OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #6 Wi-Fi Password Cracking

Michael Greene

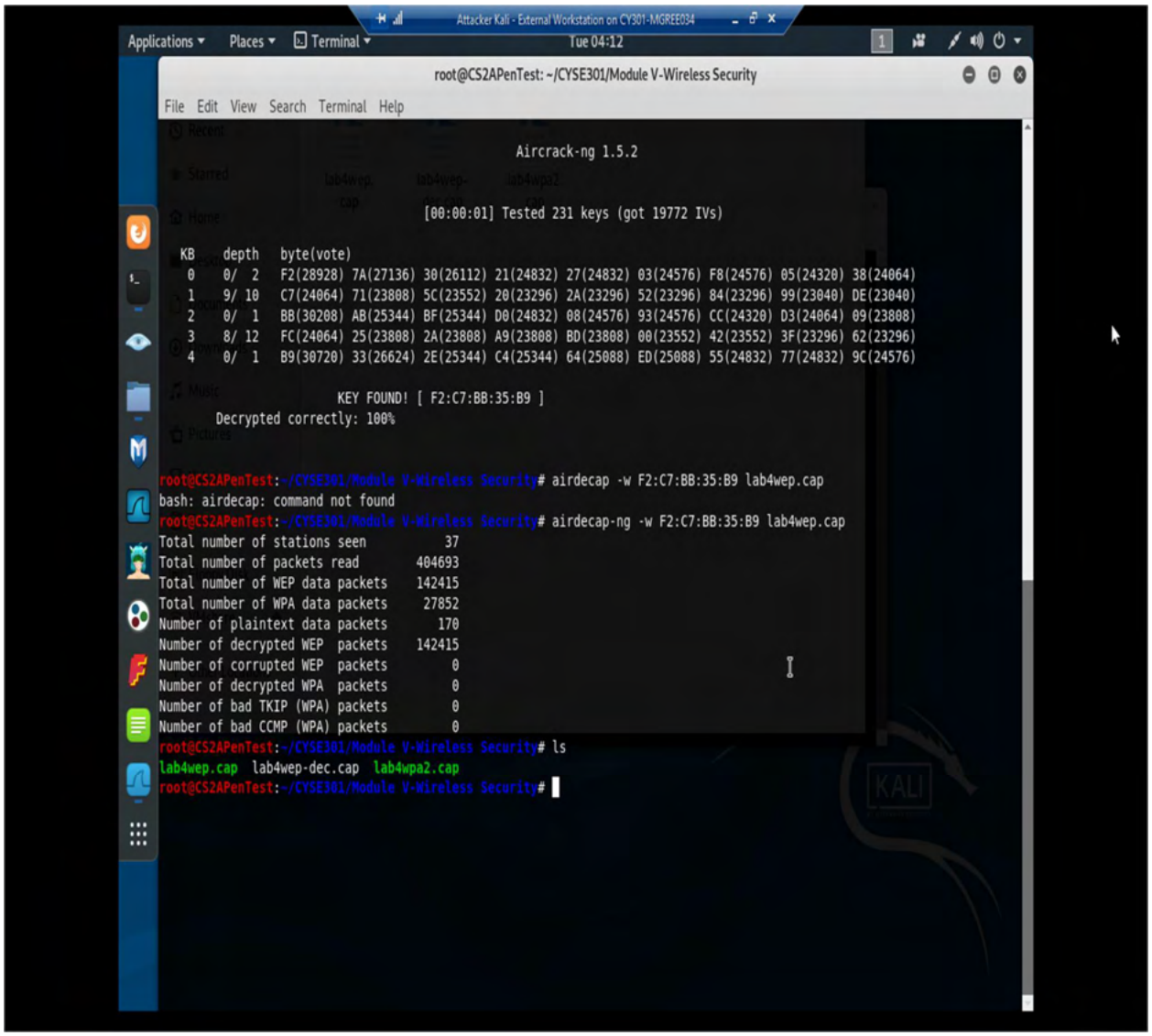
