# CYSE 301: Cybersecurity Technique and Operations

## Assignment M5: Wi-Fi Password Cracking

**Task A: 40 points**

Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

Requirements:

- Decrypt the lab4wep.cap file (10 points) and perform a detailed traffic analysis (10 points)
- Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)

**Task B: 60 points**

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. For example, the last digit of the hash for pjiang is **e**. Thus, I should pick up file "WPA2-P5-01.cap."

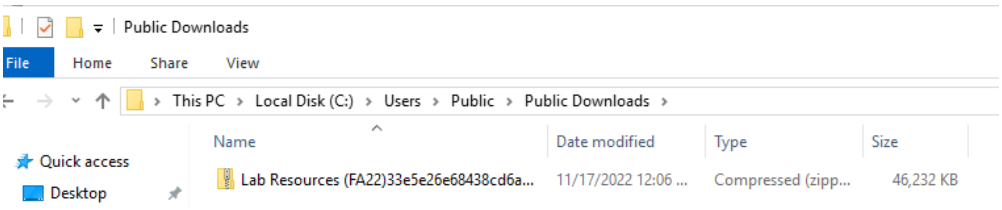
*MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e*

You can find an online MD5 hash generator or the following command to get the hash of a text string,

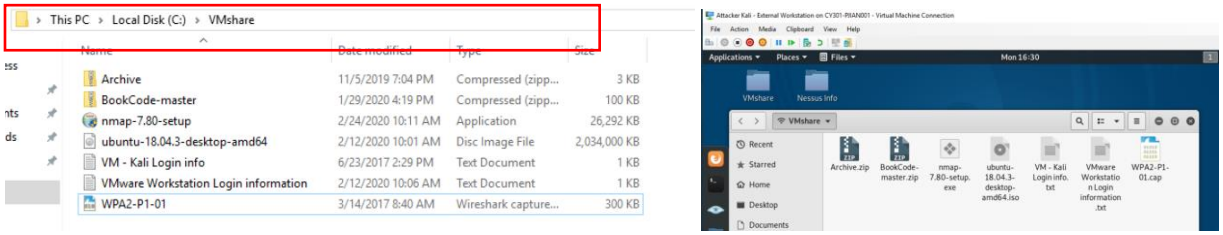
```
root@CS2APenTest:~# echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e  -
root@CS2APenTest:~#
```

| Last digit of your MD5 | Filename |
|---|---|
| **0~3** | WPA2-P1-01.cap |
| **4~5** | WPA2-P2-01.cap |
| **6~8** | WPA2-P3-01.cap |
| **9~B** | WPA2-P4-01.cap |
| **C~F** | WPA2-P5-01.cap |

The above files are zipped in a folder named "Lab Resources." You can locate zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under sub-folder “Wireless Traffic”.




Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine in order to access it from the Kali VMs.



Then complete the following steps:

1. Implement a dictionary attack and find the password. - 30 points
2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points