

Assignment 6: Wi-Fi Password Cracking

Jessiah Davis

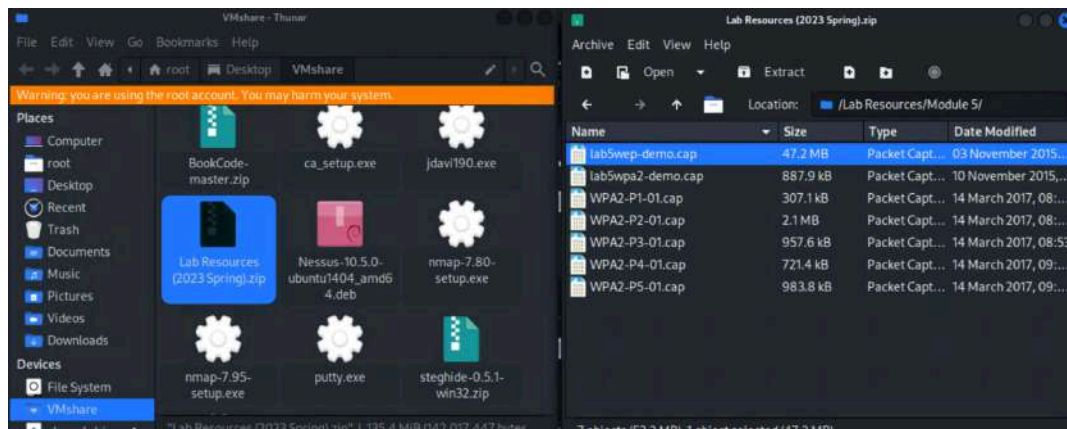
Old Dominion University

Cyse301

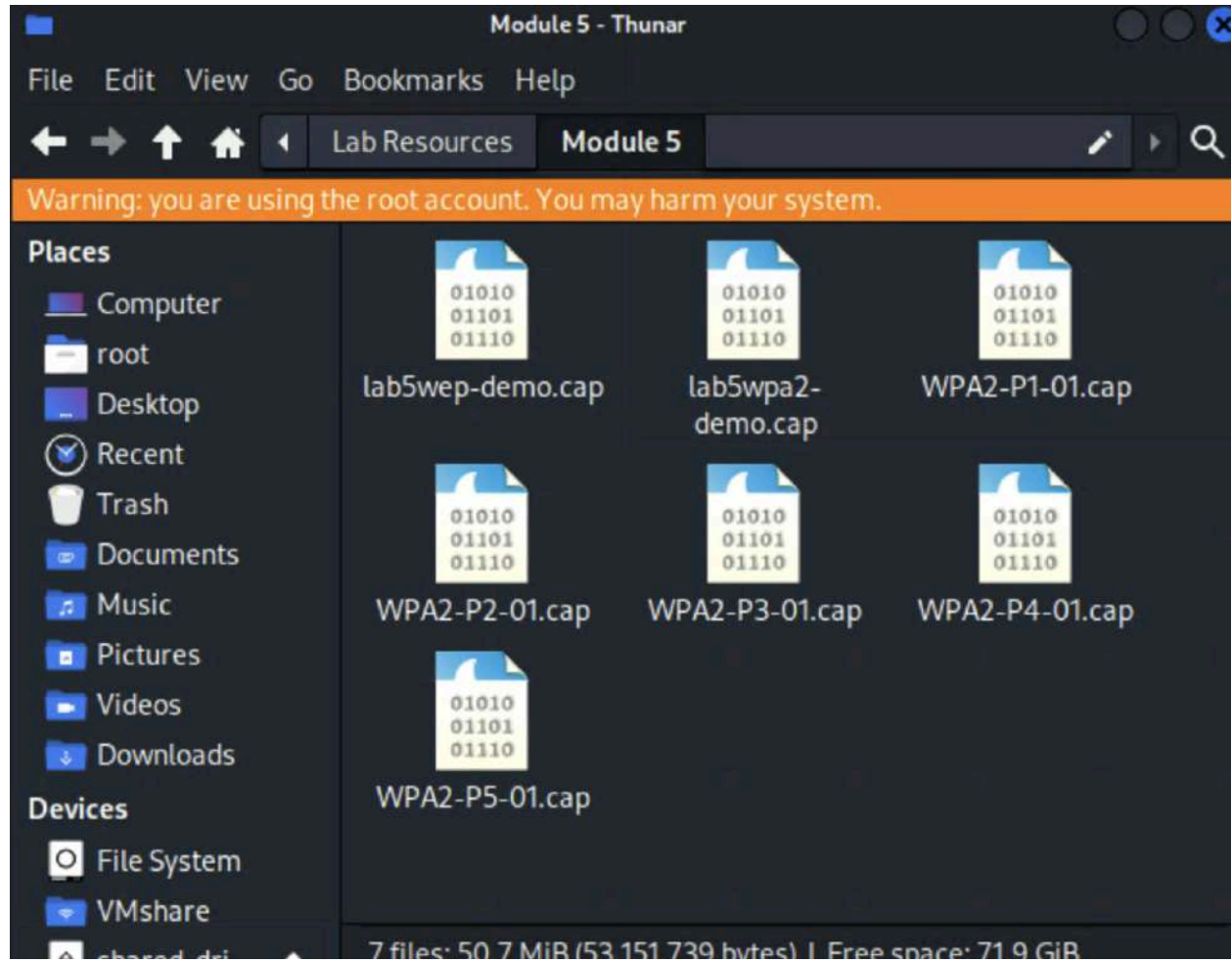
Task C: 20 points

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.



```
(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap  WPA2-P1-01.cap  WPA2-P3-01.cap  WPA2-P5-01.cap
lab5wpa2-demo.cap  WPA2-P2-01.cap  WPA2-P4-01.cap
(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─#
```

```
(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# aircrack-ng lab5wep-demo.cap
Reading packets, please wait ...
Opening lab5wep-demo.cap
Read 404693 packets.
```

#	BSSID	ESSID	Encryption
1	00:16:B6:DA:CF:32	ccni-test	WEP (19772 IVs)
2	00:25:84:FD:66:00		Unknown
3	00:25:84:FD:66:03		Unknown
4	02:21:F1:A6:B0:A0	hpsetup	Unknown
5	04:DA:D2:82:92:D1		Unknown
6	18:9C:5D:EF:46:70		Unknown
7	18:9C:5D:EF:48:50		Unknown
8	18:9C:5D:EF:4D:A0		Unknown
9	58:BF:EA:0F:F9:00		Unknown
10	58:BF:EA:0F:F9:01		Unknown
11	58:BF:EA:24:98:91		WPA (0 handshake)
12	58:BF:EA:FA:16:10		Unknown
13	58:BF:EA:FA:38:B0		Unknown
14	58:BF:EA:FA:3B:A0		Unknown
15	58:BF:EA:FA:38:A2	MonarchODU	WPA (0 handshake)
16	5C:50:15:E7:FE:42	MonarchODU	EAPOL+WPA (0 handshake)
17	98:FC:11:7C:CE:63	dd-wrt	Unknown
18	98:FC:11:7C:D0:C7	CCNI	WPA (0 handshake)
19	F4:7F:35:04:01:A0		Unknown
20	F4:7F:35:04:08:20		Unknown
21	F4:7F:35:04:65:A0		Unknown
22	F4:7F:35:04:7D:E0	AccessODU	Unknown
23	F4:7F:35:04:7D:E1		Unknown
24	F4:7F:35:04:7D:E2	MonarchODU	WPA (0 handshake)
25	F4:7F:35:04:7D:E4	eduroam	Unknown
26	F4:7F:35:39:0A:A0		Unknown
