.168.1.3	Destination unreachable (Port unreachable)
3	0.010983	192.168.1.3	DNS	86	147.102.40.15	Standard query 0x0002 PTR 15.40.102.147.in-addr.arpa
4	0.016521	147.102.40.15	ICMP	70	192.168.1.3	Destination unreachable (Port unreachable)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$..E.  
 0010 00 48 48 09 00 00 80 11 75 7b c0 a8 01 03 93 66 .HH.....u{....f  
 0020 28 0f c0 69 00 35 00 34 d7 49 00 01 01 00 00 01 (.i..5.4 ..I.....  
 0030 00 00 00 00 00 00 02 31 35 02 34 30 03 31 30 32 .....1 5.40 102  
 0040 03 31 34 37 07 69 6e 2d 61 64 64 72 04 61 72 70 .147.in-addr.arp  
 0050 61 00 00 0c 00 01 a.....

5.5 Το πρωτόκολλο μεταφοράς είναι το UDP (User Datagram Protocol) και η θύρα προορισμού είναι η 53 (Φαίνονται στο παραπάνω στιγμιότυπο οθόνης)

## 5.6 Ναι

Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.3  
 Internet Control Message Protocol  
 Type: 3 (Destination unreachable)  
 Code: 3 (Port unreachable)  
 Checksum: 0x64e0 [correct]  
 [Checksum Status: Good]  
 [Inlined: 00000000]

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.3	DNS	86	147.102.40.15	Standard query 0x0001 PTR 15.40.102.147.in-addr.arpa
2	0.012660	147.102.40.15	ICMP	70	192.168.1.3	Destination unreachable (Port unreachable)
3	0.010983	192.168.1.3	DNS	86	147.102.40.15	Standard query 0x0002 PTR 15.40.102.147.in-addr.arpa
4	0.016521	147.102.40.15	ICMP	70	192.168.1.3	Destination unreachable (Port unreachable)

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y\$ 8...@.E.  
 0010 00 38 49 05 00 00 39 01 bb 9f 93 66 28 0f c0 a8 .81...9...f(...  
 0020 01 03 03 64 e0 00 00 00 45 b8 00 48 48 09 ..i.d...E..HH..  
 0030 00 00 79 11 7b c3 c0 a8 01 03 93 66 28 0f c0 69 .y{....f(..i  
 0040 00 35 00 34 d7 49 .5.4.I

5.7 Type: 3 (0x03) Code: 3(0x03)

5.8 Το πεδίο Code

5.9 Η θύρα 53 είναι προκαθορισμένη για χρήση DNS Queries

5.10 Παρότι έχω windows, υποθέτω απαντά με ICMP Destination Unreachable (το ίδιο πράγμα ακριβώς δηλαδή)

