



CompTIA Security+® Lab Series

Lab 5: Secure Implementation of Wireless Networking

CompTIA Security+® Domain 1 - Network Security

Objective 1.6: Implement wireless network in a secure manner

Document Version: **2013-08-02**

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).



This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Objective: Implement a Wireless Network In a Secure Manner	3
Pod Topology	5
Lab Settings	6
1 Examining Plain Text Traffic.....	7
1.1 Viewing Plain Text Wireless Traffic	7
1.2 Conclusion	14
1.3 Discussion Questions.....	14
2 Exploiting and Examining WEP Traffic	15
2.1 Decrypt and Analyze WEP Traffic	15
2.2 Conclusion	21
2.3 Discussion Questions.....	21
3 Exploiting and Examining WPA Traffic	22
3.1 Exploiting WPA and Analyzing the Traffic	22
3.2 Conclusion	29
3.3 Discussion Questions.....	29
References	30

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will view files and clear text traffic from an unsecured wireless capture file. Students will also obtain a Wired Equivalent Privacy (WEP) key and a Wi-Fi Protected Access (WPA) passphrase using the aircrack-ng utility. After obtaining the WEP Key and WPA passphrase, students will decrypt the traffic using airdecap-ng. By completing these exercises, students will become more cognizant of the dangers involved in using unsecure wireless network, wireless networks with WEP, and wireless networks using WPA or WPA2 with a weak passphrase that is in the dictionary.

This lab includes the following tasks:

- 1 – Examining Plain Text Traffic
- 2 – Exploiting and Examining WEP Traffic
- 3 – Exploiting and Examining WPA Traffic

Objective: Implement a Wireless Network In a Secure Manner

Wireless networks present a far greater security risk than their wired counterparts. People who connect their computers to an unsecure wireless access point are putting their information at risk. Most people choose to use some form of encryption for their wireless networks in order to protect their data and privacy. Some forms of encryption are better than others. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are two methods that can be used to encrypt wireless traffic. The WEP encryption scheme is flawed and can be broken easily by an attacker. For better wireless security, it is recommended that WPA or WPA2 be used to encrypt your wireless network traffic. While the use of WPA or WPA2 is more secure, an attacker can break into networks using these security protocols if they are able to obtain the passphrase. For this reason, the use of any words found in a dictionary should be avoided.

Monitor Mode – Certain versions of wireless cards can be put into monitor mode and will be able to capture all of the wireless traffic in range of their card. This is the equivalent of promiscuous mode for wired adapters where addressing is ignored and all network data is processed. Wireless networks use Carrier Sense Multiple Access Collision Avoidance, or CSMA/CA. So, by using a wireless card in monitor mode, all wireless traffic can be passively captured.

WEP – Wired Equivalent Privacy (WEP) is an encryption protocol that was designed to be about as secure as “using the wire”, thus the name **Wired** Equivalent Privacy. The WEP encryption scheme has a weakness in the way it was implemented in that if a hacker generates enough Initialization Vectors, or IVs, they can break the 64-bit or 128-bit WEP key. A good hacker can break WEP in less than 5 minutes, so its use should be avoided.

WPA – Wi-Fi Protected Access (WPA) and WPA2 are much better encryption schemes to use for wireless networks. While they have far better security protection than networks using WEP, WPA and WPA2 are not flawless in their security implementation either. If an attacker can obtain the passphrase, they will be able to decrypt the network traffic and read all of the plain text information. In order to properly secure a network utilizing WPA or WPA2 encryption, use a strong passphrase that includes uppercase and lowercase letters, numbers, and special characters. Avoid using dictionary words.

Aircrack-ng – Aircrack-ng is actually a suite of tools that can be utilized for monitoring, exploiting, and decrypting wireless network traffic. The aircrack-ng suite is part of the BackTrack distribution. There is a version of the aircrack-ng suite for Windows, but it requires special AirPcap hardware, and may trigger anti-virus software.

Wireshark – Wireshark is a protocol analyzer that allows you to capture or analyze network traffic. You can analyze plain text Wireless traffic within Wireshark and even decrypt wireless traffic if you provide the WEP key or the WPA/WPA2 passphrase.

Pod Topology

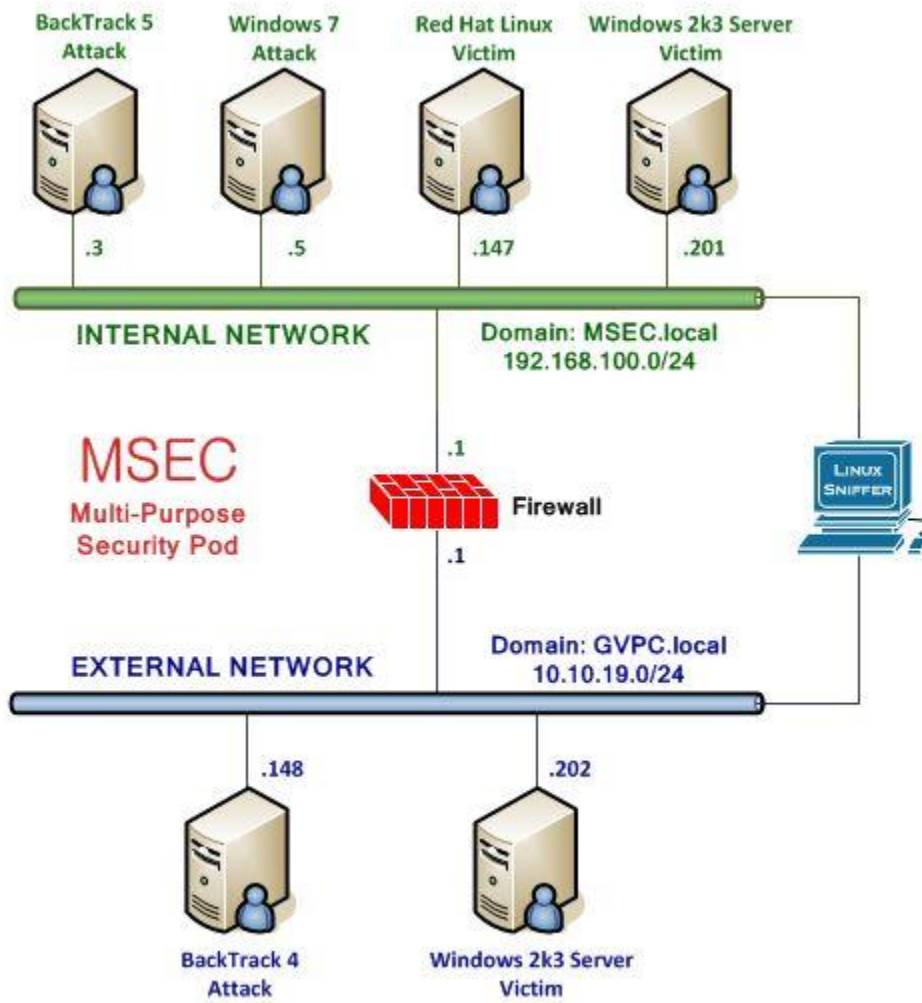


Figure 1: MSEC Network Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password

BackTrack 5 Internal Attack Login:

1. Click on the **BackTrack 5 Internal Attack** icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the **Password:** prompt.

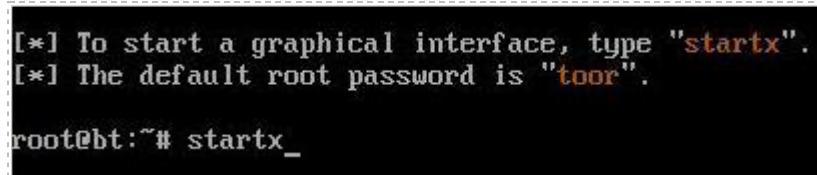
For security purposes, the password will not be displayed.

A terminal window with a black background and green text. The text reads: "BackTrack 5 R1 - Code Name", "bt login: root", and "Password: _".

```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the **root@bt:~#** prompt.

A terminal window with a black background and green text. The text reads: "[*] To start a graphical interface, type 'startx'.", "[*] The default root password is 'toor'.", and "root@bt:~# startx _".

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".
root@bt:~# startx _
```

Figure 3: BackTrack 5 GUI start up

1 Examining Plain Text Traffic

When someone runs a wireless network card in monitor mode, they can capture all of the wireless traffic within range of their card. Managed Mode is the normal state in which a wireless card operates; your device needs to be in managed mode if you want to connect to a wireless network. Not all cards operate in monitor mode, and very few cards function in monitor mode in Microsoft Windows. If someone is using monitor mode to capture network traffic, they are likely using the Linux operating system.

Wireless cards that operate in monitor mode capture network traffic passively. Cards that operate in managed mode actively scan and their presence can be detected. Not only will cards operating in monitor mode be able to capture all the network traffic in range, their presence will not be detected on the network. If the user has the WEP key or WPA/WPA2 passphrase, they can enter it and the traffic will be decrypted.

1.1 Viewing Plain Text Wireless Traffic

Open a Terminal to Get Started

Keep in mind that Linux commands are case sensitive. The commands must be entered exactly as shown, or errors will occur.

1. Open a terminal on the BackTrack 5 Internal Attack Machine by clicking on the picture to the right of the word **System** in the task bar in the top of the screen. Type **wireshark** (all lowercase) to bring up the Wireshark program.

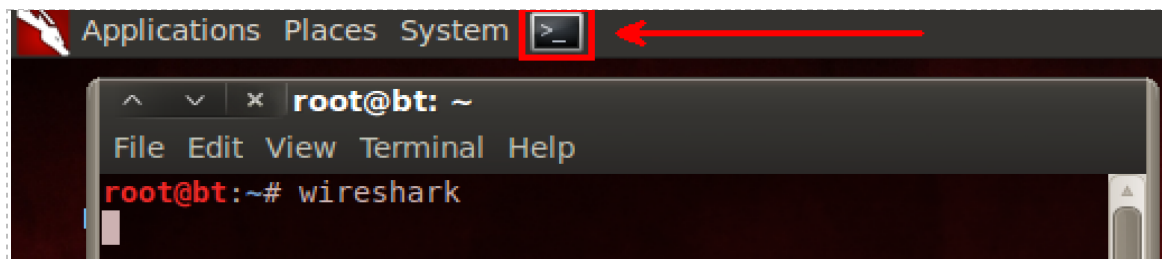


Figure 4: The Terminal Windows within BackTrack

2. Click the button that says **Don't show this message again**, and click OK.

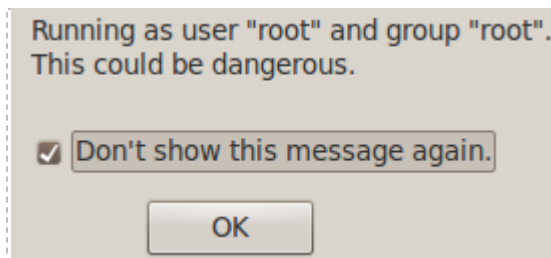


Figure 5: Allow Wireshark to run as root

Wireshark is a protocol analyzer that allows you to capture network traffic in real time. You can also use it to analyze network traffic that you have captured previously.

3. Select **File** from the Wireshark menu and select **Open**. Double-click on the **root** folder then double-click on the **lab5** folder. Double-click on the file **PLAIN-01.cap**.

