Data Loss Prevention - Disk Analysis

- Disk Structure.
- Finding Files.
- Mining Content.
- Carving Files (Undeleting)

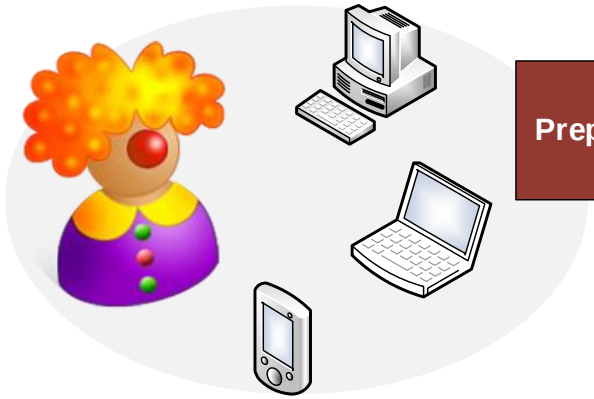
http://asecuritysite.com/dlp

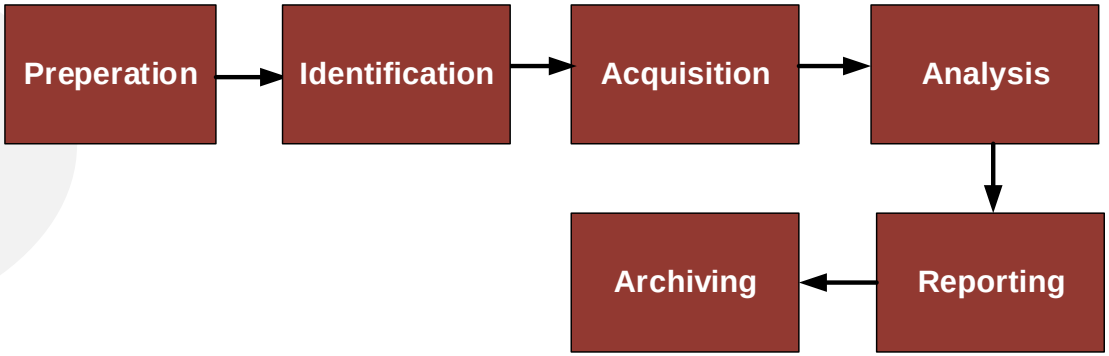
Author: Prof Bill Buchanan

Data Loss Detection/ Prevention

Outline

Author: Prof Bill Buchanan

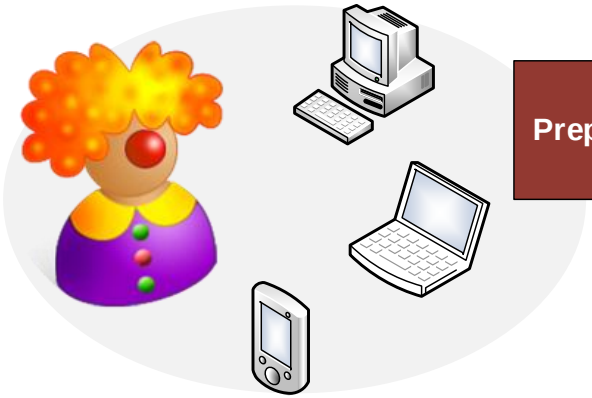




ACPO Good Practice Guide for Computer-Based Evidence

- No action taken by law enforcement agencies or their agents should **change data held on a computer or storage media** which may subsequently be relied upon in court.
- In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be **competent to do so** and be able to give evidence explaining the relevance and the implications of their actions.
- **An audit trail** or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Author: Prof Bill Buchanan



Preperation → Identification → Acquisition → Analysis → Reporting → Archiving

HDD

HDD Analysis (3TB SATA HDD)
- Archive: 6 hours
- Cost: $0.04/GB
- Throughput: 123 MB/s
- IOPS (Input/Output Operations Per Second): 135

SSD

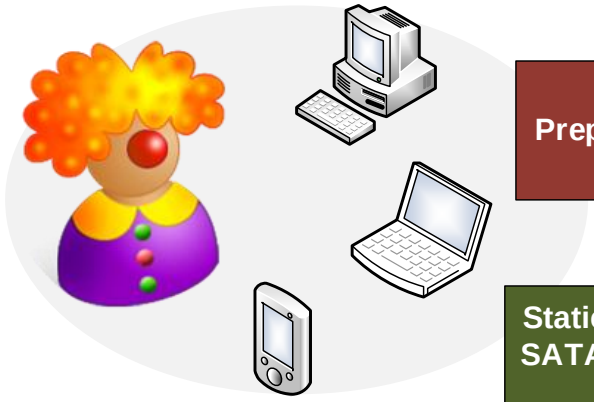
SDD Analysis (512GB SATA SSD)
- Archive: 17 mins
- Cost: $0.74/GB
- Throughput: 500 MB/s
- IOPS (Input/Output Operations Per Second): 80,000

Flash

SD 2.0
- Throughput: 25MB/s.
- Cost: $0.74/GB.

UHS-II
Throughput: 312MB/s.

Author: Prof Bill Buchanan



Preperation → Identification → Acquisition → Analysis → Reporting → Archiving

Static Analysis (3TB SATA HDD disk: >11 hrs

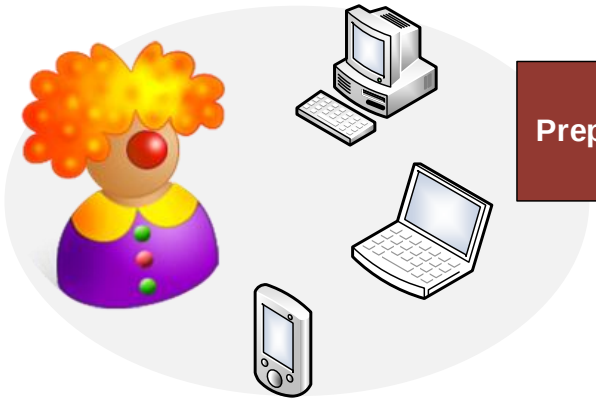
Static Analysis (512GB SATA SDD disk: >17 mins

Collection (dd/FTK/EnCase) → Open Source Forensics Analysis (Sleuthkit)

Bit-by-bit copy:
.dd (produces RAW format)

Meta-data:
.E01 (EnCase Evidence File)
.AFF (Advanced Forensics Format)

Author: Prof Bill Buchanan

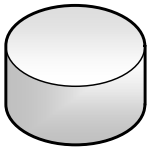


Preperation → Identification → Acquisition → Analysis → Reporting → Archiving

Open Source Forensics Analysis (Sleuthkit)

MD5/SHA1 Hash	Hash Lookup	File Type ID (Magic No)	ZIP extract	Text added to Keywords	...

File Analysis Phase

Collection (dd/FTK/EnCase) →  **Database (SQL, MySQL)**

Post Processing Phase

RegRipper	Web Browser Analysis	Search Keyword Search	Check for Known File/ Folder names	Summary Report	...

Ref: V.Rousev, Digital Investigator (2013), 1-10

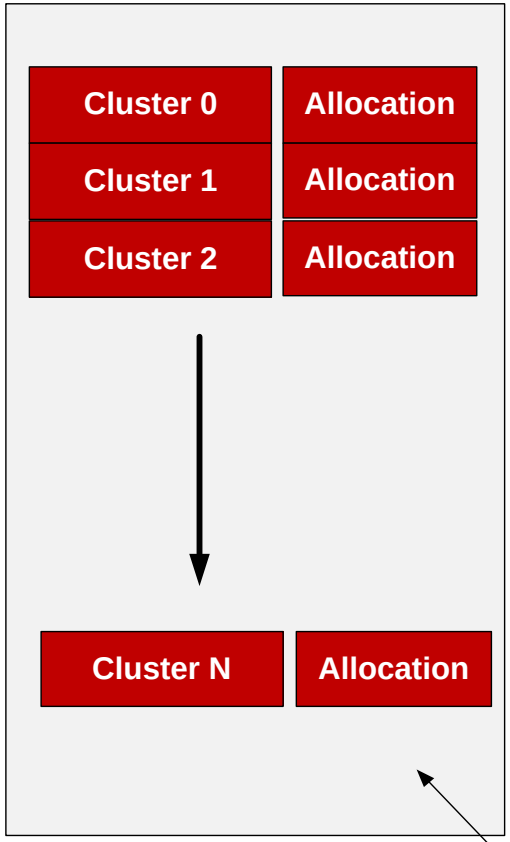
Author: Prof Bill Buchanan

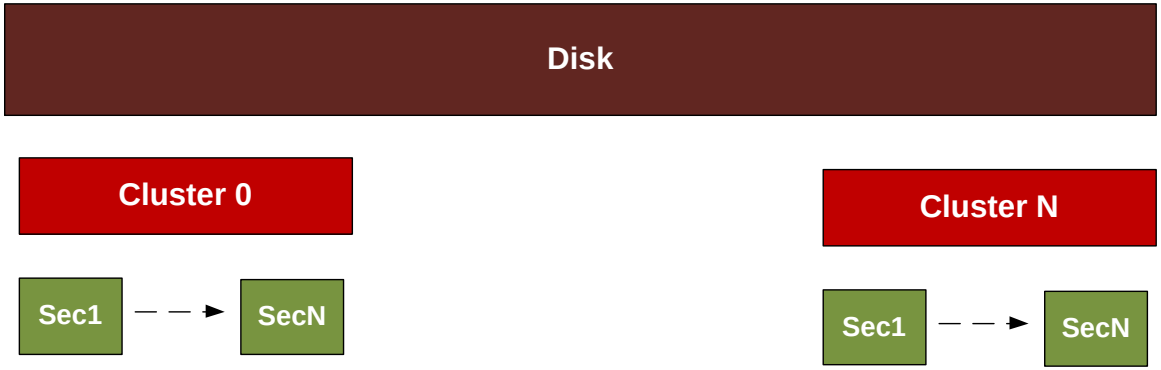
Data Loss Detection/ Prevention

Disk Structures

Author: Prof Bill Buchanan

File Allocation Table



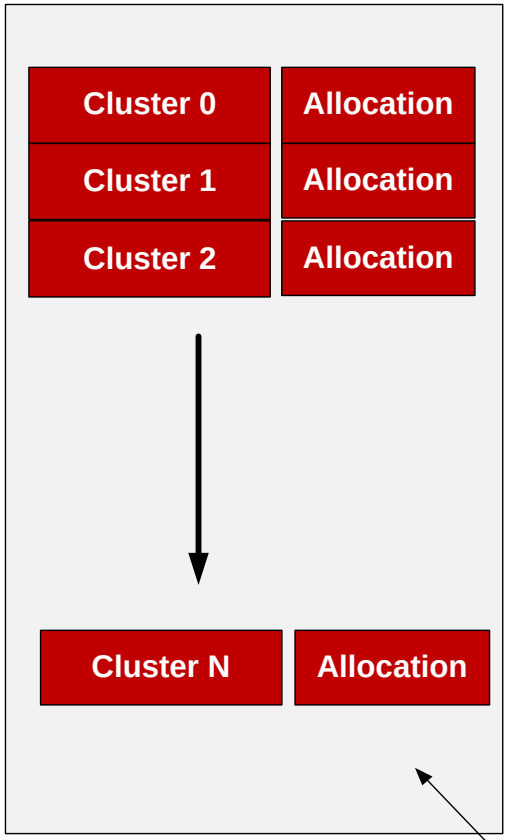


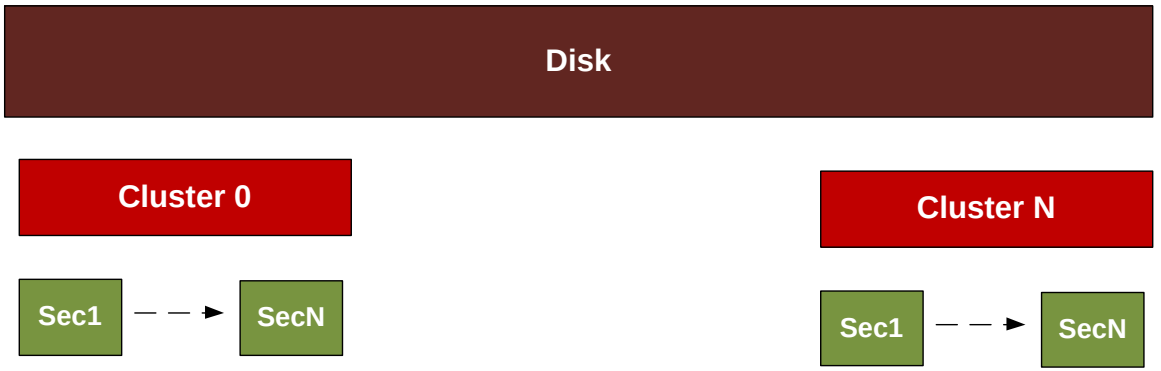
No of Clusters:	N
No of sectors per cluster:	1, 2, 4, 6, 16, 32, 64 or 128
No of bytes per sector:	512 bytes, 1KB, 2KB or 4KB

For 16-bit Cluster entry -> 2^{16} entries -> 65,536 (64K) – **FAT16**
For 28-bit Cluster entry -> 2^{28} entries -> 268,435,456 (256M) – **FAT32**

