WAYNE STATE UNIVERSITY

COLLEGE OF ENGINEERING

CSC 5991 Cyber Security Practice

Lab 7: Wireless Exploitation & Defenses

Introduction

In this lab students will explore ways to perform wireless attacks and understand potential defenses. The attacks that will be covered are inspecting & modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WPA2 protected networks.

Software Requirements

All required files are packed and configured in the provided virtual machine image.

- The VMWare Software
  http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The Kali Linux, Penetration Testing Distribution
  https://www.kali.org/downloads/

- Wireshark: Network protocol analyzer
  https://www.wireshark.org/#download

- Aircrack- ng: a suite of tools to assess WiFi network security
  http://aircrack-ng.en.softonic.com/

Setup an Access Point

In this lab, we use a TP-LINK Wireless N300 Home Router. Next, it explains the basic steps to setup the access point's Service Set Identifier (SSID) and security mechanism. If you have done this before, skip this section. Figure below shows a TP-LINK Wireless N300 Home Router that we are using in the classroom.

Step 1: Connect your laptop or desktop to a router.

This step depends on routers. Some routers require using Ethernet cable to physical connect the router. Some other routers may be able to connect via wireless using its Service Set Identifier (SSID). For the router that we are using in the classroom need to physically connect to one of the router's LAN ports. (Note: Think about the security implications for these two types of routers.)

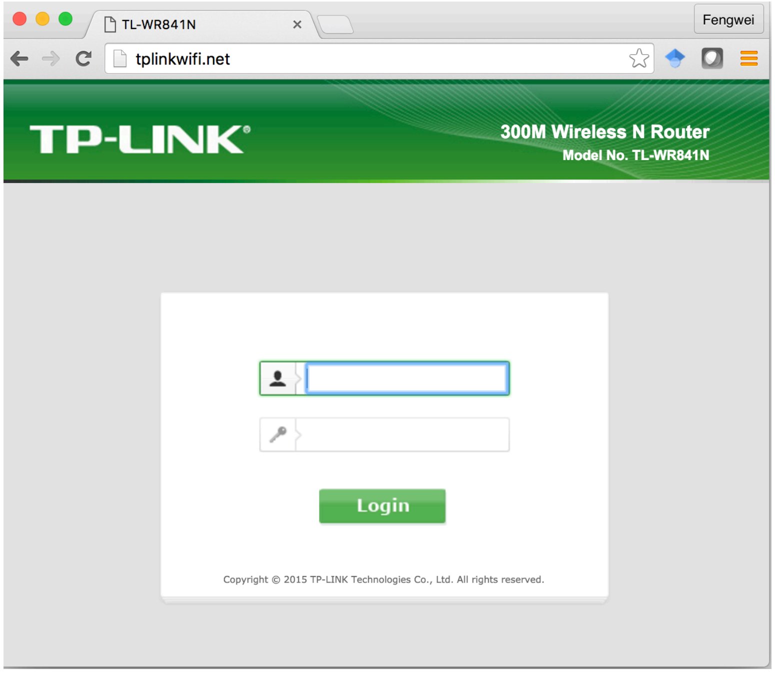
Step 2: Open the web-based setup page

Open a web browser, and type the login IP or hostname in the address field to log in the web-based management page. Normally, you can find the IP address or the hostname from the back of the router. The IP address for our router is 192.168.1.1, and hostname is http://www.tplinkwifi.net

Step 3: Enter the username and password to login

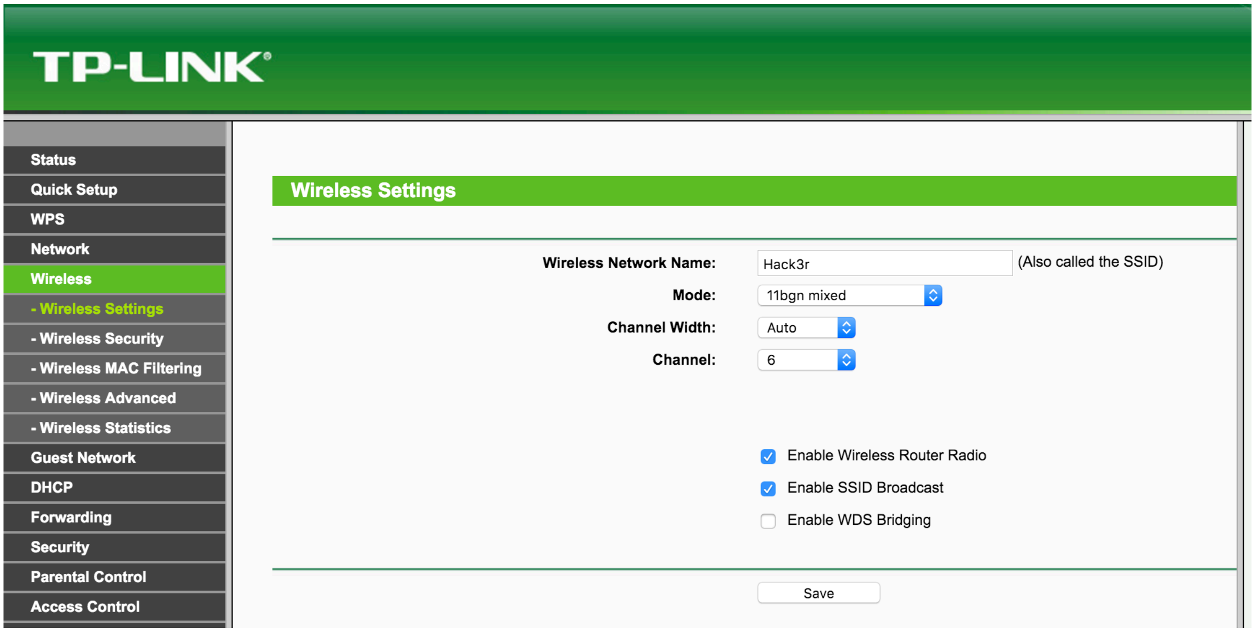
Enter the default username and password to login. For our router, its default username and password are admin and admin.

Figure below shows the login page of the router that we are using.



