



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ  
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

## Δίκτυα Υπολογιστών

**Αναφορά δης Εργαστηριακής Άσκησης**

**Ραπτόπουλος Πέτρος (ει19145)  
Ομάδα 3**

# Άσκηση 1: Εντολή ping στο τοπικό δίκτυο

Ξεκινάμε μια καταγραφή με φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή μας. Καταγράφουμε τα διερχόμενα πλαίσια όταν κάνουμε ping σε μια διεύθυνση IPv4 υπολογιστή εντός του τοπικού δικτύου (την προκαθορισμένη πύλη). Αφού τελειώσει η καταγραφή, εφαρμόζουμε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με πρωτόκολλα ARP και ICMP.

1.1) Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας: **ether host 90:78:41:15:16:66**

1.2) Καταγράψτε τη σύνταξη του φίλτρου απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP: **arp or icmp**

```
petrosrapto@petrosraptoAssistant:~$ ping 147.102.236.200
PING 147.102.236.200 (147.102.236.200) 56(84) bytes of data.
64 bytes from 147.102.236.200: icmp_seq=1 ttl=255 time=5.11 ms
64 bytes from 147.102.236.200: icmp_seq=2 ttl=255 time=4.86 ms
64 bytes from 147.102.236.200: icmp_seq=3 ttl=255 time=5.22 ms
64 bytes from 147.102.236.200: icmp_seq=4 ttl=255 time=2.93 ms
64 bytes from 147.102.236.200: icmp_seq=5 ttl=255 time=2.60 ms
64 bytes from 147.102.236.200: icmp_seq=6 ttl=255 time=5.09 ms
64 bytes from 147.102.236.200: icmp_seq=7 ttl=255 time=3.94 ms
64 bytes from 147.102.236.200: icmp_seq=8 ttl=255 time=2.75 ms
64 bytes from 147.102.236.200: icmp_seq=9 ttl=255 time=11.6 ms
64 bytes from 147.102.236.200: icmp_seq=10 ttl=255 time=5.96 ms
^C
--- 147.102.236.200 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 2.601/5.008/11.633/2.474 ms
```

arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.000000000	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 7)
7	0.005062492	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 1)
8	0.996137051	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 9)
9	0.004827740	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 1)
10	0.997126483	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 1)
11	0.005183378	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 1)
12	0.995236480	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 1)
13	0.002893223	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 1)
16	0.998136173	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 1)
17	0.002572157	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=255 (request in 1)
18	0.998872452	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 1)
19	0.005049410	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=255 (request in 1)
22	0.996139487	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 1)
23	0.003897469	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=255 (request in 1)
24	0.997137661	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 1)
25	0.002706900	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=255 (request in 1)
28	0.999969647	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 1)
29	0.011602729	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=255 (request in 1)
30	0.990144720	147.102.236.33	147.102.236.200	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 1)
31	0.005921437	147.102.236.200	147.102.236.33	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=255 (request in 1)
32	5.044307713	IntelCor_15:16:66	Cisco_d0:d9:1d	ARP	42	Who has 147.102.236.200? Tell 147.102.236.33
33	0.004105897	Cisco_d0:d9:1d	IntelCor_15:16:66	ARP	56	147.102.236.200 is at 08:ec:f5:d0:d9:1d

1.3) Εάν καταγράφηκαν, εξηγήστε τον σκοπό των πακέτων πρωτοκόλλου ARP που ανταλλάχθηκαν:

Τα πακέτα πρωτοκόλλου ARP που ανταλλάχθηκαν φαίνονται στην ανωτέρω εικόνα.

Στέλνεται ένα ARP request από τον υπολογιστή μας ώστε να αντιστοιχίσει την διεύθυνση IPv4 που κάνει ping (τον default gateway) με το MAC της. Η προκαθορισμένη πύλη απαντάει στον υπολογιστή μας με ARP reply δίνοντας την διεύθυνση MAC της. Η διεύθυνση αυτή είναι απαραίτητη για να επιτευχθεί η επικοινωνία στο στρώμα ζεύξης δεδομένων (Ethernet).

1.4) Βρείτε το πρώτο μήνυμα Echo request του πρωτοκόλλου ICMP. Ποιο είναι το όνομα και η τιμή του πεδίου της επικεφαλίδας IPv4 που προσδιορίζει ότι πρόκειται για μήνυμα ICMP:: **Πεδίο: Protocol, Τιμή: 1**

1.5) Ποιο είναι το μήκος της επικεφαλίδας των μηνυμάτων ICMP Echo request:: **16 bytes**

1.6) Καταγράψτε ονόματα και μήκος σε byte των πεδίων της επικεφαλίδας των μηνυμάτων ICMP Echo request::

Type: 1 byte, Code: 1 byte, Checksum: 2 bytes, Identifier (BE)/(LE): 2 bytes, Sequence number (BE)/(LE): 2 bytes  
Timestamp from icmp data: 8 bytes

1.7) Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας των μηνυμάτων ICMP Echo request.: Type: 8, Code: 0

**1.8) Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και του αύξοντα αριθμού (Sequence number) της επικεφαλίδας ενός μηνύματος ICMP Echo request.:**

**Identifier (BE): 1, Identifier (LE): 256, Sequence number (BE): 1, Sequence number (LE): 256**

Σημείωση: (BE) συντομογραφία του big endian και (LE) συντομογραφία του little endian

No.	Time	Source	Destination	Protocol	Length	Info
6	0.0000000000	147.102.236.33	147.102.236.33	ICMP	80	Echo (ping) request 3d=0x0001, seq=1/256, ttl=64 (reply in 1)
7	0.0000000000	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=1/256, ttl=64 (reply in 1)
8	0.000137851	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=2/256, ttl=64 (reply in 9)
9	0.000482774	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=2/512, ttl=255 (request in 9)
10	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=3/256, ttl=64 (reply in 1)
11	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=3/512, ttl=255 (request in 1)
12	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=4/256, ttl=64 (reply in 1)
13	0.002893223	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=4/1024, ttl=255 (request in 1)
14	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=5/256, ttl=64 (reply in 1)
15	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=5/512, ttl=255 (request in 1)
16	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=6/256, ttl=64 (reply in 1)
17	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=6/512, ttl=255 (request in 1)
18	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=7/256, ttl=64 (reply in 1)
19	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=7/512, ttl=255 (request in 1)
20	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=8/256, ttl=64 (reply in 1)
21	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=8/512, ttl=255 (request in 1)
22	0.000139487	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=9/256, ttl=64 (reply in 1)
23	0.000139487	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=9/512, ttl=255 (request in 1)
24	0.000139487	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=10/256, ttl=64 (reply in 1)
25	0.002705690	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=10/512, ttl=255 (request in 1)
26	0.000996064	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=11/256, ttl=64 (reply in 1)
27	0.000996064	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=11/512, ttl=255 (request in 1)
28	0.011602727	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=12/256, ttl=64 (reply in 1)
29	0.011602727	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=12/512, ttl=255 (request in 1)
30	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 3d=0x0001, seq=13/256, ttl=64 (reply in 1)
31	0.0059521437	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 3d=0x0001, seq=13/512, ttl=255 (request in 1)
32	5.044307713	Cisco_0d:09:id	Cisco_0d:09:id	ARP	42	Who has 147.102.236.208? Tell 147.102.236.33
33	0.004105897	Cisco_0d:09:id	Cisco_0d:16:66	ARP	56	147.102.236.200 is at 08:ec:f5:d0:d9:1d

