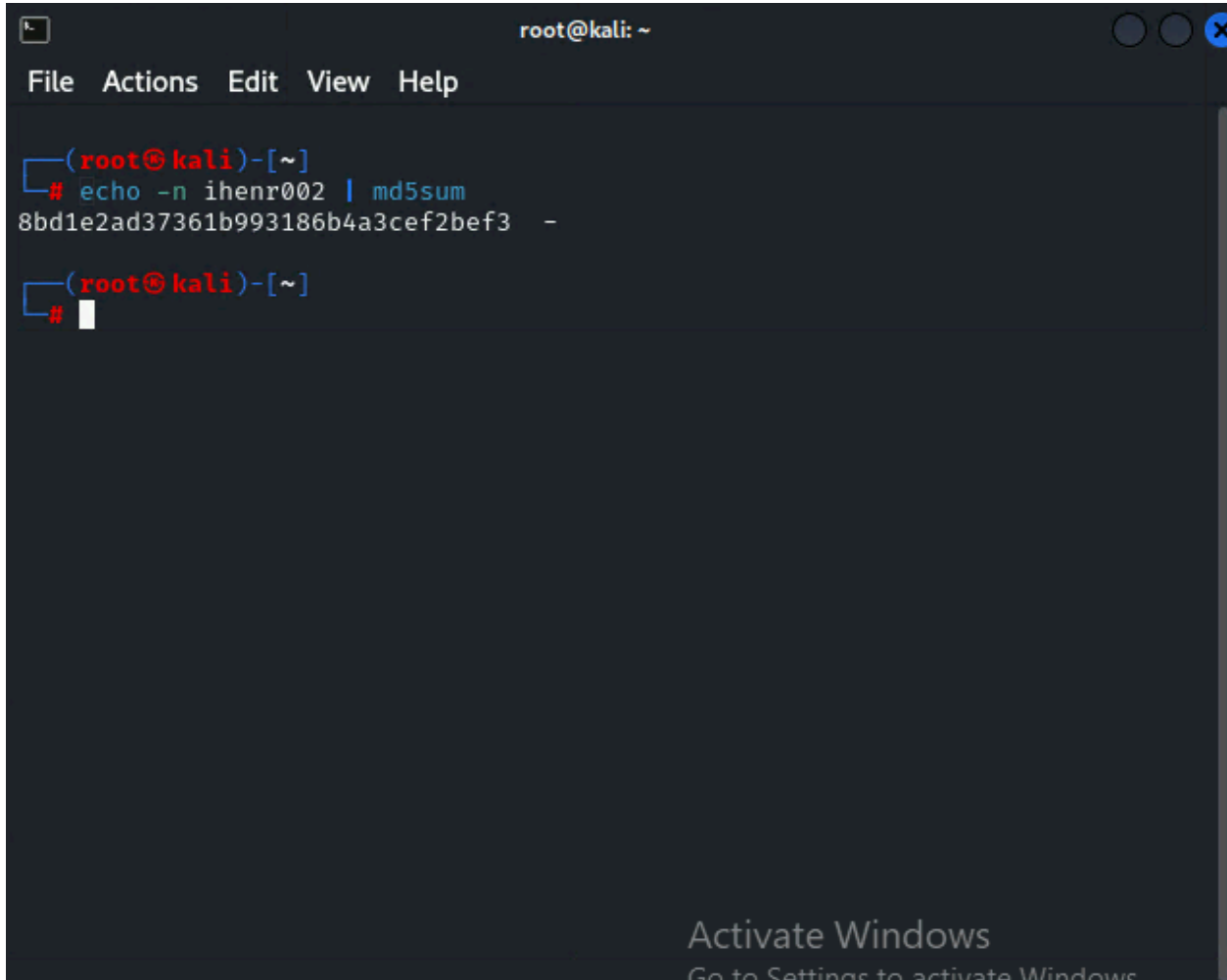


## Task D

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID.

A terminal window titled 'root@kali: ~' with a menu bar containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a command prompt '(root@kali)-[~]' followed by the command '# echo -n ihenr002 | md5sum'. The output is '8bd1e2ad37361b993186b4a3cef2bef3 -'. A second prompt '(root@kali)-[~]' is shown with a cursor on the '#' character. At the bottom right, there is a watermark that says 'Activate Windows Go to Settings to activate Windows'.

