

Εργαστηριακή Άσκηση 2 Ενθυλάκωση και Επικεφαλίδες

Θοδωρής Φρίζος Παπαρρηγόπουλος

el18040

21/10/2021

Ομάδα 4η.

Ipn6: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a

MAC: 40-1C-83-38-F7-20

Λειτουργικό: Windows

DESKTOP-1403ER3

Άσκηση 1

1.1) Το φίλτρο μας επιτρέπει να δούμε μόνο πακέτα με πρωτόκολλο ip ή arp.

1.2) Destination, Source, Type

1.3) Όχι, δεν υπάρχει τέτοιο αντίστοιχο πεδίο

1.4) Έχουν μήκος 6 bytes

1.5) Έχει μήκος 14 bytes

1.6) Type: ARP (0x0806)

1.7) Τα τελευταία 2 bytes

1.8) Protocol type: IPv4 (0x0800)

1.9) 0x0806

Ασκηση 2

2.1) Μου δείχνει την απεικόνιση μόνο πρωτοκόλλων ICMP στο στρώμα δικτύου

2.2) Είναι 4 byte

2.3) Τα πρώτα 2 πεδία είναι Version & Header Length

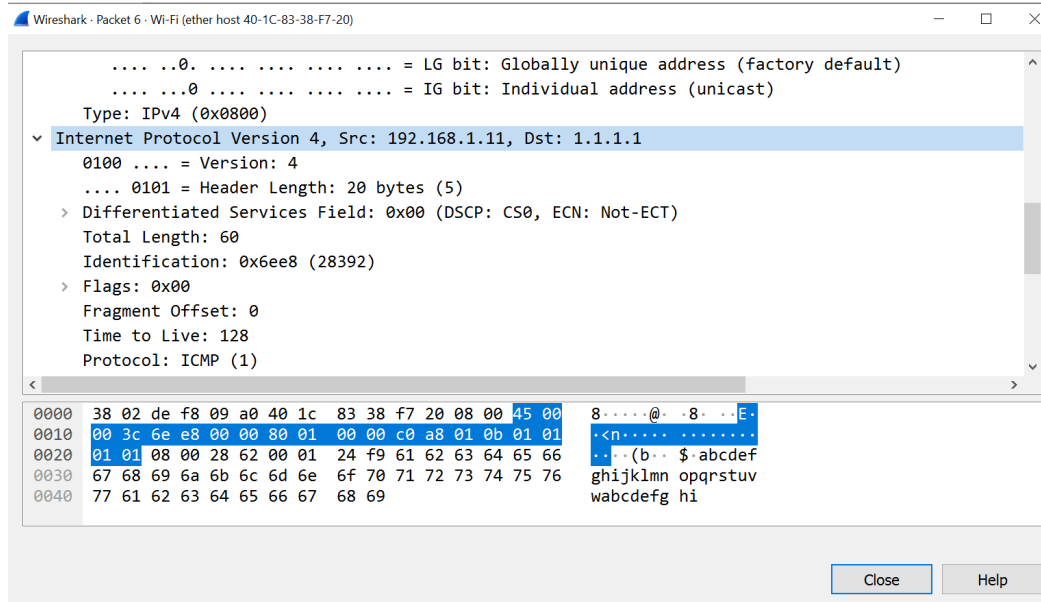
2.4)

Version: 0b0100

Header Length: 0b0101

2.5) 20 bytes

2.6) Αρχικά μπορούμε να μετρήσουμε 20 bytes. Επιπλέον, γνωρίζουμε ότι το μέγεθος της επικεφαλίδας είναι 5 και το πολλαπλασιάζουμε με το 4 βρίσκουμε το μήκος της επικεφαλίδας (= 20).



2.7) Frame Length: 74 bytes (592 bits)

2.8) Στην επικεφαλίδα υπάρχει πεδίο με τη τιμή 74.

2.9) 44 bytes.

2.10) Αν αφαιρέσουμε το συνολικό μήκος μείον το μήκος της επικεφαλίδας είναι $74 - 20 = 44$ bytes.

2.11) Το πεδίο Protocol

2.12) Στο 10ο byte της επικεφαλίδας.

2.13) 0x01

Άσκηση 3

3.1) Επιτρέπει την απεικόνιση μόνο πακέτων με πρωτόκολλο TCP ή UDP στο στρώμα μεταφοράς

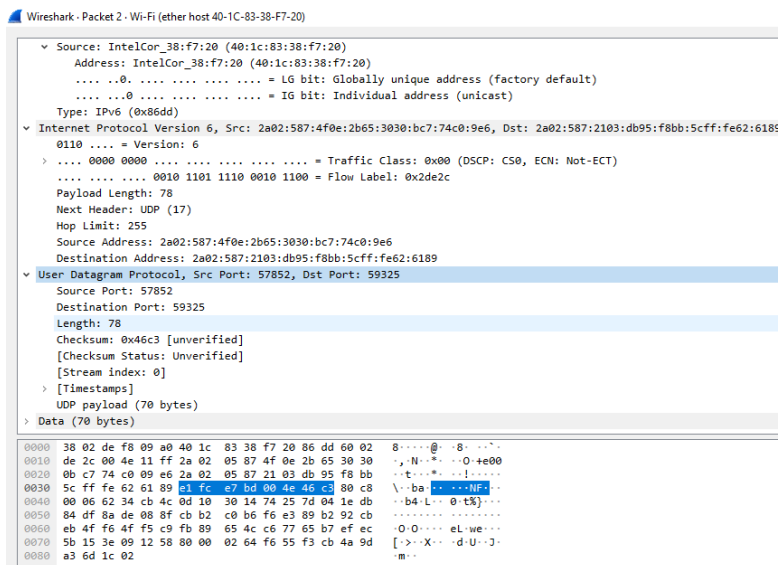
3.2) Παρατηρώ TCP, TCPv1.2, TCPv1.3, DNS, UDP, TLSv1.2, TLSv1.3, HTTP

