SAT1: 006: Carving Files in Wireshark

Overview

According to research, 90% of malware is installed via http through a web site transaction. In this lab, we are going to learn how to extract files from a packet capture, which can save valuable time in an incident.

Time: 45 Minutes

Learning Objectives

Upon completion of this lab, you should be able to:

1. Understand what data can be obtained from a PCAP file, and how it can be extracted.
2. Use the extraction menu to extract files from a PCAP file.
3. Use the TCP Follow comman to extract file from PCAP file.
4. Edit an extracted file in order to open it in an image viewer.

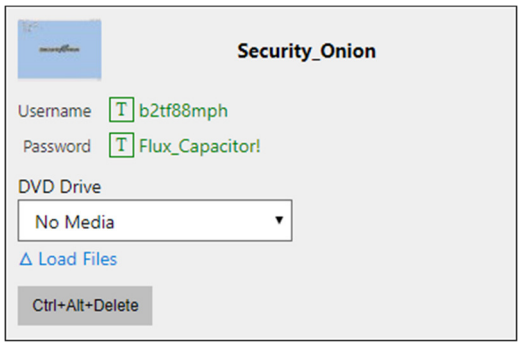
Resources

The following documents have been provided to assist you in this lab.

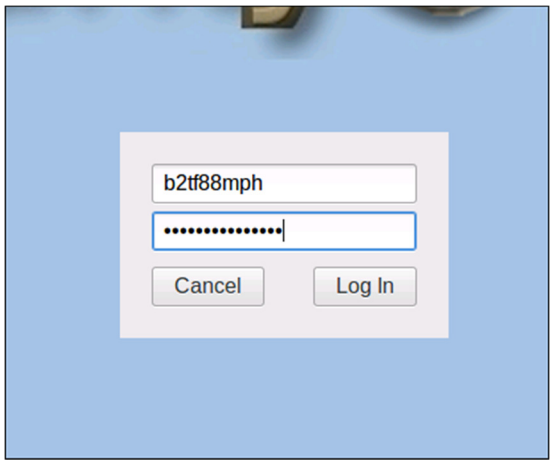
Wireshark Cheat Sheet

Log in to the Lab Machine

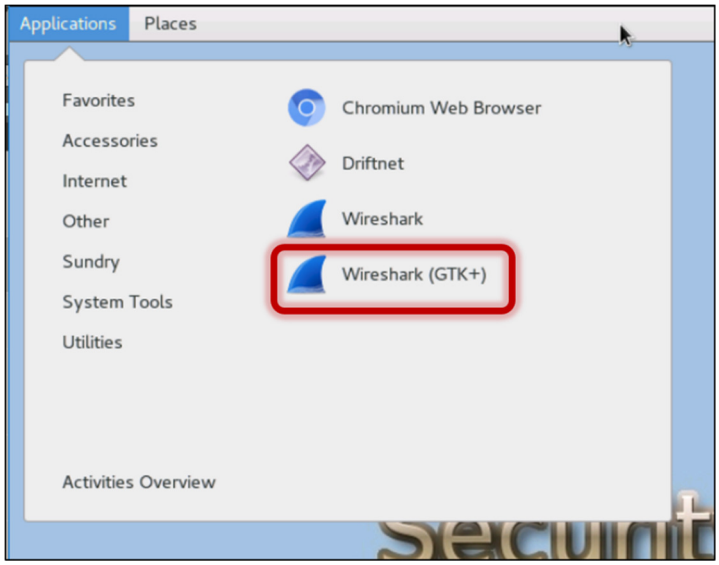
Select the **Security_Onion** machine on the Machines Tab.



Enter the Username and Password on the **Security_Onion** machine, and click Log In.



First, you will need to open the Wireshark application. In **Security_Onion**, Wireshark can be found by clicking on **Applications**, move your mouse over **Internet**, and click on **Wireshark (GTK+)**.



1.0 Carving Files with Wireshark

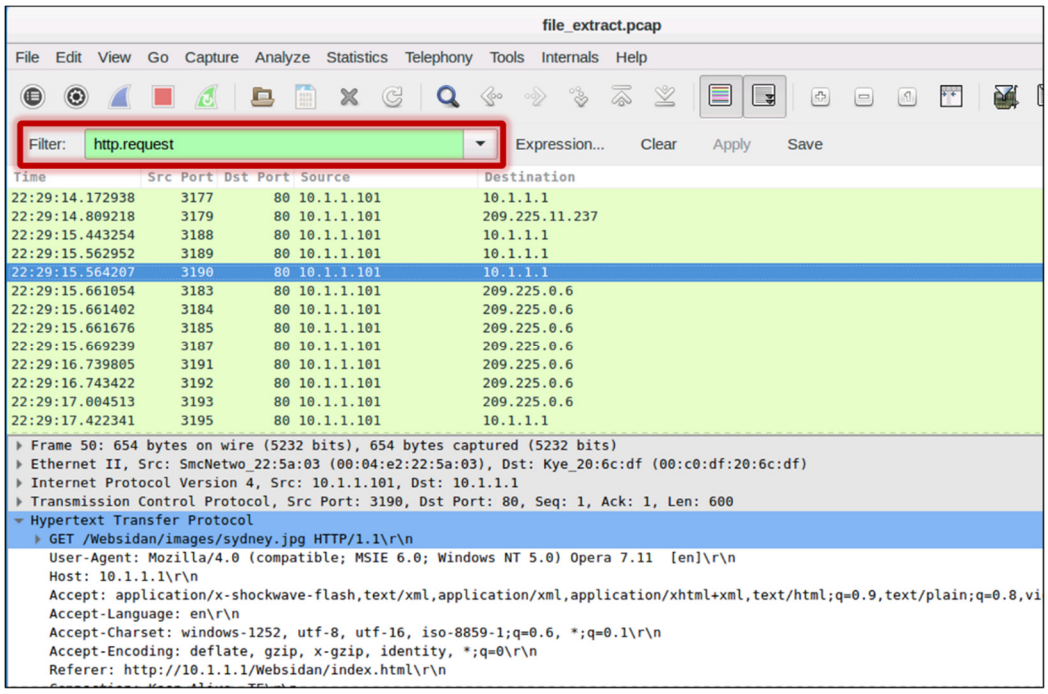
1.1 On the Main Menu, click **File**, then click **Open**.

