Ονοματεπώνυμο: Μάρκος Δεληγιάννης	**Ομάδα:** 3
Όνομα PC/ΛΣ: MarkiniHP / Linux Mint	**Ημερομηνία:** 05 / 10 / 2022
Διεύθυνση IP: 192 . 168 . 1 . 14	**Διεύθυνση MAC:** A4 - 17 - 31 - 50 - E0 - BD

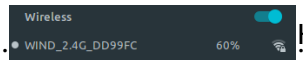
Εργαστηριακή Άσκηση 1
Αναλυτής Πρωτοκόλλων Wireshark

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 Εντολή: lspci | grep Network

Αποτέλεσμα: "Network controller: Ralink corp. RT3290 Wireless 802.11n 1T/1R PCIe"

1.2 Ασύρματη σύνδεση 

Κλικάροντας το εικονίδιο κάτω δεξιά στην οθόνη

1.3 Για τα 1.3 - 1.8 κλικάρουμε το "Network Settings" στο μενού του 1.2 και έπειτα στις ρυθμίσεις του δικτύου που είμαστε συνδεδεμένοι. Στο μενού που εμφανίζεται υπάρχουν όλες οι πληροφορίες.

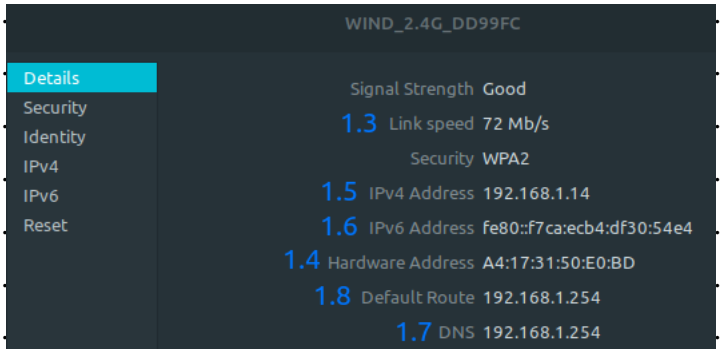
1.4

1.5

1.6

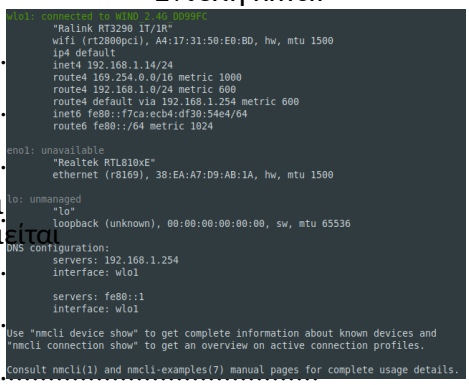
1.7

1.8



Άσκηση 2

Εντολή nmcli



2.1 Εντολή: hostname

Αποτέλεσμα: "MarkiniHP"

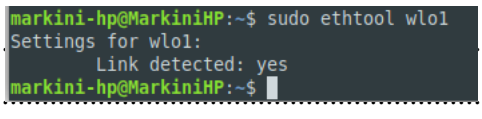
2.2 Εντολή: nmcli (Πιο ευανάγνωστο αποτέλεσμα από τις ifconfig και ip link)

Αποτέλεσμα: 3 κάρτες:
1) wlo1: wifi - αυτή που χρησιμοποιείται
2) eno1: ethernet - δεν χρησιμοποιείται
3) lo: loopback

2.3 Εντολή: nmcli

Αποτέλεσμα: A4:17:31:50:E0:BD

2.4 Εντολή: sudo ethtool wlo1

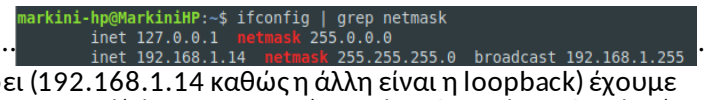


Αποτέλεσμα: Το συγκεκριμένο μοντέλο κάρτας δικτύου δεν παρέχει αναλυτικές πληροφορίες, οπότε δεν μπορούμε να αποφανθούμε για την ταχύτητα της σύνδεσης

2.5 Εντολή: nmcli

Αποτέλεσμα: inet4 192.168.1.14

2.6 Εντολή: ifconfig | grep netmask



Αποτέλεσμα: Για την ip που μας ενδιαφέρει (192.168.1.14 καθώς η άλλη είναι η loopback) έχουμε μάσκα δικτύου 255.255.255.0 (24 bits 1 στην αρχή) άρα i. 24 ii. (λογικό and με μάσκα δικτύου) 192.168.1.0

2.7 Εντολή: nmcli

Αποτέλεσμα: inet6 fe80::f7ca:ecb4:df30:54e4/64

2.8 Εντολή: nmcli

Αποτέλεσμα: route4 default via (=default gateway IPv4 address) 192.168.1.254

2.9 Εντολή: nmcli

Αποτέλεσμα: IPv4: 192.168.1.254 IPv6: fe80::1

2.10 Εντολή: ip r | grep default

Αποτέλεσμα: Η IPv4 του DHCP είναι 192.168.1.254

```
markini-hp@MarkiniHP:~$ ip r | grep default
default via 192.168.1.254 dev wlo1
default via 192.168.1.254 dev wlo1 proto dhcp metric 600
markini-hp@MarkiniHP:~$
```

