KNOPPIX UND CO. ALS NOTFALL- UND RETTUNGS-LINUX

Rettungspinguin

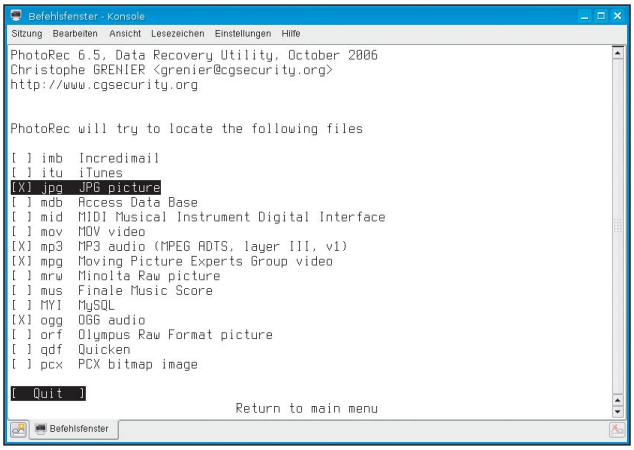
Live-CDs liefern weit mehr als nur einen Eindruck von Linux. Sie bringen Tools zum Partitionieren, Klonen und zur Analyse havarierter Rechner mit. Wir stellen mächtige Werkzeuge vor, die Sie unabhängig von vielen kommerziellen Lösungen machen. VON **MATTIAS SCHLENKER**

Fast jeder Computernutzer kennt den Fall, dass sein Arbeitsgerät nicht startet. Zu DOS-Zeiten konnte man von Floppy starten. Die logische Weiterentwicklung dieses Konzeptes ist die Knoppix-CD, mit der sich mehr als das Kopieren und Brennen von Daten anstellen lässt.

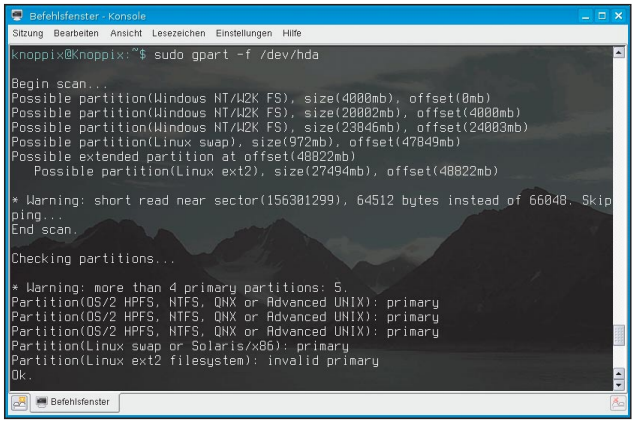
Flotte Forensik

Gerade bei Speicherkarten, die mit dem FAT-Dateisystem formatiert sind, kommt es häufig vor, dass nach einer Beschädigung des Dateisystems auf gespeicherte Fotos nicht mehr zugegriffen werden kann. Aber auch aus Versehen formatierte Festplatten oder defekte Partitionstabellen vereiteln den Zugriff auf gespeicherte Daten. Inhaltsverzeichnis und Stichwortverzeichnis sind vollständig weg, die gespeicherten Daten sind jedoch noch vorhanden. Knoppix bringt für die Suche das Werkzeug *PhotoRec* mit, das gespeicherte Dateien anhand typischer Byte-Sequenzen erkennt und wiederherstellen kann.

Auch wenn PhotoRec primär Foto- und Videodateien erkennt, ist die Liste



Feintuning: *PhotoRec* kann auf bestimmte Dateitypen angesetzt werden. Das spart Platz und Zeit.



