



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Δίκτυα Υπολογιστών

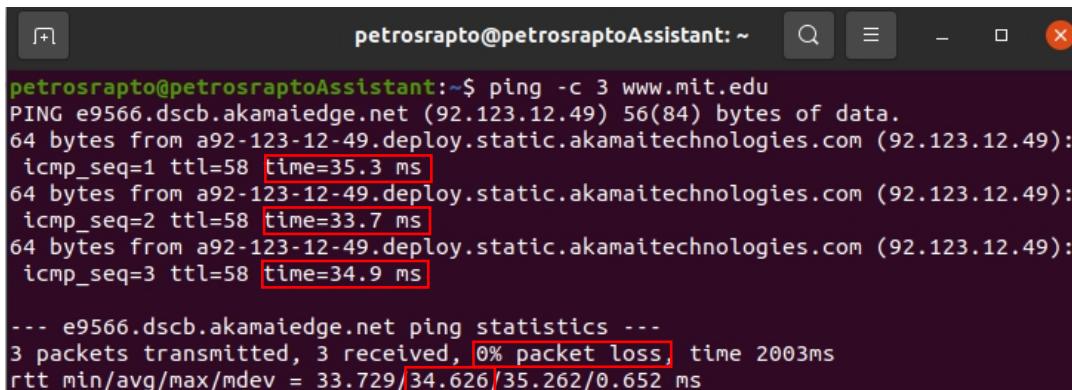
Αναφορά 4ης Εργαστηριακής Άσκησης

**Ραπτόπουλος Πέτρος (ει19145)
Ομάδα 3**

Άσκηση 1: Μετρήστε την καθυστέρηση

Ξεκινάμε μια καταγραφή Wireshark επιλέγοντας την κάρτα δικτύου του υπολογιστή μας και εφαρμόζοντας το φίλτρο σύλληψης *not multicast and not broadcast* προκειμένου να περιορισθεί το πλήθος των πλαισίων που καταγράφονται. Μέσω της εντολής ping παράγουμε τρία πακέτα IPv4/ICMP προς τον εξυπηρετητή ιστού με όνομα www.mit.edu και σταματάμε την καταγραφή μόλις ολοκληρωθεί η εκτέλεση της εντολής.

- 1.1) Ακριβής σύνταξη της εντολής ping που χρησιμοποιήσαμε: **ping -c 3 www.mit.edu**



```
petrosrapto@petrosraptoAssistant:~$ ping -c 3 www.mit.edu
PING e9566.dscb.akamaiedge.net (92.123.12.49) 56(84) bytes of data.
64 bytes from a92-123-12-49.deploy.static.akamaitechnologies.com (92.123.12.49):
  icmp_seq=1 ttl=58 time=35.3 ms
64 bytes from a92-123-12-49.deploy.static.akamaitechnologies.com (92.123.12.49):
  icmp_seq=2 ttl=58 time=33.7 ms
64 bytes from a92-123-12-49.deploy.static.akamaitechnologies.com (92.123.12.49):
  icmp_seq=3 ttl=58 time=34.9 ms

--- e9566.dscb.akamaiedge.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 33.729/34.626/35.262/0.652 ms
```

- 1.2) Σημασία φίλτρου σύλληψης που εφαρμόσαμε: **Δεν καταγράφονται τα πλαίσια που είχαν χαρακτήρα multicast ή broadcast. Δηλαδή καταγράφονται μόνο τα πλαίσια unicast (συγκεκριμένος αποστολέας και παραλήπτης).** ποσοστό απωλειών πακέτων και τη μέση καθυστέρηση.

- 1.3) Ποσοστό απωλειών πακέτων: **0% packet loss** Μέση καθυστέρηση: **34.626ms**

- 1.4) Τιμές RTT (Round-Trip Time):

Echo Request-Reply 1: **35.3ms**

Echo Request-Reply 2: **33.7ms**

Echo Request-Reply 3: **34.9ms**

Από το μενού View επιλέγοντας Time Display Format και Seconds Since Previous Displayed Packet.

Εφαρμόζουμε φίλτρο απεικόνισης icmp ώστε να εμφανίζονται μόνο τα πακέτα ICMP.

- 1.5) Τιμές RTT (Round-Trip Time) με τη βοήθεια του Wireshark:

