





# **Hacking Wireless Networks**

## **Module 15**

# Hacking Wireless Networks

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

## ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

## Lab Scenario

Wireless network technology is becoming increasingly popular but, at the same time, it has many security issues. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. However, the convenience of WLANs also introduces security concerns that do not exist in a wired world. Connecting to a network no longer requires an Ethernet cable. Instead, data packets are airborne and available to anyone with ability to intercept and decode them. Several reports have explained weaknesses in the Wired Equivalent Privacy (WEP) algorithm by 802.11x standard to encrypt wireless data.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of wireless concepts, wireless encryption, and their related threats. As a security administrator of your company, you must protect the wireless network from hacking.

## Lab Objectives

The objective of this lab is to protect the 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

## Lab Environment

In the lab you will need a web browser with an Internet connection.


- This lab requires **AirPcap** adapter installed on your machine for all labs

## Lab Duration

Time: 30 Minutes

## Overview of Wireless Network

A wireless network refers to any type of computer network that is **wireless** and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented 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

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks**

radio waves for the **carrier**. The implementation usually takes place at the physical level or layer of the network.



#### TASK 1

##### Overview

## Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in Wireless Networks:

- WiFi Packet Sniffing Using AirPcap with Wireshark
- Cracking a WEP Network with Aircrack-ng for Windows
- Sniffing the Network Using the OmniPeek Network Analyzer

## Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS  
RELATED TO THIS LAB.

---




## WiFi Packet Sniffing Using AirPcap with Wireshark

*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.*

### ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

### Lab Scenario

Wireless networks can be open to active and also passive attacks. These types of 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 the Wireshark tool, which can sniff the network using a wireless adapter. Since 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 WEP for your organization.

### Lab Objectives

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

- Discover WEP packets

## Lab Environment

 **Tools**  
demonstrated in  
this lab are  
available in  
**D:\CEH-  
Tools\CEHv8  
Module 15  
Hacking Wireless  
Networks**

To execute the lab, you need:

- Install AirPcap adapter drivers; to install navigate to **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled 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 compatibility mode (right-click the **AirPcap adapter driver** exe file, select **Properties** → **Compatibility**, in compatibility mode, and select **Windows7**)
- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\wireshark-win64-1.4.4.exe**
- Run this lab in Windows Server 2012 (host machine)
- An access point configured with WEP on the host machine
- **This lab requires the AirPcap adapter installed on your machine. If you don't have this adapter, please do not proceed with this lab**
- A standard AirPcap adapter with its drivers installed on your host machine
- WinPcap libraries, Wireshark, and Cain & Abel installed on your host machine
- Administrative privileges to run AirPcap and other tools



- A client connected to a wireless access point

## Lab Duration

Time: 15 Minutes

## 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

onto a network, a skilled hacker can **modify** software, **network settings**, and other **security** settings.

Wired Equivalent Privacy (WEP) is a deprecated security **algorithm** for IEEE 802.11 wireless networks.

### TASK 1

#### Configure AirPcap

You can download AirPcap drivers from <http://www.airdemon.net/riverbed.html>

## Lab Tasks

Download AirPcap drivers from the site and follow the wizard-driven installation steps to install AirPcap drivers.

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

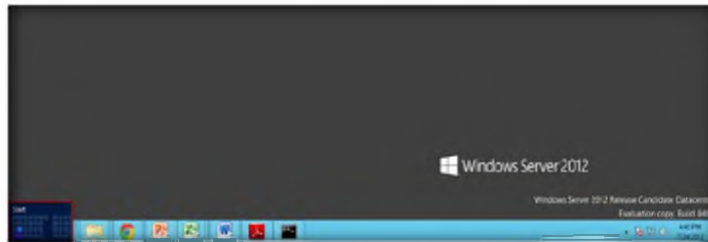


FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **AirPcap Control Panel** app to open the **AirPcap Control Panel** window.

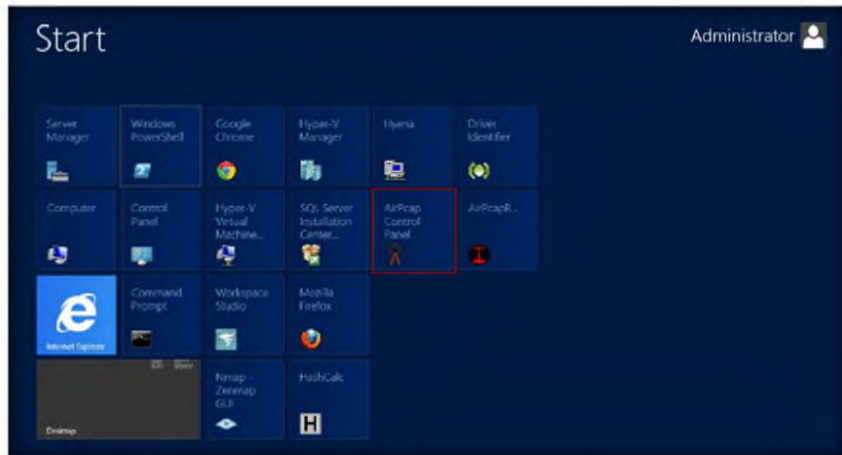


FIGURE 1.2: Windows Server 2012 – Apps

3. The **AirPcap Control Panel** window appears.

The AirPcap adapters can work in monitor mode. In this mode, the AirPcap adapter captures all of the frames that are transferred on a channel, not just frames that are addressed to it.

The Multi-Channel Aggregator can be configured like any real AirPcap device, and therefore can have its own decryption, FCS checking and packet filtering settings.

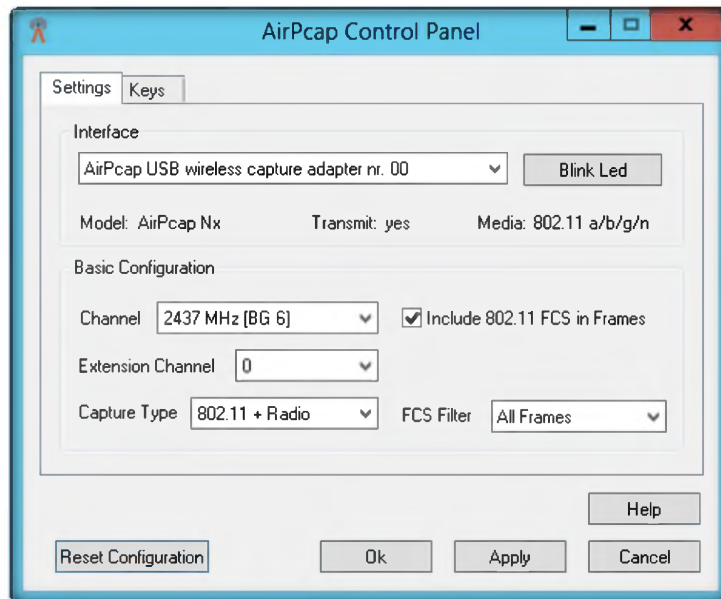


FIGURE 1.3: AirPcap Control Panel window

4. On the **Settings** tab, click the **Interface** drop-down list and select **AirPcap USB wireless capture adapter**.
5. In the **Basic Configuration** section, select suitable **Channel**, **Capture Type**, and **FCS Filter** and check the **Include 802.11 FCS in Frames** check box.

In Basic Configuration box settings: Channel: The channels available in the Channel list box depend upon the selected adapter. Since channel numbers 14 in the 2.4GHz and 5GHz bands overlap and there are center frequencies (channels) that do not have channel numbers., Each available channel is given by its center frequency.