UIN: 01213114

TASK A

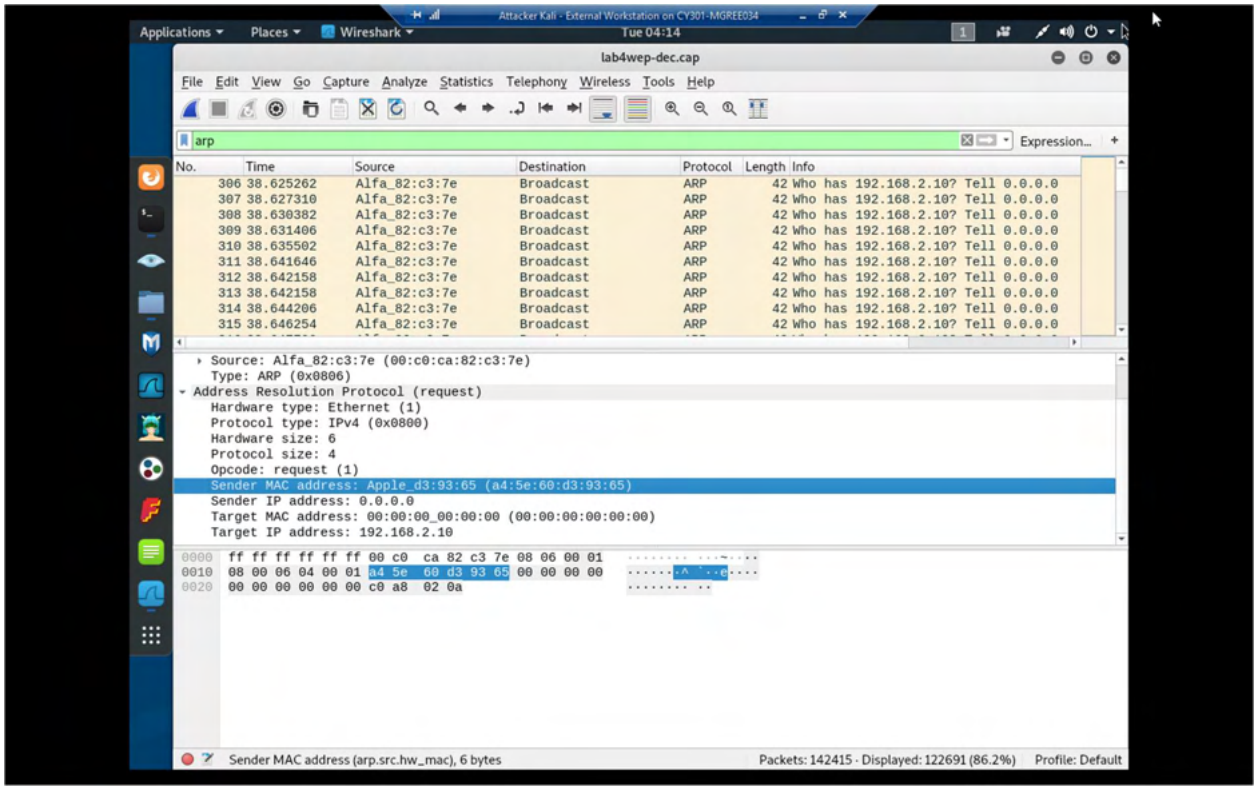
Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

Requirements:

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

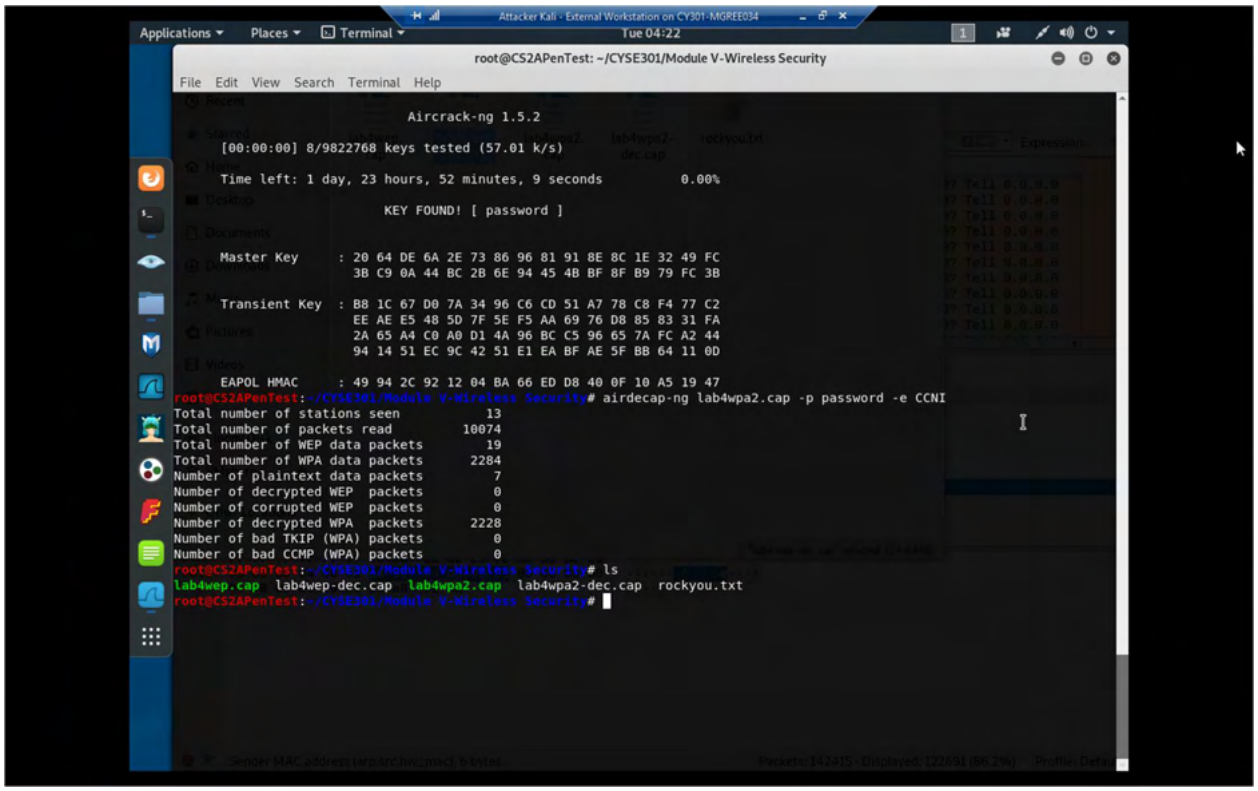


To decrypt the lab4wep.cap file I opened up a terminal within the folder containing the file. I then used the command **aircrack-ng lab4wep.cap** and chose the target network 1 with the WEP encryption. Once I found the key I used **airdecap -w F2:C7:BB:35:b9 lab4wep.cap** and was given the lab4wep-dec.cap file containing the decrypted data.

