AUBURN

UNIVERSITY

Investigation of Foreign Disk Drive

Blake Moore and Nico Marthe

9/27/2023

1 Executive Summary

A laptop was collected during a forensics investigation, and we were tasked with investigating a copy of the disk drive found on the laptop. The goal of our investigation was to examine the drive for any potential evidence of criminal activity. Throughout our investigation of the disk drive, we found that the drive had three partitions. The first and third were FAT16 partitions and the second one was a NTFS partition.

Throughout our investigation we were able to find starting sectors for each partition found on the drive. Through this we were able to investigate the sectors reserved for each partition and found the relevant information related to the files on the disk drive. Each partition had its own set of files that we were able to retrieve for the investigation.

We found that whoever was in possession of the laptop used various methods to hide their data. The methods were the deletion of entire files, encryption, password protection and the separation of all these files among the different partitions. With these methods in mind and the information gathered from the recovered files we discovered that the original owners of the disk drive were planning to steal the Hope Diamond necklace from the Smithsonian Institute.

To see the executive summary table, see Table 5.

2 Collaboration Summary

This project was worked on by both Nico Marthe and Blake Moore. We divided up our investigation by each choosing one of the FAT16 partitions to work on, then shared our findings. We later investigated the NTFS partition individually and then verified our findings with one another to ensure that we had the same findings as each other. Combining our findings, we put together all our evidence to discover the mystery of this disk image and write this report.

Table of Contents

List of Figures

List of Tables

3 Problem Description

This report is meant to showcase our findings after examining a disk image provided to us that was collected from a laptop during a forensics investigation. This goal was to properly analyze both FAT16 and NTFS partitions of this disk image to recover data from each partition.

4 Analysis Techniques

We began the analysis by pulling a copy of the original disk image into a virtual machine. We then examined the contents to determine what and how many partitions it had. See Figure 1.

This revealed that we had a disk drive with three partitions. Two were FAT16 and one was an NTFS volume set. Knowing this the next step for our investigation was to make a deep dive into each partition, starting with the first FAT16 partition.

4.1 Techniques Used on Partition 1 (FAT16)

The first step when analyzing the FAT16 partitions was to check the reserved area of this FAT16 partition that held the boot sector. This contains information relevant to the partition like the bytes/sector, sectors/cluster, reserved sectors, and sectors found per FAT area. See Figure 2. With this information along with the information we obtained when first examining the entire disk we were able to calculate the starting sectors for each FAT area found among the partitions.

Using this information from the boot sector we knew where the first FAT area and root directory of this partition began. This allowed us to examine that section of the partition to find out information about the files stored within that partition. See Figure 3.

This FAT area of the first FAT16 partition told us both how many files were stored in the partition, and the clusters for each of them. Knowing this, we could move on to the root directory of the partition to find more information about the files.

The root directory told us lots of information about the files stored within this partition. See Figure 4. From this hex dump we were able to find the following information about each of the four files: file name, file extension, file attributes, file size, starting cluster, and more. We used this information to calculate how many sectors and the starting sector of each file. Knowing this, we could use recovery commands to retrieve the files as seen in Figures 5, 6, 7 and 8. To see the specific information for each file on this partition, see Table 1. To see confirmation that each file was recovered properly, see Figures 21, 22, 23, and 24.

4.2 Techniques Used on Partition 2 (NTFS)

The second partition was a slightly different process since it was an NTFS partition instead of a FAT16. We took a deep dive into the NTFS partition using the Active @ Disk Editor program on our virtual machines. We began by looking at the partition's boot sector like we would for any other partition. Inside the boot sector we found relevant information such as: bytes/sector, sectors/cluster and the reserved sectors. See Figure 9.

Afterwards, with the information we had gathered from looking at the boot sector we were able to calculate the starting sectors for each of the MFT records found in the partition. We then stepped through each MFT record and found all the information relevant to recovering the file. Such as: the file sizes, location, file name, file extension, attributes, non-resident flag, and cluster start. We found two password protected zip files, but we managed to unlock them using the password that we found in Email.docx in partition 1. For the MFT records of each recovered file see Figures 10, 11, 12 and 13. For the recovery commands and the specified file information for the files found in partition 2, see Tables 2 and 3. To see confirmation that each file was recovered and unlocked properly, see Figures 25, 26, 27, and 28.

4.3 Techniques Used on Partition 3 (FAT16)

We used a very similar methodology as partition 1 when tackling the third partition. This was another FAT16 partition, so we knew how to approach it since we had already completed the analysis of the first partition. Once again, the first step was to begin to analyze the reserved area of the partition that held the boot sector. This contained information relevant to the partition like the bytes/sector, sectors/cluster, reserved sectors, and sectors found per FAT area. See Figure 14. With this information along with the information we obtained when first examining the entire disk we were able to calculate the starting sectors for each FAT area found among the partitions just like we did with the first partition.

Using this information from the boot sector we knew where the FAT area and root directory of this partition began. This allowed us to examine the FAT area to find out information about the files stored within the third partition and get to the bottom of this investigation. See Figure 15.

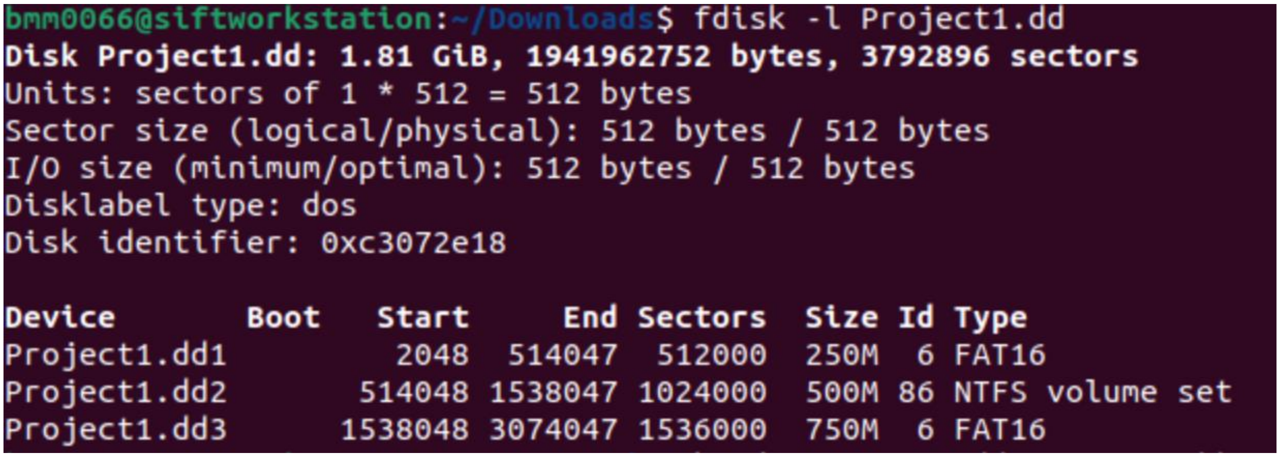
The FAT area of the third partition told us both how many files were stored in the partition, and the clusters for each of them. Knowing this, we could move on to the root directory of the partition to find more information about the total of four files that we found.

Just like with the first partition, the root directory of the third partition told us the necessary information about the files stored within the partition. See Figure 16. From this hex dump we were able to find the following information about each of the four files: file name, file extension, file attributes, file size, starting cluster, and more. Using this information, we calculated the number of sectors that each file took up and which sector they started on.

Knowing this, we used recovery commands to recover all four files stored in this partition. See Figures 17, 18, 19, and 20. However, all the files on this partition were GPG files. GPG files are files that have been encrypted using GNU Privacy Guard, an encryption program. When files are encrypted this way, they’re turned into binary files that require a specified key to decrypt. We were able to find the key to decrypt the GPG files by decoding the ascii string found in the mystery.zip file that we discovered in partition 2. To see the specific information for each file on this partition, see Table 4. To see confirmation each file was recovered and decrypted properly, see Figures 29, 30, 31, and 32.

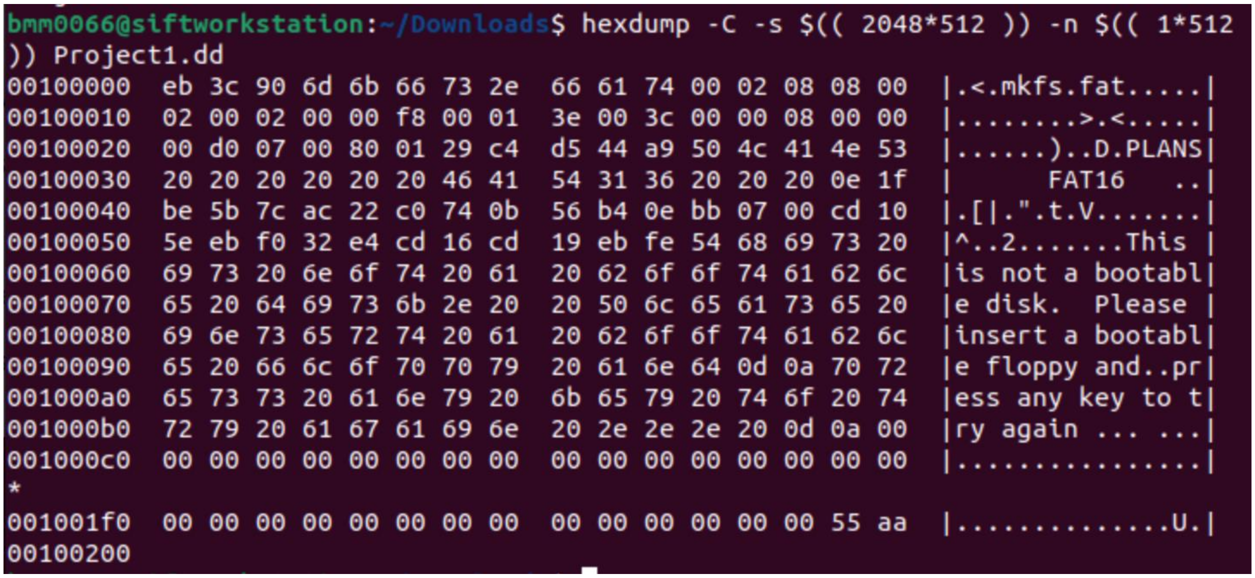
5 Tables and Screenshots

All screenshots referenced are shown here.



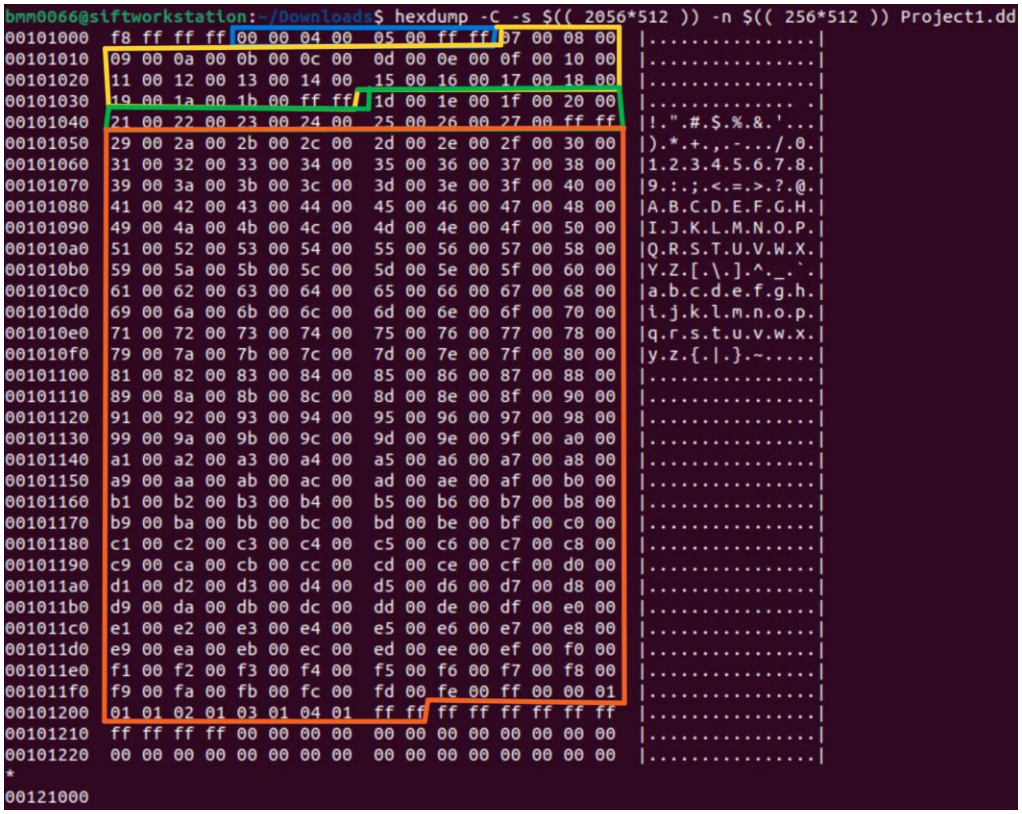
```
bmm0066@siftworkstation:~/Downloads$ fdisk -l Project1.dd
Disk Project1.dd: 1.81 GiB, 1941962752 bytes, 3792896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 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
```

