**Ονοματεπώνυμο:** Χαράλαμπος Καμπουγέρης

**Ομάδα:** 3, Τετάρτη 10:45-12:30, Αιθ.Α2

**Όνομα PC/ΛΣ:** CHARALAMPOSs-MacBook-Air/ macOS 14.0

**Ημερομηνία:** 11/10/2023

**Διεύθυνση IP:** 147.102.237.77

**Διεύθυνση MAC:** 0c:e4:41:e1:6c:74

# Εργαστηριακή Άσκηση 1<br>Αναλυτής Πρωτοκόλλων Wireshark

## Άσκηση 1

**1.1** Όλες οι εργαστηριακές ασκήσεις γίνονται σε Mac με unified SoC Apple M1 με αποτέλεσμα να μην φαίνεται ξεχωριστά η κάρτα δικτύου.

**1.2** Wi-Fi

**1.3** 300 Mbps (πατώντας option+click στο wifi εικονίδιο στο menu bar).

**1.4** 0c:e4:41:e1:6c:74 (About this Mac -> System Report -> Network -> Active Services -> Wi-Fi -> MAC address)

**1.5** 147.102.237.77 (About this Mac -> System Report -> Network -> Active Services -> Wi-Fi -> IPv4 -> Addresses)

**1.6** H IPv6 καθορίζεται αυτόματα και σε αυτήν την περίπτωση το macOS δεν την δείχνει.

**1.7** 147.102.224.243 (About this Mac -> System Report -> Network -> Active Services -> Wi-Fi -> DNS -> Server Addresses)

**1.8** 147.102.236.200 (About this Mac -> System Report -> Network -> Active Services -> Wi-Fi  -> DHCP Server Addresses -> Routers)

## Άσκηση 2

**2.1** CHARALAMPOSs–MacBook–Air/ macOS

**2.2** en0

**2.3** 0c:e4:41:e1:6c:74 (ifconfig)

**2.4** Μέσω της εντολής speedQuality βρίσκουμε τις ταχύτητες upload και download:

```
Uplink capacity: 22.145 Mbps
Downlink capacity: 260.386 Mbps
```

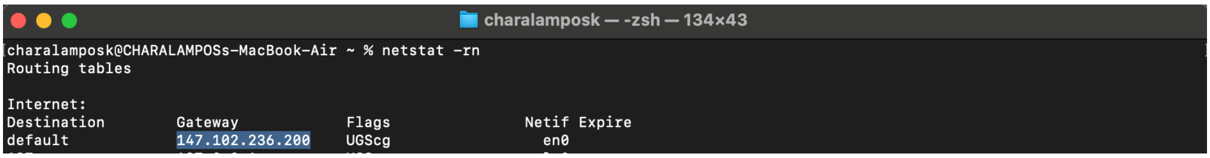
**2.5** IPv4 address: 147.102.239.190

**2.6** i) Subnet Mask: 0xff ff fc 00

ii) Διεύθυνση υποδικτύου: 147.102.236.0 (εφαρμόζουμε τη μάσκα δικτύου πάνω στη διεύθυνση IPv4)

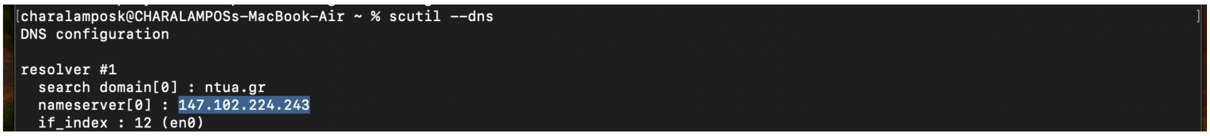
**2.7** IPv6 address: `fe80::cfe:ba7d:4e97:c0c9`

