COMP 5350 / 6350

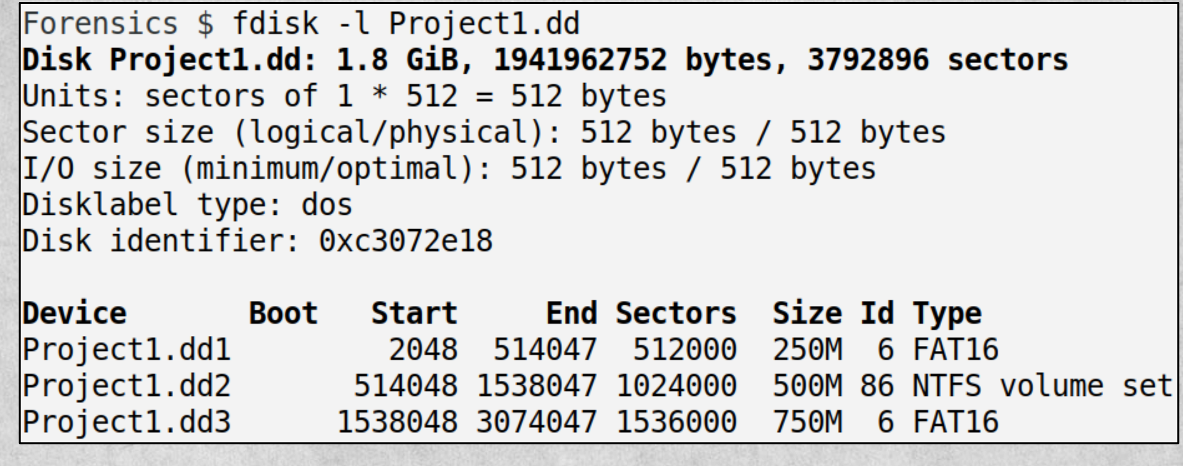
Digital Forensics

Project #1 Review

Forensic Challenges

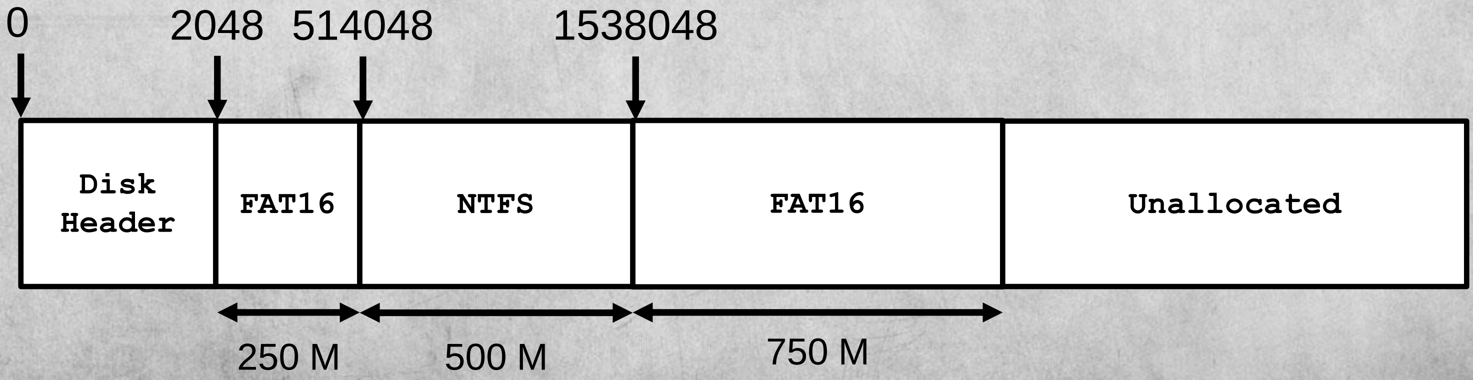
Project #1 Review

Partition Identification



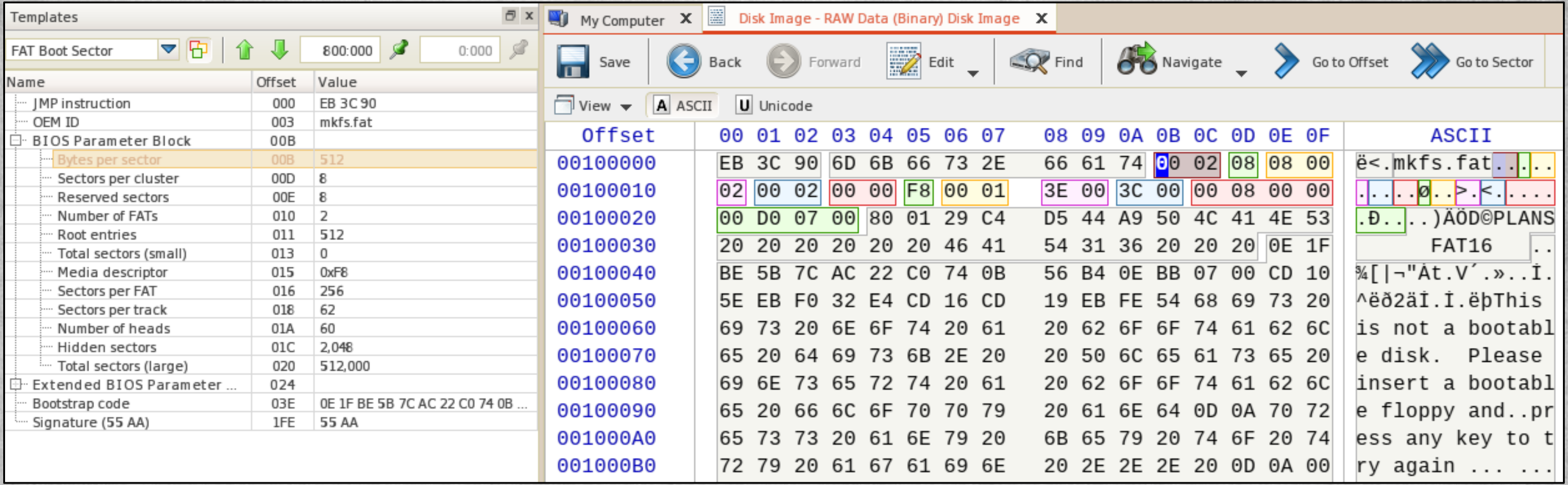
```
Forensics $ fdisk -l Project1.dd
Disk Project1.dd: 1.8 GiB, 1941962752 bytes, 3792896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3072e18

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
```



