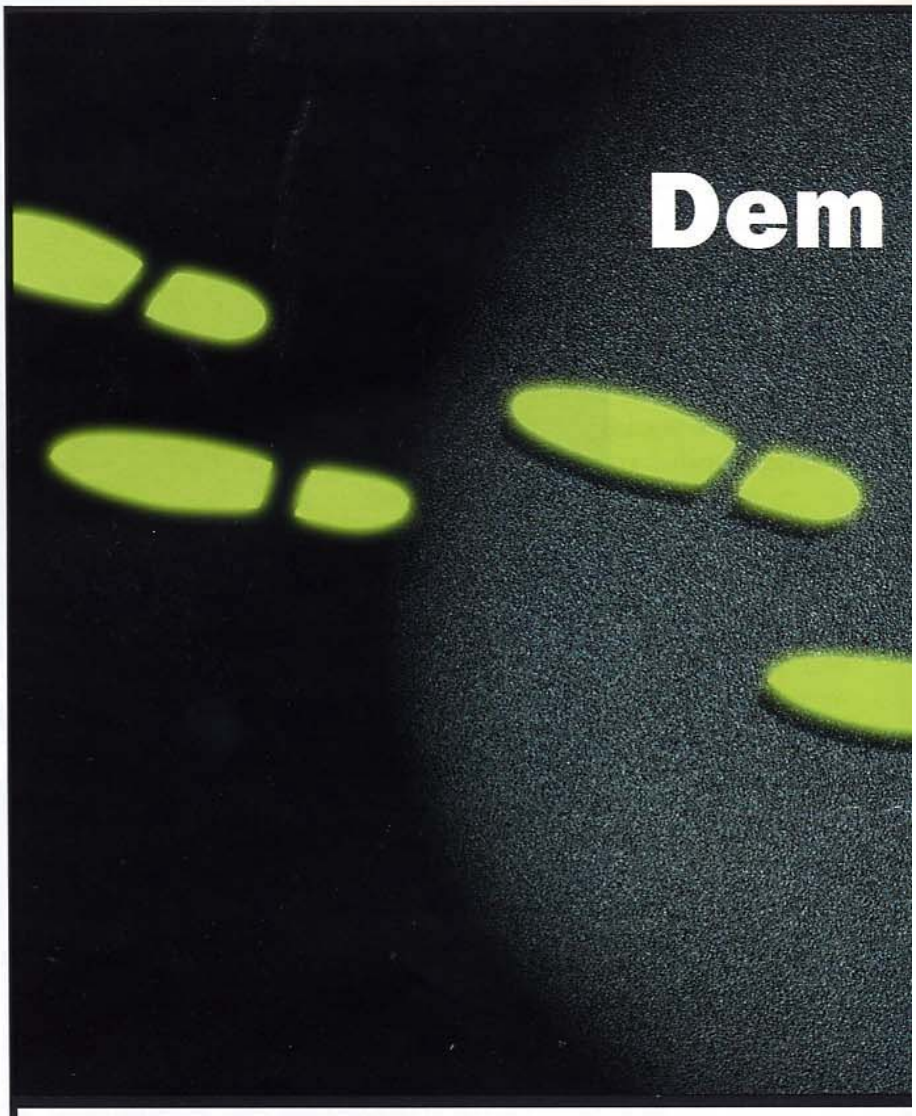
Forensic: Sicherheitsvorfallbehandlung



Fast jedes Unternehmen wird in seiner Geschichte gezwungen, sich mit dem Thema Sicherheitsvorfallbehandlung zu beschäftigen. Die wenigsten sind gut darauf vorbereitet. Zu den Vorbereitungen gehören neben organisatorischen Grundlagen auch technische Hilfsmittel. In diesem Artikel soll ein erster Überblick gegeben werden, welche Erstmaßnahmen sinnvoll sind und welche Tools in die Werkzeugkiste eines Analysten gehören.

Die ersten Schritte bei der Analyse eines Sicherheitsvorfalles können entscheidend sein für die Qualität des Untersuchungsergebnisses. Macht man hier Fehler, können entweder wichtige Beweise zerstört oder deren Verwendung bei der strafrechtlichen Verfolgung erheblich eingeschränkt werden. Das Untersuchungsteam sollte so klein wie möglich sein, die Mitglieder namentlich benannt werden. Für dieses Team oder den konkreten Fall sollte es einen Koordinator geben. Zu Beginn der Analyse sollte ein Protokoll angefertigt werden, in dem alle durchgeführten Schritte zu vermerken sind. Mitunter kommt es bei der Bewertung der Untersuchungsergebnisse vor Gericht auf jedes einzelne Detail an. Jeder Schritt, der zu einer weiteren Erkenntnis führt, muss durch eine zweite Person bezeugt werden.