Echo Request-Reply 1: **0.035234601s**

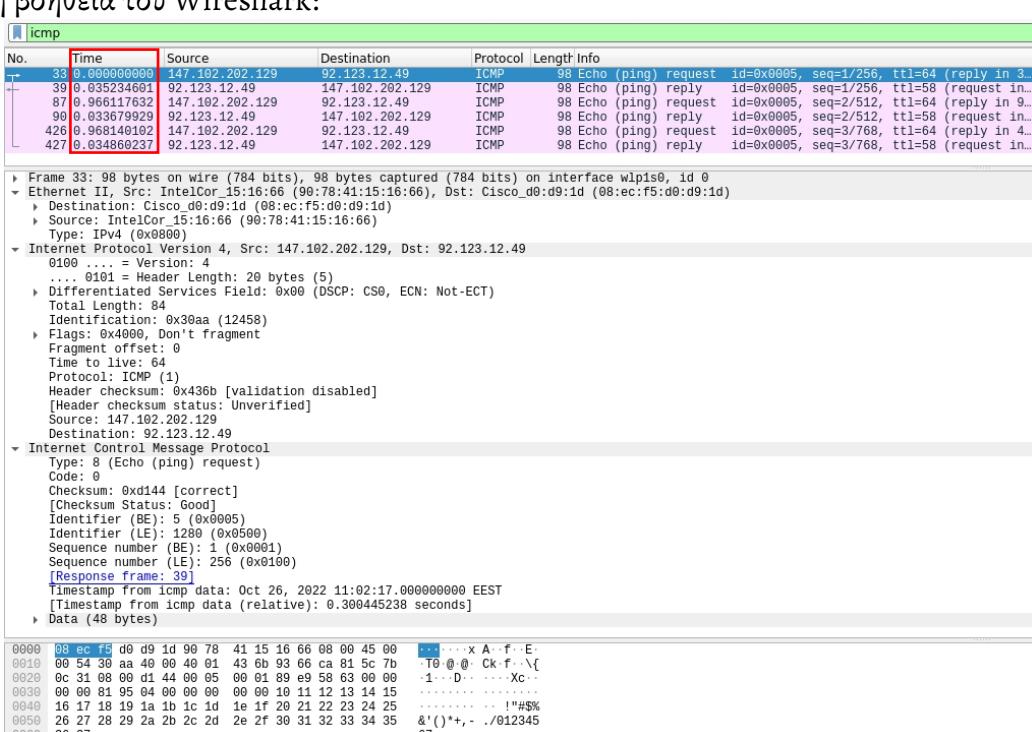
Echo Request-Reply 2: **0.033679929s**

Echo Request-Reply 3: **0.034860237s**

Παρατηρούμε ότι οι καταγραφείσες τιμές με τη βοήθεια του Wireshark συμφωνούν (με μικρή απόκλιση) με τις αντίστοιχες στο terminal.

- 1.6) Φίλτρο απεικόνισης ώστε να εμφανίζονται μόνο πακέτα IPv4: **ip**

Παρατηρούμε ότι το πεδίο type στο Internet Control Message Protocol



No.	Time	Source	Destination	Protocol	Length	Info
32	0.000000000	147.102.202.129	92.123.12.49	ICMP	98	Echo (ping) request id=0x0005, seq=1/256, ttl=64 (reply in 3...)
39	0.035234601	92.123.12.49	147.102.202.129	ICMP	98	Echo (ping) reply id=0x0005, seq=1/256, ttl=58 (request in 3...)
87	0.03679929	147.102.202.129	92.123.12.49	ICMP	98	Echo (ping) request id=0x0006, seq=2/512, ttl=64 (reply in 9...)
90	0.03679929	92.123.12.49	147.102.202.129	ICMP	98	Echo (ping) reply id=0x0006, seq=2/512, ttl=58 (request in 9...)
426	0.034860237	147.102.202.129	92.123.12.49	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 4...)
427	0.034860237	92.123.12.49	147.102.202.129	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=58 (request in 4...)

Frame 33: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlpis0, id 0
Ethernet II, Src: IntelCor_15:16:66 (90:78:41:15:16:66), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 147.102.202.129, Dst: 92.123.12.49
 Version: 4
 Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x30aa (12458)
 Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: ICMP (1)
 Header checksum: 0x436b [validation disabled]
 [Header checksum status: Unverified]
 Source: 147.102.202.129
 Destination: 92.123.12.49
 Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xd144 [correct]
 [Checksum Status: Good]
 Identifier (BE): 5 (0x0005)
 Identifier (LE): 1280 (0x0500)
 Sequence number (BE): 1 (0x0001)
 Sequence number (LE): 256 (0x0100)
 [Response frame: 39]
 Timestamp from icmp data: Oct 26, 2022 11:02:17.000000000 EEST
 [Timestamp from icmp data (relative): 0.300445238 seconds]
 Data (48 bytes)

έχει συγκεκριμένες τιμές για Echo (ping) Request (τιμή 8) και Echo (ping) Reply (τιμή 0).

1.7) Φίλτρο απεικόνισης προκειμένου να εμφανίζεται μόνο η κίνηση ICMP που προκάλεσε η εντολή ping:

`icmp.type == 0 or icmp.type == 8`

1.8) Είδος μηνυμάτων ICMP που στάλθηκαν από τον υπολογιστή μας κατά την εκτέλεση της εντολής ping:

Echo (ping) Request

1.9) Διευθύνσεις IPv4 πηγής: **147.102.202.129** και προορισμού: **92.123.12.49** των παραπάνω μηνυμάτων.

1.10) Είδος μηνυμάτων ICMP που ελήφθησαν από τον υπολογιστή μας κατά την εκτέλεση της εντολής ping:

Echo (ping) Reply

1.11) Διευθύνσεις IPv4 πηγής: **92.123.12.49** και προορισμού: **147.102.202.129** των παραπάνω μηνυμάτων.

1.12) Τι έχει αλλάξει σε σχέση με την καταγραφή του παρελθόντος;

Αν με την λέξη παρελθόν εννοείται το παράδειγμα στην αρχή της Άσκησης 1: **'Έχει αλλάξει η διεύθυνση IPv4 του εξυπηρετητή ιστού με όνομα www.mit.edu από 18.7.22.83 σε 92.123.12.49.**

Άσκηση 2: Περισσότερα για το Ping

Ξεκινάμε μια καταγραφή Wireshark χρησιμοποιώντας το ίδιο φίλτρο σύλληψης και φίλτρο απεικόνισης όπως στην Άσκηση 1. Εκτελούμε διαδοχικά ping με τη βοήθεια του terminal στέλνοντας 5 πακέτα IPv4/ICMP στις διευθύνσεις:

i. Τη διεύθυνση IPv4 της προκαθορισμένης πύλης: 147.102.200.200

```
petrosrapto@petrosraptoAssistant:~$ ip r
default via 147.102.200.200 dev wlp1s0 proto dhcp metric 600
147.102.200.0/22 dev wlp1s0 proto kernel scope link src 147.102.202.129 metric 6
00
169.254.0.0/16 dev virbr0 scope link metric 1000 linkdown
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

ii. Τη διεύθυνση IPv4 της διεπαφής δικτύου του υπολογιστή σας: 147.102.202.129

