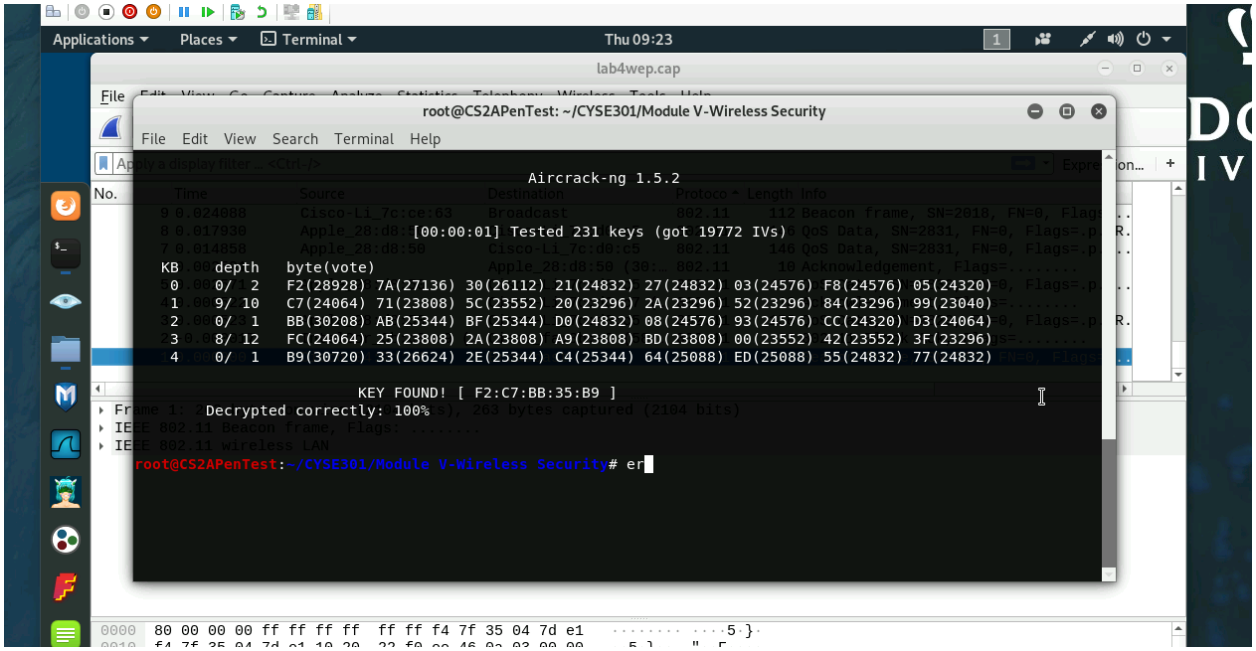
Task A: 40 points

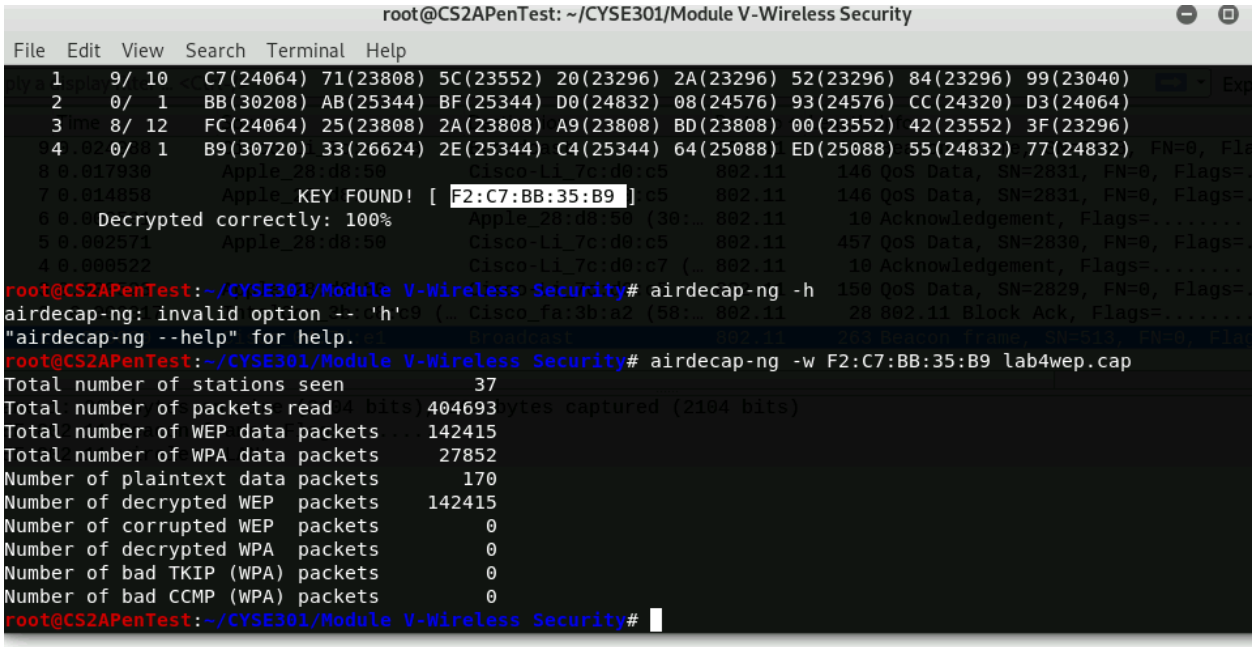
Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

