AUBURN

UNIVERSITY

Digital Forensics Analysis Report

Virginia Hudson

Casey Waid

Samuel Walden

10/08/2020

Executive Summary

A disk image was provided for analysis. While implementing various digital forensics techniques, the analysis team retrieved data that led to the alleged Hope Diamond jewelry heist at the Smithsonian National Museum of Natural History in Washington, D.C. With the availability of SIFT Workstation and Active@ Disc Editor, the analysis team manually recovered all files from each disk image. The disk image consisted of three partitions: FAT16, NTFS, and FAT 16, respectively. Each partition contained four files:

- Partition 1 – Fat16: Email.docx, Necklace.pdf, Dash.jpg, Gems.pdf
- Partition 2 – NTFS: Encoding.pdf, Surveil1.jpg, Surveil2.zip, Mystery.zip
- Partition 3 – FAT16: Plan.gpg, History.gpg, Goal.gpg, Surveil.gpg

To hide the data, some of the files found were deleted, such as Email.docs, Dash.jpg, Surveil2.zip, Mystery.zip, Plan.gpg, and Goal.gpg. Password protection was also implemented with the two zip files found in the NTFS partition and all of the GPG files in the second FAT16. The actors used GPG files as an encryption tool to hide the data in the third partition. Sequentially identifying and analyzing the three partitions was key to retrieving the necessary data for identifying the alleged jewelry heist. Email.docx from Partition 1 contained the password for the two deleted ZIP files in the NTFS partition. Once extracted, Mystery.zip contained a text file consisting of hex-encoded string, which, when decoded, provided the password for gaining access to the GPG files' data.

Table of Contents

List of Tables

Table 1 - Partition 1 Root Directory:

Filename	Extension	Attribute	TIme	Data	Clusters	# Sectors	File Size (B)	Status
Email	.docx	Long File Name	00:20:25	09/02/2020	0x3	24	11,700	Name Used But Deleted
Necklace	.pdf	Long File Name	00:02:03	09/02/2020	0x6	176	86,321	Normal File
Dash	.jpg	Long File Name	00:12:34	09/02/2020	0x1C	96	46,678	Name Used but Deleted
Gems	.pdf	Long FIle Name	00:12:34	09/02/2020	0x28	1,768	901,175	Normal File

Table 2 - Partition 3 Root Directory:

Filename	Extension	Attribute	TIme	Data	Clusters	# Sectors	File Size (B)	Status
Plan	.docx	Archive	23:58:57	08/31/2020	0x3	96	7,584	Name Used But Deleted
History	.pdf	Archive	23:58:57	08/31/2020	0x4	128	1,627,994	Normal File
Goal	.jpg	Archive	23:58:57	08/31/2020	0x68	3,328	48,660	Name Used but Deleted
Surveil	.pdf	Archive	23:58:57	08/31/2020	0x6B	3,424	5,702	Normal File

Table 3 - Partition 2 NTFS Attributes:

Attribute	Encoding	Surveil1	Surveil2	Mystery
0x10	✔	✔	✔	✔
0x30	✔	✔	✔	✔
0x50	✔	✔	✔	✔

0x80	✔	✔	✔	✔

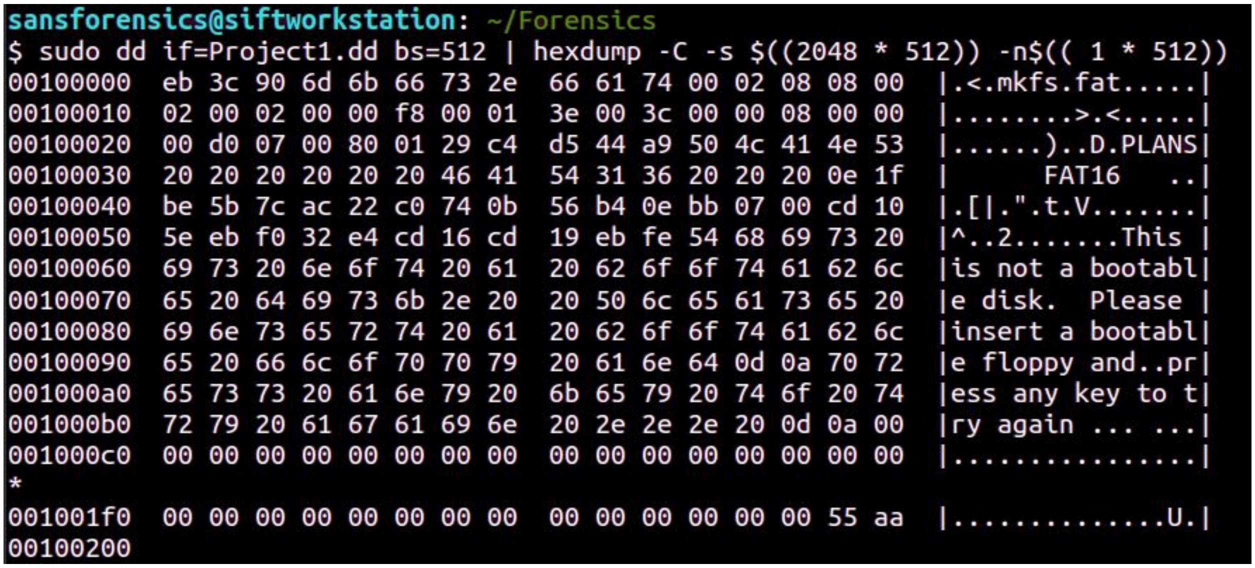
Table - Summary Table

Partition	Filename	Extension	Attribute	Status	Byte Offset	File Size	Recovery Command
FAT16	Email	.docx	$DATA	Deleted	1335296 - 1347072	11700	sudo dd if=Project1.dd of=email.docx bs=512 skip=2608 count=23
FAT16	Necklace	.pdf	$DATA	Normal	1347584 - 1434112	86321	sudo dd if=Project1.dd of=necklace.pdf bs=512 skip=2632 count=169
FAT16	Dash	.jpg	$DATA	Deleted	1335296 - 1382400	46678	sudo dd if=Project1.dd of=Dash.jpg bs=512 skip=2808 count=92
FAT16	Gems	.pdf	$DATA	Normal	1486848 - 2388480	901175	sudo dd if=Project1.dd of=Gems.pdf bs=512 skip=2904 count=1761
NTFS	Mystery	.txt	$DATA	Deleted	263274496 - 263274754	258	sudo dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258
NTFS	Surveil1	.jpg	$DATA	Normal	329170944 - 335111168	11602	sudo dd if=Project1.dd of=Surveil1.JPG bs=512 skip=642912 count=11602
NTFS	Surveil2	.jpg	$DATA	Deleted	345931776 - 351655424	11179	sudo dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=11179
NTFS	Encoding	.pdf	$DATA	Normal	362708992 - 362813952	104632	sudo dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=205
FAT16	Plan	.ole2	$DATA	Deleted	787726336 - 787734016	7584	sudo dd if=Project1.dd of=Plan.gpg bs=512 skip=1538528 count=15
FAT16	History	.pdf	$DATA	Normal	787742720 - 789370880	1627994	sudo dd if=Project1.dd of=History.gpg bs=512 skip=1538560 count=3180
FAT16	Goal	.jpg	$DATA	Deleted	789381120 - 789430272	48660	sudo dd if=Project1.dd of=Goal.gpg bs=512 skip=1541760 count=96
FAT16	Surveil	.jpg	$DATA	Normal	789430272 -	5702	sudo dd if=Project1.dd of=Surveil.gpg bs=512