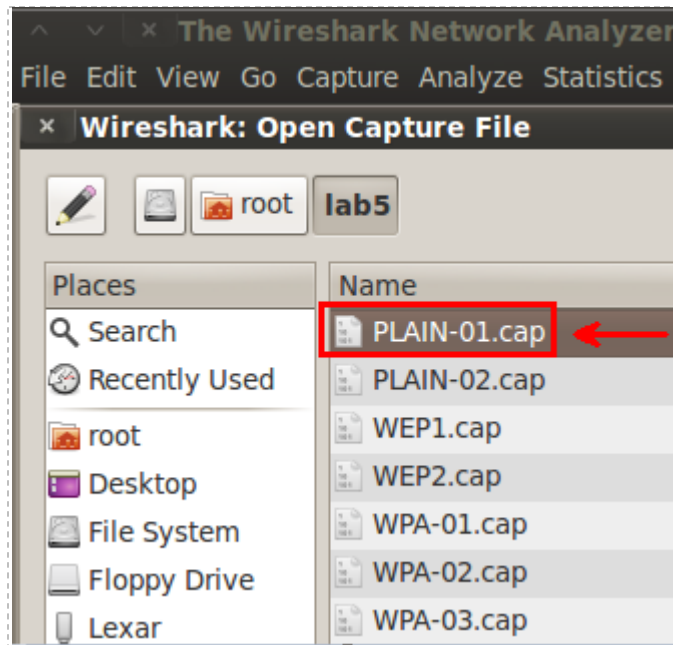


Figure 6: Opening the First Capture File

4. Right-click on the **Info** column and select **Resize Column**. This will allow you to see all of the information contained within this column.

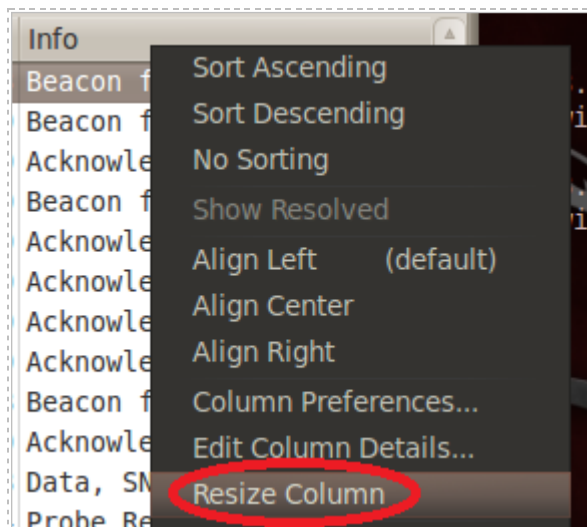


Figure 7: Resizing the Info Column in Wireshark

5. Scroll over by clicking the right arrow to see the results of the **Info** Column.

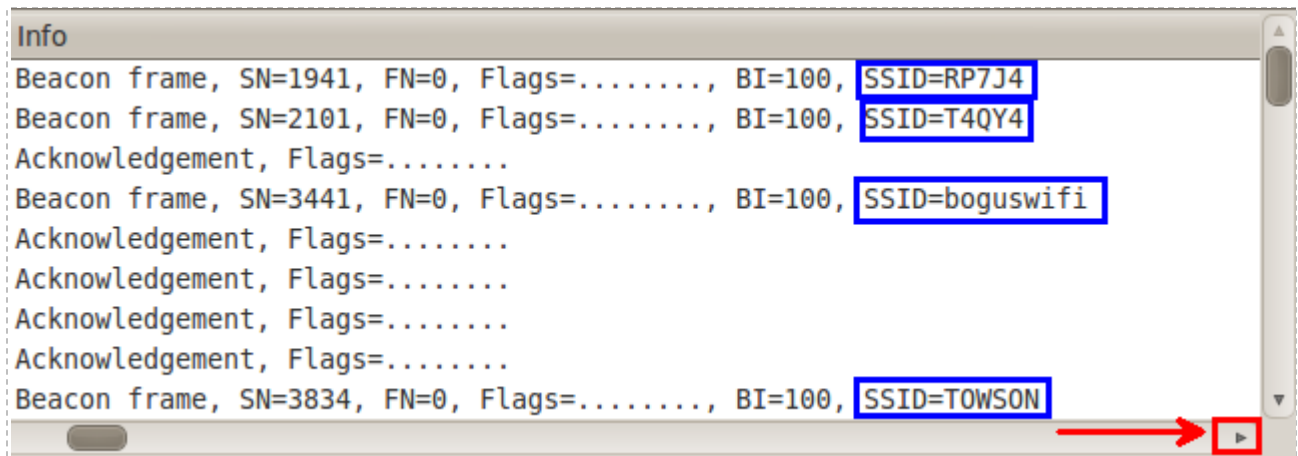


Figure 8: Wireless Networks are Broadcasting their Service Set Identifiers (SSIDs)

Media Access Control (MAC) addresses are visible within captures of wireless network traffic whether encryption is being utilized or not. While you will see the layer two addresses, you will not see traffic from layers above two if WEP, WPA, or WPA2 encryption is being utilized. Even though a MAC address is a 12 digit hexadecimal address, the default settings of Wireshark will replace the first six digits with the name of the vendor. The first six digits of a MAC address are referred to as an Organizational Unique Identifier, or OUI.

6. Click on the second frame in the Wireshark capture file. In the lower screen, click the + in front of *IEEE 802.11 wireless LAN management frame*, the + in front of *Tagged parameters*, then, click the + in front of *Tag: Vendor Specific*. View the **WPA Version**.

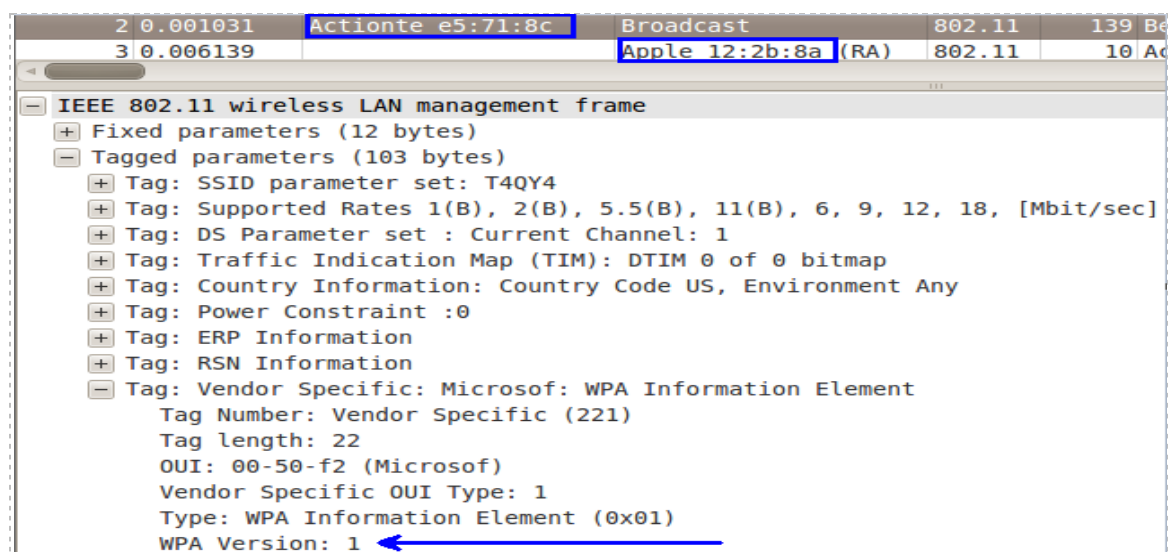


Figure 9: The Version of WPA is Displayed in a Broadcast Packet

- In the filter pane, type **dns** (all lowercase) and click apply. You will be able to see a virtual roadmap of the wireless activity on this network, as viewing the DNS requests will show you the name of almost every site visited by users. In this capture, you can see a request for the IP address of Google and lasvegas.com.

No.	Time	Source	Destination	Protocol	Length	Info
3827	60.585289	192.168.2.3	192.168.2.1	DNS	95	Standard query A news.google.com
3830	60.585849	192.168.2.1	192.168.2.3	DNS	111	Standard query response A 72.14.204.9
3836	60.603721	192.168.2.3	192.168.2.1	DNS	96	Standard query A video.google.com
3844	60.622151	192.168.2.3	192.168.2.1	DNS	95	Standard query A img.youtube.com
3845	60.631417	192.168.2.1	192.168.2.3	DNS	112	Standard query response A 72.14.204.1
3847	60.642169	192.168.2.1	192.168.2.3	DNS	111	Standard query response A 72.14.204.1
3952	61.589386	192.168.2.3	192.168.1.1	DNS	96	Standard query A video.google.com
3954	61.609913	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3955	61.610425	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3956	61.610425	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3991	62.456265	192.168.2.3	192.168.1.1	DNS	96	Standard query A www.lasvegas.com

Figure 10: The DNS Requests on a Wireless Network

Wireshark also gives users the ability to parse out Hyper Text Transfer Protocol, or HTTP, objects from a capture file. This will allow us to determine websites users on the wireless networks visited, as well as the names of the files they downloaded. Taking it a step further, we will actually be able to pull images from the capture file. This exercise should raise your awareness of the dangers of using an unsecured network.

- From the Wireshark menu, select **File>Export>Objects>HTTP**. A new window will open showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Under the **Filename** column, find the picture **cookie-monster-cupcake.jpg**, click on the file, and click **Save As**. Verify the save in folder is **root** by clicking the down arrow to the right of **Save in folder**: and click **Save**.

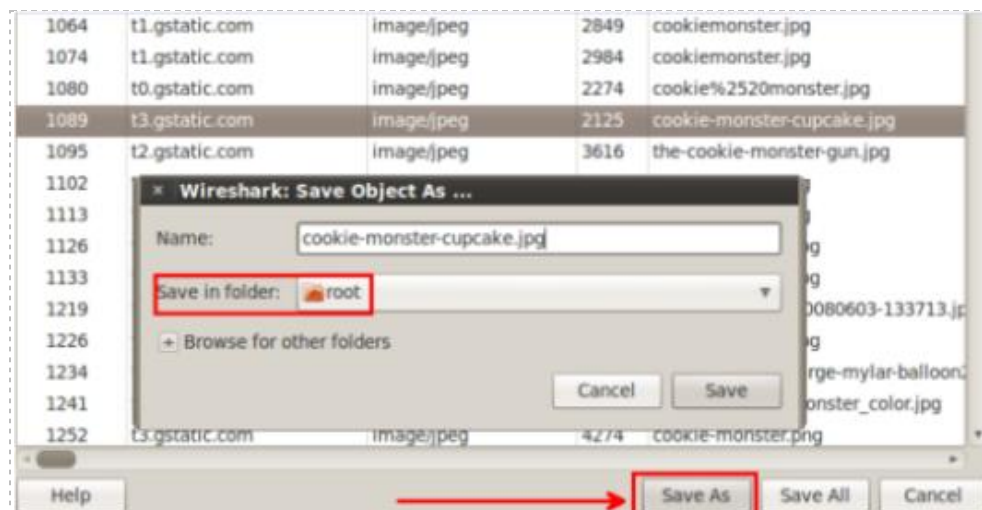


Figure 11: Saving an HTTP Object Parsed from Wireshark

9. To view the file, click **Places** from the BackTrack 5 Menu Bar and select **Home Folder**. Click **Cancel** to close the Wireshark: HTTP Object List

