
OpenSource Forensik-Werkzeuge

Dipl.-Ing. Mathias Gärtner

Sachverständigenbüro Prof. Pausch & Partner
Heinheimer Strasse 38

D-64289 Darmstadt

Tel.: +49 6151 9712640

Fax.: +49 6151 9712641

Email: Mathias.Gaertner@it-svbuero.de
<http://www.it-svbuero.de>



- Was ist Computer-Forensik
- Closed-Source Systeme und deren Vor- und Nachteile
- Open-Source Systeme und deren Vor- und Nachteile

- Zusammenfassung
- Fazit

Was ist Computerforensik (I)

- Erlangen von Informationen über das Nutzerverhalten sowie gespeicherte Nutzerdaten entweder
 - Online oder
 - Offline
- Unterschied zum Hacking:
 - Legitimer Eigentümer/Besitzer ist Auftraggeber
 - Strafverfolgung



Tätigkeitsfelder der Computerforensik (II)

- Strafverfolgung: *Was hat wer wann was und wie oft getan?*
(meistens Offline, aber...)
- Strafprävention: *Was macht wer gerade?*
(Stichwort: Bundestrojaner)
- Industriespionage: *Wer „klaut“ Daten?*
- Kontrolle: *Wer macht was, bzw. macht jemand was unerlaubtes?*



- Beweise/Spuren sichern ohne zu verändern, soweit das möglich ist
- Neutralität wahren
- Nachvollziehbar „Beweise“ zusammenstellen

- Keine illegalen Aktivitäten ausschließen
-> Beweis sonst ggf. unverwertbar

Closed-Source Programme

- Kommerziell erhältliche Programme mit einem durch den Anwender nicht, oder schwer veränderbaren Datenakquisitions-, Auswerte- und Präsentationsumfang
- In der Regel als „One-Shop“ System entwickelt
- Gebräuchlichste Systeme
 - Encase
 - iLook
 - Xways
 - Undelete-Software
 - (perkeo)



Forensic-Werkzeuge (Beispiel)

Evidence 0 (Set up new evidence items in the evidence management screen)

Device 29,2933Gb, Used 29,2933Gb

Partition (0) - Type NTFS, Size (29,2933Gb)

Files

- \$Extend
- ATI
- Config Msi
- Dokumente und Einstellungen
- ILook Unchained Object Recovery
- ILook Virtual Folders
 - Currently Eliminated Files
 - Currently Tagged Files
 - Currently Tagged Sectors
- ILook Categories
 - Compressed_Archives
 - Database
 - Encrypted_Volumes
 - Graphics
 - And_More (*.pic,*.psd,*.raw,*.rie,*.tga,*.tif,*.wpg)
 - AOL (*.art)
 - GIF (*.gif)
 - JPG (*.jpg,*.jpeg)
 - More (*.jif,*.cdr,*.dib,*.img,*.mac,*.msg,*.pcm,*.pcd)
 - Others (*.png,*.pcx,*.bmp,*.ico,*.wmf)
- Internet
- Mail_Boxes
- Movies
- Programming_Files
- SpreadSheets
- System_Files