Partition #1, FAT16

Partition #1 – FAT16 Boot Sector

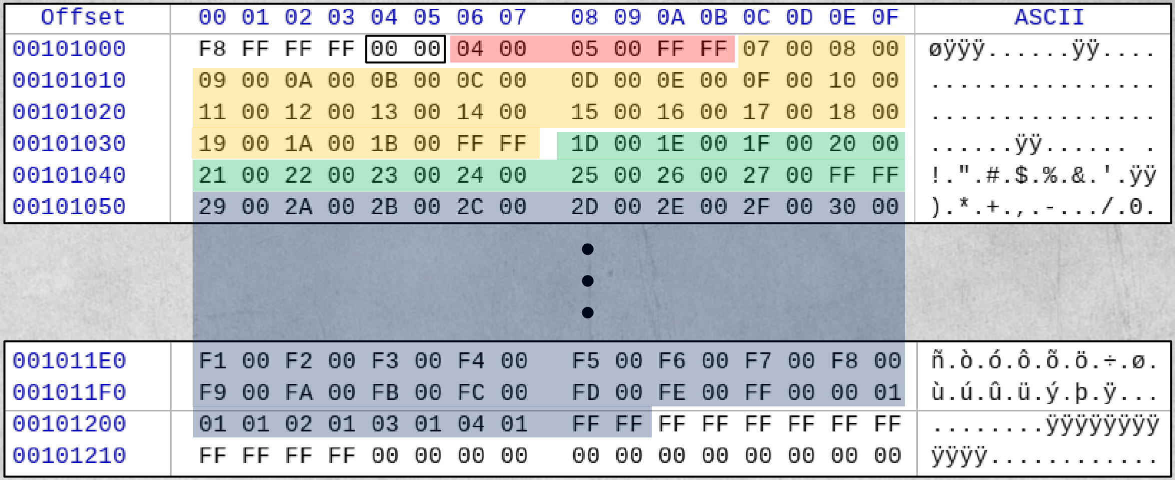


Name	Offset	Value
JMP instruction	000	EB 3C 90
OEM ID	003	mkfs.fat
BIOS Parameter Block	00B	
Bytes per sector	00B	512
Sectors per cluster	00D	8
Reserved sectors	00E	8
Number of FATs	010	2
Root entries	011	512
Total sectors (small)	013	0
Media descriptor	015	0xF8
Sectors per FAT	016	256
Sectors per track	018	62
Number of heads	01A	60
Hidden sectors	01C	2,048
Total sectors (large)	020	512,000
Extended BIOS Parameter ...	024	
Bootstrap code	03E	0E 1F BE 5B 7C AC 22 C0 74 0B ...
Signature (55 AA)	1FE	55 AA

```
 Offset    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F       ASCII
00100000   EB 3C 90 6D 6B 66 73 2E  66 61 74 00 02 08 08 00   ë<.mkfs.fat.....
00100010   02 00 02 00 00 F8 00 01  3E 00 3C 00 00 08 00 00   .....ø..>.<.....
00100020   00 D0 07 00 80 01 29 C4  D5 44 A9 50 4C 41 4E 53   .Ð....)ÄÕD©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   ¾[|¬"Àt.V´.»..Í.
00100050   5E EB F0 32 E4 CD 16 CD  19 EB FE 54 68 69 73 20   ^ëð2äÍ.Í.ëþThis 
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 ... ...
```

- Bytes / Sector: 512
- Sectors / Cluster: 8
- Reserved Sectors: 8
- Sectors Before Partition: 2048
- Sectors / FAT: 256

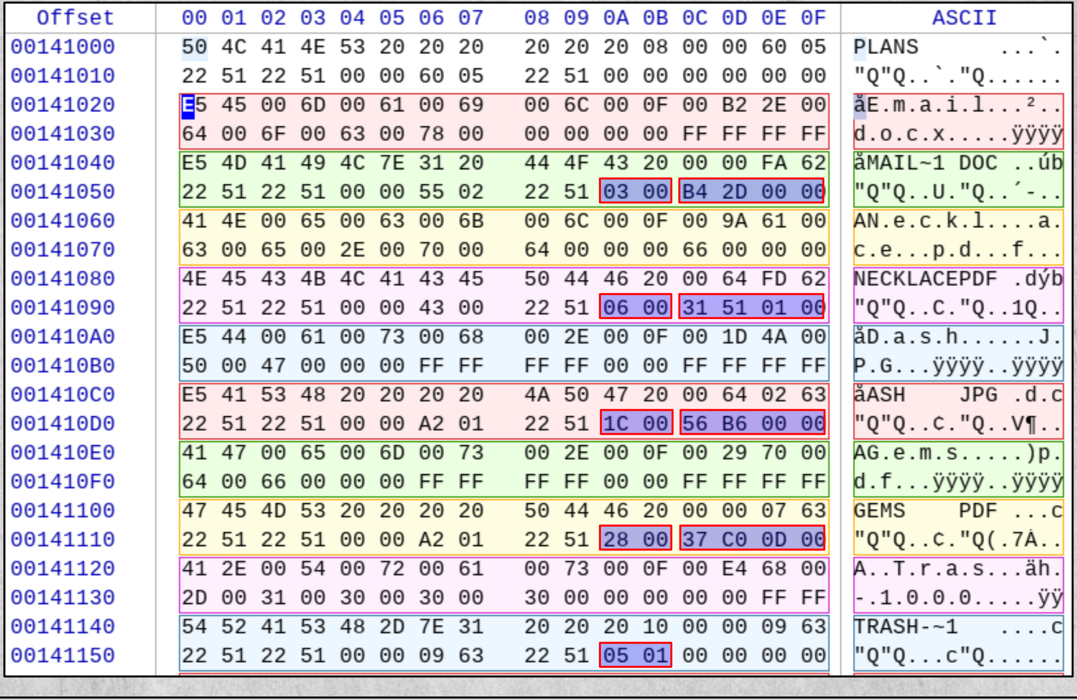
Partition #1 – FAT16 File Allocation Table



```
Offset     00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F   ASCII
00101000   F8 FF FF FF 00 00 04 00  05 00 FF FF 07 00 08 00   øÿÿÿ......ÿÿ....
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   ......ÿÿ...... .
00101040   21 00 22 00 23 00 24 00  25 00 26 00 27 00 FF FF   !.".#.$.%.&.'.ÿÿ
00101050   29 00 2A 00 2B 00 2C 00  2D 00 2E 00 2F 00 30 00   ).*.+.,.-.../.0.
                                   •
                                   •
                                   •
001011E0   F1 00 F2 00 F3 00 F4 00  F5 00 F6 00 F7 00 F8 00   ñ.ò.ó.ô.õ.ö.÷.ø.
001011F0   F9 00 FA 00 FB 00 FC 00  FD 00 FE 00 FF 00 00 01   ù.ú.û.ü.ý.þ.ÿ...
00101200   01 01 02 01 03 01 04 01  FF FF FF FF FF FF FF FF   ........ÿÿÿÿÿÿÿÿ
00101210   FF FF FF FF 00 00 00 00  00 00 00 00 00 00 00 00   ÿÿÿÿ............
```

- 4 files on FAT16 partition
- 1 Cluster Data Offset => 8 sectors before start of user data
- Clusters allocated for each file
  - File 1: 3
  - File 2: 22
  - File 3: 12
  - File 4: 221