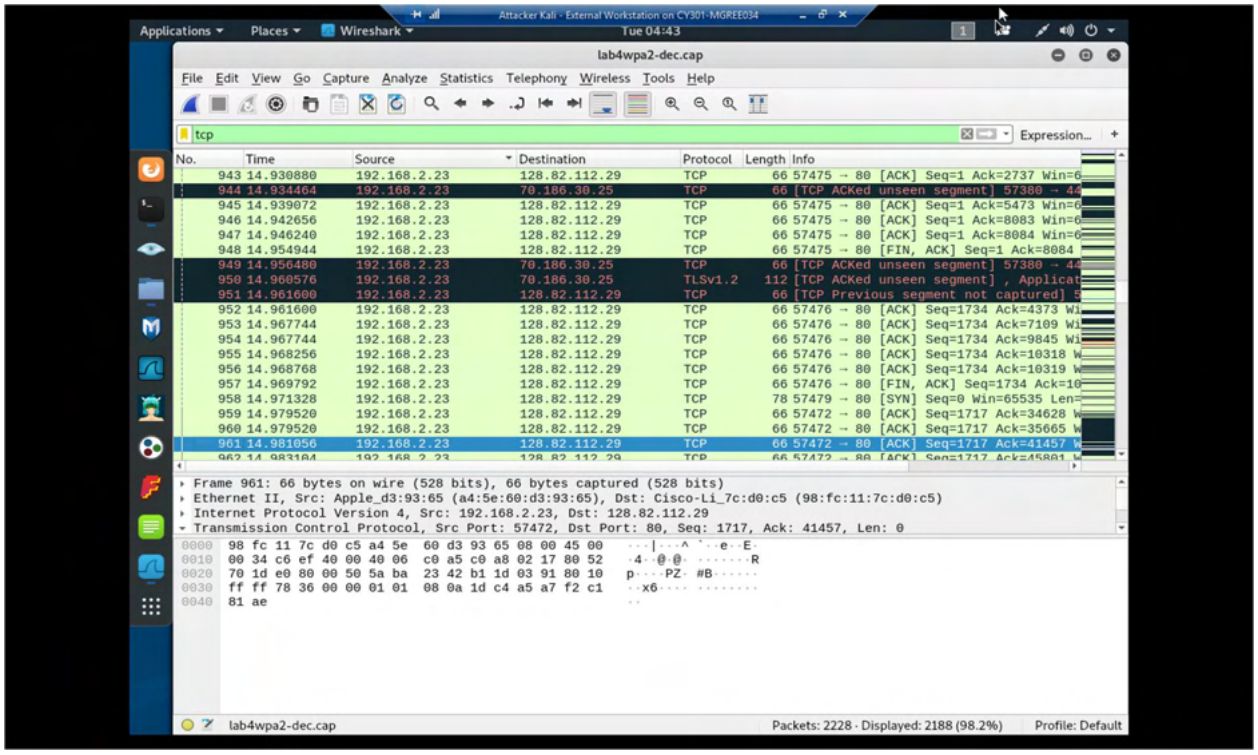


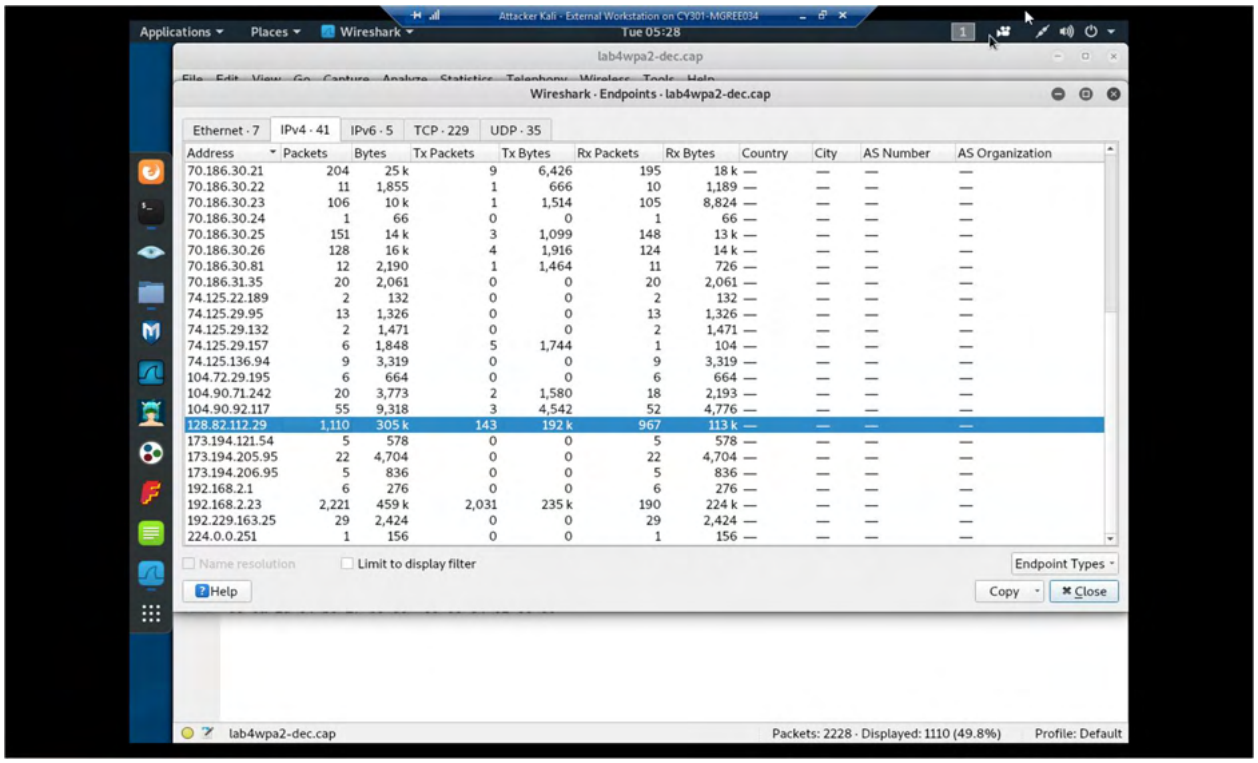
Opening the decrypted file in Wireshark, I observed a high amount of ARP request coming from Alfa_82:c3:7e. The ARP request appear to target one specific IP address 192.168.2.10. This could be an attacker attempting to deny traffic to that IP by flooding it with ARP requests.

