

Ad-hoc File System Forensics

Andreas Schuster



Introduction

Standard Operating Procedure



- Extract disk drive
- Connect to write-blocking device
- Create image
- Load image into analysis software
- Analyze!

Introduction

But how about printers?

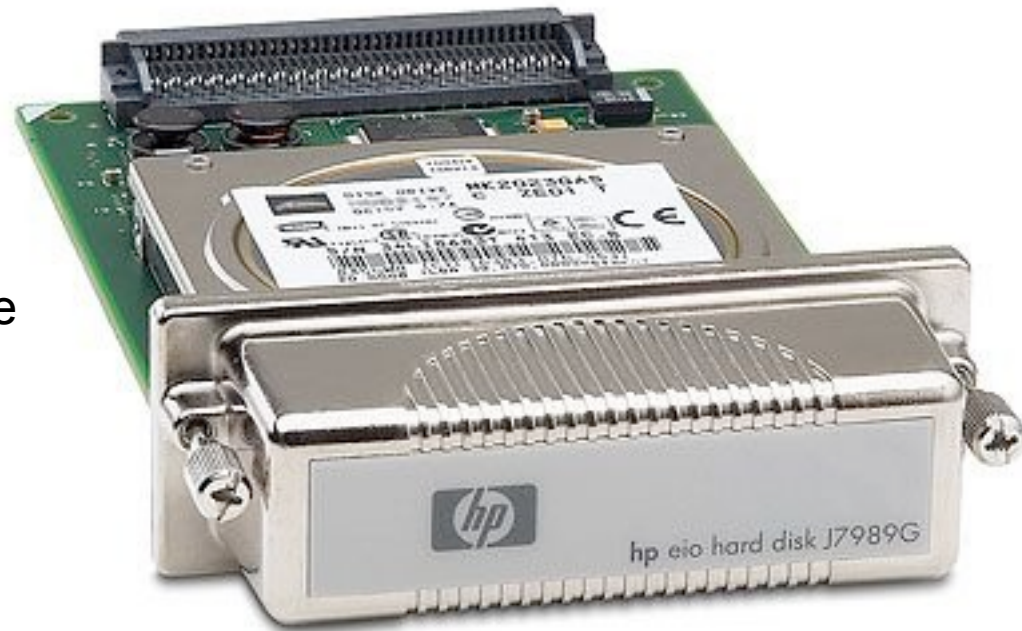


- Printer
- Scanner
- Photocopier
- Fax
- File server
- Web server
- ... and it is equipped with a disk drive!

Introduction

Standard hardware?

- Carrier plate
- Standard ATA disk
- Apply Standard Operating Procedure
- Extract disk drive
- Connect to write-blocking device
- Create image
- Load into analysis software



Introduction

Unrecognized file system - now what?

The screenshot shows the AccessData FTK Imager 2.7.0.33 interface. The Evidence Tree on the left shows a file named '4100_haxord.001' containing 'Partition 1 [38025MB]', which includes an 'Unrecognized file system [Unknown]' and 'Unpartitioned Space [basic disk]'. The File List pane is empty. The Custom Content Sources pane is also empty. The main hex view displays the following data:

Address	Hex Value	ASCII
00000000	00 00 00 48 50 75 78 31-2E 30 30 00 00 00 00	...HPux1.00...
00000010	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000020	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000030	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000040	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000050	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000080	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000090	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000c0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00

At the bottom of the hex view, it says 'Cursor pos = 0; phy sec = 0'. The status bar at the bottom left indicates 'For Help, press F1'.

1. Physical disk examination
2. Volume examination
3. File system layout
4. File name information
5. File metadata
6. File content

Physical Disk Examination

Tools

- Tableau write-blocking ATA/FW bridge
- Tableau Disk Monitor
<http://www.tableau.com/>
- tableau-parm
<http://projects.sentinelchicken.org/tableau-parm>

