Security+ Lab Series

Lab 06: Wireless Networking Attack and Mitigation Techniques

Document Version: 2018-08-28

Contents

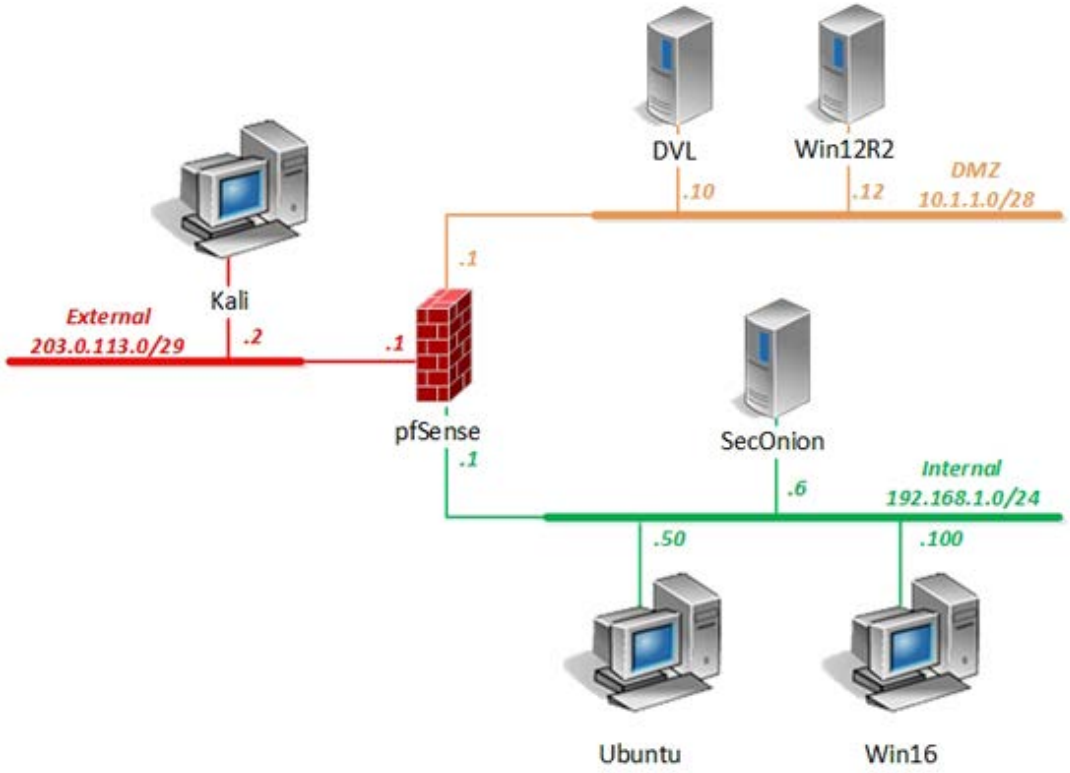
Introduction

In this lab, you will be conducting wireless security practices using various tools.

Objectives

- Compare and contrast types of attacks

Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng$
Win16	192.168.1.100 /24	lab-user	Train1ng$
		Administrator	Train1ng$

1 Examining Plain Text Traffic

1.1 Viewing Plain Text Wireless Traffic

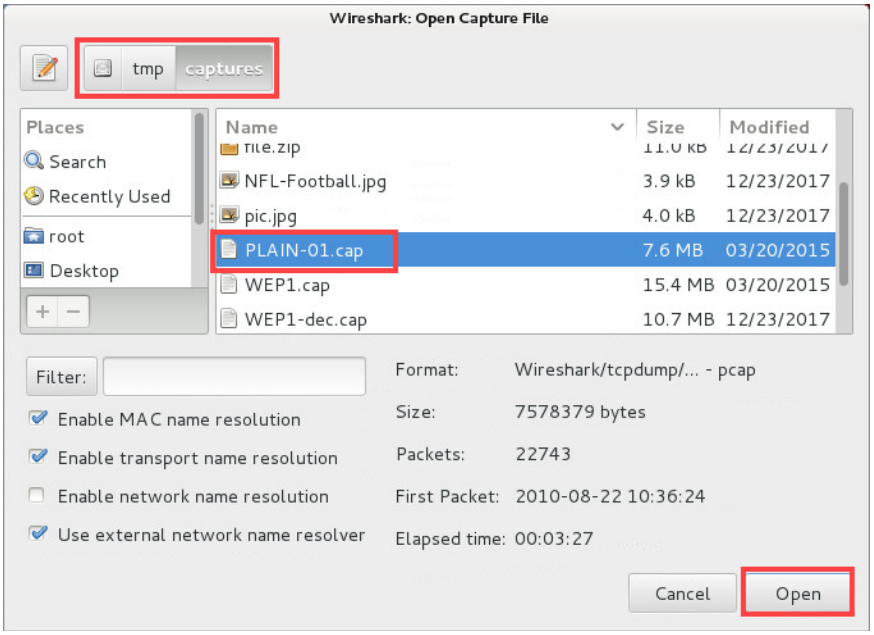
1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Log in as **root** with **toor** as the password.
3. Open a new terminal window by clicking on the **terminal** icon located in the top toolbar.

4. Open the **Wireshark** application by typing the command below in the *terminal* window, followed by pressing the **Enter** key. If prompted for a password, enter **securepassword**.

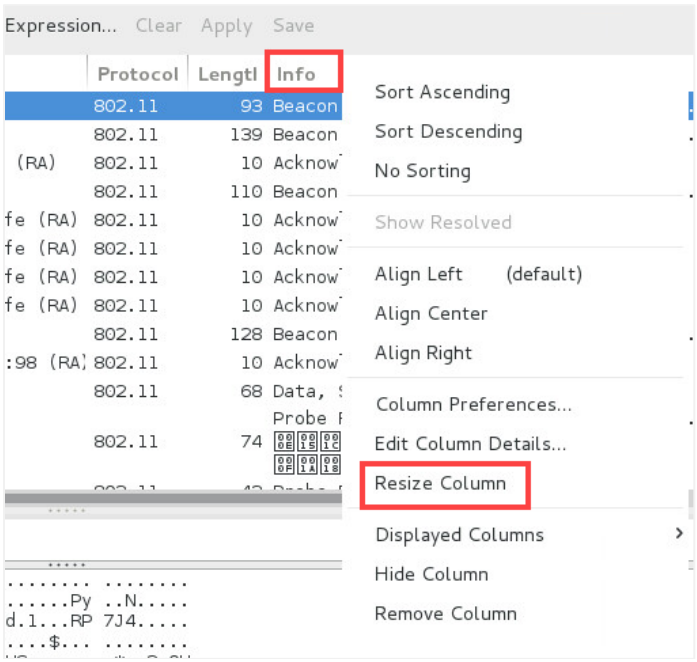
```
root@Kali-Attacker:~# sudo wireshark
```

5. If prompted with a security warning, click **OK** to continue.
6. If an error appears regarding *init.lua*, click **OK** to continue.
7. Select the **File** menu option at the top of the *Wireshark* window and click on **Open**.

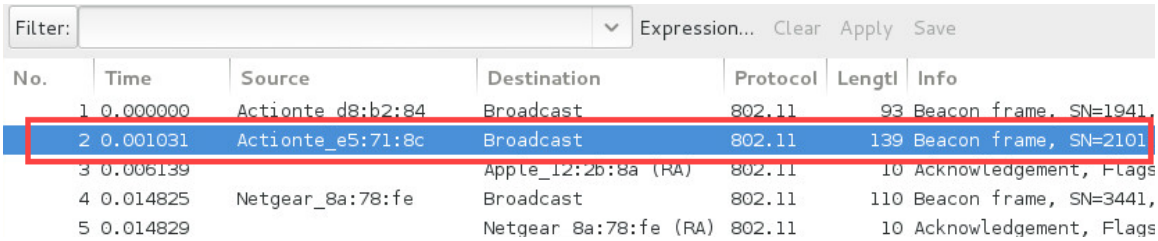
8. A new window appears. Navigate to **File System > tmp > captures** and select the **PLAIN-01.cap** file. Click the **Open** button.



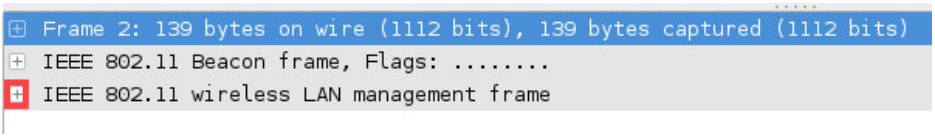
9. Right-click on the **Info** column header and select **Resize Column** to see all information contained within this column.



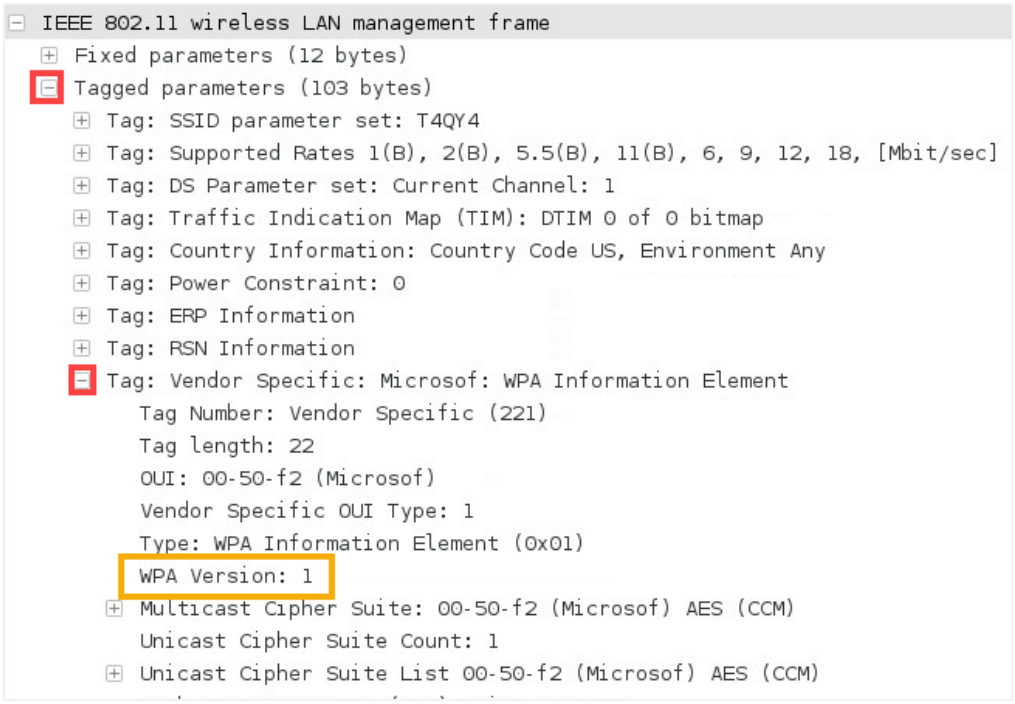
10. Select on the **second frame** in the *Wireshark* capture file.