Figure 1: fdisk -l Project1.dd



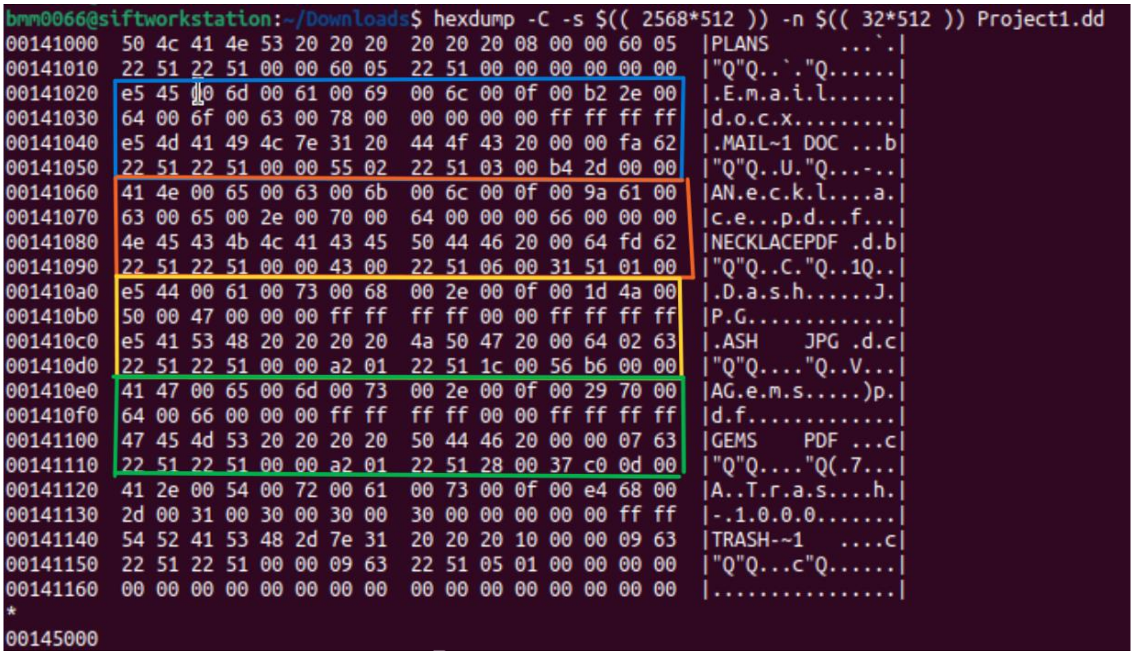
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 2048*512 )) -n $(( 1*512
)) Project1.dd
00100000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 08 08 00  |.<.mkfs.fat.....|
00100010  02 00 02 00 00 f8 00 01  3e 00 3c 00 00 08 00 00  |........>.<.....|
00100020  00 d0 07 00 80 01 29 c4  d5 44 a9 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
```

Figure 2: Boot Sector Partition 1



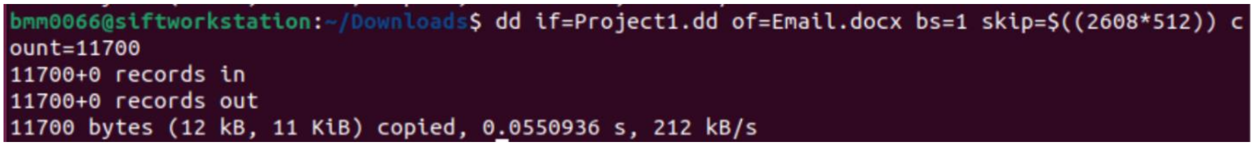
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 2056*512 )) -n $(( 256*512 )) Project1.dd
00101000  f8 ff ff ff 00 00 04 00  05 00 ff ff 07 00 08 00  |................|
00101010  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
00101020  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
00101030  19 00 1a 00 1b 00 ff ff  1d 00 1e 00 1f 00 20 00  |.............. .|
00101040  21 00 22 00 23 00 24 00  25 00 26 00 27 00 ff ff  |!.".#.$.%.&.'...|
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 00 01  |................|
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  |................|
00101220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00121000
```

Figure 3: Partition 1 FAT Area 1



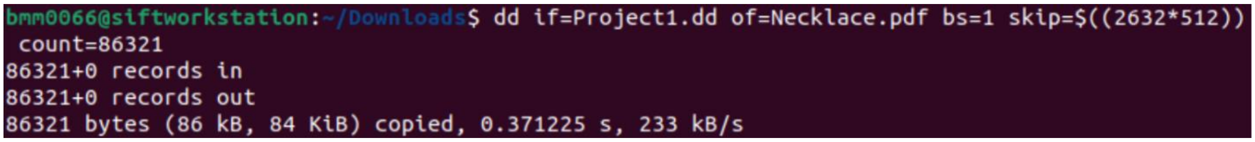
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 2568*512 )) -n $(( 32*512 )) Project1.dd
00141000  50 4c 41 4e 53 20 20 20  20 20 20 08 00 00 60 05  |PLANS      ...`.|
00141010  22 51 22 51 00 00 60 05  22 51 00 00 00 00 00 00  |"Q"Q..`."Q......|
00141020  e5 45 00 6d 00 61 00 69  00 6c 00 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  |"Q"Q...c"Q......|
00141160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00145000
```

Figure 4: Partition 1 Root Directory



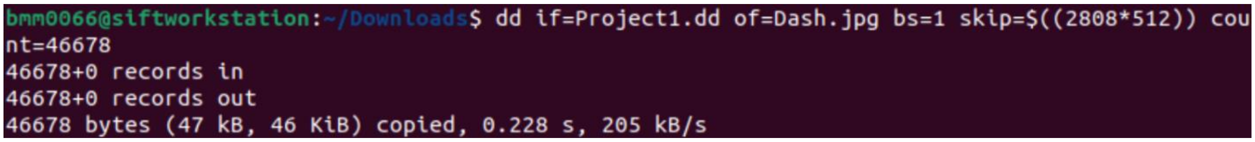
```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Email.docx bs=1 skip=$((2608*512)) c
ount=11700
11700+0 records in
11700+0 records out
11700 bytes (12 kB, 11 KiB) copied, 0.0550936 s, 212 kB/s
```

Figure 5: Email.docx Recovery



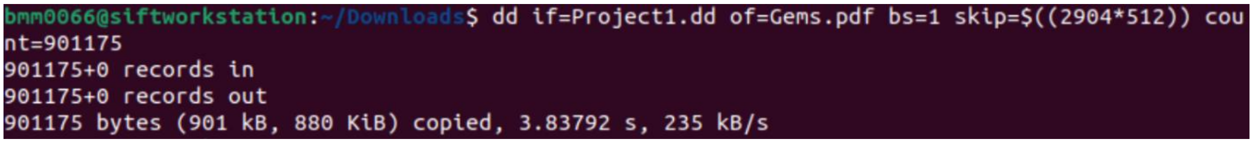
```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Necklace.pdf bs=1 skip=$((2632*512))
 count=86321
86321+0 records in
86321+0 records out
86321 bytes (86 kB, 84 KiB) copied, 0.371225 s, 233 kB/s
```

Figure 6: Necklace.pdf Recovery



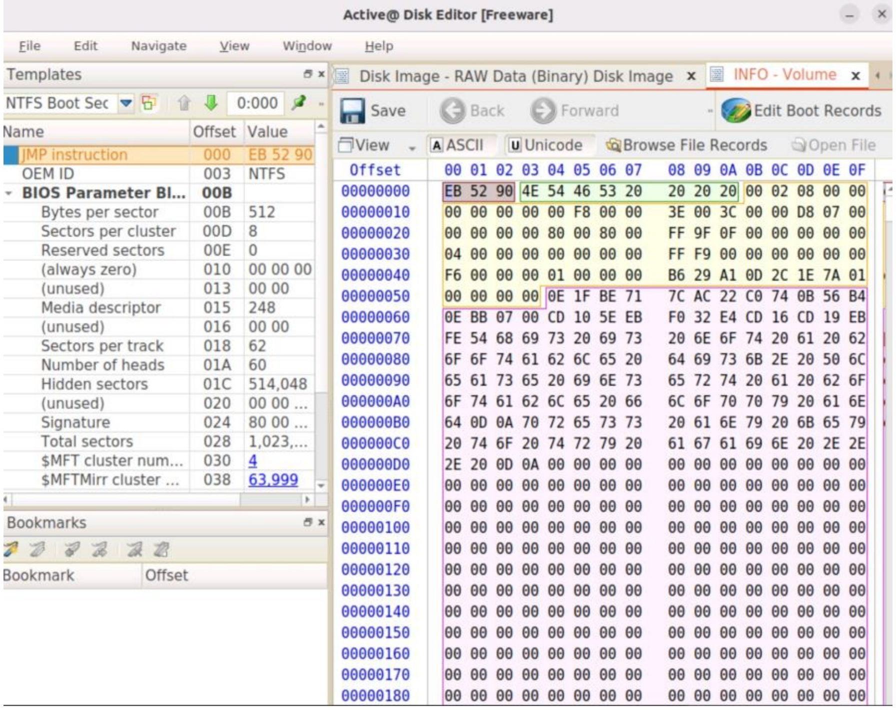
```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Dash.jpg bs=1 skip=$((2808*512)) cou
nt=46678
46678+0 records in
46678+0 records out
46678 bytes (47 kB, 46 KiB) copied, 0.228 s, 205 kB/s
```

Figure 7: Dash.jpg Recovery



```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Gems.pdf bs=1 skip=$((2904*512)) cou
nt=901175
901175+0 records in
901175+0 records out
901175 bytes (901 kB, 880 KiB) copied, 3.83792 s, 235 kB/s
```

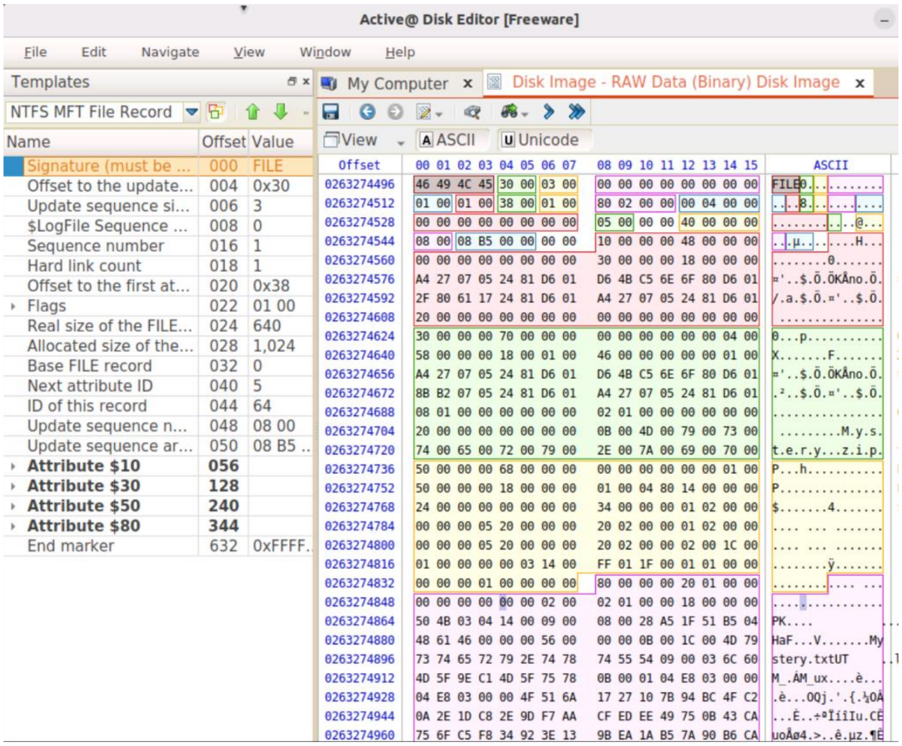
Figure 8: Gems.pdf Recovery



Name	Offset	Value
JMP instruction	000	EB 52 90
OEM ID	003	NTFS
BIOS Parameter Bl...	00B	
Bytes per sector	00B	512
Sectors per cluster	00D	8
Reserved sectors	00E	0
(always zero)	010	00 00 00
(unused)	013	00 00
Media descriptor	015	248
(unused)	016	00 00
Sectors per track	018	62
Number of heads	01A	60
Hidden sectors	01C	514,048
(unused)	020	00 00 ...
Signature	024	80 00 ...
Total sectors	028	1,023,...
$MFT cluster num...	030	4
$MFTMirr cluster ...	038	63,999

