



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Hacking Wireless Networks

**Faculty of Architecture, Computing &
Engineering
School of Applied Computing
IQ Building, Room 205
Swansea
SA1 8EW**

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to application and data throughout a radio network.

Task 1: WiFi Packet Sniffing Using AirPcap with Wirehark

The AirPcap adapter is a USB device that, when used in tangent with the AirPcap drivers and WinPcap libraries, allows a pen tester to monitor 802.11b/g traffic in monitor mode.

Lab Scenario

Wireless networks can be open to active or passive attacks. These attacks include DoS, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab, we discuss Wireshark, a tool that can sniff s network using a wireless adapter. Because you are the ethical hacker and penetration tester of an organization, you need to check the wireless security, exploit the flaws in WEP, and evaluate weaknesses present in the WEP of your organization.

Lab Objectives

The objective of this lab is to help students learn and understand how to:

- Discover WEP packets

Pre- Activity exercise

To carry out the lab, you need:

- To install AirPcap adapter drivers located in the Shared OneDrive. Enable Open Source Tools and double click setup_airpcap_4_1_1.exe to install
- When you are installing the AirPcap adapter drivers, if any installation error occurs, install the AirPcap adapter drivers in compatible mode (right-click AirPcap adapter driver exe file, select properties → compatibility, check Run this program in compatibility mode for, and select Windows 7)

- Wireshark should already running on all machine but you may need to download and install in the virtual machine. (All labs are recommended to use the VM environment and there may be ITS restrictions using the normal lab PCs)
- An access point configured with WEP on the host machine
- This lab requires AirPcap adapter installed on your machine. If you don't have this adapter, it is recommended not to proceed.
- A standard AirPcap adapter with its drivers installed on your host machine.
- Administrative privileges to run AirPcap and other tools.
- A client connected to a wireless access point

Overview of WEP (Wired Equivalent Privacy)

Several serious weaknesses in the protocol have been identified by cryptanalysts with the result that, today, a WEP connection can be easily cracked. Once entered into a network, a skilled hacker can modify software, network settings, and other security setting.

WEP is a deprecated security algorithm for IEEE 802.11 wireless networks.

Activity:

Note: Screenshot may varies from the one in this lab.

Download AirPcap drivers from the site and follow the steps to install AirPcap drivers.

1. Plug in the AirPcap device in a USB port and wait for the hardware installation to complete.
2. Launch the **AirPcap Control Panel** application from the **Apps** screen.

