Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ	**ΑΜ: 03119005**	**Ομάδα: 4**
Όνομα PC/ΛΣ: ΥΠΟΛΟΓΙΣΤΗΣ ΣΧΟΛΗΣ / WINDOWS		**Ημερομηνία: 15/10/2022**
Διεύθυνση IP:147.102.38.175	**Διεύθυνση MAC: 00-1D-09-0C-E5-E4**	

Άσκηση 1:

1.1: Το φίλτρο μας δείχνει μόνο πακέτα πρωτοκόλλου ARP ή IP.

1.2: Ονόματα πεδίων επικεφαλίδας του Ethernet: Destination, Source, Type
Τα πεδία αυτά τα βλέπουμε ανοίγοντας στο Wireshark το menu Ethernet II ενός πακέτου.

1.3: Πεδίο για το συνολικό μήκος πλαισίου: Το Wireshark έχει το πεδίο Frame #N (Frame Number) το οποίο μας πληροφορεί για το συνολικό μήκος του πλαισίου.
Πεδίο για το μήκος των μεταφερόμενων δεδομένων: Σε κάποια πακέτα υπάρχει ξεχωριστό πεδίο Data που έχει αυτήν την πληροφορία, ενώ σε κάποια άλλα πακέτα πρέπει πρώτα να ανοίξουμε το Internet Control Message Protocol και εκεί να βρούμε το πεδίο Data (όπως συμβαίνει με τα μηνύματα ICMP σε αυτήν την άσκηση).

1.4: Μήκος Ethernet Address: 6 bytes (είναι η MAC Address)

1.5: Στο Wireshark διαλέγουμε το πεδίο Ethernet II και στην περιοχή που μας δείχνει ποια byte του πλαισίου καταλαμβάνει βλέπουμε μετρώντας τα ότι είναι 14 byte.
Destination = 6 bytes
Source = 6 bytes
Type = 2 bytes

1.6: Πεδίο του πλαισίου Ethernet που καθορίζει το πρωτόκολλο δικτύου: Type

1.7: Θέση που καταλαμβάνει το Type μέσα στην επικεφαλίδα: Τα πρώτα 12 bytes είναι οι δύο Ethernet Addresses και τα τελευταία 2 bytes είναι το Type.

1.8: Τιμή Type για IPv4 πακέτα: Στο Wireshark ανοίγουμε ένα πακέτο IPv4 και πάμε στην Ethernet επικεφαλίδα του. Εκεί βλέπουμε ότι το πεδίο Type έχει τιμή 0x0800 για πακέτα Ipv4.

1.9: Βάζοντας στο φίλτρο σκέτο arp δεν εμφανίζεται κάποιο πακέτο. Δεν καταγράφηκαν τέτοια πακέτα.

Άσκηση 2:

2.1: Σημασία φίλτρου που εφαρμόσαμε: Εμφανίζει μόνο πακέτα πρωτοκόλλου ICMP.

2.2: Μήκος διευθύνσεων IPv4: 4 bytes

2.3: Ονόματα δύο πρώτων πεδίων της επικεφαλίδας IPv4: Version, Header Length

2.4: Μήκος των πεδίων αυτών: 4 bit το καθένα
Η τιμή των πεδίων αυτών:
Version: αναγράφει την μορφή της επικεφαλίδας του IP πακέτου
(Internet) Header Length: αναγράφει το μήκος την επικεφαλίδας IP σε πλήθος 32 – bit λέξεων.
Η ελάχιστη τιμή του είναι 5.