11. On the bottom part of the screen, click the **+** icon in front of the **IEEE 802.11 wireless LAN management frame** to expand its view.

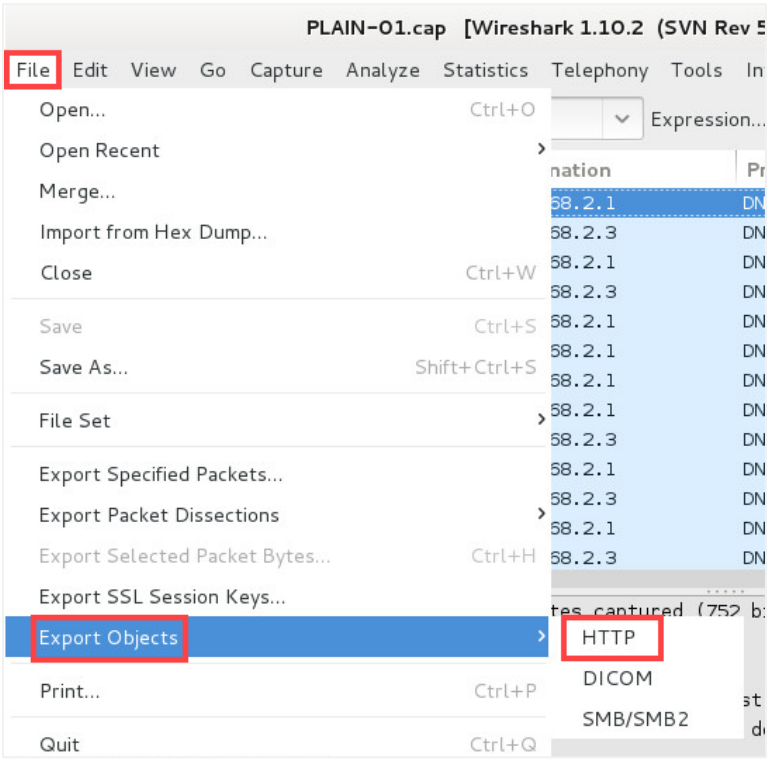


12. Dive in further by clicking the **+** icon in front of **Tagged parameters** followed by clicking the **+** icon in front of **Tag: Vender Specific: Microsof: WPA Information Element**. View the *WPA Version*.

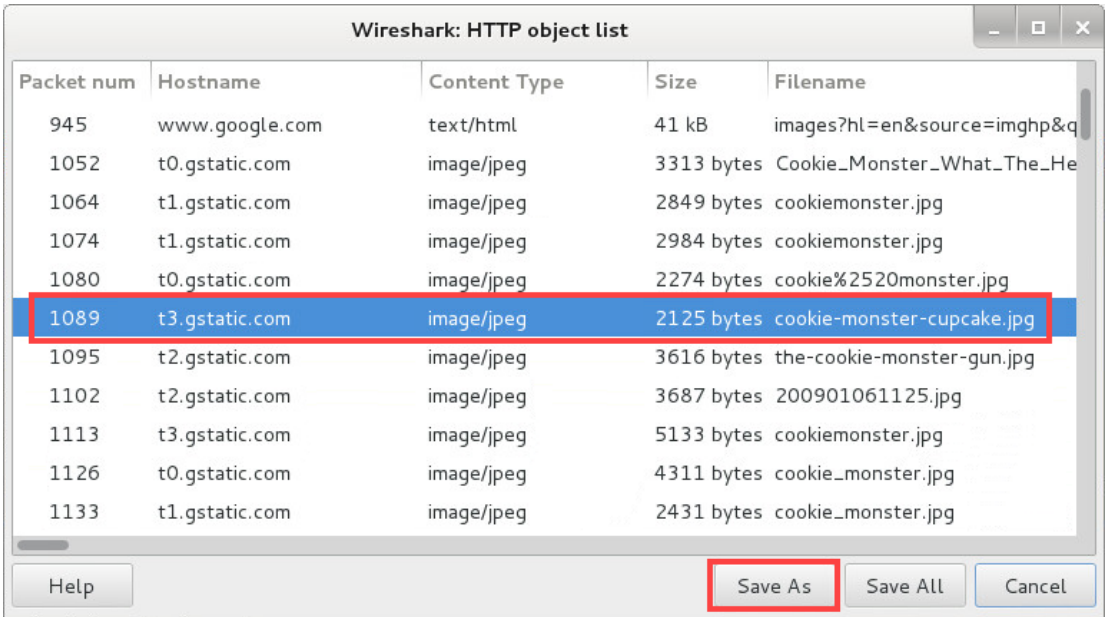


13. View captured *DNS requests* by typing **dns** in the *Filter:* pane. Click **Apply**.

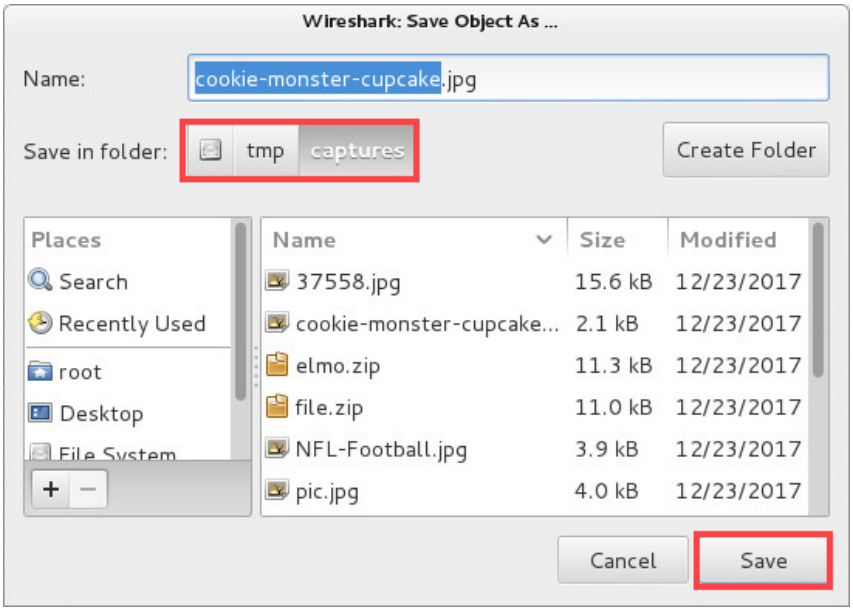
14. With *Wireshark*, we can export images and files that have passed through the capture communication channel. Try exporting a file by clicking on the **File** menu option on the top pane and navigate to **Export Objects > HTTP**.



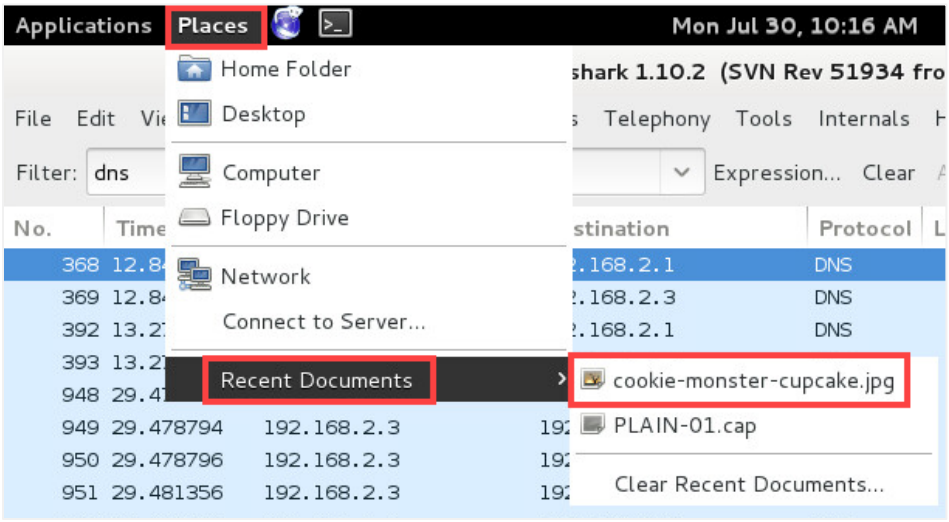
15. A new window appears. Look through the list of files that have been downloaded by wireless users. Under the *Filename* column, find the image file **cookie-monster-cupcake.jpg** and select the file. With the file selected, click the **Save As** button.



16. In the *Save Object As* window, choose the **/tmp/captures** directory to save to and then click the **Save** button.

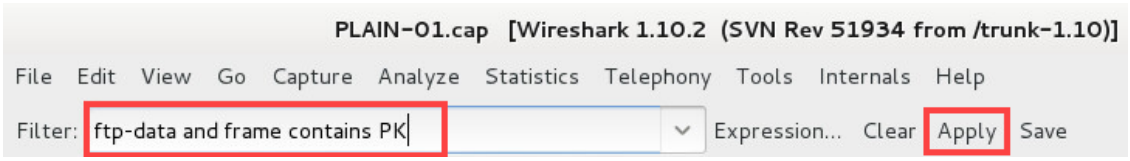


17. View the image by selecting the **Places** menu option located next to the *Applications* menu. Navigate to **Recent Documents > cookie-monster-cupcake.jpg**.