**2.8** `147.102.236.200`



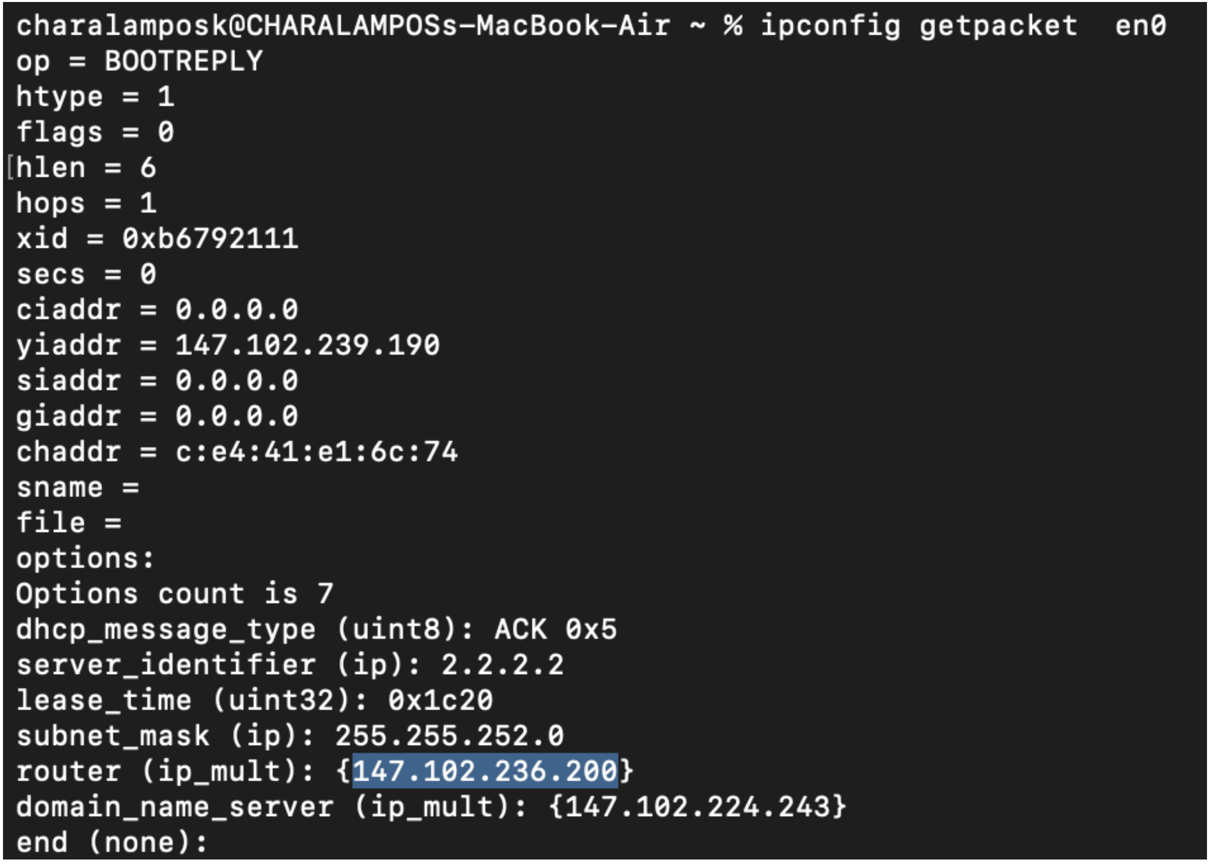
```
charalamposk@CHARALAMPOSs-MacBook-Air ~ % netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags               Netif Expire
default            147.102.236.200    UGScg                 en0
```

**2.9** `147.102.224.243 (scutil --dns)`



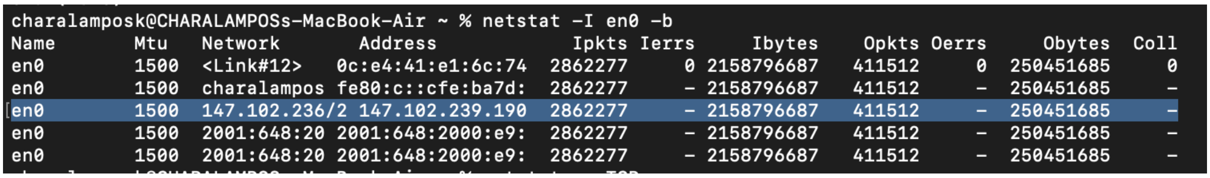
```
charalamposk@CHARALAMPOSs-MacBook-Air ~ % scutil --dns
DNS configuration

resolver #1
  search domain[0] : ntua.gr
  nameserver[0] : 147.102.224.243
  if_index : 12 (en0)
```

