

System Rescue CDRom manual
<http://www.sysresccd.org/>

Francois DUPOUX

Gregory NOWAK
partimage@romuald.net.eu.org

Franck LADURELLE
ladurelf@partimage.org

This document is available under the FDL license Version 1.2
(GNU Free Documentation License)

April 28, 2006

Contents

1	Overview	4
1.1	Description	4
1.2	Contents	5
1.3	website	6
2	Downloading and burning	7
2.1	Downloading	7
2.2	Burning	7
3	Booting the CDRom	8
3.1	Enable the option	8
3.2	Choosing options	8
3.3	Booting from the CDRom	10
3.4	Booting without a CDRom drive	10
3.5	Booting with an old computer	11
3.6	Booting with Loadlin from Dos/Win95/Win98	11
3.7	Booting from Windows NT/XP	11
4	Starting to use the system	12
5	Network	13
5.1	Setting up the network	13
5.2	Running an SSH Server	13
5.3	Access a Windows computer with Samba	14
5.4	Mount remote FTP/SSH shares as local file systems	14
5.5	Using an ADSL USB modem	15
6	System software	16
6.1	Graphical Partition Tools	16
6.2	Backing up your partition table	16
6.3	Backing up the contents of a partition	17

6.4	DAR (Disk Archiver)	17
6.5	Clam AntiVirus	18
7	Secure Deletion of Data	20
7.1	Introduction	20
7.2	Tools	21
7.3	Other Tools	22
7.4	Testing	23
8	How to personalize SystemRescueCd	24
8.1	Introduction	24
8.2	Usage	25
8.3	procedure	25
8.4	Result of your changes	28
8.5	Autorun: scripts to be run at startup	28
8.5.1	Summary of rules	29
8.5.2	Examples of autorun scripts	30
9	How to burn a DVD with SystemRescue and 4 GB more files	32
9.1	Introduction	32
9.2	Requirements	32
9.3	First step: burn the official SysResCd ISO image	33
9.4	Second step: add your own files	33
10	How to install SystemRescueCd on harddisk	34
10.1	Introduction	34
10.2	Usage	34
10.3	procedure	34
10.4	Changes as boot time	36
11	Easy install SystemRescueCd on harddisk	37
11.1	Introduction	37
11.2	Requirements	37
11.3	First step: copy important files	38
11.4	Second step: update the bootmanager	38
12	How to install SystemRescueCd on an USB-stick	40
12.1	Introduction	40
12.2	Installation from Linux	40
12.3	Installation from Windows	42
12.4	Bootng from the USB stick	43

13 Mounting an NTFS partition with full Read-Write support	44
13.1 Introduction	44
13.2 Getting the Windows drivers	45
13.3 Mounting NTFS with full support	46
13.4 Remarks	46
14 System boot floppy disks	47
14.1 Introduction	47
14.2 Overview of the boot floppy disks	47

Chapter 1

Overview

1.1 Description

SystemRescueCd is a linux system available on a bootable cdrom in order to repair your system and your data after a crash. It also aims to provide an easy way to do admin tasks on your computer, such as creating and editing the partitions of the hard disk. It contains a lot of system utilities (parted, partimage, fstools, ...) and basic ones (editors, midnight commander, network tools). It aims to be very easy to use: just boot from the cdrom, and you can do everything. The kernel of the system supports most important file systems (ext2/ext3, reiserfs, reiser4, xfs, jfs, vfat, ntfs, iso9660), and network ones (samba and nfs).

You can use SystemRescueCd for many tasks:

- The first time you use the computer, when no operating system is installed. The first task is creating partitions on the hard disk, and installing the operating system. With this CDROM, you can make partitions easily with graphical partition tools (QtParted and PartGui), and you can install Gentoo Linux.
- After a crash, or a mistake, you may have problems booting. For example, after installing Windows, your bootloader (LILO, Grub) may have been erased from the MBR. With this CDROM, you have all you need for reinstalling Grub or Lilo.
- For windows users that don't have Linux installed, it provides a tiny Linux System with most important system tools. For example, Win-

dows users can backup their system partition using Partimage. They need Linux to run partimage.

1.2 Contents

Here is a short list that describes what you will find on this CDROM:

- A recent linux kernel, that supports most important file systems, and the most important hardware. Supported file systems: Ext2/Ext3, ReiserFs, Reiser4, Fat16/Fat32, XFS, JFS, NTFS, ... The kernel supports NFS and Samba.
- Graphical partition tools, that aim to be free partitionmagic clones for Linux. You can use QtParted and PartGui.
- Most important console system tools for Linux. Of course, you have GNU Parted (partition editor), Partimage (drive image clone) for backing up partitions to an image file, File system tools (e2fsprogs for ext2/ext3, Reiserfsprogs for ReiserFS, xfsprogs for XFS, jfsutils for JFS, dosfstools for FAT, NtfsProgs for NTFS). You can use dump/restore for backing up an ext2/ext3 partition.
- Clam-AntiVirus. This is a free AntiVirus software.
- Usual tools for Linux users: tar/gzip/bzip2 for archiving files. The same tools for Windows users: zip/unzip, rar/unrar are provided. This means that you are able to backup/restore your windows data. We have added DAR (Disk Archiver). This is a program like tar, but more powerful.
- Midnight-Commander (type "mc" on the console command line) is a free nortoncommander clone for linux. With mc, it's easy to browse, copy, move, edit all files on your computer. If you don't know all the linux shell commands well, you can start with mc.
- You can use lynx or links. Both are lightweight web browsers. Under FrameBuffer mode, you can pass parameters to the commande line of the links program. It will allow you to enable the graphical mode. It would show images, and you gets a nice interface.

- Of course, editors are important when you have problems. Nano (easy editor) and vim (vi improved) are provided for the text mode. A very basic graphical editor is available for newbies. You can run this editor with "run_qtineditor". It runs with Qt-embedded.

1.3 website

Please, visit the official homepage when you have problems.

- You should read the FAQ (Frequently Asked Questions) before sending questions to the author
- Post ideas, contributions, problems in the forum:
<http://www.sysresccd.org/forums/>
- If you encounter a bug (crash, or another kind of error) that is really related to this CDROM, please, post a detailed message in our forums. Don't submit bug reports that are related to software provided by SystemRescueCd, such as Partimage, ... Only bug reports related to this CDROM are valid (missing module in the kernel, a boot script that crashes, ...)
- Please, download the latest version available before submitting bugs or ideas. Your request may have been already processed.

Chapter 2

Downloading and burning

2.1 Downloading

SystemRescueCd is provided as an ISO image file. This ISO has to be burned and will produce a bootable CDROM. It means SystemRescueCd is not software that can be installed over an existing operating system.

You can download the ISO image file with your favorite browser. Sometimes, the file is shown in the navigator's main window instead of being downloaded. If you have problems, please, download the file with wget. Wget is often installed by default under Linux, and a Windows version is available (search for wget.exe with google). Downloading with wget is easy: just type "wget <address-of-the-iso-file>".

Once the file is downloaded, you can check that there was no error, with md5sum. Run md5sum on the iso file, and compare with the MD5 number that is given on the website. If this is the same number, the file has no errors.

