LAB-02 (OSI Layers)

Ex. 1 | Link layer

1.1 | Φίλτρο `arp or ip`
Εμφανίζονται όλα τα πακέτα που περιέχουν επικεφαλίδες ARP (Address Resolution Protocol) ή IP (Internet Protocol)

1.2 | Πεδία επικεφαλίδας Ethernet
- Destination
- Source
- Type

1.3 | Πεδίο μήκους ethernet πλαισίου
Όχι, δεν υπάρχει

1.4 | Μήκος διεύθυνσης Ethernet
6 bytes

1.5 | Μήκος επικεφαλίδας Ethernet
14 bytes (6 → Destination, 6 → Source, 2 → Type)

1.6 | Πρωτόκολλο δικτύου
Το πεδίο type του πλαισίου Ethernet

1.7 | Θέση πρωτοκόλλου στην επικεφαλίδα
Καταλαμβάνει τα δύο τελευταία bytes

1.8 | Τιμή για πακέτα IPv4
HEX τιμή για IPv4 : 08 00

1.9 | Τιμή για πακέτα IPv4 (πακέτα ARP)
HEX τιμή για IPv4 (με πακέτα ARP) : 08 06

Ex. 2 | Network layer

2.1 | Φίλτρο `icmp`
Εμφανίζονται όλα τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol)

2.2 | Μήκος διεύθυνσης IPv4
Μία διεύθυνση IPv4 εχει μήκος 4 bytes

2.3 | Ονόματα πρώτων 2 πεδίων IPv4 επικεφαλίδας
Πρώτο πεδίο : Version
Δεύτερο πεδίο : Header Length

2.4 | Μήκος πεδίων
Τα πεδία έχουν μήκος 4 bit το καθένα. Το πρώτο έχει τιμή 4 (τύπος πρωτοκόλου) και το δεύτερο τιμή 5

2.5 | Μήκος επικεφαλίδας IPv4
Μήκος επικεφαλίδας IPv4 : 20 bytes

2.6 | Αντίστοιχο πεδίο της IPv4 επικεφαλίδας
Ταυτίζεται με τη τιμή που αναγράφεται στο πεδίο Header Length της επικεφαλίδας IPv4

DIRECTORY

DICTIONARY

Πλαίσιο → Link layer

Πακέτο → Internet layer

Τεμάχιο TCP → Transport layer

Μήνυμα → Application layer

Display filter / Φίλτρο απεικόνσης
Φίλτρο που εφαρμόζεται από το wireshark μετά από τη συλλογή πλαισίων

Capture filter / Φίλτρο σύλληψης
Φίλτρο που εφαρμόζεται από το npcap κατά την συλλογή πλαισίων

ICMP (Internet Control Message Protocol)
Supporting

2.7 | Μήκος με βάση το παράθυρο περιεχομένων
Μήκος πακέτου IPv4 (με βάση τα περιεχόμενα) : 74 bytes

2.8 | Πεδίο για μήκος πακέτου IPv4
Το μήκος του πακέτου αναγράφεται και στη λίστα πακέτων και στην επικεφαλίδα Frame και ναι συμφωνεί με αυτό που βρίκαμε παραπάνω

2.9 | Μήκος δεδομένων πακέτου IPv4
Μήκος δεδομένων / Data : 32 bytes

2.10 | Πως προκύπτει το μήκος δεδομένων
Από την επικεφαλίδα Internet Control Message Protocol κοιτάμε το πεδίο Data στο οποιο αναγράφεται δίπλα το μήκος του

2.11 | Πεδίο για πρωτόκολλο στρώματος μεταφοράς
Το πεδίο που λέγεται `Protocol`

2.12 | Σχετική θέση Protocol
Βρίσκεται στο 10 byte από την αρχή της επικεφαλίδας IPv4

2.13 | Τιμή για πρωτόκολο ICMP
Τιμή Protocol για ICMP : 01 (HEX)