Physical Disk Examination

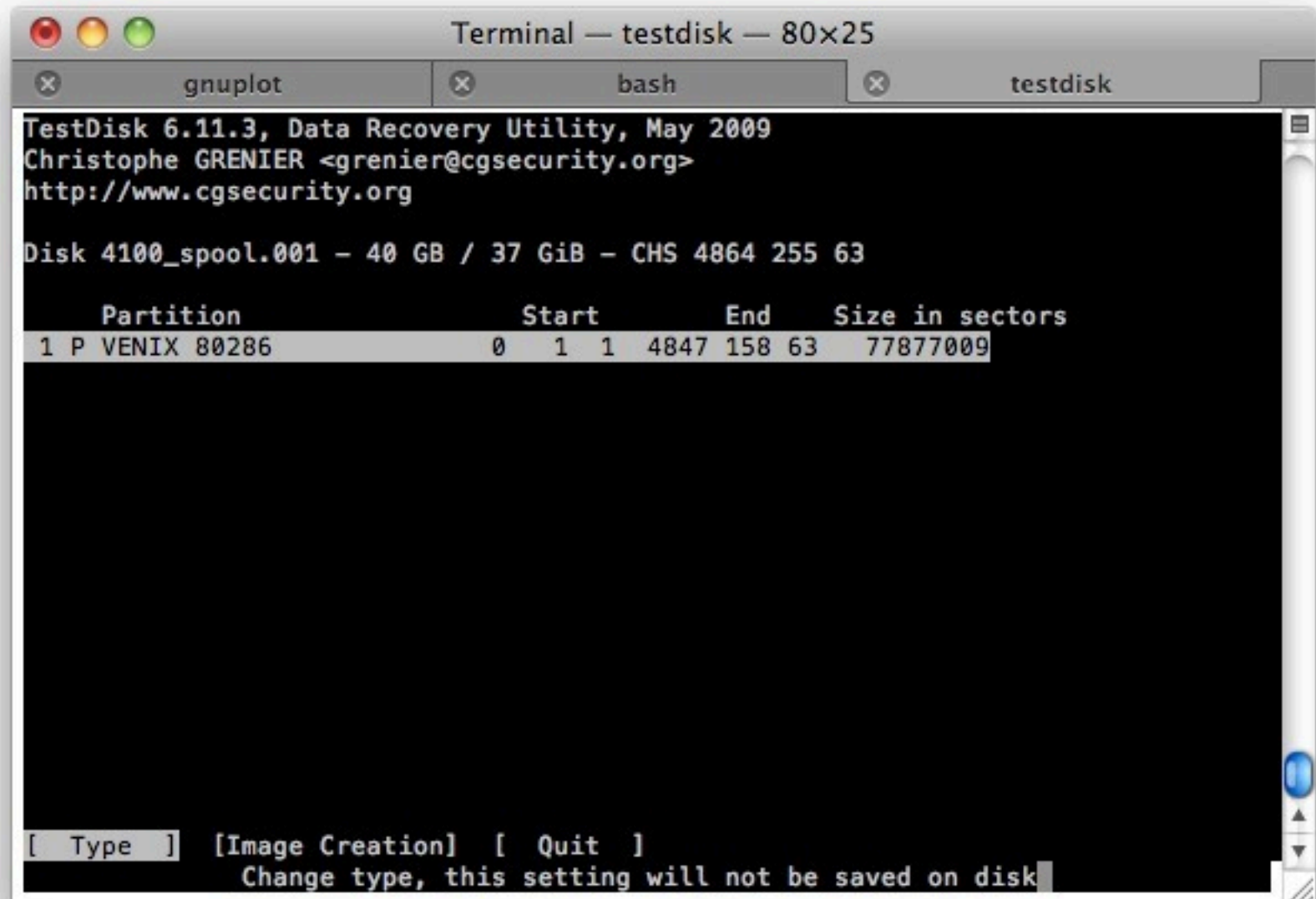
Disk Information

Vendor (empty)
Model HP J6054B
Revision AD101A
Serial number 169V0029T
Bus type IDE
Device type Simplified Direct Access
Removable media? No
Sector size 512 bytes
HPA in use? Yes
DCO in use? No
Security extensions in use? No
Reported capacity 37,1 GB (77.878.016 sectors)
HPA capacity 37,3 GB (78.140.160 sectors)
DCO capacity 37,3 GB (78.140.160 sectors)

