

SystemRecovery mit RescueCD

Workshop vom 3. Oktober 2006 by Archivista GmbH, Urs Pfister

Inhaltsverzeichnis

1	Einleitung	2		
1.1	Copyright-Notiz	2		
2	Bevor wir loslegen	3		
2.1	Haftungsausschluss	3		
2.2	VMWare-Player	3		
2.3	RescueCD and VMWare Player	4		
3	Starten im Normalmodus	5		
4	Linux-Crashkurs	6		
4.1	Hilfe zur CD	6		
4.2	Netzwerkkarte überprüfen . .	6		
4.3	Recherchen im Internet . . .	7		
4.4	SSH-Server und Passwort setzen (root)	8		
4.5	Dateien editieren	8		
4.6	Partitionen einrichten	9		
4.7	Arbeiten mit MidnightCom- mander	10		
4.8	Laufwerke einbinden	10		
5	Schreibzugriff auf NTFS- Platten herstellen	12		
			5.1	Dateien kopieren 12
			6	Windows-Passwörter zurück- setzen 14
			6.1	RescueCD neu starten 14
			6.2	F2 bzw. ntpass beim Start- screen wählen 14
			6.3	Festplatte, Registry und Ac- count bearbeiten 15
			6.4	Änderungen definitiv auf Platte schreiben 17
			6.5	Neustart und Festplattenre- organisation 17
			7	Zugriff von Windows auf Ext3-Dateisysteme 19
			8	PartImage 21
			8.1	Client-Modus 21
			8.2	Server-Modus 21
			9	QTParted 24
			10	Backup mit flexbackup 25

© 2.10.2006 by Archivista GmbH, Homepage: www.archivista.ch

1 Einleitung

Wer zu spät kommt, der hat das Nachsehen. Backups sind keine Frage des Budgets. Wie können Installationen sauber gesichert werden, welche Backup-Technologien bieten sich an, was tun, wenn es trotzdem einmal brennt und was können wir weit vor dem 'Ernstfall' tun, damit wir sicher über die Runden kommen?

1.1 Copyright-Notiz

Copyright (c) 2006 by Archivista GmbH, Urs Pfister. Dieses Dokument untersteht der Open Publication Lizenz, v1.0 (8. Juni 1999) oder später (siehe www.opencontent.org/openpub für die letzte Version).

Die Weitergabe ist ausdrücklich unter diesen Konditionen erlaubt und erwünscht.

2 Bevor wir loslegen

Damit wir arbeiten können, benötigen wir eine sogenannte SystemRescue-CD, in unserem Fall arbeiten wir mit der auf Gentoo basierenden LiveCD SystemRescueCD, die wir unter www.sysresccd.org beziehen können.

Die ISO-Datei ist (Stand Oktober 2006) ca. 120 MByte gross. Was ist nun eine SystemRescueCD? Wie der Name erahnen lässt, verwenden wir diese im Falle des (Not-)Falles, um z.B. Backups zu erstellen, mit Partitionen zu arbeiten, Passwörter wieder herzustellen usw.

2.1 Haftungsausschluss

Beim Arbeiten mit einer SystemRescueCD ist Vorsicht geboten. Eine falsche Eingabe und die gesamte Installation (die wir ja eigentlich hätten retten bzw. backupen wollen) ist definitiv verloren. Daher als Warnung vorweg: Spielen wir mit der SystemRescueCD in 'guten' Zeiten mit einer Testmaschine (bzw. dem VMWare-Player), bevor wir diese im Notfall einsetzen! Falsch eingesetzt, können wir mit der RescueCD relativ schnell sehr viel zerstören; und darum geht es hier ja nicht.

2.2 VMWare-Player

Damit wir 'sorgenfrei' üben können, empfiehlt sich der Einsatz des VMWare-Players. Wir können diesen sowohl für Windows als auch Linux unter www.vmware.com/download/player/ beziehen und installieren.

Anschliessend können wir ab unserer Homepage die Dateien für eine virtuelle ArchivistaBox beziehen und diese installieren. Die Datei `avbox.zip` finden wir unter www.archivista.ch/avbox.zip. Nach dem Entpacken finden wir im Unterordner ArchivistaBox die Datei 'ArchivistaBox.vmx'. Kopieren wir nun die ISO-Datei der SystemRescue CD in diesen Ordner und geben ihr den Namen (Gross-/Kleinschreibung beachten) 'archivista_cd1.iso'.

Anschliessend können wir die Datei 'ArchivistaBox.vmx' starten.

Hinweis: Die Datei 'ArchivistaBox.vmx' (bzw. sämtliche VMWare-Player-Dateien) kann auch editiert werden, dazu kann das Windows-Programm 'vmmanager' (siehe www.sourceforge.net) verwendet werden.

2.3 RescueCD and VMWare Player

Grundsätzlich arbeitet die RescueCD problemlos mit dem VMWare Player zusammen. Beim Starten muss einfach die ESC-Taste gedrückt werden, damit wir das CD-Rom-Laufwerk als Boot-Laufwerk auswählen können.

Zu beachten gilt es allerdings, dass (zumindest bei mir) die virtuellen Terminals 2 bis 6 nicht funktionierten. Ein Umschalten in diesen Modus führte bei mir zu einem schwarzen Screen, den ich nur noch mit `killall X` rückgängig machen konnte.

3 Starten im Normalmodus

Stellen wir sicher, dass der Computer ab CD/DVD-Rom bootet, legen wir die CD ein und starten wir den PC neu.



**System
Rescue-CD**

- * Linux kernel-2.6.16
(with Reiser4 and FrameBuffer)
- * Logical Volumes (EVMS, LVM)
- * Hardware autodetection
- * QtParted (graphical partition tool)
- * Most important system tools
(parted, partimage, dump/restore,
sfdisk, dar, *fs-tools, ClamAV)
- * Midnight Commander (mc)
- * Editors (vim, nano, QTinyEditor)
- * Network tools
(Samba, NFS, LUFS, SSH)

<http://www.sysresccd.org>

```
Welcome to SystemRescueCd version 0.2.19
F2,F3,F4 for boot options help, or menu
Enter to boot.
boot:
```

Im Normalfall drücken wir die Enter-Taste, um nach einer Weile eine Abfrage betr. der Tastatur zu erhalten.



```
ebt_olog: not logging via ulog since somebody else already registered for PF_BRI
DGE
NET: Registered protocol family 8
NET: Registered protocol family 20
802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
All bugs added by David S. Miller <davem@redhat.com>
Using IPI Shortcut mode
md: Autodetecting RAID arrays.
md: autorun ...
md: ... autorun DONE.
RAMDISK: Compressed image found at block 0
UFS: Mounted root (ext2 filesystem) readonly.
Freeing unused kernel memory: 516k freed
Creating initial device nodes...
Please select a keymap from the following list by typing in the appropriate
name or number. Hit Enter for the default "speakup-us" keymap.

 1 azerty   7 cf       13 es      19 il      25 nk      31 ru       37 trf
 2 be       8 croat    14 et      20 is      26 nl      32 se       38 trq
 3 bg       9 cz       15 fi      21 it      27 no      33 sg       39 ua
 4 br-a     10 de     16 fr      22 jp      28 pl      34 sk-y     40 uk
 5 br-l     11 dk     17 gr      23 la      29 pt      35 sk-z     41 us
 6 by      12 dvorak  18 hu      24 lt      30 ro      36 slovene  42 wangbe
43 fr_CH   44 speakup 45 cs_CZ

Keymap selection: 33
```

Beim ersten Aufstarten habe ich verkrampft nach de_CH gesucht, und nur fr_CH gefunden, nach einiger Zeit (wer möchte sich schon die Blöße geben zuzugeben, dass er ob eines solchen Details lange Zeit verliert) hab ich dann sg für SwissGerman entdeckt, worauf die Disk auch mit dem richtigen Tastatur-Layout bootete.

