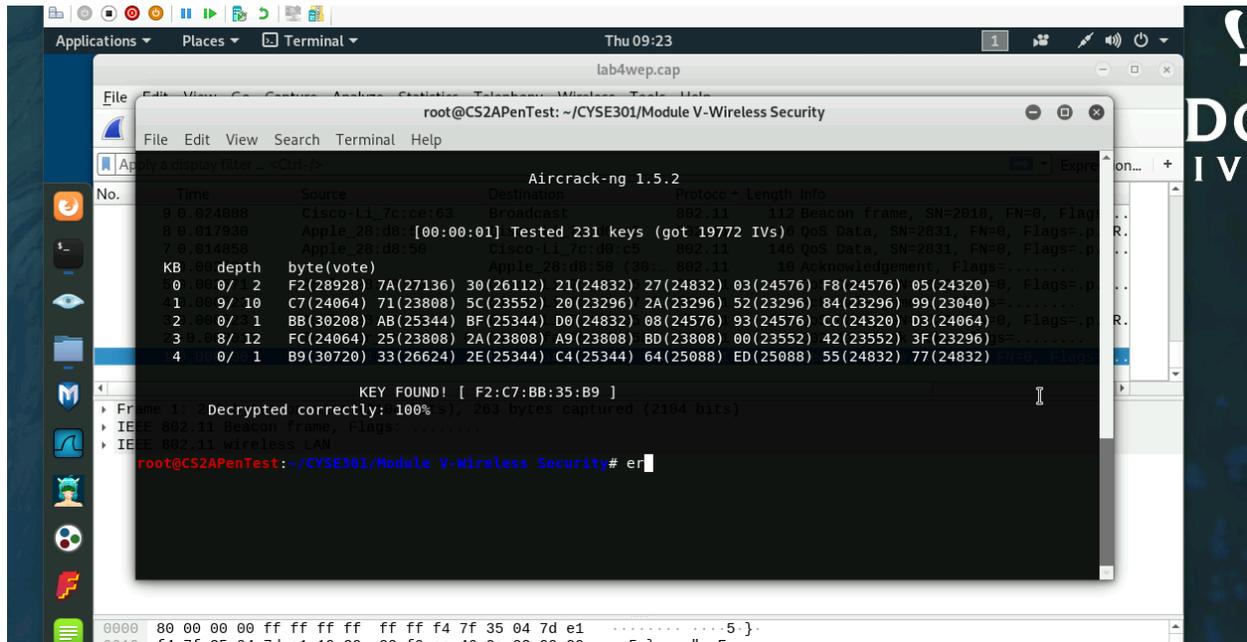


Task A: 40 points

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

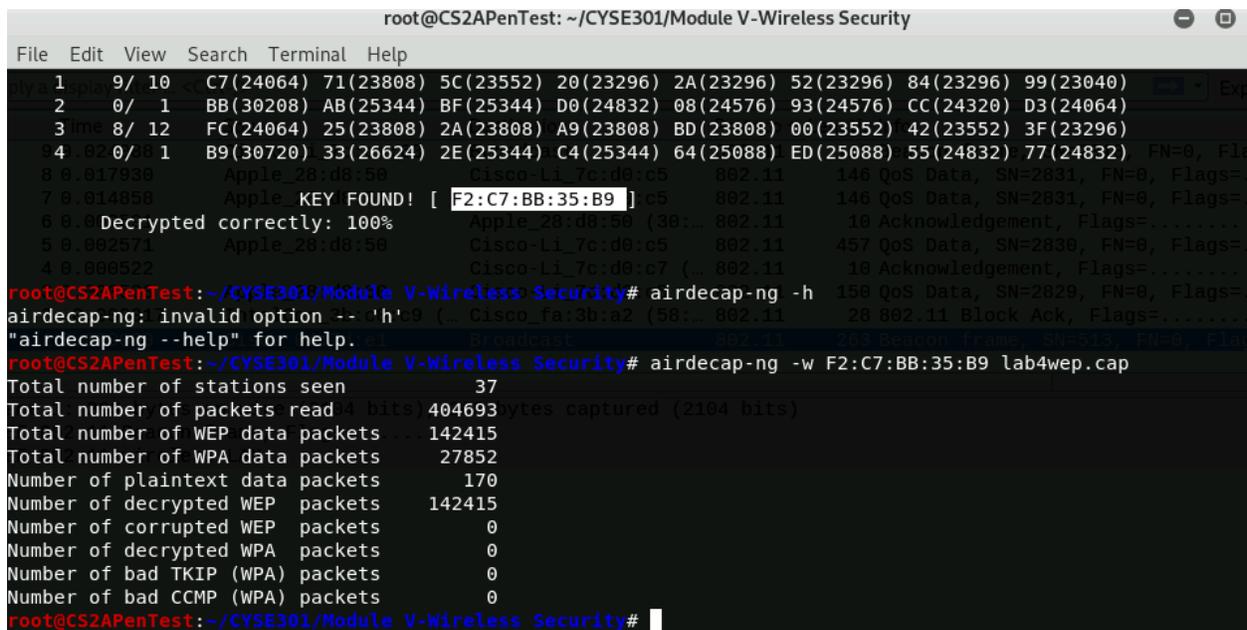
Requirements:

- 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)

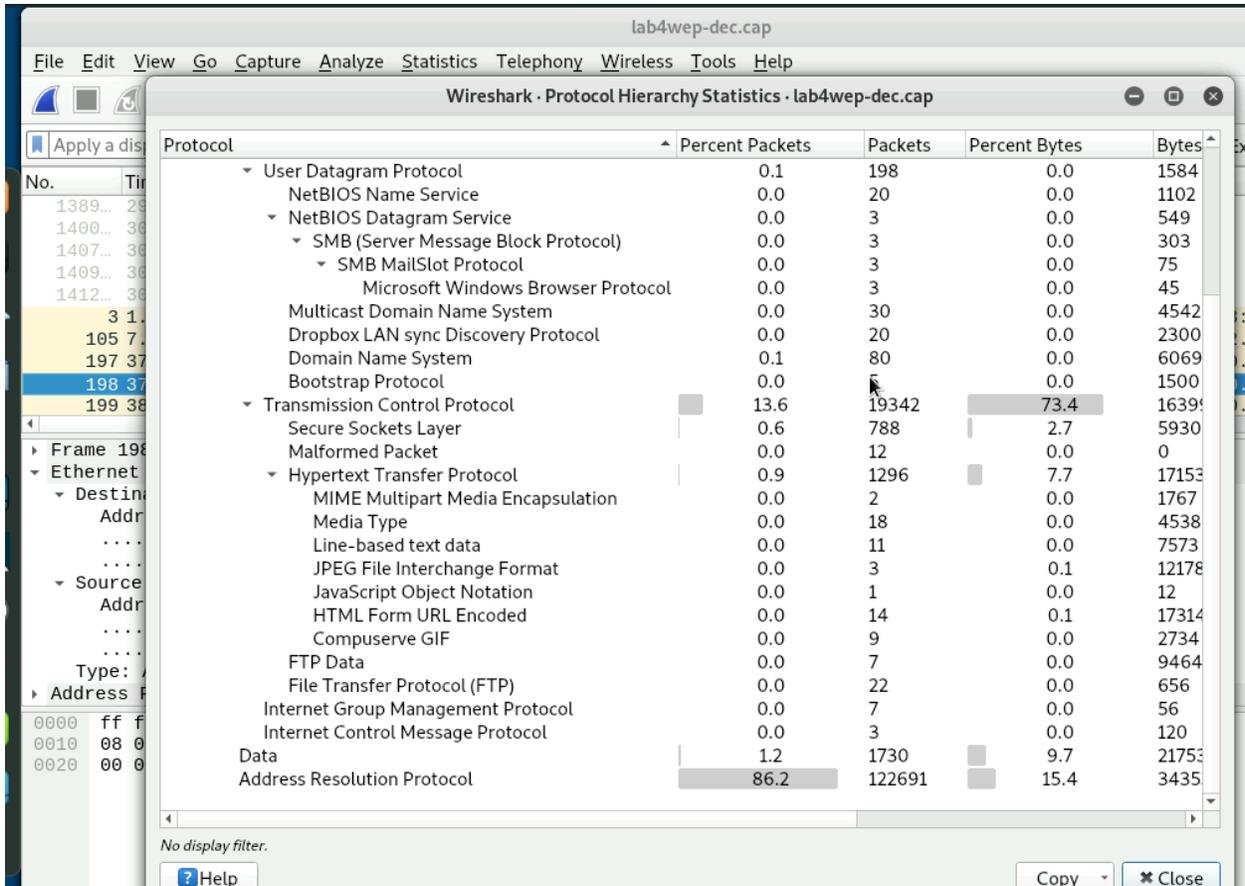


```
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
No. Time Source Destination Protocol Length Info
9 0.024000 Cisco-L1_7c:d0:c5 Broadcast 802.11 112 Beacon Frame, SN=2818, FN=0, Flag
8 0.017930 Apple 28:d8:50 [00:00:01] Tested 231 keys (got 1972 IVs) 005 Data, SN=2831, FN=0, Flags=
7 0.014850 Apple 28:d8:50 Cisco-L1_7c:d0:c5 802.11 146 QoS Data, SN=2831, FN=0, Flags=
KB enc depth byte(vote)
0 00/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 00, Flags=
1 00/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040)
2 00/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 00, Flags=
3 08/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296)
4 00/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832)

KEY FOUND! [ F2:C7:BB:35:B9 ]
> Frame 1: Decrypted correctly: 100% (204 bytes captured (2194 bits))
> IEEE 802.11 Beacon Frame, Flags=
> IEEE 802.11 Wireless LAN
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng
```



