AUBURN

UNIVERSITY

Digital Forensics: Project 1

Rachel Sowada, Haden Stuart, Lucia Bajo

October 8, 2020

Executive Summary

A laptop has been collected from the accused offender during a forensics investigation and our digital forensic analysts have obtained a complete copy of its memory. We needed to determine if there was enough evidence on it to prove any criminal activity. After the disk was copied, the next step was determining how many partitions there were, in this case there were 3, the first and last were FAT16 partitions and the second was a NTFS partition.

Examining these partitions consisted of checking the master boot record to find starting sectors and FAT/NTFS boot sectors. We pulled valuable information about the partitions from the boot sectors and eventually found the start of the files. From there we were able to use the recovery command to retrieve the files.

The accused offenders utilized multiple data hiding methods to encrypt their data, including spreading files across different file systems, deletion of files, password protected zip files, and file encryption. They had password protected ZIP files, GPG encryption, and hex encryption, which they used to encrypt the key. With the information and files we decrypted, we concluded that they were planning to rob the Smithsonian Institute to steal the Hope Diamond necklace.

Table of Contents

Contents

List of Figures

List of Tables

1 Introduction

The focus of this assignment is to properly analyze FAT16 and NTFS partitions in order to appropriately recover data from each.

2 Problem Description

Given a disk image collected from a laptop during a forensic investigation, we must critically evaluate and analyze the digital artifacts on it. The objective is to recover data in order to determine if there is proof of criminal activity.

3 Analysis Techniques

In order to determine if any criminal activity has taken place, our digital forensic analysts pulled a complete copy of the memory on the laptop of the accused offender. The following section describes what methods were used to pull the data off of the accused's laptop.
The very first step done after copying the entire disk was to determine how disk partitions existed and what type of file systems lived on each one.

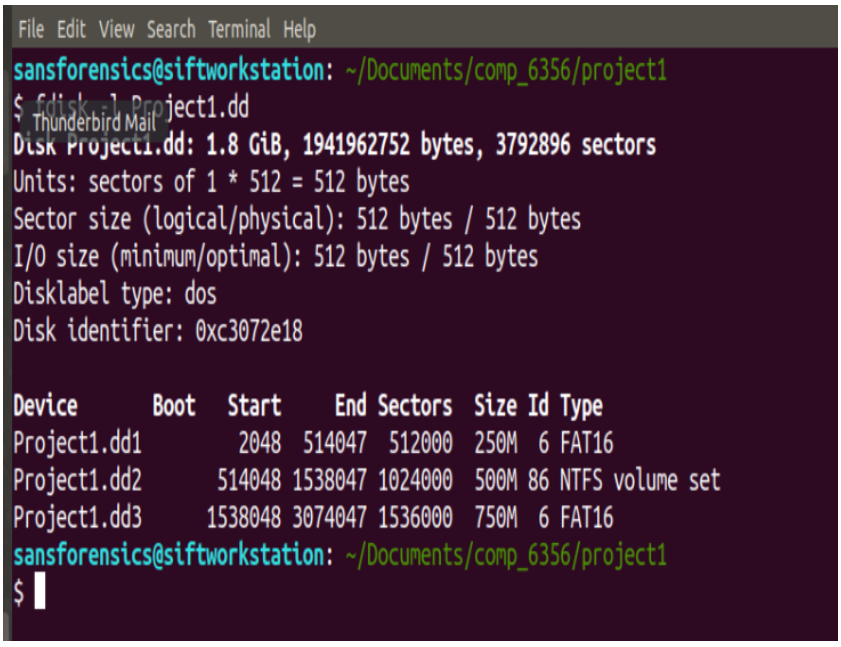

Figure 1: fdisk

2.1 Techniques used on FAT16 File Systems

The first step taken with the FAT16 partitions was checking the master boot record to find the starting sector of the partition, which is where the FAT boot sector was located. From this boot sector we were able to find information about the partition such as sectors before the partition, bytes/sector, sector/cluster, reserved sectors, and the number of sectors in each FAT Area. This information can be combined with the knowledge that FAT16 file systems always follow the same format.

