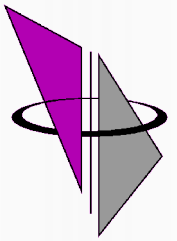


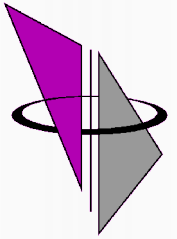
Post Mortem Analysen

mit

OpenSource Software

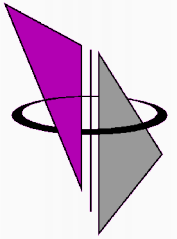
Matthias_Hofherr@genua.de

Zielstellung



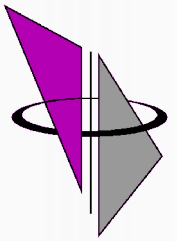
- Überblick über OpenSource Hilfsmittel für forensische Analysen
- Basis: The Sleuth Kit und Autopsy
- Nur Beweis-Analyse, keine Beweissicherung
- Beispiele: Analyse eines eigenen Honeypot-Systems

Übersicht



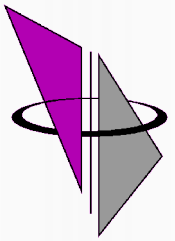
- OpenSource Analysen in der Vergangenheit
- The Sleuth Kit
- Autopsy
- Hilfsprogramme

Vergangenheit



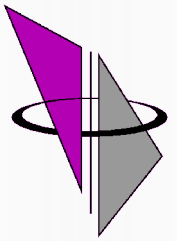
- The Coroner's Toolkit (TCT)
  - Dan Farmer und Wietse Venema, 1999
  - Erstes frei erhältliches forensisches Toolkit (*nix)
- Tctutils
  - Brian Carrier 2000
  - Ergänzungen zu TCT
- Autopsy
  - Brian Carrier 2000
  - Weboberfläche für tct + tctutils

TSK



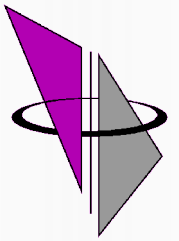
- The Sleuth Kit (TSK)
  - Sammlung von Kommandozeilen basierten Analyse-Tools
  - Hauptsächlich Dateisystem-Analysen (Berkeley Fast File System und Ableger davon, NTFS, FAT)
  - Analyse-System muss nicht selbes OS haben wie analysiertes System
  - Alle Kommandos geben auf stdout aus -> einfacher Datentransport bei Beweissicherung (netcat)

TSK



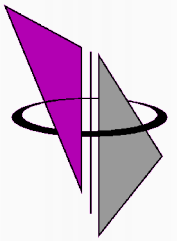
- Früher bekannt als TASK
- TSK analysiert
  - Meta-Daten (ils,icat,istat,ifind)
  - Dateinamen (fls,ffind)
  - Dateisystem (fsstat)
  - Datenblöcke (dls,dstat,dcalc,dcat)
- Jede Ebene bietet einen eigenen Toolsatz
- Tools sind statisch kompilierbar