Author: Prof Bill Buchanan

File Allocation Table





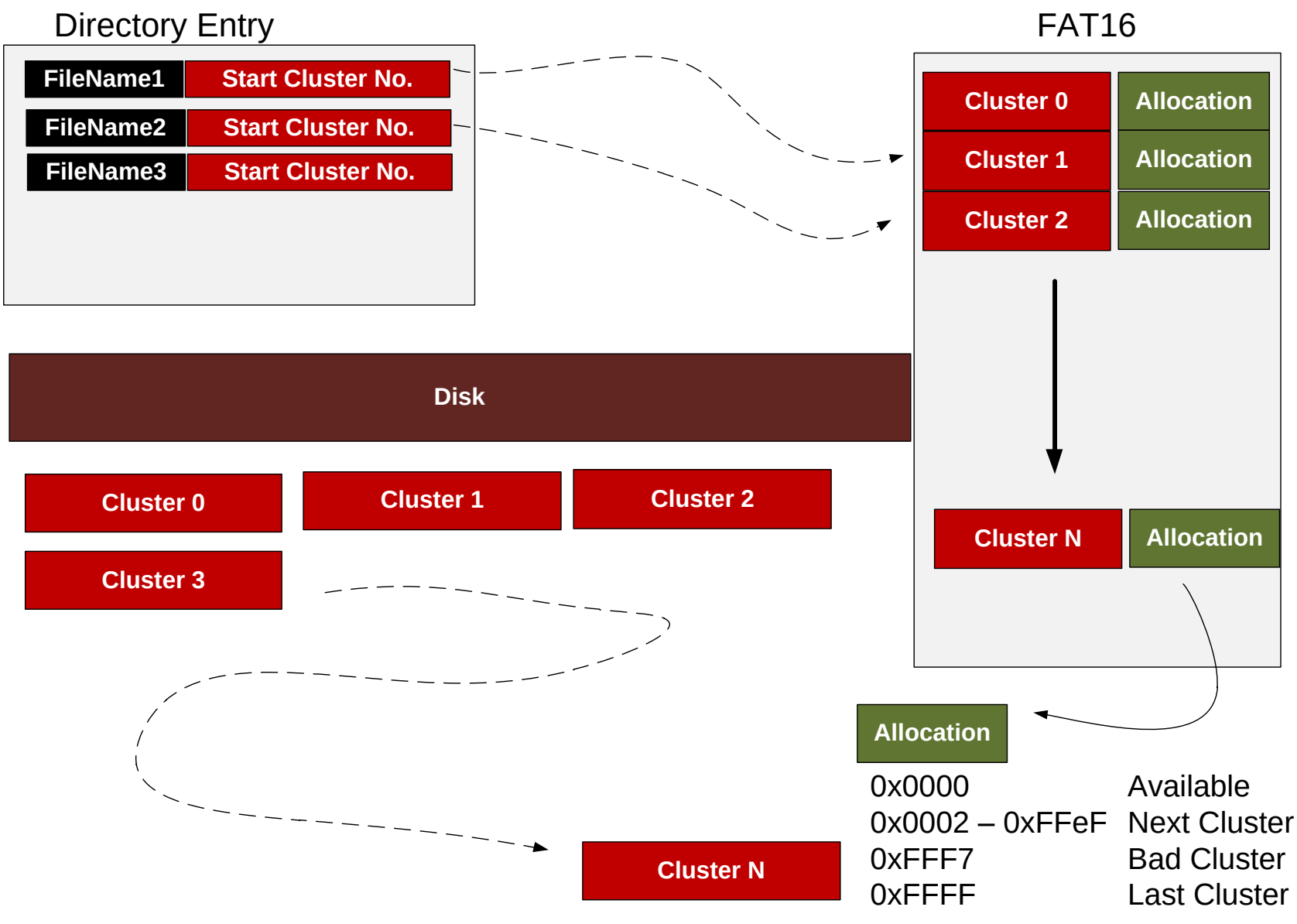
No of Clusters: N
No of sectors per cluster: 1, 2, 4, 6, 16, 32, 64 or 128
No of bytes per sector: 512 bytes, 1KB, 2KB or 4KB

Example:
FAT16 - 64 sectors per cluster, 512 Bytes per sector
= 32kB per cluster
Disk space = 64K * 32KB = 2048MB = 2 GB

FAT32 - 16 sectors per cluster, 512 Bytes per sector
= 8kB per cluster
Disk space = 256M * 8KB = 2048GB = 2TB

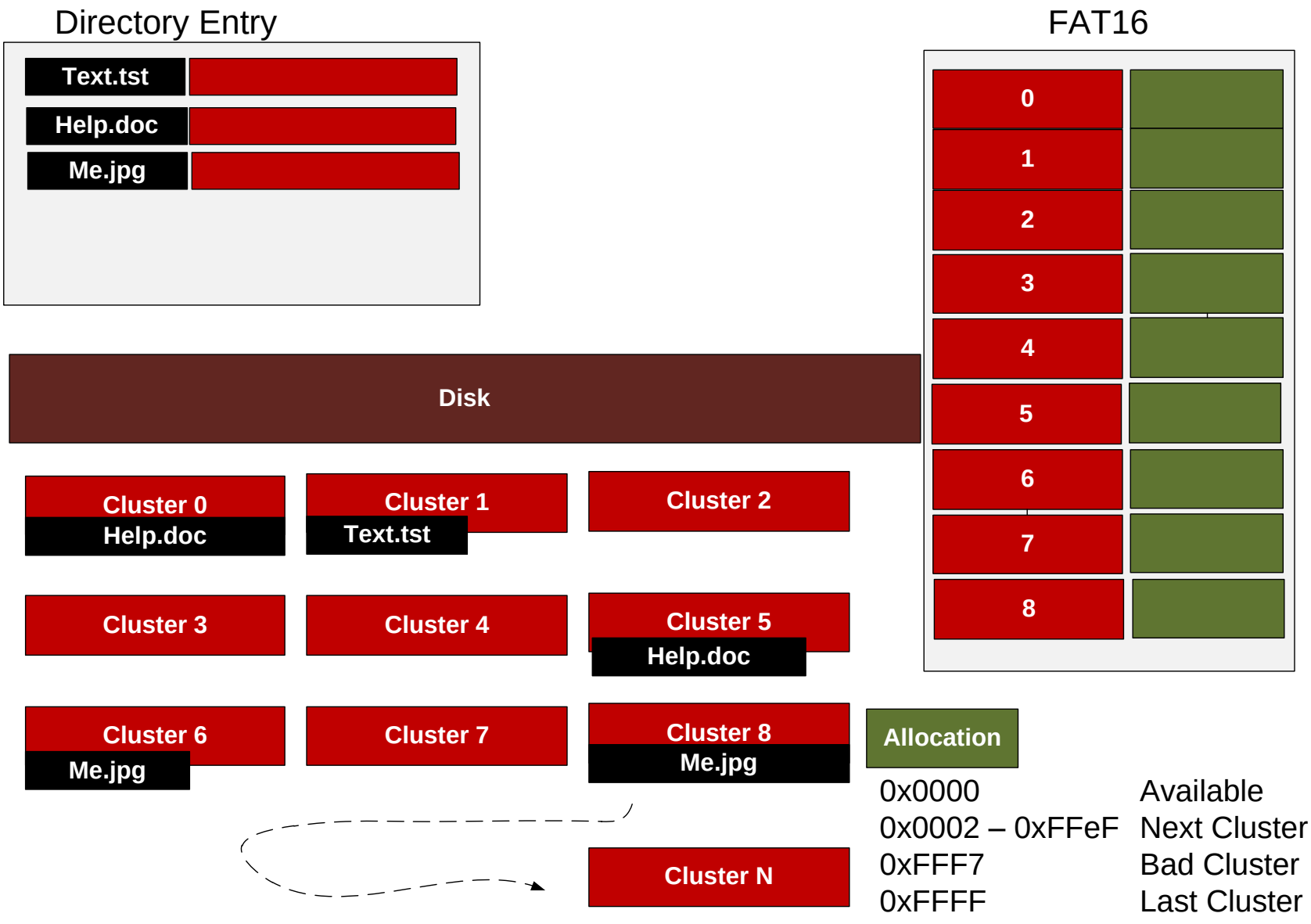
For 16-bit Cluster entry -> 2^{16} entries -> 65,536 (64K) – **FAT16**
For 28-bit Cluster entry -> 2^{28} entries -> 268,435,456 (256M) – **FAT32**

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

FAT16 Example



Structure

Disk Forensics

Author: Prof Bill Buchanan

Fragmentation

Directory Entry

Text.tst	1
Help.doc	0
Me.jpg	8

FAT16

0	0x0005
1	0xFFFF
2	0x0000
3	0x0000
4	0x0000
5	0xFFFF
6	0xFFFF
7	0x0000
8	0x0006

Disk

Cluster 0 Help.doc	Cluster 1 Text.tst	Cluster 2
Cluster 3	Cluster 4	Cluster 5 Help.doc
Cluster 6 Me.jpg	Cluster 7	Cluster 8 Me.jpg
		Cluster N

Allocation	
0x0000	Available
0x0002 – 0xFFeF	Next Cluster
0xFFF7	Bad Cluster
0xFFFF	Last Cluster

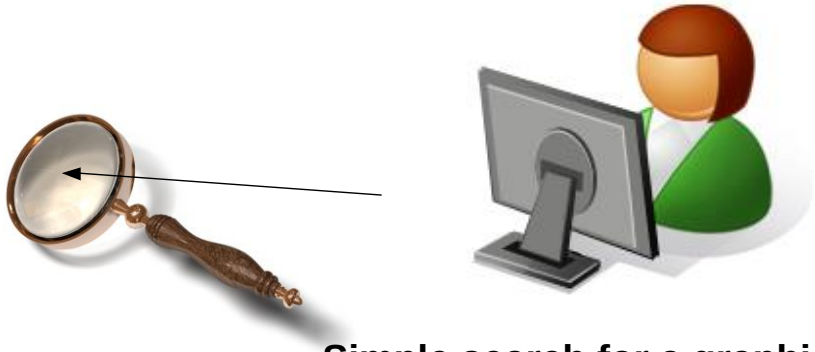
Author: Prof Bill Buchanan

Data Loss Detection/ Prevention

File Signatures

Author: Prof Bill Buchanan

File Allocation Table:
1.txt
2.doc
Test.doc
-Delete.gif [deleted]



Simple search for a graphic file will not find the deleted file

Deep scan of the Disk (byte-by-byte)

Author: Prof Bill Buchanan

Toolkit 1.7 (Author: ProfSIMS)

File

Network | Client | Server | Packet Capture | WinDump | Snort | Events | Binary Reader | Encryption | Coding | OS | IP | Demo

View GIFs | View JPGs | View ZIPs | Open Any | -- Open Mystery File -- | Identify file type

F:\docs\src\clientToolkit\log\cat01_with_hidden_text.gif

Tutorial

Hex viewer

00	47	49	46	38	39	61	64	00	55	00	E6	00	00	FF	FF	FF
10	F7	F7	F6	F1	F4	F2	EE	EE	EF	E7	E7	E7	E1	E4	E6	DF
20	DE	DF	D7	DA	DD	EF	CE	CE	D5	D5	D5	D5	D3	D0	D9	D1
30	A1	CC	CC	CC	C4	C8	CC	68	65	6C	6C	6F	C0	D1	C6	84
40	C0	BF	BD	BD	BB	B8	B8	B6	B5	B5	B3	AE	AA	B1	B6	AB
50	AC	AD	AB	A9	A5	A6	A6	A6	A7	A5	9E	AB	A8	70	AC	9C
60	9F	99	99	99	94	9A	A0	8B	95	9C	93	92	8E	8C	8D	8A
70	86	8C	96	98	8B	66	90	87	82	83	83	83	7A	84	8A	CB
80	5E	5E	FB	48	48	82	7C	73	7C	7A	7C	85	7A	5E	73	7C
90	82	99	66	66	74	75	72	61	80	66	6A	73	80	7B	72	4D
A0	7D	6E	52	6B	6A	6E	77	63	5F	F8	2A	2A	74	68	45	66
B0	66	66	5C	66	74	FC	20	20	55	62	6B	6B	5F	3F	E9	22
C0	22	82	4D	4F	55	5D	66	61	56	61	51	5C	6C	55	58	5A
D0	57	55	53	4B	55	62	63	4A	4A	55	51	48	D8	17	17	4A
E0	52	58	F2	09	09	30	50	86	FF	00	00	43	4B	56	48	4A
F0	48	7B	33	36	E1	04	05	44	45	42	37	45	52	42	41	39
1...	26	43	78	47	3A	2C	34	3F	49	52	30	31	3A	3A	3C	AC
1...	09	09	3C	38	35	66	25	28	2F	3A	42	2F	3A	3C	33	33
1...	33	6B	18	19	29	31	41	2A	31	39	34	2F	2A	7A	0F	10
1...	29	2D	31	30	2B	28	21	2E	38	33	28	22	29	29	28	21

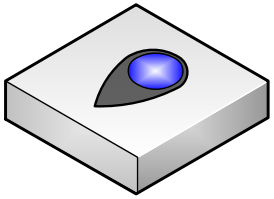
Char viewer

G	I	F	8	9	a	d	.	U.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	h	e	l	l	o	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	p	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	f	.	.	.	.	.	.	z	.	.	.
^	^	.	H	H	.	.	s	.	z	.	.	z	^	s	.
.	.	f	f	t	u	r	a	.	f	j	s	.	.	r	M.
.	n	R	k	j	n	w	c	_	.	*	*	t	h	E	f
f	f	\	f	t	.			U.	b	k	k	_	?	.	"
"	.	M.	O	U	]	f	a	V	a	Q	\	I	U	X	Z
W	U	S	K	U	b	c	J	J	U	Q	H	.	.	.	J
R	X	.	.	.	0	P	.	.	.	.	C	K	V	H	J
H	.	3	6	.	.	.	D	E	B	7	E	R	B	A	9
&	C	x	G	:	,	4	?	I	R	0	1	:	:	<	.
.	.	<	8	5	f	%	(	/	:	B	/	:	<	3	3
3	k	.	.	)	1	A	*	1	9	4	/	*	z	.	.
)	-	1	0	+	(	!	.	8	3	(	"	)	)	(	!

