ETHICAL HACKING LAB SERIES

Lab 10: Breaking WEP and WPA Encryption

Certified Ethical Hacking Domain: Hacking Wireless Networks

Document Version: 2015-08-14

Development was funded 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 an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Lab Settings

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. Wireless Commands and Tools
2. Examining Plain text Wireless Traffic
3. Cracking and Examining Wired Equivalent (WEP) Privacy Traffic
4. Cracking and Examining Wi-Fi Protected Access (WPA) Traffic

Domain: Hacking Wireless Networks

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 than 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 is used to encrypt your wireless network traffic. While the use of WPA or WPA2 is more secure, an attacker can break into networks 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. 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 Initiation Vectors, or IV’s, they can break the 64-bit or 128-bit WEP key. A good hacker can break WEP in less than 5 minutes, so avoid using it.

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 with uppercase letters 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

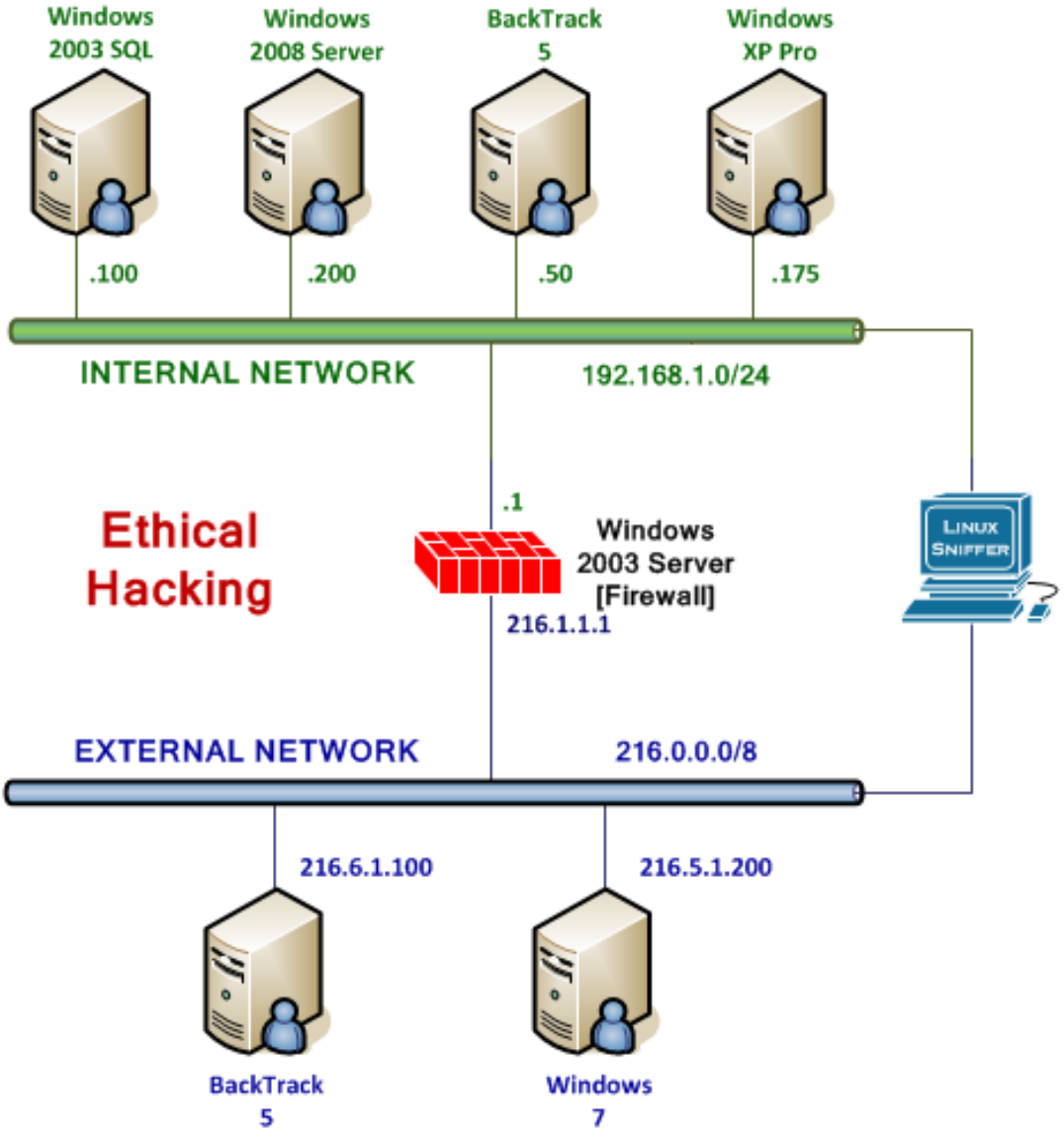

Figure 1: Lab Topology

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.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
External Backtrack 5	216.6.1.100	root	toor

1 Wireless Commands and Tools

There are many command line utilities that were designed for the use with wireless networking cards. Although you do not have a wireless card in your NETLAB+ system, you can still examine commands to see their options and become familiar with them.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Viewing Wireless Card Options

1. On the *External* Attack Machine running BackTrack Linux (version 5 R3), type **root** for the login and **toor** (root spelled backwards) for the password.

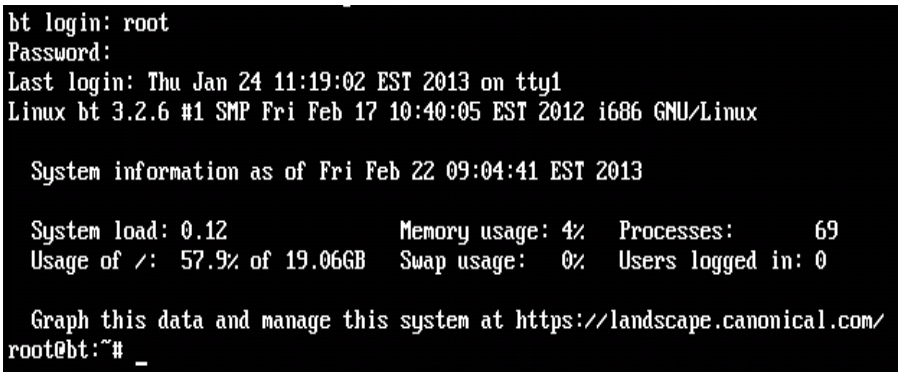

Figure 2: Logging in as root

2. Type the following command to start the Graphical User Interface (GUI).
root@bt:~# **startx**

Figure 3: The startx command

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

Figure 4: The Linux Terminal

4. Type the following command to determine if you have any wireless cards:
root@bt:~# **iwconfig**

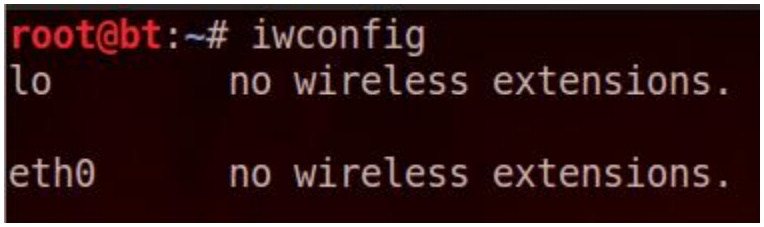

Figure 5: The iwconfig command

If you had a wireless card, the interface would appear, likely a wlan0 .

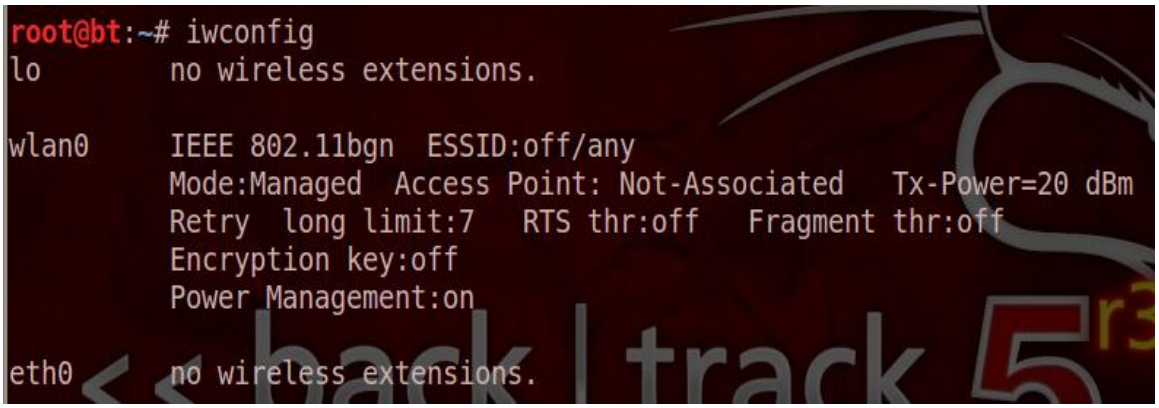

Figure 6: The iwconfig command

Notice that the card is in managed mode. Managed mode is the normal mode of operation for wireless cards. The card can be put into monitor mode using iwconfig.

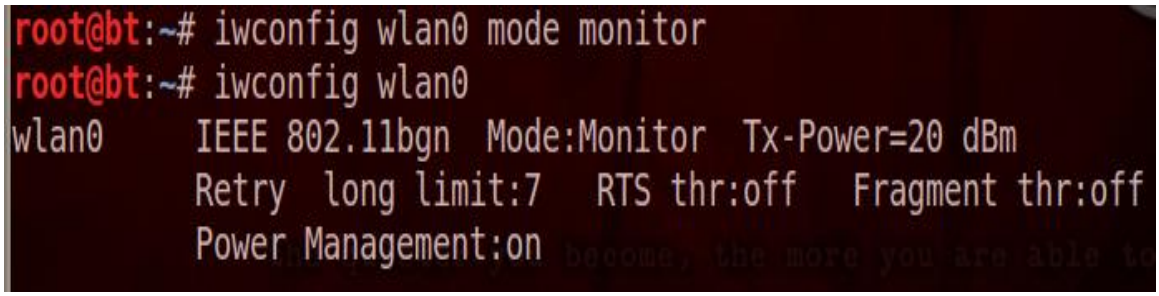

Figure 7: Putting the Card in Monitor Mode

Do not type the above command; there is no Wi-Fi card on the NETLAB+ system.

The **airodump-ng** command can be used to passively capture wireless traffic.

5. Type the following command to view the options
   root@bt:~# **airodump-ng --help**

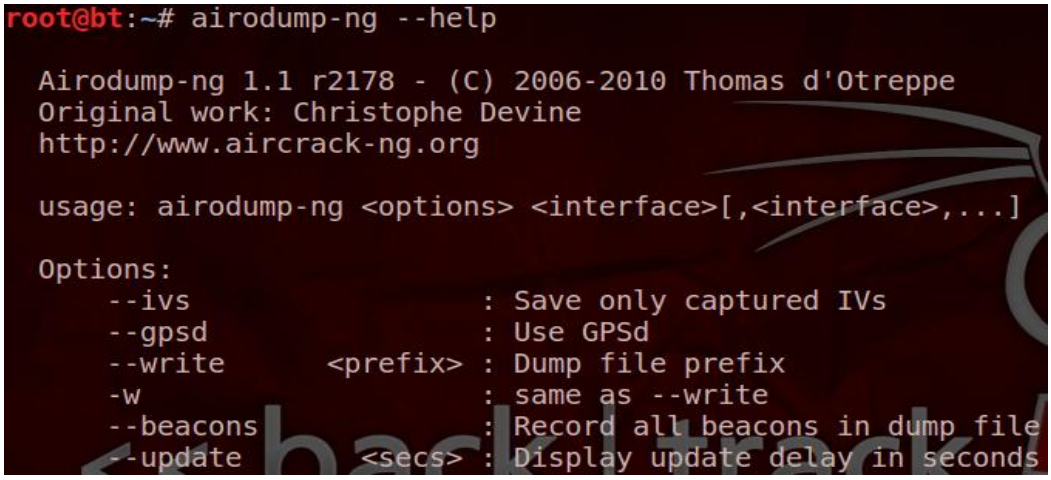

Figure 8: The airodump-ng command

When the program runs, you will see the MAC addresses and AP names in the top pane. You will see the MAC address of the AP and the MAC of the stations in the bottom pane.