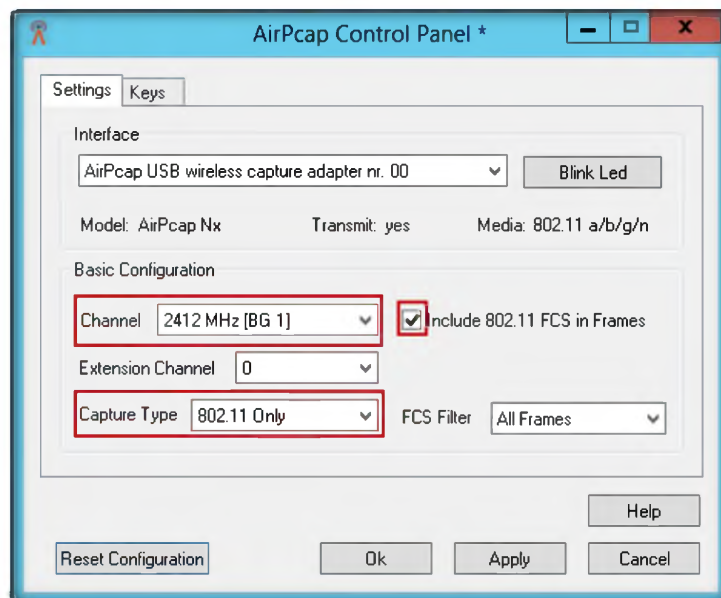



FIGURE 1.4: AirPcap Control Panel window

6. Now, click the **Keys** tab. Check the **Enable WEP Decryption** check box. This enables the WEP decryption algorithm. You can **Add New Key**, **Remove Key**, **Edit Key**, and **Move Key UP and Down**.



- After configuring settings and keys, click **OK**.

 In Basic Configuration Settings: Extension Channel: For 802.11n adapters, one can use the Extension Channel list to create a “wide” channel. The choices are -1 (the preceding 20MHz frequency band), 0 (no extension channel), or +1 (the succeeding 20MHz frequency band). The channel of the additional frequency band is called the extension channel.

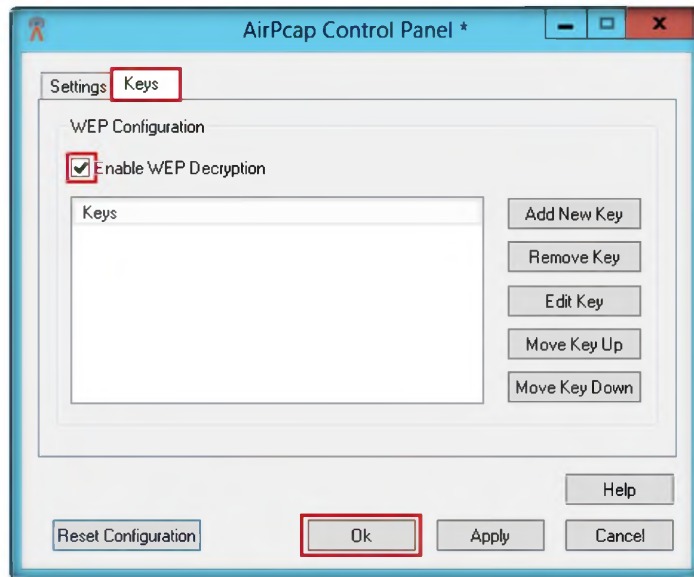



FIGURE 1.5: AirPcap Control Panel window

- Launch **Wireshark Network Analyzer**. The **Wireshark** main window appears.

### TASK 2 Capturing the packets

 You can download Wireshark from <http://www.wireshark.org>.

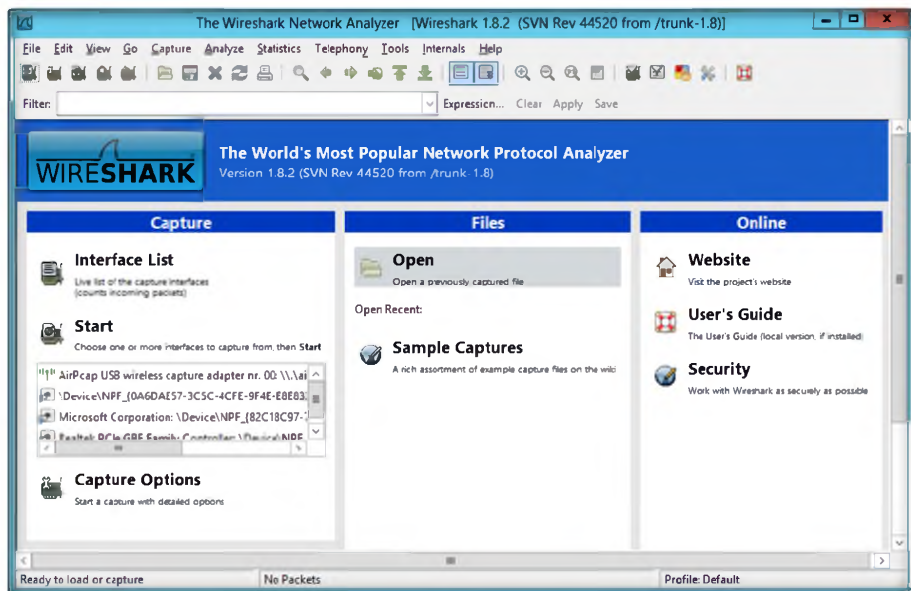



FIGURE 1.6: Wireshark Network Analyzer main window



The following are some of the many features Wireshark provides available for UNIX and Windows.

- Capture live packet data from a network interface.
- Display packets with very detailed protocol information.
- Open and Save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics

9. Configure AirPcap as an interface to Wireshark. Select **Capture** → **Interface... (Ctrl +I)**. You can also click the  icon on the toolbar.

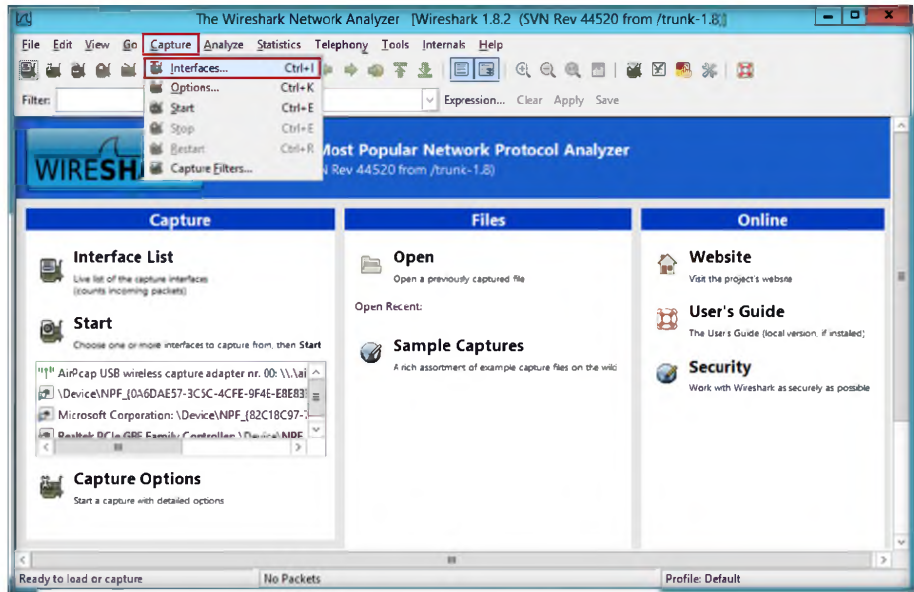


FIGURE 1.7: Wireshark Network Analyzer with interface option

10. 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. Click **Start**.

