ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

a0:36:bc:a9:7e:58

christos-System-Product-Name

LINUX Ubuntu 22.04.3 LTS

2η Εργαστηριακή Αναφορά

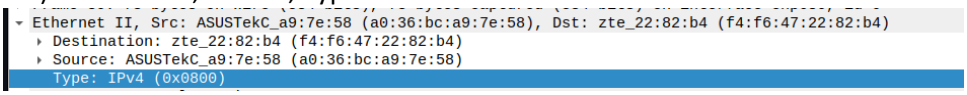
Χρήστος Ηλιακόπουλος

ΑΜ: 03120233

ΑΣΚΗΣΗ 1

1.1) Κάνοντας χρήση του συγκεκριμένου φίλτρου (arp or ip) θα εμφανιστούν στο παράθυρο του wireshark τα πακέτα που έχουν είτε πρωτόκολλο ARP είτε IP.

1.2) Destination, Source, Type



1.3)Δεν υπάρχει στο πλαίσιο ETHERNET

1.4)6 bytes (ή αλλιώς το μέγεθος της MAC)

1.5)Η επικεφαλίδα αποτελείται συνολικά από 14 bytes(destination -> 6 bytes, Source -> 6bytes, Type -> 2bytes)

1.6)Στο πεδίο Type φαίνεται το πρωτόκολλο δικτύου

1.7)Καταλαμβάνει τα 2 τελευταία bytes του τίτλου

1.8) 0x0800 (800 στο δεκαεξαδικό)

1.9)Εφαρμόζω στο φίλτρο μόνο τη λέξη ARP (για να βρω τα πακέτα IPv4 ARP) και βρίσκω ότι έχει τιμή 0x0806 (στο δεκαεξαδικό)]

ΑΣΚΗΣΗ 2

2.1) Θα εμφανιστούν τα πακέτα που χρησιμοποιούν το πρωτόκολλο ICMP

2.2) Το μήκος είναι 4 bytes (4*8bits = 32bits)

2.3) Version(έκδοση) και Header Length (Μήκος επικεφαλίδας)

2.4)Το πεδίο Version έχει μήκος 4bits και η τυπική τιμή του είναι 4. Το πεδίο Header length έχει μήκος και αυτό 4 bits και ελάχιστη τιμή του σύμφωνα με το σάιτ που αναφέρεται στο pdf είναι 5

IHL, Internet Header Length. 4 bits.
Specifies the length of the IP packet header in 32 bit words. The minimum value for a valid header is 5.

2.5) Σύμφωνα με την καταγραφή το μέγεθος σε bytes της επικεφαλίδας IPv4 είναι 20bytes

```
Internet Protocol Version 4, Src: 192.168.1.14, Dst: 1.1.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

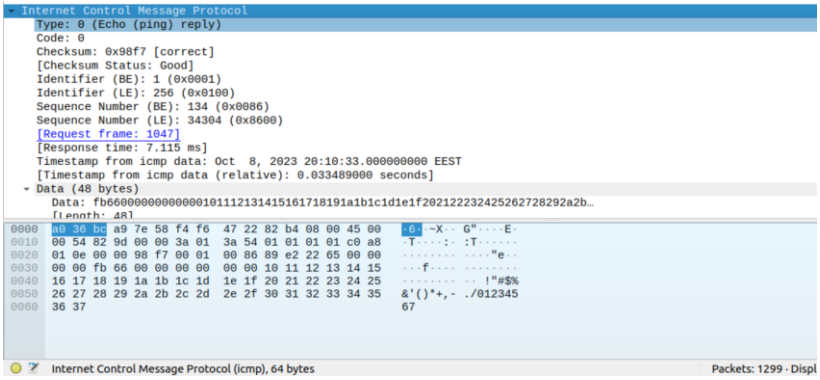
2.6) Η ελάχιστη τιμή του μήκους επικεφαλίδας είναι 5 bytes. Εφόσον το μήκος της λέξης είναι 32bits άρα 4bytes πολλαπλασιάζουμε τα bytes που είναι η ελάχιστη τιμή με τα 4 bytes της λέξης και έχουμε 20 bytes. --> 5 (τιμή πεδίου "Μήκος Επικεφαλίδας") * 4 (μήκος μιας 32-bit λέξης σε bytes) = 20 bytes.

2.7) Με βάση το παράθυρο των περιεχομένων έχουμε τον αριθμό 0054 στο δεκαεξαδικό για το μήκος της επικεφαλίδας που είναι ο αριθμός 84. Άρα 84 bytes

2.8) Υπάρχει το πεδίο total length, στο οποίο εμφανίζεται ο αριθμός 84 και επιβεβαιώνει το προηγούμενο ερώτημα