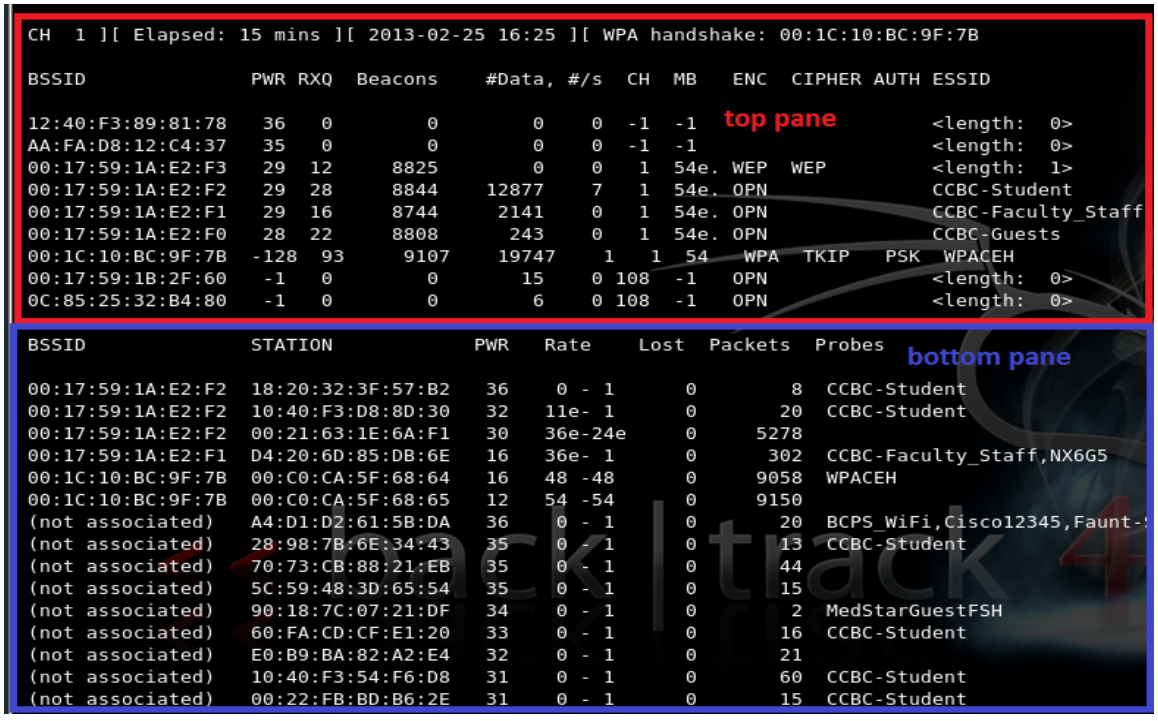

Figure 9: airodump-ng in action

Another command that can be utilized for wireless purposes is **aireplay-ng**. This command is used to perform replay attacks for WEP cracking or de-authentication attacks. A de-authentication attack can be used during WEP and WPA attacks to knock a

client off the network. All cards do not have support for the de-authentication capability, but most of the ALFA cards do support it. These cards on available from a variety of vendors, such as, http://www.data-alliance.net/.

6. To see all of the available options for the aireplay-ng command, type: root@bt:~# **aireplay-ng**

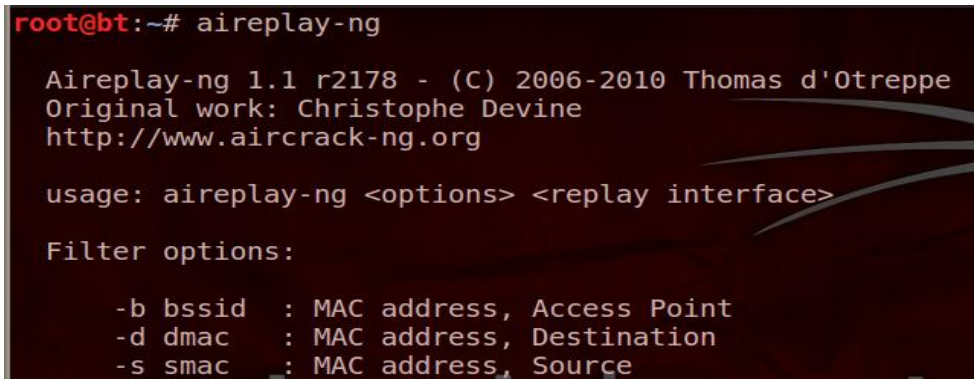

Figure 10: aireplay-ng command

An example of the aireplay-ng command being used in a de-authentication attack.

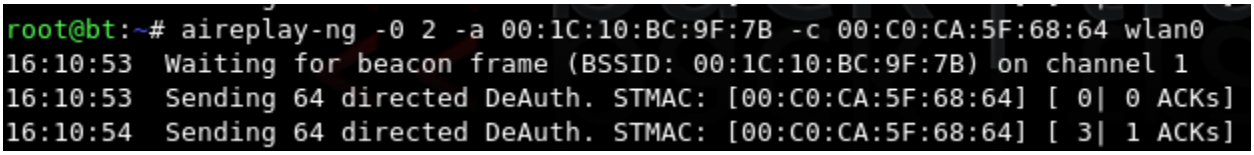

Figure 11: aireplay-ng Command in Action

1.2 Conclusion

There are many Linux commands that are specifically for use with wireless cards. Even though there is not a wireless card present in the NETLAB system, we can still get familiar with the commands by typing them and viewing the available switches.

2 Examining Plain Text Traffic

When a wireless network card is run in monitor mode, it can capture all of the wireless traffic within range of the 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 at all work 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.

2.1 Using Wireshark to Examine Text Traffic

1. Type **wireshark** (all lowercase) to bring up the Wireshark program.

Figure 12: Wireshark

2. Select the checkbox marked **Don't show this message again**, and click **OK**.

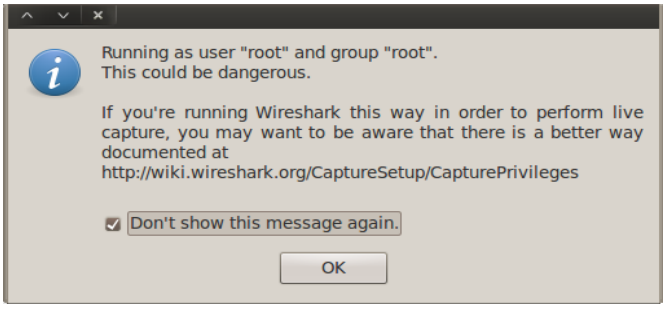

Figure 13: Allow Wireshark to run as root

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 **Lab10** folder. Double-click on the file **lab10open.cap**.

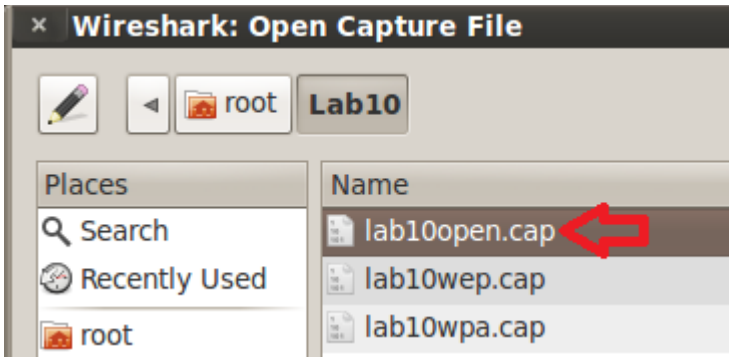

Figure 14: Opening the First Capture File

4. Type **icmp** in the Wireshark filter pane and hit **Enter**. View the IP addresses that are displayed. If the traffic was encrypted, you would be able to see MAC addresses, but not IP addresses.

Filter: icmp Expression... Cl

No.	Time	Source	Destination	Protocol
15595	240.053778	192.168.1.106	192.168.1.105	ICMP
15597	240.053762	192.168.1.106	192.168.1.105	ICMP
15600	240.086032	192.168.1.105	192.168.1.106	ICMP
15602	240.086018	192.168.1.105	192.168.1.106	ICMP
15640	240.906832	192.168.1.106	192.168.1.105	ICMP
15642	240.906818	192.168.1.106	192.168.1.105	ICMP
15665	240.959055	192.168.1.105	192.168.1.106	ICMP
15677	240.988226	192.168.1.105	192.168.1.106	ICMP
15714	241.904779	192.168.1.106	192.168.1.105	ICMP
15716	241.905282	192.168.1.106	192.168.1.105	ICMP
15733	241.957519	192.168.1.105	192.168.1.106	ICMP
15746	242.012290	192.168.1.105	192.168.1.106	ICMP

Figure 15: Filter of ICMP

While IP address disclosure is one concern, there are far greater concerns to be worried about than giving away an IP address. For one, usernames and passwords can also be extracted from the traffic. Data, like PDF files, can also be extracted.

5. In order to view file transfer protocol traffic, type **ftp** in the Wireshark filter pane and click **Apply**. You can view usernames and passwords in clear text.