**Note:** Wireshark isn't an intrusion detection system. It does not warn you when someone does things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

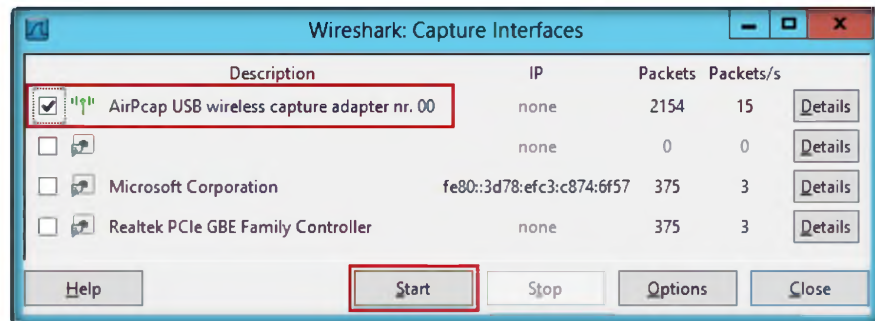


FIGURE 1.8: Wireshark: Capture Interface

11. Automatically, the **Capturing from AirPcap USB wireless capture adaptor nr. 00 – Wireshark** window appears, and it starts capturing packets from AirPcap Adapter.

## Module 15 – Hacking Wireless Networks



Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things, such as the operating system you are using.

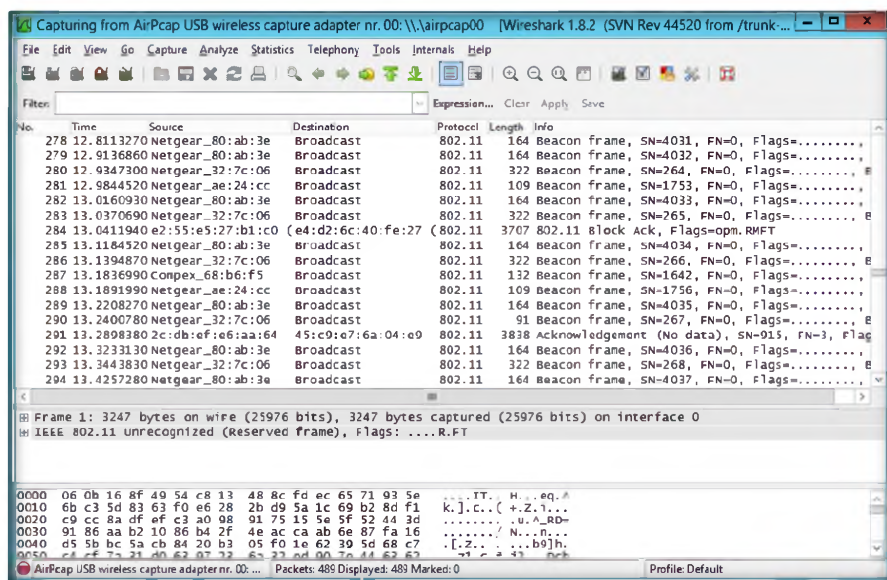


FIGURE 1.9: Wireshark Network Analyzer window with packets captured

- Wait while Wireshark captures packets from AirPcap. If the **Filter Toolbar** option is not visible on the toolbar, select **View → Filter Toolbar**. The Filter Toolbar appears.

**Note:** Wireshark doesn't benefit much from Multiprocessor/Hyperthread systems as time-consuming tasks, like filtering packets, are single threaded. No rule is without exception: During an “update list of packets in real time” capture, capturing traffic runs in one process and dissecting and displaying packets runs in another process, which should benefit from two processors.



Wireshark can open packets captured from a large number of other capture programs.

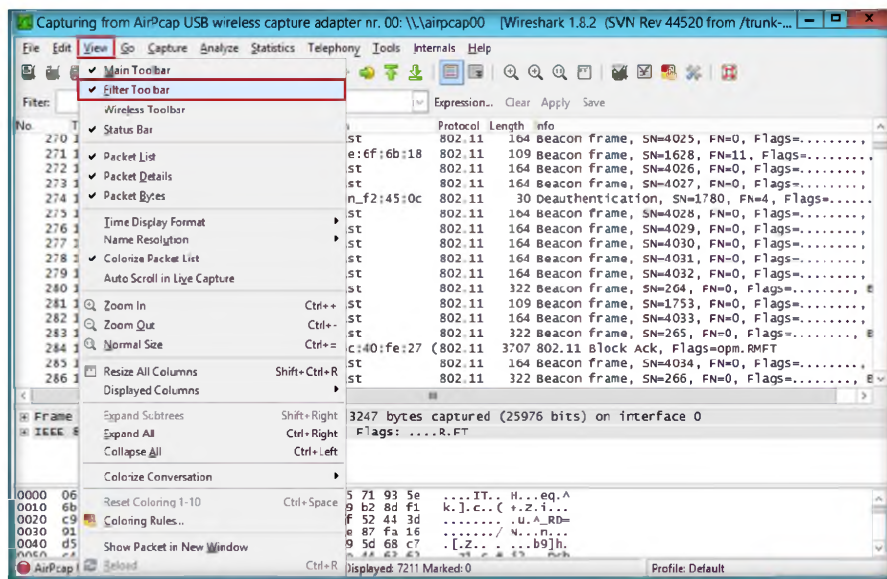


FIGURE 1.10: Wireshark Network Analyzer window with interface option

## Module 15 – Hacking Wireless Networks

- Now select **View → Wireless Toolbar**. The wireless toolbar appears in the window.

Wireshark is a network packet analyzer that captures network packets and tries to display that packet data as detailed as possible.

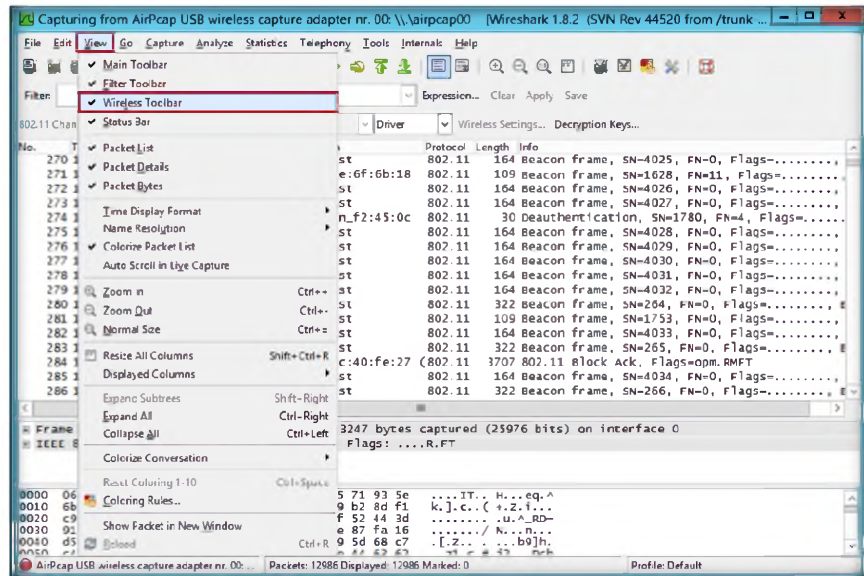


FIGURE 1.11: Wireshark Network Analyzer window with wireless toolbar option

- You will see the **source** and **destination** of the packet captured by Wireshark.

