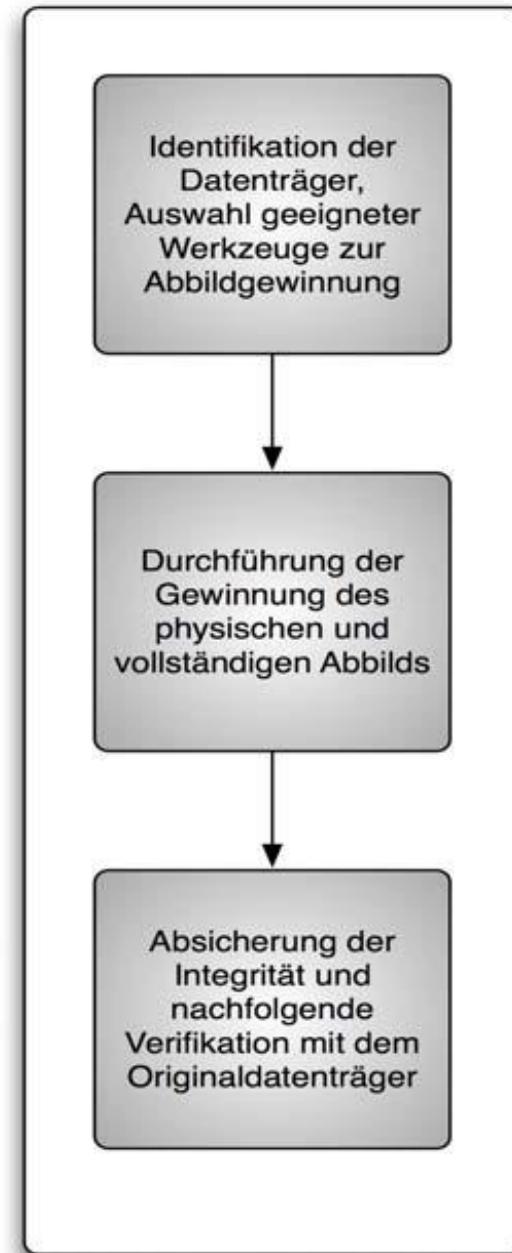


Abbildungserstellung



Forensische Kopie mit DD

dd if=/dev/hda of=myfile.img

if => Ankündigung Eingabedatei / Device

/dev/hda => Eingabedatei / Device

of => Ankündigung

myfile.img => zu erstellende Image-Datei

Weitere ggf. Relevante Parameter im Internet bzw. Man-Pages

Forensische Kopie mit DD (2)

```
sha256sum /dev/hda > /media/SHA256original
```

```
sha256sum /media/myfile.img > /media/SHA256image
```

dc3dd ist eine verbesserte Version von dd, z. B. mit eingebauter Hashprüfung, aber im wesentlichen mit dd identisch (Parameter sind leicht bei Google zu finden)

Dokumentation

- Wer hat das Image erstellt
- Wie (mit welchen Befehlen, Switches, Tools wurde das Image erstellt)
- Hashwerte des Images und wenn möglich auch des Originaldatenträgers
- Ggf. physische Parameter, Partitionen, logische Größen

Expert Witness Disk Image Format (EWF)

- komprimierte Images
 - mit integrierter (rudimentärer) Dokumentation
 - aufteilbar auf mehrere Dateien
 - z. B. apt install ewf-tools (ggf. noch libewf)
 - sudo ewfacquire -t /Case/myfile /dev/sdc
-
- Umwandeln von DD in EWF z. B. mit xmount
 - xmount --in Quellformat QUELLE --out Zielformat ZIEL

joshua@Zeus /media/joshua/Storage/temp \$ sudo ewfacquire /dev/sde
ewfacquire 20140608

Device information:

Bus type: USB
Vendor: SMI
Model: USB DISK
Serial: AA00000000000485D

Storage media information:

Type: Device
Media type: Removable
Media size: 4.0 GB (4051697664 bytes)
Bytes per sector: 512

Acquiry parameters required, please provide the necessary input

Image path and filename without extension: /media/joshua/Storage/temp/2017-USB-Gold-4G-001

Case number: 001

Description: Gold 4G USB case murder

Evidence number: 001

Examiner name: Joshua

Notes:

Media type (fixed, removable, optical, memory) [removable]:

Media characteristics (logical, physical) [logical]: physical

Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3, encase4, encase5, encase6, linen5, linen6, x) [encase6]:

Compression method (deflate) [deflate]:

Compression level (none, empty-block, fast, best) [none]: fast

Start to acquire at offset (0 <= value <= 4051697664) [0]: █

GYMAGER

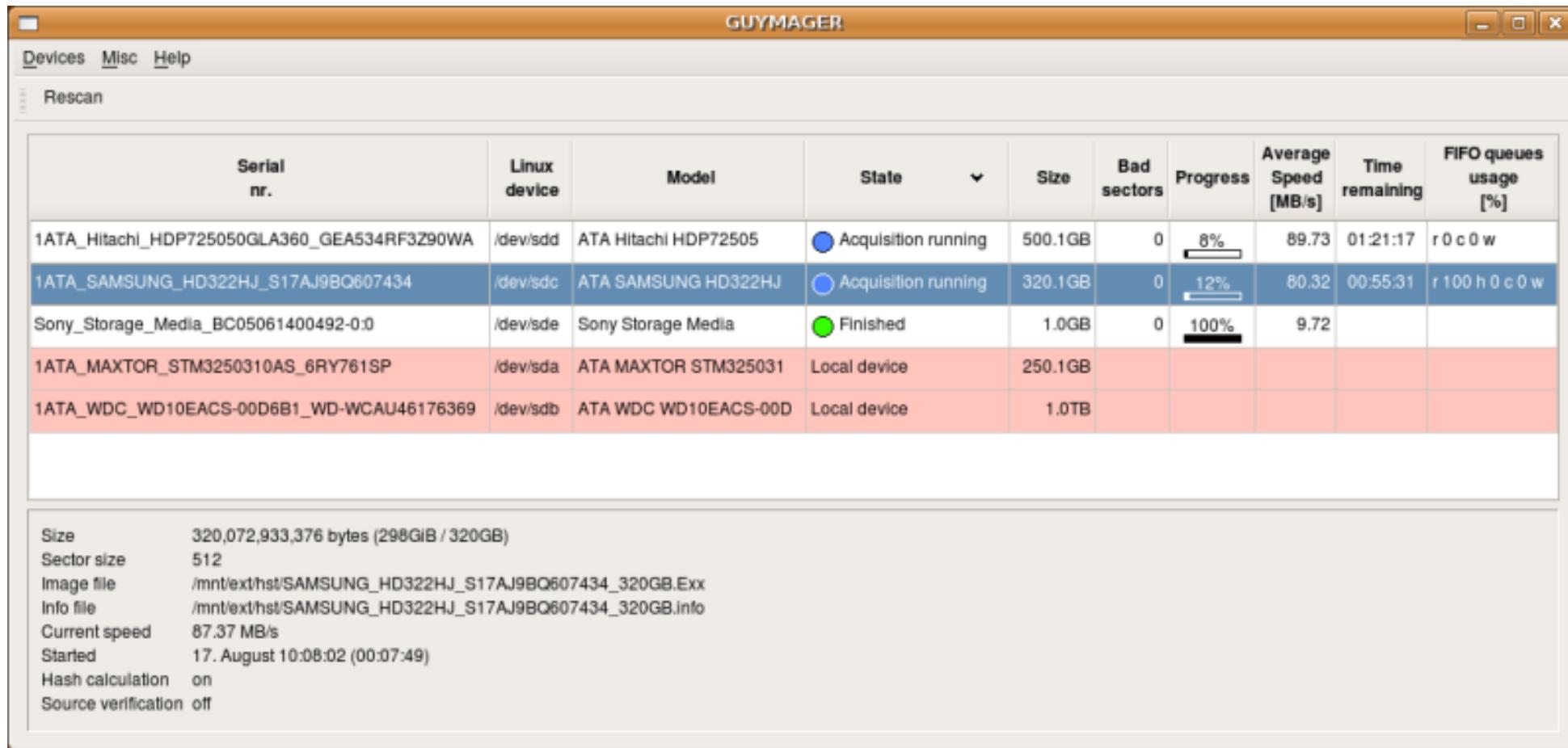


Abbildung erstellen: FTK Imager

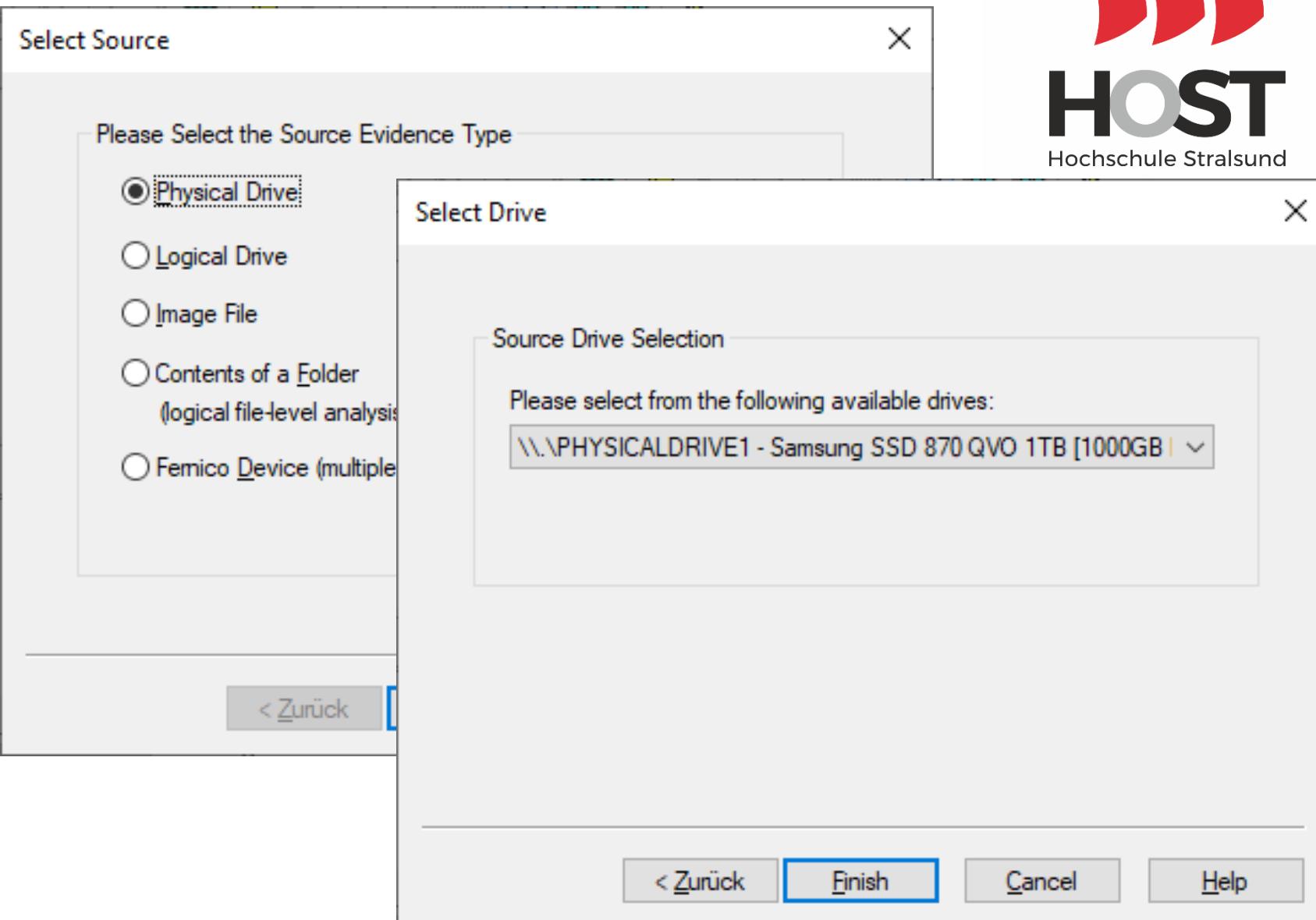
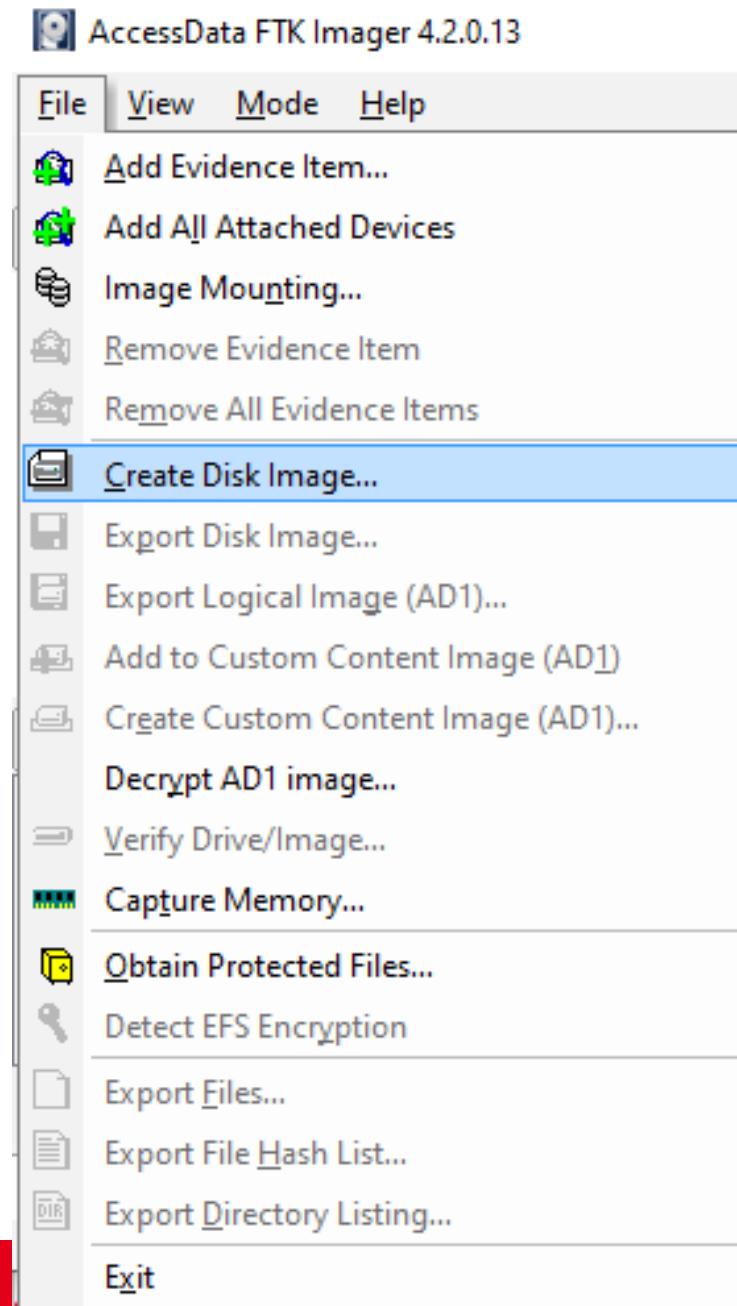


Abbildung erstellen: FTK Imager



Select Image Type

Please Select the Destination Image Type

Raw (dd)

SMART

E01

AFF

Evidence Item Information

Case Number:

12132

Evidence Number:

2

Unique Description:

SSD aus Rechensystem Acer 22139

Examiner:

Wilfried Honekamp

Notes:

Unterer Festplattenslott, graues SATA-Kabel

< Zurück

Weiter >

Abbrechen

< Zurück

Weiter >

Cancel

Help

Abbildung erstellen: FTK Imager

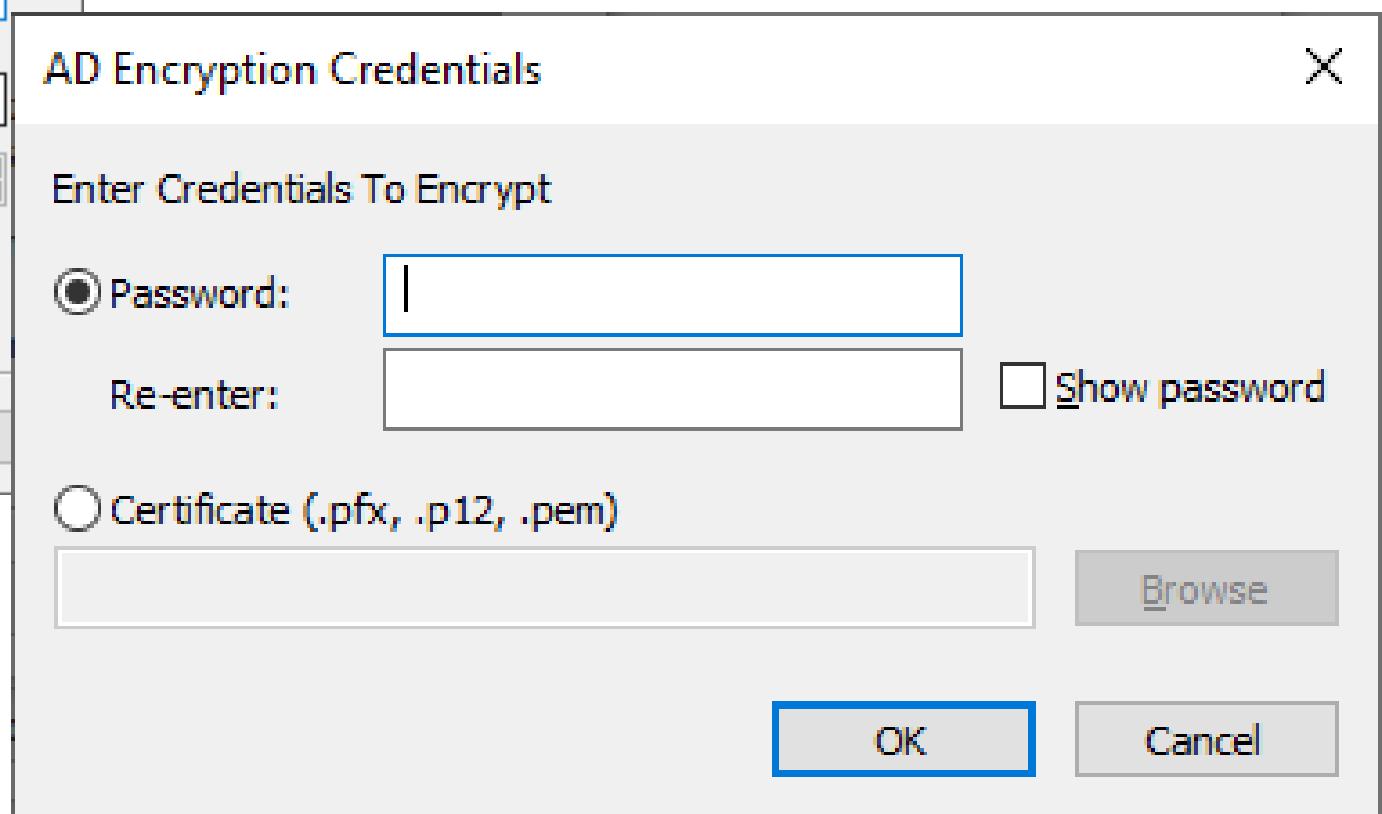
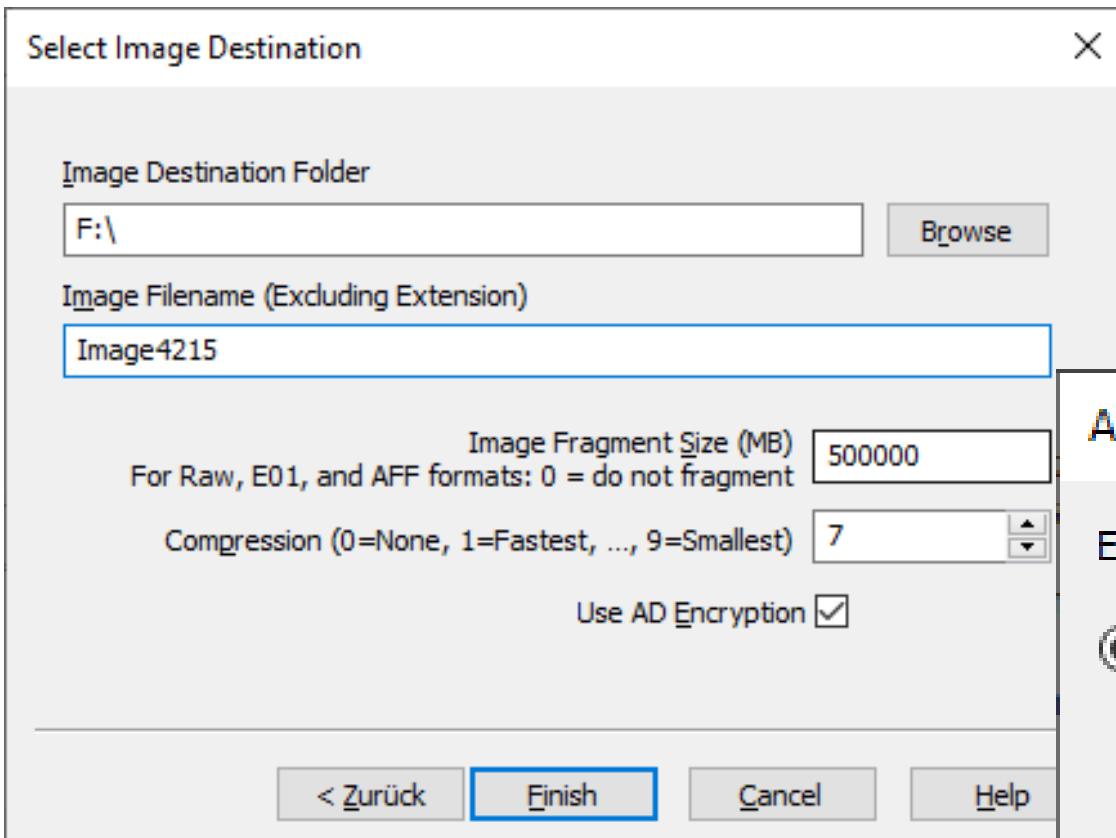


Abbildung auswerten: FTK Imager

AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- Image1.E01
 - NONAME [FAT12]
 - [root]
 - Privat
 - Bilder
 - Dokumente
 - Sprachen
 - French
 - Greek
 - [unallocated space]

File List

Name	Size	Type	Date Modified
CHRISTMA.GIF	94	Regular File	01.02.2001 09:5...
CHRISTMA.BMP	513	Regular File	01.02.2001 09:5...
CARLOS.ART	4	Regular File	27.05.1999 09:5...
2.JPG	2	Regular File	21.09.2000 14:4...

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value Inter... Custom Conte...

Cursor pos = 0; clus = 317; log sec = 348

000 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 48
010 00 48 00 00 FF DB 00 43-00 0D 09 0A 0B 0A 08 0D
020 0B 0A 0B 0E 0E 0D 0F 13-20 15 13 12 12 13 27 1C
030 1E 17 20 2E 29 31 30 2E-29 2D 2C 33 3A 4A 3E 33
040 36 46 37 2C 2D 40 57 41-46 4C 4E 52 53 52 32 3E
050 5A 61 5A 50 60 4A 51 52-4F FF DB 00 43 01 0E 0E
060 0E 13 11 13 26 15 15 26-4F 35 2D 35 4F 4F 4F 4F
070 4F 4F 4F 4F 4F 4F-4F 4F 4F 4F 4F 4F 4F 4F 4F
080 4F 4F 4F 4F 4F 4F-4F 4F 4F 4F 4F 4F 4F 4F 4F
090 4F 4F 4F 4F 4F 4F-4F 4F 4F 4F 4F 4F 4F FF C0
0a0 00 11 08 00 68 00 60 03-01 22 00 02 11 01 03 11
0b0 01 FF C4 00 1F 00 00 01-05 01 01 01 01 01 01 00

...ý0ýà · JFIF H
·H .. ýÜ ·C
.....
.. .)10 .)-,3:J>3
6F7,-@WAFLNRSR2>
ZaZP`JQROýÜ ·C ...
.....& ..&05-50000
0000000000000000
0000000000000000
00000000000000ýÀ
.....h .."
.....ýÄ

Abbildung auswerten: X-Ways

Benutzeroberfläche

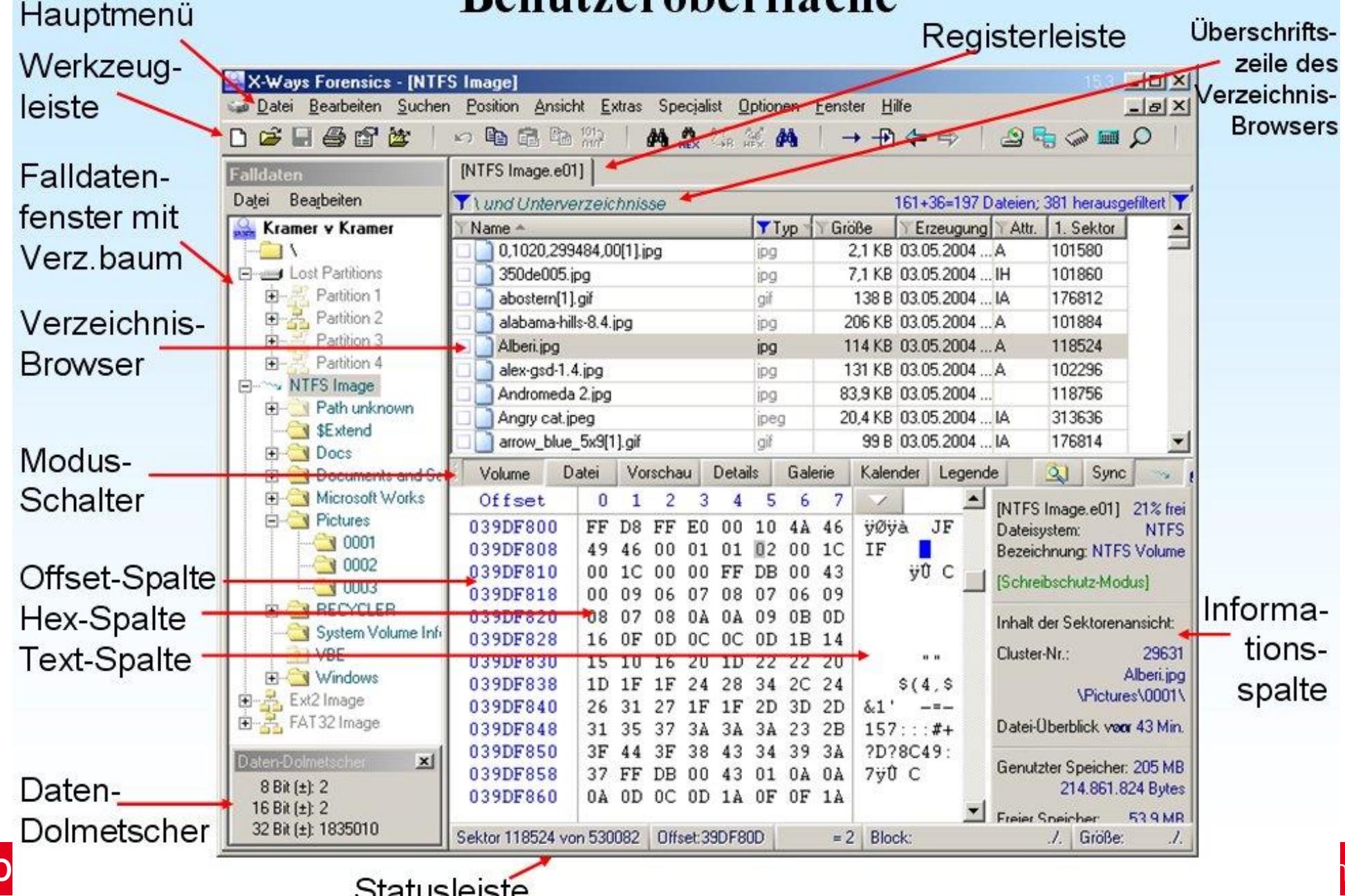


Abbildung auswerten: EnCase

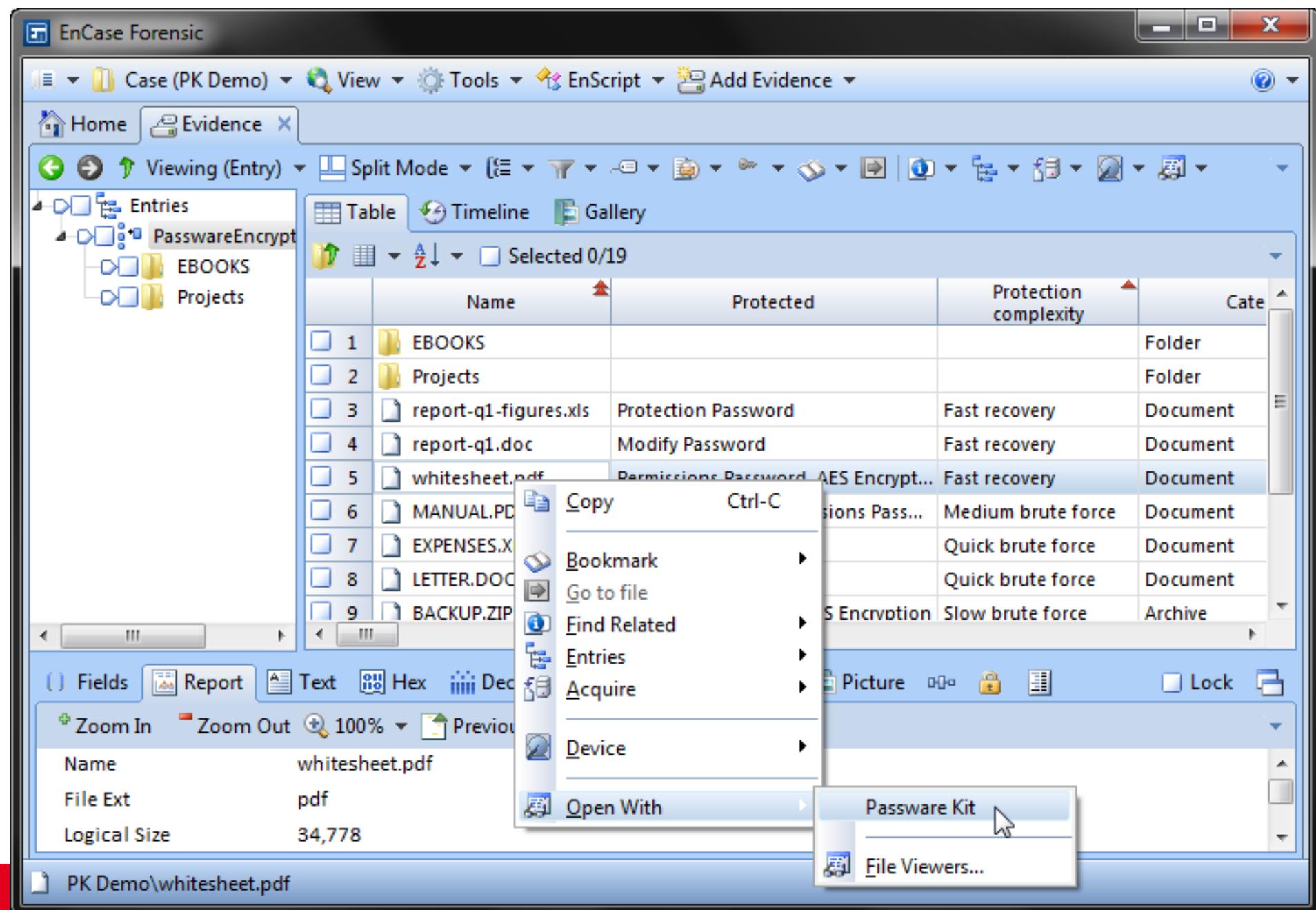


Abbildung auswerten: OSForensics

OSForensics - Gully

Workflow

- Start
- Auto Triage
- Manage Case**
- Create Forensic Image
- Mount Drive Image
- Add Device
- Boot Virtual Machine
- File System Browser**
- File Viewer
- System Information
- Memory Viewer
- User Activity
- Passwords
- File Name Search
- Deleted Files Search
- Mismatch Files Search
- Program Artifacts

File System Browser

File View Tools Help

Image1:\Privat\Bilder

F:\ [Local]

Name	Type	Date modified
..		02.09.2003, 15:11:26.0000...
2.JPG	JPG-Datei	21.09.2000, 14:46:04.0000...
CARLOS.ART	ART-Datei	27.05.1999, 09:50:20.0000...
CHRISTMA.BMP	BMP-Datei	01.02.2001, 09:57:18.0000...
CHRISTMA.GIF	GIF-Datei	01.02.2001, 09:54:00.0000...

Image1:\Privat\Bilder\CARLOS.ART

Automatically open selected item in list Visible

File Viewer Hex/String Viewer Text Viewer File Info Metadata OCR

Extract Use Regex Filter Presets

Enter filter text Filter Search...

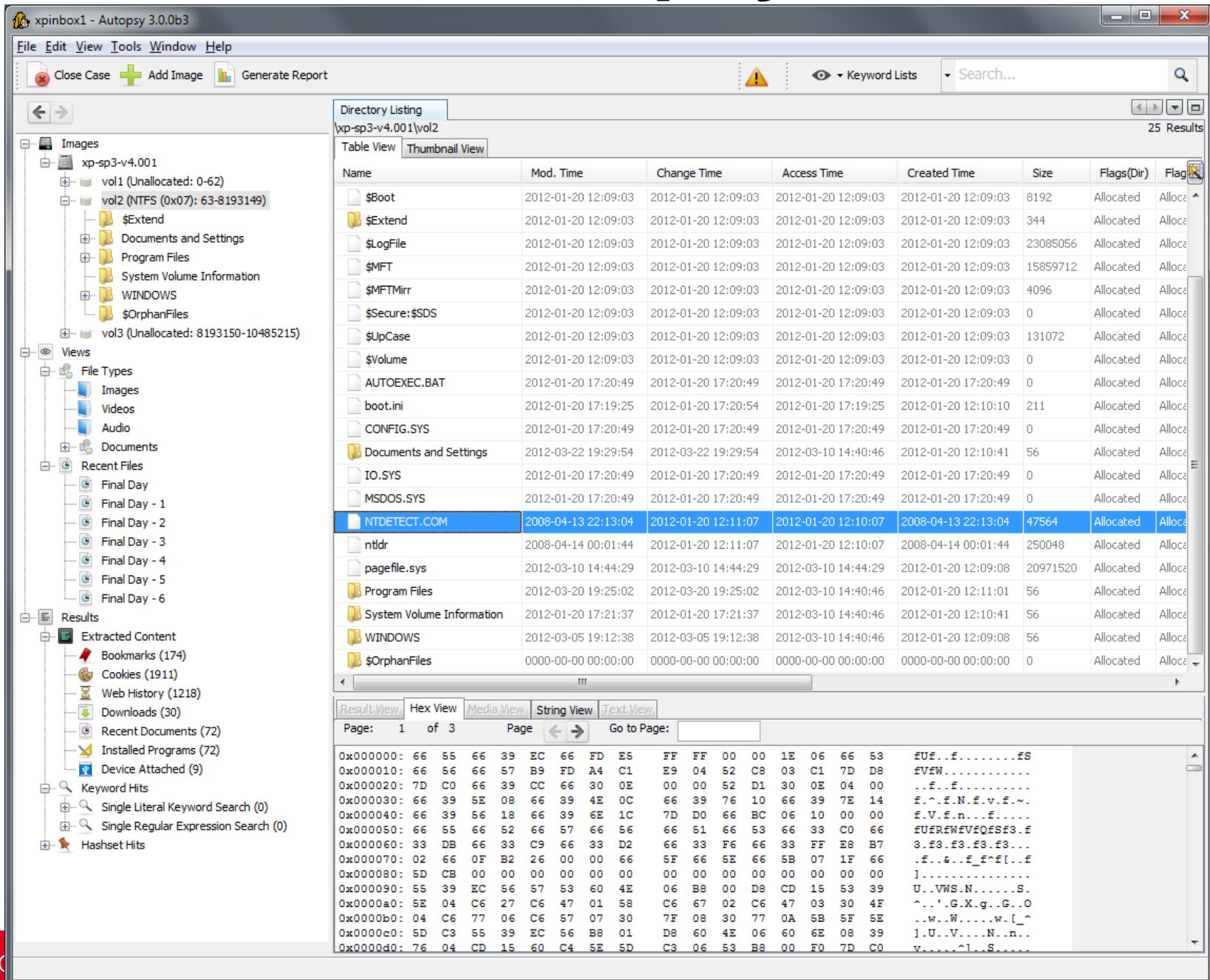
Settings

00 08
0x000000C0 4C6E70AFFE902998 463FDCE8A8749C5
0x000000D0 FEBF9CBC626AFE7C A55F6F54DC71858
0x000000E0 C584BF761EFE9EBC FC7941BDF4FC79I
0x000000F0 7096849E7A7A95B0 3C64FEA0732EB68
0x00000100 8A9E948D7D9971B2 65997DFC80A1FEE
0x00000110 3C4465C4879B9478 909870C66267A32
0x00000120 B9DD3CADBE807699 A1789DB07F8A7B8
0x00000130 83606F9CB164C665 96B9484701410FC
0x00000140 DF1E2AE4FE592BA9 CF78237E50DD0DC
0x00000150 026C50BF248E89FC 9A812068137C9A2
0x00000160 EE26FC9A11BDC731 A706E9797783148
0x00000170 C01C8CCC8123A8C4 51DD2E662473637
Press 'Extract' to parse for strings.