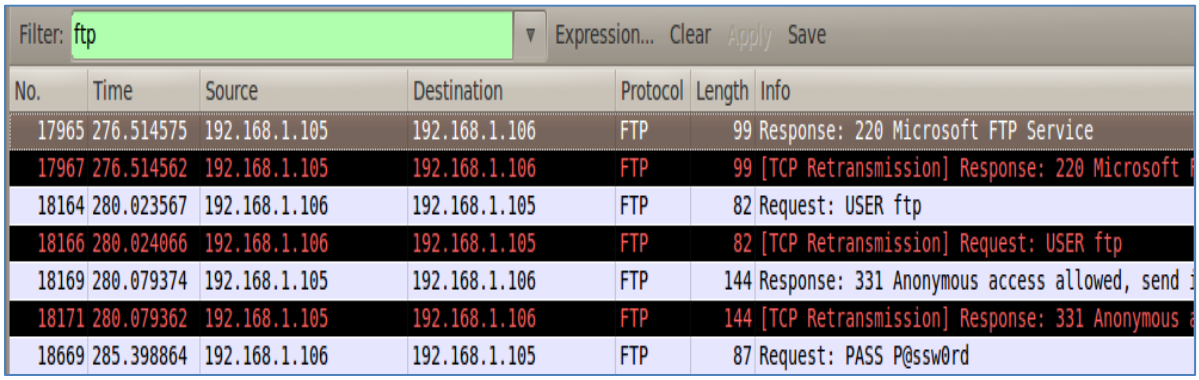

Figure 16: ftp Filter in Wireshark

6. Click **Clear** to remove the ftp filter. From the Wireshark menu, select **File > Export Objects > HTTP.**

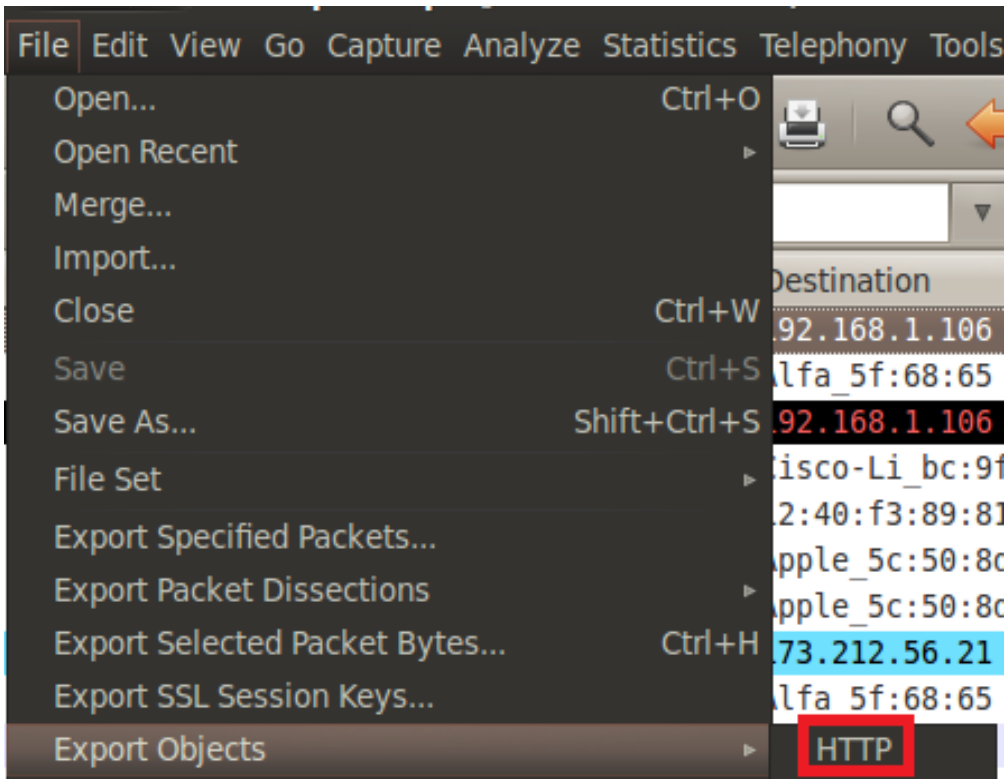

Figure 17: Saving an HTTP Object Parsed from Wireshark

7. Click the **Save All** button in the lower-right side of the HTTP object list.

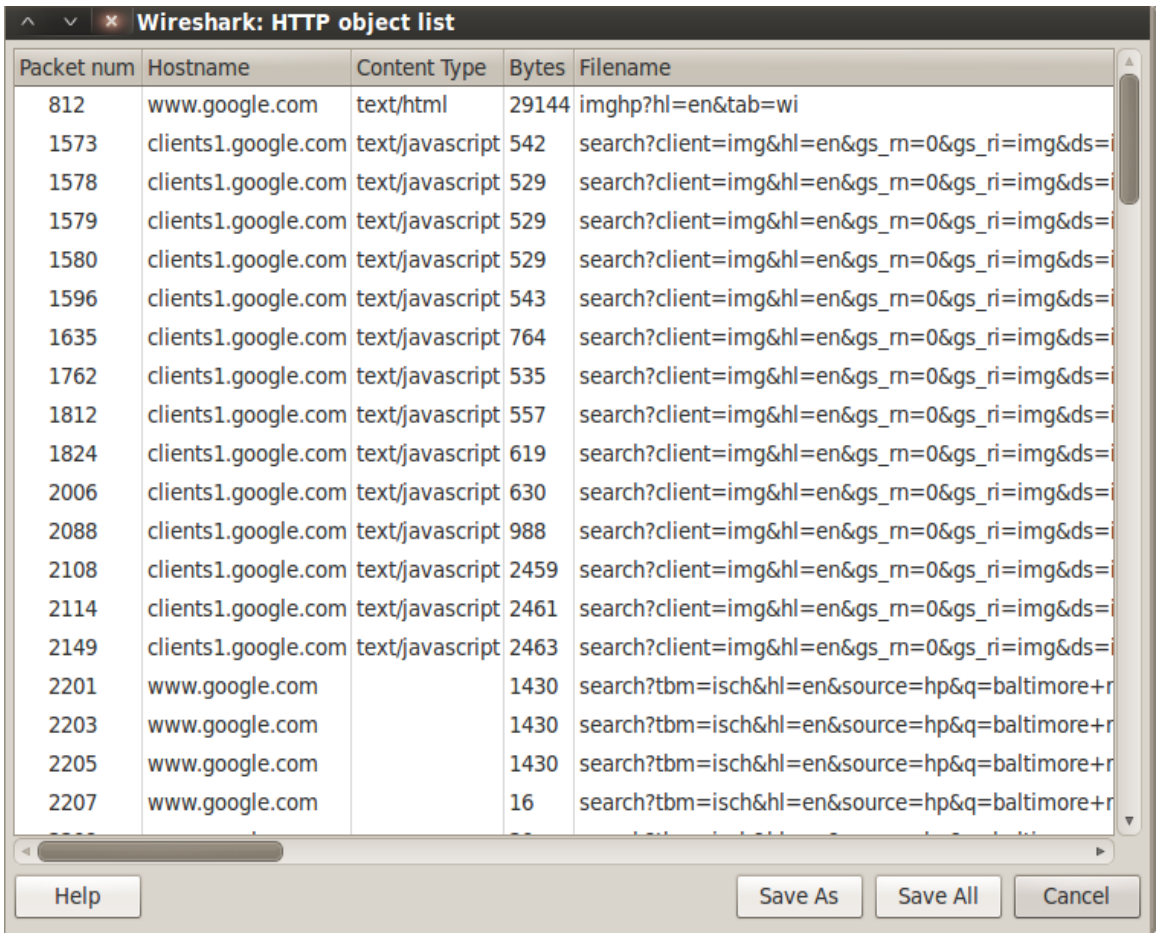

Figure 18: Saving an HTTP Object Parsed from Wireshark

8. In the Name box, type **open** and click **OK**.

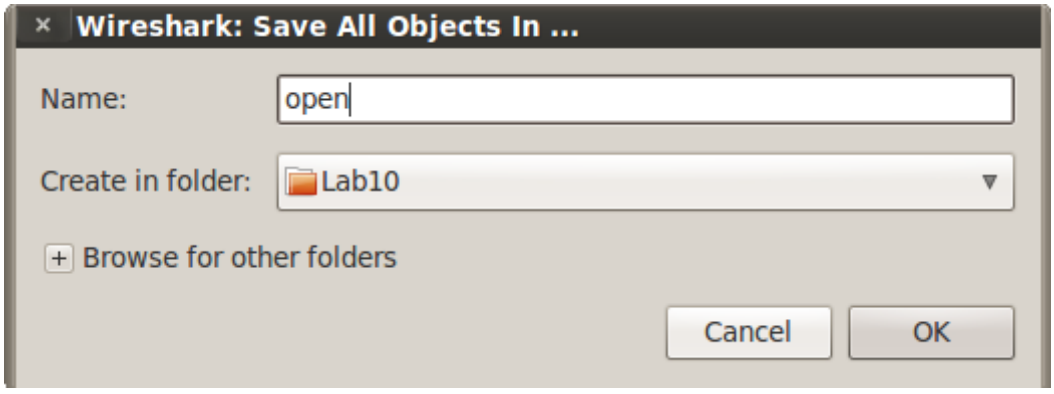

Figure 19: Saving HTTP Objects Parsed from Wireshark

9. Click **OK** to some files cannot be saved (if you receive this message, some users may not).

10. To view the file, click **Places** from the Linux menu bar and select **Home Folder**. Double-click on the **Lab 10** folder, and then double-click on the **Open** folder. You will see pictures of the Baltimore Ravens logos as well as Angry Birds pictures.

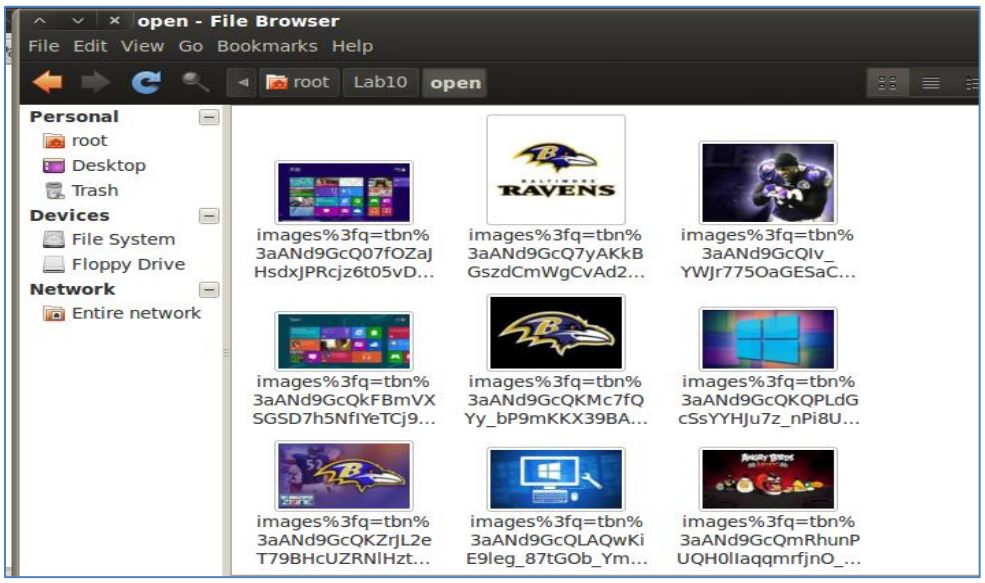

Figure 20: The Pictures Carved From Wireshark

Close the Open picture folder and close the Wireshark HTTP object list.

11. To pull a PDF file transferred via FTP out of the wireless capture file, type the following filter into Wireshark and select **Apply**:
    frame contains PDF
12. Right-click on frame **23478** in the list and select **Follow TCP Stream**.

