



A U B U R N
U N I V E R S I T Y

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

Executive Summary	2
Table of Contents	3
List of Figures	4
List of Tables	5
1 Introduction	6
2 Problem Description	6
3 Analysis Techniques	6
2.1 Techniques used on FAT16 File Systems	7
2.2 Techniques used on NTFS File Systems	9
4 Technical Findings (Tables and Screen Shots)	9
Overall Disk	9
Partition 1	10
Partition 2	12
Partition 3	15
4. 1 Data Hiding Methods Used	16
4.2 Tools & Applications Used to Hide Data	16
4.3 Ultimate Objective of Laptop Users	16
5 Conclusions and Recommendations	17

List of Figures

Figure 1: fdisk.....	6
Figure 2: Partition 1 Boot Sector.....	7
Figure 3: Partition 1 Root Directory.....	8
Figure 4: fdisk.....	10
Figure 6: Partition 1 FAT 1	11
Figure 5: Partition 1 Root Directory.....	11
Figure 7: NTFS Boot Sector	12
Figure 8: MFT Record for Mystery	13
Figure 9: MFT Record for Surveil 1.....	14
Figure 10: MFT Record for Surveil 2.....	14
Figure 11: MFT Record for Encoding.....	15
Figure 12: Partition 3 FAT	15
Figure 13: Partition 3 Root Directory.....	16

List of Tables

Table 1: Project Results.....	10
-------------------------------	----

1 Introduction

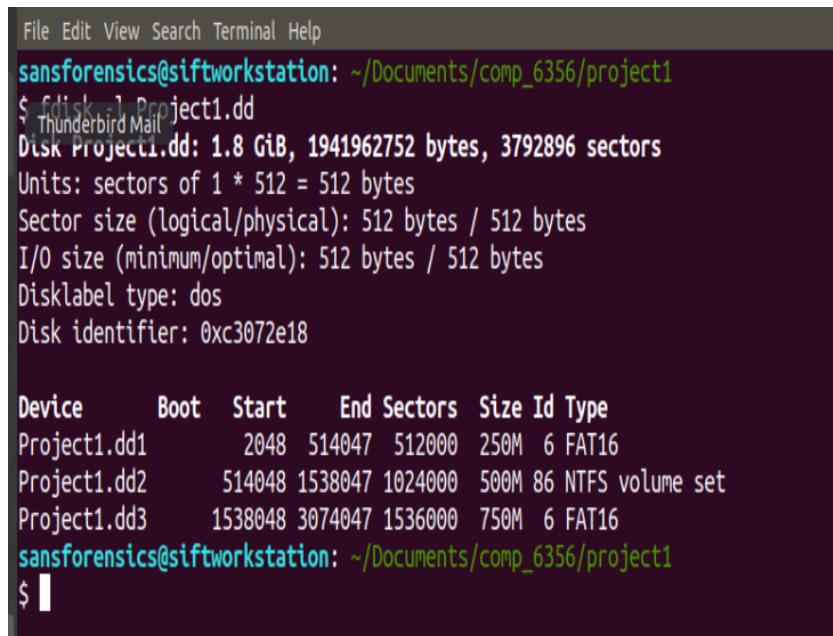
The focus of this assignment is to properly analyze FAT16 and NTFS partitions in order to appropriately recover data from each.

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.



A screenshot of a terminal window on a Linux system. The window title is 'Terminal'. The command entered is '\$ fdisk -l Project1.dd'. The output shows the following details about the disk image:

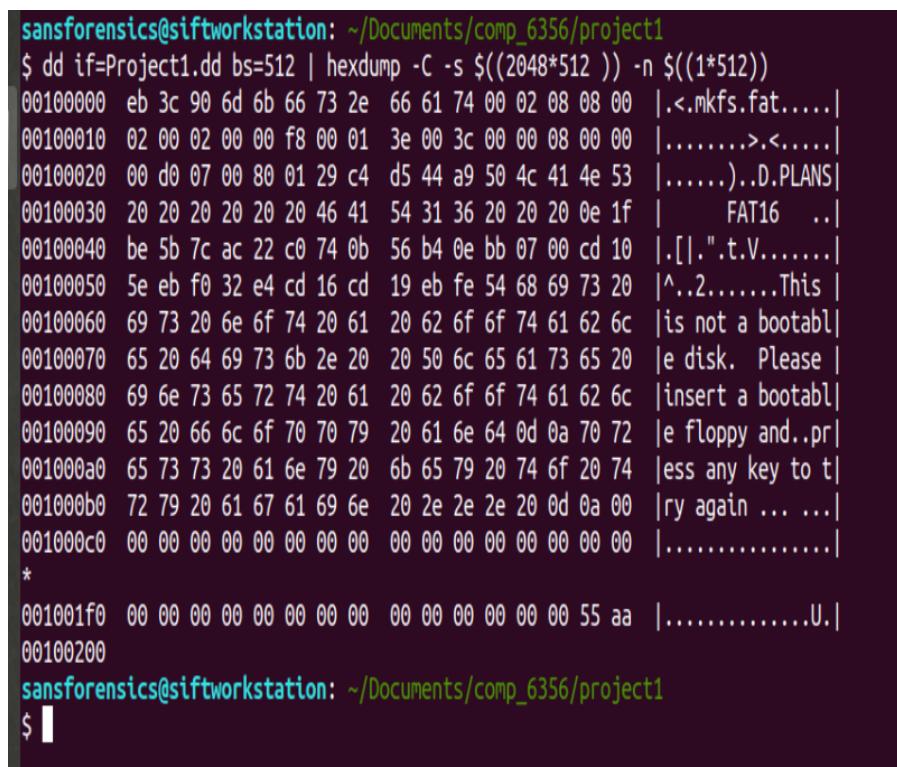
```
File Edit View Search Terminal Help
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ fdisk -l Project1.dd
Disk Project1.dd: 1.8 GiB, 1941962752 bytes, 3792896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3072e18

Device      Boot  Start    End Sectors  Size Id Type
Project1.dd1          2048 514047 512000 250M  6 FAT16
Project1.dd2          514048 1538047 1024000 500M 86 NTFS volume set
Project1.dd3          1538048 3074047 1536000 750M  6 FAT16
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$
```