0x00000160 - 0x00000170 (16 Bytes) Selected

CARLOS.ART (2 of 4)

Abbild auswerten: Autopsy



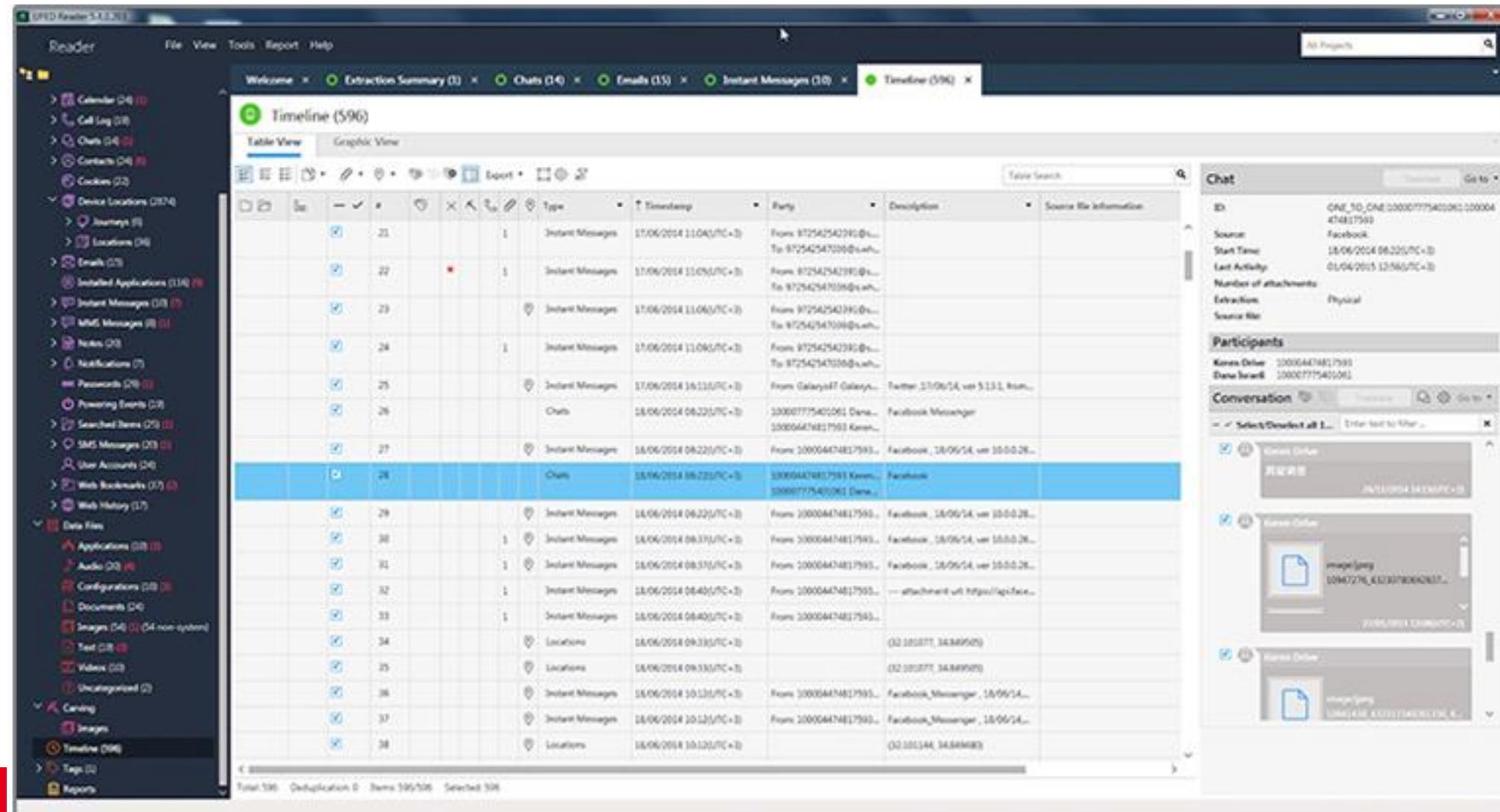
The screenshot shows the Autopsy 3.0.0b3 interface. The left pane displays a hierarchical tree of the image file structure, including volumes (vol1, vol2, vol3) and extracted content (Bookmarks, Cookies, Web History, Downloads, Recent Documents, Installed Programs, Device Attached). The right pane shows a table of found files with the following columns: Name, Mod. Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags. A specific file, 'NTDETECT.COM', is selected and highlighted in blue. Below the table is a hex viewer showing binary data for page 1 of 3.

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$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	Allocated
\$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	Allocated
\$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	Allocated
\$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	Allocated
\$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	Allocated
\$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	Allocated
\$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	Allocated
\$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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
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	Allocated
\$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	Allocated

Result View | Hex View | Media View | String View | Text View
Page: 1 of 3 Page Go to Page:

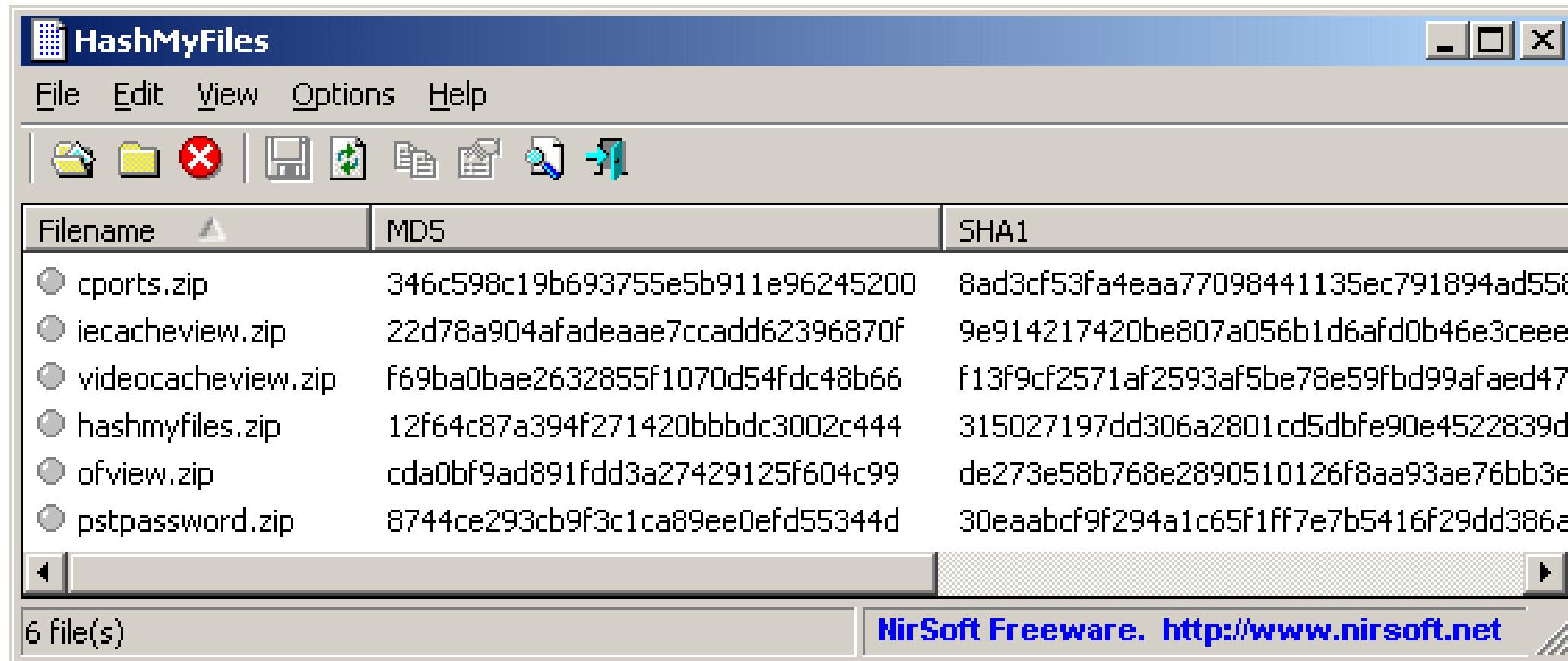
0x000000:	66 55 66 39 EC 66 FD E5 FF FF 00 00 1E 06 66 53	fUF..f.....ES
0x000010:	66 56 66 57 B9 FD A4 C1 E9 04 52 C8 03 C1 7D D8	fEVW.....
0x000020:	7D C0 66 39 CC 66 30 0E 00 00 52 D1 30 0E 04 00	..f..f.....
0x000030:	66 39 5E 08 66 39 4E 0C 66 39 76 10 66 39 7E 14	f.^..N.f.v.f.^..
0x000040:	66 39 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 CO 66	EUREWEVEQESf3.E
0x000060:	33 DB 66 33 C9 66 33 D2 66 33 F6 66 33 FF EB B7	3..f3.f3.f3.f3...
0x000070:	02 66 0F B2 26 00 00 65 F6 5E 66 5B 07 1F 66	.f..&..f^F[..f
0x000080:	5D CB 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1.....
0x000090:	5E 39 EC 56 57 53 60 4E 06 BB 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	J.U..V...N..n..
0x0000d0:	76 04 CD 15 60 C4 5E SD C3 06 53 B8 00 F0 7D C0	v.....1.S.....

Abbildung auswerten: Cellebrite Reader (UFED Reader)



The screenshot displays the UFED Reader software interface, specifically the Timeline view. The main window title is "Timeline (596)". The left sidebar lists various data categories such as Calendar, Call Log, Chats, Contacts, Cookies, Device Locations, Emails, Installed Applications, Instant Messages, MMS Messages, Notes, Notifications, Passwords, Powering Events, Search Results, SMS Messages, User Accounts, Web Bookmarks, Web History, Data Files, Applications, Audio, Configurations, Documents, Images, Text, Videos, Uncategorized, and Caving. The Timeline view shows a grid of 596 entries, each with a timestamp, type (e.g., Instant Message, Chat), parties involved, description, and source file information. A detailed Chat panel on the right shows a conversation between two participants, Karen.Diller and Diane.Sawill, with specific message content and attachments visible. The bottom status bar indicates a total of 596 items, no duplicates, and 595 selected.

Hashes erstellen

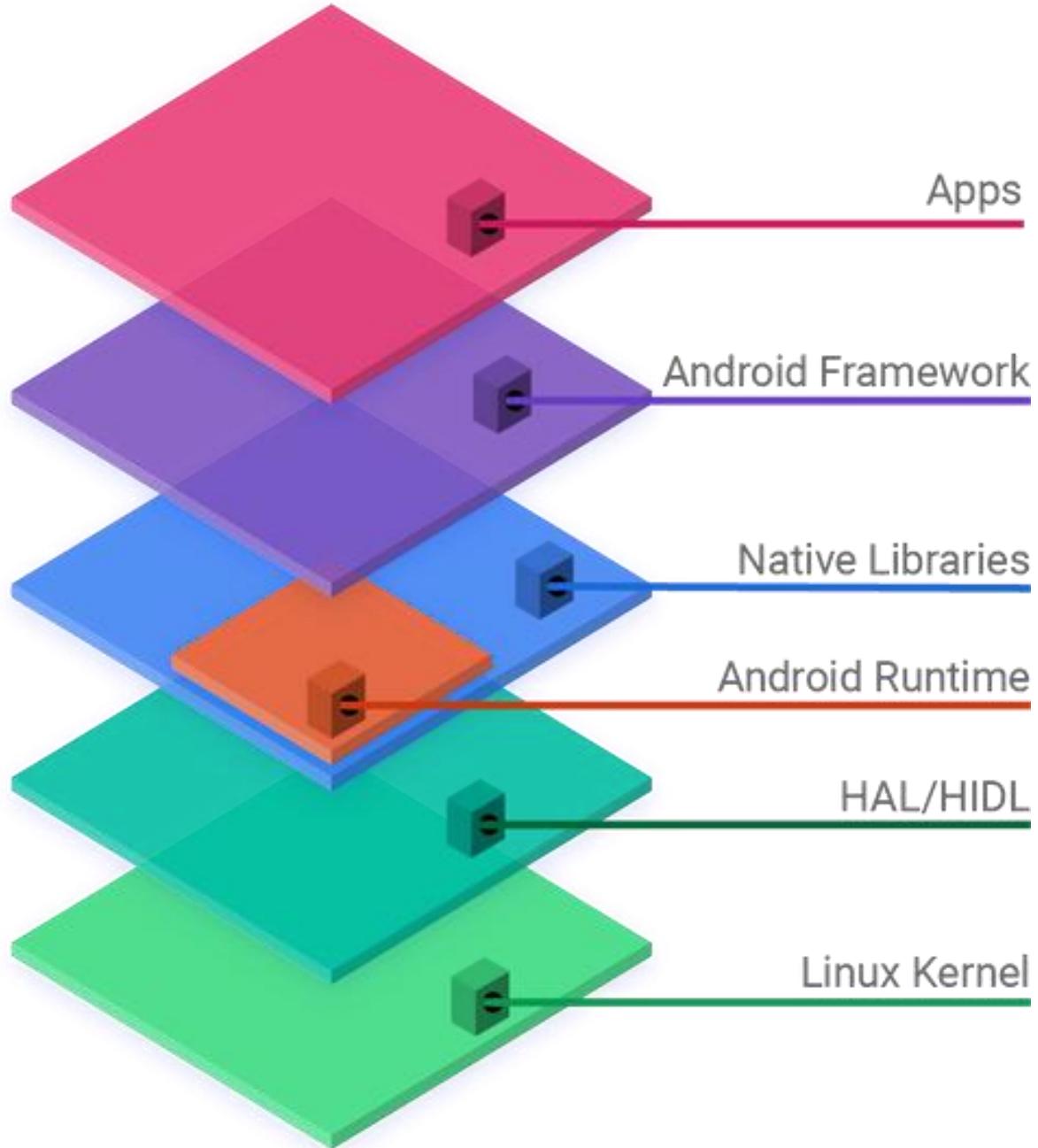


Android-Sicherung



- Datei-Sicherung
- Android Debug Bridge
- Physische Sicherung

Android



 .backups	 .fileManager	 .Ota
 android	 CFANS	 com.mdv.VMWCompanion
 CrashLogs	 DCIM	 Documents
 Download	 Dtfj	 Movies
 Music	 Photo Editor	 Pictures
 Qmove	 reolink	 WhatsApp
 .fe_tmp FE_TMP-Datei 0 Bytes	 .ReolinkCacheFile REOLINKCACHEFILE-Datei 32 Bytes	 .sd.txt Textdokument 25 Bytes
 db_copy.db Data Base File 292 KB		

Android: Logische Sicherung ohne Rootzugriff



Android Debug Bridge

aktivieren!

Einstellungen -> Über das Telefon -> Build Nummer x 7





Android Debug Bridge

- **ADB DEVICES**
- **ADB BACKUP**
- **ADB TCPIP, ADB CONNECT**
- **ADB SHELL**

Android Partitionen (Auszug)

- **boot**
- **system**
- **recovery**
- **data**
- **cache**
- **misc**

Android mount

```
/dev/root on / type ext4 (ro,seclabel,relatime)
tmpfs on /dev type tmpfs (rw,seclabel,nosuid,relatime,size=3896588k,nr_inodes=974147,mode=755)
devpts on /dev/pts type devpts (rw,seclabel,relatime,mode=600,ptmxmode=000)
proc on /proc type proc (rw,relatime,gid=3009,hidepid=2)
sysfs on /sys type sysfs (rw,seclabel,relatime)
selinuxfs on /sys/fs/selinux type selinuxfs (rw,relatime)
tmpfs on /mnt type tmpfs (rw,seclabel,nosuid,nodev,noexec,relatime,size=3896588k,nr_inodes=974147,mode=755,gid=1000)
tmpfs on /apex type tmpfs (rw,seclabel,nosuid,nodev,noexec,relatime,size=3896588k,nr_inodes=974147,mode=755)
/dev/block/dm-1 on /vendor type ext4 (ro,seclabel,relatime,discard)
none on /dev/cg2_bpf type cgroup2 (rw,nosuid,nodev,noexec,relatime)
none on /dev/cpuctl type cgroup (rw,nosuid,nodev,noexec,relatime,cpu)
none on /acct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct)
none on /dev/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset,noprefix,release_agent=/sbin/cpuset_release_agent)
none on /dev/stune type cgroup (rw,nosuid,nodev,noexec,relatime,schedtune)
debugfs on /sys/kernel/debug type debugfs (rw,seclabel,relatime)
none on /config type configfs (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime)
pstree on /sys/fs/pstree type pstree (rw,seclabel,nosuid,nodev,noexec,relatime)
none on /sys/fs/cgroup type tmpfs (rw,seclabel,relatime,size=3896588k,nr_inodes=974147,mode=750,gid=1000)
none on /sys/fs/cgroup/freezer type cgroup (rw,relatime,freezer)
none on /sys/fs/cgroup/net_cls type cgroup (rw,relatime,net_cls)
tracefs on /sys/kernel/debug/tracing type tracefs (rw,seclabel,relatime)
/dev/block/sda17 on /data type ext4 (rw,seclabel,nosuid,nodev,noatime,discard,noauto_da_alloc,resgid=1065,data=ordered)
/dev/block/sde4 on /vendor/firmware_mnt type vfat (ro,context=u:object_r:firmware_file:s0,relatime,uid=1000,gid=1000,fmask=0337,dmask=0227,codepage=437,iocharset=iso8859_1)
/dev/block/sd9 on /audio/dsp type ext4 (ro,seclabel,nosuid,nodev,relatime,data=ordered)
/dev/block/sda2 on /mnt/vendor/persist type ext4 (rw,seclabel,nosuid,nodev,noatime,data=ordered)
/dev/block/sde5 on /vendor/bt_firmware type vfat (ro,context=u:object_r:bt_firmware_file:s0,relatime,uid=1002,gid=3002,fmask=0337,dmask=0227,codepage=437,iocharset=iso8859_1)
/dev/block/sde59 on /op1 type ext4 (ro,context=u:object_r:op1_file:s0,relatime,data=ordered)
/dev/block/sda7 on /op2 type ext4 (rw,seclabel,nosuid,nodev,noatime,data=ordered)
/dev/block/sda15 on /op_odm type ext4 (ro,context=u:object_r:system_file:s0,nosuid,nodev,noatime,data=ordered)
tmpfs on /storage type tmpfs (rw,seclabel,nosuid,nodev,noexec,relatime,size=3896588k,nr_inodes=974147,mode=755,gid=1000)
/dev/block/loop2 on /system/reserve type ext4 (ro,context=u:object_r:system_file:s0,relatime,data=ordered)
/dev/block/dm-2 on /apex/com.android.media@301800204 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-2 on /apex/com.android.media type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-3 on /apex/com.android.conscrypt@301800104 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-3 on /apex/com.android.conscrypt type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-4 on /apex/com.android.media.swcodec@301700000 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-4 on /apex/com.android.media.swcodec type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-5 on /apex/com.android.tzdata@293500000 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/dm-5 on /apex/com.android.tzdata type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop7 on /apex/com.android.resolv@290000000 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop7 on /apex/com.android.resolv type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop8 on /apex/com.android.runtime@1 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop8 on /apex/com.android.runtime type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop9 on /apex/com.android.apex.cts.shim@1 type ext4 (ro,dirsSync,seclabel,nodev,noatime)
/dev/block/loop9 on /apex/com.android.apex.cts.shim type ext4 (ro,dirsSync,seclabel,nodev,noatime)
adb on /dev/usb-ffs/adb type functions (rw,relatime)
/data/media on /mnt/runtime/default/emulated type sdcardfs (rw,nosuid,nodev,noexec,noatime,fsuid=1023,fsgid=1023,gid=1015,multiuser,mask=6,derive_gid,default_normal)
/data/media on /storage/emulated type sdcardfs (rw,nosuid,nodev,noexec,noatime,fsuid=1023,fsgid=1023,gid=1015,multiuser,mask=6,derive_gid,default_normal)
/data/media on /mnt/runtime/read/emulated type sdcardfs (rw,nosuid,nodev,noexec,noatime,fsuid=1023,fsgid=1023,gid=9997,multiuser,mask=23,derive_gid,default_normal)
/data/media on /mnt/runtime/write/emulated type sdcardfs (rw,nosuid,nodev,noexec,noatime,fsuid=1023,fsgid=1023,gid=9997,multiuser,mask=7,derive_gid,default_normal)
/data/media on /mnt/runtime/full/emulated type sdcardfs (rw,nosuid,nodev,noexec,noatime,fsuid=1023,fsgid=1023,gid=9997,multiuser,mask=7,derive_gid,default_normal)
```

Android mount

/dev/block/sda17 on /data type ext4

Physische Sicherung

- Root -> dd am besten mit | nc
- All-In-One Tools mit Exploits

iOS-Sicherung



- **Finder -> Mac**
- **iTunes File Sharing**
- **Apps**
- **iCloud**
- **Backup Tools**
- **Physische Sicherung**

iOS

Cocoa (Application)

Media

Core Services

Address Book

Core Data

Core Foundation

Foundation

Quick Look

Social

Security

WebKit

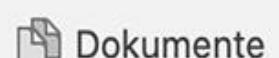
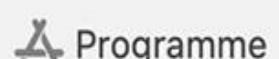
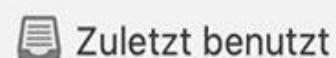
Core OS

Kernel and Device Drivers



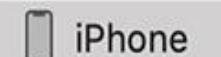
Suchen

Favoriten



iCloud

Orte



Tags

apple.com



iPhone

iPhone 11 Pro · 57,63 GB (43,16 GB verfügbar) · 100 %

[Allgemein](#) [Musik](#) [Filme](#) [TV-Sendungen](#) [Podcasts](#) [Hörbücher](#) [Bücher](#) [Fotos](#) [Dateien](#) [Infos](#)

Name	Größe	Änderungsdatum
------	-------	----------------

▶ Clips		
▶ iMovie		
▶ Keynote		
▶ Numbers		
▼ Pages		
Chocolate Chip Cookies.pages	3,8 MB	07.02.2020, 11:10
District Market.pdf	4,9 MB	07.02.2020, 11:09
Kitchen Stories.pages	7,3 MB	07.02.2020, 11:07
Street Food in Bangkok Ep 3.pages	51,2 MB	07.02.2020, 11:03

Fotos

Dokumente & Daten

Sync

iTunes File Sharing

- Kabel oder WLAN
- Nur Daten von Apps, die mit File Sharing arbeiten, wie Keynotes, Numbers oder Pages
- verwenden

apple.com



Q, Search

John's iPhone

 John's iPhone
256GB 100%

Settings

Summary

Music

Movies

TV Shows

Podcasts

Books

Photos

Info

File Sharing

On My Device

Music

Movies

TV Shows

Books

Audiobooks

Tones

File Sharing

The apps listed below can transfer documents between your iPhone and this computer.

Apps



Keynote Documents

Getting Started.key	252 KB	Today 9:41 AM
September 2017	298 KB	Today 9:41 AM

Add... Save to...

226.91 GB Free

Sync

Done

iCloud-Backup

- **Bietet bis zu 2 TB Speicherplatz
(die ersten 5 GB sind kostenlos)**
- **Verschlüsselt Backups immer**
- **Erlaubt, Backups überall per WLAN zu erstellen und zu verwenden**

apple.com

iCloud

7.11



iCloud

[iTunes Store](#)

[iTunes Store](#)

[Account details...](#)

[iCloud Help](#)

[Sign out](#)

 iCloud Drive

 Photos

 Bookmarks

You have 5.00 GB of iCloud storage.

 Backups 4.26 GB Storage

Backup Tools

- Speichert Backups auf Mac oder PC
- Bietet verschlüsselte Backups
(standardmäßig deaktiviert)
- Erlaubt, Backups auf dem Mac oder PC zu erstellen und zu verwenden

EaseUS MobiMover

Manager

Content Management

Data Transfer

Phone to PC

PC to Phone

Phone to Phone

Media

Video Downloader

Backup & Restore (New)

Backup Manager

WhatsApp Manager

Select categories you want to transfer to:

C:\Users\Owner\Desktop

C:\Users\Owner\Desktop
Custom Path

Audio



Pictures



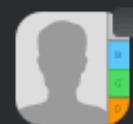
Videos



Books



Voice Mails



Contacts



Podcasts



Messages



Notes

Transfer

Grundlagen der IT-Forensik



Windows-Forensik

Gliederung

- Windows Analyse
 - Registry
 - Prefetching
 - Eventlogs

Toolsammlung NirSoft

NirLauncher - NirSoft Utilities

File Edit View Options Launcher Packages Help

Password Recovery Utilities		Network Monitoring Tools	Web Browser Tools	Video/Audio Related Utilities
Internet Related Utilities		Command-Line Utilities	Desktop Utilities	Outlook/Office Utilities
Programmer Tools		System Utilities	Other Utilities	All Utilities
 MessenPass	Recover the passwords of instant messenger programs	1.28	01/12/2009 12:00:16	http://www.nirsoft.net/tools/messengerpw.htm
 WirelessKeyView	recovery lost wireless network keys (WEP/WPA) stored...	1.31	01/12/2009 11:32:44	http://www.nirsoft.net/tools/wirelesskeyview.htm
 LSASecretsDump	Dump the LSA secrets from the Registry.	1.21	29/11/2009 12:25:40	http://www.nirsoft.net/tools/lsasecretsdump.htm
 LSASecretsView	display the list of all LSA secrets stored in the Registr...	1.21	29/11/2009 12:19:38	http://www.nirsoft.net/tools/lsasecretsview.htm
 Network Password Rec...	Recover network passwords on Windows XP/2003/Vista.	1.23	29/11/2009 12:15:40	http://www.nirsoft.net/tools/networkpasswordrec.htm
 PasswordFox	View passwords stored in Firefox Web browser.	1.15	17/10/2009 13:15:16	http://www.nirsoft.net/tools/passwordfox.htm
 Dialupass	Recover Dial-Up passwords in all versions of Windows.	3.05	07/10/2009 20:02:08	http://www.nirsoft.net/tools/dialupass.htm
 IE PassView	Recover passwords stored by Internet Explorer (Versi...	1.17	28/09/2009 12:26:54	http://www.nirsoft.net/tools/iepassview.htm
 Mail PassView	Recover email passwords	1.52	21/09/2009 11:35:52	http://www.nirsoft.net/tools/mailpassview.htm
 VNCPassView	Recover the passwords stored by the VNC tool.	1.02	18/05/2009 11:57:20	http://www.nirsoft.net/tools/vncpassview.htm
 PstPassword	Recover lost password of Outlook PST file.	1.12	23/02/2009 12:22:46	http://www.nirsoft.net/tools/pstpassword.htm
 ChromePass	Password recovery tool for Google Chrome Web brows...	1.05	17/11/2008 22:34:34	http://www.nirsoft.net/tools/chromepass.htm
 Asterisk Logger	Reveals the passwords stored behind the asterisks (*...	1.04	12/05/2008 20:16:44	http://www.nirsoft.net/tools/asterisklogger.htm

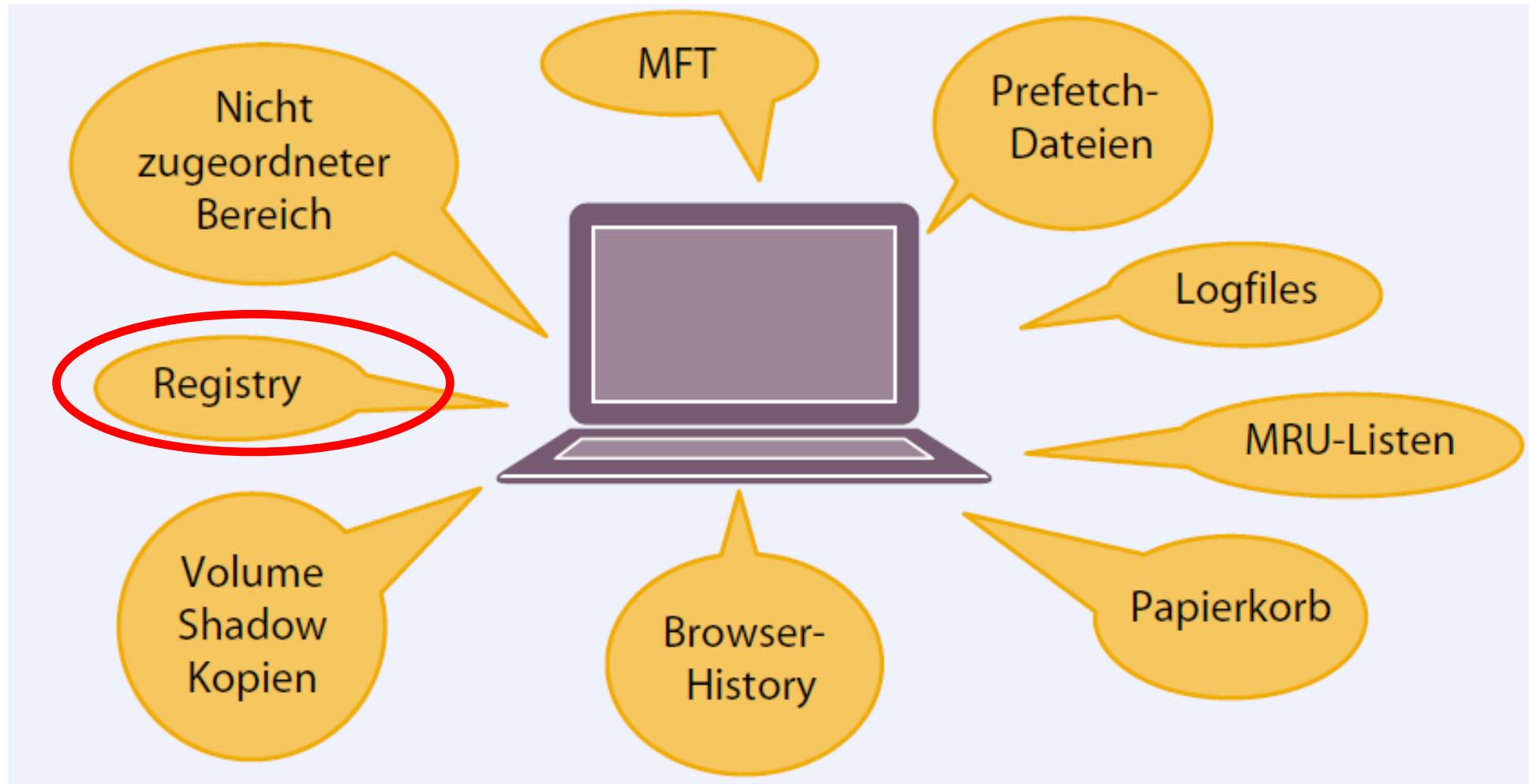
Run Advanced Run Web Page Help File Web Search Package Package

15 Utilities, 1 Selected

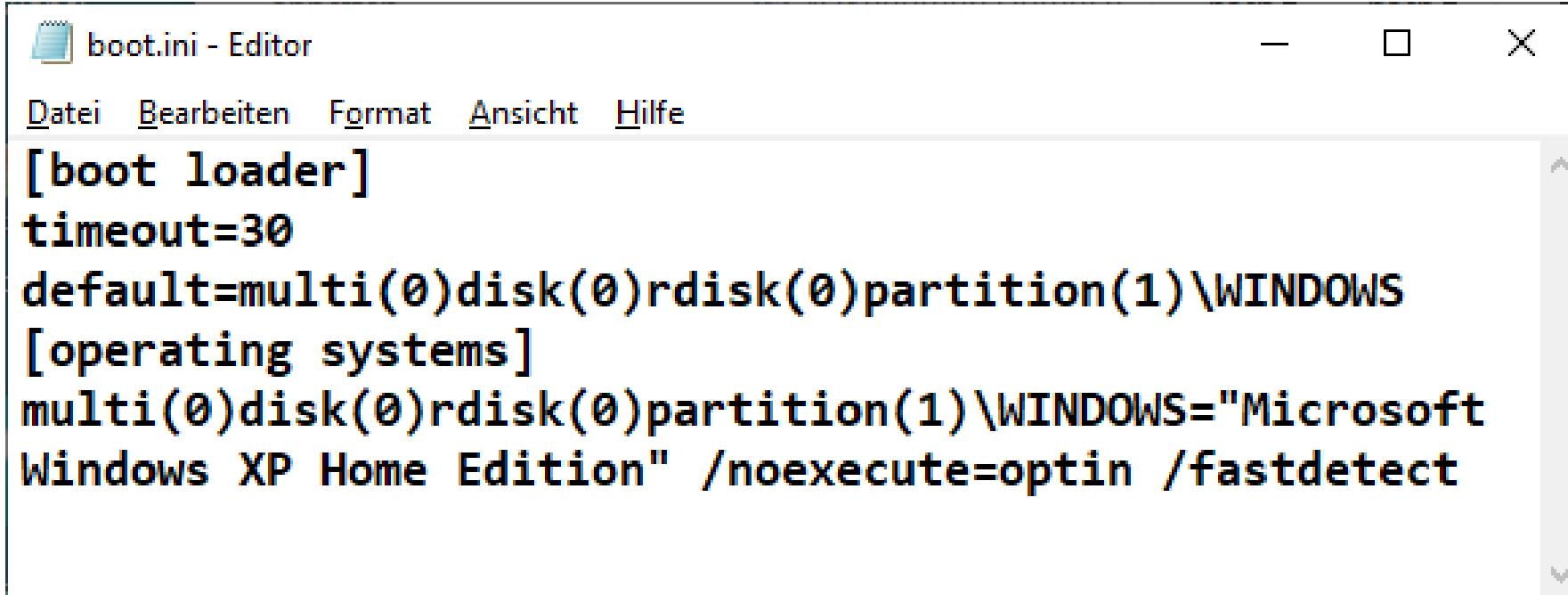
NirSoft Freeware. <http://www.nirsoft.net>