**2.10** `147.102.224.243.200 (ipconfig getpacket en0)`



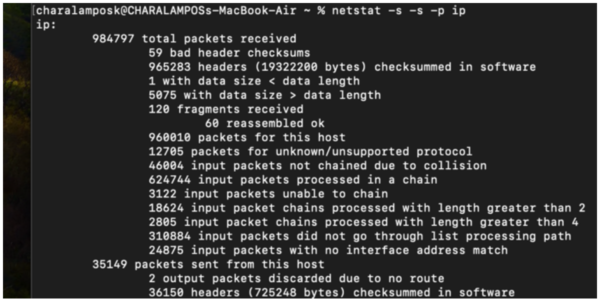
```
charalamposk@CHARALAMPOSs-MacBook-Air ~ % ipconfig getpacket  en0
op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 1
xid = 0xb6792111
secs = 0
ciaddr = 0.0.0.0
yiaddr = 147.102.239.190
siaddr = 0.0.0.0
giaddr = 0.0.0.0
chaddr = c:e4:41:e1:6c:74
sname =
file =
options:
Options count is 7
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 2.2.2.2
lease_time (uint32): 0x1c20
subnet_mask (ip): 255.255.252.0
router (ip_mult): {147.102.236.200}
domain_name_server (ip_mult): {147.102.224.243}
end (none):
```

**2.11** `Incoming:2862277(netstat -I en0 -b)`
`Bytes:2158796687`
`Outcoming:411512`
`Bytes:250451685`



```
charalamposk@CHARALAMPOSs-MacBook-Air ~ % netstat -I en0 -b
Name         Mtu   Network       Address            Ipkts Ierrs     Ibytes    Opkts Oerrs     Obytes  Coll
en0          1500  <Link#12>     0c:e4:41:e1:6c:74  2862277     0 2158796687  411512     0  250451685     0
en0          1500  charalampos fe80::c:cfe:ba7d:   2862277     - 2158796687  411512     -  250451685     -
en0          1500  147.102.236/2 147.102.239.190   2862277     - 2158796687  411512     -  250451685     -
en0          1500  2001:648:20 2001:648:2000:e9:   2862277     - 2158796687  411512     -  250451685     -
en0          1500  2001:648:20 2001:648:2000:e9:   2862277     - 2158796687  411512     -  250451685     -
```

**2.12** 984797 received and 35149 sent (netstat -s -s -p ip)



```
charalamposk@CHARALAMPOSs-MacBook-Air ~ % netstat -s -s -p ip
ip:
        984797 total packets received
                59 bad header checksums
                965283 headers (19322200 bytes) checksummed in software
                1 with data size < data length
                5075 with data size > data length
                120 fragments received
                        60 reassembled ok
                960010 packets for this host
                12705 packets for unknown/unsupported protocol
                46004 input packets not chained due to collision
                624744 input packets processed in a chain
                3122 input packets unable to chain
                18624 input packet chains processed with length greater than 2
                2805 input packet chains processed with length greater than 4
                310884 input packets did not go through list processing path
                24875 input packets with no interface address match
        35149 packets sent from this host
                2 output packets discarded due to no route
                36150 headers (725248 bytes) checksummed in software
```