- TestDisk by Christophe Grennier
<http://www.cgsecurity.org/wiki/TestDisk>
- Available for MS Win, Linux, *BSD, SunOS, Mac OS X
- Override disk geometry parameters for a really deep scan
 - sectors = 1
 - heads = 1

Volume Examination

Testdisk



```
Terminal — testdisk — 80x25
gnuplot  bash  testdisk
TestDisk 6.11.3, Data Recovery Utility, May 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk 4100_spool.001 — 40 GB / 37 GiB — CHS 4864 255 63

Partition              Start          End      Size in sectors
1 P VENIX 80286         0 1 1 4847 158 63 77877009

[ Type ] [Image Creation] [ Quit ]
Change type, this setting will not be saved on disk
```

Shannon's Entropy

Assumptions

- Alphabet of 256 characters
- 1 byte per character
- Block size \gg size of alphabet

$$H(X) = - \sum_{i=1}^n p(x_i) \log_b p(x_i)$$

Shannon's Entropy

Tools

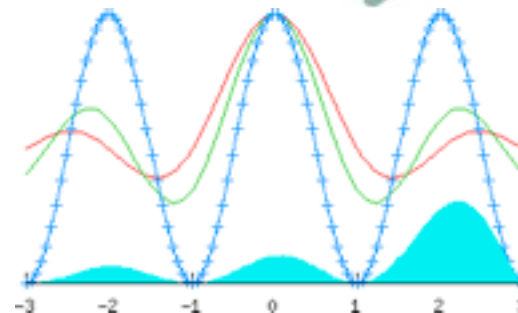
- Python
<http://www.python.org/>



- SQLite
<http://www.sqlite.org/>



- Gnuplot
<http://www.gnuplot.info/>



```
gnuplot> set style data dots
```

```
gnuplot> set datafile separator "|"
```

```
gnuplot> plot "< sqlite3 myfile.db3
```

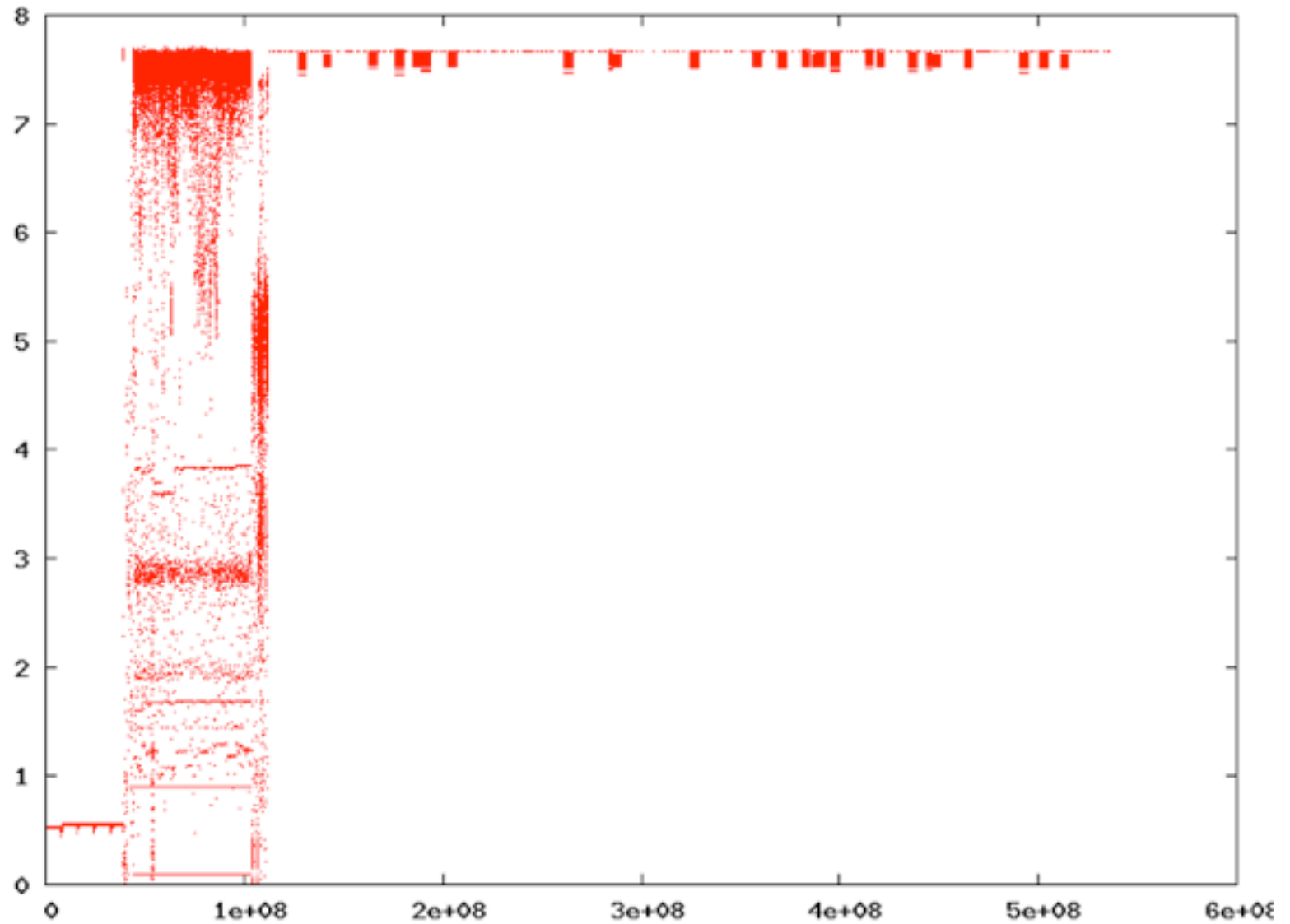
```
'SELECT * FROM tbl_entropy
```

```
WHERE offset BETWEEN 0 AND 1*512*1024*1024;'"
```

```
notitle
```

