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?

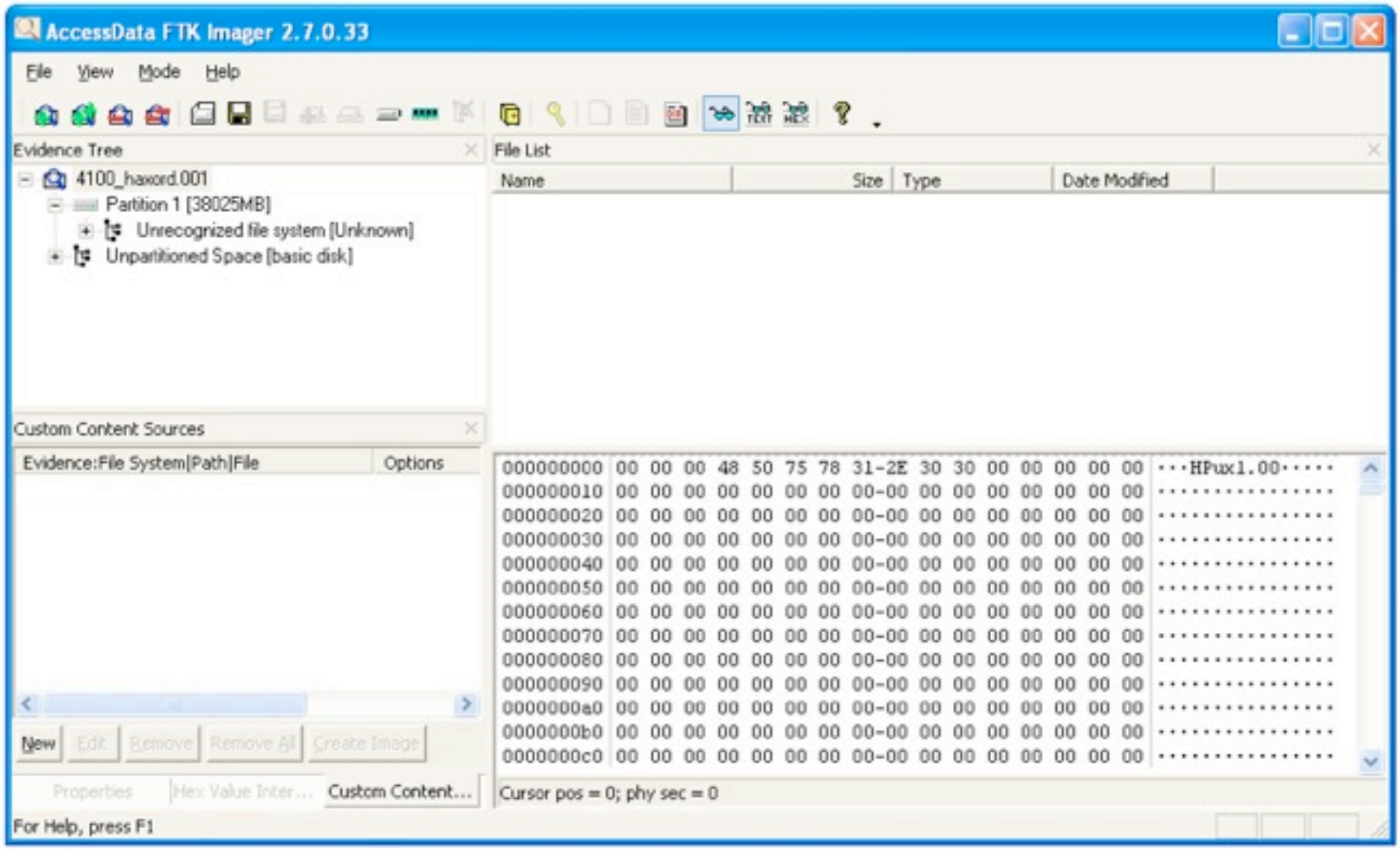
- Printer
- Scanner
- Photocopier
- Fax
- File server
- Web server
- ... and it is equipped with a disk drive!

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?



