

**ΟΙΚΟΝΟΜΙΚΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΑΘΗΝΩΝ**



**ATHENS UNIVERSITY  
OF ECONOMICS  
AND BUSINESS**

---

# Δίκτυα Επικοινωνίων

## Εργασία 1<sup>η</sup> – Wireshark

20 Νοεμβρίου 2016

3100161 – Σάκος Ιωσήφ

## Περιεχόμενα

1.Γενικές Πληροφορίες.....	3
2.Διαδικασία Ping: Ανάλυση με Wireshark.....	3
2.1.Ping: Απαντήσεις Ερωτήσεων.....	5
3.Διαδικασία Traceroute: Ανάλυση με Wireshark.....	12
3.1.Traceroute: Απαντήσεις Ερωτήσεων.....	13
4.Βιβλιογραφία.....	19

## Εικόνες

Εικόνα 2.1: Εκτέλεση Whireshark και έναρξη διαδικασίας ανίχνευσης πακέτων.....	3
Εικόνα 2.2: Εκτέλεση της εντολής ping -c 3 scholar.google.com.....	4
Εικόνα 2.3: Ολοκλήρωση διαδικασίας ανίχνευσης πακέτων.....	4
Εικόνα 2.4: Στατιστικά της ανίχνευσης.....	5
Εικόνα 2.5: Ιεραρχία πρωτοκόλλων της ανίχνευσης.....	6
Εικόνα 2.6: Εφαρμογή φίλτρου icmp.....	6
Εικόνα 2.7: Καρτέλα Internet Protocol Version 4, σε πακέτο Echo Request.....	7
Εικόνα 2.8: Καρτέλα Internet Control Message Protocol, σε πακέτο Echo Request.....	8
Εικόνα 2.9: Καρτέλα Internet Control Message Protocol, σε πακέτο Echo Reply.....	9
Εικόνα 2.10: Καρτέλα Internet Protocol Version 4, σε πακέτο Echo Reply.....	10
Εικόνα 2.11: Ταξινόμηση με βάση τους χρόνους απόκρισης.....	11
Εικόνα 3.1: Εκτέλεση της εντολής sudo traceroute -I -N 1 scholar.google.com.....	12
Εικόνα 3.2: Ολοκλήρωση διαδικασίας ανίχνευσης πακέτων.....	13
Εικόνα 3.3: Καρτέλα Internet Protocol Version 4, σε πακέτο Echo Request.....	14
Εικόνα 3.4: Καρτέλα Internet Protocol Version 4, σε πακέτο Time Exceeded Message.....	15
Εικόνα 3.5: TTL των πακέτων Echo Request.....	16
Εικόνα 3.6: Χρονικό διάστημα μέχρι το πρώτο Time Exceeded Message.....	17
Εικόνα 3.7: Διευθύνσεις IP που αντοπίστηκαν στην ανίχνευση.....	18

## Πίνακες

Πίνακας 2.1: Χρόνοι Απόκρισης.....	11
Πίνακας 3.1: Διευθύνσεις Κόμβων του Μονοπατιού.....	18

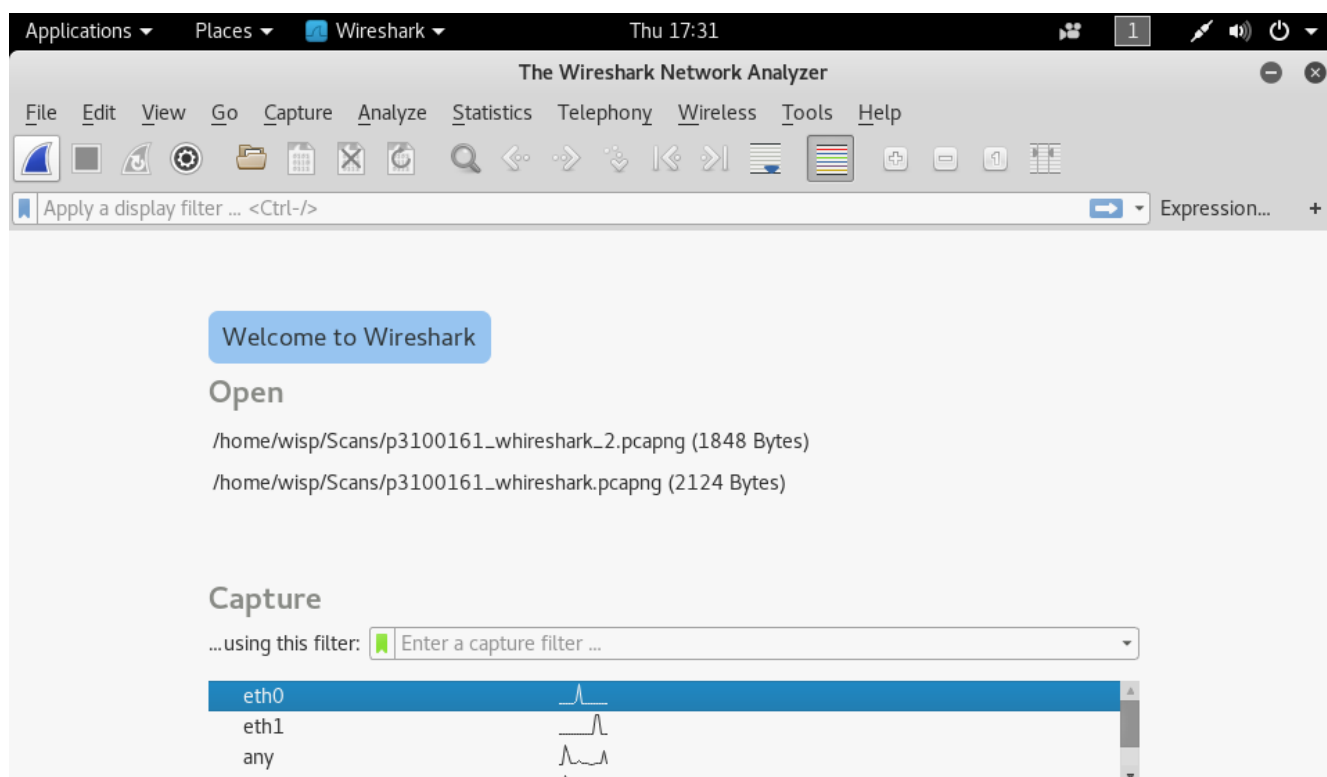
# 1. Γενικές Πληροφορίες

Το λειτουργικό σύστημα που θα χρησιμοποιήσω για την παρουσίαση του λογισμικού Wireshark είναι το Kali Rolling (2016.2) x64 το οποίο βασίζεται στο λειτουργικό Debian. Το ίδιο το λειτουργικό είναι εγκατεστημένο σε ένα Virtual Box και είναι συνδεδεμένο σε ένα δίκτυο NAT μέσω της διεπαφής eth0.

Κατά την διάρκεια των αναλύσεων η διεύθυνση IPv4 του μηχανήματος για την διεπαφή eth0 ήταν η 10.0.2.15.

## 2. Διαδικασία Ping: Ανάλυση με Wireshark

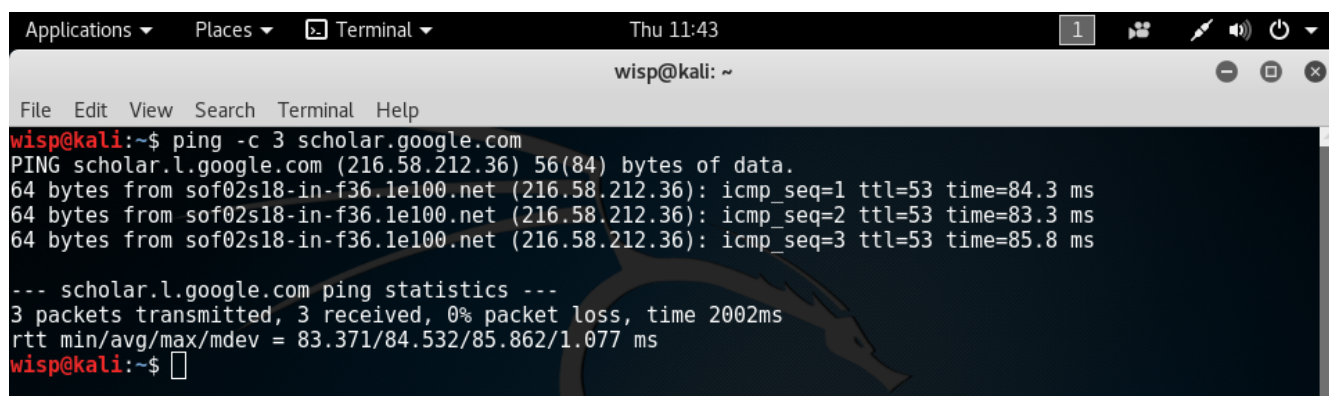
Αρχικά εκτελώ το Wireshark και ξεκινάω την διαδικασία της ανίχνευσης επιλέγοντας την διεπαφή eth0 και πατώντας την επιλογή **Start Capturing Packets**.



