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 warrantees are implied or given.

Help

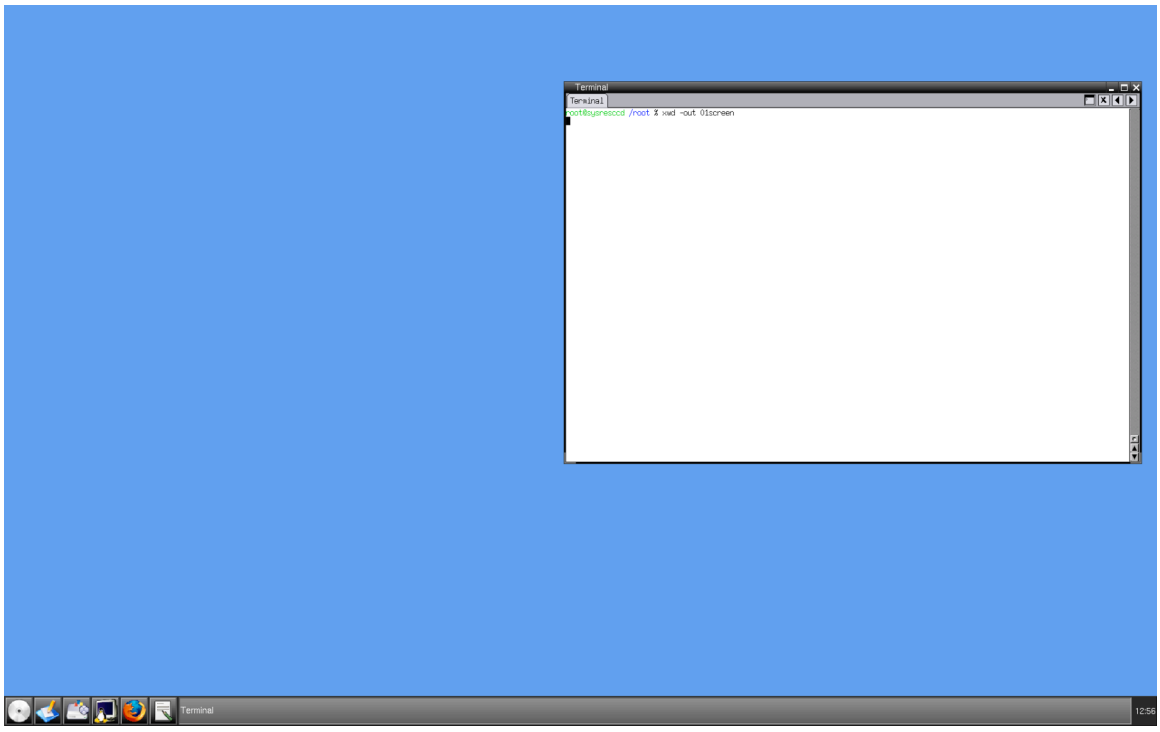
The above link to the SystemRescueCD page is a good resource, as is a quick search of Google. You can also use the "man" function within a shell. For example, "man mount.cifs" would bring up a manual page on the mounting of CIFS (Windows shares).

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

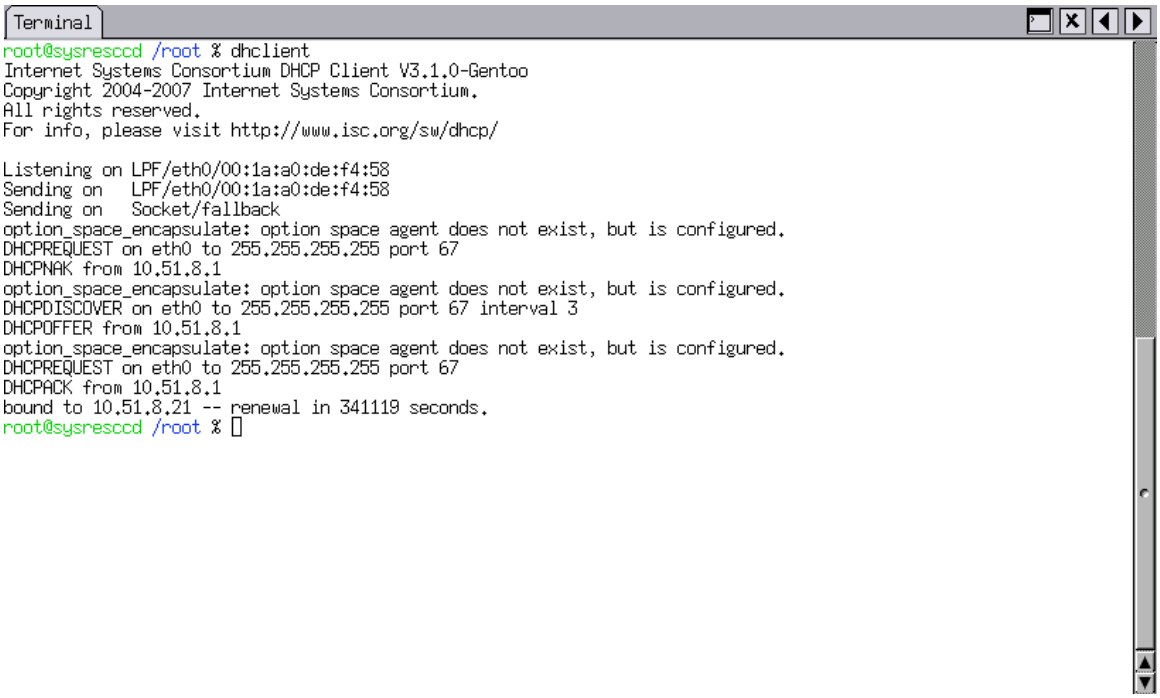
like:



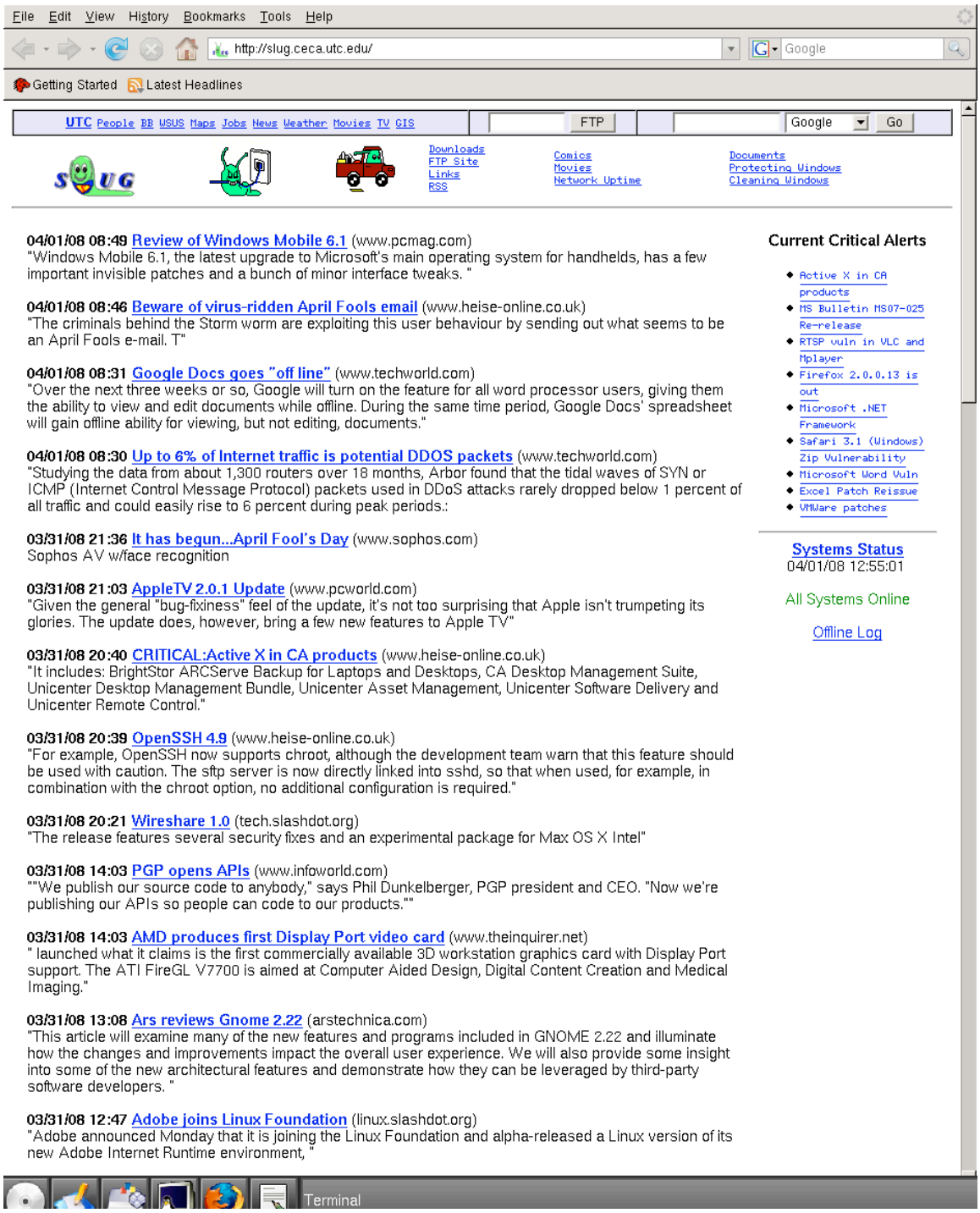
The major tools are presented as icons at the lower left of the screen. For the rest of this guide you will need an open zsh session. Click on the "penguin with a TV" icon.

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"

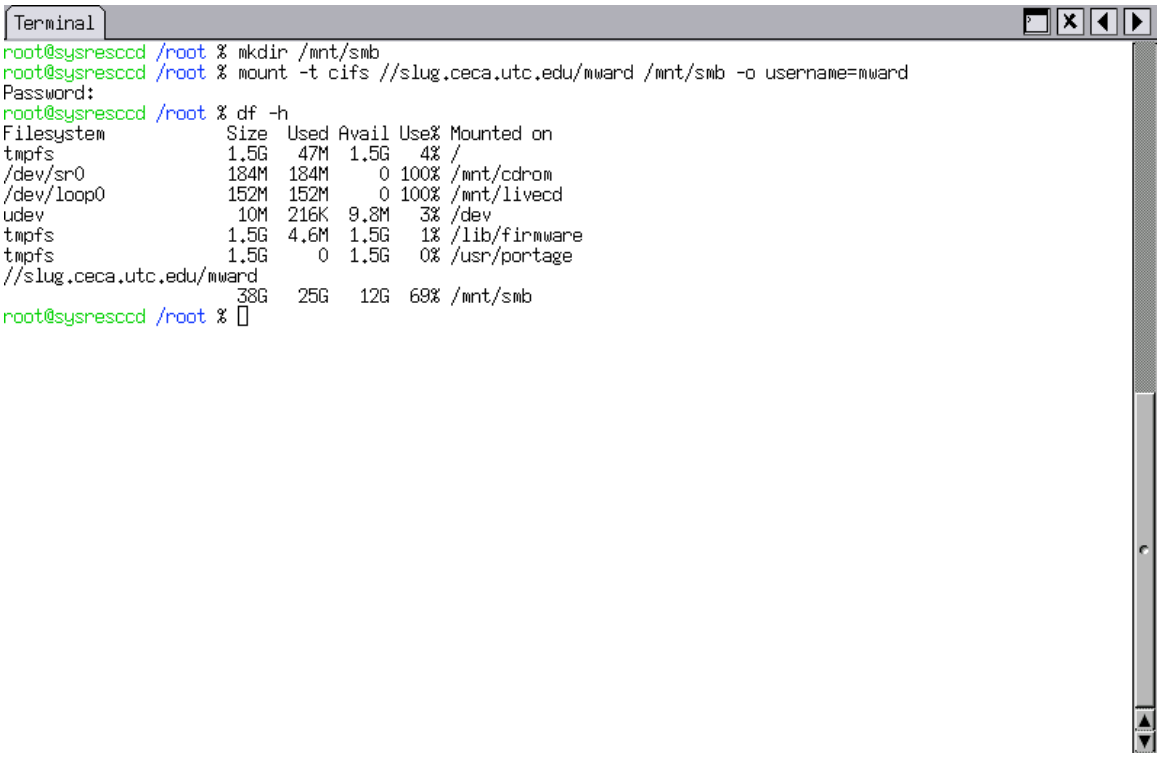


You need to test your network connection, and since you'll probably need a browser at some time, launch Firefox via its icon.

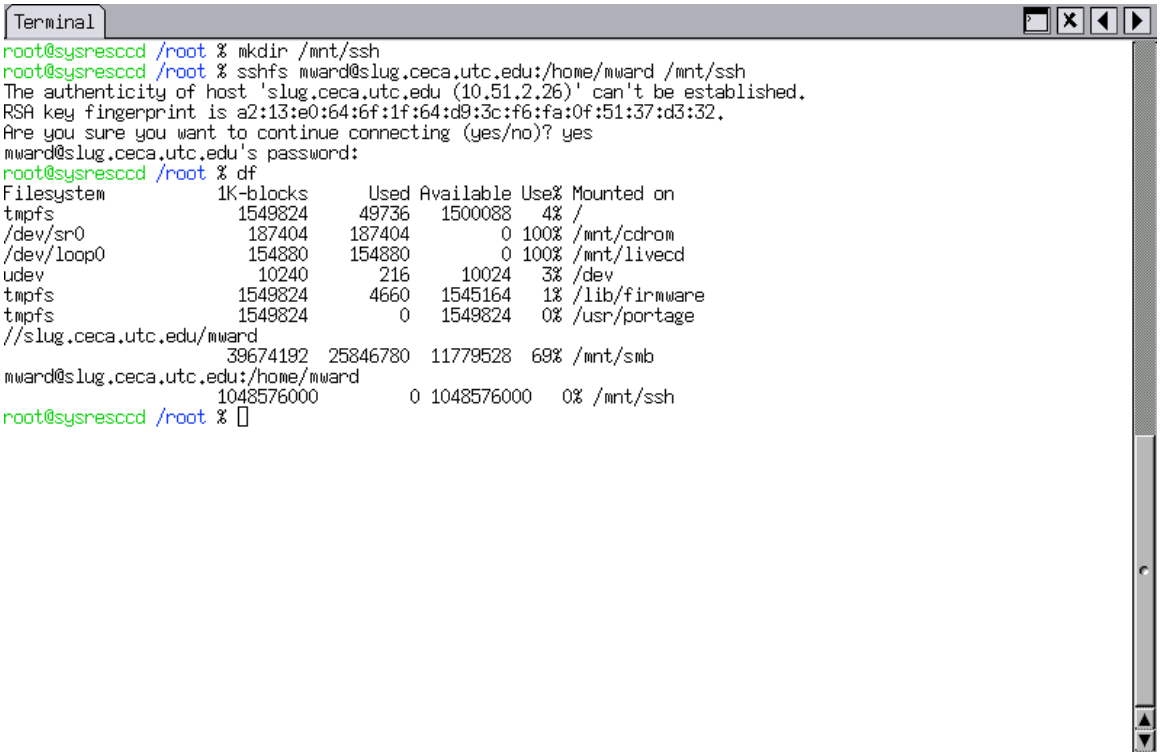


Connecting to a Networked Server

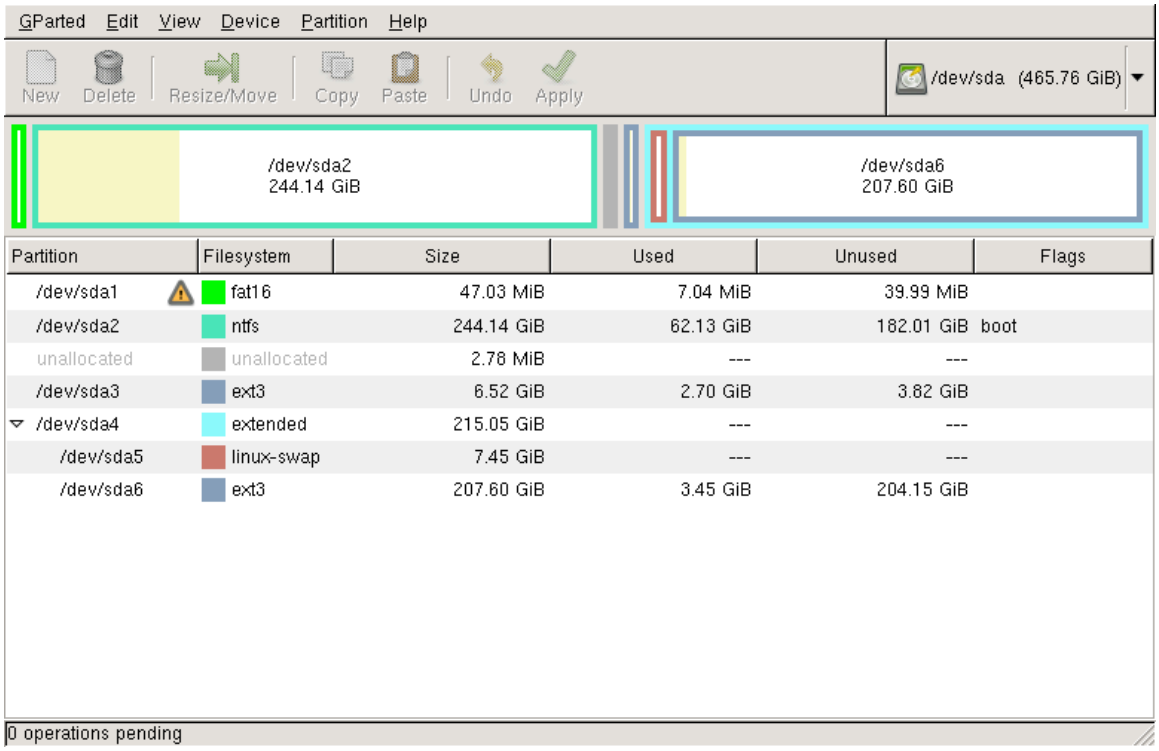
Now we've got to copy the data to a networked server which can be a ftp server, a Windows server, or via ssh to a Linux/BSD box. For the first example, we'll attach to a Windows share using mount.cifs. As demonstrated in the following image, you need to create a mount point and then attach the server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



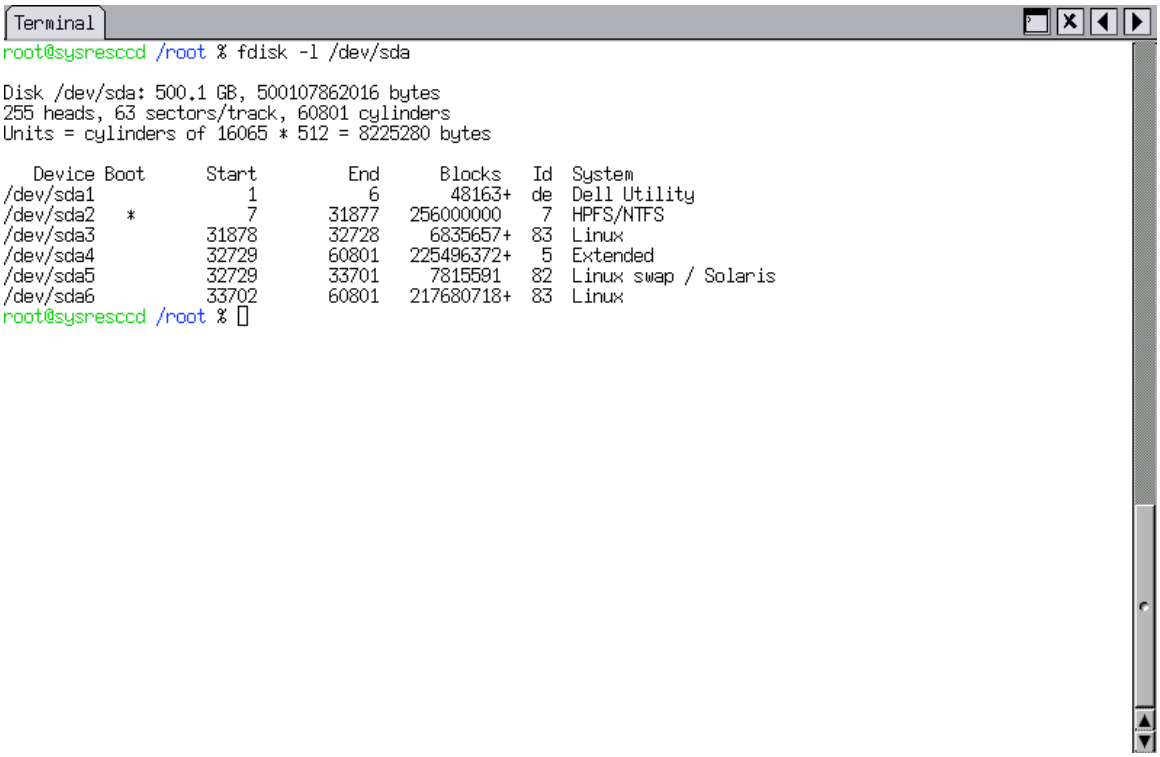
The "df –h" command lists the mounted file systems. You can also mount a remote system using ssh.



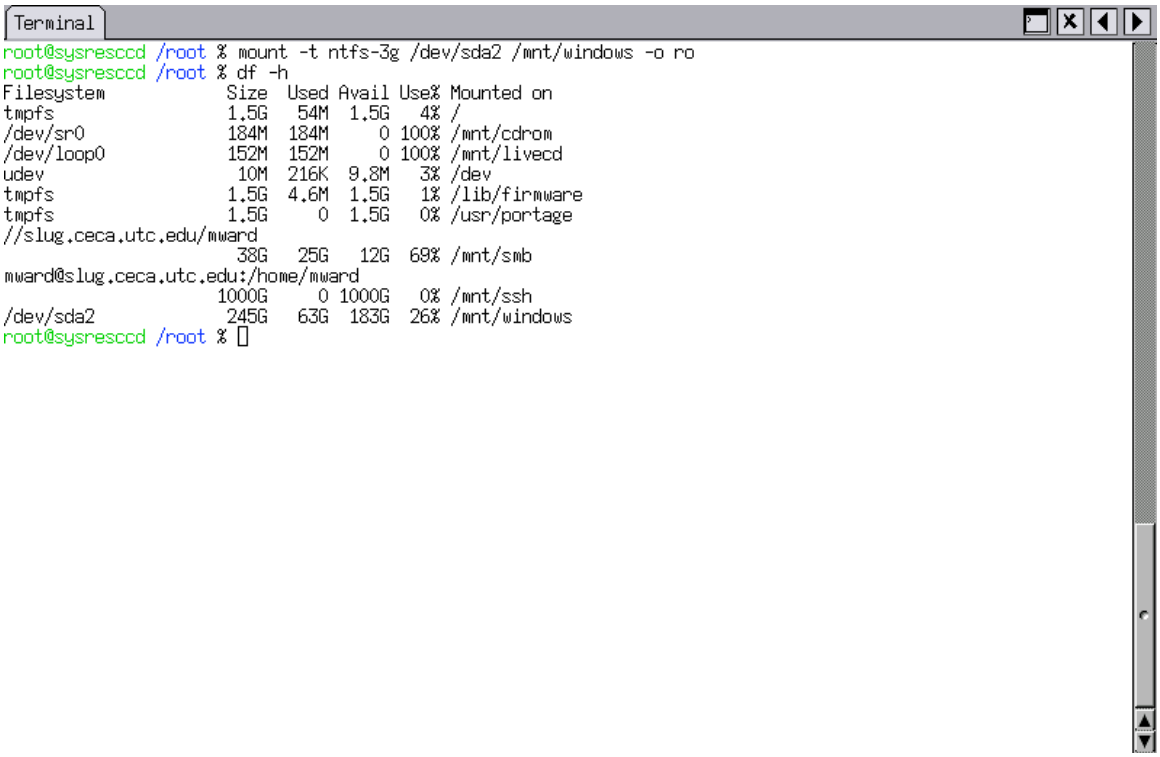
Now that we have a location for backup, we have to mount the filesystem on the hard drive. The easiest way to find out what partitions are on a disk is to use Gparted (the disk icon).



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.

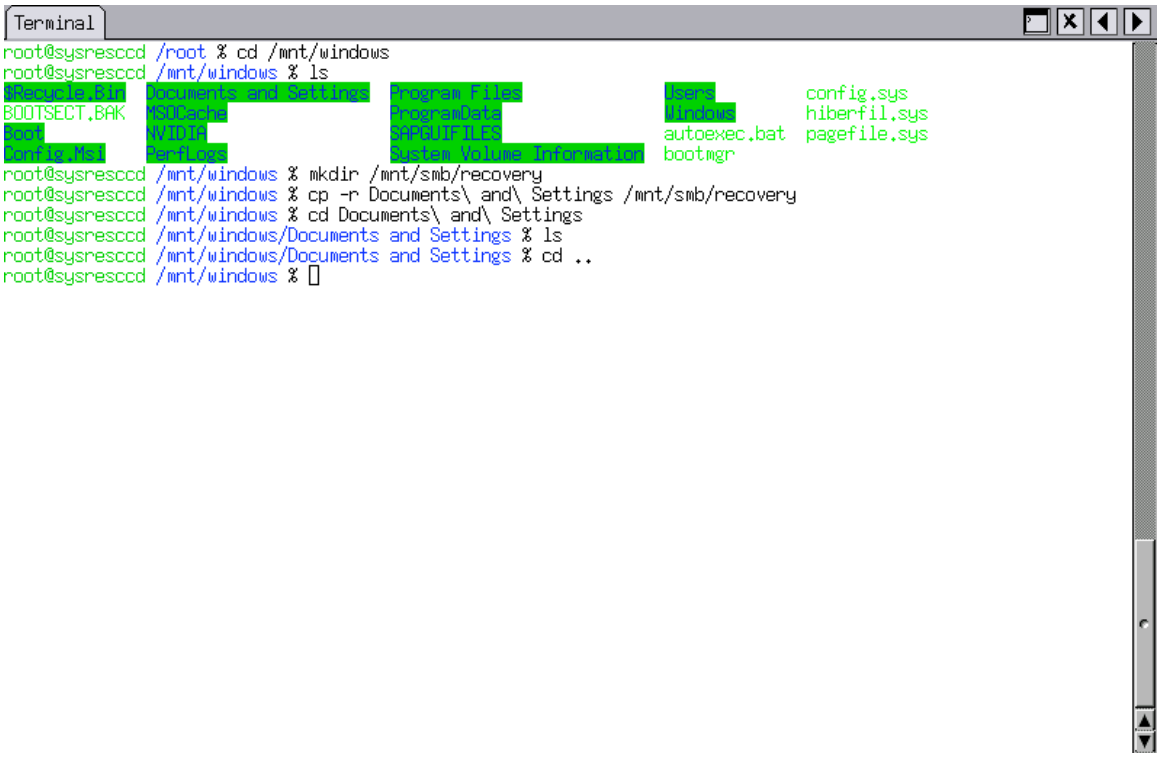


We want to copy from the Windows partition, so we have to mount it. **Note the use of "ro" as an option. This is read-only and prevents any changes to the Windows partition. If you want to change the Windows files, such as when doing virus removal, you would leave off the "-o ro".** If the mount program 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.



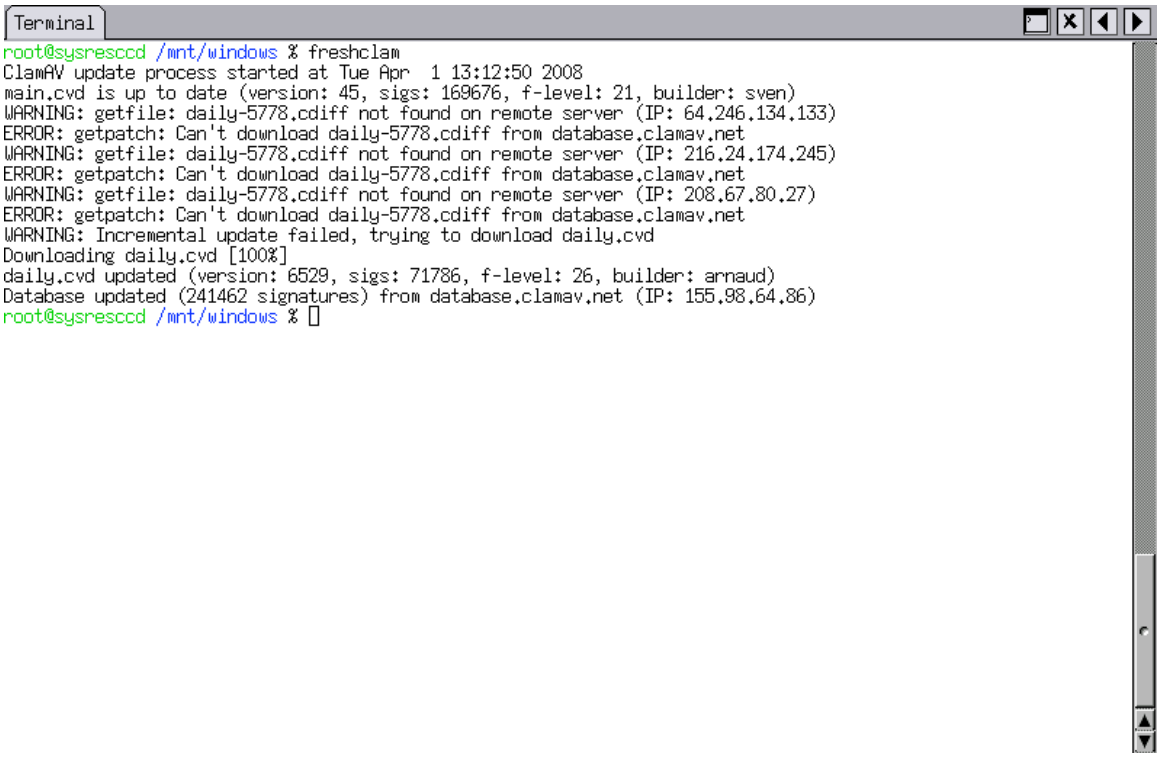
In the above example we have a Windows partition mounted at “/mnt/windows”, a Windows server share mounted at “/mnt/smb”, and a ssh filesystem mounted at “/mnt/ssh”.

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.

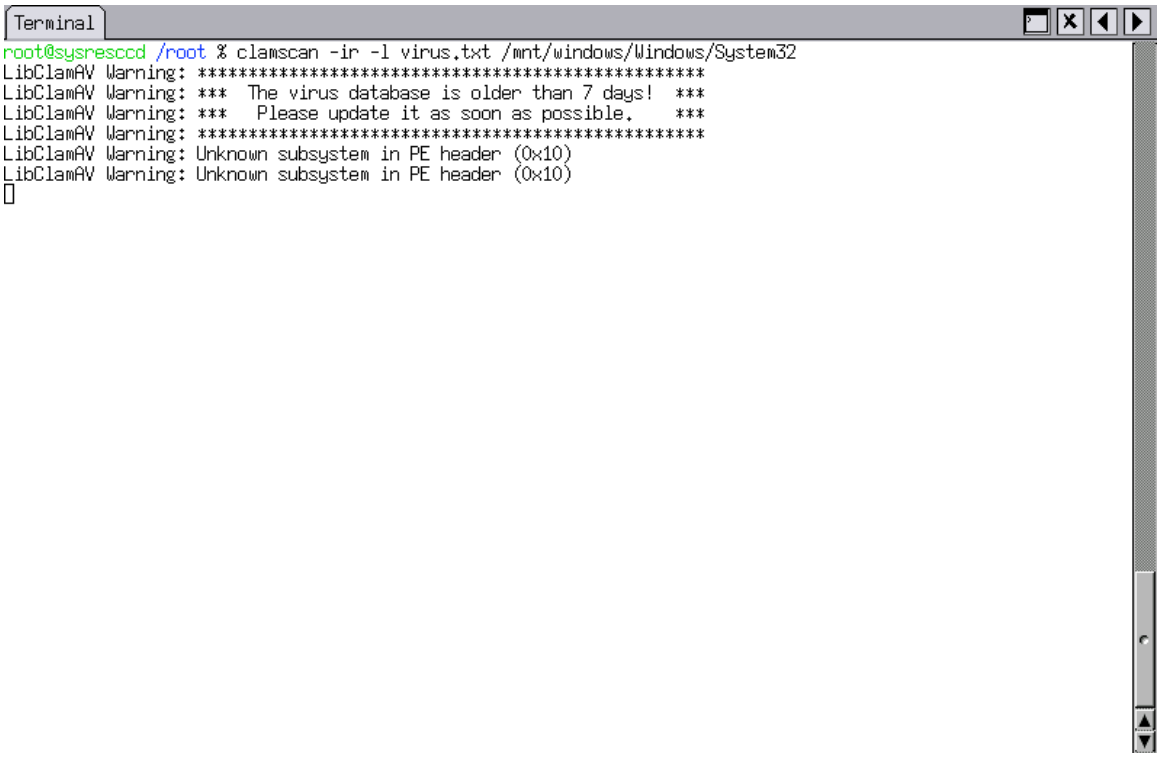


Removing Viruses

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.

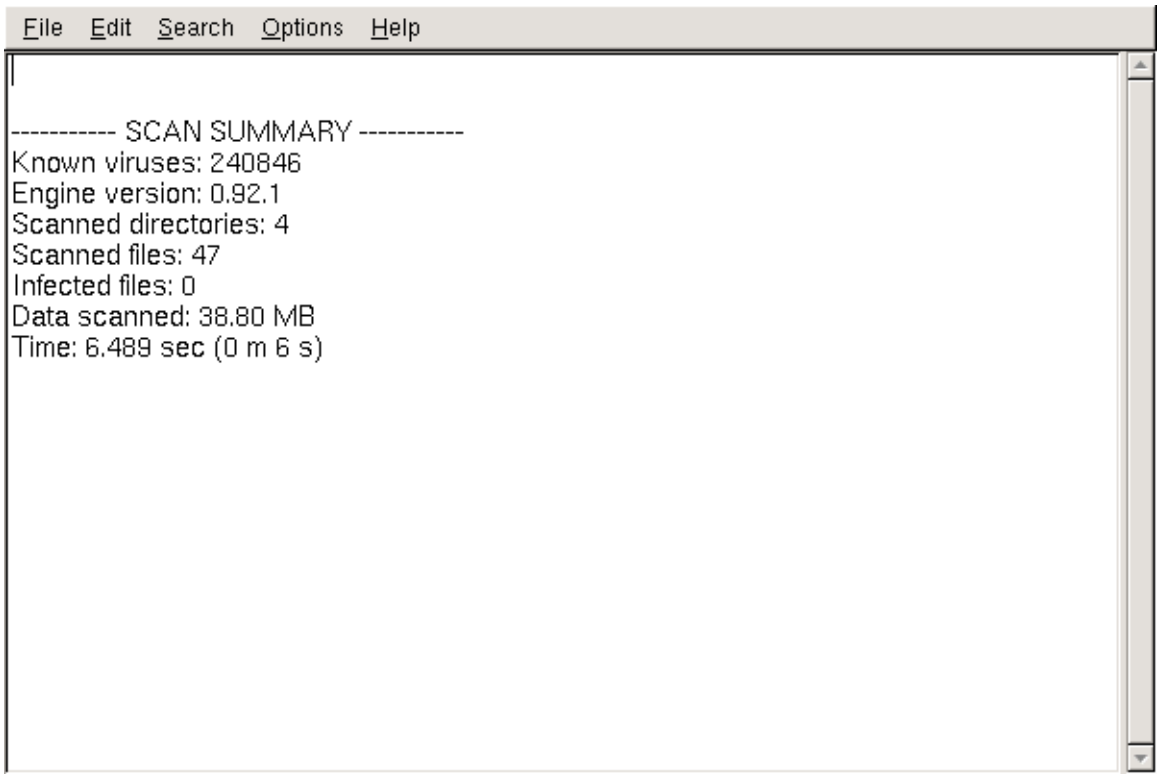


Once the definitions are up to date, you want to scan your mounted Windows partition. You will have to mount the Windows partition with “write enabled” by leaving off the “-o ro” as mentioned above. You can “remount” the filesystem by using “umount /mnt/windows” followed by “mount –t ntfs-3g /dev/sda2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



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.

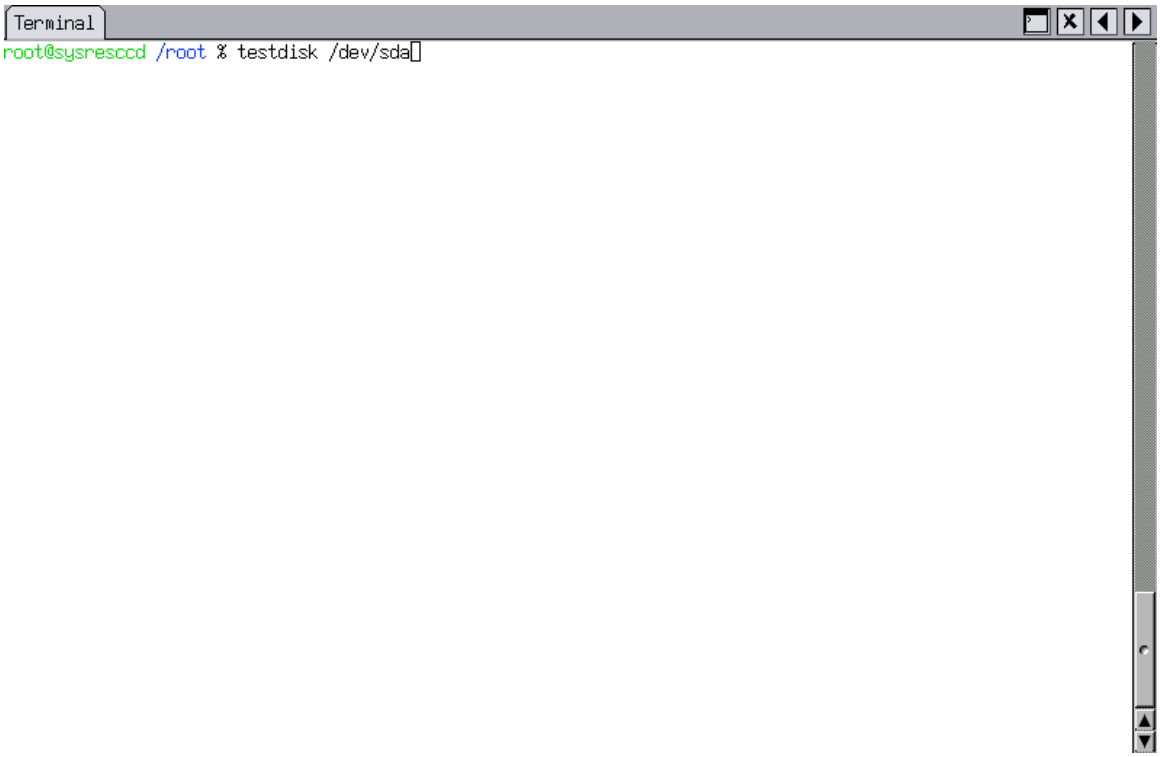


You can remove any infected file manually with the "rm" command. To delete a directory, use "rm –rf /directoryname". When you delete something in Linux, it's hard to recover it, so be sure.

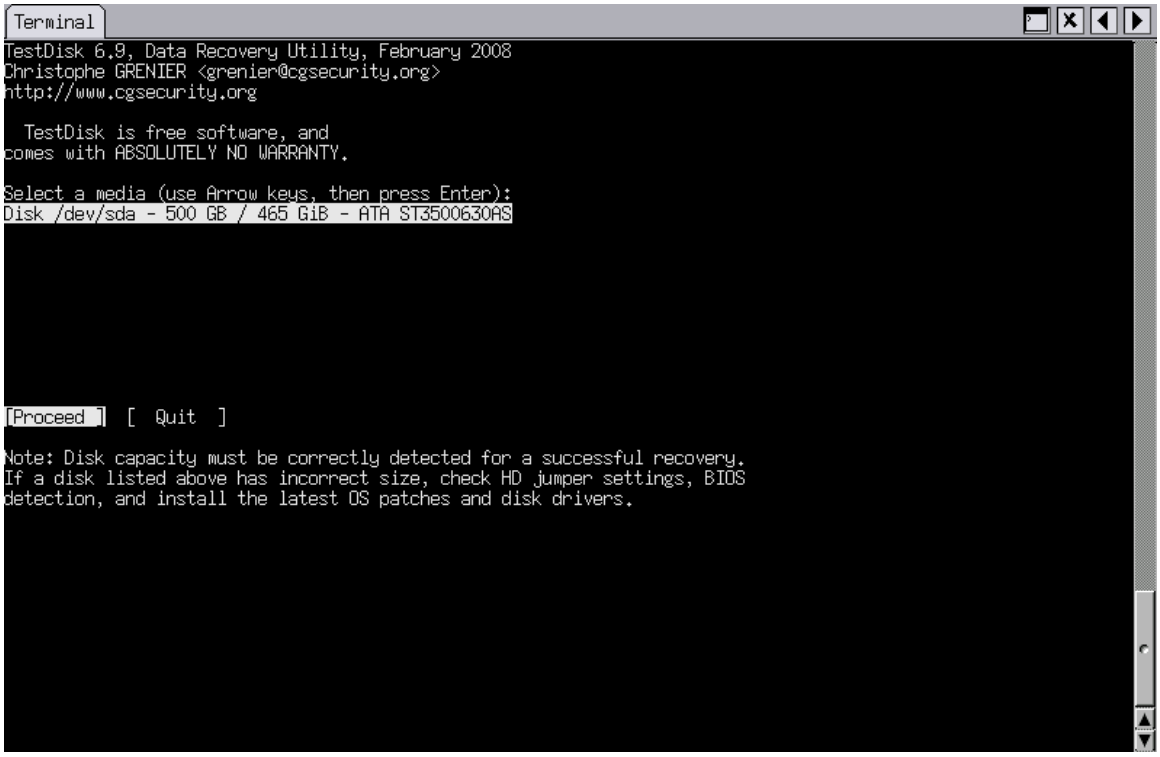
Recovering Files

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.

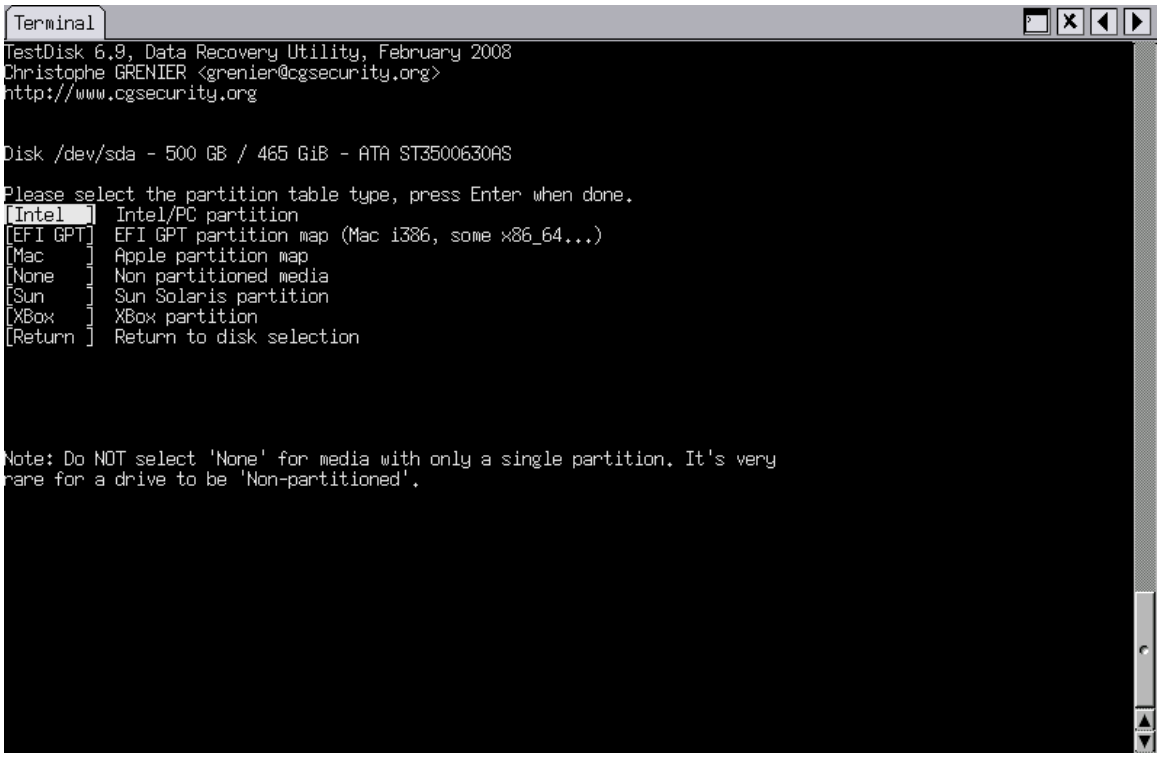
You'll need to know the device (here sda) of your failed drive.



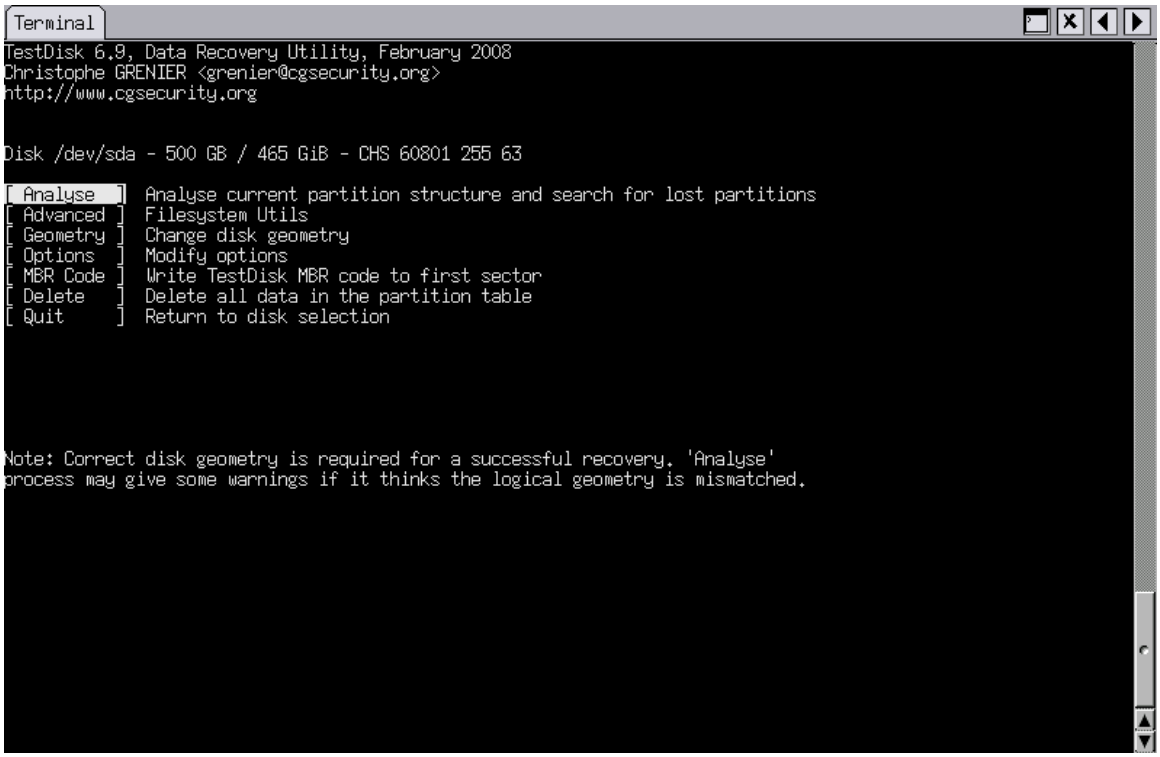
You'll have to select your drive.



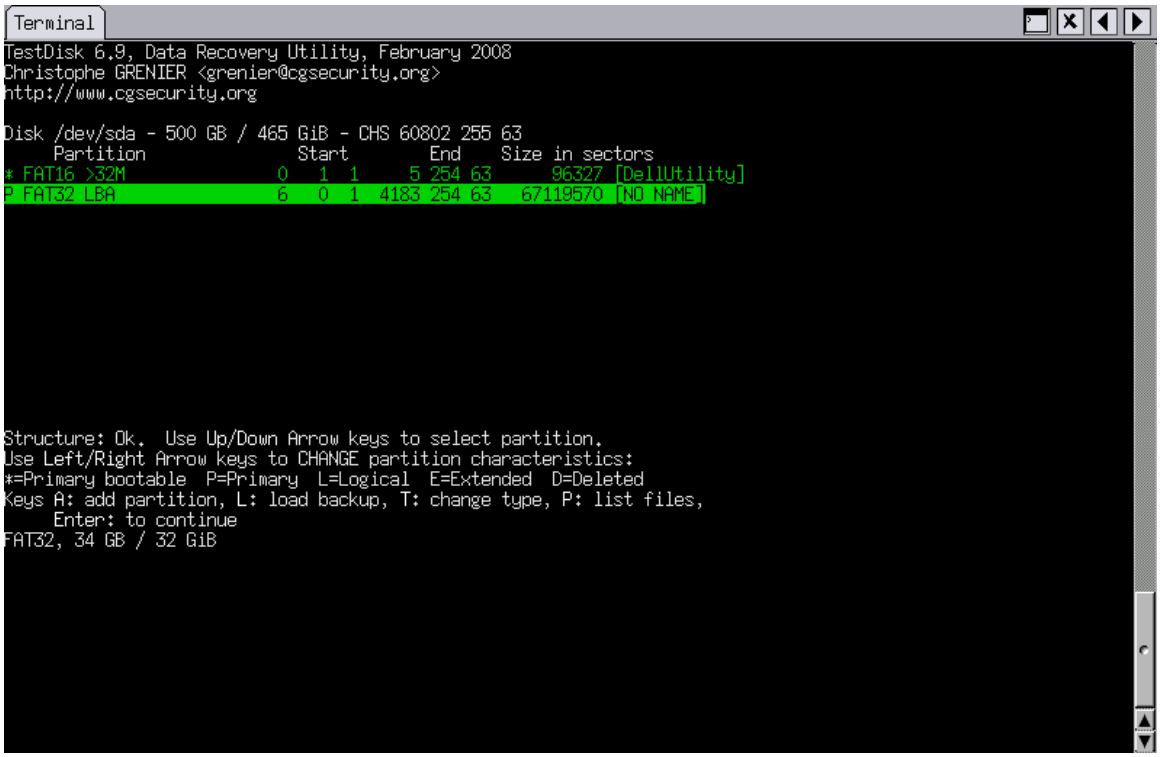
You'll then have to select the partition type, Intel is the most common.



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



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



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.