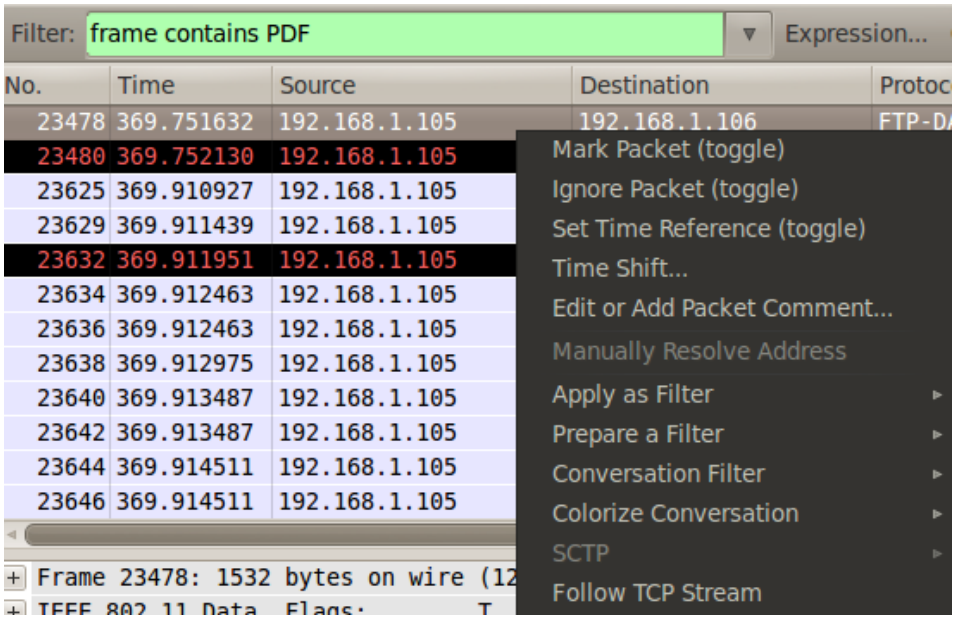

Figure 21: frame contains PDF

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

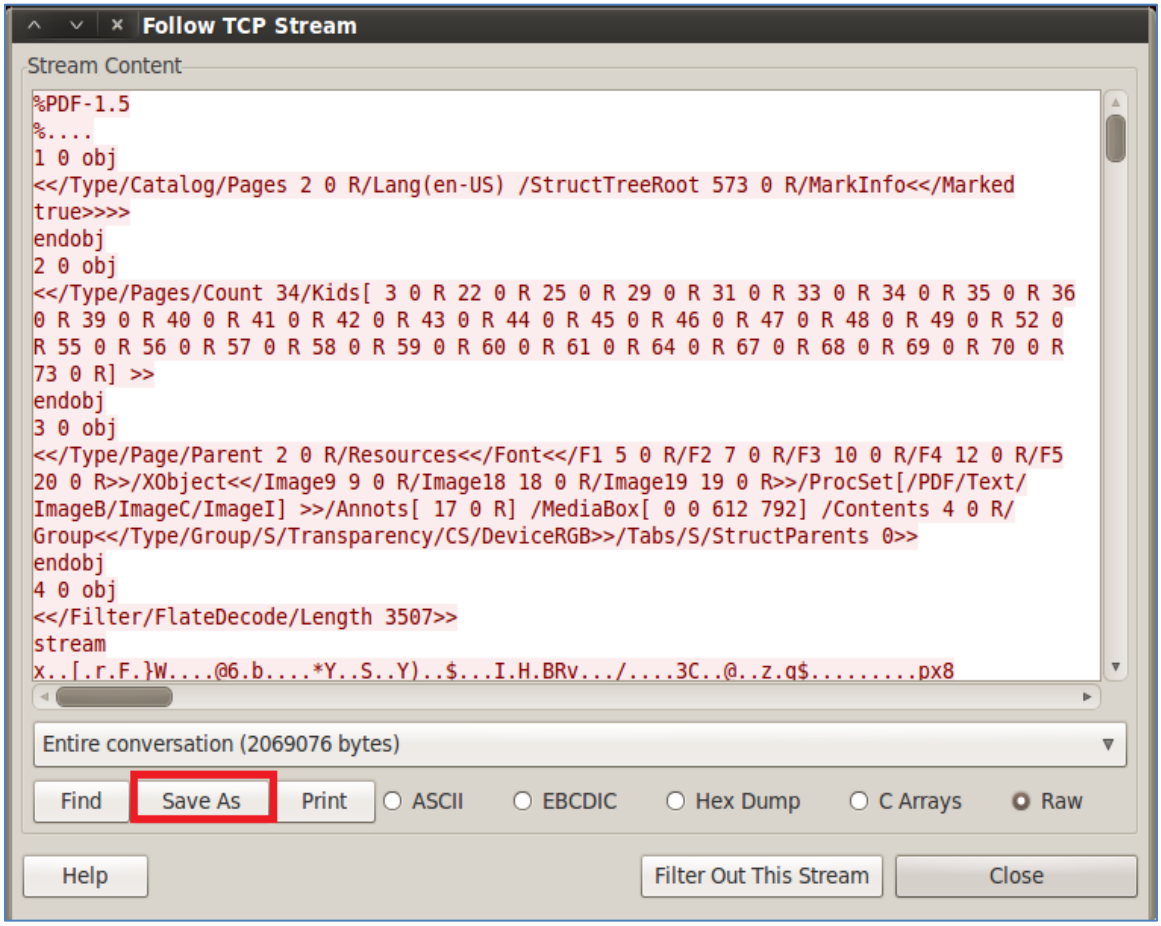

Figure 22: The Follow TCP Stream Window

14. For the name of the file, put **1.pdf**. Make sure the Save in folder is **Lab10**, and click **Save**.

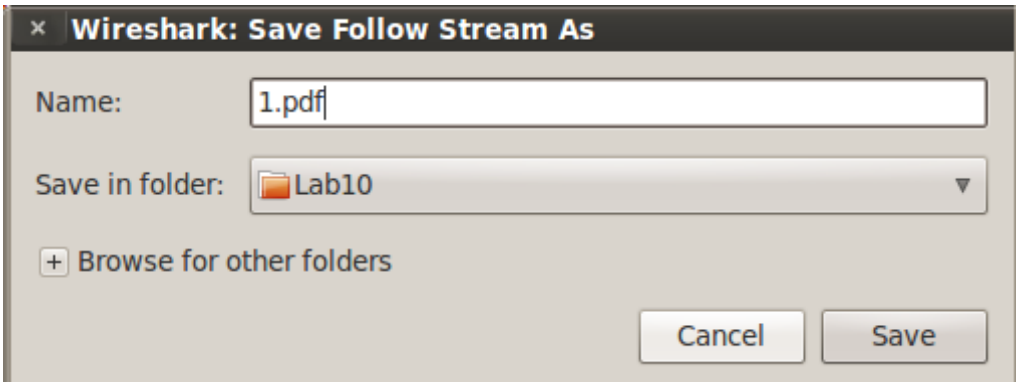

Figure 23: Saving the Zip file From the TCP Stream

15. To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Double-click on the **Lab10** folder and double-click **1.pdf** to open it.

Figure 24: Opening the PDF File and Viewing the Pictures.

16. Close the PDF file and all of the other windows you have open, except the terminal.

2.2 Conclusion

Using an unsecured wireless network has serious security risks. If a wireless card is running in monitor mode, it can capture all traffic to and from the access point. This includes the ability to view DNS requests, view HTTP traffic, and the ability 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.

3 Cracking and Examining WEP Traffic

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.

3.1 Using Wireshark to Crack and Examine WEP Traffic

1. In the terminal window, type the following command:
   root@bt:~# **cd Lab10**

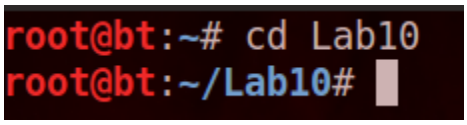

Figure 25: Selecting the Number of the Target Network

2. In the terminal window, type the following command:
   root@bt:~/Lab10# **aircrack-ng lab10wep.cap**
3. Enter **3** as the Index number of the target network.

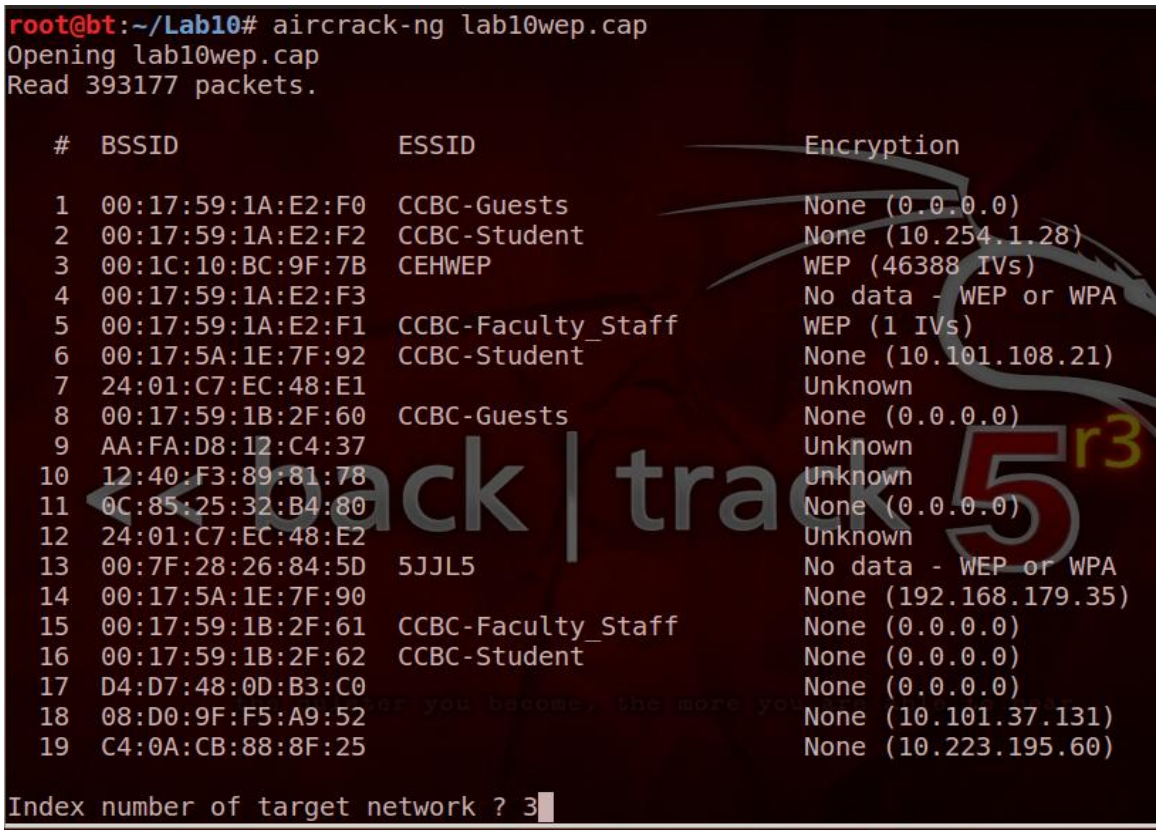

Figure 26: Selecting the Number of the Target Network

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

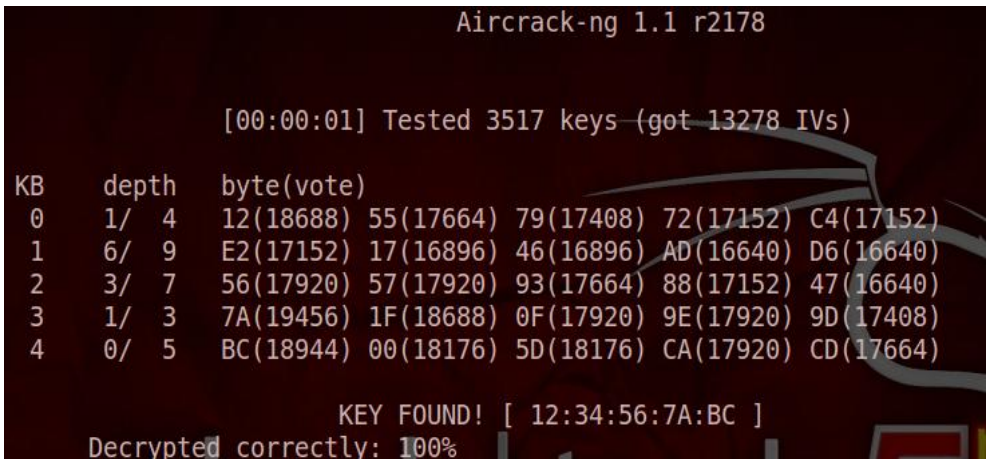

Figure 27: Aircrack-ng provides you with the WEP key to the Network

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

4. From the terminal, type the following command to decrypt the traffic (10 A's):
   root@bt:~/Lab10# **airdecap-ng –w 1234567ABC lab10wep.cap**

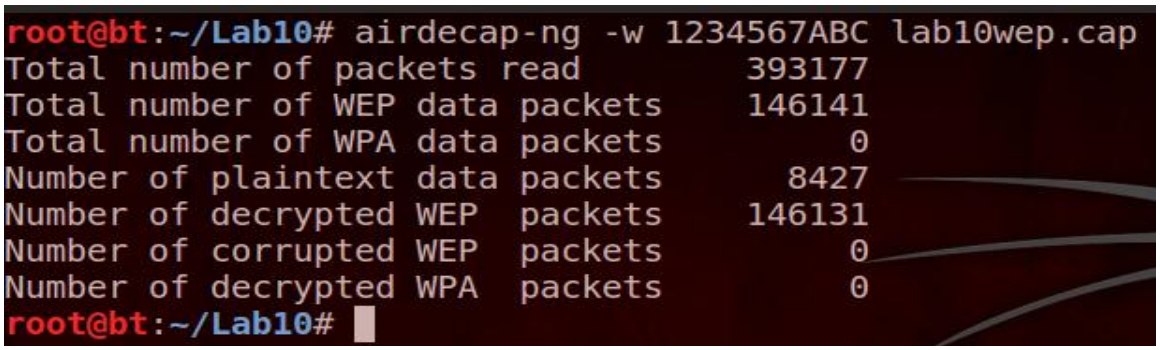

Figure 28: WEP Packets are Decrypted with the Key

5. Type the following to list all of the files and folders within the lab10 directory:
   root@bt:~/Lab10# **ls**

Figure 29: Newly Created Decrypted Capture File

The lab10wep-dec.cap file was created when you ran the airdecap-ng program.