Εικόνα 2.1: Εκτέλεση Whireshark και έναρξη διαδικασίας ανίχνευσης πακέτων

Στην συνέχεια εκτελώ την εντολή **ping -c 3 scholar.google.com** στην γραμμή εντολών ώστε να αποστείλω τρία ICMP πακέτα τύπου Echo Request (8) στον host, scholar.google.com με διεύθυνση IPv4, 216.58.212.36<sup>1</sup> όπως φαίνεται και στην εικόνα 2.2

<sup>1</sup> Η εφαρμογή Ping θα πρέπει πρώτα να προσδιορίσει την διεύθυνση IP του host μέσω του DNS πρωτοκόλλου προτού αποστείλει τα ICMP πακέτα. Αυτά τα DNS πακέτα θα εμφανιστούν και στην ανίχνευση του Whireshark.

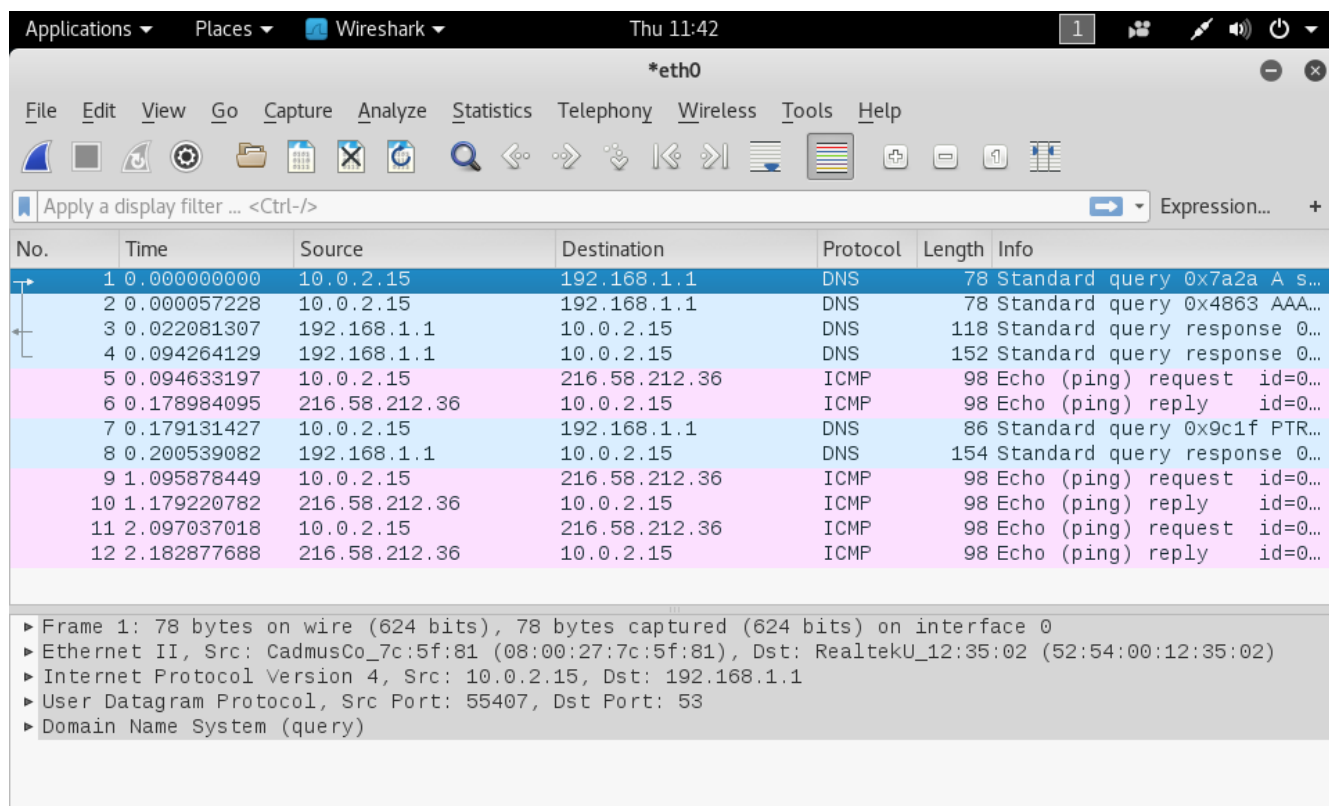


```
wisp@kali:~$ ping -c 3 scholar.google.com
PING scholar.l.google.com (216.58.212.36) 56(84) bytes of data.
64 bytes from sof02s18-in-f36.1e100.net (216.58.212.36): icmp_seq=1 ttl=53 time=84.3 ms
64 bytes from sof02s18-in-f36.1e100.net (216.58.212.36): icmp_seq=2 ttl=53 time=83.3 ms
64 bytes from sof02s18-in-f36.1e100.net (216.58.212.36): icmp_seq=3 ttl=53 time=85.8 ms

--- scholar.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 83.371/84.532/85.862/1.077 ms
wisp@kali:~$
```

Εικόνα 2.2: Εκτέλεση της εντολής **ping -c 3 scholar.google.com**

Μετά την ολοκλήρωση της εντολής, το παράθυρο του Wireshark περιέχει μία λίστα με τα πακέτα που εντόπισε ο ανιχνευτής<sup>2</sup>. Από την στιγμή που έχω συλλέξει τα πακέτα που θέλω να αναλύσω μπορώ πλέον να σταματήσω την ανίχνευση πατώντας την επιλογή **Stop Capturing Packets**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	DNS	78	Standard query 0x7a2a A s...
2	0.000057228	10.0.2.15	192.168.1.1	DNS	78	Standard query 0x4863 AAA...
3	0.022081307	192.168.1.1	10.0.2.15	DNS	118	Standard query response 0...
4	0.094264129	192.168.1.1	10.0.2.15	DNS	152	Standard query response 0...
5	0.094633197	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
6	0.178984095	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...
7	0.179131427	10.0.2.15	192.168.1.1	DNS	86	Standard query 0x9c1f PTR...
8	0.200539082	192.168.1.1	10.0.2.15	DNS	154	Standard query response 0...
9	1.095878449	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
10	1.179220782	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...
11	2.097037018	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
12	2.182877688	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...

► Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
► Ethernet II, Src: CadmusCo\_7c:5f:81 (08:00:27:7c:5f:81), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
► Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1  
► User Datagram Protocol, Src Port: 55407, Dst Port: 53  
► Domain Name System (query)

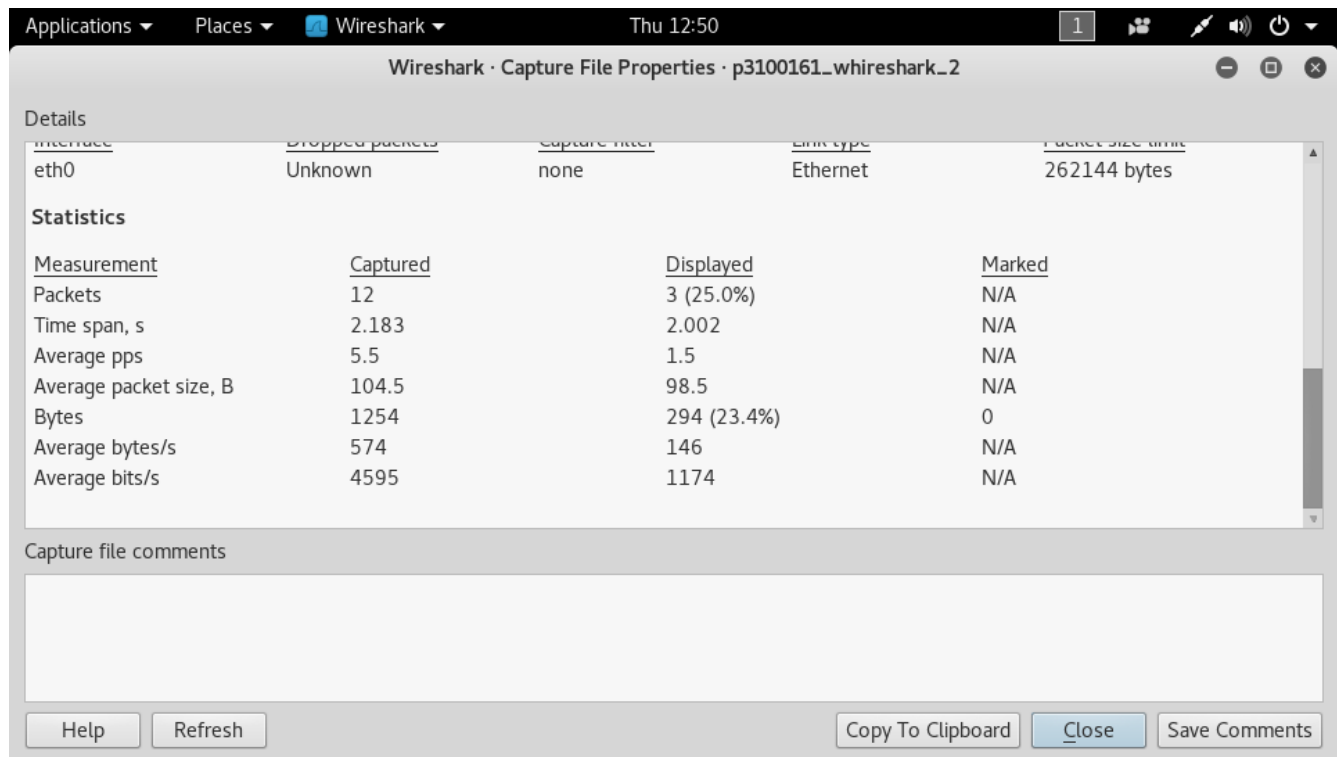
Εικόνα 2.3: Ολοκλήρωση διαδικασίας ανίχνευσης πακέτων

2 Το περιβάλλον στο οποίο εκτέλεσα το Wireshark είναι ιδιαίτερα ελεγχόμενο. Υπό κανονικές συνθήκες αυτή η λίστα θα περιέχει πολλά διαφορετικά είδη πακέτων.

