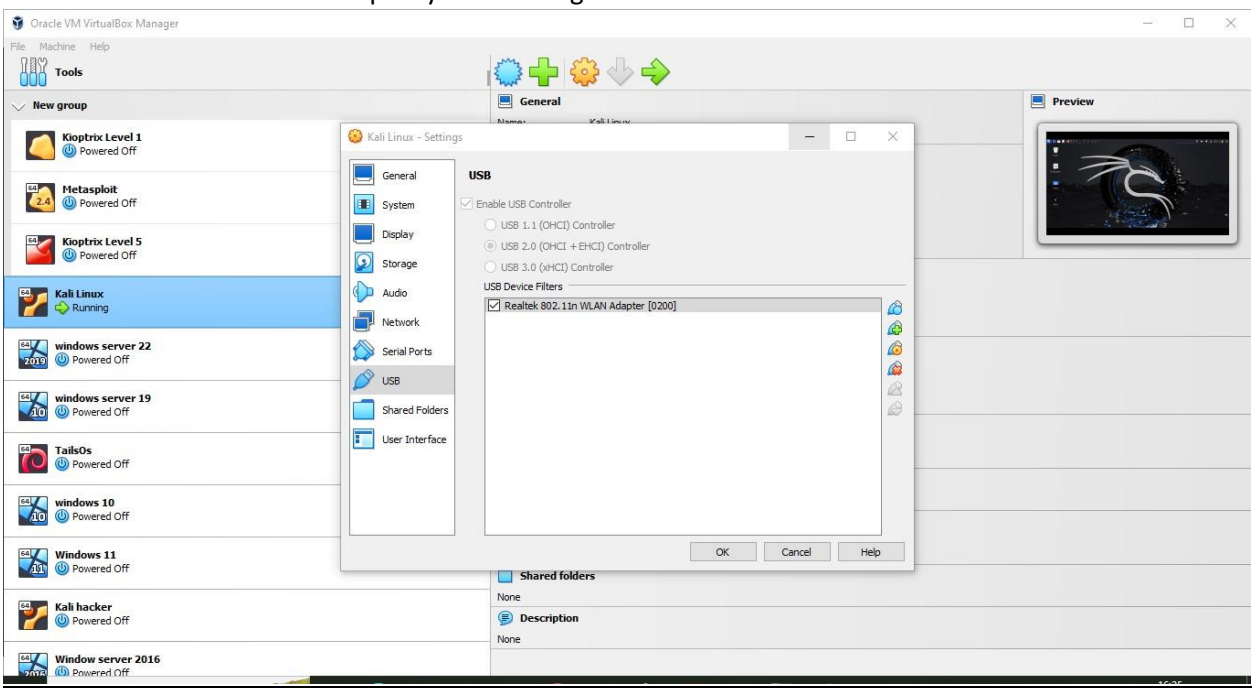
WIRELESS HACKING

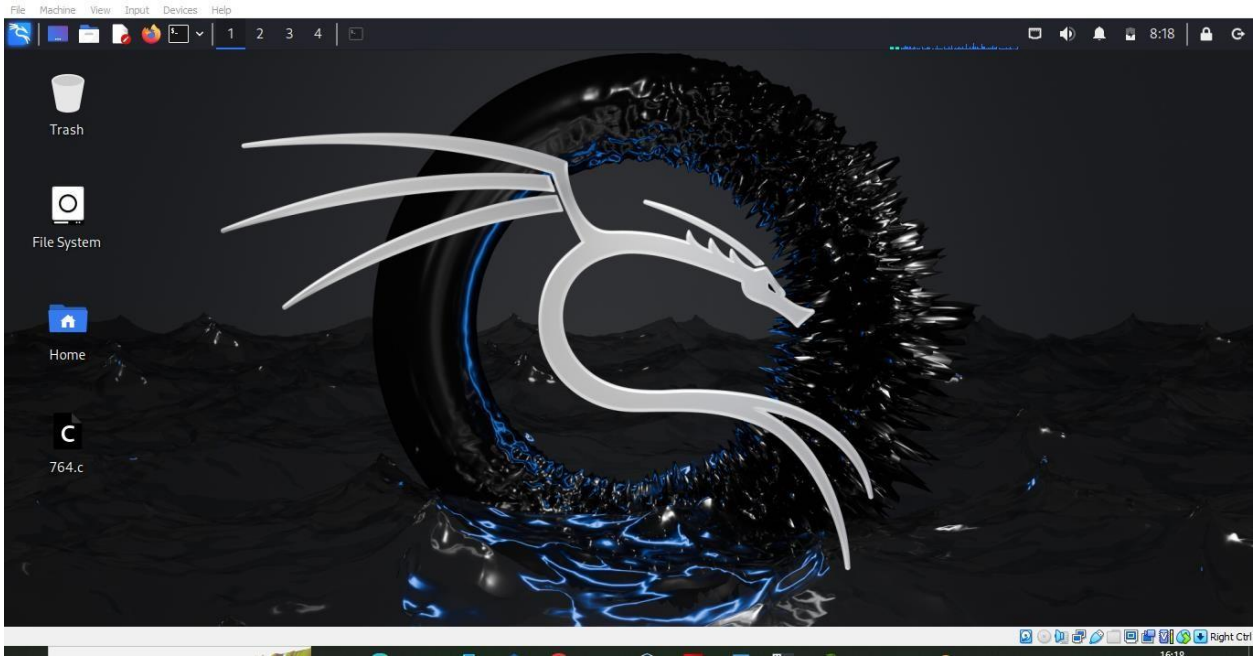
Lab 1

Task : Find Wi-Fi Network and Sniff Wi-Fi Packets using Wash and Wireshark

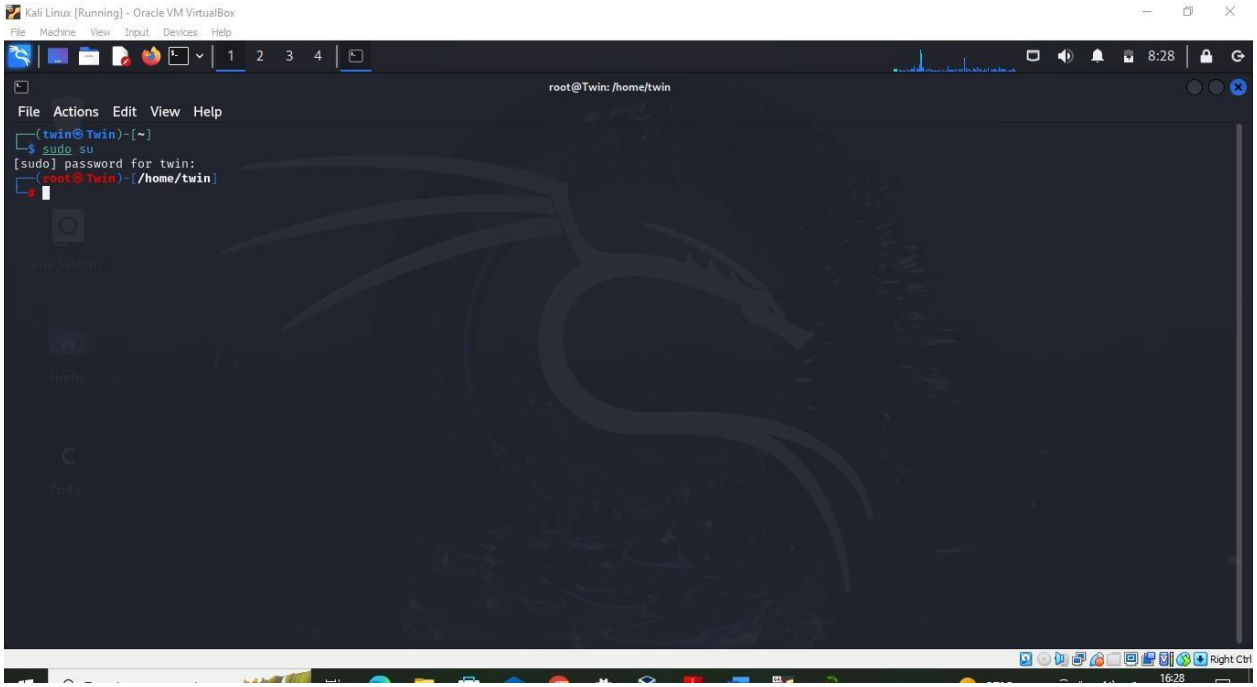
- On your virtual machine, go to your attacking machine setting tab, navigate through **USB** tab, and select the network adapter you are using.



- Turn on **Kali linux** virtual machine.



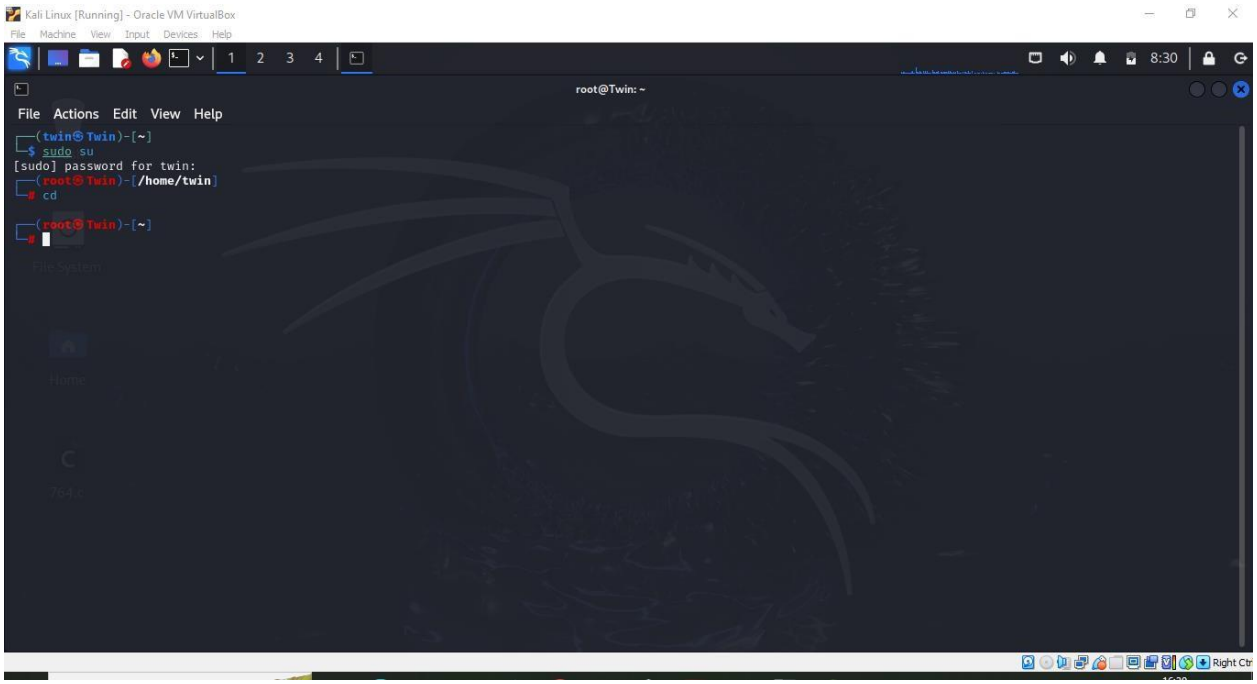
- **In kali linux** terminal window, type sudo **su** and press **Enter** to the programs as a root user.



- In the [sudo]**password for attacker** field, type your password and **press Enter**.