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=1/256, ttl=64 (reply in 1)
2	0.000137851	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=2/512, ttl=255 (request in 1)
3	0.000482774	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=3/256, ttl=64 (reply in 1)
4	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=4/512, ttl=255 (request in 1)
5	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=5/256, ttl=64 (reply in 1)
6	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=6/512, ttl=255 (request in 1)
7	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=7/256, ttl=64 (reply in 1)
8	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=8/512, ttl=255 (request in 1)
9	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=9/256, ttl=64 (reply in 1)
10	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=10/512, ttl=255 (request in 1)
11	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=11/256, ttl=64 (reply in 1)
12	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=12/512, ttl=255 (request in 1)
13	0.002893223	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=13/256, ttl=64 (reply in 1)
14	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=14/512, ttl=255 (request in 1)
15	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=15/256, ttl=64 (reply in 1)
16	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=16/512, ttl=255 (request in 1)
17	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=17/256, ttl=64 (reply in 1)
18	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=18/512, ttl=255 (request in 1)
19	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=19/256, ttl=64 (reply in 1)
20	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=20/512, ttl=255 (request in 1)
21	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=21/256, ttl=64 (reply in 1)
22	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=22/512, ttl=255 (request in 1)
23	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=23/256, ttl=64 (reply in 1)
24	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=24/512, ttl=255 (request in 1)
25	0.002705690	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=25/256, ttl=64 (reply in 1)
26	0.000996064	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=26/512, ttl=255 (request in 1)
27	0.011602727	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=27/256, ttl=64 (reply in 1)
28	0.011602727	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=28/512, ttl=255 (request in 1)
29	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=29/256, ttl=64 (reply in 1)
30	0.000126486	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) reply 1d=0x0001, seq=30/512, ttl=255 (request in 1)
31	0.0059521437	147.102.236.33	147.102.236.33	ICMP	96	Echo (ping) request 1d=0x0001, seq=31/256, ttl=64 (reply in 1)
32	5.044307713	Cisco_0d:09:id	Cisco_0d:16:66	ARP	42	Who has 147.102.236.208? Tell 147.102.236.33
33	0.004105897	Cisco_0d:09:id	Cisco_0d:16:66	ARP	56	147.102.236.200 is at 08:ec:f5:d0:d9:1d

**Echo Request**

**Echo Reply**

**1.9) Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή ping;: Μήκος: 48 bytes, Περιεχόμενο του πεδίου δεδομένων: Τυχαία πληροφορία**

(Σημείωση: Δεν είναι υποχρεωτικό το μέγεθος του data θα είναι μεγαλύτερο από μηδέν).

Αποσκοπεί στον έλεγχο της σύνδεσης, καθώς το Echo Reply υποχρεούται να συμπεριλάβει τα data του Echo Request. Συνεπώς ο αποστολέας του Echo Request μόλις παραλάβει το Echo Reply μπορεί να ελέγξει πόσα από τα bit του πεδίου data είναι εσφαλμένα.

Ακόμη αποσκοπεί στον έλεγχο του θρυμματισμού κατά μήκος μιας σύνδεσης.

**1.10) Βρείτε ένα μήνυμα Echo reply του πρωτοκόλλου ICMP. Ποιο είναι το μήκος της επικεφαλίδας μηνυμάτων ICMP Echo reply;: 16 bytes Έχει την ίδια δομή με αυτή του Echo request;: Ναι έχει την ίδια δομή.**

**1.11) Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP των μηνυμάτων Echo reply.: Type: 0, Code: 0**

**1.12) Με βάση τις απαντήσεις σας στις ερωτήσεις 1.7 και 1.11, ποιο από τα πεδία Type και Code καθορίζει το είδους του μηνύματος ICMP;: Το πεδίο Type**

**1.13) Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και αύξοντα αριθμού (Sequence number) της επικεφαλίδας ICMP ενός μηνύματος Echo reply.: Identifier (BE): 1, Identifier (LE): 6, Sequence number (BE): 6, Sequence number (LE): 6 (Ιδιες με 1.13)**

**1.14) Εντοπίστε το μήνυμα ICMP Echo request σε απάντηση του οποίου παράχθηκε το προηγούμενο μήνυμα ICMP Echo reply. Ποιες είναι οι αντίστοιχες τιμές των πεδίων ταυτότητας και αύξοντα αριθμού;**

**Identifier (BE): 1, Identifier (LE): 256, Sequence number (BE): 6, Sequence number (LE): 6 (Ιδιες με 1.13)**

**1.15) Ποιος νομίζετε ότι είναι ο ρόλος των πεδίων ταυτότητας και αύξοντα αριθμού στην επικεφαλίδα των μηνυμάτων ICMP Echo request και Echo reply;**

**Ο ρόλος τους είναι η αντιστοίχιση των Echo Reply στα Echo Request που τα προκάλεσαν.**

**1.16) Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo reply;**

**Μήκος: 48 bytes, Περιεχόμενο: Το περιεχόμενο του data πεδίου του αντίστοιχου Echo Request.**

**1.17) Διαφέρει αυτό το περιεχόμενο από το αντίστοιχο του μηνύματος ICMP Echo request; Εν γένει ταυτίζονται. Αν υπάρχει διαφορά σε κάποια bits σημαίνει ότι έγινε σφάλμα κατά την μετάδοση.**

- 1.18) Πώς σχετίζονται οι ανταλλαγές μηνυμάτων ICMP με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών; Κάθε γραμμή στα αποτελέσματα της εντολής ping στο terminal αντιστοιχεί σε ένα Echo Request. Αναγράφεται το μήκος του προς αποστολή πακέτου (64 bytes) το οποίο έρχεται σε συμφωνία με το μέγεθος του ICMP πακέτου (IPv4(Total Length)-IPv4(Header Length)), όπως φαίνεται στο Wireshark. Επίσης αναγράφεται το Sequence Number που ανατίθεται σε κάθε πακέτο που αποστέλλεται. Μόλις ολοκληρωθεί η ping, αναγράφεται πόσα πακέτα στάλθηκαν(Echo Requests) και πόσα λήφθηκαν(Echo Replies).**

Ξεκινάμε πάλι τη διαδικασία καταγραφής των πακέτων με το ίδιο φίλτρο σύλληψης και εκτελούμε την εντολή ping προς μια διεύθυνση IPv4 που δεν αντιστοιχεί σε ενεργό υπολογιστή του τοπικού μας δικτύου ζητώντας να παραχθούν δύο μηνύματα ICMP Echo request.