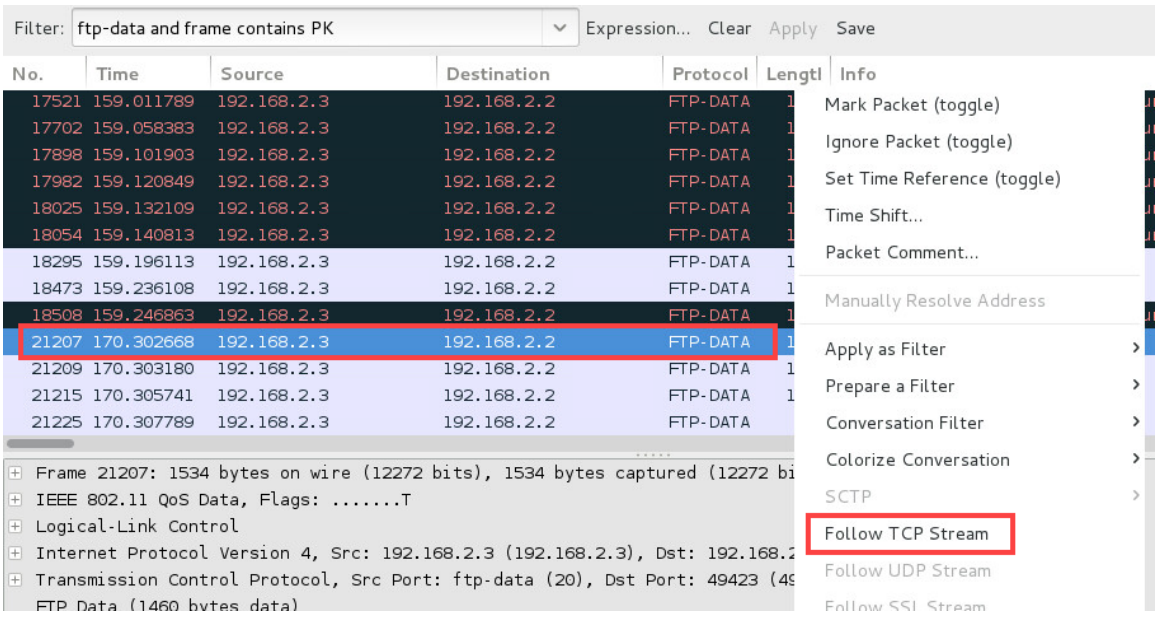


18. Notice the image. **Close** the *image viewer* and close out the *HTTP object list* window.

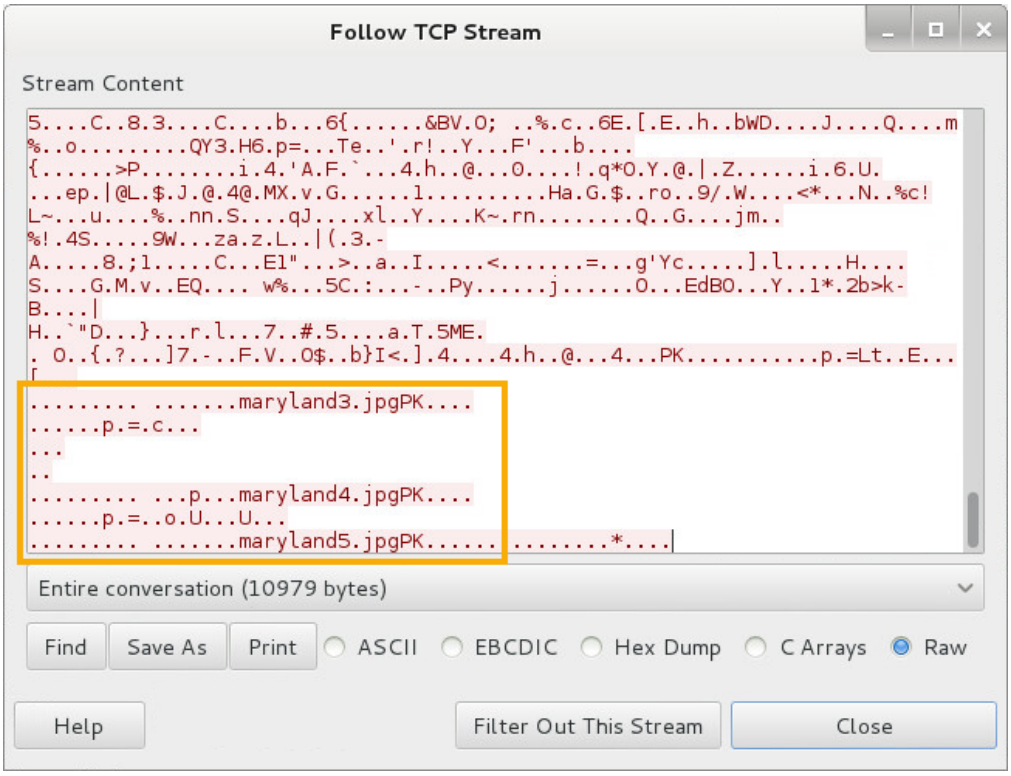
19. Within the *Wireshark* interface, pull a zip file via *FTP* out of the wireless capture file. Type **`ftp-data and frame contains PK`** into the *Wireshark Filter:* and click **Apply**.



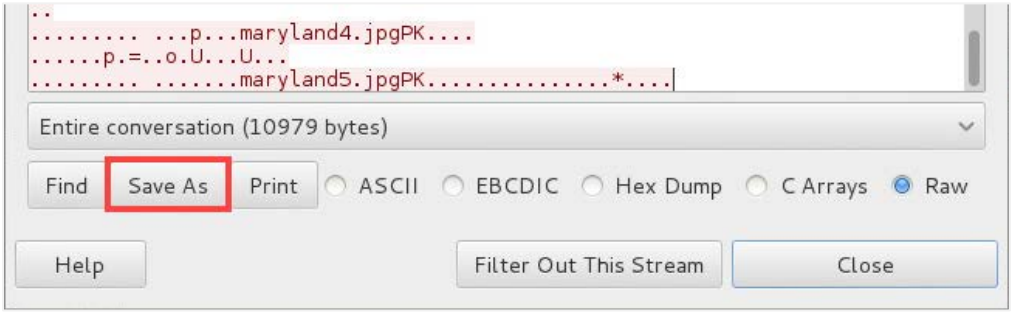
20. Right-click on the **frame 21207** in the list and select **Follow TCP Stream**.



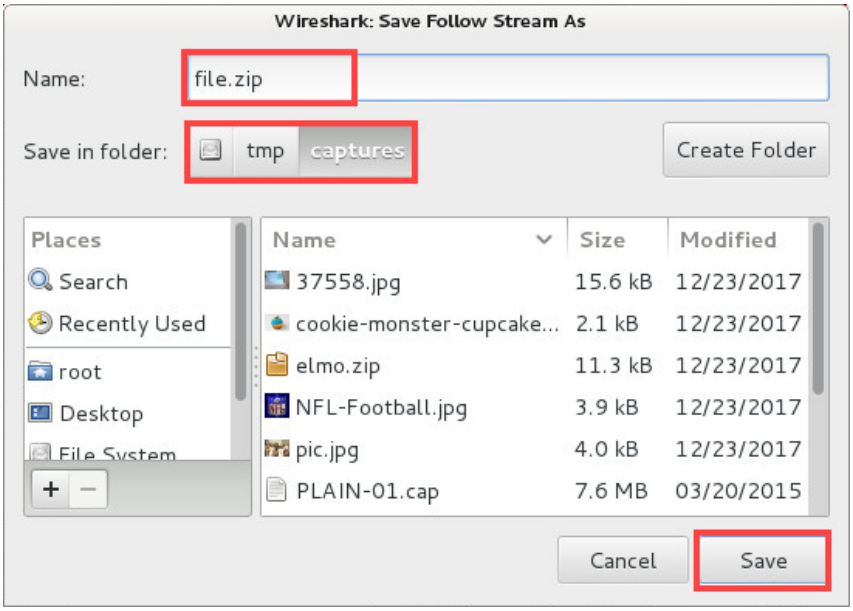
21. Examine the data shown in the *TCP stream*. Scroll to the bottom of the window and notice the "*PK*" attached to the end of filenames.



22. Within the *Follow TCP Stream* window, click **Save As**.



23. Type **`file.zip`** in the *Name* text field. Make sure the save destination is set to **/tmp/captures** and click the **Save** button.

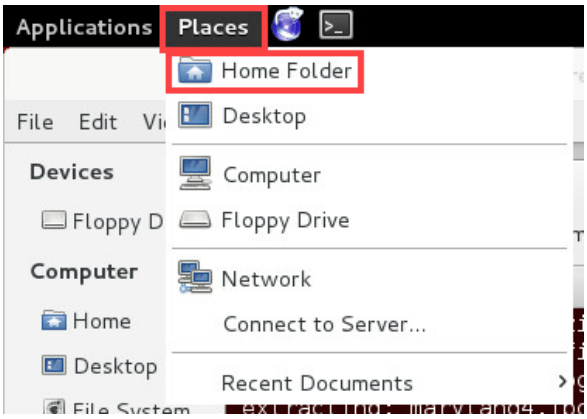


24. **Close** the *Follow TCP Stream* window.
25. Open a new **terminal** window and type the command below to **unzip** the file that was just pulled from the *Wireshark* capture file.

```
root@Kali-Attacker:~# unzip /tmp/captures/file.zip
```

```
root@Kali-Attacker:~# unzip /tmp/captures/file.zip
Archive:  /tmp/captures/file.zip
  inflating: maryland3.jpg
 extracting: maryland4.jpg
 extracting: maryland5.jpg
```

26. Select the **Places** menu option from the top menu pane and click on **Home Folder**.



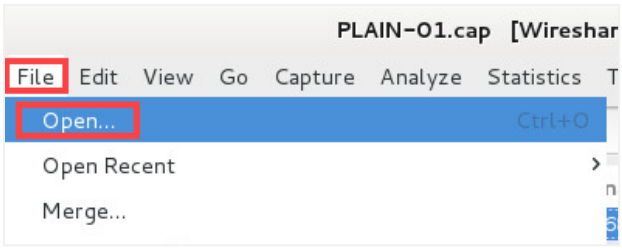
27. Notice the three different *maryland* image files in the **/root** directory that were extracted from *file.zip*.

28. **Close** the *File Manager* window.
29. Leave the *Kali* window open to continue with the next task.

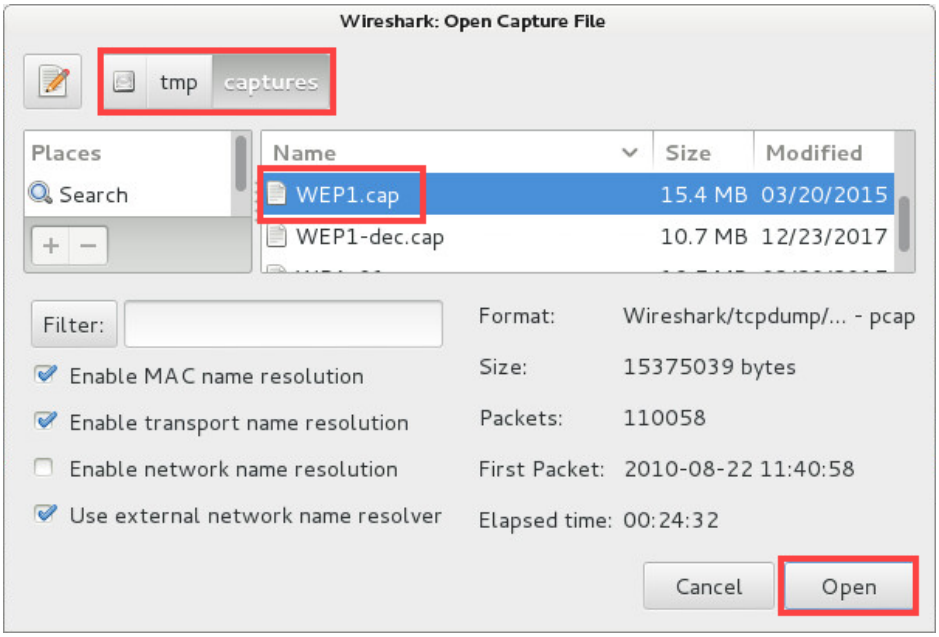
2 Exploiting and Examining WEP Traffic

2.1 Decrypt and Analyze WEP Traffic

1. Change focus on the **Wireshark** window. Select the **File** menu option and click on **Open**.



2. A new window appears. Verify that you are in the **/tmp/captures** directory. Select the **WEP1.cap** file and click the **Open** button.



