# Assignment 6: Wi-Fi Password Cracking

Jessiah Davis

Old Dominion University

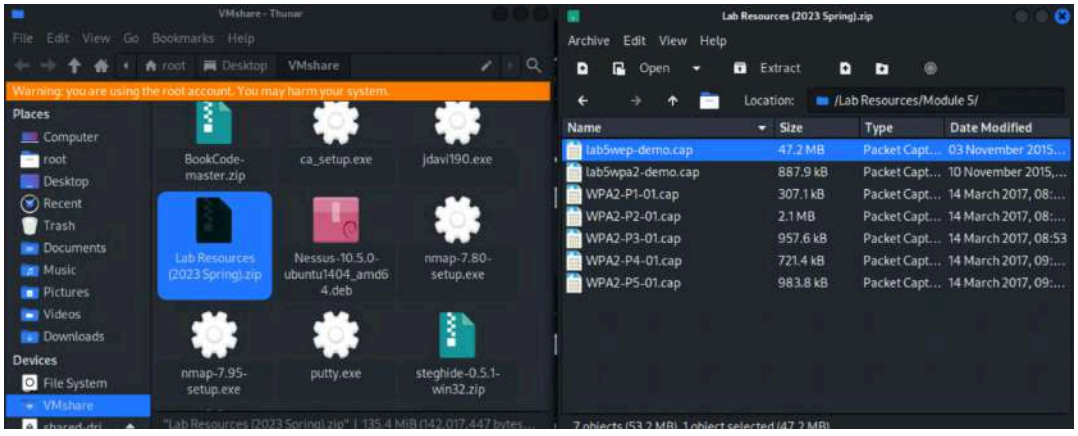
Cyse301

Task C: 20 points

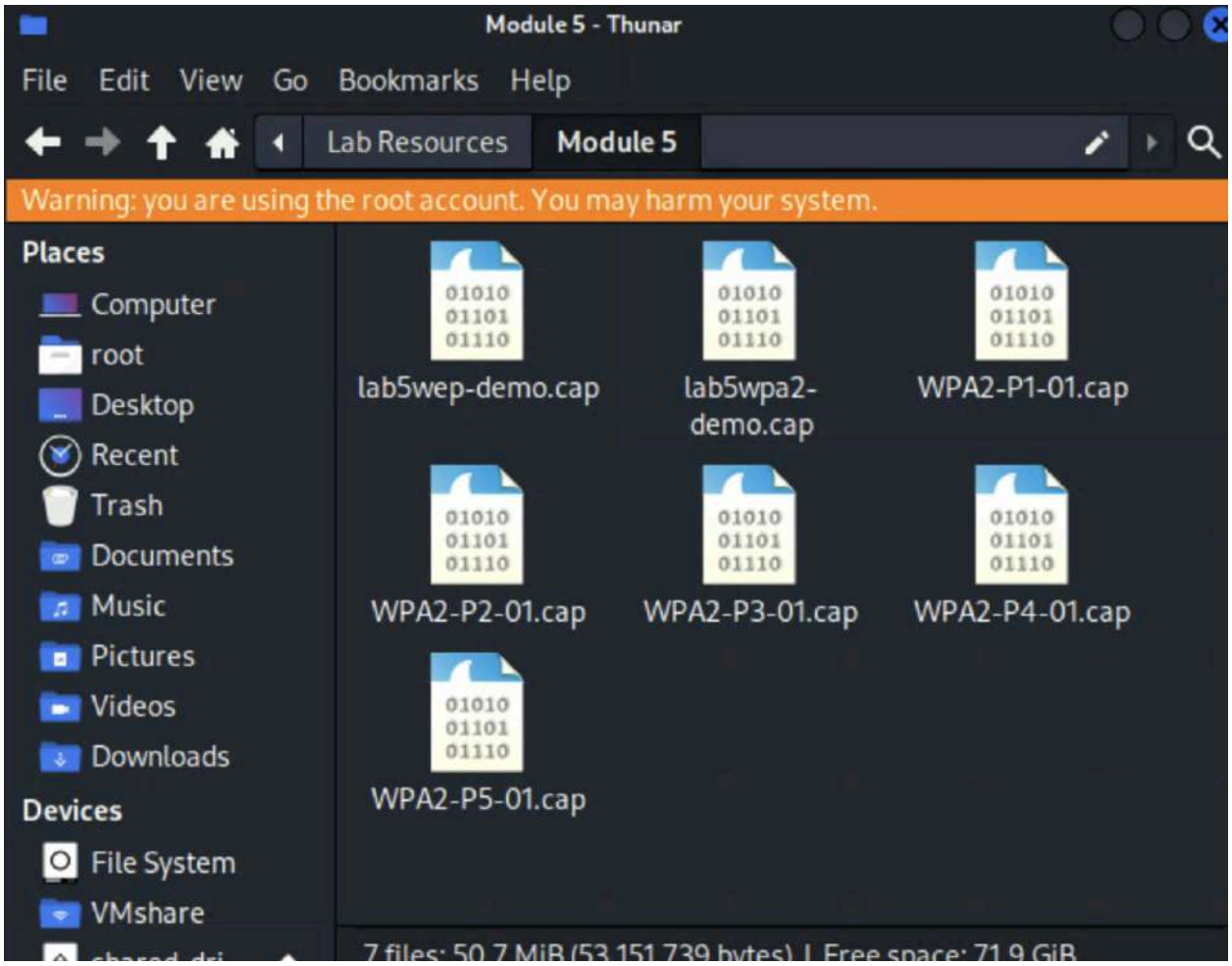
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

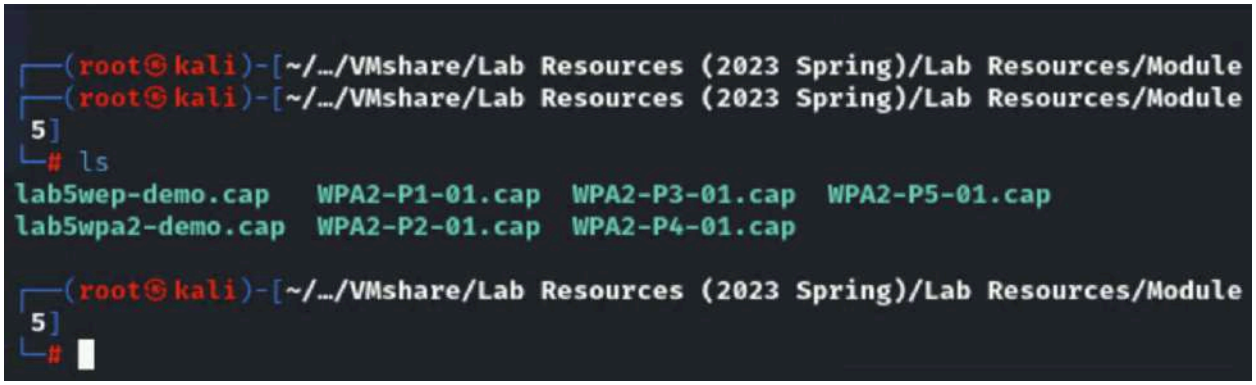
1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