4 Linux-Crashkurs

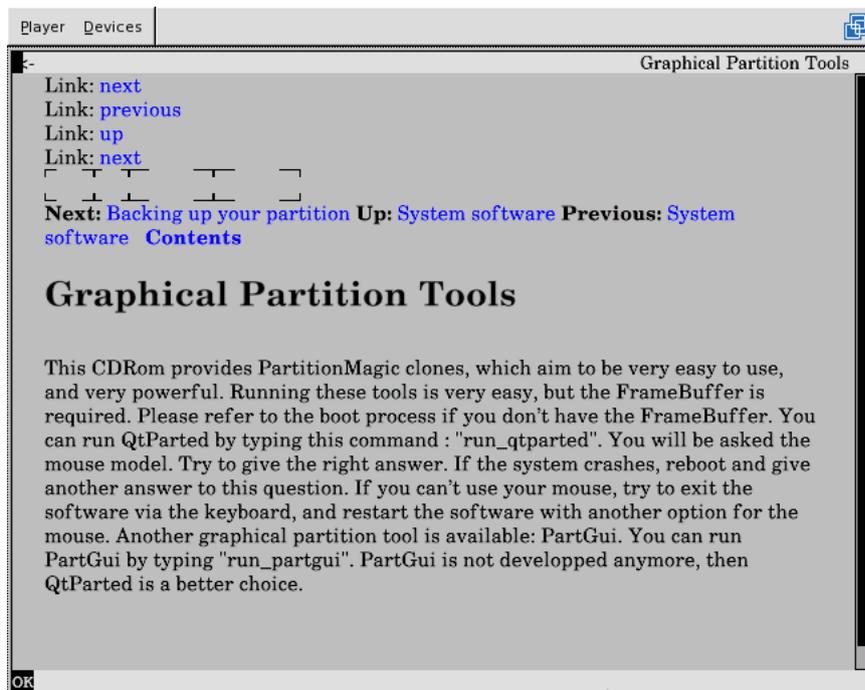
Nach dem Start gelangen wir auf eine Linux-Konsole. Doch keine Bange, wir benötigen nicht wirklich Linux-Kenntnisse, um mit der RescueCD arbeiten zu können.

4.1 Hilfe zur CD

Rufen wir zunächst einmal die Hilfe der CD auf. Dazu geben wir ein:

```
links -g /root/manual-en/index.html
```

Oh Wunder, da erscheint die Hilfe ja richtig in einem grafischen Browser:



Um die Hilfe zu verlassen, geben wir ein q ein.

4.2 Netzwerkkarte überprüfen

Normalerweise started die RescueCD so, dass ein bestehendes Netzwerk (DHCP) automatisch erkannt und die IP-Adresse selbstredend zugewiesen wird. Mit `ifconfig` können wir nun nachsehen, welche Einstellungen für uns gültig sind.

```
Player Devices
14:29 root@sysresccd /root %
14:29 root@sysresccd /root % ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F9:47:43
          inet addr:192.168.2.231  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2823 (2.7 Kb)  TX bytes:1728 (1.6 Kb)
          Interrupt:10 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:216 (216.0 b)  TX bytes:216 (216.0 b)

14:29 root@sysresccd /root % _
```

Die Netzwerkkarte kann zudem mit `net-setup eth0` (erste Netzwerkkarte) manuell konfiguriert werden.

4.3 Recherchen im Internet

Wenn immer möglich sollte eine zweite Maschine zum Browsen bereitstehen, damit wir z.B. nachsehen könnten, wie wir eine Festplatte partitionieren etc. Wir können allerdings auch mit der RescueCD browsen:

```
links -g www.archivista.ch
```

Wichtig zu wissen ist, dass wir nur immer eine Adresse wählen können. 'Links' ist etwas limitiert und mit komplexeren Layouts kann es auch mal gewisse Darstellungsprobleme geben.



4.4 SSH-Server und Passwort setzen (root)

Damit wir von aussen auf die Maschine zugreifen können (z.B. um Dateien aufzuspielen), verwenden wir am einfachsten den SSH-Server. Dazu muss zunächst der Dienst gestartet werden. Geben wir dazu ein:

```
/etc/init.d/sshd start
```

Dabei werden beim ersten Aufruf einige Schlüssel (keys) erstellt. Anschliessend sollten wir der Maschine noch ein Passwort spendieren, damit wir mit diesem Passwort von aussen zugreifen können.

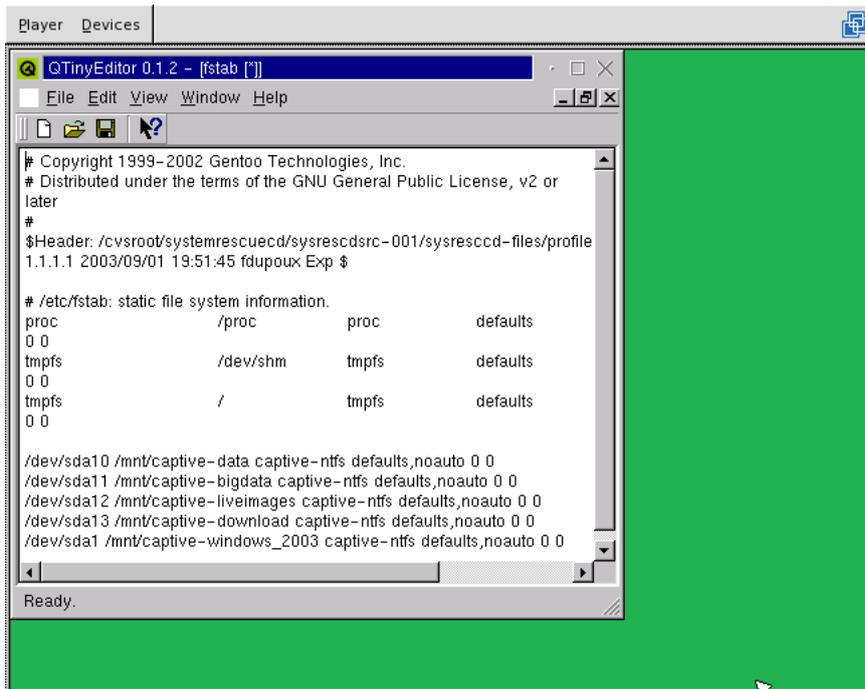
```
passwd
```

Geben wir nun zweimal das Passwort ein, am Ende sollten wir die Meldung 'password updated successfully' erhalten.

Nun können wir von einem beliebigen anderen Rechner auf die Maschine mit SSH zugreifen. Unter Linux werden wir wohl scp, sftp oder ssh verwenden wollen, für Windows-Benutzer/innen empfehle ich das Programm WinSCP (Download über www.winscp.org, mit dem sich bequem Dateien hin- und herschieben lassen.