**2.13** 15 Established connections (10 IPv4, 5 IPv6)

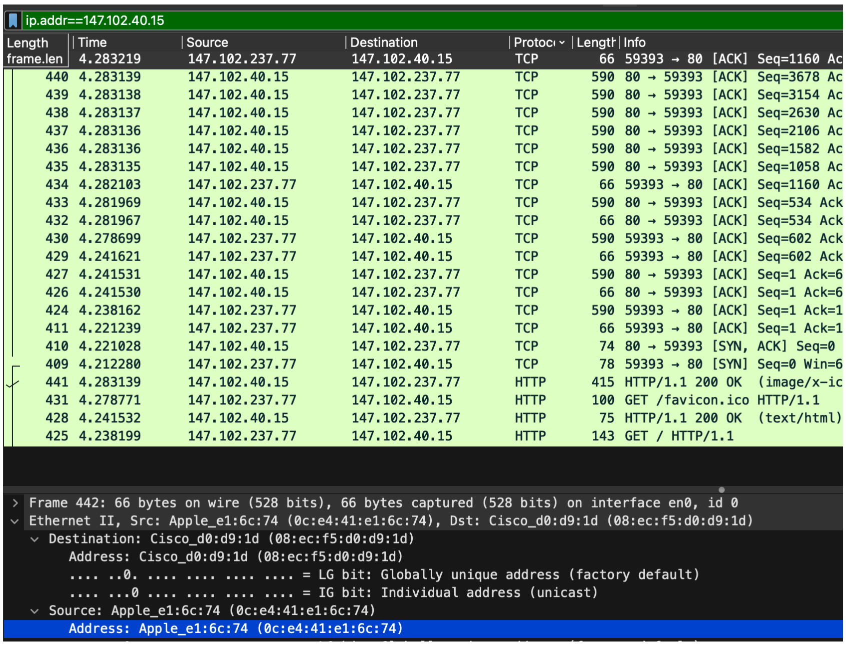
**2.14** Θύρες πηγής(source) και προορισμού (destination):

1) 49484(source), https(destination)
2) 53934(source), 5223(destination)

## Άσκηση 3

**3.1** Εμφανίζονται τα πρωτόκολλα ARP, DNS, HTTP, MDNS, TCP,  TLSv1.2

**3.2** 0c:e4:41:e1:6c:74



ip.addr==147.102.40.15

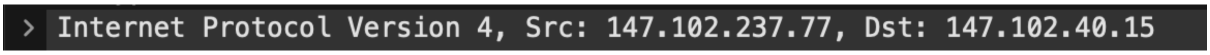
```
Length    | Time     | Source          | Destination     | Protoc | Length | Info
frame.len  4.283219   147.102.237.77    147.102.40.15     TCP        66  59393 → 80 [ACK] Seq=1160 Ac
      440  4.283139   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=3678 Ac
      439  4.283138   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=3154 Ac
      438  4.283137   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=2630 Ac
      437  4.283136   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=2106 Ac
      436  4.283136   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=1582 Ac
      435  4.283135   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=1058 Ac
      434  4.282103   147.102.237.77    147.102.40.15     TCP        66  59393 → 80 [ACK] Seq=1160 Ac
      433  4.281969   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=534 Ack
      432  4.281967   147.102.40.15     147.102.237.77    TCP        66  80 → 59393 [ACK] Seq=534 Ack
      430  4.278699   147.102.237.77    147.102.40.15     TCP       590  59393 → 80 [ACK] Seq=602 Ack
      429  4.241621   147.102.237.77    147.102.40.15     TCP        66  59393 → 80 [ACK] Seq=602 Ack
      427  4.241531   147.102.40.15     147.102.237.77    TCP       590  80 → 59393 [ACK] Seq=1 Ack=6
      426  4.241530   147.102.40.15     147.102.237.77    TCP        66  80 → 59393 [ACK] Seq=1 Ack=6
      424  4.238162   147.102.237.77    147.102.40.15     TCP       590  59393 → 80 [ACK] Seq=1 Ack=1
      411  4.221239   147.102.237.77    147.102.40.15     TCP        66  59393 → 80 [ACK] Seq=1 Ack=1
      410  4.221028   147.102.40.15     147.102.237.77    TCP        74  80 → 59393 [SYN, ACK] Seq=0
      409  4.212280   147.102.237.77    147.102.40.15     TCP        78  59393 → 80 [SYN] Seq=0 Win=6
      441  4.283139   147.102.40.15     147.102.237.77    HTTP      415  HTTP/1.1 200 OK  (image/x-ic
      431  4.278771   147.102.237.77    147.102.40.15     HTTP      100  GET /favicon.ico HTTP/1.1
      428  4.241532   147.102.40.15     147.102.237.77    HTTP       75  HTTP/1.1 200 OK  (text/html)
      425  4.238199   147.102.237.77    147.102.40.15     HTTP      143  GET / HTTP/1.1
```

```
> Frame 442: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
v Ethernet II, Src: Apple_e1:6c:74 (0c:e4:41:e1:6c:74), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
  v Destination: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
      Address: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Apple_e1:6c:74 (0c:e4:41:e1:6c:74)
      Address: Apple_e1:6c:74 (0c:e4:41:e1:6c:74)
```