Αφού τελειώσει η καταγραφή, εφαρμόζουμε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

```
petrosrapto@petrosraptoAssistant:~$ ping -c 2 147.102.236.32
PING 147.102.236.32 (147.102.236.32) 56(84) bytes of data.
From 147.102.236.33 icmp_seq=1 Destination Host Unreachable
From 147.102.236.33 icmp_seq=2 Destination Host Unreachable

--- 147.102.236.32 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1019ms
pipe 2
```

arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000000	IntelCor_15:16:66	Broadcast	ARP	42	Who has 147.102.236.32? Tell 147.102.236.33
4	0.219905031	84:14:4d:30:4a:bc	IntelCor_15:16:66	ARP	56	147.102.203.252 is at 84:14:4d:30:4a:bc
5	0.007639396	a0:e7:0b:f2:1f:5c	IntelCor_15:16:66	ARP	56	147.102.239.199 is at a0:e7:0b:f2:1f:5c
6	0.791273922	IntelCor_15:16:66	Broadcast	ARP	42	Who has 147.102.236.32? Tell 147.102.236.33
19	1.023959996	IntelCor_15:16:66	Broadcast	ARP	42	Who has 147.102.236.32? Tell 147.102.236.33
20	0.160546456	84:14:4d:30:4a:bc	IntelCor_15:16:66	ARP	56	147.102.203.252 is at 84:14:4d:30:4a:bc
21	0.000000090	a0:e7:0b:f2:1f:5c	IntelCor_15:16:66	ARP	56	147.102.239.199 is at a0:e7:0b:f2:1f:5c
22	0.000000080	7c:21:4a:35:09:ad	IntelCor_15:16:66	ARP	56	147.102.237.118 is at 7c:21:4a:35:09:ad
41	40.579004747	IntelCor_15:16:66	Cisco_d0:d9:1d	ARP	42	Who has 147.102.236.200? Tell 147.102.236.33
42	0.002170226	Cisco_d0:d9:1d	IntelCor_15:16:66	ARP	56	147.102.236.200 is at 08:ec:f5:d0:d9:1d

- 1.19) Ποια σύνταξη της εντολής ping χρησιμοποιήσατε ώστε να παραχθούν δύο μηνύματα ICMP;;:**

```
ping -c 2 147.102.236.32
```

- 1.20) Πόσα πακέτα ARP request στάλθηκαν για την ανεύρεση της διεύθυνσης MAC του μη ενεργού υπολογιστή;; 3**

**1.21) Κάθε πότε στέλνονται; Περίπου κάθε ένα δευτερόλεπτο.**

**1.22) Πόσα μηνύματα ICMP στάλθηκεν; Δεν στάλθηκε κανένα μήνυμα ICMP.**

**1.23) Πώς σχετίζονται τα προηγούμενα με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;**

**Στο terminal για κάθε απόπειρα αποστολής πακέτου αναγράφεται "Destination Host Unreachable".**

Αυτό γιατί ο υπολογιστής μας δεν λαμβάνει ARP reply (όπως φαίνεται στο Wireshark) και συνεπώς δεν γνωρίζει την διεύθυνση MAC του υπολογιστή που θέλει να στείλει το πλαίσιο.

## Άσκηση 2: Εντολή ping σε άλλο υποδίκτυο

Πίνακας ARP του υπολογιστή μας:

Address	HWtype	HWaddress	Flags	Mask	Iface
147.102.236.32	(incomplete)				wlp1s0
_gateway	ether	08:ec:f5:d0:d9:1d	C		wlp1s0
147.102.236.230	ether	00:50:56:b5:aa:aa	C		wlp1s0

Χρησιμοποιώντας το φίλτρο σύλληψης των προηγούμενων ερωτήσεων, καταγράφουμε τα διερχόμενα πλαίσια όταν κάνουμε ping σε έναν υπολογιστή εκτός του τοπικού δικτύου (IPv4 διεύθυνση 147.102.1.1)

Αφού τελειώσει η καταγραφή εφαρμόζουμε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

```

petrosrapto@petrosraptoAssistant:~$ ping 147.102.1.1
PING 147.102.1.1 (147.102.1.1) 56(84) bytes of data.
64 bytes from 147.102.1.1: icmp_seq=1 ttl=63 time=6.25 ms
64 bytes from 147.102.1.1: icmp_seq=2 ttl=63 time=4.41 ms
64 bytes from 147.102.1.1: icmp_seq=3 ttl=63 time=2.83 ms
64 bytes from 147.102.1.1: icmp_seq=4 ttl=63 time=8.70 ms
64 bytes from 147.102.1.1: icmp_seq=5 ttl=63 time=2.69 ms
64 bytes from 147.102.1.1: icmp_seq=6 ttl=63 time=2.53 ms
64 bytes from 147.102.1.1: icmp_seq=7 ttl=63 time=2.62 ms
64 bytes from 147.102.1.1: icmp_seq=8 ttl=63 time=3.09 ms
^C
--- 147.102.1.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.527/4.138/8.699/2.095 ms

```

**2.1)** Καταγράψτε τις διευθύνσεις IPv4 που περιέχει ο πίνακας arp μετά την παραπάνω καταγραφή:

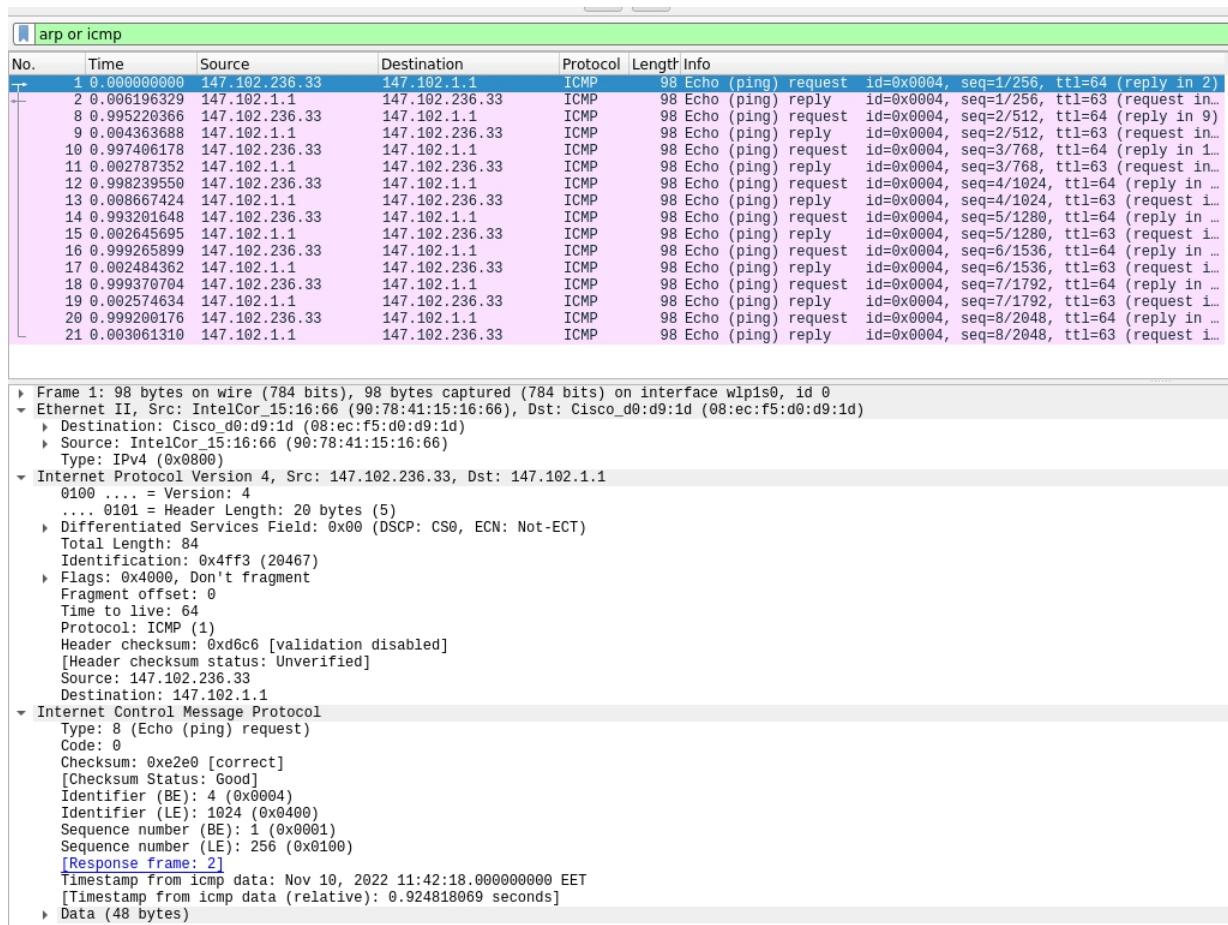
```

petrosrapto@petrosraptoAssistant:~$ arp
Address          HWtype  HWaddress          Flags Mask   Iface
147.102.236.32      ether  08:ec:f5:d0:d9:1d  C      wlp1s0
_gateway          ether  00:50:56:b5:aa:aa  C      wlp1s0
147.102.236.230      ether  00:50:56:b5:aa:aa  C      wlp1s0

