**CRYTPOGRAPHY**

**LAB - 2: Breaching WPA2 Personal**

**CS 6343, Summer 2022**

**Venkata Vijaya Vasavi Manyala**

**R1176833**

**Part-1:**

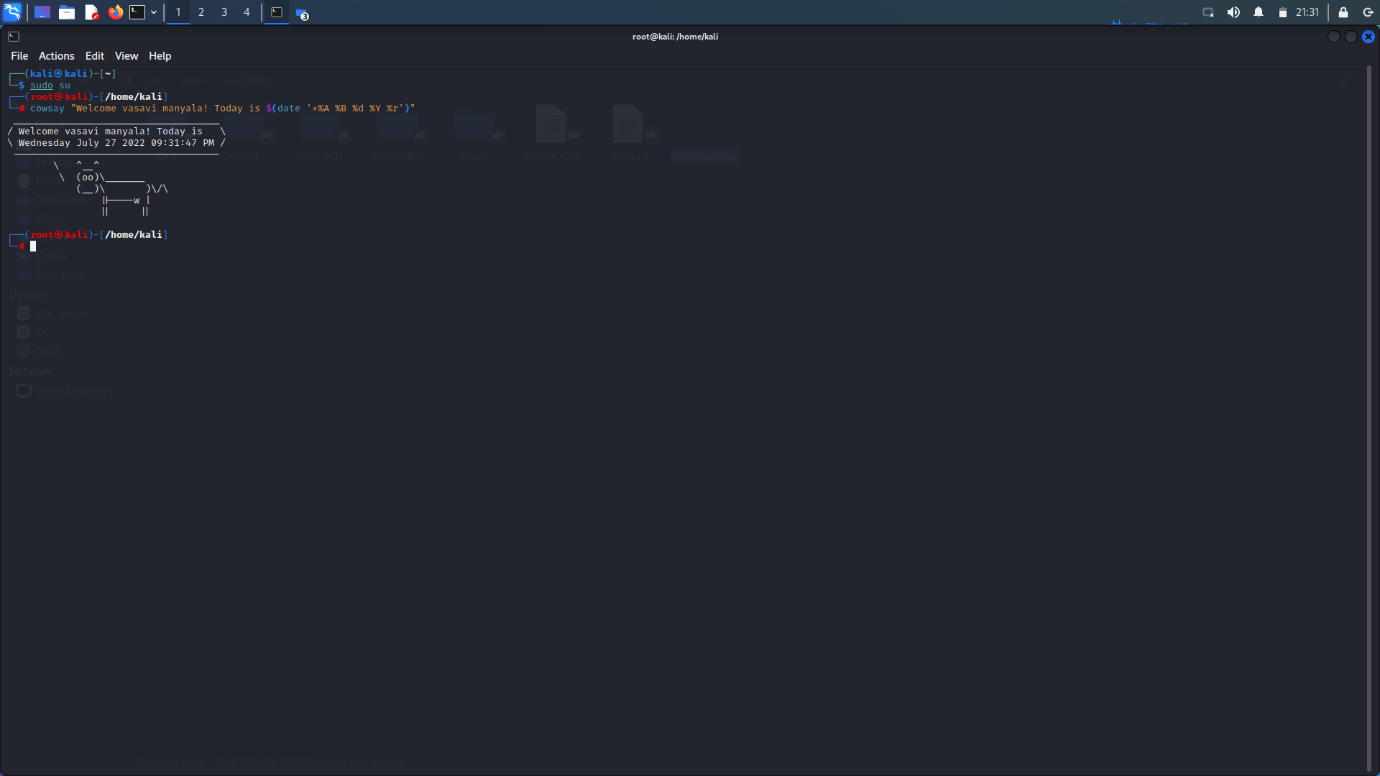
As per instructed ive installed cowsay and aircrack –ng for timestamp and cracking the password respectively.

Below are the options that we can use to implement assigned task.

