



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ  
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

## Δίκτυα Υπολογιστών

**Αναφορά 1ης Εργαστηριακής Άσκησης**

**Ραπτόπουλος Πέτρος (ει19145)  
Ομάδα 3**

# Άσκηση 1

## 1.1) Ονομασία Κάρτας Δικτύου: Wireless 8265/8275 by Intel Corporation

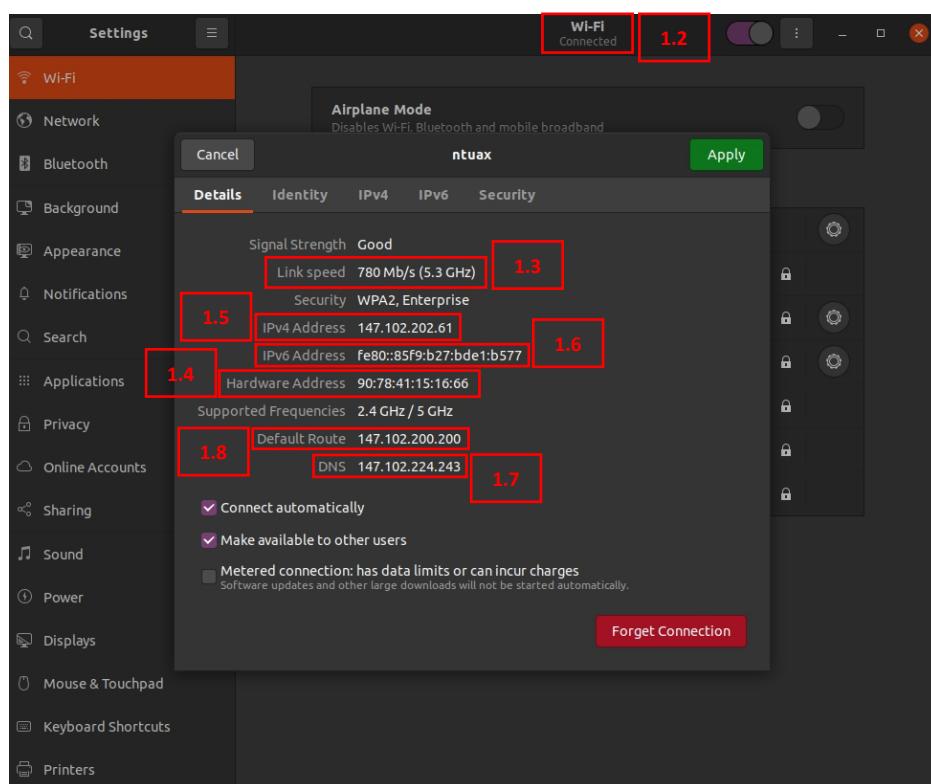
Χρησιμοποιώντας το terminal βρίσκουμε την ονομασία της κάρτας δικτύου μέσω της οποίας συνδεόμαστε στο διαδίκτυο (δεν υπάρχει αντίστοιχος τρόπος εύρεσης μέσω του γραφικού περιβάλλοντος του ubuntu):

```
petrosrapt0@petrosrapt0Assistant:~$ lspci
00:00.0 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Root Complex
00:00.2 IOMMU: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 IOMMU
00:01.0 Host bridge: Advanced Micro Devices, Inc. [AMD] Family 17h (Models 00h-1fh) PCIe Dummy Host Bridge
00:01.2 PCI bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 PCIe GPP Bridge [0:0]
00:01.3 PCI bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 PCIe GPP Bridge [0:0]
00:08.0 Host bridge: Advanced Micro Devices, Inc. [AMD] Family 17h (Models 00h-1fh) PCIe Dummy Host Bridge
00:08.1 PCI bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Internal PCIe GPP Bridge 0 to Bus A
00:08.2 PCI bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Internal PCIe GPP Bridge 0 to Bus B
00:14.0 SMBus: Advanced Micro Devices, Inc. [AMD] FCH SMBus Controller (rev 61)
00:14.3 ISA bridge: Advanced Micro Devices, Inc. [AMD] FCH LP Bridge (rev 51)
00:18.0 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 0
00:18.1 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 1
00:18.2 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 2
00:18.3 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 3
00:18.4 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 4
00:18.5 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 5
00:18.6 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 6
00:18.7 Host bridge: Advanced Micro Devices, Inc. [AMD] Raven/Raven2 Device 24: Function 7
01:00.0 Network controller: Intel Corporation Wireless 8265 / 8275 (rev 78)
02:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN520 NVMe SSD (rev 01)
03:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/ATI] Picasso (rev c1)
03:00.1 Audio device: Advanced Micro Devices, Inc. [AMD/ATI] Raven/Raven2/Fenghuang HDMI/DP Audio Controller
03:00.2 Encryption controller: Advanced Micro Devices, Inc. [AMD] Family 17h (Models 10h-1fh) Platform Security Processor
03:00.3 USB controller: Advanced Micro Devices, Inc. [AMD] Raven USB 3.1
03:00.4 USB controller: Advanced Micro Devices, Inc. [AMD] Raven USB 3.1
03:00.5 Multimedia controller: Advanced Micro Devices, Inc. [AMD] Raven/Raven2/FireFlight/Renoir Audio Processor
03:00.6 Audio device: Advanced Micro Devices, Inc. [AMD] Family 17h (Models 10h-1fh) HD Audio Controller
04:00.0 SATA controller: Advanced Micro Devices, Inc. [AMD] FCH SATA Controller [AHCI mode] (rev 61)
```

ή εναλλακτικά:

```
petrosrapt0@petrosrapt0Assistant:~$ lshw -c network
WARNING: you should run this program as super-user.
*-network
    description: Wireless interface
    product: Wireless 8265 / 8275
    vendor: Intel Corporation
    physical id: 0
    bus info: pci@0000:01:00.0
    logical name: wlpiis0
    version: 78
    serial: 90:78:41:15:16:66
    width: 64 bits
    clock: 33MHz
    capabilities: bus_master cap_list ethernet physical wireless
    configuration: broadcast=yes driver=iwlwifi driverversion=5.4.0-126-generic firmware=...
    resources: irq:69 memory:fea00000fea01fff
WARNING: output may be incomplete or inaccurate, you should run this program as super-user.
```

Χρησιμοποιώντας το γραφικό περιβάλλον του υπολογιστή μας βρίσκουμε πληροφορίες σχετικές με τη σύνδεσή μας στο διαδίκτυο. Επιλέγοντας “Wifi Settings” και στη συνέχεια το icon “settings” του δικτύου ntuaX που είμαστε συνδεδεμένοι έχουμε:



Άρα:

1.2) Είδος Σύνδεσης: **Ασύρματη Σύνδεση (Wifi)**

1.3) Ταχύτητα Σύνδεσης: **780 (Mb/s)**

Σημείωση: Η παραπάνω τιμή είναι μη ρεαλιστικά μεγάλη. Αποτελεί πιθανόν την ονομαστική τιμή της ταχύτητας και όχι την πραγματική.