2.2 Burning

You can burn the ISO image file with most burning software. Under Windows, Nero does this very well. Under Linux, you can use cdrecord. For example: "cdrecord dev=0,0,0 speed=8 -v sysresccd-x.y.z.iso" You can find your device identifier by typing "cdrecord -scanbus".

Chapter 3

Booting the CDRom

3.1 Enable the option

In order to allow this CDRom to boot, you have to check that your BIOS is configured properly. In the boot order priorities, the CDRom drive must be shown before your hard disk.

3.2 Choosing options

To use SystemRescueCd, just insert the disc in the CDRom drive, and power on your computer. The logo screen should be displayed. You can start by pressing Enter, but you may choose other options.

If you want to choose the way the CDRom will boot, you have to enter this at the prompt: "`<image> <kernel-parameters>`". For example "`fb1204 nokeymap cdcache`" will let you boot in the FrameBuffer, with no questions about the keymap, and the CDRom will be fully loaded into memory. Look at the possible choices below:

First, you will have to choose the image file to start. If you want to be able to run graphical programs such as QtParted and PartGui, you will have to enable the FrameBuffer. Most video cards supports VESA. With these cards, you can choose `fb640`, `fb800`, `fb1024`, ... If your computer has an intel video chipset, you will have to choice either `i810fb` (for intel chipsets 810 et 815) or `intelfb` (for intel chipsets 830M, 810E845G, 852GM, 855GM, 865G, 915G). If none of these three drivers works, you won't be able to run grphical programs.

Here are the possible choices:

- fb640 (FrameBuffer 640x480 for VESA) is the default boot image. It's recommended if your screen can't display 800x600 images. FrameBuffer allows you to have graphical tools without XFree86. You need the FrameBuffer if you want to use QtParted and PartGui. Low resolutions are required on several intel chipsets and dell computers in order to have FrameBuffer working
- fb800 (FrameBuffer 800x600 for VESA) It's recommended if working, and not able to display 1024x768 images. FrameBuffer allows you to have graphical tools without XFree86. You need the FrameBuffer if you want to use QtParted and PartGui.
- fb1024 (FrameBuffer 1024x768 for VESA). This is the best choice if your screen is able to display images at this resolution.
- i810fb640 (FrameBuffer 640x480 for i810/i815). The most basic resolution for intel chipsets 810 and 815.
- i810fb800 (FrameBuffer 800x600 for i810/i815). A better resolution for intel chipsets 810 and 815.
- intel_fb640 (FrameBuffer 640x480 for new intel chipsets). The most basic resolution for intel chipsets 830M, 810E845G, 852GM, 855GM, 865G, 915G.
- intel_fb800 (FrameBuffer 800x600 for new intel chipsets). A better resolution for intel chipsets 830M, 810E845G, 852GM, 855GM, 865G, 915G.
- nofb (Pas de FrameBuffer). You should use this image if your hardware does not support FrameBuffer.

Now, you can give kernel parameters. There are a lot of parameters you can use. Here are the important ones:

- nokeymap: at startup, you will be asked for the keymap. It will let you choose the keyboard configuration. For example, if you have an azerty keyboard, it will configure it for you, instead of leaving you with a qwerty configuration.

- `cdcache`: this option is very useful if you need to insert another disc in the CDRom drive after booting. The CDRom will be fully loaded into memory, and you will be able to unmount it (with the command `"umount /mnt/cdrom"`), and then you can remove the disc from the drive.
- `root`: this option lets you boot an existing linux system. For example, if you have linux gentoo installed on `/dev/hda6`, you can type `"root=/dev/hda6"` and Gentoo Linux will be started instead of the system that is on the CDRom.
- `nonet`: this will disable the network autodetection at startup
- `usbstick`: use this option if you try to boot from an USB stick where SysRescCd is installed.

3.3 Booting from the CDRom

Once you have pressed "Enter" at the prompt, the system will begin to load. First, if you didn't disable this option, the map for your keyboard will be loaded. You just have to choose the best one for you. Next, the kernel will continue to load, and there will be many boot scripts that are run. The hardware configuration will be autodetected. For example, all kernel modules required for an USB mouse will be loaded automatically. And you will get a shell prompt. You have several linux consoles available. You can change between them by pressing `Alt+F1` for the first one, `Alt+F2` for the second, ...

3.4 Booting without a CDRom drive

If your computer doesn't have a CDRom drive, it may be possible to boot from the network, if another computer on the network has a CDRom drive. You will use the PXE protocol. More help is available at this homepage: `"http://syslinux.zytor.com/pxe.php"`.

3.5 Booting with an old computer

Many old computers cannot boot CDROM. The problem may come from the Bios, from the CD-drive, ... If you have such a problem, you can try to create a boot floppy, that allow to to start the system on the CDROM. Smart BootManager can do such a boot floppy for you. If you have no floppy, you can install this bootloader on the hard disk too. Using this boot manager is easy. You must download sbminst, and run the installer from Linux. Here is the most common install process: `./sbminst -t us -d /dev/fd0`

3.6 Booting with Loadlin from Dos/Win95/Win98

If you cannot boot SystemRescueCd from the CDROM drive, you can use loadlin. This program let you boot a linux system from Dos/Win9x. It's not possible to use loadlin from Windows NT/XP. If you are using win9x, you have to exit the graphical user interface. The best way is pressing F8 during the boot process of Windows, and going to the command line mode.

- Step-1: Create a new directory: `c:/srcd`
- Step-2: Copy all files from the loadlin and isolinux directories (especially `vmlinuz1`, `initrd1`, `loadlin.exe`) to `c:/srcd`
- Step-3: Copy `sysrcd.dat` to `c:/`
- Step-4: Go in the new directory: `"cd c:/srcd"`
- Step-5: Run the following command:

```
loadlin vmlinuz1 initrd=initrd1 acpi=off root=/dev/ram0 init=/linuxrcdos
```

3.7 Booting from Windows NT/XP

It's possible to use SystemRescueCd from Windows NT/XP with a complete computer emulator, such as VMWare and Virtual PC. You have to declare the ISO image as the virtual CDROM drive. In the virtual BIOS, you must ask the computer to boot on the CDROM. It's even possible to use the network. The virtual machine will have a new IP address.

Chapter 4

Starting to use the system

When you start, you should read the message that give you the most important informations about how to use this system. Here is a copy of this text:

You can login on another consoles. The root password is empty. Type "dhcpcd eth0" (or similar) to auto-configure eth0. Type "net-setup eth0" to specify eth0 IP address settings by hand.

To start an ssh server on this system, type "/etc/init.d/sshd start". If you need to log in remotely as root, type "passwd root" to reset root's password to a known value.

You can run graphical partition tools. First, it's recommended to check the modules for your mouse are loaded, with "lsmod". Then, you can use these commands: run_qtparted and run_partgui. Editors available: vim, nano and run_qtineditor

Be careful: this is beta software, and it can be dangerous. And if the mouse fails, try to use the keyboard. The graphical tools won't work if you started without the FrameBuffer option. (F2 at startup for more details)

Note: Never mount anything on /mnt ! It would freeze the system. Use "mkdir /mnt/mydir" and mount on /mnt/mydir instead.

Chapter 5

Network

With the System Rescue CDRom, you will be able to use the network. Here are the main important information about the network.