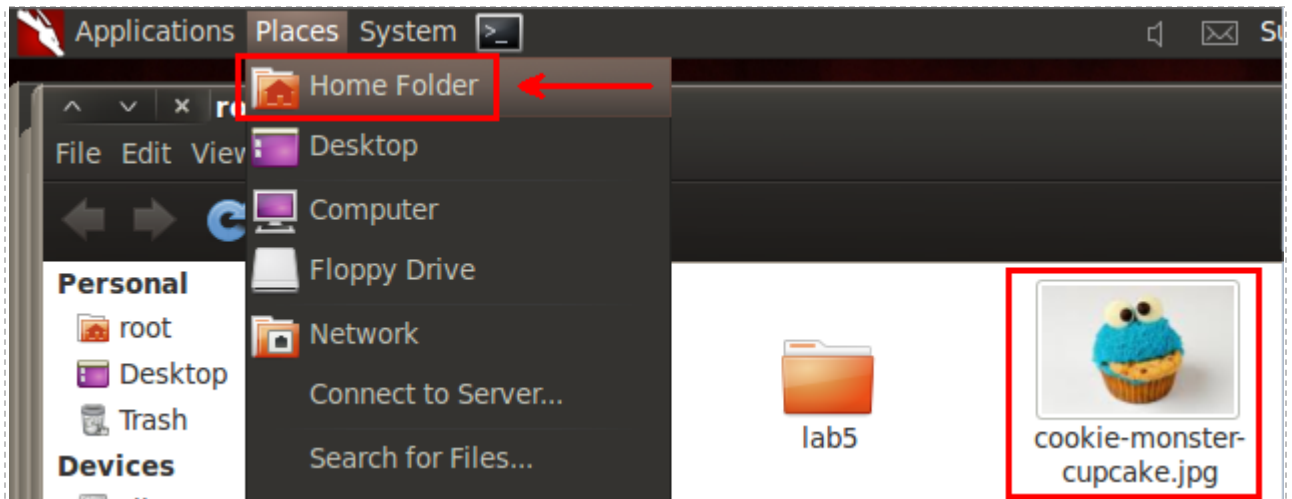


Figure 12: The Picture Carved From Wireshark

While Wireshark will easily parse HTTP objects in the method previously described, it does not provide a convenient means of parsing objects from traffic utilizing other protocols such as File Transfer Protocol, or FTP. However, other tools such as Network Miner will parse objects from other protocols like FTP. Network Miner is free and can be downloaded from SourceForge.

To find FTP data within Wireshark, we can use the ftp-data filter and the file signature to carve out traffic. A file signature is a unique identifier at the beginning of a file that identifies what the true type of the file is. A person could try to hide a jpeg picture by renaming the file extension to .doc but the signature will be JFIF.

The free hexeditor tool **HxD** allows you to view the file signature of files.

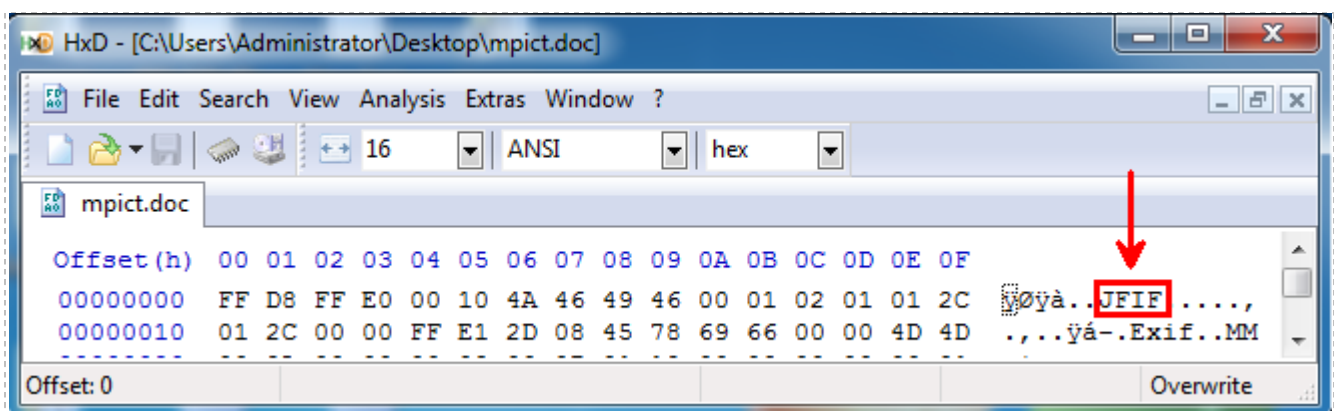


Figure 13: The File Signature of a JPEG file

10. To pull a zip file transferred via FTP out of the wireless capture file, type **ftp-data and frame contains PK** into the Wireshark filter and hit **Apply**. Right-click on frame **21207** in the list and select **Follow TCP Stream**.

The "PK" file signature indicates a zip file format.

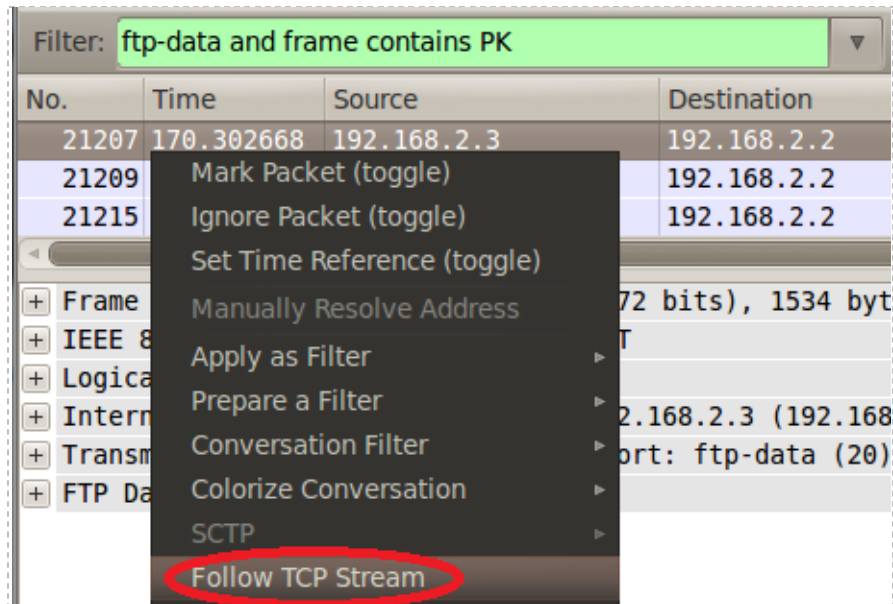


Figure 14: Following the TCP Stream

11. Examine the data shown in the TCP stream.

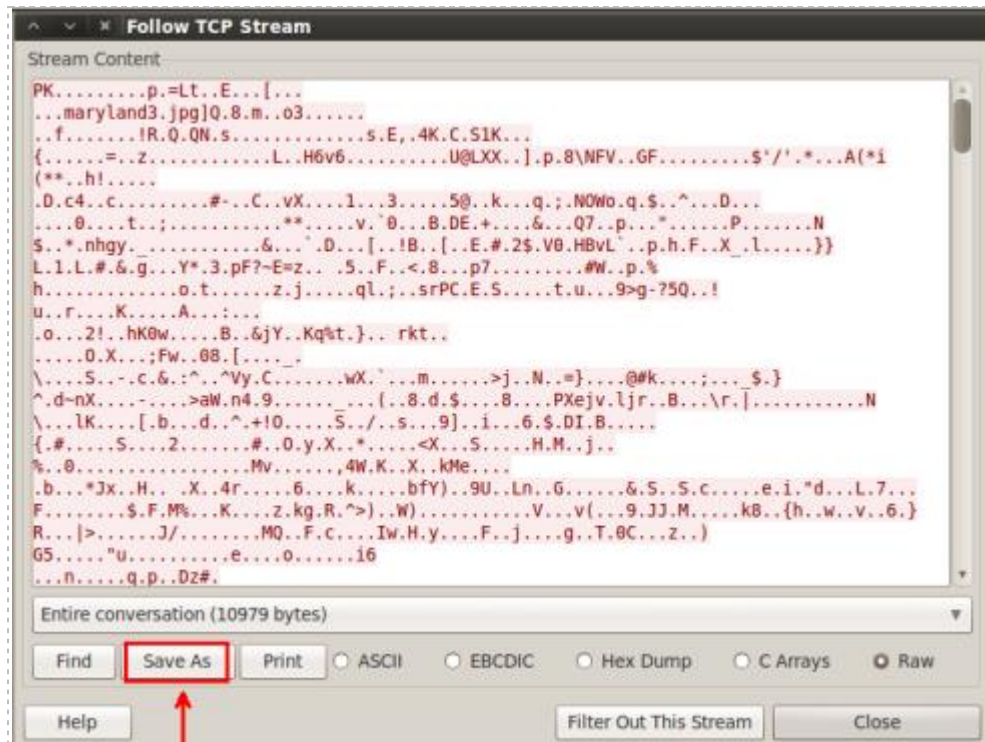


Figure 15: The Follow TCP Stream Window

12. Scroll down to see the "PK" attached to the end of filenames.

```

...F.V...0$.b}I<.] .4...
...maryland3.jpgPK....

)...maryland4.jpgPK....
)...U....
...maryland5.jpgPK.....
tion (10979 bytes)

```

Figure 16: Scroll down to see filename with PK signature

13. In the **Follow the TCP Stream** pane (see Figure 15), click the Save As button.
14. For the name of the file, put **file.zip**. Make sure the Save in Folder is **Desktop** and click **Save**.

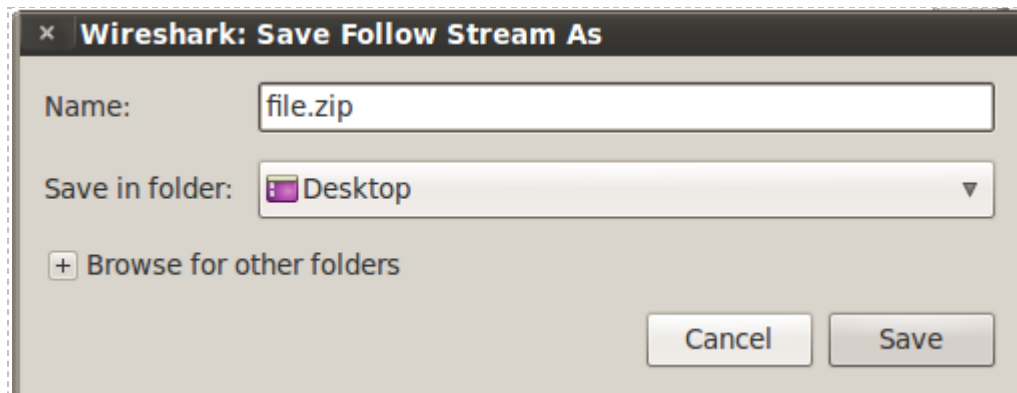


Figure 17: Saving the Zip file From the TCP Stream

15. Minimize open applications and look for the zip file you saved on the Desktop. Double-click on the brown **file.zip** icon. A white **file.zip** icon will appear below it. Double-click on the white **file.zip** icon and the three pictures should appear.

