

**δικτυα υπολογιστων**

**Εργαστηριακη ασκηση 2: Ενθυλακωση και επικεφαλιδεσ**





18 οκτωβριου, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | | **Ομάδα:** 2 |
| **Όνομα PC/ΛΣ:** DESKTOP-JGHL94V/ WINDOWS 10 | | **Ημερομηνία:** 18/10/2022 |
| **Διεύθυνση IP:** 192.168.1.5 | **Διεύθυνση MAC:** 70-85-C2-88-FD-B1 | |

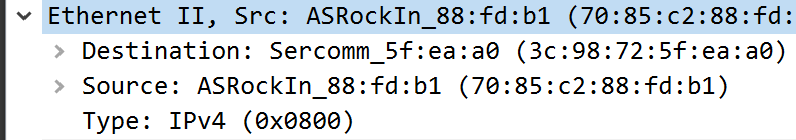
\*\* Η εργασία ξεκίνησε στο PCLAB της σχολής αλλά λόγω περιορισμού δικαιωμάτων χρήστη στο pc επέλεξα να ξανακάνω από την αρχή την εργασία στον προσωπικό μου υπολογιστή. \*\*

**Άσκηση 1: Στρώμα ζεύξης δεδομένων**

***1.1***

Το φίλτρο «arp or ip» μας εμφανίζει τα πλαίσια που διέπονται είτε από το πρωτόκολλο ARP είτε το IPv4.

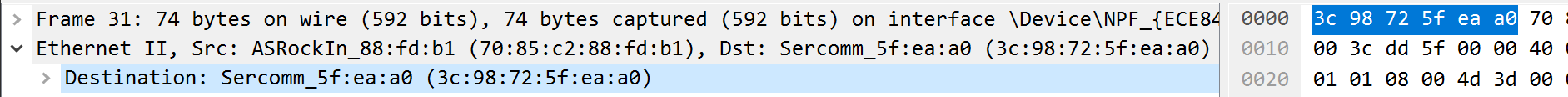
***1.2***

Οι επικεφαλίδες είναι: Destination, Source και Type.

***1.3***

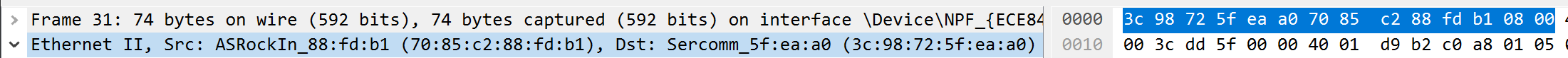
Όχι, δεν εμφανίζεται κάποιο σχετικό πεδίο.

***1.4***

Το μήκος των διευθύνσεων Ethernet είναι 6 bytes (6 διψήφιοι δεκαεξαδικόι αριθμοί για διεύθυνση MAC).

***1.5***

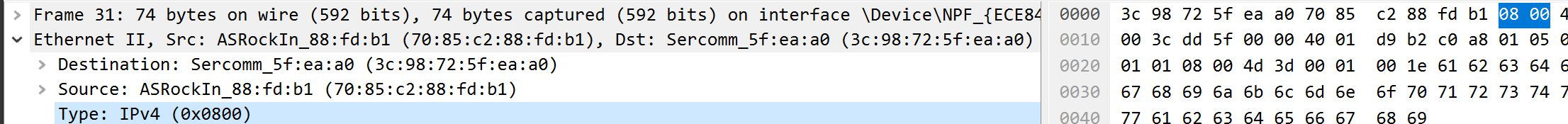
Το συνολικό μήκος της επικεφαλίδας Ethernet είναι 14 bytes (6 bytes Destination, 6 bytes Source και 2 Bytes Type).



***1.6***

Το πεδίο Type καθορίζει το πρωτόκολλο δικτύου (π.χ. 0x0806 για ARP, 0x0800 για IP).