5.1 Setting up the network

If you have standard hardware, your network card will be autodetected, and the driver loaded. It will even have an IP address. Type `"ifconfig -a"` in order to see your hardware configuration. If you want to give a static IP address, just type `"ifconfig eth0 192.168.10.1"`. Once your IP address is set, you should make sure the default route is configured properly. For example, if your computer has a network card (address 192.168.10.1) that is connected to a gateway (192.168.10.2) which shares its internet connection, you can type this: `"route add default gw 192.168.10.2"`.

5.2 Running an SSH Server

SSH allows you to use a shell on another computer (as telnet does), and you can copy files (with scp). If you want to run an SSH server, you have to change the root password. Just type `"passwd"` and give a valid password. Then, run the server: `"/etc/init.d/sshd start"`. You can stop it with `"/etc/init.d/sshd stop"` Of course, this computer can be an SSH client: just use `"ssh login@ssh.server.org"` or `"scp source dest"`. Both source and dest may be local or remote. Use `"login@ssh.server.org:/path/filename"` for remote files.

5.3 Access a Windows computer with Samba

The samba package allows you to access a windows computer on the network. For example, if the windows server (192.168.10.3) has a share named "my-share", then you can mount it with these commands:

```
# mkdir /mnt/win
# mount -t smbfs -o lfs //192.168.10.3/my-share/ /mnt/win/
# cd /mnt/win
# umount /mnt/win
```

Samba is supported in the kernel, and samba tools are provided (smbcacls, smbcontrol, smbfilter, smbmount, smbpool, smbtar, smbclient, smbdrive, smbmount, smbpasswd, smbstatus, smbmount). It's important not to forget option "lfs" (Large File Support), because it allows to handle files that are larger than 2 GB. Big file are often used when making a backup or an image file. Without this option, the copy would fail, with an error. Large files are supported since version 0.2.12 (linux kernel 2.4.25). More help with samba: "<http://www.samba.org/>"

5.4 Mount remote FTP/SSH shares as local file systems

If you want to access files located on an FTP server, there is a new very powerful way to do this. The "userLand FileSystem" allows you to mount the share, and work on the remote files just as you would work on any local files. With all these file systems, you can unmount the share with the standard umount command.

Here is an example of how to mount an FTP file system in /mnt/ftp as anonymous (read only)

```
# mkdir /mnt/ftp
# lufsmount ftpfs://ftp.server.org /mnt/ftp
# cd /mnt/ftp
# umount /mnt/ftp
```

Here is an example of how to mount a private FTP account in /mnt/ftp2

```
# mkdir /mnt/ftp2
# lufsmount ftpfs://login:password@ftp.server.org /mnt/ftp2
# cd /mnt/ftp2
# umount /mnt/ftp2
```

Here is an example of how to mount an SSH file system in `/mnt/ssh` as anonymous (read only)

```
# mkdir /mnt/ssh
# lufsmount sshfs://login@ssh.server.org /mnt/ssh
# cd /mnt/ssh
# umount /mnt/ssh
```

5.5 Using an ADSL USB modem

Since version 0.2.19, le system comes with driver for several USB modems, such as SagemFast800 that is based on an eagle chipset. These drivers have been merged in Linux-2.6.16. If you have such a modem, you will probably need firmware images, that are not provided with this disc. You will have to download these files, and access it by mounting a partition of your harddisk, where you have downloaded theses files.

Chapter 6

System software

This CDROM aims to provide all the important pieces of software for system administration. Here are the most important tasks you can execute:

6.1 Graphical Partition Tools

This CDROM provides PartitionMagic clones, which aim to be very easy to use, and very powerful. Running these tools is very easy, but the FrameBuffer is required. Please refer to the boot process if you don't have the FrameBuffer. You can run QtParted by typing this command : "run_qtparted". You will be asked the mouse model. Try to give the right answer. If the system crashes, reboot and give another answer to this question. If you can't use your mouse, try to exit the software via the keyboard, and restart the software with another option for the mouse. Another graphical partition tool is available: PartGui. You can run PartGui by typing "run_partgui". PartGui is not developed anymore, then QtParted is a better choice.

6.2 Backing up your partition table

sfdisk is a tiny program that allows you to save your partition table. If you delete a partition accidentally, you can try to restore the table. The backup is done into a file. Of course, you must keep this file on a removeable media (such as a floppy disk), or on another computer. If your hard disk is damaged, you won't be able to read the backup from the disk itself !

This command allows you to backup the full partition table of your disk HDA: "sfdisk -d /dev/hda > bak-hda" Now, this command allows you to

restore from the file: "sfdisk /dev/hda < bak-hda". Of course, this command is very dangerous, because it overwrites the existing partition table !!! Before restoring, you should back up the current version, even if it seems to be damaged. This would allow you to undo the restoration.

6.3 Backing up the contents of a partition

Partimage (client and server) are provided. Partimage allows you to save an existing partition into an image file. If something goes wrong, you can restore the partition from the image. Here is the official homepage of the project: <http://www.partimage.org/>. A semi-text interface is provided, and this should not be very hard to use. You need a partition with a lot of free space in order to store the image file.

Since version 0.2.14 of SysRescCd, two partimage versions are provided:

- The default version is compiled without SSL and without login support. The client is available by typing "partimage", and the server with "partimaged". You should use this client in most cases, and when you connect a partimaged server that does not support SSL.
- The secured version is compiled with SSL and login support. The client is available by typing "partimagessl", and the server with "partimagedssl". You should use this client when you connect a partimaged server that expects and SSL encrypted connexion with login.

6.4 DAR (Disk Archiver)

Dar is an archiver like tar. But it's more powerful. Even using compression dar has not to read the whole backup to extract one file. This way if you just want to restore one file from a huge backup, the process will be much faster than using tar. Dar first reads the catalogue (i.e. the contents of the backup), then it goes directly to the location of the saved file(s) you want to restore and then proceed to restoration. In particular using slices dar will ask only for the slice(s) containing the file(s) to restore. But you can also restore all files from an archive, dar will then read sequentially without seeking into the file, except for the first and last slice, dar will not ask twice the same slice.

6.5 Clam AntiVirus

Clam AntiVirus is a free anti-virus software provided since version 0.2.3 of SystemRescueCd. It provides several commands:

- "clamscan -r /path/to/dir". It scan all files of this directory an search for viruses.
- "freshclam". This command updates the virus definitions. Of course, you need to be connected to internet for updating.

Before scanning for virus, you have to update virus definitions. Because this is run from a CDROM, you may have read-only related problems. That's why you have to specify a read-write directory for definitions. Here is how to update definitions and make a scan:

- Step-01. Make empty directories

```
# mkdir /virdefs /mnt/testpart
# chmod 777 /virdefs
```

- Step-02. Copy the current virus definitions

```
# cp /usr/share/clamav/* /virdefs/
```

- Step-03. Download the latest virus definitions

```
# freshclam --datadir /virdefs
```

- Step-04. Mount the partition to be scanned

```
# mount /dev/hda1 /mnt/testpart
```

- Step-05. Perform the scan on the files.

```
# clamscan -r -d /virdefs /mnt/testpart
```

If you really don't have any internet connexion, you can scan for virus without updaing virus definitions. Of course, it's less safe, and only old virus can be detected. Here are the steps:

- Step-01. Make empty directories

```
# mkdir /mnt/testpart
```

- Step-02. Mount the partition to be scanned

```
# mount /dev/hda1 /mnt/testpart
```

- Step-03. Perform the scan on the files.

```
# clamscan -r /mnt/testpart
```

Chapter 7

Secure Deletion of Data

7.1 Introduction

The secure removal of data is not as easy as you may think. When you delete a file using the default commands of the operating system (for example "rm" in UNIX or "del" in DOS or emptying the recycle bin in WINDOWS) the operating system does NOT delete the file, the contents of the file remains on your harddisk.