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



In order to decrypt the lab4wpa2.cap file I opened the terminal back up and unzipped the rockyou.txt wordlist.I used the command **aircrack-ng lab4wpa2.cap** and noted the ESSID which was CCNI for later in the decryption. I then used the command **aircrack-ng lab4wpa2.cap -w rockyou.txt** to perform a dictionary attack on the file. Once I found the password which was password. I used the command **airdecap-ng lab4wpa2.cap -p password -e CCNI** and received the decrypted file lab4wpa2-dec.cap.





Opening the decrypted file in Wireshark I noticed a high amount of TCP ACK's coming from 192.168.2.23 to 128.82.112.29 on port 80. The IP address with port 80 appears to be a server since port 80 is commonly associated with HTTP. The source IP appears to be sending request from multiple ports on their own machine. This may be an attempt flood the server with ACK packets to deny legitimate traffic.

TASK B

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."

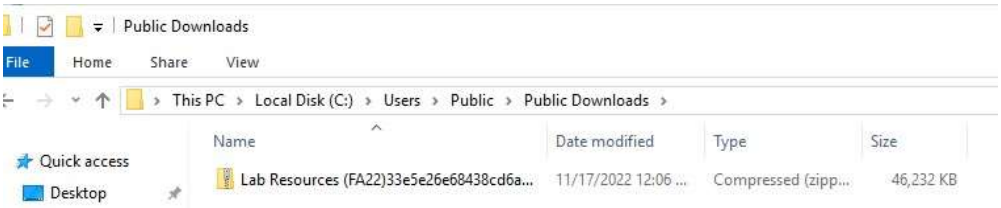
MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

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

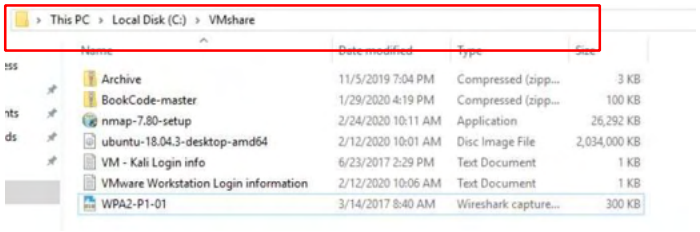
```
root@CS2APenTest:~# echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e  -
root@CS2APenTest:~#
```

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.

