

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



Introduction

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)

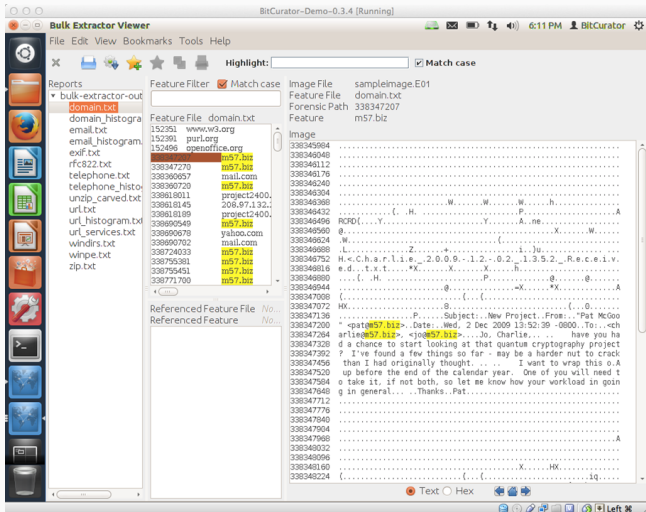
- Introduction (15 min)
- Forensic Imaging, Analysis and Recovery Tools (45 min)
 - Forensic imaging
 - Forensic System Analysis: Sleuthkit, Autopsy
 - File and data recovery (file undelete, carving, drive slack analysis, fragmented files, system restore points, other)
 - File structures (Fatsave, RSID)
 - 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)



The screenshot shows the BitCurator application window with the GUYMAGER interface. The interface includes a menu bar (Devices, Misc, Help), a toolbar (Rescan), and a table of detected storage devices. The table has columns for Serial no., Linux device, Model, State, Size, Hidden Areas, Bad sectors, and Progress. Two devices are listed: a VBOX VBOX CD-ROM and an ATA VBOX HARDISK. A context menu is open over the first device, with 'Acquire image' circled in red. Below the table, a status bar displays various metrics such as Size, Sector size, Image file, Info file, Current speed, Started, Hash calculation, Source verification, and Image verification.

Serial no.	Linux device	Model	State	Size	Hidden Areas	Bad sectors	Progress
VB2-01790376	/dev/rb	VBOX VBOX CD-ROM	● Idle	154.6MB	unknown		
VB19f64265-78d31aa4	/dev/sda	ATA VBOX HARDISK	○ Idle	137.4GB	unknown		

Size: 154,636,288 bytes (147MB / 155MB)
Sector size: 2,048
Image file:
Info file:
Current speed:
Started:
Hash calculation:
Source verification:
Image verification:



The screenshot shows a web browser window titled "Forensig 2.0 - Opera" with the address bar displaying "www.forensig.de/scriptmanager/". The page header includes navigation links for "Home", "Generator", "Manual", "Theory", a user profile "beta@tester.de", and a "Logout" button. The main content area is titled "Scriptmanager" and features two buttons: "Upload new script" and "Create empty Script". Below these is a table listing scripts with columns for ID, Name, Validity, Errors, and Status.

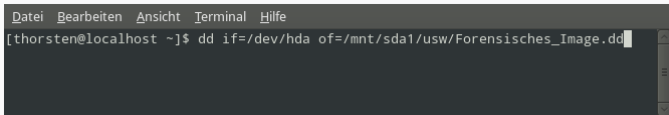
	#	Name	Valid	Errors	Status
delete edit	244	ossimple	True		▶ run script
delete edit	245	oscomplex	True		▶ run script
delete edit	246	android	True		▶ run script
delete edit	247	fatsimple	True		▶ run script
delete edit	248	fatcomplex	True		▶ run script
delete edit	251	android2	True		▶ run script
delete 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](#)