Name	DOS Name	Type	Size	Created	Last Accessed	Last Modified	MFT Modified	Path
lpp_0002.gif	lpp_0002.gif	GIF-Bild	1518	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
lpp_0003.gif	lpp_0003.gif	GIF-Bild	899	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
lpp_0004.gif	lpp_0004.gif	GIF-Bild	895	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
lpp_0005.gif	lpp_0005.gif	GIF-Bild	255	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
lpp_0012.gif	lpp_0012.gif	GIF-Bild	1265	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
lpp_0015.gif	lpp_0015.gif	GIF-Bild	802	28.02.2006 12:00:00	10.12.2006 14:15:58	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
ntimage.gif	ntimage.gif	GIF-Bild	8794	28.02.2006 12:00:00	10.12.2006 14:16:12	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSsys
tips.gif	tips.gif	GIF-Bild	1045	28.02.2006 12:00:00	10.12.2006 14:16:39	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
bluearrow.gif	BLUEAR~1.GIF	GIF-Bild	166	28.02.2006 12:00:00	10.12.2006 14:18:05	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSWe
bot_bar.gif	bot_bar.gif	GIF-Bild	53	28.02.2006 12:00:00	10.12.2006 14:18:05	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_blank.gif	NAV_BL~1.GIF	GIF-Bild	855	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_best.gif	nav_best.gif	GIF-Bild	1221	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_best_down.gif	NAV_BE~1.GIF	GIF-Bild	1161	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_connected.gif	NAV_CO~1.GIF	GIF-Bild	1211	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_connected_down.gif	NAV_CO~2.GIF	GIF-Bild	1179	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_gray.gif	nav_gray.gif	GIF-Bild	1496	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_safe_easy.gif	NAV_SA~1.GIF	GIF-Bild	1237	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_safe_easy_down.gif	NAV_SA~2.GIF	GIF-Bild	1176	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_start_here.gif	NAV_ST~1.GIF	GIF-Bild	1130	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_start_here_down.gif	NAV_ST~2.GIF	GIF-Bild	761	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_unlock.gif	NAV_UN~1.GIF	GIF-Bild	1237	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
nav_unlock_down.gif	NAV_UN~2.GIF	GIF-Bild	1131	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
spacer.gif	spacer.gif	GIF-Bild	43	28.02.2006 12:00:00	10.12.2006 14:18:06	28.02.2006 12:00:00	10.12.2006 13:21:5	WINDOWSHe
logowin.gif	logowin.gif	GIF-Bild	4821	10.12.2006 14:26:58	10.12.2006 14:26:58	04.08.2004 00:11:2	10.12.2006 14:26:5	ProgrammeMi
lback.gif	lback.gif	GIF-Bild	7047	10.12.2006 14:26:58	10.12.2006 14:26:58	04.08.2004 00:11:2	10.12.2006 14:26:5	ProgrammeMi
greenshd.gif	greenshd.gif	GIF-Bild	2135	10.12.2006 14:27:58	10.12.2006 14:27:58	28.02.2006 12:00:00	10.12.2006 14:27:5	WINDOWSsys
redshd.gif	redshd.gif	GIF-Bild	2119	10.12.2006 14:27:58	10.12.2006 14:27:58	28.02.2006 12:00:00	10.12.2006 14:27:5	WINDOWSsys
aleabanr.gif	aleabanr.gif	GIF-Bild	7830	10.12.2006 14:28:08	10.12.2006 14:28:08	28.02.2006 12:00:00	10.12.2006 14:28:0	ProgrammeGi
amaizrul.gif	amaizrul.gif	GIF-Bild	2184	10.12.2006 14:28:08	10.12.2006 14:28:08	28.02.2006 12:00:00	10.12.2006 14:28:0	ProgrammeGi
anabnr2.gif	anabnr2.gif	GIF-Bild	5492	10.12.2006 14:28:08	10.12.2006 14:28:08	28.02.2006 12:00:00	10.12.2006 14:28:0	ProgrammeGi
aswrule.gif	aswrule.gif	GIF-Bild	2086	10.12.2006 14:28:08	10.12.2006 14:28:08	28.02.2006 12:00:00	10.12.2006 14:28:0	ProgrammeGi
Hintergrund fr Schlicht.gif	HINTER~1.GIF	GIF-Bild	145	10.12.2006 14:28:08	10.12.2006 14:28:08	28.02.2006 12:00:00	10.12.2006 14:28:0	ProgrammeGi

