ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ
ΑΜ: 031 18 014
ΕΞΑΜΗΝΟ: 7ο
MAC ADDRESS: B4-69-21-1B-6C-FF
IPv4: Άσκ1: 147.102.238.161, Άσκ2: 10.3.20.33, Άσκ3: 10.3.20.20
ΌΝΟΜΑ ΥΠΟΛΟΓΙΣΤΗ: LAPTOP-B2DVAJKK
ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ: WINDOWS 10

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 1: ΑΝΑΛΥΤΗΣ ΠΡΩΤΟΚΟΛΛΩΝ WIRESHARK

Για την άσκηση 1 χρησιμοποιήθηκε το δίκτυο ntuax

Άσκηση 1: Βρείτε την κάρτα δικτύου: (δίκτυο: ntuax)

Για να βρούμε τις ζητούμενες πληροφορίες, πατάμε το Windows Key, το οποίο και μας παραπέμπει στη γραμμή αναζήτησής του. Εκεί πληκτρολογούμε “Ρυθμίσεις” και από το μενού που μας εμφανίζει επιλέγουμε “Δίκτυο και Ίντερνετ”. Αφού το πατήσουμε, βρισκόμαστε σε νεό μενού και όντας στην επιλογή “Κατάσταση” επιλέγουμε “Αλλαγή επιλογών προσαρμογέα”. Εκεί βρίσκουμε τον προσαρμογέα ο οποίος είναι ενεργοποιημένος και συνδεδεμένος στο Ίντερνετ. Αφού τον διπλοκλικάρουμε, μάς εμφανίζει ένα παραθυράκι, το οποίο έχει κάποιες βασικές πληροφορίες όπως η ταχύτητα, ενώ για να αντλήσουμε και τις υπόλοιπες, επιλέγουμε “Λεπτομέρειες”. Εκεί βρίσκουμε τα κάτωθι:

1.1) Όνομα προσαρμογέα: **Intel(R) Dual Band Wireless-AC 8265**

1.2) Από το εικονίδιο του προσαρμογέα, εύκολα συμπεραίνουμε πως πρόκειται για **ασύρματη σύνδεση Wi-Fi**:

1.3) Ταχύτητα σύνδεσης: **9Mbit/s**

1.4) MAC διεύθυνση: **B4-69-21-1B-6C-FF**

1.5) Διεύθυνση IPv4: **147.102.238.161**

1.6) Διεύθυνση IPv6: **2001:648:2000:e9:2d24:e1a9:4d62:714a**

1.7) Διακομιστές DNS IPv4: **147.102.224.243**
Διακομιστές DNS IPv6: **2001:648:2000:2000::1**

1.8) Προεπιλεγμένη Πύλη IPv4: **147.102.236.200**
Προεπιλεγμένη Πύλη IPv6: **fe80::aec:f5ff:fed0:d91d**

Για την άσκηση 2 χρησιμοποιήθηκε το δίκτυο eduroam

Άσκηση 2: Ρυθμίσεις και στατιστικά: (δίκτυο: eduroam)

2.1) Χρησιμοποιούμε την εντολή **“ipconfig/all”** και βρίσκουμε Όνομα Υπολογιστή (Host Name): **LAPTOP-B2DVAJKK**.

2.2) Εισάγουμε την εντολή:
“wmic nic get AdapterType, Name, Name, Installed, MACAddress” οπότε και παίρνουμε τα εξής αποτελέσματα (εντός κόκκινου πλαισίου τα ονόματα των καρτών δικτύου):

```
C:\Users\Άλεξ>wmic nic get AdapterType, Name, Installed, MACAddress
AdapterType     Installed  MACAddress         Name
                TRUE                          Microsoft Kernel Debug Network Adapter
Ethernet 802.3  TRUE       00:FF:BA:25:E7:2C  TAP-Windows Adapter V9
Ethernet 802.3  TRUE       B4:69:21:1B:6C:FF  Intel(R) Dual Band Wireless-AC 8265
Ethernet 802.3  TRUE       04:92:26:6F:F2:29  Realtek PCIe GbE Family Controller
Ethernet 802.3  TRUE       B4:69:21:1B:6D:03  Bluetooth Device (Personal Area Network)
Ethernet 802.3  TRUE       B4:69:21:1B:6C:00  Microsoft Wi-Fi Direct Virtual Adapter #4
                TRUE                          WAN Miniport (SSTP)
                TRUE                          WAN Miniport (IKEv2)
                TRUE                          WAN Miniport (L2TP)
                TRUE                          WAN Miniport (PPTP)
                TRUE                          WAN Miniport (PPPOE)
Ethernet 802.3  TRUE       EE:C1:20:52:41:53  WAN Miniport (IP)
Ethernet 802.3  TRUE       F2:2C:20:52:41:53  WAN Miniport (IPv6)
Ethernet 802.3  TRUE       F4:8E:20:52:41:53  WAN Miniport (Network Monitor)
Ethernet 802.3  TRUE       B6:69:21:1B:6C:FF  Microsoft Wi-Fi Direct Virtual Adapter #5
Ethernet 802.3  TRUE       0A:00:27:00:00:14  VirtualBox Host-Only Ethernet Adapter
```