## 6

### 6.1 ping -6 2001:648:2000:329::101 και tracert -6 2001:648:2000:329::101

```

Administrator: Windows PowerShell
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 16ms, Average = 15ms
PS C:\Windows\system32> ping -6 2001:648:2000:329::101

Pinging 2001:648:2000:329::101 with 32 bytes of data:
Reply from 2001:648:2000:329::101: time=14ms
Reply from 2001:648:2000:329::101: time=18ms
Reply from 2001:648:2000:329::101: time=15ms
Reply from 2001:648:2000:329::101: time=15ms

Ping statistics for 2001:648:2000:329::101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 18ms, Average = 15ms
PS C:\Windows\system32> tracert -6 2001:648:2000:329::101

Tracing route to 2001:648:2000:329::101 over a maximum of 30 hops
  1   2 ms    1 ms    6 ms  2a02:587:2129:d827:3a02:deff:fef7:d340
  2   *         *         * Request timed out.
  3   *         *         * Request timed out.
  4   *        10 ms    *  2a02:580:50da:471::1
  5  13 ms   15 ms   12 ms  grnet-2.gr-ix.gr [2001:7f8:6e::31]
  6  14 ms   14 ms   13 ms  ntua-zogr-2.koletir.access-link.grnet.gr [2001:648:2ffd:3323:2::2]
  7  13 ms   16 ms   12 ms  2001:648:2000:329::101

Trace complete.
PS C:\Windows\system32>

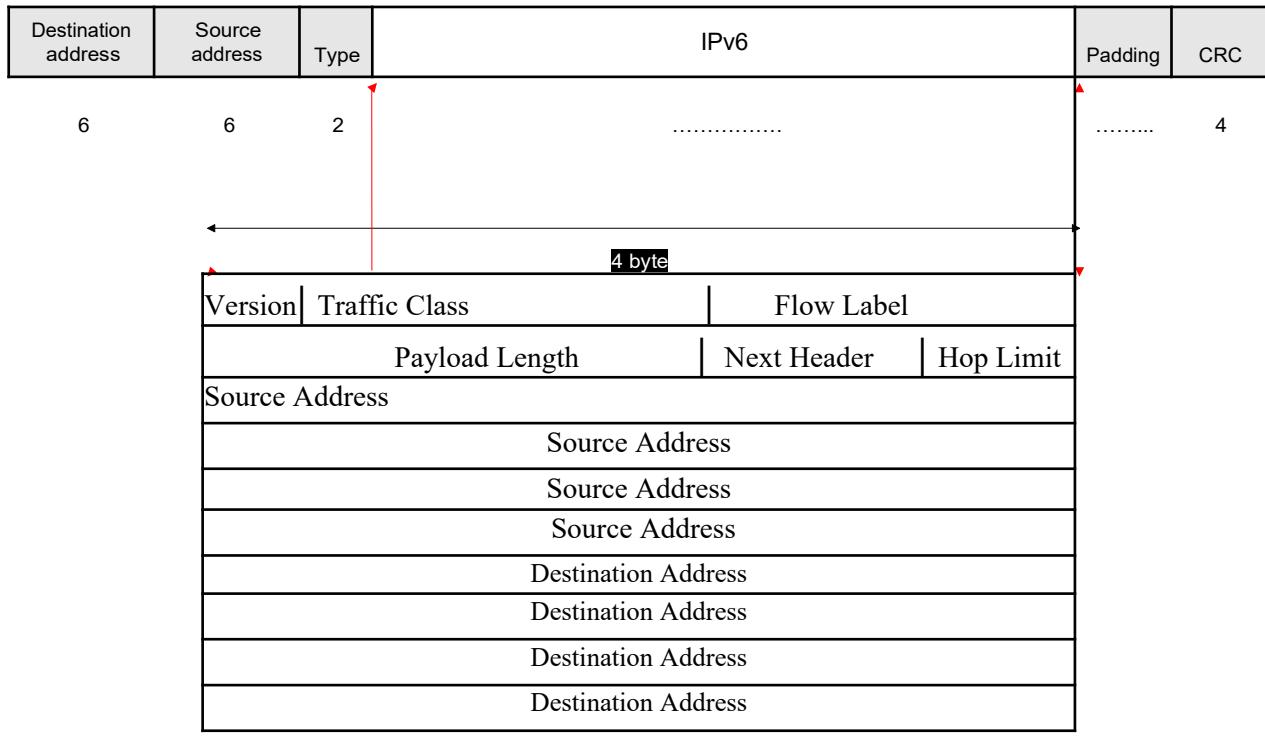
```