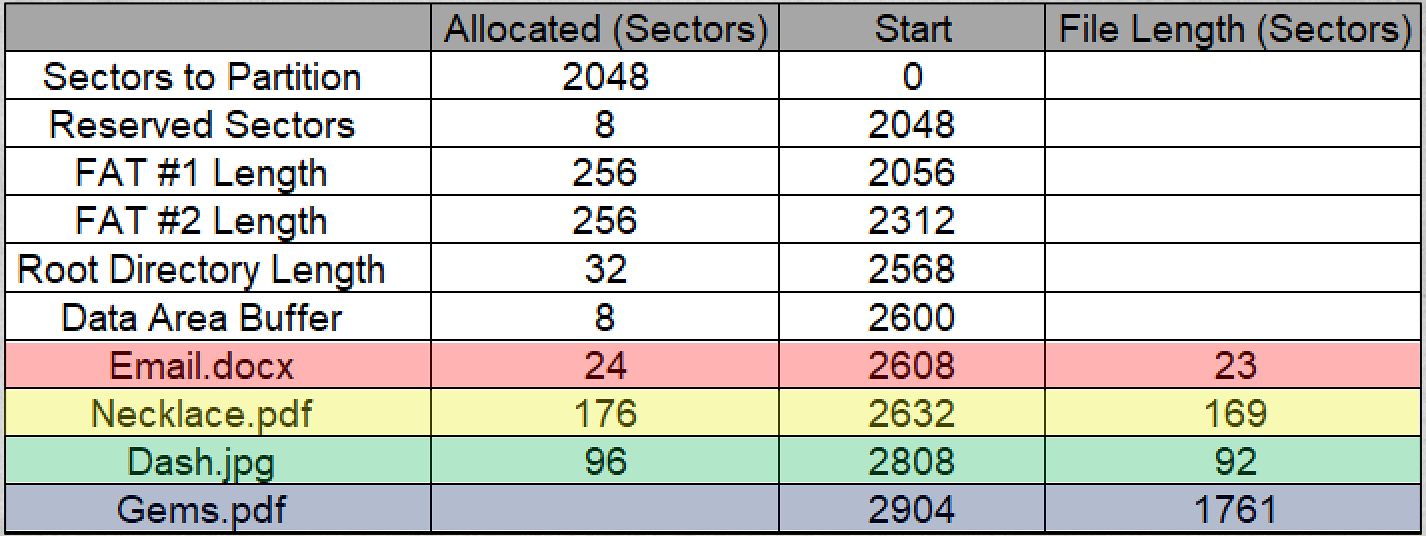
Partition #1 – FAT16 Root Directory



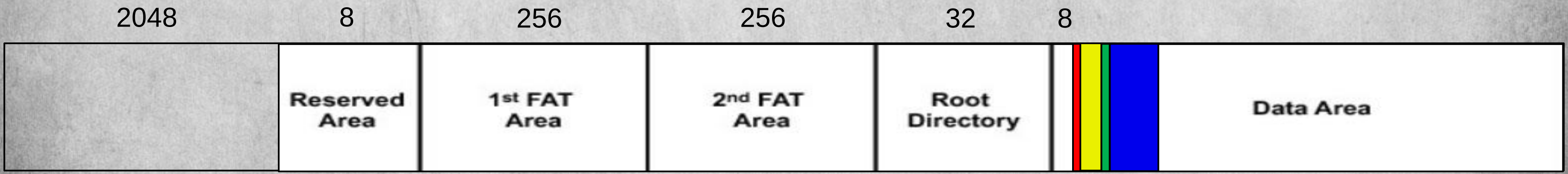
```
Offset      00 01 02 03 04 05 06 07   08 09 0A 0B 0C 0D 0E 0F   ASCII
00141000    50 4C 41 4E 53 20 20 20   20 20 20 08 00 00 60 05   PLANS      ...`.
00141010    22 51 22 51 00 00 60 05   22 51 00 00 00 00 00 00   "Q"Q..`."Q......
00141020    E5 45 00 6D 00 61 00 69   00 6C 00 0F 00 B2 2E 00   åE.m.a.i.l...²..
00141030    64 00 6F 00 63 00 78 00   00 00 00 00 FF FF FF FF   d.o.c.x.....ÿÿÿÿ
00141040    E5 4D 41 49 4C 7E 31 20   44 4F 43 20 00 00 FA 62   åMAIL~1 DOC ..úb
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 .dýb
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   åD.a.s.h......J.
001410B0    50 00 47 00 00 00 FF FF   FF FF 00 00 FF FF FF FF   P.G...ÿÿÿÿ..ÿÿÿÿ
001410C0    E5 41 53 48 20 20 20 20   4A 50 47 20 00 64 02 63   åASH    JPG .d.c
001410D0    22 51 22 51 00 00 A2 01   22 51 1C 00 56 B6 00 00   "Q"Q..c."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...ÿÿÿÿ..ÿÿÿÿ
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..c."Q(.7À..
00141120    41 2E 00 54 00 72 00 61   00 73 00 0F 00 E4 68 00   A..T.r.a.s...äh.
00141130    2D 00 31 00 30 00 30 00   30 00 00 00 00 00 FF FF   -.1.0.0.0.....ÿÿ
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......
```

Filename	Ext	Status	Clust Start (Hex)	Cluster Start	# Clusters	# Sectors	File Size (Hex)	File Size	File Size (Sectors)
Email	docx	Deleted	3	3	3	24	2db4	11700	23
Necklace	pdf	Active	6	6	22	176	15131	86321	169
Dash	jpg	Deleted	1C	28	12	96	b656	46678	92
Gems	pdf	Active	28	40	221	1768	dc037	901175	1761
Trash			105	261					

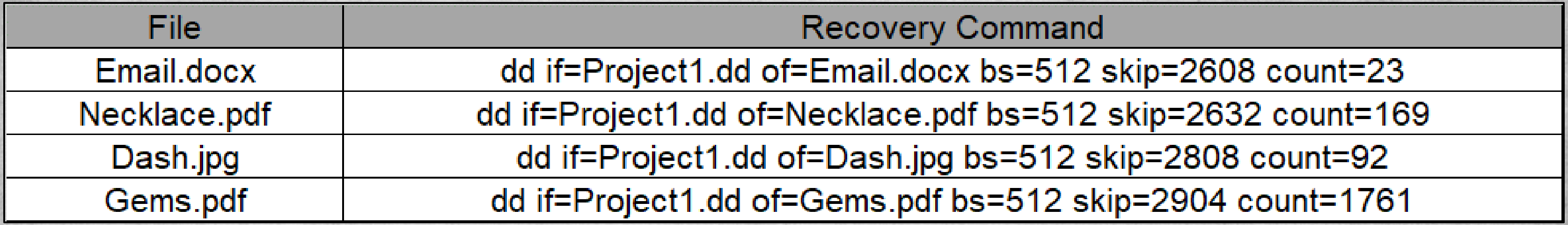
Partition #1 – FAT16 Data Area



	Allocated (Sectors)	Start	File Length (Sectors)
Sectors to Partition	2048	0	
Reserved Sectors	8	2048	
FAT #1 Length	256	2056	
FAT #2 Length	256	2312	
Root Directory Length	32	2568	
Data Area Buffer	8	2600	
Email.docx	24	2608	23
Necklace.pdf	176	2632	169
Dash.jpg	96	2808	92
Gems.pdf		2904	1761



Partition #1 – File Recovery and Analysis

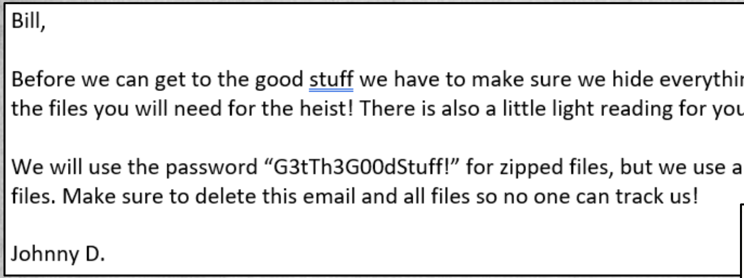


File	Recovery Command
Email.docx	dd if=Project1.dd of=Email.docx bs=512 skip=2608 count=23
Necklace.pdf	dd if=Project1.dd of=Necklace.pdf bs=512 skip=2632 count=169
Dash.jpg	dd if=Project1.dd of=Dash.jpg bs=512 skip=2808 count=92
Gems.pdf	dd if=Project1.dd of=Gems.pdf bs=512 skip=2904 count=1761

- Email.docx, Deleted
    - ✓ Email between John Disco and Bill Taker
        - o Zip file password: G3tTh3G00dStuff!
        - o Indicates gpg files will also be used
- Necklace.pdf, Active
    - ✓ A short story about a diamond necklace
- Dash.jpg, Deleted
    - ✓ An image for a game called diamond dash
- Gems.pdf, Active
    - ✓ Technical paper on gemology

Partition #1 – Recovered Files

Email.docx



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 for the heist! There is also a little light reading for you during your travels.

We will use the password “G3tTh3G00dStuff!” for zipped files, but we use another password for gpg files. Make sure to delete this email and all files so no one can track us!

Johnny D.

Gems.pdf

Gemology: The Developing Science of Gems

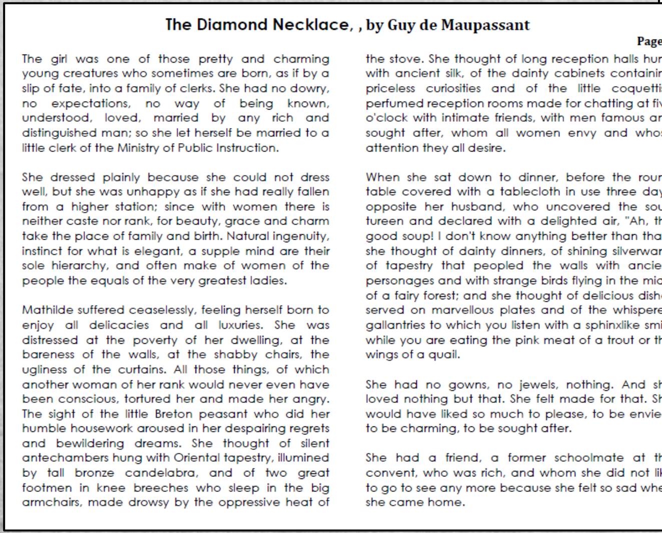
Emmanuel Fritsch[1] and Benjamin Rondeau[2]

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 i
its activities and its terminology. Gemology is becoming an
of specialization for mineralogists. If the study of beautiful, fa
seems frivolous to some, it is worth noting that 20 to 25 bil
year are at stake, and the study of natural gem materials ar

has evolved from a trade practice
to a recognized science. Its economic
field of application is the gems and
jewelry trade. About 150 billion

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 armchairs, made drowsy by the oppressive heat of 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.

