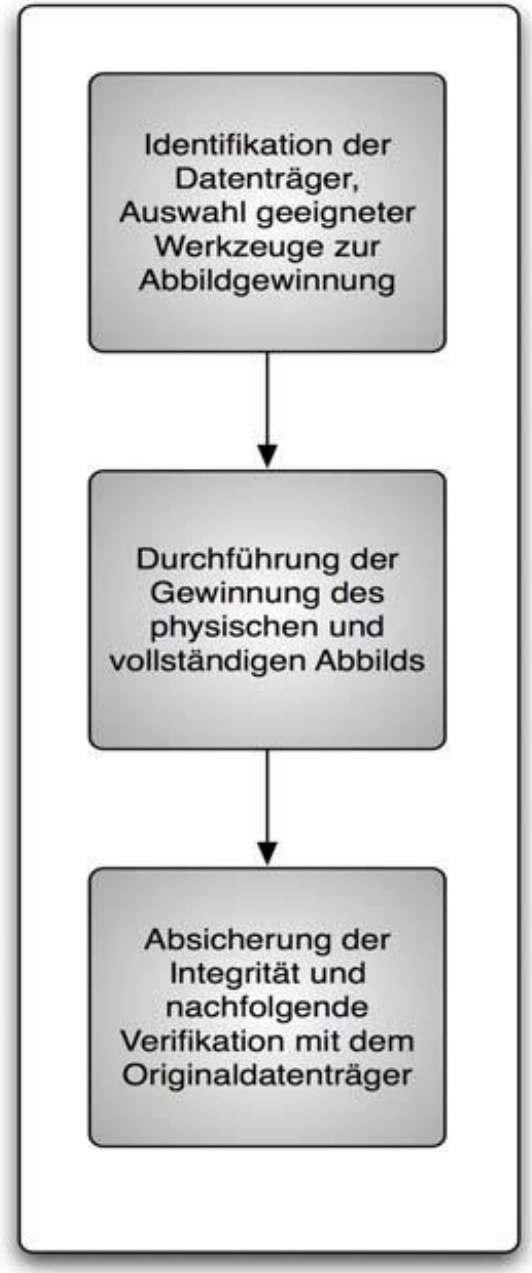
# Abbilderstellung



# Forensische Kopie mit DD

Hochschule Stralsund

**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

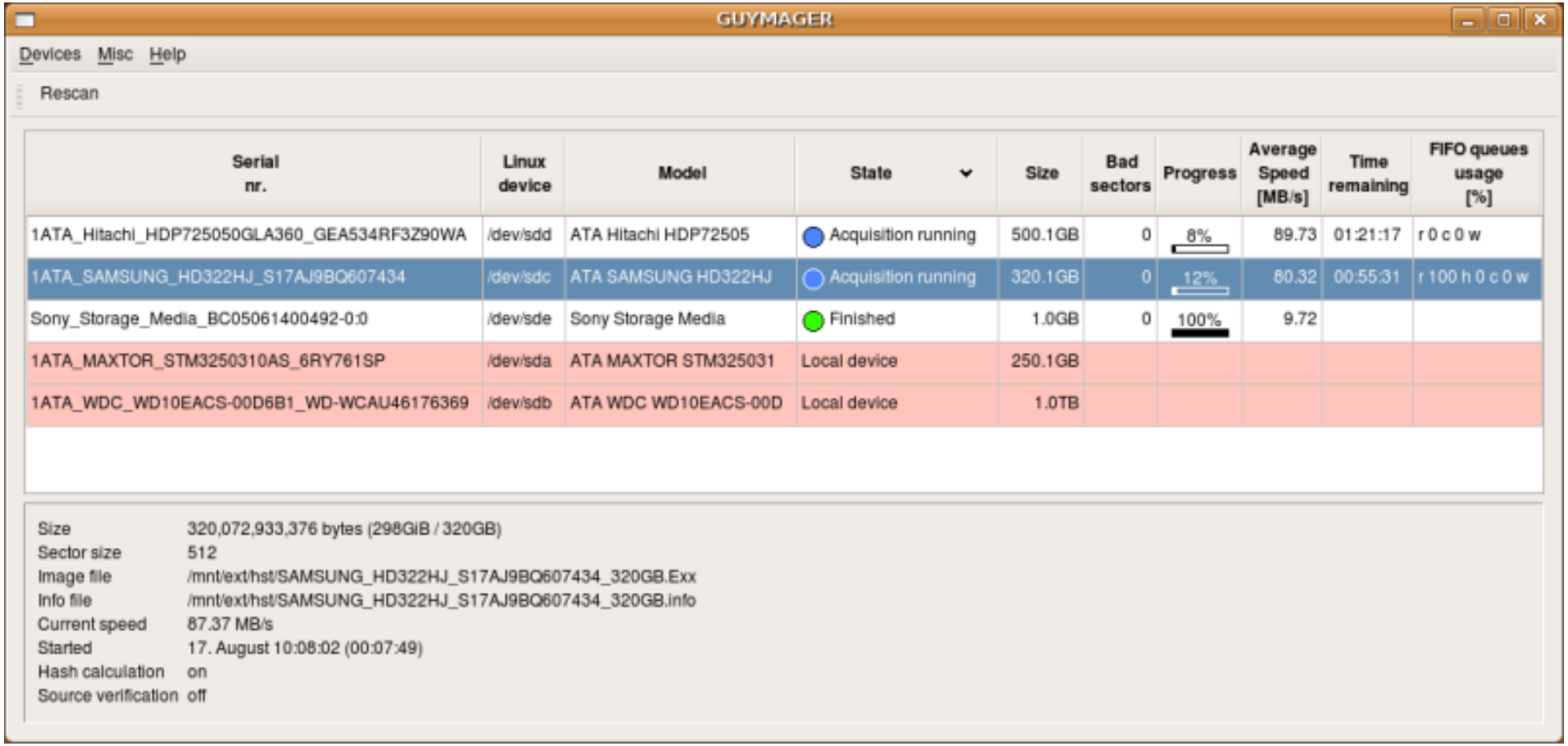
# Expert Witness Disk Image Format (EWF)

- 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

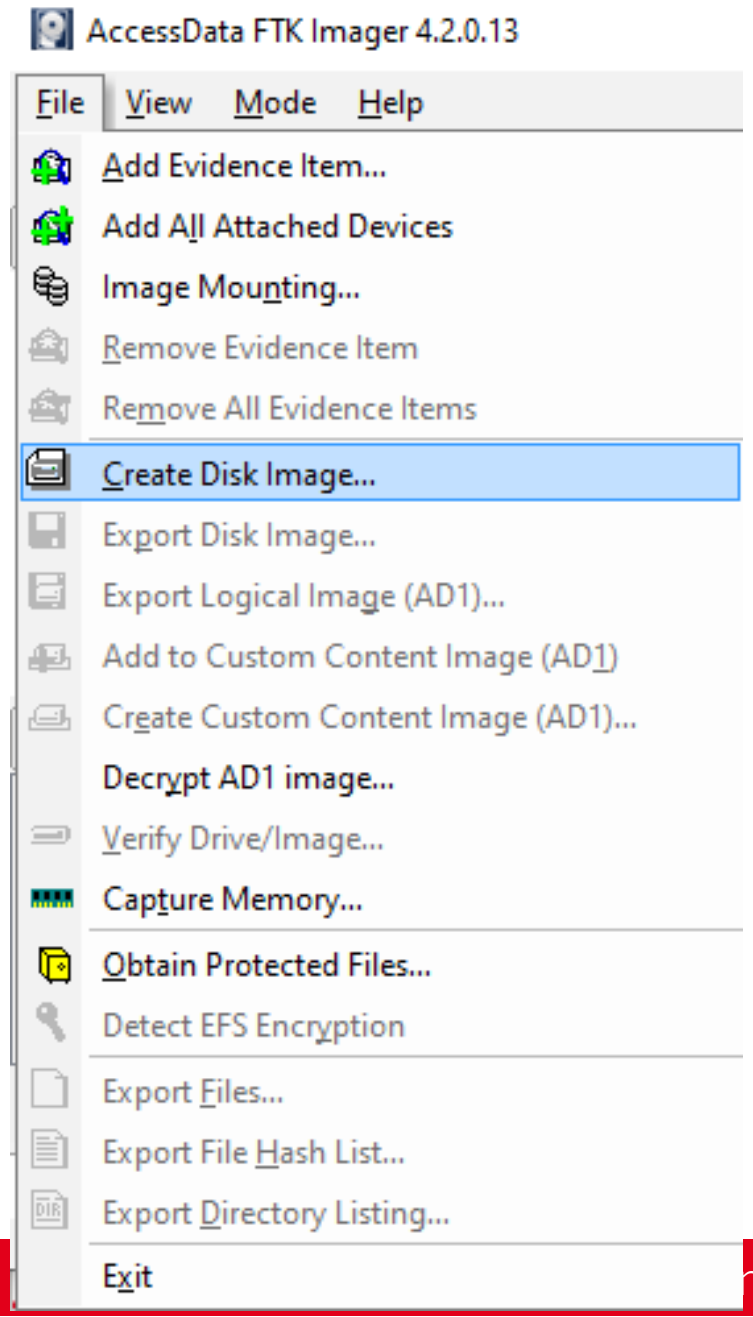
- Umwandeln von DD in EWF z. B. mit xmount
  - xmount --in Quellformat QUELLE --out Zielformat ZIEL

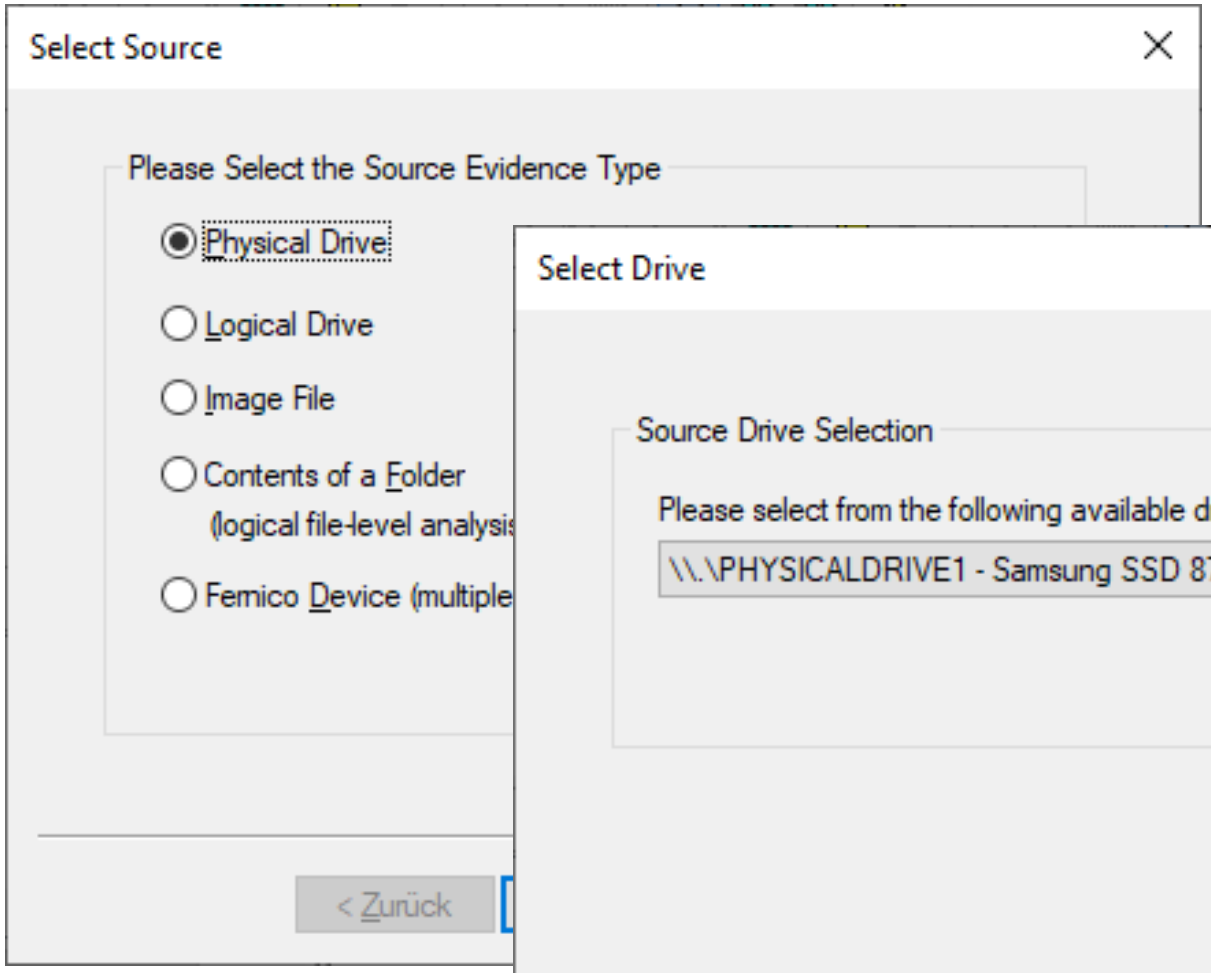
```
joshua@Zeus /media/joshua/Storage/temp $ sudo ewfacquire /dev/sde
ewfacquire 20140608

Device information:
Bus type:                                       USB
Vendor:                                         SMI
Model:                                          USB DISK
Serial:                                         AA000000000000485D

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]:
```

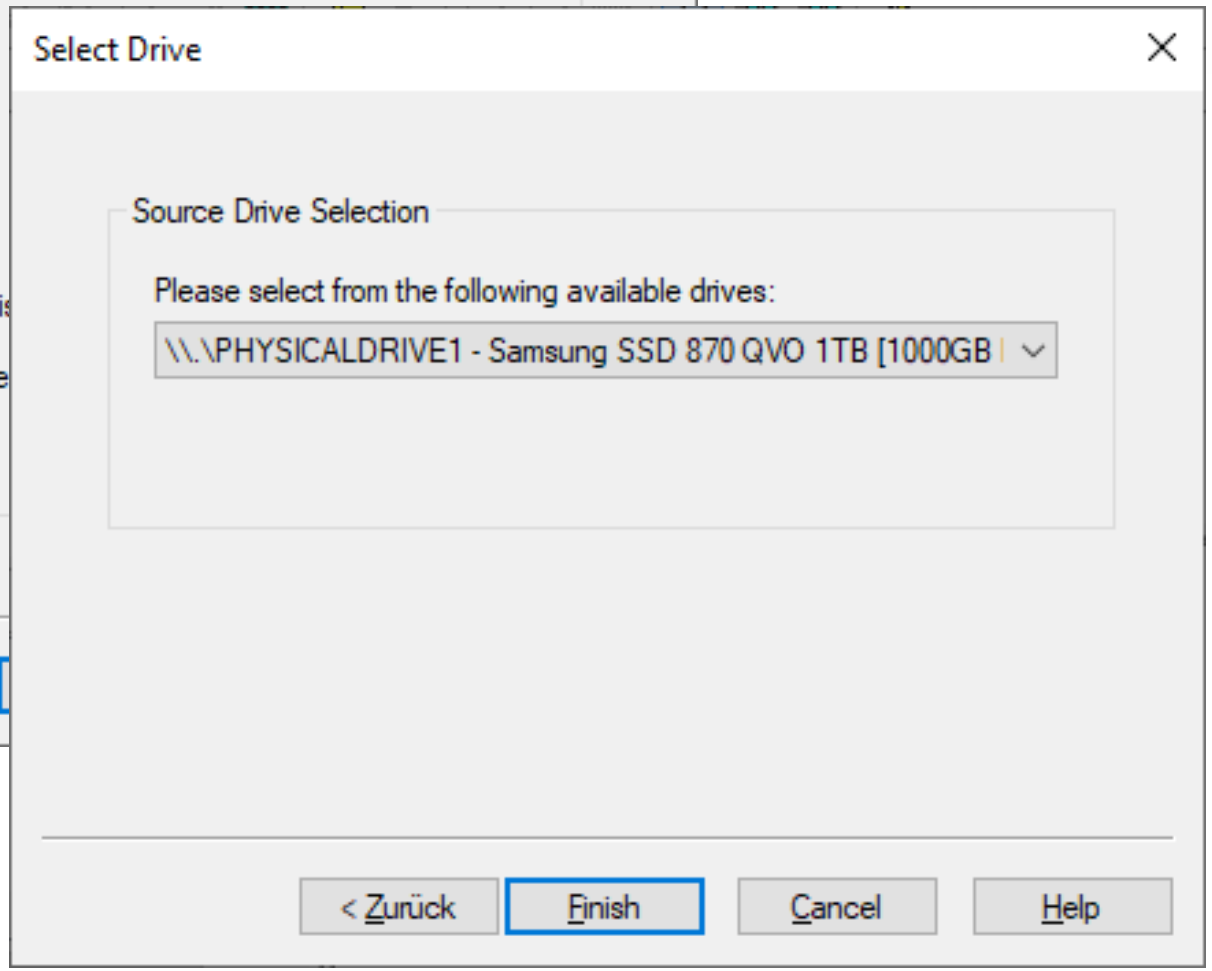
# GUYMAGER


GUYMAGER
Devices Misc Help
Rescan
Serial nr.
Linux device
Model
State
Size
Bad sectors
Progress
Average Speed [MB/s]
Time remaining
FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA /dev/sdd ATA Hitachi HDP72505 Acquisition running 500.1GB 0 8% 89.73 01:21:17 r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434 /dev/sdc ATA SAMSUNG HD322HJ Acquisition running 320.1GB 0 12% 80.32 00:55:31 r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0 /dev/sde Sony Storage Media Finished 1.0GB 0 100% 9.72
1ATA_MAXTOR_STM3250310AS_6RY761SP /dev/sda ATA MAXTOR STM325031 Local device 250.1GB
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369 /dev/sdb ATA WDC WD10EACS-00D Local device 1.0TB
Size 320,072,933,376 bytes (298GiB / 320GB)
Sector size 512
Image file /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed 87.37 MB/s
Started 17. August 10:08:02 (00:07:49)
Hash calculation on
Source verification off