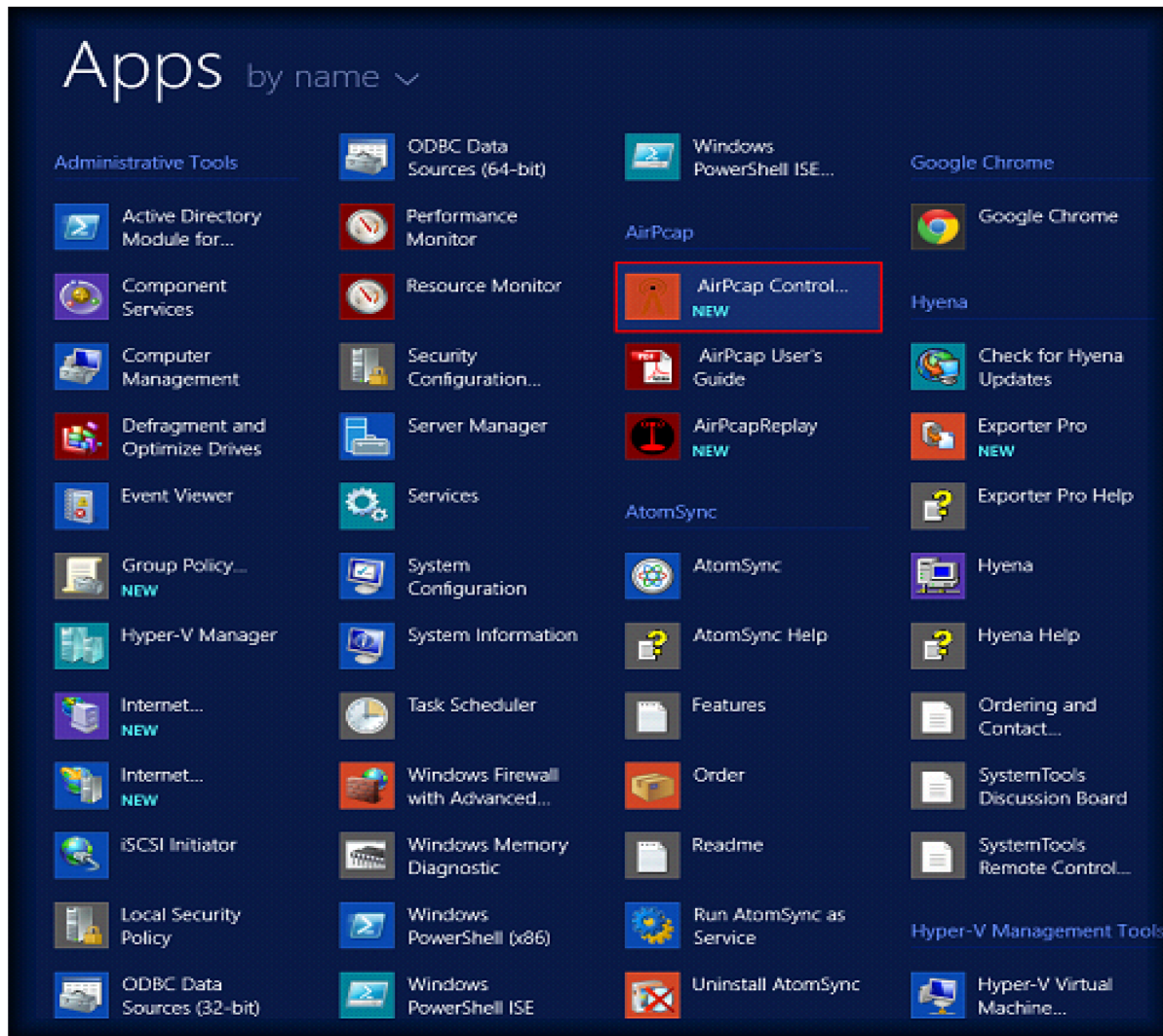


FIGURE 1.1: Launching AirPcap Control Panel application from the Apps screen

3. The **AirPcap Control Panel** window appears, as shown in the screenshot:

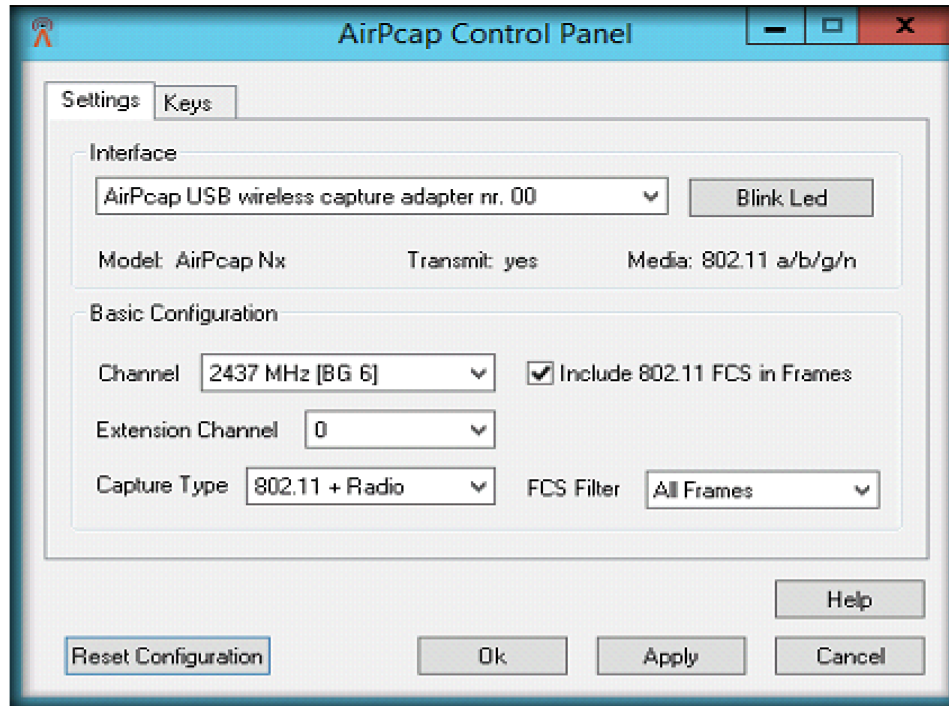


FIGURE 1.2: AirPcap Control Panel window

4. In the **Basic Configuration** section, select a suitable **channel** from the **Channel** drop-down list, and set a frequency you want to capture from the **Capture Type** drop-down list.

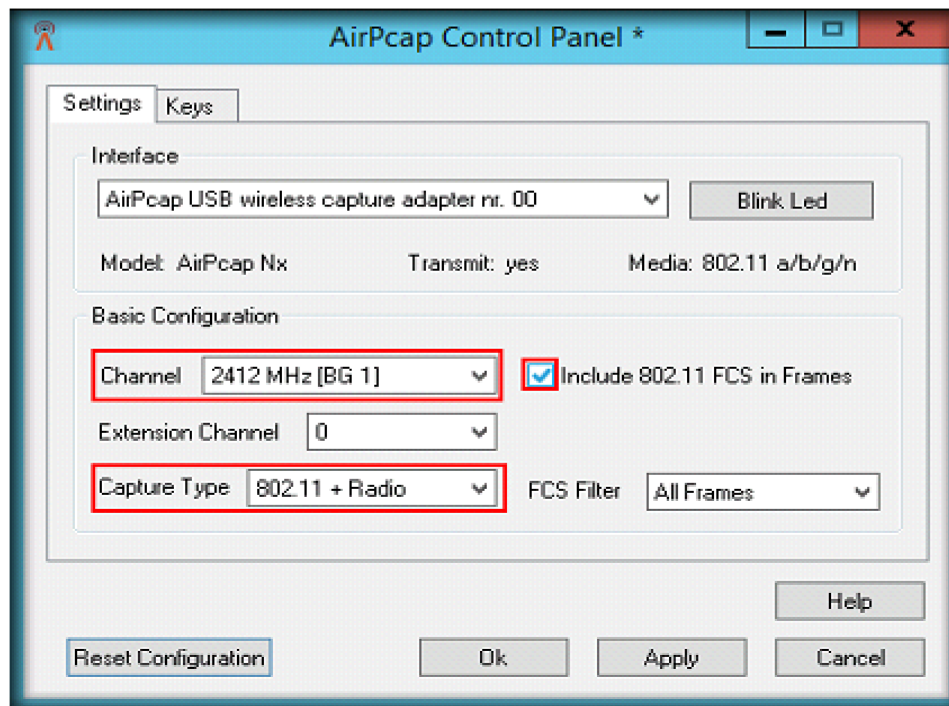


FIGURE 1.3: Configuring AirPcap Control Panel

5. Click the **Keys** tab. Ensure that the **Enable WEP Decryption** check box is selected. This enables the WEP decryption algorithm. You can **Add New Key**, **Remove Key**, **Edit Key**, and **Move Key UP or Down**.
6. After configuring settings and keys, click **OK**.

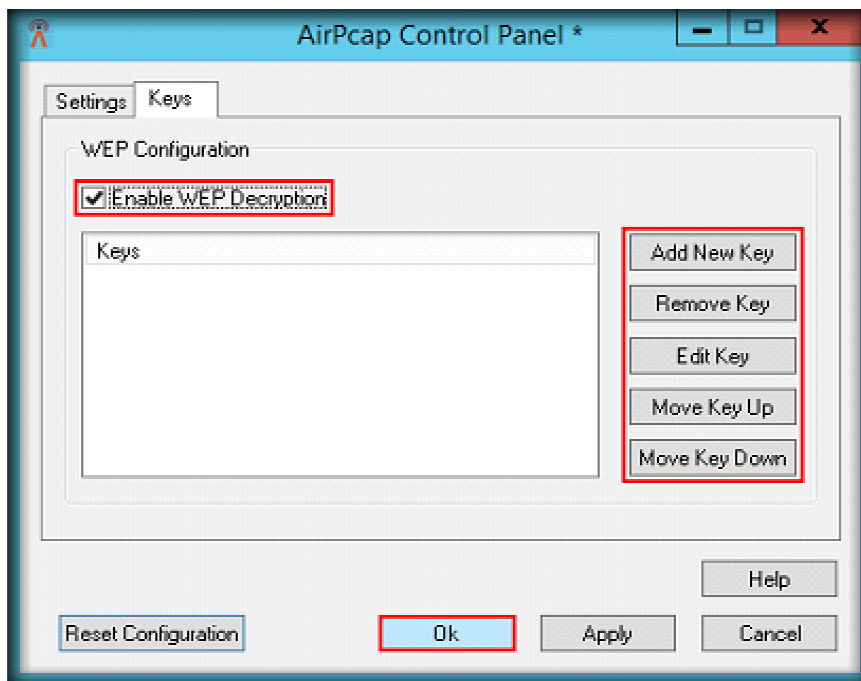


FIGURE 1.4: Configuring AirPcap Control Panel

7. Launch **Wireshark Network Analyzer** from the **Apps** screen. The **Wireshark** main window appears, as shown in the following screenshot:

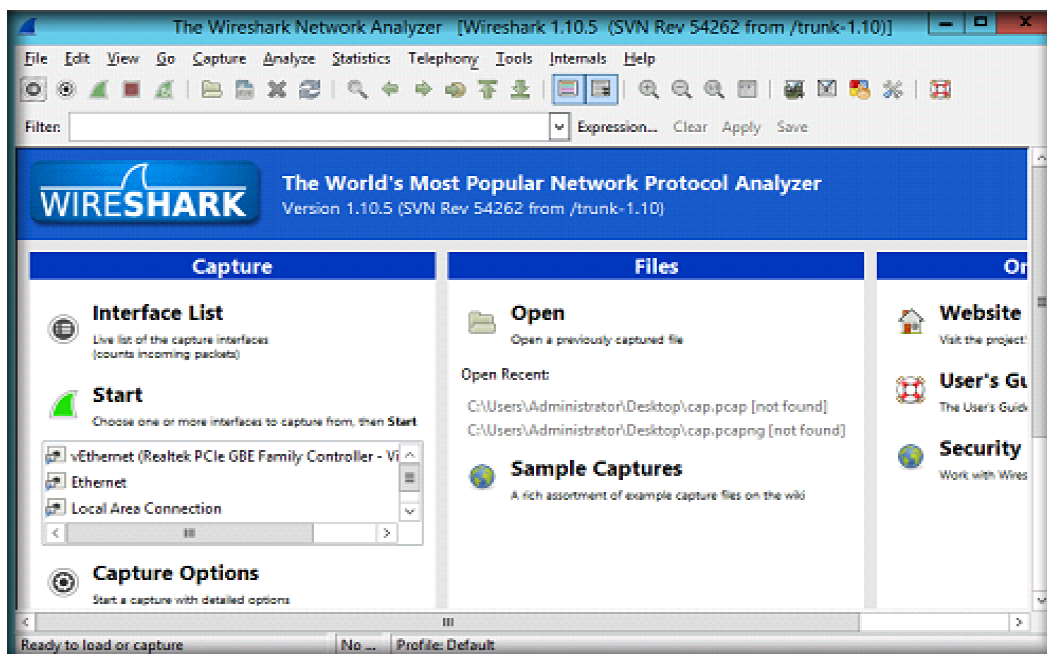


FIGURE 1.5: Wireshark Network Analyzer main window

- Configure AirPcap as an interface to Wireshark. To do this, select **Capture** → **Interfaces....**

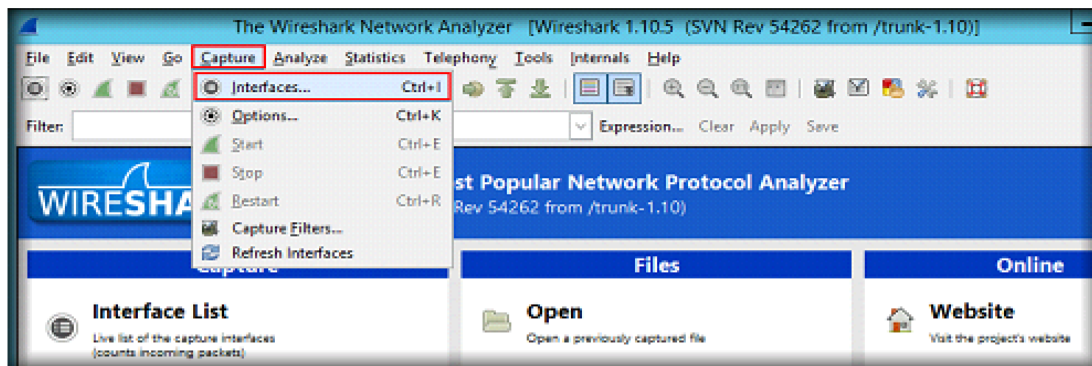


FIGURE 1.6: Wireshark Network Analyzer with interface option

- The **Wireshark: Capture Interfaces** window appears. By default, the AirPcap adapter is not in running mode. Select the **Airpcap USB wireless capture adapter nr. 00** check box, and click **Start**.

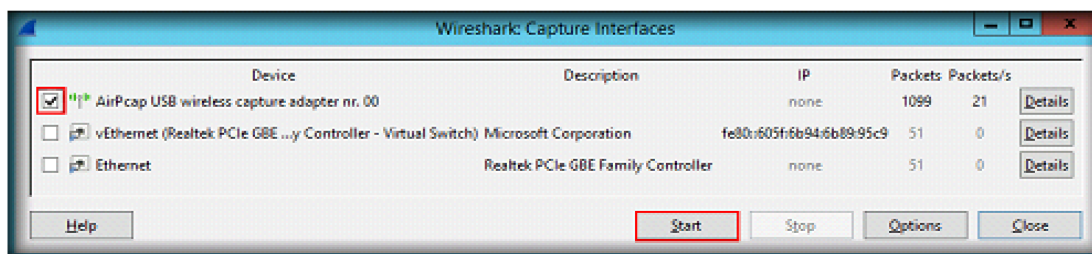


FIGURE 1.7: Wireshark: Capture Interface

- The Wireshark capture window appears and starts capturing wireless packets using the AirPcap Adapter, as shown in the following screenshot:

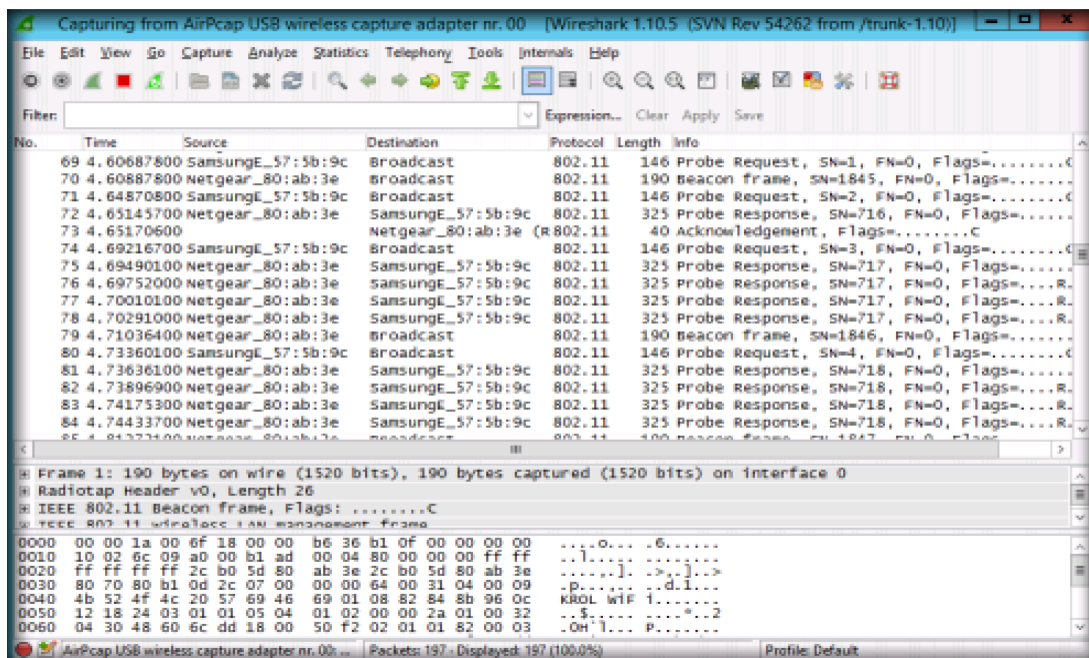


FIGURE 1.8: Wireshark Network Analyzer window with packets captured

11. You will be able to view the **source** and **destination** of the packets captured by Wireshark.

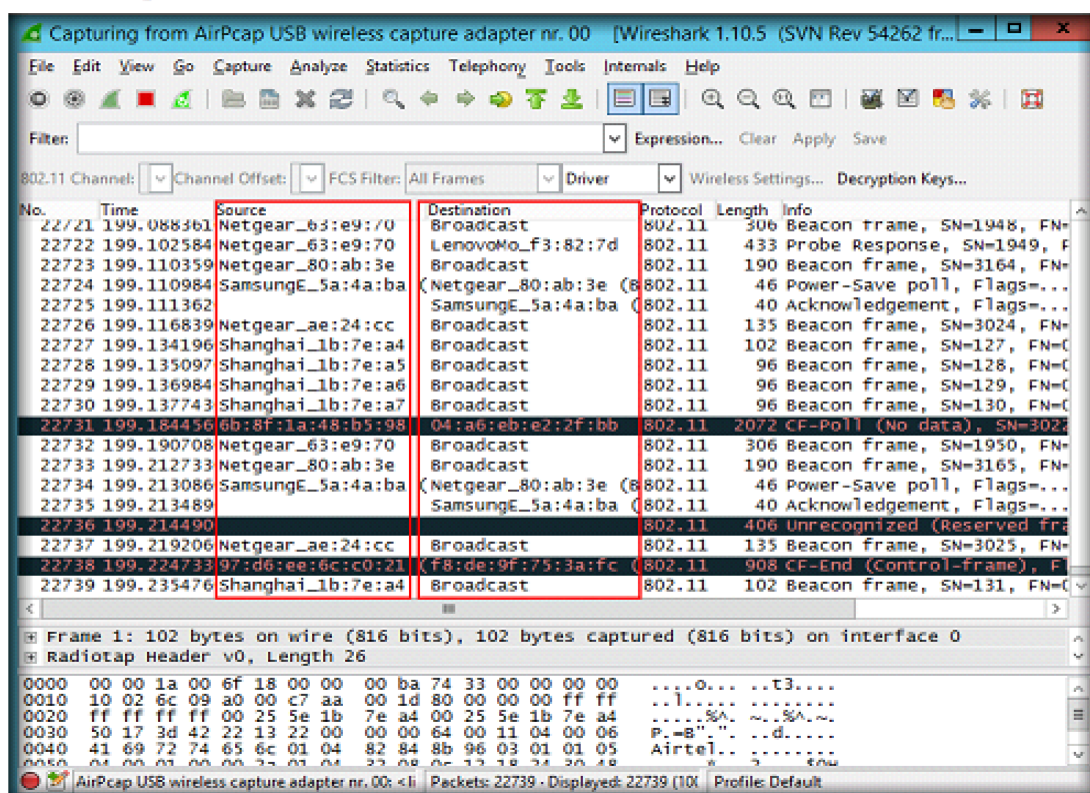


FIGURE 1.9: Wireshark Network Analyzer window with 802.11 channel captured packets

