COMP-5350

Digital Forensics

FROM: Ally Bennett, Megan Crews, & Jacob Howard

TO: Dr. Jason Cuneo & Jiaxiang Ren

DUE DATE: 12/3/21

Project 2

Overview

The goal of this project and for our team was to create a script that was capable of recovering files from a disk in ".dd" format. After examining the disk image provided, we discovered it was too large to recover the files manually, so our team developed a Python script to find the number of files inside of the disk image. The python script also found the starting byte offsets and ending byte offsets of each file and displayed the information in the output. We used the signatures of each type of file that could be on the disk image and their footers to locate them and used the file size information to find the starting and ending offsets of each. We continued to do this for each file found on the disk image. After everything for each file was found, we then did a sha256 hash for every file. After carefully going through the script and making corrections where needed, we found there to be 13 files on the Project2.dd file. When all files were recovered and all information was given in the output of the python script, we had the script put everything into a directory called RecoveredFiles.

To run the python script in Linux, you must open the script location with the included ".dd" file in terminal, and type "*python3 filename.py filename.dd*", where *filename* is the name of the file.

Analysis Techniques

Firstly, our goal was to find a way to write a python script to find the information we needed on the disk image that was given to us. We knew we had to somehow write a script that took the disk image as an input and searched through it to find all the files on the disk. We also knew that while it was looking for all the files, that we needed certain information about all the files like where each file started and ended. Along with that information we also needed the sha256 of each file and even though it was not asked for we also decided to find the size of each file.

Our team decided to try and start our code by finding the files using their file types and their footers. Each file has its own signature and its own file type, so by using these we could easily find each file. Our team put at the beginning of the code an error message if you tried to run the code wrong or typed in something wrong it gives you a warning that says "Missing disk file. Format python 3 RecoveryFile.py File.dd". This error message allows you to retry and input the right things so the code will run properly.

Next, we used if statements inside of a while statement to find the starting offset, the ending offset, and to generate the sha256 of each file. In order to find those three things for each file, we used an if statement that located a certain file like this statement, "if f == "AVI"". That if statement allows the code to go through the disk image and find the files with the signatures "AVI" and to generate its starting offset, ending offset, and sha256. We continued to do this for every file inside the disk image.

Lastly, after we found everything, we needed from each file we made a spot in the code to make a new directory and to move all recovered files into the directory. Not only were the files moved into that directory, but also all the information we needed was moved into it as well. You can find all that information in a directory called RecoveredFiles. Our code also creates a texted file to put all the information into as well, and it is called ConsolOutput.txt.

Recovery

During our recovery process, we found a total of 13 files on the disk drive. The files produced are shown below in *Table 1*, labeled *Files Recovered*. The table will describe each file found as there are large pdf files and media files that cannot be displayed on this report. *Table 2*, labeled *Script Output*, shows the console output from the script. Our script also creates a text file of the console output and stores it in the same directory as the script.

Files Recovered			
File #	**Name**	**Type**	**Description**
1	File1	mpg	**Video:** Space Video
2	File2	pdf	**Book:** A Tale of Two Cities by Charles Dickens
3	File3	pdf	**Book:** Great Expectations by Charles Dickens
4	File4	docx	**Word File:** Displays encoded message in base58 and an image from the movie "A Christmas Story".
5	File5	avi	**Video:** Video **recording** a Black Bear
6	File6	avi	**Video:** The ocean with a small rock-island

7	File7	png	**Photo:** Dice
8	File8	png	**Photo:** Encoded Message
9	File9	jpg	**Photo:** Auburn logo
10	File10	jpg	**Photo:** Iron Man
11	File11	gif	**Photo:** Animated Mandelbrot
12	File12	gif	**Photo:** Animated Minion
13	File13	bmp	**Photo:** Flowers

