2η Εργαστηριακή Άσκηση στα "Δίκτυα Υπολογιστών" Κυριάκος Τσαρτσαράκος ΑΜ: 03118054

1. Στρώμα ζεύξης δεδομένων

- 1.1) Με το φίλτρο απεικόνισης arp or ip επιτρέπονται να εισέλθουν στο σύστημα μόνο πακέτα με πρωτόκολλο arp ή ip
- 1.2) Τα ονόματα των πεδίων της επικεφαλίδας του πλαισίου Ethernet είναι τα εξής: Destination, Source, Type

```
Fethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b
Destination: Broadcast (ff:ff:ff:ff:ff)
Source: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
Type: ARP (0x0806)
```

- 1.3) Όχι δεν υπάρχει πεδίο για το συνολικό μήκος του πλαισίου ή των δεδομένων που μεταφέρει
- 1.4) Το μήκος των διευθύνσεων Ethernet είναι ίσο με 6 bytes.
- 1.5) Έχοντας επιλεγμένο το κομμάτι του πλαισίου που αναφέρεται μόνο την επικεφαλίδα του Ethernet, μπορούμε να καταλάβουμε ότι έχει μήκος ισό με 14 bytes

1.6) Το πεδίο Type του πλαισίου Ethernet καθορίζει το πρωτόκολλο δικτύου κάθε φορα π.χ ένα παράδειγμα για το πρωτόκολλο δικτύου ARP

```
    Destination: Broadcast (ff:ff:ff:ff:ff)
    Source: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
    Type: ARP (0x0806)
```

1.7) Το πεδίο Type καταλαμβάνει τα δύο τελευταία bytes της επικεφαλίδας του Ethernet Όπως αποδεικνύεται και από το παρακάτω παράδειγμα:

```
Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlo1, id 0
 Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   Destination: Broadcast (ff:ff:ff:ff:ff)
   > Source: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
     Type: ARP (0x0806
 Address Resolution Protocol (request)
 0000 ff ff ff ff ff 60 e9 3a 0b 0b f3 08 06 00 01
                                                         08 00 06 04 00 01 00 e9
                               3a 0b 0b f3 c0 a8 01 09
                                                         . . . . . . . . . . . . . . . .
 0020 00 00 00 00 00 c0 a8 01 03
1.8) Η τιμή του πεδίου για πακέτα ΙΡν4 είναι η εξής: 0x0800
Frame 244: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0
Ethernet II, Src: 04:71:53:7d:25:80 (04:71:53:7d:25:80), Dst: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
  > Destination: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
  > Source: 04:71:53:7d:25:80 (04:71:53:7d:25:80)
 Internet Protocol Version 4, Src: 35.232.111.17, Dst: 192.168.1.9
> Transmission Control Protocol, Src Port: 80, Dst Port: 55458, Seq: 149, Ack: 88, Len: 0
1.9) Η τιμή του πεδίου για πακέτα ARP είναι η εξής: 0x0806
Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlo1, id 0
Ethernet II, Src: 00:e9:3a:0b:6b:f3 (00:e9:3a:0b:0b:f3), Dst: Broadcast (ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff)
   > Source: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
     Type: ARP (0x0806

    Address Resolution Protocol (request)

     ff ff ff ff ff 00 e9 3a 0b 0b f3 08 06 00 01
                               3a 0b 0b f3 c0 a8 01 09
 0010 08 00 06 04 00 01 00 e9
 0020 00 00 00 00 00 c0 a8 01 03
```

2. Στρώμα Δικτύου

- 2.1) Με την εφαρμογή του φίλτρου απεικόνισης icmp επιτρέπεται μόνο η απεικόνιση των πακέτων με πρωτόκολλο ICMP στο στρώμα δικτύου
- 2.2) Το μήκος των διευθύνσεων IPv4 είναι το εξής: 4 bytes

```
Time to live: 64
   Protocol: ICMP (1)
   Header checksum: 0xd4fa [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.9
   Destination: 1.1.1.1
Internet Control Message Protocol
     04 71 53 7d 25 80 00 e9
                              3a 0b 0b f3 08 00 45 00
                                                        qS}%···
                                                       0010 00 54 a1 fb 40 00 40 01 d4 fa c0 a8 01 09 01 01
0020 01 01 08 00 82 28 00 02
                             00 01 b8 d9 7e 61 00 00
                                                       · · · · · ( · · · · · · ~a · ·
0030 00 00 7c c6 03 00 00 00 00 10 11 12 13 14 15
                                                       1e 1f 20 21 22 23 24 25
                                                       . . . . . . . . . ! "#$%
     16 17 18 19 1a 1b 1c 1d
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                       &'()*+,- ./012345
0060 36 37
```

2.3) Τα δύο πρώτα πεδία της επικεφαλίδας IPv4 είναι τα εξής: Version, Header Length

```
→ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 1.1.1.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
```

2.4) Σύμφωνα με το λινκ που δόθηκε και τα δύο παραπάνω πεδία έχουν μήκος ίσο με 4 bits και οι τιμές τους είναι οι εξής:

Version: 01000b (=4)

Header Length: 0*b*0101 (=5)

2.5) Το συνολικό μήκος της επικεφαλίδας IPv4 είναι ίσο με 20 byte

```
Frame 51: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
Fig. Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: 04:71:53:7d:25:80 (04:71:53:7d:25:80)
Internet Control Message Protocol
      04 71 53 7d 25 80 00 e9
                                3a 0b 0b f3 08 00 45
                                                             qS}%·
       00 54 a1 fb 40 00 40 01
01 01 08 00 82 28 00 02
0020
                                 00 01 b8 d9 7e 61 00 00
0030
      00 00 7c c6 03 00 00 00 00 00 10 11 12 13 14 15
                                                                        ! "#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
                                                                 +, - ./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                            &'()
0060 36 37
```