Ex. 3 | Transport layer

3.1 | Φίλτρο `tcp or udp`
Εμφανίζει όλα τα πακέτα που περιέχουν επικεφαλίδες TCP ή UDP

3.2 | Πρωτόκολλα στρώματος μεταφοράς
UDP, TCP, QUIC, TLS

3.3 | Τιμή Protocol (IPv4) για TCP και UDP
Για TCP : 06 (HEX), για UDP : 11 (HEX)

3.4 | Κοινά ονόματα πεδίων για επικεφαλίδες TCP, UDP
Source Port, Destination Port, Checksum

3.5 | Μήκος επικεφαλίδας UDP
8 bytes

3.6 | Πεδίο μήκους UDP
Υπάρχει το πεδίο Length

3.7 | Πεδίο για μήκος επικεφαλίδας TCP
Υπάρχει το πεδίο Header Length (1 byte) το οποίο είναι το 13ο byte από την αρχή της επικεφαλίδας

3.8 | Πεδία για συνολικό μήκος τεμαχίων TCP
Οχι, δεν υπάρχει. Προκύπτει από το άθροισμα σε bytes του Header Length και του TCP Payload

3.9 | Πεδίο TCP / UDP για τύπο πρωτοκόλλου εφαρμογής
Το Destination ή το Source Port μπορεί να αποκαλύπτει το τύπο πρωτοκόλλου εφαρμογής (πχ. η πόρτα 443 υποδηλώνει το HTTPS)

3.10 | Πρωτόκολλα στρώματος εφαρμογής
DNS, HTTP

Ex. 4 | Application layer

4.1 | Πρωτόκολλο μεταφοράς για DNS
Το UDP πρωτόκολλο

> *internet protocol for error messages*

> **QUIC**
> *transport protocol, alternative to TCP. Sits on top of UDP*

> **DNS (Domain Naim System)**

> **TLS (Transport Layer Security**
> *Protocol that provides security in the communication between two hosts*

4.2 | Πρωτόκολλο μεταφοράς για TCP
Το TCP πρωτόκολλο

4.3 | Bit για ερώτηση/απάντηση από πεδίο flags
Το πρώτο bit. 0 για ερώτηση και 1 για απάντηση

4.4 | Θύρα προορισμού για DNS queries
Destination port (DNS query) : 53

4.5 | Θύρα προέλευσης για DNS queries
Source port (DNS query) : 59374

4.6 | Θύρα προέλευσης για DNS responses
Source port (DNS reponse) : 53

4.7 | Θύρα προορισμού για DNS responses
Destination port (DNS response) : 59374

4.8 | Σχέση για Source port (query) και Dest. port (response)
Η DNS ερώτηση με την DNS απάντηση "περνάνε" από την ίδια πόρτα

4.9 | Πασίγνωστη θύρα DNS
DNS Port : 53

4.10 | Θύρα προορισμού για HTTP request
Destination Port : 80

4.11 | Θύρα προέλευσης για HTTP request
Source Port : 49451

4.12 | Θύρα προέλευσης για HTTP response
Source Port : 80

4.13 | Θύρα προορισμού για HTTP response
Destination Port : 49451

4.14 | Πασίγνωστη θύρα HTTP
HTTP Port : 80

4.15 | Σχέση Source Port (request) με Dest. Port (response)
Οι δύο πόρτες αυτες (source και destination) ταυτίζονται

4.16 | Ονομασία πρώτου μηνύματος HTTP από τον υπολογιστή
GET /lab2/ HTTP/1.1

4.17 | Κωδικός απάντησης από web-server
HTTP/1.1 200 OK

4.18 | Χρησιμότητα της εντολής ipconfig /flushdns
Η εντολή `ipconfig /flushdns` χρειάζεται για το καθαρισμό της cache από DNS αρχεία, διότι αν έχουμε επισκευτεί ήδη τη σελίδα τα DNS requests θα απαντηθούν από τη cache και όχι από το DNS server.