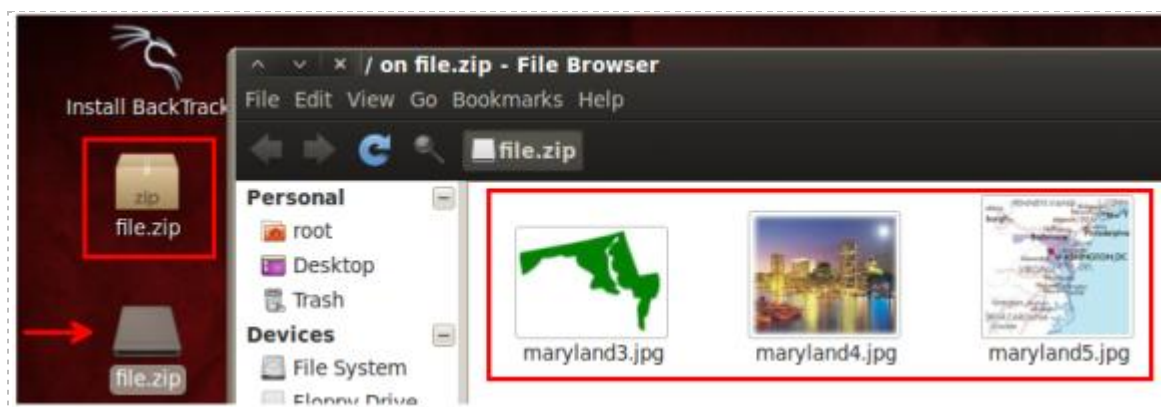


Figure 18: Opening the Zip File and Viewing the Pictures.

1.2 Conclusion

Using an unsecured wireless network has serious security risks. If someone has a wireless card running in monitor mode, they can capture all traffic to and from the access point. This includes the ability to view DNS request, view HTTP traffic, and the ability for to extract images out of the wireless capture traffic. For this reason, it is a better practice to use a wireless network using encryption, like WEP, WPA or WPA2.

1.3 Discussion Questions

1. What is the type or router (name of company) being used on the wireless network with the Service Set Identifier (SSID) of *boguswifi*? (Examples: Belkin, Netgear)
2. See if you can locate the channel that the TOWSON wireless network is using. Click the + in front of IEEE 802.11 wireless LAN management frame, the + in front of Tagged parameters, then, click the + in front of DS Parameter Set.
3. From the Wireshark menu, select File,>Export,>Objects,>HTTP. Find the Hoover_dam.jpg picture and save it to your home folder. View the picture.

2 Exploiting and Examining WEP Traffic

Wired Equivalent Privacy, or WEP, was never meant to be used in environments where security is paramount. The developers of the encryption scheme tried to emphasize this by naming it **Wired** Equivalent Privacy. There are flaws in the way that the WEP encryption scheme was implemented, making it possible for an attacker to obtain the 64-bit or 128-bit WEP key. One of the reasons WEP is so widely used is because some older hardware and software is not WPA compliant, meaning it does not support WPA/WPA2. Some people, including vendors, feel that it is easier to set up a wireless network using WEP.

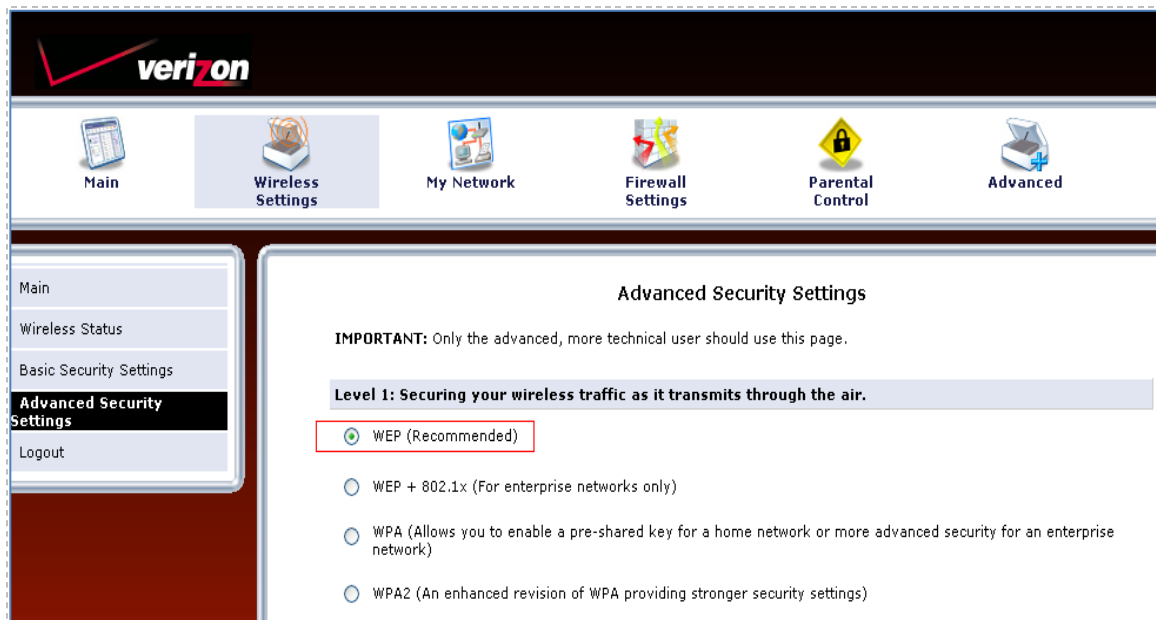


Figure 19: The Vendor is Recommending the Use of WEP

Even though a good hacker can obtain the WEP key to someone's network is less than 5 minutes, it is still better to use WEP than to leave your network completely unsecured. If someone has their wireless card in monitor mode and they are monitoring wireless network traffic, they will be unable to see the traffic unless they have the WEP key.

2.1 Decrypt and Analyze WEP Traffic

1. Open the WEP Capture File:
 - a. Select **File** from the Wireshark menu and select **Open**.
 - b. Double-click on the **root** folder, and then double-click on the **lab5** folder.
 - c. Double click on the file **WEP1.cap**

- In the filter pane, type **dns** (all lowercase) and click **Apply**. You will not be able to see any traffic because the wireless network traffic is encrypted.

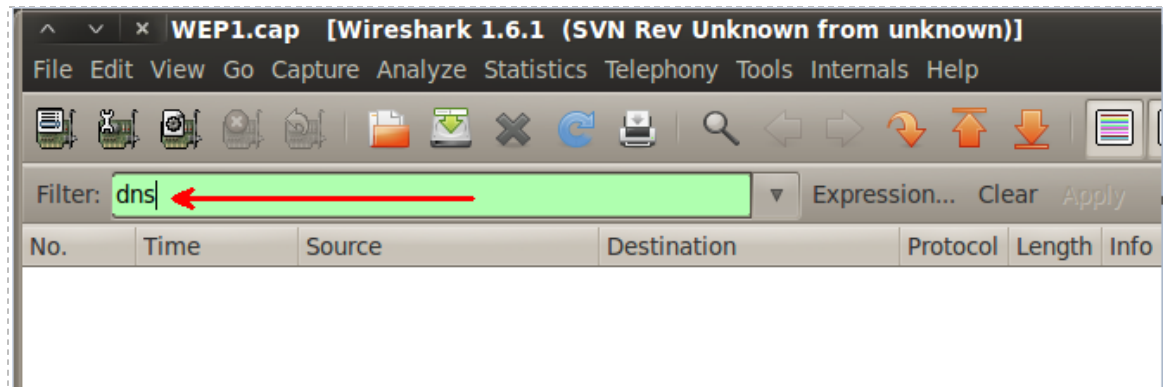


Figure 20: No Results for dns Filter in Wireshark due to Encryption

- Close Wireshark by selecting **File** from the menu bar and selecting **Quit**.

The WEP key can be obtained by an attacker if they are able to generate enough Initialization Vectors, or IVs. IVs are random 24-bit values that are added to your WEP key to assist in the process of securing the data. IVs are generated when the attacker replays traffic over and over again, and knocks the client off the network for a short time (less than one second). Due to the limitations of the IVs being only 24-bits, eventually these IVs will start to repeat themselves. Once this occurs, an attacker has enough information to break the encryption. The attacker's wireless card must be in monitor mode to perform the attack.

- In the terminal window, type the following command.
`root@bt:~# aircrack-ng lab5/WEPI1.cap`
- Select **5** for the target network. Notice that there are 43,210 IVs.

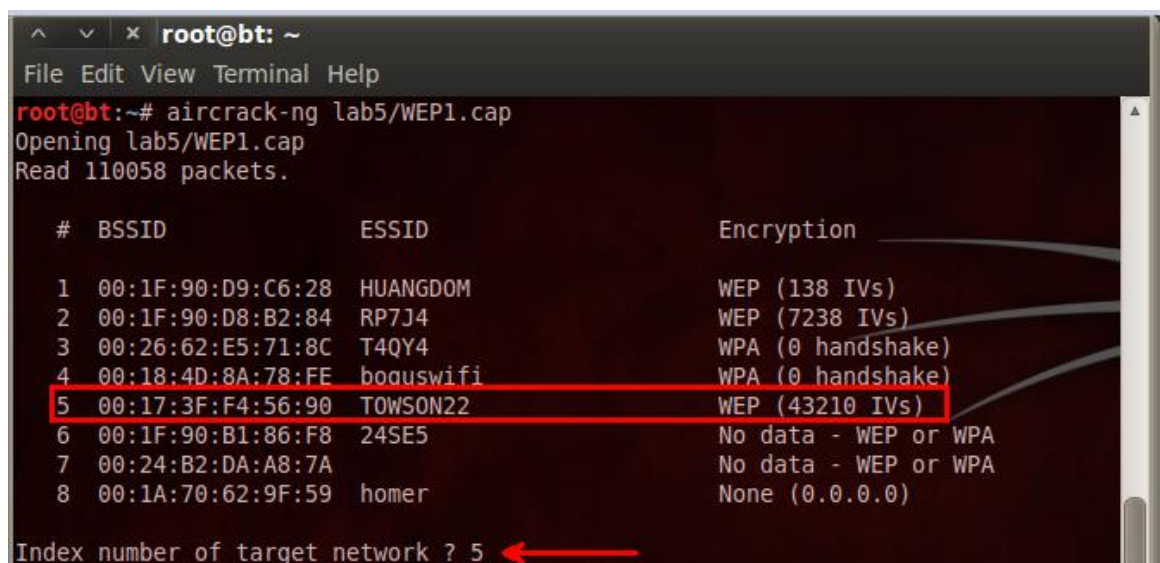


Figure 21: Selecting the Number of the Target Network

After a few seconds, the aircrack-ng program will be able to crack the 64-bit WEP key.

```

root@bt: ~/lab5
File Edit View Terminal Help

Aircrack-ng 1.1 r1904

[00:00:02] Tested 7030 keys (got 29937 IVs)

KB   depth  byte(vote)
0    0/ 11  AA(39424) 2F(38656) BF(37888) BC(36608) FC(36352)
1    5/ 11  AA(35840) 93(35840) 18(35584) 28(35584) A5(35328)
2    0/  1  AA(44032) 65(37376) EB(36608) 2C(36096) 55(35840)
3   24/ 30  A0(33536) 35(33280) 4D(33280) 76(33280) 97(33280)
4    0/  2  AA(41728) D9(38144) 8E(36096) 4C(35072) F7(35072)

KEY FOUND! [ AA:AA:AA:AA:AA ]
Decrypted correctly: 100%
  
```

Figure 22: Aircrack-ng provides you with the WEP key to the Network

After the WEP key is obtained, we can decrypt the network traffic with **airdecap-ng**.