					789436416		skip=1541856 count=12

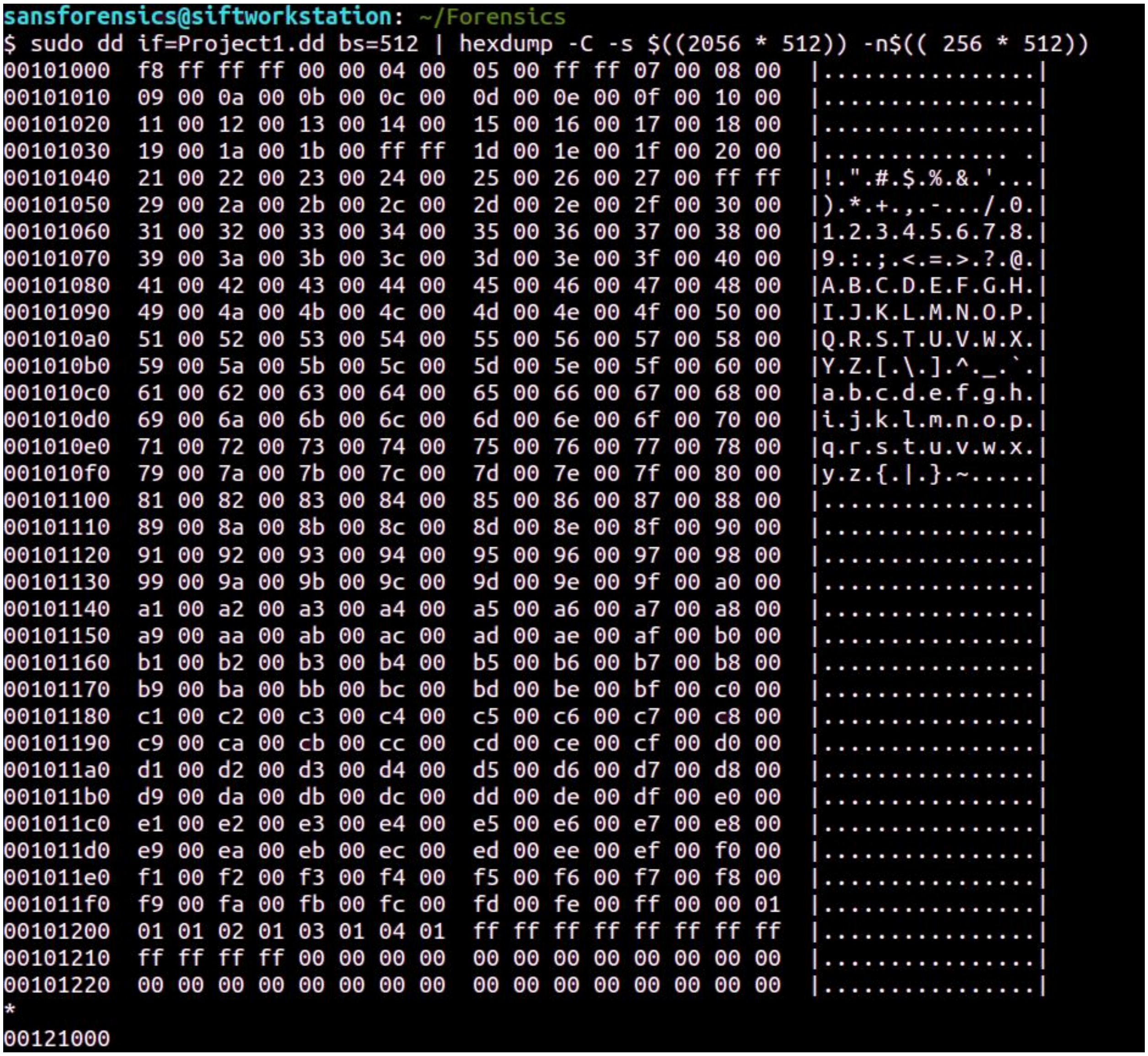
List of Figures

Figure 1 → Partition 1 Boot Sector



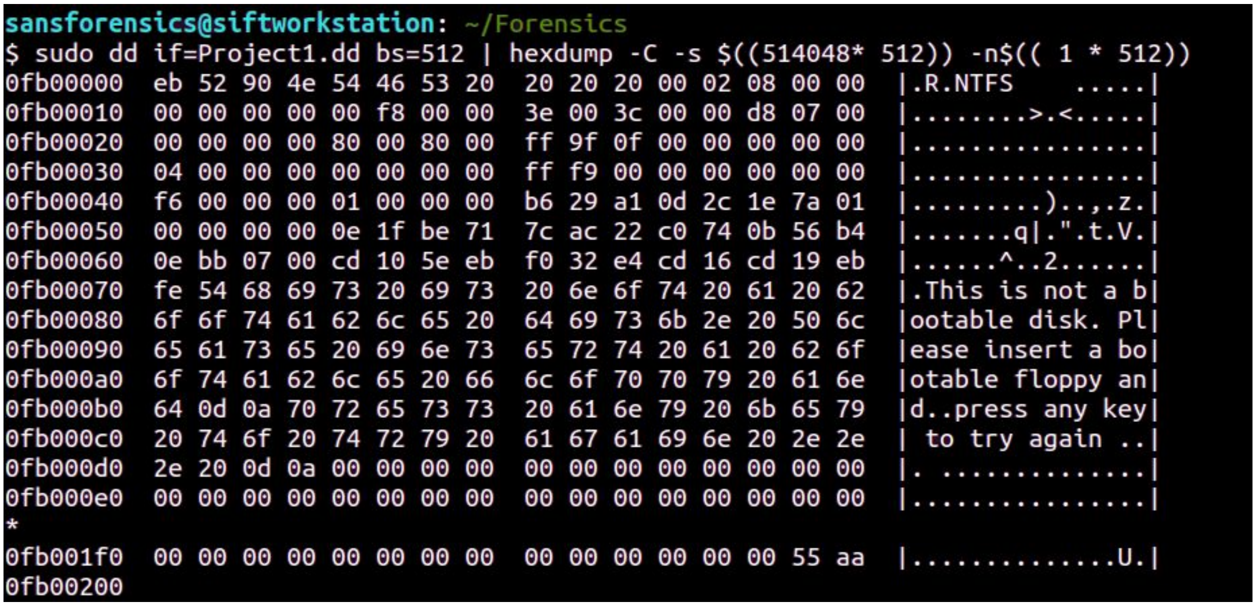
```
sansforensics@siftworkstation: ~/Forensics
$ sudo dd if=Project1.dd bs=512 | hexdump -C -s $((2048 * 512)) -n$(( 1 * 512))
00100000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 08 08 00  |.<.mkfs.fat.....|
00100010  02 00 02 00 00 f8 00 01  3e 00 3c 00 00 08 00 00  |........>.<.....|
00100020  00 d0 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
```