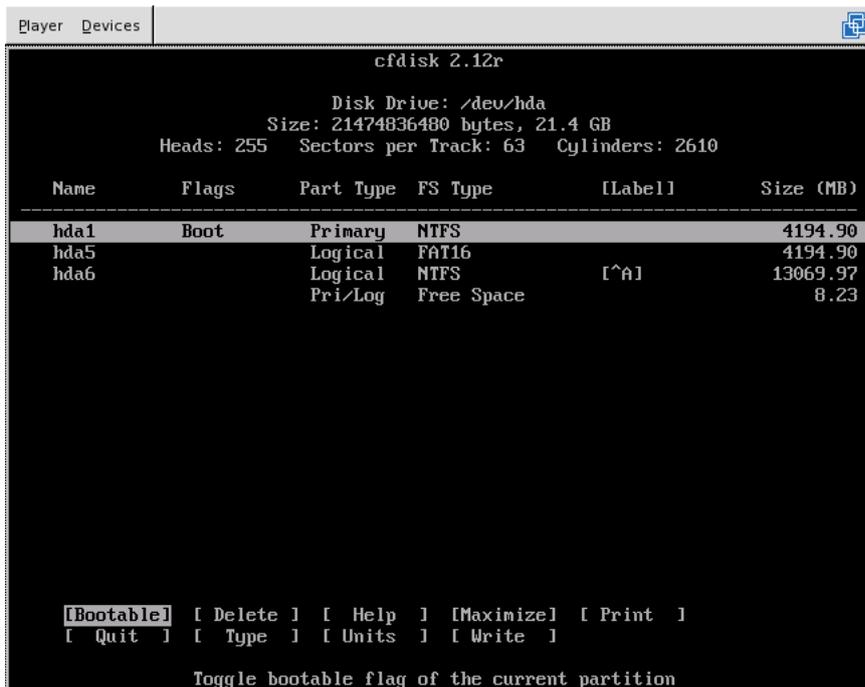
4.5 Dateien editieren

Ab und zu werden wir auch Dateien editieren wollen/müssen. Dazu kann der grafische Editor `run_qtineditor` verwendet werden.



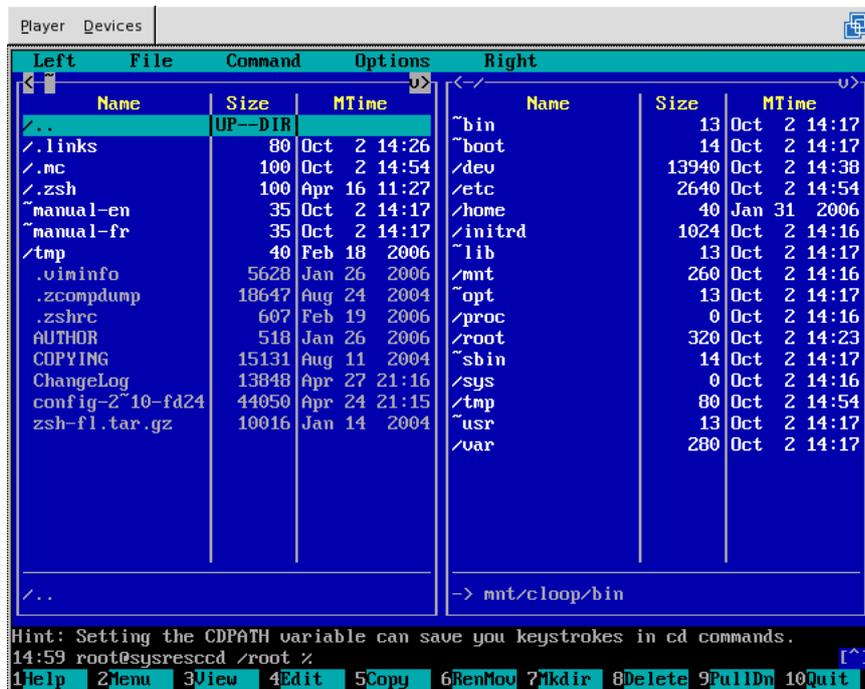
4.6 Partitionen einrichten

Um Partitionen einzurichten (nur falls diese noch nicht existieren), können wir analog zu fdisk (Windows) unter Linux `cdisk` verwenden.



4.7 Arbeiten mit MidnightCommander

Leider habe ich schon in jungen Jahren den legendären NortonCommander verpasst (die DOS-Shell fand ich damals praktischer¹). Viele Systemadministratoren/innen sind damit jedoch gross geworden und daher gibt es ein ähnliches Programm auch für Linux unter dem Namen MidnightCommander, kurz `mc`. Starten wir diesen kurz, finden wir die gewohnte Umgebung vor:



Soll noch jemand sagen, er könne mit diesem Programm keine Dateien bearbeiten.

4.8 Laufwerke einbinden

Beim Start der RescueCD werden keine Laufwerke eingebunden. Daher ist hier etwas Handarbeit notwendig. Und kurz zur Erläuterung: Unter Linux verwenden wir den Befehl `mount`, um Laufwerke einzubinden und `umount` um die Verbindung wieder zu lösen. Danach geben wir meist den Typ an mit `-t ntfs`, gefolgt vom Laufwerk, das eingebunden werden soll (z.B. erste Partition auf erster Platte mit `/dev/hda1`) sowie jenen Ort, wo wir 'hinmounten' wollen (z.B. `/mnt/part`). Das gesamte Beispiel nochmals auf einer Zeile:

```
mount -t ntfs /dev/hda1 /mnt/part
```

Falls wir eine klassische Windows-Installation haben, können wir danach mit `cd /mnt/part` sowie `ls -ls` nachsehen, dass wir eine Windows-Partition haben. Alternativ verwenden wir `mc`.

¹Leider gab es damals Linux noch nicht, sodass ich erst später die Stärken der Shell kennen und schätzen lernte

Um die Verbindung wieder zu lösen, geben wir `umount /mnt/part` ein.

5 Schreibzugriff auf NTFS-Platten herstellen

Heutzutage sind praktisch sämtliche Windows-Festplatten mit dem Format 'NTFS' formatiert. Leider sind die Spezifikationen dazu nicht vorhanden, sodass wir mit der RescueCD vorerst (wie oben beschrieben) nur NTFS-Platten lesend einbinden können.

Dank dem Hilfsprogramm 'captive-ntfs' können solche Platten auch schreibend eingebunden werden. Allerdings ist der Weg dahin etwas steinig, weil wir dazu zwei Original-Windows-Dateien (ntfs.sys sowie ntoskrnl.exe) benötigen. Damit ist auch gesagt, dass das nachfolgende Vorgehen nur zulässig ist, wer eine Windows-Installation sein eigen nennt. Leider kann es zudem noch sein, dass erst die besagten Dateien des ServicePacks 1 ausreichen, um auf NTFS-Platten zuzugreifen. In diesem Falle können die Dateien aber vor der Installation des ServicePacks herauskopiert werden (unter Hilfestellung von WinRar, mit dem die Datei ntoskrnl.ex_ in ntoskrnl.exe umgewandelt werden muss).

