

# Linux in der Computer-Forensik

Alexander Geschonneck, CFE  
HiSolutions AG



## Folien und Tools

Folien und das vorgestellte Toolset finden sich unter

<http://computer-forensik.org>

### Kontakt

alexander AT geschonneck DOTcom

geschonneck AT computer-forensik DOT org



## Agenda

- Was ist Computer-Forensik?
- Was ist wichtiger als Tools und Betriebssystem?
- Anforderungen an Werkzeuge und Vorgehen
- Linux-Systeme analysieren
- mit Linux-Systemen analysieren
- Live Response mit ForensiX

# Was ist Computer Forensik?

Computer-Forensik<sup>1</sup> (oder auch Digitale Forensik, IT-Forensik, IuK Forensik):

- Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität
- Nachweis und Aufklärung von anderen rechtswidrigen und sonst wie sozialschädlichen Verhaltensweisen die unter Einbeziehung von IT vorgenommen wurden durch Analyse von digitalen Spuren

Kriminalistische Fragestellungen:

**Wer, Was, Wo, Wann, Womit, Wie und Weshalb (evtl.)**

Ziel der Ermittlung

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
- Ermittlung des entstandenen Schadens nach einem Systemeinbruch,
- Identifikation des Angreifers,
- Sicherung der Beweise für weitere juristische Aktionen.

<sup>1</sup> forensisch [lat. sinngemäß]: gerichtlich oder auch kriminaltechnisch; andere Beispiele: forensische Medizin; forensische Psychologie

# „Eisberg“ der Daten



Daten, die von normalen Tools gefunden werden

Zusätzliche Daten, die nur durch  
Spezialwerkzeuge gefunden werden können  
(gelöscht, umbenannt, versteckt, unvollständig,  
schwer aufzufinden)

# Welche Daten können gesammelt werden?



Unabhängig von der konkreten Fragestellung und dem zu untersuchenden System (Server Workstation, PDA, Router, Notebook etc.) lassen sich grundsätzlich einige empfindliche Datentypen, die für die Ermittlung von Interesse sind, finden:

- Flüchtige Daten
  - Informationen, die beim geordneten Shutdown oder Ausschalten verloren gehen (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse und deren Speicherbelegung, angemeldete User etc.)
  
- Fragile Daten
  - Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann
  
- Temporär zugängliche Daten
  - Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z.B. während der Laufzeit einer Anwendung.

Die Kenntnis um die Halbwertszeit dieser Daten ist sehr wichtig, da damit die Reihenfolge der Datensammlung bestimmt wird.

# Grundsätzlich gilt: SAP-Modell

## Secure (Erfassung der Daten)

- „Tatort“ und Untersuchungsbereich absichern
- Beweisspuren sorgfältig sichern
- Integrität der Daten bewahren bzw. nachweisen: Hashes, Vieraugenprinzip, Protokollierung
- Rechtmäßigkeit beachten

## Analyze (Auswertung der Daten)

- Spuren sorgfältig auswerten
- Ergebnisse objektiv bewerten
- Schlüsse kritisch hinterfragen

## Present (Präsentieren der Ergebnisse)

- Detaillierungsgrad und Methoden sind abhängig von der Fragestellung
- Erkenntnisse schlüssig und nachvollziehbar dokumentieren
- Erkenntnisse überzeugend zielgruppenorientiert präsentieren

## Anforderung an den Ermittlungsprozess (lässt sich auch auf Werkzeuge übertragen)

### Akzeptanz

- Schritte und Methoden müssen allgemein akzeptiert sein

### Glaubwürdigkeit

- Funktionalität und Robustheit der Methoden kann nachgewiesen werden (kein Kaninchen aus dem Hut zaubern)

### Wiederholbarkeit

- Der gesamte Ermittlungsprozess kann von Dritten wiederholt werden (und zu den gleichen Ergebnissen führen)

### Integrität

- Die Spuren dürfen nicht verändert werden.
- Es muss demonstriert werden können, dass die Spuren nicht verändert wurden bzw. welche Spuren genau verändert wurden.

### Ursache und Auswirkungen

- logisch nachvollziehbare Verbindungen zwischen Personen, Ereignisse und Beweisspuren können dargelegt werden

### Dokumentation

- Jeder Schritt des gesamten Prozess ist angemessen dokumentiert

## Anforderungen an Tools

- Arbeiten die Forensiktools wie sie es sollen?
- Welche Technologie liegt dem Tool zu Grunde?
- Tools sollten von anerkannten Spezialisten
  - Getestet sein
  - Einem Peer Review unterzogen worden sein und
  - Grundsätzlich in der Community akzeptiert sein
- Die Ergebnisse der Werkzeuge müssen vor Gericht akzeptiert werden
  - Wo kommt das Tool her? Habe ich die eingesetzte Version archiviert?
  - Wurde das Tool modifiziert? Würde ich eine Veränderung erkennen?
  - Hat sich das Tool bereits in anderen Ermittlungen bewährt oder bin ich Alpha-Tester?
- Dokumentation und Support sind ebenfalls ausschlaggebend

# Linux in der Ermittlung

- Vorteile Open Source Forensik
  - Qualität der Tools ist kommerzieller Konkurrenz oft ebenbürtig
  - Fehler werden schneller entdeckt
  - Komplexe Probleme durch Kommandozeilen-Tools lösbar
  - Einfache Erweiterbarkeit
  - Durch leichteren Zugang häufigerer Einsatz außerhalb von LE
- Vorteile Forensik mit Linux
  - Der Ermittler kontrolliert das Betriebssystem und die Anwendungen
  - Alle Tätigkeiten sind mit Bordmitteln protokollierbar
  - Viele Dateisystemtreiber sind vom Grundsatz enthalten
  - Freies Loopback Device!
  - Sniffer eingebaut, Unterstützung für viele Protokolle
- 2.4 oder 2.6?
  - In der Secure-Phase ist 2.4 ok (Vorsicht mit ungeraden Sektoren!)
- Welche Distro ist am besten geeignet?
  - ;-)

## Werkzeugkiste der Ermittler



- Tools zum Erstellen und Prüfen von Prüfsummen (mehrere Verfahren)
- Tools zur Sicherung von flüchtigen Daten in der Live Response
- Schlüsselwortsuchtools (auch fremde Zeichensätze) in logischen und physischen Strukturen von Datenträgerimages
- Tools zur Dateianalyse und –wiederherstellung anhand von Dateisignaturen
- Tools zum kompletten oder gefilterten Wiederherstellen von gelöschten Daten
- Tools zum Betrachten unterschiedlicher Dateiformate
- Tools zum Erstellen Timeline durch Auswertung der MAC-Times
- Tool zum Erstellen und Zusammenfassen aller Berichte mit bedarfsweisen Detailinformationen
- Tool zum Löschen der verwendeten eigenen Speichermedien vor Aufnahme von Beweisspuren
- Verschlüsselungswerkzeuge zur Sicherung der Ermittlungsergebnisse
- Hardware Writeblocker mit Adaptern für unterschiedliche Speichermedien

Die verwendeten Werkzeuge müssen beherrscht werden – vorher üben!

## Unterschiedliche Analyseansätze

**Live Response (Untersuchung am Live System)  
= Notaufnahme**



**Post Mortem Analyse (Untersuchung einer Forensischen Kopie)  
= Pathologie bzw. Gerichtsmedizin**



## Was ist bei Datenträgeranalysen möglich?

### Was ist möglich?

- Wiederherstellung von gelöschten Daten
- Erkennen, zu welchem Zeitpunkt Dateien erzeugt, verändert, aufgerufen/angesehen oder gelöscht wurden
- Erkennen welche externen Speichergeräte angeschlossen waren
- Welche Anwendungen sind/waren installiert
- Welche Webseiten wurden besucht
- Mailverkehr
- ...

### Was ist nicht möglich?

- Ist der Datenträger physisch zerstört, ist eine Wiederherstellung der Daten nicht möglich
- Ist der Datenträger „sicher“ überschrieben worden, ist eine Wiederherstellung der Daten nicht möglich
- Ist der Datenträger mit „0“ überschrieben, ist eine Wiederherstellung der Daten nur sehr schwer möglich, wenn überhaupt

## Was ist bei der Live Response möglich?

Was ist möglich?

- Welche Programme sind im Speicher aktiv? Sockets?
- Wie wurden diese Programme gestartet? Aus welchem Pfad? In welcher Reihenfolge? Durch welchen User?
- Welche Informationen werden durch das Programm im RAM verarbeitet?
- Welche User sind angemeldet?
- Wie ist der Status der Netzverbindungen?

Was ist nicht möglich?

- Ist das System mehrfach gebootet worden, sind die relevanten Informationen weg.
- Liegt der Vorfall länger zurück und ist das System gut ausgelastet, sind die relevanten Informationen weg.

# Immer noch wichtig: MAC-Time Analyse

## Modification-, Access- and Change-Time unter Linux

- Modification-Time (mtime) ist der Zeitpunkt, zu dem eine Datei das letzte Mal geschrieben wurde,
- Access-Time (atime) ist der Zeitpunkt, zu dem eine Datei das letzte Mal gelesen oder ausgeführt wurde,
- Change-Time (ctime) ist der Zeitpunkt, zu dem bestimmte Meta-Daten der Datei verändert wurden (Ändern der Zugriffsrechte oder des Eigentümers).

