SECURITY+ V4 LAB SERIES

Lab 18: Wireless Networking Attack and Mitigation Techniques

Document Version: 2023-02-27

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	3.4: Given a scenario, install and configure wireless security settings
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	20: Wireless Security

Contents

Introduction

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

Objective

In this lab, you will perform the following tasks:

- Examining Plain Text Traffic
- Exploiting and Examining WEP Traffic
- Exploiting and Examining WPA Traffic

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.

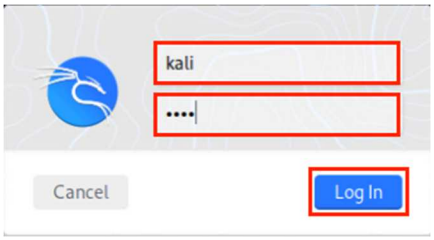
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali	`203.0.113.2`	`kali`	`kali`

1 Examining Plain Text Traffic

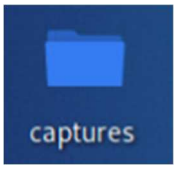
1.1 Viewing Plain Text Wireless Traffic

1. Click on the **Kali** tab to access the *Kali* VM.

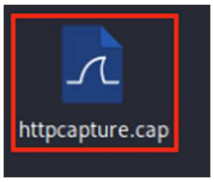
2. Log in to the *Kali* VM as username `kali`, password `kali`.



3. On the desktop, find and double-click to open the folder named **captures**.

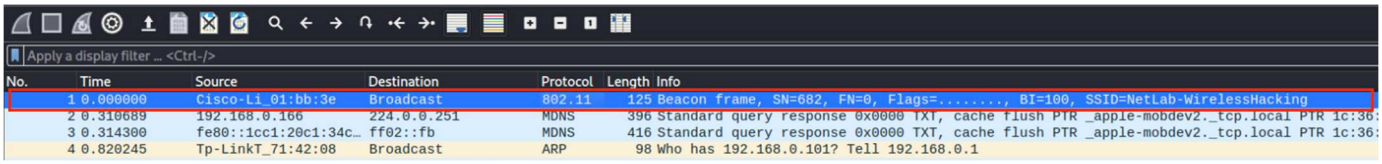


4. In the pop-up window. Double-click the **httpcapture.cap** file to open it in *Wireshark*.

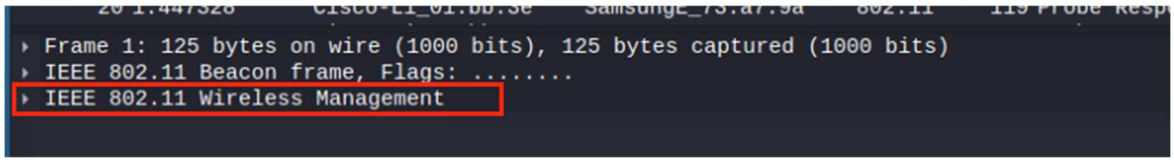


5. Click the **maximize** button shown on the screenshot to maximize the window to full-screen inside the VM.

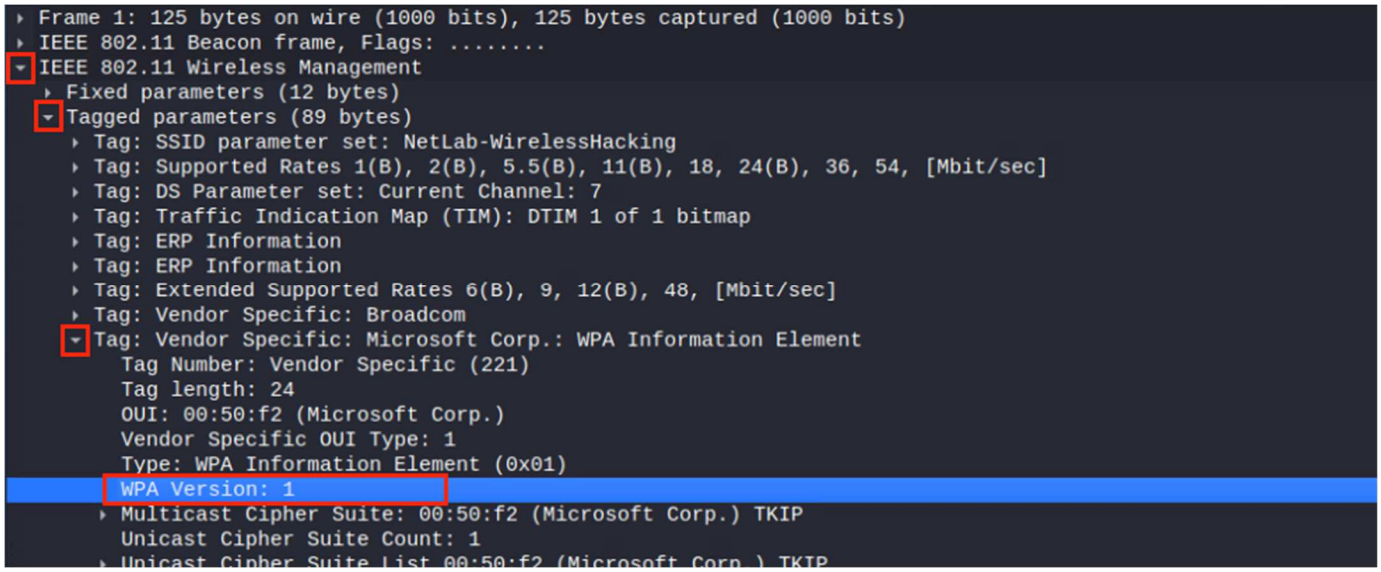
6. Select the **first frame** in the *Wireshark* capture file.



7. In the middle of the screen, click the **arrow** icon in front of the *IEEE 802.11 Wireless Management* to expand its view.

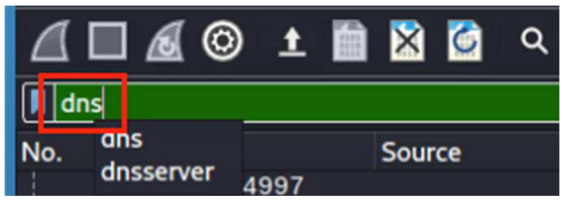


8. Dive in further by clicking the arrow icon in front of *Tagged parameters* followed by clicking the **arrow** icon in front of *Tag: Vender Specific: Microsoft Corp.: WPA Information Element*. View the *WPA Version*.



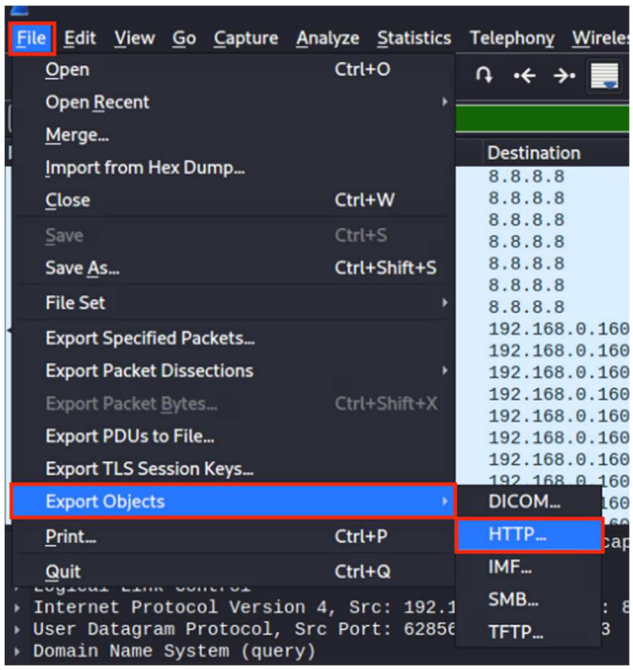
Drag the handle to make the packet detail section area larger.