1.2 Navigate to the folder on the Desktop named **Captures**.

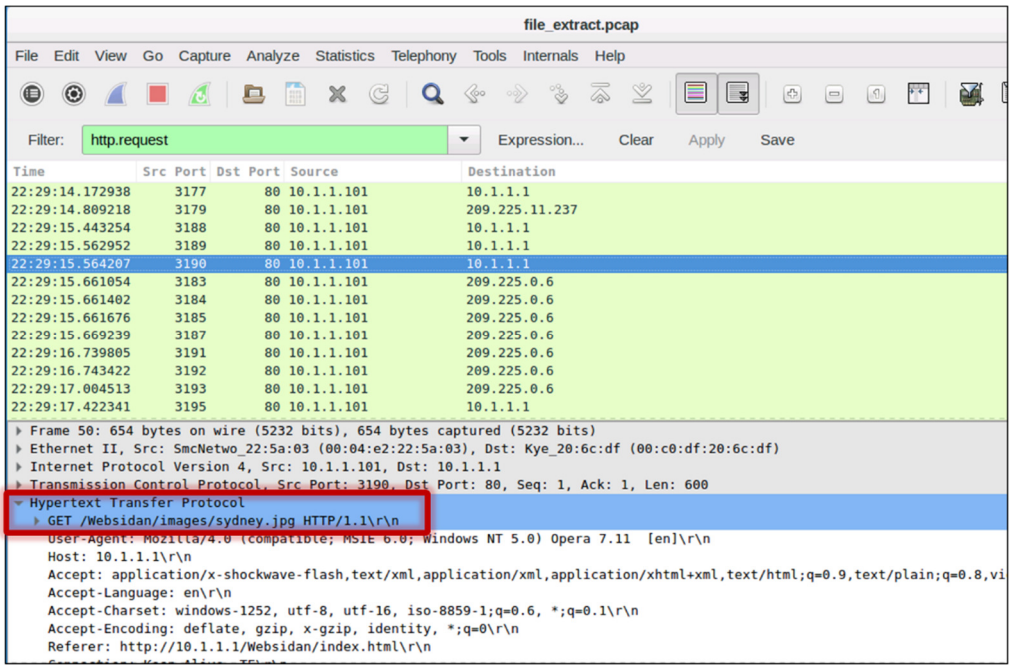
1.3 Open the file named `file_extract.pcap`.

In the Filter Toolbar, we are going to search for http requests using the filter `http.request`. This will filter out all traffic except `HTTP GET` and `HTTP POST` requests so we can see what information was obtained from the web server.

1.4 Enter `http.request` in the Filter Toolbar.



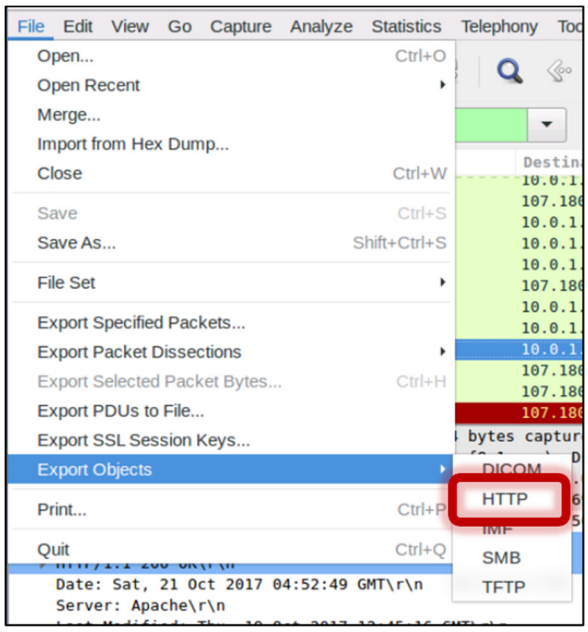
If we look in the packet list, we can see that several jpg files were downloaded. Now that we know we are looking for image files, there are a couple of methods for extracting these files.