```

**2.2)** Επιλέξτε ένα μήνυμα ICMP Echo request. Καταγράψτε τη διεύθυνση MAC του αποστολέα και του παραλήπτη του αντίστοιχου πλαισίου.: **MAC αποστολέα: 90:78:41:15:16:66**

**MAC παραλήπτη: 08:ec:f5:d0:d9:1d (διεύθυνση MAC του default\_gateway)**



**2.3)** Καταγράψτε τις διευθύνσεις IPv4 (αποστολέα και παραλήπτη) του πακέτου IPv4 που μεταφέρει το μήνυμα ICMP Echo request: **IPv4 αποστολέα: 147.102.236.33, IPv4 παραλήπτη: 147.102.1.1**

**2.4)** Οι παραπάνω διευθύνσεις MAC σε ποιες διευθύνσεις IPv4 αντιστοιχούν;;

Η διεύθυνση MAC αποστολέα αντιστοιχεί στην διεύθυνση IPv4 αποστολέα (MAC, IPv4 του υπολογιστή μας)

Η διεύθυνση MAC παραλήπτη αντιστοιχεί στην διεύθυνση IPv4 της προκαθορισμένης πύλης (147.102.236.200).

**2.5)** Παρατηρήσατε πακέτα πρωτοκόλλου ARP κατά την καταγραφή; **Όχι**

**2.6)** Αν ναι, ποιος ήταν ο σκοπός τους; Εάν όχι, αιτιολογήστε γιατί δεν υπήρξαν.

Η διεύθυνση IPv4 που κάνουμε ping δεν είναι εντός τοπικού δικτύου. Η κάρτα δικτύου το αντιλαμβάνεται αφού έχει

στην κατοχή της την δικιά της IPv4, την μάσκα υποδικτύου και την IPv4 του παραλήπτη.

Συνεπώς το πλαίσιό μας θα μεταδοθεί μέσω του πρωτοκόλλου Ethernet πρώτα στην προκαθορισμένη πύλη, για την οποία έχει αποθηκευτεί η διεύθυνση MAC της στο arp table του υπολογιστή μας.

Συνεπώς δεν υπάρχει ανάγκη για ARP request.

Αφού απενεργοποιήσουμε το προηγούμενο φίλτρο απεικόνισης, εφαρμόζουμε ένα νέο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα ICMP Echo reply.

## 2.7) Να καταγραφεί η σύνταξη του: icmp.type == 0

2.8) Παρατηρώντας τις τιμές των πεδίων της επικεφαλίδας των πακέτων IPv4 που μεταφέρουν το μήνυμα ICMP Echo reply, εξηγήστε πώς προκύπτει η τιμή της παραμέτρου TTL που εμφανίζεται στις απαντήσεις του παραθύρου εντολών. Παρατηρούμε ότι η τιμή στο πεδίο Time to live είναι 63. Το ίδιο αναγράφεται και στο terminal.

Ξεκινάμε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης, όταν εκτελούμε την εντολή ping σε έναν υπολογιστή εκτός του υποδικτύου σας, που δεν είναι ενεργός (στον 147.102.7.90).

Όταν τελειώσει η καταγραφή εφαρμόζουμε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

```
petrosrapto@petrosraptoAssistant:~$ ping 147.102.7.90
PING 147.102.7.90 (147.102.7.90) 56(84) bytes of data.
^C
--- 147.102.7.90 ping statistics ---
52 packets transmitted, 0 received, 100% packet loss, time 52206ms
```

No.	Time	Source	Destination	Protocol	Length	Info
11	0.000000000	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=1/256 ttl=64 (no respons...
12	1.002021208	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=2/512 ttl=64 (no respons...
19	1.024047584	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=3/768 ttl=64 (no respons...
20	1.027953692	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=4/1024 ttl=64 (no respons...
21	1.019982484	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=5/1280 ttl=64 (no respons...
22	1.024016210	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=6/1536 ttl=64 (no respons...
24	1.024013690	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=7//1792 ttl=64 (no respons...
26	1.027993953	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=8/2048 ttl=64 (no respons...
28	1.020281688	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=9/2384 ttl=64 (no respons...
29	1.023737764	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=10/2560 ttl=64 (no respons...
30	1.024619116	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=11/2816 ttl=64 (no respons...
31	1.023997992	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=12/3072 ttl=64 (no respons...
33	1.023438378	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=13/3328 ttl=64 (no respons...
34	1.024398674	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=14/3584 ttl=64 (no respons...
35	1.023756155	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=15/3840 ttl=64 (no respons...
36	1.023997591	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=16/4096 ttl=64 (no respons...
38	1.028377952	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=17/4352 ttl=64 (no respons...
41	1.019586174	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=18/4608 ttl=64 (no respons...
42	1.023973694	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=19/4864 ttl=64 (no respons...
43	1.024047206	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=20/5120 ttl=64 (no respons...
44	1.023962416	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=21/5376 ttl=64 (no respons...
46	1.024913439	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=22/5632 ttl=64 (no respons...
47	1.023981990	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=23/5888 ttl=64 (no respons...
48	1.024009285	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=24/6144 ttl=64 (no respons...
49	1.027990601	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=25/6400 ttl=64 (no respons...
50	1.028220738	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=26/6656 ttl=64 (no respons...
51	1.023809105	147.102.236.33	147.102.7.90	ICMP	98	Echo (ping) request id=0x0005 seq=27/6912 ttl=64 (no respons...