Siehe auch: <https://www.gaijin.at/de/>

Der Computer als Zeuge



Windows ini-Dateien



boot.ini - Editor

Datei Bearbeiten Format Ansicht Hilfe

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft
Windows XP Home Edition" /noexecute=optin /fastdetect
```

Windows Registry

- **Windows-Registrierungsdatenbank,
oft einfach nur Registry**
- **zentrale hierarchische Konfigurationsdatenbank des
Betriebssystems**
- **Datenbank für die Verwaltung des Systems und aller
integrierten Systemdienste und Prozesse**
- **sehr gute Quelle von Informationen um
Argumentationsketten zu untermauern**
- **Struktur einzelner Keys ändert sich von Windows-
Version zu Windows-Version**
- **IT-ForenikerInnen müssen am Ball bleiben**

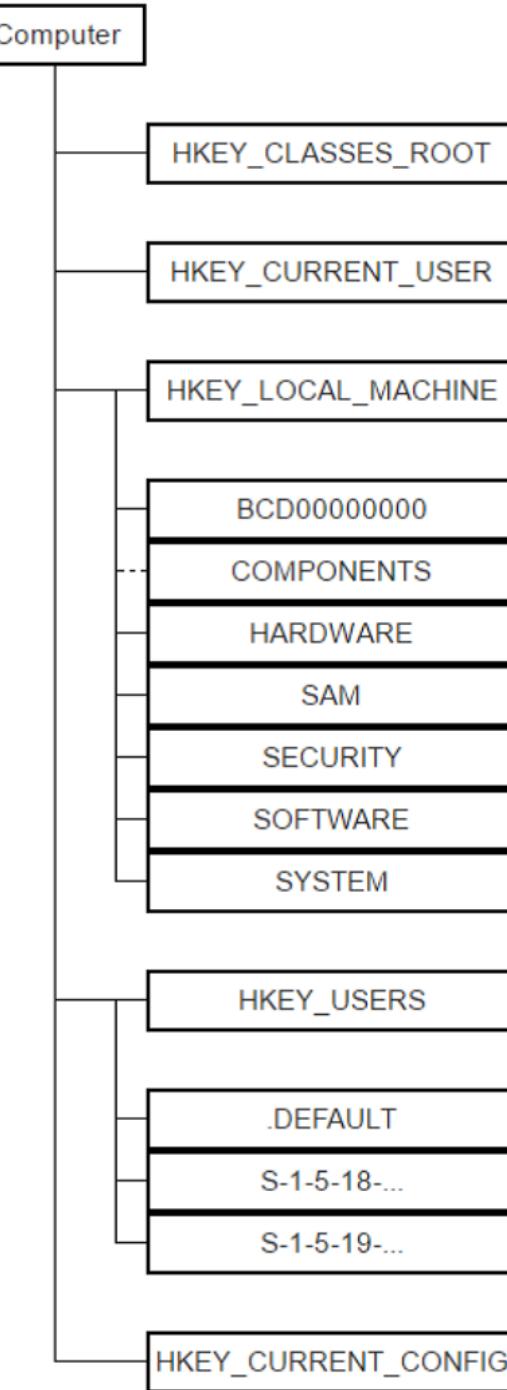
Registry Hauptschlüssel

- **HKEY_CLASSES_ROOT:** enthält Informationen über unterstützte Dateitypen des Rechners und die dazugehörigen Dateiendungen. Der Hauptschlüssel ist bei den neueren Windows-Versionen seit Windows 2000 nicht real, sondern eine Kombination aus:
HKEY_LOCAL_MACHINE\Software\Classes und
HKEY_CURRENT_USER\Software\Classes
- **HKEY_CURRENT_USER:** ist eine Spiegelung von:
HKEY_USERS\<Benutzer-SID> (des aktuell am System angemeldeten Benutzers)
- **HKEY_LOCAL_MACHINE:** speichert Einstellungen, die alle am System angemeldeten Benutzerkonten betreffen
HKEY_LOCAL_MACHINE wird auch HKLM abgekürzt

Registry Hauptschlüssel

- **HKEY_USERS** enthält die Schlüssel der einzelnen Benutzerkonten. Für jeden Benutzer ist dort ein eigener Unterschlüssel angelegt, benannt nach dem SID des jeweiligen Benutzerkontos. Diese Unterschlüssel sind Sammelstellen für alle Einstellungen, die nur für das jeweilige Benutzerkonto gelten. HKEY_USERS wird auch HKU abgekürzt
- **HKEY_CURRENT_CONFIG:** ist eine Spiegelung von HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\HardwareProfiles\Current

Registry



Hives

- **Binär-Dateien, über die die Registry-Einträge verteilt sind**
- **Die Dateien können nur mit speziellen Viewern, z.B. Regedit oder Auswertetools wie X-Ways ausgelesen werden**
- **Freeware:** <https://www.gaijin.at/en/files?dir=old-software>

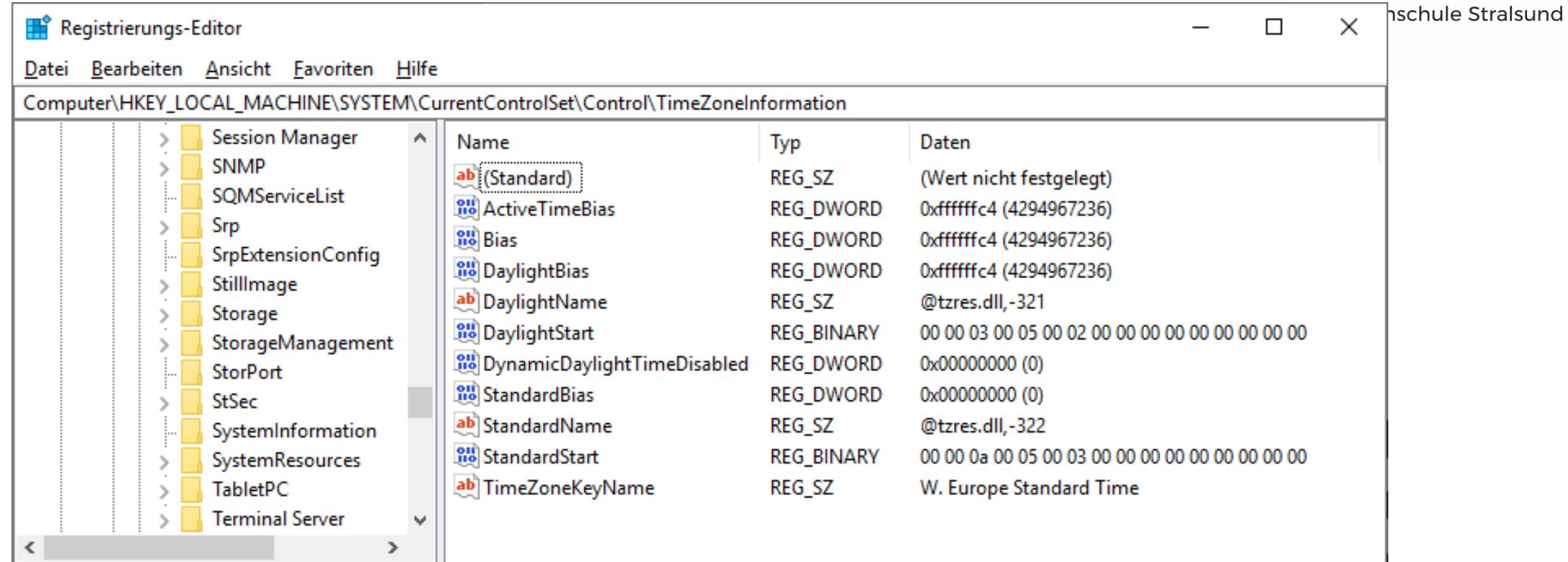
Hives

- **%systemdrive%\Users\%username%\NTUSER.DAT**
speichert die Keys unter HKEY_USERS und HKEY_CURRENT_USER
- **%systemroot%\System32\config\SAM**
speichert die Keys unter HKEY_LOCAL_MACHINE\SAM und enthält die Benutzerinformationen wie Anmeldename und Kennwort. SAM steht für Security Accounts Manager
- **%systemroot%\System32\config\SECURITY**
speichert die Keys unter HKEY_LOCAL_MACHINE\SECURITY. Speichert die systemweit gültigen Sicherheitsrichtlinien und Benutzerrechte
- **%systemroot%\System32\config\SYSTEM**
speichert die Keys unter HKEY_LOCAL_MACHINE\SYSTEM. Enthält Windows-Einstellungen, die bereits während des Bootens benötigt werden. Dazu gehören Einstellungen und Zustand der Treiber und Systemdienste
- **%systemroot%\System32\config\SOFTWARE**
speichert die Keys unter HKEY_LOCAL_MACHINE\SOFTWARE. Enthält systemweite Windows-Einstellungen, die nicht zum Booten benötigt werden, sowie Einstellungen der Anwendungsprogramme

Hives

- **%systemroot%\System32\config\.DEFAULT**
HKU\.DEFAULT und HKU\HKUnS-1-5-18 für User Local System
- **%systemroot%\ServiceProfiles\LocalService\Ntuser.dat**
HKU\HKU\S-1-5-19 für User Local Service
- **%systemroot%\ServiceProfiles\NetworkService\Ntuser.dat**
HKU\HKU\S-1-5-20 für User Network Service
- **\Device\HarddiskVolume1\Boot\BCD**
HKLM\BCD00000000 Konfiguration für den Bootloader
- **%systemroot%\System32\config\COMPONENTS**
HKLM\COMPONENTS Informationen über den Zustand von Windows-Features und Updates abgelegt
- **%systemroot%\System32\config\HARDWARE**
HKLM\HARDWARE Informationen über die Hardware, wird beim Systemstart neu generiert

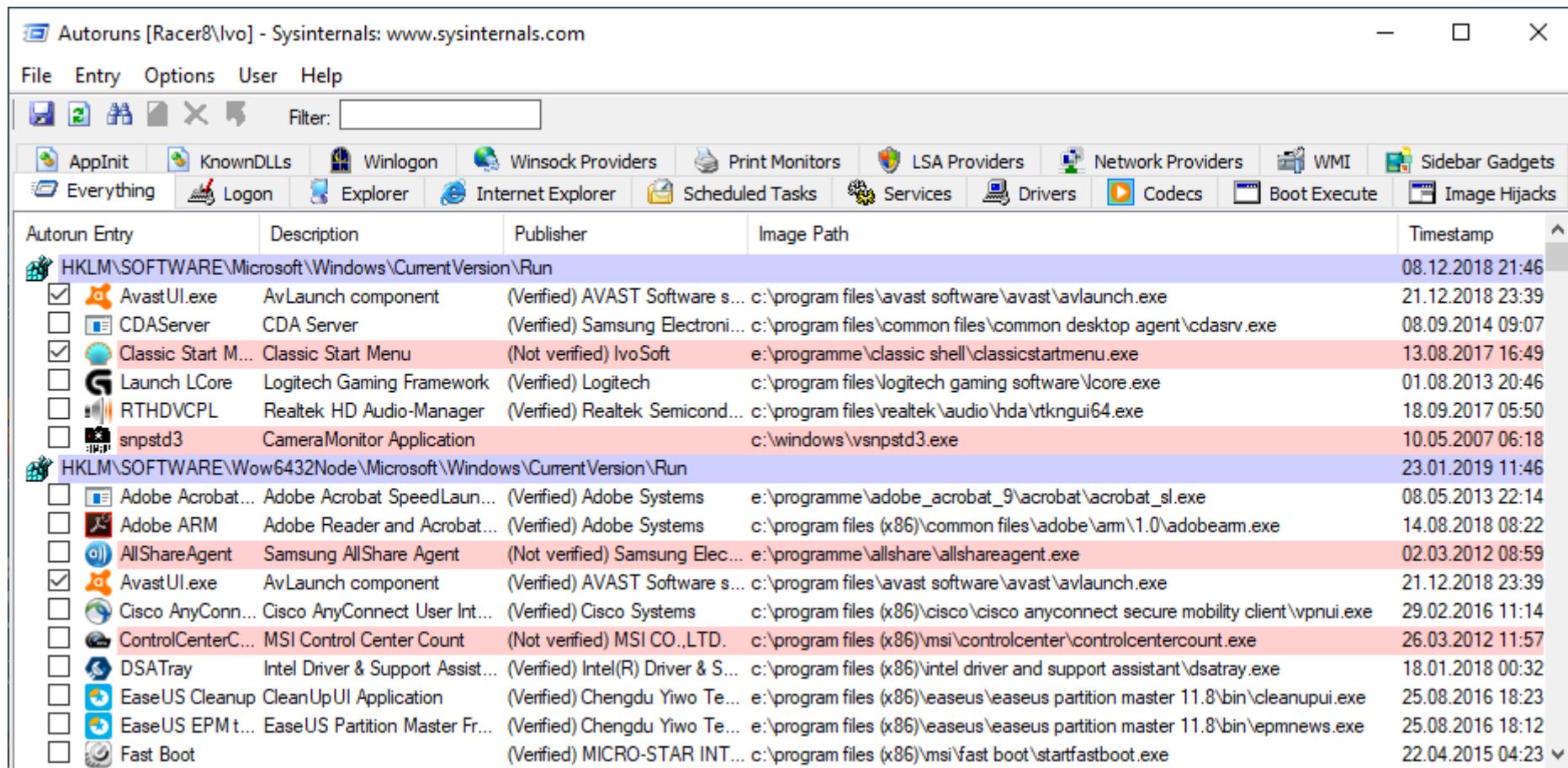
TimeZoneInformation



Der Zeitstempel zählt die Nanosekunden seit dem 01.01.1601

Local Time = UTC - ActiveTimeBias

Autorun Locations



The screenshot shows the Autoruns application interface. The menu bar includes File, Entry, Options, User, and Help. Below the menu is a toolbar with icons for AppInit, KnownDLLs, Winlogon, Winsock Providers, Print Monitors, LSA Providers, Network Providers, WMI, Sidebar Gadgets, Everything, Logon, Explorer, Internet Explorer, Scheduled Tasks, Services, Drivers, Codecs, Boot Execute, and Image Hijacks. A filter input field is also present. The main window displays two tables of autorun entries:

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
<input checked="" type="checkbox"/>	AvastUI.exe	AvLaunch component	(Verified) AVAST Software s... c:\program files\avast software\avaunch.exe	21.12.2018 23:39
<input type="checkbox"/>	CDA Server	CDA Server	(Verified) Samsung Electroni... c:\program files\common files\common desktop agent\cdasrv.exe	08.09.2014 09:07
<input checked="" type="checkbox"/>	Classic Start M...	Classic Start Menu	(Not verified) IvoSoft e:\programme\classic shell\classicstartmenu.exe	13.08.2017 16:49
<input type="checkbox"/>	Launch LCore	Logitech Gaming Framework	(Verified) Logitech c:\program files\logitech gaming software\lcore.exe	01.08.2013 20:46
<input type="checkbox"/>	RTHDVCPL	Realtek HD Audio-Manager	(Verified) Realtek Semicond... c:\program files\realtek\audio\vhd\vtkngui64.exe	18.09.2017 05:50
<input type="checkbox"/>	snpstd3	CameraMonitor Application	c:\windows\vsnpstd3.exe	10.05.2007 06:18
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				
<input type="checkbox"/>	Adobe Acrobat...	Adobe Acrobat SpeedLaun...	(Verified) Adobe Systems e:\programme\adobe_acrobat_9\acrobat\acrobat_sl.exe	08.05.2013 22:14
<input type="checkbox"/>	Adobe ARM	Adobe Reader and Acrobat...	(Verified) Adobe Systems c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe	14.08.2018 08:22
<input type="checkbox"/>	AllShareAgent	Samsung AllShare Agent	(Not verified) Samsung Elec... e:\programme\allshare\allshareagent.exe	02.03.2012 08:59
<input checked="" type="checkbox"/>	AvastUI.exe	AvLaunch component	(Verified) AVAST Software s... c:\program files\avast software\avaunch.exe	21.12.2018 23:39
<input type="checkbox"/>	Cisco AnyConn...	Cisco AnyConnect User Int...	(Verified) Cisco Systems c:\program files (x86)\cisco\cisco anyconnect secure mobility client\wpnui.exe	29.02.2016 11:14
<input type="checkbox"/>	ControlCenterC...	MSI Control Center Count	(Not verified) MSI CO.,LTD. c:\program files (x86)\msi\controlcenter\controlcentercount.exe	26.03.2012 11:57
<input type="checkbox"/>	DSATray	Intel Driver & Support Assist...	(Verified) Intel(R) Driver & S... c:\program files (x86)\intel driver and support assistant\dsatray.exe	18.01.2018 00:32
<input type="checkbox"/>	EaseUS CleanUp	CleanUp UI Application	(Verified) Chengdu Yiw... e:\program files (x86)\easeus\cleanups partition master 11.8\bin\cleanupui.exe	25.08.2016 18:23
<input type="checkbox"/>	EaseUS EPM t...	EaseUS Partition Master Fr...	(Verified) Chengdu Yiw... e:\program files (x86)\easeus\partition master 11.8\bin\epmnews.exe	25.08.2016 18:12
<input type="checkbox"/>	Fast Boot		(Verified) MICRO-STAR INT... c:\program files (x86)\msi\fast boot\startfastboot.exe	22.04.2015 04:23

Autorun Locations

HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce

HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce(Profile Path)\StartMenu\Programs\Startup

Most Recently Used

Suche

- Datei Suche:

HKCU\Software\Microsoft\Search Assistant\ACMru\5603

- Internet Search Assistant:

HKCU\Software\Microsoft\Search Assistant\ACMru\5001

- Drucker, Computer, Leute:

HKCU\Software\Microsoft\Search Assistant\ACMru\5647

- Media Player:

HKCU\Software\Microsoft\Search Assistant\ACMru\5604

Most Recently Used

Zuletzt verwendete Dateien (Startmenu):

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Recent Docs

Remote Desktop letzte Verbindungen:

HKCU\Software\Microsoft\Terminal Server Client\Default[MRUNumber]

Netzlaufwerke:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

Kommandozeile letzte Befehle:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Most Recently Used

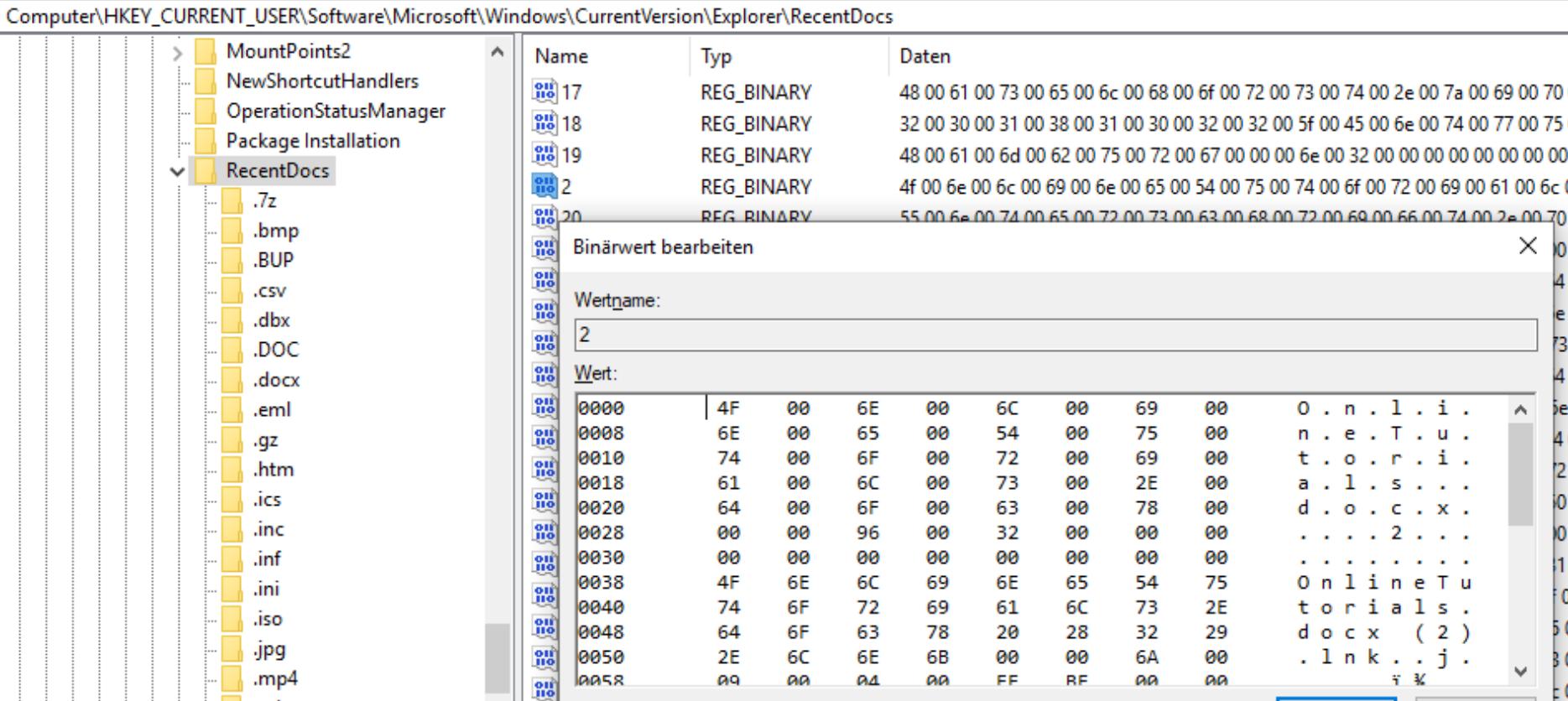
Zuletzt verwendete Dateien (Startmenu):

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Registrierungs-Editor

Datei Bearbeiten Ansicht Favoriten Hilfe

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Name	Typ	Daten
17	REG_BINARY	48 00 61 00 73 00 65 00 6c 00 68 00 6f 00 72 00 73 00 74 00 2e 00 7a 00 69 00 70
18	REG_BINARY	32 00 30 00 31 00 38 00 31 00 30 00 32 00 32 00 5f 00 45 00 6e 00 74 00 77 00 75
19	REG_BINARY	48 00 61 00 6d 00 62 00 75 00 72 00 67 00 00 00 6e 00 32 00 00 00 00 00 00 00 00
2	REG_BINARY	4f 00 6e 00 6c 00 69 00 6e 00 65 00 54 00 75 00 74 00 6f 00 72 00 69 00 61 00 6c 00
20	REG_BINARY	55 00 6e 00 74 00 65 00 72 00 73 00 63 00 68 00 72 00 69 00 66 00 74 00 2e 00 70

Binärwert bearbeiten

Wertname:

2

Wert:

Index	0000	0008	0010	0018	0020	0028	0030	0038	0040	0048	0050	0058
0000	4F	00	6E	00	6C	00	69	00	0 . n . 1 . i .			
0008	6E	00	65	00	54	00	75	00	n . e . T . u .			
0010	74	00	6F	00	72	00	69	00	t . o . r . i .			
0018	61	00	6C	00	73	00	2E	00	a . 1 . s . . .			
0020	64	00	6F	00	63	00	78	00	d . o . c . x .			
0028	00	00	96	00	32	00	00	00 2 . . .			
0030	00	00	00	00	00	00	00	00			
0038	4F	6E	6C	69	6E	65	54	75	o n l i n e T u			
0040	74	6F	72	69	61	6C	73	2E	t o r i a l s .			
0048	64	6F	63	78	20	28	32	29	d o c x (2)			
0050	2E	6C	6E	6B	00	00	6A	00	. l n k . . j .			
0058	09	00	04	00	FF	RF	00	00	i %			

OK Abbrechen

Most Recently Used

Remote Desktop letzte Verbindungen:

HKCU\Software\Microsoft\Terminal Server Client\Default[MRUNumber]

Netzlaufwerke:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

Kommandozeile letzte Befehle:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Regedit - Last accessed key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Most Recently Used

- Word - Recent Files:

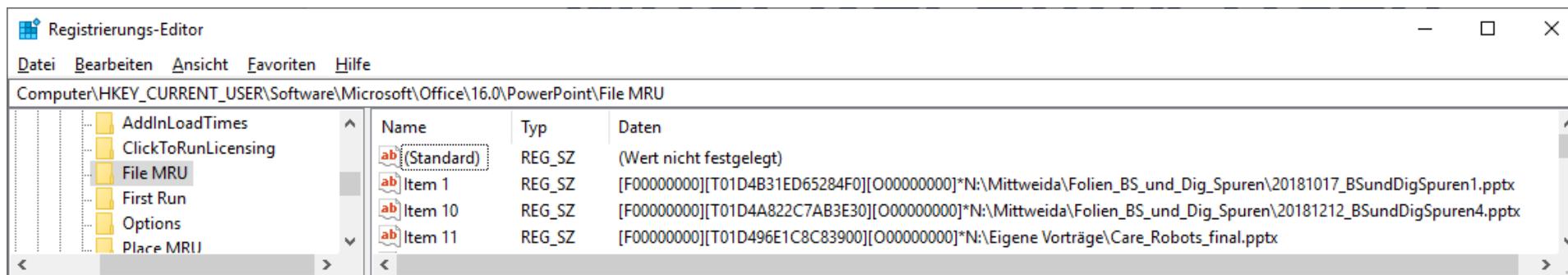
HKCU\Software\Microsoft\Office\10.0\Word\Data

- Excel - Recent Files:

Software\Microsoft\Officen10.0\Excel\Recent Files

- Power Point - Recent Files:

Software\Microsoft\Officen10.0\Powerpoint\Recent File List

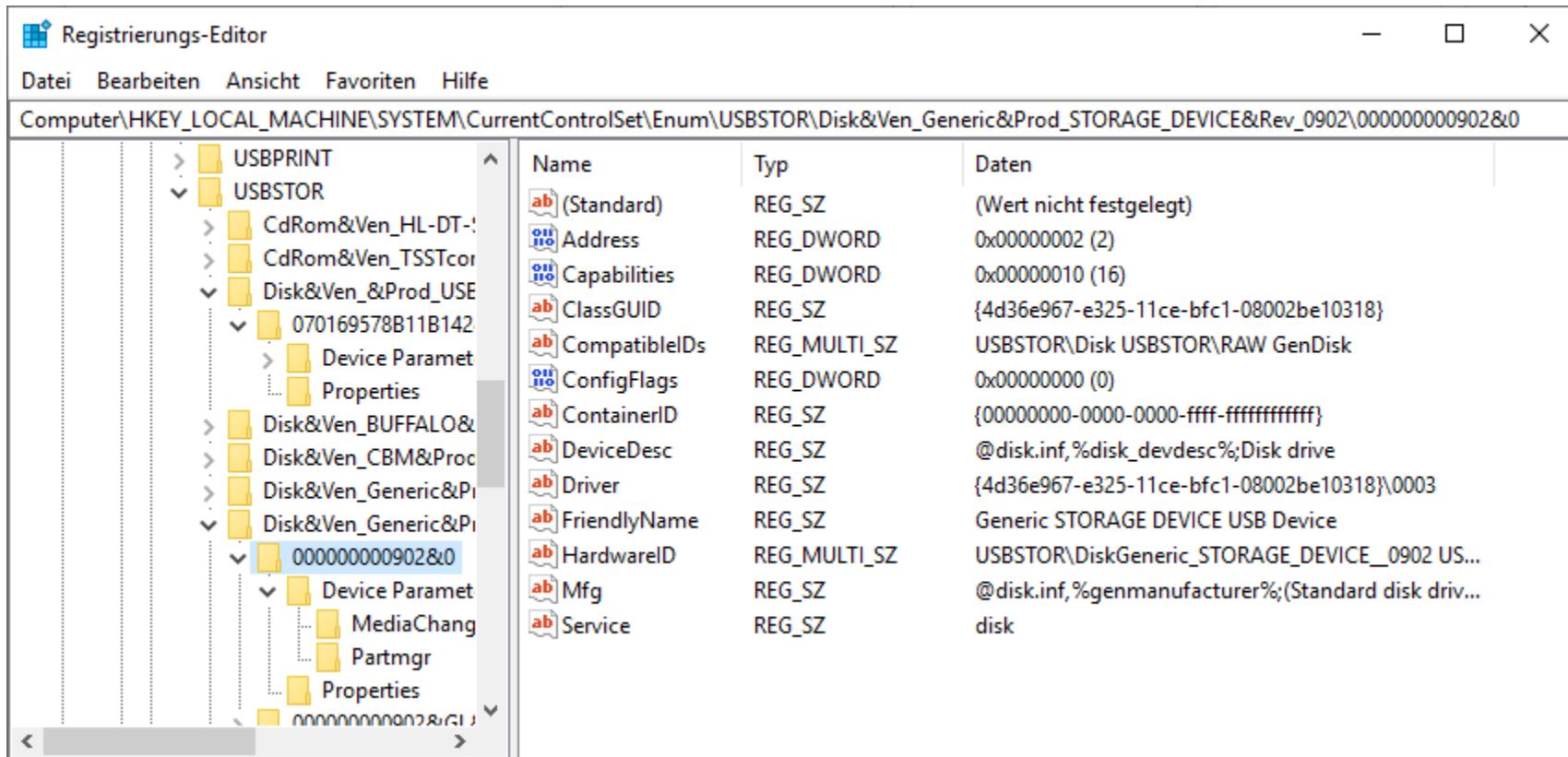


Mehr unter: <https://www.andreafortuna.org/cybersecurity/windows-registry-in-forensic-analysis/> und

<https://www.winhelponline.com/blog/run-mru-history-not-saved-windows/>

USB Devices

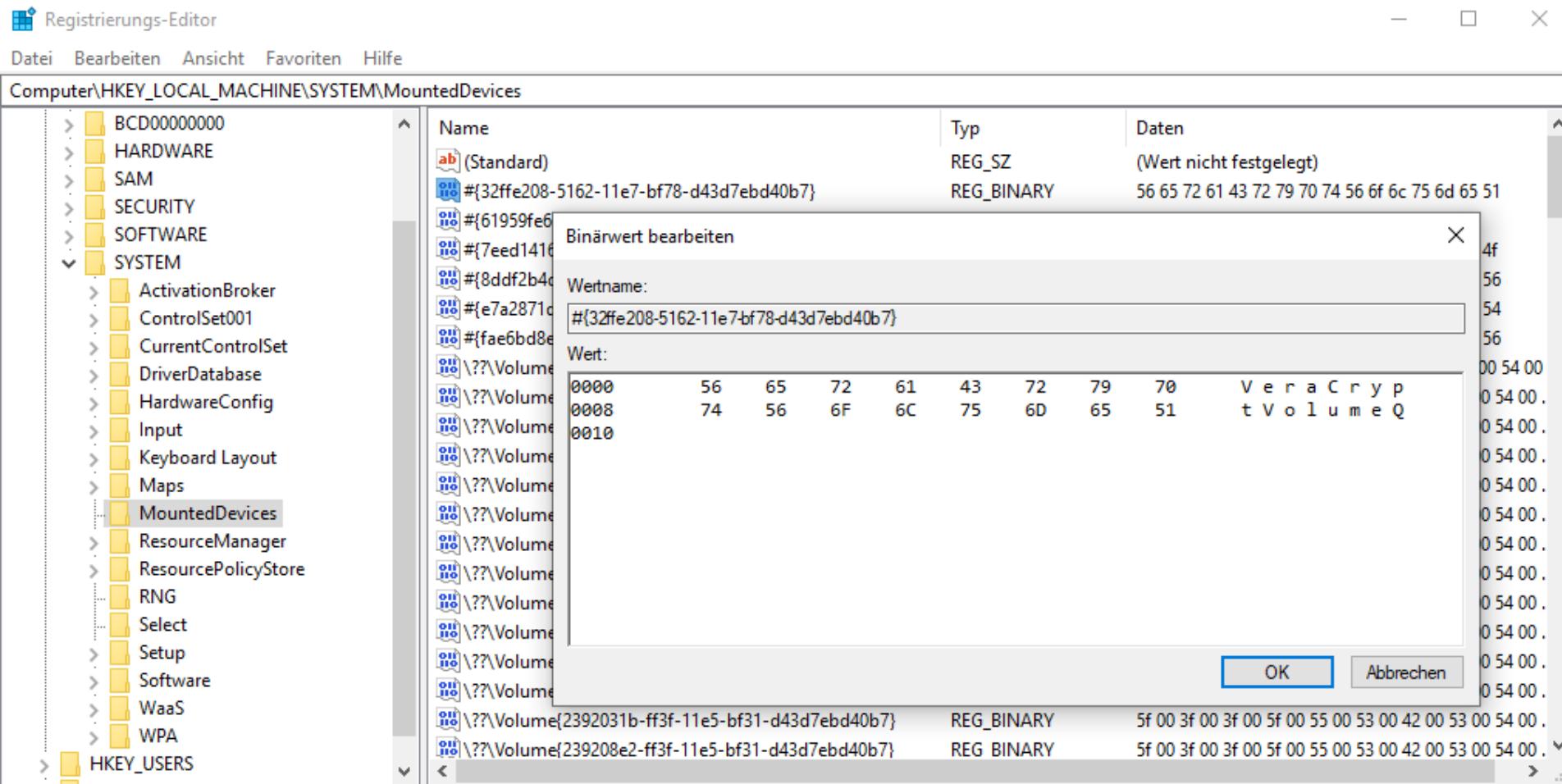
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
Address	REG_DWORD	0x00000002 (2)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffff}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0003
FriendlyName	REG_SZ	Generic STORAGE DEVICE USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskGeneric_STORAGE_DEVICE_0902 US...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv...
Service	REG_SZ	disk

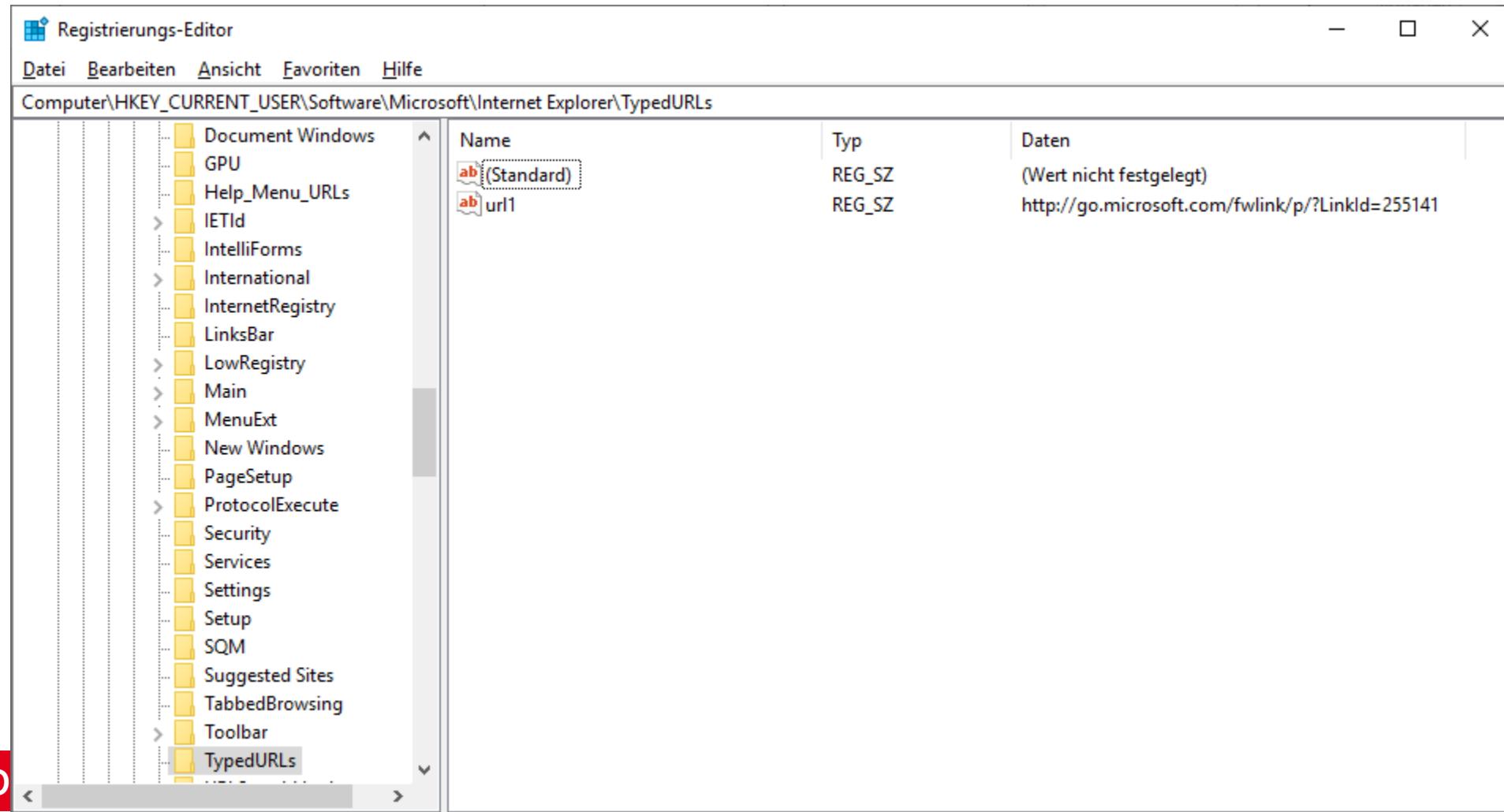
Laufwerke

HKLM\SYSTEM\MountedDevices



Webseiten

HKCU\Software\Microsoft\Internet Explorer\TypedURLs



Toolsammlung NirSoft

NirLauncher - NirSoft Utilities

File Edit View Options Launcher Packages Help

Password Recovery Utilities	Network Monitoring Tools	Web Browser Tools	Video/Audio Related Utilities
Internet Related Utilities	Command-Line Utilities	Desktop Utilities	Outlook/Office Utilities
Programmer Tools	Disk Utilities	System Utilities	Other Utilities
All Utilities			

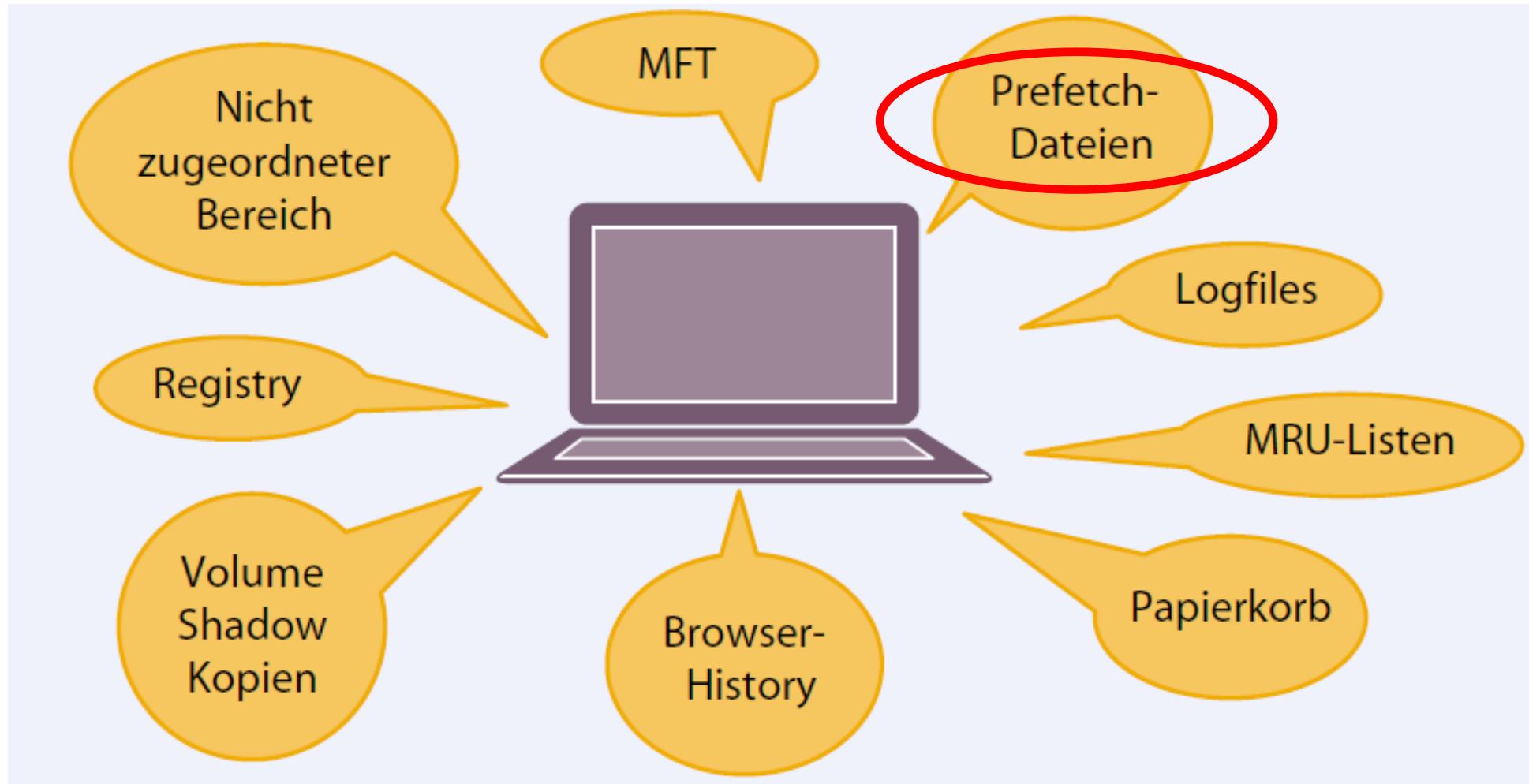
Name	Description	Version	Updated On	Web Page URL
MultiMonitorTool	Enable, disable, and set the primary monitor in Mu...	1.95	22.12.2018 12:14:18	http://www.nirsoft.net
DevManView	Alternative to the standard Device Manager of Wi...	1.56	13.12.2018 10:10:30	http://www.nirsoft.net
WinLogOnView	Displays logon/logoff times on Windows Vista/7/...	1.32	10.12.2018 17:32:24	http://www.nirsoft.net
FolderChangesView	Monitor folder/drive changes.	2.26	08.12.2018 19:46:12	http://www.nirsoft.net
ControlMyMonitor	View and modify the settings of your monitor.	1.11	07.12.2018 17:42:04	http://www.nirsoft.net
RegistryChangesView	Compares 2 snapshots of Windows Registry.	1.10	03.12.2018 18:05:54	http://www.nirsoft.net
AdvancedRun	Run a program with different settings that you ch...	1.07	02.12.2018 08:39:16	http://www.nirsoft.net
USBDeview	<u>Lists all installed USB devices that you previously ...</u>	2.78	28.11.2018 23:15:42	http://www.nirsoft.net
FullEventLogView	Event log viewer for Windows 10/8/7/Vista.	1.31	25.11.2018 16:03:36	http://www.nirsoft.net
InstalledPackagesView	Displays installed MSI packages on your system.	1.02	18.11.2018 10:15:54	http://www.nirsoft.net
UninstallView	Shows installed programs on your system and all...	1.24	16.11.2018 20:45:56	http://www.nirsoft.net
BulkFileChanger	Change date/time/attributes of multiple files.	1.52	12.11.2018 16:22:02	http://www.nirsoft.net
AppCrashView	Displays the details of all application crashes occu...	1.35	10.11.2018 08:42:42	http://www.nirsoft.net
TurnedOnTimesView	View the time/date ranges that your computer wa...	1.40	02.11.2018 16:14:30	http://www.nirsoft.net
MonitorInfoView	displays essential information about your monitor.	1.21	06.10.2018 11:05:20	http://www.nirsoft.net
SimpleWMIView	Displays the result of WMI queries in a simple table	1.23	21.09.2018 16:13:50	http://www.nirsoft.net

Run Advanced Run Web Page Help File Web Search Package Package

76 Utilities, 1 Selected NirSoft Freeware. <http://www.nirsoft.net>

Siehe auch: <https://www.gaijin.at/de/>

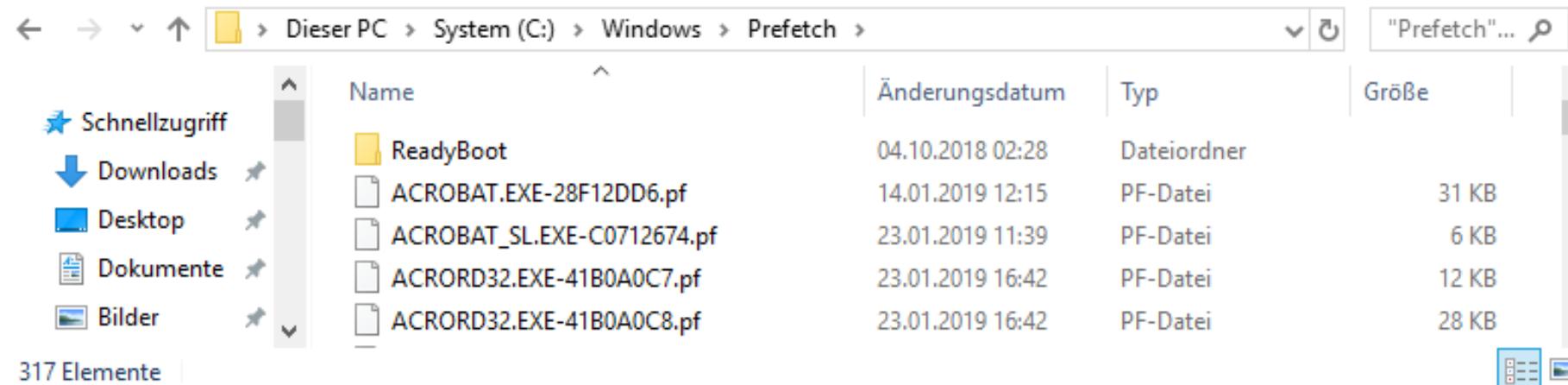
Der Computer als Zeuge



Windows Prefetching

- Speicherinhalte einer Applikation werden im voraus geladen, um den Programmstart zu beschleunigen
- Prefetch-Dateien speichern eine Anzahl für die Computer-Forensik relevanten Daten
- unter anderem Zeitstempel und einen Counter für Programmstarts
- **%SystemRoot%\Prefetch**

Windows Prefetching



A screenshot of a Windows File Explorer window. The address bar shows the path: Dieser PC > System (C:) > Windows > Prefetch. The left sidebar shows icons for Schnellzugriff, Downloads, Desktop, Dokumente, and Bilder. The main area displays a list of files and folders in the Prefetch folder. The columns are Name, Änderungsdatum, Typ, and Größe. The list includes:

Name	Änderungsdatum	Typ	Größe
ReadyBoot	04.10.2018 02:28	Dateiordner	
ACROBAT.EXE-28F12DD6(pf)	14.01.2019 12:15	PF-Datei	31 KB
ACROBAT_SL.EXE-C0712674(pf)	23.01.2019 11:39	PF-Datei	6 KB
ACRORD32.EXE-41B0A0C7(pf)	23.01.2019 16:42	PF-Datei	12 KB
ACRORD32.EXE-41B0A0C8(pf)	23.01.2019 16:42	PF-Datei	28 KB

317 Elemente

Windows Prefetching

- Die Dateinamen der Prefetch-Dateien enthalten den Namen der zugehörigen Applikation, gefolgt von einem Bindestrich und einem 8 Byte langem Hash und der .pf Dateierweiterung
- Der Name ist stets uppercase mit Ausnahme der Dateierweiterung
- Beispiele:
ACORD32.EXE-1CE22EA3.pf
CHMOD.EXE-371390CD.pf

Windows Prefetching

- Beispiele:
ACRORD32.EXE-1CE22EA3(pf)
CHMOD.EXE-371390CD(pf)
- Der Hash kodiert den Pfad in dem die Applikation ausgeführt wurde
- wurde die Applikation mehrmals an unterschiedlichen Positionen ausgeführt, können auch mehrere Prefetch-Dateien zu einer Applikation existieren

Windows Prefetching