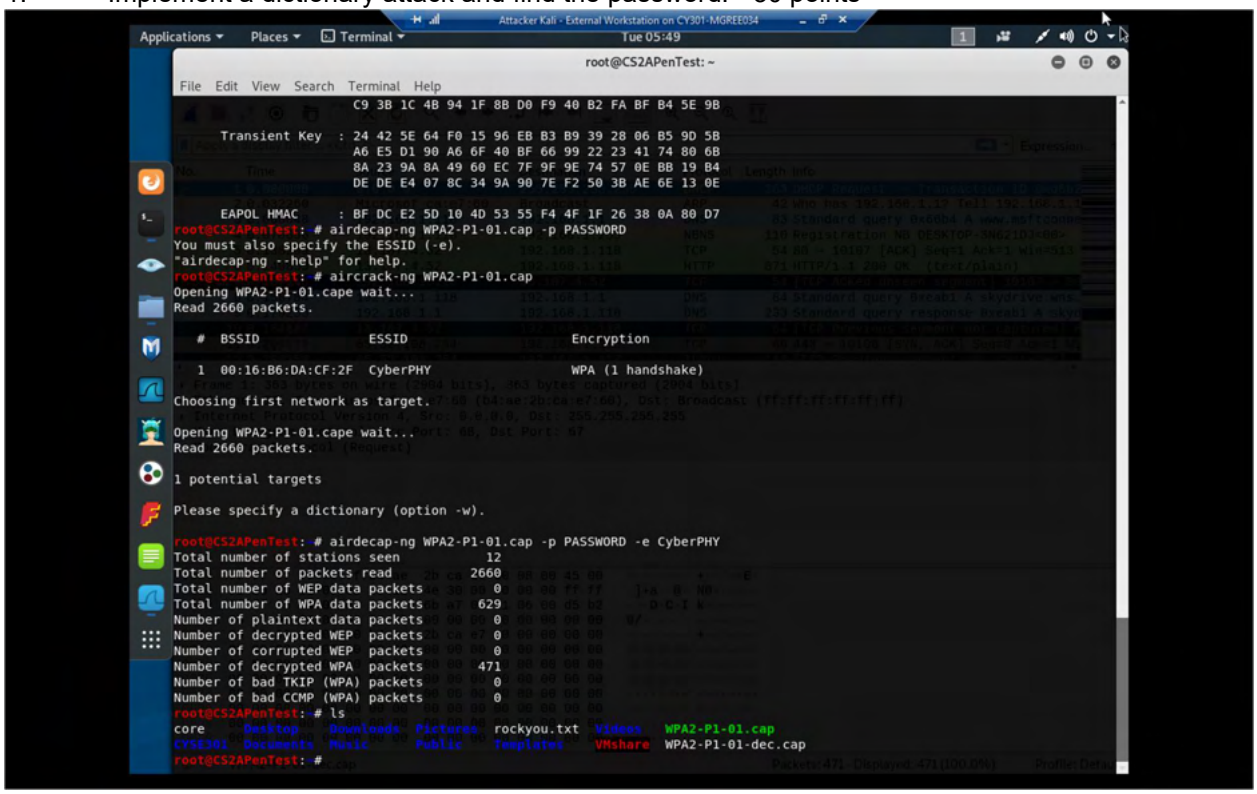


Then complete the following steps:

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

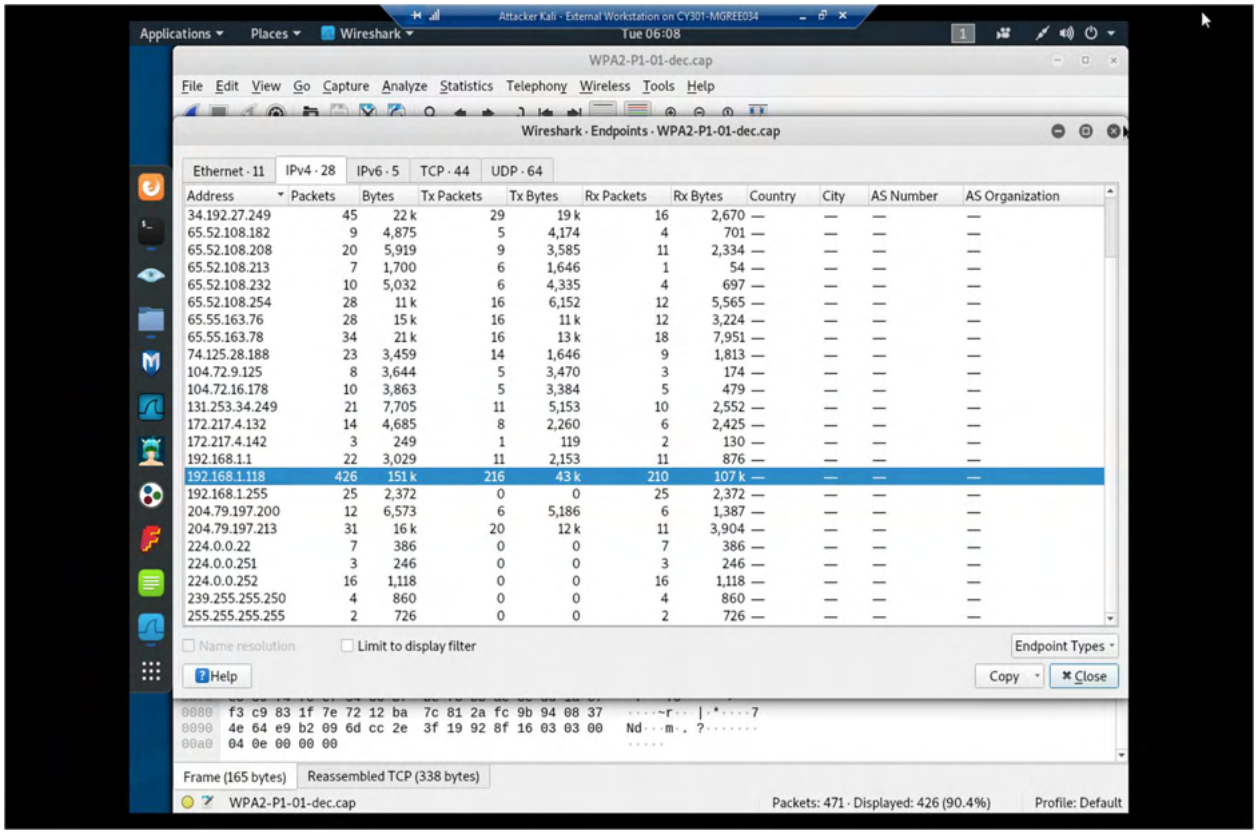
Mgree034 encrypted with MD5 was b74d4d0993f405d1411315b18a1c507***1***. So, I picked the file with the name **WPA2-P1-01.cap**.