12. After capturing enough number of packets, stop Wireshark by clicking the  icon in the Wireshark toolbar.

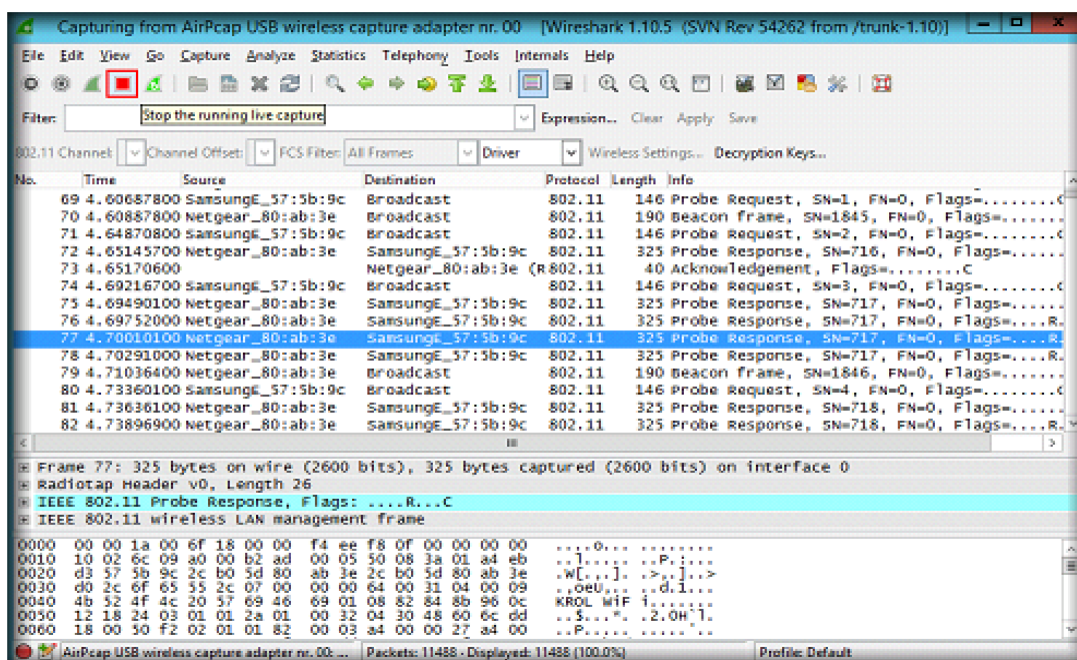


FIGURE 1.10: Stop Wireshark packet capture

13. Go to **File** in the menu bar, and select **Save**.

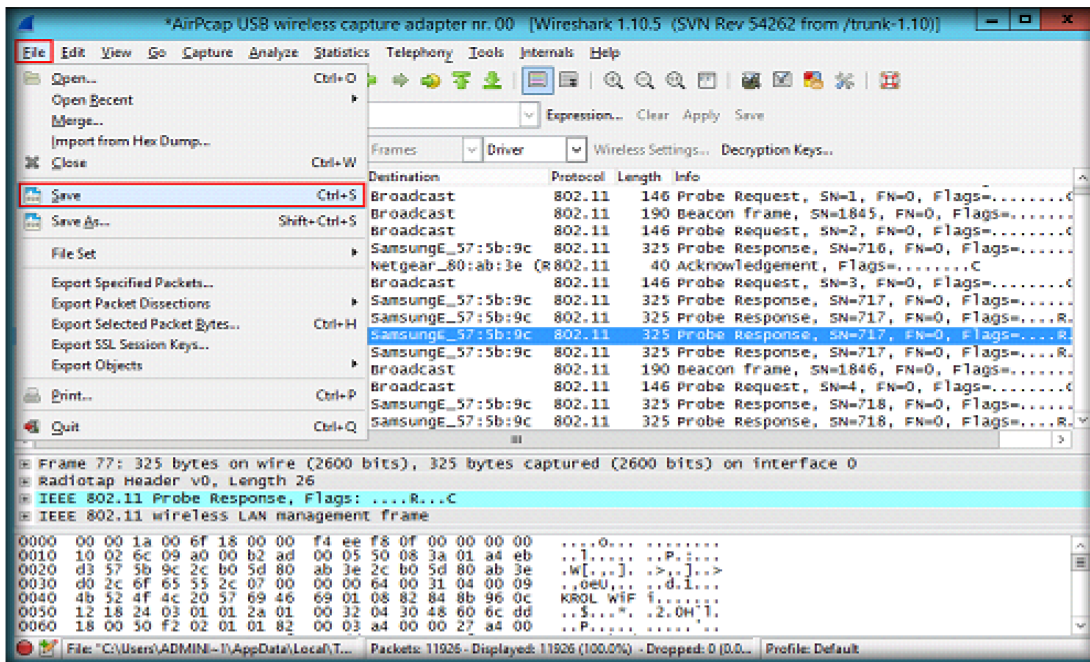


FIGURE 1.11: Save the captured packets

14. Enter the **File name**, and click **Save**.

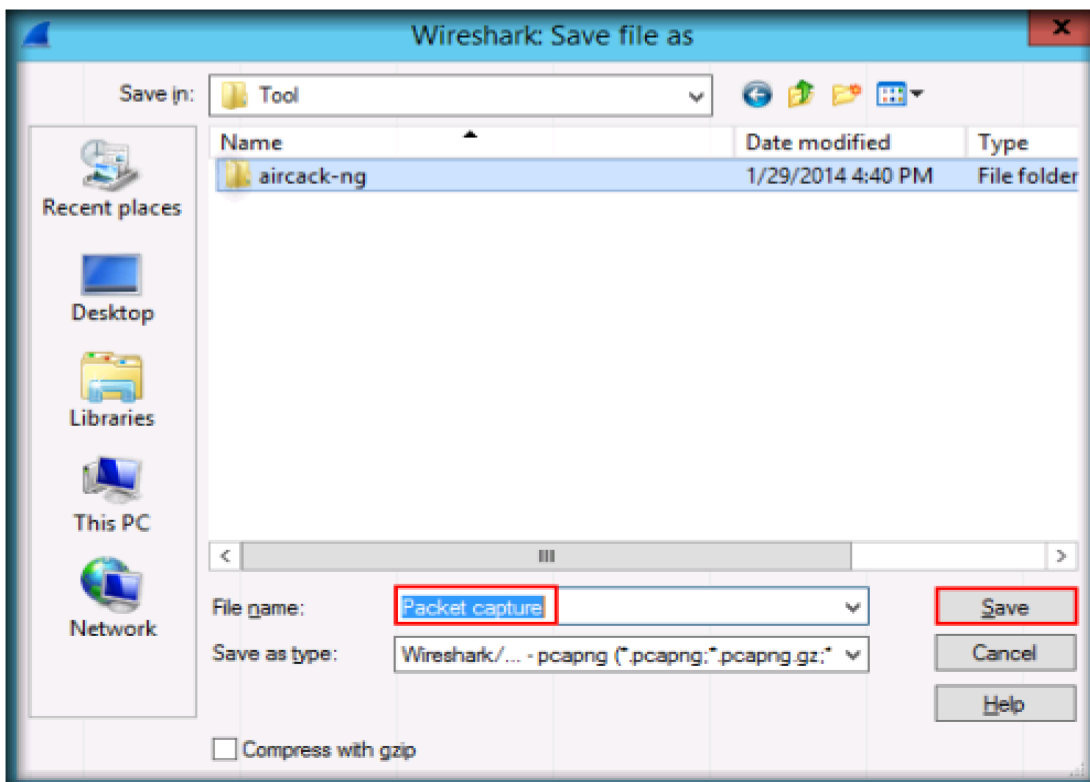


FIGURE 1.12: Save the Captured packet file

15. You can access the saved packet capture file anytime, and by issuing packet filtering commands in the Filter field, you can narrow down the packet search in an attempt to find packets containing sensible information.
16. In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

Task 2: Cracking a WEP Network with Aircrack-ng for Windows

Aircrack-ng is an 802.11 WEP and WPA-PSK keys-cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, and the all-new PTW attack, thus making this attack much faster than those using other WEP cracking tools.

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, attackers will descend in droves to test your wireless network with it.

WEP is used for wireless networks; always change your SSID from the default, before you actually connect the wireless router for the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used, because war-driving tools can easily detect your internal IP addressing if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in your organization's WEP. In this lab, we discuss how WPA keys are cracked using standard attacks such as KoreK and PTW.

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Pre- Activity exercise

To carry out the lab, you need:

- MovieScope website configured during the lab setup
- GoodShopping website configured during the lab setup
- Windows host machine
- Windows Server2008 or Windows 7 or Windows 10an Attacker Machine
- Windows Server2008 or Windows 7 or Windows 10 as a Victim Machine
- Microsoft SQL server 2012 or later
- A web browser with an Internet connection

Overview

A “wireless network” is any type of computer telecommunications network, the interconnections between the nodes of which are made without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier, and this implementation usually takes place at the physical level, or layer, of the network.

Activity:

1. Launch airodump-ng (a subset of aircrack-ng suite) GUI from the shared oneDrive by7 double-clicking airodump-ng-airpcap.exe.
2. If the Open-File Security Warning pop-up appears, click run.

3. The **airodump-ng** GUI appears, as shown in the following screenshot:

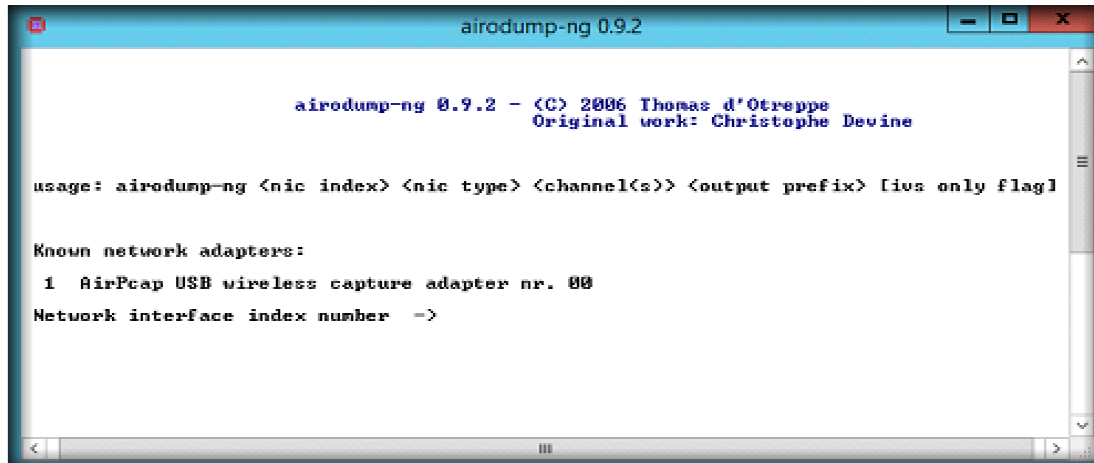


FIGURE 3.1: Airodump-ng selecting adapter window

4. Type the Airpcap adapter index number **0** and select channel number **0**. Then press **Enter**.
5. Channel 0 refers to all the 2.4 GHz channels. In this lab, we are configuring airodump-ng to capture 2.4 GHz channels.