Hinweis: Leider ist die Hilfestellung der RescueCD nicht korrekt, daher beschreibe ich das Vorgehen hier nochmals.

5.1 Dateien kopieren

Angenommen, wir haben auf /dev/hda6 unser Windows installiert. Geben wir danach die folgenden Befehle ein:

```
mount -t ntfs /dev/hda6 /mnt/part
cp /mnt/part/WINDOWS/system32/drivers/ntfs.sys /var/lib/captive
cp /mnt/part/WINDOWS/system32/ntoskrnl.exe /var/lib/captive
chmod 0000 /
umount /mnt/part
mount -t captive-ntfs /dev/hda6 /mnt/part
```

Die nachfolgende Abbildung zeigt das nochmals (inkl. der etwas 'sinnlosen' Aktion, die Datei /etc/fstab auf die Windows-Partition zu kopieren):

```
Player  Devices 
15:19 root@sysresccd / %
15:19 root@sysresccd / % mount -t ntfs /dev/hda6 /mnt/part
15:19 root@sysresccd / % cp /mnt/part/WINDOWS/system32/drivers/ntfs.sys /var/lib
/captive
15:19 root@sysresccd / % cp /mnt/part/WINDOWS/system32/ntoskrnl.exe /var/lib/cap
tive
15:20 root@sysresccd / % chmod 0000 /
15:20 root@sysresccd / % umount /mnt/part
15:20 root@sysresccd / % mount -t captive-ntfs /dev/hda6 /mnt/part
15:20 root@sysresccd / % cd /mnt/part
15:20 root@sysresccd /mnt/part % ls
Dokumente und Einstellungen System Volume Information pagefile.sys
Programme WINDOWS
15:20 root@sysresccd /mnt/part % cp /etc/fstab .
15:21 root@sysresccd /mnt/part % ls
Dokumente und Einstellungen System Volume Information fstab
Programme WINDOWS pagefile.sys
15:21 root@sysresccd /mnt/part %
```

6 Windows-Passwörter zurücksetzen

6.1 RescueCD neu starten

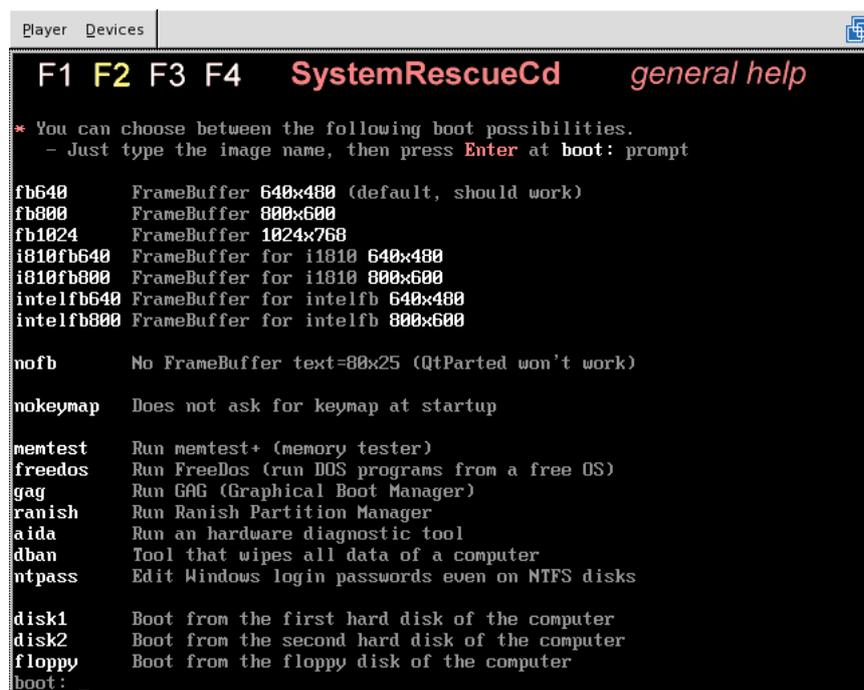
Eine der schönsten Funktionen der RescueCD dürfte sein, dass wir in einem speziellen Modus Passwörter der Benutzer zurücksetzen können, ohne in Windows angemeldet zu sein. Dazu starten wir zunächst einmal die RescueCD neu mit:

```
shutdown now -r
```

Anstelle von `-r` könnten wir auch `-h` eingeben, um die Maschine ganz auszuschalten (doch das wollen wir hier ja nicht).

6.2 F2 bzw. ntpass beim Startscreen wählen

Beim Startscreen drücken wir bitte F2, um den folgenden Screen zu erhalten:



```
Player  Devices  [icon]
F1 F2 F3 F4  SystemRescueCd  general help
* You can choose between the following boot possibilities.
  - Just type the image name, then press Enter at boot: prompt
fb640      FrameBuffer 640x480 (default, should work)
fb800      FrameBuffer 800x600
fb1024     FrameBuffer 1024x768
i810fb640  FrameBuffer for i810 640x480
i810fb800  FrameBuffer for i810 800x600
intelfb640 FrameBuffer for intelfb 640x480
intelfb800 FrameBuffer for intelfb 800x600
nofb       No FrameBuffer text=80x25 (QtParted won't work)
nokeymap   Does not ask for keymap at startup
mentest    Run mentest+ (memory tester)
freedos    Run FreeDos (run DOS programs from a free OS)
gag        Run GAG (Graphical Boot Manager)
ranish     Run Ranish Partition Manager
aida       Run an hardware diagnostic tool
dban       Tool that wipes all data of a computer
ntpass     Edit Windows login passwords even on NTFS disks
disk1      Boot from the first hard disk of the computer
disk2      Boot from the second hard disk of the computer
floppy     Boot from the floppy disk of the computer
boot: _
```

Im unteren Bereich sehen wir sogenannte Disk-Startdateien (z.B. freedos, gag, ranish und eben unser ntpass). Wenn wir beim Starten einen dieser Befehle eingeben, so wird nicht die RescueCD selber, sondern ein Disk-Image (Floppy-Emulator) mit der Utility-Diskette gestartet. In unserem Fall geben wir ein:

```
ntpass
```

Wir erhalten nun Statusmeldungen und am Ende sollten wir den folgenden Screen sehen:

6.3 Festplatte, Registry und Account bearbeiten

```
Player Devices
mkdir: Cannot create directory '/floppy': File exists
Initialization complete!
usb 1-1: new full speed USB device using uhci_hcd and address 2
*****
** Win/NT Registry Edit Utility Floppy / chntpw
** (C) 1997 - 2004 Peter N Hagen - pnh@h13sunet.no
** See file named "license" on floppy for licensing info and credits
**
** This utility will enable you to change or blank the password of
** any user (incl. administrator) on an Windows NT/2K/XP installation
** WITHOUT knowing the old password
** Unlocking locked/disabled accounts also supported.
**
** It also has a registry editor, and there is now support for
** adding and deleting keys and values.
**
** Tested on: NT3.51 & NT4: Workstation Server PDC.
**            Win2k Prof & Server to SP4. Cannot change AD.
**            XP Home & Prof: up to SP2.
**            Win 2003 Server (all?): Seems to work
**
** HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN
*****
=====
There are several steps to go through:
- Disk select, with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
= Step ONE: Select disk where the Windows installation is
=====
Disks:
/dev/ide/host0/bus0/target0/lun0/disc NT partitions found:
1 ..... /dev/ide/host0/bus0/target0/lun0/part1 4000MB Boot
3 ..... /dev/ide/host0/bus0/target0/lun0/part3 4000MB
3 ..... /dev/ide/host0/bus0/target0/lun0/part6 12464MB

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] 3
```

