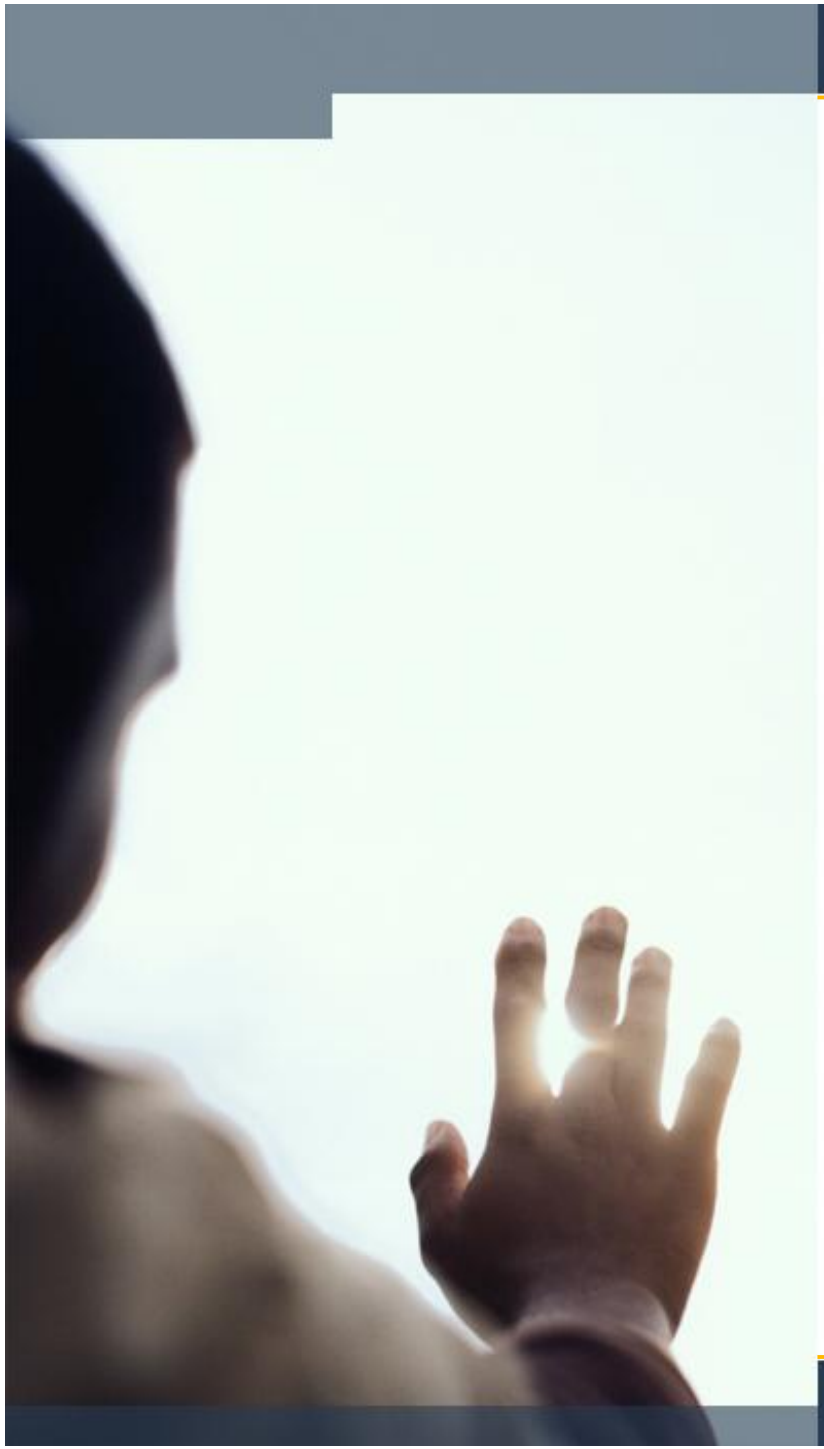


Linux in der Computer-Forensik

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

Hisolutions

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[1] (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 entstanden Schadens nach einem Systemeinbruch,
- Identifikation des Angreifers,
- Sicherung der Beweise für weitere juristische Aktionen.

[1] 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)

©Darren Harlow, Computer Forensics 101

Welche Daten können gesammelt werden?

Unabhängig von der konkreten Fragestellung und dem zu untersuchenden System (Serve 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 Halbwertzeit 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 Betriebssystems 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

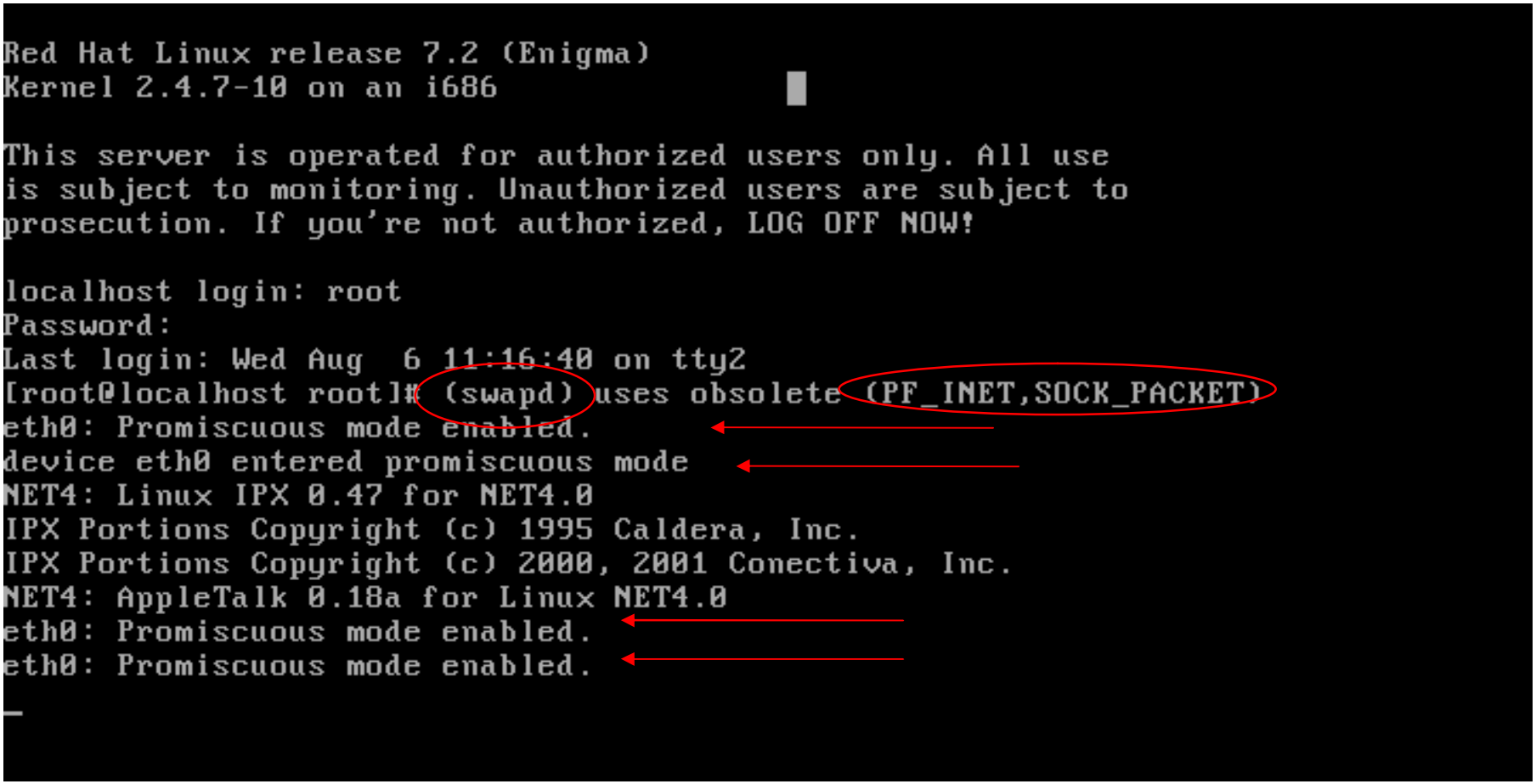
Modification-, **A**ccess- and **C**hange-Time unter Linux

- 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 lsof!