6. Type the following command to open the decrypted file with Wireshark:
root@bt:~/Lab10# **wireshark lab10wep-dec.cap**

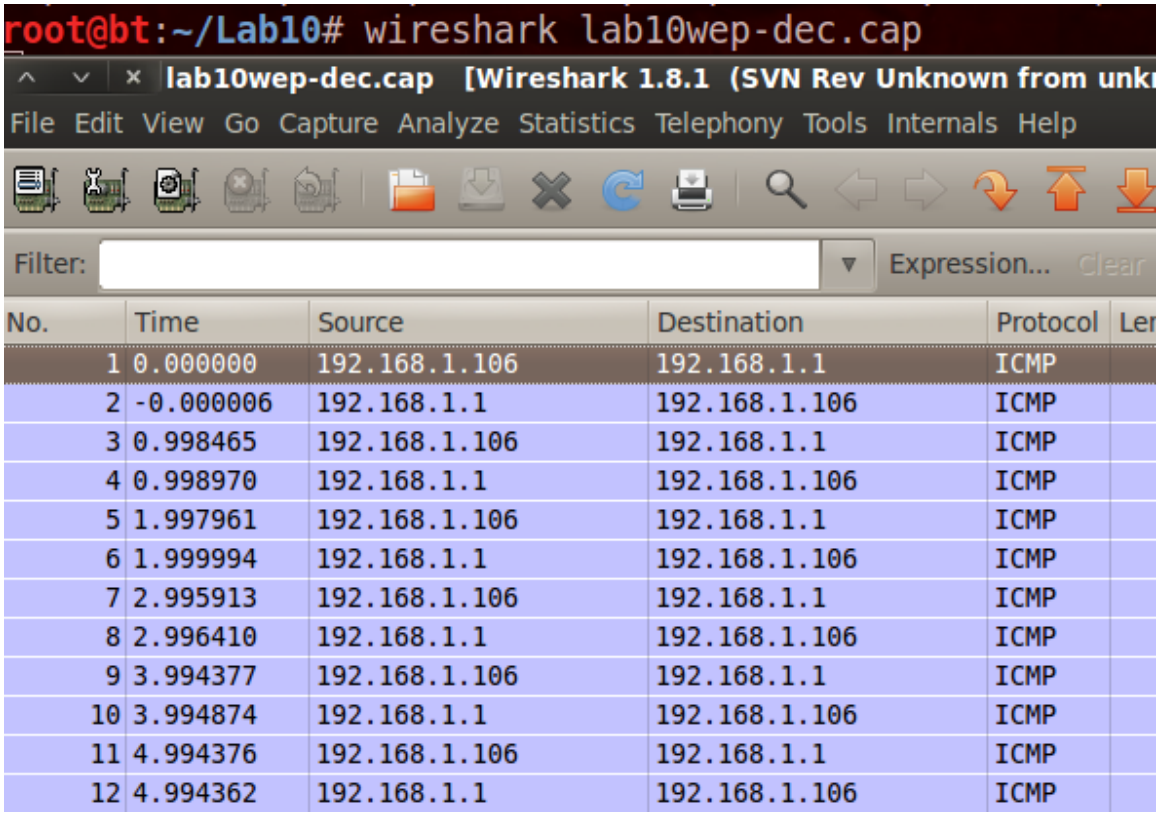

Figure 30: The Newly Created lab10-wep Capture File

7. In order to view post office protocol traffic, type **pop** in the Wireshark filter pane and click **Apply**. You can view usernames and passwords in clear text.

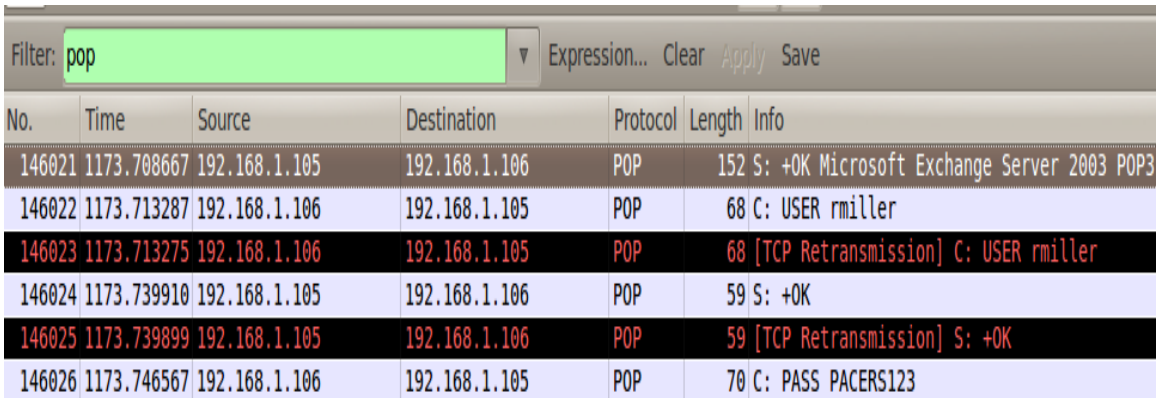

Figure 31: pop Filter in Wireshark

8. **Clear** the pop filter. From the Wireshark menu, select **File > Export Objects > HTTP**.

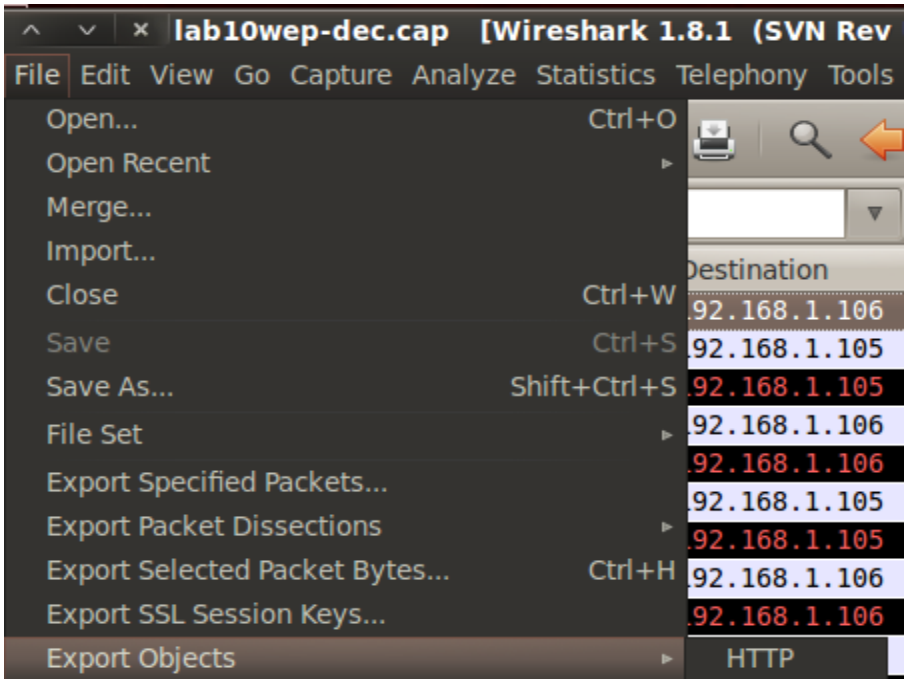

Figure 32: Saving an HTTP Object Parsed from Wireshark

9. Click the **Save All** button in the lower-right side of the HTTP object list.

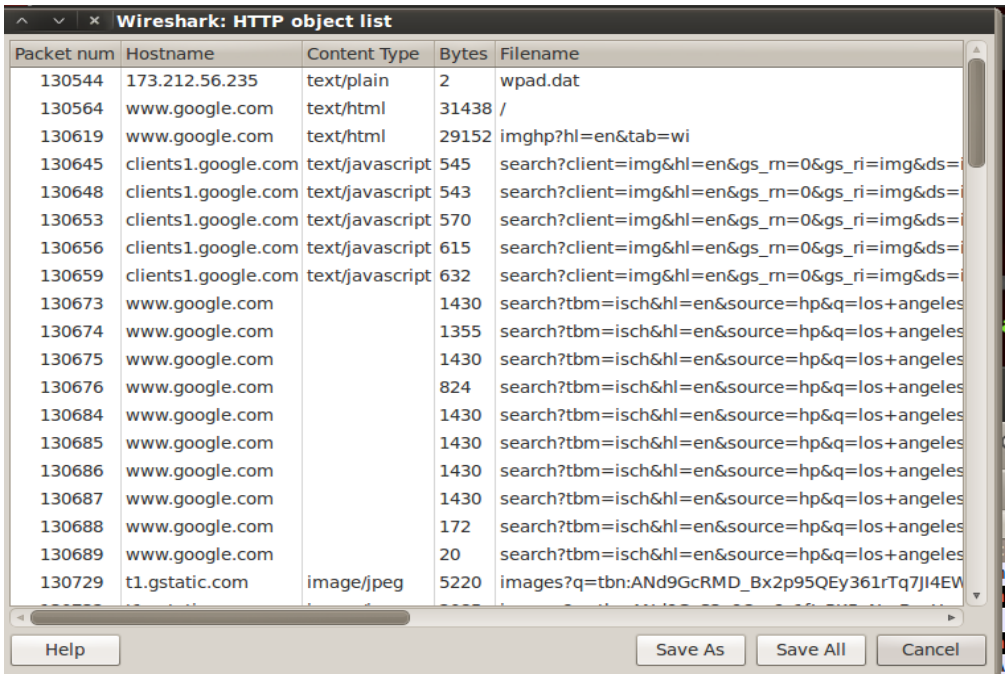

Figure 33: Saving HTTP Objects Parsed from Wireshark

10. In the Name box, type **wep** and click **OK**.

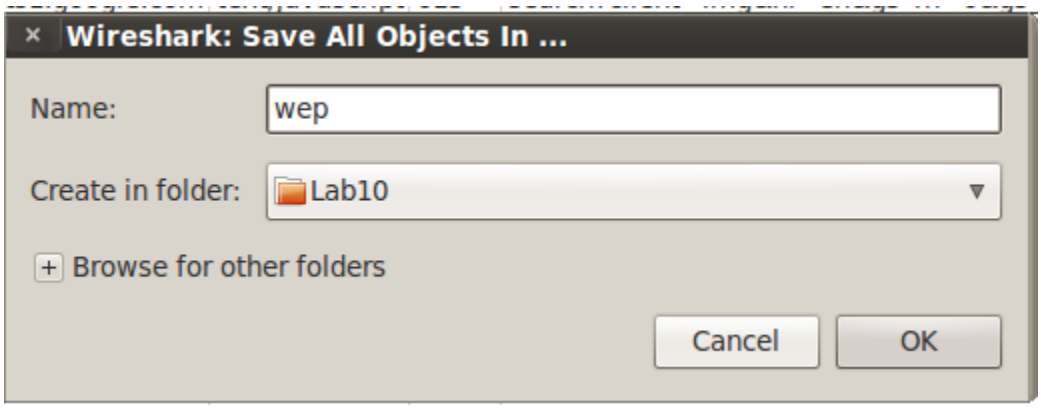

Figure 34: Saving HTTP Objects Parsed from Wireshark

11. Click **OK** to some files cannot be saved. Some users may not receive this message.
12. To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Double-click on the **Lab10** folder, then double-click on the **wep** folder. You will see pictures of the Los Angeles Lakers as well as Angry Birds and Star Wars pictures.

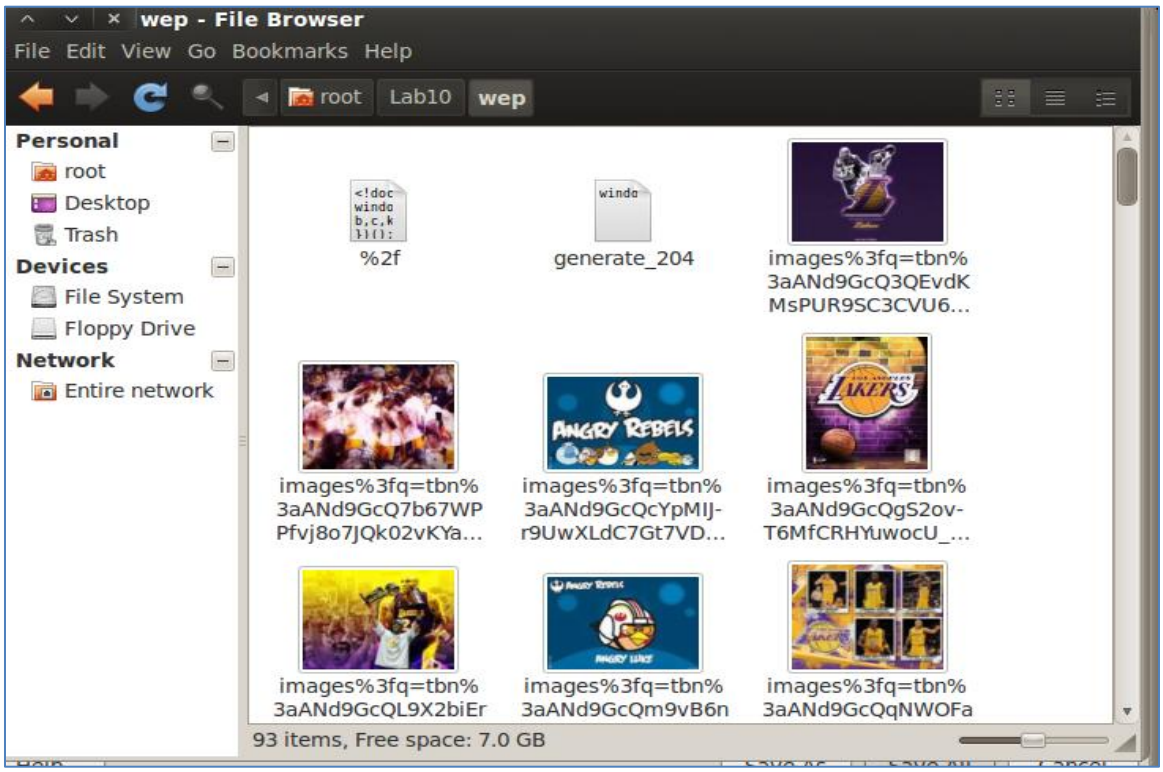

Figure 35: The Pictures Carved From Wireshark

13. **Close** the open picture folder and **close** the Wireshark HTTP object list.
14. To pull a PDF file transferred via FTP out of the wireless capture file, type the following filter into Wireshark and hit **Apply**: **frame contains PDF**
15. Right-click on frame **140353** in the list and select **Follow TCP Stream**.