## Maßnahmen nach erkanntem Sicherheitsvorfall

- Sämtliche Programme auf dem kompromittierten System sind nicht vertrauenswürdig!
  - Ausgaben von installierten Werkzeugen können manipuliert sein
  - trojanisierte Versionen der Werkzeuge und Root-Kits können installiert sein
  - Weiterer Schaden kann durch Verwendung der Tools entstehen
  - Routinen zum Löschen von Spuren können ausgelöst werden
  - Auslöser könnte auch Trennung vom Netzwerk sein (logische Bomben)
  - System isolieren, aber im Netzwerk belassen
  - Ausschließlich Verwendung von eigenen statisch kompilierten Werkzeugen ohne Schreibzugriff
- Niemals ungewollt auf den Datenträger schreiben!
- Keine Werkzeuge verwenden, die Zeitstempel verändern (tar, cp etc.)
- aufpassen bei Isof!

## Beispiel

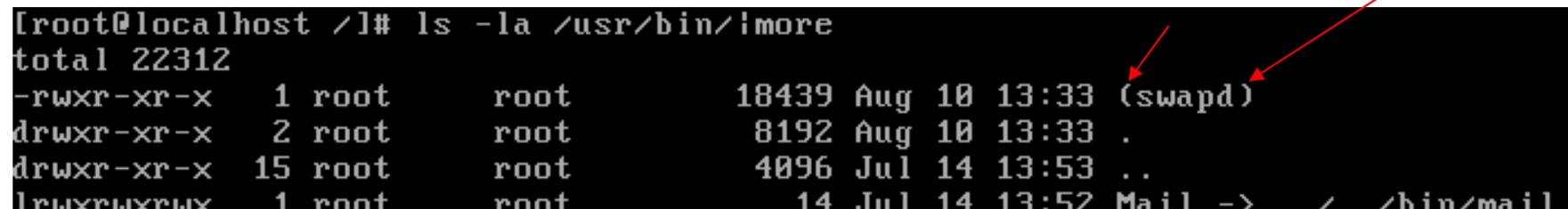
```
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686

This server is operated for authorized users only. All use
is subject to monitoring. Unauthorized users are subject to
prosecution. If you're not authorized, LOG OFF NOW!

localhost login: root
Password:
Last login: Wed Aug 6 11:16:40 on tty2
[root@localhost root]# (swamd) uses obsolete (PF_INET,SOCK_PACKET)
eth0: Promiscuous mode enabled.
device eth0 entered promiscuous mode
NET4: Linux IPX 0.47 for NET4.0
IPX Portions Copyright (c) 1995 Caldera, Inc.
IPX Portions Copyright (c) 2000, 2001 Conectiva, Inc.
NET4: AppleTalk 0.18a for Linux NET4.0
eth0: Promiscuous mode enabled.
eth0: Promiscuous mode enabled.
```

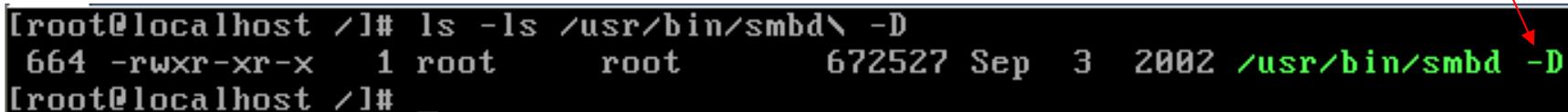
## Beispiel

```
[root@localhost /]# ls -la /usr/bin/!more
total 22312
-rwxr-xr-x  1 root  root    18439 Aug 10 13:33 (swapd)
drwxr-xr-x  2 root  root     8192 Aug 10 13:33 .
drwxr-xr-x 15 root  root    4096 Jul 14 13:53 ..
lrwxrwxrwx  1 root  root         14 Jul 14 13:52 Mail -> /bin/mail
```



Dateiname lautet „(swapd)“

```
[root@localhost /]# ls -ls /usr/bin/smbd\ -D
664 -rwxr-xr-x  1 root  root    672527 Sep  3 2002 /usr/bin/smbd -D
[root@localhost /]#
```



Dateiname lautet „smbd -D“

## Beispiel

```
[root@localhost ~]# ls -la /dev/ttyo*  
-rwxr-xr-x  1 root  root    134 Sep  4  2002 /dev/ttyoa  
-rwxr-xr-x  1 root  root    59 Sep  4  2002 /dev/ttyof  
-rwxr-xr-x  1 root  root    74 Mar 18  2002 /dev/ttyop
```

### RootKit-Konfigdateien in /dev/

```
[root@localhost ~]# ll lib/.x/  
total 160  
-rwxr-xr-x  1 apache  apache  17931 Jan  8  2003 cl  
-rwxr-xr-x  1 apache  apache   303 Dec 23  2002 hide  
-rw-r--r--  1 root    root     222 Aug 10 15:32 hide.log  
-rwxr-xr-x  1 apache  apache  59137 Mar 22 09:00 inst  
-rw-r--r--  1 root    root    2442 Aug 10 15:32 install.log  
-rw-r--r--  1 root    root      1 Aug 10 15:32 ip  
-rwxr-xr-x  1 apache  apache  25795 Jan  8  2003 log  
drwxrwxrwx  2 root    root    4096 Aug 10 15:32 s  
-rwxr-xr-x  1 root    root   28632 Aug 10 15:32 sk  
[root@localhost ~]# _
```

### RootKit in /lib/.x

## Beispiel

```
[root@localhost root]# /sbin/ifconfig eth0 ←
eth0      Link encap:10Mbps Ethernet  HWaddr 00:0C:29:89:42:93
          inet addr:192.168.1.79  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6618588 errors:9788 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:871337
          Interrupt:10 Base address:0x10e0

[root@localhost root]# /mnt/cdrom/Static-Binaries/linux_x86/ifconfig eth0 ←
eth0      Link encap:Ethernet  HWaddr 00:0C:29:89:42:93
          inet addr:192.168.1.79  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:9788 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
```

# Forensische Duplikation mit Linux

- Das Unix-Kommando dd ist in den allermeisten Fällen das Werkzeug der Wahl, um Diskimages anzulegen.
- Stark abhängig vom Betriebssystem und der Abstraktion von Devices als Files
- Kann ganze Devices, Partitionen oder Teile davon kopieren
- Weitere auf dd basierende Dupliziertools
  - dd\_rescue
  - sdd - <http://ftp.berlios.de/pub/schily/sdd/README>
  - dcfldd - <http://dcfldd.sourceforge.net/> (DoD Computer Forensics Laboratory )
  - DCCldd (Nur auf Anfrage beim DoD Cyber Crime Center)
  - Dc3dd (Patch für dd, <http://dc3dd.sourceforge.net/>)
- Diverse grafische Tools
  - GRAB
  - Adepto
  - LinEn
  - SMART
  - GYMAGER