Beispiel



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

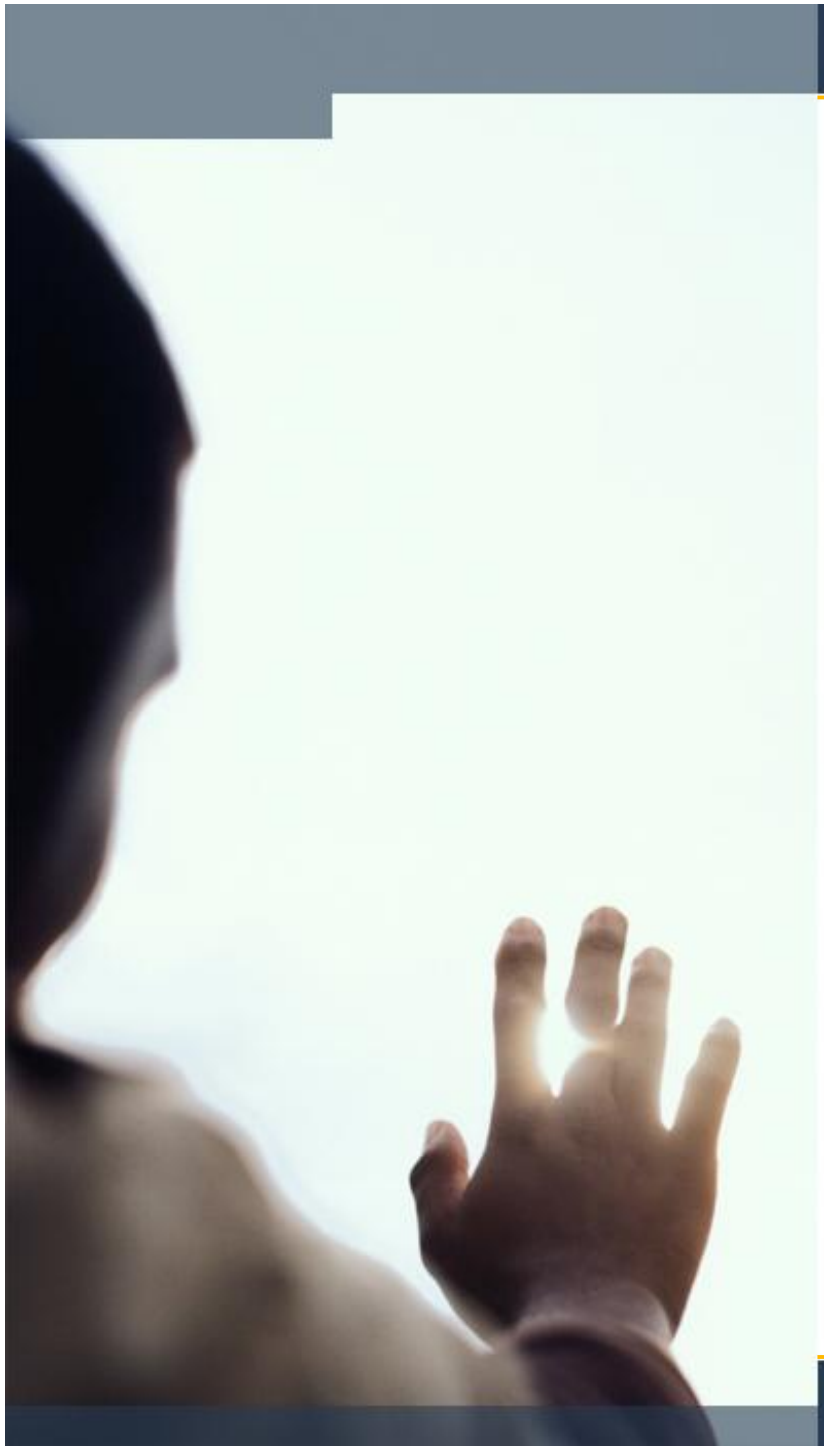
Beispiel

```
[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)
  - DCCIdd (Nur auf Anfrage beim DoD Cyber Crime Center)
  - Dc3dd (Patch für dd, http://dc3dd.sourceforge.net/)
- Diverse grafische Tools
  - GRAB
  - Adepto
  - LinEn