```
wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 147.102.202.129 netmask 255.255.252.0 broadcast 147.102.203.255
inet6 fe80::85f9:b27:bde1:b577 prefixlen 64 scopeid 0x20<link>
ether 90:78:41:15:16:66 txqueuelen 1000 (Ethernet)
RX packets 1755622 bytes 2093369954 (2.0 GB)
RX errors 0 dropped 3 overruns 0 frame 0
TX packets 322782 bytes 53979986 (53.9 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

iii. Τη διεύθυνση του βρόχου επιστροφής (loopback): 127.0.0.1

```
petrosrapto@petrosraptoAssistant:~$ ping -c 5 147.102.200.200
PING 147.102.200.200 (147.102.200.200) 56(84) bytes of data.
64 bytes from 147.102.200.200: icmp_seq=1 ttl=255 time=3.48 ms
64 bytes from 147.102.200.200: icmp_seq=2 ttl=255 time=2.82 ms
64 bytes from 147.102.200.200: icmp_seq=3 ttl=255 time=22.5 ms
64 bytes from 147.102.200.200: icmp_seq=4 ttl=255 time=3.21 ms
64 bytes from 147.102.200.200: icmp_seq=5 ttl=255 time=3.17 ms
```

```
--- 147.102.200.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 2.822/7.034/22.500/7.735 ms
```

```
petrosrapto@petrosraptoAssistant:~$ ping -c 5 147.102.202.129
PING 147.102.202.129 (147.102.202.129) 56(84) bytes of data.
```

```
64 bytes from 147.102.202.129: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 147.102.202.129: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 147.102.202.129: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 147.102.202.129: icmp_seq=4 ttl=64 time=0.065 ms
64 bytes from 147.102.202.129: icmp_seq=5 ttl=64 time=0.053 ms
```

```
--- 147.102.202.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4090ms
rtt min/avg/max/mdev = 0.041/0.055/0.065/0.009 ms
```

```
petrosrapto@petrosraptoAssistant:~$ ping -c 5 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
```

```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.053 ms
```

```
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4092ms
rtt min/avg/max/mdev = 0.048/0.053/0.058/0.003 ms
```

Σταματάμε την καταγραφή όταν ολοκληρωθεί η εκτέλεση δόλων των εντολών.

2.1) Ακριβής σύνταξη της εντολής ping που χρησιμοποιήσαμε: `ping -c 5 <ip_address>`

Για να εμφανίσουμε τα Echo Requests/Replies που έστειλε/έλαβε ο υπολογιστής μας εφαρμόζουμε το φίλτρο απεικόνισης `icmp and ip.addr == 147.102.202.129`.

2.2) Πόσα από τα μηνύματα ICMP Echo request που έχουν αποσταλεί από τον υπολογιστή σας έχει καταγράψει το Wireshark;; **Μόνο 5**

2.3) Προορισμός: **147.102.200.200 (default gateway)**

2.4) Παρατηρήσατε αποστολή μηνυμάτων ICMP Echo request στο δίκτυο με πηγή και προορισμό τη διεύθυνση IPv4 του υπολογιστή σας;; **'Όχι. Σύμφωνα με το σχήμα**

τα πακέτα αυτά τοποθετούνται στην ουρά εισόδου IPv4 (οδηγός loopback) και “τροφοδοτούν” την είσοδο πακέτων IPv4 του υπολογιστή μας. Συνεπώς δεν εκπέμπονται στο τοπικό δίκτυο και δεν καταγράφονται από το Wireshark.

2.5) Παρατηρήσατε αποστολή μηνυμάτων ICMP Echo request προς τη διεύθυνση του βρόχου επιστροφής::

Όχι. Τα πακέτα αυτά οδηγούνται στο local loopback και δεν εκπέμπονται στο Τοπικό Δίκτυο. Άρα δεν καταγράφονται από το Wireshark.

2.6) Ποια η διαφορά όταν κάνετε ping στη διεπαφή του υπολογιστή σε σχέση με ping στη διεύθυνση loopback αυτού 127.0.0.1;: Όταν κάνουμε ping στο loopback ελέγχεται αν η TCP/IP στοίβα πρωτοκόλλου είναι επιτυχώς εγκαταστημένη. Ελέγχουμε με άλλα λόγια αν το network software του υπολογιστή μας λειτουργεί ορθά. Μπορούμε να κάνουμε ping στο loopback ακόμα και αν ο υπολογιστής μας δεν είναι συνδεδεμένος στο διαδίκτυο. Από την άλλη όταν κάνουμε ping στο IP address του υπολογιστή μας ελέγχεται αν λειτουργεί ορθά το network Hardware. Μπορούμε να κάνουμε ping στην δικιά μας IP διεύθυνση μόνο αν είμαστε συνδεδεμένοι στο διαδίκτυο. Δηλαδή: Όταν κάνουμε ping στο loopback τα πακέτα εισέρχονται στον βρόγχο επανατροφοδότησης μέσω του loopback adapter ο οποίος είναι kernel based. Από την άλλη όταν κάνουμε ping στη δικιά μας διεύθυνση IP τα πακέτα εισέρχονται στον βρόγχο επανατροφοδότησης μέσω της κάρτας δικτύου (Network adapter).

Ανοίγουμε τον φυλλομετρητή και επισκεπτόμαστε την ιστοσελίδα της Netflix (<https://www.netflix.com>).

Μόλις η σελίδα φορτώσει, χρησιμοποιούμε την εντολή ping ώστε να παράγονται πακέτα IPv4/ICMP με προορισμό τον εξυπηρετητή www.netflix.com.

Στη συνέχεια επισκεπτόμαστε την ιστοσελίδα της Amazon (<https://www.amazon.com>).