Step 4: Configure the SSID

In our router, go to Wireless -> Wireless settings. Here you can rename your wireless network (i.e., SSID). The SSID for our router is "Hack3r"



Wireless Settings

Wireless Network Name: Hack3r (Also called the SSID)

Mode: 11bgn mixed

Channel Width: Auto

Channel: 6

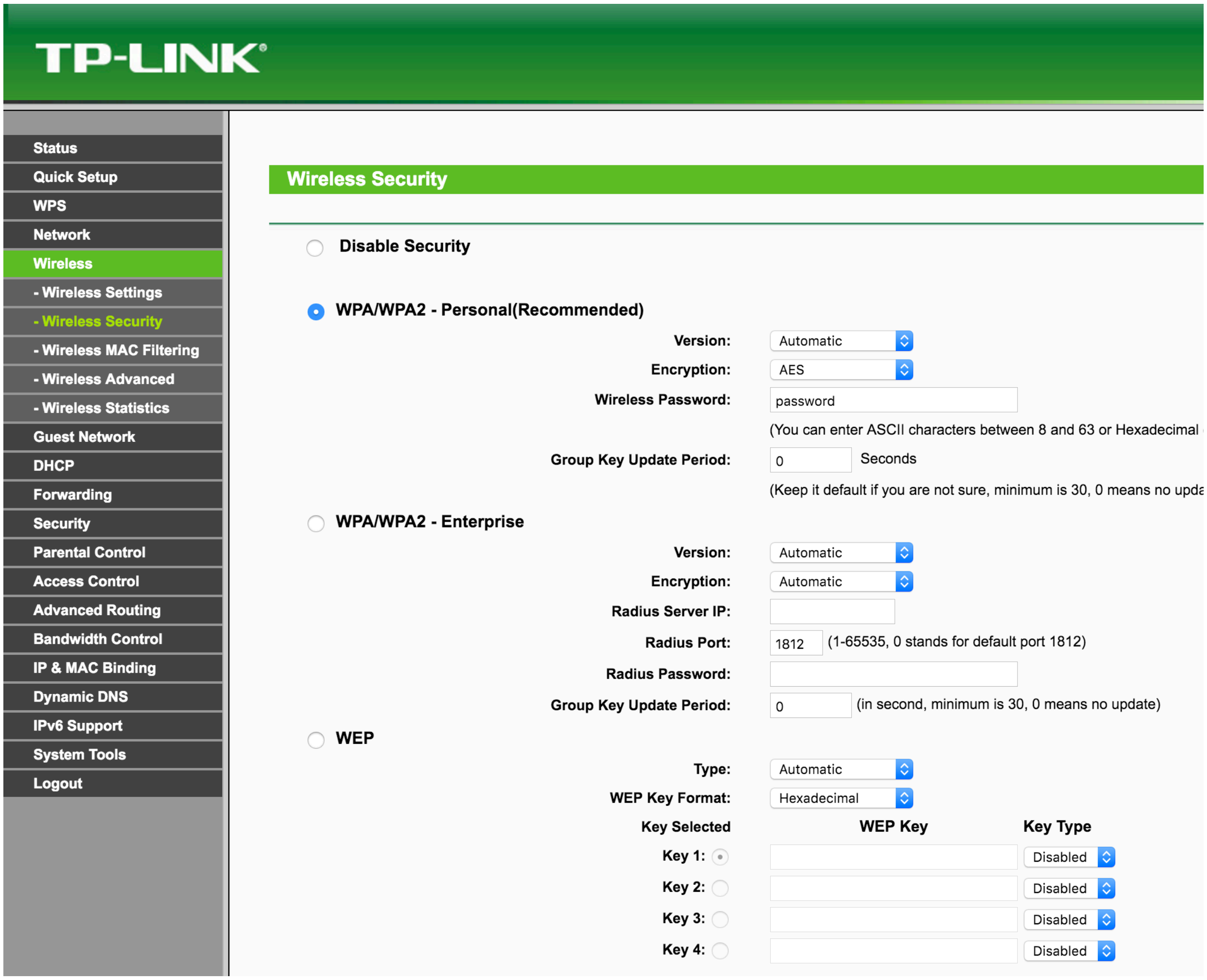
☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

□ Enable WDS Bridging

Step 4: Confugure the passphrase and wireless security.

In our router, go to Wireless -> Wireless Security. Then you can configure the security for the router. In the screenshot below, we configure the security protocol to WPA/WPA2, use AES as the encryption, and the passphrase is “password”. Other Security protocols are available such as WEP.



Wireless Security

○ Disable Security

● WPA/WPA2 - Personal(Recommended)

Version: Automatic

Encryption: AES

Wireless Password: password

(You can enter ASCII characters between 8 and 63 or Hexadecimal

Group Key Update Period: 0 Seconds

(Keep it default if you are not sure, minimum is 30, 0 means no upda

○ WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

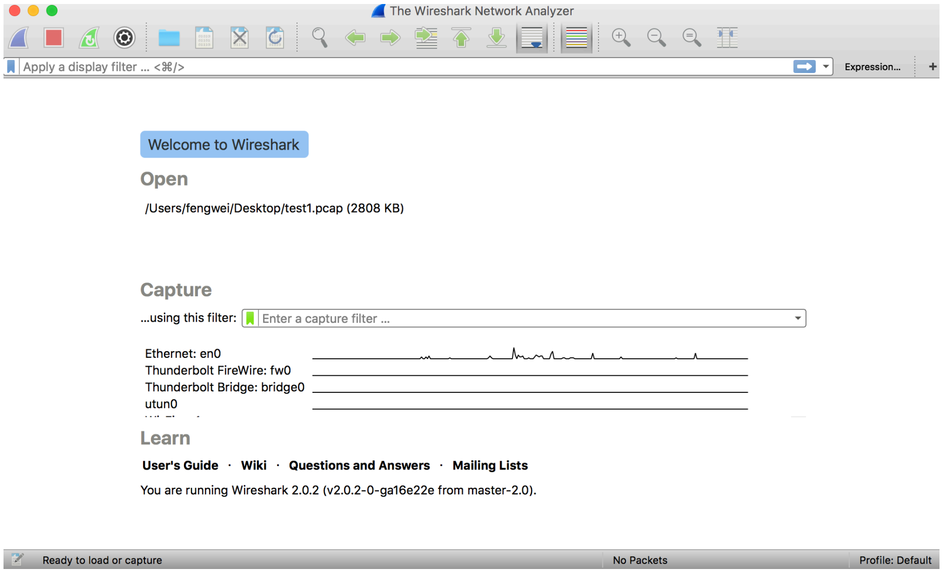
Capturing Wireless Packets via Wireshark

To capture wireless packets, you need to have a wireless network card installed on your machine. There are two kinds of wireless network interface: One is the internal NIC. Most of the laptops will have an internal NIC; the other one is the external NIC. The picture below shows an external network. This is a Wi-Fi USB Adapter from Alfa Network (1000mW High Power Wireless G 802.11g with 5dBi Antenna).

Once you have a wireless network card, you can run packet-sniffing tool to capture the packets as we did in Lab 1.