- From the terminal, type the following command to decrypt the traffic (10 "A"s):
 root@bt:~# **airdecap-ng -w AAAAAAAAAA lab5/WEP1.cap**

```

root@bt: ~
File Edit View Terminal Help

root@bt:~# airdecap-ng -w AAAAAAAAAA lab5/WEP1.cap
Total number of packets read      110058
Total number of WEP data packets  50596
Total number of WPA data packets   808
Number of plaintext data packets   0
Number of decrypted WEP packets    43220
Number of corrupted WEP packets    0
Number of decrypted WPA packets    0
  
```

Figure 23: WEP Packets are Decrypted with the Key

The number of decrypted WEP packets should be 43220. Now, we will be able to analyze TCP/IP traffic as well as carve files from the decrypted capture file.

- Type **wireshark** in the terminal (all lowercase) to bring up Wireshark. Select **File** from the Wireshark menu and select **Open**. If you are not already in the **lab5** folder, double-click on the **root** folder, and then double-click on the **lab5** folder. Double-click on the file **WEP1-dec.cap**.

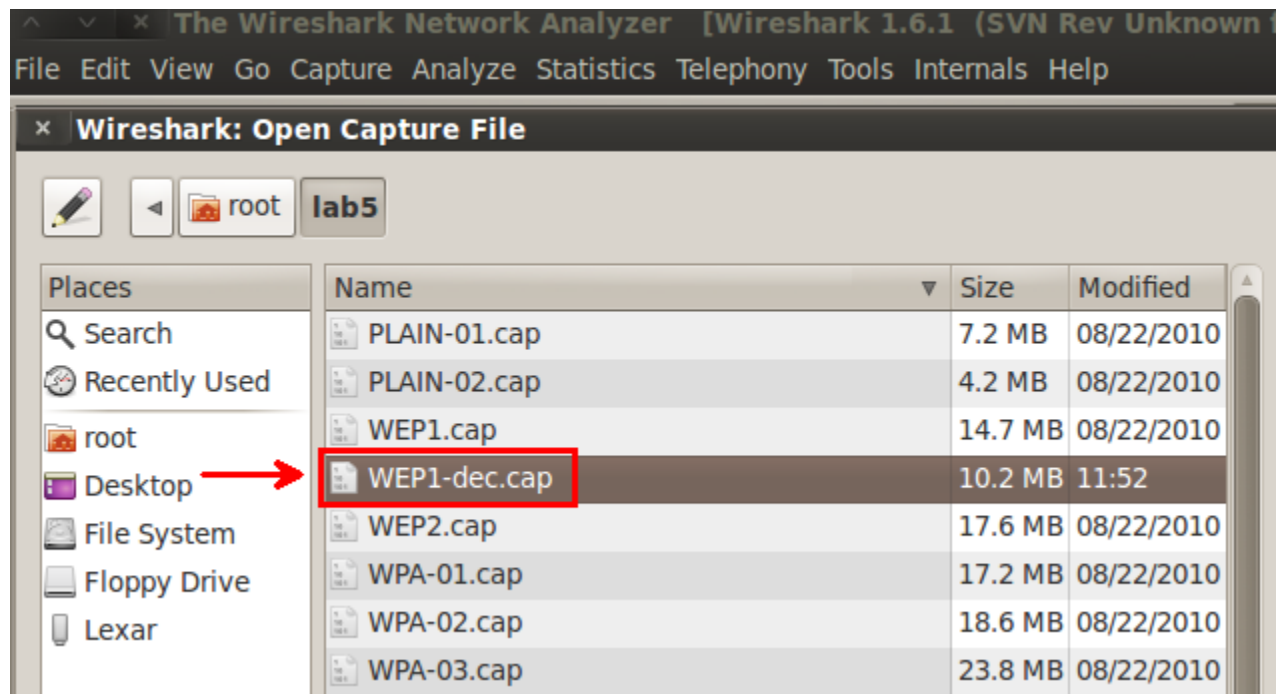


Figure 24: The Newly Created WEP1-dec Capture File

When **airdecap-ng** was used, the traffic from the wireless network with the SSID of **TOWSON22** was decrypted because the correct WEP key was provided. A brand new capture file, **WEP1-dec.cap** is created with the traffic decrypted.

- In the filter pane, type **dns** (all lowercase) and click **Apply**. You will be able to see DNS requests within the wireless traffic because the WEP traffic was decrypted.

Filter: dns		Expression... Clear Apply			
Time	Source	Destination	Protocol	Length	Info
59.352370	192.168.1.1	192.168.2.5	DNS	261	Standard query response CNAME b.scorecard
60.606790	192.168.2.5	192.168.1.1	DNS	75	Standard query A news.google.com
60.628850	192.168.1.1	192.168.2.5	DNS	160	Standard query response CNAME news.l.goog
61.278597	192.168.2.5	192.168.1.1	DNS	73	Standard query A id.google.com
71.825928	192.168.2.5	192.168.1.1	DNS	83	Standard query A core.caster.espn.go.com
71.847474	192.168.1.1	192.168.2.5	DNS	99	Standard query response A 68.71.209.229
80.520262	192.168.2.5	192.168.1.1	DNS	83	Standard query A www.baltimoreravens.com

Figure 25: DNS traffic is Now Viewable

9. From the Wireshark menu, select **File>Export>Objects>HTTP**. A new window will open, showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Under the **Packet number** column, find item **#6988 (NFL-Football.jpg)**, click on the file, and click **Save As**. Verify the **Save in folder** is **root** and click **Save**.

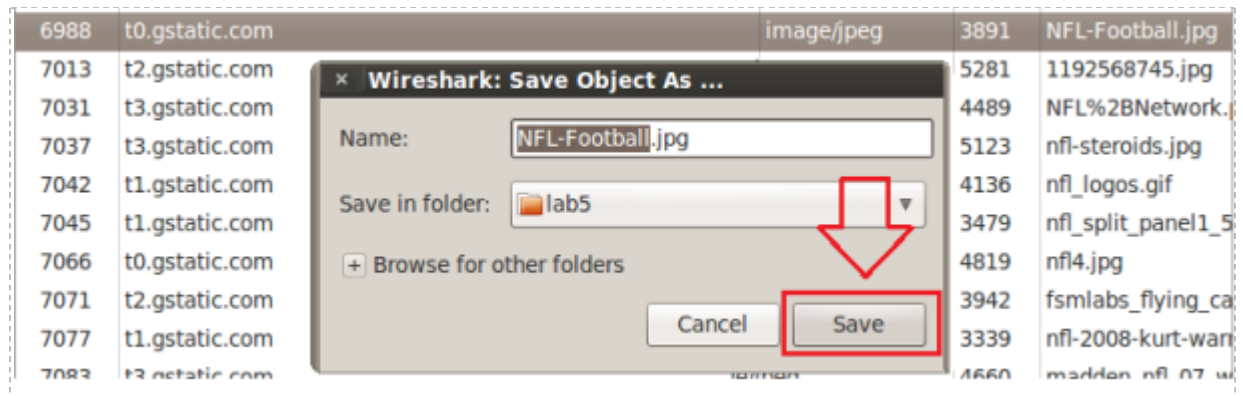


Figure 26: Carving the Image form Wireshark

10. To view the file, click **Places** from the BackTrack 5 Menu Bar and select **Home Folder**. Close the **Home folder** and click **Cancel** to close the Wireshark: HTTP Object List

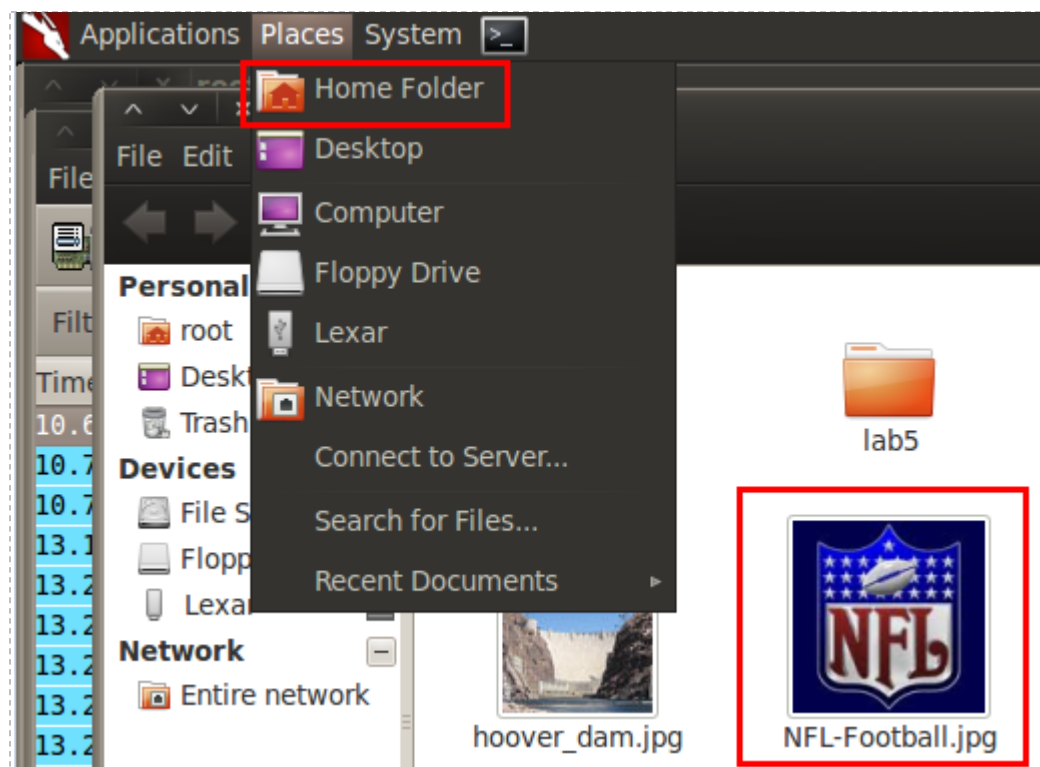
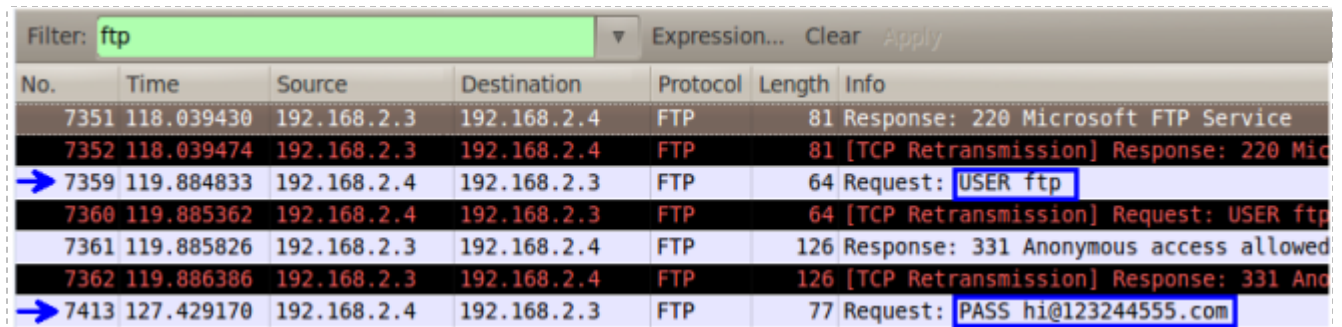


Figure 27: Viewing the Picture Carved From Wireshark

After the WEP traffic for the TOWSON22 network was decrypted, we will be able to view any of the clear text traffic within the capture file. We will examine the FTP traffic.