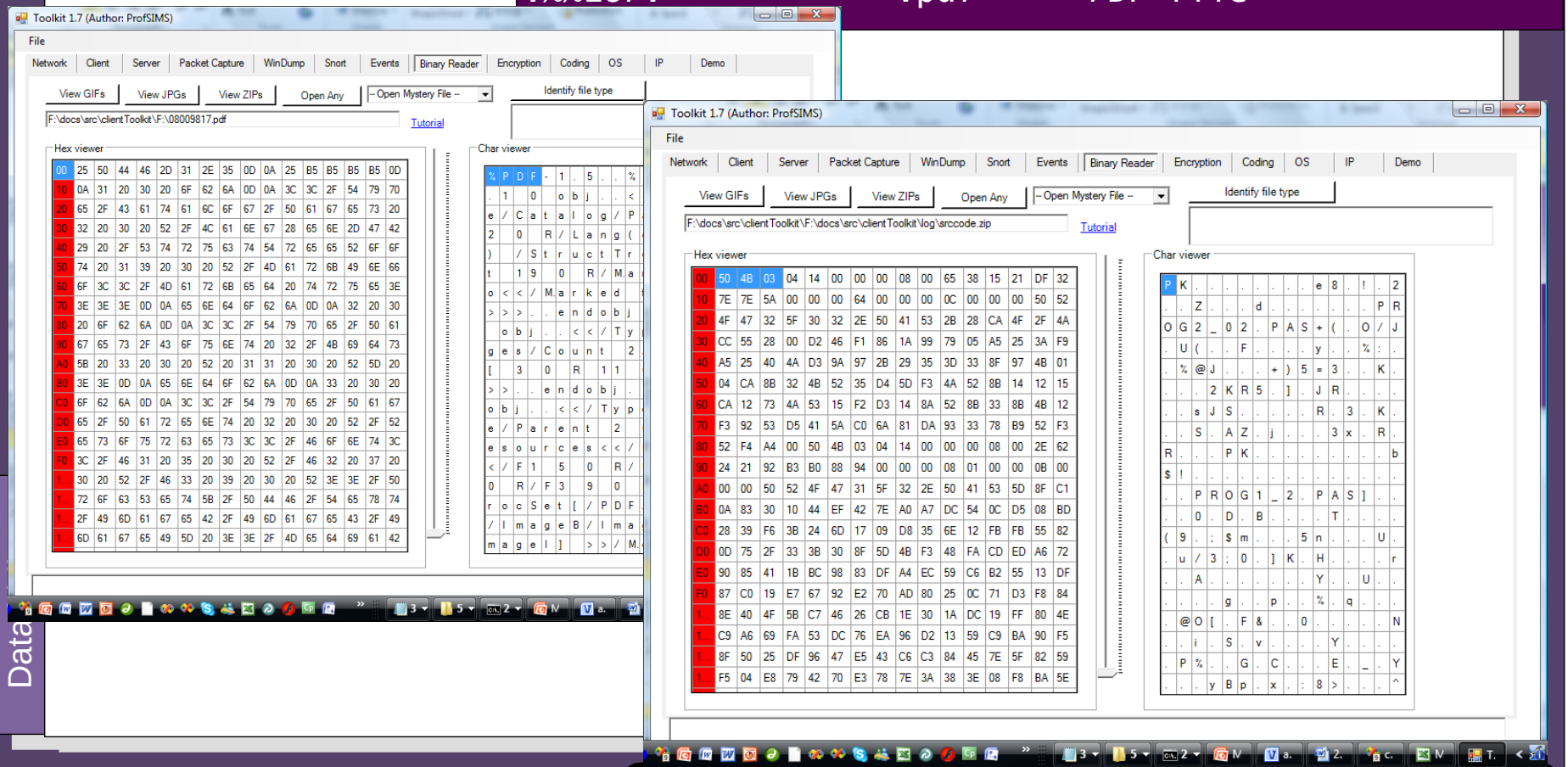
Obfuscation

Forensic

File Analysis

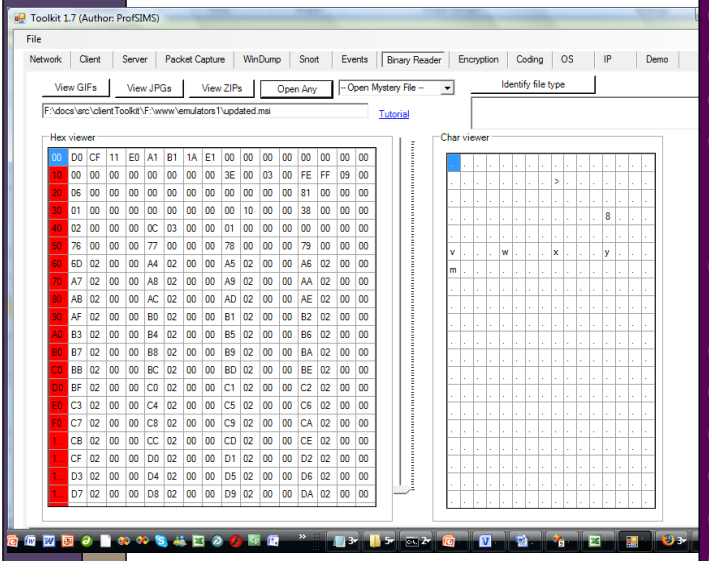


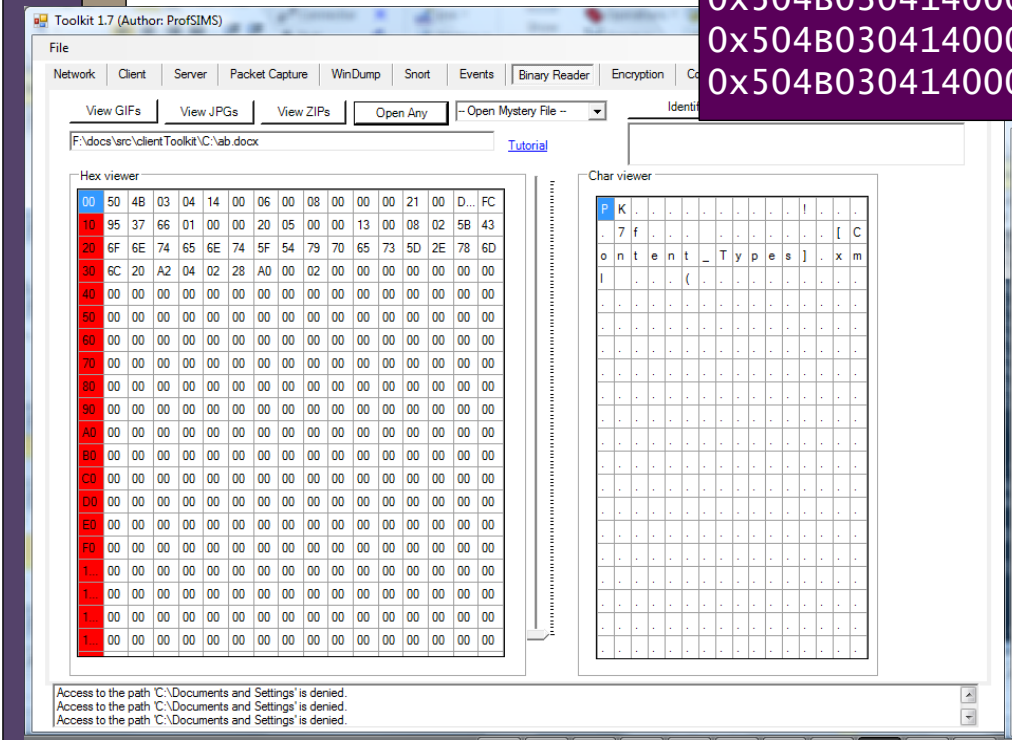
Sig	File ext	File type
0x474946	*.gif	GIF files
GIF89a	*.gif	GIF files
0xFFD8FF	*.jpg	JPEG files
JFIF	*.jpg	JPEG files
0x504B03	*.zip	ZIP files
0x25504446	*.pdf	PDF files
%PDF	*.pdf	PDF files
0x0A2525454F460A	*.pdf	PDF file
.%%EOF.	*.pdf	PDF file

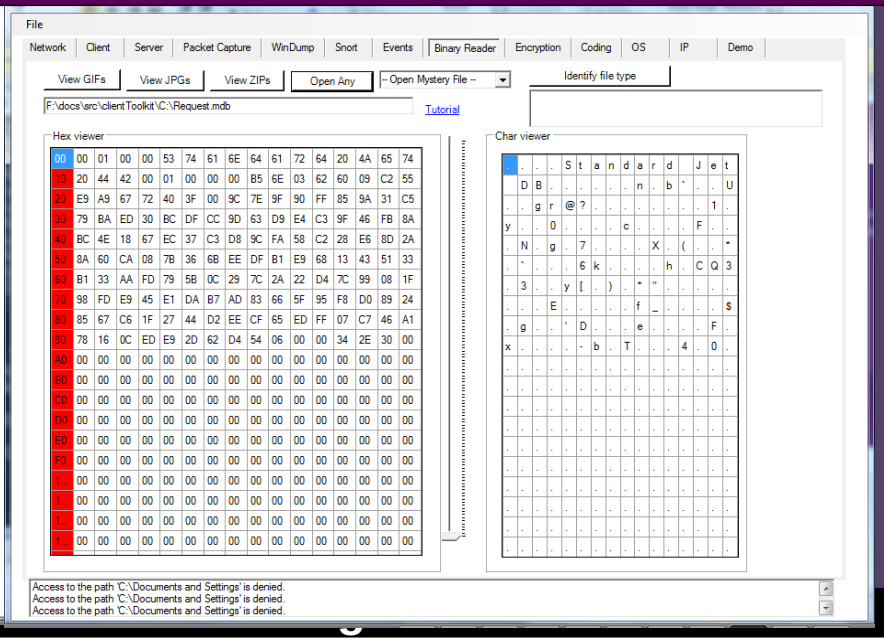


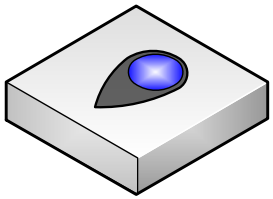
File signature

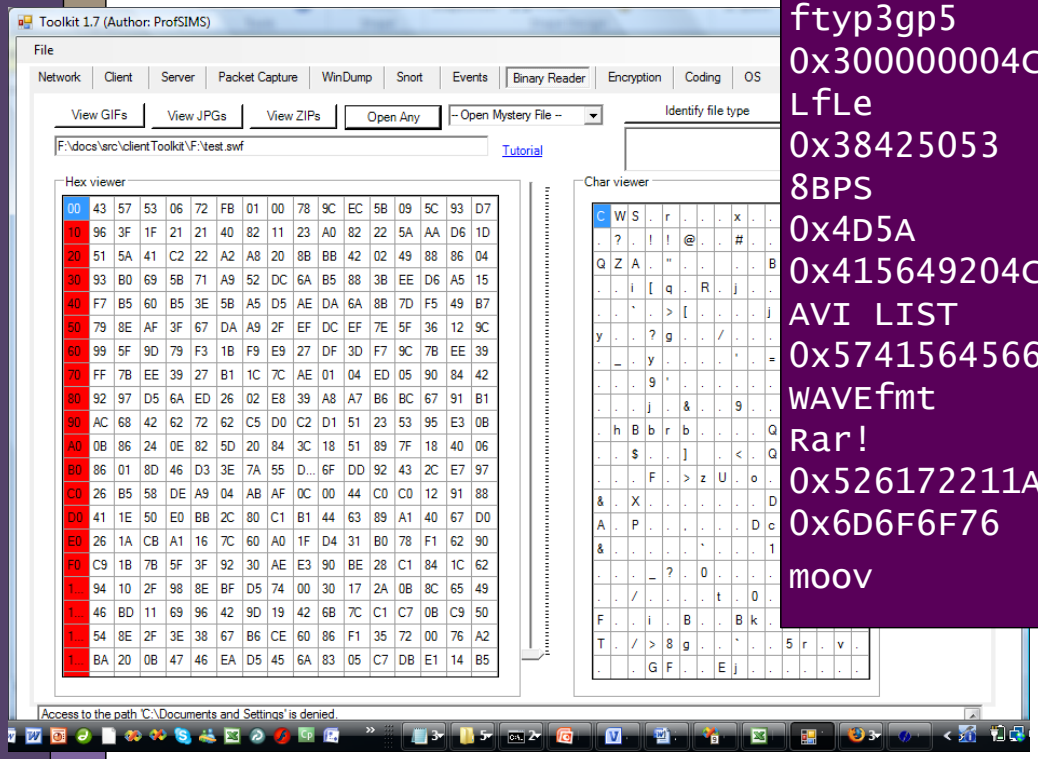
Sig	File ext	File type
0x006E1EF0	*.ppt	PPT
0xA0461DF0	*.ppt	PPT
0xECA5C100	*.doc	Doc file
0x00010000 5374616E 64617264 204A6574 204442		
	*.mdb	Microsoft database
Standard Jet DB	*.mdb	Microsoft database
0x2142444E	*.pst	PST file
!BDN	*.pst	PST file
0x0908100000060500	*.xls	XLS file
0xD0CF11E0A1B11AE1	*.msi	MSI file
0xD0CF11E0A1B11AE1	*.doc	DOC
0xD0CF11E0A1B11AE1	*.xls	Excel
0xD0CF11E0A1B11AE1	*.vsd	Visio
0xD0CF11E0A1B11AE1	*.ppt	PPT
0x504B030414000600	*.docx	Microsoft DOCX file
0x504B030414000600	*.pptx	Microsoft PPTX file
0x504B030414000600	*.xlsx	Microsoft XLSX file