Step 1: Start the Wireshark program.

In order to sniff the packets, you may need to grant Wireshark root privilege by typing $ sudo wireshark in a terminal. Below is the screenshot of the Wireshark interface on my iMac desktop.



Welcome to Wireshark

Open

/Users/fengwei/Desktop/test1.pcap (2808 KB)

Capture

…using this filter: Enter a capture filter …

Ethernet: en0
Thunderbolt FireWire: fw0
Thunderbolt Bridge: bridge0
utun0

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0).

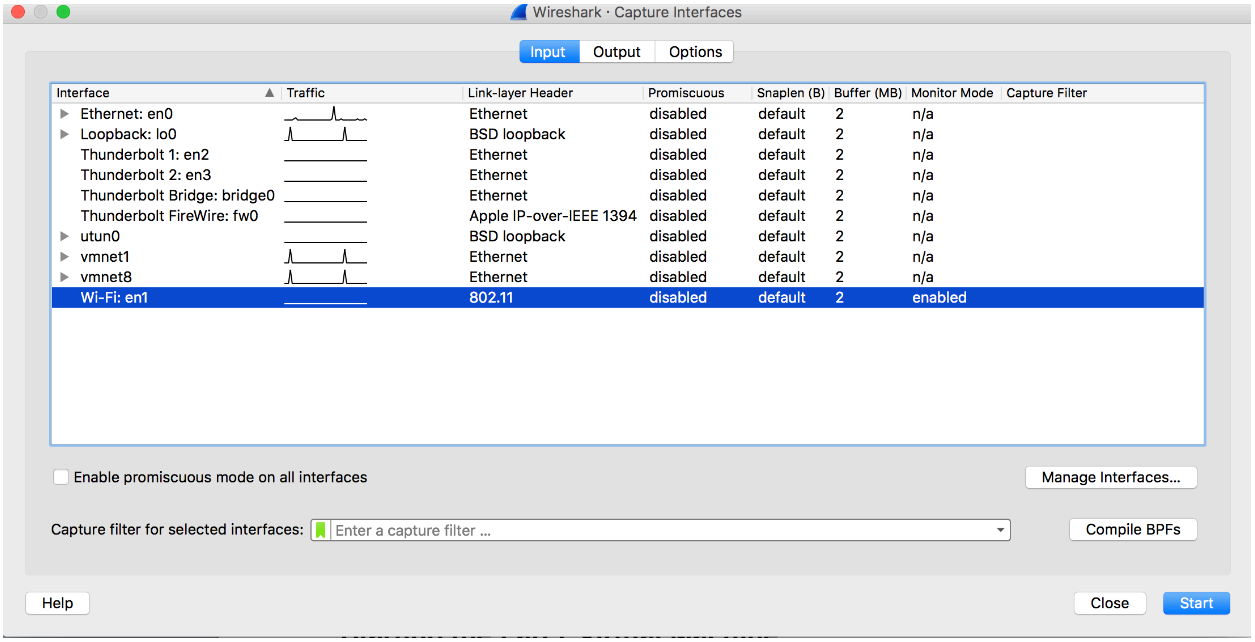
Ready to load or capture | No Packets | Profile: Default

Step 2: Select the WiFi Interface

Click the Capture -> Options in the Wireshark program. Look for the interface for WiFi. Normally, the interface name is wlan0, but it may be a different name that depends on your configuration. For instance, the name of the WiFi interface on my iMac is "Wi-Fi:en1".

Step 3: Enable the **Monitor Mode**

In Monitor Mode, it captures all packets from all SSID in its distance range. Please note that Monitor Mode is different from Promiscuous Mode. For the purpose of this lab, we need to capture all the traffic so that we need to enable the monitor mode. The screenshot below shows the configuration of the capture interface in Wireshark program on my iMac. You need to enable monitor mode and configure the Link-layer Head as 802.11.



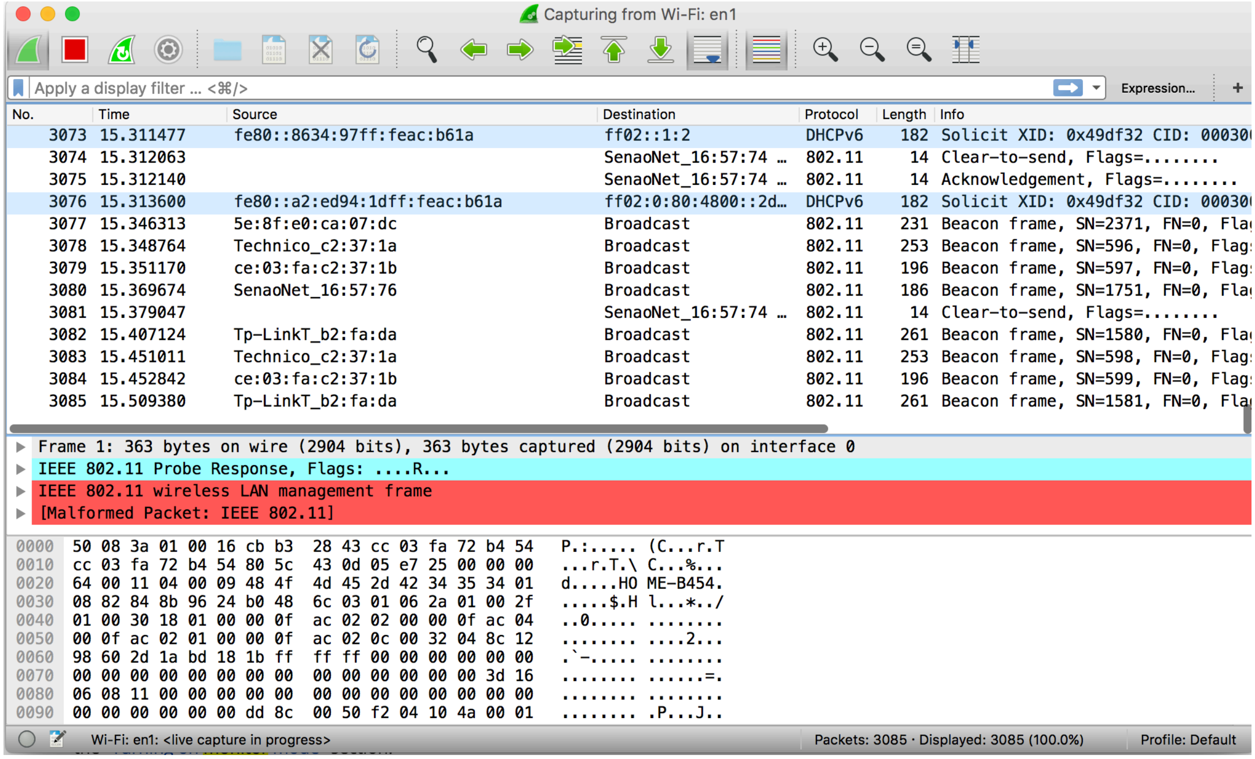
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
▶ Ethernet: en0		Ethernet	disabled	default	2	n/a	
▶ Loopback: lo0		BSD loopback	disabled	default	2	n/a	
Thunderbolt 1: en2		Ethernet	disabled	default	2	n/a	
Thunderbolt 2: en3		Ethernet	disabled	default	2	n/a	
Thunderbolt Bridge: bridge0		Ethernet	disabled	default	2	n/a	
Thunderbolt FireWire: fw0		Apple IP-over-IEEE 1394	disabled	default	2	n/a	
▶ utun0		BSD loopback	disabled	default	2	n/a	
▶ vmnet1		Ethernet	disabled	default	2	n/a	
▶ vmnet8		Ethernet	disabled	default	2	n/a	
Wi-Fi: en1		802.11	disabled	default	2	enabled	

□ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Step 4: Start Capturing

Click on start in the capture interfaces window and start capture. The screenshot below shows the interface of Wireshark program while capturing in Monitor Mode.



```
No.   Time       Source                      Destination           Protocol  Length  Info
 3073 15.311477  fe80::8634:97ff:feac:b61a   ff02::1:2             DHCPv6     182  Solicit XID: 0x49df32 CID: 00030
 3074 15.312063                              SenaoNet_16:57:74 …   802.11      14  Clear-to-send, Flags=........
 3075 15.312140                              SenaoNet_16:57:74 …   802.11      14  Acknowledgement, Flags=........
 3076 15.313600  fe80::a2:ed94:1dff:feac:b61a ff02:0:80:4800::2d…  DHCPv6     182  Solicit XID: 0x49df32 CID: 00030
 3077 15.346313  5e:8f:e0:ca:07:dc           Broadcast             802.11     231  Beacon frame, SN=2371, FN=0, Fla
 3078 15.348764  Technico_c2:37:1a           Broadcast             802.11     253  Beacon frame, SN=596, FN=0, Flag
 3079 15.351170  ce:03:fa:c2:37:1b           Broadcast             802.11     196  Beacon frame, SN=597, FN=0, Flag
 3080 15.369674  SenaoNet_16:57:76           Broadcast             802.11     186  Beacon frame, SN=1751, FN=0, Fla
 3081 15.379047                              SenaoNet_16:57:74 …   802.11      14  Clear-to-send, Flags=........
 3082 15.407124  Tp-LinkT_b2:fa:da           Broadcast             802.11     261  Beacon frame, SN=1580, FN=0, Fla
 3083 15.451011  Technico_c2:37:1a           Broadcast             802.11     253  Beacon frame, SN=598, FN=0, Flag
 3084 15.452842  ce:03:fa:c2:37:1b           Broadcast             802.11     196  Beacon frame, SN=599, FN=0, Flag
 3085 15.509380  Tp-LinkT_b2:fa:da           Broadcast             802.11     261  Beacon frame, SN=1581, FN=0, Fla
```

```
▶ Frame 1: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0
▶ IEEE 802.11 Probe Response, Flags: ....R...
▶ IEEE 802.11 wireless LAN management frame
▶ [Malformed Packet: IEEE 802.11]
```

```
0000  50 08 3a 01 00 16 cb b3  28 43 cc 03 fa 72 b4 54   P.:..... (C...r.T
0010  cc 03 fa 72 b4 54 80 5c  43 0d 05 e7 25 00 00 00   ...r.T.\ C...%...
0020  64 00 11 04 00 09 48 4f  4d 45 2d 42 34 35 34 01   d.....HO ME-B454.
0030  08 82 84 8b 96 24 b0 48  6c 03 01 06 2a 01 00 2f   .....$.H l...*../
0040  01 00 30 18 01 00 00 0f  ac 02 02 00 00 0f ac 04   ..0..... ........
0050  00 0f ac 02 01 00 00 0f  ac 02 0c 00 32 04 8c 12   ........ ....2...
0060  98 60 2d 1a bd 18 1b ff  ff ff 00 00 00 00 00 00   .`-..... ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 3d 16   ........ ......=.
0080  06 08 11 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 dd 8c  00 50 f2 04 10 4a 00 01   ........ .P...J..
```

```
Wi-Fi: en1: <live capture in progress>    Packets: 3085 · Displayed: 3085 (100.0%)    Profile: Default
```

Capturing the Four-way Handshake

To crack the WPA/WPA2 passphrase, we first need to capture the four-way handshake that contains

Step 1: Start to capture all the traffic

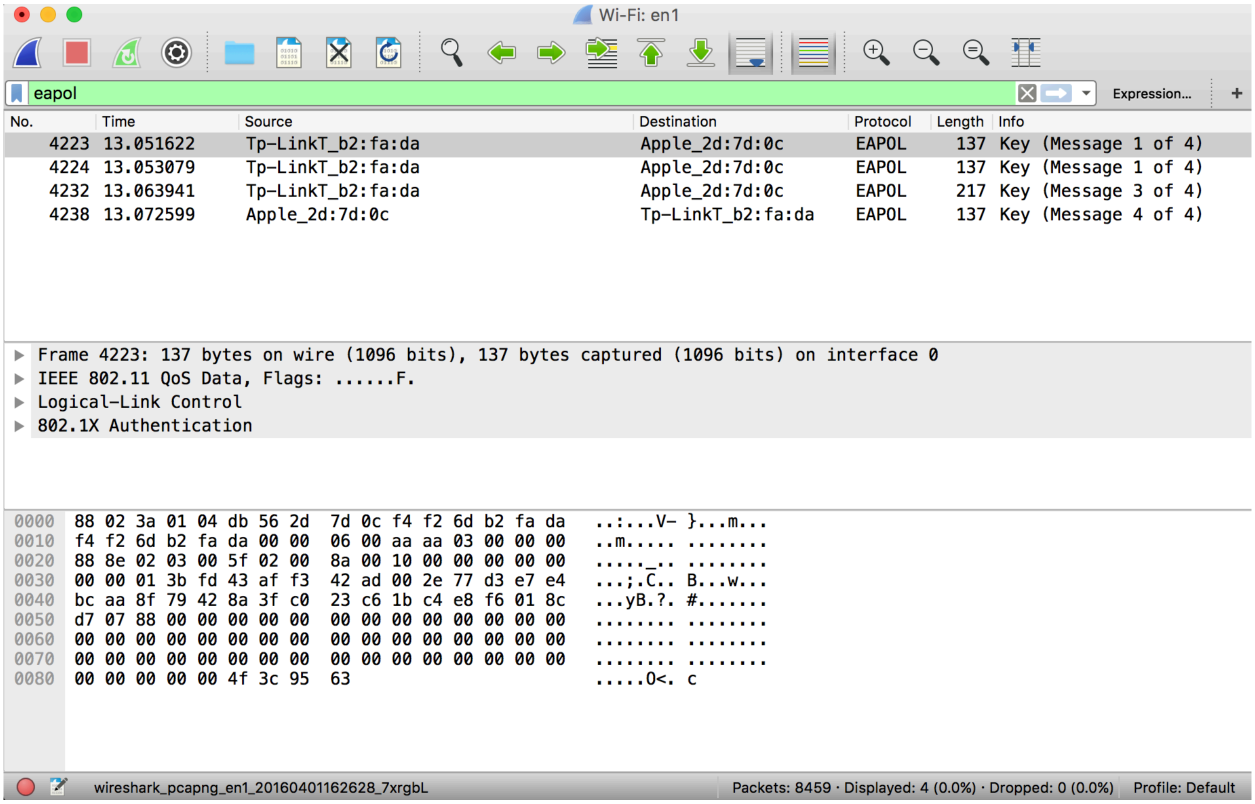
This is what we just did in our previous step. Just the Wireshark program into Monitor Mode and run