11. Type **ftp** (all lowercase) in the Wireshark filter pane and click **Apply**. You will be able to see the decrypted FTP traffic, as well as the usernames and passwords.



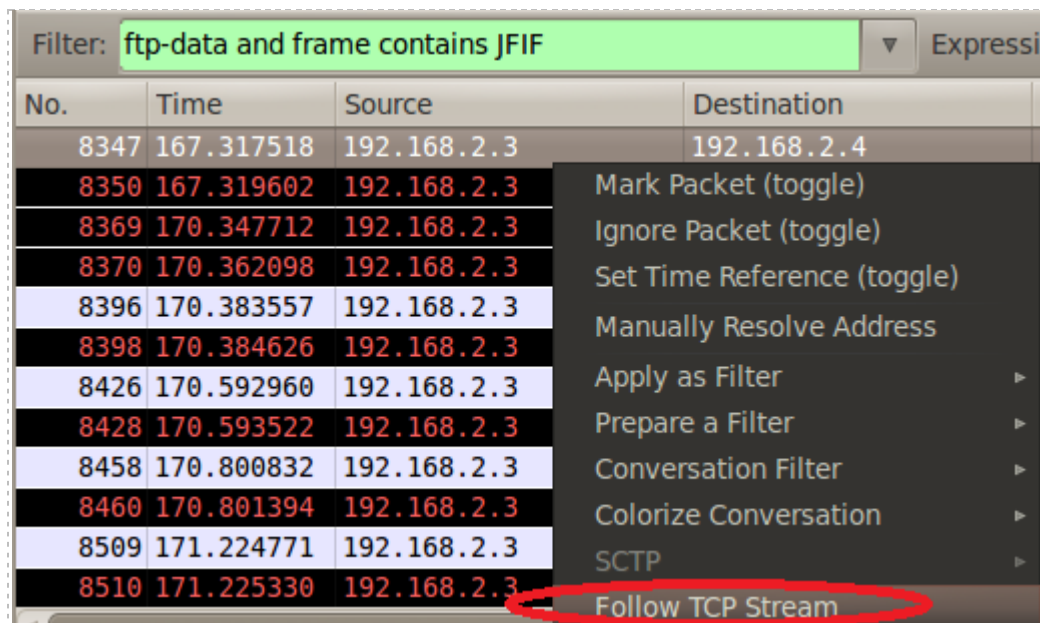
The image shows a Wireshark packet capture window with the filter 'ftp' applied. The packet list shows several FTP packets. The packet details pane for packet 7359 shows the 'Request' field with the text 'USER ftp'. The packet details pane for packet 7413 shows the 'Request' field with the text 'PASS hi@123244555.com'.

No.	Time	Source	Destination	Protocol	Length	Info
7351	118.039430	192.168.2.3	192.168.2.4	FTP	81	Response: 220 Microsoft FTP Service
7352	118.039474	192.168.2.3	192.168.2.4	FTP	81	[TCP Retransmission] Response: 220 Mic
7359	119.884833	192.168.2.4	192.168.2.3	FTP	64	Request: USER ftp
7360	119.885362	192.168.2.4	192.168.2.3	FTP	64	[TCP Retransmission] Request: USER ftp
7361	119.885826	192.168.2.3	192.168.2.4	FTP	126	Response: 331 Anonymous access allowed
7362	119.886386	192.168.2.3	192.168.2.4	FTP	126	[TCP Retransmission] Response: 331 And
7413	127.429170	192.168.2.4	192.168.2.3	FTP	77	Request: PASS hi@123244555.com

Figure 28: Viewing the Clear Text Traffic from the Decrypted Capture File

If you scroll down further in the WEP1-dec.cap file, you will be able to see the names of the files that were transferred by the wireless user with the FTP protocol.

12. To pull a JPEG file transferred via FTP out of the wireless capture file, type **ftp-data and frame contains JFIF** into the Wireshark filter and hit **Apply**:
Right-click on the first frame in the list and select **Follow TCP Stream**.



The image shows a Wireshark packet capture window with the filter 'ftp-data and frame contains JFIF' applied. The packet list shows several packets. The packet details pane for packet 8347 shows the 'Request' field with the text 'USER ftp'. The packet details pane for packet 8510 shows the 'Request' field with the text 'PASS hi@123244555.com'. A right-click context menu is open over packet 8510, and the 'Follow TCP Stream' option is highlighted with a red circle.

No.	Time	Source	Destination
8347	167.317518	192.168.2.3	192.168.2.4
8350	167.319602	192.168.2.3	192.168.2.4
8369	170.347712	192.168.2.3	192.168.2.4
8370	170.362098	192.168.2.3	192.168.2.4
8396	170.383557	192.168.2.3	192.168.2.4
8398	170.384626	192.168.2.3	192.168.2.4
8426	170.592960	192.168.2.3	192.168.2.4
8428	170.593522	192.168.2.3	192.168.2.4
8458	170.800832	192.168.2.3	192.168.2.4
8460	170.801394	192.168.2.3	192.168.2.4
8509	171.224771	192.168.2.3	192.168.2.4
8510	171.225330	192.168.2.3	192.168.2.4

Figure 29: Following a TCP Stream

13. In the Follow the TCP Stream pane, click the **Save As** button.
For the name of the file, put **pic.jpg**. Make sure the **Save in Folder** is **Desktop**.
Double-click on picture on your Desktop. It should be men playing basketball.
Close the picture window and the **Follow TCP Stream** window when finished.

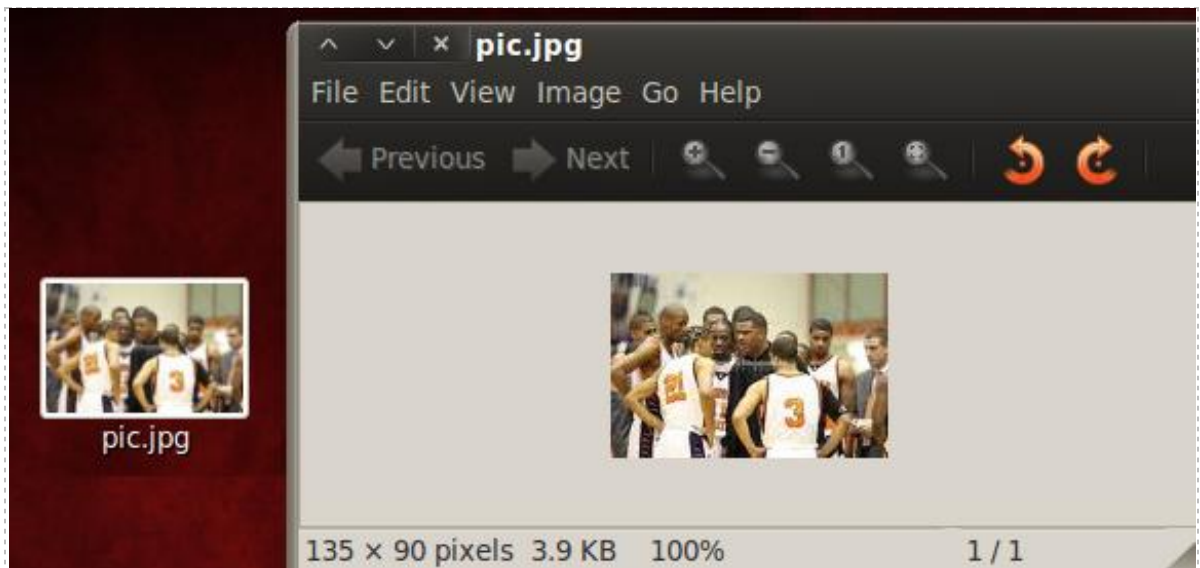


Figure 30: The Picture is Successfully Carved from the FTP Transfer

2.2 Conclusion

Wired Equivalent Privacy, or WEP, encrypts traffic and protects your wireless network from people monitoring wireless networks using a Wi-Fi card in monitor mode. If an attacker is able to get the WEP key by generating enough Initialization Vectors, or IVs, they can decrypt the traffic using airdecap-ng. Traffic can then be viewed and analyzed.

2.3 Discussion Questions

1. Provide the name of at least one file that was transferred during the FTP session.
2. What is the name of the tool that can be utilized to decrypt WEP traffic? What must you do in conjunction with the tool for the traffic to be decrypted?
3. Which 2 IP addresses were involved in the transfer of data via the FTP protocol?

3 Exploiting and Examining WPA Traffic

Wi-Fi Protected Access, or WPA, and WPA2 are much more secure than WEP encryption. An attacker can break WEP, regardless of what WEP key is used, if they are able to generate enough Initiation Vectors (IVs). Wi-Fi Protected Access (WPA) and WPA2 are more secure but it also is vulnerable to being hacked if a weak passphrase, like a dictionary word, is used. A good passphrase should be at least 16 characters long, use uppercase, lowercase, and special characters. Avoid the use of dictionary words.

3.1 Exploiting WPA and Analyzing the Traffic

1. Open the **WPA Capture File**
 - a. Select **File** from the Wireshark menu and select **Open**.
 - b. Double click on the **root** folder, and then double click on the **lab5** folder.
 - c. Double click on the file **WPA-01.cap**.
2. In the filter pane, type **ftp** (all lowercase) and click **Apply**. You will not be able to see any traffic because the wireless network traffic is encrypted. Close Wireshark.

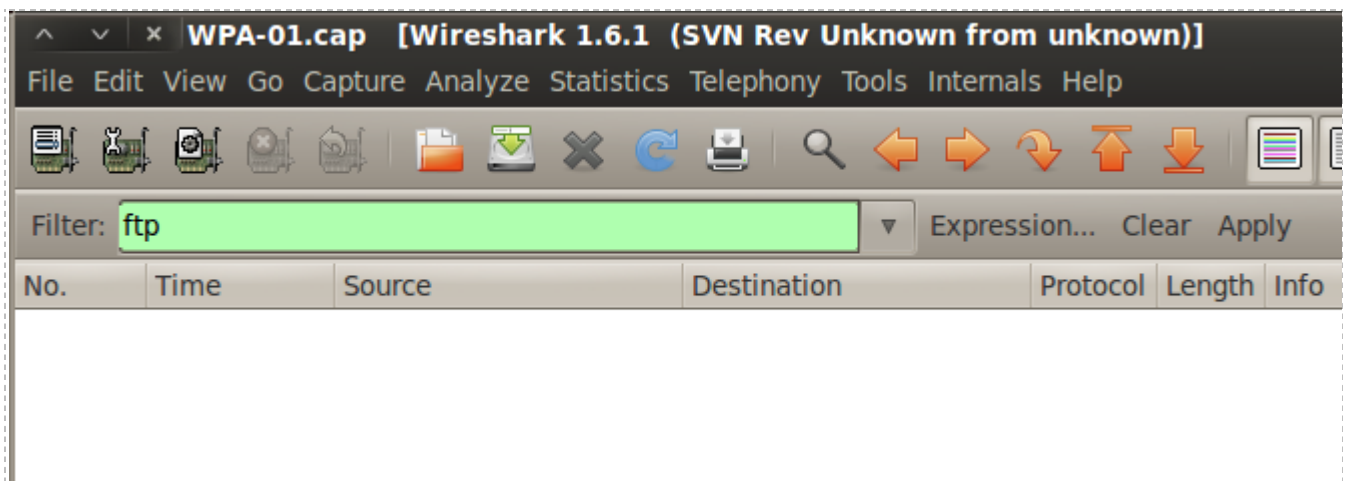


Figure 31: FTP Traffic is Un-viewable in the WPA Encrypted Capture File

In order to break the WPA passphrase, you need the following items:

- The SSID (Service Set Identifier), or name, of the wireless network
- A WPA handshake
- A dictionary file

The SSID of our target wireless network is TOWSON333. In order to get a WPA handshake, the attacker must have a wireless card that supports monitor mode and needs to perform a de-authentication attack, which will remove a client from the Access Point (AP) for less than a second. The attacker will also need a dictionary file. In order for the attacker to obtain the WPA passphrase, the phrase must be in the dictionary file.