Analysis Process

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

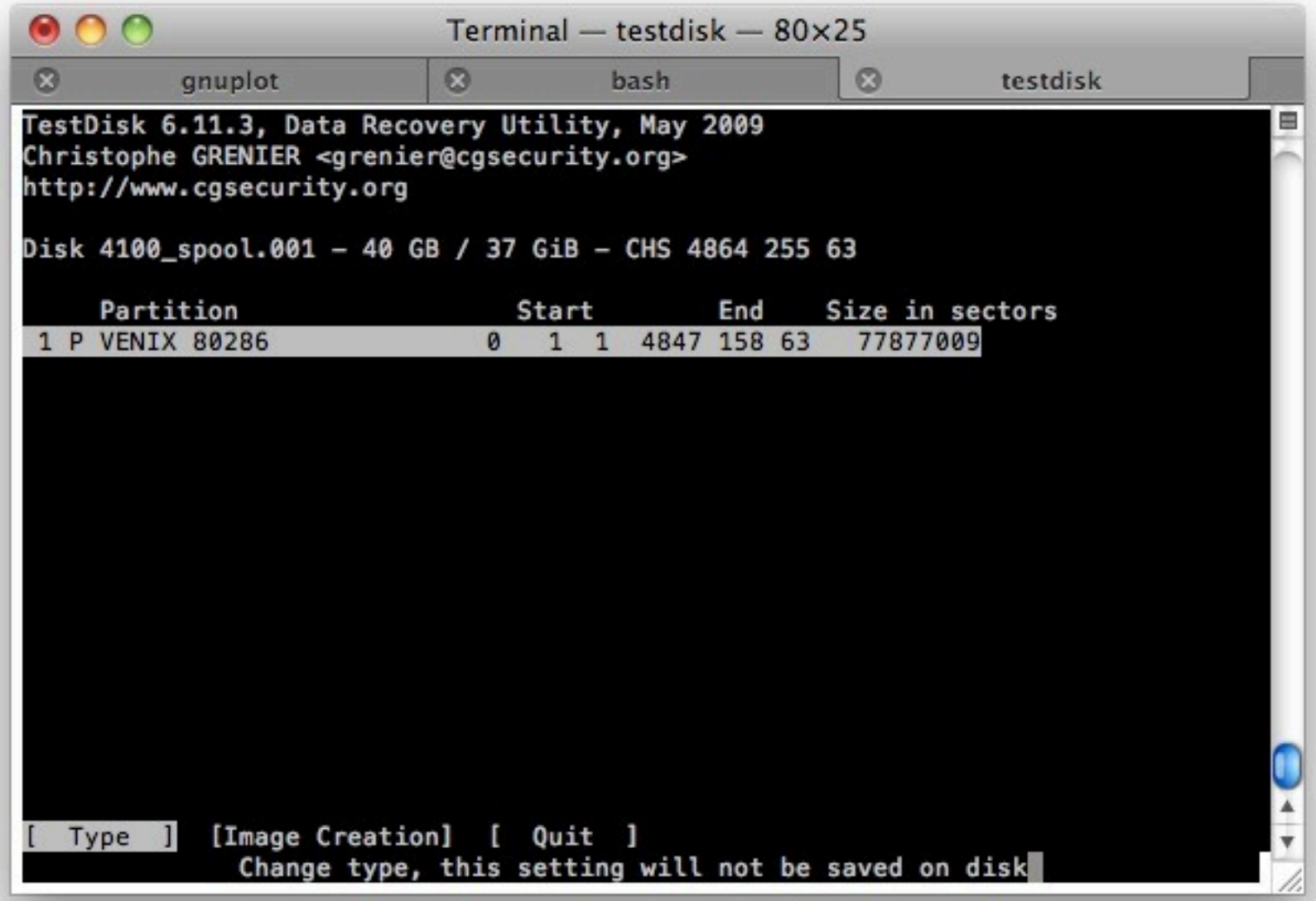
Disk Information

```
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



Shannon‘s Entropy
Assumptions

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

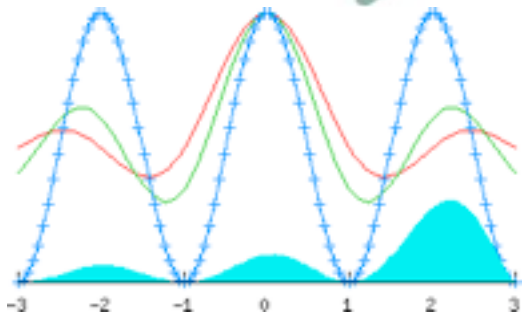
