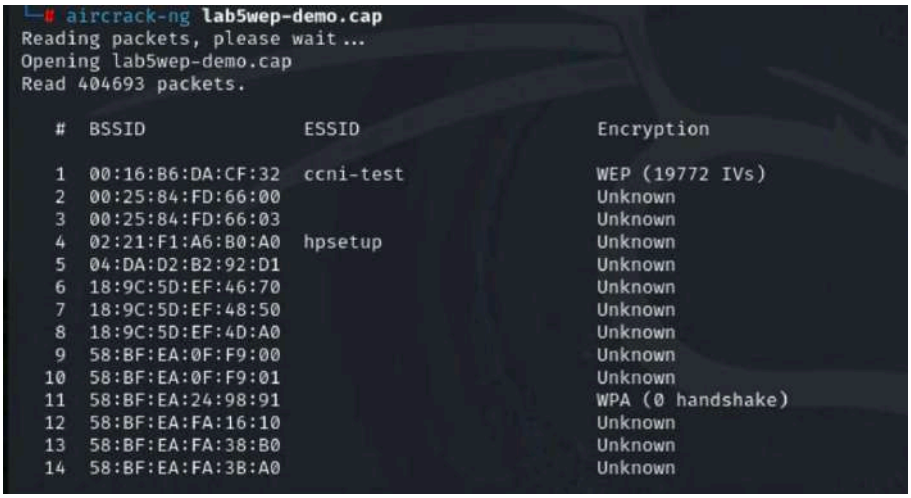
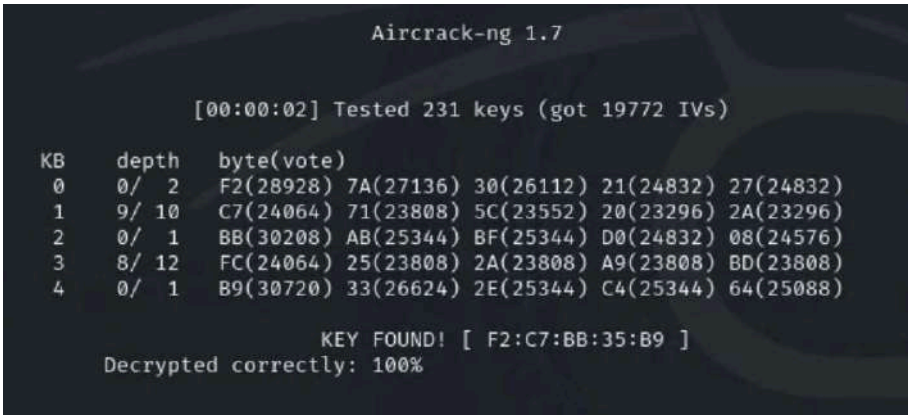
CYSE 301 Assignment 6

Derek D. Hillman
UIN:00861968

Task C

Step 1.) I decrypted the lab 5 file and performed an analysis of the traffic. Since it had WEP security I did not need to use a dictionary attack. There were 142415 packets in the capture. After following the UDP stream I see there were DNS queries to itunes.apple.com coming from the mobile device. From analyzing the http stream, I found the device to be a Macintosh Intel Mac OS X 10_11_1. I gathered this information from the user agent string by using the filter tcp.stream eq 11. The gateway router was a Cisco Linksys router with the mac of da:cf:30





Derek D. Hillman
UIN:00861968

```
┌──(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
```

Step 2.) I executed aircrack-ng on the lab5wpanfile to examine the traffic to find the Wi-Fi networks captured. I utilized a dictionary attack by using the rockyou.txt I copied from the kali Linux system. I was able to obtain the password to then decrypt the files. After analyzing the udp stream I see that a device is the ip address of www.apple.com. The packet capture of this shows a MacBook using Mozilla/5.0 accessing an image at www.odu.edu. I am assuming it's a student because of the login portion of the Odu site string.

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

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (19 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

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

1 potential targets
```

CYSE 301 Assignment 6

Derek D. Hillman
UIN:00861968

```
                    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)
  1    9/ 10   C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296)
  2    0/  1   BB(30208) AB(25344) BF(25344) D0(24832) 08(24576)
  3    8/ 12   FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808)
  4    0/  1   B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088)

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

Task D

Step 1.) I obtained my hash value from the command given in the assignments

```
5]
└─# echo -n dhill036 | md5sum
7ed597a2375aae7ab0d564d1e560b6bf  -
```

