SystemRecovery mit RescueCD

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

Inhaltsverzeichnis

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

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

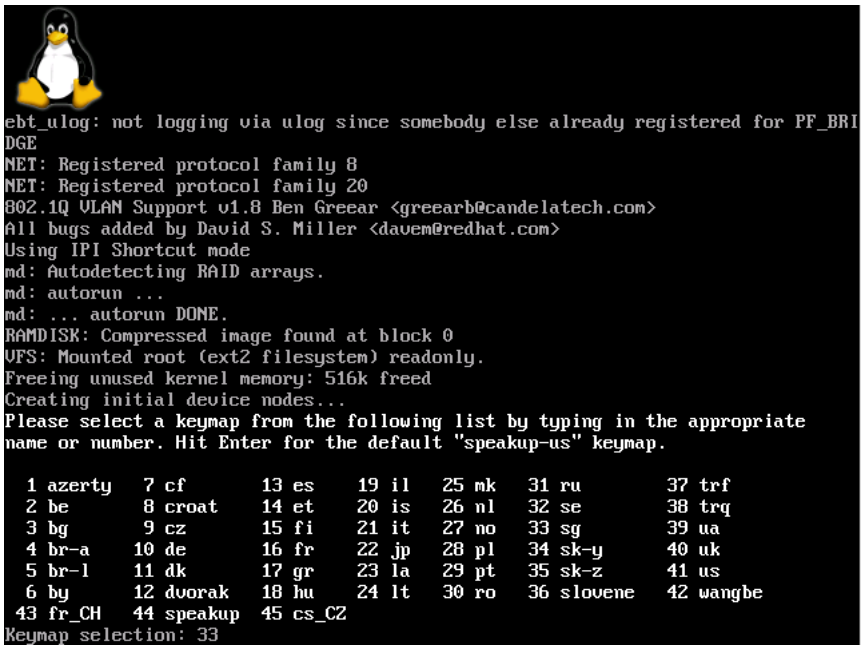
Grundsätzlich arbeitet die RescueCD problemlos mit dem VMWare Player zusammen. Beim Starten muss einfach die ESC-Taste gedrückt werden, damit wir das CD-Rom-Laufwerk als Boot-Laufwerk auswählen können.

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.

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



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

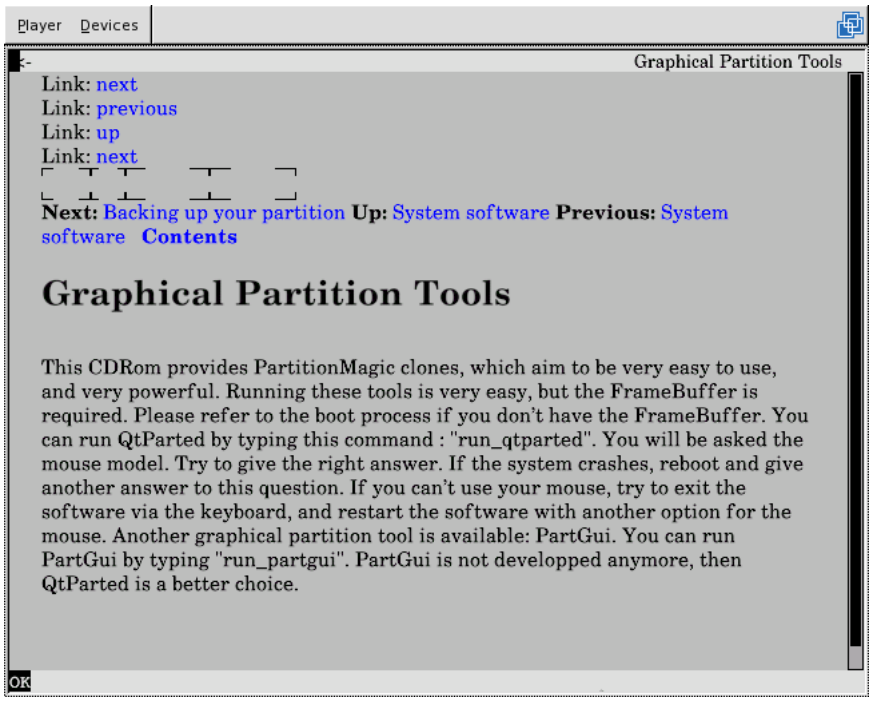
Nach dem Start gelangen wir auf eine Linux-Konsole. Doch keine Bange, wir benötigen nicht wirklich Linux-Kenntnisse, um mit der RescueCD arbeiten zu können.