```
Offset     00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
00000000   EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00
00000010   00 00 00 00 00 F8 00 00  3E 00 3C 00 00 D8 07 00
00000020   00 00 00 00 80 00 80 00  FF 9F 0F 00 00 00 00 00
00000030   04 00 00 00 00 00 00 00  FF F9 00 00 00 00 00 00
00000040   F6 00 00 00 01 00 00 00  B6 29 A1 0D 2C 1E 7A 01
00000050   00 00 00 00 0E 1F BE 71  7C AC 22 C0 74 0B 56 B4
00000060   0E BB 07 00 CD 10 5E EB  F0 32 E4 CD 16 CD 19 EB
00000070   FE 54 68 69 73 20 69 73  20 6E 6F 74 20 61 20 62
00000080   6F 6F 74 61 62 6C 65 20  64 69 73 6B 2E 20 50 6C
00000090   65 61 73 65 20 69 6E 73  65 72 74 20 61 20 62 6F
000000A0   6F 74 61 62 6C 65 20 66  6C 6F 70 70 79 20 61 6E
000000B0   64 0D 0A 70 72 65 73 73  20 61 6E 79 20 6B 65 79
000000C0   20 74 6F 20 74 72 79 20  61 67 61 69 6E 20 2E 2E
000000D0   2E 20 0D 0A 00 00 00 00  00 00 00 00 00 00 00 00
000000E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

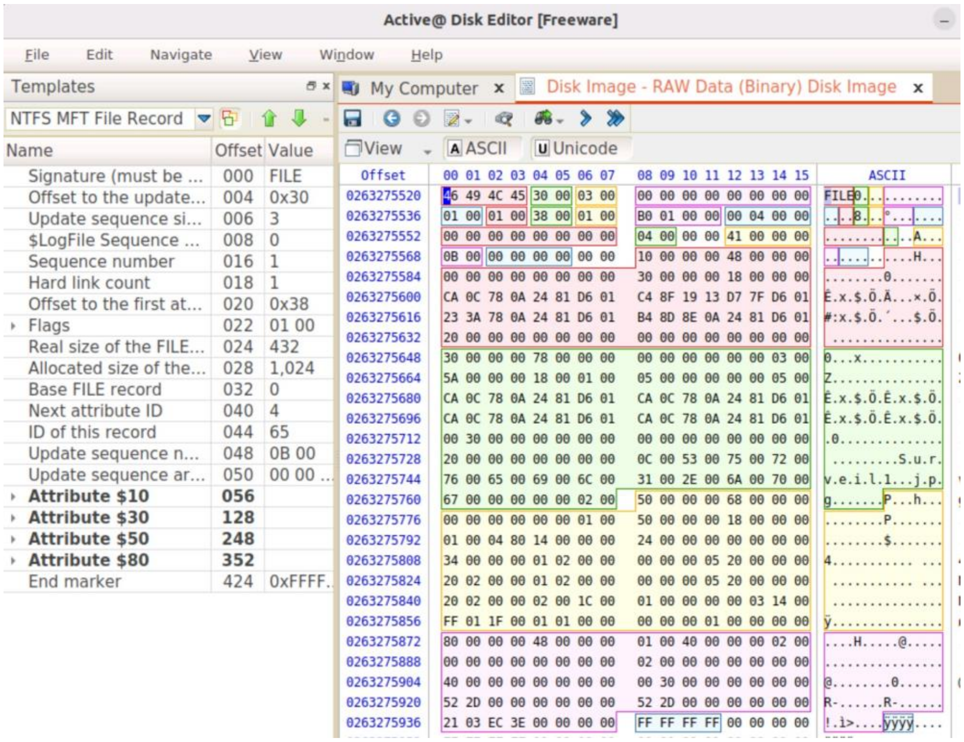
Figure 9: NTFS Boot Sector Partition 2



Name	Offset	Value
Signature (must be ...	000	FILE
Offset to the update...	004	0x30
Update sequence si...	006	3
$LogFile Sequence ...	008	0
Sequence number	016	1
Hard link count	018	1
Offset to the first at...	020	0x38
Flags	022	01 00
Real size of the FILE...	024	640
Allocated size of the...	028	1,024
Base FILE record	032	0
Next attribute ID	040	5
ID of this record	044	64
Update sequence n...	048	08 00
Update sequence ar...	050	08 B5 ..
Attribute $10	**056**	
Attribute $30	**128**	
Attribute $50	**240**	
Attribute $80	**344**	
End marker	632	0xFFFF..

```
Offset      00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15  ASCII
0263274496  46 49 4C 45 30 00 03 00  00 00 00 00 00 00 00 00  FILE0...........
0263274512  01 00 01 00 38 00 01 00  80 02 00 00 00 04 00 00  ....8...........
0263274528  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 00  ..µ.........H...
0263274560  00 00 00 00 00 00 00 00  30 00 00 00 18 00 00 00  ........0.......
0263274576  A4 27 07 05 24 81 D6 01  D6 4B C5 6E 6F 80 D6 01  ¤'..$.Ö.ÖKÅno.Ö.
0263274592  2F 80 61 17 24 81 D6 01  A4 27 07 05 24 81 D6 01  /.a.$.Ö.¤'..$.Ö.
0263274608  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
0263274624  30 00 00 00 70 00 00 00  00 00 00 00 00 00 04 00  0...p...........
0263274640  58 00 00 00 18 00 01 00  46 00 00 00 00 00 01 00  X.......F.......
0263274656  A4 27 07 05 24 81 D6 01  D6 4B C5 6E 6F 80 D6 01  ¤'..$.Ö.ÖKÅno.Ö.
0263274672  8B B2 07 05 24 81 D6 01  A4 27 07 05 24 81 D6 01  .²..$.Ö.¤'..$.Ö.
0263274688  08 01 00 00 00 00 00 00  02 01 00 00 00 00 00 00  ................
0263274704  20 00 00 00 00 00 00 00  0B 00 4D 00 79 00 73 00   .........M.y.s.
0263274720  74 00 65 00 72 00 79 00  2E 00 7A 00 69 00 70 00  t.e.r.y...z.i.p.
0263274736  50 00 00 00 68 00 00 00  00 00 00 00 00 00 01 00  P...h...........
0263274752  50 00 00 00 18 00 00 00  01 00 04 80 14 00 00 00  P...............
0263274768  24 00 00 00 00 00 00 00  34 00 00 00 01 02 00 00  $.......4.......
0263274784  00 00 00 05 20 00 00 00  20 02 00 00 01 02 00 00  .... ... .......
0263274800  00 00 00 05 20 00 00 00  20 02 00 00 02 00 1C 00  .... ... .......
0263274816  01 00 00 00 00 03 14 00  FF 01 1F 00 01 01 00 00  ........ÿ.......
0263274832  00 00 00 01 00 00 00 00  80 00 00 00 20 01 00 00  ............ ...
0263274848  00 00 00 00 00 00 02 00  02 01 00 00 18 00 00 00  ................
0263274864  50 4B 03 04 14 00 09 00  08 00 28 A5 1F 51 B5 04  PK....
0263274880  48 61 46 00 00 00 56 00  00 00 0B 00 1C 00 4D 79  HaF...V.......My
0263274896  73 74 65 72 79 2E 74 78  74 55 54 09 00 03 6C 60  stery.txtUT
0263274912  4D 5F 9E C1 4D 5F 75 78  0B 00 01 04 E8 03 00 00  M_.ÁM_ux....è...
0263274928  04 E8 03 00 00 4F 51 6A  17 27 10 7B 94 BC 4F C2  .è...OQj.'.{.¼OÂ
0263274944  0A 2E 1D C8 2E 9D F7 AA  CF ED EE 49 75 0B 43 CA  ...È..÷ªÏíîIu.CÊ
0263274960  75 6F C5 F8 34 92 3E 13  9B EA 1A B5 7A 90 B6 CA  uoÅø4.>..ê.µz.¶Ê
```

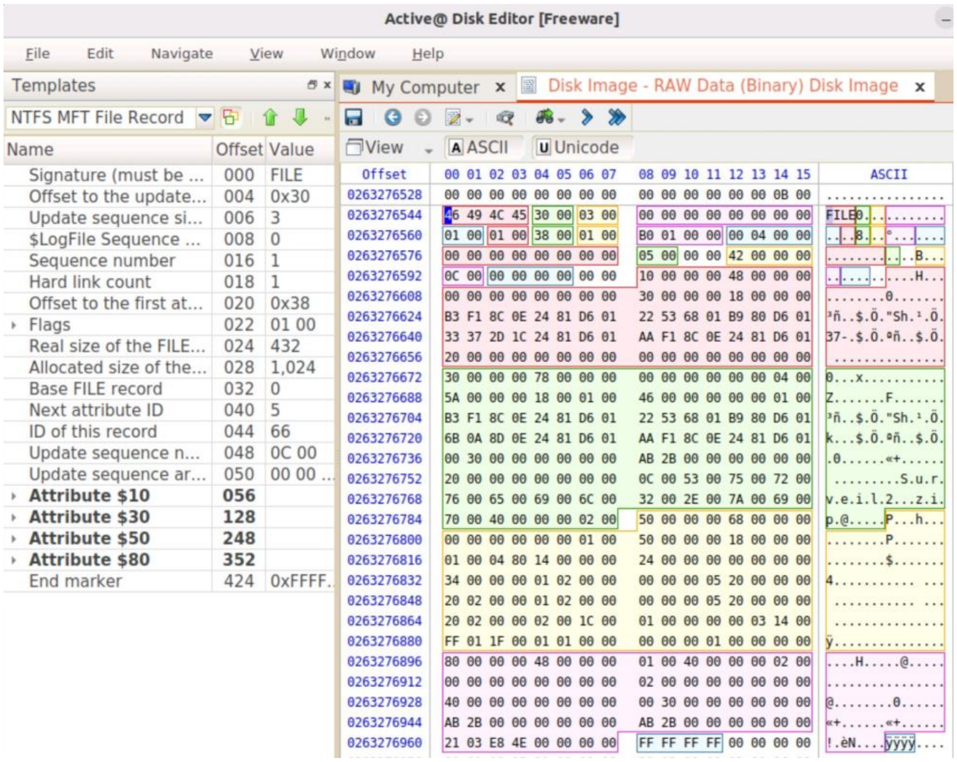
Figure 10: MFT Record for Mystery.zip Partition 2



Name	Offset	Value
Signature (must be ...	000	FILE
Offset to the update...	004	0x30
Update sequence si...	006	3
$LogFile Sequence ...	008	0
Sequence number	016	1
Hard link count	018	1
Offset to the first at...	020	0x38
Flags	022	01 00
Real size of the FILE...	024	432
Allocated size of the...	028	1,024
Base FILE record	032	0
Next attribute ID	040	4
ID of this record	044	65
Update sequence n...	048	0B 00
Update sequence ar...	050	00 00 ...
Attribute $10	**056**	
Attribute $30	**128**	
Attribute $50	**248**	
Attribute $80	**352**	
End marker	424	0xFFFF..

```
Offset      00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15  ASCII
0263275520  46 49 4C 45 30 00 03 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  04 00 00 00 41 00 00 00  ............A...
0263275568  0B 00 00 00 00 00 00 00  10 00 00 00 48 00 00 00  ............H...
0263275584  00 00 00 00 00 00 00 00  30 00 00 00 18 00 00 00  ........0.......
0263275600  CA 0C 78 0A 24 81 D6 01  C4 8F 19 13 D7 7F D6 01  Ê.x.$.Ö.Ä...×.Ö.
0263275616  23 3A 78 0A 24 81 D6 01  B4 8D 8E 0A 24 81 D6 01  #:x.$.Ö.´...$.Ö.
0263275632  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
0263275648  30 00 00 00 78 00 00 00  00 00 00 00 00 00 03 00  0...x...........
0263275664  5A 00 00 00 18 00 01 00  05 00 00 00 00 00 05 00  Z...............
0263275680  CA 0C 78 0A 24 81 D6 01  CA 0C 78 0A 24 81 D6 01  Ê.x.$.Ö.Ê.x.$.Ö.
0263275696  CA 0C 78 0A 24 81 D6 01  CA 0C 78 0A 24 81 D6 01  Ê.x.$.Ö.Ê.x.$.Ö.
0263275712  00 30 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .0..............
0263275728  20 00 00 00 00 00 00 00  0C 00 53 00 75 00 72 00   .........S.u.r.
0263275744  76 00 65 00 69 00 6C 00  31 00 2E 00 6A 00 70 00  v.e.i.l.1...j.p.
0263275760  67 00 00 00 00 00 02 00  50 00 00 00 68 00 00 00  g.......P...h...
0263275776  00 00 00 00 00 00 01 00  50 00 00 00 18 00 00 00  ........P.......
0263275792  01 00 04 80 14 00 00 00  24 00 00 00 00 00 00 00  ........$.......
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 00 03 14 00   ...............
0263275856  FF 01 1F 00 01 01 00 00  00 00 00 01 00 00 00 00  ÿ...............
0263275872  80 00 00 00 48 00 00 00  01 00 40 00 00 00 02 00  ....H.....@.....
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  !.ì>....ÿÿÿÿ....
```