One possible alternative is to run tcpdump, or the dumpcap utility that comes with Wireshark, with superuser privileges to capture packets into a file, and later analyze these packets by running Wireshark with restricted privileges on the packet capture dump file

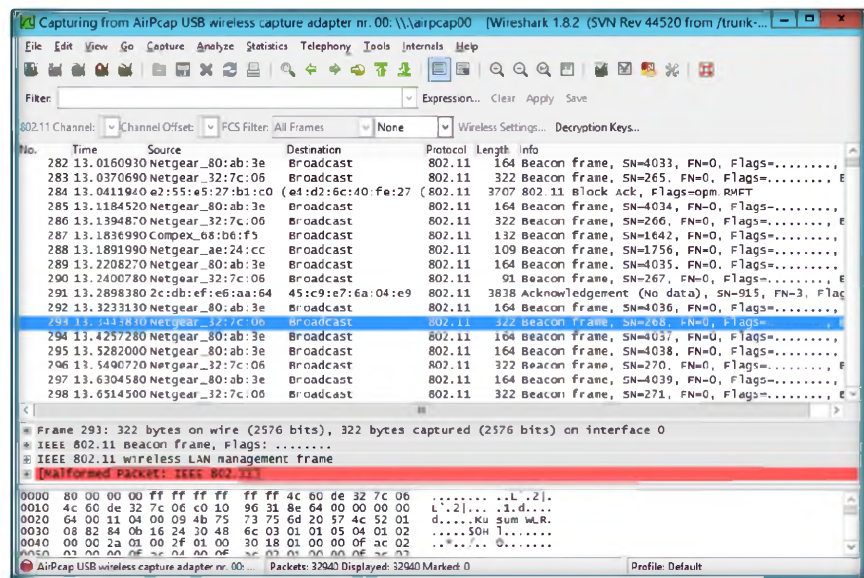


FIGURE 1.12: Wireshark Network Analyzer window with 802.11 channel captured packets

- After enough packet captures, stop Wireshark





## Module 15 – Hacking Wireless Networks

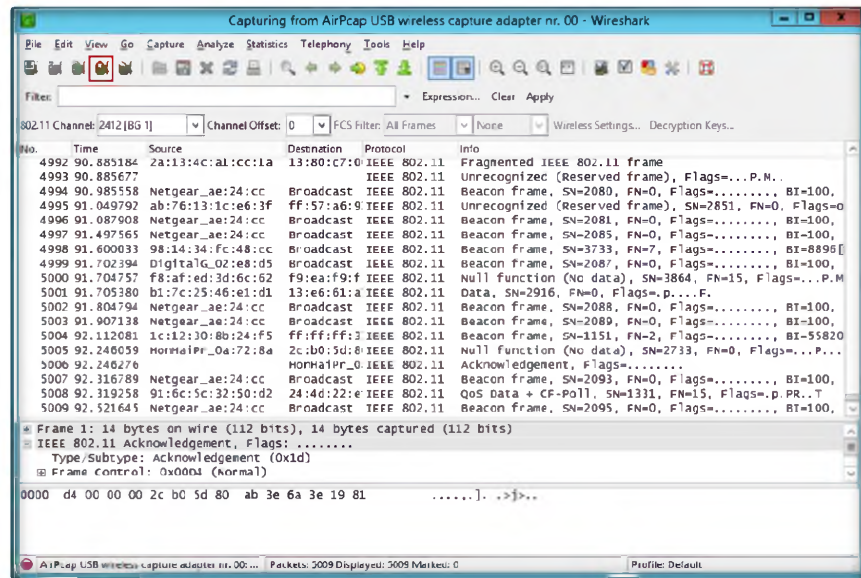


FIGURE 1.13: Stop Wireshark packet capture

- Go to **File** from menu bar, and select **Save**.

The latest version is faster and contains a lot of new features, like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

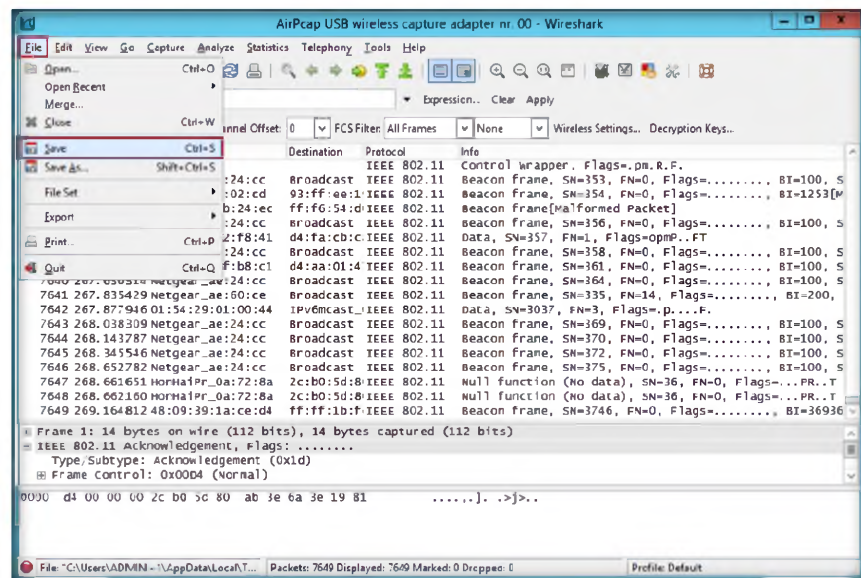


FIGURE 1.14: Save the captured packets

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

Module 15 – Hacking Wireless Networks

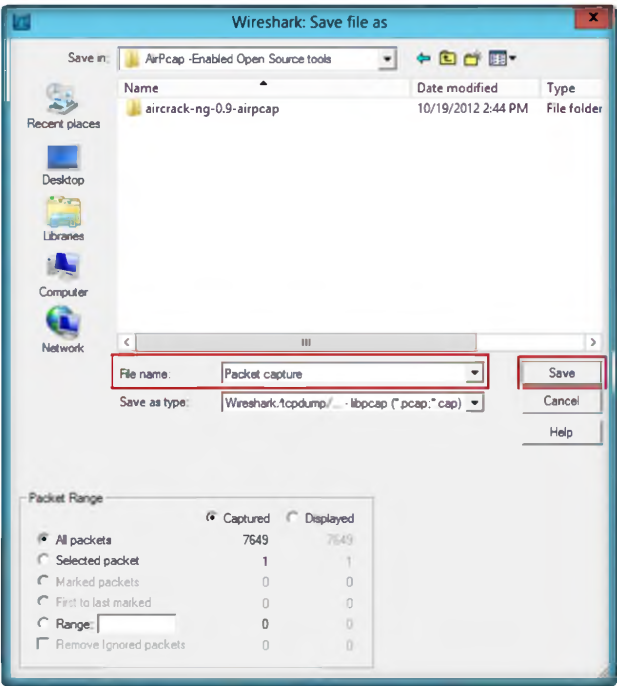


FIGURE 1.15: Save the Captured packet file

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target’s security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Wireshark	<b>Used Adapter:</b> AirPcap USB wireless capture adapter nr.00
	<b>Result:</b> Number of sniffed packets captured by Wireshark in network, which include: Packet Number, Time, Source, Destination, Protocol, and Info

## Questions

1. Evaluate and determine the number of wireless cards supported by the wireless scanner.
2. Analyze and evaluate how AirPcap adapters operate.





Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



## 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, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.*


### ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

### 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, they will come 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 WEP of an organization. In this lab we discuss how WPA key are cracked using standard attacks such as korek attacks and PTW attacks.

 **Tools demonstrated in this lab are available on D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks**

### 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



## Lab Environment

To execute the lab, you need:

- **Aircrack-ng** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin**
- This tool requires Administrative privileges to run
- A client connected to a wireless access point
- **This lab requires AirPcap adapter installed on your machine. If you don't have this adapter please do not proceed with the lab**

Visit Backtrack home site <http://www.backtrack-linux.org> for a complete list of compatible Wi-Fi adapters.

## Lab Duration

Time: 20 Minutes

## Overview of Aircrack-ng

Airplay filter options: -b bssid: MAC address, access point.

A wireless network refers to any type of computer network that is **wireless**, and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented 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.