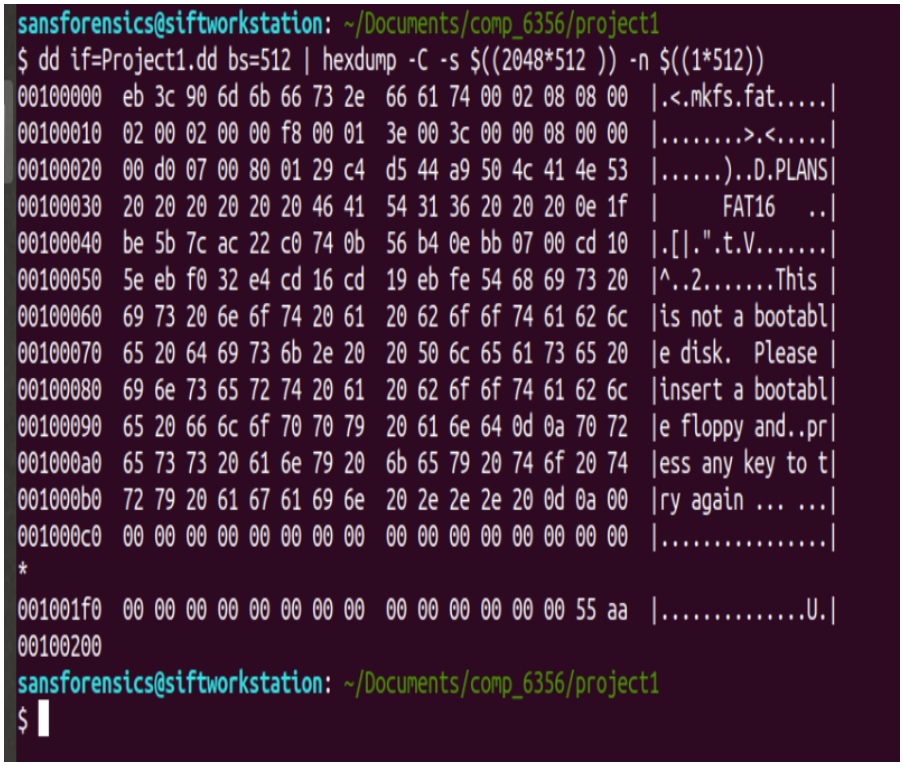

Figure 2: Partition 1 Boot Sector

Using this information, we were able to find the location of the root directory. Since we know that the FAT16 File system follows the format. This contained all of the directory entries of the user created files. The directory entries located in the root directory contained information on each of the user created files such as the file name, file extension, file size, and the starting cluster.