1.4) Διεύθυνση υποστρώματος MAC (δεκαεξαδική μορφή): **90:78:41:15:16:66**

1.5) Διεύθυνση IPv4 (Wifi) του υπολογιστή (δεκαδικός συμβολισμός): **147.102.202.61**

1.6) Διεύθυνση IPv6 (Wifi) του υπολογιστή: **fe80::85f9:b27:bde1:b577**

1.7) Διεύθυνση IPv4 του εξυπηρετητή DNS: **147.102.224.243**

1.8) Διεύθυνση IPv4 της προκαθορισμένης πύλης: **147.102.200.200**

## Άσκηση 2

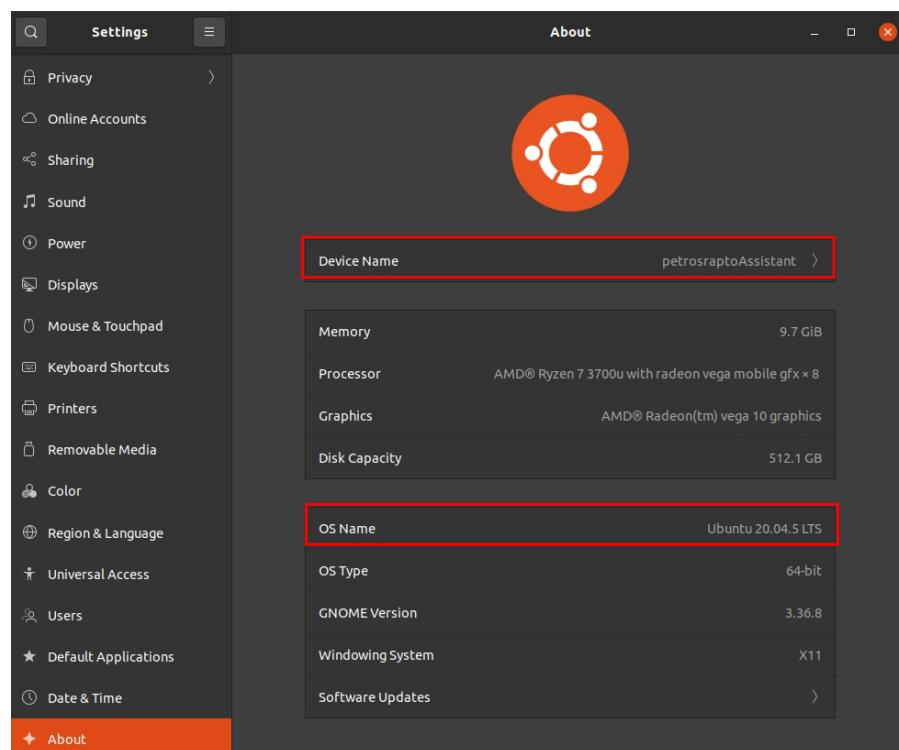
Αντλούμε αντίστοιχα στοιχεία σχετικά με τις παραμέτρους δικτύωσης του υπολογιστή μας μέσω εντολών φλοιού:

2.1) Όνομα Υπολογιστή: **petrosraptoAssistant**

```
petrosrapto@petrosraptoAssistant:~$ hostname  
petrosraptoAssistant
```

Μπορούμε να επαληθεύσουμε το παραπάνω μέσω του γραφικού περιβάλλοντος του Ubuntu.

Μεταβαίνουμε στις ρυθμίσεις (“Settings”) και μετά “About”:



Επιπλέον βλέπουμε το όνομα του λειτουργικού μας: **Ubuntu 20.04.5 LTS**

2.2) Ονόματα καρτών δικτύου: **lo, wlp1s0**.

Η (εικονική) κάρτα δικτύου “lo” λειτουργεί ως “Local Loopback”. Χρησιμοποιείται από το σύστημα για να στείλει ένα μήνυμα στον εαυτό του ώστε να ελέγχει αν η στοίβα TCP/IP λειτουργεί ορθά.

Η κάρτα δικτύου “wlp1s0” είναι η φυσική κάρτα δικτύου του υπολογιστή μας μέσω της οποίας γίνεται η επικοινωνία με το δίκτυο.

```

petrosrapto@petrosraptoAssistant:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 1408 bytes 136853 (136.8 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1408 bytes 136853 (136.8 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

2.2

2.6

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 147.102.202.61 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 128716 bytes 55427262 (55.4 MB)
            RX errors 0 dropped 9 overruns 0 frame 0
            TX packets 18699 bytes 4619899 (4.6 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

2.5
2.7
2.3

```

### 2.3) Διεύθυνση υποστρώματος MAC της "wlp1s0": 90:78:41:15:16:66

Σημείωση: Για την εκδοχή των net-tools του Linux, η λέξη ether είναι η "hardware class" και η τιμή που ακολουθεί είναι η "hardware address".

### 2.4) Ταχύτητα Σύνδεσης: 866.7 (Mb/s)

Σημείωση: Η παραπάνω τιμή είναι μη ρεαλιστικά μεγάλη. Αποτελεί πιθανόν την ονομαστική τιμή της ταχύτητας και όχι την πραγματική.

```

petrosrapto@petrosraptoAssistant:~$ iwconfig
wlp1s0    IEEE 802.11 ESSID:"ntuax"
          Mode:Managed Frequency:5.32 GHz Access Point: 00:35:1A:E2:7C:AE
          Bit Rate=866.7 Mb/s Tx-Power=17 dBm
          Retry short limit:7 RTS thr:off Fragment thr:off
          Power Management:on
          Link Quality=58/70 Signal level=-52 dBm
          Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
          Tx excessive retries:2 Invalid misc:29 Missed beacon:0

lo        no wireless extensions.

```

### 2.5) Διεύθυνση IPv4 (Wifi) του υπολογιστή (δεκαδικός συμβολισμός): 147.102.202.61

### 2.6) Μάσκα Υποδικτύου: 255.255.252.0

Σε δυαδική αναπαράσταση: 11111111.11111111.11111100.00000000. Γνωρίζουμε ότι για να βρούμε την διεύθυνση του υποδικτύου αρκεί να εκτελέσουμε λογικό "and" μεταξύ της μάσκας υποδικτύου και της διεύθυνσης IP. Άρα:

i) Μέγεθος σε bit του τμήματος δικτύου της διεύθυνσης IPv4 του υπολογιστή: 22

Η IPv4 σε δυαδική αναπαράσταση: \_.\_.\_. 11001010.\_.\_

Τα πρώτα δύο bytes περνάνε. Το τελευταίο byte αποκόπτεται. Τα πρώτα 6 ψηφία του 3ου byte περνάνε ενώ τα υπόλοιπα αποκόπτονται. Συνεπώς έχουμε:

ii) Διεύθυνση Υποδικτύου: 147.102.200.0

### 2.7) Διεύθυνση IPv6 (Wifi) του υπολογιστή: fe80::85f9:b27:bde1:b577

### 2.8) 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 147.102.202.61 metric 600
169.254.0.0/16 dev wlp1s0 scope link metric 1000

```

### 2.9) Διεύθυνση IPv4 του εξυπηρετητή DNS: 147.102.224.243

```

petrosrapto@petrosraptoAssistant:~$ systemd-resolve --status | grep Current
  Current Scopes: DNS
  Current DNS Server: 147.102.224.243

```

Σημείωση: Παρατηρούμε ότι τα αποτελέσματα της Άσκησης 2 έρχονται σε πλήρη συμφωνία με τα αυτά της Άσκησης 1.

**2.10) Διεύθυνση IPv4 του εξυπηρετητή DHCP: 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 147.102.202.61 metric 600
169.254.0.0/16 dev wlp1s0 scope link metric 1000
```

Σημείωση: Παρατηρούμε ότι ταυτίζεται με την διεύθυνση IPv4 του DNS.