Figure 2 → Partition 1 first FAT



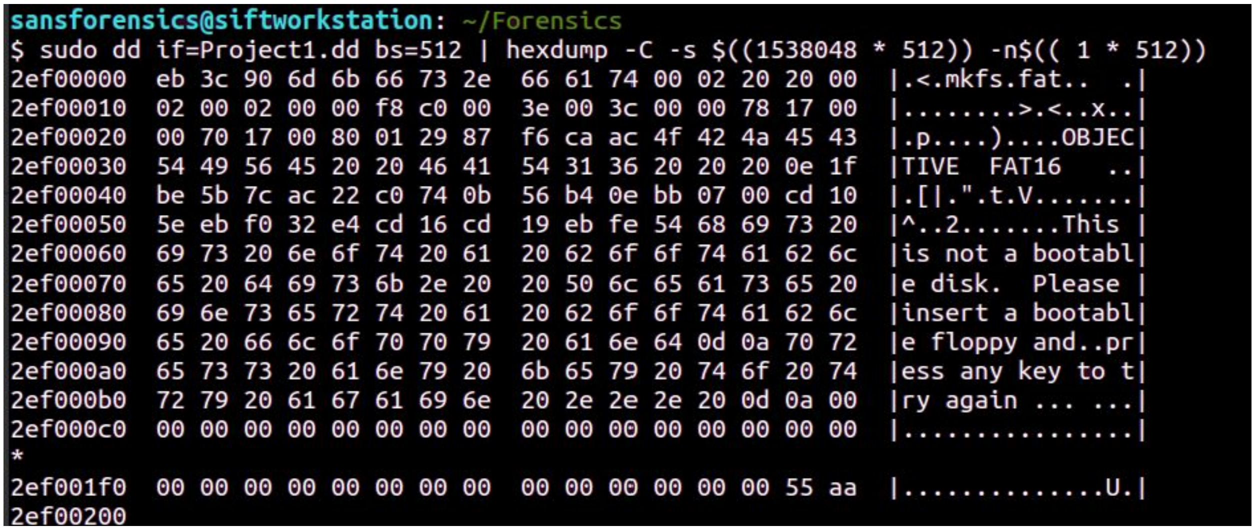
```
sansforensics@siftworkstation: ~/Forensics
$ sudo dd if=Project1.dd bs=512 | hexdump -C -s $((2056 * 512)) -n$(( 256 * 512))
00101000  f8 ff ff ff 00 00 04 00  05 00 ff ff 07 00 08 00  |................|
00101010  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
00101020  11 00 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 2 NTFS Master Boot Record



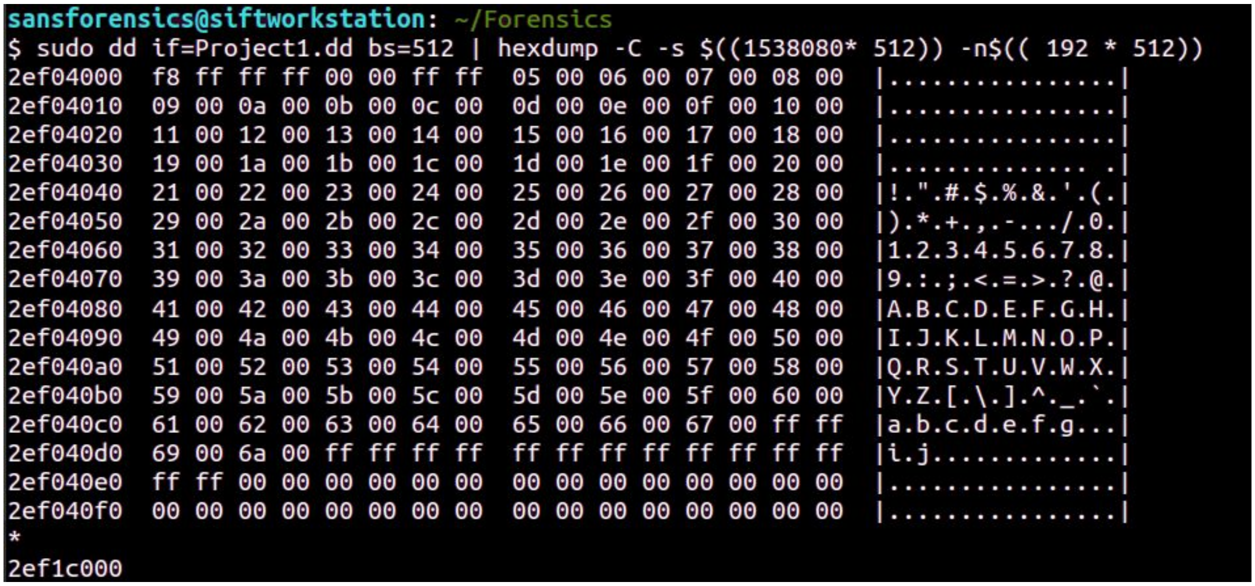
```
sansforensics@siftworkstation: ~/Forensics
$ sudo dd if=Project1.dd bs=512 | hexdump -C -s $((514048* 512)) -n$(( 1 * 512))
0fb00000  eb 52 90 4e 54 46 53 20  20 20 20 00 02 08 00 00  |.R.NTFS    .....|
0fb00010  00 00 00 00 00 f8 00 00  3e 00 3c 00 00 d8 07 00  |........>.<.....|
0fb00020  00 00 00 00 80 00 80 00  ff 9f 0f 00 00 00 00 00  |................|
0fb00030  04 00 00 00 00 00 00 00  ff f9 00 00 00 00 00 00  |................|
0fb00040  f6 00 00 00 01 00 00 00  b6 29 a1 0d 2c 1e 7a 01  |.........)..,.z.|
0fb00050  00 00 00 00 0e 1f be 71  7c ac 22 c0 74 0b 56 b4  |.......q|.".t.V.|
0fb00060  0e bb 07 00 cd 10 5e eb  f0 32 e4 cd 16 cd 19 eb  |......^..2......|
0fb00070  fe 54 68 69 73 20 69 73  20 6e 6f 74 20 61 20 62  |.This is not a b|
0fb00080  6f 6f 74 61 62 6c 65 20  64 69 73 6b 2e 20 50 6c  |ootable disk. Pl|
0fb00090  65 61 73 65 20 69 6e 73  65 72 74 20 61 20 62 6f  |ease insert a bo|
0fb000a0  6f 74 61 62 6c 65 20 66  6c 6f 70 70 79 20 61 6e  |otable floppy an|
0fb000b0  64 0d 0a 70 72 65 73 73  20 61 6e 79 20 6b 65 79  |d..press any key|
0fb000c0  20 74 6f 20 74 72 79 20  61 67 61 69 6e 20 2e 2e  | to try again ..|
0fb000d0  2e 20 0d 0a 00 00 00 00  00 00 00 00 00 00 00 00  |. ..............|
0fb000e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
0fb001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
0fb00200
```

Figure 4 → Partition 3 Boot Sector



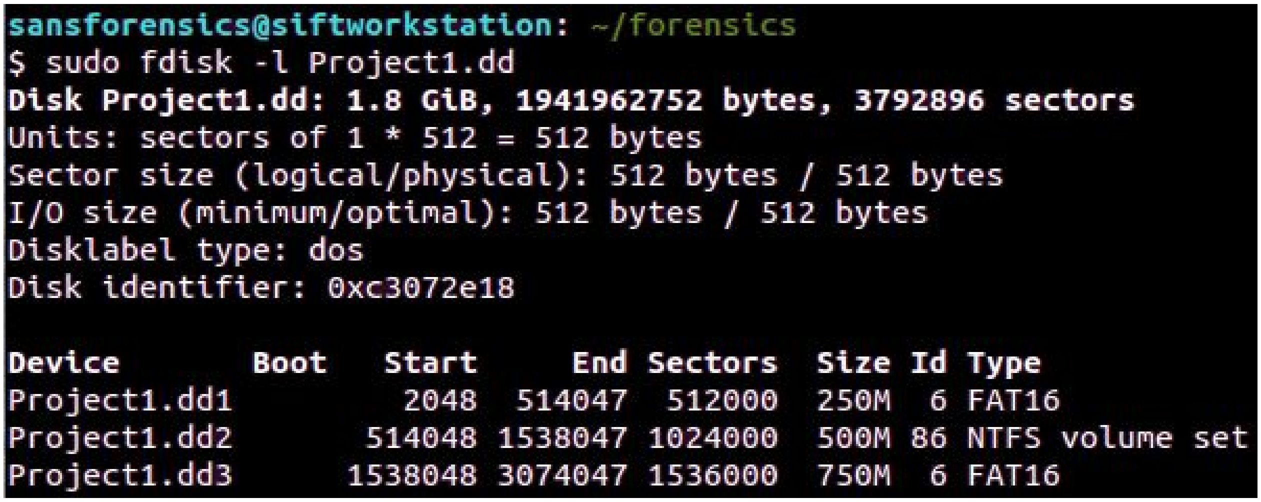
```
sansforensics@siftworkstation: ~/Forensics
$ sudo dd if=Project1.dd bs=512 | hexdump -C -s $((1538048 * 512)) -n$(( 1 * 512))
2ef00000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 20 20 00  |.<.mkfs.fat..  .|
2ef00010  02 00 02 00 00 f8 c0 00  3e 00 3c 00 00 78 17 00  |........>.<..x..|
2ef00020  00 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 5 → Partition 3 first FAT



```
sansforensics@siftworkstation: ~/Forensics
$ sudo dd if=Project1.dd bs=512 | hexdump -C -s $((1538080* 512)) -n$(( 192 * 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  |).*.+.,.-.../.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  |................|
*
2ef1c000
```