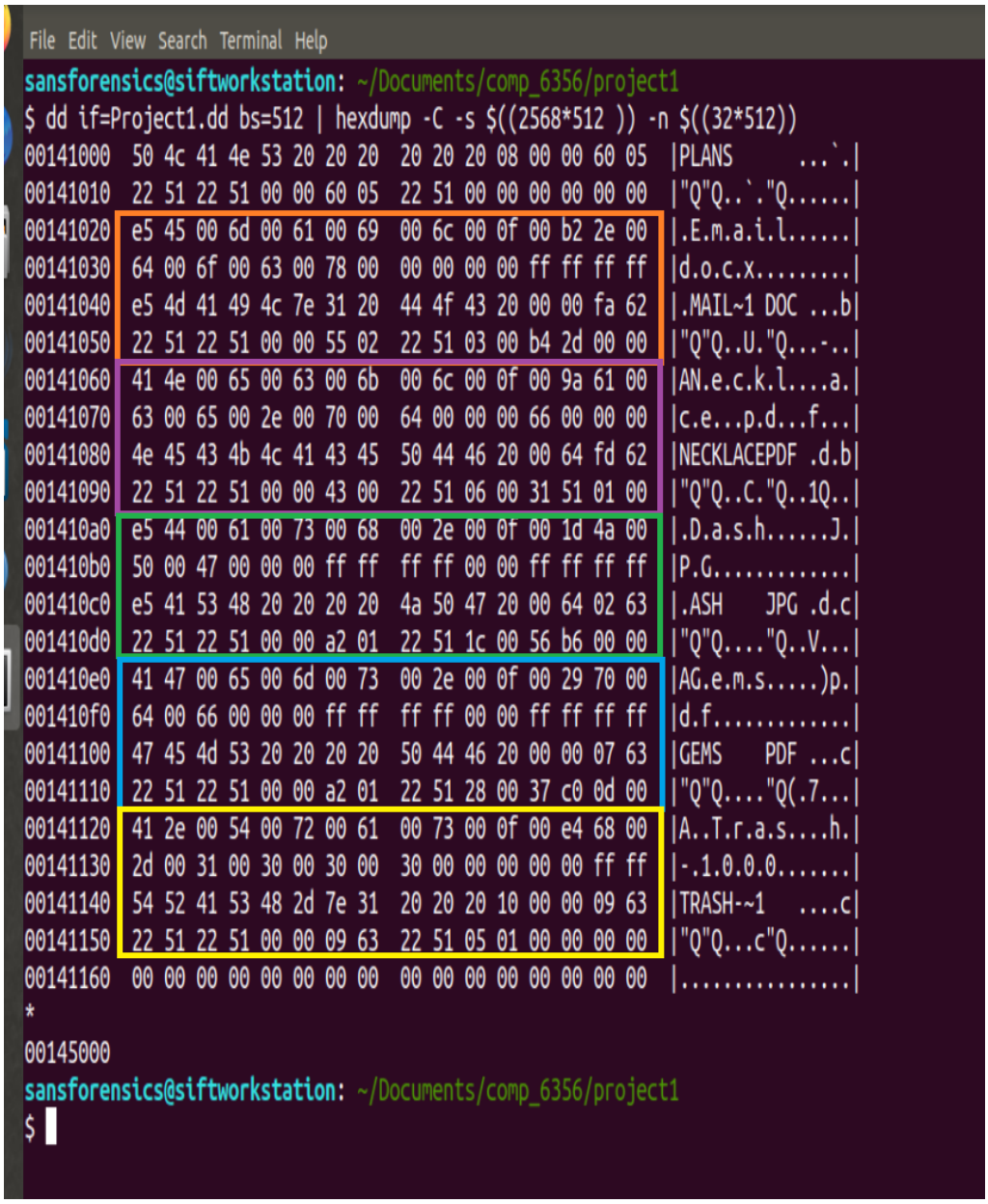

Figure 3: Partition 1 Root Directory

We then used the cluster start to figure out exactly how many clusters each file had, which allowed us to calculate how many sectors each file had. We were then able to use the start of the partition and the location of each FAT system file to locate the starting sector of each of the user created files. After finding the start of the files we were able to use the recovery command to retrieve the files using the starting sector and the size of each file.

2.2 Techniques used on NTFS File Systems

The first step taken with the NTFS partition was checking the master boot record to find the starting sector of the partition. This is where the NTFS boot sector was located. Next we used this boot sector to find the information about the partition as well as the start of the MFT. After we found the MFT we were able to move past the system MFT records to find the user created MFT records. Using these user created records, we were able to discover information for each file, such as: filename, file extension, file size, attributes, non-resident flag, and cluster start. The file size and bytes/sector were used to figure out how many sectors each file had. Using the starting cluster, we were able to then calculate the starting sector by multiplying it by the sectors/cluster. After that we added the starting sector to the beginning of the partition in order to get the sector in which the file was located at. However, for the resident file we had to use the offset located directly after the MFT record for that file.

4 Technical Findings (Tables and Screen Shots)

The following section describes what data was found on the laptop and the various methods used by the accused to hide the information on their device that reveals their attempt to steal the Hope Diamond necklace.

Overall Disk

When looking over the entire disk, it was found that there were three different partitions each with their own file system. Partition 1 and 2 contained FAT16 files systems while partition 2 contained an NTFS File system.