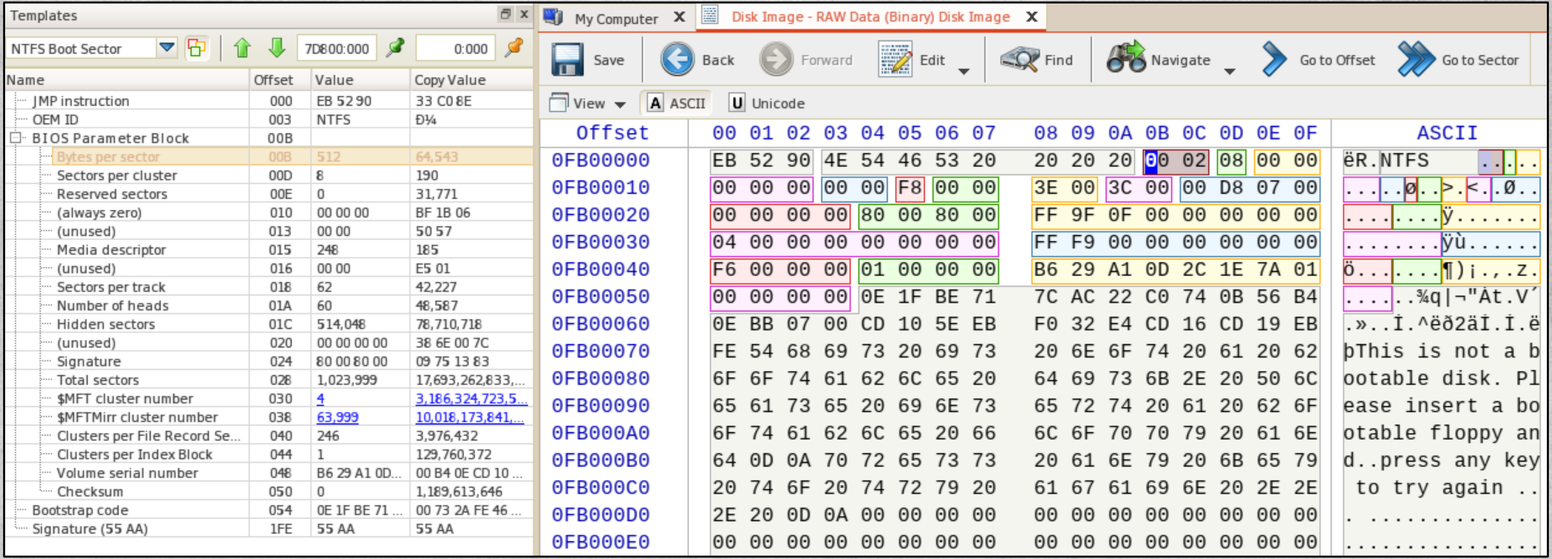
She had no gowns, no jewels, nothing. And she loved nothing but that. She felt made for that. She would have liked so much to please, to be envied, to be charming, to be sought after.

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 she came home.

Dash.jpg

Partition #2, NTFS

Partition #2 – NTFS Master Boot Record

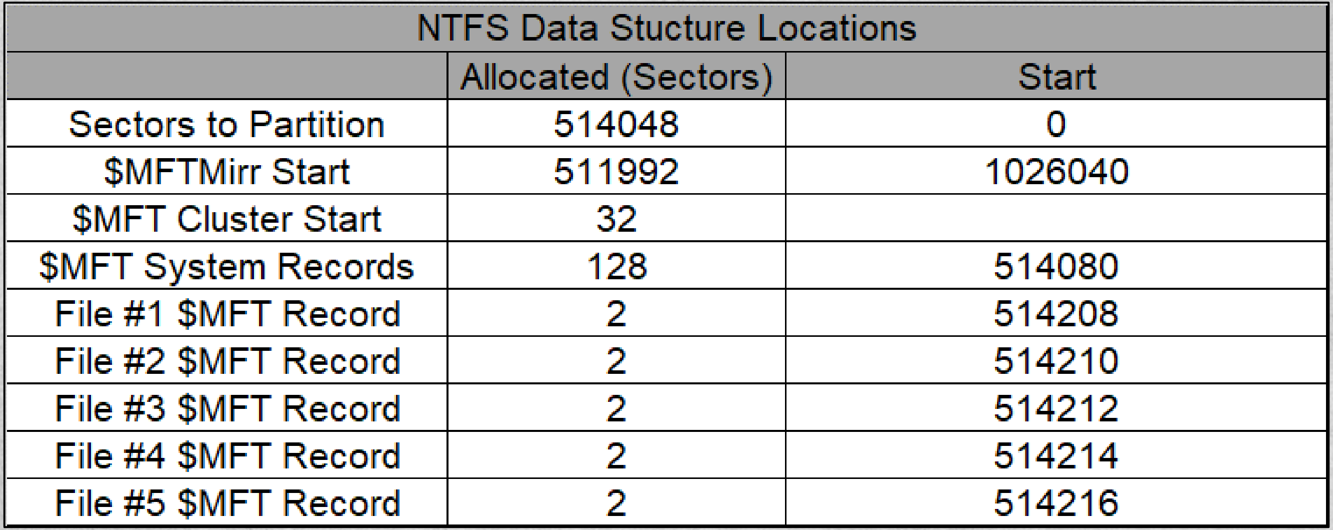


Name	Offset	Value	Copy Value
JMP instruction	000	EB 52 90	33 C0 8E
OEM ID	003	NTFS	Ð¼
BIOS Parameter Block	00B		
Bytes per sector	00B	512	64,543
Sectors per cluster	00D	8	190
Reserved sectors	00E	0	31,771
(always zero)	010	00 00 00	BF 1B 06
(unused)	013	00 00	50 57
Media descriptor	015	248	185
(unused)	016	00 00	E5 01
Sectors per track	018	62	42,227
Number of heads	01A	60	48,587
Hidden sectors	01C	514,048	78,710,718
(unused)	020	00 00 00 00	38 6E 00 7C
Signature	024	80 00 80 00	09 75 13 83
Total sectors	028	1,023,999	17,693,262,833,...
$MFT cluster number	030	4	3,186,324,723,5...
$MFTMirr cluster number	038	63,999	10,018,173,841,...
Clusters per File Record Se...	040	246	3,976,432
Clusters per Index Block	044	1	129,760,372
Volume serial number	048	B6 29 A1 0D...	00 B4 0E CD 10 ...
Checksum	050	0	1,189,613,646
Bootstrap code	054	0E 1F BE 71 ...	00 73 2A FE 46 ...
Signature (55 AA)	1FE	55 AA	55 AA

```
  Offset    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F       ASCII
0FB00000   EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00   ëR.NTFS     .....
0FB00010   00 00 00 00 00 F8 00 00  3E 00 3C 00 00 D8 07 00   .....ø..>.<..Ø..
0FB00020   00 00 00 00 80 00 80 00  FF 9F 0F 00 00 00 00 00   ........ÿ.......
0FB00030   04 00 00 00 00 00 00 00  FF F9 00 00 00 00 00 00   ........ÿù......
0FB00040   F6 00 00 00 01 00 00 00  B6 29 A1 0D 2C 1E 7A 01   ö.......¶)¡.,.z.
0FB00050   00 00 00 00 0E 1F BE 71  7C AC 22 C0 74 0B 56 B4   ......¾q|¬"Àt.V´
0FB00060   0E BB 07 00 CD 10 5E EB  F0 32 E4 CD 16 CD 19 EB   .»..Í.^ëð2äÍ.Í.ë
0FB00070   FE 54 68 69 73 20 69 73  20 6E 6F 74 20 61 20 62   þThis 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   ................
```