## 2.1. Ping: Απαντήσεις Ερωτήσεων

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσης σας;

Μεταβαίνω στην επιλογή **Statistics** → **Capture File Properties** από το μενού. Μπορώ να δω την διάρκεια της ανίχνευσης στην περιοχή **Time: Elapsed** ή πιο αναλυτικά στην περιοχή **Statistics: Time span, s**. Η συγκεκριμένη ανίχνευση διήρκησε 2.183 δευτερόλεπτα.



Εικόνα 2.4: Στατιστικά της ανίχνευσης

2. Προσδιορίστε ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στην χρονική διάρκεια της ανίχνευσης.

Μεταβαίνω στην επιλογή **Statistics** → **Protocol Hierarchy** από το μενού. Στο νέο παράθυρο εμφανίζονται όλα τα πρωτόκολλα που εντοπίστηκαν στην ανίχνευση, σε ιεραρχική δομή, και διάφορα στατιστικά στοιχεία σχετικά με αυτά. Τα πρωτόκολλα του ανώτερου επιπέδου για κάθε πακέτο που εντοπιστικό στην συγκεκριμένη ανίχνευση είναι τα: Domain Name System (DNS) και Internet Control Message Protocol (ICMP).

Wireshark · Protocol Hierarchy Statistics · p3100161\_whoreshark\_2

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Pa
▼ Frame	100.0	12	100.0	1254	4595	0
▼ Ethernet	100.0	12	13.4	168	615	0
▼ Internet Protocol Version 4	100.0	12	19.1	240	879	0
▼ User Datagram Protocol	50.0	6	3.8	48	175	0
Domain Name System	50.0	6	33.0	414	1517	6
Internet Control Message Protocol	50.0	6	30.6	384	1407	6

No display filter.

Help Copy Close

Εικόνα 2.5: Ιεραρχία πρωτοκόλλων της ανίχνευσης

3. Πως θα δείτε μόνο τα πακέτα αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;

Στο κεντρικό παράθυρο του Wireshark εισάγω το φίλτρο **icmp** και τον εφαρμόζω πατώντας την επιλογή **Apply this filter string to the display** από την δεξιά μεριά της μπάρας.

p3100161\_whoreshark\_2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp Expression...

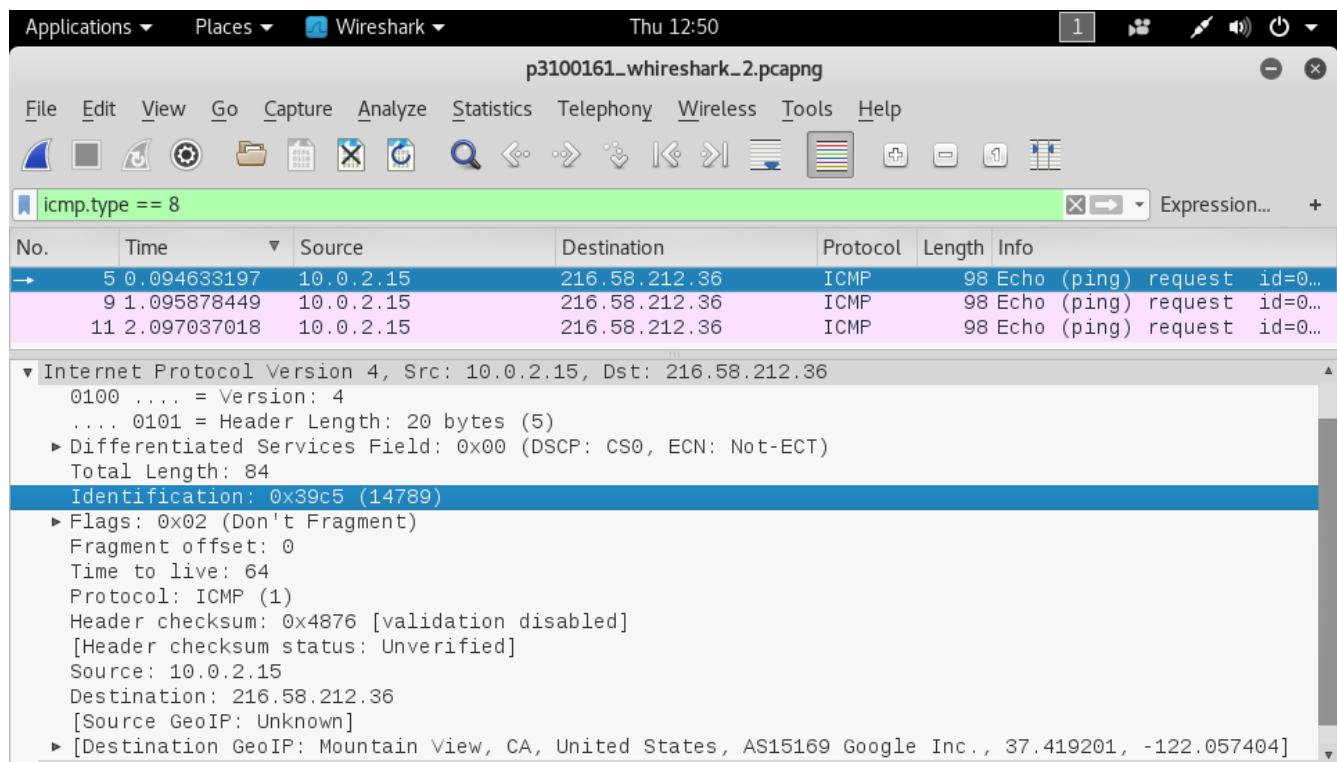
No.	Time	Source	Destination	Protocol	Length	Info
→ 5	0.094633197	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
← 6	0.178984095	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...
9	1.095878449	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
10	1.179220782	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...
11	2.097037018	10.0.2.15	216.58.212.36	ICMP	98	Echo (ping) request id=0...
12	2.182877688	216.58.212.36	10.0.2.15	ICMP	98	Echo (ping) reply id=0...

Εικόνα 2.6: Εφαρμογή φίλτρου icmp

4. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.
  - a. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του source;
  - b. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;
  - c. Πόσο είναι το time-to-live του πακέτου;
  - d. Ποιος είναι ο τύπος του ICMP πρωτοκόλλου;

Εφαρμόζω το φίλτρο **icmp.type == 8** ώστε στον κατάλογο των πακέτων να εμφανιστούν μόνο τα πακέτα ICMP τύπου Echo Request (8). Στην συνέχεια ταξινομώ τα πακέτα βάση της στήλης **Time** και επιλέγω το πρώτο πακέτο.

Στην περιοχή ανάλυσης εμφανίζονται όλα τα επίπεδα του συγκεκριμένου πακέτου. Επιλέγω την καρτέλα για να εξετάσω το συγκεκριμένο πρωτόκολλο.



