

**ΟΙΚΟΝΟΜΙΚΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΑΘΗΝΩΝ**



**ATHENS UNIVERSITY  
OF ECONOMICS  
AND BUSINESS**

# Δίκτυα Επικοινωνιών

## Εργασία 2<sup>η</sup> – Wireshark

14 Ιανουαρίου 2017

## Περιεχόμενα

1.Γενικές Πληροφορίες.....	1
2.Διερεύνηση DNS και HTTP με Wireshark.....	1
2.1.Απαντήσεις Ερωτήσεων.....	2
Βιβλιογραφία.....	13

## Εικόνες

Εικόνα 2.1: Εκτέλεση ipconfig /flushdns.....	1
Εικόνα 2.2: Αποτελέσματα ανίχνευσης.....	2
Εικόνα 2.3: Ιεραρχία πρωτοκόλλων.....	3
Εικόνα 2.4: Ιεραρχία πρωτοκόλλων των απεσταλμένων πακέτων.....	4
Εικόνα 2.5: Endpoints επιπέδου Σύνδεσης Δεδομένων.....	5
Εικόνα 2.6: Endpoints επιπέδου Δικτύου.....	6
Εικόνα 2.7: Εφαρμογή φίλτρου dns.qry.name == “www.cs.aueb.gr”.....	7
Εικόνα 2.8: Πρωτόκολλο DNS.....	8
Εικόνα 2.9: TCP, Χειραψία τριών βημάτων.....	9
Εικόνα 2.10: TCP θύρες που χρησιμοποιήθηκαν από το πρωτόκολλο HTTP.....	10
Εικόνα 2.11: HTTP GET Requests.....	11
Εικόνα 2.12: HTTP GET Reply.....	12

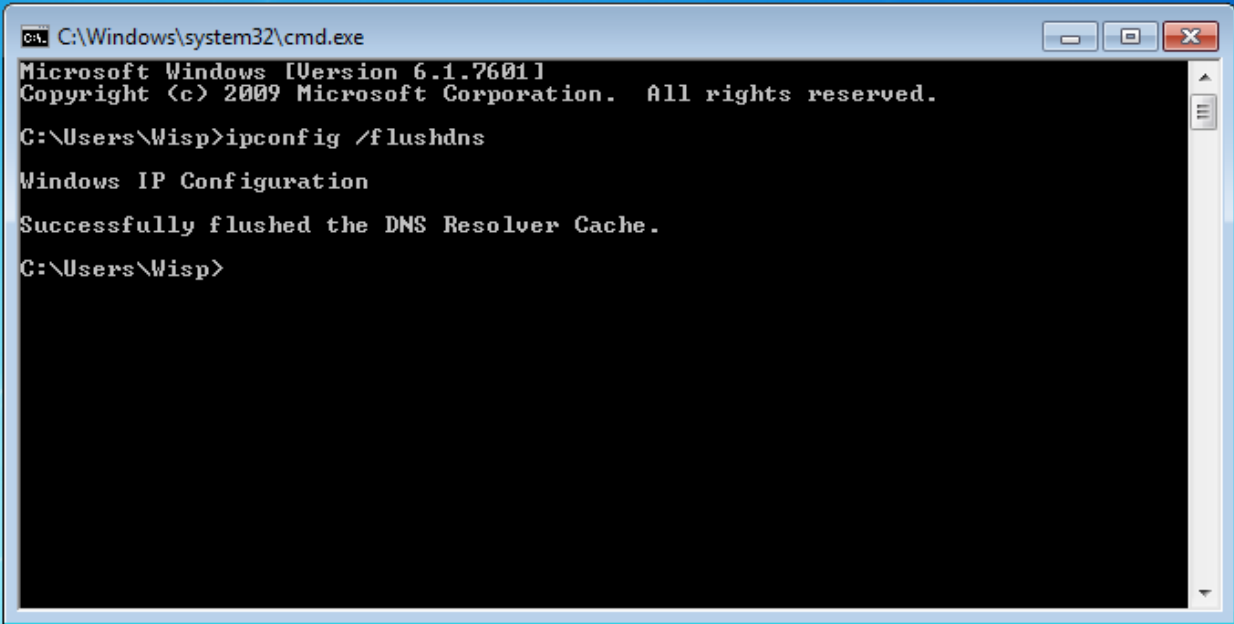
# 1. Γενικές Πληροφορίες

Το λειτουργικό σύστημα που θα χρησιμοποιήσω για την παρουσίαση του λογισμικού Wireshark είναι το Windows 7 Ultimate (Service Pack 1) x64. Το ίδιο το λειτουργικό είναι εγκατεστημένο σε ένα Virtual Machine και είναι συνδεδεμένο σε ένα δίκτυο NAT μέσω της διεπαφής Local Area Connection.

Κατά την διάρκεια των αναλύσεων η διεύθυνση IPv4 του μηχανήματος για την διεπαφή Local Area Connection ήταν η 10.0.2.15.

## 2. Διερεύνηση DNS και HTTP με Wireshark

Αρχικά εκτελώ την εντολή `ipconfig /flushdns`. Η εντολή αυτή θα καθαρίσει την τοπική cache και νέα DNS ερωτήματα θα πρέπει οπωσδήποτε να αποσταλούν στον τοπικό nameserver προκειμένου να απαντηθούν.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Wisp>ipconfig /flushdns