## 2.9) Ποιοι τύποι μηνυμάτων ICMP εμφανίζονται; Εμφανίζονται μόνο ICMP Echo Requests

2.10) Σε τι διαφέρει η κίνηση που καταγράψατε σε σχέση με την αντίστοιχη όταν εκτελέσατε την προηγούμενως ping προς μια διεύθυνση IPv4 εκτός του υποδικτύου σας, που δεν αντιστοιχεί σε ενεργό υπολογιστή.

Αιτιολογήστε τη διαφορά.

-Στην Άσκηση 1 κάνοντας ping σε διεύθυνση IPv4 εκτός του τοπικού δικτύου η κάρτα δικτύου αντιλήφθηκε ότι ο εν λόγω υπολογιστής βρίσκεται στο ίδιο υποδίκτυο και δεν έστειλε το πακέτο στον δρομολογητή. Αντίθετα έκανε broadcast ARP request ώστε να λάβει την διεύθυνση MAC του υπολογιστή στόχου. Ο υπολογιστής-στόχος δεν απαντούσε και είχαμε επανεκπομπή ARP request. Εν τέλει δεν λήφθηκε η διεύθυνση MAC του υπολογιστή-στόχου και πλαίσιο με ενθυλακωμένο πακέτο ICMP request δεν στάλθηκε ποτέ.

-Αντίθετα στην Άσκηση 2 η κάρτα δικτύου αντιλαμβάνεται ότι η διεύθυνση IPv4 που κάνουμε ping βρίσκεται εκτός τοπικού δικτύου και στέλνει τα ICMP requests στον δρομολογητή. Αυτός με τη σειρά του τα προωθεί στον επόμενο δρομολογητή ώστε να καταλήξουν σε δρομολογητή με IP interface στο ίδιο υποδίκτυο με τον υπολογιστή-στόχο. Αυτός τα εκπέμπει μέσω Ethernet στον υπολογιστή στόχο, ο οποίος είναι ανενεργός και δεν λαμβάνει τα πακέτα. Κατά αυτόν τον τρόπο δεν έχουμε ICMP Echo Replies.

## Άσκηση 3: Εντολή tracert/traceroute

Ξεκινάμε μια νέα καταγραφή της δικτυακής κίνησης με φίλτρο σύλληψης ώστε να συλλαμβάνουμε μόνο πακέτα IPv4 που περιέχουν την IPv4 διεύθυνση του υπολογιστή μας.

Σε παράθυρο εντολών εκτελούμε την εντολή traceroute χωρίς επίλυση ονομάτων με προορισμό το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Χρησιμοποιούμε την κατάλληλη σύνταξη ώστε να παραχθούν μηνύματα ICMP Echo request. Όταν τελειώσει η εκτέλεση της εντολής σταματάμε την καταγραφή και εφαρμόζουμε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

```
petrosrapto@petrosraptoAssistant:~$ traceroute -4 -n -I 147.102.40.15
traceroute to 147.102.40.15 (147.102.40.15), 30 hops max, 60 byte packets
 1  147.102.236.200  3.639 ms  5.091 ms  5.078 ms
 2  147.102.40.15  5.067 ms  5.058 ms  5.048 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
2	0.0000060000	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=1/256, ttl=1 (no response..
3	0.000036476	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=2/512, ttl=1 (no response..
4	0.000011488	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=3/768, ttl=1 (no response..
5	0.000011247	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=4/1024, ttl=2 (reply in 2..
6	0.000009886	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=5/1280, ttl=2 (reply in 2..
7	0.000009685	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=6/1536, ttl=2 (reply in 2..
8	0.000010255	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=7/1792, ttl=3 (reply in 2..
9	0.000009315	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=8/2048, ttl=3 (reply in 2..
10	0.000009274	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=9/2304, ttl=3 (reply in 2..
11	0.000010406	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=10/2560, ttl=4 (reply in ..
12	0.000009405	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=11/2816, ttl=4 (reply in ..
13	0.000009394	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=12/3072, ttl=4 (reply in ..
14	0.000009976	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=13/3328, ttl=5 (reply in ..
15	0.0000099284	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=14/3584, ttl=5 (reply in ..
16	0.000009274	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=15/3840, ttl=5 (reply in ..
17	0.000011067	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=16/4096, ttl=6 (reply in ..
18	8.003432444	147.102.236.200	147.102.236.33	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
19	8.000194602	147.102.236.33	147.102.40.15	ICMP	74	Echo (ping) request id=0x0006, seq=17/4352, ttl=6 (reply in ..
20	8.0001407534	147.102.236.200	147.102.236.33	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
21	8.000000331	147.102.236.200	147.102.236.33	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
22	0.000006090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=4/1024, ttl=63 (request i..
23	0.000006090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=5/1280, ttl=63 (request i..
24	0.000006090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=6/1536, ttl=63 (request i..
25	0.002810874	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=7/1792, ttl=63 (request i..
26	0.000494932	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=8/2048, ttl=63 (request i..
27	0.000006023	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=9/2304, ttl=63 (request i..
28	0.000006090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=10/2560, ttl=63 (request i..
29	0.000006080	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=11/2816, ttl=63 (request i..
30	0.000006090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=12/3072, ttl=63 (request i..
31	0.000006081	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=13/3328, ttl=63 (request i..
32	0.004722126	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=14/3584, ttl=63 (request i..
33	0.0000283939	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=15/3840, ttl=63 (request i..
34	0.0000060180	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=16/4096, ttl=63 (request i..
35	0.000000090	147.102.40.15	147.102.236.33	ICMP	74	Echo (ping) reply id=0x0006, seq=17/4352, ttl=63 (request i..

3.1) Ποιο είναι το μήκος και το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή tracert ή traceroute;: **32 bytes**

3.2) Συγκρίνετε το παραπάνω μήκος και περιεχόμενο του πεδίου δεδομένων με τα αντίστοιχα στην περίπτωση της εντολής ping (Ερώτηση 1.9); Τώρα έχουμε μικρότερο μήκος δεδομένων σε σύγκριση με την εντολή ping στην Ερ. 1.9. Πάλι το περιεχόμενο είναι τυχαίο, δεν μεταφέρει κάποια συγκεκριμένη πληροφορία.

Οστόσο είναι ίδιο το περιεχόμενο για κάθε πακέτο και δεν μεταβάλλεται όπως συμβαίνει στην ping.

3.3) Ποιο ICMP μήνυμα λάθους παρατηρείτε στις απαντήσεις των ενδιάμεσων κόμβων (πριν τον 147.102.40.15); **Time-to-live exceeded (Time to live exceeded in transit)**

3.4) Ποια είναι η τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP για το προηγούμενο μήνυμα λάθους;: **Type: 11, Code: 0**

3.5) Ποια άλλα πεδία έχει η επικεφαλίδα του μηνυμάτος λάθους πριν τα δεδομένα και ποιο το μέγεθός τους;

**Checksum: 2 bytes, Unused: 1 byte, Length: 1 byte, Unused: 2 bytes**

3.6) Ποιο είναι το μήκος της επικεφαλίδας και ποιο των δεδομένων του ICMP μηνυμάτος λάθους της ερώτησης 3.3;

**Επικεφαλίδα: 8 bytes, Δεδομένα: 68 bytes**

3.7) Τι είναι το περιεχόμενο του πεδίου δεδομένων του προηγούμενου ICMP μηνυμάτος λάθους και ποια η σχέση του με το πακέτο IPv4 εξ αιτίας του οποίου παράχθηκε;;

Το πεδίο δεδομένων του μηνυμάτος λάθους ICMP έχει “ενθυλακώσει” (μεταφέρει) το πακέτο IPv4 για το οποίο εμφανίστηκε το σφάλμα.

#### Άσκηση 4: Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

Ξεκινάμε μια νέα καταγραφή με φίλτρο σύλληψης ώστε να συλλαμβάνουμε μόνο μηνύματα ICMP και μετά εκτελούμε διαδοχικά την εντολή ping στέλνοντας χωρίς θρυμματισμό ένα μόνο πακέτο για τιμές μεγέθους δεδομένων ICMP σύμφωνες με τις συνήθεις τιμές MTU που δίδονται πιο πάνω, ξεκινώντας από τη μεγαλύτερη προς τη μικρότερη. Σταματάμε τα ping και την καταγραφή όταν λάβουμε επιτυχή απάντηση από το 147.102.40.15.