27	F4:7F:35:42:0E:C2		Unknown

```
Index number of target network ? █
```

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

```

Index number of target network ? 1
Reading packets, please wait ...
Opening lab5wep-demo.cap
Read 404693 packets.

1 potential targets
Attack will be restarted every 5000 captured ivs.

Aircrack-ng 1.7

[00:00:02] Tested 231 keys (got 19772 IVs)

KB  depth  byte(vote)
0   0/ 2    F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064) 84(24064) 9A(24064) 86(24064) 29(23552)
1   9/ 10   C7(24064) 71(23808) 5C(23552) 28(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040) 5B(22784) 62(22784) 8A(22784) E8(22784)
2   0/ 1    BB(30208) AB(25344) BF(25344) D8(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808) 1C(23552) 4E(23552) ED(23552) 98(23296)
3   8/ 12   FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296) 2C(23040) 3C(23040) 3E(23040) BA(23040)
4   0/ 1    B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576) FF(24576) 69(24064) 6D(24064) 49(23552)

KEY FOUND! [ F2:C7:BB:35:B9 ]
Decrypted correctly: 100%

```

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

```

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen          37
Total number of packets read          404693
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
Warning: WDS packets detected, but no BSSID specified

```

Wireshark - Protocol Hierarchy Statistics - lab5wep-demo-dec.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
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
- 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.