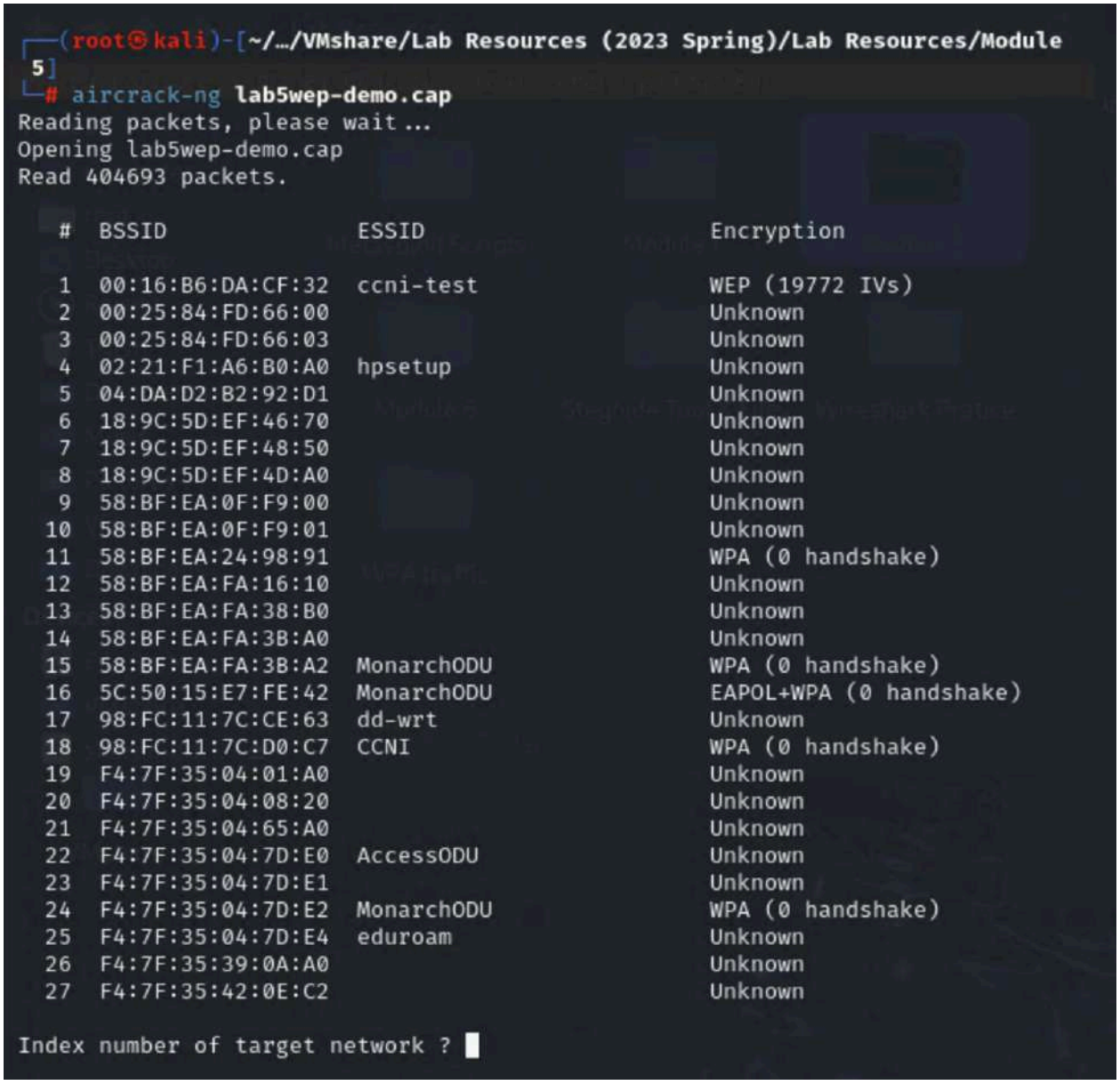
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)



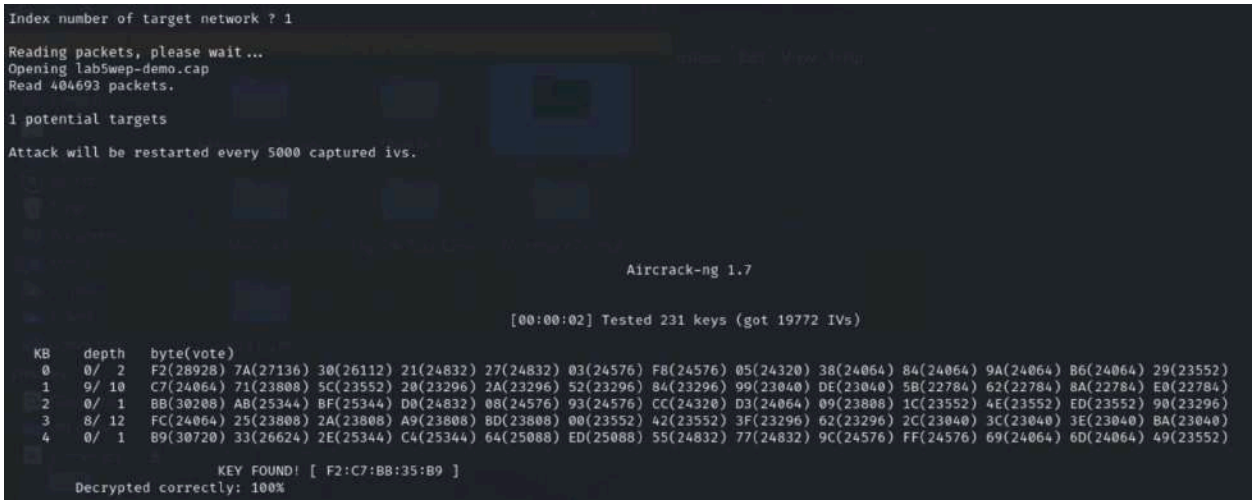
I was able to go back and fix my mistake and I extracted the file for the lab resources so i can get the correct sources for this lab.