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.



```
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $((2048*512 )) -n $((1*512))
00100000 eb 3c 90 6d 6b 66 73 2e 66 61 74 00 02 08 08 00 |.<.mkfs.fat.....|
00100010 02 00 02 00 00 f8 00 01 3e 00 3c 00 00 08 00 00 |.....>.<....|
00100020 00 d0 07 00 80 01 29 c4 d5 44 a9 50 4c 41 4e 53 |.....)..D.PLANS|
00100030 20 20 20 20 20 20 46 41 54 31 36 20 20 20 0e 1f |      FAT16   ..|
00100040 be 5b 7c ac 22 c0 74 0b 56 b4 0e bb 07 00 cd 10 |.[|." .t.V.....|
00100050 5e eb f0 32 e4 cd 16 cd 19 eb fe 54 68 69 73 20 |^.2.....This |
00100060 69 73 20 6e 6f 74 20 61 20 62 6f 6f 74 61 62 6c |is not a bootabl|
00100070 65 20 64 69 73 6b 2e 20 20 50 6c 65 61 73 65 20 |e disk. Please |
00100080 69 6e 73 65 72 74 20 61 20 62 6f 6f 74 61 62 6c |insert a bootabl|
00100090 65 20 66 6c 6f 70 70 79 20 61 6e 64 0d 0a 70 72 |e floppy and..pr|
001000a0 65 73 73 20 61 6e 79 20 6b 65 79 20 74 6f 20 74 |ess any key to t|
001000b0 72 79 20 61 67 61 69 6e 20 2e 2e 2e 20 0d 0a 00 |ry again ... ...|
001000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
001001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa |.....U.|
00100200
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$
```

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.

```

File Edit View Search Terminal Help
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $((2568*512)) -n $((32*512))
00141000 50 4c 41 4e 53 20 20 20 20 20 20 08 00 00 60 05 |PLANS ...`|
00141010 22 51 22 51 00 00 60 05 22 51 00 00 00 00 00 00 |"Q"Q.. ."Q.....|
00141020 e5 45 00 6d 00 61 00 69 00 6c 00 0f 00 b2 2e 00 |.E.m.a.i.l.....|
00141030 64 00 6f 00 63 00 78 00 00 00 00 00 ff ff ff ff |d.o.c.x.....|
00141040 e5 4d 41 49 4c 7e 31 20 44 4f 43 20 00 00 fa 62 |.MAIL~1 DOC ...b|
00141050 22 51 22 51 00 00 55 02 22 51 03 00 b4 2d 00 00 |"Q"Q..U."Q...-..|
00141060 41 4e 00 65 00 63 00 6b 00 6c 00 0f 00 9a 61 00 |AN.e.c.k.l....a.|
00141070 63 00 65 00 2e 00 70 00 64 00 00 00 66 00 00 00 |c.e...p.d...f...|
00141080 4e 45 43 4b 4c 41 43 45 50 44 46 20 00 64 fd 62 |NECKLACEPDF .d.b|
00141090 22 51 22 51 00 00 43 00 22 51 06 00 31 51 01 00 |"Q"Q..C."Q..1Q..|
001410a0 e5 44 00 61 00 73 00 68 00 2e 00 0f 00 1d 4a 00 |.D.a.s.h.....J.|
001410b0 50 00 47 00 00 00 ff ff ff ff 00 00 ff ff ff ff |P.G.....|
001410c0 e5 41 53 48 20 20 20 20 4a 50 47 20 00 64 02 63 |.ASH JPG .d.c|
001410d0 22 51 22 51 00 00 a2 01 22 51 1c 00 56 b6 00 00 |"Q"Q...."Q..V...|
001410e0 41 47 00 65 00 6d 00 73 00 2e 00 0f 00 29 70 00 |AG.e.m.s.....)p.|
001410f0 64 00 66 00 00 00 ff ff ff ff 00 00 ff ff ff ff |d.f.....|
00141100 47 45 4d 53 20 20 20 20 50 44 46 20 00 00 07 63 |GEMS PDF ...c|
00141110 22 51 22 51 00 00 a2 01 22 51 28 00 37 c0 0d 00 |"Q"Q...."Q(.7...|
00141120 41 2e 00 54 00 72 00 61 00 73 00 0f 00 e4 68 00 |A..T.r.a.s....h.|
00141130 2d 00 31 00 30 00 30 00 30 00 00 00 00 00 ff ff |-.1.0.0.0.....|
00141140 54 52 41 53 48 2d 7e 31 20 20 20 10 00 00 09 63 |TRASH~1 ....c|
00141150 22 51 22 51 00 00 09 63 22 51 05 01 00 00 00 00 00 |"Q"Q...c"Q.....|
00141160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00145000
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ |

```

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.

```

File Edit View Search Terminal Help
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ fdisk -l Project1.dd
Disk Project1.dd: 1.8 GiB, 1941962752 bytes, 3792896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3072e18

Device      Boot   Start     End Sectors  Size Id Type
Project1.dd1          2048 514047 512000 250M  6 FAT16
Project1.dd2          514048 1538047 1024000 500M 86 NTFS volume set
Project1.dd3          1538048 3074047 1536000 750M  6 FAT16
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ 

```

Figure 4: fdisk

There were a total of 12 files found across the three different partitions. The basic information for each recovered file 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.

```
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $(($2056*512)) -n $((256*512))
00101000 f8 ff ff ff 00 00 04 00 05 00 ff ff 37 00 08 00 |.....|
00101010 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 |.....|
00101020 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 |.....|
00101030 19 00 1a 00 1b 00 ff ff 1d 00 1c 00 1f 00 20 00 |.....|
00101040 21 00 22 00 23 00 24 00 25 00 26 00 27 00 ff ff |!.#,$.%.&.'|.....|
00101050 29 00 2a 00 2b 00 2c 00 2d 00 2e 00 2f 00 30 00 |).*.,.-./.0.|.....|
00101060 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 |1.2.3.4.5.6.7.8.|.....|
00101070 39 00 3a 00 3b 00 3c 00 3d 00 3e 00 3f 00 40 00 |9.;.,<.=,>?.@.|.....|
00101080 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 |A.B.C.D.E.F.G.H.|.....|
00101090 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 4f 00 50 00 |I.J.K.L.M.N.O.P.|.....|
001010a0 51 00 52 00 53 00 54 00 55 00 56 00 57 00 58 00 |Q.R.S.T.U.V.W.X.|.....|
001010b0 59 00 5a 00 5b 00 5c 00 5d 00 5e 00 5f 00 60 00 |Y.Z.[.,].^._.`|.....|
001010c0 61 00 62 00 63 00 64 00 65 00 66 00 67 00 68 00 |a.b.c.d.e.f.g.h.|.....|
001010d0 69 00 6a 00 6b 00 6c 00 6d 00 6e 00 6f 00 70 00 |i.j.k.l.m.n.o.p.|.....|
001010e0 71 00 72 00 73 00 74 00 75 00 76 00 77 00 78 00 |q.r.s.t.u.v.w.x.|.....|
001010f0 79 00 7a 00 7b 00 7c 00 7d 00 7e 00 7f 00 80 00 |y.z.[.,].~.....|
00101100 81 00 82 00 83 00 84 00 85 00 86 00 87 00 88 00 |.....|
00101110 89 00 8a 00 8b 00 8c 00 8d 00 8e 00 8f 00 90 00 |.....|
00101120 91 00 92 00 93 00 94 00 95 00 96 00 97 00 98 00 |.....|
00101130 99 00 9a 00 9b 00 9c 00 9d 00 9e 00 9f 00 a0 00 |.....|
00101140 a1 00 a2 00 a3 00 a4 00 a5 00 a6 00 a7 00 a8 00 |.....|
00101150 a9 00 aa 00 ab 00 ac 00 ad 00 ae 00 af 00 b0 00 |.....|
00101160 b1 00 b2 00 b3 00 b4 00 b5 00 b6 00 b7 00 b8 00 |.....|
00101170 b9 00 ba 00 bb 00 bc 00 bd 00 be 00 bf 00 c0 00 |.....|
00101180 c1 00 c2 00 c3 00 c4 00 c5 00 c6 00 c7 00 c8 00 |.....|
00101190 c9 00 ca 00 cb 00 cc 00 cd 00 ce 00 cf 00 d0 00 |.....|
001011a0 d1 00 d2 00 d3 00 d4 00 d5 00 d6 00 d7 00 d8 00 |.....|
001011b0 d9 00 da 00 db 00 dc 00 dd 00 de 00 df 00 e0 00 |.....|
001011c0 e1 00 e2 00 e3 00 e4 00 e5 00 e6 00 e7 00 e8 00 |.....|
001011d0 e9 00 ea 00 eb 00 ec 00 ed 00 ee 00 ef 00 f0 00 |.....|
001011e0 f1 00 f2 00 f3 00 f4 00 f5 00 f6 00 f7 00 f8 00 |.....|
001011f0 f9 00 fa 00 fb 00 fc 00 fd 00 fe 00 ff 00 01 00 |.....|
00101200 01 01 02 01 03 01 04 01 ff ff ff ff ff ff ff ff |.....|
00101210 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00101220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
```