Shannon's Entropy

Plot of first 512 MiB



Shannon's Entropy

Zoom in on the first sectors

```
gnuplot> set style data dots
```

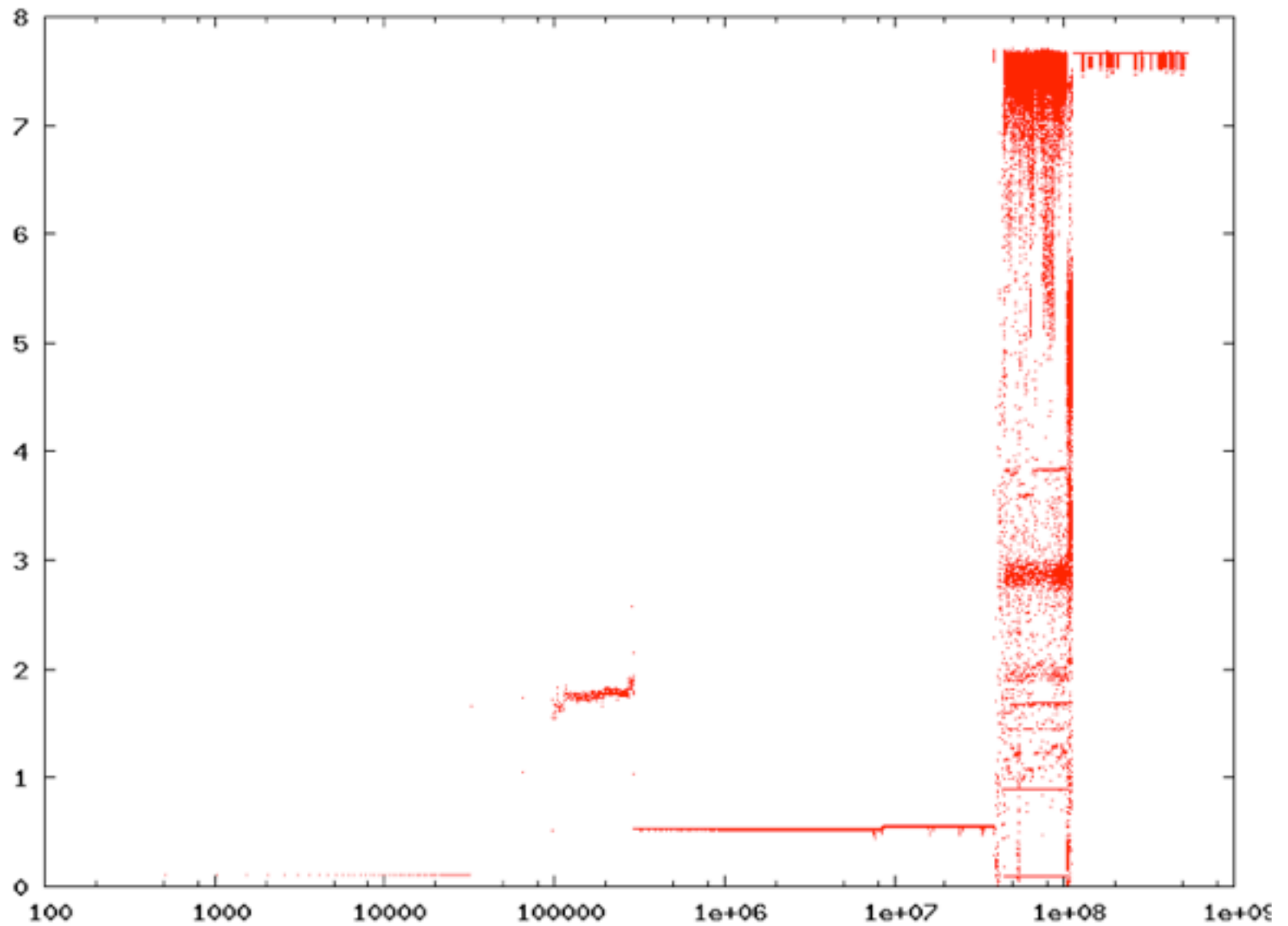
```
gnuplot> set logscale x 10
```

```
gnuplot> set datafile separator "|"
```

```
gnuplot> plot "< sqlite3 myfile.db3  
'SELECT * FROM tbl_entropy  
WHERE offset BETWEEN 0 AND 1*512*1024*1024;'"  
notitle
```