***1.7***

Καταλαμβάνει τα δύο τελευταία byte της επικεφαλίδας Ethernet.

***1.8***

Το πεδίο αυτό για πακέτα IPv4 έχει τιμή 0x0800.

***1.9***

Δοκιμάζουμε σαν φίλτρο αντί για «arp or ip» σκέτο «arp» και δεν εμφανίζεται καμία καταγραφή. Εκτελώντας άλλες καταγραφές όμως, βρίσκουμε πως η τιμή θα ήταν 0x0806.

**Άσκηση 2: Στρώμα ζεύξης δεδομένων**

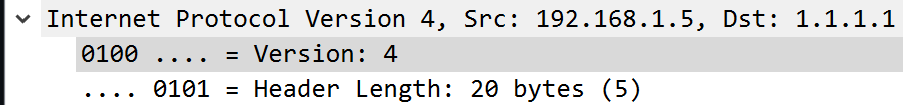
***2.1***

Το φίλτρο «icmp» εμφανίζει τα πακέτα του Στρώματος δικτύου που διέπονται από το πρωτόκολλο ICMP.

***2.2***

Οι διευθύνσεις στο πρωτόκολλο IPv4 έχουν μήκος 4 bytes (0.0.0.0 έως 255.255.255.255)

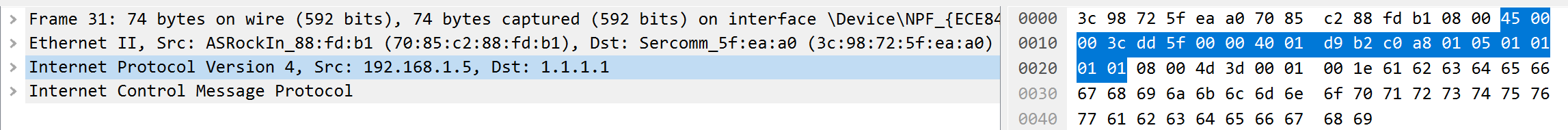
***2.3***

Το πρώτο πεδίο είναι το version και το δεύτερο είναι το Header Length.

***2.4***

Το κάθε πεδίο έχει μήκος 4 bit και έχουν τιμές Version και Header Length .

***2.5***

Επιλέγουμε ένα τυχαίο πακέτο και κάνουμε κλικ στην επικεφαλίδα του IPv4. Στα περιεχόμενα βλέπουμε ότι υπογραμμίζονται 20 διψήφιοι δεκαεξαδικόι αριθμοί. Άρα, η επικεφαλίδα IPv4 έχει μήκος 20 bytes.

***2.6***

Έχουμε από πριν ότι Header Length . Σύμφωνα με το Documentation, το Header Length: *“Specifies the length of the IP packet header in 32 bit words”*. Συνεπώς θα ισχύει ότι (32 bits = 4 bytes) bytes.

***2.7***

Πατώντας την επικεφαλίδα του Ethernet Layer, βρίσκουμε ότι καταλαμβάνει 14 bytes από τα συνολικά 74 bytes (on wire) του πλαισίου. Άρα, 60 bytes αντιστοιχούν στο πακέτο IPv4, θεωρώντας ότι το ICMP πρωτόκολλο είναι μέρος του IP Layer.

***2.8***

Ναι, υπάρχει το πεδίο total length που περιέχει την τιμή του συνολικού μήκους του datagram.

***2.9***

Το payload του πακέτου έχει μήκος 40 bytes.