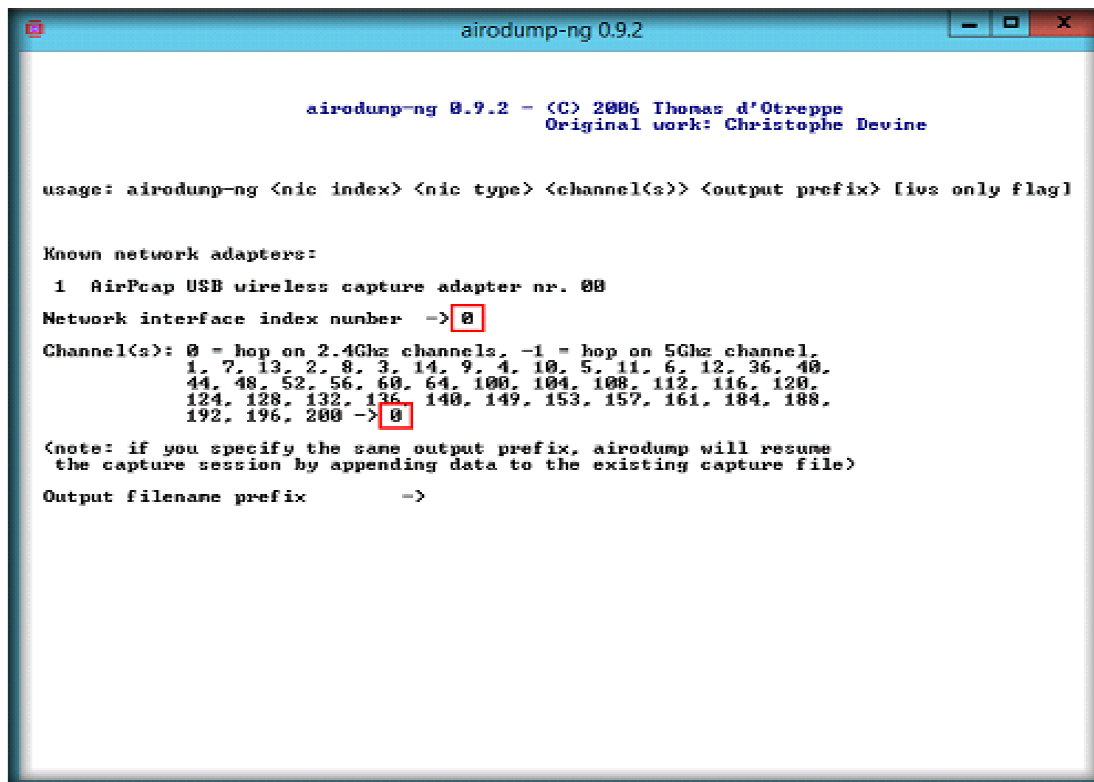


FIGURE 3.2: Airodump-ng selecting adapter window

- It will prompt you for a file name. Specify the name as **capture** and press **Enter**.
- Type **y** in **Only write WEP IVs**. Press **Enter**.

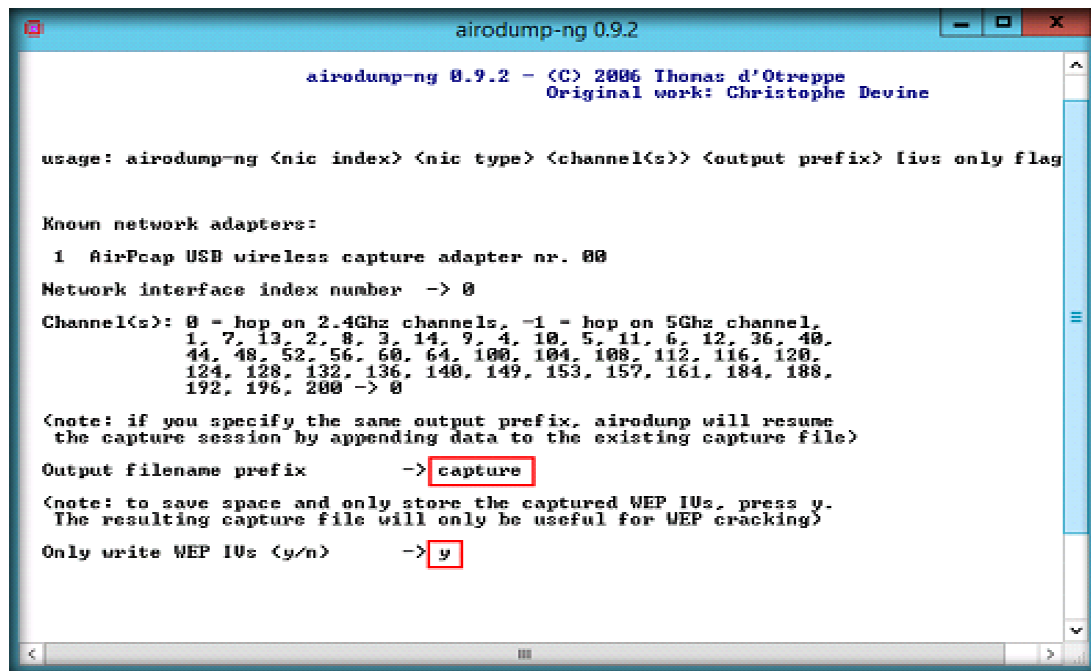


FIGURE 3.3: Airodump-ng assigning output filename

- Airodump-ng begins to capture the wireless traffic, as shown in the following screenshot.
- Allow airodump-ng to capture a large number of packets (above 2,000,000).