- 2.6) Γνωρίζοντας ότι η τιμή του αντίστοιχου πεδίου της επικεφαλίδας είναι το Header Length, όπου είναι ίσο με 0b0101 = 5, πολλαπλασιάζοντας επί 4, βρίσκουμε εύκολα το μήκος της επικεφαλίδας, δηλαδή 5*4 = 20 bytes.
- 2.7) Το συνολικό μήκος του πακέτου IPv4 είναι ίσο με 84 bytes, καθώς το μήκος του είναι ίσο με τα συνολικά bytes του πλαισίου (98) μείων τα bytes του της επικεφαλίδας του Ethernet (14), επομένως 98 14 = 84 bytes
- 2.8) Ναι υπάρχει σχετικό πεδίο με το μήκος του πακέτου ΙΡν4 στην επικεφαλίδα του και είναι το εξής:

Είναι το πεδίο που ονομάζεται Total Length και έχει μήκος ίσο με 84 bytes, η οποία σαν τιμή συμφώνει με το αποτέλεσμα στο ερώτημα 2.8

2.9) Το μήκος των δεδομένων του πακέτου IPv4 (payload) είναι ίσο με 64 bytes.

- 2.10) Το μήκος των δεδομένων του πακέτου IPv4 (payload) προκύπτει αν αφαιρέσουμε από το συνολικό μήκος (Total Length) το μήκος της επικεφαλίδας IPv4 (Header Length), επομένως προκύπτει το μήκος των δεδομένων του IPv4, το οποίο είναι ίσο με Total Length Header Length = 84 20 = 64 bytes
- 2.11) Το πεδίο της επικεφαλίδας IPv4 που καθορίζει το πρωτόκολλο στρώματος μεταφοράς της σουίτας TCP/IP είναι το Protocol

```
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xd4fa [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.9
Destination: 1.1.1.1
```

2.12) Βρίσκεται στο δέκατο (10o) byte της επικεφαλίδας, όπως φαίνεται και από τον πίνακα περιεχομένων παρακάτω:

```
ightarrow Frame 51: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: 04:71:53:7d:25:80 (04:71:53:7d:25:80)
                     Version 4. Src:
Internet Control Message Protocol
0000
       04 71 53 7d 25 80 00 e9
                                 3a 0b 0b f3 08 00 45
                                                              as}%···
0010
       00 54 a1 fb 40 00 40 01
01 01 08 00 82 28 00 02
0020
                                 00 01 b8 d9 7e 61 00 00
       00 00 7c c6 03 00 00 00 00 00 10 11 12 13 14 15
0040
      16 17 18 19 1a 1b 1c 1d
                                 1e 1f 20 21 22 23 24 25
                                                                         ! "#$%
0050
      26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                             &'()*+,- ./012345
0060
      36 37
```

```
Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xd4fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.9
    Destination: 1.1.1.1
0000 04 71 53 7d 25 80 00 e9 3a 0b 0b f3 08 00 45 00 0010 00 54 a1 fb 40 00 40 01 d4 fa c0 a8 01 09 01 01
                                                                      ·qs}%··· : · · · · E ·
·T · ·@ ·@<mark>·</mark>
0020 01 01 08 00 82 28 00 02 00 01 b8 d9 7e 61 00 00
                                                                      ················~a··
0030 00 00 7c c6 03 00 00 00 00 10 11 12 13 14 15
                                                                     0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                                      . . . . . . . . ! "#$%
                                                                     &'()*+,- ./012345
0060 36 37
```

2.13) Η τιμή του για το πρωτόκολλο ICMP είναι ίση με 0x01 όπως αποδικνύεται από τον πίνακα περιεχομένων:

```
Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xd4fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.9
   Destination: 1.1.1.1
0000 04 71 53 7d 25 80 00 e9 3a 0b 0b f3 08 00 45 00
                                                                ·qS}%···· : · · · · · E ·
                                                                ·T··@·@·
0010 00 54 a1 fb 40 00 40 <mark>01</mark> d4 fa c0 a8 01 09 01 01
0020 01 01 08 00 82 28 00 02 00 01 b8 d9 7e 61 00 00
                                                                · · · · · ( · · · · · · ~a · ·
0030 00 00 7c c6 03 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                                . . . . . . . . ! "#$%
                                                                &'()*+,- ./012345
0060 36 37
```

