ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ
ΑΜ: 031 18 014
ΕΞΑΜΗΝΟ: 7ο
ΟΜΑΔΑ: 4
MAC ADDRESS: B4-69-21-1B-6C-FF
IPv4: 10.3.20.15
ΌΝΟΜΑ ΥΠΟΛΟΓΙΣΤΗ: LAPTOP-B2DVAJKK
ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ: WINDOWS 10

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 2: ΕΝΘΥΛΑΚΩΣΗ ΚΑΙ ΕΠΙΚΕΦΑΛΙΔΕΣ

Άσκηση 1: Στρώμα ζεύξης δεδομένων

1.1) Βλέπουμε τα πλαίσια εκείνα, τα οποία στο Layer 3 διέπονται από το **πρωτόκολλο ARP είτε IPv4**.

1.2) Destination, Source και Type.

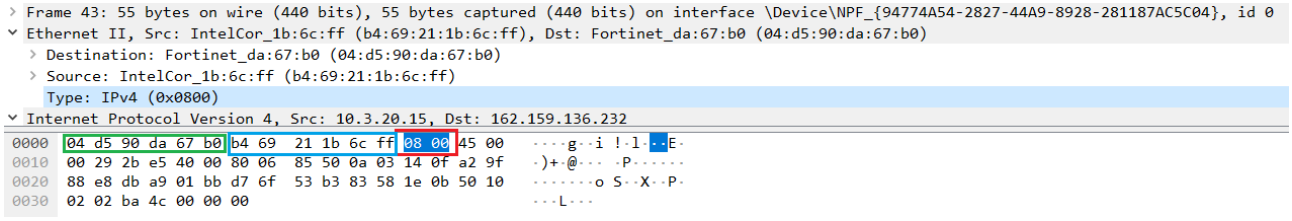
1.3) Όχι, υπάρχουν μόνο τα πεδία που είδαμε στο ερώτημα 1.2.

1.4) Το μήκος των διευθύνσεων Ethernet είναι **6bytes**, αναμενόμενο αφού αντιστοιχούν σε MAC addresses.

1.5) Η επικεφαλίδα Ethernet είναι **14bytes** (6 + 6 για τις MAC διευθύνσεις προορισμού και πηγής και άλλα 2 για τον τύπο).

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

1.7) Το πεδίο Type καταλαμβάνει τα **2 τελευταία bytes της επικεφαλίδας** Ethernet, όπως βλέπουμε παρακάτω: (πράσινο πλαίσιο: MAC destination, γαλάζιο πλαίσιο MAC source, και κόκκινο πλαίσιο το Type).



1.8) Type = 0x0800 για IPv4 πακέτα όπως αναφέραμε.

1.9) Μπορούμε να αλλάξουμε το φίλτρο σε **“arp”** αντί για **“arp or ip”**. Τότε έχουμε 2 πακέτα, τα οποία έχουν **Type = 0x0806**, επαληθεύοντας όσα ήδη αναφέραμε.