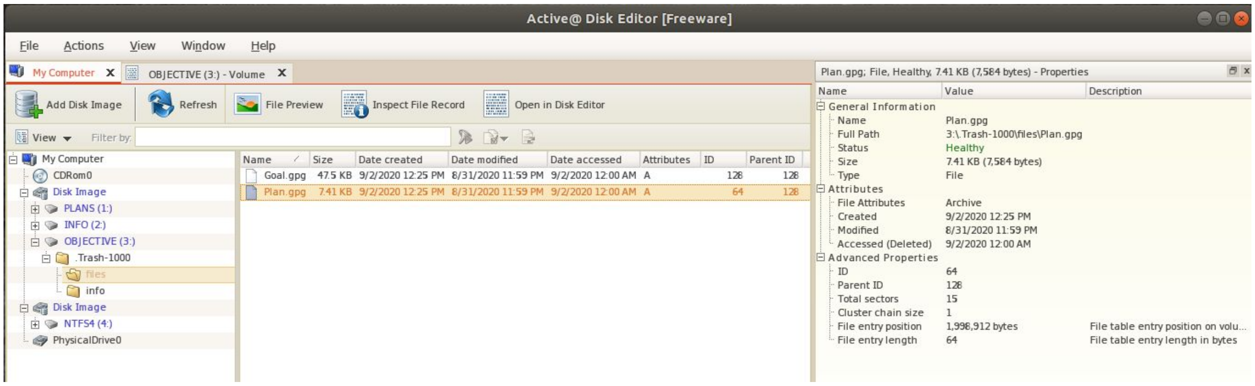
Figure 6 → Disk information command



```
sansforensics@siftworkstation: ~/forensics
$ sudo 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
```

Figure 7 → File inventory in Active Disk Editor

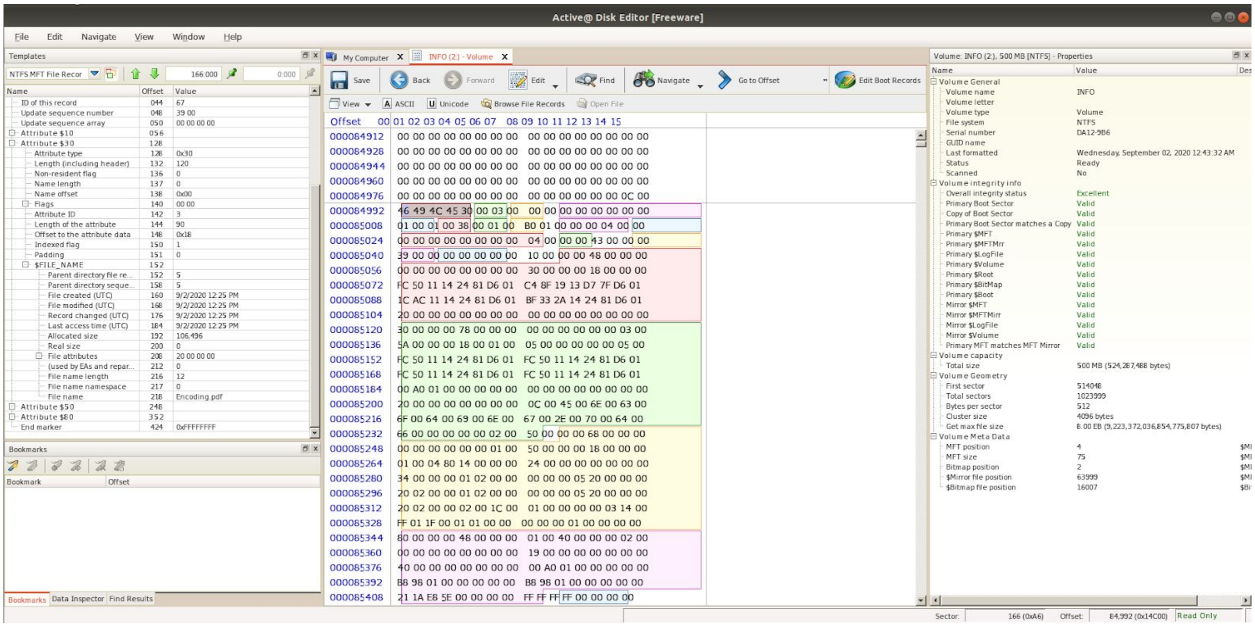


Name	Size	Date created	Date modified	Date accessed	Attributes	ID	Parent ID
Goal.gpg	47.5 KB	9/2/2020 12:25 PM	8/31/2020 11:59 PM	9/2/2020 12:00 AM	A	128	128
Plan.gpg	7.41 KB	9/2/2020 12:25 PM	8/31/2020 11:59 PM	9/2/2020 12:00 AM	A	64	128

