The Born Digital Record of the Writing Process

Digital Forensics and Concepts of Representation for the DSE

Thorsten Ries

Workshop 3 at ESTS 2016 / DiXiT 3 at Antwerp University, 4 October 2016

GHENT UNIVERSITY

fwo

Introduction

Outline

Introduction (15 min)

Forensic Imaging, Analysis and Recovery Tools (45 min)

Break (10 min)

Hands-on Session:
Forensic Analysis of the Digital Dossier Génétique (120 min)

Discussion: The Born Digital Record and the DSE (20 min)

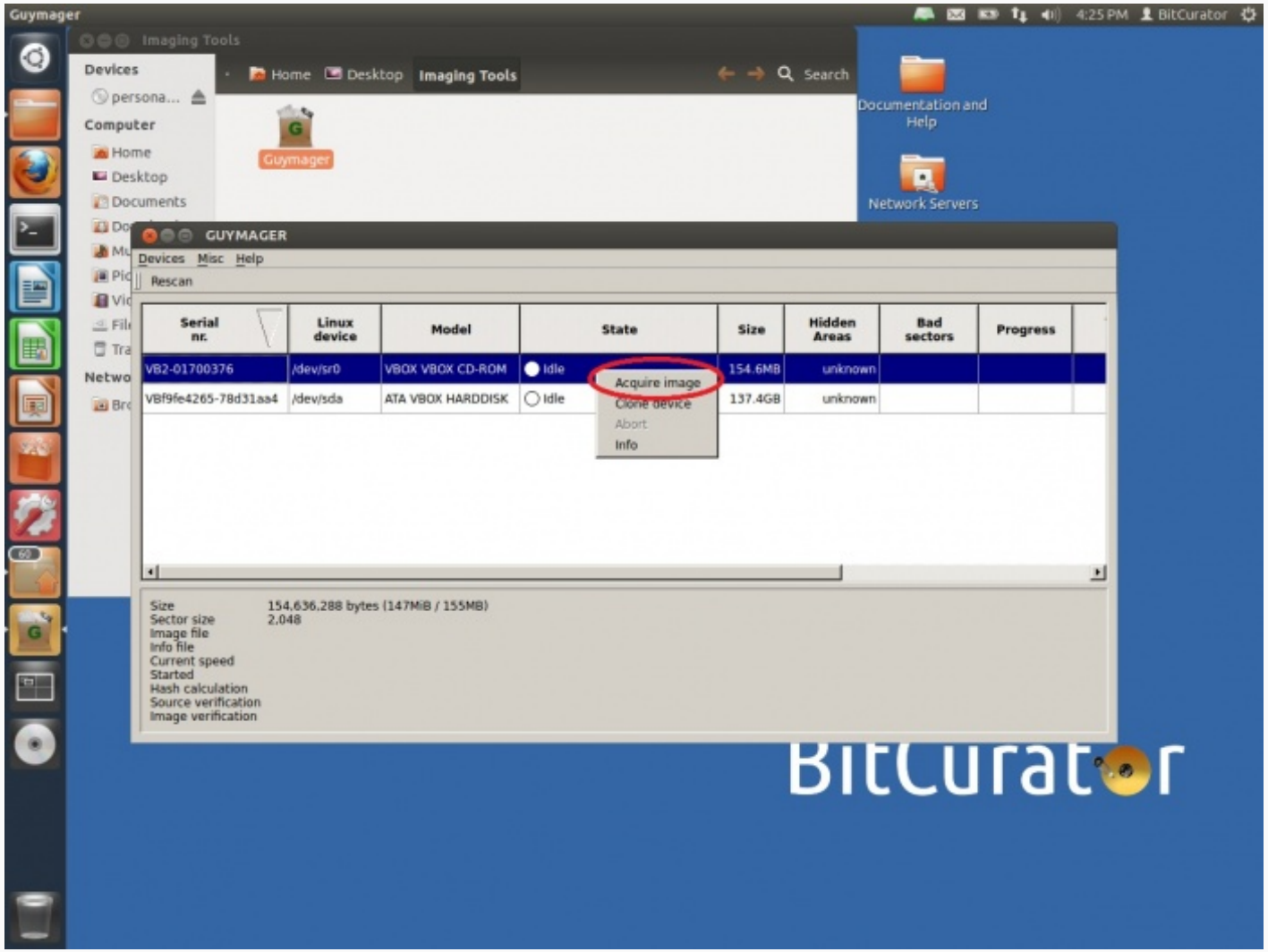
Outline (a bit more detailed)

- Introduction (15 min)
- Forensic Imaging, Analysis and Recovery Tools (45 min)
  - Forensic imaging
  - Forensic System Analysis: Sleuthkit, Autopsy
  - File and data recovery (file undelete, carving, drive slack analysis, fragmented files, system restore points, other)
  - File structures (Fastsave, RSID)
  - Cloud forensics (Dropbox, Google Docs)
- Break (10 min)
- Hands-on Session: Forensic Analysis of the Digital Dossier Génétique (120 min) – Caine Linux, evidence: artificial Win2k, Win7, Win10 images
- Discussion: The Born Digital Record and the DSE (20 min)

Caine Linux

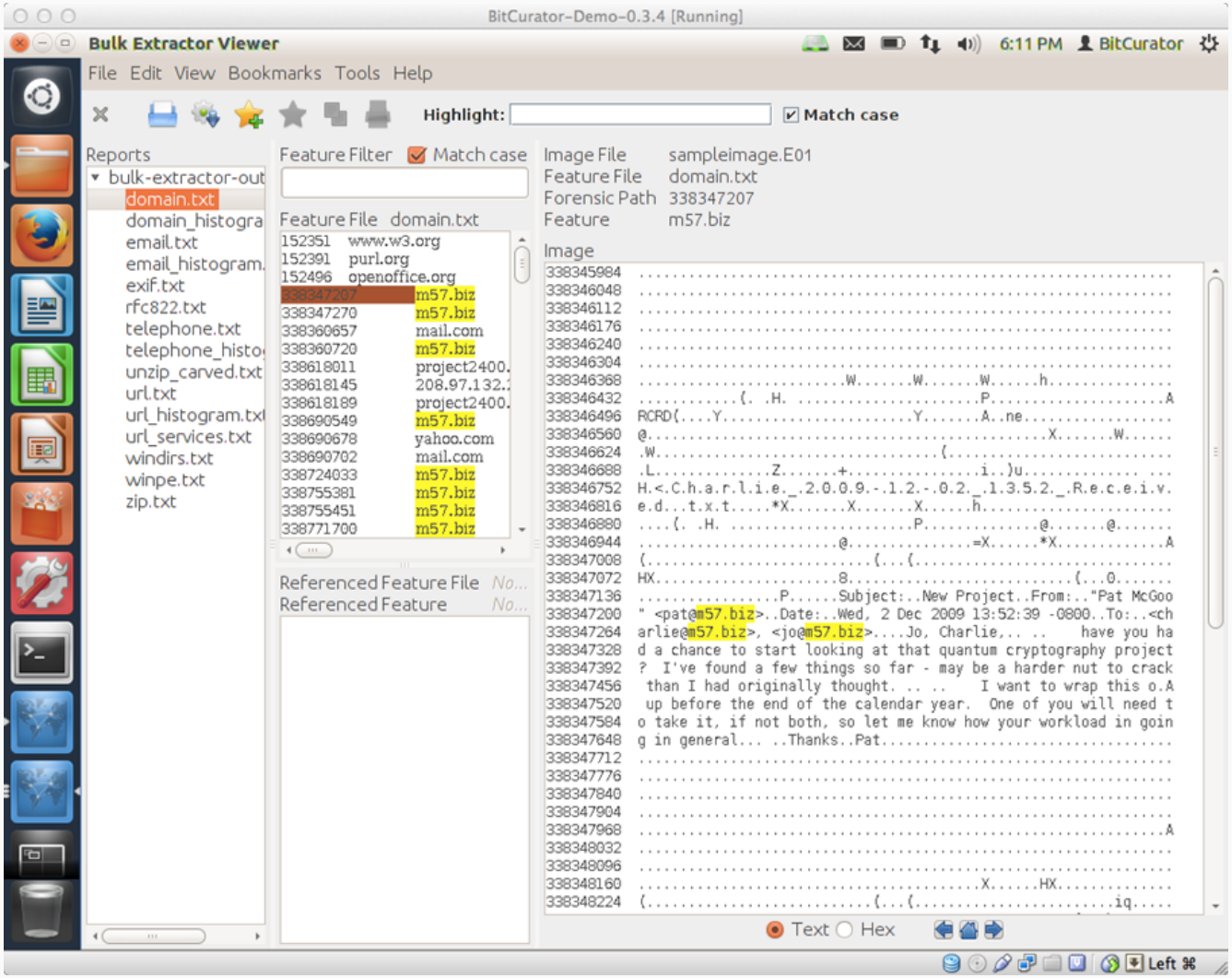

Computer
Network
Caine's Home
Firefox Web Browser
Trash
Systemback (installer)
Mixed scripts
Caja (root)
INFO
BlockON/OFF
Keyboard changer
DEEPSPACE
CAINE
Computer Aided INvestigative Environment
Guymager
FMount - mount image file
XAll
0 B/s
0 B/s
dom nov 1
08:49

BitCurator



http://www.bitcurator.net/ (running guymager).