Wählen wir nun die gewünschte Partition, auf der Windows installiert ist. In unserem Falle ist dies 3, weil wir Windows nicht in der ersten Partition installiert haben. Nach einer Weile erfolgt die Abfrage 'What is the path of the registry directory'. Diese Abfragen bestätigen wir ganz einfach mit Enter. Nun können wir mit der 1 den Modus wählen, um Passwörter zurückzusetzen. Dazu der folgende Screen:

```
Player Devices
=====
There are several steps to go through:
- Disk select, with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
= Step ONE: Select disk where the Windows installation is
=====
Disks:
/dev/ide/host0/bus0/target0/lun0/disc NT partitions found:
1 ..... /dev/ide/host0/bus0/target0/lun0/part1 4000MB Boot
3 ..... /dev/ide/host0/bus0/target0/lun0/part3 4000MB
3 ..... /dev/ide/host0/bus0/target0/lun0/part6 12464MB

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] 3
Selected: 3
Mounting on /dev/ide/host0/bus0/target0/lun0/part6
NTFS volume versio 3.1.
Filesystem is: NTFS
=====
= Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config]
-rw-r--r-- 1 0 0 262144 Oct 10 09:07 SAM
-rw-r--r-- 1 0 0 262144 Oct 10 09:07 SECURITY
-rw-r--r-- 1 0 0 262144 Oct 10 09:07 default
-rw-r--r-- 1 0 0 262144 Oct 10 09:07 software
-rw-r--r-- 1 0 0 4096 Oct 10 09:07 system
drwxr-xr-x 1 0 0 262144 Oct 10 09:07 systemprofile
-rw-r--r-- 1 0 0 262144 Oct 10 09:07 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset (sam system security)
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1]
```

Danach wählen wir mit 1 'Edit user data and passwords', um die Liste mit den vorhandenen Benutzern/innen zu erhalten.

```

Player  Devices
-----
* Step THREE: Password or registry edit
=====
chntpw version 0.99.3 041207 (c) Petter N Hagen
hive name (from header): \Systemroot\System32\Config\SAM
ROOT Key at offset 0x001020 * Subkey indexing type is: 886c <lf>
Page at 0x0000 is not 'hbin', assuming file contains garbage at end
File size 252144 [10000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 23018376 blocks/bytes, unused: 771944 blocks/bytes.
Hive's name (from header): SYSTEM
ROOT Key at offset 0x001020 * Subkey indexing type is: 886c <lh>
Page at 0x209000 is not 'hbin', assuming file contains garbage at end
File size 2359296 [240000] bytes, containing 496 pages (+ 1 headerpage)
Used for data: 37740/2195395 blocks/bytes, unused: 763/8712 blocks/bytes.
Hive's name (from header): \emRoot\System32\Config\SECURITY
ROOT Key at offset 0x001020 * Subkey indexing type is: 886c <lf>
File size 252144 [10000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 750/34528 blocks/bytes, unused: 4/2048 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>
  1 - Edit user data and passwords
  3 - RecoveryConsole settings
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====
RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <Hilfessistent>
RID: 03e9, Username: <SUPPORT_389943a0>, *disabled or locked*
RID: 03eb, Username: <up>, *disabled or locked*

Select: ? - quit, - list users, 0x(RID) - User with RID (hex)
or simply enter the username to change: [Administrator] _

```

Jetzt müssen wir jene Zahl eingeben die auf 'RID' folgt, in unserem Falle also:

0x01f4

Wir erhalten nun die nachfolgende Abbildung, d.h. wir werden aufgefordert, das Passwort neu zu vergeben:

```

Player  Devices
-----
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>
  1 - Edit user data and passwords
  3 - RecoveryConsole settings
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====
RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <Hilfessistent>
RID: 03e9, Username: <SUPPORT_389943a0>, *disabled or locked*
RID: 03eb, Username: <up>, *disabled or locked*

Select: ? - quit, - list users, 0x(RID) - User with RID (hex)
or simply enter the username to change: [Administrator] 0x01f4
RID      : 0500 [01f4]
Username: Administrator
fullname:
comment  : Vordeterminiertes Konto für die Verwaltung des Computers bzw. der Domäne
homedir  :
Account bits: 0x0210 =
[ ] Disabled
[ ] Temp. duplicate
[ ] Domain trust ac
[ ] Password expires
[ ] (unknown 0x10)
[ ] Homedir req.
[ ] Normal account
[ ] NKS trust act.
[ ] Auto lockout
[ ] (unknown 0x20)
[ ] Passwd not req.
[ ] NMS account
[ ] Srv trust act
[ ] (unknown 0x02)
[ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *

```

Hinweis: Leider funktioniert das Setzen eines anderen Passwortes bei mir nicht. Ich konnte das Passwort nur löschen, nicht verändern. Dies erreichen wir mit dem Sternchen *. Und damit wir das Sternchen finden, bedarf es bei einer Schweizer Tastatur, die auf Englisch voreingestellt ist, der Kombination Shift+8.

Die nachfolgende Kontrollabfrage 'Do you really want to change it', müssen wir mit 'y' beantworten, auch hier gilt, wir benötigen wegen der englisch voreingestellten Tastatur die z-Taste. Es muss danach changed! erscheinen. Mit ! (findet sich auf Shift+1) gelangen wir zurück und können mit q das Beenden erzwingen.

```

Player  Devices
=====(<) chntpw Main Interactive Menu (<)=====(<)
Loaded Hives: <sam> <system> <security>
  1 - Edit user data and passwords
  00 - Syskey status & change
  - RecoveryConsole settings
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <sam> - OK

=====
= Step FOUR: Writing back changes
=====
About to write file(s) back? Do it? [n] : y
Writing sam
NTFS-fs error (device hda6): ntfs_prepare_nonresident_write(): Writing beyond in
itialized size is not supported yet. Sorry.
NTFS-fs error (device hda6): ntfs_prepare_nonresident_write(): Writing beyond in
itialized size is not supported yet. Sorry.
cpnt: error while writing: Operation not supported
NOTE: A disk fixup will now be done.. it may take some time
Mounting volume... OK
Processing of $MFT and $MFTMirr completed successfully.
NTFS volume version is 3.1.
Setting required flags on partition... OK
Going to empty the journal ($LogFile)... OK
NTFS partition /dev/ide/host0/bus0/target0/lun0/part6 was processed successfully
NOTE: Windows will run a diskcheck (chkdsk) on next boot.
NOTE: this is to ensure disk integrity after the changes
***** EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [n] : ^P

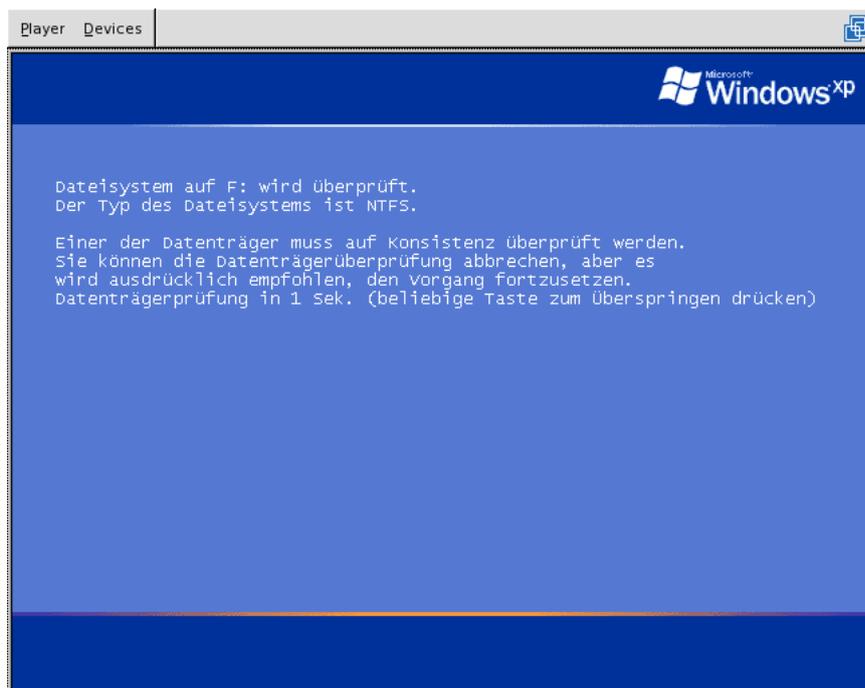
```