3. Στρώμα Μεταφοράς

- 3.1) Επιτρέπει την απεικόνιση πακέτων με πρωτόκολλα TCP, UDP στο στρώμα μεταφοράς
- 3.2) Τα πρωτόκολλα του στρώματος μεταφοράς που παρατηρώ είναι τα εξής: TCP, UDP, TLSv1.2, HTTP, SSDP, DNS, MDNS
- 3.3) Για το πρωτόκολλο TCP η τιμή του πεδίου Protocol είναι ίση με 0x06, όπως αποδεικνύεται

```
Fragment offset: 0
     Time to live: 64
     Protocol: TCP (6)
     Header checksum: 0x2bfb [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.9
     Destination: 147.102.40.15
 Transmission Control Protocol Src Port: 48790 Dst Port: 80 Sec: 0 Len: 0
 0000 04 71 53 7d 25 80 00 e9
                                  3a 0b 0b f3 08 00 45 00
                                                              ·qS}%···· : · · · · · E ·
                                                              ·<··@·@ +·····f
 0010 00 3c 91 9a 40 00 40 06
                                  2b fb c0 a8 01 09 93 66
                                                              ( · · · P? · · · · · · · D
       28 Of be 96 00 50 3f a1
 0020
                                  e5 13 00 00 00 00 a0 02
       fa f0 e3 8f 00 00 02 04
                                  05 b4 04 02 08 0a 44 b9
 0040 c4 03 00 00 00 00 01 03
                                  03 07
Επίσης η τιμή του πεδίου Protocol για το πρωτόκολλο UDP είναι ίση με 0x11
     Total Length: 411
     Identification: 0x280f (10255)
   Flags: 0x4000, Don't fragment
     Fragment offset: 0
     Time to live: 4
     Protocol: UDP (17)
     Header checksum: 0x9b9f [validation disabled]
     [Header checksum status: Unverified]
 0000 00 e9 3a 0b 0b f3 04 71
                                53 7d 25 80 08 00 45 00
                                                           · · : · · · · q S}%· · · E ·
 0010
       01 9b 28 0f 40 00 04 11
                                9b 9f c0 a8 01 01 ef ff
                                                           ..(.@...
                                                           * HTTP/ 1.1 HOS
                                                                     "NOTIFY
 0020
       ff fa 9a 97 07 6c 01 87
                                20 22 4e 4f 54 49 46 59
 0030
       20 2a 20 48 54 54 50 2f
                                31 2e 31 0d 0a 48 4f 53
                                                           T: 239.2 55.255.2
       54 3a 20 32 33 39 2e 32
                                35 35 2e 32 35 35 2e 32
 0050
       35 30 3a 31 39 30 30 0d
                                0a 43 41 43 48 45 2d 43
                                                           50:1900 - CACHE-C
 0060
       4f 4e 54 52 4f 4c 3a 20
                                6d 61 78 2d 61 67 65 3d
                                                           ONTROL: max-age=
 0070
       31 32 30 30 0d 0a 4c 4f
                                43 41 54 49 4f 4e 3a 20
                                                           1200 - LO CATION:
       68 74 74 70 3a 2f 2f 31
                                39 32 2e 31 36 38 2e 31
 0080
                                                           http://1 92.168.1
 0090
       2e 31 3a 34 39 31 35 32
                                2f 67 61 74 65 77 61 79
                                                          .1:49152 /gateway
       2e 78 6d 6c 0d 0a 4e 54
                                3a 20 75 72 6e 3a 73 63
                                                           .xml · NT : urn:sc
 00h0
       68 65 6d 61 73 2d 75 70
                                6e 70 2d 6f 72 67 3a 73
                                                           hemas-up np-org:s
                                41 4e 43 6f 6d 6d 6f 6e
 0000
       65 72 76 69 63 65 3a 57
                                                           ervice:W ANCommon
 00d0 49 6e 74 65 72 66 61 63
                                65 43 6f 6e 66 69 67 3a
                                                           Interfac eConfig:
 00e0
       31 0d 0a 4e 54 53 3a 20
                                73 73 64 70 3a 61 6c 69
                                                           1 · NTS: ssdp:ali
 00f0
       76 65 0d 0a 53 45 52 56
                                45 52 3a 20 4c 69 6e 75
                                                           ve · · SERV ER: Linu
                                30 2d 73 76 6e 36 35 39
 0100
       78 2f 33 2e 31 38 2e 32
                                                          x/3.18.2 0-svn659
 0110
       31 2c 20 55 50 6e 50 2f
                                31 2e 30 2c 20 49 6e 74
                                                          1, UPnP/ 1.0, Int
                                                           el SDK f or UPnP
 0120
       65 6c 20 53 44 4b 20 66
                                6f 72 20 55 50 6e 50 20
 0130
       64 65 76 69 63 65 73 20
                                2f 31 2e 32 0d 0a 55 53
                                                           devices /1.2 ·· US
                                                           N: uuid: fc4ec57e
       4e 3a 20 75 75 69 64 3a
                                66 63 34 65 63 35 37 65
 0150
       2d 32 38 62 31 2d 31 31
                                64 62 2d 38 38 66 38 2d
                                                           -28b1-11 db-88f8-
       30 30 36 30 30 38 35 64
                                62 33 66 36 3a 3a 75 72
                                                           0060085d b3f6::ur
       6e 3a 73 63 68 65 6d 61
                                73 2d 75 70 6e 70 2d 6f
                                                           n:schema s-upnp-o
                                63 65 3a 57 41 4e 43 6f
       72 67 3a 73 65 72 76 69
                                                           rg:servi ce:WANCo
 0190
       6d 6d 6f 6e 49 6e 74 65
                                72 66 61 63 65 43 6f 6e
                                                           mmonInte rfaceCon
 01a0
       66 69 67 3a 31 0d 0a 0d
                                0a
                                                           fig:1···
```

3.4) Τα κοινά πεδία που εντοπίζονται μεταξύ των των επικεφαλίδων των τεμαχίων TCP και των δεδομενογραμμάτων UDP είναι τα εξής: Source Port, Destination Port

```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 38842, Seq: 1, Ack: 1, Len: 0
Source Port: 80
Destination Port: 38842
[Stream index: 2]
[TCP Segment Len: 0]
```

```
    User Datagram Protocol, Src Port: 58672, Dst Port: 1900

       Source Port: 58672
       Destination Port: 1900
       Lenath: 133
      Checksum: 0x3312 [unverified]
3.5) Το μήκος της επικεφαλίδας των δεδομενογραμμάτων UDP είναι ίσο με 8 bytes,
σύμφωνα και με τον πίνακα περιεχομένων
Frame 65: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface wlo1, id 0

→ Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 239.255.255.250
    Source Port: 58672
    Destination Port: 1900
    Length: 133
    Checksum: 0x3312 [unverified]
 0000 01 00 5e 7f ff fa 00 e9 3a 0b 0b f3 08 00 45 00
                                                     ...@.....M-SEAR
CH * HTT P/1.1.H
 0010 00 99 f4 b0 40 00 ff 11
                             d4 f6 c0 a8 01 09 ef ff
     ff fa e5 30 07 6c 00 85 33 12 4d 2d 53 45 41 52
43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
 0020 ff fa e5 30 07 6c 00 85
 0030
                                                     OST: 239 .255.255
 0040 4f 53 54 3a 20 32 33 39
                             2e 32 35 35 2e 32 35 35
                                                     .250:190 0 · MAN:
"ssdp:di scover"
 0050 2e 32 35 30 3a 31 39 30
                             30 0d 0a 4d 41 4e 3a 20
 0060 22 73 73 64 70 3a 64 69
                             73 63 6f 76 65 72 22 0d
 0070 0a 4d 58 3a 20 31 0d 0a
                             53 54 3a 20 75 72 6e 3a
                                                     ·MX: 1 ·· ST: urn:
 0080 64 69 61 6c 2d 6d 75 6c
                             74 69 73 63 72 65 65 6e
                                                     dial-mul tiscreen
 0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61
                                                     -org:ser vice:dia
 00a0 6c 3a 31 0d 0a 0d 0a
3.6) Ναι υπάρχει και το πεδίο ονομάζεται Length

    User Datagram Protocol, Src Port: 58672, Dst Port: 1900

       Source Port: 58672
       Destination Port: 1900
       Length: 133
       Checksum: 0x3312 [unverified]
       [Checksum Status: Unverified]
       [Stream index: 15]
3.7) Ναι υπάρχει πεδίο που να καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP και
ονομάζεται Header Length
       [Next sequence number: 525
                                                  (relative sequence number)]
       Acknowledgment number: 310
                                                  (relative ack number)
       Acknowledgment number (raw): 194670270
       1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
       Window size value: 1031
```