00121000
sansforensics@siftworkstation: ~/Documents/comp_6356/project1

```
File Edit View Search Terminal Help
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $(($2056*512)) -n $((32*512))
00141000 50 4c 41 4e 53 20 20 20 20 20 08 00 00 60 05 |PLANS ...`|.....|
00141010 22 51 22 51 00 00 60 05 22 51 00 00 00 00 00 00 |"Q"Q..`"Q.....|
00141020 e5 45 00 6d 00 61 00 69 00 66 00 0f 00 b2 2e 00 |.E.m.a.i.l.....|
00141030 64 00 6f 00 63 00 78 00 00 00 00 ff ff ff ff ff |.d.o.c.x.....|
00141040 e5 4d 41 49 4c 7e 31 20 44 4f 43 20 00 00 fa 62 |.MAIL~1 DOC ...b|.....|
00141050 22 51 22 51 00 00 55 02 22 51 03 00 b4 2d 00 00 |"Q"Q..J."Q....|.....|
00141060 41 4e 00 65 00 63 00 6b 00 6c 00 0f 00 9a 61 00 |[AN.e.c.k.l..a.|.....|
00141070 63 00 65 00 2e 00 70 00 64 00 00 00 66 00 00 00 |[c.e...p.d...f...]|.....|
00141080 4e 45 43 4b 4c 41 43 45 50 44 46 20 00 64 fd 62 |[NECKLACEPDF .d.b|.....|
00141090 22 51 22 51 00 00 43 00 22 51 06 00 31 51 01 00 |"Q"Q..C."Q..1Q..|.....|
001410a0 e5 44 00 61 00 73 00 68 00 2e 00 0f 00 1d 4a 00 |[D.a.s.h....J.|.....|
001410b0 50 00 47 00 00 00 ff ff ff ff 00 00 ff ff ff ff ff |[P.G.....|.....|
001410c0 e5 41 53 48 20 20 20 4a 50 47 20 00 64 02 63 |[ASH JPG .d.c|.....|
001410d0 22 51 22 51 00 00 a2 01 22 51 1c 00 56 b6 00 00 |"Q"Q...."Q..V...|.....|
001410e0 41 47 00 65 00 6d 00 73 00 2e 00 0f 00 29 70 00 |[AG.e.m.s....p.|.....|
001410f0 64 00 66 00 00 00 ff ff ff ff 00 ff ff ff ff ff ff |[d.f.....|.....|
00141100 47 45 4d 53 20 20 20 50 44 46 20 00 00 07 63 |[GEMS PDF ...c|.....|
00141110 22 51 22 51 00 00 a2 01 22 51 28 00 37 c0 0d 00 |"Q"Q...."Q(.....|.....|
00141120 41 2e 00 54 00 72 00 61 00 73 00 0f 00 e4 68 00 |[A..T.r.a.s....h.|.....|
00141130 2d 00 31 00 30 00 30 00 30 00 00 00 00 00 ff ff ff |[-1.0.0.0.....|.....|
00141140 54 52 41 53 48 2d 7e 31 20 20 28 10 00 00 09 63 |[TRASH~1 ....c|.....|
00141150 22 51 22 51 00 00 09 63 22 51 05 01 00 00 00 00 00 |"Q"Q...c"Q.....|.....|
00141160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |[.....|.....|
*
```

00145000
sansforensics@siftworkstation: ~/Documents/comp_6356/project1

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.

0263192576	EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00	BR.NTFS
0263192592	00 00 00 00 00 F8 00 00 3E 00 3C 00 00 D8 07 00>.<..Ø..
0263192608	00 00 00 00 80 00 80 00 FF 9F 0F 00 00 00 00 00 00y.....
0263192624	04 00 00 00 00 00 00 00 FF F9 00 00 00 00 00 00 00v.....
0263192640	F6 00 00 00 01 00 00 00 B6 29 A1 0D 2C 1E 7A 01	Ø.....\$)...z.
0263192656	00 00 00 00 0E 1F BE 71 7C AC 22 C0 74 0B 56 B4%q —"Àt.V'
0263192672	0E BB 07 00 CD 10 5E EB F0 32 E4 CD 16 CD 19 EB	..»..í.^ëð2äí.í.ë
0263192688	FE 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 62	This is not a b
0263192704	6F 6F 74 61 62 6C 65 20 64 69 73 6B 2E 20 50 6C	ootable disk. Pl
0263192720	65 61 73 65 20 69 6E 73 65 72 74 20 61 20 62 6F	ease insert a bo
0263192736	6F 74 61 62 6C 65 20 66 6C 6F 70 70 79 20 61 6E	otable floppy an
0263192752	64 0D 0A 70 72 65 73 73 20 61 6E 79 20 6B 65 79	d..press any key
0263192768	20 74 6F 20 74 72 79 20 61 67 61 69 6E 20 2E 2E	to try again ..
0263192784	2E 20 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192816	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192832	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192848	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192864	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192880	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192896	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192912	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192928	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192944	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192960	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192976	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263192992	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263193008	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263193024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263193040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263193056	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0263193072	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ua