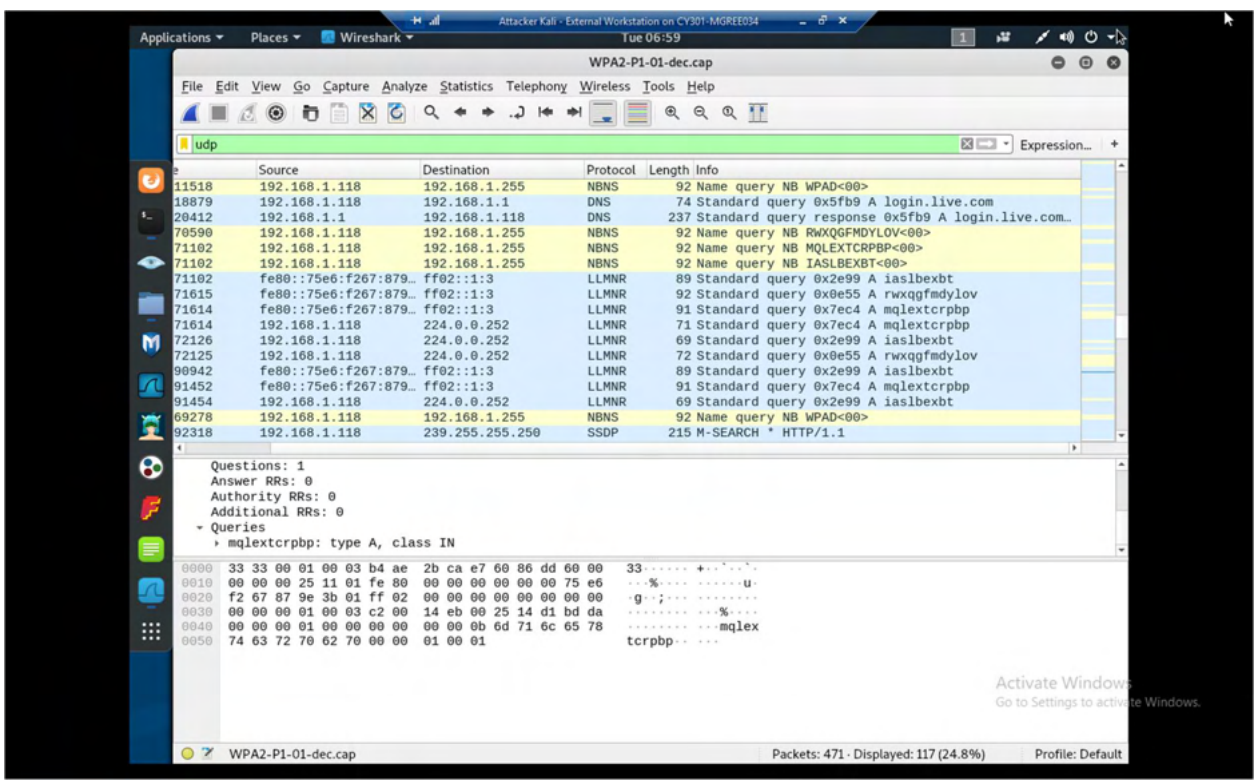
1. Implement a dictionary attack and find the password. - 30 points