2.3) Με την εντολή “**ipconfig/all**”, βρίσκουμε και επαληθεύουμε πως η MAC διεύθυνση της κάρτας δικτύου που χρησιμοποιούμε για την ασύρματη σύνδεση στο διαδίκτυο είναι: **B4-69-21-1B-6C-FF**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : B4-69-21-1B-6C-FF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:648:2d00:1020:2d24:e1a9:4d62:714a(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:648:2d00:1020:79db:3713:65b5:136e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2d24:e1a9:4d62:714a%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.3.20.33(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : Παρασκευή, 15 Οκτωβρίου 2021 9:03:25 πμ
   Lease Expires . . . . . . . . . . : Παρασκευή, 15 Οκτωβρίου 2021 1:09:37 μμ
   Default Gateway . . . . . . . . . : fe80::6d5:90ff:feda:67b0%18
                                       10.3.20.1
   DHCP Server . . . . . . . . . . . : 10.3.20.1
   DHCPv6 IAID . . . . . . . . . . . : 213149985
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-6D-6F-4D-04-92-26-6F-F2-29
   DNS Servers . . . . . . . . . . . : 62.217.126.164
                                       194.177.210.210
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2.4) Με την εντολή **“netsh wlan show interface”**, βρίσκουμε ταχύτητα λήψης και μετάδοσης ίση με **243Mbps**, όπως και φαίνεται παρακάτω:

```
C:\Users\Αλεξ>netsh wlan show interface

There is 1 interface on the system:

    Name                   : Wi-Fi
    Description            : Intel(R) Dual Band Wireless-AC 8265
    GUID                   : 94774a54-2827-44a9-8928-281187ac5c04
    Physical address       : b4:69:21:1b:6c:ff
    State                  : connected
    SSID                   : eduroam
    BSSID                  : 5c:e8:83:37:c1:f0
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 132
    Receive rate (Mbps)    : 243
    Transmit rate (Mbps)   : 243
    Signal                 : 78%
    Profile                : eduroam

    Hosted network status  : Not available
```

2.5) Χρησιμοποιούμε την εντολή **“ipconfig”**: και βρίσκουμε, για τον adapter ασύρματου δικτύου που χρησιμοποιούμε, IPv4 διεύθυνση την εξής: **10.3.20.33 .**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:648:2d00:1020:2d24:e1a9:4d62:714a
   Temporary IPv6 Address. . . . . . : 2001:648:2d00:1020:a5d9:7b03:cfc2:1977
   Link-local IPv6 Address . . . . . : fe80::2d24:e1a9:4d62:714a%18
   IPv4 Address. . . . . . . . . . . : 10.3.20.33
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::6d5:90ff:feda:67b0%18
                                       10.3.20.1
```

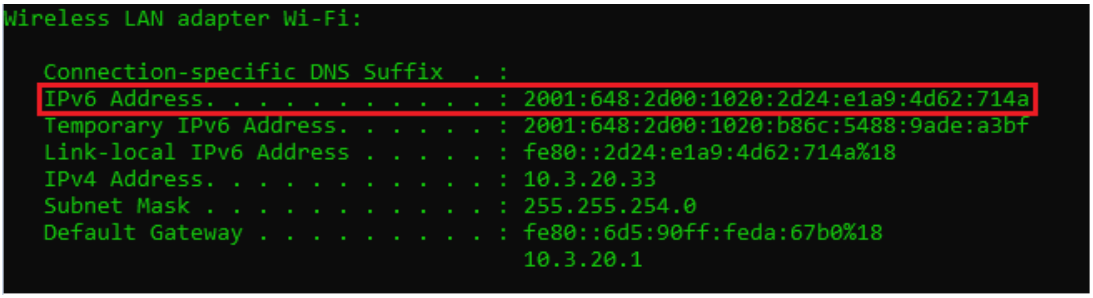
2.6) Με την ίδια εντολή **“ipconfig”**, βρίσκουμε τη μάσκα υποδικτύου: **255.255.254.0**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:648:2d00:1020:2d24:e1a9:4d62:714a
   Temporary IPv6 Address. . . . . . : 2001:648:2d00:1020:81d5:8440:adc8:aa9d
   Link-local IPv6 Address . . . . . : fe80::2d24:e1a9:4d62:714a%18
   IPv4 Address. . . . . . . . . . . : 10.3.20.33
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::6d5:90ff:feda:67b0%18
                                       10.3.20.1
```