# Abbild erstellen: FTK Imager

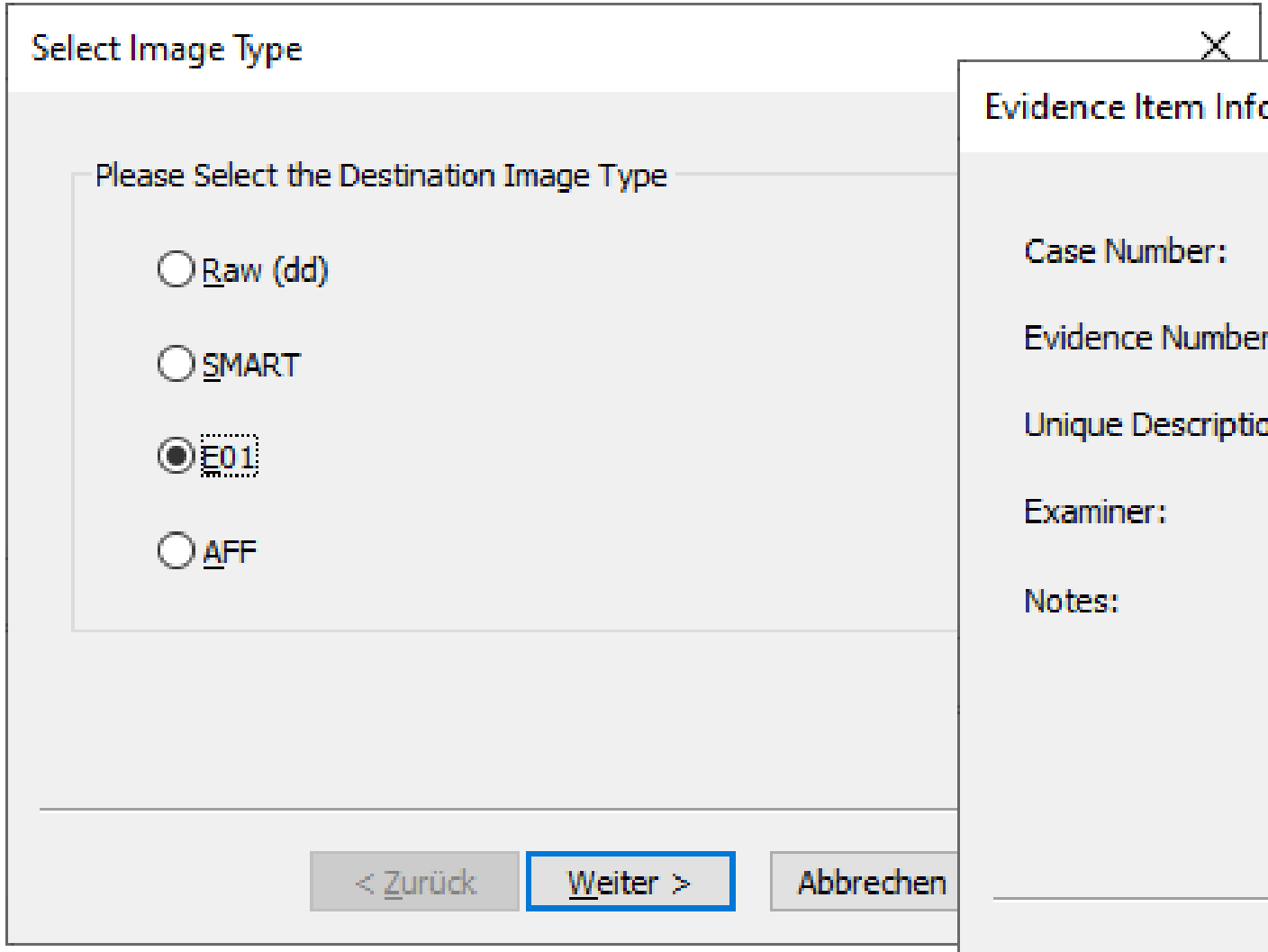


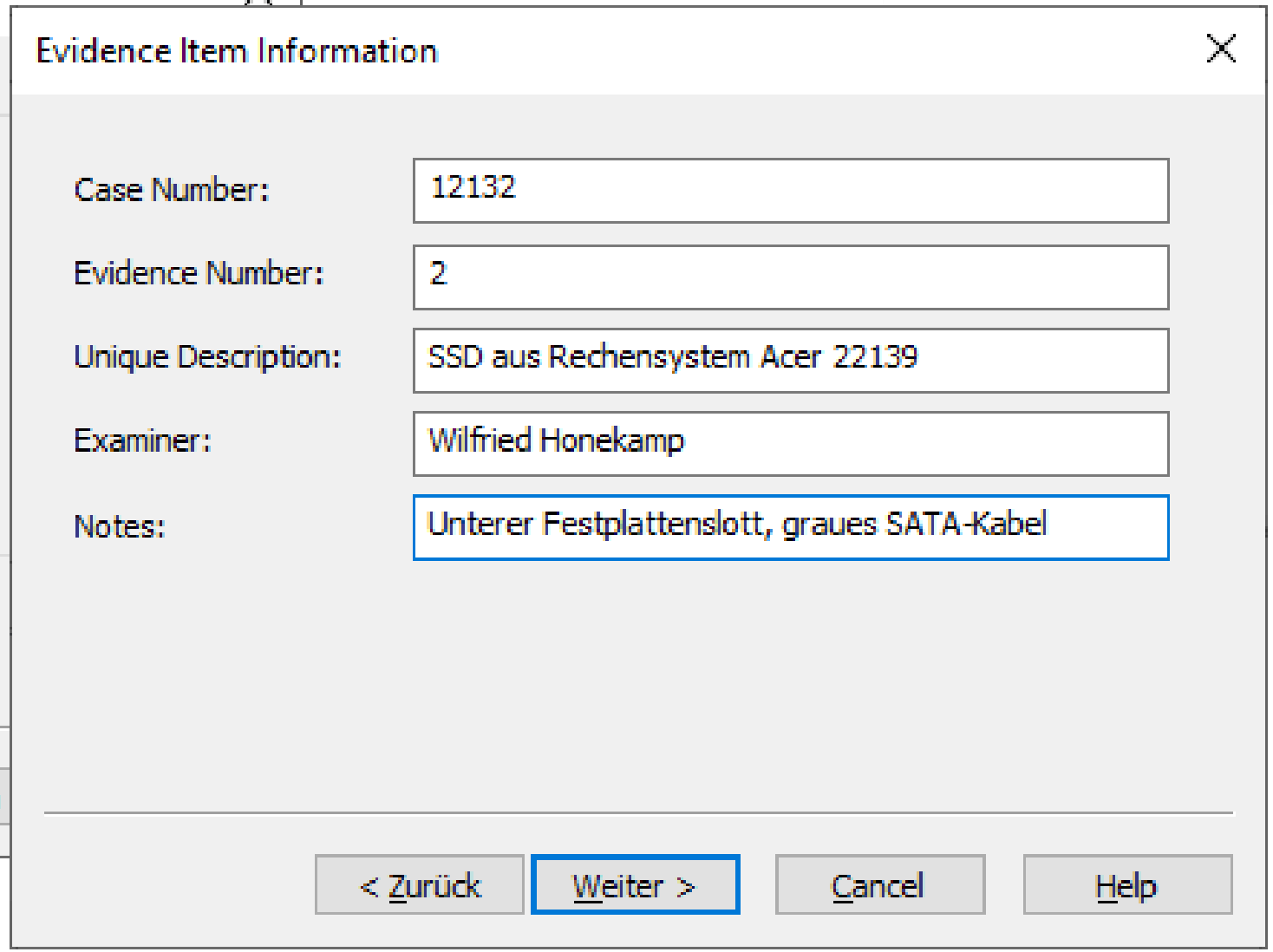



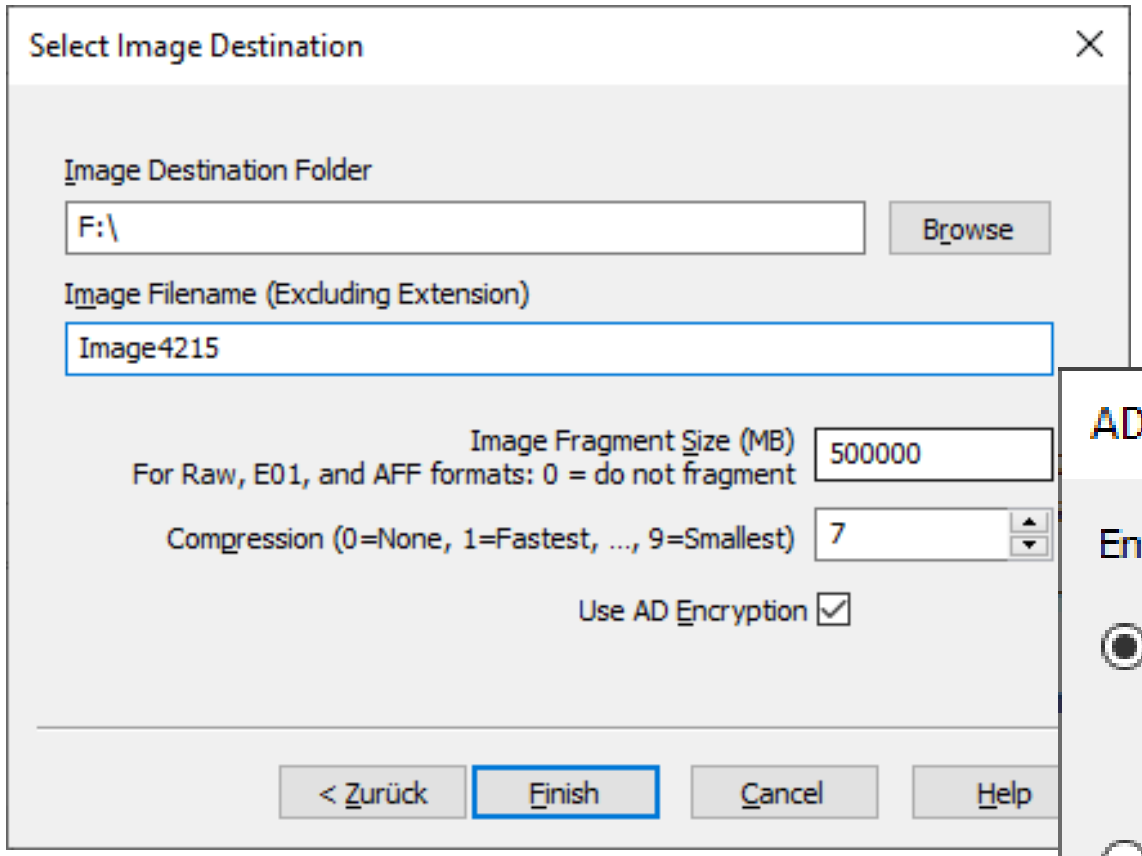

HOST
Hochschule Stralsund

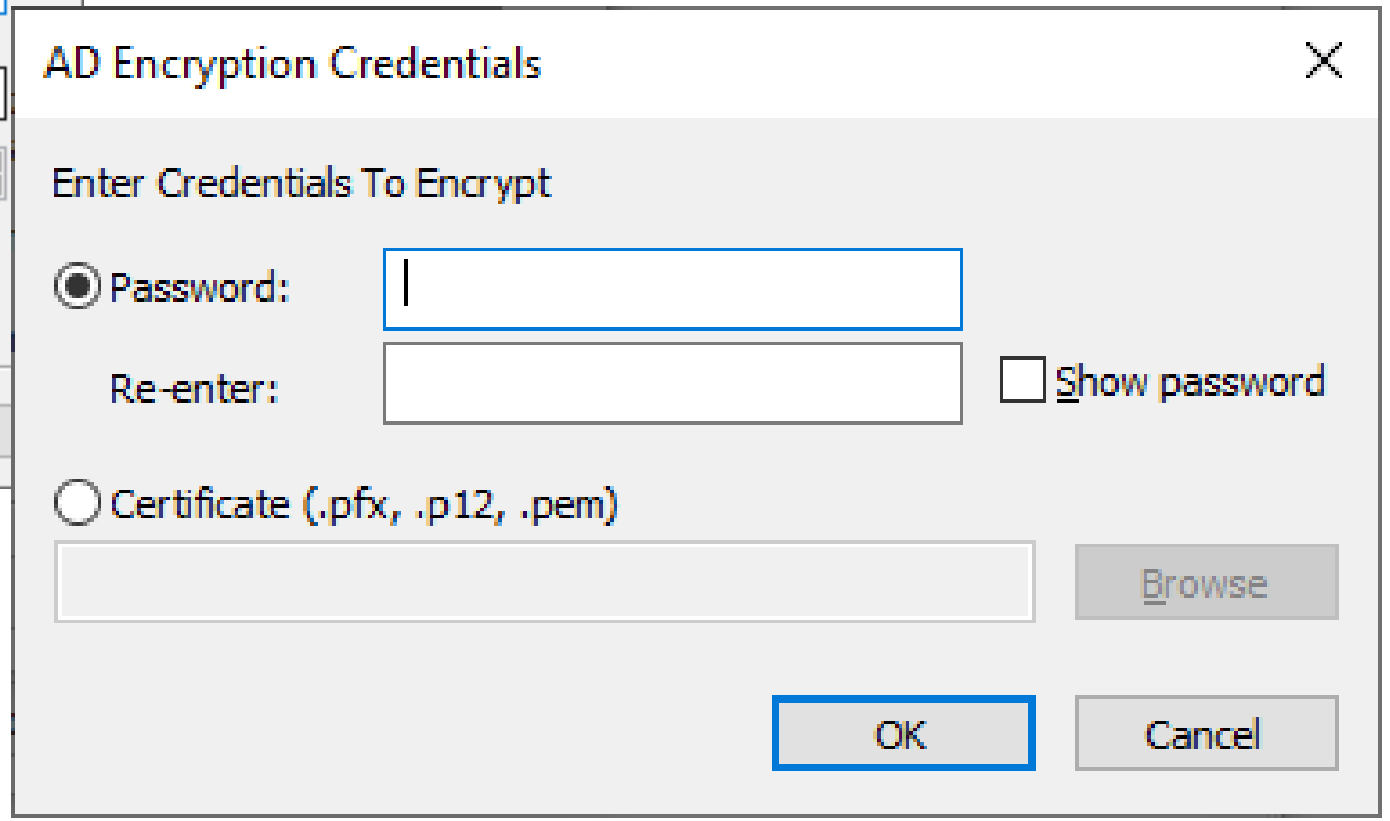
# Abbild erstellen: FTK Imager



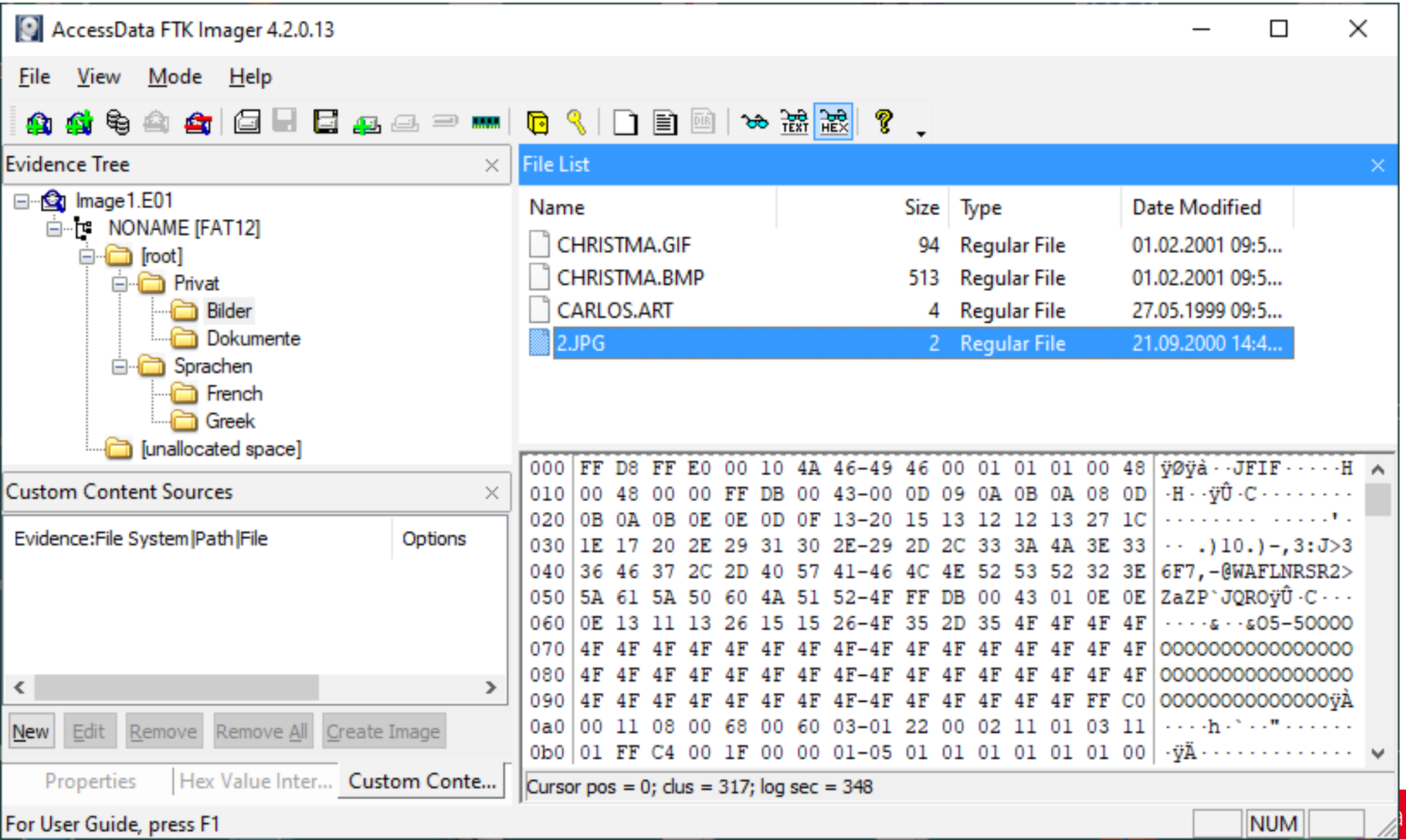



# Abbild erstellen: FTK Imager

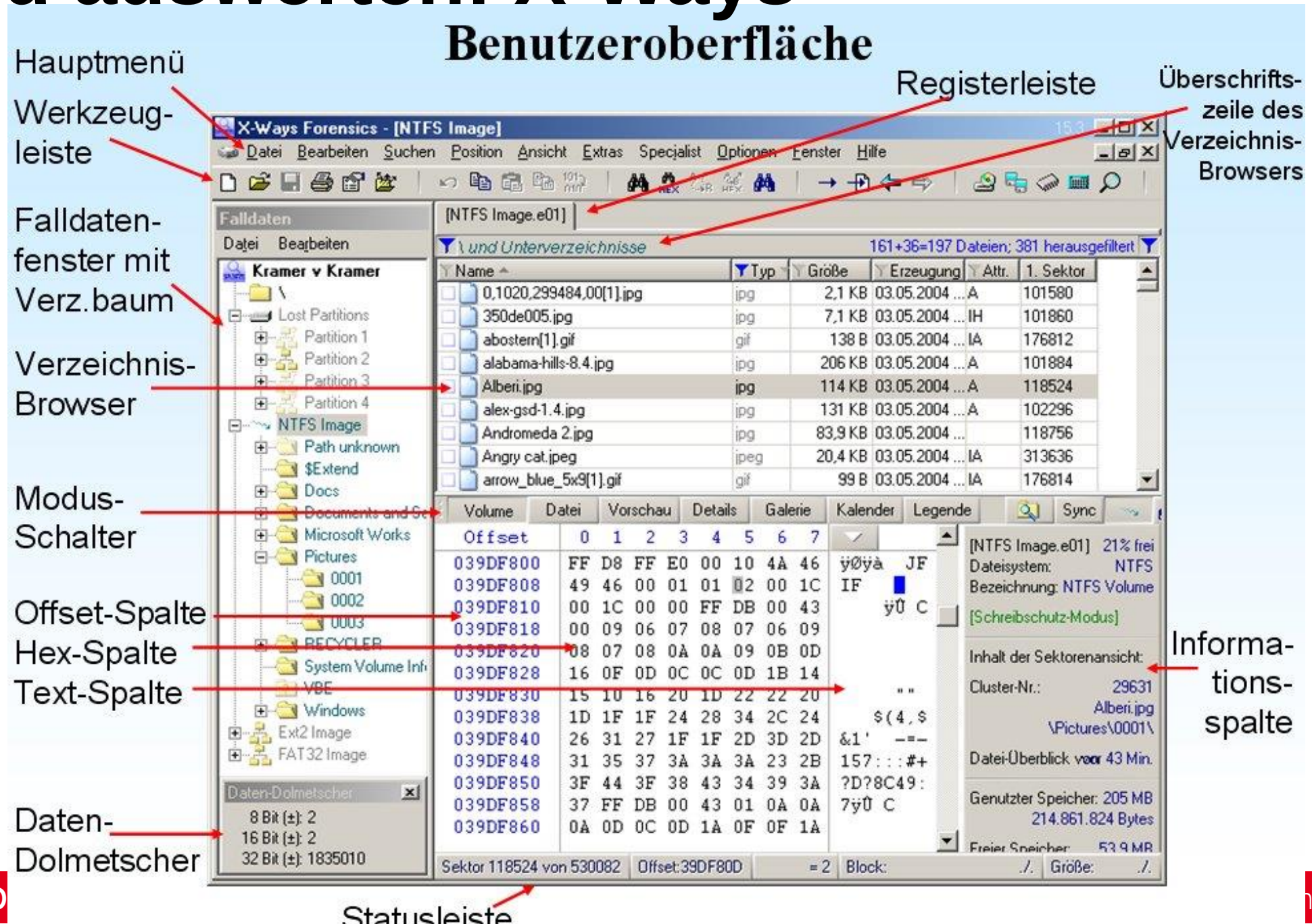


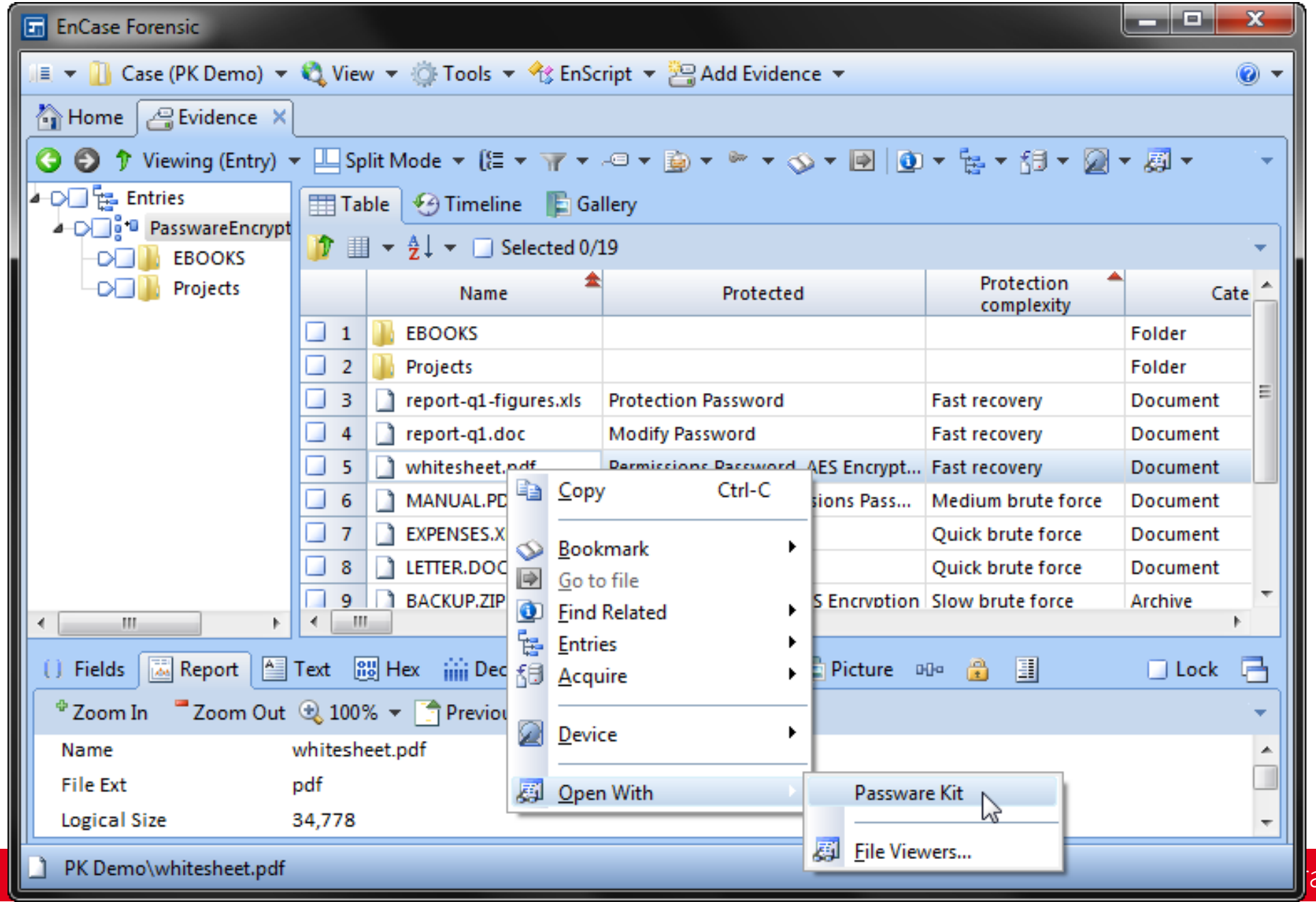
# Abbild auswerten: FTK Imager



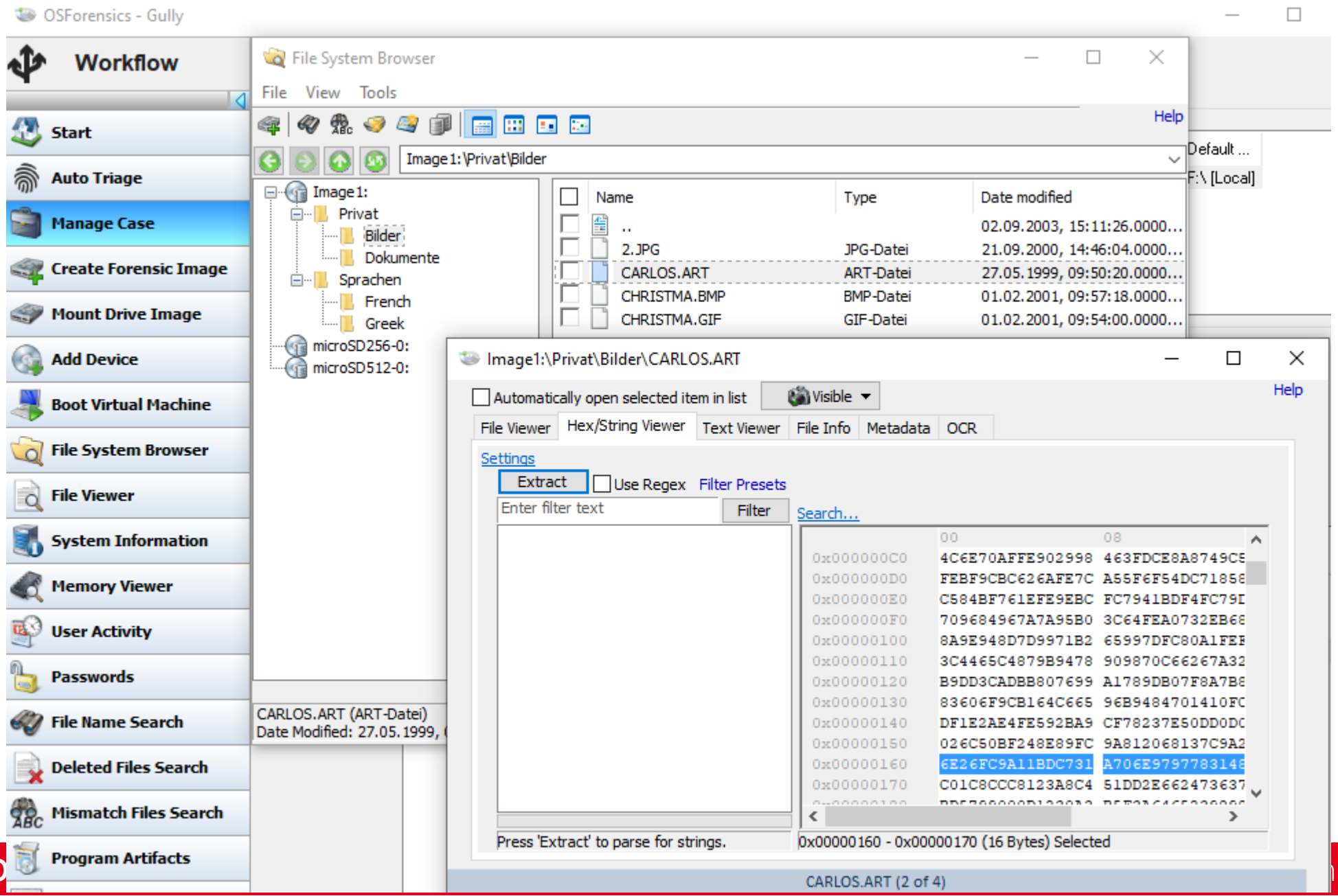
# Abbild auswerten: X-Ways



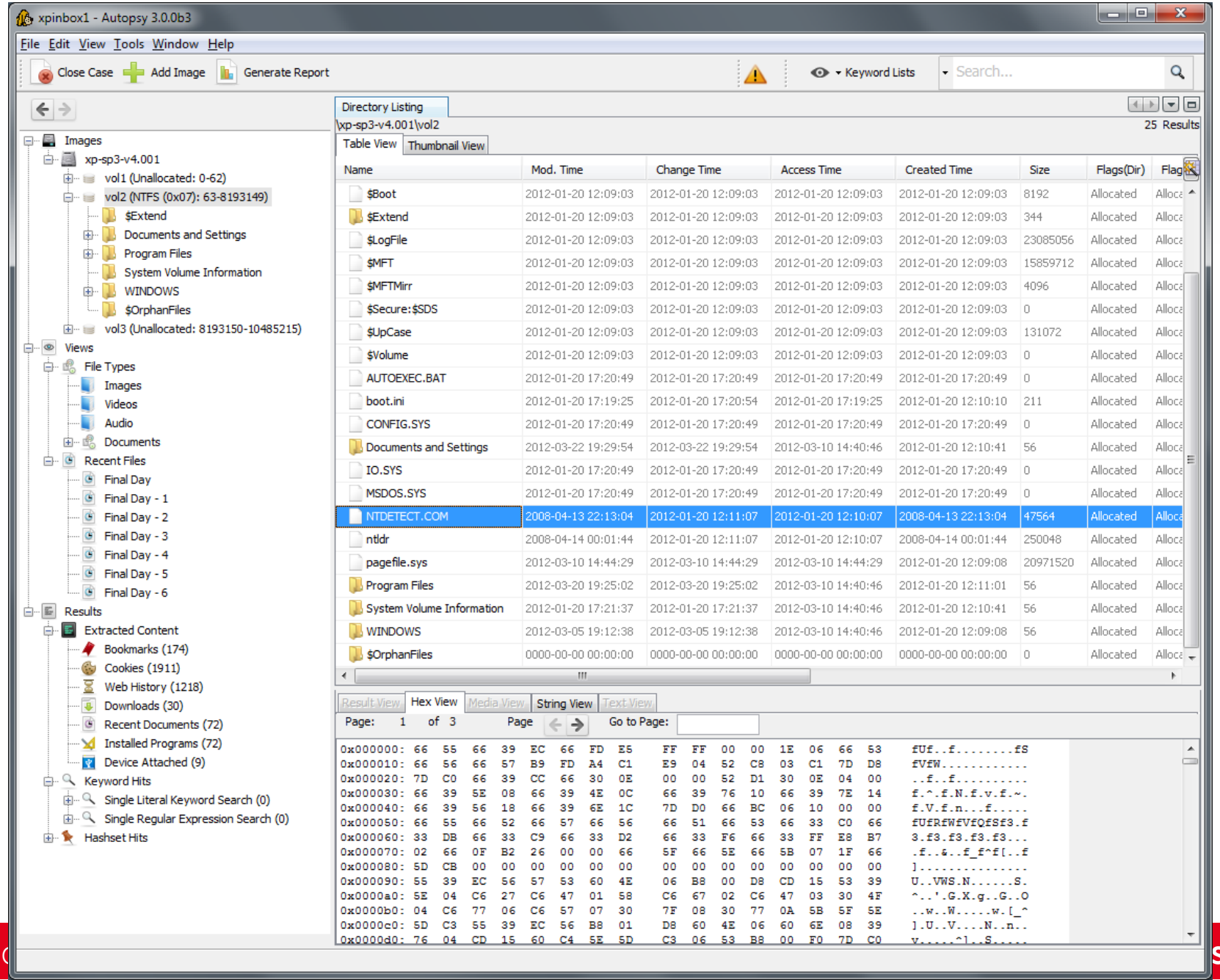
# Abbild auswerten: EnCase



# Abbild auswerten: OSForensics

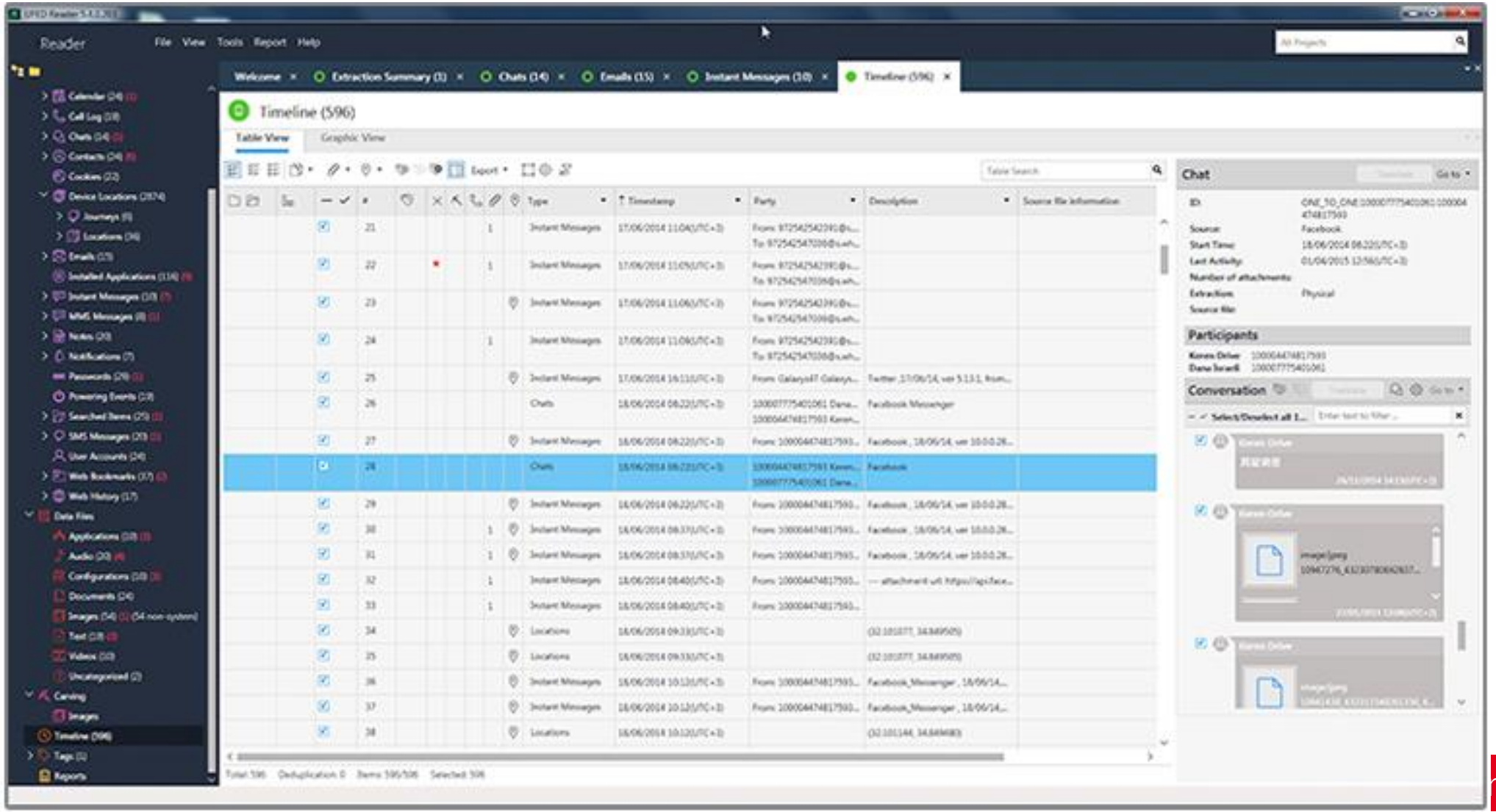


# Abbild auswerten: Autopsy

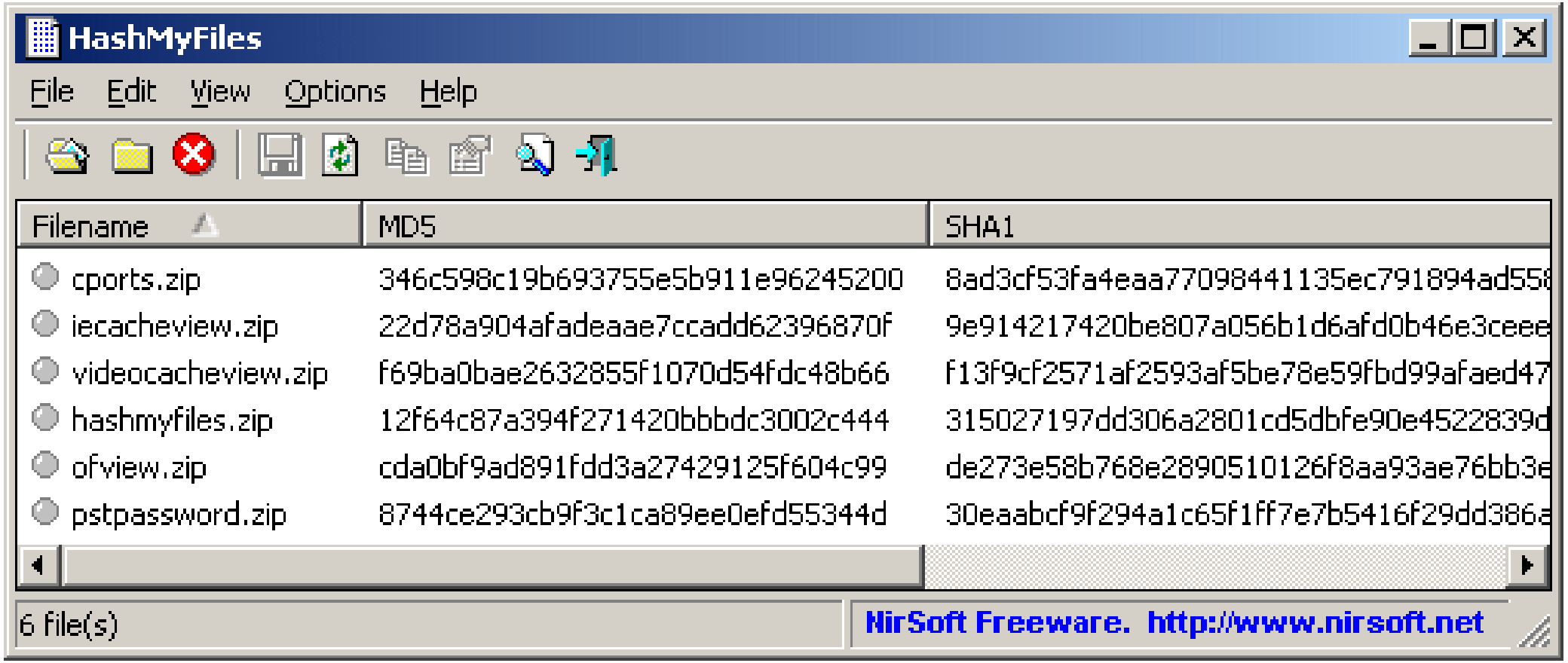



HOST
Hochschule Stralsund

# Abbild auswerten: Cellebrite Reader (UFED Reader)



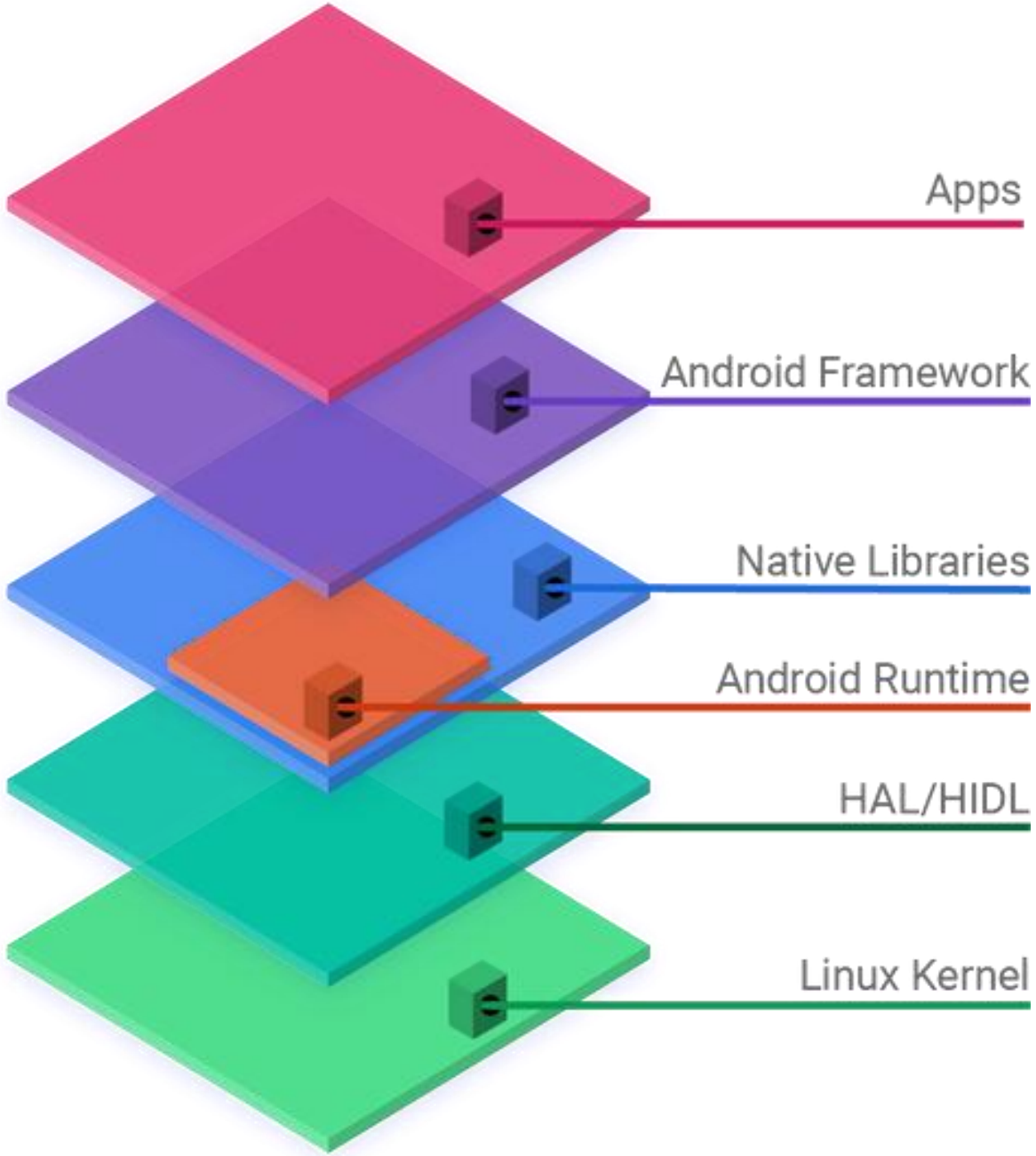
# Hashes erstellen



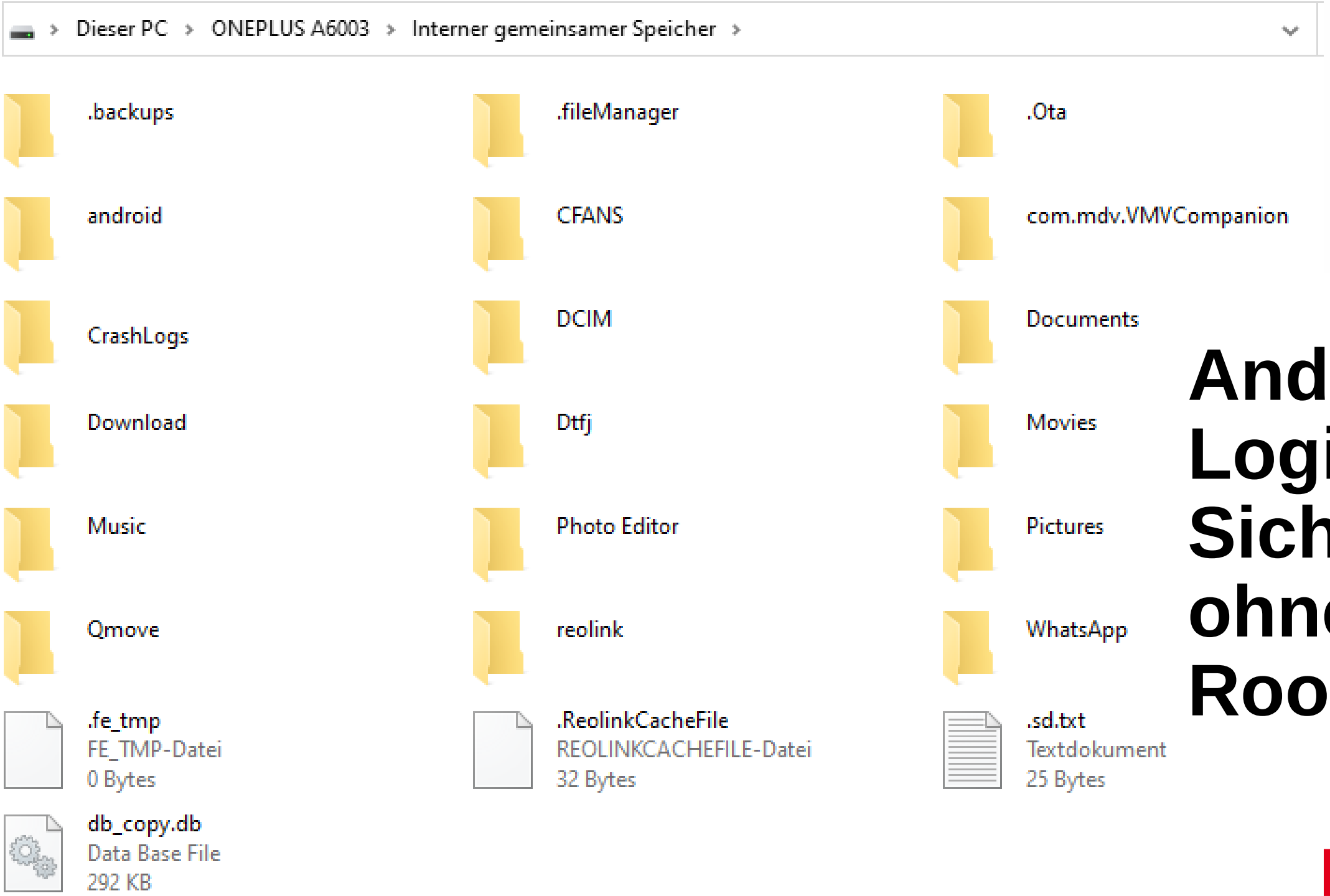
# Android-Sicherung

- Datei-Sicherung
- Android Debug Bridge
- Physische Sicherung

# Android




Wikipedia




HOST
Hochschule Stralsund

# Android: Logische Sicherung ohne Rootzugriff

# Android Debug Bridge

# aktivieren!

HOST
Hochschule Stralsund

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

# Android Debug Bridge

Hochschule Stralsund

- **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)
pstore on /sys/fs/pstore type pstore (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=iso885
/dev/block/sde9 on /vendor/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=iso88
/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,dirsync,seclabel,nodev,noatime)
/dev/block/dm-2 on /apex/com.android.media type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-3 on /apex/com.android.conscrypt@301800104 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-3 on /apex/com.android.conscrypt type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-4 on /apex/com.android.media.swcodec@301700000 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-4 on /apex/com.android.media.swcodec type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-5 on /apex/com.android.tzdata@293500000 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/dm-5 on /apex/com.android.tzdata type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop7 on /apex/com.android.resolv@290000000 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop7 on /apex/com.android.resolv type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop8 on /apex/com.android.runtime@1 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop8 on /apex/com.android.runtime type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop9 on /apex/com.android.apex.cts.shim@1 type ext4 (ro,dirsync,seclabel,nodev,noatime)
/dev/block/loop9 on /apex/com.android.apex.cts.shim type ext4 (ro,dirsync,seclabel,nodev,noatime)
adb on /dev/usb-ffs/adb type functionfs (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

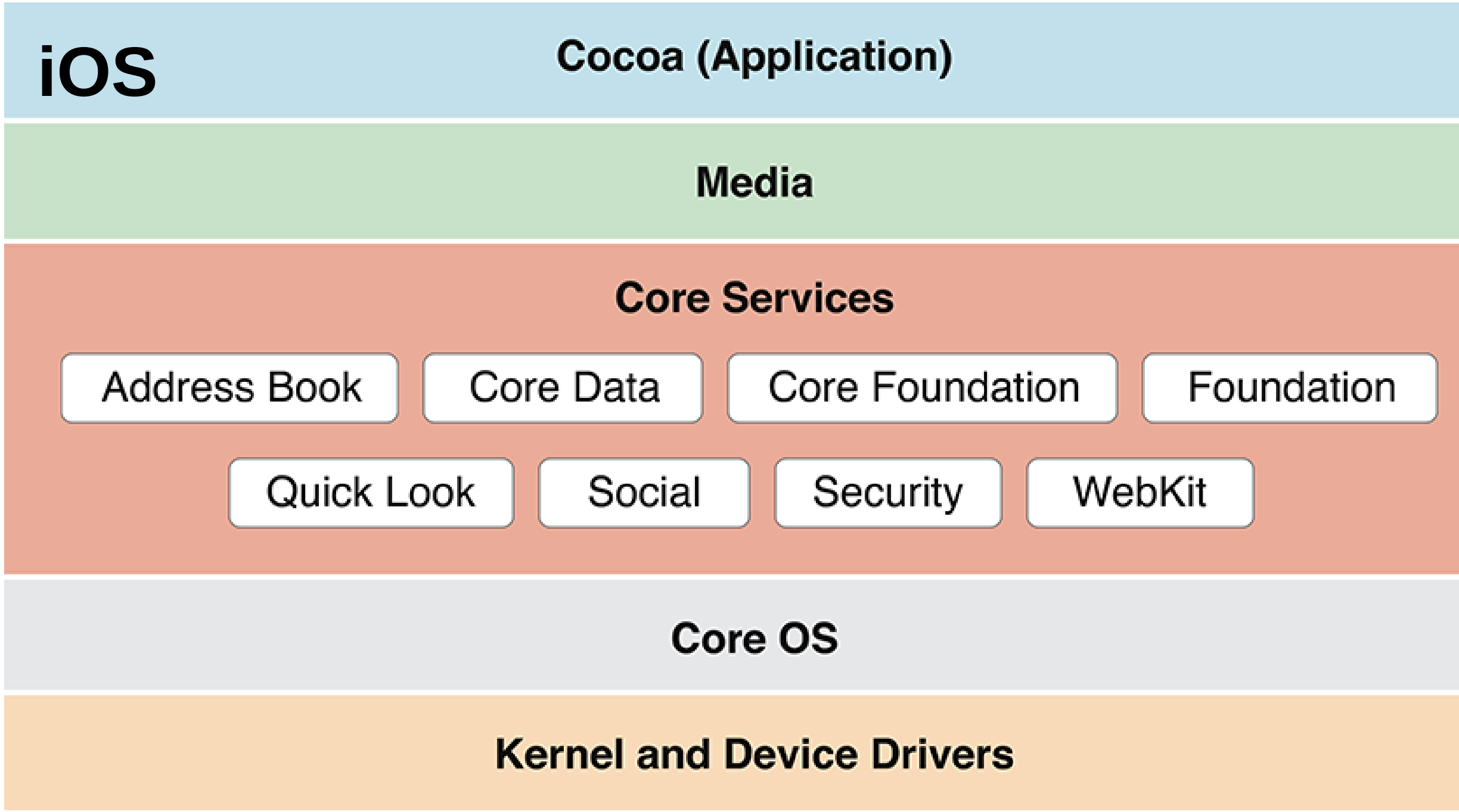
```
/dev/block/sda17 on /data type ext4
```

# 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


iPhone
Suchen
Finder
Favoriten
AirDrop
Zuletzt benutzt
Programme
Dokumente
Schreibtisch
Downloads
Bilder
iCloud
Orte
iPhone
Macintosh HD
Netzwerk
Tags
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
apple.com

# iTunes File Sharing

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

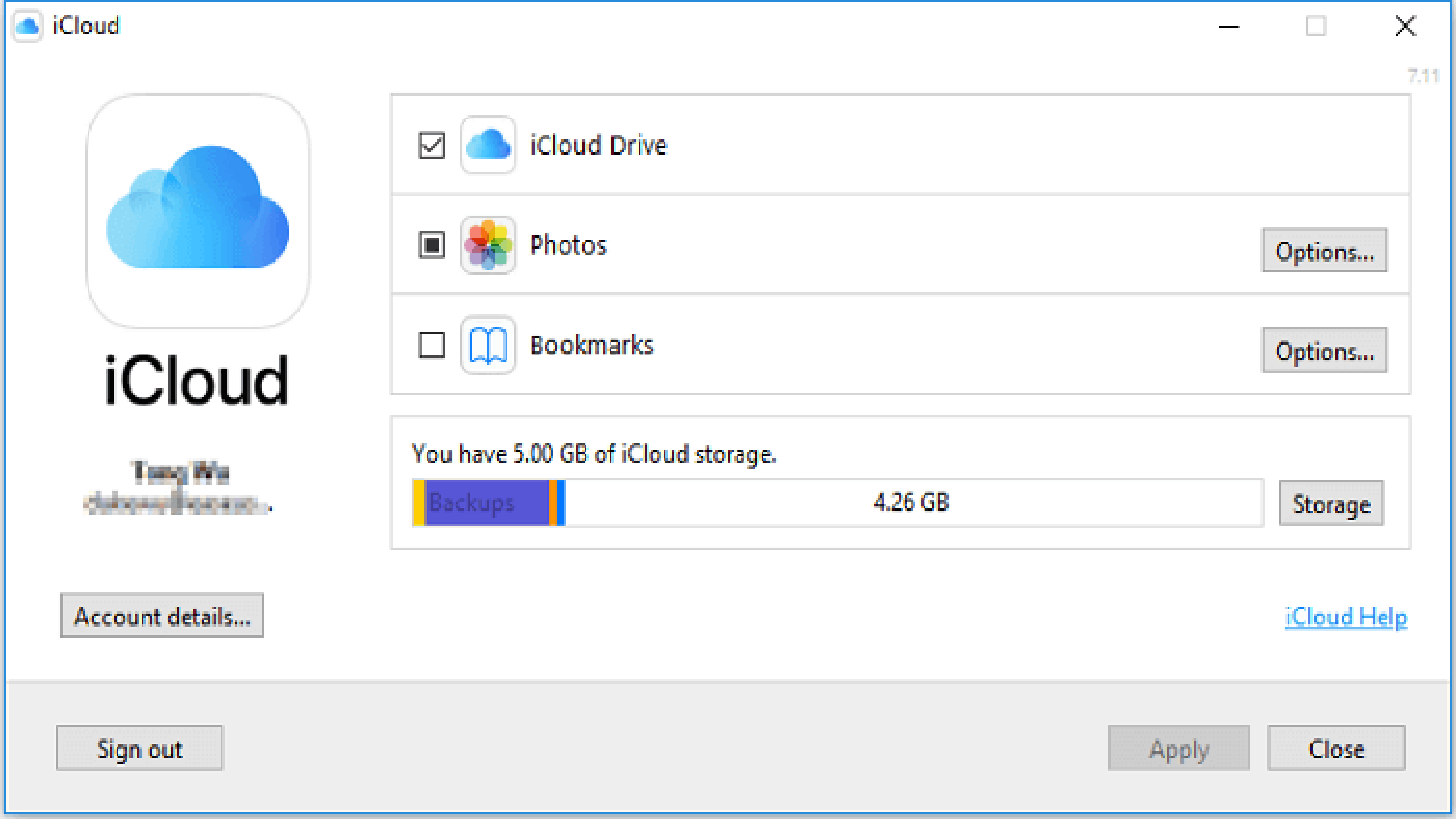
apple.com


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
Numbers
Pages
Keynote Documents
Getting Started.key
252 KB
Today 9:41 AM
September 2017
296 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**

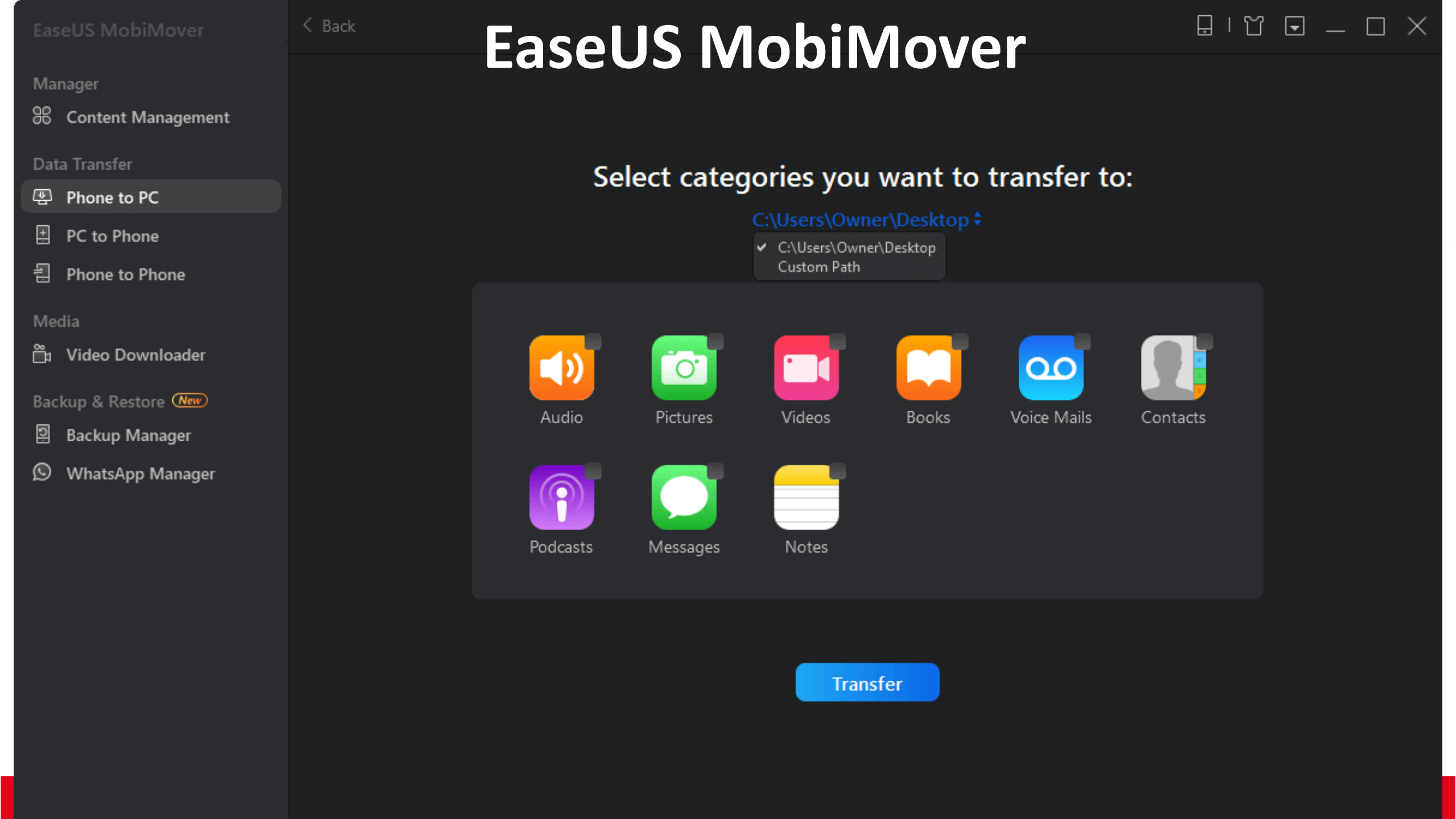
apple.com


iCloud
7.11
iCloud
iCloud Drive
Photos
Options...
Bookmarks
Options...
You have 5.00 GB of iCloud storage.
Backups
4.26 GB
Storage
Account details...
iCloud Help
Sign out
Apply
Close

# 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



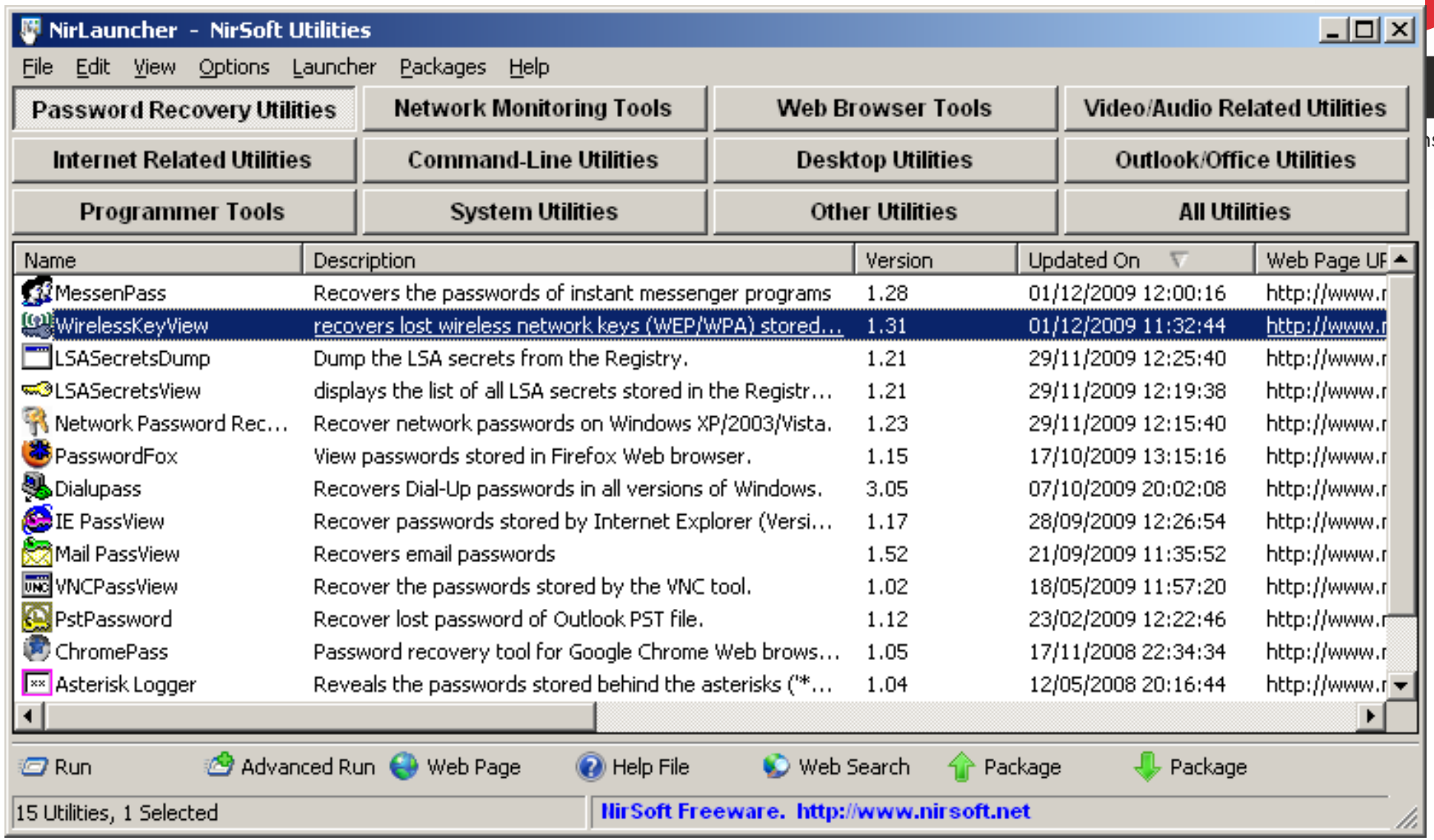
Hochschule Stralsund

# Windows-Forensik

# Gliederung

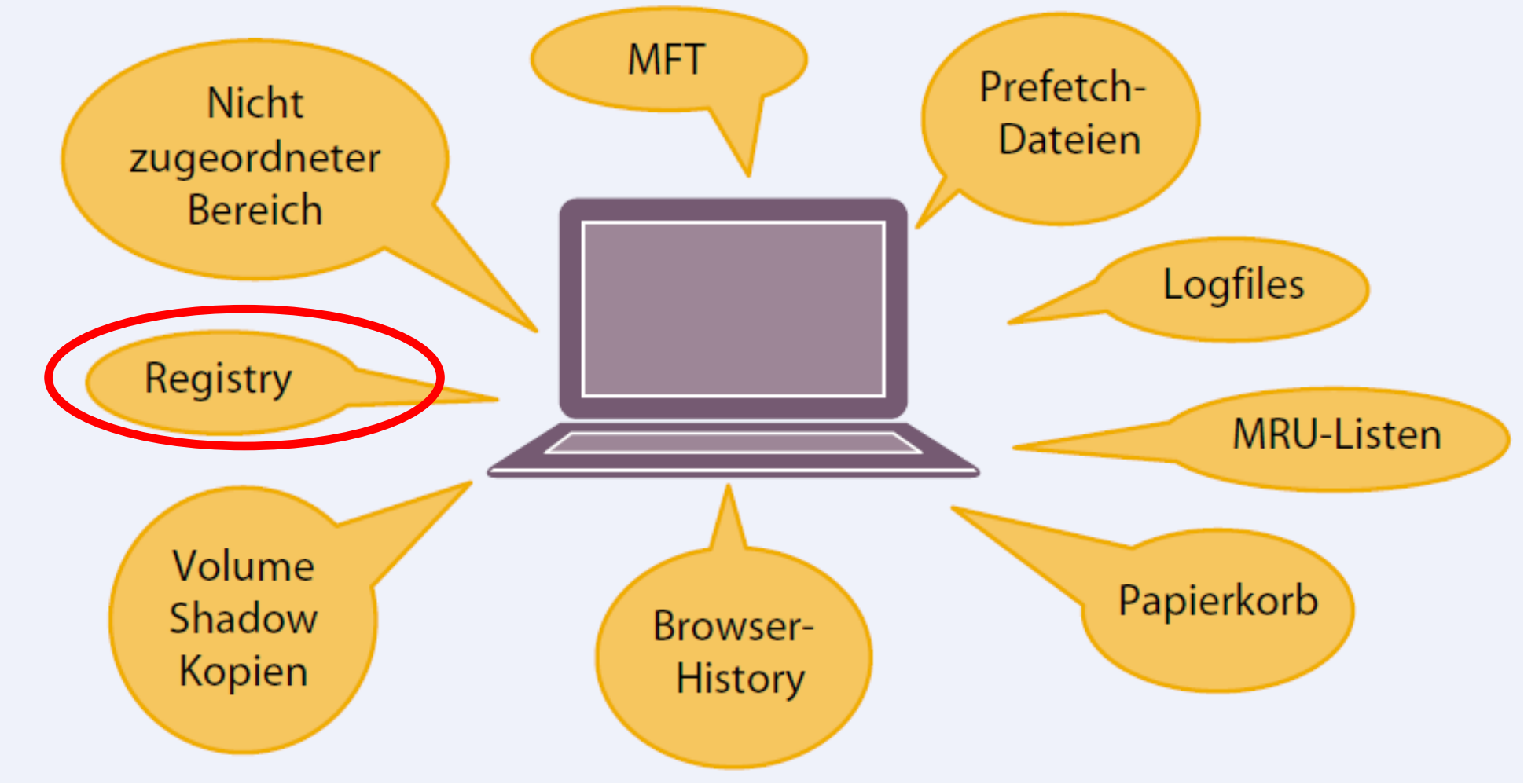
- **Windows Analyse**
  - **Registry**
  - **Prefetching**
  - **Eventlogs**