$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i)$$

Shannon‘s Entropy
Tools

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

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

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

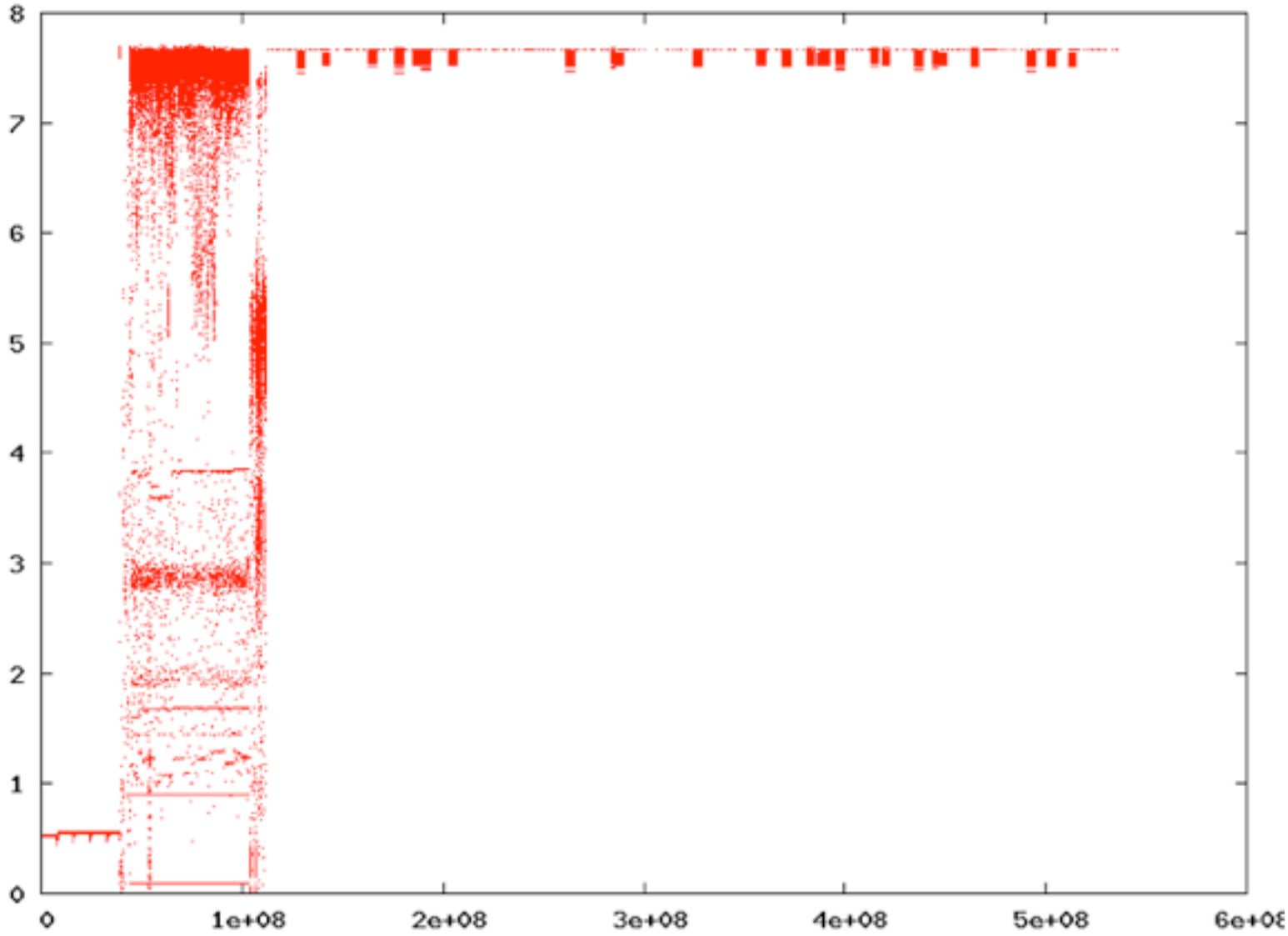


Shannon‘s Entropy
1st attempt

