

Dieser Artikel ist Teil der **HOWTO Sammlung**

Trotz Backup kann es passieren, dass Dateien, die gelöscht wurden, vom Originaldatenträgern wiederhergestellt werden müssen, wenn zum Beispiel gerade kein Zugriff auf die Backup-Medien vorhanden oder eben kein Backup vorhanden ist. foremost ist ein Konsolen-Programm, welches da behilflich sein kann. Es kann Dateien auf Basis deren Headers, Footers und internen Datenstrukturen wiederherstellen.

Inhaltsverzeichnis

- 1 Installation
- 2 Konfiguration
- 3 Verwendung
- 4 Siehe auch

Installation

Die Installation ist mit yum, pirut oder yumex schnell erledigt.

```
[root]# yum install foremost
```

Konfiguration

foremost besitzt ein Konfigurations-File [/etc/foremost.conf](#). Dieses enthält Informationen für die Wiederherstellung von diversen Dateien, die nach der Installation alle auskommentiert sind. Die Erweiterungen, welche mit *NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION* angegeben sind, sind bereits eingebaut und müssen nicht aktiviert werden.

Ein Auszug für MPEG-Video

```
# MPEG Video
#     mpg      y      4000000  mpg      eof
#     mpg      y      20000000 \x00\x00\x01\xba  \x00\x00\x01\xb9
#     mpg      y      20000000 \x00\x00\x01\xb3  \x00\x00\x01\xb7
```

Es ist angegeben in jedem Absatz angegeben, ob foremost die Funktion eingebaut hat oder nicht. Es wäre auch möglich, dass man eigene Erweiterungen hinzufügt.

Verwendung

Zur Sicherheit sollte vor der Manipulation ein Abbild des Dateisystems gemacht werden, so dass nicht noch mehr Schaden angerichtet wird. Dazu wird Disk Dump, kurz `dd` verwendet. Als Beispiel wird ein Abbild eines USB-Memorystick ([/dev/sdc](#)) in ein Benutzer-Verzeichnis gemacht.

```
[root]# dd if=/dev/sdc of=/home/user01/sicherung.dd
```

Die Ausgabe nach erfolgreichem Kopieren sieht wie folgt aus.

```
3917824+0 Datensätze ein
3917824+0 Datensätze aus
2005925888 Bytes (2,0 GB) kopiert, 193,708 Sekunden, 10,4 MB/s
```

Nun kann `foremost` gestartet werden. Mit dem Parameter `-t` und `all` werden alle Dateien wiederhergestellt. Für eine vollständige Liste der Parameter kann `foremost` mit `-h` gestartet werden oder das Man-File konsultiert werden.

```
[root]# foremost -t all -i /home/user01/sicherung.dd
```

`foremost` informiert über den Fortschritt

```
Processing: /home/user01/sicherung.dd
|*****|
```

nach Beendigung sind alle wiederhergestellten Daten im Verzeichnis [/home/user01/output](#) nach Dateiendungen sortiert und aufgelistet.

Siehe auch

- ◇ [Foremost Website](#)
- ◇ [TestDrive](#)