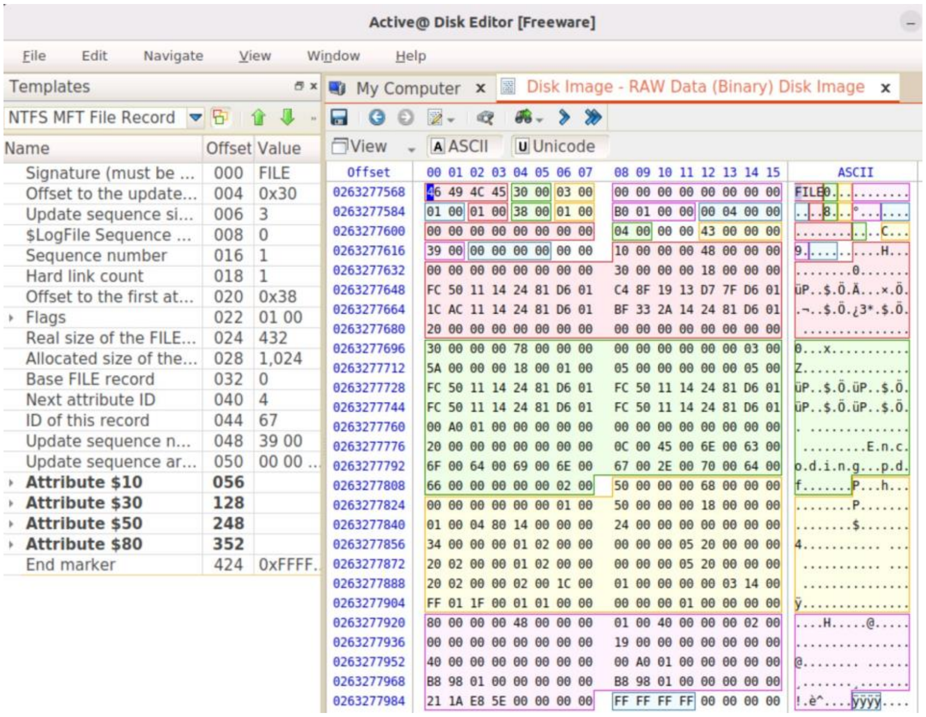
Figure 11: MFT Record for Surveil1.jpg Partition 2



Name	Offset	Value
Signature (must be ...	000	FILE
Offset to the update...	004	0x30
Update sequence si...	006	3
$LogFile Sequence ...	008	0
Sequence number	016	1
Hard link count	018	1
Offset to the first at...	020	0x38
Flags	022	01 00
Real size of the FILE...	024	432
Allocated size of the...	028	1,024
Base FILE record	032	0
Next attribute ID	040	5
ID of this record	044	66
Update sequence n...	048	0C 00
Update sequence ar...	050	00 00 ...
Attribute $10	**056**	
Attribute $30	**128**	
Attribute $50	**248**	
Attribute $80	**352**	
End marker	424	0xFFFF...

```
 Offset     00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15        ASCII
0263276528  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0B 00  ................
0263276544  46 49 4C 45 30 00 03 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  05 00 00 00 42 00 00 00  ............B...
0263276592  0C 00 00 00 00 00 00 00  10 00 00 00 48 00 00 00  ............H...
0263276608  00 00 00 00 00 00 00 00  30 00 00 00 18 00 00 00  ........0.......
0263276624  B3 F1 8C 0E 24 81 D6 01  22 53 68 01 B9 80 D6 01  ³ñ..$.Ö."Sh.¹.Ö.
0263276640  33 37 2D 1C 24 81 D6 01  AA F1 8C 0E 24 81 D6 01  37-.$.Ö.ªñ..$.Ö.
0263276656  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
0263276672  30 00 00 00 78 00 00 00  00 00 00 00 00 00 04 00  0...x...........
0263276688  5A 00 00 00 18 00 01 00  46 00 00 00 00 00 01 00  Z.......F.......
0263276704  B3 F1 8C 0E 24 81 D6 01  22 53 68 01 B9 80 D6 01  ³ñ..$.Ö."Sh.¹.Ö.
0263276720  6B 0A 8D 0E 24 81 D6 01  AA F1 8C 0E 24 81 D6 01  k...$.Ö.ªñ..$.Ö.
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 00   .........S.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 01 00  50 00 00 00 18 00 00 00  ........P.......
0263276816  01 00 04 80 14 00 00 00  24 00 00 00 00 00 00 00  ........$.......
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 00 03 14 00   ...............
0263276880  FF 01 1F 00 01 01 00 00  00 00 00 01 00 00 00 00  ÿ...............
0263276896  80 00 00 00 48 00 00 00  01 00 40 00 00 00 02 00  ....H.....@.....
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....ÿÿÿÿ....
```

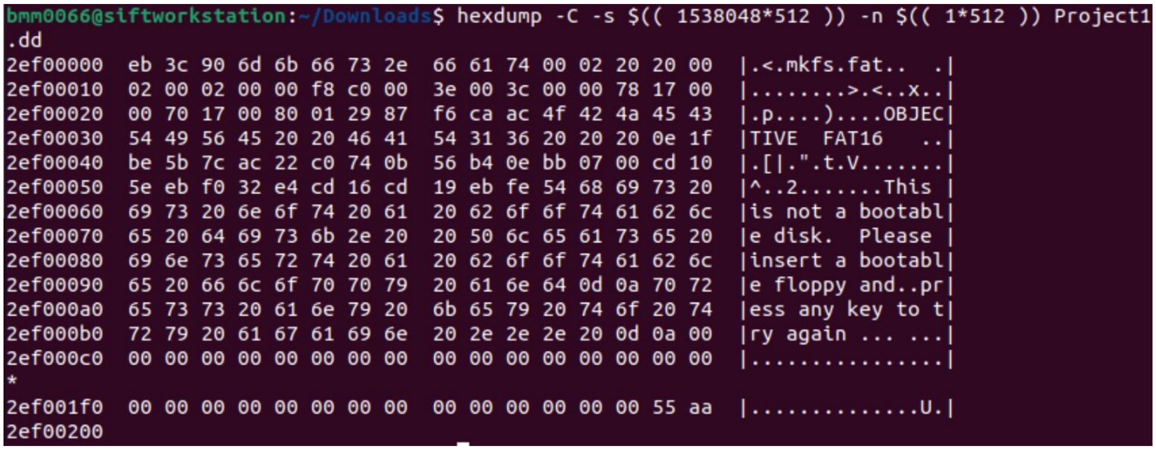
Figure 12: MFT Record for Surveil2.zip Partition 2



Name	Offset	Value
Signature (must be ...	000	FILE
Offset to the update...	004	0x30
Update sequence si...	006	3
$LogFile Sequence ...	008	0
Sequence number	016	1
Hard link count	018	1
Offset to the first at...	020	0x38
Flags	022	01 00
Real size of the FILE...	024	432
Allocated size of the...	028	1,024
Base FILE record	032	0
Next attribute ID	040	4
ID of this record	044	67
Update sequence n...	048	39 00
Update sequence ar...	050	00 00 ...
Attribute $10	**056**	
Attribute $30	**128**	
Attribute $50	**248**	
Attribute $80	**352**	
End marker	424	0xFFFF...

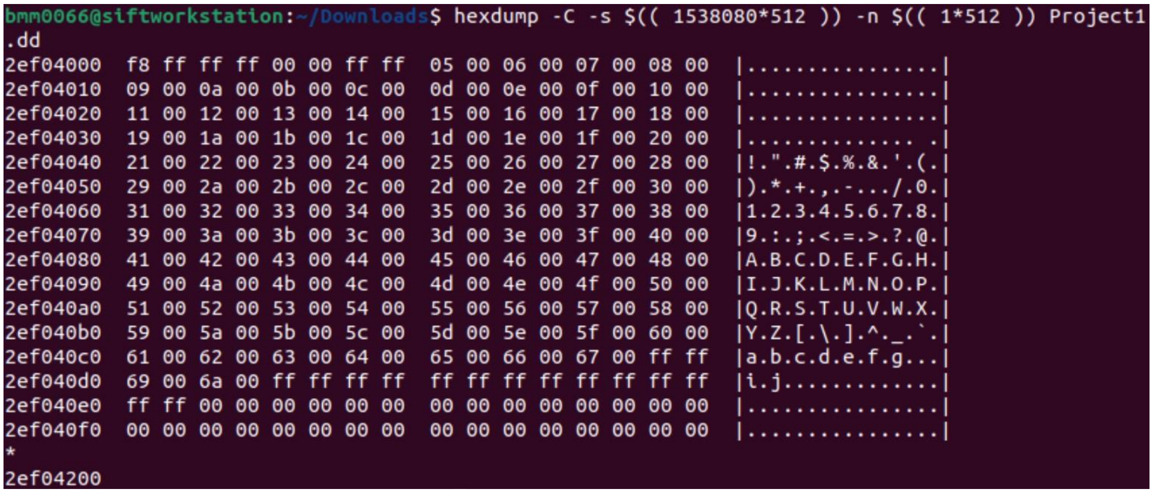
```
 Offset     00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15        ASCII
0263277568  46 49 4C 45 30 00 03 00  00 00 00 00 00 00 00 00  FILE0...........
0263277584  01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00  ....8...°.......
0263277600  00 00 00 00 00 00 00 00  04 00 00 00 43 00 00 00  ............C...
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 00  ........0.......
0263277648  FC 50 11 14 24 81 D6 01  C4 8F 19 13 D7 7F D6 01  üP..$.Ö.Ä...×.Ö.
0263277664  1C AC 11 14 24 81 D6 01  BF 33 2A 14 24 81 D6 01  .¬..$.Ö.¿3*.$.Ö.
0263277680  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
0263277696  30 00 00 00 78 00 00 00  00 00 00 00 00 00 03 00  0...x...........
0263277712  5A 00 00 00 18 00 01 00  05 00 00 00 00 00 05 00  Z...............
0263277728  FC 50 11 14 24 81 D6 01  FC 50 11 14 24 81 D6 01  üP..$.Ö.üP..$.Ö.
0263277744  FC 50 11 14 24 81 D6 01  FC 50 11 14 24 81 D6 01  üP..$.Ö.üP..$.Ö.
0263277760  00 A0 01 00 00 00 00 00  00 00 00 00 00 00 00 00  . ..............
0263277776  20 00 00 00 00 00 00 00  0C 00 45 00 6E 00 63 00   .........E.n.c.
0263277792  6F 00 64 00 69 00 6E 00  67 00 2E 00 70 00 64 00  o.d.i.n.g...p.d.
0263277808  66 00 00 00 00 00 02 00  50 00 00 00 68 00 00 00  f.......P...h...
0263277824  00 00 00 00 00 00 01 00  50 00 00 00 18 00 00 00  ........P.......
0263277840  01 00 04 80 14 00 00 00  24 00 00 00 00 00 00 00  ........$.......
0263277856  34 00 00 00 01 02 00 00  00 00 00 05 20 00 00 00  4........... ...
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  ÿ...............
0263277920  80 00 00 00 48 00 00 00  01 00 40 00 00 00 02 00  ....H.....@.....
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  !.è^....ÿÿÿÿ....
```