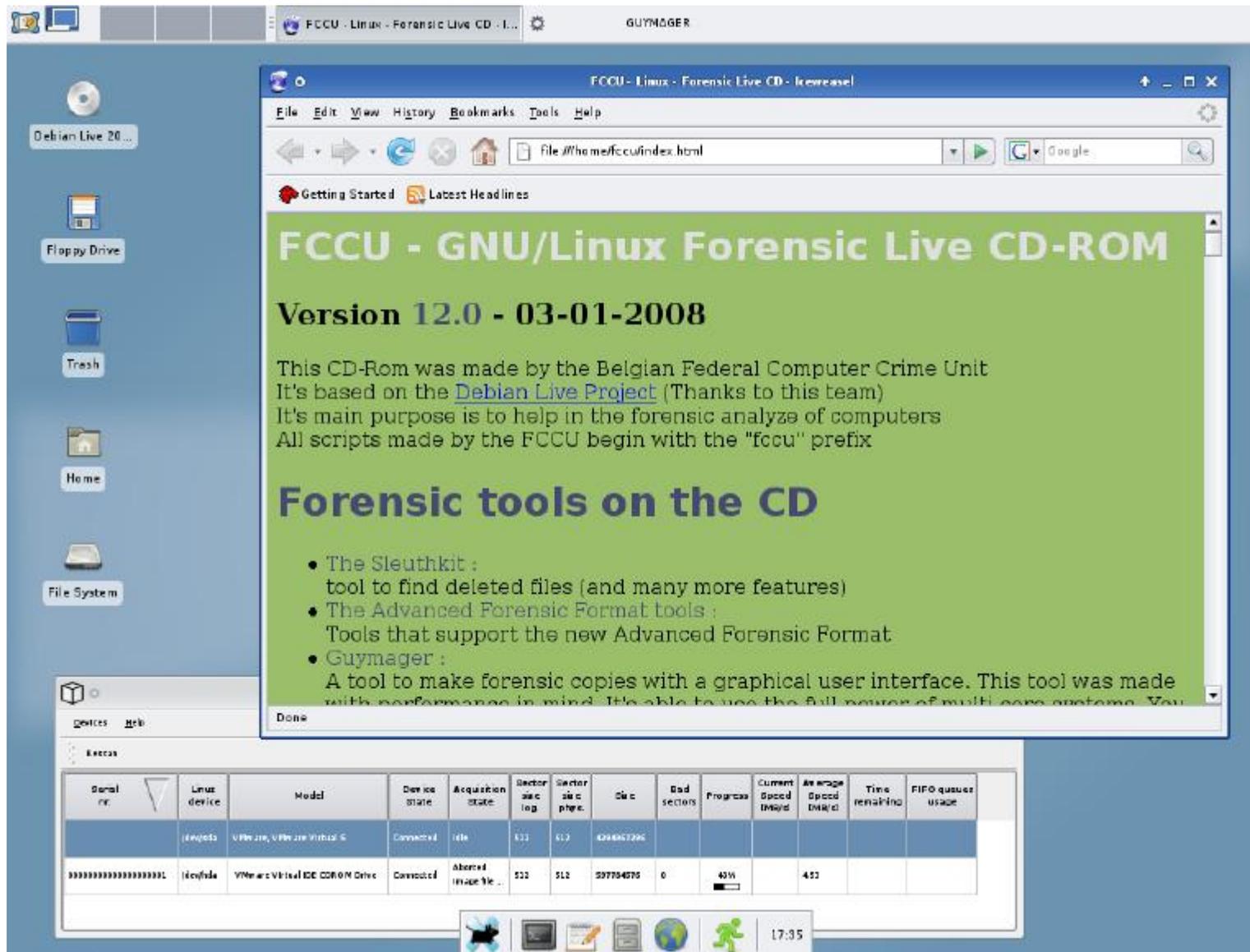
## Linux Live CDs

# FCCU

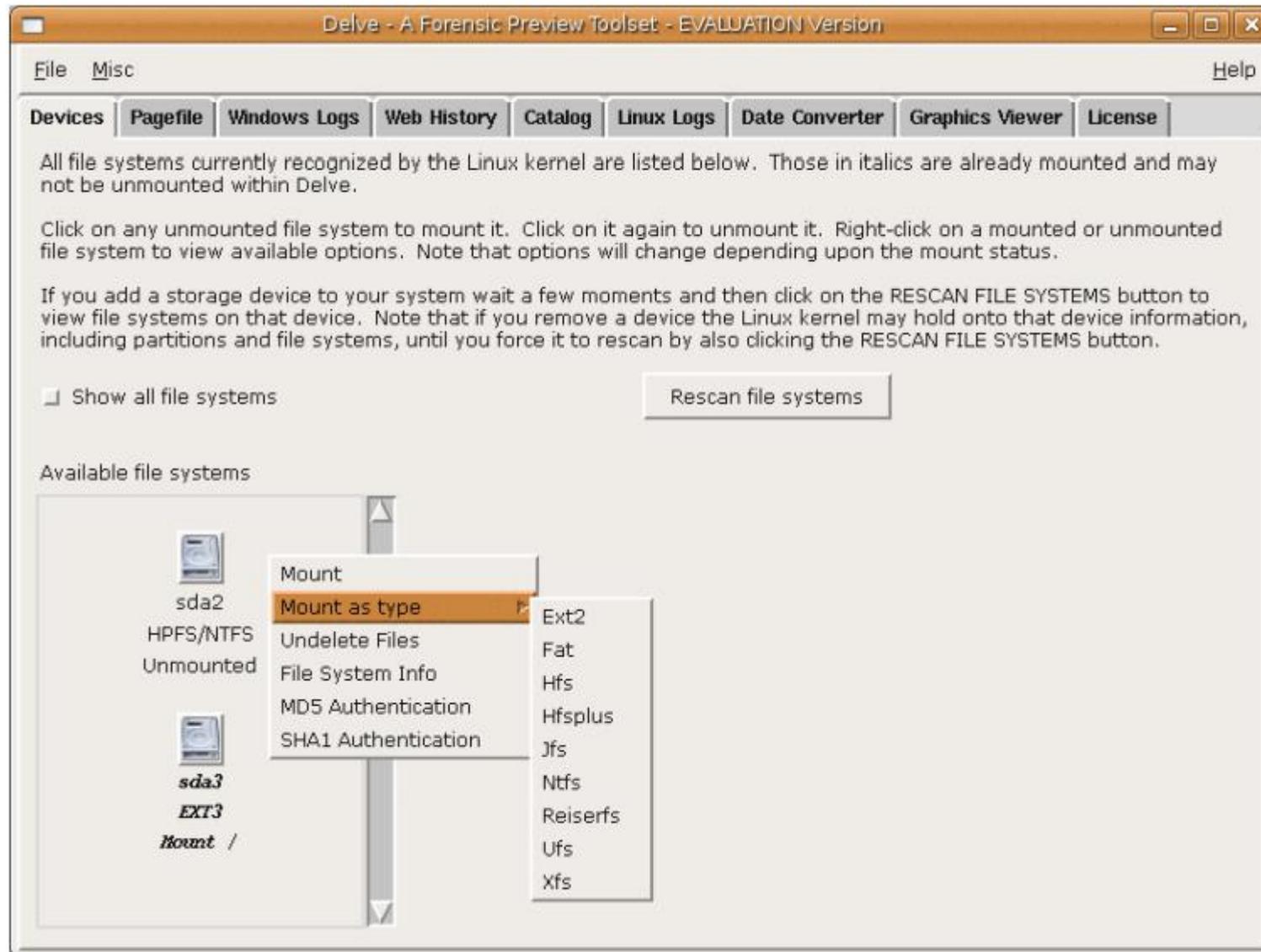


[www.lnx4n6.be](http://www.lnx4n6.be)