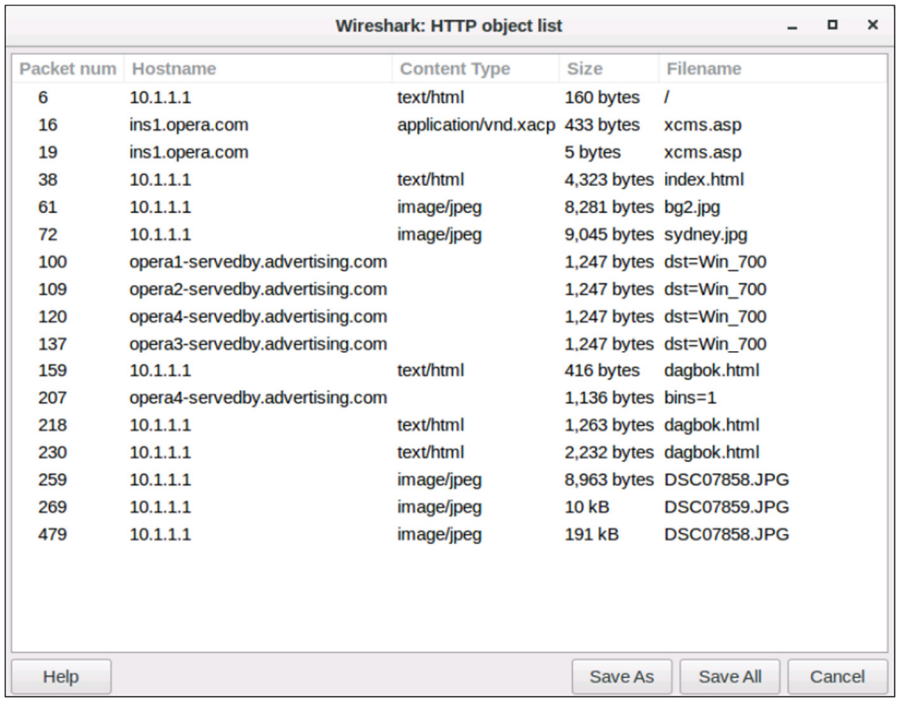
Extracting Files from Wireshark

2.0 Using the Extraction Menu

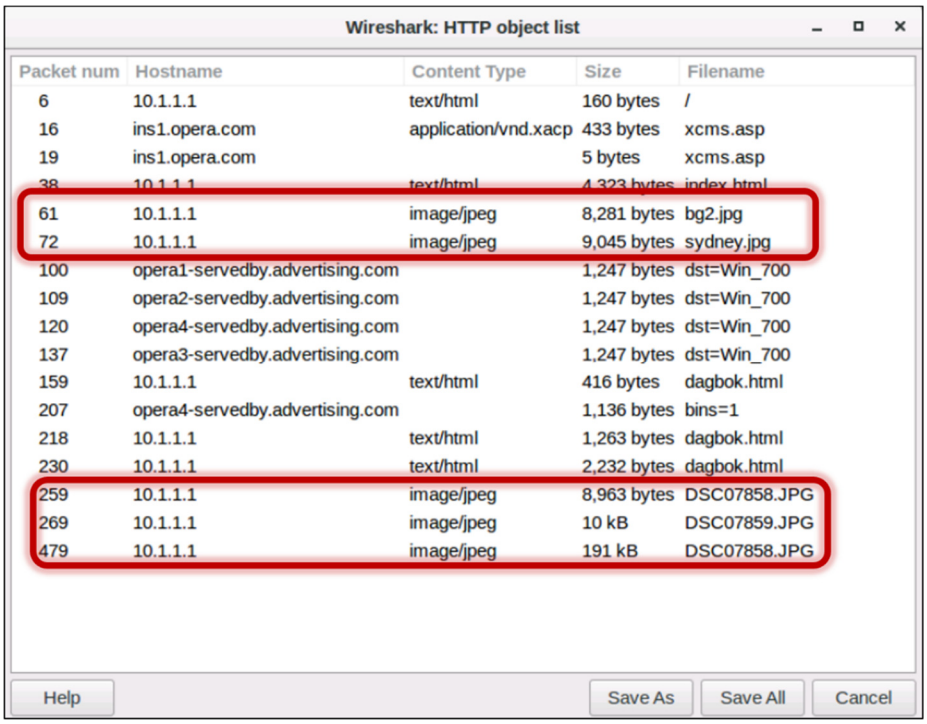
2.1. Using Wireshark, we can extract the file from the TCP stream. In Wireshark, click **File**, then move your mouse over **Export Objects**, and click **HTTP**.



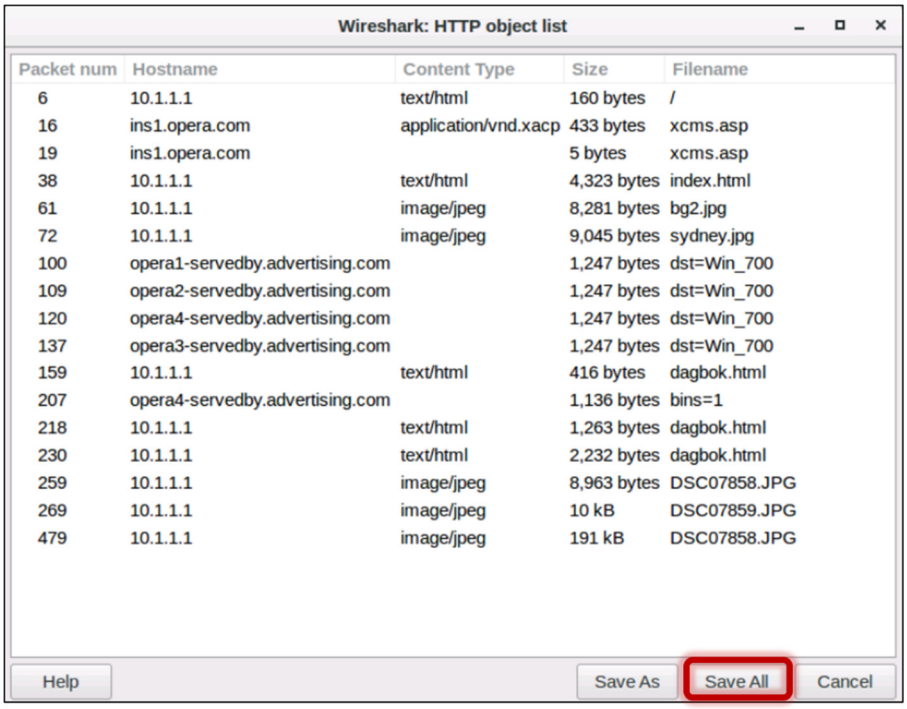
2.2 This will produce an **HTTP Object List**.



2.3 We can see that there are multiple .jpg files in the traffic.



2.4 Because we cannot choose to save a specific file type, we will use the **Save All** command to capture all the files, and place them in **Pictures** folder.



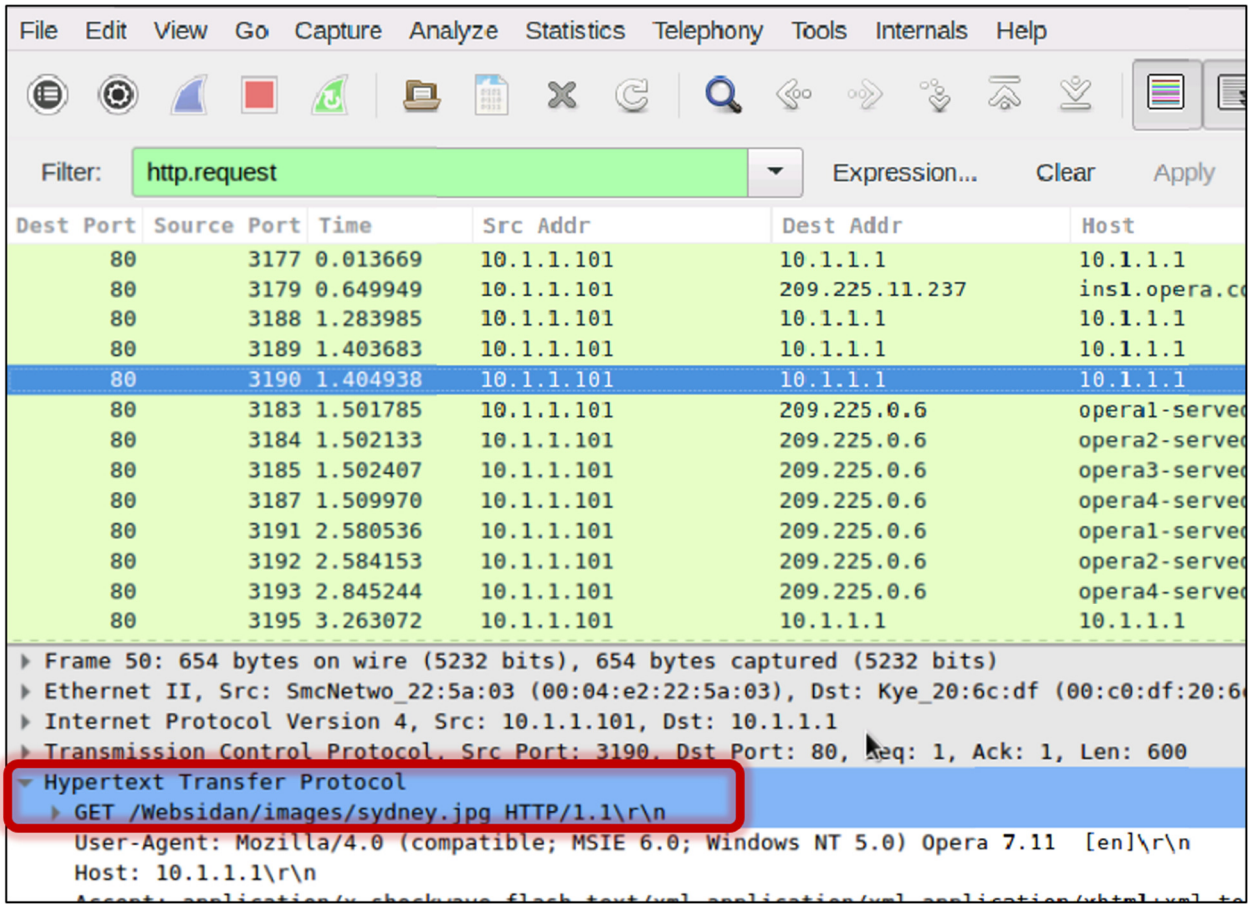
2.5 Wireshark will give you the chance to create a folder, which we named Images here. (We will analyze these files later).