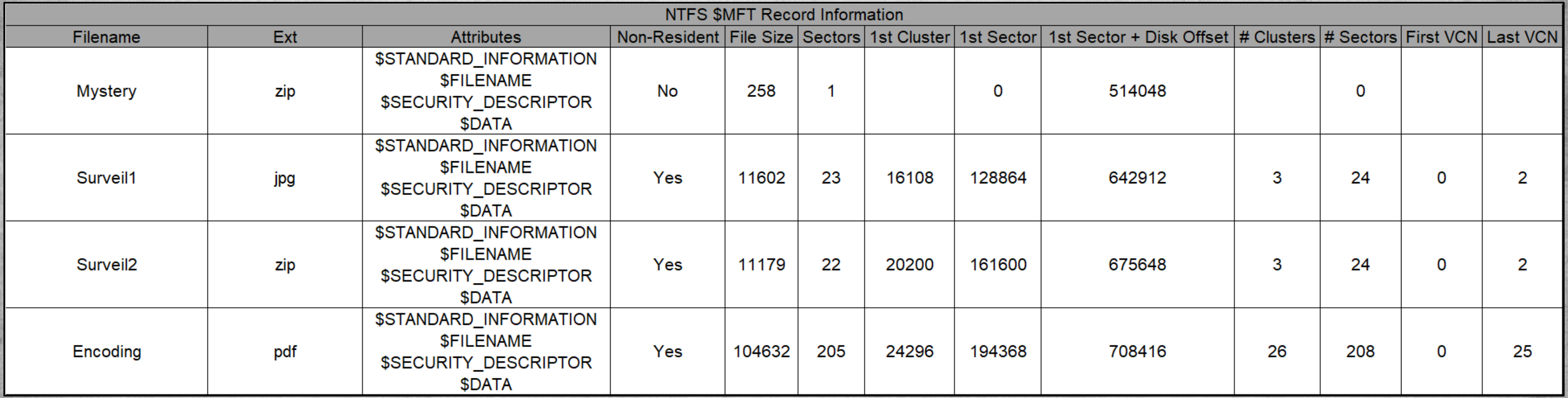
- Bytes / Sector: 512
- Sectors / Cluster: 8
- Reserved Sectors: 0
- Sectors Before Partition: 514048
- $MFT Cluster Start: 4
- # System $MFT Records: 64

Partition #2 – NTFS Data Structures



NTFS Data Stucture Locations		
	Allocated (Sectors)	Start
Sectors to Partition	514048	0
$MFTMirr Start	511992	1026040
$MFT Cluster Start	32	
$MFT System Records	128	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
File #5 $MFT Record	2	514216

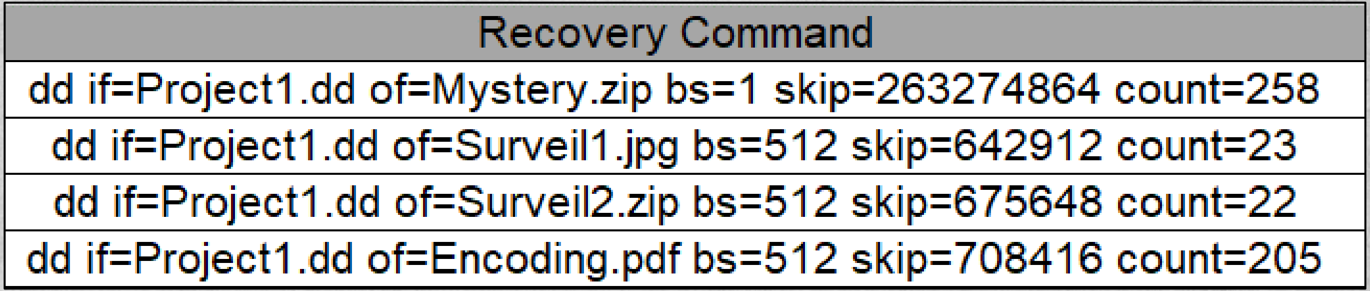
Partition #2 – $MFT Records



NTFS $MFT Record Information

Filename	Ext	Attributes	Non-Resident	File Size	Sectors	1st Cluster	1st Sector	1st Sector + Disk Offset	# Clusters	# Sectors	First VCN	Last VCN
Mystery	zip	$STANDARD_INFORMATION $FILENAME $SECURITY_DESCRIPTOR $DATA	No	258	1		0	514048		0		
Surveil1	jpg	$STANDARD_INFORMATION $FILENAME $SECURITY_DESCRIPTOR $DATA	Yes	11602	23	16108	128864	642912	3	24	0	2
Surveil2	zip	$STANDARD_INFORMATION $FILENAME $SECURITY_DESCRIPTOR $DATA	Yes	11179	22	20200	161600	675648	3	24	0	2
Encoding	pdf	$STANDARD_INFORMATION $FILENAME $SECURITY_DESCRIPTOR $DATA	Yes	104632	205	24296	194368	708416	26	208	0	25

Partition #2 – File Recovery and Analysis

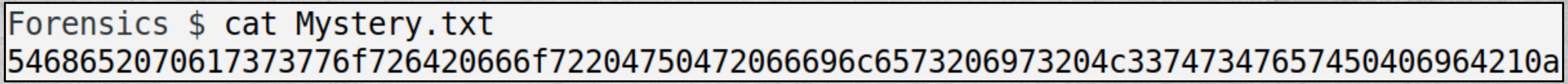


Recovery Command
dd if=Project1.dd of=Mystery.zip bs=1 skip=263274864 count=258
dd if=Project1.dd of=Surveil1.jpg bs=512 skip=642912 count=23
dd if=Project1.dd of=Surveil2.zip bs=512 skip=675648 count=22
dd if=Project1.dd of=Encoding.pdf bs=512 skip=708416 count=205

- Mystery.zip, Deleted, Zip Encrypted
  - ✓ Hex encoded payload
  - ✓ Decodes to “The password for GPG files is L3tsGetP@id!”
- Surveil1.jpg, Active, Unencrypted
  - ✓ An aerial view of the U.S. capital
- Surveil2.zip, Deleted, Zip Encrypted
  - ✓ An image of the Smithsonian Museum in Washington D.C.
- Encoding.pdf. Active, Unencrypted
  - ✓ A guide on encoding schemes useful for decoding Mystery.zip

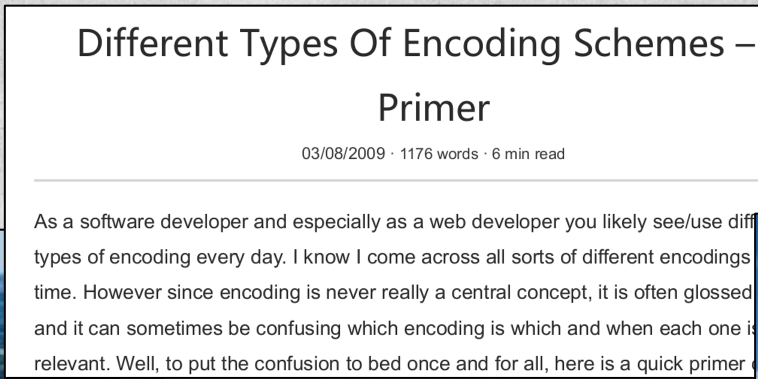
Partition #2 – Recovered Files

Mystery.txt



```
Forensics $ cat Mystery.txt
5468652070617373776f726420666f72204750472066696c6573206973204c33747347657450406964210a
```

Encoding.pdf



Different Types Of Encoding Schemes – A Primer

03/08/2009 · 1176 words · 6 min read

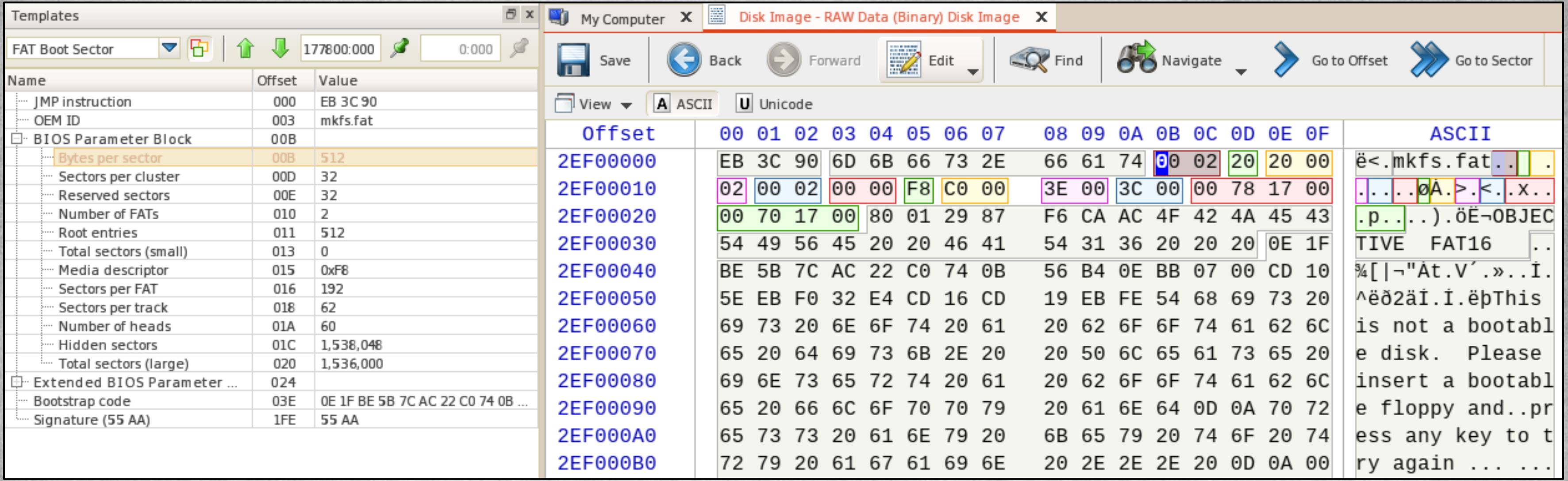
As a software developer and especially as a web developer you likely see/use diff types of encoding every day. I know I come across all sorts of different encodings time. However since encoding is never really a central concept, it is often glossed and it can sometimes be confusing which encoding is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