* Dual Boot OS option
* Using a virtual box
* Using live USB

1. **Cowsay:**

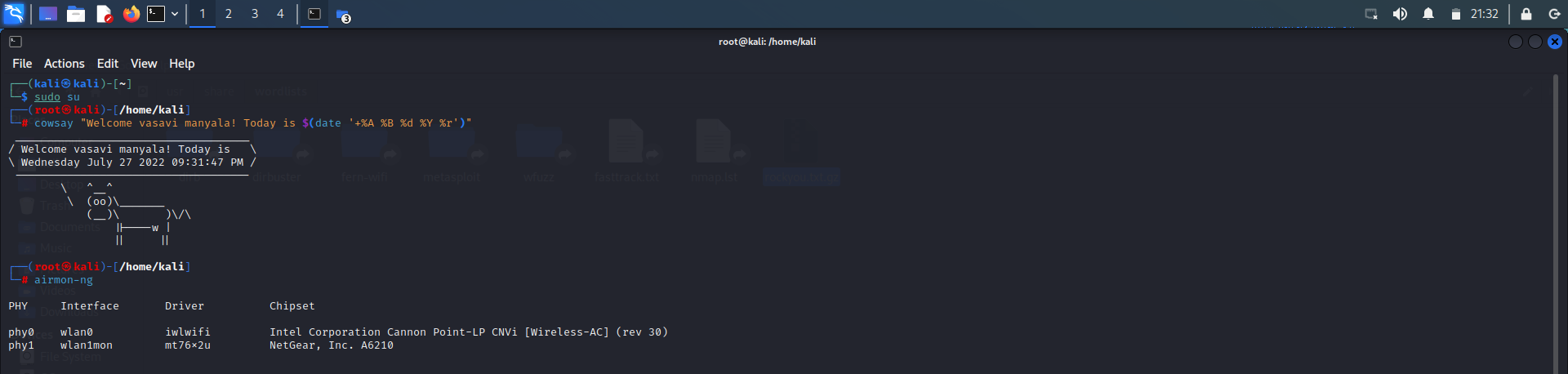
To install we use command - *sudo apt-get install cowsay*.



**2. Airmon-ng**

This will be helpful to detect the wireless adapter. Airmon-ng is a command we used to switch to monitor mode and managed mode and it will display the status of the interfaces without any parameters in the command

