**Name – Devasy Patel**

**Roll Number – 20BCE057**

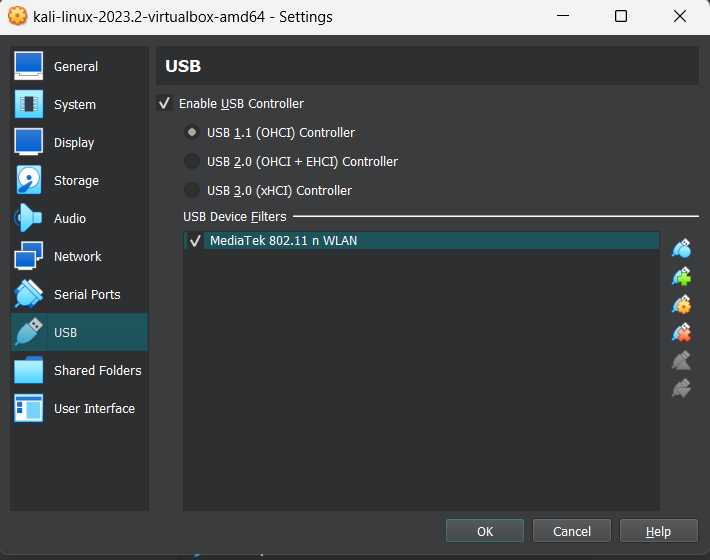
**Subject – Ethical Hacking and Vulnerability Assessment**

**Practical – 4**

**AIM:** To carry out Wi-Fi based Network Hacking related attacks.

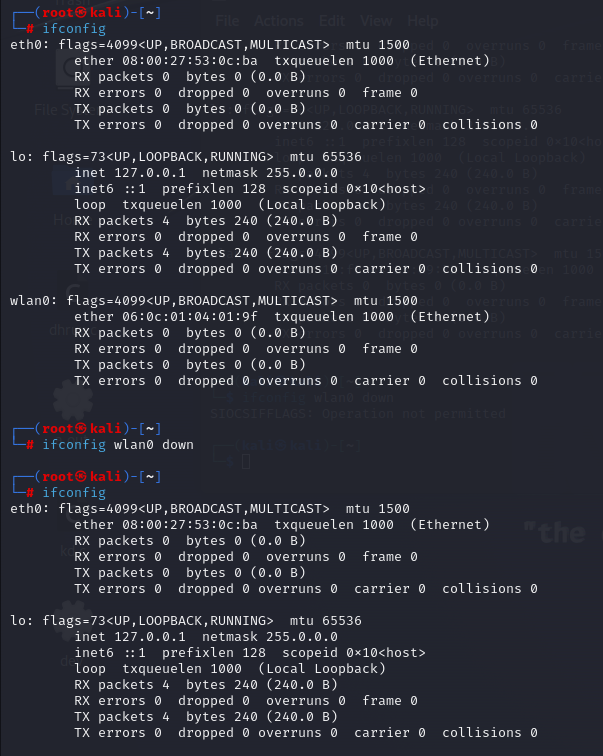
**Procedure:**

1. **Configuring the Dongle**

****

1. **Changing the MAC Address**

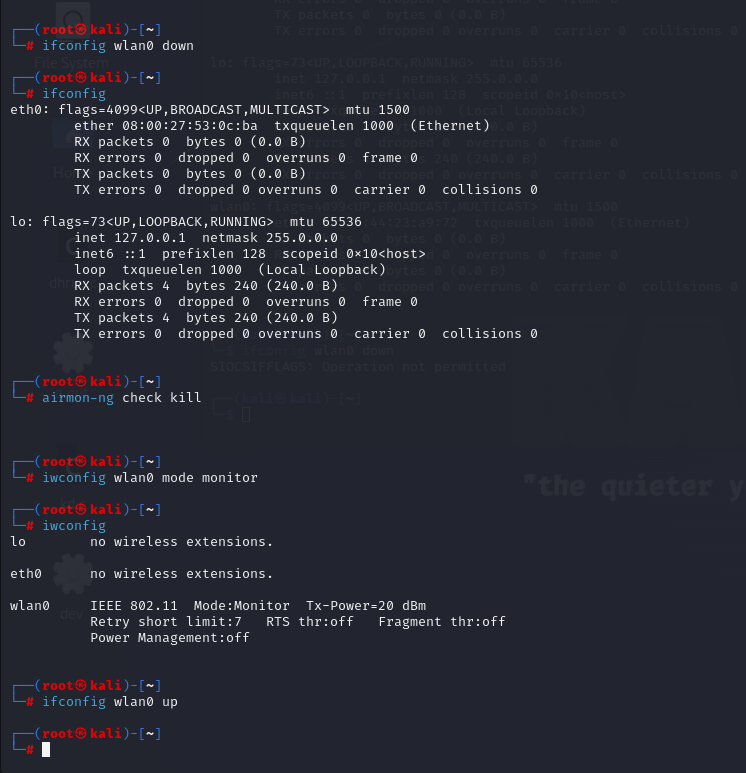
* Using ifconfig, we found details of network
* Changed the MAC Address