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
```

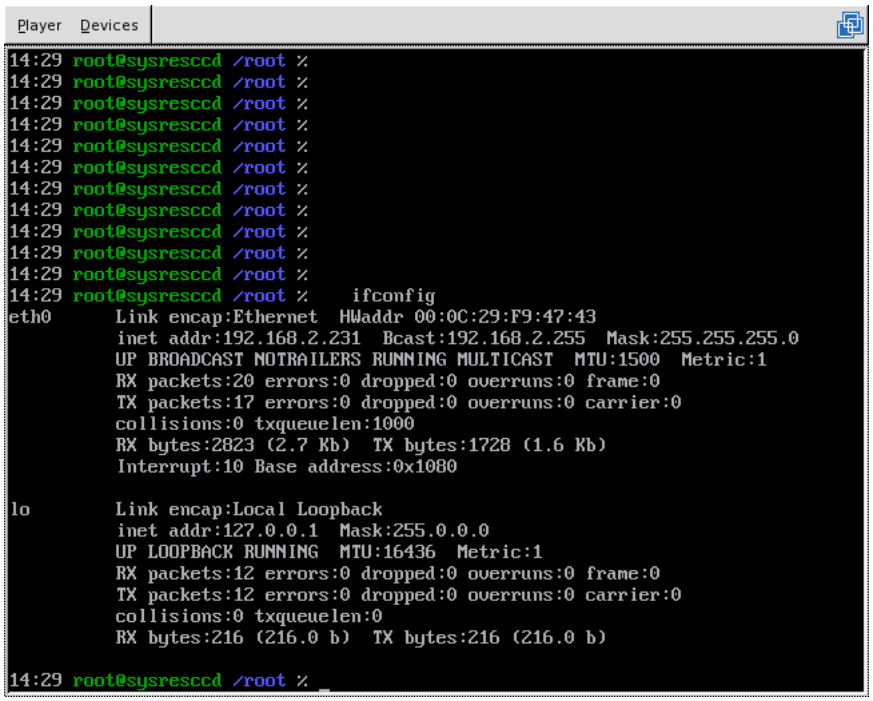
Oh Wunder, da erscheint die Hilfe ja richtig in einem grafischen Browser:



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.



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.

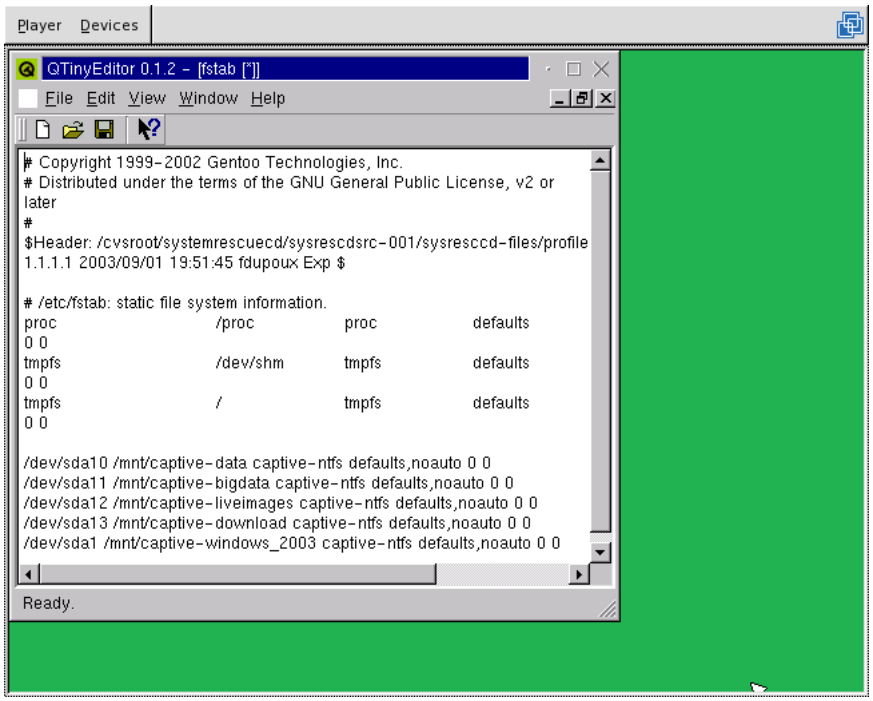
```
passwd
```

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.

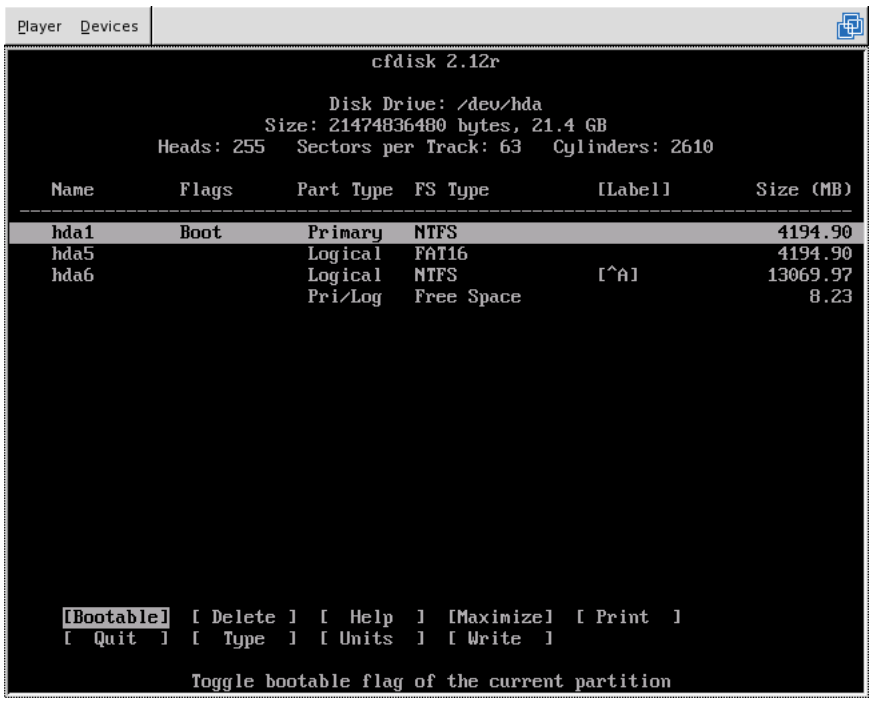
4.5 Dateien editieren

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



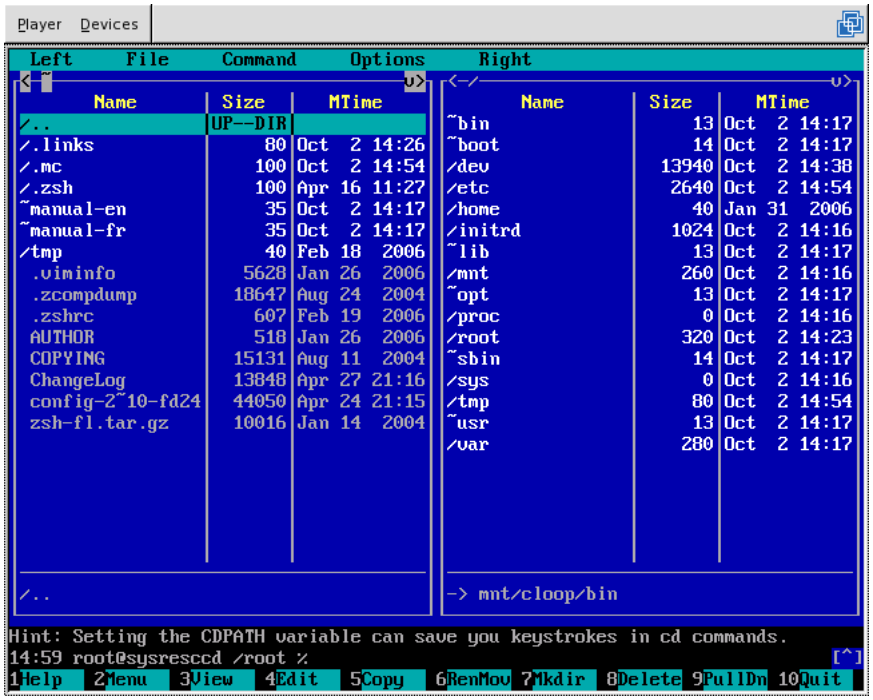
4.6 Partitionen einrichten

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



4.7 Arbeiten mit MidnightCommander