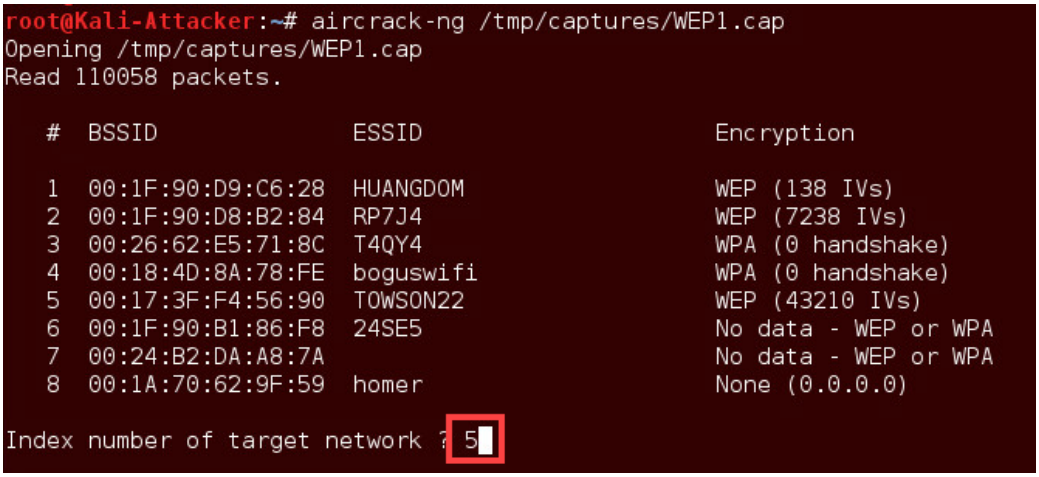
3. In the *Filter:* pane, type **dns** and click **Apply**.

You will not see any traffic displayed because the wireless traffic is encrypted.

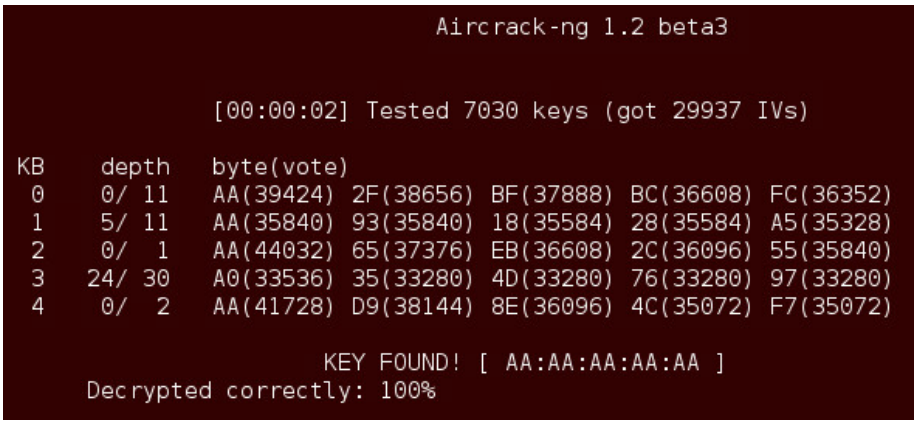
4. Close the **Wireshark** application by selecting the **File** menu option and clicking on **Quit**.
5. Change focus to the **terminal** window and enter the command below.

```
root@Kali-Attacker:~# aircrack-ng /tmp/captures/WEP1.cap
```

6. Type **5** for the target network. Press **Enter**.

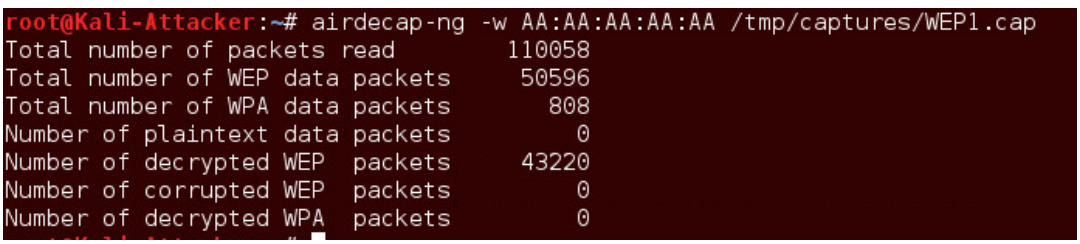


7. After a few seconds, the *aircrack-ng* program will be able to crack the *64-bit WEP key*. Notice the output.



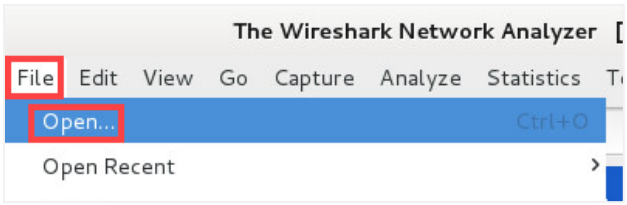
8. After the *WEP* key is obtained, decrypt the network traffic with **airdecap-ng**. Enter the command below to decrypt the traffic.

```
root@Kali-Attacker:~# airdecap-ng –w AA:AA:AA:AA:AA /tmp/captures/WEP1.cap
```

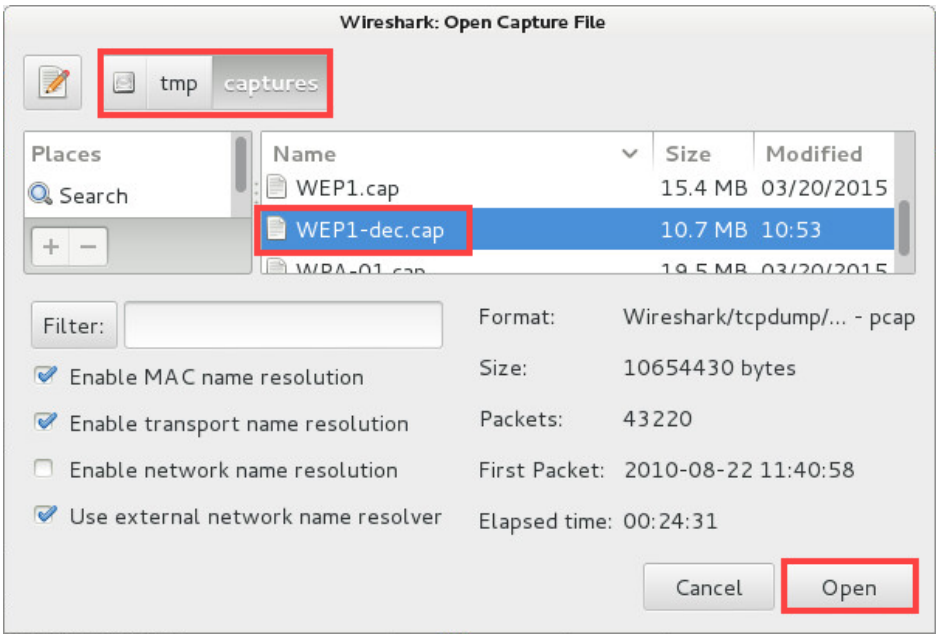


The number of *decrypted WEP packets* should be *43220*.

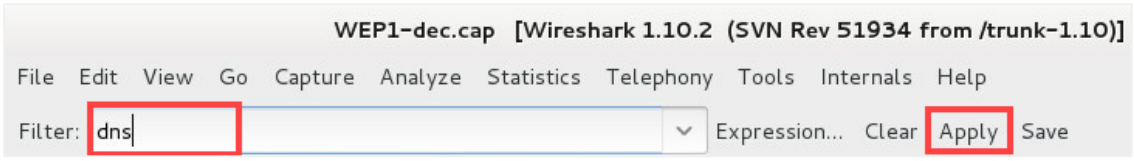
9. Analyze the decrypted traffic with *Wireshark*. Type `sudo wireshark` into the *terminal* and then press **Enter**.
10. If prompted with *Lua* loading error, click **OK** to continue.
11. Within the *Wireshark* application, select the **File** menu option and click **Open**.



12. A new window appears. Navigate to the **/tmp/capture** directory and select the **WEP1-dec.cap** file. Click **Open**.

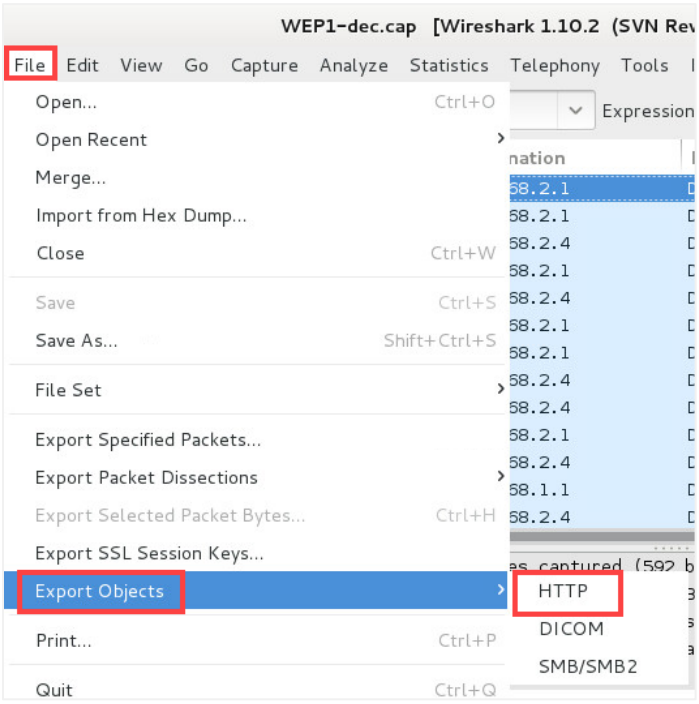


13. In the *Filter:* pane, type **dns** and click **Apply**.

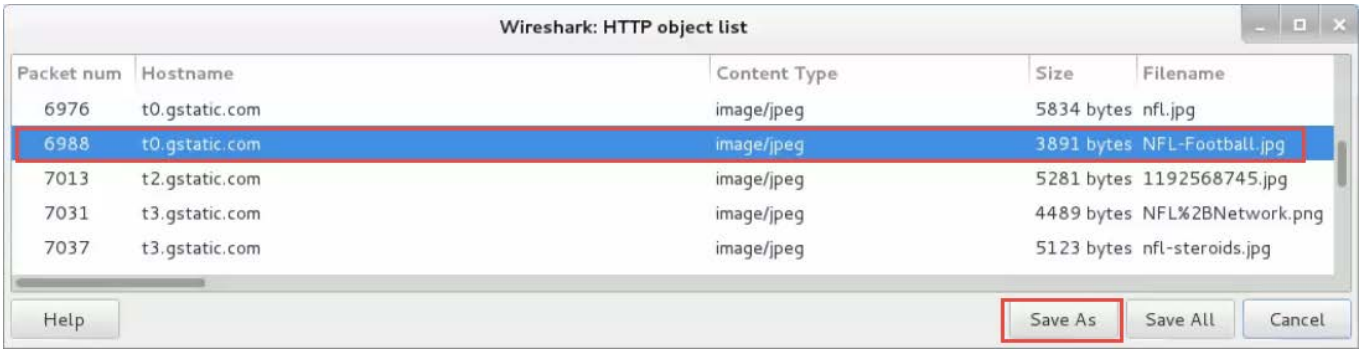


Notice that you can now see the *DNS* requests within the wireless traffic because the WEP traffic was decrypted with *airdecap-ng*.