Most operating systems only remove references to the file when they are asked to delete a file. The file - you thought has gone forever - remains on the disk until another file is created over it (until another file overwrites the disk space where the "deleted" file is still stored), and even after that, it might be possible to recover the data by studying the magnetic fields on the disk platter surface using forensic equipment.

Before the file is overwritten by a new file, everyone can easily retrieve the data for example by using a disk undelete utility. And even after that some people (for example the three-letter-agencies) with special equipment are able to restore your data at least partially.

Everybody has sensitive data which they want to keep private. For example financial data, private emails, tracks of your internet surfing habits etc. I have heard of cases where people sold their old computers or harddisks and the buyer recovered their financial business data.

The only way to try to make recovering of your sensitive data nearly impossible is to overwrite ("wipe" or "shred") the data with several defined

patterns. For detailed information see the famous Paper by Peter Gutmann http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

CAUTION: The use of wiping or shredding tools relies on a very important assumption: that the filesystem overwrites the data in place. This is the traditional way to do things, but many modern filesystem designs do not satisfy this assumption for example ReiserFS, Reiser4, XFS, Ext3 etc.

See <http://www.die.net/doc/linux/man/man1/shred.1.html> for more information. In this case a solution could be to wipe/shred the entire device (partition) where the sensitive data was stored to ensure that the data is really overwritten.

SystemrescueCD provides a few tools which are able to make recovering of data nearly impossible - I say nearly impossible, because no one can give you a guarantee that for example the NSA or the FBI could not recover at least a part of that data. but using those tools makes it harder.

CAUTION: On the other hand you will not be able to recover any data, deleted by those tools. Take care. We will not take responsibility for loss of data.

If you want to have ultimate security, use encryption for example LOOP-AES <http://loop-aes.sourceforge.net/>. Encrypt your home directory or create an encrypted partition or container to save your data there.

7.2 Tools

- SHRED from the GNU coreutils (Fileutils) see <http://www.gnu.org/software/coreutils/> or <http://www.gnu.org/software/fileutils/doc/manual/html/fileutils.html#shred> You can use shred to securely delete simple files but also entire partitions or harddisks. Shred uses by default 25 overwriting passes, you can increase and decrease the number of overwriting passes. Therefore shred is faster than wipe (see above).

For example securely deleting all data on the first IDE harddrive:

```
# shred -v /dev/hda.
```

- WIPE from Sourceforge see <http://wipe.sourceforge.net> Similar to shred you can use wipe to securely delete simple files but also entire partitions or harddisks. Wipe uses by default 35 overwriting passes according to the Paper by Peter Gutmann http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html. Wipe is slower than shred, because it uses by default more overwriting passes and therefore it is more secure.

For example securely deleting the Windows 98 Swap File from a mounted (FAT) windows partition using 35 overwriting passes:

```
# wipe -D /mnt/windows/win386.swp
```

- SRM from the THC-Secure Deletion Tools see <http://www.thc.org/releases.php?q=delete> srm does secure deletion of files
- SFILL from the THC-Secure Deletion Tools see <http://www.thc.org/releases.php?q=delete> sfill does a secure overwriting of the unused disk space on the harddisk. sfill is the only UNIX tool I know which is able to clean the unused (free) disk space of a partition/harddisk.
You can also use the "dd" command to overwrite the unused disk space with zero or random bytes.
- SSWAP from the THC-Secure Deletion Tools see <http://www.thc.org/releases.php?q=delete> sswap does a secure overwriting and cleaning of the swap filesystem.
- SMEM from the THC-Secure Deletion Tools see <http://www.thc.org/releases.php?q=delete> smem does a secure overwriting of unused memory (RAM)

The THC-Secure Deletion Tools use by default 38 overwriting passes based on the Paper by Peter Gutmann http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, you can decrease the number of passes.

7.3 Other Tools

There are other tools on the SystemRescue CD which you can use similarly to overwrite especially devices, for example

- "dd": if=/dev/zero or /dev/urandom, of=device

- "dd_rescue": works similar to "dd"
- "badblocks": with -w option for writes 4 static passes

For more information take a look at the manuals.

7.4 Testing

In order to see how the tools work and to check if all sectors for example of a floppy have been overwritten, you can use VCHE the virtual console hex editor. In our example we will securely erase all data from a floppy.

First type the following command:

```
# shred -v -n 1 /dev/fd0
```

Shred will overwrite the floppy with one random pass.

Then let's run:

```
# vche-raw /dev/fd0
```

The floppy should be filled with random values.

Then we type the following command:

```
# shred -v -n 1 -z /dev/fd0
```

The -z Option will make a additional pass with zero values.

And we run VCHE again

```
# vche-raw /dev/fd0
```

The floppy should be filled with zero values.

Critical Comments, and Suggestions are welcome: klemens(dot)hofer(at)aon(dot)at

Chapter 8

How to personalize SystemRescueCd

8.1 Introduction

Being able to make one's own version of SystemRescueCd was a frequently requested feature. It's now possible to make your own version of SystemRescueCd.

This means you will be able to add files to the sysrcd.dat compressed image file, which will be the filesystem of SystemRescueCd. For example, you can add script files that make a full backup of a server, or a binary program that you need. It's also possible to add data files, in order to have everything on the CDRom (data and system files which allow you to restore data). For now, it's not possible to change the kernel. If you need a kernel option that is disabled, please contact us.

The goal is to produce a new ISO image file, with an updated sysrcd.dat. In order to be able to make your own version of SystemRescueCd, you will need a recent official version of this CDRom, and a partition with read-write access from within linux, with at least 500 MB. If you make a very large version of the CDRom, you may need a lot more space.

Be aware that this operation requires a large amount of memory (both RAM and space on the hard disk). If you don't have 128 MB of RAM, and at least 300 MB free on your hard disk, it will fail. You can create a swap partition in order to avoid problems with the cloop step in the script.

8.2 Usage

All the personalization is processed from the CDRom system with a script. This means you have to burn the official version, boot your computer from this official SystemRescueCd version, and then you are able to make your own version. The script needs to be run from the CDRom system, because it's easier to use this way. I am sure all programs are installed. If this script was designed to run from any linux installed system, you would have to install several programs, such as a module for the kernel, and it would be a lot more complex.

Here are the instructions to follow in order to make your own ISO image. We assume that the /dev/hda1 partition is formatted for linux (ext2, ext3, reiserfs, reiser4, xfs, jfs, ...), and that it has at least 500 MB free. It must really be a linux disk space, because other filesystem, such as FAT, NTFS don't support symbolic links and files permissions. If you only have a FAT partition available, you can create a virtual linux filesystem image inside the FAT partition:

```
# mount /dev/hda1 /mnt/fat
# cd /mnt/fat
# dd if=/dev/zero of=fsimage bs=1M count=500
# mke2fs -F -q -N 50000 fsimage
# mount -t ext2 -o loop fsimage /mnt/custom
```

If you use the "cdcach" boot option, the original SystemRescueCd disc must be mounted when you run the first step (extract) of the script.