BitCurator



http://www.bitcurator.net/ (running bulkextractor).

Forensig 2.0

Forensig 2.0 – Opera

Menü | Forensig 2.0

www.forensig.de/scriptmanager/

Forensig 2.0 | Home | Generator | Manual | Theory | beta@tester.de | Logout

Scriptmanager

Upload new script | Create empty Script

	#	Name	Valid	Errors	Status
delete edit	244	ossimple	True		▶ run script
delete edit	245	oscomplex	True		▶ run script
delete edit	246	android	True		▶ run script
delete edit	247	fatsimple	True		▶ run script
delete edit	248	fatcomplex	True		▶ run script
delete edit	251	android2	True		▶ run script
delete edit	253	example	True		▶ run script
delete edit	254	Ottawa_...	True		▶ run script
delete edit	255	GPT	True		▶ run script
delete edit	256	defs	True		▶ run script

Kontakt: Forensig 2.0 - Lehrstuhl für Informatik 1 - Universität Erlangen - Christian Moch

By Christian Moch, PhD thesis, Erlangen University, 2010, http://d-nb.info/1068781181/04.

Forensic Imaging, Analysis and Recovery Tools

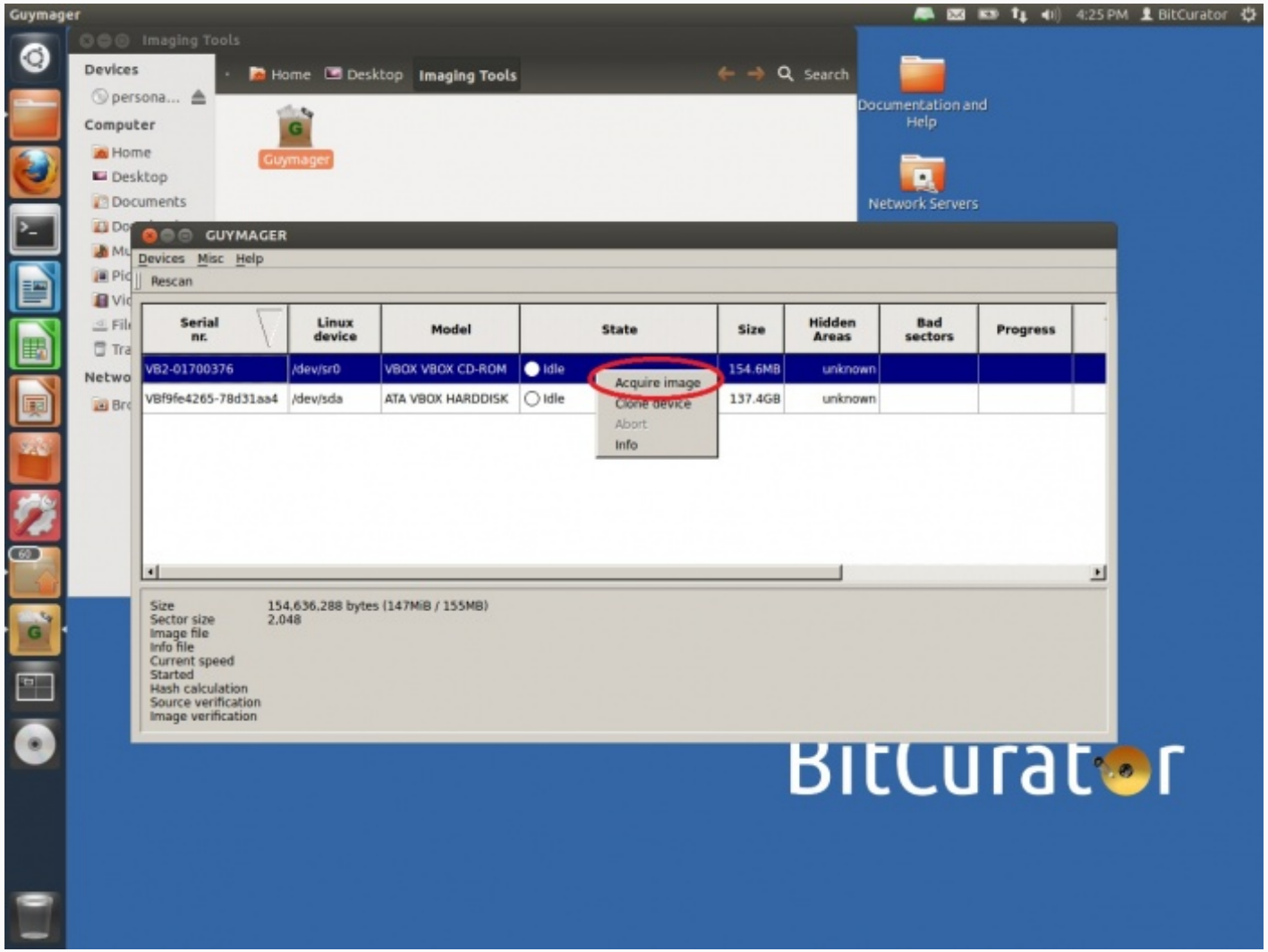
Forensic Imaging: »dd«

- bit-by-bit imaging of the harddrive platter with »dd« or one of its variants dc3dd, dd_rescue, FTKimager, EnCase, aimage

```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
[thorsten@localhost ~]$ dd if=/dev/hda of=/mnt/sda1/usw/Forensisches_Image.dd
```

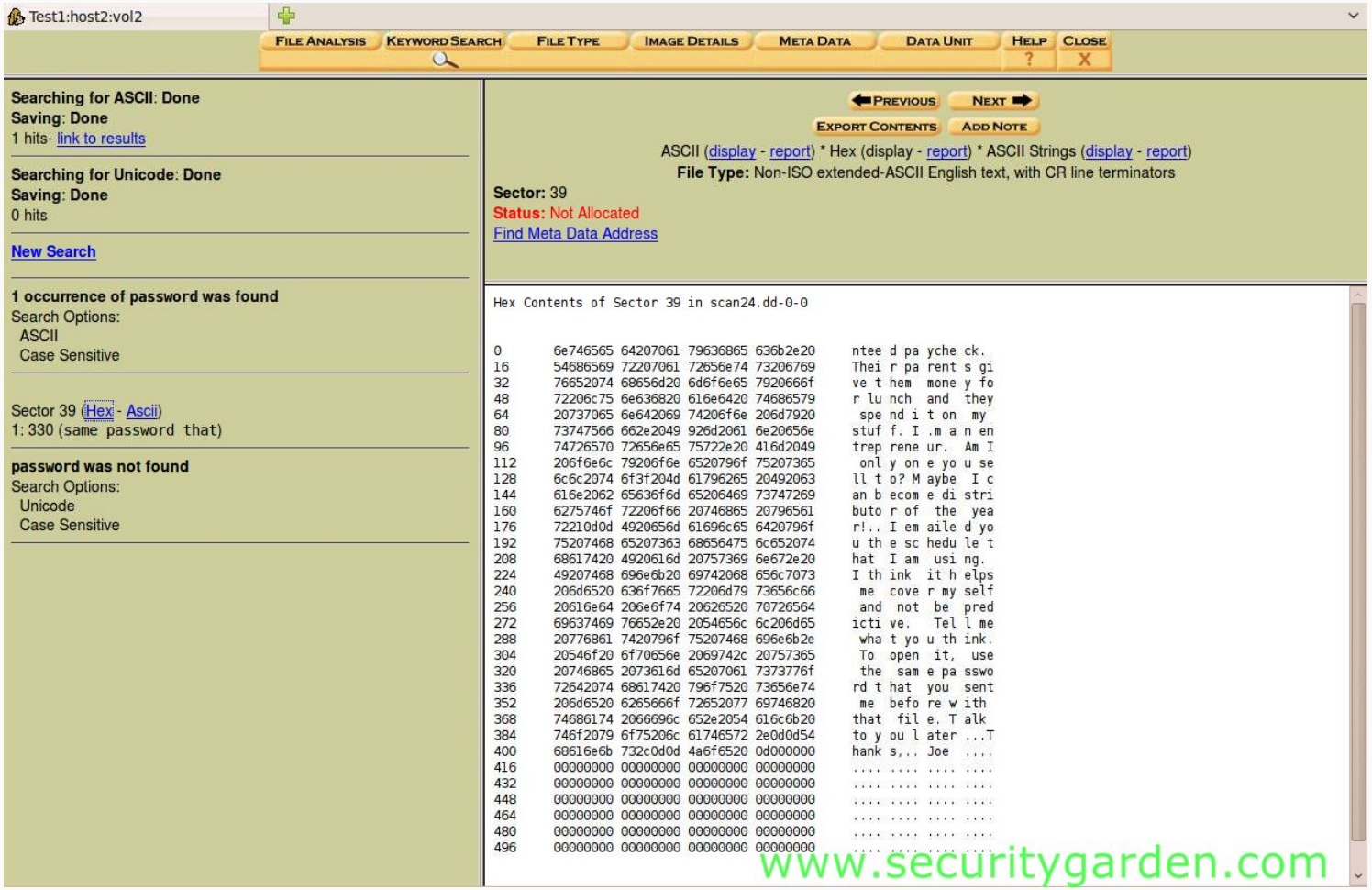
- Please note: Just copying the visible folders and ›ISO-Images‹ are useless for forensic use.
- In cases of severe damage a laboratory can help
- Can be performed on any kind of block-based storage
- Can be authenticated thru hashing
- Should be done asap, as long as the drive works and the wafer is intact.