```
petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 1472 -M do edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 1472(1500) bytes of data.

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 1464 -M do edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 1464(1492) bytes of data.

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 978 -M do edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 978(1006) bytes of data.

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 548 -M do edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 548(576) bytes of data.
556 bytes from edu-dy.cn.ece.ntua.gr (147.102.40.15): icmp_seq=1 ttl=63 time=6.69 ms

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.687/6.687/6.687/0.000 ms
petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 524 -M do edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 524(552) bytes of data.
532 bytes from edu-dy.cn.ece.ntua.gr (147.102.40.15): icmp_seq=1 ttl=63 time=9.55 ms

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.548/9.548/9.548/0.000 ms
```

Σημείωση: Πρέπει να αφαιρέσουμε 28 bytes (header IP και ICMP) από τις δοθείσες τιμές για να βρούμε τις τιμές του data του ICMP γιατί η MTU αφορά την τιμή του ολόκληρου πακέτου IPv4.

**4.1) Ποιες τιμές μήκους δεδομένων ICMP χρησιμοποιήσατε για να παράγετε πακέτα IPv4 με μήκος τις επιθυμητές τιμές MTU: 1472, 1464, 978, 548, 524, 516, 484**

4.2. Παρατηρήσατε μήνυμα λάθους ICMP Destination Unreachable; 'Όχι δεν παρατηρήσαμε. Για αυτό για το υπόλοιπο μέρος της 4ης Άσκησης θα γραπτικοίσσουμε τις καταγραφές Wireshark που δόθηκαν.

Στην καταγραφή αυτή παρατηρούμε μόνης α λόγων ICMP Destination Unreachable

**4.3) Εάν ναι, ποιος κόμβος της διαδρομής το παρήγαγε:: 79.129.213.16**

**4.4) Καταγράψτε την τιμή των πεδίων Type και Code της επικεφαλίδας του ICMP Destination Unreachable.**

**Type:3, Code:4**

**4.5) Στο προηγούμενο μήνυμα, ποιο πεδίο δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού του πακέτου IPv4 και ποια τιμή έχει η επικεφαλίδα Next-Hop MTU;; Το πεδίο Code, Next-Hop MTU: 1492**

**4.6) Για το προηγούμενο μήνυμα, τι περιέχει το πεδίο των δεδομένων;**

**Περιέχει το IPv4 Header και ICMP header για το πακέτο IPv4 (που έχει ενθυλακώσει το αντίστοιχο ICMP Echo Request) για το οποίο προκλήθηκε Destination Unreachable.**

**4.7) Ποια είναι η MTU για την οποία δεν λαμβάνετε για πρώτη φορά μήνυμα λάθους ICMP Destination Unreachable, άσχετα από το εάν απαντά ή όχι το 147.102.40.15; Μέγεθος IPv4 πακέτου 1492 bytes (data ICMP 1464 bytes)**

**4.8) Για ποιες άλλες τιμές MTU δεν απαντά το 147.102.40.15; Μέγεθος IPv4 πακέτου 1006 bytes (data ICMP 978 bytes) (και Μέγεθος IPv4 πακέτου 1492 bytes (data ICMP 1464 bytes))**

**4.9) Ποια είναι η τιμή MTU για την οποία λαμβάνετε απάντηση από το 147.102.40.15;**

**Μέγεθος IPv4 πακέτου 576 bytes (data ICMP 548 bytes)**

**4.10) Είναι αυτή η MTU της δικτυακής διεπαφής του 147.102.40.15 ή κάποιου άλλου ενδιάμεσου κόμβου; Γιατί; Είναι η MTU της δικτυακής διεπαφής του 147.102.40.15, διότι για μεγαλύτερες τιμές παρατηρούμε ότι οι ενδιάμεσοι κόμβοι δεν επιστρέφουν Destination Unreachable και συνεπώς τα πακέτα παραλαμβάνονται επιτυχώς από τον 147.102.40.15. Ωστόσο για τις τιμές αυτές παρατηρούμε ότι δεν λαμβάνουμε ICMP Echo Reply που σημαίνει ότι το μέγεθος των Replies υπερβαίνει την MTU της διεπαφής του 147.102.40.15.**

**4.11) Για ποιο λόγο νομίζετε ότι το 147.102.40.15 δεν παράγει ICMP Destination Unreachable όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής του; Επειδή είναι ο προορισμός του πακέτου και δεν χρειάζεται να το προωθήσει.**

Ξεκινάμε μια νέα καταγραφή και κάνουμε ping στο 147.102.40.15 στέλνοντας ένα μόνο πακέτο ICMP μεγέθους αντίστοιχου της MTU της ερώτησης 4.7 χωρίς την απαίτηση μη θρυμματισμού.

```
petrosrapto@petrosraptoAssistant:~$ ping -c 1 -s 1464 -M dont 147.102.40.15
PING 147.102.40.15 (147.102.40.15) 1464(1492) bytes of data.
1472 bytes from 147.102.40.15: icmp_seq=1 ttl=63 time=99.1 ms