TSK



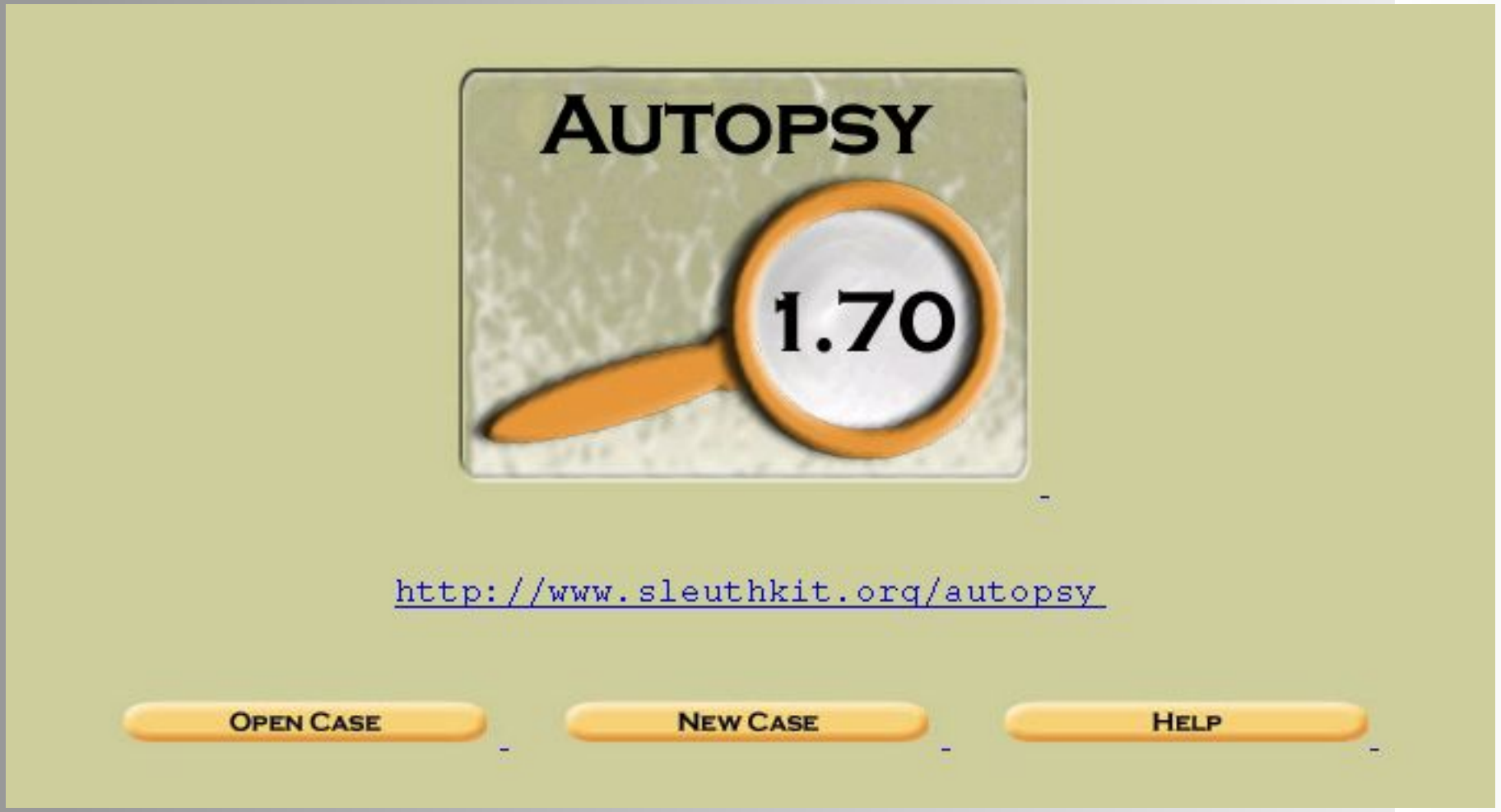
- Ergänzende Funktionen ausserhalb dieses Schemas:
  - hfind: Hashsummen-Schnittstelle
  - mactime: Zeitverlauf
  - sorter: Sammlung von Dateien auf Typ-Basis

Autopsy

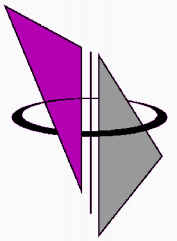


- Autopsy
  - Graphische Oberfläche für TSK
  - Perl-Programm
  - Analyse per Browser
  - Zugriffsschutz mittels Cookie und Beschränkung auf konfigurierbare Zugriffsadresse
  - Geeignet für Analyse-CD