# Toolsammlung NirSoft



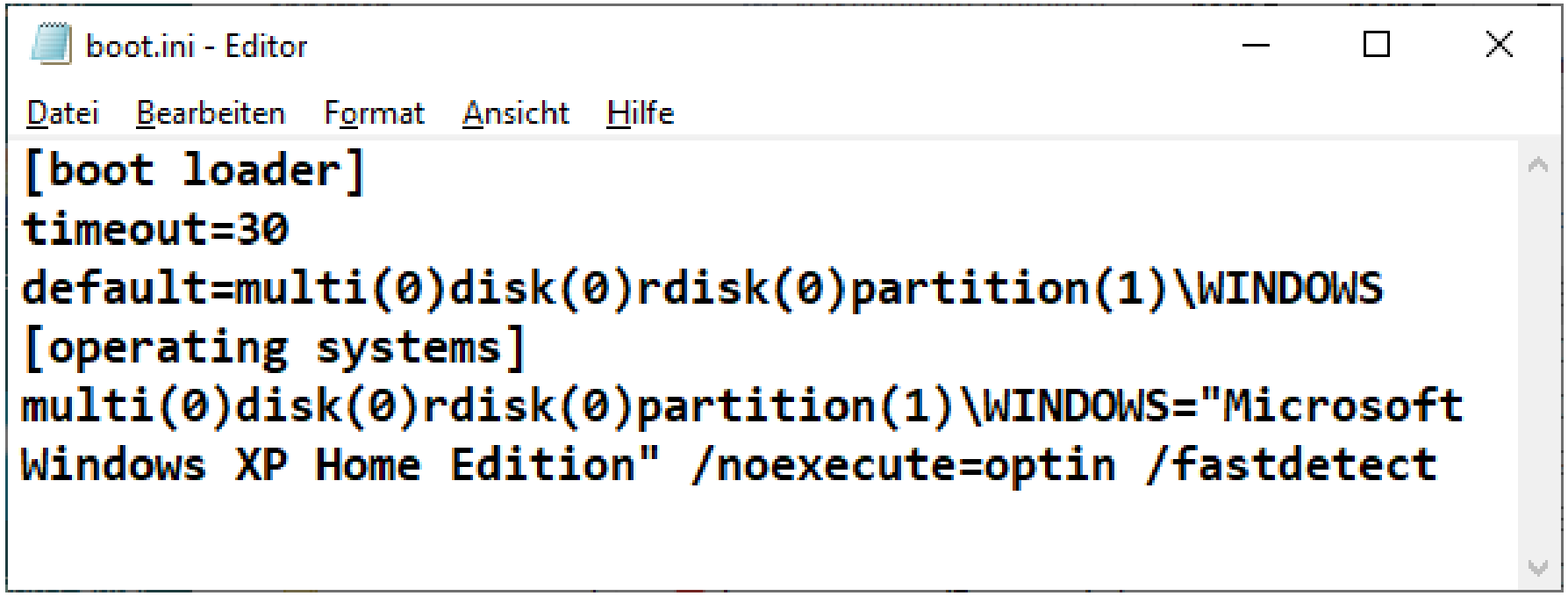

Siehe auch: https://www.gaijin.at/de/

# Der Computer als Zeuge




Lautenschläger 2014

# Windows ini-Dateien



# 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**

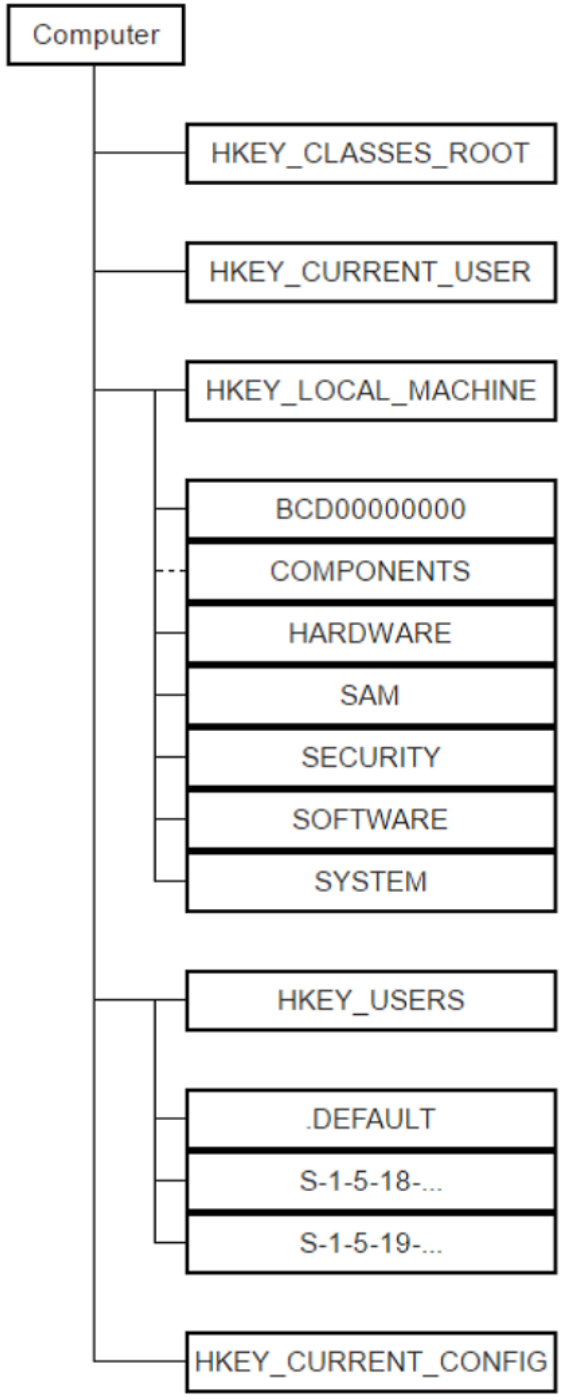
# Registry Hauptschlüssel

- **HKEY_CLASSES_ROOT:** enthält Informationen über unterstützte Dateitypen des Rechners und die dazuge-hörigen 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


Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
COMPONENTS
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
HKEY_USERS
.DEFAULT
S-1-5-18-...
S-1-5-19-...
HKEY_CURRENT_CONFIG

# 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**

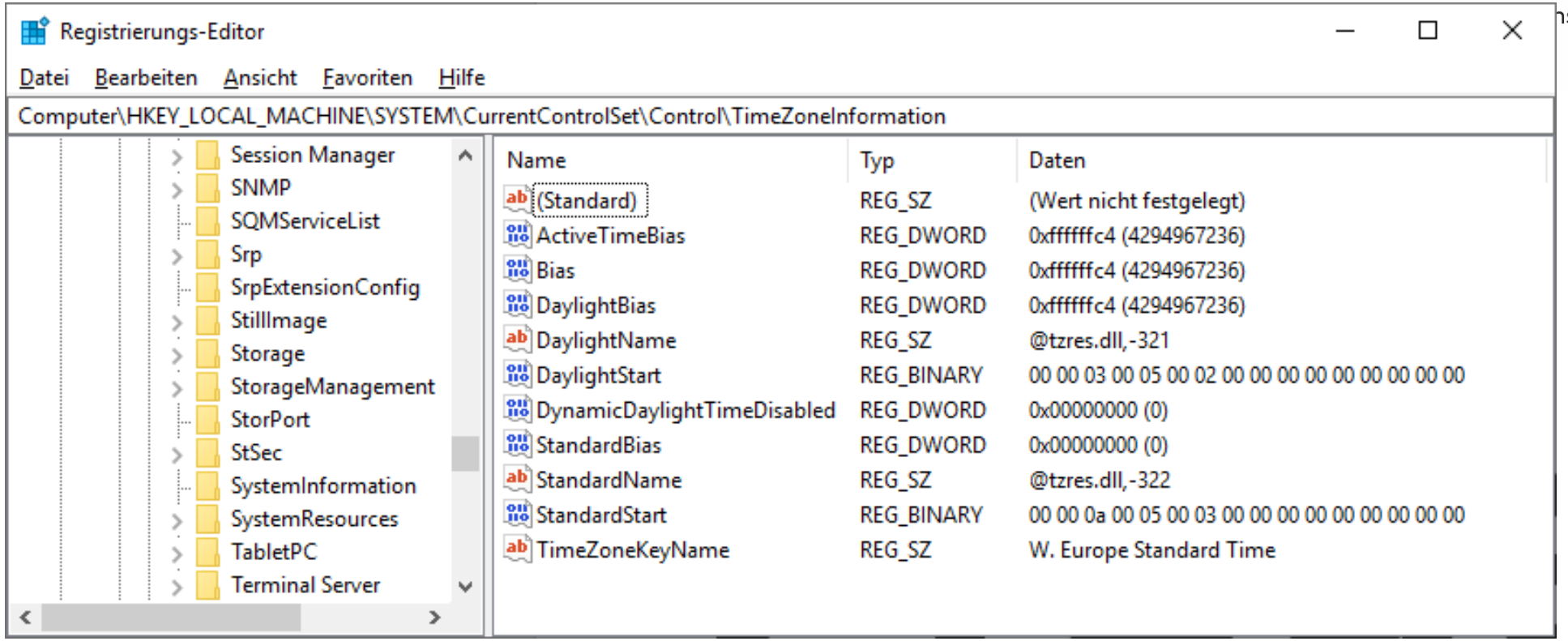
# Hives

- **%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

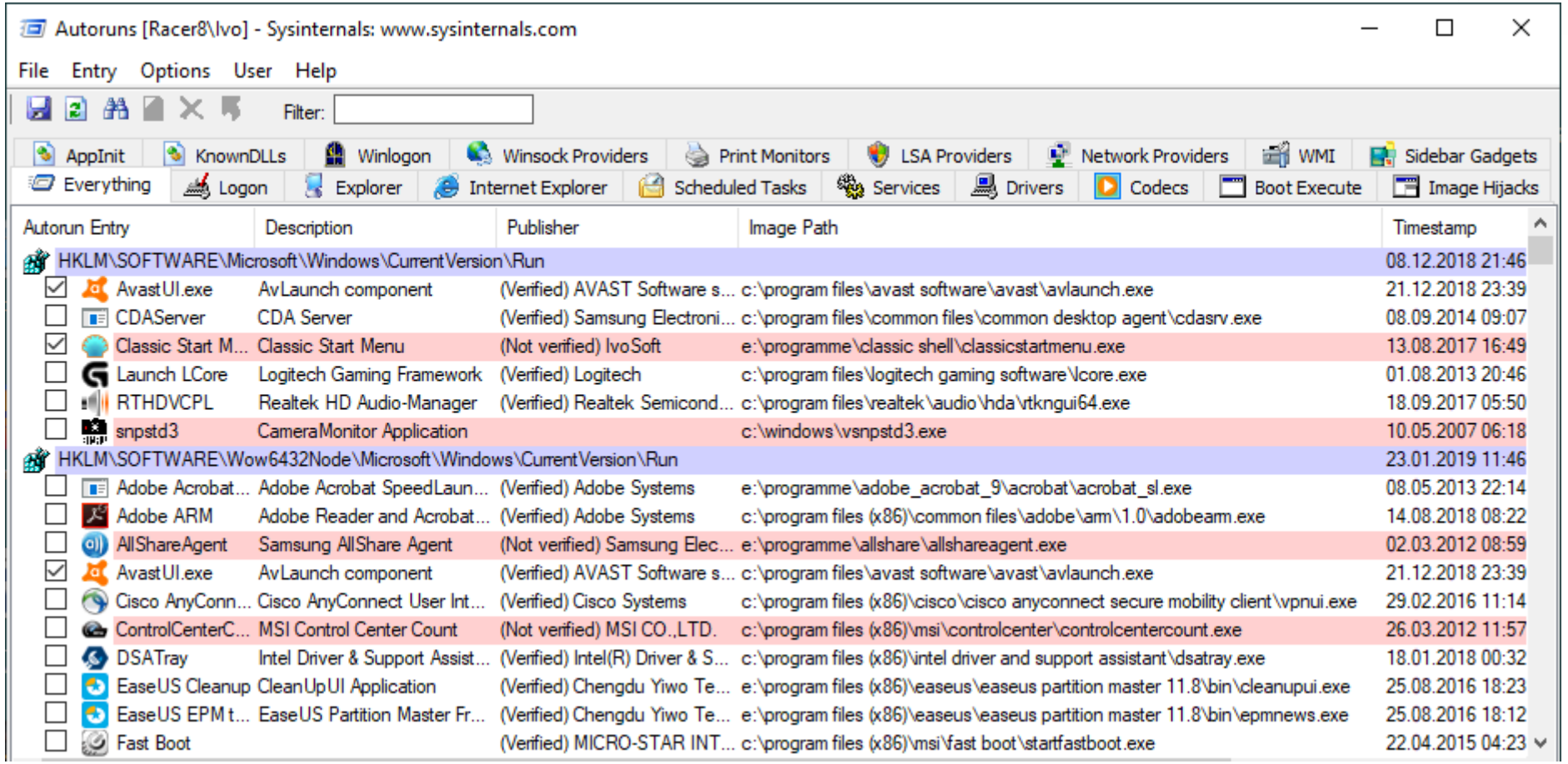
- **%systemroot%\System32\config\.DEFAULT**
  HKU\.DEFAULT und HKU\HKUnS-1-5-18 für User Local System
- **%systemroot%\ServiceProfiles\LocalService\Ntuser.dat**
  HKU\HKU\S-1-5-19 für User Local Service
- **%systemroot%\ServiceProfiles\NetworkService\Ntuser.dat**
  HKU\HKU\S-1-5-20 für User Network Service
- **\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



# 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

HOST
Hochschule Stralsund

**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**

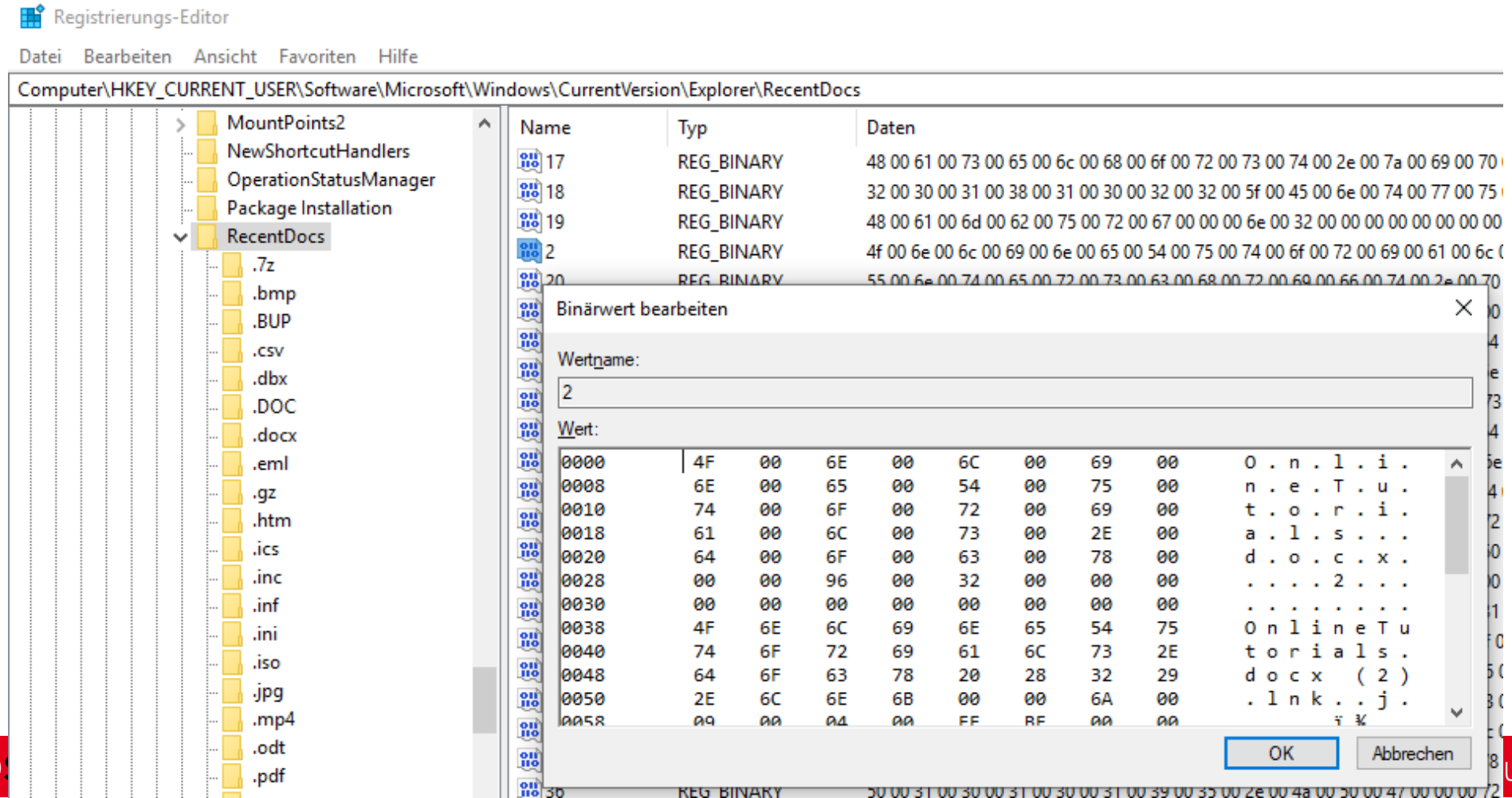
**Kommandozeile letzte Befehle:**

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

# Most Recently Used

## Zuletzt verwendete Dateien (Startmenu):

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



# 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:**

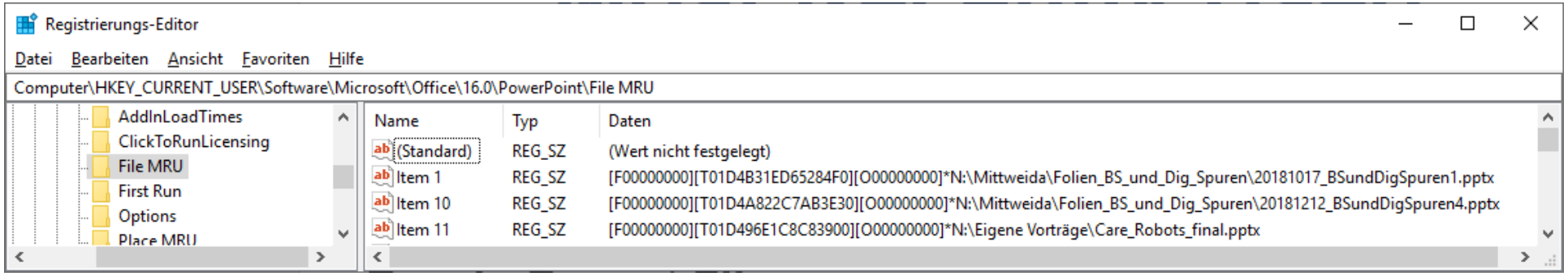
**HKCU\Software\Microsoft\Office\10.0\Word\Data**

- **Excel - Recent Files:**

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

- **Power Point - Recent Files:**

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

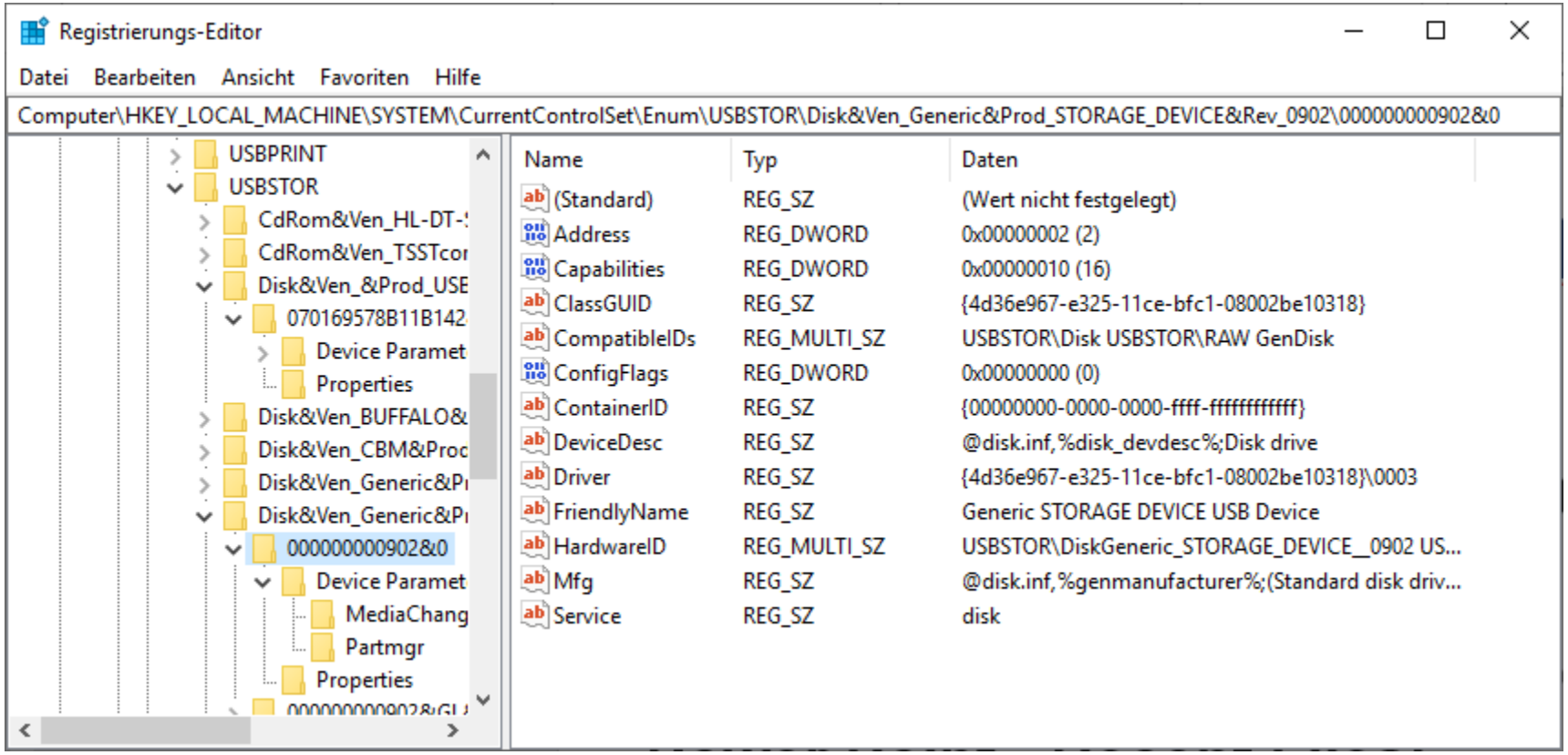



Mehr unter: https://www.andreafortuna.org/cybersecurity/windows-registry-in-forensic-analysis/ und

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

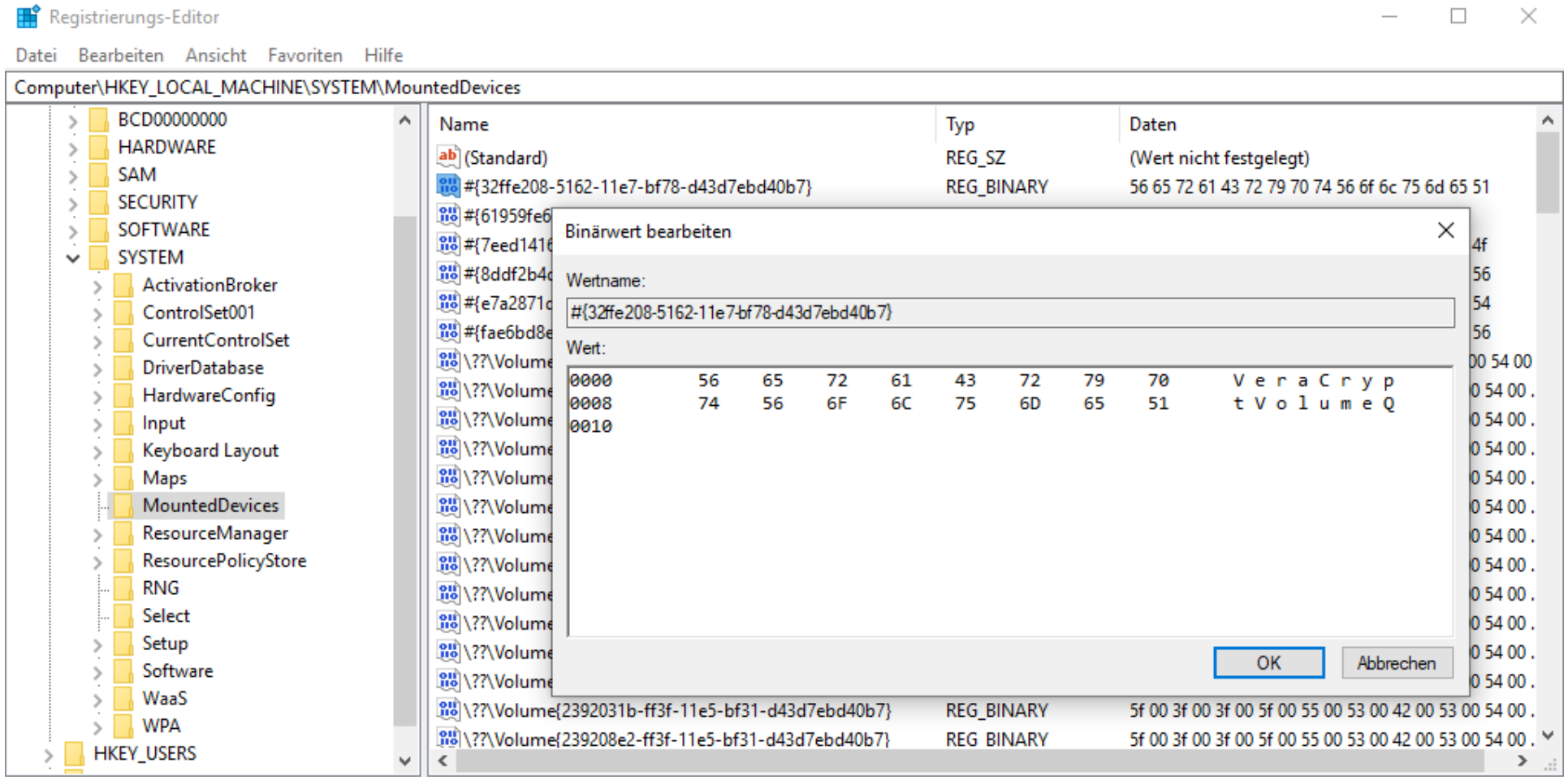
# USB Devices

## HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



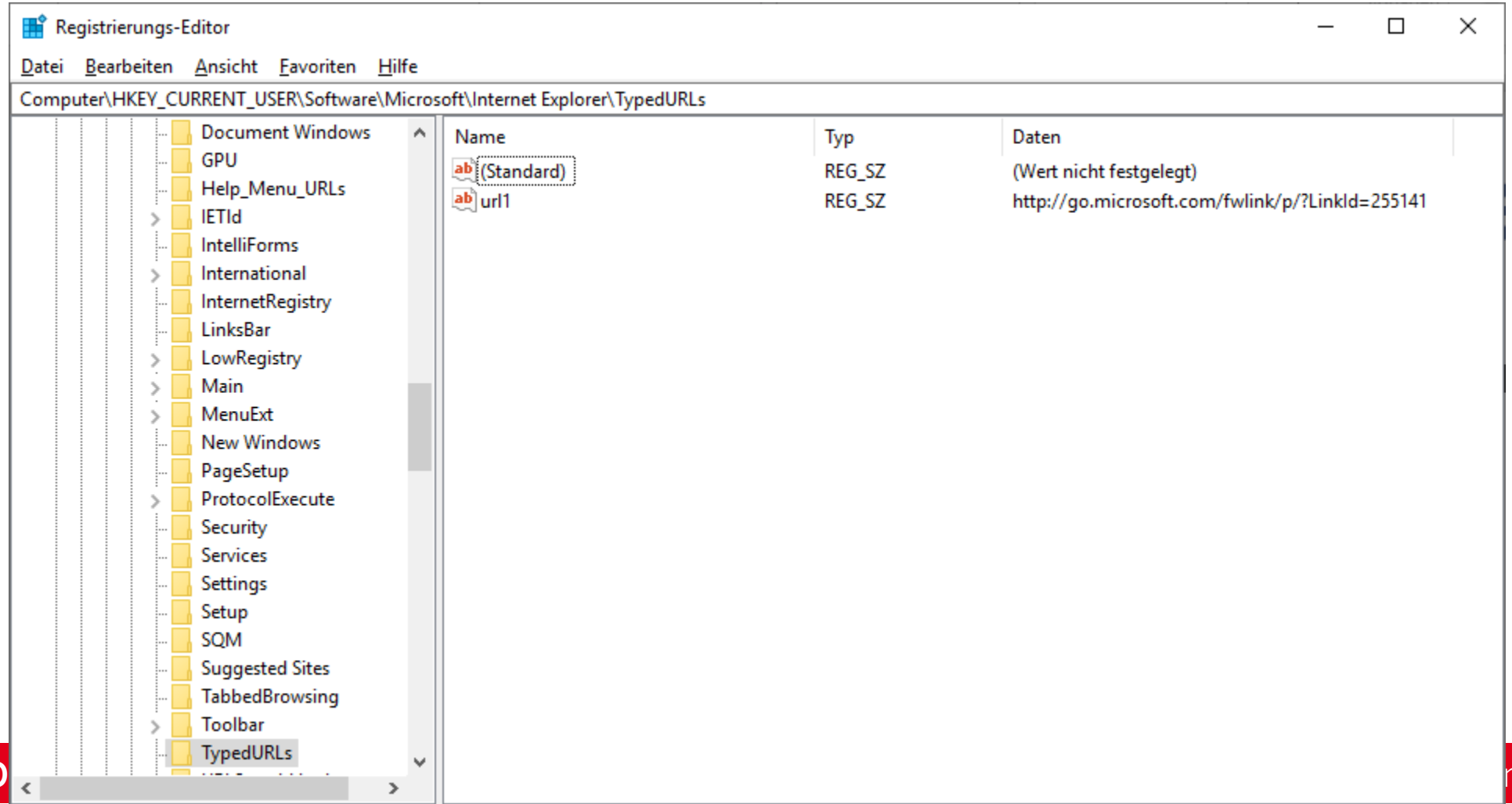
# Laufwerke

## HKLM\SYSTEM\MountedDevices

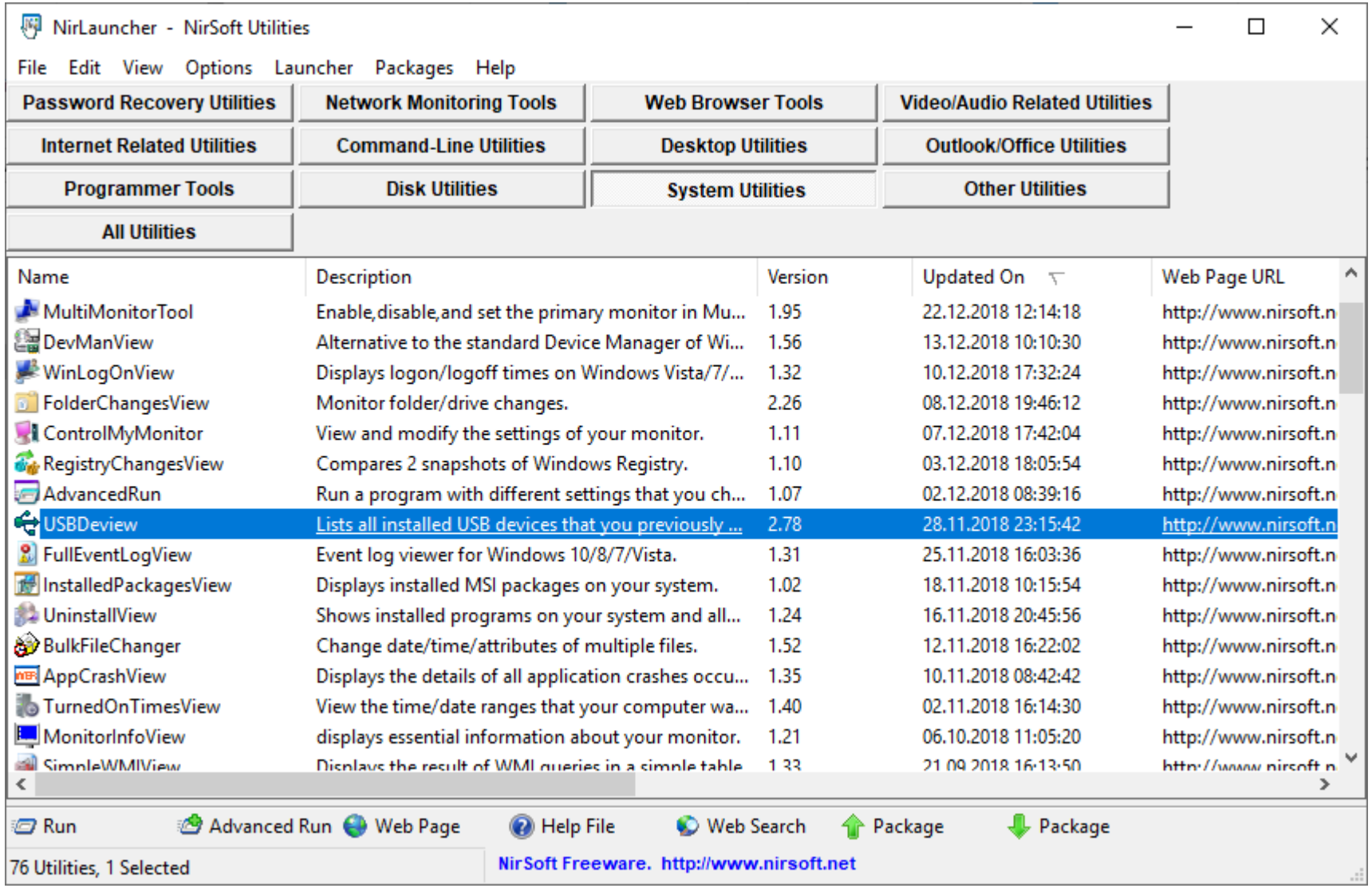


# Webseiten

## HKCU\Software\Microsoft\Internet Explorer\TypedURLs

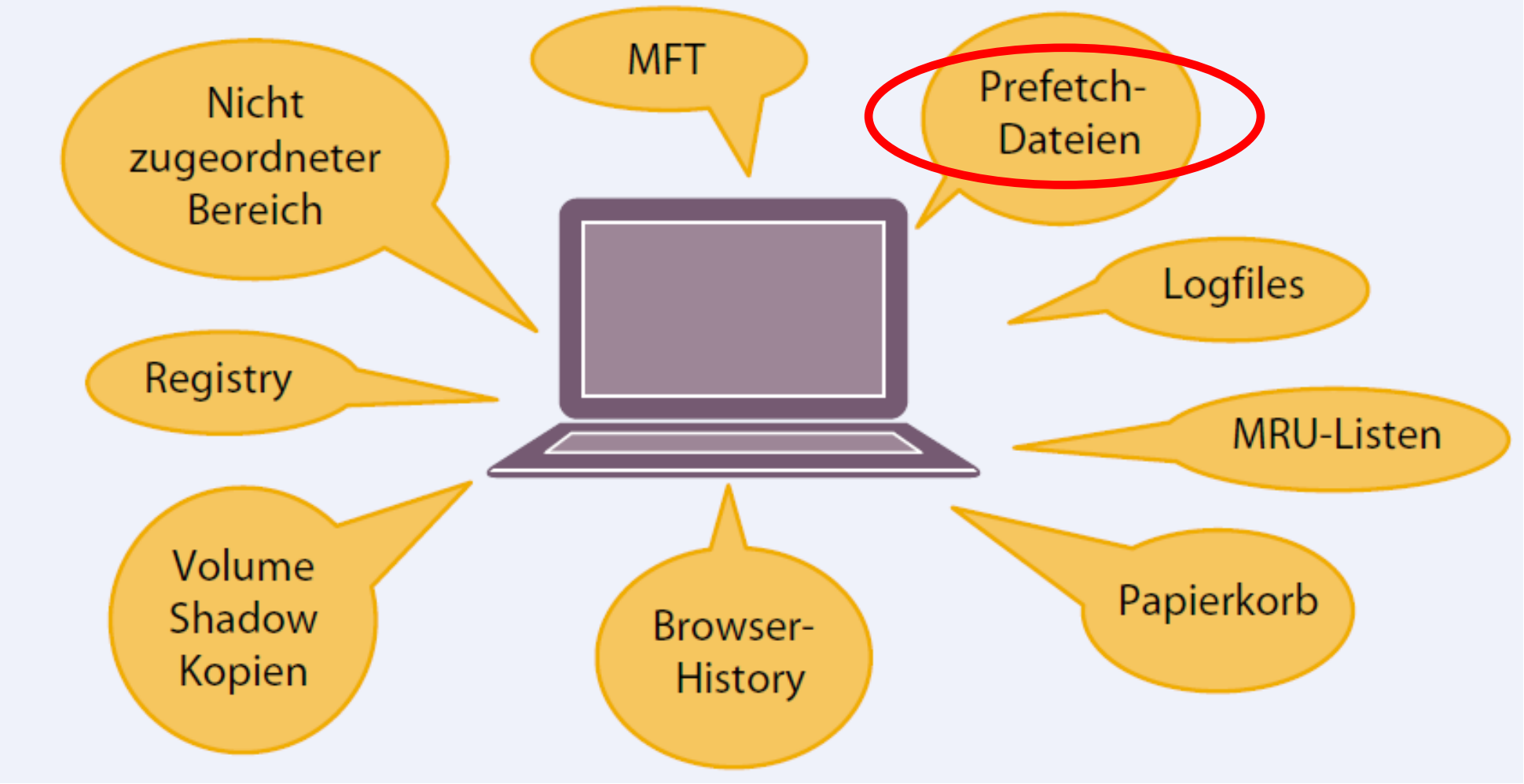


# Toolsammlung NirSoft




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

# Der Computer als Zeuge

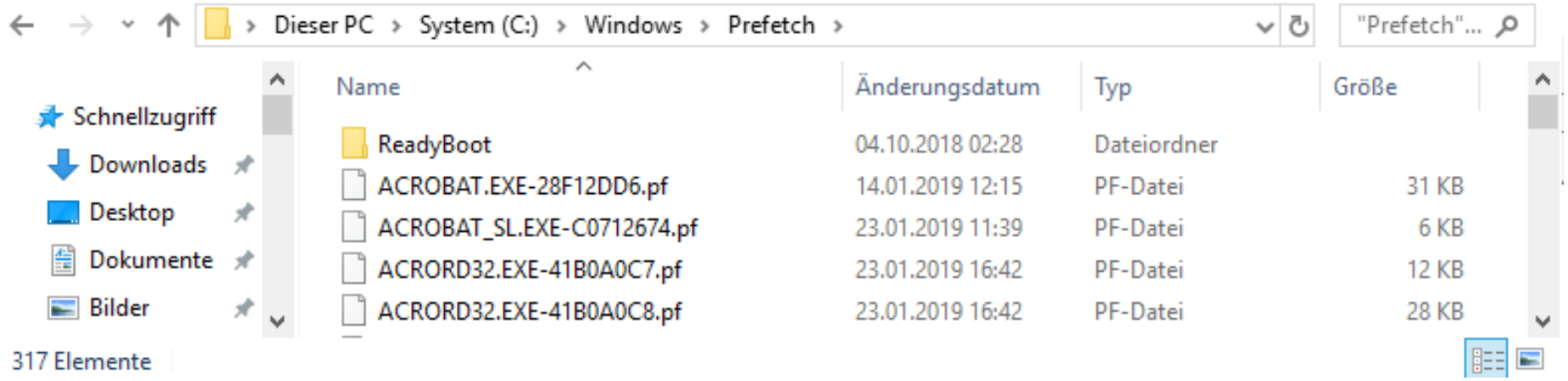



Lautenschläger 2014

# 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



# 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:
  ACRORD32.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://digitalforensicsurvivalpodcast.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 letzen 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