Log messages (Duplicate name detected):

```

70W Duplicate name detected (contact.html changed to !!Duplicate 7!! contact.html)
70W Duplicate name detected (help.css changed to !!Duplicate 8!! help.css)
70W Duplicate name detected (tmp changed to !!Duplicate 9!! tmp)
70W Duplicate name detected (home.jsp changed to !!Duplicate 10!! home.jsp)
70W Duplicate name detected (hostSet_ljisp changed to !!Duplicate 11!! hostSet_ljisp)
70W Duplicate name detected (host_ljisp changed to !!Duplicate 12!! host_ljisp)
70W Duplicate name detected (icons changed to !!Duplicate 13!! icons)
70W Duplicate name detected (drivetable.txt changed to !!Duplicate 14!! drivetable.txt)
70W Duplicate name detected (drivetable.txt changed to !!Duplicate 15!! drivetable.txt)
70W Duplicate name detected (drivetable.txt changed to !!Duplicate 16!! drivetable.txt)
70W Duplicate name detected (WSCNTFY.EXE-1B24F5EB.pf changed to !!Duplicate 17!! WSCN
70W Duplicate name detected (VMSERVERDWIN32.EXE-06EE2FA1.pf changed to !!Duplicate 1
70W Duplicate name detected (ALG.EXE-0F138680.pf changed to !!Duplicate 19!! ALG.EXE-0F1
70W Duplicate name detected (CMD.EXE-087B4001.pf changed to !!Duplicate 20!! CMD.EXE-08
70W Duplicate name detected (MCCONSOL.EXE-137F9AD2.pf changed to !!Duplicate 21!! MCC
70W Duplicate name detected (R-STUDIO.EXE-2B676A42.pf changed to !!Duplicate 22!! R-STUI
70W Duplicate name detected (images changed to !!Duplicate 23!! images)
70W Duplicate name detected (VMSERVERDWIN32.EXE-1A4132F5.pf changed to !!Duplicate 2
70W Duplicate name detected (WSCNTFY.EXE-314238A5.pf changed to !!Duplicate 25!! WSCN
70W Duplicate name detected (JAVA.EXE-27A54C75.pf changed to !!Duplicate 26!! JAVA.EXE-
70W Duplicate name detected (WMIAPSRV.EXE-1846DF82.pf changed to !!Duplicate 27!! WMI/
70W Duplicate name detected (WUUAUCLT.EXE-141D0725.pf changed to !!Duplicate 28!! WUUAU
70W Duplicate name detected (ALG.EXE-30390E8C.pf changed to !!Duplicate 29!! ALG.EXE-30
70W Duplicate name detected (RUNDLL32.EXE-6A480868.pf changed to !!Duplicate 30!! RUNDL
70W Duplicate name detected (CLLEXE-02B0DB56.pf changed to !!Duplicate 31!! CLLEXE-02B
70W Duplicate name detected (index.jsp changed to !!Duplicate 32!! index.jsp)
70W Duplicate name detected (index.jsp changed to !!Duplicate 33!! index.jsp)
70W Duplicate name detected (js changed to !!Duplicate 34!! js)
70W Duplicate name detected (js changed to !!Duplicate 35!! js)
70W Duplicate name detected (logout.jsp changed to !!Duplicate 36!! logout.jsp)
70W Duplicate name detected (logout.jsp changed to !!Duplicate 37!! logout.jsp)
70W Duplicate name detected (objMod.jsp changed to !!Duplicate 38!! objMod.jsp)
70W Duplicate name detected (objMod.jsp changed to !!Duplicate 39!! objMod.jsp)
70W Duplicate name detected (raidAct.jsp changed to !!Duplicate 40!! raidAct.jsp)