Plan.gpg; File, Healthy, 7.41 KB (7,584 bytes) - Properties

Name	Value	Description
General Information		
Name	Plan.gpg	
Full Path	3:\.Trash-1000\files\Plan.gpg	
Status	Healthy	
Size	7.41 KB (7,584 bytes)	
Type	File	
Attributes		
File Attributes	Archive	
Created	9/2/2020 12:25 PM	
Modified	8/31/2020 11:59 PM	
Accessed (Deleted)	9/2/2020 12:00 AM	
Advanced Properties		
ID	64	
Parent ID	128	
Total sectors	15	
Cluster chain size	1	
File entry position	1,998,912 bytes	File table entry position on volu...
File entry length	64	File table entry length in bytes

Figure 8 → File record in Active Disk Editor



Name	Offset	Value
ID of this record	044	67
Update sequence number	048	39 00
Update sequence array	050	00 00 00 00
Attribute $10	056	
Attribute $30	128	
Attribute type	128	0x30
Length (including header)	132	120
Non-resident flag	136	0
Name length	137	0
Name offset	138	0x00
Flags	140	00 00
Attribute ID	142	3
Length of the attribute	144	90
Offset to the attribute data	148	0x18
Indexed flag	150	1
Padding	151	0
$FILE_NAME	152	
Parent directory file re...	152	5
Parent directory seque...	158	5
File created (UTC)	160	9/2/2020 12:25 PM
File modified (UTC)	168	9/2/2020 12:25 PM
Record changed (UTC)	176	9/2/2020 12:25 PM
Last access time (UTC)	184	9/2/2020 12:25 PM
Allocated size	192	106,496
Real size	200	0
File attributes	208	20 00 00 00
(used by EAs and repar...	212	0
File name length	216	12
File name namespace	217	0
File name	218	Encoding.pdf
Attribute $50	248	
Attribute $80	352	
End marker	424	0xFFFFFFFF

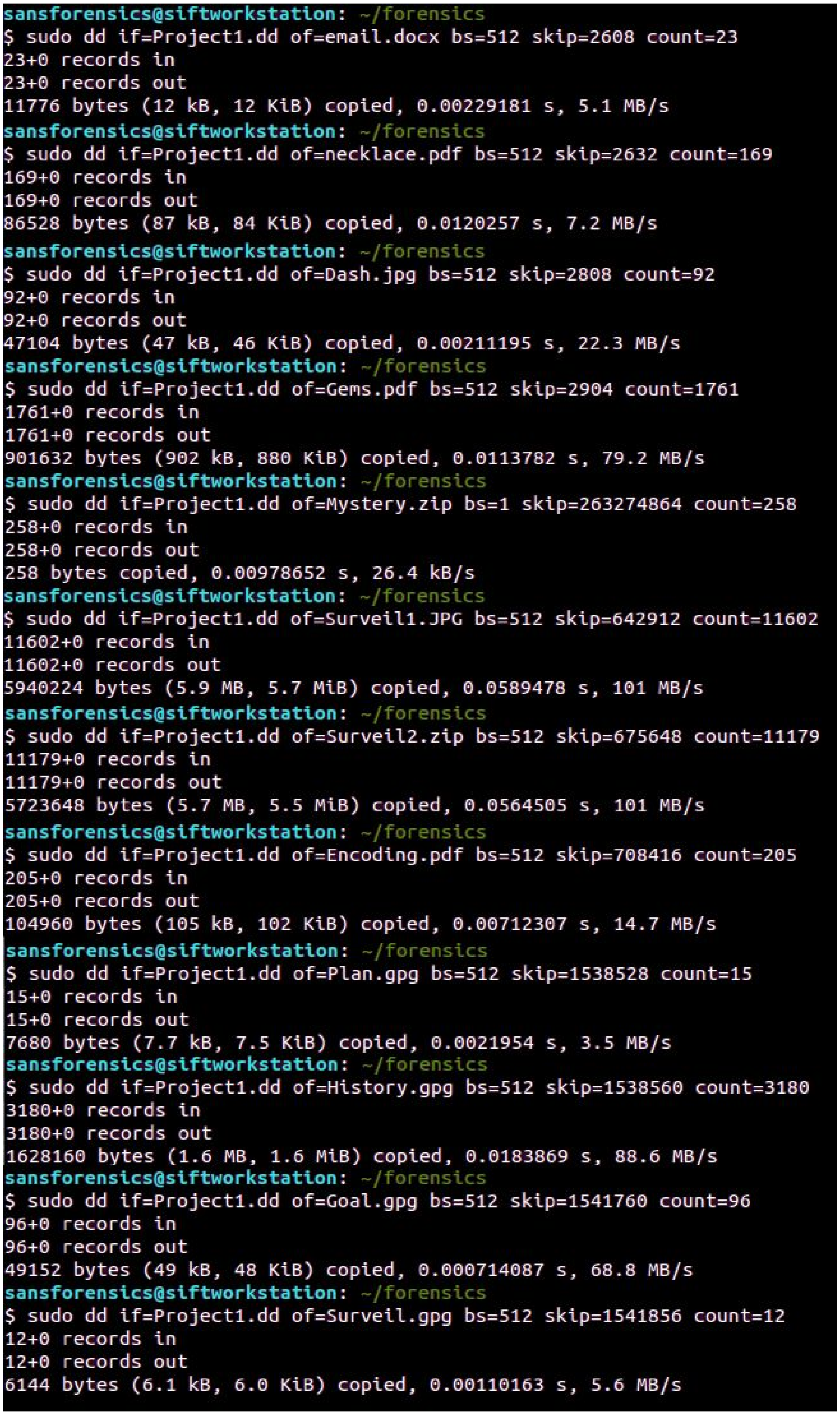
```
Offset     00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15
000084912  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000084928  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000084944  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000084960  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000084976  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0C 00
000084992  46 49 4C 45 30 00 03 00  00 00 00 00 00 00 00 00
000085008  01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00
000085024  00 00 00 00 00 00 00 00  04 00 00 00 43 00 00 00
000085040  39 00 00 00 00 00 00 00  10 00 00 00 48 00 00 00
000085056  00 00 00 00 00 00 00 00  30 00 00 00 18 00 00 00
000085072  FC 50 11 14 24 81 D6 01  C4 8F 19 13 D7 7F D6 01
000085088  1C AC 11 14 24 81 D6 01  BF 33 2A 14 24 81 D6 01
000085104  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000085120  30 00 00 00 78 00 00 00  00 00 00 00 00 00 03 00
000085136  5A 00 00 00 18 00 01 00  05 00 00 00 00 00 05 00
000085152  FC 50 11 14 24 81 D6 01  FC 50 11 14 24 81 D6 01
000085168  FC 50 11 14 24 81 D6 01  FC 50 11 14 24 81 D6 01
000085184  00 A0 01 00 00 00 00 00  00 00 00 00 00 00 00 00
000085200  20 00 00 00 00 00 00 00  0C 00 45 00 6E 00 63 00
000085216  6F 00 64 00 69 00 6E 00  67 00 2E 00 70 00 64 00
000085232  66 00 00 00 00 00 02 00  50 00 00 00 68 00 00 00
000085248  00 00 00 00 00 00 01 00  50 00 00 00 18 00 00 00
000085264  01 00 04 80 14 00 00 00  24 00 00 00 00 00 00 00
000085280  34 00 00 00 01 02 00 00  00 00 00 05 20 00 00 00
000085296  20 02 00 00 01 02 00 00  00 00 00 05 20 00 00 00
000085312  20 02 00 00 02 00 1C 00  01 00 00 00 00 03 14 00
000085328  FF 01 1F 00 01 01 00 00  00 00 00 01 00 00 00 00
000085344  80 00 00 00 48 00 00 00  01 00 40 00 00 00 02 00
000085360  00 00 00 00 00 00 00 00  19 00 00 00 00 00 00 00
000085376  40 00 00 00 00 00 00 00  00 A0 01 00 00 00 00 00
000085392  B8 98 01 00 00 00 00 00  B8 98 01 00 00 00 00 00
000085408  21 1A E8 5E 00 00 00 00  FF FF FF FF 00 00 00 00
```