**2.11) Εμφανίζεται μήνυμα μη πρόσβασης στα Ethernet frames για την εντολή ethtool.**

```
petrosrapto@petrosraptoAssistant:~$ sudo ethtool --phy-statistics wlp1s0
no stats available
petrosrapto@petrosraptoAssistant:~$ sudo ethtool wlp1s0
Settings for wlp1s0:
      Link detected: yes
petrosrapto@petrosraptoAssistant:~$ sudo ethtool -a wlp1s0
Pause parameters for wlp1s0:
Cannot get device pause settings: Operation not supported
```

**2.12) Αριθμός πακέτων IPv4 που έστειλε/έλαβε η κάρτα δικτύου του υπολογιστή: 3986547/4103689**

```
petrosrapto@petrosraptoAssistant:~$ netstat -s
Ip:
      Forwarding: 2
      4103689 total packets received
        25 with invalid headers
        19782 with invalid addresses
        0 forwarded
        0 incoming packets discarded
      3986547 incoming packets delivered
        1195607 requests sent out
        38 outgoing packets dropped
        1069 dropped because of missing route
        17 fragments dropped after timeout
        207 reassemblies required
        95 packets reassembled ok
        17 packet reassemblies failed
        46 fragments received ok
        92 fragments created
```

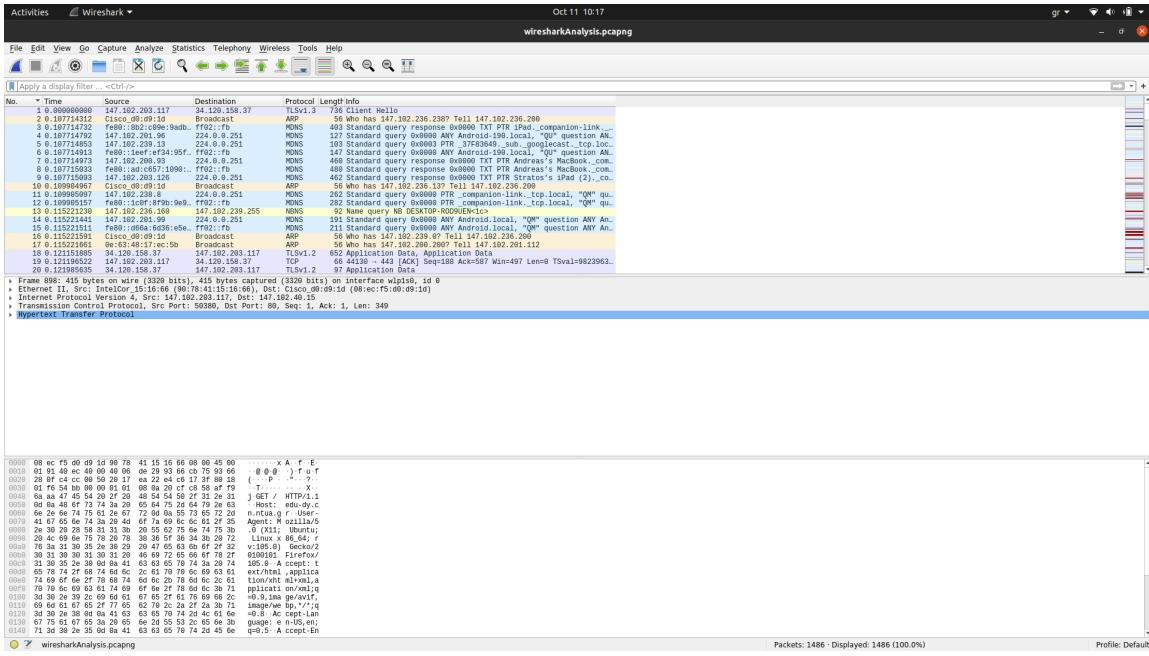
**2.12) Αριθμός established συνδέσεων TCP του υπολογιστή με άλλους υπολογιστές: 20**

```
petrosrapto@petrosraptoAssistant:~$ netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 petrosraptoAssist:48994  eh-in-f188.1e100.:https ESTABLISHED
tcp     0      0 [localhost:52000]           localhost:37109    ESTABLISHED
tcp     0      0 [localhost:37109]           localhost:52000    ESTABLISHED
tcp     0      0 petrosraptoAssist:58586   helios.ntua.gr:https ESTABLISHED
tcp     0      0 localhost:33614            localhost:40017    ESTABLISHED
tcp     0      0 petrosraptoAssist:57898   a104-122-198-127.:https ESTABLISHED
tcp     0      0 localhost:40017            localhost:33614    ESTABLISHED
tcp     0      0 petrosraptoAssist:54298   lb-140-82-113-25:https ESTABLISHED
tcp     0      0 petrosraptoAssist:42516   162.159.136.234:https ESTABLISHED
tcp     0      0 petrosraptoAssist:57872   a104-122-198-127.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:38042   249.195.120.34.bc:https ESTABLISHED
tcp     0      0 petrosraptoAssist:39732   stackoverflow.com:https ESTABLISHED
tcp     0      0 petrosraptoAssist:57932   a104-122-198-127.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:56232   146.75.0.65:https    ESTABLISHED
tcp     0      0 petrosraptoAssist:57886   a104-122-198-127.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:57916   a104-122-198-127.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:36912   ec2-3-65-102-105.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:35324   57.26.190.35.bc.g:https ESTABLISHED
tcp     0      0 petrosraptoAssist:57908   a104-122-198-127.:https ESTABLISHED
tcp     0      0 petrosraptoAssist:32882   146.75.1.51:https    ESTABLISHED
```

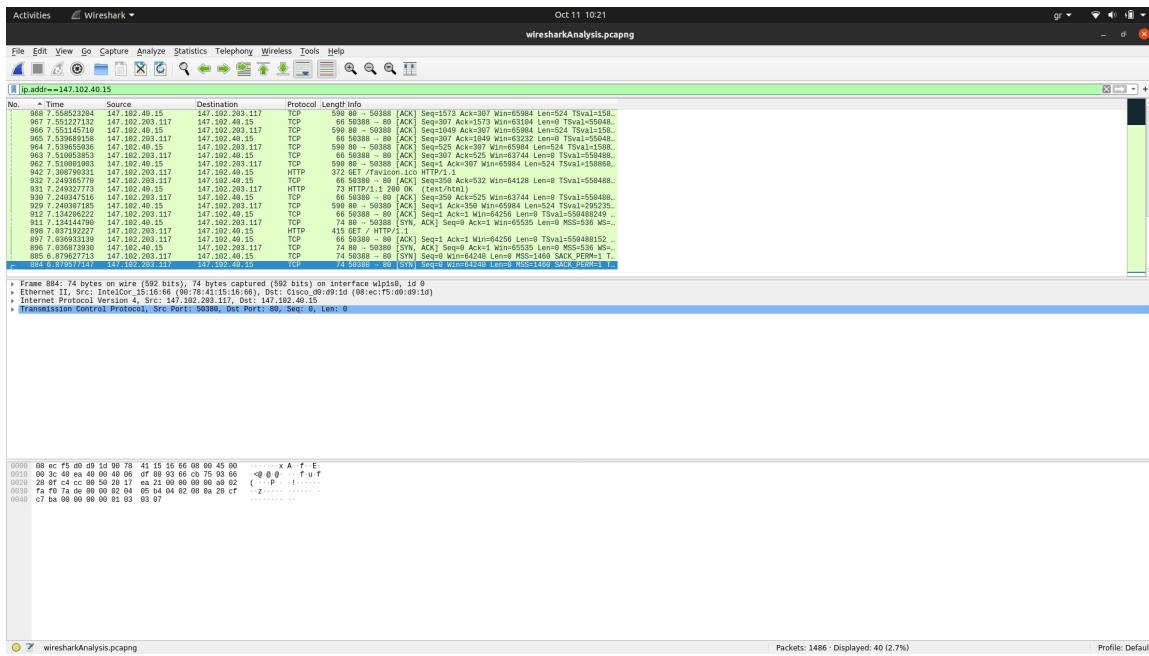
**2.12) Για δύο από τις παραπάνω συνδέσεις TCP, θύρες πηγής/προορισμού: 37109/52000, 52000/37109**