--- 147.102.40.15 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 99.112/99.112/99.112/0.000 ms
```

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
152	0.000000000	147.102.236.33	147.102.40.15	ICMP	1506	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (reply in 1...)
155	0.099072224	147.102.40.15	147.102.236.33	ICMP	402	Echo (ping) reply id=0x0013, seq=1/256, ttl=63 (request in...
<hr/>						
▶ Frame 155: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface wlp1s0, id 0   Ethernet II, Src: Cisco_00:d9:1d (08:ec:f5:d0:09:1d), Dst: IntelCor_15:16:66 (90:78:41:15:16:66)   ▶ Internet Protocol Version 4, Src: 147.102.40.15, Dst: 147.102.236.33     0100 ... = Version: 4     ... 0101 = Header Length: 20 bytes (5)   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)     Total Length: 388     Identification: 0x8fba (36794)     Flags: 0x008a       Fragment offset: 1104       Time to live: 63     Protocol: ICMP (1)     Header checksum: 0xaf37 [validation disabled]     [Header checksum status: Unverified]     Source: 147.102.40.15     Destination: 147.102.236.33   ▶ [3 IPv4 Fragments (1472 bytes): #153(552), #154(552), #155(368)]     [Frame: 153, payload: 0-551 (552 bytes)]     [Frame: 154, payload: 552-1103 (552 bytes)]     [Frame: 155, payload: 1104-1471 (368 bytes)]     [Fragment count: 3]     [Reassembled IPv4 length: 1472]     [Reassembled IPv4 data: 0000eec4001300012dd96c63000000000ccb0c0000000000...]   ▶ Internet Control Message Protocol						

**4.12) Καταγράψτε το μέγεθος του πρώτου θραύσματος που λαμβάνει ο υπολογιστής σας. Είναι το ίδιο με την MTU που προσδιορίσατε προηγουμένως; Γιατί; Το μέγεθος του πρώτου θραύσματος είναι 572 bytes (IPv4 header 20 bytes + IPv4 data 552 bytes). Παρατηρούμε ότι δεν είναι το ίδιο με την MTU που προσδιορίσαμε στο ερώτημα 4.9. Αυτό γιατί μόλις πραγματοποιείται ο τεμαχισμός αφενός κάποια από τα byte θα καταναλωθούν για την δημιουργία νέου IPv4 header**

και αφετέρου το fragment offset “δείχνει” 8άδες bytes. Όμως το 556 δεν διαιρείται με το 8 ενώ το 552 διαιρείται.

## Άσκηση 5: Απρόσιτη Θύρα (Port Unreachable)

Ξεκινάμε μια καταγραφή με φίλτρο ώστε να συλλαμβάνουμε μόνο πακέτα IPv4 από και προς το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Στη συνέχεια τρέχουμε το πρόγραμμα host σε περιβάλλον Unix, για να ζητήσουμε από τον εξυπηρετητή DNS 147.102.40.15 τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr.

```
[petrosrapto@petrosraptoAssistant:~]$ host edu-dy.cn.ntua.gr 147.102.40.15
;; connection timed out; no servers could be reached
```

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	147.102.236.33	147.102.40.15	DNS	77 Standard query 0x2689 A edu-dy.cn.ntua.gr
2	0.005908335	147.102.40.15	147.102.236.33	ICMP	70 Destination unreachable (Port unreachable)
3	4.992432949	147.102.236.33	147.102.40.15	DNS	77 Standard query 0x2689 A edu-dy.cn.ntua.gr
4	0.014027663	147.102.40.15	147.102.236.33	ICMP	70 Destination unreachable (Port unreachable)

Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlp1s0, id 0  
Ethernet II, Src: Cisco\_d9:d9:1d (08:ec:f5:d9:d9:1d), Dst: IntelCor\_15:16:66 (90:78:41:15:16:66)  
Internet Protocol Version 4, Src: 147.102.40.15, Dst: 147.102.236.33  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 56  
Identification: 0x9080 (36902)  
Flags: 0x0000  
Fragment offset: 0  
Time to live: 63  
Protocol: ICMP (1)  
Header checksum: 0xb047 [validation disabled]  
[Header checksum status: Unverified]  
Source: 147.102.40.15  
Destination: 147.102.236.33  
Internet Control Message Protocol  
Type: 3 (Destination unreachable)  
Code: 3 (Port unreachable)  
Checksum: 0x17c9 [correct]  
[Checksum Status: Good]  
Unused: 00000000  
Internet Protocol Version 4, Src: 147.102.236.33, Dst: 147.102.40.15  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 63  
Identification: 0xb260 (45664)  
Flags: 0x0000  
Fragment offset: 0  
Time to live: 63  
Protocol: UDP (17)  
Header checksum: 0x8e50 [validation disabled]  
[Header checksum status: Unverified]  
Source: 147.102.236.33  
Destination: 147.102.40.15  
User Datagram Protocol, Src Port: 40061, Dst Port: 53  
Source Port: 40061  
Destination Port: 53  
Length: 43  
Checksum: 0x4856 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]

5.1) Ποιο φίλτρο σύλληψης χρησιμοποιήσατε; **host 147.102.40.15**

5.2) Ποια η ακριβής σύνταξη της εντολής nslookup, dig ή host που χρησιμοποιήσατε;

**host edu-dy.cn.ntua.gr 147.102.40.15**

5.3) Λάβατε κάποια απάντηση στο παράθυρο εντολών; Ποιο το νόημά της;

**Connection timed out; no servers could be reached**, ο εξυπηρετητής DNS 147.102.40.15 δεν ανταποκρίθηκε στο αίτημά μας για τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr.

5.4) Παρατηρήσατε μηνύματα DNS στην καταγραφή; **Ναι, δύο**

5.5) Ποιο είναι το πρωτόκολλο μεταφοράς; **UDP**

Ποια είναι η θύρα προορισμού τους; **53**

5.6) Παρατηρήσατε μηνύματα λάθους ICMP Destination Unreachable με πηγή το 147.102.40.15; **Ναι, δύο**

5.7) Καταγράψτε την τιμή των πεδίων Type και Code της επικεφαλίδας. **Type: 3, Code: 3**

5.8) Ποιο πεδίο δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα; **Πεδίο Code**

5.9) Πώς προκύπτει ότι πρόκειται για τη θύρα προορισμού των μηνυμάτων DNS; **To πακέτο που φέρει το μήνυμα λάθους ICMP Destination Unreachable έχει “ενθυλακώσει” τις επικεφαλίδες IPv4, UDP του πακέτου για το οποίο προέκυψε το σφάλμα. Εκεί μπορούμε να διακρίνουμε την θύρα προορισμού που είναι το 53. Συνεπώς το σφάλμα αφορά εξυπηρέτηση DNS.**

Στα συστήματα Unix η traceroute παράγει μηνύματα UDP με θύρες προορισμού στην περιοχή από 33434 έως 33534.

5.10) Όταν αντά φτάνουν στον προορισμό τους με ποιο μήνυμα ICMP απαντά αυτός; **Destination(Port) Unreachable**

## Άσκηση 6: IPv6 και ICMPv6

Θα χρησιμοποιήσουμε την καταγραφή που δίνεται στην ιστοσελίδα του μαθήματος.

Στην καταγραφή αυτή συλλαμβάνουμε μόνο πακέτα IPv6. Έχουμε κάνει ping προς το μηχάνημα με IPv6 διεύθυνση 2001:648:2000:329::101 και μετά traceroute ή traceroute στην ίδια διεύθυνση. .

Εφαρμόζουμε φίλτρο ώστε να παρατηρούμε μόνο μηνύματα ICMPv6.

icmpv6						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
2	1.320699	fe80::aec:f5ff:fea1...	ff02::1:ff07:3e0c	ICMPv6	86	Neighbor Solicitation for 2001:648:2000:7:215:5dff:fe07:3e0c ...
3	2.320195	fe80::aec:f5ff:fea1...	ff02::1:ff07:3e0c	ICMPv6	86	Neighbor Solicitation for 2001:648:2000:7:215:5dff:fe07:3e0c ...
4	2.437033	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
5	3.000254	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
6	3.903586	fe80::aec:f5ff:fea1...	fe80::6ced:ded:91e7...	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
7	3.994007	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Advertisement fe80::6ced:ded:91e7:3662 (sol, ovr) is...
8	3.999774	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
9	5.322216	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=123, hop limit=128 (reply ...
10	5.322867	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=123, hop limit=63 (request i...
11	6.323034	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=124, hop limit=128 (reply ...
12	6.323467	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=124, hop limit=63 (request i...
13	7.324068	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=125, hop limit=128 (reply ...
14	7.324574	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=125, hop limit=63 (request i...
15	8.326072	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=126, hop limit=128 (reply ...
16	8.326749	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=126, hop limit=63 (request i...
17	8.473462	fe80::6ced:ded:91e7...	fe80::aec:f5ff:fea1...	ICMPv6	86	Neighbor Solicitation for fe80::aec:f5ff:fea1:a427 from 98:90:...
18	8.473938	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Advertisement fe80::aec:f5ff:fea1:a427 (rtr, sol, ov...
19	10.436382	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
20	11.000757	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
21	11.623980	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for 2001:648:2000:7:215:5dff:fe07:3e0c ...
22	12.000658	fe80::602e:ae6:8803...	ff02::1:ffdc:130c	ICMPv6	86	Neighbor Solicitation for fe80::88a2:fcf8:1edc:130c from 00:e...
23	12.461273	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=127, hop limit=1 (no respo...
24	12.461942	2001:648:2000:7:c5b...	2001:648:2000:7:c5b...	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
25	12.462236	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=128, hop limit=1 (no respo...
26	12.462972	2001:648:2000:7:c5b...	2001:648:2000:7:c5b...	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
27	12.463154	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=129, hop limit=1 (no respo...
28	12.463996	2001:648:2000:7:c5b...	2001:648:2000:7:c5b...	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
29	12.464714	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=130, hop limit=2 (reply in...
30	13.465732	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	126	Echo (ping) reply id=0x0001, seq=130, hop limit=63 (request i...
31	13.466877	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=131, hop limit=2 (reply in...
32	13.467231	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	126	Echo (ping) reply id=0x0001, seq=131, hop limit=63 (request i...
33	13.468292	2001:648:2000:7:c5b...	2001:648:2000:329::...	ICMPv6	126	Echo (ping) request id=0x0001, seq=132, hop limit=2 (reply in...
34	13.468694	2001:648:2000:329::...	2001:648:2000:7:c5b...	ICMPv6	126	Echo (ping) reply id=0x0001, seq=132, hop limit=63 (request i...

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)  
Ethernet II, Src: Realtek\_Ethernet (00:0e:4c:68:02:26), Dst: IPv6mcast\_ff:dc:dc:13:0c (33:33:ff:dc:13:0c)  
Internet Protocol Version 6, Src: fe80::602e:ae6:8803:5878, Dst: ff02::1:ffdc:130c  
Internet Control Message Protocol v6