  - SMART
  - GYMAGER

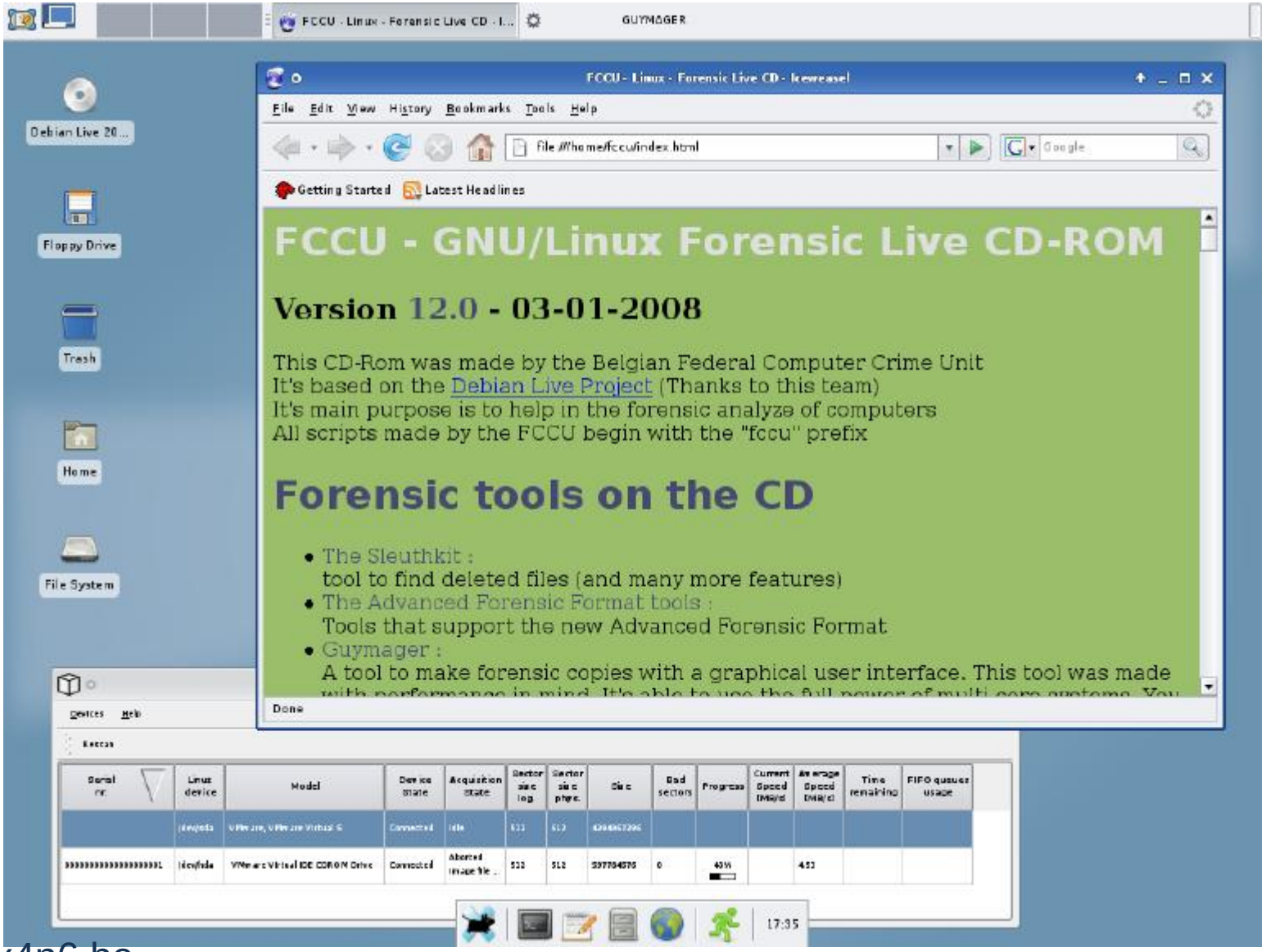


Linux Live CDs

FCCU

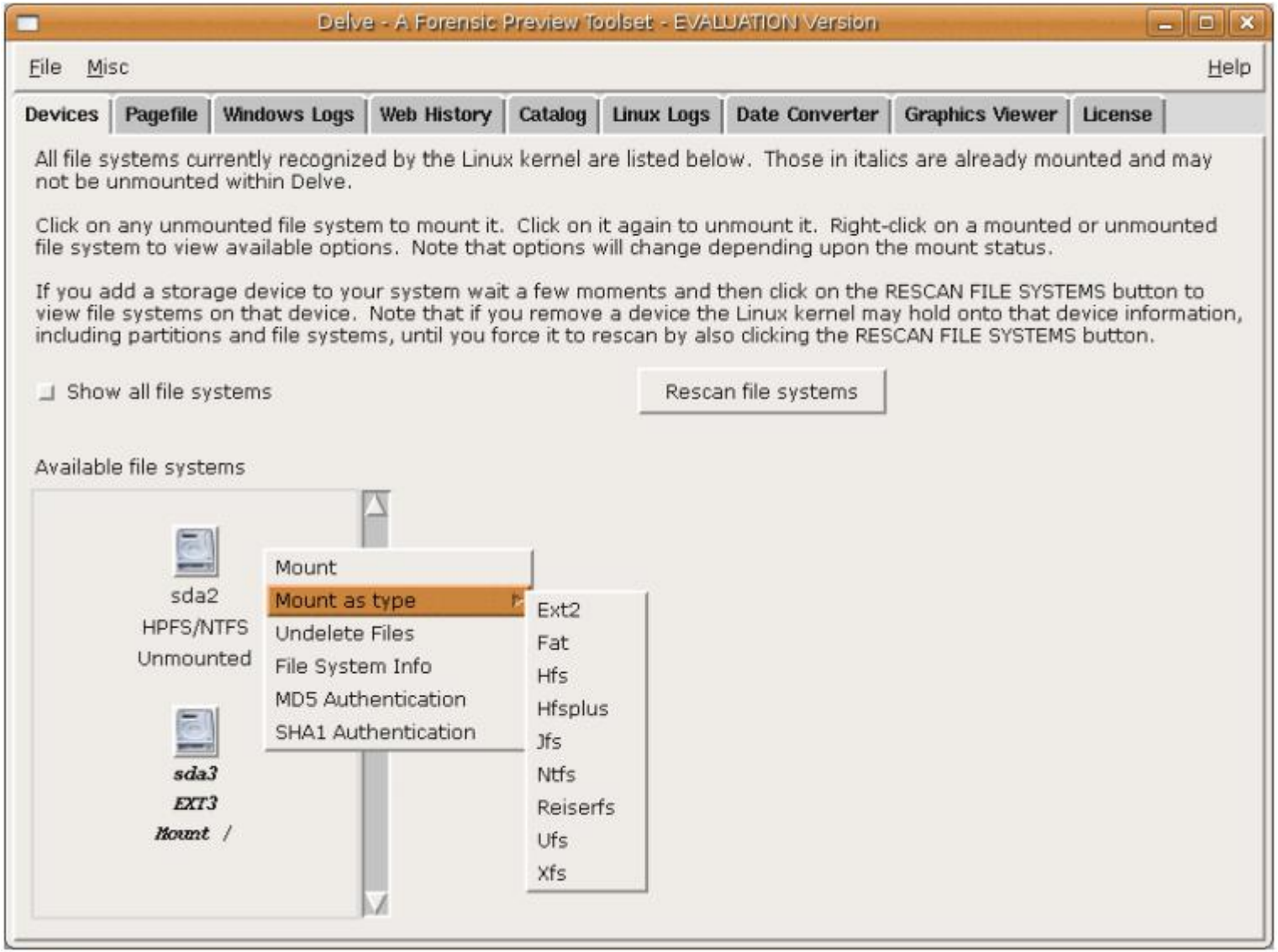
www.lnx4n6.be

FCCU



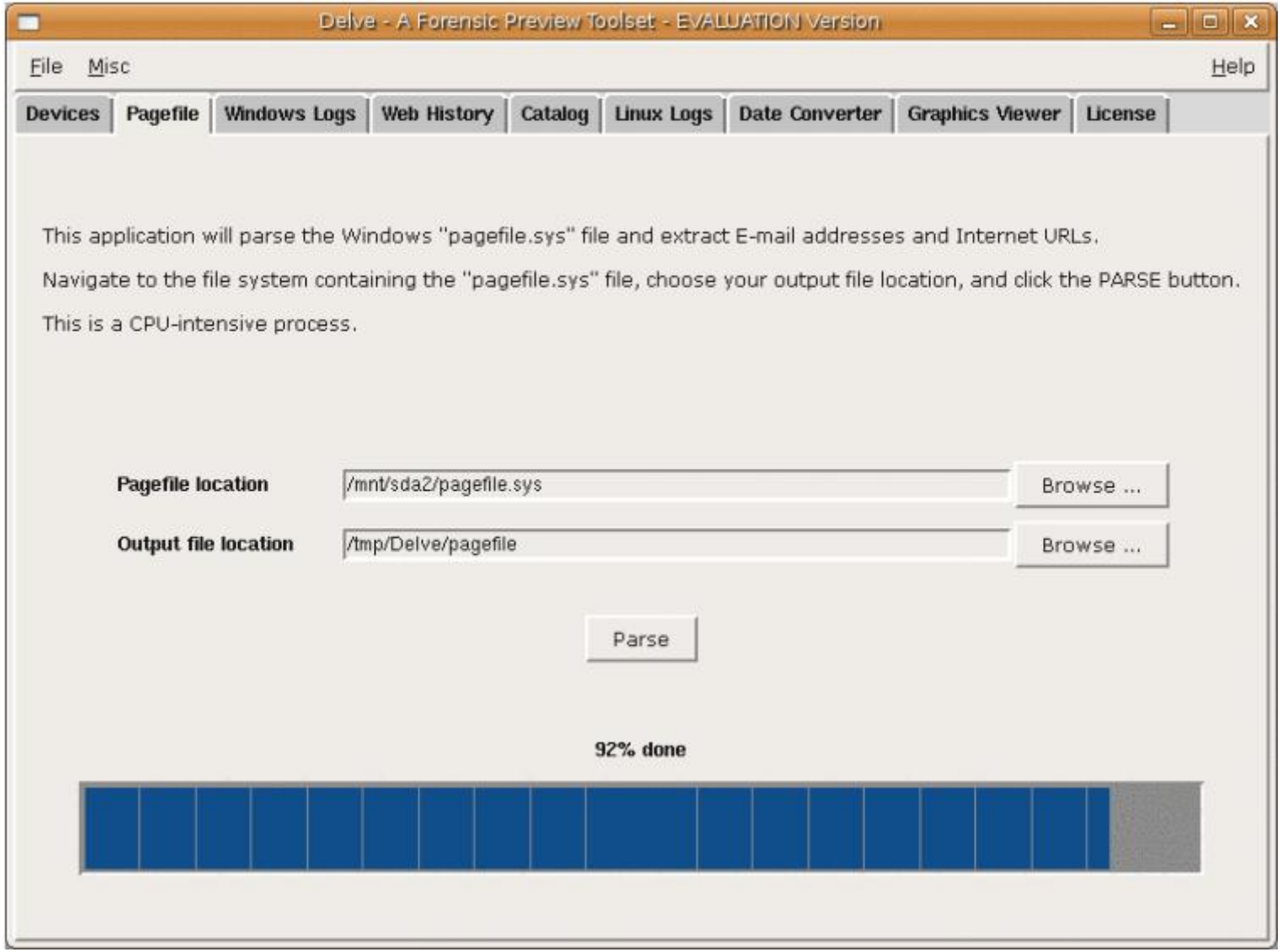
www.lnx4n6.be

THE FARMER'S BOOT CD



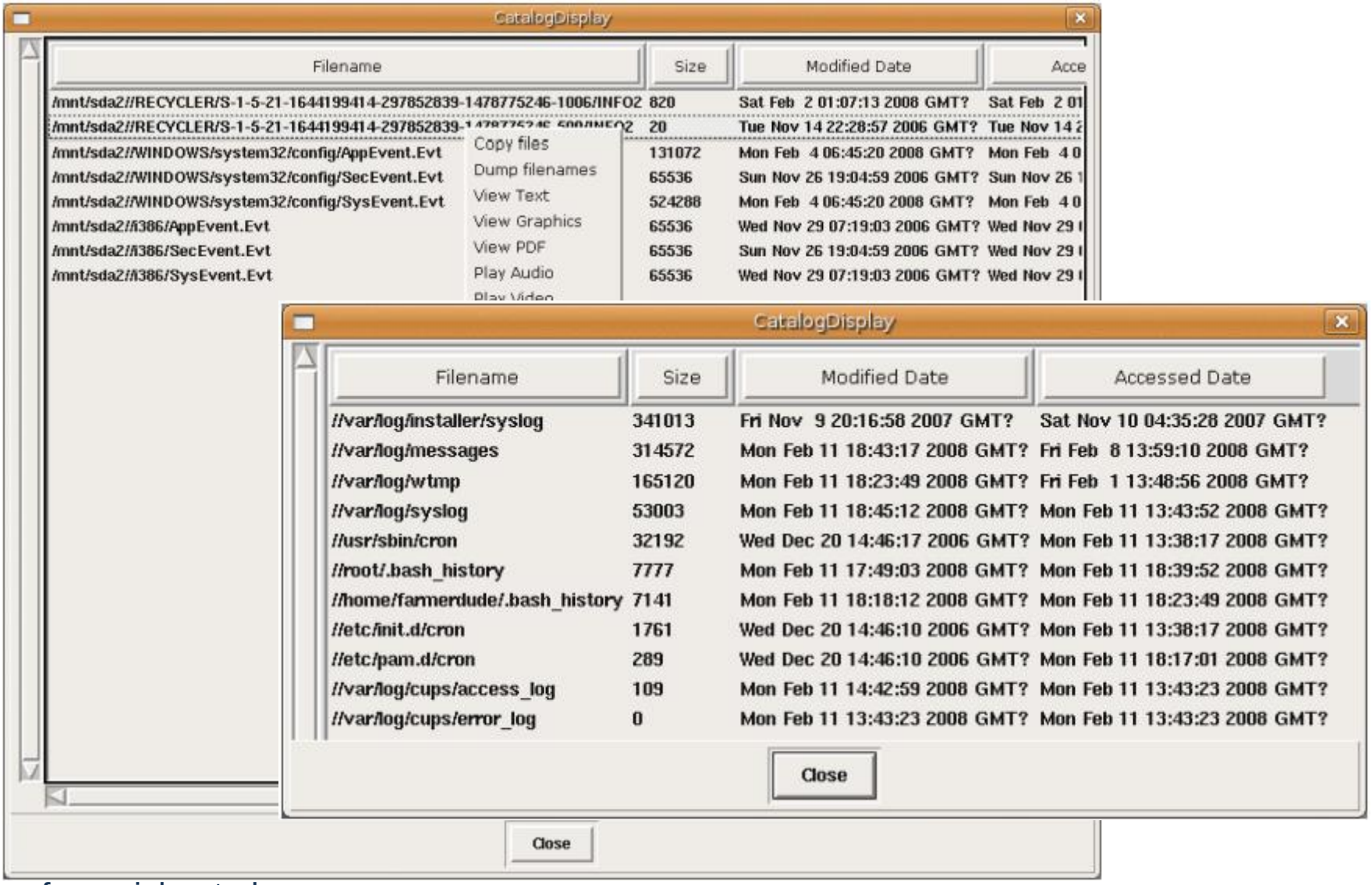
www.forensicbootcd.com

THE FARMER'S BOOT CD



www.forensicbootcd.com