Ein wichtiger Grundsatz ist, dass man Änderungen am Originalsystem so weit wie möglich vermeidet. Sobald der Verdacht eines Sicherheitsvorfalls besteht, sollte im Rahmen der aktuellen Situation jede weitere normale Arbeit am System beendet werden. Bitte beachten Sie, dass ein übereiltes Ausschalten des Systems wichtige Hinweise über den aktuellen Zustand des Systems vernichten kann.

Wichtig hierbei ist auch, dass eine erweiterte Datenanalyse mit den nachfolgend beschriebenen Zusatzwerkzeugen nur an einer Kopie des kompromittierten Systems durchgeführt werden sollte; die Gefahr der Zerstörung essentieller Beweise ist zu groß. Aus diesem Grund sollten die Daten zunächst gesammelt und erst später analysiert werden. Um im Nachhinein eine Unversehrtheit der Daten nachweisen zu können, sollte man SHA1- oder MD5-Prüfsummen erzeugen. Einige Tools wie grave-robber und IRCR erstellen diese Prüfsummen automatisch.

Die Daten sollten in der Reihenfolge ihrer Halbwertzeit gesichert werden. Als erstes ist hier der Inhalt des Caches zu nennen, dann folgen die Sicherung des Hauptspeicherinhalts, Informationen über den Netzwerkstatus (offene Ports, aktive Verbindungen, gerade beendete Verbindungen) und laufende Prozesse (alle Informationen: Mutterprozesse, Eigentümer, Prozessorzeiten, Aufrufparameter). Wichtig ist auch der Inhalt der /proc Filesystems, da sich hier die Binaries der laufenden Programme befinden.

Täter auf der Spur

Wenn ein Programm nach dem Start gelöscht wurde, findet man es hier (Beispiel: # cat /proc/PID/exe > filename).

Zum Schluss werden vom betroffenen System die Informationen der Festplatten gesichert. Dieses kann sowohl offline als auch online geschehen. Gesichert werden sollte mit dem Unix-Tool dd, da ein bitweises Kopieren möglich ist. Bei einer Sicherung auf Dateiebene würden viele wichtige Informationen verloren gehen. Die Sicherung kann – wenn genug Platz auf einem zusätzlichen Datenträger vorhanden ist – sowohl lokal, als auch über das Netz geschehen. Hierbei ist zu beachten, dass der Status des Systems bei beiden Sicherungsweisen verändert wird. Dieses sollte man bei der Auswertung der gewonnenen Informationen im Hinterkopf behalten.

Unter einem Unix-Betriebssystem stehen einem Analysten viele Möglichkeiten zur Verfügung, um einen aktuellen Status der laufenden Umgebung zu erfassen. Solche Befehle sind etwa last, who / w, ps, netstat, arp und lsof. Lsof bewährt sich häufig, wenn es darum geht, herauszufinden, welche Dateien von welchem Prozess geöffnet sind. Lsof ist dabei nicht nur auf „normale" Dateien beschränkt. Es können sowohl Informationen über Block- und Character-Devices als auch über Libraries, Streams oder Netzwerkdateien abgefragt werden.

Es ist wichtig, dass man für die Analyse Zugriff auf Logfiles zusätzlicher Sicherheitstechnik hat. Hierzu zählen neben Firewall- und Logfiles auch die Protokolle von Intrusion-Detection-Systemen.

