Learn about the invisible world of Wi-Fi with aircrack-ng

What is aircrack-ng?

- Complete suite of tools that allow you to assess Wi-Fi security
- Allows you to monitor network traffic and capture data for analysis
- Provides tools for attacking networks using replay attacks, deauthentication, fake AP’s, and packet injection
- Capable of cracking some Wi-Fi networks

We can see:

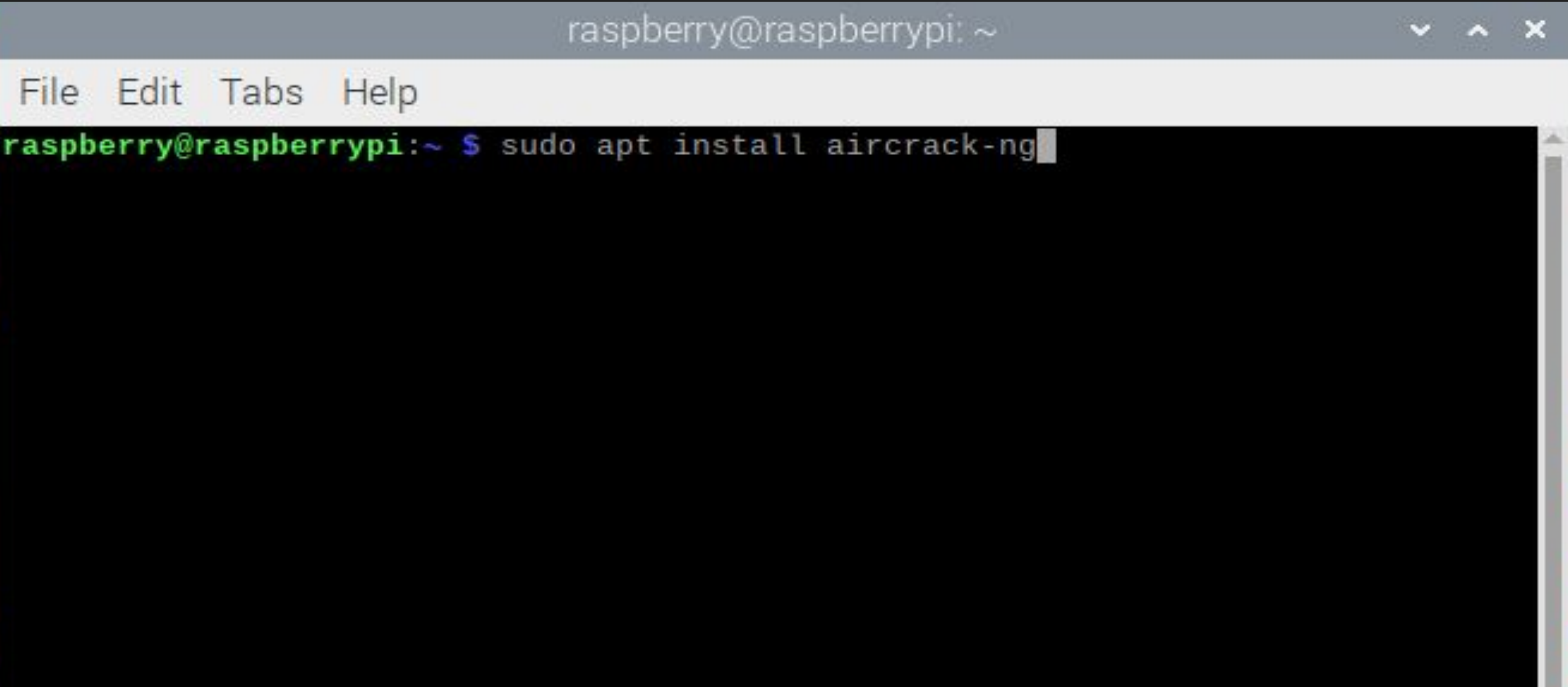
- Wi-Fi networks (**access points**) around us, like your home Wi-Fi network
- Which devices are connected to nearby Wi-Fi networks
- Who makes the Wi-Fi devices you can see (like Apple, Dell, HP)
- Which devices are being used, and which are not
- How strong a signal is, and if the signal gets stronger or weaker
- And more!

Tools Included

- **Airmon-ng** can let your Wi-Fi card listen to all traffic around you
- **Airodump-ng** will gather information about what networks and access points are available and which devices are connected to those access points
- **Airgraph-ng** allows you to take the information gathered by airodump-ng and create an easy to read graph of devices and networks