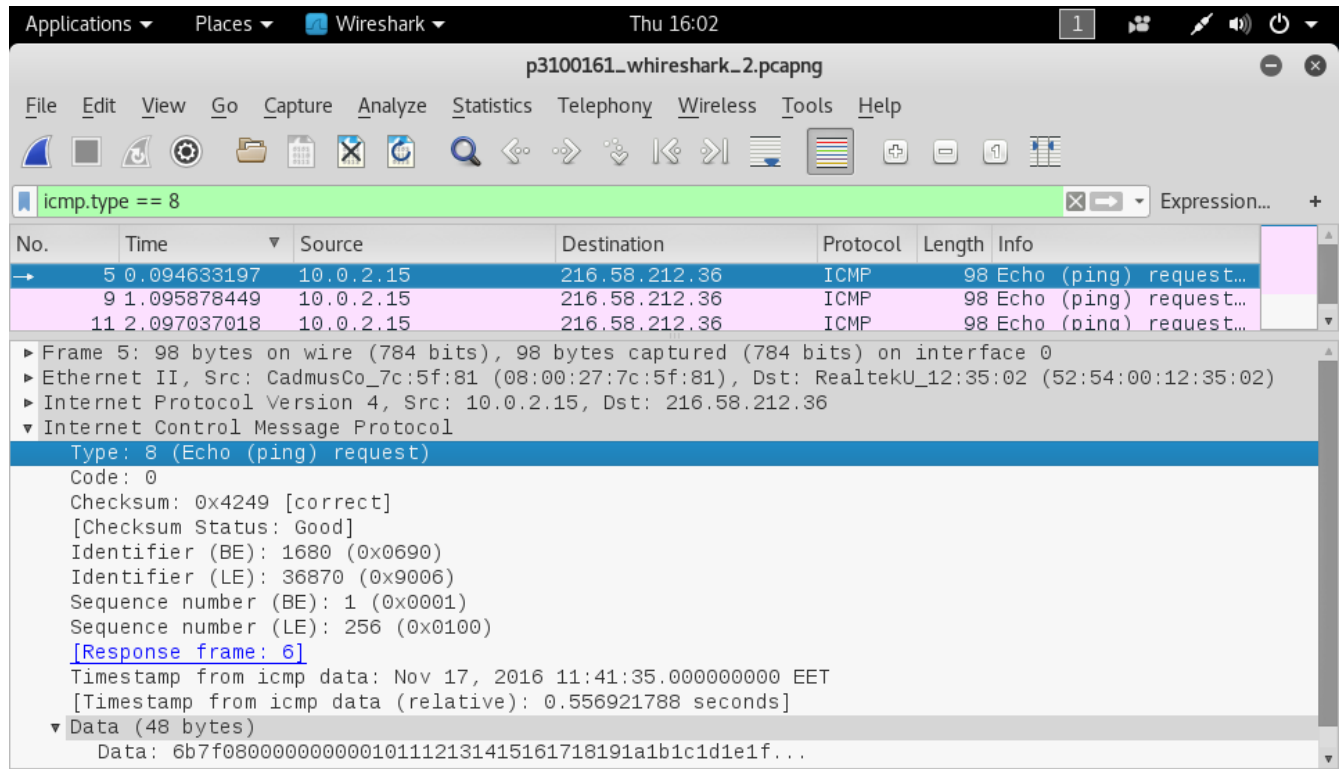
Εικόνα 2.7: Καρτέλα **Internet Protocol Version 4**, σε πακέτο Echo Request

Οι διευθύνσεις IP του αποστολέα (Source) και του παραλήπτη (Destination) αναφέρονται στα πεδία **Source** και **Destination** αντίστοιχα. Η ίδια πληροφορία αναφέρεται και στον τίτλο της καρτέλας **Internet Protocol Version 4**. Η διεύθυνση αποστολέα του συγκεκριμένου πακέτου όπως ήταν αναμενόμενο είναι η 10.0.2.15 και του παραλήπτη η 216.58.212.36.

Το μέγεθος των δεδομένων μπορεί να υπολογιστεί από το συνολικό μέγεθος του πακέτου, το οποίο αναφέρεται στο πεδίο **Total Length**, και το μέγεθος της επικεφαλίδας του πρωτοκόλλου, το οποίο αναφέρεται στο πεδίο **Header Length**. Το μέγεθος των δεδομένων που μεταφέρει το συγκεκριμένο πακέτο ισούται με  $84 - 20 = 64$  Bytes.

Το time-to-live (TTL) του πακέτου αναφέρεται στο πεδίο **Time to live** και για το συγκεκριμένο πακέτο είναι 64 Hops.

Προκειμένου να προσδιορίσω τον τύπο του ICMP μεταβαίνω στην καρτέλα **Internet Control Message Protocol**, εικόνα 2.8.



Εικόνα 2.8: Καρτέλα **Internet Control Message Protocol**, σε πακέτο Echo Request

Ο τύπος του πρωτοκόλλου ICMP αναφέρεται στο πεδίο **Type** και όπως ήταν αναμενόμενο για το συγκεκριμένο πακέτο είναι 8 (Echo (Ping) Request).

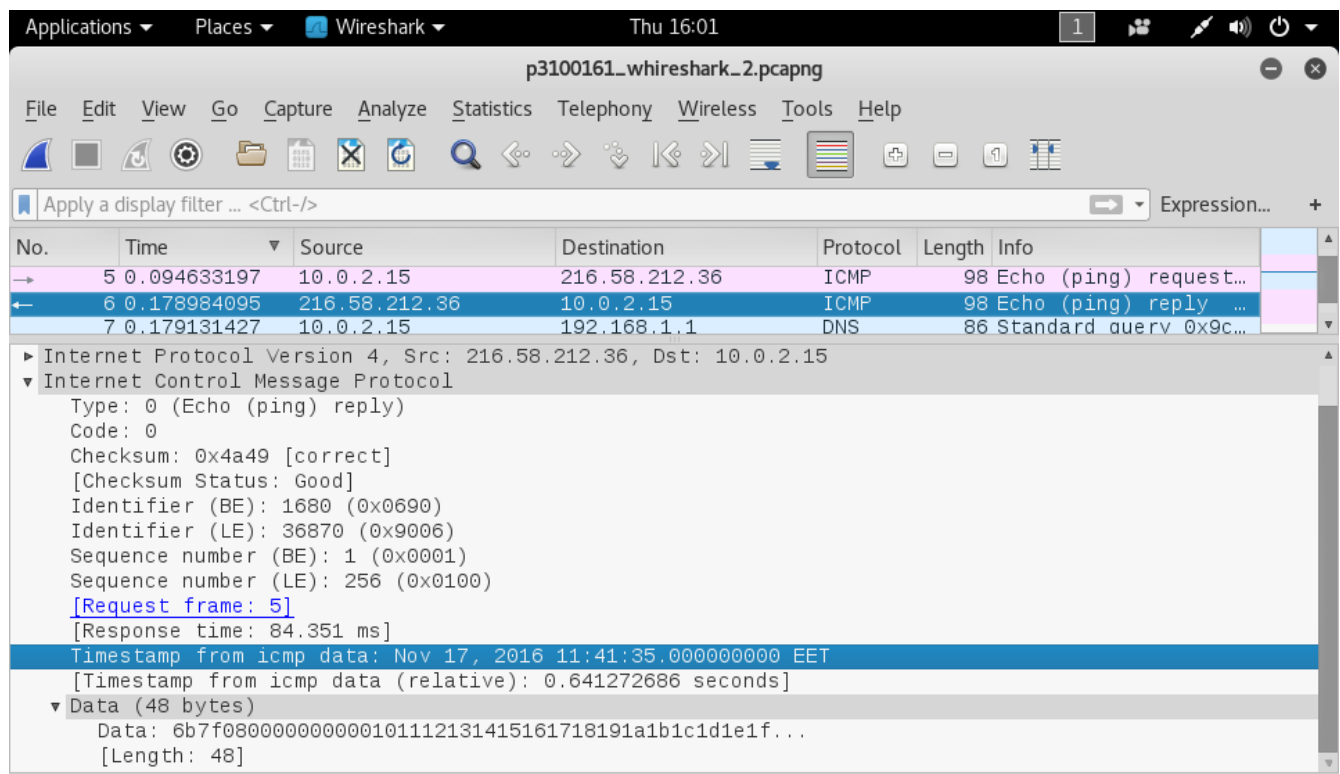
5. Εξετάστε το IP πακέτο που μεταφέρει το αντίστοιχο (πρώτο) ICMP Echo Reply.
  - a. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του source;
  - b. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;
  - c. Πόσο είναι το time-to-live του πακέτου;
  - d. Ποιος είναι ο τύπος του ICMP πρωτοκόλλου;
  - e. Συγκρίνεται τα πεδία Identifier και Sequence number στα δύο πακέτα (Request και αντίστοιχο Reply), τι διαπιστώνετε; Τι διαπιστώνετε σχετικά με τα δεδομένα που μεταφέρουν τα δύο αυτά πακέτα;

Αρχικά αφαιρώ το υπάρχον φίλτρο ώστε να εμφανιστούν στην λίστα του Wireshark όλα τα πακέτα της ανίχνευσης.