6.4 Änderungen definitiv auf Platte schreiben

Nun müssen wir die Änderungen noch definitiv auf die Platte schreiben, dies erreichen wir abermals mit 'y' bzw. der Taste z. Danach anschliessend sollte die Meldung '**** Edit complete ****' erscheinen, ehe wir mit Ctrl+Alt+Del den Neustart erzwingen können.

6.5 Neustart und Festplattenreorganisation

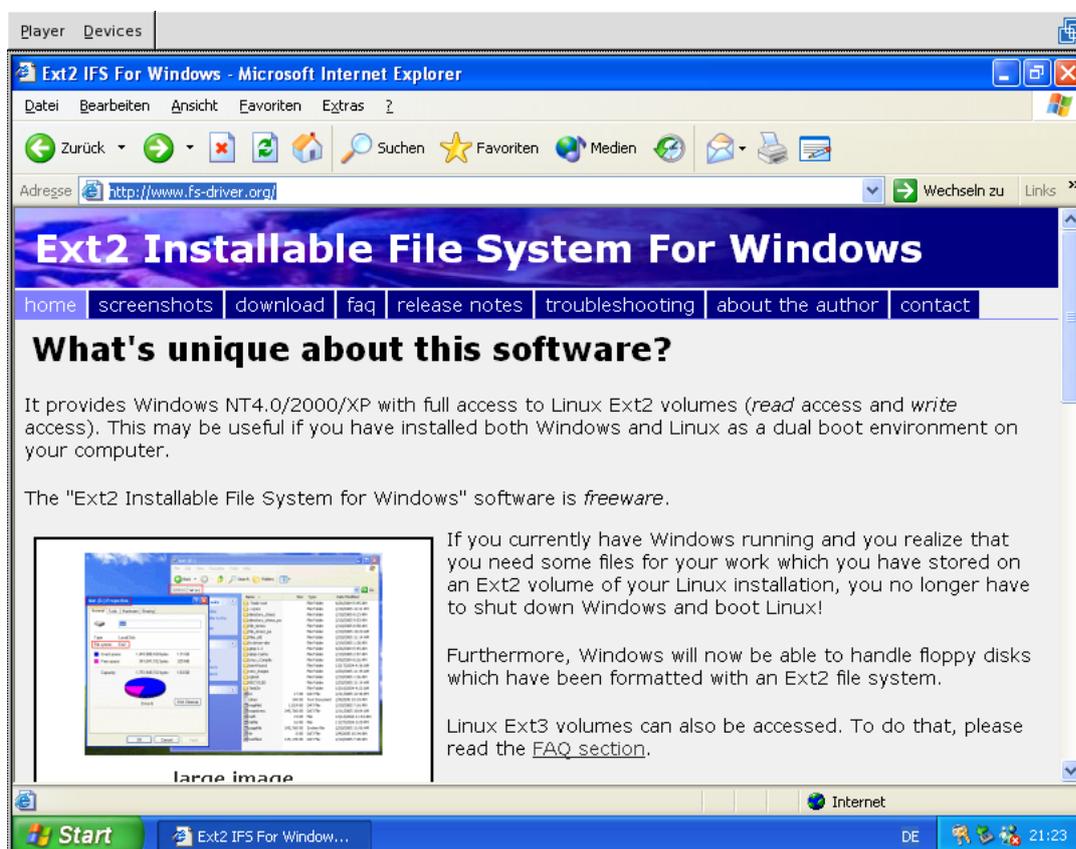
Beim Neustart bitte nicht erschrecken, es erfolgt in jedem Falle eine Meldung, die Festplatte müsse reorganisiert werden.



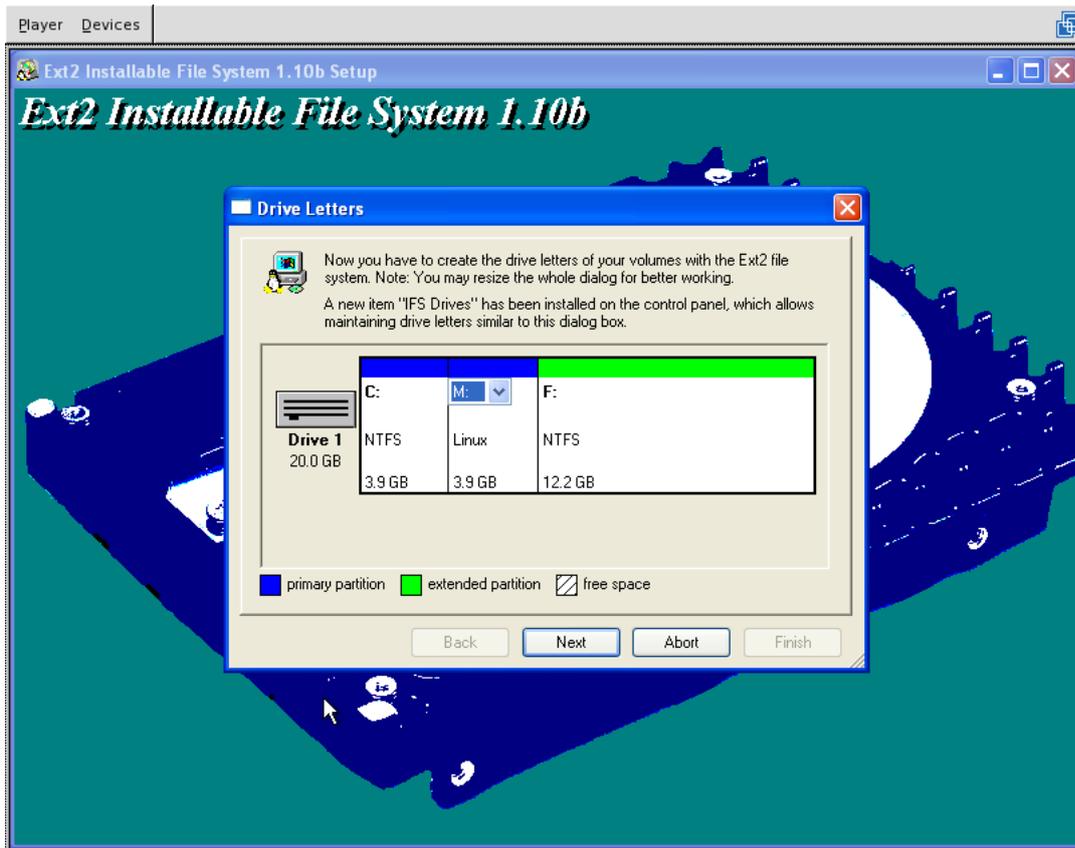
Das ist normal und ändert nichts an der Tatsache, dass wir soeben den Administratoren-Account zurückgesetzt haben.