TSK + Autopsy

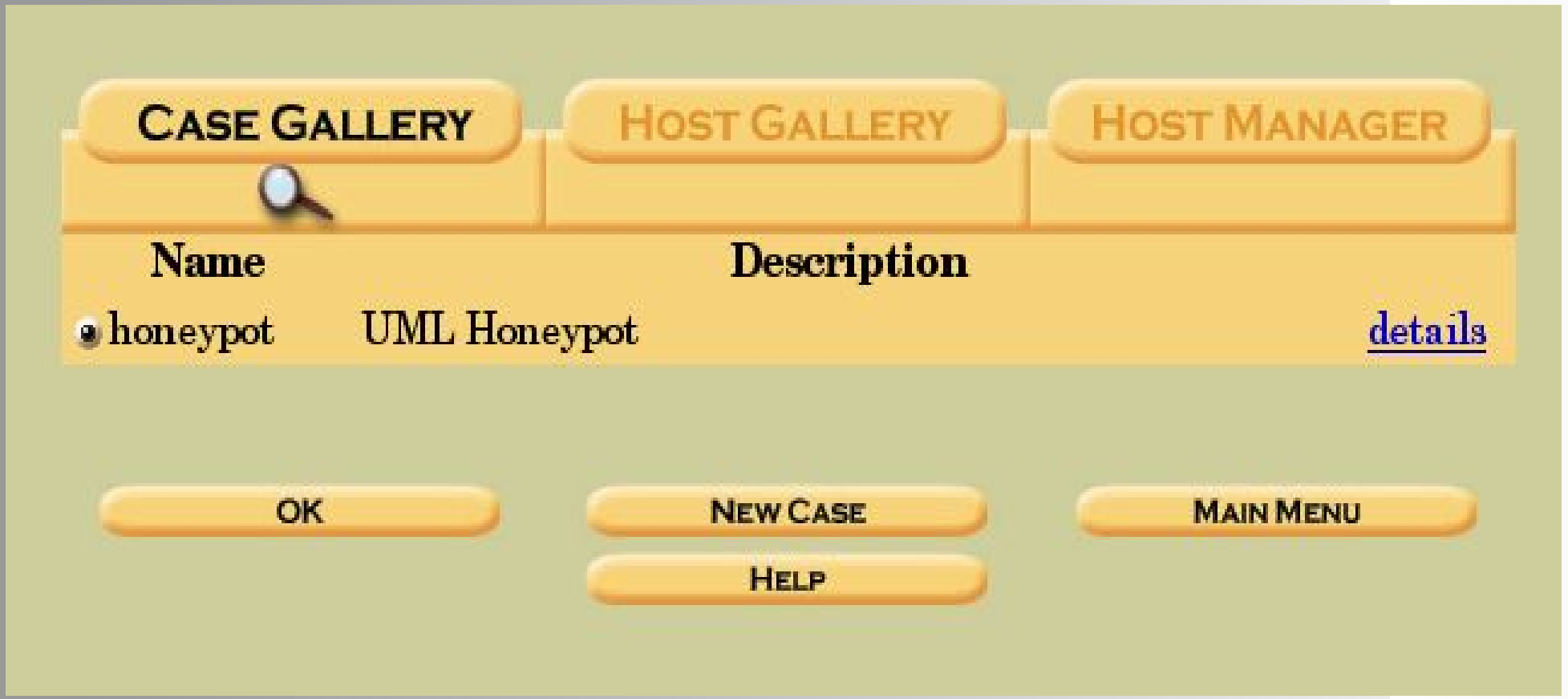

AUTOPSY
1.70
http://www.sleuthkit.org/autopsy
OPEN CASE
NEW CASE
HELP

Case Management

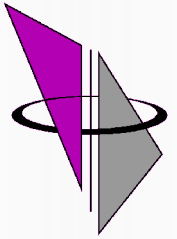


- Case Management
  - Verschiedene Fälle werden separat verwaltet
  - Pro Fall beliebige Host-Systeme
  - Jedem Host werden Images zugeordnet
  - Pro Host mehrere 'Investigators' möglich
  - Eigene Kommentare pro Investigator
  - Analyse-Ergebnisse werden in ASCII-Dateien gespeichert
  - Damit einfache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

