Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Windows Dead Analysis

DFIR-06-L3
Image Carving

Lab Objective

Understand how to access hidden data and retrieve it using file carving techniques.

Lab Mission

Extract hidden information from an image file using **Binwalk** and a hex editor.

Lab Duration

20–30 minutes

Requirements

- Basic understanding of file carving

Resources

- Environment & Tools
    - VirtualBox
        - Windows 10
            - ***Pscp.exe***
        - SIFT Workstation
- Extra Lab Files
    - ***Cat.jpg***
    - ***HxDSetup.exe***
    - **PuTTY**
- Extra Links
    - File size calculator: ***https://toolstud.io/photo/filesize.php***
    - File signature list: ***https://en.wikipedia.org/wiki/List_of_file_signatures***

Textbook References

- Chapter 6: Windows Dead Analysis
    - Section 5: File Carving

Lab Task: Investigate an Image and Find Hidden Data

You will need to employ your investigation skills for this task. Investigate the provided image and find the data hidden within it.

1. Make sure Windows 10 and SIFT have access to the internet by using two adapters, one for the internal network and one for the internet.

2. On the Windows 10 VM, go to ***https://toolstud.io/photo/filesize.php*** to examine the ***Cat.jpg*** image size and its file size. Compare the file size to its estimation on the website. You can see the image size and file size in the properties of the file.

3. Install **PuTTY** on the Windows 10 machine to transfer the document to the SIFT workstation via SSH on port 22.

4. Start the SSH service on the SIFT workstation with ***sudo service ssh start*** to transfer the ***Cat.jpg*** file to SIFT using ***PSCP*** for examination. Make sure you are in the proper directory on the Windows machine before running the command ***"C:\Program Files\PuTTY\pscp.exe" -P 22 Cat.jpg sansforensics@[Ip]:/home/sansforensics/Desktop***.

5. On the SIFT machine, run ***apt update*** and then ***sudo apt-get install -y binwalk***.

   Note: You may need to run ***sudo apt install -y binwalk --fix-missing***.

6. Examine ***Cat.jpg*** with the ***binwalk*** command.

   Note: The result confirms multiple images are hidden within the JPEG; also, note the hexadecimals.

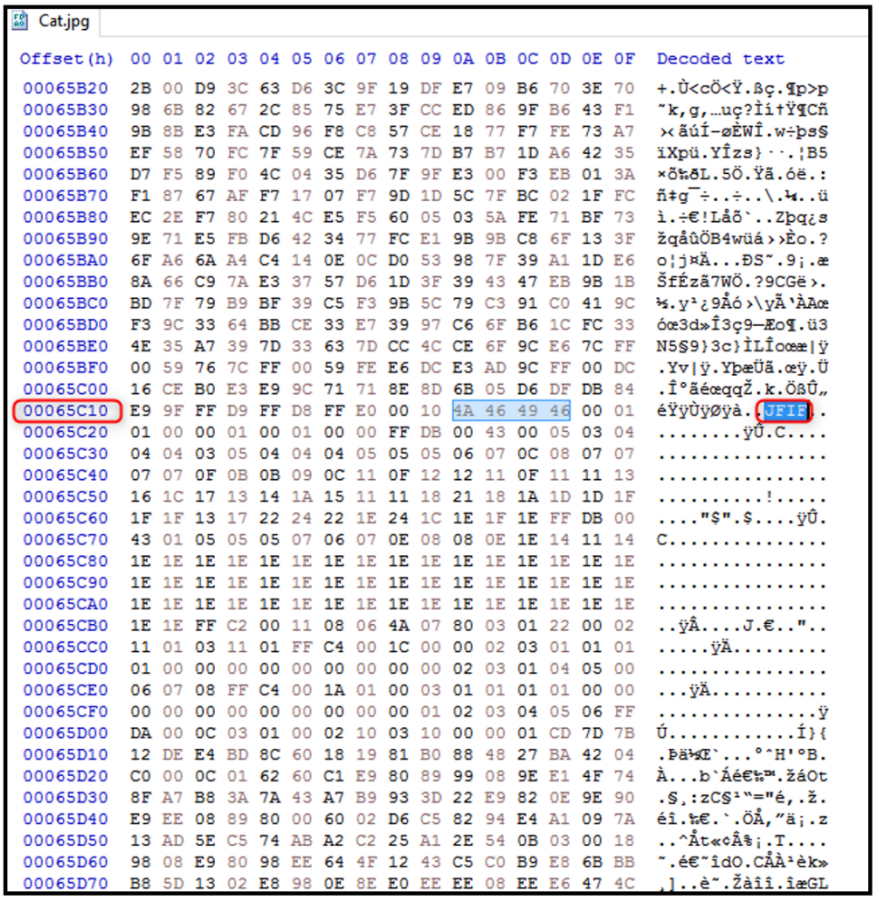
```
sansforensics@siftworkstation: ~/Desktop
$ binwalk Cat.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
416788        0x65C14         JPEG image data, JFIF standard 1.01
998740        0xF3D54         JPEG image data, JFIF standard 1.01

sansforensics@siftworkstation: ~/Desktop
$
```