- In the terminal window, type the following command.
`root@bt:~# aircrack-ng lab5/WPA-01.cap -w Wordlist.txt`

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# aircrack-ng lab5/WPA-02.cap -w Wordlist.txt
Opening lab5/WPA-02.cap
Read 33915 packets.

# BSSID ESSID Encryption
1 00:1F:90:D9:C6:28 HUANGDOM WEP (19 IVs)
2 00:18:4D:8A:78:FE boquswifi WPA (0 handshake)
3 00:17:3F:F4:56:90 TOWSON333 WPA (1 handshake)
4 00:1F:90:D8:B2:84 RP7J4 WEP (6583 IVs)
5 00:26:62:E5:71:8C T4QY4 WPA (0 handshake)
6 00:24:B2:DA:A8:7A No data - WEP or WPA
7 00:26:F2:9B:08:4C Anthony98 No data - WEP or WPA

Index number of target network ? 3

```

Figure 32: Selecting the Target Network Using WPA

- Select **3** for the target network. Notice that there is 1 WPA handshake

```

Aircrack-ng 1.1 r1904

[00:00:31] 25316 keys tested (813.29 k/s)

KEY FOUND! [ breezeless ]

Master Key   : 69 24 A8 65 AF BF 71 4E 9E 25 25 C0 2A 71 E3 AB
              59 E9 B3 6E 9A 4D B1 47 5E 1E 01 BD 9E 7B 80 AE

Transient Key : FB 91 BB 94 87 12 4D E6 F9 D2 CC 82 71 CC 0F E5
              DD D2 2A 9B 79 47 A9 B5 7C 0C 46 C6 30 82 C2 A8
              3E CB 55 CD 6F 86 67 18 71 2C B8 22 D3 E2 43 F2
              67 E8 63 6D EF 93 F9 EF 03 77 F5 80 5F 0A 43 61

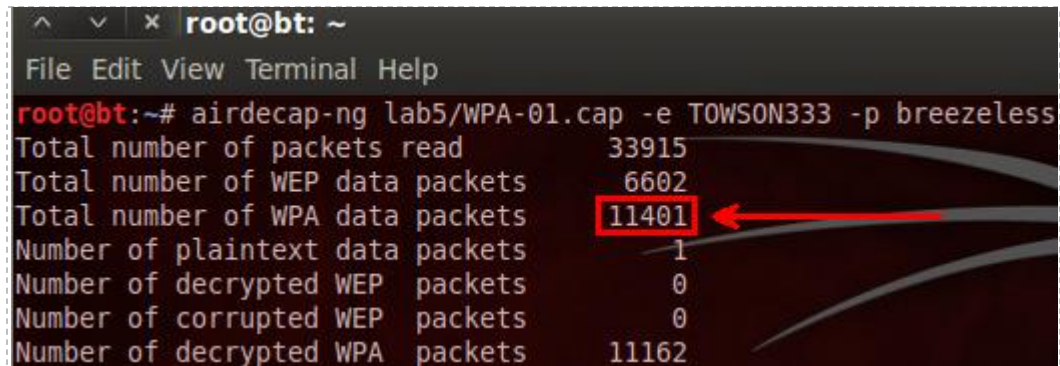
EAPOL HMAC   : 8C EA C6 47 4C 5A CB 75 7C D2 71 82 52 9E 85 54

```

Figure 33: The WPA Passphrase

Now that the WPA passphrase has been obtained, we can decrypt the traffic for the wireless network TOWSON333. In order to do this, the SSID must be specified.

5. Type the From the terminal, type the following command to decrypt the traffic:
`root@bt:~# airdecap-ng lab5/WPA-01.cap -e TOWSON333 -p breezeless`



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# airdecap-ng lab5/WPA-01.cap -e TOWSON333 -p breezeless
Total number of packets read      33915
Total number of WEP data packets   6602
Total number of WPA data packets  11401
Number of plaintext data packets    1
Number of decrypted WEP packets     0
Number of corrupted WEP packets     0
Number of decrypted WPA packets    11162
```

Figure 34: The WPA Packets are Decrypted

The number of decrypted WPA packets should be 11,401. Now, we will be able to analyze TCP/IP traffic as well as carve files from the decrypted capture file.

6. Type **wireshark** (all lowercase) in the terminal to bring up Wireshark. Select **File** from the Wireshark menu and select open. If necessary, double-click on the **root** folder, and then double-click on the **lab5** folder. Double-click on the file **WPA-01-dec.cap**.

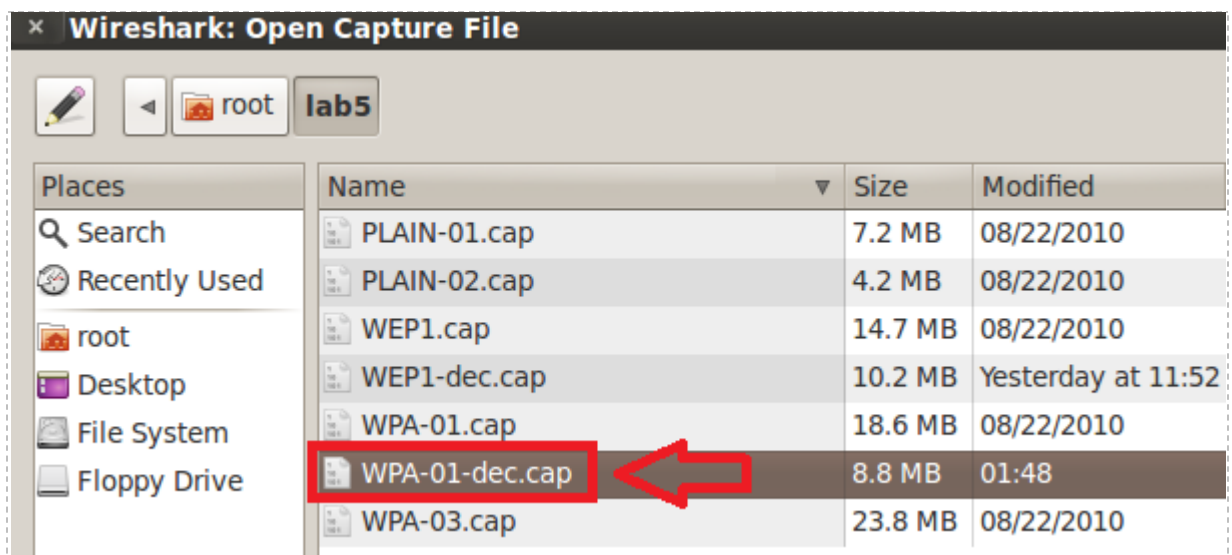


Figure 35: The Decrypted WPA file Created by airdecap-ng

- In the filter pane, type **dns** (all lowercase) and click apply. You will be able to see DNS requests within the wireless traffic because the WPA traffic was decrypted.

Filter: dns Expression... Clear Apply						
No.	Time	Source	Destination	Protocol	Length	Info
10370	73.204794	192.168.2.3	192.168.1.1	DNS	76	Standard query A video.google.com
10371	73.209401	192.168.2.3	192.168.1.1	DNS	75	Standard query A img.youtube.com
10372	73.225842	192.168.1.1	192.168.2.3	DNS	162	Standard query response CNAME vide
10373	73.232498	192.168.1.1	192.168.2.3	DNS	120	Standard query response CNAME ytim
10450	74.206838	192.168.2.3	192.168.1.1	DNS	75	Standard query A maps.google.com

Figure 36: Viewing the DNS Requests after the Traffic has been Decrypted

- From the Wireshark menu, select **File>Export>Objects>HTTP**. A new window will open showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Under the **Packet number** column, find item **#10349 (37558.jpg)**, click on the file, and click **Save As**. Verify the save in folder is **root** and click **Save**.

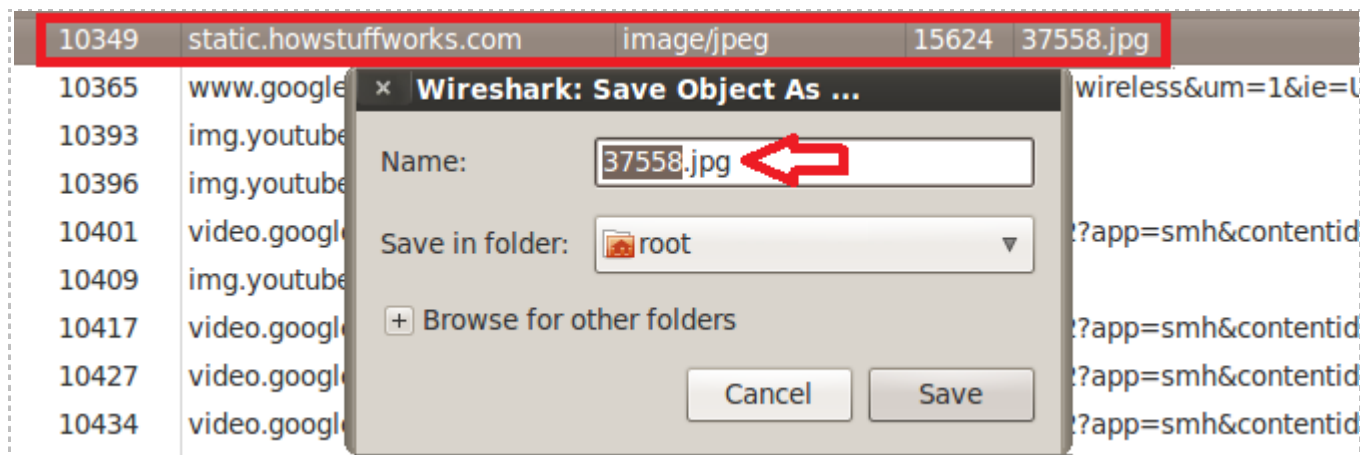


Figure 37: Extracting the JPEG from the HTTP Traffic

9. To view the file, click **Places** from the Backtrack 5 Menu Bar and select **Home Folder**. Close the **Home folder** and click **Cancel** to close the Wireshark: HTTP Object List

