Partitionen retten mit TestDisk

Restaurator

Thomas Drilling

Aus Unachtsamkeit oder durch Malware-Befall verloren gegangene Partitionstabellen und Bootsektoren kann das kostenlose Werkzeug TestDisk wieder restaurieren.

Nicht nur Dateien, auch Partitionen und Dateisysteme können Opfer von Angriffen oder unachtsamen Anwendern sein. Diese zu restaurieren tritt TestDisk an. Das Kommandozeilentool läuft auf allen gängigen Betriebssystemen; Linux-Distributionen bringen es meist mit.

Da beschädigte Partitionen häufig das Boot-Medium betreffen, benötigt der Nutzer zwangsläufig ein Reparatur-Medium. Deshalb wird er meist zu einem Linux-Live-System wie SystemRescue greifen, das TeskDisk an Bord hat.

Es kann unter anderem Bootsektoren der üblichen FAT- und NTFS-Versionen wiederherstellen, File Allocation Tables (FAT) und NTFS Master File Tables (MFT) reparieren, ext2/3/4-Superblock-Backups finden, gelöschte Dateien in FAT-, NTFS- und ext2-Partitionen restaurieren sowie zusätzlich solche von gelöschten ext3/4-Partitionen kopieren. Außer den von Windows oder Linux im MBR angelegten Partitionstabellen kennt es Apples Partition Maps, EFI GPT (GUID Partition Table), BSD- und Solaris-Disklabel. TestDisk identifiziert neben den Partitionen für die oben genannten Dateisysteme solche für BeOS, Btrfs, CramFS, HFS/HFSX, JFS, GFS2, ReiserFS UFS/UFS2, Wii WBFS, XBox FATX, XFS und ZFS. Darüber hinaus kann es unter Linux mit Swap-, verschlüsselten LUKS-Partitionen, mit dem LVM sowie mit Software-RAIDs 1, 4, 5 und 6 (*md*) umgehen, außerdem mit Novells Storage Services (NSS).

Zum Auslesen der Festplattendaten benötigt TestDisk aber Hilfe vom BIOS und vom Betriebssystem. Daher liefert es, auch wenn ein Reparaturversuch scheitert, wertvolle Informationen. Dazu benötigt es *root*-Rechte und kann bei unsachgemäßer Anwendung großen Schaden anrichten.

Je nach Ursache zeigen kompromittierte Festplatten unterschiedliche Symptome. So könnte der Windows-Explorer eine gelöschte Partition als „RAW“ oder als „nicht zugeordneten Speicher“ melden. Auch fehlende oder falsche Laufwerksbezeichnungen deuten auf beschädigte Partitionstabellen oder Partitionen hin.

Wiederherstellen fast wie von selbst

Ohne Parameter aufgerufen, zeigt TestDisk alle identifizierten Geräte an. Hat der Nutzer das gewünschte Laufwerk ausgewählt, fragt es den Typ der Partitionstabelle ab und präsentiert dann das Hauptmenü. Mit *MBR Code* lässt sich ein neuer MBR schreiben, sofern die Geometrie noch stimmt. Am Anfang steht aber in der Regel eine grundlegende Analyse des gegenwärtigen Zustands. Bei fehlenden Partitionen sollte man das Ergebnis gewissenhaft auf entsprechende Einträge prüfen.

So deuten „Bad relative sector. No partition is bootable“ und eine leere Partitionsliste auf einen Partitionstabellentyp hin. Taucht eine Partition zweimal mit identischem Eintrag auf oder ein zweiter mit falschem Partitionstyp, ist das ein Hinweis auf eine beschädigte Partition oder einen ungültigen Eintrag in der Partitionstabelle. Ein „Invalid NTFS boot“ lässt auf einen fehlerhaften Bootsektor und ein kaputtes Dateisystem schließen. Stimmt „nur“ die Festplattengeometrie nicht, zeigt sich das an „Incorrect number of heads/cylinder 255 (NTFS) = 240 (HD)“ oder „Bad sector count“, „Bad relative sector“ und „Bad ending head“, sodass sich Partitionen unter Umständen überlappen. In diesem Fall kann der Nutzer im Menü *Geometry* die Laufwerksgeometrie korrigieren und anschließend im Menü *Analyse* eine gründliche Untersuchung starten.

Mit etwas Glück fördert hierbei *QuickSearch* schon im ersten Schritt verlorenen gegangene Partitionen wieder zu Tage. Bei Erfolg lässt sich die restaurierte Partitionsstruktur mit *Write* sichern. Bei logischen Laufwerken in einer erweiterten Partition kann der Nutzer im Menü *Extd Part* festlegen, ob die erweiterte Partition den verfügbaren oder den benötigten Speicherplatz belegt. Zudem lassen sich mit *p* die enthaltenen Dateien anzeigen. Im ungünstigsten Fall führt das zum Ergebnis „file found, filesystem may be damaged“.

Dann oder wenn QuickSearch keine Partitionen identifiziert, verlässt man die Dateiliste mit *q* und wählt die *Deeper Search*. Sie fahndet nach den Backups von FAT, MFT und – bei Dateisystemen der Unixoiden – nach Superblocks. Sie finden sich ausgehend vom Original-Superblock an bestimmten Offsets.

Versucht man, ein korruptes ext-Dateisystem allein mit *fsck* zu reparieren, kann die Fahndung nach alternativen Superblocks schnell scheitern, weil ihre Positionen von der Blockgröße des Dateisystems abhängen, deren Größe dummerweise ebenfalls im ersten Superblock steht. So liefert etwa *dumpe2fs –h /dev/<partition>* alle im Superblock gespeicherten Informationen. Mit TestDisk lassen sich die Positionen von Superblock-Kopien im Menü *Advanced* ermitteln und anschließend mit *fsck* verwenden, etwa mit */sbin/fsck.ext4 –b 8193 –B 1024 /dev/sda2* für eine Superblock-Kopie beim Block 8193 und einer Blockgröße von 1024 Bytes.

Tauchen verlorene Partitionen wieder auf, liefert *p* mit etwas Glück die restaurierte Struktur mit gültiger Dateiliste. Man kann sie übernehmen oder die Dateien an einen sicheren Ort kopieren. Unter *Advanced* bietet TestDisk zudem an, ein *dd*-Image der Partition zu erzeugen. Dort lassen sich etwa auch gelöschte Dateien in ext2-Dateisystemen wiederherstellen. Dieser Querschnitt der Fähigkeiten zeigt, dass TestDisk wertvolle Dienste leistet, wenn man es mit Bedacht einsetzt. (sun)

Thomas Drilling

arbeitet als IT- und Technik-Journalist.

Alle Links: www.ix.de/ix1503152