70W Duplicate name detected (raidAct.jsp changed to !!Duplicate 41!! raidAct.jsp)
70W Duplicate name detected (refreshTree.jsp changed to !!Duplicate 42!! refreshTree.jsp)
70W Duplicate name detected (refreshTree.jsp changed to !!Duplicate 43!! refreshTree.jsp)
70W Duplicate name detected (screen.jsp changed to !!Duplicate 44!! screen.jsp)
70W Duplicate name detected (screen.jsp changed to !!Duplicate 45!! screen.jsp)
70W Duplicate name detected (tools changed to !!Duplicate 46!! tools)
70W Duplicate name detected (tools changed to !!Duplicate 47!! tools)
70W Duplicate name detected (CLLEXE-0785DEFA.pf changed to !!Duplicate 48!! CLLEXE-0785
70W Duplicate name detected (cmis_cs.tlv changed to !!Duplicate 49!! cmis_cs.tlv)
70W Duplicate name detected (cmis_cs.tlv changed to !!Duplicate 50!! cmis_cs.tlv)
70W Duplicate name detected (cmis_cs.tlv changed to !!Duplicate 51!! cmis_cs.tlv)
70W Duplicate name detected (treeframe.jsp changed to !!Duplicate 52!! treeframe.jsp)
70W Duplicate name detected (treeframe.jsp changed to !!Duplicate 53!! treeframe.jsp)
70W Duplicate name detected (usrSet_ljisp changed to !!Duplicate 54!! usrSet_ljisp)
70W Duplicate name detected (usrSet_ljisp changed to !!Duplicate 55!! usrSet_ljisp)
70W Duplicate name detected (usr_c.jsp changed to !!Duplicate 56!! usr_c.jsp)
70W Duplicate name detected (usr_c.jsp changed to !!Duplicate 57!! usr_c.jsp)
70W Duplicate name detected (usr_d.jsp changed to !!Duplicate 58!! usr_d.jsp)
70W Duplicate name detected (usr_d.jsp changed to !!Duplicate 59!! usr_d.jsp)
70W Duplicate name detected (usr_ent.jsp changed to !!Duplicate 60!! usr_ent.jsp)
70W Duplicate name detected (usr_ent.jsp changed to !!Duplicate 61!! usr_ent.jsp)
70W Duplicate name detected (usr_ljisp changed to !!Duplicate 62!! usr_ljisp)
70W Duplicate name detected (usr_ljisp changed to !!Duplicate 63!! usr_ljisp)
70W Duplicate name detected (usr_ljisp changed to !!Duplicate 64!! usr_ljisp)
70W Duplicate name detected (usr_ljisp changed to !!Duplicate 65!! usr_ljisp)
70W Duplicate name detected (utCfg_ljisp changed to !!Duplicate 66!! utCfg_ljisp)
70W Duplicate name detected (utCfg_ljisp changed to !!Duplicate 67!! utCfg_ljisp)
70W Duplicate name detected (cmis_ms.tlv changed to !!Duplicate 68!! cmis_ms.tlv)
70W Duplicate name detected (cmis_ms.tlv changed to !!Duplicate 69!! cmis_ms.tlv)
70W Duplicate name detected (tmp.edb changed to !!Duplicate 70!! tmp.edb)
25W 71 Duplicate file names detected - these files renamed to avoid extraction problems
26I Finished checking for duplicate file names
08I Building the filesystem meta data, please wait ...
09I Initialised file system driver
01I Calculating partition free space, this may take some time ...
02I Finished calculating partition free space
    
```