8.3 procedure

This procedure will make a directory "customcd" at the root of this partition. All the files located in other directories won't be affected by this script. If you have an old version of this personalized CDRom in this directory, please make a backup. All files of "/dev/hda1/customcd/" may be lost! Note that you must keep the name "/mnt/custom" that we used in this example. You can't simply use "/mnt/another-name".

- Step-01: Mount the working partition:

```
# mount /dev/hda1 /mnt/custom
```

If you don't want the main temporary directory to be written to the root of `/mnt/custom`, you can choose another directory. For example, if the free space is an NFS share, you can try this:

```
# mount -o loop /mnt/nfs/usr/dir1/dir2 /mnt/custom
```

- Step-02: Extract the current files from the cloop image:

```
# /usr/sbin/sysresccd-custom extract
```

If there is no error, all the files of the cloop image should have been copied in `/mnt/custom/customcd/files/`

- Step-03: Customize files (optional)

You have to customize the files which you have just extracted. You can do this from the SystemRescueCd, but it's also possible to restart the computer and do it from any other installed linux system. If you choose to restart, you will have to restart from the SystemRescueCd, and mount files again (follow step-01 again). All the changes have to be made in the following directory: (This is the root of the new filesystem) `/mnt/custom/customcd/files/`

- Step-04: Create the new cloop image

In this step, all files from `/mnt/custom/customcd/files/` are read, and put inside the new cloop image. The new cloop image is copied in `"/mnt/custom/customcd/isoroot/sysrdd.dat"`, but you don't have to concern yourself with this.

```
# /usr/sbin/sysresccd-custom cloop 300 20000
```

This creates a cloop for a filesystem that uses 300 MB, and with less than 20000 files. If the command complains about space missing, try to increase these two parameters. For example, if your filesystem contains 50000 files and uses 10 MB, the previous command will complain (no space left on device).

- Step-05: Add files to the ISO image (optional)

By default, you only need the big cloop image file and the isolinux directory. The CDROM can work with only these two items on the disc. In this step, you can add other files to the ISO image, outside of the cloop image. For example, you can put big backup files inside the CDROM, and outside the cloop image, in order to avoid

overloading the cloop. If you are interested in adding such files, you just have to copy the files along with the sysrcd.dat, in this directory: "/mnt/custom/customcd/isoroot"

```
# cp -a my-files /mnt/custom/customcd/isoroot
```

You may add an autorun script to the root of the CDROM, outside of the cloop image. If you put an autorun script there, it can be run at startup. It allows to automake many tasks, such as doing a backup. See the autorun section for more details.

```
# cp autorun /mnt/custom/customcd/isoroot
# chmod 755 /mnt/custom/customcd/isoroot/autorun
```

Of course, you need to make sure that the size of the isoroot directory is not too big for your CDR (usually 700 MB). You can use the "du /mnt/custom/customcd/" command for that.

- Step-06: Select your keymap (optional)
In the official version, SystemRescueCd asks you to select a keymap at startup. If you want to avoid seeing this menu and define a permanent keymap, you can run this command:

```
# /usr/sbin/sysresccd-custom setkmap <your-keymap>
```

The second parameter is the name or the number of your keymap in the menu. For example, french users will use this:

```
# /usr/sbin/sysresccd-custom setkmap fr
```

- Step-07: Create the new ISO image
You just have to type this command. The second parameter to provide is the volume name for the CDROM.

```
# /usr/sbin/sysresccd-custom isogen my_srcd
```

- Step-08: Synchronize your disks
Before leaving the system and rebooting, you should make sure all your disks are cleanly unmounted. The best way to be sure not to lose data is to umount all mounted partitions, especially the temporary one (/dev/hda1 in this example), and then type "sync"

```
# cd / ; umount /mnt/custom ; sync
```

- Step-09: Test and burn the ISO image
The new final ISO image is located in `"/mnt/custom/customcd/isofile/sysresccd-new.iso"`. You can burn it with `cdrecord`, Nero, or any other burning software. If you don't want to burn a CDR, you can test it with VMWare. You have to tell this software that the CDRom drive to use is the virtual ISO-image file drive.

8.4 Result of your changes

When you start your computer with your own SystemRescueCd version, you can see all the files in `/mnt/cloop`. If your new files belong to a standard directory, you can access it without a problem. If you made a new directory in the root of the filesystem, it will appear in `/mnt/cloop`, but you won't see that in the root of the system. In fact, the root of the system contains symbolic links to `/mnt/cloop`. You may have to make the link yourself.

8.5 Autorun: scripts to be run at startup

SystemRescueCd 0.2.6 added the autorun script feature. It allows to run scripts automatically at startup of the system. Each autorun script can manage a task. For example, you can create a backup script that makes a backup of a database, another for cleaning a system, ...

By default, the autorun script(s) may be copied in the root of the CDRom, outside of the compressed loop image file (`sysrcd.dat`), but other sources are available : floppy disk, HD partition, network share.

The script may be named "autorun" if alone. If many scripts have to be chained, you may name them "autorun0", "autorun1",... . In this case, specific autorun scripts may be allowed with an "autoruns=" startup option given at boot time prompt. For example, you may type "fb800 autoruns=2,3,4".

If you want to use floppy or network source for autorun files, you will have to specify another special boot parameter to enable it. More on this in next section.

8.5.1 Summary of rules

At startup, a list of locations are checked against the presence of autorun files. They are, successively:

- if the `ar_source=` parameter was passed at startup, the root directory of the given mountable device. This is primarily intended for floppy disks :

- `fb800 ar_source=/dev/fd0`

but may be used with hard disk partitions too :

- `fb800 ar_source=/dev/hda2`

- to look for autorun scripts in 2nd partition of 1st IDE hard disk

- `fb800 ar_source=/dev/sdb6`

- to look in 6th partition of 2nd SCSI hard disk

and with network shares. The syntax is :

- `fb800 ar_source=nfs-server:/nfs/exported/directory`
for NFS shares

- `fb800 ar_source=//samba-server/share`
for SMB shares (recommended without user/password)

Source devices are mounted to `/mnt/autorun`, allowing writing data into them if the device is not write-protected.

- the root directory of the CDrom
- the superuser home directory (`/root`)
- the `/usr/share/sys.autorun` directory

If autorun files are found in some location, they are run and the process ends. Last two locations require rebuilding of SystemRescueCd and are to be used for advanced or test purposes.

In each source location, there are two possible modes of operation :

- simple one : if a shell script named "autorun" is found, it is run
- more flexible : if "autorun#" scripts are found (# is a digit from 0 to 9) and either

- autoruns= boot parameter was NOT specified, or
- autoruns= boot parameter value contains #
(ex: "fb800 autoruns=0,1,4" - In this example, only autorun0, autorun1 or autorun4 scripts may be run if present. Other scripts, such as autorun2, autorun3 and autorun5, will be ignored)

then authorized scripts are run in alphabetic order. Whenever a script returns a non-zero code, the processing stops and next scripts are not run. You can prevent any "autorun#" execution with an autorun= boot parameter without any digit, ex: "autoruns=no". This has no effect on "autorun" script.