Partitionen raten: Auf dem Testsystem erkannte *gpart* die Linux-Partitionen nicht ganz richtig – für eine manuelle Korrektur waren die Daten aber ausreichend.

der erkannten Dateitypen lang genug, um z.B. auch MySQL-Tabellen und Excel-, Word- und Access-Dateien suchen zu lassen. Wie gut die Suchleistungen von PhotoRec sind, hängt neben dem Beschädigungs- und Fragmentierungsgrad des Dateisystems ganz stark vom Dateisystemtyp ab: „Flache" Dateisysteme wie FAT schneiden besser ab als komplexe Dateisysteme wie ReiserFS, die kleine Dateien im Binärbaum ablegen und die Anfänge großer Dateien nicht zwangsläufig auf Blockgrenzen legen. Die Wiederherstellung erfolgt dabei nicht auf dem untersuchten Datenträger, sondern in ein beim Aufruf anzugebendes Verzeichnis. Achten Sie auf genügend Platz, da PhotoRec auf vielen Dateisystemen auch alte, nur gelöschte Dateien findet. Der folgende Aufruf scannt */dev/hda* und kopiert gefundene Dateien nach */tmp*:

```
photorec /d /tmp /dev /hda
```

Ist ein Datenträger physikalisch beschädigt, sollten Sie unbedingt eine Image-Datei anlegen. Die Bit-getreue Kopie kann auch mit den nachfolgend vorgestellten Programmen *testdisk* und *gpart* untersucht werden. Ideales Tool für dieses „Notfall-Imaging" ist *dd_rescue*. Mit

```
dd_rescue -A /dev/hda1 hda1.img
```

erstellt man ein Image der Partition */dev/hda1*. Defekte Blöcke werden dabei mit Nullen aufgefüllt. Images leicht beschädigter Partitionen können Sie mit der Mount-Option *-o loop* – vorzugsweise „read-only" – einhängen. Abbilder stark beschädigter Partitionen eignen sich immer noch für den Scan mit PhotoRec.

Um eine gesamte Festplatte auf eine gleich große oder größere Platte zu klonen, genügt die Angabe des Zielgerätes als Ausgabedatei:

```
dd_rescue -A /dev/hda
➥/dev/hdc
```

Wies eine Festplatte vor dem Klonen nur leichte Beschädigungen auf, genügt oft die Nutzung des passenden Prüfprogrammes (*chkdisk* oder *fsck*), um ein konsistentes Dateisystem zu erhalten. Da die Ergebnisse des Checks schwer vorhersehbar sind, ist ein Scan mit PhotoRec vorher sinnvoll.

Jäger der verlorenen Partition

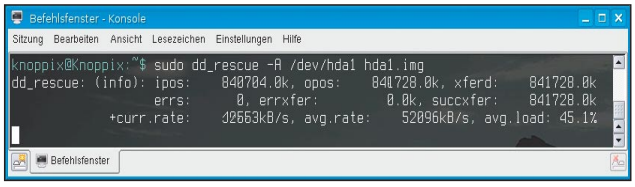
Ist die Partitionstabelle beschädigt oder versehentlich überschrieben, lassen sich Typ und Anfang der vorhandenen Dateisysteme nicht ermitteln, weshalb eine Reparatur nicht möglich ist. Bei Festplatten, die nur eine große Windows-Partition enthalten, ist schnell eine Lösung geschaffen: Mit *fdisk* eine Partition des richtigen Typs von vorne bis hinten anzulegen, genügt. Anders die Situation, wenn mehrere Partitionen (Windows, Linux, Linux Swap) auf einer Festplatte koexistieren. Für die Suche nach den Partitionsanfängen schicken Knoppix und Co. die beiden Werkzeuge *TestDisk* und *gpart* („guess partition"– nicht zu verwechseln mit dem Partitionierungswerkzeug *gparted*) ins Rennen. Beide Werkzeuge kennen die typische Struktur der gängigen Dateisysteme und durchsuchen Block für Block nach ihnen. Einen vollen Scan nach Partitionen starten Sie mit

```
gpart -f /dev/hda
```

Sind Sie mit dem Scan-Ergebnis zu 100% zufrieden, schreiben Sie die Partitionstabelle mit

```
gpart -W /dev/hda /dev/hda
```

Erscheint die vermutete Partitionstabelle nicht plausibel, sollten sie die Partitionstabelle in eine Datei schreiben, diese mit *fdisk* bearbeiten und später mit *dd* auf die Festplatte kopieren. Da *gpart* auch Partitionen findet, die vor langer Zeit gelöscht wurden, aber noch Überreste von Dateisystemen enthalten, sollten Sie jede gefundene Partition



Letzte Hoffnung: *dd_rescue* bricht auch bei defekten Sektoren nicht ab und ermöglicht so oft die Rettung wichtiger Daten.