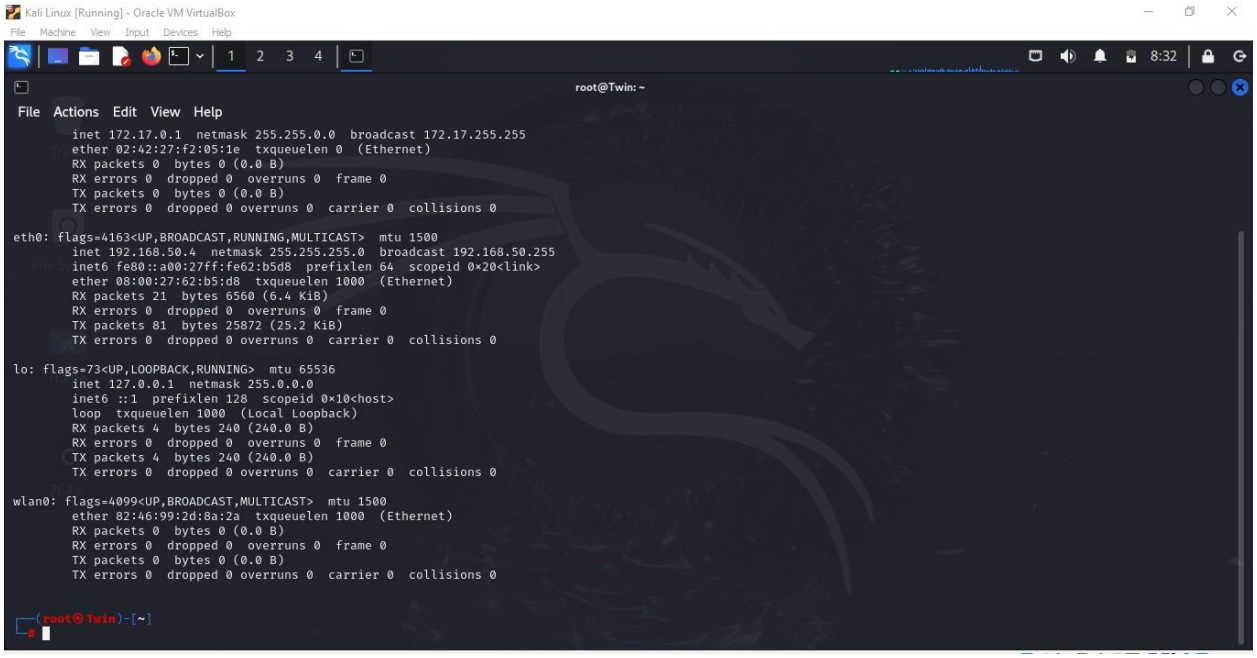
Note: the password that you type will not be visible

- Now, type **cd** and press **Enter** to jump to the root directory.

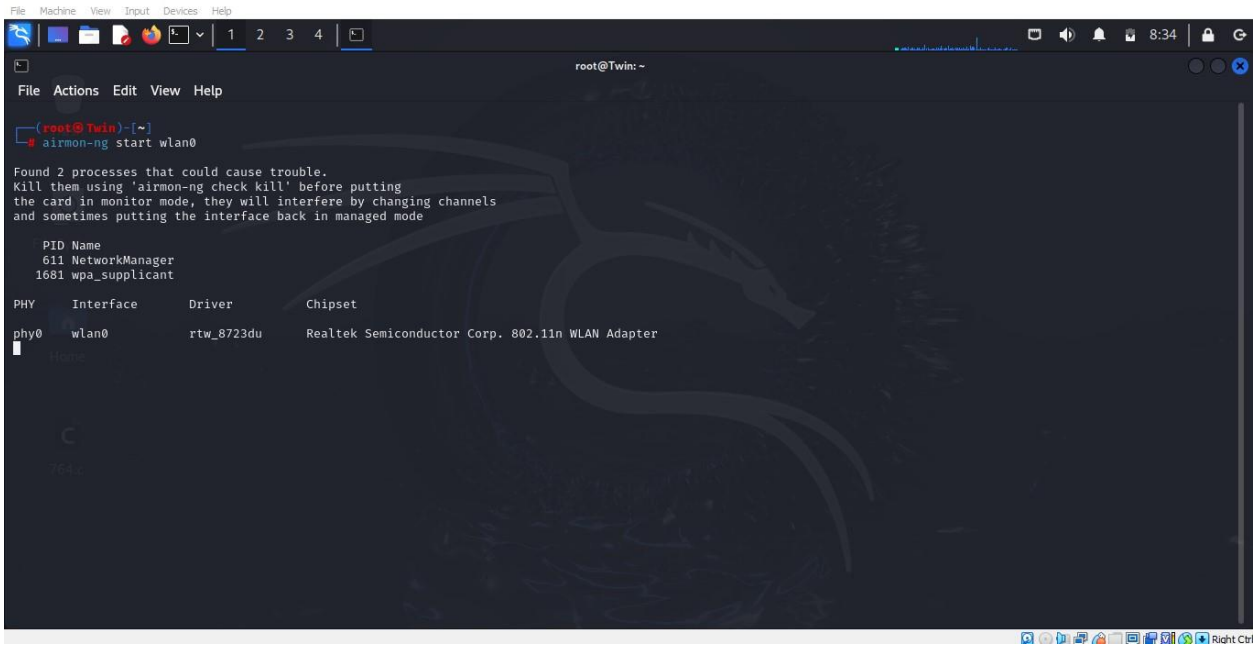


- In the kali linux terminal window, type **ipconfig** and press **enter. Observe** that the wireless interface (in this case, **wlan0)** gets connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.



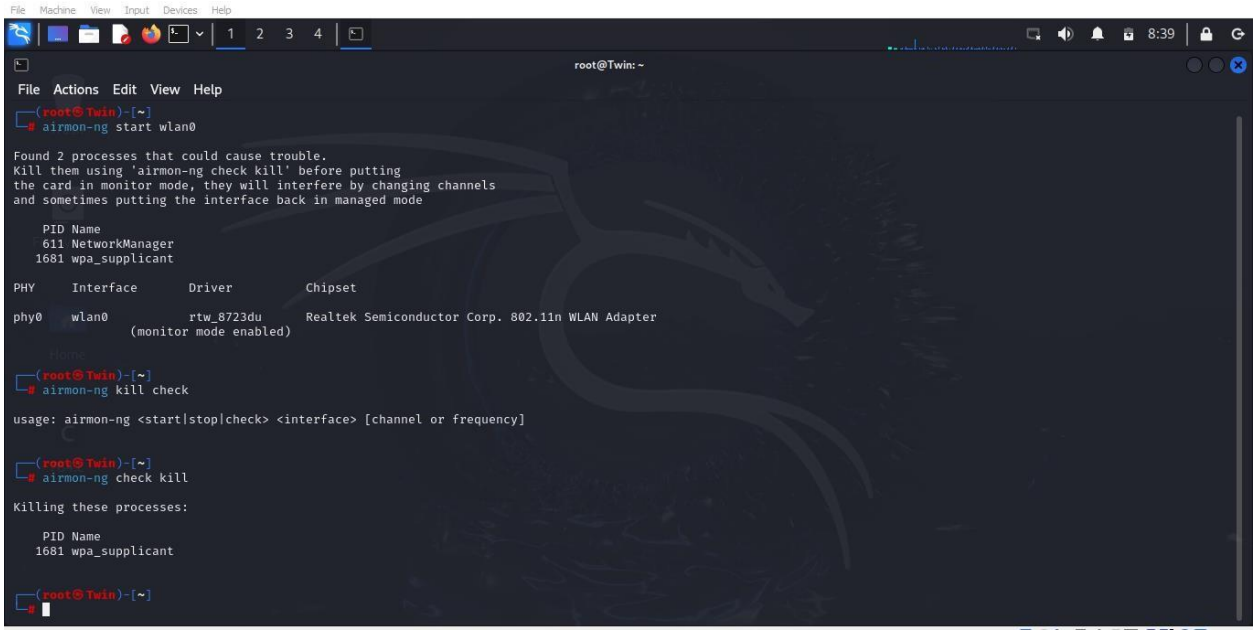
9.in the terminal window, type **airmon-ng start wlan0** and press **enter.** This command puts the wireless interface (in this case, **wlan0)** into monitor mode.



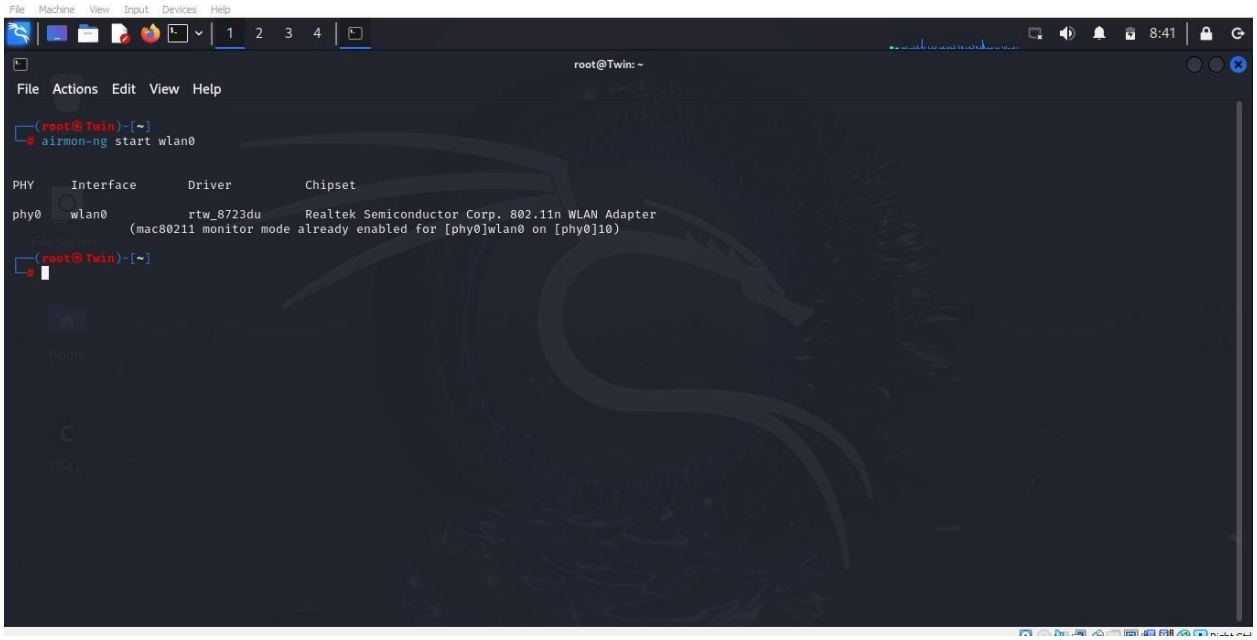
- The result appears, displaying the error:” found **2 processes that could cause trouble.”**

To put the wireless interface in monitor mode, these processes must be killed.

- Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



- Now, run the command **airmon-ng start wian0mon** again to put the wireless interface in monitor mode.