# FCCU

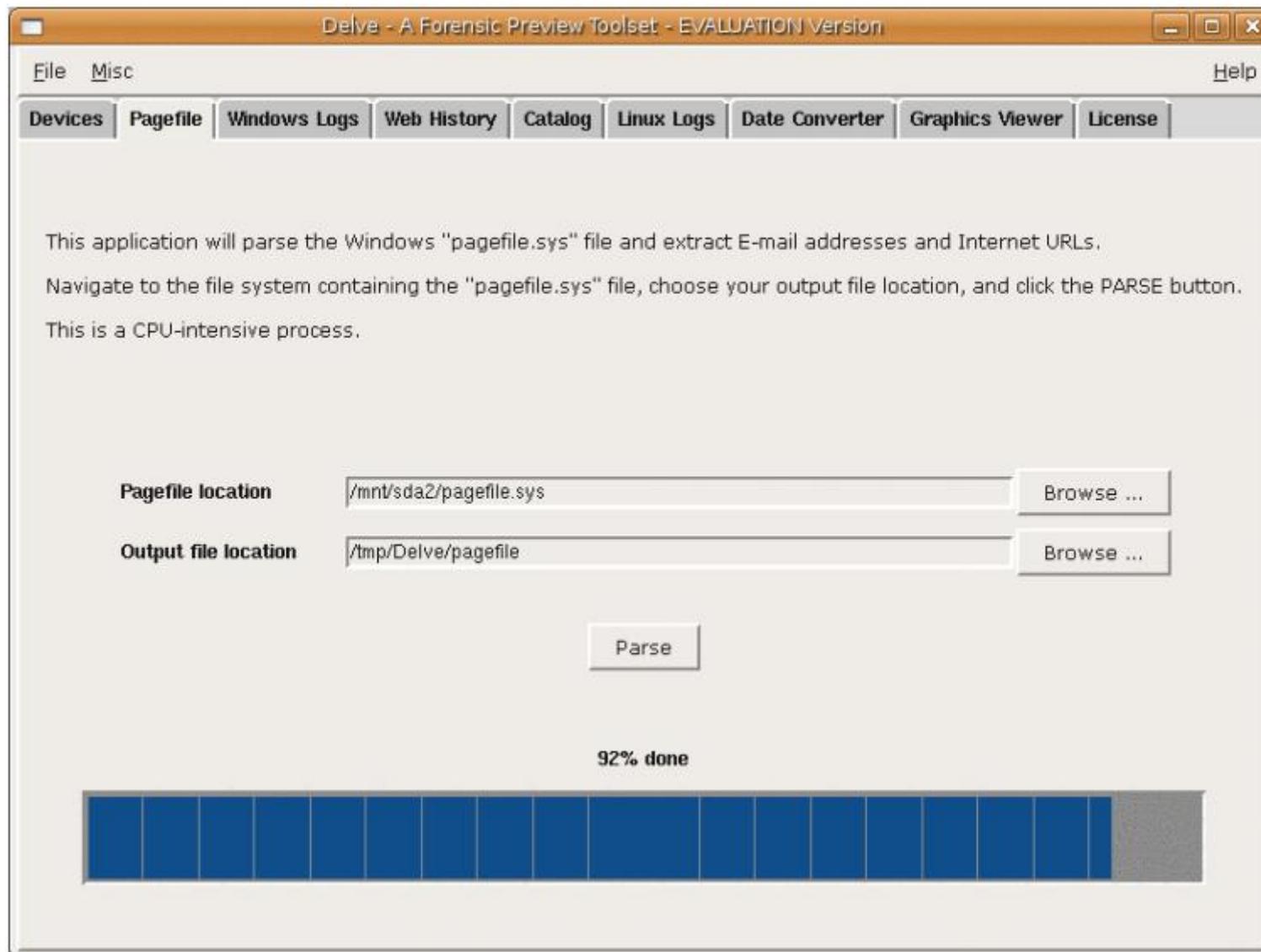


# THE FARMER'S BOOT CD

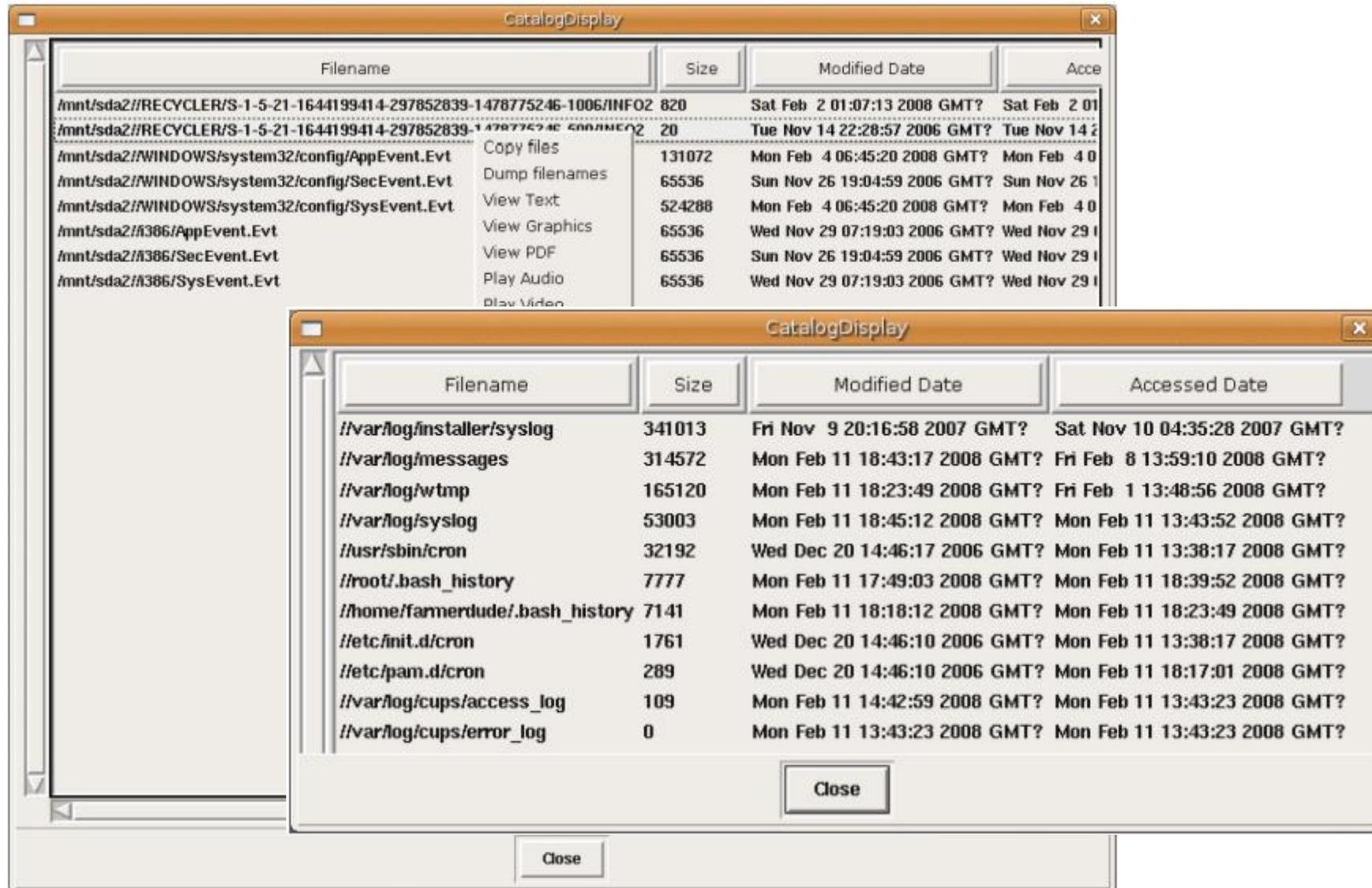


[www.forensicbootcd.com](http://www.forensicbootcd.com)

# THE FARMER'S BOOT CD



# THE FARMER'S BOOT CD



[www.forensicbootcd.com](http://www.forensicbootcd.com)

## Helix




```

PCI: Cannot allocate resource region 4 of device 0000:00:07.1

HELIX
3

Incident Response, Electronic Discovery, & Forensics Live CD

Scanning for USB/Firewire devices... Done.
Found primary HELIX compressed image at /cdrom/KNOPPIX/KNOPPIX.
Total memory found: 286364 kB
Creating /ramdisk (dynamic size=221288k) on shared memory...Done.
Creating unionfs and symlinks on ramdisk...
>> Read-only CD system successfully merged with read-write (unionfs) /ramdisk.
Done.
Starting init process.
INIT: version 2.78-knoppix booting
Running Linux Kernel 2.6.14-Helix.
Processor 0 is Intel(R) Pentium(R) M processor 1.86GHz 1862MHz, 2048 KB Cache
ACPI Bios found, activating modules: ac battery button container fan processor thermal
video
PCMCIA found, starting cardmgr.
USB found, managed by hotplug.
^Firewire found, managed by hotplug: (Re-)scanning firewire devices... Done.
Autoconfiguring devices... ██████████
  
```



[www.e-fense.com](http://www.e-fense.com)

We secure your business. (tm)

© 2008, HiSolutions AG | Computer-Forensik 28

# Helix



Root Terminal    Adepto 2.0 (To Obtain, ...    Autopsy Shell    Autopsy Forensic Brow...

Autopsy Forensic Browser - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:9999/autopsy

e-fense™ Helix™ forensics ids wireless pen test crypto sniffers firewalls

**WARNING: Your browser currently has Java Script enabled.**

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

To Obtain, Get, Acquire)

Help

Acquire Restore/Clone Log Chain of Custody

Autopsy Forensic Browser 2.08

Enter a user name to proceed:

Alexander Geschonneck

Enter a case number (optional):

200736401

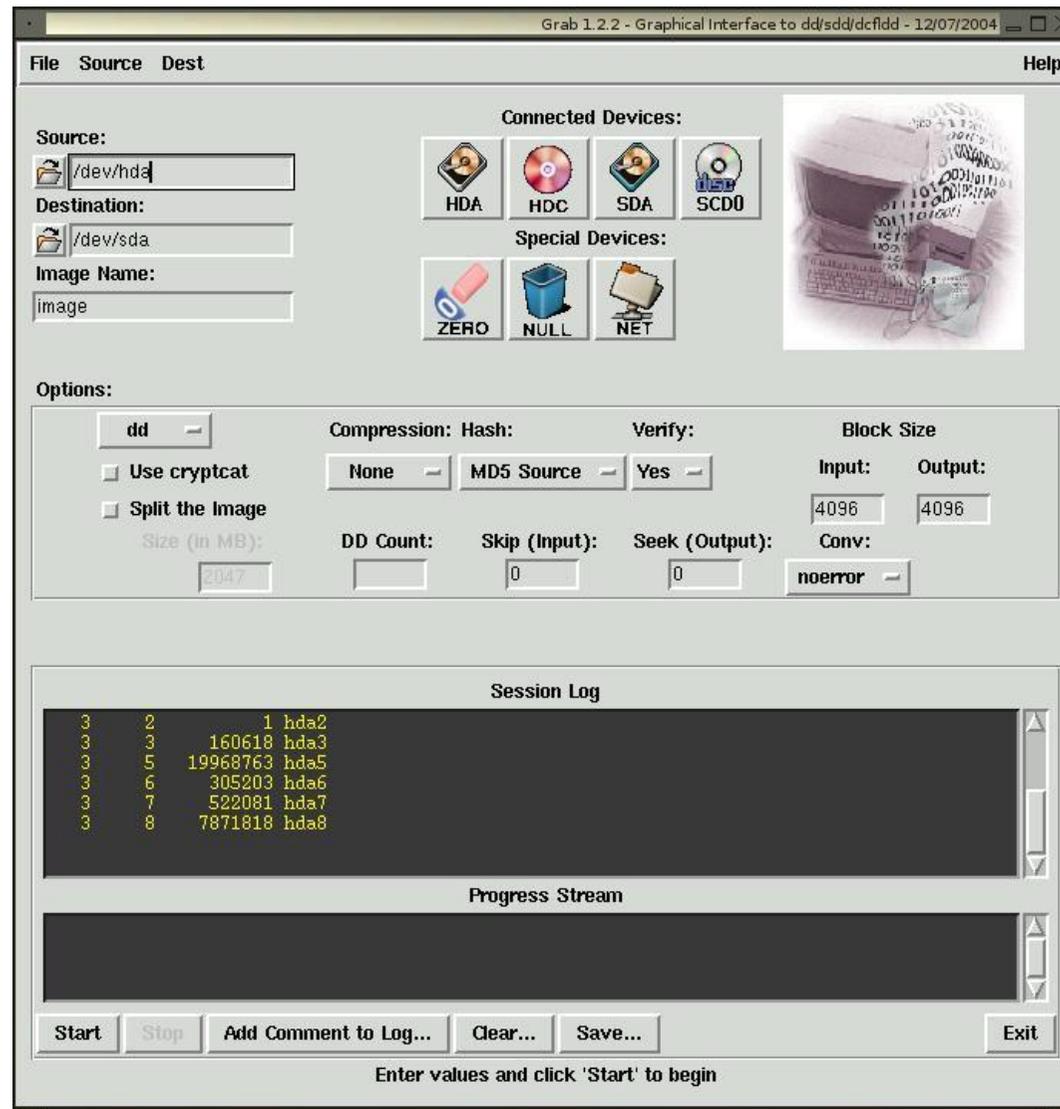
Root Terminal

```

EnCase(R) LinEn (6.8.0.22)                               Guidance Software, Inc (t*)
Code Type          Sectors   Size    LP  Label  System  Size
Disk0 /dev/hda Linux 1430308 Sectors
Size 698,4MB
No Partitions Found
Disk1 /dev/sda Linux 22020096 Sectors
Size 10,5GB
80 07 NTFS 22016000 10,5GB
    
```

cpu mem Net hda sda 6:01 PM

# Grab



# Adepto



# EnCase für Linux

```
Root Terminal
EnCase(R) LinEn (6.8.0.22)                               Guidance Software, Inc (tm)

Code Type          Sectors  Size  LP  Label      System  Size
-----
Disk0 /dev/hda Linux 1430308 Sectors
Size 698.4MB
No Partitions Found

Disk1 /dev/sda Linux 22020096 Sectors
Size 10.5GB
80  07      NTFS 22016000  10.5GB

acquire Hash Server License Quit
```

# Helix



Encase Linux Acquisition Util [Root Terminal]