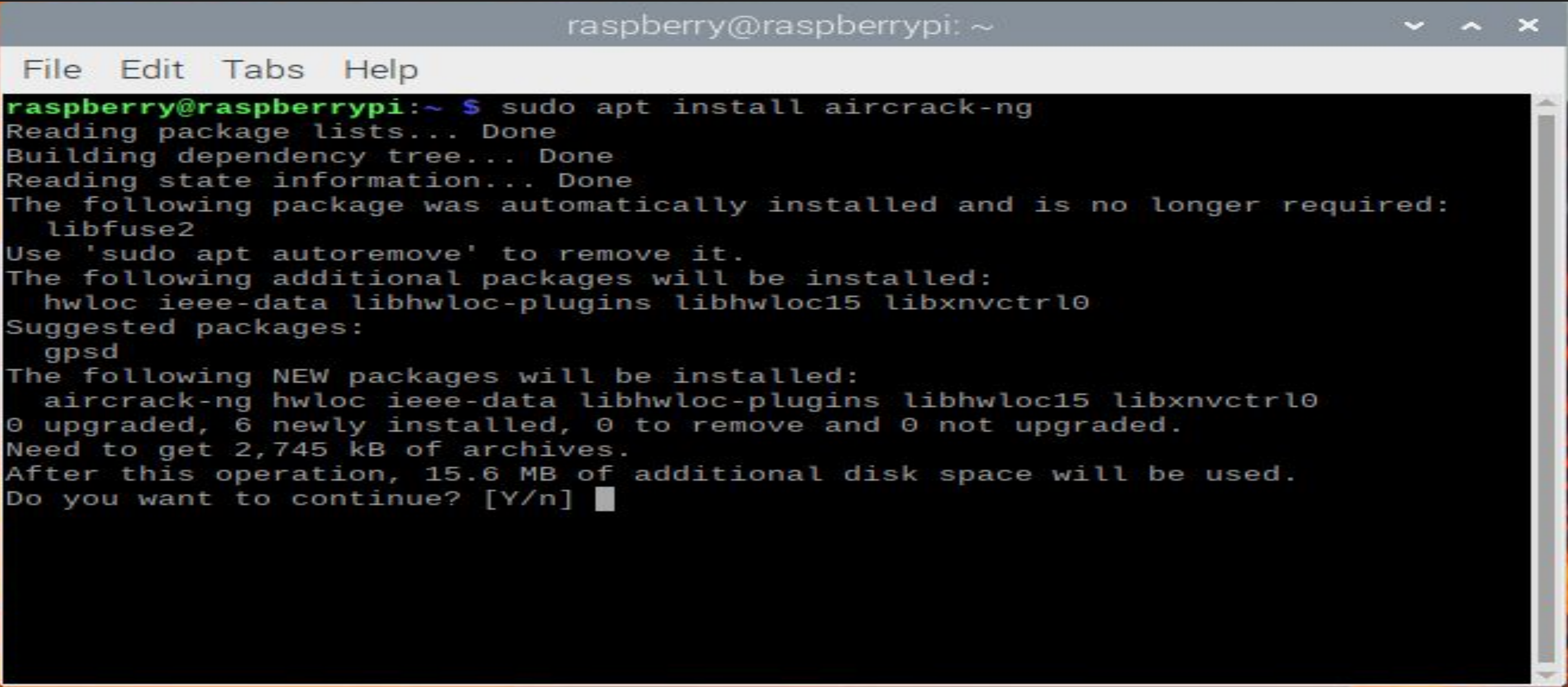
Lets install some software

Step #1 sudo apt install aircrack-ng



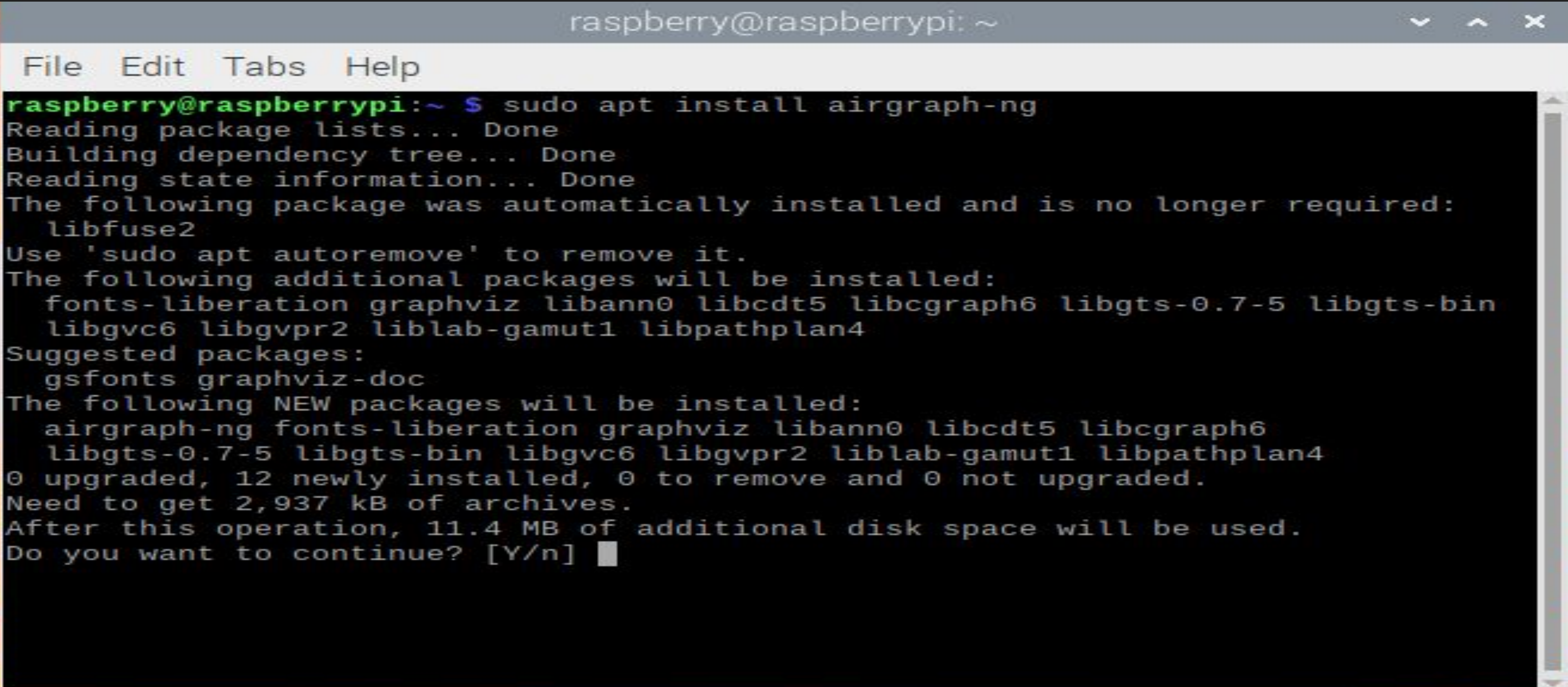
```
raspberry@raspberrypi:~ $ sudo apt install aircrack-ng
```

Step #2   Y



```
raspberry@raspberrypi:~ $ sudo apt install aircrack-ng
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfuse2
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  hwloc ieee-data libhwloc-plugins libhwloc15 libxnvctrl0
Suggested packages:
  gpsd
The following NEW packages will be installed:
  aircrack-ng hwloc ieee-data libhwloc-plugins libhwloc15 libxnvctrl0
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,745 kB of archives.
After this operation, 15.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

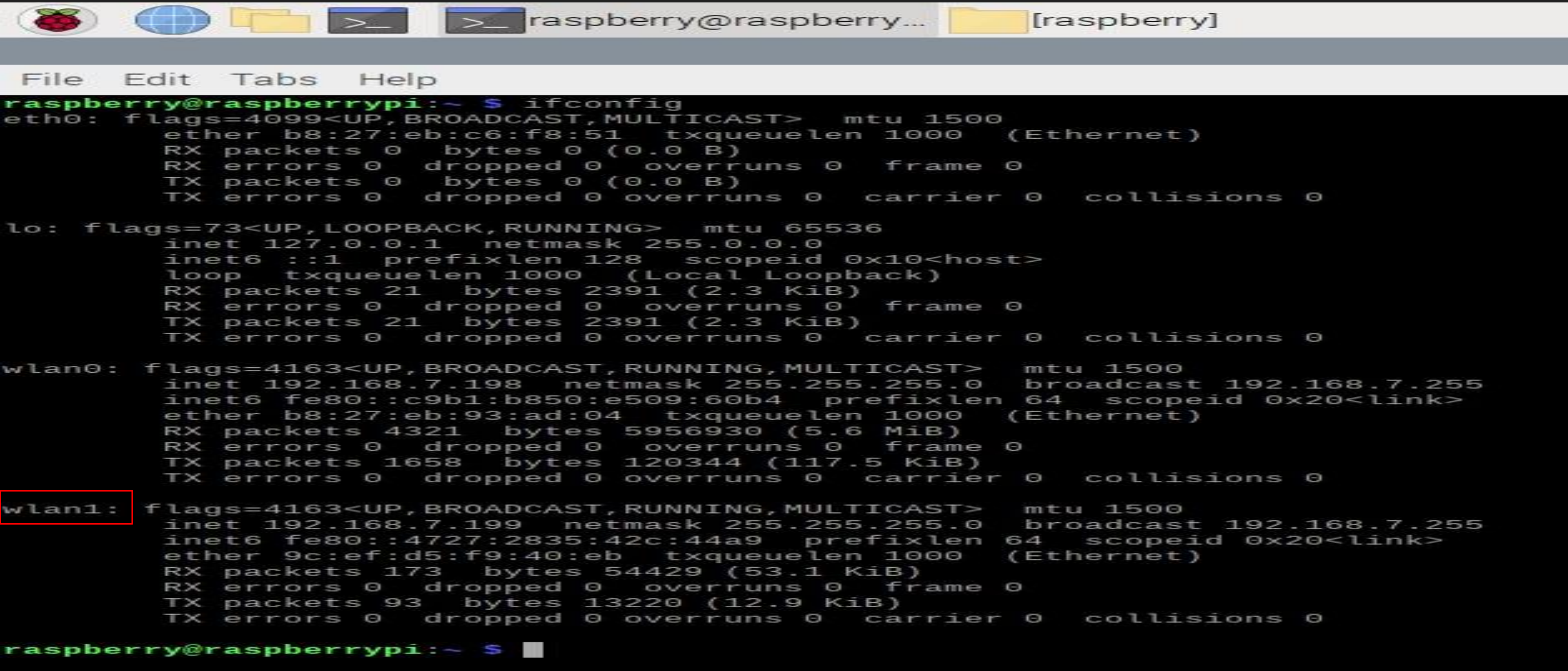
Step #3   sudo apt install airgraph-ng



```
raspberry@raspberrypi:~ $ sudo apt install airgraph-ng
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfuse2
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  fonts-liberation graphviz libann0 libcdt5 libcgraph6 libgts-0.7-5 libgts-bin
  libgvc6 libgvpr2 liblab-gamut1 libpathplan4
Suggested packages:
  gsfonts graphviz-doc
The following NEW packages will be installed:
  airgraph-ng fonts-liberation graphviz libann0 libcdt5 libcgraph6
  libgts-0.7-5 libgts-bin libgvc6 libgvpr2 liblab-gamut1 libpathplan4
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,937 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