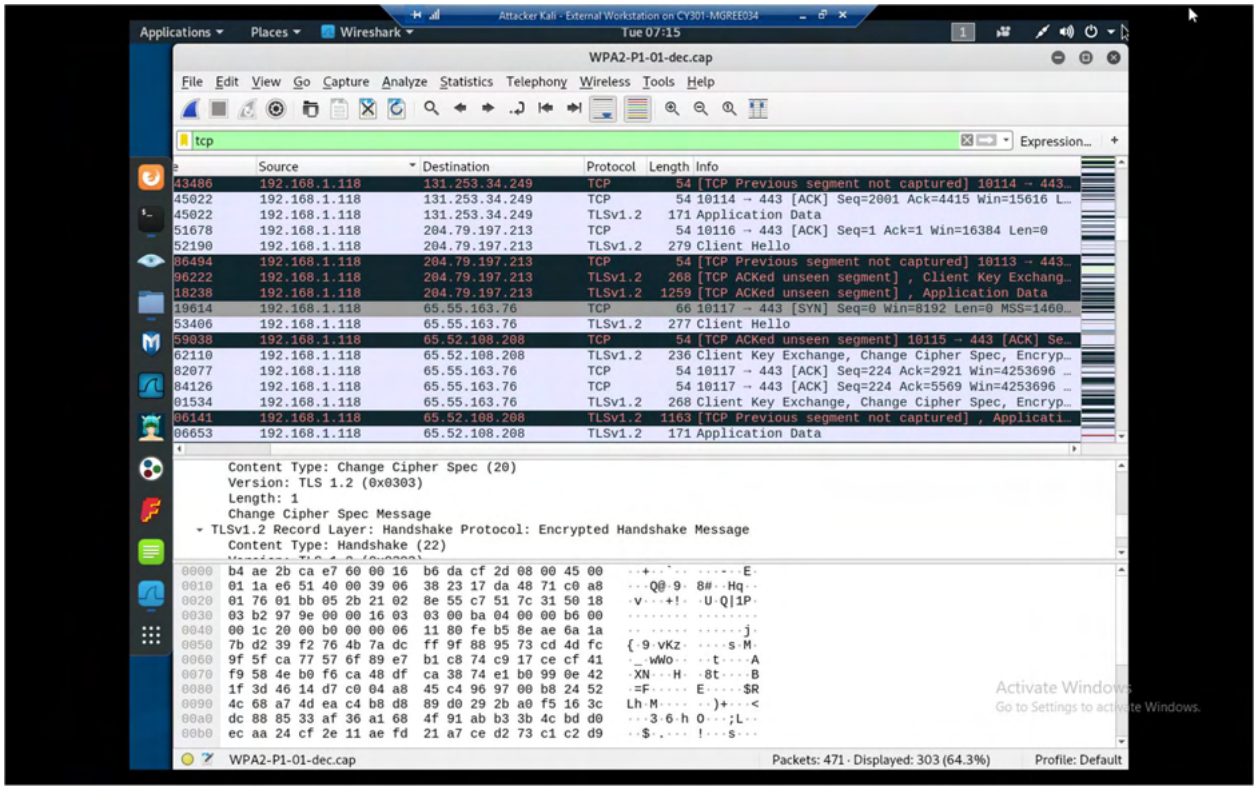


Using the same method as before with the WPA2 file. I first moved the file onto the Linux Kali VM. I then used the command **aircrack-ng WPA2-P1-01.cap -w rockyou.txt** to perform a dictionary attack on the file with the rockyou.txt wordlist. Once I found the password which was PASSWORD. I used the command aircrack-ng lab4wpa2.cap and noted the ESSID which was CyberPHY. I used the command **airdecap-ng WPA2-P1-01.cap -p PASSWORD -e CyberPHY** and received the decrypted file lab4wpa2-dec.cap.

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points







After analyzing the decrypted file in Wireshark, I noticed a high amount of traffic with the IP address 192.168.1.118. There was a high amount of encrypted traffic between the suspicious IP address and various other IP addresses. I also noticed payload exchanges, and a high amount of name queries with NetBIOS and Link-Local Multicast protocols. This may be a possible intruder in the network snooping around the network for other devices.