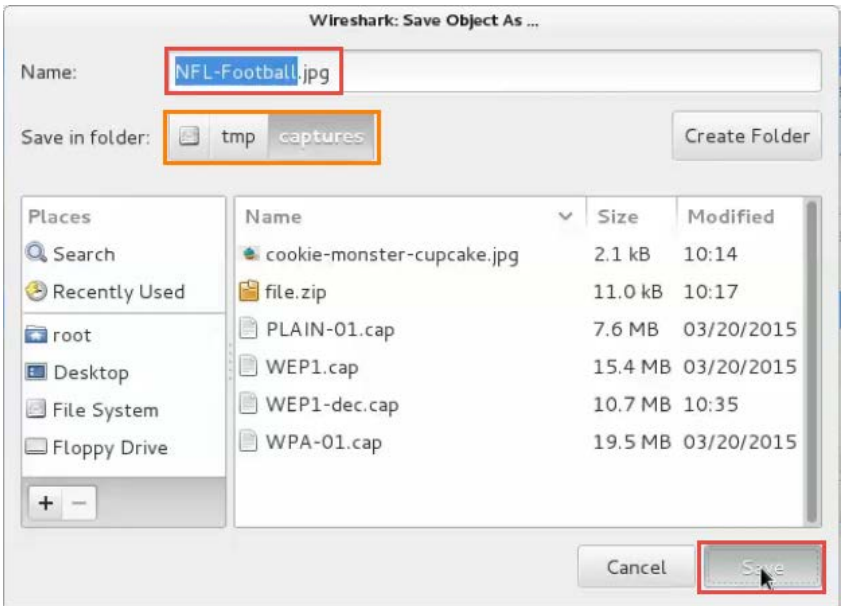
14. Select the **File** menu option and navigate to **Export Objects > HTTP**.



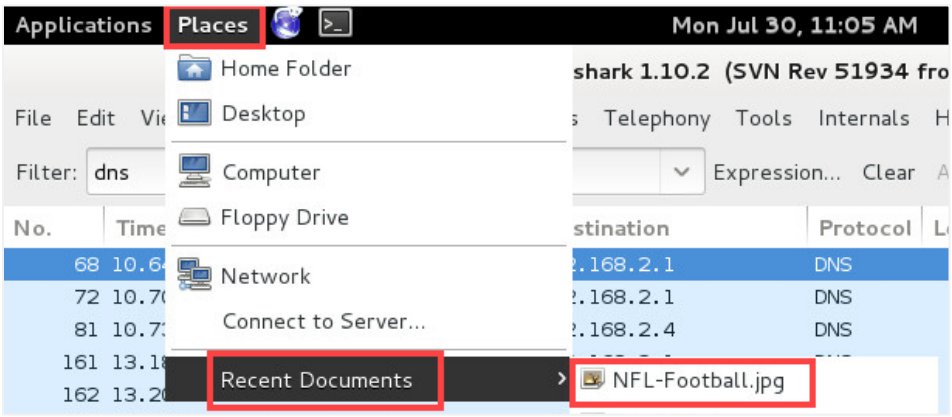
15. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, select the item **#6988 (NFL-Football.jpg)**. Once selected, click the **Save As** button.



16. Verify that the directory you are saving to is **/tmp/captures**. Click the **Save** button.

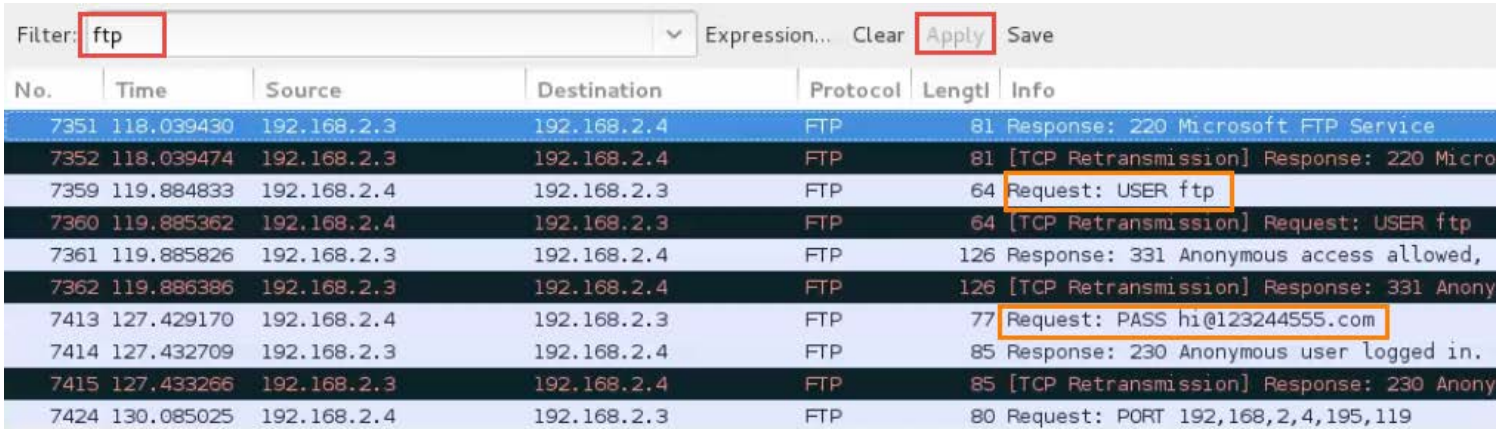


17. **Close** the *HTTP object list* window.
18. Click on the **Places** menu option and navigate to **Recent Documents**. Click on the **NFL-Football.jpg** entry to view the file.

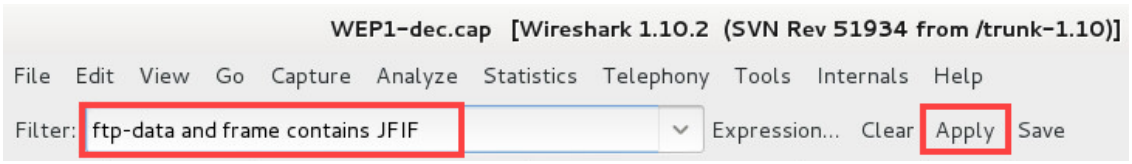


19. Notice the image that appears. **Close** the image viewer.

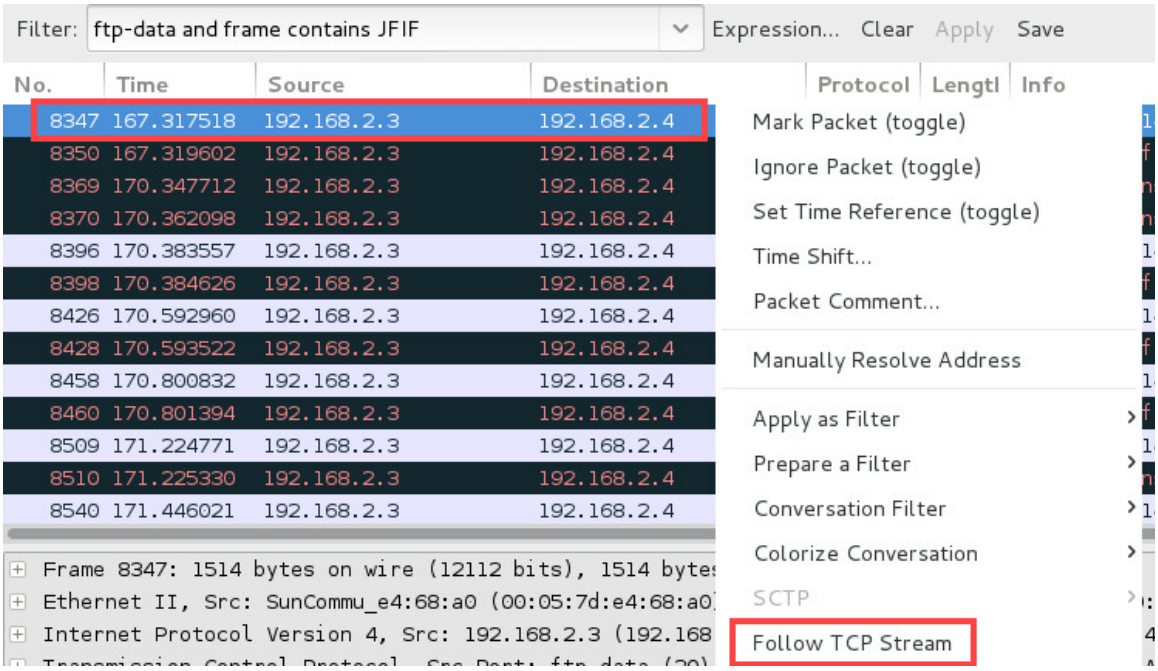
20. Change focus to the **Wireshark** application and type ***ftp*** into the *Filter:* pane. Click **Apply**. You will be able to see decrypted FTP traffic as well as clear-text usernames and passwords. Analyze the FTP traffic.



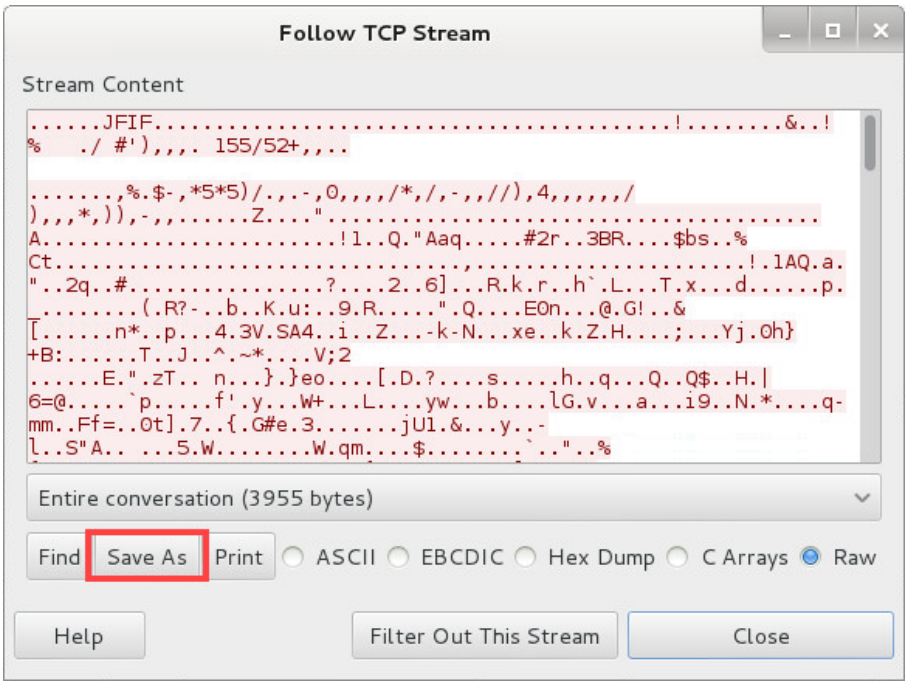
21. Let's pull a *JPEG* file transferred via *FTP* from the wireless capture. Type **`ftp-data and frame contains JFIF`** in the *Filter:* pane. Click **Apply**.