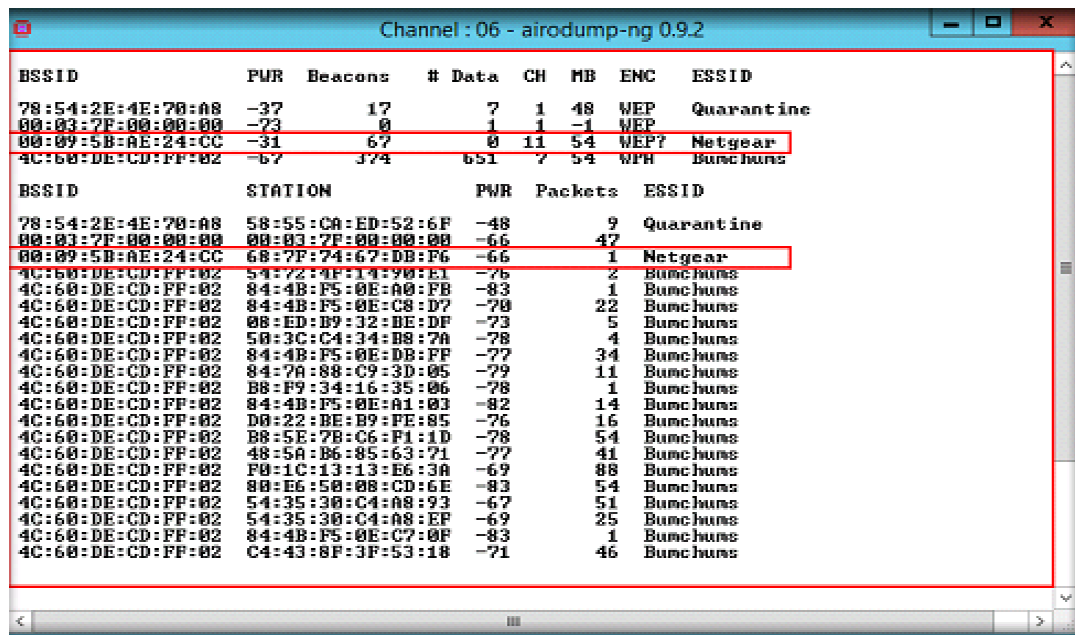


FIGURE 3.4: Airodump-ng capture window

10. Because airodump-ng requires a lot of time to capture enough number of packets and IVs, we are providing a sample capture file that contains the required number of packets and IVs in order to save time. Close the capture window by pressing **Ctrl+C**.
11. Navigate to **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin** and double-click **Aircrack-ng GUI.exe** to launch **Aircrack-ng**. Then click **Choose...**.

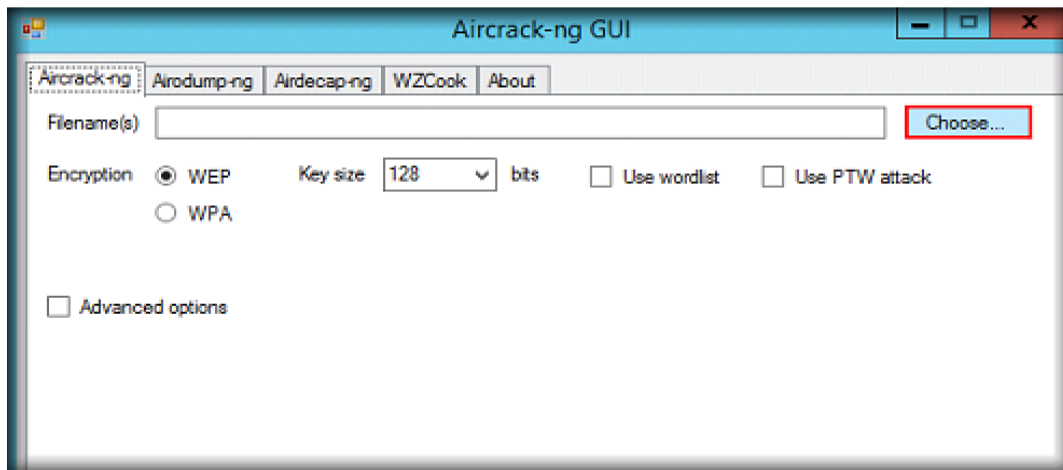


FIGURE 3.5: Aircrack-ng main window

12. The **Open** window appears; navigate to **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng**, select **wepcapture.cap**, and click **Open**.

Note: This is a different file from the one you recorded; this file contains pre-captured IVS keys.