Step 2: Connect to the access point using its passphrase

Use your cell phone or laptop connects to the access point. For the purpose of this lab, the SSID of the router in our classroom is “Hack3r”.

Step 3: Stop Wireshark program and identify the four-way handsake

Press the stop button to stop capturing in Wireshark; type keyword “EAPOL” in the filter to identify the four-way handshake. Screenshot below shows the example.



```
eapol
```

```
No.   Time       Source             Destination        Protocol  Length  Info
4223  13.051622  Tp-LinkT_b2:fa:da  Apple_2d:7d:0c     EAPOL     137     Key (Message 1 of 4)
4224  13.053079  Tp-LinkT_b2:fa:da  Apple_2d:7d:0c     EAPOL     137     Key (Message 1 of 4)
4232  13.063941  Tp-LinkT_b2:fa:da  Apple_2d:7d:0c     EAPOL     217     Key (Message 3 of 4)
4238  13.072599  Apple_2d:7d:0c     Tp-LinkT_b2:fa:da  EAPOL     137     Key (Message 4 of 4)
```

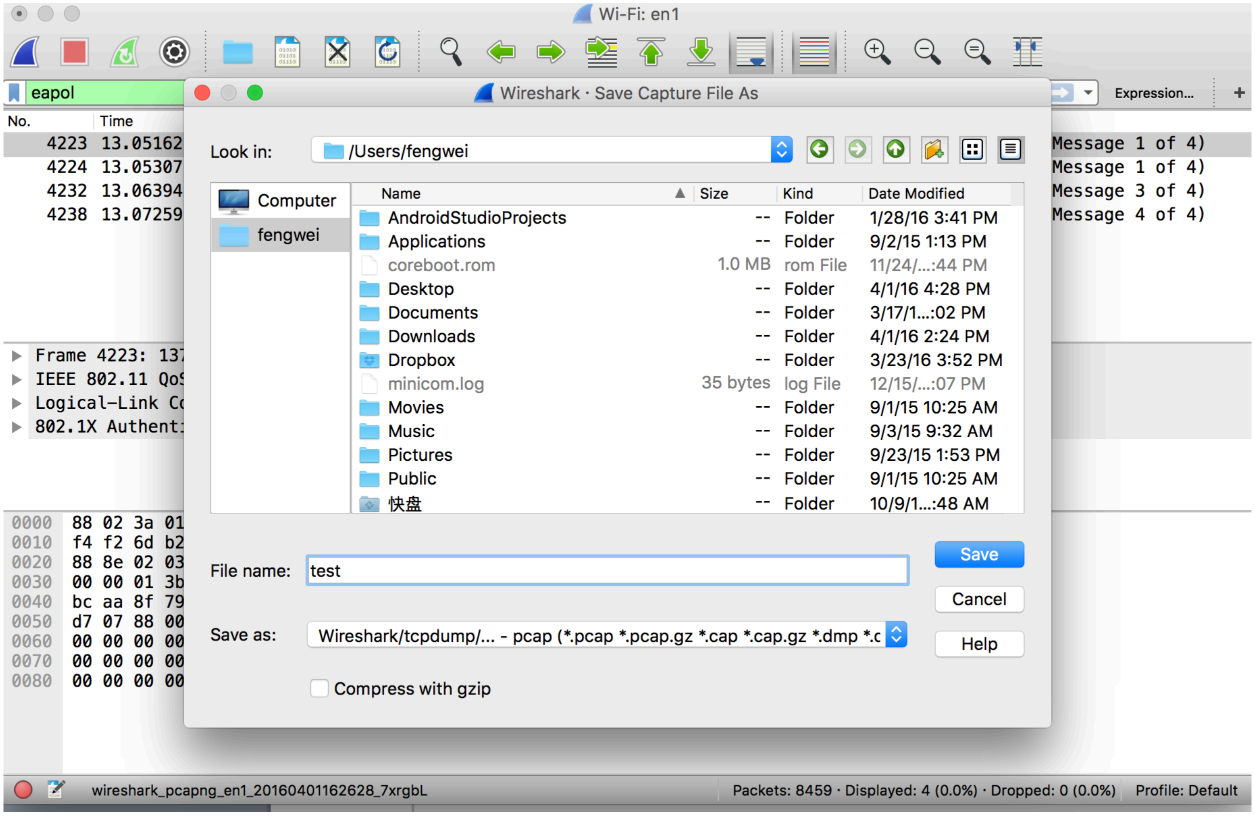
```
▶ Frame 4223: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
▶ IEEE 802.11 QoS Data, Flags: ......F.
▶ Logical-Link Control
▶ 802.1X Authentication
```

```
0000  88 02 3a 01 04 db 56 2d  7d 0c f4 f2 6d b2 fa da   ..:...V- }...m...
0010  f4 f2 6d b2 fa da 00 00  06 00 aa aa 03 00 00 00   ..m..... ........
0020  88 8e 02 03 00 5f 02 00  8a 00 10 00 00 00 00 00   ....._.. ........
0030  00 00 01 3b fd 43 af f3  42 ad 00 2e 77 d3 e7 e4   ...;.C.. B...w...
0040  bc aa 8f 79 42 8a 3f c0  23 c6 1b c4 e8 f6 01 8c   ...yB.?. #.......
0050  d7 07 88 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 4f 3c 95  63                        .....O<. c
```

wireshark_pcapng_en1_20160401162628_7xrgbL   Packets: 8459 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)   Profile: Default