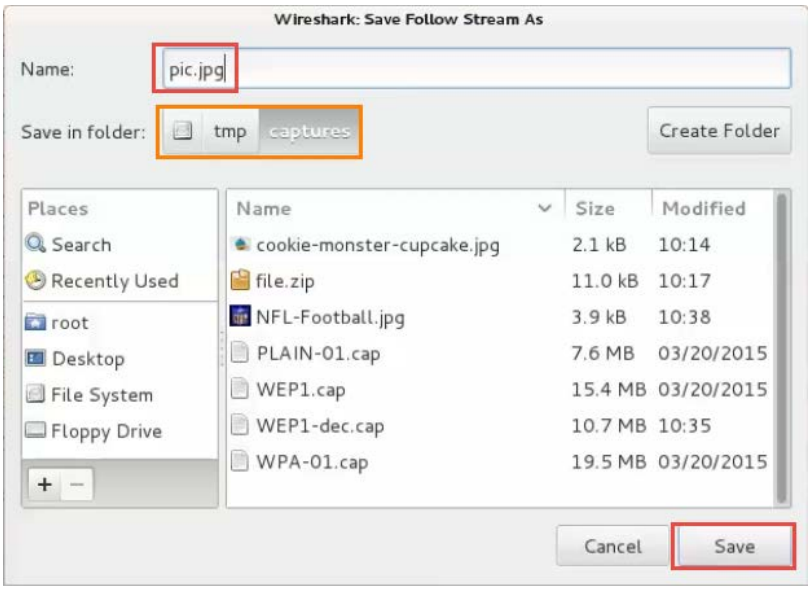
22. Right-click on the **first frame** in the list and select **Follow TCP Stream**.



23. A new window appears. Click the **Save As** button.

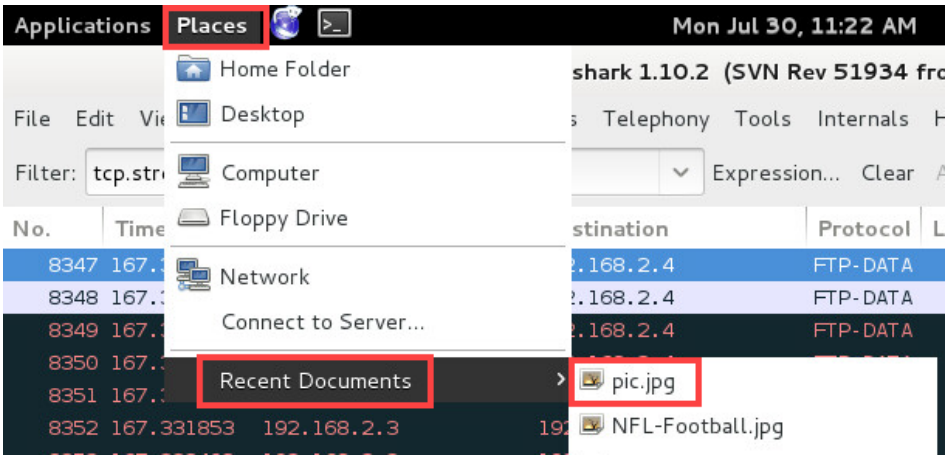


24. For the filename, type **`pic.jpg`**. Make sure the directory is set to **/tmp/captures** and click the **Save** button.



25. **Close** the *Follow TCP Stream* window.

26. Select the **Places** menu option and navigate to **Recent Documents > pic.jpg**.

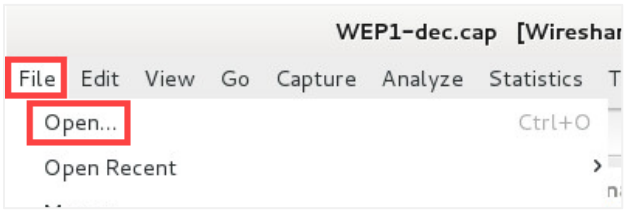


27. Notice the image in the *image viewer* window. **Close** the image viewer.
28. Leave the *Kali* window open to continue with the next task.

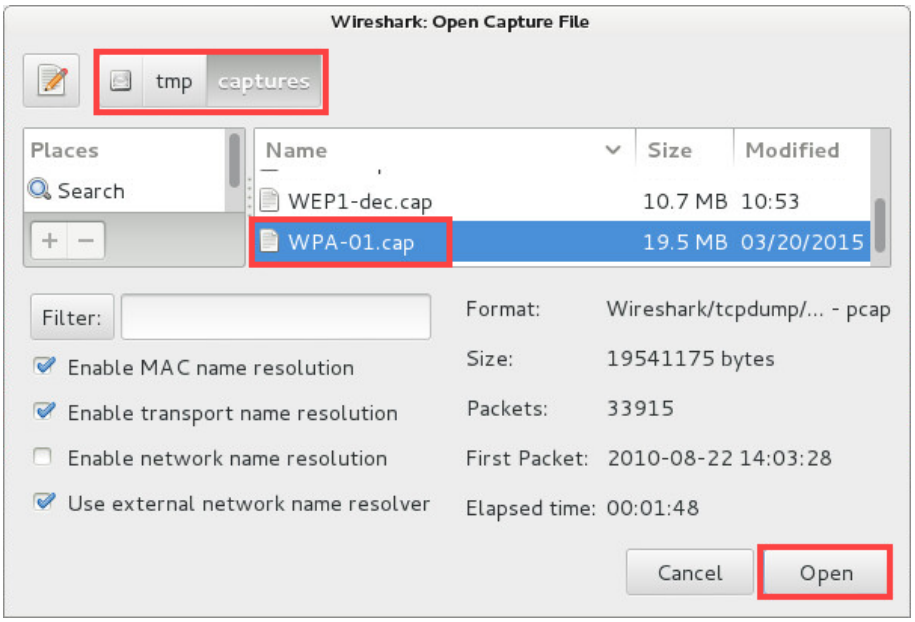
3 Exploiting and Examining WPA Traffic

3.1 Decrypt and Analyze WPA Traffic

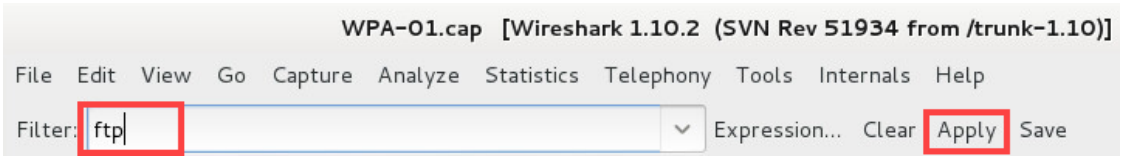
1. Change focus to the **Wireshark** application. Open a new *WPA* capture file by selecting the **File** menu option. Click **Open**.



2. Navigate to the **/tmp/captures** directory and select the **WPA-01.cap** file. Click the **Open** button.



3. In the *Filter:* pane, type **`ftp`** and click **Apply**.

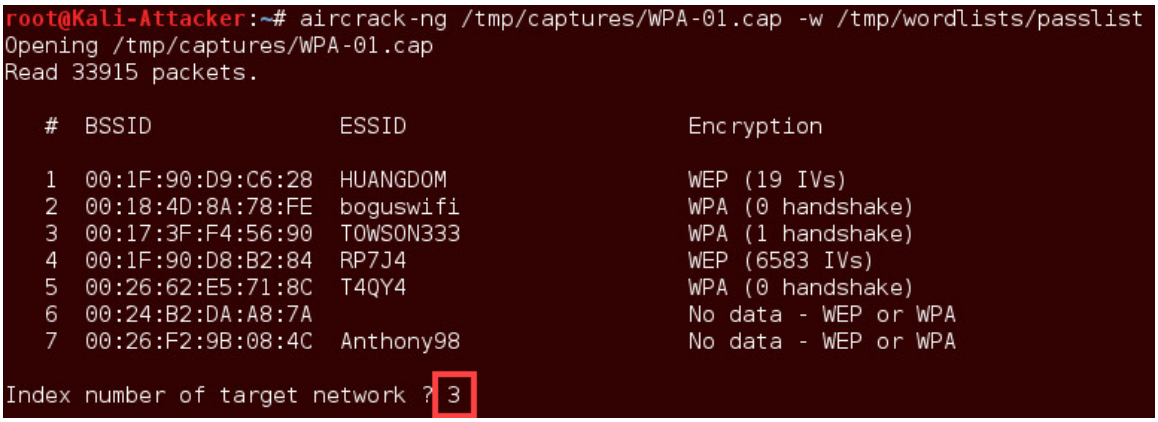


You will not see any traffic because the wireless network traffic is encrypted.