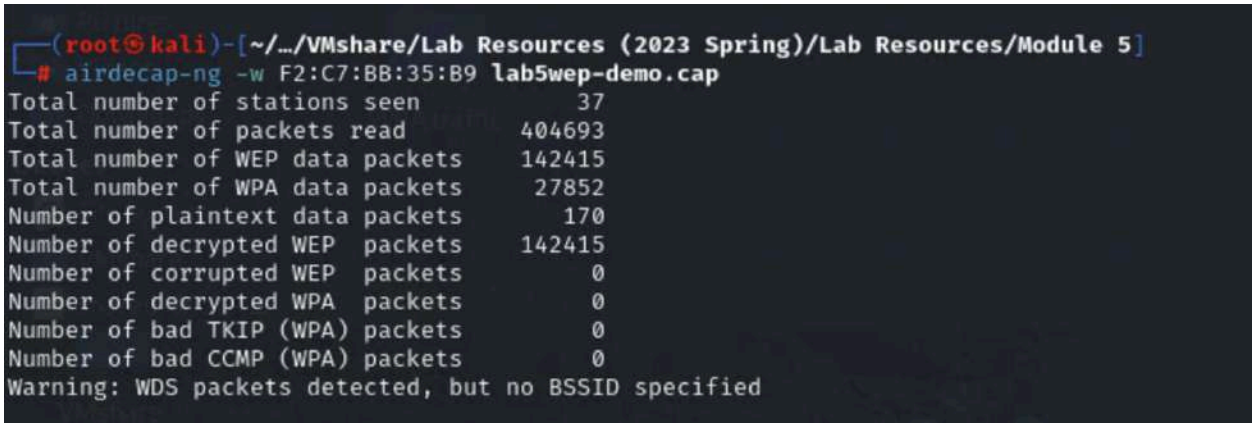



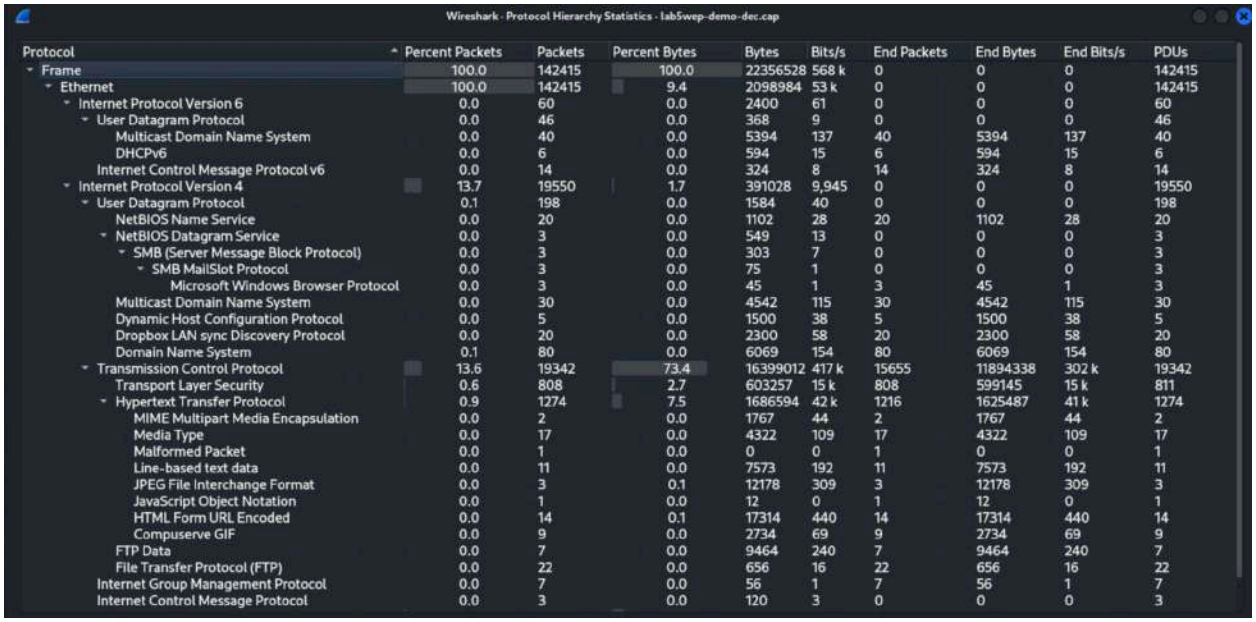



I used the command aircrack-ng and then added the demo.cap




Found key: F2:C7:BB:35:B9



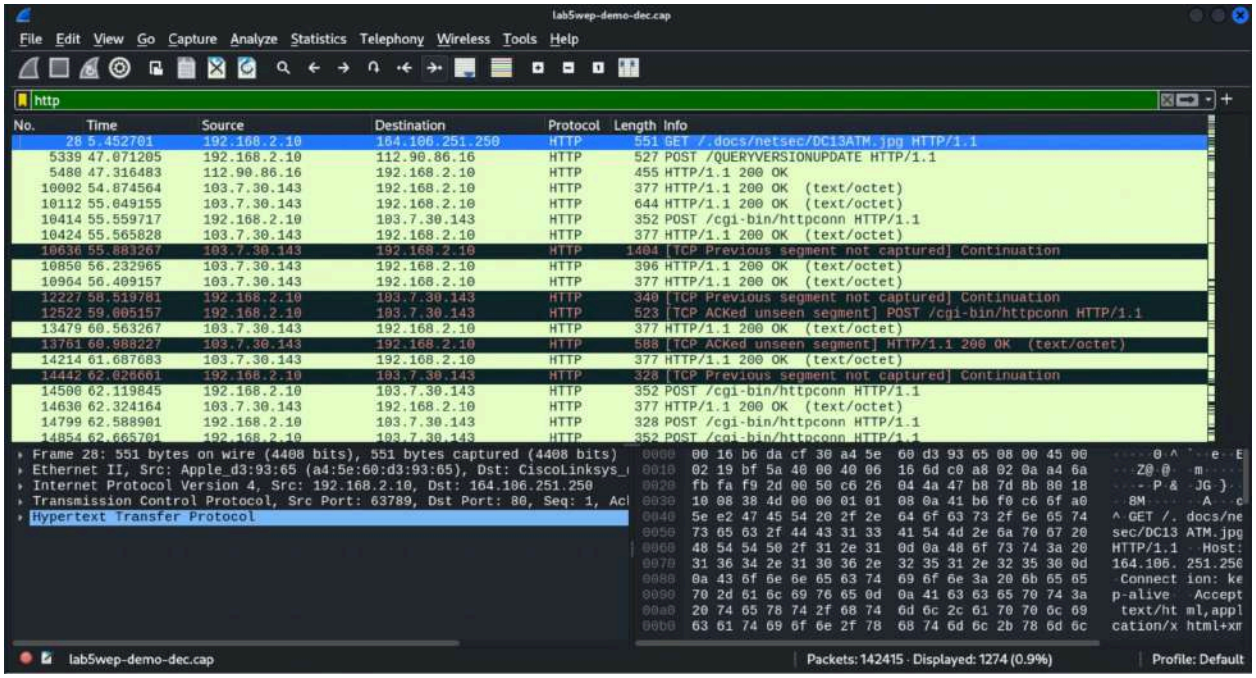



| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs |
|---|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 142415 | 100.0 | 22356528 | 568 k | 0 | 0 | 0 | 142415 |
| Ethernet | 100.0 | 142415 | 9.4 | 2098984 | 53 k | 0 | 0 | 0 | 142415 |
| Internet Protocol Version 6 | 0.0 | 60 | 0.0 | 2400 | 61 | 0 | 0 | 0 | 60 |
| User Datagram Protocol | 0.0 | 46 | 0.0 | 368 | 9 | 0 | 0 | 0 | 46 |
| Multicast Domain Name System | 0.0 | 40 | 0.0 | 5394 | 137 | 40 | 5394 | 137 | 40 |
| DHCPv6 | 0.0 | 6 | 0.0 | 594 | 15 | 6 | 594 | 15 | 6 |
| Internet Control Message Protocol v6 | 0.0 | 14 | 0.0 | 324 | 8 | 14 | 324 | 8 | 14 |
| Internet Protocol Version 4 | 13.7 | 19550 | 1.7 | 391028 | 9,945 | 0 | 0 | 0 | 19550 |
| User Datagram Protocol | 0.1 | 198 | 0.0 | 1584 | 40 | 0 | 0 | 0 | 198 |
| NetBIOS Name Service | 0.0 | 20 | 0.0 | 1102 | 28 | 20 | 1102 | 28 | 20 |
| NetBIOS Datagram Service | 0.0 | 3 | 0.0 | 549 | 13 | 0 | 0 | 0 | 3 |
| SMB (Server Message Block Protocol) | 0.0 | 3 | 0.0 | 303 | 7 | 0 | 0 | 0 | 3 |
| SMB MailSlot Protocol | 0.0 | 3 | 0.0 | 75 | 1 | 0 | 0 | 0 | 3 |
| Microsoft Windows Browser Protocol | 0.0 | 3 | 0.0 | 45 | 1 | 3 | 45 | 1 | 3 |
| Multicast Domain Name System | 0.0 | 30 | 0.0 | 4542 | 115 | 30 | 4542 | 115 | 30 |
| Dynamic Host Configuration Protocol | 0.0 | 5 | 0.0 | 1500 | 38 | 5 | 1500 | 38 | 5 |
| Dropbox LAN sync Discovery Protocol | 0.0 | 20 | 0.0 | 2300 | 58 | 20 | 2300 | 58 | 20 |
| Domain Name System | 0.1 | 80 | 0.0 | 6069 | 154 | 80 | 6069 | 154 | 80 |
| Transmission Control Protocol | 13.6 | 19342 | 73.4 | 16399012 | 417 k | 15655 | 11894338 | 302 k | 19342 |