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

A terminal window with a dark background and light text. The menu bar at the top contains 'Datei', 'Bearbeiten', 'Ansicht', 'Terminal', and 'Hilfe'. The command prompt shows the user 'thorsten@localhost' in the directory '~'. The command entered is 'dd if=/dev/hda of=/mnt/sda1/usw/Forensisches_Image.dd'.

```
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)

The screenshot displays the Guymager application window. The interface includes a menu bar with 'Devices', 'Misc', and 'Help'. Below the menu is a 'Rescan' button. The main area contains a table with the following data:

Serial no.	Linux device	Model	State	Size	Hidden Areas	Bad sectors	Progress
VB2-01790376	/devr0	VBOX VBOX CD-ROM	<input checked="" type="radio"/> Idle	154.6MB	unknown		
VB19f64265-78d31aa4	/devvda	ATA VBOX HARDISK	<input type="radio"/> Idle	137.4GB	unknown		

A context menu is open over the second device, with the following options: 'Acquire image', 'Clone device', 'Abort', and 'Info'. The 'Acquire image' option is circled in red. Below the table, there is a section for device details:

Size: 134,636,288 bytes (147MB / 155MB)
Sector size: 2,048
Image file:
Info file:
Current speed:
Started:
Hash calculation:
Source verification:
Image verification:

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

System Analysis: Sleuthkit

The screenshot shows the Sleuthkit application interface. The top menu bar includes FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. The main window is divided into several sections:

- Searching for ASCII:** Done. Saving: Done. 1 hits. [Link to results](#)
- Searching for Unicode:** Done. Saving: Done. 0 hits. [New Search](#)
- 1 occurrence of password was found:** Search Options: ASCII, Case Sensitive. Sector 39 ([Hex](#) - [Ascii](#)). 1:330 (same password that)
- password was not found:** Search Options: Unicode, Case Sensitive.

Navigation buttons include PREVIOUS, NEXT, EXPORT CONTENTS, and ADD NOTE. The current view is ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report). File Type: Non-ISO extended-ASCII English text, with CR line terminators.

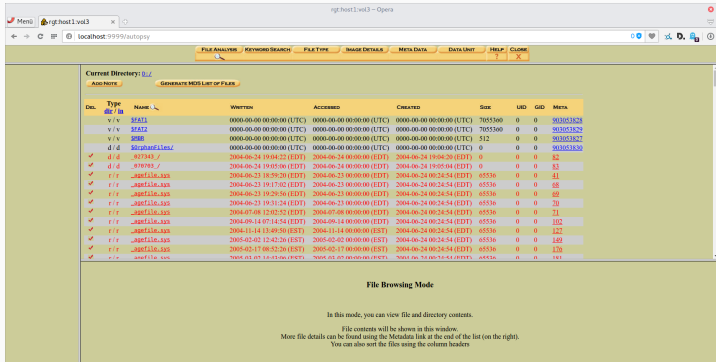
The hex view shows the contents of Sector 39 in scan24.dd-0-0. The hex data is displayed in columns, with the corresponding ASCII characters shown to the right. The text in the hex view is:

```
0  6e746565 64207061 79636985 636b2e20  ntee d pa yche ck.
16 54695659 72207061 72656474 73206769  The l r pa rent s gi
32 79552074 68656d20 665f6a55 79206661  ve t hea sone y fo
48 72206c75 6e636820 616e6420 74686579  r lu nch and they
64 20737065 6e642069 74206f6e 206d7920  spe nd i t on ay
80 73747566 662e2049 626a2061 6e206566  stuff f. I a a n en
96 74720570 72656a55 73722e20 416d2049  treg rene ur. Ae I
112 206f6e6c 79206f6e 6520796f 75207365  onl y on e yo u se
128 6c6c2074 6f3f204d 61796265 20462063  ll t o? M aybe I c
144 616e2062 65636f6d 65206a69 73747269  an b ecom e di stri
160 6275746f 72206f6e 20746865 20796561  buto r of the yea
176 72210d0d 4920656d 61696c65 6420796f  ri.. I ee aile d yo
192 75207468 65207363 68656475 6c652074  u th e sc hedu le t
208 68617420 4920616d 20737969 6e672e20  hat I an usi ng.
224 49207468 696e6b20 69742068 656c7073  I th ink it h e lps
240 20666520 636f7865 72206479 73656c66  me covr r my self
256 20616e64 206e6f74 20626520 70726564  and not be pred
272 69637469 76652e20 2094656c 6c206d65  iccti ve. Tel l me
288 20776961 7420796f 75207468 696e6b2e  what t yo u th ink.
304 20546f20 6f70656e 2069742c 20757365  To open it, use
320 20746865 2073616d 65207061 7373776f  the sae e pa ssw
336 72642074 68617420 796f7520 73656e74  rd t hat yo sent
352 20666520 6265666f 72652077 69746820  me befo re w ith
368 74686174 2066696c 652e2054 616c6b20  that fil e. T alk
384 748f2079 6f75206c 61746572 2e0d0d54  to yo u l ater ...T
400 68616e68 73c00d0d 48f6520 0d000000  hank s... Joe ....
416 00000000 00000000 00000000 00000000  ....
432 00000000 00000000 00000000 00000000  ....
448 00000000 00000000 00000000 00000000  ....
464 00000000 00000000 00000000 00000000  ....
480 00000000 00000000 00000000 00000000  ....
496 00000000 00000000 00000000 00000000  ....
```

www.securitygarden.com

Sleuthkit (hex view)

System Analysis: Autopsy Browser (Linux)



The screenshot shows the Autopsy web interface in 'File Browsing Mode'. The browser address bar shows 'localhost:9999/autopsy'. The interface includes a navigation menu with options like 'FILE ANALYSER', 'KEYWORD SEARCH', 'FILE TYPE', 'IMAGE DETAILS', 'META DATA', 'DATA LIST', 'HELP', and 'CLOSE'. Below the menu, the 'Current Directory' is set to '/'. A 'GENERATE META LIST OF FILES' button is visible. The main area displays a table of files and directories with columns for 'Del.', 'Type', 'Name', 'Written', 'Accessed', 'Created', 'Size', 'UID', 'GID', and 'Meta'. The table lists various files, including directories like '32bit', '386', and 'SdghasFiles', and files named '32743_7', '376793_7', and several 'agfFile_333' files. Each row has a checkbox in the 'Del.' column and a metadata link at the end.

Del.	Type	Name	WRITTEN	ACCESSED	CREATED	Size	UID	GID	Meta
	v / v	32bit	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	7055360	0	0	903053828
	v / v	32bit2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	7055360	0	0	903053829
	v / v	386	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	903053830
	d / d	SdghasFiles	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	903053830
<input checked="" type="checkbox"/>	d / d	32743_7	2004-06-24 19:04:22 (EDT)	2004-06-24 00:00:00 (EDT)	2004-06-24 19:04:20 (EDT)	0	0	0	82
<input checked="" type="checkbox"/>	d / d	376793_7	2004-06-24 19:05:06 (EDT)	2004-06-24 00:00:00 (EDT)	2004-06-24 19:05:04 (EDT)	0	0	0	83
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-06-23 18:59:20 (EDT)	2004-06-23 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	81
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-06-23 19:17:02 (EDT)	2004-06-23 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	88