Επίσης, βρίσκεται στα 4 MSB (Most Significant Beat) του 13ου byte της επικεφαλίδας, όπως αποδεικνύεται από τον πίνακα περιεχομένων

[Calculated window size: 65984]
[Window size scaling factor: 64]

```
    ▶ Frame 70: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface wlo1, id 0
    ▶ Ethernet II, Src: 04:71:53:7d:25:80 (04:71:53:7d:25:80), Dst: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
    ▶ Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.9
    ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 48792, Seq: 1, Ack: 310, Len: 524
    Source Port: 80
    Destination Port: 48792
    [Stream index: 6]
    [TCP Segment Len: 524]
```

01 09 00 50 be 98 a1 90 04 07 e0 aa 00 00 01 01 c4 63 48 54 54 50 2f 31 0030 0040 31 2e 31 20 32 30 30 20 4f cHTTP/1 .1 200 0 20 53 75 6e 2c 20 33 31 4b 0d 0a 44 61 74 65 3a K Date: Sun, 31 20 4f 63 74 20 32 30 32 31 20 30 30 3a 35 33 3a Oct 202 1 00:53: 00 GMT Server: Apache/2 .2.22 (F 30 30 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 2e 32 2e 32 32 20 28 46 41 70 61 63 68 65 2f 32 0090 72 65 65 42 53 44 29 20 6d 6f 64 5f 73 73 6c 2f reeBSD) mod_ssl/ 32 2e 32 2e 32 32 20 4f 70 65 6e 53 53 4c 2f 30 2.2.22 0 penSSL/0 00b0 2e 39 2e 38 7a 68 2d 66 72 65 65 62 73 64 20 44 .9.8zh-f reebsd D 00c0 41 56 2f 32 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 AV/2 · La st-Modif ied: Wed , 12 Feb 2014 07 :10:26 G MT ETAG : "175ab 69 65 64 3a 20 57 65 64 2c 20 31 32 20 46 65 62 20 32 30 31 34 20 30 37 3a 31 30 3a 32 36 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 37 35 61 62 64 2d 65 33 36 2d 34 66 32 33 30 34 34 35 61 64 d-e36-4f 230445ad 0100 63 38 30 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e c80" · · Ac cept-Ran 0110 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74 ges: byt es Cont 0130 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 36 33 38 ent-Leng th: 3638 0140 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74 69 ·· Keep-A live: ti 0150 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30 meout=5, max=100 0160 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ··Connec tion: Ke 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e ep-Alive ... Conten 0170 74 2d 54 79 70 65 3a 20 t-Type: image/x-icon 69 6d 61 67 65 2f 78 2d 0180 0190 69 63 6f 6e 0d 0a 0d 0a 00 00 01 00 02 00 10 10 00 00 00 00 00 00 68 05 00 00 26 00 00 00 20 20(. 01b0 00 00 00 00 00 00 a8 08 00 00 8e 05 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 08 00 00 00 01c0 01d0 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00 00 . . @ Z·····{I !······ 01e0 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 a5 7d 5a 00 ce ba ad 00 7b 49 01f0 21 00 e7 db d6 00 b5 9e ...eB....s... 0200 84 00 8c 65 42 00 de cb bd 00 ad 8a 73 00 ef eb 0210 e7 00 8c 55 29 00 94 71 52 00 bd a6 94 00 f7 f3 0220 f7 00 de d3 ce 00 d6 c3 b5 00 9c 7d 63 00 ef e3 de 00 8c 5d 39 00 b5 96 7b 00 84 51 21 00 84 59 0240 31 00 9c 75 5a 00 7b 51 29 00 94 69 4a 00

Acknowledgment number: 310 (relative ack number) Acknowledgment number (raw): 194670270