```
Internet Protocol Version 4, Src: 192.168.1.14, Dst: 1.1.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x19a3 (6563)
```

2.9)64bytes.



2.10) Προκύπτει από το total length-header length=84-20=64bytes

2.11)Το πεδίο της επικεφαλίδας που κάνει αυτόν τον καθορισμό είναι το πεδίο PROTOCOL

2.12) Όπως φαίνεται και στην εικόνα, η θέση του πεδίου PROTOCOL βρίσκεται στην 9η θέση της επικεφαλίδας (10 byte)

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL				Differentiated Services								Total length															
Identification																Flags			Fragment offset											
TTL								Protocol								Header checksum															
Source IP address																															
Destination IP address																															
Options and padding :::																															

2.13) Η τιμή του είναι 1 για την περίπτωση ICMP

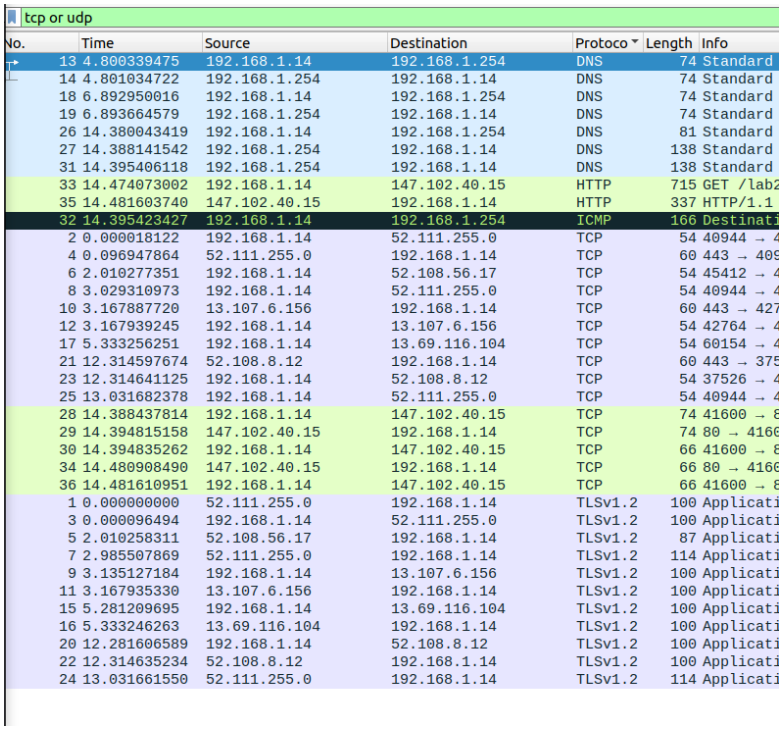
Protocol. 8 bits.
This field specifies the next encapsulated protocol.

Value	Protocol	References
0	HOPOPT, IPv6 Hop-by-Hop Option.	RFC 2460
1	ICMP, Internet Control Message Protocol.	RFC 792
2	IGAP, IGMP for user Authentication Protocol. IGMP, Internet Group Management Protocol. RGMP, Router-port Group Management Protocol.	RFC 1112
3	GGP, Gateway to Gateway Protocol	RFC 823

ΑΣΚΗΣΗ 3

3.1) Με τη χρήση του συγκεκριμένου φίλτρου, εμφανίζονται μόνο τα πρωτόκολλα TCP ή UDP

3.2)Βλέπουμε να υπάρχουν τα πρωτόκολλα του στρώματος μεταφοράς TCP και UDP.



tcp or udp

No.	Time	Source	Destination	Protoco	Length	Info
13	4.800339475	192.168.1.14	192.168.1.254	DNS	74	Standard
14	4.801034722	192.168.1.254	192.168.1.14	DNS	74	Standard
18	6.892950016	192.168.1.14	192.168.1.254	DNS	74	Standard
19	6.893664579	192.168.1.254	192.168.1.14	DNS	74	Standard
26	14.380043419	192.168.1.14	192.168.1.254	DNS	81	Standard
27	14.388141542	192.168.1.254	192.168.1.14	DNS	138	Standard
31	14.395406118	192.168.1.254	192.168.1.14	DNS	138	Standard
33	14.474073002	192.168.1.14	147.102.40.15	HTTP	715	GET /lab2