| Transport Layer Security | 0.6 | 808 | 2.7 | 603257 | 15 k | 808 | 599145 | 15 k | 811 |
| Hypertext Transfer Protocol | 0.9 | 1274 | 7.5 | 1686594 | 42 k | 1216 | 1625487 | 41 k | 1274 |
| MIME Multipart Media Encapsulation | 0.0 | 2 | 0.0 | 1767 | 44 | 2 | 1767 | 44 | 2 |
| Media Type | 0.0 | 17 | 0.0 | 4322 | 109 | 17 | 4322 | 109 | 17 |
| Malformed Packet | 0.0 | 1 | 0.0 | 0 | 0 | 1 | 0 | 0 | 1 |
| Line-based text data | 0.0 | 11 | 0.0 | 7573 | 192 | 11 | 7573 | 192 | 11 |
| JPEG File Interchange Format | 0.0 | 3 | 0.1 | 12178 | 309 | 3 | 12178 | 309 | 3 |
| JavaScript Object Notation | 0.0 | 1 | 0.0 | 12 | 0 | 1 | 12 | 0 | 1 |
| HTML Form URL Encoded | 0.0 | 14 | 0.1 | 17314 | 440 | 14 | 17314 | 440 | 14 |
| Compuserve GIF | 0.0 | 9 | 0.0 | 2734 | 69 | 9 | 2734 | 69 | 9 |
| FTP Data | 0.0 | 7 | 0.0 | 9464 | 240 | 7 | 9464 | 240 | 7 |
| File Transfer Protocol (FTP) | 0.0 | 22 | 0.0 | 656 | 16 | 22 | 656 | 16 | 22 |
| Internet Group Management Protocol | 0.0 | 7 | 0.0 | 56 | 1 | 7 | 56 | 1 | 7 |
| Internet Control Message Protocol | 0.0 | 3 | 0.0 | 120 | 3 | 0 | 0 | 0 | 3 |
| Data | 1.2 | 1733 | 9.7 | 2175402 | 55 k | 1733 | 2175402 | 55 k | 1733 |
| Address Resolution Protocol | 86.2 | 122691 | 15.8 | 3540522 | 90 k | 122691 | 3540522 | 90 k | 122691 |

| File Transfer Protocol (FTP) | 0.0 | 22 | 0.0 | 656 | 16 | 22 | 656 | 16 | 22 |
|---|---|---|---|---|---|---|---|---|---|
| Internet Group Management Protocol | 0.0 | 7 | 0.0 | 56 | 1 | 7 | 56 | 1 | 7 |
| Internet Control Message Protocol | 0.0 | 3 | 0.0 | 120 | 3 | 0 | 0 | 0 | 3 |
| Data | 1.2 | 1733 | 9.7 | 2175402 | 55 k | 1733 | 2175402 | 55 k | 1733 |
| Address Resolution Protocol | 86.2 | 122691 | 15.8 | 3540522 | 90 k | 122691 | 3540522 | 90 k | 122691 |