Sig	File ext	File type
0x465753	*.swf	SWF file
FWS	*.swf	SWF file
0x494433	*.mp3	MP3 file
ID3	*.mp3	MP3 file
0x4C00000001140200	*.lnk	Link file
0x4C01	*.obj	OBJ file
0x4D4D002A	*.tif	TIF graphics
MM	*.tif	TIF graphics
0x0000001866747970336770 35	*.mp4	MP4 Video
ftyp3gp5	*.mp4	MP4 Video
0x300000004C664C65	*.evt	Event file
LfLe	*.evt	Event file
0x38425053	*.psd	Photoshop file
8BPS	*.psd	Photoshop file
0x4D5A	*.ocx	Active X
0x415649204C495354	*.avi	AVI file
AVI LIST	*.avi	AVI file
0x57415645666D7420	*.wav	WAV file
WAVEfmt	*.wav	WAV file
Rar!	*.rar	RAR file
0x526172211A0700	*.rar	RAR file
0x6D6F6F76	*.mov	MOV file
moov	*.mov	MOV file

Author: Prof Bill Buchanan

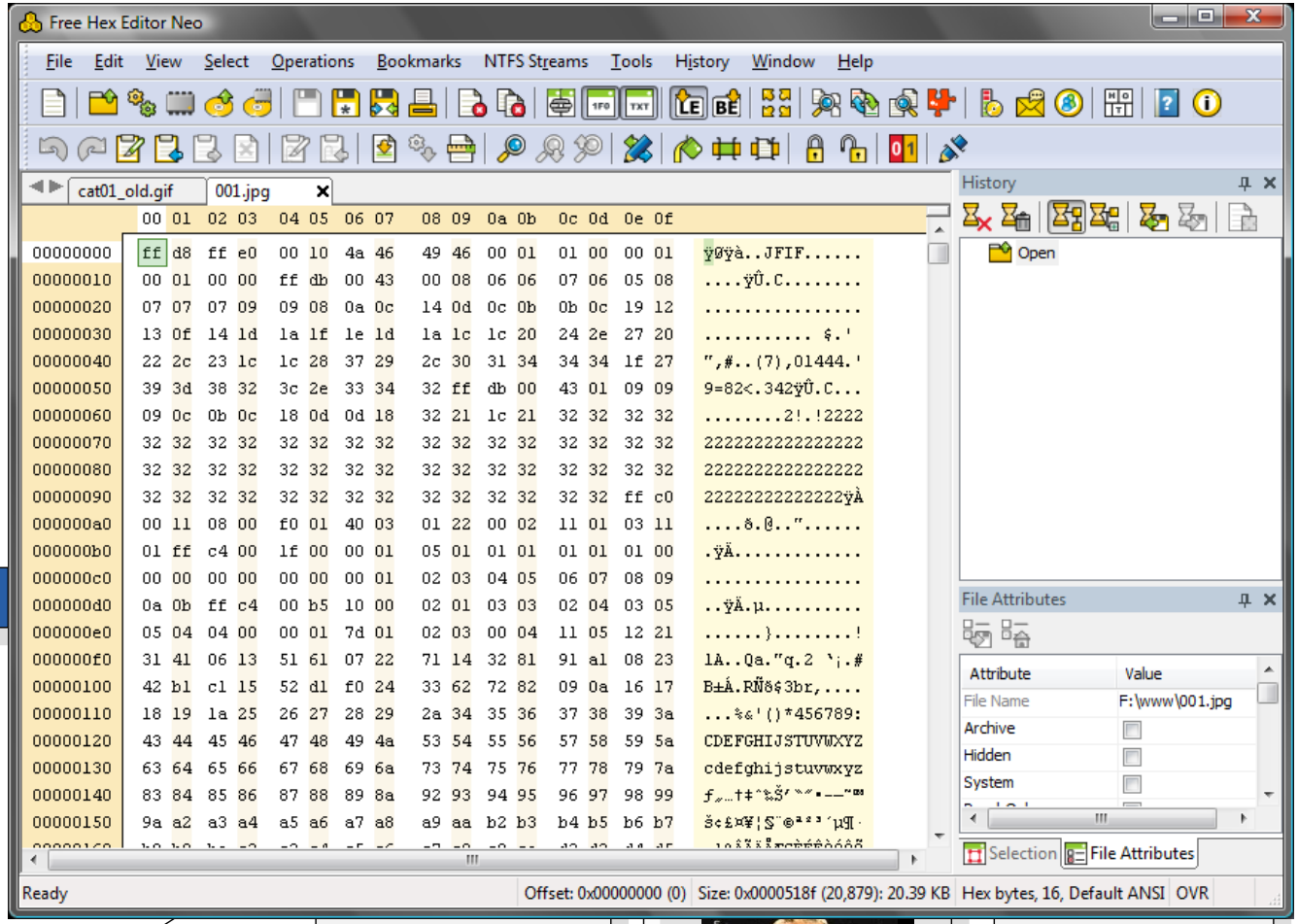
File signature

Myphoto.jpg

↓

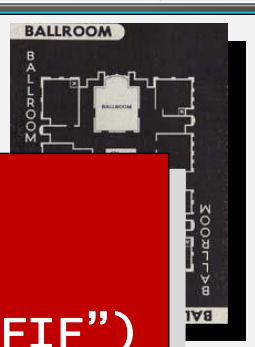
Myphoto.dll

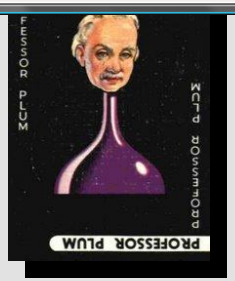
Obfuscation

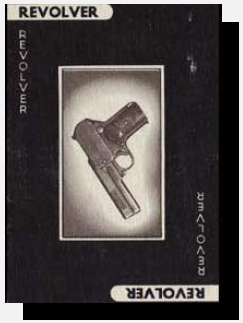


….JFIF...

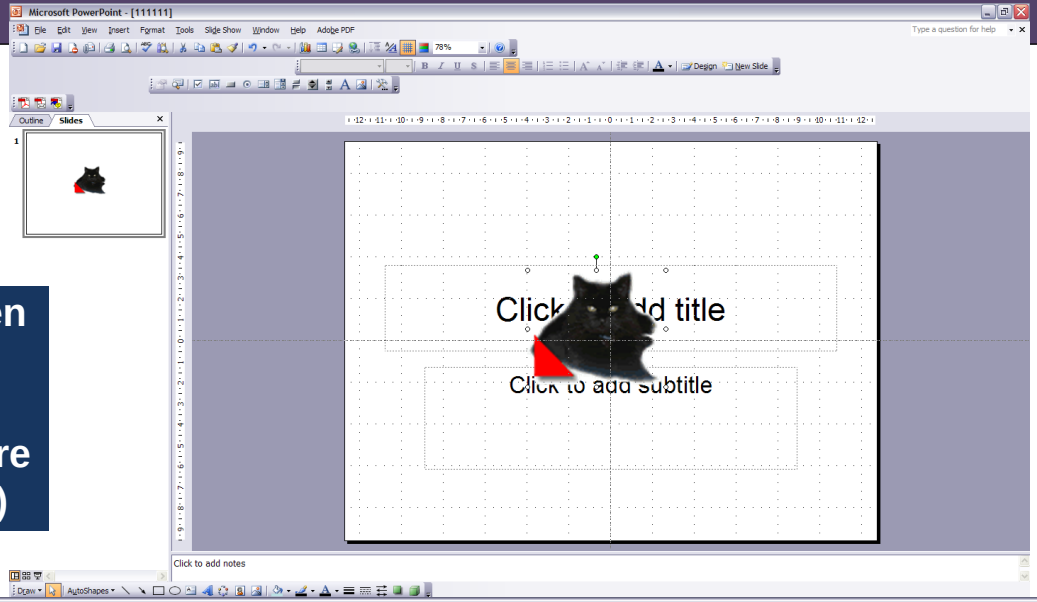
```
Header:   FFD8
Length:   <2 bytes>
Next:     4A,46,49,46,00 ("JFIF")
```





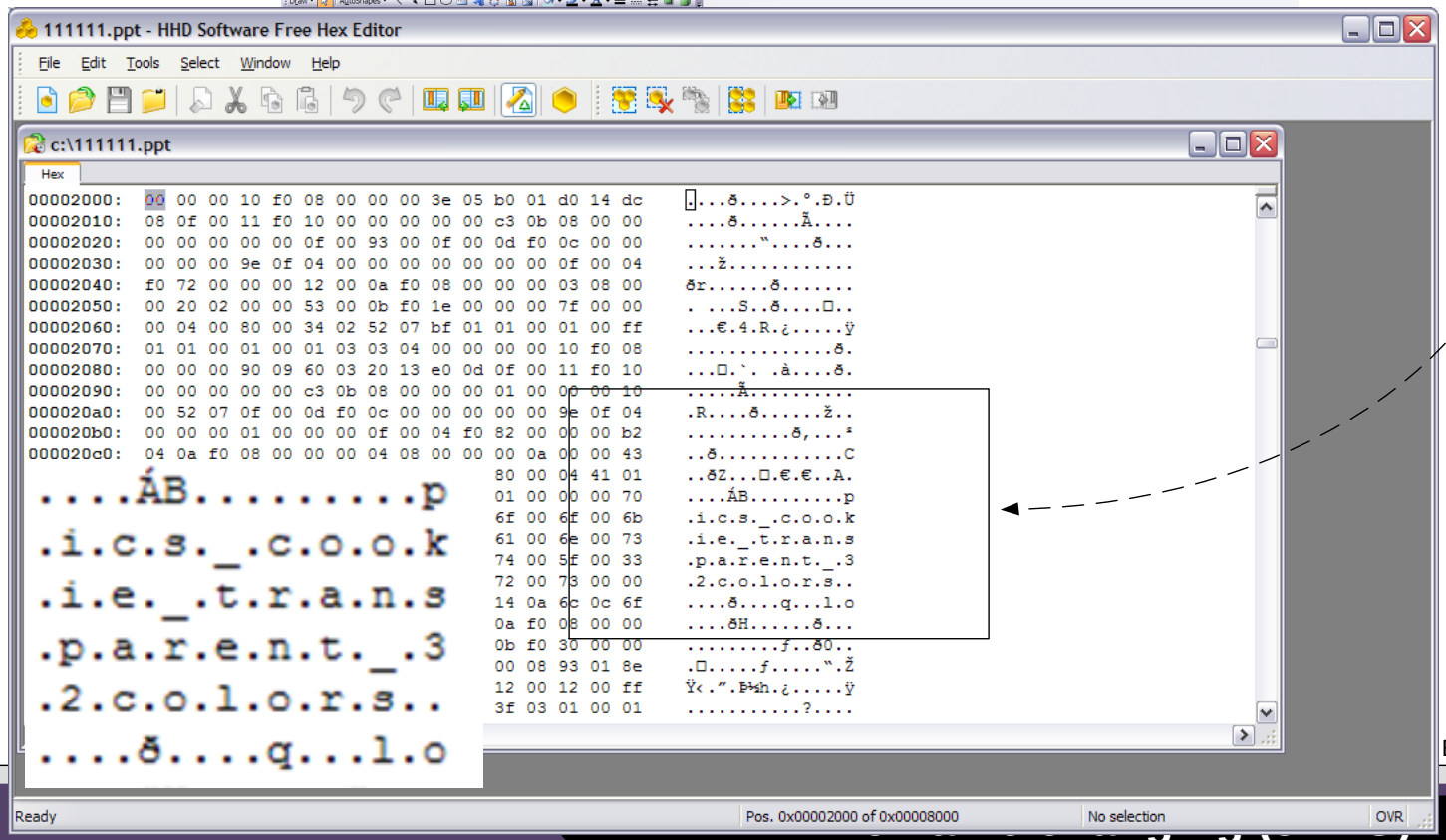


File name changing (JPEG)



Graphic has been imported into PowerPoint (cookie_transparent_32colors.gif)

Meta-data Is still stored in file (but 16-bit character format)