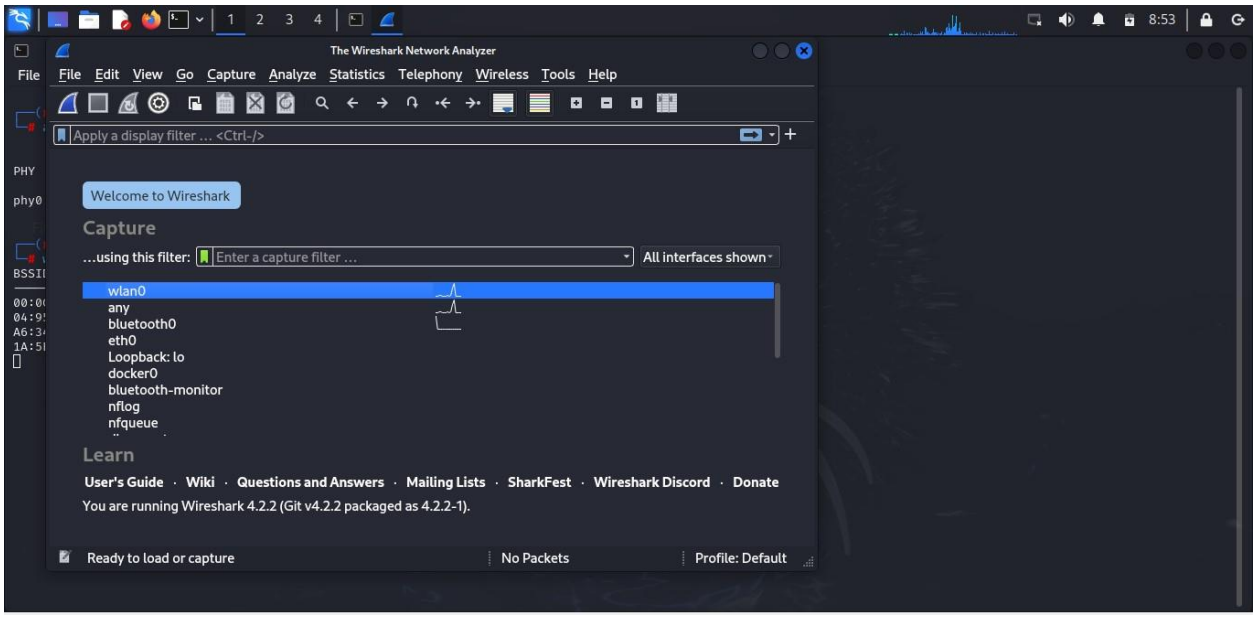


- Note that **802.11 Adapter** now runs in monitor mode on the **wla0** interface, as shown in the screenshot**.**
- Now we shall find Wi-Fi network (access points) by using the wireless interface **wlan0**.
- Type **wash -i wla0** and press **enter** to detect WPS-enabled devices.

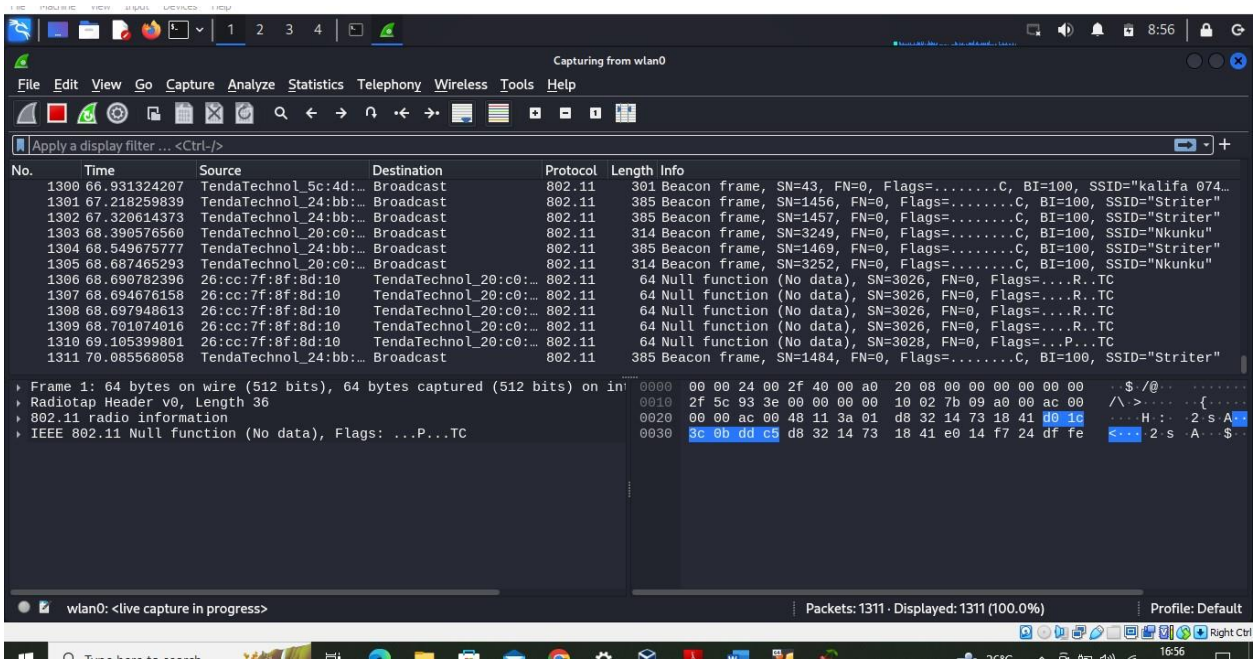
Note: The command, **-I ..interface=<iface>**specifies the interface to capture the packets

- The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

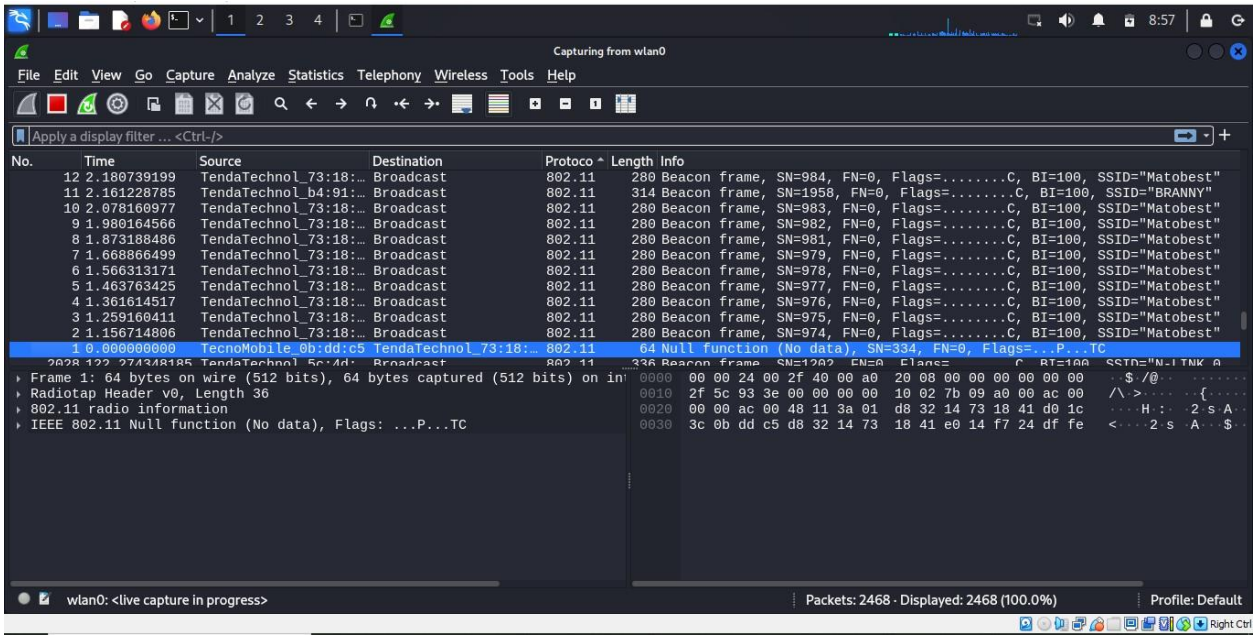
- Now click applications in the top – left corner of desktop and navigate **to pentesting ❼information gathering ❼ Wireshark.**



- A security pop up appears, enter **password** in the password field and click **OK**
- **The Wireshark network analyzer** window appears; double click the wireless network interface (in this case **,wian0mon**)to start capturing network network traffic.



- Wireshark start capturing network traffic. Note that the captured wireless packets are labelled 802.11 under **the protocol** column as shown in the screenshot.



NOTE: In a real-life attack attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites) perform attacks like session hijacking.

- This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.

Lab 2

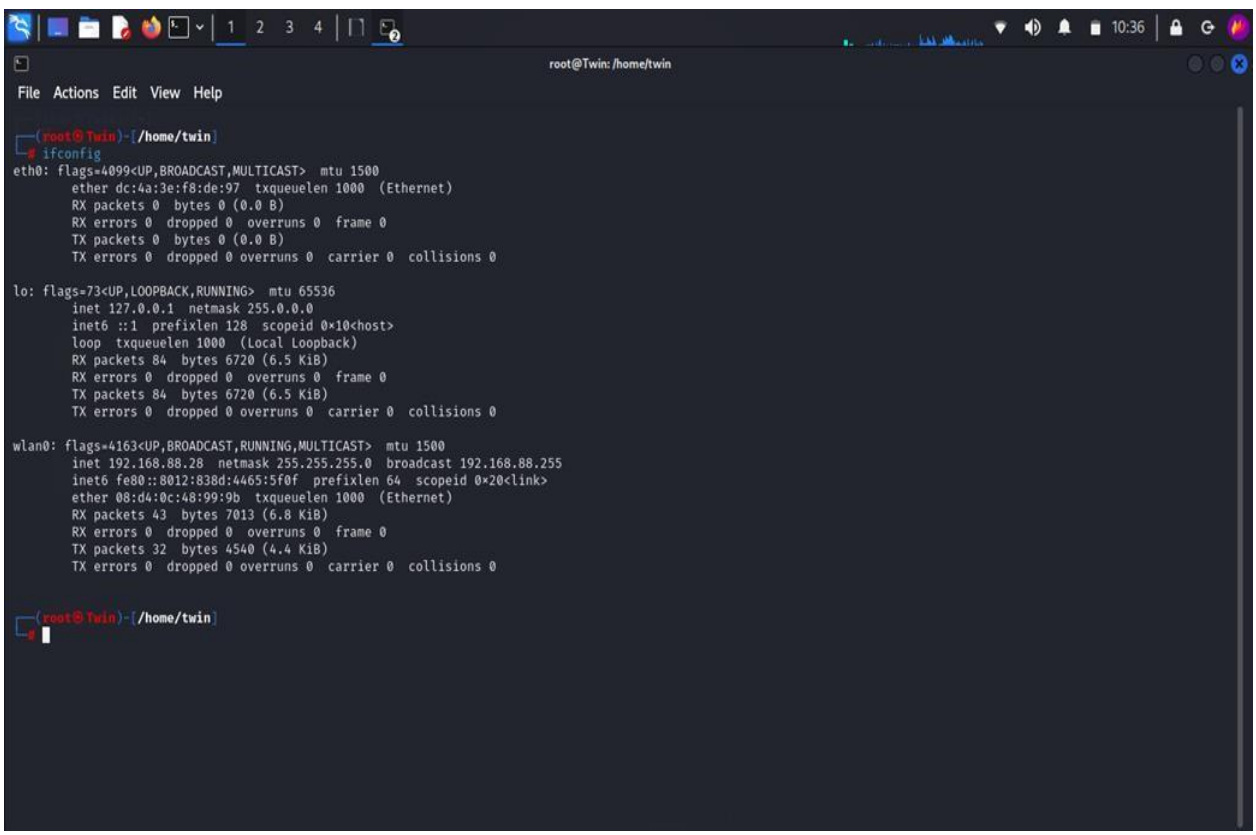
Task: Crack a WAP & WAP2 network using Aircrack-ng