Case Management



Case Management



Add a New Host

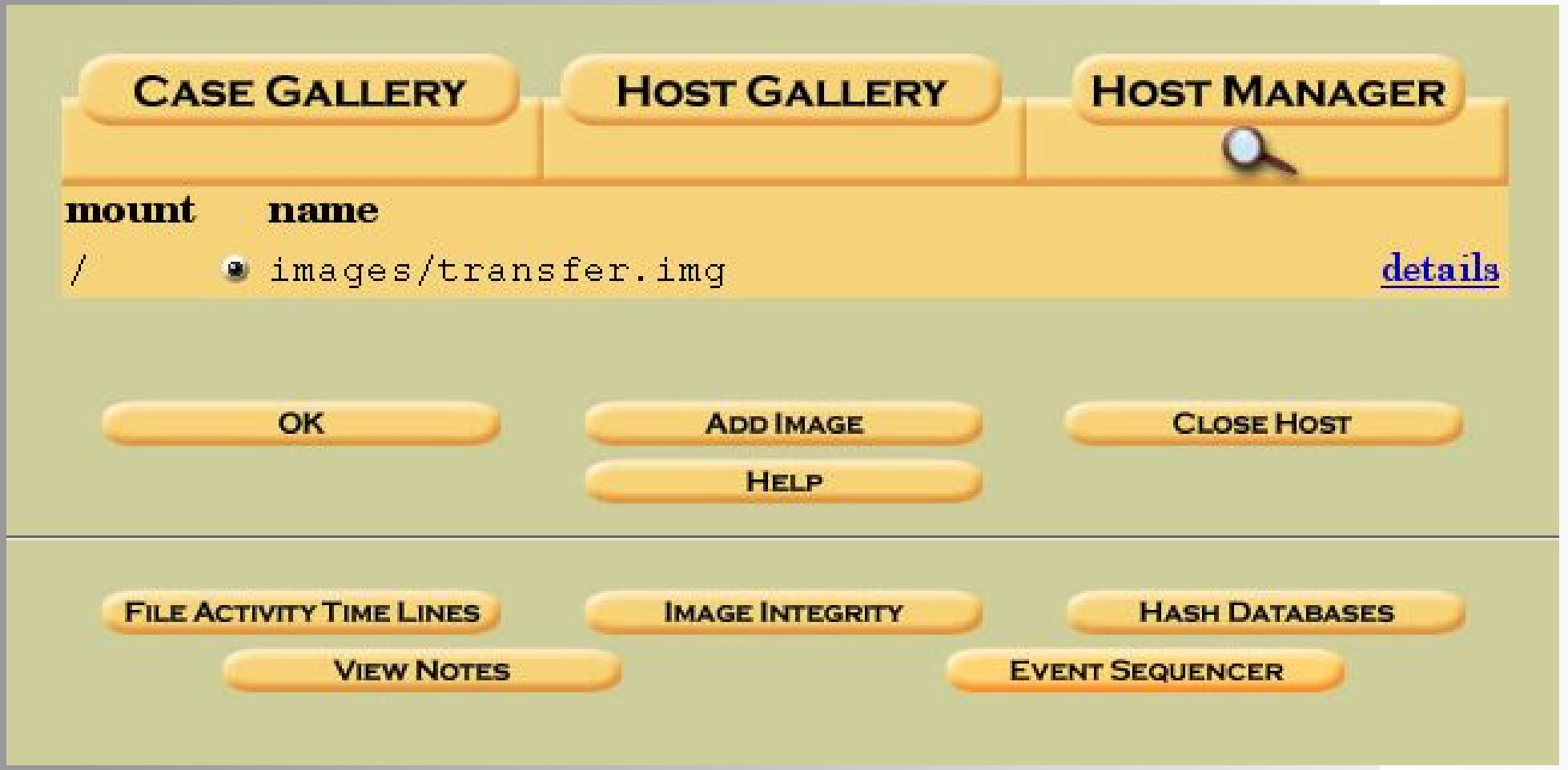
1. Host Name (directory name): transfer
2. Description (one line, optional): User Mode Linux Honeypot Host

3. Timezone: GMT+1
4. Timeskew (in +/- seconds): 0

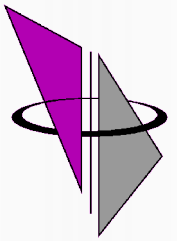
5. Path of Alert Hash Database (optional) i.e. known bad files:
6. Path of Ignore Hash Database (optional) i.e. known good files: /data/hp/transfer.md5

Add Host | Cancel | Help

Case Management

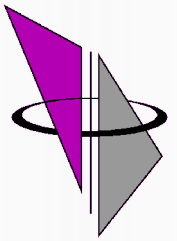


Case Management



- Sequencer
  - Erlaubt Notation von Funden in korrekter zeitlicher Reihenfolge
  - Freie Anmerkungen möglich
  - Verlinkung auf Dateien, Datenblöcke etc.

Case Management



Event Sequencer

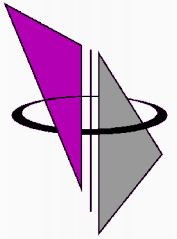
Date & Time	Source	Event & Note
Aug 04, 2003 03:15:05	ids	ssh CRC32 exploit
Aug 04, 2003 06:28:09	Inode: 51888	[C-Time]rootkit kopiert
Aug 04, 2003 06:28:36	/root/.ssh/login/rk.h	[C-Time]LOGFILE "/dev/ttypz", PASSWORD "ohadneu"
Aug 04, 2003 06:38:59	/root/.ssh/DX81NTeng.exe	[C-Time]MS DirectX 8.1