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-06-23 19:29:56 (EDT)	2004-06-23 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	89
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-06-23 19:31:54 (EDT)	2004-06-23 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	20
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-07-08 12:02:52 (EDT)	2004-07-08 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	21
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-09-14 07:14:54 (EDT)	2004-09-14 00:00:00 (EDT)	2004-06-24 00:24:54 (EDT)	65536	0	0	102
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2004-11-14 13:49:50 (EST)	2004-11-14 00:00:00 (EST)	2004-06-24 00:24:54 (EDT)	65536	0	0	122
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2005-02-02 12:02:26 (EST)	2005-02-02 00:00:00 (EST)	2004-06-24 00:24:54 (EDT)	65536	0	0	180
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2005-02-17 06:52:36 (EST)	2005-02-17 00:00:00 (EST)	2004-06-24 00:24:54 (EDT)	65536	0	0	170
<input checked="" type="checkbox"/>	f / f	_agfFile_333	2005-03-07 18:43:06 (EST)	2005-03-07 00:00:00 (EST)	2004-06-24 00:24:54 (EDT)	65536	0	0	161

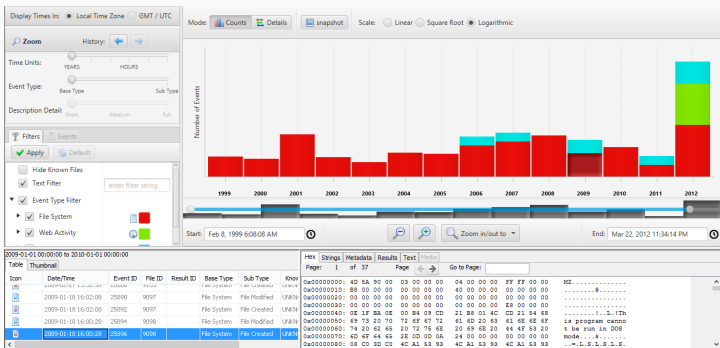
File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Autopsy, Orphaned File View

System Analysis: Autopsy Browser



Autopsy: timeline

System Analysis: Autopsy Browser

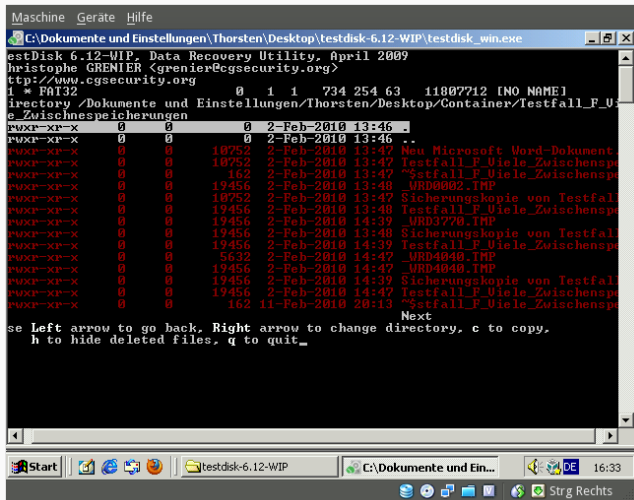
The screenshot displays the Autopsy Browser interface. The top section includes a navigation bar with 'Counts' and 'Details' tabs, a 'snapshot' button, and layout options like 'Band by Type' and 'One Event Per Row'. A zoom control is also present. The main area is a timeline view showing a sequence of events from March 10, 2012, to March 11, 2012. The timeline is divided into hourly segments. Several events are highlighted with colored boxes and labels, such as 'img_xp-sp3-v3.001\vol2\Documents and Settings (432)', 'img_xp-sp3-v3.001_wml2\WINDOWS (78)', 'img_xp-sp3-v3.001\vol2\Documents and Settings (1576)', 'C:\Documents and Settings\John (5)', 'C:\Documents and Settings\John\My Documents (6)', 'img_xp-sp3-v3.001\vol2\Program Files (133)', and 'doubleclick.net (1)'. The bottom section features a table with columns for 'Icon', 'Date/Time', 'Event ID', 'File ID', 'Result ID', 'Base Type', 'Sub-Type', 'Known', and 'Desc'. The table contains several rows of data, with the second row highlighted in blue. The table data is as follows:

Icon	Date/Time	Event ID	File ID	Result ID	Base Type	Sub-Type	Known	Desc
	2012-03-10 19:19:23	39681	13409		File System	File Accessed	K3N76M	Ang...
	2012-03-10 19:23:09	44359	14758		File System	File Accessed	K3N76M	Ang...
	2012-03-10 19:23:05	57347	18438		File System	File Changed	K3N76M	Ang...
	2012-03-10 19:23:07	44165	14720		File System	File Accessed	K3N76M	Ang...
	2012-03-10 19:23:06	44165	14721		File System	File Accessed	K3N76M	Ang...

Autopsy: timeline

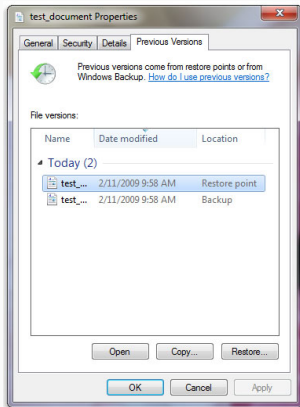
- never (really immediately) deleted
- if deleted, partially recoverable through undelete, carving etc. (if not overwritten, redundancy!)
- system-specific: restore points, backup data
- file structure.

Forensic Data Recovery: Undelete



TestDisk undelete operation

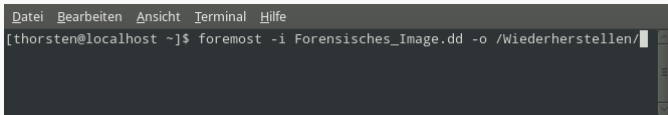
Forensic Data Recovery: restore points



Mac Time Machine

Win7 Virtual Snapshot Service restore

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

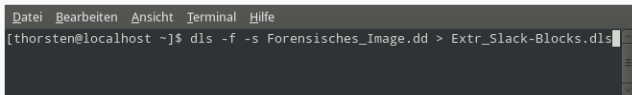
A terminal window with a dark background and light text. The title bar at the top reads "Datei Bearbeiten Ansicht Terminal Hilfe". The command prompt shows the user "thorsten@localhost" in the directory "~". The command entered is "foremost -i Forensisches_Image.dd -o /Wiederherstellen/". The cursor is at the end of the command line.