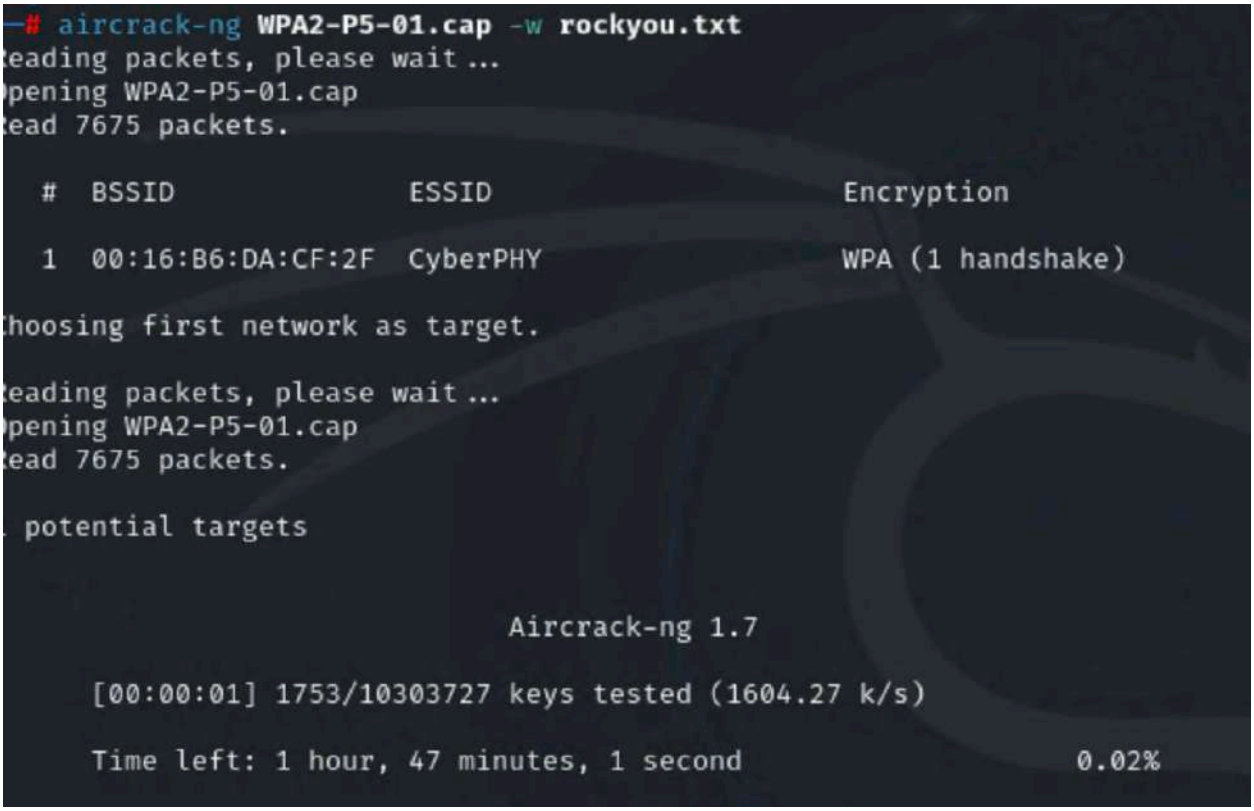
Step 2.) I executed the aircrack-mg command on the file that pertained to the last value of my MIDAS hash.

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# aircrack-ng WPA2-P5-01.cap
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 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-P5-01.cap
Read 7675 packets.

1 potential targets

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

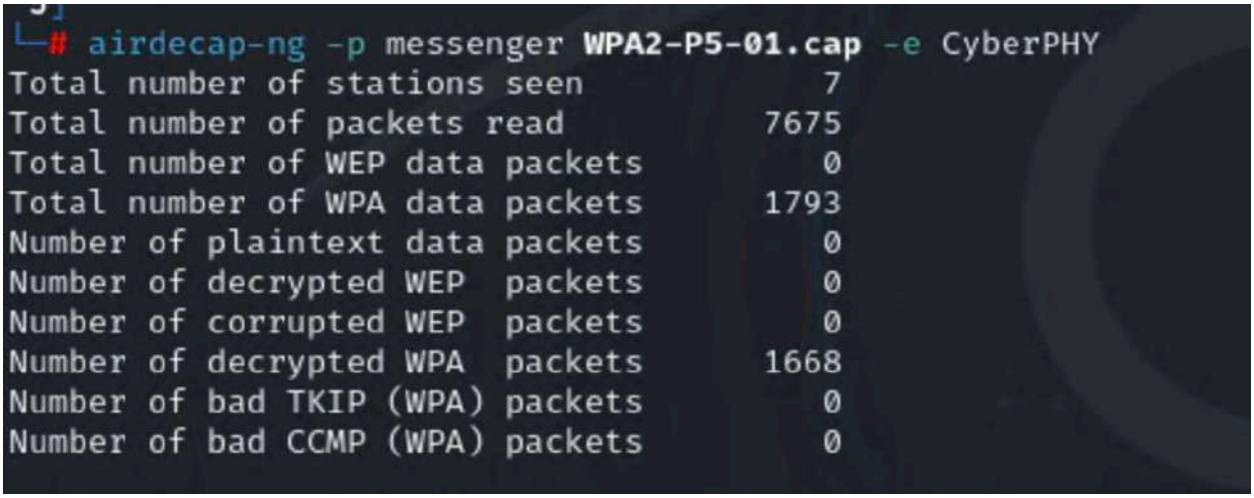
CYSE 301 Assignment 6

Derek D. Hillman
UIN:00861968

Step 3.) I obtained the password “messenger” and then executed the dictionary attack.



Step 4.) once I obtained the password, I decrypted it with airdecap-ng Step



Step 5.) I opened the files in wireshark and analyzed the files as requested. After looking through the files I see that there are arp broadcast coming from a Cisco Linksys router to a Huawei Techno device. Huawei is a Chinese smart phone manufacturer. When filtering for http packets I see that the device was trying to gain access to

CYSE 301 Assignment 6

Derek D. Hillman
UIN:00861968

www.taobao.com.