Die folgenden Zusatzwerkzeuge helfen dem geübten Spezialisten, einem gehackten System wertvolle Informationen zu entlocken. Diese Tools sollten vorher auf sauberen Systemen kompiliert und auf sauberen Medien gespeichert werden. Für die post-mortale Analyse lassen sich u.a. spezielle Linux-Distributionen wie Trinux (http://www.trinux. org) oder Knoppix (http://www. kopper. net) verwenden, da sie komplett

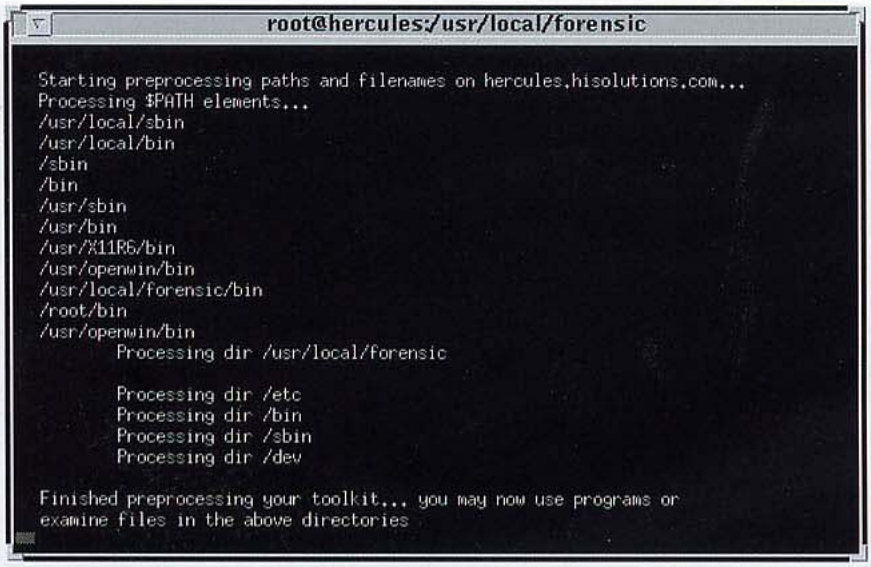


Bild 1: grave-robber bei der Datensammlung.

von Floppy oder CD-ROM gebootet werden können.

The Coroners Toolkit (TCT) von Dan Farmer und Wietse Venema (www.porcupine.org/forensics/tct.html) liefert Kommandozeilentools, die die post-mortale Untersuchung eines Unix-Systems ermöglichen. Es ermöglicht auch die Analyse von Inodes oder ganzen Blöcken von UFS- und EXTFS-Dateisystemen:

- *grave-robber:* Sammelt von einem aktiven System alle wichtigen Informationen zur weiteren Analyse. Es kann aber auch nachträglich (mit einigen Einschränkungen) mit einem Image verwendet werden. Zusätzlich erhält man eine Übersicht aller auf dem System befindlichen Dateien (Bild 1).
- *pcat:* Zeigt den Hauptspeicherinhalt eines laufenden Prozesses an. Auch wenn das zugehörige Programm nach dem Start gelöscht wurde, kann man hier noch aussagekräftige Ergebnisse erhalten.
- *icat:* Zeigt den Inhalt von Inodes an.
- *ils:* Alle Informationen über nicht allokierte Inodes einer Partition können angezeigt werden.
- *unrm:* Speichert alle nicht allokierten Blöcke einer Partition in eine Datei.
- *lazarus:* Ermöglicht das teilweise Zusammensetzen von Dateien aus Images mit gelöschten Blöcken. Diese Images können mit unrm erstellt werden.
- *mactime:* Analyse von Zugriffszeiten in einem definierbaren Zeitraum

TCTUTILs von Brian Carrier (http://www.cerias.purdue.edu/homes/carrier/forensics) ergänzt das TCT um weitere Systemanalyse-Tools für die Untersuchung kompromittierter Dateisysteme:

- *ilstat:* Zeigt alle vorhandenen Informationen und Daten zu einem Inode an.
- *fls:* Erweitert das TCT um die Möglichkeit, eine Liste aller Dateien und Verzeichnisse mit Zugriffszeiten und kurz vorher gelöschten Dateien zu erstellen.
- *bcat:* Gibt den Inhalt eines Blocks in ASCII, HTML oder HEX aus.

Der Autopsy Forensic Browser, ebenfalls von Brian Carrier, (http://www.cerias.purdue.edu/homes/carrier/forensics) ist ein HTML-Interface, das die Tools aus TCT und TCTUTILs mit Standard-Unix-Werkzeugen (strings, md5sum, grep etc.) wirkungsvoll verbindet. Ein kompromittiertes Dateisystem kann als Image oder auf Block- beziehungsweise Inode-Ebene untersucht werden. Autospy enthält keine eigenen Forensic-Tools, sondern fasst Werkzeuge anderer Pakete sinnvoll zusammen (Bild 2 und 3).