Successfully changed the MAC Address!

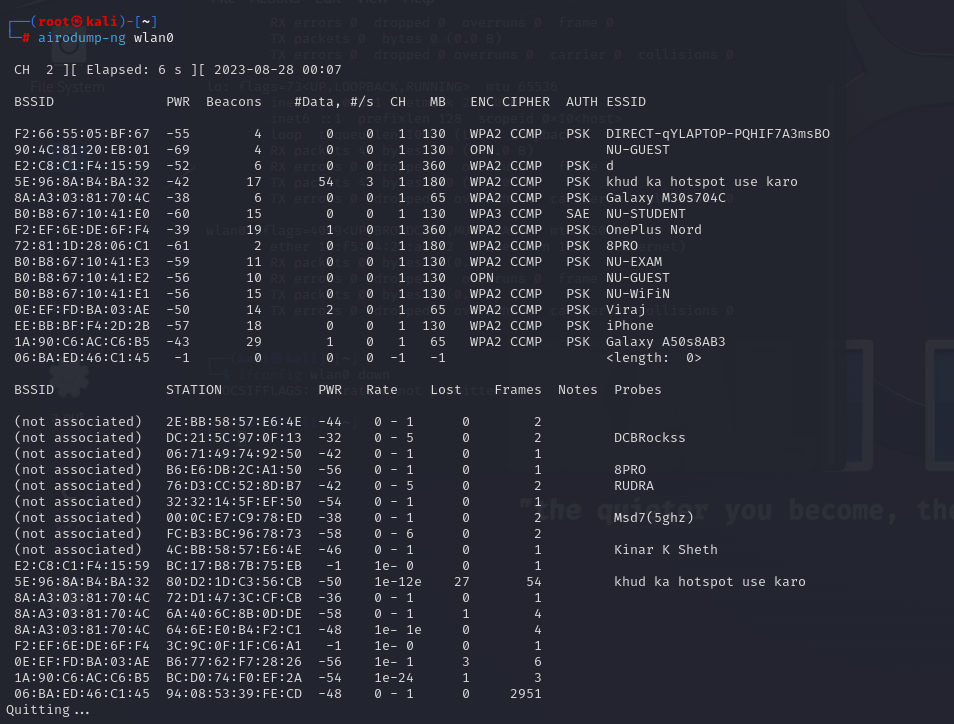
1. **Changing mode from managed to monitored**
   * Using iwconfig command to analyze the network and change mode from managed to monitored



As we see in above image, the Mode of wlan0 has successfully been changed from Managed to Monitored.

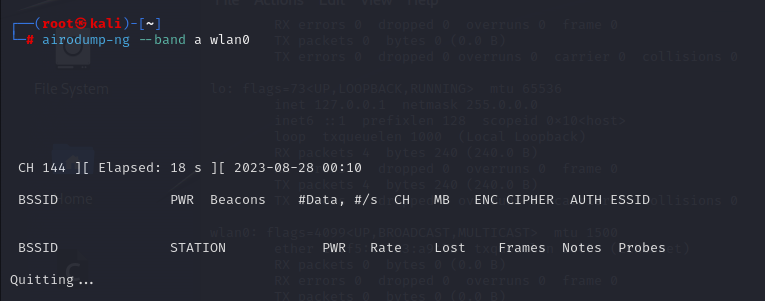
1. **Packet Sniffing using airodump-ng**

It gets the information of all the packets of the environment – in the below image, we can see the different WiFi Networks available under the ESSID column and the corresponding MAC Addressed of source.