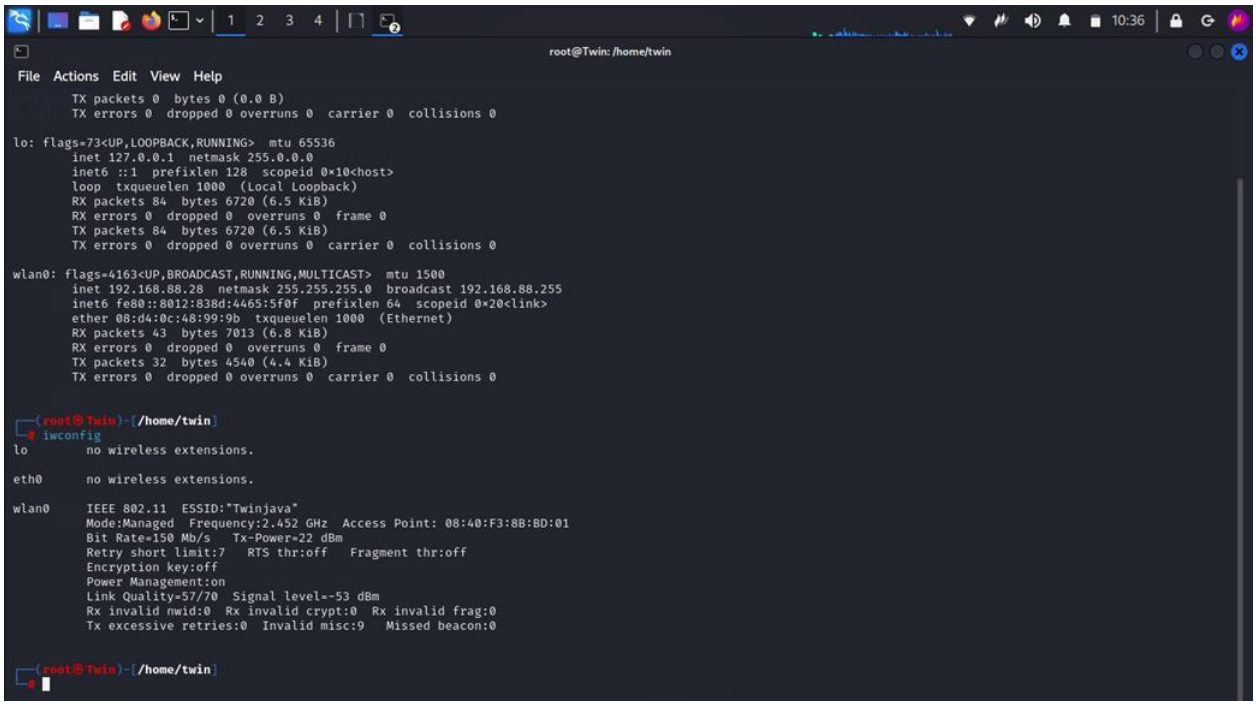
Based on the principle of "security through obscurity", many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization's SSID does not, in fact, add any level of security.

Aircack- ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

Here, we will use Air crack-ng to reveal a hidden SSID.

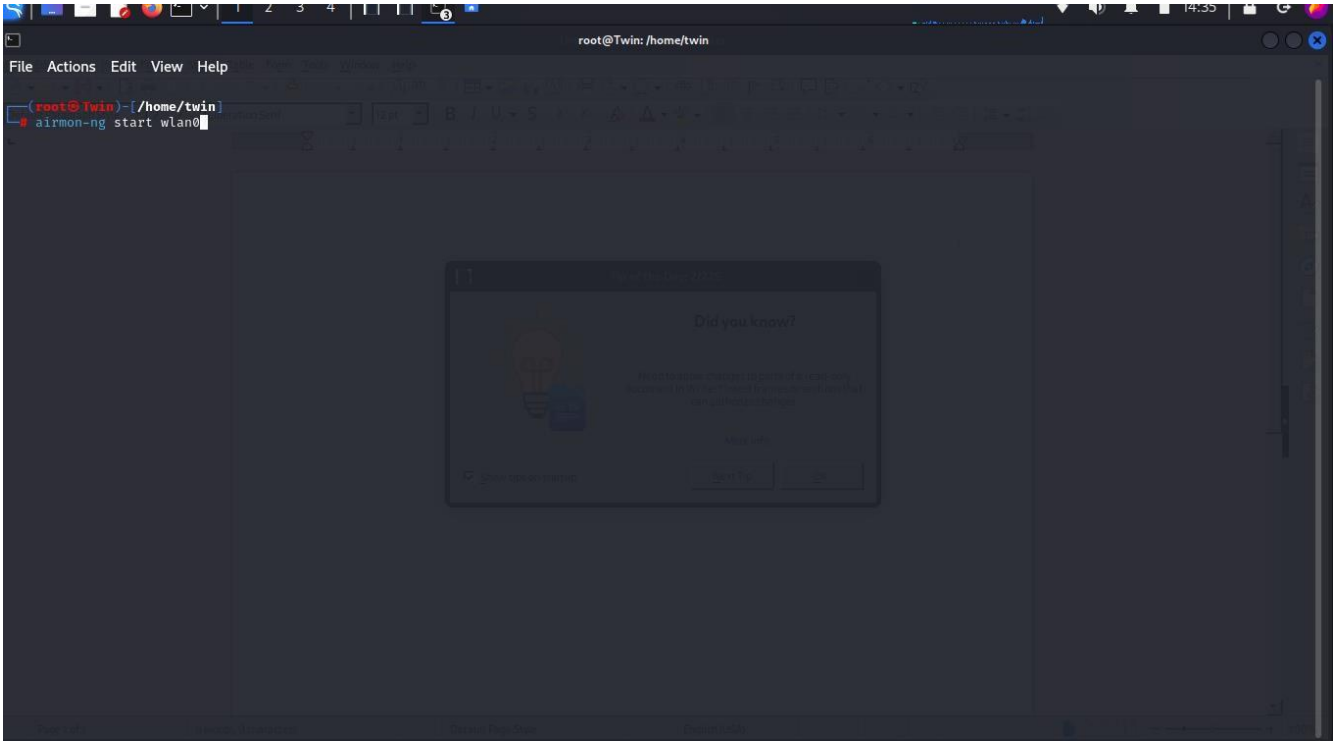
1. In the linux Terminal Window, type ifconfig and press Enter. Observe that the wireless interface (in this case, wlan0) gets connected to the machine, as shown in the screenshot.



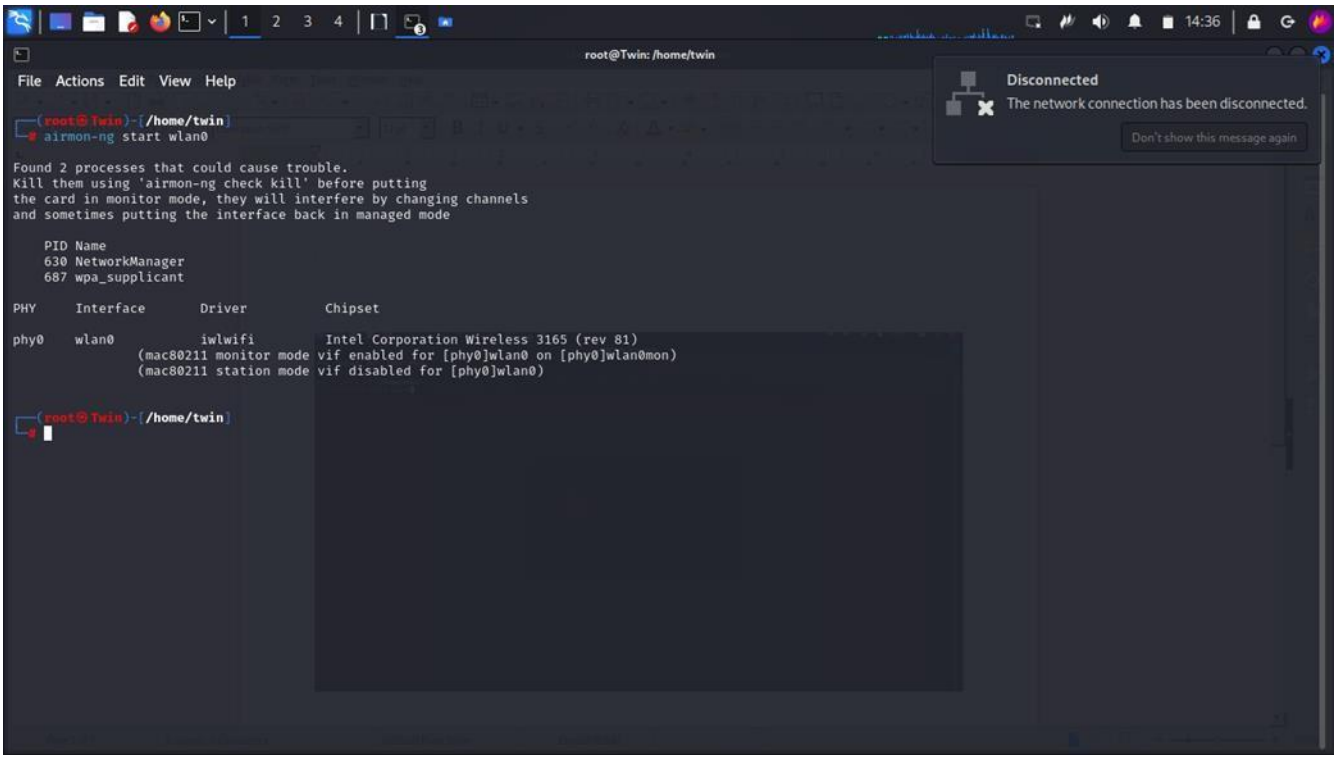


Note: The name of wireless interface might vary in your lab environment.

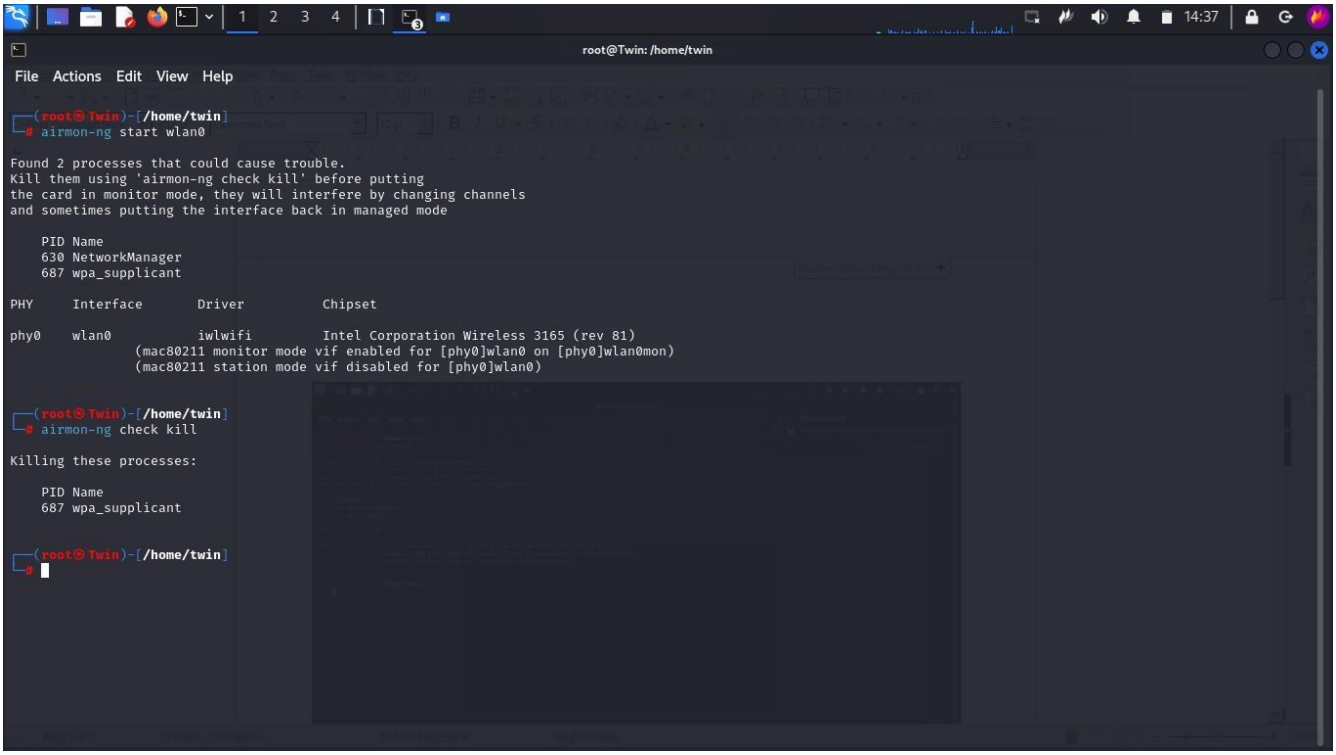
2. In the terminal Window, type airmon- ng start wlan0 and press Enter. This command puts the wireless interface (in this case, wlan0) into monitor mode.