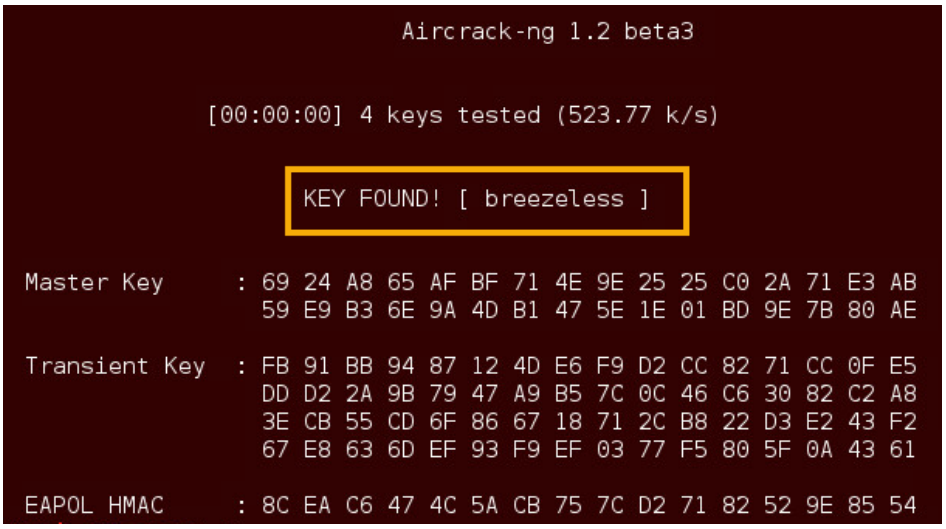
4. Change focus to the **terminal** window and type the command below.

```
root@Kali-Attacker:~# aircrack-ng /tmp/captures/WPA-01.cap –w
/tmp/wordlists/passlist
```

5. Type ***3*** as the menu option. Press **Enter**.

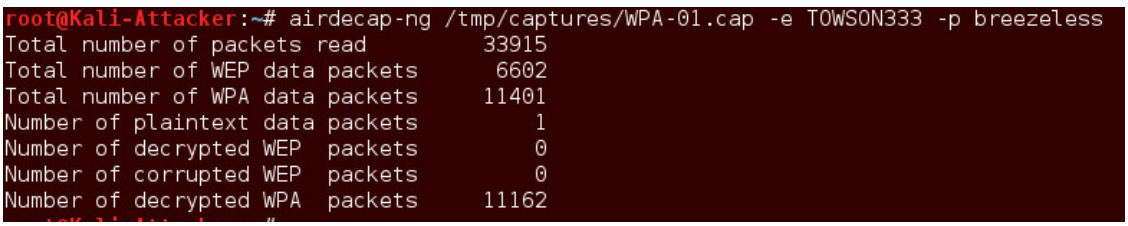


After a couple of seconds, the *WPA passphrase* is obtained.



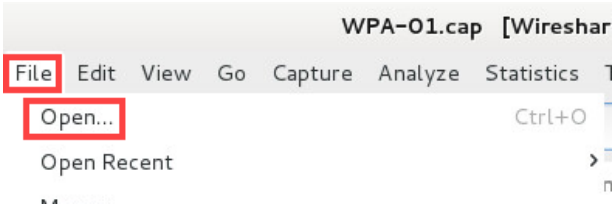
6. Decrypt the traffic for the wireless network **TOWSON333**. Type the command below to decrypt the traffic.

```
root@Kali-Attacker:~# airdecap-ng /tmp/captures/WPA-01.cap –e TOWSON333 –p
breezeless
```

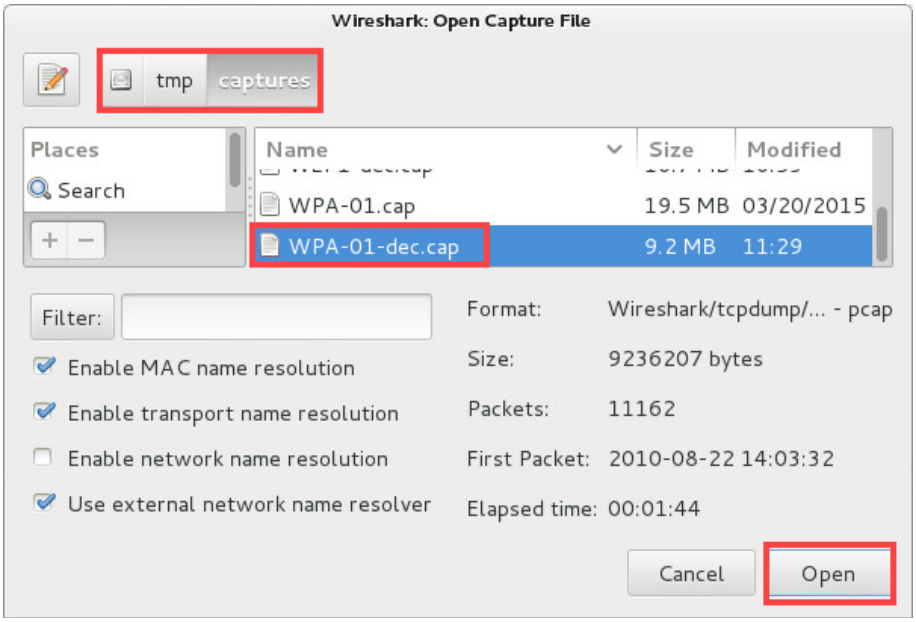


The number of decrypted of WPA packets should be *11,401.*

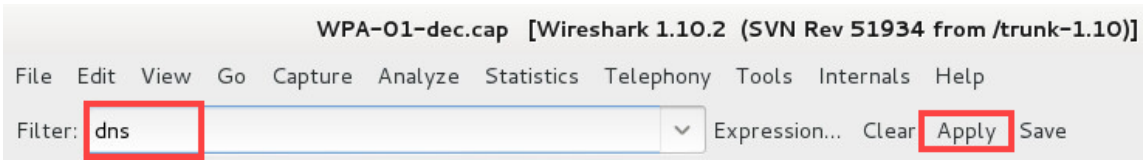
7. Change focus to the **Wireshark** application.
8. Within the *Wireshark* application, select the **File** menu option and click **Open**.



9. Navigate to the **/tmp/captures** directory and select the **WPA-01-dec.cap** file. Click **Open**.

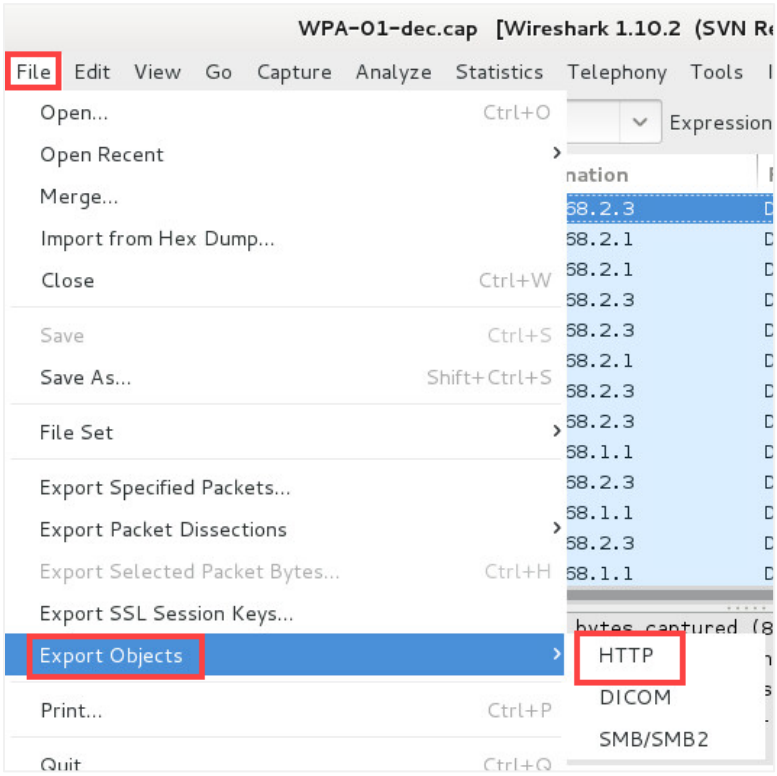


10. In the *Filter:* pane, type **dns** and click **Apply**.

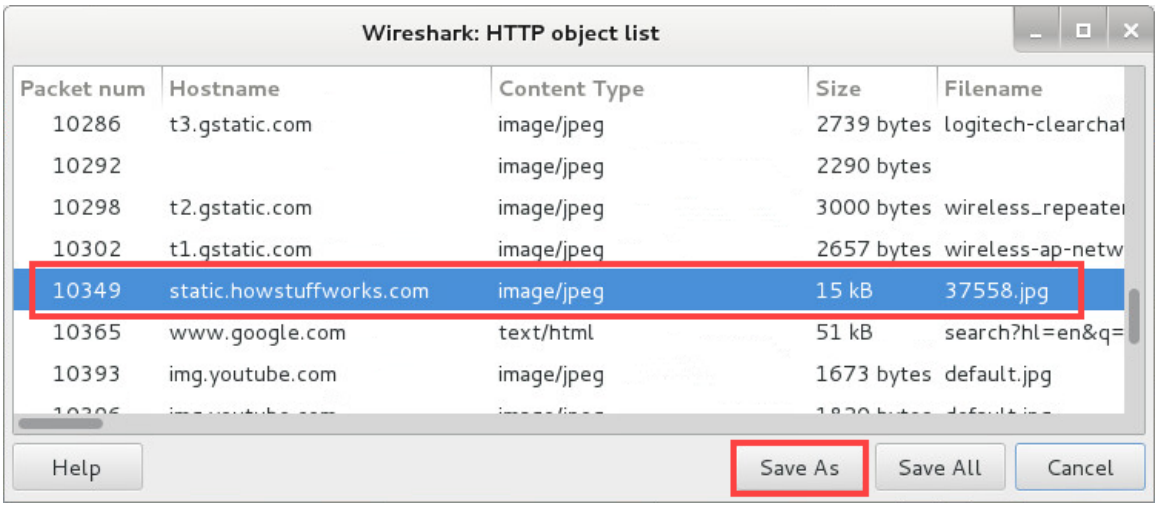


You will now be able to see *DNS* requests with the decrypted wireless traffic.

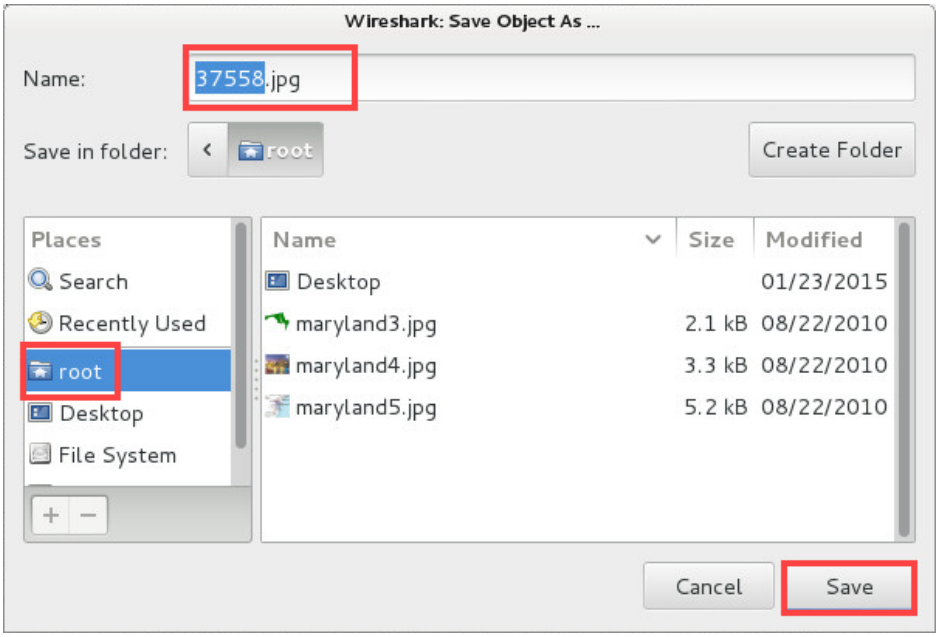
11. Select the **File** menu option and navigate to **Export Objects > HTTP**.