/mnt/sda1

Encase Linux Acquisition Utility

Encase (5.03) (Linux)

| Code                | Type     | Sectors       | Size    | LP | Label | System | Size  |
|---------------------|----------|---------------|---------|----|-------|--------|-------|
| Disk0               | /dev/hdc | Linux 1414468 | Sectors |    |       |        |       |
| Size 690.7MB        |          |               |         |    |       |        |       |
| No Partitions Found |          |               |         |    |       |        |       |
| Disk1               | /dev/sda | Linux 8388608 | Sectors |    |       |        |       |
| Size 4.0GB          |          |               |         |    |       |        |       |
| 80                  | 07       | NIFS          | 8369865 |    |       |        | 4.0GB |

Network Server

Connected...\  
 Searched 0 bytes  
 Transferred 326.0MB

Cancel

cpu mem Net hda sda 6:37 PM

# Automatisierung durch IR-Toolkits



- Live Response Skript „linux\_ir.sh“ auf Helix CD
  - Unvollständig
  - Statische Tools stellenweise nicht auf aktuellen Distributionen / Kernels lauffähig
  - Teilweise fehlerhaft

## ForesiX-CD

- HiSolutions hat eigenes Toolkit zusammengestellt (in iX 07/07 veröffentlicht)
  - Diverse Forensik-Tools
  - Statisch kompilierte Werkzeuge für 2.4er und 2.6er Kernel
  - Vertrauenswürdige Shell
  - Sicherung über Netzwerk und auf externe Datenträger
  - Benötigte Dateien: /dev/null und /proc
  - Gelesene Dateien (MAC-Timestamps!)
    - /dev/mem
    - /etc/passwd
    - /var/run/utmp
    - /var/log/wtmp
  
- Mitte 2008 wird eine komplett aktualisierte Version veröffentlicht:



# Live Response mit der ForensiX-CD

```

root@banana: ~/case-mulga-01234
file Edit View Terminal Tabs Help

Ermittersystem

root@banana:~# mkdir case-mulga-01234
root@banana:~# cd case-mulga-01234/
root@banana:~/case-mulga-01234# nc -v -l -p 5556
listening on [any] 5556 ...

root@banana:~/case-mulga-01234# nc -v -l -p 5556 > mulga-ir-log-2905.log
listening on [any] 5556 ...

```



Verdächtiges System

```

bin-x86-2.4/bash ~ $ ./ir-linux.sh
Usage: bash ./ir-linux.sh <host> <port>
       or: bash ./ir-linux.sh <outputfilename>
bin-x86-2.4/bash ~ $ ./ir-linux.sh 172.23.17.128 5556
=== Start of ir-linux.sh Version 0.3 $Revision: 1.29 $

Available options:
checksum  Checksum every external command with 'sha256sum -b' (which is
           also external) before running it.
date      Run 'date' before every command to log exact start times. If
           not set, only start and end times of the script will be logged.
kmem      Dump kernel memory from /dev/kmem (may not work, may only dump
           the first Mbyte, may in rare cases hang the system)
kmemfirst Because the memory dump may hang, it is executed last.
           With this option, it is executed first to preserve as much
           information as possible.
procmem   Dump process memory. Takes a long time. May hang in rare cases
           if executed under X11.

Current options: >checksum date procmem kmem<
Enter option to toggle or press enter to continue> kmemfirst
Current options: >checksum date procmem kmem kmemfirst<
Enter option to toggle or press enter to continue> _

```

# Live Response mit der ForensiX-CD



```
bin-x86-2.4/bash ~ $ ./ir-linux.sh
Usage: bash ./ir-linux.sh <host> <port>
or: bash ./ir-linux.sh <outputfilename>
bin-x86-2.4/bash ~ $ ./ir-linux.sh 172.23.17.128 5556
=== Start of ir-linux.sh Version 0.3 $Revision: 1.29 $
```

## Available options:

```
checksum Checksum every external command with 'sha256sum -b' (which is
also external) before running it.
date Run 'date' before every command to log exact start times. If
not set, only start and end times of the script will be logged.
kmem Dump kernel memory from /dev/kmem (may not work, may only dump
the first Mbyte, may in rare cases hang the system)
kmemfirst Because the memory dump may hang, it is executed last.
With this option, it is executed first to preserve as much
Information as possible.
procmem Dump process memory. Takes a long time. May hang in rare cases
if executed under X11.
```

```
Current options: >checksum date procmem kmem<
```

```
Enter option to toggle or press enter to continue> kmemfirst
```

```
Current options: >checksum date procmem kmem kmemfirst<
```

```
Enter option to toggle or press enter to continue> _
```

```
=== Start of ir-linux.sh Version 0.3 $Revision: 1.29 $
=== CMD: ./ir-linux.sh 172.23.17.128 5556
=== BASH: /mnt/ir/linux/bin-x86-2.4/bash
=== PATH: /mnt/ir/linux/bin-x86-2.4
=== SCRIPTDIR: ./
=== OPTIONS: checksum date procmem kmem kmemfirst
=== OUTPUT: remote /dev/tcp/172.23.17.128/5556
```

```
Start TCP listener on target host 172.23.17.128 port 5556:
```

```
e.g.: # nc -l [-p] 5556 | tee logfile.out
```

```
Press Enter to start>
```

```
I> Date/Time: Script started
```

```
I> Selfcheck: SHA256sums
```

```
=== CMD: ./ir-linux.sh 172.23.17.128 5556
=== BASH: /mnt/ir/linux/bin-x86-2.4/bash
=== PATH: /mnt/ir/linux/bin-x86-2.4
=== SCRIPTDIR: ./
=== OPTIONS: checksum date procmem kmem kmemfirst
=== OUTPUT: remote /dev/tcp/172.23.17.128/5556
```

```
Start TCP listener on target host 172.23.17.128 port 5556:
```

```
e.g.: # nc -l [-p] 5556 | tee logfile.out
```

```
Press Enter to start>
```

```
I> Date/Time: Script started
```

```
I> Selfcheck: SHA256sums
```

```
I> Basics: Hostname
```

```
I> Basics: System date and uptime
```

```
I> Kernel: Kernel version
```

```
I> Basics: Loadavg
```

```
I> Basics: Script environment
```

```
I> Kernel: Dmesg output
```

```
I> Kernel: Kernel meminfo
```

```
==> Error running: cat /proc/vmstat (Exit code: 1)
```

```
I> Kernel: Memory dump allowed? (devmem_is_allowed should appear when yes)
```

```
==> Error running: grep devmem /proc/kallsyms (Exit code: 2)
```

```
I> Kernel: Base memory dump (dd if=/dev/mem)
```

```
I> Hardware: Hardware info and devices
```

```
I> Userinfo: User mappings and logins (reads /etc/passwd, utmp and wtmp)
```

```
I> Processes: Running processes by /proc (some errors are expected)
```

```
==> Error running: ls -nN /proc/12 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/1595 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/1596 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/2 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/3 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/304 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/4 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/5 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/6 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/7 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/799 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/8 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/800 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/801 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/802 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/803 (Exit code: 1)
```

```
==> Error running: ls -nN /proc/805 (Exit code: 1)
```

```
I> Processes: Process memory dump
```

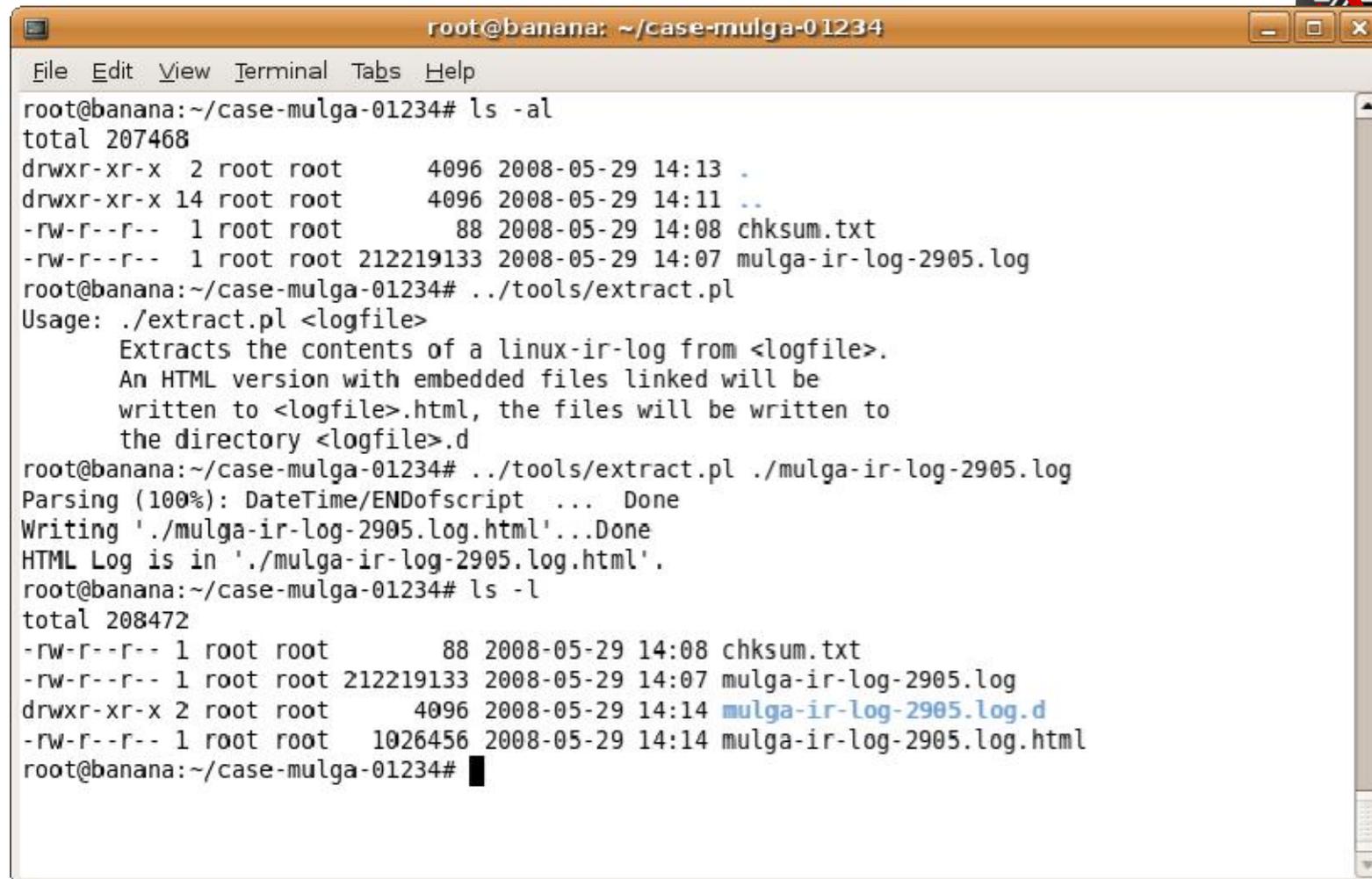
```
I> Date/Time: END of main part - start of additional tests (may hang)
```

```
I> Additional Tests: Devices (may hang)
```

```
I> Date/Time: END of script
```

```
bin-x86-2.4/bash ~ $ _
```