THE FARMER'S BOOT CD

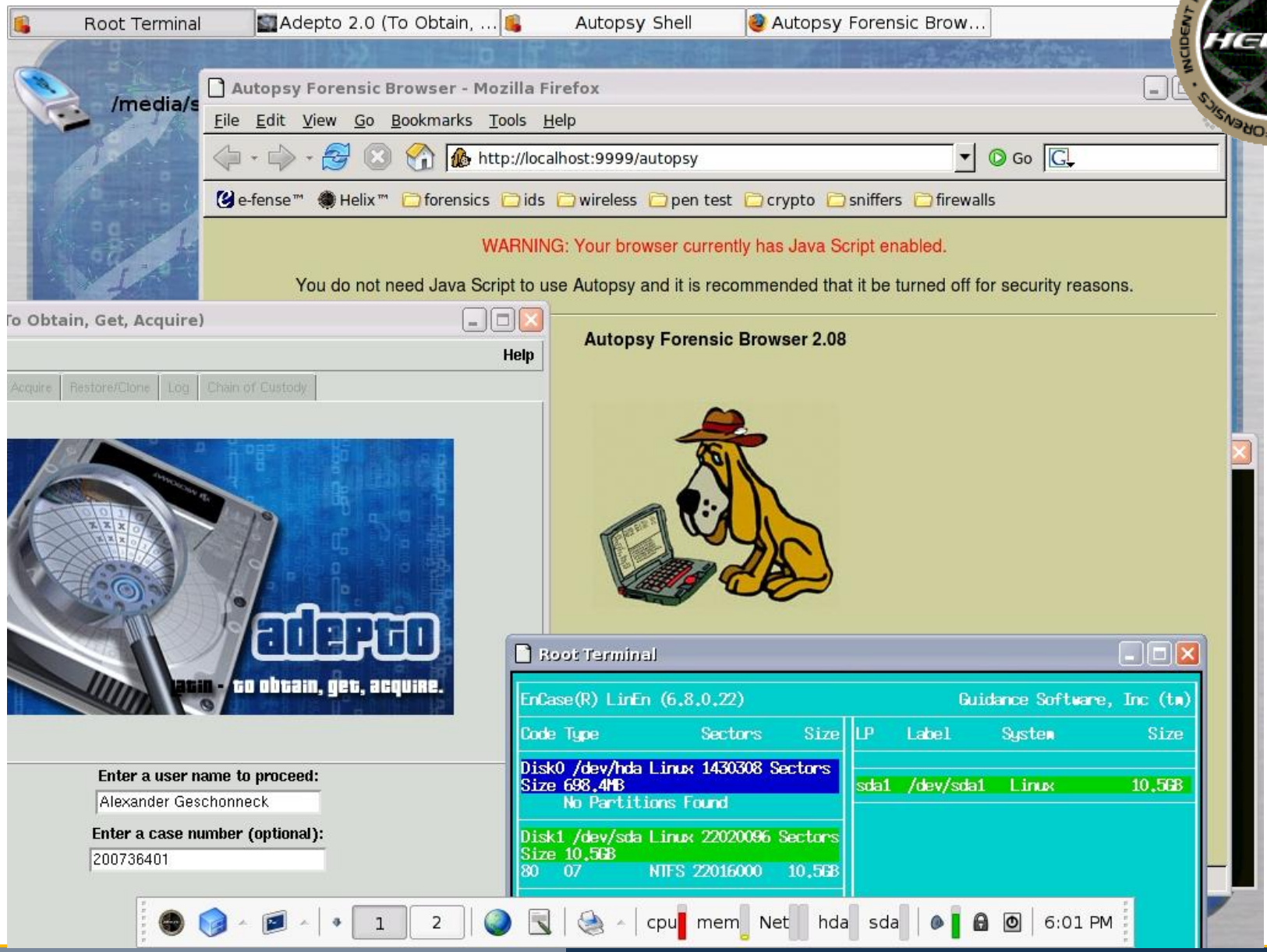


www.forensicbootcd.com

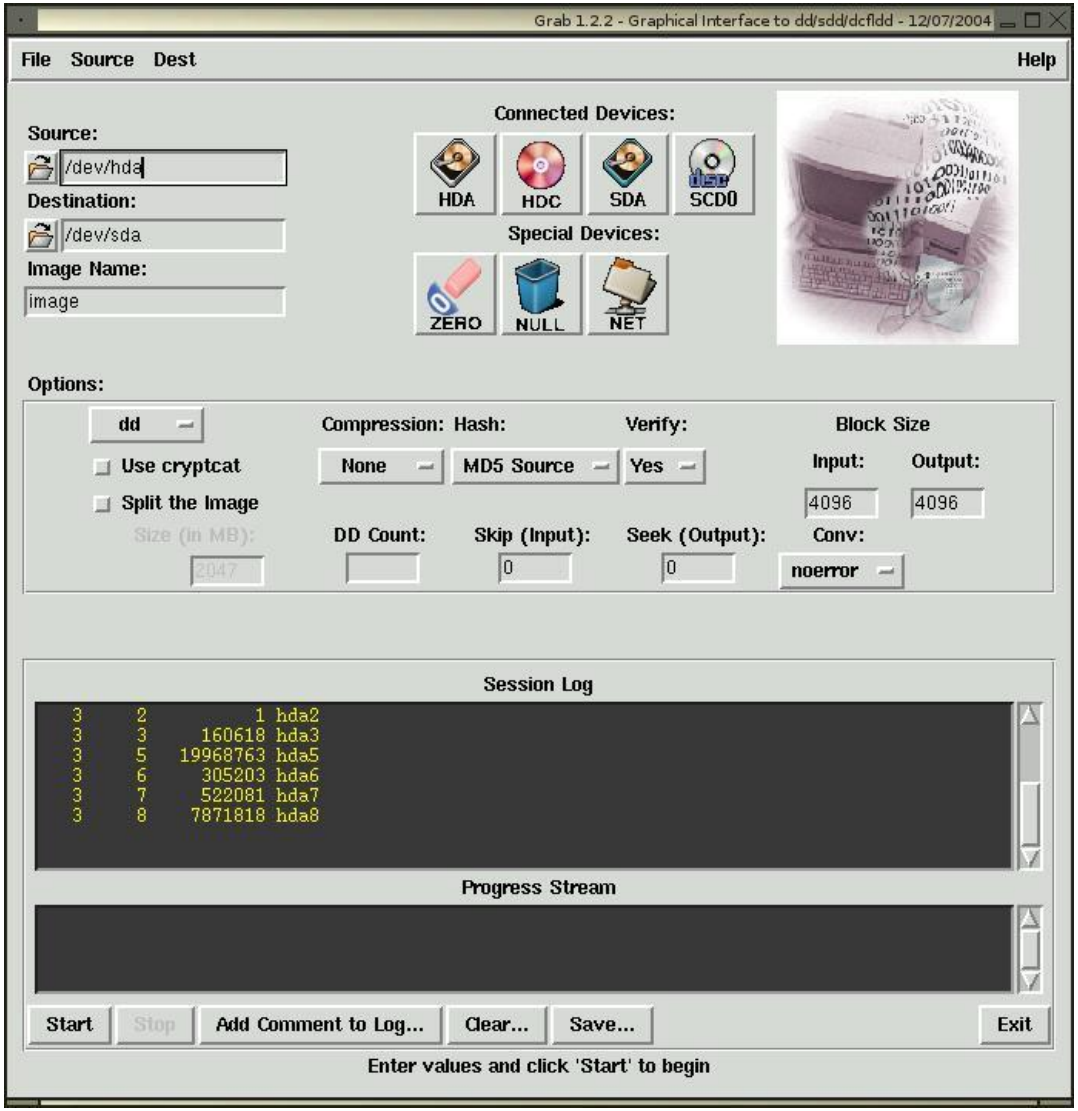
Helix

www.e-fense.com

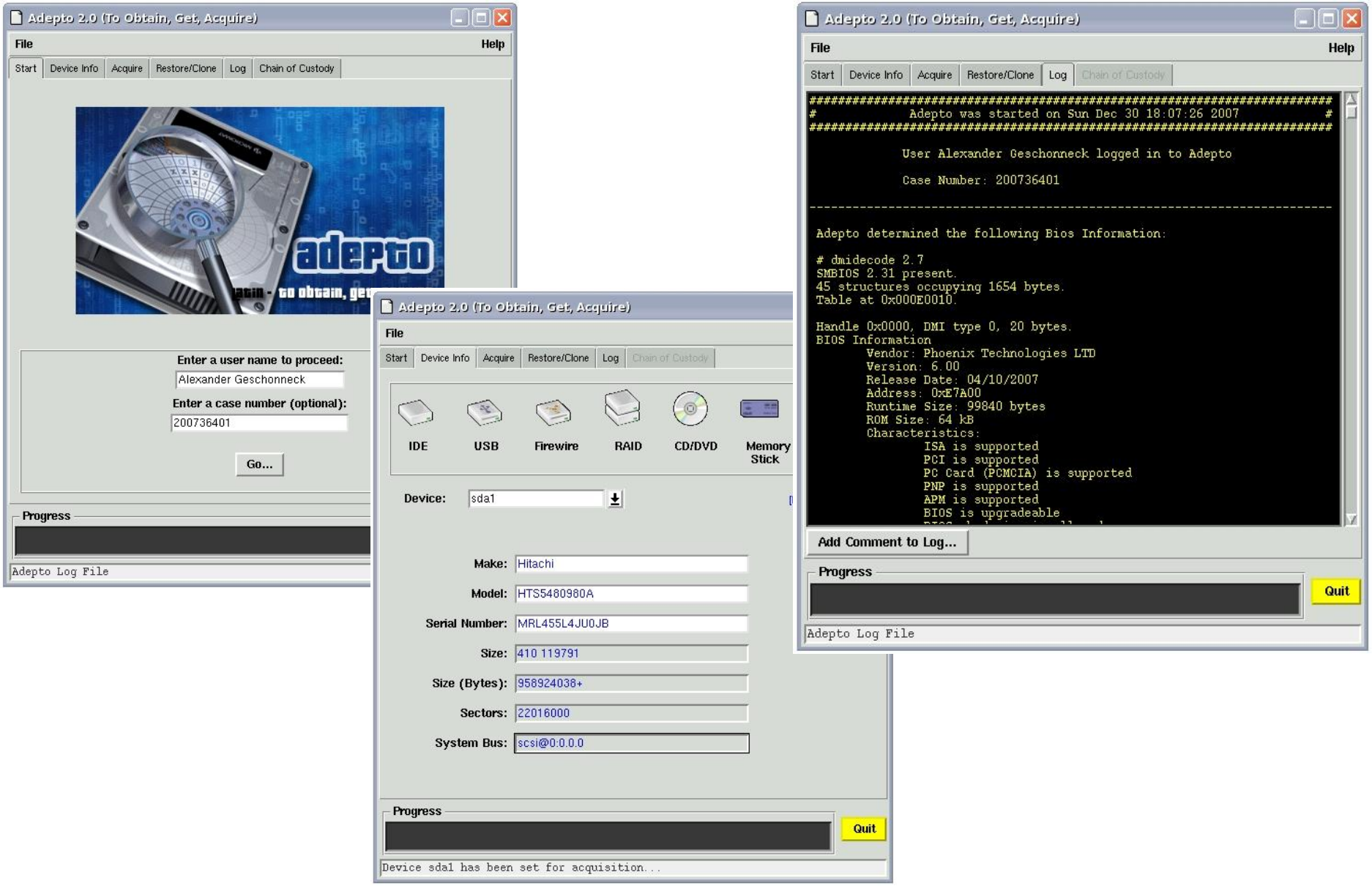
Helix



Grab

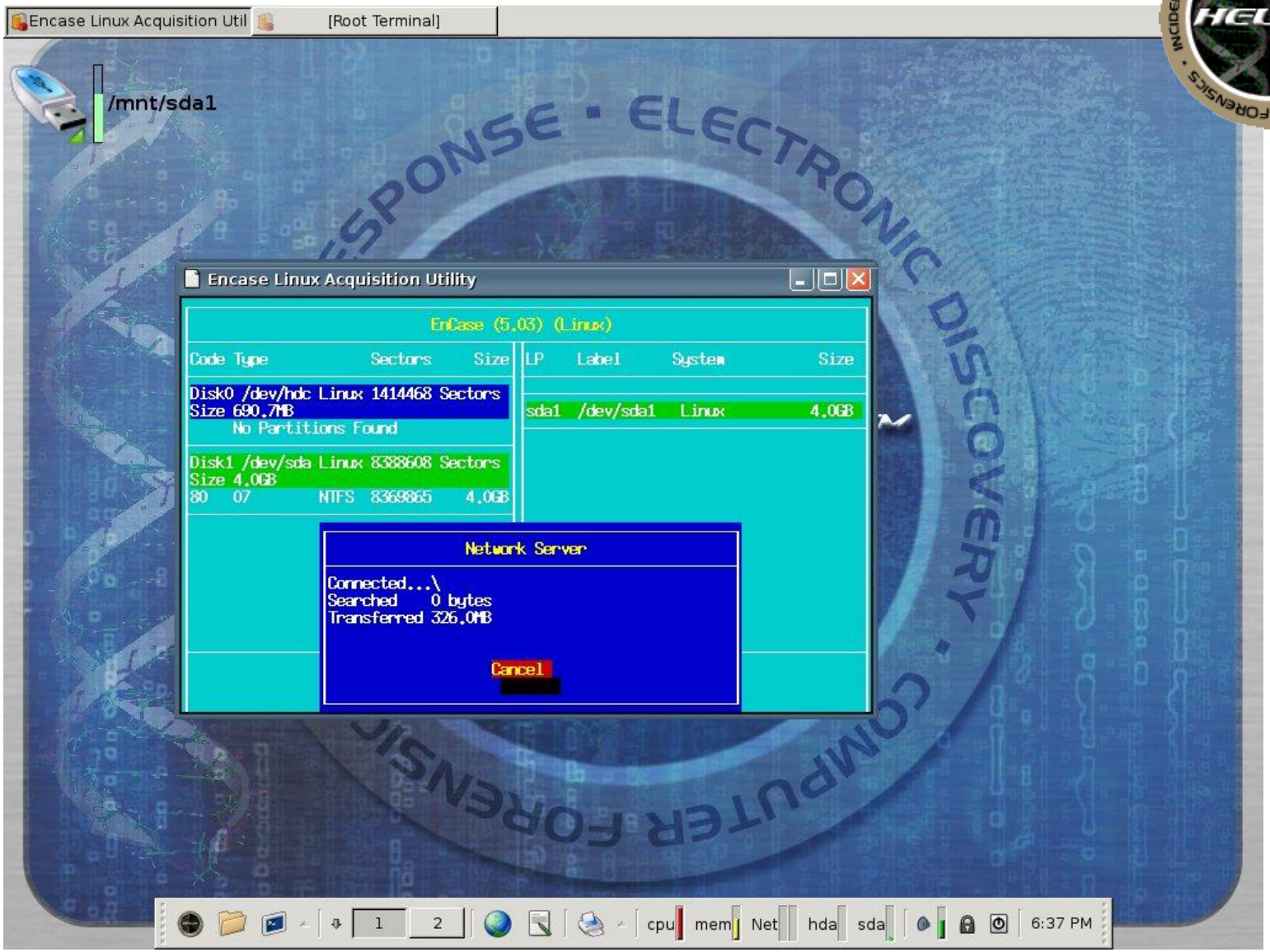


Adepto



EnCase für Linux

Helix



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

Ermittlersystem