9. View captured *DNS requests* by typing **dns** in the *Filter* pane, then press **Enter**.

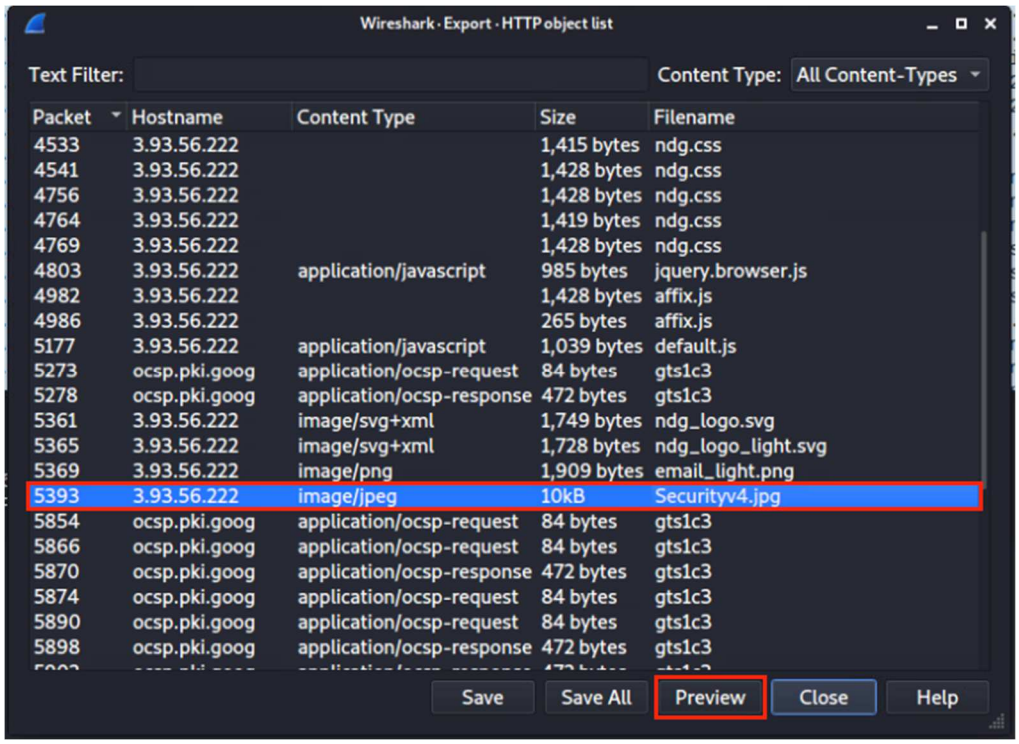


1.1.1 Extract Image from Capture

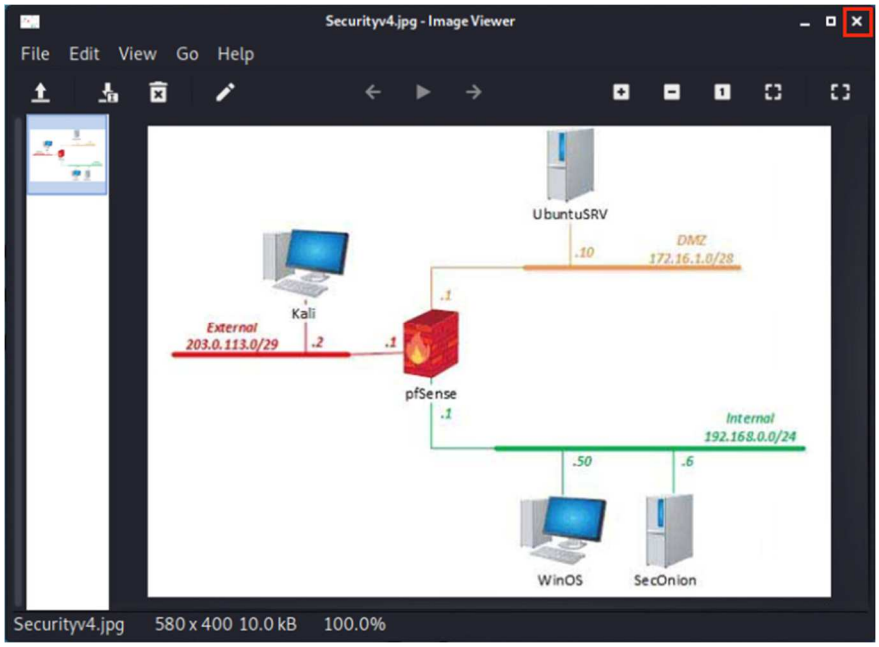
1. With *Wireshark*, we can export images and files that have passed through the capture communication channel. Try exporting a file by clicking on the **File** menu option on the top pane and navigating to **Export Objects > HTTP**.



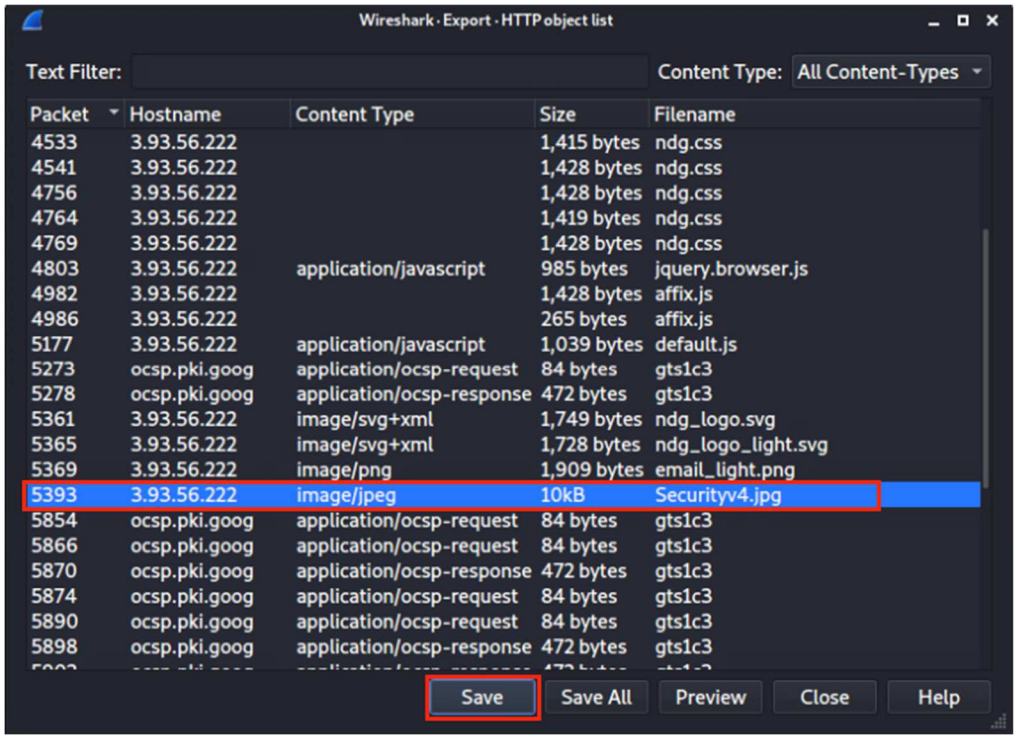
2. A new window appears. Look through the list of files that have been downloaded by wireless users. Under the *Filename* column, find the image file **Securityv4.jpg** and select the file. (Or, find the number *5393* under the *Packet* column.). With the file selected, click the **Preview** button.



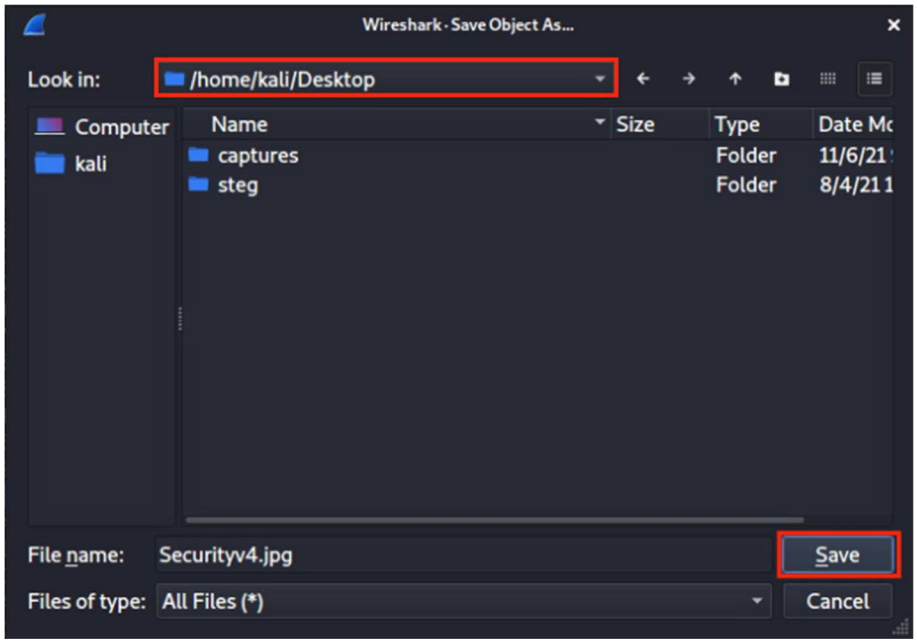
3. A preview window will open, showing a topology. Click the **X** to close the preview. Feel free to select and preview other image files being captured. Close the preview window once you finish examining them.



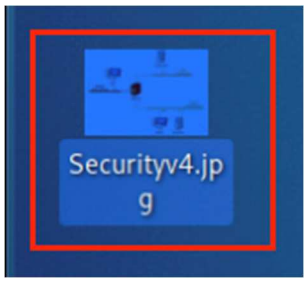
4. Alternatively, you can choose to save the *Securityv4.jpg* file. Having the file selected, click the **Save** button.



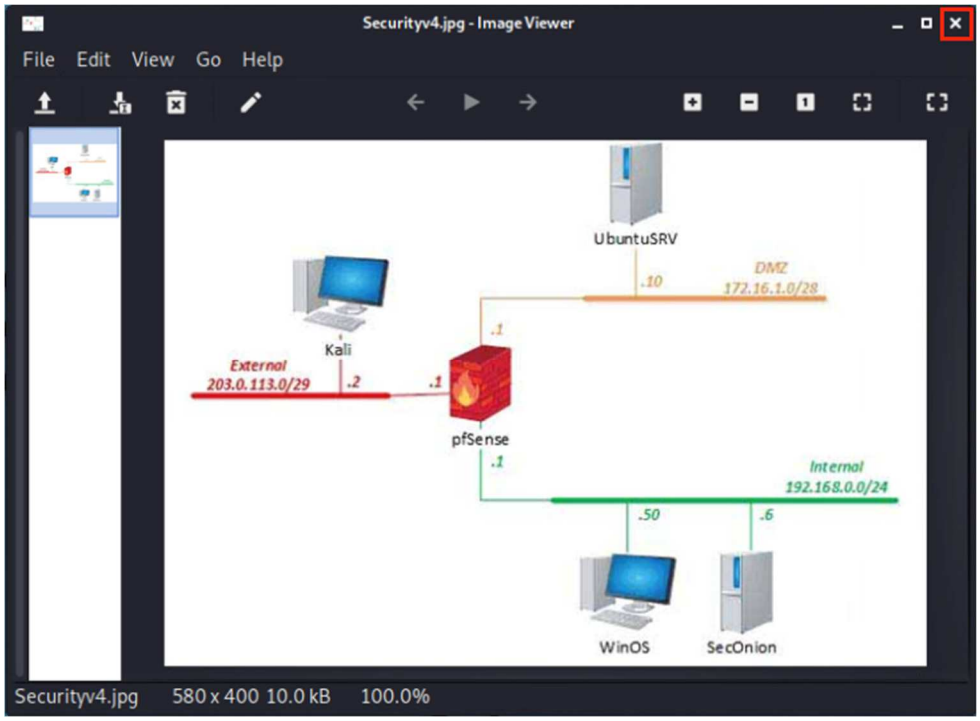
5. In the *Save Object As* window, choose the **/home/kali/Desktop** directory to save to and click the **Save** button.