Leider habe ich schon in jungen Jahren den legendären NortonCommander verpasst (die DOS-Shell fand ich damals praktischer[1]). 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`.

[1] Leider 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).

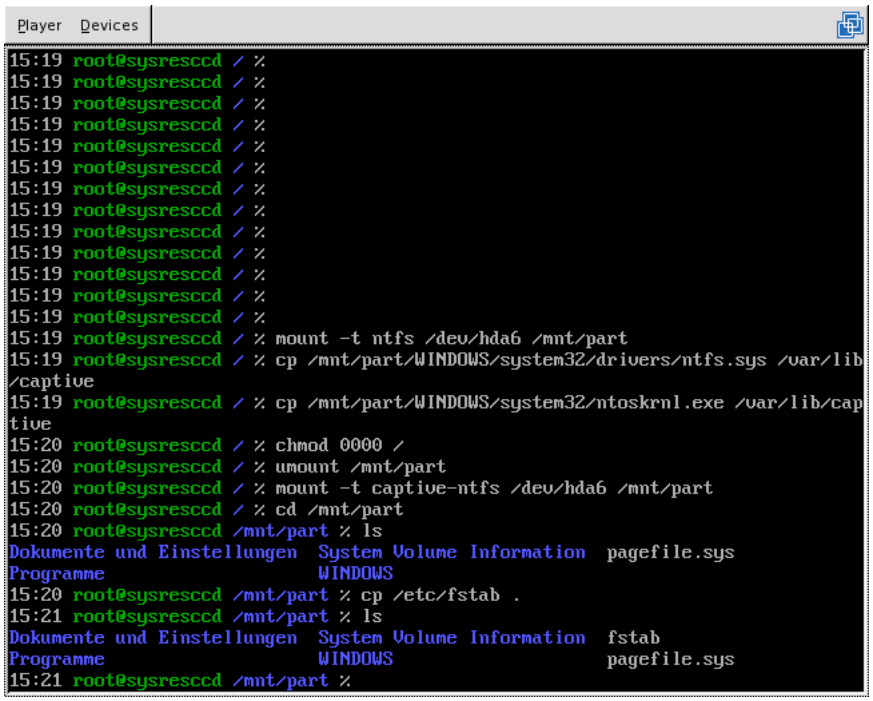
Hinweis: Leider ist die Hilfestellung der RescueCD nicht korrekt, daher beschreibe ich das Vorgehen hier nochmals.

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 / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
15:19 root@sysresccd / %
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

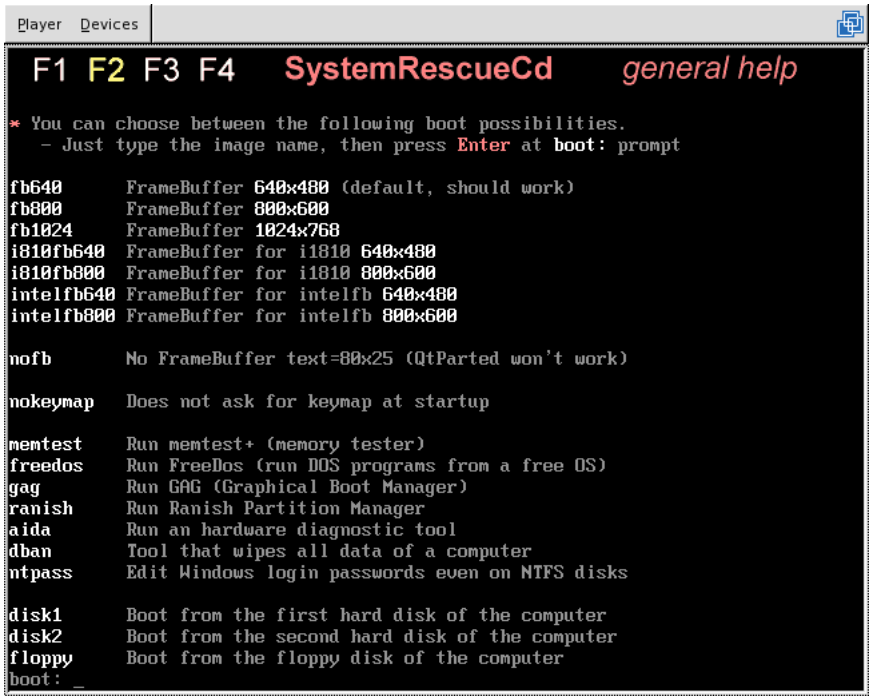
Eine der schönsten Funktionen der RescueCD dürfte sein, dass wir in einem speziellen Modus Passwörter der Benutzer zurücksetzen können, ohne in Windows angemeldet zu sein. Dazu starten wir zunächst einmal die RescueCD neu mit:

```
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:

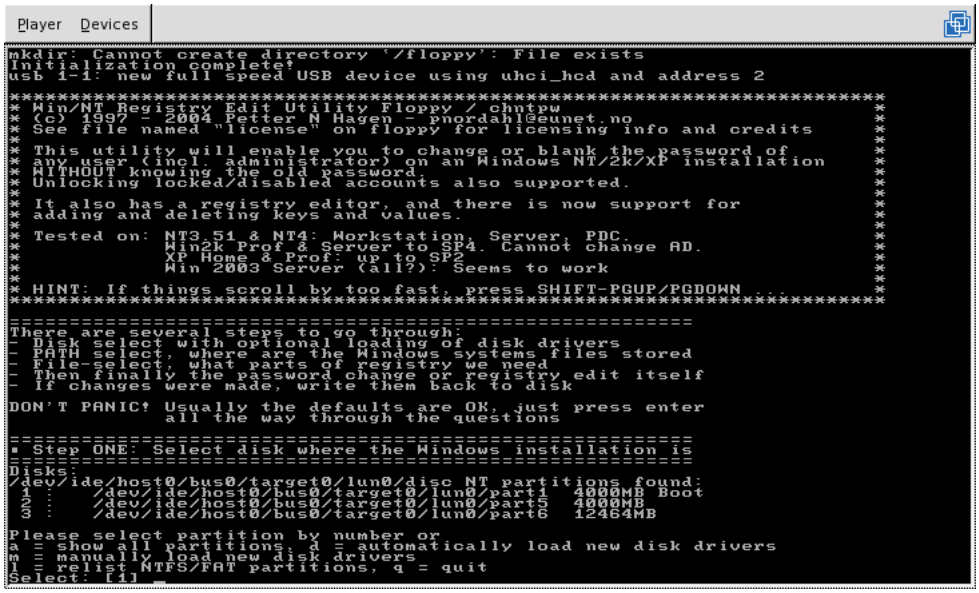


Im unteren Bereich sehen wir sogenannte Disk-Startdateien (z.B. freedos, gag, ranish und eben unser ntpass). Wenn wir beim Starten einen dieser Befehle eingeben, so wird nicht die RescueCD selber, sondern ein Disk-Image (Floppy-Emulator) mit der Utility-Diskette gestartet. In unserem Fall geben wir ein:

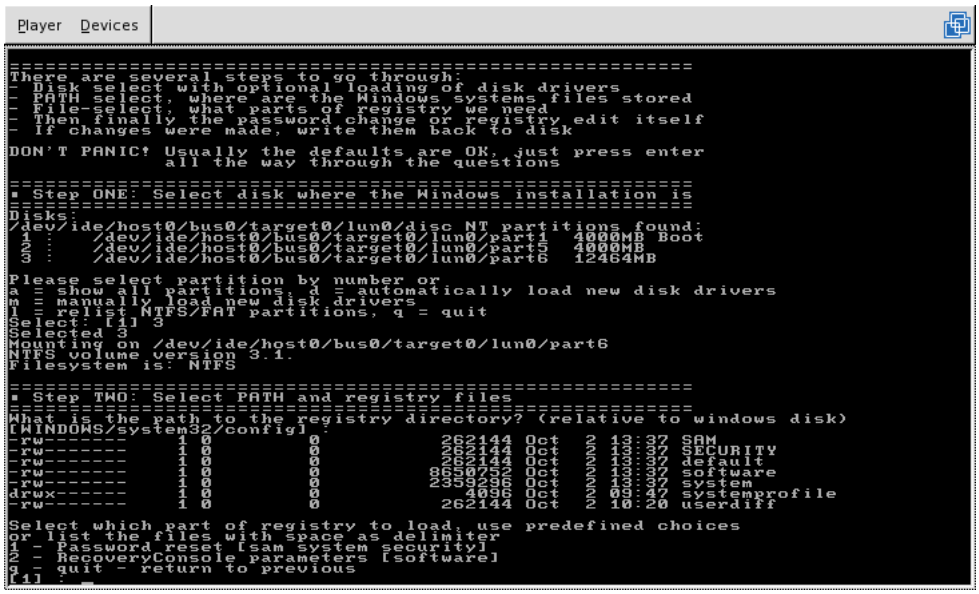
```
ntpass
```

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

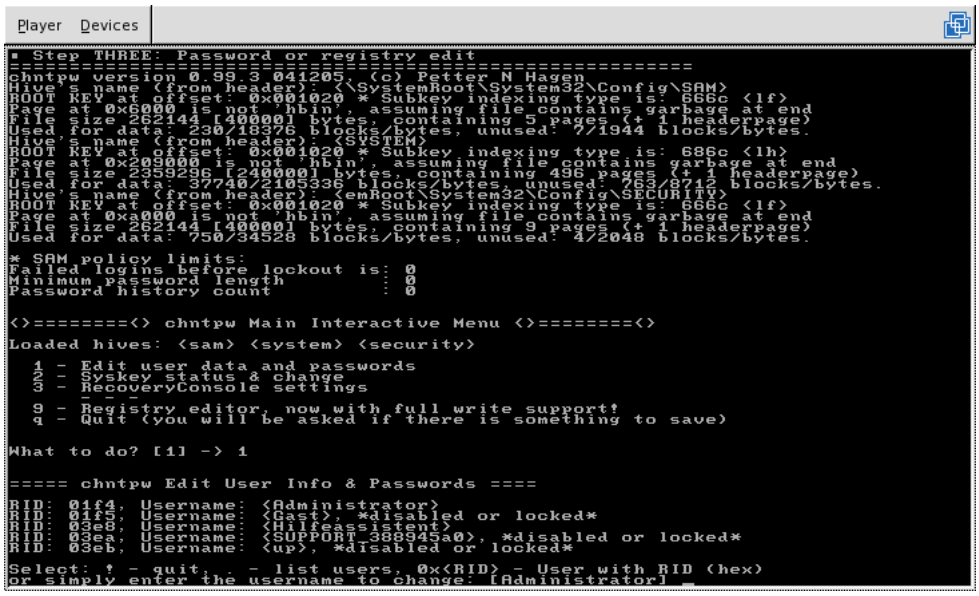
6.3 Festplatte, Registry und Account bearbeiten