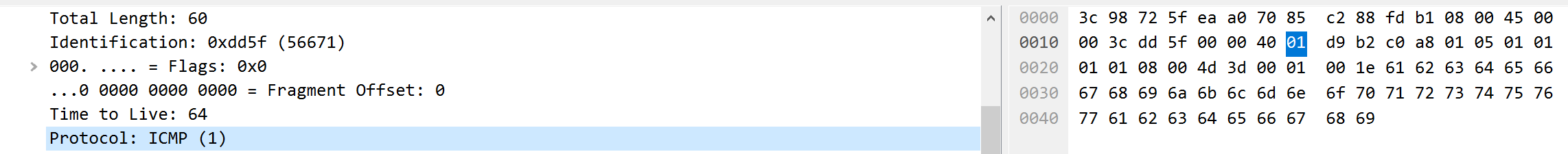
***2.10***

Το payload του πακέτου IPv4 προκύπτει αν από το Total Length του πακέτου (60 bytes) αφαιρέσουμε το Header Length (20 bytes).

***2.11***

Το πεδίο Protocol της επικεφαλίδας IPv4 καθορίζει το πρωτόκολλο ανωτέρου στρώματος.

***2.12***

Το πεδίο αυτό βρίσκεται στο 10ο byte της επικεφαλίδας IPv4.

***2.13***

Για το πρωτόκολλο ICMP η τιμή του είναι 1.

**Άσκηση 3: Στρώμα Μεταφοράς**

***3.1***

Το φίλτρο «tcp or udp» εμφανίζει τα πακέτα τα οποία ενθυλακώνουν είτε το πρωτόκολλο TCP είτε το UDP στο στρώμα μεταφοράς τους.

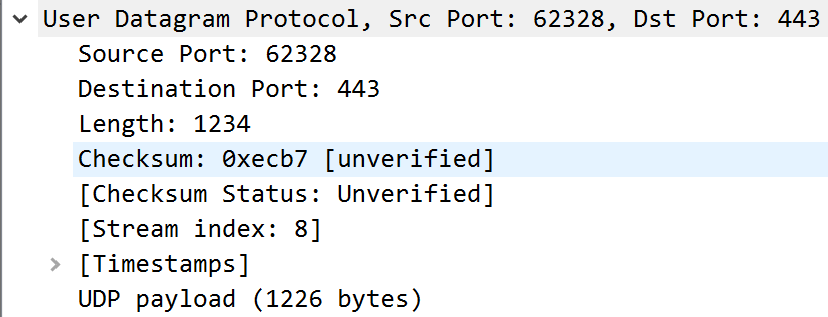
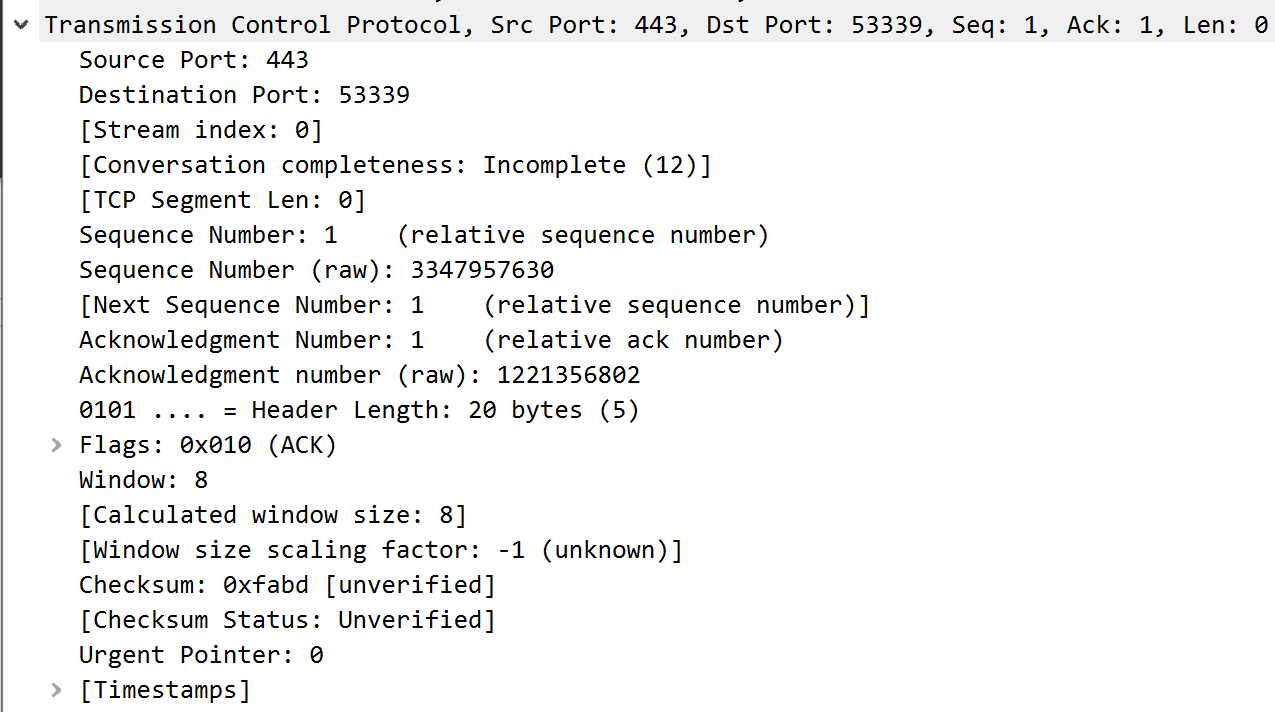
***3.2***