Undelete-Software

R-STUDIO - File View H: on SAMSUNG HD401LJZZ100-15

Drive File Tools View Help

Metfiles
Root
\$\$\$Folder02014
mgaertne
.AppleDouble
.ssh
.xemacs
Diashow
EGVP-postfach
Excel
Haus
ISP
Mail
Network Trash Folder
Powerppt
Schulungen
temp
TheFindByContentFolder
TheVolumeSettingsFolder
Vorlesung
WinWord
RECYCLER
System Volume Information
\$\$\$Folder30512
\$\$\$Folder29821
\$\$\$Folder28729
\$\$\$Folder27823
\$\$\$Folder27393
\$\$\$Folder21962
\$\$\$Folder06341
\$\$\$Folder00057
\$\$\$Folder00056
\$\$\$Folder00000

Name	Size	Created	Modified	File Id	Permissions
396431.jpg	28672	18.11.2007 10:56:02	18.11.2007 10:56:02	34181	
396432.jpg	28672	18.11.2007 10:56:02	18.11.2007 10:56:02	34182	
396433.jpg	40960	18.11.2007 10:56:02	18.11.2007 10:56:02	34183	
396434.jpg	36864	18.11.2007 10:56:02	18.11.2007 10:56:02	34184	
396436.jpg	20480	18.11.2007 10:56:02	18.11.2007 10:56:02	34185	
396437.jpg	16384	18.11.2007 10:56:02	18.11.2007 10:56:02	34186	
396438.jpg	24576	18.11.2007 10:56:02	18.11.2007 10:56:02	34187	
396439.jpg	24576	18.11.2007 10:56:02	18.11.2007 10:56:02	34188	
396440.jpg	28672	18.11.2007 10:56:02	18.11.2007 10:56:02	34189	
396441.jpg	24576	18.11.2007 10:56:02	18.11.2007 10:56:02	34190	
396442.jpg	36864	18.11.2007 10:56:02	18.11.2007 10:56:02	34191	
396443.jpg	32768	18.11.2007 10:56:02	18.11.2007 10:56:02	34192	
396449.jpg	36864	18.11.2007 10:56:02	18.11.2007 10:56:02	34193	
396454.jpg	49152	18.11.2007 10:56:02	18.11.2007 10:56:02	34194	
396455.jpg	32768	18.11.2007 10:56:02	18.11.2007 10:56:02	34195	
397147.jpg	57344	18.11.2007 10:56:03	18.11.2007 10:56:03	34196	
397206.jpg	25088	18.11.2007 10:56:03	18.11.2007 10:56:03	34197	
397232.jpg	33280	18.11.2007 10:56:03	18.11.2007 10:56:03	34198	
397274.jpg	29184	18.11.2007 10:56:03	18.11.2007 10:56:03	34199	
397641.jpg	217600	18.11.2007 10:56:03	18.11.2007 10:56:03	34200	
397647.jpg	168448	18.11.2007 10:56:03	18.11.2007 10:56:03	34201	
397671.jpg	180224	18.11.2007 10:56:03	18.11.2007 10:56:03	34202	
397682.jpg	14848	18.11.2007 10:56:03	18.11.2007 10:56:03	34203	
398327.jpg	140800	18.11.2007 10:56:03	18.11.2007 10:56:03	34204	
398329.jpg	364544	18.11.2007 10:56:03	18.11.2007 10:56:03	34205	
398330.jpg	57344	18.11.2007 10:56:03	18.11.2007 10:56:03	34206	
398331.jpg	72192	18.11.2007 10:56:03	18.11.2007 10:56:03	34207	
398333.jpg	53248	18.11.2007 10:56:03	18.11.2007 10:56:03	34208	
398381.jpg	49152	18.11.2007 10:56:03	18.11.2007 10:56:03	34209	
398451.jpg	39424	18.11.2007 10:56:03	18.11.2007 10:56:03	34210	
398453.jpg	36864	18.11.2007 10:56:03	18.11.2007 10:56:03	34211	
398454.jpg	81920	18.11.2007 10:56:03	18.11.2007 10:56:03	34212	
398770.jpg	64512	18.11.2007 10:56:03	18.11.2007 10:56:03	34213	
398772.jpg	93184	18.11.2007 10:56:03	18.11.2007 10:56:03	34214	

Log

Type	Date	Time	Text
System	16.03.2009	14:48:41	Enumeration of files started for H:
File System	16.03.2009	14:52:05	[FileId: 27831] MFT record child's claimed parent mismatch, aborting
System	16.03.2009	14:52:05	Enumeration of files finished for H:

Ready

Marked 0 in 0 files in 0 folders Total 71.1 GB in 1025690 files in 1693 folders



Closed-Source Software: Vor- und Nachteile

Vorteile:

- Es wird wenig technisches Know-How zur Bedienung und Herstellung von brauchbaren Ergebnissen benötigt.
- Es kann (im Rahmen der Softwaremöglichkeiten) wenig „vergessen“ werden.
- Es sind häufig sehr umfangreiche Funktionen und Auswertungen möglich.
- Sehr beweissicher, da Software darauf ausgelegt ist (Protokolle, Checksummen etc.).

