Ονοματεπώνυμο: Ανδρέας Στάμος (03120***)	**Ομάδα:** 1
Όνομα PC/ΛΣ: linux / Ubuntu 22.04.2 LTS	**Ημερομηνία:** 10/10/2023
Διεύθυνση IP: 192.168.1.10	**Διεύθυνση MAC:** DE–3F–DC–B2–E0–D0

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 Να εμφανιστούν τα πακέτα που περιέχουν δεδομένα είτε του πρωτοκόλλου ARP είτε του πρωτοκόλλου IP

1.2 Destination, Source, Type

1.3 Όχι

1.4 6 bytes

1.5 14 bytes

1.6 Το Type

1.7 13ο-14ο byte

1.8 0x0800

1.9 0x0806

Άσκηση 2

2.1 Να εμφανιστούν τα πακέτα που περιέχουν δεδομένα του πρωτοκόλλου ICMP

2.2 4 bytes

2.3 Version, Header Length

2.4 Version 4 bits με τιμή 0b0100=4 και Header Length 4 bits με τιμή 0b0101=5

2.5 20 bytes

2.6 Το Header Length εκφράζεται ως πλήθος 32-bit=4-byte λέξεων. Άρα εδώ η επικεφαλίδα έχει μέγεθος $5 \cdot 4 =$ 20 bytes, όπως πράγματι και έχει.

2.7 84 bytes

2.8 Υπάρχει το Total Length και η τιμή του συμφωνεί με αυτό που μετρήθηκε στο 2.7

2.9 64 bytes

2.10 μέγεθος δεδομένων = Total Length − Header Length = 84 bytes − 20 bytes = 64 bytes

2.11 Το Protocol

2.12 10ο byte

2.13 0x01

Άσκηση 3

3.1 Να εμφανιστούν τα πακέτα που περιέχουν δεδομένα ή του πρωτοκόλλου TCP ή του πρωτοκόλλου UDP

3.2 TCP και UDP

3.3 Για το TCP είναι 0x06 και για το UDP είναι 0x17

3.4 Source Port, Destination Port, Checksum

3.5 8 bytes

3.6 Ναι το Length.

3.7 Ναι το Header Length που είναι τα 4 MSB bits του 13ου byte.

3.8 Όχι. Ο αποστολέας γράφει στο Sequence Number την θέση στο μήνυμα που αντιστοίχει το 1ο byte του segment. Ο παραλήπτης μετράει το μέγεθος του Payload και αφού επαληθεύσει το checksum στέλνει επόμενο tcp packet με:

$$\text{Acknowledgment Number} = \text{Sequence Number του πακέτου που παραλήφθηκε} + \text{μέγεθος του payload που παραλήφθηκε} + 1$$

δηλαδή την θέση 1ου byte μηνύματος που ακόμα δεν έχει λάβει. Άρα:

$$\text{Μέγεθος μήνυματος} = \text{Acknowledgment Number επόμενου πακέτου [Receiver} \rightarrow \text{Sender]} - \text{Sequence Number [Sender} \rightarrow \text{Receiver]} - 1$$

Η τιμή αυτή ταιριάζει με αυτή που μετράμε για το payload του πακέτου στο Wireshark.
Το Wireshark λογικά απλά μετράει το μέγεθος του Payload και δεν χρειάζεται να κάνει την παραπάνω αφαίρεση.

3.9 Για τις well-known εφαρμογές το port υποδηλώνει τον τύπο του πρωτοκόλλου εφαρμογής. πχ. 80 για HTTP, 443 HTTPS, 53 DNS

3.10 DNS, HTTP

Άσκηση 4

4.1 UDP

4.2 TCP

4.3 Αν το MSB (1ο) bit των σημαιών (flags) είναι 0, πρόκειται για ερώτηση, ενώ αν είναι 1 πρόκειται για απάντηση

4.4 53

4.5 41312, 48797, 60610

4.6 53

4.7 48797, 41312, 60610

4.8 Η απάντηση ενός ερωτήματος πηγαίνει (θύρα προορισμού) στην θύρα από όπου έγινε η ερώτηση (θύρα προέλευσης)

4.9 53

4.10 80

4.11 46092

4.12 80

4.13 46092

4.14 80

4.15 Η απάντηση ενός αιτήματος πηγαίνει (θύρα προορισμού) στην θύρα από όπου έγινε το αίτημα (θύρα προέλευσης)

4.16 GET

4.17 200

4.18 Επειδή το Linux μέσω του deamon systemd-resolved αποθηκεύει σε cache τα αποτελέσματα DNS Query Response που λαμβάνονται, οπότε όταν γίνει ερώτημα για γνωστό domain δεν στέλνει DNS Query στον DNS Server αλλά το απαντάει απευθείας από την cache. Εμείς όμως θέλαμε να δούμε το DNS Query προς τον DNS Server.