**Command:** *airmon-ng*

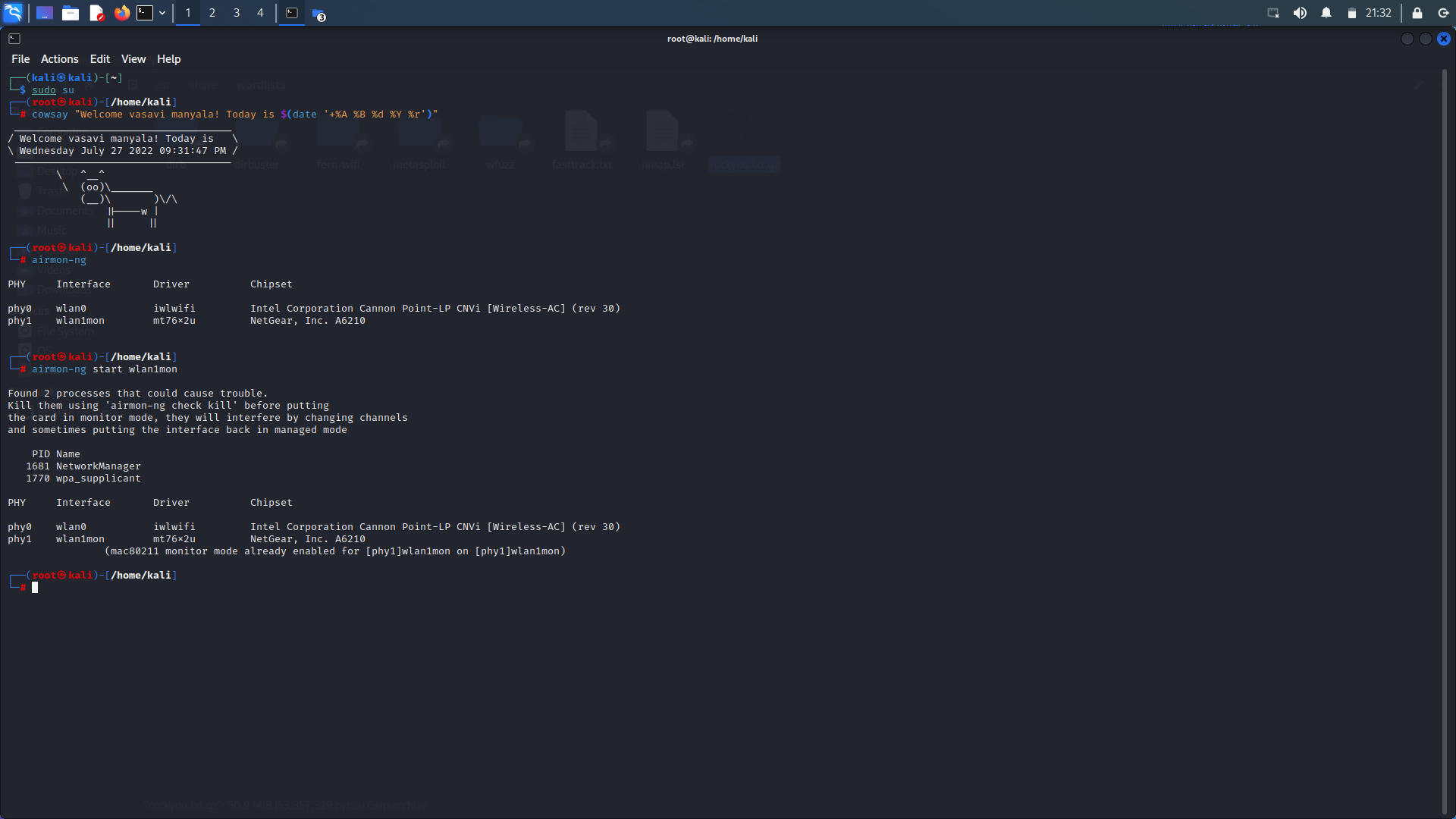


We can observe, airmon –ng has detected the network adapter (Netgear) which is used in the experiment.

**Command:** *airmon-ng start wlan1*

It is used to switch the interface to the monitor mode and if we can observe it has detected 2 errors which has to be killed and switched back to monitor mode.

Here we can see the wlan1 interface into monitor mode.



3. **Airodump-ng:**

airodump-ng is used to generate a text file which contains the information about all the access points and clients encountered. Airodump-ng can log the coordinates of detected access sites.

**Command:** *airodump-ng wlan1*

****

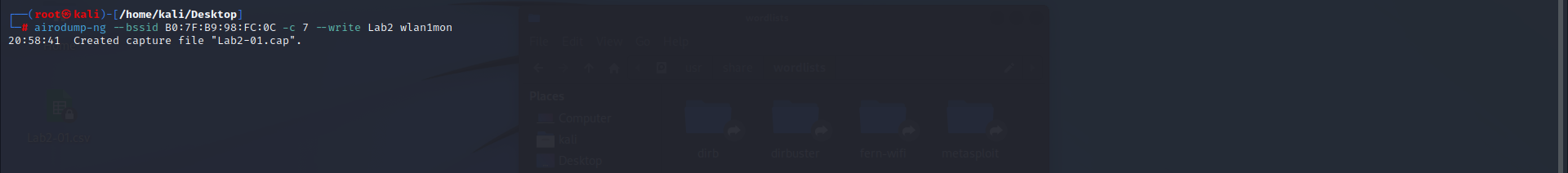
4. In the above picture we can observe the ssid ‘***CS-6343-2022*’** the SSID in-turn contains BSSID.