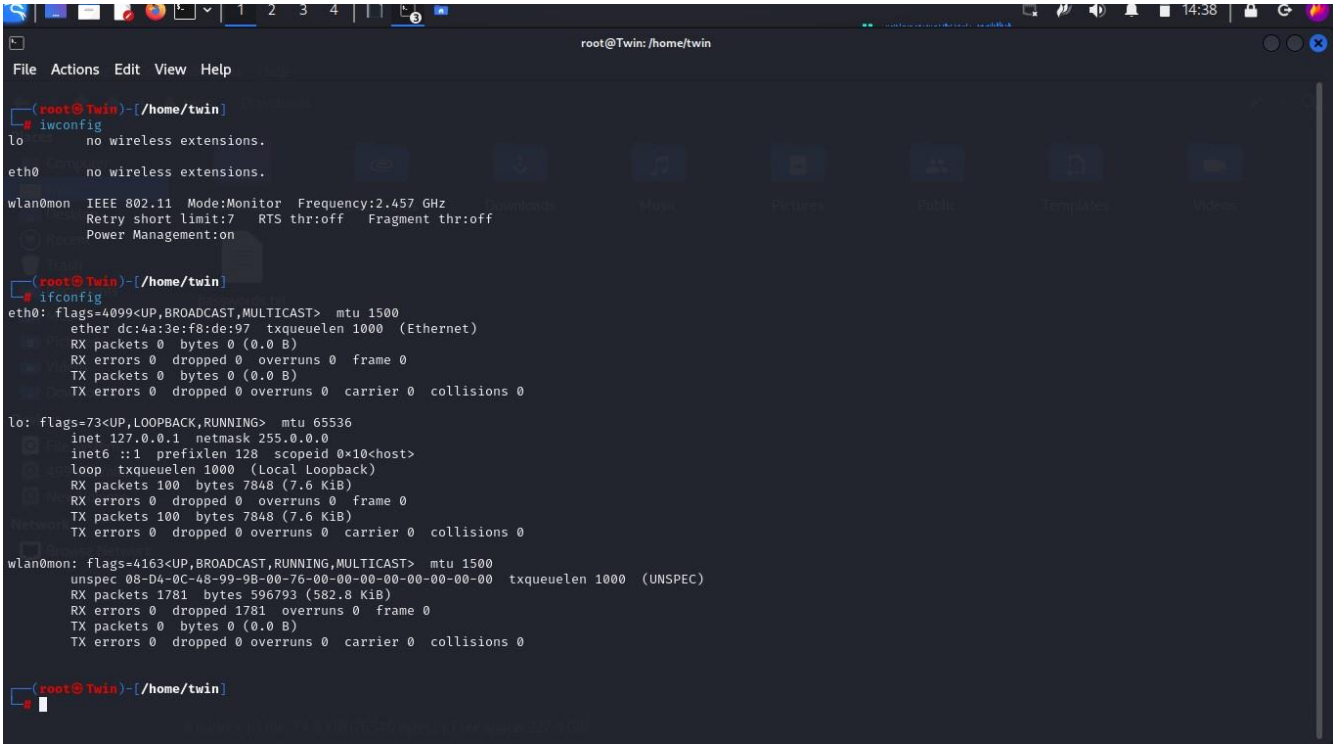


3. The result appears, displaying the error: “Found 2 processes that could cause trouble.” To put the interface in monitor mode, these processes must be killed. here, the name of wireless interface (wlan0) would automatically be renamed to wlan0mon.