```
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, Photorec, 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.

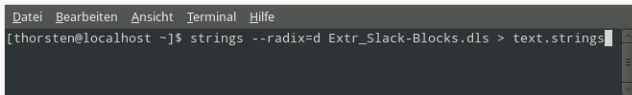
Forensic Data Recovery: drive slack, raw image inspect

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 ...

- 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

The screenshot displays the O&O Defrag 12 Professional Edition software interface. The main window shows a table of drives and their defragmentation status. A context menu is open over the 'C:' drive, with 'Monitoring' selected. A 'Disk Defragmenter: Modify Schedule' dialog box is overlaid on the right side of the screen.

Drive	Name	Action	Status	Total files	Frag. files	Degree of fragmentation	Size	Free	File system
Un...	System ...	Ready - Monitored	0%	250	3	0.00%	99.00 MB	71.00 MB	NTFS
C:	Win7	Ready		190,903	6	0.12%	232.76 ...	202.97 GB	NTFS

Disk Defragmenter: Modify Schedule

Run on a schedule (recommended)

Frequency: Weekly

Day: Wednesday

Time: 1:00 AM

Disks: Select disks...

OK Cancel

Win7 autodefragmentation feature

- 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

The screenshot shows the Dolphin file manager window titled "Testfall A - Win7Word2007 - Dolphin". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Gehe zu", "Extras", "Einstellungen", and "Hilfe". The toolbar contains navigation icons and buttons for "Suchen", "Vorschau", and "Teilen". The breadcrumb path is "neuer > thorsten > Desktop > Testfall A - Win7Word2007".

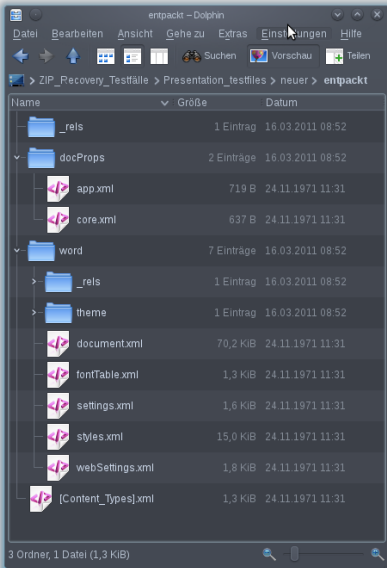
Name	Größe	Datum
~\$tfall A.docx	162 B	12.03.2011 03:30
~WRL2794.tmp	13,0 KiB	12.03.2011 03:32

The information panel on the right, titled "Informationen", shows a preview of a zip archive icon. Below the icon, the file name is "~WRL2794.tmp". The details listed are:

- Typ: Zip-Archiv
- Größe: 13,0 KiB
- Bewertung: ★★★★★
- Eigentümer: thorsten
- Geändert: Samstag 03:32
- Kommentar: [Kommentar hinzufügen ...](#)
- Stichwörter: [Stichwörter hinzufügen](#)

At the bottom of the window, a status bar indicates: "~WRL2794.tmp (Zip-Archiv, 13,0 KiB)".