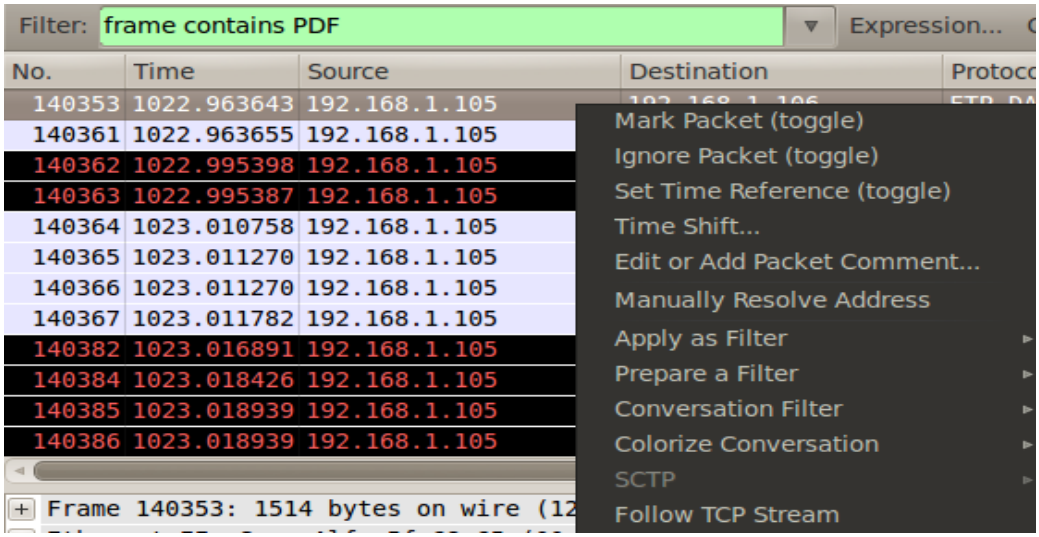

Figure 36: Following the TCP Stream

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

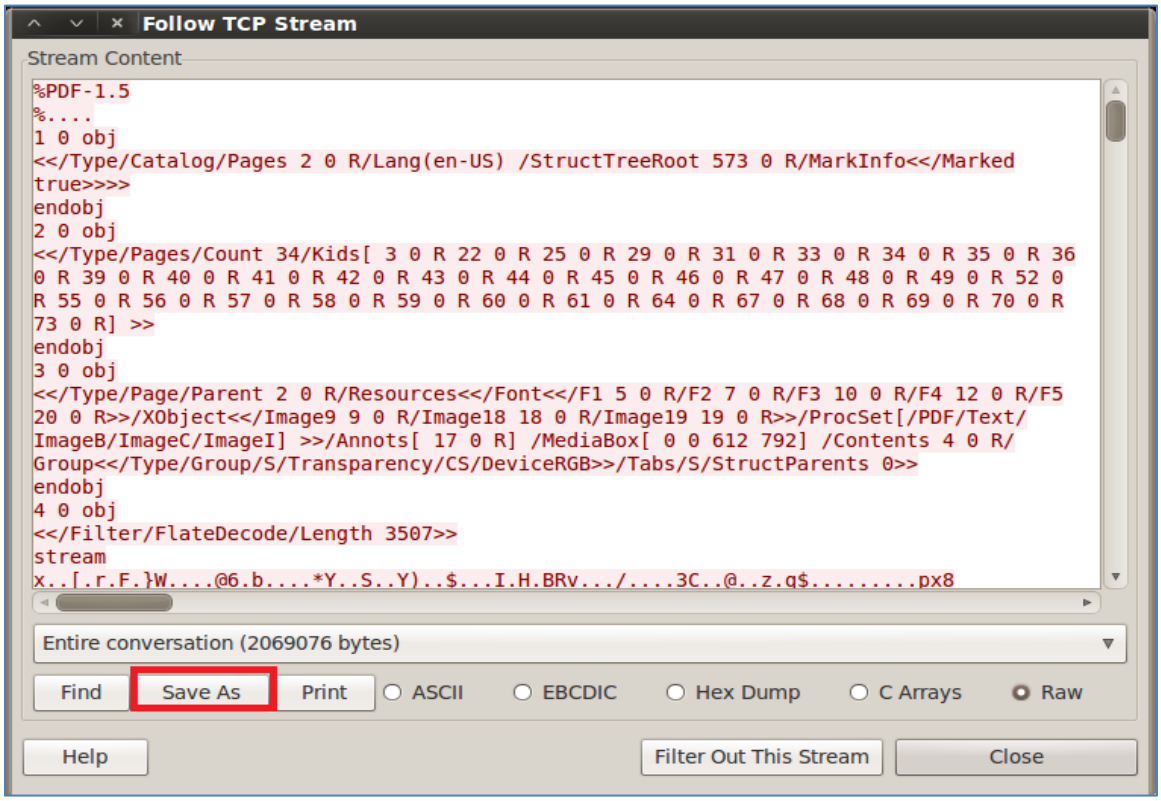

Figure 37: The Follow TCP Stream Window

17. For the name of the file, put **16.pdf**. Make sure the Save in Folder is **Lab10** and click **Save**.

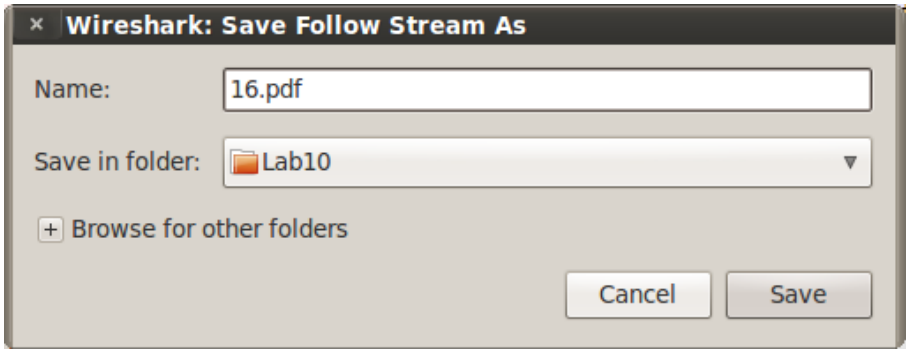

Figure 38: Saving the PDF file From the TCP Stream

18. To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Double-click on the **Lab 10** folder and then double-click **16.pdf** to open it.

Figure 39: Opening the Zip File and Viewing the Pictures.

19. **Close** the PDF file and all of the windows you have open, except for the Terminal.

3.2 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.

4 Cracking 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.

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 WPACEH. 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.

4.1 Using Wireshark to Crack and Examine WPA Traffic

1. In the terminal window, type the following commands:
   root@bt:~/Lab10# **aircrack-ng lab10wpa.cap -w /root/Wordlist.txt**
2. Select **3** for the target network. Notice that there is 1 WPA handshake.

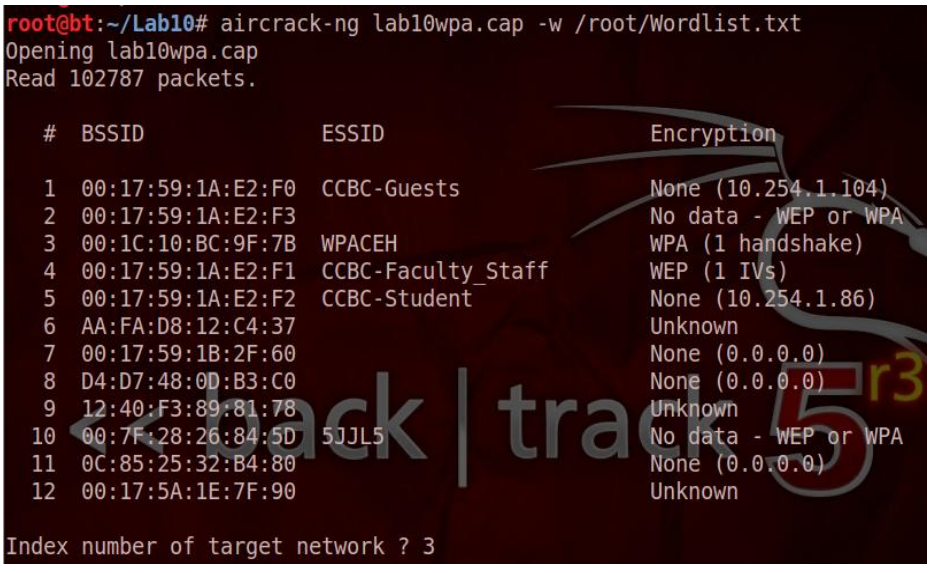

Figure 40: Selecting the Target Network Using WPA

The passphrase, ***blackmail*** will appear after a short time. The file was cracked because it existed in the Wordlist.txt file.

Do not use dictionary words for WPA passphrases.

Figure 41: The WPA Passphrase

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

2. From the terminal, type the following command to decrypt the traffic:
   root@bt:~/Lab10# **airdecap-ng lab10wpa.cap –e WPACEH –p blackmail**

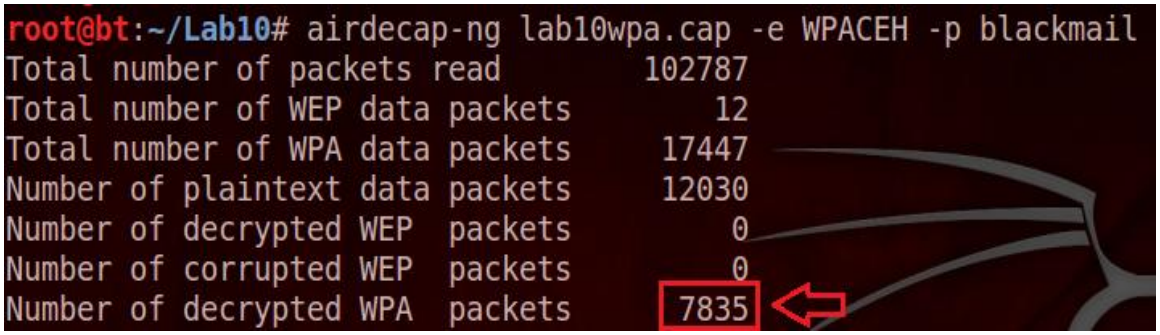

Figure 42: The WPA Packets are Decrypted

The number of decrypted WPA packets should be **7835**. Now, we will be able to analyze TCP/IP traffic as well as carve files from the decrypted capture file.

3. Type the following to list all of the files and folders within the lab2 directory:
   root@bt:~/Lab10# **ls**

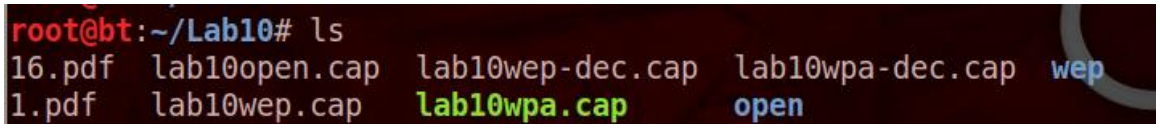

Figure 43: Decrypted WPA Capture File

The lab10wpa-dec file was created when you ran the airdecap-ng program.