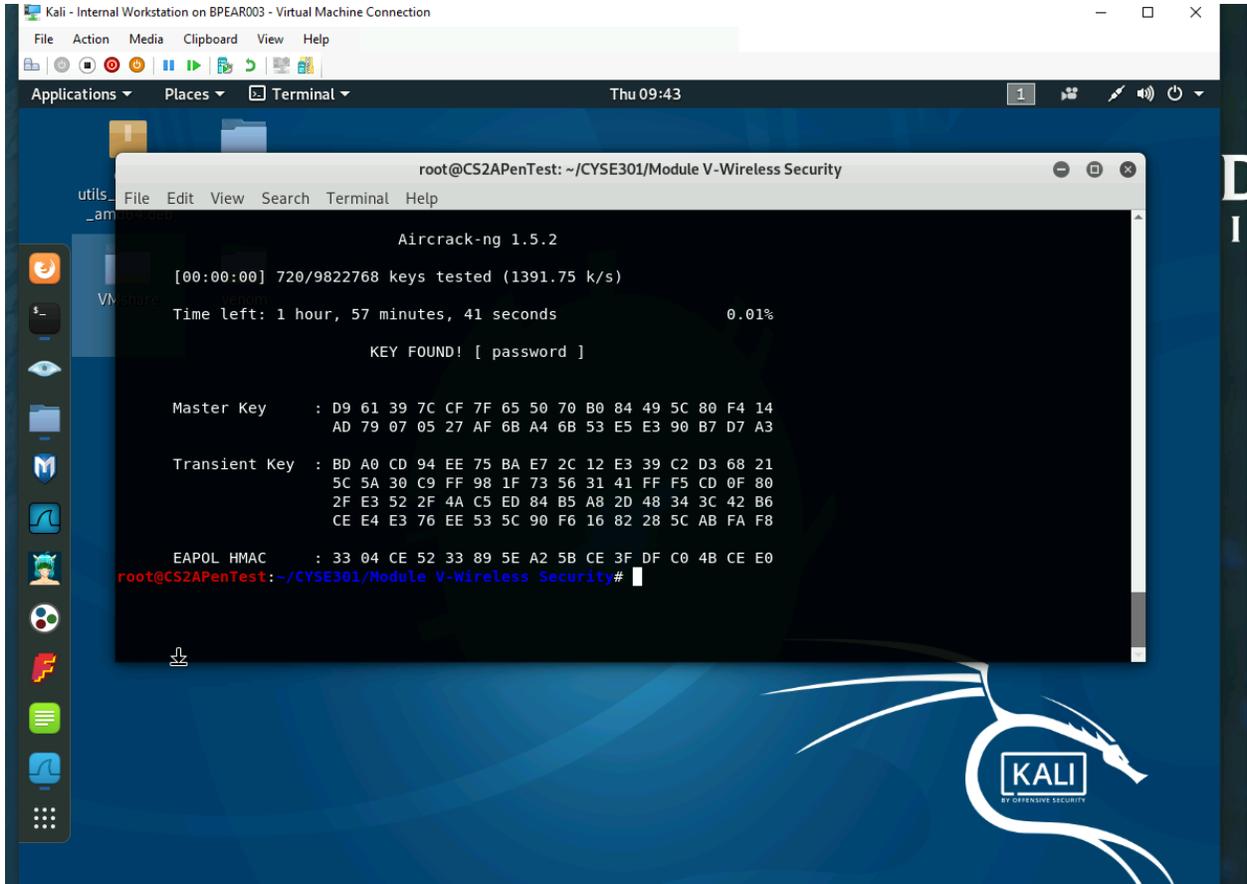
```
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064)
3 08/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296)
4 00/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) FN=0, Fl
8 0.017930 Apple 28:d8:50 Cisco-L1_7c:d0:c5 802.11 146 QoS Data, SN=2831, FN=0, Flags=
7 0.014850 Apple KEY FOUND! [ F2:C7:BB:35:B9 ] c5 802.11 146 QoS Data, SN=2831, FN=0, Flags=
6 0.0 Decrypted correctly: 100% Apple 28:d8:50 (30 802.11 10 Acknowledgement, Flags=
5 0.002571 Apple 26:d8:50 Cisco-L1_7c:d0:c7 802.11 457 QoS Data, SN=2830, FN=0, Flags=
4 0.000522 Cisco-L1_7c:d0:c7 802.11 10 Acknowledgement, Flags=
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -h
airdecap-ng: invalid option -- 'h' ( Cisco-Ta:3b:a2 (58 802.11 28 802.11 Block Ack, Flags=
"airdecap-ng --help" for help.
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -w F2:C7:BB:35:B9 lab4wep.cap
Total number of stations seen 37
Total number of packets read 404693 bytes captured (2104 bits)
Total number of WEP data packets 142415
Total number of WPA data packets 27852
Number of plaintext data packets 170
Number of decrypted WEP packets 142415
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
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
```