Forensic Imaging: Guymager (dd GUI)



http://www.bitcurator.net/ (running guymager).

System Analysis: Sleuthkit



Sleuthkit (hex view)

System Analysis: Autopsy Browser

xpinbox1 - Autopsy 3.0.0b3

File Edit View Tools Window Help

Close Case | Add Image | Generate Report | Keyword Lists | Search...

- Images
  - xp-sp3-v4.001
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS (0x07): 63-8193149)
      - $Extend
      - Documents and Settings
      - Program Files
      - System Volume Information
      - WINDOWS
      - $OrphanFiles
    - vol3 (Unallocated: 8193150-10485215)
- Views
  - File Types
    - Images
    - Videos
    - Audio
    - Documents
  - Recent Files
    - Final Day
    - Final Day - 1
    - Final Day - 2
    - Final Day - 3
    - Final Day - 4
    - Final Day - 5
    - Final Day - 6
- Results
  - Extracted Content
    - Bookmarks (174)
    - Cookies (1911)
    - Web History (1218)
    - Downloads (30)
    - Recent Documents (72)
    - Installed Programs (72)
    - Device Attached (9)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits

Directory Listing

\xp-sp3-v4.001\vol2 — 25 Results

Table View | Thumbnail View

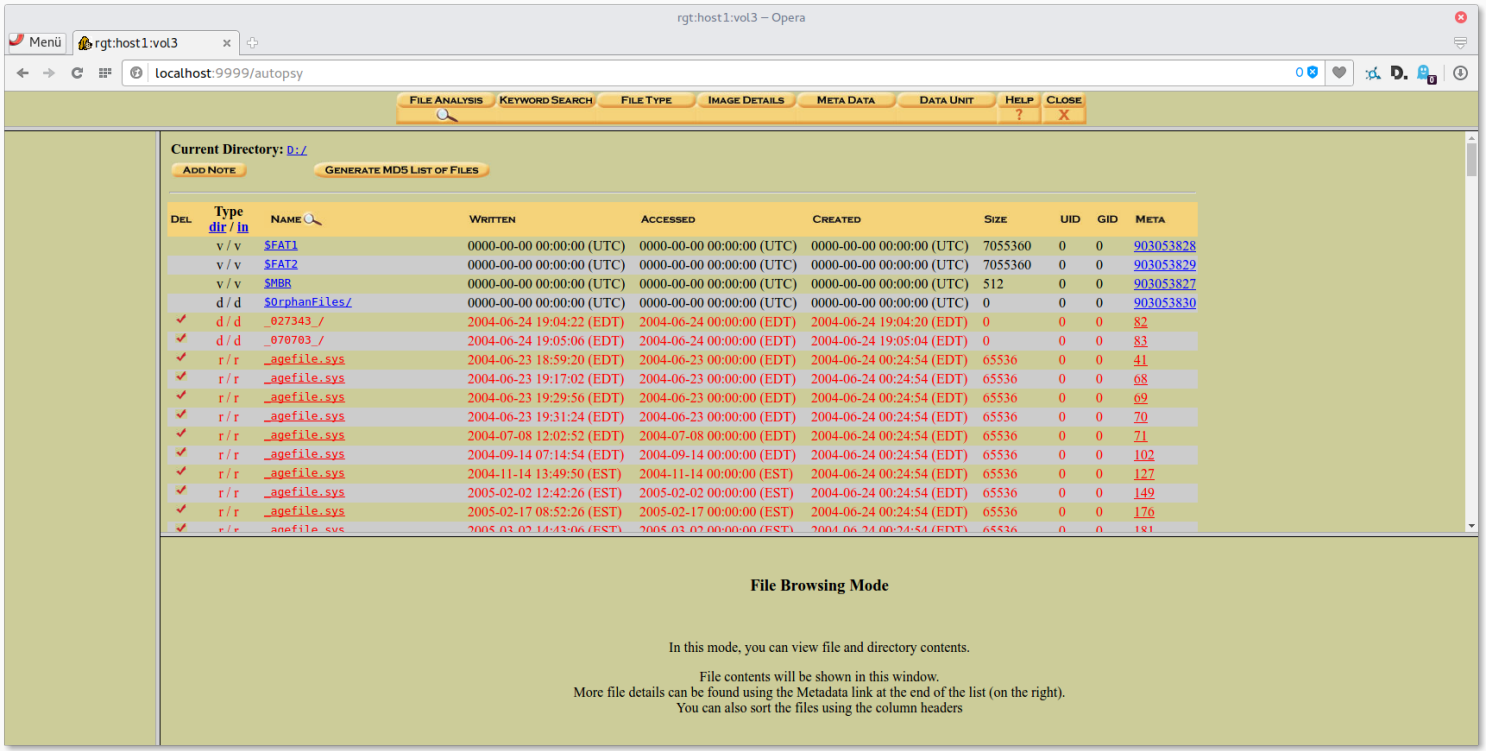
Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Alloca
$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alloca
$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Alloca
$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Alloca
$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Alloca
$Secure:$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloca
$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Alloca
$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloca
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alloca
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloca
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Alloca
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Alloca
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alloca
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alloca
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloca
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Alloca
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Alloca

Result View | Hex View | Media View | String View | Text View

Page: 1 of 3 Page Go to Page:

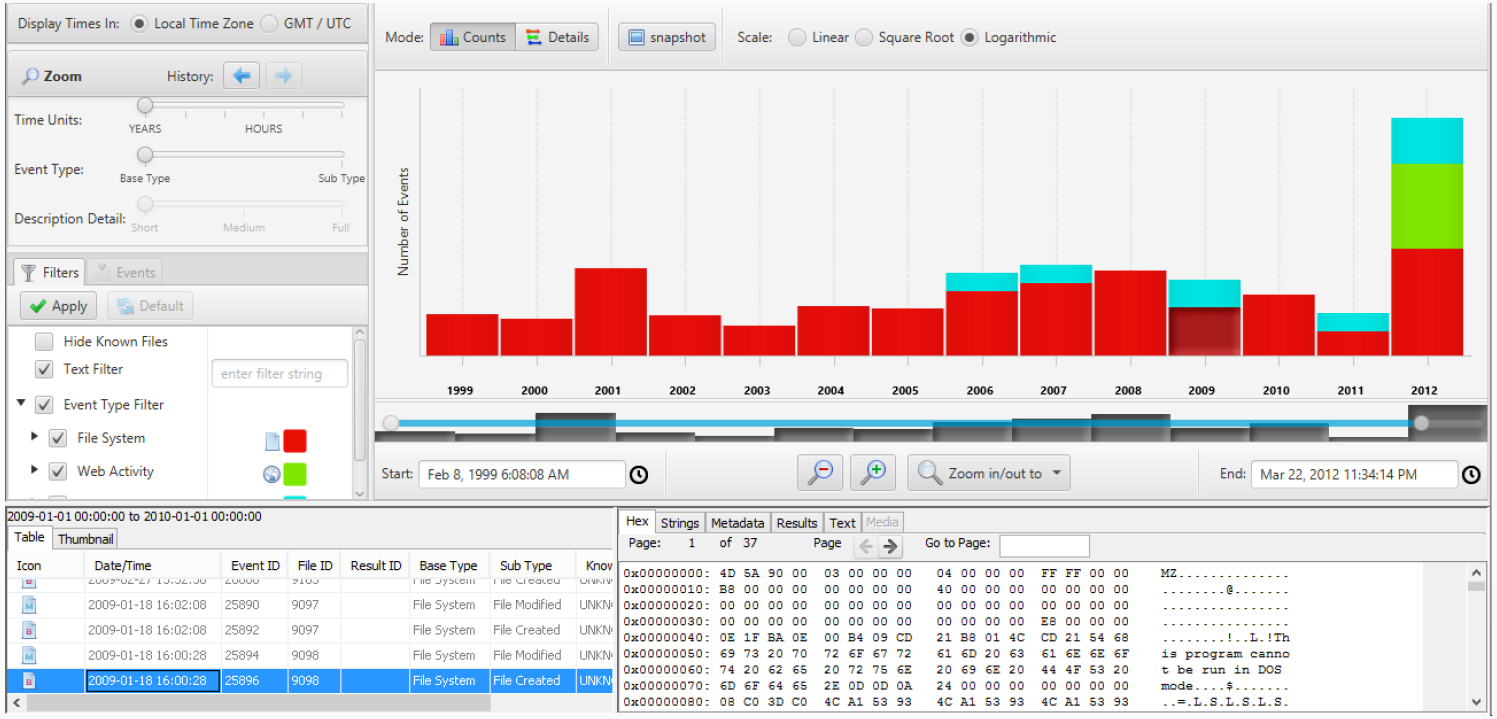
```
0x000000: 66 55 66 39 EC 66 FD E5   FF FF 00 00 1E 06 66 53   fUf..f........fS
0x000010: 66 56 66 57 B9 FD A4 C1   E9 04 52 C8 03 C1 7D D8   fVfW............
0x000020: 7D C0 66 39 CC 66 30 0E   00 00 52 D1 30 0E 04 00   ..f..f..........
0x000030: 66 39 5E 08 66 39 4E 0C   66 39 76 10 66 39 7E 14   f.^.f.N.f.v.f.~.
0x000040: 66 39 56 18 66 39 6E 1C   7D D0 66 BC 06 10 00 00   f.V.f.n...f.....
0x000050: 66 55 66 52 66 57 66 56   66 51 66 53 66 33 C0 66   fUfRfWfVfQfSf3.f
0x000060: 33 DB 66 33 C9 66 33 D2   66 33 F6 66 33 FF E8 B7   3.f3.f3.f3.f3...
0x000070: 02 66 0F B2 26 00 00 66   5F 66 5E 66 5B 07 1F 66   .f..&..f_f^f[..f
0x000080: 5D CB 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ]...............
0x000090: 55 39 EC 56 57 53 60 4E   06 B8 00 D8 CD 15 53 39   U..VWS.N......S.
0x0000a0: 5E 04 C6 27 C6 47 01 58   C6 67 02 C6 47 03 30 4F   ^..'.G.X.g..G..O
0x0000b0: 04 C6 77 06 C6 57 07 30   7F 08 30 77 0A 5B 5F 5E   ..w..W.....w.[_^
0x0000c0: 5D C3 55 39 EC 56 B8 01   D8 60 4E 06 60 6E 08 39   ].U..V....N..n..
0x0000d0: 76 04 CD 15 60 C4 5E 5D   C3 06 53 B8 00 F0 7D C0   v...`.^]..S.....
```