The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The packet list pane is highlighted in blue, showing a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 28) is highlighted in blue. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
28	5.452701	192.168.2.10	164.106.251.250	HTTP	551	GET /docs/netser/DC13ATM.jpg HTTP/1.1
5339	47.071295	192.168.2.10	112.90.86.16	HTTP	527	POST /QUERYVERSIONUPDATE HTTP/1.1
5480	47.316483	112.90.86.16	192.168.2.10	HTTP	455	HTTP/1.1 200 OK
10092	54.874564	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
10112	55.049155	103.7.30.143	192.168.2.10	HTTP	644	HTTP/1.1 200 OK (text/octet)
10414	55.559717	192.168.2.10	103.7.30.143	HTTP	352	POST /cgi-bin/httpconn HTTP/1.1
10424	55.565828	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
10636	55.883267	103.7.30.143	192.168.2.10	HTTP	1404	[TCP Previous segment not captured] Continuation
10856	56.232965	103.7.30.143	192.168.2.10	HTTP	396	HTTP/1.1 200 OK (text/octet)
10904	56.409157	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
12227	58.519781	192.168.2.10	103.7.30.143	HTTP	349	[TCP Previous segment not captured] Continuation
12522	59.005157	192.168.2.10	103.7.30.143	HTTP	523	[TCP ACKed unseen segment] POST /cgi-bin/httpconn HTTP/1.1
13479	60.563267	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
13761	60.988227	103.7.30.143	192.168.2.10	HTTP	588	[TCP ACKed unseen segment] HTTP/1.1 200 OK (text/octet)
14214	61.687683	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
14442	62.026601	192.168.2.10	103.7.30.143	HTTP	328	[TCP Previous segment not captured] Continuation
14500	62.119845	192.168.2.10	103.7.30.143	HTTP	352	POST /cgi-bin/httpconn HTTP/1.1
14630	62.324164	103.7.30.143	192.168.2.10	HTTP	377	HTTP/1.1 200 OK (text/octet)
14799	62.588901	192.168.2.10	103.7.30.143	HTTP	328	POST /cgi-bin/httpconn HTTP/1.1
14854	62.665701	192.168.2.10	103.7.30.143	HTTP	352	POST /cgi-bin/httpconn HTTP/1.1

Frame 28: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface 0
 Ethernet II, Src: Apple_d3:93:65 (a4:5e:60:d3:93:65), Dst: CiscoLinksys_... (08:00:0c:29:00:00)
 Internet Protocol Version 4, Src: 192.168.2.10, Dst: 164.106.251.250
 Transmission Control Protocol, Src Port: 63789, Dst Port: 80, Seq: 1, Acl...
 Hypertext Transfer Protocol

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

```

lab5wep-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp
No. Time Source Destination Protocol Length Info
82728 179.288132 195.42.179.201 192.168.2.10 FTP 88 [TCP Previous segment not captured] Response: 331 Please specify
82917 179.587331 195.42.179.201 192.168.2.10 FTP 73 [TCP Previous segment not captured] Response: 215 UNIX Type: L8
83297 180.193027 195.42.179.201 192.168.2.10 FTP 91 [TCP Previous segment not captured] Response: 250 Directory succ...
83568 180.655939 195.42.179.201 192.168.2.10 FTP 93 [TCP Previous segment not captured] Response: 150 Here comes the...
83761 180.968968 195.42.179.201 192.168.2.10 FTP 68 [TCP Previous segment not captured] Response: 221 Goodbye.
84876 182.663166 195.42.179.201 192.168.2.10 FTP 88 Response: 331 Please specify the password.
85038 182.975938 195.42.179.201 192.168.2.10 FTP 73 [TCP Previous segment not captured] Response: 215 UNIX Type: L8
85128 183.135683 195.42.179.201 192.168.2.10 FTP 63 Response: 257 "/"
85324 183.447843 195.42.179.201 192.168.2.10 FTP 68 [TCP Previous segment not captured] Response: 213 13228267
85406 183.609130 195.42.179.201 192.168.2.10 FTP 87 Response: 550 Failed to change directory.
85700 184.070660 195.42.179.201 192.168.2.10 FTP 139 [TCP Previous segment not captured] Response: 150 Opening BINARY
93539 197.662884 195.42.179.201 192.168.2.10 FTP 73 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
93637 197.819267 195.42.179.201 192.168.2.10 FTP 63 [TCP ACKed unseen segment] Response: 257 "/"
94193 198.603204 195.42.179.201 192.168.2.10 FTP 84 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
94201 198.758330 195.42.179.201 192.168.2.10 FTP 91 [TCP ACKed unseen segment] Response: 250 Directory successfully ...
94601 199.394309 195.42.179.201 192.168.2.10 FTP 78 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
96162 201.696967 195.42.179.201 192.168.2.10 FTP 77 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
96255 202.053252 195.42.179.201 192.168.2.10 FTP 73 [TCP ACKed unseen segment] Response: 215 UNIX Type: L8
96444 202.360093 195.42.179.201 192.168.2.10 FTP 85 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
96547 202.512065 192.168.2.10 195.42.179.201 FTP 96 [TCP ACKed unseen segment] [TCP Previous segment not captured] R...
Frame 82728: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on 0
Ethernet II, Src: CiscoLinksys_da:cf:30 (00:16:b0:da:cf:30), Dst: Apple...
Internet Protocol Version 4, Src: 195.42.179.201, Dst: 192.168.2.10
Transmission Control Protocol, Src Port: 21, Dst Port: 63923, Seq: 79, A...
File Transfer Protocol (FTP)
[Current working directory: ]