1000 = Header Length: 32 bytes

Flags: 0x010 (ACK) Window size value: 1031

[Calculated window size: 65984] [Window size scaling factor: 64] Checksum: OxeOaa [unverified]

```
...P.... ....n.
0020 01 09 00 50 be 98 a1 90 ed be 0b 9a 6e be 80
0030 04 07 e0 aa 00 00 01 01 08 0a b6 67 6d 59 44 b9
                                                          .....mYD.
0040 c4 63 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f
                                                          ·cHTTP/1 .1 200 0
                                                          K Date: Sun, 31
     4b 0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 33 31
0060
     20 4f 63 74 20 32 30 32
                               31 20 30 30 3a 35 33 3a
                                                          Oct 202 1 00:53:
     30 30 20 47 4d 54 0d 0a
0070
                               53 65 72 76 65 72 3a 20
                                                          00 GMT ⋅ Server:
0080 41 70 61 63 68 65 2f 32
                               2e 32 2e 32 32 20 28 46
                                                         Apache/2 .2.22 (F
     72 65 65 42 53 44 29 20
                               6d 6f 64 5f 73 73 6c 2f
                                                          reeBSD) mod_ssl/
                                                          2.2.22 0 penSSL/0
     32 2e 32 2e 32 32 20 4f
                               70 65 6e 53 53 4c 2f 30
00a0
     2e 39 2e 38 7a 68 2d 66
                               72 65 65 62 73 64 20 44
                                                          .9.8zh-f reebsd D
     41 56 2f 32 0d 0a 4c 61
00c0
                                                          AV/2 · La st-Modif
                               73 74 2d 4d 6f 64 69 66
                                                          ied: Wed , 12 Feb
     69 65 64 3a 20 57 65 64
                               2c 20 31 32 20 46 65 62
     20 32 30 31 34 20 30 37
                               3a 31 30 3a 32 36 20 47
                                                          2014 07 :10:26 G
00f0
     4d 54 0d 0a 45 54 61 67
                               3a 20 22 31 37 35 61 62
                                                          MT · · ETag : "175ab
                                                          d-e36-4f 230445ad
     64 2d 65 33 36 2d 34 66
                               32 33 30 34 34 35 61 64
0110 63 38 30 22 0d 0a 41 63
                              63 65 70 74 2d 52 61 6e
                                                         c80" · · Ac cept-Ran
     67 65 73 3a 20 62 79 74
                               65 73 0d 0a 43 6f 6e 74
                                                          ges: byt es ·· Cont
0120
     65 6e 74 2d 4c 65 6e 67
                               74 68 3a 20 33 36 33 38
0130
                                                          ent-Leng th: 3638
     0d 0a 4b 65 65 70 2d 41
0140
                               6c 69 76 65 3a 20 74 69
                                                          ··Keep-A live: ti
0150
     6d 65 6f 75 74 3d 35 2c
                               20 6d 61 78 3d 31 30 30
                                                         meout=5, max=100
                                                         ·· Connec tion: Ke
0160
     0d 0a 43 6f 6e 6e 65 63
                              74 69 6f 6e 3a 20 4b 65
0170
     65 70 2d 41 6c 69 76 65
                               0d 0a 43 6f 6e 74 65 6e
                                                          ep-Alive ⋅ Conten
     74 2d 54 79 70 65 3a 20
                               69 6d 61 67 65 2f 78 2d
                                                          t-Type: image/x-
0180
0190
     69 63 6f 6e 0d 0a 0d 0a
                               00 00 01 00 02 00 10 10
                                                          icon····
                                                          · · · · · · · h · · · · & · · · ·
01a0
     00 00 00 00 00 00 68 05
                               00 00 26 00 00 00 20 20
                               00 00 8e 05 00 00 28 00
                                                          . . . . . . . . . . . . . . . . . . ( .
01b0
     00 00 00 00 00 00 a8 08
                                                          00 00 01 00 08 00 00 00
01c0
     00 00 10 00 00 00 20 00
                                                          .......
01d0
     00 00 40 01 00 00 00 00
                               00 00 00 00 00 00 00 00
                               00 00 ff ff ff 00 a5 7d
01e0
     00 00 00 00 00 00 00 00
                                                          Z·····{I !······
01f0
     5a 00 ce ba ad 00 7b 49
                               21 00 e7 db d6 00 b5 9e
                                                          · · · eB · · · · · · · s · · ·
0200
     84 00 8c 65 42 00 de cb
                               bd 00 ad 8a 73 00 ef eb
     e7 00 8c 55 29 00 94 71
                               52 00 bd a6 94 00 f7 f3
                                                          · · · U) · · q R · · · · · · ·
0210
                                                         ····]9···{··Q!··Y
     f7 00 de d3 ce 00 d6 c3
                               b5 00 9c 7d 63 00 ef e3
0230 de 00 8c 5d 39 00 b5 96
                               7b 00 84 51 21 00 84 59
                                                          1··úZ·{Q j··iJ·
0240 31 00 9c 75 5a 00 7b 51 29 00 94 69 4a 00
```

```
Acknowledgment number: 310
                                  (relative ack number)
    Acknowledgment number (raw): 194670270
    1000 .... = Header Length: 32 bytes (8)
 ▶ Flags: 0x010 (ACK)
    Window size value: 1031
    [Calculated window size: 65984]
    [Window size scaling factor: 64]
   Checksum: OxeOaa [unverified]
0020 01 09 00 50 be 98 a1 90 ed be 0b 9a 6e be 80 10
0060 20 4f 63 74 20 32 30 32 31 20 30 30 3a 35 33 3a Oct 202 1 00:53 0070 30 30 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 00 GMT · Server:
                                                           Oct 202 1 00:53:
0080 41 70 61 63 68 65 2f 32 2e 32 2e 32 20 28 46 Apache/2 .2.22 (F
0090
     72 65 65 42 53 44 29 20
                                6d 6f 64 5f 73 73 6c 2f
                                                          reeBSD) mod ssl/
                                                         2.2.22 0 penSSL/0
                                70 65 6e 53 53 4c 2f 30
00a0 32 2e 32 2e 32 32 20 4f
00b0 2e 39 2e 38 7a 68 2d 66 72 65 65 62 73 64 20 44 .9.8zh-f reebsd D
00c0
     41 56 2f 32 0d 0a 4c 61
                                73 74 2d 4d 6f 64 69 66
                                                          AV/2 La st-Modif
                               2c 20 31 32 20 46 65 62 ied: Wed , 12 Feb
00d0 69 65 64 3a 20 57 65 64
00e0 20 32 30 31 34 20 30 37
                                3a 31 30 3a 32 36 20 47
                                                           2014 07 :10:26 G
00f0 4d 54 0d 0a 45 54 61 67
                                3a 20 22 31 37 35 61 62
                                                          MT⋅⋅ETag
                                                                    : "175ab
                                32 33 30 34 34 35 61 64 d-e36-4f 230445ad
0100 64 2d 65 33 36 2d 34 66
                               63 65 70 74 2d 52 61 6e c80" Ac cept-Ran
65 73 0d 0a 43 6f 6e 74 ges: byt es Cont
0110 63 38 30 22 0d 0a 41 63
0120 67 65 73 3a 20 62 79 74
                                                          ges: byt es . Cont
0130 65 6e 74 2d 4c 65 6e 67
                                74 68 3a 20 33 36 33 38 ent-Leng th: 3638
0140 Od 0a 4b 65 65 70 2d 41
                                6c 69 76 65 3a 20 74 69
                                                          ··Keep-A live: ti
                                20 6d 61 78 3d 31 30 30 meout=5, max=100
0150 6d 65 6f 75 74 3d 35 2c
                                74 69 6f 6e 3a 20 4b 65
                                                         ··Connec tion: Ke
0160 Od 0a 43 6f 6e 6e 65 63
0170 65 70 2d 41 6c 69 76 65
                                0d 0a 43 6f 6e 74 65 6e
                                                          ep-Alive ... Conten
                                69 6d 61 67 65 2f 78 2d t-Type: image/x-
0180 74 2d 54 79 70 65 3a 20
                               00 00 01 00 02 00 10 10 icon···· 00 00 26 00 00 00 20 20 ·····h· ··&···
0190 69 63 6f 6e 0d 0a 0d 0a
01a0 00 00 00 00 00 00 68 05
01b0 00 00 00 00 00 00 a8 08
                                00 00 8e 05 00 00 28 00
                                                         . . . . . . . . . . . . . . . . ( .
01c0 00 00 10 00 00 00 20 00
                                00 00 01 00 08 00 00 00
                                                         01d0 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00
01e0 00 00 00 00 00 00 00
                               00 00 ff ff ff 00 a5 7d
01f0 5a 00 ce ba ad 00 7b 49
                                21 00 e7 db d6 00 b5 9e
                                                          Z·····{I !······
                               bd 00 ad 8a 73 00 ef eb ...eB....s...
0200 84 00 8c 65 42 00 de cb
                                                         ...U) · · q R · · · · · · · }c · · · · . }c · · · · . }c · · · · · ]9 · · · { · · Q! · · Y
                                52 00 bd a6 94 00 f7 f3
0210 e7 00 8c 55 29 00 94 71
0220 f7 00 de d3 ce 00 d6 c3
                                b5 00 9c 7d 63 00 ef e3
0230 de 00 8c 5d 39 00 b5 96 7b 00 84 51 21 00 84 59
0240 31 00 9c 75 5a 00 7b 51 29 00 94 69 4a 00
                                                          1 · · uZ · {Q ) · · iJ ·
```