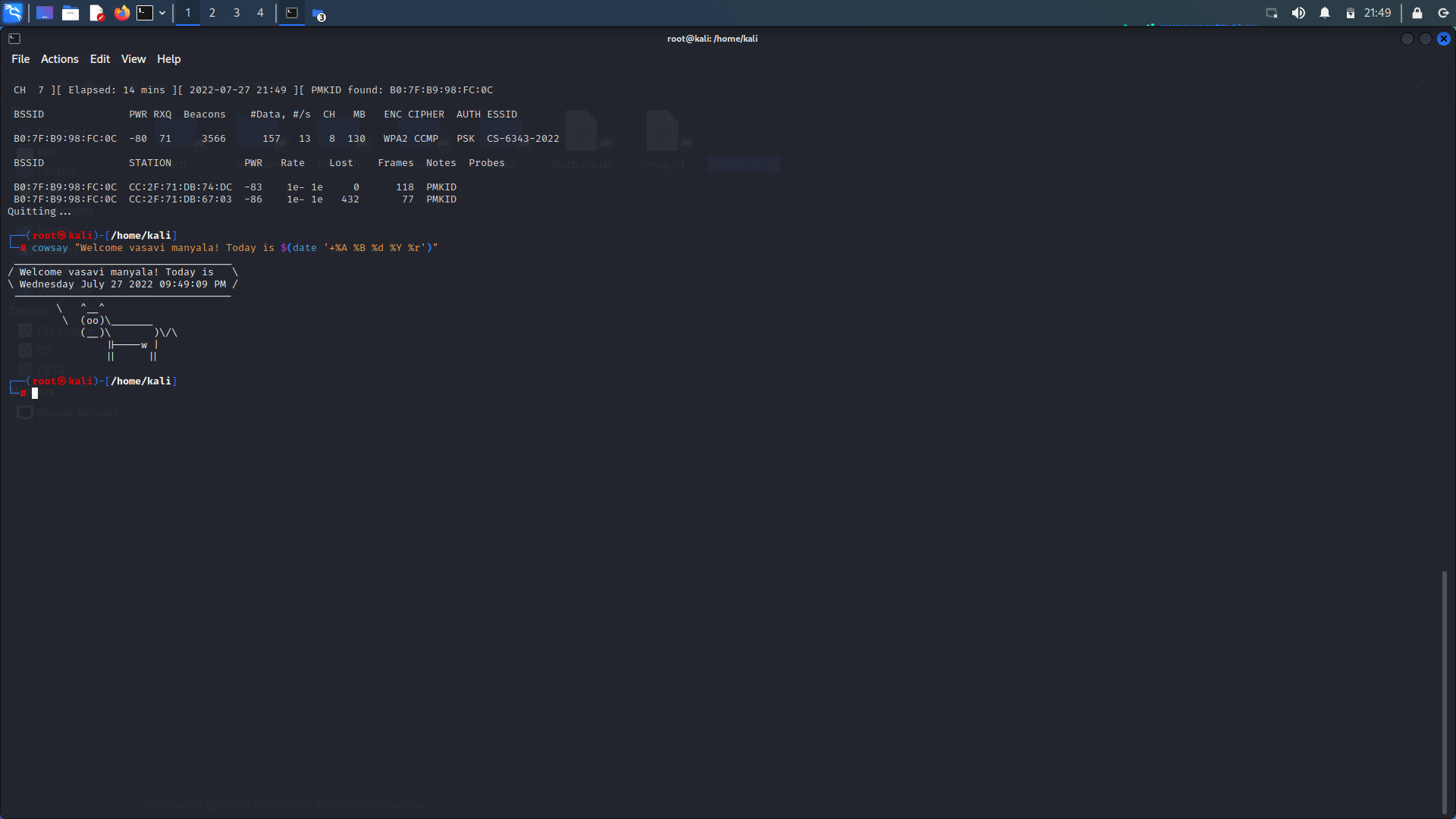
Next step is to capture the WPA handshake by using the below command.

**Command:** *airodump-ng –bssid B0:7F:B9:98:FC:0C -c 7 –write Lab2 wlan1mon*

I have taken the BSSID of CS-6343-2022 and -c which is the channel of the SSID. And it will create a file to save the data which is captured.

Therefore we can observe wlan1which is in monitor mode.





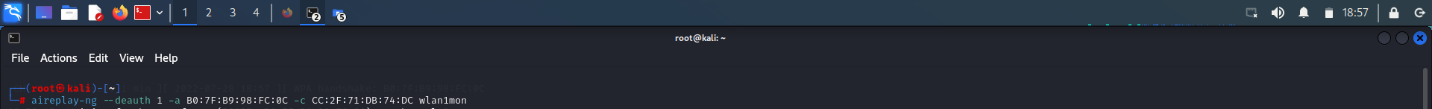
5. It is observed that the 4 way handshake is happened in channel 7 which has elapsed in 14 minutes.