Immer dabei: Knoppix und Co. am Schlüsselbund

Fast alle aktuellen Live-Distributionen sind darauf ausgelegt, ihre Containerdatei auch auf einer FAT32- oder EXT3-Partition zu suchen. Zusammen mit der Fähigkeit moderner Hardware, von USB-Sticks zu booten, vereinfacht dies die Entscheidung, einige der praktischen Distributionen auf einem schon ab 10 Euro erhältlichen Stick mit einem GByte unterzubringen. Der Stick kann zudem weitere Tools wie den Virenscanner aufnehmen. Die Installation ist zumindest bei Knoppix 5.1.1 denkbar einfach: Sowohl die Inhalte der Live-CD als auch die Dateien in */boot/isolinux* müssen in das Wurzelverzeichnis des Sticks kopiert werden. Dann benennen Sie die Konfigurationsdatei *isolinux.cfg* um in *syslinux.cfg*. Der Befehl *syslinux* aus dem gleichnamigen Software-Paket schreibt schließlich den Bootloader auf den nicht gemounteten Stick:

```
./syslinux /dev/sda1
```

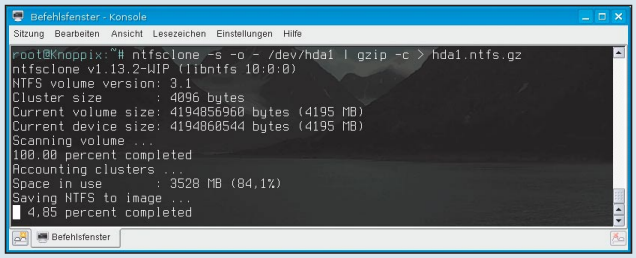
Achtet man auf die unterschiedliche Benennung von Kernel, Initrd und Containerdatei, können sich mehrere Distributionen einen Stick teilen.

Eine umfangreiche Anleitung zur Verwendung von „syslinux" und den verwandten Bootloadern finden Sie auf der Webseite des PC Magazin unter www.pc-magazin.de/praxis/linux/a/LINUX_VON_USB_STICK_UND_FESTPLATTE_BOOTEN.

Von der Webseite des Autors können Sie eine fertige ZIP-Datei herunterladen, die Knoppix und Insert mit einigen weiteren Tools zusammenfasst und viel Konfigurationsaufwand erspart: www.mattiasschlenker.de/070031.

Intelligent geklont: *ntfsclone*

Möchte man eine intakte Windows-Partition sichern, ist *dd* kein probates Mittel, da die Sicherung auf Blockebene unbelegte Blöcke mitsichert und damit so groß wie die zu sichernde Partition ist. Eine Komprimierung der Bit-getreuen Images bringt wenig Platzersparnis, besonders wenn auf nicht alloziierten Blöcken die Reste von Multimedia-Dateien liegen.



Mit Köpfchen: *ntfsclone* kopiert nur belegte Sektoren einer vorhandenen NTFS-Partition.

Clever gesichert…

Das Tool *ntfsclone* kennt die Strukturen von NTFS und spart unbelegte Blöcke aus. Ein Image ist damit nur etwas größer als der belegte Platz plus Dateisystem-Metadaten.

Optimale Ergebnisse erzielen Sie, wenn Sie Windows vor der Sicherung die Auslagerungsdatei löschen lassen.

Gehen Sie wie folgt vor, um das Dateisystem der Partition */dev/hda1* in eine Datei *hda1.ntfs* zu sichern:

```
ntfsclone -s -o hda1.ntfs /dev/hda1
```

Um nicht unnötig Platz für große Dateien zu verschenken, ist es ratsam gleich zu komprimieren. Statt in eine Datei schreibt *ntfsclone* mit – in eine Pipeline. Recht effizient packt dann *gzip*:

```
ntfsclone -s -o -- /dev/hda1 | \
gzip -c > hda1.ntfs.gz
```

Eine frische Windows-Installation mit einigen Programmen passt so auf ca. 600 bis 800 MByte.

