

**δικτυα υπολογιστων**

**Εργαστηριακη ασκηση 1: αναλυτησ πρωτοκολλων wireshark**





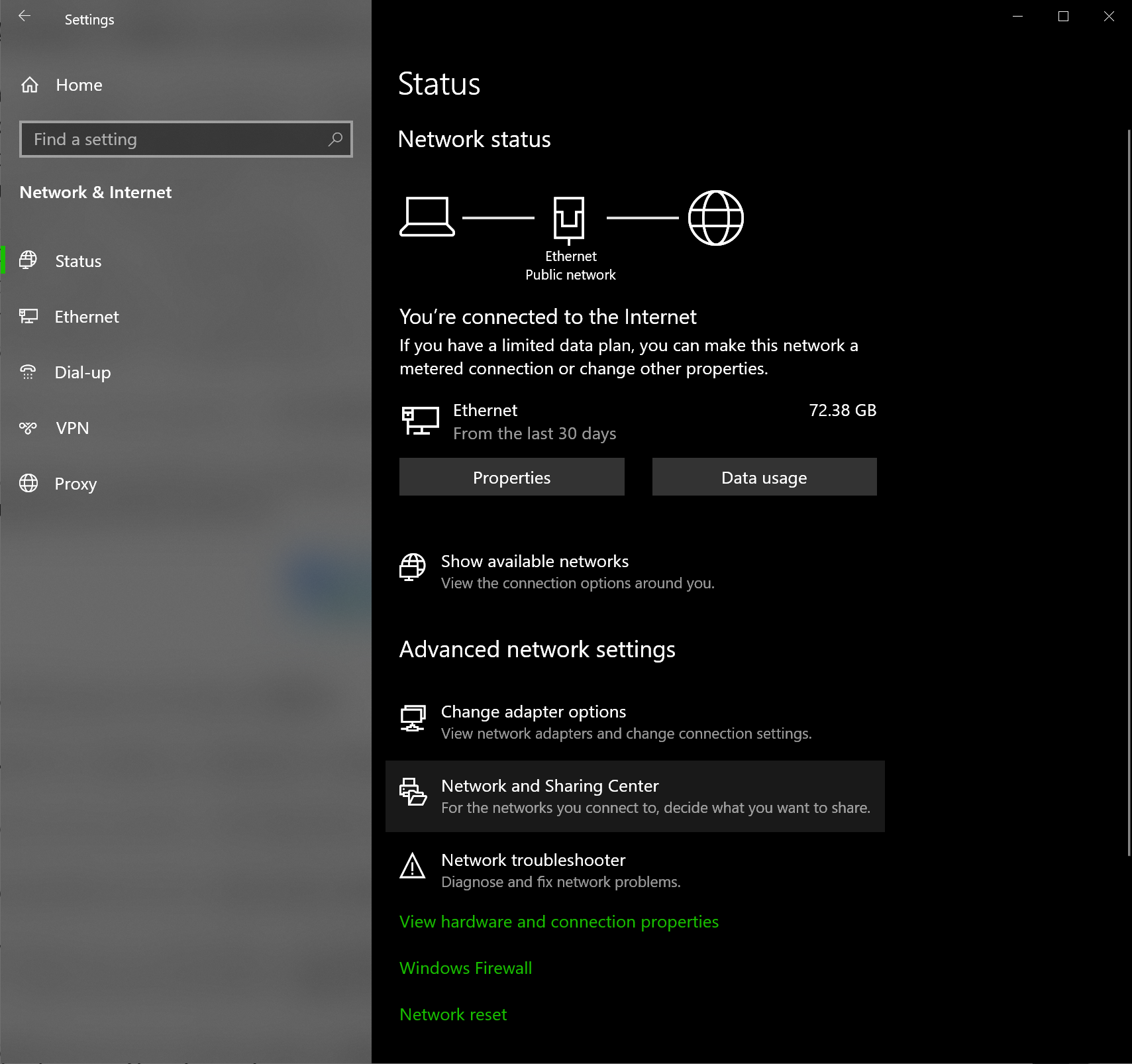
11 οκτωβριου, 2022

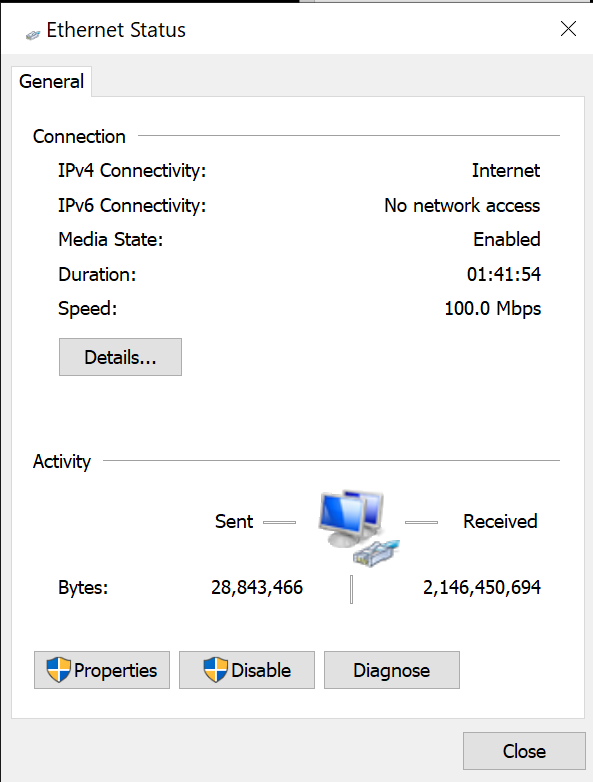
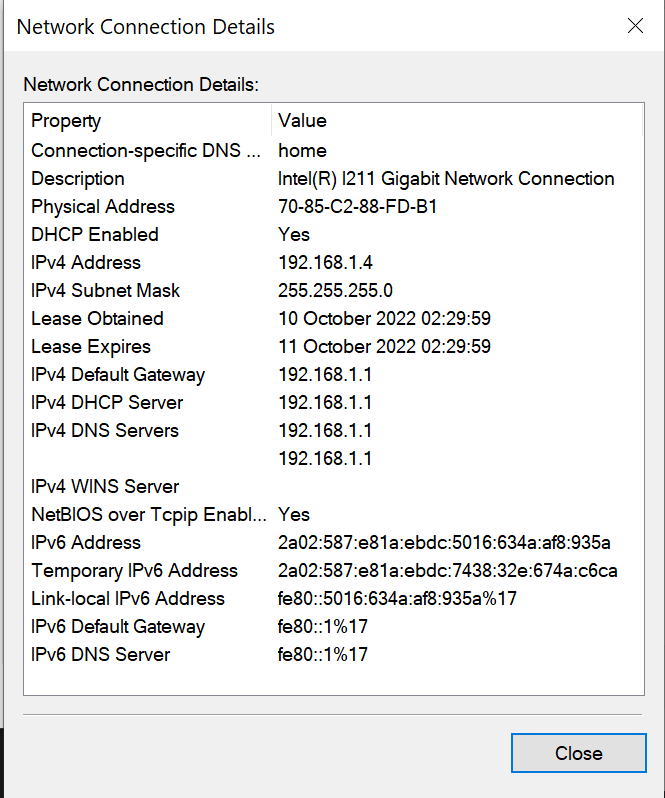
ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | | **Ομάδα:** 2 |
| **Όνομα PC/ΛΣ:** DESKTOP-JGHL94V/ WINDOWS 10 | | **Ημερομηνία:** 11/10/2022 |
| **Διεύθυνση IP:** 192.168.1.4 | **Διεύθυνση MAC:** 70-85-C2-88-FD-B1 | |