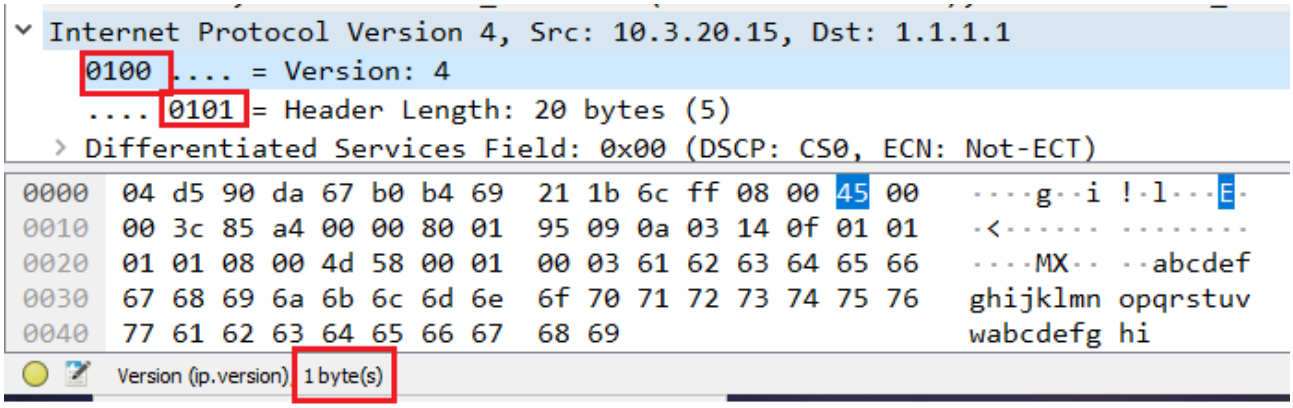
Άσκηση 2: Στρώμα Δικτύου

2.1) Απεικονίζει τα πακέτα που **εφαρμόζουν το πρωτόκολλο ICMP**.

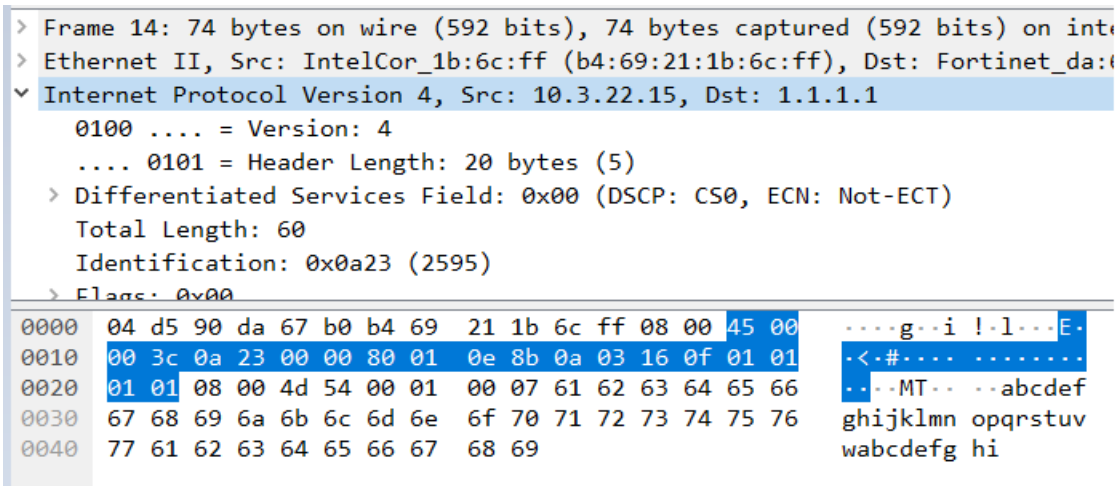
2.2) Οι IPv4 διευθύνσεις είναι **4 byte**, όπως φαίνεται και από την ονομασία τους (από 0.0.0.0 έως 255.255.255.255).

2.3) Το όνομα του πρώτου πεδίου είναι **Version**, ενώ του δευτέρου **Header Length**.

2.4) Από τη μορφή που δίνονται, συμπεραίνουμε πως έκαστο αποτελείται από **4bits** και είναι ίσα με: Version = 0100 (4_{10}) και Header Length = 0101 (5_{10}), όπως βλέπουμε και παρακάτω: (τα 2 αυτά πεδία συναποτελούν το “μπλε” 45 που βλέπουμε, δίνοντας συνολικά 1 byte).



2.5) Αφού επιλέξουμε την επικεφαλίδα IPv4 ενός τυχαίου πακέτου, μετράμε τους δι-ψήφιους δεκαεξαδικούς αριθμούς (1 byte ο καθένας) στα αριστερά και τους βρίσκου-με ίσους με 20, επομένως **20 bytes**. (σημειωμένοι με μπλε στα αριστερά-δεκαεξαδική μορφή).



2.6) Όπως είδαμε παραπάνω, το πεδίο **Header Length** είναι 20 bytes. Από την τιμή του Header Length ($0101 = 5_{10}$), και διαβάζοντας από το documentation σχετικά με το Header Length ότι: **“Specifies the length of the IP packet header in 32bit words”**, προκύπτει το μήκος ίσο με 5 * 4bytes.

2.7) Πατώντας λεπτομέρειες για το Ethernet Layer, βλέπουμε πως τα περιεχόμενα του είναι 14 bytes, επομένως το μήκος του IPv4 προκύπτει από το συνολικό (74 bytes on wire) μείον αυτά τα 14 bytes, άρα **60 bytes**. (δεδομένου ότι το ICMP protocol είναι μέρος του IP Layer).