Μόλις η σελίδα φορτώσει, χρησιμοποιούμε όπως πριν την εντολή ping με προορισμό τον εξυπηρετητή www.amazon.com.

```
petrosrapto@petrosraptoAssistant:~$ ping www.netflix.com
PING apiproxy-website-nlb-prod-2-b4de62b516adfbbf.elb.eu-west-1.amazonaws.com (5
4.73.148.110) 56(84) bytes of data.
^C
--- apiproxy-website-nlb-prod-2-b4de62b516adfbbf.elb.eu-west-1.amazonaws.com ping
g statistics ---
31 packets transmitted, 0 received, 100% packet loss, time 30708ms

petrosrapto@petrosraptoAssistant:~$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (52.85.159.175) 56(84) bytes of data.
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=1 ttl=248 time=2.83 ms
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=2 ttl=248 time=3.96 ms
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=3 ttl=248 time=2.86 ms
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=4 ttl=248 time=5.64 ms
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=5 ttl=248 time=3.78 ms
64 bytes from server-52-85-159-175.ath50.r.cloudfront.net (52.85.159.175): icmp_
seq=6 ttl=248 time=3.07 ms
^C
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 2.825/3.687/5.638/0.975 ms
```

2.7) Τι παράδοξο παρατηρείτε και τι μπορείτε να υποθέσετε για να το εξηγήσετε::

Παρατηρούμε ότι η εκτέλεση της εντολής ping www.netflix.com μπλοκάρει. Μόλις τερματίζουμε βιαίως την εκτέλεσή της, πληροφορούμαστε ότι έχουμε 100% packet loss.

Αντίθετα η εντολή ping www.amazon.com εκτελείται ορθά με 0% packet loss.

Σύμφωνα με τη θεωρία η εντολή ping ελέγχει εάν μια διεπαφή (interface) με δεδομένη διεύθυνση IP είναι ενεργή.

Όμως αν βρεθεί μια επαφή ανενεργή (όπως στην περίπτωσή μας επειδή δεν έχουμε Echo Reply), δεν εξυπακούεται ότι πράγματι είναι. Αν δε ληφθεί Echo Reply από τον προορισμό, υπάρχει πιθανότητα να παρεμβάλλεται στη διαδρομή κάποιο τείχος προστασίας (firewall), που να μπλοκάρει τα μηνύματα του πρωτοκόλλου ICMP.

Επίσης είναι δυνατό ο κόμβος προορισμού ή κάποια ενδιάμεση συσκευή να μην είναι επαρκώς πληροφορημένη

για το δίκτυο του αποστολέα και έτσι να μην είναι δυνατή η σωστή επιστροφή της απάντησης.

Άσκηση 3: Επικεφαλίδες IPv4

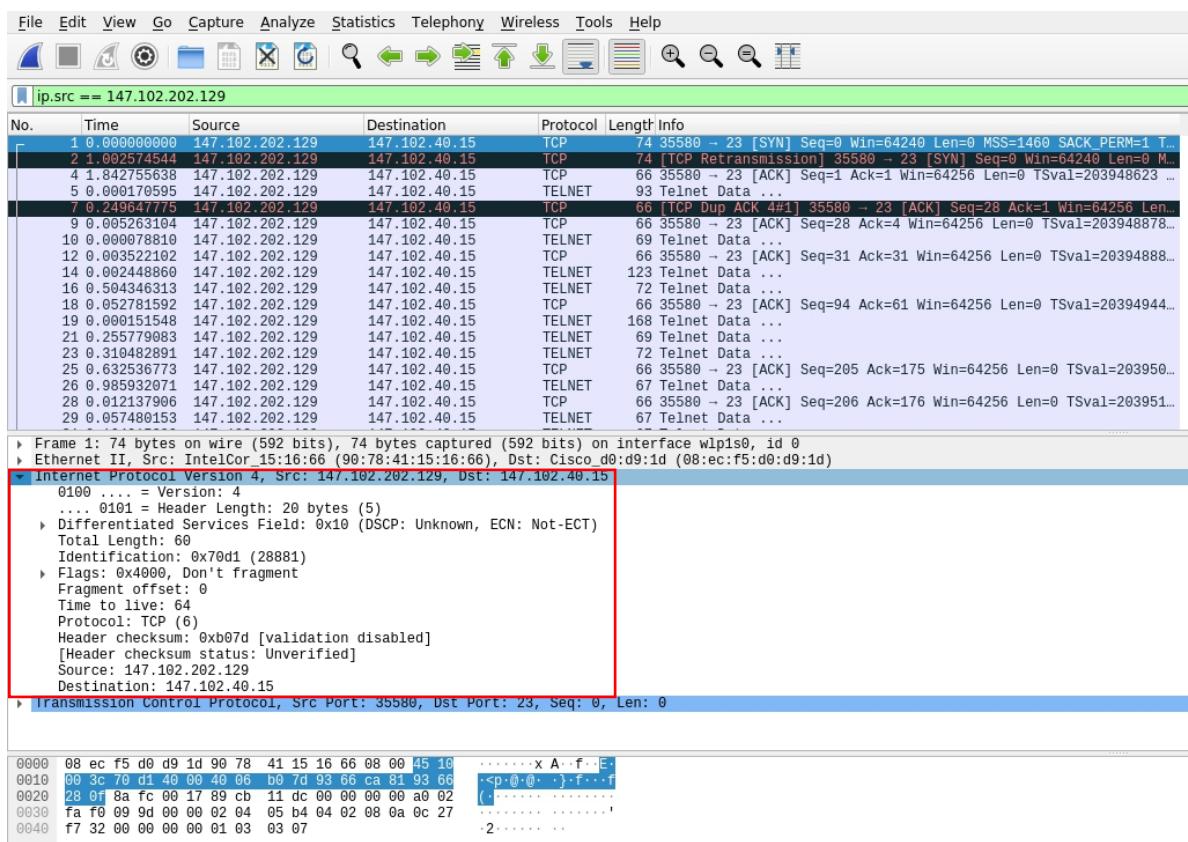
Ξεκινάμε μια νέα καταγραφή Wireshark με φίλτρο σύλληψης τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr.

Στη συνέχεια κάνουμε χρήση των υπηρεσιών Telnet και FTP του υπολογιστή edu-dy.cn.ntua.gr με IPv4 διεύθυνση 147.102.40.15.