# Live Response mit der ForensiX-CD



```
root@banana: ~/case-mulga-01234
File Edit View Terminal Tabs Help
root@banana:~/case-mulga-01234# ls -al
total 207468
drwxr-xr-x  2 root root    4096 2008-05-29 14:13 .
drwxr-xr-x 14 root root    4096 2008-05-29 14:11 ..
-rw-r--r--  1 root root      88 2008-05-29 14:08 chksum.txt
-rw-r--r--  1 root root 212219133 2008-05-29 14:07 mulga-ir-log-2905.log
root@banana:~/case-mulga-01234# ../tools/extract.pl
Usage: ./extract.pl <logfile>
       Extracts the contents of a linux-ir-log from <logfile>.
       An HTML version with embedded files linked will be
       written to <logfile>.html, the files will be written to
       the directory <logfile>.d
root@banana:~/case-mulga-01234# ../tools/extract.pl ./mulga-ir-log-2905.log
Parsing (100%): DateTime/ENDofscript ... Done
Writing './mulga-ir-log-2905.log.html'...Done
HTML Log is in './mulga-ir-log-2905.log.html'.
root@banana:~/case-mulga-01234# ls -l
total 208472
-rw-r--r--  1 root root      88 2008-05-29 14:08 chksum.txt
-rw-r--r--  1 root root 212219133 2008-05-29 14:07 mulga-ir-log-2905.log
drwxr-xr-x  2 root root    4096 2008-05-29 14:14 mulga-ir-log-2905.log.d
-rw-r--r--  1 root root 1026456 2008-05-29 14:14 mulga-ir-log-2905.log.html
root@banana:~/case-mulga-01234#
```

[Video](#)  
[Ergebnis](#)

# Live Response mit der ForensiX-CD



Initial Response Log './mulga-ir-log-2905.log' - ir-linux.sh - Mozilla Firefox 3 Beta 5

file:///root/case/mulga\_01234/mulga\_ir\_log\_2905.log.html

Getting Started Latest - cadlines

[collapse] [expand]

Main

Date/Time

Script started

END of main part - start of additional tests (may hang)

END of script

Selfcheck

SHA256sums

basics

Features

System date and uptime

LOADAVG

Script environment

Kernel

Kernel version

Dmesg output

Kernel memory

Memory dump allowed?

(devmem\_is\_allowed should appear when yes)

Base memory dump (dd if=/dev/mem)

Kernel boot parameters

Kernel modules

Systcl. values (incl. netw crk parameters)

Kernel symbols

filesystems

Mounted filesystems and storage

Processes

Running processes overview

Running processes by /proc (some errors are expected)

Process memory dump

Network

Network interfaces

Routing and arp tables

Running network connections

Complete socket info

Hardware

Hardware info and devices

Userinfo

User mappings and logins (reads)

Initial Response Log './mulga-ir-log-2905.log' - ir-linux.sh

**ir-linux.sh** Version 0.3 \$Revision: 1.29 \$

**Command invocation** ./ir-linux.sh 172.23.17.128/5556

**bash** /mnt/ir/linux/bin-x86-2.4/bash

**PATH** /mnt/ir/linux/bin-x86-2.4

**SCRIPTDIR** ./

**Options** ochecksum date procmem knem knemfirst

**Output** /dev/tcp/172.23.17.128/5556

Date/Time

Script started

**Command:** date

**Exit status:** Success (0)

**full path** /mnt/ir/linux/bin-x86-2.4/date

**sha256sum** db74254d0233ab5d430c53f41a531b93c8a3e0e080c324db28b6106270ab7413

**date** Thu May 29 05:06:28 CEST 2008

Thu May 29 05:06:28 CEST 2008

END of main part - start of additional tests (may hang)

**Command:** date

**Exit status:** Success (0)

**full path** /mnt/ir/linux/bin-x86-2.4/date

**sha256sum** db74254d0233ab5d430c53f41a531b93c8a3e0e080c324db28b6106270ab7413

Done

## Weitere Werkzeuge



# EXT IFS

The screenshot shows the 'IFS Drives' application window. It displays three drives with their respective details:

| Drive   | Letter | File System | Size     | Mount Point | File System | Size    |
|---------|--------|-------------|----------|-------------|-------------|---------|
| Drive 1 | C:     | System NTFS | 186.3 GB |             |             |         |
| Drive 2 | D:     | Daten_NTFS  | 95.2 GB  |             |             |         |
|         | E:     | DATEN_FAT32 | 502.0 MB | (none)      | Linux swap  | 3.9 GB  |
| Drive 3 | J:     |             |          |             | Linux       | 76.9 GB |
|         | Y:     | Linux       | 186.3 GB |             |             |         |
| Drive 3 | G:     | Daten_NTFS  | 149.0 GB |             |             |         |

Legend: ■ primary partition, ■ extended partition,  free space

[www.fs-driver.org](http://www.fs-driver.org)

# Mount Image Pro

[www.getdata.com](http://www.getdata.com)

| Name                     | Typ                 | Gesamtgröße | Freier Speicher | Kommentare |
|--------------------------|---------------------|-------------|-----------------|------------|
| <b>Festplatten</b>       |                     |             |                 |            |
| System (C:)              | Lokaler Datenträger | 67,7 GB     | 58,8 GB         |            |
| Daten (D:)               | Lokaler Datenträger | 836 GB      | 525 GB          |            |
| Lokaler Datenträger (E:) | Lokaler Datenträger |             |                 |            |
| Lokaler Datenträger (G:) | Lokaler Datenträger |             |                 |            |
| Lokaler Datenträger (H:) | Lokaler Datenträger | 99,9 MB     | 19,4 MB         |            |
| forensic-test (I:)       | Lokaler Datenträger | 125 MB      | 36,0 MB         |            |
| Lokaler Datenträger (J:) | Lokaler Datenträger | 298 GB      | 23,6 GB         |            |
| Lokaler Datenträger (K:) | Lokaler Datenträger | 465 GB      | 265 GB          |            |
| Lokaler Datenträger (L:) | Lokaler Datenträger | 298 GB      | 23,6 GB         |            |
| Lokaler Datenträger (M:) | Lokaler Datenträger | 4,53 GB     | 2,86 GB         |            |

**Mount Image Pro v2.44**

File Options Help

Mount... Unmount View... Options Update Help

**Mounted Images**

| Filename   | Files | Partition | As  | Label         | File System | Date Acquired |
|--|-------|-----------|-----|---------------|-------------|---------------|
| D:\Cases\ForensiX_CD_07-07.iso                           | 1     | 0         | E:\ | (none)        | (none)      |               |
| D:\Cases\07.Test.HackingCase\Akquisition\hacking_case.dd | 1     | 0         | G:\ | (none)        | (none)      |               |
| D:\Cases\image_g_ntfs.dd                                 | 1     | 0         | H:\ |               | HPFS/NTFS   |               |
| D:\Cases\usbkey.dd                                       | 1     | 1         | I:\ | forensic-test | FAT32 LBA   |               |
| D:\Cases\images%255C4Dell Latitude CPl.E01               | 2     | 1         | M:\ |               | HPFS/NTFS   | 22.09.2004    |

**Image Details**

Filename: D:\Cases\images%255C4Dell Latitude CPl.E01

Image Geometry Encase P

| Parameter | Value   |
|-----------|---------|
| Capacity  | 4645 Mb |
| Cylinders | 593     |
| Tracks    | 255     |
| Sectors   | 63      |
| Bytes     | 512     |

| Id | Active | Media | Capacity | Label | File System |
|----|--------|-------|----------|-------|-------------|
| 0  | No     | Hard  | 4645 Mb  |       | (none)      |
| 1  | Yes    | Hard  | 4643 Mb  |       | HPFS/NTFS   |