```

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.

```

Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:00] 16/14344392 keys tested (101.42 k/s)

Time left: 1 day, 15 hours, 17 minutes, 17 seconds      0.00%

KEY FOUND! [ password ]

Master Key      : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
                  3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B

Transient Key   : 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA 2A 65 A4
                  C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44 94 14 51
                  EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D 60 70 24
                  77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00

EAPOL HMAC     : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47

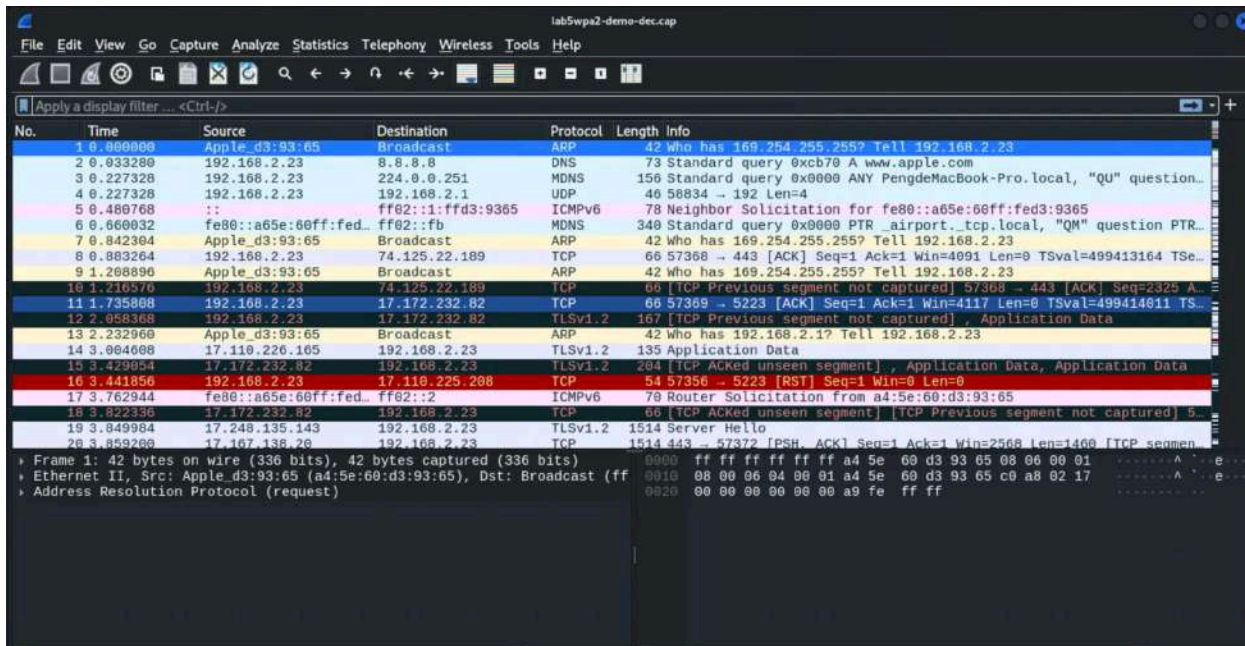
```