Όπου υπάρχει μία "επικάλυψη" του πεδίου Header Length με το πεδίο Flags, αλλά από τον αριθμό 8 καταλαβαίνουμε ότι το Header Length καταλαμβάνει την θέση των 4 MSB και τα υπόλοιπα 4 LSB ανήκουν στο πεδίο Flags

- 3.8) Όχι, δεν υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος των τεμαχίων TCP, αλλά μπορεί να προκύψει το συνολικό μήκος σαν άθροισμα του IPv4 Header Length και του TCP Header Length ή αλλιώς Total TCP Length = IPv4 Header Length + TCP Header Length
- 3.9) Υπάρχει πεδίο στην επικεφαλίδα TCP ή UDP που να προσδιορίζει τον τύπο του πρωτοκόλλου εφαρμογής και είναι συνδεδεμένο με το Destination Port που συμπεραίνουμε βάση του πίνακα του παρεχόμενου λινκ της εκφώνησης και του αντιστοίχου πρωτοκόλλου εφαρμογής.
- 3.10) Τα πρωτόκολλα του στρώματος εφαρμογής (Application Layer) που παρατηρήθηκαν είναι τα εξής: DNS, MDNS, HTTP, SSDP

4. Στρώμα Εφαρμογής

4.1) Χρησιμοποιεί το πρωτόκολλο μεταφοράς UDP

```
+ 63 0.028425133 192.168.1.9 192.168.1.1 DNS 103 Standard query 0x2ctc AAAA connectivity-check.ubuntu.com 50 0.000182631 192.168.1.9 192.168.1.1 DNS 89 Standard query 0x2ctc AAAA connectivity-check.ubuntu.com 108 0.000309880 192.168.1.9 192.168.1.1 DNS 77 Standard query 0x4d87 AAAA edu-dy.cn.ntua.gr 108 0.000309880 192.168.1.9 192.168.1.1 DNS 94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home 52 0.00040209 102.168 1 0 102.168.1.1 DNS 94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home 63: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface wlod, id 0 Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: 04:71:53:7d:25:80 (04:71:53:7d:25:80)

Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 45664, Dst Port: 53

Domain Name System (query)

TRANSUM RTE Data
```

4.2) Χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP

- 4.3) Είναι το 16ο bit της επικεφαλίδας DNS, δηλαδή το πρώτο bit της σημαίας flag στην επικεφαλίδα DNS καθορίζει το κατά πόσον πρόκειται για ερώτηση ή απάντηση και οι αντίστοιχες τιμές σε κάθε περίπτωση είναι οι εξής: η τιμή 0 αντιστοιχεί σε ερώτηση (query) και η τιμή 1 αντιστοιχεί σε απάντηση (response)
- 4.4) Η θύρα προορισμού (Destination Port) των ερωτήσεων (query) DNS είναι η εξής: 53

```
89 Standard query 0x2c1c AAAA connectivity-check.ubuntu.com
77 Standard query 0x4487 AAAA edu-dy.cn.ntua.gr
           50 0.000182631 192.168.1.9
                                                                                      192.168.1.1
                                                                                                                                  DNS
         108 0.000309880 192.168.1.9
                                                                                      192.168.1.1
                                                                                                                                                           94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home
 Frame 63: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface wlo1, id 0 Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: 04:71:53:7d:25:80 (04:71:53:7d:25:80)
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 45664, Dst Port: 53
Source Port: 45664
       Lenath: 69
                            0x8957
0000 04 71 53 7d 25 80 00 e9 3a 0b 0b f3 08 00 45 00 0010 00 59 45 b5 40 00 40 11 71 84 c0 a8 01 09 c0 a8 0020 01 01 b2 60 03 05 00 45 89 57 14 34 01 00 00 01 01 00 00 01 00 77 72 6f 64 0e 69 6e 67 65
                                                                                                                         qS}%···:····
YE·@·@· q····
···•5·E··W·4·
                                                                                                                       stion-ed ge prod
dataops mozgcp n
           73 74 69 6f 6e 2d 65 64
64 61 74 61 6f 70 73 06
65 74 00 00 1c 00 01
                                                                67 65 04 70 72 6f 64 07
                                                                6d 6f 7a 67 63 70 03 6e
```