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

0263274496	46 49 4C 45	30 00	03 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	FILE0.....
0263274512	01 00	01 00	38 00	01 00	...B.....
0263274528	00 00	00 00	00 00	00 00 00	05 00 00 00 40 00 00 00
0263274544	08 00	08 B5 00 00	00 00	10 00 00 00 48 00 00 00B.....
0263274560	00 00 00 00 00 00 00 00 00	30 00 00 00 18 00 00 00	D6 4B C5 6E 6F 80 D6 01H.....	
0263274576	A4 27 07 05 24 81 D6 01	D6 4B C5 6E 6F 80 D6 01	A4 27 07 05 24 81 D6 010.....	
0263274592	2F 80 61 17 24 81 D6 01	A4 27 07 05 24 81 D6 01	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00\$.\$.\$.\$.\$.	
0263274608	20 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0263274624	30 00 00 00 70 00 00 00 00	00 00 00 00 00 00 00 04 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0...p.....	
0263274640	58 00 00 00 18 00 01 00	46 00 00 00 00 00 00 01 00	46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	X.....F.....	
0263274656	A4 27 07 05 24 81 D6 01	D6 4B C5 6E 6F 80 D6 01	A4 27 07 05 24 81 D6 01\$.\$.\$.\$.	
0263274672	8B B2 07 05 24 81 D6 01	A4 27 07 05 24 81 D6 01	08 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00\$.\$.	
0263274688	20 00 00 00 00 00 00 00 00	02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0B 00 4D 00 79 00 73 00M.y.s.	
0263274704	74 00 65 00 72 00 79 00	2E 00 7A 00 69 00 70 00	2E 00 7A 00 69 00 70 00	t.e.r.y...z.i.p.	
0263274720	50 00 00 00 68 00 00 00	00 00 00 00 00 00 00 01 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	P...h.....	
0263274736	50 00 00 00 18 00 00 00	01 00 04 80 14 00 00 00	01 00 04 80 14 00 00 00	P.....	
0263274752	24 00 00 00 00 00 00 00 00	34 00 00 00 01 02 00 00	34 00 00 00 01 02 00 00	S.....4.....	
0263274768	00 00 00 05 20 00 00 00	20 02 00 00 01 02 00 00	20 02 00 00 01 02 00 00	
0263274784	00 00 00 05 20 00 00 00	20 02 00 00 02 00 1C 00	20 02 00 00 02 00 1C 00	
0263274800	01 00 00 00 00 03 14 00	FF 01 1F 00 01 01 00 00	FF 01 1F 00 01 01 00 00y.....	
0263274816	00 00 00 01 00 00 00 00 00	80 00 00 00 20 01 00 00	80 00 00 00 20 01 00 00	
0263274832	00 00 00 00 00 02 00	02 01 00 00 18 00 00 00	02 01 00 00 18 00 00 00	PK.....(?.Qu.	
0263274848	50 4B 03 04 14 00 09 00	08 00 28 A5 1F 51 B5 04	08 00 28 A5 1F 51 B5 04	HaF...V.....My	
0263274864	48 61 46 00 00 00 56 00	00 00 0B 00 1C 00 4D 79	74 55 54 09 00 03 6C 60	stery.txtUT...l`	
0263274880	73 74 65 72 79 2E 74 78	74 55 54 09 00 03 6C 60	74 55 54 09 00 03 6C 60	M..ÅM_ux....è...	
0263274896	4D 5F 9E C1 4D 5F 75 78	0B 00 01 04 E8 03 00 00	0B 00 01 04 E8 03 00 00	.è...OQj.'(.4OÀ	
0263274912	04 E8 03 00 00 4F 51 6A	17 27 10 7B 94 BC 4F C2	17 27 10 7B 94 BC 4F C2	...È..=^iiliu.CÈ	
0263274928	0A 2E 1D C8 2E 9D F7 AA	CF ED EE 49 75 0B 43 CA	CF ED EE 49 75 0B 43 CA	uoÅø4.>..è..uz.QÈ	
0263274944	75 6F C5 F8 34 92 3E 13	9B EA 1A B5 7A 90 B6 CA	9B EA 1A B5 7A 90 B6 CA	ÀÌÀ(Zi.)H@Ù..Ù.X	
0263274960	C4 A5 E2 28 C6 69 03 5D	48 A9 DA 0D 16 DC 1F 58	48 A9 DA 0D 16 DC 1F 58	>y0-vT-pgl.PK...	
0263274976	3E FF 30 2D 76 54 2D 70	67 7C 81 50 4B 07 08 00	67 7C 81 50 4B 07 08 00	.HaF...V...PK...	
0263274992	04 48 61 46 00 00 00 56	00 00 00 50 4B 01 02 1E	00 00 00 50 4B 01 02 1E(?.Qu.HaF	
0263275008	03 14 00 09 00 08 00 28	A5 1F 51 B5 04 48 61 46	A5 1F 51 B5 04 48 61 46	...V.....	
0263275024	00 00 00 56 00 00 00 0B	00 18 00 00 00 00 00 01	00 18 00 00 00 00 00 01Mystery	
0263275040	00 00 00 80 81 00 00 00	00 4D 79 73 74 65 72 79	00 4D 79 73 74 65 72 79	.txtUT...l'M_ux.	
0263275056	2E 74 78 74 55 54 05 00	03 6C 60 4D 5F 75 78 0B	03 6C 60 4D 5F 75 78 0B	...è....è...PK..	
0263275072	00 01 04 E8 03 00 00 04	E8 03 00 00 50 4B 05 06	E8 03 00 00 50 4B 05 06Q.....	
0263275088	00 00 00 00 01 00 01 00	51 00 00 00 9B 00 00 00	51 00 00 00 9B 00 00 00y...y....	
0263275104	00 00 00 00 00 00 00 00	FF FF FF FF	FF FF FF FF	
0263275120	00 00 00 00 00 00 00 00	FF FF FF FF	FF FF FF FF	