Volume: INFO (2:), 500 MB [NTFS] - Properties

Name	Value	Des
Volume General		
Volume name	INFO	
Volume letter		
Volume type	Volume	
File system	NTFS	
Serial number	DA12-9B6	
GUID name		
Last formatted	Wednesday, September 02, 2020 12:43:32 AM	
Status	Ready	
Scanned	No	
Volume integrity info		
Overall integrity status	Excellent	
Primary Boot Sector	Valid	
Copy of Boot Sector	Valid	
Primary Boot Sector matches a Copy	Valid	
Primary $MFT	Valid	
Primary $MFTMrr	Valid	
Primary $LogFile	Valid	
Primary $Volume	Valid	
Primary $Root	Valid	
Primary $BitMap	Valid	
Primary $Boot	Valid	
Mirror $MFT	Valid	
Mirror $MFTMirr	Valid	
Mirror $LogFile	Valid	
Mirror $Volume	Valid	
Primary MFT matches MFT Mirror	Valid	
Volume capacity		
Total size	500 MB (524,287,488 bytes)	
Volume Geometry		
First sector	514048	
Total sectors	1023999	
Bytes per sector	512	
Cluster size	4096 bytes	
Get max file size	8.00 EB (9,223,372,036,854,775,807 bytes)	
Volume Meta Data		
MFT position	4	$MI
MFT size	75	$MI
Bitmap position	2	$MI
$Mirror file position	63999	$MI
$Bitmap file position	16007	$Bi

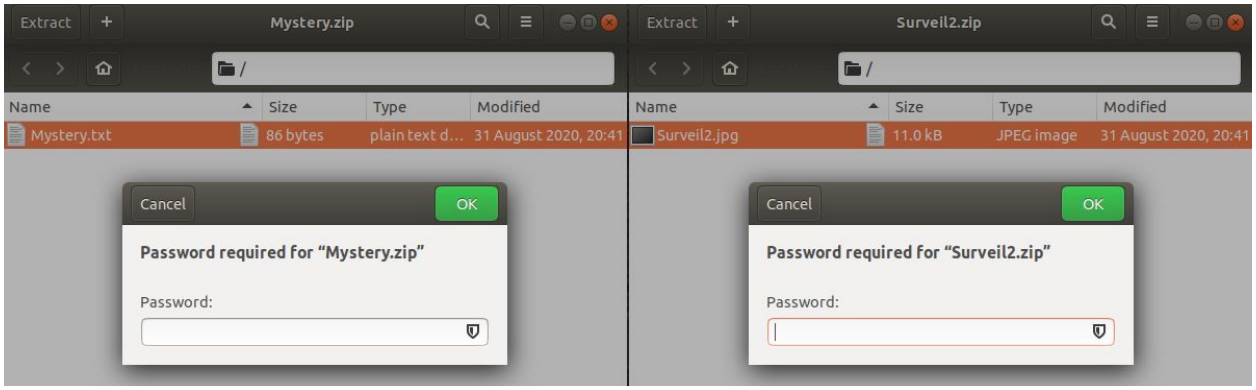
Sector: 166 (0xA6) Offset: 84,992 (0x14C00) Read Only

Figure 9 → File recovery



```
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=email.docx bs=512 skip=2608 count=23
23+0 records in
23+0 records out
11776 bytes (12 kB, 12 KiB) copied, 0.00229181 s, 5.1 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=necklace.pdf bs=512 skip=2632 count=169
169+0 records in
169+0 records out
86528 bytes (87 kB, 84 KiB) copied, 0.0120257 s, 7.2 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Dash.jpg bs=512 skip=2808 count=92
92+0 records in
92+0 records out
47104 bytes (47 kB, 46 KiB) copied, 0.00211195 s, 22.3 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Gems.pdf bs=512 skip=2904 count=1761
1761+0 records in
1761+0 records out
901632 bytes (902 kB, 880 KiB) copied, 0.0113782 s, 79.2 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258
258+0 records in
258+0 records out
258 bytes copied, 0.00978652 s, 26.4 kB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Surveil1.JPG bs=512 skip=642912 count=11602
11602+0 records in
11602+0 records out
5940224 bytes (5.9 MB, 5.7 MiB) copied, 0.0589478 s, 101 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=11179
11179+0 records in
11179+0 records out
5723648 bytes (5.7 MB, 5.5 MiB) copied, 0.0564505 s, 101 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=205
205+0 records in
205+0 records out
104960 bytes (105 kB, 102 KiB) copied, 0.00712307 s, 14.7 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Plan.gpg bs=512 skip=1538528 count=15
15+0 records in
15+0 records out
7680 bytes (7.7 kB, 7.5 KiB) copied, 0.0021954 s, 3.5 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=History.gpg bs=512 skip=1538560 count=3180
3180+0 records in
3180+0 records out
1628160 bytes (1.6 MB, 1.6 MiB) copied, 0.0183869 s, 88.6 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Goal.gpg bs=512 skip=1541760 count=96
96+0 records in
96+0 records out
49152 bytes (49 kB, 48 KiB) copied, 0.000714087 s, 68.8 MB/s
sansforensics@siftworkstation: ~/forensics
$ sudo dd if=Project1.dd of=Surveil.gpg bs=512 skip=1541856 count=12
12+0 records in
12+0 records out
6144 bytes (6.1 kB, 6.0 KiB) copied, 0.00110163 s, 5.6 MB/s
```

Figure 10 → Password prompts from .zip files Mystery and Surveil2



Name	Size	Type	Modified
Mystery.txt	86 bytes	plain text d…	31 August 2020, 20:41

Password required for “Mystery.zip”