Although it is possible to put both "autorun" and "autorun#" scripts, this should probably be avoided.

The script has to be any valid shell script. Perl, python, ... etc. scripts are not supported at this time. Windows end-of-line terminators are translated to allow running shell scripts written with a MS editor.

8.5.2 Examples of autorun scripts

```
#!/bin/bash
(
  ifconfig eth0 | head -n 3
  fdisk -l /dev/hda
) | tee -a /mnt/autorun/report
sync
exit 0
```

This script will accumulate infos about eth0 network interface and disk partitions into a file named "report" on first floppy drive. BIOS boot sequence must specify CD first, ar_source= boot parameter has to be correctly set, diskette must be write-enabled, CD and diskette must be inserted at startup time.

If network is automatically configured at boot (DHCP), you may send infos through a NFS or samba share for example.

Don't forget to give autorun location at startup. Say that you share through NFS a writable directory named /nfs/backup on host myserver, you have to specify :

- fb800 ar_source=myserver:/nfs/backup

at SystemRescueCd boot prompt and to put in the shared directory an "autorun" script like this one :

```
#!/bin/bash
date=$(date +%Y%m%d)
cat /dev/hda | gzip > /mnt/autorun/$date.hda.gz && exit 0
echo $date hda backup error
exit 1
```

If sufficient space is provided in NFS share, this will copy there a compressed image of your first IDE disk.

You must ensure that name resolution works if you will access NFS server by its name instead of its IP address.

Chapter 9

How to burn a DVD with SystemRescue and 4 GB more files

9.1 Introduction

It is possible to burn SysResCd on a DVD disc (DVD-R, DVD+R, DVD-RW, DVD+RW), and to copy 4 GB of data files on this disc. It allows to make a disc with both your backup files, and the system that allows to restore it. A simple layer DVD provides 4.3 GB of space. Since SysResCd uses about 100 MB, you will have about 4.2 GB of free space. It allows to copy quite big image files (you can make an image of your system with partimage, ntfsclone, ghost, DriveImage, ...)

This manual explains how to make such a bootable DVD under Linux, but it should be possible to do the same under Windows with Nero.

9.2 Requirements

Of course, you need a DVD burner, a disc. You also need an installed Linux system, with dvd+rw-tools. If you don't have this software, you can download on the following homepage:

<http://fy.chalmers.se/~appro/linux/DVD+RW/>

You need to know the device name of your DVD burner. If you don't know it, you may find it with dmesg. You should see something like this:

```
# dmesg | grep DVD
hdd: PIONEER DVD-RW DVR-106D, ATAPI CD/DVD-ROM drive
hdd: ATAPI 32X DVD-ROM DVD-R CD-R/RW drive, 2000kB Cache, UDMA(33)
```

In this example, the two output lines allow to know the device name. It's `/dev/hdd`.

This was tested under Linux-2.4.26, with `dvd+rw-tools-5.17`, on a DVD+RW, and the device was "Pioneer DVR-106D". It is supposed to work with all kind of DVD discs, and all DVD burners.

9.3 First step: burn the official SysRescCd ISO image

In this first step, we will just burn the official 100 MB image on the DVD disc.

```
growisofs -Z /dev/hdd=systemrescuecd-x86-0.2.14.iso
```

Of course, you have to replace "hdd" with the device name of your burner, and update the path to the ISO file.

9.4 Second step: add your own files

Now, we will add files to the disc. All the files you want to add have to be stored in the same directory. In this example, we suppose files are stored in `/home/user/mydvd-data-files/`:

```
growisofs -M /dev/hdd -J -R /home/user/mydvd-data-files/
```

It should be possible to add files several times by running this command several times.

Chapter 10

How to install SystemRescueCd on hddisk

10.1 Introduction

The idea is to install SystemRescueCd tools onto a Linux partition to easily recover your system in case something goes wrong. You will have an installed system that works like other linux systems installed by other distributions. If you just want to be able to run SystemRescueCd from your hard disk, and have an entry in your bootmanager (Lilo or Grub), there is an easier method, that is explainted in the next chapter.

WARNING: Be aware that this operation may give you an useless system if you don't strictly follow instructions below.

10.2 Usage

All the job is processed from the official SystemRescueCd CDRom. This means you have to burn the official version and boot your computer from it.

10.3 procedure

- step-01: Create a new partition
You have to resize an existing partition and then create an empty ext2fs partition. Note: only ext2fs is supported at the moment.

```
# run_qtparted
```

I will suppose you now have an NTFS partition `/dev/hda1` and an ext2 partition `/dev/hda2`. You have to update this to your setup.

- step-02: Mount the new partition

```
# mount /dev/hda2 /mnt/custom
```

- step-03: Extract the current files from the cloop image

```
# sysresccd-custom extract-nosizecheck
# rm -rf /mnt/custom/customcd/isoroot
# mv /mnt/custom/customcd/files/* /mnt/custom
# rm -rf /mnt/custom/customcd
```

- step-04: Copy the SystemRescueCD kernel

```
# cp /mnt/cdrom/isolinux/vmlinuz1 /mnt/custom/boot
```

- step-05: Customize setup to your hard disk
Add this line to `/mnt/custom/etc/fstab` file

```
/dev/hda2 / ext2 errors=remount-ro 0 1
```

Copy this file from `/usr/share/sysresccd/hdinstall/lilo.conf.in` to `/mnt/custom/etc/lilo.conf`

```
lba32
boot = /dev/hda
map = /boot/.map
prompt
install = /boot/boot-menu.b
delay = 50
vga = normal
default=win
image = /boot/vmlinuz1
    root = /dev/hda2
    label = sysrcd
    read-only
other = /dev/hda1
    label = win
    table = /dev/hda
```

WARNING: do not forget to replace /dev/hda1 and /dev/hda2 with your values if you want your system to boot.

- step-06: Run lilo

```
# mount -t devfs none /mnt/custom/dev
# chroot /mnt/custom lilo
# umount /mnt/custom/dev
```

- step-07: Umount the new partition

```
# umount /mnt/custom
```

10.4 Changes as boot time

At boot time, you should now have a prompt like this one:

```
LILO 22.5.1
```

This means that LILO is installed and running. If you let the timer going down (about 5 secondes), your default target will be launched. With previous lilo.conf file, it will be Windows.

If you wish to test your new SystemRescue partition, press left shift key. You will get

```
LILO 22.5.1 boot:
```

Then enter "sysrcd".

If you do not remember your target list, hit tabulation key and LILO will show you

```
LILO 22.5.1 boot:
```

```
win sysrcd
```

Chapter 11

Easy install SystemRescueCd on harddisk

11.1 Introduction

Since version 0.2.19, there is an easy way to boot SystemRescueCd from the harddisk. This method allows to use SystemRescueCd as you do with the CDRom version. But this method does not require to insert the disc in the drive each time you need it. It also allows to boot SystemRescueCd if you don't have an optic drive in your computer. You can use another operating system to process the installation of SystemRescueCd, and enable it.

Thus, this method is recommended if you often use SystemRescueCd and you want to avoid having to insert the disc in the drive each time.

11.2 Requirements

There are two steps in this installation: first you will have to copy main SysResCd files on a partition of your disk. Then, you will have to configure your bootmanager. The installation process requires a partition with about 130 MB free space, and you must have a working linux bootmanager installed, such as Lilo or Grub. (maybe it can work with other boot managers).