Shannon's Entropy

Plot of first 512 MiB



Shannon's Entropy

Add a bit of color

```
gnuplot> set style data impulses
```

```
gnuplot> set cbrange [0:8]
```

```
gnuplot> set logscale x 10
```

```
gnuplot> set datafile separator "|"
```

```
gnuplot> plot "< sqlite3 myfile.db3
```

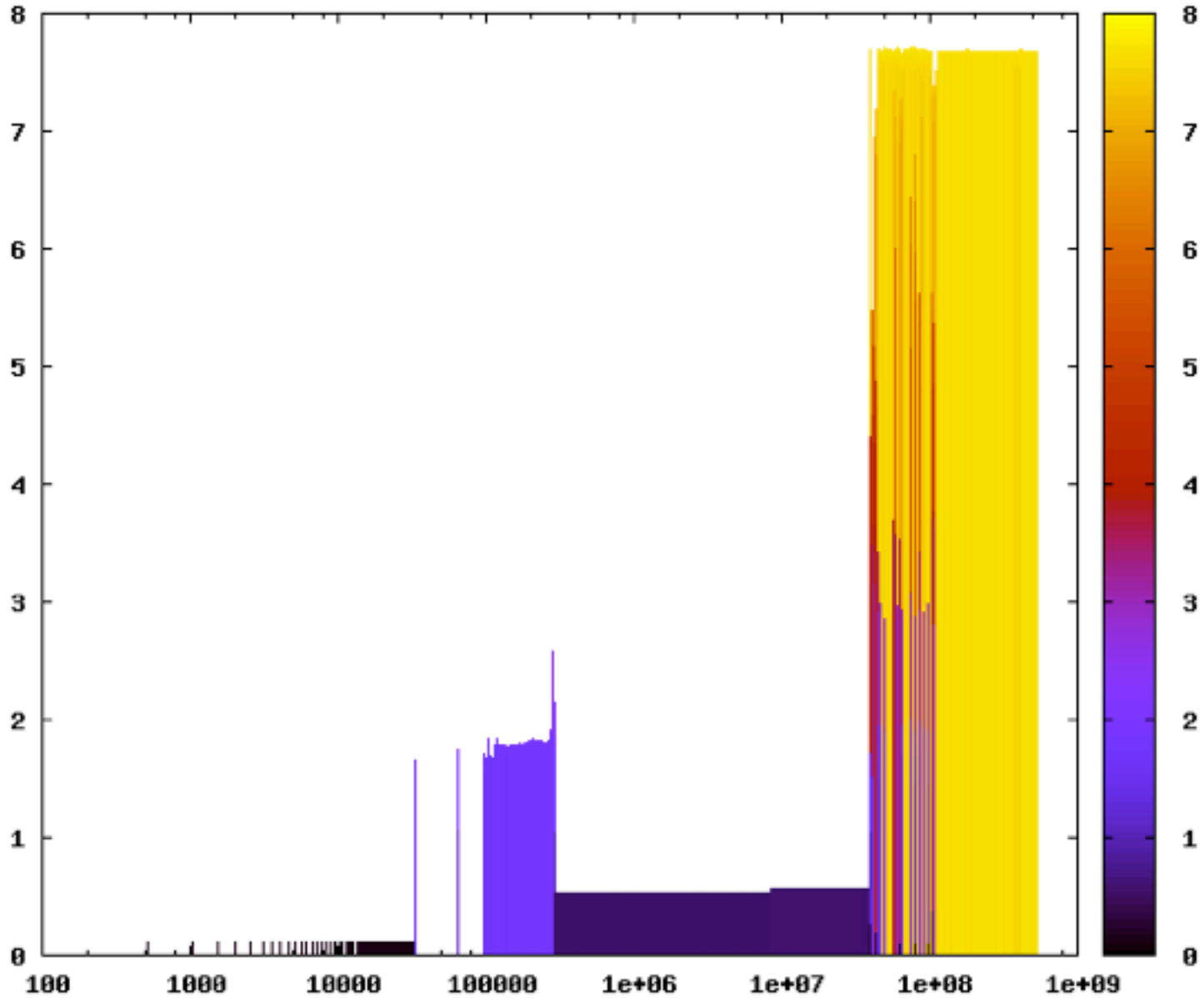
```
'SELECT * FROM tbl_entropy
```

```
WHERE offset BETWEEN 0 AND 1*512*1024*1024;'"
```

```
notitle palette
```

Shannon's Entropy

Plot of first 512 MiB



File system layout

```

$ hexdump -C -n 32768 -s 32768 4100_spool.001
00008000  00 00 00 02 00 00 00 00  00 04 a4 00 00 12 91 3c  |.....<|
00008010  00 00 00 00 00 00 00 00  00 04 a3 ff 00 12 8c 91  |.....|
00008020  00 00 00 00 00 00 00 00  11 11 22 22 00 00 00 1b  |....." "....|
00008030  ca fe fe ca 00 00 80 00  1f ed fa ce 00 00 04 a7  |.....|
00008040  00 00 00 10 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 e5  |.....|
00008050  e5 e5 e5 e5 e5 e5 e5 e5  3f ff ff ff ff ff ff ff  |.....?.....|
00008060  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |.....|
*
00008180  ff 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
00008190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
*
00008200  a5 a5 a5 a5 a5 a5 a5 a5  a5 a5 a5 a5 a5 a5 a5 a5  |.....|
*
0000fe00  00 00 06 03 00 00 00 00  00 04 a4 00 00 12 91 3c  |.....<|
0000fe10  00 00 00 01 e5 e5 e5 e5  00 04 9d fc 00 12 84 06  |.....|
0000fe20  e5 e5 e5 e5 00 00 01 00  11 11 22 22 00 00 00 1b  |....." "....|
0000fe30  ca fe fe ca 00 00 80 00  1f ed fa ce 00 00 04 a7  |.....|
0000fe40  00 00 00 10 e5 e5 e5 e5  00 04 a2 03 00 00 00 00  |.....|
0000fe50  ff ff e5 e5 e5 e5 e5 e5  03 ff ff ff ff ff ff ff  |.....|
0000fe60  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |.....|
*
0000ff80  ff 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
0000ff90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
*
00010000