Brian Carrier hat seine Tools mittlerweile überarbeitet und mit erweiterten Funktionen ausgestattet.

Netcat (nc) ist ein universelles Tool, um unter anderem Daten über ein Netz zu transportieren. Bei der Übertragung vertraulicher Daten über ungesicherte Netze sollte auf cryptcat (http://farm9.com/content/Free_Tools/Cryptcat) zurückgegriffen werden. Netcat kann unter http://www.atstake.com/research/tools/nc110.tgz heruntergeladen werden.

Beispiel:

```
# dd if=/dev/hda2 | nc
10.0.0.1 8000
```

(der komplette Inhalt der Partition hda2 wird mittels netcat an ein anderes System auf Port 8000 gesendet)

Auf dem System 10.0.0.1 sollte dann folgender Befehl verwendet werden:

```
# nc -l -p 8000 |dd of=
/forensic/image.hda2
```

Mac-robber von Brian Carrier ist ein Forensic- und Response-Tool, das Modified-, Access- und Change-Times (MAC) von Dateien und Verzeichnissen sammelt. Das verwendete Zeitformat ist mit

Für die post-mortale Analyse lassen sich spezielle Linux-Distributionen wie Trinux oder Knoppix verwenden, da sie komplett von Floppy oder CD-ROM gebootet werden können.

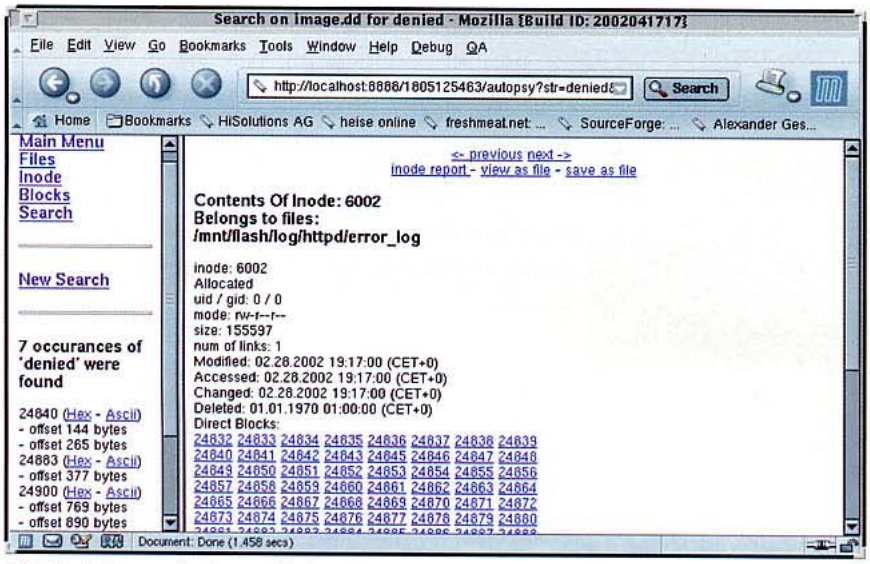


Bild 2: Autopsy: Suche nach dem Wort „denied" in einzelnen Blöcken.

Mit dem Forensic ToolKit von NT OBJECTives (www.ntobjectives.com) kann man einen forensischen Snapshot von Microsoft-Windows-Systemen erzeugen. Es enthält folgende Tools:

- *Afind:* zeigt Informationen über den letzten Dateizugriff an
- *Sfind:* zeigt Hidden Data Streams an
- *Hfind:* zeigt versteckte Dateien an
- *FileStat:* zeigt diverse Dateistatistiken an
- *Hunt:* zeigt die verfügbaren Netbios-Informationen und die Administratorkennungen an

dem von The Coroners Toolkit (TCT) identisch und kann gleich damit weiterverwendet werden. Mac-robber basiert auf dem Werkzeug grave-robber aus dem TCT. Im Gegensatz zu grave-robber aus dem TCT ist Mac-robber nicht in Perl, sondern in C geschrieben. Dadurch ist es leicht auf andere Plattformen portierbar. Mac-robber kann auf einem „sauberen" System statisch vorkompiliert und auf eine IR-CD beziehungsweise IR-Floppy kopiert werden. Durch Kombination mit Netcat ist der Einsatz über ein Netzwerk möglich.