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 mir mit der 1 den Modus wählen, um Passwörter zurückzusetzen. Dazu der folgende Screen:



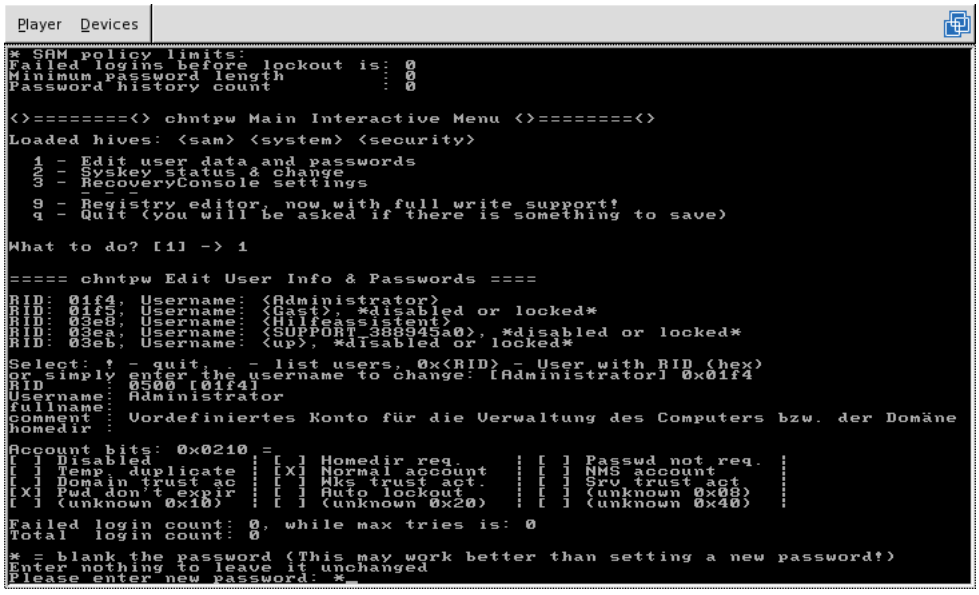
Danach wählen wir mit 1 'Edit user data and passwords', um die Liste mit den vorhandenen Benutzern/innen zu erhalten.



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

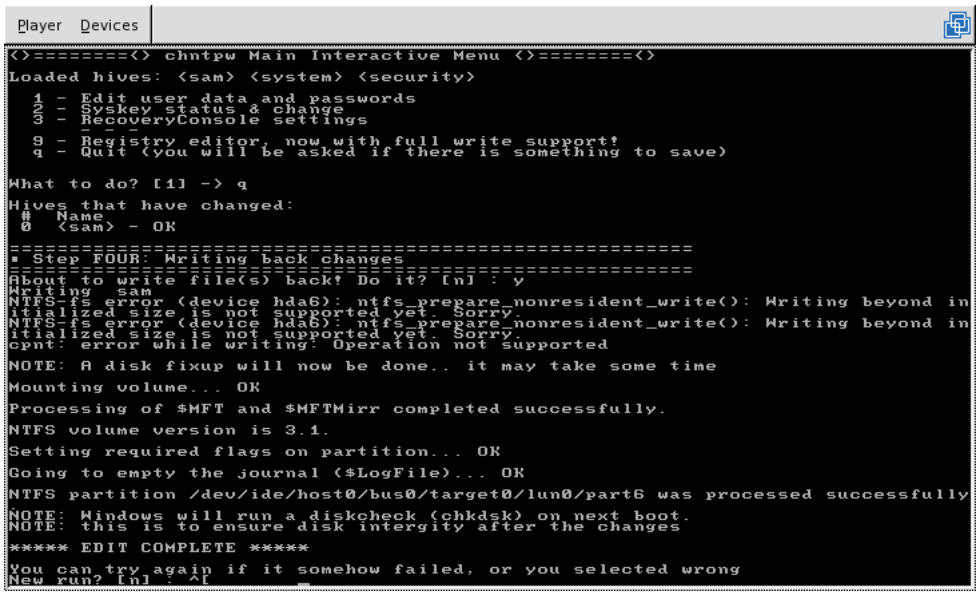
`0x01f4`

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



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 Schwizer 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.