Step 4: Save the captured traffic

Click File -> Save as option to save the captured traffic to a pcap file. Screenshot below shows the example. The saved pcap file name is: test.pcap



Wi-Fi: en1

eapol

```
No.   Time
4223  13.05162                                        Message 1 of 4)
4224  13.05307                                        Message 1 of 4)
4232  13.06394                                        Message 3 of 4)
4238  13.07259                                        Message 4 of 4)

▶ Frame 4223: 137
▶ IEEE 802.11 QoS
▶ Logical-Link Co
▶ 802.1X Authenti

0000  88 02 3a 01
0010  f4 f2 6d b2
0020  88 8e 02 03
0030  00 00 01 3b
0040  bc aa 8f 79
0050  d7 07 88 00
0060  00 00 00 00
0070  00 00 00 00
0080  00 00 00 00
```

Wireshark · Save Capture File As

Look in: /Users/fengwei

Name	Size	Kind	Date Modified
AndroidStudioProjects	--	Folder	1/28/16 3:41 PM
Applications	--	Folder	9/2/15 1:13 PM
coreboot.rom	1.0 MB	rom File	11/24/...:44 PM
Desktop	--	Folder	4/1/16 4:28 PM
Documents	--	Folder	3/17/1...:02 PM
Downloads	--	Folder	4/1/16 2:24 PM
Dropbox	--	Folder	3/23/16 3:52 PM
minicom.log	35 bytes	log File	12/15/...:07 PM
Movies	--	Folder	9/1/15 10:25 AM
Music	--	Folder	9/3/15 9:32 AM
Pictures	--	Folder	9/23/15 1:53 PM
Public	--	Folder	9/1/15 10:25 AM
快盘	--	Folder	10/9/1...:48 AM

File name: test

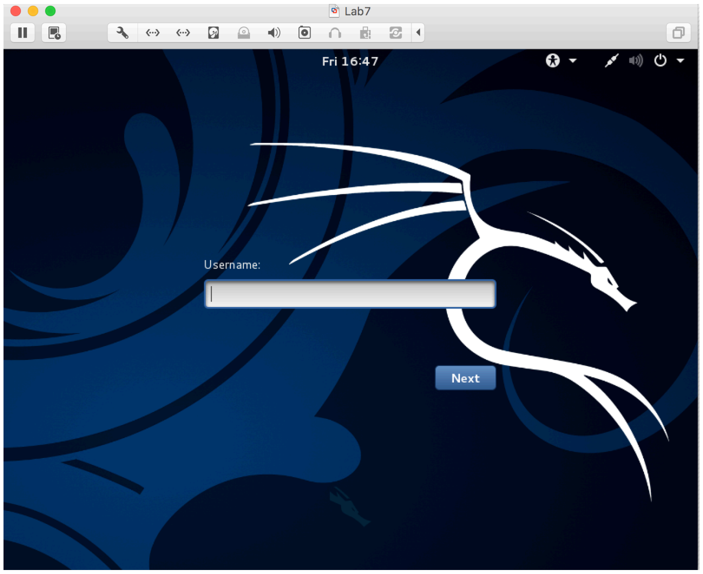
Save as: Wireshark/tcpdump/... - pcap (*.pcap *.pcap.gz *.cap *.cap.gz *.dmp *.c

□ Compress with gzip

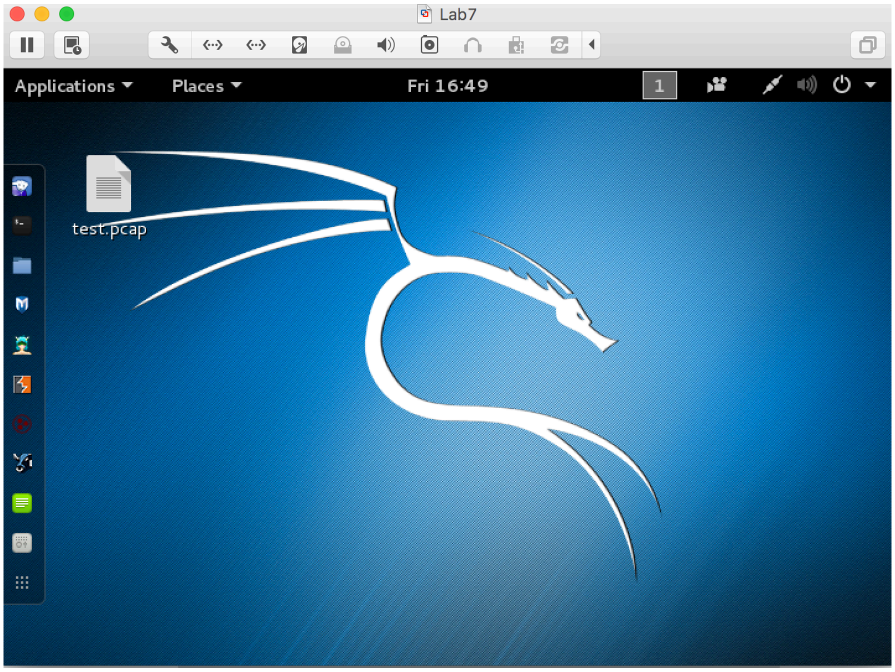
wireshark_pcapng_en1_20160401162628_7xrgbL   Packets: 8459 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)   Profile: Default

Cracking WPA2 WiFi Passphrase Using Kali Linux

In this lab, we use a Kali Linux to crack the WPA2 WiFi passphrase. Select the VM image named “Lab7”.



Login the Kali image with username root, and password [TBA in the class]. Below is the screen snapshot after login.



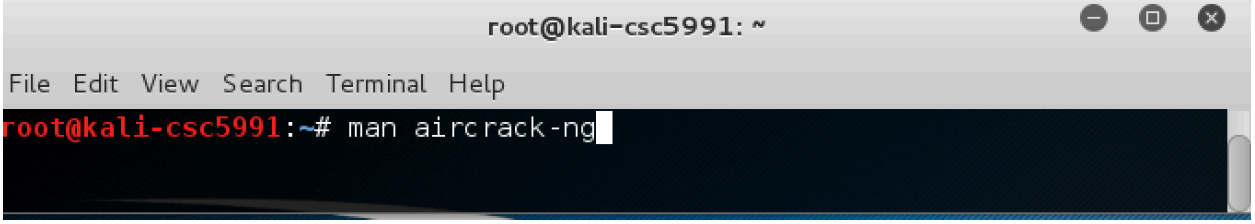
Step 1: Copy the test.pcap file into the Kali Linux

In our Kali Linux image, there is a copy of the test-instructor.pcap file. If you do not have your copy of test.pcap, you can also use the test-intructor.pcap file.