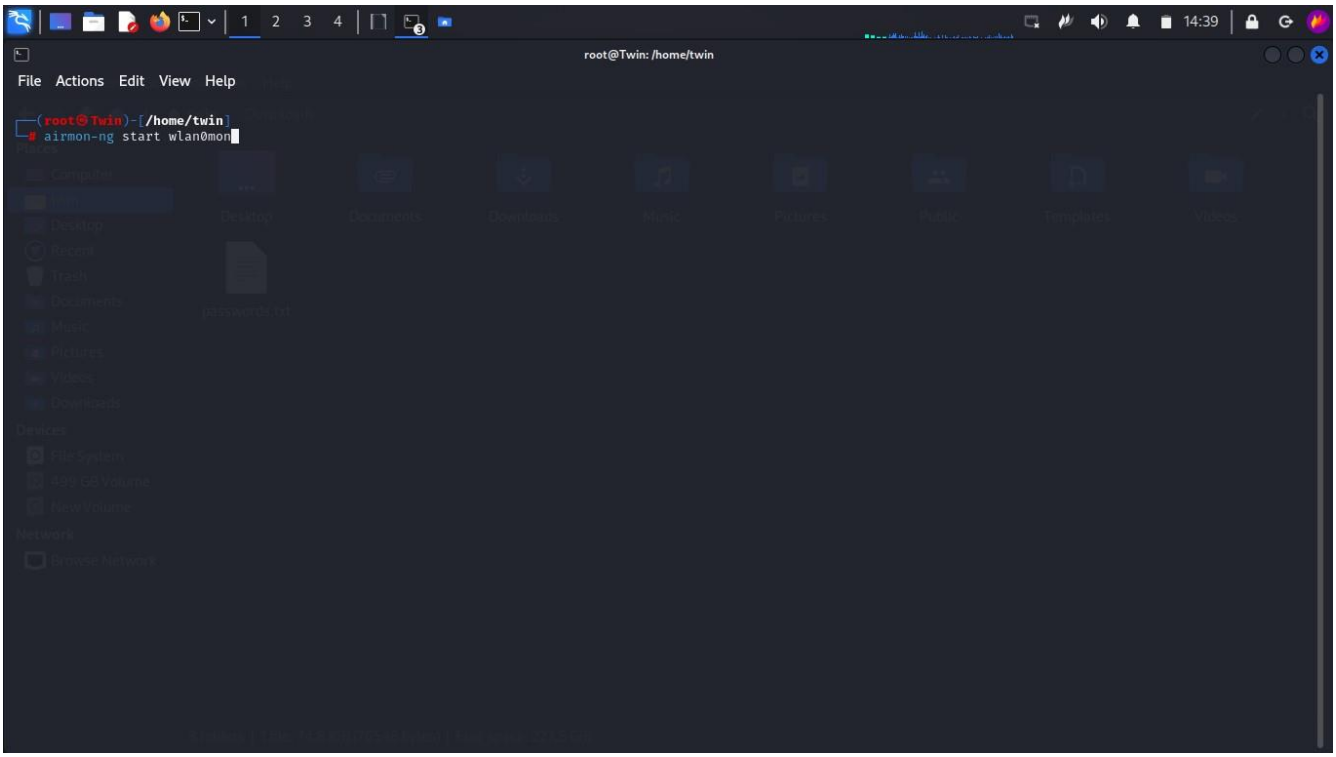


4. Type airmon- ng check kill and press Enter to stop the network managers and kill the interfering processes.



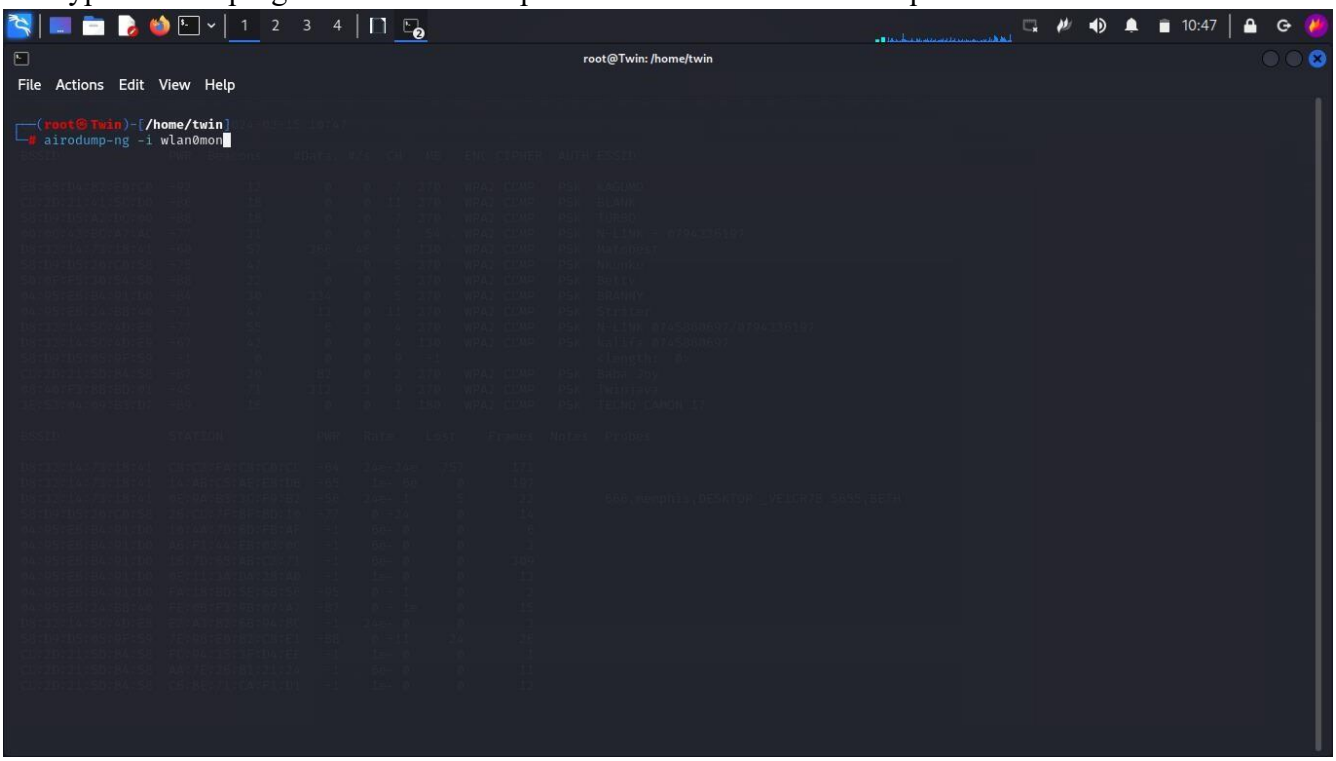


5. Now, run the command airmon-ng start wlan0mon again to put the wireless interface in



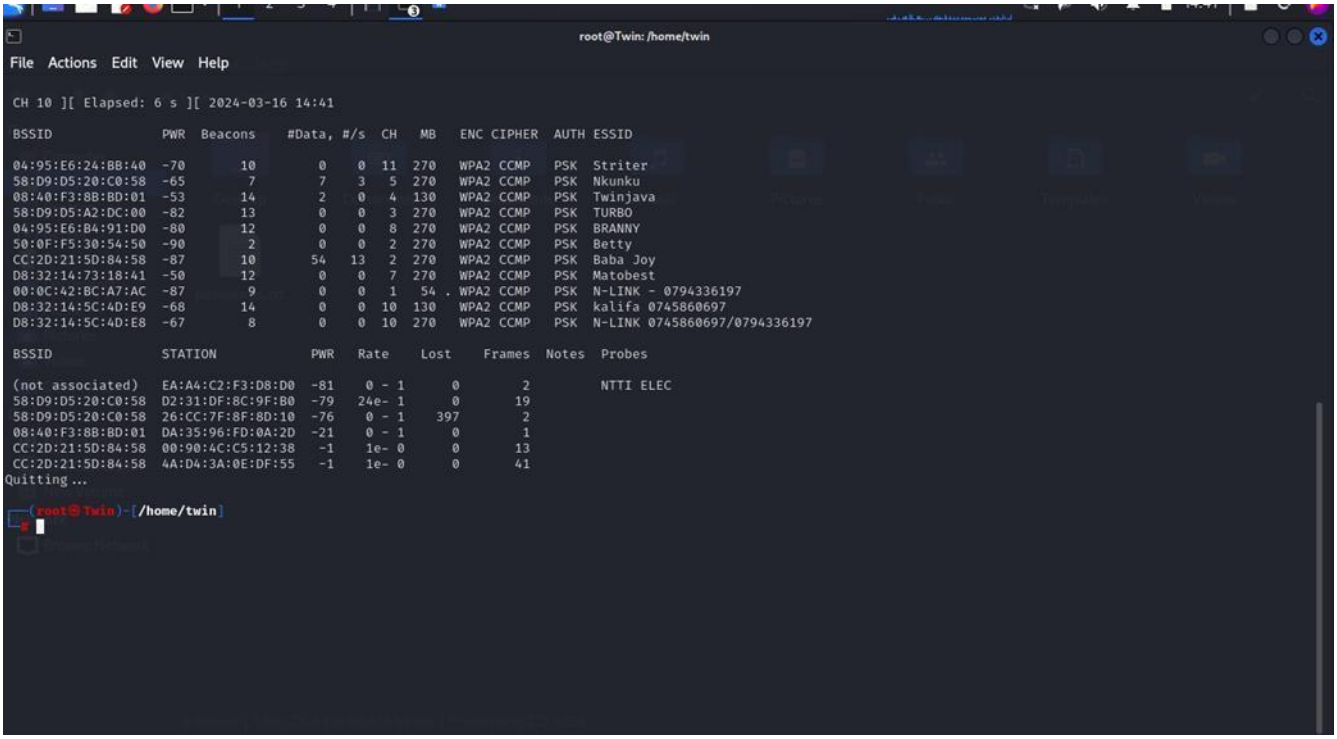
monitor mode.

6. Type airodump-ng -i wlan0mon and press Enter. This command requests a list of detected



access points, and connected clients(“stations”).

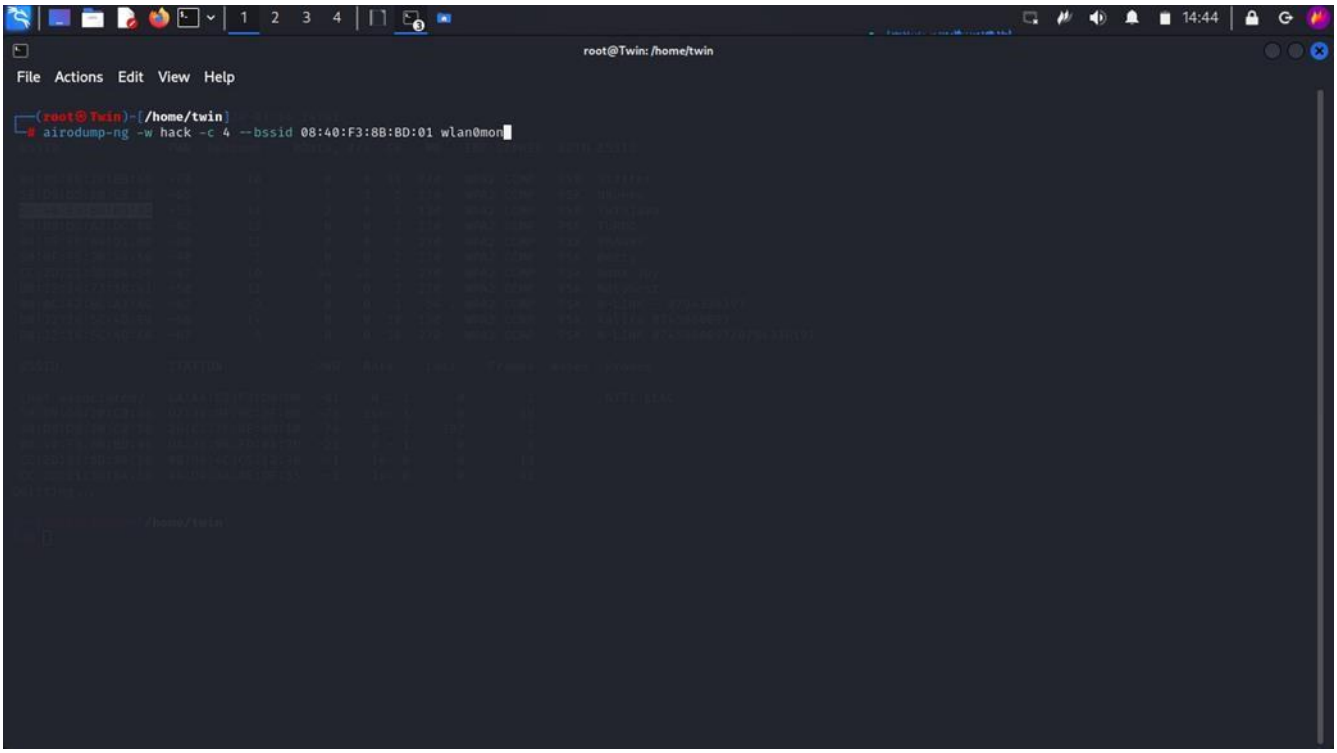
7. The result appears, displaying the available access points. Note the hidden ESSID associated with BSSID (MAC address).



NOTE: The BSSID associated with the hidden ESSID will differ in your lab environment.

NOTE: airodump-ng hops from channel to channel and shows all access points from which it can receive beacons.

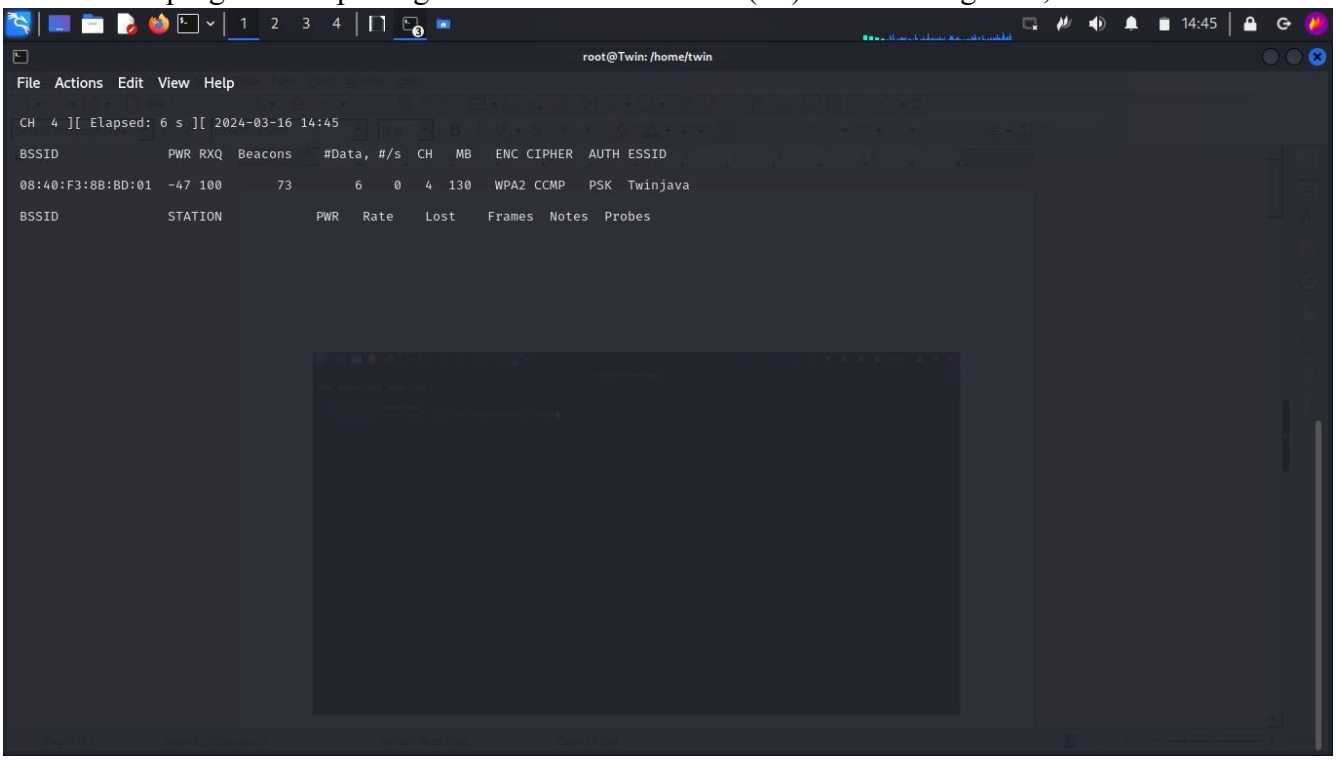
8. In the terminal window type airodump-ng-bssid (your Target MAC address) wlan0mon and press Enter.



NOTE: In this command,

- --bssid: MAC address of the target access point (in this example,08:40:F38B:01 wlan0mon): Wireless interface
- Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.

9. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in



the screenshot.