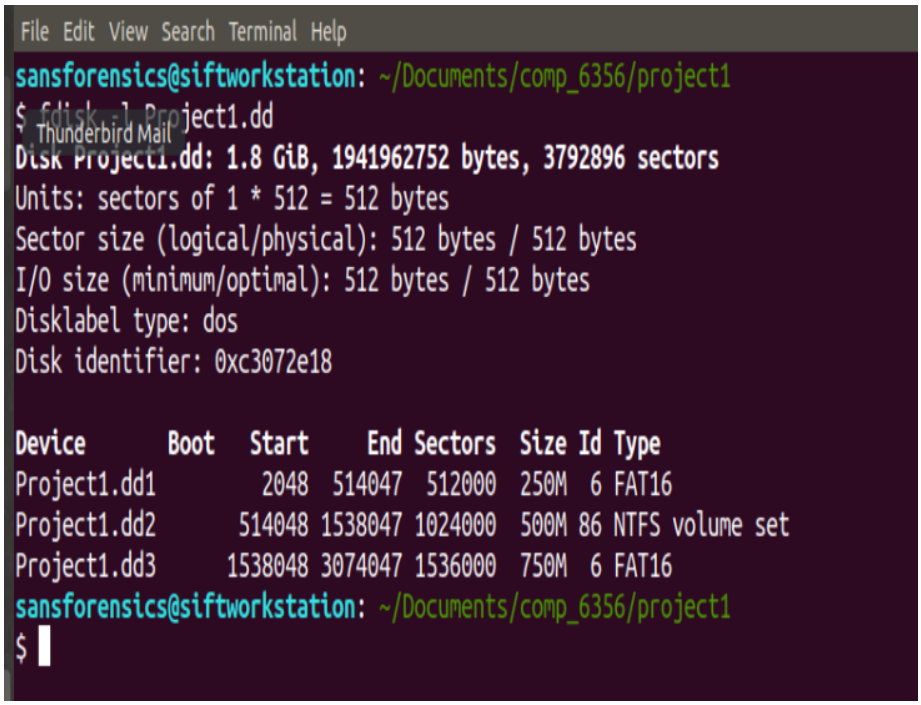

Figure 4: fdisk

There were a total of 12 files found across the three different partitions. The basic information for each recovered information is found in the table below. The recovered files themselves are also included in the submittal of this report for later viewing.

Table 1: Project Results

Project Results						
Partition	Filename	Extension	Status	Byte Offset	File Size	Recovery Command
FAT16	Email	doc	Deleted	1335296	11700	sudo dd if=Project1.dd of=Email.doc bs=1 skip=$((2608*512)) count=11700
FAT16	Necklace	pdf	Normal File	1351680	86321	sudo dd if=Project1.dd of=Necklace.pdf bs=1 skip=$((2640*512)) count=86321
FAT16	Dash	jpg	Deleted	1437696	46678	sudo dd if=Project1.dd of=dash.jpg bs=1 skip=$((2808 * 512)) count=46678
FAT16	Gems	pdf	Normal File	1486848	901175	sudo dd if=Project1.dd of=gems.pdf bs=1 skip=$((2904*512)) count=901175
NTFS	Mystery	zip	Normal File	263274864	258	dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=24296
NTFS	Surveil1	jpg	Normal File	329170944	11602	dd if=Project1.dd of=Surveil1.jpg bs=512 skip=642912 count=11602
NTFS	Surveil2	zip	Normal File	345931776	11179	dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=11179
NTFS	Encoding	pdf	Normal File	362708992	104632	dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258 iflag=skip_bytes,count_bytes
Fat16	Plan	gpg	Deleted	787726336	7584	sudo dd if=Project1.dd of=Plan.gpg bs=1 skip=$((1538528*512)) count=7584
Fat16	History	gpg	Normal File	787742720	1627994	sudo dd if=Project1.dd of=History.gpg bs=1 skip=$((1538560*512)) count=1627994
Fat16	Goal	gpg	Deleted	789381120	48660	sudo dd if=Project1.dd of=Goal.gpg bs=1 skip=$((1541760*512)) count=48660
Fat16	Surveil	gpg	Normal File	789430272	5702	sudo dd if=Project1.dd of=Surveil.gpg bs=1 skip=$((1541856*512)) count=5702

Partition 1

Since Partition 1 contains a FAT16 file system, two of the most important aspects to look at are the FAT Area and the Root Directory. Both of these are shown below respectively. The FAT area (left) can be used to determine how many files are contained inside the file system as well

as which memory segments they are stored in. For partition 1, it can be seen that there are four files and each one is stored in continuous sectors. The root directory of partition 1 (right) can have a total of 32 files inside of it, but in reality only hold 4 user files along with the trash bin. From this root directory we are able to get the state of the file (valid or deleted) as well as the name and starting cluster of each file.