35	14.481603740	147.102.40.15	192.168.1.14	HTTP	337	HTTP/1.1
32	14.395423427	192.168.1.14	192.168.1.254	ICMP	166	Destinati
2	0.000018122	192.168.1.14	52.111.255.0	TCP	54	40944 → 4
4	0.096947864	52.111.255.0	192.168.1.14	TCP	60	443 → 409
6	2.010277351	192.168.1.14	52.108.56.17	TCP	54	45412 → 4
8	3.029310973	192.168.1.14	52.111.255.0	TCP	54	40944 → 4
10	3.167887720	13.107.6.156	192.168.1.14	TCP	60	443 → 427
12	3.167939245	192.168.1.14	13.107.6.156	TCP	54	42764 → 4
17	5.333256251	192.168.1.14	13.69.116.104	TCP	54	60154 → 4
21	12.314597674	52.108.8.12	192.168.1.14	TCP	60	443 → 375
23	12.314641125	192.168.1.14	52.108.8.12	TCP	54	37526 → 4
25	13.031682378	192.168.1.14	52.111.255.0	TCP	54	40944 → 4
28	14.388437814	192.168.1.14	147.102.40.15	TCP	74	41600 → 8
29	14.394815158	147.102.40.15	192.168.1.14	TCP	74	80 → 4160
30	14.394835262	192.168.1.14	147.102.40.15	TCP	66	41600 → 8
34	14.480908490	147.102.40.15	192.168.1.14	TCP	66	80 → 4160
36	14.481610951	192.168.1.14	147.102.40.15	TCP	66	41600 → 8
1	0.000000000	52.111.255.0	192.168.1.14	TLSv1.2	100	Applicati
3	0.000096494	192.168.1.14	52.111.255.0	TLSv1.2	100	Applicati
5	2.010258311	52.108.56.17	192.168.1.14	TLSv1.2	87	Applicati
7	2.985507869	52.111.255.0	192.168.1.14	TLSv1.2	114	Applicati
9	3.135127184	192.168.1.14	13.107.6.156	TLSv1.2	100	Applicati
11	3.167935330	13.107.6.156	192.168.1.14	TLSv1.2	100	Applicati
15	5.281209695	192.168.1.14	13.69.116.104	TLSv1.2	100	Applicati
16	5.333246263	13.69.116.104	192.168.1.14	TLSv1.2	100	Applicati
20	12.281606589	192.168.1.14	52.108.8.12	TLSv1.2	100	Applicati
22	12.314635234	52.108.8.12	192.168.1.14	TLSv1.2	100	Applicati
24	13.031661550	52.111.255.0	192.168.1.14	TLSv1.2	114	Applicati

3.3) Για το TCP είναι 6, ενώ για το UDP είναι 17

Description:

Protocol suite: TCP/IP.
Protocol type: Transport layer connection oriented byte stream protocol.
IP Protocol: 6.

Description:

Protocol suite: TCP/IP.
Protocol type: Connectionless transport layer protocol.
IP Protocol: 17.