1. **Forcing the airodump-ng to listen to other frequencies**

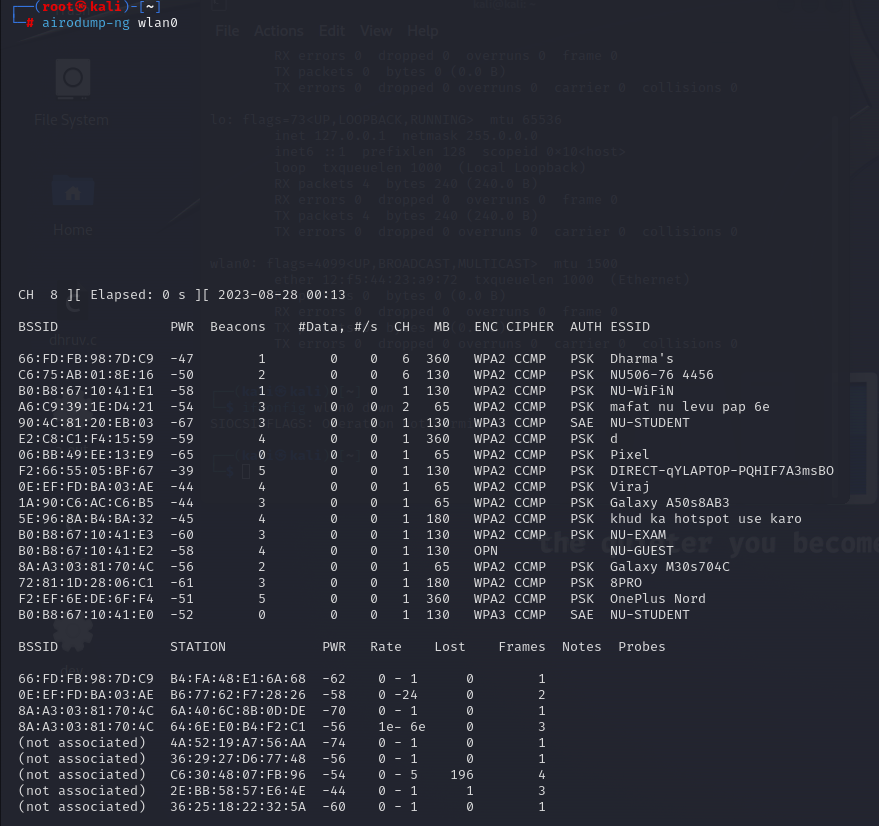
Here, as our laptop doesn’t support 5G Frequency band, none of the networks are visible.



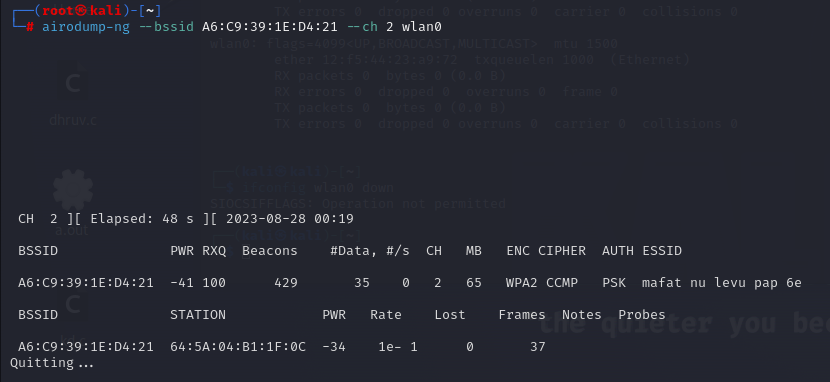
We tried sniffing 2.4 GHz bandwidth – here, we can see available frequencies!