3.3) TCP (6 = 0x06) και UDP (17 = 0x11)

3.4) Τα κοινά πεδία είναι τα Src Port, Dst Port

3.5) 8 bytes

3.6) Ναι υπάρχει Length



```
Wireshark - Packet 2 - Wi-Fi (ether host 40-1c-83-38-f7-20)

  ▾ Source: IntelCor_38:f7:20 (40:1c:83:38:f7:20)
    Address: IntelCor_38:f7:20 (40:1c:83:38:f7:20)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
  ▾ Internet Protocol Version 6, Src: 2a02:587:4f0e:2b65:3030:bc7:74c0:9e6, Dst: 2a02:587:2103:db95:f8bb:5cff:fe62:618f
    0110 .... = Version: 6
    > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0010 1101 1110 0010 1100 = Flow Label: 0x2de2c
    Payload Length: 78
    Next Header: UDP (17)
    Hop Limit: 255
    Source Address: 2a02:587:4f0e:2b65:3030:bc7:74c0:9e6
    Destination Address: 2a02:587:2103:db95:f8bb:5cff:fe62:6189
  ▾ User Datagram Protocol, Src Port: 57852, Dst Port: 59325
    Source Port: 57852
    Destination Port: 59325
    Length: 78
    Checksum: 0x46c3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    > [Timestamps]
    UDP payload (70 bytes)
  > Data (70 bytes)

0000 38 02 de f8 09 a0 40 1c 83 38 f7 20 86 dd 60 02 8.....@.....
0010 de 2c 00 4e 11 ff 2a 02 05 87 4f 0e 2b 65 30 30 ,N... ..O+e00
0020 0b c7 74 c0 09 e6 2a 02 05 87 21 03 db 95 f8 bb ..t... ..!....
0030 5c ff fe 62 61 89 a1 fc e7 bd 00 4e 46 c8 80 c8 \..ba...NF...
0040 00 06 62 34 cb 4c 0d 10 30 14 74 25 7d 04 1e db ..b4L...0t%}...
0050 84 df 8a de 08 8f cb b2 c0 b6 f6 e3 89 b2 92 cb .....
0060 eb 4f f6 4f f5 c9 fb 89 65 4c c6 77 65 b7 ef ec .O.O...eLwe...
0070 5b 15 3e 09 12 58 80 00 02 64 f6 55 f3 cb 4a 9d [->...X...d-U...
0080 a3 6d 1c 02 ..m...
```

3.7) Το Header Length βρίσκεται στο 13ο byte της επικεφαλίδας στο 5 MSB.

3.8) Δεν υπάρχει αντίστοιχο πεδίο. Προκύπτει από το άθροισμα των Ipv4 Header Length + TCP Header Length

3.9) Είναι συνδεδεμένο με το Destination Port που με βάση του πίνακα στο link συμπεραίνουμε πως είναι το αντίστοιχο πρωτόκολλο εφαρμογής.

3.10) STUN, QUIC, MDNS, SSDP

Άσκηση 4

4.1) Το UDP

4.2) Το TCP

4.3) Το καθορίζει το πρώτο bit της σημαίας (flag) όπου όταν είναι 0 σημαίνει query ενώ για 1 σημαίνει response

4.4) Destination Port: 53

4.5) Source Ports: 49665, 51708, 52330, 52809 , 53770, 55182, 56977, 57567, 58531, 58997, 59704, 61389, 63296, 64324

4.6) Source Port: 53

4.7) Destination Ports: 49665, 51708, 52330, 52809 , 53770, 55182, 56977, 57567, 58531, 58997, 59704, 61389, 63296, 64324

4.8) Παρατηρώ πως είναι οι ίδιες ακριβώς θύρες.

4.9) Είναι η θύρα 53

4.10) Destination Port: 80

4.11) Source Port: 55541

4.12) Source Port: 80

4.13) Destination Port: 55541

4.14) Είναι η θύρα 80

4.15) Παρατηρώ πως είναι οι ίδιες ακριβώς θύρες.

4.16) Το όνομα του πρώτου μηνύματος είναι: GET //lab2/HTTP/1.1

4.17) Ο κωδικός απάντησης είναι: HTTP/1.1 200 OK

4.18) Χωρίς αυτή την εντολή δεν θα γίνονταν DNS Queries πριν την λήψη του πακέτου GET αφού το DNS αποτέλεσμα είναι αποθηκευμένο στην DNS Cache του υπολογιστή μου. Έτσι για να τα δω θα έπρεπε να διαγράψω από την μνήμη των DNS αποτελεσμάτων.