南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

计算机科学与工程系

Department of Computer Science and Engineering

CS 315 Computer Security Course

Lab 6 Part 2: 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 as an example, but the same concepts or ideas are applicable on other routers. 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.)

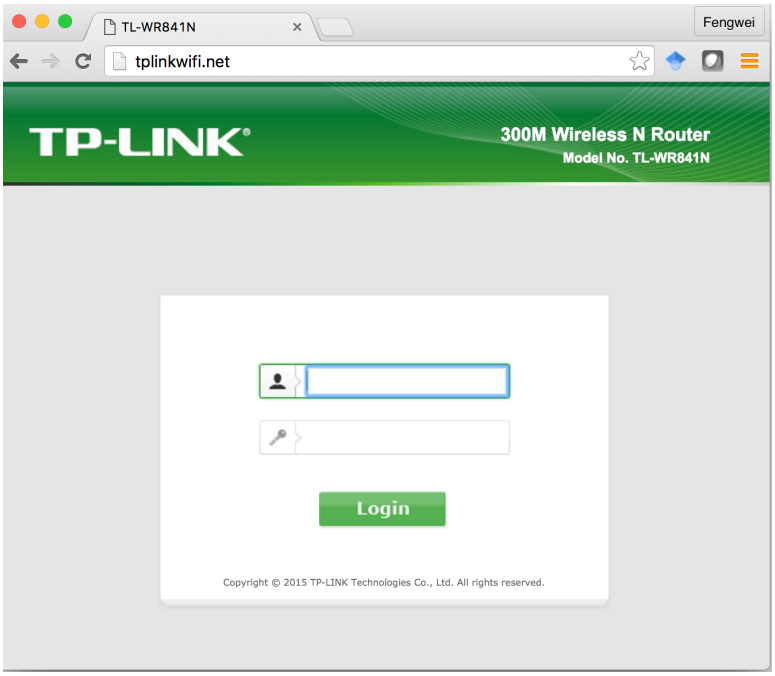
Step 2: Open the web-based setup page

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

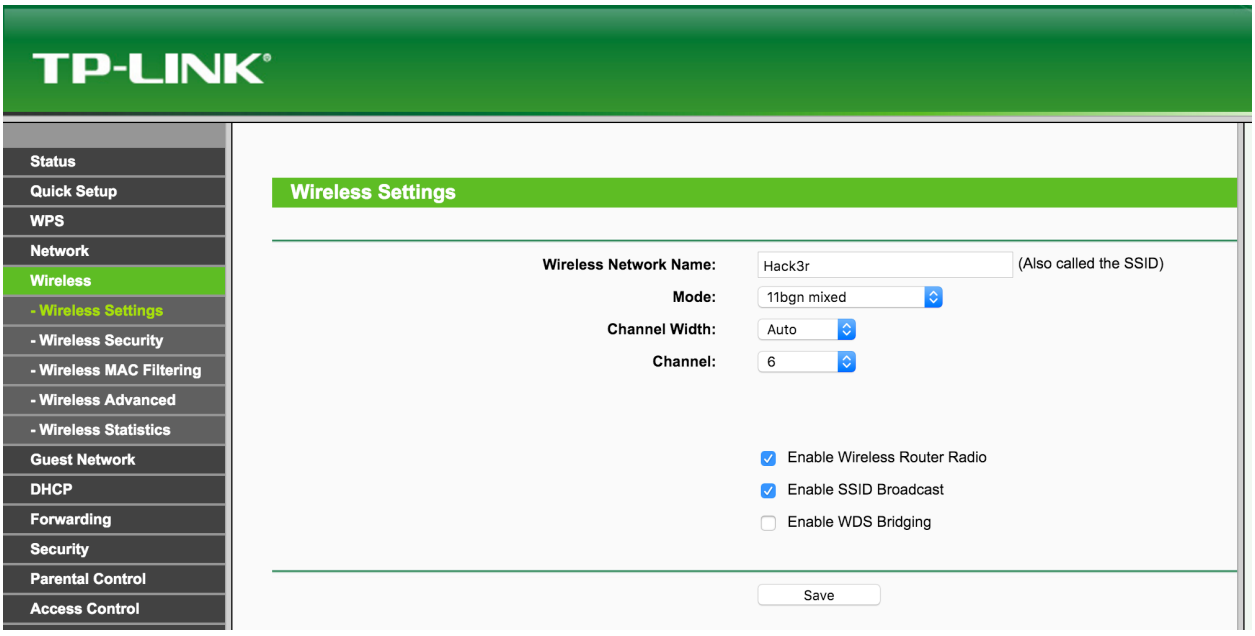
Enter the default username and password to login. For our router, its default username and password are admin and [Same-Password-As-Kali-Linux].