# Άσκηση 3

Ανοίγουμε έναν φυλλομετρητή, εκκαθαρίζουμε την cache και ξεκινάμε καταγραφή στο Wireshark για την διεπαφή κάρτας δικτύου του υπολογιστή μας με την οποία συνδέομαστε στο διαδίκτυο. Επισκεπτόμαστε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/> και σταματάμε την καταγραφή μόλις φορτώσει πλήρως. Έχουμε:



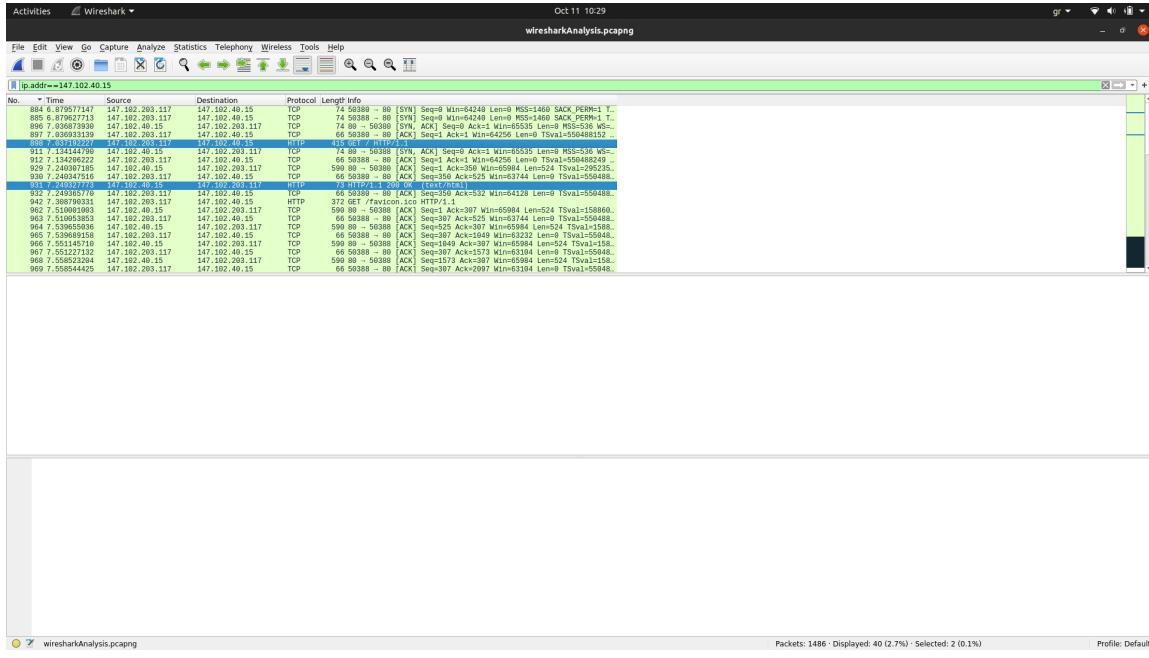
Απομονώνουμε τα πακέτα που ανταλλάχθηκαν μόνο με την ιστοσελίδα που μας ενδιαφέρει εφαρμόζοντας φίλτρο απεικόνισης (ip.addr==147.102.40.15). Έχουμε:



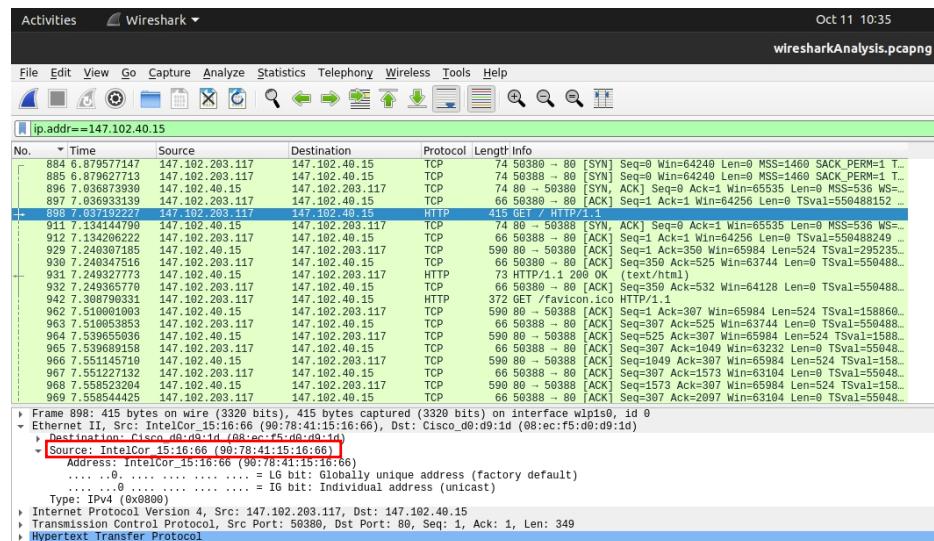
Καταγράφουμε τα διαφορετικά πρωτόκολλα που εμφανίζονται στη λίστα. Άρα:

## 3.1) Πρωτόκολλα: TCP, HTTP

Ταξινομούμε τα πλαίσια με αύξουσα σειρά και εντοπίζουμε το πρώτο μήνυμα HTTP με την εντολή GET που έστειλε ο υπολογιστής μας για να κατεβάσει την σελίδα καθώς και την αντίστοιχη απόκριση 200 OK του εξυπηρετητή:



Η διεύθυνση MAC του υπολογιστή μας απεικονίζεται παρακάτω. Άρα:



### 3.2) Διεύθυνση MAC υπολογιστή (σε δεκαεξαδική μορφή): 90:78:41:15:16:66

Παρατηρούμε ότι έρχεται σε συμφωνία με τα αποτελέσματα των προηγούμενων ασκήσεων.

Σύμφωνα με τις σημειώσεις της Ι<sup>ης</sup> Εργαστηριακής Ασκησης:

Στο Ethernet κάθε δικτύου διαθέτει μία μοναδική φυσική διεύθυνση, αυτήν την υποστρώματος MAC.

Το πρώτο bit ορίζει αν η διεύθυνση είναι Ομαδική ή Ατομική.

Το δεύτερο bit ορίζει αν η διεύθυνση είναι τοπική ή παγκόσμια.