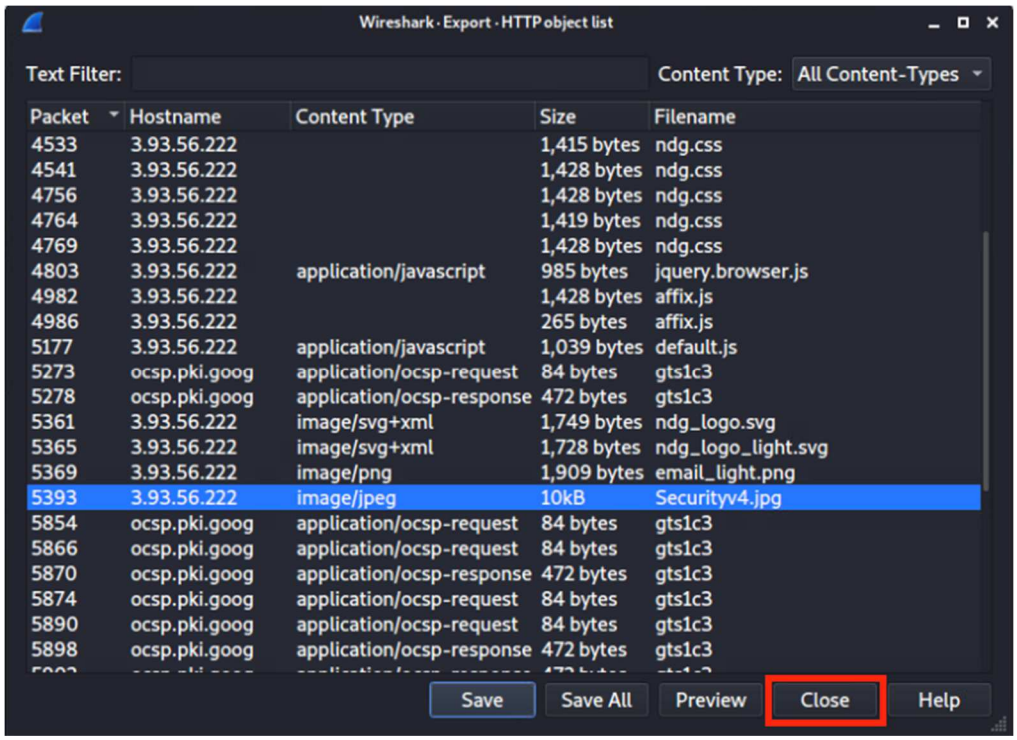
6. View the image by selecting the **Show desktop** menu option located next to the *Applications* menu. Double-click to open **Securityv4.jpg**.



7. The same topology image opens. **Close** the *image viewer*.

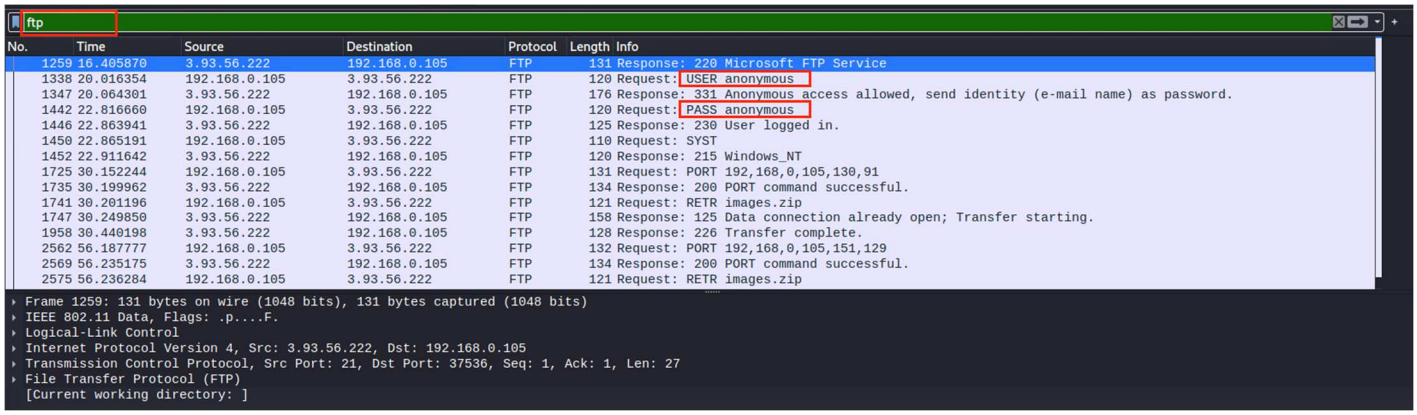


8. Click the **Show** desktop button again to restore the windows. Close the *HTTP object list* window.



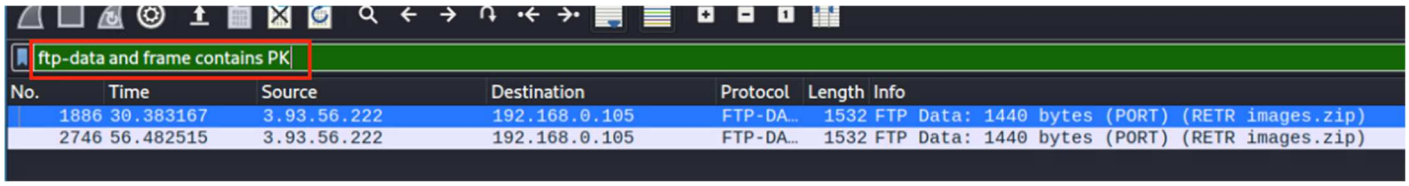
1.1.2 Extract Zip File from FTP Traffic

1. Within the *Wireshark* interface, type `ftp` into the *Filter:* and press **Enter**. Because FTP is not encrypted, you will be able to see captured FTP traffic as well as clear-text usernames and passwords. Analyze the FTP traffic.

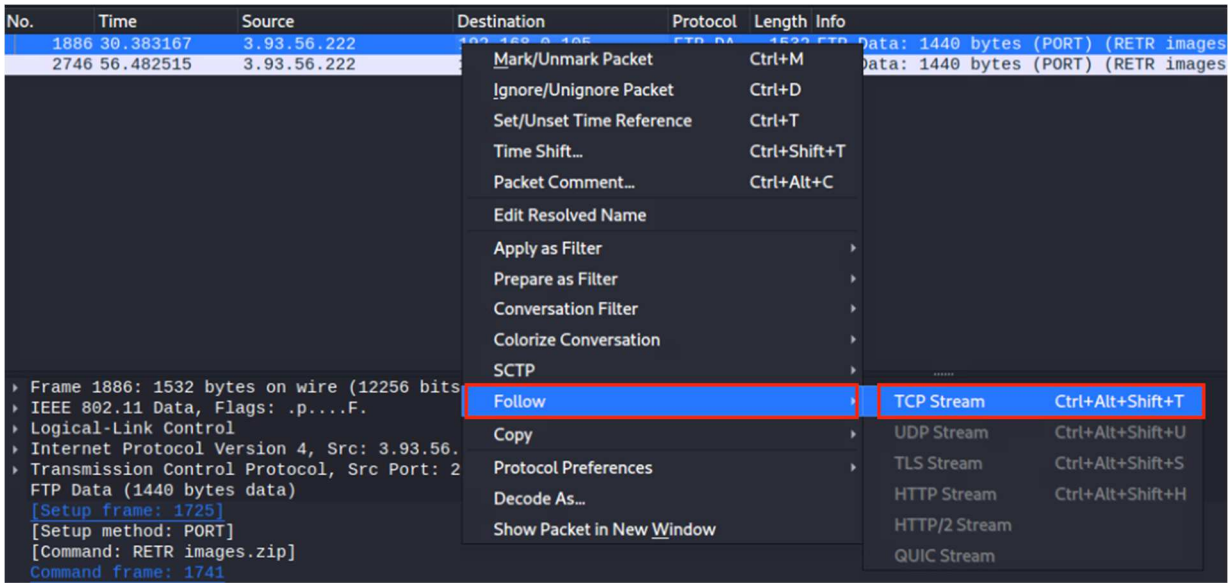


You will want to disable the anonymous user access and use a secured FTP service for file sharing.

2. Next, we will pull a zip file via *FTP* out of the wireless capture file. Type `ftp-data and frame contains PK` into the *Wireshark Filter:* and press **Enter**.

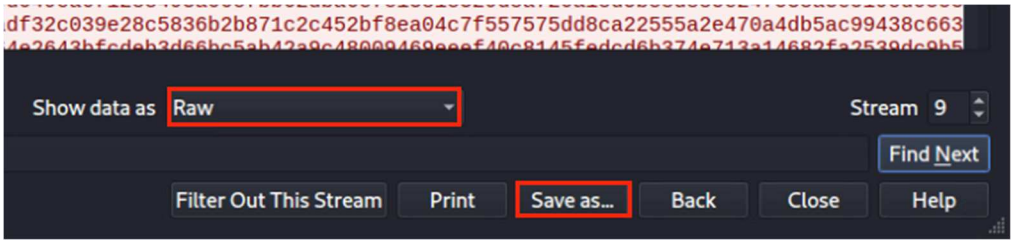


3. Right-click on either the **frame 1886** or **2746** in the list and select **Follow**, **TCP Stream**.

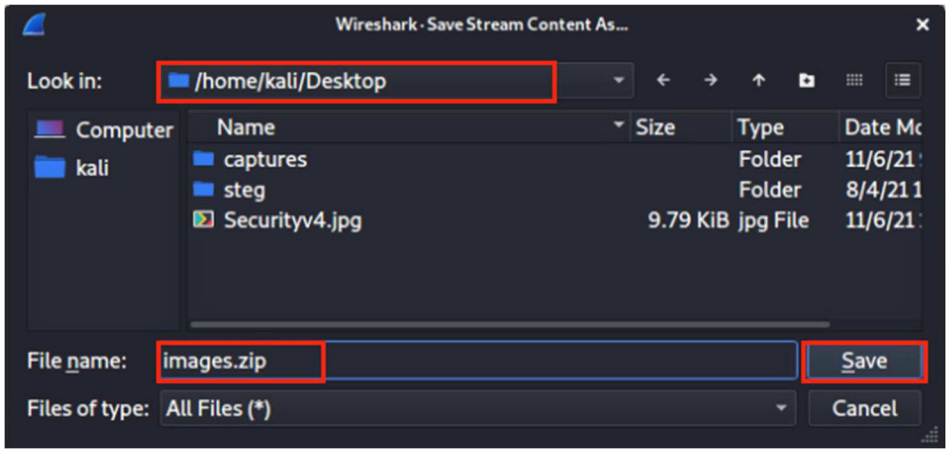


4. Examine the data shown in the *TCP stream*. Scroll to the bottom of the window and notice the *PK*" attached to the end of filenames.