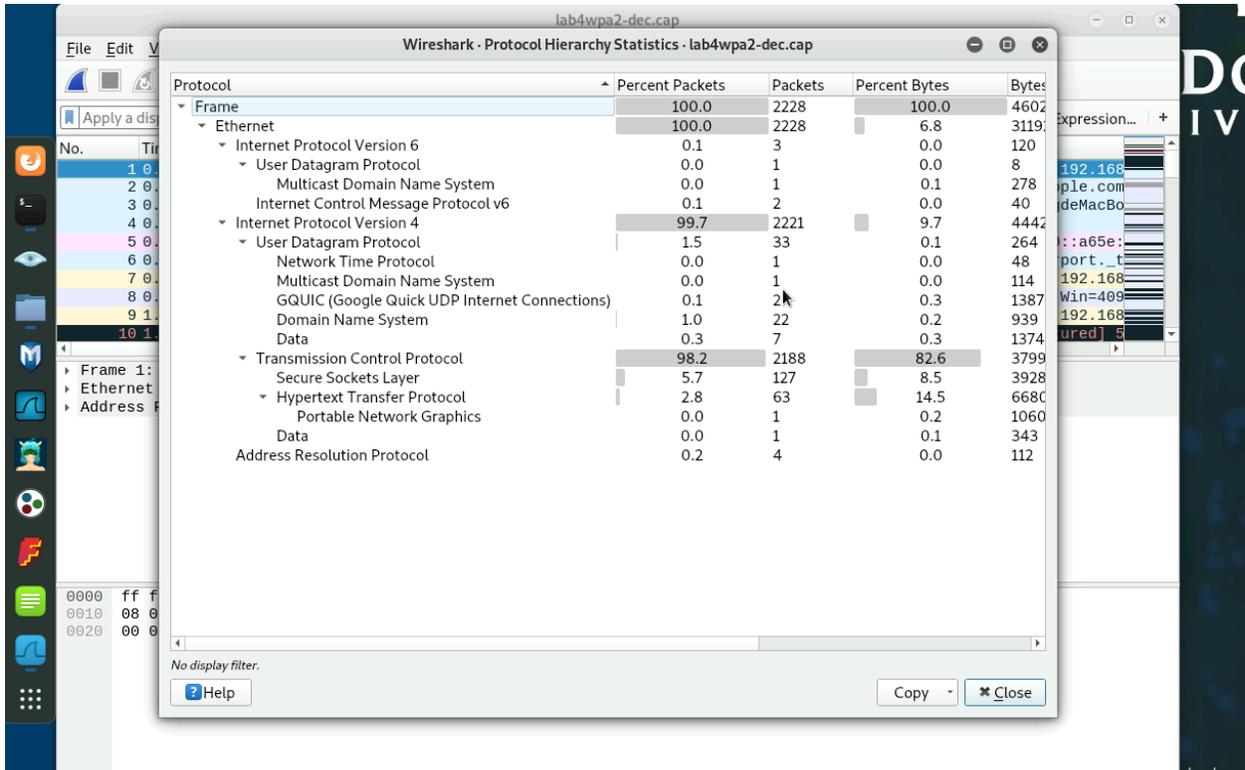


```

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# cp /usr/share/wordlists/rockyou.txt.gz /Cyse301/Module 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#