Figure 8: MFT Record for Mystery

MFT Record for Surveil1.jpg

0263275520	D	46 49 4C 45	30 00	03 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	FILE0..
0263275536	01 00	01 00	38 00	01 00	B0 01 00 00 00 04 00 00	...8..
0263275552	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00	00 00 41 00 00 00A..		
0263275568	0B 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	10 00	00 00 48 00 00 00H..	
0263275584	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	30 00	00 18 00 00 00 000....		
0263275600	C4 8F 19 13 D7 7F D6 01	B4 8D 8E 0A 24 81 D6 01E.x.\$.O.A...x.O.			
0263275616	23 3A 78 0A 24 81 D6 01	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	#:x.\$.O.'...S.O.			
0263275632	20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00			
0263275648	30 00 00 00 78 00 00 00	00 00 00 00 00 00 03 00	0...x.....			
0263275664	5A 00 00 00 18 00 01 00	05 00 00 00 00 05 00	Z.....			
0263275680	CA 0C 78 0A 24 81 D6 01	CA 0C 78 0A 24 81 D6 01	E.x.\$.O.E.x.S.O.			
0263275696	CA 0C 78 0A 24 81 D6 01	CA 0C 78 0A 24 81 D6 01	E.x.\$.O.E.x.S.O.			
0263275712	00 30 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.0.....			
0263275728	20 00 00 00 00 00 00 00	0C 00 53 00 75 00 72 00S.u.r.			
0263275744	76 00 65 00 69 00 6C 00	31 00 2E 00 6A 00 70 00	v.e.i.l.1..j.p.			
0263275760	67 00 00 00 00 00 02 00	50 00 00 00 68 00 00 00	g.....P..h..			
0263275776	00 00 00 00 00 00 01 00	50 00 00 00 18 00 00 00P.....			
0263275792	01 00 04 80 14 00 00 00	24 00 00 00 00 00 00 00S.....			
0263275808	34 00 00 00 01 02 00 00	00 00 00 05 20 00 00 00	4.....			
0263275824	20 02 00 00 01 02 00 00	00 00 00 05 20 00 00 00			
0263275840	20 02 00 00 02 00 1C 00	01 00 00 00 03 14 00			
0263275856	FF 01 1F 00 01 01 00 00	00 00 00 01 00 00 00 00	y.....			
0263275872	80 00 00 00 48 00 00 00	01 00 40 00 00 00 02 00H....@..			
0263275888	00 00 00 00 00 00 00 00	02 00 00 00 00 00 00 00			
0263275904	40 00 00 00 00 00 00 00	00 30 00 00 00 00 00 00	@.....0.....			
0263275920	52 2D 00 00 00 00 00 00	52 2D 00 00 00 00 00 00	R-.....R-..			
0263275936	21 03 EC 3E 00 00 00 00	FF FF FF FF 00 00 00 00	!i>....yyyy.....			
0263275952	FF FF FF FF 00 00 00 00	00 00 00 00 00 00 00 00	yyyy.....			