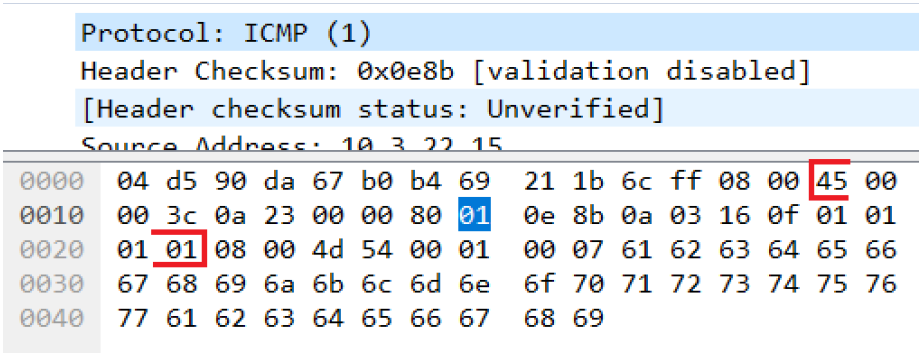
2.8) Στην επικεφαλίδα IPv4, βλέπουμε το πεδίο **Total Length ίσο με 60 bytes**, επομένως συμφωνεί με αυτό που υπολογίσαμε.

2.9) Το μήκος δεδομένων του πακέτου IPv4 είναι **40 bytes**.

2.10) Το payload του IPv4 πακέτου προκύπτει εάν από το **Total Length (60 bytes) αφαιρέσουμε το Header Length (20 bytes)**, αφήνοντας έτσι **40 bytes**.

2.11) Το πεδίο **Protocol:** καθορίζει το πρωτόκολλο στρώματος μεταφοράς.

2.12) Σε σχέση με την αρχή της επικεφαλίδας IPv4, βρίσκεται στο **10ο byte**.



2.13) Η τιμή του για το πρωτόκολλο ICMP είναι **1**.

Άσκηση 3: Στρώμα Μεταφοράς

3.1) Το φίλτρο απεικόνισης “tcp or udp”, μάς εμφανίζει τα πακέτα εκείνα τα οποία **ενθυλακώνουν είτε το πρωτόκολλο TCP είτε το UDP** στο στρώμα μεταφοράς τους.

3.2) Στο στρώμα μεταφοράς, παρατηρούμε τα πρωτόκολλα **TCP/UDP** όπως και αναμέναμε.

3.3) Η τιμή του πεδίου Protocol στο IPv4 header είναι **UDP (17)**, για τα πακέτα UDP, ενώ είναι **TCP (6)** για αυτά του πρωτοκόλλου TCP.

3.4) Source Port, **Destination Port**, **Checksum**.

3.5) Το μήκος της επικεφαλίδας των UDP datagrams είναι **8 bytes**.

3.6) Ναι, το πεδίο **Length** μας δίνει το συνολικό μήκος των UDP datagrams.

3.7) Στα τεμάχια TCP, το πεδίο **Header Length** μας πληροφορεί για το μήκος της επικεφαλίδας, το οποίο και βρίσκεται στα πρώτα **4 bits του 13^{ου} byte της επικεφαλίδας**.

3.8) Ενώ δεν υπάρχει πεδίο, το οποίο να μας πληροφορεί σχετικά με το συνολικό μήκος των τεμαχίων TCP, αυτό προκύπτει εύκολα από το **άθροισμα που μας δίνει το πεδίο Header Length και το πεδίο TCP payload**.

3.9) Στις επικεφαλίδες TCP, βλέπουμε ότι υπάρχει η **θύρα 80 είτε έως Source είτε ως Destination**, ενώ στις επικεφαλίδες UDP βλέπουμε να εμφανίζεται η **θύρα 53 αντίστοιχα**.

3.10) Εφαρμόζοντας το φίλτρο **“not (tcp or udp)”** βρίσκουμε τα υπόλοιπα πρωτόκολλα του **Transport Layer**. Το μοναδικό που μας εμφανίζεται είναι το **ICMPv6**. Όσον αφορά π**ρωτόκολλα στρώματος εφαρμογής**, βρίσκουμε τα **HTTP και DNS.**

Άσκηση 4: Στρώμα Εφαρμογής

4.1) Το DNS χρησιμοποιεί **UDP**.