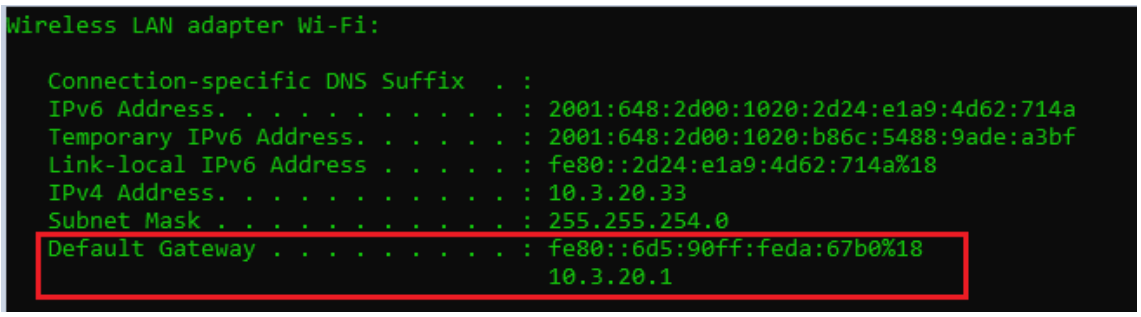
i) Η μάσκα δικτύου 255.255.254.0, γράφεται σε δυαδική μορφή ως 11111111.11111111.11111110.00000000, οπότε το μέγεθος του τμήματος δικτύου είναι τα πρώτα **23 bits**.

ii) Η διεύθυνση του υποδικτύου είναι αυτή που προκύπτει από το λογικό AND μεταξύ των αριθμών 00001010.00000011.00010100.00100001 (IPv4 διεύθυνση σε δυαδική μορφή) και 11111111.11111111.11111110.00000000 (subnet mask σε δυαδική μορφή). Επομένως, η διεύθυνση του υποδικτύου είναι: 00001010.00000011.00010100.00000000 ή αλλιώς **10.3.20.0** .

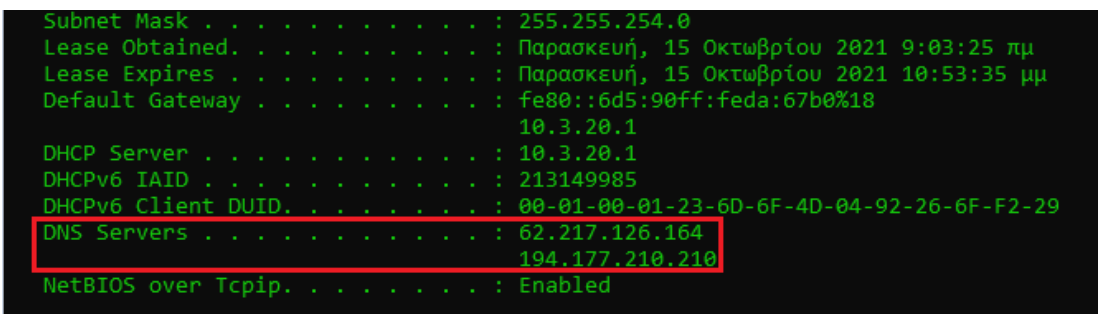
2.7) Με την εντολή **“ipconfig”**, βρίσκουμε την IPv6 διεύθυνση: **2001:648:2d00:1020:2d24:e1a9:4d62:714a .**



2.8) Με την ίδια εντολή, από το παραπάνω στιγμιότυπο βρίσκουμε τις διευθύνσεις IPv4, IPv6 της προκαθορισμένης πύλης, ίσες με **10.3.20.1** και **fe80::6d5:90ff:feda:67b0** αντίστοιχα.