Obfuscation

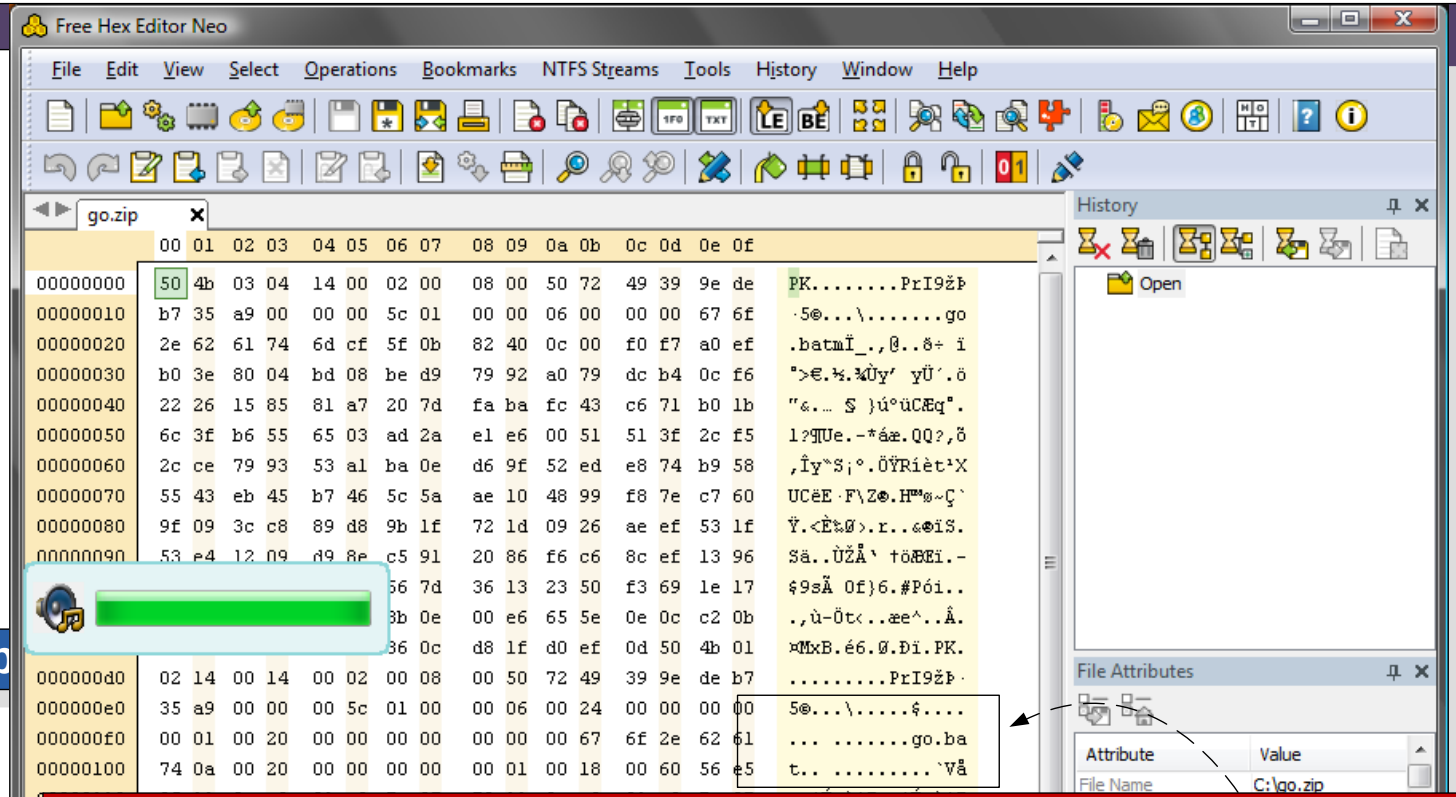
Forensic

Myzip.zip

Myzip.doc

Obfuscation

Forensic




```
00    ZIPLOCSIG   HEX   04034B50    ;Local File Header Signature
04    ZIPVER      DW    0000       ;Version needed to extract
06    ZIPGENFLG   DW    0000       ;General purpose bit flag
08    ZIPMTHD     DW    0000       ;Compression method
0A    ZIPTIME     DW    0000       ;Last mod file time (MS-DOS)
0C    ZIPDATE     DW    0000       ;Last mod file date (MS-DOS)
0E    ZIPCRC      HEX   00000000   ;CRC-32
12    ZIPSIZE     HEX   00000000   ;Compressed size
16    ZIPUNCMP    HEX   00000000   ;Uncompressed size
1A    ZIPFNLN     DW    0000       ;Filename length
1C    ZIPXTRALN   DW    0000       ;Extra field length
1E    ZIPNAME     DS    ZIPFNLN    ;filename
```

File name changing (ZIP)

```
c:\SMALL_~1>scalpel.exe "nps-2010-emails (1).raw" -o out5
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Multi-core CPU threading model enabled.
Initializing thread group data structures.
Creating threads...
Thread creation completed.

Opening target "c:\SMALL_~1\nps-2010-emails (1).raw"

Image file pass 1/2.
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building work queues...
Work queues built.  Workload:
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 19 files
Carving files from image.
Image file pass 2/2.
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 19, elapsed  = 1 secs.
```

Maximum carve size

	case	size	header	footer
jpg	y	5000:100000	\xff\xd8\xff\xe0\x00\x10	\xff\xd9
avi	y	50000000	RIFF????AVI	
mov	y	10000000	????moov	
fws	y	4000000	FWS	
mp3	y	8000000	\xFF\xFB??\x44\x00\x00	

Author: Prof Bill Buchanan

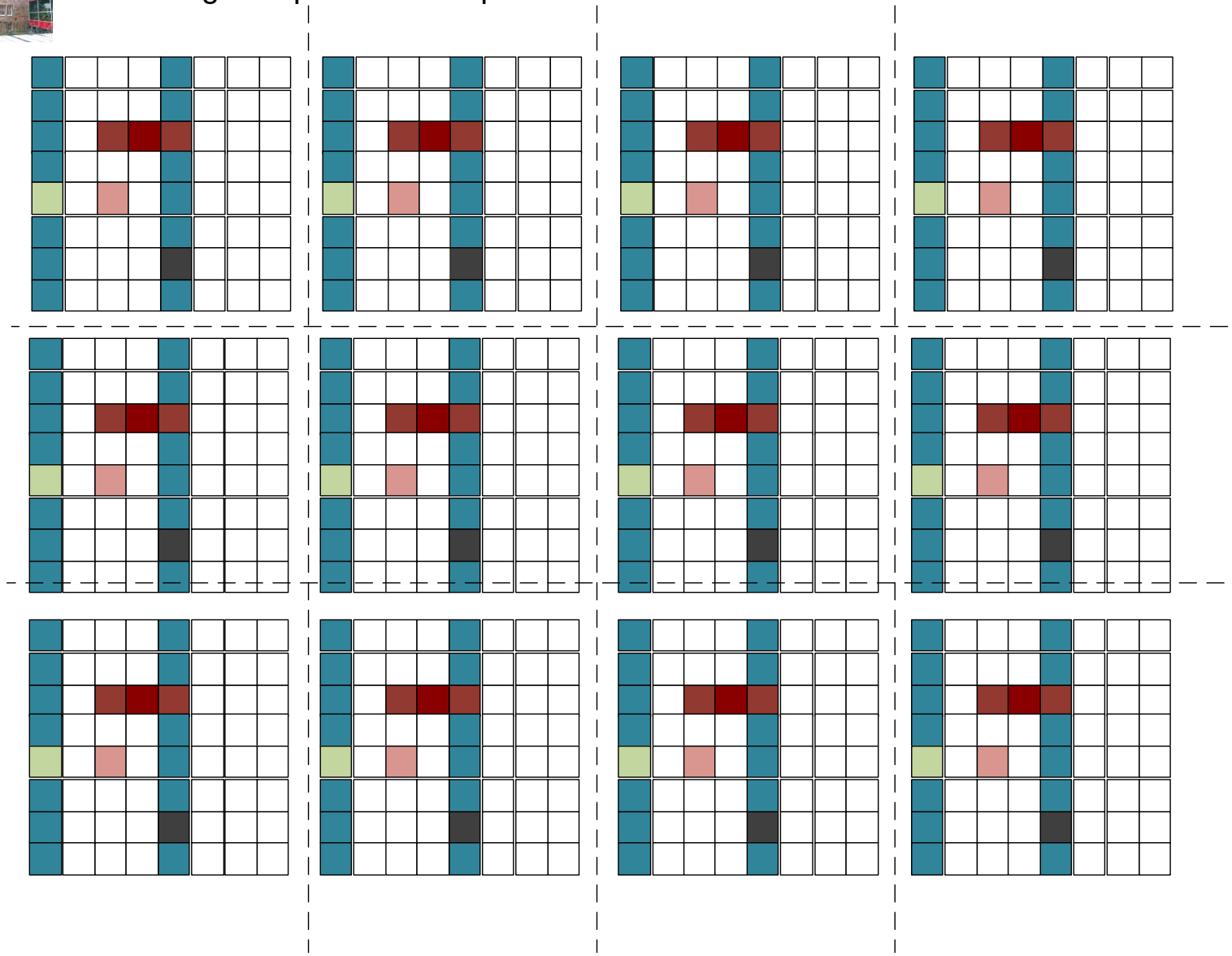
Using scalpel

Data Loss Detection/ Prevention

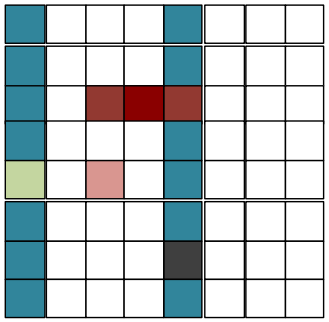
Discriminators

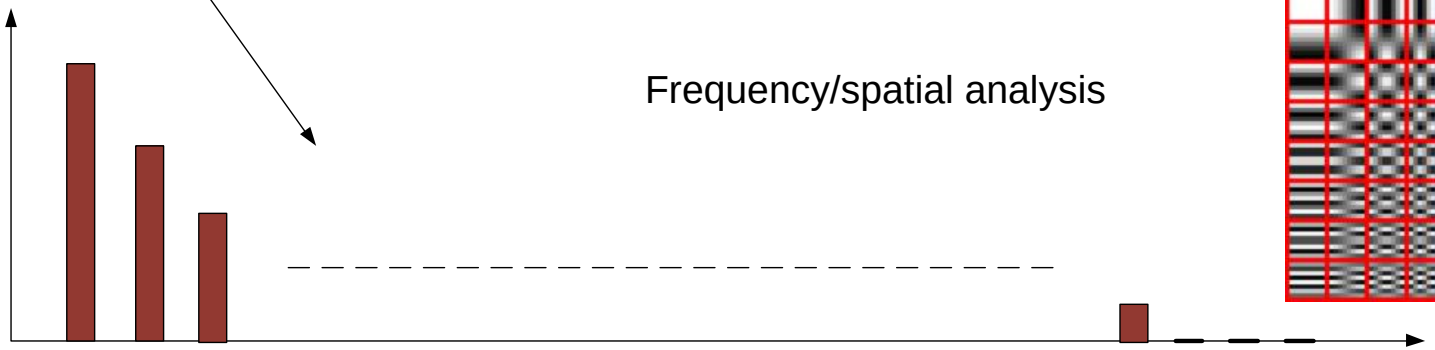
Author: Prof Bill Buchanan

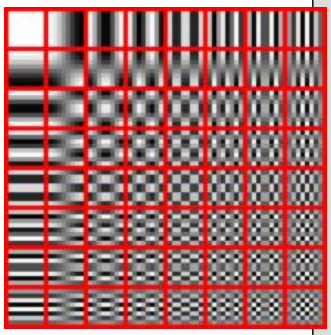
Image is split into 8 x 8 pixel blocks



Author: Prof Bill Buchanan







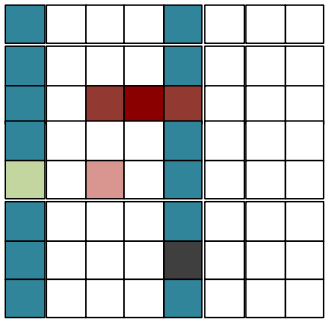
F(0,0)
Low frequency changes

F(7,7)
High frequency changes

Sample values

1257.9	2.3	-9.7	-4.1	3.9	0.6	-2.1	0.7
-21.0	-15.3	-4.3	-2.7	2.3	3.5	2.1	-3.1
-11.2	-7.6	-0.9	4.1	2.0	3.4	1.4	0.9
-4.9	-5.8	1.8	1.1	1.6	2.7	2.8	-0.7
0.1	-3.8	0.5	1.3	-1.4	0.7	1.0	0.9
0.9	-1.6	0.9	-0.3	-1.8	-0.3	1.4	0.8
-4.4	2.7	-4.4	-1.5	-0.1	1.1	0.4	1.9
-6.4	3.8	-5.0	-2.6	1.6	0.6	0.1	1.5

Author: Prof Bill Buchanan



After DCT

1257.9	2.3	-9.7	-4.1	3.9	0.6	-2.1	0.7
-21.0	-15.3	-4.3	-2.7	2.3	3.5	2.1	-3.1
-11.2	-7.6	-0.9	4.1	2.0	3.4	1.4	0.9
-4.9	-5.8	1.8	1.1	1.6	2.7	2.8	-0.7
0.1	-3.8	0.5	1.3	-1.4	0.7	1.0	0.9
0.9	-1.6	0.9	-0.3	-1.8	-0.3	1.4	0.8
-4.4	2.7	-4.4	-1.5	-0.1	1.1	0.4	1.9
-6.4	3.8	-5.0	-2.6	1.6	0.6	0.1	1.5

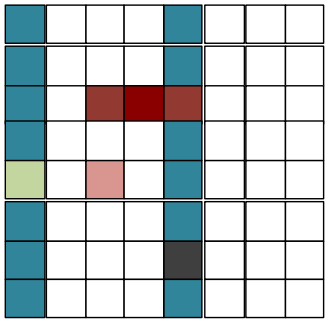
Divide by a certain value and find the nearest integer