Μπορώ να μεταβώ στο αντίστοιχο Echo Reply του Echo Request του ερωτήματος 4 επιλέγοντας τον σύνδεσμο Response Frame που έχει προσθέσει το Wireshark στην καρτέλα **Internet Control Message Protocol** του πακέτου, εικόνα 2.8. Εναλλακτικά θα μπορούσα να χρησιμοποιήσω ένα φίλτρο

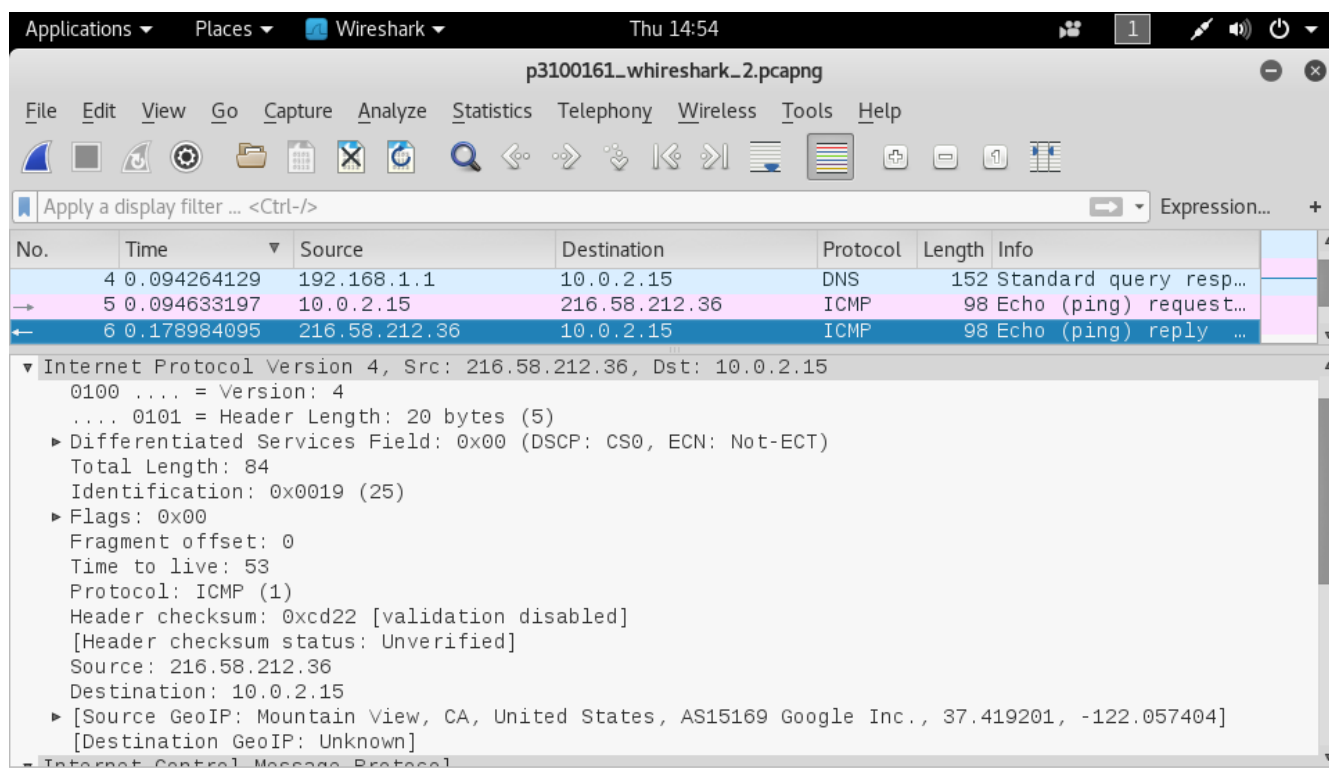


βασισμένο στα πεδία **Identifier** και **Sequence Number**.



Εικόνα 2.9: Καρτέλα **Internet Control Message Protocol**, σε πακέτο **Echo Reply**

Μετά την μεταβίβαση είναι ανοιχτή η καρτέλα **Internet Control Message Protocol** του πακέτου **Echo Reply**. Για να συλλέξω πληροφορίες για το πρωτόκολλο IP επιλέγω την καρτέλα **Internet Protocol Version 4**, εικόνα 2.10.



Εικόνα 2.10: Καρτέλα Internet Protocol Version 4, σε πακέτο Echo Reply

Τι περισσότερες πληροφορίες τις συλλέγω όπως και στο ερώτημα 4:

- Η διεύθυνση IP του αποστολέα (Source) είναι η 216.58.212.36.
- Η διεύθυνση IP του παραλήπτη (Destination) είναι η τοπική διεύθυνση 10.0.2.15.

Παρατηρώ ότι στο πακέτο Echo Reply ο αποστολέας και ο παραλήπτης έχουν αντιστραφεί.

- Το μέγεθος των δεδομένων είναι  $84 - 20 = 64$  Bytes.
- Το TTL είναι 53 Hops.

Τις εναπομείναντες πληροφορίες τις συλλέγω από την καρτέλα **Internet Control Message Protocol**, εικόνα 2.9:

- Ο τύπος του πρωτοκόλλου ICMP του πακέτου είναι 0 (Echo (Ping) Reply).

Τέλος παρατηρώ ότι τα πεδία **Identifier**, **Sequence Number** και **Data** είναι κοινά και στα δύο πακέτα. Τα πεδία **Identifier** και **Sequence Number** χρησιμοποιούνται για την συσχέτιση του πακέτου Echo Request και του πακέτου Echo Reply. Ενώ το πεδίο **Data** του Echo Request πρέπει να επιστρέφεται και από αντίστοιχο Echo Reply για επιβεβαίωση όπως περιγράφεται στο RFC 792<sup>3</sup>.

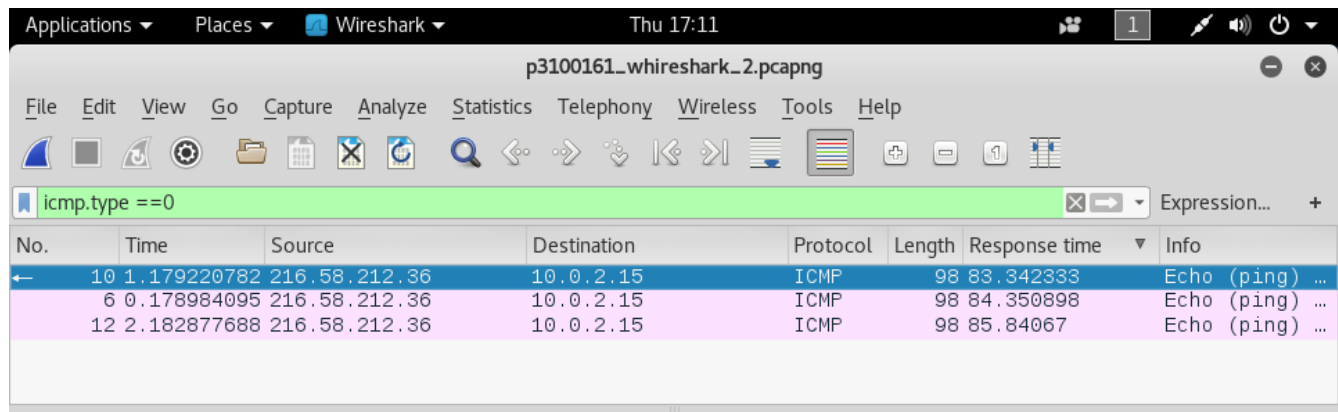
3 J. Postel, "RFC 792: INTERNET CONTROL MESSAGE PROTOCOL," September 1981, 14–15, <http://www.ietf.org/rfc/rfc792.txt>.

6. Υπολογίστε το χρόνο που περνάει ανάμεσα στην αποστολή κάθε Echo Request μέχρι την λήψη του αντίστοιχου Echo Reply. Συγκρίνετε τους χρόνους αυτούς με το minimum, average και maximum χρόνο που σας είχε δώσει το λειτουργικό στο command prompt παράθυρο όταν εκτελέσατε τα pings.

Αρχικά εφαρμόζω το φίλτρο **icmp.type == 0** ώστε το Wireshark να εμφανίσει μόνο τα ICMP πακέτα τύπου Echo Reply (0). Επιλέγω ένα από τα πακέτα και μεταβαίνω στην καρτέλα **Internet Control Message Protocol**.

Στην συνέχεια προσθέτω το πεδίο Response time στις στήλες της λίστας πατώντας στο πεδίο **Response time** (δεξί κλικ) → **Apply As Column**.

Τέλος, ταξινομώ την λίστα των πακέτων σε αύξουσα σειρά πατώντας πάνω στην νέα στήλη **Response time**. Με αυτόν τον τρόπο μπορώ εύκολα να συγκρίνω το ελάχιστο και μέγιστο χρόνο αποκρίσεις.



Εικόνα 2.11: Ταξινόμηση με βάση τους χρόνους απόκρισης

Καθώς υπάρχουν μόνο τρία πακέτα ICMP τύπου Echo Reply ο μέσος χρόνος απόκρισης μπορεί να υπολογιστεί εύκολα<sup>4</sup>.

Πίνακας 2.1: Χρόνοι Απόκρισης

Response Time	Ping (ms)	Wireshark (ms)
Min.	83.371	83.342
Avg.	84.532	84.511
Max.	85.862	85.841

Παρατηρώ ότι οι χρόνοι απόκρισης που αναφέρει η εφαρμογή Ping σχεδόν<sup>5</sup> ταυτίζονται με αυτούς που αναφέρει το Wireshark.

4 Αν είχαμε μεγάλο αριθμό πακέτων θα ήταν καλύτερα να χρησιμοποιήσουμε την tty έκδοση του εργαλείου, tshark, για να επεξεργαστούμε τις πληροφορίες των πακέτων.