**3.3** Apple (Τα τρία πρώτα bytes που αναγράφονται στη MAC Address)

**3.4** Src: 147.102.237.77

**3.5** Dst: 147.102.40.15



```
> Internet Protocol Version 4, Src: 147.102.237.77, Dst: 147.102.40.15
```

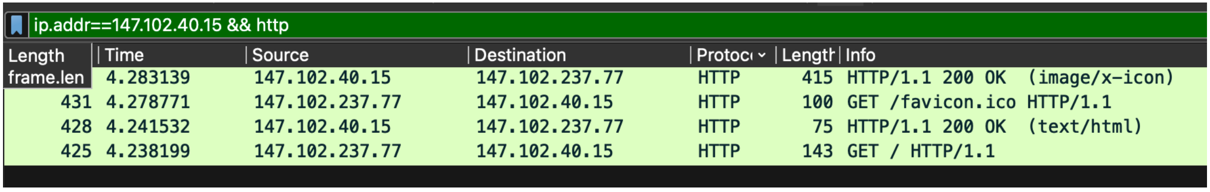
**3.6** tcp.stream eq 4

**3.7** i)Apache/2.2.22 (FreeBSD)

ii) <title>CN Lab1</title>

iii) Εμφανίζεται στον τίτλο της καρτέλας (label του παραθύρου).

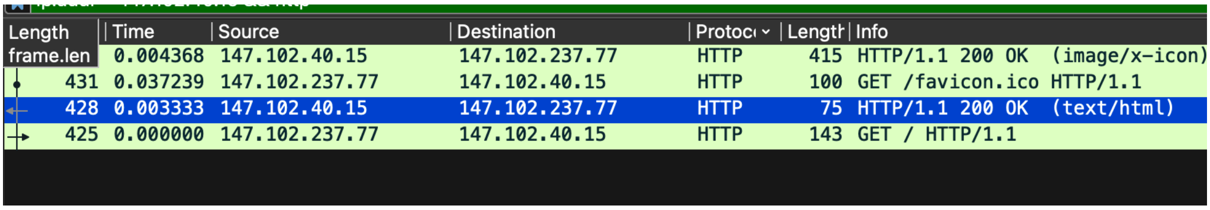
**3.8** ip.addr==147.102.40.15 && http



```
ip.addr==147.102.40.15 && http
Length    | Time      | Source          | Destination      | Protoc | Length | Info
frame.len   4.283139   147.102.40.15     147.102.237.77     HTTP       415  HTTP/1.1 200 OK  (image/x-icon)
      431   4.278771   147.102.237.77    147.102.40.15      HTTP       100  GET /favicon.ico HTTP/1.1
      428   4.241532   147.102.40.15     147.102.237.77     HTTP        75  HTTP/1.1 200 OK  (text/html)
      425   4.238199   147.102.237.77    147.102.40.15      HTTP       143  GET / HTTP/1.1
```

**3.9** Στάλθηκαν 2 (147.102.237.77 -> 147.102.40.15) και λήφθησαν 2 μηνύματα.

**3.10** 0.004368 sec



```
Length    | Time     | Source          | Destination      | Protoc | Length | Info
frame.len  0.004368  147.102.40.15     147.102.237.77     HTTP       415  HTTP/1.1 200 OK  (image/x-icon)
      431  0.037239  147.102.237.77    147.102.40.15      HTTP       100  GET /favicon.ico HTTP/1.1
      428  0.003333  147.102.40.15     147.102.237.77     HTTP        75  HTTP/1.1 200 OK  (text/html)
      425  0.000000  147.102.237.77    147.102.40.15      HTTP       143  GET / HTTP/1.1
```

**3.11** [8 Reassembled TCP Segments (4017 bytes): #433(524), #435(524), #436(524), #437(524), #438(524), #439(524), #440(524), #441(349)]