File Structures: .docx



File Structures: .docx

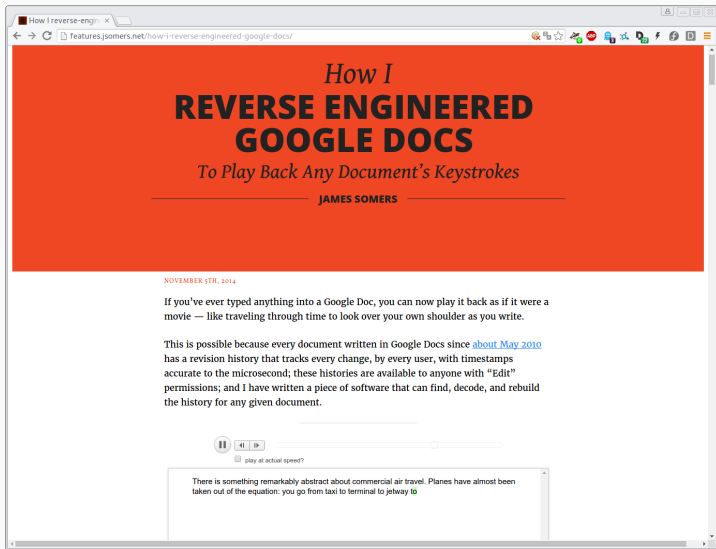
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:ve="http://schemas.openxmlformats.org/wordprocessingcompatibility/2006"
xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" 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="004800F7" 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="Standard" /><w:rPr><w:rFonts w:ascii="Verdana"
w:hAnsi="Verdana" /><w:sz w:val="12" /><w:szCs w:val="12" /></w:rPr></w:pPr><w:r
w:rsidRPr="00F61330"><w:rPr><w:rFonts w:ascii="Verdana" w:hAnsi="Verdana" /><w:sz
w:val="12" /><w:szCs w:val="12" /><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>
```

Draftback Plugin for Google Docs



The screenshot shows a web browser window with the address bar containing "Features.jsomers.net/how-i-reverse-engineered-google-docs/". The page has a large orange header with the title "How I REVERSE ENGINEERED GOOGLE DOCS" and subtitle "To Play Back Any Document's Keystrokes" by JAMES SOMERS. Below the header, the date "NOVEMBER 5TH, 2014" is displayed. The main text explains that Google Docs documents have a revision history that tracks every change, and the author has written software to find, decode, and rebuild this history. A playback interface is visible, including a play button, a progress bar, and a checkbox labeled "play at actual speed?". A text box at the bottom contains the sentence: "There is something remarkably abstract about commercial air travel. Planes have almost been taken out of the equation: you go from taxi to terminal to jetway to".

How I
**REVERSE ENGINEERED
GOOGLE DOCS**
To Play Back Any Document's Keystrokes
JAMES SOMERS

NOVEMBER 5TH, 2014

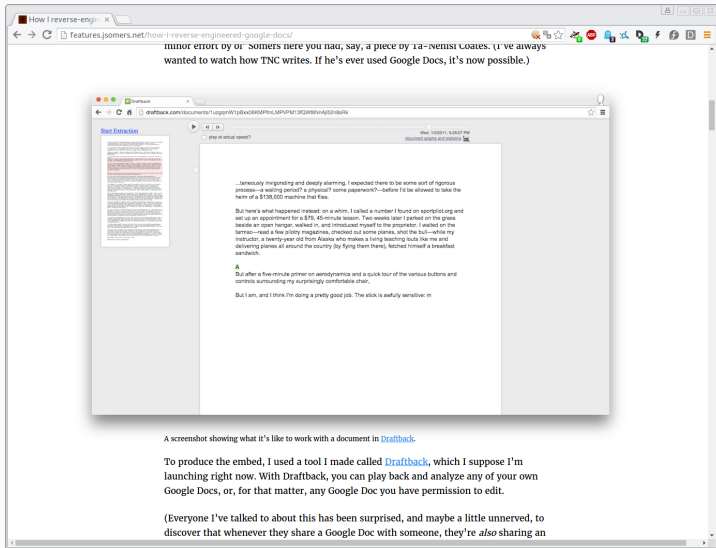
If you've ever typed anything into a Google Doc, you can now play it back as if it were a movie — like traveling through time to look over your own shoulder as you write.

This is possible because every document written in Google Docs since [about May 2010](#) has a revision history that tracks every change, by every user, with timestamps accurate to the microsecond; these histories are available to anyone with "Edit" permissions; and I have written a piece of software that can find, decode, and rebuild the history for any given document.

play at actual speed?

There is something remarkably abstract about commercial air travel. Planes have almost been taken out of the equation: you go from taxi to terminal to jetway to

Cloud Forensics: Draftback Plugin for Google Docs



minor error by or somers here you nau, say, a piece of 1a-ismist Coates. (I've always wanted to watch how TNC writes. If he's ever used Google Docs, it's now possible.)

