COMP-5350

Digital Forensics

FROM: Jacob Howard, Ally Bennett, & Megan Crews

TO: Dr. Jason Cuneo & Jiaxiang Ren

DUE DATE: 10/15/21

Project1

# **Overview**

This project was designed to help us understand digital forensics and data recovery. We went through multiple senearious on how to recover deleted/modified files on different drive formats.

# **Part 1: Technical Analysis**

Firstly, our goal was to find out how many partitions were on the drive given to us and what the partition types were. We can easily find this out by going to our fold containing the disk image through terminal and typing in the command “*fdisk -l Project1.dd*”. This command will list all the partitons and types on the image.

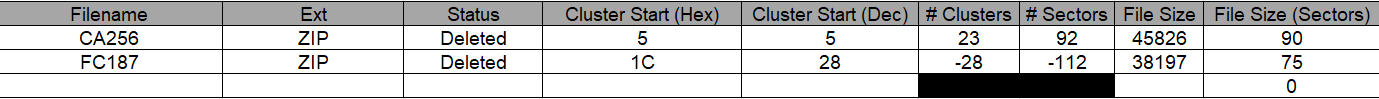
After using the command, it was found that there were 4 partitons; 1 FAT16 partion, 1 FAT32 partiton, and 2 NTSF Partitions. Once we knew the types of drive paritions, we could hexdump at specific partition locations to read certain data off the drives.

For the first FAT16 partition, we saw that there had been 2 deleted files. This information was found in the file allocation table. By collecting data from the FAT, as seen below in Table 1, we were able to find the root directory location and data area location where the deleted files were stored. We were then able ultimately find the File locations of the 2 deleted files and use the “dd” command to copy the data. Two password protected zip files were found containing .jpg files. The images can be seen below in Image 1 and Image 2 while Table 2 shows all relative data for the partiton. The password used to unzip the files was found in a file in the first NTFS partition.

Application, table, Excel

Description automatically generated

*Table 1*

**

*A picture containing table

Description automatically generated*

*Table 2*

**

*Image 1*

**

*Image 2*

Next, we dove into the first NTFS partition. This partition contained 2 deleted files. Using Active Disk Editor, we were able to pull the information we needed about where the files started and ended, so that we could copy them into our vm. The tables below show all the data collected, the Filenames and data, and the commands we used in the terminal to retrieve these files. The files contained an email with a password for unzipping the previously recovered zip files and an Encoding pdf file for encoding and decoding messages. The pdf was used to decode messages in from files in the second NTFS partition.

Table

Description automatically generated

*General NTFS Values*

Table

Description automatically generated

*NTFS Data Structure Locations*

---------------------------------------------------------------------------------------------------------------------

Info For files: Top row is Email.docx info and bottom row is for Encoding.pdf

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

---------------------------------------------------------------------------------------------------------------------

Graphical user interface, application, Word

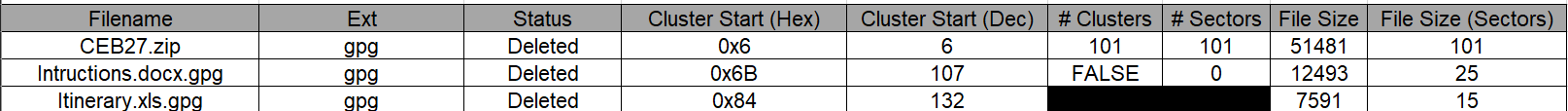
Description automatically generated

*Commands used to Recover Files*

Next, we went to the location of the FAT32 and reading data using active disk editor, we were able to find that there were 3 deleted files. All files were incripted in .gpg formant with a password. The data tables are shown below with all values for the FAT32 partition. We were able to use the dd command to recover these files. For file 1, the command was “dd if=Project1.dd of=CEB27.zip.gpg bs=512 skip=407431 count=101”. We just make the skip=Start and the count=File Length for all files on the drive. The Itinerary file contained the dates and times of a team for a heist and can be seen below.

Table

Description automatically generated



Graphical user interface

Description automatically generated with medium confidence

*Disk/File Information*

Table

Description automatically generated

*Itinerary*

Lastly, we dove into the last NTFS file. This was probaboly the most difficult partition to recover data, because even though we were able to see 3 files on the drive, the last 2 files were actually stored in the MFT, making it more difficult to find location and files size so that one could retreieve the data. We used the ordinary dd command for the first file, but for the other 2 files, we had to slightly alter it so that we could retrieve the files. The data tables and commands are shown below for the second NTFS partition. The Mystery.txt file contrained a hex format, that once decoded, gave the password to decript the previous .gpg files that were recovered. The ECC424 file contained a recon.txt file that had an encoded message in base64. The FC187.zip contained a location.jpg image, which is the assumed location of the heist.

Table

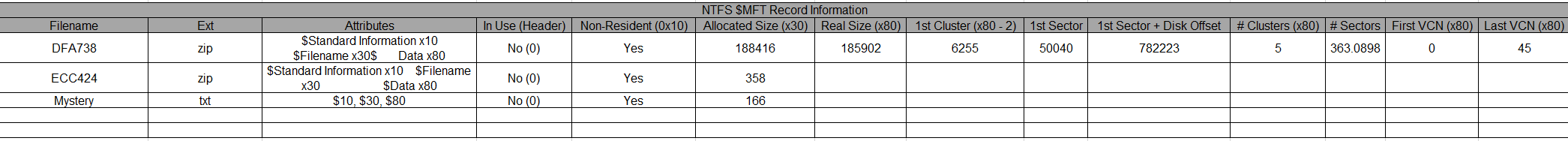
Description automatically generated

*Generic Values*

Table

Description automatically generated

*NTFS Data Structure Locations*



*NTFS $MFT Record Information*

Table

Description automatically generated with low confidence

*Commands*

A large brick building with towers

Description automatically generated with low confidence

*Location (from FC187.zip)*

# **Part 2: Operational Analysis**

In part 2, we were asked questions about the contents of the drives. The first question asked what methods were used to hide the files on the disk. The method for all files besides the last 2 files recovered in the second NTFS partion was file deletion. Since the files were marked as deleted but not overwriten, we were able to recover all those files. The second method, which the last two files in the NTFS partition used, was file manipulation to make it more difficult to recover the data.

The tools that were use to hide the data once recovered were encryption and password protection. The users seemed to want these files protected because their objective seemed to be a heist. They seemed to be interested in stealing from a specific location. One of the Base64 encoded messages, once decoded, gave a location as well. The location seemed to be the Smithsoniam Museum. The file this location was found, was from the Recon.txt file recovered and the exact decoded message is ”https://www.google.com/maps/d/u/0/viewer?msa=0&ie=UTF8&t=h&ll=38.89028798326893%2C-77.0293097175214&mid=1JEkfH9bJtMKrVCMHrKGPP\_QmMys&z=17”