Surveil1.jpg

Surveil2.jpg

Partition #3, FAT16

Partition #3 – FAT16 Boot Sector

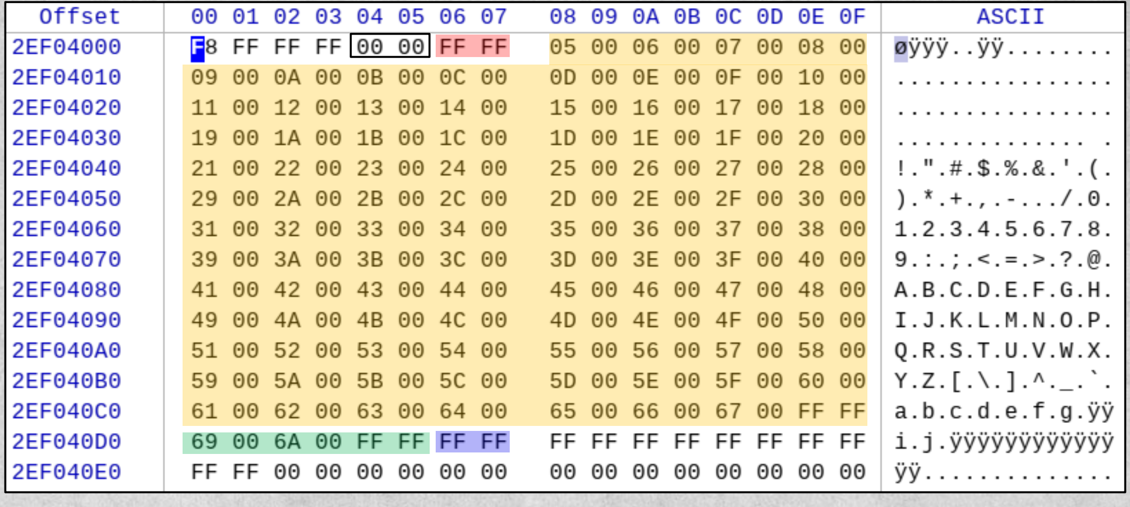


Name	Offset	Value
JMP instruction	000	EB 3C 90
OEM ID	003	mkfs.fat
BIOS Parameter Block	00B	
Bytes per sector	00B	512
Sectors per cluster	00D	32
Reserved sectors	00E	32
Number of FATs	010	2
Root entries	011	512
Total sectors (small)	013	0
Media descriptor	015	0xF8
Sectors per FAT	016	192
Sectors per track	018	62
Number of heads	01A	60
Hidden sectors	01C	1,538,048
Total sectors (large)	020	1,536,000
Extended BIOS Parameter ...	024	
Bootstrap code	03E	0E 1F BE 5B 7C AC 22 C0 74 0B ...
Signature (55 AA)	1FE	55 AA

```
Offset     00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F       ASCII
2EF00000   EB 3C 90 6D 6B 66 73 2E  66 61 74 00 02 20 20 00   ë<.mkfs.fat.. .
2EF00010   02 00 02 00 00 F8 C0 00  3E 00 3C 00 00 78 17 00   ......øÀ.>.<..x..
2EF00020   00 70 17 00 80 01 29 87  F6 CA AC 4F 42 4A 45 43   .p....).öÊ¬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   ¾[|¬"Àt.V´.»..Í.
2EF00050   5E EB F0 32 E4 CD 16 CD  19 EB FE 54 68 69 73 20   ^ëð2äÍ.Í.ëþThis
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 ... ...
```

- Bytes / Sector: 512
- Sectors / Cluster: 32
- Reserved Sectors: 32
- Sectors Before Partition: 1,538,048
- Sectors / FAT: 192

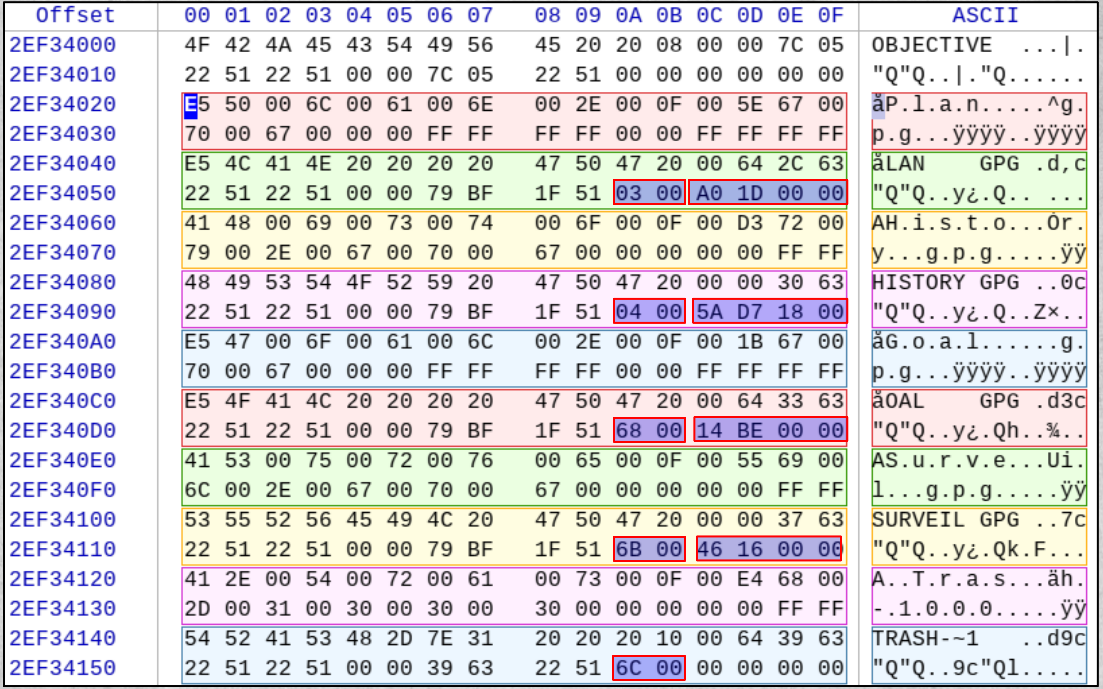
Partition #3 – FAT16 File Allocation Table



```
Offset    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F      ASCII
2EF04000  F8 FF FF FF 00 00 FF FF  05 00 06 00 07 00 08 00  øÿÿÿ..ÿÿ........
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.ÿÿ
2EF040D0  69 00 6A 00 FF FF FF FF  FF FF FF FF FF FF FF FF  i.j.ÿÿÿÿÿÿÿÿÿÿÿÿ
2EF040E0  FF FF 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ÿÿ..............
```

- 4 files on FAT16 partition
- 1 Cluster = 32 sectors into data area before start of user data
- Clusters allocated for each file
  - File 1: 1
  - File 2: 100
  - File 3: 3
  - File 4: 1