Figure 13: MFT Record for Encoding.pdf Partition 2



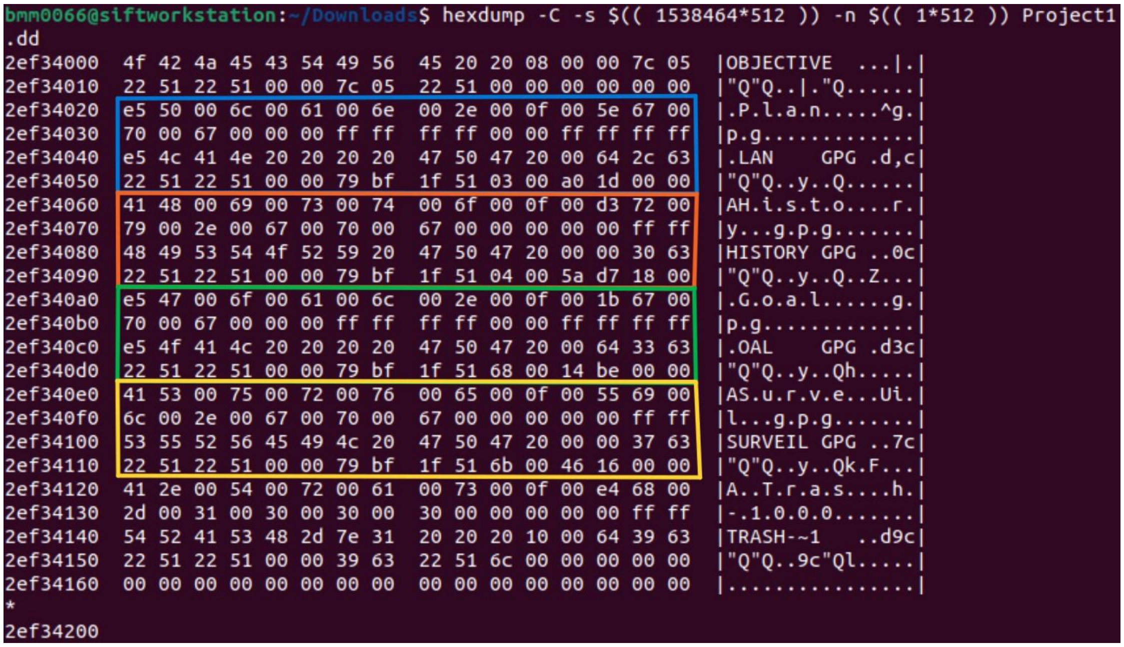
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 1538048*512 )) -n $(( 1*512 )) Project1
.dd
2ef00000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 20 20 00  |.<.mkfs.fat..  .|
2ef00010  02 00 02 00 00 f8 c0 00  3e 00 3c 00 00 78 17 00  |........>.<..x..|
2ef00020  00 70 17 00 80 01 29 87  f6 ca ac 4f 42 4a 45 43  |.p....)....OBJEC|
2ef00030  54 49 56 45 20 20 46 41  54 31 36 20 20 20 0e 1f  |TIVE  FAT16   ..|
2ef00040  be 5b 7c ac 22 c0 74 0b  56 b4 0e bb 07 00 cd 10  |.[|.".t.V.......|
2ef00050  5e eb f0 32 e4 cd 16 cd  19 eb fe 54 68 69 73 20  |^..2.......This |
2ef00060  69 73 20 6e 6f 74 20 61  20 62 6f 6f 74 61 62 6c  |is not a bootabl|
2ef00070  65 20 64 69 73 6b 2e 20  20 50 6c 65 61 73 65 20  |e disk.  Please |
2ef00080  69 6e 73 65 72 74 20 61  20 62 6f 6f 74 61 62 6c  |insert a bootabl|
2ef00090  65 20 66 6c 6f 70 70 79  20 61 6e 64 0d 0a 70 72  |e floppy and..pr|
2ef000a0  65 73 73 20 61 6e 79 20  6b 65 79 20 74 6f 20 74  |ess any key to t|
2ef000b0  72 79 20 61 67 61 69 6e  20 2e 2e 2e 20 0d 0a 00  |ry again ... ...|
2ef000c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
2ef001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
2ef00200
```

Figure 14: Boot Sector Partition 3



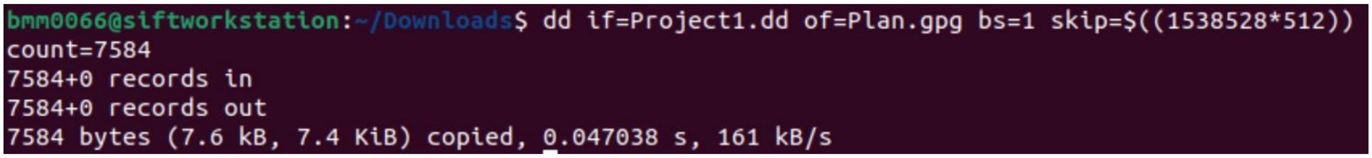
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 1538080*512 )) -n $(( 1*512 )) Project1
.dd
2ef04000  f8 ff ff ff 00 00 ff ff  05 00 06 00 07 00 08 00  |................|
2ef04010  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
2ef04020  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
2ef04030  19 00 1a 00 1b 00 1c 00  1d 00 1e 00 1f 00 20 00  |.............. .|
2ef04040  21 00 22 00 23 00 24 00  25 00 26 00 27 00 28 00  |!.".#.$.%.&.'.(.|
2ef04050  29 00 2a 00 2b 00 2c 00  2d 00 2e 00 2f 00 30 00  |).*.+.,.-.../.0.|
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 ff ff ff  ff ff ff ff ff ff ff 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
```

Figure 15: FAT Area 1 Partition 3



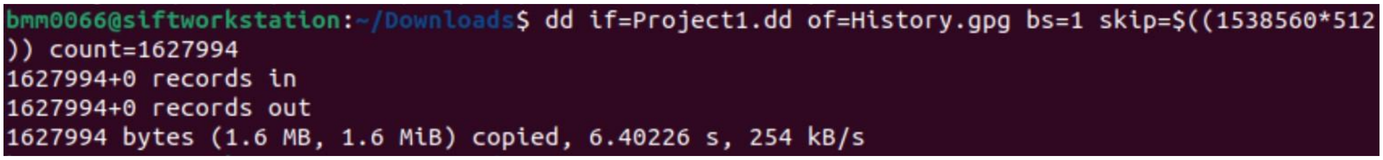
```
bmm0066@siftworkstation:~/Downloads$ hexdump -C -s $(( 1538464*512 )) -n $(( 1*512 )) Project1
.dd
2ef34000  4f 42 4a 45 43 54 49 56  45 20 20 08 00 00 7c 05  |OBJECTIVE  ...|.|
2ef34010  22 51 22 51 00 00 7c 05  22 51 00 00 00 00 00 00  |"Q"Q..|."Q......|
2ef34020  e5 50 00 6c 00 61 00 6e  00 2e 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 .d,c|
2ef34050  22 51 22 51 00 00 79 bf  1f 51 03 00 a0 1d 00 00  |"Q"Q..y..Q......|
2ef34060  41 48 00 69 00 73 00 74  00 6f 00 0f 00 d3 72 00  |AH.i.s.t.o....r.|
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 00 30 63  |HISTORY GPG ..0c|
2ef34090  22 51 22 51 00 00 79 bf  1f 51 04 00 5a d7 18 00  |"Q"Q..y..Q..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"Q..y..Qh.....|
2ef340e0  41 53 00 75 00 72 00 76  00 65 00 0f 00 55 69 00  |AS.u.r.v.e...Ui.|
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"Q..y..Qk.F...|
2ef34120  41 2e 00 54 00 72 00 61  00 73 00 0f 00 e4 68 00  |A..T.r.a.s....h.|
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"Q..9c"Ql.....|
2ef34160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
2ef34200
```

Figure 16: Root Directory Partition 3



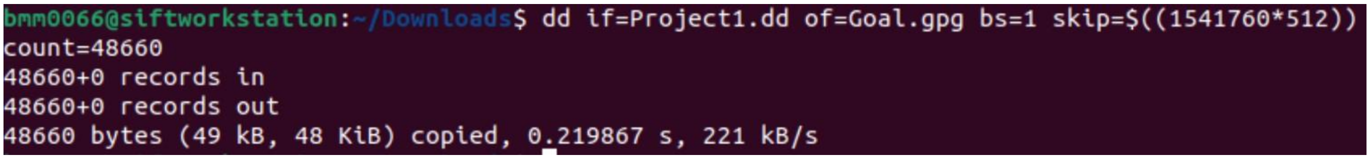
```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Plan.gpg bs=1 skip=$((1538528*512))
count=7584
7584+0 records in
7584+0 records out
7584 bytes (7.6 kB, 7.4 KiB) copied, 0.047038 s, 161 kB/s
```

Figure 17: Plan.gpg Recovery Command



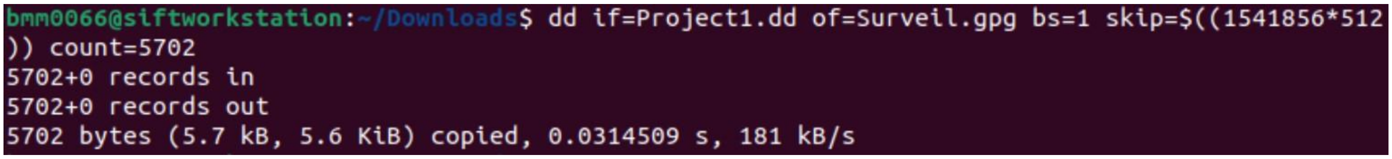
```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=History.gpg bs=1 skip=$((1538560*512
)) count=1627994
1627994+0 records in
1627994+0 records out
1627994 bytes (1.6 MB, 1.6 MiB) copied, 6.40226 s, 254 kB/s
```

Figure 18: History.gpg Recovery Command



```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Goal.gpg bs=1 skip=$((1541760*512))
count=48660
48660+0 records in
48660+0 records out
48660 bytes (49 kB, 48 KiB) copied, 0.219867 s, 221 kB/s
```

Figure 19: Goal.gpg Recovery Command



```
bmm0066@siftworkstation:~/Downloads$ dd if=Project1.dd of=Surveil.gpg bs=1 skip=$((1541856*512
)) count=5702
5702+0 records in
5702+0 records out
5702 bytes (5.7 kB, 5.6 KiB) copied, 0.0314509 s, 181 kB/s
```

Figure 20: Surveil.gpg Recovery Command

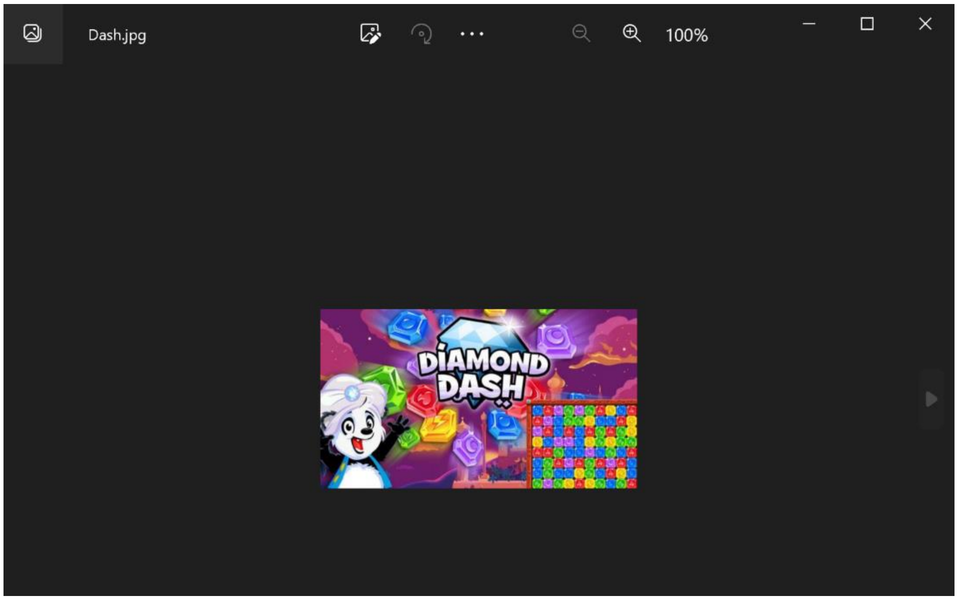
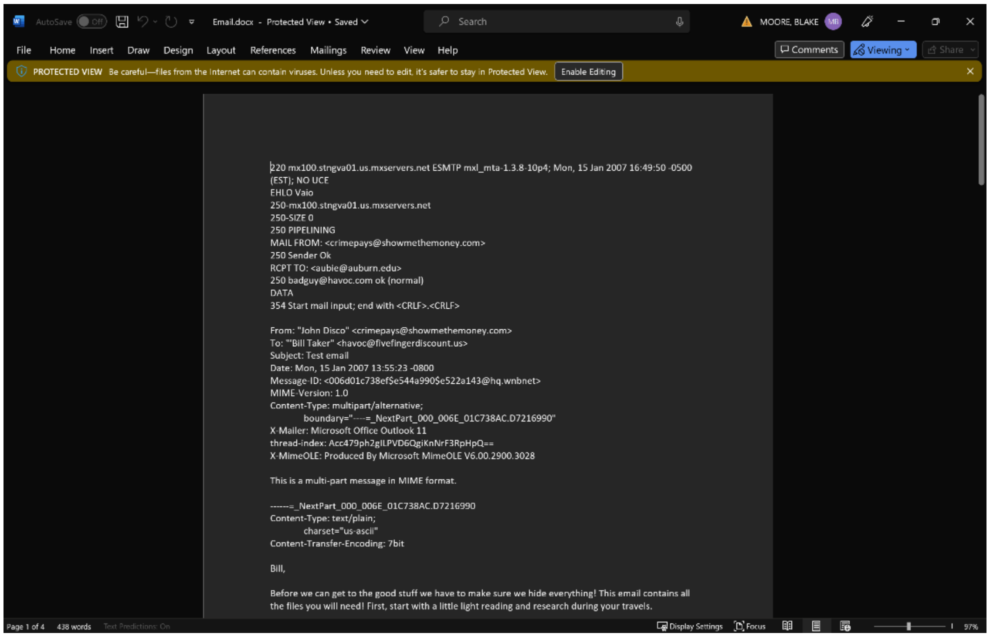