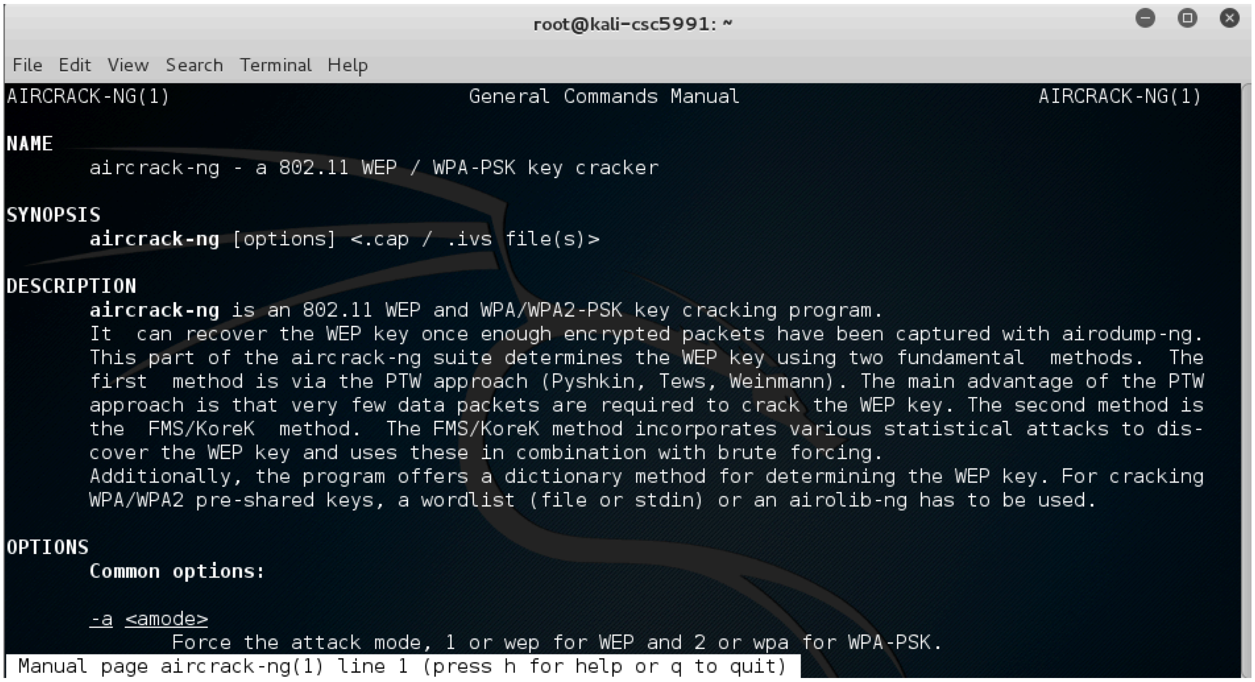
Step 2: Use aircrack-ng to crack the passphrase

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. Kali Linux has installed it as default.

You can type $ man aircrack-ng to see the manual page of the tool



```
root@kali-csc5991:~# man aircrack-ng
```



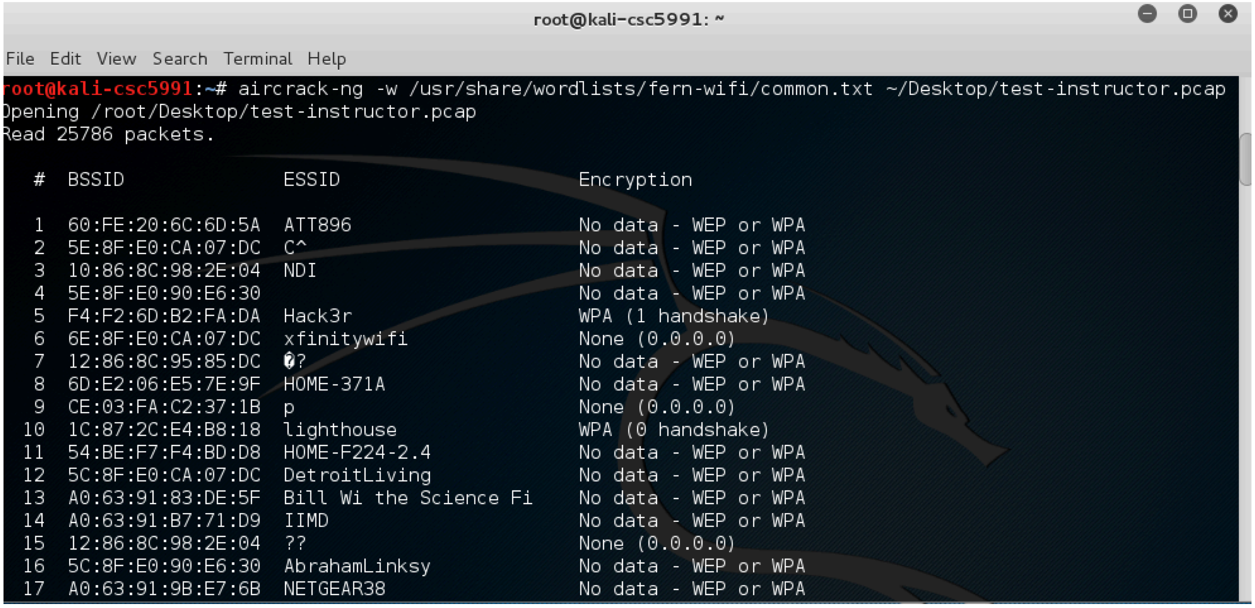
```
AIRCRACK-NG(1)                General Commands Manual                AIRCRACK-NG(1)

NAME
       aircrack-ng - a 802.11 WEP / WPA-PSK key cracker

SYNOPSIS
       aircrack-ng [options] <.cap / .ivs file(s)>

DESCRIPTION
       aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.
       It  can recover the WEP key once enough encrypted packets have been captured with airodump-ng.
       This part of the aircrack-ng suite determines the WEP key using two fundamental  methods.  The
       first  method is via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage of the PTW
       approach is that very few data packets are required to crack the WEP key. The second method is
       the  FMS/KoreK  method.  The FMS/KoreK method incorporates various statistical attacks to dis-
       cover the WEP key and uses these in combination with brute forcing.
       Additionally, the program offers a dictionary method for determining the WEP key. For cracking
       WPA/WPA2 pre-shared keys, a wordlist (file or stdin) or an airolib-ng has to be used.

OPTIONS
       Common options:

       -a <amode>
              Force the attack mode, 1 or wep for WEP and 2 or wpa for WPA-PSK.
 Manual page aircrack-ng(1) line 1 (press h for help or q to quit)
```