Key was found: Password

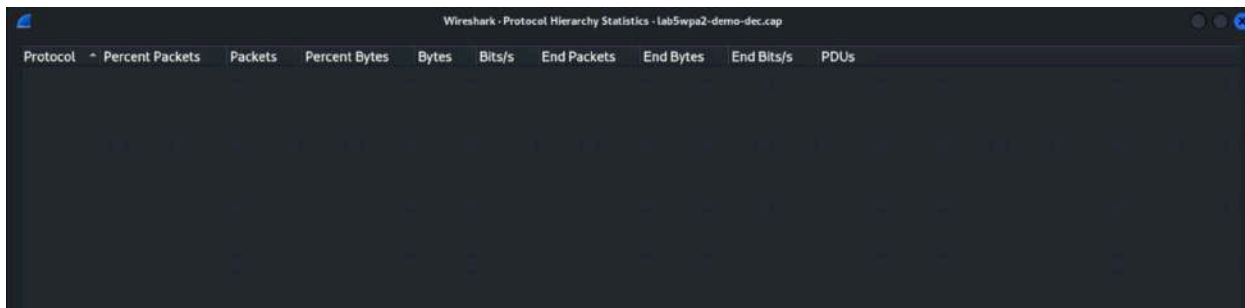
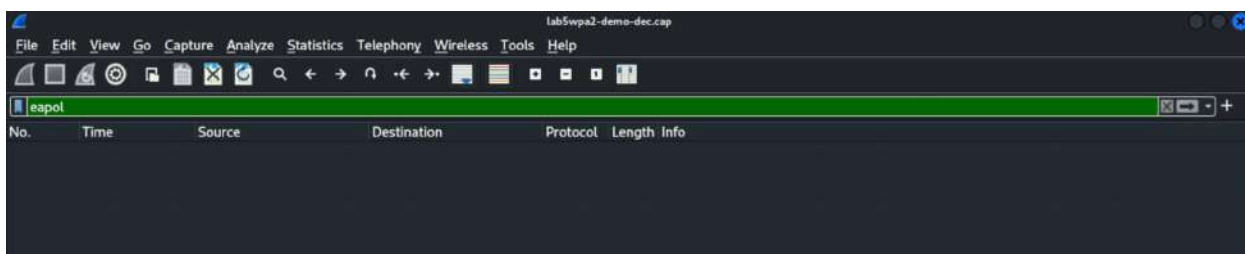
```

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen      13
Total number of packets read      10074
Total number of WEP data packets   19
Total number of WPA data packets  2284
Number of plaintext data packets   7
Number of decrypted WEP packets    0
Number of corrupted WEP packets    0
Number of decrypted WPA packets   2228
Number of bad TKIP (WPA) packets   0
Number of bad CCMP (WPA) packets   0
Warning: WDS packets detected, but no BSSID specified

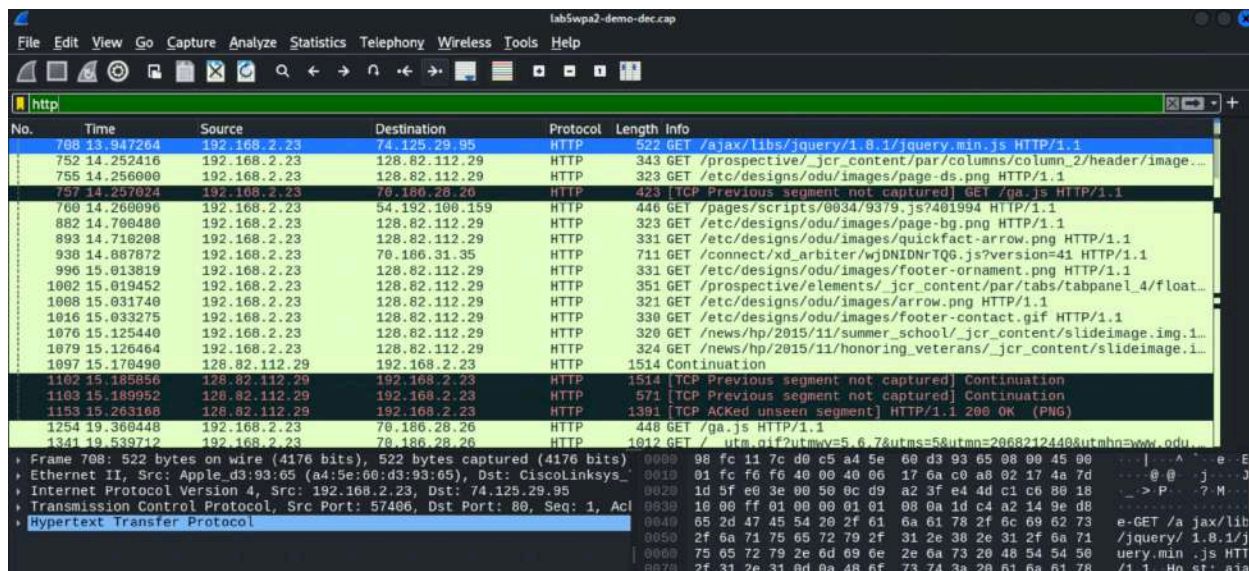
```