3.0 Following the TCP Stream

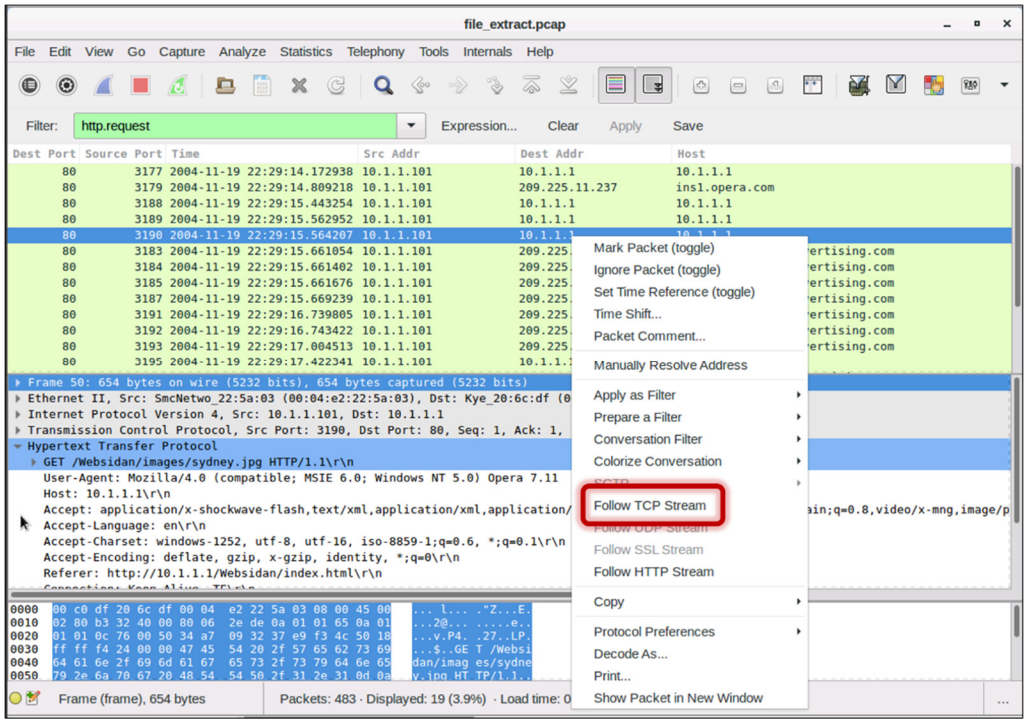
NOTE: For this method we are only going to extract the sydney.jpg file.

3.1 In the Filter Toolbar, type `http.request` again.

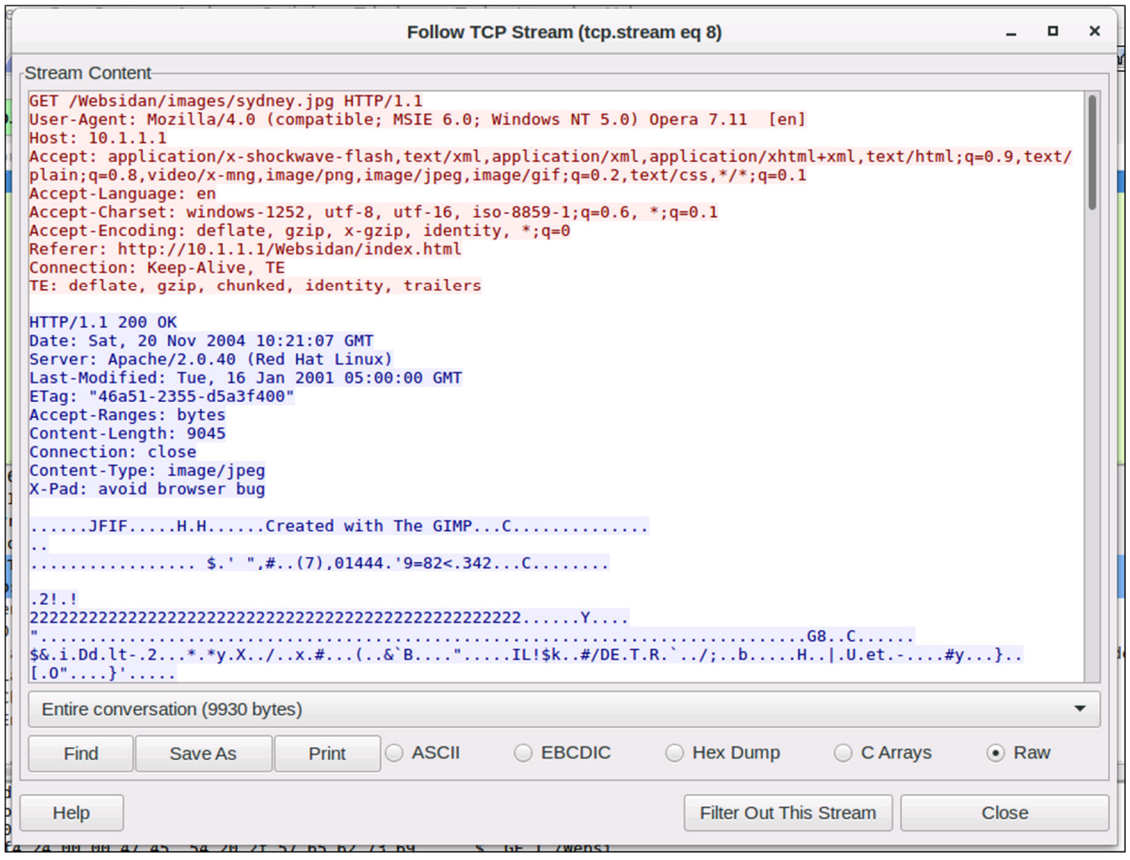
3.2 Look for the GET request for the sydney.jpg file and click on it.



