

Όνοματεπώνυμο:	Ζευγολατάκος Παναγιώτης	Ομάδα: 3
Όνομα PC/ΛΣ:	panos-PC / Windows 10	Ημερομηνία: 13/10/2020
Διεύθυνση IP: 192.168.10.24	Διεύθυνση MAC: D0-50-99-75-F8-F8	

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 Με τη χρήση αυτού του φίλτρου εμφανίζονται τα πλαίσια με πρωτόκολλα IP ή ARP.

1.2

Destination: ThomsonT_d7:d3:c6 (00:24:17:d7:d3:c6)

Source: ASRockIn_75:f8:f8 (d0:50:99:75:f8:f8)

Type: IPv4 (0x0800)

1.3 Όχι, δεν υπάρχει.

1.4 Το μήκος των διευθύνσεων Ethernet είναι 6 Bytes (00:24:17:d7:d3:c6)

1.5 Το συνολικό μήκος της επικεφαλίδας Ethernet είναι 14 Bytes.

1.6 Το πεδίο του πλαισίου Ethernet που καθορίζει το πρωτόκολλο δικτύου είναι το Type.

1.7 Το τελευταίο πεδίο, που αποτελείται από 2 Bytes.

1.8 0x0800

1.9 0x0806

Άσκηση 2

2.1 Εμφανίζει τα πλαίσια που μεταδόθηκαν με πρωτόκολλο ICMP.

2.2 Το μήκος των διευθύνσεων IPv4 είναι 4 Bytes.

2.3 Πρώτα είναι το Version και μετά το IHL (Internet Header Length)

2.4 Είναι και τα δύο 4-bit αριθμοί και οι τιμές τους είναι: Version=4 και IHL=5

2.5 20 Bytes.

2.6 Πολλαπλασιάζουμε την τιμή του πεδίου IHL με το 4, έτσι ώστε να βρούμε το μέγεθος της επικεφαλίδας σε Bytes.

.... 0101 = Header Length: 20 bytes (5)

2.7 60 Bytes (Total Length: 60).

2.8 Ναι, υπάρχει, το Total Length και συμφωνεί με το μήκος που βρήκα προηγουμένως, επειδή το μέγεθος πακέτου IPv4 είναι ίσο με το μέγεθος του πλαισίου Ethernet – την επικεφαλίδα του (74-14, άρα 60).

2.9 40 Bytes.

2.10 Payload = Total Length – IHL (Internet Header Length)

2.11 Το πεδίο Protocol.

2.12 Είναι τα bit 72-79 (10^ο Byte).

2.13 0x0001

Άσκηση 3

3.1 Μας δίνει όλα τα πακέτα που μεταδόθηκαν με πρωτόκολλο TCP ή UDP.

3.2 Πρωτόκολλα TCP, UDP.

3.3 TCP: 6
UDP: 17

3.4 Source Port, Destination Port, Checksum.

3.5 8 Bytes.

3.6 Ναι, το πεδίο Length.

3.7 Ναι, το Data Offset (στο Wireshark 'Header Length') και είναι τα 4MSB από το 13^ο Byte.

3.8 Όχι, δεν υπάρχει τέτοιο πεδίο στην επικεφαλίδα, αλλά προκύπτει αν από το Total Length του IPv4 αφαιρέσουμε την επικεφαλίδα του. Είναι, δηλαδή, το Payload.

3.9 Ναι, υπάρχουν δύο, το Source Port (request) και το Destination Port (response). Αυτά αντιστοιχούν σε μια υπηρεσία.

3.10 HTTP: 80
HTTPS: 443
DNS: 53
NBNS: 137

Άσκηση 4

4.1 Το πρωτόκολλο UDP.

4.2 Το πρωτόκολλο TCP.

4.3 Το MSB του 3^{ου} Byte και για ερώτηση είναι 0, ενώ για απάντηση είναι 1.

4.4 Port 53.

4.5 Port 60047.

4.6 Port 53.

4.7 Port 60047.

4.8 Ταυτίζονται.

4.9 Port 53.

4.10 Port 80.

4.11 Port 52220.

4.12 Port 80.

4.13 Port 52220.

4.14 Port 80.

4.15 Ταυτίζονται.

4.16 GET /lab2/ HTTP/1.1

4.17 HTTP /1.1 200 OK

4.18 Τα Windows αποθηκεύουν cache για called and resolved διευθύνσεις σελίδων. Επομένως, πρέπει να κάνουμε flush την DNS cache αν θέλουμε να δούμε το internet trafficking.

(Σημείωση: στα 4.5, 4.7, 4.11 και 4.13, λόγω του μεγάλου αριθμού των απαντήσεων επέλεξα να βάλω μόνο της ζητούμενης ιστοσελίδας του μαθήματος)