3.1) Σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσαμε: host 147.102.40.15

3.2) Σύνταξη φίλτρου απεικόνισης ώστε να παραμένουν μόνο τα πακέτα IPv4 που έστειλε ο υπολογιστής μας:

ip.src == 147.102.202.129



3.3) Ονόματα και μήκος σε bit των πεδίων της επικεφαλίδας του πακέτου IPv4:

Όπως φαίνεται στην παραπάνω εικόνα, η επικεφαλίδα IPv4 αρχίζει από το 15^o byte του πλαισίου.

Τα παρακάτω πεδία βρίσκονται διαδοχικά στην επικεφαλίδα IPv4:

Version - 4 bits, Header Length 4 bits, Differentiated Services Field - 8 bits, Total Length - 16 bits,

Identification - 16 bits, Flags και Fragment Offset - 16 bits, Time to live - 8 bits, Protocol - 8 bits,

Header checksum - 16 bits, Source - 32 bits, Destination - 32 bits

Χρησιμοποιώντας το πλήκτρο ↓ (κάτω βέλος) μετακινούμαστε από το πρώτο στο τελευταίο μήνυμα της σειράς πακέτων IPv4 που έστειλε ο υπολογιστής μας.

3.4) Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν τιμές;

Differentiated Services Field, Total Length, Identification, Header checksum

3.5) Είναι το μήκος της επικεφαλίδας IPv4 το ίδιο σε όλα τα πακέτα;; Ναι

3.6) Μικρότερο: 52 bytes και μεγαλύτερο: 154 bytes μήκος πακέτου IPv4 που παρατηρήσαμε.

3.7) Τι τιμή έχει το πεδίο Differentiated Services Field και σε ποια ποιότητα υπηρεσίας αντιστοιχεί;

Παρατηρούμε ότι όλα τα πακέτα έχουν την τιμή οχιο (Network operations, administration and management) στο πεδίο Differentiated Services Field εκτός από ένα το οποίο έχει την τιμή οχοο (Standard Service Class).

3.8) Τι παρατηρείτε για τις τιμές του πεδίου Identification; Καθώς κατεβαίνουμε αυξάνονται κατά ένα.

3.9) Τι τιμή έχει η σημαία Don't Fragment;; Έχει την τιμή 1.

3.10) Τι τιμή έχει το πεδίο Fragment Offset;; Έχει την τιμή 0.

3.11) Τι τιμή έχει το πεδίο Protocol και σε ποιο πρωτόκολλο αντιστοιχεί;; 0x06 (TCP)

3.12) Γιατί σε κάθε πακέτο IPv4 αλλάζει η τιμή του πεδίου Header Checksum;;

Το πεδίο Header Checksum αποτελεί μηχανισμό διόρθωσης σφαλμάτων στην επικεφαλίδα του IPv4 και προκύπτει από αριθμητικές πράξεις πάνω στα bits της εκάστοτε επικεφαλίδας.

Αφού οι επικεφαλίδες των πακέτων δεν είναι ίδιες (σύμφωνα με το ερώτημα 3.4) και το πεδίο Header Checksum δεν θα έχει την ίδια τιμή για κάθε πακέτο.

Άσκηση 4: Θρυμματισμός στο IPv4

4.1) Ποια είναι η ακριβής σύνταξη της εντολής ping που πρέπει να χρησιμοποιήσετε ώστε να στείλετε χωρίς θρυμματισμό ένα μόνο πακέτο IPv4 που να μεταφέρει μήνυμα ICMP Echo request με συγκεκριμένο μέγεθος δεδομένων;; ping -n 1 -l <number of bytes> -f <IP_address>

Εφαρμόζοντας την παραπάνω σύνταξη της εντολής δοκιμάζουμε στους υπολογιστές του εργαστηρίου διάφορες τιμές για το μέγεθος δεδομένων ICMP στην περιοχή των 1480 byte κάνοντας ping με προορισμό τη διεύθυνση IPv4 κάποιου ενεργού κόμβου στο τοπικό μας δίκτυο (πχ default gateway).

4.2) Ποια είναι η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή; 1472 bytes

4.3) Ποια η μικρότερη τιμή για την οποία απαιτείται θρυμματισμός; 1473 bytes

The image shows two side-by-side windows from a Microsoft Windows XP system. Both windows are titled 'C:\WINDOWS\system32\cmd.exe' and show command-line outputs.

Left Window (Ping 1480 bytes):

```
C:\Documents and Settings\labuser>ping -n 1 -l 1480 -f 147.102.38.200
Pinging 147.102.38.200 with 1480 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 147.102.38.200:
  Packets: Sent = 1, Received = 0, Lost = 1 <100% loss>,
```

Right Window (Ping --help):

```
C:\Documents and Settings\labuser>ping --help
Bad option --help.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [-j host-list] [-k host-list]
           [-w timeout] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet.
  -i TTL      Time To Live.
  -v TOS      Type Of Service.
  -r count    Record route for count hops.
  -s count    Timestamp for count hops.
  -j host-list Loose source route along host-list.
  -k host-list Strict source route along host-list.
  -w timeout  Timeout in milliseconds to wait for each reply.
```

Bottom Taskbar:

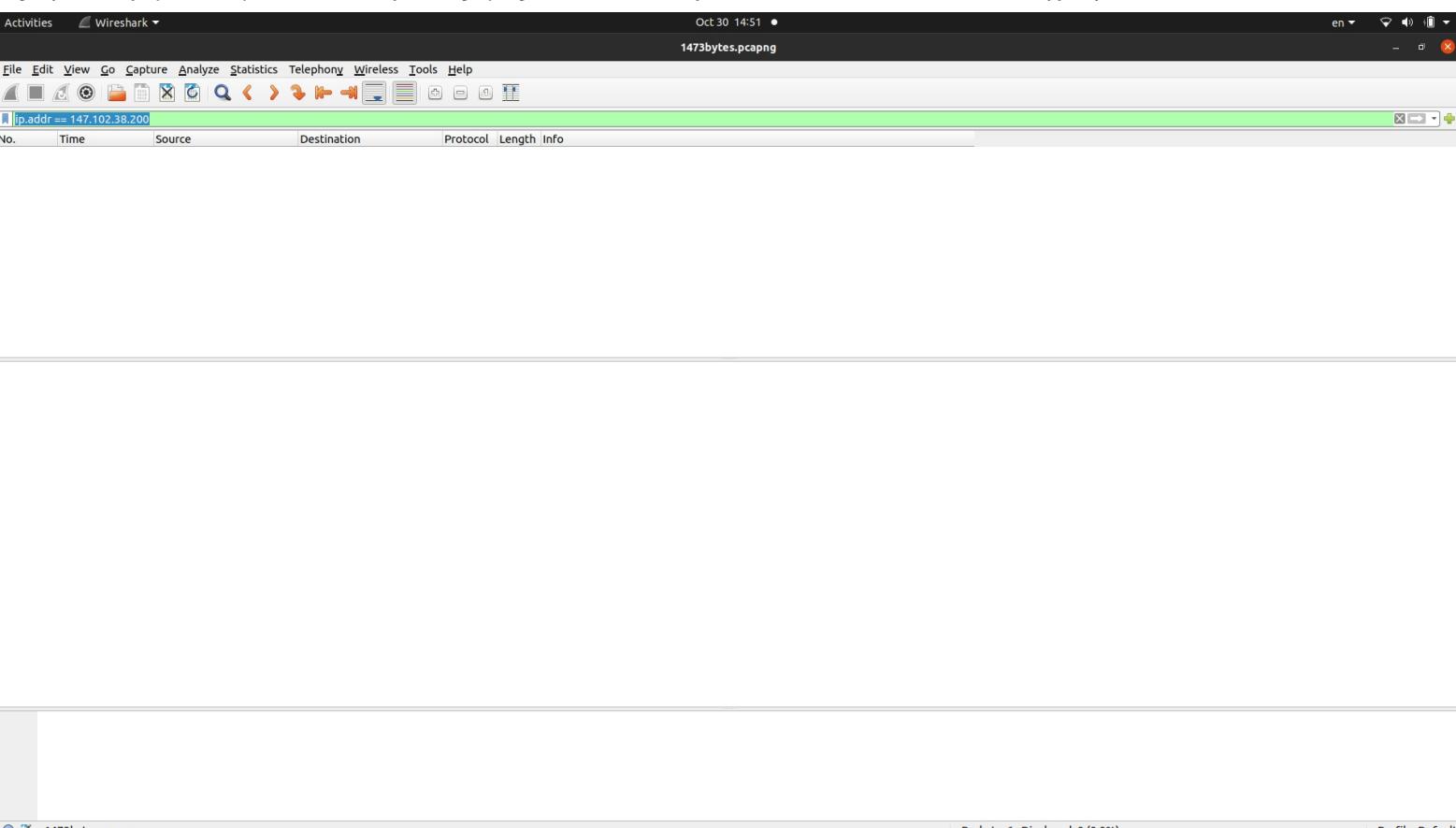
Start | Internet Explorer | New OpenDocument Tex... | C:\WINDOWS\system32... | 11:16 πμ

Στη συνέχεια χρησιμοποιούμε το Wireshark με φίλτρο σύλληψης ώστε να καταγράφονται μόνο πλαίσια μονο-εκπομπής (unicast). Επαναλαμβάνουμε τα ping για τις δύο τιμές που προσδιορίσαμε προηγουμένως στα ερωτήματα 4.2 και 4.3, αντίστοιχα. Μόλις ολοκληρωθεί η καταγραφή, εφαρμόζουμε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα IPv4 από και προς τη διεύθυνση IPv4 όπου κάνατε ping.

4.4) Γράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε: not multicast and not broadcast

4.5) Γράψτε τη σύνταξη του φίλτρου απεικόνισης που εφαρμόσατε: ip.addr == 147.102.38.200

4.6) Παράγονται πακέτα IPv4 όταν χρησιμοποιείτε την τιμή της ερώτησης 4.3; Γιατί; Όχι. Η τιμή αυτή είναι μεγαλύτερη από την MTU και άρα το μήνυμα ICMP δεν προωθείται. Συνεπώς δεν καταγράφεται από το Wireshark.



4.7) Ποιο είναι το μέγεθος της MTU της διεπαφής του υπολογιστή σας; Αιτιολογήστε.: 1500 bytes

Γνωρίζουμε ότι η MTU (Maximum Transmission Unit) αντιπροσωπεύει το μέγεθος του μεγαλύτερου πακέτου IPv4 που μπορεί να μεταδοθεί χωρίς θρυμματισμό. Συνεπώς στο Total Length βλέπουμε το μέγεθος του πακέτου που καταγράφει το Wireshark, το οποίο εκτελέστηκε επιτυχώς και ήταν η μεγαλύτερη τιμή του ping.

4.8) Ποια τιμή του μεγέθους δεδομένων ICMP οδηγεί σε πακέτο IPv4 μέγιστου μήκους: 1472 bytes

No.	Time	Source	Destination	Protocol	Length	Info
46	5.841949	147.102.38.52	147.102.38.200	ICMP	1514	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in...
47	5.842472	147.102.38.200	147.102.38.52	ICMP	1514	Echo (ping) reply id=0x0200, seq=2304/9, ttl=255 (request ...