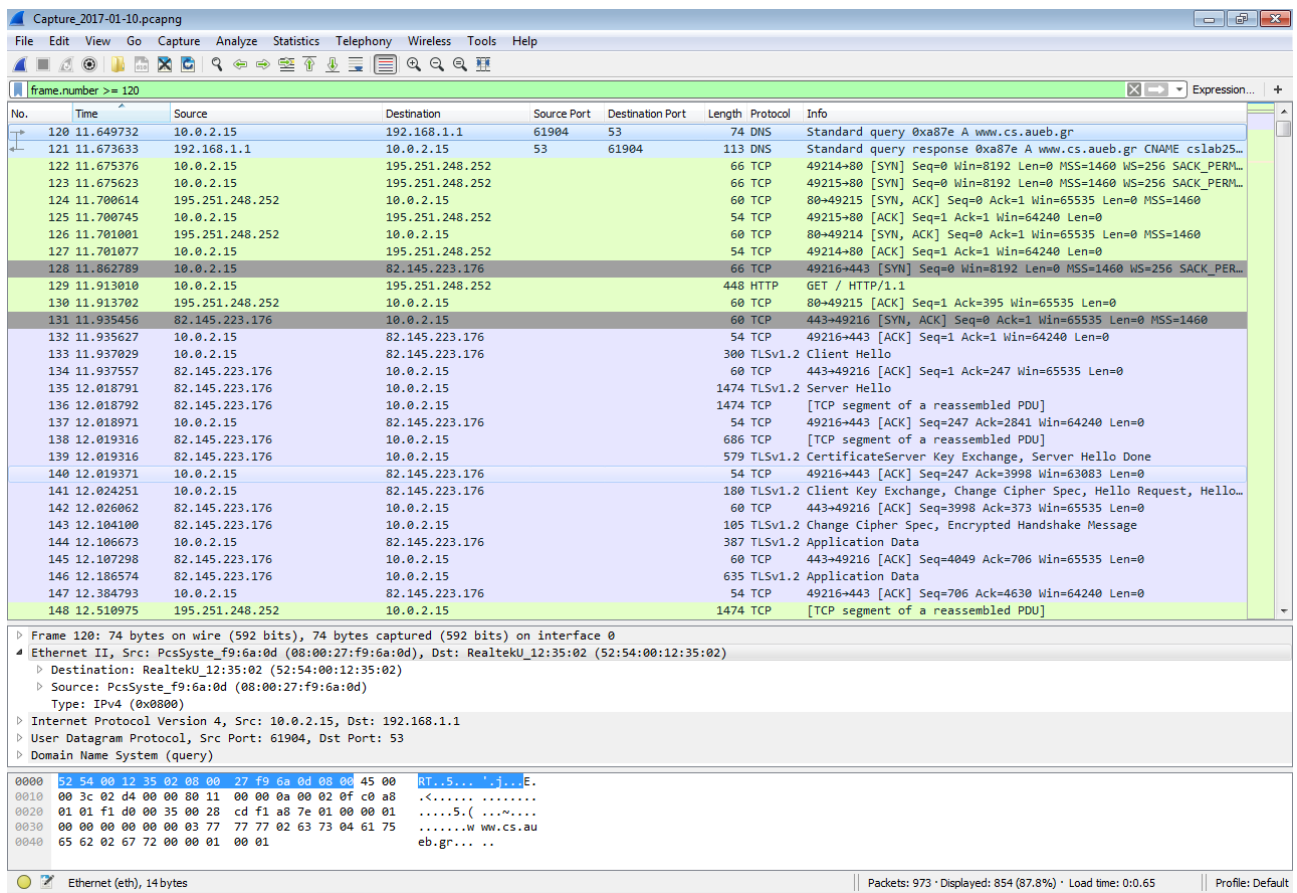
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Wisp>
```

Εικόνα 2.1: Εκτέλεση `ipconfig /flushdns`

Στην συνέχεια εκτελώ το Wireshark και επιλέγω την διεπαφή Local Area Connection.



Εικόνα 2.2: Αποτελέσματα ανίχνευσης

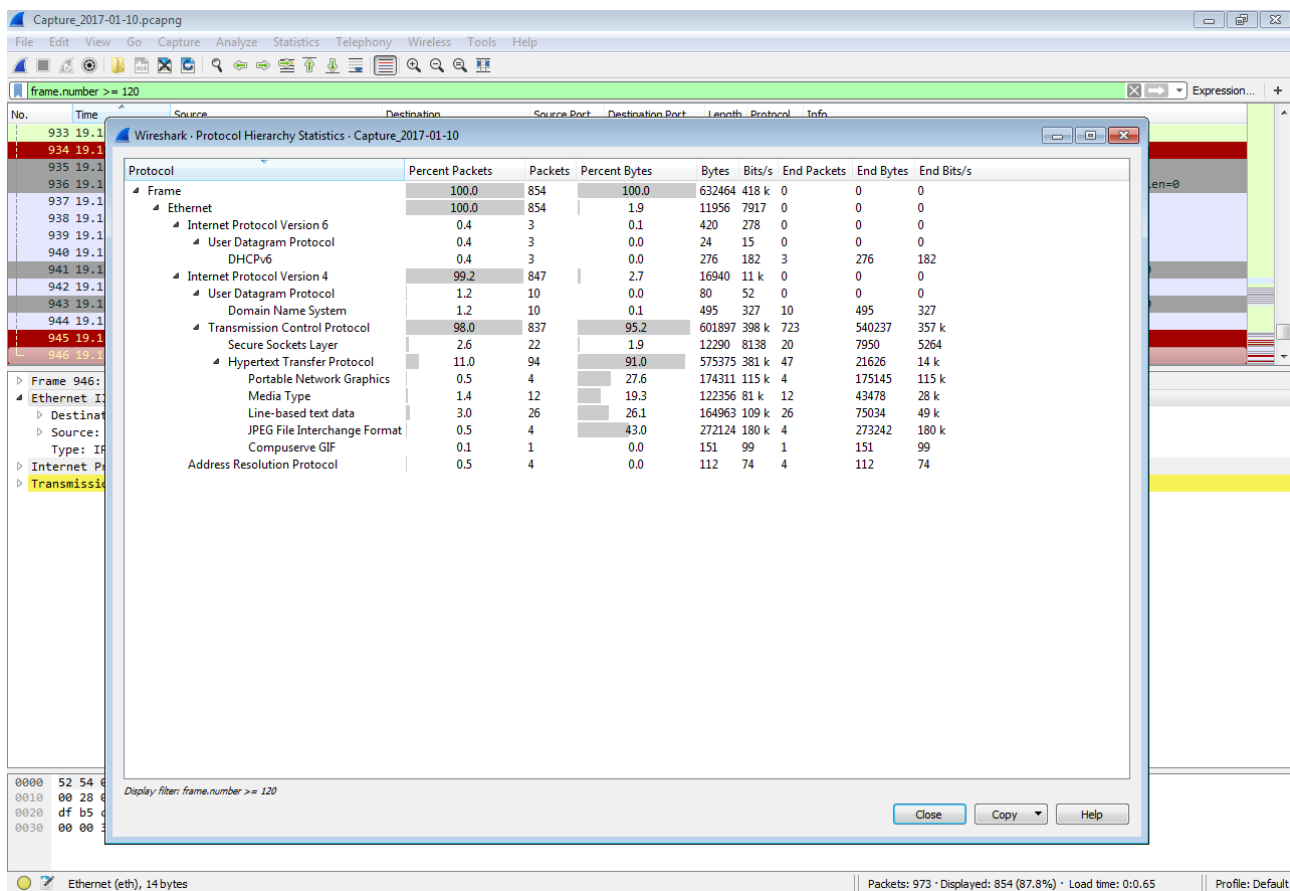
Πραγματοποιώ ένα HTTP Request στην σελίδα <http://www.aueb.gr> και τερματίζω την ανίχνευση.

Προκειμένου να παραβλέψω πακέτα που λήφθηκαν πριν πραγματοποιηθεί το HTTP Request εφαρμόζω το φίλτρο **frame.number >= 120** κατά την διάρκεια την ανάλυσης.

## 2.1. Απαντήσεις Ερωτήσεων

1. Προσδιορίστε ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στη χρονική διάρκεια της ανίχνευσης. Διαχωρίστε τα συγκεκριμένα πρωτόκολλα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

Μεταβαίνω στην επιλογή **Statistics** → **Protocol Hierarchy** από το μενού. Στο νέο παράθυρο εμφανίζονται τα πρωτόκολλα που χρησιμοποιήθηκαν κατά την διάρκεια της ανίχνευσης.



Εικόνα 2.3: Ιεραρχία πρωτοκόλλων

- Στο **Φυσικό Επίπεδο** και στο **Επίπεδο Σύνδεσης Δεδομένων** χρησιμοποιήθηκε το πρωτόκολλο Ethernet II.
- Στο **Επίπεδο Δικτύου** χρησιμοποιήθηκε κυρίως το πρωτόκολλο IPv4, ARP, αλλά και το IPv6<sup>1</sup>.
- Στο **Επίπεδο Μεταφοράς** χρησιμοποιήθηκαν τα πρωτόκολλα UDP και TCP.
- Στο **Επίπεδο Εφαρμογής** χρησιμοποιήθηκαν τα πρωτόκολλα DNS, HTTP και SSL, αλλά και κάποια ειδικότερα πρωτόκολλα όπως φαίνεται στην εικόνα 2.3.

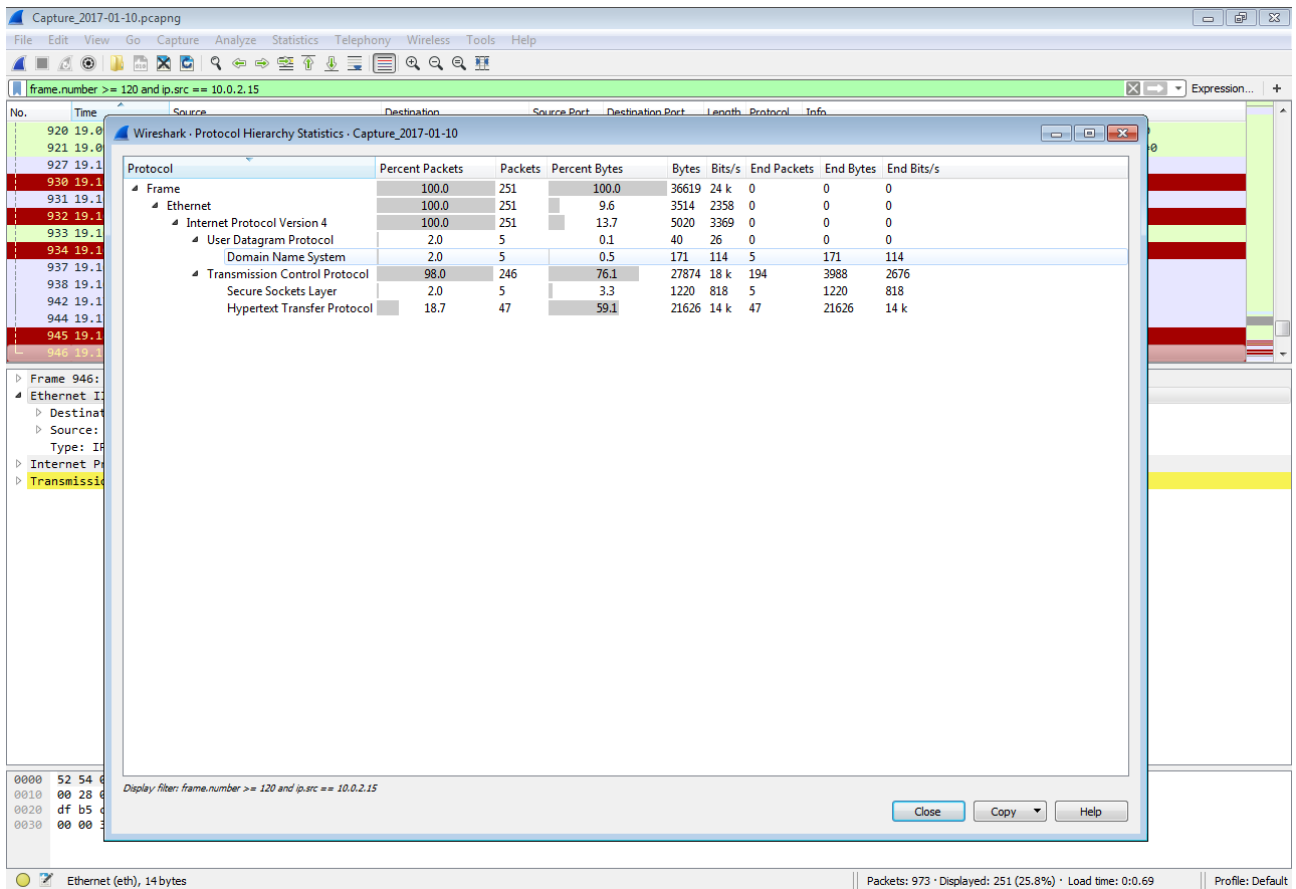
2. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

Όπως φαίνεται και από την εικόνα 2.3, το πρωτόκολλο DNS χρησιμοποιεί το πρωτόκολλο UDP, ενώ τα υπόλοιπα πρωτόκολλα, συμπεριλαμβανομένου των HTTP και SSL, χρησιμοποιούν το πρωτόκολλο TCP.

1. Το πρωτόκολλο IPv6 χρησιμοποιήθηκε μαζί με το πρωτόκολλο DHCPv6 για ρυθμίσεις του τοπικού δικτύου και δεν επηρεάζει τα αποτελέσματα της ανάλυσης.

### 3. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Στην στήλη Packets του πίνακα ιεραρχία πρωτοκόλλων εμφανίζονται τα πακέτα που στάλθηκαν ανά πρωτόκολλο. Για να προσμετρηθούν μόνο τα πακέτα με αποστολέα το τοπικό μηχάνημα εφαρμόζω το φίλτρο **ip.src == 10.0.2.15** και ανανεώνω τον πίνακα.

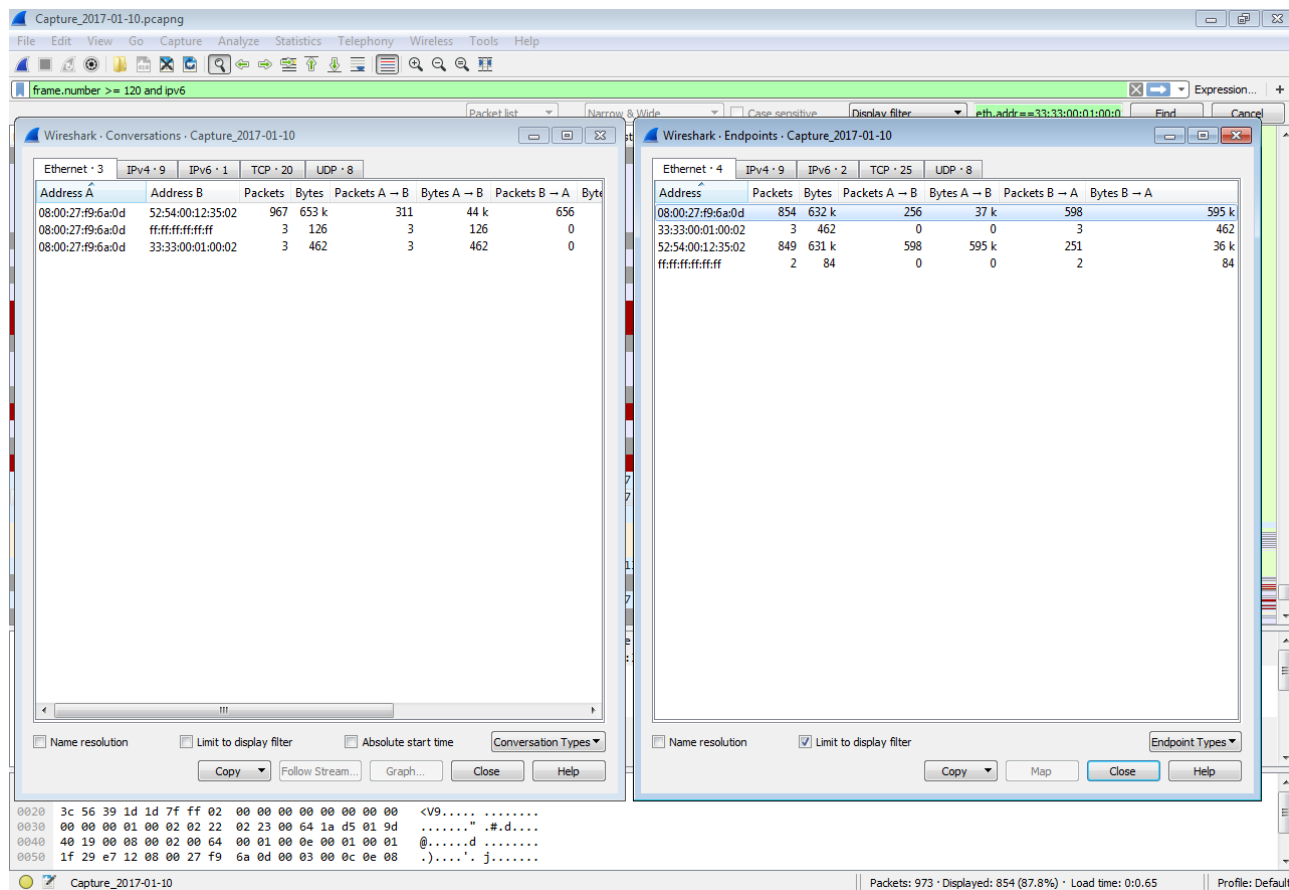


Εικόνα 2.4: Ιεραρχία πρωτοκόλλων των απεσταλμένων πακέτων

Από το τοπικό μηχάνημα στάλθηκαν 5 UDP και 246 TCP πακέτα.

4. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε ποιες συσκευές αντιστοιχούν;

Μεταβαίνω στις επιλογές **Statistics** → **Endpoints** και **Statistics** → **Conversations** από το μενού.



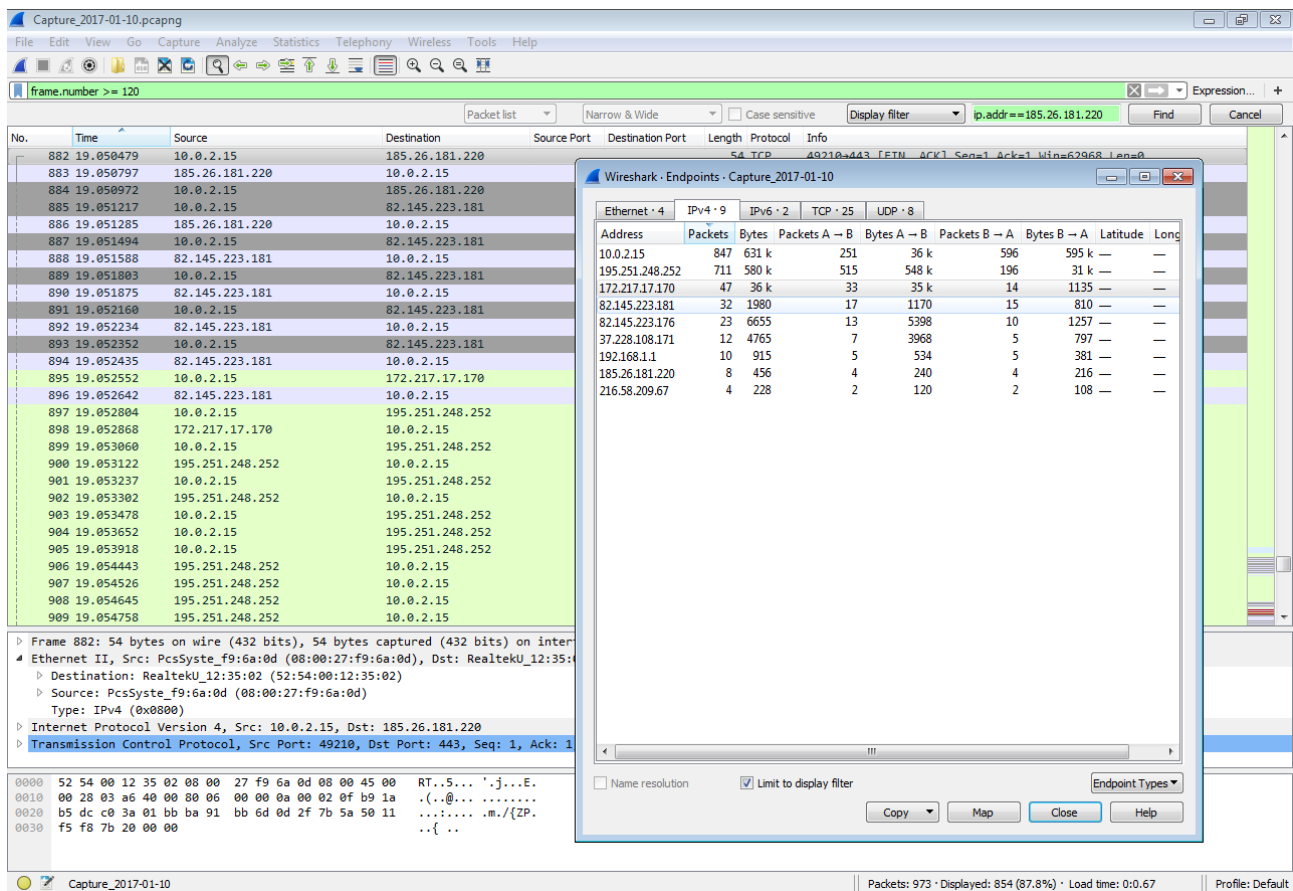
Εικόνα 2.5: Endpoints επιπέδου Σύνδεσης Λεδομένων

Στον πίνακα Endpoints, εικόνα 2.5 (δεξιά), εμφανίζονται οι MAC διευθύνσεις των διαφορετικών συσκευών:

- Η διεύθυνση 08-02-27-f9-6a-0d αντιστοιχεί στο τοπικό μηχάνημα όπως φαίνεται από τον πίνακα Conversations, εικόνα 2.5 (αριστερά).
- Η διεύθυνση 33-33-00-01-00-02 χρησιμοποιείται για IPv6 Multicast<sup>2</sup>.
- Η διεύθυνση FF-FF-FF-FF-FF-FF χρησιμοποιείται για Broadcast.
- Η διεύθυνση 52-54-00-12-35-02 αντιστοιχεί στο Default Gateway του τοπικού δικτύου όπως φαίνεται και από τον πίνακα Conversations.

2. M. Crawford, “RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks,” December 1998, 5, <https://tools.ietf.org/html/rfc2464>.

5. Πόσα και ποια είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, σε τι διαφέρουν;



Εικόνα 2.6: Endpoints επιπέδου Δικτύου

Οι διευθύνσεις IPv4 που εντοπίστηκαν κατά την διάρκεια της ανίχνευσης ήταν 9, εικόνα 2.6 (δεξιά), αρκετά περισσότερες από τις MAC διευθύνσεις καθώς το επίπεδο Δικτύου επικοινωνεί με κόμβος του Διαδικτύου ενώ το επίπεδο Σύνδεσης Δεδομένων με κόμβος στους οποίους το τοπικό μηχάνημα συνδέεται άμεσα.

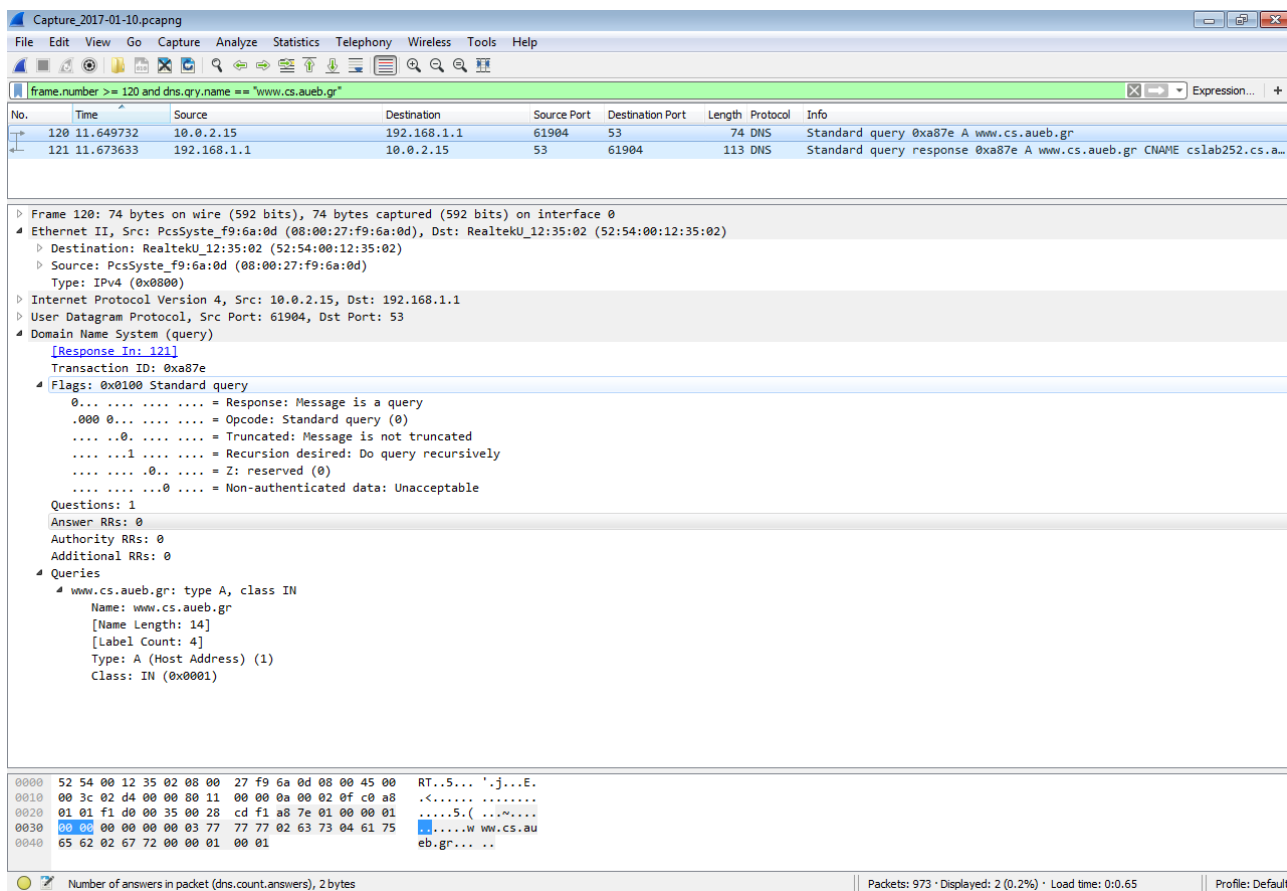
Η μόνη αντιστοιχία μεταξύ διευθύνσεων MAC και IPv4 είναι για το τοπικό μηχάνημα, 08-02-27-f9-6a-0d → 10.0.2.15<sup>3</sup>.

6. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.

Εφαρμόζω το φίλτρο **dns.qry.name == "www.cs.aueb.gr"**. Τα μόνα πακέτα που παραμένουν στην λίστα είναι τα πακέτα από και προς τον DNS Server σχετικά με το Domain Name: **www.cs.aueb.gr**.

3. Αν τοπικό μηχάνημα δεν ένα Virtual Machine πιθανόν να υπήρχε και αντιστοιχία μεταξύ των διευθύνσεων του Default Gateway και της διεύθυνσης 192.168.1.1, όμως στην προκειμένη περίπτωση το πραγματικό Router βρίσκεται σε άλλο υποδίκτυο.





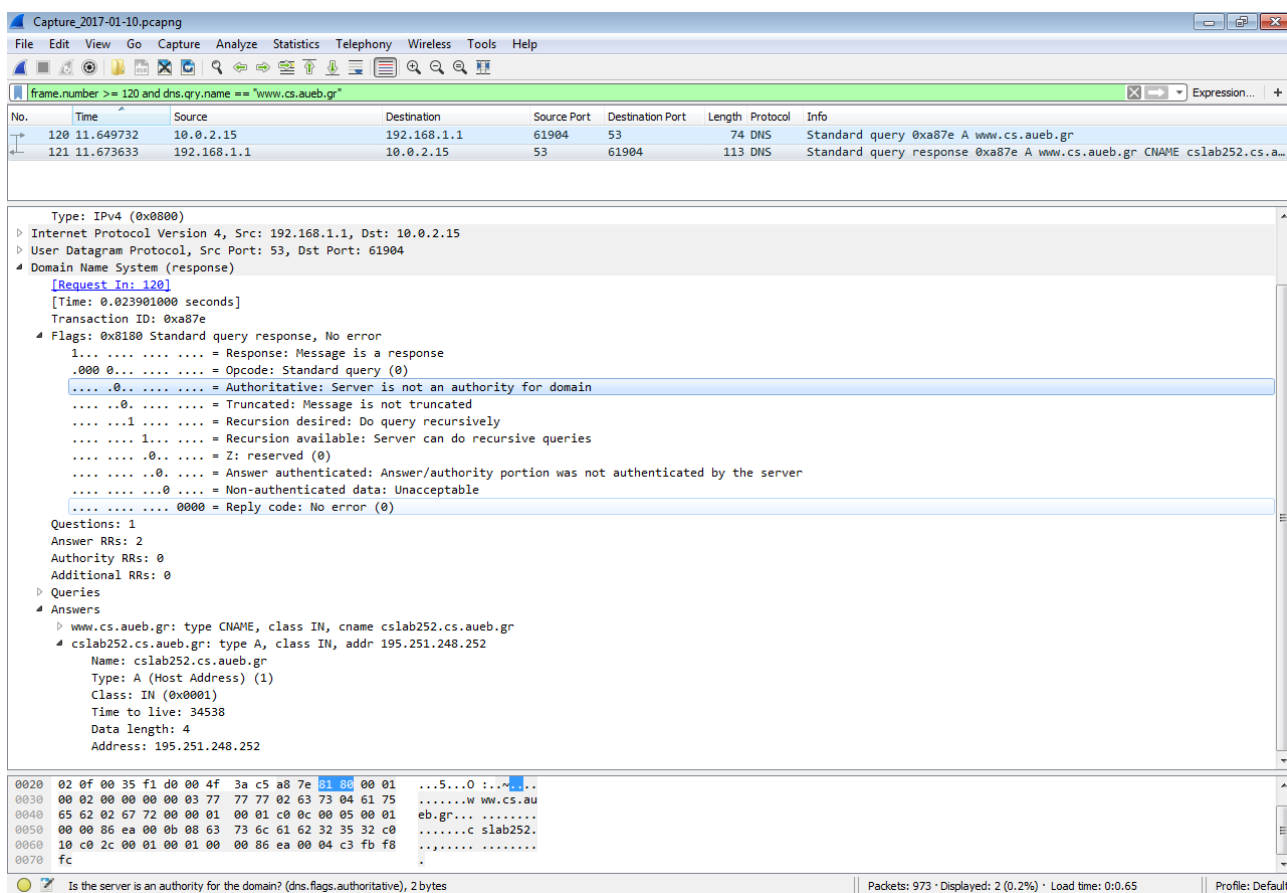
Εικόνα 2.7: Εφαρμογή φίλτρου `dns.qry.name == "www.cs.aueb.gr"`

Κατά την αποστολή το ερωτήματος η UDP θύρα προέλευσης είναι τυχαία, 61904 στην συγκεκριμένη περίπτωση, ενώ η UDP θύρα παραλήπτη είναι η θύρα 53, που χρησιμοποιείται από την υπηρεσία Domain Name Service.

Η απάντηση περιέχει τις θύρες αποστολέα και παραλήπτη αντεστραμμένες.

7. Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

Αρχικά μπορούμε να αναγνωρίσουμε τον τύπο του πακέτου από την διεύθυνση του παραλήπτη και του αποστολέα καθώς το συγκεκριμένο τοπικό μηχάνημα δεν λειτουργεί ως DNS server, αλλά γενικότερα μπορούμε να αναγνωρίσουμε αν το πακέτο αντιστοιχεί σε ερώτημα ή απάντηση βάση εκτός των άλλων του πεδίου **Answer RRs** της επικεφαλίδας του DNS πρωτοκόλλου, εικόνα 2.8. Επιπλέον το πεδίο **Transaction ID** χρησιμοποιείται για την αντιστοίχιση του ερωτήματος και της απάντησης.



Εικόνα 2.8: Πρωτόκολλο DNS

8. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει είναι authoritative για το συγκεκριμένο domain; Ο name server που μας έχει απαντήσει είναι authoritative για το συγκεκριμένο domain;

Το πεδίο **Flags** και συγκεκριμένα το 6 ποιο σημαντικό bit αυτού του πεδίου χρησιμοποιείται για να προσδιορίσει αν ο Name Server που έστειλε την απάντηση είναι authoritative. Ο συγκεκριμένος server, δεν είναι authoritative, εικόνα 2.8, όπως ήταν αναμενόμενο καθώς η IPv4 του αποστολέα αντιστοιχεί σε διεύθυνση του τοπικού μου δικτύου.

9. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.cs.aueb.gr; Ποια η IP διεύθυνση του δικού σας υπολογιστή;

Στο πεδίο **Answers** που ανέλυσε ο analyzer του Wireshark φαίνεται πως η διεύθυνση www.cs.aueb.gr είναι ψευδώνυμο της διεύθυνσης cs1ab252.cs.aueb.gr και συγκεκριμένη διεύθυνση αντιστοιχεί στην IPv4: 195.251.248.252, εικόνα 2.8.

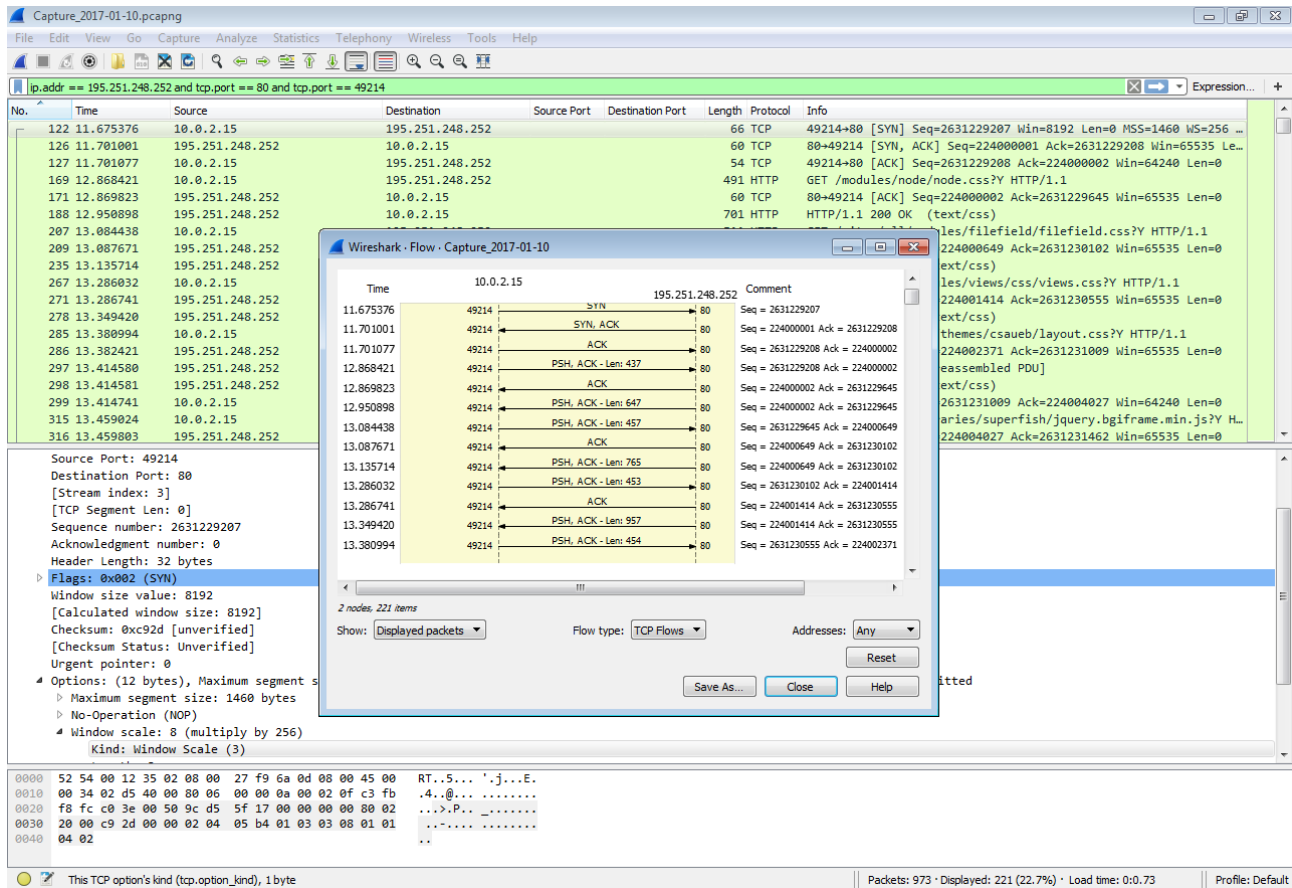
10. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.cs.aueb.gr υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

Για να πραγματοποιήσω την ανάλυση απενεργοποιώ αρχικά την επιλογή **Relative sequence numbers** από τις ρυθμίσεις του πρωτοκόλλου TCP επιλέγοντας **Edit** → **Preferences** από το μενού και μεταβαίνοντας στην καρτέλα **Protocols** → **TCP**.

Στην συνέχεια εφαρμόζω το φίλτρο **ip.addr == 195.251.248.252 and tcp.port == 80 and tcp.port**

== 49214<sup>4</sup> προκειμένου να εμφανιστούν στην λίστα μόνο τα πακέτα που σχετίζονται με μία συγκεκριμένη σύνδεση στον server. Τα τρία πρώτα πακέτα στην λίστα πραγματοποιούν τη χειραγία τριών βημάτων για την εγκαθίδρυση της σύνδεσης.

Τέλος επιλέγω **Statistics** → **Flow Graph** από το μενού, και στο νέο παράθυρο επιλέγω **Displayed Packets** και **TCP Flows** στα πεδία Show και Flow Type αντίστοιχα. Το νέο παράθυρο δίνει μία πιο συνοπτική εικόνα της χειραγίας.



Εικόνα 2.9: TCP, Χειραγία τριών βημάτων

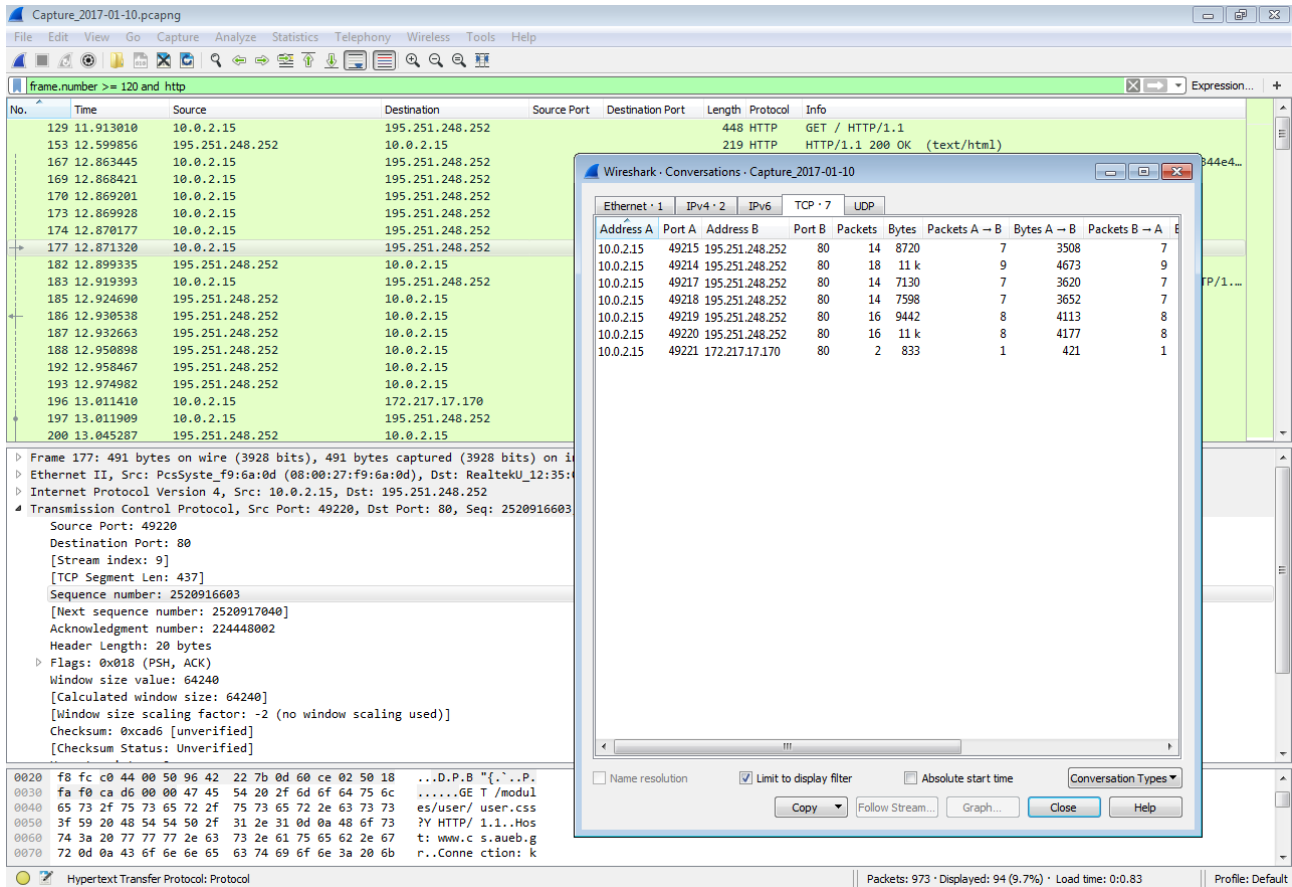
Η χειραγία τριών βημάτων είναι απαραίτητη για τον συγχρονισμό των αριθμών σειράς των πακέτων που στέλνονται χρησιμοποιώντας το πρωτόκολλο TCP και άρα για την εξασφάλιση της αξιοπιστίας του πρωτοκόλλου.

1. Το πρώτο βήμα είναι η αποστολή ενός πακέτου από το τοπικό μηχάνημα στον server με ενεργοποιημένο μόνο το flag: **SYN**. Ο αριθμός σειράς, **Sequence number**, του πακέτου αυτού είναι 2631229207 ο οποίος επιλέχτηκε από το τοπικό μηχάνημα.
  2. Το δεύτερο βήμα είναι αποστολή ενός πακέτου από τον server στο τοπικό μηχάνημα με ενεργοποιημένα μόνο τα flag: **SYN** και **ACK**. Ο αριθμός σειράς του πακέτου αυτού επιλέγεται από τον server, 224000001. Στο ίδιο πακέτο ο αριθμός επιβεβαίωσης, **Acknowledgment number**, είναι 2631229208. Ο αριθμός αυτό δηλώνει τον επόμενο αριθμό σειράς που περιμένει να λάβει ο server από το τοπικό μηχάνημα.
  3. Το τελευταίο βήμα είναι το τοπικό μηχάνημα να στείλει στον server ένα πακέτο με ενεργοποιημένο μόνο το flag: **ACK**, στο οποίο επιβεβαιώνει ότι το επόμενο πακέτο που
- 
4. Το φίλτρο tcp.port == 49214 προστέθηκε διότι ο περιηγητής επιλέγει να πραγματοποιήσει παράλληλες συνδέσεις στον server.

περιμένει να λάβει είναι το πακέτο με αριθμό σειράς 224000002.

11. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο.

Εφαρμόζω το πρωτόκολλο **http**. Στην συνέχεια επιλέγω **Statistics** → **Conversations** → **TCP** από το μενού και ενεργοποιώ την επιλογή **Limit to display filter**.



Εικόνα 2.10: TCP θύρες που χρησιμοποιήθηκαν από το πρωτόκολλο HTTP

Στο HTTP πρωτόκολλο οι TCP θύρα του server είναι η 80.

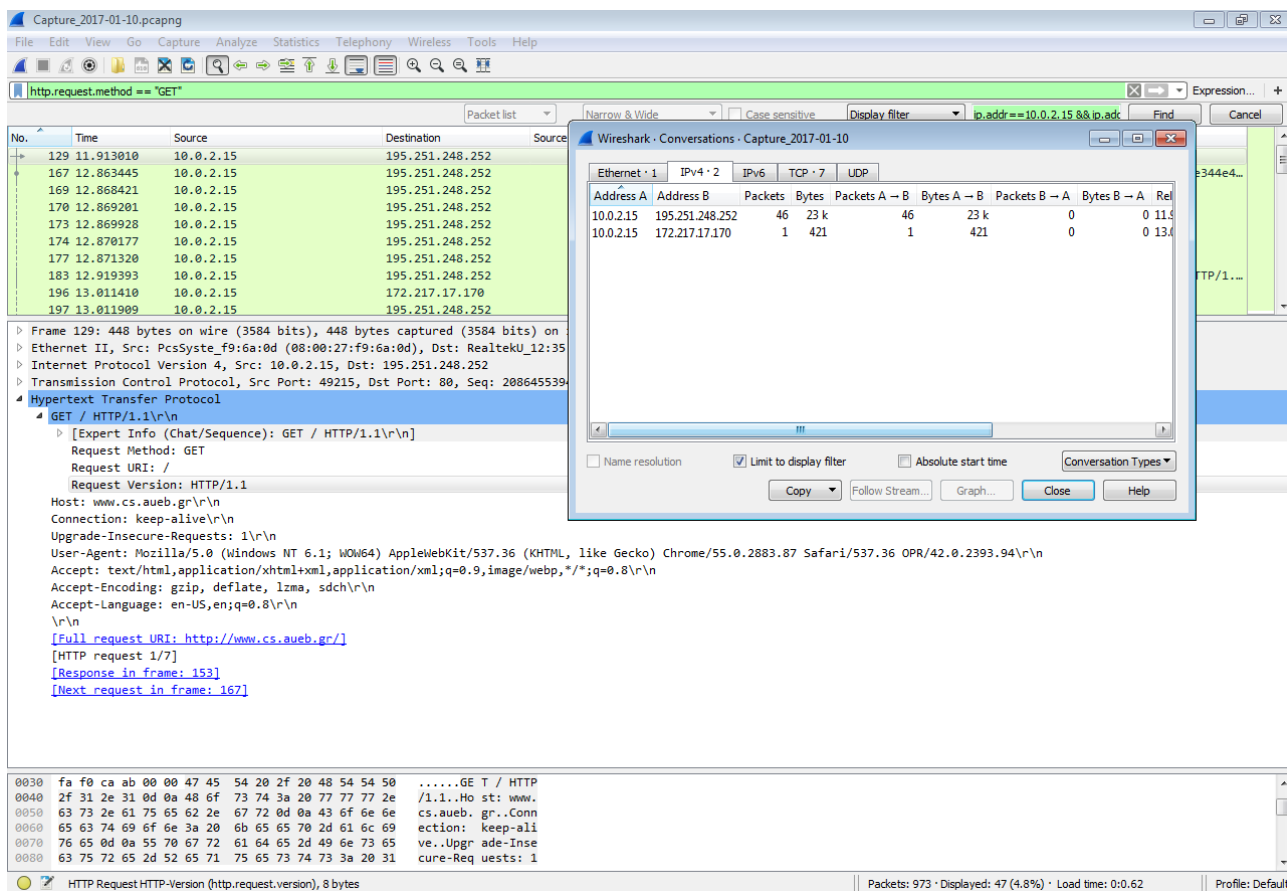
Ο αριθμός το TCP θυρών που χρησιμοποιήθηκαν από τον client είναι σχετικός του αριθμού των αρχείων που σχετίζονται με την Ιστοσελίδα και των αριθμό των συνδέσεων που χρειαστήκαν μέχρι τα αρχεία να μεταφερθούν επιτυχώς.

Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκαν 7 διαφορετικές θύρες όπως φαίνεται στην εικόνα 2.10.

12. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;

Εφαρμόζω το φίλτρο **http.request.method == "GET"**. Στην συνέχεια επιλέγω **Statistics** → **Conversations** → **IPv4** από το μενού και ενεργοποιώ την επιλογή **Limit to display filter**.

Τέλος για να συσχετίσω τις IPv4 διευθύνσεις επιλέγω **Statistics** → **Resolved Addresses** από το μενού.



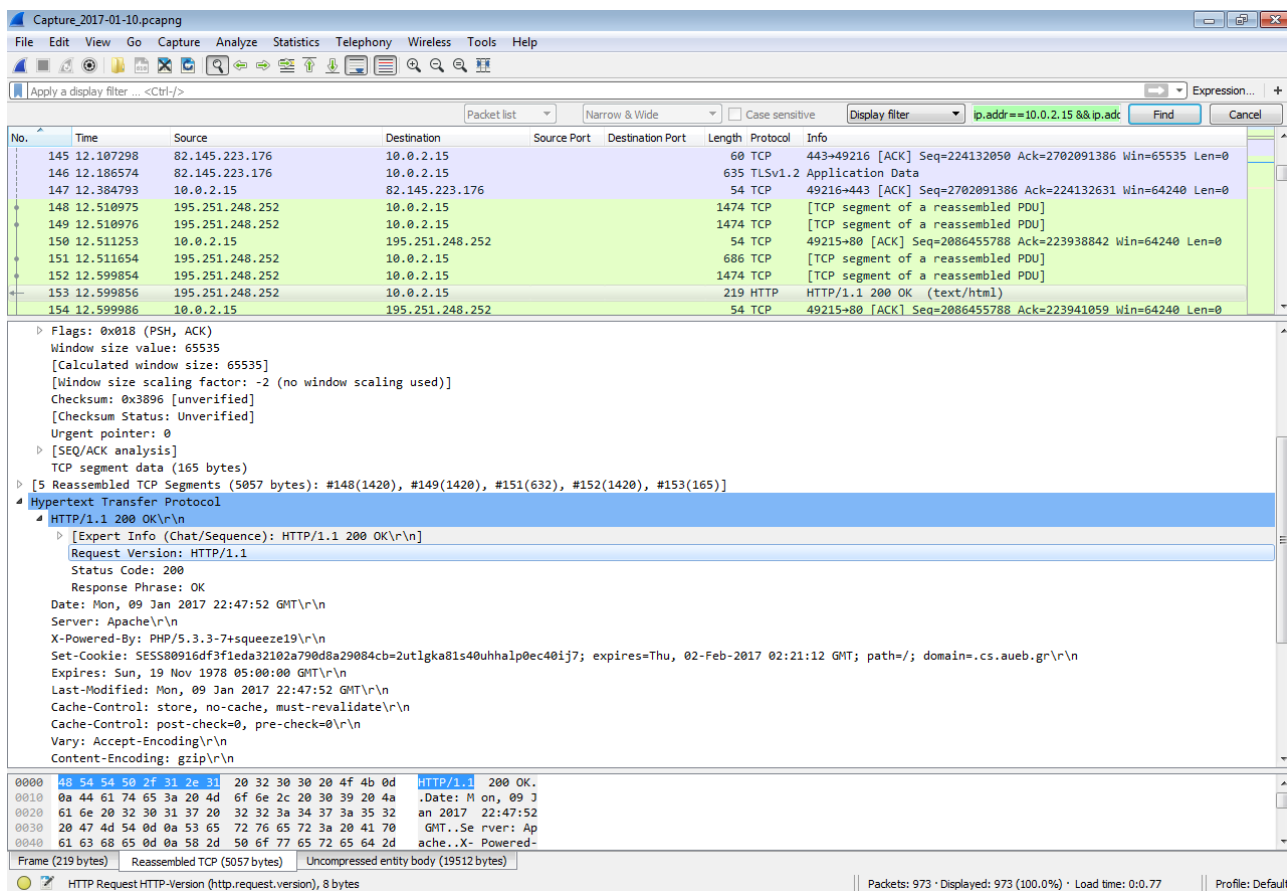
Εικόνα 2.11: HTTP GET Requests

Συνολικά στάλθηκαν 47 HTTP Get Requests, από τα οποία τα περισσότερα (46), απευθύνονται στην διεύθυνση 195.251.248.252.

Ένα HTTP Get Request στάλθηκε στην διεύθυνση 172.217.17.170, η οποία αντιστοιχεί στο `ajax.googleapis.com`.

13. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server;

Χρειάζεται απλά να μελετήσω τα header ενός HTTP Request, εικόνα 2.11 και του αντίστοιχου Reply, εικόνα 2.12, επιλέγοντας την επιλογή **Response in frame 153** από την περιοχή **Hypertext Transfer Protocol** του Analyzer.



Εικόνα 2.12: HTTP GET Reply

Τόσο ο server όσο και ο client χρησιμοποιούν την έκδοση HTTP 1.1, όπως φαίνεται στο πεδίο **Request Version**.

14. Ποιες γλώσσες υποδεικνύει ο browser στον server ότι μπορεί να δεχθεί;

Ο περιηγητής δηλώνει ότι μπορεί να δεχθεί κείμενο στις γλώσσες en-US και en (μικρότερη προτίμηση), όπως φαίνεται και στο πεδίο **Accept-Language**, εικόνα 2.11.

15. Ποιος είναι ο κωδικός κατάστασης (status code) που επιστρέφεται από το server στον browser σας;

Ο κωδικός κατάστασης φαίνεται στο πεδίο **Status Code**, εικόνα 2.12. Ο server επέστρεψε σε όλα τα ερωτήματα των κωδικό: 200. Που σημαίνει ότι δεν υπήρξε σφάλμα.

## Βιβλιογραφία

M. Crawford. “RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks,” December 1998. <https://tools.ietf.org/html/rfc2464>.