### 6.2 ip6, icmpv6

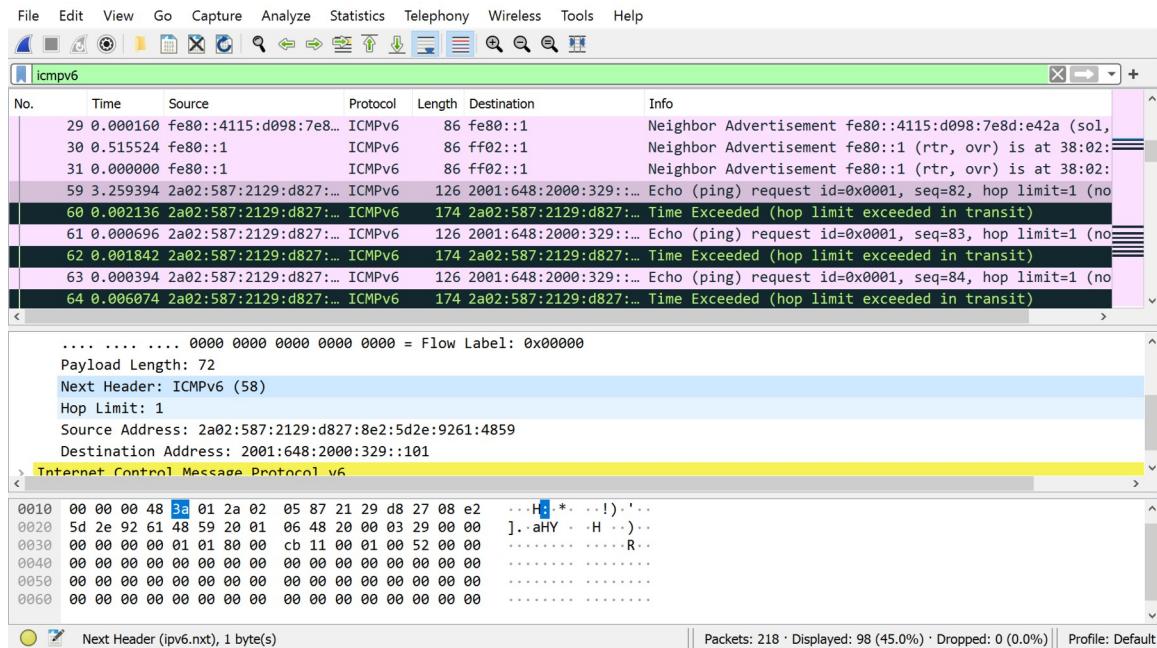
### 6.3 Type: IPv6 (0x86dd)

### 6.4 40 bytes

6.5 Version: 4 bits, Traffic Class: 8 bits, Flow Label: 4 bits + 2 bytes, Payload Length: 2 bytes, Next Header: 1 byte, Hop Limit: 1 byte, Source Address: 16 bytes, Destination Address: 16 bytes



## 6.6 H Hop Limit



## 6.7 To Next Header, η τιμή της ICMPv6 : 58 (0x3a)

### 6.8 Ναι

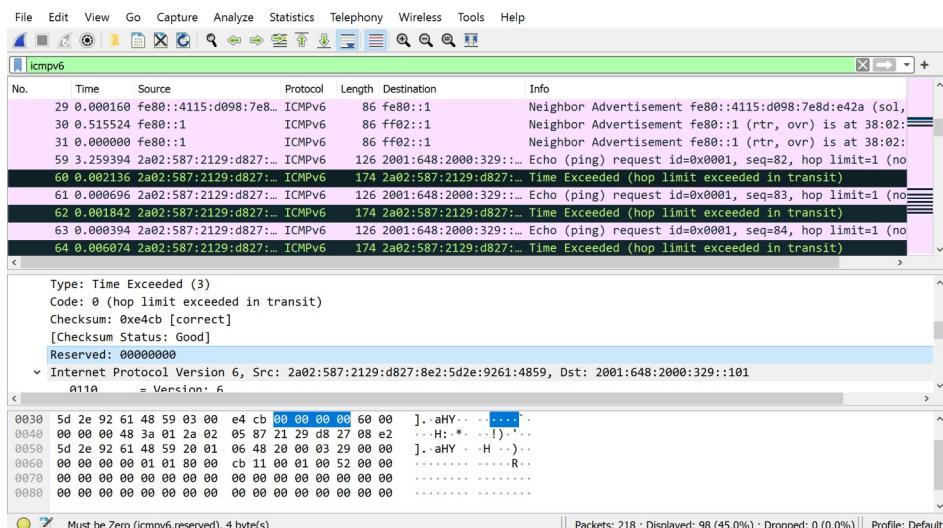
6.9 Type: 128(0x80), το μήκος των δεδομένων είναι 8 bytes