Nachteile:

- Es kann nur das ausgewertet werden, was durch die Entwickler programmiert wurde.
- Reports oft sehr „amerikanisiert“ und u.U. nur bedingt für deutsche Strafverfolger sinnvoll.
- Vorgefertigte Module/Auswertungen benötigen kein umfassendes Know-How
 - „Was nicht von XXX angezeigt wird, existiert nicht“

■ LINUX/UNIX-Tools

- dd_rescue zum Erzeugen von Festplatteinimages
- md5sum zum Erzeugen von Hashcodes
- ntfsundelete zum Wiederherstellen von gelöschten Dateien
- find zum finden von Dateien
- file zum Feststellen von Dateiformaten
- Screenshot zum Herstellen von Bildschirmabbildungen

Open Source Werkzeuge (II)

- Sleuthkit und dessen Werkzeuge
- Foremost, recoverjpeg zum Wiederherstellen von Bild- und anderen Dateiformaten
- z.B. mplayer zum Darstellen von Videos
- gwenview/irfanview zum Ansehen von Bilddateien und Erstellen von Zusammenfassungen (thumbnails)
- Wireshark zum Mitschneiden von Netzwerkaktivitäten
- ClamAV zum Überprüfen auf Viren oder Trojaner
- Quellen auf dem Internet
(www.endungen.de, Forensik- Veröffentlichungen usw.)
- Und, und, und



Open-Source Beispiele, sleuthkit

Image File Details

Local Name: images/windows-disk-basis.img

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- Ignore the hash value for this image.
- Calculate the hash value for this image.
- Add the following MD5 hash value for this image:

Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: NTFS (0x07))

Sector Range: 63 to 12562829

Mount Point:

File System Type:

ADD

CANCEL

HELP

REPORT

V

Pointed to by file:

C:/Dokumente und Einstellungen/All Users:\$I30

File Type:

data

MD5 of content:

8e215da06984db90d45f84386e562799 -

SHA-1 of content:

02d61a186293f7b5fc2c66b5dc3359ff6ebc683b -

Details:

MFT Entry Header Values:

Entry: 3418 Sequence: 1

\$LogFile Sequence Number: 43994488

Allocated Directory

Links: 2

\$STANDARD_INFORMATION Attribute Values:

Flags:

Owner ID: 0

Security ID: 267 ()

Created: Fri Mar 13 14:57:39 2009

File Modified: Fri Mar 13 15:18:02 2009

MFT Modified: Fri Mar 13 15:18:02 2009

Accessed: Fri Mar 13 16:20:48 2009

\$FILE_NAME Attribute Values:

Flags: Directory

Name: All Users

Parent MFT Entry: 3416 Sequence: 1

Allocated Size: 0 Actual Size: 0

Created: Fri Mar 13 14:57:39 2009

File Modified: Fri Mar 13 14:57:39 2009

MFT Modified: Fri Mar 13 14:57:39 2009

Accessed: Fri Mar 13 14:57:39 2009

Attributes:

\$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72

\$FILE_NAME (48-3) Name: N/A Resident size: 82

\$FILE_NAME (48-2) Name: N/A Resident size: 84

\$INDEX_ROOT (144-6) Name: \$I30 Resident size: 56

\$INDEX_ALLOCATION (160-4) Name: \$I30 Non-Resident size: 4096

14242

\$BITMAP (176-5) Name: \$I30 Resident size: 8

Open-Source Beispiele, sleuthkit und dd_rescue

Current Directory: C:/ /Dokumente und Einstellungen/

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

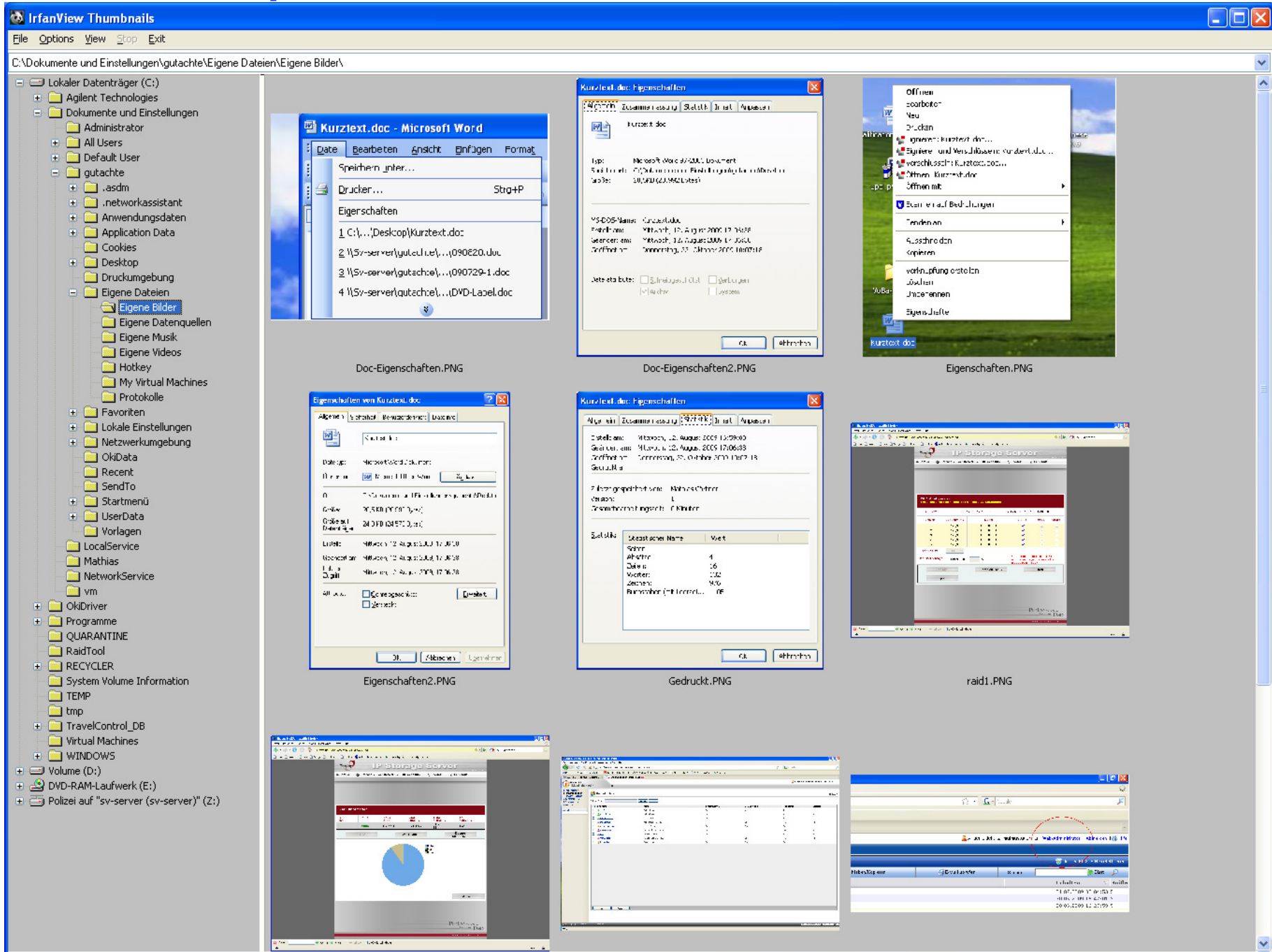
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
d / d	../		2009-03-13 16:09:51 (MET)	2009-03-13 16:09:51 (MET)	2009-03-13 16:09:51 (MET)	2009-03-13 15:51:42 (MET)	56	48	0	5-144-6
d / d	../		2009-03-13 15:34:09 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3416-144-6
d / d	All Users/		2009-03-13 15:18:02 (MET)	2009-03-13 16:20:48 (MET)	2009-03-13 15:18:02 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3418-144-6
d / d	Default User/		2009-03-13 15:33:51 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 15:33:51 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3417-144-7
d / d	Gutachte/		2009-03-13 15:34:20 (MET)	2009-03-13 15:34:20 (MET)	2009-03-13 15:34:20 (MET)	2009-03-13 15:34:09 (MET)	56	0	0	9970-144-5
d / d	LocalService/		2009-03-13 15:32:20 (MET)	2009-03-13 15:32:20 (MET)	2009-03-13 15:32:20 (MET)	2009-03-13 15:32:19 (MET)	56	0	0	9973-144-6
d / d	NetworkService/		2009-03-13 15:32:02 (MET)	2009-03-13 15:32:02 (MET)	2009-03-13 15:32:02 (MET)	2009-03-13 15:32:01 (MET)	56	0	0	3395-144-6

```
auswerter:/Disk1/autopsy-2.22 # dd_rescue /dev/sda /Disk1/test
```

```
dd_rescue: (info): ipos:          64512.0k, opos:          64512.0k, xferd:          64512.0k
                   errs:           0, errxfer:           0.0k, succxfer:          64512.0k
                   +curr.rate:     54479kB/s, avg.rate:      29880kB/s, avg.load:    1.4%
```