5. Within the *Follow TCP Stream* window, click Show data as **Raw**, then click **Save As**.

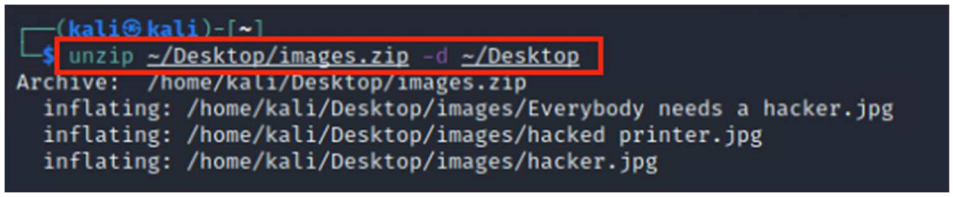


6. Type **images.zip** in the *Name* text field. Set the save destination to **/home/kali/Desktop** and click the **Save** button.

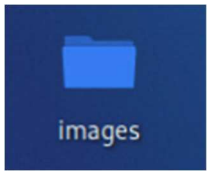


7. **Close** the *Follow TCP Stream* window.
8. Open a new *Terminal* window and type the command below to **unzip** the file that was just pulled from the *Wireshark* capture file.

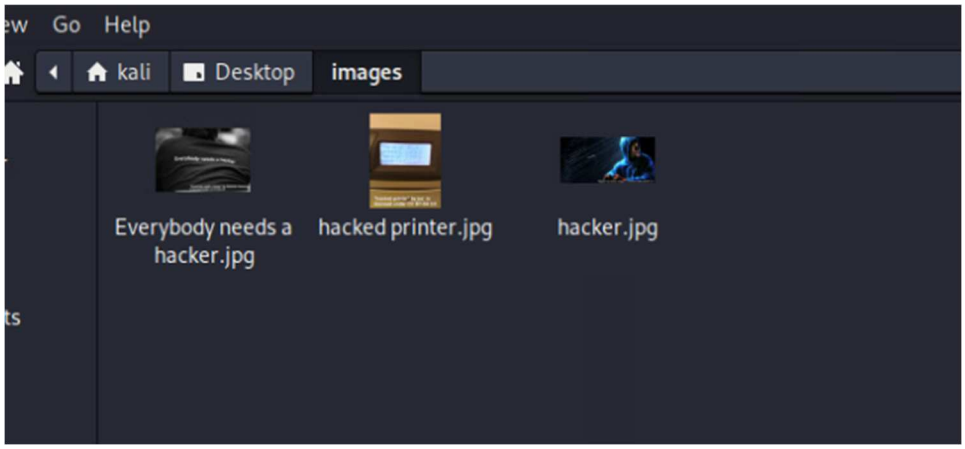
```
kali@kali$ unzip ~/Desktop/images.zip -d ~/Desktop
```



9. Select the **Show desktop** menu option from the top menu pane and double-click on the **images** Folder.



10. Notice the three different image files in the **images** directory that were extracted from *images.zip*. Feel free to open each of them and check the content.

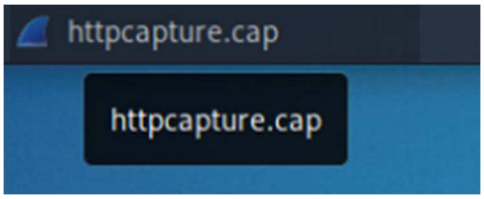


11. **Close** the *images* window.
12. Leave the *Kali* window open to continue with the next task.

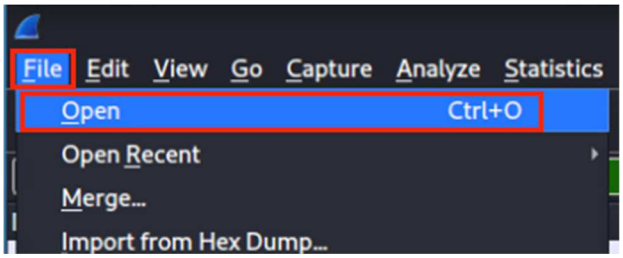
2 Exploiting and Examining WEP Traffic

2.1 Decrypt and Analyze WEP Traffic

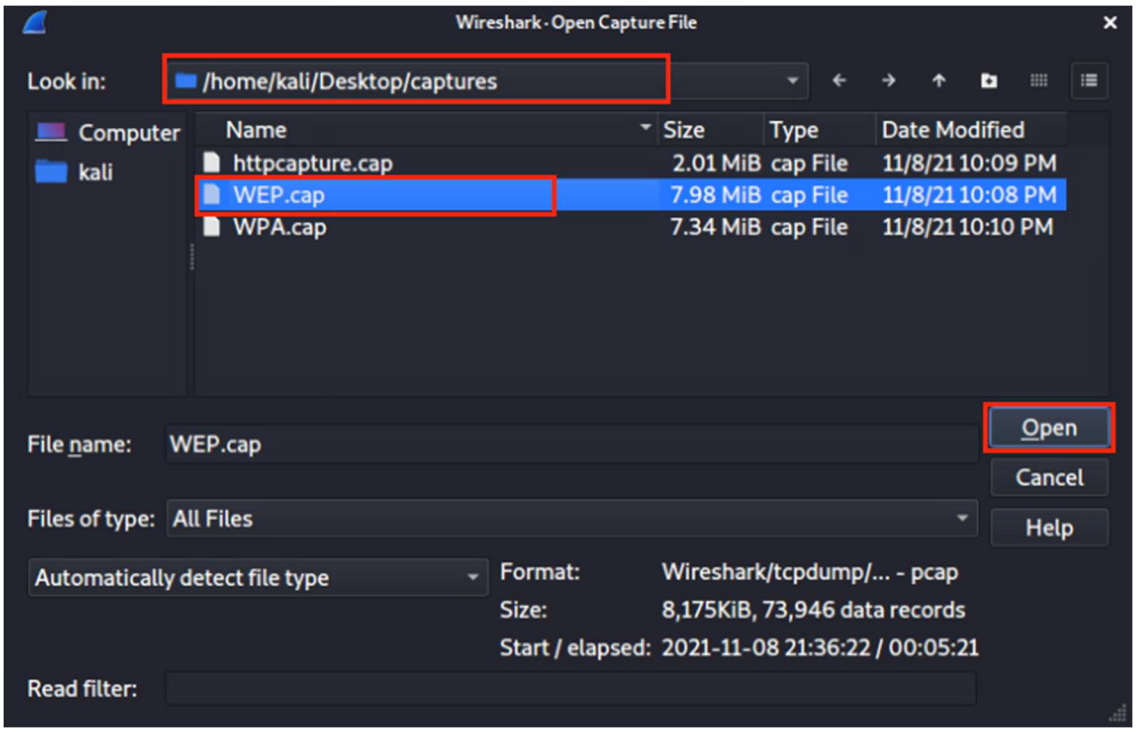
1. Click on the **httpcapture.cap** Wireshark window to restore it.



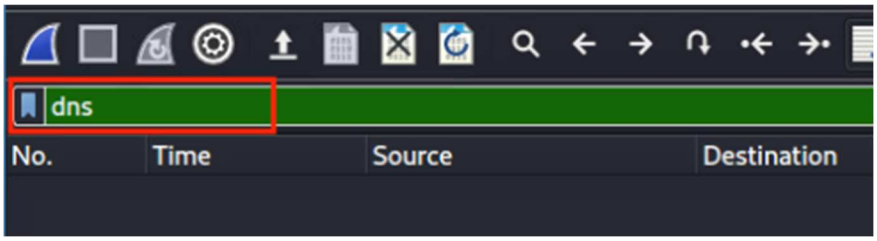
2. Select the **File** menu option and click on **Open**.



3. A new window appears. Verify that you are in the **/home/kali/Desktop/captures** directory. Select the **WEP.cap** file and click the **Open** button.



4. In the *Filter:* pane, type **dns** and press **Enter**.

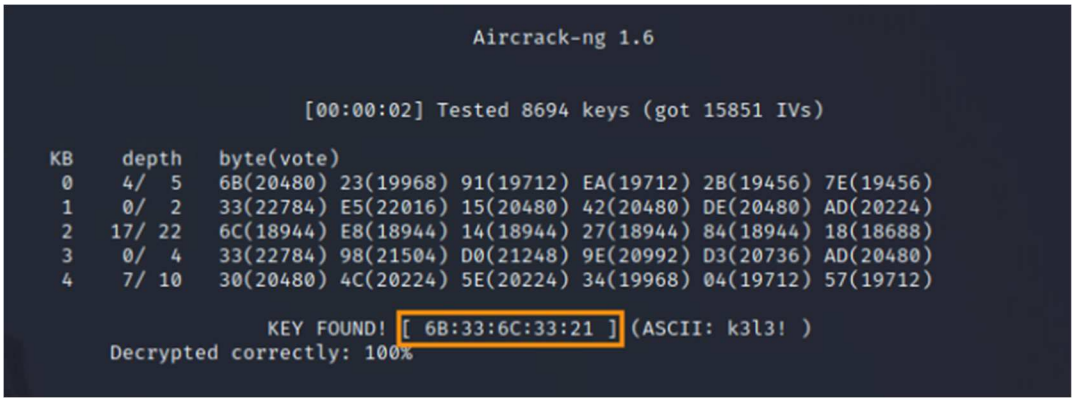


You will not see any traffic displayed because the wireless traffic is encrypted.