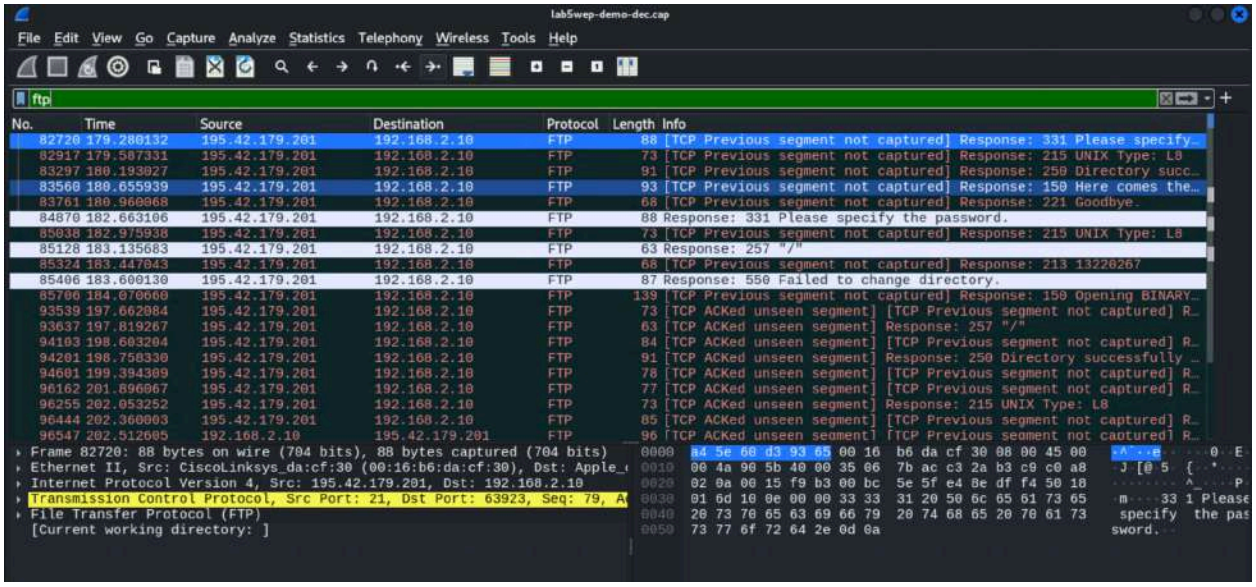
I went to statistics and pressed the option protocol Hierarchy so I could see this screen.

Protocol showing HTTP (Hypertext transfer protocol 1274 packets, 7.5 bytes) and FTP (file transfer protocol 22 packets, 656 bytes) my apologies for not pointing at them with a red marker or something, typing it out simplified it for me.




Highlighted in blue to show what I surveyed. Its source, destination, and length info. I will do the same for ftp.

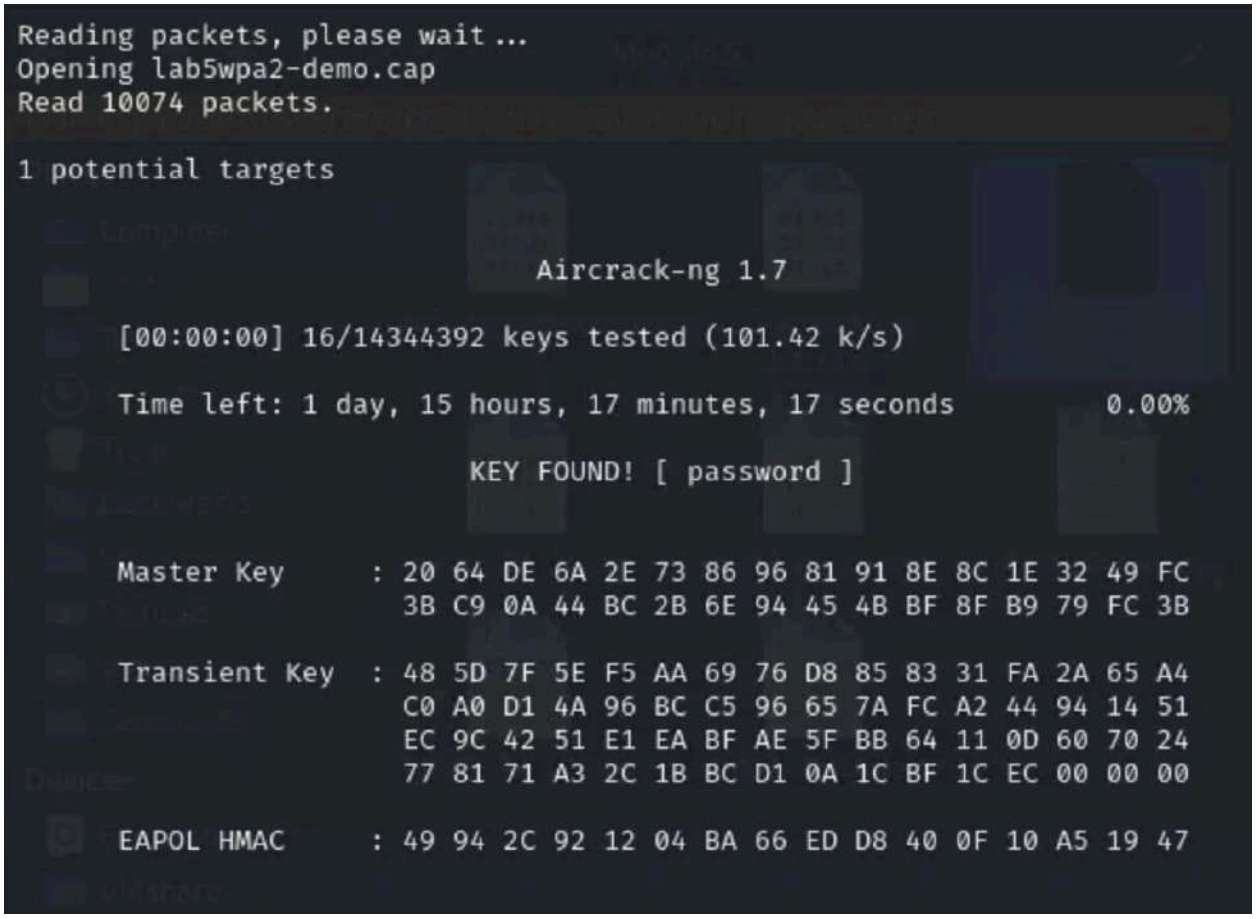
| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs |
|---|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 22 | 100.0 | 1844 | 626 | 0 | 0 | 0 | 22 |
| Ethernet | 100.0 | 22 | 16.7 | 308 | 104 | 0 | 0 | 0 | 22 |
| Internet Protocol Version 4 | 100.0 | 22 | 23.9 | 440 | 149 | 0 | 0 | 0 | 22 |
| Transmission Control Protocol | 100.0 | 22 | 59.4 | 1096 | 372 | 0 | 0 | 0 | 22 |
| File Transfer Protocol (FTP) | 100.0 | 22 | 35.6 | 656 | 222 | 22 | 656 | 222 | 22 |