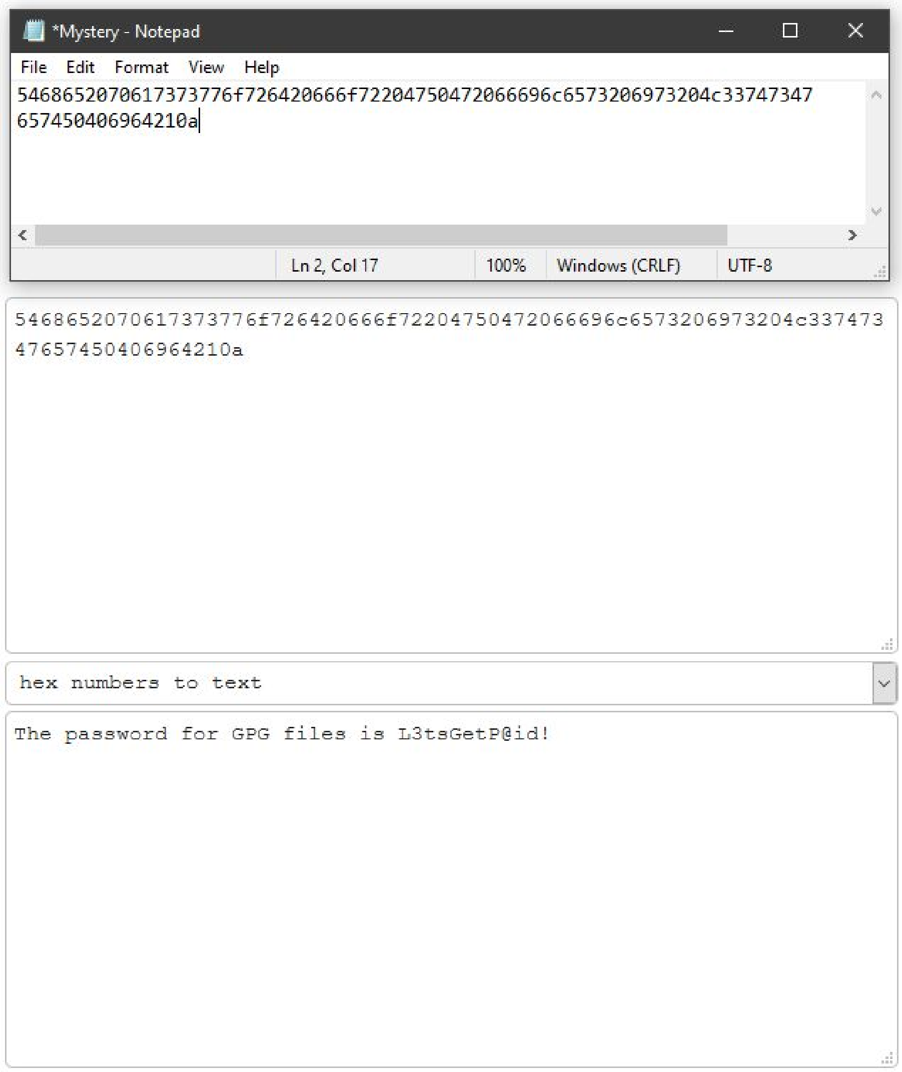
Password:

Name	Size	Type	Modified
Surveil2.jpg	11.0 kB	JPEG image	31 August 2020, 20:41

Password required for “Surveil2.zip”

Password:

Figure 11 → Mystery contents and conversion



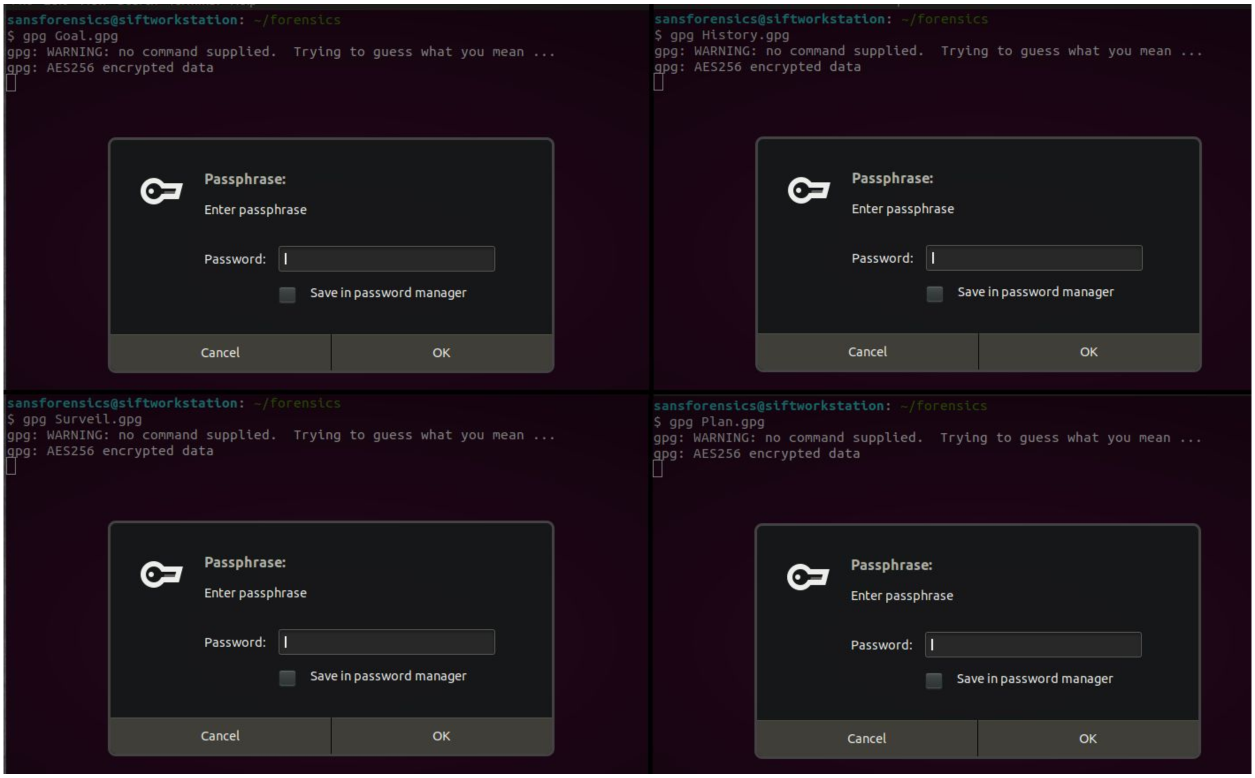
```
5468652070617373776f726420666f72204750472066696c6573206973204c33747347
657450406964210a
```

```
5468652070617373776f726420666f72204750472066696c6573206973204c337473
47657450406964210a
```

hex numbers to text

```
The password for GPG files is L3tsGetP@id!
```

Figure 12 → Decryption key prompts from .gpg files Goal, Plan, History, Surveil



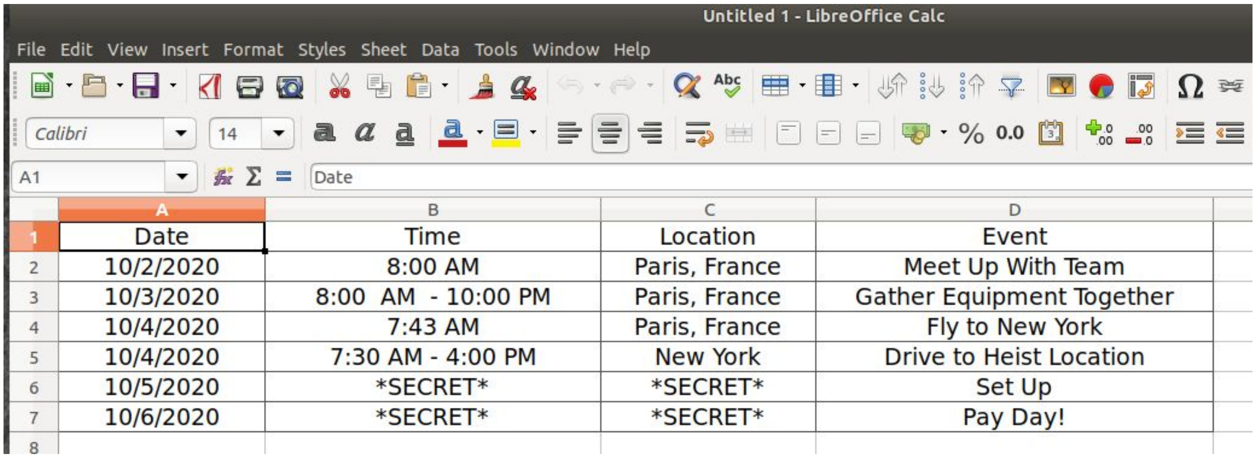
```
sansforensics@siftworkstation: ~/forensics
$ gpg Goal.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
```

```
sansforensics@siftworkstation: ~/forensics
$ gpg History.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
```

```
sansforensics@siftworkstation: ~/forensics
$ gpg Surveil.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
```

```
sansforensics@siftworkstation: ~/forensics
$ gpg Plan.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
```