Frame 46: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0
Ethernet II, Src: IBM_f8:f8:f3 (00:11:25:f8:f8:f3), Dst: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
Destination: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
Source: IBM_f8:f8:f3 (00:11:25:f8:f8:f3)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 147.102.38.52, Dst: 147.102.38.200
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xf3a7 (62375)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x8db0 [validation disabled]
[Header checksum status: Unverified]
Source: 147.102.38.52
Destination: 147.102.38.200
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x3548 [correct]
[Checksum Status: Good]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)
Sequence number (BE): 2304 (0x0900)
Sequence number (LE): 9 (0x0009)
[Response frame: 47]
Data (1472 bytes)

4.9) Για την προηγούμενη τιμή μεγέθους δεδομένων ICMP και με απαίτηση μη θρυμματισμού, επιτυγχάνει το ping προς τη διεύθυνση IPv4 του υπολογιστή σας; Εάν όχι, ποια είναι η μέγιστη τιμή για την οποία είναι επιτυχές;;

Επιτυγχάνει το ping

4.10) Τι μέγεθος έχει το μεγαλύτερο πακέτο IPv4 που μπορεί να παράγει η εντολή ping;

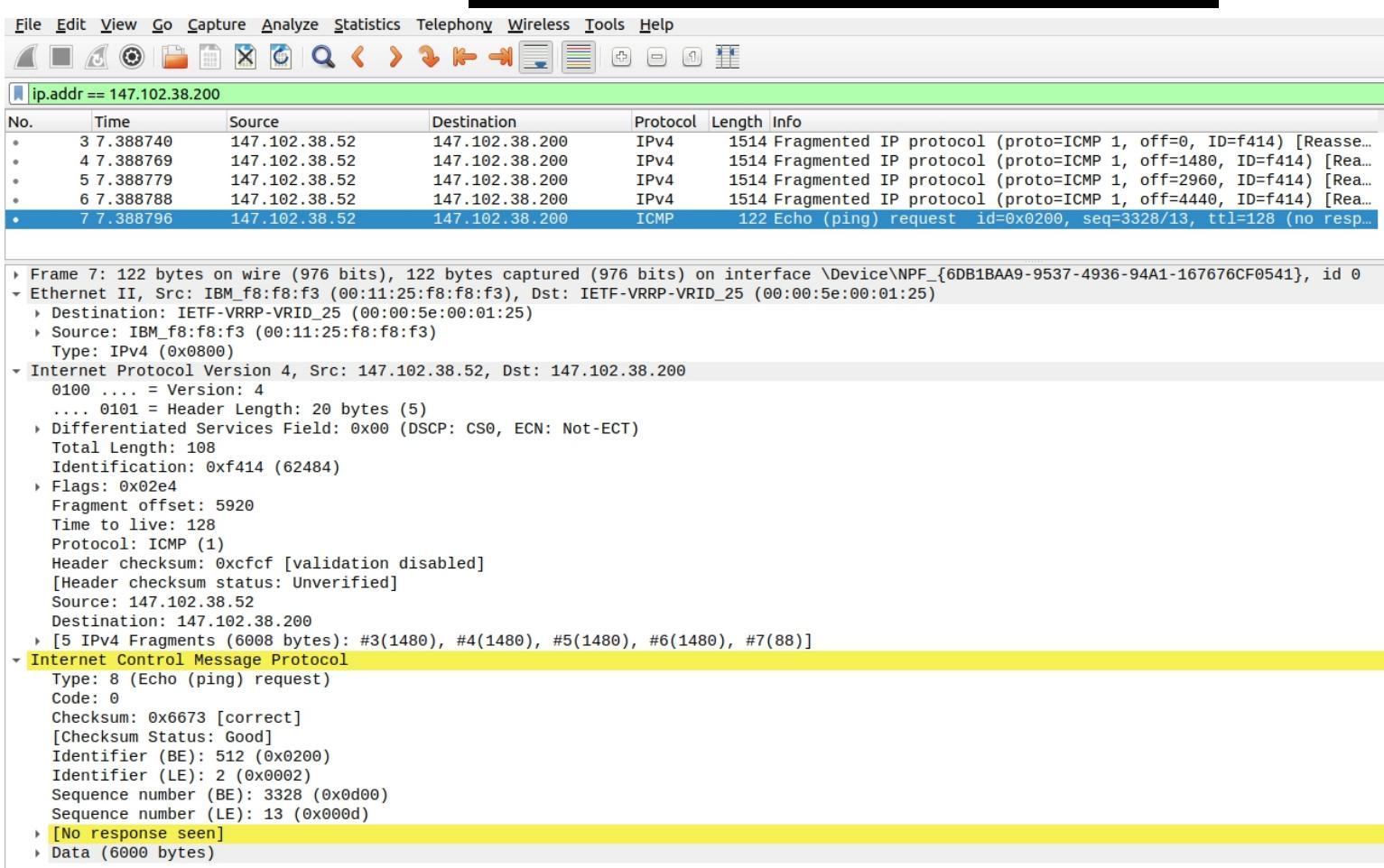
Σύμφωνα με τη θεωρία το μέγιστο μέγεθος πακέτου IPv4 είναι 65.535 byte. Όμως σε ένα Ethernet LAN το μέγιστο μέγεθος πλαισίου είναι το πολύ 1.518 byte (δηλαδή μέγιστο μέγεθος πακέτου IPv4 περίπου 1500 bytes).

Συνεπώς αυτά είναι τα όρια για τα πακέτα που παράγει η εντολή ping.

Με τα ίδια φίλτρα σύλληψης και απεικόνισης ξεκινάμε μια καταγραφή και κάνουμε ping προς προορισμό εντός του τοπικού σας δικτύου στέλνοντας ένα μόνο μήνυμα ICMP με μέγεθος δεδομένων 6.000, χωρίς την απαίτηση μη θρυμματισμού του πακέτου IPv4.

```
C:\Documents and Settings\labuser>ping -n 1 -l 6000 147.102.38.200
Pinging 147.102.38.200 with 6000 bytes of data:
Request timed out.

Ping statistics for 147.102.38.200:
    Packets: Sent = 1, Received = 0, Lost = 1 <100% loss>,
```



4.11) Βρείτε το πρώτο μήνυμα ICMP Echo Request που έστειλε ο υπολογιστής σας. Έχει μεταφερθεί μήνυμα αυτό ως ένα πακέτο IPv4; Όχι, το μήνυμα ICMP Echo Request δεν έχει μεταφερθεί ως ένα πακέτο IPv4.