5	3	4	4	4	3	5	4
4	4	5	5	5	6	7	12
8	7	7	7	7	15	11	11
9	12	13	15	18	18	17	15
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

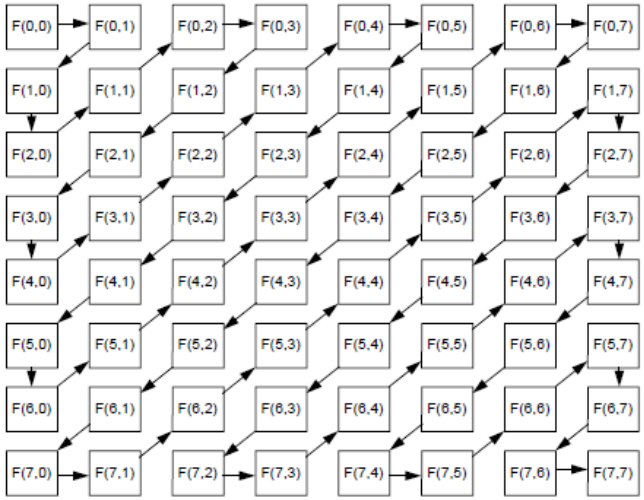
Result:

251	0	-2	-1	0	0	0	0
-5	-3	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Author: Prof Bill Buchanan



```
251  0  -2  -1  0  0  0  0
-5  -3  0  0  0  0  0  0
-1  -1  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
```



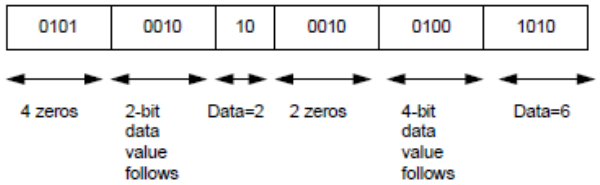
Order in Zig-zag

251, 0, -5, -1, -3, -2, 0, -1, 0, 0, 0, 0, -1, 0, 0, 0, 0,…,0

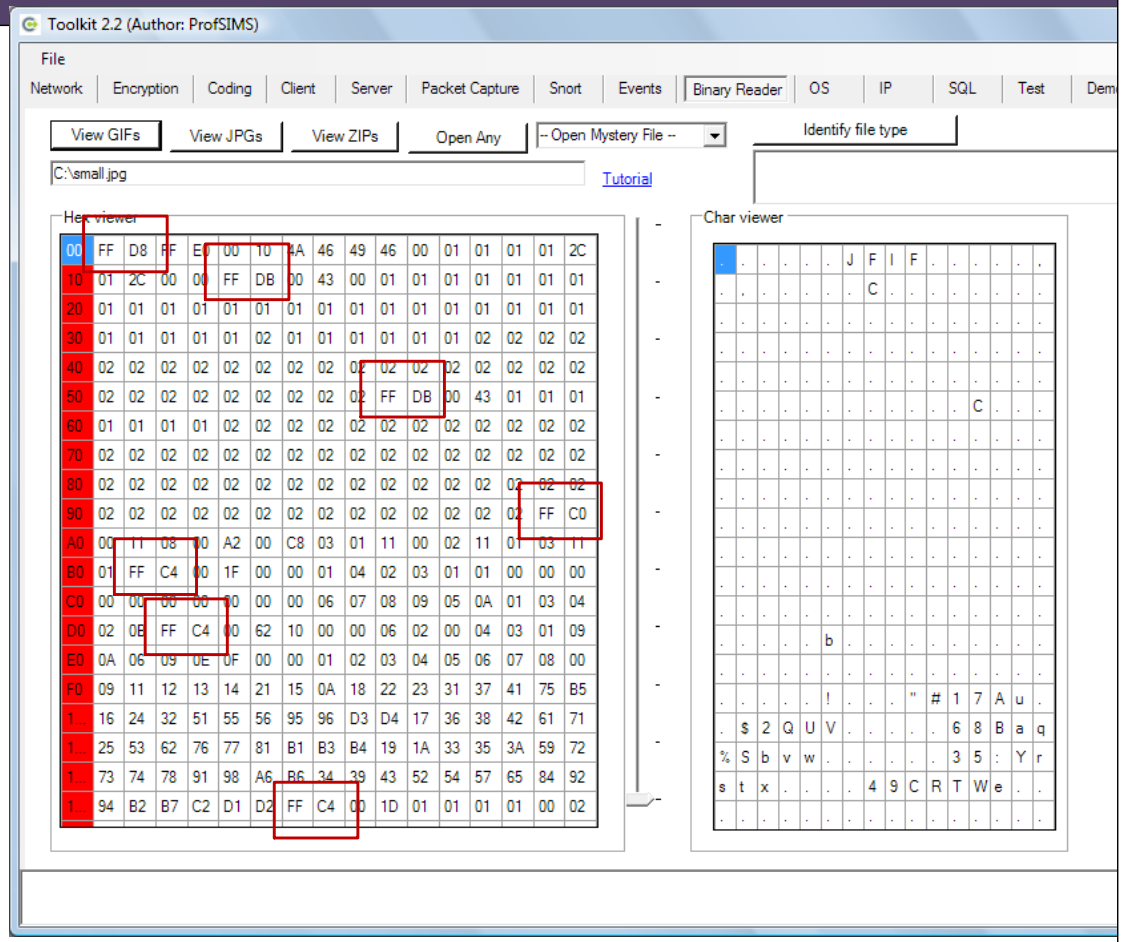
The binary value of 0000 0000 (00h) can never occur in the AC coding scheme. This code is used as a special code to identify that all of the values until the end of a block are zero. This is a common occurrence and thus saves coding bits.

Use Modified Huffman Code:

Data: 0, 0, 0, 0, 2, 0, 0, 6



Author: Prof Bill Buchanan



Found FFD8 tag (Start of image). Pos: 0
Found FFE0 tag (JPEG file identifier). Pos: 2
Length: 16
Found FFDB tag (Quantization Table). Pos: 20, Block 0
Found FFDB tag (Quantization Table). Pos: 89, Block 0
Found FFC0 tag (Start Of Frame (Baseline DCT)). Pos: 158, Block 0
Found FFC4 tag (Huffman Table). Pos: 177, Block 0
Found FFC4 tag (Huffman Table). Pos: 210, Block 0
Found FFC4 tag (Huffman Table). Pos: 310, Block 0
Found FFC4 tag (Huffman Table). Pos: 341, Block 0
Found FFDA tag (Start Of Scan). Pos: 412, Block 0
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 1209, Block 2
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3720, Block 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3977, Block 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 4304, Block 8
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5489, Block 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5507, Block 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5970, Block 11
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7115, Block 13
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7620, Block 14
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7892, Block 15
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8309, Block 16
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8938, Block 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 9082, Block 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10014, Block 19
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10626, Block 20
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10926, Block 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11033, Block 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11310, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11556, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11738, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11748, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11751, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11761, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11765, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12162, Block 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12236, Block 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12507, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12736, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12759, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13706, Block 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13776, Block 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13835, Block 27
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14427, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14441, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14447, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14476, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14572, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14740, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15372, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15447, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15501, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15893, Block 31
...
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 18943, Block 36
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19224, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19293, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19430, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19459, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19595, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19632, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19906, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19943, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20153, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20182, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20446, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20448, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20495, Block 40
Found FFD9 tag (End of image). Pos: 21684, Block 42

Discriminator

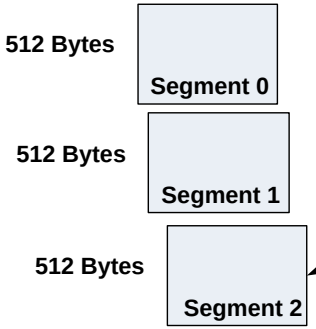
Authentication

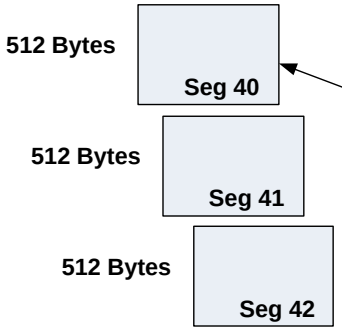
FFC0 tag (Start Of Frame (Baseline DCT)).
FFC2 tag (Start Of Frame (Progressive DCT)).
FFC4 tag (Huffman Table).
FFDB tag (Quantization Table).
FFC2 tag (Define Restart Interval).
FFDA tag (Start Of Scan).
FFDE tag (Comment).
FF00 stuffed FF (Likely Huffman Coding).

2011 UK IT INDUSTRY AWARDS
bcs The Chartered Institute for IT computing
FINALIST

Small.jpg

Detecting a JPEG file





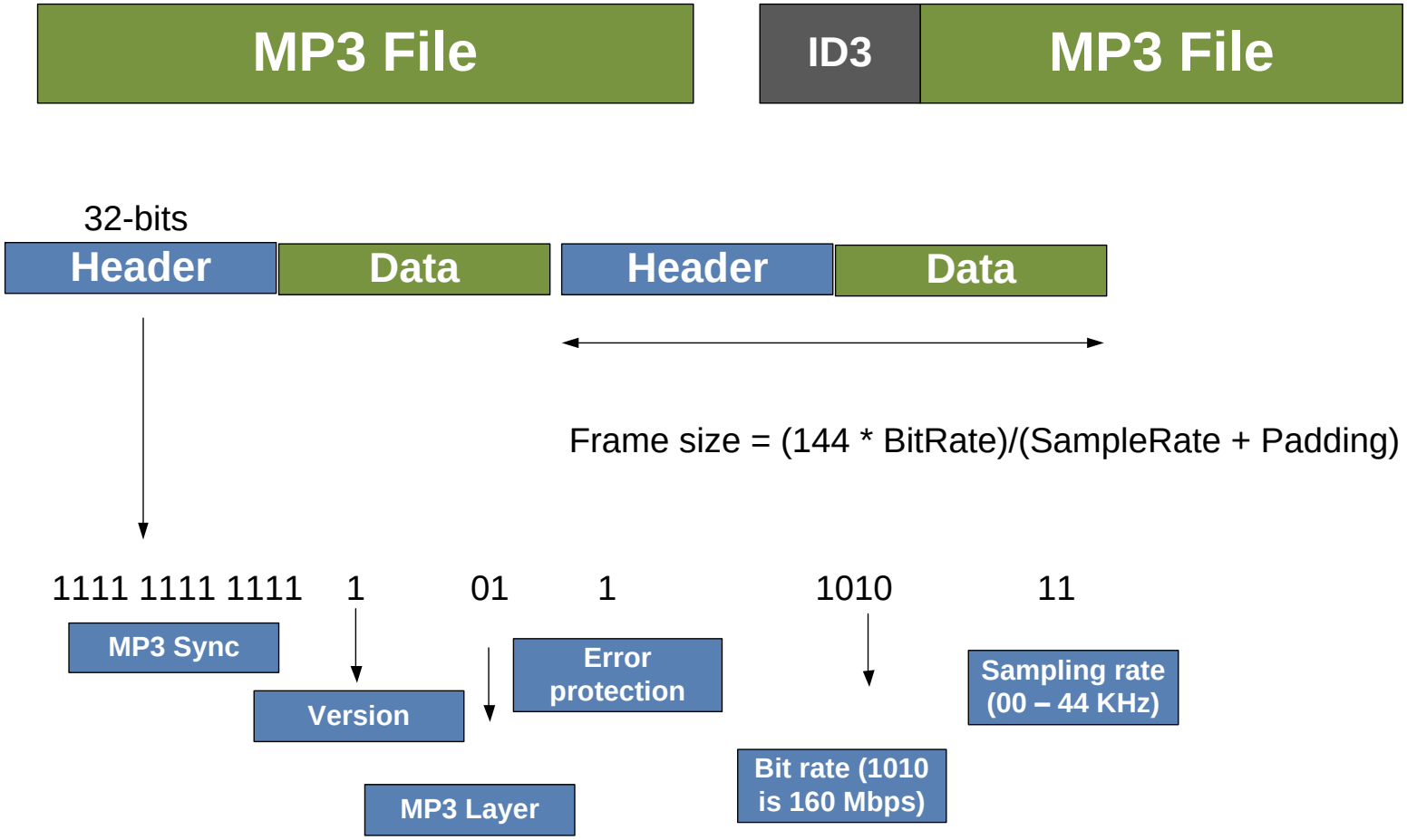
Segment No	Detected
1	Not detected
2	1 Found
3	Not detected
4	Not detected
5	Not detected
6	Not detected

7 2 Found
8 1 Found
9 Not detect
10 2 Found
11 1 Found
12 Not detected
13 1 Found
14 1 Found
15 1 Found
16 1 Found
17 2 Found
18 Not detected
19 1 Found
20 1 Found
21 2 Found
22 7 Found
23 2 Found
24 3 Found
25 Not detected
26 2 Found
27 1 Found
28 6 Found
29 Not detected
30 3 Found
31 6 Found