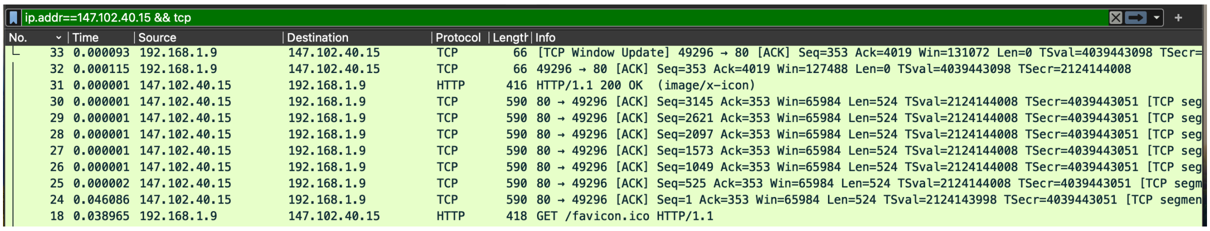
**3.12** ip.addr==147.102.40.15 && tcp && !http

**3.13**

i) Χρόνος για να ληφθεί το πρώτο πακέτο (first TCP Packet – HTTP GET(favicon)): 0.046086

ii)Χρόνος για να ληφθεί το δεύτερο πακέρο (last TCP Packet – first TCP Packet): 0.00000800

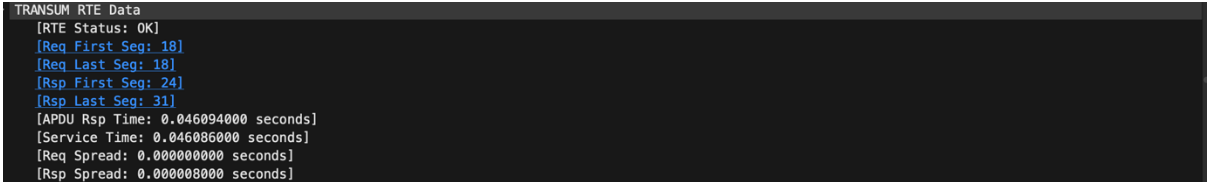
iii) GET to response / Application Response Time: i) + ii) = 0.046094000



```
ip.addr==147.102.40.15 && tcp
No.  | Time     | Source          | Destination     | Protocol | Length | Info
  33  0.000093  192.168.1.9       147.102.40.15     TCP        66  [TCP Window Update] 49296 → 80 [ACK] Seq=353 Ack=4019 Win=131072 Len=0 TSval=4039443098 TSecr=
  32  0.000115  192.168.1.9       147.102.40.15     TCP        66  49296 → 80 [ACK] Seq=353 Ack=4019 Win=127488 Len=0 TSval=4039443098 TSecr=2124144008
  31  0.000001  147.102.40.15     192.168.1.9       HTTP      416  HTTP/1.1 200 OK  (image/x-icon)
  30  0.000001  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=3145 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP seg
  29  0.000001  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=2621 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP seg
  28  0.000001  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=2097 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP seg
  27  0.000001  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=1573 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP seg
  26  0.000001  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=1049 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP seg
  25  0.000002  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=525 Ack=353 Win=65984 Len=524 TSval=2124144008 TSecr=4039443051 [TCP segm
  24  0.046086  147.102.40.15     192.168.1.9       TCP       590  80 → 49296 [ACK] Seq=1 Ack=353 Win=65984 Len=524 TSval=2124143998 TSecr=4039443051 [TCP segmen
  18  0.038965  192.168.1.9       147.102.40.15     HTTP      418  GET /favicon.ico HTTP/1.1
```

**3.14** Παρατηρώ ότι οι χρόνοι Service Time, Response Spread και Application PDU ταυτίζονται με αυτούς που βρήκαμε στο προηγούμενο ερώτημα.

[APDU Rsp Time: 0.046094000 seconds]
    [Service Time: 0.046086000 seconds]
    [Rsp Spread: 0.000008000 seconds]



```
TRANSUM RTE Data
   [RTE Status: OK]
   [Req First Seg: 18]
   [Req Last Seg: 18]
   [Rsp First Seg: 24]
   [Rsp Last Seg: 31]
   [APDU Rsp Time: 0.046094000 seconds]
   [Service Time: 0.046086000 seconds]
   [Req Spread: 0.000000000 seconds]
   [Rsp Spread: 0.000008000 seconds]
```

**3.15** ip.source==147.102.237.77 && http