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

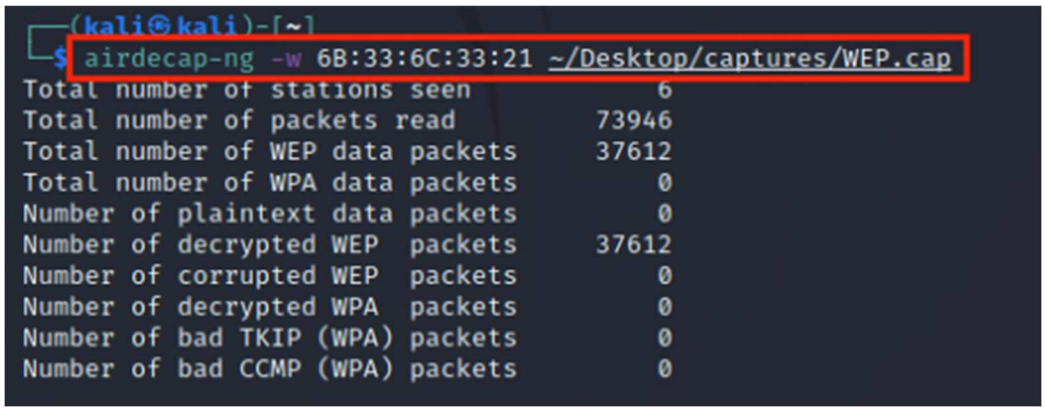
```
kali@kali$ aircrack-ng ~/Desktop/captures/WEP.cap
```

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



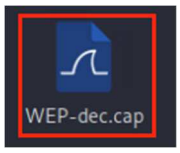
8. After the *WEP* key is obtained, decrypt the network traffic with **airdecap-ng**. Enter the command shown below to decrypt the traffic.

```
kali@kali$ airdecap-ng -w 6B:33:6C:33:21 ~/Desktop/captures/WEP.cap
```

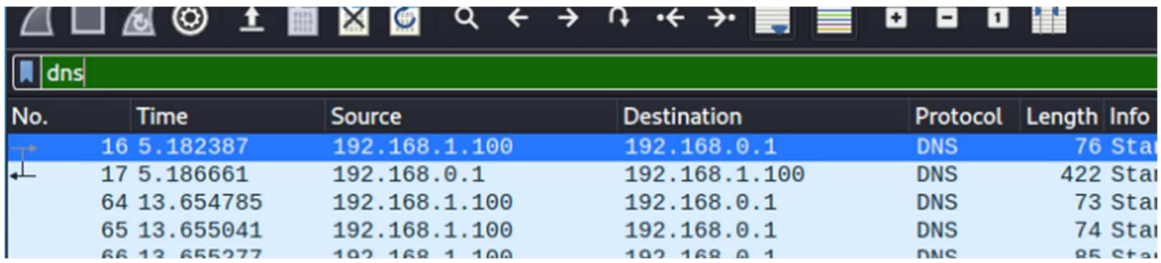


The number of *decrypted WEP packets* should be *37612*.

9. Analyze the decrypted traffic with *Wireshark*. Change the focus to the captures window, double-click the **WEP-dec.cap** to open it in *Wireshark*.

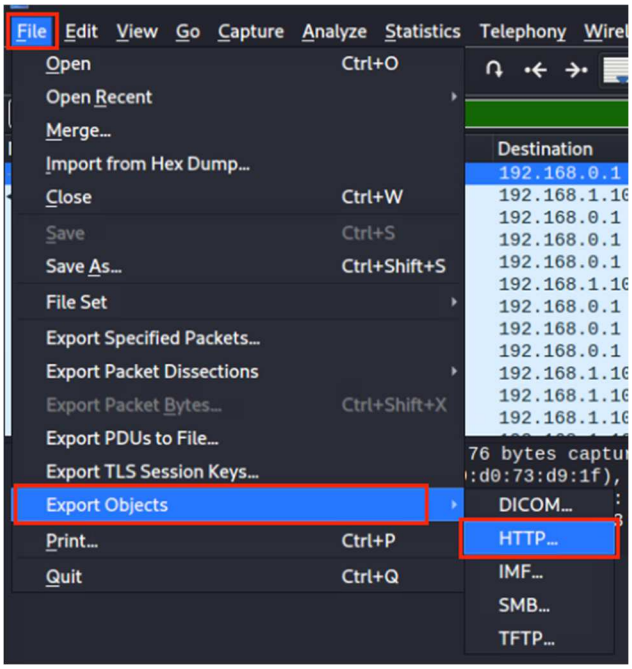


10. In the *Filter:* pane, type **dns** and press **Enter**.

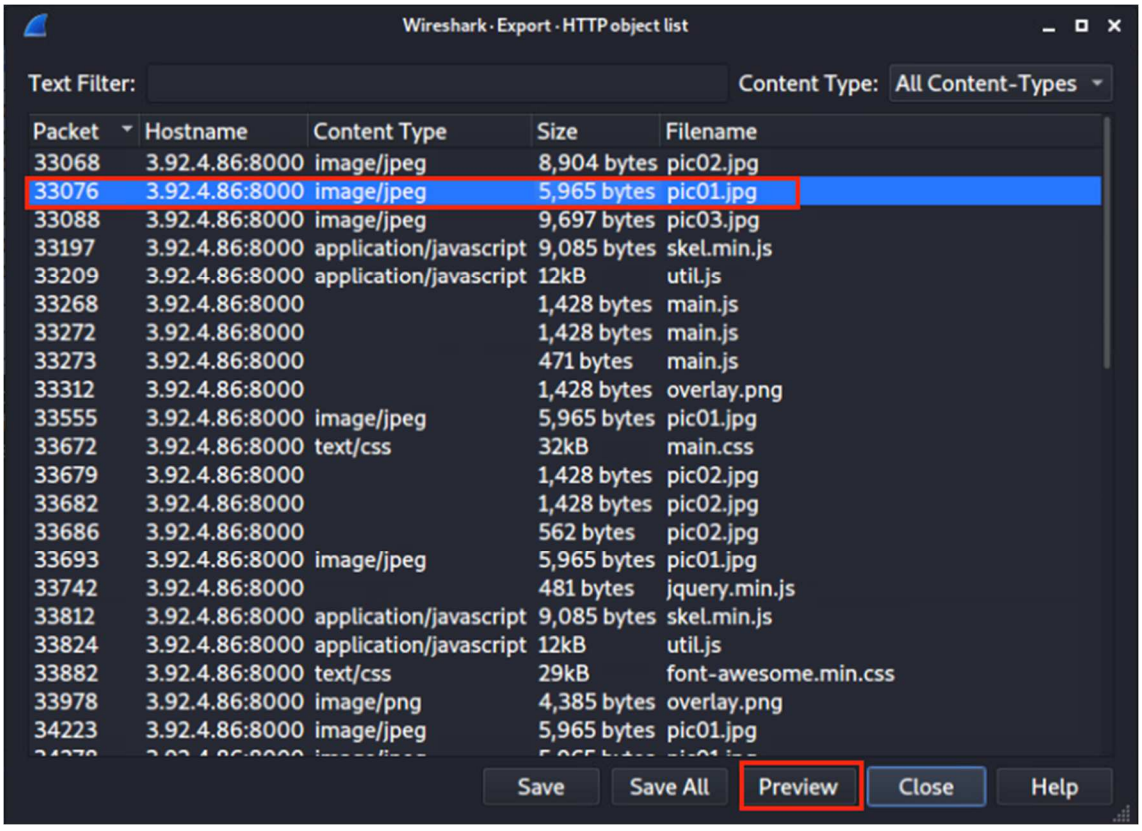


Notice that you can now see the *DNS* requests within the wireless traffic because the WEP traffic was decrypted with *airdecap-ng*.

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

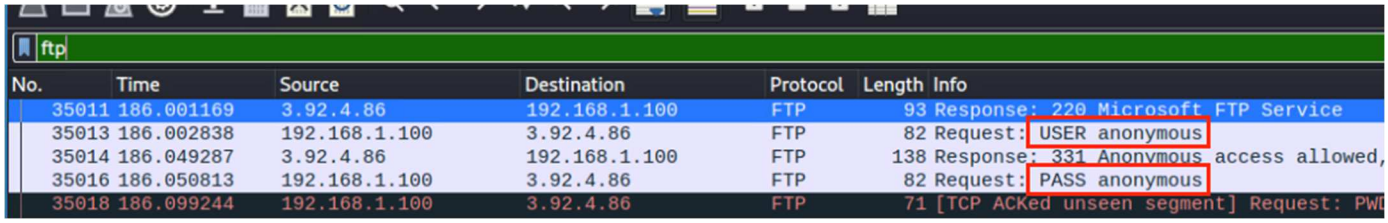


12. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, select item **#33076 (pic01.jpg)**. Once selected, click the **Preview** button.

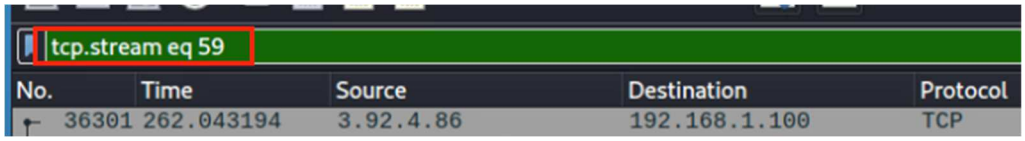


13. The *Image Viewer* window opens, showing the image content.

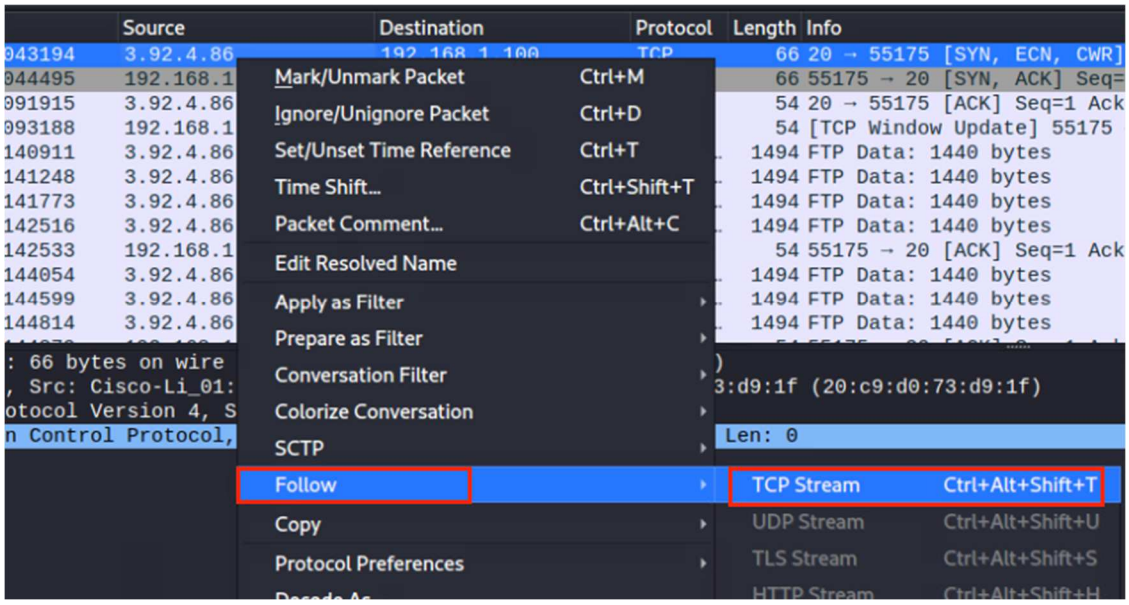
14. **Close** the *Image Viewer* window.
15. **Close** the HTTP object list window.
16. Change focus to the **Wireshark** application and type `ftp` into the *Filter:* pane. Click **Apply**. You will be able to see decrypted FTP traffic as well as clear-text usernames and passwords. Analyze the FTP traffic.