4. Type the following command to open the decrypted file with Wireshark:
   root@bt:~/Lab10# **wireshark lab10wpa-dec.cap**

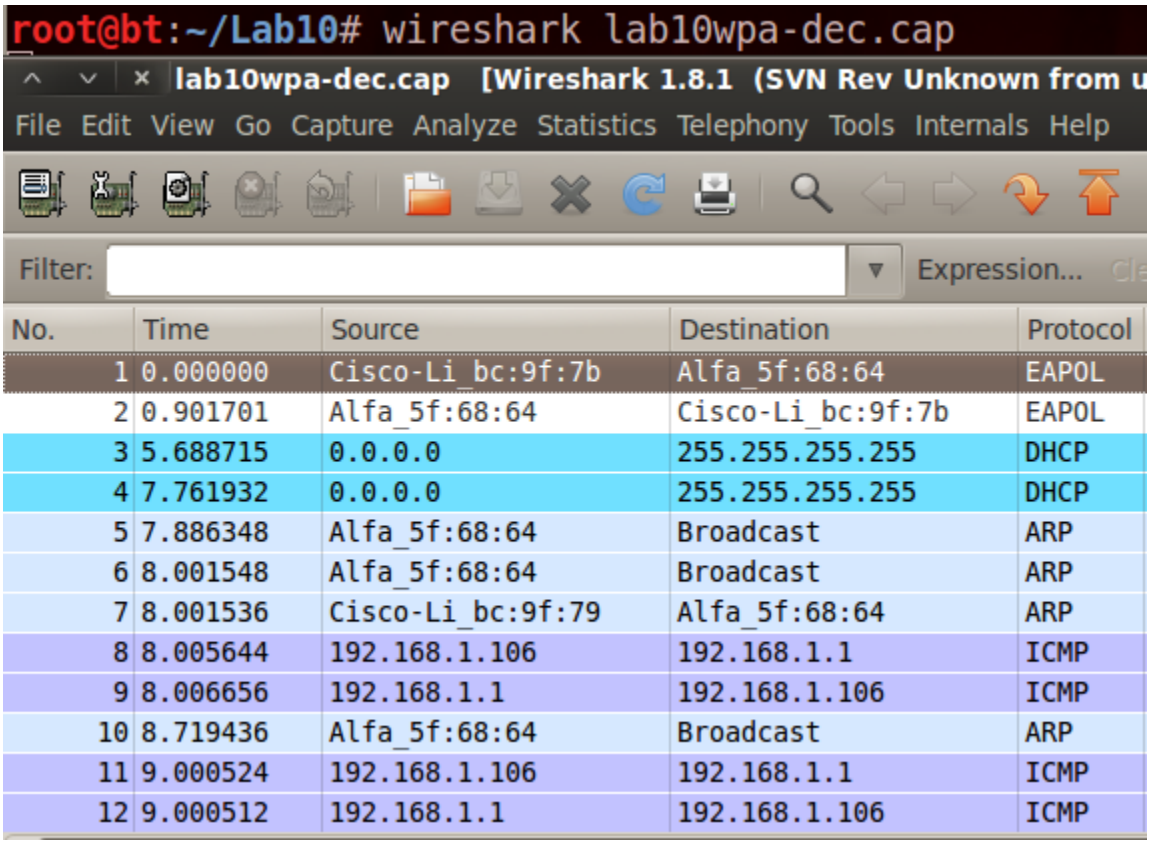

Figure 44: The Newly Created WEP1-dec Capture File

5. In order to view post office protocol traffic, type **pop** in the Wireshark filter pane and click **Apply**. You can view usernames and passwords in clear text.

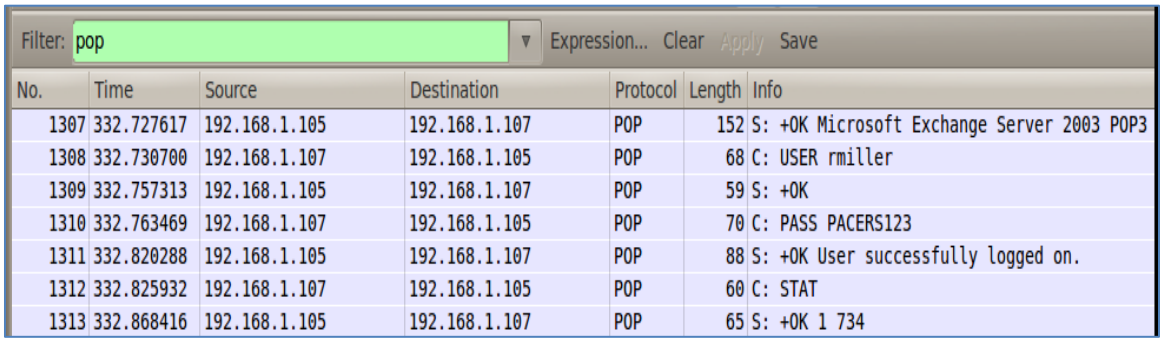

Figure 45: Saving an HTTP Object Parsed from Wireshark

6. Right-click on frame **1307** and select **Follow TCP Stream**. Read the email. Click **Close**.

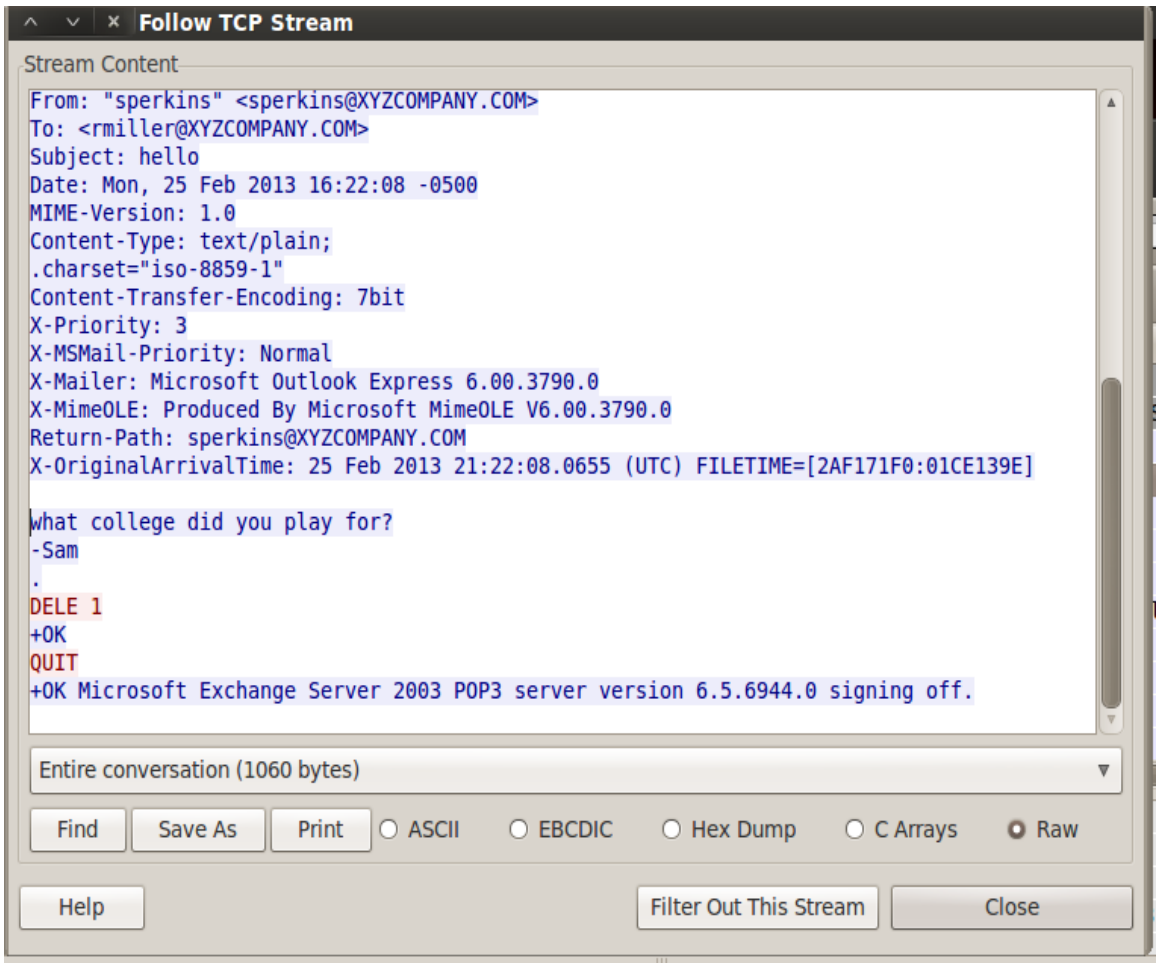

Figure 46: Saving an HTTP Object Parsed from Wireshark

7. Clear the pop filter. From the Wireshark menu, select **File**, **Export Objects**, **HTTP**.

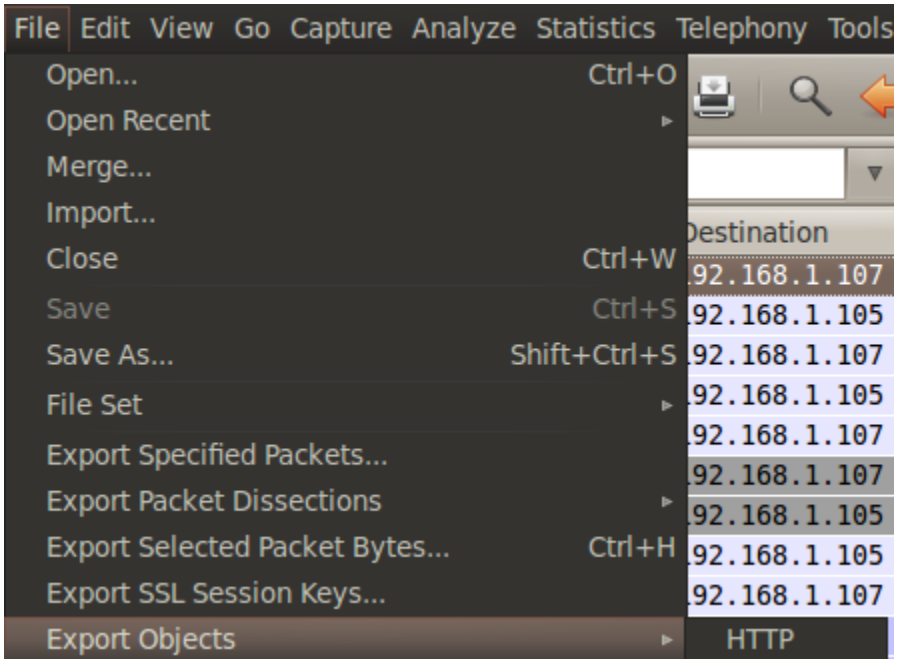

Figure 47: Saving an HTTP Object Parsed from Wireshark

8. Click the **Save All** button in the lower-right side of the HTTP object list.

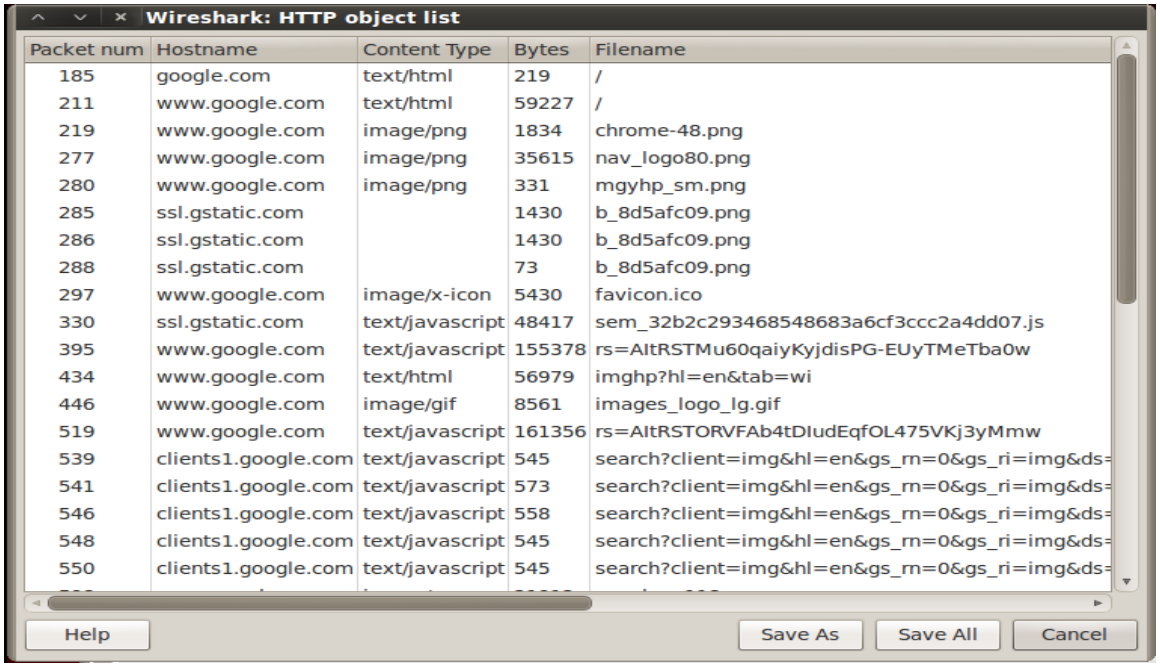

Figure 48: Saving an HTTP Object Parsed from Wireshark

9. In the Name box, type **wpa** and click **OK**. If you receive another message, click **OK** to some files cannot be saved.