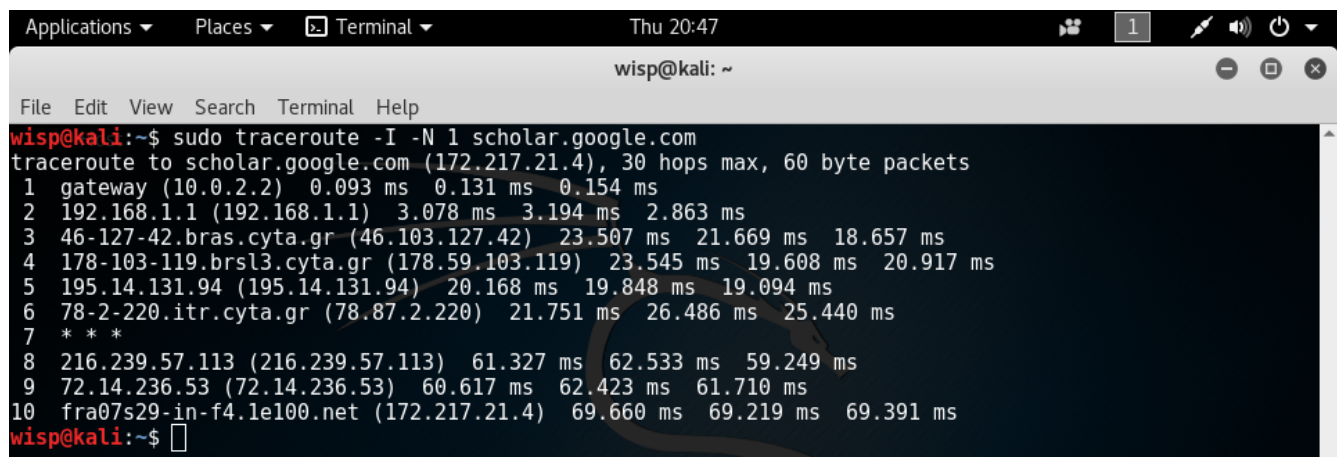
5 Η Ελάχιστη απόκριση πιθανόν να οφείλεται στην υλοποίηση της εφαρμογής ping.

### 3. Διαδικασία Traceroute: Ανάλυση με Wireshark

Η αντιστοιχεί διαδικασία **tracert**<sup>6</sup> (Windows) είναι διαθέσιμη στο λειτουργικό Debian με την ονομασία **traceroute**<sup>7</sup>. Για να προσομοιώσω την ακριβή λειτουργία της εντολής **tracert** scholar.google.com θα χρησιμοποιήσω την εντολή **sudo traceroute -I -N 1 scholar.google.com**.

- Η παράμετρος **-I** αναγκάζει την διαδικασία να χρησιμοποιήσει το πρωτόκολλο ICMP αντί για το UDP. Για να χρησιμοποιηθεί αυτή η παράμετρος θα πρέπει ο χρήστης να έχει διακαιώματα διαχειριστή.
- Η παράμετρος **-N 1** αναγκάζει την διαδικασία να περιμένει απάντηση πριν στείλει το επόμενο πακέτο, αφαιρώντας έτσι τον παραλληλισμό.

Εκτελώ το Wireshark και ξεκινάω την διαδικασία της ανίχνευσης. Στην συνέχεια εκτελώ την εντολή **sudo traceroute -I -N 1 scholar.google.com**. Η διαδικασία διαρκεί αρκετή ώρα λόγω του περιορισμού **-N 1**.



```
wisp@kali: ~  
File Edit View Search Terminal Help  
wisp@kali:~$ sudo traceroute -I -N 1 scholar.google.com  
traceroute to scholar.google.com (172.217.21.4), 30 hops max, 60 byte packets  
1 gateway (10.0.2.2) 0.093 ms 0.131 ms 0.154 ms  
2 192.168.1.1 (192.168.1.1) 3.078 ms 3.194 ms 2.863 ms  
3 46-127-42.bras.cyta.gr (46.103.127.42) 23.507 ms 21.669 ms 18.657 ms  
4 178-103-119.brs13.cyta.gr (178.59.103.119) 23.545 ms 19.608 ms 20.917 ms  
5 195.14.131.94 (195.14.131.94) 20.168 ms 19.848 ms 19.094 ms  
6 78-2-220.itr.cyta.gr (78.87.2.220) 21.751 ms 26.486 ms 25.440 ms  
7 * * *  
8 216.239.57.113 (216.239.57.113) 61.327 ms 62.533 ms 59.249 ms  
9 72.14.236.53 (72.14.236.53) 60.617 ms 62.423 ms 61.710 ms  
10 fra07s29-in-f4.1e100.net (172.217.21.4) 69.660 ms 69.219 ms 69.391 ms  
wisp@kali:~$
```

Εικόνα 3.1: Εκτέλεση της εντολής **sudo traceroute -I -N 1 scholar.google.com**

Μόλις η εντολή ολοκληρωθεί τερματίζω την διαδικασία της ανίχνευσης στο Wireshark.

6 “Tracert,” *Windows XP Professional Product Documentation*, accessed November 17, 2016, <https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tracert.msp?mfr=true>.

7 Michael Kerrisk, “traceroute(8) - Linux Manual Page,” *The Linux Man-Pages Project*, October 11, 2006, <http://man7.org/linux/man-pages/man8/traceroute.8.html>.

No.	Time	Source	Destination	Protocol	Length	Response time	Info
1	0.000000000	10.0.2.15	192.168.1.1	DNS	78		Standard
2	0.000060014	10.0.2.15	192.168.1.1	DNS	78		Standard
3	0.016669406	192.168.1.1	10.0.2.15	DNS	118		Standard
4	0.037967734	192.168.1.1	10.0.2.15	DNS	152		Standard
5	0.039128667	10.0.2.15	172.217.21.4	ICMP	74		Echo (pi
6	0.039205956	10.0.2.2	10.0.2.15	ICMP	70		Time-to-
7	0.039400266	10.0.2.15	192.168.1.1	DNS	81		Standard
8	0.062406539	192.168.1.1	10.0.2.15	DNS	158		Standard
9	0.063891255	10.0.2.15	172.217.21.4	ICMP	74		Echo (pi
10	0.064005451	10.0.2.2	10.0.2.15	ICMP	70		Time-to-
11	0.066452617	10.0.2.15	172.217.21.4	ICMP	74		Echo (pi
12	0.066585873	10.0.2.2	10.0.2.15	ICMP	70		Time-to-
13	0.066707368	10.0.2.15	172.217.21.4	ICMP	74		Echo (pi
14	0.069776508	192.168.1.1	10.0.2.15	ICMP	70		Time-to-
15	0.071614076	10.0.2.15	192.168.1.1	DNS	84		Standard

▶ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
 ▶ Ethernet II, Src: CadmusCo\_7c:5f:81 (08:00:27:7c:5f:81), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1  
 ▶ User Datagram Protocol, Src Port: 60532, Dst Port: 53  
 ▶ Domain Name System (query)

Εικόνα 3.2: Ολοκλήρωση διαδικασίας ανίχνευσης πακέτων

### 3.1. Traceroute: Απαντήσεις Ερωτήσεων

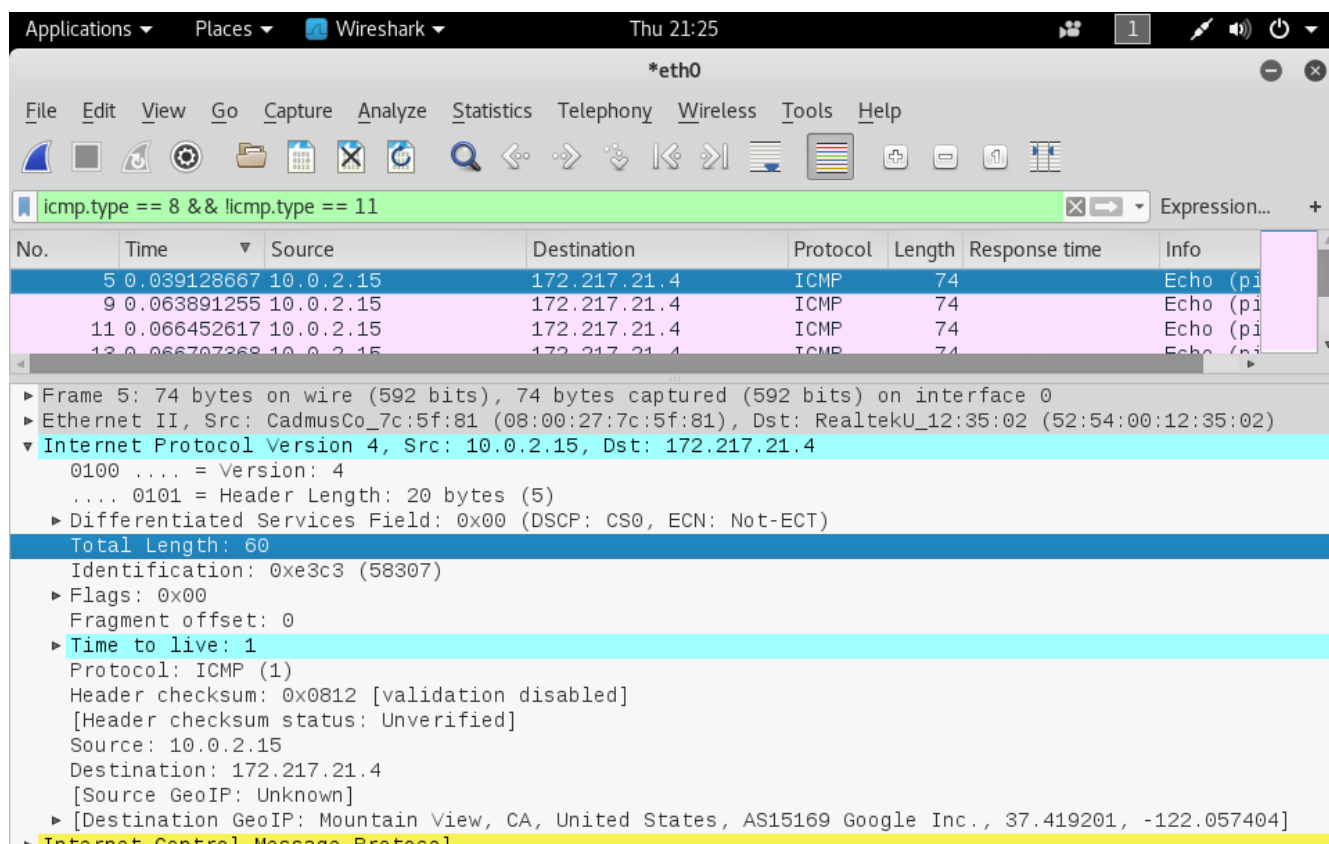
1. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.
  - a. Ποια είναι η IP διεύθυνση του destination;
  - b. Πόσο είναι το time-to-live του πακέτου;
  - c. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;