Start Extraction

play actual video?

Mon, 10/20/11, 8:28:17 PM
DOCUMENT GENERATED BY DRAFTBACK

...intensely imagining and deeply alarming, I expected there to be some sort of rigorous process—a waiting period? a physical? some paperwork?—before I'd be allowed to take the helm of a \$138,000 machine that flies.

But here's what happened instead: on a whim, I called a number I found on sportplot.org and set up an appointment for a \$79, 45-minute lesson. Two weeks later I parked on the grass beside an open hangar, walked in, and introduced myself to the proprietor. I walked on the tarmac—read a few pilot magazines, checked out some planes, shot the bull—while my instructor, a twenty-year old from Alaska who makes a living teaching kids like me and delivering planes all around the country (by flying them there), fetched himself a breakfast sandwich.

A

But after a five-minute primer on aerodynamics and a quick tour of the various buttons and controls surrounding my surprisingly comfortable chair,

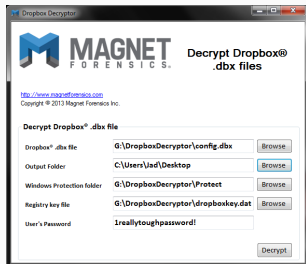
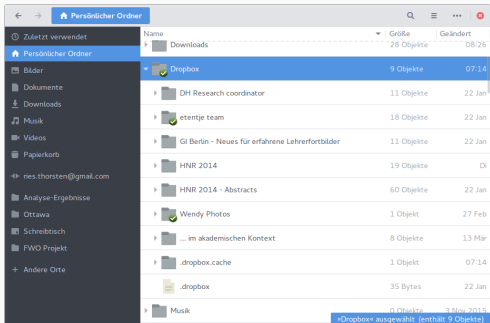
But I am, and I think I'm doing a pretty good job. The stick is awfully sensitive: m

A screenshot showing what it's like to work with a document in [Draftback](#).

To produce the embed, I used a tool I made called [Draftback](#), which I suppose I'm launching right now. With Draftback, you can play back and analyze any of your own Google Docs, or, for that matter, any Google Doc you have permission to edit.

(Everyone I've talked to about this has been surprised, and maybe a little unnerved, to discover that whenever they share a Google Doc with someone, they're *also* sharing an

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 archaeology, 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.

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.

'A primary record', the MLA told us in 1995, 'can appropriately be defined as a physical object produced or used at a particular past time that one was concerned with in a given instance.'[...] But in that aspect the MLA was only addressing half the issue. Today the concept of a primary record can no longer be assumed to be coterminous 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

[...] 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.

[...] 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 precise 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

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.

- 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)

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)