Figure 9: MFT Record for Surveil 1

MFT Record for Surveil2.zip

0263276544	D	46 49 4C 45	30 00	03 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	FILE0..
0263276560	01 00	01 00	38 00	01 00	B0 01 00 00 00 04 00 00	...8..
0263276576	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00	00 42 00 00 00B..		
0263276592	0C 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	10 00	00 48 00 00 00 00H..	
0263276608	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	30 00	00 18 00 00 00 000....		
0263276624	B3 F1 8C 0E 24 81 D6 01	22 53 68 01 B9 80 D6 01	*R..S.O."Sh..1.O.			
0263276640	33 37 2D 1C 24 81 D6 01	AA F1 8C 0E 24 81 D6 01	37-.S.O.*n..S.O.			
0263276656	20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00			
0263276672	30 00 00 00 78 00 00 00	00 00 00 00 00 00 04 00	0...x.....			
0263276688	5A 00 00 00 18 00 01 00	46 00 00 00 00 00 01 00	Z.....F.....			
0263276704	B3 F1 8C 0E 24 81 D6 01	22 53 68 01 B9 80 D6 01	*R..S.O."Sh..1.O.			
0263276720	6B 0A 8D 0E 24 81 D6 01	AA F1 8C 0E 24 81 D6 01	k...S.O.*n..S.O.			
0263276736	00 30 00 00 00 00 00 00	AB 2B 00 00 00 00 00 00	.0.....<+.....			
0263276752	20 00 00 00 00 00 00 00	0C 00 53 00 75 00 72 00S.u.r.			
0263276768	76 00 65 00 69 00 6C 00	32 00 2E 00 7A 00 69 00	v.e.i.l.2..z.i.			
0263276784	70 00 40 00 00 00 02 00	50 00 00 00 68 00 00 00	p.@.....P..h..			
0263276800	00 00 00 00 00 00 00 01 00	50 00 00 00 18 00 00 00P.....			
0263276816	01 00 04 80 14 00 00 00	24 00 00 00 00 00 00 00S.....			
0263276832	34 00 00 00 01 02 00 00	00 00 00 05 20 00 00 00	4.....			
0263276848	20 02 00 00 01 02 00 00	00 00 00 05 20 00 00 00			
0263276864	20 02 00 00 02 00 1C 00	01 00 00 00 03 14 00			
0263276880	FF 01 1F 00 01 01 00 00	00 00 00 01 00 00 00 00	y.....			
0263276896	80 00 00 00 48 00 00 00	01 00 40 00 00 00 02 00H....@..			
0263276912	00 00 00 00 00 00 00 00	02 00 00 00 00 00 00 00			
0263276928	40 00 00 00 00 00 00 00	00 30 00 00 00 00 00 00	@.....0.....			
0263276944	AB 2B 00 00 00 00 00 00	AB 2B 00 00 00 00 00 00	<+.....<+.....			
0263276960	21 03 E8 4E 00 00 00 00	FF FF FF FF 00 00 00 00	!..èN.....yyyy.....			
0263276976	00 00 00 05 20 00 00 00	20 02 00 00 02 00 1C 00			
0263276992	01 00 00 00 03 14 00	FF 01 1F 00 01 01 00 00y.....			
0263277008	00 00 00 01 00 00 00 00	80 00 00 00 48 00 00 00H.....			
0263277024	01 00 40 00 00 00 02 00	00 00 00 00 00 00 00 00	..@.....			
0263277040	02 00 00 00 00 00 00 00	40 00 00 00 00 00 00 0C 00@.....			
0263277056	00 30 00 00 00 00 00 00	AB 2B 00 00 00 00 00 00	.0.....<+.....			
0263277072	AB 2B 00 00 00 00 00 00	21 03 E8 4E 00 00 00 00	<+.....!..èN.....			
0263277088	FF FF FF FF 00 00 00 00	00 00 00 00 00 00 00 00	yyyy.....			

Figure 10: MFT Record for Surveil 2

MFT Record for Encoding.pdf

0263277568	[46 49 4C 45]	30 00 03 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	FILE0...
0263277584	01 00	01 00	38 00 01 00	B0 01 00 00	00 04 00 00
0263277600	00 00	00 00	00 00 00 00 00 00	04 00 00 00	43 00 00 00
0263277616	39 00	00 00 00 00 00 00	10 00 00 00 48 00 00 00	9...H..
0263277632	00 00 00 00 00 00 00 00	30 00 00 00 18 00 00 000.....
0263277648	FC 50 11 14 24 81 D6 01	C4 8F 19 13 D7 7F D6 01	üP..\$.ö.Ä...x.ö.	üP..\$.ö.üP..\$.ö.	üP..\$.ö.üP..\$.ö.
0263277664	1C AC 11 14 24 81 D6 01	BF 33 2A 14 24 81 D6 01
0263277680	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00
0263277696	30 00 00 00 78 00 00 00	00 00 00 00 00 00 00 03 00	0...x.....	Z.....
0263277712	5A 00 00 00 18 00 01 00	05 00 00 00 00 00 05 00	üP..\$.ö.üP..\$.ö.	üP..\$.ö.üP..\$.ö.
0263277728	FC 50 11 14 24 81 D6 01	FC 50 11 14 24 81 D6 01
0263277744	FC 50 11 14 24 81 D6 01	FC 50 11 14 24 81 D6 01
0263277760	00 A0 01 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00E.n.c.
0263277776	20 00 00 00 00 00 00 00	0C 00 45 00 6E 00 63 00	o.d.i.n.g...p.d.
0263277792	6F 00 64 00 69 00 6E 00	67 00 2E 00 70 00 64 00	f.....P.h...
0263277808	66 00 00 00 00 02 00	50 00 00 00 68 00 00 00P.....\$.....
0263277824	00 00 00 00 00 00 01 00	50 00 00 00 18 00 00 00	4.....
0263277840	01 00 04 80 14 00 00 00	24 00 00 00 00 00 00 00	y.....
0263277856	34 00 00 00 01 02 00 00	00 00 00 05 20 00 00 00H....@.....
0263277872	20 02 00 00 01 02 00 00	00 00 00 05 20 00 00 00	@.....
0263277888	20 02 00 00 02 00 1C 00	01 00 00 00 00 03 14 00	,	,.....
0263277904	FF 01 1F 00 01 01 00 00	00 00 00 01 00 00 00 00	!..^.....VVVY.....
0263277920	80 00 00 00 48 00 00 00	01 00 40 00 00 00 02 00
0263277936	00 00 00 00 00 00 00 00	19 00 00 00 00 00 00 00
0263277952	40 00 00 00 00 00 00 00	00 A0 01 00 00 00 00 00
0263277968	B8 98 01 00 00 00 00 00	B8 98 01 00 00 00 00 00
0263277984	21 1A E8 5E 00 00 00 00	FF FF FF FF 00 00 00 00
0263278000	FF FF FF FF 00 00 00 00	00 00 00 00 00 00 00 00	VVVY.....
0263278016	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