2.9) Ξανά, με **“ipconfig/all”**, βρίσκουμε την IPv4 DNS διεύθυνση (δε διατίθεται η αντίστοιχη IPv6), η οποία είναι: **62.217.126.164 (η primary) / 194.177.210.210 (η secondary)**, όπως φαίνεται παρακάτω (στις πληροφορίες του ενεργού adapter):



2.10) Βρίσκουμε με την εντολή **“ipconfig/all”**, DCHP IPv4 την εξής: **10.3.20.1 .** Επαληθεύουμε ότι πρόκειται για ίδια τιμή με την IPv4 του default getaway (router)

```
IPv4 Address. . . . . . . . . . . : 10.3.20.33(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.254.0
Lease Obtained. . . . . . . . . . : Παρασκευή, 15 Οκτωβρίου 2021 9:03:25 πμ
Lease Expires . . . . . . . . . . : Παρασκευή, 15 Οκτωβρίου 2021 10:53:35 μμ
Default Gateway . . . . . . . . . : fe80::6d5:90ff:feda:67b0%18
                                    10.3.20.1
DHCP Server . . . . . . . . . . . : 10.3.20.1
DHCPv6 IAID . . . . . . . . . . . : 213149985
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-6D-6F-4D-04-92-26-6F-F2-29
DNS Servers . . . . . . . . . . . : 62.217.126.164
                                    194.177.210.210
NetBIOS over Tcpip. . . . . . . . : Enabled
```

2.11) Με την εντολή **“netstat -e”**, αντλούμε τις ζητούμενες πληροφορίες:

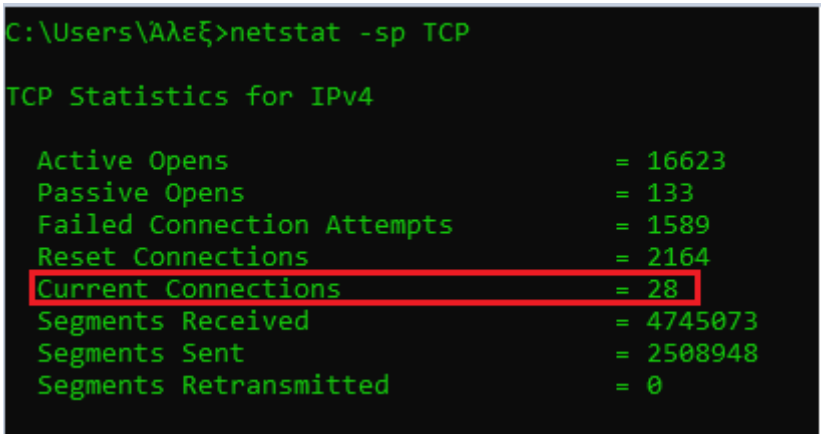
```
C:\Users\Άλεξ>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     391657729      1473601037
Unicast packets            34440476        24943199
Non-unicast packets           36440          316252
Discards                          0               0
Errors                            0               5
Unknown protocols                 0
```

Αναφορικά με τη διάκριση των πακέτων σε Unicast και Non-Unicast, τα μεν αφορούν πακέτα τα οποία στάλθηκαν/ελήφθησαν άμεσα από την κάρτα δικτύου, ενώ τα δε αφορούν Broadcast/Multicast πακέτα τα οποία “μάζεψε” η κάρτα δικτύου μας αλλά δε προοριζόταν άμεσα για αυτήν.