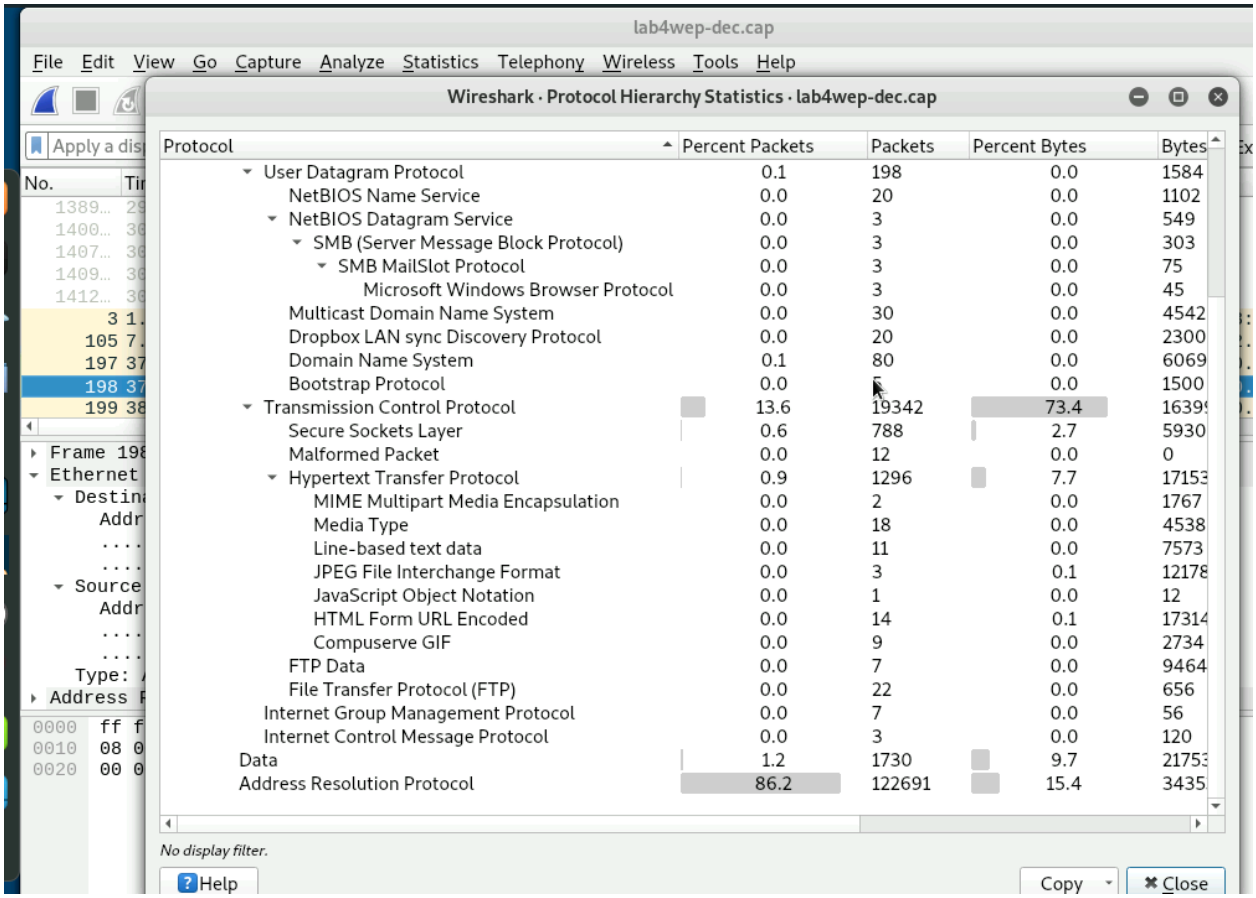
Requirements:

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