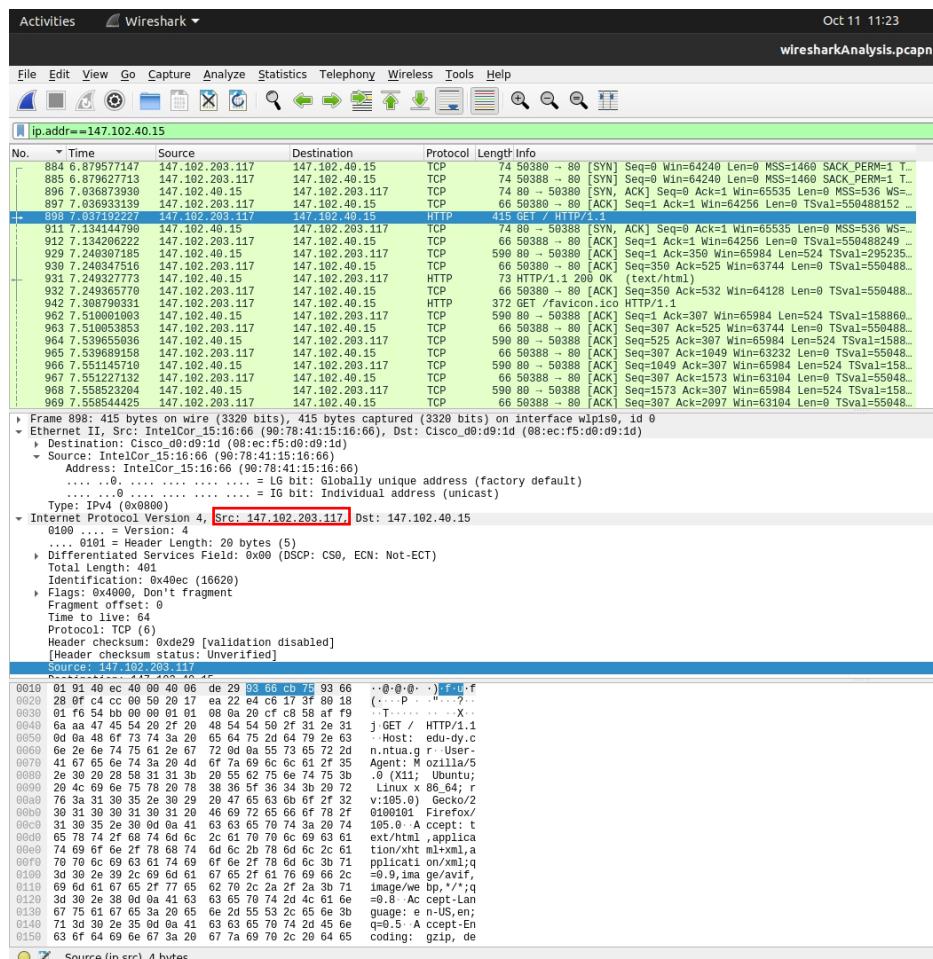
Τα επόμενα 22 bit της διεύθυνσης προσδιορίζουν τον κατασκευαστή της κάρτας.

Τα τελευταία 24 bit είναι ο αύξων αριθμός της κάρτας.

Συνεπώς, μπορούμε να προσδιορίζουμε τον κατασκευαστή της κάρτας δικτύου από την διεύθυνση MAC:

### 3.3) Κατασκευαστής κάρτας δικτύου: Intel

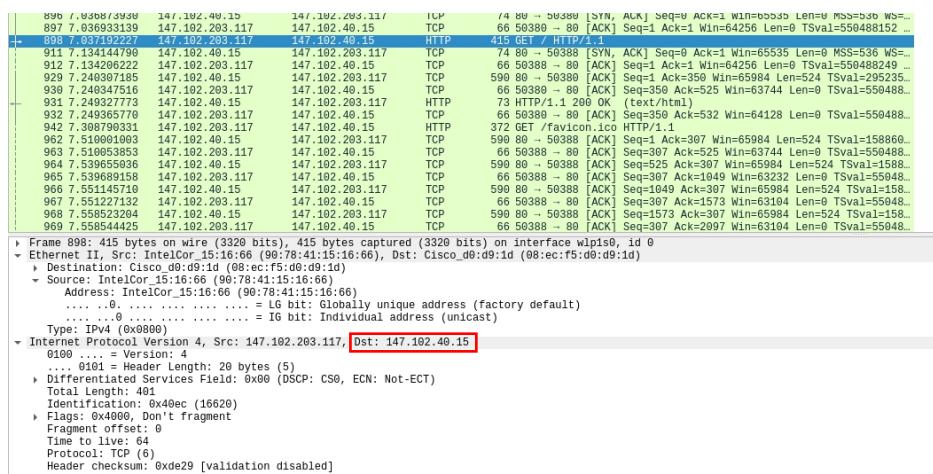
Για να βρούμε τη διεύθυνση IPv4 του υπολογιστή μας, αρκεί να παρατηρήσουμε το source IPv4 στο πακέτο GET.



### 3.4) Διεύθυνση IPv4 του υπολογιστή: 147.102.203.117

Σημείωση: Παρατηρούμε ότι διαφέρει από το IPv4 των Ασκήσεων 1,2. Γνωρίζουμε ότι ο DHCP server έχει την "δικαιοδοσία" να αλλάζει το κομμάτι Host του IPv4 χωρίς ωστόσο να μεταβάλλει την διεύθυνση υποδικτύου του. Παρατηρούμε λοιπόν στην παραπάνω IPv4 διεύθυνση ότι η διεύθυνση υποδικτύου έχει παραμείνει η ίδια, ενώ το κομμάτι του Host έχει αλλάξει.

Για να βρούμε τη διεύθυνση IPv4 του <http://edu-dy.cn.ntua.gr/>, αρκεί να παρατηρήσουμε το destination IPv4 στο πακέτο GET.



### 3.5) Διεύθυνση IPv4 του <http://edu-dy.cn.ntua.gr/>: 147.102.40.15

Τοποθετούμε τον δείκτη στο πρώτο πλαίσιο που περιέχει τεμάχιο TCP. Πατάμε δεξί κλικ -> Follow -> TCP Stream.