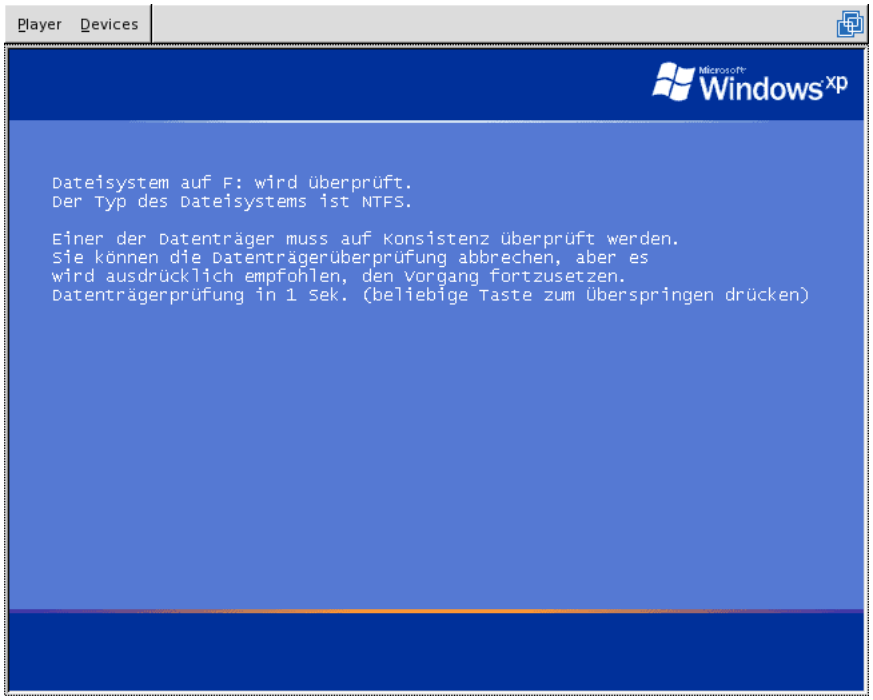


6.4 Änderungen definitiv auf Platte schreiben

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

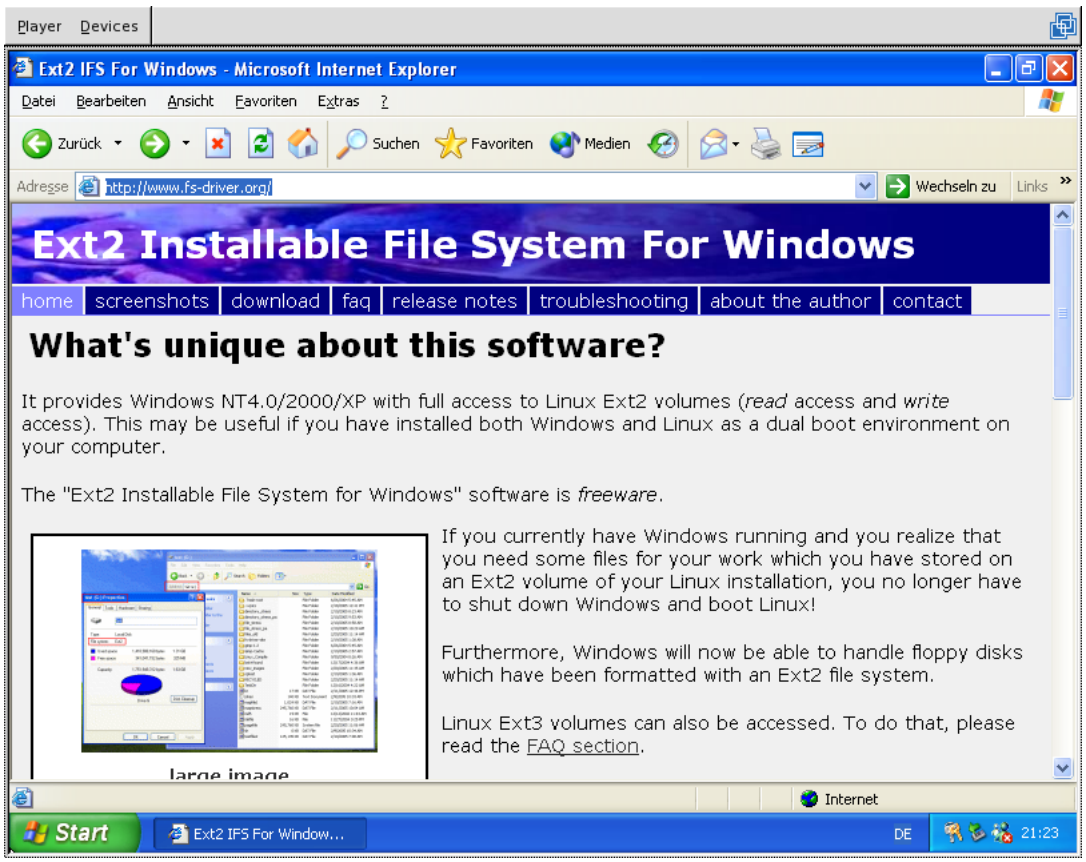
Beim Neustart bitte nicht erschrecken, es erfolgt in jedem Falle eine Meldung, die Festplatte müsse reorganisiert werden.



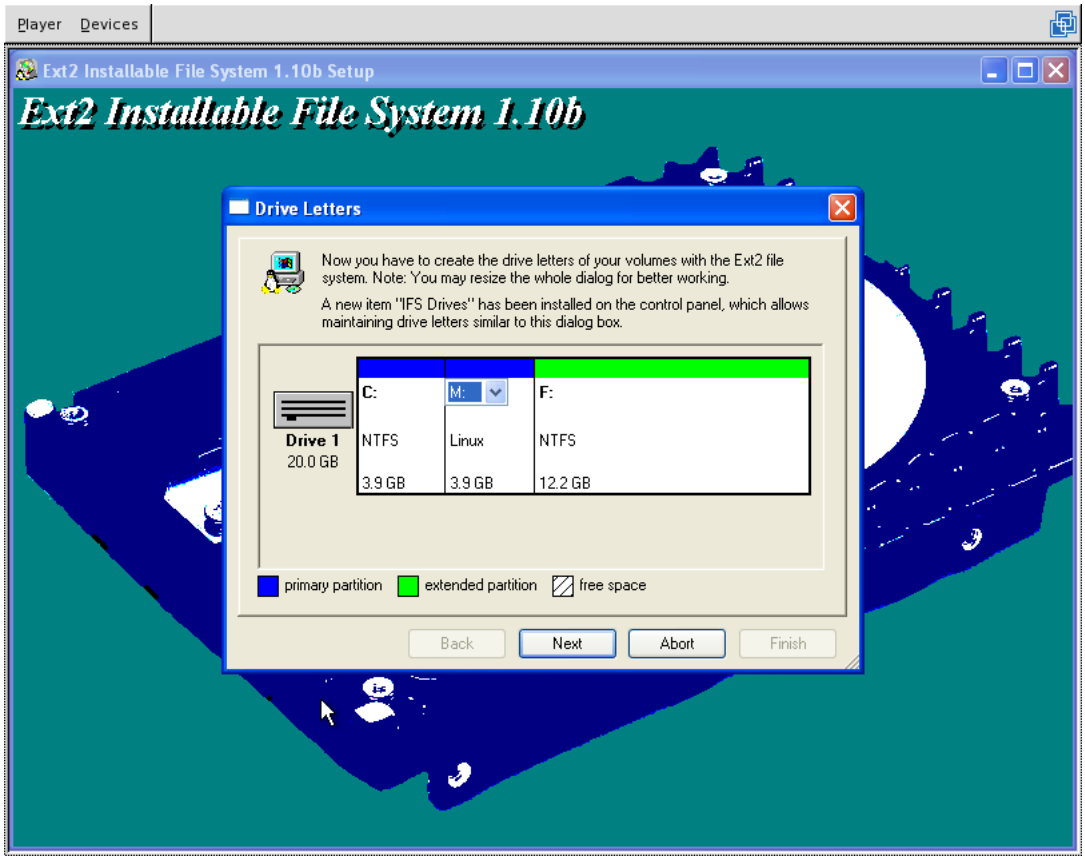
Das ist normal und ändert nichts an der Tatsache, dass wir soeben den Administratoren-Account zurückgesetzt haben.