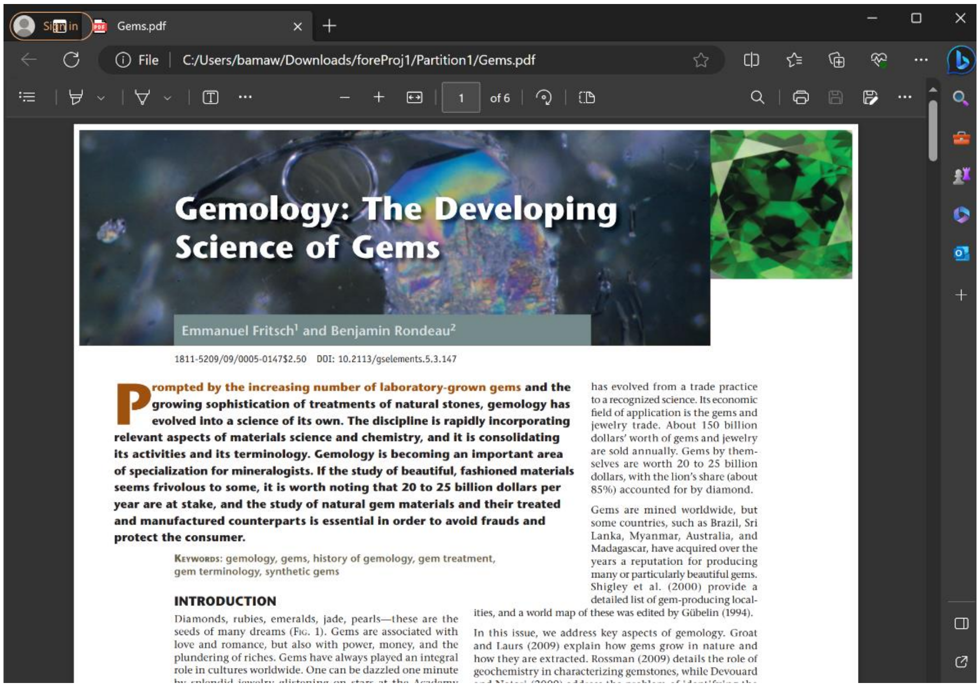
Figure 21: Dash.jpg Recovery Confirmation



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

```
220 mx100.stngva01.us.mxservers.net ESMTP mxl_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:49:50 -0500
(EST); NO UCE
EHLO Vaio
250-mx100.stngva01.us.mxservers.net
250-SIZE 0
250 PIPELINING
MAIL FROM: <crimepays@showmethemoney.com>
250 Sender Ok
RCPT TO: <aubie@auburn.edu>
250 badguy@havoc.com ok (normal)
DATA
354 Start mail input; end with <CRLF>.<CRLF>

From: "John Disco" <crimepays@showmethemoney.com>
To: "'Bill Taker" <havoc@fivefingerdiscount.us>
Subject: Test email
Date: Mon, 15 Jan 2007 13:55:23 -0800
Message-ID: <006d01c738ef$e544a990$e522a143@hq.wnbnet>
MIME-Version: 1.0
Content-Type: multipart/alternative;
          boundary="----=_NextPart_000_006E_01C738AC.D7216990"
X-Mailer: Microsoft Office Outlook 11
thread-index: Acc479ph2gILPVD6QgiKnNrF3RpHpQ==
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028

This is a multi-part message in MIME format.

------=_NextPart_000_006E_01C738AC.D7216990
Content-Type: text/plain;
          charset="us-ascii"
Content-Transfer-Encoding: 7bit

Bill,

Before we can get to the good stuff we have to make sure we hide everything! This email contains all
the files you will need! First, start with a little light reading and research during your travels.
```

Figure 22: Email.docx Recovery Confirmation



C:/Users/bamaw/Downloads/foreProj1/Partition1/Gems.pdf

Gemology: The Developing Science of Gems

Emmanuel Fritsch[1] and Benjamin Rondeau[2]

1811-5209/09/0005-0147$2.50 DOI: 10.2113/gselements.5.3.147

Prompted by the increasing number of laboratory-grown gems and the growing sophistication of treatments of natural stones, gemology has evolved into a science of its own. The discipline is rapidly incorporating relevant aspects of materials science and chemistry, and it is consolidating its activities and its terminology. Gemology is becoming an important area of specialization for mineralogists. If the study of beautiful, fashioned materials seems frivolous to some, it is worth noting that 20 to 25 billion dollars per year are at stake, and the study of natural gem materials and their treated and manufactured counterparts is essential in order to avoid frauds and protect the consumer.

Keywords: gemology, gems, history of gemology, gem treatment, gem terminology, synthetic gems

INTRODUCTION

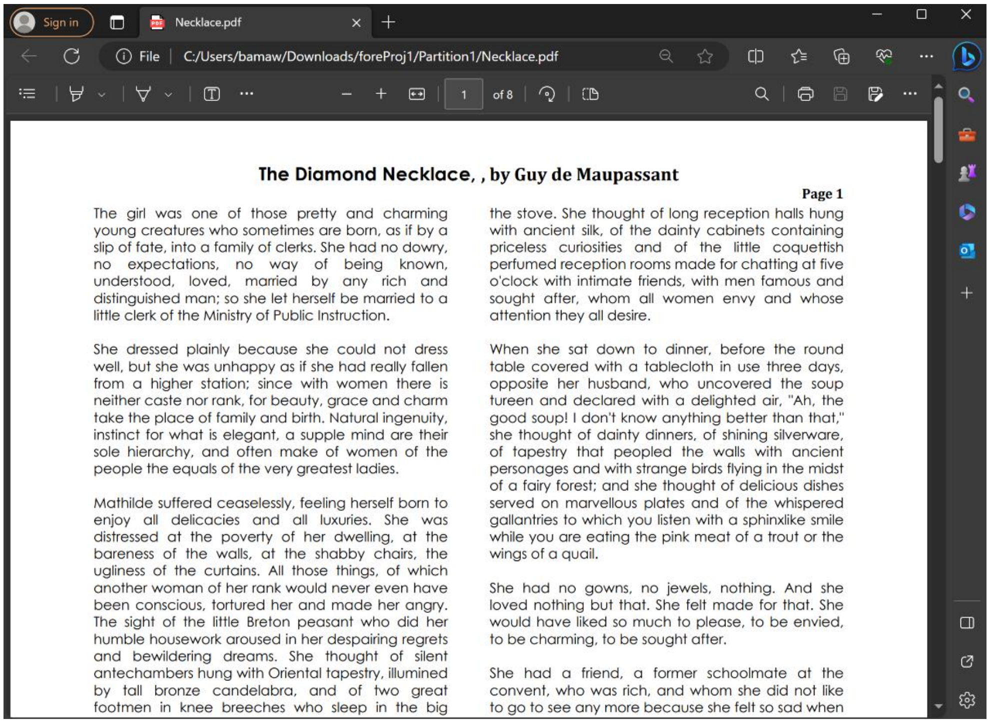
Diamonds, rubies, emeralds, jade, pearls—these are the seeds of many dreams (Fig. 1). Gems are associated with love and romance, but also with power, money, and the plundering of riches. Gems have always played an integral role in cultures worldwide. One can be dazzled one minute

has evolved from a trade practice to a recognized science. Its economic field of application is the gems and jewelry trade. About 150 billion dollars' worth of gems and jewelry are sold annually. Gems by themselves are worth 20 to 25 billion dollars, with the lion's share (about 85%) accounted for by diamond.

Gems are mined worldwide, but some countries, such as Brazil, Sri Lanka, Myanmar, Australia, and Madagascar, have acquired over the years a reputation for producing many or particularly beautiful gems. Shigley et al. (2000) provide a detailed list of gem-producing localities, and a world map of these was edited by Gübelin (1994).

In this issue, we address key aspects of gemology. Groat and Laurs (2009) explain how gems grow in nature and how they are extracted. Rossman (2009) details the role of geochemistry in characterizing gemstones, while Devouard

Figure 23: Gems.pdf Recovery Confirmation



C:/Users/bamaw/Downloads/foreProj1/Partition1/Necklace.pdf

The Diamond Necklace, , by Guy de Maupassant

Page 1

The girl was one of those pretty and charming young creatures who sometimes are born, as if by a slip of fate, into a family of clerks. She had no dowry, no expectations, no way of being known, understood, loved, married by any rich and distinguished man; so she let herself be married to a little clerk of the Ministry of Public Instruction.

She dressed plainly because she could not dress well, but she was unhappy as if she had really fallen from a higher station; since with women there is neither caste nor rank, for beauty, grace and charm take the place of family and birth. Natural ingenuity, instinct for what is elegant, a supple mind are their sole hierarchy, and often make of women of the people the equals of the very greatest ladies.

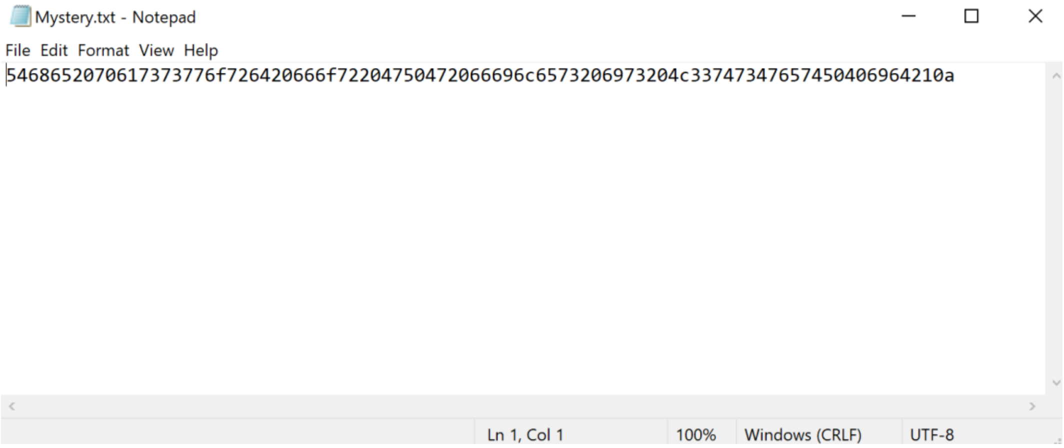
Mathilde suffered ceaselessly, feeling herself born to enjoy all delicacies and all luxuries. She was distressed at the poverty of her dwelling, at the bareness of the walls, at the shabby chairs, the ugliness of the curtains. All those things, of which another woman of her rank would never even have been conscious, tortured her and made her angry. The sight of the little Breton peasant who did her humble housework aroused in her despairing regrets and bewildering dreams. She thought of silent antechambers hung with Oriental tapestry, illumined by tall bronze candelabra, and of two great footmen in knee breeches who sleep in the big the stove. She thought of long reception halls hung with ancient silk, of the dainty cabinets containing priceless curiosities and of the little coquettish perfumed reception rooms made for chatting at five o'clock with intimate friends, with men famous and sought after, whom all women envy and whose attention they all desire.

When she sat down to dinner, before the round table covered with a tablecloth in use three days, opposite her husband, who uncovered the soup tureen and declared with a delighted air, "Ah, the good soup! I don't know anything better than that," she thought of dainty dinners, of shining silverware, of tapestry that peopled the walls with ancient personages and with strange birds flying in the midst of a fairy forest; and she thought of delicious dishes served on marvellous plates and of the whispered gallantries to which you listen with a sphinxlike smile while you are eating the pink meat of a trout or the wings of a quail.

She had no gowns, no jewels, nothing. And she loved nothing but that. She felt made for that. She would have liked so much to please, to be envied, to be charming, to be sought after.