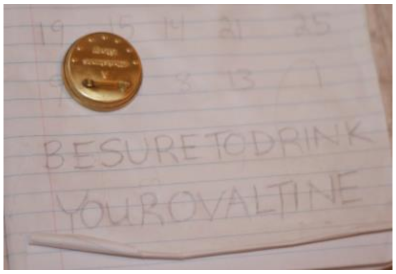
Table 1

<table>
<tr><th colspan="5">Script Output</th></tr>
<tr><td colspan="5">The disk image contains 13 files</td></tr>
<tr><th>FileName</th><th>FileStart</th><th>FileEnd</th><th>FileSize</th><th>SHA256</th></tr>
<tr><td>file1.mpg</td><td>47960064</td><td>50002092</td><td>2042028</td><td>c9ed8592d0b31b24e5a7286469497cd817e7c32dd6a9347891db8c27c26d0153</td></tr>
<tr><td>file2.pdf</td><td>29233152</td><td>31294603</td><td>2061451</td><td>d1531276564ac6785944f2110dcc48e45a1211f4693a947808217cc215913354</td></tr>
<tr><td>file3.pdf</td><td>31703040</td><td>35305456</td><td>3602416</td><td>027927506bd47335d8c3060c1b92bb18002a9576f0355eabaab834e7552e6aad</td></tr>
<tr><td>file4.docx</td><td>47820800</td><td>47957431</td><td>136631</td><td>0b6793b6beade3d5cf5ed4dfd2fa8e2ab76bd6a98e02f88fce5ce794cabd0b88</td></tr>
<tr><td>file5.avi</td><td>00245760</td><td>29231744</td><td>28985984</td><td>1e424df16136eb568113dfeaec0142fedbdef76838d3c6b995ba4ce4a5a7df16</td></tr>
<tr><td>file6.avi</td><td>37908480</td><td>47817572</td><td>9909092</td><td>145d0a0e4870e02b0d80432c4b945add0c8b5178705a8ef21816d84a6ecd8aa6</td></tr>
<tr><td>file7.png</td><td>31297536</td><td>31525499</td><td>227963</td><td>3967b4fc85eca8a835cc5c69800362a7c4c5050abe3e36260251edc63eba518f</td></tr>
<tr><td>file8.png</td><td>47824425</td><td>47948428</td><td>124003</td><td>79766e0f0c031cf727a5488e40113941202fafa25b24f72b1488db1f699226c2</td></tr>
<tr><td>file9.jpg</td><td>00229376</td><td>00241749</td><td>12373</td><td>59e0ec78f30c50db44d24a413ca1cccbd7ef5910cad4d3cf0e4753095725ec94</td></tr>
<tr><td>file10.jpg</td><td>34897920</td><td>34920239</td><td>22319</td><td>bde9e54f4e1ec3b6ab8d439aa64eef33216880685f8a4621100533397d114bf9</td></tr>
<tr><td>file11.gif</td><td>34922496</td><td>37575141</td><td>2652645</td><td>c3c82461c8d7cd3974a82967d5c6cf18449e1b373c8123b01508be277df725e4</td></tr>
<tr><td>file12.gif</td><td>37576704</td><td>37904878</td><td>328174</td><td>8869dd5fcb077005be3195028db6fe58938c4ec2786a5ff7e818d2f5411ded52</td></tr>
<tr><td>file13.bmp</td><td>31621120</td><td>31699062</td><td>77942</td><td>e03847846808d152d5ecbc9e4477eee28d92e4930a5c0db4bffda4d9b7a27dfc</td></tr>
<tr><td colspan="5">Files stored in /home/sansforensics/Documents/Project2/RecoveredFiles</td></tr>
</table>

Table 2

Below are the images we found when running our script on the disk drive. Each image is labeled in the order that the file was found and recovered.

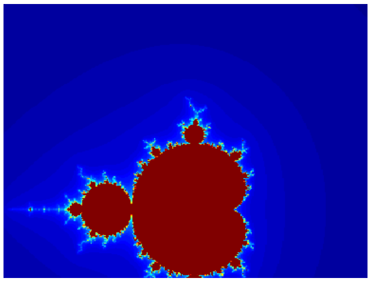
File 7



File 8

File 9

File 10



Fille 11

File 12

File 13

Conclusion

A total of 13 files were recovered from the disk image and stored in our RecoveredFiles directory. The python script our team developed was successful in finding files, recovering them, and printing out information about each file.