```
sub hash_xp
{
    my $devpath_u = shift;
    my $hash = 0;
    for (my $i=0; $i<length($devpath_u); $i++)
    {
        my $char = ord(substr($devpath_u,$i,1));
        $hash = ( ($hash * 37) + $char ) % 4294967296;
        #print STDERR sprintf("%08lx",$hash).' '.substr($devpath_u,$i,1)."\n"
    }
    $hash = ($hash * 314159269) % 4294967296;

    $hash = 0x100000000-$hash if ($hash>0x80000000);
    $hash = (abs($hash) % 1000000007) % 4294967296;
    return $hash;
}
```

Perl Sub, die den CcPfHashValue berechnet (Code: Hexacorn.com)

Prefetch-Dateien

- Jede Prefetch Datei hat eine 4-Byte Signatur an Offset 4 "SCCA" (oder in hexadecimaler Notation 0x53 43 43 41).
- Der Signatur ist ein 4-Byte großer Format Version Indicator vorangestellt:
 - 17 (= 0x00000011) für Windows XP und Windows 2003
 - 23 (= 0x00000017) für Windows Vista und Windows 7
 - 26 (= 0x0000001a) für Windows 8.1
 - 30 (= 0x0000001e) für Windows 10 (die Dateien sind komprimiert und müssen erst entpackt werden)*
- Jede Version hat ein unterschiedliches Format!

*<http://digitalforensicssurvivalpodcast.com/2016/12/06/dfsp-042-windows-10-prefetch/>

Prefetch-Datei-Header

Offset	Größe	Beschreibung
0x0000	4	Format Version Indicator
0x0004	4	Signatur "SCCA"
0x0008	4	Unbekannt
0x000C	4	Größe der Prefetch Datei
0x0010	60	Name der Executable in UTF16LE
0x004C	4	PF-Hash
0x0050	4	Unbekannt

Prefetch File Information Header

Offset	Größe	Beschreibung
0x0054	4	Offset zu Sektion A (Ab Dateianfang)
0x0058	4	Anzahl der Einträge in Sektion A
0x005C	4	Offset zu Sektion B (Ab Dateianfang)
0x0060	4	Anzahl der Einträge in Sektion B
0x0064	4	Offset zu Sektion C (Ab Dateianfang)
0x0068	4	Anzahl der Einträge in Sektion C
0x006C	4	Offset zu Sektion D (Ab Dateianfang)
0x0070	4	Anzahl der Einträge in Sektion D
0x0074	4	Länge der Sektion D
0x0078	8	Unbekannt
0x0080	8	Zeitstempel der letzten Ausführung der Executable
0x0088	7x8=56	Zeitstempel der 7 letzten Ausführungen davor
0x00C0	16	Unbekannt
0x00D0	4	Counter - Anzahl der Ausführungen
0x00D4	4	Unbekannt
0x00D8	4	Unbekannt
0x00DC	88	Unbekannt

Sektion A: File Metrics Record

Offset	Größe	Beschreibung
0x0000	4	Dauer der Programmstarts in ms
0x0004	4	Laufzeit des Programms in ms
0x0008	4	Durchschnittliche Laufzeit des Programms in ms
0x000C	4	Offset zum Filename in Sektion C
0x0010	4	Anzahl Chars im Filename
0x0014	4	Unbekannt
0x0018	8	Offset auf Executable im NTFS-Dateisystem (sonst 0)

Sektion C

**Sektion C enthält eine Liste aller Executables und
Bibliotheken, die nachgeladen wurden**

Sektion D

- **Enthält die Volumes Informations**
- **Wenn die Applikation und alle nachgeladenen Executables und Bibliotheken von einem Volume stammen enthält Sektion D nur eine Volume Information**
- **Falls sie von mehreren Volumes stammen, gibt es mehrere Volume Informations**
- **Sektion D enthält zwei Untersektionen Sektion E und Sektion F**

Sektion D

Offset	Größe	Beschreibung
+0x0000	4	Offset zum Volume Device Pfad
+0x0004	4	Länge des Volume Device Pfad
+0x0008	8	Volume Creation Time
+0x0010	4	Volume Serial Number
+0x0014	4	Offset zur Untersektion E
+0x0018	4	Länge der Untersektion E
+0x001C	4	Offset zur Untersektion F
+0x0020	4	Anzahl der Strings in Untersektion F
+0x0024	4	Unbekannt
+0x0028	28	Unbekannt
+0x0044	4	Unbekannt
+0x0048	28	Unbekannt
+0x0064	4	Unbekannt

Untersektionen E und F

- **Untersektion E enthält Pointer auf die einzelnen Executables und Bibliotheken im NTFS Dateisystem**
- **Untersektion F enthält die Verzeichnisse der Executables und Bibliotheken als Unicode Strings**

Wichtig

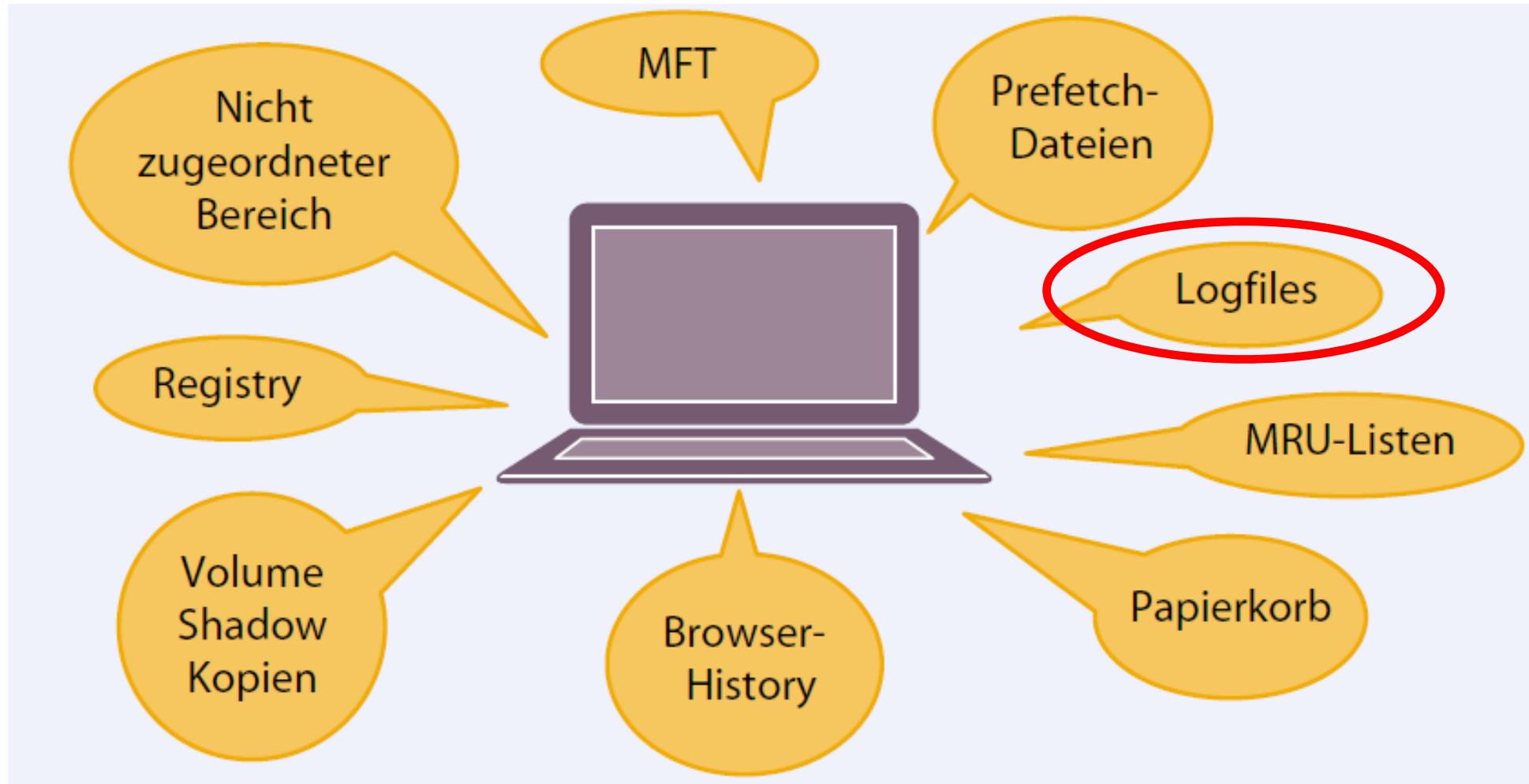
- Prefetching lässt sich in der Registry abschalten:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
EnablePrefetcher Value auf 0 setzen
- Prefetch-Dateien können Aufschluss über U3-verschlüsselte USB-Sticks geben

Filename	Created	Modified	Accessed		
LAUNCHU3.EXE-XXXXXXX.pf	2/5/2007	13:56	2/13/2007	5:52	
2/13/2007 5:52					
LAUNCHPAD.EXE-XXXXXXX.pf	2/5/2007	13:57	2/13/2007	5:52	
2/13/2007 5:52					
CLEANUP.EXE-XXXXXXX.pf	2/12/2007	21:54	2/13/2007	7:01	
2/13/2007 7:01					

Stick war am 05.02.2007 von 13:56 bis 21:54 angeschlossen und entschlüsselt

Stick war am 13.02.2007 von 5:52 bis 7:01 angeschlossen und entschlüsselt

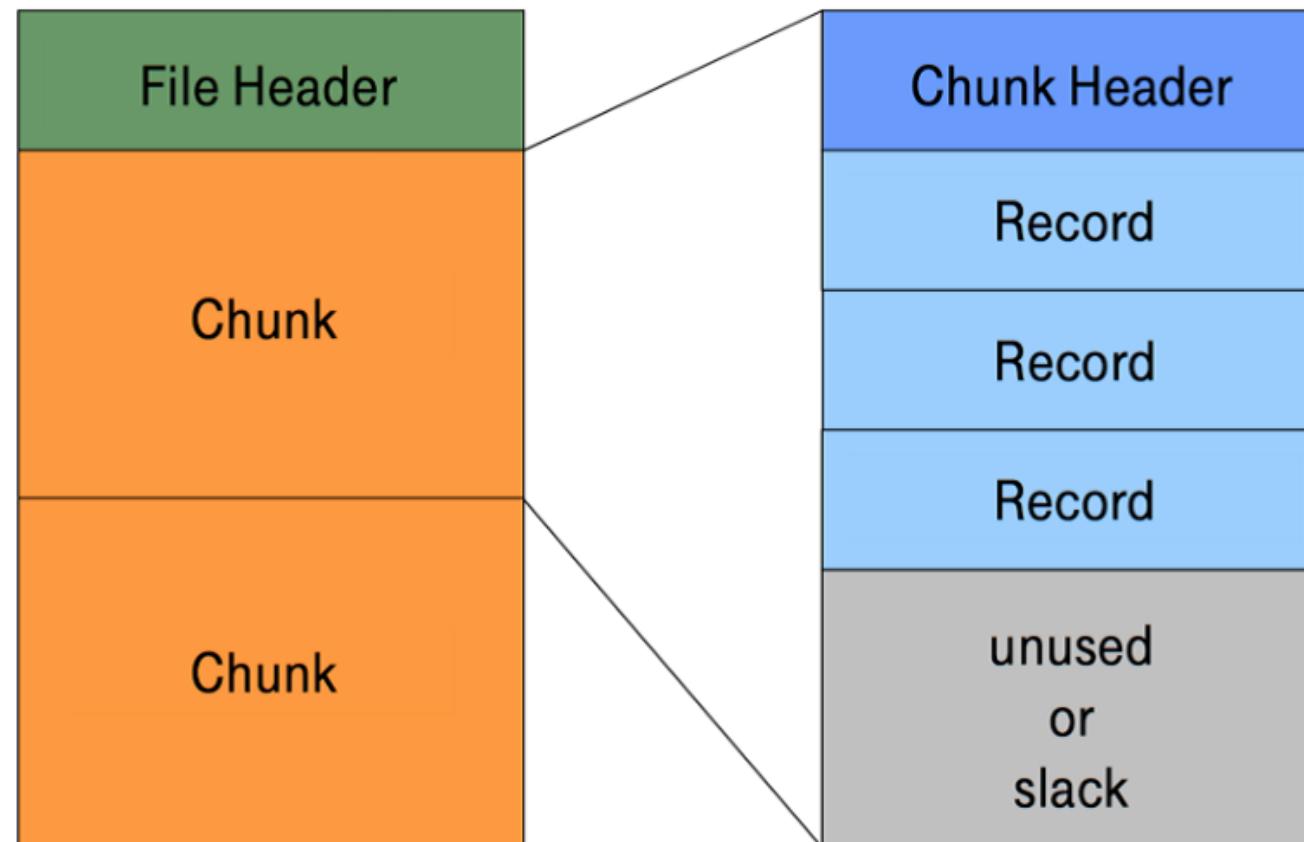
Der Computer als Zeuge



Eventlogs

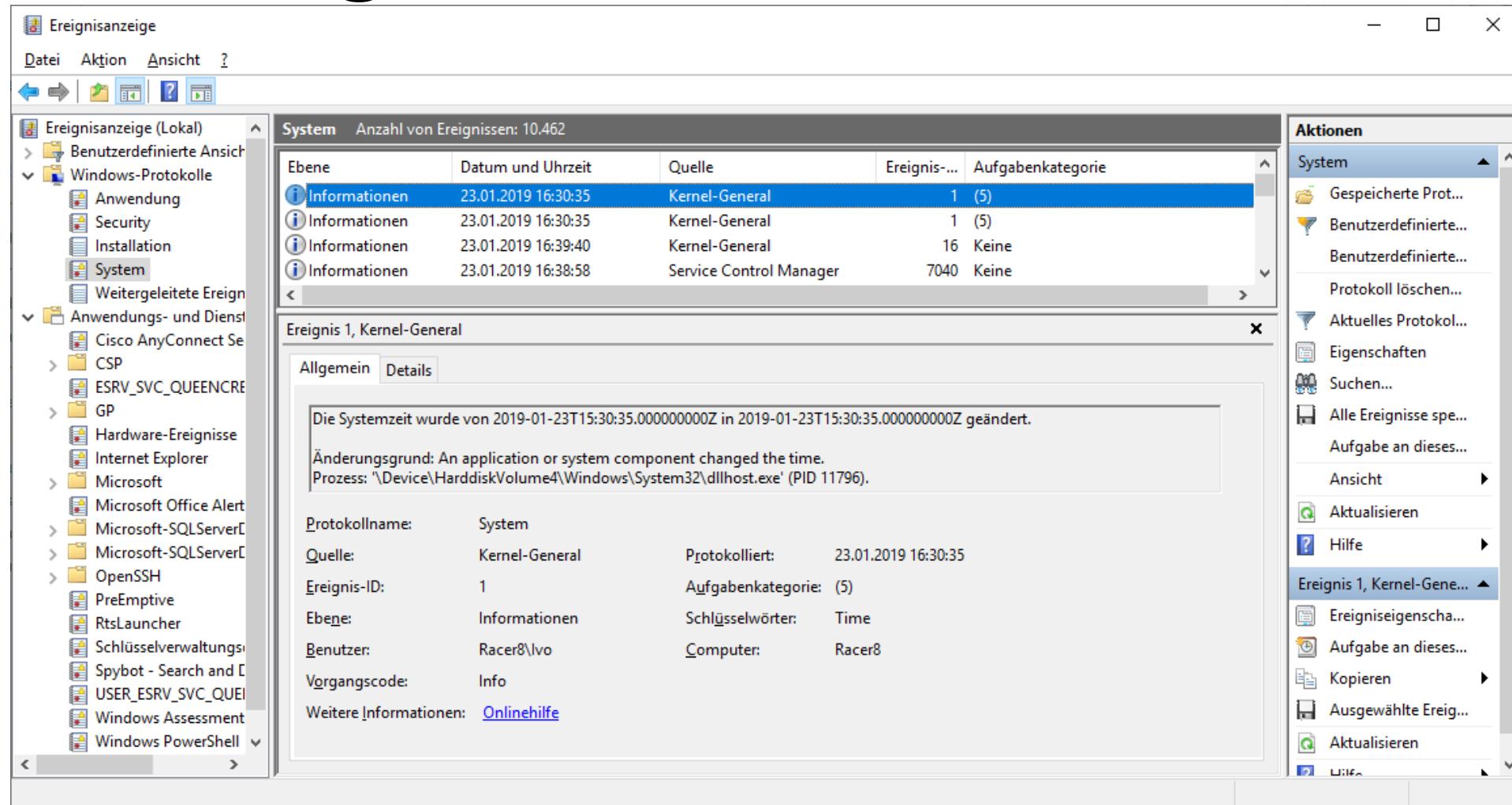
- **bis WinXP: %System%\system32\config**
- **ab Vista: %System%\system32\winevt\logs**
- **Es gibt viel mehr Log-Dateien (einfaches Win 7 > 60; einfaches Win 10 > 250)**
 - Application.evtx
 - System.evtx
 - Security.evtx
 - HardwareEvents.evtx
 - InternetExplorer.evtx
 - MediaCenter.evtx

Eventlogs



Hummert (2017)

Eventlog-Viewer



The screenshot shows the Windows Eventlog Viewer interface. The left pane displays a tree view of log sources, with 'Windows-Protokolle' expanded to show 'System'. The main pane shows a list of events under the 'System' category, with four entries visible:

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	23.01.2019 16:30:35	Kernel-General	1 (5)	
Informationen	23.01.2019 16:30:35	Kernel-General	1 (5)	
Informationen	23.01.2019 16:39:40	Kernel-General	16	Keine
Informationen	23.01.2019 16:38:58	Service Control Manager	7040	Keine

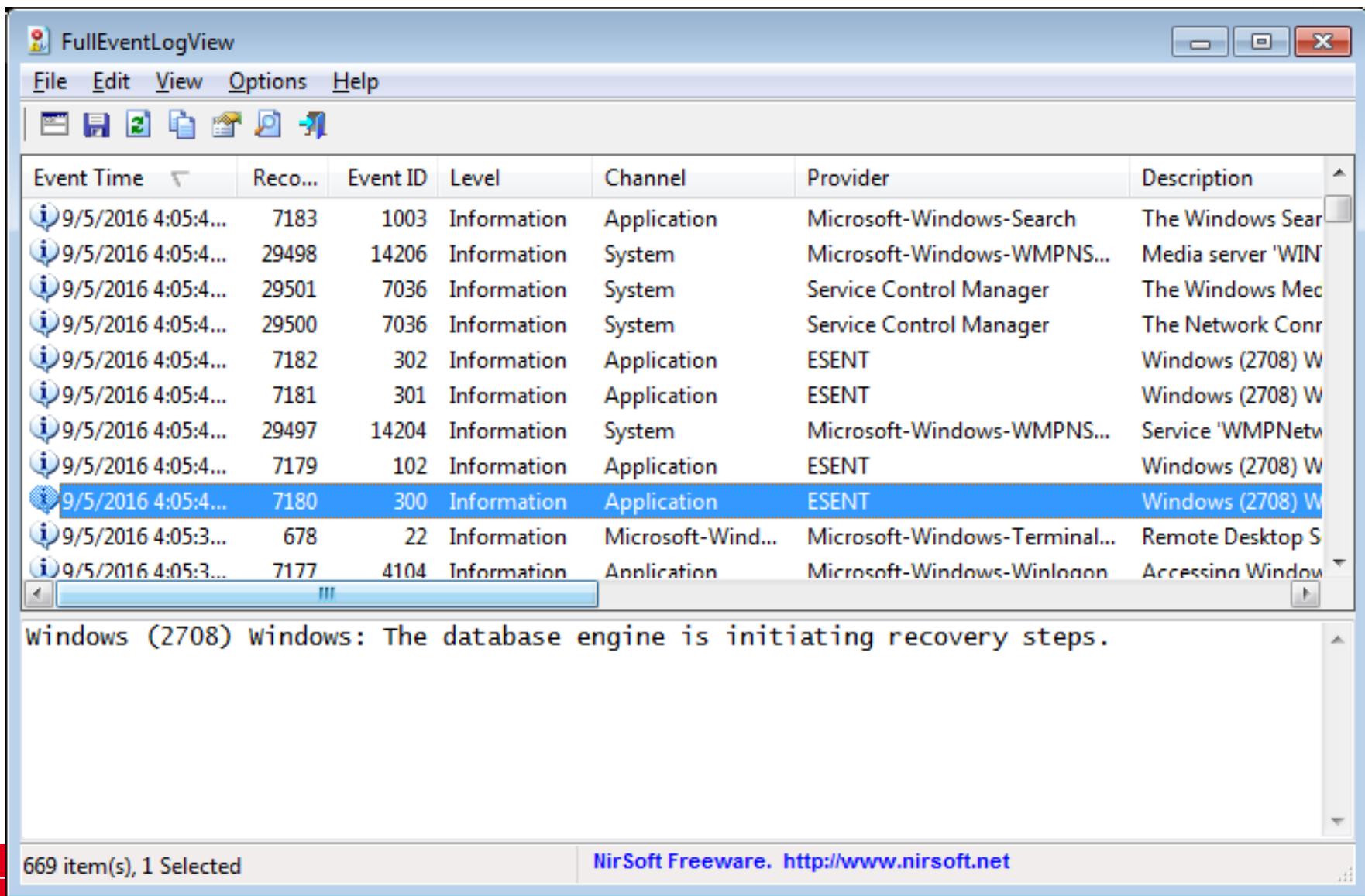
The details for the first event ('Ereignis 1, Kernel-General') are shown in the center pane. The 'Allgemein' tab is selected, displaying the following information:

Die Systemzeit wurde von 2019-01-23T15:30:35.000000000Z in 2019-01-23T15:30:35.000000000Z geändert.
Änderungsgrund: An application or system component changed the time.
Prozess: '\Device\HarddiskVolume4\Windows\System32\dllhost.exe' (PID 11796).

Protocol name: System
Source: Kernel-General
Logged: 23.01.2019 16:30:35
Event ID: 1
Category: (5)
Level: Information
User: Racer8\lvo
Computer: Racer8
Process: \Device\HarddiskVolume4\Windows\System32\dllhost.exe (PID 11796)
Timestamp: 2019-01-23T15:30:35.000000000Z

The right pane shows a context menu titled 'Aktionen' (Actions) with various options like 'Gespeicherte Prot...' (Saved Log), 'Protokoll löschen...' (Delete Log), and 'Aktuelles Protokol...' (Current Log). The 'Ereignis 1, Kernel-General' entry is also listed in the action history.

Eventlog-Viewer



The screenshot shows the 'FullEventLogView' window of the Eventlog-Viewer application. The window has a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for opening files, saving, and filtering. A table lists 12 log entries. The columns are: Event Time, Reco..., Event ID, Level, Channel, Provider, and Description. The entries are as follows:

Event Time	Reco...	Event ID	Level	Channel	Provider	Description
9/5/2016 4:05:4...	7183	1003	Information	Application	Microsoft-Windows-Search	The Windows Sear...
9/5/2016 4:05:4...	29498	14206	Information	System	Microsoft-Windows-WMPNS...	Media server 'WIN'
9/5/2016 4:05:4...	29501	7036	Information	System	Service Control Manager	The Windows Med...
9/5/2016 4:05:4...	29500	7036	Information	System	Service Control Manager	The Network Con...
9/5/2016 4:05:4...	7182	302	Information	Application	ESENT	Windows (2708) W...
9/5/2016 4:05:4...	7181	301	Information	Application	ESENT	Windows (2708) W...
9/5/2016 4:05:4...	29497	14204	Information	System	Microsoft-Windows-WMPNS...	Service 'WMPNetw...
9/5/2016 4:05:4...	7179	102	Information	Application	ESENT	Windows (2708) W...
9/5/2016 4:05:4...	7180	300	Information	Application	ESENT	Windows (2708) W...
9/5/2016 4:05:3...	678	22	Information	Microsoft-Wind...	Microsoft-Windows-Terminal...	Remote Desktop S...
9/5/2016 4:05:3...	7177	4104	Information	Annlication	Microsoft-Windows-WinInet...	Accessing Window...

A status message at the bottom left says "Windows (2708) Windows: The database engine is initiating recovery steps." The bottom right shows "669 item(s), 1 Selected". The footer also includes the NirSoft Freeware link.

Beispiel für einen Vorfall: Konboot



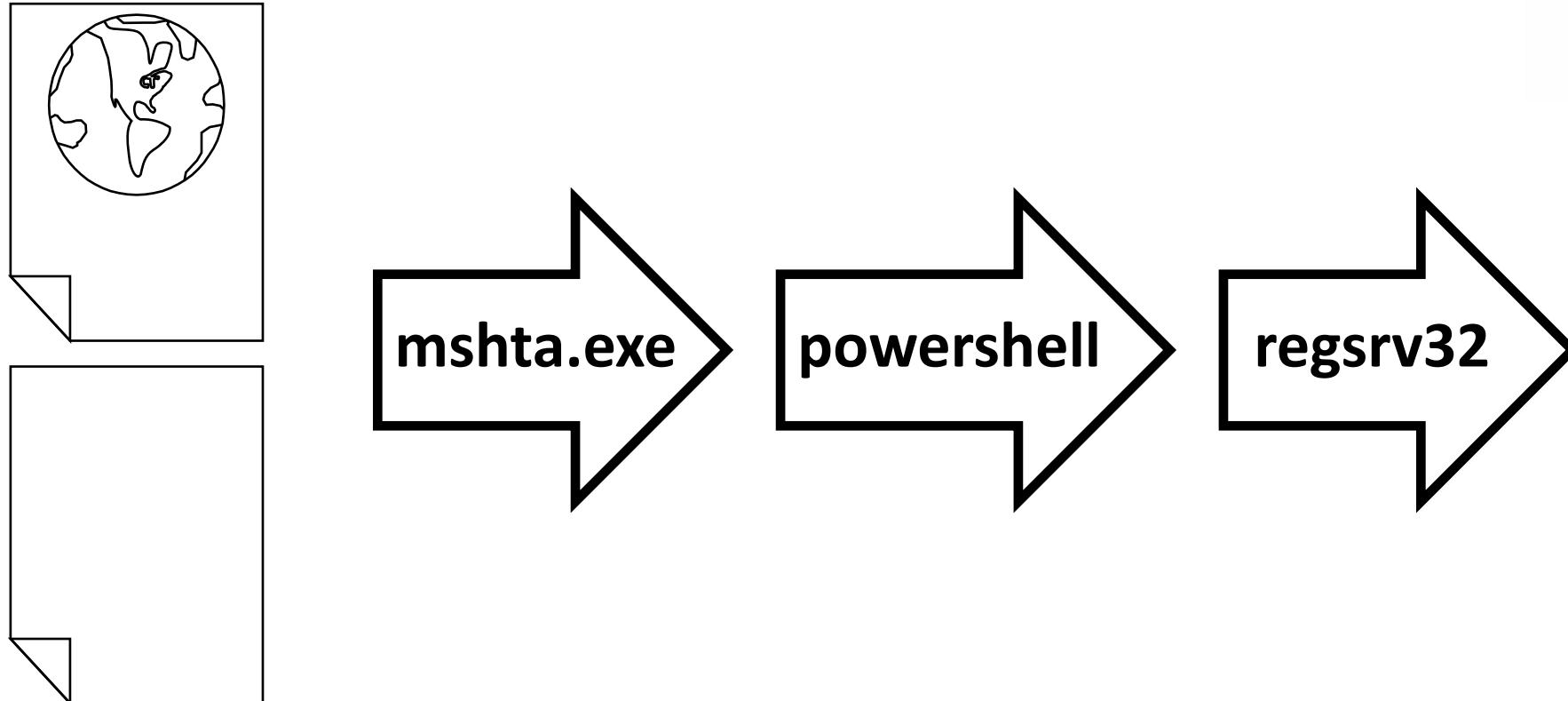
Arbeitsspeicher-Forensik



Wonach suche ich?

- Prozesse
- Passwörter
- Systemhinweise
- Texte
- Treiber
- Logs
- Bilder
- Schadsoftware

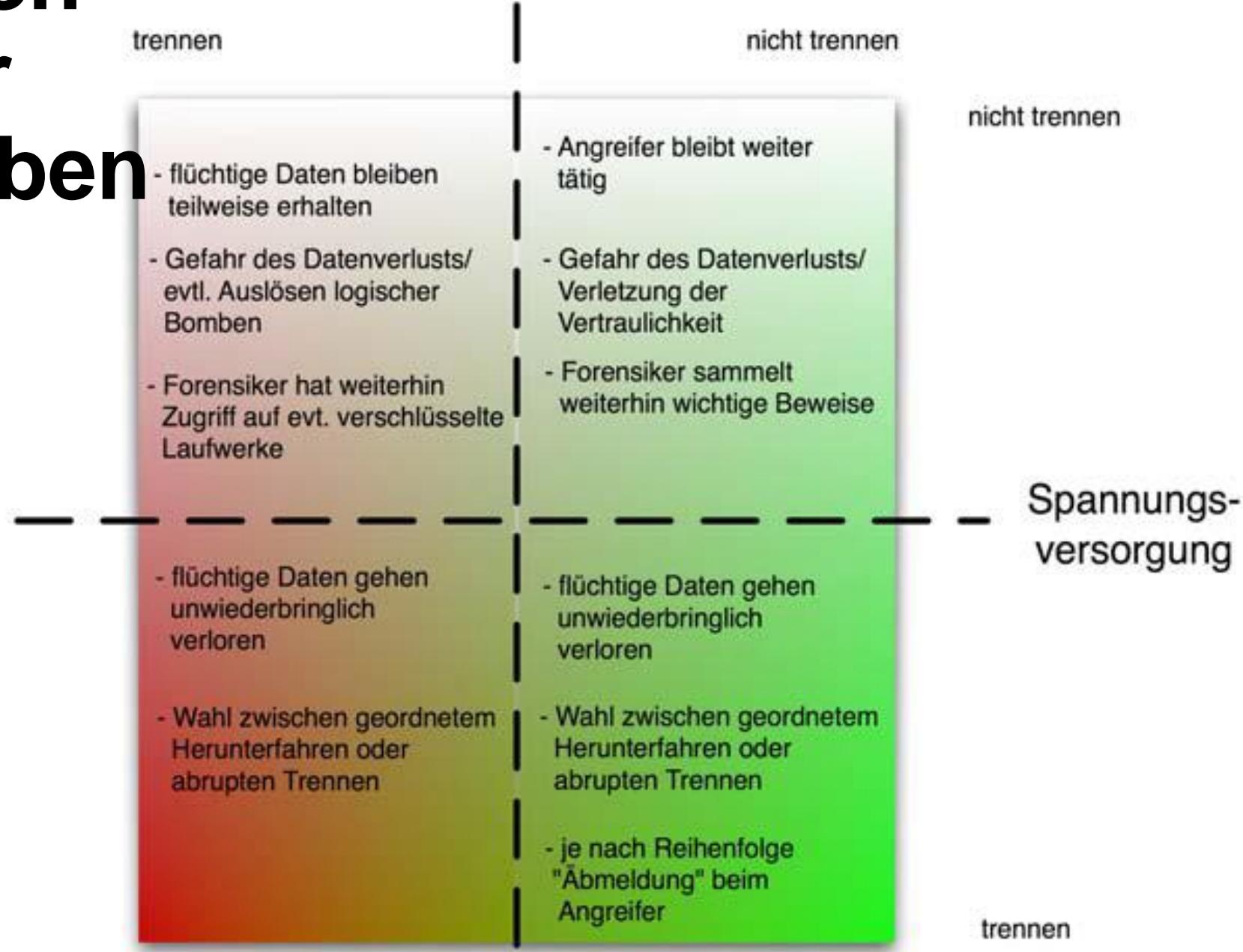
Fileless Malware



Quelle: aeksecurity.tech

Leben oder Sterben

Netzverbindung



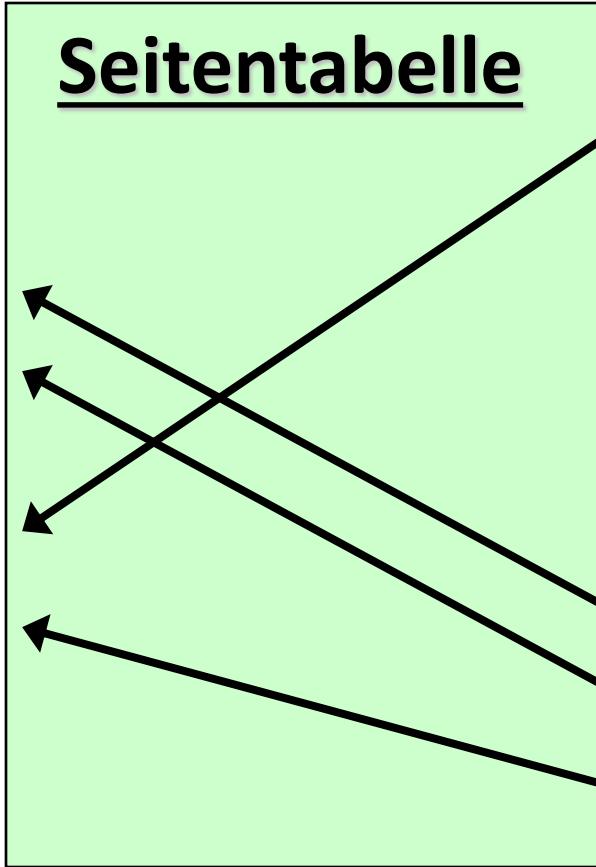
Live vs Post Mortem: Flüchtigkeit

- CPU Register, CPU Cache
- Routing-Tabellen, ARP-Caches, Prozesstabellen, Kernel Statistiken
- Arbeitsspeicherinhalt
- geöffnete, verschlüsselte Dateisysteme
- temporäre Dateisysteme (z.B. Cloudspeicher)
- entfernt geführte Logging- und Monitordaten
- Massenspeicherinhalte
- physische Konfiguration, Netzwerktopologie
- Archivmedien

Virtueller Speicher

00000	1
Programm	2
	3
	4
	5
Programm	6
Seitenrahmen	7
Frame	8
Kachel	9
Programm	10
	11
65536	12

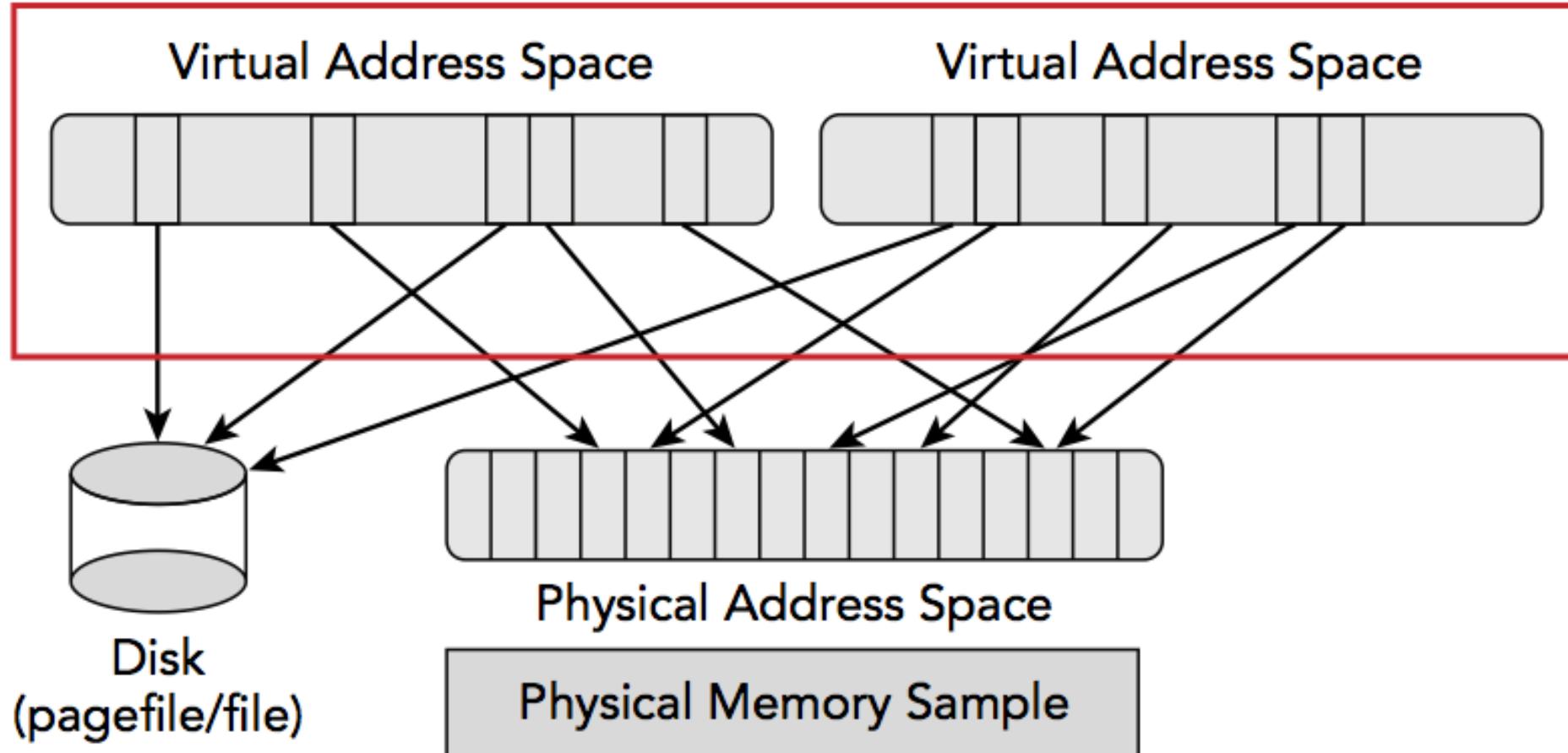
Fragmentierter
endlicher Speicher



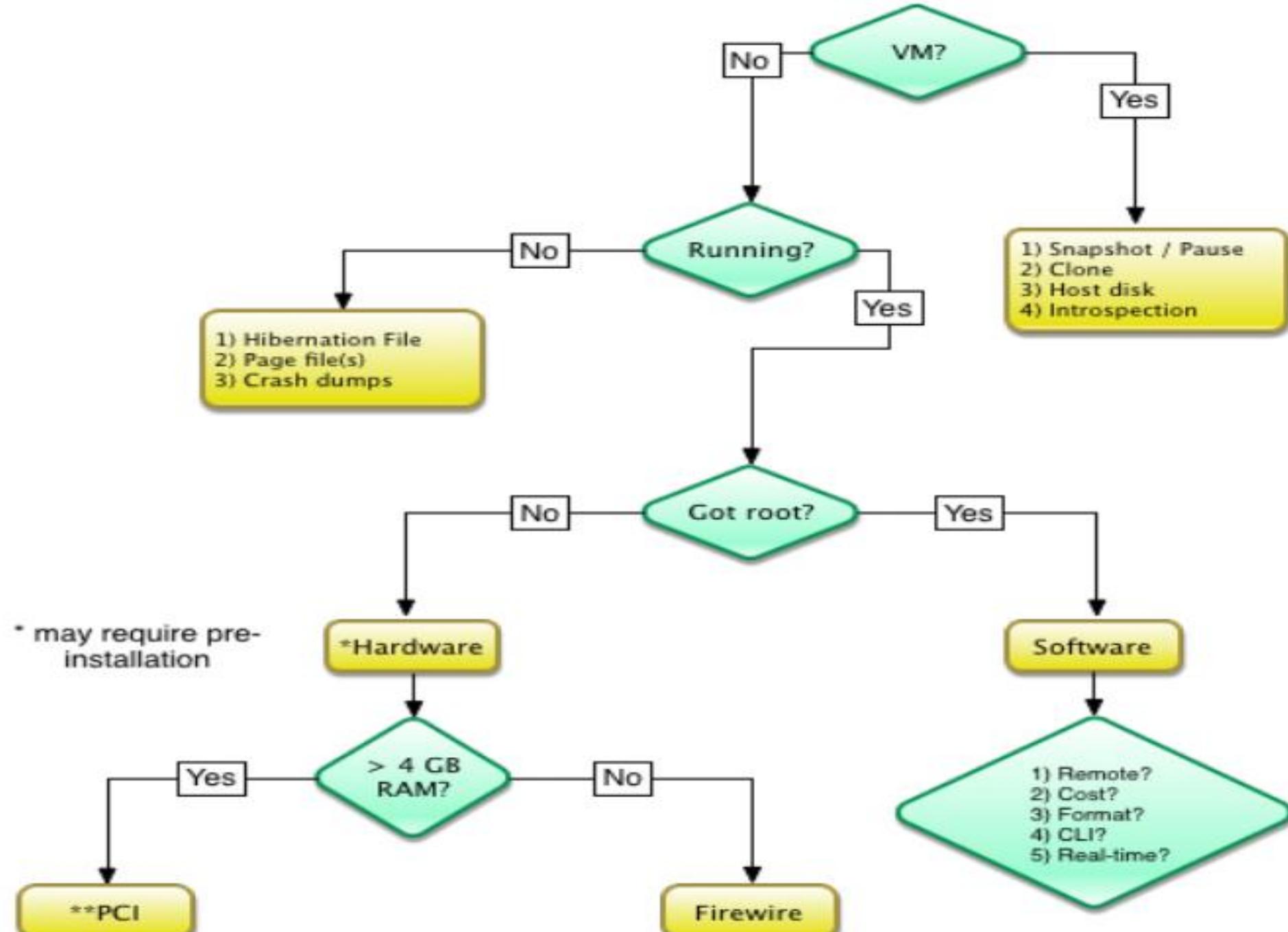
00000	1
	2
	3
	4
Seite	5
	6
	7
	8
	9
	10
	...
	n

Beliebig langer, durch-
gehender Speicher

Virtueller Speicher



Glendowne/Pape 2018



Arbeitsspeicher-Forensik

1. Speicherabbild erstellen

- RAW memory dump z. B. mit Dumpl
- Swap Drive Imaging
- Crash Dumps
- Virtual Machine Dumps
- Pagefile, Swapfile, Hibernate

2. Abbild auswerten, z. B. mit

- Volatility
- Bulk Extractor

Speichersicherung

- **GMG Systems, Inc. KnTTools**
- **F-Response**
- **Dumplt**
- **Mandiant Memoryze**
- **HBGary FastDump**
- **MoonSols Windows Memory Toolkit**
- **AccessData FTK Imager**
- **EnCase WinEn**
- **Belkasoft Live RAM Capturer**
- **ATC-NY Windows Memory Reader**
- **Winpmem (Rekall)**

Dumplt

E:\Downloads\DumpIt\x64\DumpIt.exe