\*\*Η εργασία ξεκίνησε στο PCLAB της σχολής αλλά λόγω περιορισμού δικαιωμάτων χρήστη στο pc επέλεξα να ξανακάνω από την αρχή την εργασία στον προσωπικό μου υπολογιστή.\*\*

**Άσκηση 1: Βρείτε την κάρτα δικτύου**

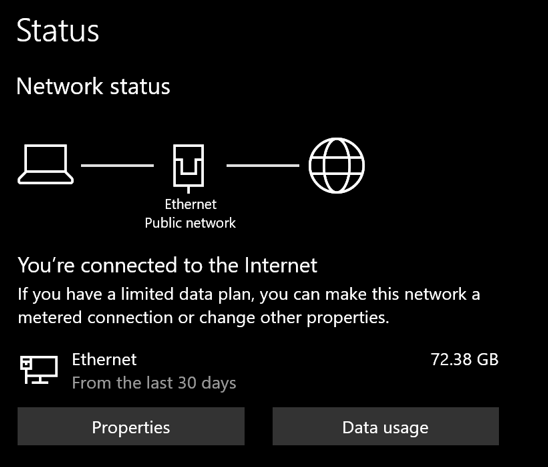
Θέλουμε να μεταβούμε στις ρυθμίσεις δικτύου και Internet των windows. Αυτό μπορούμε να το κάνουμε είτε πατώντας στο εικονίδιο «internet access» κάτω δεξιά στη γραμμή εργασιών είτε πατώντας το hot key των windows και από εκεί επιλέγουμε ρυθμίσεις και τέλος επιλέγουμε «Network and Internet settings».

Το παράθυρο που αναδύεται έχει τίτλο Ethernet Status. Εκεί επιλέγουμε «Change adapter options» και από το παράθυρο που αναδύεται (με τίτλο «Ethernet Status») επιλέγουμε «Details…». Ύστερα αναδύεται το ακόλουθο παράθυρο με τίτλο «Network Connection Details».

***1.1***

Το όνομα του network adapter είναι: ***Intel(R) I211 Gigabit Network Connection***

***1.2***

Από το πεδίο Status στις ρυθμίσεις «Network & Internet», μπορούμε να δούμε να αναγράφεται ότι η σύνδεσή μας είναι με **Ethernet**.

***1.3***

Στο παράθυρο Ethernet Status βλέπουμε ότι η ταχύτητα σύνδεσης είναι: **100Mbps**

***1.4***

Στο παράθυρο Network Connection Details βλέπουμε ότι η διεύθυνση MAC (physical address) είναι: **70-85-C2-88-FD-B1**

***1.5***

Στο παράθυρο Network Connection Details βλέπουμε ότι η διεύθυνση IPv4 είναι: **192.168.1.4**

***1.6***

Στο παράθυρο Network Connection Details βλέπουμε ότι η διεύθυνση IPv6 είναι:

**2a02:587:e81a:ebdc:5016:634a:af8:935a**

***1.7***

Στο παράθυρο Network Connection Details βλέπουμε ότι οι διευθύνσεις IPv4 και IPv6 των εξυπηρετητών DNS είναι:

***IPv4 DNS Servers:* 192.168.1.1, 192.168.1.1**

***IPv6 DNS Server:* fe80::1%17**

***1.8***

Στο παράθυρο Network Connection Details βλέπουμε ότι οι διευθύνσεις IPv4 και IPv6 των προκαθορισμένων πυλών (default gateway/route) είναι:

***IPv4 Default Gateway:* 192.168.1.1**

***IPv6 Default Gateway:* fe80::1%17**

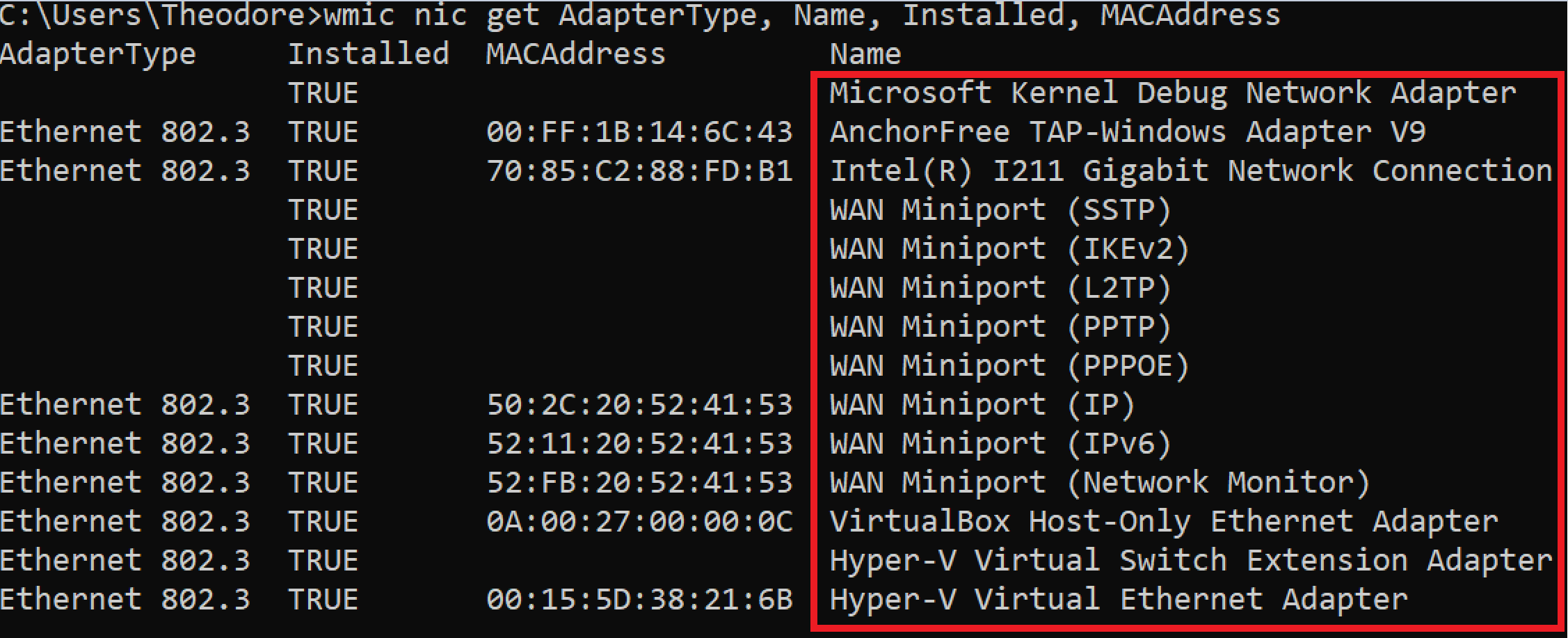
**Άσκηση 2: Ρυθμίσεις και στατιστικά**

***2.1***

Εκτελούμε την εντολή “**ipconfig/all**” στο command prompt των Windows και το όνομα χρήστη εμφανίζεται στην αρχή και είναι: **DESKTOP-JGHL94**

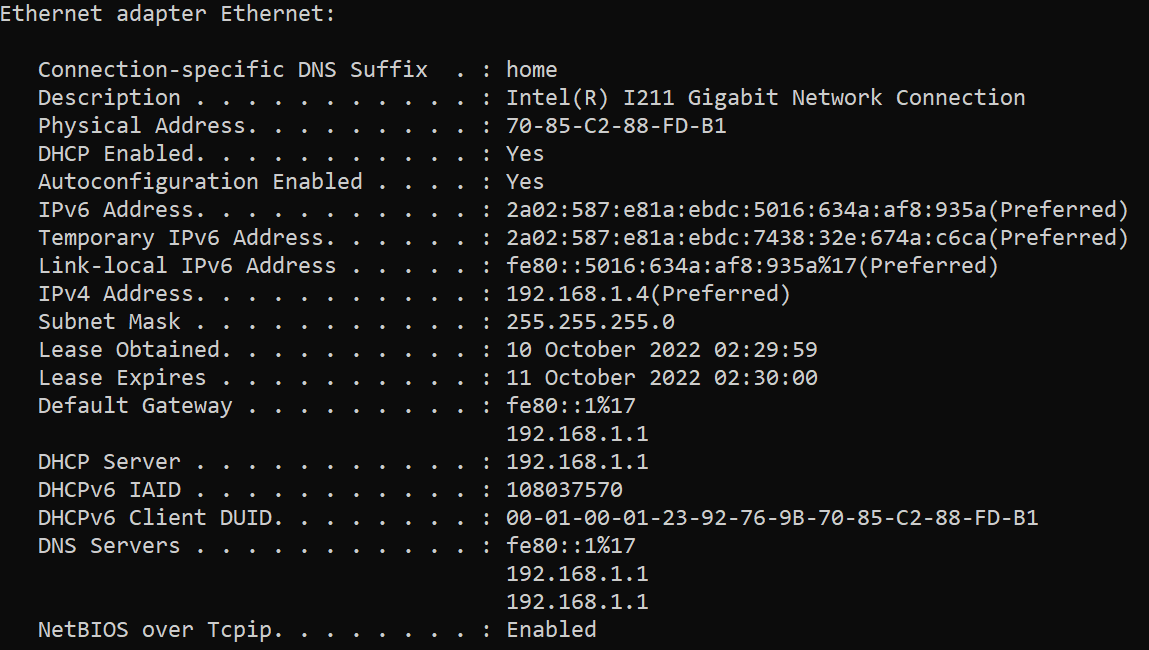
Το όνομα του network adapter είναι: ***Intel(R) I211 Gigabit Network Connection***

***2.2***

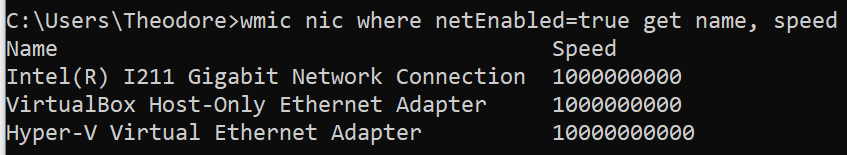
Εκτελούμε την εντολή “**wmic nic get AdapterType, Name, Installed, MACAddress**” στο command prompt των Windows και παίρνουμε τις αντίστοιχες πληροφορίες για τις κάρτες δικτύου. Τα ονόματα των καρτών δικτύου είναι:

***2.3***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τη διεύθυνση MAC (physical address): **70-85-C2-88-FD-B1**



***2.4***

Εκτελούμε την εντολή “**wmic nic where netEnabled=true get name, speed**” στο command prompt των Windows και βλέπουμε την ταχύτητα σύνδεσης της κάρτας δικτύου μας, η οποία είναι: **100MBps**

***2.5***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τη διεύθυνση IPv4 της διεπαφής Ethernet:

**192.168.1.4**

***2.6***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τη μάσκα υποδικτύου: **255.255.255.0**

**i)** το μέγεθος σε bit του τμήματος δικτύου της διεύθυνσης IPv4 του υπολογιστή:

, άρα **24 bits** μάσκα δικτύου

**ii)** και τη διεύθυνση του υποδικτύου:

IPv4:

Subnet mask:

Εκτελούμε το λογικό AND μεταξύ αυτών των δύο και λαμβάνουμε τη διεύθυνση υποδικτύου: **192.168.1.0**

***2.7***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τη διεύθυνση IPv6 της διεπαφής Ethernet:

**2a02:587:e81a:ebdc:5016:634a:af8:935a**

***2.8***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τις διευθύνσεις IPv4 και IPv6 των προκαθορισμένων πυλών (default gateway/route):