```

Area 3

Inodes

```
$ hexdump -C -n 512 -s 97792 4100_spool.001
```

```
00017e00 41 ff 00 0a 00 00 00 00 00 00 00 00 00 02 00 |A.....|
00017e10 00 00 0e ea 00 00 0e 4b 00 00 0e 4b 00 00 00 01 |.....K...K....|
00017e20 00 04 a6 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00017e30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00017e40 00 00 00 00 00 00 00 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
00017e50 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
```

*

```
00017e80 41 f8 00 02 00 00 00 00 00 00 00 00 00 04 00 |A.....|
00017e90 00 00 0e e4 00 00 00 20 00 00 00 20 00 00 00 01 |..... ..|
00017ea0 00 04 ab 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00017eb0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00017ec0 00 00 00 00 00 00 00 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
00017ed0 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
```

```
$ hexdump -C -n 512 -s 284160 4100_spool.001
```

```
00045600 81 ff 00 01 00 00 00 01 00 06 00 00 00 05 6c 76 |.....lv|
00045610 00 00 0e 4c 00 00 0e 4d 00 00 0e 4d 00 00 00 0c |...L...M...M....|
00045620 00 0c e7 00 0c e8 00 0c e9 00 0c ea 00 0c eb 00 |.....|
00045630 0c ec 00 0c ed 00 0c ee 00 0c ef 00 0c f0 00 0c |.....|
00045640 f1 00 00 00 00 00 00 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
00045650 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
```

*

Unused inodes and endianness

```

$ hexdump -C -n 1024 -s 295424 4100_spool.001
00048200 00 00 06 0a 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048210 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048280 00 00 06 0b 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048290 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048300 00 00 06 0c 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048310 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048380 00 00 06 0d 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048390 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048400 00 00 06 0e 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048410 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048480 00 00 06 0f 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048490 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048500 00 00 06 10 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048510 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|
*
00048580 00 00 06 11 00 00 00 00 ff ff e5 e5 e5 e5 e5 e5 |.....|
00048590 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 e5 |.....|

```

Data and directories

```

$ hexdump -C -n 512 -s 39026176 4100_spool.001
02537e00  00 00 00 01 00 0c 00 01  2e 00 00 00 00 00 00 01  |.....|
02537e10  00 0c 00 02 2e 2e 00 00  00 00 00 02 00 14 00 09  |.....|
02537e20  50 65 72 6d 53 74 6f 72  65 00 00 00 00 00 00 2c  |PermStore.....,|
02537e30  00 14 00 0a 50 6f 73 74  53 63 72 69 70 74 00 00  |....PostScript..|
02537e40  00 00 00 2d 00 0c 00 03  50 4a 4c 00 00 00 00 2e  |...-....PJL.....|
02537e50  00 14 00 0a 73 61 76 65  44 65 76 69 63 65 00 e5  |....saveDevice..|
02537e60  00 00 00 87 00 14 00 08  73 6f 6c 75 74 69 6f 6e  |.....solution|
02537e70  00 00 e5 e5 00 00 00 33  00 14 00 09 77 65 62 53  |.....3....webS|
02537e80  65 72 76 65 72 00 00 00  00 00 00 8d 00 10 00 06  |erver.....|
02537e90  63 70 62 4c 6f 67 00 e5  00 00 05 ae 01 68 00 03  |cpbLog.....h..|
02537ea0  43 56 53 00 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 e5  |CVS.....|
02537eb0  e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 e5  |.....|

```

Estimating the cluster size

Foremost started at Mon Jan 11 22:53:22 2010

Invocation: foremost -i Data/4100_spool.001 -t gif -q -w -o carve/ -v

Output directory: carve

Configuration file: /usr/local/etc

Processing: Data/4100_spool.001

|-----

File: Data/4100_spool.001

Start: Mon Jan 11 22:53:22 2010

Length: Unknown

Num	Name (bs=512)	Size	File Offset	Comment
0:	81791.gif	224 B	41876992	(140 x 40)
1:	81919.gif	208 B	41942528	(140 x 40)
2:	81983.gif	787 B	41975296	(59 x 14)
3:	82047.gif	180 B	42008064	(64 x 14)
4:	82111.gif	185 B	42040832	(64 x 14)
5:	82175.gif	185 B	42073600	(64 x 14)
6:	82239.gif	787 B	42106368	(59 x 14)
7:	82303.gif	182 B	42139136	(64 x 14)
8:	82367.gif	787 B	42171904	(59 x 14)
9:	82431.gif	186 B	42204672	(64 x 14)
10:	82495.gif	787 B	42237440	(59 x 14)
...				

