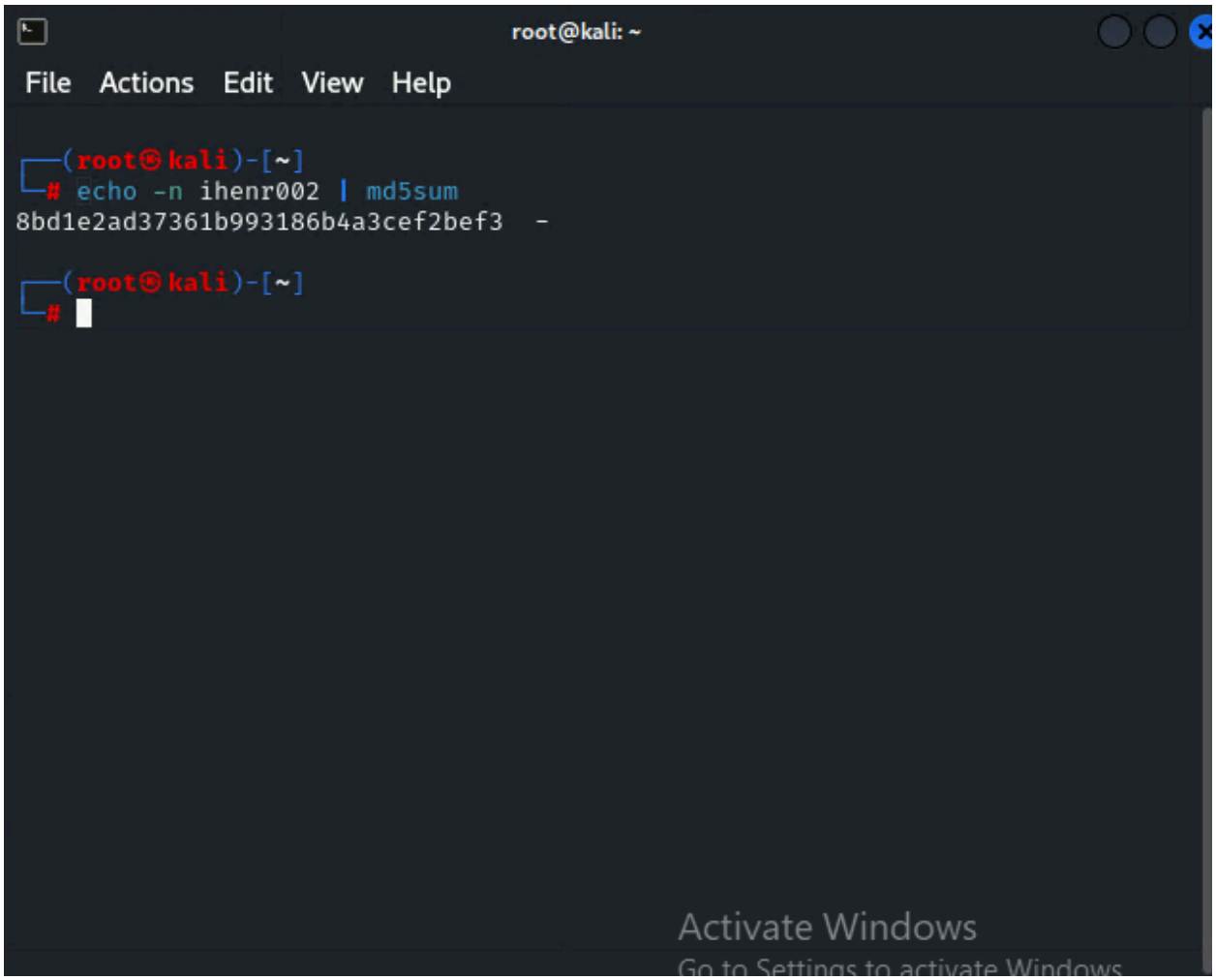