She had a friend, a former schoolmate at the convent, who was rich, and whom she did not like to go to see any more because she felt so sad when

Figure 24: Necklace.pdf Recovery Confirmation



```
5468652070617373776f726420666f72204750472066696c6573206973204c33747347657450406964210a
```

Figure 25: Mystery.zip/Mystery.txt Recovery Confirmation

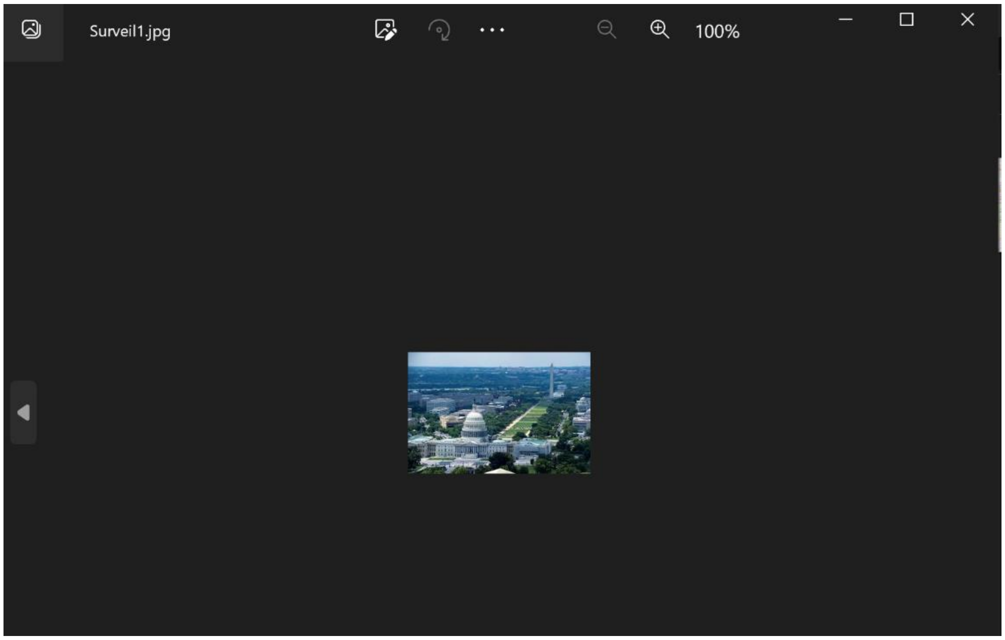


Figure 26: Surveil1.jpg Recovery Confirmation

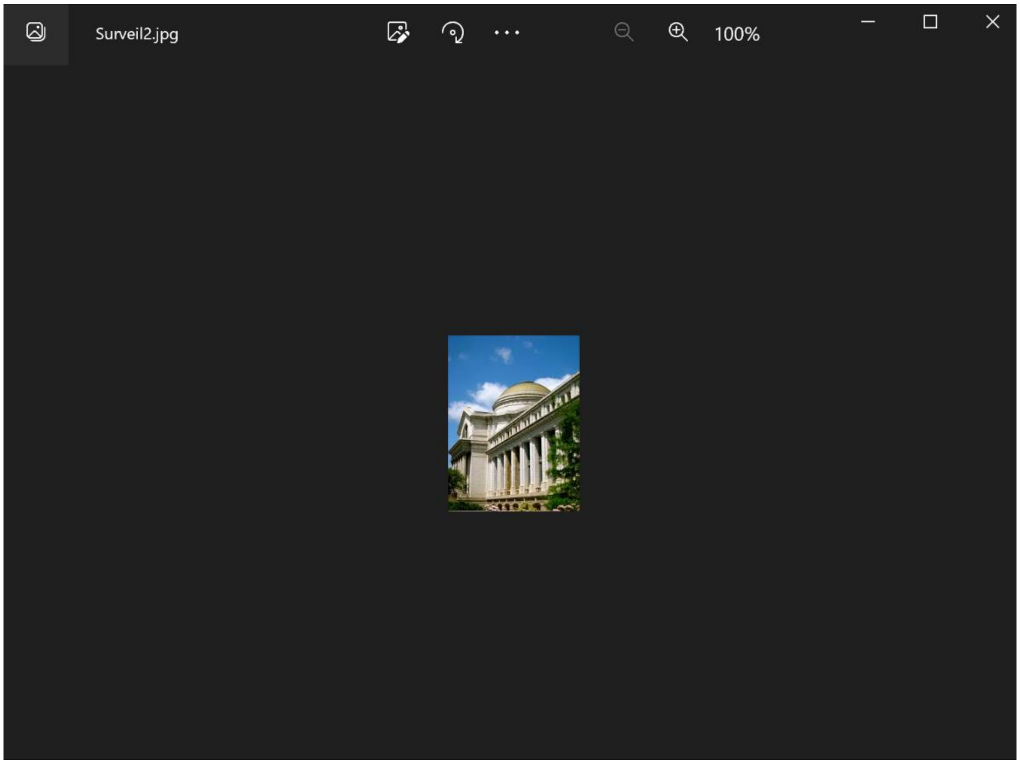
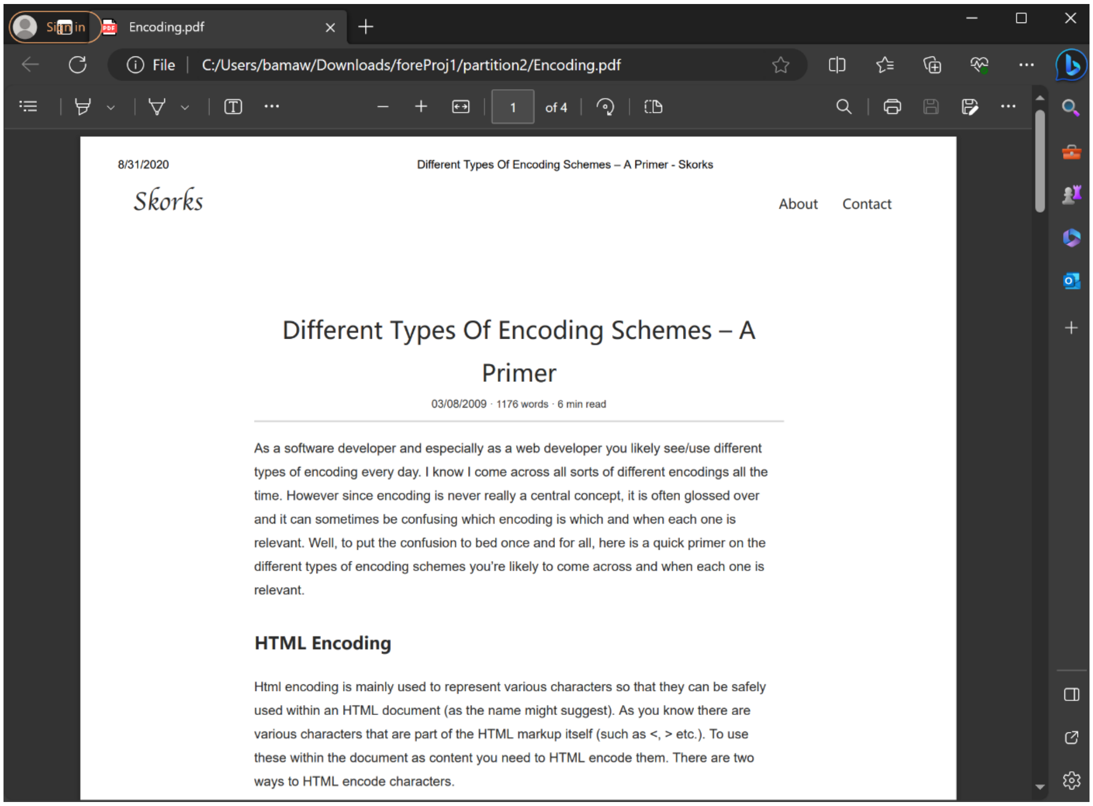


Figure 27: Surveil2.zip/Surveil2.jpg Recovery Confirmation



8/31/2020 Different Types Of Encoding Schemes – A Primer - Skorks

Skorks

About Contact

Different Types Of Encoding Schemes – A Primer

03/08/2009 · 1176 words · 6 min read

As a software developer and especially as a web developer you likely see/use different types of encoding every day. I know I come across all sorts of different encodings all the time. However since encoding is never really a central concept, it is often glossed over and it can sometimes be confusing which encoding is which and when each one is relevant. Well, to put the confusion to bed once and for all, here is a quick primer on the different types of encoding schemes you're likely to come across and when each one is relevant.

HTML Encoding

Html encoding is mainly used to represent various characters so that they can be safely used within an HTML document (as the name might suggest). As you know there are various characters that are part of the HTML markup itself (such as <, > etc.). To use these within the document as content you need to HTML encode them. There are two ways to HTML encode characters.

Figure 28: Encoding.pdf Recovery Confirmation

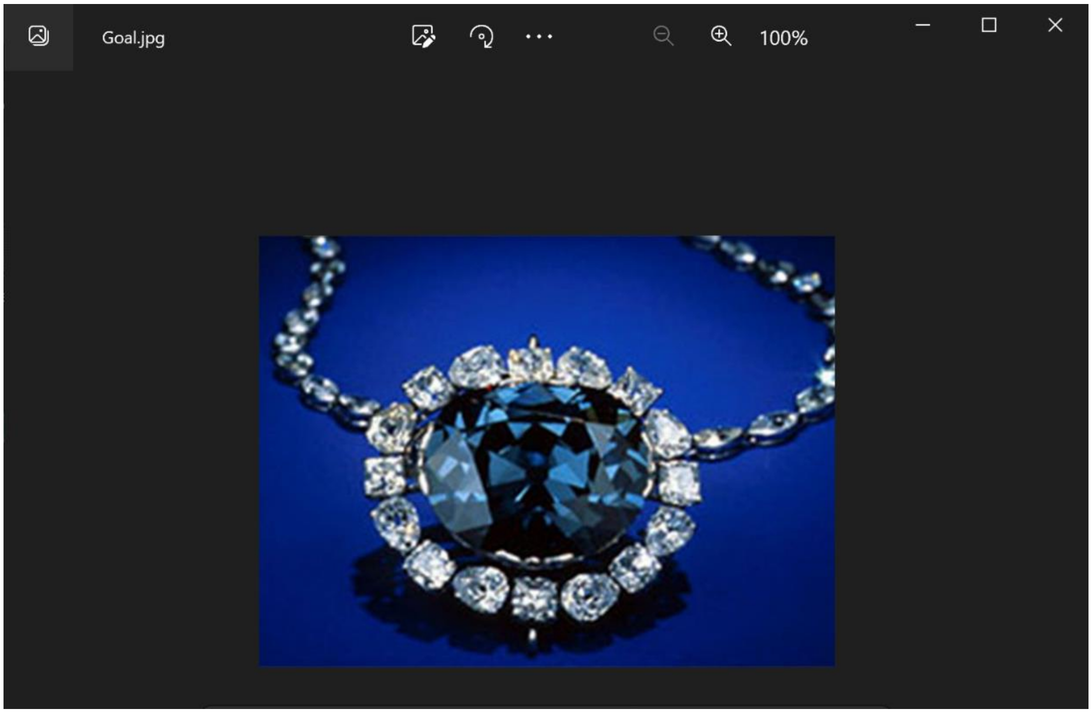
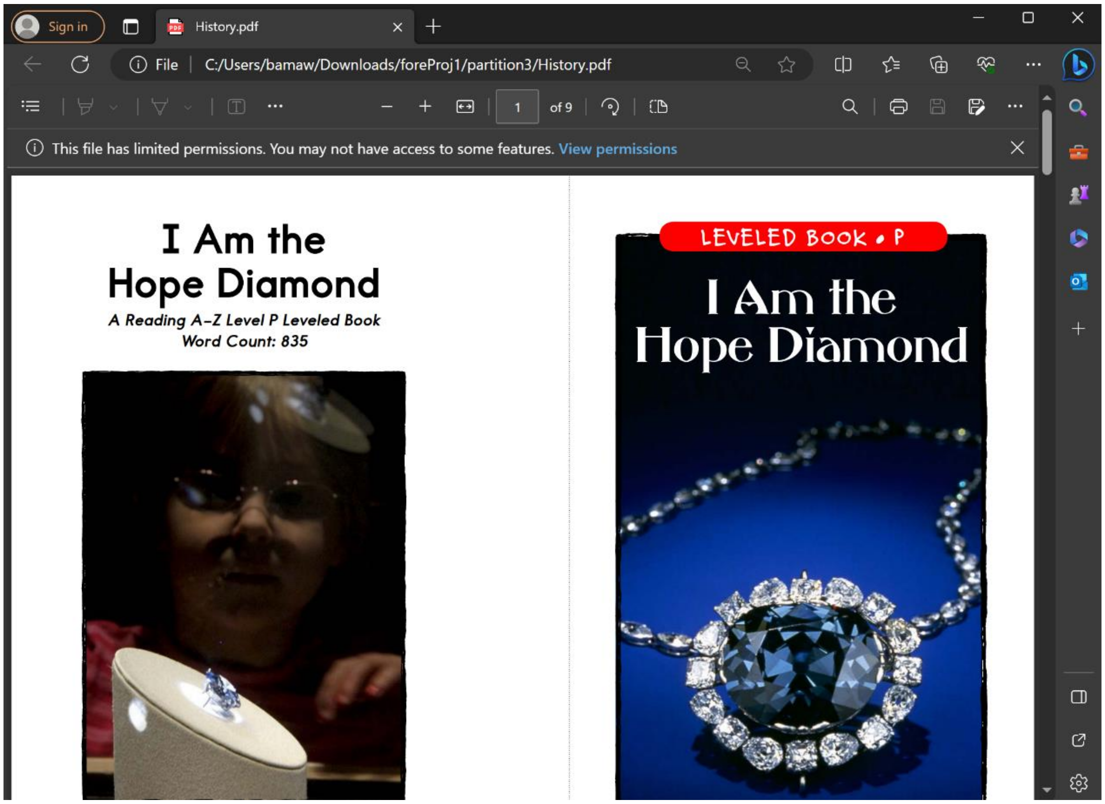