2.5: Επιλέγουμε το πρώτο πακέτο IPv4 το οποίο στείλαμε.
Συνολικό μήκος επικεφαλίδας IPv4: 20 bytes

2.6: Πως προκύπτει το μήκος από την τιμή του αντίστοιχου πεδίου της επικεφαλίδας IPv4: Το πεδίο είναι το Header Length. Για το πακέτο αυτό έχει τιμή 5. Με βάση το 2.4 ερώτημα συμπεραίνουμε ότι η επικεφαλίδα έχει μήκος 5 * 32 = 160 bit = 160/8 = 20 bytes

2.7: Συνολικό μήκος: 60 bytes (χωρίς την Ethernet επικεφαλίδα)

2.8: Πεδίο σχετικό με το μήκος του IPv4 πακέτου στην επικεφαλίδα: Υπάρχει το Total Length πεδίο, το οποίο περιέχει το μήκος του πακέτου αυτού. Η τιμή του είναι 0x003c = 3 * 16 + 12 = 60. Η τιμή του συμφωνεί με το μήκος που βρήκα προηγουμένως.

2.9: Μήκος δεδομένων του πακέτου IPv4: 40 bytes

2.10: Πώς προκύπτει το μήκος αυτό: Total Length – Header Length = 60 – 40 = 20 bytes

2.11: Πεδίο της επικεφαλίδας IPv4 που καθορίζει το πρωτόκολλο του ανωτέρου στρώματος της σουίτας TCP/IP: Το πεδίο Protocol (έχει μήκος 1 byte)

2.12: Θέση του σε σχέση με την αρχή της επικεφαλίδας: Είναι το 10ο byte της επικεφαλίδας

2.13: Τιμή Protocol πεδίου για το πρωτόκολλο ICMP: 0x01. Το βλέπουμε από τα δεδομένα του Wireshark.

Τα επόμενα ερωτήματα τα έκανα στο σπίτι, δεν πρόλαβα στο εργαστήριο.

Όνομα PC/ΛΣ: dimitris-Laptop / WINDOWS 11 HOME	
Διεύθυνση IP: 192.168.2.6	**Διεύθυνση MAC: 7C-8A-E1-C3-47-5C**

Άσκηση 3:

3.1: Σημασία του φίλτρου απεικόνισης: δείχνει πακέτα tcp ή udp (ή πακέτα που ενθυλακώνουν αυτά τα πρωτόκολλα)

3.2: Πρωτόκολλα του στρώματος μεταφοράς: Εμφανίζονται πακέτα TCP, UDP.

3.3: Τιμή πεδίου Protocol στην επικεφαλίδα του IPv4 για το TCP: 0x06
Τιμή πεδίου Protocol στην επικεφαλίδα του IPv4 για το UDP: 0x11

3.4: Πεδία επικεφαλίδας TCP:

- Source Port
- Destination Port
- Sequence Number
- Acknowledgment Number
- Data Offset
- ECN
- Control Bits
- Window
- Checksum
- Urgent Pointer

Πεδία επικεφαλίδας UDP:

- Source Port
- Destination Port
- Length
- Checksum

Κοινά είναι τα πεδία Source Port, Destination Port, Checksum.

3.5: Μήκος επικεφαλίδας UDP: 8 bytes

3.6: Πεδίο επικεφαλίδας UDP για το συνολικό μήκος του δεδομενογράμματος: Length

3.7: Πεδίο μήκους επικεφαλίδας TCP: Το πεδίο Data Offset (ή Header Length στο Wireshark) αναγράφει το πλήθος των 32 – bit λέξεων που εμπεριέχονται στην επικεφαλίδα του TCP. Επομένως, από το πεδίο αυτό πληροφορούμαστε για το μήκος της επικεφαλίδας. Είναι το 5^{ο} πεδίο της επικεφαλίδας και αποτελεί τα 4 πρώτα bit του 13^{ου} byte της επικεφαλίδας.

3.8: Πεδίο στην επικεφαλίδα του τεμαχίου TCP για το συνολικό μήκος: Δεν υπάρχει τέτοιο πεδίο. Η πληροφορία για το μέγεθος προκύπτει αν από το συνολικό μέγεθος του πακέτο αφαιρέσουμε το μέγεθος της επικεφαλίδας. Από το πακέτο IPv4 παίρνουμε το Total Length και το Header Length του και αφαιρώντας το δεύτερο από το πρώτο βρίσκουμε το μέγεθος του πακέτου TCP.