```
Protocol: UDP (17)
Protocol: TCP (6)
```

3.4) Το Source Port, το Destination Port και το CheckSum

TCP header:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port																Destination Port															
Sequence Number																															
Acknowledgment Number																															
Data Offset				reserved				ECN				Control Bits				Window															
Checksum																Urgent Pointer															
Options and padding :::																															
Data :::																															

UDP header:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port																Destination Port															
Length																Checksum															
Data :::																															

3.5) 8 bytes

UDP header:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port																Destination Port															
Length																Checksum															
Data :::																															

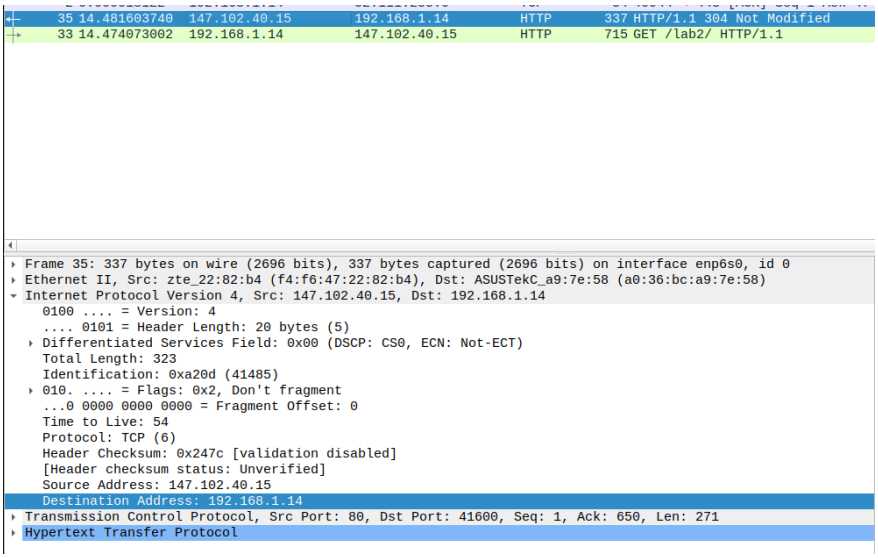
3.6) Ναι, το length όπως φαίνεται και στην προηγούμενη εικόνα

3.7) Το πεδίο DATA OFFSET(αλλιώς πολλές φορές και header length) που βρίσκεται στο 13 byte

3.8)Δεν υπάρχει, αλλά μπορούμε να το βρούμε μέσω του συνολικού μήκους του IP πλαισίου, total length, και να αφαιρέσουμε από αυτό το μέγεθος της επικεφαλίδας που είναι σταθερά 20 bytes

3.9) Όχι δεν υπάρχει αλλά μπορεί να φανερωθεί από τον αριθμό του Destination και του Source port με αντιστοίχηση στον πίνακα της ιστοσελίδας networksorcery για τα TCP/UDP ports.

80	TCP	HTTP, HyperText Transfer Protocol.