WPA Handshake is a 4-way handshake:

* The client delivers his SNONCE to the AP along with a MIC. The MIC is used by the AP to verify that the message is truly from this client, like a signature.
* Now that the AP has received the message, he has everything he needs to generate the PTK, which he accomplishes.
* Because he will be his new client, the Access Point transmits the GTK to the client.
* The client downloads and installs GTK (Group Temporal Key).
* The client informs the AP that everything is in working order and that it has been installed.

6. To observe and detect the handshake, force one or more clients who are currently associated with the Access Point (AP) to disassociate.

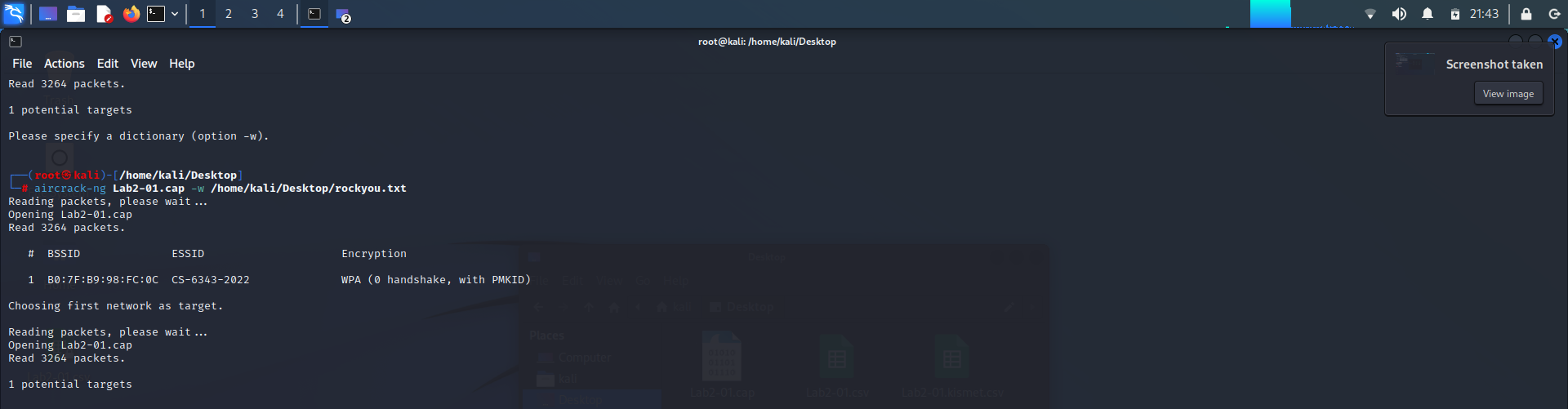
**command**: *aireplay-ng -- deauth 1 –a B0:7f:B9:98:fC:0C –c CC:2F:71:DB:74:DC wlan1mon*