Figure 29: Goal.gpg/Goal.jpg Recovery Confirmation



C:/Users/bamaw/Downloads/foreProj1/partition3/History.pdf

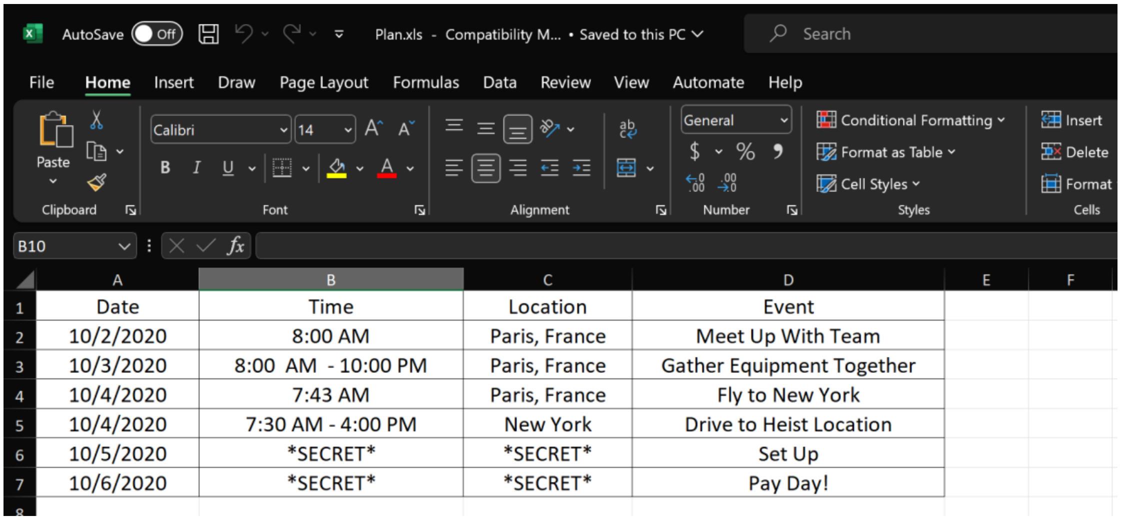
This file has limited permissions. You may not have access to some features. View permissions

I Am the Hope Diamond

A Reading A–Z Level P Leveled Book
Word Count: 835

I Am the Hope Diamond

Figure 30: History.gpg/History.pdf Recovery Confirmation



	A	B	C	D
1	Date	Time	Location	Event
2	10/2/2020	8:00 AM	Paris, France	Meet Up With Team
3	10/3/2020	8:00 AM - 10:00 PM	Paris, France	Gather Equipment Together
4	10/4/2020	7:43 AM	Paris, France	Fly to New York
5	10/4/2020	7:30 AM - 4:00 PM	New York	Drive to Heist Location
6	10/5/2020	*SECRET*	*SECRET*	Set Up
7	10/6/2020	*SECRET*	*SECRET*	Pay Day!

Figure 31: Plan.gpg/Plan.xls Recovery Confirmation

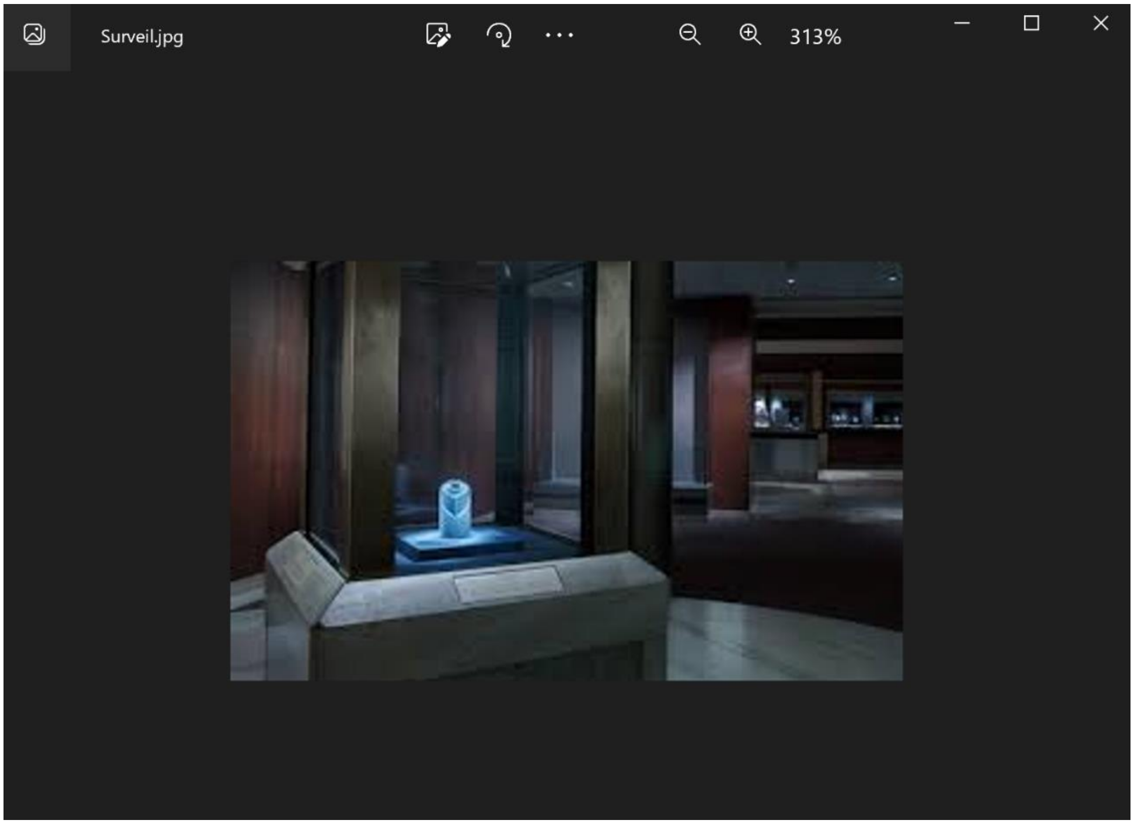
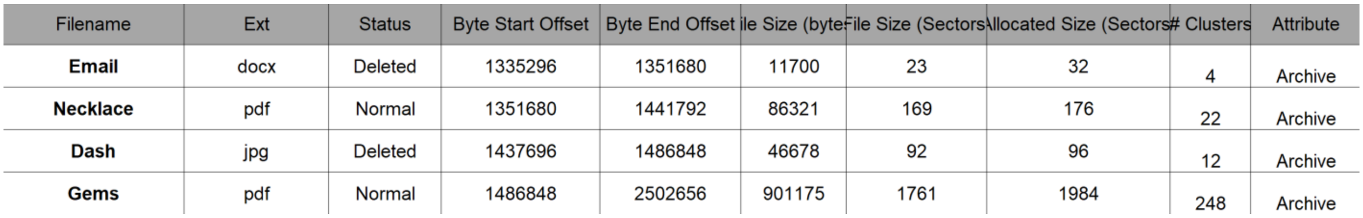
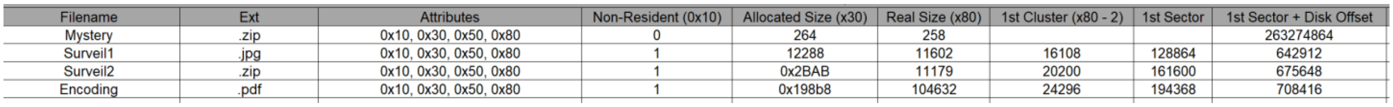


Figure 32: Surveil.gpg/Surveil.jpg Recovery Confirmation



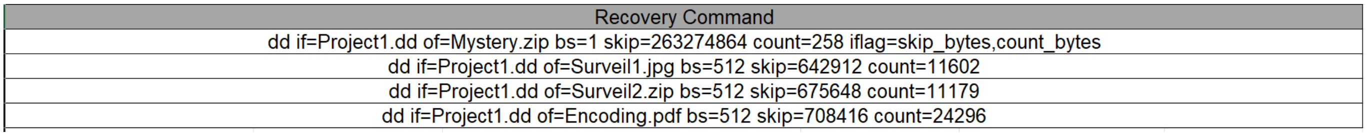
Filename	Ext	Status	Byte Start Offset	Byte End Offset	ile Size (byte	File Size (Sectors	llocated Size (Sectors	# Clusters	Attribute
Email	docx	Deleted	1335296	1351680	11700	23	32	4	Archive
Necklace	pdf	Normal	1351680	1441792	86321	169	176	22	Archive
Dash	jpg	Deleted	1437696	1486848	46678	92	96	12	Archive
Gems	pdf	Normal	1486848	2502656	901175	1761	1984	248	Archive

Table 1: Specific File Information Partition 1



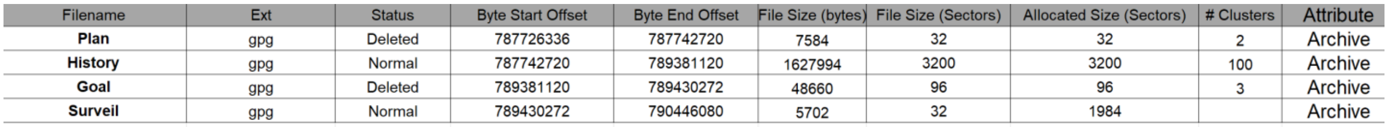
Filename	Ext	Attributes	Non-Resident (0x10)	Allocated Size (x30)	Real Size (x80)	1st Cluster (x80 - 2)	1st Sector	1st Sector + Disk Offset
Mystery	.zip	0x10, 0x30, 0x50, 0x80	0	264	258			263274864
Surveil1	.jpg	0x10, 0x30, 0x50, 0x80	1	12288	11602	16108	128864	642912
Surveil2	.zip	0x10, 0x30, 0x50, 0x80	1	0x2BAB	11179	20200	161600	675648
Encoding	.pdf	0x10, 0x30, 0x50, 0x80	1	0x198b8	104632	24296	194368	708416

Table 2: Specific File Information Partition 2



Recovery Command
dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258 iflag=skip_bytes,count_bytes
dd if=Project1.dd of=Surveil1.jpg bs=512 skip=642912 count=11602
dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=11179
dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=24296

Table 3: Recovery Commands for Files Partition 2



Filename	Ext	Status	Byte Start Offset	Byte End Offset	File Size (bytes)	File Size (Sectors)	Allocated Size (Sectors)	# Clusters	Attribute
Plan	gpg	Deleted	787726336	787742720	7584	32	32	2	Archive
History	gpg	Normal	787742720	789381120	1627994	3200	3200	100	Archive
Goal	gpg	Deleted	789381120	789430272	48660	96	96	3	Archive
Surveil	gpg	Normal	789430272	790446080	5702	32	1984		Archive

Table 4: Specific File Information Partition 3

Executive Summary Table

Partition	Filename	Ext	Attribute	Status	Byte Offset	File Size	Recovery Command
FAT16 (Partition 1)	Email	doc	Archive	Deleted	1335296	11700	dd if=Project1.dd of=Email.docx bs=1 skip=$((2608*512)) count=11700
FAT16 (Partition 1)	Necklace	pdf	Archive	Normal File	1351680	86321	dd if=Project1.dd of=Necklace.pdf bs=1 skip=$((2640*512)) count=86321
FAT16 (Partition 1)	Dash	jpg	Archive	Deleted	1437696	46678	dd if=Project1.dd of=Dash.jpg bs=1 skip=$((2808 * 512)) count=46678
FAT16 (Partition 1)	Gems	pdf	Archive	Normal File	1486848	901175	dd if=Project1.dd of=Gems.pdf bs=1 skip=$((2904*512)) count=901175
NTFS (Partition 2)	Mystery	zip	0x10, 0x30, 0x50, 0x80	Normal File	263274864	258	dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=24296
NTFS (Partition 2)	Surveil1	jpg	0x10, 0x30, 0x50, 0x80	Normal File	329170944	11602	dd if=Project1.dd of=Surveil1.jpg bs=512 skip=642912 count=11602
NTFS (Partition 2)	Surveil2	zip	0x10, 0x30, 0x50, 0x80	Normal File	345931776	11179	dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=11179
NTFS (Partition 2)	Encoding	pdf	0x10, 0x30, 0x50, 0x80	Normal File	362708992	104632	dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258 iflag=skip_bytes,count_bytes
FAT16 (Partition 2)	Plan	gpg	Archive	Deleted	787726336	7584	dd if=Project1.dd of=Plan.gpg bs=1 skip=$((1538528*512)) count=7584
FAT16 (Partition 2)	History	gpg	Archive	Normal File	787742720	1627994	dd if=Project1.dd of=History.gpg bs=1 skip=$((1538560*512)) count=1627994
FAT16 (Partition 2)	Goal	gpg	Archive	Deleted	789381120	48660	dd if=Project1.dd of=Goal.gpg bs=1 skip=$((1541760*512)) count=48660
FAT16 (Partition 2)	Surveil	gpg	Archive	Normal File	789430272	5702	dd if=Project1.dd of=Surveil.gpg bs=1 skip=$((1541856*512)) count=5702

Table 5: Executive Summary Table

6 Conclusions and Recommendations

Through our investigation of the disk image provided to us we made many discoveries that pointed towards the ultimate objective of the original laptop owners being to steal the Hope Diamond necklace from the Smithsonian Institute, then sell it. This plan was to be carried out over October 2nd-6th 2020.

The original owners of the laptop used multiple different data hiding methods. They deleted files, created password protected zip files, and utilized GPG encryption. They also spread these different files across different partitions, and encoded strings into ascii representation.

Given all the evidence found on this disk image, we can assume that the original owners of the laptop were involved in some criminal activity. We would recommend passing our findings on to law enforcement and legal teams to review and decide on next steps.