### TASK 1

#### Cracking a WEP Network

1. Launch **Aircrack-ng GUI** from **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap\bin** by double-clicking **Aircrack-ng GUI.exe**.
2. Click the **Airdump-ng** tab.

To start wlan0 in monitor mode type:  
airmon-ng start wlan0.

To stop wlan0 type:  
airmon-ng stop wlan0.

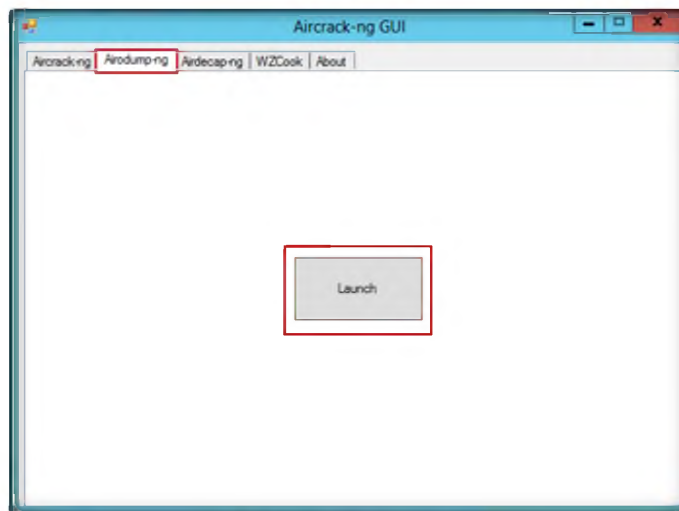



FIGURE 2.1: Airdump-ng window

## Module 15 – Hacking Wireless Networks

3. Click **Launch**. This will show the **airodump-ng** window.

 To confirm that the card is in monitor mode, run the command “iwconfig”. You can then confirm the mode is “monitor” and the interface name.

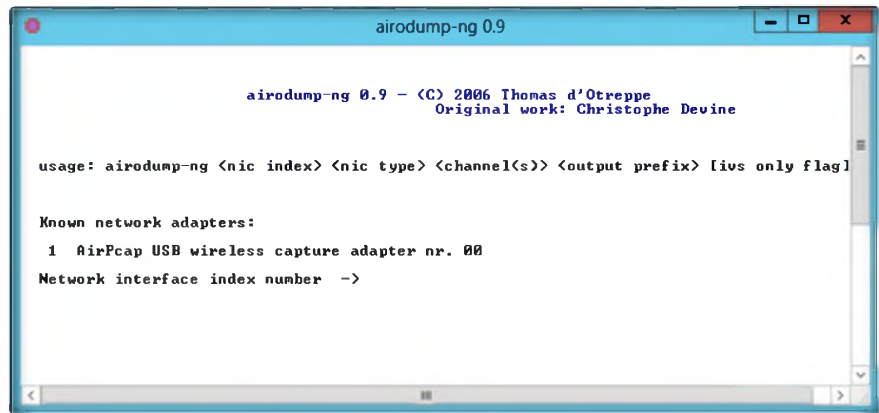



FIGURE 2.2: Airodump-ng selecting adapter window

4. Type the Airpcap adapter index number as **0** and select all channels by typing **11**. Press **Enter**.

 Aircrack-ng option: -b bssid Long version – bssid. Select the target network based on the access point's MAC address.

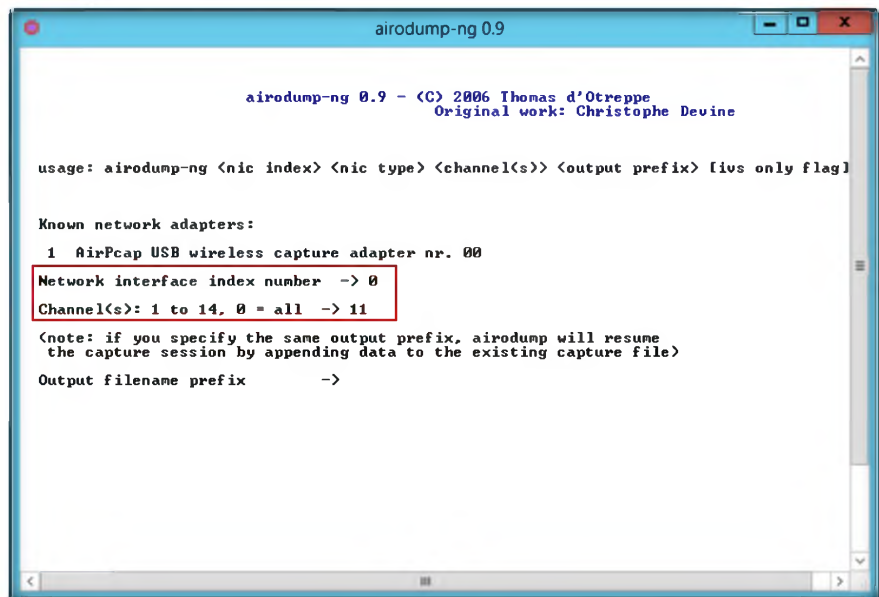




FIGURE 2.3: Airodump-ng selecting adapter window

5. It will prompt you for a file name. Enter **Capture** and press **Enter**.

 For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. SSE2 support is included to dramatically speed up WPA/WPA2 key processing.

## Module 15 – Hacking Wireless Networks

 Aircrack-ng completes determining the key; it is presented to you in hexadecimal format such as KEY FOUND! [BF:53:9E:DB:37].

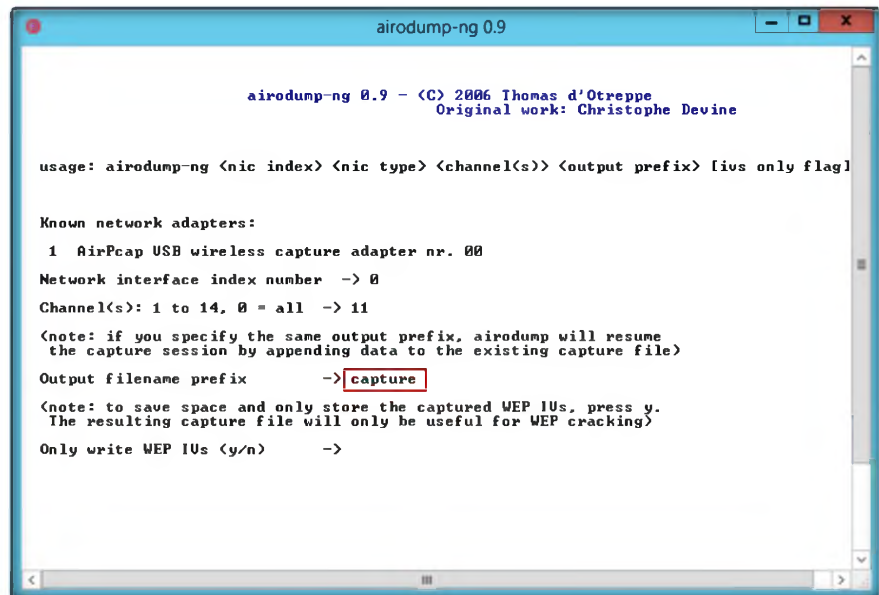



FIGURE 2.4: Airodump-ng selecting adapter window

### 6. Type **y** in **Only write WEP IVs**. Press **Enter**.

 Airodump option: -f <msecs> : Time in ms between hopping channels.