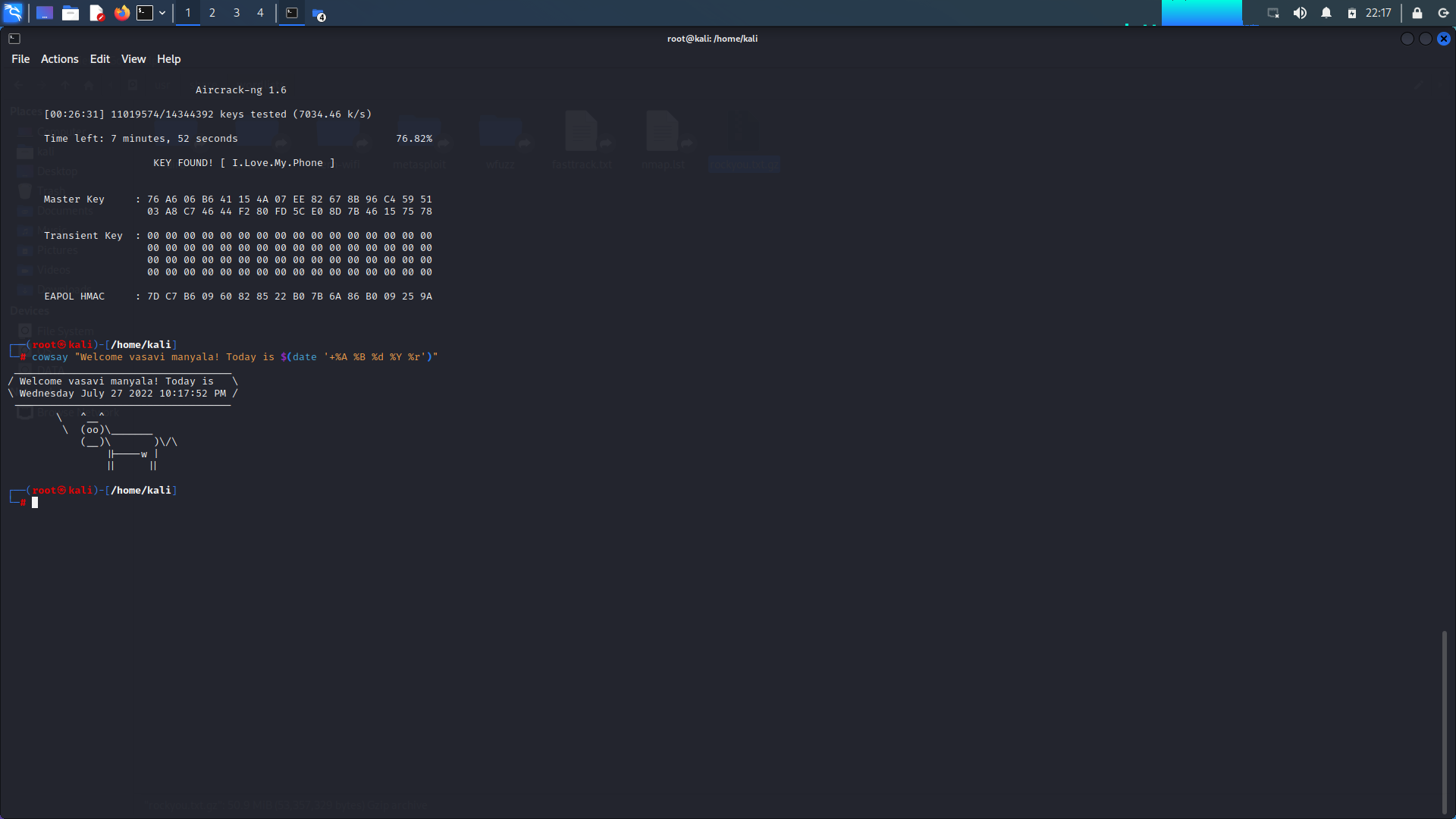


**7. Aircrack-ng**

It is used to capture the data packets and extract them to .txt files for future analysis.

The main function of aircrack-ng is that it is used to detect flaws in Wi-Fi networks security.





After running the above command it will search all the possible packets and crack the password.