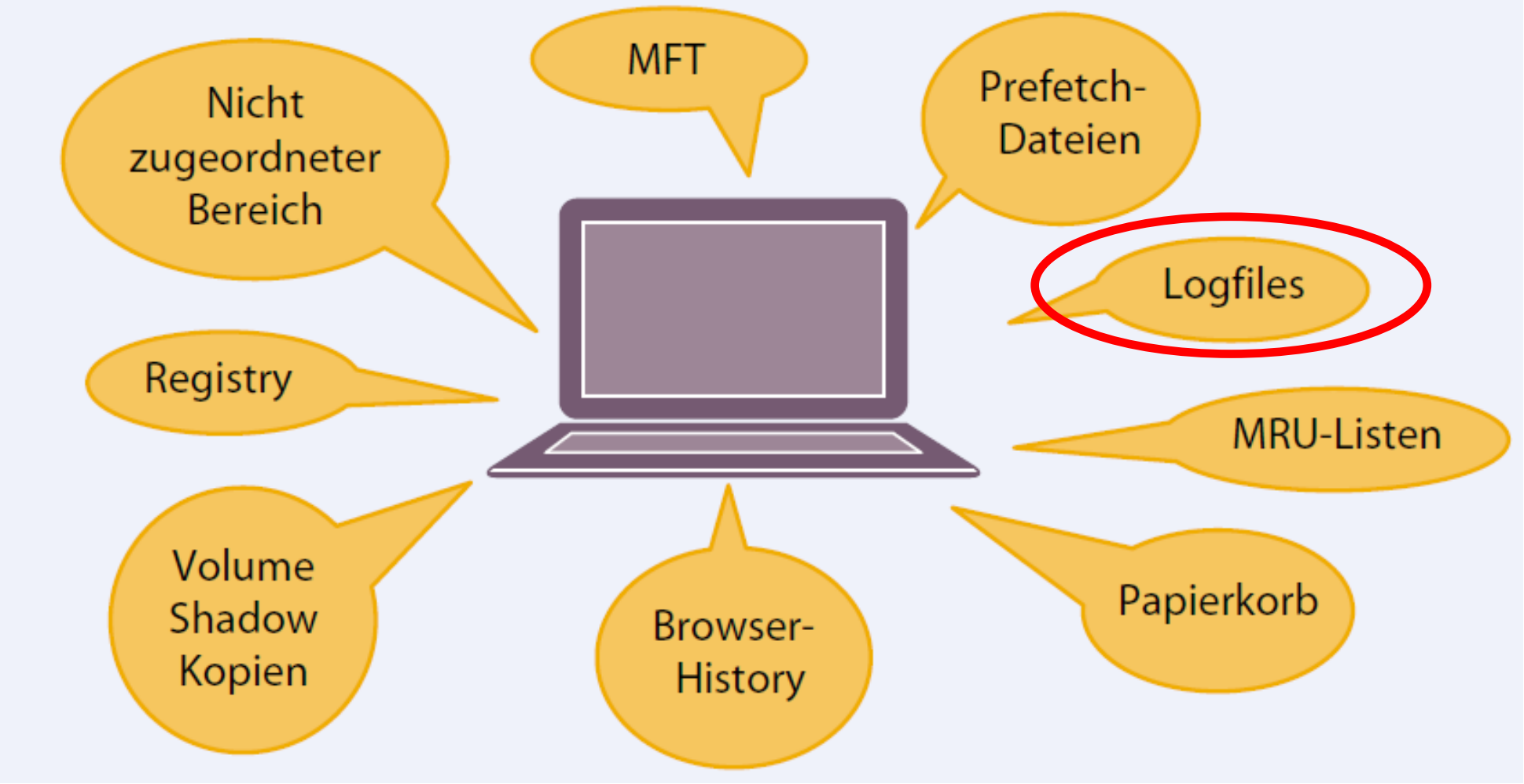
- **Prefetching lässt sich in der Registry abschalten:**
  **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters**
  EnablePrefetcher Value auf 0 setzen
- **Prefetch-Dateien können Aufschluss über U3-verschlüsselte USB-Sticks geben**

| Filename | Created | Modified | Accessed |
|---|---|---|---|
| LAUNCHU3.EXE-XXXXXXXX.pf | 2/5/2007 13:56 | 2/13/2007 5:52 | 2/13/2007 5:52 |
| LAUNCHPAD.EXE-XXXXXXXX.pf | 2/5/2007 13:57 | 2/13/2007 5:52 | 2/13/2007 5:52 |
| CLEANUP.EXE-XXXXXXXX.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

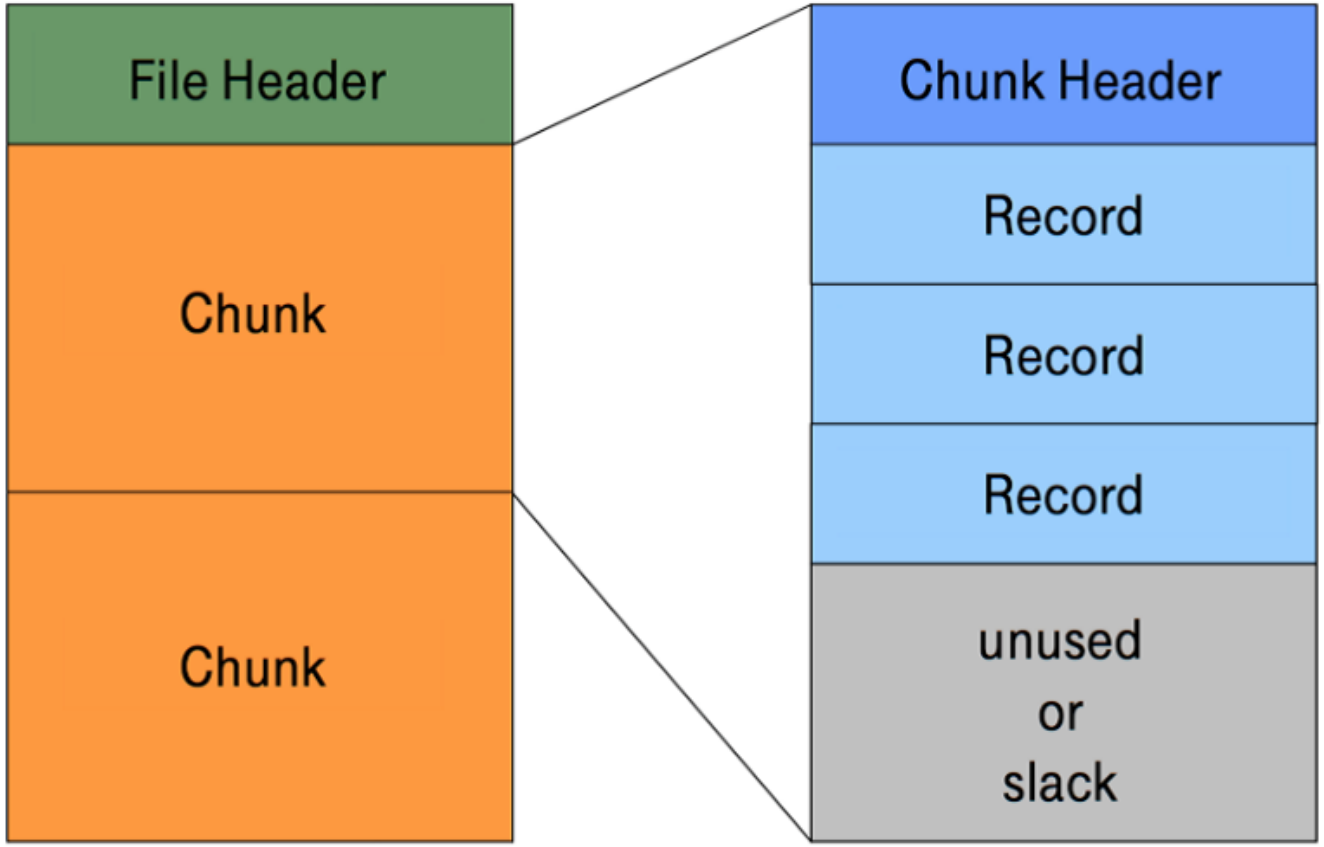



Lautenschläger 2014

# Eventlogs

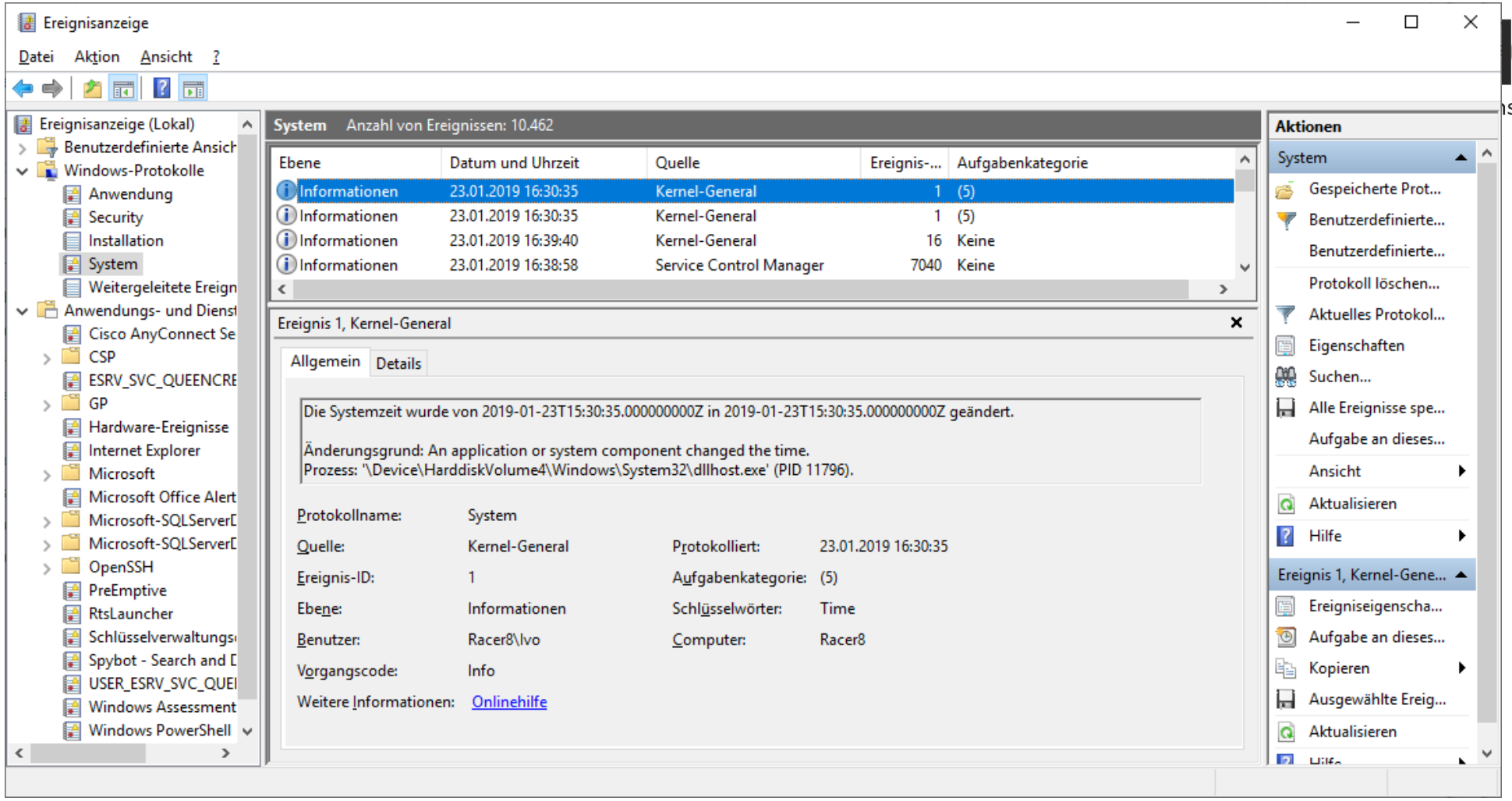
- **bis WinXP: %System%\system32\config**
- **ab Vista: %System%\system32\winevt\logs**
- **Es gibt viel mehr Log-Dateien (einfaches Win 7 > 60; einfaches Win 10 > 250)**
  - Application.evtx
  - System.evtx
  - Security.evtx
  - HardwareEvents.evtx
  - InternetExplorer.evtx
  - MediaCenter.evtx

# Eventlogs

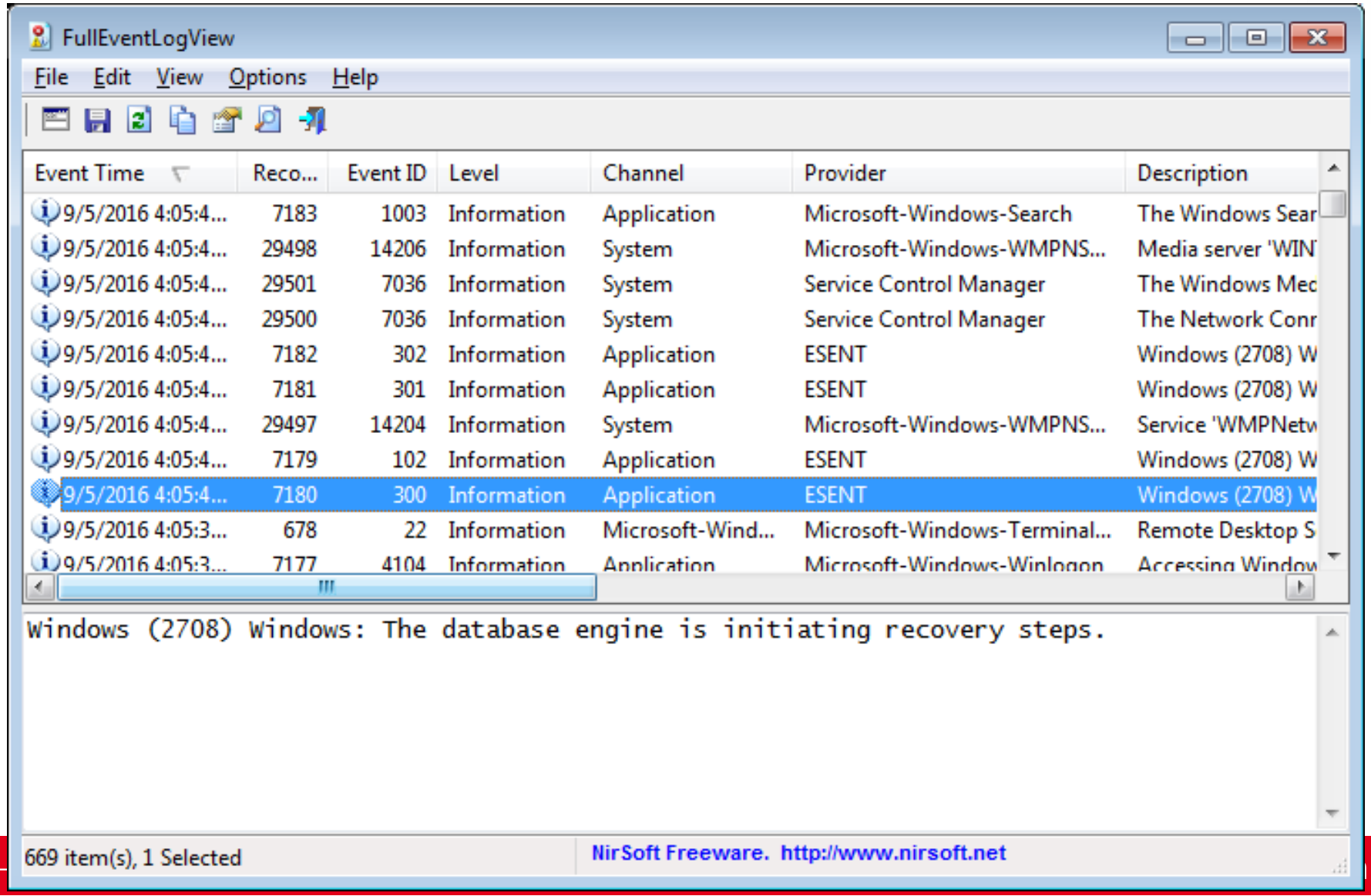



Hummert (2017)

# Eventlog-Viewer



# Eventlog-Viewer



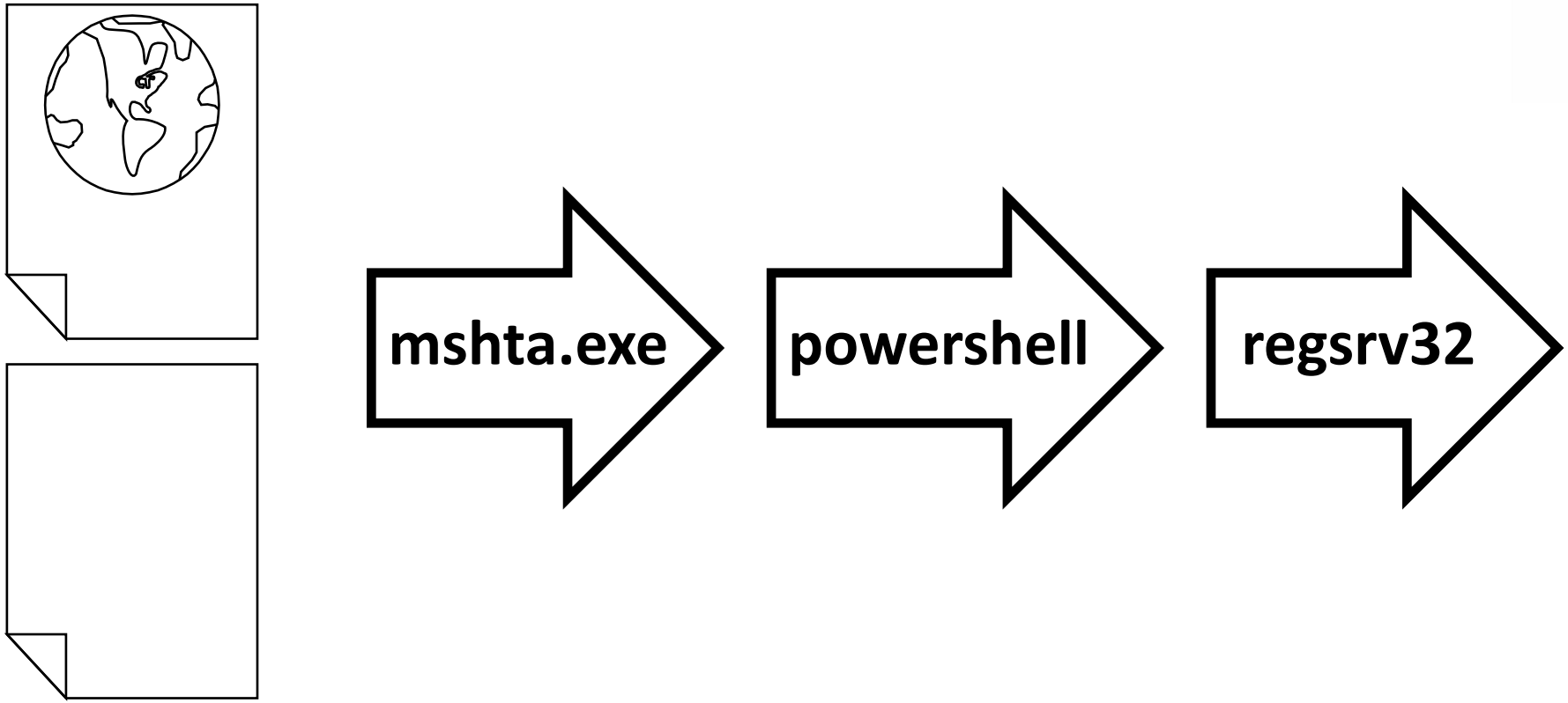
# Beispiel für einen Vorfall: Konboot

# Arbeitsspeicher-Forensik

# Wonach suche ich?

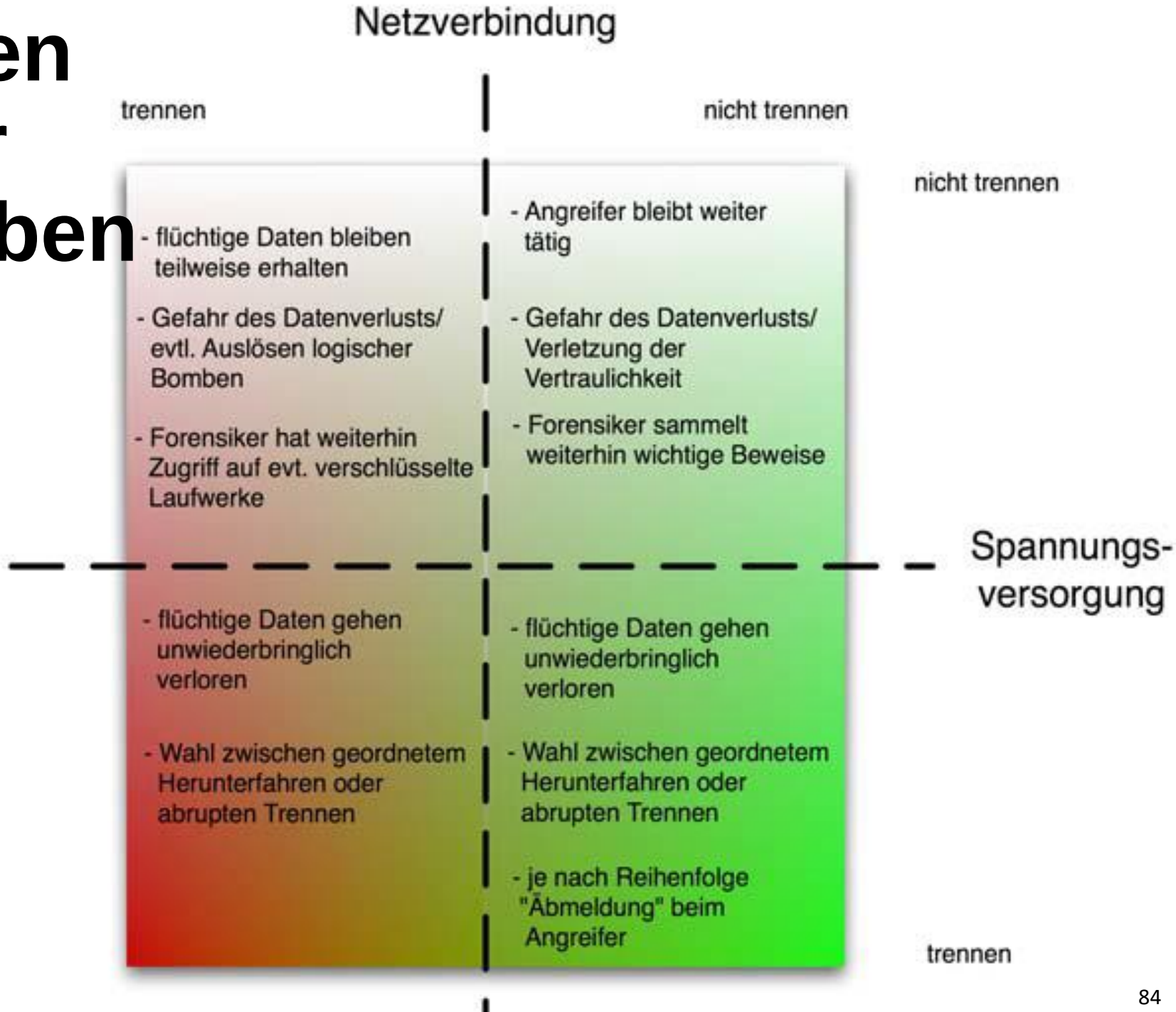
- Prozesse
- Passwörter
- Systemhinweise
- Texte
- Treiber
- Logs
- Bilder
- Schadsoftware

# Fileless Malware




Quelle: aeksecurity.tech

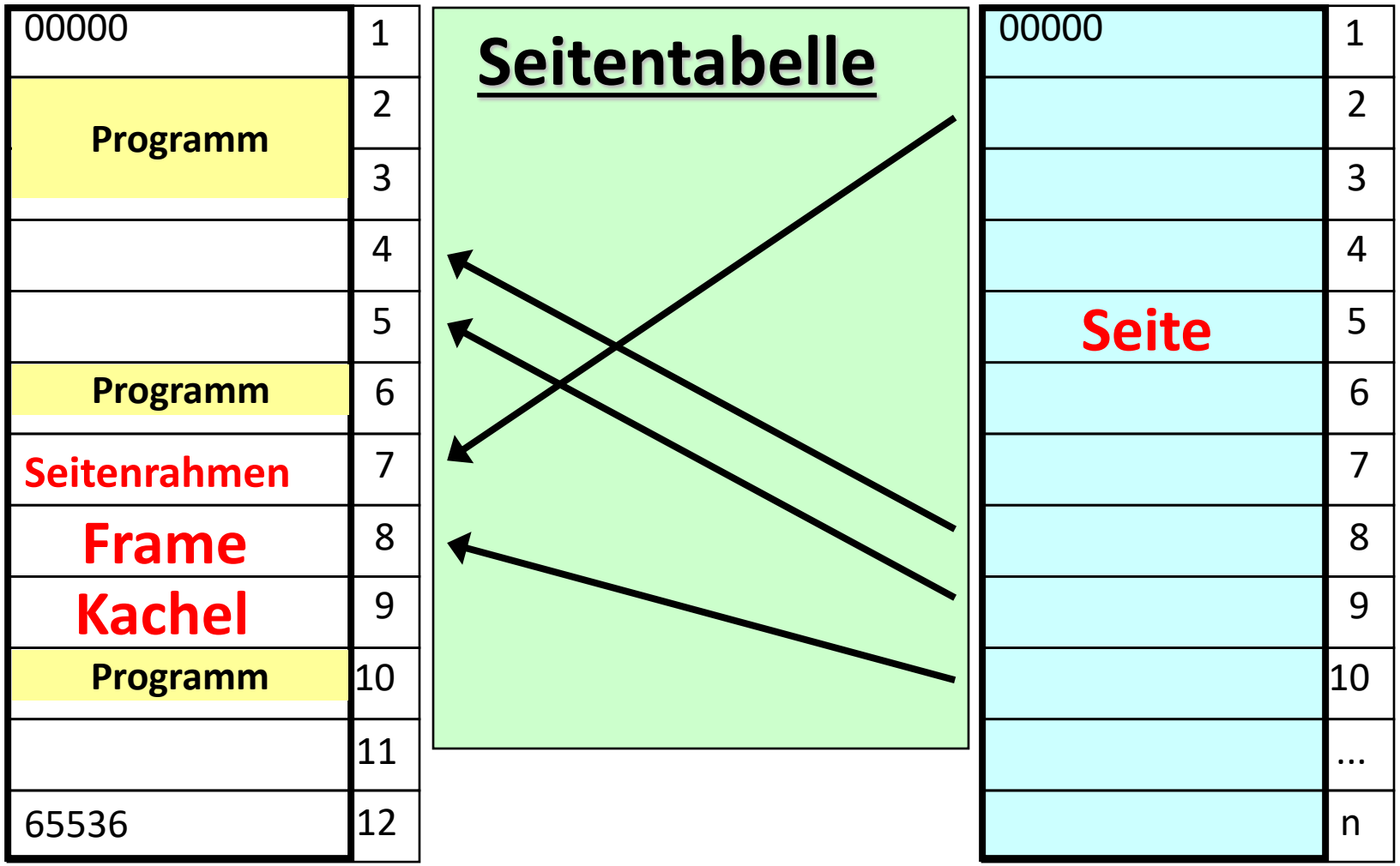
# Leben oder Sterben



# 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

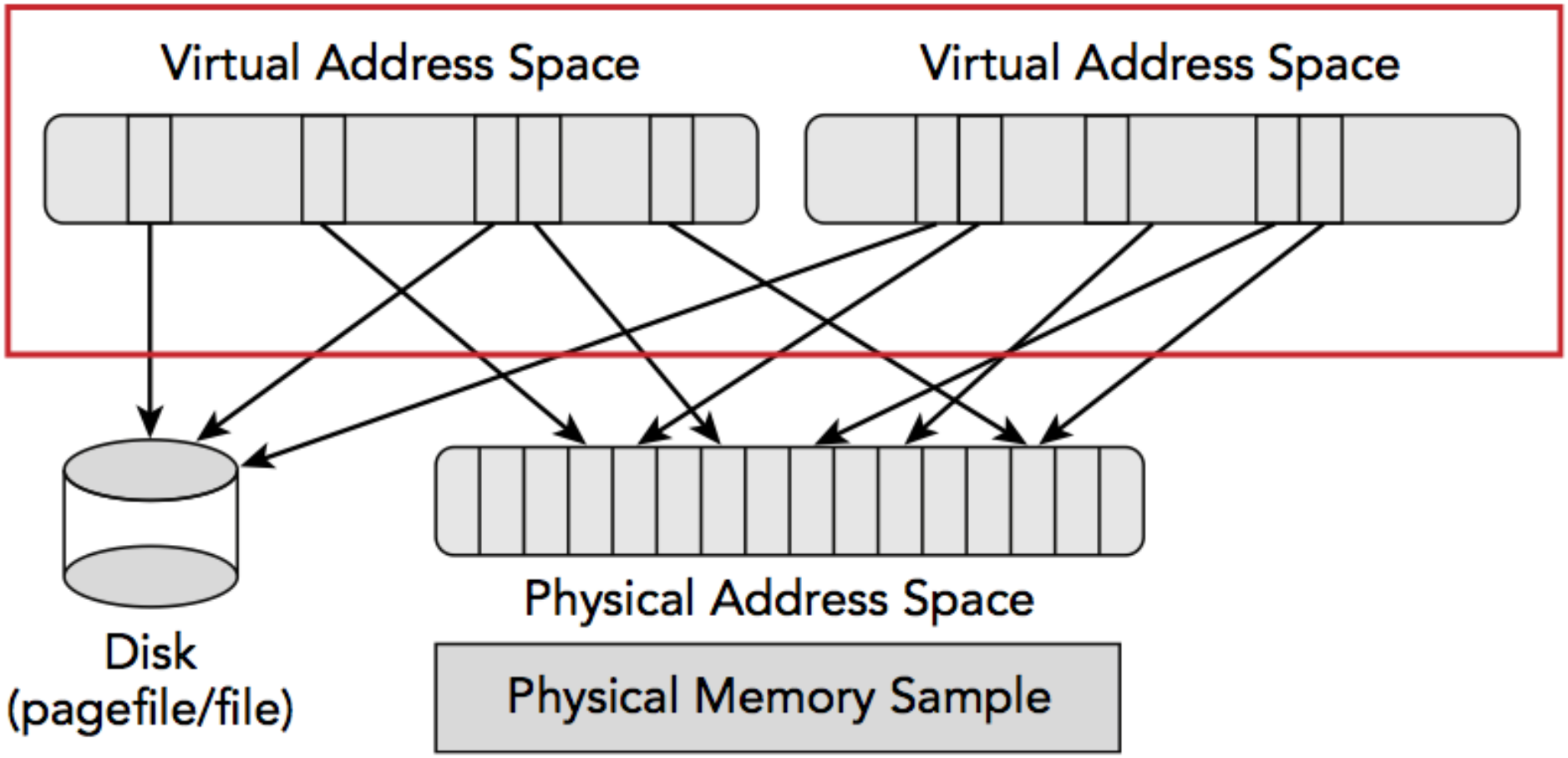
# Virtueller Speicher



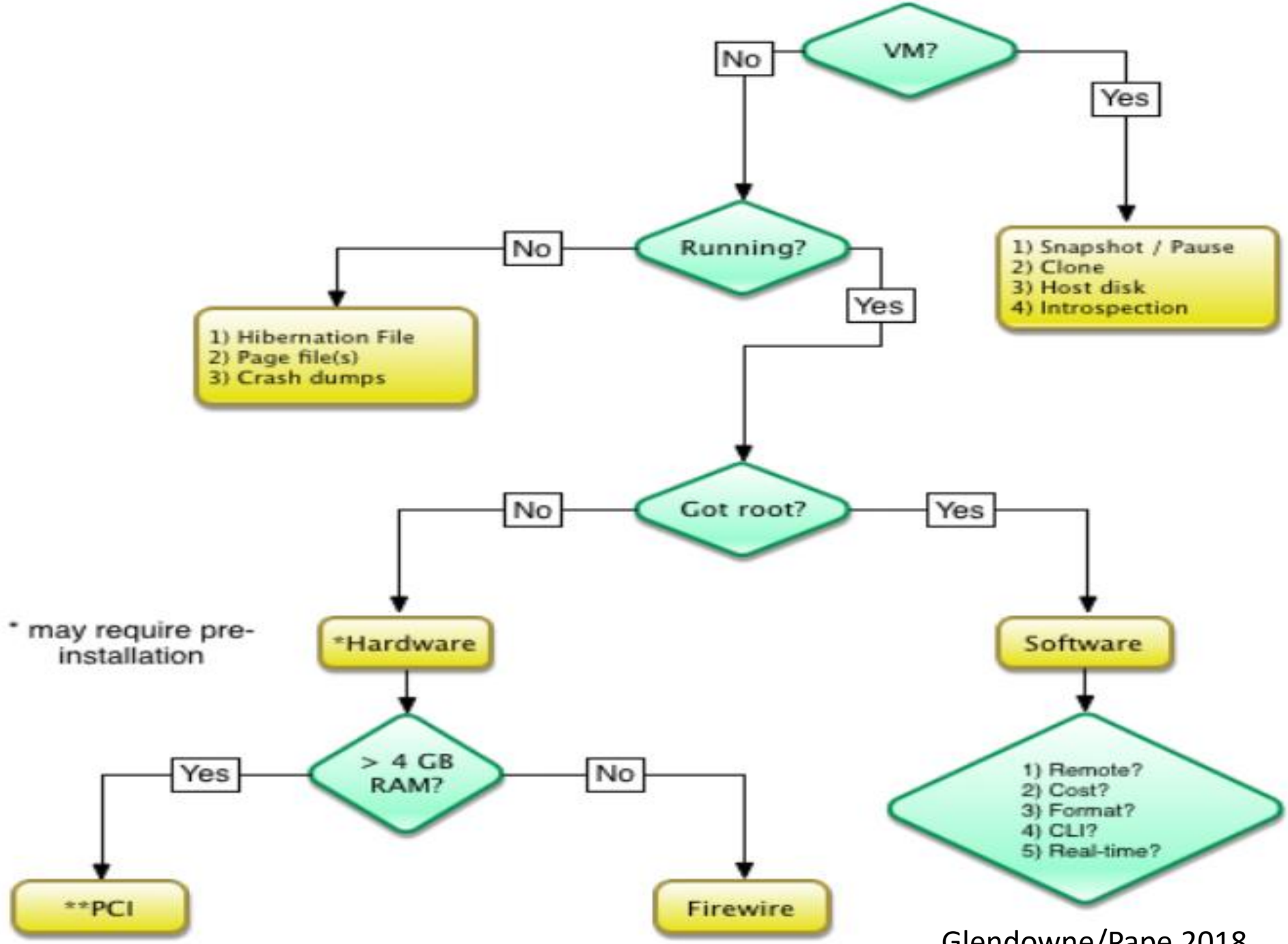

**Fragmentierter endlicher Speicher**

**Beliebig langer, durch-gehender Speicher**

# Virtueller Speicher




Glendowne/Pape 2018


VM?
No
Yes
Running?
No
Yes
1) Hibernation File
2) Page file(s)
3) Crash dumps
1) Snapshot / Pause
2) Clone
3) Host disk
4) Introspection
Got root?
No
Yes
* may require pre-installation
*Hardware
Software
> 4 GB RAM?
Yes
No
1) Remote?
2) Cost?
3) Format?
4) CLI?
5) Real-time?
**PCI
Firewire
**very expensive

# Arbeitsspeicher-Forensik

1. Speicherabbild erstellen
   - RAW memory dump z. B. mit DumpIt
   - 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
- DumpIt
- Mandiant Memoryze
- HBGary FastDump
- MoonSols Windows Memory Toolkit
- AccessData FTK Imager
- EnCase WinEn
- Belkasoft Live RAM Capturer
- ATC-NY Windows Memory Reader
- Winpmem (Rekall)

# DumpIt

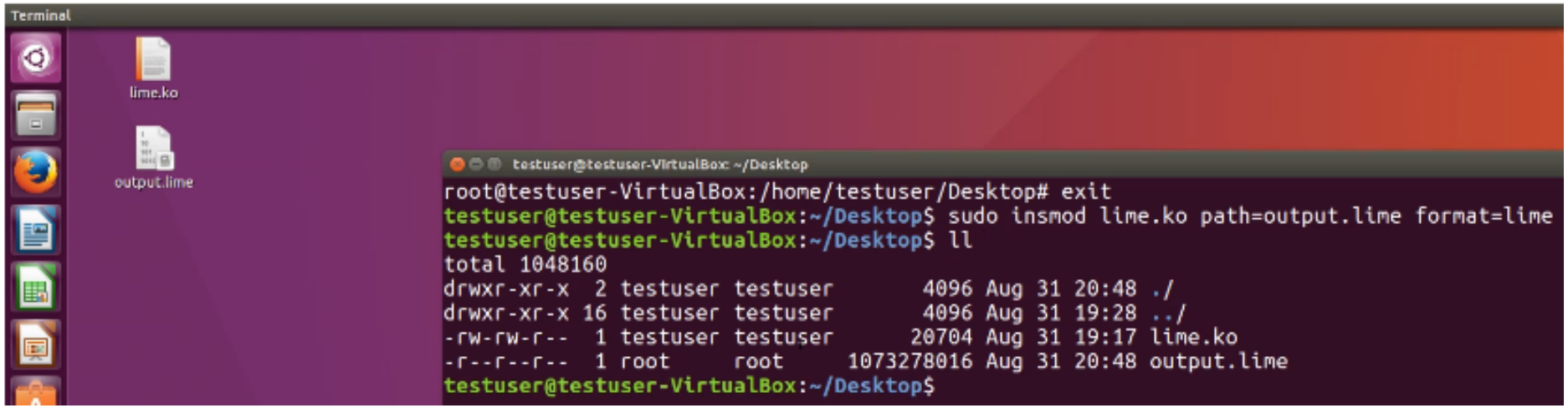
E:\Downloads\DumpIt\x64\DumpIt.exe

```
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)]
  + Processing...
```

# Linux Memory Dump

Hochschule Stralsund

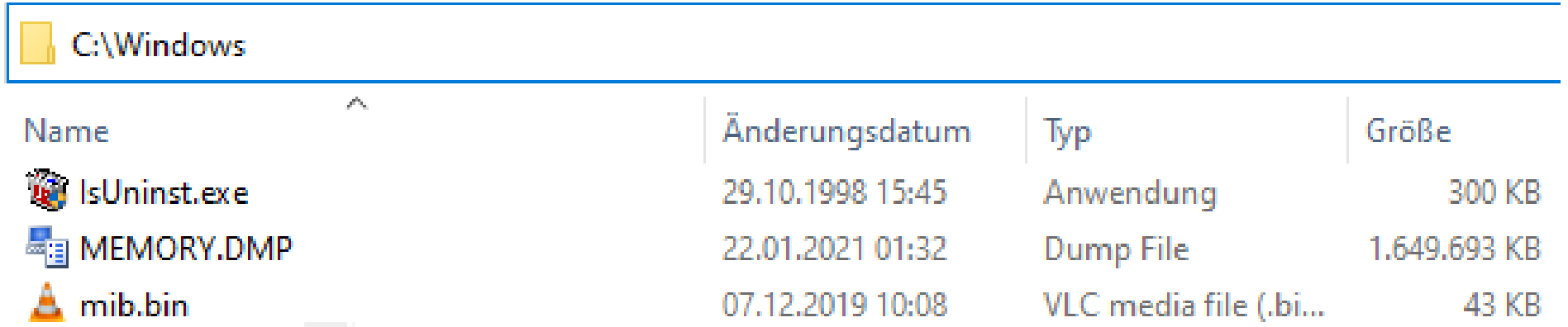
```
sudo insmod lime.ko path=output.lime format=lime
```



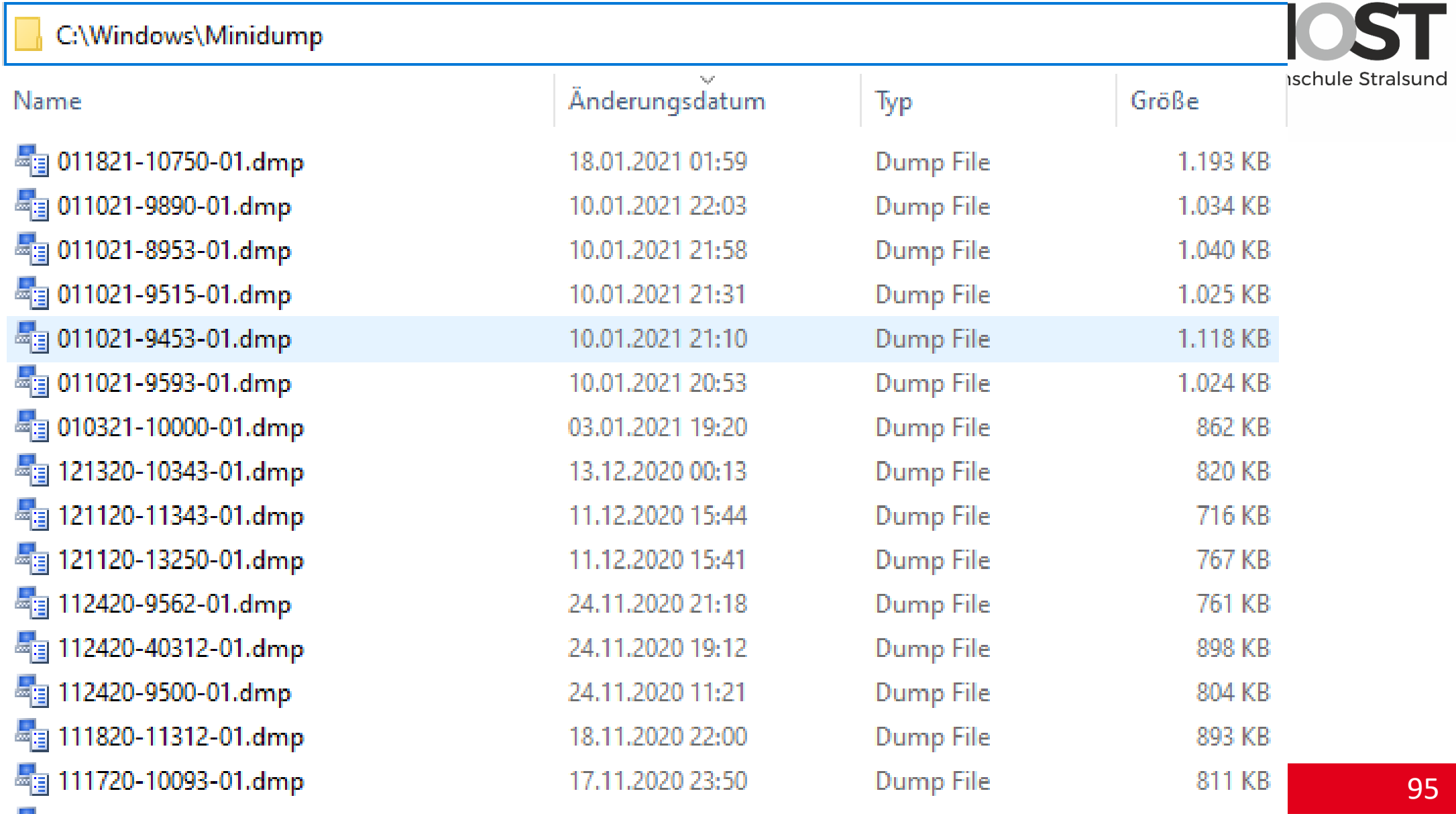
# macOS Memory Dump

```
$ 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
```