### 6.10 Ναι

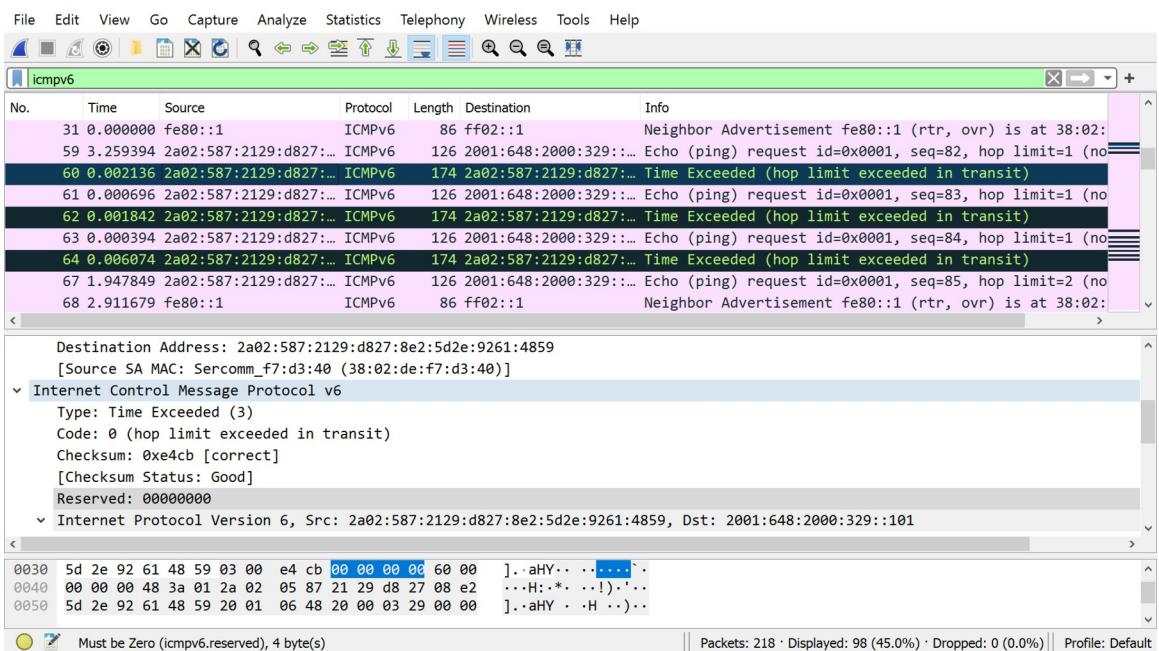
6.11 Type: 129(0x81), το μήκος των δεδομένων είναι 8 bytes

6.12 Διαφέρει στα πάντα εκτός από τα πεδία Type και Code.

6.13 Δεν είναι ίδια, διαφέρει μόνο στο ότι τώρα έχει το πεδίο Reversed εκεί που πρίν είχε το πεδίο Unused