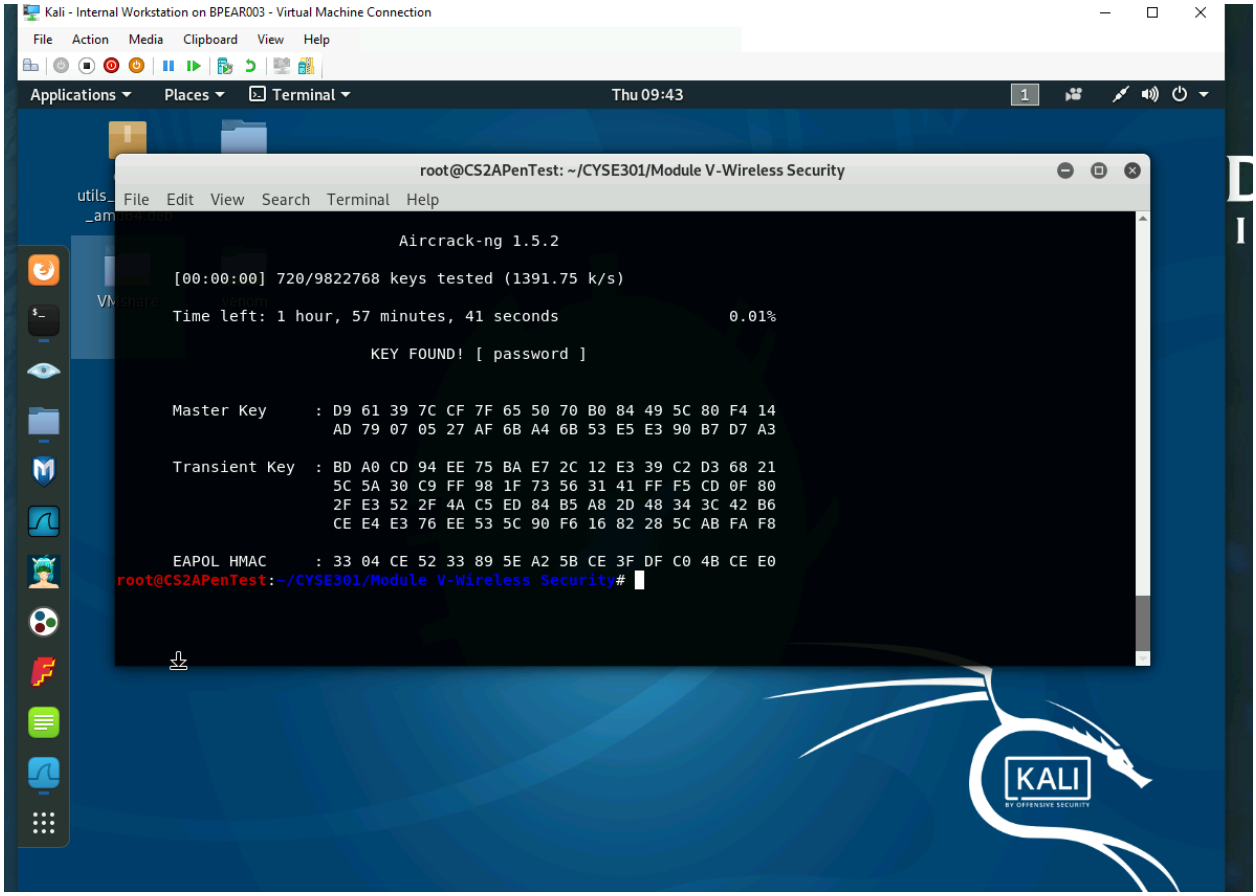
• Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)

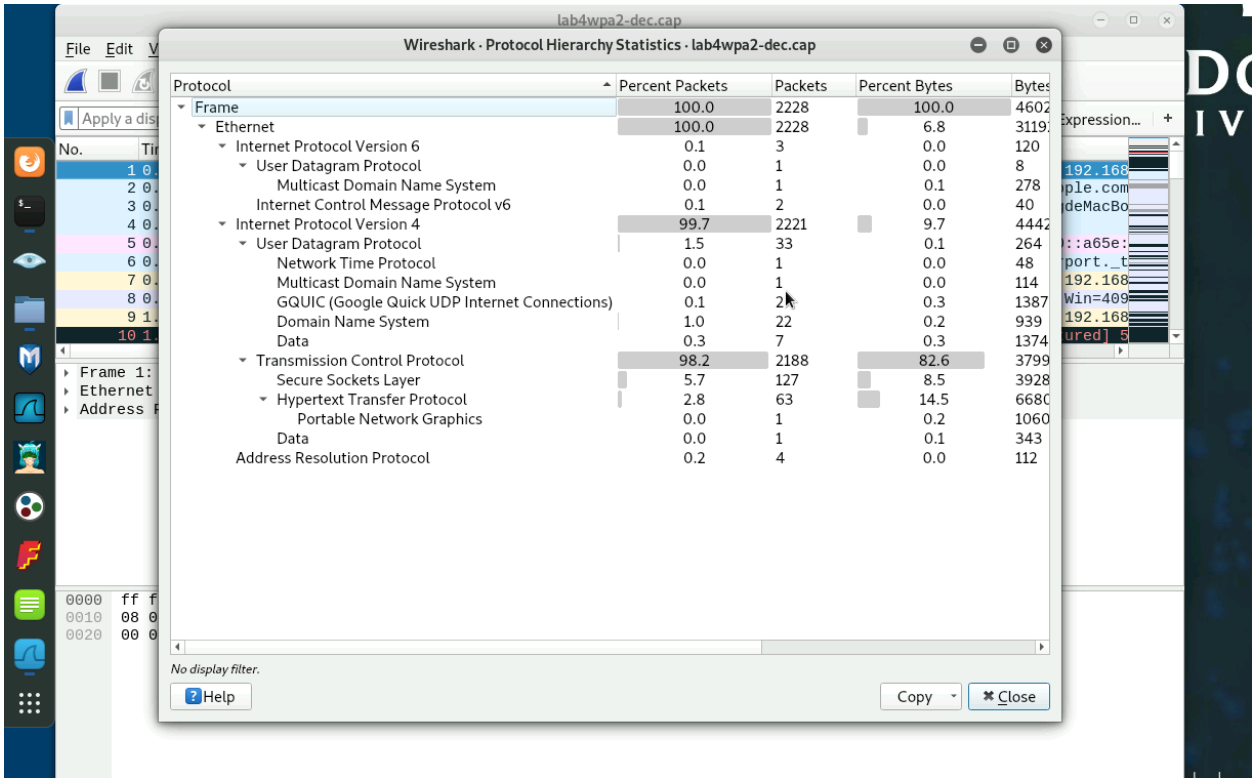







```
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# cp /usr/share/wordlists/rockyou.txt.gz /Cyse301
e V-Wireless Security .