Mounted Drives: 5

**Mount Image Pro v2**

Mount Details

Filename: D:\...\07.Test.HackingCase\Akquisition\hacking\_case.dd

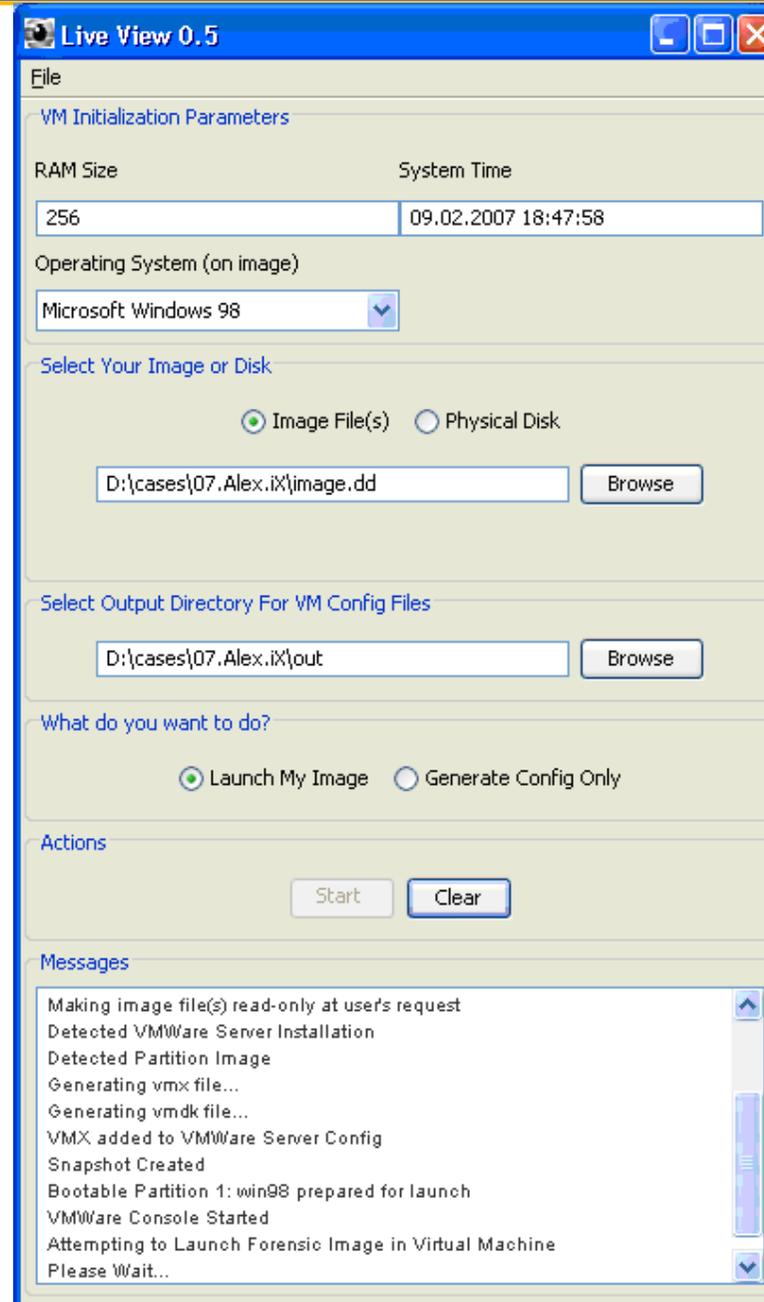
Start drive letter: First

Mount as single drive:

Ok Cancel

# Live View

<http://liveview.sourceforge.net/>



# The Sleuthkit



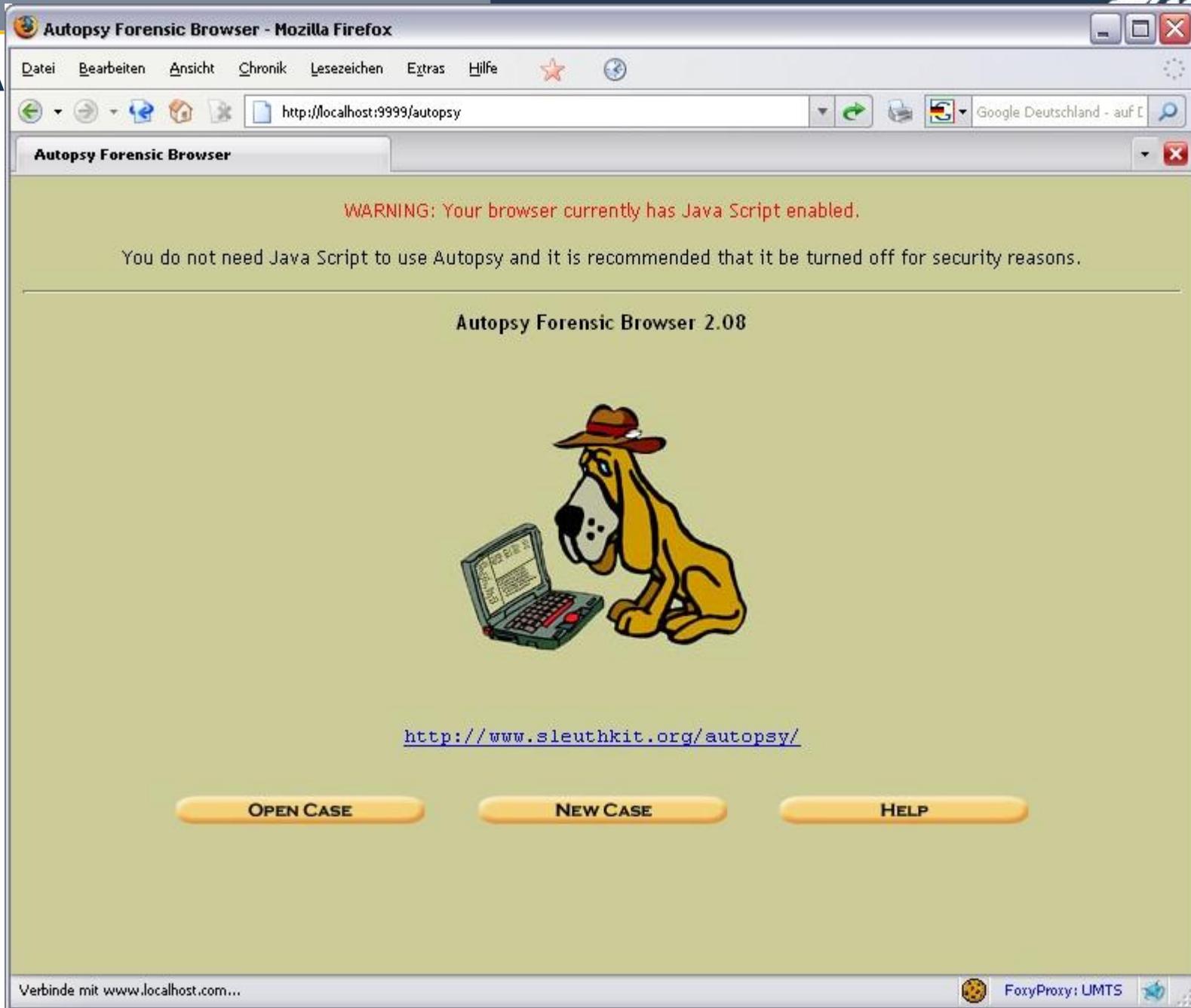
- The Sleuthkit (TSK)
  - Brian Carrier Anfang 2001
  - Sammlung von mehr als 20 Werkzeugen für die Analyse von Datenträgern und Dateisystemen
  - Werkzeuge werden in Gruppen zusammengefasst
    - Datenträger
    - Volume
    - Dateisystem
      - Struktur und Größen Informationen des Dateisystems
      - Dateinamen
      - Metadaten
      - Daten
    - Suchwerkzeuge

# Autopsy



- Autopsy
  - Graphische Oberfläche für TSK
    - HTML basiert
  - Post-Mortem-Analyse möglich
  - Perl-Programm
  - Analyse per Browser
  - Protokollierung aller Analyseschritte
  - Zugriffsschutz mittels Cookie und Beschränkung auf konfigurierbaren Port
  - Bestandteil vieler forensischer Live-CD's

A



# Autopsy

Seminar:host1:vol2 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:9999/autopsy?mod=1&submod=2&case=Seminar&host=host1&inv

e-fense™ Helix™ forensics ids wireless pen test crypto sniffers firewalls

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

Directory Seek

Enter the name of a directory that you want to view.  
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

| DEL | Type   | NAME                      | WRITTEN                      | ACCESSED                     | CREATED                      | SIZE   | UID | GID | META |
|-----|--------|---------------------------|------------------------------|------------------------------|------------------------------|--------|-----|-----|------|
| d/d | dir/in | ../                       | 0000.00.00<br>00:00:00 (UTC) | 0000.00.00<br>00:00:00 (UTC) | 0000.00.00<br>00:00:00 (UTC) | 2048   | 0   | 0   | 2    |
| d/d | dir/in | ./                        | 2006.07.21<br>10:26:28 (MDT) | 2006.07.21<br>00:00:00 (MDT) | 2006.07.21<br>10:26:26 (MDT) | 2048   | 0   | 0   | 4    |
| r/r | file   | <u>eiger_original.exe</u> | 2006.07.18<br>14:27:32 (MDT) | 2006.07.21<br>00:00:00 (MDT) | 2006.07.21<br>10:26:26 (MDT) | 421216 | 0   | 0   | 71   |
| r/r | file   | <u>evidence.txt</u>       | 2006.07.18<br>14:29:22 (MDT) | 2006.07.21<br>00:00:00 (MDT) | 2006.07.21<br>10:26:26 (MDT) | 53     | 0   | 0   | 72   |
| r/r | file   | <u>adk-1.3.dll</u>        | 2006.07.21<br>10:26:26 (MDT) | 2006.07.21<br>00:00:00 (MDT) | 2006.07.21<br>10:26:26 (MDT) | 428431 | 0   | 0   | 74   |

ASCII ([display - report](#)) \* ASCII Strings ([display - report](#)) \* [Export](#) \* [View](#) \* [Add Note](#)

File Type: GIF image data, version 87a, 1024 x 682

C:/stegdetect/eiger\_original.exe

Thumbnail: [View Full Size Image](#)



http://localhost:9999/autopsy?mod=2&view=8&case=Seminar&host=host1&inv=Sebastian&vol=vol2&meta=71&sort=2&dir=/stegdetect/eiger\_original...

