*ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ*

*2O ΕΡΓΑΣΤΗΡΙΟ*

**Σεραφείμ Τζελέπης AM:el18849,**

**Huawei MateBook 14, Windows 10,**

**Mac Address : 5C-3A-45-DC-95-1D**

*1)*

*1.1* Το φίλτρο απεικόνισης arp or ip κρατάει μόνο τα πλαίσια με πακέτα πρωτοκόλλου arp or ip

*1.2* Destination, Source, Type

*1.3* Όχι

*1.4* 6 Bytes

*1.5* 14 Bytes

*1.6* Το πεδίο Type

*1.7* Τα τελευταία δυο Bytes

*1.8* 0x0800

*1.9* 0x0806

*2)*

*2.1* Πλέον απεικονίζουμε μόνο τα πακέτα πρωτοκόλλου(στρώμα δικτύου) ICMP

*2.2* 8 Bytes

*2.3* Version, Header Length

*2.4* Από 4 bits το καθένα με Version = 4(0100) και Header Length = 5(0101)

*2.5* 20 Bytes

*2.6* Γνωρίζουμε ότι το header length είναι 5 άρα πολλαπλασιάζοντας με 4 παίρνουμε τα 20 Bytes

*2.7* 60 Bytes

*2.8* Ναι, Total Length: 60 Bytes

*2.9* 40 Bytes

*2.10* Total Length – Header Length = 60 – 20 = 40 Bytes(Payload)

*2.11* Protocol

*2.12* Στο 10ο byte της επικεφαλίδας

*2.13* 0x01

*3)*

*3.1* To φίλτρο απεικόνισης αυτό απεικονίζει μόνο τα πακέτα πρωτοκόλλου(στρώμα μεταφοράς) udp ή tcp

*3.2* TCP και UDP

3.3 TCP Protocol: 0x06, UDP Protocol: 0x11

*3.4* Src Port, Dst Port

*3.5* 8 Bytes

*3.6* Length: 34

*3.7* Header Length , 4 MSB του 13ου Byte

*3.8* Όχι δεν υπάρχει, ένας τρόπος είναι να πάρουμε από την επικεφαλίδα του ipv4 το total length και από εκεί να αφαιρέσουμε ip header length και το tcp header length

*3.9* Μπορούμε από το Destination Port να βρούμε το πρωτόκολλο στρώματος εφαρμογής βρίσκοντας την αντιστοίχιση του port στην δοσμένη λύση

*3.10* HTTPS,DNS

*4)*

*4.1* To DNS χρησιμοποιεί πρωτόκολλο μεταφοράς UDP

*4.2* Το HTTP χρησιμοποιεί πρωτόκολλο μεταφοράς TCP

*4.3* To 1ο Bit των Flags αν είναι 0 πρόκειται για response και αν είναι 1 πρόκειται για query

*4.4* Destination Port:53

*4.5* Source Port:51595, 54220, 61312, 52975

*4.6* Source Port:53

*4.7* Destination Port: 51595, 54220, 61312, 52975

*4.8* Είναι ίδιες

*4.9* Port 53

*4.10* Destination Port:80

*4.11* Source Port:50428

*4.12* Source Port:80

*4.13* Destination Port:50428

*4.14* Port 80

*4.15* Είναι ίδιες

*4.16* Το πρώτο μήνυμα είναι το GET /lab2/ HTTP/1.1

*4.17* Το μήνυμα της απάντησης είναι HTTP/1.1 200 OK

*4.18* Παρατηρώ ότι δεν γίνονται DNS queries πριν την λήψη του πακέτου «GET /lab2/ HTTP/1.1>> καθώς είναι αποθηκευμένα στην cache του υπολογιστή οπότε για να τα ξαναδώ πρέπει να χρησιμοποιήσω την εντολή “ipconfig /flushdns”.