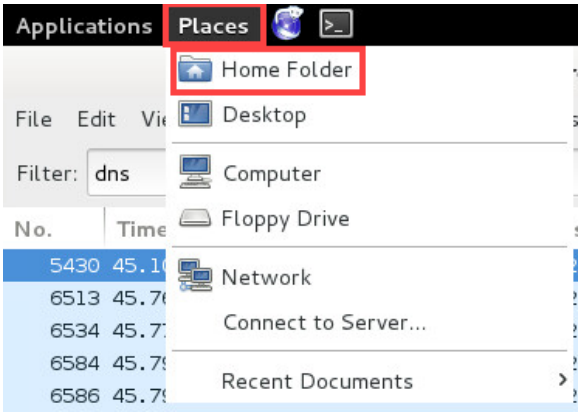
12. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, find item **#10349 (37558.jpg)** and select it. Click the **Save As** button.



13. In the *Save Object As* window, select **root** from the *Places* column located on the left and click **Save**.



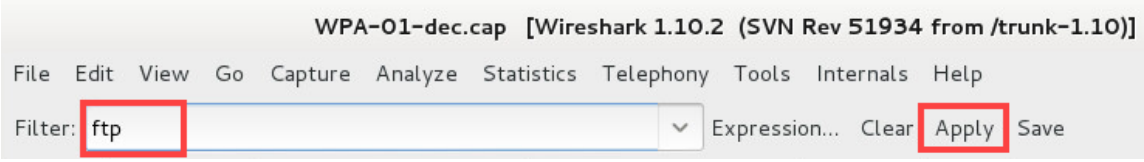
14. **Close** the *HTTP object list* window.
15. View the file by selecting the **Places** menu option from the top menu pane and click **Home Folder**.



Notice the new *JPEG* file in the *Home* folder.

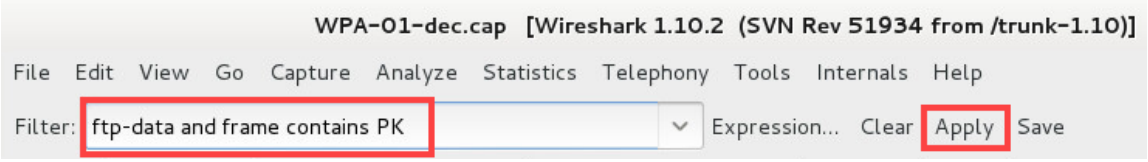
16. **Close** the *File Manager* window.

17. Change focus to the **Wireshark** application and type **ftp** in the *Filter:* pane. Click **Apply**.

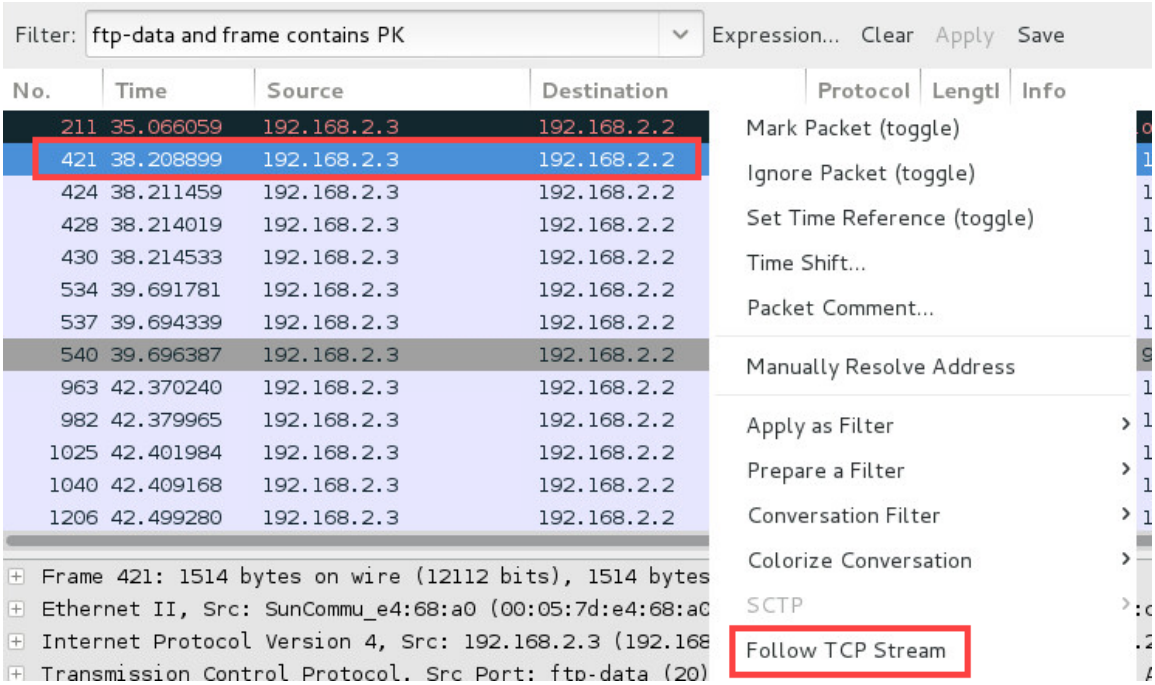


You will now be able to see the decrypted *FTP* traffic along with clear text usernames and passwords.

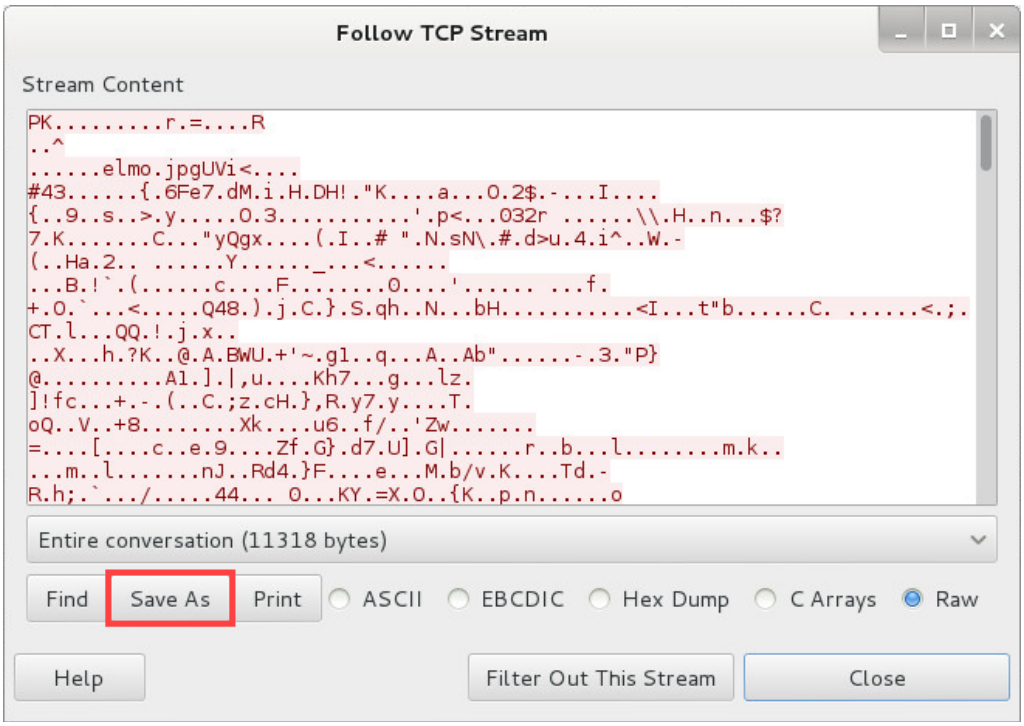
18. Scroll down through the *ftp frames* and examine some of the file names that were transferred.
19. Pull one of the zip files transferred via *FTP*. Type **`ftp-data and frame contains PK`** into the *Filter:* pane. Click **Apply**.



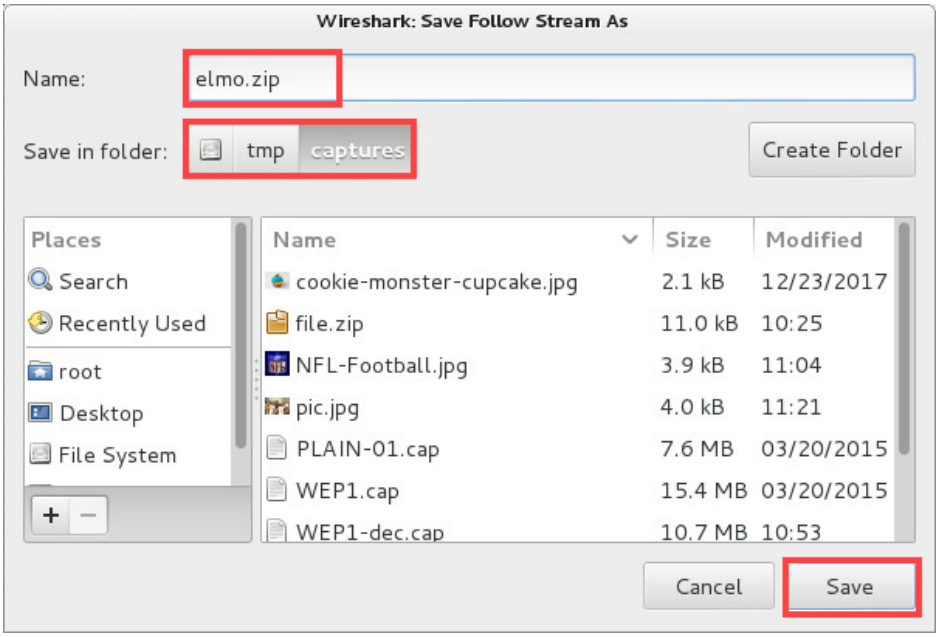
20. Right-click on the **second frame** in the list (**#421**) and select **Follow TCP Stream**.



21. A new window appears. Click the **Save As** button.



22. For the name, type **`elmo.zip`**. Verify the directory you are saving the file to **/tmp/captures**. Click **Save**.



23. **Close** the *Follow TCP Stream* window.

24. Open a new **terminal** window. Verify that you are in the **/root** directory by typing the command below, followed by pressing **Enter**.

```
root@Kali-Attacker:~# pwd
```

```
root@Kali-Attacker:~# pwd
/root
```

25. Type the command below to **unzip** the contents of **elmo.zip**.

```
root@Kali-Attacker:~# unzip /tmp/captures/elmo.zip
```

```
root@Kali-Attacker:~# unzip /tmp/captures/elmo.zip
Archive:  /tmp/captures/elmo.zip
  inflating: elmo.jpg
 extracting: elmo2.jpg
 extracting: elmo3.jpg
```

26. Select the **Places** menu option located on the top menu pane and click on **Home Folder**.

Notice the extracted *Elmo* images from the zipped file.

27. The lab is now complete; you may end the reservation.