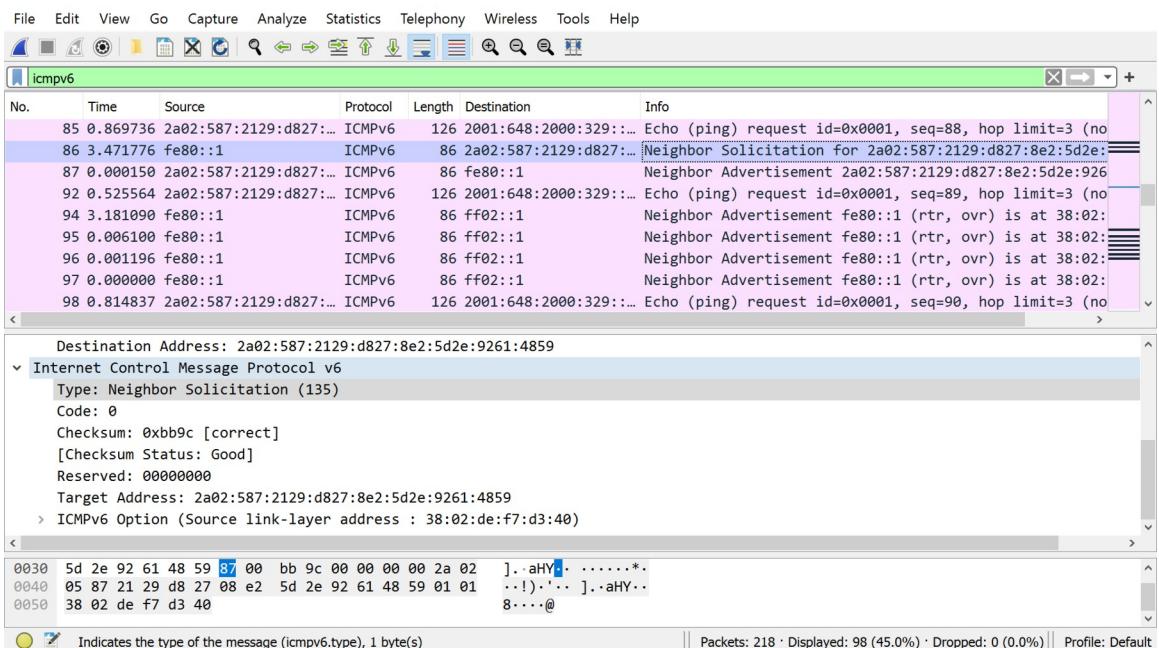


### 6.14 Type: Time Exceeded 3 (0x03), με μήκος δεδομένων 64 bytes.

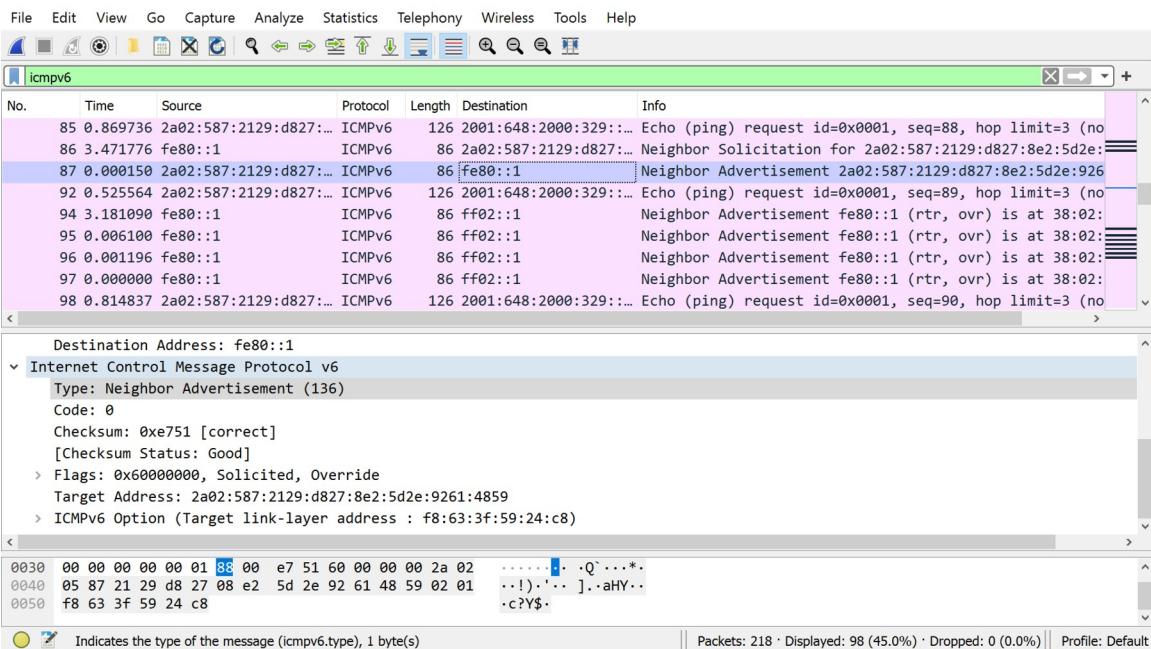


6.15 Τις επικεφαλίδες των IPv6 και ICMPv6 του μηνύματος που έλαβα μαζί με τα δεδομένα αυτού του μηνύματος.

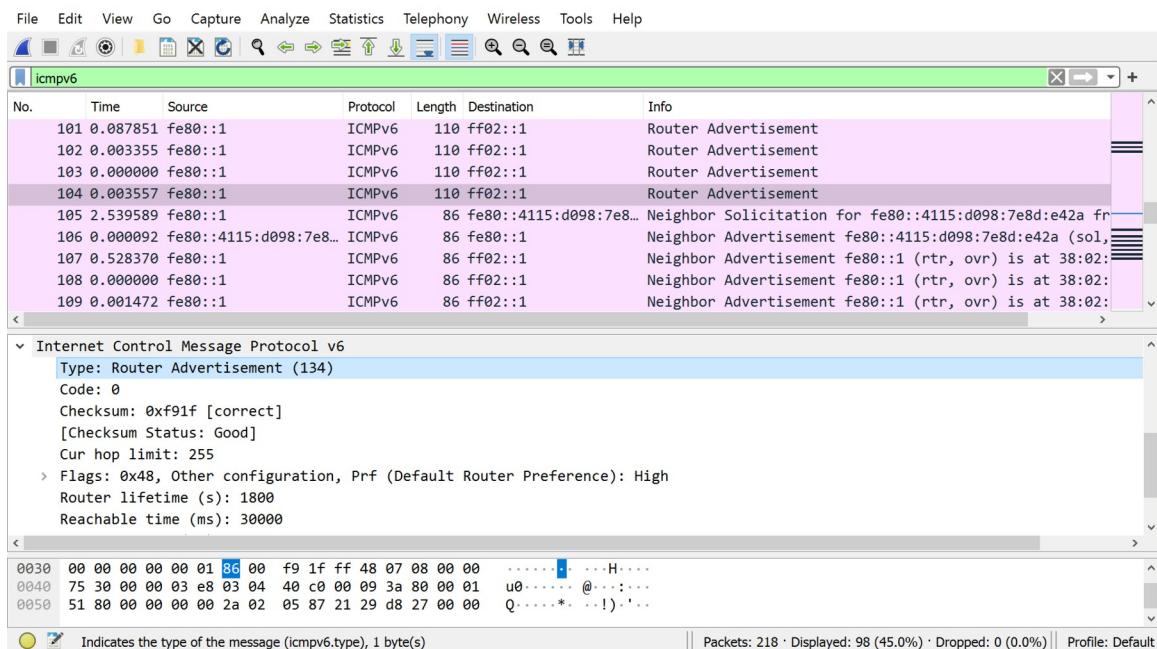
### 6.16 Ναι, παρατήρησα μηνύματα ICMPv6 Neighbor Solicitation,



## ICMPv6 Neighbor Advertisement



## και Router Advertisement



6.17 Type: Neighbor Solicitation (135) (0x87) με μήκος δεδομένων 32 bytes

Type: Neighbor Advertisement (136) (0x88) με μήκος δεδομένων 32 bytes

Type: Router Advertisement (134) (0x86) με μήκος δεδομένων 32 bytes