```
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 Edit View History Bookmarks Tools Help

file:///root/case_mulga_01234/mulga_ir_log_2905.log.html

Getting Started Latest Headlines

[collapse] [expand]

Main
Date/Time
Script started
END of main part - start of additional tests (may hang)
END of script
Selfcheck
SHA256sums
Basics
Hostname
System date and uptime
Loadavg
Script environment
Kernel
Kernel version
Dmesg output
Kernel meminfo
Memory dump allowed? (devmem_is_allowed should appear when yes)
Base memory dump (dd if=/dev/mem)
Kernel boot parameters
Kernel modules
Sysctl values (incl. network 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	checksum date procmem kmem kmemfirst
Output	/dev/tcp/172.23.17.128/5556

Date/Time

Script started

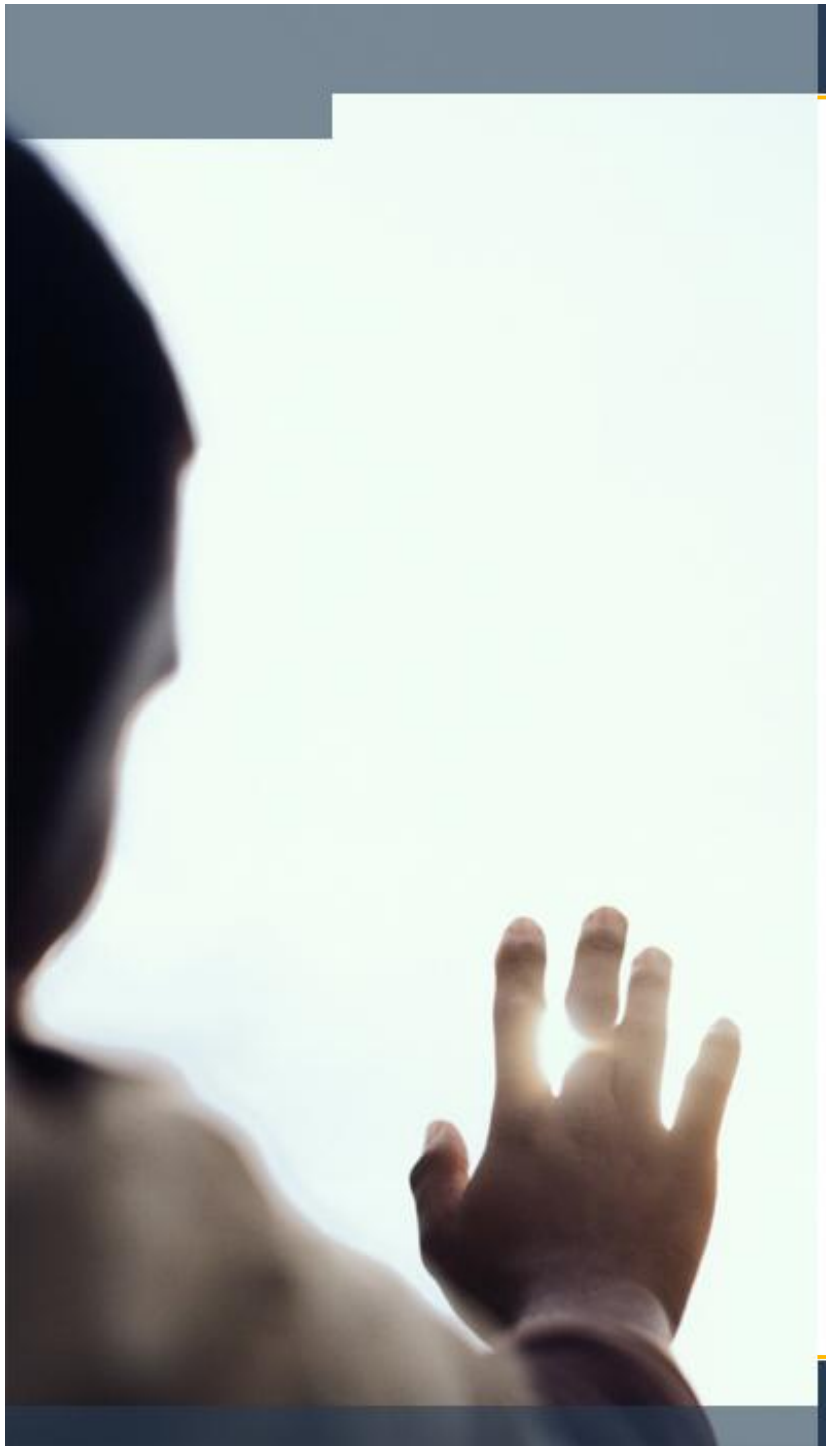
Command:	date
Exit status:	Sucess (0)
full path	/mnt/ir/linux/bin-x86-2.4/date
sha256sum	db74254d0233ab5d430c53f41a551b93c8a3e0e080c324db28b6106270ab7413
date	Thu May 29 05:06:28 CEST 2008

