

Hard Drive Recovery Using SystemRescueCD

Michael Ward
4/1/2008

Introduction

SystemRecoveryCD is a bootable “live CD” featuring a version of Linux specifically created to recover data from damaged or infected hard drives. You will need to download and burn the ISO file to a CD. You can get the ISO from:

http://www.sysresccd.org/Main_Page
<http://slug.ceca.utc.edu/ftp/pub/systemrescuecd/>

Disclaimer

WARNING: While not likely, it is possible to erase your entire hard drive with SystemRescueCD beyond any hopes of recovery. You are using the software and this guide at your own risk. No warranties are implied or given.

Help

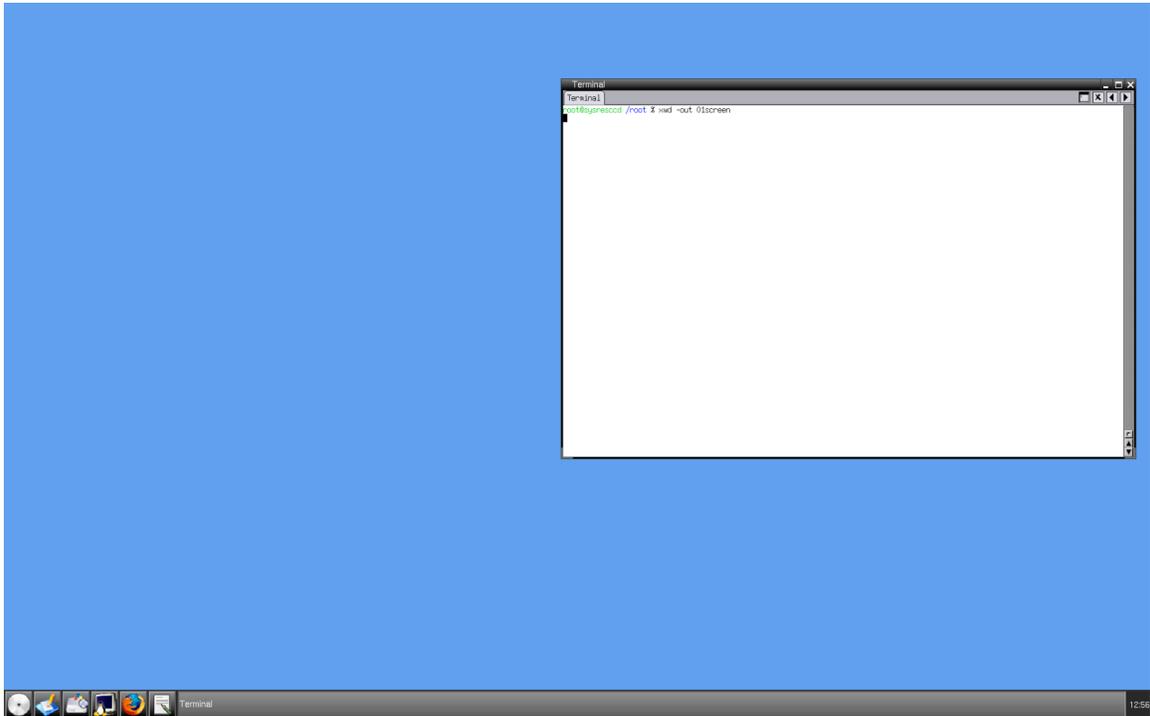
The above link to the SystemRescueCD page is a good resource, as is a quick search of Google. You can also use the “man” function within a shell. For example, “man mount.cifs” would bring up a manual page on the mounting of CIFS (Windows shares).

Booting

Assuming you’ve set your BIOS to boot from CD, after booting you should be with an zsh (command line) shell session as root. If you don’t know how to set your BIOS to boot from CD, you shouldn’t be using this guide. Go find an expert.

It is much easier to perform a system rescue with multiple terminals available, so you should start the X-Windows system by typing “startx” followed by the return key. You should see something

like:



The major tools are presented as icons at the lower left of the screen. For the rest of this guide you will need an open zsh session. Click on the “penguin with a TV” icon.

Networking

Assuming you’ll be copying data to another server, you’ll need to setup the network connection. The easiest way is to use DHCP via the `dhclient`. From within the zsh type “`dhclient`”

```
Terminal
root@sysresccd /root % dhclient
Internet Systems Consortium DHCP Client V3.1.0-Gentoo
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:1a:a0:de:f4:58
Sending on   LPF/eth0/00:1a:a0:de:f4:58
Sending on   Socket/fallback
option_space_encapsulate: option space agent does not exist, but is configured.
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCNACK from 10.51.8.1
option_space_encapsulate: option space agent does not exist, but is configured.
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 10.51.8.1
option_space_encapsulate: option space agent does not exist, but is configured.
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPCACK from 10.51.8.1
bound to 10.51.8.21 -- renewal in 341119 seconds.
root@sysresccd /root %
```

You need to test your network connection, and since you'll probably need a browser at some time, launch Firefox via its icon.

The screenshot shows a web browser window with the address bar displaying `http://slug.ceca.utc.edu/`. The browser's menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. Below the address bar, there are navigation icons and a search bar with the text "Getting Started" and "Latest Headlines".

The website content is organized into a header with navigation links: UTC, People, BB, USUS, Maps, Jobs, News, Weather, Movies, TV, GIS, FTP, and a search bar with "Google" and "Go" buttons. Below the header are several icons: a green alien-like character, a green robot, a red truck, and a blue car. There are also links for Downloads, FTP Site, Links, RSS, Comics, Movies, Network Uptime, Documents, Protecting Windows, and Cleaning Windows.

The main content area features a list of news articles, each with a timestamp, a title, and a brief description:

- 04/01/08 08:49 Review of Windows Mobile 6.1** (www.pcmag.com)

"Windows Mobile 6.1, the latest upgrade to Microsoft's main operating system for handhelds, has a few important invisible patches and a bunch of minor interface tweaks."
- 04/01/08 08:46 Beware of virus-ridden April Fools email** (www.heise-online.co.uk)

"The criminals behind the Storm worm are exploiting this user behaviour by sending out what seems to be an April Fools e-mail. T"
- 04/01/08 08:31 Google Docs goes "off line"** (www.techworld.com)

"Over the next three weeks or so, Google will turn on the feature for all word processor users, giving them the ability to view and edit documents while offline. During the same time period, Google Docs' spreadsheet will gain offline ability for viewing, but not editing, documents."
- 04/01/08 08:30 Up to 6% of Internet traffic is potential DDOS packets** (www.techworld.com)

"Studying the data from about 1,300 routers over 18 months, Arbor found that the tidal waves of SYN or ICMP (Internet Control Message Protocol) packets used in DDos attacks rarely dropped below 1 percent of all traffic and could easily rise to 6 percent during peak periods."
- 03/31/08 21:36 It has begun...April Fool's Day** (www.sophos.com)

Sophos AV w/face recognition
- 03/31/08 21:03 AppleTV 2.0.1 Update** (www.pcworld.com)

"Given the general "bug-fixiness" feel of the update, it's not too surprising that Apple isn't trumpeting its glories. The update does, however, bring a few new features to Apple TV"
- 03/31/08 20:40 CRITICAL:Active X in CA products** (www.heise-online.co.uk)

"It includes: BrightStor ARCServe Backup for Laptops and Desktops, CA Desktop Management Suite, Unicenter Desktop Management Bundle, Unicenter Asset Management, Unicenter Software Delivery and Unicenter Remote Control."
- 03/31/08 20:39 OpenSSH 4.9** (www.heise-online.co.uk)

"For example, OpenSSH now supports chroot, although the development team warn that this feature should be used with caution. The sftp server is now directly linked into sshd, so that when used, for example, in combination with the chroot option, no additional configuration is required."
- 03/31/08 20:21 Wireshark 1.0** (tech.slashdot.org)

"The release features several security fixes and an experimental package for Max OS X Intel"
- 03/31/08 14:03 PGP opens APIs** (www.infoworld.com)

"We publish our source code to anybody," says Phil Dunkelberger, PGP president and CEO. "Now we're publishing our APIs so people can code to our products."
- 03/31/08 14:03 AMD produces first Display Port video card** (www.theinquirer.net)

"launched what it claims is the first commercially available 3D workstation graphics card with Display Port support. The ATI FireGL V7700 is aimed at Computer Aided Design, Digital Content Creation and Medical Imaging."
- 03/31/08 13:08 Ars reviews Gnome 2.22** (arstechnica.com)

"This article will examine many of the new features and programs included in GNOME 2.22 and illuminate how the changes and improvements impact the overall user experience. We will also provide some insight into some of the new architectural features and demonstrate how they can be leveraged by third-party software developers."
- 03/31/08 12:47 Adobe joins Linux Foundation** (linux.slashdot.org)

"Adobe announced Monday that it is joining the Linux Foundation and alpha-released a Linux version of its new Adobe Internet Runtime environment."

On the right side of the page, there is a sidebar titled "Current Critical Alerts" with a list of security-related items:

- Active X in CA products
- MS Bulletin MS07-025 Re-release
- RTSP vuln in VLC and Mplayer
- Firefox 2.0.0.13 is out
- Microsoft .NET Framework
- Safari 3.1 (Windows) Zip Vulnerability
- Microsoft Word Vuln
- Excel Patch Reissue
- VMware patches

Below the alerts is a "Systems Status" section showing "04/01/08 12:55:01" and "All Systems Online" with a link to "Offline Log".

At the bottom of the browser window, there is a taskbar with several application icons, including a terminal window labeled "Terminal".

Connecting to a Networked Server

Now we've got to copy the data to a networked server which can be a ftp server, a Windows server, or via ssh to a Linux/BSD box. For the first example, we'll attach to a Windows share using `mount.cifs`. As demonstrated in the following image, you need to create a mount point and then attach the server to that mount point.

```
Terminal
root@sysresccd /root % mkdir /mnt/smb
root@sysresccd /root % mount -t cifs //slug.ceca.utc.edu/mward /mnt/smb -o username=mward
Password:
root@sysresccd /root % df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           1.5G  47M  1.5G   4% /
/dev/sr0        184M  184M   0 100% /mnt/cdrom
/dev/loop0     152M  152M   0 100% /mnt/livecd
udev           10M   216K  9.8M   3% /dev
tmpfs           1.5G  4.6M  1.5G   1% /lib/firmware
tmpfs           1.5G   0  1.5G   0% /usr/portage
//slug.ceca.utc.edu/mward
38G   25G   12G  69% /mnt/smb
root@sysresccd /root %
```

The “df -h” command lists the mounted file systems. You can also mount a remote system using ssh.

```
Terminal
root@sysresccd /root % mkdir /mnt/ssh
root@sysresccd /root % sshfs mward@slug.ceca.utc.edu:/home/mward /mnt/ssh
The authenticity of host 'slug.ceca.utc.edu (10.51.2.26)' can't be established.
RSA key fingerprint is a2:13:e0:64:6f:1f:64:d9:3c:f6:fa:0f:51:37:d3:32.
Are you sure you want to continue connecting (yes/no)? yes
mward@slug.ceca.utc.edu's password:
root@sysresccd /root % df
Filesystem      1K-blocks    Used Available Use% Mounted on
tmpfs           1549824      49736  1500088   4% /
/dev/sr0        187404      187404     0 100% /mnt/cdrom
/dev/loop0     154880      154880     0 100% /mnt/livecd
udev           10240         216   10024    3% /dev
tmpfs           1549824      4660  1545164   1% /lib/firmware
tmpfs           1549824         0  1549824   0% /usr/portage
//slug.ceca.utc.edu/mward
39674192  25846780  11779528  69% /mnt/smb
mward@slug.ceca.utc.edu:/home/mward
1048576000         0  1048576000   0% /mnt/ssh
root@sysresccd /root %
```

Now that we have a location for backup, we have to mount the filesystem on the hard drive. The easiest way to find out what partitions are on a disk is to use Gparted (the disk icon).

Partition	Filesystem	Size	Used	Unused	Flags
/dev/sda1	fat16	47.03 MiB	7.04 MiB	39.99 MiB	
/dev/sda2	ntfs	244.14 GiB	62.13 GiB	182.01 GiB	boot
unallocated	unallocated	2.78 MiB	---	---	
/dev/sda3	ext3	6.52 GiB	2.70 GiB	3.82 GiB	
▼ /dev/sda4	extended	215.05 GiB	---	---	
/dev/sda5	linux-swap	7.45 GiB	---	---	
/dev/sda6	ext3	207.60 GiB	3.45 GiB	204.15 GiB	

0 operations pending

You can see that this particular disk is 500G, with a 47M Dell recovery partition, a 244G Windows (NTFS) partition, 2 Linux (ext3) partitions, and a Linux swap partition. Now that we know the device (sda here) we can verify the partition map with fdisk.

```
Terminal
root@sysresccd /root % fdisk -l /dev/sda

Disk /dev/sda: 500.1 GB, 500107862016 bytes
255 heads, 63 sectors/track, 60801 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            1           6     48163+   de  Dell Utility
/dev/sda2 *          7        31877    256000000   7  HPFS/NTFS
/dev/sda3            31878       32728     6835657+  83  Linux
/dev/sda4            32729       60801    225496372+  5  Extended
/dev/sda5            32729       33701     7815591   82  Linux swap / Solaris
/dev/sda6            33702       60801    217680718+  83  Linux

root@sysresccd /root %
```

We want to copy from the Windows partition, so we have to mount it. **Note the use of “ro” as an option. This is read-only and prevents any changes to the Windows partition. If you want to change the Windows files, such as when doing virus removal, you would leave off the “-o ro”.** If the mount program produces errors, you may have to add “force” to the options, “-o ro,force”. If the mount fails, you should move onto the section on Recovering Files.

```
Terminal
root@sysresccd /root % mount -t ntfs-3g /dev/sda2 /mnt/windows -o ro
root@sysresccd /root % df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           1.5G  54M  1.5G   4% /
/dev/sr0        184M  184M    0 100% /mnt/cdrom
/dev/loop0      152M  152M    0 100% /mnt/livecd
udev            10M   216K  9.8M   3% /dev
tmpfs           1.5G  4.6M  1.5G   1% /lib/firmware
tmpfs           1.5G    0  1.5G   0% /usr/portage
//slug.ceca.utc.edu/mward
      38G   25G   12G  69% /mnt/smb
mward@slug.ceca.utc.edu:/home/mward
/dev/sda2       100G    0 1000G   0% /mnt/ssh
/dev/sda2       245G   63G  183G  26% /mnt/windows
root@sysresccd /root %
```

In the above example we have a Windows partition mounted at “/mnt/windows”, a Windows server share mounted at “/mnt/smb”, and a ssh filesystem mounted at “/mnt/ssh”.

You can now copy files from the Windows partition to your remote file system using the standard “cp” command. Make sure to include “-r” if you’re copying directories.

```
Terminal
root@sysresccd /root % cd /mnt/windows
root@sysresccd /mnt/windows % ls
BOOTSECT.BAK  Documents and Settings  Program Files  User  config.sys
bootmgr       hibernfil.sys           System Volume Information  autoexec.bat  pagefile.sys
root@sysresccd /mnt/windows % mkdir /mnt/smb/recovery
root@sysresccd /mnt/windows % cp -r Documents\ and\ Settings /mnt/smb/recovery
root@sysresccd /mnt/windows % cd Documents\ and\ Settings
root@sysresccd /mnt/windows/Documents and Settings % ls
root@sysresccd /mnt/windows/Documents and Settings % cd ..
root@sysresccd /mnt/windows %
```

Removing Viruses

The open source virus scanner ClamAV is included on the SystemRescueCD. **Be warned, ClamAV can only delete infected files. It cannot disinfect them as with other AV products.** You will need to update the virus signatures using freshclam.

```
Terminal
root@sysresccd /mnt/windows % freshclam
ClamAV update process started at Tue Apr  1 13:12:50 2008
main.cvd is up to date (version: 45, sigs: 169676, f-level: 21, builder: sven)
WARNING: getfile: daily-5778.cdifff not found on remote server (IP: 64.246.134.133)
ERROR: getpatch: Can't download daily-5778.cdifff from database.clamav.net
WARNING: getfile: daily-5778.cdifff not found on remote server (IP: 216.24.174.245)
ERROR: getpatch: Can't download daily-5778.cdifff from database.clamav.net
WARNING: getfile: daily-5778.cdifff not found on remote server (IP: 208.67.80.27)
ERROR: getpatch: Can't download daily-5778.cdifff from database.clamav.net
WARNING: Incremental update failed, trying to download daily.cvd
Downloading daily.cvd [100%]
daily.cvd updated (version: 6529, sigs: 71786, f-level: 26, builder: arnaud)
Database updated (241462 signatures) from database.clamav.net (IP: 155.98.64.86)
root@sysresccd /mnt/windows %
```

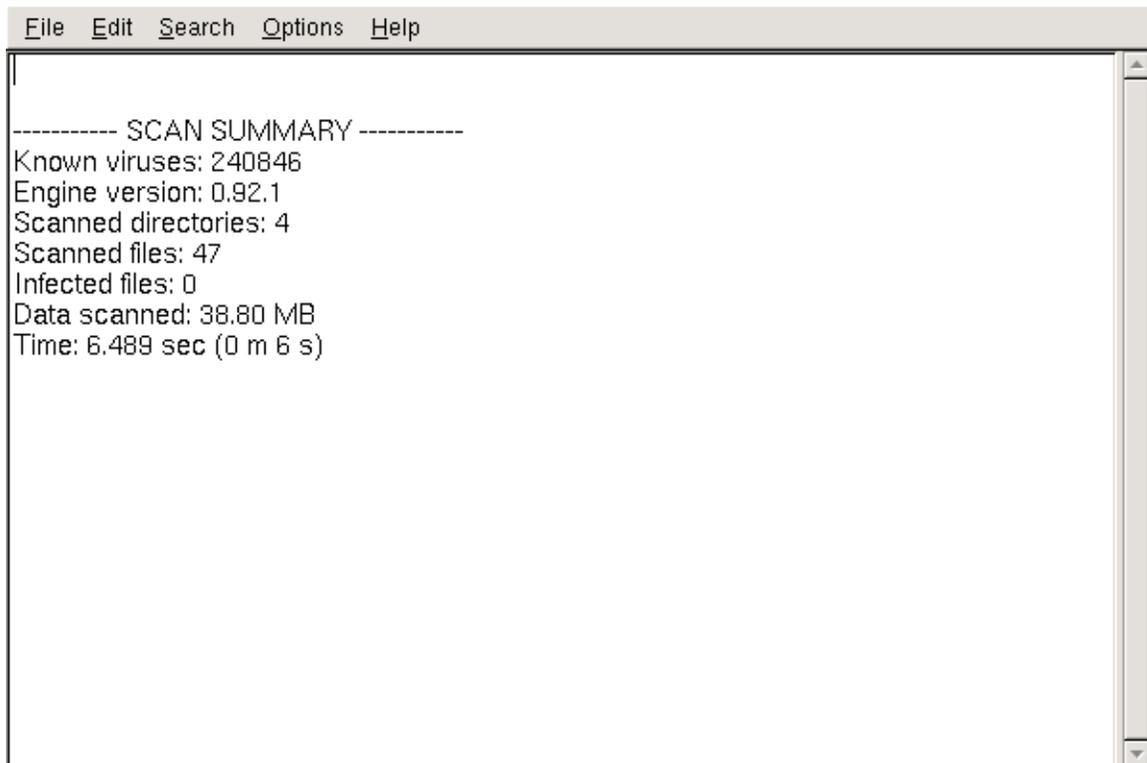
Once the definitions are up to date, you want to scan your mounted Windows partition. You will have to mount the Windows partition with “write enabled” by leaving off the “-o ro” as mentioned above. You can “remount” the filesystem by using “umount /mnt/windows” followed by “mount -t ntfs-3g /dev/sda2 /mnt/windows” . Make sure to use the correct “sda” partition. I strongly suggest that you have clamscan only report infected files.

A terminal window titled "Terminal" with standard window controls (minimize, maximize, close, back, forward) in the title bar. The terminal shows a command prompt at root@sysresccd /root. The command executed is clamscan -ir -l virus.txt /mnt/windows/Windows/System32. The output consists of several warning messages from LibClamAV: a warning about the virus database being older than 7 days, a warning to update it, and two warnings about unknown subsystems in PE headers (0x10). The terminal ends with a blank line.

```
root@sysresccd /root % clamscan -ir -l virus.txt /mnt/windows/Windows/System32
LibClamAV Warning: *****
LibClamAV Warning: *** The virus database is older than 7 days! ***
LibClamAV Warning: *** Please update it as soon as possible. ***
LibClamAV Warning: *****
LibClamAV Warning: Unknown subsystem in PE header (0x10)
LibClamAV Warning: Unknown subsystem in PE header (0x10)
□
```

In the above example, “-ir” stands for “report infected files only” and “recurse into subdirectories.” A report is created (virus.txt) via the log option of “-l”. The above example scans the System32 directory within the Windows directory and prints out infected file names. You can add the “—delete” switch to automatically delete infected files, but that may render your system inoperable. Clamscan may take hours to completely scan your PC.

Here is the report, opened by Leafpad, containing the results of the clamscan.

A screenshot of a terminal window with a menu bar containing 'File', 'Edit', 'Search', 'Options', and 'Help'. The terminal displays a scan summary with the following text:

```
----- SCAN SUMMARY -----  
Known viruses: 240846  
Engine version: 0.92.1  
Scanned directories: 4  
Scanned files: 47  
Infected files: 0  
Data scanned: 38.80 MB  
Time: 6.489 sec (0 m 6 s)
```

You can remove any infected file manually with the “rm” command. To delete a directory, use “rm -rf /directoryname”. When you delete something in Linux, it’s hard to recover it, so be sure.

Recovering Files

SystemRescueCD includes one of the best recovery tools, testdisk. These directions assume that your PC won’t boot due to disk errors, or that some other drive failure has occurred. If your drive has suffered a serious hardware failure, such as those that involve read heads or motors, than testdisk will not be able to help you. In short, if your drive “clicks” or the motor won’t spin up you’ll need the help of a professional recovery service.

You’ll need to know the device (here sda) of your failed drive.

```
Terminal
root@sysresccd /root % testdisk /dev/sda
```

You'll have to select your drive.

```
Terminal
TestDisk 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 500 GB / 465 GiB - ATA ST3500630AS

[Proceed] [ Quit ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

You'll then have to select the partition type, Intel is the most common.

```
Terminal
TestDisk 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 500 GB / 465 GiB - ATA ST3500630AS

Please select the partition table type, press Enter when done.
[Intel ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Mac ] Apple partition map
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return] Return to disk selection

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

Testdisk will then analyze the disk looking for lost partitions. The analysis may take a long time.

```
Terminal
TestDisk 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 500 GB / 465 GiB - CHS 60801 255 63

[Analyse ] Analyse current partition structure and search for lost partitions
[Advanced] Filesystem Utils
[Geometry] Change disk geometry
[Options ] Modify options
[MBR Code] Write TestDisk MBR code to first sector
[Delete ] Delete all data in the partition table
[Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

You should then have a list of partitions. Select the correct one and do a “List Files.”

```
Terminal
TestDisk 6.8, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 500 GB / 465 GiB - CHS 60802 255 63
Partition      Start      End      Size in sectors
+ FAT16 >32M   0 1 1     5 254 63   96327 [DellUtility]
P FAT32 LBA    6 0 1   4183 254 63 67119570 [NO NAME]
```

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
FAT32, 34 GB / 32 GiB

You should then see a list of files and directories, which you can then copy to your network mounted partition.

Wiping Drives and Files

SystemRescueCD contains two applications for erasing files, directories, and partitions. “Wipe” and “Shred” are both useful, but I prefer shred. The command “shred -f -n5 /dev/sda” will write random data to the entire hard drive 5 times.