Παρατηρούμε τα πρωτόκολλα TCP Και UDP του στρώματος μεταφοράς.

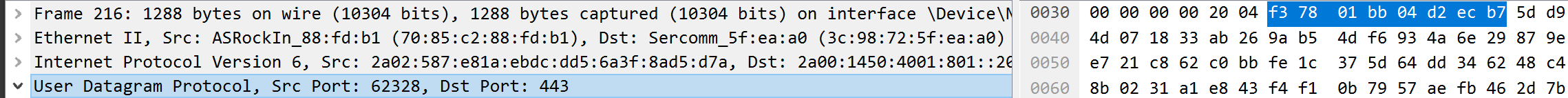
***3.3***

Για πακέτα που μεταφέρονται με πρωτόκολλο TCP, στο πεδίο protocol έχουν τιμή 6, ενώ αυτά που μεταφέροντα με UDP (IPv6 protocol) έχουν τιμή 17.

***3.4***

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

***3.5***

Το μήκος της επικεφαλίδας UDP είναι 8 bytes.

***3.6***

Ναι, υπάρχει το πεδίο Length που μας δίνει το συνολικό μήκος των UDP datagrams.

***3.7***

Το πεδίο Header Length στην επικεφαλίδα IPv4 μας πληροφορεί για το μήκος της επικεφαλίδας και βρίσκεται στα πρώτα 4 bits του 13ου byte της επικεφαλίδας TCP.

***3.8***

Όχι δεν υπάρχει πεδίο που να μας πληροφορεί για το συνολικό μήκος των τεμαχίων TCP. Αυτό μπορεί να προκύψει αφαιρώντας την τιμή του πεδίου Header Length από την τιμή του πεδίου Total Length της επικεφαλίδας IPv4.

***3.9***

Στην επικεφαλίδα TCP υπάρχει η θύρα 443 (HTTPS, HTTP over SSL/TLS) είτε ως Source είτε ως Destination. Όμοια και στην επικεφαλίδα UDP υπάρχει η θύρα 443 πάλι είτε ως Source είτε ως Destination.

***3.10***

Παρατηρήσαμε επίσης (με την ίδια διαδικασία με το προηγούμενο ερώτημα) ορισμένες επικεφαλίδες TCP με την θύρα 80 (HTTP). Ακόμη παρατηρήσαμε πακέτα που ενθυλακώνουν το πρωτόκολλο στρώματος εφαρμογής DNS.

**Άσκηση 4: Στρώμα Εφαρμογής**

***4.1***

Παρατηρούμε ότι το DNS χρησιμοποιεί το πρωτόκολλο του στρώματος μεταφοράς UDP.