3.3 Right-click the **GET** request and select **Follow TCP Stream**.

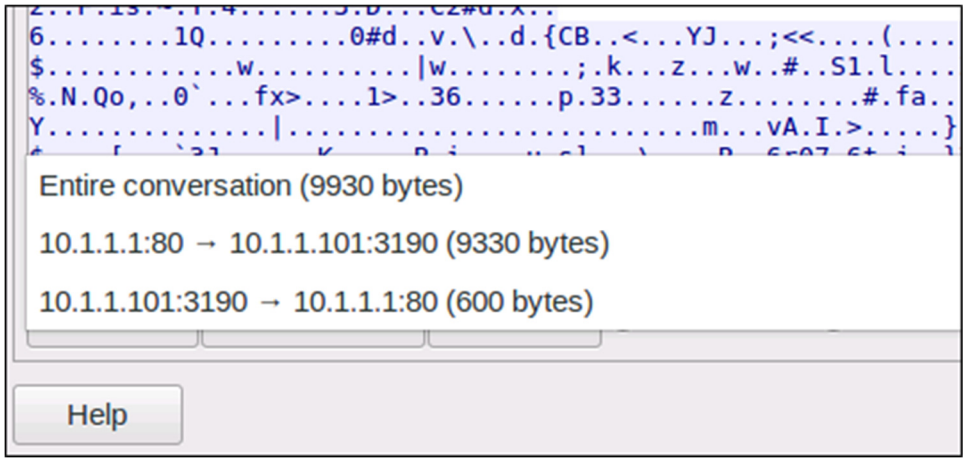


NOTE: The stream will be in red and blue text. The red text is from the source machine and the blue text is from the destination machine.

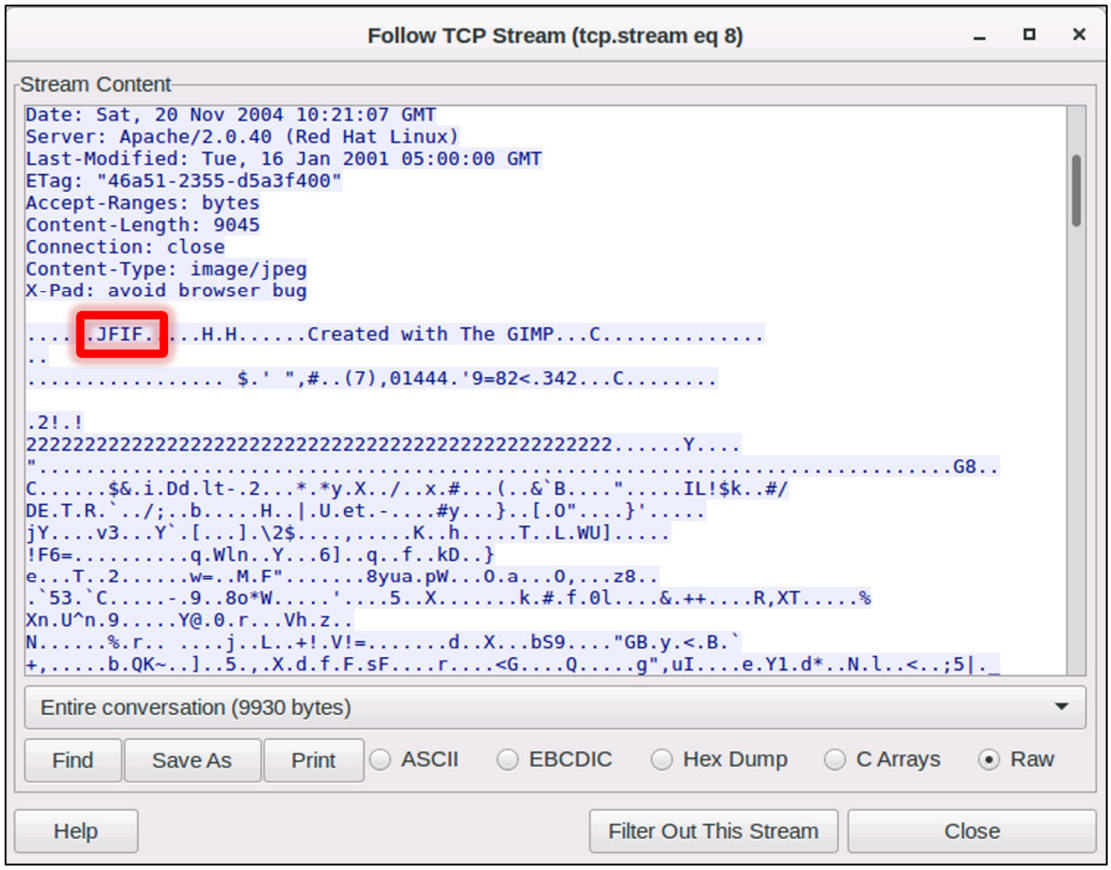


3.4 In the drop down menu at the bottom, change the conversation from 'Entire Conversation (9930 bytes)' to '10.1.1.1:80 to 10.1.1.101:3190 (9330 bytes)'.