Φαίνεται παραπάνω για τον αριθμό 80 στο source port ότι είναι HTTP

3.10) DNS, HTTP, TLSv1.2, ICMP

ΑΣΚΗΣΗ 4

4.1) Χρησιμοποιεί το UDP πρωτόκολλο

4.2)Χρησιμοποιεί το TCP πρωτόκολλο

4.3)Είναι το πρώτο bit της σημαίας και για 0 μηδέν έχουμε ερώτηση, ενώ για 1 έχουμε απάντηση

4.4)Παρατηρούμε ότι για τα queries το destination port είναι το 53 σε όλα

4.5)Οι θύρες πηγής για τα querries είναι οι εξείς: 37.618, 40.802, 51.908

4.6)Σε όλες τις θύρες πηγής για της απαντήσεις το port είναι το 53

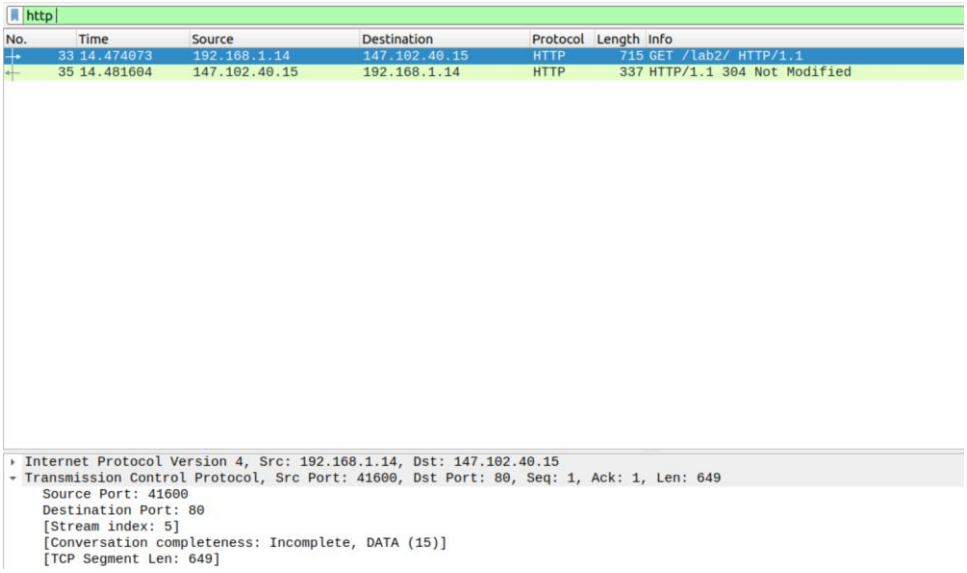
4.7)Αντίστοιχα είναι τα port από τα destination ports των querries: 37.618, 40.802, 51.908

4.8) Παρατηρούμε ότι είναι ίδιες, εφόσον αφού στέλνει από συγκεκριμένα ports ερωτήσεις, περιμένει να λάβει και από αυτά τα ports απάντηση

4.9)Η θύρα 53, όπως έγινε αντιληπτό και από τα προηγούμενα ερωτήματα

4.10)Η θύρα προορισμού είναι η 80 για τα μηνύματα HTTP

4.11) 41.600 είναι η θύρα πηγής



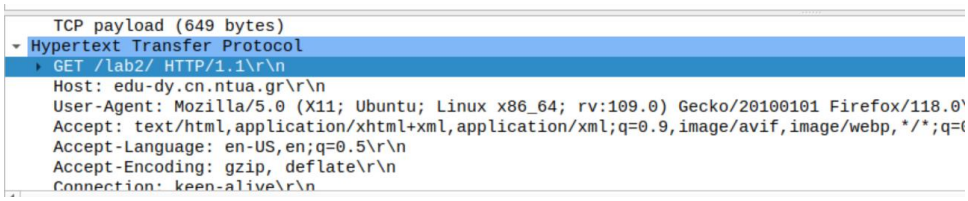
4.12) Αντίστοιχα, είναι η θύρα προορισμού για τα HTTP που έστειλε ο υπολογιστής μας, άρα είναι η θύρα 80

4.13)Είναι η θύρα 41.600

4.14)Η πασίγνωστη θύρα, είναι η θύρα 80

4.15)Είναι η ίδια θύρα, καθώς περιμένουμε μία απάντηση από αυτήν όταν στείλουμε μία ερώτηση(query)

4.16)GET /lab2/ HTTP/1.1



4.17)200

4.18) Γιατί τότε η διεύθυνση θα υπάρχει στην μνήμη cache και το μήνυμα που θα πάρουμε δεν θα είναι το 200. Αυτό θα συμβεί γιατί η απάντηση που θα πάρουμε θα είναι από την μνήμη cache και όχι από τον DNS server απευθείας. Επομένως με την συγκεκριμένη εντολή θα καθαριστεί η cache.