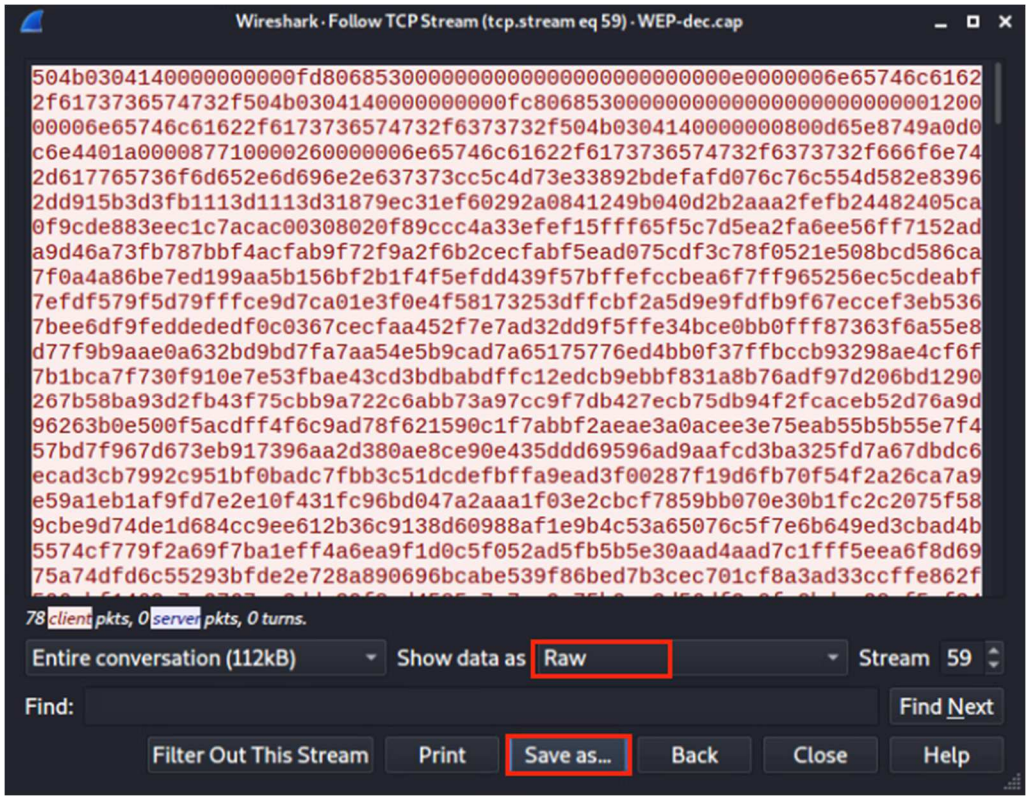
17. Let's pull a *ZIP* file transferred via *FTP* from the wireless capture. Type `tcp.stream eq 59` in the *Filter:* pane. Press **Enter**.



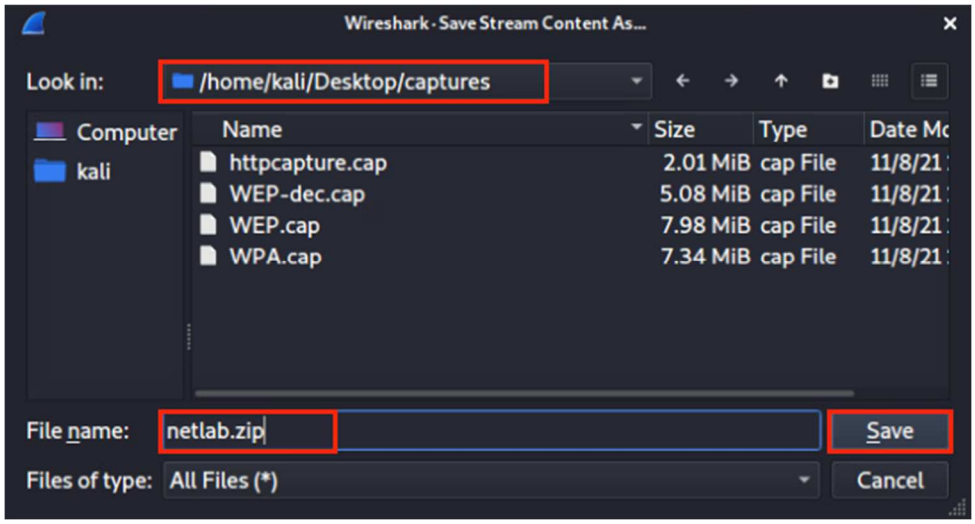
18. Right-click on the **first frame** in the list and select **Follow, TCP Stream**.



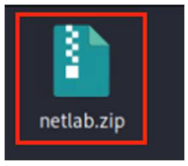
19. A new window appears. Change the *Show data as* to **Raw**, then click the **Save as** button.



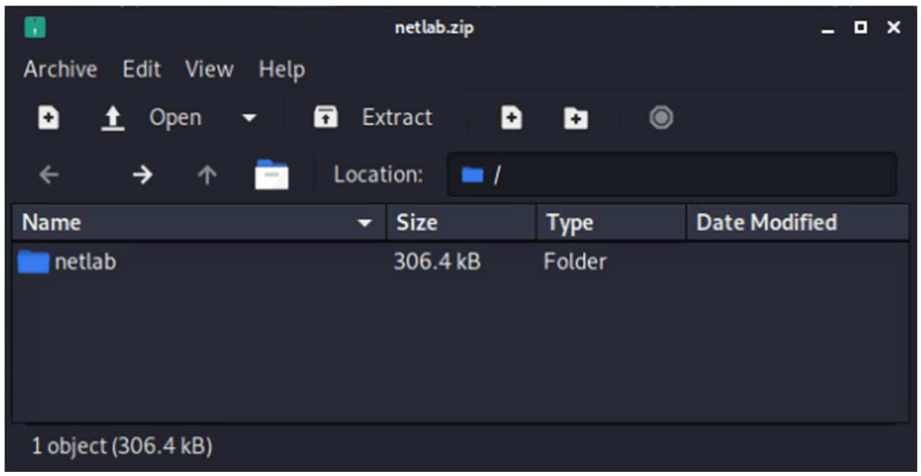
20. For the filename, type `netlab.zip`. Make sure the directory is set to `/home/kali/Desktop/captures` and click the **Save** button.



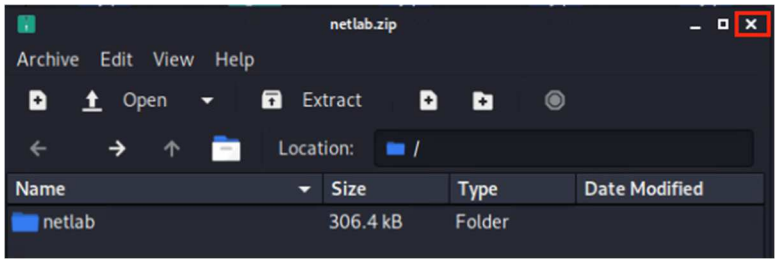
21. **Close** the *Follow TCP Stream* window.
22. Change focus to the captures window. Double-click on the **netlab.zip** file to open it.



23. A new window opens, showing the content of the zip file. Feel free to check the content in the **netlab** folder.



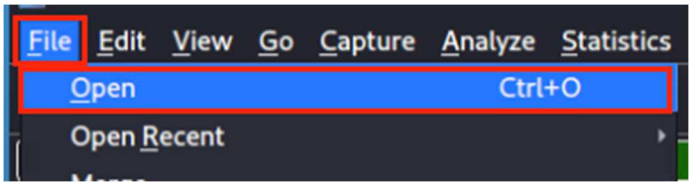
24. Once you finished observing the files, close the **netlab.zip** window.



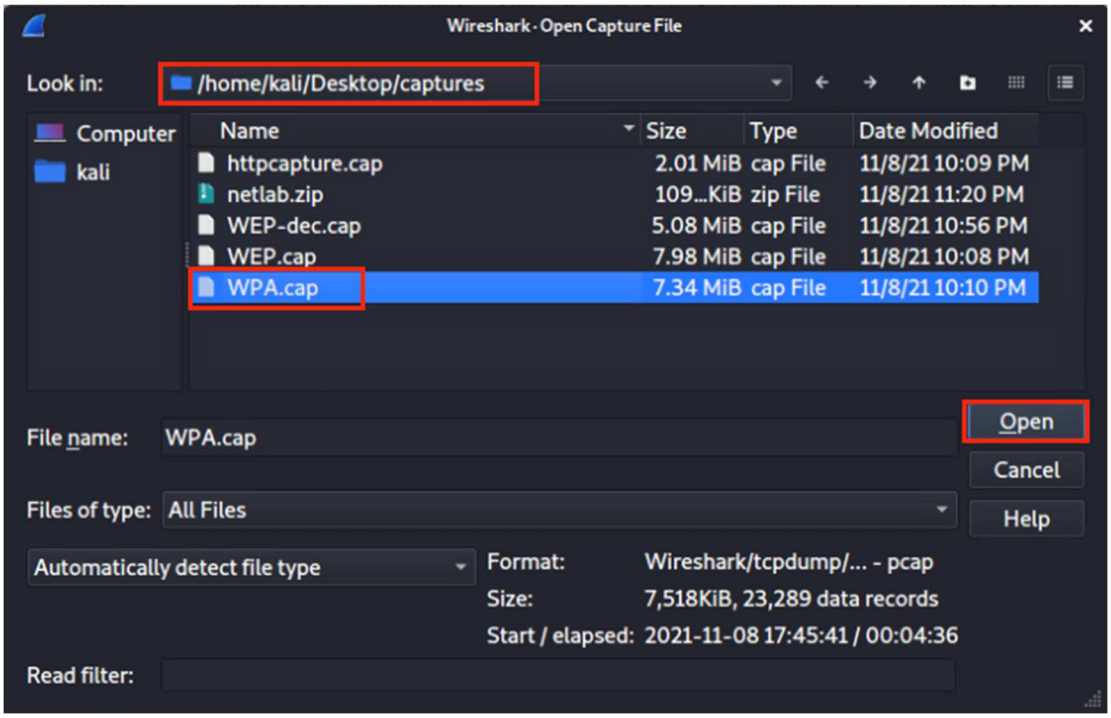
3 Exploiting and Examining WPA Traffic

3.1 Exploiting and Examining WPA Traffic

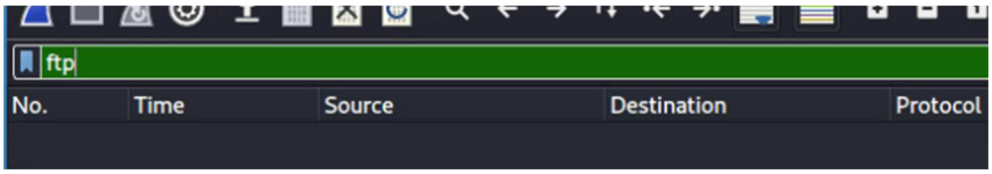
1. Change focus to the **Wireshark** application. Open a *WPA* capture file by selecting the **File** menu option. Click **Open**.