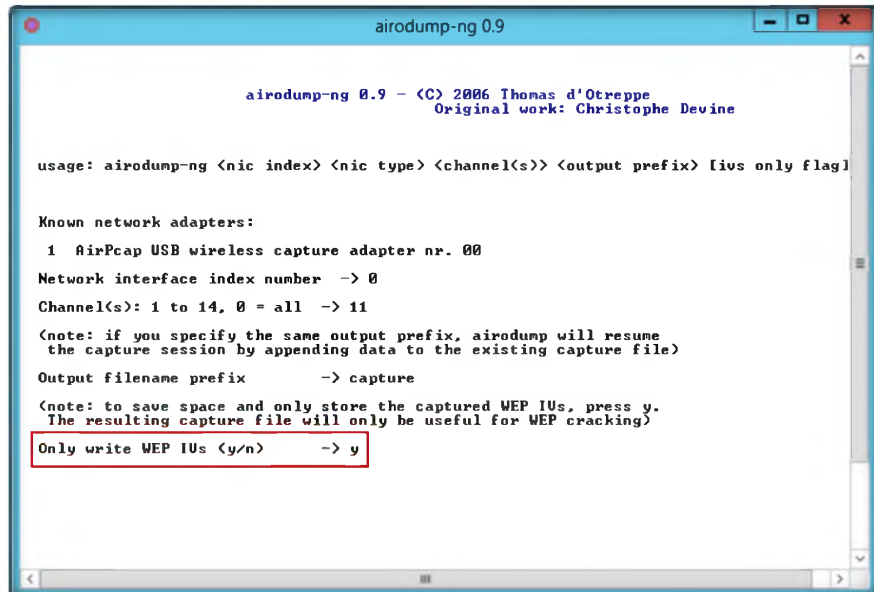


FIGURE 2.5: Airodump-ng dumping the captured packets window

 Airplay filter option: -d dmac : MAC address, Destination.

7. After pressing **y** it will display Wi-Fi traffic; leave it running for few minutes.
8. Allow airodump-ng to capture a large number of packets (above 2,000,000).

## Module 15 – Hacking Wireless Networks


Channel : 11 - airodump-ng 0.9.3


BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
B8:A3:86:3E:2F:37	-78	5	0	1	48	WEP?	SAACHI
1C:7E:E5:53:A4:48	-80	5496	2146	11	48	WPA	D-Link_DIR-524
4C:60:DE:32:3B:4E	-80	181	1	6	48	WPA	lthey lthey
4C:60:DE:32:7C:06	-81	5	0	11	48	WEP?	Kusun WLR
80:A1:D7:25:63:13	-77	13	0	1	54	OPN	
80:A1:D7:25:63:10	-78	21	0	1	54	WEP?	G0E
80:A1:D7:25:63:12	-80	12	0	1	54	OPN	
80:A1:D7:25:63:11	-78	18	0	1	54	OPN	
94:44:52:F2:45:0C	-78	13889	22804	11	48	WPA	GANTEC
00:09:5B:AE:24:CC	-10	53036	224385	11	54	WEP	NETGEAR

BSSID	STATION	PWR	Packets	ESSID
B8:A3:86:3E:2F:37	00:24:2C:38:39:96	-75	1	SAACHI
1C:7E:E5:53:A4:48	AC:72:89:6B:BD:B3	-81	38	D-Link_DIR-524
1C:7E:E5:53:A4:48	30:69:4B:C7:F9:F7	-84	29	D-Link_DIR-524
1C:7E:E5:53:A4:48	D0:B3:3F:12:A1:FF	-79	7	D-Link_DIR-524
1C:7E:E5:53:A4:48	E0:F8:47:95:05:D6	-82	421	D-Link_DIR-524
94:44:52:F2:45:0C	4C:ED:DE:A2:5B:BF	-80	2	GANTEC
94:44:52:F2:45:0C	4C:ED:DE:94:CE:E1	-80	5	GANTEC
94:44:52:F2:45:0C	00:26:82:CF:09:C2	-80	16256	GANTEC
94:44:52:F2:45:0C	50:01:BB:58:A5:27	-76	1	GANTEC
94:44:52:F2:45:0C	00:23:15:73:E7:E4	-73	293	GANTEC
00:09:5B:AE:24:CC	1C:66:AA:7C:F0:79	-81	213	NETGEAR
00:09:5B:AE:24:CC	04:54:53:0E:2C:AB	-33	125920	NETGEAR

FIGURE 2.6: Airodump-ng Channel listing window

 airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and run the right commands.

 Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

9. Now close the window.

10. Go to **Aircrack-ng** and click **Advanced Options**.

Aircrack-ng GUI

**Aircrack-ng** | Airodump-ng | Airdecap-ng | WZCook | About

Filename(s)

Encryption ☒ WEP ☐ WPA

Key size  bits ☐ Use wordlist ☐ Use PTW attack

☒ **Advanced options**

☐ Specify ESSID

☐ Specify BSSID

Fudge factor

Disable KoreK attacks ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8

Key search filter ☐ Alphanumeric characters ☐ BCD characters ☐ Numeric (Fritz!BOX)

Bruteforce  Last keybytes bruteforce ☒ Multithreading bruteforce ☐ Single Bruteforce attack

FIGURE 2.7: Aircrack-ng options window


11. Click **Choose** and select the filename **capture.ivs**.

**Note:** This is a different file from the one you recorded; this file contains precaptured IVS keys. The path is **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap**.

## Module 15 – Hacking Wireless Networks

**Note:** To save time capturing the packets, for your reference, the **capture.ivs** file (this **capture.ivs** file contain more than 200000 packets) is at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap**.

12. After selecting file, click **Launch**.

 To put your wireless card into monitor mode: `airmon-ng start rausb0`.

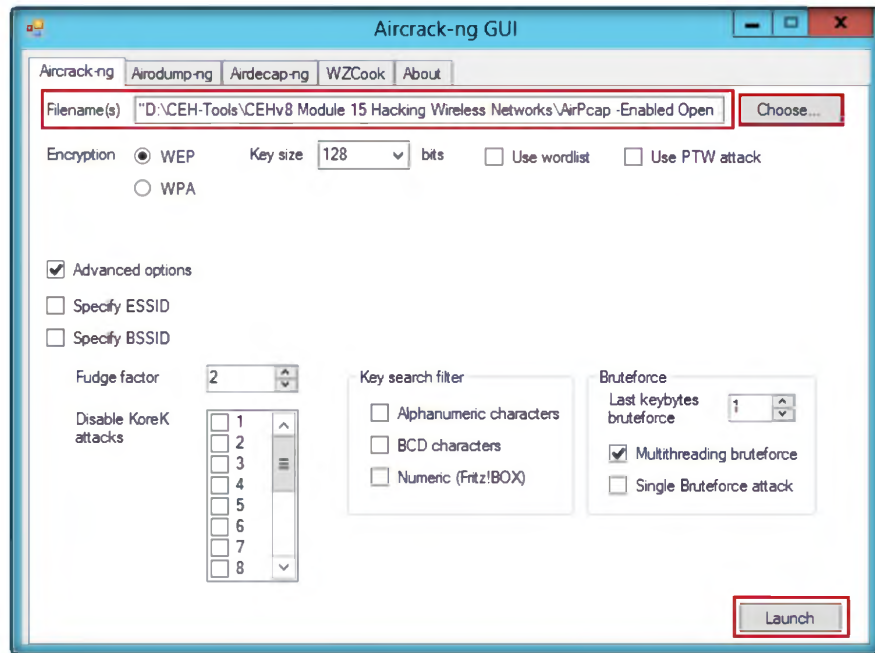



FIGURE 2.8: Aircrack-ng launch window

 You may use this key without the ":" in your wireless client connection prompt and specify that the key is in hexadecimal format to connect to the wireless network.