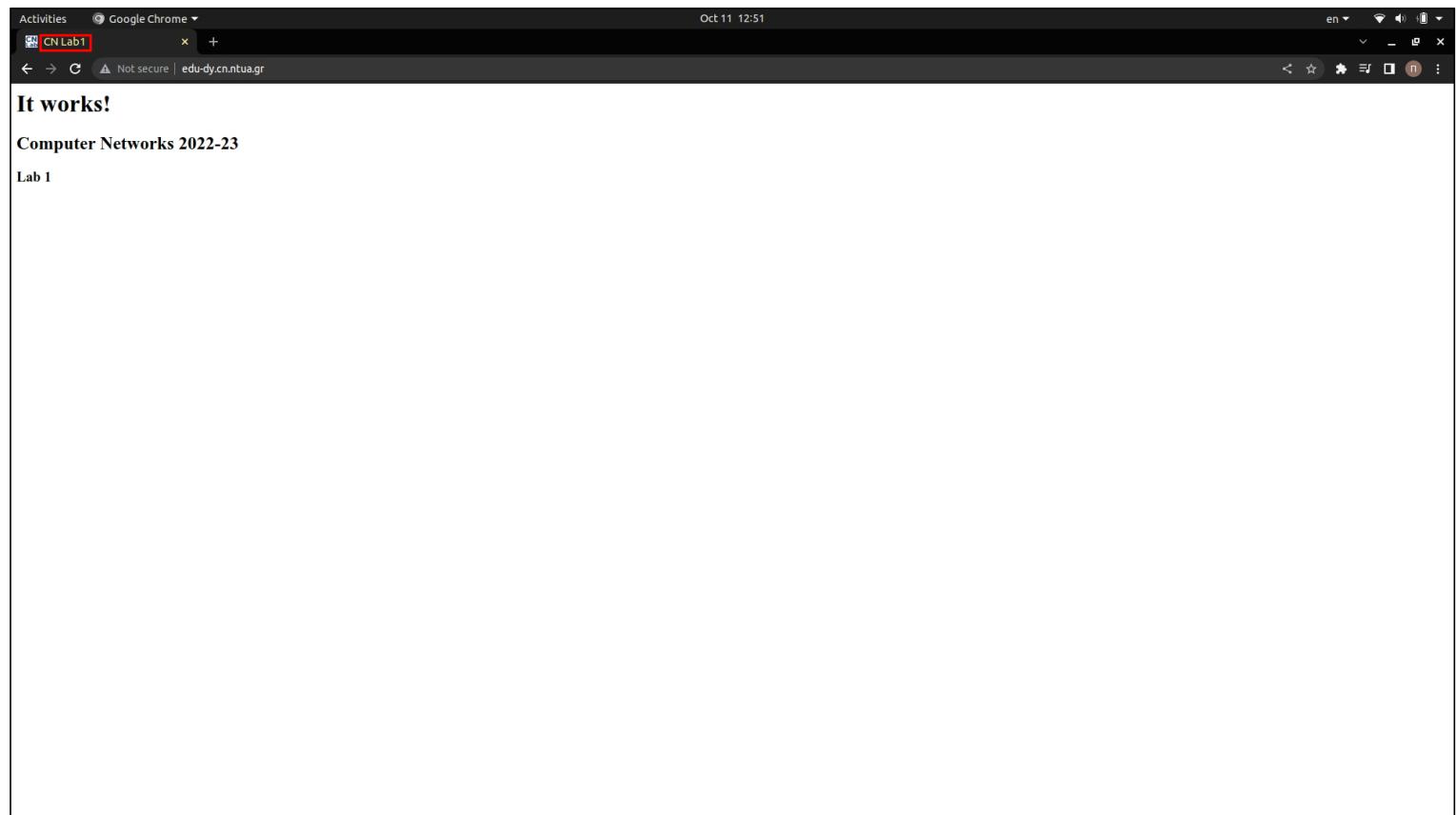
### 3.6) Σύνταξη φίλτρου που εμφανίζεται στο φίλτρο απεικόνισης: **tcp.stream eq 43**

Ακόμη έχουμε:

```
GET / HTTP/1.1
Host: edu-dy.cn.ntua.gr
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 06 Oct 2022 15:55:09 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Thu, 06 Oct 2022 12:46:53 GMT
ETag: "172914-9c-5ea5d16724940"
Accept-Ranges: bytes
Content-Length: 156
Cache-Control: max-age=84600, public
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
  <head>
    <title>CN Lab</title>
  </head>
  <body>
    <h1>It works!</h1>
    <h2>Computer Networks 2022-23</h2>
    <h3>Lab1</h3>
  </body>
</html>
```



### 3.7) i) Τύπος εξυπηρετητή ιστού που φιλοξενεί τη σελίδα: **Apache/2.2.22**

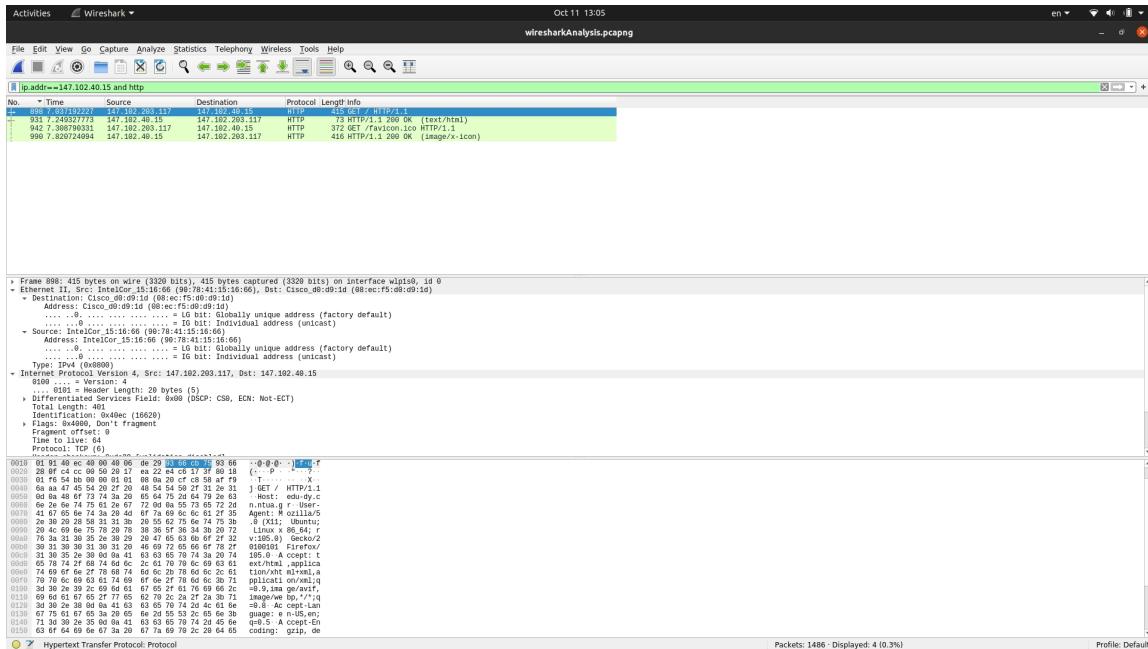
ii) Τίτλος (και HTML tag) της σελίδας: **<title>CN Lab</title>**

iii) Σημείο του παραθύρου που εμφανίζεται ο τίτλος: **Πάνω αριστερά στην καρτέλα**

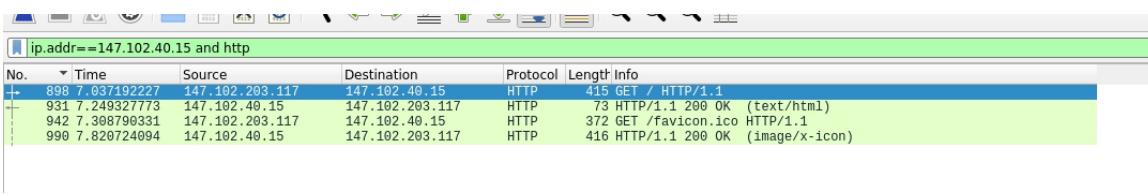
Για να εμφανίσουμε μόνο τα μηνύματα HTTP εφαρμόζουμε κατάλληλο φίλτρο με την κάτωθι σύνταξη.