```
DumpIt 3.0.20190123.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2016 - 2018, Comae Technologies DMCC <http://www.comae.io>
```

```
Destination path: \??\E:\Downloads\DumpIt\x64\RACER8-20210621-210350.dmp
```

```
Computer name: RACER8
```

```
--> Proceed with the acquisition ? [y/n] y
```

```
[+] Information:
```

```
Dump Type: Microsoft Crash Dump
```

```
[+] Machine Information:
```

```
Windows version: 10.0.19042
```

```
MachineId: 00000000-0000-0000-0000-D43D7EBD40B7
```

```
TimeStamp: 132687830450783068
```

```
Cr3: 0x1aa002
```

```
KdCopyDataBlock: 0xfffff8026d70b538
```

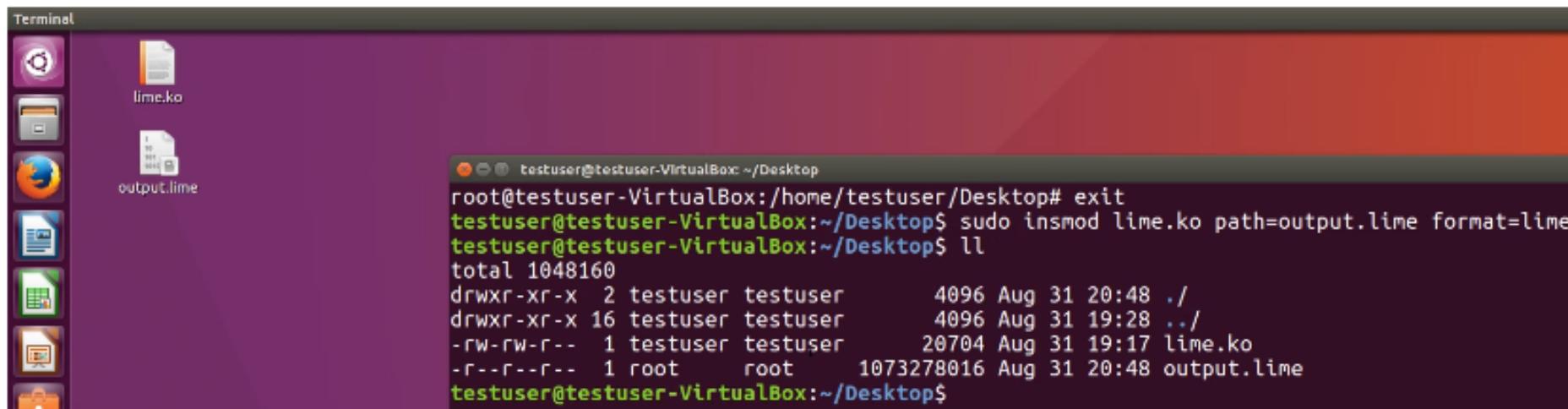
```
KdDebuggerData: 0xfffff8026de00b20
```

```
KdpDataBlockEncoded: 0xfffff8026de50ab0
```

```
Current date/time: [2021-06-21 (YYYY-MM-DD) 21:04:05 (UTC)]
```

Linux Memory Dump

```
sudo insmod lime.ko path=output.lime format=lime
```



macOS Memory Dump

```
$ sudo osxpmem.app/osxpmem -o Memory_Captures/mem.aff4
Imaging memory
E1229 15:17:26.335978 3375588288 aff4_file.cc:289] Can not open file
/dev/pmem :No such file or directory
/Users/jp/Projects/osxpmem.app/MacPmem.kext failed to load -
(libkern/kext) authentication failure (file ownership/permissions);
check the system/kernel logs for errors or try kextutil(8).
E1229 15:17:26.606639 3375588288 osxpmem.cc:283] Unable to load
driver at /Users/jp/Projects/osxpmem.app/MacPmem.kext
E1229 15:17:26.606714 3375588288 pmem_imager.cc:328] Imaging failed
with error: -8
```

Windows Crashdumps

C:\Windows			
Name	Änderungsdatum	Typ	Größe
lsUninst.exe	29.10.1998 15:45	Anwendung	300 KB
MEMORY.DMP	22.01.2021 01:32	Dump File	1.649.693 KB
mib.bin	07.12.2019 10:08	VLC media file (.bi...)	43 KB

Windows Crashdumps

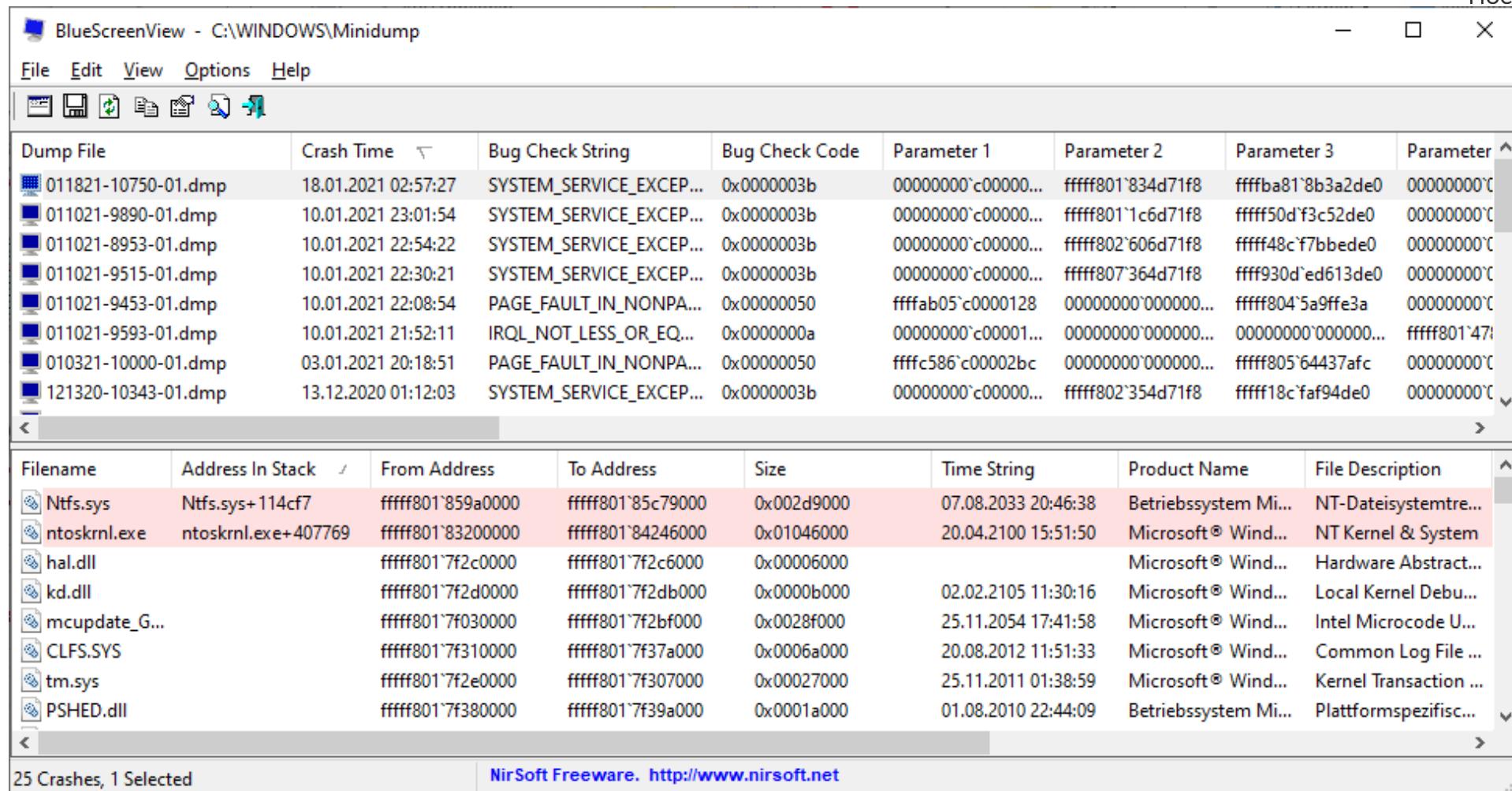


HTWK
Hochschule Stralsund

C:\Windows\Minidump

Name	Änderungsdatum	Typ	Größe
011821-10750-01.dmp	18.01.2021 01:59	Dump File	1.193 KB
011021-9890-01.dmp	10.01.2021 22:03	Dump File	1.034 KB
011021-8953-01.dmp	10.01.2021 21:58	Dump File	1.040 KB
011021-9515-01.dmp	10.01.2021 21:31	Dump File	1.025 KB
011021-9453-01.dmp	10.01.2021 21:10	Dump File	1.118 KB
011021-9593-01.dmp	10.01.2021 20:53	Dump File	1.024 KB
010321-10000-01.dmp	03.01.2021 19:20	Dump File	862 KB
121320-10343-01.dmp	13.12.2020 00:13	Dump File	820 KB
121120-11343-01.dmp	11.12.2020 15:44	Dump File	716 KB
121120-13250-01.dmp	11.12.2020 15:41	Dump File	767 KB
112420-9562-01.dmp	24.11.2020 21:18	Dump File	761 KB
112420-40312-01.dmp	24.11.2020 19:12	Dump File	898 KB
112420-9500-01.dmp	24.11.2020 11:21	Dump File	804 KB
111820-11312-01.dmp	18.11.2020 22:00	Dump File	893 KB
Martin 111720-10093-01.dmp	17.11.2020 23:50	Dump File	811 KB

Windows Crashdumps



The screenshot shows the BlueScreenView application interface. The main window displays a list of crash dump files (DMP files) with columns for Dump File, Crash Time, Bug Check String, Bug Check Code, and several parameters. Below this is a detailed view of kernel modules with columns for Filename, Address In Stack, From Address, To Address, Size, Time String, Product Name, and File Description.

Dump File	Crash Time	Bug Check String	Bug Check Code	Parameter 1	Parameter 2	Parameter 3	Parameter 4
011821-10750-01.dmp	18.01.2021 02:57:27	SYSTEM_SERVICE_EXCEP...	0x0000003b	00000000`c00000...	fffff801`834d71f8	fffffb81`8b3a2de0	00000000`000000...
011021-9890-01.dmp	10.01.2021 23:01:54	SYSTEM_SERVICE_EXCEP...	0x0000003b	00000000`c00000...	fffff801`1c6d71f8	fffff50d`f3c52de0	00000000`000000...
011021-8953-01.dmp	10.01.2021 22:54:22	SYSTEM_SERVICE_EXCEP...	0x0000003b	00000000`c00000...	fffff802`606d71f8	fffff48c`f7bbe0	00000000`000000...
011021-9515-01.dmp	10.01.2021 22:30:21	SYSTEM_SERVICE_EXCEP...	0x0000003b	00000000`c00000...	fffff807`364d71f8	fffff930d`ed613de0	00000000`000000...
011021-9453-01.dmp	10.01.2021 22:08:54	PAGE_FAULT_IN_NONPA...	0x00000050	fffffab05`c0000128	00000000`000000...	fffff804`5a9ffe3a	00000000`000000...
011021-9593-01.dmp	10.01.2021 21:52:11	IRQL_NOT_LESS_OR_EQ...	0x0000000a	00000000`c00001...	00000000`000000...	00000000`000000...	fffff801`471e0
010321-10000-01.dmp	03.01.2021 20:18:51	PAGE_FAULT_IN_NONPA...	0x00000050	fffffc586`c00002bc	00000000`000000...	fffff805`64437afc	00000000`000000...
121320-10343-01.dmp	13.12.2020 01:12:03	SYSTEM_SERVICE_EXCEP...	0x0000003b	00000000`c00000...	fffff802`354d71f8	fffff18c`faf94de0	00000000`000000...

Filename	Address In Stack	From Address	To Address	Size	Time String	Product Name	File Description
Ntfs.sys	Ntfs.sys+114cf7	ffffff801`859a0000	fffff801`85c79000	0x002d9000	07.08.2033 20:46:38	Betriebssystem Mi...	NT-Dateisystemtre...
ntoskrnl.exe	ntoskrnl.exe+407769	fffff801`83200000	fffff801`84246000	0x01046000	20.04.2100 15:51:50	Microsoft® Wind...	NT Kernel & System
hal.dll		fffff801`7f2c0000	fffff801`7f2c6000	0x00006000		Microsoft® Wind...	Hardware Abstract...
kd.dll		fffff801`7f2d0000	fffff801`7f2db000	0x0000b000	02.02.2105 11:30:16	Microsoft® Wind...	Local Kernel Debu...
mcupdate_G...		fffff801`7f030000	fffff801`7f2bf000	0x0028f000	25.11.2054 17:41:58	Microsoft® Wind...	Intel Microcode U...
CLFS.SYS		fffff801`7f310000	fffff801`7f37a000	0x0006a000	20.08.2012 11:51:33	Microsoft® Wind...	Common Log File ...
tm.sys		fffff801`7f2e0000	fffff801`7f307000	0x00027000	25.11.2011 01:38:59	Microsoft® Wind...	Kernel Transaction ...
PSHED.dll		fffff801`7f380000	fffff801`7f39a000	0x0001a000	01.08.2010 22:44:09	Betriebssystem Mi...	Plattformspezifisc...

25 Crashes, 1 Selected NirSoft Freeware. <http://www.nirsoft.net>

Windows Crashdumps

- **Admin Powershell**
- **NotMyFault-Tool**
- **Registry-Schlüssel erzeugen**
- **Hardware**

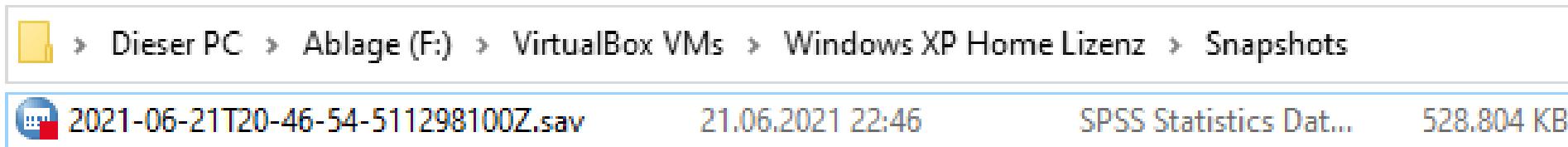
Windows User Crashdumps

C:\Users\horst\AppData\Local\CrashDumps			
Name	Änderungsdatum	Typ	Größe
cnc3game.dat.8068.dmp	31.05.2021 20:05	Dump File	9.372 KB
MongoDBCompass.exe.7608.dmp	03.06.2021 09:48	Dump File	3.797 KB
OUTLOOK.EXE.3140.dmp	18.05.2021 08:55	Dump File	30.785 KB
OUTLOOK.EXE.12716.dmp	17.05.2021 16:06	Dump File	31.431 KB
OUTLOOK.EXE.14724.dmp	17.05.2021 16:07	Dump File	31.171 KB
OUTLOOK.EXE.15532.dmp	17.05.2021 16:08	Dump File	31.088 KB
Personify ChromaCam.exe.38048.dmp	27.05.2021 14:00	Dump File	22.131 KB
SP_Connector.exe.8708.dmp	22.05.2021 16:39	Dump File	598 KB
SP_Connector.exe.15232.dmp	13.05.2021 22:14	Dump File	591 KB

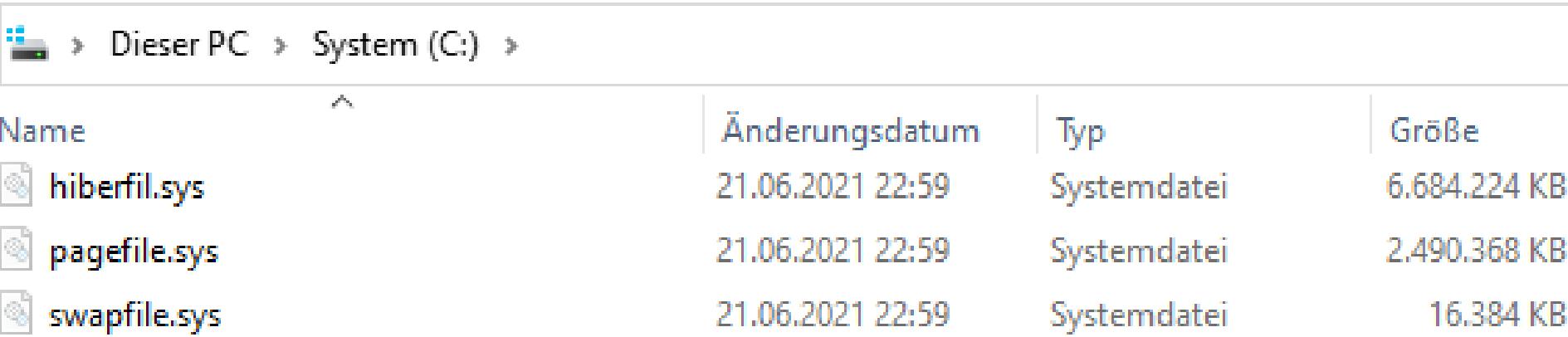
Windows System Crashdumps

C:\Windows\System32\config\systemprofile\AppData\Local\CrashDumps			
Name	Änderungsdatum	Typ	Größe
NVDisplay.Container.exe.1928.dmp	10.04.2021 09:27	Dump File	1.223 KB
NVDisplay.Container.exe.2000.dmp	01.04.2021 00:20	Dump File	1.609 KB
NVDisplay.Container.exe.2060.dmp	12.03.2021 15:52	Dump File	1.218 KB
NVDisplay.Container.exe.7512.dmp	16.02.2021 23:44	Dump File	3.571 KB
PrintIsolationHost.exe.5932.dmp	15.03.2021 11:11	Dump File	809 KB
PrintIsolationHost.exe.9120.dmp	25.02.2021 23:06	Dump File	807 KB
PrintIsolationHost.exe.14176.dmp	22.02.2021 12:05	Dump File	840 KB
spoolsv.exe.4108.dmp	02.03.2021 21:10	Dump File	1.980 KB

Virtual Maschine Dumps



Pagefile, Swapfile, Hiberfile



Name	Änderungsdatum	Typ	Größe
hiberfil.sys	21.06.2021 22:59	Systemdatei	6.684.224 KB
pagefile.sys	21.06.2021 22:59	Systemdatei	2.490.368 KB
swapfile.sys	21.06.2021 22:59	Systemdatei	16.384 KB

Hiberfil dekomprimieren



comaeio / Hibr2Bin

Notifications Star 118 Fork 47

Code Issues Pull requests Actions Projects Wiki Security ...

master Hibr2Bin / Hibr2Bin / Go to file

msuiche up v142 ... on 16 Feb 2020 History

CommonLibLight @ ae952f8 Up Hibr2Bin/CommonLibLight 2 years ago

Disk.cpp - Update Visual Studio project. 2 years ago

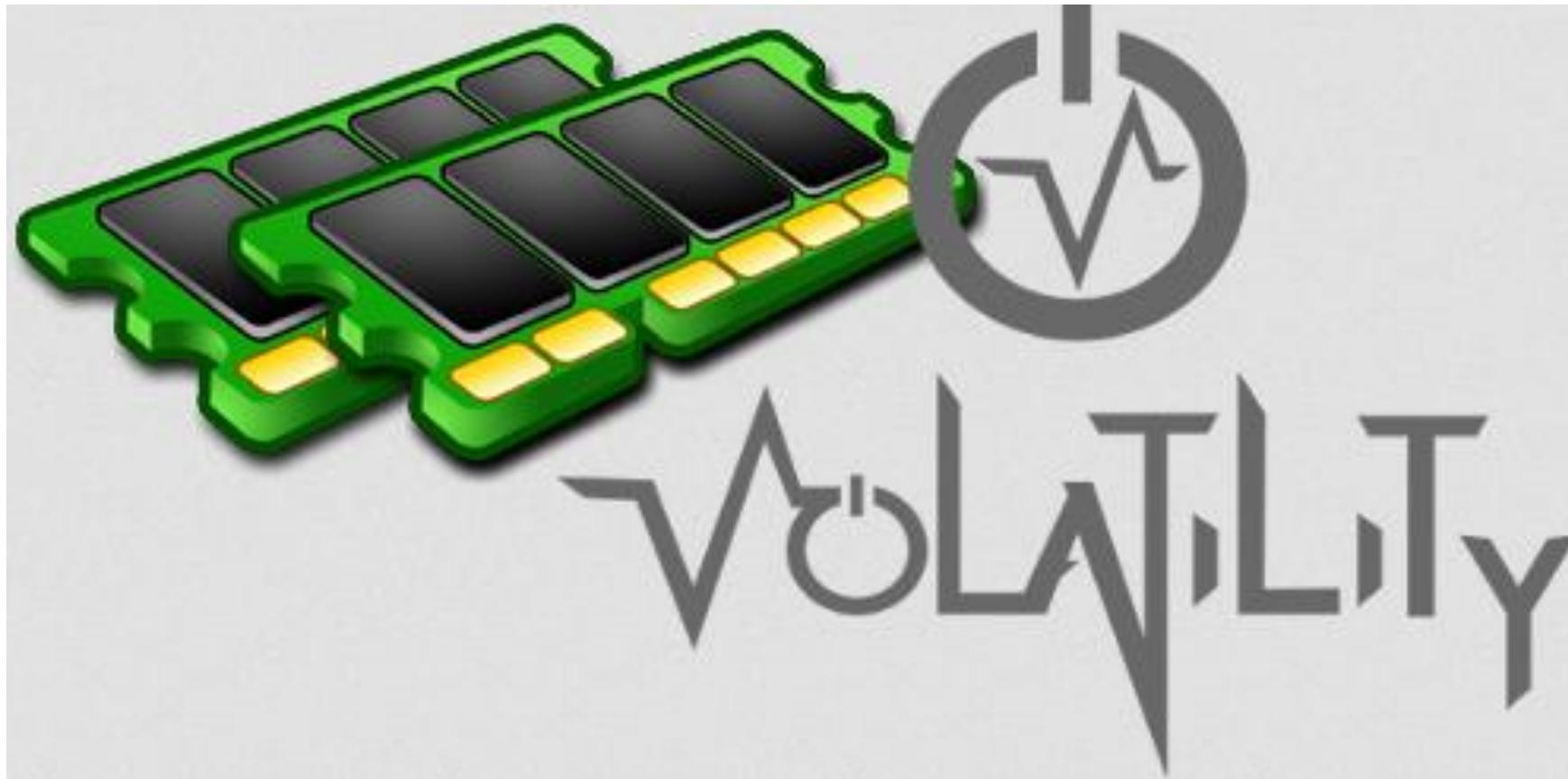
Hiber.h Update copyright 3 years ago

Hiberfil.cpp - Update Visual Studio project. 2 years ago

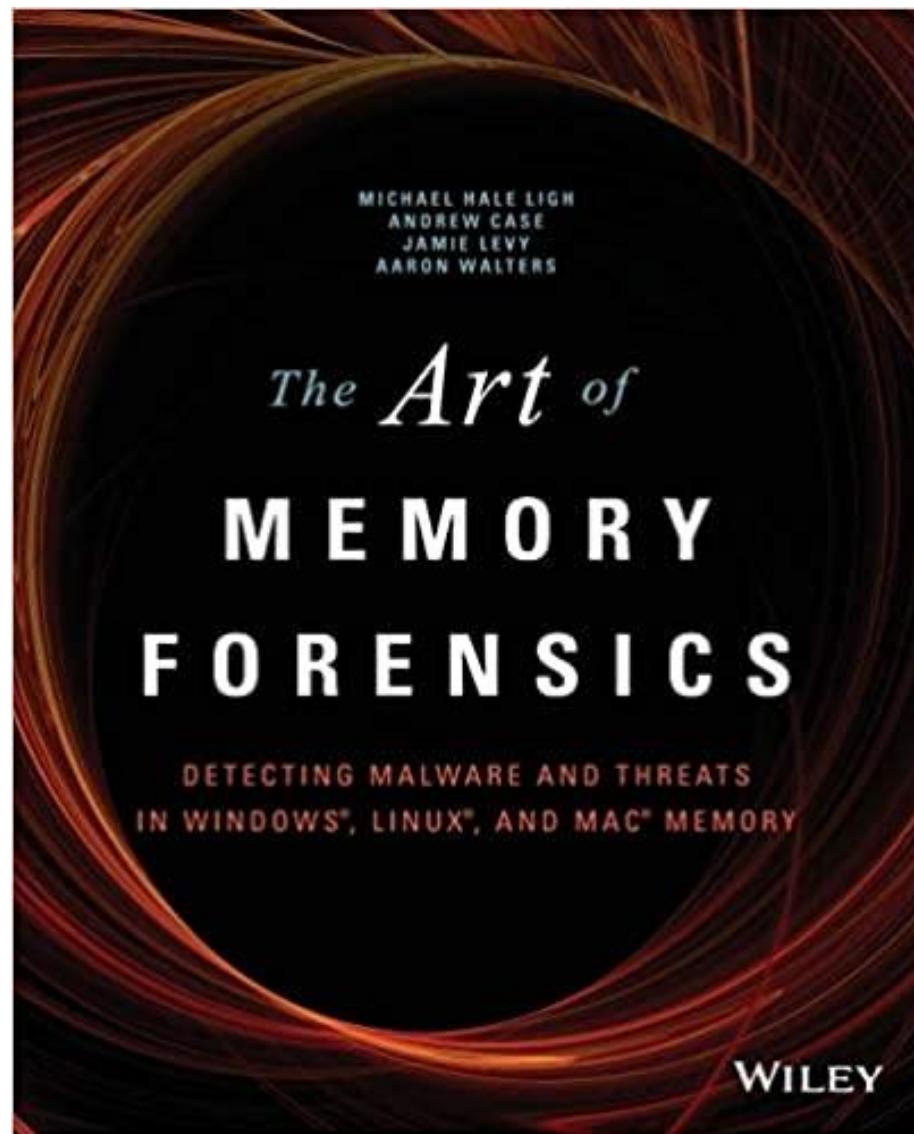
A screenshot of a GitHub repository page for "comaeio / Hibr2Bin". The repository has 118 stars and 47 forks. The "Code" tab is selected. A pull request from "msuiche" titled "up v142" was merged on February 16, 2020. The commit message was "Up Hibr2Bin/CommonLibLight". The commit history shows several other changes, including updates to "Disk.cpp", "Hiber.h", and "Hiberfil.cpp", all made between 2 and 3 years ago.



Arbeitsspeicher-Forensik



Arbeitsspeicher-Forensik



Volatility

vol.py -h
Hilfe

vol.py -info
Alle Profile, Adressräume, und Plugins

Volatility Imageinfo

```
(rekall_env)DMP:Mem_Images dae$ vol.py -f XP/coreflood.vmem imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                                AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                                AS Layer2 : FileAddressSpace (/Users/dae/Mem_Images/XP/coreflood.vmem)
                                PAE type : PAE
                                DTB   : 0x319000L
                                KDBG  : 0x80544ce0L
Number of Processors : 1
Image Type (Service Pack) : 2
          KPCR for CPU 0 : 0xffdff000L
          KUSER_SHARED_DATA : 0xffdf0000L
Image date and time  : 2010-08-15 18:24:00 UTC+0000
Image local date and time : 2010-08-15 14:24:00 -0400
```

Volatility Imageinfo

```
C:\Windows\system32\cmd.exe

C:\Users\Haider\Downloads\volatility>volatility.exe imageinfo -f H-HP-20121209-120703.raw
Volatile Systems Volatility Framework 2.1
Determining profile based on KDBG search...

        Suggested Profile(s) : Win2008R2SP0x64, Win7SP1x64, Win7SP0x64, Win2008R2SP1x64
                        AS Layer1 : AMD64PagedMemory <Kernel AS>
                        AS Layer2 : FileAddressSpace <C:\Users\Haider\Downloads\volatility\H-HP-20121209-120703.raw>
                           PAE type : PAE
                           DIB : 0x187000L
                           KDBG : 0xf800031f50a0L
      Number of Processors : 4
Image Type <Service Pack> : 0
          KPCR for CPU 0 : 0xfffffff800031f6d000L
          KPCR for CPU 1 : 0xfffffff880009e9000L
          KPCR for CPU 2 : 0xfffffff88003964000L
          KPCR for CPU 3 : 0xfffffff880039d5000L
          KUSER_SHARED_DATA : 0xfffffff7800000000000L
    Image date and time : 2012-12-09 12:07:22 UTC+0000
Image local date and time : 2012-12-09 12:07:22 +0000

C:\Users\Haider\Downloads\volatility>
```

Volatility kdbgscan

```
C:\Windows\system32\cmd.exe

C:\Users\Haider\Downloads\volatility>volatility.exe imageinfo -f H-HP-20121209-120703.raw
Volatile Systems Volatility Framework 2.1
Determining profile based on KDBG search...

        Suggested Profile(s) : Win2008R2SP0x64, Win7SP1x64, Win7SP0x64, Win2008R2SP1x64
                        AS Layer1 : AMD64PagedMemory <Kernel AS>
                        AS Layer2 : FileAddressSpace <C:\Users\Haider\Downloads\volatility\H-HP-20121209-120703.raw>
                           PAE type : PAE
                           DIB : 0x187000L
                           KDBG : 0xf800031f50a0L
      Number of Processors : 4
Image Type <Service Pack> : 0
                        KPCR for CPU 0 : 0xfffffff800031f6d000L
                        KPCR for CPU 1 : 0xfffffff880009e9000L
                        KPCR for CPU 2 : 0xfffffff88003964000L
                        KPCR for CPU 3 : 0xfffffff880039d5000L
                        KUSER_SHARED_DATA : 0xfffffff780000000000L
    Image date and time : 2012-12-09 12:07:22 UTC+0000
Image local date and time : 2012-12-09 12:07:22 +0000

C:\Users\Haider\Downloads\volatility>
```

Volatility kdbgscan

```
$ python vol.py -f memory.raw kdbgscan
Volatility Foundation Volatility Framework 2.4
*****
Offset (V) : 0xf80002803070
Offset (P) : 0x2803070
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP0x64
Version64 : 0xf80002803030 (Major: 15, Minor: 7600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab) : 7600.16385.amd64fre.win7_rtm.090
PsActiveProcessHead : 0xfffff80002839b30 (32 processes)
PsLoadedModuleList : 0xfffff80002857e50 (133 modules)
KernelBase : 0xfffff8000261a000 (Matches MZ: True)
Major (OptionalHeader) : 6
Minor (OptionalHeader) : 1
KPCR : 0xfffff80002804d00 (CPU 0)
```

Arbeitsspeicher-Forensik



HOST
Hochschule Stralsund

```
$ vol.py -f ~/Desktop/win7_trial_64bit.raw --profile=Win7SP0x64 pslist
```

```
Volatility Foundation Volatility Framework 2.4
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
<hr/>								
0xfffffa80004b09e0	System	4	0	78	489	-----	0	2012-02-22 19:58:20
0xfffffa8000ce97f0	smss.exe	208	4	2	29	-----	0	2012-02-22 19:58:20
0xfffffa8000c006c0	csrss.exe	296	288	9	385	0	0	2012-02-22 19:58:24
0xfffffa8000c92300	wininit.exe	332	288	3	74	0	0	2012-02-22 19:58:30
0xfffffa8000c06b30	csrss.exe	344	324	7	252	1	0	2012-02-22 19:58:30
0xfffffa8000c80b30	winlogon.exe	372	324	5	136	1	0	2012-02-22 19:58:31
0xfffffa8000c5eb30	services.exe	428	332	6	193	0	0	2012-02-22 19:58:32
0xfffffa80011c5700	lsass.exe	444	332	6	557	0	0	2012-02-22 19:58:32
0xfffffa8000ea31b0	lsm.exe	452	332	10	133	0	0	2012-02-22 19:58:32
0xfffffa8001296b30	svchost.exe	568	428	10	352	0	0	2012-02-22 19:58:34
0xfffffa80012c3620	svchost.exe	628	428	6	247	0	0	2012-02-22 19:58:34
0xfffffa8001325950	sppsvc.exe	816	428	5	154	0	0	2012-02-22 19:58:41
0xfffffa80007b7960	svchost.exe	856	428	16	404	0	0	2012-02-22 19:58:43
0xfffffa80007bb750	svchost.exe	880	428	34	1118	0	0	2012-02-22 19:58:43
0xfffffa80007d09e0	svchost.exe	916	428	19	443	0	0	2012-02-22 19:58:43
0xfffffa8000c64840	svchost.exe	348	428	14	338	0	0	2012-02-22 20:02:07
0xfffffa8000c09630	svchost.exe	504	428	16	496	0	0	2012-02-22 20:02:07
0xfffffa8000e86690	spoolsv.exe	1076	428	12	271	0	0	2012-02-22 20:02:10
0xfffffa8000518b30	svchost.exe	1104	428	18	307	0	0	2012-02-22 20:02:10
0xfffffa800094d960	wlms.exe	1264	428	4	43	0	0	2012-02-22 20:02:11

Arbeitsspeicher-Forensik

Handles repräsentieren Zugriff auf Objekte

- Datei zum Lesen oder Schreiben geöffnet
- Registry-Schlüssel modifiziert
- Kindprozess erstellt
- Thread gestartet

Arbeitsspeicher-Forensik

handles

zeigt die Handles aller laufenden Prozesse

- -p PID
- -n Prozessname
- -t <object/handle type(s)>
- -s ignoriert namenlose Handles

Arbeitsspeicher-Forensik

handles

vol.py -f memory.dd handles -p

Zeigt alle Handles für explorer.exe

vol.py -f memory.dd handles -n explorer

Arbeitsspeicher-Forensik

- connections
- connscan
- sockets
- sockscan
- netscan

Arbeitsspeicher-Forensik

Legen Netzwerk-Aktivitäten offen, z. B.