3.5 This will allow us to see the data only from the web server to the host.

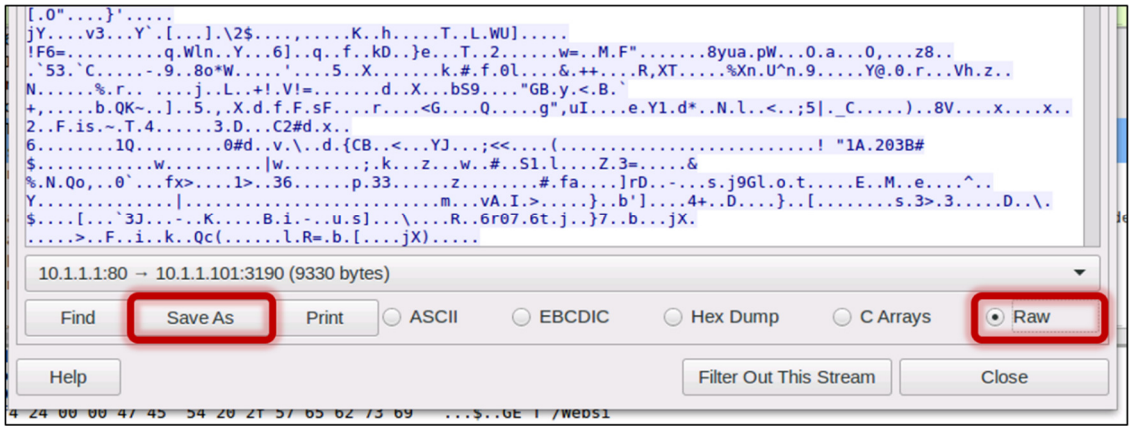


Note: After the header information, you will see a line that contains the file information. The 'JFIF' is the file type and we need that to search for the magic number.



3.6 In the menu at the bottom of the TCP Stream window, change the data from 'ASCII' to 'Raw'. This will allow us to view the raw data.

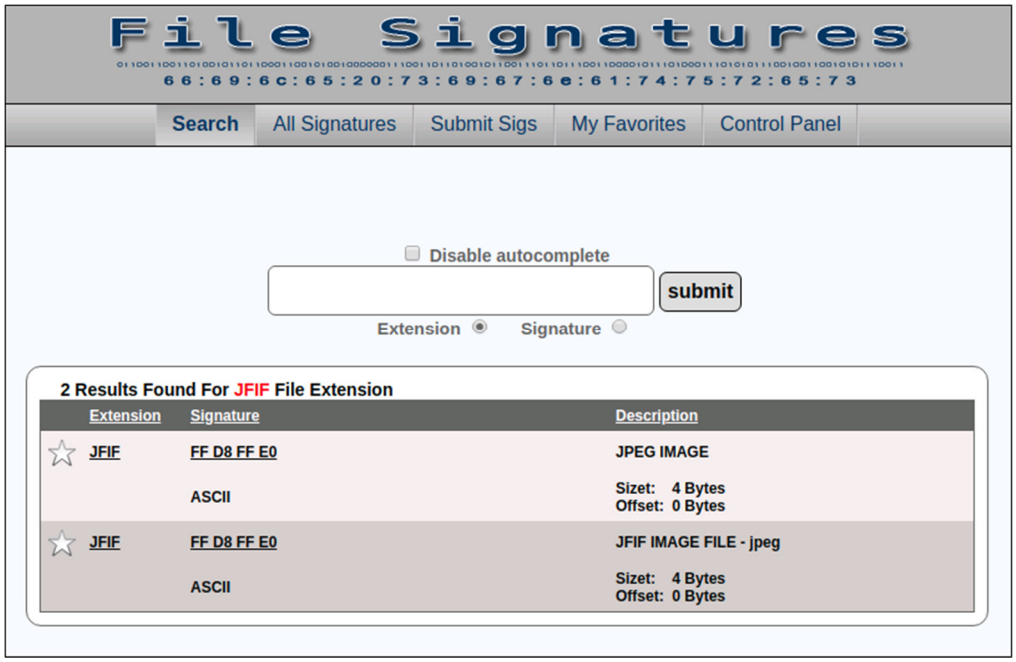
3.7 Click **Save As** and save the file in the **Captures** folder, as Sydney.jpg.



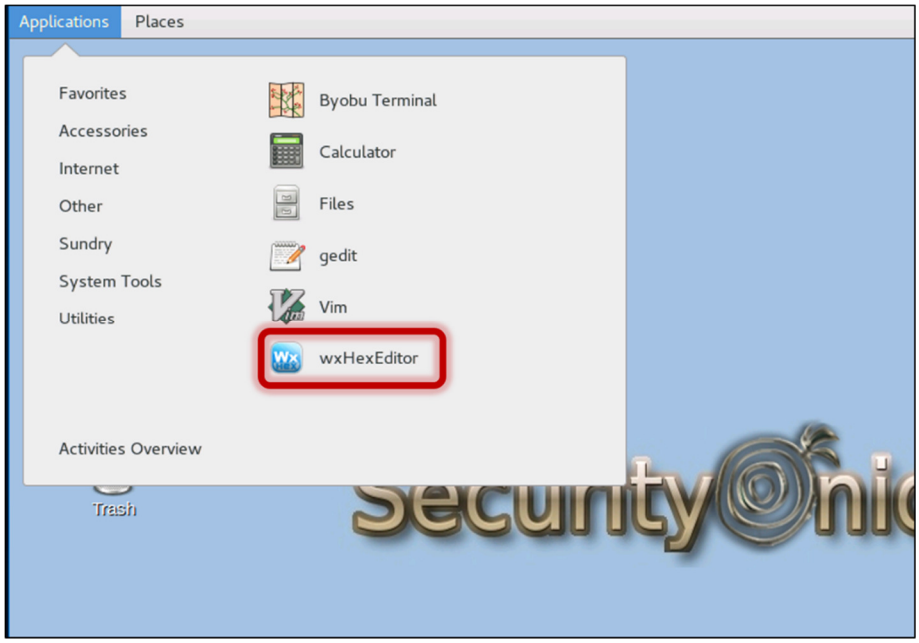
3.8 Close the TCP stream window.

3.9 Open Chromium Web Browser (click **Applications**, move your mouse over **Internet**, and click **Chromium Web Browser**). Then, click on the **File Signature Database** bookmark in the toolbar. This is a well maintained list of HEX file signatures (aka "magic numbers").