Ως υποσημείωση εδώ: το Wireshark βρίσκει το Segment Length, το οποίο προκύπτει αν από το παραπάνω αποτέλεσμα αφαιρέσουμε το μέγεθος της επικεφαλίδας το οποίο βρίσκουμε από το πεδίο Data Offset.

3.9: Από τα πεδία Source Port και Destination Port μπορούμε να καταλάβουμε ποιο πρωτόκολλο στρώματος εφαρμογής (application layer) χρησιμοποιείται, γιατί συγκεκριμένες θύρες χρησιμοποιούνται για συγκεκριμένες υπηρεσίες.

3.10: Πρωτόκολλα στρώματος εφαρμογής που παρατηρούμε: DNS, HTTP.

Άσκηση 4:

4.1: Πρωτόκολλο μεταφοράς που χρησιμοποιεί το DNS: UDP

4.2: Πρωτόκολλο μεταφοράς που χρησιμοποιεί το HTTP: TCP

4.3: Bit σημαίας της επικεφαλίδας DNS που καθορίζει ερώτηση/απάντηση: Το QR bit της σημαίας καθορίζει να πρόκειται για ερώτηση ή απάντηση. Είναι το πρώτο bit της σημαίας και οι τιμές του αντιστοιχίζονται ως:

0 → ερώτηση
1 → απάντηση

4.4: Θύρα προορισμού των ερωτήσεων DNS: 53

4.5: Θύρες πηγής ερωτήσεων DNS: 59984 (είχε μόνο μία)

4.6: Θύρα πηγής των απαντήσεων DNS: 53

4.7: Θύρες προορισμού των απαντήσεων DNS: 59984 (είχε μόνο μία)

Επειδή υπήρχε για κάποιο λόγο κάθε φορά μόνο ένα ζευγάρι query – response, επέλεξα να κάνω capture πολλές φορές το άνοιγμα το συνδέσμου αυτού στο διαδίκτυο και να καταγράψω τις τιμές της θύρας πηγής ερωτήσεων/ προορισμού απαντήσεων κάθε φορά (πάνω δείχνω το αποτέλεσμα από μία μόνο φορά).

4.8: Σχέση θυρών προέλευσης (πηγή) ερωτήσεων και θύρες προορισμού απαντήσεων: Ταυτίζονται

4.9: Θύρα όπου ακούει ο εξυπηρετητής DNS: 53

4.10: Θύρα προορισμού μηνυμάτων HTTP που έστειλε ο υπολογιστής μου: 80

4.11: Θύρες προέλευσης των μηνυμάτων HTTP που έστειλε ο υπολογιστής μου: 62801
(και τα δύο μηνύματα στάλθηκαν από αυτή τη θύρα)

4.12: Θύρα προέλευσης των απαντήσεων: 80

4.13: Θύρες προορισμού των απαντήσεων: 62801

4.14: Θύρα όπου ακούει ο εξυπηρετητής HTTP: 80

4.15: Οι θύρες αυτές ταυτίζονται

4.16: GET /lab2/ HTTP/1.1

4.17: 200, από το όνομα HTTP/1.1 200 OK του μηνύματος απάντησης

4.18: Δοκιμάσαμε να επισκεφθούμε την παραπάνω σελίδα χωρίς την εκτέλεση της εντολής. Τα αποτελέσματα επαληθεύουν την ακόλουθη παρατήρηση:

Πρέπει κάπως να βρούμε την IP της σελίδας στην οποία θέλουμε να έχουμε πρόσβαση. Τον ρόλο της απόκτησης της πληροφορίας αυτής αναλαμβάνουν τα DNS πακέτα, τα οποία στέλνονται στην αρχή. Αν δεν είχαμε κάνει flush τότε θα υπήρχε ήδη αποθηκευμένη η IP αυτή άρα δεν θα είχαμε ανάγκη εκ νέου απόκτησής της άρα δεν θα παρατηρούσαμε DNS πακέτα στο capture.