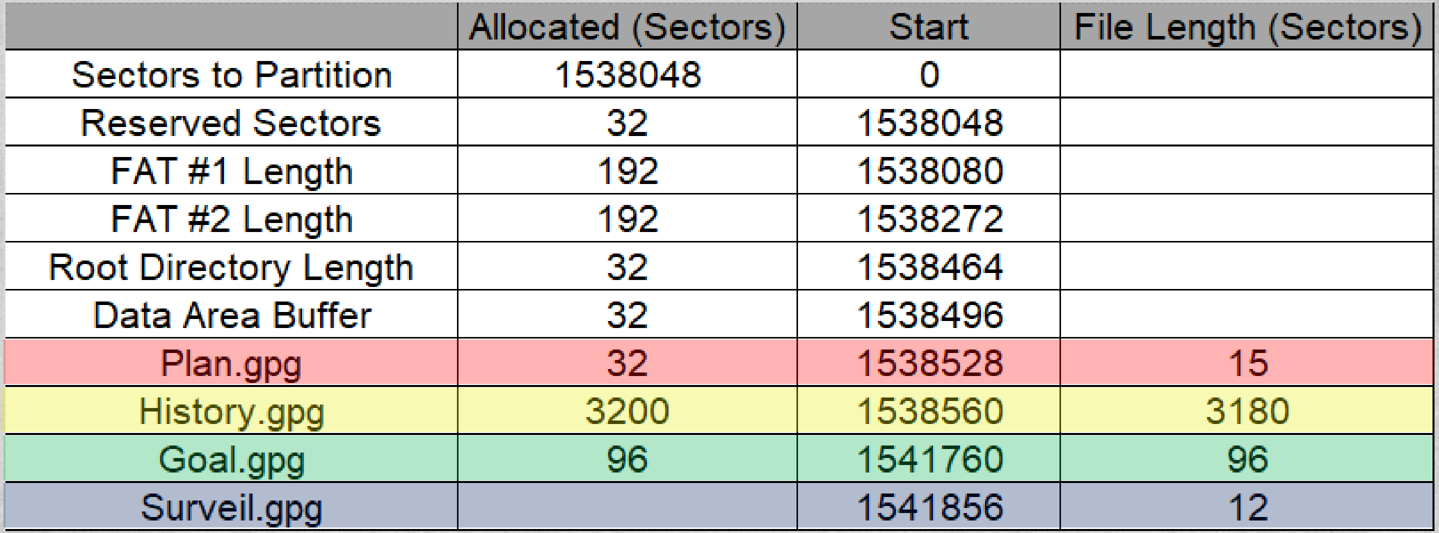
Partition #3 – FAT16 Root Directory



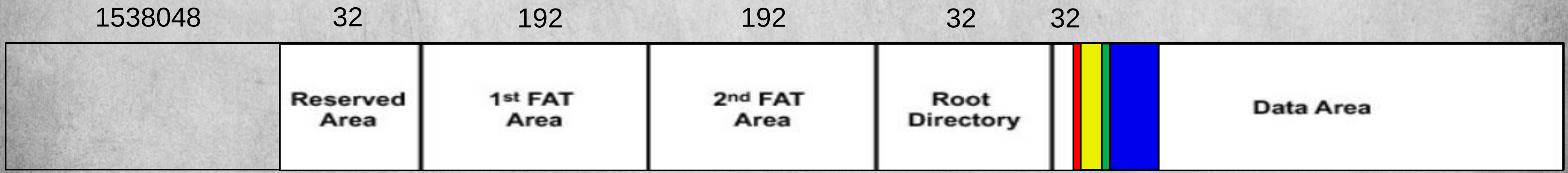
```
Offset     00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F       ASCII
2EF34000   4F 42 4A 45 43 54 49 56  45 20 20 08 00 00 7C 05   OBJECTIVE  ...|.
2EF34010   22 51 22 51 00 00 7C 05  22 51 00 00 00 00 00 00   "Q"Q..|."Q......
2EF34020   E5 50 00 6C 00 61 00 6E  00 2E 00 0F 00 5E 67 00   åP.l.a.n.....^g.
2EF34030   70 00 67 00 00 00 FF FF  FF FF 00 00 FF FF FF FF   p.g...ÿÿÿÿ..ÿÿÿÿ
2EF34040   E5 4C 41 4E 20 20 20 20  47 50 47 20 00 64 2C 63   åLAN    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...Ór.
2EF34070   79 00 2E 00 67 00 70 00  67 00 00 00 00 00 FF FF   y...g.p.g.....ÿÿ
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   åG.o.a.l......g.
2EF340B0   70 00 67 00 00 00 FF FF  FF FF 00 00 FF FF FF FF   p.g...ÿÿÿÿ..ÿÿÿÿ
2EF340C0   E5 4F 41 4C 20 20 20 20  47 50 47 20 00 64 33 63   åOAL    GPG .d3c
2EF340D0   22 51 22 51 00 00 79 BF  1F 51 68 00 14 BE 00 00   "Q"Q..y¿.Qh..¾..
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.....ÿÿ
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...äh.
2EF34130   2D 00 31 00 30 00 30 00  30 00 00 00 00 00 FF FF   -.1.0.0.0.....ÿÿ
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.....
```

Filename	Ext	Status	Clust Start (Hex)	Cluster Start	# Clusters	# Sectors	File Size (Hex)	File Size	File Size (Sectors)
Plan	gpg	Deleted	3	3	1	32	1da0	7584	15
History	gpg	Active	4	4	100	3200	18d75a	1627994	3180
Goal	gpg	Deleted	68	104	3	96	be14	48660	96
Surveil	gpg	Active	6b	107	1	32	1646	5702	12
Trash			6c	108					

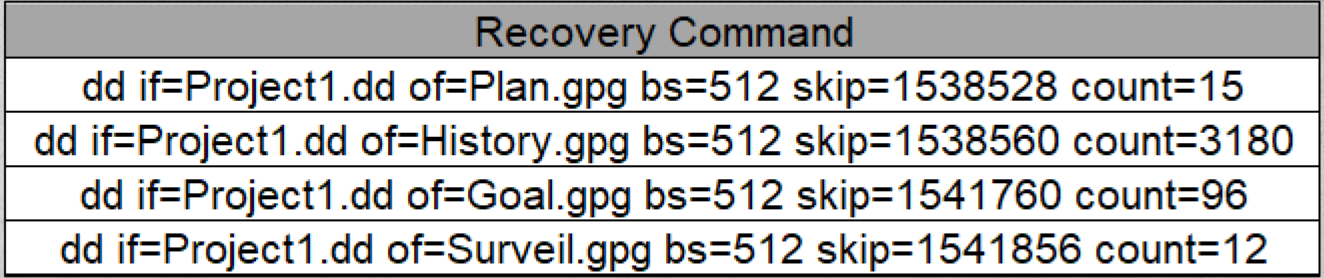
Partition #3 – FAT16 Data Area



	Allocated (Sectors)	Start	File Length (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	
Plan.gpg	32	1538528	15
History.gpg	3200	1538560	3180
Goal.gpg	96	1541760	96
Surveil.gpg		1541856	12



Partition #3 – File Recovery and Analysis



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

- Using “L3tsGetP@id!” from partititon #2 to decrypt gpg files

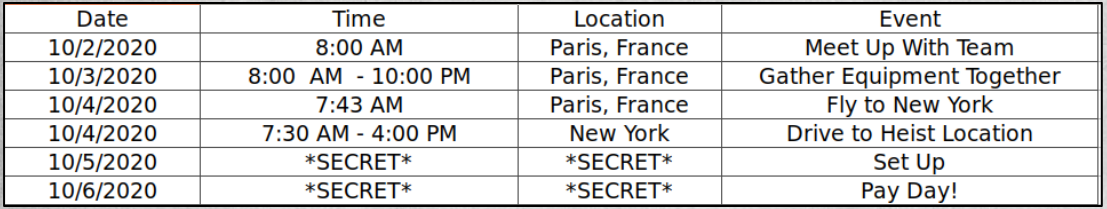
- Plan.gpg, Deleted, Encrypted
  - ✓ gpg -d Plan.gpg > Plan
  - ✓ file Plan
  - ✓ mv Plan Plan.xls

- History.gpg, Active, Encrypted
  - ✓ gpg -d History.gpg > History
  - ✓ file History
  - ✓ Mv History History,pdf

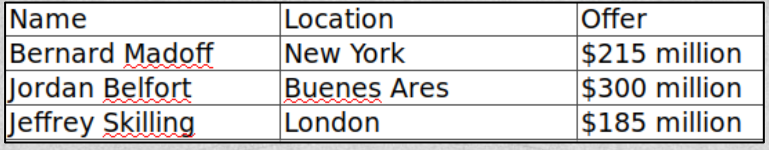
- Goal.gpg, Deleted, Encrypted
  - ✓ gpg -d Goal.gpg > Goal
  - ✓ file Goal
  - ✓ mv Goal Goal.jpg
- Surveil.gpg, Deleted, Encrypted
  - ✓ gpg -d Surveil.gpg > Surveil
  - ✓ file Surveil
  - ✓ mv Surveil Surveil.jpg