Thu May 29 05:06:28 CEST 2008

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

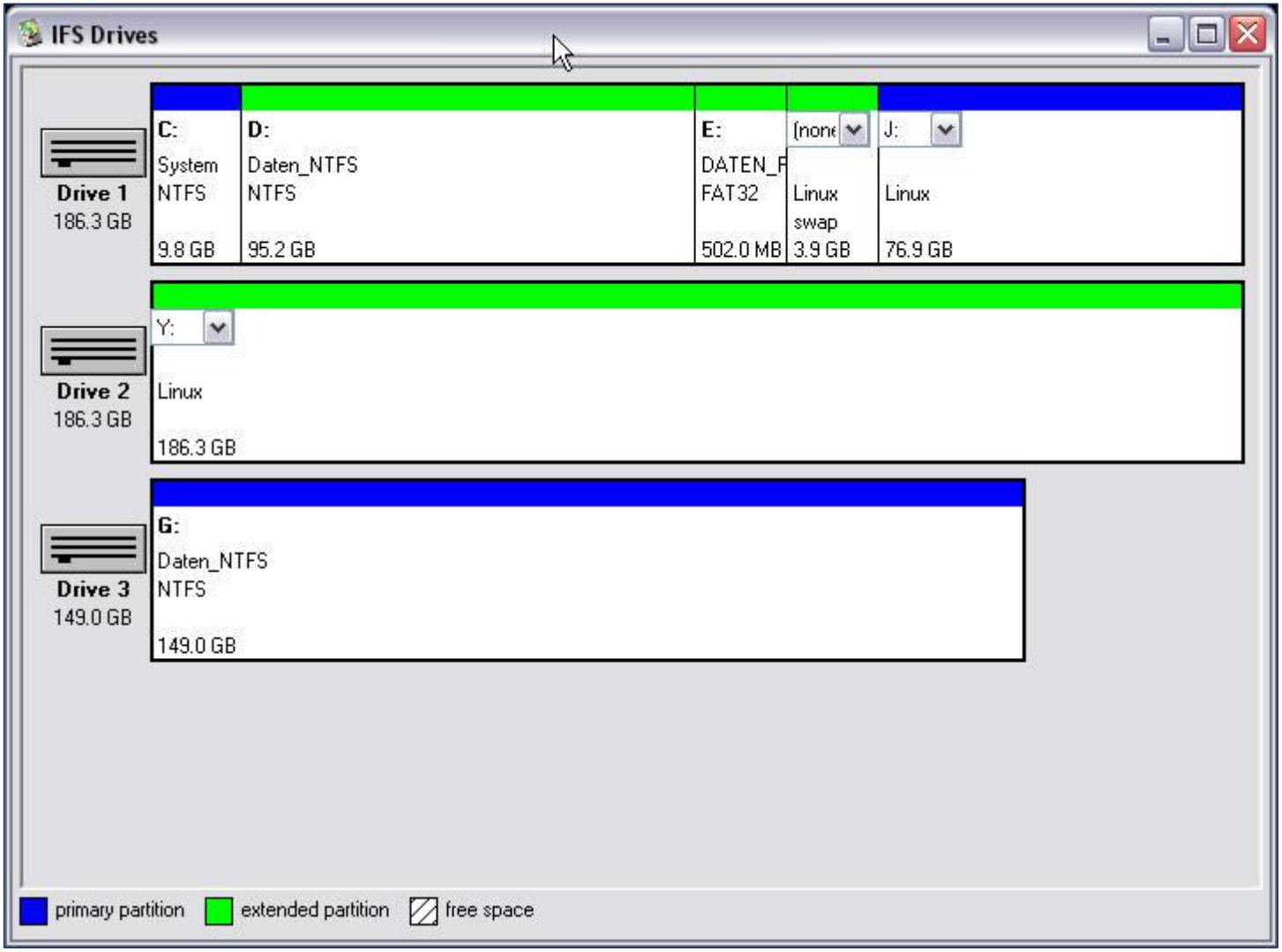
Command:	date
Exit status:	Sucess (0)
full path	/mnt/ir/linux/bin-x86-2.4/date
sha256sum	db74254d0233ab5d430c53f41a551b93c8a3e0e080c324db28b6106270ab7413