```





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 bppear003 | 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 get 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 intended. 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

```

root@CS2APenTest:~/Desktop/Lab Resources (2023 Spring)/Lab Resources/Module 5# aircrack-ng WPA2-P1-01.cap
Opening WPA2-P1-01.cape wait...
Read 2660 packets.

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

Choosing first network as target.

Opening WPA2-P1-01.cape wait...
Read 2660 packets.

1 potential targets

Please specify a dictionary (option -w).

```

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-P1-01.cap

This worked and gave me key found screen **PASSWORD**

```

root@CS2APenTest:~/Desktop/Lab Resources (2023 Spring)/Lab Resources/Module 5# aircrack-ng -w rockyou.txt WPA2-P1-01.cap
AirCrack-ng 1.5.2
[00:00:10] 22641/7120712 keys tested (2141.62 k/s)
Time left: 55 minutes, 15 seconds 0.32%
Frame 1: 130 bytes on wire (1040 bits) captured (1940 bits) on 0
IEEE 802.11 Probe Response, FI, KEY FOUND! [ PASSWORD ]
IEEE 802.11 Wireless LAN

Master Key      : D0 CF 0D 1E 7F F2 3C 7D 9B 52 39 E8 9D B0 B7 81
                  33 AE E6 A3 1E BA 4E 9A 2E 43 41 23 5B 30 90 22

Transient Key   : 11 B5 8E DC C6 96 01 01 84 41 6D 2A AF 8E 23 79
                  EF A0 D6 6E F8 DB 3D 10 74 04 3C 96 55 EC FE 28
                  A8 FD 03 DE F5 FC E0 1F 9E 30 69 EA EF 7C 96 4B
                  30 AC 43 7F FB ED 7C 39 49 7E 3C 3E E2 01 11 97

EAPOL HMAC     : 0E E5 34 4B B1 58 41 53 6F DC 73 CF 46 A8 FD BB
root@CS2APenTest:~/Desktop/Lab Resources (2023 Spring)/Lab Resources/Module 5# aircrack-ng -w rockyou.txt WPA2-P1-01.cap