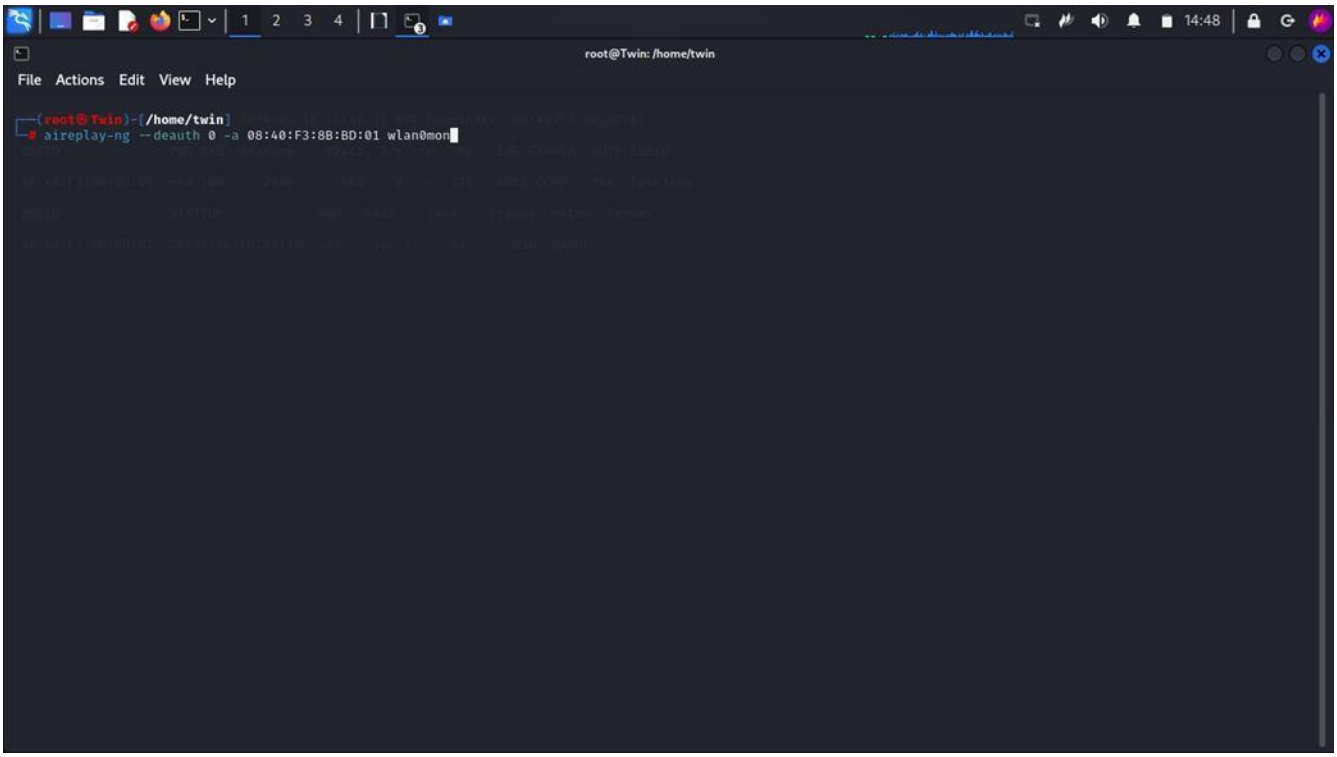
NOTE: The client station BSSID will differ in your lab environment.

10. Open another terminal by clicking new Terminal icon from the top at the desktop.
11. A Terminal window appears. In the terminal window, type sudo su and press enter to run the programs as a root user.
12. In the [sudo] password for attacker field, type your password and press enter.

NOTE: The password that you type will not be visible.

Now, type cd and press Enter to jump to the roof directory.

13. In this new terminal, type **aireplay – ng -deauth 0 (activates deauthentication mode) -a mac address interfac**e and press enter.

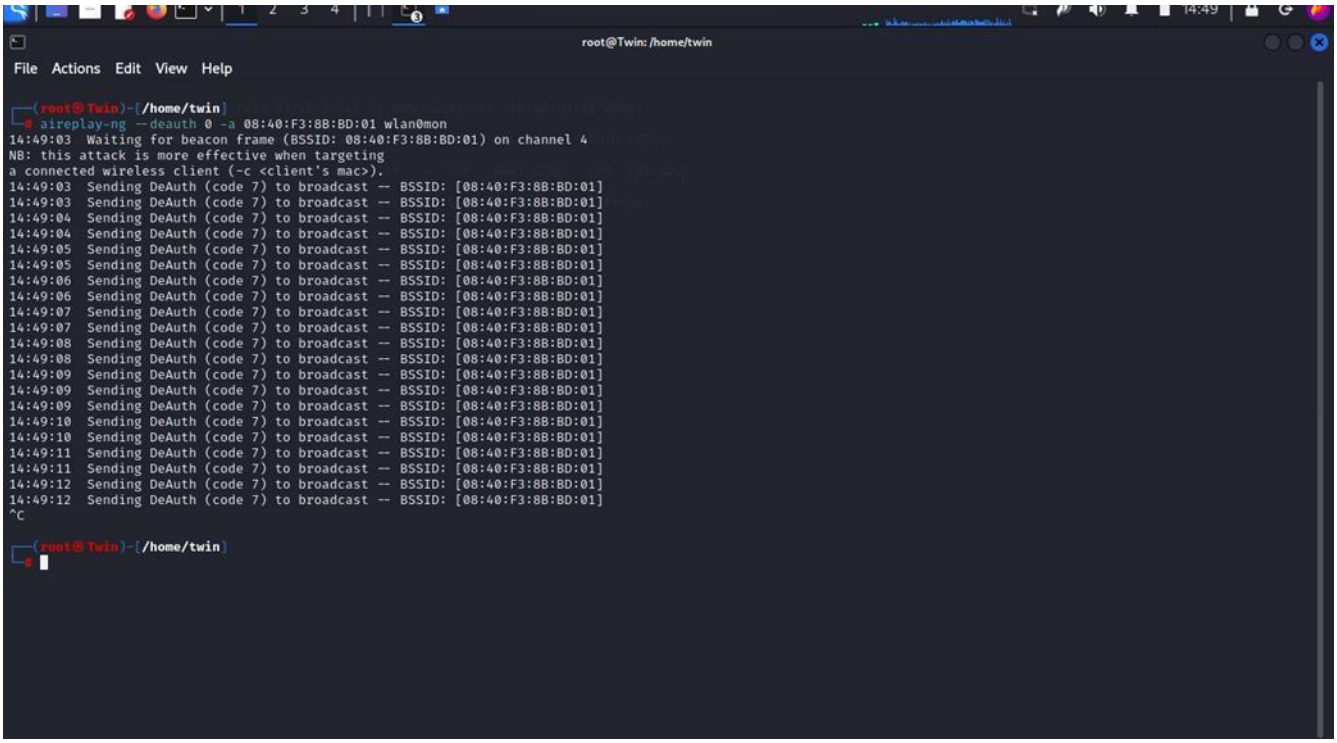


NOTE: In this command,

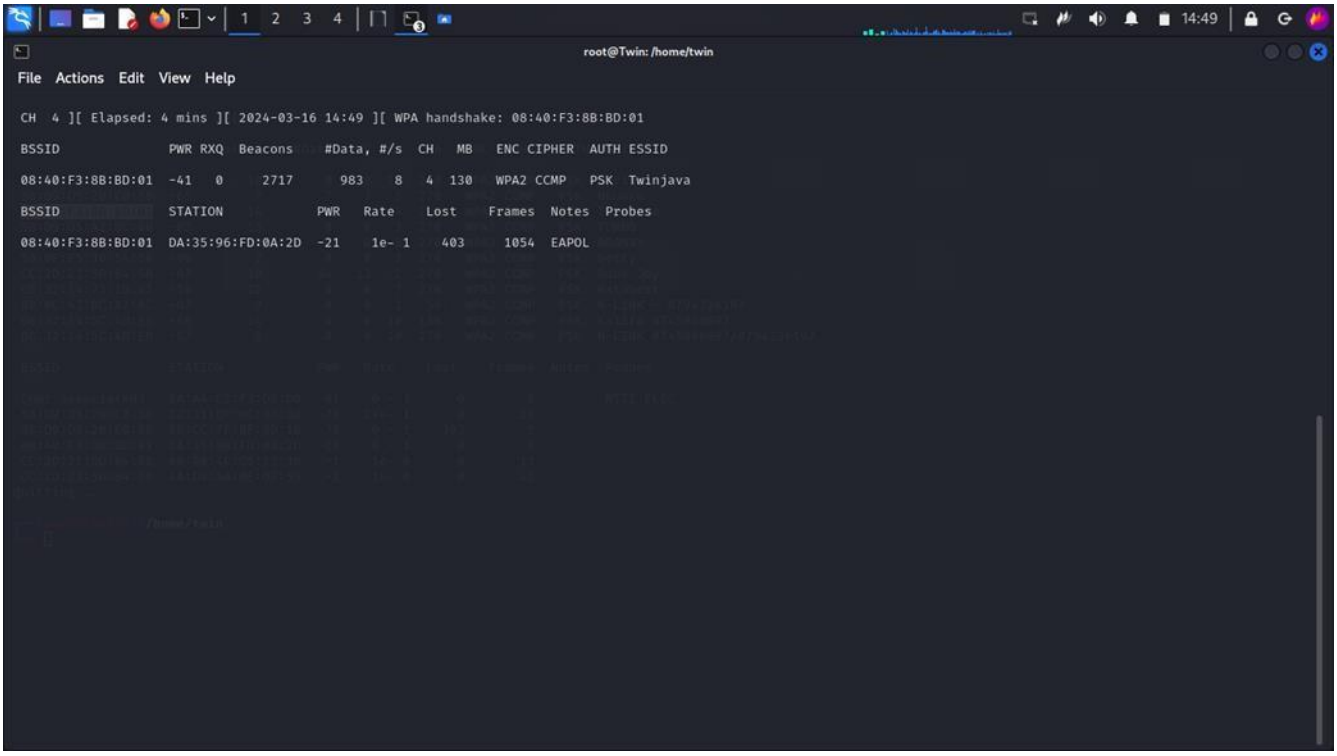
- Deuth 0: Activates deauthentication mode
- -a: sets the access point MAC address
- Wlan0mon: wireless interface

NOTE: if you get any errors while running the command, reissue the command multiple times until it executes successfully.

14. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connections with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.