Done



Weitere Werkzeuge

EXT IFS

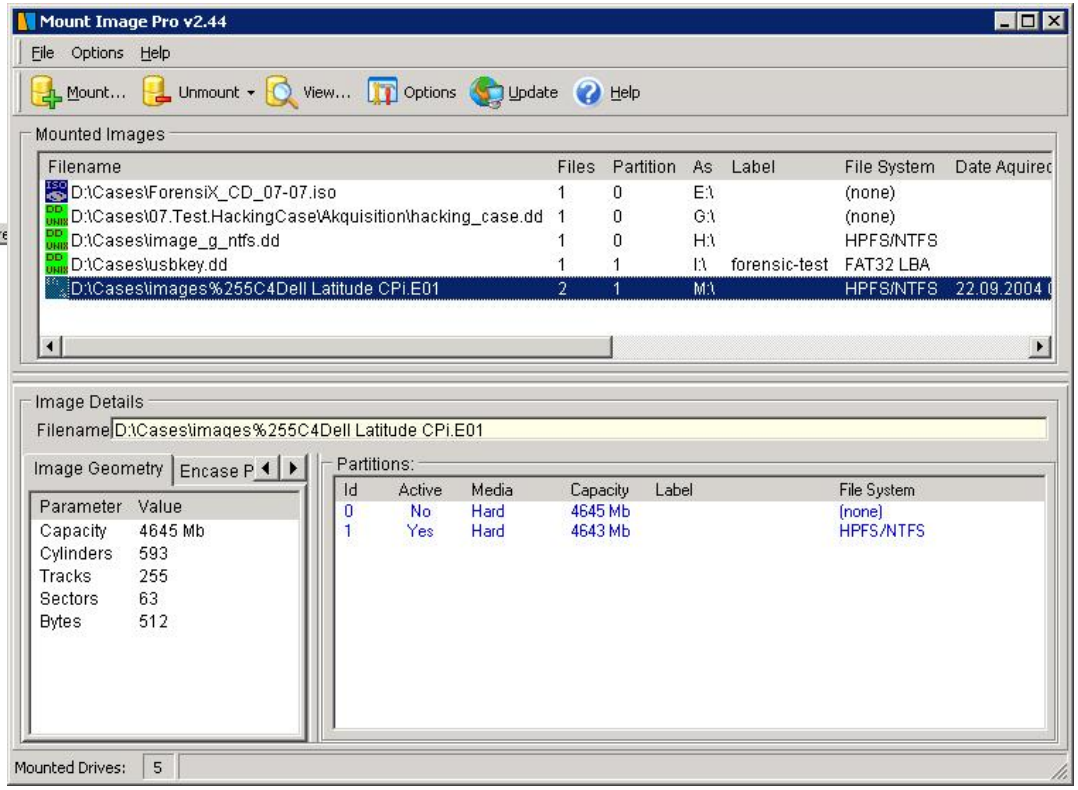


www.fs-driver.org

Mount Image Pro

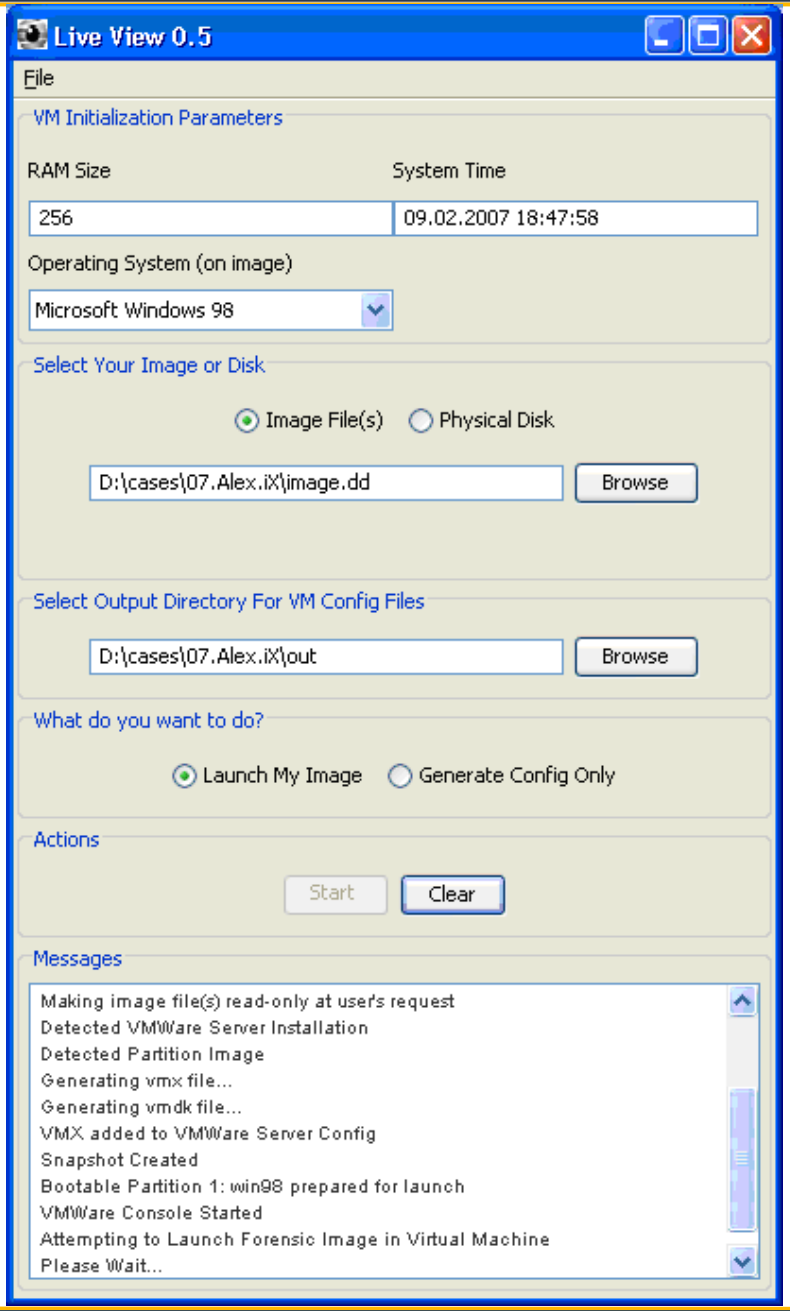
www.getdata.com

Name	Typ	Gesamtgröße	Freier Speicher	Kommentare
Festplatten				
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	



Live View

http://liveview.sourceforge.net/

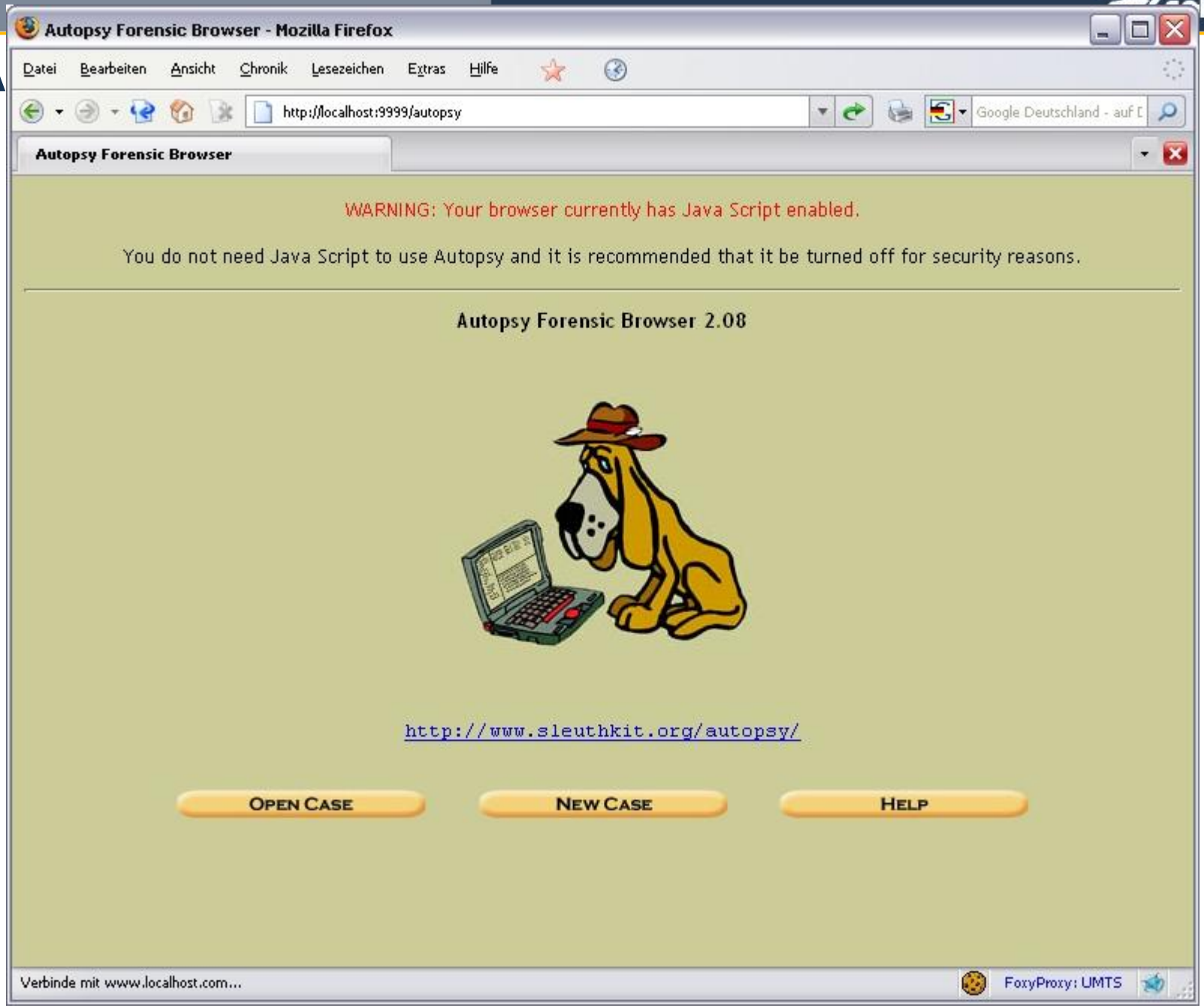


The Sleuthkit

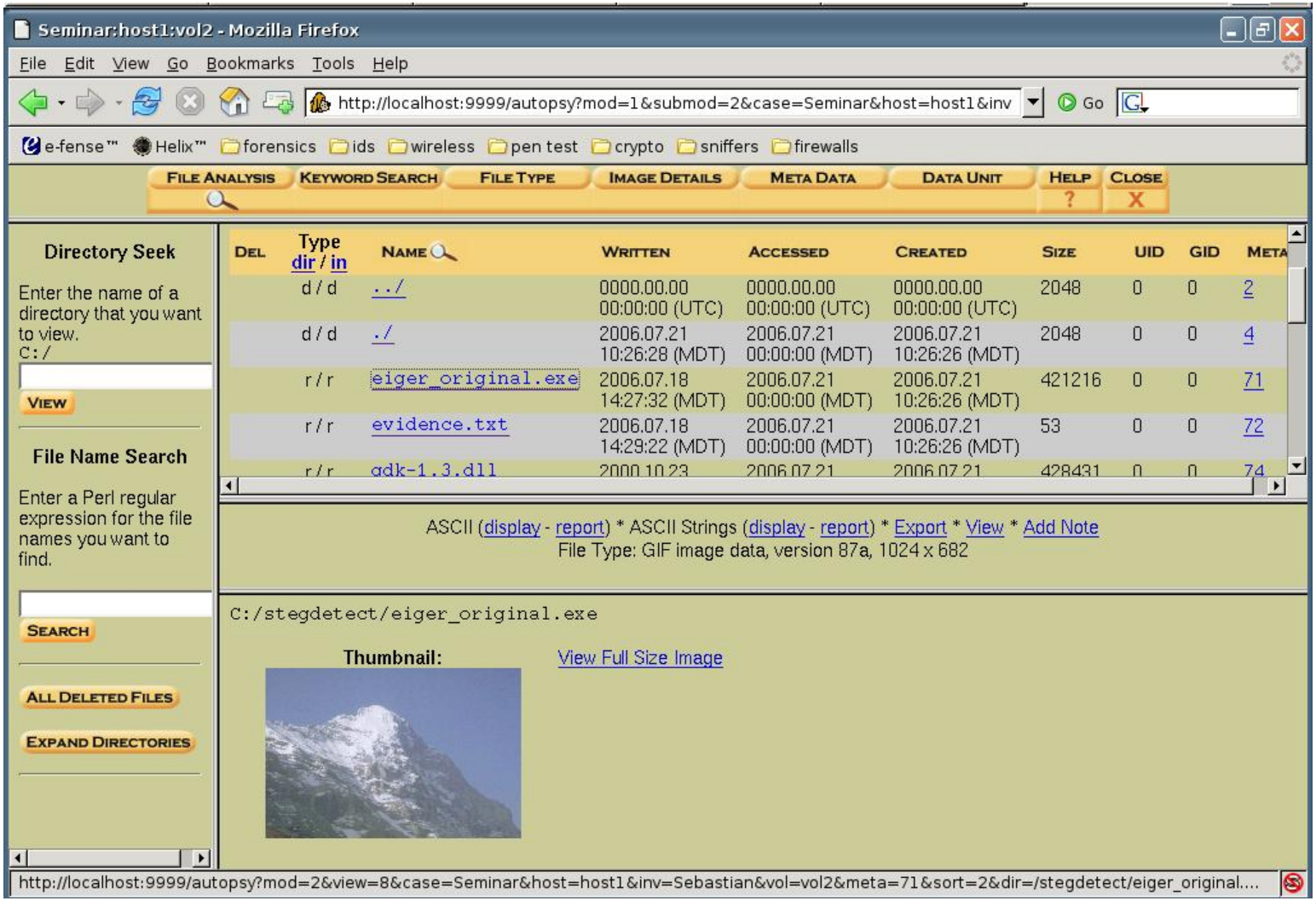
- The Sleuthkit (TSK)
  - Brian Carrier Anfang 2001
  - Sammlung von mehr als 20 Werkzeugen für die Analyse von Datenträgern und Dateisystemen
  - Werkzeuge werden in Gruppen zusammengefasst
    - Datenträger
    - Volume
    - Dateisystem
      - Struktur und Größen Informationen des Dateisystems
 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