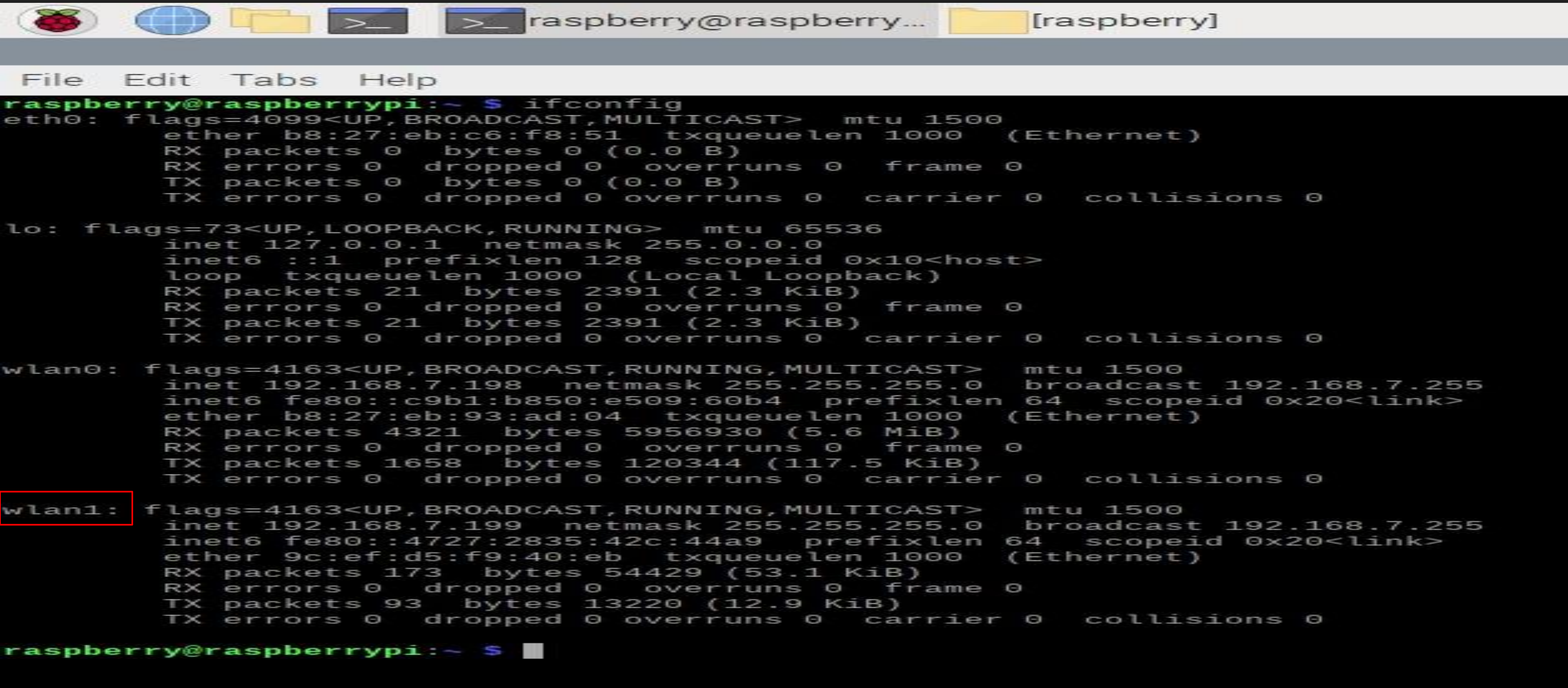
Turning Your Wireless Card Into a Wi-Fi Spy

Step #4 ifconfig



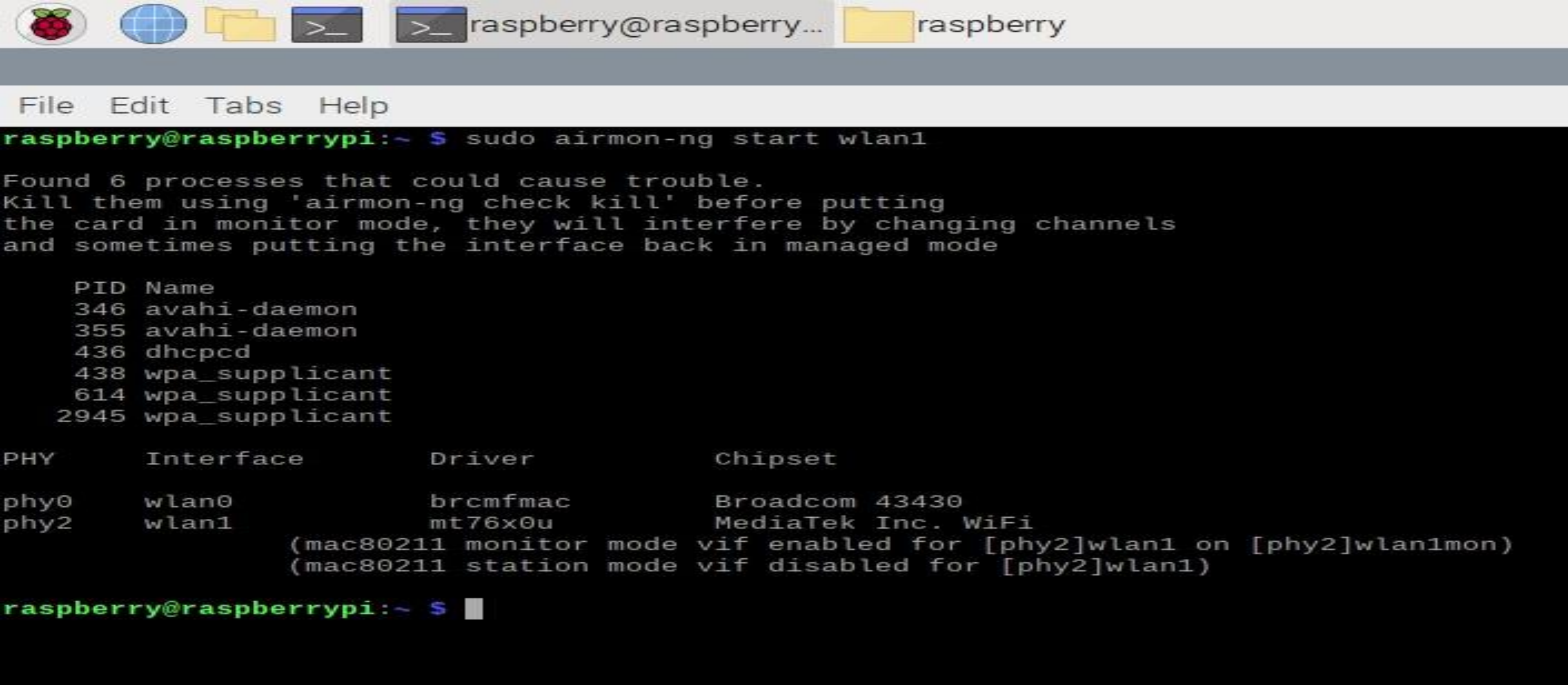
```
raspberry@raspberrypi:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:27:eb:c6:f8:51  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 21  bytes 2391 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2391 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.198  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::c9b1:b850:e509:60b4  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:93:ad:04  txqueuelen 1000  (Ethernet)
        RX packets 4321  bytes 5956930 (5.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1658  bytes 120344 (117.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.199  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::4727:2835:42c:44a9  prefixlen 64  scopeid 0x20<link>
        ether 9c:ef:d5:f9:40:eb  txqueuelen 1000  (Ethernet)
        RX packets 173  bytes 54429 (53.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93  bytes 13220 (12.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

raspberry@raspberrypi:~ $ 
```

This is the Wi-Fi card we will use to listen!