Putting it all together

Prototyping in 010 Editor

The image shows the 010 Editor interface with two main panes. The left pane is the 'Inspector' showing a file structure for 'HPux100template.bt'. The right pane is a hex dump of the file content, with a yellow highlight on a specific entry.

Name	Value	Start
struct MER mbr		0h
struct PART partition		7E00h
uint32 inodestotal	304128	FE08h
uint32 blockstotal	1216828	FE0Ch
uint32 inodesfree	302588	FE18h
uint32 blocksfree	1213446	FE1Ch
struct INODE inode[0]	dir (0)	17E00h
uint32 is_file : 1	0	17E00h
uint32 is_dir : 1	1	17E00h
uint32 unknown1 : 1	0	17E00h
uint32 unknown2 : 4	00000000,b	17E00h
uint32 access : 9	00000001 11111111,b	17E00h
uint32 unknown3 : 16	00001010,b	17E02h
uint32 unknown4	0	17E04h
int16 owner	0	17E08h
uint16 padding	0	17E0Ah
uint32 filesize	512	17E0Ch
time_t timestamp[3]		17E10h
uint32 unknown5	1	17E1Ch
uint32 offset	4A600h	17E20h
byte unknown6[92]		17E24h
struct DIRENTRY entry[0]	.. (1)	2537E00h
struct DIRENTRY entry[1]	.. (1)	2537E0Ch
struct DIRENTRY entry[2]	PermStore (2)	2537E18h
struct DIRENTRY entry[3]	PostScript (44)	2537E2Ch
struct DIRENTRY entry[4]	PJL (45)	2537E40h
struct DIRENTRY entry[5]	saveDevice (46)	2537E4Ch
struct DIRENTRY entry[6]	solution (135)	2537E60h
struct DIRENTRY entry[7]	webServer (51)	2537E74h
struct DIRENTRY entry[8]	cpbLog (141)	2537E88h
struct DIRENTRY entry[9]	CVS (1454)	2537E98h
struct INODE inode[1]	dir (0)	17E80h

Address	Hex	ASCII
253:7D90h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DA0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DB0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DC0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DD0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DE0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7DF0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7E00h:	00 00 00 01 00 0C 00 01 2E 00 00 00 00 00 00 01
253:7E10h:	00 0C 00 02 2E 2E 00 00 00 00 00 02 00 14 00 09
253:7E20h:	50 65 72 6D 53 74 6F 72 65 00 00 00 00 00 00 2C	PermStore.....
253:7E30h:	00 14 00 0A 50 6F 73 74 53 63 72 69 70 74 00 00	...PostScript..
253:7E40h:	00 00 00 2D 00 0C 00 03 50 4A 4C 00 00 00 00 2E	...-...PJL.....
253:7E50h:	00 14 00 0A 73 61 76 65 44 65 76 69 63 65 00 E5	...saveDevice.&
253:7E60h:	00 00 00 87 00 14 00 08 73 6F 6C 75 74 69 6F 6E	...+.solution
253:7E70h:	00 00 E5 E5 00 00 00 33 00 14 00 09 77 65 62 53	..&&...3....webS
253:7E80h:	65 72 76 65 72 00 00 00 00 00 00 8D 00 10 00 06	erver.....
253:7E90h:	63 70 62 4C 6F 67 00 E5 00 00 05 AE 01 68 00 03	cpbLog.&...@.h..
253:7EA0h:	43 56 53 00 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	CVS.AAAAAAAAAAAAAA
253:7EB0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7EC0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7ED0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7EE0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7EF0h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F00h:	00 00 00 04 00 00 00 00 FF FF E5 E5 E5 E5 E5 E5yy&&&&&&
253:7F10h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F20h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F30h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F40h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F50h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F60h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F70h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA
253:7F80h:	00 00 00 05 00 00 00 00 FF FF E5 E5 E5 E5 E5 E5yy&&&&&&
253:7F90h:	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	AAAAAAAAAAAAAAAAAAAA

Questions & Answers

Thank You for Your Attention!

Andreas Schuster

a.schuster@yendor.net

<http://computer.forensikblog.de/en/>