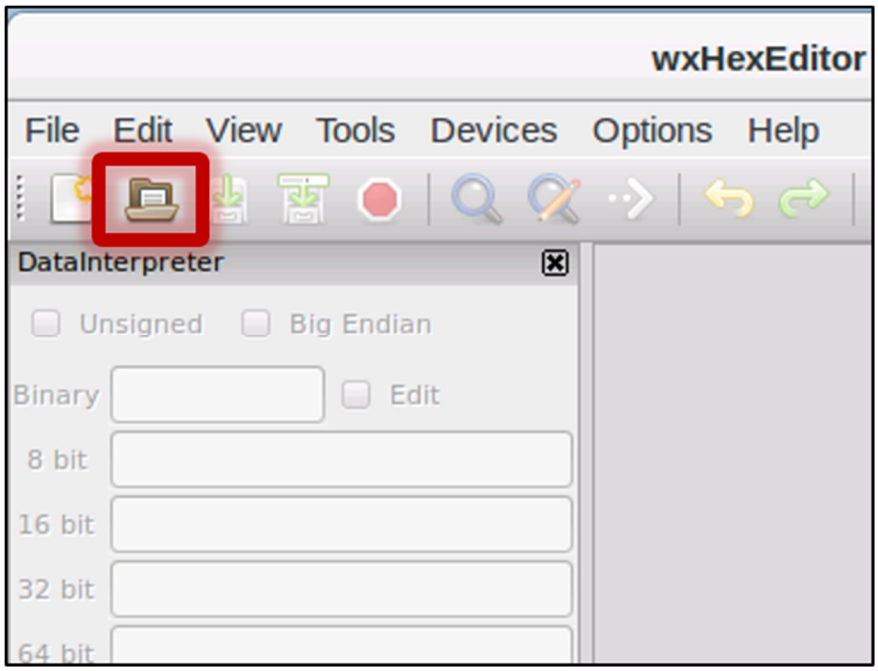
3.10 We know the file is a JFIF so we can search the webpage for 'JFIF'. Enter **JFIF** in the **Search** and click **Submit** to view the results. The magic number we will use is `FF D8 FF E0`



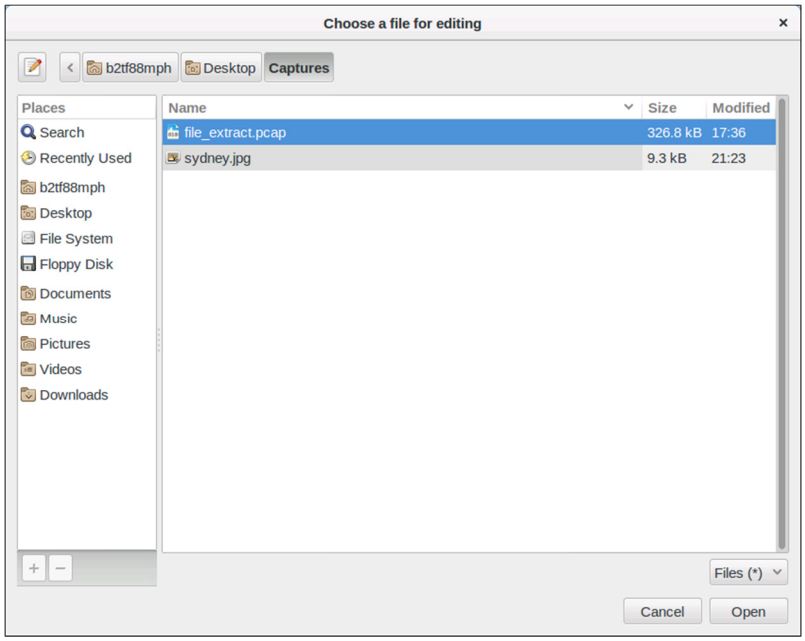
3.11 Open the raw dump file using wxHexEditor. Click on **Applications**, then move your mouse over **Accessories**, then click **wxHexEditor**.



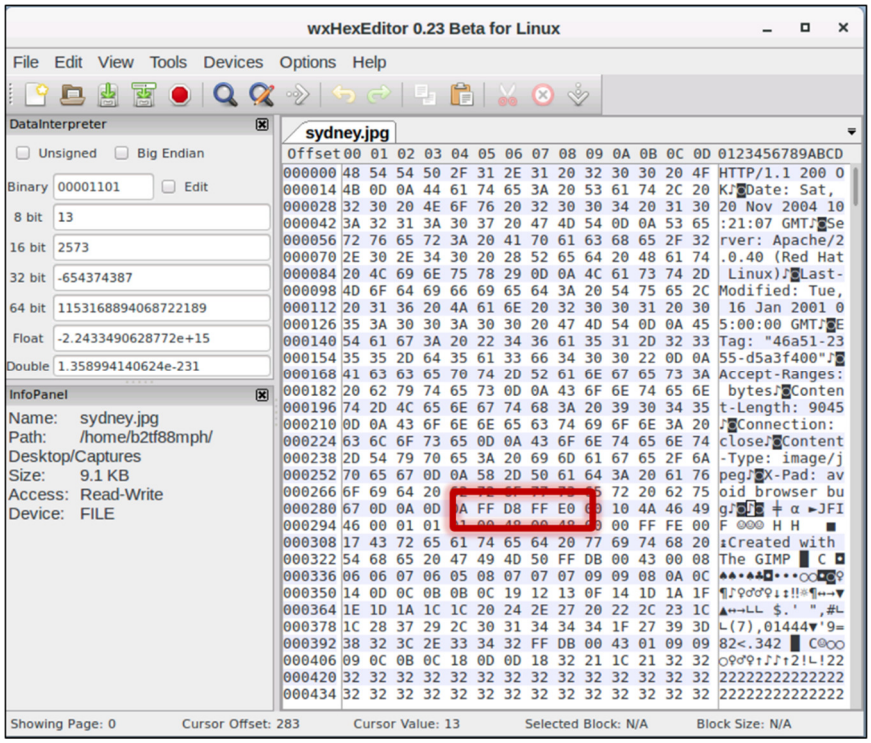
3.12 Click the folder icon.