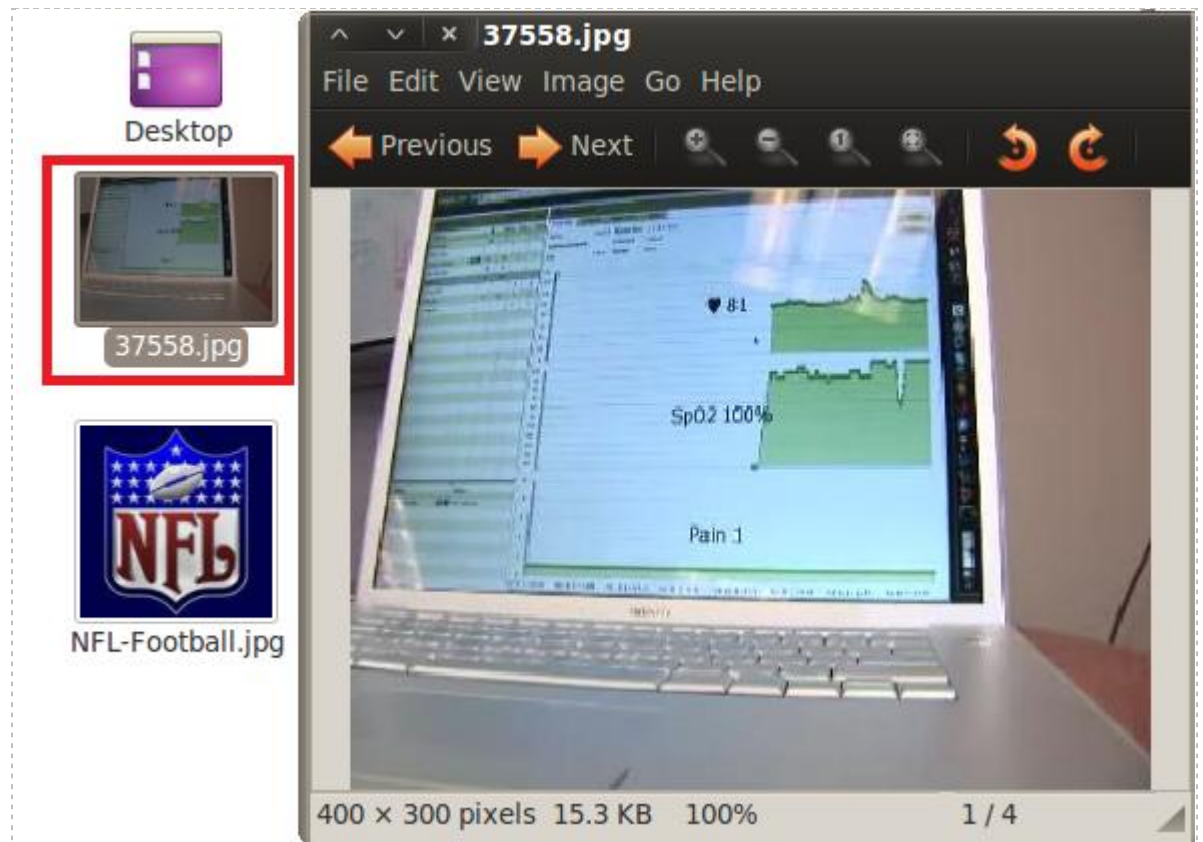


Figure 38: The File Carved from HTTP Traffic

10. Type **ftp** (all lowercase) in the Wireshark filter pane and click **Apply**. You will be able to see the decrypted FTP traffic, as well as the usernames and passwords.

Filter: ftp						Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info		
43	8.218674	192.168.2.2	192.168.2.3	FTP	60	Request: QUIT		
112	19.449104	192.168.2.3	192.168.2.2	FTP	81	Response: 220 Microsoft FTP Service		
118	21.661618	192.168.2.2	192.168.2.3	FTP	64	Request: USER ftp		
119	21.662093	192.168.2.3	192.168.2.2	FTP	126	Response: 331 Anonymous access allowed		
134	24.484978	192.168.2.2	192.168.2.3	FTP	66	Request: PASS hfafh		

Figure 39: The FTP Username and Password in Clear Text

11. Scroll down through the ftp frames and find the names of some of the files that were transferred. They include JPEG, PDF, executable, and zip files.

No.	Time	Source	Destination	Protocol	Length	Info
8745	50.187442	192.168.2.2	192.168.2.3	FTP	78	Request: RETR WinPcap 4 1 2.exe
8746	50.188430	192.168.2.3	192.168.2.2	FTP	131	Response: 150 Opening ASCII mode data c
9625	50.782928	192.168.2.3	192.168.2.2	FTP	78	Response: 226 Transfer complete.
9628	50.788594	192.168.2.2	192.168.2.3	FTP	80	Request: PORT 192,168,2,2,201,174
9629	50.790096	192.168.2.3	192.168.2.2	FTP	84	Response: 200 PORT command successful.
9630	50.797298	192.168.2.2	192.168.2.3	FTP	69	Request: RETR zip1.zip
9647	51.001040	192.168.2.3	192.168.2.2	FTP	78	Response: 226 Transfer complete.

Figure 40: The Frame Indicates the Name of the Transferred Executable and Zip File

12. To pull one of the zip files transferred via FTP out of the capture file, type **ftp-data and frame contains PK** into the Wireshark filter and hit **Apply**. Right-click on the second frame in the list (421) and select **Follow TCP Stream**.

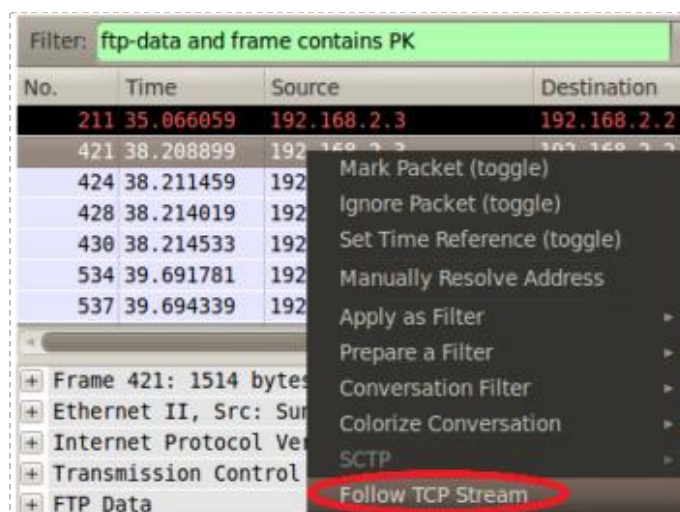


Figure 41: Following the TCP Stream

13. In the Follow the TCP Stream pane, click the **Save As** button.

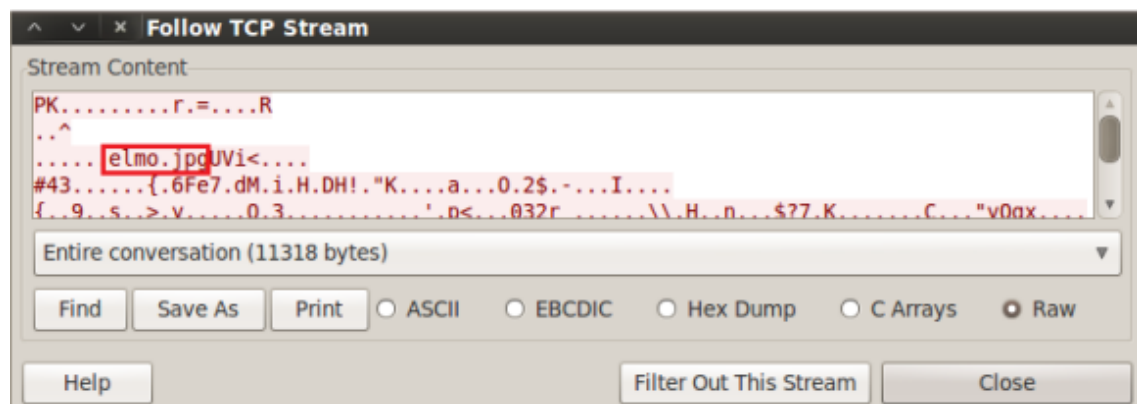


Figure 42: Saving the Zip File

14. For the name of the file, put **elmo.zip**. Use **Desktop** as the **Save in folder**.

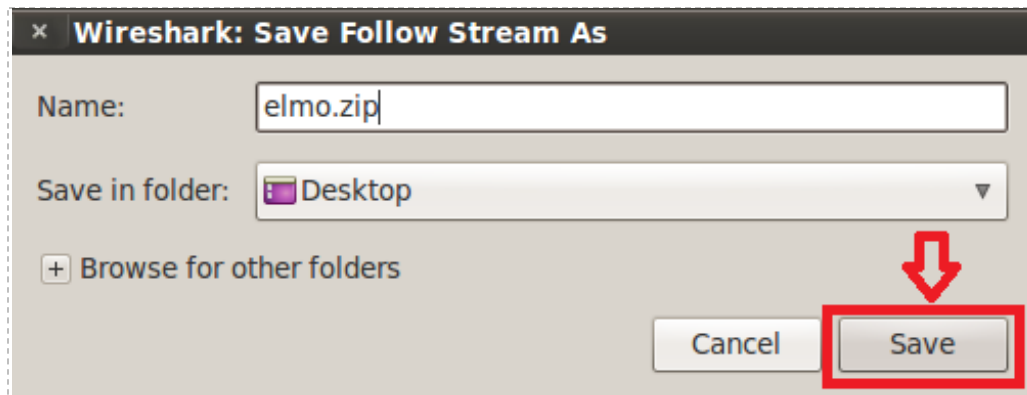


Figure 43: Naming the File and Saving it to the Desktop

15. Minimize open applications and look for the zip file you saved on the Desktop. Double-click on the brown elmo.zip icon. A white file.zip icon will appear below it. Double-click on the white elmo.zip icon and the three pictures should appear.



Figure 44: The Extracted Pictures of a Zip File

16. Close all remaining applications and terminals.

3.2 Conclusion

Although Wi-Fi Protected Access (WPA/WPA2) offers far superior security to that of its older counterpart Wired Equivalent Privacy (WEP), it also has some security risks associated with its use. If the user selects a weak passphrase, an attacker can try to obtain the password by performing a dictionary attack. In order for the attacker to obtain the WPA passphrase, they must get the WPA handshake by performing a de-authentication attack with a wireless card running in monitor mode. To properly secure a wireless network use WPA, or preferably WPA2, and a strong passphrase with at least 16 characters, and use uppercase and lowercase letters, as well as special characters.

3.3 Discussion Questions

1. Type **ftp** in the filter pane of Wireshark. Find the names of at least 2 picture files (JPEGs) that were transferred.
2. Using the same **ftp** filter in Wireshark, and find the name of the two executable (EXE) files that were transferred.
3. Type **frame contains PASS** in the filter pane of Wireshark. What was the password used to log on to the FTP site?

References

1. Wireshark:
<http://www.wireshark.org/>
2. Wi-Fi Alliance:
<http://www.wi-fi.org/>
3. Institute of Electrical and Electronics Engineers:
<http://www.ieee.org/index.html>
4. BackTrack Linux:
<http://www.backtrack-linux.org/>
5. Wireless Hacking Video:
<http://vimeo.com/3410674>