***IPv4 Default Gateway:* 192.168.1.1**

***IPv6 Default Gateway:* fe80::1%17**

***2.9***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε τις διευθύνσεις IPv4 και IPv6 των εξυπηρετητών DNS:

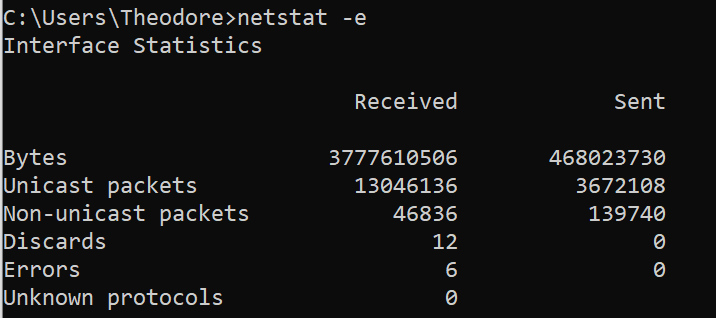
***IPv4 DNS Servers:* 192.168.1.1, 192.168.1.1**

***IPv6 DNS Server:* fe80::1%17**

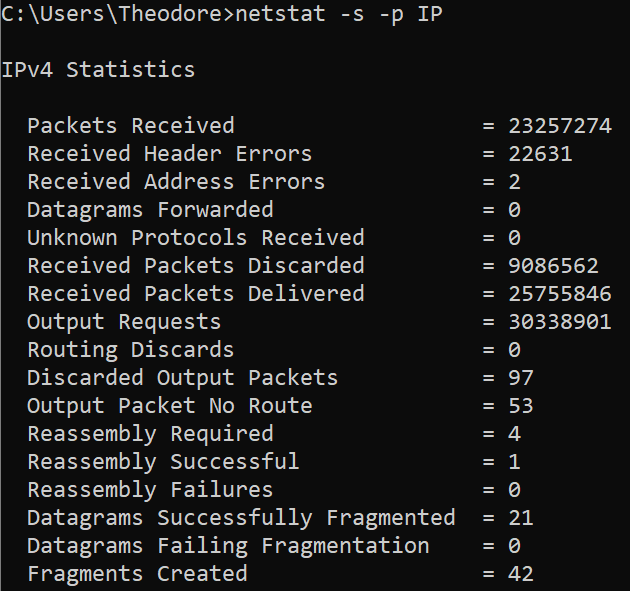
***2.10***

Εκτελούμε την εντολή “**ipconfig /all**” στο command prompt των Windows και στο πεδίο Ethernet adapter Ethernet βρίσκουμε την διεύθυνση IPv4 του DHCP server: **192.168.1.1**

***2.11***

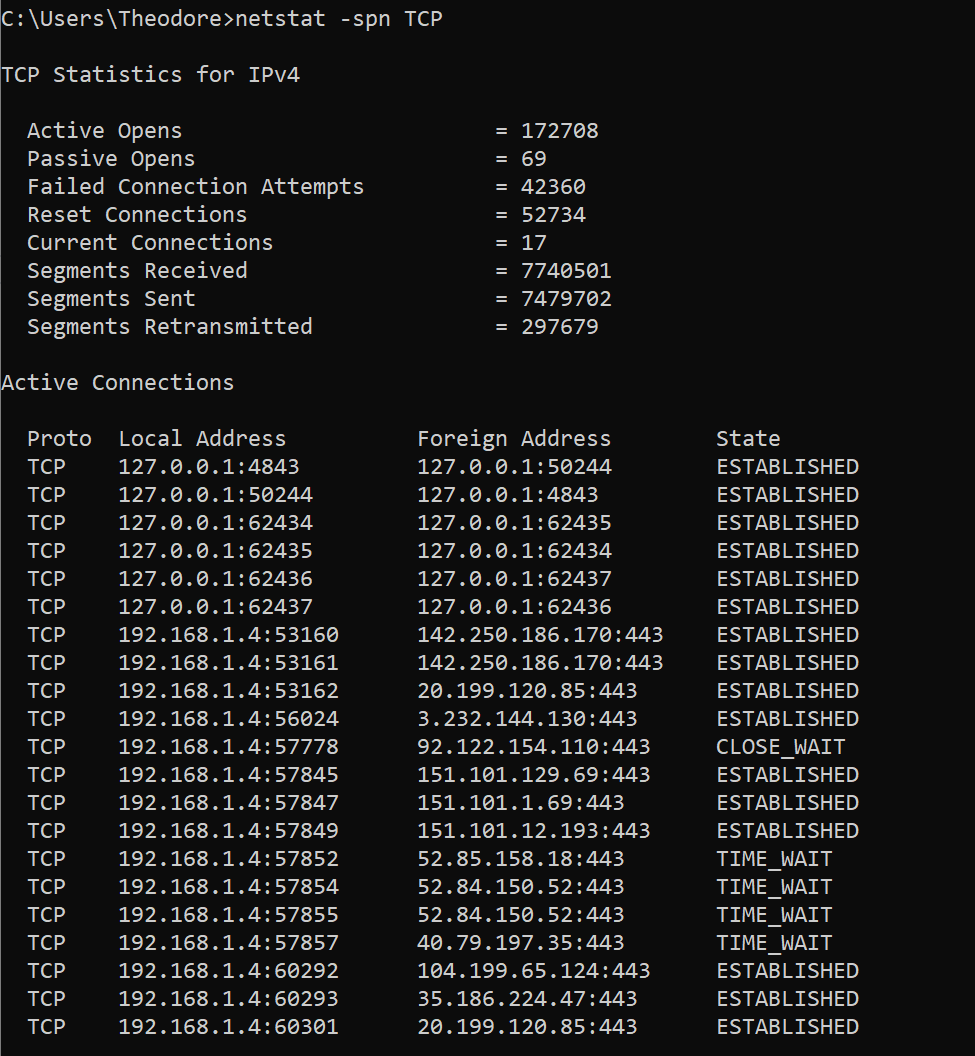
Εκτελούμε την εντολή “**netstat -e**” στο command prompt των Windows και αντλούμε πληροφορίες για τα πακέτα που στέλνονται και λαμβάνονται. Συγκεκριμένα τα unicast packets είναι πακέτα επικοινωνίας μεταξύ της δικής μας κάρτας δικτύου και μιας άλλης στο διαδίκτυο, ενώ τα non-unicast packets είναι πακέτα που προορίζονται για πολλές διεπαφές, μαζί και εμάς.

***2.12***

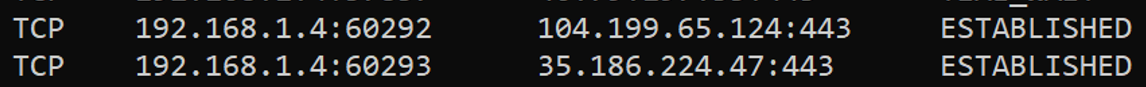
Εκτελούμε την εντολή “**netstat –s –p IP**”, όπου το –s μας δείχνει τ στατιστικά ανά πρωτόκολλο, ενώ το –p prototype δείχνει τις συνδέσεις για το συγκεκριμένο πρωτόκολλο. Επομένως, δίνοντας ως όρισμα το IP (IPv4), αντλούμε τα ακόλουθα στοιχεία για το πλήθος των πακέτων που στέλνονται και λαμβάνονται μέσω IPv4 πρωτοκόλλου:

***2.13***

Εκτελούμε την εντολή “**netstat –spn TCP**” και βλέπουμε ότι έχουμε 17 TCP συνδέσεις συνολικά. Από τις 17, οι established είναι οι συνδέσεις που αναγράφονται στο πεδίο «Active Connections» και δεν έχουν ως πηγή και προορισμό την διεύθυνση 127.0.0.1. Αυτές είναι συνολικά 10. Το “–n” εμφανίζει τι ενεργές συνδέσεις TCP χωρίς να αναζητεί τα ονόματά τους.



***2.14***

Εκτελούμε την ίδια εντολή με προηγουμένως και επιλέγουμε δύο τυχαίες συνδέσεις:

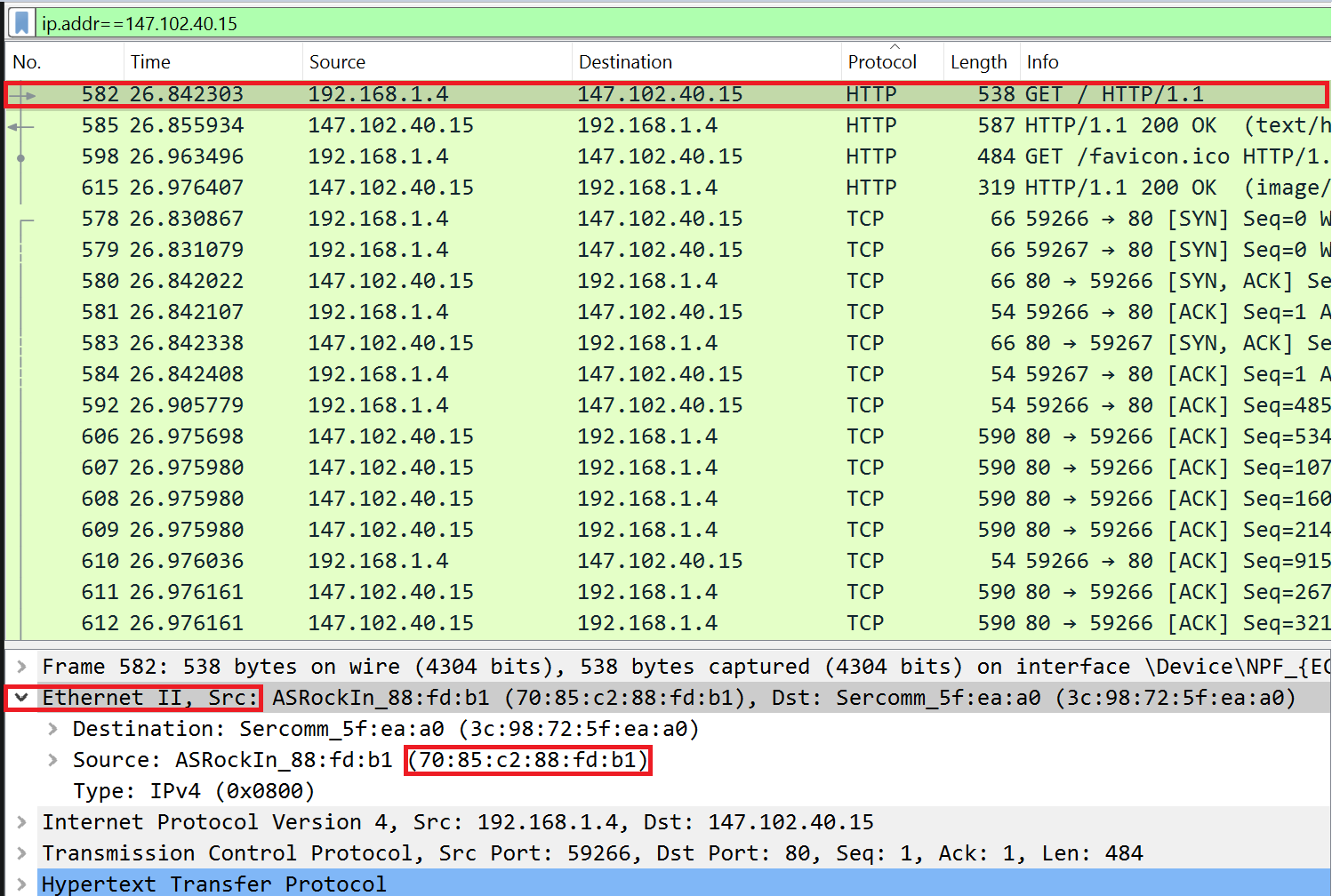
Οι θύρες προορισμού είναι 443 και για τις δύο συνδέσεις, ενώ οι θύρες πηγής είναι 60292 για την μία και 60293 για την άλλη.

**Άσκηση 3: Αναλυτής πρωτοκόλλων Wireshark**

***3.1***

Τα διάφορα πρωτόκολλα που εμφανίζονται είναι: **ARP, DNS, HTTP, ICMPv6, LLDP, MDNS, QUIC, SSDP, STP, TCP, TLSv1.2, TLSv1.3, UDP**

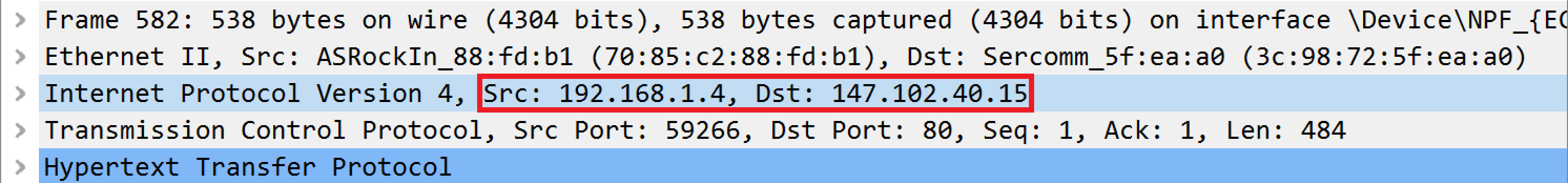
***3.2***

Βρίσκουμε το πρώτο GET που στέλνει ο υπολογιστής μας στην ιστοσελίδα (frame 582). Το επιλέγουμε από την λίστα πακέτων και εμφανίζονται οι λεπτομέρειές του στο αντίστοιχο πεδίο. Από εκεί επιλέγουμε το Ethernet II, Src (το οποίο αποτελεί το Layer 2 και αναμένουμε να βρούμε έτσι την διεύθυνση MAC). Πράγματι εντοπίσαμε την MAC address της κάρτας δικτύου, η οποία είναι: **70-85-C2-88-FD-B1**

***3.3***

Στην παραπάνω εικόνα και στο ίδιο πεδίο μπορούμε να δούμε ότι το όνομα του κατασκευαστή της κάρτας δικτύου είναι **ASRockIN**.

***3.4***

Για να βρούμε τώρα τη διεύθυνση IPv4 του υπολογιστή μας, κοιτάμε το πεδίο Internet Protocol Version 4, Src, όπου και βλέπουμε ότι η διεύθυνση του source (δηλαδή του υπολογιστή μας που έστειλε το μήνυμα GET) είναι: **192.168.1.4**

***3.5***

Για να βρούμε τώρα τη διεύθυνση IPv4 της δοσμένης ιστοσελίδας, κοιτάμε πάλι το πεδίο Internet Protocol Version 4, Src, όπου και βλέπουμε ότι η διεύθυνση του destination (δηλαδή της σελίδας που έλαβε το μήνυμα GET) είναι: **147.102.40.15**

***3.6***

Η σύνταξη του φίλτρου είναι τώρα: **tcp.stream eq 34**

***3.7***

Από τα αποτελέσματα που λαμβάνουμε κάνοντας follow TCP stream βρίσκουμε:

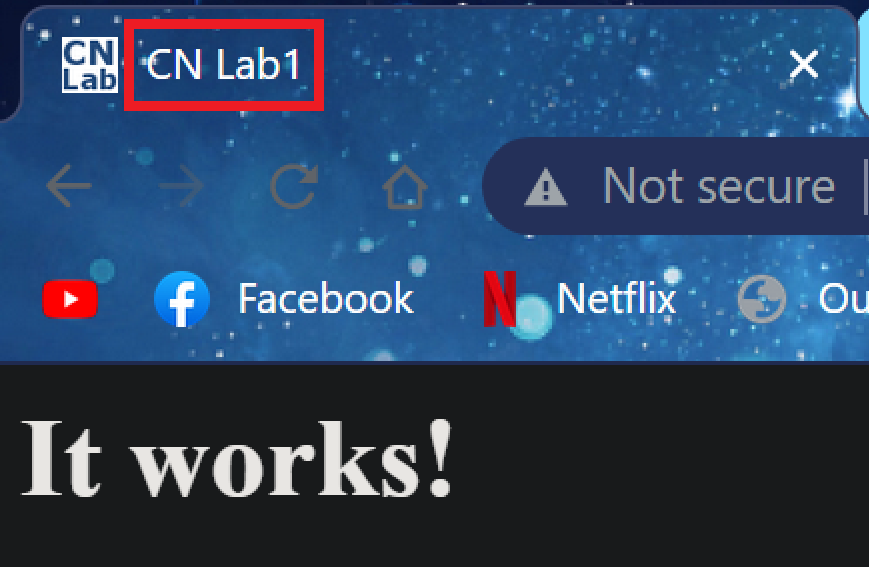
**i)** Τον τύπο του εξυπηρετητή της ιστοσελίδας που επισκεφτήκαμε:

**Apache/2.2.22 (FreeBSD) mod\_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2**

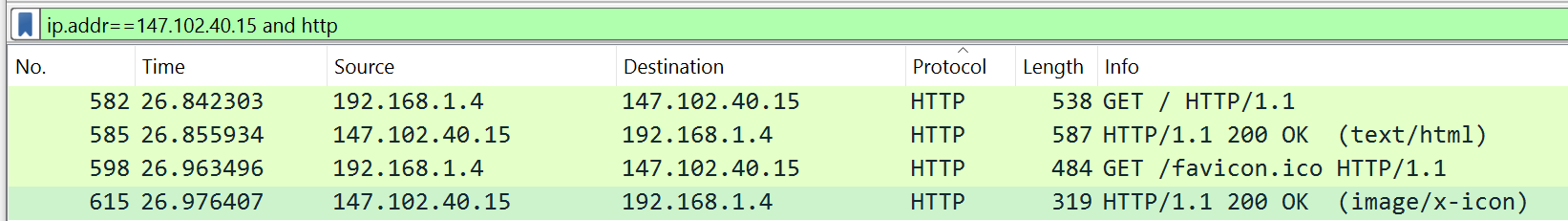
**ii)** τον τίτλο και το αντίστοιχο HTML tag της ιστοσελίδας που επισκεφτήκαμε:

τίτλος: **CN Lab1**

HTML tag: **<head><title>CN Lab1</title></head**>

**iii)** Εμφανίζεται ως τίτλος στην καρτέλα της ιστοσελίδας.

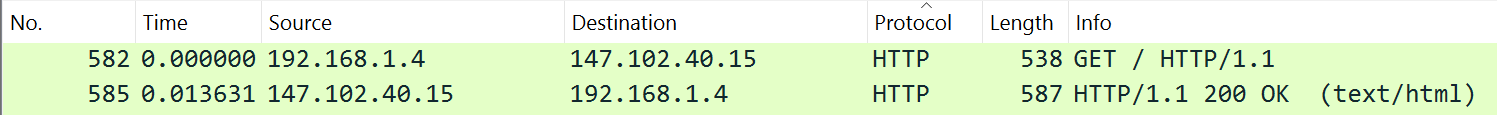
***3.8***

Χρησιμοποιούμε το φίλτρο «**ip.addr==147.102.40.15 and http**» και λαμβάνουμε τα ζητούμενα πακέτα.

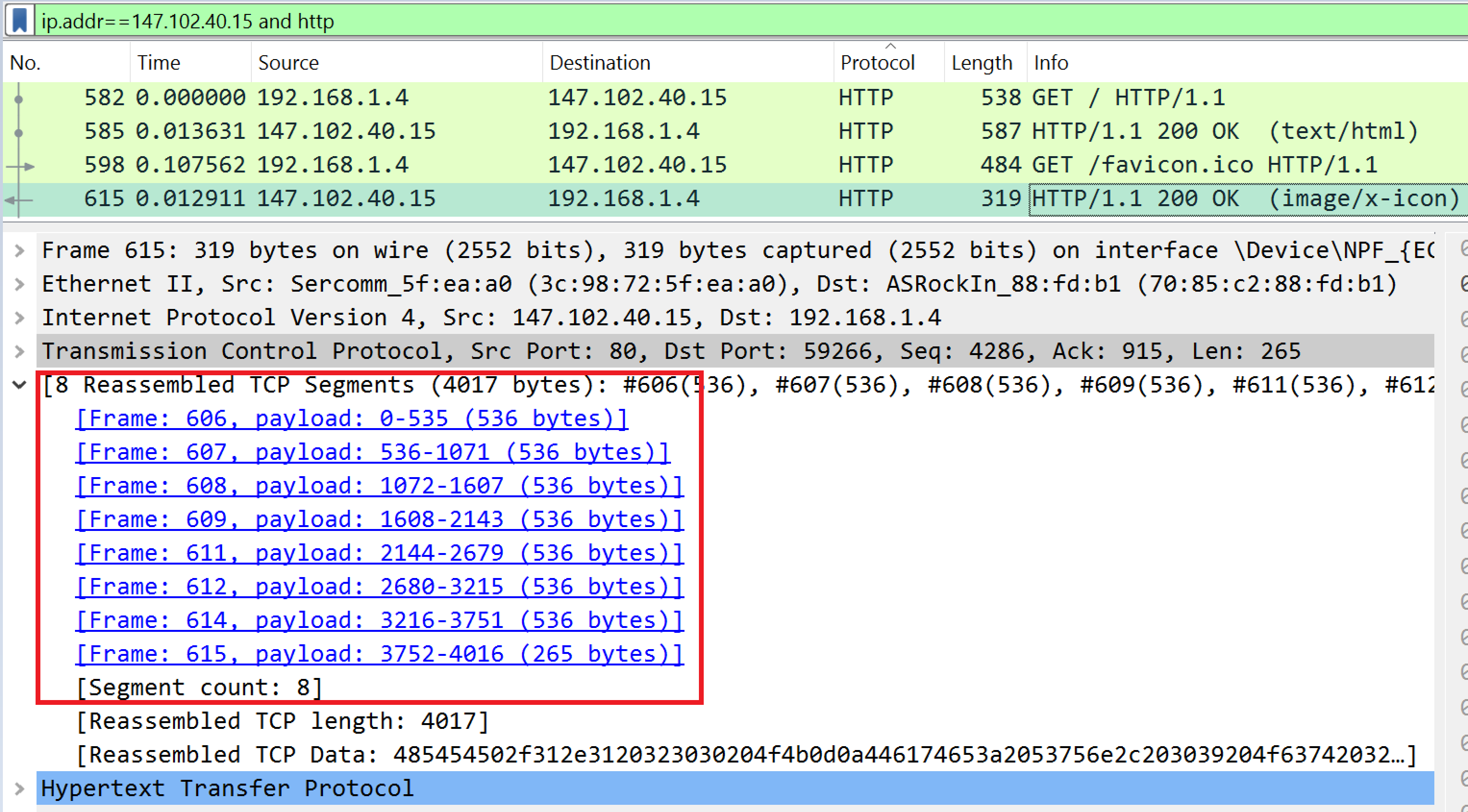
***3.9***

Με χρήση του παραπάνω φίλτρο εύκολα βλέπουμε ότι δύο μνήματα HTTP στάλθηκαν και δύο λήφθηκαν. Τα μηνύματα που έχουν source την IP μας είναι αυτά που στάλθηκαν από εμάς ενώ αυτά που έχουν ως destination την IP μας λήφθηκαν από εμάς.

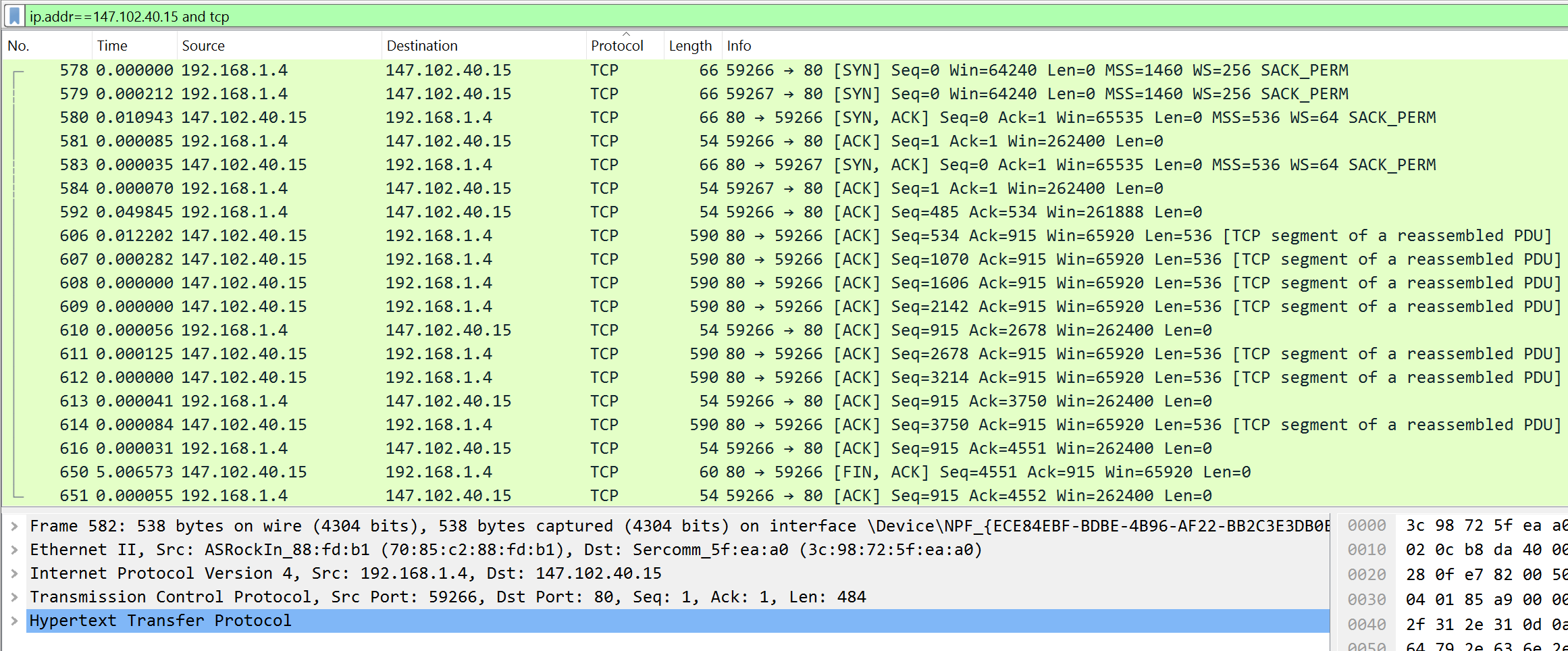
***3.10***

Ακολουθώντας την υπόδειξη, στο πεδίο time μπορούμε να δούμε ότι ο χρόνος που πέρασε από την στιγμή που στάλθηκε το πρώτο GET μέχρι να ληφθεί η απόκριση 200 OK είναι: 0.013631 seconds (-0.0000000, τον χρόνο που έκανε να σταλθεί το αίτημα GET).