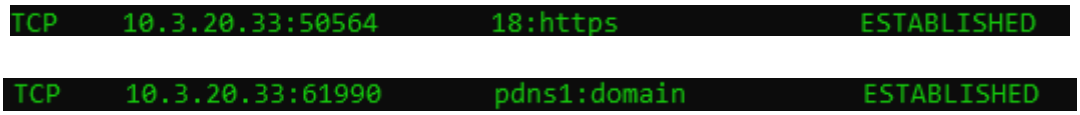
2.12) Για τα πακέτα IPv4 που έστειλε/έλαβε η κάρτα δικτύου του υπολογιστή μας, εισάγουμε την εντολή **“netstat -s -p IP”**, όπου το -s μας δείχνει στατιστικά ανά πρωτόκολλο, ενώ το -p prototype δείχνει τις συνδέσεις για το συγκεκριμένο πρωτόκολλο. Επομένως, δίνοντας ως όρισμα IP (το οποίο είναι το IPv4), αντλούμε τα παρακάτω στοιχεία:

```
C:\Users\Άλεξ>netstat -s -p IP

IPv4 Statistics

  Packets Received                   = 6636541
  Received Header Errors             = 0
  Received Address Errors            = 99
  Datagrams Forwarded                = 676663
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 292553
  Received Packets Delivered         = 8086709
  Output Requests                    = 5682438
  Routing Discards                   = 0
  Discarded Output Packets           = 3691
  Output Packet No Route             = 137
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

2.13) Με την εντολή **“netstat -s -p TCP”**, παίρνουμε 28 TCP συνδέσεις του υπολογιστή μας συνολικά. Για να βρούμε τις established που δεν είναι στον ίδιο μας τον υπολογιστή, ανατρέχουμε στη λίστα των αποτελεσμάτων, η οποία εμφανίζεται κάτω από τα περιεχόμενα της ακόλουθης φωτογραφίας και βρίσκουμε όσες είναι established και δεν έχουν ως πηγή και προορισμό την IP διεύθυνση 127.0.0.1. Μετρώνται ίσες με **5 συνδέσεις**. (εκτελέστηκε στην πραγματικότητα η εντολή **netstat -s -n -p TCP** προκειμένου να έχουμε numeric format των διευθύνσεων και να διευκολυνθεί η καταμέτρηση, αλλά παρουσιάζονται τα αποτελέσματα της netstat -sp TCP)



2.14) Επιλέγουμε 2 τυχαίες συνδέσεις: (με την ίδια εντολή του βήματος 2.13)



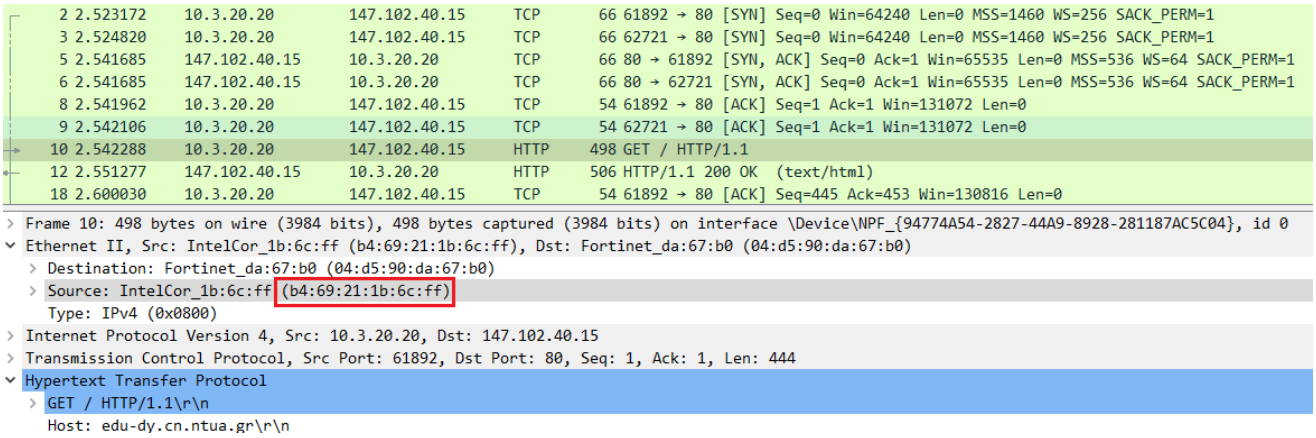
Προφανώς, οι θύρες πηγής είναι **50564** και **61990** αντίστοιχα, ενώ οι θύρες προορισμού είναι οι **80** και **53** αντίστοιχα (αντιστοιχούν στο https και στο domain κατά σειρά).

Για την άσκηση 3 χρησιμοποιήθηκε το δίκτυο eduroam, ανατέθηκε, ωστόσο διαφορετική IP από τον DHCP, καθώς πλέον έχουμε την 10.3.20.20 αντί της 10.3.20.33

Άσκηση 3: Αναλυτής πρωτοκόλλων Wireshark: (δίκτυο: eduroam)

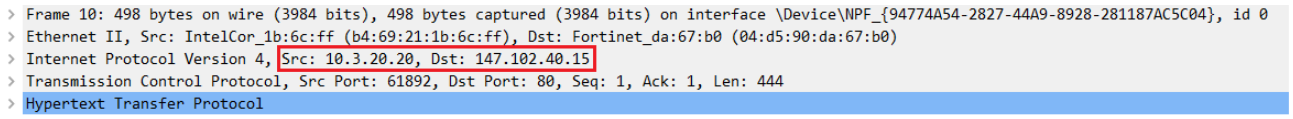
3.1) Τα διάφορα πρωτόκολλα που εμφανίζονται είναι: **UDP, TLSv1.3, TLSv1.2, TLSv1, TCP, HTTP, DNS**

3.2) Για να βρούμε τη MAC διεύθυνση του υπολογιστή μας, ανατρέχουμε στο υπ' αριθμόν frame 10 (το πρώτο κατά σειρά με πρωτόκολλο HTTP), και στις πληροφορίες του, πηγαίνουμε στο βελάκι με την ένδειξη Ethernet II (το οποίο αποτελεί το Layer 2, οπότε αναμένουμε να βρούμε εκεί τη MAC address). Πατώντας το ">" βλέπουμε στις αναλυτικές πληροφορίες τη ζητούμενη διεύθυνση στη γραμμή του Source: **b4:69:21:1b:6c:ff** .



3.3) Στην παραπάνω εικόνα, διακρίνουμε ξανά στο τμήμα του Source, τον κατασκευαστή: **IntelCor**.

3.4, 3.5) Εφόσον, θέλουμε τις IPv4 διευθύνσεις, ανατρέχουμε στο Internet Protocol Version 4 (Layer 3), όπου και βρίσκουμε τις εξής διευθύνσεις: **10.3.20.20** και **147.102.40.15** για την πηγή και τον προορισμό αντίστοιχα, όπως φαίνεται παρακάτω:



3.6) Παρατηρούμε πως πλέον το φίλτρο που εμφανίζεται είναι το **"tcp.stream eq 0"**.

3.7) Από τα αποτελέσματα που παίρνουμε για τις αποκρίσεις του εξυπηρετητή ιστού, βρίσκουμε:

i. Τύπος του εξυπηρετητή της σελίδας που επισκεφτήκαμε: **Apache/2.2.22(FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8.zh-freebsd DAV/2**