7 Zugriff von Windows auf Ext3-Dateisysteme

Um auf eine Ext3-Festplatte anzusprechen, können wir das nachfolgende Tool verwenden:



Wir finden die Homepage unter www.fs-driver.org. Die Exe-Datei ist klein (ca. 300 KByte). Nach dem Download starten wir das Programm und nach zwei drei Klicks können wir die gewünschte(n) Laufwerke einem Laufwerksbuchstaben zuordnen.



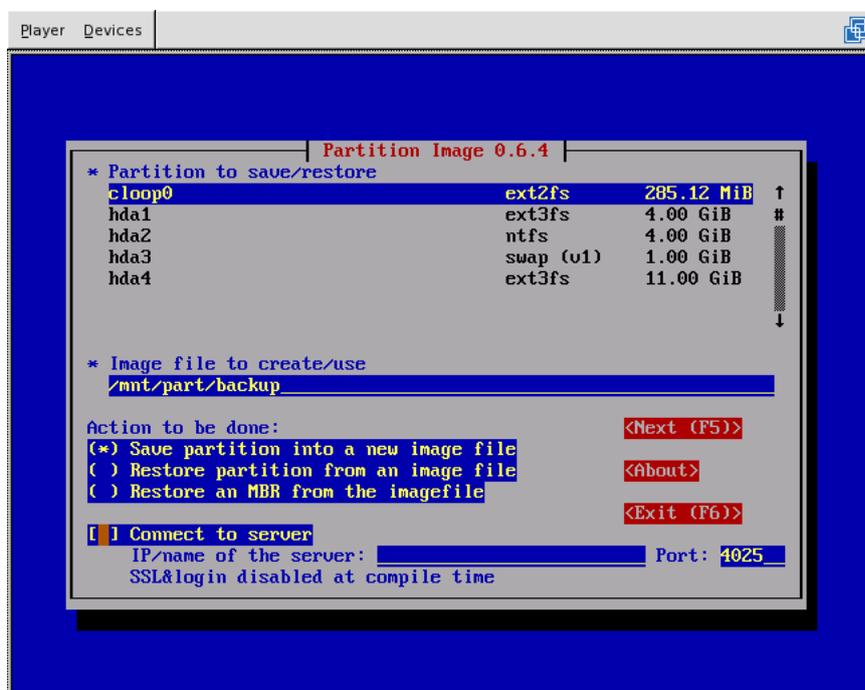
8 PartImage

8.1 Client-Modus

PartImage dient dazu, gesamte Festplatteninhalte (einzelne Partitionen) zu sichern. Zunächst sollten wir nach dem Start einer RescueCD sicherstellen, dass wir eine Partition mit genügend freiem Speicherplatz haben. Dazu mounten wir am besten ein Laufwerk:

```
mount /dev/hda4 /mnt/part
```

Anschliessend geben wir `partimage` ein, und gelangen in die folgende Maske:



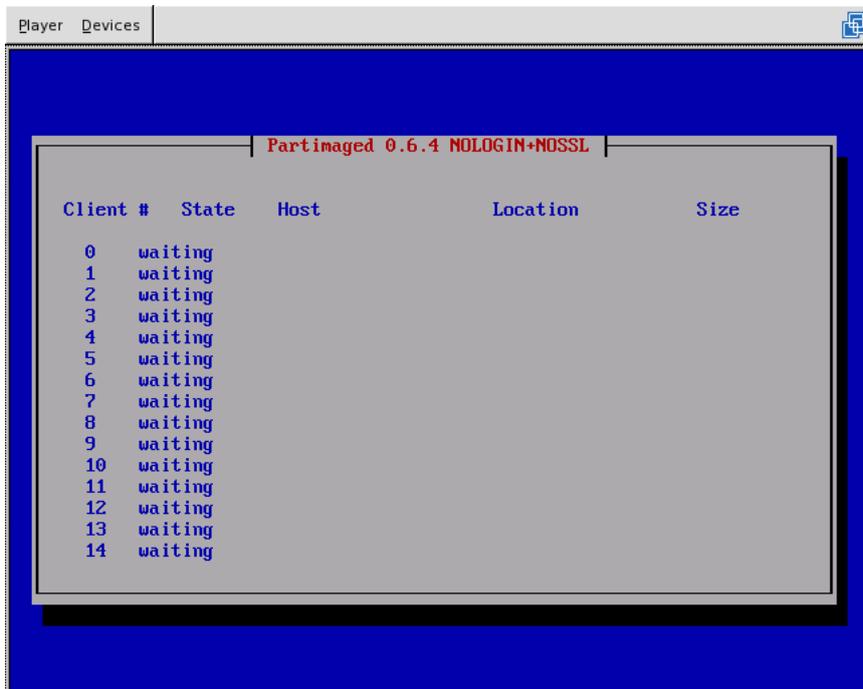
Hier können wir sowohl ein Backup (Sichern) als auch ein Restore (Zurückspielen) einzelner Partitionen durchführen.

Sofern es schnell gehen muss, sollte auf eine Komprimierung verzichtet werden, ansonsten sparen wir mit einer solchen 3:1 an Speicherplatz.