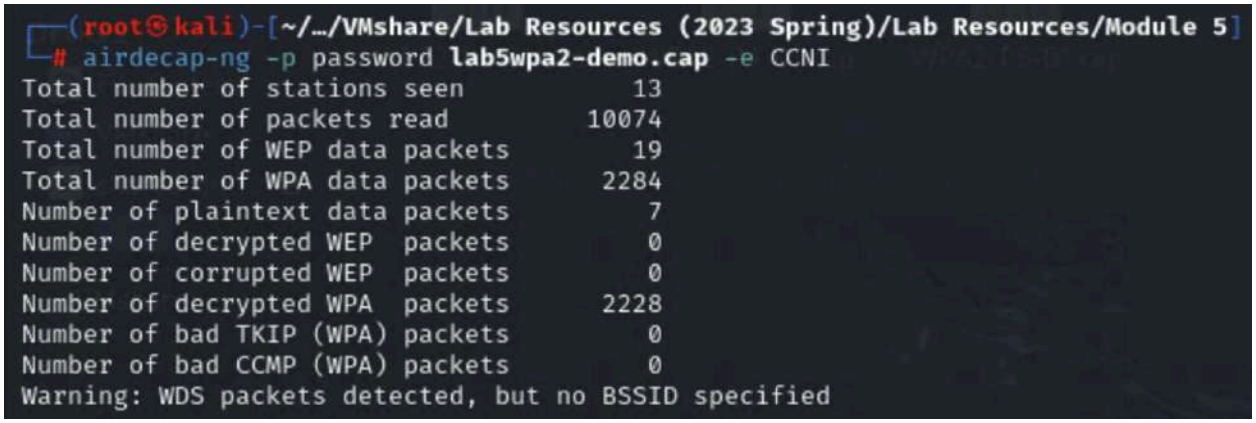

***Now repeat these same steps with the Lab5 Wpa2 file.***

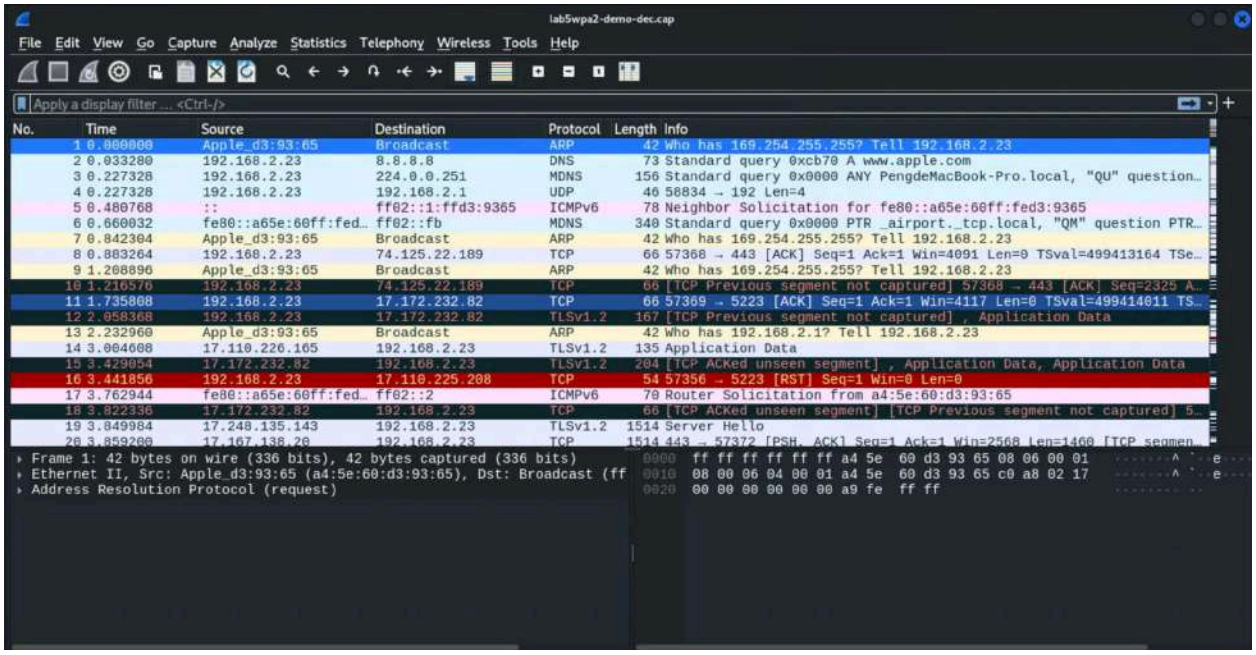
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng lab5wpa2-demo.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (0 IVs)
   2  58:BF:EA:FA:38:B0                            Unknown
   3  58:BF:EA:FA:3B:A0                            Unknown
   4  98:FC:11:7C:D0:C7  CCNI                      WPA (1 handshake)
   5  F4:7F:35:04:7D:E0                            Unknown
   6  F4:7F:35:39:0A:A0  AccessODU                 Unknown
   7  F4:7F:35:39:0A:A1                            Unknown
   8  F4:7F:35:39:0A:A2  MonarchODU                Unknown
   9  F4:7F:35:39:0A:A4  eduroam                   Unknown