2. Navigate to the **/home/kali/Desktop/captures** directory and select the **WPA.cap** file. Click the **Open** button.



3. In the *Filter:* pane, type `ftp` and press **Enter**.

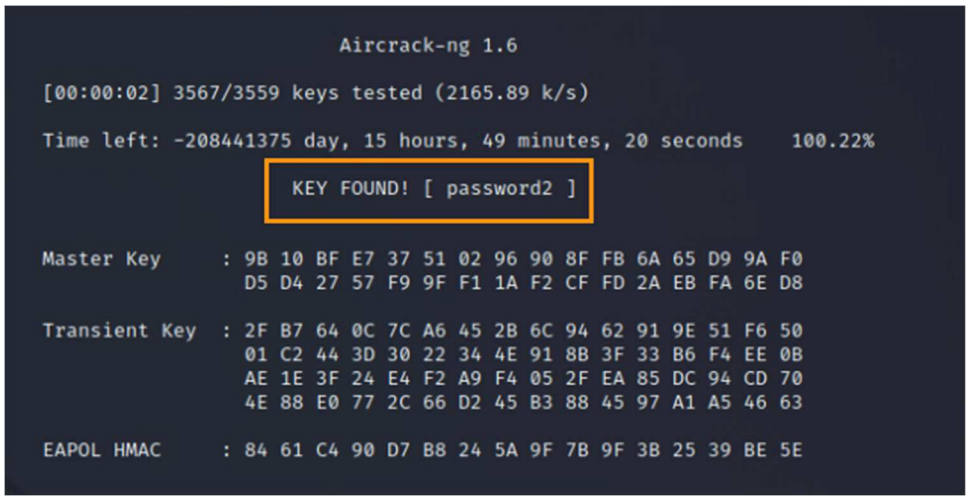


You will not see any traffic because the wireless network traffic is encrypted.

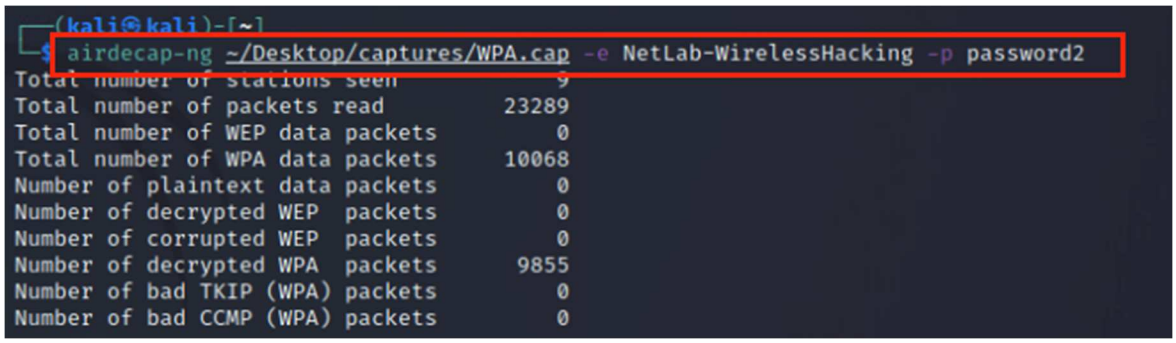
4. Close Wireshark, change focus to the terminal window, and type the command shown below.

```
kali@kali$ aircrack-ng ~/Desktop/captures/WPA.cap -w /usr/share/john/password.lst
```

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



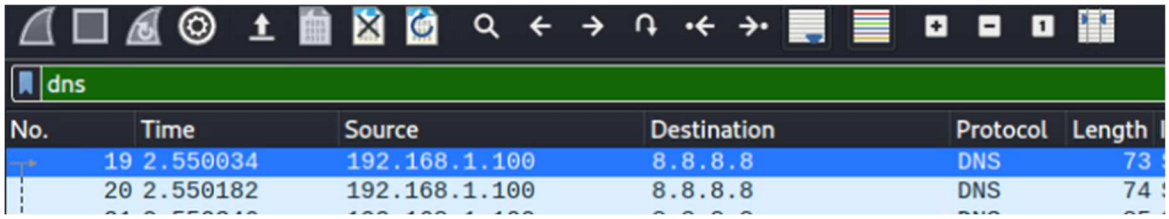
6. Decrypt the traffic for the wireless network **NetLab-WirelessHacking**. Type the command shown below to decrypt the traffic.



The number of decrypted of WPA packets should be 9855.

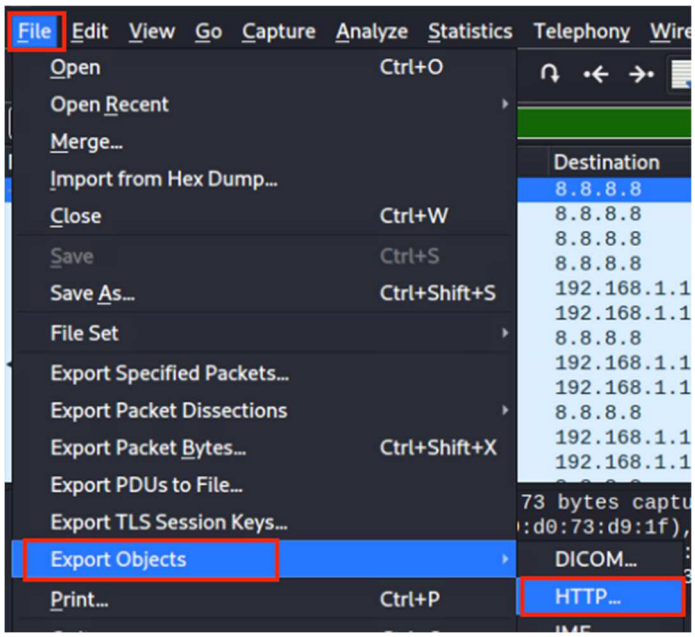
7. Change focus to the **Captures** window.
8. Double-click the **WPA-dec.cap** file to open it in *Wireshark*.

9. In the *Filter:* pane, type **dns** and press **Enter**.

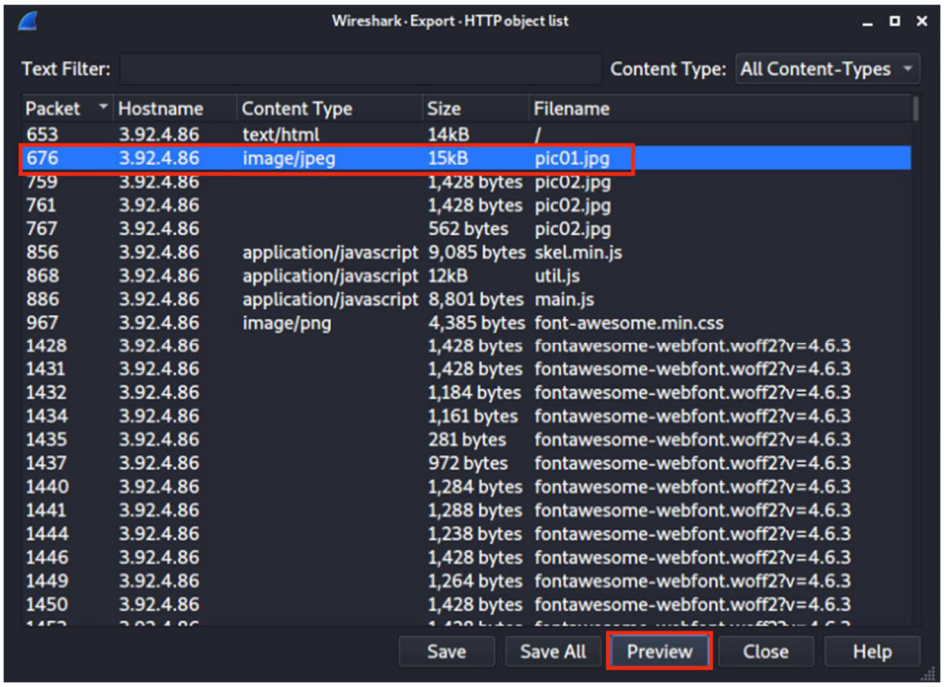


You will now be able to see *DNS* requests with the decrypted wireless traffic.

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



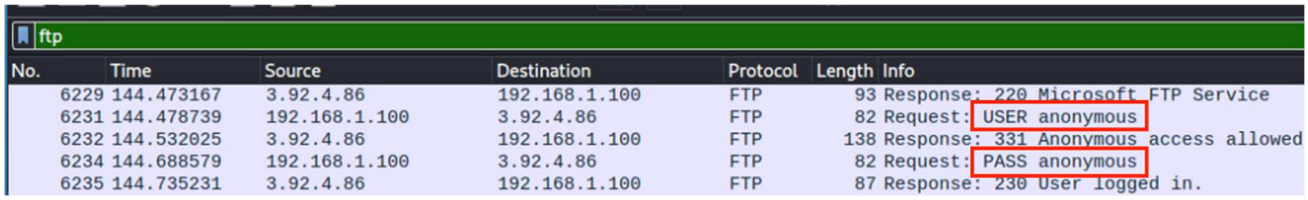
11. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, find item **#676 (pic01.jpg)** and select it. Click the **Preview** button.