```
HTTP/1.1 200 OK
Date: Fri, 15 Oct 2021 14:57:00 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Fri, 08 Oct 2021 20:53:36 GMT
ETag: "172914-73-5cddd92af9400"
Accept-Ranges: bytes
Content-Length: 115
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

ii. Ο τίτλος της σελίδας είναι **“DY2021 CN Lab”**, ενώ το αντίστοιχο HTML tag **<head><title>DY2021 CN Lab </title> < head>**.

```
HTTP/1.1 200 OK
Date: Fri, 15 Oct 2021 14:57:00 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Fri, 08 Oct 2021 20:53:36 GMT
ETag: "172914-73-5cddd92af9400"
Accept-Ranges: bytes
Content-Length: 115
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><title>DY2021 CN Lab</title></head>
<body><h1>It works!</h1><h2>Lab1</h2><h3>2021-2</h3></body></html>
```

iii. Εμφανίζεται ως τίτλος της καρτέλας του φυλλομετρητή:

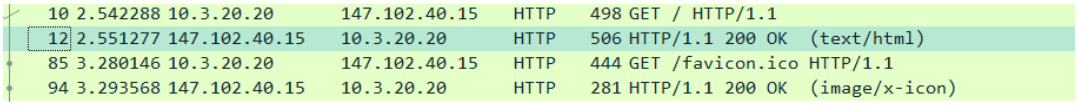
3.8) Το κατάλληλο φίλτρο είναι το: **ip.addr==147.102.40.15 and http** .