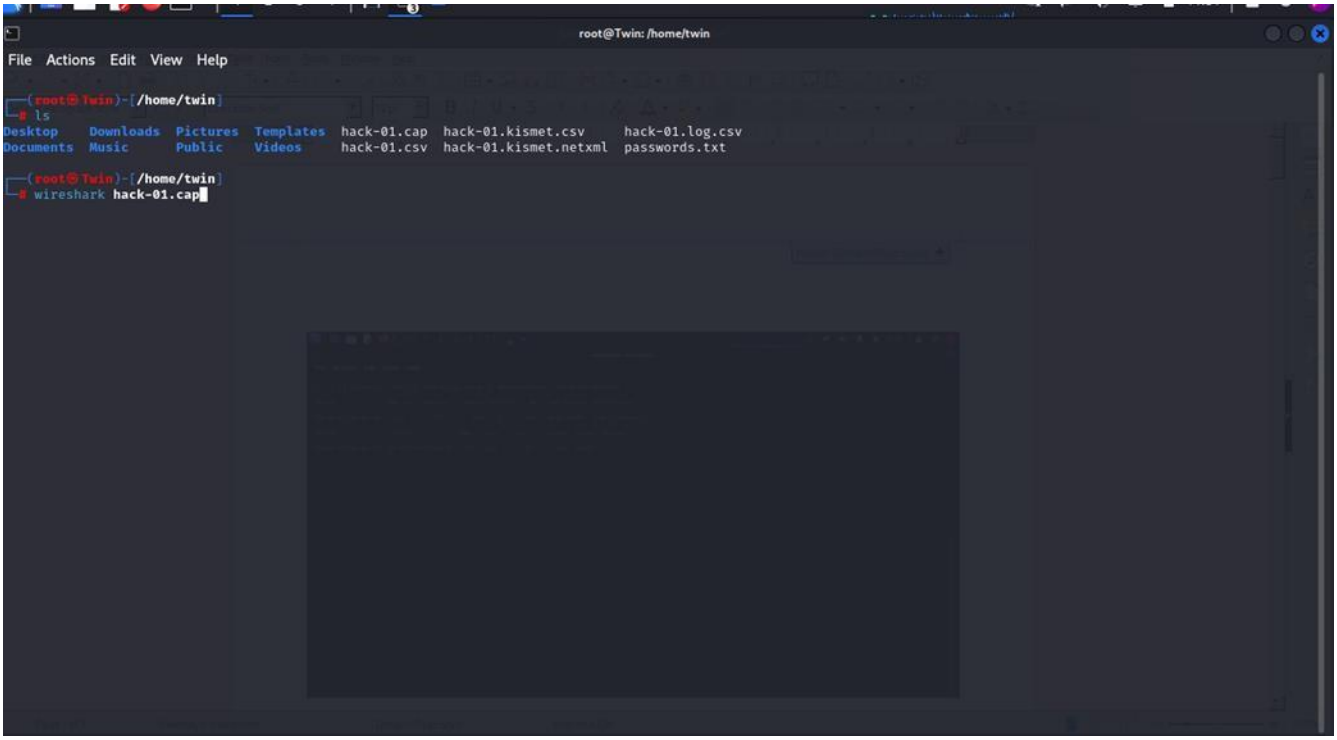


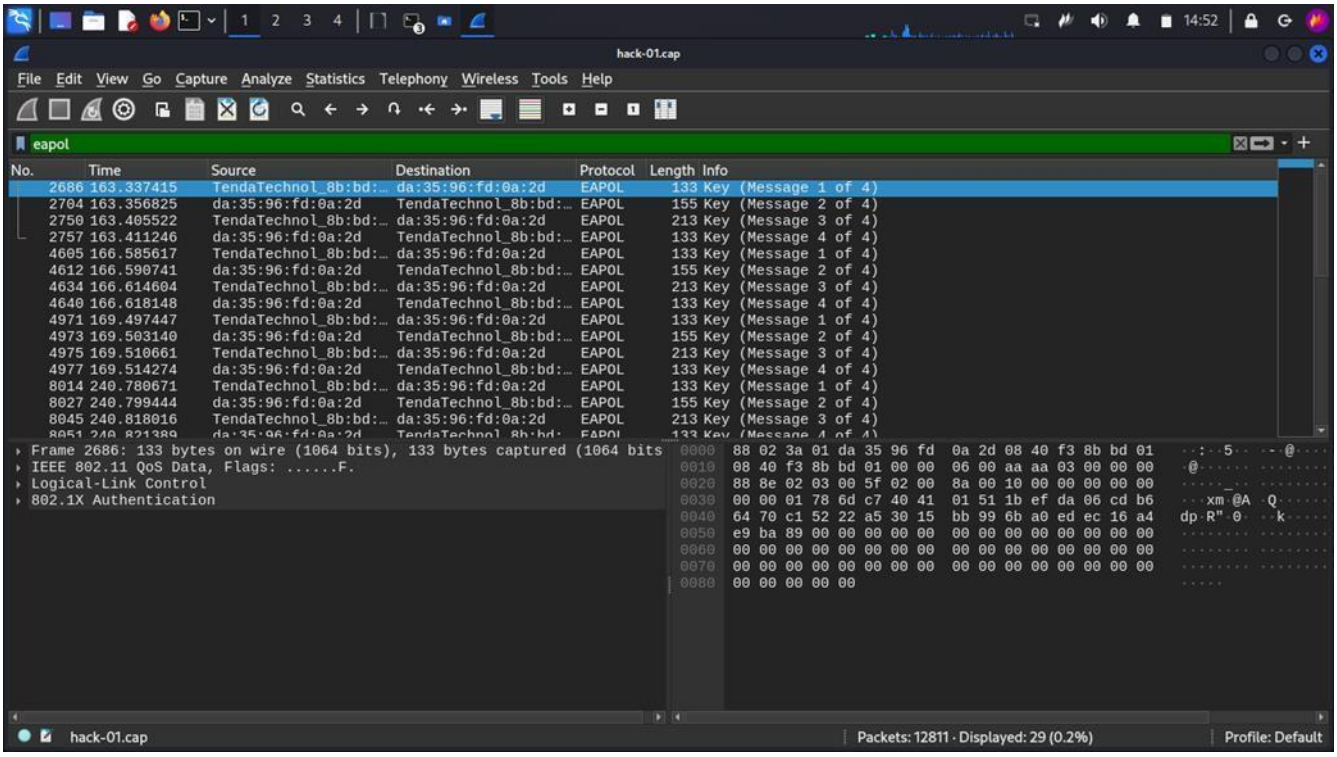
15. Which back to the terminal where airdrop is running and keep capturing packet until you receive **WPA handshake: mac address** packet, which indicates that the WPA/WPA2 handshake was successfully captured for the target BSSID.



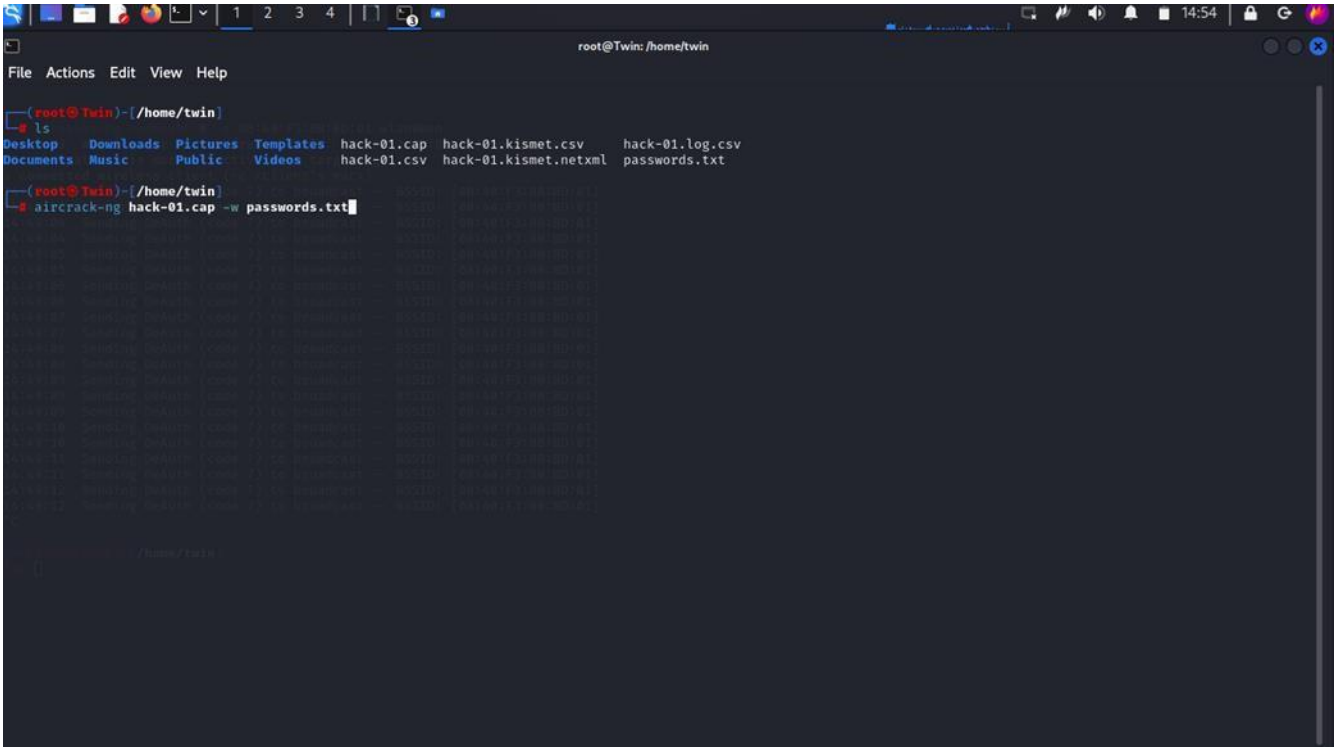
16. Rerun the above command several times to send a large number of de-authentication packets. press ctrl +c to stop the capture.
17. Open a new terminal window, type **sudo su** and press enter to run the program as a root user.
18. In the **sudo** field type password and press enter.

19. You can check the if the communication succeeded in Wireshark.

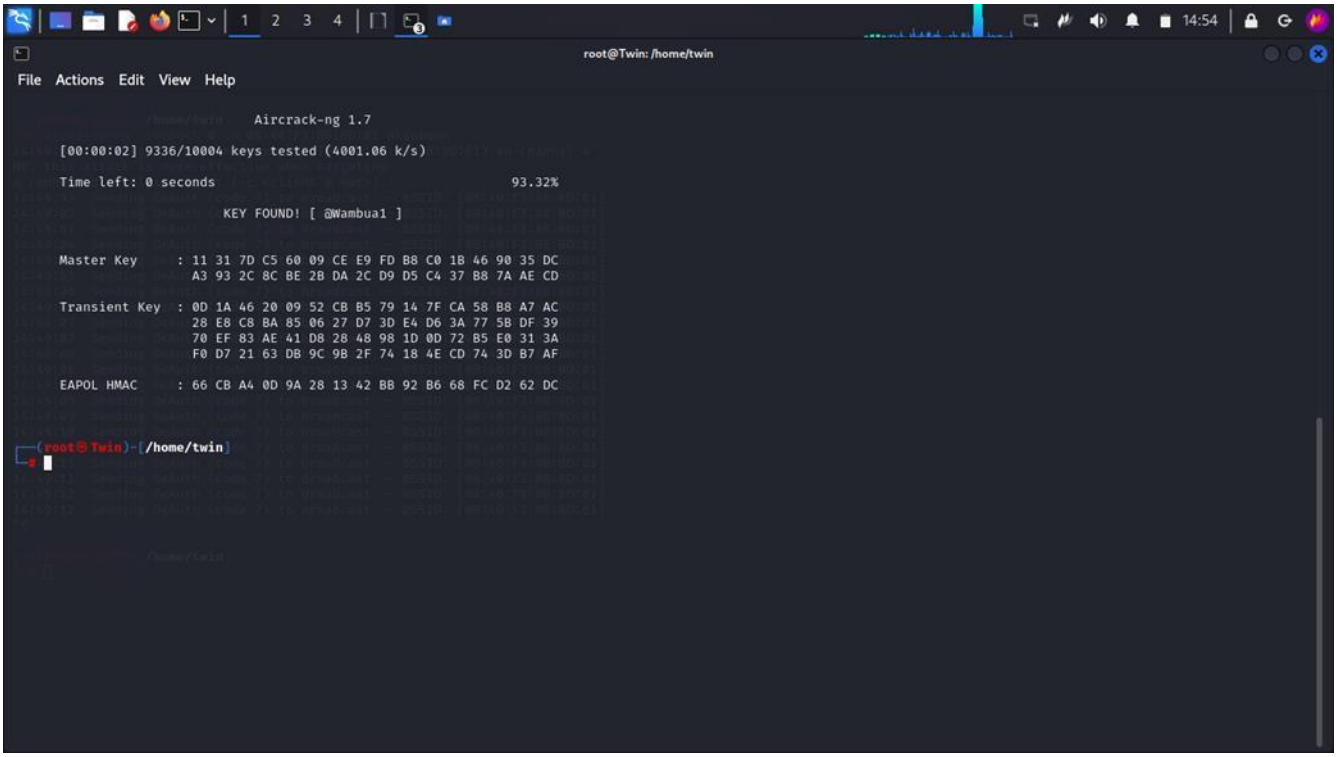




20. In the terminal window **type aircrack -ng - a (identifies attack mode) mac address -w (specifies the path to a word list)** and press enter.



34.The results appears showing a WPA handshake packet captured with the airdrop -ng. The target access point's password is cracked and displayed in the plain text next to the message **KEY FOUND!** as shown



Note: it takes long if the password to be cracked is complex