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.


Player Devices
Ext2 Installable File System 1.10b Setup
Ext2 Installable File System 1.10b
Drive Letters
Now you have to create the drive letters of your volumes with the Ext2 file system. Note: You may resize the whole dialog for better working.
A new item "IFS Drives" has been installed on the control panel, which allows maintaining drive letters similar to this dialog box.
C:
M:
F:
Drive 1
20.0 GB
NTFS
3.9 GB
Linux
3.9 GB
NTFS
12.2 GB
primary partition
extended partition
free space
Back
Next
Abort
Finish

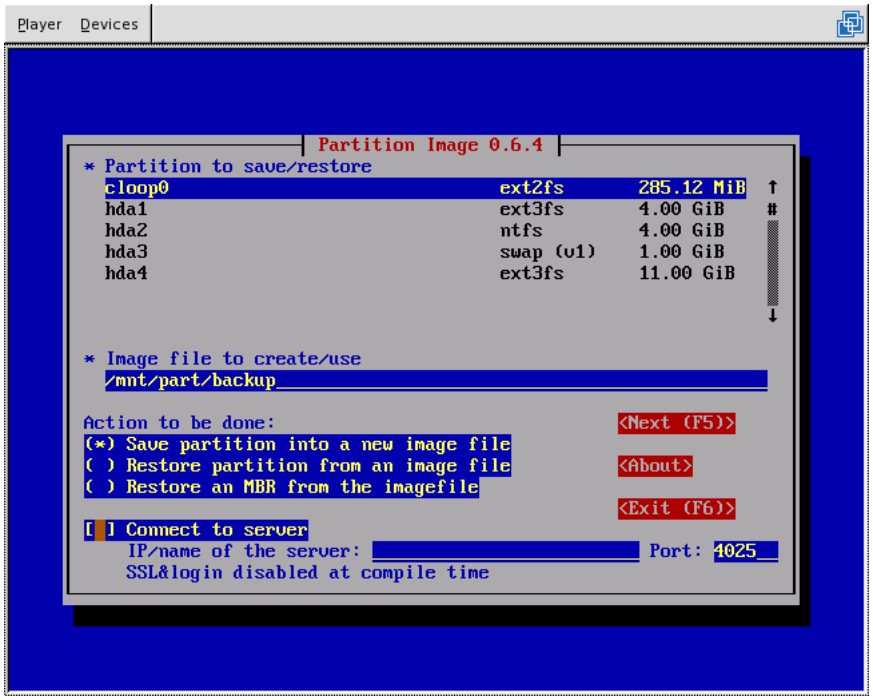
8 PartImage

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:



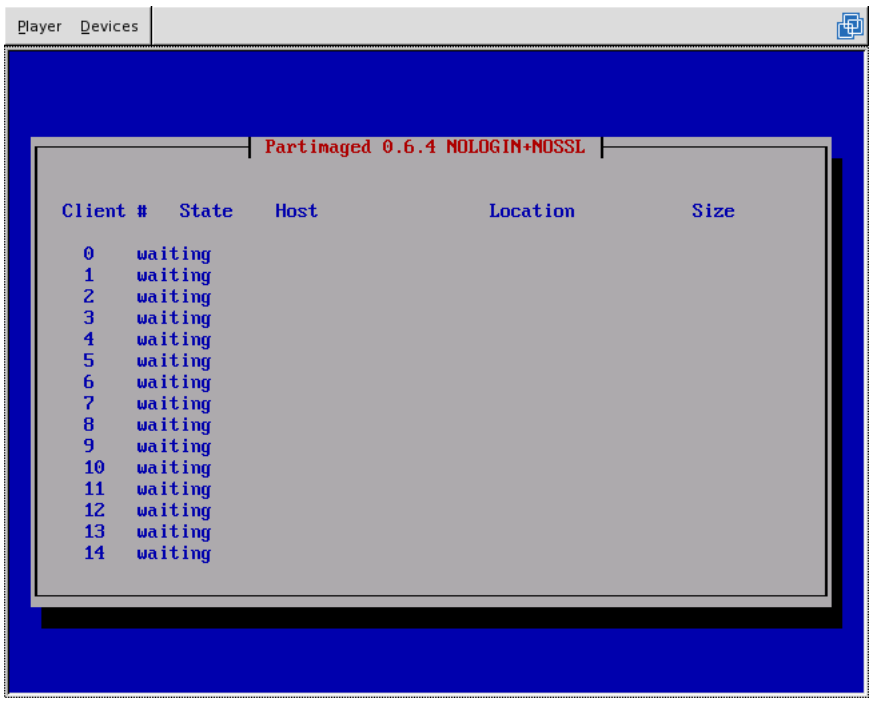
Hier können wir sowohl ein Backup (Sichern) als auch ein Restore (Zurückspielen) einzelner Partitionen durchführen.