12. The *Image Viewer* window opens, showing the content of the image.

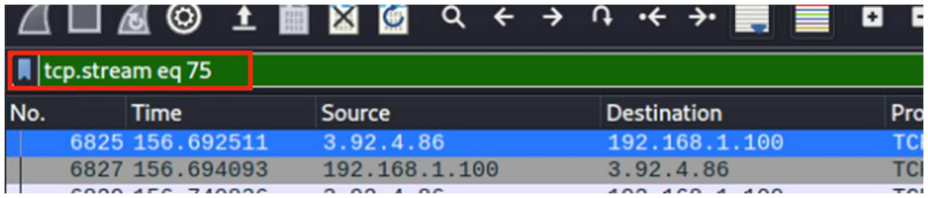
13. **Close** the *Image Viewer* window and the HTTP object list window.

14. Change focus to the **Wireshark** application and type `ftp` in the *Filter:* pane. Press **Enter**.

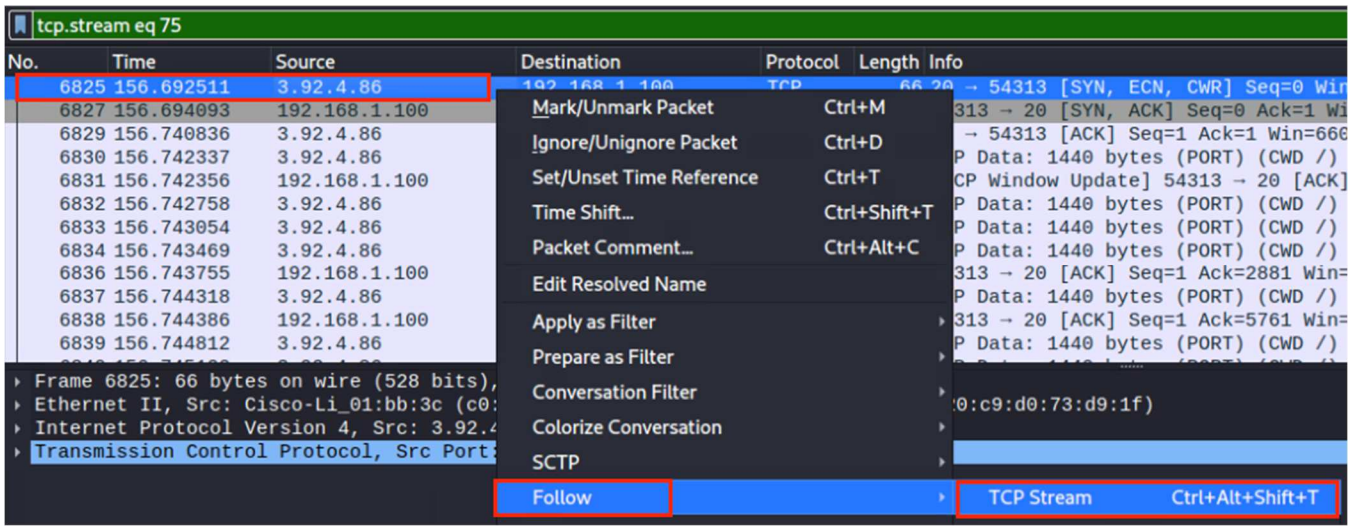


You will now be able to see the decrypted *FTP* traffic along with clear text usernames and passwords.

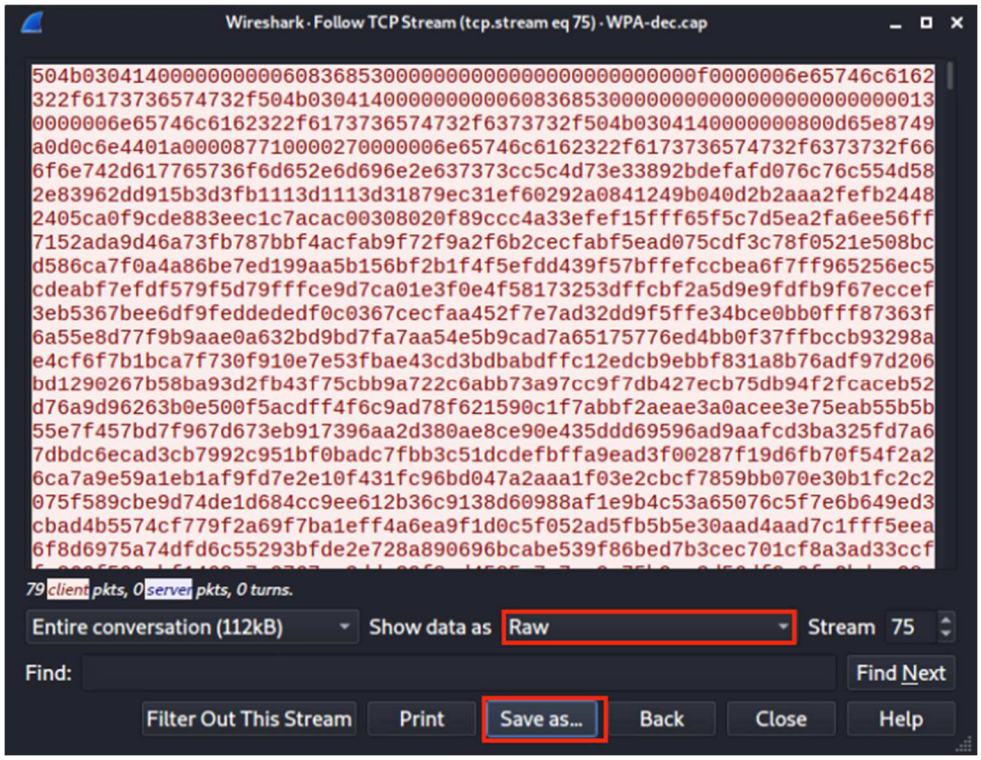
15. Scroll down through the *ftp frames* and examine some of the file names that were transferred.
16. Pull one of the zip files transferred via *FTP*. Type `tcp.stream eq 75` into the *Filter:* pane. Press **Enter**.



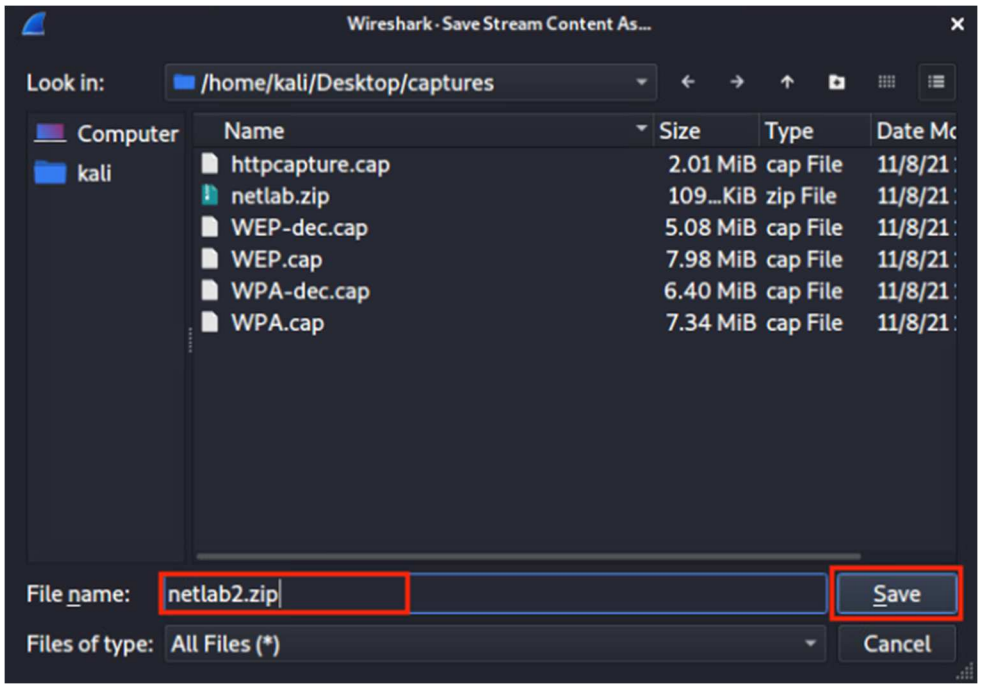
17. Right-click on the **first frame** in the list (**#6825**) and select **Follow > TCP Stream**.



18. A new window appears. Change the *Show data as* to **Raw**, then click the **Save as** button.

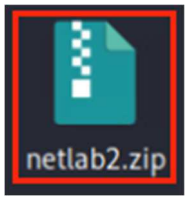


19. For the name, type `netlab2.zip`. Verify the directory you are saving the file to is **/home/kali/Desktop/captures**. Click **Save**.

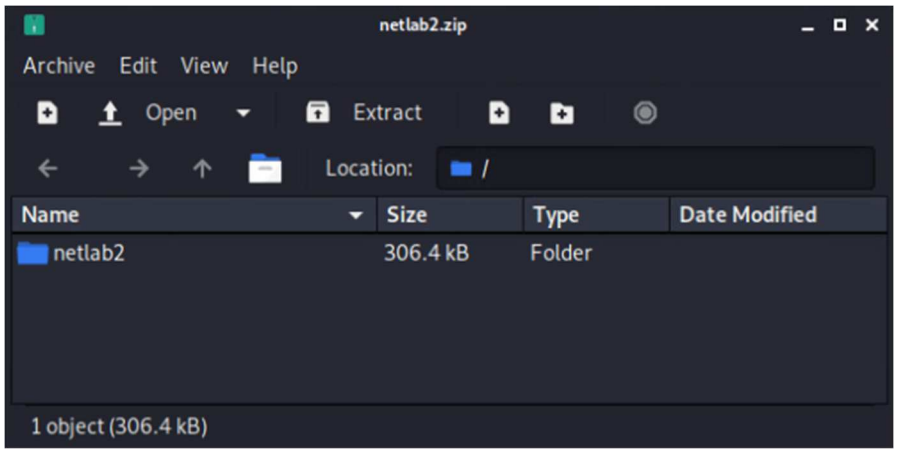


20. **Close** the *Follow TCP Stream* window.

21. Change focus to the captures window. Double-click the **netlab2.zip** file to open it.



22. A new window opens, showing the content of the zip file. Feel free to check the content in the **netlab2** folder.



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