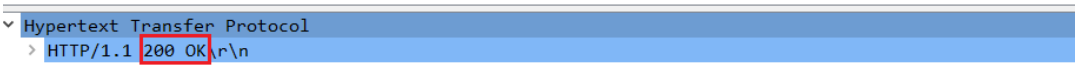
3.9) Παρατηρούμε πως στείλαμε 2 HTTP μηνύματα και λάβαμε επίσης 2:
(2 φορές ως Source και 2 φορές ως Destination η IP μας)

ip.addr==147.102.40.15 and http

No.	Time	Source	Destination	Protocol	Length	Info
10	2.542288	10.3.20.20	147.102.40.15	HTTP	498	GET / HTTP/1.1
12	2.551277	147.102.40.15	10.3.20.20	HTTP	506	HTTP/1.1 200 OK (text/html)
85	3.280146	10.3.20.20	147.102.40.15	HTTP	444	GET /favicon.ico HTTP/1.1
94	3.293568	147.102.40.15	10.3.20.20	HTTP	281	HTTP/1.1 200 OK (image/x-icon)

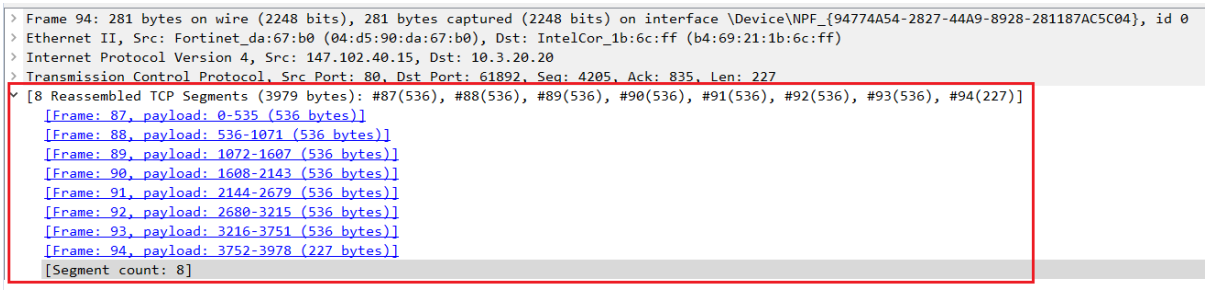
3.10) Στις πληροφορίες του πακέτου 10 και συγκεκριμένα στο Label Hypertext Transfer Protocol (ανώτατο Layer), βρίσκουμε το εξής **“[Response in frame: 12]”**. Δεδομένου ότι το πακέτο 10 είναι το πρώτο που έστειλε το σήμα GET, το πακέτο 12 είναι αυτό που έχει την απόκριση 200 OK, όπως και εύκολα επαληθεύουμε πατώντας επάνω του:



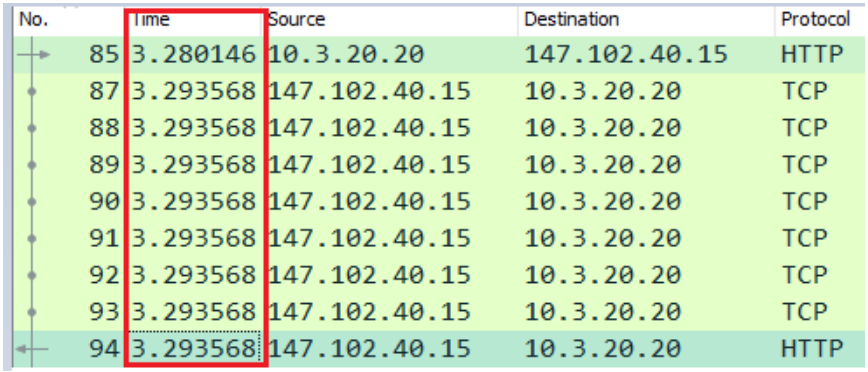


Για να βρούμε επομένως τη χρονική διαφορά από όταν στάλθηκε το πρώτο αίτημα GET μέχρι να ληφθεί η πρώτη απόκριση 200 OK, αρκεί να αφαιρέσουμε από τον χρόνο που πιάστηκε για πρώτη φορά το πακέτο 12, αυτόν του πακέτου 10, άρα ο ζητούμενος χρόνος είναι: 2.551277 – 2.542288 = **0.008989sec**.