7. Install **HxD** to examine ***Cat.jpg*** and extract the hidden images.

8. Once you have **HxD** running, drag and drop ***Cat.jpg*** into **HxD**.

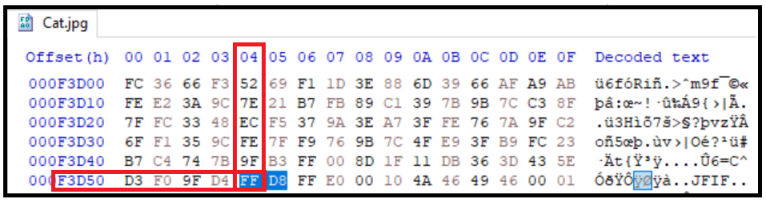
9 Use the hexadecimals found on the SIFT machine to locate the **65C14** offset.

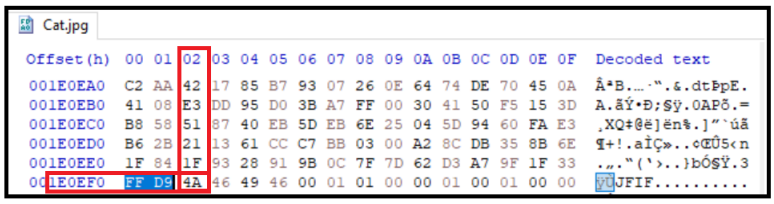
Note: There is evidence of a JPEG File Interchange Format (JFIF). This may hint at the existence of an embedded data stream. At this stage, a researcher may conclude there are more images hidden in the ***Cat.jpg*** file.



10 Go to the Windows Calculator and use the Programmer Calculator to determine the byte range of the hidden images.

Note: The beginning of a JPEG is **FF D9** and the end of a JPEG is **FF D8 FF.**

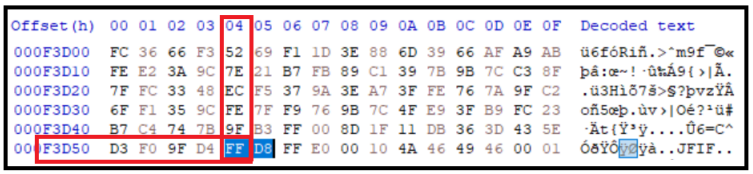


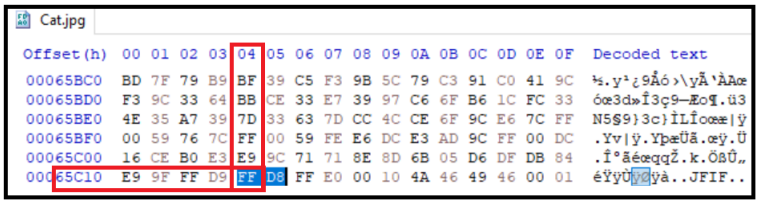


11 Make sure the hex is highlighted to use it properly. You will be subtracting **1E0EF2** by **F3D54**. This should give the result **ED19E**.

12 Select the beginning of the image **F3D4**, then select length and put **ED19E**, the length found when subtracting the two hexadecimal numbers. This will highlight the image, which you should copy. Create a new hex file, paste the copied hex, and save the document as ***carved1.jpg***.

13 To find the other hidden JPEG, you need to find the beginning and end of the image. Perform a search again for the **FF D8** values. Subtract the values again to get the highlighted image, which you should copy and paste to new a hex document. Save the file as ***carved2.jpg***.





14 Switch back to **text-string** in the ***Ctrl+F*** search to further investigate the provided ***Cat.jpg*** file for more information using a string search in **HxD**. Search for the fourth JFIF string in the documented image. Note that the fourth is incomplete compared to the other files.

15 Copy from the JFIF to the bottom of the hex document. Paste the copied hex to a new hex file and add the beginning hex to the file and then save as ***carved3.jpg***. Compared to the other JFIFs, you should note that what is missing is **FF D8 FF E0 00 10**.

16 You have found all the hidden images within ***Cat.jpg***.

Hints

Lab Task: Investigate an Image and Find Hidden Data

- Use the machine's network options to configure the network adapter for internet access.
- Inspect the image properties to view its dimensions.
- Start the SSH service in SIFT.
- Ensure the SIFT and Windows 10 machines are on the same network.
- Use ***"C:\Program Files\PuTTY\pscp.exe" -P 22 Cat.jpg sansforensics@[SIFT Box IP]:/home/sansforensics/Desktop*** to transfer files with PSCP.
- Use APT Package Manager to install **Binwalk**.
- The **Binwalk** results are locations of potential data to be extracted.
- Follow the basic installation of **HxD**.
- Import the ***.jpg*** file to the editor.
- Look for JFIF, which is interchangeable with JPEG.
- Use the Windows Calculator to calculate the length of the files by subtracting the hex values.
- To select the correct range, right-click the start position and then click to select a block.
- Copy the selected content and paste it in a new file to be saved.
- Use **HxD**'s string search capability to search for additional images.
- Use all methods learned in the file carving section, calculate the image size, and extract it.
- Note the patterns of the images to fill in the missing hex for the last image.
- You should have a total of four images.