```

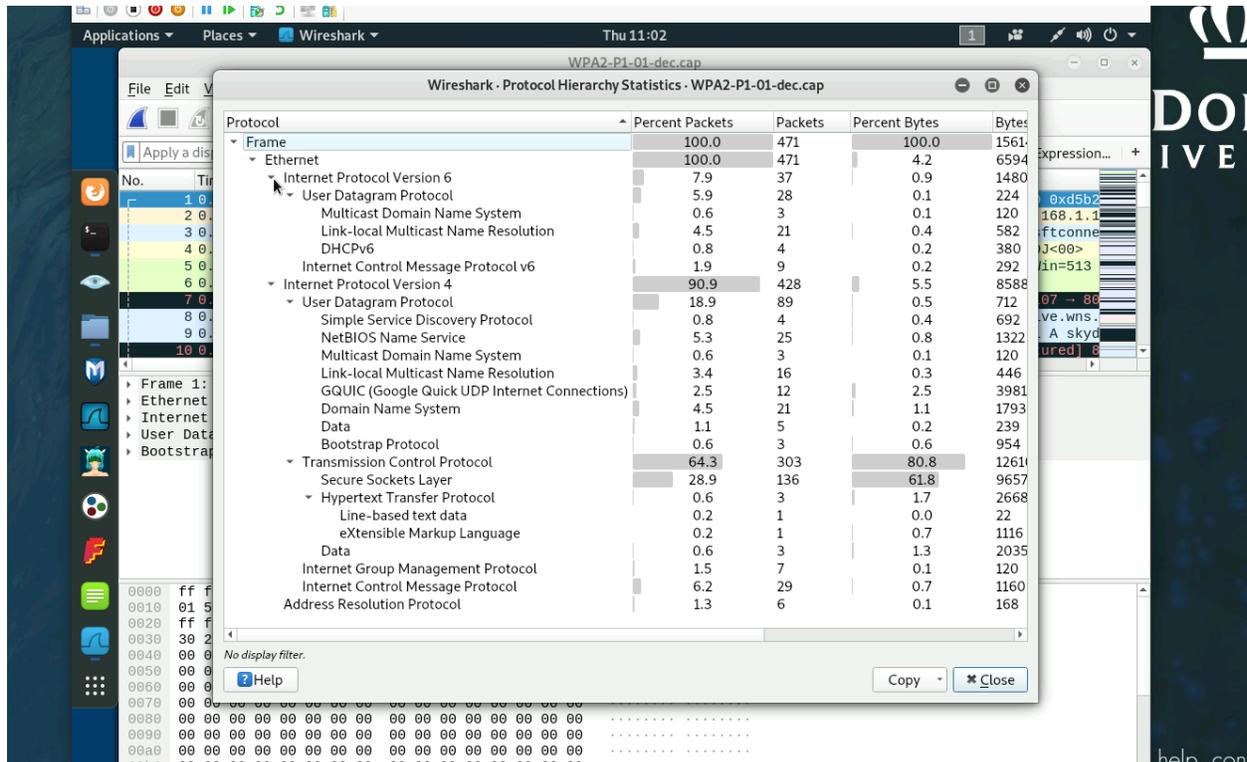
After this, I used the command **Airdecap-ng -p PASSWORD WPA2-p1-01.cap -e CyberPHY**

```

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