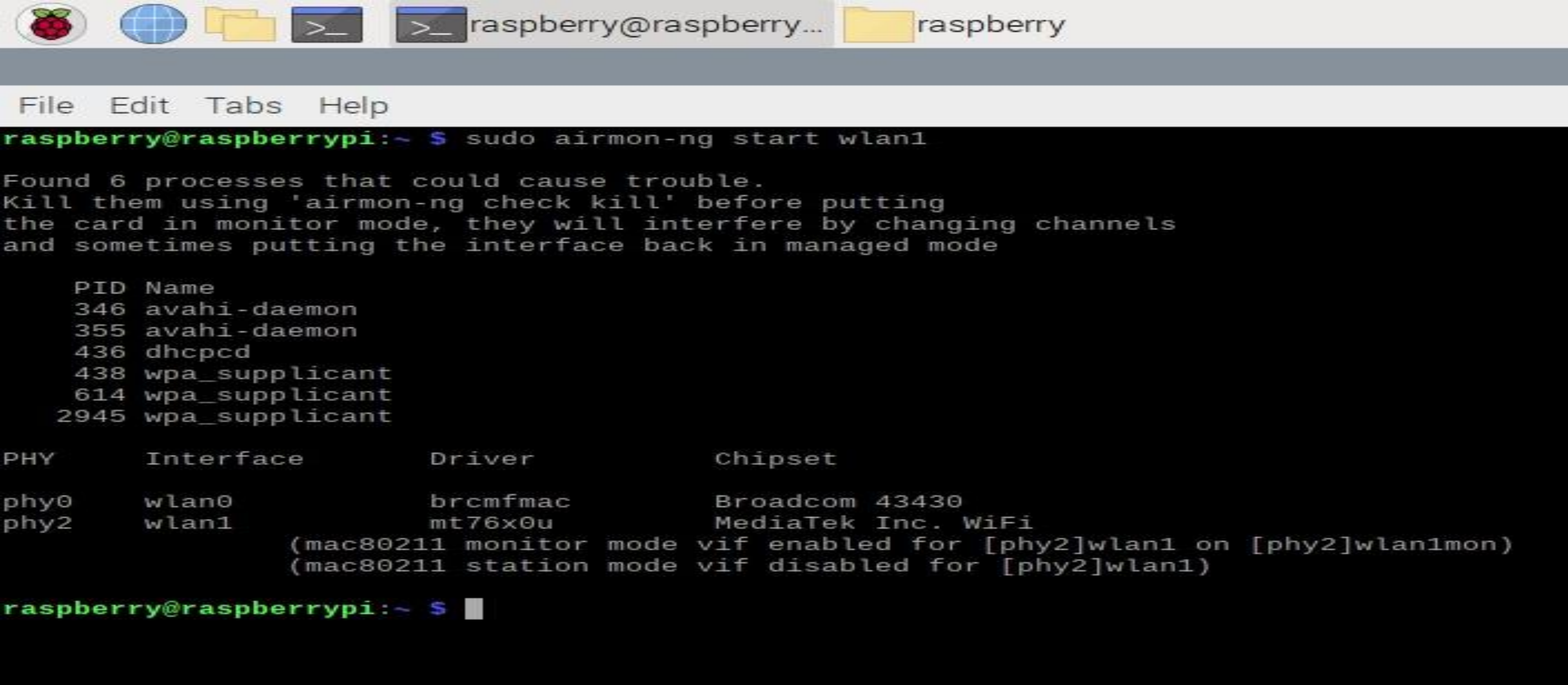
```
raspberry@raspberrypi:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:27:eb:c6:f8:51  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 21  bytes 2391 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2391 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.198  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::c9b1:b850:e509:60b4  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:93:ad:04  txqueuelen 1000  (Ethernet)
        RX packets 4321  bytes 5956930 (5.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1658  bytes 120344 (117.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.199  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::4727:2835:42c:44a9  prefixlen 64  scopeid 0x20<link>
        ether 9c:ef:d5:f9:40:eb  txqueuelen 1000  (Ethernet)
        RX packets 173  bytes 54429 (53.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93  bytes 13220 (12.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

raspberry@raspberrypi:~ $
```

Step #5   sudo airmon-ng start wlan1



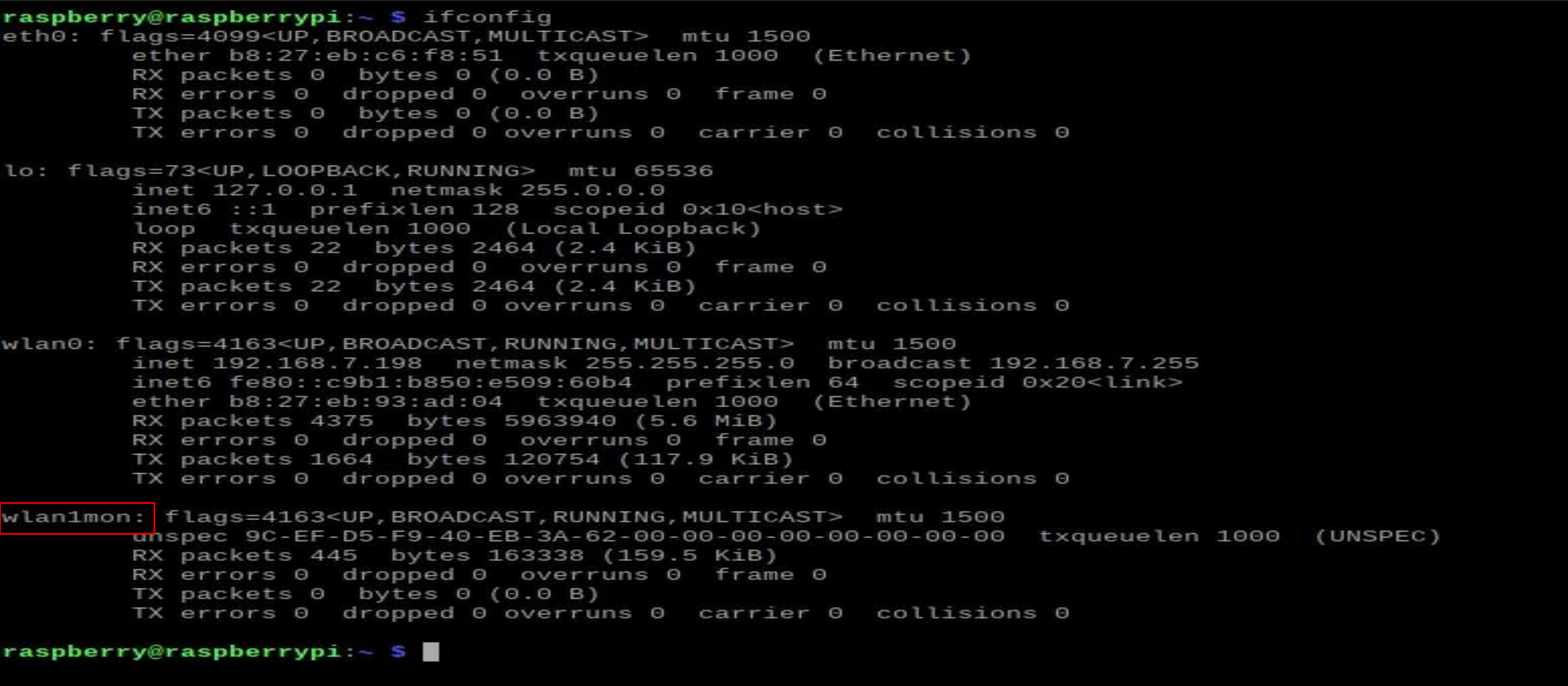
```
raspberry@raspberrypi:~ $ sudo airmon-ng start wlan1

Found 6 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    346 avahi-daemon
    355 avahi-daemon
    436 dhcpcd
    438 wpa_supplicant
    614 wpa_supplicant
   2945 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy2    wlan1           mt76x0u         MediaTek Inc. WiFi
                (mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
                (mac80211 station mode vif disabled for [phy2]wlan1)

raspberry@raspberrypi:~ $ 
```

This puts our Wi-Fi card into listening mode



```
raspberry@raspberrypi:~ $ sudo airmon-ng start wlan1

Found 6 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    346 avahi-daemon
    355 avahi-daemon
    436 dhcpcd
    438 wpa_supplicant
    614 wpa_supplicant
   2945 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy2    wlan1           mt76x0u         MediaTek Inc. WiFi
                (mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
                (mac80211 station mode vif disabled for [phy2]wlan1)

raspberry@raspberrypi:~ $ 
```

Step #6 ifconfig (Who can spot the difference)



```
raspberry@raspberrypi:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:27:eb:c6:f8:51  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

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 22  bytes 2464 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2464 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.198  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::c9b1:b850:e509:60b4  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:93:ad:04  txqueuelen 1000  (Ethernet)
        RX packets 4375  bytes 5963940 (5.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1664  bytes 120754 (117.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 9C-EF-D5-F9-40-EB-3A-62-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 445  bytes 163338 (159.5 KiB)
        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

raspberry@raspberrypi:~ $ 
```

