Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Ονοματεπώνυμο: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

Ομάδα: 3

Όνομα PC/ΛΣ: LAPTOP-TK5Q3T95 / Windows 11

Ημερομηνία: 10/10/2023

Διεύθυνση IP: 192.168.1.14

Διεύθυνση MAC: B4-B5-B6-79-4B-09

1. Data Link Layer

1.1 Ποια η σημασία του φίλτρου απεικόνισης που εφαρμόσατε;

Εμφανίζονται μόνο τα πακέτα που έχουν IP(Internet Protocol) or ARP (Address Resolution Protocol) επικεφαλίδες.

1.2 Ποια είναι τα ονόματα των πεδίων της επικεφαλίδας του πλαισίου Ethernet;

Τα ονόματα των επικεφαλίδων του πλαισίου Internet είναι:

- Destination
- Source
- Type

1.3 Υπάρχει πεδίο για το συνολικό μήκος του πλαισίου ή των δεδομένων που μεταφέρει;

Όχι. Στο πλαίσιο Ethernet δεν υπάρχει πεδίο για το συνολικό μήκος του πλαισίου ή των δεδομένων που μεταφέρει.

1.4 Ποιο είναι το μήκος των διευθύνσεων Ethernet σε byte;

6 bytes.

1.5 Ποιο είναι το συνολικό μήκος της επικεφαλίδας Ethernet σε byte;

14 bytes = 6 bytes(Destination) + 6 bytes(Source) + 2 bytes(Type)

1.6 Ποιο πεδίο του πλαισίου Ethernet καθορίζει το πρωτόκολλο δικτύου;

Το πεδίο Type του πλαισίου Ethernet.

1.7 Ποια είναι η θέση που καταλαμβάνει μέσα στην επικεφαλίδα Ethernet;

Καταλαμβάνει τα δύο τελεταία bytes.

1.8 Ποια είναι η τιμή του πεδίου αυτού για πακέτα IPv4;
Η τιμή του πεδίου αυτού είναι 0x0800 για πακέτα IPv4.

1.9 Εάν καταγράφηκαν, ποια είναι η τιμή του πεδίου αυτού για πακέτα ARP.
Δεν καταγράφηκαν ARP πακέτα ωστόσο το αντίστοιχο πεδίο για αυτά έχει τιμή 0x0806.

2. Network Layer

2.1 Ποια η σημασία του φίλτρου απεικόνισης που εφαρμόσατε;
Εμφανίζονται μόνο τα πακέτα με ICMP (Internet Control Message Protocol).

2.2 Ποιο είναι το μήκος των διευθύνσεων IPv4 σε byte;
Οι IPv4 διευθύνσεις έχουν μήκος 4 bytes.

2.3 Ποια είναι τα ονόματα των πρώτων δύο πεδίων της επικεφαλίδας IPv4;
1. Version
2. Header Length

2.4 Ποιο είναι το μήκος σε bit και ποια η τιμή των πεδίων αυτών; [Υπόδειξη: Για τη δομή της επικεφαλίδας του πρωτοκόλλου IPv4 μπορείτε να συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας το “IP protocol suite” από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο IP στο δεξιό της μέρος. Επειδή εδώ και πολύ καιρό η ιστοσελίδα δεν ανταποκρίνεται αναζητήστε την στο Internet Archive.]
Τα πεδία έχουν μήκος 4 bit το καθένα. Το πρώτο έχει τιμή 4(Version of protocol) και το δεύτερο τιμή 5.

2.5 Επιλέξτε ένα πακέτο IPv4. Ποιο είναι το συνολικό μήκος σε byte της επικεφαλίδας IPv4 με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα;
20 bytes =

1(Version & Header Length) + 1(Differentiated Services Field)

+2(Total Length) + 2(Identification)

+2(Flags & Fragment Offset) + 1(Time to Live)

+1(Protocol) + 2(Header Checksum)

+4(Source) + 4(Destination)

2.6 Πώς προκύπτει αυτό το μήκος από την τιμή του αντίστοιχου πεδίου της επικεφαλίδας IPv4;
Από το πεδίο Header Length η τιμή 5 εκφράζει το μέγεθος της διεύθυνσης σε λέξεις των 32 bits. Άρα έχουμε 5 * 32 = 160 bits, δηλαδή 160/8 = 20 bytes μέγεθος επικεφαλίδας.

2.7 Ποιο είναι το συνολικό μήκος σε byte αυτού του πακέτου IPv4 με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα;
Με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα το συνολικό μήκος σε bytes αυτού του πακέτου IPv4 είναι 74 bytes.

2.8 Υπάρχει πεδίο σχετικό με το μήκος του πακέτου IPv4 στην επικεφαλίδα του; Συμφωνεί η τιμή του με το μήκος που βρήκατε προηγουμένως;
Στην επικεφαλίδα Frame αναγράφεται το μέγεθος του πακέτου (74 bytes) το οποίο συμφωνεί με την τιμή υπολογίσαμε στον 2.7.

2.9 Ποιο είναι το μήκος δεδομένων (payload) του πακέτου IPv4 σε byte;
Το μήκος των δεδομένων(payload) σε bytes είναι 32 bytes.