4.2) Το HTTP χρησιμοποιεί **TCP**.

4.3) Το πρώτο bit από τα 16 της σημαίας καθορίζει το αν πρόκειται για **query/response** με την αντίστοιχη τιμή να είναι **0/1** αντίστοιχα.

4.4) Θύρα προορισμού των DNS ερωτήσεων η **53**.

4.5) Θύρες πηγής των DNS ερωτήσεων: **61613, 60326, 53090, 64282, 55290, 56744, 59740, 61563, 62755, 51195, 61392, 50060, 63772, 64783**.

4.6) Προφανώς η θύρα προέλευσης των DNS απαντήσεων είναι η **53**.

4.7) Αντίστοιχα, οι θύρες προορισμού των απαντήσεων είναι οι θύρες προέλευσης των DNS απαντήσεων, δηλαδή: **61613, 60326, 53090, 64282, 55290, 56744, 59740, 61563, 62755, 51195, 61392, 50060, 63772, 64783**.

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

4.9) Εύκολα προκύπτει πως ο DNS Server ακούει στη θύρα **53**.

4.10) Παρατηρώντας τα μηνύματα εκείνα (τα HTTP προφανώς), τα οποία έχουν ως Source την IP του υπολογιστή μας προκύπτει πως η θύρα προορισμού των HTTP μηνυμάτων είναι η **θύρα 80**.

4.11) Θύρες προέλευσης των HTTP μηνυμάτων που έστειλε ο υπολογιστής μας είναι οι **55557** και **50858**.

4.12) Προφανώς η θύρα των πηγών των HTTP απαντήσεων που λαμβάνει ο υπολογιστής μας είναι η **θύρα 80**.

4.13) Θύρες προορισμού των απαντήσεων του εξυπηρετητή ιστού είναι οι **55557** και **50858**.

4.14) Ο HTTP server ακούει στη **θύρα 80**.

4.15) Όμοια με το DNS, οι θύρες προέλευσης των ερωτήσεων HTTP είναι οι ίδιες με τις θύρες προορισμού των απαντήσεων του web server.

4.16) *Σημείωση: Καθώς έτρεχαν και άλλες διεργασίες παράλληλα με την εκτέλεση του flushdns και του ανοίγματος της σελίδας του εργαστηρίου, το πρώτο http μήνυμα δεν αφορά επικοινωνία με τη σελίδα του εργαστηρίου, αλλά με κάποιο άλλο site. Θα ασχοληθούμε με το πρώτο http μήνυμα προς την IP του εργαστηρίου.*

Το πρώτο μήνυμα HTTP προς τον web server είναι **“GET /lab2/ HTTP/1.1”**.

4.17) Ο κωδικός απάντησης που μας επιστρέφει ο εξυπηρετητής ιστού είναι **“HTTP/1.1 200 OK”** αν έχουμε καθαρίσει cache προηγουμένως και **“HTTP/1/1 304 Not Modified”** αν δεν έχουμε καθαρίσει την cache.

4.18) Έχοντας επισκεφτεί πρόσφατα την ιστοσελίδα, το DNS της έχει αποθηκευτεί σε έναν τοπικό buffer προκειμένου η επόμενη σύνδεση στη σελίδα να είναι ταχύτερη, δηλαδή να μη χρειαστεί να γίνει μετάφραση από DNS σε IP στο Ίντερνετ αλλά τοπι-

κά. Κάνοντας **“flushdns”**, καθαρίζουμε αυτή τη μνήμη, επομένως για να συνδεθούμε σε κάποια σελίδα θα πρέπει να γίνει εκ νέου η μετάφραση του ονόματος της σελίδας σε IP μη τοπικά. Για αυτό και στη 2η καταγραφή, δε καταγράφηκε κανένα πρωτόκολλο DNS χρησιμοποιώντας, ωστόσο, το ίδιο φίλτρο **“http or dns”** , καθώς η μετάφραση έγινε μέσω της τοπικής μνήμης εφόσον είχαμε επισκεφτεί νωρίτερα την ιστοσελίδα.