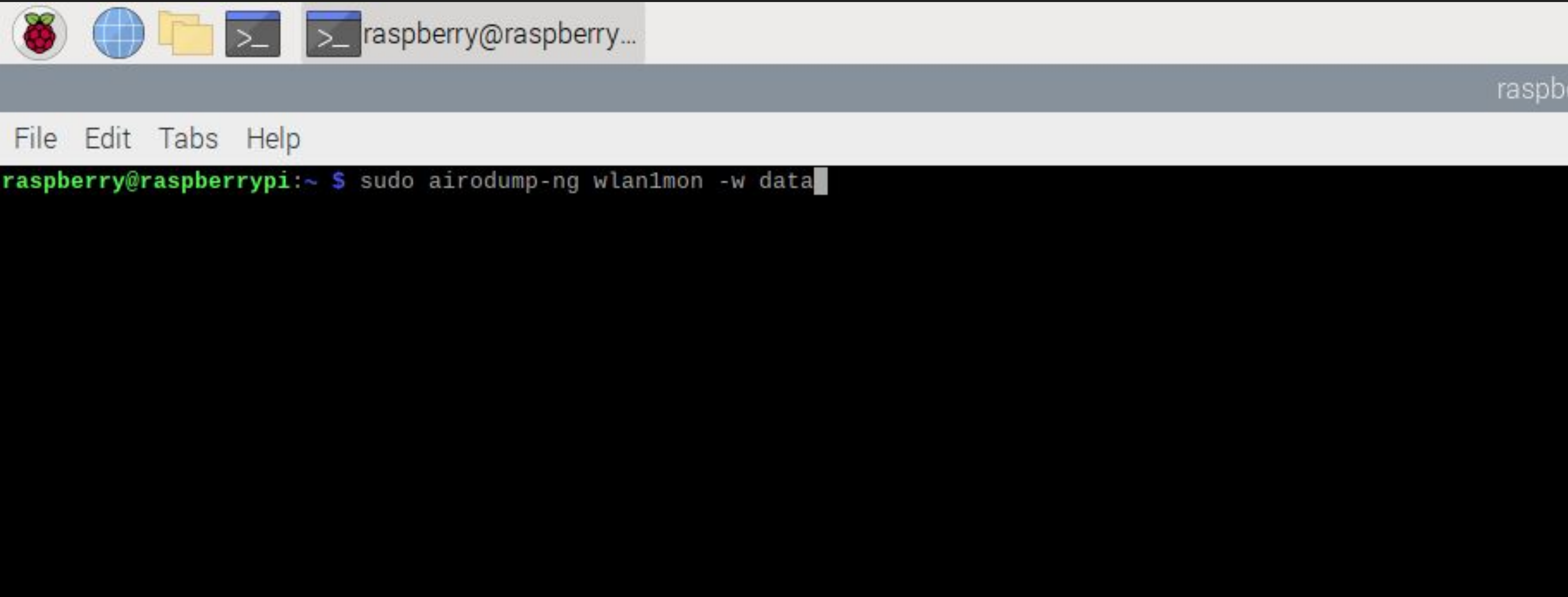
Gather data!

Let’s take a picture of the invisible word of Wi-Fi!

We’re going to learn:

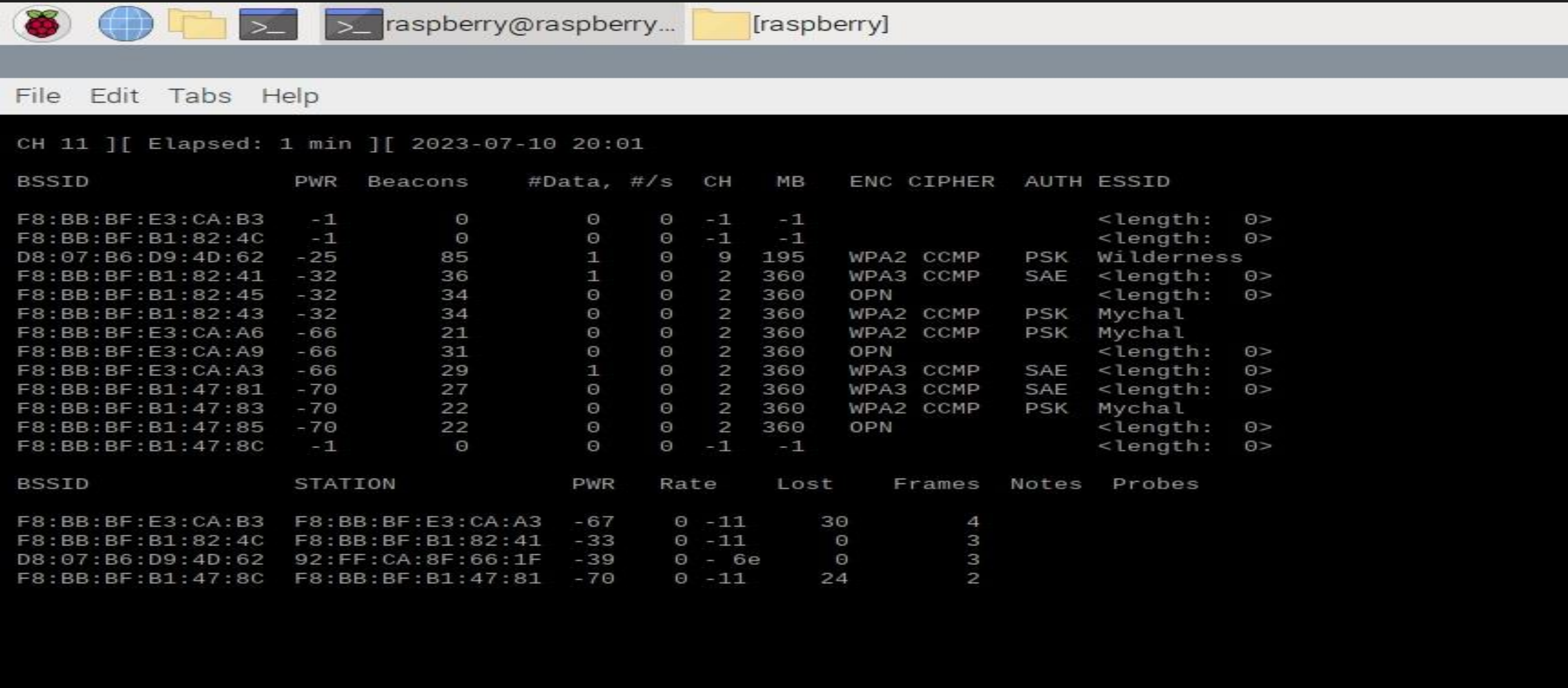
- What Wi-Fi networks are around us
- What devices are connected to those networks

Step #7 sudo airodump-ng wlan1mon -w data



```
raspberry@raspberrypi:~ $ sudo airodump-ng wlan1mon -w data
```