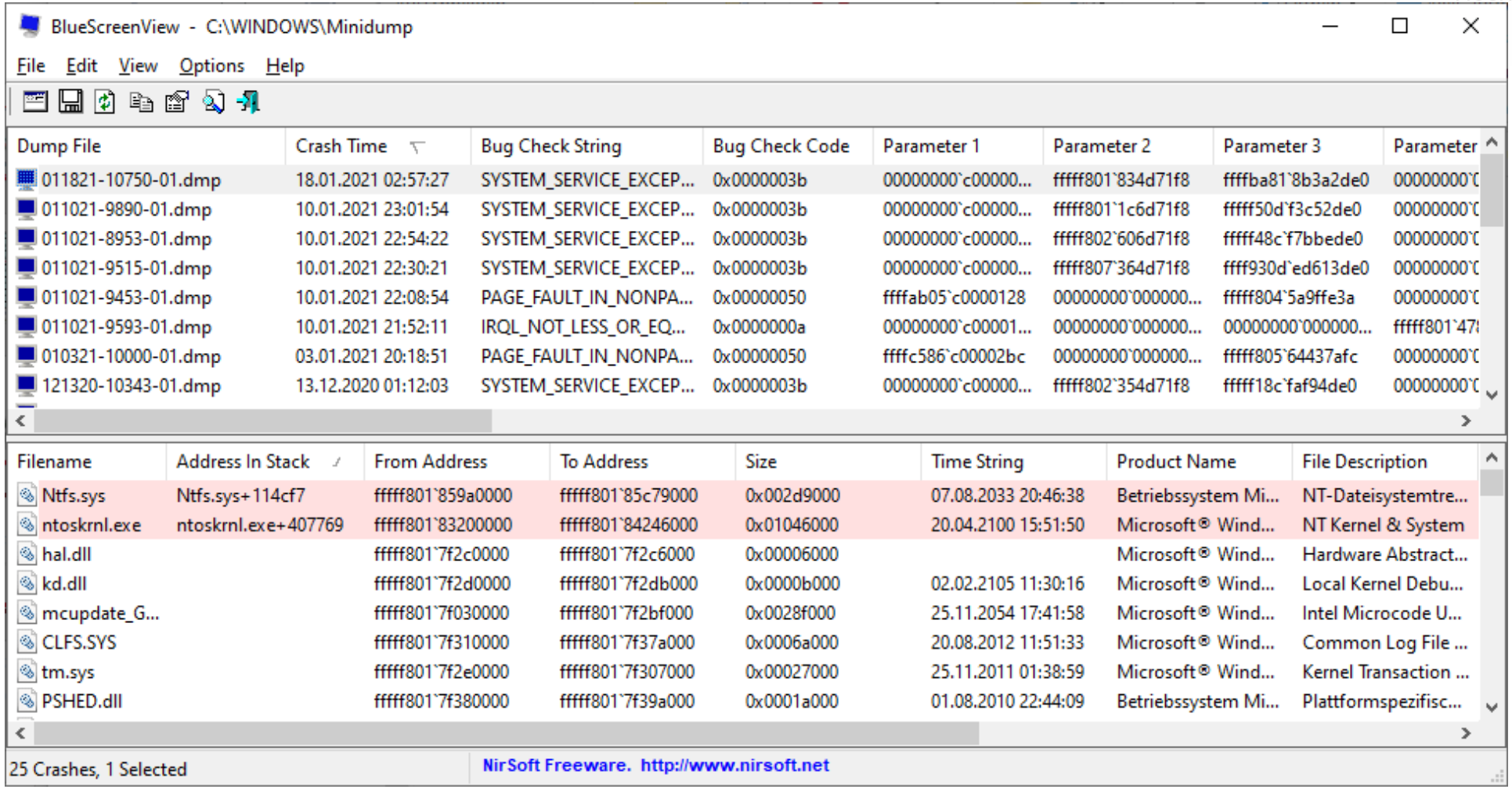
# Windows Crashdumps



# Windows Crashdumps



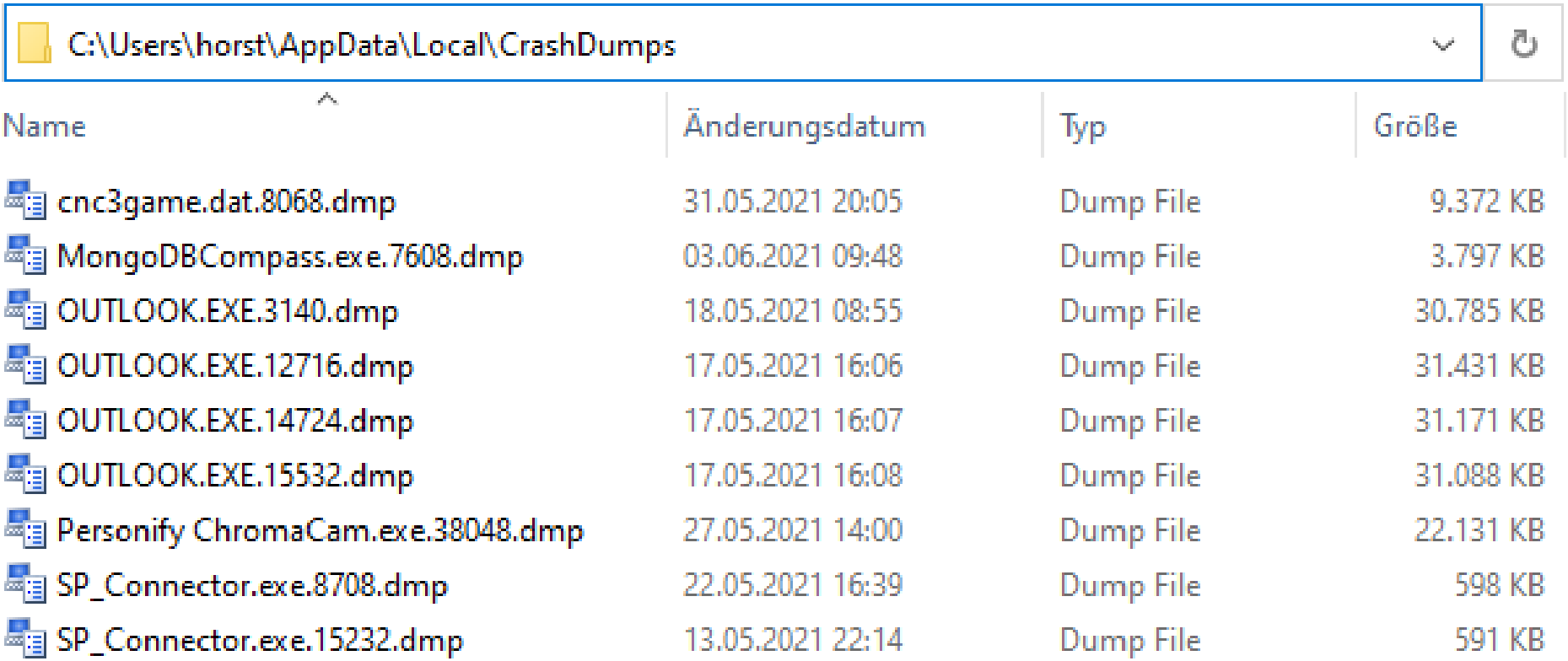
# Windows Crashdumps



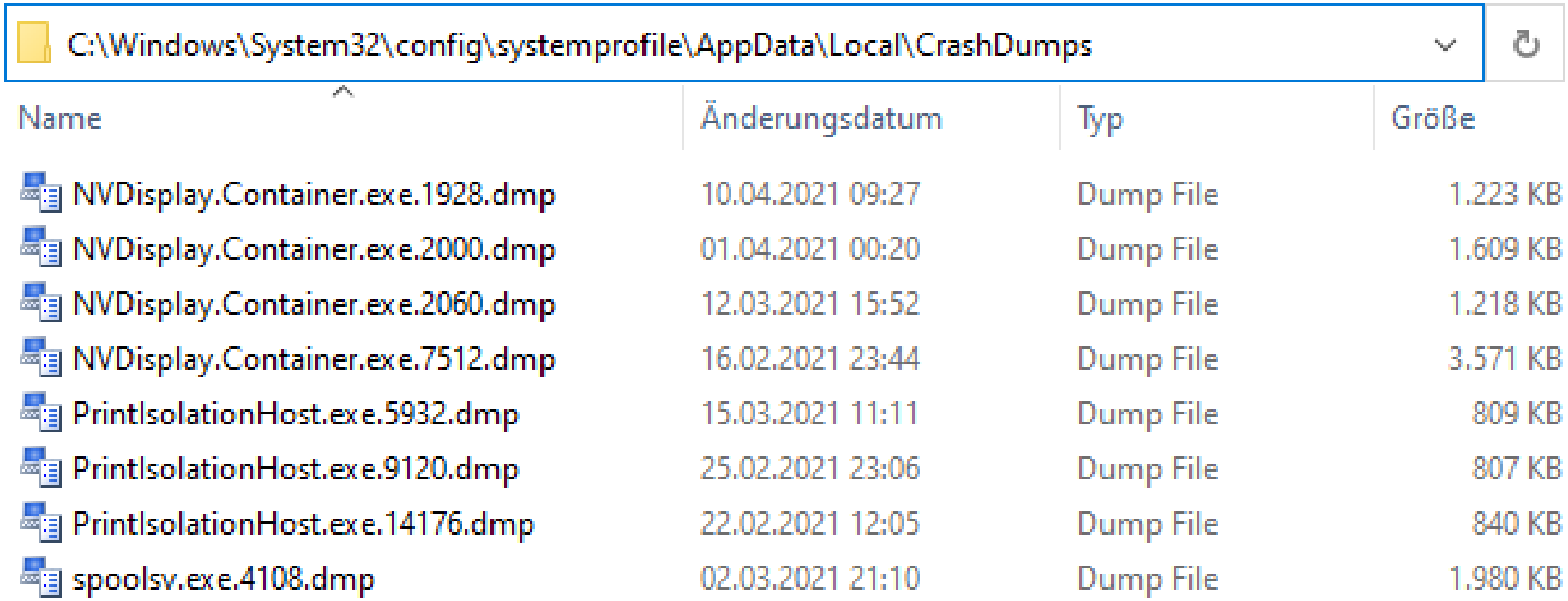
# Windows Crashdumps

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

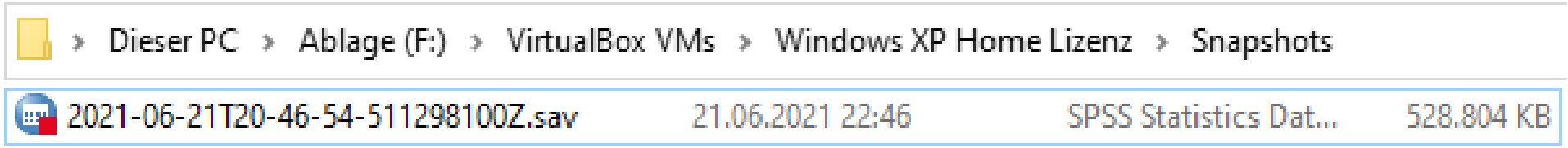
# Windows User Crashdumps



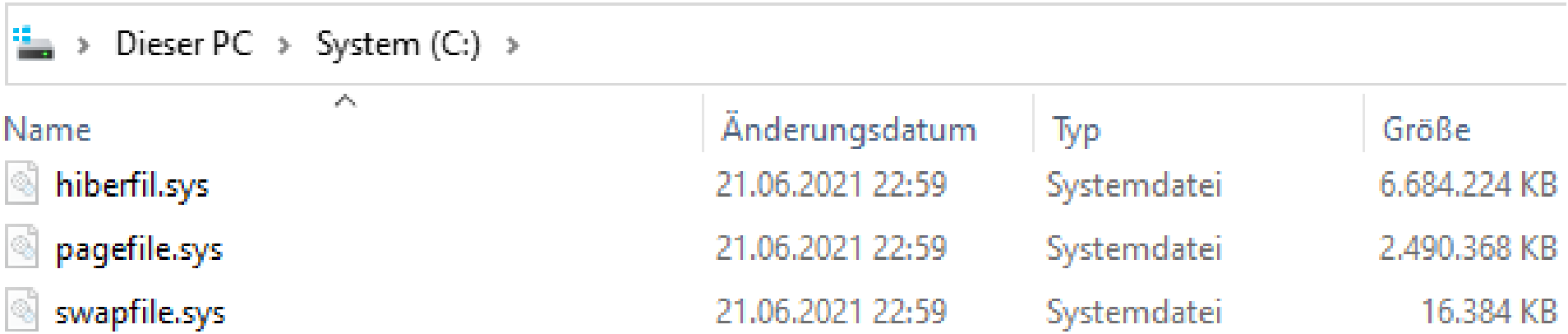
# Windows System Crashdumps



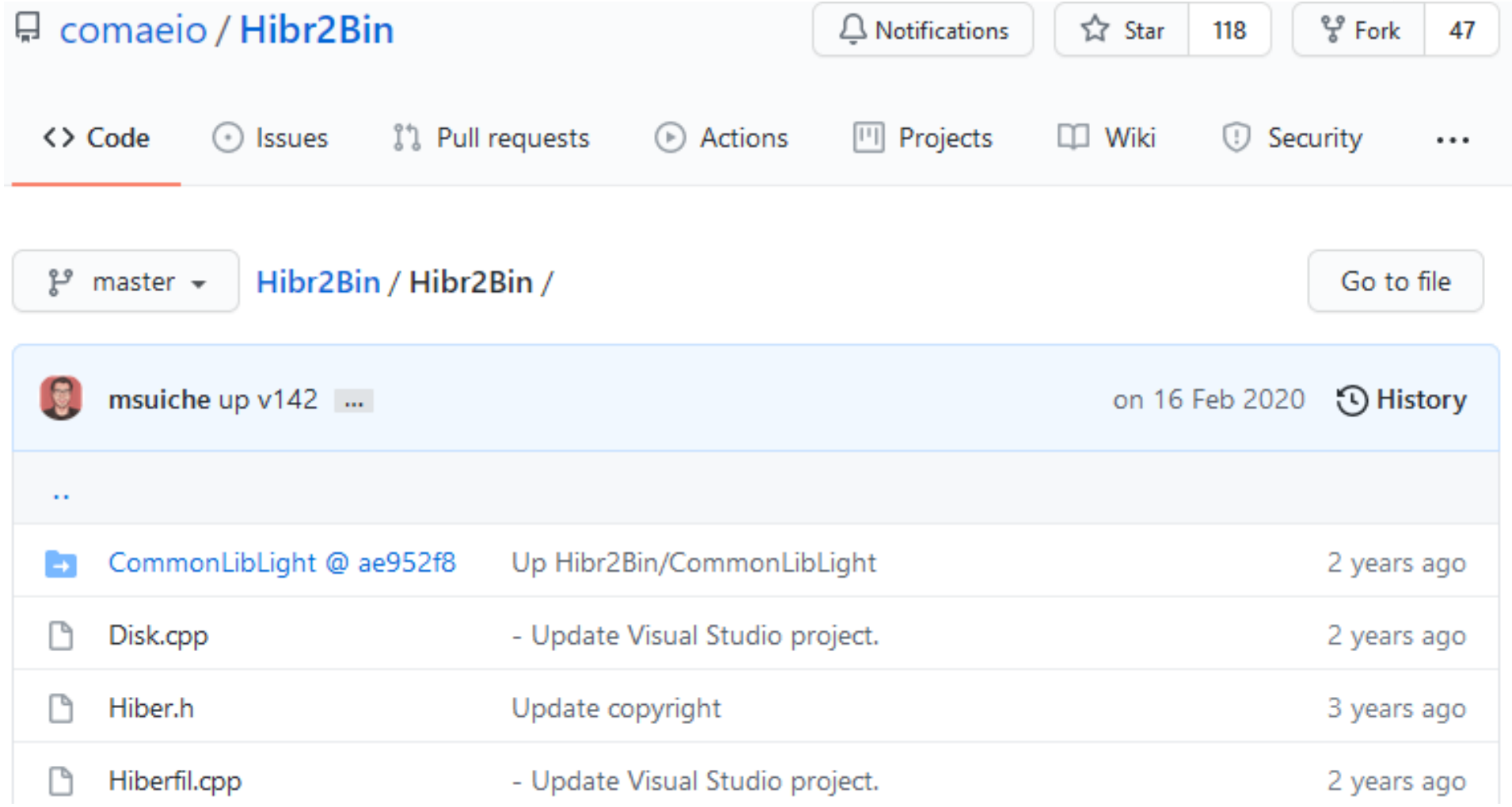
# Virtual Maschine Dumps



# Pagefile, Swapfile, Hiberfile



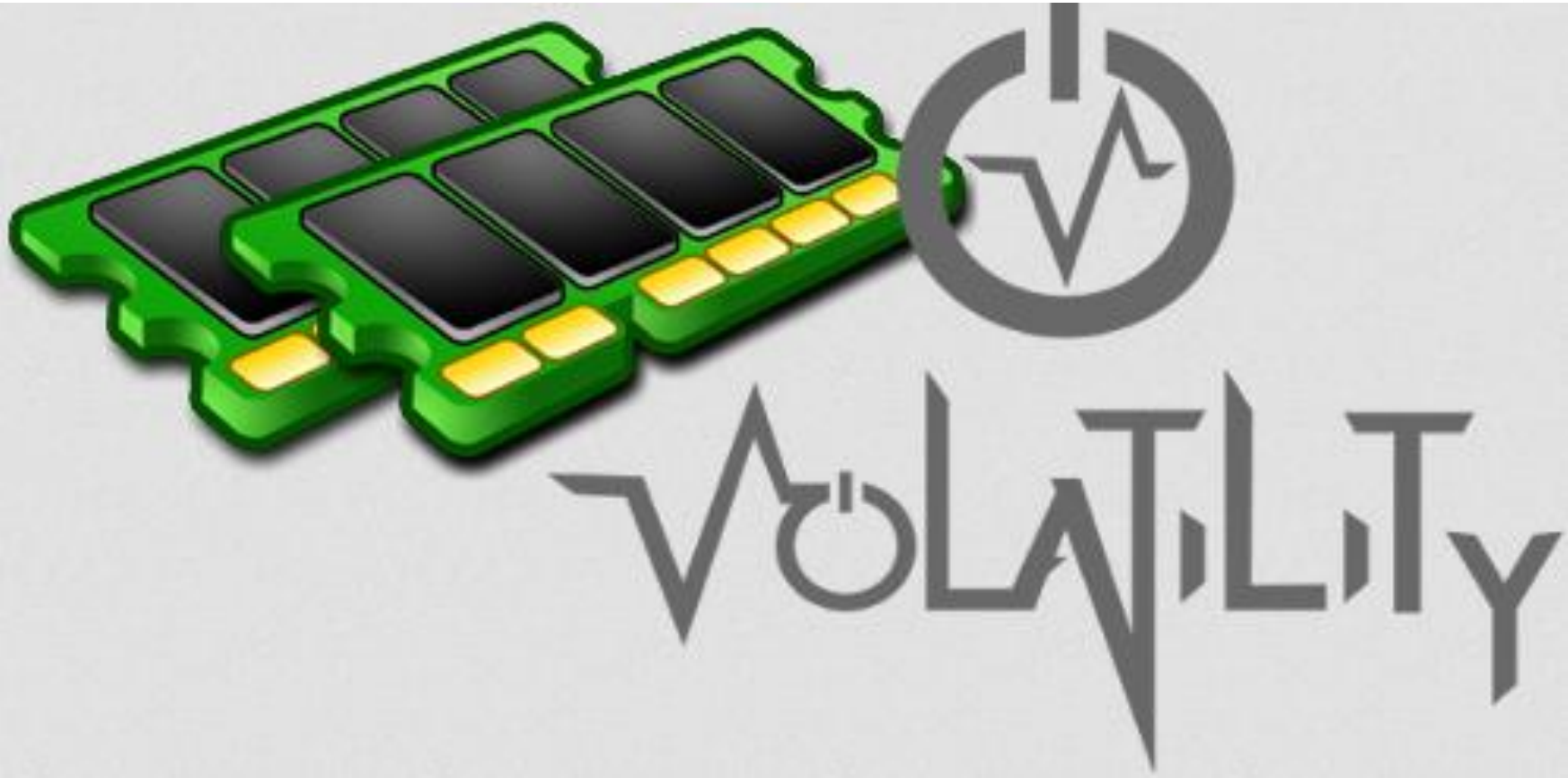
# Hiberfil dekomprimieren



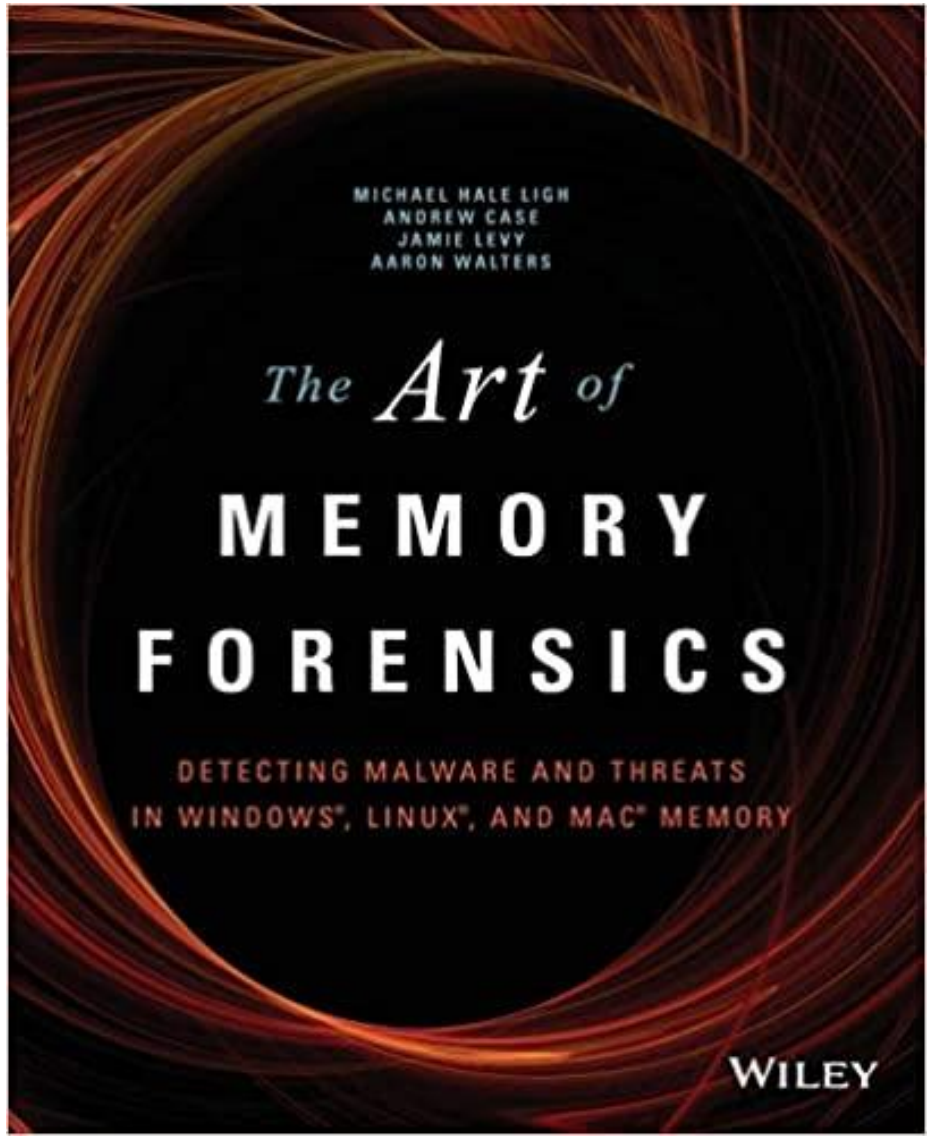

IBM Content Manager
& OnDemand
OnBase
a Hyland Software solution
Microsoft Office
SharePoint
OPENTEXT
FILENET
An IBM Company
BULK EXTRACTOR
Documents
Meta Data
PDF
PC data files with associated
index information

# Arbeitsspeicher-Forensik

HOST
Hochschule Stralsund



# Arbeitsspeicher-Forensik




HOST
Hochschule Stralsund

# Volatility

vol.py -h
Hilfe

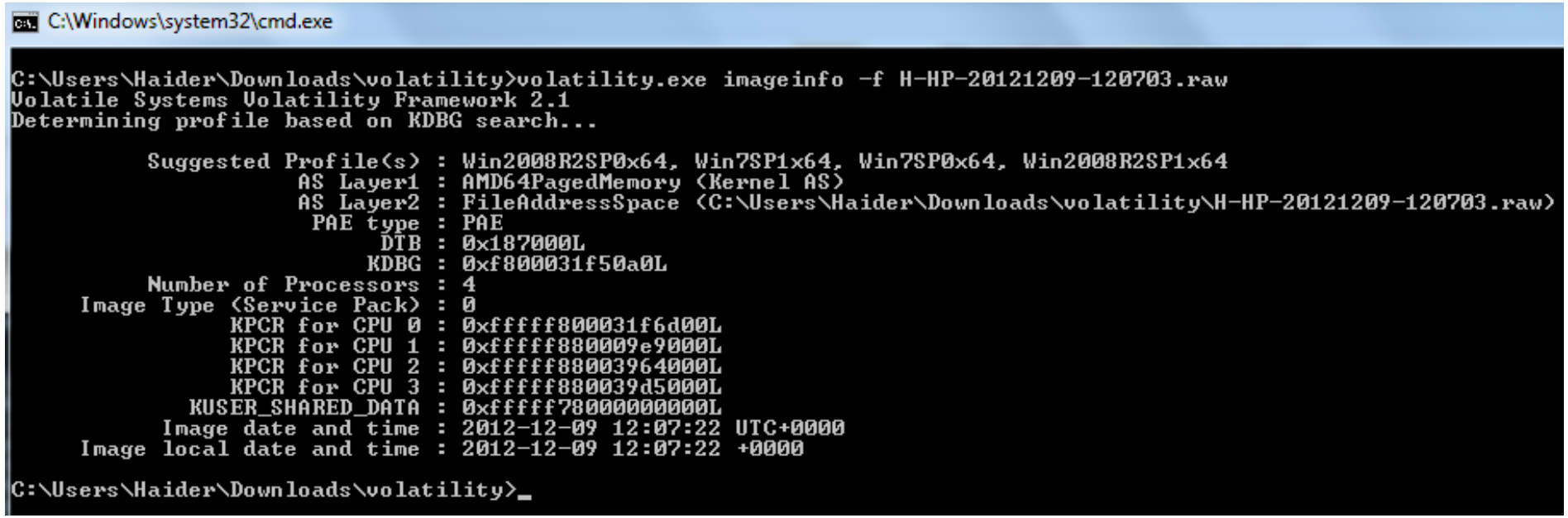
vol.py -info
Alle Profile, Adressräume, und Plugins

# Volatility Imageinfo

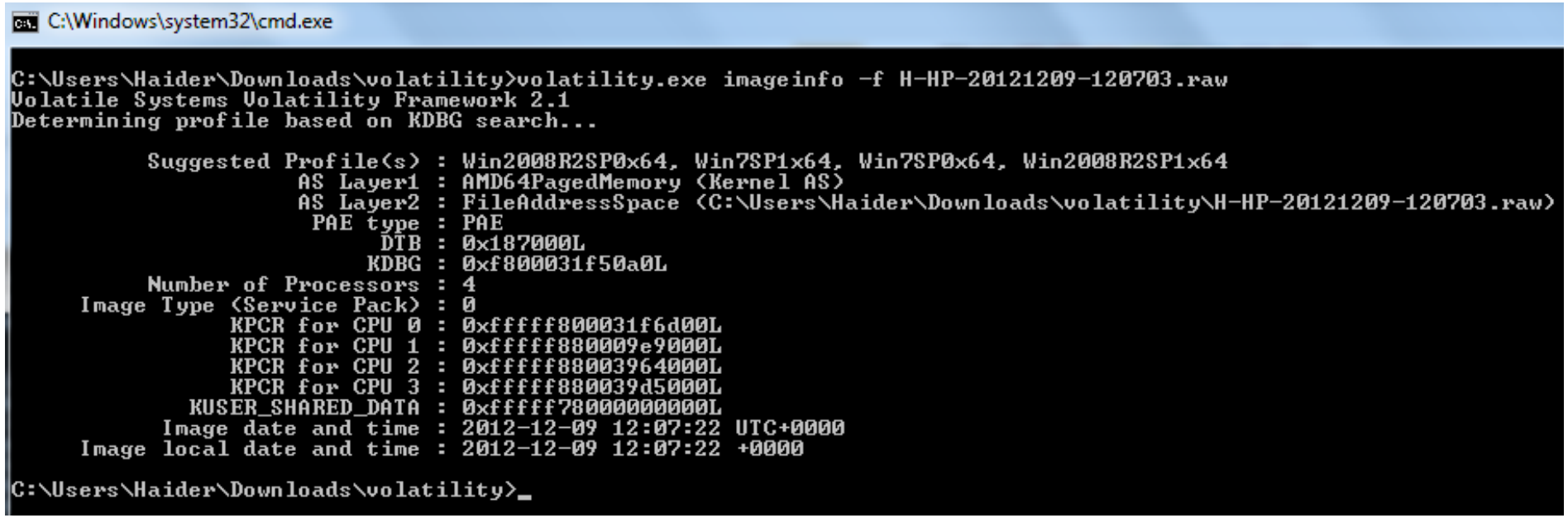
Hochschule Stralsund

```
(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



# Volatility kdbgscan



# 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

```
$ 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
------------------ -------------------- ------ ------ ------ -------- ------ ------ -------------------
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

Hochschule Stralsund

**Handles repräsentieren Zugriff auf Objekte**

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

# Arbeitsspeicher-Forensik

Hochschule Stralsund

*handles*

**zeigt die Handles aller laufenden Prozesse**

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

# Arbeitsspeicher-Forensik

Hochschule Stralsund

***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

Hochschule Stralsund

**Legen Netzwerk-Aktivitäten offen, z. B.**

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

# Arbeitsspeicher-Forensik

Hochschule Stralsund

```
(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

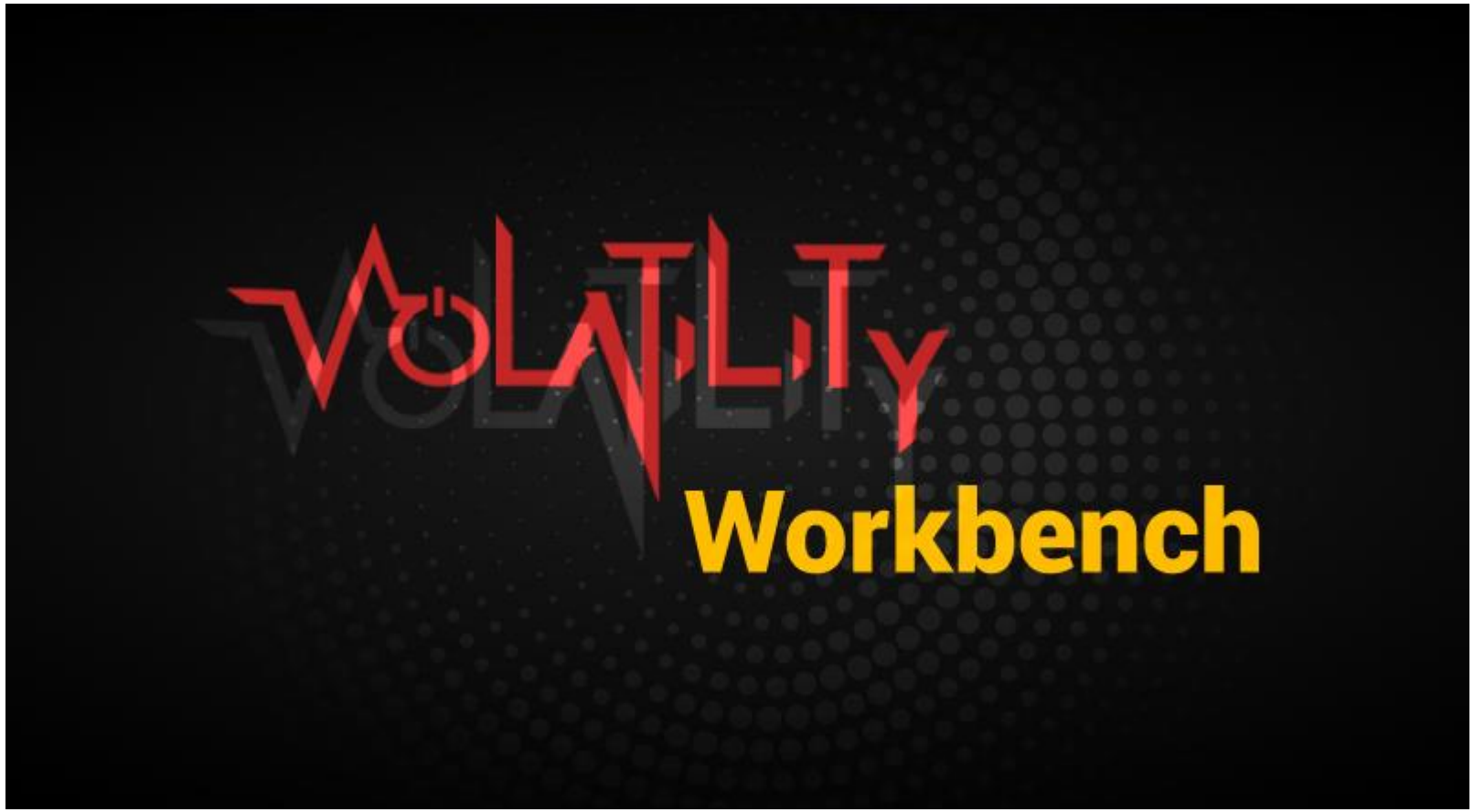
Hochschule Stralsund

```
(rekall_env)DMP:Mem_Images dae$ vol.py -f Win7/shelly.vmem --profile=Win7SP1x86 dumpfiles -Q 0x000000007d602d48 -n -D .
Volatility Foundation Volatility Framework 2.5
ImageSectionObject 0x7d602d48   None   \Device\HarddiskVolume1\Windows\explorer.exe
DataSectionObject 0x7d602d48   None   \Device\HarddiskVolume1\Windows\explorer.exe
```

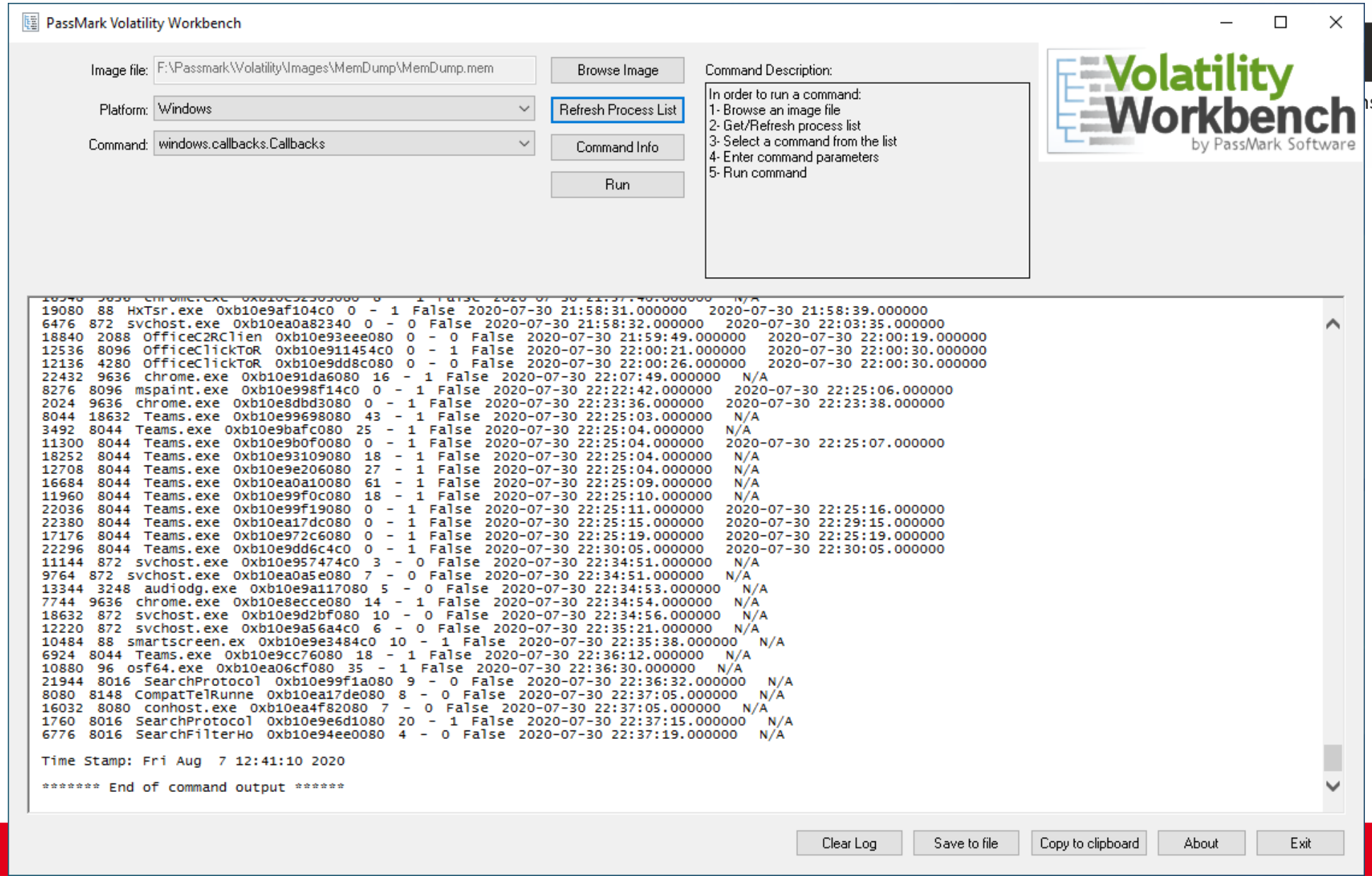
# Arbeitsspeicher-Forensik