Σύμφωνα με το RFC 792<sup>8</sup> τα πακέτα ICMP τύπου Time Exceeded Message (11) πρέπει να περιέχουν την κεφαλίδα του πρωτοκόλλου IPv4 και 8 Bytes δεδομένων του πακέτου στο οποίο αναφέρονται. Στην συγκεκριμένη περίπτωση τα 8 Bytes περιλαμβάνουν την κεφαλίδα του πρωτοκόλλου ICMP.

Γι αυτόν τον λόγο θα χρησιμοποιήσω το φίλτρο **icmp.type == 8 && !icmp.type == 11** (όχι το φίλτρο **icmp.type == 8**) ώστε το Wireshark να περιορίσει την λίστα των πακέτων που ανίχνευσε σε πακέτα ICMP τύπου Echo Request (8).

Στην συνέχεια ταξινομώ τα πακέτα σε χρονολογική σειρά και επιλέγω το πρώτο από τη λίστα.

8 J. Postel, "RFC 792," 6–7.



Εικόνα 3.3: Καρτέλα **Internet Protocol Version 4**, σε πακέτο **Echo Request**

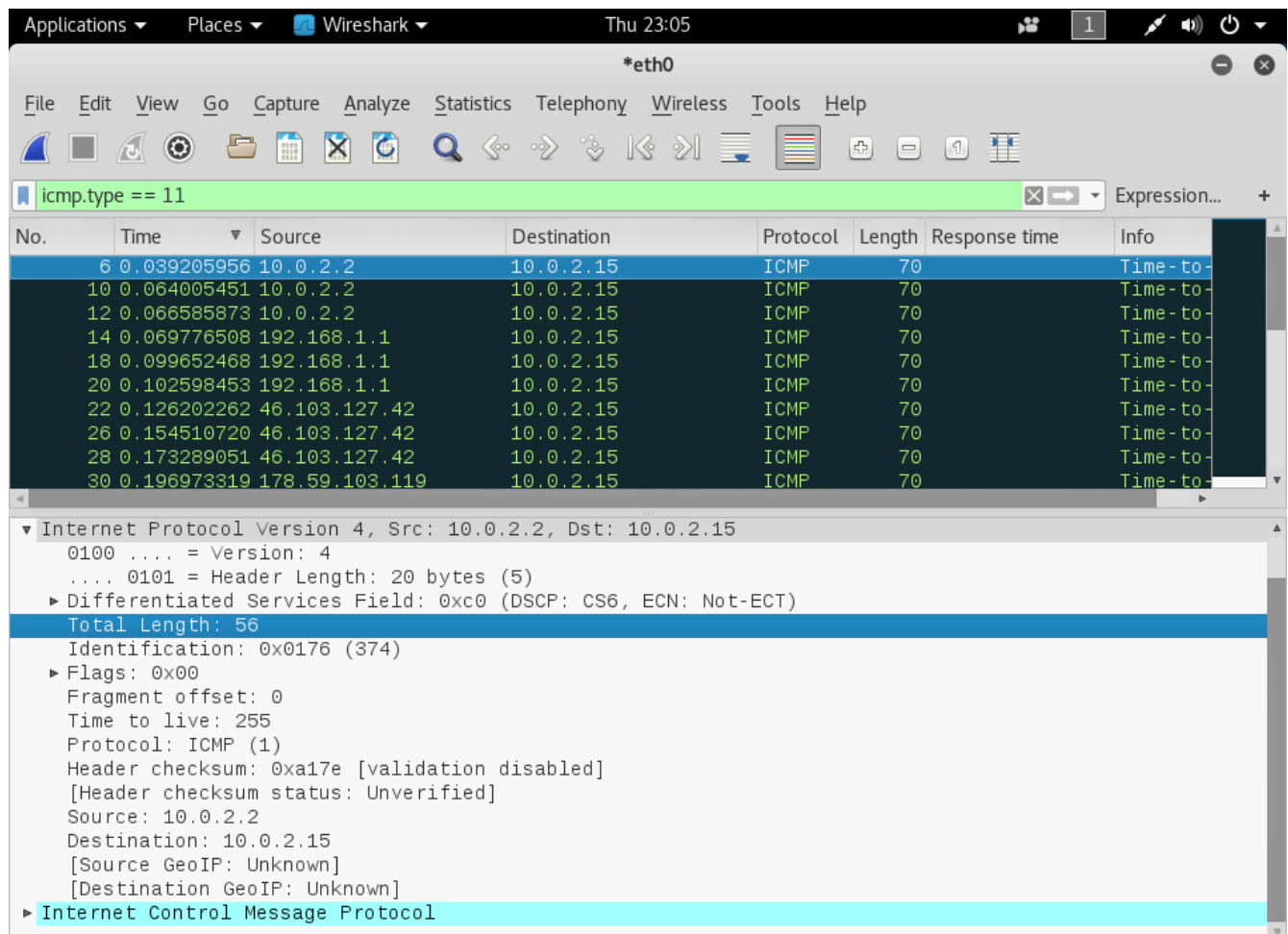
Μπορώ να συγκεντρώσω τις σχετικές πληροφορίες από την καρτέλα **Internet Protocol Version 4**:

- Η διεύθυνση του παραλήπτη (Destination) είναι 172.217.21.4<sup>9</sup>.
  - Το TTL του πακέτου είναι 1.
  - Το μέγεθος των δεδομένων του πακέτου IP είναι  $60 - 20 = 40$  Bytes.
2. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded.
- α. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του source;

Εφαρμόζω το φίλτρο **icmp.type == 11** ώστε η λίστα των πακέτων να περιοριστεί σε πακέτα ICMP τύπου Time Exceeded Message (11).

Στην συνέχεια ταξινομώ τα πακέτα χρονολογικά και επιλέγω το πρώτο από τη λίστα.

<sup>9</sup> Προφανώς ο host, scholar.google.com είναι προσβάσιμος από περισσότερες από μία διευθύνσεις IP.



Εικόνα 3.4: Καρτέλα **Internet Protocol Version 4**, σε πακέτο Time Exceeded Message

Μπορώ να συγκεντρώσω τις σχετικές πληροφορίες από την καρτέλα **Internet Protocol Version 4**:

- Η διεύθυνση IP του παραλήπτη (Destination) είναι η 10.0.2.15.
  - Η διεύθυνση IP του αποστολέα (Source) είναι η 10.0.2.2.
3. Ελέγχοντας το time-to-live των διαδοχικών πακέτων ICMP Echo Request, τί παρατηρείται; Για ποιο λόγο γίνεται αυτό;

Εφαρμόζω το φίλτρο `icmp.type == 8 && !icmp.type == 11` όπως στο ερώτημα 1 και επιλέγω ένα πακέτο. Μεταβαίνω στην καρτέλα **Internet Protocol Version 4** και προσθέτω το πεδίο Time to live στις στήλες της λίστας πατώντας στο πεδίο Time to live (δεξί κλικ) → **Apply As Column**.

Τέλος ταξινομώ τα πακέτα σε χρονολογική σειρά.