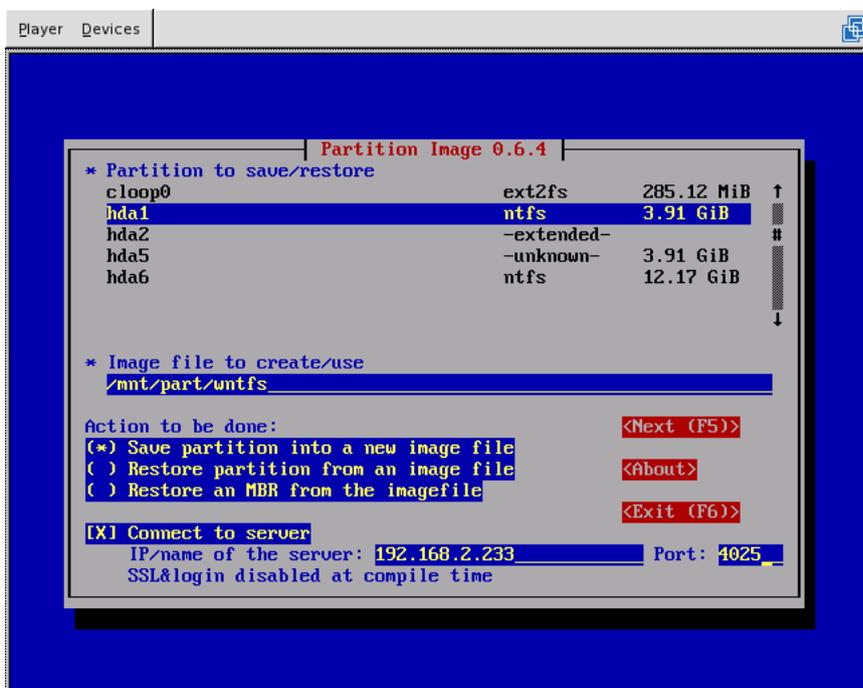
8.2 Server-Modus

Damit wir sämtliche Partitionen aller PCs auf einem Rechner ablegen können, gibt es neben dem normalen `partimage` eine Server-Version mit dem Namen `partimaged`. Damit können wir direkt über das Netzwerk Partitionen bestimmter Rechner sichern. Nach dem Start wartet das Programm ganz einfach auf Client-Zugriffe und sieht daher zunächst unspektakulär aus.

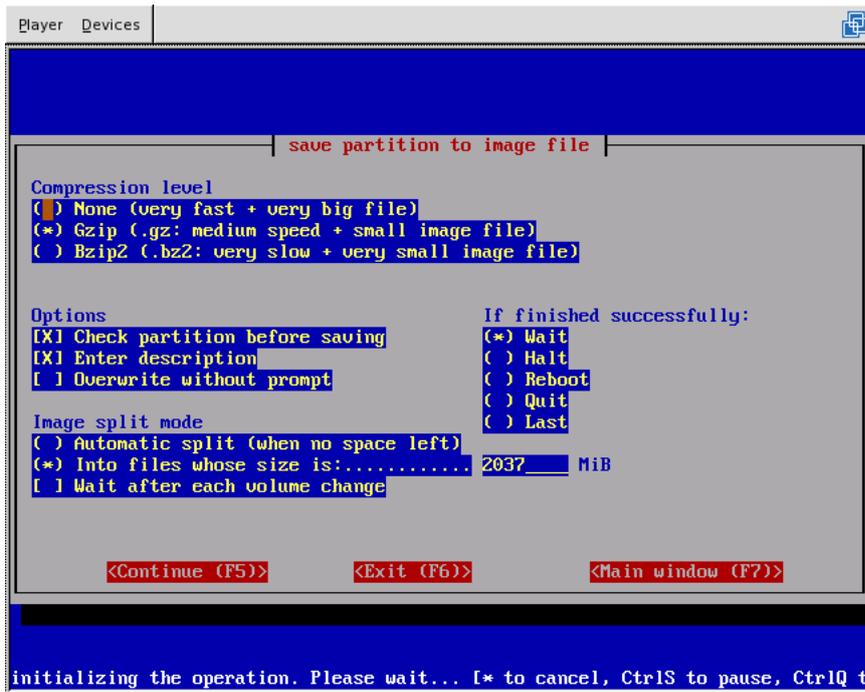
Bevor wir partimaged starten sollten wir daran denken, dass wir mit ipconfig die Netzwerkadresse in Kenntnis bringen und dass wir mit mount /dev/hda4 /mnt/part auch eine Partition zum Schreiben öffnen.



Danach können wir auf der Maschine, auf der wir ein Backup durchführen wollen, ganz normal partimage starten.



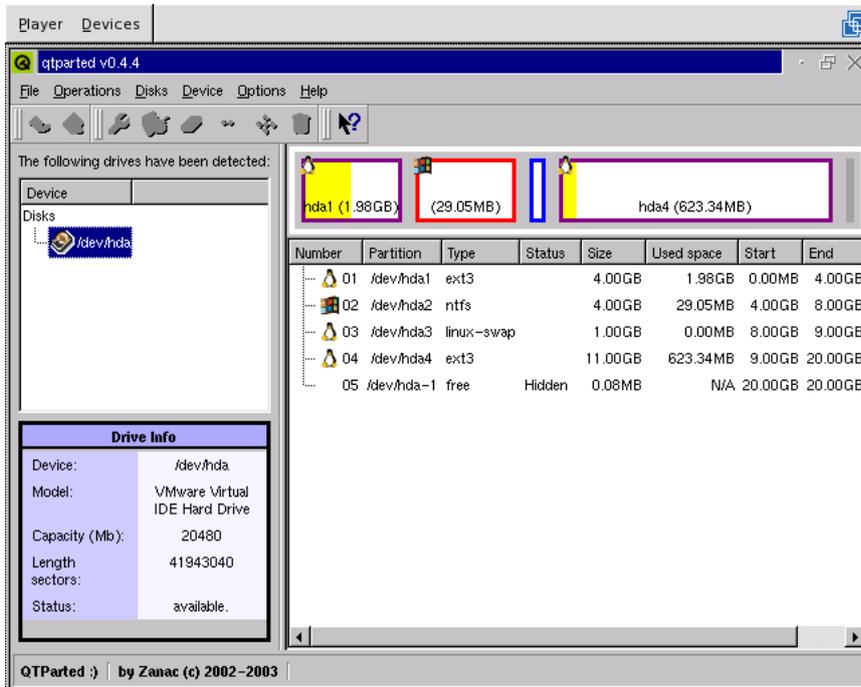
Bei 'Connect to Server' tragen wir nun die IP-Adresse unseres zuvor eingerichteten PartImage-Servers ein. Danach 'F5' drücken.



Wenn wir den obenstehenden Screen erhalten, so ist alles ok, der Rest passiert auf die genau gleiche Art und Weise, wie wenn wir nur mit partimage arbeiten würden.

9 QTParted

Um einzelne Partitionen direkt zu bearbeiten, können wir auf das Programm QTParted zurückgreifen.



Da das Programm in einem Fenstermodus arbeitet, dürfte die Bedienung selber kaum zu Schwierigkeiten führen.

Achtung: QTParted hat bei mir auch schon mal zur Zerstörung einer Partiton geführt. Verwenden wir das Tool daher mit der nötigen Umsicht.

10 Backup mit flexbackup

Für das Backup grösserer Datenmengen (z.B. bis ca. 200 GByte) im Zusammenhang mit Tape-Laufwerken verwenden wir im Rahmen von 'ArchivistaBox' das Perl-Programm 'flexbackup'. Flexbackup ist nicht auf der RescueCD enthalten, es kann aber einfach auf der Homepage www.flexbackup.org bezogen werden. Flexbackup ist im Vergleich zu komplexeren Backupprogrammen (wie z.B. amanda) recht schnell aufgesetzt, es kann aber (mindestens derzeit) keine Tape-Backup-Roboter unterstützen. Innerhalb der ArchivistaBox verwenden wir Flexbackup zusammen mit `afio` und können damit selbst Datenbankdateien sichern, die mehr als 100 GByte gross sind.

Und noch was, keine Bange, die stabile Version datiert vom 12. Oktober 2003; das ist so und es würde mich freuen, wenn das auch in Zukunft so bliebe.



Kontakt: Archivista GmbH, Postfach, CH-8042 Zürich
Tel: +41 (0)1 254 54 00, Fax: +41 (0)1 254 54 02, Web: www.archivista.ch