```
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/Des
2020-09-26 11:42:11 UTC+0000|[IEHISTORY]| explorer.exe→Visited: raj@file:///C:/Users/raj/Des
2020-09-17 17:43:58 UTC+0000|[IEHISTORY]| explorer.exe→Visited: raj@file:///E:/raj.txt| PID
2020-09-26 11:48:11 UTC+0000|[IEHISTORY]| explorer.exe→Visited: raj@file:///C:/Users/raj/Des
2020-10-01 21:56:04 UTC+0000|[IEHISTORY]| explorer.exe->:20201001202010O2: raj@file:///C:/Use
2020-10-01 21:56:04 UTC+0000|[IEHISTORY]| explorer.exe->:20201001202010O2: raj@:Host: Compute
2020-10-01 16:26:04 UTC+0000|[IEHISTORY]| iexplore.exe→Visited: raj@file:///C:/Users/raj/Des
2020-09-26 11:42:11 UTC+0000|[IEHISTORY]| iexplore.exe→Visited: raj@file:///C:/Users/raj/Des
2020-09-17 17:43:58 UTC+0000|[IEHISTORY]| iexplore.exe→Visited: raj@file:///E:/raj.txt| PID
2020-09-26 11:48:11 UTC+0000|[IEHISTORY]| iexplore.exe→Visited: raj@file:///C:/Users/raj/Des
```

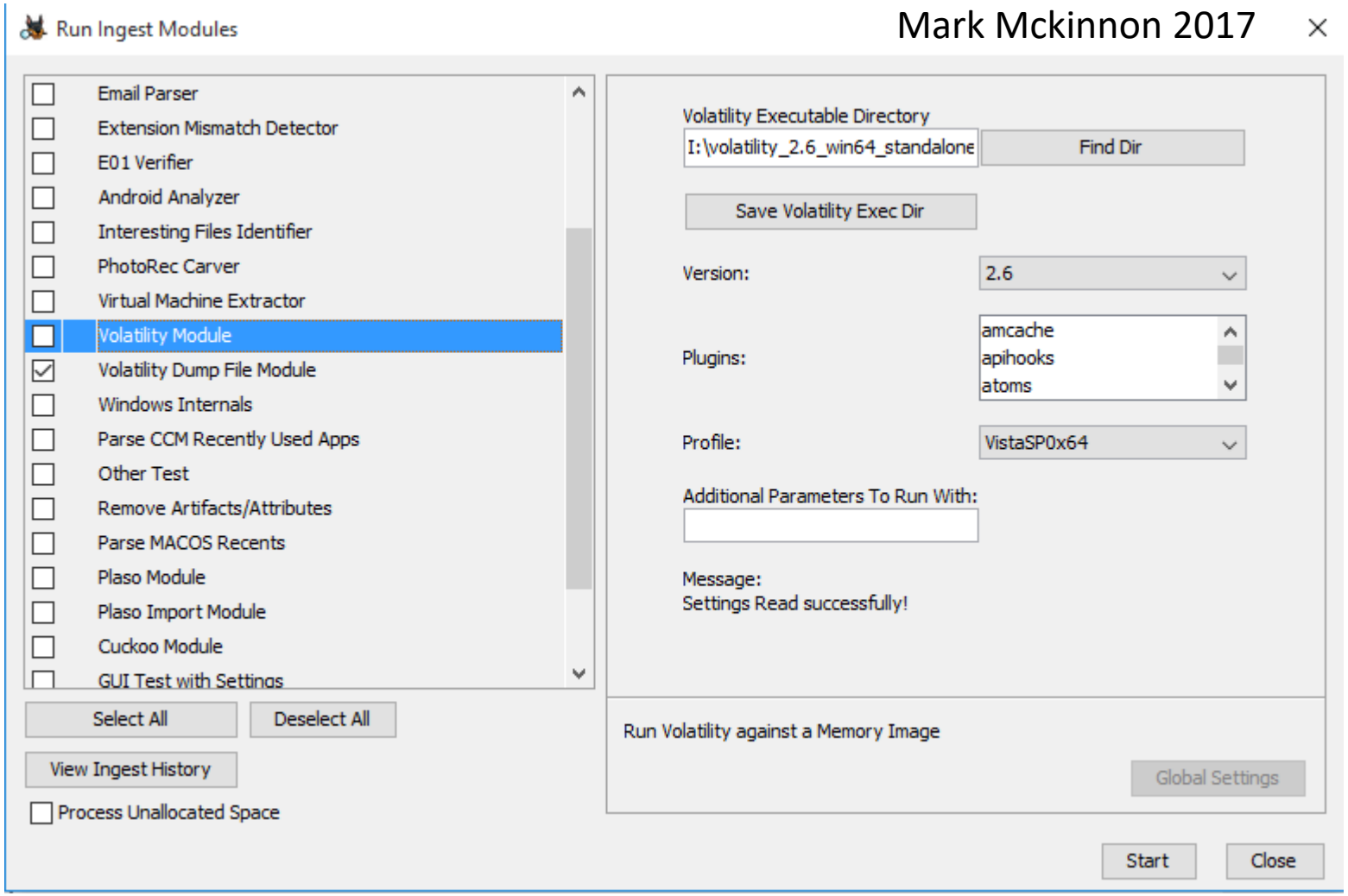
# Arbeitsspeicher-Forensik



# Arbeitsspeicher-Forensik

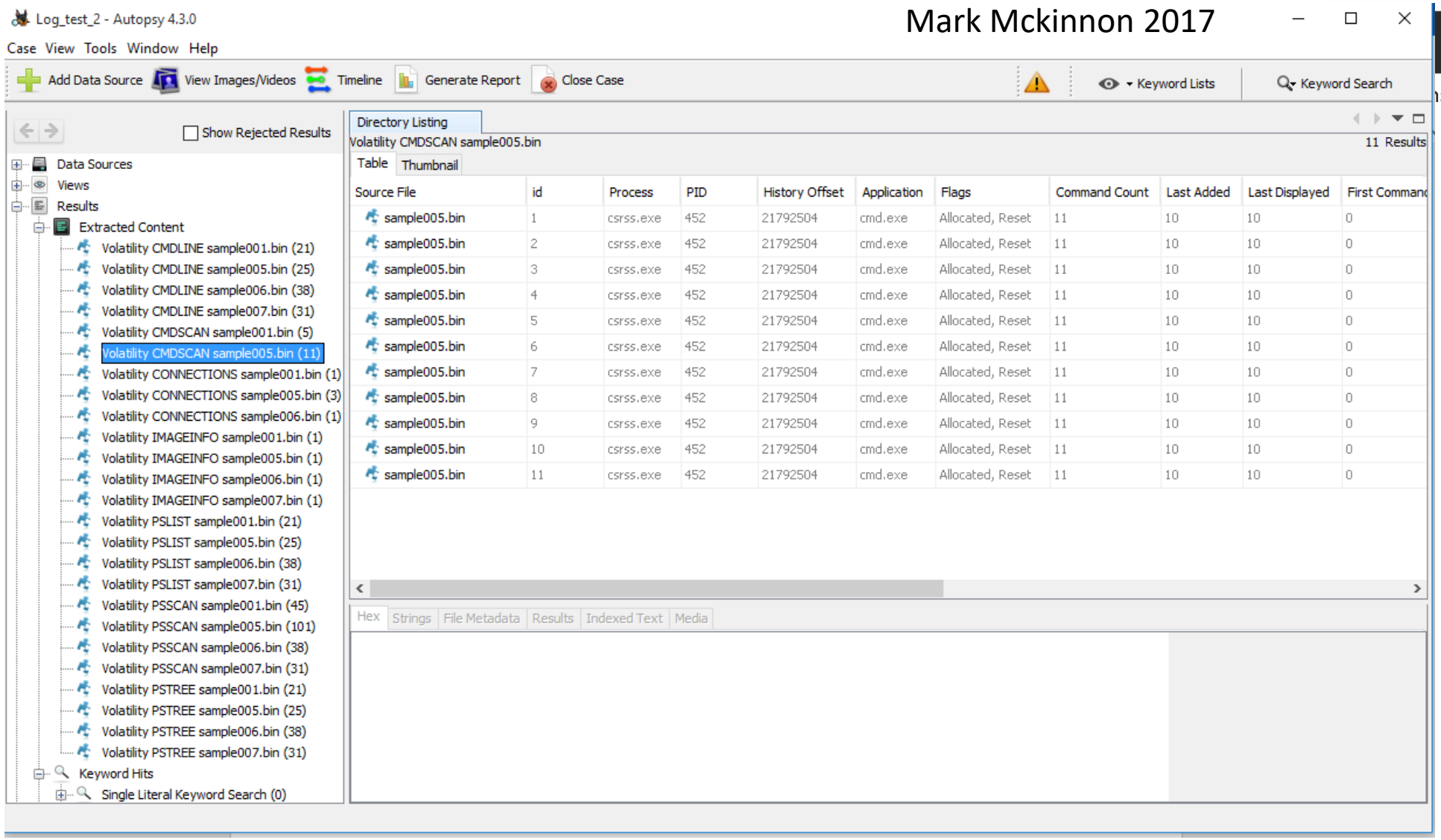


# Arbeitsspeicher-Forensik

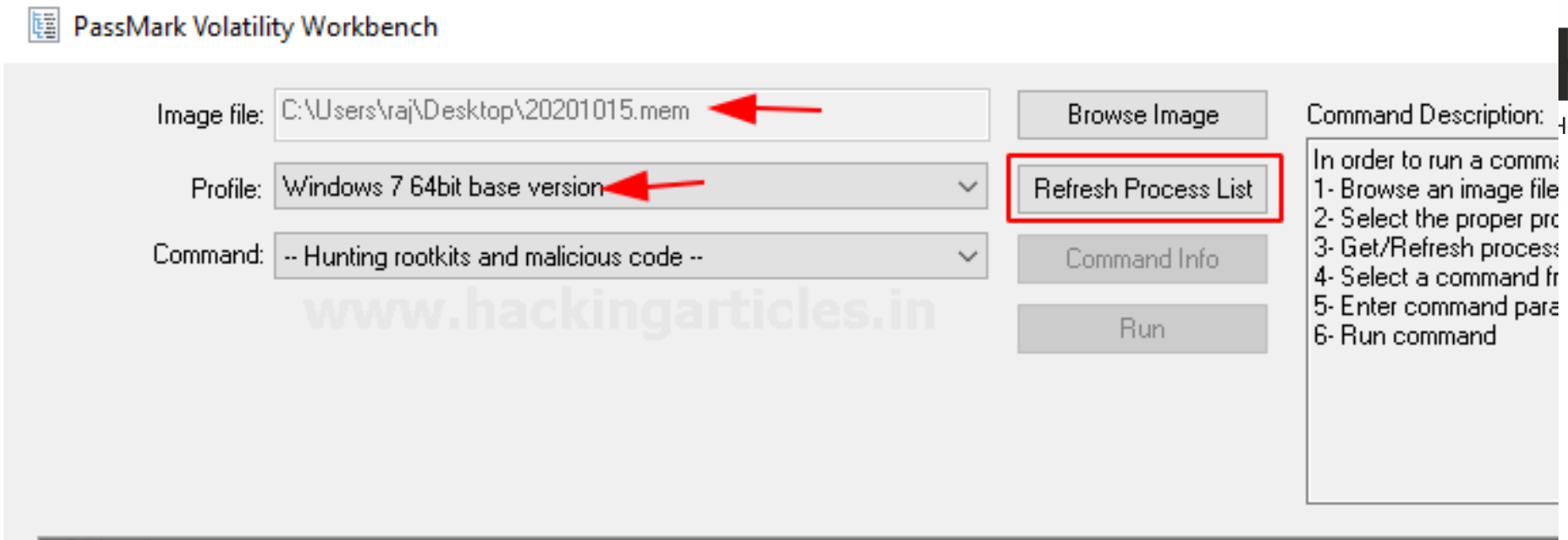


# Arbeitsspeicher-Forensik

Mark Mckinnon 2017

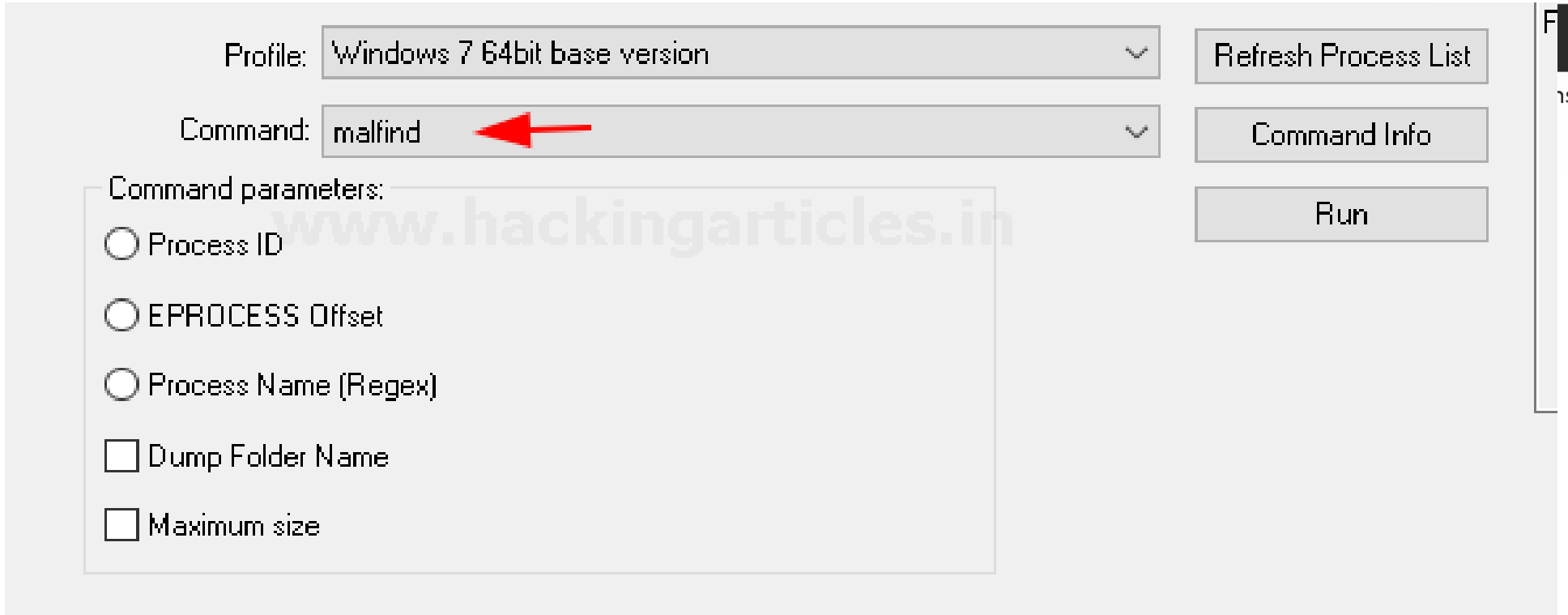


# Arbeitsspeicher-Forensik




```
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




```
0x0fc6003f 00                   DB 0x0

Process: windows-meterp Pid: 4572 Address: 0x20000
Vad Tag: VadS 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   ......`..1.d.P0.
0x00020010  52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c   R..R..r(..J&1..<
0x00020020  61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52   a|.,........RW.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




```
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

HOST
Hochschule Stralsund

## 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
```

SANS 2019

# Arbeitsspeicher-Forensik

**truecryptsummery**

**truecryptmaster**

**truecryptpassphrase**

# Arbeitsspeicher-Forensik


volatility-labs.blogspot.com

```
$ python vol.py -f WIN-QBTA4959AO9.raw --profile=Win2012SP0x64 truecryptsummary
Volatility Foundation Volatility Framework 2.3.1 (T)

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\$Mft 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)
Host Length: 7743995904 (bytes)
Encryption Algorithm: SERPENT
Mode: XTS
Master Key
0xfffffa8018eb71a8 bbe1dc7a8e87e9f1f7eef37e6bb30a25   ...z.......~k..%
0xfffffa8018eb71b8 90b8948fefee425e5105054e3258b1a7   ......B^Q..N2X..
0xfffffa8018eb71c8 a76c5e96d67892335008a8c60d09fb69   .l^..x.3P......i
0xfffffa8018eb71d8 efb0b5fc759d44ec8c057fbc94ec3cc9   ....u.D.......<.
Dumped 64 bytes to ./0xfffffa8018eb71a8_master.key
```

volatility-labs.blogspot.com

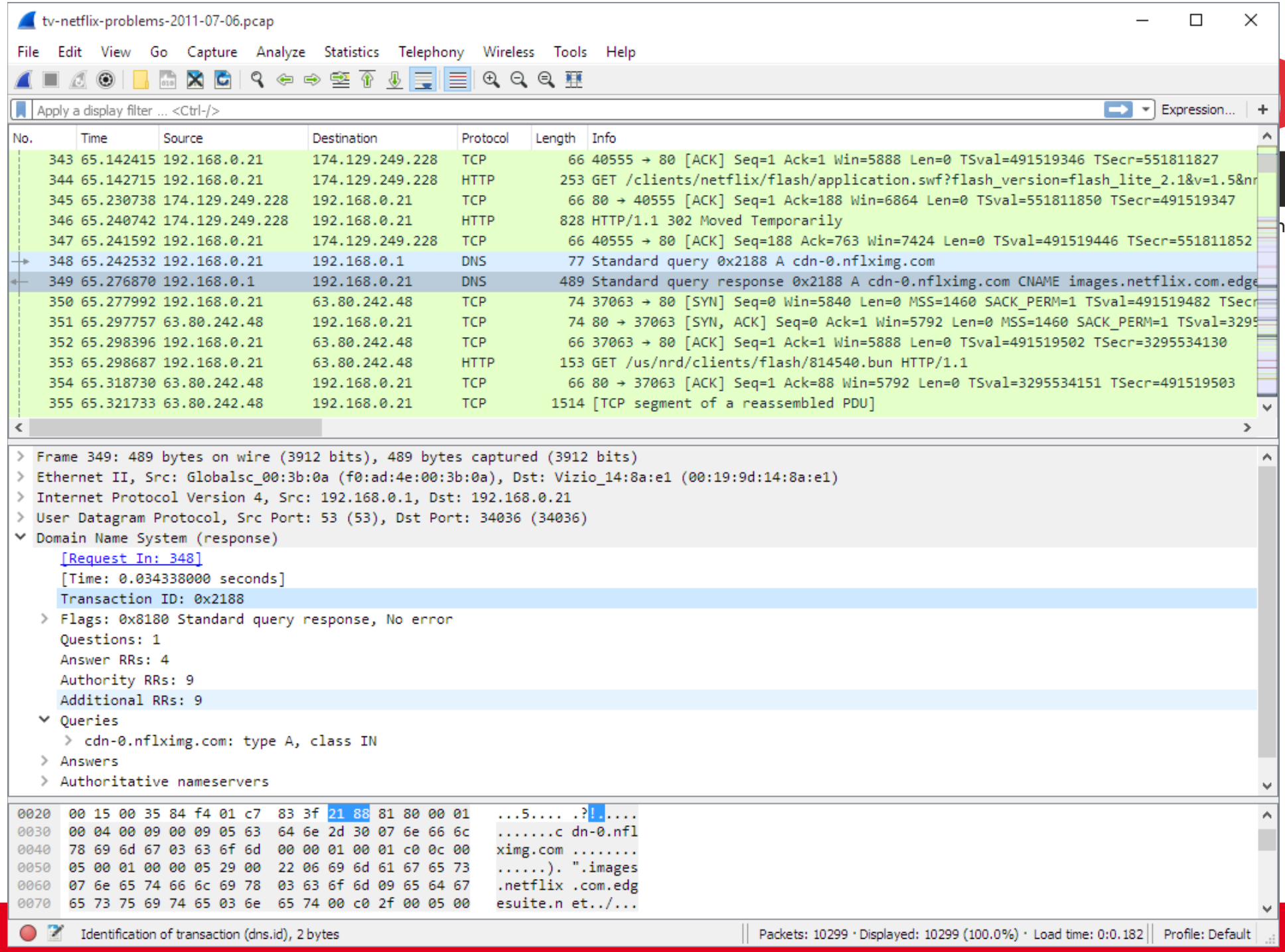
# Forensische Netzwerk-Informationen

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

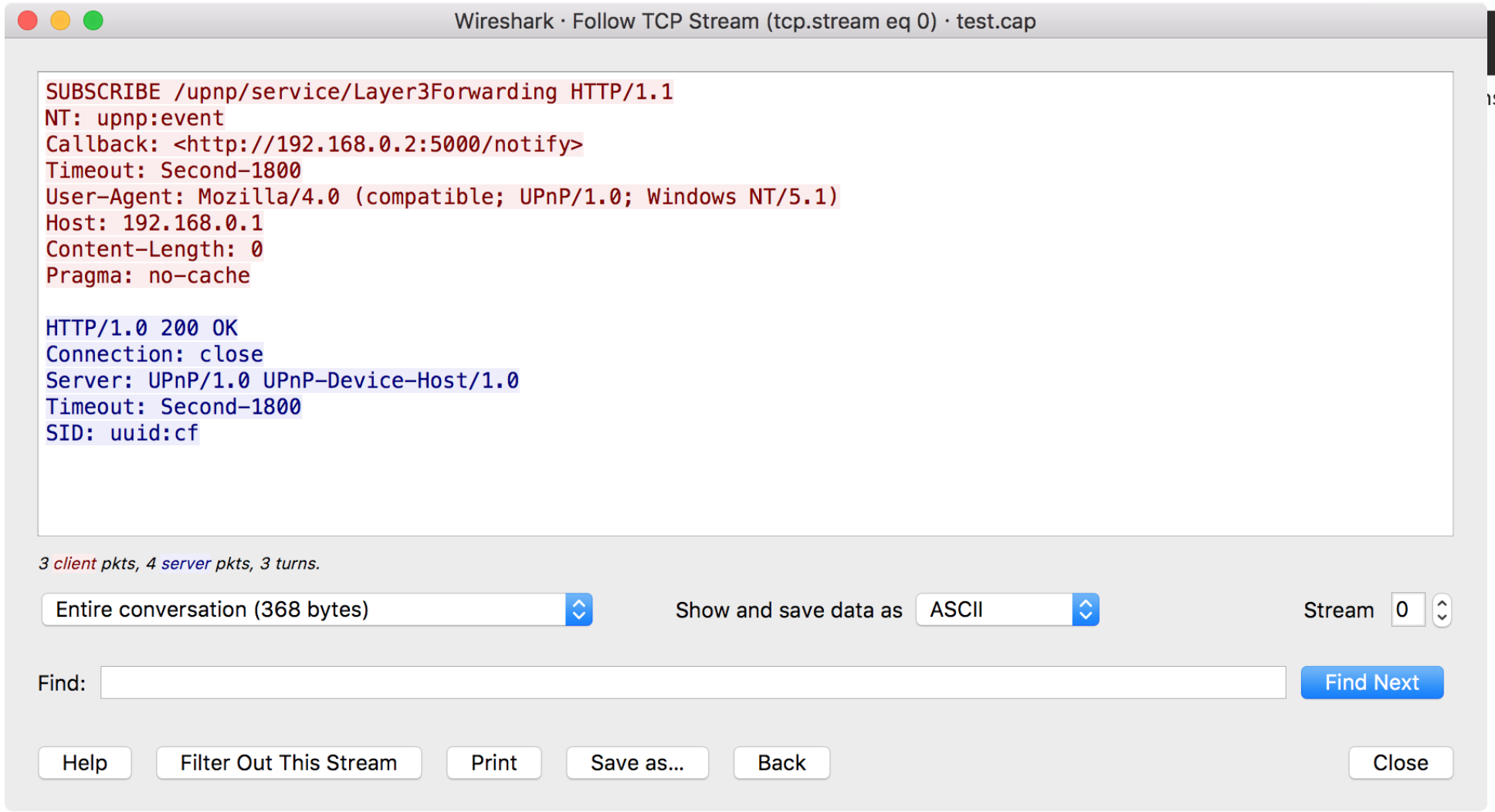
# Netzwerk-Sniffing

HOST
Hochschule Stralsund

# 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&nr
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.nflximg.com
349 65.276870 192.168.0.1 192.168.0.21 DNS 489 Standard query response 0x2188 A cdn-0.nflximg.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.nflximg.com: type A, class IN
Answers
Authoritative nameservers
0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... .?!.....
0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c .......c dn-0.nfl
0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com ........
0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73 ......). ".images
0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg
0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...
Identification of transaction (dns.id), 2 bytes
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182
Profile: Default

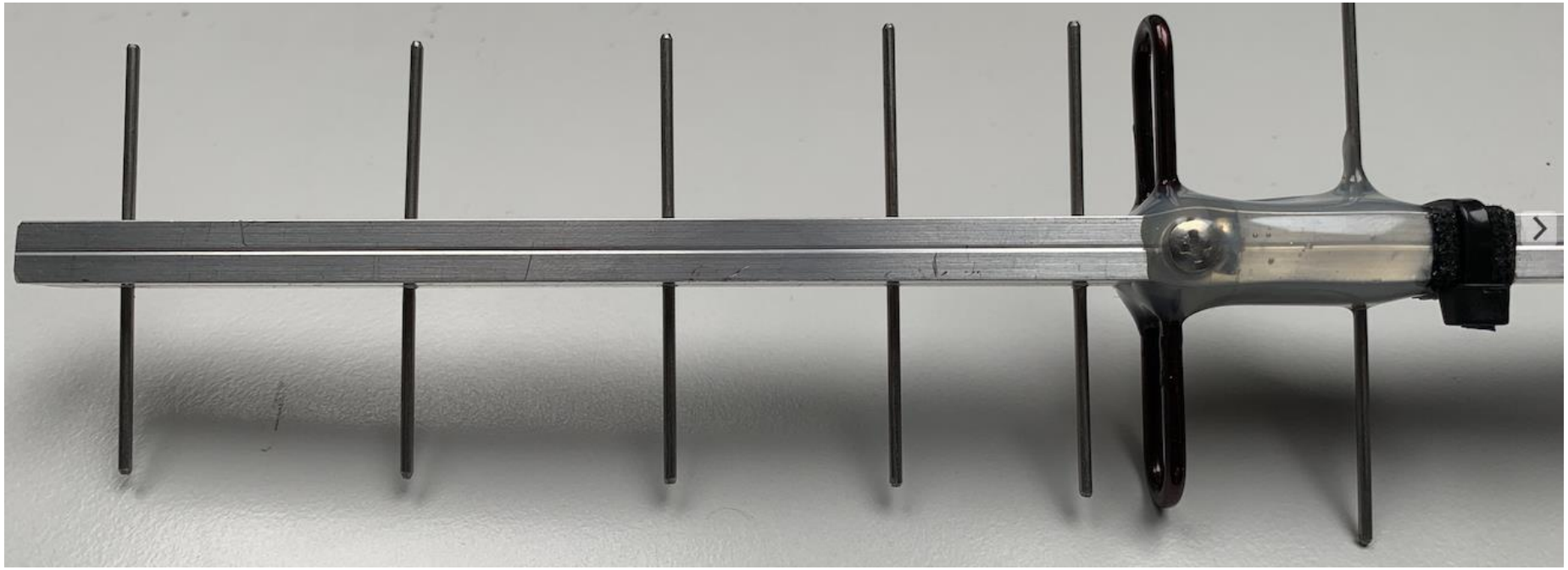
# Netzwerk-Sniffing



# WLAN-Infos


Wifi Analyzer
VIEW
SETTINGS
dlink_RM4*
dlink_Rm7
ITREE450
dlink_Rm3
Verizon-890L-3025
AGECW*
O'Brian's iPhone
-30
-40
-50
-60
-70
-80
-90
Signal Strength [dBm]
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Wifi Channels

# WLAN-Infos



Rittelmeier 2021

# WLAN-Infos

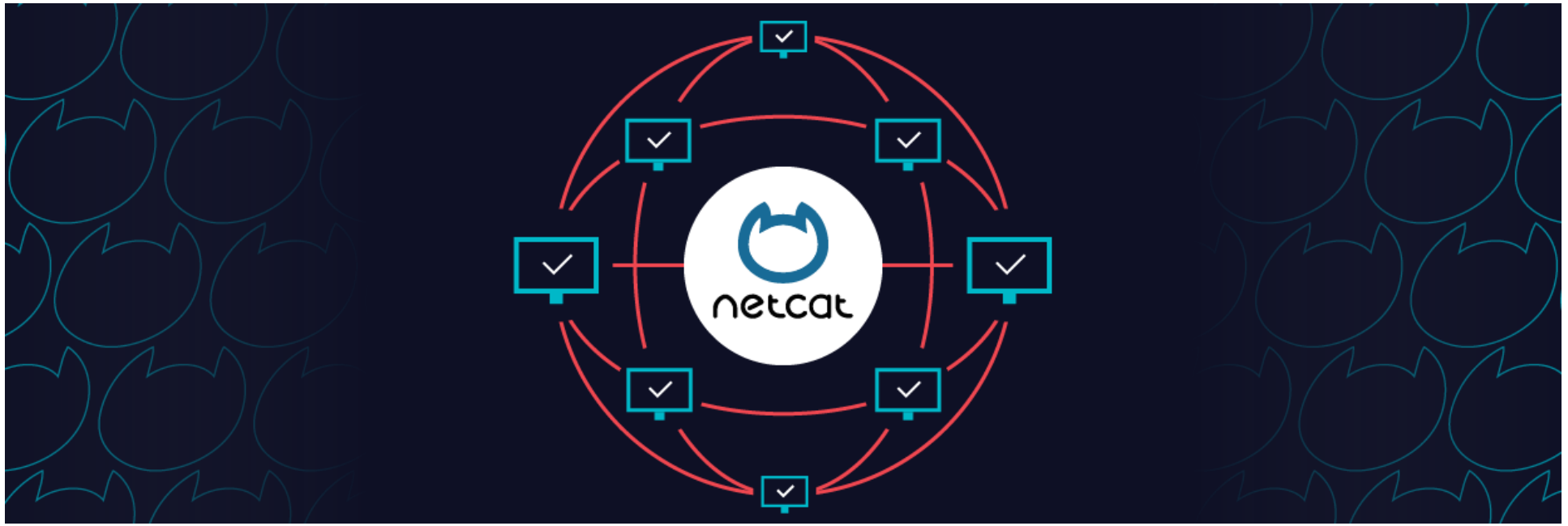

Network List (Autofit)
Name T W Ch Packts Flags IP Range Size
! pwn A Y 006 436 0.0.0.0 1k
Info
Ntwrks
1
Pckets
436
Cryptd
4
Weak
0
Noise
0
Discrd
0
Pkts/s
4
orinoc
Ch: 8
Elapsd
00:02:52
Status
Connected to Kismet server version 2004.10.R1 build 20041025233409 on localhost:2501
Battery: AC 100% 596523h14m8s

Android
Debug
Bridge

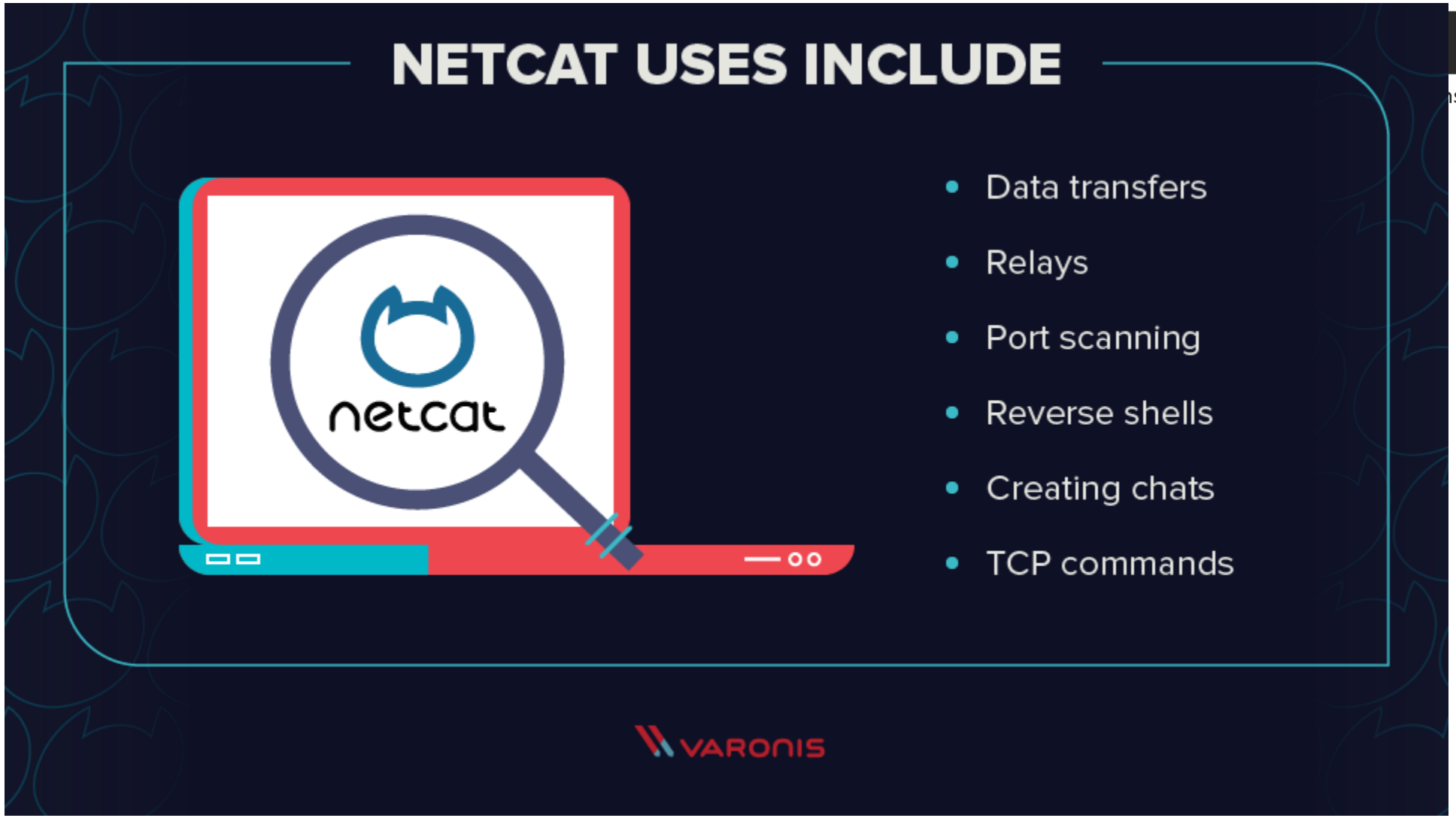
Hochschule Stralsund

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

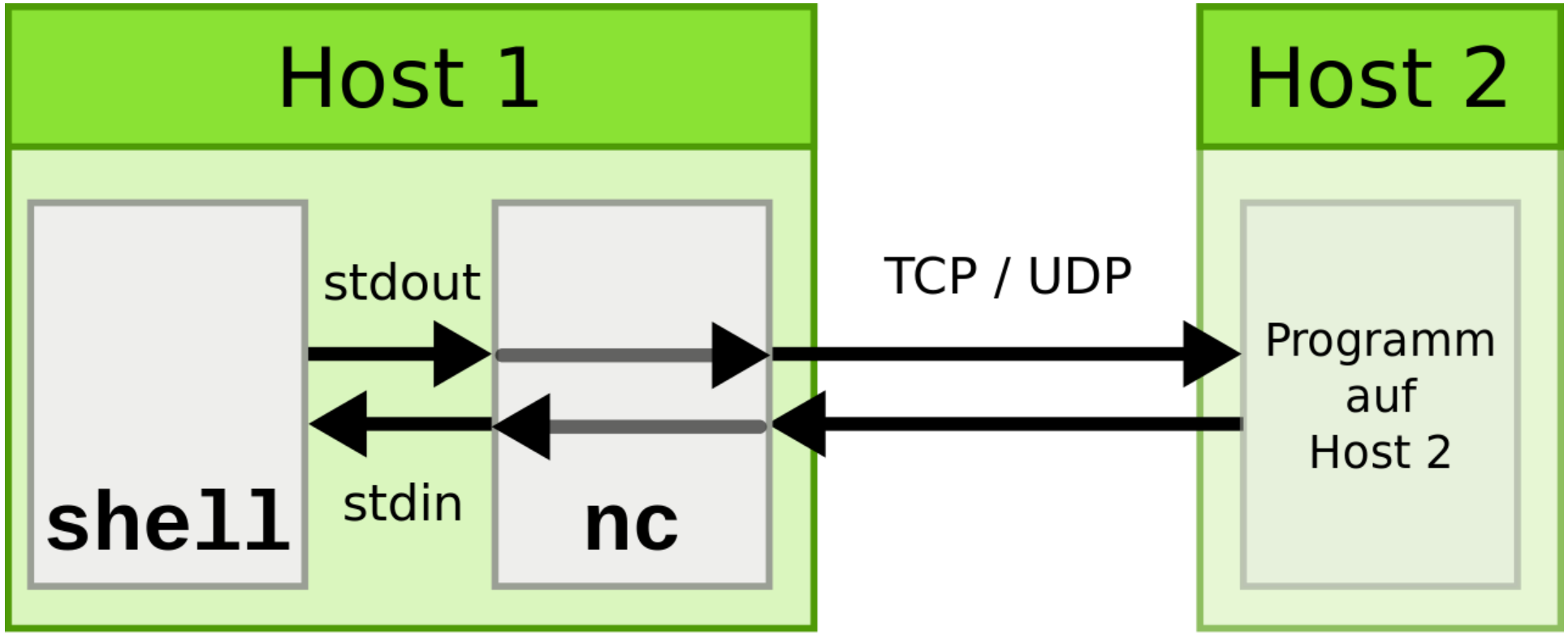
# Netcat



# Netcat


NETCAT USES INCLUDE
netcat
Data transfers
Relays
Port scanning
Reverse shells
Creating chats
TCP commands
VARONIS

# Netcat


Host 1
Host 2
stdout
stdin
TCP / UDP
shell
nc
Programm
auf
Host 2

# Netcat

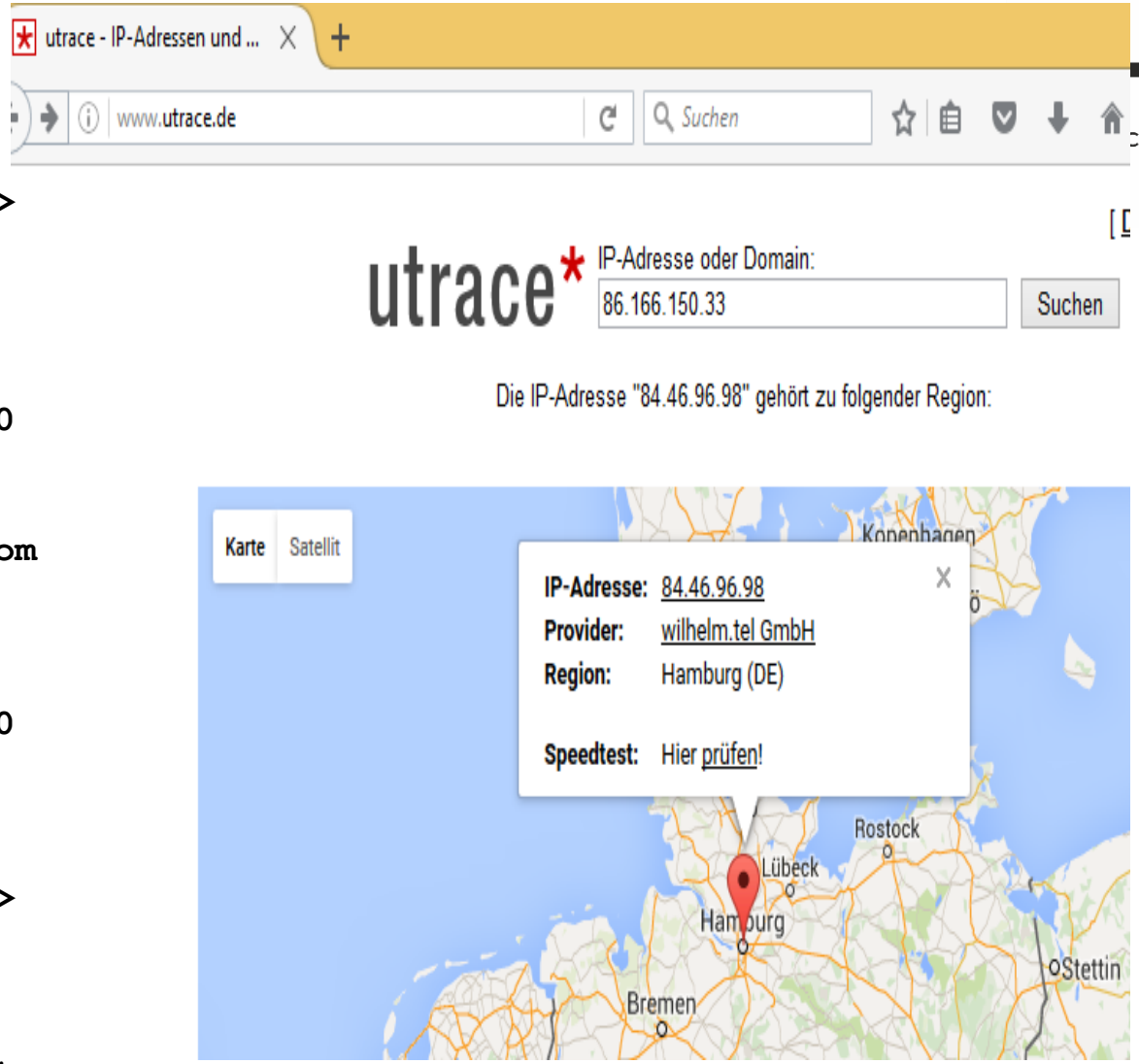
Hochschule Stralsund

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

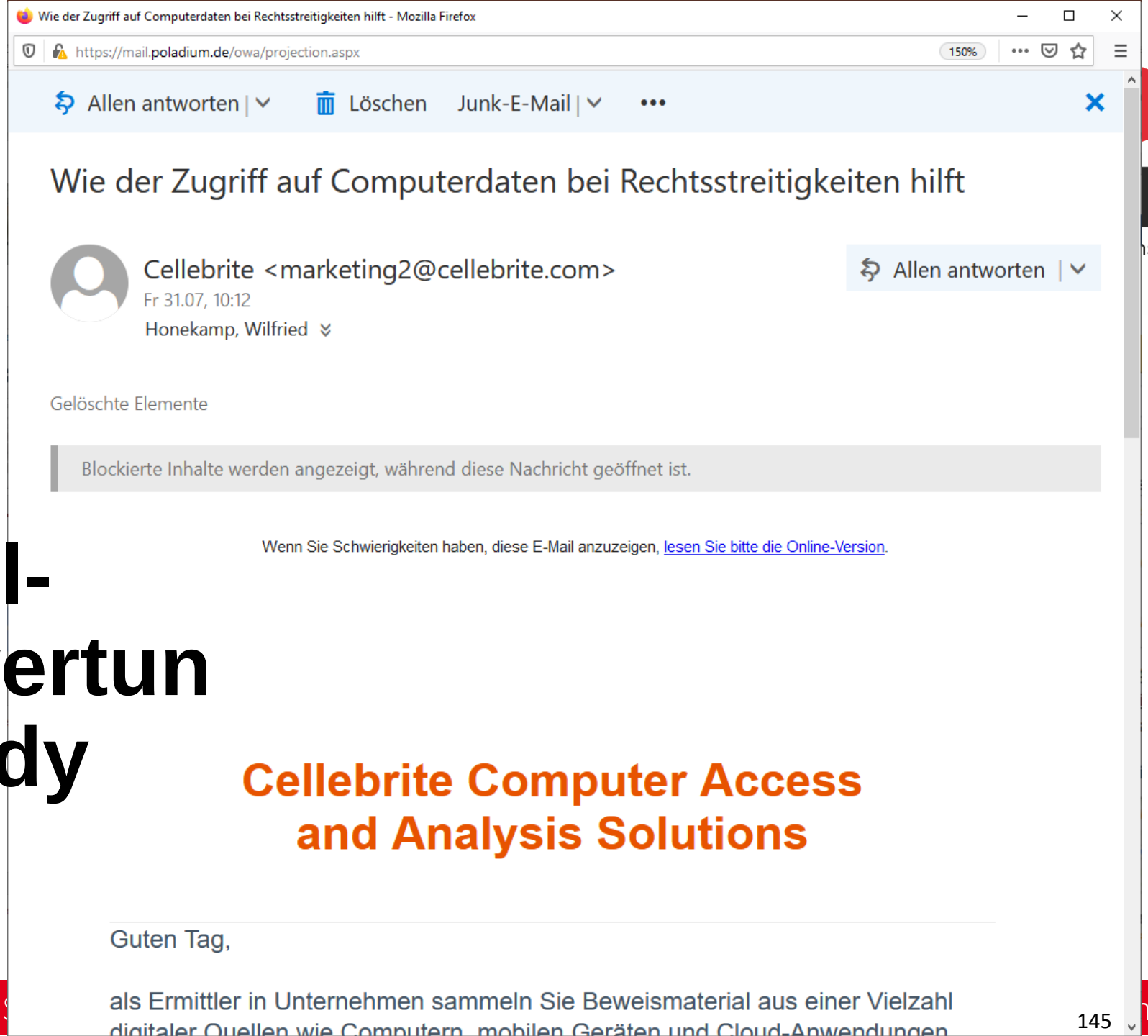
```
dd if=/dev/sdb conv=sync,noerror | nc 10.10.0.253 80
```

# E-Mail-Auswertung

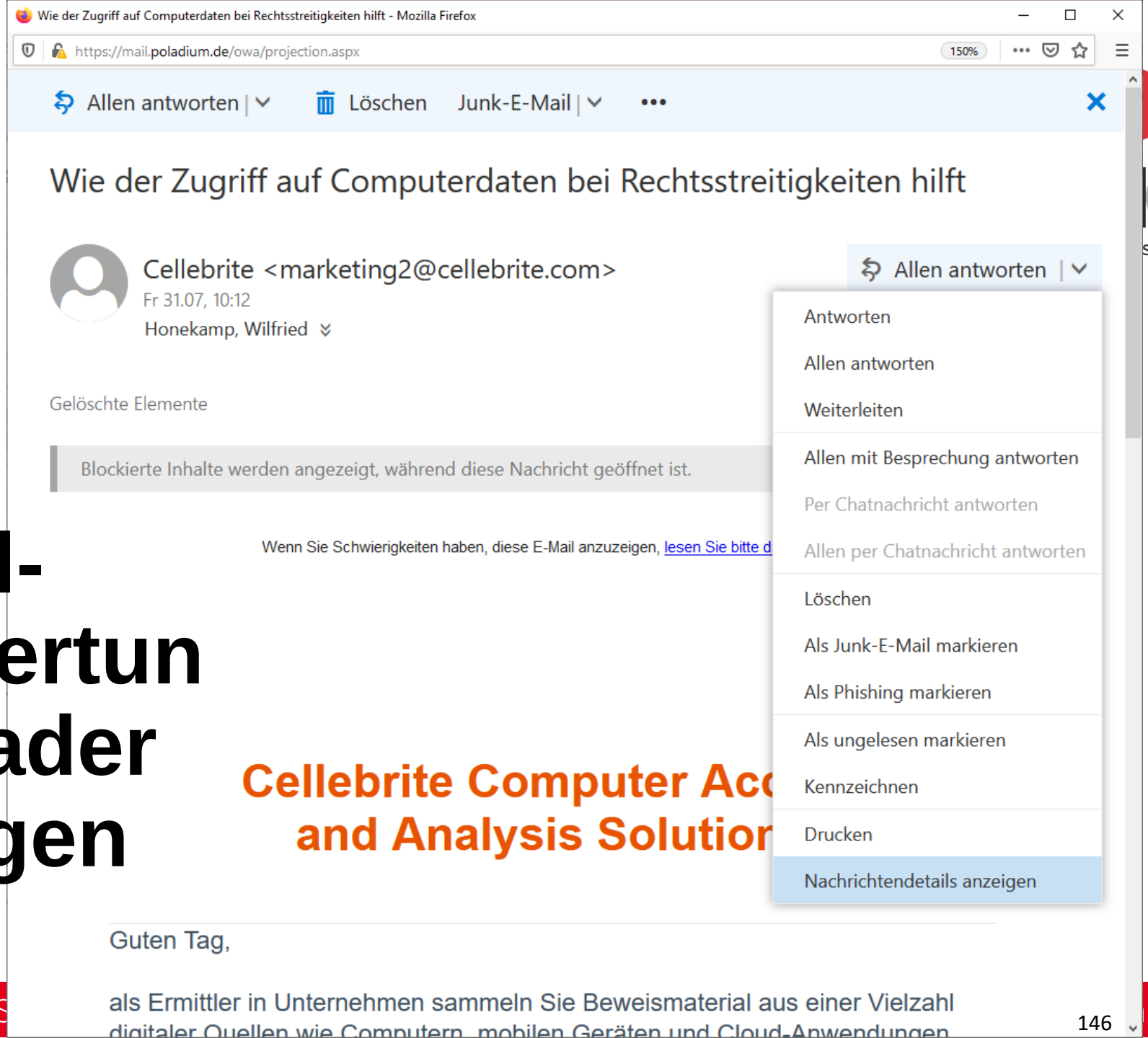
```
Return-Path:
<sisxxx1957@iconsystemplus.com>
Received: from mailin12.aul.t-
online.de (mailin12.aul.t-
online.de [172.20.26.48])
by mhead406 with LMTP;
Sun, 19 Apr 2009 14:02:10 +0200
X-Sieve: CMU Sieve 2.3
Received: from host86-166-150-
33.range86-166.btcentralplus.com
([86.166.150.33]) by
mailin12.aul.t-online.de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