System Analysis: Autopsy Browser (Linux)



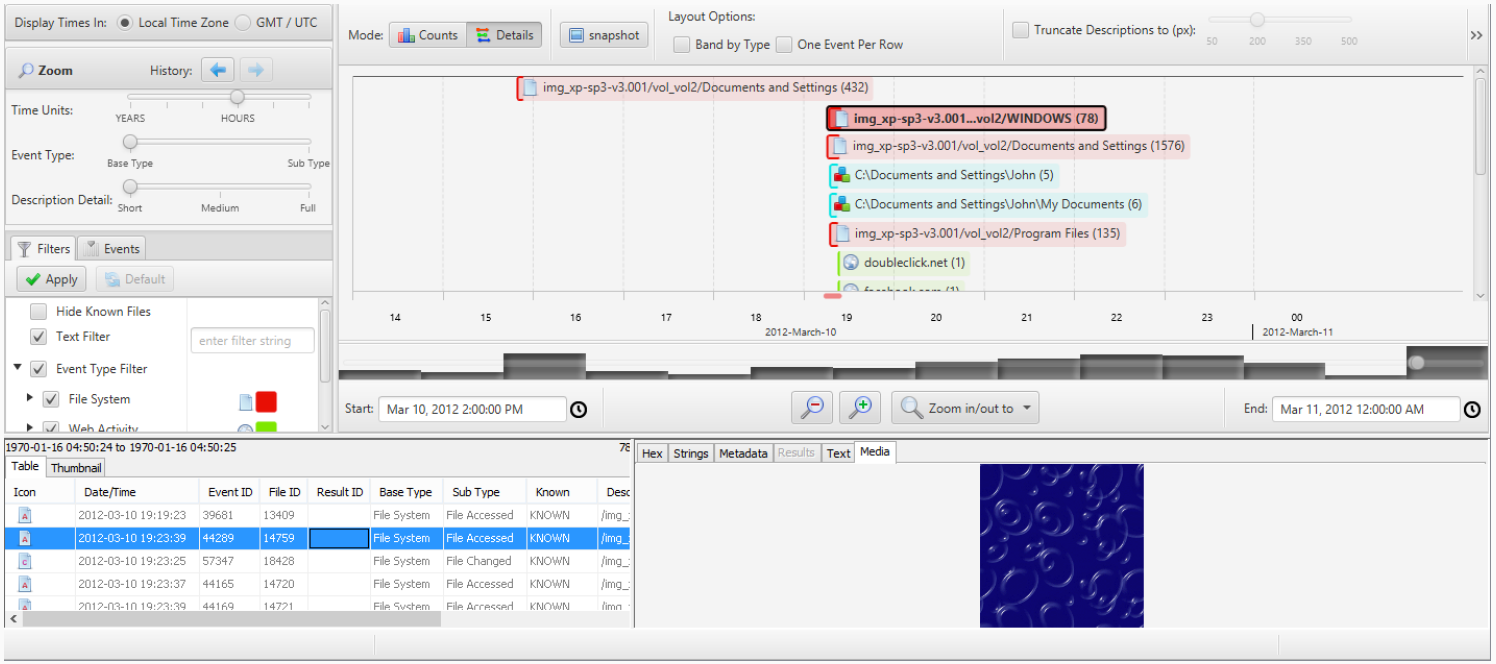
Autopsy, Orphaned File View

System Analysis: Autopsy Browser



Autopsy: timeline

System Analysis: Autopsy Browser



Autopsy: timeline

Forensic Data Recovery: retrieving the text

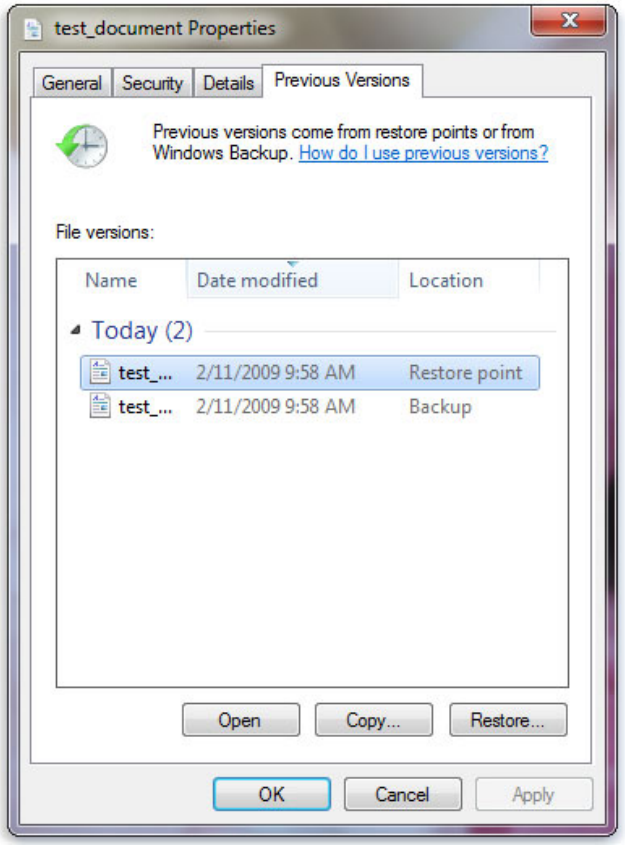
- never (really immediately) deleted
- if deleted, partially recoverable through undelete, carving etc. (if not overwritten, redundancy!)
- system-specific: restore points, backup data
- file structure.

Forensic Data Recovery: Undelete

```
Maschine  Geräte  Hilfe
C:\Dokumente und Einstellungen\Thorsten\Desktop\testdisk-6.12-WIP\testdisk_win.exe
estDisk 6.12-WIP, Data Recovery Utility, April 2009
hristophe GRENIER <grenier@cgsecurity.org>
ttp://www.cgsecurity.org
1 * FAT32                    0   1  1   734 254 63   11807712 [NO NAME]
irectory /Dokumente und Einstellungen/Thorsten/Desktop/Container/Testfall_F_Vi
e_Zwischnespeicherungen
rwxr-xr-x     0     0         0  2-Feb-2010 13:46 .
rwxr-xr-x     0     0         0  2-Feb-2010 13:46 ..
rwxr-xr-x     0     0     10752  2-Feb-2010 13:47 Neu Microsoft Word-Dokument.
rwxr-xr-x     0     0     10752  2-Feb-2010 13:47 Testfall_F_Viele_Zwischenspe
rwxr-xr-x     0     0       162  2-Feb-2010 13:47 ~$stfall_F_Viele_Zwischenspe
rwxr-xr-x     0     0     19456  2-Feb-2010 13:48 _WRD0002.TMP
rwxr-xr-x     0     0     10752  2-Feb-2010 13:47 Sicherungskopie von Testfall
rwxr-xr-x     0     0     19456  2-Feb-2010 13:48 Testfall_F_Viele_Zwischenspe
rwxr-xr-x     0     0     19456  2-Feb-2010 14:39 _WRD3770.TMP
rwxr-xr-x     0     0     19456  2-Feb-2010 13:48 Sicherungskopie von Testfall
rwxr-xr-x     0     0     19456  2-Feb-2010 14:39 Testfall_F_Viele_Zwischenspe
rwxr-xr-x     0     0      5632  2-Feb-2010 14:47 _WRD4040.TMP
rwxr-xr-x     0     0     19456  2-Feb-2010 14:47 _WRD4040.TMP
rwxr-xr-x     0     0     19456  2-Feb-2010 14:39 Sicherungskopie von Testfall
rwxr-xr-x     0     0     19456  2-Feb-2010 14:47 Testfall_F_Viele_Zwischenspe
rwxr-xr-x     0     0       162 11-Feb-2010 20:13 ~$stfall_F_Viele_Zwischenspe
                                                  Next
se Left arrow to go back, Right arrow to change directory, c to copy,
   h to hide deleted files, q to quit_
Start   testdisk-6.12-WIP   C:\Dokumente und Ein...   DE   16:33
Strg Rechts
```