Index number of target network ? 4
```

So i used the same command as earlier with aircrack-ng and this time I used the lab5wpa2 demo cap file.

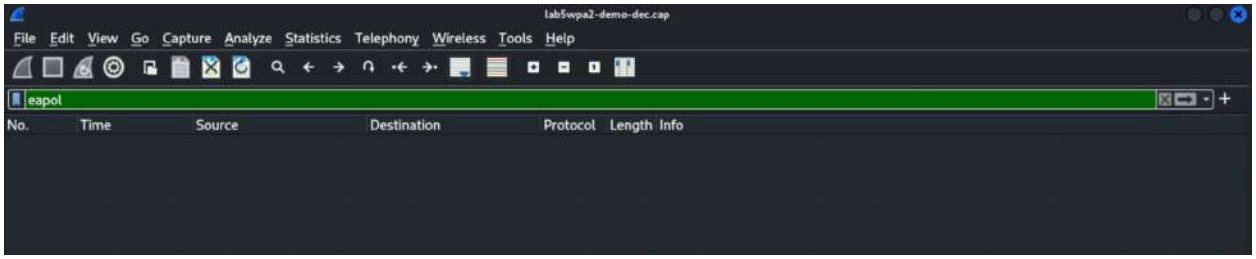



Key was found: Password



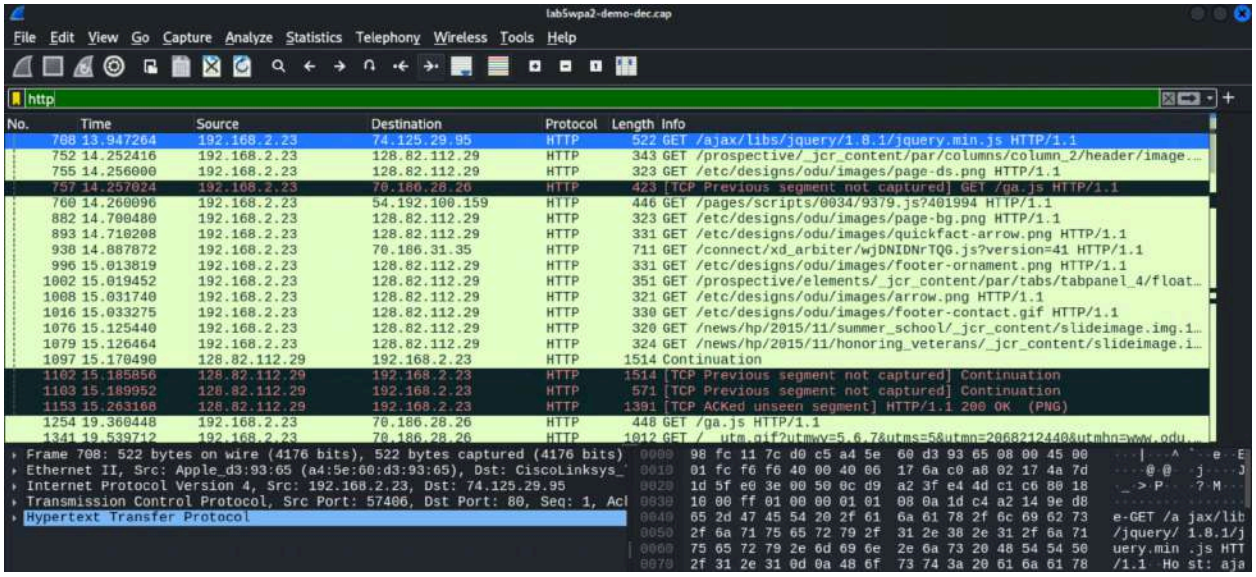



Opened up the decrypted file using wireshark . lab5wpa2 dec

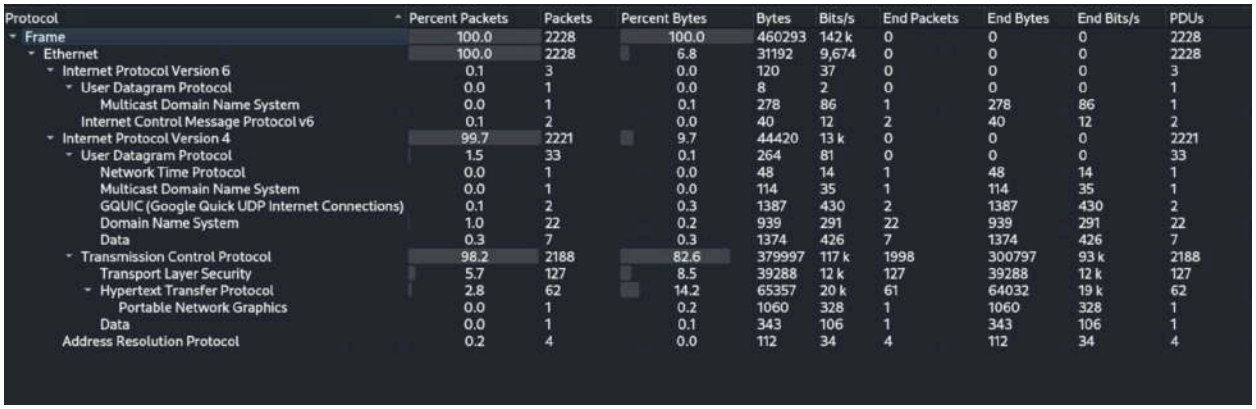




No results for the eapol filter, i went to the statistics tab and pressed on the protocol hierarchy option and was able to get the second screen that you see with no results. (all within wireshark)




Results appeared using the http filter



| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs |
|---|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 2228 | 100.0 | 460293 | 142 k | 0 | 0 | 0 | 2228 |
| Ethernet | 100.0 | 2228 | 6.8 | 31192 | 9,674 | 0 | 0 | 0 | 2228 |
| Internet Protocol Version 6 | 0.1 | 3 | 0.0 | 120 | 37 | 0 | 0 | 0 | 3 |
| User Datagram Protocol | 0.0 | 1 | 0.0 | 8 | 2 | 0 | 0 | 0 | 1 |
| Multicast Domain Name System | 0.0 | 1 | 0.1 | 278 | 86 | 1 | 278 | 86 | 1 |
| Internet Control Message Protocol v6 | 0.1 | 2 | 0.0 | 40 | 12 | 2 | 40 | 12 | 2 |
| Internet Protocol Version 4 | 99.7 | 2221 | 9.7 | 44420 | 13 k | 0 | 0 | 0 | 2221 |
| User Datagram Protocol | 1.5 | 33 | 0.1 | 264 | 81 | 0 | 0 | 0 | 33 |
| Network Time Protocol | 0.0 | 1 | 0.0 | 48 | 14 | 1 | 48 | 14 | 1 |
| Multicast Domain Name System | 0.0 | 1 | 0.0 | 114 | 35 | 1 | 114 | 35 | 1 |
| GQUIC (Google Quick UDP Internet Connections) | 0.1 | 2 | 0.3 | 1387 | 430 | 2 | 1387 | 430 | 2 |
| Domain Name System | 1.0 | 22 | 0.2 | 939 | 291 | 22 | 939 | 291 | 22 |
| Data | 0.3 | 7 | 0.3 | 1374 | 426 | 7 | 1374 | 426 | 7 |
| Transmission Control Protocol | 98.2 | 2188 | 82.6 | 379997 | 117 k | 1998 | 300797 | 93 k | 2188 |
| Transport Layer Security | 5.7 | 127 | 8.5 | 39288 | 12 k | 127 | 39288 | 12 k | 127 |
| Hypertext Transfer Protocol | 2.8 | 62 | 14.2 | 65357 | 20 k | 61 | 64032 | 19 k | 62 |
| Portable Network Graphics | 0.0 | 1 | 0.2 | 1060 | 328 | 1 | 1060 | 328 | 1 |
| Data | 0.0 | 1 | 0.1 | 343 | 106 | 1 | 343 | 106 | 1 |
| Address Resolution Protocol | 0.2 | 4 | 0.0 | 112 | 34 | 4 | 112 | 34 | 4 |

These were the general results without using any filters in the wireshark. This screen is from clicking the statistics tab and pressing on protocol hierarchy option.

Task D: 30 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 svatsa is 8. Thus, I should pick up the file "WPA2-P3-01.cap." You can find an online MD5 hash generator or the following command to get the hash of a text string

The above files are in a folder named "Lab Resources (2023 Spring)." You can locate the folder in your VMshare in any Kali Linux VM.

• Please make sure to follow the steps mentioned in the Module 6 Lab manual and find the assigned WPA file under the sub-folder "Module 5.

**Now, complete the following steps:**

1. Implement a dictionary attack and decrypt the traffic. - 20 points

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -10 points

I am going to put the screenshots of what I do and leave all the questions at the top.


Last digit is 2 in my md5. WPA2-P1-01.cap is the file I will be using based on the requirements for this part.


Key found: Password

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng WPA2-P1-01.cap
Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

1 potential targets

Please specify a dictionary (option -w).
```