Bei der Sicherung großer Partitionen auf eine USB-Festplatte mit dem FAT32-Dateisystem (maximale Dateigröße knapp unter 4GB) oder DVDs muss das Image gesplittet werden. Das erledigt ein weiterer Eintrag in der Pipeline:

```
ntfsclone -s -o - /dev/hda1 | gzip -c
➥| split -a 3 -b 700m - hda1.ntfs.gz.
```

Das Resultat sind 700 Megabyte große Happen, die von *hda1.ntfs.gz.aaa* bis *hda1.ntfs.gz.zzz* durchgezählt werden.

…und zackig zurückgespielt

Für das Zurückspielen eines Backups muss eine gleich große oder größere NTFS-Partition vorhanden sein, die kein Dateisystem benötigt. Am einfachsten ist es natürlich bei einem unkomprimierten Image. Statt des kleinen *o* ist ein großes *O* zu verwenden:

```
ntfsclone -r -O /dev/hda1
➥hda1.ntfs
```

Ist das Image gepackt, muss die Pipeline umgedreht werden:

```
gunzip -c hda1.ntfs.gz | \
ntfsclone -r -O /dev/hda1 -
```

Gesplittete Images setzt *cat* zusammen:

```
cat hda1.ntfs.gz.* | gunzip -c | \
ntfsclone -r -O /dev/hda1 -
```

Haben Sie die Sicherung auf eine größere Partition zurückgespielt, können Sie nach dem ersten Start von Windows erneut Knoppix booten und mit

```
ntfsresize /dev/hda1
```

das Dateisystem bis an die Partitionsgrenzen strecken. Bei der Rücksicherung auf eine frische oder zuvor „genullte" Platte benötigt Windows einen Master Boot Record:

```
ms-sys -m /dev/hda
```

auf Plausibilität prüfen. Nach dem gleichen Prinzip, aber mit einem etwas komfortableren Frontend arbeitet *testdisk*, das zudem Fehler korrigieren kann, die durch defekte Bootloader verursacht sind. Dafür ist die Erkennungsleistung von *gpart* oft etwas besser, was sich allerdings auch in einer höheren Zahl von Fehlalarmen niederschlägt.

Virtueller Kammerjäger

Dank Start vom sauberen Medium scheinen Live-Medien ideal zur Viren- und Wurmsuche geeignet sein. Leider hinken die meist enthaltenen freien Virenscanner deutlich der kommerziellen Konkurrenz hinterher. Sie bringen zwar beim Aufspüren typischer Mailwürmer gute Erkennungsleistungen, finden aber selten Schad-Software, die sich bereits eingenistet hat. Dank UnionFS kann jedoch unter Knoppix und Insert zusätzliche Software nachinstalliert werden. Recht gut mit Live-CDs harmoniert der Virenscanner *AntiVir* von **www. freeav.de**, der nach Download und Entpacken mit dem Kommando

```
./install
```

ins UnionFS installiert wird. Anschließend aktualisiert

```
antivir --update
```

die Signaturen, woraufhin der Scanner bereitsteht. Zu überprüfende Partitionen müssen gemountet sein:

```
antivir -z -s
➥/media/hda1
```

Zum Testzeitpunkt harmonierte die in Java programmierte grafische Oberfläche leider nicht optimal mit Live-CDs, da sie alle Dateisysteme unterhalb vom Wurzelverzeichnis scannte, also den Inhalt des komprimierten Live-Dateisystems und dessen Containerdatei.