Partition #3 – Recovered Files

Plan.xls

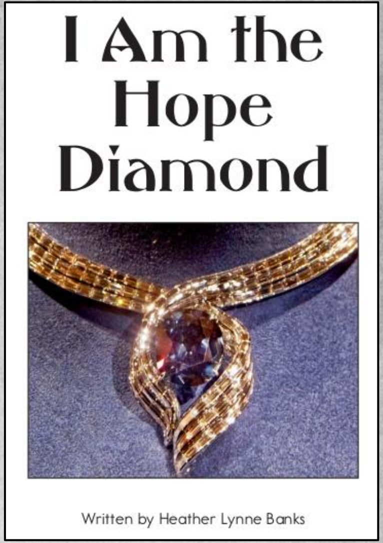


Date	Time	Location	Event
10/2/2020	8:00 AM	Paris, France	Meet Up With Team
10/3/2020	8:00 AM - 10:00 PM	Paris, France	Gather Equipment Together
10/4/2020	7:43 AM	Paris, France	Fly to New York
10/4/2020	7:30 AM - 4:00 PM	New York	Drive to Heist Location
10/5/2020	*SECRET*	*SECRET*	Set Up
10/6/2020	*SECRET*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



Name	Location	Offer
Bernard Madoff	New York	$215 million
Jordan Belfort	Buenes Ares	$300 million
Jeffrey Skilling	London	$185 million

History.pdf



I Am the Hope Diamond

Written by Heather Lynne Banks

Goal.jpg

Surveil.jpg

Project #1 Lessons Learned

Project #1 Considerations

- Each of the partitions provided parts of the project solution
- A solid technical understanding of each partition type is necessary to move forward with the project
  - ✓ FAT16 File Allocation Tables
    - Data area starting point
    - Cluster locations
  - ✓ FAT16 Root Directory
    - File Size
  - ✓ NTFS Formatting
  - ✓ NTFS MFT Records

Forensics Challenges

Capture The Flag

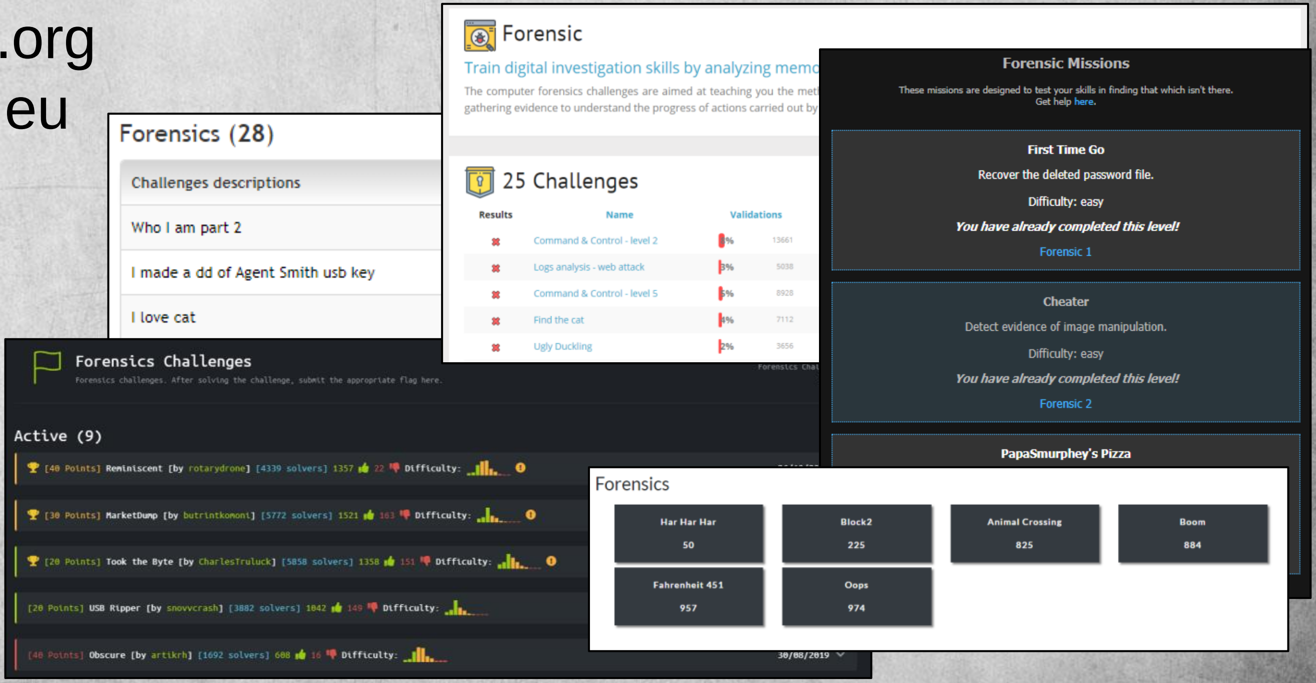
- One of the methods used in maintaining proficiency with digital forensics or any technical field is participation in “Capture The Flag” (i.e. CTF) events
- CTF events are very common in both cybersecurity education and industry and there are numerous CTF events on campus this year
  - ✓ Auburn Ethical Hacking Club
  - ✓ Cyber Fire Puzzles
  - ✓ Auburn ACM Hackathon
- The next few scenarios will introduce you to the CTF type questions and walk you through the process of answering them

CTF Flags

- There are several methods used in CTF’s to prove that a problem has been solved
- Generally a “flag” is embedded somewhere in a problem set and must be recovered by the participant
- Some examples of CTF flags include:
  - ✓ Flag(This_Is_A_Flag)
  - ✓ flag{rdnf099304jgewd}
  - ✓ Aubie(AuburnSpecificFlag)
  - ✓ CTF(0x43807328083)

CTF Platforms

- There are a wide variety of openly available and commercial CTF events available to develop your technical skillset
  - ✓ ctf.auburn.edu
  - ✓ hackthissite.org
  - ✓ hackthebox.eu
  - ✓ root-me.org



Forensics (28)

Challenges descriptions

Who I am part 2

I made a dd of Agent Smith usb key

I love cat

Forensic

Train digital investigation skills by analyzing memo

The computer forensics challenges are aimed at teaching you the met
gathering evidence to understand the progress of actions carried out by

25 Challenges

Results	Name	Validations	
✖	Command & Control - level 2	8%	13661
✖	Logs analysis - web attack	3%	5038
✖	Command & Control - level 5	5%	8928
✖	Find the cat	4%	7112
✖	Ugly Duckling	2%	3656

Forensic Missions

These missions are designed to test your skills in finding that which isn't there.
Get help here.

First Time Go

Recover the deleted password file.

Difficulty: easy

You have already completed this level!

Forensic 1

Cheater

Detect evidence of image manipulation.

Difficulty: easy

You have already completed this level!

Forensic 2

PapaSmurphey's Pizza

Forensics Challenges

Forensics challenges. After solving the challenge, submit the appropriate flag here.

Active (9)

```
🏆 [40 Points] Reminiscent [by rotarydrone] [4339 solvers] 1357 👍 22 👎 Difficulty:
🏆 [30 Points] MarketDump [by butrintkomoni] [5772 solvers] 1521 👍 163 👎 Difficulty:
🏆 [20 Points] Took the Byte [by CharlesTruluck] [5858 solvers] 1358 👍 151 👎 Difficulty:
[20 Points] USB Ripper [by snovvcrash] [3882 solvers] 1042 👍 149 👎 Difficulty:
[40 Points] Obscure [by artikrh] [1692 solvers] 608 👍 16 👎 Difficulty:                30/08/2019
```

Forensics

Har Har Har 50	Block2 225	Animal Crossing 825	Boom 884
Fahrenheit 451 957	Oops 974		

Challenge #1 – Metamorphosis

A user generated a digital artifact named “Mystery1” which contains an obfuscated password. Using your analysis skills, determine the password.

Challenge #2 – Flag Finding

A digital artifact named “Mystery2” contains an embedded flag. What is the flag?

Challenge #3 – Tesseract

An image contains a long set of characters. Extract the characters from the image.

References

- CTF Resources
  - ✓ https://github.com/apsdehal/awesome-ctf

- CTF Platforms
  - ✓ https://ctf.auburn.edu
  - ✓ https://www.root-me.org
  - ✓ https://ringzer0ctf.com
  - ✓ https://www.hackthebox.eu