# E-Mail-Auswertung: Body



# E-Mail-Auswertung: Header anzeigen



# E-Mail-Auswertung: Header anzeigen

**https://hilfe.uni-paderborn.de/Mail_Header_anzeigen**

**oder Google**

**https://www.google.com/search?q=e-mail-header+anzigen**

**oder Ermittlungshilfe im Intrapol**

# E-Mail-Forensik


```
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 Skrubenek"
<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
X-TOI-MSGID: 4499eec6-bdb3-4912-82a0-
24e3dedaedf0
```

# 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 Skrubenek"
<sisxxx1957@iconsystemplus.com>
Mime-Version: 1.0
Content-Type: text/html; charset=iso-
8859-1
Content-Transfer-Encoding: 7bit
```

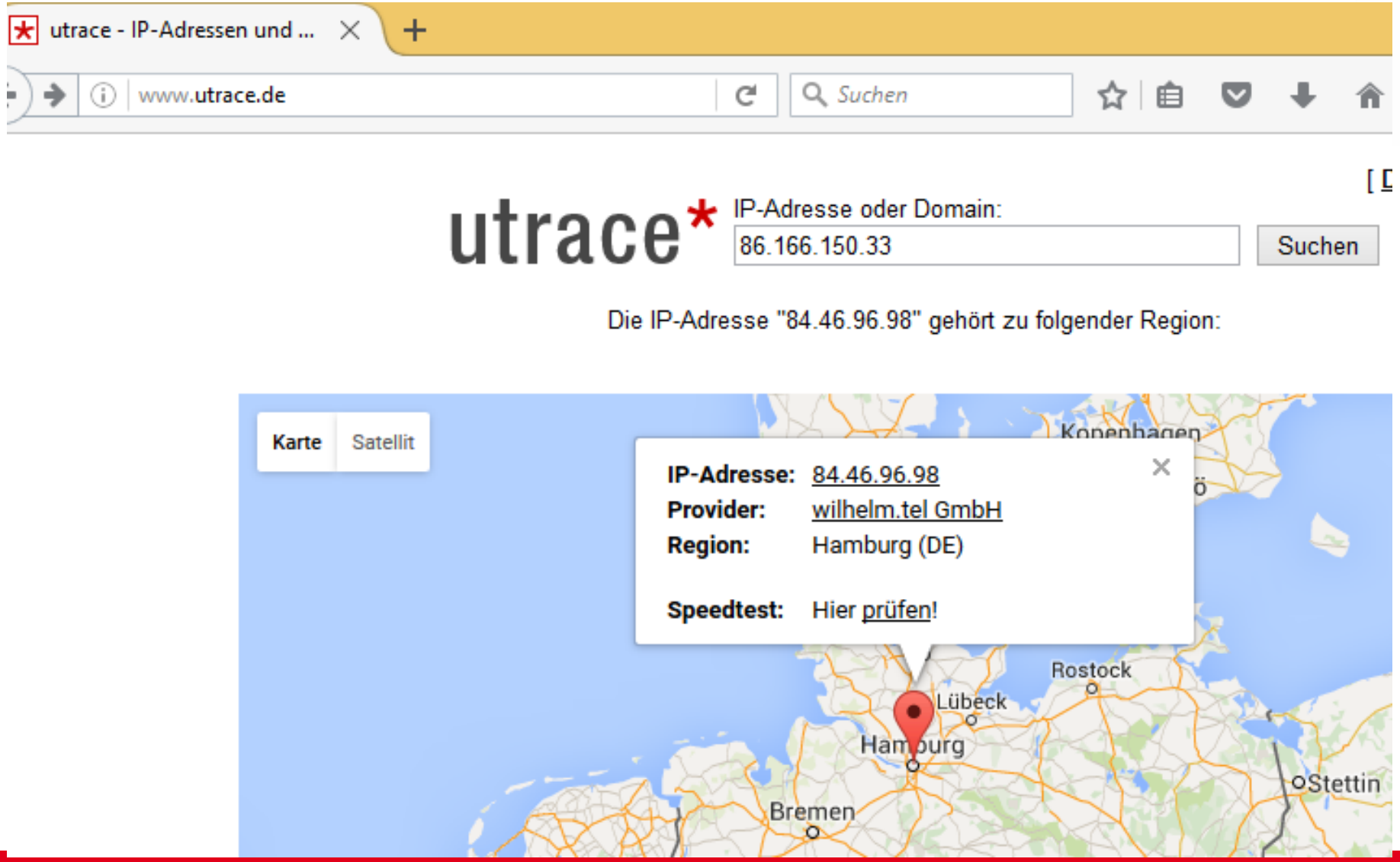
# E-Mail-Forensik