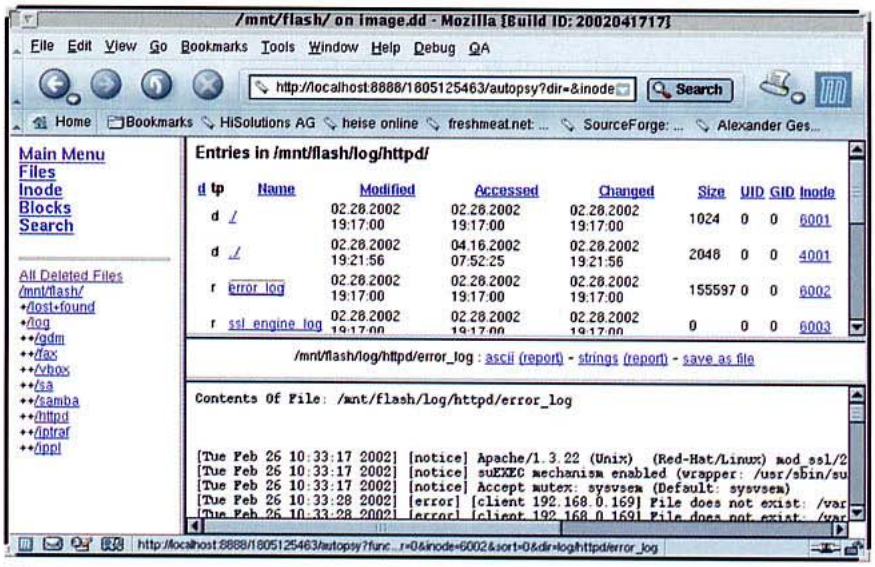


Bild 3: Autopsy: Suche nach gelöschten Dateien in einem Image.

Beispiel:

```
# mac-robber /var/log > data/var_log.mac
```

(mac-robber analysiert das Verzeichnis /var/log und sendet die Ausgabe in eine Datei)

```
# mac-robber /var/log | nc 10.0.0.1 8000
```

(mac-robber analysiert das Verzeichnis und sendet die Ausgabe mittels netcat an ein anderes System auf Port 8000)

Auf dem System 10.0.0.1 sollte dann folgender Befehl verwendet werden:

```
# nc -l -p 8000 > /forensic/var_log.mac
```

Um die Daten zu analysieren, wird das mactime-Tool aus dem TCT benötigt. Es werden alle Dateien angezeigt, deren MAC-Time sich seit dem angegebenen Datum geändert haben.

```
# mactime -b /forensic/var_log.mac 01/01/2002
 (date     time     size  MAC  perms     owner   group   file)
 [....]
 Jan 05 02 04:05:00 5506499  m.. -rw-rw-rw- root      mailman /var/log/syslog .7
 Jan 10 02 04:05:00 6389017  m.. -rw-rw-rw- root      mailman /var/log/syslog .6
 Jan 12 02 01:04:39    3978  .a. -rw------- root      mailman /var/log/arclog
 Jan 12 02 14:10:15    3978  m.c -rw------- root      mailman /var/log/arclog
[....]
```

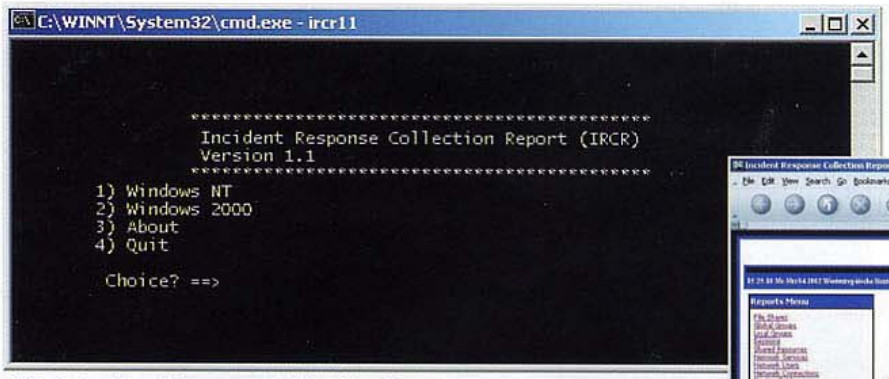


Bild 4: Incident Response Collection Report.

gie der halbe Weg zur erfolgreichen Aufklärung von Systemeinbrüchen ist.