Result: 29 out of 40 (0 and 41 also detected)
With 2048 byte blocks: Nearly 100%

```
Found FFD8 tag (Start of image). Pos: 0
Found FFE0 tag (JPEG file identifier). Pos: 2
  Length: 16
Found FFDB tag (Quantization Table). Pos: 20, Segment 0
Found FFDB tag (Quantization Table). Pos: 89, Segment 0
Found FFC0 tag (Start Of Frame (Baseline DCT)). Pos: 158, Segment 0
Found FFC4 tag (Huffman Table). Pos: 177, Segment 0
Found FFC4 tag (Huffman Table). Pos: 210, Segment 0
Found FFC4 tag (Huffman Table). Pos: 310, Segment 0
Found FFC4 tag (Huffman Table). Pos: 341, Segment 0
Found FFDA tag (Start Of Scan). Pos: 412, Segment 0
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 1209, Segment 2
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3720, Segment 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3977, Segment 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 4304, Segment 8
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5489, Segment 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5507, Segment 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5970, Segment 11
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7115, Segment 13
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7620, Segment 14
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7892, Segment 15
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8309, Segment 16
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8938, Segment 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 9082, Segment 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10014, Segment 19
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10626, Segment 20
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10926, Segment 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11033, Segment 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11310, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11556, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11738, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11748, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11751, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11761, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11765, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12162, Segment 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12236, Segment 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12507, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12736, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12759, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13706, Segment 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13776, Segment 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13835, Segment 27
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14427, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14441, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14447, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14476, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14572, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14740, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15372, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15447, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15501, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15893, Segment 31
...
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 18943, Segment 36
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19224, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19293, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19430, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19459, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19595, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19632, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19906, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19943, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20153, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20182, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20446, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20448, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20495, Segment 40
Found FFD9 tag (End of image). Pos: 21684, Segment 42
```


Detecting an MP3 file



Discriminator

Authentication

Author: Prof Bill Buchanan

Track258.mp3

512 Bytes **Segment 0**

512 Bytes **Segment 1**

512 Bytes **Segment 2**

Segment No	Detected
0	Found
2	Found
...	
20	Found

Found in all segments

512 Bytes **Seg 18**

512 Bytes **Seg 19**

512 Bytes **Seg 20**

```
MP3 Analysis ... looking for 11 or 12-bit sequences for 1's for the frames in 512 byte sectors
MP3: Found 12-bit sequence. Pos: 63, Segment: 0 out of 21 segments
MP3: Found 11-bit sequence. Pos: 234, Segment: 0 out of 21 segments
MP3: Found 11-bit sequence. Pos: 704, Segment: 1 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1152, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1228, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1239, Segment: 2 out of 21 segments
MP3: Found 11-bit sequence. Pos: 1488, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1755, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1802, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1862, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1928, Segment: 3 out of 21 segments
MP3: Found 11-bit sequence. Pos: 2015, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2145, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2146, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2489, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2622, Segment: 5 out of 21 segments
MP3: Found 11-bit sequence. Pos: 2765, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2866, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2977, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3005, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3011, Segment: 5 out of 21 segments
MP3: Found 11-bit sequence. Pos: 3080, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3081, Segment: 6 out of 21 segments
MP3: Found 11-bit sequence. Pos: 3086, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3087, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3134, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3212, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3231, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3499, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3500, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3704, Segment: 7 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3761, Segment: 7 out of 21 segments
MP3: Found 11-bit sequence. Pos: 4044, Segment: 7 out of 21 segments
MP3: Found 12-bit sequence. Pos: 4231, Segment: 8 out of 21 segments
...
MP3: Found 12-bit sequence. Pos: 7312, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 7366, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 7495, Segment: 14 out of 21 segments
MP3: Found 11-bit sequence. Pos: 7666, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8031, Segment: 15 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8164, Segment: 15 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8195, Segment: 16 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8427, Segment: 16 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8497, Segment: 16 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8634, Segment: 16 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8716, Segment: 17 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8907, Segment: 17 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8973, Segment: 17 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9279, Segment: 18 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9474, Segment: 18 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9761, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9776, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9777, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9778, Segment: 19 out of 21 segments
MP3: Found 11-bit sequence. Pos: 9795, Segment: 19 out of 21 segments
MP3: Found 11-bit sequence. Pos: 9952, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10264, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10265, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10407, Segment: 20 out of 21 segments
MP3: Found 11-bit sequence. Pos: 10422, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10657, Segment: 20 out of 21 segments
```

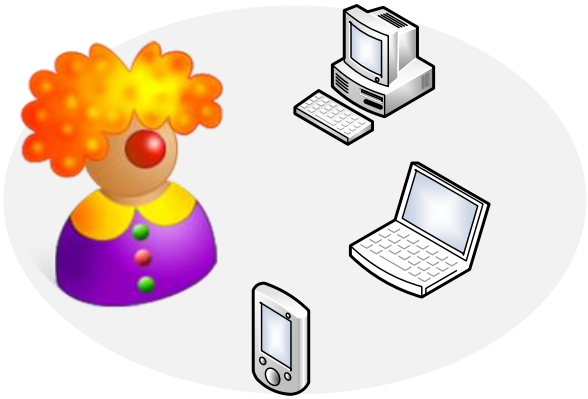
Author: Prof Bill Buchanan

Detecting an MP3 file

Data Loss Detection/ Prevention

Disk Partitions

Author: Prof Bill Buchanan



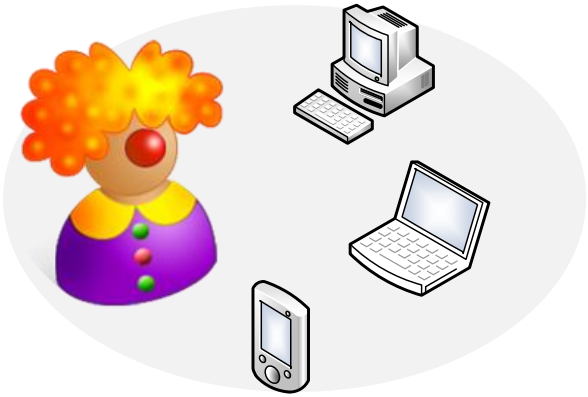
Executable Code:
0 [00h] - 138 [8Ah]. The first 139 bytes is executable code

```
7C00 FA     CLI        ; Disable maskable Interrupts
7C01 33C0   XOR   AX,AX ; Zero out both the Acc. an
7C03 8ED0   MOV   SS,AX ;  the Stack Segment regist
7C05 BC007C MOV   SP,7C00; Set Stack Pointer to
0000:7C00
7C08 8BF4   MOV   SI,SP ; Source Index: Copy from
here...
7C0A 50     PUSH  AX
7C0B 07     POP   ES     ; Zero-out Extra Segment
7C0C 50     PUSH  AX
7C0D 1F     POP   DS     ; Zero-out  Data Segment
7C0E FB     STI        ; Enable Interrupts again
```

```
0000  FA 33 C0 8E D0 BC 00 7C 8B F4 50 07 50 1F FB FC  .3.....|..P.P...
0010  BF 00 06 B9 00 01 F2 A5 EA 1D 06 00 00 BE BE 07  ................
0020  B3 04 80 3C 80 74 0E 80 3C 00 75 1C 83 C6 10 FE  ...<.t..<.u.....
0030  CB 75 EF CD 18 8B 14 8B 4C 02 8B EE 83 C6 10 FE  .u......L.......
0040  CB 74 1A 80 3C 00 74 F4 BE 8B 06 AC 3C 00 74 0B  .t..<.t.....<.t.
0050  56 BB 07 00 B4 0E CD 10 5E EB F0 EB FE BF 05 00  V.......^.......
0060  BB 00 7C B8 01 02 57 CD 13 5F 73 0C 33 C0 CD 13  ..|...W._s.3...
0070  4F 75 ED BE A3 06 EB D3 BE C2 06 BF FE 7D 81 3D  Ou...........}.=
0080  55 AA 75 C7 8B F5 EA 00 7C 00 00 49 6E 76 61 6C  U.u.....|..Inval
0090  69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 62  id partition tab
00A0  6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E 67  le.Error loading
00B0  20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65   operating syste
00C0  6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61 74  m.Missing operat
00D0  69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00 00  ing system.....
00E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01  ................
01C0  14 00 04 03 60 DA 33 00 00 00 4D ED 00 00 00 00   ....`.3...M.....
01D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............U.
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
```

Ref: thestarman.pcministry.com/asm/mbr/STDMBR.htm#CHS

Author: Prof Bill Buchanan



Error Message

```
0000  FA 33 C0 8E D0 BC 00 7C 8B F4 50 07 50 1F FB FC  .3.....|..P.P...
0010  BF 00 06 B9 00 01 F2 A5 EA 1D 06 00 00 BE BE 07  ................
0020  B3 04 80 3C 80 74 0E 80 3C 00 75 1C 83 C6 10 FE  ...<.t..<.u.....
0030  CB 75 EF CD 18 8B 14 8B 4C 02 8B EE 83 C6 10 FE  .u......L.......
0040  CB 74 1A 80 3C 00 74 F4 BE 8B 06 AC 3C 00 74 0B  .t..<.t.....<.t.
0050  56 BB 07 00 B4 0E CD 10 5E EB F0 EB FE BF 05 00  V.......^.......
0060  BB 00 7C B8 01 02 57 CD 13 5F 73 0C 33 C0 CD 13  ..|...W.._s.3...
0070  4F 75 ED BE A3 06 EB D3 BE C2 06 BF FE 7D 81 3D  Ou..........}.=
0080  55 AA 75 C7 8B F5 EA 00 7C 00 00 49 6E 76 61 6C  U.u.....|..Inval
0090  69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 62  id partition tab
00A0  6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E 67  le.Error loading
00B0  20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65   operating syste
00C0  6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61 74  m.Missing operat
00D0  69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00 00  ing system.....
00E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01  ................
01C0  14 00 04 03 60 DA 33 00 00 00 4D ED 00 00 00 00   ....`.3...M.....
01D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............U.
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
```

Author: Prof Bill Buchanan

Partition Table:
446 [1BEh] - 511 [1FFh]. This is a 64 byte partition table followed by the magic number is stored at position 510 [1FEh] and 511 [1FFh] where the values at "55 AA".

```
From 01BE - 01CD - Partition 1 data table (16 bytes
From 01CE - 01DD - Partition 2 data table (16 bytes
From 01DE - 01ED - Partition 3 data table (16 bytes
From 01EE - 01ED - Partition 4 data table (16 bytes
```

00 boot indicator (80h bootable, 00h non-bootable) (byte)
01 beginning sector head number (byte)
02 beginning sector (2 high bits of cylinder #)
03 beginning cylinder# (low order bits of cylinder #)
04 system indicator (04h - DOS Fat16, 06h - DOS Fat32)
05 ending sector head number
06 ending sector (2 high bits of cylinder #)
07 ending cylinder# (low order bits of cylinder #)
08 number of sectors preceding the partition (dword)
0B number of sectors in the partition (dword)

00 Boot indicator (non-bootable)
01 Beginning sector head (01).
14 Being Sector (Cylinder).
00 Being Sector (Cylinder).
04 System Indicator (04 – FAT16)
03 End Sector.
60 End Sector
DA End Sector
33 00 00 00 Number of sectors proceeding partition.
4D ED 00 00 Number sectors in partition (60,749)

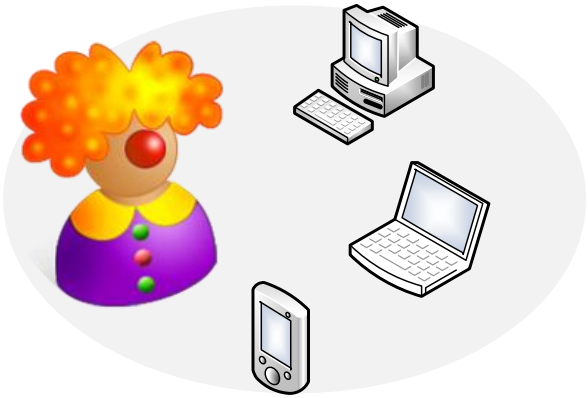
```
0000  FA 33 C0 8E D0 BC 00 7C 8B F4 50 07 50 1F FB FC  .3.....|..P.P...
0010  BF 00 06 B9 00 01 F2 A5 EA 1D 06 00 00 BE BE 07  ................
0020  B3 04 80 3C 80 74 0E 80 3C 00 75 1C 83 C6 10 FE  ...<.t..<.u.....
0030  CB 75 EF CD 18 8B 14 8B 4C 02 8B EE 83 C6 10 FE  .u......L.......
0040  CB 74 1A 80 3C 00 74 F4 BE 8B 06 AC 3C 00 74 0B  .t..<.t.....<.t.
0050  56 BB 07 00 B4 0E CD 10 5E EB F0 EB FE BF 05 00  V.......^.......
0060  BB 00 7C B8 01 02 57 CD 13 5F 73 0C 33 C0 CD 13  ..|...W._s.3...
0070  4F 75 ED BE A3 06 EB D3 BE C2 06 BF FE 7D 81 3D  Ou...........}.=
0080  55 AA 75 C7 8B F5 EA 00 7C 00 00 49 6E 76 61 6C  U.u.....|..Inval
0090  69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 62  id partition tab
00A0  6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E 67  le.Error loading
00B0  20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65   operating syste
00C0  6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61 74  m.Missing operat
00D0  69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00 00  ing system......
00E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01  ................
01C0  14 00 04 03 60 DA 33 00 00 00 4D ED 00 00 00 00   ....`.3...M.....
01D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............U.
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
```

Author: Prof Bill Buchanan

Data Loss Detection/ Prevention

Open Source Analysis

Author: Prof Bill Buchanan



```
01B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
01C0  14 00 04 03 60 DA 33 00 00 00 4D ED 00 00 00 00
```

00 Boot indicator (non-bootable)
01 Beginning sector head (01).
14 Being Sector (Cylinder).
00 Being Sector (Cylinder).
04 System Indicator (04 – FAT16)
03 End Sector.
60 End Sector
DA End Sector
33 00 00 00 Number of sectors proceeding partition (51).
4D ED 00 00 Number sectors in partition (60,749)

Mmls – View partition table

```
C:\> mmls -t dos nps-2009-canon2-gen1.raw
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000050   0000000051   Unallocated
02:  00:00   0000000051   0000060799   0000060749   DOS FAT16 (0x04)
```

Analysis

Adv Dig For.