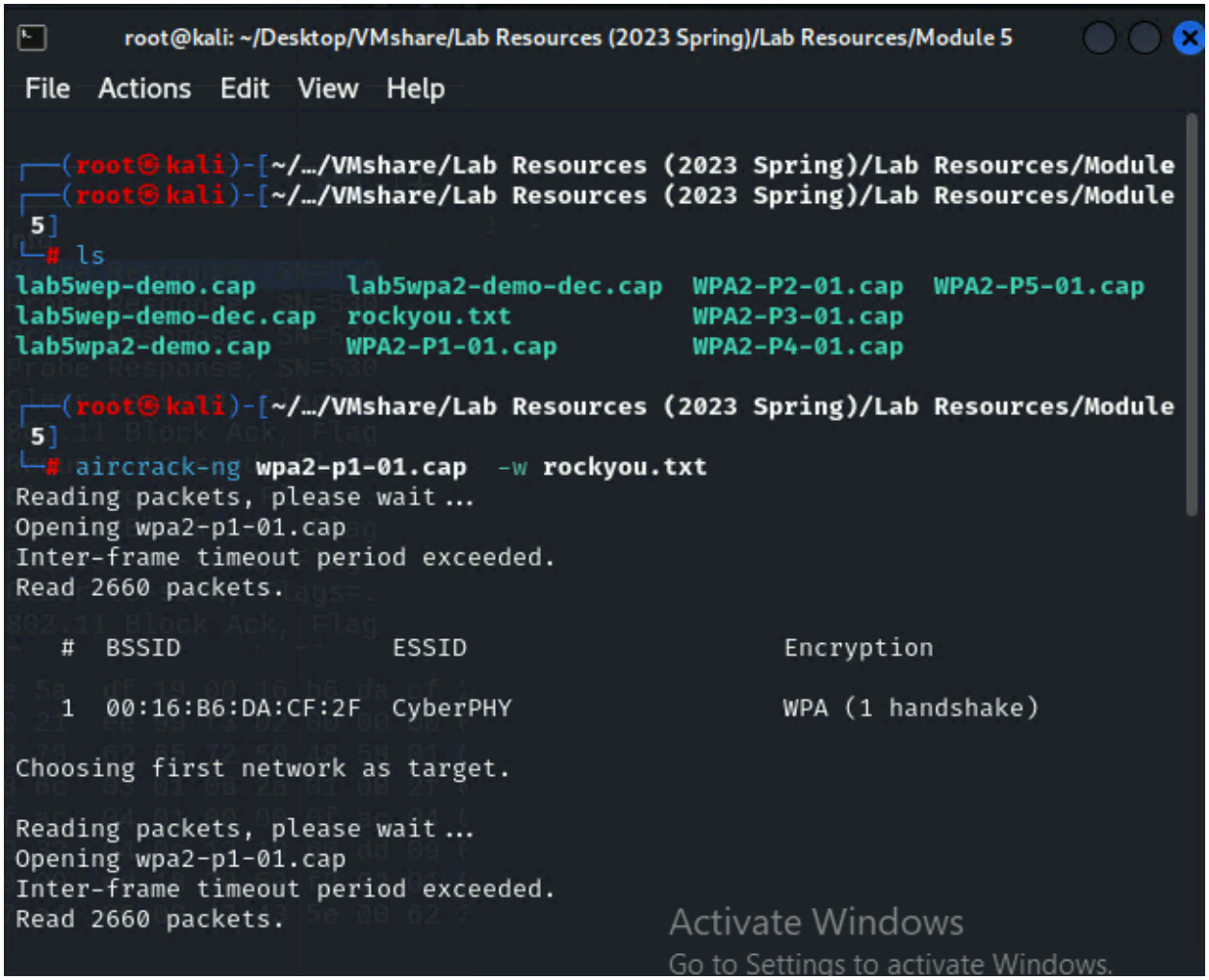
Task D