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

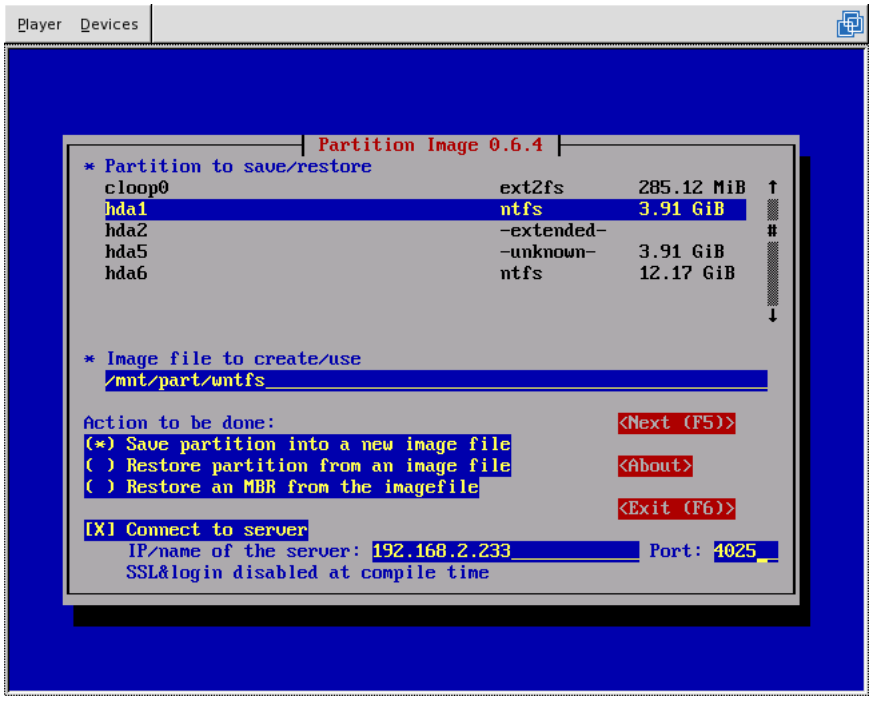
8.2 Server-Modus

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.

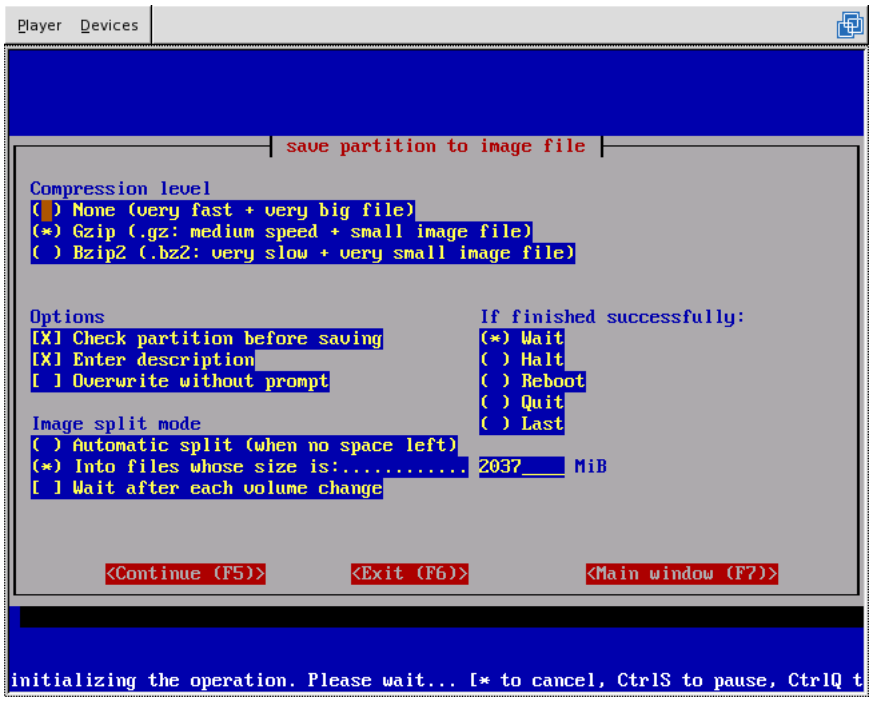
Bevor wir `partimaged` starten sollten wir daran denken, dass wir mit `ipconfig` die Netzwerkadresse in Kenntnis bringen und dass wir mit `mount /dev/hda4 /mnt/part` auch eine Partition zum Schreiben öffnen.



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



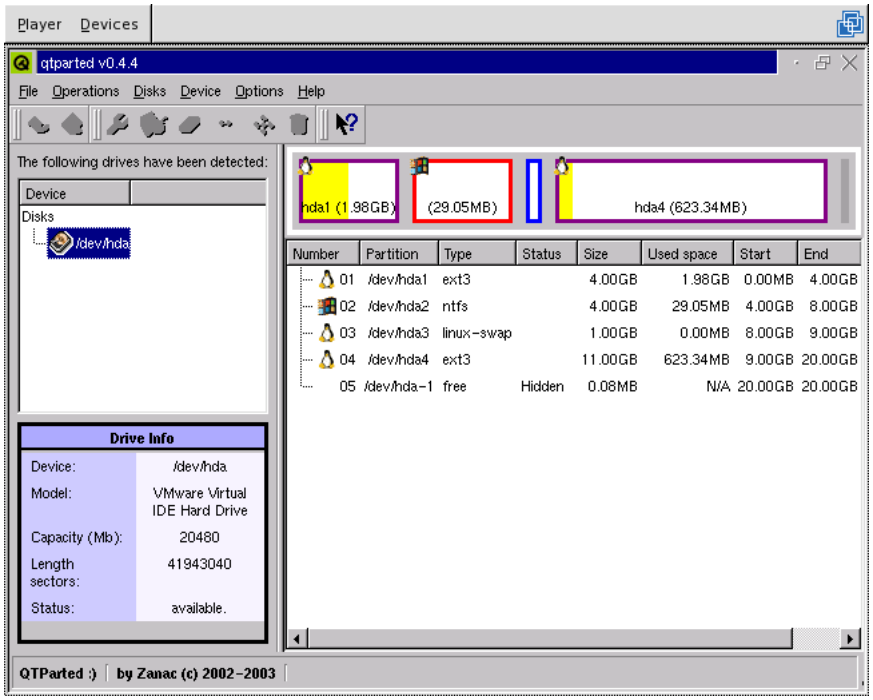
Bei 'Connect to Server' tragen wir nun die IP-Adresse unseres zuvor eingerichteten PartImage-Servers ein. Danach 'F5' drücken.



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 unterstützten. 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