1. **Targetted Packet Sniffing**

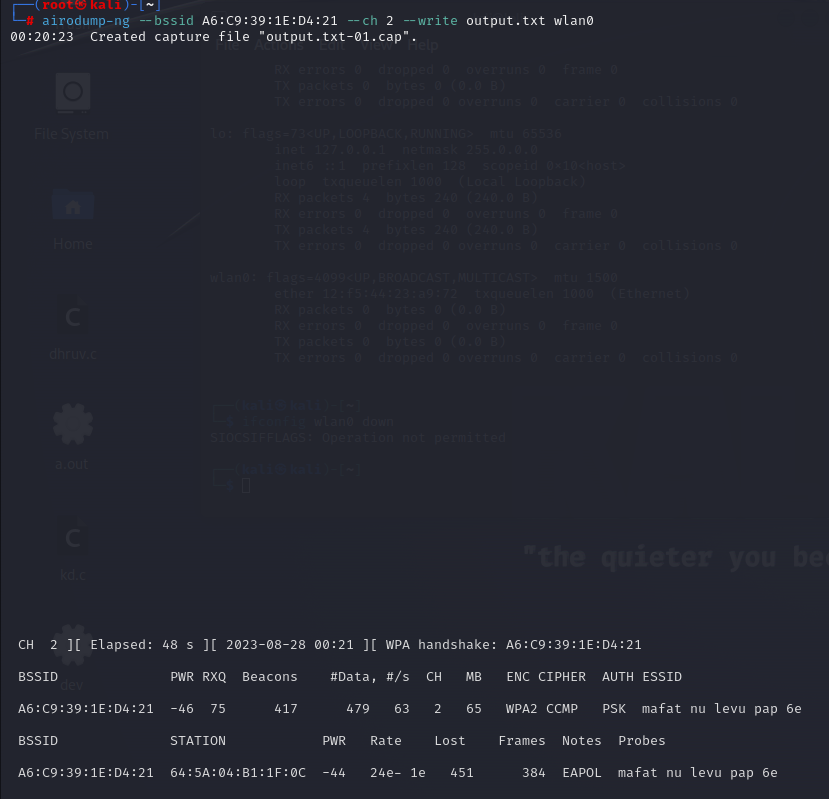
Here, we explicitly sniff the packets of those network that we want to attack



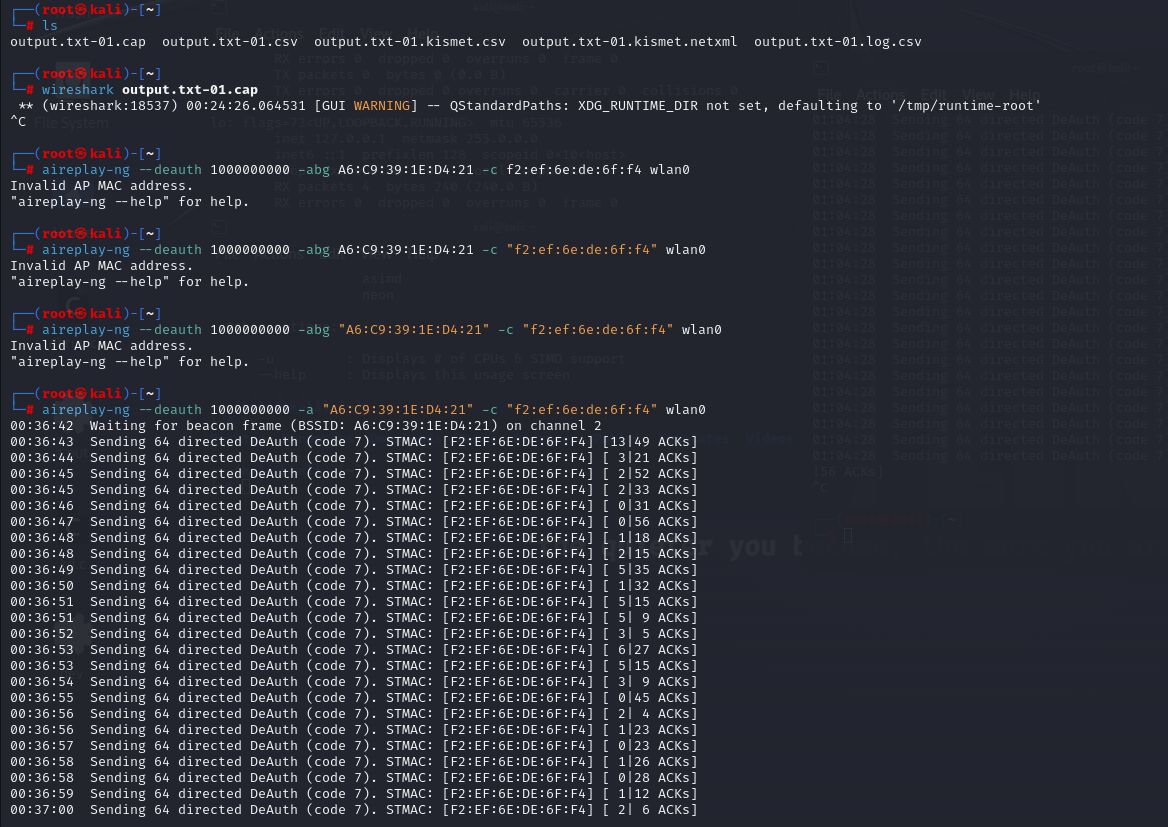
Specifying the 4th WiFi (ESSID), we give its BSSID and Channel as arguments and get the following result:



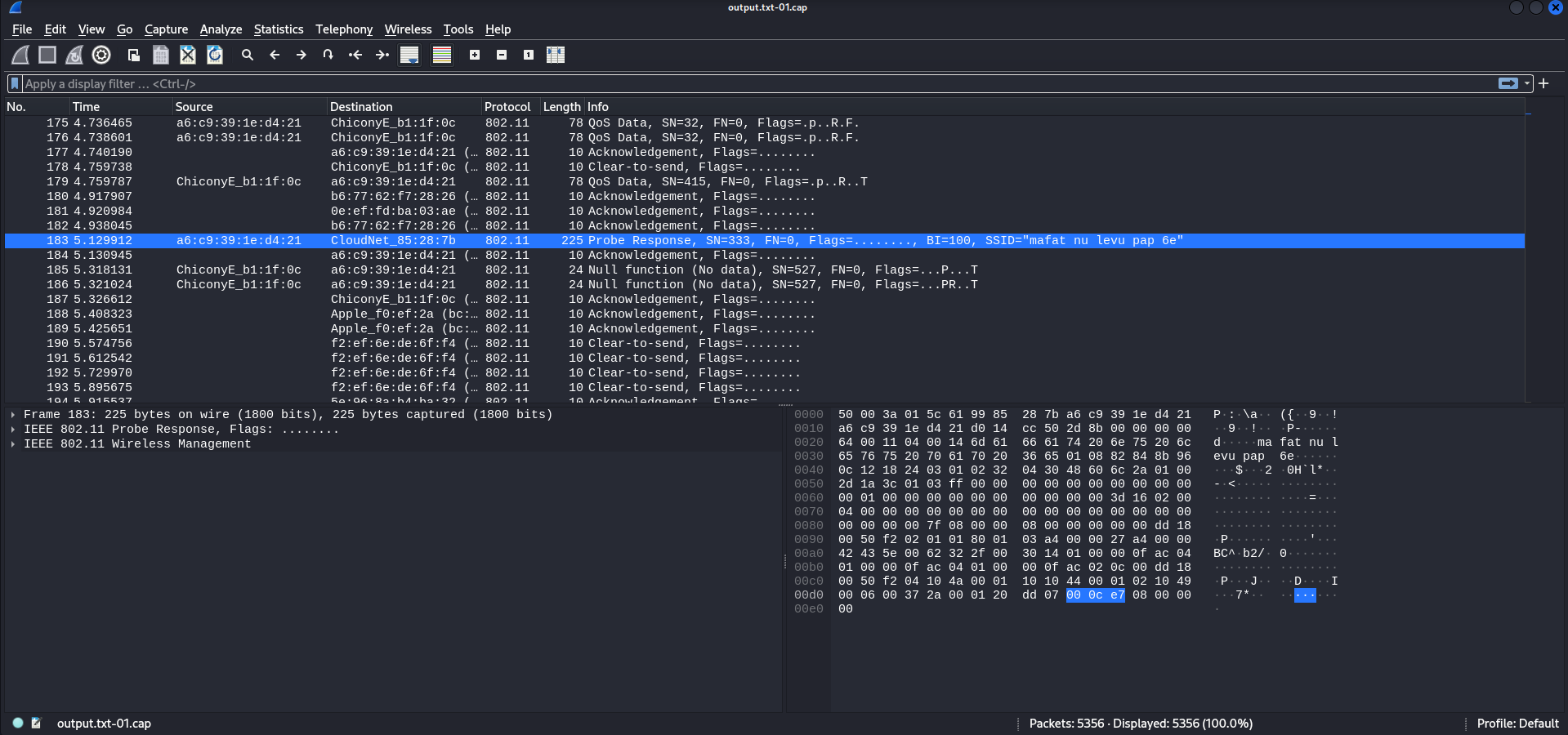
Here, we ask airodump-ng to sniff the particular bbsid and channel and write the results to output.txt file!



On checking, 4 files have been created where the entire logs have been saved. Now, giving the .cap file as argument to wireshark and opening:



This is the wireshark window that opened! We can clearly see all packets being sniffed. If the network was open, here only, we would have found messages in normal text!



1. **Now, performing De-authentication attack**