### 3.8) Σύνταξη Φίλτρου: **ip.addr==147.102.40.15 and http**

Έχουμε:

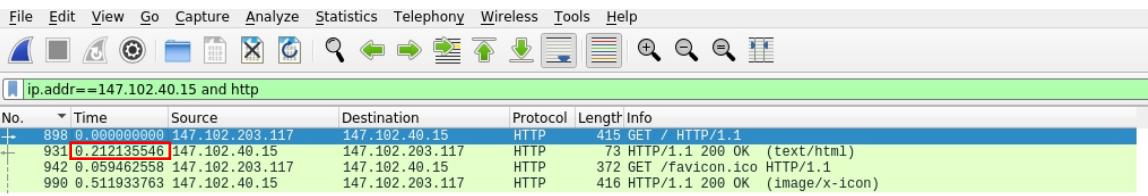


Για να δούμε αν ένα πακέτο στάλθηκε ή παραδόθηκε κοιτάμε τα πεδία Source/Destination ώστε να τα αντιστοιχήσουμε στα IP του υπολογιστή μας είτε στο IP της ιστοσελίδας. Άρα:



### 3.9) Στάλθηκαν 2 / Δήθηκαν 2 μηνύματα HTTP.

Από το μενού View επιλέγουμε Time Display Format και Seconds Since Previous Displayed Packet:



### 3.10) Χρόνος που πέρασε: ≈0.2121 (seconds)

Επιλέγουμε το ληφθέν πακέτο που αφορά τη μεταφορά της εικόνας και έχουμε:

**3.11) Αριθμός πακέτων για την ολοκλήρωση της μετάδοσης: 8**

Αύξοντες αριθμούς πακέτων:

**962, 964, 966, 968, 971, 983, 985, 990**

Στη δεύτερη εικόνα, στην άκρη της παραθύρου, θα δείτε την πληροφορία για την παραδοσης της εικόνας:

No.	Time	Source	Destination	Protocol	Length: Info
898	0.000000000	147.102.203.117	147.102.40.15	HTTP	415 GET / HTTP/1.1
931	0.212135546	147.102.40.15	147.102.203.117	HTTP	73 HTTP/1.1 200 OK (text/html)
942	0.059462558	147.102.203.117	147.102.40.15	HTTP	372 GET /favicon.ico HTTP/1.1
990	0.511933763	147.102.40.15	147.102.203.117	HTTP	416 HTTP/1.1 200 OK (image/x-icon)

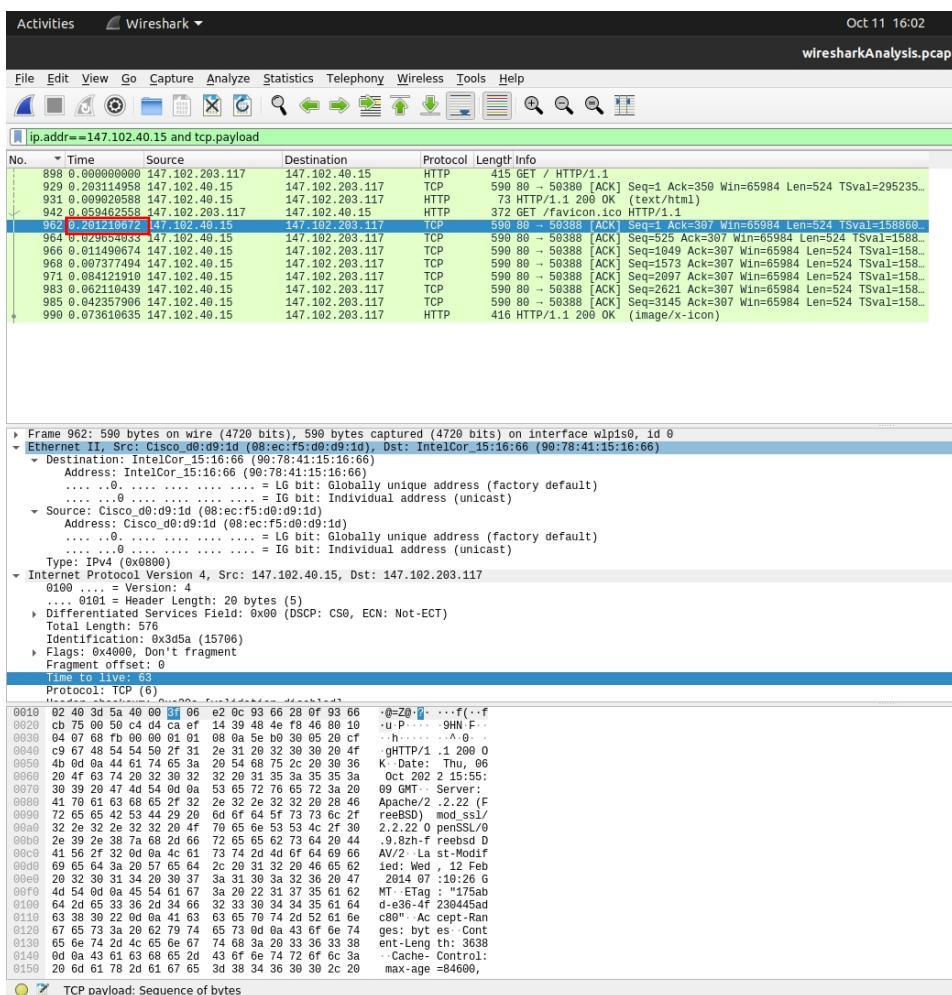
Πληροφορίες για την παραδοσης της εικόνας:

- Time to live: 63
- Protocol: TCP (6)
- Header checksum: 0xe2b3 [validation disabled]
- [Header checksum status: Unverified]
- Source: 147.102.40.15
- Destination: 147.102.203.117
- Transmission Control Protocol, Src Port: 80, Dst Port: 50388, Seq: 3669, Ack: 307, Len: 350
- Reassembled TCP Segments (4018 bytes): #962(524), #964(524), #966(524), #968(524), #971(524), #983(524), #985(524), #990(350)
- Frame: 962, payload: 0-523 (524 bytes)
- Frame: 964, payload: 524-1047 (524 bytes)
- Frame: 966, payload: 1048-1571 (524 bytes)
- Frame: 968, payload: 1572-2095 (524 bytes)
- Frame: 971, payload: 2096-2619 (524 bytes)
- Frame: 983, payload: 2620-3143 (524 bytes)
- Frame: 985, payload: 3144-3667 (524 bytes)
- Frame: 990, payload: 3668-4017 (350 bytes)
- Segment count: 81
- [Reassembled TCP length: 4018]
- [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...]

Πληροφορίες για την παραδοσης της εικόνας:

- HyperText Transfer Protocol
- Media Type

Με εφαρμογή κατάλληλου φίλτρου εμφανίζουμε μόνο τεμάχια TCP:

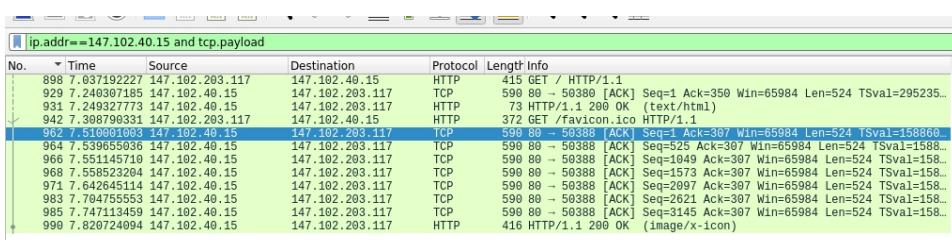


### 3.12) Σύνταξη: ip.addr==147.102.40.15 and tcp.payload

Στην παραπάνω εικόνα έχουμε “Seconds Since Previous Displayed Packet”. Συνεπώς:

3.13) Χρόνος που πέρασε μέχρι να ληφθεί το πρώτο πακέτο (τεμάχιο TCP) της μετάδοσης για το κατέβασμα της εικόνας: **≈0.201210672 (seconds)**

Αλλάζουμε σε “Seconds Since Beginning of Capture” και έχουμε:



Αφαιρούμε τους αντίστοιχους χρόνους για να βρούμε τα ζητούμενα.