OK REFRESH

Timeline

- Erstellung einer Timeline
  - MAC (Modify,Access,Change)-Zeiten lesbar aufbereiten
  - Kann wertvolle Hinweise auf Aktivitäten eines Angreifers liefern
  - Ein Angreifer kann jede dieser Daten allerdings sehr einfach unbrauchbar machen (touch, touch2) bzw. gezielt manipulieren

Timeline



1. Select the data input file (`body`):

- body

2. Enter the starting date:

None:

Specify: May 1 2003

3. Enter the ending date:

None:

Specify: Nov 1 2003

4. Enter the file name to save as:

`output/` timeline

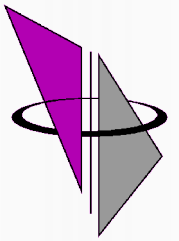
5. Select the UNIX image that contains the /etc/passwd and /etc/group files:

images/transfer.img (/)

6. Generate MD5 Value?

OK

Timeline

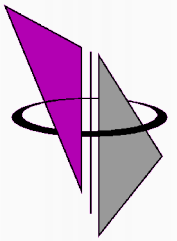


<- Jul 2003 Summary Sep 2003 ->

Aug 2003 OK

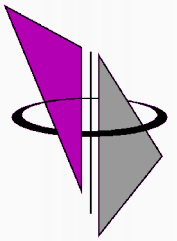
	1024	mac	d/drwxr-xr-x	102402	/usr/share/locale/sv/LC_MESSAGES
Mon Aug 04 2003 06:27:55	6	.a.	l/lrwxrwxrwx	63518	/var/spool/squid/0E/05/modprobe
	6	.a.	l/lrwxrwxrwx	63518	/sbin/modprobe -> insmod
	2736	.a.	-/-rw-r--r--	8315	/etc/modules.devfs
Mon Aug 04 2003 06:28:09	16792	.a.	-/-rw-r--r--	116746	/root/.ssh/login/ansi2knr.c
	2073	.a.	-/-rw-r--r--	153607	/root/.ssh/login/lib/mkdir.c
	2030	.a.	-/-rw-r--r--	153668	/root/.ssh/login/lib/lastlog_.h
	327624	..c	-/-rw-r--r--	51888	/root/.ssh/1login.tgz
	2781	.a.	-/-rw-r--r--	153661	/root/.ssh/login/lib/spdbm.c

sorter



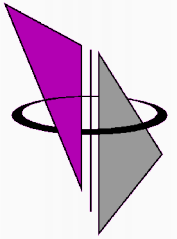
- Sorter
  - bündelt Dateien zu logischen Gruppen
  - Gruppenverteilung kann selbst definiert werden
  - Bietet guten Startpunkt für Analyse
  - Daten-Reduktion durch Hash-Summen (Known Goods)
  - Markiert extension mismatches

sorter



- Sorter
  - Kann Vorschau-Bilder erzeugen für schnellen Überblick
  - Momentan noch nicht vollständig in Autopsy integriert, erzeugt separate html-Dateien

sorter



Hash Databases

- Hash Database Exclusions (22090)

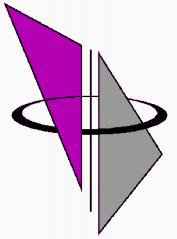
Extensions

- Extension Mismatches (48)
- Hash Database Exclusions with Extension Mismatch (3568)

Categories (508)

- archive (35)
- audio (0)
- compress (25)
- crypto (0)
- data (92)
- disk (0)
- documents (0)
- exec (105)
- images (1)
- system (0)
- text (204)
- unknown (46)
- video (0)

sorter

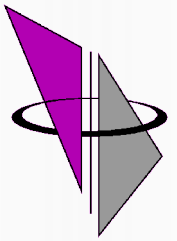


/root/.ssh/login/src/login.o
  ELF 32-bit LSB relocatable, Intel 80386, version 1 (SYSV), not stripped
  Image: /usr/local/security/forensics/evidence//honeypot/transfer/images/transfer.img Inode: 180231
  MD5: f0d9602264039a9466451d63fab32120

/root/.ssh/DX81NTeng.exe
  MS-DOS executable (EXE), OS/2 or MS Windows
  Image: /usr/local/security/forensics/evidence//honeypot/transfer/images/transfer.img Inode: 51889
  MD5: a0683bd9722f2e507befdbe0a96ba886