```
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 Skrubenek"
<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 Skrubenek"
<sisxxx1957@iconsystemplus.com>
Mime-Version: 1.0
Content-Type: text/html; charset=iso-
8859-1
Content-Transfer-Encoding: 7bit
```

# E-Mail-Forensik



# Wie arbeiten die Strafverfolgungsbehörden?

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

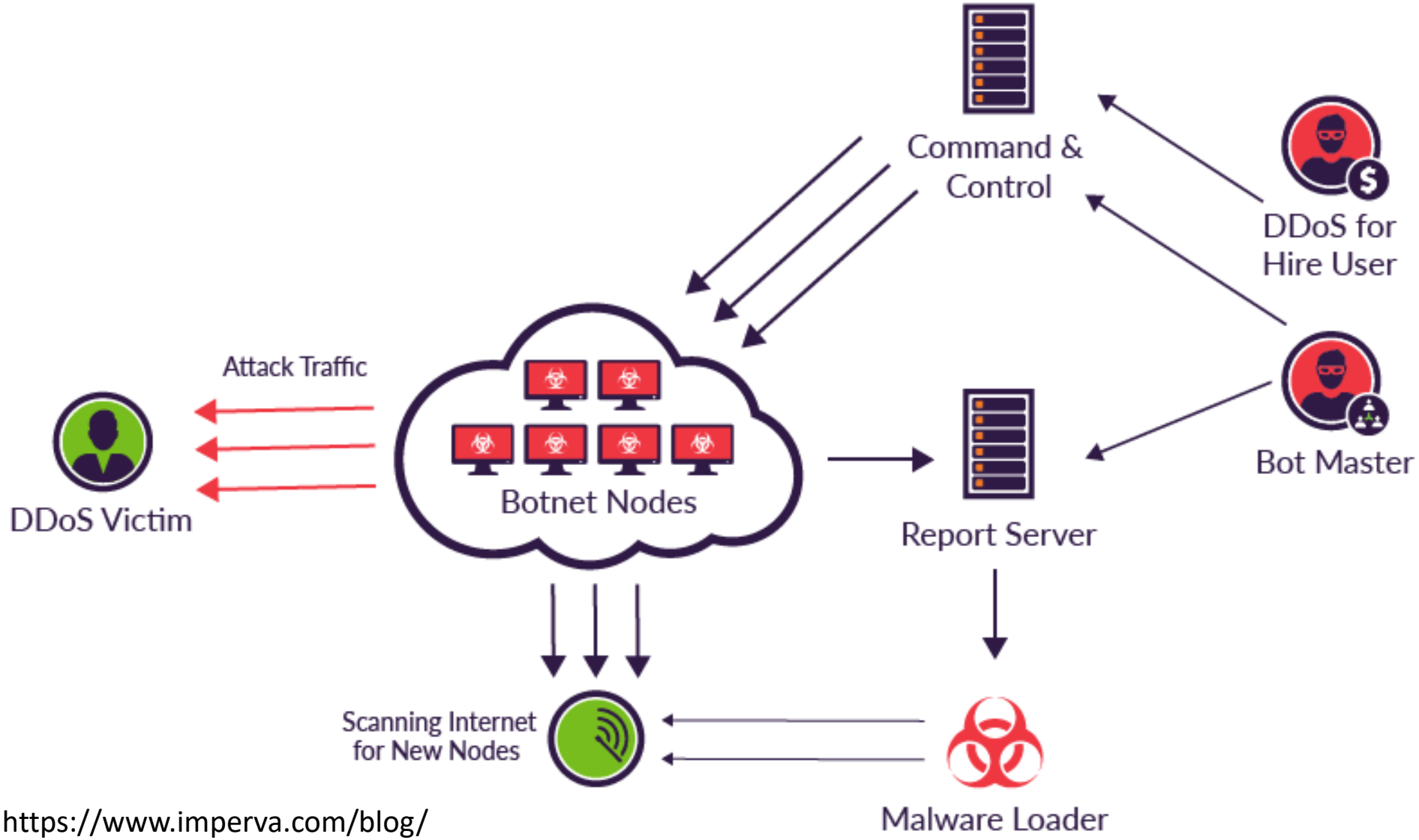
# IoT: Internet of Things

**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

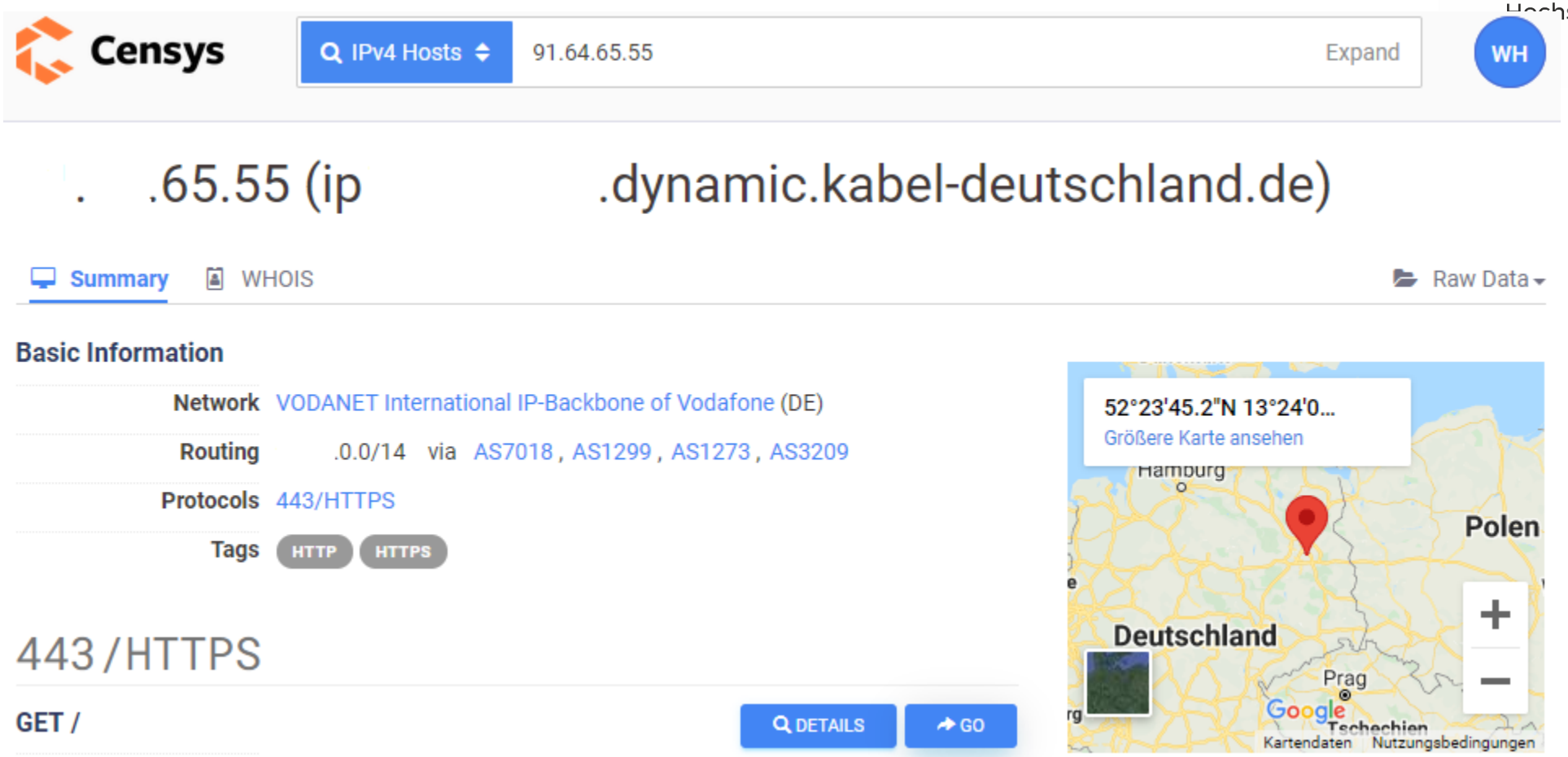
# IoT DDOS mit Mirai

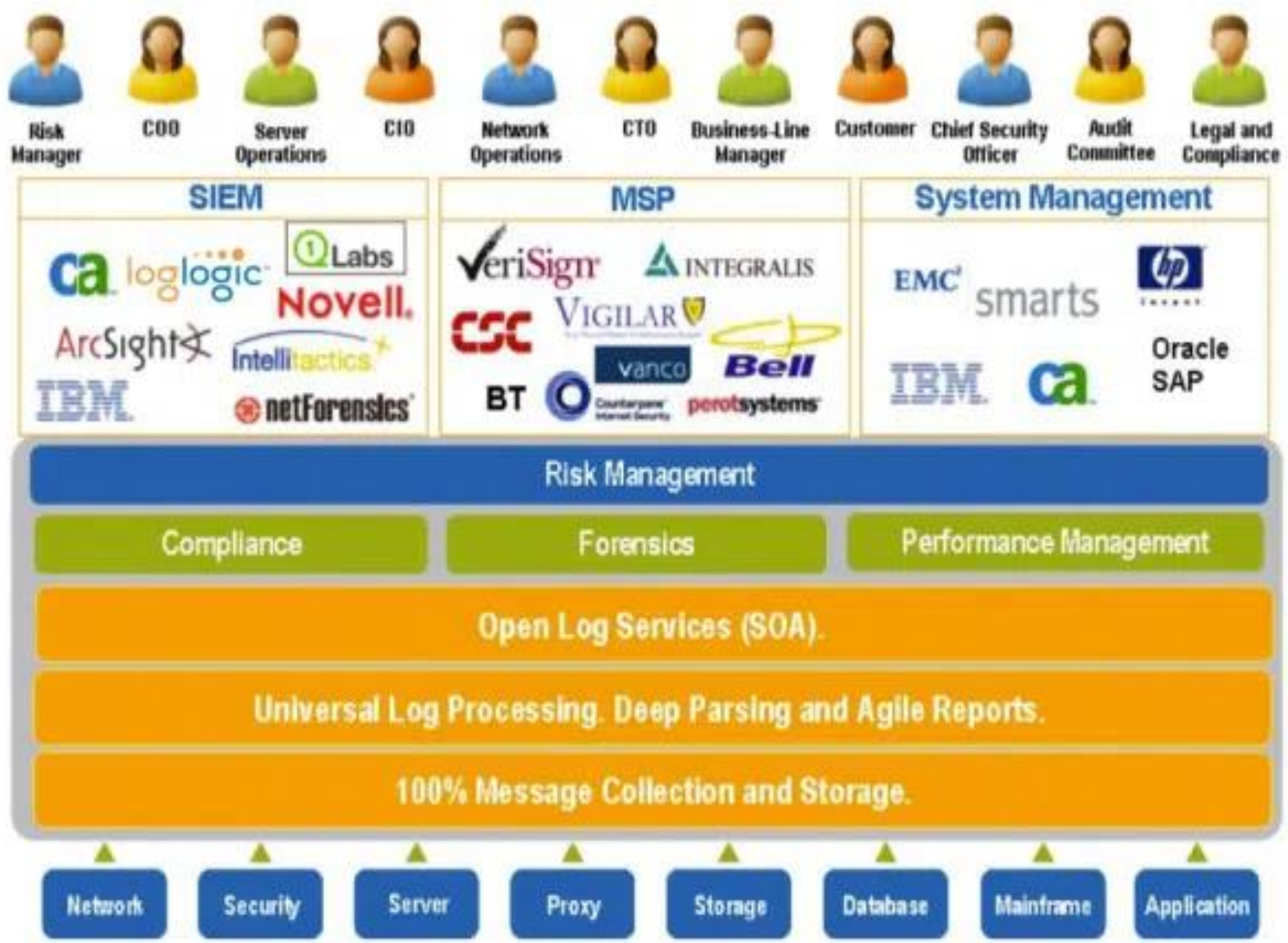


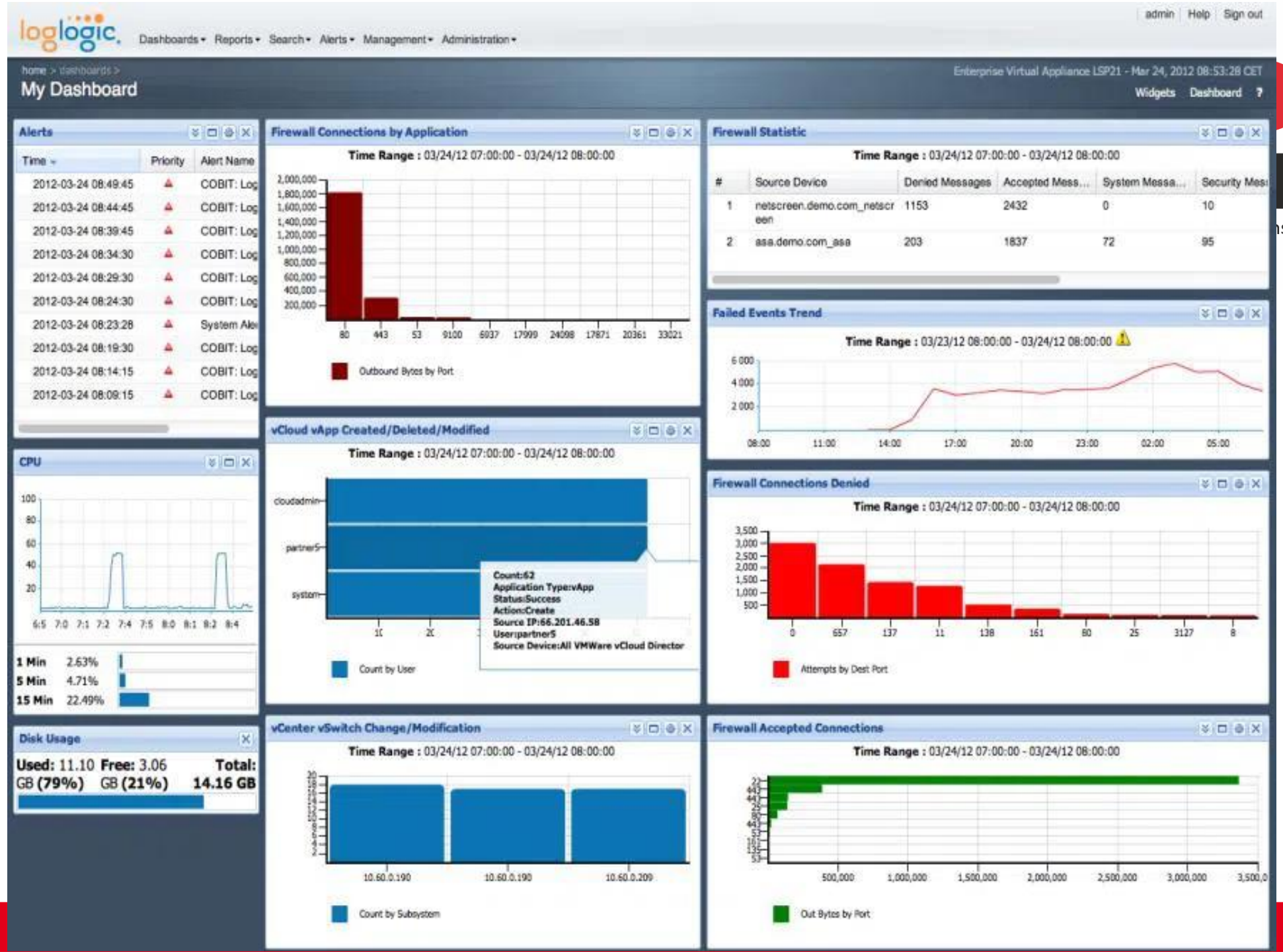

https://www.imperva.com/blog/
how-to-identify-a-mirai-style-ddos-attack/

# IoT-Suche mit Shodan

# IOT-Suchmaschinen




Risk Manager
COO
Server Operations
CIO
Network Operations
CTO
Business-Line Manager
Customer
Chief Security Officer
Audit Committee
Legal and Compliance
SIEM
ca
loglogic
Labs
Novell
ArcSight
Intellitactics
IBM
netForensics
MSP
VeriSign
INTEGRALIS
CSC
VIGILAR
vanco
Bell
BT
perotsystems
System Management
EMC
smarts
hp
IBM
ca
Oracle
SAP
Risk Management
Compliance
Forensics
Performance Management
Open Log Services (SOA).
Universal Log Processing. Deep Parsing and Agile Reports.
100% Message Collection and Storage.
Network
Security
Server
Proxy
Storage
Database
Mainframe
Application


loglogic
Dashboards
Reports
Search
Alerts
Management
Administration
admin
Help
Sign out
home > dashboards >
My Dashboard
Enterprise Virtual Appliance LSP21 - Mar 24, 2012 08:53:28 CET
Widgets
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 Ale
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 Connections by Application
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
2,000,000
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
80
443
53
9100
6037
17999
24098
17871
20361
33021
Outbound Bytes by Port
Firewall Statistic
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
# Source Device Denied Messages Accepted Mess... System Messa... Security Mes
1 netscreen.demo.com_netscreen 1153 2432 0 10
2 asa.demo.com_asa 203 1837 72 95
Failed Events Trend
Time Range : 03/23/12 08:00:00 - 03/24/12 08:00:00
6 000
4 000
2 000
08:00
11:00
14:00
17:00
20:00
23:00
02:00
05:00
vCloud vApp Created/Deleted/Modified
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
cloudadmin
partnerS
system
Count:62
Application Type:vApp
Status:Success
Action:Create
Source IP:66.201.46.58
User:partnerS
Source Device:All VMWare vCloud Director
Count by User
CPU
100
80
60
40
20
6:5 7:0 7:1 7:2 7:4 7:5 8:0 8:1 8:2 8:4
1 Min 2.63%
5 Min 4.71%
15 Min 22.49%
Firewall Connections Denied
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
3,500
3,000
2,500
2,000
1,500
1,000
500
0
657
137
11
138
161
80
25
3127
8
Attempts by Dest Port
Disk Usage
Used: 11.10 GB (79%)
Free: 3.06 GB (21%)
Total: 14.16 GB
vCenter vSwitch Change/Modification
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
10.60.0.190
10.60.0.190
10.60.0.209
Count by Subsystem
Firewall Accepted Connections
Time Range : 03/24/12 07:00:00 - 03/24/12 08:00:00
500,000
1,000,000
1,500,000
2,000,000
2,500,000
3,000,000
Out Bytes by Port

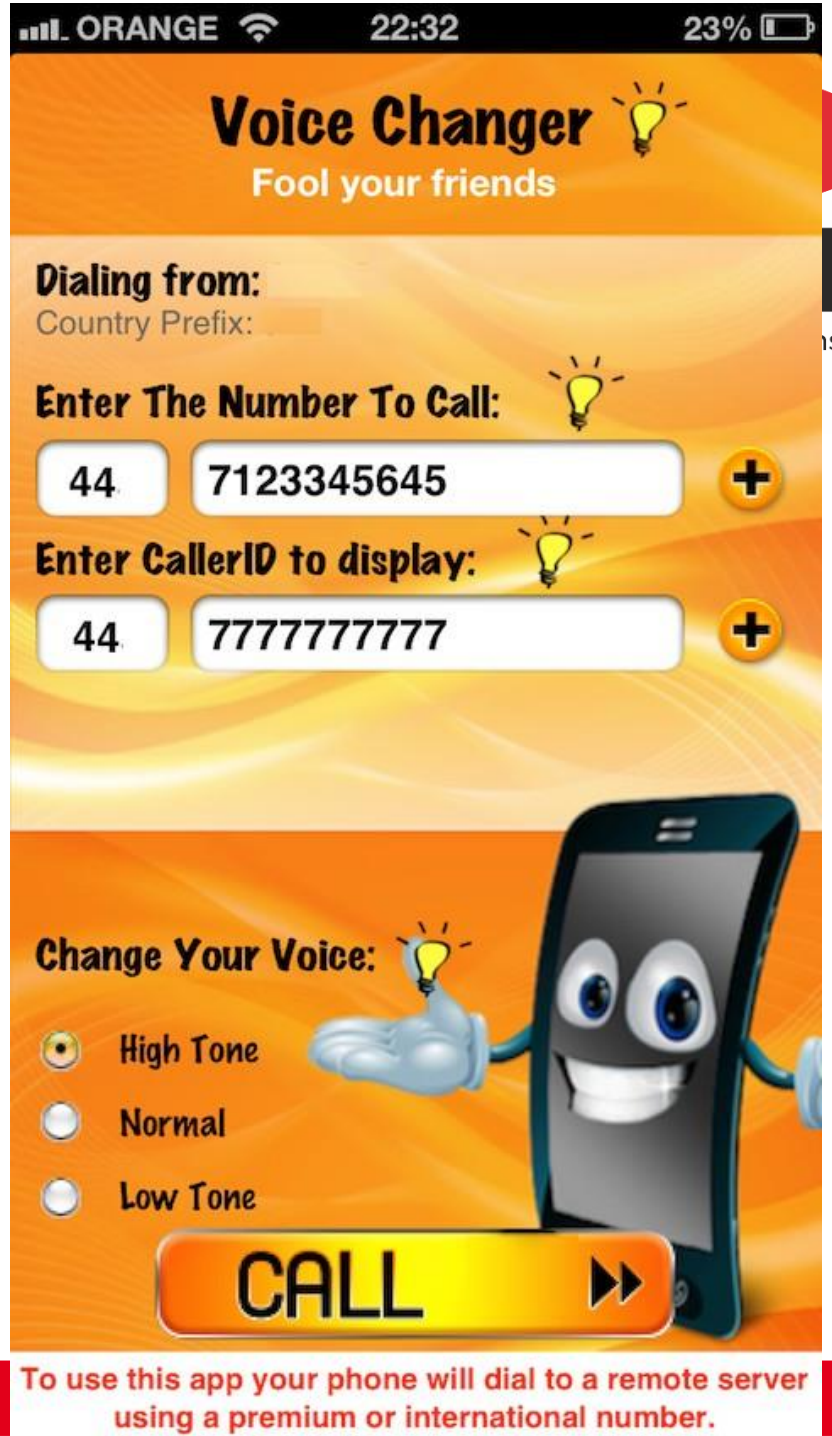
# Angriffserkennung

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

# Spoofing

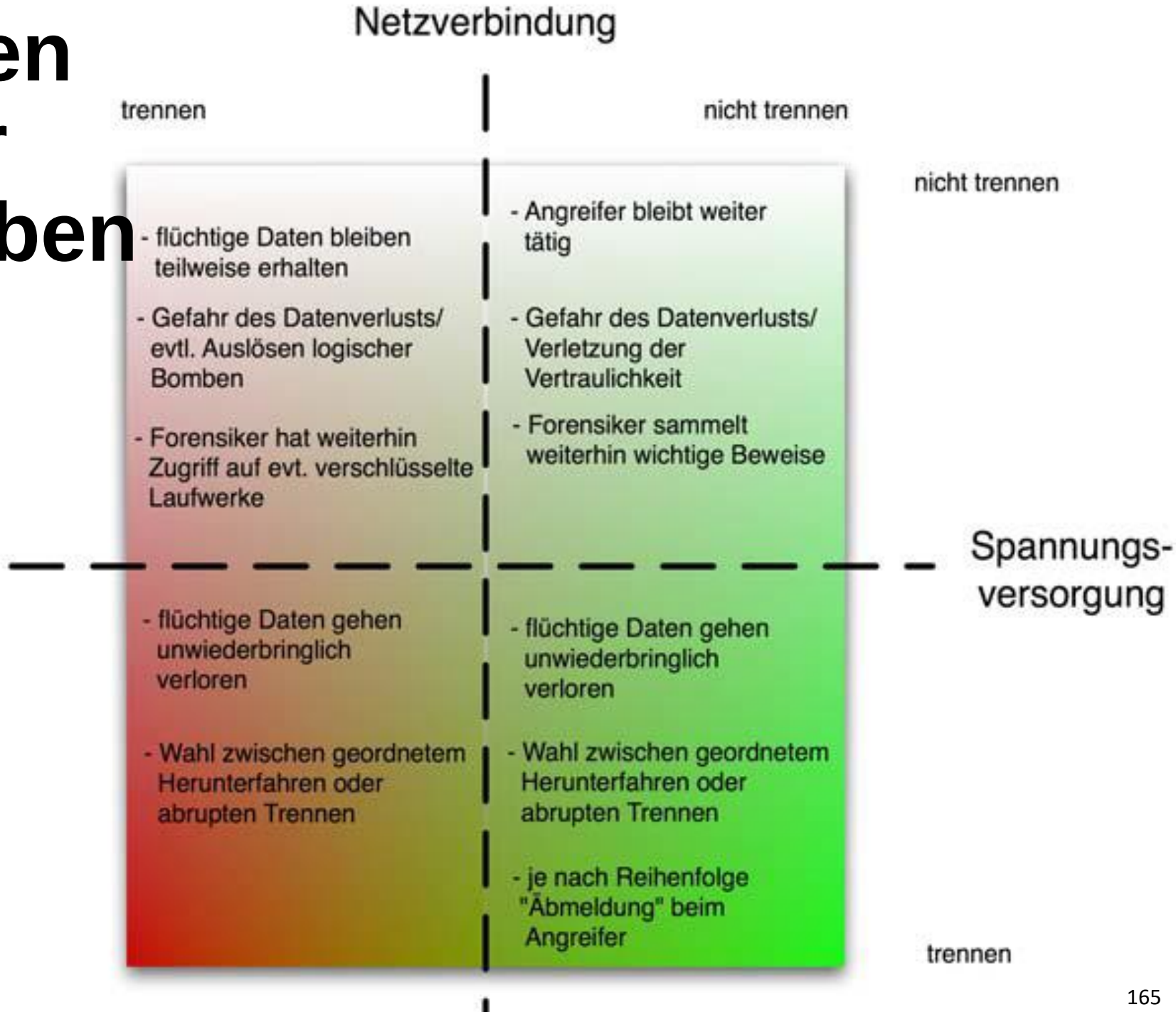
- Arp-Spoofing
- IP-Spoofing
- Call(er)-ID-Spoofing

# Call-ID-Spoofing



# Live-Forensik

# Leben oder Sterben



# Live vs Post Mortem: Flüchtigkeit

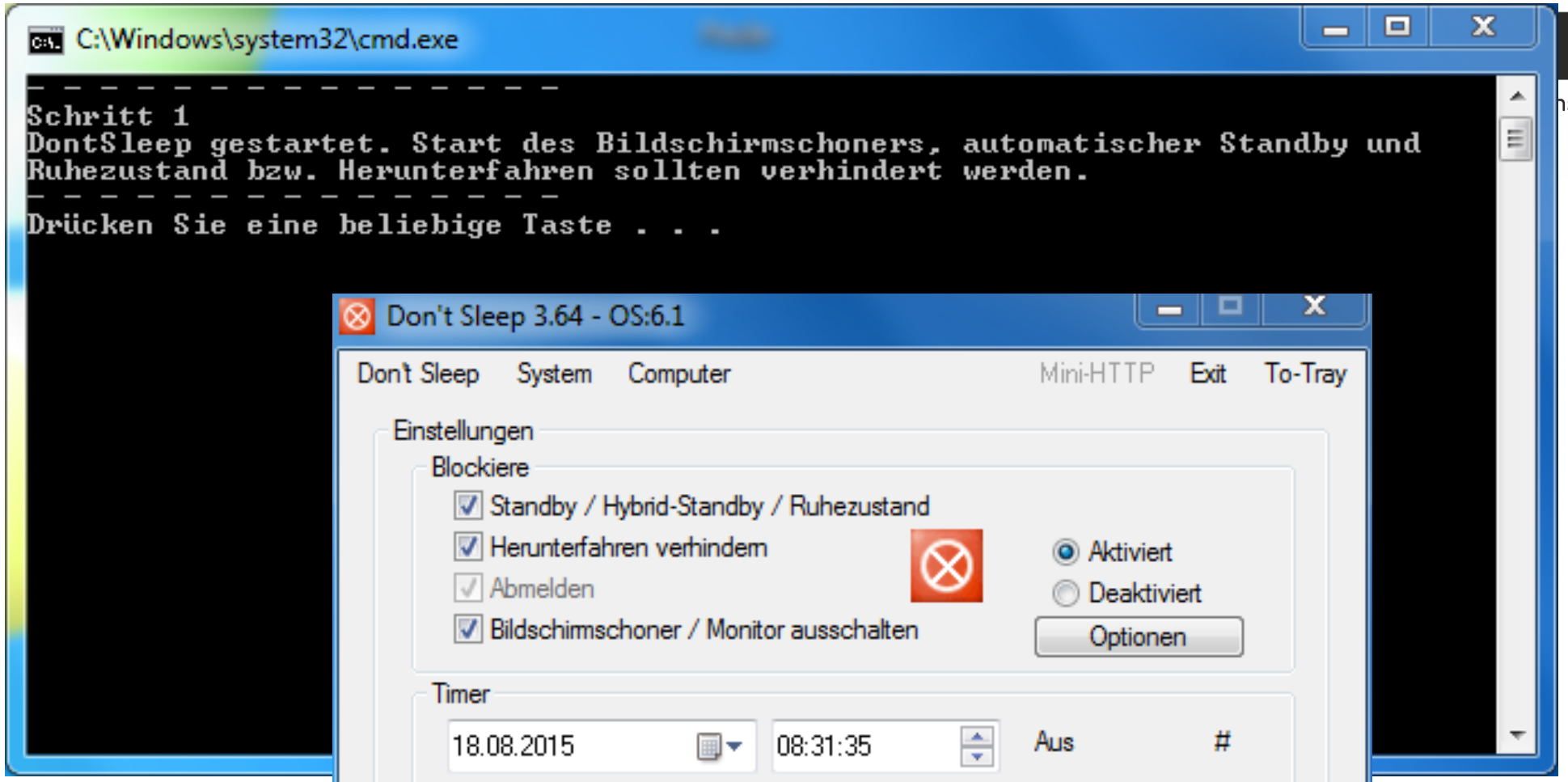
- CPU Register, CPU Cache
- Routing-Tabellen, ARP-Caches, Prozesstabellen, Kernel Statistiken
- Arbeitsspeicherinhalt
- geöffnete, verschlüsselte Dateisysteme
- temporäre Dateisysteme (z.B. Cloudspeicher)
- entfernt geführte Logging- und Monitordaten
- Massenspeicherinhalte
- physische Konfiguration,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

# Live Untersuchung: laufender PC

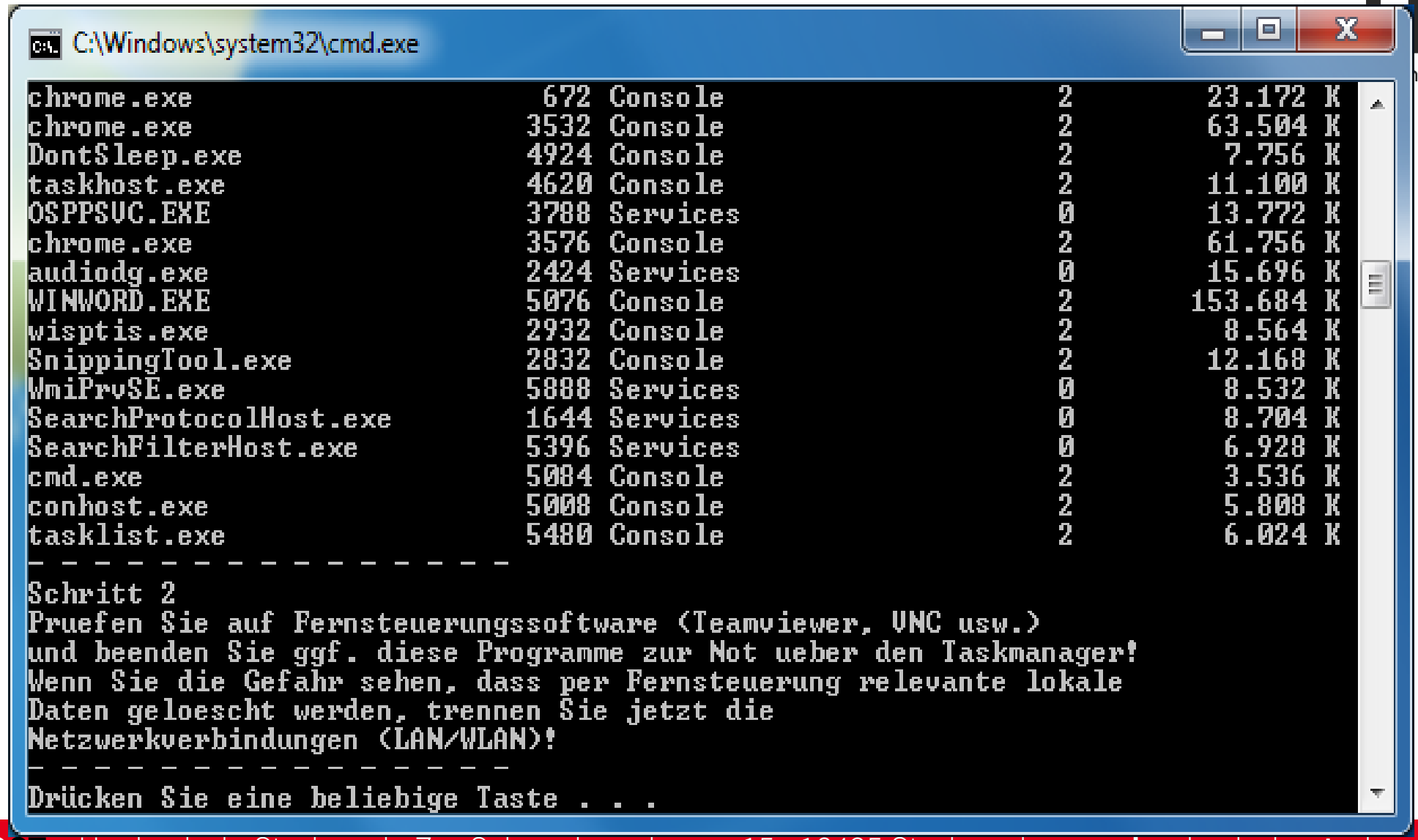
- Routing-Tabellen, ARP-Caches, Prozesstabellen, Kernel Statistiken
- Arbeitsspeicherinhalt
- geöffnete, verschlüsselte Dateisysteme
- temporäre Dateisysteme (z.B. Cloudspeicher)

→ Durchsuchungskonzept

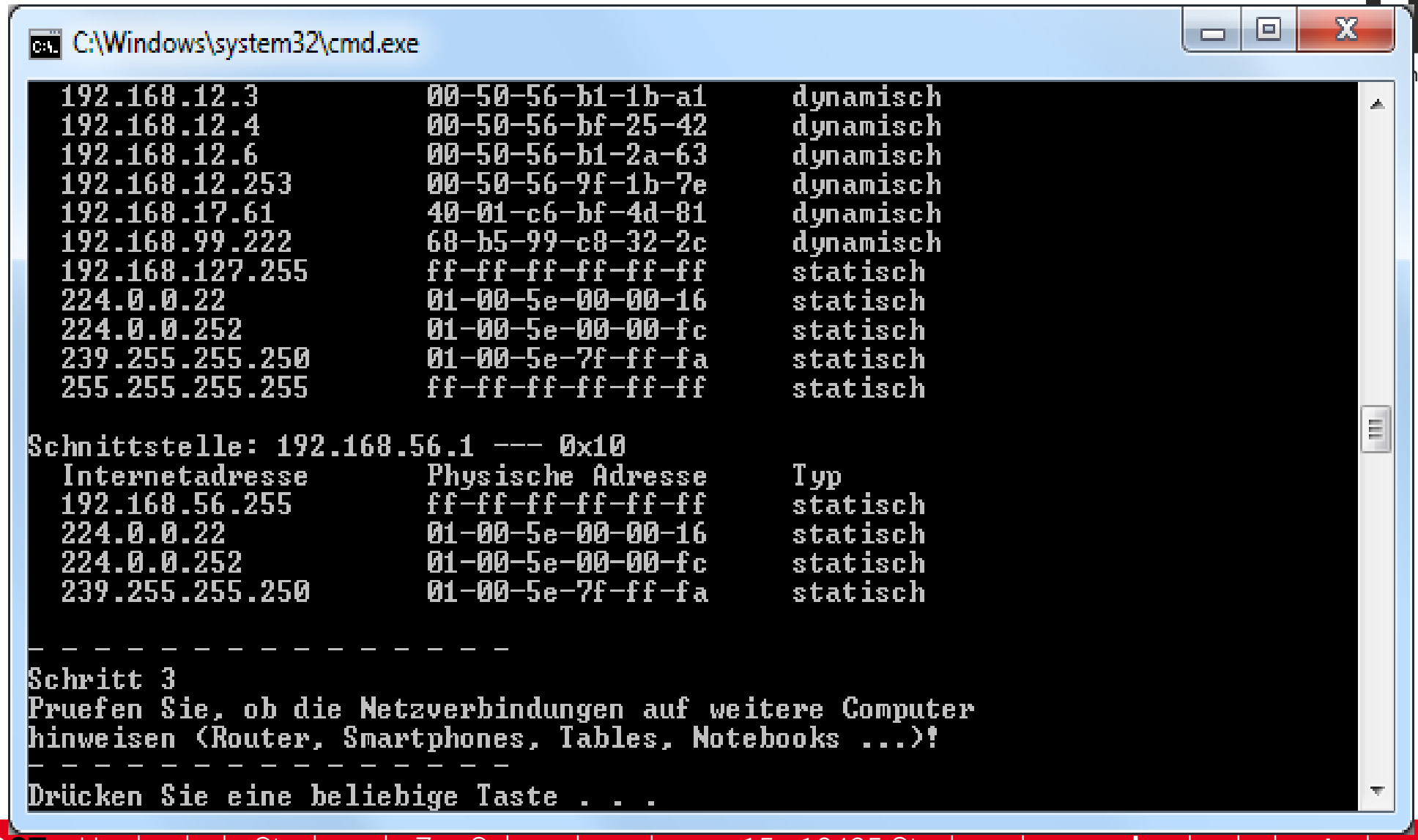
# Durchsuchungskonzept



# Durchsuchungskonzept



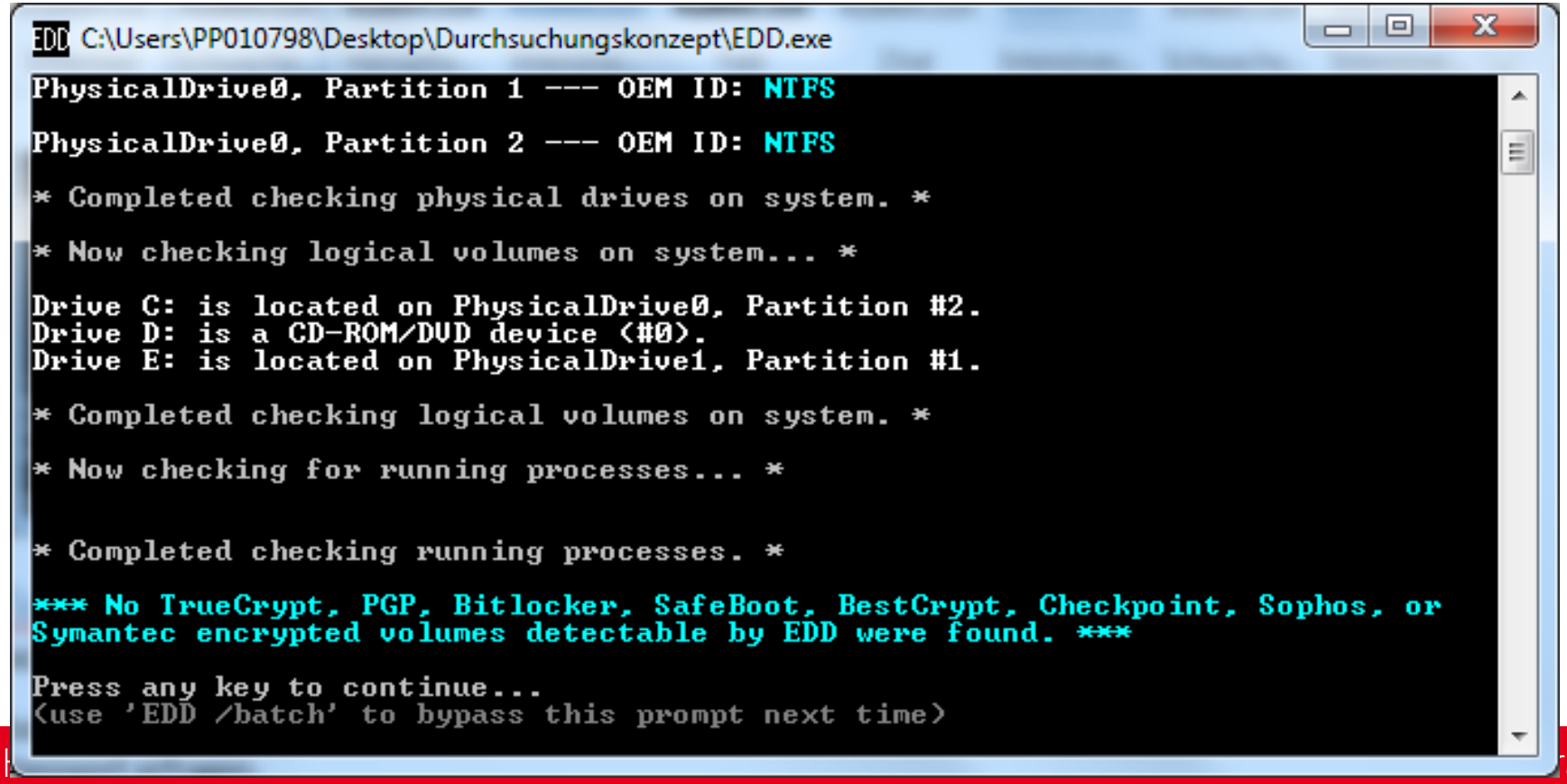
# Durchsuchungskonzept



# Durchsuchungskonzept

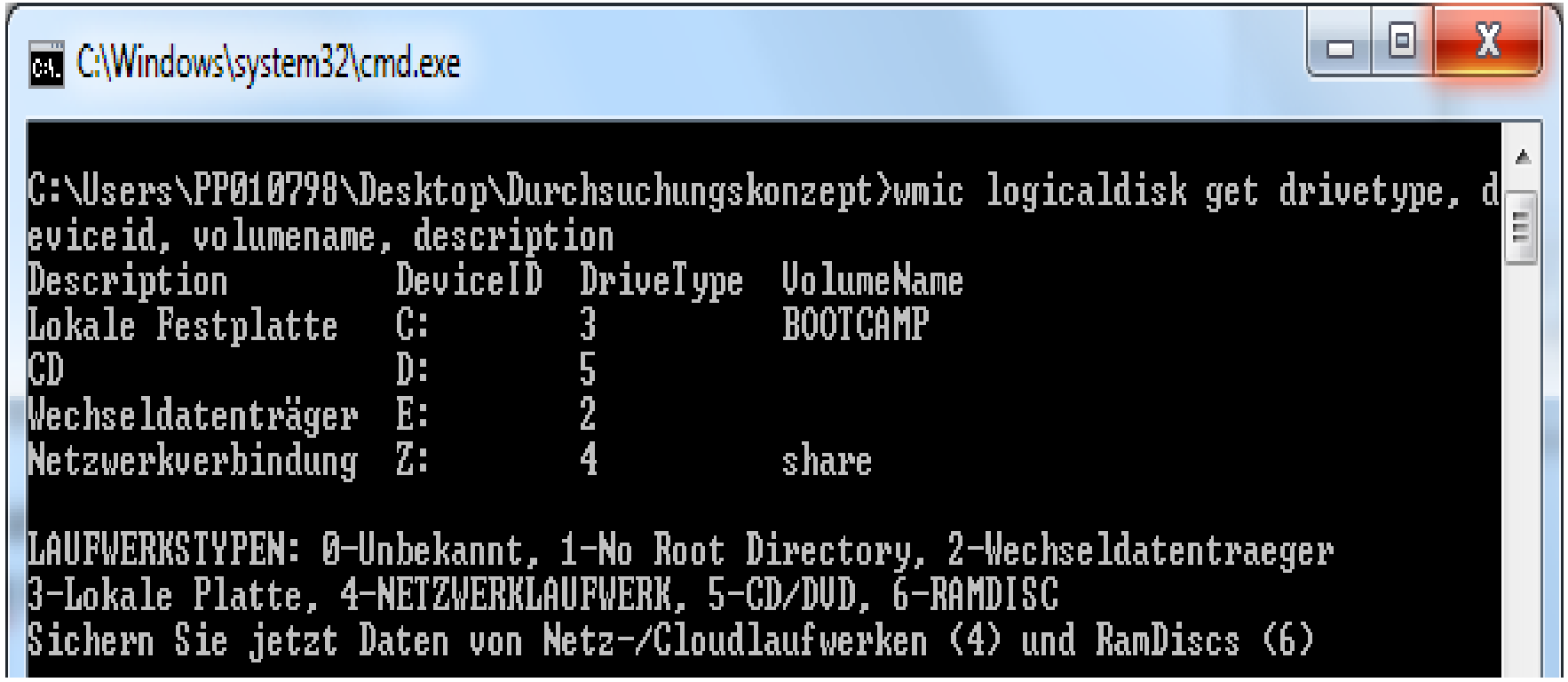
**ACHTUNG: Administratorrechte erforderlich.**

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

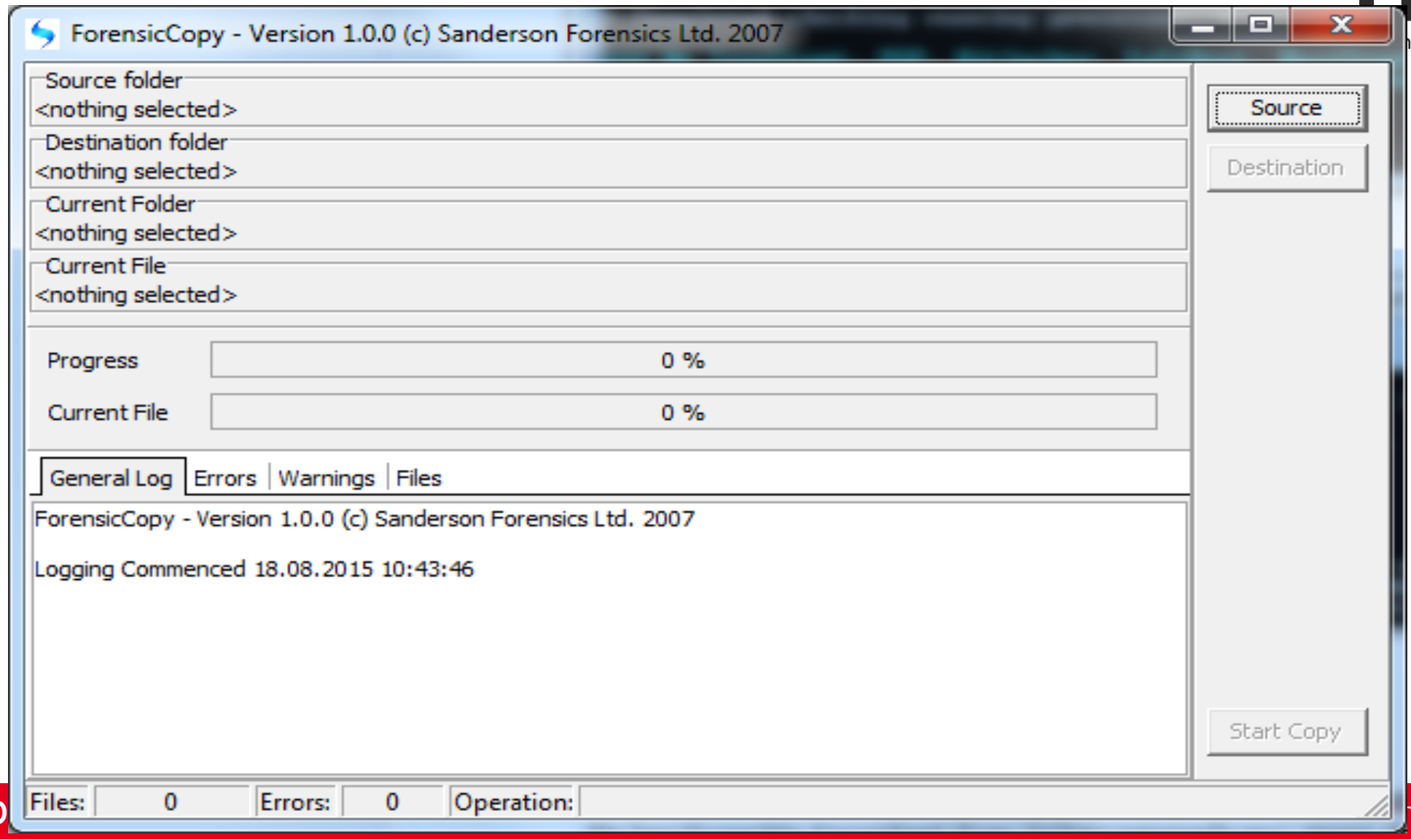


# Durchsuchungskonzept

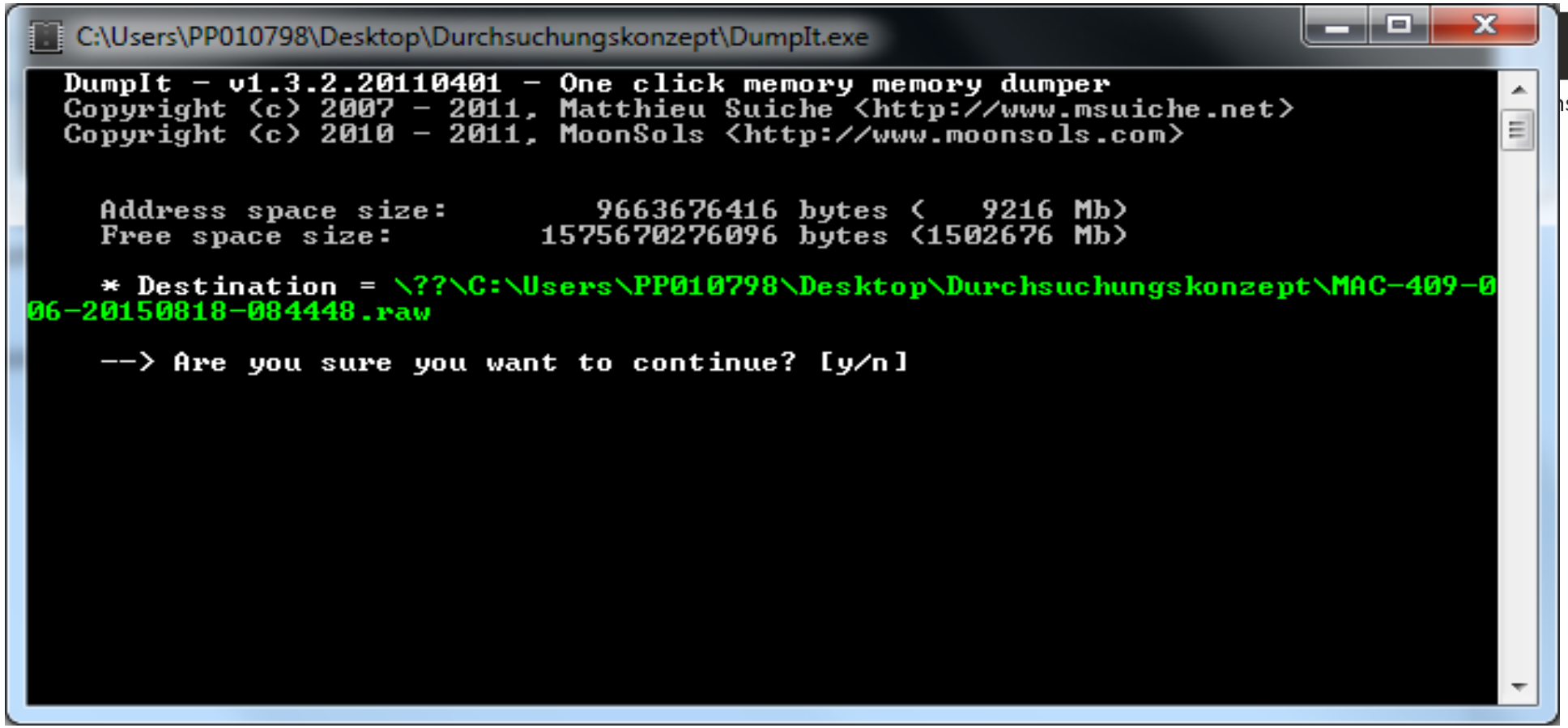
**Sichern Sie nun relevante Daten von Netz-, Cloud- und/oder kryptierten Laufwerken. Denken Sie an die beschraenkte Kapazitaet Ihres Sicherungsmediums! Wenn der Speicher nicht ausreicht, jetzt Unterstuetzung anfordern!**



# Durchsuchungskonzept



# Durchsuchungskonzept

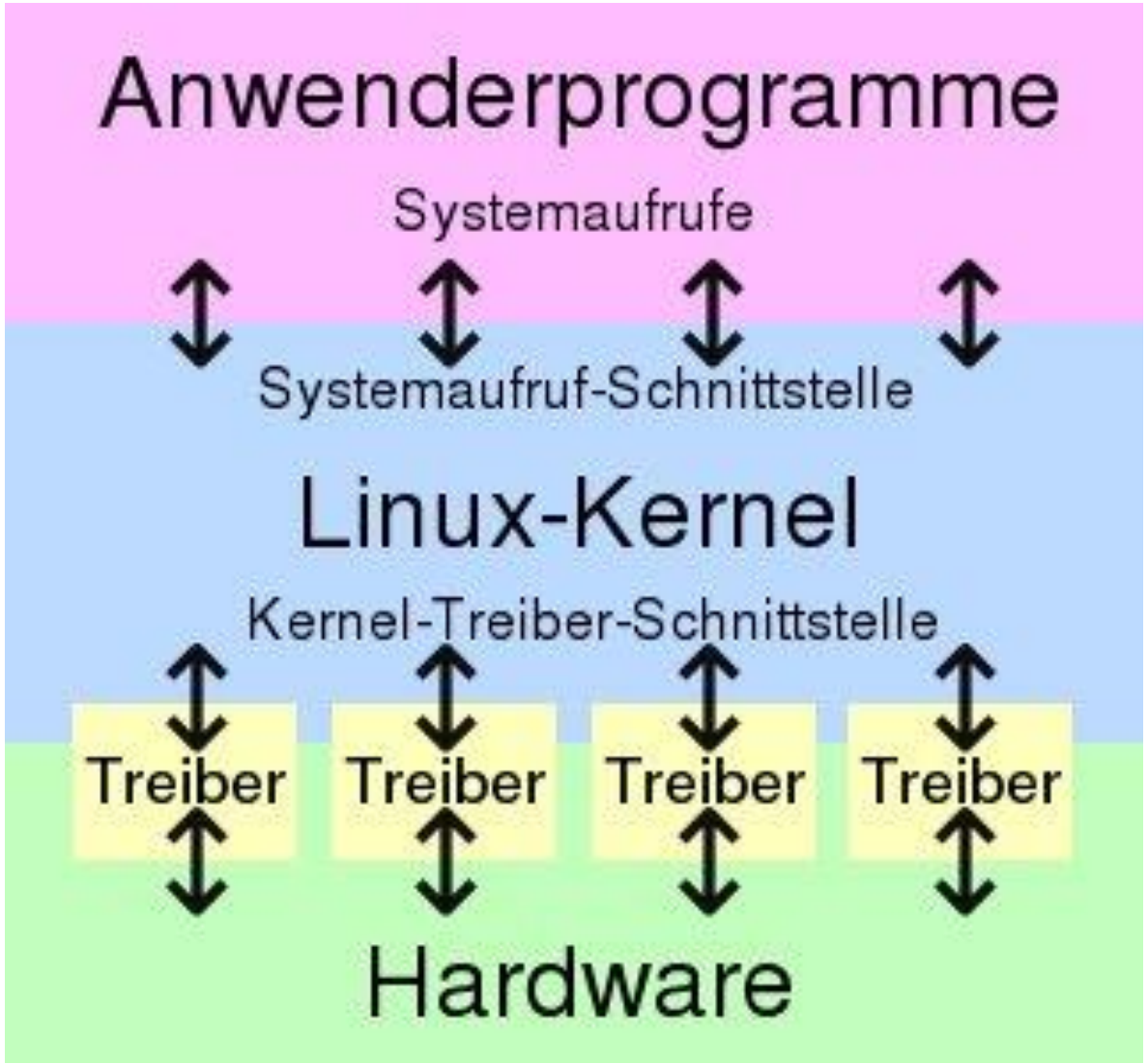



**Wenn der Speicher gesichert wurde (Meldung: Success), oder die Sicherung nicht möglich war, ist die Live-Sicherung beendet. Wenn nichts Aussergewöhnliches dagegen spricht, jetzt Netzstecker ziehen.**

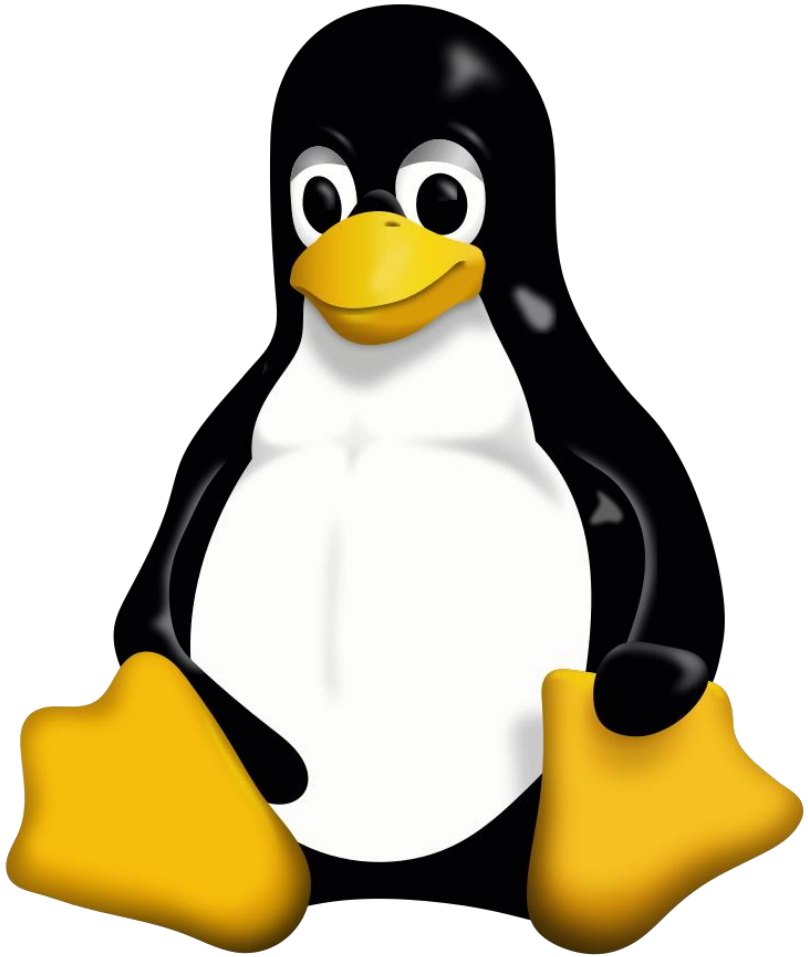
# Linux-Forensik

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

# Linux


Anwenderprogramme
Systemaufrufe
Systemaufruf-Schnittstelle
Linux-Kernel
Kernel-Treiber-Schnittstelle
Treiber
Treiber
Treiber
Treiber
Hardware

# Warum Linux als Auswertesystem?



# Warum nicht Linux als Auswertesystem?

HOST
Hochschule Stralsund

The Law Enforcement and Forensic Examiner's Introduction to Linux

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

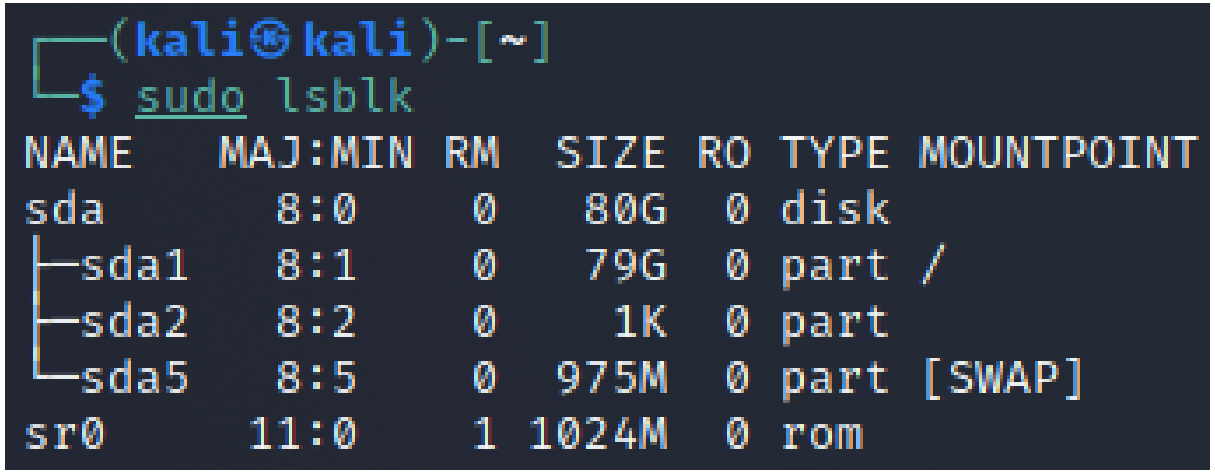
# Linux als Auswertesystem

# Linux Forensic Distributions

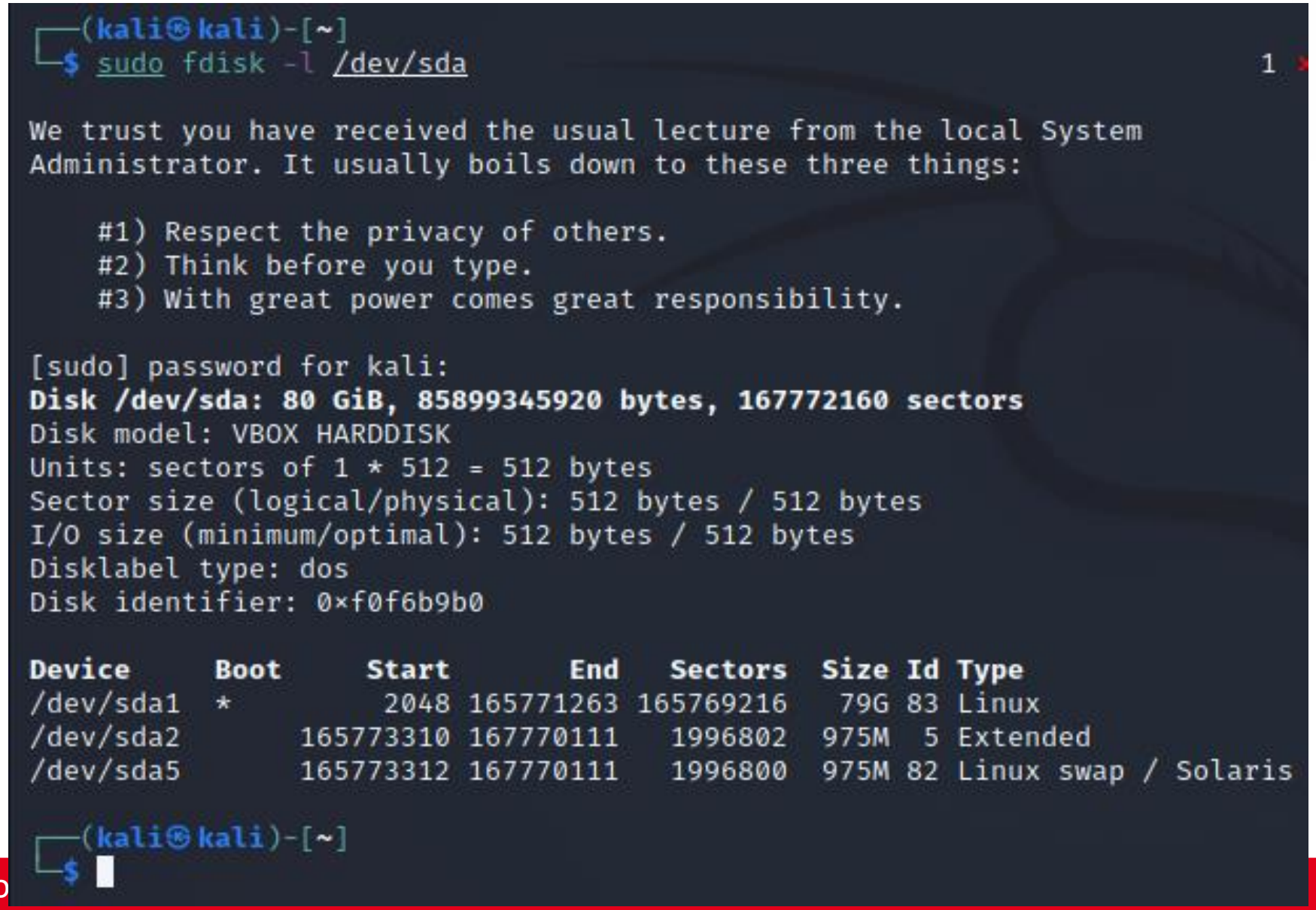


slackware
linux

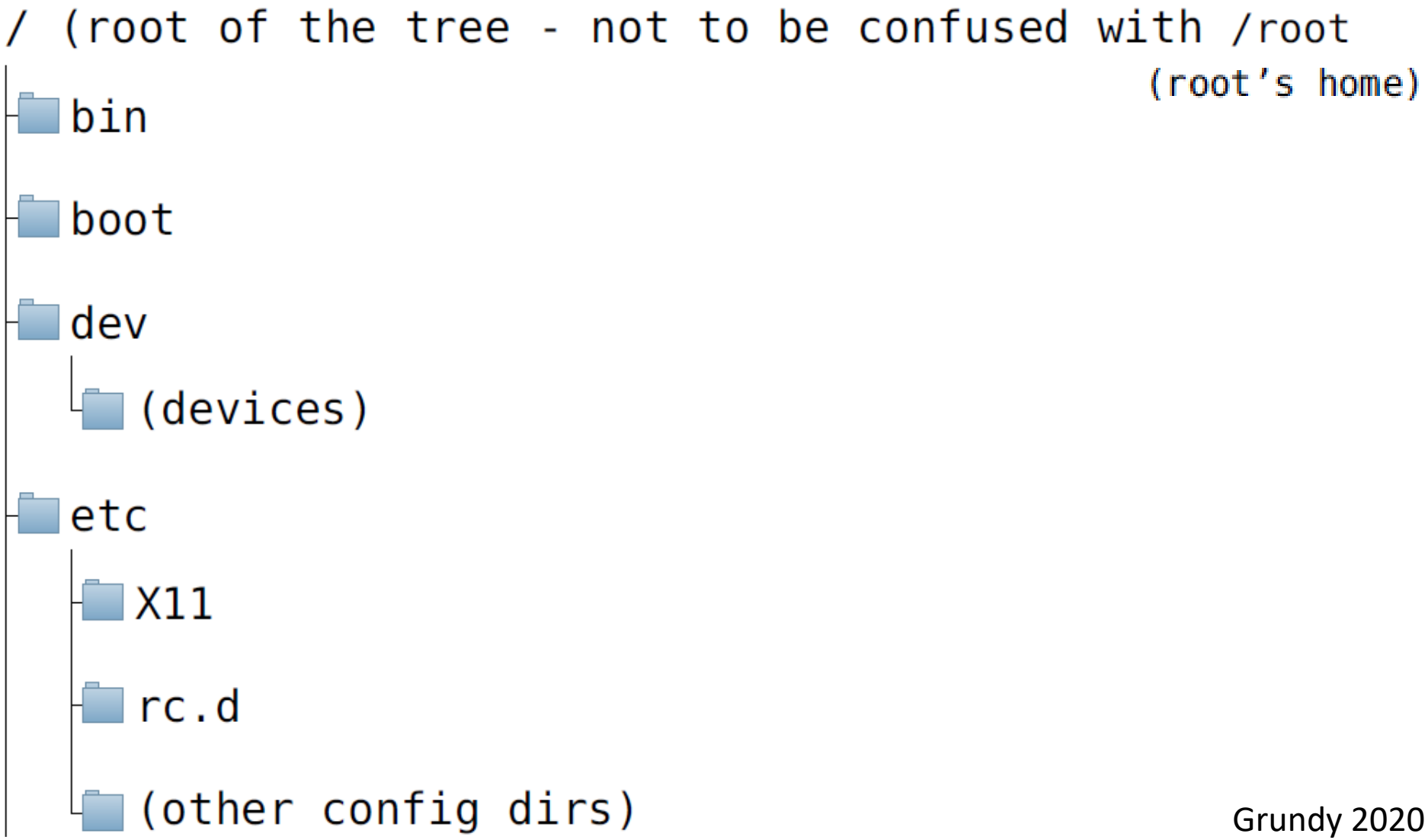

# Linux Commands



# Linux Commands

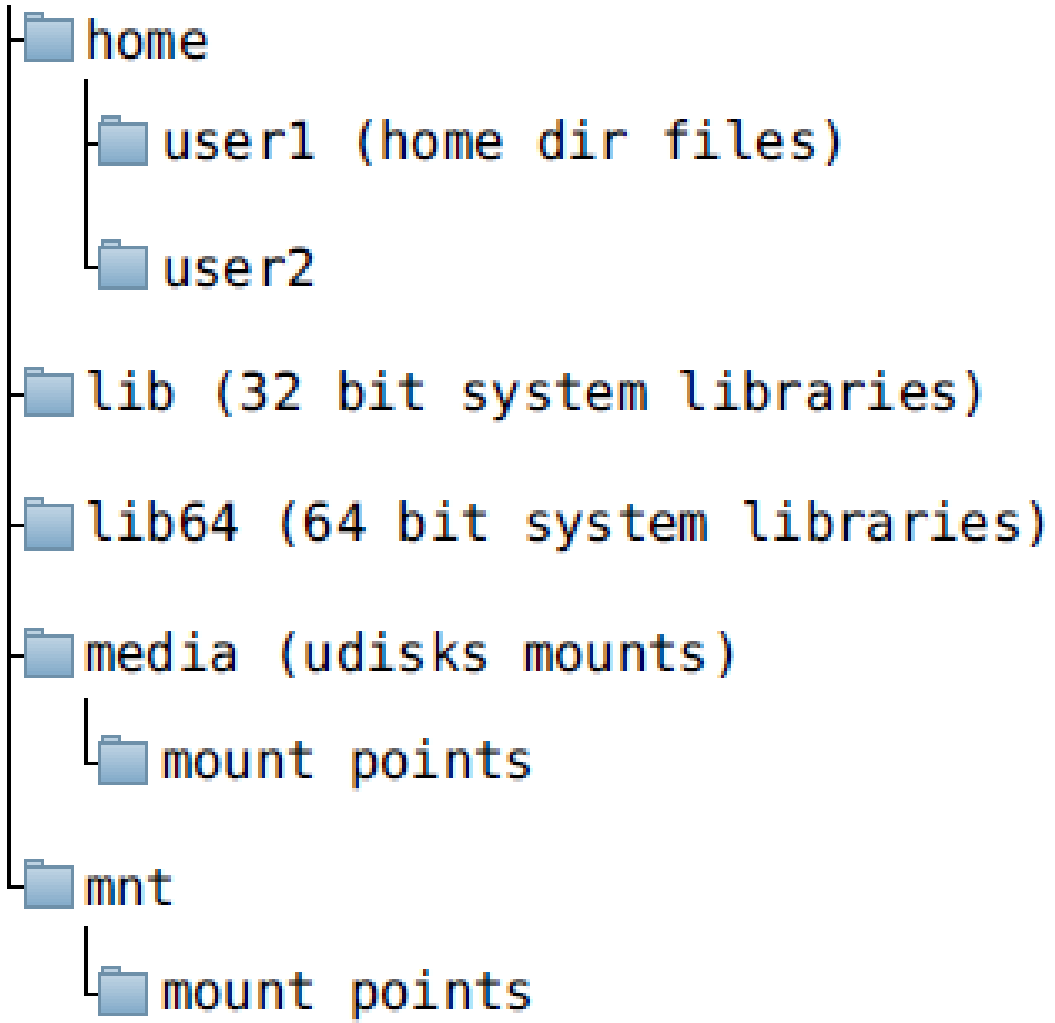


# Linux Verzeichnisbaum



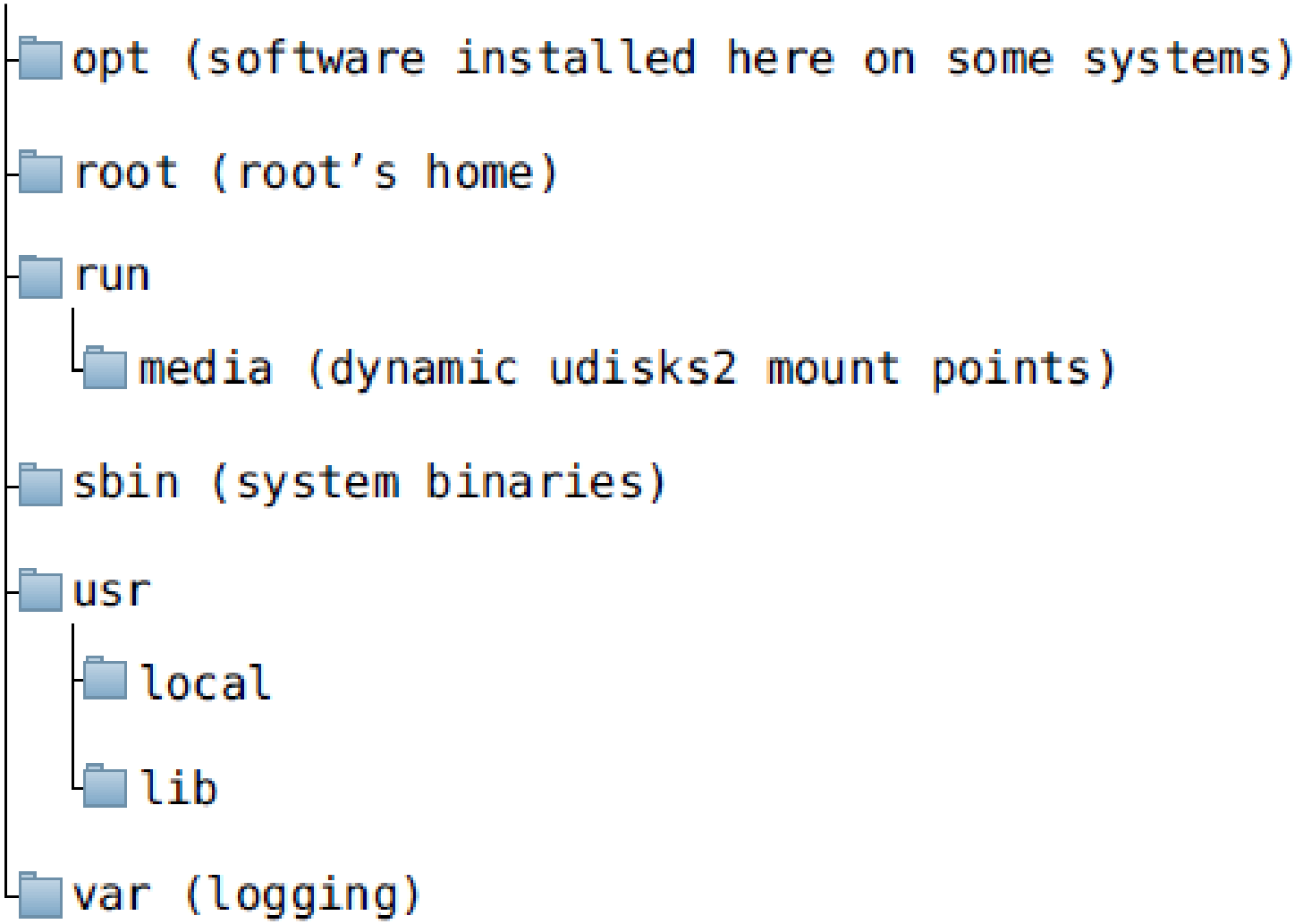

Grundy 2020

# 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
```

Grundy 2020

# 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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Zeitzone

/etc/timezone

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Befehle beim Systemstart

/etc/rc.local

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Hauptspeicherdaten

/proc/kcore

Teile des virtuellen Adressraums können dort gesichert werden.

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Auslagerungsdaten

/proc/swaps

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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Dateisysteme

/proc/mounts

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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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.

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Systemeinstellungen

/proc/sys

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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Aktuelle Kernel-Version

/proc/version

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Speicherauslastung

/proc/meminfo

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Kernel-Konfiguration

/proc/config.gz

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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 |

BSI 2011

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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
root@utopia:~#
```

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## MAC-Adresse

/sys/class/net/***eth0***/address

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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/

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## 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***

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Prozessdaten

/proc/Prozessnummer

/fd Liste der verwendeten Dateien
*status* Prozessstatus

# Linux

# Forensisch relevante Daten

## Kernel-Logs

/proc/kmsg

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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Durchschnittliche Systemauslastung

/proc/loadavg

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

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## User Accounts

/etc/passwd

# Linux

# 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 |

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## User Accounts, Gruppen

/etc/group

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Logdateien

/var/log

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

Mehr unter:
https://wiki.ubuntuusers.de/Logdateien/

# Linux

# Forensisch relevante Daten

Hochschule Stralsund

## Apache Webserver

/var/log/apache2

# Linux

# Forensisch relevante Daten

## Bereitgestellte Webserver-Dateien

/var/www