2.10 Πώς προκύπτει το μήκος των δεδομένων (payload) του πακέτου IPv4 από τα στοιχεία της επικεφαλίδας;
Από την επικεφαλίδα Internet Control Message Protocol στο πεδίο Data αναγράφεται δίπλα το μέγεθος των δεδομένων που είναι 32 bytes.

2.11 Ποιο πεδίο της επικεφαλίδας IPv4 καθορίζει το πρωτόκολλο ανωτέρου στρώματος της σουίτας TCP/IP;
Το πεδίο Protocol της IPv4 επικεφαλίδας.

2.12 Ποια είναι η θέση του (σε σχέση με την αρχή της επικεφαλίδας IPv4);
Βρίσκεται στο 10ο byte από την αρχή της IPv4 επικεφαλίδας.

2.13 Ποια είναι η τιμή του για το πρωτόκολλο ICMP;
Η τιμή του πεδίου αυτού για το πρωτόκολλο ICMP είναι 01_{16}.

3. Transport Layer

3.1 Ποια η σημασία του παραπάνω φίλτρου απεικόνισης;
Εμφανίζονται μόνο πακέτα με επικεφαλίδες TCP ή UDP.

3.2 Ποια πρωτοκόλλα του στρώματος μεταφοράς παρατηρείτε;
Τα πρωτόκολλα στρώματος μεταφοράς που εμφανίζονται είναι:

- ✓ TCP(Transmission Control Protocol)
- ✓ UDP(User Datagram Protocol)
- ✓ QUIC(Quick UDP Internet Connections)
- ✓ TLS(Transport Layer Security)

3.3 Ποια είναι η τιμή του πεδίου Protocol στην επικεφαλίδα IPv4 για το πρωτόκολλο TCP και ποια για το UDP; [Υπόδειξη: Εάν τα δεδομενογράμματα UDP μεταφέρθηκαν ως πακέτα IPv6, καταγράψτε την τιμή του πεδίου Next Header.]

- ➢ TCP : 6 (=06_{16})
- ➢ UDP : 17 (=11_{16})

3.4 Ποια είναι τα ονόματα των πεδίων της επικεφαλίδας των τεμαχίων TCP και δεδομενογραμμάτων UDP που είναι κοινά και στα δύο πρωτόκολλα;
Τα κοινά και στα δύο πρωτόκολλα πεδία των επικεφαλίδων τους είναι:

- Source port
- Destination port

TCP: *Βασικό χαρακτηριστικό του είναι ότι κάθε byte μιας σύνδεσης TCP έχει τον δικό του αριθμό ακολουθίας των 32 bit. Το τμήμα TCP αποτελείται από μία σταθερή κεφαλίδα των 20 bytes η οποία ακολουθείται από bytes δεδομένων. Πιο αξιόπιστο από το UDP*

UDP: *Ασυνδεσμικό πρωτόκολλο που παρέχει στις εφαρμογές μία μέθοδο για την αποστολή ενθυλακωμένων αυτοδύναμων πακέτων IP χωρίς να χρείαζεται να εγκαθιδρύσουν σύνδεση.*

QUIC: *Πρωτόκολλο που σχεδιάστηκε με σκοπό την βελτίωση της διεκπεραιωτικής ικνανότητας και καθυστέρησης του TCP. Βελτίωση της απόδοσης ειδικά συνδέσμων με μεγάλα ποσοστά σφαλμάτων μετάδοσης.*

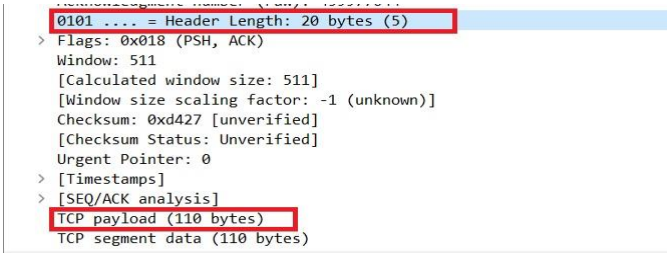
- Checksum

3.5 Ποιο είναι το μήκος σε byte της επικεφαλίδας των δεδομενογραμμάτων UDP;
8 bytes.

3.6 Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος των δεδομενογραμμάτων UDP;
Το πεδίο Length.

3.7 Ποιο πεδίο καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP και ποια η θέση του στην επικεφαλίδα;
Υπάρχει το πεδίο Header Length(1 byte) που έχει τιμή 5 (words των 32 bit δηλαδή 20 bytes μηκος TCP επικεφαλίδας) και μέγεθος 1 byte, το 13ο byte από την αρχή της επικεφαλίδας.

3.8 Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος τεμαχίων TCP; Εάν όχι, πώς προκύπτει αυτό; Προσοχή, οι γραμμές εντός αγκυλών [και] στο παράθυρο με τις λεπτομέρειες δεν αντιστοιχούν σε επικεφαλίδες αλλά προκύπτουν από την ανάλυση που κάνει το Wireshark.
Όχι, δεν υπάρχει. Το συνολικό μήκος τεμαχίων προκύπτει ως άθροισμα του TCP payload και του Header Length.