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



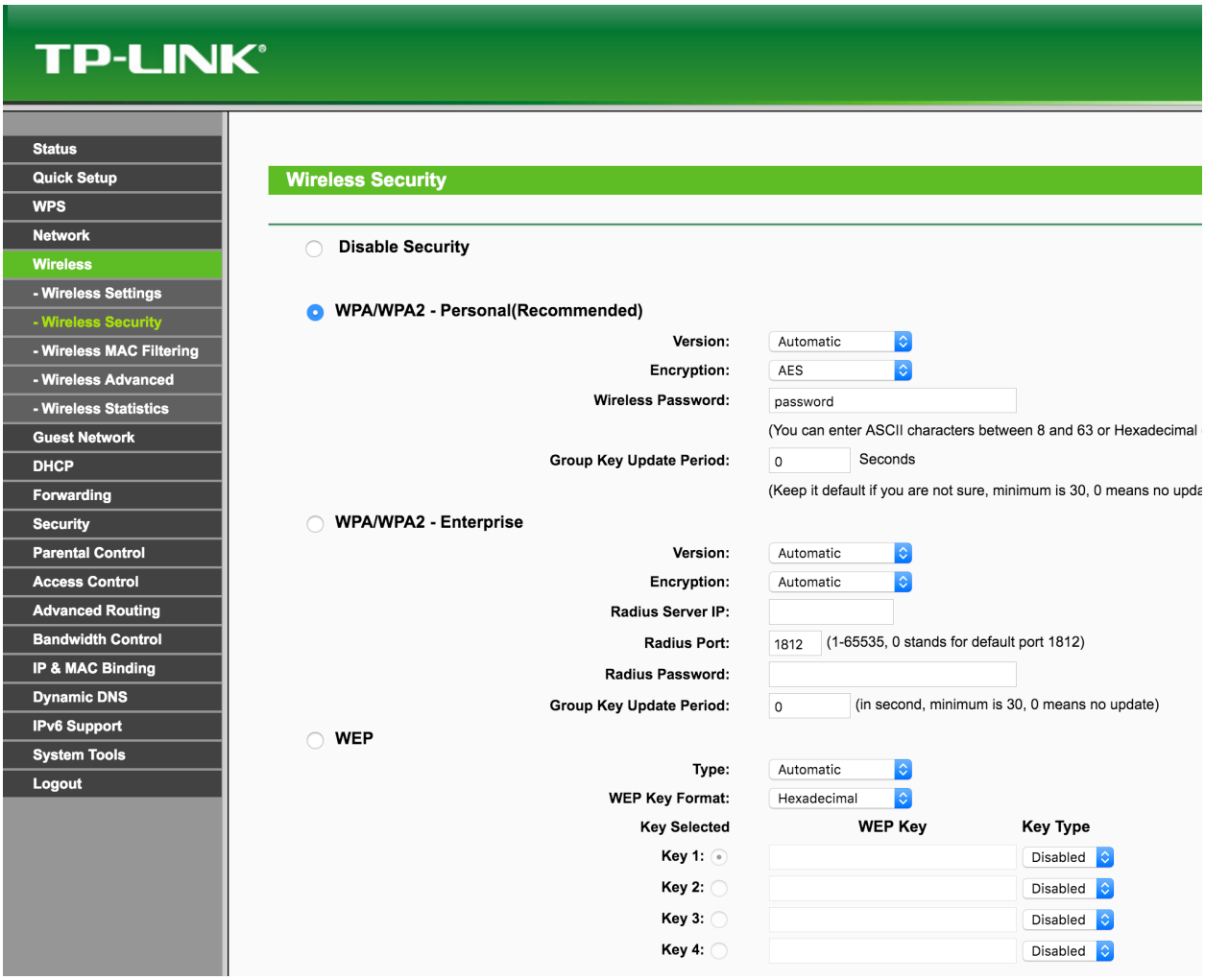
Step 4: Configure the SSID

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”



Step 5: 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.



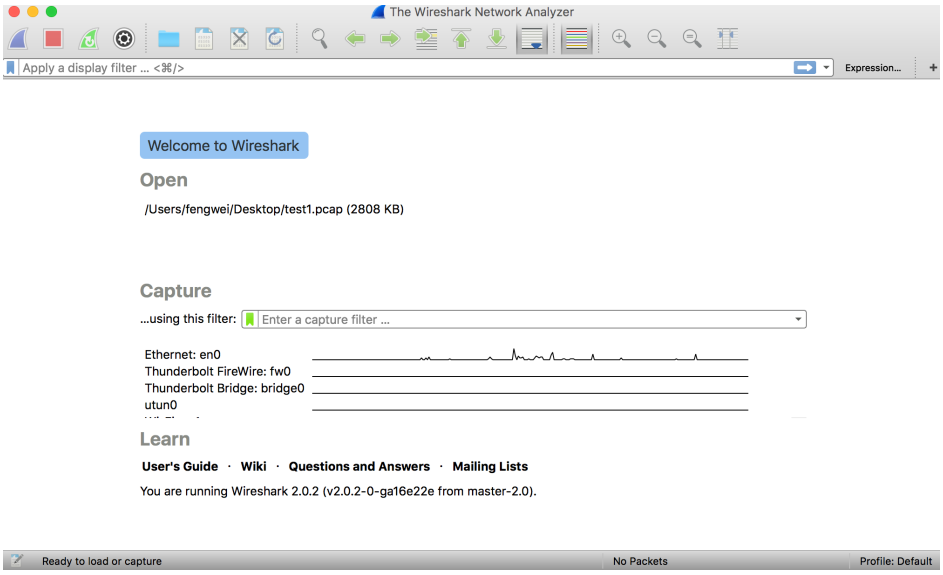
Capturing Wireless Packets via Wireshark

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.