***3.11***

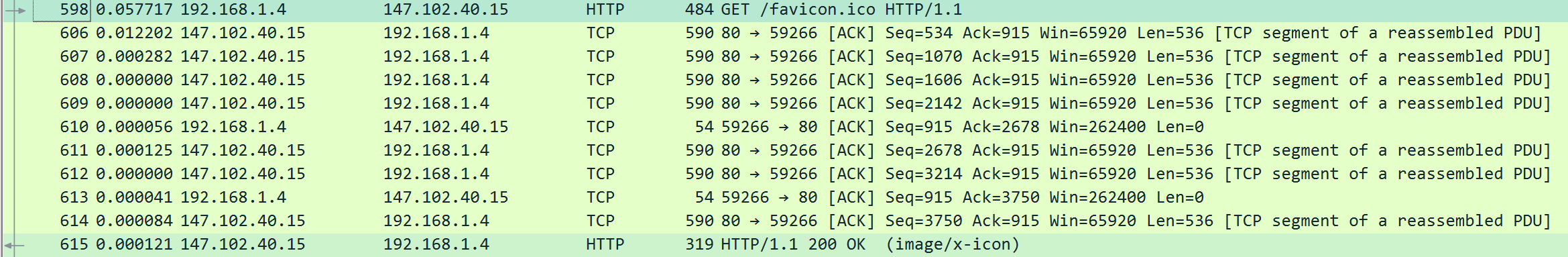
Επιλέγουμε την απόκριση της σελίδας στο δεύτερο μήνυμα GET από την λίστα πακέτων και ύστερα στις λεπτομέρειες επιλέγουμε την επικεφαλίδα που αναφέρει τα Reassembled TCP Segments. Εκεί βλέπουμε ότι το πλήθος των πακέτων είναι 8 (frames 606-615).

***3.12***

Χρησιμοποιούμε το φίλτρο «**ip.addr==147.102.40.15 and tcp**» και λαμβάνουμε τα ζητούμενα πακέτα.

***3.13***

Ταξινομούμε την λίστα πακέτων με βάση τον χρόνο. Έχουμε επιλέξει από πριν να εμφανίζεται ο χρόνος από το προηγούμενο πακέτο που εμφανίζεται στην λίστα.

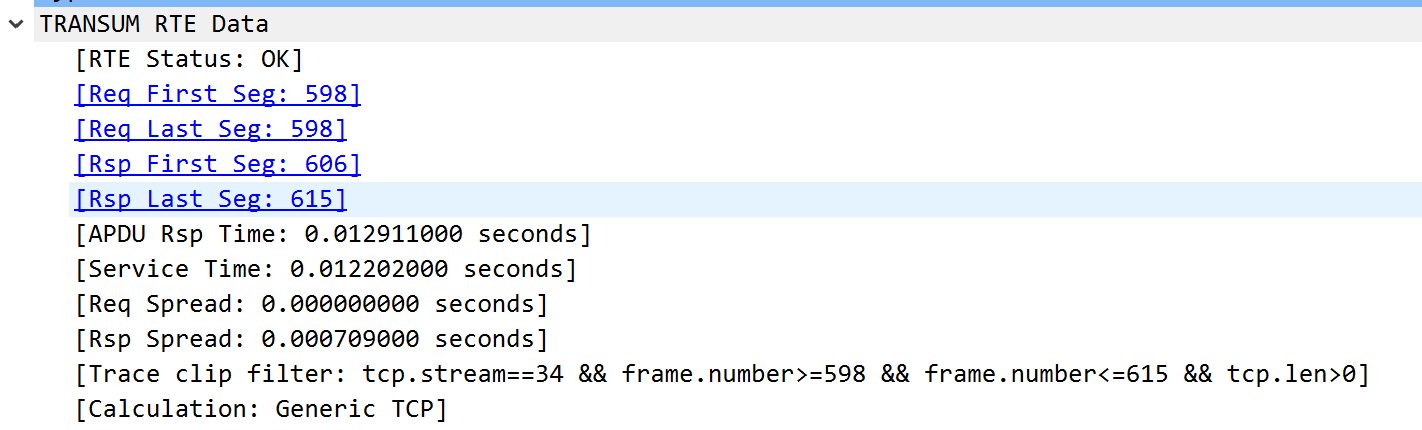
**α)** Το πρώτο πακέτο με τα δεδομένα της εικόνας λήφθηκε **0.12202 sec** αργότερα.

Επιλέγουμε στο πεδίο time να εμφανίζεται ο χρόνος από το πρώτο πακέτο που «πιάστηκε».

**β)** Ο χρόνος που πέρασε από την προηγούμενη στιγμή (26.975698) μέχρι να ολοκληρωθεί η μετάδοση των άλλων (26.976407) πακέτων είναι: **0.000709 sec**

**γ)** Τέλος ο χρόνος απόκρισης στο αίτημα GET είναι: 26.976407 – 26.963496 = **0.12911 sec**

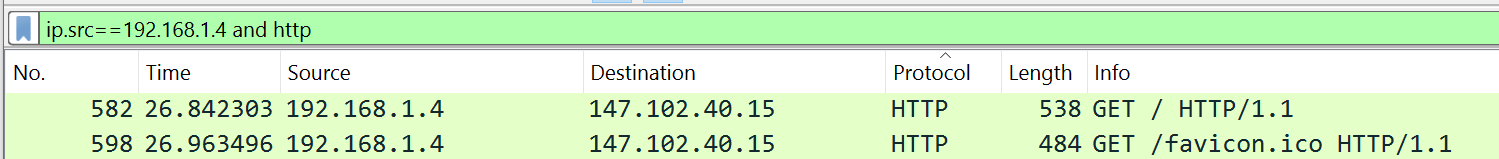
***3.14***

Ακολουθούμε τις οδηγίες και λαμβάνουμε τις εξής πληροφορίες:

Παρατηρούμε ότι οι χρόνοι ταυτίζονται με τους δικούς μας που βρήκαμε παραπάνω ως εξής:

**α) Service Time, β) Rsp Spread, γ) APDU Rsp Time**

***3.15***

Χρησιμοποιούμε το φίλτρο «**ip.src==192.168.1.4 and http**» και λαμβάνουμε τα ζητούμενα πακέτα.