Run the following command to crack the passphrase

$ aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Desktop/test-instructor.pcap

-w: specify the path to the wordlist

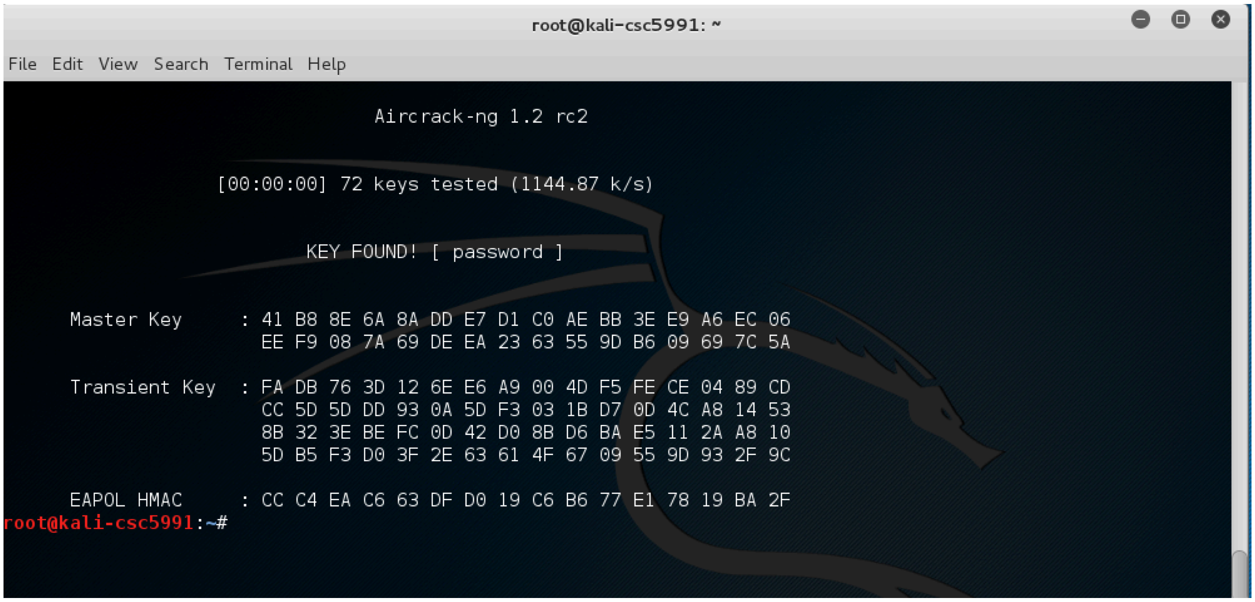
Followed by the pcap file. The screenshot below shows the execution of the command.



```
root@kali-csc5991:~# aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Desktop/test-instructor.pcap
Opening /root/Desktop/test-instructor.pcap
Read 25786 packets.

   #  BSSID              ESSID                     Encryption

   1  60:FE:20:6C:6D:5A  ATT896                    No data - WEP or WPA
   2  5E:8F:E0:CA:07:DC  C^                        No data - WEP or WPA
   3  10:86:8C:98:2E:04  NDI                       No data - WEP or WPA
   4  5E:8F:E0:90:E6:30                            No data - WEP or WPA
   5  F4:F2:6D:B2:FA:DA  Hack3r                    WPA (1 handshake)
   6  6E:8F:E0:CA:07:DC  xfinitywifi               None (0.0.0.0)
   7  12:86:8C:95:85:DC  �?                        No data - WEP or WPA
   8  6D:E2:06:E5:7E:9F  HOME-371A                 No data - WEP or WPA
   9  CE:03:FA:C2:37:1B  p                         None (0.0.0.0)
  10  1C:87:2C:E4:B8:18  lighthouse                WPA (0 handshake)
  11  54:BE:F7:F4:BD:D8  HOME-F224-2.4             No data - WEP or WPA
  12  5C:8F:E0:CA:07:DC  DetroitLiving             No data - WEP or WPA
  13  A0:63:91:83:DE:5F  Bill Wi the Science Fi    No data - WEP or WPA
  14  A0:63:91:B7:71:D9  IIMD                      No data - WEP or WPA
  15  12:86:8C:98:2E:04  ??                        None (0.0.0.0)
  16  5C:8F:E0:90:E6:30  AbrahamLinksy             No data - WEP or WPA
  17  A0:63:91:9B:E7:6B  NETGEAR38                 No data - WEP or WPA
```

Then, we choose index for the WPA2 handshake. We can identify the index by using the SSID. From the screenshot we can see that the index for “Hack3r” is 5.

After enter 5, we can see that aircrack has successfully crack the passphrase as shown in the screenshot below.



```
                                 Aircrack-ng 1.2 rc2


                   [00:00:00] 72 keys tested (1144.87 k/s)


                           KEY FOUND! [ password ]


      Master Key     : 41 B8 8E 6A 8A DD E7 D1 C0 AE BB 3E E9 A6 EC 06
                       EE F9 08 7A 69 DE EA 23 63 55 9D B6 09 69 7C 5A

      Transient Key  : FA DB 76 3D 12 6E E6 A9 00 4D F5 FE CE 04 89 CD
                       CC 5D 5D DD 93 0A 5D F3 03 1B D7 0D 4C A8 14 53
                       8B 32 3E BE FC 0D 42 D0 8B D6 BA E5 11 2A A8 10
                       5D B5 F3 D0 3F 2E 63 61 4F 67 09 55 9D 93 2F 9C

      EAPOL HMAC     : CC C4 EA C6 63 DF D0 19 C6 B6 77 E1 78 19 BA 2F
root@kali-csc5991:~#
```

Assignments for Lab 7

1. Read the lab instructions above and finish all the tasks.
2. Answer the questions in the Introduction section, and justify your answers. Simple yes or no answer will not get any credits.
   a. What is the difference between Monitor Mode and Promiscuous Mode
   b. What lessons we learned from this lab about setting the WiFi password?
3. Change your router to a different passphrase, and use the Wireshark and Aircrach-ng to crack the passphrase. Show screenshots of the result.

Extra Credit (5pt): Send a broadcast de-authentication packet to force clients to reconnect. Then you can capture the four-way handshake.

Happy Hacking!