Alexander Geschonneck
geschonneck@hisolution.com

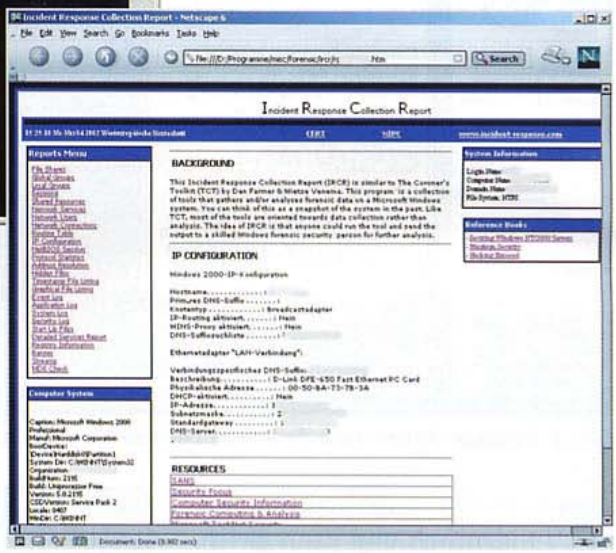


Bild 5: IRCR-Ausgabe.

Der Incident Response Collection Report (IRCR) ist dem Coroner's Toolkit (TCT) ähnlich (Bild 4). Dieses Programm sammelt mit diversen Tools forensische Daten von Microsoft-Windows-Systemen. Das Ergebnis wird als HTML-Output erstellt (Bild 5).

Mit Fatback von Nicholas Harbour (DoD Computer Forensics Lab) hat man auch unter Unix die Möglichkeit, FAT-Partitionen zu untersuchen und gelöschte Dateien sichtbar zu machen. Dies funktioniert analog zum DOS-Befehl undelete (Bild 6).

Fazit

Es ist aber auch wichtig, dass man für die Analyse Zugriff auf Logfiles zusätzlicher Sicherheitstechnik hat. Hierzu zählen neben Firewall- und Logfiles auch die Protokolle von Intrusion-Detection-Systemen. Wenn ein interner Täter vermutet wird, sind darüber hinaus Informationen von Zutrittskontrollsystemen von Interesse. Uns stehen heute innovative und sehr effektive Tools zur Unterstützung bei der Aufklärung von Systemeinbrüchen zur Verfügung. Die durchzuführenden Tätigkeiten hingegen sind nicht neu. Die Verfügbarkeit dieser komfortablen Werkzeuge darf aber nicht darüber hinwegtäuschen, dass eine sinnvolle Sicherheitsvorfall-Behandlungsstrate-

```
# fatback morgue/image2.dd
Running Fatback v1.3
Command Line: fatback morgue/image2.dd
Time: Tue Apr 16 08:28:52 2002
uname: Linux Ripper 2.4.18 #1 Fri Mar 15 12:40:44 CET 2002 i686
Working Dir: /usr/local/forensic
Unable to map partitions
1 characters of the OEM name in the VBR are invalid
The VBR reports no hidden sectors
oem_name: mkdosfs
bytes_per_sect: 512
reserved_sects: 1
fat_copies: 2
max_rdir_entries: 512
total_sects_s: 0
media_descriptor: f8
sects_per_fat: 125
sects_per_track: 32
num_heads: 8
hidden_sects: 0
total_sects_l: 127968
serial_num: 3c7e78de
fs_id: FAT16
Filesystem type is FAT16
Rood dir location: 0
fatback> ls
??? Mar  7  20:25:32 2002  129024  ?ENTEST.DOC Pentest.doc
??? Mar 15  09:49:54 2002   20480  ?ONFUS~1.C confuse_router.c
??? Mar 15  09:49:54 2002  278638  ?RAGRO~1.TGZ fragrouter.tgz
Sun Mar 15  09:49:52 2002    5942  ?BNBS.C
Sun Mar 15  09:50:22 2002   61897  ?MBAT-~1.GZ smbat-src-1.0.5.tar.gz
Sun Mar 15  09:50:22 2002   43398  ?MBPRO~1.TGZ smbproxy-src-1.0.0.tg
Sun Mar 15  09:49:54 2002     315  ?RIPWI~1 tripwire-check
fatback>
```

Bild 6: undelete von FAT-Partitionen unter Unix.