The partition where you will copy SystemRescueCd files does not have to be formatted for Linux. It can have any file system that Linux-2.6 is able to mount in read-only, and with a file system your boot manager is able to use. It mean you can use a FAT16 or FAT32 partition or a Linux native partition (ext2, ext3, reiserfs, reiser4, xfs, jfs). You can store sysrcd.dat on an NTFS partition, but this file system cannot store vmlinuz1 and initrd1, since there is a problem with grub and lilo when loading a file from an NTFS disk at

boot time. This partition may be already used for something else (Linux installed on), or it can be a partition you made only for SystemRescueCd.

In the second step, you will need the Linux device name of this partition (a name such as `/dev/hda1`, `/dev/sda1`, `/dev/hdb5`, ...)

11.3 First step: copy important files

This step is very trivial: you just have to copy the three SysRescCd main files to the partition. If that's a FAT16/FAT32 partition, you can perform the copy with any operating system. Of course, if you choose a Linux native partition, you will have to copy from Linux (you can copy from SystemRescueCd itself).

You must create a directory `/sysrcd/` that's in the root of the partition. The name and the position of this directory cannot be changed.

Now, take the disc with the latest SystemRescueCd version (you may prefer to mount the ISO image with `mount` under Linux or you can use a software such as DaemonTools under Windows if you did not burn the disc), in order to have the three main files.

Finally, just copy `sysrcd.dat`, `initrd1` and `vmlinuz1` from the CDRom to the directory you made (`/sysrcd/`). Two of these files are located in `isolinux` inside of the CDRom.

11.4 Second step: update the bootmanager

Now, you must update your bootmanager (Lilo or Grub).

You need the Linux device name of the partition you have chosen (a name such as `/dev/hda1`, `/dev/sda1`, `/dev/hdb5`, ...). If you don't know this name, you should boot SystemRescueCd from the CDRom drive, and list all devices seen by the linux kernel. Just type `"cat /proc/partitions"` in a console. You may also run `QtParted` to identify the partition.

We will have to add several lines to the configuration file of the bootmanager (usually `/etc/lilo.conf` for Lilo, and `/boot/grub/menu.lst` or `/boot/grub/grub.conf` for grub). You have to personnalize the configuration given there. You must replace `/dev/xxx` with the device name of your partition. With grub, you will have to give the grub device name for the partition you have choosen. It's usually a name like `(hd0,0)` instead of `hda1` (`hd0,1`) instead of `hda2`, ... Then, you may update several options related to your keyboard (`setkmap=xxx`), and your video settings (`vga=xxx`) You may have a look at `isolinux.cfg` that's in the CDRom, if you don't know the values you can use for these options.

First, here is an example of the Lilo configuration (edit `/etc/lilo.conf`) The path `/mount-point/` must be replaced with the mount point for the partition at the time you run lilo, and you must replace `/dev/xxx` with the linux device name for the partition files were copied on.

```
image=/mount-point/sysrkd/vmlinuz1
root=/dev/ram0
initrd=/mount-point/sysrkd/initrd1
label=SysRescCd
append="bootfrom=/dev/xxx init=/linuxrc setkmap=us"
vga=5
```

Here is an example of Grub configuration (edit `menu.lst` or `grub.conf` in `/boot/grub/`) In this example, files are located in `/dev/hda5`. The grub device name is `(hd0,4)`

Warning: There is no line break for the line beginning with kernel.

```
title      SystemRescueCd
kernel    (hd0,4)/sysrkd/vmlinuz1 root=/dev/ram0 vga=5
          bootfrom=/dev/xxx init=/linuxrc setkmap=us
initrd    (hd0,4)/sysrkd/initrd1
boot
```

If your bootmanager is Lilo, don't forget to run lilo after lilo.conf was edited. With Grub, this step is not required.

Now, the installation process is complete. SystemRescueCd should appear in your bootmanager menu the next time you start your computer.

Chapter 12

How to install SystemRescueCd on an USB-stick

12.1 Introduction

This chapter explains how to install SystemRescueCd on an USB-stick. It allows to use this system from an USB stick (mini hard disk) instead of using a CDRom. First, you need SystemRescueCd 0.2.18 or newer, and an USB stick with enough space. If you use the official version, you need 128 Mb or better. Of course, you need a computer that supports USB, with almost a free USB socket. Your BIOS must be able to boot on USB hard disks, and it must be defined before other devices in the boot devices order.

12.2 Installation from Linux

If you don't have Linux installed, you can burn SystemRescueCd on a CDRom, and perform the install from this system itself.

- step-01: Find the device name

You need the device of the USB stick. In most cases, Linux detects this device as an SCSI hard disk. In other words, it is detected as `/dev/sda1` (first partition of first SCSI device), or `/dev/sdb1` if you have another SCSI device. Since kernel 2.6.8 USB sticks may be seen as `/dev/uba`, `/dev/ubb`, ...

Here is how you can know the device name. First, start your computer under Linux with the USB stick unplugged. Then, load all USB modules (you may need to load other USB modules first). This command should not be required if the USB storage support is build-in the kernel. If `modprobe` can't find this module, it might be normal.

```
# modprobe usb-storage
```

Now, you have to plug your USB stick, and have a look at the kernel messages. You may find the device name.

```
# dmesg | tail -n 50
```

Here is a example of report from the kernel:

```
Initializing USB Mass Storage driver...
usb.c: registered new driver usb-storage
USB Mass Storage support registered.
hub.c: new USB device 00:02.0-2, assigned address 3
scsi1 : SCSI emulation for USB Mass Storage devices
  Vendor: EXATEL    Model: i-BEAD100    Rev: 0001
  Type:   Direct-Access          ANSI SCSI revision: 02
WARNING: USB Mass Storage data integrity not assured
USB Mass Storage device found at 3
```

Then, you should try to mount the device:

```
# mkdir /mnt/usbstick
# mount -t vfat /dev/sda1 /mnt/usbstick
```

If there is no space enough left on the device (about 120 MB), you will have to erase the current files (all data will be lost):

```
# rm -rf /mnt/usbstick/*
```

- step-02: Copy files from the CD Rom

Now, you have to copy the most important files. The SystemRescueCd disc must be mounted on `/mnt/cdrom`. You can mount the ISO file too, in order to avoid burning a CD-R. The stick is mounted on `/mnt/usbstick`.

```
# cp /mnt/cdrom/syslinux/syslinux.cfg /mnt/usbstick/
# cp /mnt/cdrom/sysrcd.dat /mnt/usbstick/
# cp /mnt/cdrom/isolinux/* /mnt/usbstick/
# cp /mnt/cdrom/bootdisk/* /mnt/usbstick/
```

- step-03: Make the disk bootable

Now, you have to unmount the USB stick, and make it bootable with syslinux. Of course, you have to replace `/dev/sda1` with the device name of your stick:

```
# umount /mnt/usbstick
# syslinux /dev/sda1
# sync
```

12.3 Installation from Windows

- step-01: Find the device letter

You have to plug your USB stick while Windows is running. In the explorer, a new drive letter will appear, and you can access the file of this USB stick. In this manual, we will suppose your USB stick letter is E:. Don't forget to change this letter in the commands if required.

