Gelöschte Dateien mit PhotoRec wiederherstellen

# Gerettet

**Thomas Drilling**

Bei irrtümlich gelöschten Dateien hilft das kostenlose Werkzeug PhotoRec rasch aus der Klemme.

Auf dem Desktop bringt der Papierkorb versehentlich gelöschte Dateien wieder zum Vorschein. Mit externen Datenträgern hingegen funktioniert das meist nicht. Die beiden quelloffenen Datenrettungstools PhotoRec und TestDisk kommen im Paket daher. Während letzteres beschädigte Partitionen oder Partitionstabellen repariert, stellt PhotoRec die gewünschten Dateien wieder her.

Die Software gibt es für Linux, diverse BSD-Distributionen, Solaris, Apples OS X und Windows. Unter Linux installiert man das Paket *testdisk*, dem PhotoRec beiliegt, aus den Standardpaketquellen der Distribution.

PhotoRec durchsucht Festplatten sowie wechselbare Medien wie CD-ROM/DVDs, Compact-Flash- und SD-Karten, SmartMedia, Microdrives, MMCs, Speicher-Sticks und USB-Laufwerke. Mit *dd* erstellte Raw-Images kann es ebenfalls verarbeiten. Ferner kann es den internen Speicher von Fotokameras analysieren. Eine Liste der unterstützten Modelle und Dateiformate findet sich auf der Projektseite www.cgsecurity.org/wiki/PhotoRec.

## Carving auf der Datenpiste

Beim Wiederherstellen arbeitet PhotoRec nach dem Carving-Prinzip (engl. für „herausschälen“). Eine Carving-Engine durchsucht ohne Kenntnis des jeweiligen Dateisystems den Rohdatenstrom auf dem angegebenen Medium nach Signaturen bekannter Dateiformate. Da das Werkzeug auf Blockebene arbeitet, funktioniert das sogar mit beschädigten oder formatierten Datenträgern. Die Software kennt mehr als 180 Dateiformate – ursprünglich für Digitalkameras entwickelt, befinden sich vor allem Bilddateien darunter, inzwischen allerdings auch eine zunehmende Zahl anderer Dateiformate.

Auf der vom Nutzer angegebenen Zielpartition (die nicht mit der analysierten Partition identisch sein sollte) erzeugt PhotoRec ein Verzeichnis, in dem es alle rekonstruierten Dateien in nummerierten Unterordnern speichert. Da die Software das untersuchte Dateisystem ignoriert und daher nicht auf den Index des Datenträgers zugreifen kann, ist die ursprüngliche Verzeichnisstruktur samt allen Dateinamen unwiderruflich verloren. Die erzeugten Unterordner enthalten immerhin intakte Dateien, die man mit Werkzeugen wie dem Explorer, *find* oder etwas BASH-Know-how durchsuchen kann.

Der PhotoRec-Assistent hilft beim Finden gelöschter Dateien und führt den Nutzer interaktiv durch den Wiederherstellungsprozess. Unter Linux muss man das Programm mit *root*-Rechten starten und die Geräte- oder eine Image-Datei samt Pfad angeben. Zu forensischen Zwecken lässt sich mit der Option */log* eine Protokolldatei anlegen.

Zunächst möchte der Assistent wissen, welches Medium er analysieren soll. Hat man diese Angabe als Parameter übergeben, ist die Gerätedatei bereits markiert. Danach kann der Nutzer entscheiden, ob PhotoRec die komplette Festplatte analysieren soll oder nur eine bestimmte Partition, sofern nicht auch diese Angabe als Parameter übermittelt wurde. Im Menüpunkt „Optionen“ lassen sich unter anderem der Expertenmodus aktivieren oder das Löschen beschädigter Dateien unterbinden. Der Expertenmodus erlaubt das Einstellen von Blockgröße und Offset für das Dateisystem.

Standardmäßig eingestellt ist die Suchart „Paranoid“, womit PhotoRec wiederhergestellte Dateien überprüft und alle ungültigen Einträge, also nicht wiederherstellbare Dateien, verwirft. Mit „Brute force“ lassen sich hingegen sogar fragmentierte JPEG-Dateien retten, allerdings erfordert die Operation viel Prozessorleistung. Mit „Low memory“ schließlich verhindert man einen Absturz der Software wegen zu wenig Arbeitsspeicher, was bei besonders großen Dateisystemen passieren kann.

## Rohe Kräfte retten Bilder

Vom Hauptmenü aus lässt sich die Suche mit „Search“ starten. Den Partitionstyp muss man nur auswählen, falls PhotoRec ihn nicht erkennt. Mit „Free“ durchsucht die Software nur nicht zugewiesene Bereiche, mit „Whole“ das gesamte Laufwerk, was deutlich länger dauert. Schließlich wählt der Nutzer ein Verzeichnis für die rekonstruierten Daten. Der automatisch erstellte Zielordner *recup_dir* darf nicht auf dem korrumpierten Laufwerk liegen. Mit der Taste C startet man die Wiederherstellung. Der Vorgang kann je nach Laufwerkgröße einige Stunden dauern. In der Bildschirmanzeige lässt sich die Anzahl wiederhergestellter Dateien in Echtzeit verfolgen.

Das anschließende Durchsuchen des Wiederherstellungsverzeichnisses nach den gewünschten Dateien gleicht zwar einer Sisyphusarbeit, allerdings bieten Linux- und Unix-Systeme zahlreiche Möglichkeiten der Unterstützung. Folgendes Kommando etwa findet JPEG-Dateien und überträgt sie in ein *tar*-Archiv:

```
find ./ -iname "*.jpg" -exec tar -rf
bilder.tar {} \;
```

Unter Windows erledigt die PowerShell die Suche mit einem

```
Get-ChildItem -Include "*.jpg" -Recurse
```

Die Kommandozeilenversion von PhotoRec funktioniert unter Linux, Unix, OS X und Windows nahezu identisch. Die kommende Version 7 soll eine auf Qt basierende grafische Oberfläche erhalten, eine Betaversion kann man bereits herunterladen. (tiw)

**Thomas Drilling**

arbeitet seit 15 Jahren als freiberuflicher IT- und Technik-Journalist mit Schwerpunkt Linux und Open Source.

Alle Links: www.ix.de/ix1502134