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	PDU/s
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	444220	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.

```
(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module  
5]  
└─# echo -n jdavi190 | md5sum  
49eb04756ceec8ae4de05c3c14998a52 -
```

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.

```

(root@kali)-[~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# aircrack-ng WPA2-P1-01.cap -w /usr/share/wordlists/rockyou.txt
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

Devices:
Aircrack-ng 1.7

[00:00:00] 995/10303727 keys tested (2359.53 k/s)

Time left: 1 hour, 12 minutes, 46 seconds      0.01%

KEY FOUND! [ PASSWORD ]

Master Key      : F1 5F 48 C3 DC 4B E3 2A BE 2E 2D 87 FB 98 28 89
                  30 BC 6F 72 60 96 04 86 46 54 84 B6 24 11 B8 56

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29

```

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).
```

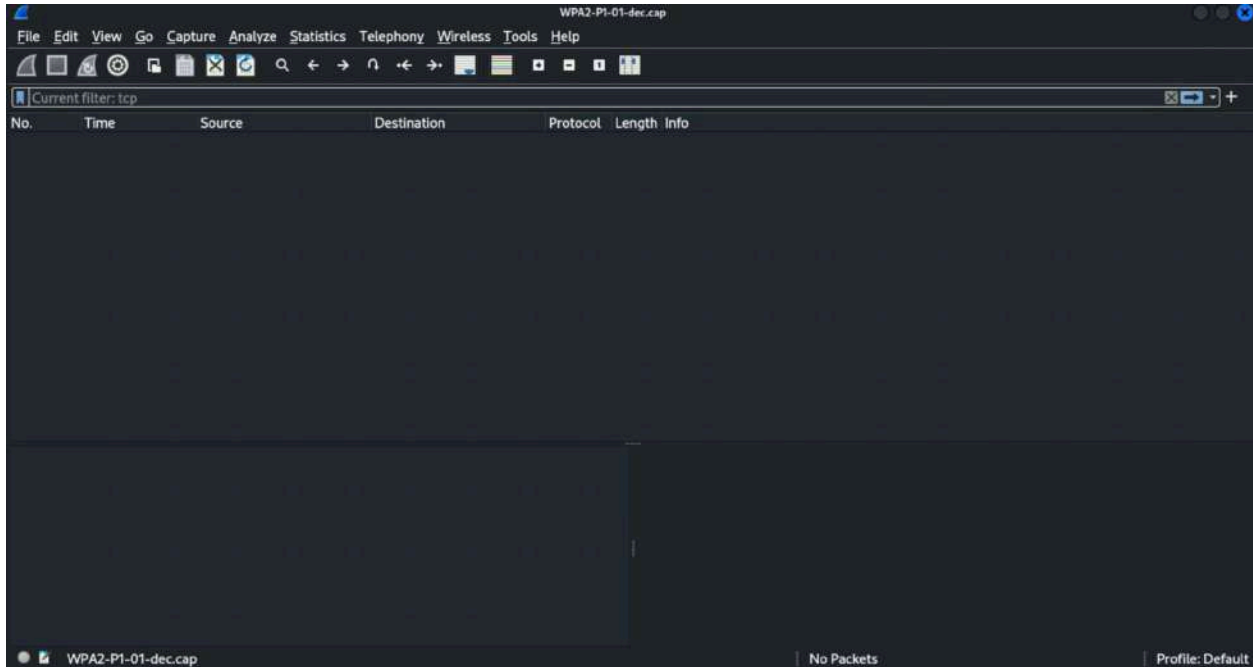
ESSID: CyberPHY

```
(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.