13. If you get the enough captured packets, you will be able to crack the packets.

14. Select your target network from **BSSID** and press **Enter**.

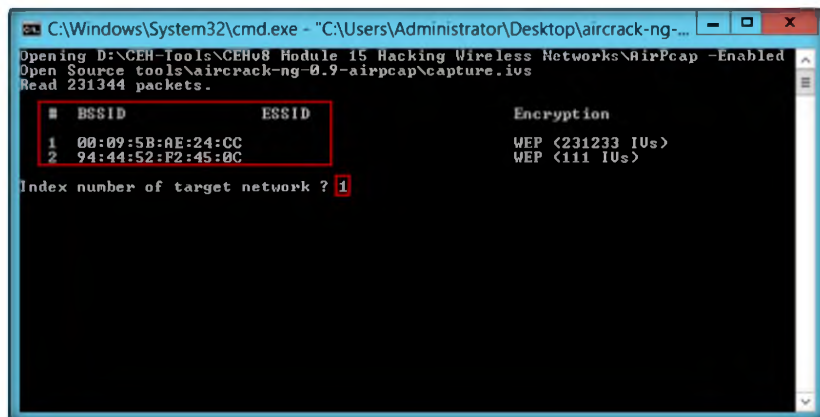


FIGURE 2.9: Select target network

Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.

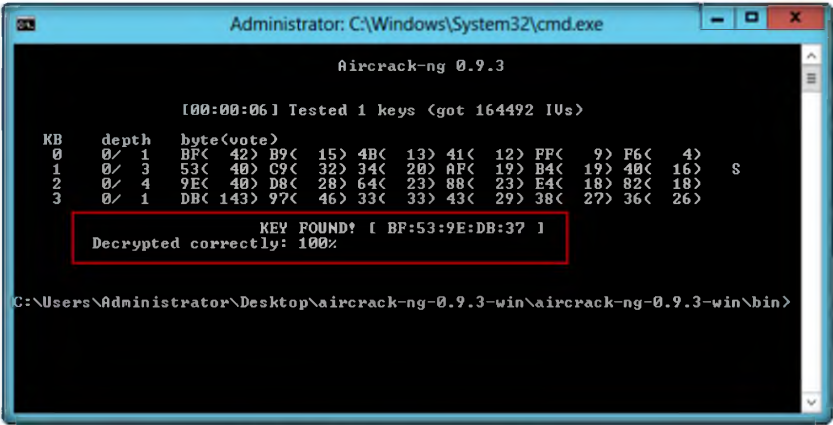


FIGURE 2.10: aircrack-ng with WEP crack key

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.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Aircrack-ng	Number of packet captured: 224385
	Cracked wireless adaptor name: NETGEAR
	Output: Decrypted key BF:53:9E:DB:37

Questions

- 1. Analyze and evaluate how aircrack-ng operates.
- 2. Does the aircrack-ng suite support Airpcap Adapter?

## Module 15 – Hacking Wireless Networks

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs









## Sniffing the Network Using the OmniPeek Network Analyzer

*OmniPeek is a standalone network analysis tool used to solve network problems.*

### ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

### Lab Scenario

Packet sniffing is a form of wire-tapping applied to computer networks. It came into vogue with Ethernet; this means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone's traffic. Most of the hubs/switches allow the intruder to sniff remotely using SNMP, which has weak authentication. Using POP, IMAP, HTTP Basic, and talent authentication, an intruder reads the password off the wire in cleartext.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. OmniPeek network analysis performs deep packet inspection, network forensics, troubleshooting, and packet and protocol analysis of wired and wireless networks. In this lab we discuss wireless packet analysis of captured packets.


### Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

### Lab Environment

In this lab, you need:

- **Advanced OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\Wi-Fi Packet Sniffer\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link <http://www.wildpackets.com>

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks**

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in Windows Server 2008
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install OmniPeek
- Administrative privileges to run tools

## Lab Duration

Time: 20 Minutes

## Overview of OmniPeek Network Analyzer

 You can download OmniPeek Network Analyzer from <http://www.wildpackets.com>.

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, Video to remote offices, and 802.11 a/b/g/n.

## Lab Tasks

### TASK 1

#### Analyzing WEP Packets

1. Launch OmniPeek by selecting **Start → All Programs → Wildpackets Omni packets Demo**.
2. Click **View sample files**.

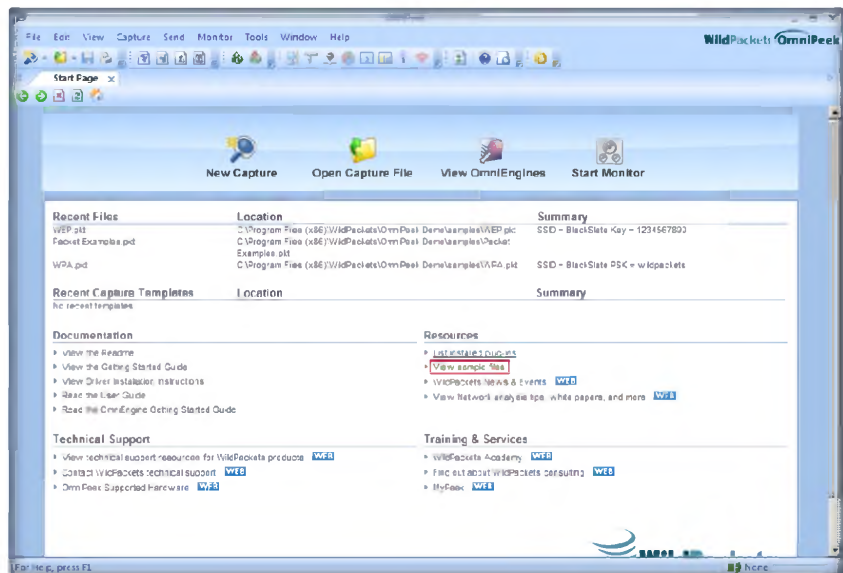


FIGURE 3.1: Omnippeek main window

3. Select **WEP.pkt**.

## Module 15 – Hacking Wireless Networks

**OmniPeek** gives network engineers real-time visibility and Expert Analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices.

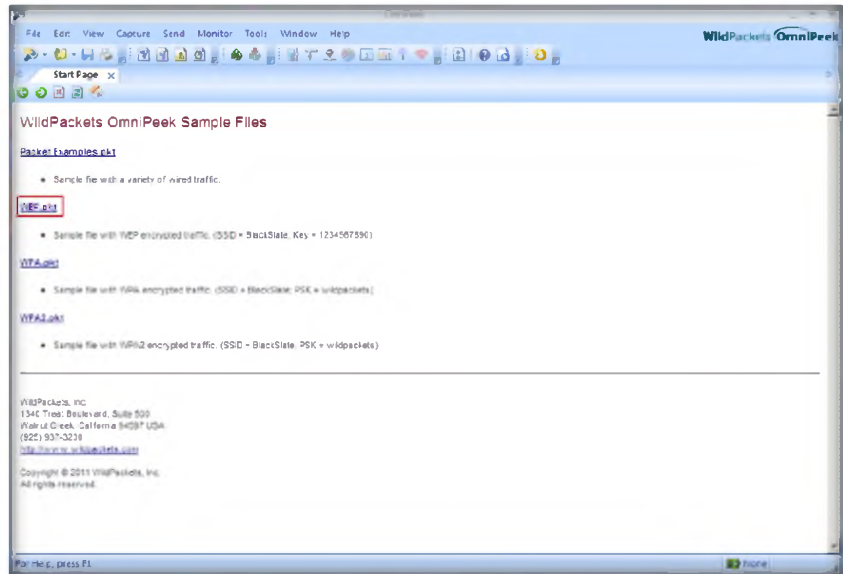


FIGURE 3.2: Omnipeek Sample Files Window

- It will open **WEP.pkt** in the window. Select **Packets** from the left pane.