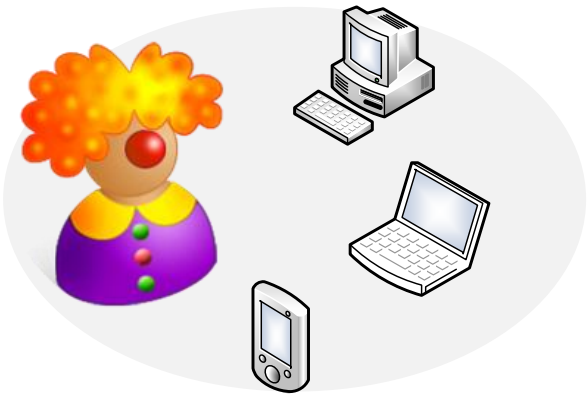
Author: Prof Bill Buchanan

```
     Slot     Start          End            Length         Description
00:  Meta     0000000000     0000000000     0000000001     Primary Table (#0)
01:  -----    0000000000     0000000050     0000000051     Unallocated
02:  00:00    0000000051     0000060799     0000060749     DOS FAT16 (0x04)
```

Ils – i-node information

i-Node contains information of file (and not the contents)

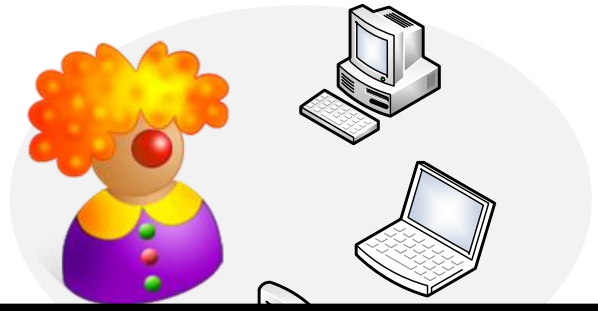
```
C:\>ils -o 51 -f fat16 -i raw nps-2009-canon2-gen1.raw
class|host|device|start_time
ils|unknown||1389703189
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mo
de|st_nlink|st_size
1029|f|0|0|1230041558|1229990400|0|1230041558|777|1|855935
1030|f|0|0|1230041566|1229990400|0|1230041566|777|1|871587
..
1061|f|0|0|1230041718|1229990400|0|1230041718|777|1|845375
1062|f|0|0|1230041722|1229990400|0|1230041722|777|1|812465
1063|f|0|0|1230041728|1229990400|0|1230041728|777|1|820105
1064|f|0|0|1230041736|1229990400|0|1230041736|777|1|882337
```



fls – lists files and folders (including deleting ones)

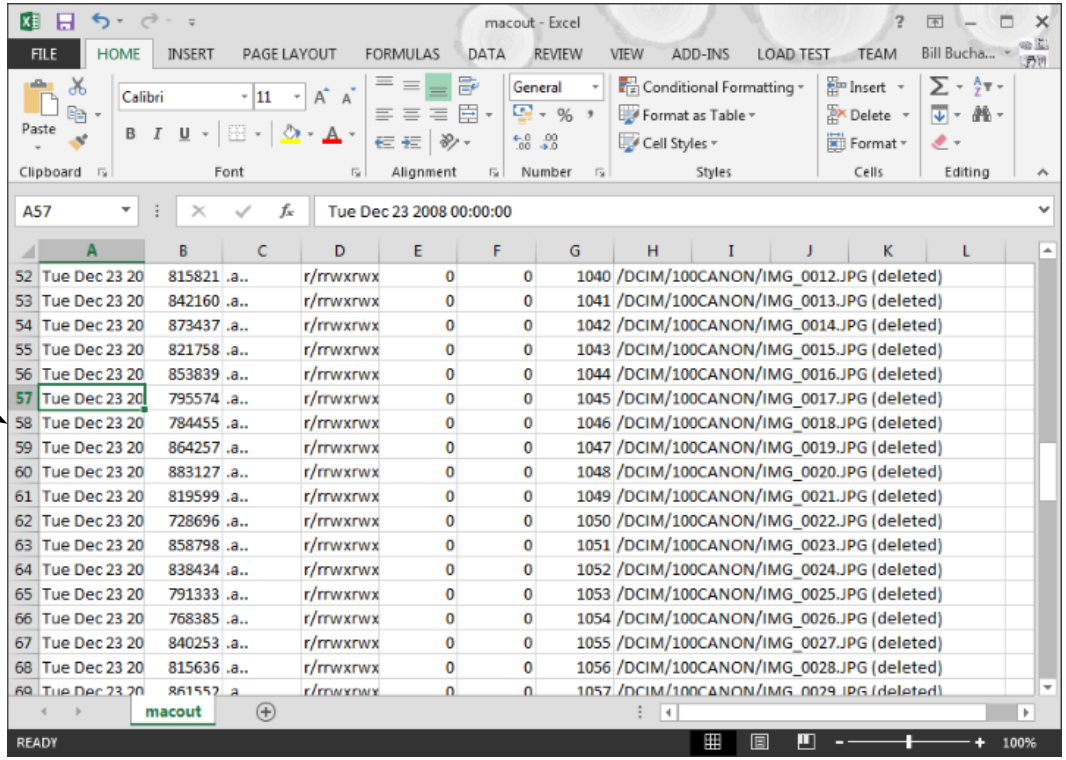
```
C:\>fls -o 51 -f fat16 -i raw -r nps-2009-canon2-gen1.raw
r/r 3:  CANON_DC    (Volume Label Entry)
d/d 4:  DCIM
+ d/d 517:      100CANON
++ r/r * 1029:  IMG_0001.JPG
++ r/r * 1030:  IMG_0002.JPG
++ r/r * 1031:  IMG_0003.JPG
++ r/r * 1032:  IMG_0004.JPG
..
++ r/r * 1063:  IMG_0035.JPG
++ r/r * 1064:  IMG_0036.JPG
v/v 971779:     $MBR
v/v 971780:     $FAT1
v/v 971781:     $FAT2
d/d 971782:     $OrphanFiles
```


Author: Prof Bill Buchanan



Bodyfile.txt – contains time line

```
C:\> fls -o 51 -f fat16 -i raw -m / -r nps-2009-canon2-gen1.raw >
bodyfile.txt
C:\> perl mactime.pl -b bodyfile.txt -d > macout.csv
```

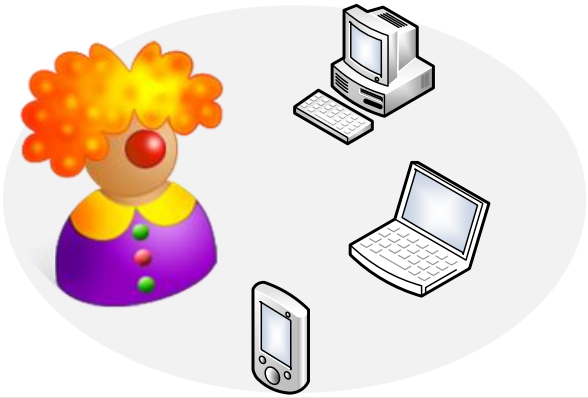


macout - Excel

A57 | Tue Dec 23 2008 00:00:00

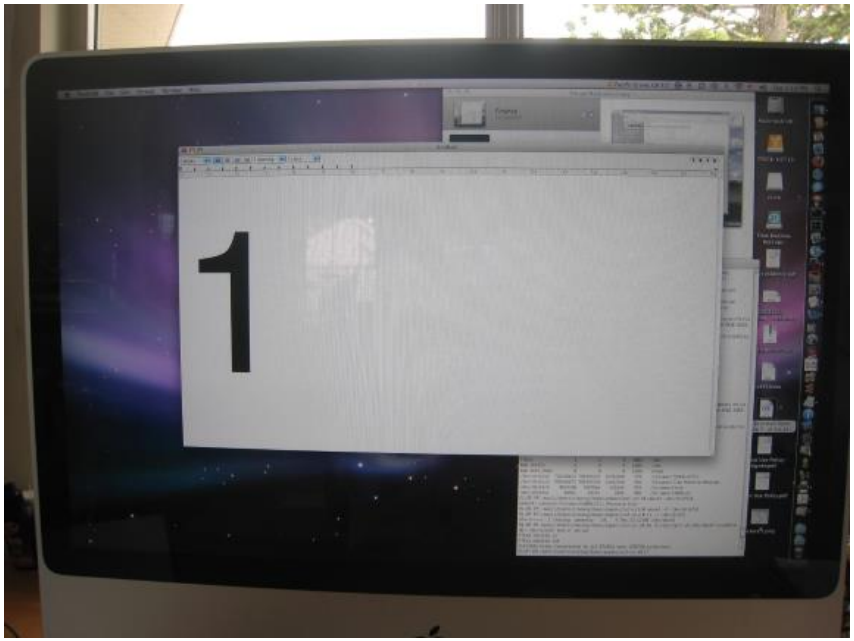
	A	B	C	D	E	F	G	H
52	Tue Dec 23 20	815821	.a..	r/rrwxrwx	0	0	1040	/DCIM/100CANON/IMG_0012.JPG (deleted)
53	Tue Dec 23 20	842160	.a..	r/rrwxrwx	0	0	1041	/DCIM/100CANON/IMG_0013.JPG (deleted)
54	Tue Dec 23 20	873437	.a..	r/rrwxrwx	0	0	1042	/DCIM/100CANON/IMG_0014.JPG (deleted)
55	Tue Dec 23 20	821758	.a..	r/rrwxrwx	0	0	1043	/DCIM/100CANON/IMG_0015.JPG (deleted)
56	Tue Dec 23 20	853839	.a..	r/rrwxrwx	0	0	1044	/DCIM/100CANON/IMG_0016.JPG (deleted)
57	Tue Dec 23 20	795574	.a..	r/rrwxrwx	0	0	1045	/DCIM/100CANON/IMG_0017.JPG (deleted)
58	Tue Dec 23 20	784455	.a..	r/rrwxrwx	0	0	1046	/DCIM/100CANON/IMG_0018.JPG (deleted)
59	Tue Dec 23 20	864257	.a..	r/rrwxrwx	0	0	1047	/DCIM/100CANON/IMG_0019.JPG (deleted)
60	Tue Dec 23 20	883127	.a..	r/rrwxrwx	0	0	1048	/DCIM/100CANON/IMG_0020.JPG (deleted)
61	Tue Dec 23 20	819599	.a..	r/rrwxrwx	0	0	1049	/DCIM/100CANON/IMG_0021.JPG (deleted)
62	Tue Dec 23 20	728696	.a..	r/rrwxrwx	0	0	1050	/DCIM/100CANON/IMG_0022.JPG (deleted)
63	Tue Dec 23 20	858798	.a..	r/rrwxrwx	0	0	1051	/DCIM/100CANON/IMG_0023.JPG (deleted)
64	Tue Dec 23 20	838434	.a..	r/rrwxrwx	0	0	1052	/DCIM/100CANON/IMG_0024.JPG (deleted)
65	Tue Dec 23 20	791333	.a..	r/rrwxrwx	0	0	1053	/DCIM/100CANON/IMG_0025.JPG (deleted)
66	Tue Dec 23 20	768385	.a..	r/rrwxrwx	0	0	1054	/DCIM/100CANON/IMG_0026.JPG (deleted)
67	Tue Dec 23 20	840253	.a..	r/rrwxrwx	0	0	1055	/DCIM/100CANON/IMG_0027.JPG (deleted)
68	Tue Dec 23 20	815636	.a..	r/rrwxrwx	0	0	1056	/DCIM/100CANON/IMG_0028.JPG (deleted)
69	Tue Dec 23 20	861552	.a	r/rrwxrwx	0	0	1057	/DCIM/100CANON/IMG_0029.JPG (deleted)

Author: Prof Bill Buchanan



icat – Extract content from image

```
C:\> icat -o 51 nps-2009-canon2-gen1.raw 1029 > img_0001.jpg
```



Author: Prof Bill Buchanan

```
C:\>fsstat -o 51 -f fat16 -i raw nps-2009-canon2-gen1.raw
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16

OEM Name: PwrShot
Volume ID: 0x29d22811
Volume Label (Boot Sector): CANON_DC
Volume Label (Root Directory):
File System Type Label: FAT12

Sectors before file system: 51

File System Layout (in sectors)
Total Range: 0 - 60748
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 6
* FAT 1: 7 - 12
* Data Area: 13 - 60748
** Root Directory: 13 - 44
** Cluster Area: 45 - 60748
METADATA INFORMATION
--------------------------------------------
Range: 2 - 971782
Root Directory: 2
CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 16384
Total Cluster Range: 2 - 1898
Bad Sectors: 44205 44206 44207 44208 44209 44210 44211 44212
FAT CONTENTS (in sectors)
--------------------------------------------
45-76 (32) -> EOF
109-140 (32) -> 57325
```

Fsstat – displays file details of image

Data Loss Prevention - Disk Analysis

- Disk Structure.
- Finding Files.
- Mining Content.
- Carving Files (Undeleting)

http://asecuritysite.com/dlp

Author: Prof Bill Buchanan