```
0000 33 33 ff dc 13 0c 00 e0 4c 68 02 26 86 dd 60 00 33 ..... Lh & ...
0010 00 00 00 20 3a ff e8 00 00 00 00 00 00 60 2e ..... : ..... .
0020 0a e8 03 58 78 ff 02 00 00 00 00 00 00 00 00 ..... XX ..... .
0030 00 01 ff dc 13 0c 87 00 16 33 00 00 00 00 fe 80 ..... 3 ..... .
0040 00 00 00 00 00 00 00 88 a2 fc f8 1e dc 13 0c 01 01 ..... : ..... .
0050 00 e0 4c 68 02 26 ..... Lh & ...
```

6.1) Ποια είναι η σύνταξη των ping, traceroute ή traceroute που χρησιμοποιήσατε;; **traceroute -6 2001:648:2000:329::101**

6.2) Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;; **ip6**

Ποια του φίλτρου απεικόνισης;; **icmpv6**

6.3) Τι τιμή έχει το πεδίο Type της επικεφαλίδας Ethernet όταν μεταφέρονται πακέτα IPv6;; **0x86dd**

6.4) Ποιο είναι το μήκος επικεφαλίδας των πακέτων IPv6;; **40 bytes**

6.5) Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος IPv6.

**Version(1 byte), Traffic Class/Flow Label(3 bytes), Payload Length(2 bytes), Next Header(1 byte), Hop Limit(1 byte), Source (16 bytes), Destination (16 bytes)**

6.6) Ποια επικεφαλίδα είναι η αντίστοιχη της TTL των πακέτων IPv4; **Hop Limit**

6.7) Ποια επικεφαλίδα δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 και ποια η τιμή της για το ICMPv6; **Πεδίο: Next Header και έχει τιμή 58 για ICMPv6**

6.8) Εντοπίστε ένα μήνυμα ICMPv6 Echo request που να έχει παραχθεί από την εντολή ping. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP Echo request στην ερώτηση 1.6;

**Περίπου ναι. Λείπει το πεδίο "Timestamp from icmp data" (8 bytes) το οποίο μάλλον προστίθεται μόνο για τα συστήματα Unix, ενώ τώρα μάλλον έχουμε ping από Windows.**

6.9) Ποια η τιμή του πεδίου Type;; **128**

Ποιο το μήκος δεδομένων που μεταφέρει το ICMP Echo request;; **32 bytes**

6.10) Εντοπίστε το μήνυμα ICMPv6 Echo reply που παράχθηκε σε απάντηση του προηγούμενου ICMPv6 Echo request. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν του ICMPv6 Echo request; **Ναι είναι ίδια.**

6.11) Ποια η τιμή του πεδίου Type;; **129**

Ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 Echo reply; **32 bytes**

6.12) Εντοπίστε ένα μήνυμα ICMPv6 Echo request που να έχει παραχθεί από την εντολή traceroute. Σε τι διαφέρει από το αντίστοιχο που παράγει η εντολή ping; **To πεδίο των δεδομένων έχει πλέον 64 bytes.**

**6.13)** Εντοπίστε ένα μήνυμα λάθους ICMPv6 Time exceeded. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP Time exceeded στις ερωτήσεις 3.4 και 3.5::

**Τα πεδία Unused (3 bytes) και Length (1 byte) απονοτιάζουν, ενώ έχουμε νέο πεδίο Reserved.**

**6.14)** Ποια η τιμή του πεδίου Type: **Το πεδίο type έχει πλέον τιμή 3 και όχι 11.**

Ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 Time exceeded; **112 bytes**

**6.15)** Τι περιέχει το πεδίο δεδομένων του:: **Περιέχει το πακέτο IPv6 για το οποίο προκλήθηκε Time Exceeded.**

**Σε σύγκριση με το ICMPv4 έχουμε στο ICMPv6 όχι μόνο τις επικεφαλίδες IPv4, ICMP αλλά και τα δεδομένα τους.**

**6.16)** Παρατηρήσατε άλλα ICMPv6 μηνύματα; Εάν ναι, τι είδους είναι;

**Ναι, "Neighbor Solicitation" και "Neighbor Advertisement"**

**6.17)** Ποια η τιμή του πεδίου Type::: **Για Neighbor Solicitation: 135 και για Neighbor Advertisement: 136**

Ποιο το μήκος των μηνυμάτων ICMPv6 (bytes)::: **Για Neighbor Solicitation: 32 και για Neighbor Advertisement: 32**