4.5) Οι θύρες προέλευσης (Source Port) των ερωτήσεων (query) DNS είναι η εξής: 45664, 51383, 53720, 54788, 37499, 52521, 47406 πχ:

4.6) Η θύρα προέλευσης (Source Port) των απαντήσεων (query response) DNS είναι η εξής:

```
## 64 0.0060975460 192.168.1.1 192.168.1.9 DNS 103 Standard query response 0x1434 AAAA prod.ingestion-edge.prod.

107 0.002122371 192.168.1.1 192.168.1.9 DNS 89 Standard query response 0x2ctc AAAA connectivity-check.ubuntu.

52 0.000037225 192.168.1.1 192.168.1.9 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME 103.168.1.0 DNS 112 Standard query
```

4.7) Οι θύρες προορισμού (Destination Port) των απαντήσεων (query response) DNS είναι οι εξής: 45664, 51383, 53720, 54788, 37499, 52521, 47406

```
107 0.00212371 192.168.1.1 192.168.1.9 DNS 103 Standard query response 0x1434 AAAA prod.ingestion-edge.prod...
107 0.00212371 192.168.1.1 192.168.1.9 DNS 89 Standard query response 0x2c1c AAAA connectivity-check.ubuntu.
52 0.000037225 192.168.1.1 192.168.1.9 DNS 112 Standard query response 0x4d87 AAAA edu-dy.cn.ntua.gr CNAME e...
109 0.008268161 192.168.1.1 192.168.1.9 DNS 169 Standard query response 0x7559 No such name AAAA conNectivITY...

Frame 64: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface wlot, id 0

Ethernet II, Src: 04:71:53:7d:25:80 (94:71:53:7d:25:80), Dst: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.9

* User Datagram Protocol, Src Port: 53, Dst Port: 45664

Length: 69

Checksum: 0x08d7 [unverified]
```

- 4.8) Παρατηρώ ότι οι θύρες προέλευσης των ερωτήσεων ταυτίζονται με τις θύρες προορισμού των απαντήσεων, δηλαδή από όποια θύρα γίνεται η ερώτηση στην ίδια θύρα αναμένεται και η απάντηση της συγκεκριμένης ερώτησης που τέθηκε
- 4.9) Η πασίγνωστη θύρα που ακούει ο εξυπηρετητής DNS είναι η Port: 53
- 4.10) Η θύρα προορισμού των μηνυμάτων HTTP που παράγει ο υπολογιστής μου είναι η Destination Port: 80

```
378 HTTP/1.1 200 OK (image/x-icon)
103 Standard query 0x1434 AAAA prod.ingestion-edge.prod.dataops.m.
         84 0.009973866 147.102.40.15
63 0.028425133 192.168.1.9
                                                                        192.168.1.9
192.168.1.1
                                                                                                             DNS
                                                                                                                                 89 Standard query 0x1404 AAAA connectivity-check.ubuntu.com
77 Standard query 0x4d87 AAAA edu-dy.cn.ntua.gr
94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home
       106 0.001087830 192.168.1.9
                                                                        192.168.1.1
                                                                                                             DNS
       50 0.000182631 192.168.1.9
108 0.000309880 192.168.1.9
                                                                        192.168.1.1
192.168.1.1
                                                                                                             DNS
                                                                                                             DNS
 Frame 68: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface wlo1, id 0
Ethernet II, Src: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3), Dst: 04:71:53:7d:25:80 (04:71:53:7d:25:80)

Internet Protocol Version 4, Src: 192.168.1.9, Dst: 147.102.40.15

Transmission Control Protocol, Src Port: 48792, Dst Port: 80, Seq: 1, Ack: 1, Len: 309
      Source Port: 48792
     [Stream index: 6]
```

4.11) Οι θύρες προέλευσης των μηνυμάτων HTTP που έστειλε ο υπολογιστής μου είναι οι Source Ports: 48792

```
378 HTTP/1.1 200 OK (image/x-icon)
          84 0.009973866 147.102.40.15
                                                                   192.168.1.9
                                                                                                                     103 Standard query 0x1434 AAAA prod.ingestion-edge.prod.dataops.
89 Standard query 0x2c1c AAAA connectivity-check.ubuntu.com
77 Standard query 0x4d87 AAAA edu-dy.cn.ntua.gr
          63 0.028425133 192.168.1.9
                                                                   192,168,1,1
                                                                                                     DNS
        106 0.001087830 192.168.1.9
50 0.000182631 192.168.1.9
                                                                  192.168.1.1
                                                                                                                       94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home
        108 0.000309880 192.168.1.9
                                                                  192.168.1.1
                                                                                                    DNS

    Internet Protocol Version 4, Src: 192.168.1.9, Dst: 147.102.40.15
    Transmission Control Protocol, Src Port: 48792, Dst Port: 80, Seq: 1, Ack: 1, Len: 309

       Destination Port: 80
      [Stream index: 6]
[TCP Segment Len: 309]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 194668961
```