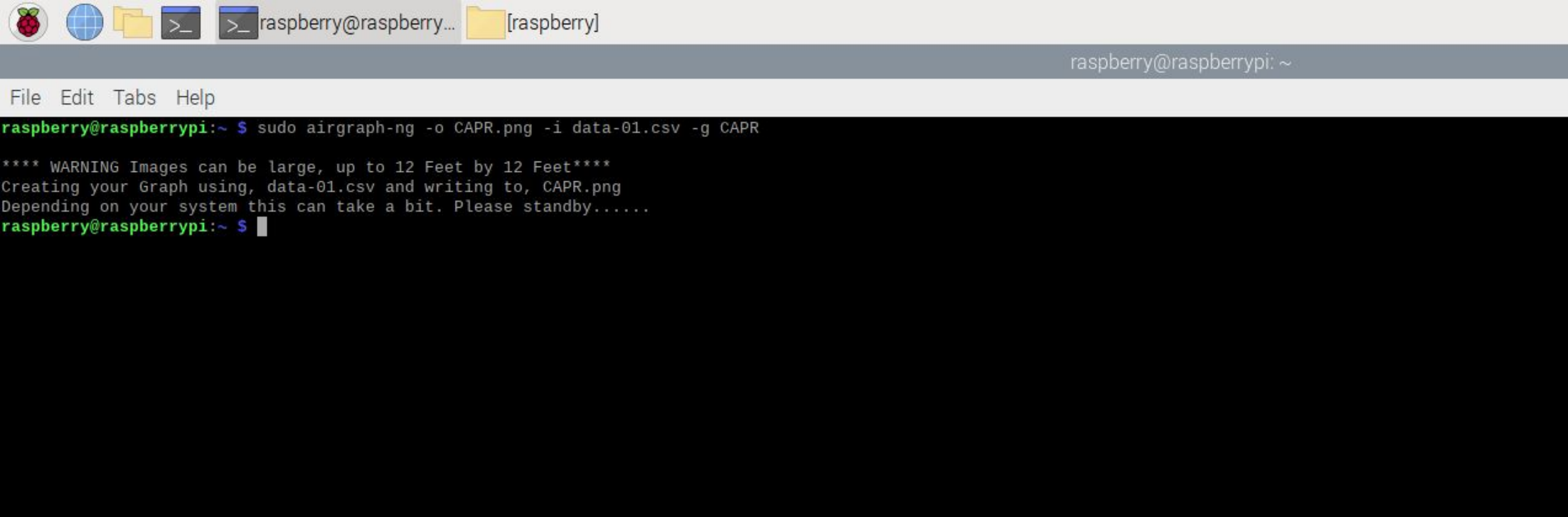
Step #8 Gather data!



```
CH 11 ][ Elapsed: 1 min ][ 2023-07-10 20:01

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER  AUTH ESSID

F8:BB:BF:E3:CA:B3   -1        0        0    0  -1   -1                     <length:  0>
F8:BB:BF:B1:82:4C   -1        0        0    0  -1   -1                     <length:  0>
D8:07:B6:D9:4D:62  -25       85        1    0   9  195   WPA2 CCMP   PSK  Wilderness
F8:BB:BF:B1:82:41  -32       36        1    0   2  360   WPA3 CCMP   SAE  <length:  0>
F8:BB:BF:B1:82:45  -32       34        0    0   2  360   OPN              <length:  0>
F8:BB:BF:B1:82:43  -32       34        0    0   2  360   WPA2 CCMP   PSK  Mychal
F8:BB:BF:E3:CA:A6  -66       21        0    0   2  360   WPA2 CCMP   PSK  Mychal
F8:BB:BF:E3:CA:A9  -66       31        0    0   2  360   OPN              <length:  0>
F8:BB:BF:E3:CA:A3  -66       29        1    0   2  360   WPA3 CCMP   SAE  <length:  0>
F8:BB:BF:B1:47:81  -70       27        0    0   2  360   WPA3 CCMP   SAE  <length:  0>
F8:BB:BF:B1:47:83  -70       22        0    0   2  360   WPA2 CCMP   PSK  Mychal
F8:BB:BF:B1:47:85  -70       22        0    0   2  360   OPN              <length:  0>
F8:BB:BF:B1:47:8C   -1        0        0    0  -1   -1                     <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F8:BB:BF:E3:CA:B3  F8:BB:BF:E3:CA:A3  -67    0 -11     30        4
F8:BB:BF:B1:82:4C  F8:BB:BF:B1:82:41  -33    0 -11      0        3
D8:07:B6:D9:4D:62  92:FF:CA:8F:66:1F  -39    0 - 6e     0        3
F8:BB:BF:B1:47:8C  F8:BB:BF:B1:47:81  -70    0 -11     24        2
```

Step #9 Create your graph

Sudo airgraph-ng -o CAPR.png -i data-01.csv -g CAPR

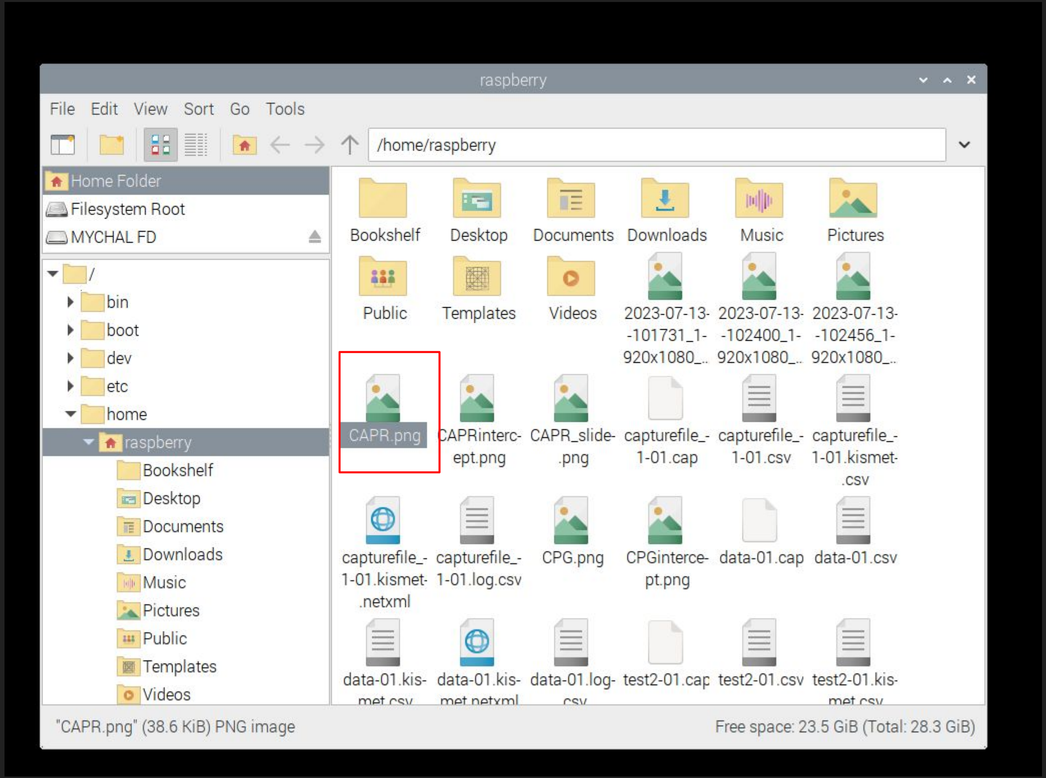


```
raspberry@raspberrypi:~ $ sudo airgraph-ng -o CAPR.png -i data-01.csv -g CAPR

**** WARNING Images can be large, up to 12 Feet by 12 Feet****
Creating your Graph using, data-01.csv and writing to, CAPR.png
Depending on your system this can take a bit. Please standby......
raspberry@raspberrypi:~ $ 
```

Review results

Step #10

- Open your the file manager and find the graph you just created.
- CAPR.png
- This graph will show us nearby access points and which clients are connected to them