Autopsy

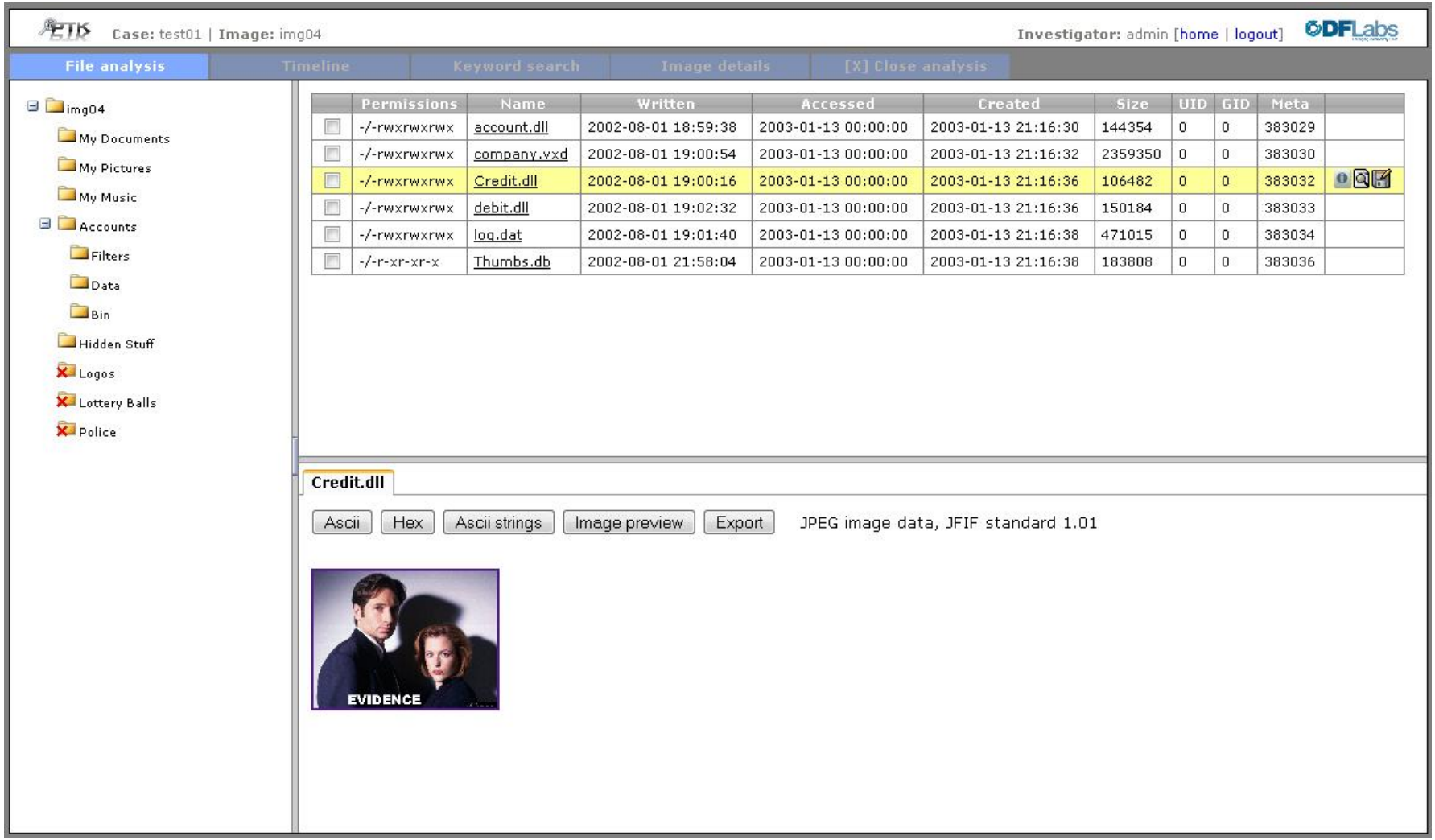


Autopsy

- 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 Zeitzonen und Hashdatenbanken
  - Eigene Kommentare pro Investigator
  - Analyse-Ergebnisse werden in ASCII-Dateien gespeichert
  - Damit einfache Archivierung kompletter Fälle

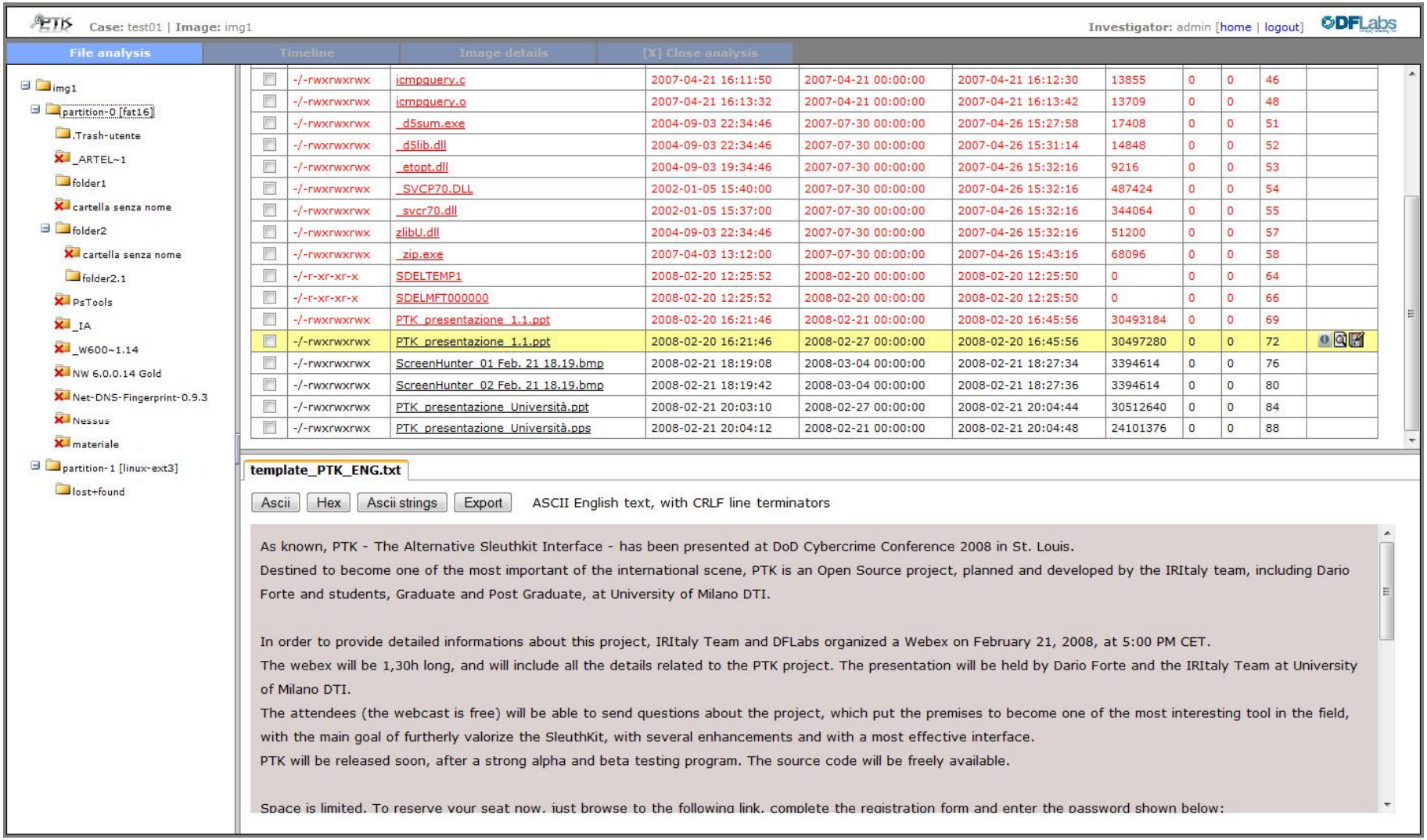
- Nachfolger PTK
  - Ab Final geplant ab 09 / 08
  - Ajax basiert
  - zentrale Datenbank
  - Index
  - http://ptk.dflabs.com

PTK



ptk.dflabs.com

PTK



ptk.dflabs.com

Vielen Dank für die Aufmerksamkeit!

Fragen ?

Alexander Geschonneck

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