Open-Source Beispiele, irfanview



Open-Source Werkzeuge Vor- und Nachteile (I)

Nachteile:

- Sehr umfangreich, man muss schon wissen was man braucht.
- Reports sind selten automatisch erstellbar
- „Vergessen“ einer Auswertung ist leicht möglich, da die Software keinen „Fahrplan“ vorgibt.
- Beweissicherheit i.d.R. nur durch zusätzliche Maßnahmen erreichbar.
- Es sind fast immer eigene Ergänzungen notwendig, um schnell brauchbare Ergebnisse zu erhalten.
- Interpretation der Ergebnisse durch den technisch Sachverständigen ist unumgänglich.

Vorteile:

- Sehr umfangreich
 - fast alles ist schon mal programmiert worden und kann genutzt werden
- Der Untersucher benötigt nach wie vor technische Kenntnisse und Informationen über den internen Ablauf von Computer-Systemen.
- Sehr schneller Einsatz (pro Werkzeug) möglich , da sehr spezialisierte Werkzeuge vorliegen.

- *Closed-Source* Programme bieten umfangreiche, aber unbekannt hinreichende Auswertemöglichkeiten.
- Open-Source Programme bieten jeweils nur eine Funktion, aber durch die Vielfalt wird (fast) alles abgedeckt.
- Beim Einsatz von *Closed-Source* ist meist wenig Know-How über das zu untersuchende System an sich notwendig (ist aber hilfreich), daher recht schnell brauchbare Ergebnisse.
- *Open-Source* liefert nur das, was man mit entsprechendem Wissen auch abfragt/erstellt.

- *Closed-Source* ist i.d.R. ein System in dem bzw. mit dem alles organisiert und ausgewertet wird.
- *Open-Source* ist eine Sammlung von nicht zusammenpassenden Einzelsystemen. Ausnahme hier ist „sleuthkit“ mit „autopsy“.
- *Closed-Source* hat systematisch (nicht programmtechnisch) wenig Fehlerquellen.
- Der Einsatz von *Open-Source* bietet viele Fehlerquellen.

- Es existiert bei *Open-Source* Systemen, anders als in *Closed-Source* Systemen, kein Forensik-Fahrplan oder Checklisten. Fehlerquelle ist hier das Übersehen bzw. Vergessen einer Auswertung.
- *Open-Source* Systeme bieten mindestens den selben Funktionsumfang wie *Closed-Source* Systeme, die einzelnen Elemente sind aber nicht aufeinander abgestimmt.
- *Open-Source* Systeme sind für die Wünsche des Forensikers umprogrammierbar und neue Auswertungen sind leicht einführbar.

- Der Vortragende verwendet ausschließlich *Open-Source*-Lösungen um jeweils für den Auftraggeber angepasste Ergebnisse liefern zu können. Auch sind die einzelnen Programme leichter bedienbar als eine *Closed-Source*-Lösung.