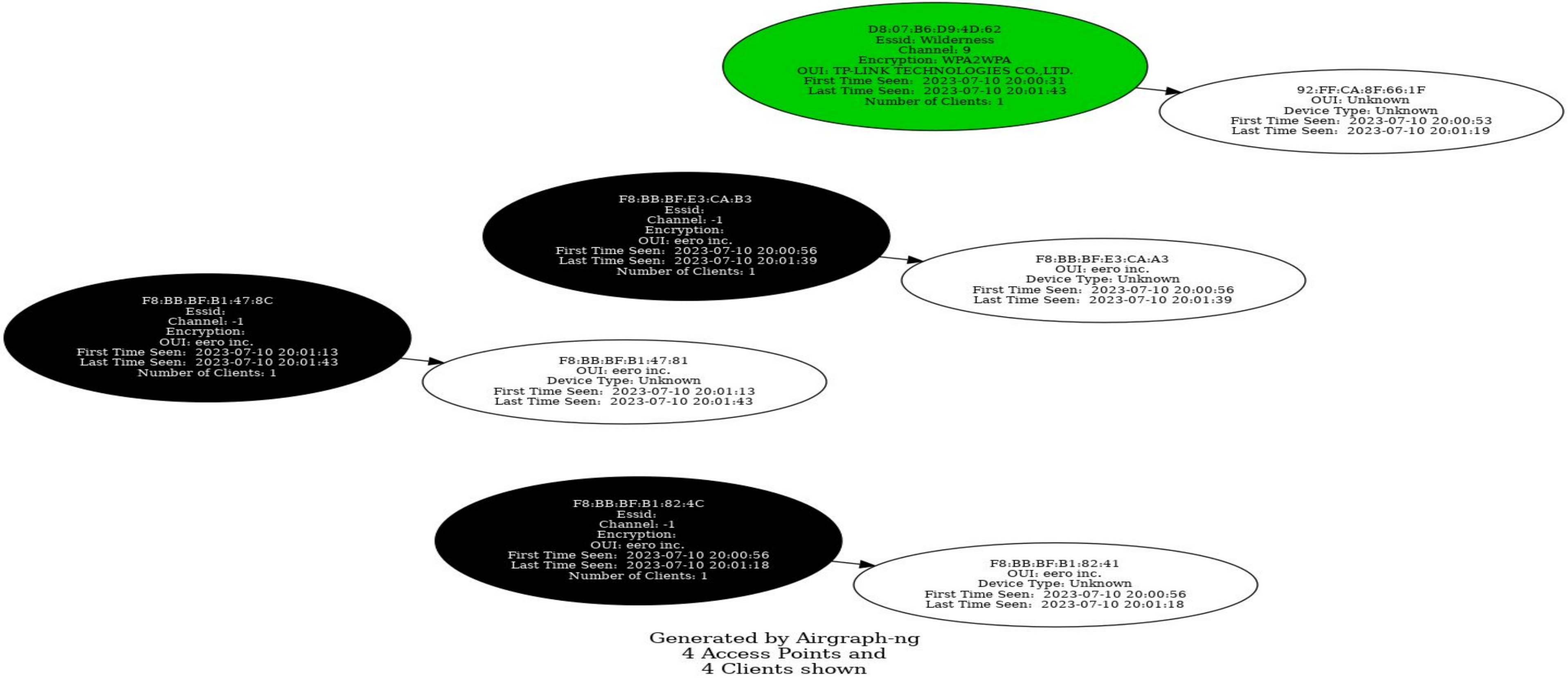


/home/raspberry

"CAPR.png" (38.6 KiB) PNG image

Free space: 23.5 GiB (Total: 28.3 GiB)

Step # 11



D8:07:B6:D9:4D:62
Essid: Wilderness
Channel: 9
Encryption: WPA2WPA
OUI: TP-LINK TECHNOLOGIES CO.,LTD.
First Time Seen: 2023-07-10 20:00:31
Last Time Seen: 2023-07-10 20:01:43
Number of Clients: 1

92:FF:CA:8F:66:1F
OUI: Unknown
Device Type: Unknown
First Time Seen: 2023-07-10 20:00:53
Last Time Seen: 2023-07-10 20:01:19

F8:BB:BF:E3:CA:B3
Essid:
Channel: -1
Encryption:
OUI: eero inc.
First Time Seen: 2023-07-10 20:00:56
Last Time Seen: 2023-07-10 20:01:39
Number of Clients: 1

F8:BB:BF:E3:CA:A3
OUI: eero inc.
Device Type: Unknown
First Time Seen: 2023-07-10 20:00:56
Last Time Seen: 2023-07-10 20:01:39

F8:BB:BF:B1:47:8C
Essid:
Channel: -1
Encryption:
OUI: eero inc.
First Time Seen: 2023-07-10 20:01:13
Last Time Seen: 2023-07-10 20:01:43
Number of Clients: 1

F8:BB:BF:B1:47:81
OUI: eero inc.
Device Type: Unknown
First Time Seen: 2023-07-10 20:01:13
Last Time Seen: 2023-07-10 20:01:43

F8:BB:BF:B1:82:4C
Essid:
Channel: -1
Encryption:
OUI: eero inc.
First Time Seen: 2023-07-10 20:00:56
Last Time Seen: 2023-07-10 20:01:18
Number of Clients: 1

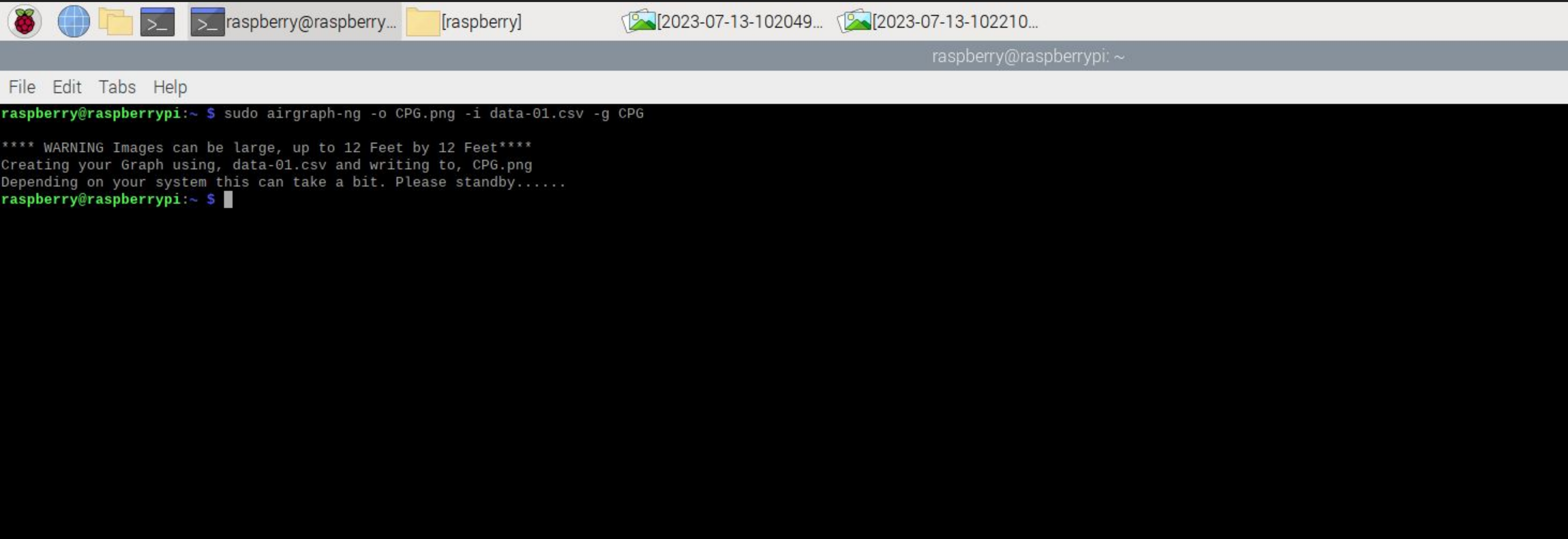
F8:BB:BF:B1:82:41
OUI: eero inc.
Device Type: Unknown
First Time Seen: 2023-07-10 20:00:56
Last Time Seen: 2023-07-10 20:01:18

Generated by Airgraph-ng
4 Access Points and
4 Clients shown

Step #12

sudo airgraph-ng -o CPG.png -i data-01.csv -g CPG

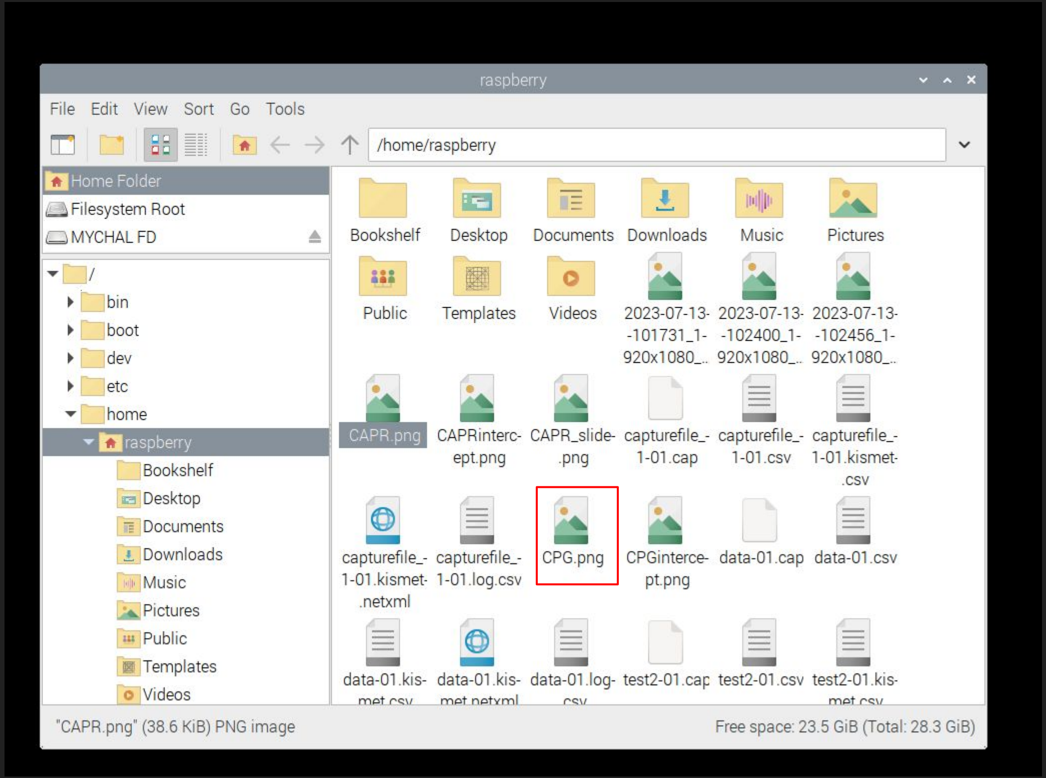
This will allow us to see other networks devices are trying to connect to