3.9 Υπάρχει πεδίο στην επικεφαλίδα TCP ή UDP που να προσδιορίζει τον τύπο του πρωτοκόλλου εφαρμογής; Αιτιολογήστε την απάντησή σας. [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm (αναζητήστε την στο Internet Archive) επιλέγοντας το “TCP/UDP ports” από το αριστερό της μέρος.]
Υποδηλώνεται από τα Source και Destination Ports. Για παράδειγμα, όταν το application layer είναι DNS τότε για πακέτα που φτάνουν στον υπολογιστή μου το Source Port είναι 53 και για πακέτα που φεύγουν από τον υπολογιστή μου το Destination Port είναι 53.

3.10 Αναφέρετε άλλα πρωτόκολλα στρώματος εφαρμογής που τυχόν παρατηρήσατε.
Τα στρώματα εφαρμογής(application layers) που παρατηρήσαμε ήτανε τα εξής:

- DNS(Domain Name System)
- HTTP(Hyper Text Transfer Protocol)
- SNMP(Simple Network Management Protocol)

4. Application Layer

4.1 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το DNS;
Το UDP.

4.2 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το HTTP;
Το TCP.

4.3 Ποιο bit της σημαίας (flag) στην επικεφαλίδα DNS καθορίζει το κατά πόσον πρόκειται για ερώτηση ή απάντηση και ποια η αντίστοιχη τιμή; [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm (αναζητήστε την στο Internet Archive) για τη δομή της επικεφαλίδας του πρωτοκόλλου DNS επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο DNS στο δεξιό της μέρος.]
Το 1ο bit από το πεδίο flags της επικεφαλίδας DNS:

- **0 για ερώτηση**
- **1 για απάντηση**

4.4 Καταγράψτε τη θύρα προορισμού των ερωτήσεων DNS.
Destination port για DNS query : 53

4.5 Καταγράψτε τις θύρες πηγής (προέλευσης) των ερωτήσεων DNS.
Source port για DNS query : 49210, 52779, 58186, 61105

4.6 Καταγράψτε τη θύρα πηγής (προέλευσης) των απαντήσεων DNS.
Source port για DNS response : 53

4.7 Καταγράψτε τις θύρες προορισμού των απαντήσεων DNS.
Destination port για DNS response : 49210, 52779, 58186, 61105

4.8 Τι παρατηρείτε για τη σχέση των θυρών προέλευσης των ερωτήσεων με τις θύρες προορισμού των απαντήσεων;
Οι θύρες προέλευσης ερωτήσεων ταυτίζονται με τις θύρες προορισμού των απαντήσεων.

4.9 Ποια είναι η πασίγνωστη θύρα όπου ακούει ο εξυπηρετητής DNS;
Η θύρα(port) 53.

4.10 Καταγράψτε τη θύρα προορισμού των μηνυμάτων HTTP που παράγει ο υπολογιστής σας.
Destination port για http requests: 80

4.11 Καταγράψτε τις θύρες πηγής (προέλευσης) των μηνυμάτων HTTP που έστειλε ο υπολογιστής σας.
Source port για http requests: 54084

4.12 Καταγράψτε τη θύρα πηγής (προέλευσης) των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού.
Source port για http responses: 80

4.13 Καταγράψτε τις θύρες προορισμού των απαντήσεων αυτών.
Destination port για http responses: 54084

4.14 Ποια είναι η πασίγνωστη θύρα όπου ακούει ο εξυπηρετητής HTTP;
Η θύρα 80.

4.15 Τι παρατηρείτε για τη σχέση των θυρών προέλευσης των μηνυμάτων HTTP με τις θύρες προορισμού των αντίστοιχων απαντήσεων του εξυπηρετητή ιστού;

Οι θύρες προέλευσης ερωτήσεων(Destination port of queries) ταυτίζονται με τις θύρες προορισμού των απαντήσεων(Source port of responses).

4.16 Ποια είναι η ονομασία του πρώτου μηνύματος (μεθόδου) HTTP από τον υπολογιστή σας προς τον εξυπηρετητή ιστού; [Υπόδειξη: Για τη δομή της επικεφαλίδας του πρωτοκόλλου HTTP συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm (αναζητήστε την στο Internet Archive) επιλέγοντας το “IP protocol suite” από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο HTTP στο δεξιό της μέρος.]

GET /lab2/ HTTP/1.1

4.17 Ποιος είναι ο κωδικός κατάστασης που επιστρέφει ο εξυπηρετητής ιστού στην απάντησή του;

Status code : 200

4.18 Γιατί χρειάζονταν η εκτέλεση της εντολής ipconfig /flushdns σε περίπτωση που είχατε ήδη επισκεφθεί την παραπάνω ιστοσελίδα.

Με την εντολή ipconfig /flushdns καθαρίζει η cache από DNS αρχεία, ώστε νέα DNS requests να μην απαντηθούν από την cache σε περίπτωση που την είχαμε φορτώσει σε προηγούμενο session την ίδια σελίδα αλλά από τον DNS server.