3.11) Αντλώντας πληροφορίες από το frame 94, δηλαδή την απόκριση της σελίδας στο αίτημά μας για την εικόνα favicon.ico, βρίσκουμε ότι χρειάστηκαν **8 πακέτα**.

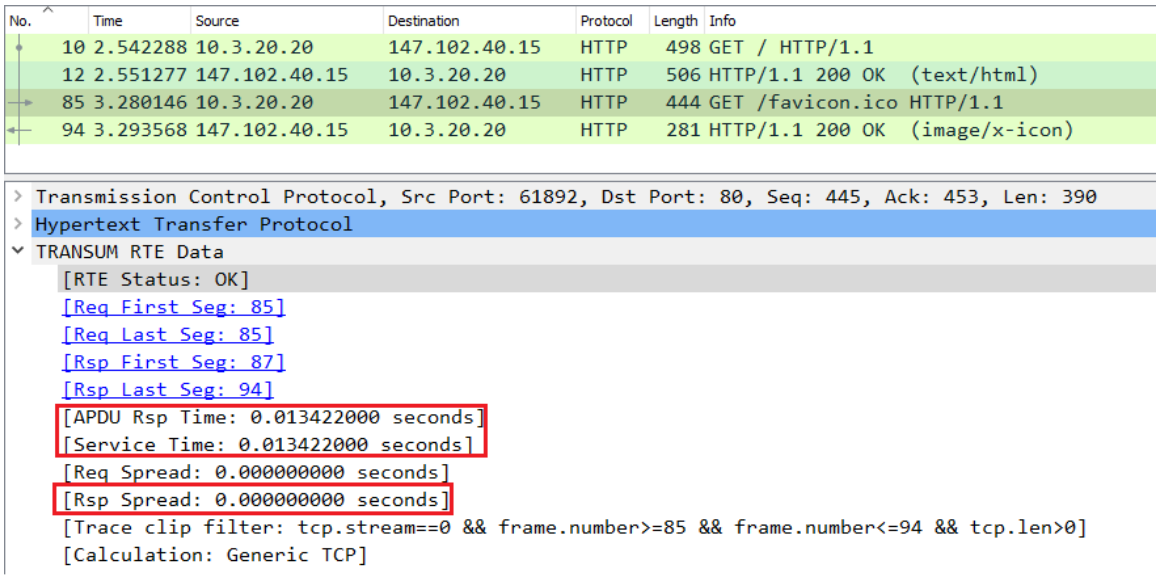


3.12) Στο προηγούμενο ερώτημα είδαμε πως η απάντηση-εικόνα εμπεριέχεται στα frames 87-94, επομένως θα δούμε τους απαραίτητους χρόνους για να απαντήσουμε τα ερωτήματα. Ο χρόνος που πέρασε μέχρι να ληφθεί το πρώτο εξ αυτών, θα υπολογιστεί ως εξής: Από την αρχή του χρόνου, το αίτημα GET για την εικόνα, έγινε στο frame 85, δηλαδή τη στιγμή 3.280146sec, ενώ επίσης βλέπουμε πως το frame 87 ήρθε από τον σέρβερ σε μας τη χρονική στιγμή 3.293568, άρα ο **χρόνος που πέρασε μέχρι να ληφθεί το πρώτο εξ αυτών** είναι 3.293568-3.280146 = **0.013422sec**. Ο χρόνος που πέρασε από την προηγούμενη στιγμή (3.293568sec) μέχρι να ολοκληρωθεί η μετάδοση των άλλων πακέτων είναι **μηδενικός**, ενώ ο χρόνος που πέρασε για την ολοκλήρωση της απόκρισης στο αίτημα GET ταυτίζεται με τον χρόνο που χρειάστηκε προκειμένου να μεταδοθεί το πρώτο πακέτο, δηλαδή **0.013422sec**.



Δηλαδή όλα τα frames που αποτελούν την εικόνα “πιάστηκαν” την ίδια χρονική στιγμή.

3.13) Αντλώντας τα παραπάνω δεδομένα από την ανάλυση του Wireshark, επαληθεύουμε όσα βρήκαμε παραπάνω:



3.14) Για να δούμε τα HTTP μηνύματα που έστειλε ο υπολογιστής μας, εισάγουμε ως φίλτρο την εξής έκφραση: “**ip.src==10.3.20.20 and http”**, όπου 10.3.20.20 η IP μας.