cp: cannot stat '/Cyse301/Module': No such file or directory
cp: cannot stat 'V-Wireless': No such file or directory
cp: cannot stat 'Security': No such file or directory
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls
lab4wep.cap  lab4wep-dec.cap  lab4wpa2.cap  rockyou.txt.gz
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# gunzip rockyou.txt.gz
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls
lab4wep.cap  lab4wep-dec.cap  lab4wpa2.cap  rockyou.txt
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
```


Kali - Internal Workstation on BPEAR003 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 09:43
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
[00:00:00] 720/9822768 keys tested (1391.75 k/s)
Time left: 1 hour, 57 minutes, 41 seconds 0.01%
KEY FOUND! [password]
Master Key : D9 61 39 7C CF 7F 65 50 70 B0 84 49 5C 80 F4 14
AD 79 07 05 27 AF 6B A4 6B 53 E5 E3 90 B7 D7 A3
Transient Key : BD A0 CD 94 EE 75 BA E7 2C 12 E3 39 C2 D3 68 21
5C 5A 30 C9 FF 98 1F 73 56 31 41 FF F5 CD 0F 80
2F E3 52 2F 4A C5 ED 84 B5 A8 2D 48 34 3C 42 B6
CE E4 E3 76 EE 53 5C 90 F6 16 82 28 5C AB FA F8
EAPOL HMAC : 33 04 CE 52 33 89 5E A2 5B CE 3F DF C0 4B CE E0
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
KALI



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:~/CYSE301/Module V-Wireless Security# echo -n bpear003 | md5sum
b8d1c2eb538b0cb05cf8ad4229250380  -
```

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 the zipped folder in the Windows 10 Host Machine under C:/VMShare. Then, unzip the following zipped file in the Kali Linux VM,find the assigned WPA file under sub-folder “Module 5”.