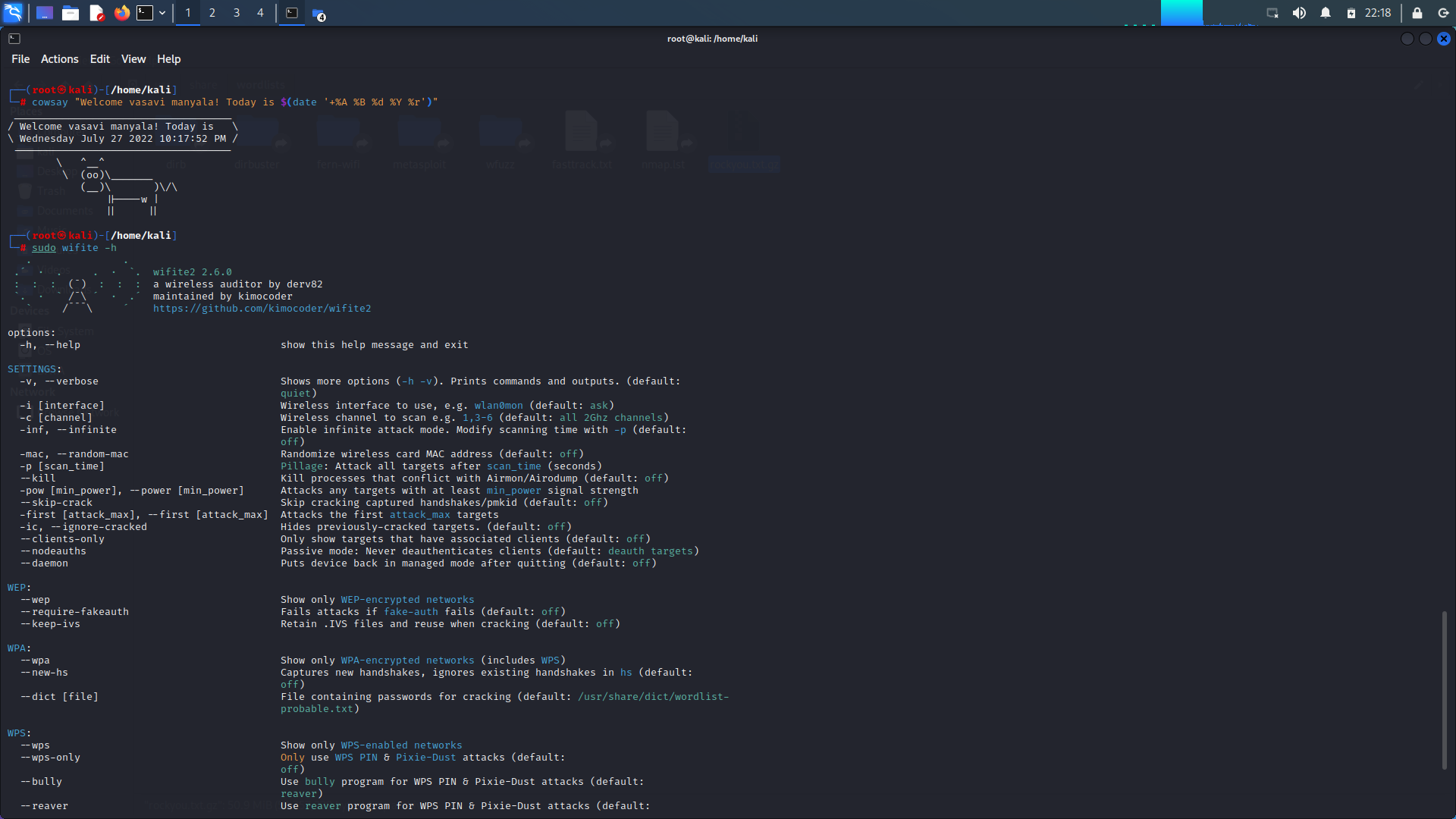
From the above picture we can see it cracked the passcode: I.Love.My.Phone