Findet AntiVir Schädlinge, sollen diese in der Regel gleich beseitigt werden. Leider bringt Linux noch keinen Kernel-NTFS-Treiber mit, der sichere Schreibzugriffe zulässt. Praktisch alle Live-CDs setzen deshalb auf so genannte Userspace-Treiber, die zwar sehr langsam arbeiten, aber immerhin für die Desinfektion einzelner Dateien ausreichen. Unter Knoppix genügt ein Rechtsklick auf die betreffende Partition und die Wahl des Menüpunktes *Lese-Schreibmodus ändern*, um Schreibrechte zu erlangen. Anschließend können mit

```
antivir -z -s -e -ren /media/hda1
```

gefundene Schädlinge ihrer angemessenen Behandlung zugeführt werden.

Kammerjäger: Dank UnionFS kann *AntiVir* auf einem laufenden Knoppix nachinstalliert werden.

Rückstandsfrei sauber

Dass die Formatierung einer Festplatte nicht genügt, um alle Daten rückstandsfrei zu löschen, zeigt bereits PhotoRec. Was also tun,

damit der Käufer Ihres Rechners nicht an Ihre Urlaubsbilder und E-Mails herankommt? Am besten ist es, die Festplatte ohne Rücksicht auf Partitionen Block für Block zu überschreiben. Ein Werkzeug, das dies nach den Spezifikationen der US-Militärs mit alternierenden Mustern tut, ist *DBAN*. Weil aber seit dem Ende der Sieben-Zoll-Floppies noch nie mittels Restmagnetismus Daten rekonstruiert werden konnten, gehört das „siebenmalige Überschreiben" als einzig sichere Löschmethode ins Reich der Agententhriller. Das „Nullen" mit einer Knoppix-CD sollte genügen und ist darüber hinaus flotter. Zum Einsatz kommt das Universal-Tool *dd*, das nichts anderes tut, als die Inhalte einer (Geräte-) Datei auf eine andere zu kopieren:

```
dd if=/dev/zero of=/dev/had
```

Mit Software alleine lassen sich jetzt keine Daten mehr rekonstruieren. Sollten Sie befürchten, dass jemand die Festplatten zerlegt und anhand kleinster Unterschiede in der Felddichte einzelne Bits wiederherstellt, können Sie zunächst Zufallszahlen als Datenquelle verwenden und in einem zweiten Durchgang noch einmal Nullen darüberschreiben:

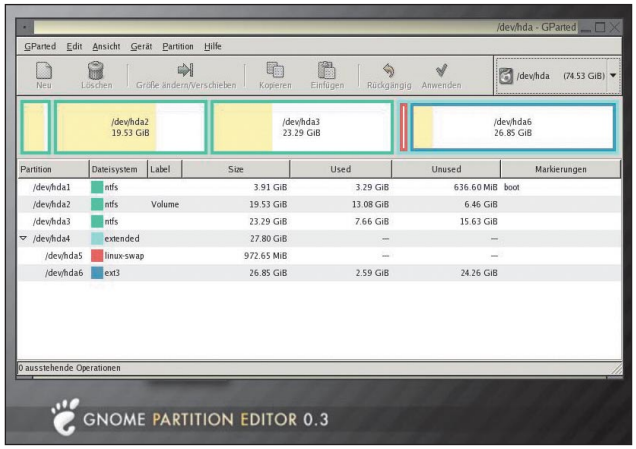
```
dd if=/dev/urandom of=/dev/hda
dd if=/dev/zero of=/dev/hda
```

Wollen Sie private Daten vor dem Einsenden einer defekten Festplatte an den Hersteller löschen, wird *dd* schnell fehlschlagen. Auch hier ist *dd_rescue* die Antwort. Der Parameter *-A* ist nicht notwendig, da bei */dev/zero* als Eingabedatei keine Lesefehler zu erwarten sind:

```
dd_rescue /dev/zero /dev/hda
```

Partitionsrochade

Auch für viele Arbeiten an der Partitionierung Ihrer Festplatten müssen Sie keine teure kommerzielle Software bemühen. Knoppix und Insert bringen mit *qtparted* und *gparted* Tools mit, die beim Verkleinern und Vergrößern von Partitionen helfen. Neuere Versionen von *garted* (ab 0.3) können NTFS-Partitionen auch verschieben. Da *gparted* aktiver entwickelt wird als *qtparted*, ist dieser Version der Vorzug zu geben. Am frischesten sind die vom *gparted*-Projekt selbst bereitgestellten Live-CDs, die meist nur wenige Tage nach neuen Versionen des Partitionierers erscheinen.