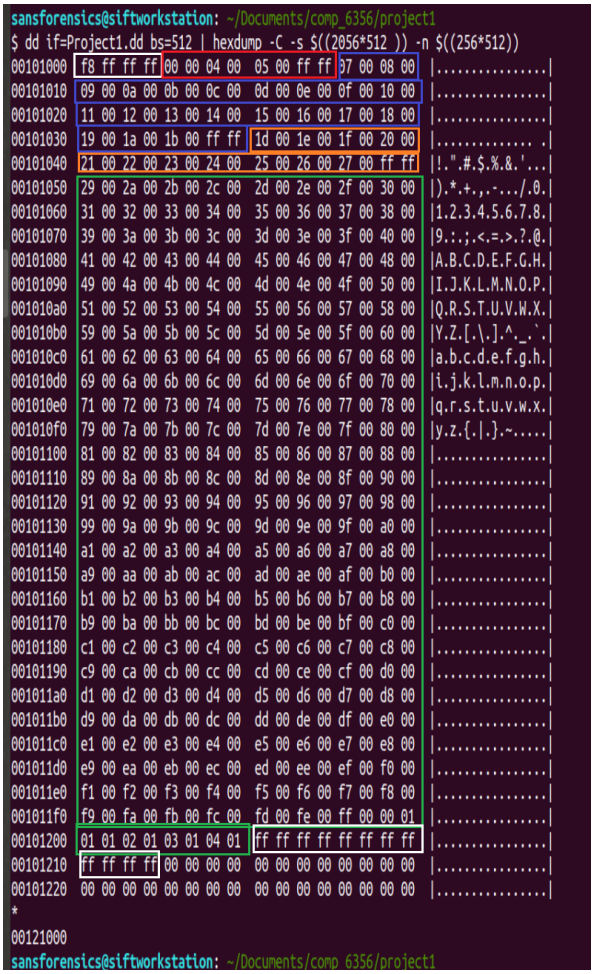

Figure 6: Partition 1 FAT 1

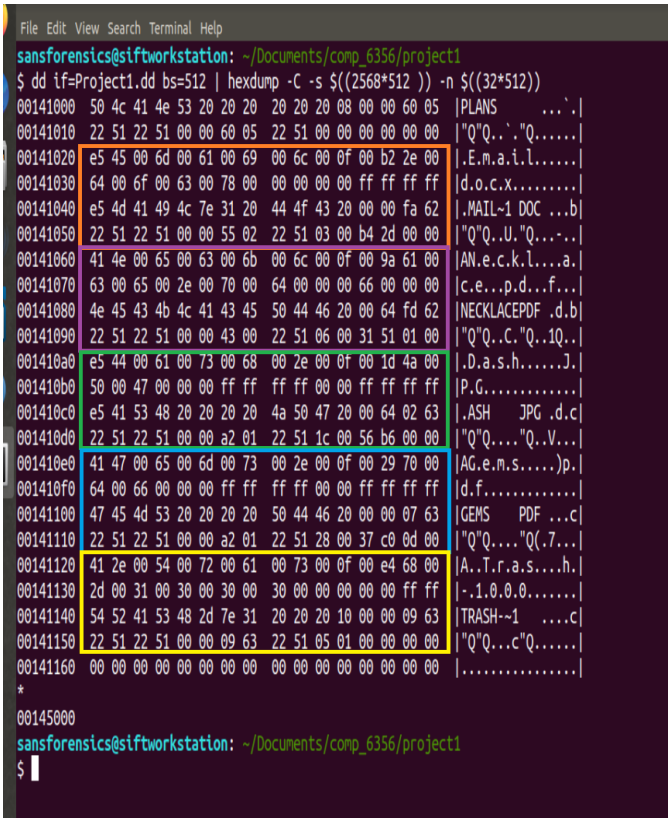

Figure 5: Partition 1 Root Directory

Partition 2

The second partition in the drive contains an NTFS file system. The picture below shows the start of the NTFS system otherwise known as the NTFS Boot Sector, which provides all of the information about the NTFS system that we needed.