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

In order to ge the password/ key for the 0~3 WPA2-P1-01.cap document. I came across many confusing parts so I am not sure if I did it the way that was entended. I had to make sure that a rockyou.txt was inside the lab resource folder and that I was in the correct directory before doing any commands.

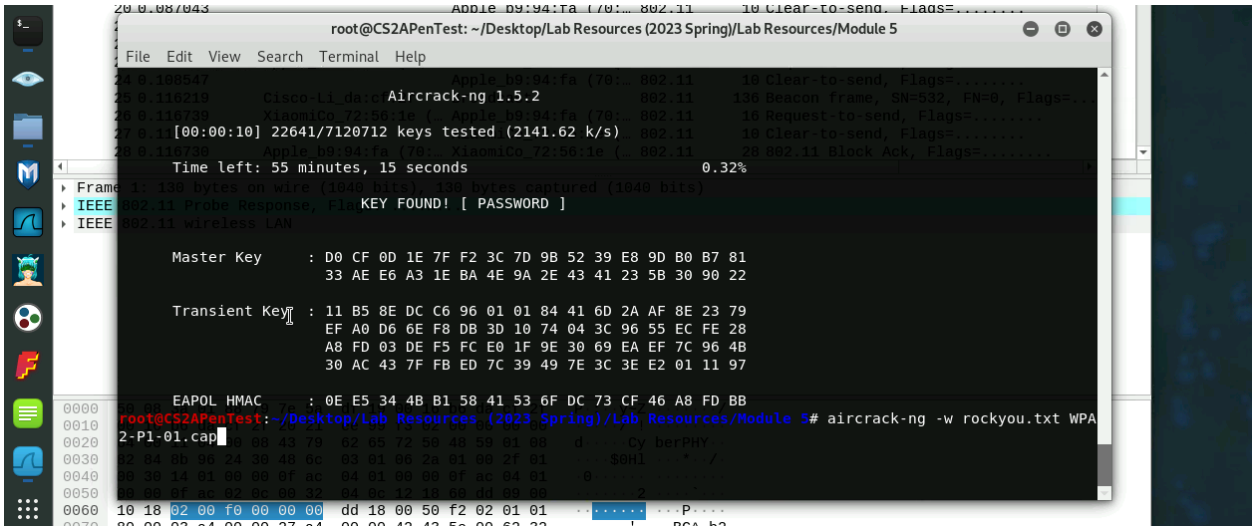
The first command I did was

aircrack-ng WPA2-P1-01.cap

I got this screen above. Usually, you would type 1 or the number that went with the encryption you wanted but it didn't let me. My solution was to use the command

aircrack-ng -w rockyou.txt WPA2-P!-01.cap

This worked and gave me key found screen PASSWORD

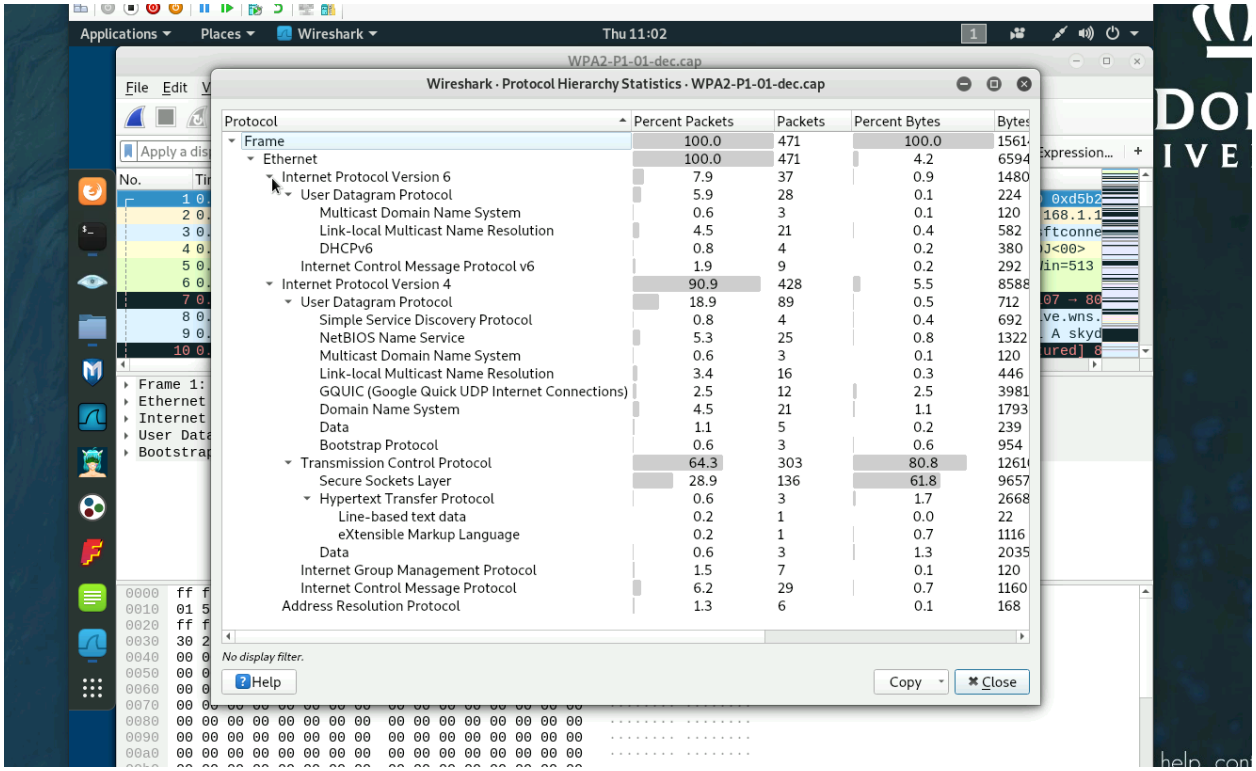


After this, I used the command Airdecap-ng -p PASSWORD WPA2-p1-01.cap -e CyberPHY

```
root@CS2APenTest:~/Desktop/Lab Resources (2023 Spring)/Lab Resources/Module 5# airdecap-ng -p PASSWORD WPA2-P1-01.cap -e
 CyberPHY
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        471
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
root@CS2APenTest:~/Desktop/Lab Resources (2023 Spring)/Lab Resources/Module 5#
```

Wireshark WPA2-p1-01.dec.cap to view the new file that is deciphered

.



This is the Protocol Hierarchy after decryption

After review, there are multiple different protocols that are used = Mostly TCP, ICMP, and NBNS

Looks like Cisco and Microsoft