TestDisk undelete operation

Forensic Data Recovery: restore points



Mac Time Machine

Win7 Virtual Snapshot Service restore

Forensic Data Recovery: file carving, e.g. foremost

```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
[thorsten@localhost ~]$ foremost -i Forensisches_Image.dd -o /Wiederherstellen/
```

- »foremost« is the oldest file carver, but still quite reliable
- More recent carvers Scalpel, PhotorRec, CarvFs, LibCarvPath, EnCase, Adroit ...
- Please note: Differing heuristics will lead to different carving results.
- Please note: Carving results are often »constructed traces«, sometimes even misleading.

Forensic Data Recovery: drive slack, raw image inspect

First step: isolate the slack blocks with the »blkls«--command (formerly »dls«):

```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
[thorsten@localhost ~]$ dls -f -s Forensisches_Image.dd > Extr_Slack-Blocks.dls
```

Second step: read the text fragments from the isolated blocks with »strings«:

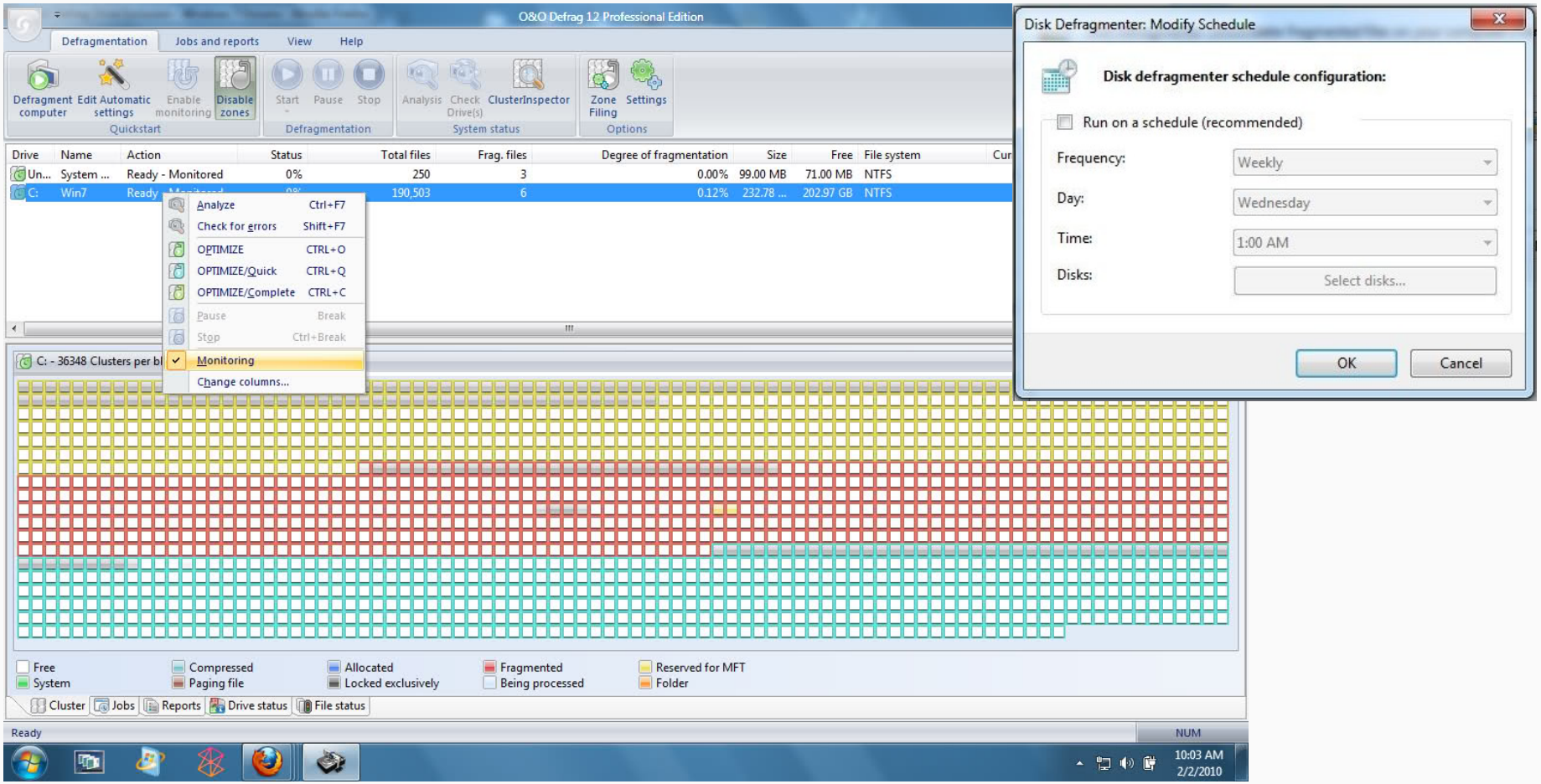
```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
[thorsten@localhost ~]$ strings --radix=d Extr_Slack-Blocks.dls > text.strings
```

In Principle, one can do this with the whole hd, just leave out dls ...

Forensic Data Recovery: other

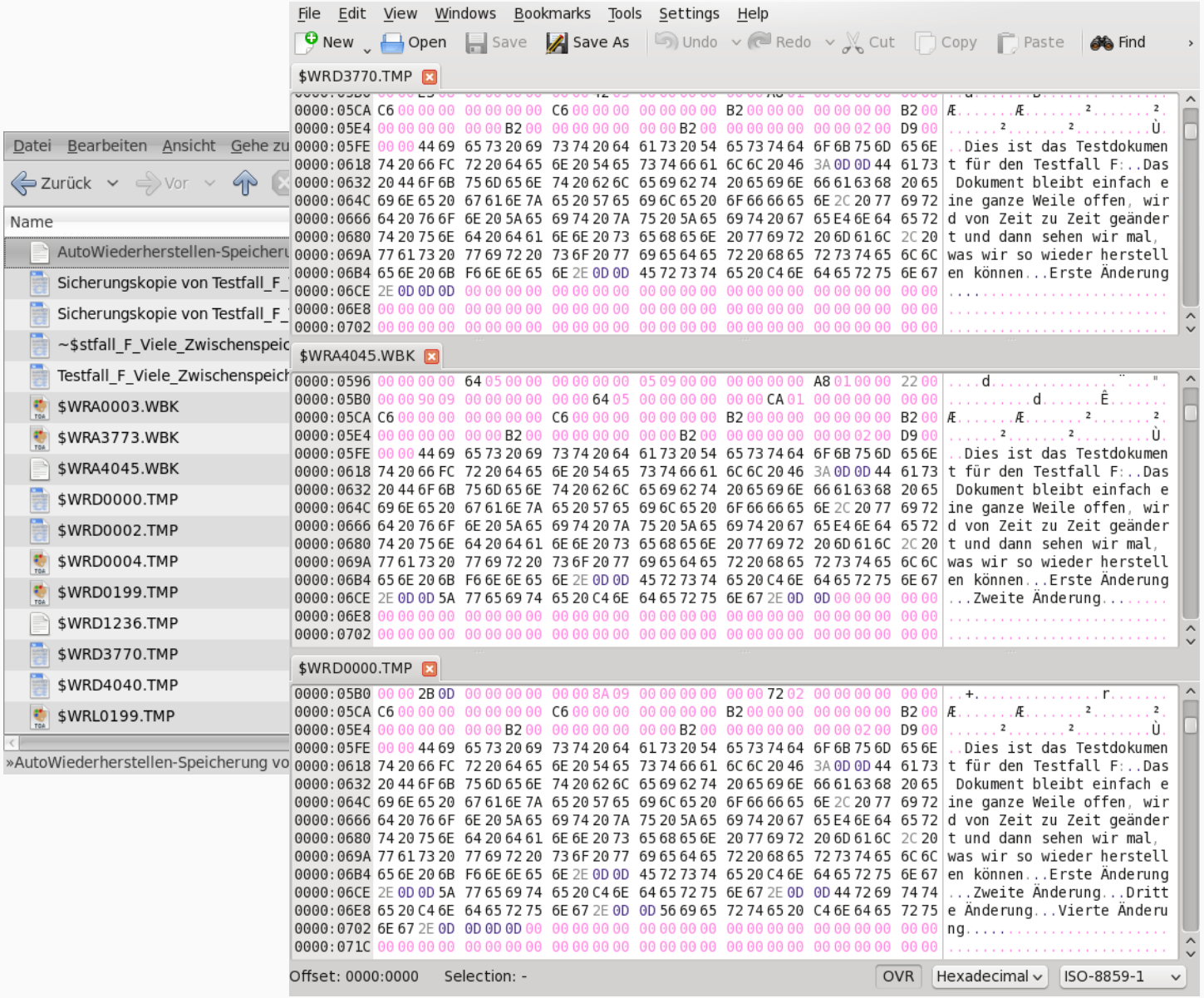
- System crashes as source (e.g. .CHK)
- Registry / Logs – Autopsy timeline feature
- Dropbox cache / deleted items / account data / recoverable sync data (Dropbox Reader, Dropbox Decryptor)
- Browser cache
- Desktop trash folder

