Εθνικό Μετσόβιο Πολυτεχνείο
Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2022-2023
Όνομα:
Ιωάννης Μπασδέκης - 03119198

2η Εργαστηριακή Αναφορά

1ο Μέρος

1.1) Σημασία Φίλτρου:
-Το χρησιμοποιούμε για να δούμε μόνο τα πλαίσια με πρωτόκολλο ARP ή όσα έχουν το πρωτόκολλο IPv4

1.2) Πεδία:
-Destination Source Type

1.3) Πεδίου μήκους Ethernet:
-Όχι

1.4) Μήκος:
-6 bytes

1.5) Συνολικό Μήκος:
- 6+6+2 =14

1.6) Πεδίο πρωτοκόλλου δικτύου:
- Το τρίτο πεδίο

1.7) Θέση:
-Είναι τα 2 τελευταία bytes

1.8) Τιμή για IPv4:
-0x0800

1.9) Τιμή για ARP:
-0x0806

2ο Μέρος

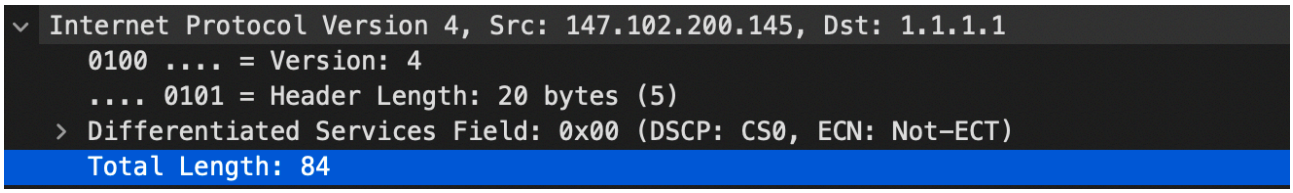
2.1) Σημασία Φίλτρου:
-Εμφανίζει μόνο τα πλαίσια που έχουν το πρωτόκολλο ICMP.

2.2) Μήκος Διευθύνσεων IPv4:
-4 bytes

2.3) Πρώτα Δύο Πεδία:
-Είναι το version και το header length.

2.4) Ονόματα και Μήκος Πεδίων:
-version = 0100 4 bits
-header length = 0101 (5 bit)

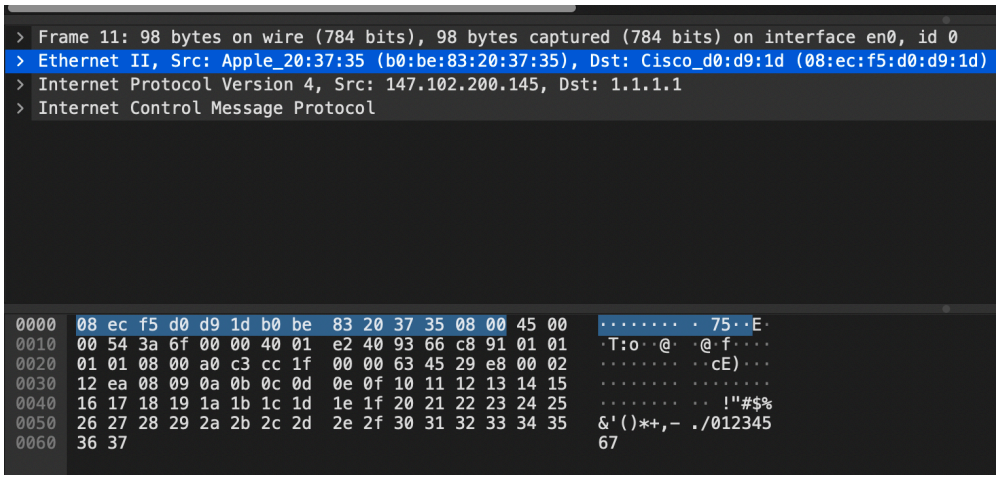
2.5) Total IP header length:
-20 bytes



2.6)Header Length:
-Με το header length βρίσκουμε από πόσες τετράμπιτες λέξεις απαρτίζεται το IP header. Εφόσον είναι 5 έχουμε 5 τετράμπιτες λέξεις από 4 bytes η κάθε μία άρα 5*4 = 20 bytes.

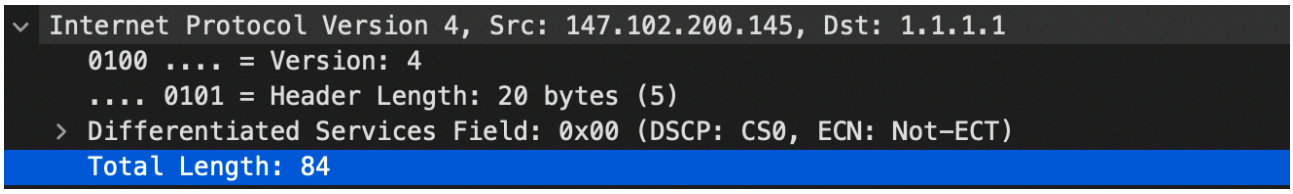
2.7) Μήκος πακέτου IPv4:

-Τα πρώτα 14 bytes του πλαισίου είναι για το ethernet. Αν μετρήσουμε τα υπόλοιπα είναι 84.