```
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

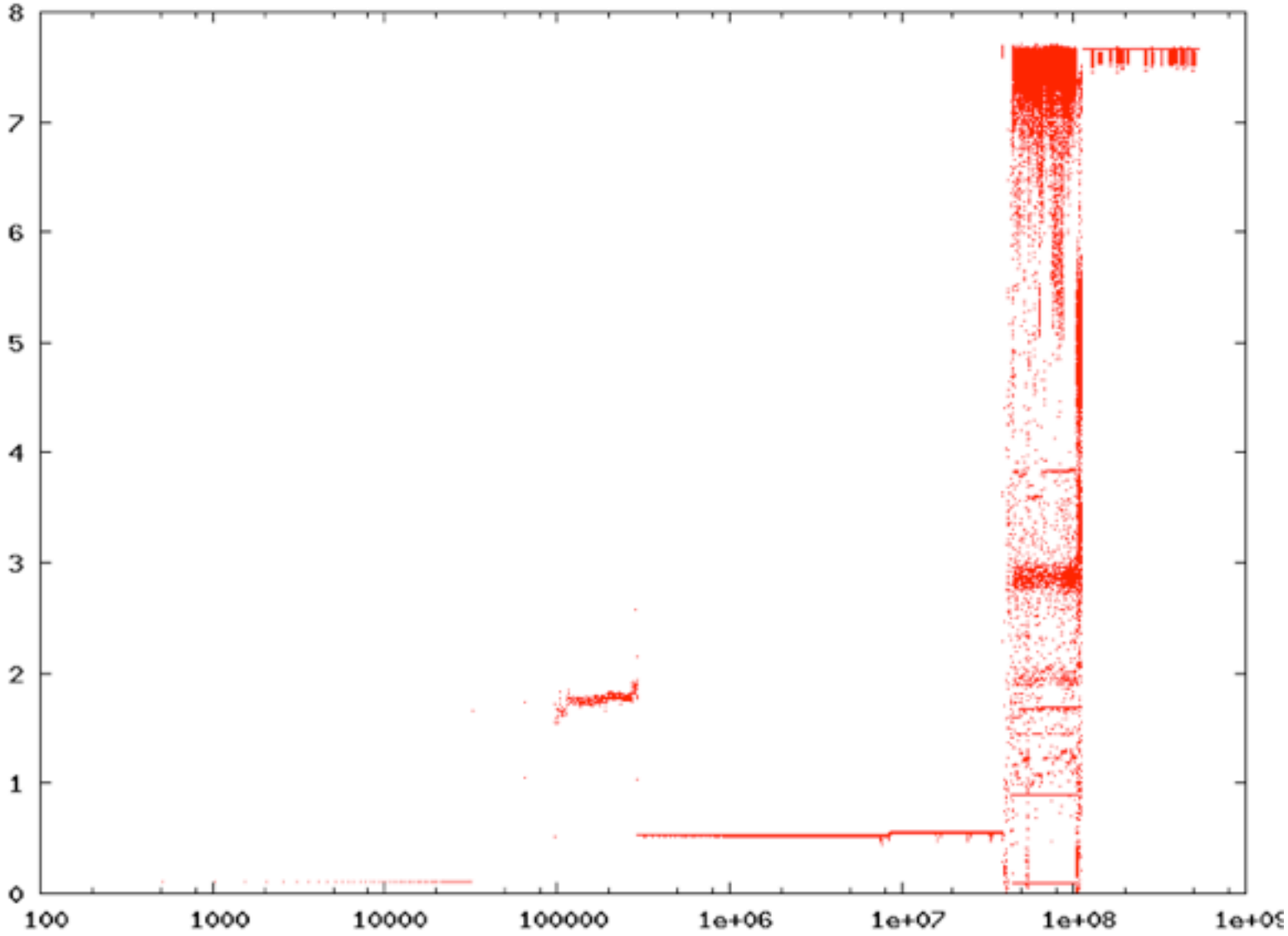


Shannon‘s Entropy
Zoom in on the first sectors

```
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



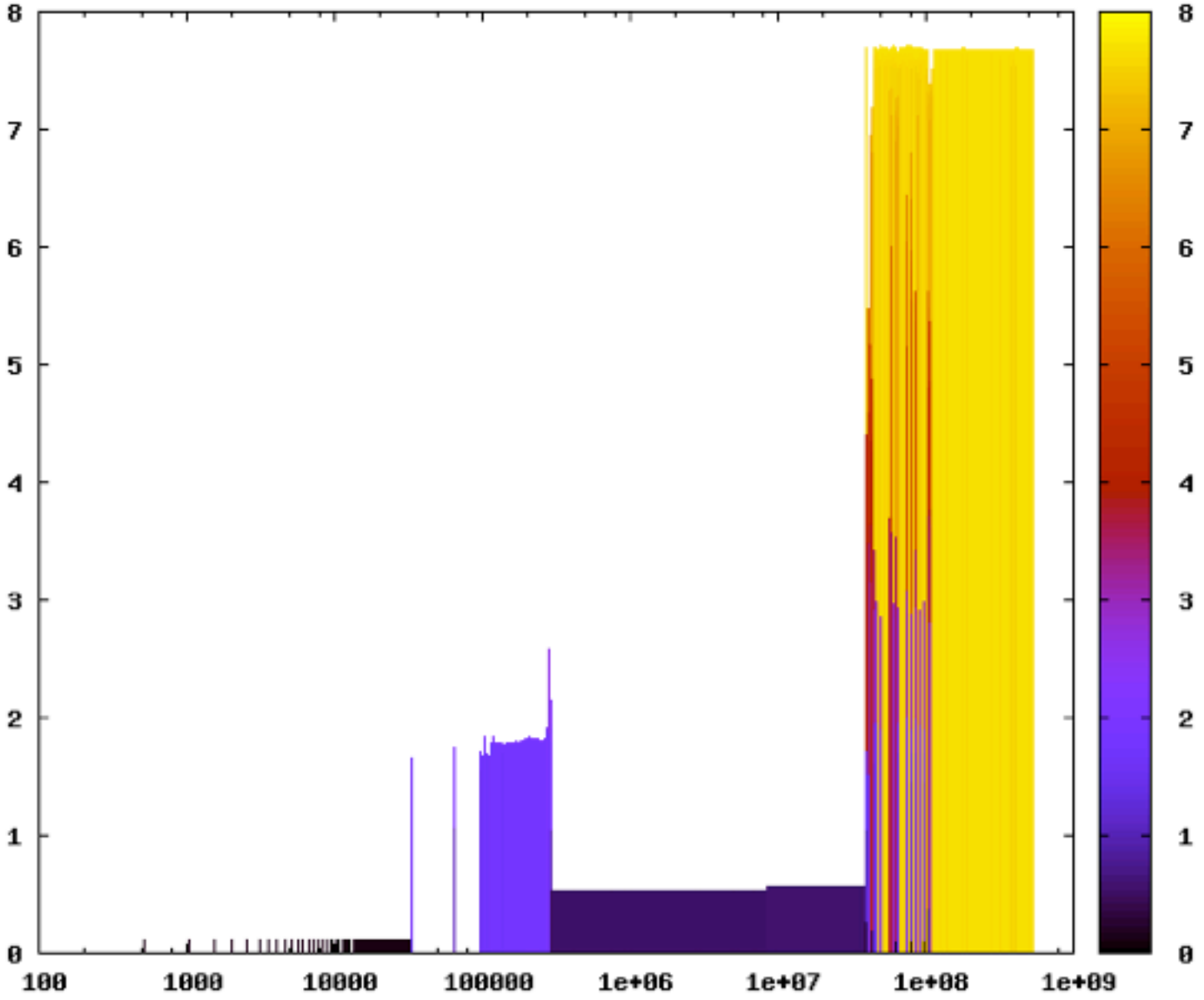
Shannon‘s Entropy

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



Area 1

MBR followed by blank sectors

```
$ hexdump -C -n 32768 -s 0 4100_spool.001
00000000  00 00 00 48 50 75 78 31  2e 30 30 00 00 00 00 00  |...HPux1.00.....|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001c0  00 00 40 00 00 00 3f 00  00 00 11 4f a4 04 00 00  |..@...?....O....|
000001d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
00000200  00 00 00 62 6c 61 6e 6b  00 00 00 00 00 00 00 00  |...blank........|
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400  00 00 00 62 6c 61 6e 6b  00 00 00 00 00 00 00 00  |...blank........|
00000410  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
...
00007c00  00 00 00 62 6c 61 6e 6b  00 00 00 00 00 00 00 00  |...blank........|
00007c10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00007e00  a5 a5 a5 a5 a5 a5 a5 a5  a5 a5 a5 a5 a5 a5 a5 a5  |................|
*
00008000
```

Area 2
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 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 e5  |................|
00017e50  e5 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 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 e5  |................|
00017ed0  e5 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 e5  |................|
00045650  e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 e5  |................|
*
```

Area 4

Unused inodes and endianess

```
$ 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 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 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 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 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 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 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 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 e5  |................|
```