Auto-defragmentation



Win7 autodefragmentation feature

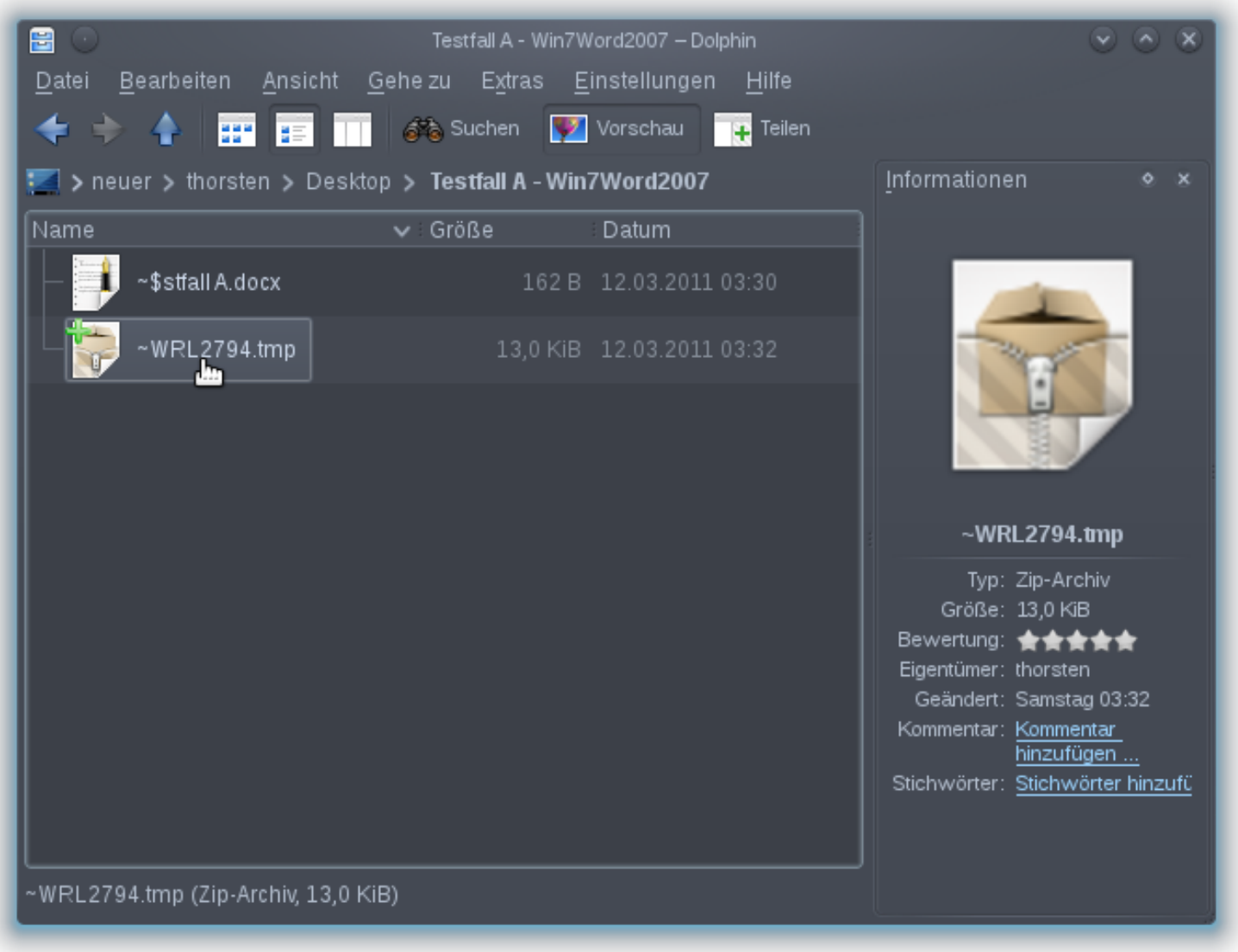
File Structures: fastsave feature



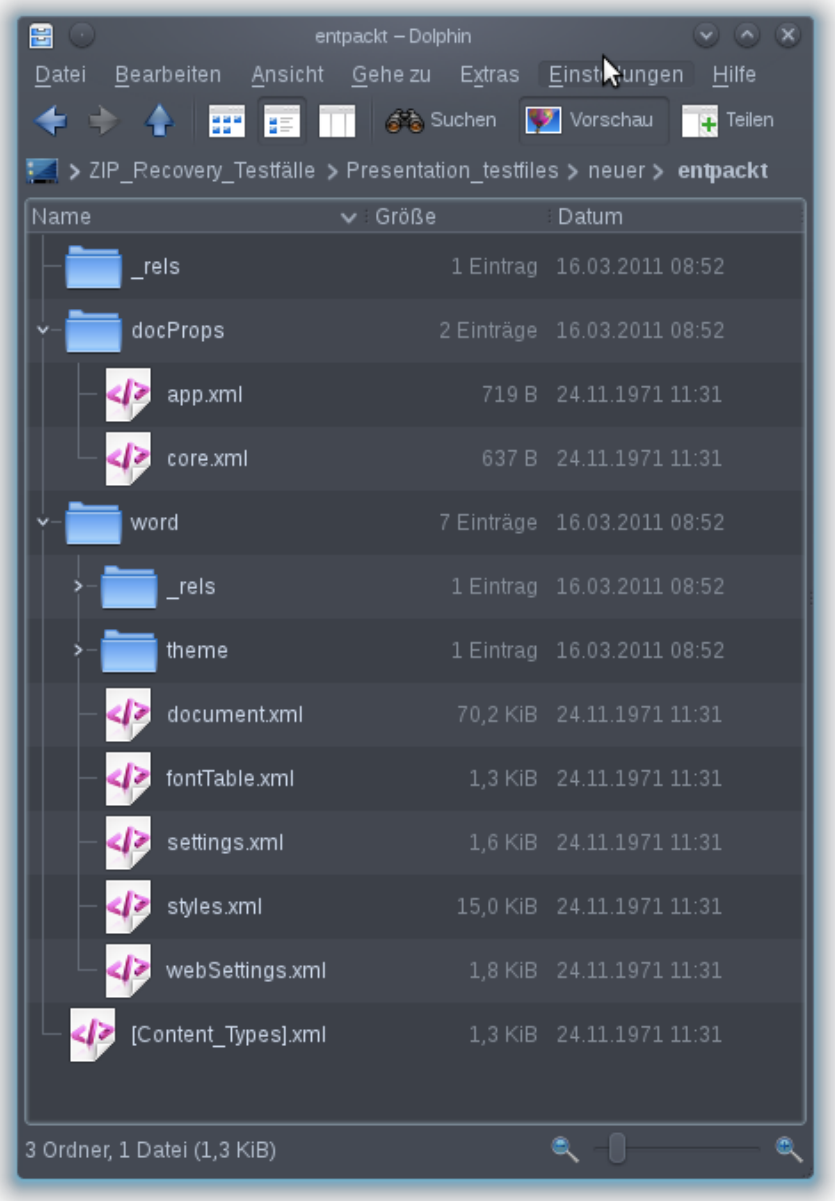
File Structures: .docx and .odt documents

- XML--based markup
- ZIP--compressed container
  - Less often overwritten, corrupted (Garfinkel)
  - Needs special carving algorithms, still under development, some cases not covered yet (e.g. ”∼WRL[xxx].TMPfiles); promising approaches: SMART and use of CRC32 checksums
  - .docx: temporary files also ZIP--compressed XML--files
  - Content cannot be extracted with command »strings«