- IP-Adressen
- Ports
- Verbindungs-Status
- Protocol
- Besitzer*in
- Prozess (PID und Name)

Arbeitsspeicher-Forensik

```
(rekall_env)DMP:Mem_Images dae$ vol.py -f Win7/shelly.vmem --profile=Win7SP1x86 filescan | grep explorer.exe
Volatility Foundation Volatility Framework 2.5
0x000000007d602d48      4      0 R--r-d \Device\HarddiskVolume1\Windows\explorer.exe
0x000000007ea35f80      8      1 R--r-d \Device\HarddiskVolume1\Windows\en-US\explorer.exe.mui
0x000000007edfc2e0      2      0 R--r-d \Device\HarddiskVolume1\Windows\explorer.exe
```

Arbeitsspeicher-Forensik

```
(rekall_env)DMP:Mem_Images dae$ vol.py -f Win7/shelly.vmem --profile=Win7SP1x86 dumpfiles -Q 0x00000007d602d48 -n -D .
Volatility Foundation Volatility Framework 2.5
ImageSectionObject 0x7d602d48  None  \Device\HarddiskVolume1\Windows\explorer.exe
DataSectionObject 0x7d602d48  None  \Device\HarddiskVolume1\Windows\explorer.exe
```

Arbeitsspeicher-Forensik

```
root@kali:~# volatility -f ram.mem --profile=Win7SP1x64 timeliner ←
Volatility Foundation Volatility Framework 2.6
2020-10-01 16:27:05 UTC+0000 [LIVE RESPONSE] | (System time)
2020-10-01 16:26:04 UTC+0000 [IEHISTORY] | explorer.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-09-26 11:42:11 UTC+0000 [IEHISTORY] | explorer.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-09-17 17:43:58 UTC+0000 [IEHISTORY] | explorer.exe→Visited: raj@file:///E:/raj.txt| PID: 1120
2020-09-26 11:48:11 UTC+0000 [IEHISTORY] | explorer.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-10-01 21:56:04 UTC+0000 [IEHISTORY] | explorer.exe->:2020100120201002: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-10-01 21:56:04 UTC+0000 [IEHISTORY] | explorer.exe->:2020100120201002: raj@Host: Computer| PID: 1120
2020-10-01 16:26:04 UTC+0000 [IEHISTORY] | iexplore.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-09-26 11:42:11 UTC+0000 [IEHISTORY] | iexplore.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
2020-09-17 17:43:58 UTC+0000 [IEHISTORY] | iexplore.exe→Visited: raj@file:///E:/raj.txt| PID: 1120
2020-09-26 11:48:11 UTC+0000 [IEHISTORY] | iexplore.exe→Visited: raj@file:///C:/Users/raj/Desktop/raj.txt| PID: 1120
```

Arbeitsspeicher-Forensik



Arbeitsspeicher-Forensik

PassMark Volatility Workbench

Image file: F:\Passmark\Volatility\Images\MemDump\MemDump.mem

Platform: Windows

Command: windows.callbacks.Callbacks

Refresh Process List

Browse Image

Command Info

Run

Command Description:

In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command

Volatility Workbench by PassMark Software

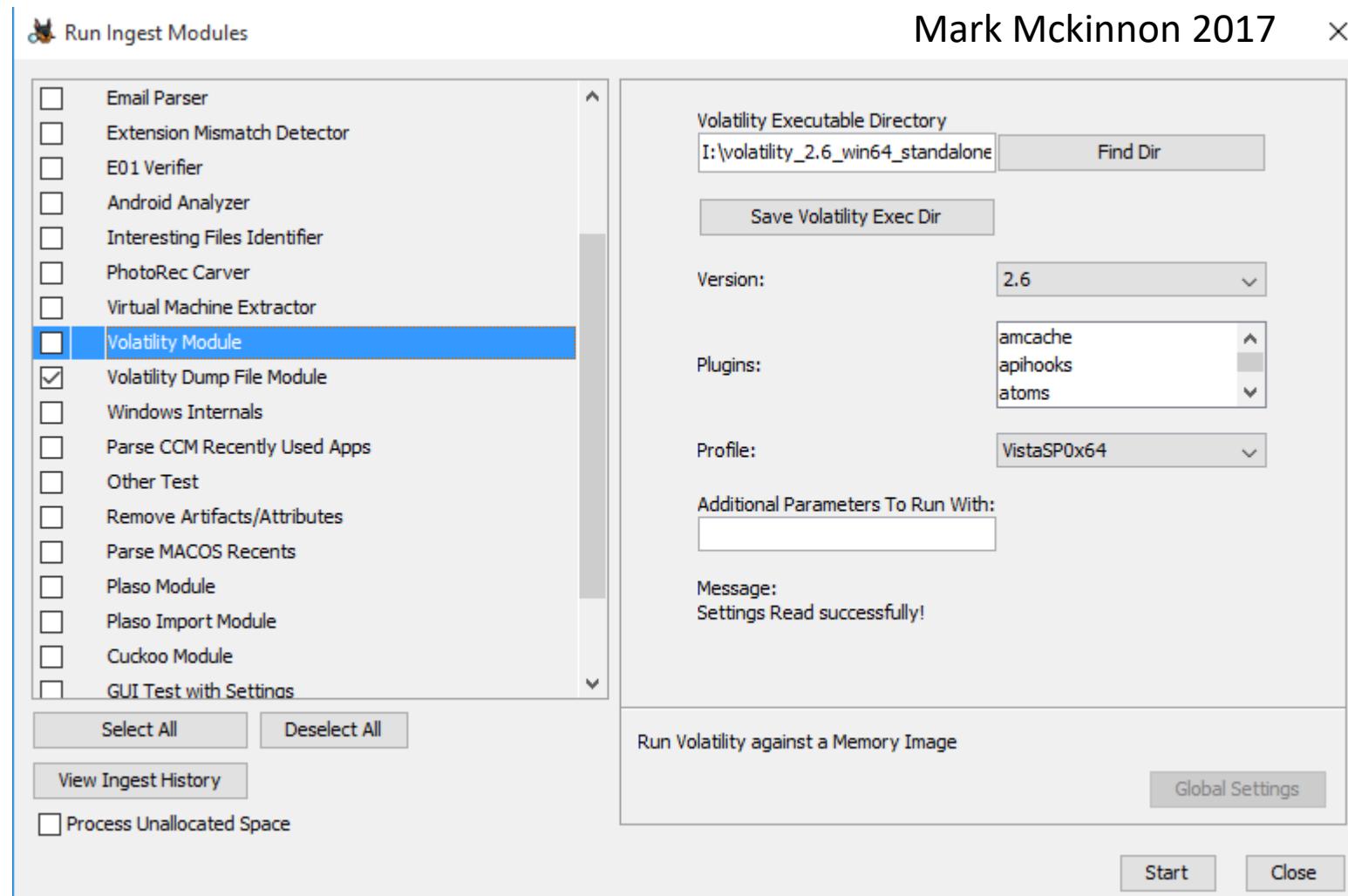
ID	Name	Process ID	Image Base	Start Address	End Address	Size	Protection	Access	Writeable	Start Time	End Time	Processor
10540	chrome.exe	0xb10e92303000	0	-1	False	2020-07-30 21:37:40.000000	N/A					
19080	HXTsr.exe	0xb10e9af104c0	0	-1	False	2020-07-30 21:58:31.000000	2020-07-30 21:58:39.000000					
6476	svchost.exe	0xb10ea0a82340	0	-0	False	2020-07-30 21:58:32.000000	2020-07-30 22:03:35.000000					
18840	OfficeC2RClien	0xb10e93eee080	0	-0	False	2020-07-30 21:59:49.000000	2020-07-30 22:00:19.000000					
12536	OfficeClickToR	0xb10e911454c0	0	-1	False	2020-07-30 22:00:21.000000	2020-07-30 22:00:30.000000					
12136	OfficeClickToR	0xb10e9dd8c080	0	-0	False	2020-07-30 22:00:26.000000	2020-07-30 22:00:30.000000					
22432	chrome.exe	0xb10e91da6080	16	-1	False	2020-07-30 22:07:49.000000	N/A					
8276	mspaint.exe	0xb10e99f814c0	0	-1	False	2020-07-30 22:22:42.000000	2020-07-30 22:25:06.000000					
2024	chrome.exe	0xb10e8dbd3080	0	-1	False	2020-07-30 22:23:36.000000	2020-07-30 22:23:38.000000					
8044	Teams.exe	0xb10e99698080	43	-1	False	2020-07-30 22:25:03.000000	N/A					
3492	Teams.exe	0xb10e9bafc080	25	-1	False	2020-07-30 22:25:04.000000	N/A					
11300	Teams.exe	0xb10e9bf0f080	0	-1	False	2020-07-30 22:25:04.000000	2020-07-30 22:25:07.000000					
18252	Teams.exe	0xb10e93109080	18	-1	False	2020-07-30 22:25:04.000000	N/A					
12708	Teams.exe	0xb10e9e206080	27	-1	False	2020-07-30 22:25:04.000000	N/A					
16684	Teams.exe	0xb10ea0a10080	61	-1	False	2020-07-30 22:25:09.000000	N/A					
11960	Teams.exe	0xb10e99f0c080	18	-1	False	2020-07-30 22:25:10.000000	N/A					
22036	Teams.exe	0xb10e99f19080	0	-1	False	2020-07-30 22:25:11.000000	2020-07-30 22:25:16.000000					
22380	Teams.exe	0xb10ea17dc080	0	-1	False	2020-07-30 22:25:15.000000	2020-07-30 22:29:15.000000					
17176	Teams.exe	0xb10e972c6080	0	-1	False	2020-07-30 22:25:19.000000	2020-07-30 22:25:19.000000					
22296	Teams.exe	0xb10e9dd6c4c0	0	-1	False	2020-07-30 22:30:05.000000	2020-07-30 22:30:05.000000					
11144	svchost.exe	0xb10e957474c0	3	-0	False	2020-07-30 22:34:51.000000	N/A					
9764	svchost.exe	0xb10ea0a5e080	7	-0	False	2020-07-30 22:34:51.000000	N/A					
13344	audiogd.exe	0xb10e9a117080	5	-0	False	2020-07-30 22:34:53.000000	N/A					
7744	chrome.exe	0xb10e8ccce080	14	-1	False	2020-07-30 22:34:54.000000	N/A					
18632	svchost.exe	0xb10e9d2bf080	10	-0	False	2020-07-30 22:34:56.000000	N/A					
12220	svchost.exe	0xb10e9a56a4c0	6	-0	False	2020-07-30 22:35:21.000000	N/A					
10484	smartscreen.ex	0xb10e9e3484c0	10	-1	False	2020-07-30 22:35:38.000000	N/A					
6924	Teams.exe	0xb10e9cc76080	18	-1	False	2020-07-30 22:36:12.000000	N/A					
10880	osf64.exe	0xb10ea06cf080	35	-1	False	2020-07-30 22:36:30.000000	N/A					
21944	SearchProtocol	0xb10e99f1a080	9	-0	False	2020-07-30 22:36:32.000000	N/A					
8080	CompatTelRunne	0xb10ea17de080	8	-0	False	2020-07-30 22:37:05.000000	N/A					
16032	conhost.exe	0xb10ea4f82080	7	-0	False	2020-07-30 22:37:05.000000	N/A					
1760	SearchProtocol	0xb10e9e6d1080	20	-1	False	2020-07-30 22:37:15.000000	N/A					
6776	SearchFilterHo	0xb10e94ee0080	4	-0	False	2020-07-30 22:37:19.000000	N/A					

Time Stamp: Fri Aug 7 12:41:10 2020

***** End of command output *****

Clear Log Save to file Copy to clipboard About Exit

Arbeitsspeicher-Forensik



Arbeitsspeicher-Forensik



Mark Mckinnon 2017

Log_test_2 - Autopsy 4.3.0

Case View Tools Window Help

Add Data Source View Images/Videos Timeline Generate Report Close Case

Directory Listing
Volatility CMDSCAN sample005.bin
Table Thumbnail

Source File	id	Process	PID	History Offset	Application	Flags	Command Count	Last Added	Last Displayed	First Command
sample005.bin	1	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	2	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	3	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	4	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	5	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	6	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	7	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	8	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	9	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	10	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	11	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0

Hex Strings File Metadata Results Indexed Text Media

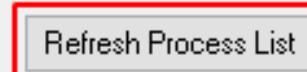
Extracted Content
Views
Results
Extracted Content
Volatility CMDLINE sample001.bin (21)
Volatility CMDLINE sample005.bin (25)
Volatility CMDLINE sample006.bin (38)
Volatility CMDLINE sample007.bin (31)
Volatility CMDSCAN sample001.bin (5)
Volatility CMDSCAN sample005.bin (11)
Volatility CONNECTIONS sample001.bin (1)
Volatility CONNECTIONS sample005.bin (3)
Volatility CONNECTIONS sample006.bin (1)
Volatility IMAGEINFO sample001.bin (1)
Volatility IMAGEINFO sample005.bin (1)
Volatility IMAGEINFO sample006.bin (1)
Volatility IMAGEINFO sample007.bin (1)
Volatility PSLIST sample001.bin (21)
Volatility PSLIST sample005.bin (25)
Volatility PSLIST sample006.bin (38)
Volatility PSLIST sample007.bin (31)
Volatility PSSCAN sample001.bin (45)
Volatility PSSCAN sample005.bin (101)
Volatility PSSCAN sample006.bin (38)
Volatility PSSCAN sample007.bin (31)
Volatility PSTREE sample001.bin (21)
Volatility PSTREE sample005.bin (25)
Volatility PSTREE sample006.bin (38)
Volatility PSTREE sample007.bin (31)

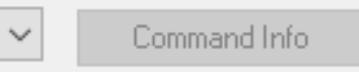
Keyword Hits
Single Literal Keyword Search (0)

Arbeitsspeicher-Forensik

PassMark Volatility Workbench

Image file: C:\Users\raj\Desktop\20201015.mem 

Profile: Windows 7 64bit base version  

Command: -- Hunting rootkits and malicious code -- 



Command Description:
In order to run a command:
1- Browse an image file
2- Select the proper profile
3- Get/Refresh process list
4- Select a command from the dropdown
5- Enter command parameters
6- Run command

Offset (V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start

0xfffffa8018dc4040	System	4	0	92	565	-----	0	2020-10-
14 20:55:37 UTC+0000								
0xfffffa8019463950	smss.exe	256	4	2	30	-----	0	2020-10-
14 20:55:37 UTC+0000								
0xfffffa8019f0c060	smss.exe	332	256	0	-----	0	0	2020-10-14
14 20:55:38 UTC+0000								
0xfffffa8019ff54a0	csrss.exe	352	332	9	469	0	0	2020-10-
14 20:55:38 UTC+0000								
0xfffffa801a191b30	smss.exe	396	256	0	-----	1	0	2020-10-14
14 20:55:38 UTC+0000								
0xfffffa801a1944d0	wininit.exe	404	332	3	77	0	0	2020-10-
14 20:55:38 UTC+0000								
0xfffffa801a195060	csrss.exe	412	396	11	485	1	0	2020-10-
14 20:55:38 UTC+0000								
0xfffffa801a1e7060	winlogon.exe	468	396	5	119	1	0	2020-10-
14 20:55:38 UTC+0000								
0xfffffa801a223440	services.exe	508	404	8	221	0	0	2020-10-
14 20:55:38 UTC+0000								

Arbeitsspeicher-Forensik

Profile: Windows 7 64bit base version

Command: malfind 

Refresh Process List

Command parameters:

- Process ID
- EPROCESS Offset
- Process Name (Regex)
- Dump Folder Name
- Maximum size

Command Info

Run

0x0fc6003f 00	DB 0x0
Process: windows-meterpreter Pid: 4572 Address: 0x20000	
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE	
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6	
0x00020000	fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30 8b
0x00020010	52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c R...R...r(...J&i...<
0x00020020	61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52 aRW.R
0x00020030	10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1 51 8b 59 20 ..J<.L.x.H..Q.Y.
0x00020000 fc	CLD
0x00020001 e882000000	CALL 0x20088

Arbeitsspeicher-Forensik

Command: cmdscan 

Command parameters:

- Process ID
- EPROCESS Offset
- Process Name (Regex)

Run

www.hackingarticles.in

```
profile=Win7SP0x64 --kdbg=0xf80002c050a0
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:32:28 2020
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 3924
CommandHistory: 0x2c0a40 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 4 LastAdded: 3 LastDisplayed: 3
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 @ 0x2a04e0: ipconfig
Cmd #1 @ 0x2a0500: netstat
Cmd #2 @ 0x2a0540: whoami
Cmd #3 @ 0x2a0580: getmac
Cmd #15 @ 0x270158: +
Cmd #16 @ 0x2bfbb0: ,
*****
CommandProcess: conhost.exe Pid: 1200
CommandHistory: 0x140c10 Application: RamCapture64.exe Flags: Allocated
```

Arbeitsspeicher-Forensik

Registry Analysis Plugins

```
hivelist - Find and list available registry hives
# vol.py hivelist

hivedump - Print all keys and subkeys in a hive
-o      Offset of registry hive to dump (virtual offset)
# vol.py hivedump -o 0xe1a14b60

printkey - Output a registry key, subkeys, and values
-K      "Registry key path"
# vol.py printkey -K
"Microsoft\Windows\CurrentVersion\Run"

dumpregistry - Extract all available registry hives
-o      Extract using virtual offset of registry hive
--dump-dir Directory to save extracted files
# vol.py dumpregistry --dump-dir ./output

userassist - Find and parse userassist key values
# vol.py userassist

hashdump - Dump user NTLM and Lanman hashes
# vol.py hashdump

autoruns - Map ASEPs to running processes
-v      Show everything
# vol.py autoruns -v
```

Arbeitsspeicher-Forensik

truecryptsummary

truecryptmaster

truecryptpassphrase

Arbeitsspeicher-Forensik

```
$ python vol.py -f WIN-QBTA4959AO9.raw --profile=Win2012SP0x64 truecryptsummary
```

```
Volatility Foundation Volatility Framework 2.3.1 (T)
```

volatility-labs.blogspot.com

```
Process           TrueCrypt.exe at 0xfffffa801af43980 pid 2096
Kernel Module    truecrypt.sys at 0xfffff88009200000 - 0xfffff88009241000
Symbolic Link    Volume{52b24c47-eb79-11e2-93eb-000c29e29398} -> \Device\TrueCryptVolumeZ mounted
2013-10-11 03:51:08 UTC+0000
Symbolic Link    Volume{52b24c50-eb79-11e2-93eb-000c29e29398} -> \Device\TrueCryptVolumeR mounted
2013-10-11 03:55:13 UTC+0000
File Object      \Device\TrueCryptVolumeR\$Directory at 0x7c2f7070
File Object      \Device\TrueCryptVolumeR\$LogFile at 0x7c39d750
File Object      \Device\TrueCryptVolumeR\$MftMirr at 0x7c67cd40
File Object      \Device\TrueCryptVolumeR\$\bR at 0x7cf05230
File Object      \Device\TrueCryptVolumeR\$Directory at 0x7cf50330
File Object      \Device\TrueCryptVolumeR\$BitMap at 0x7cfa7a00
File Object      \Device\TrueCryptVolumeR\Chats\Logs\bertha.xml at 0x7cdf4a00
Driver           \Driver\truecrypt at 0x7c9c0530 range 0xfffff88009200000 - 0xfffff88009241000
Device           TrueCryptVolumeR at 0xfffffa801b4be080 type FILE_DEVICE_DISK
Container        Path: \Device\Harddisk1\Partition1
Device           TrueCrypt at 0xfffffa801ae3f500 type FILE_DEVICE_UNKNOWN
```

Arbeitsspeicher-Forensik

```
$ python vol.py -f WIN-QBTA4.raw --profile=Win2012SP0x64 truecryptmaster -D .  
Volatility Foundation Volatility Framework 2.3.1 (T)
```

Container: \Device\Harddisk1\Partition1

Hidden Volume: No

Read Only: No

Disk Length: 7743733760 (bytes)

volatility-labs.blogspot.com

Host Length: 7743995904 (bytes)

Encryption Algorithm: **SERPENT**

Mode: **XTS**

Master Key

0xfffffa8018eb71a8 bbe1dc7a8e87e9f1f7eef37e6bb30a25 ...z.....~k..%

0xfffffa8018eb71b8 90b8948fefee425e5105054e3258b1a7B^Q..N2X..

0xfffffa8018eb71c8 a76c5e96d67892335008a8c60d09fb69 .1^..x.3P.....i

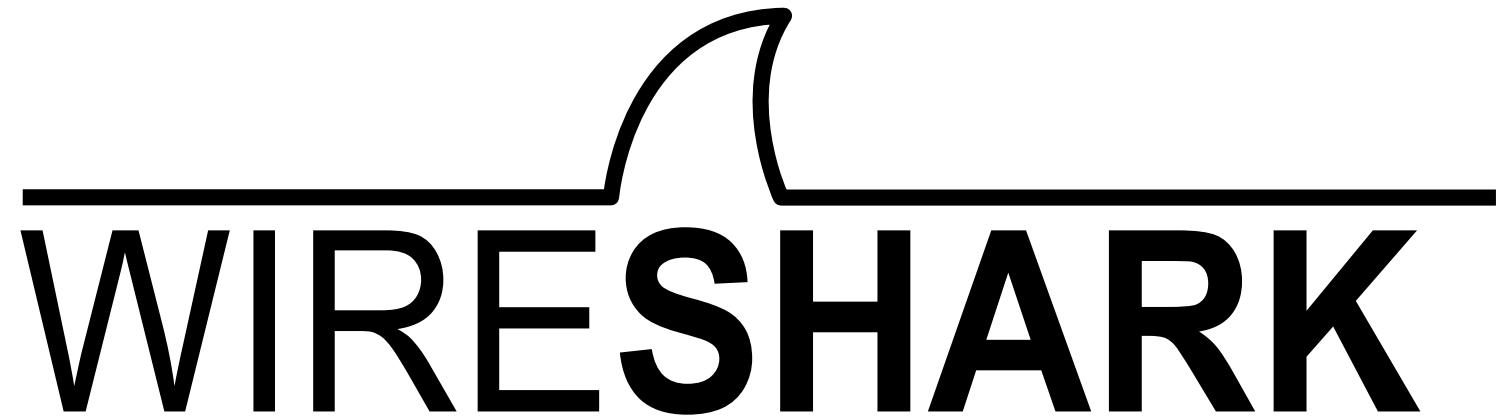
0xfffffa8018eb71d8 efb0b5fc759d44ec8c057fbc94ec3cc9u.D.....<.

Dumped 64 bytes to ./0xfffffa8018eb71a8_master.key

Forensische Netzwerk- Informationen

- **ipconfig/ifconfig**
- **route (print)**
- **arp -a**
- **netstat**

Netzwerk-Sniffing



Netzwerk-Sniffing



tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.netfliximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.netfliximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

```

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
< Domain Name System (response)
  [Request In: 348]
  [Time: 0.034338000 seconds]
  Transaction ID: 0x2188
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 9
  Additional RRs: 9
  < Queries
    > cdn-0.netfliximg.com: type A, class IN
  < Answers
  < Authoritative nameservers

```

0020	00	15	00	35	84	f4	01	c7	83	3f	21	88	81	80	00	015..... .?!.
0030	00	04	00	09	00	09	05	63	64	6e	2d	30	07	6e	66	6cc dn-0.netfliximg.com
0040	78	69	6d	67	03	63	6f	6d	00	00	01	00	01	c0	0c	00). ".images.netflix .com.edg...
0050	05	00	01	00	00	05	29	00	22	06	69	6d	61	67	65	73esuite.net.../....
0060	07	6e	65	74	66	6c	69	78	03	63	6f	6d	09	65	64	67	
0070	65	73	75	69	74	65	03	6e	65	74	00	c0	2f	00	05	00	

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 · Profile: Default

Netzwerk-Sniffing

Wireshark · Follow TCP Stream (tcp.stream eq 0) · test.cap

```
SUBSCRIBE /upnp/service/Layer3Forwarding HTTP/1.1
NT: upnp:event
Callback: <http://192.168.0.2:5000/notify>
Timeout: Second-1800
User-Agent: Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
Host: 192.168.0.1
Content-Length: 0
Pragma: no-cache

HTTP/1.0 200 OK
Connection: close
Server: UPnP/1.0 UPnP-Device-Host/1.0
Timeout: Second-1800
SID: uuid:cf
```

3 client pkts, 4 server pkts, 3 turns.

Entire conversation (368 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

WLAN-Infos



WLAN-Infos



Rittelmeier 2021

WLAN-Infos



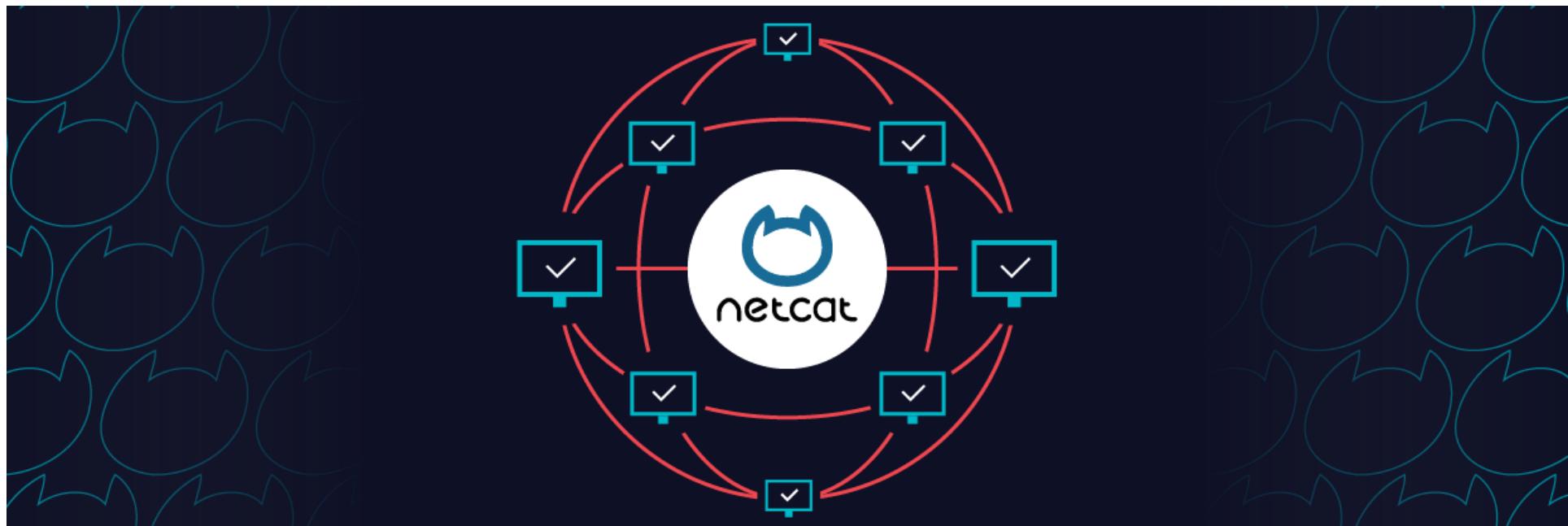
Network List (Autofit)							Info
Name	T	W	Ch	Packets	Flags	IP Range	Size
! pwn	A	Y	006	436		0.0.0.0	1k
Status							
Connected to Kismet server version 2004.10.R1 build 20041025233409 on localhost:2501							

IOST
Institut für Offene Systeme und Technologien
Stralsund



- **ADB DEVICES**
- **ADB BACKUP**
- **ADB TCPIP, ADB CONNECT**
- **ADB SHELL**

Netcat



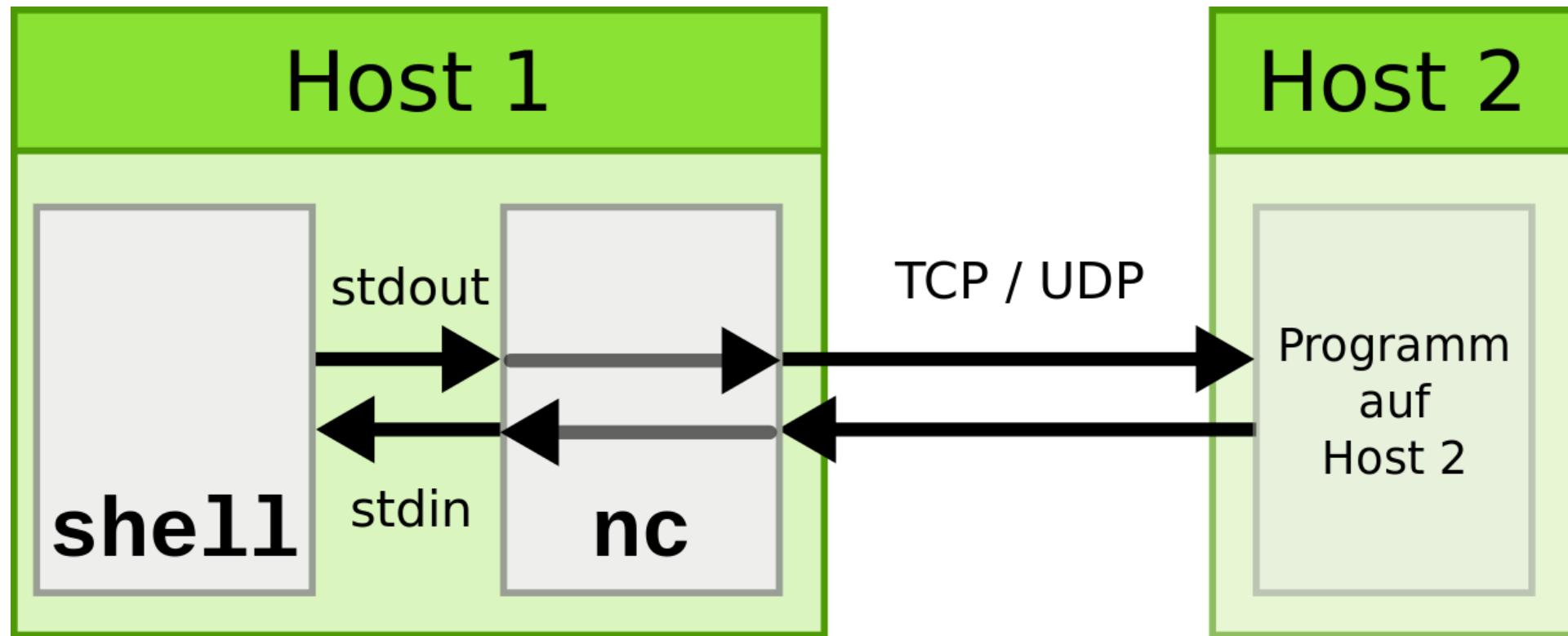
Netcat

NETCAT USES INCLUDE



- Data transfers
- Relays
- Port scanning
- Reverse shells
- Creating chats
- TCP commands

Netcat



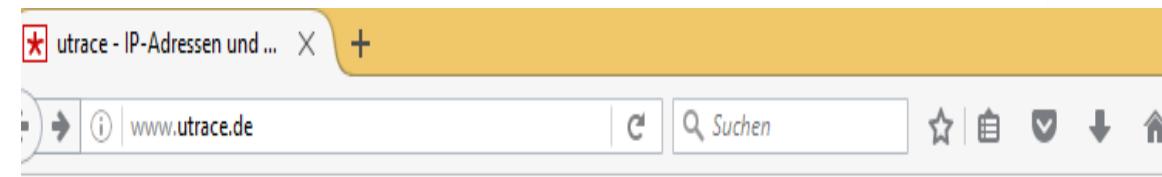
Netcat

```
nc -l 80 >>image.dd
```

```
dd if=/dev/sdb conv=sync,noerror | nc 10.10.0.253 80
```

E-Mail-Auswertung

Return-Path:
sisxxx1957@iconsystemplus.com
Received: from mailin12.aul.t-online.de (mailin12.aul.t-online.de [172.20.26.48])
by mhead406 with LMTP;
Sun, 19 Apr 2009 14:02:10 +0200
X-Sieve: CMU Sieve 2.3
Received: from host86-166-150-33.range86-166.btcentralplus.com
([86.166.150.33]) by
mailin12.aul.t-online.de
with esmtp id 1LvVik-1tia6C0;
Sun, 19 Apr 2009 14:02:02 +0200
To: <xxxIchxxx@t-online.de>
Subject: hi there
From: "Tanja Skrubenek"
sisxxx1957@iconsystemplus.com
Mime-Version: 1.0
Content-Type: text/html;
charset=iso-8859-1
Content-Transfer-Encoding: 7bit



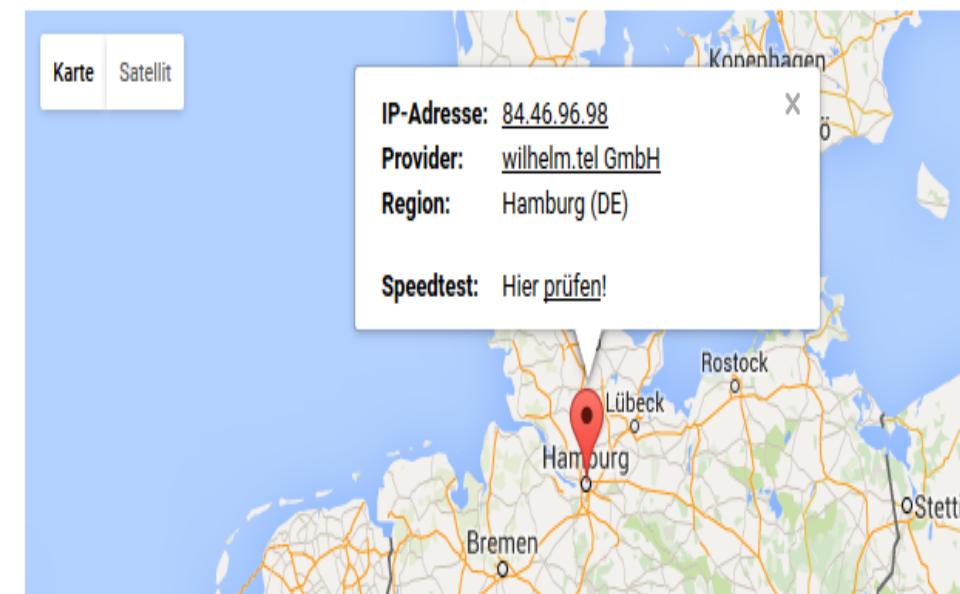
utrace*

IP-Adresse oder Domain:

86.166.150.33

Suchen

Die IP-Adresse "84.46.96.98" gehört zu folgender Region:



Wie der Zugriff auf Computerdaten bei Rechtsstreitigkeiten hilft - Mozilla Firefox
<https://mail.podium.de/owa/projection.aspx> 150% ⋮ X

Allen antworten | Löschen Junk-E-Mail | ...

Wie der Zugriff auf Computerdaten bei Rechtsstreitigkeiten hilft

Cellebrite <marketing2@cellebrite.com>
Fr 31.07.10:12
Honekamp, Wilfried

Allen antworten |

Gelöschte Elemente

Blockierte Inhalte werden angezeigt, während diese Nachricht geöffnet ist.

Wenn Sie Schwierigkeiten haben, diese E-Mail anzuzeigen, lesen Sie bitte die [Online-Version](#).

E-Mail-Auswertung: Body

Cellebrite Computer Access and Analysis Solutions

Guten Tag,

als Ermittler in Unternehmen sammeln Sie Beweismaterial aus einer Vielzahl digitaler Quellen wie Computern, mobilen Geräten und Cloud-Anwendungen

Wie der Zugriff auf Computerdaten bei Rechtsstreitigkeiten hilft - Mozilla Firefox
<https://mail.podium.de/owa/projection.aspx> 150% ⋮ X

Allen antworten | Löschen Junk-E-Mail | ...

Wie der Zugriff auf Computerdaten bei Rechtsstreitigkeiten hilft

Cellebrite <marketing2@cellebrite.com>
Fr 31.07, 10:12
Honekamp, Wilfried

Gelöschte Elemente

Blockierte Inhalte werden angezeigt, während diese Nachricht geöffnet ist.