# Autopsy



## ■ Case Management

- Verschiedene Fälle werden separat verwaltet
- Pro Fall beliebige Host-Systeme
- Jedem Host werden Images zugeordnet
- Pro Host mehrere 'Investigators' möglich
- Individuelle Einstellungen für Zeitzone und Hashdatenbanken
- Eigene Kommentare pro Investigator
- Analyse-Ergebnisse werden in ASCII-Dateien gespeichert
- Damit einfache Archivierung kompletter Fälle

## ■ Nachfolger PTK

- Ab Final geplant ab 09 / 08
- Ajax basiert
- zentrale Datenbank
- Index
- <http://ptk.dflabs.com>

# PTK

Case: test01 | Image: img04
Investigator: admin [home | logout]

File analysis

Timeline

Keyword search

Image details

[X] Close analysis

- img04
  - My Documents
  - My Pictures
  - My Music
  - Accounts
    - Filters
    - Data
    - Bin
    - Hidden Stuff
    - Logos
    - Lottery Balls
    - Police

|                          | Permissions  | Name               | Written             | Accessed            | Created             | Size    | UID | GID | Meta   |  |
|--------------------------|--------------|--------------------|---------------------|---------------------|---------------------|---------|-----|-----|--------|--|
| <input type="checkbox"/> | -/-rwxrwxrwx | <u>account.dll</u> | 2002-08-01 18:59:38 | 2003-01-13 00:00:00 | 2003-01-13 21:16:30 | 144354  | 0   | 0   | 383029 |  |
| <input type="checkbox"/> | -/-rwxrwxrwx | <u>company.vxd</u> | 2002-08-01 19:00:54 | 2003-01-13 00:00:00 | 2003-01-13 21:16:32 | 2359350 | 0   | 0   | 383030 |  |
| <input type="checkbox"/> | -/-rwxrwxrwx | <u>Credit.dll</u>  | 2002-08-01 19:00:16 | 2003-01-13 00:00:00 | 2003-01-13 21:16:36 | 106482  | 0   | 0   | 383032 |  |
| <input type="checkbox"/> | -/-rwxrwxrwx | <u>debit.dll</u>   | 2002-08-01 19:02:32 | 2003-01-13 00:00:00 | 2003-01-13 21:16:36 | 150184  | 0   | 0   | 383033 |  |
| <input type="checkbox"/> | -/-rwxrwxrwx | <u>log.dat</u>     | 2002-08-01 19:01:40 | 2003-01-13 00:00:00 | 2003-01-13 21:16:38 | 471015  | 0   | 0   | 383034 |  |
| <input type="checkbox"/> | -/-r-xr-xr-x | <u>Thumbs.db</u>   | 2002-08-01 21:58:04 | 2003-01-13 00:00:00 | 2003-01-13 21:16:38 | 183808  | 0   | 0   | 383036 |  |

Credit.dll

Ascii
Hex
Ascii strings
Image preview
Export

JPEG image data, JFIF standard 1.01

# PTK

Case: test01 | Image: img1 Investigator: admin [home] [logout]

| File analysis   | Timeline                 | Image details                                    | [X] Close analysis                                |                     |                     |                     |          |   |    |    |  |
|---|--------------------------|--|---|---------------------|---------------------|---------------------|----------|---|----|----|--|
| <ul style="list-style-type: none"> <li>img1               <ul style="list-style-type: none"> <li>partition-0 [fat16]                   <ul style="list-style-type: none"> <li>.Trash-utente</li> <li>_ARTEL~1</li> <li>folder1</li> <li>cartella senza nome</li> <li>folder2                       <ul style="list-style-type: none"> <li>cartella senza nome</li> <li>folder2.1</li> <li>PsTools</li> <li>_IA</li> <li>_W600~1.14</li> <li>NW 6.0.0.14 Gold</li> <li>Net-DNS-Fingerprint-0.9.3</li> <li>Nessus</li> <li>materiale</li> </ul> </li> <li>partition-1 [linux-ext3]                       <ul style="list-style-type: none"> <li>lost+found</li> </ul> </li> </ul> </li> </ul> </li> </ul> | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">icmpquery.c</a>                       | 2007-04-21 16:11:50 | 2007-04-21 00:00:00 | 2007-04-21 16:12:30 | 13855    | 0 | 0  | 46 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">icmpquery.o</a>                       | 2007-04-21 16:13:32 | 2007-04-21 00:00:00 | 2007-04-21 16:13:42 | 13709    | 0 | 0  | 48 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">_d5sum.exe</a>                        | 2004-09-03 22:34:46 | 2007-07-30 00:00:00 | 2007-04-26 15:27:58 | 17408    | 0 | 0  | 51 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">_d5lib.dll</a>                        | 2004-09-03 22:34:46 | 2007-07-30 00:00:00 | 2007-04-26 15:31:14 | 14848    | 0 | 0  | 52 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">etopt.dll</a>                         | 2004-09-03 19:34:46 | 2007-07-30 00:00:00 | 2007-04-26 15:32:16 | 9216     | 0 | 0  | 53 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">_SVC70_DLL</a>                        | 2002-01-05 15:40:00 | 2007-07-30 00:00:00 | 2007-04-26 15:32:16 | 487424   | 0 | 0  | 54 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">_svcr70.dll</a>                       | 2002-01-05 15:37:00 | 2007-07-30 00:00:00 | 2007-04-26 15:32:16 | 344064   | 0 | 0  | 55 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">zlibU.dll</a>                         | 2004-09-03 22:34:46 | 2007-07-30 00:00:00 | 2007-04-26 15:32:16 | 51200    | 0 | 0  | 57 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">_zip.exe</a>                          | 2007-04-03 13:12:00 | 2007-07-30 00:00:00 | 2007-04-26 15:43:16 | 68096    | 0 | 0  | 58 |  |
|   | <input type="checkbox"/> | -/-r-xr-xr-x                                     | <a href="#">SDELTEMP1</a>                         | 2008-02-20 12:25:52 | 2008-02-20 00:00:00 | 2008-02-20 12:25:50 | 0        | 0 | 0  | 64 |  |
|   | <input type="checkbox"/> | -/-r-xr-xr-x                                     | <a href="#">SDELMFT000000</a>                     | 2008-02-20 12:25:52 | 2008-02-20 00:00:00 | 2008-02-20 12:25:50 | 0        | 0 | 0  | 66 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">PTK_presentazione_1.1.ppt</a>         | 2008-02-20 16:21:46 | 2008-02-21 00:00:00 | 2008-02-20 16:45:56 | 30493184 | 0 | 0  | 69 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">PTK_presentazione_1.1.ppt</a>         | 2008-02-20 16:21:46 | 2008-02-27 00:00:00 | 2008-02-20 16:45:56 | 30497280 | 0 | 0  | 72 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">ScreenHunter_01_Feb._21_18.19.bmp</a> | 2008-02-21 18:19:08 | 2008-03-04 00:00:00 | 2008-02-21 18:27:34 | 3394614  | 0 | 0  | 76 |  |
|   | <input type="checkbox"/> | -/-rwxrwxrwx                                     | <a href="#">ScreenHunter_02_Feb._21_18.19.bmp</a> | 2008-02-21 18:19:42 | 2008-03-04 00:00:00 | 2008-02-21 18:27:36 | 3394614  | 0 | 0  | 80 |  |
| <input type="checkbox"/>  | -/-rwxrwxrwx             | <a href="#">PTK_presentazione_Università.ppt</a> | 2008-02-21 20:03:10                               | 2008-02-27 00:00:00 | 2008-02-21 20:04:44 | 30512640            | 0        | 0 | 84 |    |  |
| <input type="checkbox"/>  | -/-rwxrwxrwx             | <a href="#">PTK_presentazione_Università.pps</a> | 2008-02-21 20:04:12                               | 2008-02-21 00:00:00 | 2008-02-21 20:04:48 | 24101376            | 0        | 0 | 88 |    |  |

**template\_PTK\_ENG.txt**

ASCII English text, with CRLF line terminators

As known, PTK - The Alternative Sleuthkit Interface - has been presented at DoD Cybercrime Conference 2008 in St. Louis. Destined to become one of the most important of the international scene, PTK is an Open Source project, planned and developed by the IRItaly team, including Dario Forte and students, Graduate and Post Graduate, at University of Milano DTI.

In order to provide detailed informations about this project, IRItaly Team and DFLabs organized a Webex on February 21, 2008, at 5:00 PM CET. The webex will be 1,30h long, and will include all the details related to the PTK project. The presentation will be held by Dario Forte and the IRItaly Team at University of Milano DTI.

The attendees (the webcast is free) will be able to send questions about the project, which put the premises to become one of the most interesting tool in the field, with the main goal of furtherly valorize the SleuthKit, with several enhancements and with a most effective interface. PTK will be released soon, after a strong alpha and beta testing program. The source code will be freely available.

Space is limited. To reserve your seat now, just browse to the following link. complete the registration form and enter the password shown below:

ptk.dflabs.com

# Vielen Dank für die Aufmerksamkeit! Fragen ?

**Alexander Geschonneck**

<http://computer-forensik.org>  
alexander @ geschonneck . com