Used md5sum hash on my midas ID; the last digit was 3: WPA2-P1-01.cap

1. Implement a dictionary attack and decrypt the traffic

```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap      lab5wpa2-demo-dec.cap  WPA2-P2-01.cap  WPA2-P5-01.cap
lab5wep-demo-dec.cap  rockyou.txt            WPA2-P3-01.cap
lab5wpa2-demo.cap     WPA2-P1-01.cap        WPA2-P4-01.cap

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng wpa2-p1-01.cap -w rockyou.txt
Reading packets, please wait ...
Opening wpa2-p1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

# BSSID          ESSID          Encryption
1 00:16:B6:DA:CF:2F CyberPHY        WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening wpa2-p1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.
```

Using ls to see if rockyou file is installed; using aircrack command with the rock you file to find the passcode - "PASSWORD"

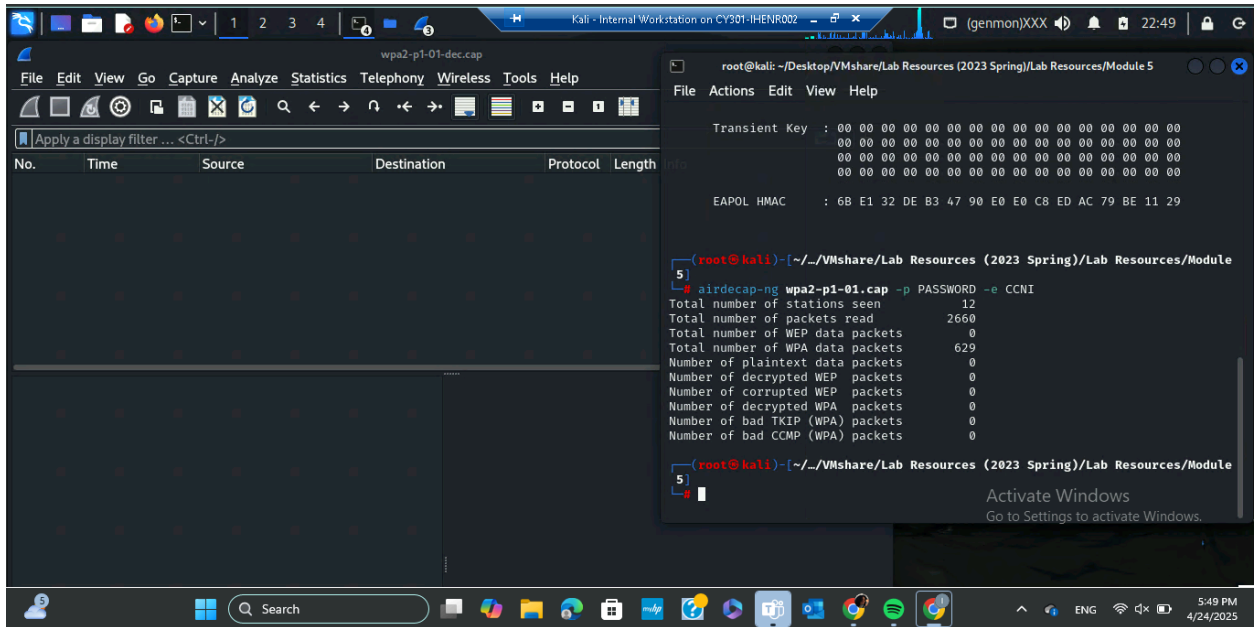
```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
info
Probe Response, SN=530
EAPOL HMAC : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29
Probe Response, SN=530
Probe Response, SN=530
Clear to send, Flags=

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# airdecap-ng wpa2-p1-01.cap -p PASSWORD -e CCNI
Total number of stations seen      12
Total number of packets read      2660
Total number of WEP data packets   0
Total number of WPA data packets   629
Number of plaintext data packets   0
Number of decrypted WEP packets    0
Number of corrupted WEP packets    0
Number of decrypted WPA packets    0
Number of bad TKIP (WPA) packets   0
Number of bad CCMP (WPA) packets   0
└─#
```

Using the decrypt command and the passcode to decrypt the wpa2-p1-01.cap traffic

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file



During the decryption process, none of the packets were decrypted, but if any packets were decrypted, I would go into Wireshark and look at the protocol hierarchy under statistics to see where most of the traffic is. Depending on what most of the traffic is, we would be able to see which patterns are being prioritized.