Wenn Sie Schwierigkeiten haben, diese E-Mail anzuzeigen, [lesen Sie bitte d](#)

Cellebrite Computer Acc and Analysis Solution

Alle Antworten

Allen mit Besprechung antworten

Per Chatnachricht antworten

Allen per Chatnachricht antworten

Löschen

Als Junk-E-Mail markieren

Als Phishing markieren

Als ungelesen markieren

Kennzeichnen

Drucken

Nachrichtendetails anzeigen

E-Mail-Auswertung: Header anzeigen

Guten Tag,

als Ermittler in Unternehmen sammeln Sie Beweismaterial aus einer Vielzahl digitaler Quellen wie Computern, mobilen Geräten und Cloud-Anwendungen

E-Mail-Auswertung: Header anzeigen

[**https://hilfe.uni-paderborn.de/Mail_Header_anzeigen**](https://hilfe.uni-paderborn.de/Mail_Header_anzeigen)

oder Google

[**https://www.google.com/search?q=e-mail-header+anzeigen**](https://www.google.com/search?q=e-mail-header+anzeigen)

oder Ermittlungshilfe im Intrapol

X-Account-Key: account2
X-UIDL: 1135386310.15082
X-Mozilla-Status: 0001
X-Mozilla-Status2: 000000000
X-Mozilla-Keys:
Return-Path:

<sisxxx1957@iconsystemplus.com>
Received: from mailin12.aul.t-online.de
(mailin12.aul.t-online.de [172.20.26.48])
by mhead406 with LMTP;
Sun, 19 Apr 2009 14:02:10 +0200
X-Sieve: CMU Sieve 2.3
Received: from host86-166-150-33.range86-
166.btcentralplus.com ([86.166.150.33])
by mailin12.aul.t-online.de
with esmtp id 1LvVik-1tia6C0; Sun, 19 Apr
2009 14:02:02 +0200

To: <xxxIchxxx@t-online.de>
Subject: hi there
From: "Tanja Skrubeneck"
<sisxxx1957@iconsystemplus.com>

Mime-Version: 1.0
Content-Type: text/html; charset=iso-
8859-1
Content-Transfer-Encoding: 7bit
X-TOI-SPAM: n;1;2009-04-19T12:02:10Z
X-TOI-VIRUSSCAN: unchecked
X-TOI-EXPURGATEID: 149288::1240142522-
00005A3E-054D958C/0-0/0-0
X-TOI-SPAMCLASS: CLEAN, NORMAL

E-Mail-Forensik

E-Mail-Forensik

```
Return-Path:  
<sisxxx1957@iconsystemplus.com>  
Received: from mailin12.aul.t-online.de  
(mailin12.aul.t-online.de [172.20.26.48])  
by mhead406 with LMTP;  
Sun, 19 Apr 2009 14:02:10 +0200  
X-Sieve: CMU Sieve 2.3  
Received: from host86-166-150-33.range86-  
166.btcentralplus.com ([86.166.150.33])  
by mailin12.aul.t-online.de  
with esmtp id 1LvVik-1tia6C0; Sun, 19 Apr  
2009 14:02:02 +0200  
To: <xxxIchxxx@t-online.de>  
Subject: hi there  
From: "Tanja Skrubeneck"  
<sisxxx1957@iconsystemplus.com>  
Mime-Version: 1.0  
Content-Type: text/html; charset=iso-  
8859-1  
Content-Transfer-Encoding: 7bit
```

E-Mail-Forensik

Return-Path:
[<sisxxx1957@iconsystemplus.com>](mailto:sisxxx1957@iconsystemplus.com)
Received: from mailin12.aul.t-online.de
(mailin12.aul.t-online.de [172.20.26.48])
by mhead406 with LMTP;
Sun, 19 Apr 2009 14:02:10 +0200
X-Sieve: CMU Sieve 2.3
Received: from host86-166-150-33.range86-
166.btcentralplus.com ([86.166.150.33])
by mailin12.aul.t-online.de
with esmtp id 1LvVik-1tia6C0; Sun, 19 Apr
2009 14:02:02 +0200

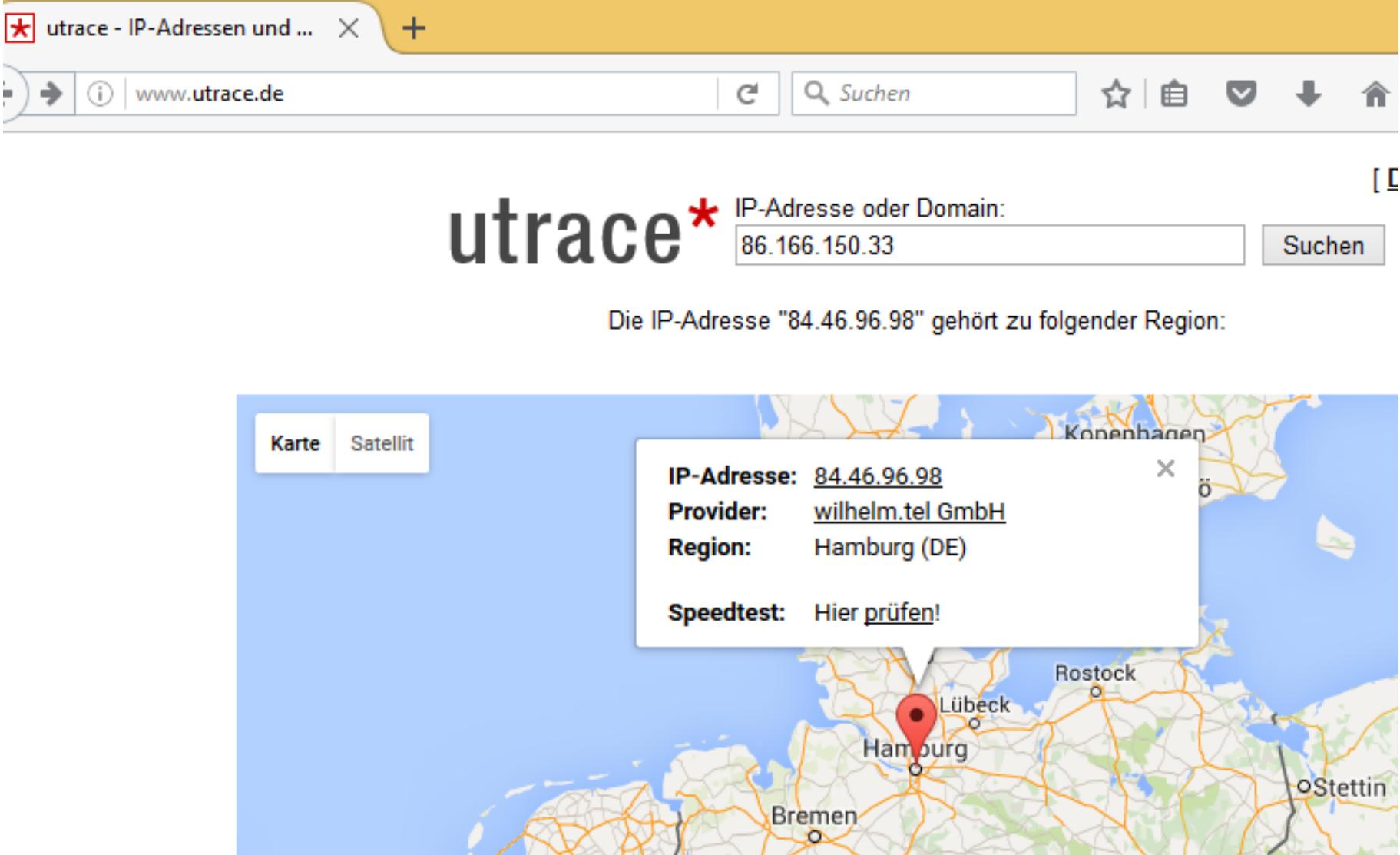
To: <xxxIchxxx@t-online.de>
Subject: hi there
From: "Tanja Skrubeneck"
[<sisxxx1957@iconsystemplus.com>](mailto:sisxxx1957@iconsystemplus.com)
Mime-Version: 1.0
Content-Type: text/html; charset=iso-
8859-1
Content-Transfer-Encoding: 7bit

E-Mail-Forensik

Return-Path:
sisxxx1957@iconsystemplus.com
Received: from mailin12.aul.t-online.de
(mailin12.aul.t-online.de [172.20.26.48])
by mhead406 with LMTP;
Sun, 19 Apr 2009 14:02:10 +0200
X-Sieve: CMU Sieve 2.3
Received: from host86-166-150-33.range86-
166.btcentralplus.com ([**86.166.150.33**])
by mailin12.aul.t-online.de
with esmtp id 1LvVik-1tia6C0; Sun, 19 Apr
2009 14:02:02 +0200

To: <xxxIchxxx@t-online.de>
Subject: hi there
From: "Tanja Skrubeneck"
sisxxx1957@iconsystemplus.com
Mime-Version: 1.0
Content-Type: text/html; charset=iso-
8859-1
Content-Transfer-Encoding: 7bit

E-Mail- Forensik



The screenshot shows a web browser window with the address bar containing "utrace - IP-Adressen und ... www.utrace.de". The main content area displays the "utrace" logo and a search bar with the placeholder "IP-Adresse oder Domain: 86.166.150.33" and a "Suchen" button. Below the search bar, a message states: "Die IP-Adresse "84.46.96.98" gehört zu folgender Region:". A map of Northern Germany highlights Hamburg, with a callout box providing details: "IP-Adresse: 84.46.96.98", "Provider: wilhelm.tel GmbH", "Region: Hamburg (DE)", and a "Speedtest: Hier prüfen!" link.

Wie arbeiten die Strafverfolgungsbehörden?

- Zentrale Providerdatenbank
- Providerabfrage
- Untersuchung/Durchsuchung/Kontaktaufnahme beim Verdächtigen

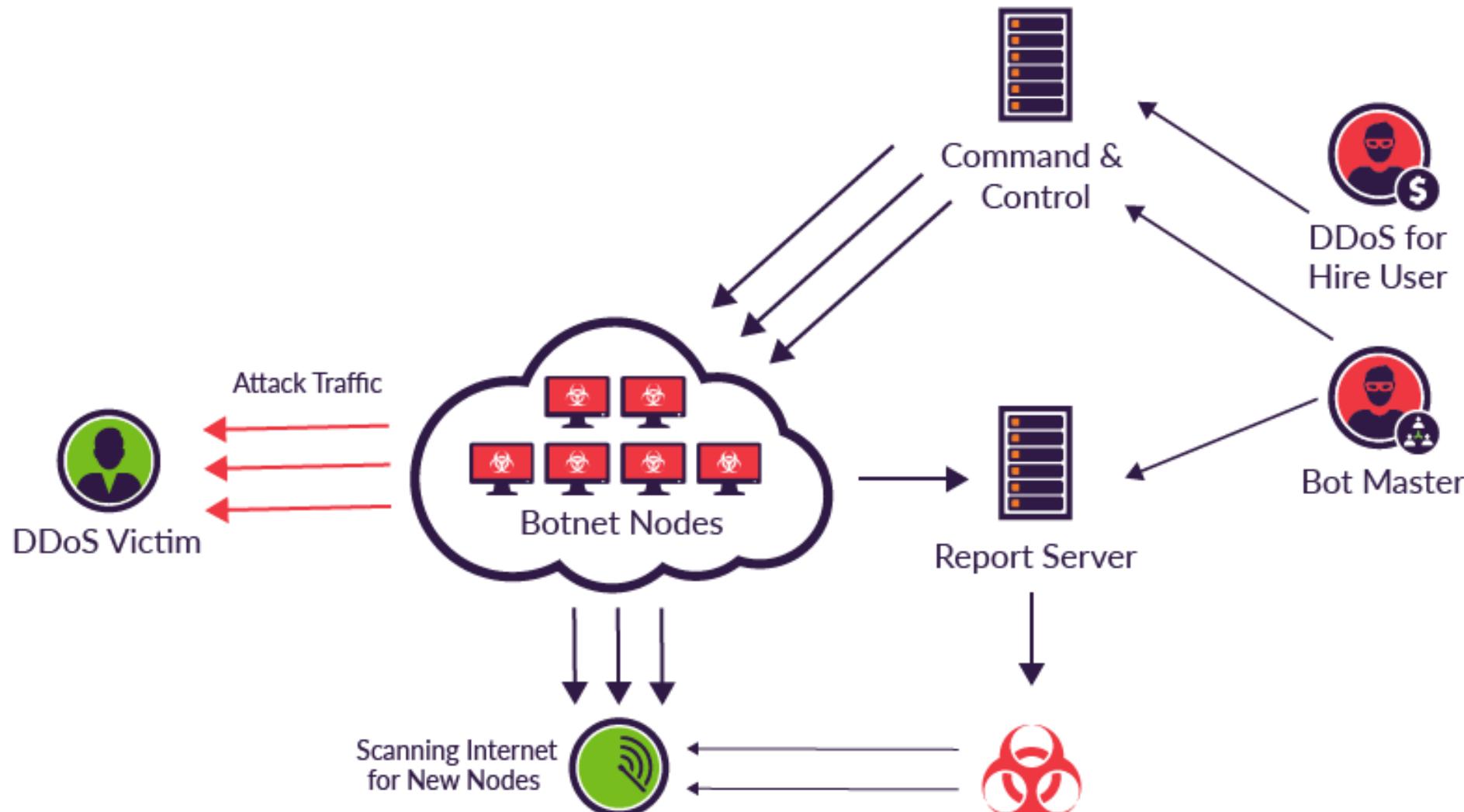
IoT: Internet of Things

Das Internet der Dinge ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen (Wikipedia).

IOT-Suchmaschinen

- **censys.io**
- **shodan.io**
- **thingful.net**
- **greynoise.io**
- **zoomeye.org**

IoT DDOS mit Mirai



<https://www.imperva.com/blog/>

how-to-identify-a-mirai-style-ddos-attack/

IoT-Suche mit Shodan



IOT-Suchmaschinen

 **Censys** 91.64.65.55 

. .65.55 (ip .dynamic.kabel-deutschland.de)

[Summary](#) [WHOIS](#) [Raw Data](#)

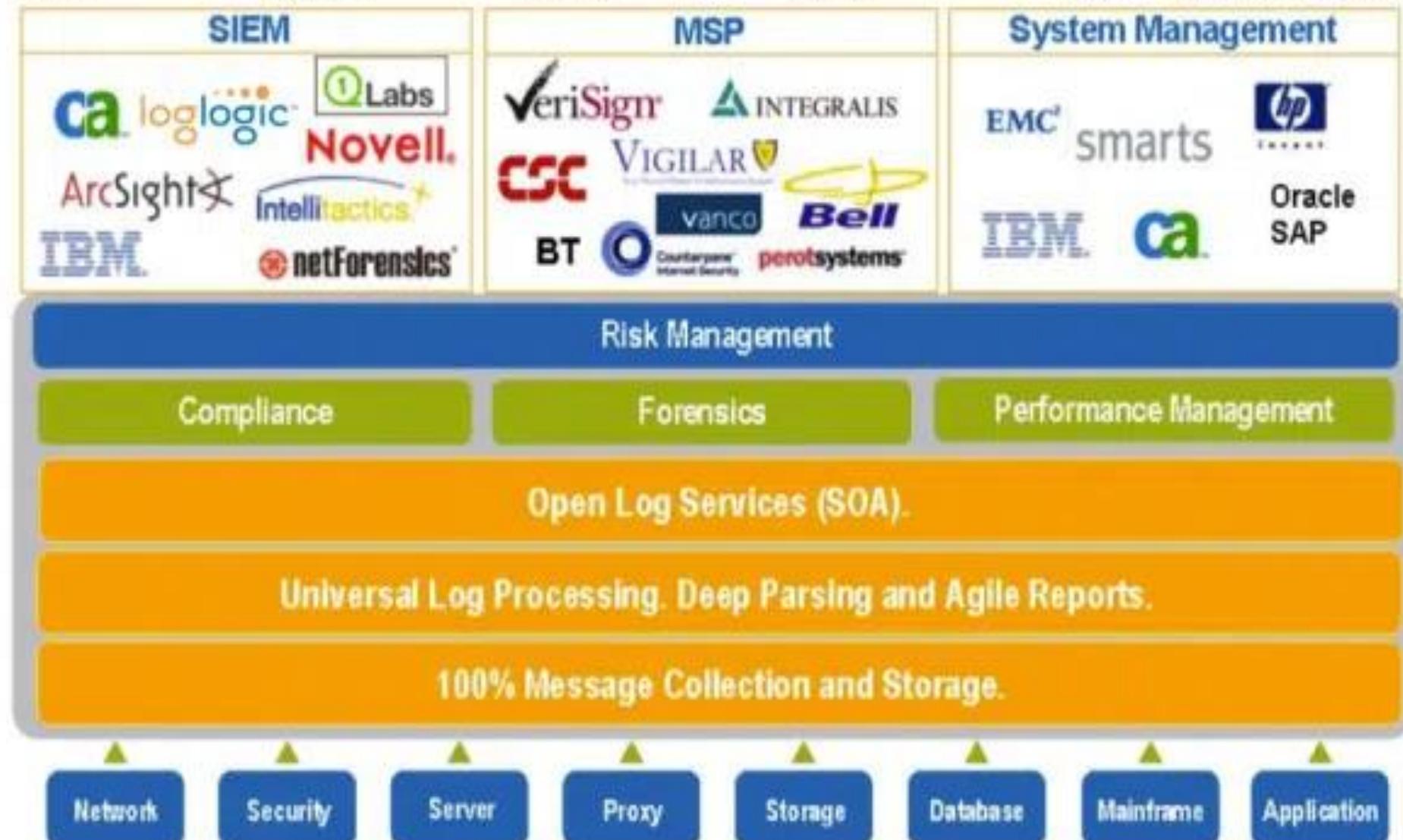
Basic Information

Network [VODANET International IP-Backbone of Vodafone \(DE\)](#)
Routing .0.0/14 via [AS7018](#), [AS1299](#), [AS1273](#), [AS3209](#)
Protocols [443/HTTPS](#)
Tags [HTTP](#) [HTTPS](#)

[443 /HTTPS](#)

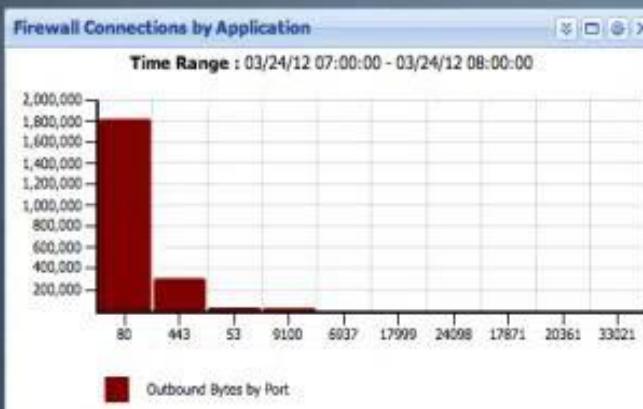
GET /

A map of Central Europe with a red pin marking a location in Germany. A callout box shows coordinates 52°23'45.2"N 13°24'0"E and the text "Größere Karte ansehen". The map also shows parts of Poland (Polen) and the Czech Republic (Tschechien). A Google logo is visible in the bottom right corner.



My Dashboard

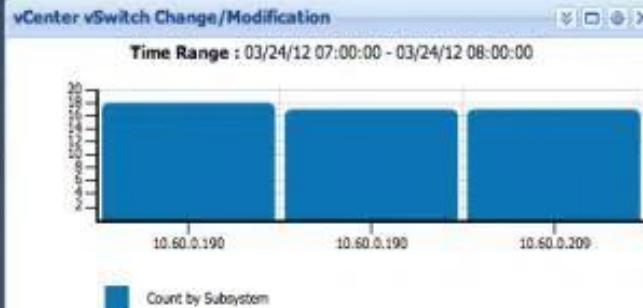
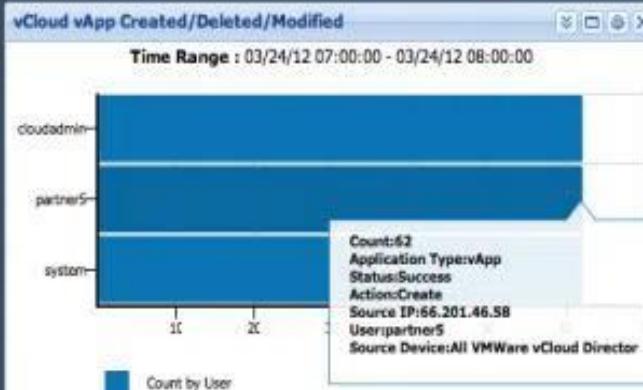
Alerts		
Time	Priority	Alert Name
2012-03-24 08:49:45	⚠	COBIT: Log
2012-03-24 08:44:45	⚠	COBIT: Log
2012-03-24 08:39:45	⚠	COBIT: Log
2012-03-24 08:34:30	⚠	COBIT: Log
2012-03-24 08:29:30	⚠	COBIT: Log
2012-03-24 08:24:30	⚠	COBIT: Log
2012-03-24 08:23:28	⚠	System Alert
2012-03-24 08:19:30	⚠	COBIT: Log
2012-03-24 08:14:15	⚠	COBIT: Log
2012-03-24 08:09:15	⚠	COBIT: Log



Firewall Statistic

Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00

#	Source Device	Denied Messages	Accepted Mess...	System Mess...	Security Mess...
1	netscreen.demo.com_netscr...	1153	2432	0	10
2	asa.demo.com_asa	203	1837	72	95



Hochschule Stralsund

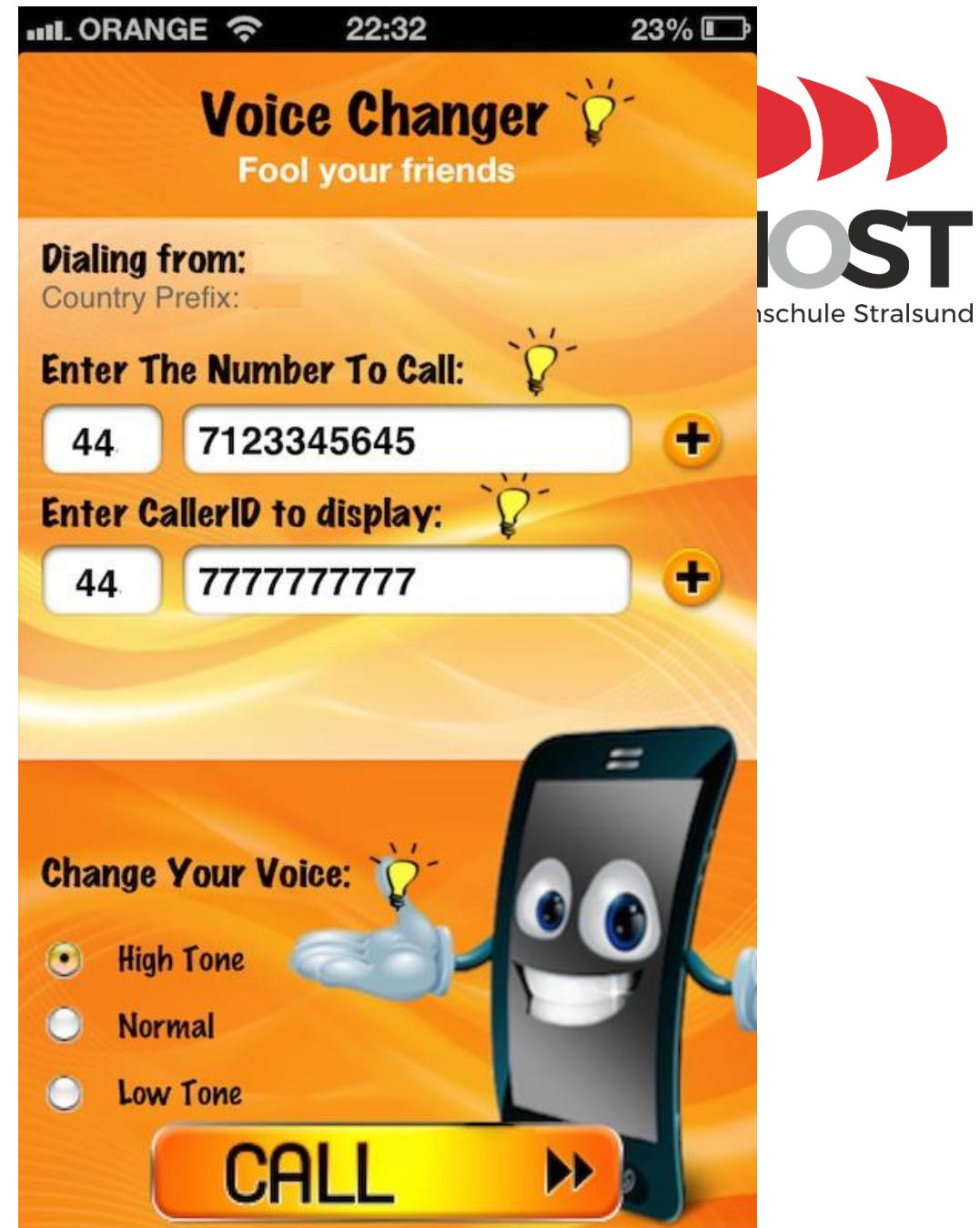
Angriffserkennung

- **LM**
- **IDS**
- **IPS**
- **SIM**
- **SEM**
- **SIEM**

Spoofing

- **Arp-Spoofing**
- **IP-Spoofing**
- **Call(er)-ID-Spoofing**

Call-ID-Spoofing



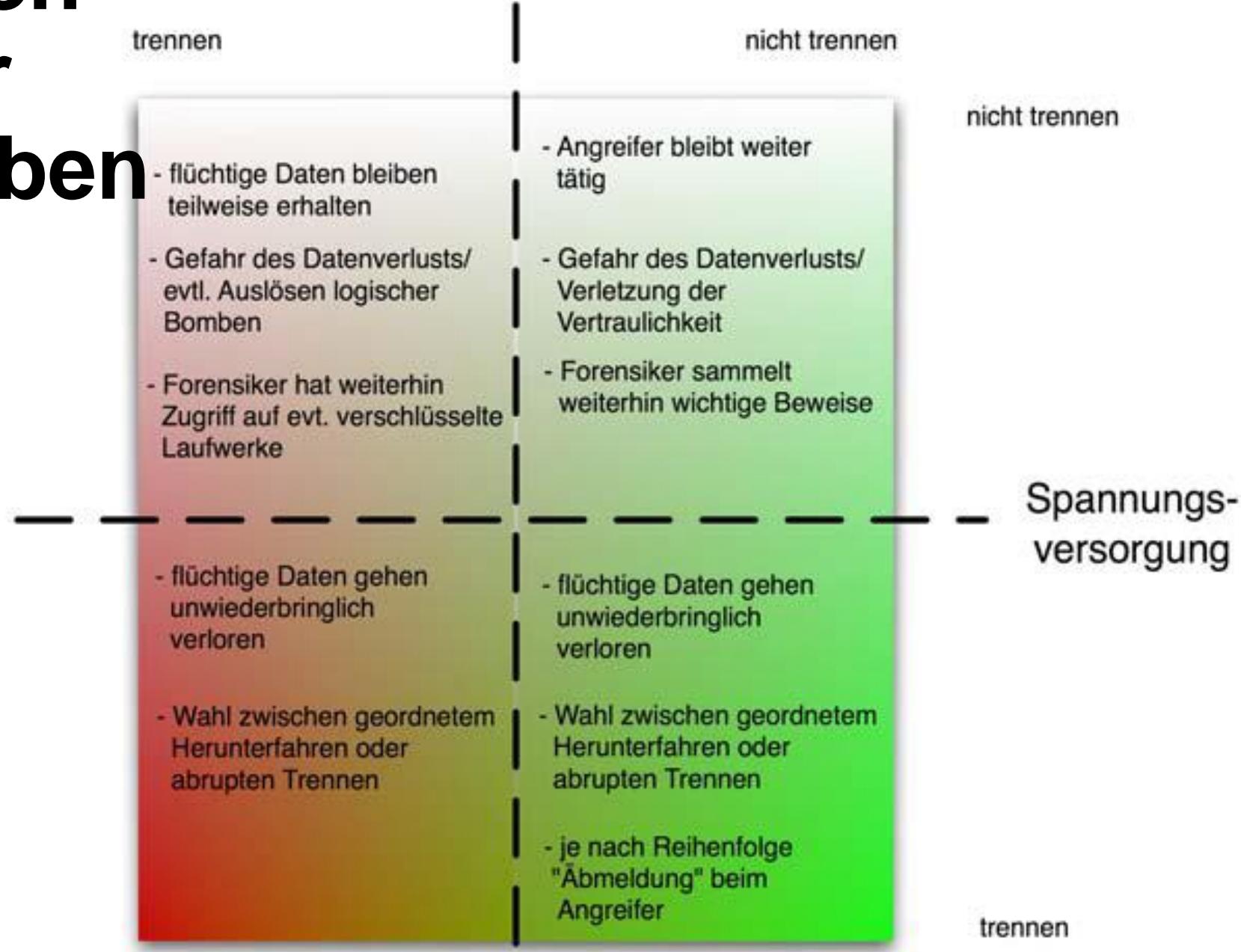
Grundlagen der IT-Forensik



Live-Forensik

Leben oder Sterben

Netzverbindung



Live vs Post Mortem: Flüchtigkeit

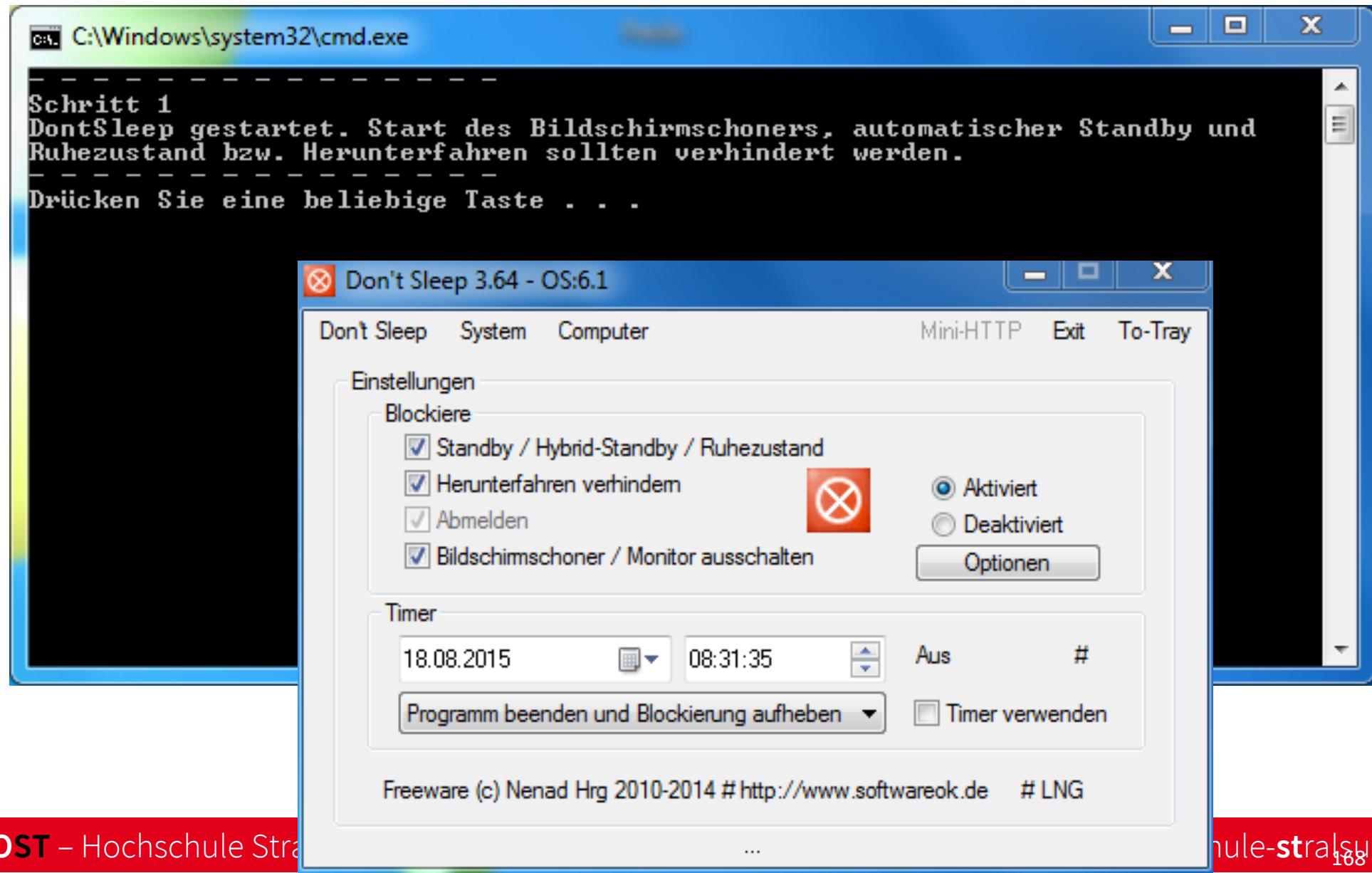
- CPU Register, CPU Cache
- Routing-Tabellen, ARP-Caches, Prozesstabellen, Kernel Statistiken
- Arbeitsspeicherinhalt
- geöffnete, verschlüsselte Dateisysteme
- temporäre Dateisysteme (z.B. Cloudspeicher)
- entfernt geführte Logging- und Monitordaten
- Massenspeicherinhalte
- physische Konfiguration, Netzwerktopologie
- Archivmedien

Live Untersuchung: laufender PC

- Routing-Tabellen, ARP-Caches, Prozesstabellen, Kernel Statistiken
- Arbeitsspeicherinhalt
- geöffnete, verschlüsselte Dateisysteme
- temporäre Dateisysteme (z.B. Cloudspeicher)

→ Durchsuchungskonzept

Durchsuchungskonzept



Durchsuchungskonzept

```
C:\Windows\system32\cmd.exe

chrome.exe          672 Console      2       23.172 K
chrome.exe          3532 Console     2       63.504 K
DontSleep.exe       4924 Console     2        7.756 K
taskhost.exe        4620 Console     2       11.100 K
OSPPSUC.EXE         3788 Services    0       13.772 K
chrome.exe          3576 Console     2       61.756 K
audiogd.exe         2424 Services    0       15.696 K
WINWORD.EXE         5076 Console     2      153.684 K
wisptis.exe         2932 Console     2        8.564 K
SnippingTool.exe   2832 Console     2       12.168 K
WmiPrvSE.exe        5888 Services    0        8.532 K
SearchProtocolHost.exe 1644 Services    0       8.704 K
SearchFilterHost.exe 5396 Services    0       6.928 K
cmd.exe             5084 Console     2        3.536 K
conhost.exe         5008 Console     2       5.808 K
tasklist.exe        5480 Console     2       6.024 K
-----
Schritt 2
Pruefen Sie auf Fernsteuerungssoftware (Teamviewer, VNC usw.)
und beenden Sie ggf. diese Programme zur Not ueber den Taskmanager!
Wenn Sie die Gefahr sehen, dass per Fernsteuerung relevante lokale
Daten geloescht werden, trennen Sie jetzt die
Netzwerkverbindungen (LAN/WLAN)!

Drücken Sie eine beliebige Taste . . .
```

Durchsuchungskonzept

```
C:\Windows\system32\cmd.exe
192.168.12.3      00-50-56-b1-1b-a1    dynamisch
192.168.12.4      00-50-56-bf-25-42    dynamisch
192.168.12.6      00-50-56-b1-2a-63    dynamisch
192.168.12.253    00-50-56-9f-1b-7e    dynamisch
192.168.17.61     40-01-c6-bf-4d-81    dynamisch
192.168.99.222    68-b5-99-c8-32-2c    dynamisch
192.168.127.255   ff-ff-ff-ff-ff-ff    statisch
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
239.255.255.250   01-00-5e-7f-ff-fa    statisch
255.255.255.255   ff-ff-ff-ff-ff-ff    statisch

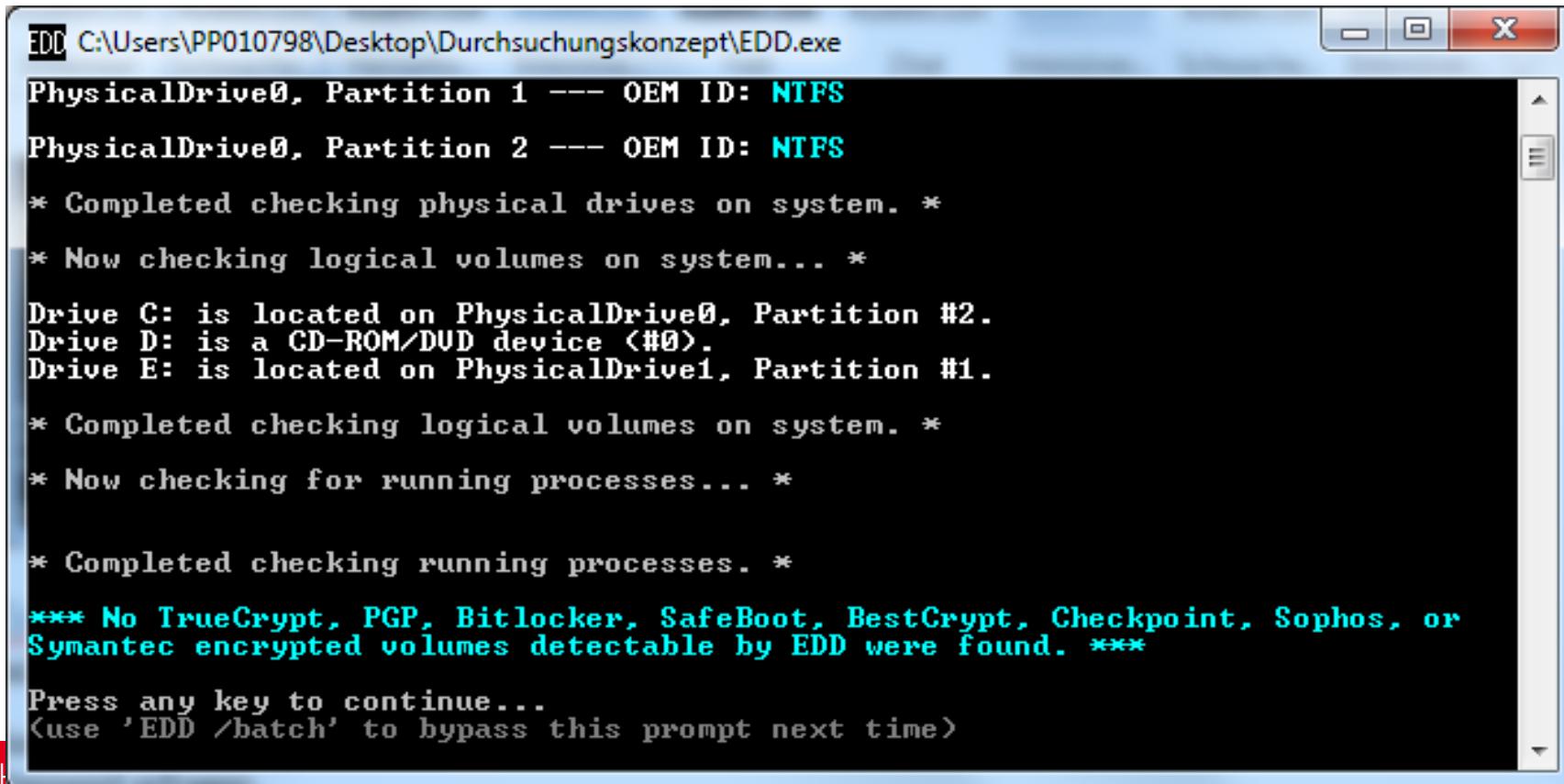
Schnittstelle: 192.168.56.1 --- 0x10
Internetadresse      Physische Adresse      Typ
192.168.56.255       ff-ff-ff-ff-ff-ff    statisch
224.0.0.22            01-00-5e-00-00-16    statisch
224.0.0.252           01-00-5e-00-00-fc    statisch
239.255.255.250      01-00-5e-7f-ff-fa    statisch

-----
Schritt 3
Pruefen Sie, ob die Netzverbindungen auf weitere Computer
hinweisen (Router, Smartphones, Tablets, Notebooks ...)?
-----
Drücken Sie eine beliebige Taste . . .
```

Durchsuchungskonzept

ACHTUNG: Administratorrechte erforderlich.