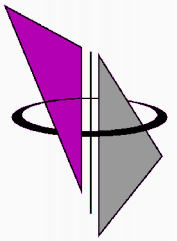
/bin/login
  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux 2.0.0, dynamically linked
  Image: /usr/local/security/forensics/evidence//honeypot/transfer/images/transfer.img Inode: 180232
  MD5: ea1a6327dbc74e60a1a1d2e0fcb7f099

Hashsummen



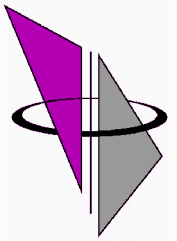
- Hashsummen-Datenbanken
  - Diverse frei verfügbare Quellen für Known-Goods
    - Known Goods Database
    - Hashkeeper
    - Solaris Fingerprint Database
    - The Cyberabuse RootkID Project
    - Dan Farmer's FUCK Archive

Hashsummen



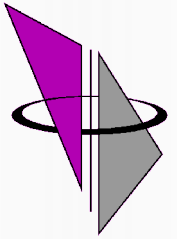
- Hashsummen-Datenbanken
  - TSK unterstützt eigene Hashsummen (md5) und Hashkeeper
  - NIST NSRL (National Software Reference Library) momentan nicht unterstützt, da gemischt Known-Good/Known-Bad
  - TSK verwaltet ASCII-Dateien und erzeugt Index-Dateien dafür

Hashsummen



- Hashsummen-Datenbanken
  - Eigene Ergänzungen möglich
    - Ersatz von hfind durch ein datenbankfähiges Tool
    - Speicherung der Datensätze in DBMS
    - Aufspaltung der Datensätze nach KnownGood/KnownBad
    - Schnelle Lookups auf indexierte Werte
    - Parser-Skript zum Import bestehender Datenbestände

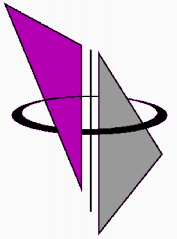
Fallbeispiel



- Tcpdump Mitschnitt:

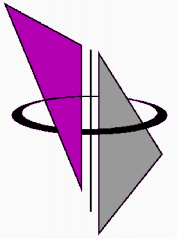
SSH-1.5-1.2.27
SSH-1.5-http://anti.security.is
^@^@^A^K^@^@^@^@^@^B<96>
[...]
<C0><FE><C0><CD><80>
@echo CHRIS CHRIS
CHRIS CHRIS
echo '***** YOU ARE IN *****'; hostname ; uname -a; id
***** YOU ARE IN *****
transfer.xyz.de
Linux transfer.xyz.de 2.4.20 #2 SMP
uid=0(root) gid=0(root)
[...]

Search



- Suchfunktionen
  - Wahlweise auf vollem Image oder auf nicht-allokierten Datenblöcken
  - Bei häufigen Suchen sollte ein Strings-File erstellt werden
  - Reguläre Ausdrücke werden unterstützt
  - Archivierung von Suchen -> einfach wiederholbar
  - Vordefinierte Suchen:
    - IP Adressen
    - Datum

Search

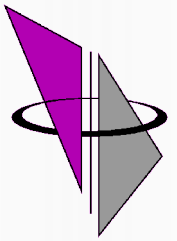


Fragment 7588
Allocated
Group: 0
Find Meta Data Address

ASCII Contents of Fragment 7588 (1024 bytes) in images/transfer.img

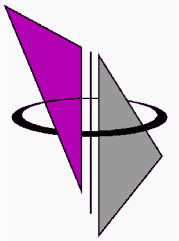
```
Aug  4 03:15:53 transfer sshd[5624]: fatal: Local: crc32 compensation attack:
Aug  4 03:16:27 transfer sshd[5652]: log: Connection from 134.96.66.203 port 64030
Aug  4 03:16:28 transfer sshd[5653]: log: Connection from 134.96.66.203 port 64050
Aug  4 03:16:28 transfer sshd[5654]: log: Connection from 134.96.66.203 port 64077
Aug  4 03:18:58 transfer PAM_unix[5679]: (su) session opened for user root by (uid=0)
Aug  4 03:38:19 transfer PAM_unix[5679]: (su) session closed for user root
Aug  4 04:07:01 transfer named[468]: USAGE 1059984421 1058635628 CPU=0.076923u/0s
Aug  4 04:07:01 transfer named[468]: NSTATS 1059984421 1058635628
Aug  4 04:07:01 transfer named[468]: XSTATS 1059984421 1058635628 RR=1 RNXD=0 RFwdR=0
```