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.

```

File Edit View Search Terminal Help
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $(($1538080 * 512)) -n $(($1*512))
2ef04000 [F8 FF FF FF] 00 00 ff FF 05 00 06 00 07 00 08 00 |.....|
2ef04010 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 |.....|
2ef04020 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 |.....|
2ef04030 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 |.....|
2ef04040 21 00 22 00 23 00 24 00 25 00 26 00 27 00 28 00 |!.,#.%,&.'(.|
2ef04050 29 00 2a 00 2b 00 2c 00 2d 00 2e 00 2f 00 30 00 |).*,+,.,./.|
2ef04060 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 |1,2,3,4,5,6,7,8,|
2ef04070 39 00 3a 00 3b 00 3c 00 3d 00 3e 00 3f 00 40 00 |9.,.;,<=>?@|
2ef04080 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 |A.B.C.D.E.F.G.H.|
2ef04090 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 4f 00 50 00 |I.J.K.L.M.N.O.P.|
2ef040a0 51 00 52 00 53 00 54 00 55 00 56 00 57 00 58 00 |Q.R.S.T.U.V.W.X.|
2ef040b0 59 00 5a 00 5b 00 5c 00 5d 00 5e 00 5f 00 60 00 |Y.Z,[.,]^_,`|
2ef040c0 61 00 62 00 63 00 64 00 65 00 66 00 67 00 ff ff |a.b.c.d.e.f.g...|
2ef040d0 69 00 6a 00 ff |i,j,.....|
2ef040e0 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
2ef040f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
2ef04200
sansforensics@siftworkstation: ~/Documents/comp_6356/project1
$ 
```

Figure 12: Partition 3 FAT

```

File Edit View Search Terminal Help
sansforensics@scs-lftworkstation: ~/Documents/comp_6356/project1
$ dd if=Project1.dd bs=512 | hexdump -C -s $((1538464* 512 )) -n $((1*512))
2ef34000 4f 42 4a 45 43 54 49 56 45 20 20 08 00 00 7c 05 |OBJECTIVE ...|.
2ef34010 22 51 22 51 00 00 7c 05 22 51 00 00 00 00 00 00 |"Q\0..|\."Q\0...|.
2ef34020 e5 50 00 6c 00 61 00 6e 00 2e 00 0f 00 5e 67 00 |.P.l.a.n....\g.|.
2ef34030 70 00 67 00 00 00 ff ff ff ff 00 00 ff ff ff ff |p.g.....|.
2ef34040 e5 4c 41 4e 20 20 20 20 47 50 47 20 00 64 2c 63 |.LAN GPG .d3c|
2ef34050 22 51 22 51 00 00 79 bf 1f 51 03 00 a0 1d 00 00 |"Q\0..y\0...|.
2ef34060 41 48 00 69 00 73 00 74 00 6f 00 0f 00 d3 72 00 |AH.i.s.t.o...|.
2ef34070 79 00 2e 00 67 00 70 00 67 00 00 00 00 00 ff ff |y..g.p.g.....|.
2ef34080 48 49 53 54 4f 52 59 20 47 50 47 20 00 39 63 |HISTORY GPG ..8c|
2ef34090 22 51 22 51 00 00 79 bf 1f 51 04 00 5a d7 18 00 |"Q\0..y\0..Z...|.
2ef340a0 e5 47 00 6f 00 61 00 6c 00 2e 00 0f 00 1b 67 00 |.G.o.a.l....\g.|.
2ef340b0 70 00 67 00 00 00 ff ff ff ff 00 00 ff ff ff ff |p.g.....|.
2ef340c0 e5 4f 41 4c 20 20 20 20 47 50 47 20 00 64 33 63 |.OAL GPG .d3c|
2ef340d0 22 51 22 51 00 00 79 bf 1f 51 68 00 14 be 00 00 |"Q\0..y\0..Qh...|.
2ef340e0 41 53 00 75 00 72 00 76 00 65 00 0f 00 55 69 00 |AS.u.r.v.e..U.|.
2ef340f0 6c 00 2e 00 67 00 70 00 67 00 00 00 00 00 ff ff |l...g.p.g.....|.
2ef34100 53 55 52 56 45 49 4c 20 47 50 47 20 00 00 37 63 |SURVEIL GPG ..7c|
2ef34110 22 51 22 51 00 00 79 bf 1f 51 6b 00 46 16 00 00 |"Q\0..y\0..Qk.F...|.
2ef34120 41 2e 00 54 00 72 00 61 00 73 00 0f 00 e4 68 00 |A..I.r.a.s....|.
2ef34130 2d 00 31 00 30 00 30 00 30 00 00 00 00 00 ff ff |..1.0.0.0.....|.
2ef34140 54 52 41 53 48 2d 7e 31 20 20 20 10 00 64 39 63 |TRASH~1 ..d9c|
2ef34150 22 51 22 51 00 00 39 63 22 51 6c 00 00 00 00 00 |"Q\0..9c"\0l....|.
2ef34160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|.
*
2ef34200
sansforensics@scs-lftworkstation: ~/Documents/comp_6356/project1
$ 

```

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.