Area 5
Data and directories

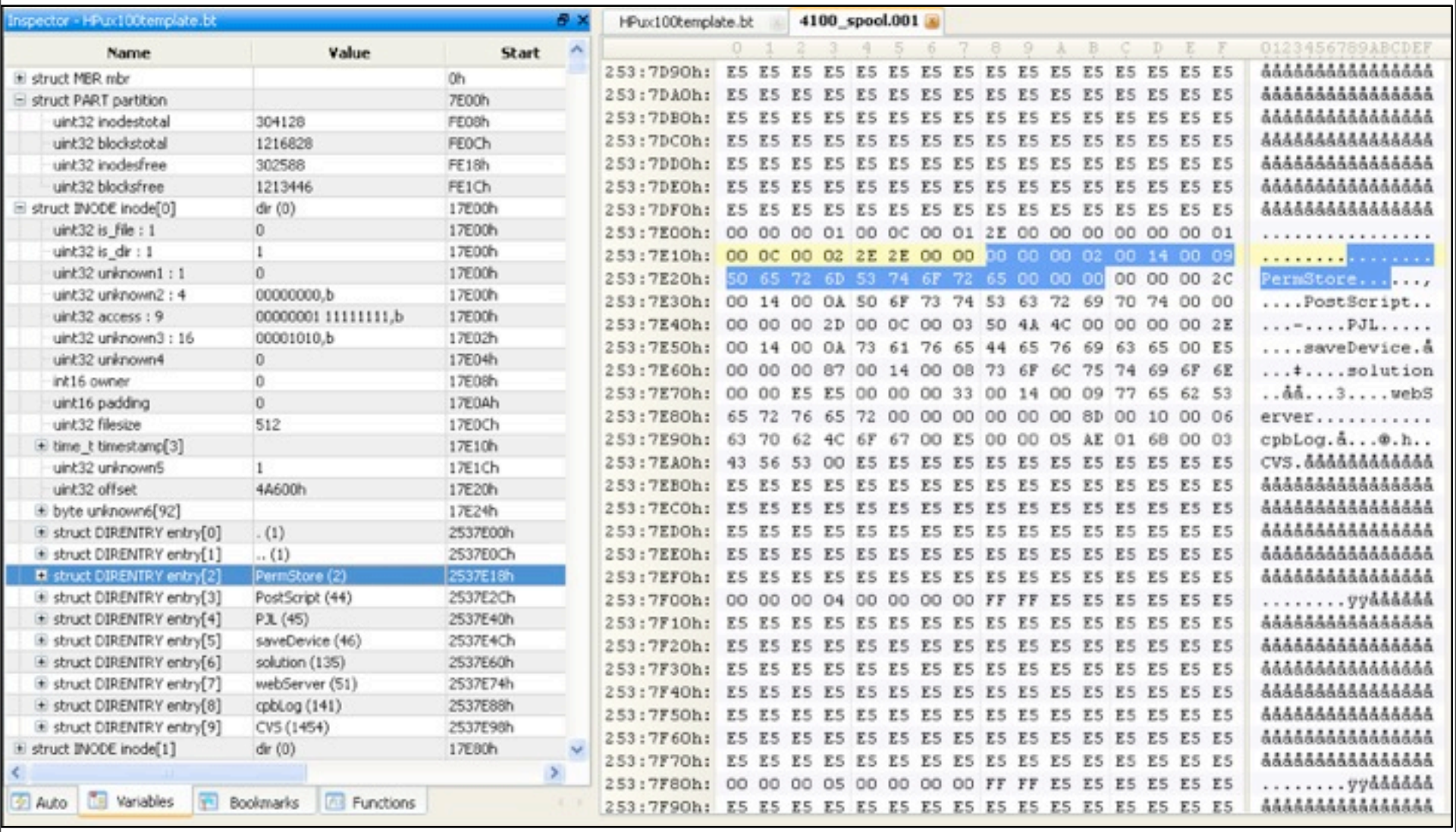
```
$ hexdump -C -n 512 -s 39026176 4100_spool.001
02537e00  00 00 00 01 00 0c 00 01  2e 00 00 00 00 00 00 01  |................|
02537e10  00 0c 00 02 2e 2e 00 00  00 00 00 02 00 14 00 09  |................|
02537e20  50 65 72 6d 53 74 6f 72  65 00 00 00 00 00 00 2c  |PermStore......,|
02537e30  00 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  |................|
```

Area 5
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



Questions & Answers

Thank You for Your Attention!

Andreas Schuster

a.schuster@yendor.net
http://computer.forensikblog.de/en/