3.13) Χρόνος που πέρασε από τη στιγμή που έγινε λήψη του πρώτου πακέτου μέχρι την μετάδοση και των υπόλοιπων: **7.820724094 - 7.510001003 ≈0.310723091 (seconds)**

3.13) Χρόνος για να ολοκληρωθεί η απόκριση στο αίτημα GET: **0.201210672 + 0.310723091 ≈0.511933763 (seconds)**

Για το GET της εικόνας αναπτύσσουμε την γραμμή TRANSUM RTE στο παράθυρο με τις λεπτομέρειες:

No.	Time	Source	Destination	Protocol	Length	Info
898	7.037192227	147.102.203.117	147.102.40.15	HTTP	415	GET / HTTP/1.1
929	7.240307185	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=1 Ack=350 Win=65984 Len=524 TSval=295235...
931	7.249327773	147.102.40.15	147.102.203.117	HTTP	73	HTTP/1.1 200 OK (text/html)
942	7.308790331	147.102.203.117	147.102.40.15	HTTP	372	GET /favicon.ico HTTP/1.1
962	7.5100801003	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=1 Ack=307 Win=65984 Len=524 TSval=158860...
964	7.539655036	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=525 Ack=307 Win=65984 Len=524 TSval=1588...
966	7.551145716	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=1049 Ack=307 Win=65984 Len=524 TSval=158...
968	7.558523204	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=1573 Ack=307 Win=65984 Len=524 TSval=158...
971	7.642645114	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=2097 Ack=307 Win=65984 Len=524 TSval=158...
983	7.704755553	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=2621 Ack=307 Win=65984 Len=524 TSval=158...
985	7.747113459	147.102.40.15	147.102.203.117	TCP	590	80 - 50388 [ACK] Seq=3145 Ack=307 Win=65984 Len=524 TSval=158...
990	7.820724094	147.102.40.15	147.102.203.117	HTTP	416	HTTP/1.1 200 OK (image/x-icon)

Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xfd5c [validation disabled]
[Header checksum status: Unverified]
Source: 147.102.203.117
Destination: 147.102.40.15
Transmission Control Protocol, Src Port: 50388, Dst Port: 80, Seq: 1, Ack: 1, Len: 306
Hypertext Transfer Protocol
TRANSMISSION CONTROL PROTOCOL
[RTE Status: OK]
[Req First Seg: 942]
[Req Last Seg: 942]
[Rsp First Seg: 962]
[Rsp Last Seg: 990]
[APDU Rsp Time: 0.511933763 seconds]
[Service Time: 0.201210672 seconds]
[Req Spread: 0.000000000 seconds]
[Rsp Spread: 0.310723091 seconds]
[Trace clip filter: tcp.stream==44 && frame.number>=942 && frame.number<=990 && tcp.len>0]
[Calculation: Generic TCP]

Συγκρίνουμε τους χρόνους Service Time, Rsp Spread και APSU Rsp Time με αυτούς που βρήκαμε προηγουμένως.

### 3.14) Οι χρόνοι που προέκυψαν μέσω ανάλυσης του wireshark ταυτίζονται με αυτούς που είχαμε καταγράψει.

Με την εφαρμογή κατάλληλου φίλτρου βλέπουμε μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής μας:

No.	Time	Source	Destination	Protocol	Length	Info
898	7.037192227	147.102.203.117	147.102.40.15	HTTP	415	GET / HTTP/1.1
942	7.308790331	147.102.203.117	147.102.40.15	HTTP	372	GET /favicon.ico HTTP/1.1

Frame 898: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface wlp1s0, id 0

Ethernet II, Src: Cisco\_d0:d9:1d (08:ec:f5:d0:d9:1d), Dst: Cisco\_d0:d9:1d (08:ec:f5:d0:d9:1d)

Address: Cisco\_d0:d9:1d (08:ec:f5:d0:d9:1d) = L6 bit: Globally unique address (factory default)

Address: Cisco\_d0:d9:1d (08:ec:f5:d0:d9:1d) = L6 bit: Individual address (unicast)

Source: IntelCor\_15:16:66 (90:78:41:15:16:66)

Address: IntelCor\_15:16:66 (90:78:41:15:16:66) = L6 bit: Globally unique address (factory default)

Address: IntelCor\_15:16:66 (90:78:41:15:16:66) = L6 bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 147.102.203.117, 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: 491

Identification: 0x40ec (16620)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

0010 01 91 40 ec 40 00 46 06 de 29 93 66 cb 75 93 66 ..@.0.0.0..f.u.f

0029 28 0f cc 00 50 20 17 ee 22 e4 c6 17 3f 81 18 (... P ..-.?.

0039 01 f6 54 bb 00 99 01 00 08 20 c8 c8 58 af f9 .GET ..-.X.

0049 00 00 45 50 2f 20 50 50 50 50 50 50 j:GET /HTTP/1.1

0059 0d 0e 48 74 03 74 03 60 65 64 75 64 64 26 63 Host: www.dude4c.com

0069 6e 2e 66 74 75 61 2e 67 72 0d 0e 55 73 65 72 2d n.ntua.gr r User-Agent: Mozilla/5

0079 41 67 65 66 74 28 28 4d 6f 7a 69 6c 6c 61 2f 35 .0 (X11; Ubuntu;

0089 2e 30 28 28 58 31 31 3b 29 55 62 75 6e 74 75 3b Linux x86\_64; r

0099 20 4c 69 66 75 78 20 28 38 36 5f 36 34 3b 29 72 v:105.0) Gecko/2

00a9 76 3a 31 30 35 2e 30 0d 0a 41 63 63 65 75 74 3a 29 74 0100101 Firefox/

00b9 31 30 35 2e 30 0d 0a 41 63 63 65 75 74 3a 29 74 105.0- A ccept: t

00c9 65 78 74 2f 68 74 6d 6c 2b 78 6d 6c 2b 61 ext/html,application/xht,ml+xml,1,a

00d9 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2b 61 tion/xht,ml+xml,1,a

00e9 70 39 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 30 71 plication/xml;q

00f9 63 60 36 69 66 65 62 75 6e 74 75 3b 2d 60 36 69 66 65 62 75 6e 74 75 3b 71

0109 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 image/w ebp;v/1.0;q

0129 3d 30 28 38 0d 0a 41 63 63 65 75 74 2d 4c 61 6e =0.8 Accept-Lan

0139 67 75 61 67 65 3a 20 65 6d 2d 55 53 2c 65 6e 3b quage: en-US,en;

0149 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.5- A ccept-En

0159 63 6f 64 69 66 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip,

### 3.15) Σύνταξη: ip.src==147.102.203.117 and http