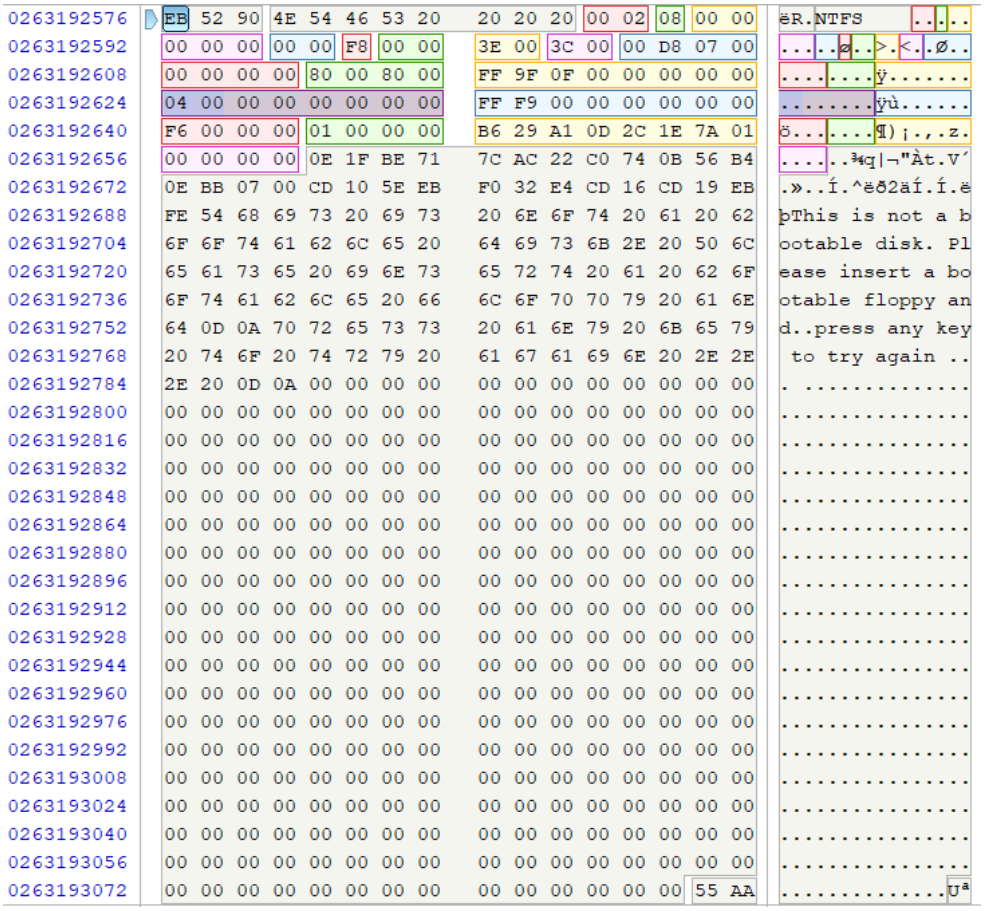

Figure 7: NTFS Boot Sector

The major parts of the NTFS system that we found were the actual user created directory entries. Each of the images below shows the entry for each of the files found in the NTFS system. From each entry we were able to gather information specific to each file, including the size and location of each for recovery.