Sollte der derzeit angemeldete Nutzer kein Administrator sein, nach Belehrung Benutzername und Passwort erfragen.



```
EDD C:\Users\PP010798\Desktop\Durchsuchungskonzept\EDD.exe
PhysicalDrive0, Partition 1 --- OEM ID: NTFS
PhysicalDrive0, Partition 2 --- OEM ID: NTFS
* Completed checking physical drives on system. *
* Now checking logical volumes on system... *
Drive C: is located on PhysicalDrive0, Partition #2.
Drive D: is a CD-ROM/DVD device (#0).
Drive E: is located on PhysicalDrive1, Partition #1.

* Completed checking logical volumes on system. *

* Now checking for running processes... *

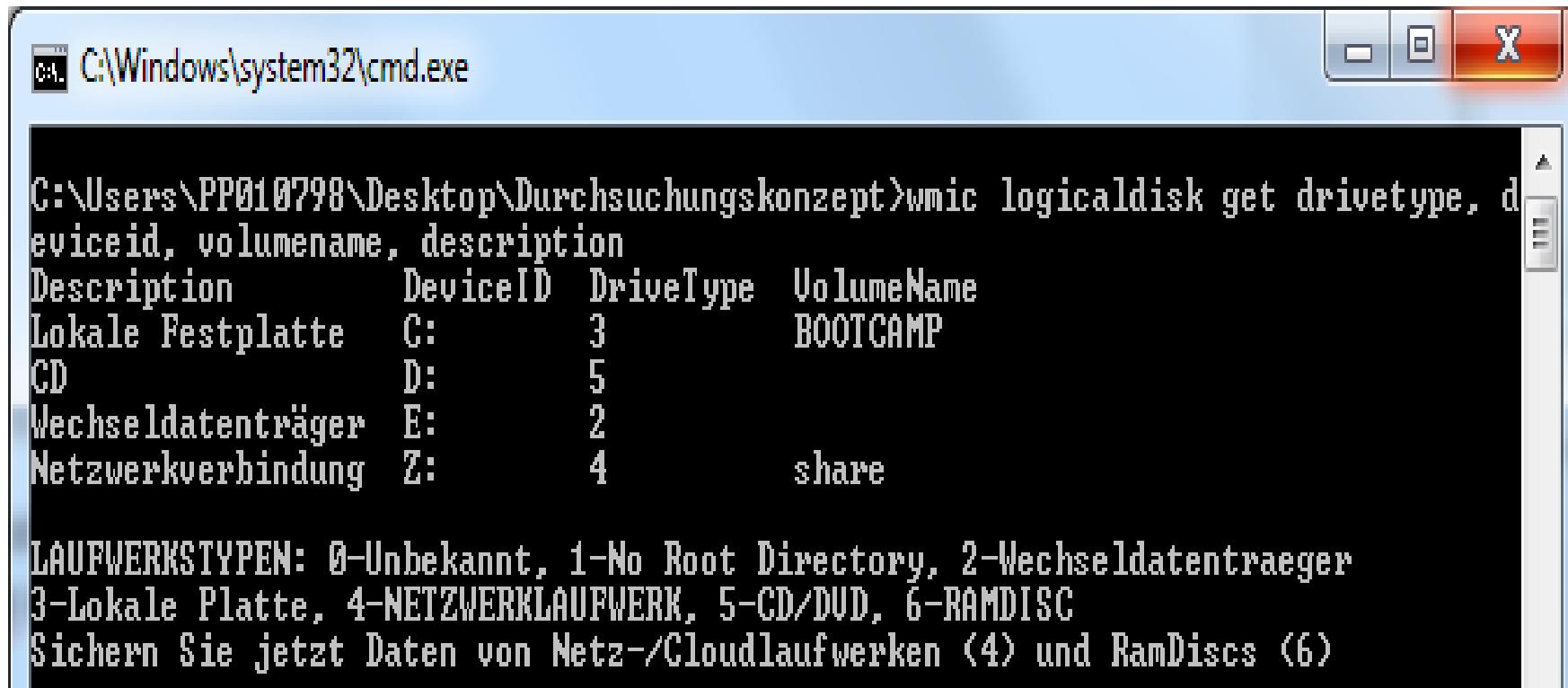
* Completed checking running processes. *

*** No TrueCrypt, PGP, BitLocker, SafeBoot, BestCrypt, Checkpoint, Sophos, or
Symantec encrypted volumes detectable by EDD were found. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

Durchsuchungskonzept

Sichern Sie nun relevante Daten von Netz-, Cloud- und/oder kryptierten Laufwerken. Denken Sie an die beschraenkte Kapazitaet Ihres Sicherungsmediums! Wenn der Speicher nicht ausreicht, jetzt Unterstuetzung anfordern!

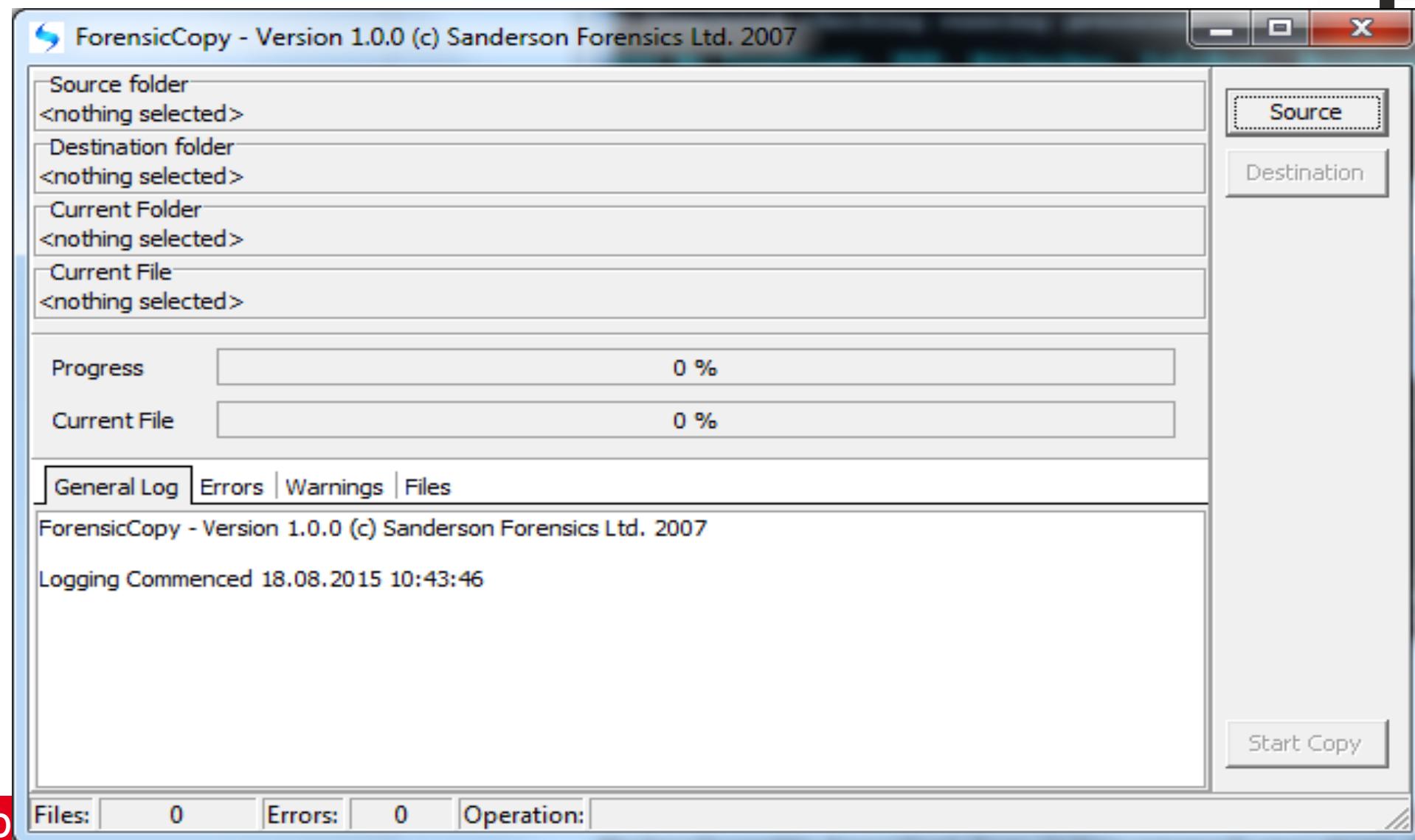


C:\Windows\system32\cmd.exe

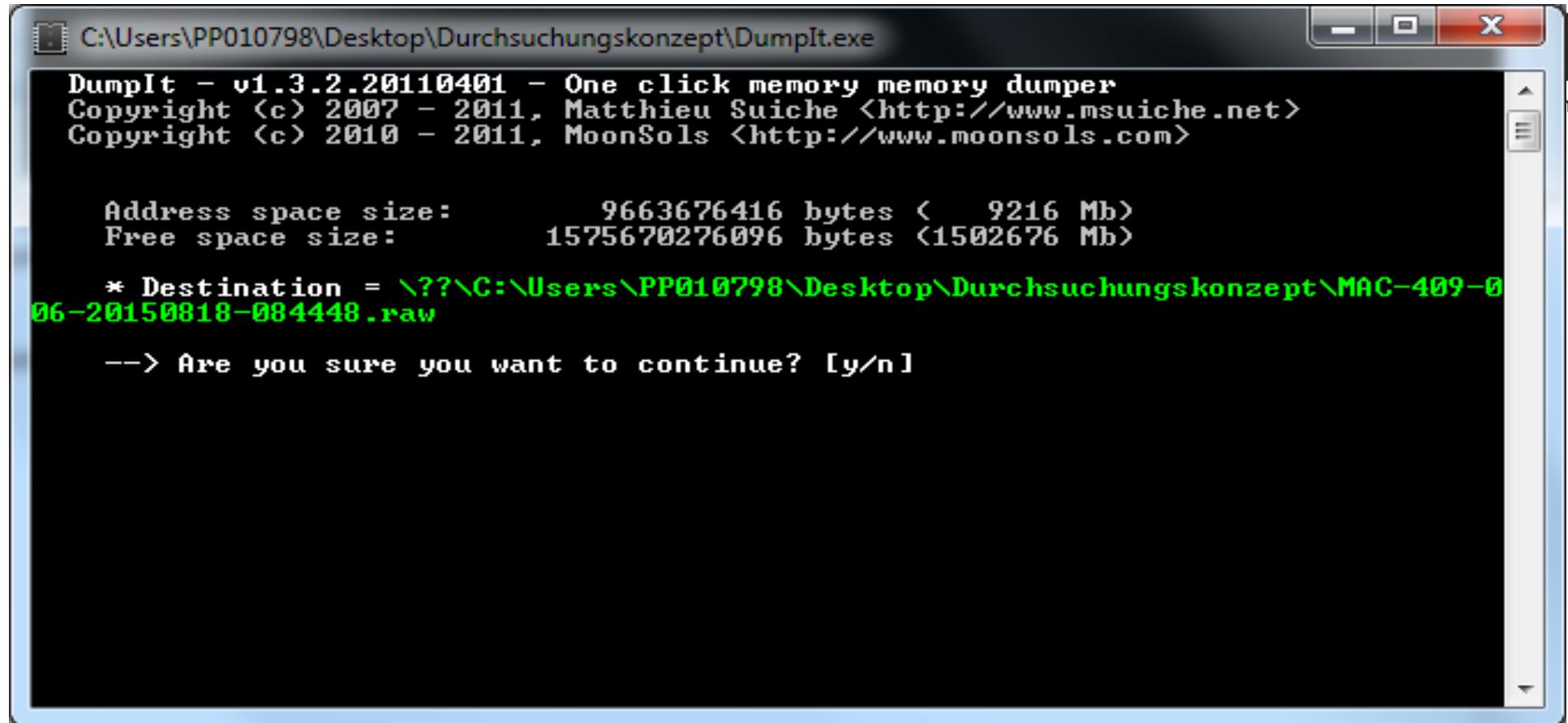
```
C:\Users\PP010798\Desktop\Durchsuchungskonzept>wmic logicaldisk get drivetype, deviceid, volumename, description
Description          DeviceID  DriveType  VolumeName
Lokale Festplatte   C:        3           BOOTCAMP
CD                  D:        5
Wechseldatenträger E:        2
Netzwerkverbindung Z:        4           share

LAUFWERKSTYPEN: 0-Unbekannt, 1-No Root Directory, 2-Wechseldatentraeger
3-Lokale Platte, 4-NETZWERKLAUFWERK, 5-CD/DVD, 6-RAMDISC
Sichern Sie jetzt Daten von Netz-/Cloudlaufwerken (4) und RamDiscs (6)
```

Durchsuchungskonzept



Durchsuchungskonzept



C:\Users\PP010798\Desktop\Durchsuchungskonzept\DumpIt.exe

```
DumpIt - v1.3.2.20110401 - One click memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      9663676416 bytes ( 9216 Mb)
Free space size:        1575670276096 bytes (1502676 Mb)

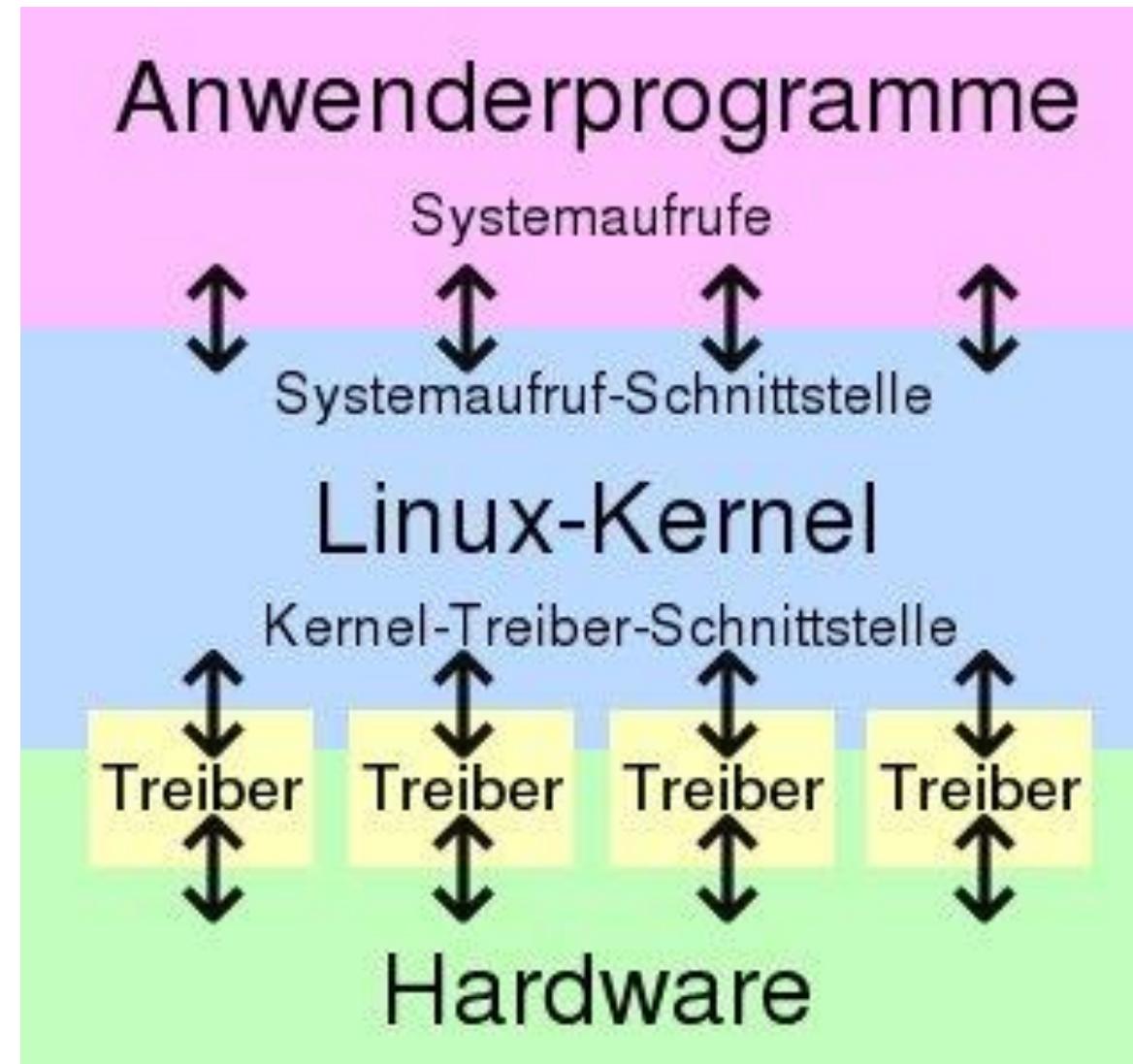
* Destination = \??\C:\Users\PP010798\Desktop\Durchsuchungskonzept\MAC-409-0
06-20150818-084448.raw

--> Are you sure you want to continue? [y/n]
```

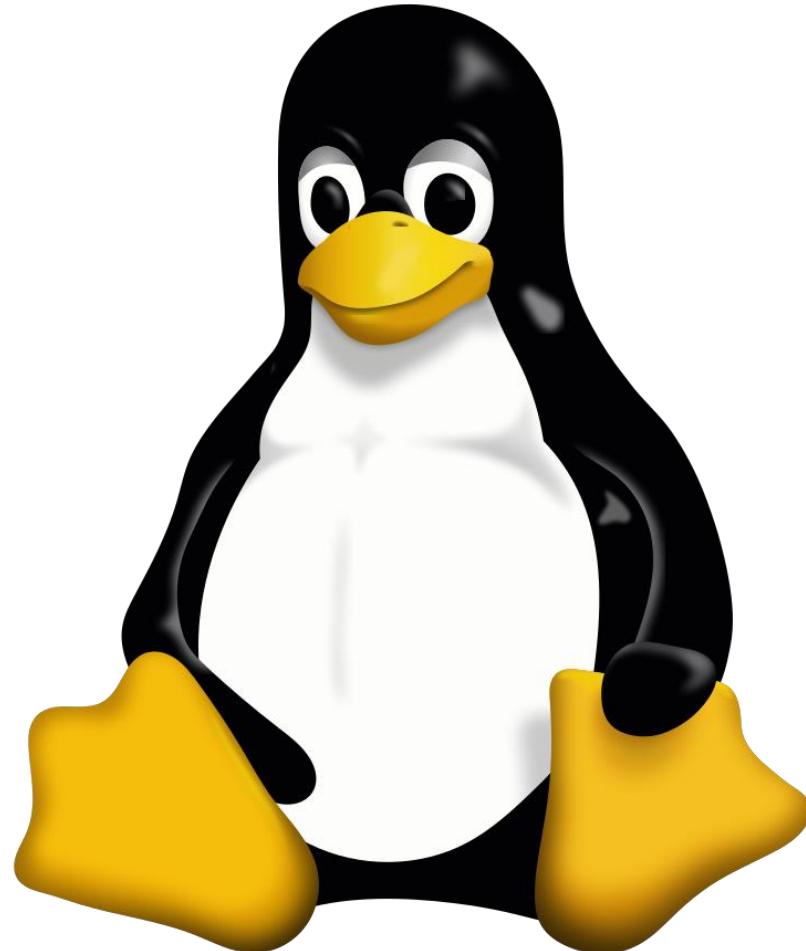
Wenn der Speicher gesichert wurde (Meldung: Success), oder die Sicherung nicht möglich war, ist die Live-Sicherung beendet. Wenn nichts Aussergewöhnliches dagegen spricht, jetzt Netzstecker ziehen.

Linux-Forensik

- **Systemaufbau**
- **Linux als Auswertesystem**
- **Einige grundlegende Befehle**
- **Verzeichnisstruktur**
- **Forensisch relevante Daten**



Warum Linux als Auswertesystem?



Warum nicht Linux als Auswertesystem?



The Law Enforcement and Forensic Examiner's Introduction to Linux

A Comprehensive Practitioner's Guide to Linux
as a Digital Forensics Platform



Linux als Auswertesystem



Linux Forensic Distributions



slackware
—linux



Linux Commands

```
(kali㉿kali)-[~]
$ sudo lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  80G  0 disk 
└─sda1   8:1    0  79G  0 part /
└─sda2   8:2    0    1K  0 part 
└─sda5   8:5    0 975M  0 part [SWAP]
sr0     11:0    1 1024M  0 rom
```

Linux Commands

```
(kali㉿kali)-[~]
$ sudo fdisk -l /dev/sda
```

1 >

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

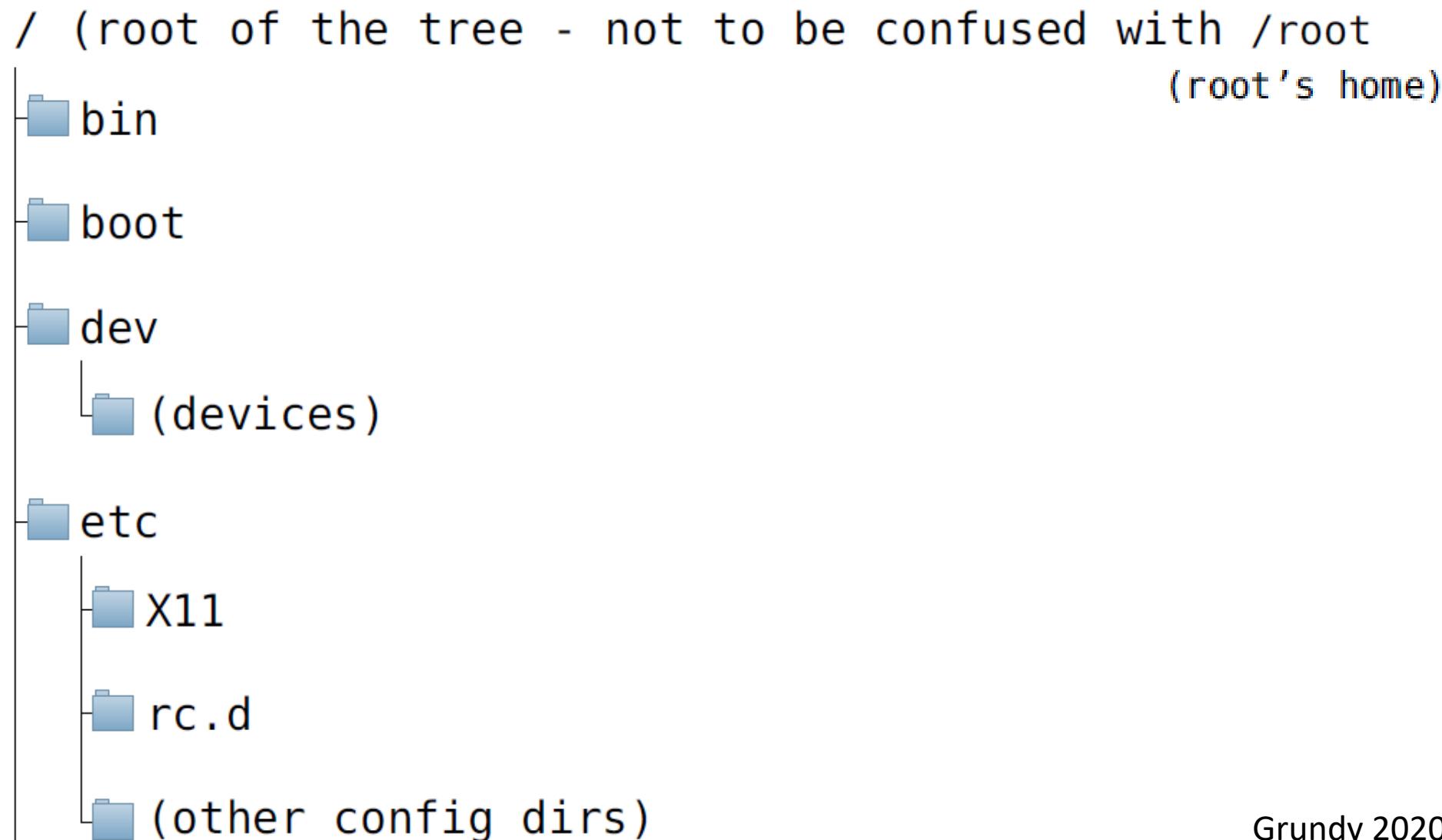
- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for kali:
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0f6b9b0

Device      Boot   Start     End   Sectors  Size Id Type
/dev/sda1    *       2048 165771263 165769216   79G 83 Linux
/dev/sda2          165773310 167770111   1996802  975M  5 Extended
/dev/sda5          165773312 167770111   1996800  975M 82 Linux swap / Solaris
```

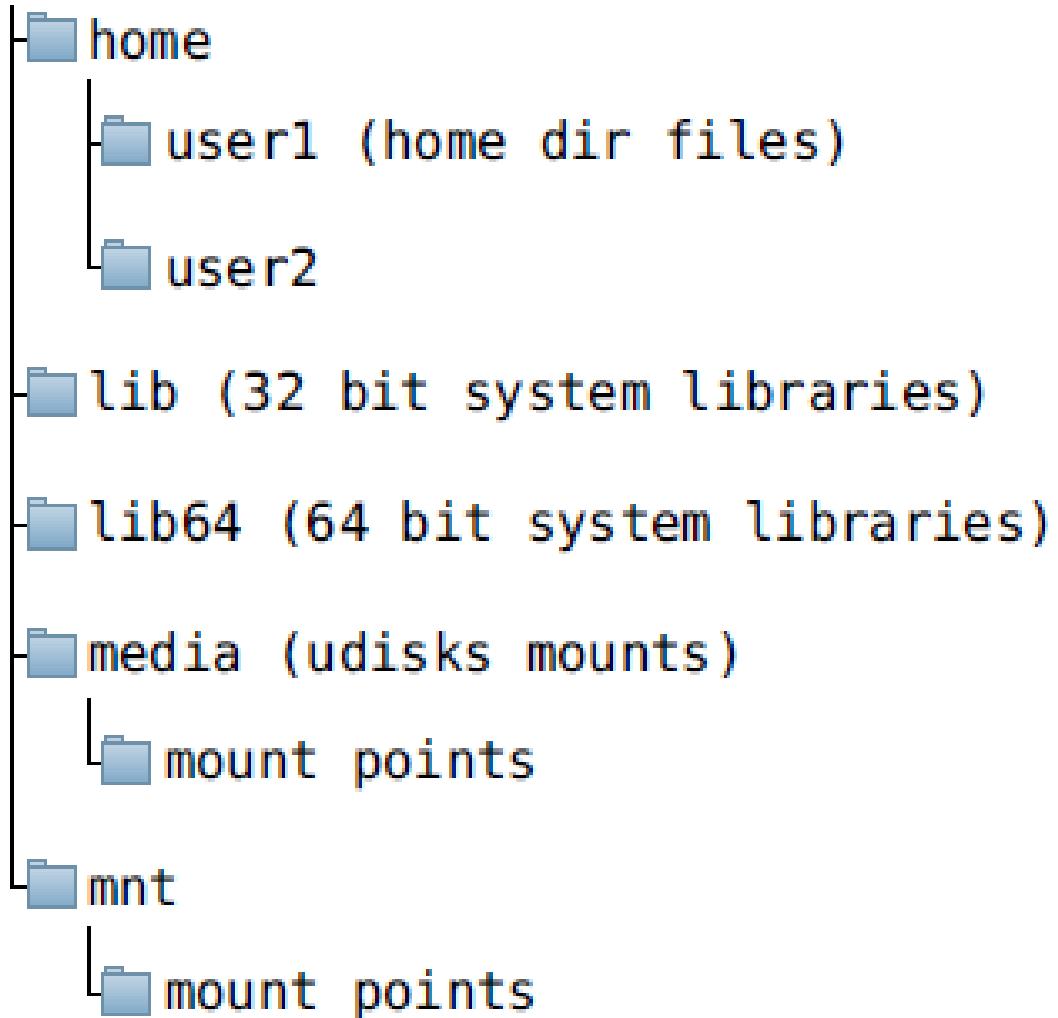
```
(kali㉿kali)-[~]
$ █
```

Linux Verzeichnisbaum



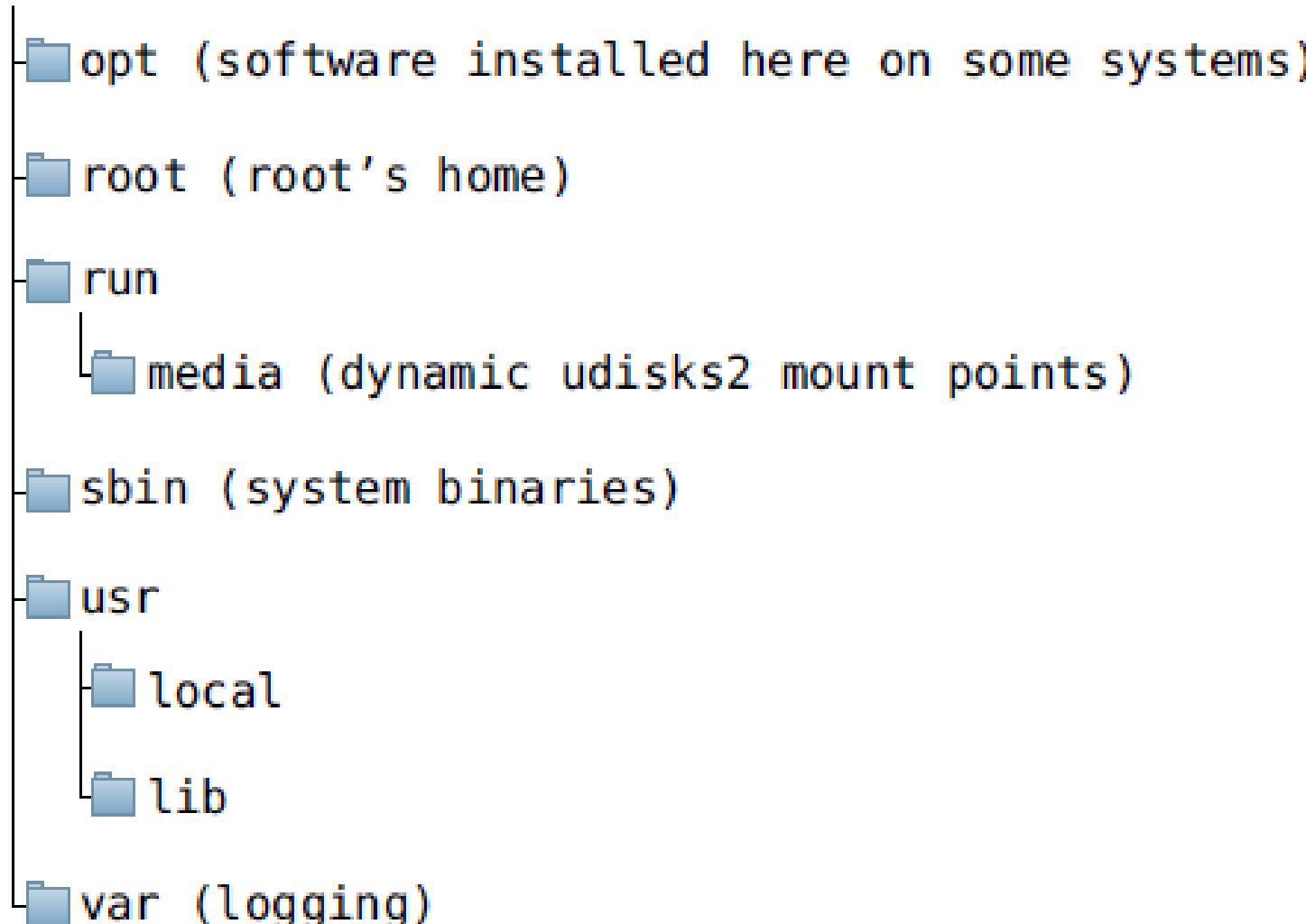
Grundy 2020

Linux Verzeichnisbaum



Grundy 2020

Linux Verzeichnisbaum



Grundy 2020

Linux mount at boot

```
root@forensicbox:~# cat /etc/fstab
```

/dev/sda2	swap	swap	defaults	0	0
/dev/sda3	/	ext4	defaults	1	1
/dev/sda1	/boot	ext4	defaults	1	2
/dev/cdrom	/mnt/cdrom	auto	noauto,owner,ro	0	0
devpts	/dev/pts	devpts	gid=5,mode=620	0	0
proc	/proc	proc	defaults	0	0
tmpfs	/dev/shm	tmpfs	defaults	0	0

Linux ls command

ls	Verzeichnisinhalt
ls -a	inkl. versteckte Dateien
ls -l	detailliert
ls -lh	detailed mit Buchstaben bei Dateigröße
ls -R	auch aller Unterverzeichnisse

Linux Dateiinformationen

- **Lesen („r“)**
- **Schreiben („w“)**
- **Ausführen („x“)**

für:

- **Dateibesitzer**
- **Mitglieder in der Gruppe des Besitzers**
- **Alle anderen**

Linux Dateiinformationen

```
drwxr-xr-x 136 ritth staff      4624  9 Jul  2011 phpwhois-4.2.2
-rw-r--r--   1 ritth staff     92362  8 Aug  2014 phpwhois-4.2.2.tar.gz
-rw-r-----   1 ritth staff  13546932 16 Nov 11:16 pqdm421x9all.dmg
-rw-r--r--   1 ritth staff  18500316  7 Jan  2014 professional_demo.dmg
-rw-r-----   1 ritth staff  1326818 16 Nov 11:18 pu2m200x9all.dmg
-rw-r--r--   1 ritth staff  149247 22 Jan 21:04 puk-handhabung-2.pdf
-rw-r--r--   1 ritth staff  149247 22 Jan 20:47 puk-handhabung.pdf
-rw-r-----   1 ritth staff  770505 16 Nov 11:18 pum14026x9all.dmg
----- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Rittelmeier 2016

Zeit der Echtzeituhr (RTC)

/proc/driver/rtc

Da unter Linux die Systemzeit bei Veränderung nicht sofort in die RTC zurückgeschrieben wird, kann man hier Manipulationen erkennen

Zeitzone

/etc/timezone

Befehle beim Systemstart

/etc/rc.local

Hauptspeicherdaten

/proc/kcore

Teile des virtuellen Adressraums können dort gesichert werden.

Auslagerungsdaten

/proc/swaps

Eine Liste der genutzten Swap-Dateisysteme.
Linux kann analog zur Pagefile.sys Dateien
verwenden oder dedizierte Swap-Partitionen.

Dateisysteme

/proc/mounts

Liste der genutzten Dateisysteme, wo deren Einhängepunkt ist und wo sie sich physisch befinden.

Datenträger und Partitionen

/proc/partitions

Liste der vorhandenen Datenträger und deren Partitionen. Zusätzlich zum Namen ist für jede Partition auch deren Größe in Blöcken angegeben.

Systemeinstellungen

/proc/sys

Weitere Systemeinstellungen, z. B. /net/ipv4/

Aktuelle Kernel-Version

/proc/version

Speicherauslastung

/proc/meminfo

Kernel-Konfiguration

/proc/config.gz

Routen-Tabelle

/proc/net/route

Iface	Destination	Gateway	Flags	RefCnt	Use	Metric	Mask	MTU	Window	IRTT
eth0	0000A8C0	00000000	0001	0	0	0	00FFFFFF	0	0	0
eth0	00000000	0100A8C0	0003	0	0	0	00000000	0	0	0

ARP-Tabelle

/proc/net/arp

Linux ARP-Tabelle

```
root@utopia:~# cat /proc/net/arp
```

IP address	HW type	Flags	HW address	Mask	Device
192.168.85.26	0x1	0x2	00:1A:4F:85:0F:6D	*	eth1
192.168.85.31	0x1	0x2	00:12:43:30:C1:E7	*	eth1
192.168.85.1	0x1	0x2	00:0C:29:8A:B1:69	*	eth1
192.168.85.88	0x1	0x2	00:21:85:FB:66:3B	*	eth1
192.168.85.157	0x1	0x2	00:24:21:9C:71:34	*	eth1
192.168.85.24	0x1	0x2	00:16:38:AE:1D:F4	*	eth1
192.168.85.86	0x1	0x2	00:00:F0:20:C8:E6	*	eth1
192.168.85.30	0x1	0x2	00:0A:8A:A2:30:B5	*	eth1
192.168.85.128	0x1	0x2	00:30:1B:B8:1E:6C	*	eth1

```
root@utopia:~# arp -n
```

Adresse	Hardware-Typ	Hardware-Adresse	Optionen	Maske	Schnittstelle
---------	--------------	------------------	----------	-------	---------------

192.168.85.26	ether	00:1A:4F:85:0F:6D	C		eth1
192.168.85.31	ether	00:12:43:30:C1:E7	C		eth1
192.168.85.1	ether	00:0C:29:8A:B1:69	C		eth1
192.168.85.88	ether	00:21:85:FB:66:3B	C		eth1
192.168.85.157	ether	00:24:21:9C:71:34	C		eth1
192.168.85.24	ether	00:16:38:AE:1D:F4	C		eth1
192.168.85.86	ether	00:00:F0:20:C8:E6	C		eth1
192.168.85.30	ether	00:0A:8A:A2:30:B5	C		eth1
192.168.85.128	ether	00:30:1B:B8:1E:6C	C		eth1

Forensisch relevante Daten

MAC-Adresse

`/sys/class/net/eth0/address`

Forensisch relevante Daten

Statistische Daten der Netzwerkadapter

/proc/net/dev

- gesendeten und empfangenen Daten
- Anzahl der verworfenen (drop) Pakete
- Anzahl aufgetretener Fehler (errors)
- Auch in /sys/class/net/**eth0/statistics/**

Verfolgung von IP-Adressen (wenn aktiviert)

/proc/net/ip_conntrack
/proc/net/nf_conntrack

*tcp 6 431968 ESTABLISHED src=192.168.0.188
dst=192.168.0.1 sport=2388 dport=22 packets=23
bytes=2995 src=192.168.0.1 dst=192.168.0.188 sport=22
dport=2388 packets=24 bytes=3909 [ASSURED] mark=0
use=1*

Prozessdaten

/proc/Prozessnummer

/fd Liste der verwendeten Dateien
status Prozessstatus

Kernel-Logs

/proc/kmsg

Beispielsweise die Verwendung eines USB-Sticks,
dessen Nutzung im Kernel-Log vermerkt wird.

Durchschnittliche Systemauslastung

/proc/loadavg

Statistik zur Auslastung des Systems innerhalb eines gewissen Zeitraums mit Anzahl der aktiven Prozesse und Gesamtanzahl von Prozessen.

User Accounts

/etc/passwd

Forensisch relevante Daten

User Accounts

/etc/passwd

UID	User name	Real name	Home directory	Created
1000	nata	Natalie Roberts	/home/nata	2021-06-14 11:58:28
1001	Mina	Mina Mone	/home/Mina	2021-06-14 19:10:51
1002	paul	Paul Roberts	/home/paul	2021-06-14 22:53:10

User Accounts, Gruppen

/etc/group

Logdateien

/var/log

Z. B. syslog, ***messages***, auth.log, wtmp, ***apt***

Mehr unter:

<https://wiki.ubuntuusers.de/Logdateien/>

Apache Webserver

/var/log/apache2

Bereitgestellte Webserver-Dateien

/var/www