3.13 Navigate to the file you extracted from the PCAP in the Captures folder on the Desktop.

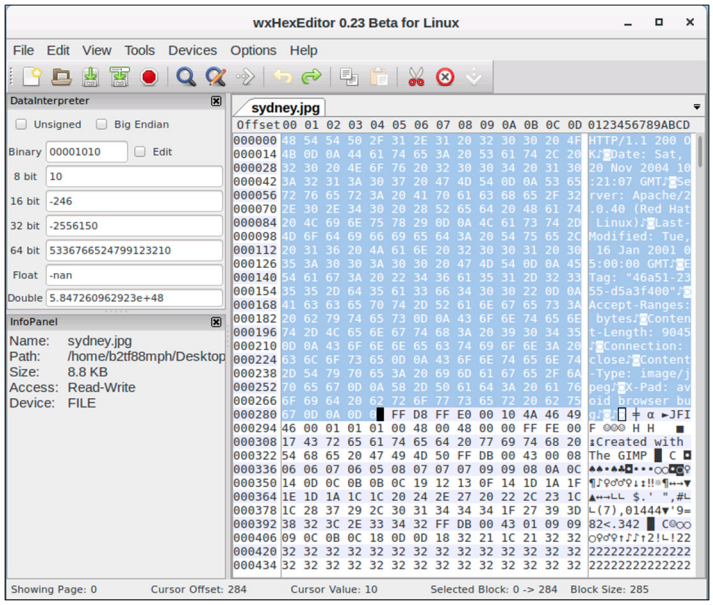


3.14 Now we look for the magic number `FF D8 FF E0`

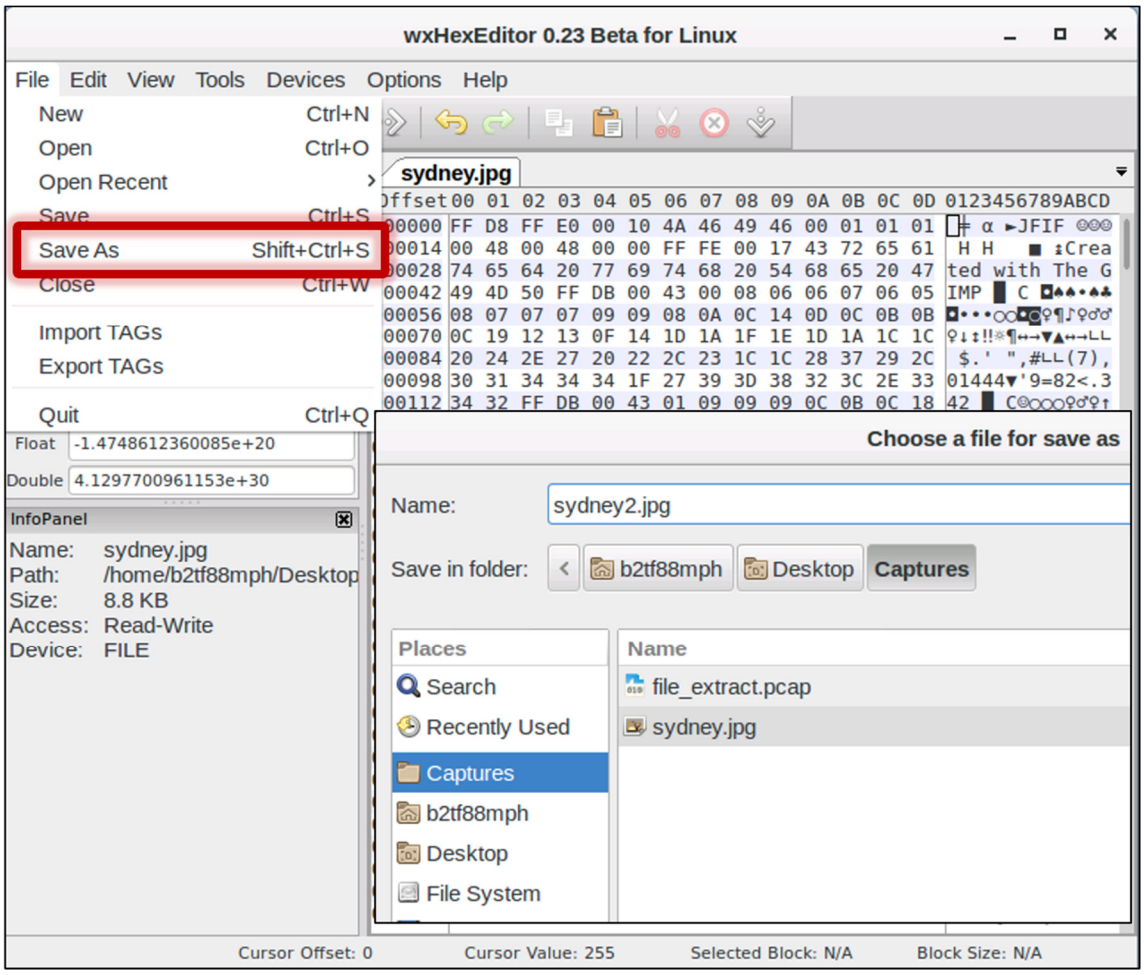


3.15 Delete all HEX prior to the magic number.

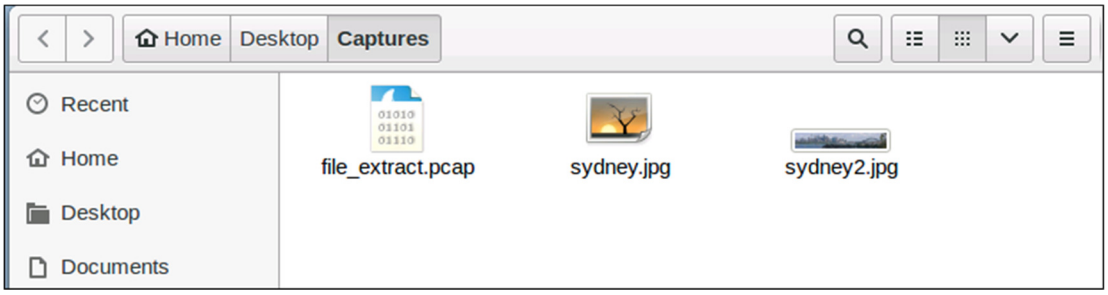
You can do this by selecting the first characters at `00` x `000000`and dragging it to the first two digits of the magic number.



3.16 Save the file as a new jpg file.



As you can see, the file is now a .jpg image instead of a broken file.



3.17 You can use the image viewer to open the file if you would like.

Great job, you have completed LAB006!

Thank You, you may now close this module.