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.

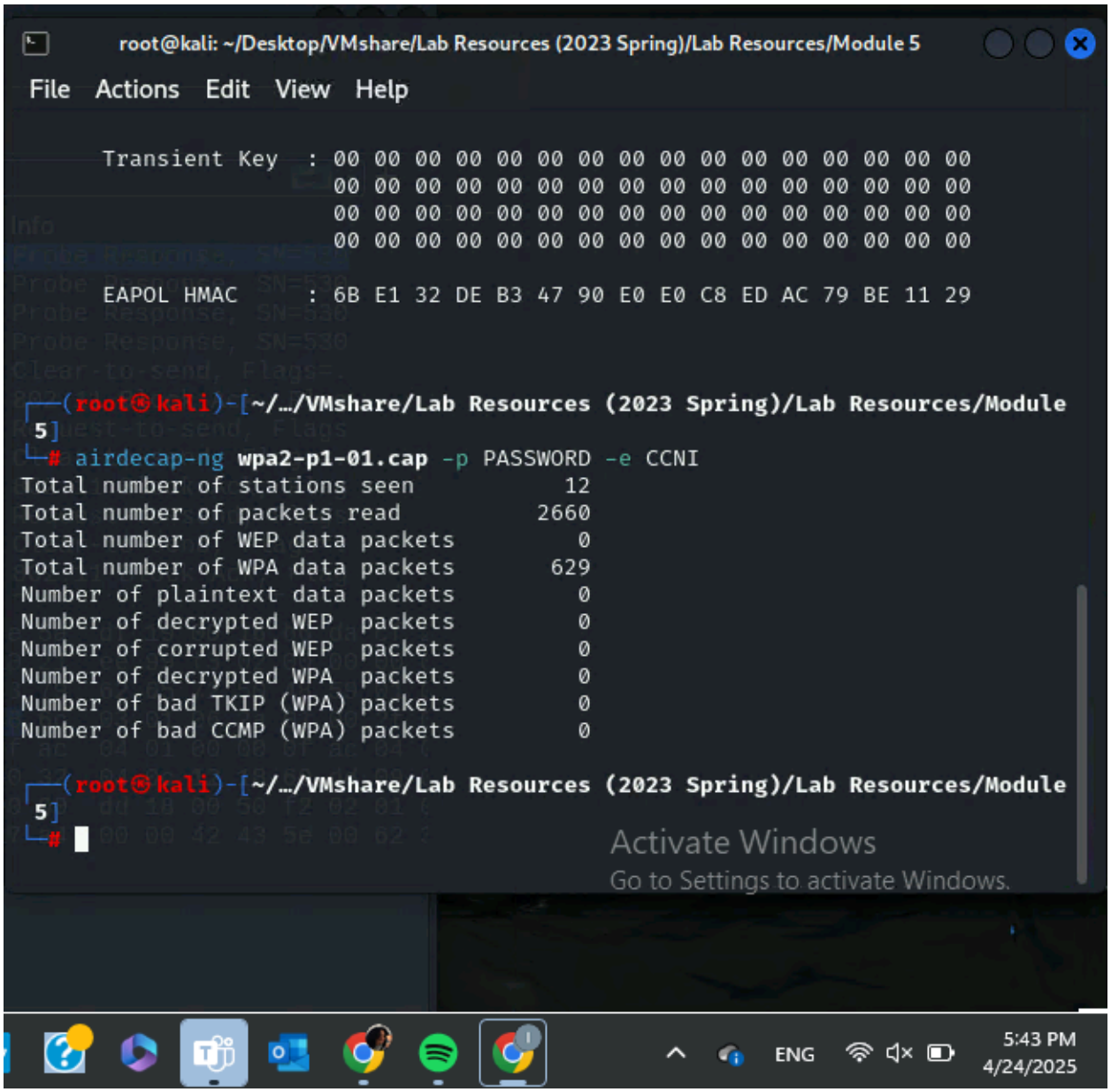


Used md5sum hash on my midas ID; the last digit was 3: WPA2-P1-01.cap

1. Implement a dictionary attack and decrypt the traffic

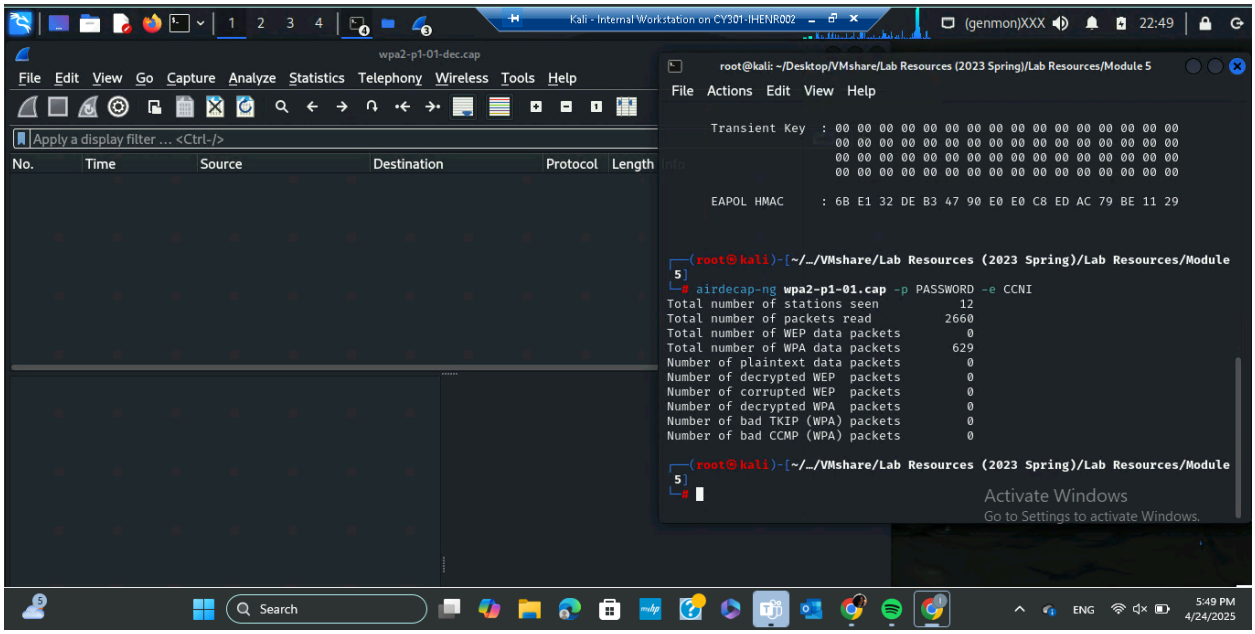


Using ls to see if rockyou file is installed; using aircrack command with the rock you file to find the passcode - “PASSWORD”



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.