Figure 13 → Plan.ole2 Contents



Untitled 1 - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Calibri
14
A1
Date

	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!
8				

1 Introduction

Our team was provided with a disk image that was collected during a forensics investigation. Our task was to recover all the files on the disk, whether deleted or not, and decrypt any encrypted files. We were also tasked with finding any hidden files. The disk was divided into three partitions that included both FAT16 and NTFS filing systems. Once all the artifacts were obtained, our team was tasked with analyzing them to see if there is any evidence of criminal activity.

2 Problem Description

Our team was tasked with recovering files from a provided disk image that was believed to contain evidence of possible criminal activity. We were to recover files on the disk, with half of them having been deleted and half of them having been encrypted or otherwise password-protected, analyze their contents, determine whether or not there is proof of illegal activity, and present evidence to either indict or excuse the potential perpetrators.

3 Methodology

After retrieving basic information about the disk image through the Linux Terminal (Figure 6), our team could see that it contained three different partitions -- a FAT16 partition, an NTFS partition, and another FAT16 partition. The first FAT16 root directory starts at sector 2,568. It's contents are provided in table 1. Within this root directory, we were able to discover the file names (Email, Necklace, Dash, Gems), extensions (.docx, .pdf, .jpg, .pdf), attributes (long file name), times (00:20:25, 00:02:03, 00:12:34, 00:12:34), dates (09/02/2020), clusters (0x3, 0x6, 0x1C, 0x28), number of sectors (24, 176, 96, 1,768), file sizes (11,700 B, 86,321 B, 46,678 B, 901,175 B) and status (name used but not deleted, normal file, name used but deleted, normal file). It's File Allocation Table (FAT) explained the number of clusters, sectors, and bytes as follows:

FIle Name	Number of Clusters	Number of Sectors
Email	3	24
Necklace	6	176
Dash	26	96
Gems	260	1768

The second FAT16 root directory starts at sector 1,538,048. It's contents are provided in table 2. Within this root directory, we were able to discover the file names (Plan, History, Goal, Surveil), extensions (.gpg), attributes (archive), times (23:58:57), dates (08/31/2020), clusters (0x3, 0x4, 0x68, 0x6B), number of sectors (96, 128, 3,328, 3,424), file sizes (7,584 B, 1,627,994 B, 48,660 B, 5,702 B) and status (name used but not deleted, normal file, name used but deleted, normal file). Its File Allocation Table (FAT) at first glance was misleading. It starts with f8 ff ff ff, and to the untrained eye shows only two files. This is because the files Surveil and Plan are 12 and 15 sectors respectively and are contained in 1 cluster each.

FIle Name	Number of Clusters	Number of Sectors
History	100	3180
Goal	3	96
Surveil	1	12
Plan	1	15

Our team then set about ascertaining the locations of each file, whether deleted or otherwise, by using information from the boot sector or master boot record of each partition (Figures 1, 3, 4), combined with the use of the provided Active Disk Editor. By observing the file inventory (Figure 7) and file records (Figure 8) in the Active Disk Editor and file allocation tables (Figures 2, 5) in the Linux Terminal, we were able to discern each appropriate recovery command to retrieve both deleted and regular files from the disk image. We observed the specific sector that each file was in, along with each file's size and name, and created our recovery commands (Figure 9).

Once we had retrieved all twelve of the files (four in each partition, half of which had been deleted) on the disk image, our team began our analysis of each file in-turn. Each file is included in a .zip file for observation. Our first lead was the content of the .docx file, Email, from the first partition, which contained email correspondence between two actors by the names of John Disco and Bill Taker. Within the email thread, the potential perpetrators discussed the use of a password, "G3tTh3G00dStuff!", for the .zip files that they planned to exchange. Although the actors had deleted other files in the disk image, this was the first instance of a real data-hiding technique that these individuals had used. Our team, having already recovered the .zip files from the NTFS partition, used this password to unlock each .zip file and retrieve its contents (Figure 10).

While the first .zip file, Surveil2, contained a .jpg file, the contents of the .zip file, Mystery, was a simple .txt file that contained hexadecimal code which our team quickly decrypted into plain text (Figure 11). The derived text indicated a passcode, "L3tsGetP@id!", that the actors planned to use as a key to encrypt the files our team retrieved from the third partition, was the second instance of data-hiding techniques being used by these individuals. Our team used this decoded password to unlock the .gpg files Goal, History, Surveil, and Plan (Figure 12) using the gpg function within the Linux Terminal and found further evidence of these actors planning a heist. After opening the .ole2 file, Plan, in LibreOffice Calc (Figure 13), our team had retrieved and analyzed all of the files from the provided disk image.

4 Conclusions and recommendations

Our team was able to recover a deleted email from an individual named John Disco, also known as Johnny D, to a recipient named Bill Taker. In the contents of this deleted email, John Disco instructed Bill Taker to hide “everything,” and gave him a password to the zip files he said would be included. This deleted email was our team’s first indication that the parties involved in the correspondence could be considering committing a crime. Our team was able to use the password mentioned in the email to open the .zip files we recovered. We also discovered another file that contained a key to all .gpg files. We were able to open all the files we found on the disk and that were contained in that deleted email.

Our team noticed that the actors here seemed to be obsessed with precious gems, specifically diamonds. We uncovered several files whose filenames led us to believe that they were surveillance photos. These photos were of different places in Washington DC, with one of them being the Smithsonian National Museum of Natural History. We uncovered a file entitled “Goal” which was a picture of the Hope Diamond that is on display at the Smithsonian National Museum of Natural History . Finally, our team uncovered a file entitled “Plan”, which was a spreadsheet that laid out a plan for our actors to fly from Paris to New York City on October 4th, 2020. The plan then had them carrying out what they called a “heist” at a secret location on October 6th 2020, two days ago. Our team believes this secret location was the Smithsonian National Museum of Natural History in Washington DC.

The actors here had clear intentions of coming to New York City on October 4th to perform a “heist” at a secret location on October 6th. They clearly were interested in the Hope Diamond, and had surveillance photos of Washington DC and the Smithsonian. Our team believes there is enough evidence to make an arrest and, ultimately, get a conviction of these actors, if there was a crime committed at the Smithsonian during this time.