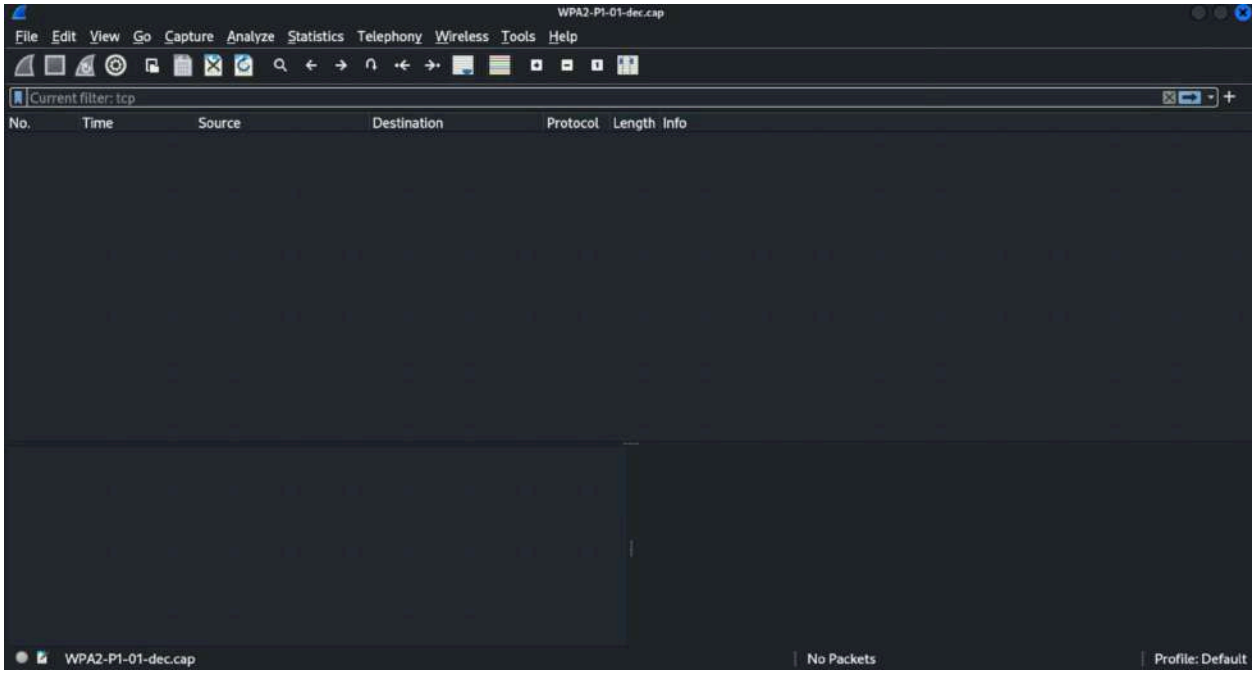
ESSID: CyberPHY

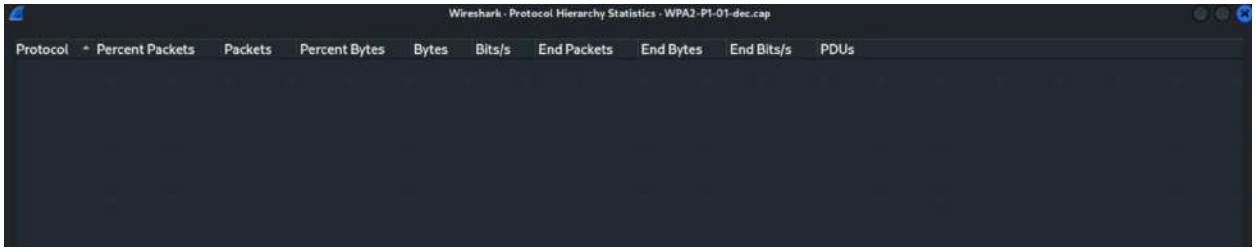
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -p password WPA2-P1-01.cap -e CyberPHY
Total number of stations seen            12
Total number of packets read           2660
Total number of WEP data packets          0
Total number of WPA data packets        629
Number of plaintext data packets          0
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets          0
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
```

WPA data packets 629

Number of packets read 2660

Stations seen 12




Regardless of filter I was not able to find anything within this file. Maybe i did something incorrectly but i am not seeing anything for any type of filter. Tcp, dns, ftp, http nothing shows up.

Traffic analysis- WPA2-P1-01.cap

After performing the dictionary attack on the file I needed for this part of the lab using rockyou.txt I was able to find the password for the cypherphy network (password) then using airdecap the wpa data packets were decrypted. When I went into wireshark however, i seen that there was nothing within the save file

even after using multiple different filters to make sure that I was not doing anything wrong i could not find anything I used ftp, tcp, dns, and http and was unable to find any active packets. I am sure that this may be the wrong-doing on my side of messing up earlier within the process but I am also confident that i carried out my part correctly.