- step-02: Copy files from the CDRom

Now, you have to copy the most important files from the CDRom. If you don't want to burn the CDRom, you can read the files from the ISO file with utilities such as WinImage.

First, format the device. You will need about 120 MB. You have to copy several files:

- * 1) Copy "syslinux/syslinux.cfg" to the root of the USB device
- * 2) Copy "sysrcd.dat" to the root of the USB device
- * 3) Copy files in the "isolinux" directory to the root of the USB device
- * 4) Copy files in the "bootdisk" directory to the root of the USB device

- step-03: Make the disk bootable

Now, you have to make your stick bootable with syslinux. You will have to run this program from a prompt console (cmd.exe). Don't forget to change this letter in the commands if required.

```
# syslinux E:
```

You can find the syslinux program on the CDRom. The Windows version is provided as a ZIP archive. You just need syslinux.exe from the archive.

12.4 Booting from the USB stick

First, check the "USB hard disk" is defined as the first boot device in your BIOS. If that works, you should see the SystemRescueCd boot splash with the prompt. It must not be required to add option "usbstick" to the command line, since it has been added in syslinux.cfg. But if you have problems, try it anyway. For example, if you want to use the FrameBuffer with a 800x600 screen, you should type this at prompt:

```
# fb800
```

You should press F2, F3, F4 for more help about boot options. Then, press enter. It must work as a regular SystemRescueCd from a CDRom drive.

Chapter 13

Mounting an NTFS partition with full Read-Write support

13.1 Introduction

NTFS (New Technology File System) is a very powerful file system provided with NT versions of Windows (Windows-NT, Windows-2000, Windows-XP). Even if Windows still supports FAT, the Windows system disk is often formatted in the NTFS format.

Linux offers a complete read support for NTFS partitions for a long time. But the NTFS write support is still partial. The write support was improved in linux-2.6.15 that is provided in SysResCd-0.2.16. It's now possible to write inside existing files, even if it makes the file grow. The write operation may fail, but it cannot damage the NTFS partition's structure. It is still not possible to create new files with the current state of the NTFS driver. The NTFS write support is safe but incomplete. You should use it if you just want to commit a change in a document, and it allows to clean infected files by a virus on a system.

If you just want a read support or a basic write support on NTFS disks, you just have to mount it with the following command (you have to replace xxx with the device name of your disk):

```
# mount -t ntfs /dev/xxx /mnt/part
```

If you really need a complete NTFS Write support, you will have to use CaptiveNtfs. It is not so easy to use, and it is a lot slower. This project uses the NTFS supports from the Windows kernel itself. These drivers have to be copied from an installed Windows XP system. You can't get these files from Windows NT4 or Windows 2000. But once you get the drivers from

XP, you can mount any NTFS version. It Captive does not want the NTFS driver that comes with the system that is installed on your computer, you will have to download Service Pack 1 for an English version of Windows XP, and extract `ntfs.sys` and `ntoskrnl.exe`.

This chapter explains how to use the Captive-Ntfs support from SystemRescueCd.

13.2 Getting the Windows drivers

We cannot distribute the Windows drivers because these files are distributed under a Microsoft license. Then you have to get these files yourself from the Windows system partition first. You have to copy these files inside the linux system:

- step-01: Mount the Windows system partition
Here is an example about how to mount the Windows-XP partition, supposed to be `/dev/hda1`:

```
# mkdir /mnt/win
# mount -o ro -t ntfs /dev/hda1 /mnt/win
```

- step-02: Copy the drivers files
Windows is supposed to be installed in `C:/WINDOWS`. Sometimes, the user can choose another directory, such as `C:/WINNT`.

```
# cp /mnt/win/WINDOWS/system32/drivers/ntfs.sys /var/lib/captive
# cp /mnt/win/WINDOWS/system32/ntoskrnl.exe /var/lib/captive
```

If a file or a directory does not exist, try to change the Case ("`System32`" instead of "`system32`" for example). You can find these files on an Windows NT4 or Windows 2000 system, but only Windows XP files will work with Captive Ntfs.

- step-03: Umount the Windows partition

```
# cd / ; umount /mnt/win
```

13.3 Mounting NTFS with full support

Now the drivers are copied, you can mount any NTFS partition, even if it does not have windows installed on:

```
# chmod 770 /  
# mount.captive-ntfs -o --rw /dev/hda1 /mnt/win
```

Now, you must be able to write file on the mounted partition:

```
# cd /mnt/win  
# touch creating-an-empty-file  
# cp -a /path/to/a/directory /mnt/win
```

Of course, you will have to unmount this partition when finished to work on:

```
# cd / ; umount /mnt/win
```

13.4 Remarks

For the moment, DF is not supported with Captive-Ntfs. It mean the program that shows the disk space usage (DF=Disk Free) won't show any information about the mounted NTFS partition. If you really need this informations, you have to remount the partition read-only, with the official linux NTFS driver.

More informations about Captive-Ntfs:

<http://www.jankratochvil.net/project/captive/>

Chapter 14

System boot floppy disks

14.1 Introduction

Of course, the most important feature of SystemRescueCd is the Linux system that is run from the CDRom, and that allows to do many administration tasks. Since version 0.2.9, SystemRescueCd allows to work from virtual bootable floppy disks. These virtual floppies offers the same feature you could have with a physical floppy disk you boot on when you start your computer. For example, several users need system DOS programs. They start from a DOS floppy disk, and they can run these tools. SystemRescueCd comes with several system floppy disks. The floppy list appears when you press F2 in the very first prompt. This page shows many option on the top, and floppy disks images at the bottom. In the next section, we will have an overview of each of them.

14.2 Overview of the boot floppy disks

- FreeDos
Just type this image name at prompt:

```
freedos
```

FreeDos is a free operating system compatible with MS-DOS. It allows to run DOS programs such as Partition Magic or Drive Image without any MS-DOS license.

- MemTest+
Just type this image name at prompt:

memtest

Memtest+ 1.0 is an update of Memtest-x86 3.0. It's a memory tester. This program will tell you if your physical memory is damaged or not.

- GAG: Graphical-Boot-Manager
Just type this image name at prompt:

gag

GAG is a boot manager, such as Lilo, Grub, or Boot-Magic. It aims to be very nice and easy to use.

- Ranish Partition Manager
Just type this image name at prompt:

ranish

Ranish Partition Manager is a low level partition manager such as Fdisk, but it's more powerful.

- Aida
Just type this image name at prompt:

aida

Aida is an advanced diagnostic system program. It will detect many pieces of hardware of your computer, such as the Processor, chipset, mainboard, network card, ... It's very useful when you want to download a driver and you don't know which one to take.

- Dban (Darik's Boot and Nuke)
Just type this image name at prompt:

dban

Dban is a bootdisk that allows to destroy all data of a computer. Be aware it's dangerous to use. You can use dban if you want to be sure nobody can be able to read data of a computer. For example, if you want to give your computer to someone, and your computer had important data, you can use dban before giving the computer. It will wipe all data from all hard disks.

- Offline NT Password and Registry editor

Just type this image name at prompt:

ntpass

This program allows to change system informations written in the Windows settings. The most interesting one is the ability to change the password of a user account. Now, you won't have to reinstall Windows if you forget the password of the administrator account. You just have to edit the password with this utility. This program also allows to edit the Windows registry. It work even when Windows is installed on an NTFS disk.