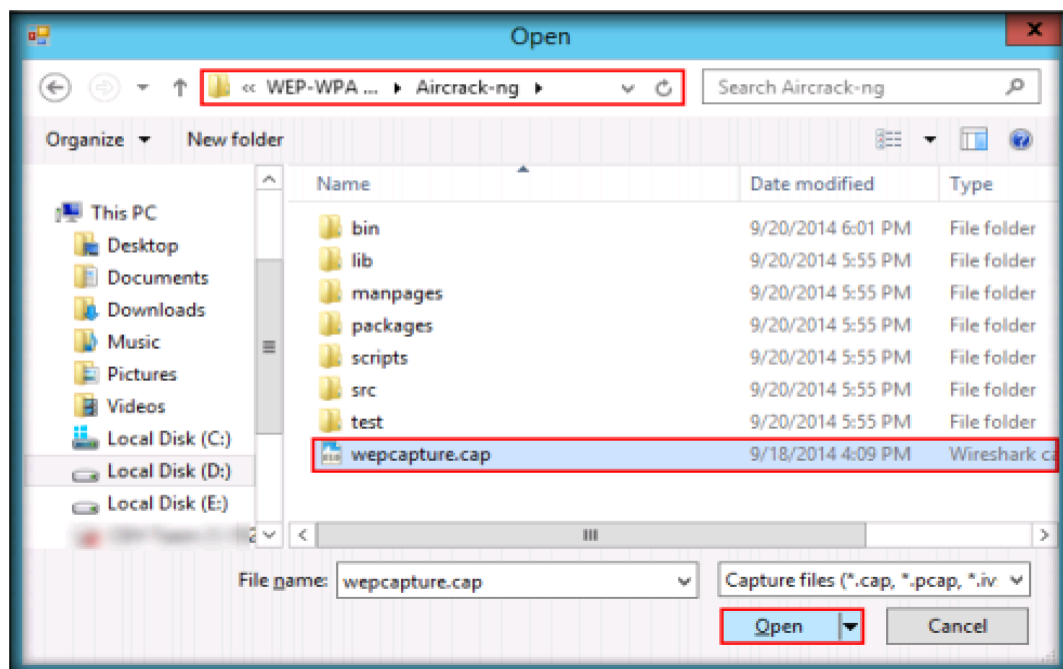


FIGURE 3.6: Selecting the pre-captured file

13. After selecting the file, click **Launch**.

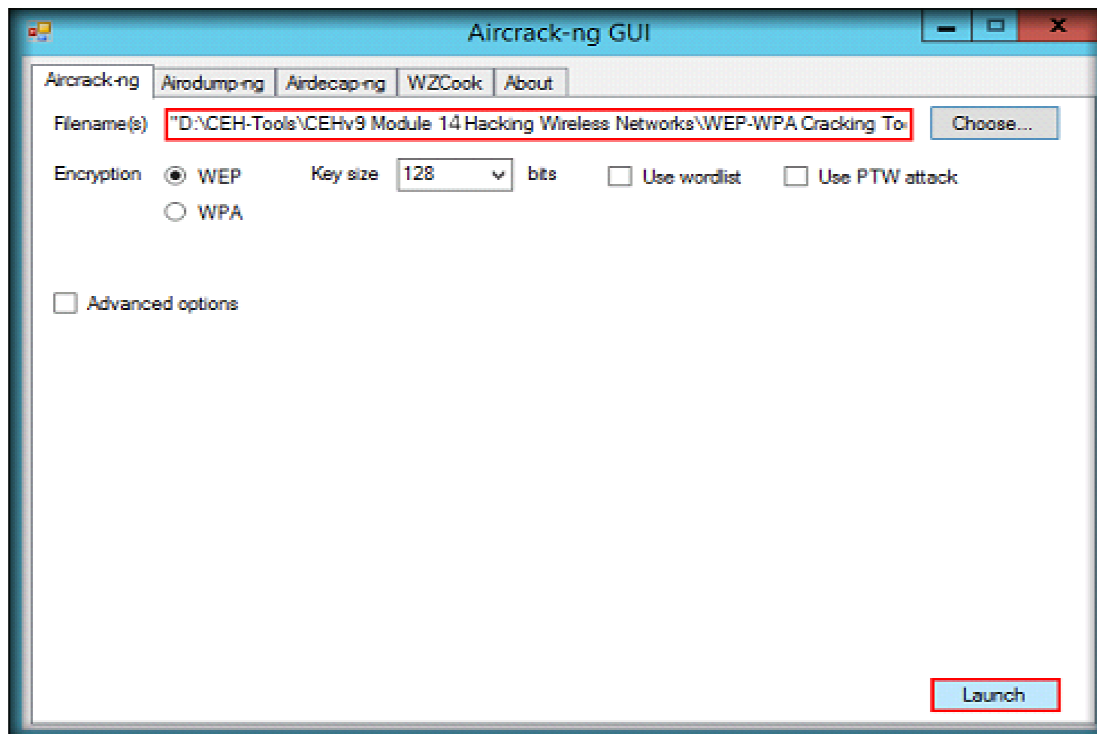


FIGURE 3.7: Aircrack-ng launch window

14. Aircrack-ng begins to decode the capture file, as shown in the following screenshot:

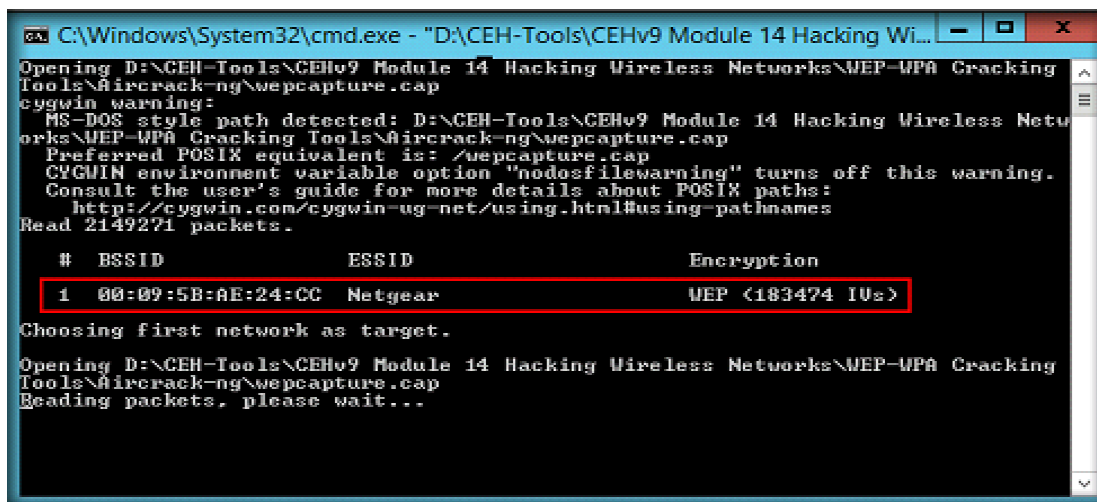
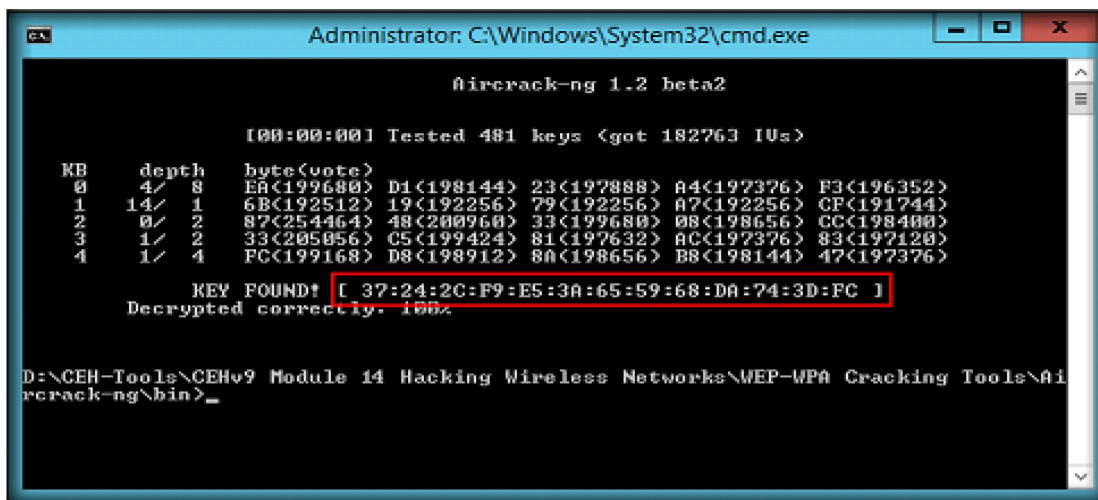


FIGURE 3.8: Aircrack-ng decrypting the key

15. On successfully decoding the file, it displays the key shown in the following screenshot:



```
Administrator: C:\Windows\System32\cmd.exe

aircrack-ng 1.2 beta2

[00:00:00] Tested 481 keys <got 182763 IVs>

KB    depth  byte(s)
0      4/ 8    EA<199680> D1<198144> 23<197888> A4<197376> F3<196352>
1     14/ 1    6B<192512> 19<192256> 79<192256> A7<192256> CF<191744>
2      0/ 2    87<254464> 48<200760> 33<199680> 08<198656> CC<198400>
3      1/ 2    33<205056> C5<199424> 81<197632> AC<197376> 83<197120>
4      1/ 4    FC<199168> D8<198912> 8A<198656> B8<198144> 47<197376>

KEY FOUND! [ 37:24:2C:F9:E5:3A:65:59:68:DA:74:3D:FC ]
Decrypted correctly. 100%

D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\aircrack-ng\bin>
```

FIGURE 3.9: aircrack-ng with WEP crack key

16. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for open devices, perform vulnerability analysis, and then start exploiting them.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Aircrack-ng attacks and their respective data packet generation rate.