2.11 Εντολή: ifconfig

Αποτέλεσμα: Η κάρτα δικτύου έχει στείλει και λάβει 0 πακέτα (0 Byte), όπως είναι αναμενόμενο, καθώς έχουμε συνδεθεί στο διαδίκτυο μέσω Wifi

```
markini-hp@MarkiniHP:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 38:ea:a7:d9:ab:1a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.12 Εντολή: netstat -4 -s

Αποτέλεσμα: Η κάρτα δικτύου έχει λάβει 844 πακέτα και έχει στείλει 828 πακέτα

```
markini-hp@MarkiniHP:~$ netstat -4 -s
Ip:
    Forwarding: 2
    844 total packets received
    0 forwarded
    0 incoming packets discarded
    828 incoming packets delivered
    820 requests sent out
    20 outgoing packets dropped
```

2.13 Εντολή: netstat --tcp -n | grep ESTABLISHED

Αποτέλεσμα: Έχουμε 3 established συνδέσεις tcp με άλλους υπολογιστές

2.14 Από το 2.13 έχουμε για τις συνδέσεις:
1) θύρα πηγής: 36648 θύρα προορισμού: 443
2) θύρα πηγής: 36150 θύρα προορισμού: 443

```
markini-hp@MarkiniHP:~$ netstat --tcp -n | grep ESTABLISHED
tcp        0      0 192.168.1.14:36648      162.159.128.233:443     ESTABLISHED
tcp        0      0 192.168.1.14:36150      162.159.130.235:443     ESTABLISHED
tcp        0      0 192.168.1.14:35150      162.159.134.234:443     ESTABLISHED
markini-hp@MarkiniHP:~$
```

Άσκηση 3

3.1 Ακολουθώντας τις οδηγίες, τα πρωτόκολλα είναι: HTTP, TCP, TLSv1.2

3.2 Επιλέγουμε το πακέτο HTTP με την εντολή GET και εστιάζουμε στο Ethernet header. Στο Src βρίσκεται η διεύθυνσή MAC του υπολογιστή, η οποία είναι a4:17:31:50:e0:bd (Το ότι αναγράφεται Ethernet και όχι 802.11 είναι ιδιοτροπία του Wireshark, η οποία δεν αλλάζει τις πληροφορίες που μας ενδιαφέρουν)`

3.3 Παρατηρώντας τα Ethernet Headers λαμβάνουμε τον κατασκευαστή της κάρτας: HonHaiPr το οποίο αντιστοιχεί στο πλήρες όνομα Hon Hai Precision Ind. Co.,Ltd.

3.4 Στο IPv4 header αναγράφεται ότι η διεύθυνση του υπολογιστή μας είναι 192.168.1.14 (source του get)

3.5 Στο IPv4 header αναγράφεται ότι η διεύθυνση του edu-dy.cn.ntua.gr είναι 147.102.40.15 (destination του get)

3.6 Το νέο φίλτρο είναι: tcp.stream eq 1

3.7 Με επισκόπηση του πακέτου 200 OK του server:
i) Τύπος εξυπηρετητή: server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
ii) Html tag: <html> και επισημαίνει την αρχή της σελίδας. Τίτλος: CN Lab (μεταξύ <title> και </title>)
iii) Ο τίτλος εμφανίζεται πάνω στην καρτέλα του φυλλομετρητή που αντιστοιχεί σε αυτή τη σελίδα

3.8 Το φίλτρο είναι: ip.addr==147.102.40.15 && http. Το φίλτρο http εμφανίζει μόνο τα http μηνύματα και το ip.addr==147.102.40.15 εμφανίζει τα σχετικά μηνύματα με την άσκηση

3.9 Γνωρίζοντας την ip του υπολογιστή μας από προηγούμενο ερώτημα, διακρίνουμε μεταξύ των εξερχόμενων και εισερχόμενων μηνυμάτων και έχουμε: 2 εξερχόμενα μηνύματα (Get requests) και 2 εισερχόμενα μηνύματα (200 OK)

3.10 Ακολουθώντας τις οδηγίες λαμβάνουμε απάντηση: 0.012286050 seconds

3.11 Ακολουθώντας τις οδηγίες λαμβάνουμε απάντηση: 8 πακέτα (8 Reassembled TCP Segments). Οι A.A. τους είναι: 25,27,29,31,33,35,37,39

3.12 Το φίλτρο είναι ip.addr==147.102.40.15 && tcp

3.13
i) 0.011641329 sec (Time since previous displayed packet για το πρώτο πακέτο TCP του δεύτερου 200 OK)
ii) 0.001135488 sec (Time since beginning of capture και αφαιρούμε τον χρόνο άφιξης του 8ου TCP πακέτου από του 1ου)
iii) 0.012776817 sec (Time since previous displayed packet με φίλτρο ip.addr==147.102.40.15 && http για το δεύτερο 200 OK)

3.14 Ακολουθούμε τις οδηγίες και παρατηρούμε ότι οι χρόνοι αυτοί ταυτίζονται απόλυτα με τους χρόνους που βρήκαμε στο 3.13

3.15 Το φίλτρο είναι: ip.src==192.168.1.14 && http
Το http φιλτράρει τα μηνύματα http και το ip.src==192.168.1.14 φιλτράρει τα μηνύματα με προέλευση (source) τον υπολογιστή μας