***4.2***

Παρατηρούμε ότι το HTTP χρησιμοποιεί το πρωτόκολλο του στρώματος μεταφοράς TCP.

***4.3***

Το 17o bit (πεδίο QR) καθορίζει αν είναι Query (τιμή 0) ή Response (τιμή 1).

***4.4***

Η θύρα προορισμού των DNS ερωτήσεων είναι η 53 (DNS, Domain Name System).

***4.5***

Οι θύρες πηγής των DNS ερωτήσεων είναι: 51970, 58062, 62516, 64865, 63536, 57521, 54333, 59083, 64759, 61710, 60674, 62357, 56309

***4.6***

Η θύρα πηγής των DNS απαντήσεων είναι η 53.

***4.7***

Οι θύρες προορισμού των DNS απαντήσεων είναι: 51970, 58062, 62516, 64865, 63536, 57521, 54333, 59083, 64759, 61710, 60674, 62357, 56309 (προφανώς οι ίδιες με τις θύρες πηγής των DNS ερωτήσεων)

***4.8***

Παρατηρούμε ότι οι θύρες προέλευσης των DNS ερωτήσεων είναι οι θύρες των DNS απαντήσεων και αντιστρόφως, η θύρα προορισμού των DNS ερωτήσεων είναι η θύρα προέλευσης των DNS απαντήσεων.

***4.9***

Εύκολα συμπεραίνουμε από τις παραπάνω παρατηρήσεις (και με βάση το documentation TCP/UDP ports) ότι η πασίγνωστη θύρα που ακούει ο DNS Server είναι η 53.

***4.10***

Τα HTTP μηνύματα που παράγει ο υπολογιστής μας (source IP είναι η IP του υπολογιστή μας) έχουν ως Destination Port την θύρα 80 (HTTP, HyperText Transfer Protocol).

***4.11***

Οι θύρες πηγής των HTTP μηνυμάτων που έστειλε ο υπολογιστής μας είναι οι 53461 και 50858.

***4.12***

Η θύρα πηγής των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού είναι η 80.

***4.13***

Οι θύρες προορισμού των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού είναι οι 53461 και 50858.

***4.14***

Εύκολα συμπεραίνουμε από τις παραπάνω παρατηρήσεις (και με βάση το documentation TCP/UDP ports) ότι η πασίγνωστη θύρα που ακούει ο HTTP Server είναι η 80.

***4.15***

Όπως περιμέναμε, οι θύρες πηγής των ερωτήσεων HTTP ταυτίζονται με τις θύρες προορισμού των απαντήσεων HTTP και αντίστροφα.

***4.16***

Το πρώτο μήνυμα HTTP έχει ονομασία GET /lab2/ HTTP/1.1.

***4.17***

Ο κωδικός απάντησης που μας επιστρέφει ο εξυπηρετητής ιστού είναι «HTTP/1.1 200 OK».

***4.18***

Παρατηρούμε ότι δεν εμφανίζεται καμία καταγραφή πρωτοκόλλων DNS. Αυτό συμβαίνει διότι όταν επισκεπτόμαστε μία σελίδα, αποθηκεύεται προσωρινά το DNS της σε ένα τοπικό buffer, με σκοπό την ταχύτερη φόρτωση της σελίδας κατά την επόμενη σύνδεσή μας εκεί. Ως εκ τούτου, αποφεύγεται η μετάφραση από DNS σε IP στο Ίντερνετ και γίνεται τοπικά. Η εντολή «flushdns» καθαρίζει αυτήν την μνήμη και έτσι επαναλαμβάνεται η διαδικασία μετάφρασης του ονόματος της σελίδας σε IP μέσω Ίντερνετ την επόμενη φορά που θα επιχειρήσουμε να συνδεθούμε στην σελίδα.