No.	Time	Source	Destination	Response time	Time to live	Protocol	Len
5	0.039128667	10.0.2.15	172.217.21.4		1	ICMP	
9	0.063891255	10.0.2.15	172.217.21.4		1	ICMP	
11	0.066452617	10.0.2.15	172.217.21.4		1	ICMP	
13	0.066707368	10.0.2.15	172.217.21.4		2	ICMP	
17	0.096476438	10.0.2.15	172.217.21.4		2	ICMP	
19	0.099744911	10.0.2.15	172.217.21.4		2	ICMP	
21	0.102706519	10.0.2.15	172.217.21.4		3	ICMP	
25	0.132860011	10.0.2.15	172.217.21.4		3	ICMP	
27	0.154649589	10.0.2.15	172.217.21.4		3	ICMP	
29	0.173445187	10.0.2.15	172.217.21.4		4	ICMP	
33	0.201936029	10.0.2.15	172.217.21.4		4	ICMP	
35	0.221731064	10.0.2.15	172.217.21.4		4	ICMP	
37	0.242817609	10.0.2.15	172.217.21.4		5	ICMP	
41	0.285654818	10.0.2.15	172.217.21.4		5	ICMP	
43	0.305618102	10.0.2.15	172.217.21.4		5	ICMP	
45	0.321810108	10.0.2.15	172.217.21.4		6	ICMP	

Εικόνα 3.5: TTL των πακέτων Echo Request

Παρατηρώ ότι το TTL αυξάνεται κατά 1 ανά τρία πακέτα ξεκινώντας από TTL ίσο με 1.

Η διαδικασία traceroute προσπαθεί να διαπιστώσει όλους του κόμβους του δικτύου μέχρι τη διεύθυνση του host που έχουμε ορίσει. Αυτό το επιτυγχάνει χρησιμοποιώντας τα ICMP πακέτα τύπου Time Exceeded που στέλνονται στον αποστολέα ενός πακέτου όταν ο χρόνος ζωής του πακέτου εξαντληθεί. Γι αυτόν τον λόγο αυξάνει σταδιακά το TTL των εξερχόμενων πακέτων ώστε αυτό να εξαντλείτε σε διαφορετικό κόμβο κάθε φορά. Για πιο έγκυρα αποτελέσματα η διαδικασία στέλνει τρία πακέτα πριν αυξήσει το TTL.

Αν οι πίνακες δρομολόγησης των ενδιάμεσων κόμβων δεν αλλάξουν την διεύθυνση Next Hop για τον συγκεκριμένο host κατά την εκτέλεση της εντολής τότε η διαδικασία επιστρέφει το μονοπάτι των κόμβων μέχρι τον ορισμένο host.

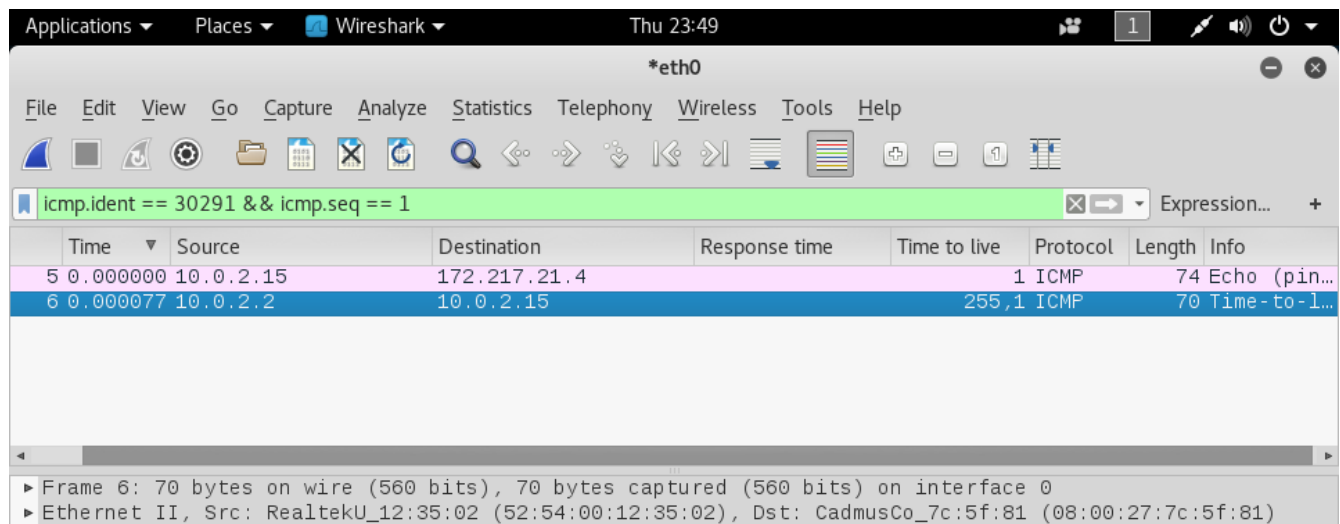
4. Υπολογίστε το χρόνο ανάμεσα στο 1<sup>ο</sup> ICMP Echo Request και το αντίστοιχο (1<sup>ο</sup>) ICMP Time Exceeded και συγκρίνετε τον με τους χρόνους που δίνει αντίστοιχα το πρώτο βήμα της εκτέλεσης της εντολής tracert στο command prompt παράθυρο.

Επιλέγω το πρώτο πακέτο ICMP τύπου Echo Request και εφαρμόζω το φίλτρο **icmp.ident == 30291 && icmp.seq == 1**, σύμφωνα με τα πεδία **Identifier (BE)** και **Sequence number (BE)** της καρτέλας **Internet Control Message Protocol** και ταξινομώ την λίστα των πακέτων σε χρονολογική σειρά.

Στην συνέχεια ρυθμίζω κατάλληλα την στήλη Time πατώντας τις επιλογές:

- **View → Time Display Format → Seconds Since Previous Displayed Package**
- **View → Time Display Format → Microseconds**





Εικόνα 3.6: Χρονικό διάστημα μέχρι το πρώτο *Time Exceeded Message*

Το διάστημα μεταξύ της αποστολής του πρώτου ICMP πακέτου, τύπου Echo Request μέχρι την παραλαβή του αντίστοιχου ICMP πακέτου, τύπου Time Exceeded Message, σύμφωνα με το Wireshark είναι 0.077 ms. Περίπου ίσο<sup>10</sup> με το 0.093 ms που επέστρεψε η διαδικασία traceroute.

5. Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής `tracert` στο command prompt παράθυρο;

Εφαρμόζω το φίλτρο `icmp.type == 0 || icmp.type == 11` ώστε η λίστα των πακέτων να περιοριστεί σε πακέτα ICMP τύπου Time Exceeded Message (11) και Echo Reply (0). Στην συνέχεια μεταβαίνω στην επιλογή **Statistics** → **Endpoints** από το μενού.

<sup>10</sup> Η Ελάχιστη απόκλιση πιθανόν να οφείλεται στην υλοποίηση της εφαρμογής traceroute.

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	City
10.0.2.2	3	210	3	210	0	0	—
10.0.2.15	27	1902	0	0	27	1902	—
46.103.127.42	3	210	3	210	0	0	—
72.14.236.53	3	210	3	210	0	0	Mountain View, CA
78.87.2.220	3	210	3	210	0	0	—
172.217.21.4	3	222	3	222	0	0	Mountain View, CA
178.59.103.119	3	210	3	210	0	0	—
192.168.1.1	3	210	3	210	0	0	—
195.14.131.94	3	210	3	210	0	0	Nicosia, 04
216.239.57.113	3	210	3	210	0	0	—

Εικόνα 3.7: Διευθύνσεις IP που αποτίστηκαν στην ανίχνευση

Στο νέο παράθυρο εμφανίζονται όλοι οι κόμβοι στους οποίους αναφέρονται τα πακέτα της ανίχνευσης. Περιορίζω την λίστα σύμφωνα με το ενεργό φίλτρο πατώντας την επιλογή **Limit to display filter**. Οι IP διεύθυνσης αποστολέα των συγκεκριμένων πακέτων είναι:

Πίνακας 3.1: Διευθύνσεις Κόμβων του Μονοπατιού<sup>11</sup>

10.0.2.2	46.103.127.42	72.14.236.53
78.87.2.220	172.217.21.4	178.59.103.119
192.168.1.1	195.14.131.94	216.239.57.113

Συγκρίνοντας με το αποτέλεσμα της διαδικασίας traceroute, εικόνα 3.1, παρατηρώ ότι διευθύνσεις IP ταυτίζονται.

11 Μπορώ να διακρίνω της διευθύνσεις αποστολέα από την στήλη **Packets B → A**. Όλες οι σχετικές διευθύνσεις έχουν τιμή 0. Αν ήθελα να γνωρίζω και την σειρά των διευθύνσεων θα έπρεπε να παρατηρήσω την λίστα των πακέτων.

## 4. Βιβλιογραφία

- J. Postel. “RFC 792: INTERNET CONTROL MESSAGE PROTOCOL,” September 1981.  
<http://www.ietf.org/rfc/rfc792.txt>.
- Michael Kerrisk. “traceroute(8) - Linux Manual Page.” *The Linux Man-Pages Project*, October 11, 2006. <http://man7.org/linux/man-pages/man8/traceroute.8.html>.
- “Tracert.” *Windows XP Professional Product Documentation*. Accessed November 17, 2016.  
<https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tracert.msp?mfr=true>.