4.12) Εάν όχι, πόσα πακέτα IPv4 χρειάσθηκαν και γιατί; Χρειάστηκαν 5 fragments. Τα fragments μεταδίδονται ως πακέτα IPv4 (και όχι ICMP) και συνεπώς μπορούν πλέον να μεταφέρουν το μέγιστο 1480 bytes, και όχι 1472 bytes όπως είδαμε στα προηγούμενα ερωτήματα, καθώς παραλείπεται η επικεφαλίδα ICMP (που είναι 8 bytes).

Άρα $6000/1480 = 4.054\dots$ συνεπώς χρειάζονται 5 πακέτα IPv4 ώστε να μεταφερθεί η συνολική πληροφορία.

4.13) Για καθένα από αυτά τα πακέτα IPv4, καταγράψτε τις τιμές των πεδίων της επικεφαλίδας που σχετίζονται με τον θρυμματισμό (Identification, Don't Fragment Bit, More Fragments Bit, Fragment Offset).:

Πακέτο #3: Identification: 62484, Don't Fragment Bit: 0, More Fragments Bit: 1, Fragment Offset: 0

Πακέτο #4: Identification: 62484, Don't Fragment Bit: 0, More Fragments Bit: 1, Fragment Offset: 1480

Πακέτο #5: Identification: 62484, Don't Fragment Bit: 0, More Fragments Bit: 1, Fragment Offset: 2960

Πακέτο #6: Identification: 62484, Don't Fragment Bit: 0, More Fragments Bit: 1, Fragment Offset: 4440

Πακέτο #7: Identification: 62484, Don't Fragment Bit: 0, More Fragments Bit: 0, Fragment Offset: 5920

4.14) Επιλέξτε το πρώτο από τα παραπάνω πακέτα IPv4 (το πρώτο θραύσμα). Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι το πακέτο έχει θρυμματιστεί;: More Fragments Bit

ip.addr == 147.102.38.200						
No.	Time	Source	Destination	Protocol	Length	Info
3	7.388740	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f414) [Reasse...
4	7.388769	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=f414) [Rea...
5	7.388779	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=f414) [Rea...
6	7.388788	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=f414) [Rea...
•	7.388796	147.102.38.52	147.102.38.200	ICMP	122	Echo (ping) request id=0x0200, seq=3328/13, ttl=128 (no resp...

```

Frame 3: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0
Ethernet II, Src: IBM_f8:f8:f3 (00:11:25:f8:f8:f3), Dst: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
  Destination: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
  Source: IBM_f8:f8:f3 (00:11:25:f8:f8:f3)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 147.102.38.52, Dst: 147.102.38.200
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xf414 (62484)
    Flags: 0x2000, More fragments
      0... .... .... = Reserved bit: Not set
      .0... .... .... = Don't fragment: Not set
      ..1. .... .... = More fragments: Set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xad43 [validation disabled]
    [Header checksum status: Unverified]
    Source: 147.102.38.52
    Destination: 147.102.38.200
    Reassembled IPv4 in frame: 7
  Data (1480 bytes)

```

4.15) Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι αυτό είναι το πρώτο θραύσμα και όχι ένα μεταγενέστερο;: Fragment Offset: 0

4.16) Ποιο είναι το μήκος του πρώτου θραύσματος;: Μήκος Πακέτου: 1500 bytes, Μήκος Πλαισίου: 1514 bytes

4.17) Επιλέξτε το δεύτερο από τα παραπάνω πακέτα IPv4 (το δεύτερο θραύσμα). Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι δεν είναι το πρώτο θραύσμα;: Fragment Offset ≠ 0

ip.addr == 147.102.38.200						
No.	Time	Source	Destination	Protocol	Length	Info
3	7.388740	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f414) [Reasse...
4	7.388769	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=f414) [Rea...
5	7.388779	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=f414) [Rea...
6	7.388788	147.102.38.52	147.102.38.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=f414) [Rea...
•	7.388796	147.102.38.52	147.102.38.200	ICMP	122	Echo (ping) request id=0x0200, seq=3328/13, ttl=128 (no resp...

```

Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0
Ethernet II, Src: IBM_f8:f8:f3 (00:11:25:f8:f8:f3), Dst: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
  Destination: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
  Source: IBM_f8:f8:f3 (00:11:25:f8:f8:f3)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 147.102.38.52, Dst: 147.102.38.200
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xf414 (62484)
    Flags: 0x20b9, More fragments
      0... .... .... = Reserved bit: Not set
      .0... .... .... = Don't fragment: Not set
      ..1. .... .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xac8a [validation disabled]
    [Header checksum status: Unverified]
    Source: 147.102.38.52
    Destination: 147.102.38.200
    Reassembled IPv4 in frame: 7
  Data (1480 bytes)

```

4.18) Ακολουθούν άλλα θραύσματα;: Ναι

4.19) Πώς το αναγνωρίζετε από τις πληροφορίες της επικεφαλίδας μόνο;: More Fragments Bit = 1

4.20) Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν μεταξύ του πρώτου και του δεύτερου θραύσματος;: Fragment Offset (και Header Checksum)

4.21) Δικαιολογήστε τις τιμές του πεδίου Fragment offset για το προτελευταίο και τελευταίο θραύσμα που στάλθηκε.: Το προτελευταίο θραύσμα είναι το 4° ενώ το τελευταίο είναι το 5°. Κάθε θραύσμα που έχει προηγθεί των εν λόγω θραυσμάτων έχει μεταφέρει 1480 bytes. Συνεπώς το fragment offset για το προτελευταίο πρέπει να είναι $3 \times 1480 = 4440$ (αρχίζουμε την μέτρηση από το 0) ενώ για το τελευταίο $4 \times 1480 = 5920$.

4.22) Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν μεταξύ των θραυσμάτων;:

Fragment Offset(, Header Checksum) και More Fragments Bit, Total Length