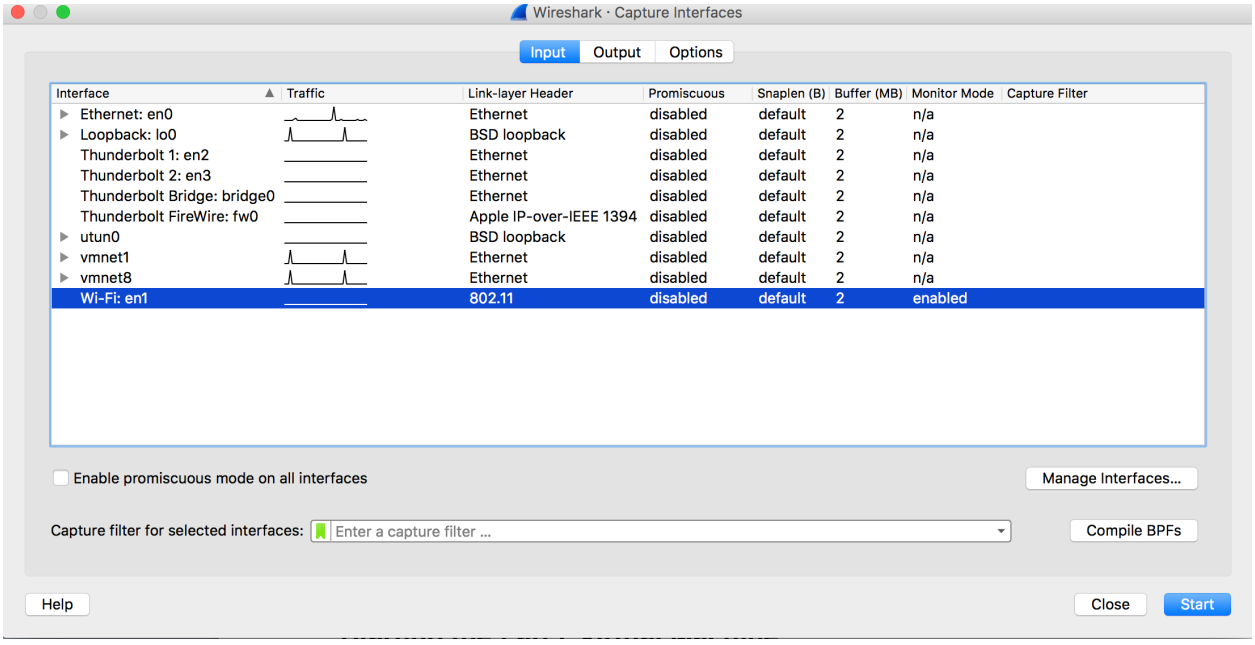
Step 2: Select the WiFi Interface

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”.

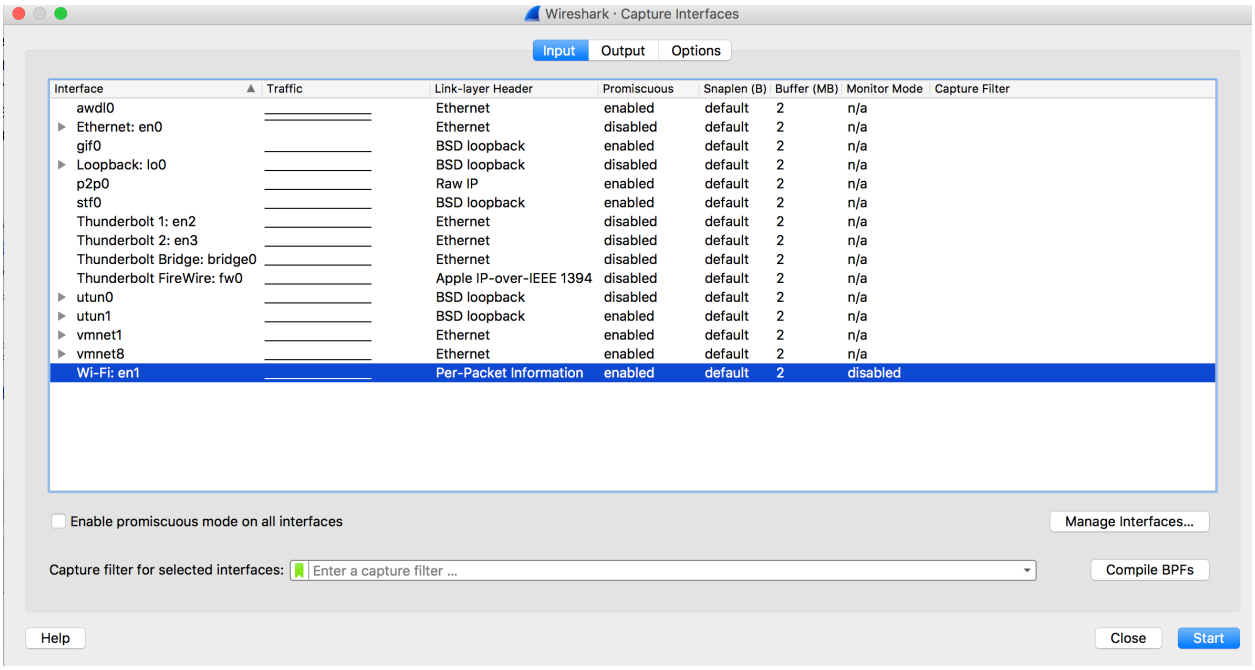
Step 3: Enable the **Monitor Mode or Promiscuous Mode**

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 or promiscuous mode.

The screenshot below shows the configuration of the capture interface in Wireshark program on my iMac with monitor mode. You need to enable monitor mode and configure the Link-layer Head as 802.11.

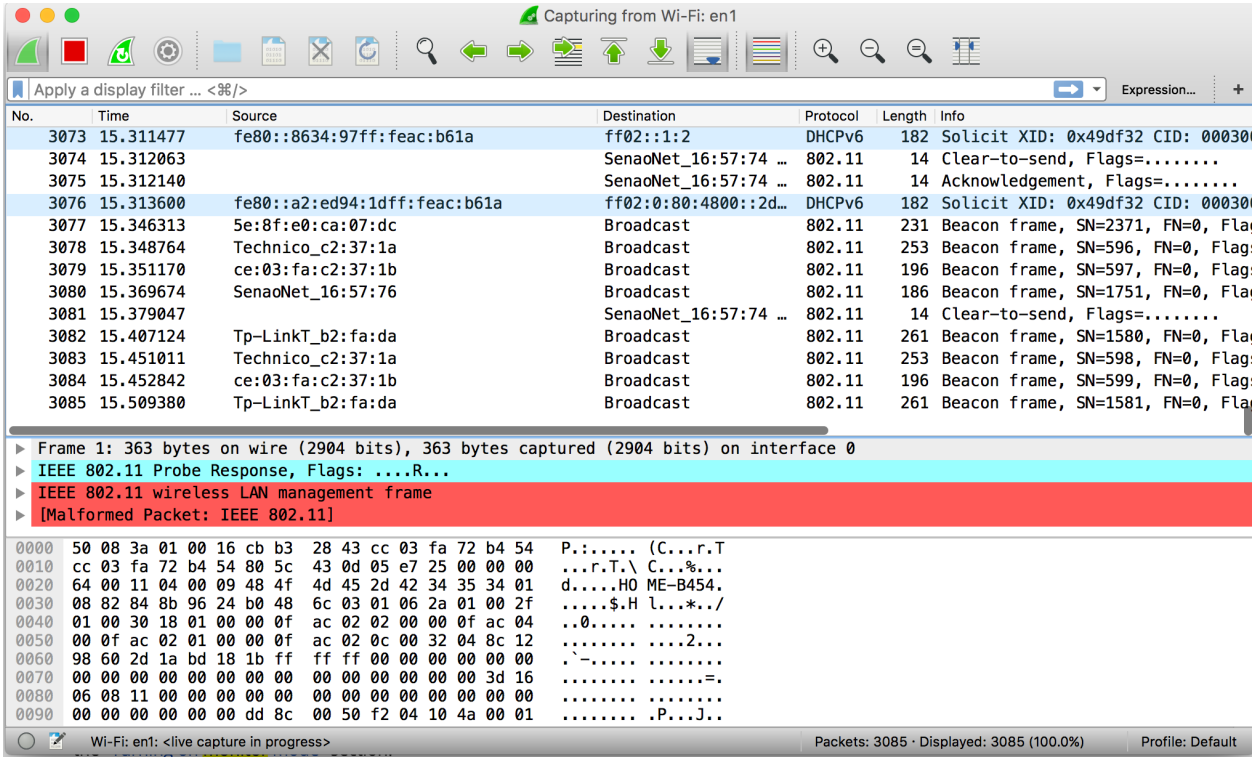


The screenshot below shows the configuration of the capture interface in Wireshark program on my iMac with promiscuous. You need to enable promiscuous mode and configure the Link-layer Head as Per-Packet Information.



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.



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

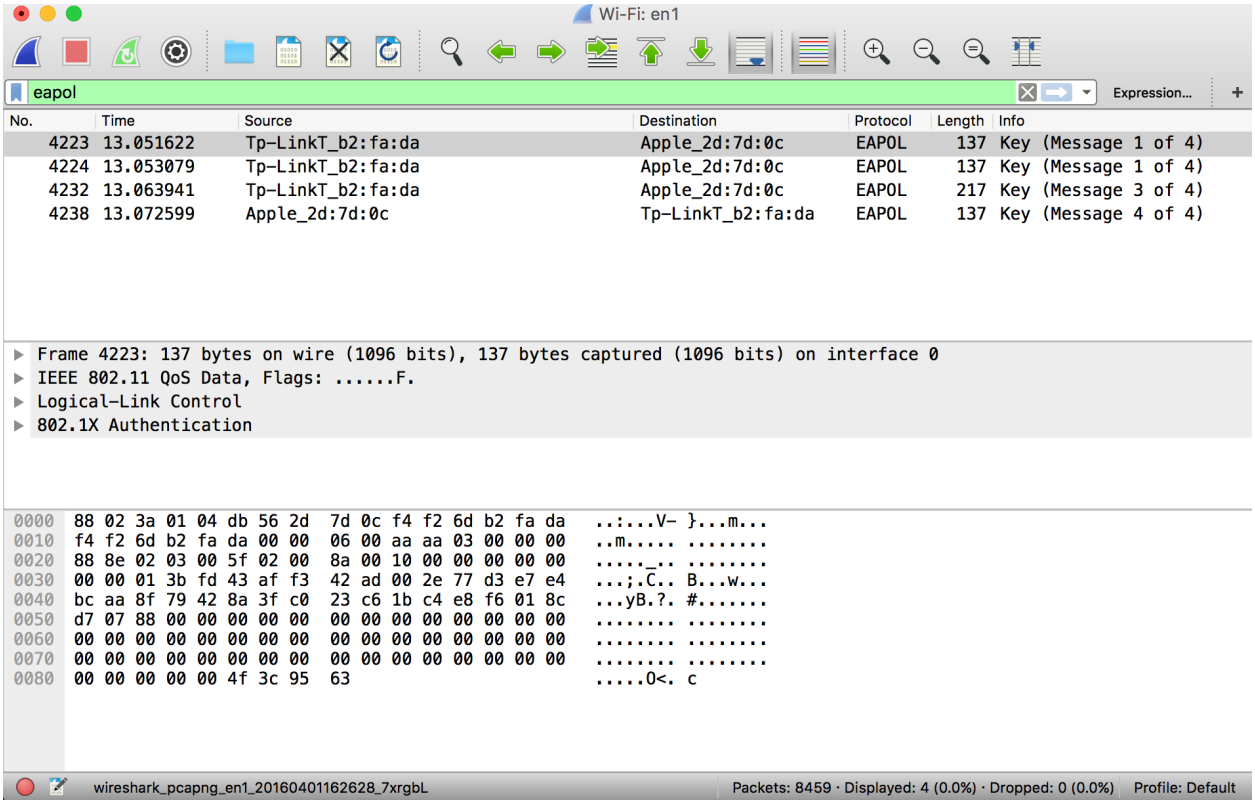
This is what we just did in our previous step. Just the Wireshark program into Monitor Mode and run

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”.

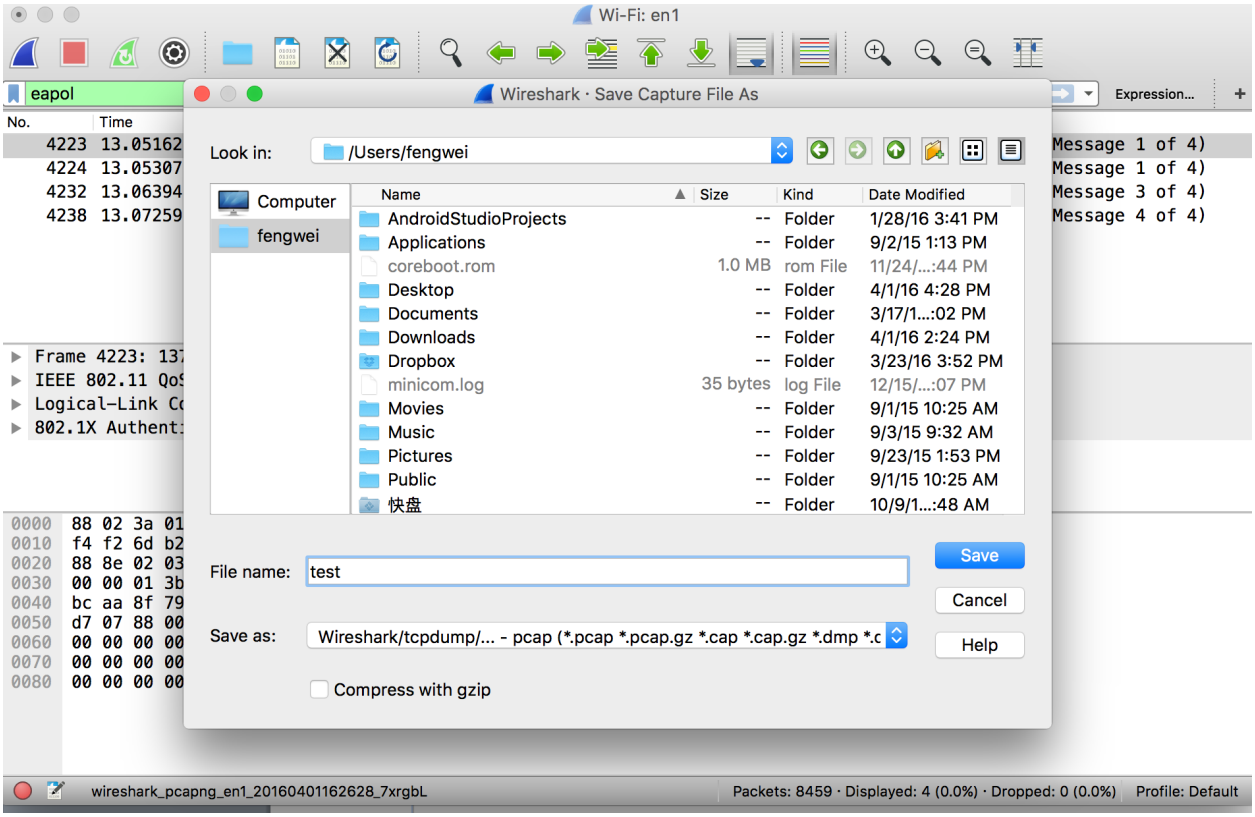
Step 3: Stop Wireshark program and identify the four-way handsake

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.



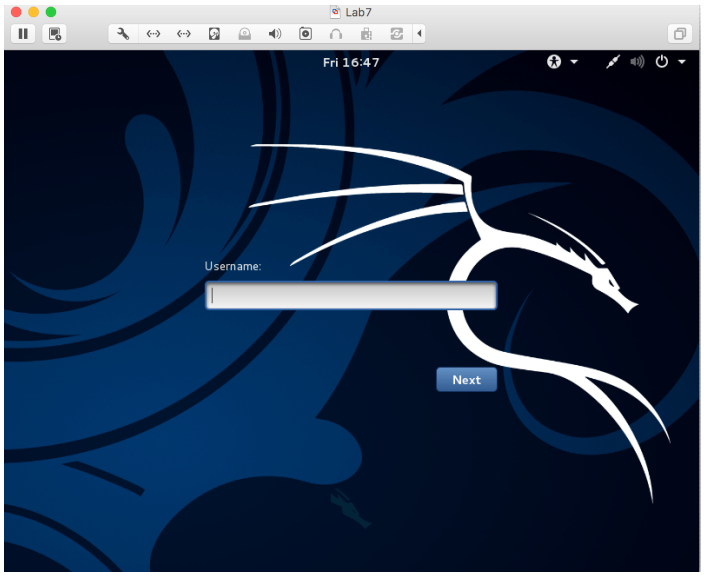
Step 4: Save the captured traffic

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



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.

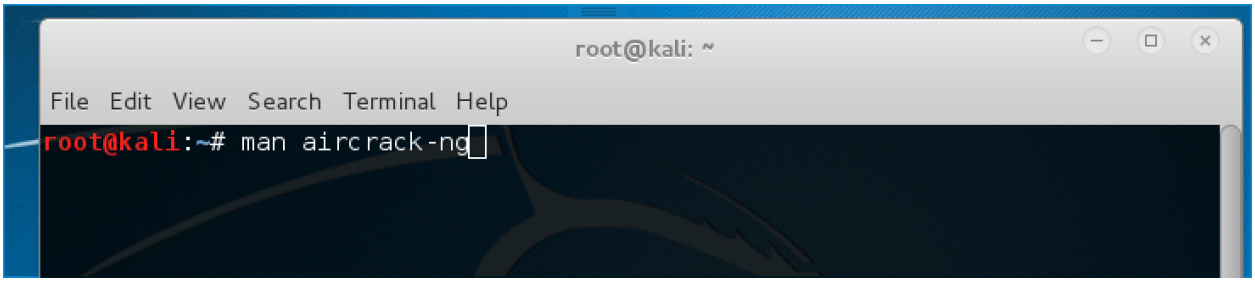
Step 1: Copy the test.pcap file into the Kali Linux

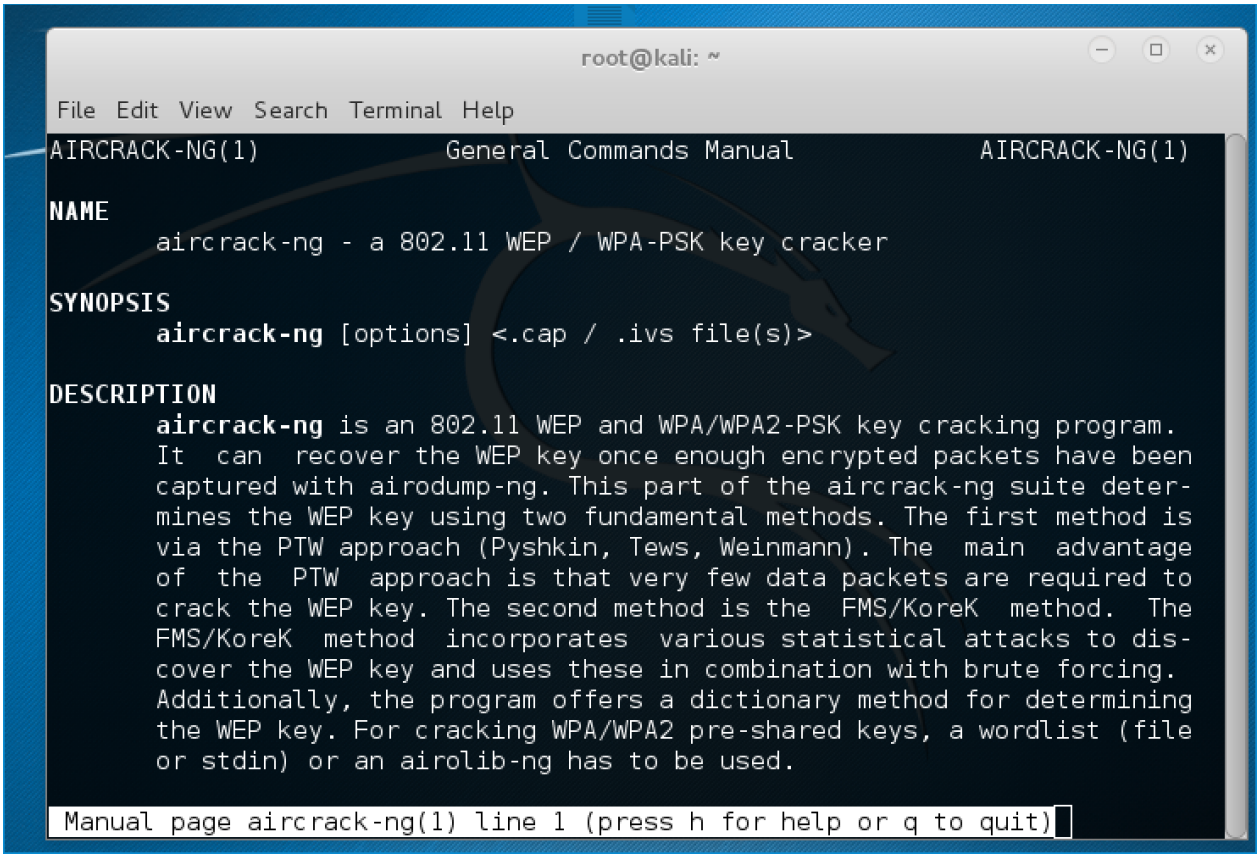
In our Kali Linux image, there is a copy of the test-instructor-monitor.pcap and test-instructor-promiscuous files. If you do not have your copy of test.pcap, you can also use these files.

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



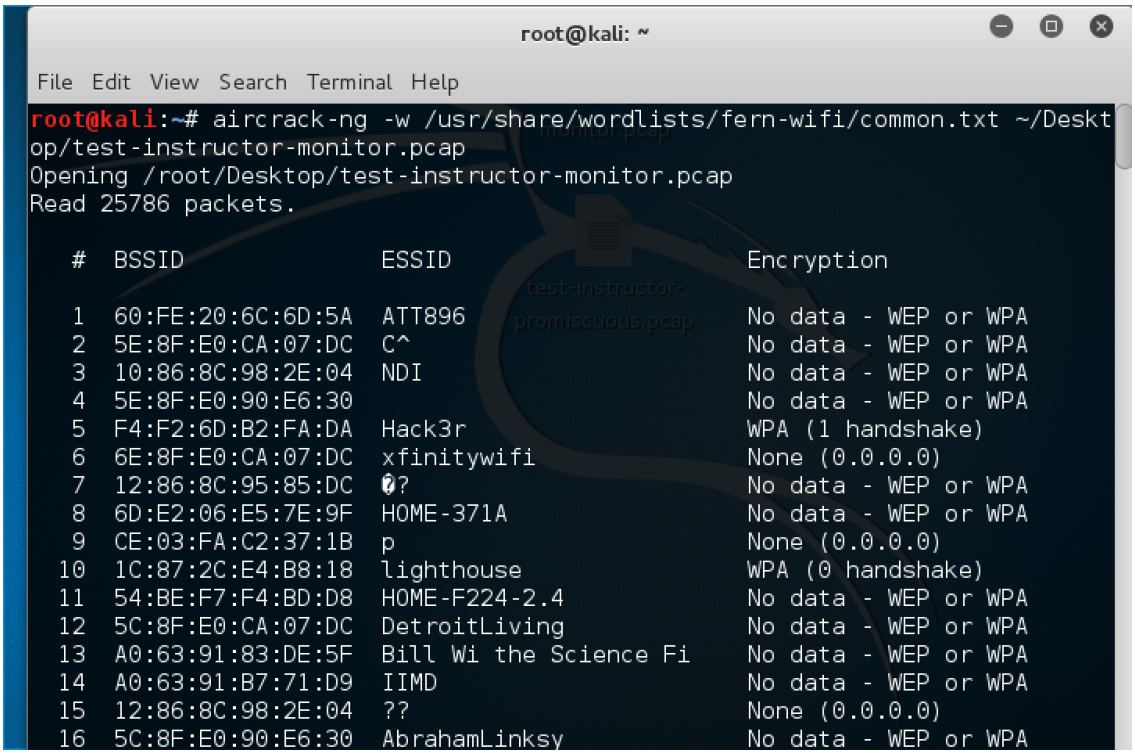


Run the following command to crack the passphrase

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

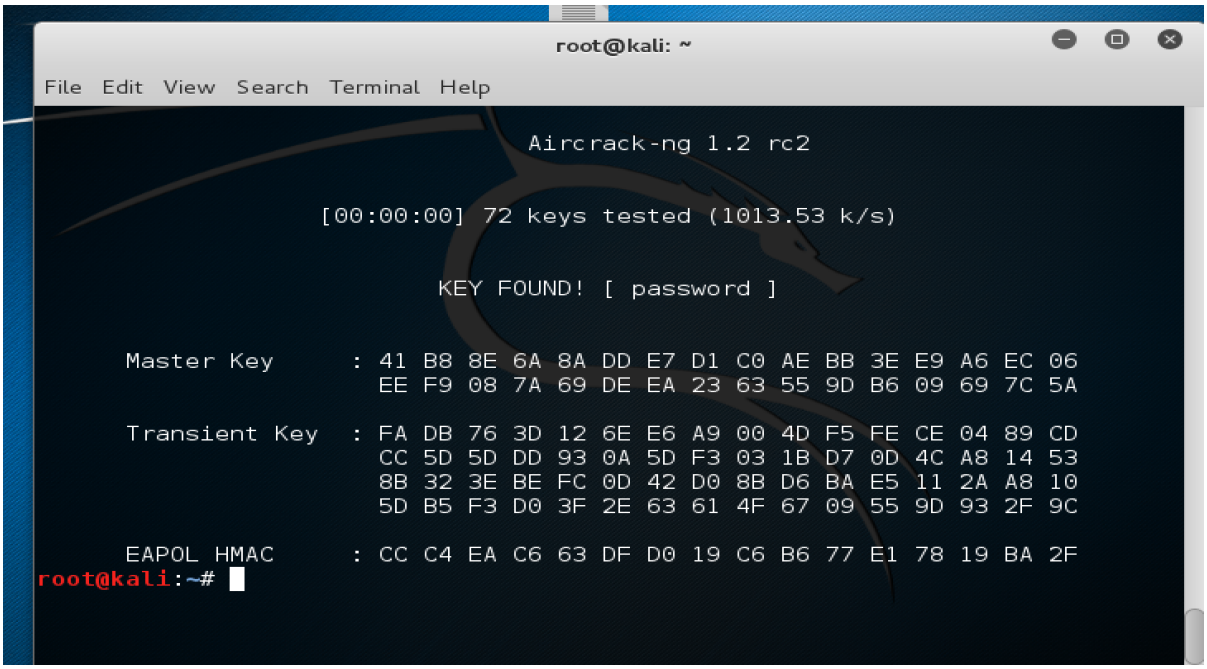
-w: specify the path to the wordlist

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

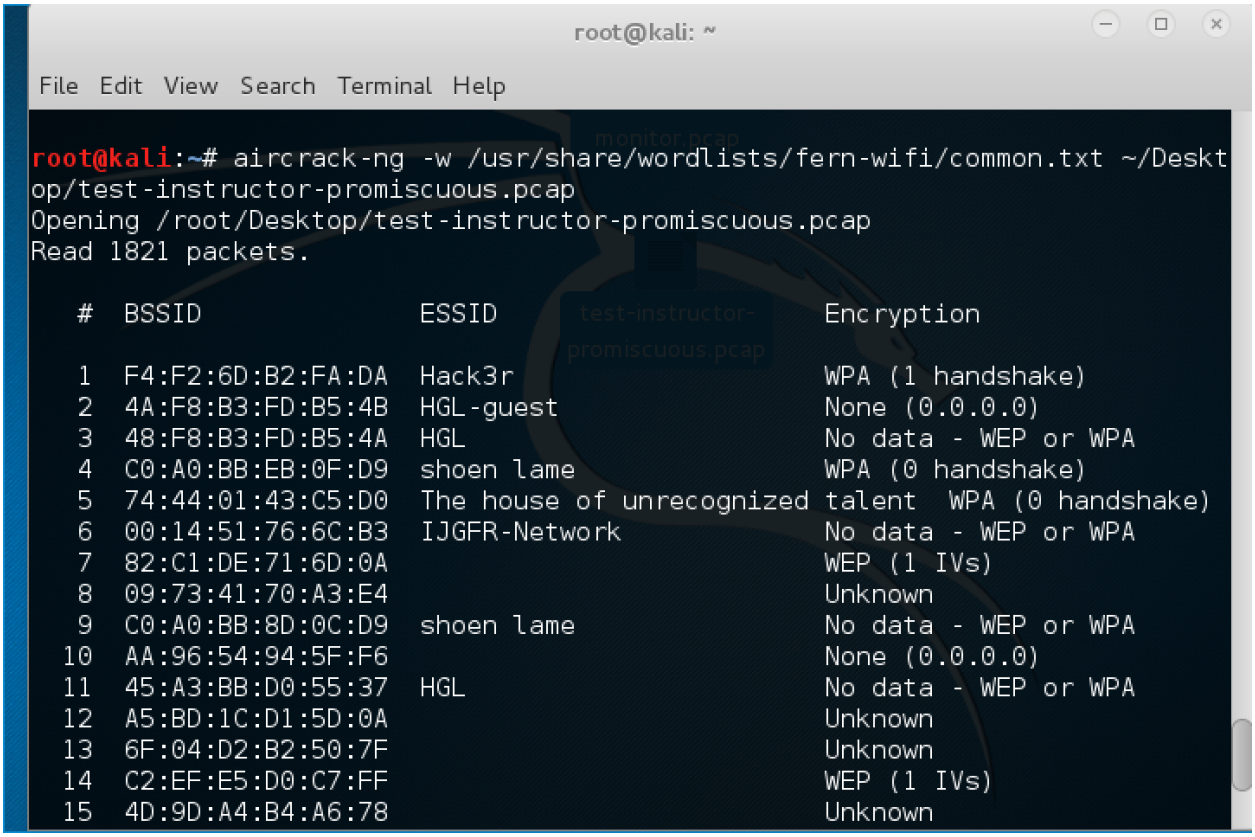


Then, we choose index for the WPA2 handshake. We can identify the index by using the SSID. From the screenshot we can see that the index for “Hack3r” is 5.

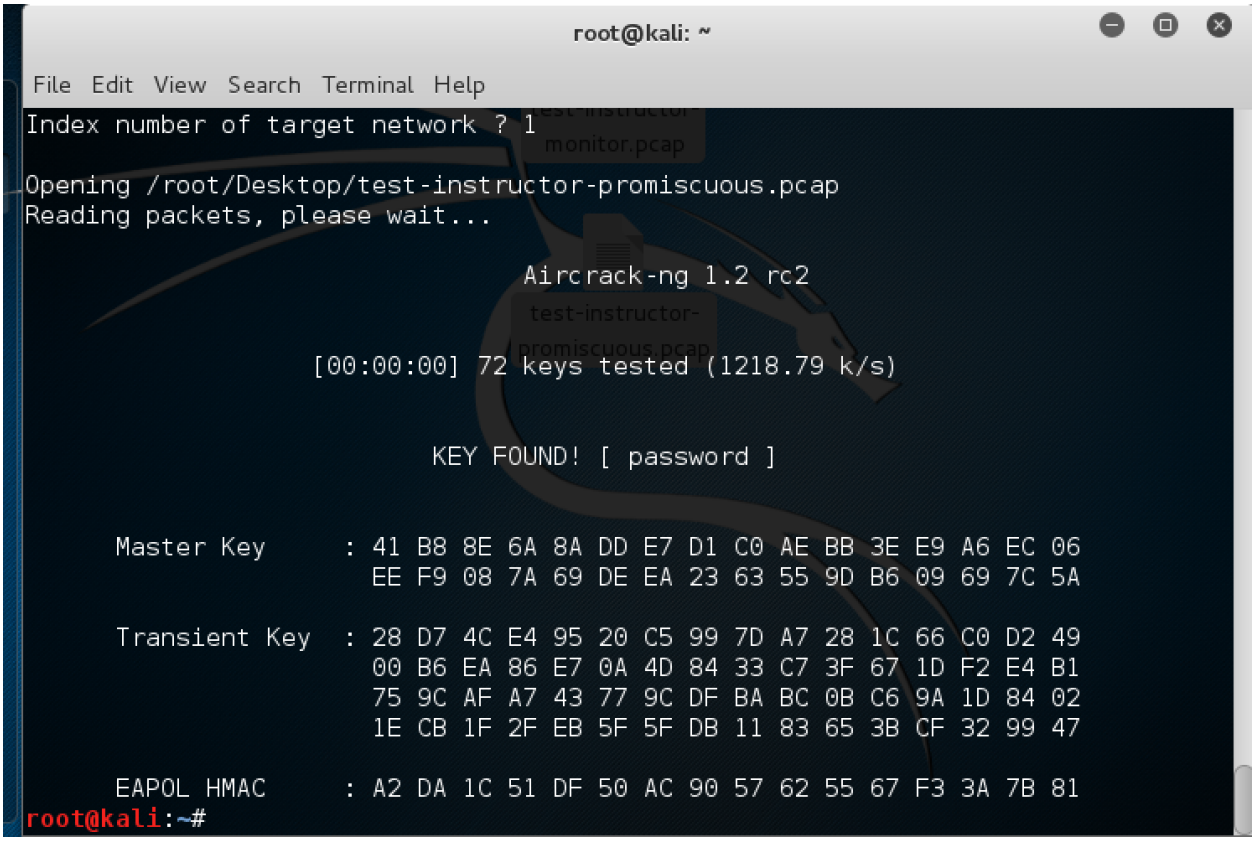
After enter 5, we can see that aircrack has successfully crack the passphrase as shown in the screenshot below.



Below are the screenshots for cracking the pcap file captured by monitor mode.



After selecting 1 as the target network interface, the screenshot below shows that the password has been cracked.



Assignments for Lab 6 Part 2

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 (3pt): Send a broadcast de-authentication packet to force clients to reconnect. Then you can capture the four-way handshake.

Happy Hacking!