File Structures: .docx



File Structures: .docx



File Structures: .docx

document.xml – KWrite

Datei Bearbeiten Ansicht Extras Einstellungen Hilfe

Neu Öffnen Speichern Speichern unter Schließen Rückgängig Wiederherstellen


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:ve="http://schemas.openxmlformats.org/markup-compatibility/2006"
xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-
microsoft-com:vml"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
xmlns:w10="urn:schemas-microsoft-com:office:word"
xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml"><w:body><w:p
w:rsidR="004858F7" w:rsidRDefault="00F61330"><w:r><w:t>Dies ist Testfall A. Ein Dokument, das
mehrere Stunden lang offen bleibt. Und groß genug ist, um gewisse Speicheranforderungen zu
stellen. Daher gibt es hier auch ein paar Blindtexte:</w:t></w:r></w:p><w:p w:rsidR="00F61330"
w:rsidRDefault="00F61330"/><w:p w:rsidR="00F61330" w:rsidRDefault="00F61330"
w:rsidP="00F61330"><w:pPr><w:pStyle w:val="StandardWeb"/><w:rPr><w:rFonts w:ascii="Verdana"
w:hAnsi="Verdana"/><w:sz w:val="13"/><w:szCs w:val="13"/></w:rPr></w:pPr><w:r
w:rsidRPr="00F61330"><w:rPr><w:rFonts w:ascii="Verdana" w:hAnsi="Verdana"/><w:sz
w:val="13"/><w:szCs w:val="13"/><w:lang w:val="en-US"/></w:rPr><w:t xml:space="preserve">Sed
ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium,
totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae
vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit
aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt.
Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit,
sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat
voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit
laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit
qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum
```


Zeile: 1 Spalte: 1 EINF ZEILE XML document.xml

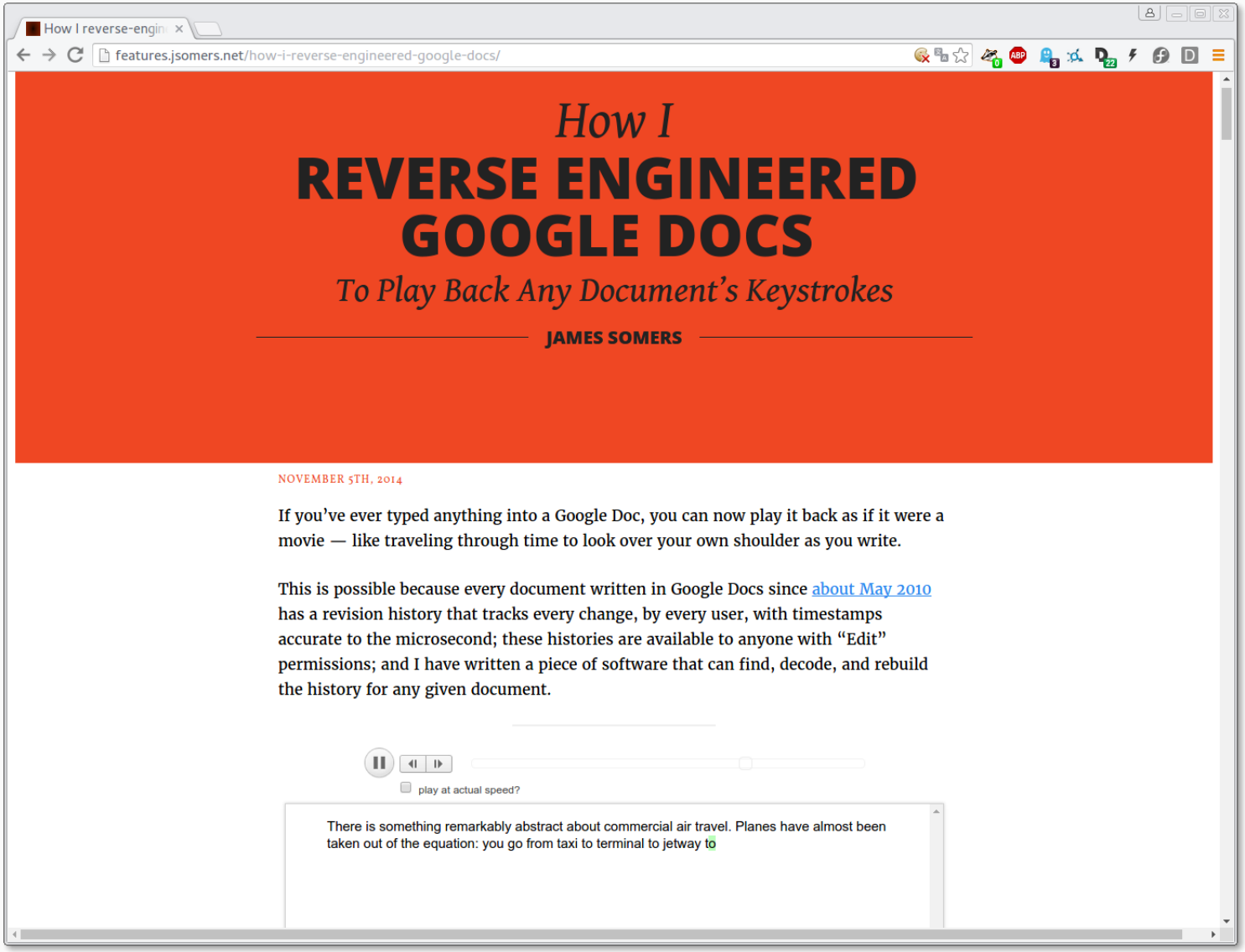
File Structures: RSID-tags in .docx

```
<w:body>
    <w:p w:rsidR="00DF326F"w:rsidRDefault="00BB246B»
        <w:r><w:t>This is a</w:t></w:r>
        <w:r w:rsidR="00007AD8»<w:t>recently altered</w:t></w:r>
        <w:r><w:t>paragraph.</w:t></w:r>
    </w:p>
    <w:p w:rsidR="00BB246B"w:rsidRDefault="00BB246B»
        <w:r><w:t>In a second</w:t></w:r>
        <w:r w:rsidR="00007AD8»<w:t>, even more recently rewritten</w:t></w:r>
        <w:r><w:t>paragraph there was</w:t></w:r>
        <w:r w:rsidR="00EB7E8F»<w:t>– surprise! –</w:t></w:r>
        <w:r><w:t>a second rewrite almost at the same time as the
            change in the first paragraph, as the identical RSID-Tag-No.00007AD8
            indicates.</w:t></w:r>
    </w:p>