MFT Record for Mystery.zip

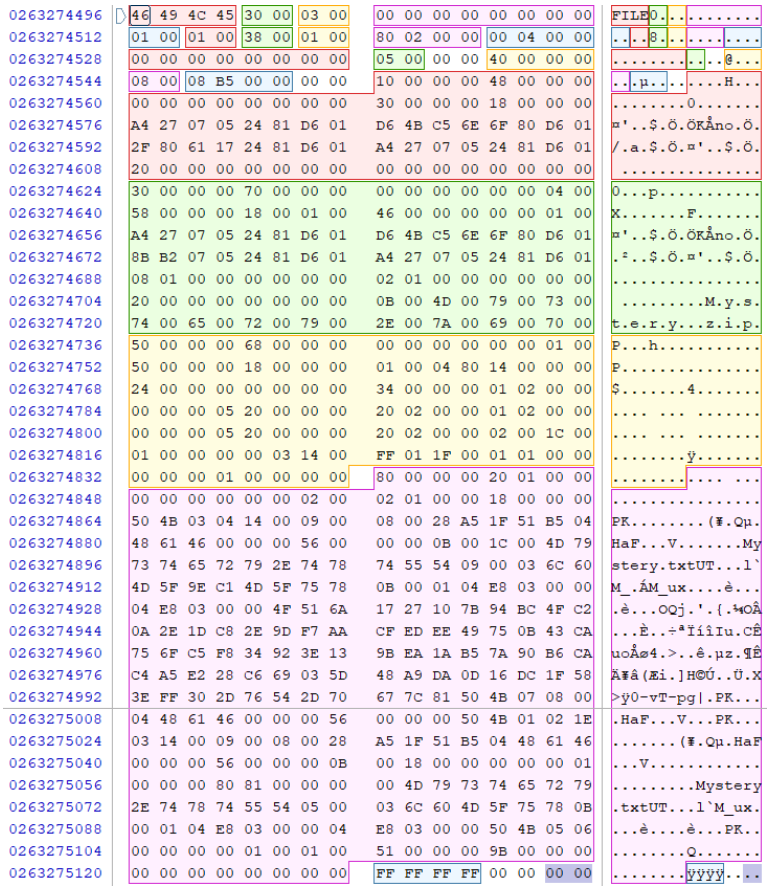

Figure 8: MFT Record for Mystery

MFT Record for Surveil1.jpg

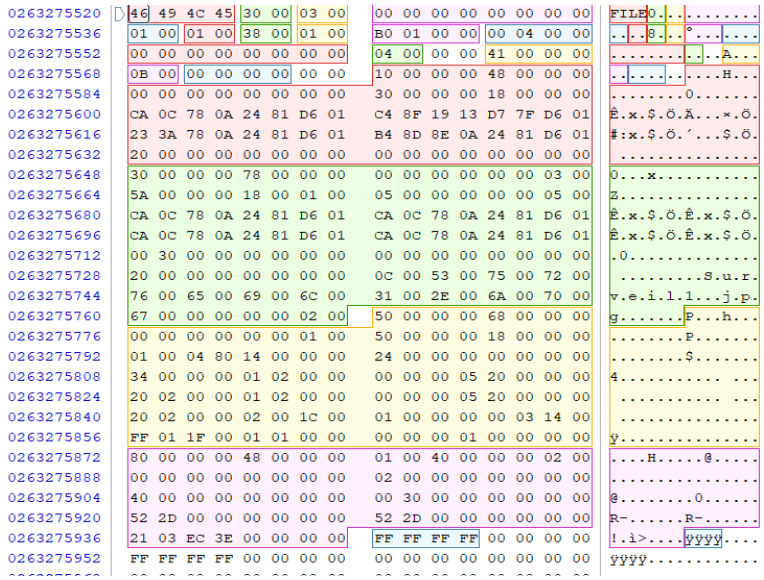

Figure 9: MFT Record for Surveil 1

MFT Record for Surveil2.zip

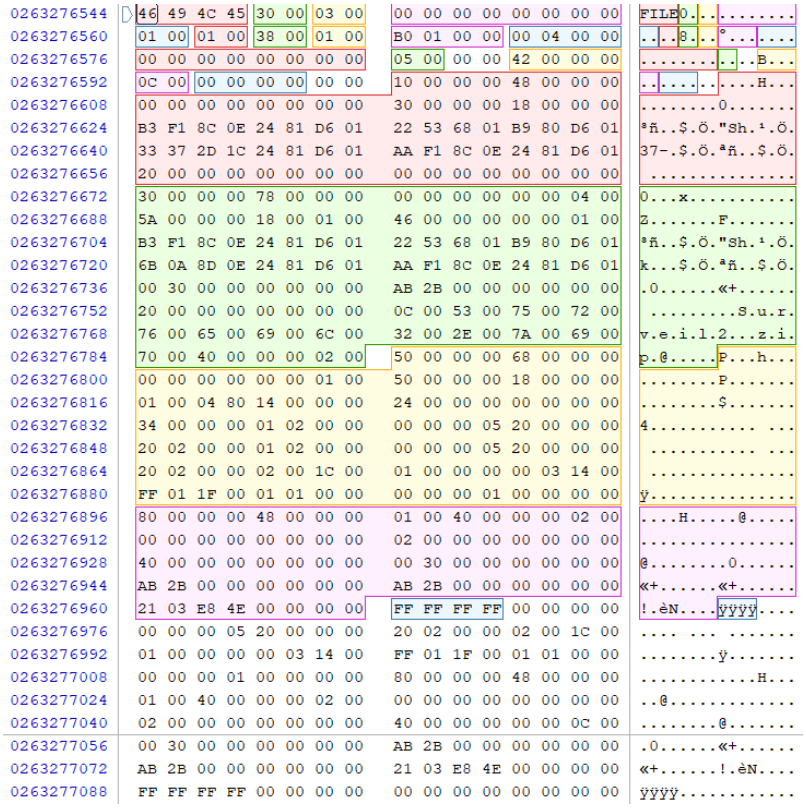

Figure 10: MFT Record for Surveil 2

MFT Record for Encoding.pdf

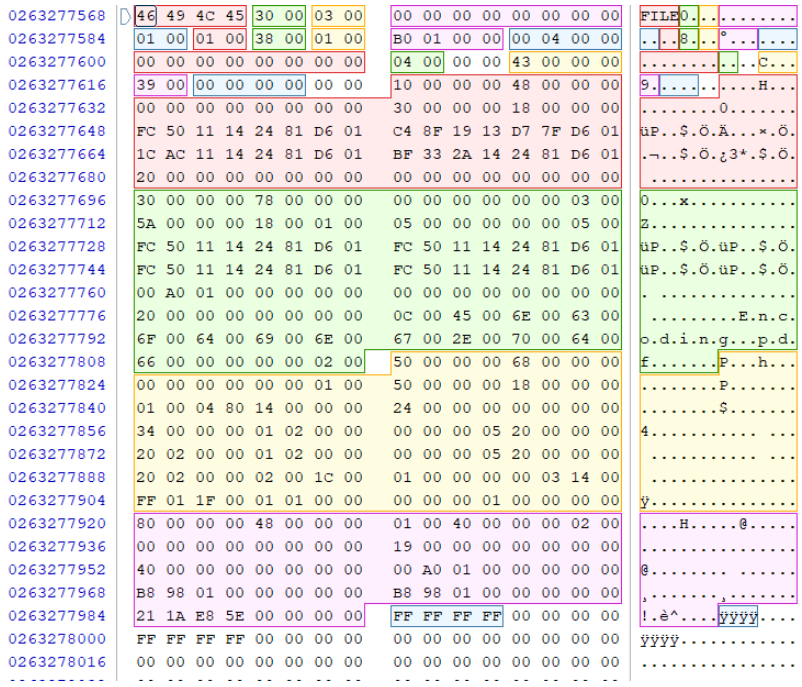

Figure 11: MFT Record for Encoding

Partition 3

Partition 3 is also a FAT16 file system. Using the same methodology as partition 1, it can be seen that partition 3 also contains 4 user files. The names, states, file sizes, and starting clusters of each file can be seen in the root directory to the right. All of this information is written out at the beginning of this section.

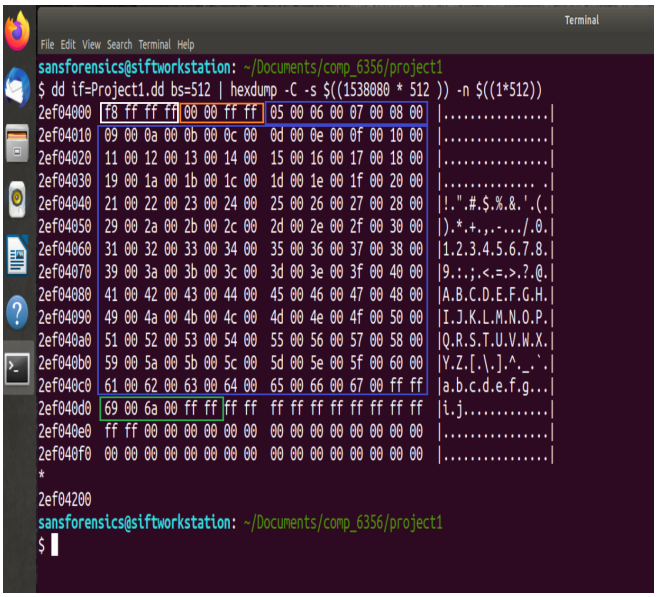

Figure 12: Partition 3 FAT

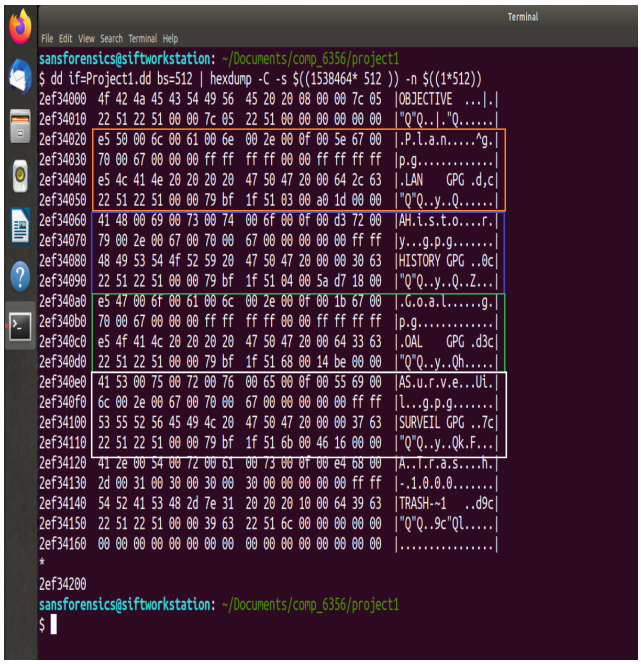

Figure 13: Partition 3 Root Directory

4. 1 Data Hiding Methods Used

The accused offenders utilized several different data hiding methods in order to hide their data. This includes spreading files across different file systems, deletion of files, password protected zip files, file encryption. They also used ascii representation to hide the password for the encryption in plain sight.

4.2 Tools & Applications Used to Hide Data

Tools and applications the laptop users took advantage of were password protected ZIP files and GPG encryption.

4.3 Ultimate Objective of Laptop Users

The objective of our accused offenders was to set up a heist at the Smithsonian Institution in Washington D.C. for the Hope Diamond necklace. The plan was to be executed this October 5th – 6th 2020.

5 Conclusions and Recommendations

We needed to determine if there was enough evidence on the disk image collected to determine if there was proof of criminal activity. Given the email, location pictures, detailed plan, and images of the targeted Hope Diamond necklace, it can be assumed that the accused offender was indeed part of the heist.