Komfortabler Partitionierer: *Gparted bzw.* Qtparted erlauben auch die Größenänderung von NTFS-Partitionen.

Vor Änderungen an der Partitionstabelle sollten Sie eingehängte Partitionen unmounten und die Verwendung von Auslagerungspartitionen stoppen:

```
swapoff -a
```

Dass keine Partition mehr gemountet ist, zeigt *df*, mit *top* oder *free* erhalten Sie die Bestätigung, dass Swap deaktiviert wurde. Sollten Sie NTFS-Partitionen verkleinern wollen, ist es ratsam, das enthaltene Dateisystem vorher unter Windows zu defragmentieren und die Auslagerungsdatei beim Herunterfahren löschen zu lassen. Den Partitionierer starten Sie schließlich mit

```
sudo qtparted
```

oder aus dem Startmenü der Live-Scheibe. Falls Sie „nur" Platz für eine Linux-Installation schaffen wollen, reicht es, die Windows-Partition zu verkleinern. Aktuelle Distributionen legen dann im freien Platz selbsttätig Partitionen an. **jkn**

Komfortabler mit Netz

Bereits die Möglichkeit, USB-Wechselmedien mit hoher Geschwindigkeit anzusprechen und CD- und DVD-Brenner nutzen zu können, ist ein gewaltiger Vorteil beim Einsatz von Linux als Rettungs- und Notfallsystem. Eine weitere große Hilfe sind die Netzwerkserver, die schnell aktiviert werden können. Am vielseitigsten ist natürlich SSH. Starten Sie den Daemon auf der Live-CD mit dem Befehl

```
sudo /etc/init.d/ssh start
```

Setzen Sie dann mit

```
sudo passwd
```

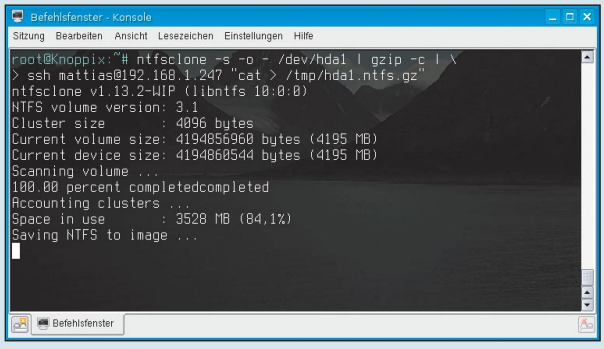
ein Passwort für den Administrator *root*. Der Befehl *ifconfig* zeigt die aktuelle IP-Adresse, unter der das Notfall-Linux erreichbar ist. Login und Datenübertragung ist von anderen Linux-Rechnern auf der Kommandozeile mit *ssh* oder *scp* möglich, ein grafisches Frontend bietet Konqueror mit dem URL-Schema

```
fish://root@123.45.67.89
```

Um von Windows-Rechnern im Netz aus per SCP auf das Knoppix zugreifen zu können, benötigen Sie das Tool *WinSCP* (www.winscp.net).

Fortgeschrittene Nutzer umgehen lokale Platzprobleme, indem sie beispielsweise ein mit *dd_rescue* oder *ntfsclone* erzeugtes Image über eine Pipeline zu einem im lokalen Netzwerk erreichbaren Rechner schicken. Der auf dem entfernten Rechner auszuführende Befehl muss in Anführungszeichen gesetzt werden:

```
ntfsclone -o -- /dev/hda1 | \
ssh ich@98.76.54.123 „cat > /tmp/hda1.ntfs"
```



Netzwerkweit: Ist unter Knoppix der SSH-Daemon aktiv, können Sie mit *WinSCP* oder *Konqueror* auch auf die Daten gemounteter Partitionen zugreifen und Daten über das Netzwerk sichern.