**Part-2:**

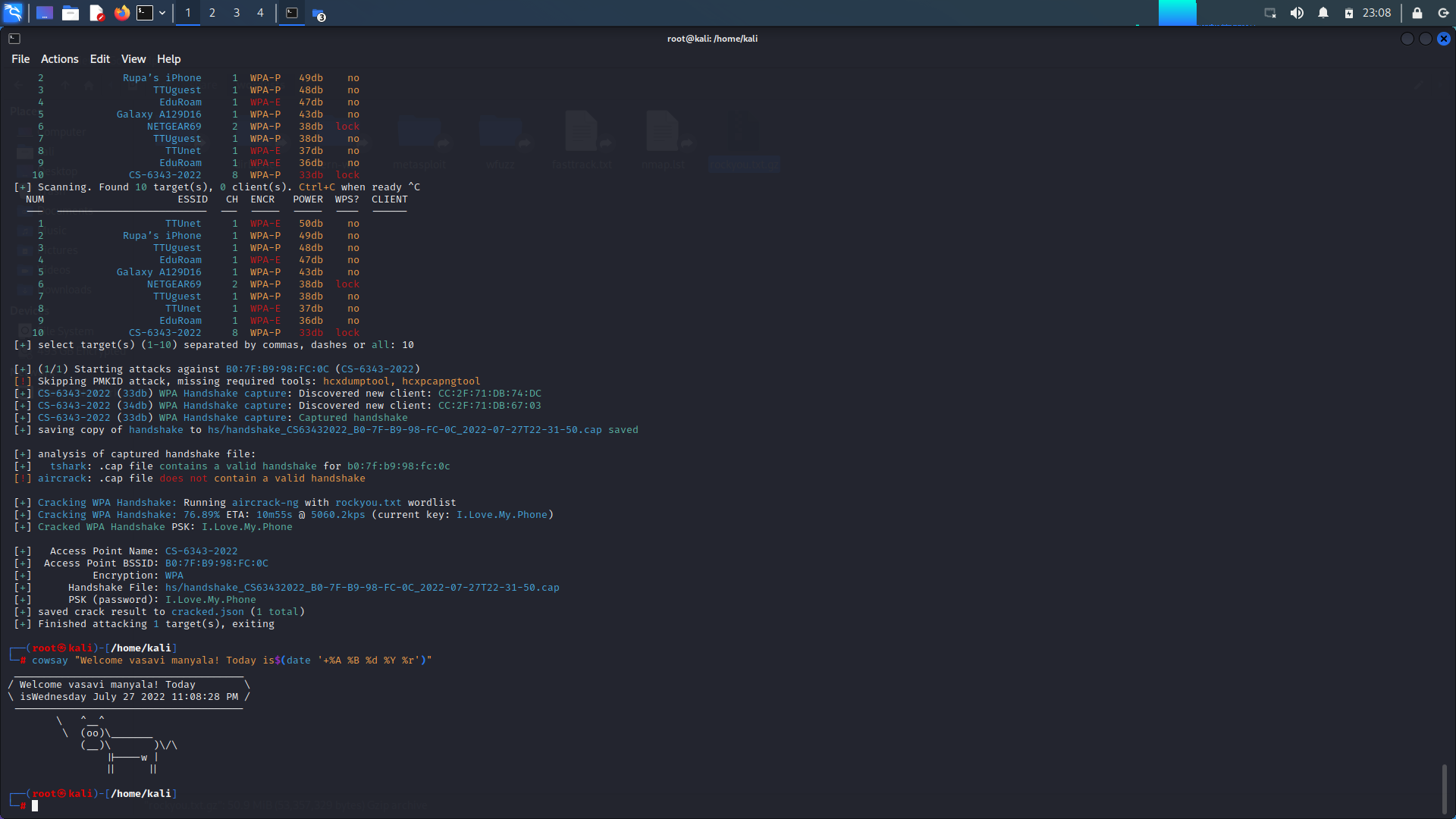
I’ve performed other technique to crack the password again using wifite tool as instructed.

To get the complete detail about wifite tool we used the command

*Sudo wifite –h*

**

**Command:** *sudo wifite –dict /home/kali/Desktop/rockyou.txt*



It is observed that it has cracked the passcode and it is similar passcode in part 1.

Private Shared Key : *I.Love.My.Phone*

* Aireplay command is used to separate message integrity code from other parameters which adds up to the PTK.
* Whereas PTK is defined as the encryption process between the client and the AP (Access Point)
* PTK might require the key factors like Master Key, ANONCE, SNONCE, MAC
* PTK = (PMK + ANONCE + SNONCE + MAC)
* The above command performs list of potential passwords and combines other parameters to check whether the MIC (Message Integrity Code) is been retrieved from the original MIC.

2. $ aircrack-ng Lab2-01.cap –w /home/kali/Desktop/rockyou.txt

It is a dictionary attack which runs on the CPU for which list of passcodes are required. If we could not find any of the passcode which is not present in the list we cannot hack the network password.

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

* The network must be safeguard with the authorized access list.
* By preventing the remote access to your router and the updates has to be done using LAN cable.
* Using a strong and unique passwords which is difficult to crack/attack
* By using a secure VPN (Virtual Private Network) such as Norton Secure VPN, your web traffic will be encrypted and protected from interception.
* Improve the WPA2 security by installing the security updates on regular basis.