4.12) Η θύρα προέλευσης των απαντήσεων των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού είναι η Source Port: 80

```
68 0.062298700 192.168.1.9
                                                                           147.102.40.15
                                                                                                                                        375 GET /favicon.ico HTTP/1.1
        63 0.028425133 192.168.1.9
                                                                            192.168.1.1
                                                                                                                                        103 Standard guery 0x1434 AAAA prod.ingestion-edge.prod.dataops.m..
                                                                                                                    DNS
                                                                                                                                         89 Standard query 0x4c1c AAAA connectivity-check.ubuntu.com
77 Standard query 0x4d87 AAAA edu-dy.cn.ntua.gr
94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home
       106 0.001087830 192.168.1.9
                                                                            192.168.1.1
                                                                                                                    DNS
      50 0.000182631 192.168.1.9
108 0.000309880 192.168.1.9
                                                                           192.168.1.1
                                                                                                                    DNS
Frame 84: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits) on interface wlo1, id 0
Ethernet II, Src: 04:71:53:76:25:80 (04:71:53:76:25:80), Dst: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)
Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.9
Transmission Control Protocol, Src Port: 80, Dst Port: 48792, Seq: 3669, Ack: 310, Len: 312
     [Stream index: 6]
```

4.13) Η θύρα προορισμού των απαντήσεων αυτών είναι η Destination Port: 48792

-	68 0.062298700 192.168.1.9	147.102.40.15	HTTP	375 GET /favicon.ico HTTP/1.1				
4	84 0.009973866 147.102.40.15	192.168.1.9	HTTP	378 HTTP/1.1 200 OK (image/x-icon)				
	63 0.028425133 192.168.1.9	192.168.1.1	DNS	103 Standard query 0x1434 AAAA prod.ingestion-edge.prod.dataops.m				
	106 0.001087830 192.168.1.9	192.168.1.1	DNS	89 Standard query 0x2c1c AAAA connectivity-check.ubuntu.com				
	50 0.000182631 192.168.1.9	192.168.1.1	DNS	77 Standard query 0x4d87 AAAA edu-dy.cn.ntua.gr				
	108 0.000309880 192.168.1.9	192.168.1.1	DNS	94 Standard query 0x7559 AAAA connectivity-check.ubuntu.com.home				
	E2 0 000404200 102 160 1 0	100 160 1 1	DMC	91 Standard quary Aydhos AAAA adu dy an aco ntua gr				
-	Frame 84: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits) on interface wlo1, id 0							
•	▶ Ethernet II, Src: 04:71:53:7d:25:80 (04:71:53:7d:25:80), Dst: 00:e9:3a:0b:0b:f3 (00:e9:3a:0b:0b:f3)							
-	• Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.9							
+	Transmission Control Protocol, Src Port: 80, Dst Port: 48792, Seq: 3669, Ack: 310, Len: 312							
	Source Port: 80							
	Destination Port: 48792							
	[Stream index: 6]							
	[TCP Segment Len: 312]							

- 4.14) Η πασίγνωστη θύρα όπου ακούει ο εξυπηρετητής HTTP είναι η Port: 80
- 4.15) Παρατηρώ ότι οι θύρες προέλευσης των μηνυμάτων HTTP ταυτίζονται με τις θύρες προορισμού των αντίστοιχων απαντήσεων, δηλαδή από όποια θύρα γίνεται η ερώτηση στην ίδια θύρα αναμένεται και η απάντηση της συγκεκριμένης ερώτησης που τέθηκε
- 4.16) Η ονομασία του πρώτου μηνύματος HTTP από τον υπολογιστή μου προς το εξυπηρετητή ιστού είναι το εξής: GET /favicon.ico HTTP/1.1

No.	Time	Source	Destination	Protocol	Length Info	*
	86 0.006428433	147.102.40.15	192.168.1.9	TCP	66 80 → 48792 [ACK]	Seq=3981 Ack=311 Win=65984 Len=0 TSval=30602
	72 0.000013758	147.102.40.15	192.168.1.9	TCP	590 80 → 48792 [ACK]	Seq=525 Ack=310 Win=65984 Len=524 TSval=3060
	88 0.000014526	147.102.40.15	192.168.1.9	TCP	66 80 → 48792 [FIN,	ACK] Seq=3981 Ack=311 Win=65984 Len=0 TSval=
	57 0.008116468	147.102.40.15	192.168.1.9	TCP	74 80 → 48792 [SYN,	ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=
+	68 0.087854731		147.102.40.15	HTTP	375 GET /favicon.ico	HTTP/1.1
+	84 0.000002794	147.102.40.15	192.168.1.9	HTTP	378 HTTP/1.1 200 OK	(image/x-icon)

4.17) Ο κωδικός απάντησης που επιστρέφει ο εξυπηρετητής ιστού είναι ο εξής: HTTP/1.1 200 OK (image/x-icon)

No.	Time	Source	Destination	Protocol	ength Info	-
	86 0.006428433	147.102.40.15	192.168.1.9	TCP	66 80 → 48792 [ACK] Seq=3981 Ack=311 Win=65984 Len=0 TSval=3060	2
+	72 0.000013758	147.102.40.15	192.168.1.9	TCP	590 80 → 48792 [ACK] Seq=525 Ack=310 Win=65984 Len=524 TSval=300	
	88 0.000014526	147.102.40.15	192.168.1.9	TCP	66 80 → 48792 [FIN, ACK] Seq=3981 Ack=311 Win=65984 Len=0 TSva	=
	57 0.008116468	147.102.40.15	192.168.1.9	TCP	74 80 → 48792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS	3=
-	68 0.087854731	192.168.1.9	147.102.40.15	HTTP	375 GET /favicon.ico HTTP/1.1	
+	84 0.000002794	147.102.40.15	192.168.1.9	HTTP	378 HTTP/1.1 200 OK (image/x-icon)	
-	68 0.087854731	192.168.1.9	147.102.40.15	HTTP	375 GET /favicon.ico HTTP/1.1	=536 WS

4.18) Παρατηρούμε ότι δεν γίνονται DNS queries (ερωτήσεις) πριν από την λήψη του πακέτου GET /favicon.ico HTTP/1.1, καθώς το αποτέλεσμα DNS (response) αποθηκεύεται στην DNS cache του υπολογιστή μου. Έτσι για να μπορώ να έχω πρόσβαση και να τα δω αυτά πρέπει να εκτελεστεί η εντολή sudo systemd-resolve --flush-caches (σε λειτουργικό Llnux), ώστε να διαγραφεί η μνήμη των DNS αποτελεσμάτων