

Inhalt der initrd

openSUSE verwendet zum Bau der initialen Ramdisk (initrd) seit einiger Zeit dracut (das auch per mkinitrd aufgerufen werden kann). Manchmal möchte man in diese Datei reinschauen, um zu sehen, was denn nun enthalten ist. Das ist nicht ganz trivial. Die Lösung habe ich auf <https://ask.fedoraproject.org/en/question/57887/how-to-coorectly-extract-initrd0img-from-fedora21-beta-livecd/> gefunden, und ich habe sie mal für eine konkrete Kernelversion auf openSUSE Leap 42.3 angepasst.

- man erstelle ein Verzeichnis und wechsele hinein:

```
mkdir /tmp/initrdmount
cd /tmp/initrdmount
```

- das Programm binwalk wird benötigt. Wenn es noch nicht installiert ist (es gehört zum Umfang der Distro, wird aber per Default nicht installiert):
zypper in binwalk
- wir sehen uns den Inhalt bzw. die Struktur der initrd an:

```
binwalk /boot/initrd-4.4.92-31-default
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	ASCII cpio archive (SVR4 with no CRC), file name: ".", file name length: "0x00000002", file size: "0x00000000"
112	0x70	ASCII cpio archive (SVR4 with no CRC), file name: "early_cpio", file name length: "0x0000000B", file size: "0x00000002"
240	0xF0	ASCII cpio archive (SVR4 with no CRC), file name: "kernel", file name length: "0x00000007", file size: "0x00000000"
360	0x168	ASCII cpio archive (SVR4 with no CRC), file name: "kernel/x86", file name length: "0x0000000B", file size: "0x00000000"
484	0x1E4	ASCII cpio archive (SVR4 with no CRC), file name: "kernel/x86/microcode", file name length: "0x00000015", file size: "0x00000000"
616	0x268	ASCII cpio archive (SVR4 with no CRC), file name: "kernel/x86/microcode/GenuineIntel.bin", file name length: "0x00000026", file size: "0x0000B000"
45820	0xB2FC	ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", file size: "0x00000000"
46080	0xB400	xz compressed data

- ab hier gibt es zwei Wege, den manuellen und den automagischen:
 - manuell:
 - wir extrahieren den komprimierten Teil:

```
dd if=/boot/inited-4.4.92-31-default of=initedramfs.xz bs=46080 skip=1
219+1 Datensätze ein
219+1 Datensätze aus
10126544 bytes (10 MB, 9,7 MiB) copied, 0,00315395 s, 3,2 GB/s
```

- die extrahierte Datei wird entkomprimiert:
unxz initedramfs.xz
- die entkomprimierte Datei wird wieder in etliche Dateien umgewandelt:

```
cpio -i -d -H newc --no-absolute-filenames < initedramfs
61140 blocks
```

- mit Automatik:
 - Auspacken und Zerlegen in einem Schritt:
/usr/lib/dracut/skipcpio /boot/inited-4.4.92-31-default | unxz | cpio -i
 - um zu Wissen, welchen Entpacker man benutzt, muss man mit binwalk den Inhalt der inited prüfen. Im vorliegenden Fall ist es xz compressed data, also nimmt man unxz. Bei gzip als Inhalt wäre es entsprechend gunzip usw.

Nun hat man ein Verzeichnis mit dem Inhalt der inited 😊

From:
<http://www.wernerflamme.net/> - **Werners Wiki**

Permanent link:
<http://www.wernerflamme.net/doku.php?id=comp:inited>

Last update: **2017-12-13 1237**