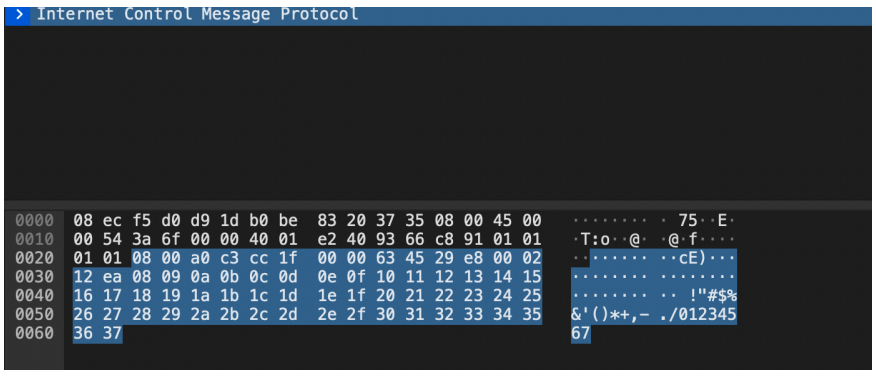
2.8)Πεδίο για Συνολικό Μήκος:

-Ναι, το length 84.



2.9)Μήκος payload του πλαισίου IPv4:

-Το IPv4 πλαίσιο αποτελείται από το ip header και payload που στην προκειμένη περίπτωση είναι ένα πακέτο ICMP του οποίου το μήκος είναι 64.



2.10) Payload length:

-Total length - Header length = 84 - 20 = 64.

2.11) Στρώμα Σουίτας:
-Πεδίο protocol.

2.12) Θέση:
-Είναι το 10ο byte μέσα στο IP header

2.13)Τιμή για ICMP:
-0x01

3ο Μέρος

3.1) Σημασία Φίλτρου:
-Με αυτό το φίλτρο εμφανίζονται μόνο τα πλαίσια με πρωτόκολλα TCP UDP.

3.2) Πρωτόκολλα Μεταφοράς:
-UDP RCP TLSV1.2

3.3) Πεδίο Protocol:
-Για TCP: protocol = TCP.
-Για UDP: next header = UDP.

3.4) Ονόματα Κοινών Πεδίων:
-common πεδία : source port, destination port, checksum.

3.5) UDP Header Length:
-8 bytes

3.6) Πεδίο για Μήκος:
-Όχι αλλά έχουμε το πεδίο length kai το πεδίο payload και αν κάνουμε την αφαίρεση βρισκούμε το 8.

3.7) Πεδίο:
-Είναι το πεδίο header length που είναι το 13ο byte από την αρχή της επικεφαλίδας tcp.

3.8) Πεδίο:
-Ναι το length.

3.9) Πεδίο για Πρωτόκολλο Εφαρμογής:
-Δεν υπάρχει κάποιο συγκεκριμένο πεδίο αλλά από το source port και destination port μπορούμε να καταλάβουμε για ποιο πρωτόκολλο εφαρμογής μιλάμε. ΠΧ 53->DNS 80-> http 443->https

3.10) Άλλα πρωτόκολλα:
-MDNS, HTTP, SSDP

4ο Μέρος

4.1) DNS:
-UDP

4.2) HTTP:
-TCP

4.3) Είδος DNS:
-το πρώτο bit από το flag. Για 0 έχουμε ερώτηση για 1 έχουμε απάντηση.

4.4) Query Destination Port:
-53

4.5) Query Source Ports (examples):
-63044 , 50556

4.6) Response Source Port:
-53

4.7) Response Destination Ports (examples):
-63044, 50556

4.8) Παρατήρηση:
-Είναι ίδιες.

4.9) Πασίγνωστη θύρα DNS:
-53

4.10) HTTP GET Destination Port:
-80

4.11) HTTP GET Source Ports:-
53165

4.12) HTTP Response Source Port:
-80

4.13) HTTP Response Destination Port:
-53165

4.14) Πασίγνωστη θύρα HTTP:
-80

4.15) Παρατήρηση:
-Είναι ίδιες.

4.16) Μέθοδος από Υπολογιστή:
-GET /lab2/ HTTP/1.1

4.17) Κώδικας Επιστροφής:
-HTTP/1.1 200 OK

4.18) Απάντηση:
-Γιατί τα ονόματα DNS είναι αποθηκευμένα στην cache και οταν κάνει query ο υπολογιστής για να βρει τις ip που θελει την ερώτηση την απαντάει η cache και οχι ο DNS server.