</w:body>
```

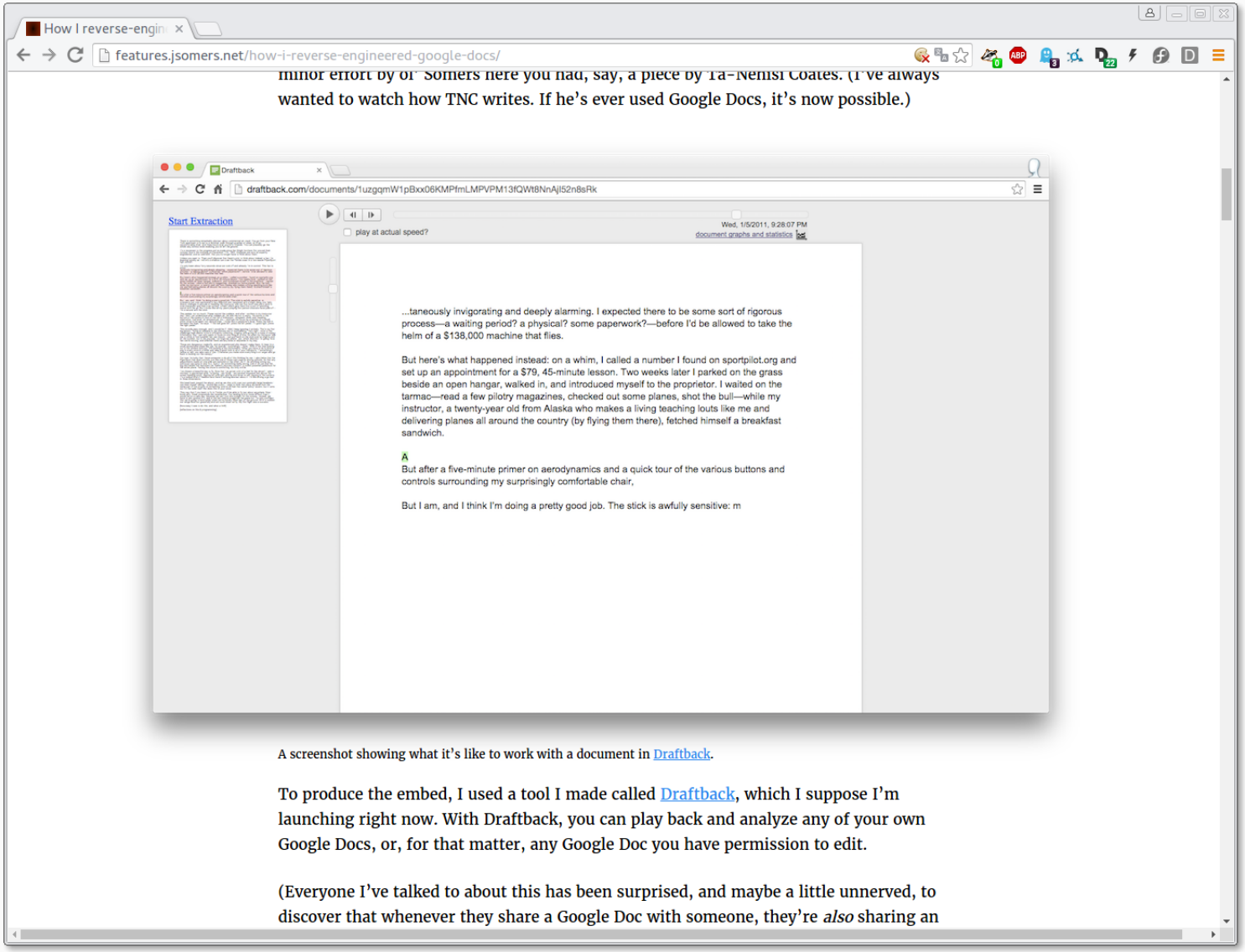

Marked red: the clear text as it appears in the document.Marked green: RSID-Layers.Blue and red: nested edits.

Draftback Plugin for Google Docs



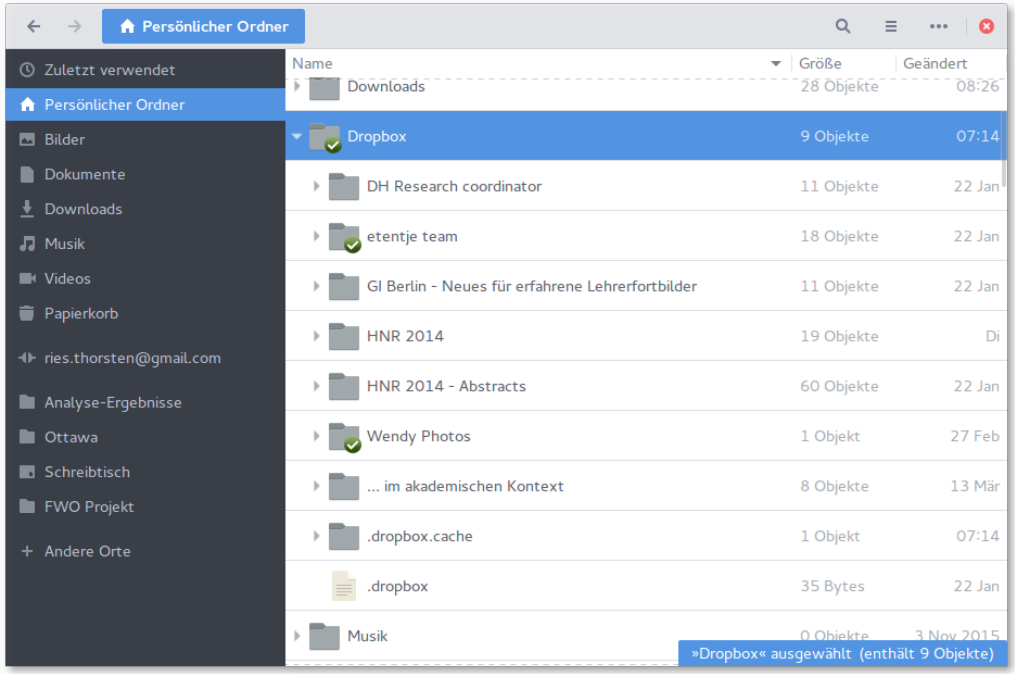
James Somers: http://features.jsomers.net/how-i-reverse-engineered-google-docs/

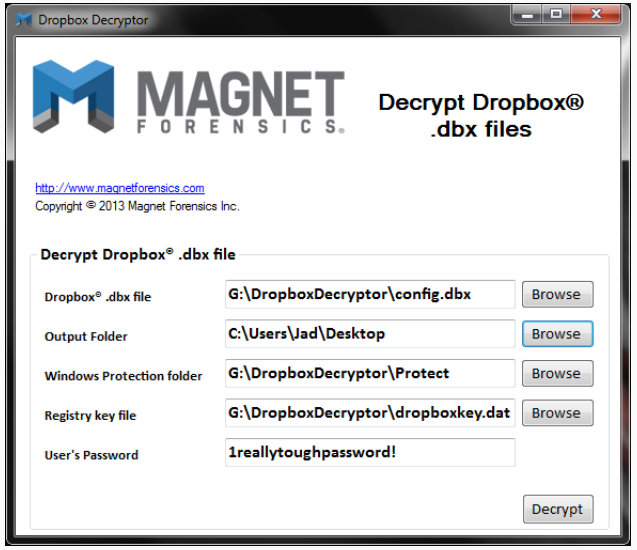
Cloud Forensics: Draftback Plugin for Google Docs



James Somers: http://features.jsomers.net/how-i-reverse-engineered-google-docs/

Cloud Forensics: Dropbox, Dropbox Decryptor





Discussion:
The Born Digital Record and the DSE

What is the »materiality« of the born digital record?

- ›Material‹ vs. ›immaterial‹
- Forensic vs. formal materiality
- Concepts of evidence / materiality, the ›document‹
  - »distributed materiality« (J.-F. Blanchette, 2011)
  - »relational materiality« (Estrid Sørensen, 2009)
  - »performative materiality« (Johanna Drucker, 2013)
  - »every access constitutes a distinct instance of the file«, »Access is thus duplication, duplication is preservation, and preservation is creation — and recreation.« (M. Kirschenbaum, 2013)
  - »in effect, a disk image or bitstream virtualizes the archive by yielding a legally and mathematically identical simulacrum.«, »The e-palaeographer works with simulations of simulations, archives of archives … self identical and not, both at the same time.« (M. Kirschenbaum, 2016)
- Aspects of media achaeology, software studies, critical code studies

Interdependent layers: distributed materiality

> Jean-François Blanchette, whose work I first encountered in 2008, draws on a very different disciplinary background for his criticism of ”immateriality.”[...] he was extending the study of digital materiality to the analysis of elaborate systems and their interdependent modular components. By adding the concept of distributed materiality to our inventory, he provides language to describe the co-dependent, layered contingencies on which the functions of drive, storage, software, hardware, systems, and networks depend. Not only are all of these elements material, but they are locked into relations with each other that are governed by their material design and constraints in ways that have an effect on the costs and efficient operation of the system.

Johanna Drucker: Performative Materiality and Theoretical Approaches to Interface, dhq 2013. 7.1. par. 6.

».txtual condition« of the Document / Trace

> One can, in a very literal sense, never access the ‘same’ electronic file twice, since each and every access constitutes a distinct instance of the file that will be addressed and stored in a unique location in computer memory. [...] each access engenders a new logical entity that is forensically individuated at the level of its physical representation on some storage medium. Access is thus duplication, duplication is preservation, and preservation is creation — and recreation. That is the catechism of the .txtual condition [...]

Matthew Kirschenbaum: The .txtual Condition: Digital Humanities, Born-Digital Archives, and the Future Literary, dhq 2013. 7.1. par. 16.

M. Kirschenbaum: Kislak lectures

> ’A primary record’, the MLA told us in 1995, ’can appropriately be defined as a physical object produced or used at a perticular past time that one was concerned with in a given instance.’[...] But in that aspact the MLA was only addressing half the issue. Today the conceipt of a primary record can no longer be assumed to be coterminus with that of a physical object. Electronic texts, files, feeds and transmissions of all sorts are also indisputably primary records.
>
> But this also means that this data is fundamentally unstable in the sense that they rest upon the foundations of other data, what is quite literally in the trade known as metadata, in order to be legible under the appropriate computational regiments, which I have previously termed as formal materiality in my own work.

Matthew Kirschenbaum: The Kislak lectures, March 2016

M. Kirschenbaum: Kislak lectures

[...] in effect, a disk image or bitstream virtualizes the archive by yielding a legally and mathematically identical simulacrum.

[...] Robert J Morris predicted 'within the next 10 years,a small and elite band of e-palaeographers will emerge who will recover data signal by signal.

The e-palaeographer works with simulations of simulations, archives of archives ... self identical and not, both at the same time.

Matthew Kirschenbaum: The Kislak lectures, March 2016

M. Kirschenbaum: Kislak lectures

> [...] not that I do not mean to suggest that media are now immaterial, quite the contrary, but it does mean that as I argued in Mechanisms, that in order to fully apprehend the import of the digital medium, we must acknowledge that its technology have been designed and engineered through excruciatingly precice tolerances that often brazenly exploit the physical properties of phenomena right up to the limits of their molecular integrity to create and sustain what I like to call an illusion or a working model of immateriality.

Matthew Kirschenbaum: The Kislak lectures, March 2016

Fred Cohen: C-Traces vs. O-Traces

Constructed trace A trace constructed from a reconstruction process. [C-trace]

Original trace A trace produced from evidence in the matter. [O-trace]

Fred Cohen: Putting the Science in Digital Forensics, Journal of Digital Forensics, Security and Law, Vol. 6(1) 2011, p. 10.

The science

- Digital traces have to be documented and evaluated, according to their context and to their method of recovery (Cohen) and also fragments have to be hashed (Garfinkel)
- Scientific testing of recovery, analytical methods, algorithms with forensic corpora to satisfy the Daubert principle (Garfinkel) – (especially important for file carving)

Discussion

How to represent the genetic born digital record?

- Hashes! (also fragments (Garfinkel)? or better offset?)
- Snapshot character
- How to represent fragments in a meaningful way?
- Commentary bridging the gap towards historical, distributed / relational materiality?
- Documentation also of recovery tools and versions? C-trace problem to be addressed in the commentary?

Thank you for your attention!

Special thanks goes to:
Christian Moch (Forensig 2.0)

GHENT UNIVERSITY

fwo