Datensicht



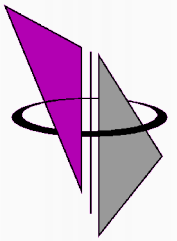
- Autopsy bietet verschiedene Sichten auf ein Image
  - Dateibaum
  - Inhalte von Dateien
  - Meta-Daten, z.B Inodes
  - Datenblöcke

Datei Ansicht



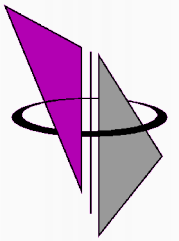
Type dir / in	Name	Modified	Accessed	Changed
d / d	../	2003.07.14 17:47:43 (GMT)	2003.08.04 06:38:21 (GMT)	2003.07.14 17:47:43 (GMT)
d / d	./	2003.08.04 06:38:38 (GMT)	2003.08.04 06:17:32 (GMT)	2003.08.04 06:38:38 (GMT)
r / r	1login.tgz	2002.01.06 14:42:03 (GMT)	2003.08.04 06:28:13 (GMT)	2003.08.04 06:28:09 (GMT)
r / r	authorized_keys	2002.03.12 19:17:51 (GMT)	2003.07.12 08:05:44 (GMT)	2002.03.12 19:17:51 (GMT)
r / r	DX81NTeng.exe	2001.10.31 21:14:00 (GMT)	2001.10.31 21:14:00 (GMT)	2003.08.04 06:38:59 (GMT)
d / d	login/	2003.08.04 06:31:21 (GMT)	2003.08.04 06:37:47 (GMT)	2003.08.04 06:31:21 (GMT)

Integritätsprüfung



- Integrität
  - Autopsy erzeugt von allen verwendeten und erzeugten Dateien md5 Summen
  - Die Summen können jederzeit während einer Untersuchung verifiziert werden

Integritätsprüfung



File System Images

images/transfer.img	C5BF2141E2BBF8E771D24FC963AFA5E3	Validate

Timeline Data Files

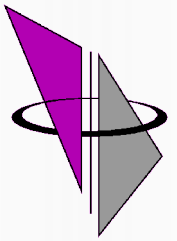
output/body	E8D9DD87E1069DB69E95A68CB3A069A2	Validate

Timeline

output/timeline	D8F95B97A2A4AB6C6330B41E6E8B085D	Validate

OK Refresh Help

Tools

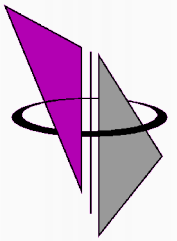


- bmap
  - Slackspace Analyse und Manipulations-Tool
  - Unabhängig von Dateisystem
  - Erlaubt derzeit keine Rekursion:

```
find .. -exec ./bmap --mode checkslack {} \;  2>&1 |
  grep 'has slack'
```

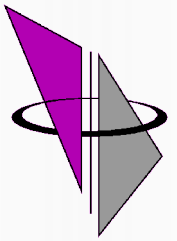
  - TSK unterstützt erst seit Version 1.66 die Darstellung von Slackspace, Autopsy noch nicht

Tools



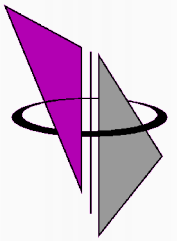
- foremost
  - Dateisuche auf bitstream image (Dateisystem-unabhängig)
  - basierend auf header und footer-Beschreibungen
  - nützlich für swap-Files / unallokierten Datenblöcke
  - Stellt gefundene Dateitypen direkt wieder her
  - Einfach erweiterbar um eigene Suchmuster
  - Momentan nur für Linux verfügbar
  - Patch für Autopsy-Integration existiert

Tools



- Rootkit-Suche
  - chkrootkit
  - rootcheck
- Schnelle, erste Suche nach Rootkit-Spuren
- Danach bei Bedarf manuelle Suche
  - Hashsummen
  - Tests mit statischen Binaries

Fazit



- OpenSource Forensics
  - Analyse mit graphischer Oberfläche möglich
  - Qualität der Tools ist kommerzieller Konkurrenz ebenbürtig
  - Komplexe Probleme durch Kommandozeilen-Tools lösbar
  - Einfache Erweiterbarkeit