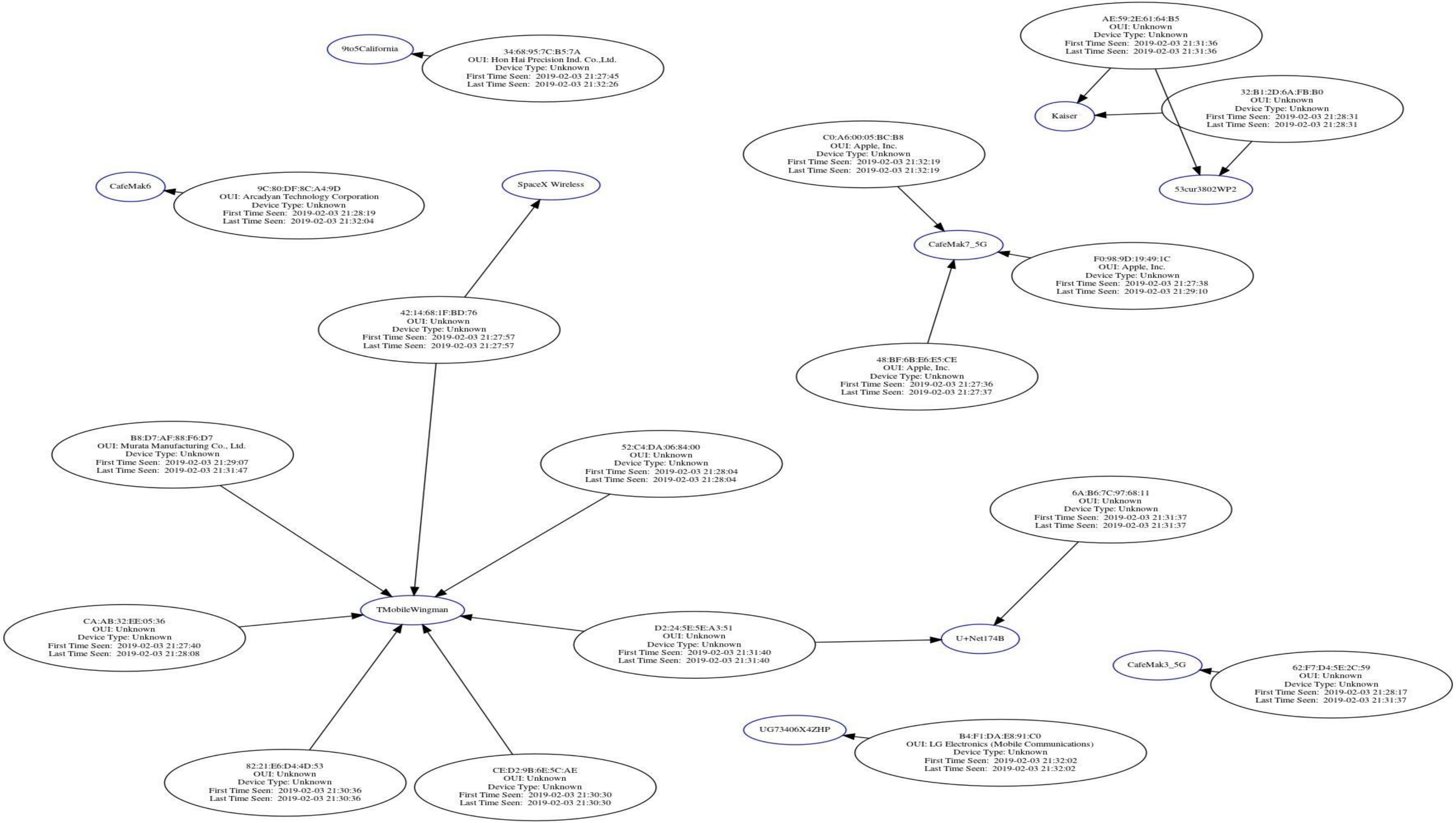


```
raspberry@raspberrypi:~ $ sudo airgraph-ng -o CPG.png -i data-01.csv -g CPG

**** WARNING Images can be large, up to 12 Feet by 12 Feet****
Creating your Graph using, data-01.csv and writing to, CPG.png
Depending on your system this can take a bit. Please standby......
raspberry@raspberrypi:~ $ 
```

Step #13

- Open your the file manager and find the graph you just created.
- CPG.png
- This graph is a little different. It will show clients and the networks they are trying to connect to




9to5California
34:68:95:7C:B5:7A
OUI: Hon Hai Precision Ind. Co.,Ltd.
Device Type: Unknown
First Time Seen: 2019-02-03 21:27:45
Last Time Seen: 2019-02-03 21:32:26
AE:59:2E:61:64:B5
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:31:36
Last Time Seen: 2019-02-03 21:31:36
Kaiser
32:B1:2D:6A:FB:B0
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:28:31
Last Time Seen: 2019-02-03 21:28:31
53cur3802WP2
C0:A6:00:05:BC:B8
OUI: Apple, Inc.
Device Type: Unknown
First Time Seen: 2019-02-03 21:32:19
Last Time Seen: 2019-02-03 21:32:19
CafeMak6
9C:80:DF:8C:A4:9D
OUI: Arcadyan Technology Corporation
Device Type: Unknown
First Time Seen: 2019-02-03 21:28:19
Last Time Seen: 2019-02-03 21:32:04
SpaceX Wireless
CafeMak7_5G
F0:98:9D:19:49:1C
OUI: Apple, Inc.
Device Type: Unknown
First Time Seen: 2019-02-03 21:27:38
Last Time Seen: 2019-02-03 21:29:10
42:14:68:1F:BD:76
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:27:57
Last Time Seen: 2019-02-03 21:27:57
48:BF:6B:E6:E5:CE
OUI: Apple, Inc.
Device Type: Unknown
First Time Seen: 2019-02-03 21:27:36
Last Time Seen: 2019-02-03 21:27:37
B8:D7:AF:88:F6:D7
OUI: Murata Manufacturing Co., Ltd.
Device Type: Unknown
First Time Seen: 2019-02-03 21:29:07
Last Time Seen: 2019-02-03 21:31:47
52:C4:DA:06:84:00
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:28:04
Last Time Seen: 2019-02-03 21:28:04
6A:B6:7C:97:68:11
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:31:37
Last Time Seen: 2019-02-03 21:31:37
TMobileWingman
CA:AB:32:EE:05:36
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:27:40
Last Time Seen: 2019-02-03 21:28:08
D2:24:5E:5E:A3:51
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:31:40
Last Time Seen: 2019-02-03 21:31:40
U+Net174B
CafeMak3_5G
62:F7:D4:5E:2C:59
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:28:17
Last Time Seen: 2019-02-03 21:31:37
UG73406X4ZHP
B4:F1:DA:E8:91:C0
OUI: LG Electronics (Mobile Communications)
Device Type: Unknown
First Time Seen: 2019-02-03 21:32:02
Last Time Seen: 2019-02-03 21:32:02
82:21:E6:D4:4D:53
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:30:36
Last Time Seen: 2019-02-03 21:30:36
CE:D2:9B:6E:5C:AE
OUI: Unknown
Device Type: Unknown
First Time Seen: 2019-02-03 21:30:30
Last Time Seen: 2019-02-03 21:30:30

What do you think?

How could these tools be useful

Do you think we can:

Tell who is home by which Wi-Fi devices are connected?

Do you think we can:

See what kind of Wi-Fi devices your neighbors have?

Do you think we can:

Find out if someone is connected to my Wi-Fi without permission?