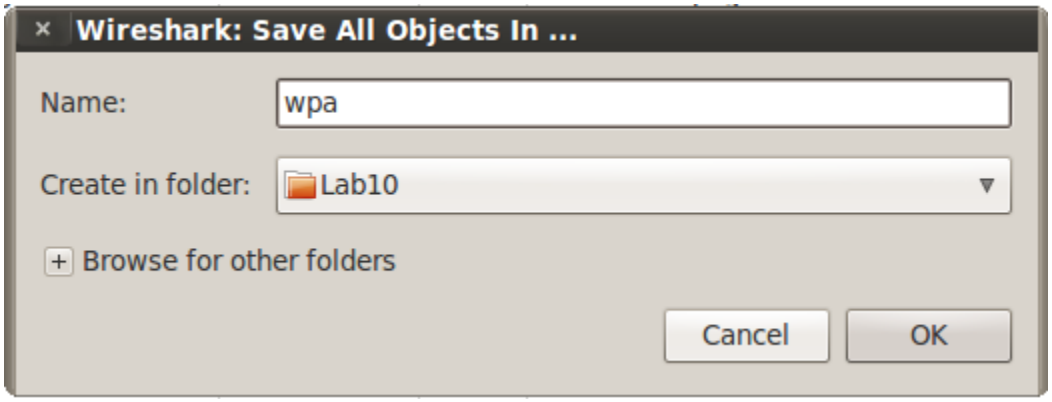

Figure 49: Saving HTTP Objects Parsed from Wireshark

10. To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Double-click on the **Lab 10** folder, and then double-click on the **wpa** folder. You will see pictures of Legos.

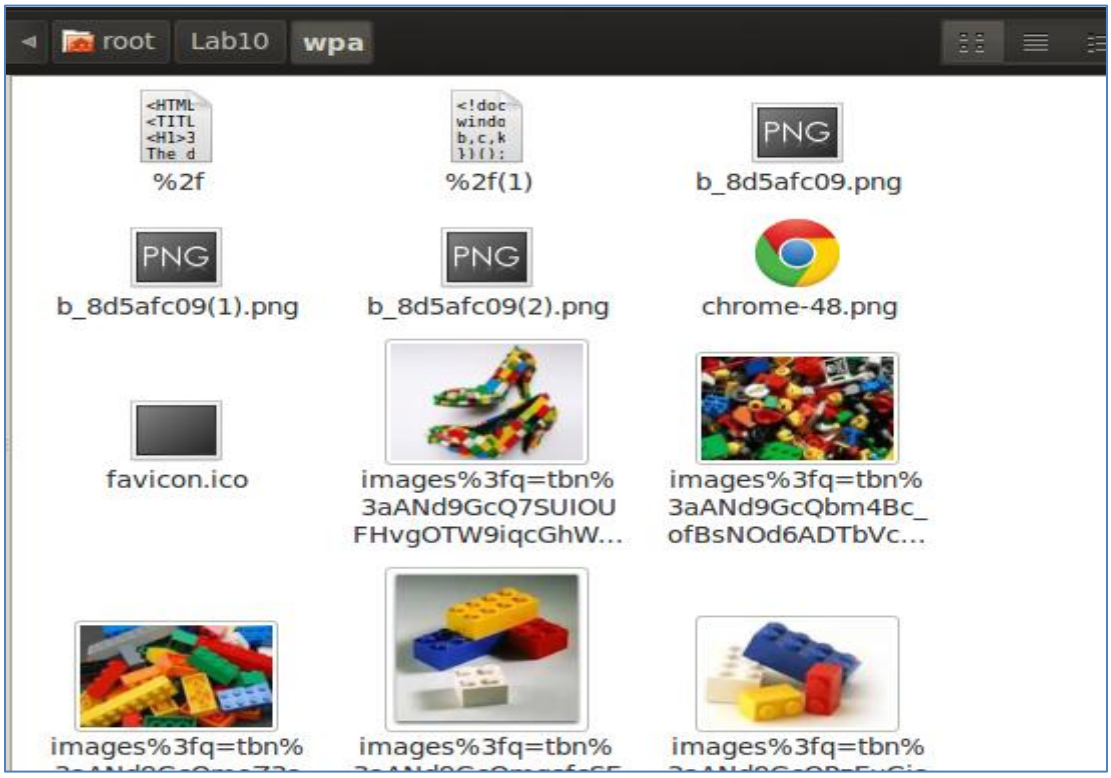

Figure 50: The Pictures Carved From Wireshark

11. **Close** the open picture folder and **close** the Wireshark HTTP object list.
12. To pull a PDF file transferred via FTP out of the wireless capture file, type the following filter into Wireshark and hit **Apply**: **frame contains PDF**

13. Right-click on frame **1792** in the list and select **Follow TCP Stream.**

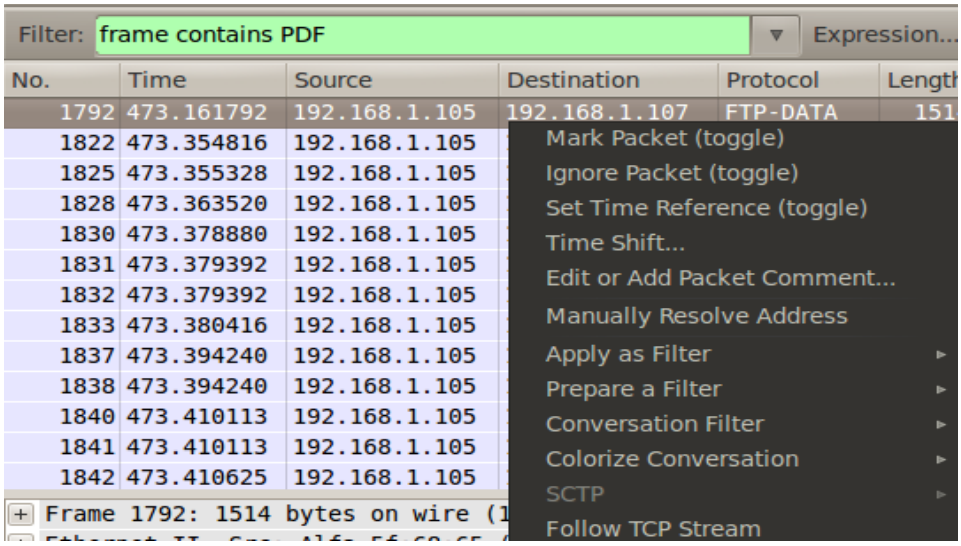

Figure 51: Following the TCP Stream

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

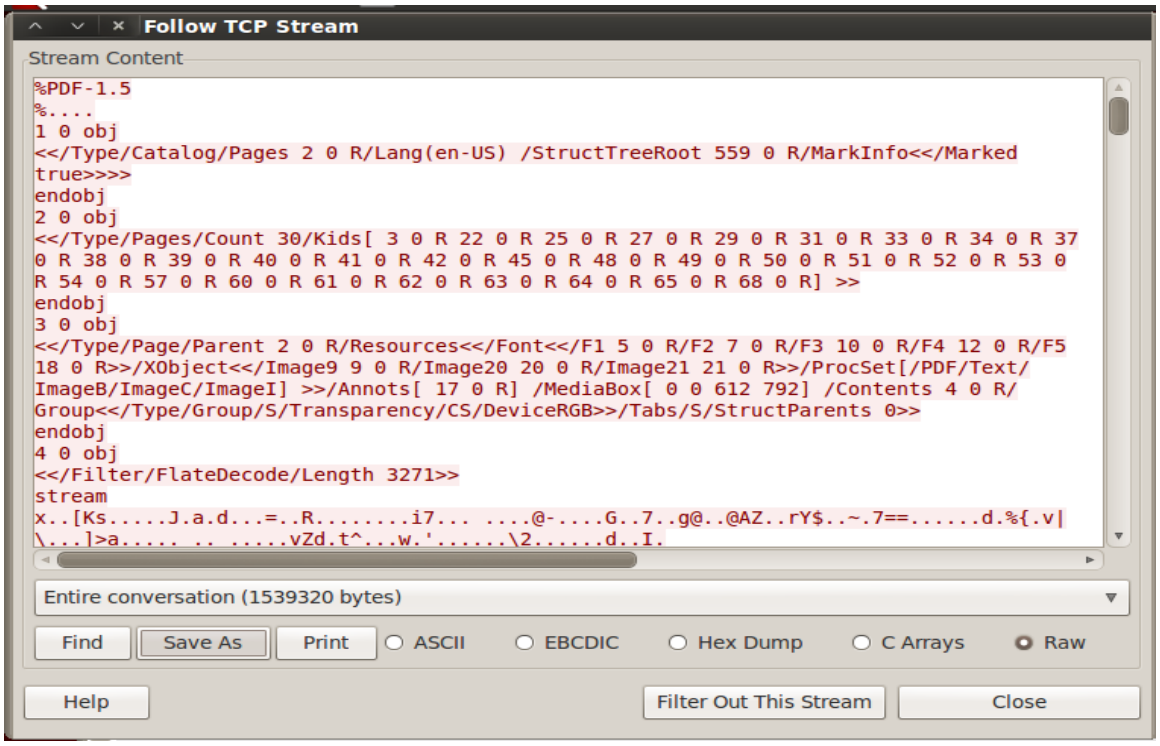

Figure 52: The Follow TCP Stream Window

15. For the name of the file, put **10.pdf**. Make sure the Save in Folder is **Lab10** and click **Save**.

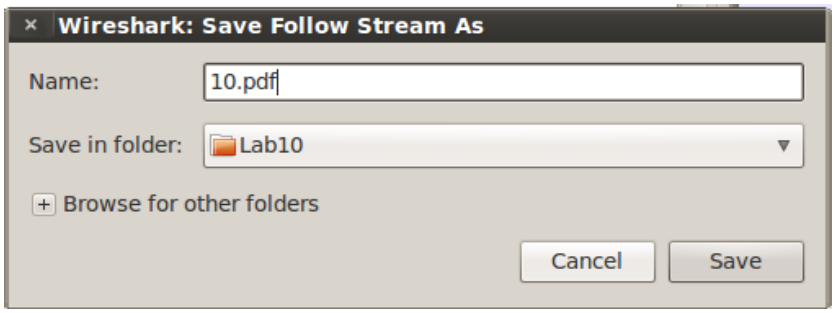

Figure 53: Saving the PDF file From the TCP Stream

16. To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Double-click on the **Lab 10** folder, and double-click to open **10.pdf.**

Figure 54: Opening the Zip File and Viewing the Pictures.

4.2 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 with aircrack-ng.

References

1. Wi-Fi Alliance:
   http://www.wi-fi.org/

2. Institute of Electrical and Electronics Engineers:
   http://www.ieee.org/index.html

3. BackTrack Linux:
   http://www.backtrack-linux.org/

4. Wireshark:
   http://www.wireshark.org/

5. Wireless Hacking Video:
   http://vimeo.com/3410674