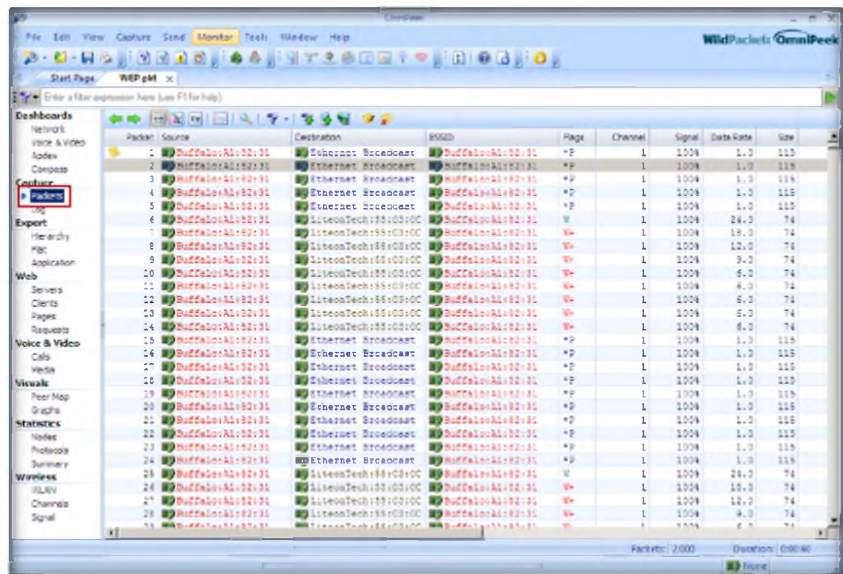


FIGURE 3.3: TELNET-UnWEP packets Window

- Double-click any of the packets in the right pane.

## Module 15 – Hacking Wireless Networks

**Comprehensive network performance management and monitoring of entire enterprise networks, including network segments at remote offices**

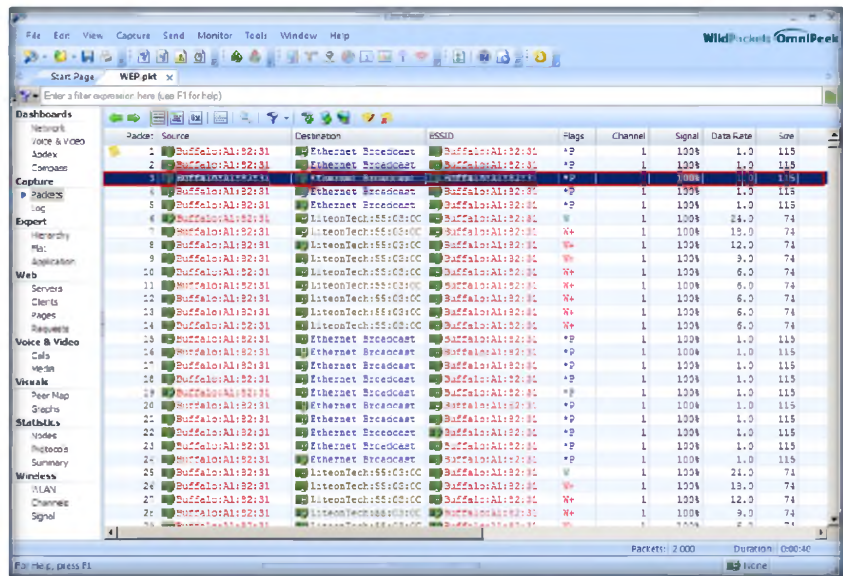


FIGURE 3.4: TELNET-UnWEP packets analyzer

- Click the right arrow to view the next packet.

**OmniPeek Connect manages an organization's Omnipliance and TimeLine network recorders, and provides all the console capabilities of OmniPeek Enterprise with the exception of local capture and VoIP call playback**

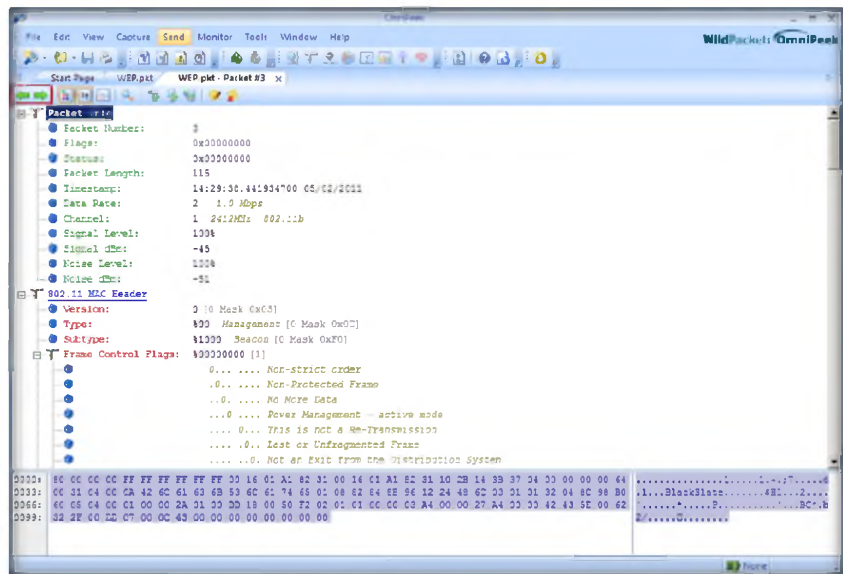


FIGURE 3.5: TELNET-UnWEP packets frame window

- Close the tab from the top and select different options from the right pane; click **Graphs**.



OmniPeek Enterprise also provides advanced Voice and Video over IP functionality including signaling and Media analyses of voice and video, VoIP playback, voice and video Expert Analysis, Visual Expert, and more

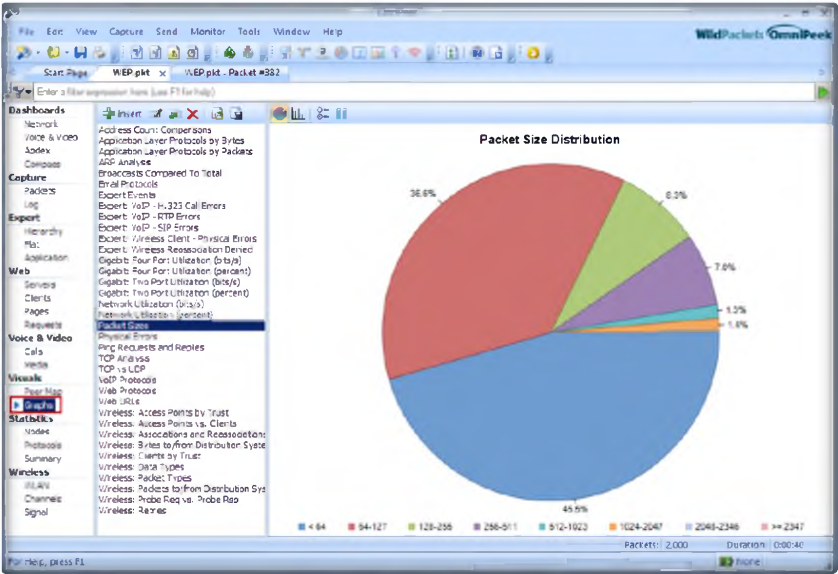


FIGURE 3.6: WEP Graphs window

8. Now traverse through all the options in the left pane of the window.

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.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	<p>Packet Information:</p> <ul style="list-style-type: none"><li>• Packet Number</li><li>• Flags</li><li>• Status</li><li>• Packet Length</li><li>• Timestamp</li><li>• Data Rate</li><li>• Channel</li><li>• Signal level</li></ul>

	<ul style="list-style-type: none"><li>• Signal dBm</li><li>• Noise Level</li><li>• Noise dBm</li><li>• 802.11 MAC Header Details</li></ul>
--	--

## Questions

1. Analyze and evaluate the list of captured packets.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs