

## Recovering an XP System that Won't Boot from the Hard Drive

These instructions are based on the corrected version of the very useful instructions written by Charlie White. Unfortunately there were still errors in the corrected version, which I have tried to eliminate, without introducing any new ones. I've also put in a lot of screen shots which may help the less experienced user. It's always reassuring to see that the screenshots are similar to what you're seeing.

I encountered a need to do a manual restore when I got an "lsass.exe" error upon booting, though there are many other situations where you may find the need to do a manual restore, for example when you get a BSOD (blue screen of death) when you try to boot.

*Many people incorrectly claim that the lsass.exe problem is a virus. There is a virus by the same name, which is confusing, but in many cases the error is because of corruption of system files. I've also seen incorrect claims that this error indicates an overheating CPU, bad RAM, etc. If the machine continually reboots, without any intervention by the user, it is possibly a virus. If you get pop-up screen indicating an lsass.exe problem when you're at the screen where you would normally click on the user name, and then when you click on the pop-up and the machine reboots, then it's most likely not a virus.*

*Whatever you do, don't delete the lsass.exe file from C:\windows\system32.*

Microsoft also has a version of these instructions at <http://support.microsoft.com/?kbid=307545>. Unfortunately, many users automatically assume that it's hopeless, and they reformat their drive and reinstall Windows, without making use of the tools that Microsoft and other providers supply for recovery.

It's far faster to do a recovery than to reformat a hard drive and reinstall Windows plus all your programs, and all your data (assuming you even have all the CDs for your programs, and that you can recover your data).

### Overview

The basic process is simple. You need to copy five older, undamaged, configuration files from the System Volume Information folder into the c:\windows\system32\config folder. Windows XP automatically saves backups of these configuration files for this purpose. The "manual system restore" procedure allows you to recover these files even when your system won't boot from the hard disk.

When the system is able to boot from the hard drive, even into Safe Mode, recovery is much easier. However even when the system won't boot from the hard drive, it is often possible to boot from a CD or from floppies, and copy the undamaged configuration files into the proper Windows folder.

These instructions are long only because they assume that the user is not experienced with DOS. The procedure is actually simple and fast. Print out these instructions to make it easier.

### Which Files will You Restore?

The five files of interest have the following names:

- system
- software
- sam
- security
- default

These files don't have extensions. They are located in the c:\windows\system32\config folder.

## Steps you will be Taking

1. Boot the system, with recovery CD or floppy diskettes, to C: prompt (also called a DOS prompt).
2. Save copies of the existing, presumably damaged, versions of the configuration files, by renaming them with the .old extension.
3. Copy the repair version of the configuration files into the \windows\system32\config folder, from the c:\windows\repair folder, over-writing the damaged files.
4. Create a folder under the Windows Folder called tmp (c:\windows\tmp) to use later.
5. Boot the System into Windows from the hard drive.
6. Retrieve a previous version of the five files from the System Volume Information Folder and save these files in c:\windows\tmp.
7. Boot the System with recovery CD or floppy diskettes.
8. Replace the repair version of the five files with the version recovered from the System Volume Information Folder (that you stored in c:\windows\tmp). Reboot
9. Plan for the future!

The reason for all this rigmarole is that when you boot from a recovery CD or floppies, you're very limited as to the folders on the C: drive that you can access. You can't go to the System Volume Information folder and retrieve the good configuration files (that Windows XP automatically saves).

### **Alternate Method: Attaching the drive from the broken machine to a working machine, as a secondary drive.**

Another way to fix this problem may be to put the hard drive from the machine that won't boot onto another system as a secondary drive, and then copy the five configuration files from the "x:\System Volume Information\\_restore {15A.....}\RP..snapshot" folder into the "x:\windows\system\config" folder (x represents whatever drive letter the secondary drive is assigned by the working system). I did stick my laptop drive into a USB drive enclosure, and I attached it to another machine, and did a virus scan because I first thought that I had a virus. I could see the System Volume Information folder, and could get the config files out, and could copy files into the folder.

If you have a damaged SAM file (Security Accounts Manager), and can't into the recovery console because of administrator password problems, this may be a way around that. The lsass.exe problem, when it's not the virus by the same name, appears to be directly related to a corrupted SAM file.

Follow the same precaution of saving the current version of the five files with a .old extension, so you can at least get back to where you were if it doesn't work.

I think that it's safer to connect the drive as a USB or 1394 drive by using a USB or 1394 enclosure (available for both laptop and desktop drives, in both SATA and regular PATA interfaces) rather than plugging it in as a slave drive on the IDE controller. Plug it in after the primary drive has booted.

It's probably a good idea to do a virus scan on the problem drive as soon as you attach it to a working machine, though the boot block won't be scanned.

You can also use the USB attached drive to recover your files, in case you have to reformat the hard drive later.

So let's get started.

## Boot the System with recovery CD or floppy diskettes

Boot the system with the recovery CD or with floppies (six). If you don't have the CD you can download the floppy images from Microsoft's web site at <http://support.microsoft.com/default.aspx?scid=kb;en-us;310994> (choose the proper version of XP, with or without SP2). A notebook can be booted with a USB floppy drive (these cost about \$20 from Amazon or other e-tailers, though you'll probably pay close to \$40 at a brick and mortar store). I didn't have a recovery CD so I had to download and boot from the floppy images, which is somewhat of a pain, but I had no choice.



The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL <http://support.microsoft.com/default.aspx?scid=kb;en-us;310994>. The page title is "How to obtain Windows XP Setup boot disks - Mozilla Firefox". The browser's menu bar includes File, Edit, View, Go, Bookmarks, Tools, and Help. The address bar has a search icon and a "Go" button. Below the address bar, there are several icons for "Latest Headlines", "Groups", "Bicycles", "W [stop]", "Getting Started", and "javascript:doHandoff...". The main content area has a blue header "Help and Support" with sub-links for "Help and Support Home", "Select a Product", and "Search Knowledge Base". The article title "How to obtain Windows XP Setup boot disks" is displayed in bold. Below the title, there is a link "View products that this article applies to." and a note "This article was previously published under Q310994". A section titled "On This Page" lists several links: "SUMMARY", "MORE INFORMATION", "Create the Setup disks", "Use the Setup disks", "Download the Setup disk program file", "Windows XP original release", "Windows XP Service Pack 1 (SP1)", and "Windows XP Service Pack 2 (SP2)". To the right of this list, a box contains the following information: "Article ID : 310994", "Last Review : October 24, 2006", and "Revision : 6.0". A "SUMMARY" section follows, stating that Microsoft Windows XP Setup boot disks are available only by download from Microsoft and are intended for computers that cannot use a bootable CD-ROM. It also notes that if a computer supports booting from a CD-ROM or network-based installation, those methods are recommended instead.

*You may have to modify the boot sequence in the CMOS setup on your computer to try to boot from the CD-ROM or floppy drive before the hard drive. Usually you enter the CMOS setup by pressing DEL, F2 or F10 at boot time (usually there will be a brief display of the method for entering setup when you first power up). Look for the section that lets you specify the boot order. You don't want the hard drive to be the first boot device; you want the CD-ROM drive or floppy drive to be the first boot device. Normally this is the default configuration, but sometimes to speed up the boot process the hard drive will be designated as the first boot device.*

You'll be prompted with several choices. You want to choose "R" for recovery. The screen will look something like this:

```
Windows XP Professional Setup
-----
Welcome to Setup.

This portion of the Setup program prepares Microsoft(R)
Windows(R) XP to run on your computer.

• To set up Windows XP now, press ENTER.
• To repair a Windows XP installation using
  Recovery Console, press R.
• To quit Setup without installing Windows XP, press F3.

ENTER=Continue  R=Repair  F3=Quit
```

This will bring up the Recovery Console.

```
Microsoft Windows XP(TM) Recovery Console.

The Recovery Console provides system repair and recovery
functionality.

Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS

Which Windows installation would you like to log onto
(To cancel, press ENTER)? █
```

For most users there will be only one choice, 1: C:\WINDOWS, So press 1 and then ENTER.

```
Microsoft Windows XP(TM) Recovery Console.

The Recovery Console provides system repair and recovery
functionality.

Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS

Which Windows installation would you like to log onto
(To cancel, press ENTER)? █
Type the Administrator password: █
```

You will be prompted for the Administrator password. Uh oh! This is where things can get dicey, since the password file, also known as the "Security Accounts Manager" (SAM) may actually be what's damaged, when you get the lsass.exe error. Try entering the password, if you know what it is. Maybe there isn't an administrator password, so try just pressing ENTER. In my case, I knew the password, but the recovery console said that it was no good, so presumably the SAM file was damaged. You get three chances to enter the password before you have to reboot the recovery console (not an issue if you have a CD, but very time-consuming if you're booting from floppy diskettes).

If you know the administrator password, and it actually works, the next screen will look like this:

```
Microsoft Windows XP(TM) Recovery Console.  
  
The Recovery Console provides system repair and recovery  
functionality.  
  
Type EXIT to quit the Recovery Console and restart the computer  
  
1: C:\WINDOWS  
  
Which Windows installation would you like to log onto  
(To cancel, press ENTER)? █  
Type the Administrator password: *****  
C:\WINDOWS> █
```

## Getting Around the Administrator Password

There are some tools available that let you recover a forgotten Administrator password, or put in a new password without knowing the old one, or eliminate the password completely. These tools may get you around a damaged SAM file. You should burn a Hiren's Boot CD, a collection of very valuable tools, which includes several password tools. See <http://www.hiren.info/pages/bootcd> for information. Also see <http://tinyurl.com/c9jr> which has more password tools. You may need to try a couple of different tools.

I was about to give up until I saw an option for disabling the password for Windows recovery. Somehow that worked, and when I then booted from the floppies it didn't ask me for a password anymore. Once you copy the repair files into the c:\windows\system32\config folder then there usually is no longer a password needed. That got me the c: prompt on recovery. Once I restored the old configuration files, my old administrator password was okay.

I think that dealing with the Administrator password problem was the most difficult part of recovery. You have to download password tools on another computer, and burn the bootable ISO image to a CD, which boots your system into Linux with a utility to work with the passwords on the hard drive. It's a process that a geek can do, but it's non-trivial, often non-intuitive, and often cryptic.

Be patient, and persistent. You can probably at least set the administrator password to nothing, and then you just press <ENTER> when the recovery console asks for it.

## Batch Files Can Make this Procedure Easier

If you have a floppy drive on the broken system, as well as on another system (presumably you're reading these instructions on another system), you can save yourself some time by using Notepad to create some text files that you run in batch mode, rather than typing in all the commands by hand (a USB floppy drive is fine). If not, skip this section. Note that the recovery console doesn't let you run ".bat" files, but you can use the "batch" command on a ".txt" file. I had never heard of this command, but it's unique to the recovery console. Microsoft's description is as follows:

### **batch** *inputfile* [*outputfile*]

Use this command to run commands that are specified in a text file. In the command syntax, *inputfile* specifies the text file that contains the list of commands to be run, and *outputfile* specifies the file that contains the output of the specified commands. If you do not specify an output file, the output appears on the screen.

Using Notepad (not Word, not Wordpad, not WordPerfect, etc.) create four text files (you can cut and paste from this document, using the "Select" tool in Adobe Reader).

### **Batch File 1**

```
ren c:\windows\system32\config\system c:\windows\system32\config\system.old
ren c:\windows\system32\config\sam c:\windows\system32\config\sam.old
ren c:\windows\system32\config\security c:\windows\system32\config\security.old
ren c:\windows\system32\config\default c:\windows\system32\config\default.old
ren c:\windows\system32\config\software c:\windows\system32\config\software.old
```

Save this as "renconfl" (which stands for "rename configuration files"). Notepad defaults to a .txt extension so you don't have to type .txt at the end.

### **Batch File 2**

```
copy c:\windows\repair\system c:\windows\system32\config\system
copy c:\windows\repair\software c:\windows\system32\config\software
copy c:\windows\repair\sam c:\windows\system32\config\sam
copy c:\windows\repair\security c:\windows\system32\config\security
copy c:\windows\repair\default c:\windows\system32\config\default
md c:\windows\tmp
```

Save this as "copyrepr" (which stands for "copy repair files")

### **Batch File 3**

```
del c:\windows\system32\config\sam
del c:\windows\system32\config\security
del c:\windows\system32\config\software
del c:\windows\system32\config\default
del c:\windows\system32\config\system
```

Save this as "delconfg" (which stands for "delete configuration files")

### **Batch File 4**

```
copy c:\windows\tmp\_REGISTRY_MACHINE_SAM c:\windows\system32\config\sam
copy c:\windows\tmp\_REGISTRY_MACHINE_SECURITY c:\windows\system32\config\security
copy c:\windows\tmp\_REGISTRY_MACHINE_SOFTWARE c:\windows\system32\config\software
copy c:\windows\tmp\_REGISTRY_MACHINE_SYSTEM c:\windows\system32\config\system
copy c:\windows\tmp\_REGISTRY_USER_DEFAULT c:\windows\system32\config\default
```

Save this as "copysnap.txt" (which stands for copy snapshot configuration files)

Once you boot into the recovery console then you need to copy these files in the c:\windows folder.

Type: "copy a:\*.txt c:\windows" which will copy the four txt files into the c:\windows folder.

*You can't automate the copying of the undamaged configuration files from the System Volume Information folder into the c:\windows\tmp folder, because the name of the sub-folder where these files are located changes. You have to do this copying manually, from within windows, but it's drag and drop.*

## The Wonderful World of DOS

Now you're about to enter the wonderful world of DOS commands. Old-timers will have no problem, but some users may be skittish about actually typing commands. Again, if you're able to create the batch files as listed above, it will make your life easier, but you'll have to have a floppy drive on both the problem machine and a good machine in order to create the batch files.

The DOS commands that you'll be using are the following:

md	Make a new directory (a directory is the same as a folder)
cd	Change directory
del	Delete a file
ren	Rename a file (doesn't make a copy of the file, just changes the name)
copy	Copy a file (leaves the original file untouched)

*Unfortunately, some of the useful DOS tools such as DOSKEY, and F3 don't work in the Recovery Console, so you're in for a lot of typing if you didn't make batch files.*

So let's get started.

## Save Copies of the Existing Versions of the Configuration files, by renaming them

If you made batch files type "batch c:\windows\renconfl.txt" which will rename the existing version of the configuration files in order to preserve them in case you need them back (if you're already at the C:\windows prompt then you can just type "batch renconfl.txt"). Otherwise, type:

```
cd c:\windows\system32\config (go to the \windows\system32\config folder)
```

Now rename the existing version of the files using the DOS rename (ren) command by typing (Note that you only type the stuff after the >):

```
C:\WINDOWS\system32\config> ren system system.old
C:\WINDOWS\system32\config> ren sam sam.old
C:\WINDOWS\system32\config> ren security security.old
C:\WINDOWS\system32\config> ren default default.old
C:\WINDOWS\system32\config> ren software software.old
C:\WINDOWS\system32\config>
```

Type dir \*.old <ENTER> and ensure that these five files have their new names. You should have five files with the .old extension.

## Copy the repair files into the \windows\system32\config folder

Since you renamed the existing config files in the previous step, you should not receive any warnings about over-writing existing files in this step.

If you're using batch files, type "batch c:\windows\copyrepr.txt" which will copy the repair versions of the configuration files into the c:\windows\system32\config folder (if you're already at the C:\windows prompt then you can just type "batch copyrepr.txt"). Otherwise:

You're still in the c:\windows\system32\config folder. If not, type "c: <ENTER>" (if somehow you're no longer in the c: drive) then type: "cd c:\windows\system32\config" Now you'll copy the repair versions of the files from the repair folder\*.

```
C:\WINDOWS\system32\config> copy c:\windows\repair\system
      1 file(s) copied.

C:\WINDOWS\system32\config> copy c:\windows\repair\software
      1 file(s) copied.

C:\WINDOWS\system32\config> copy c:\windows\repair\sam
      1 file(s) copied.

C:\WINDOWS\system32\config> copy c:\windows\repair\security
      1 file(s) copied.

C:\WINDOWS\system32\config> copy c:\windows\repair\default
      1 file (s) copied.
```

*For some reason, on my computer, the "system" file was called "system.bak".*

*\*Note that in DOS the destination defaults to the folder that you're executing these command from, and the file name will remain the same, so you don't have to type a destination folder or file name. This saves a lot of typing.*

## Create a folder under the Windows Folder called tmp

If you're using batch files, type "copyrepr.txt" file already made this folder for you. Otherwise, type:

```
md c:\windows\tmp
```

You'll use this folder later.

Type "Exit" to reboot into Windows.

## Boot the System into Windows

With those five new repair files, the system should now boot into XP. Don't panic when none of your programs are available. None of your programs will be available until you replace the five repair files with older versions of your files.

Disconnect all network connections (wired and wireless) as you're going to expose some sensitive system files for a few minutes.



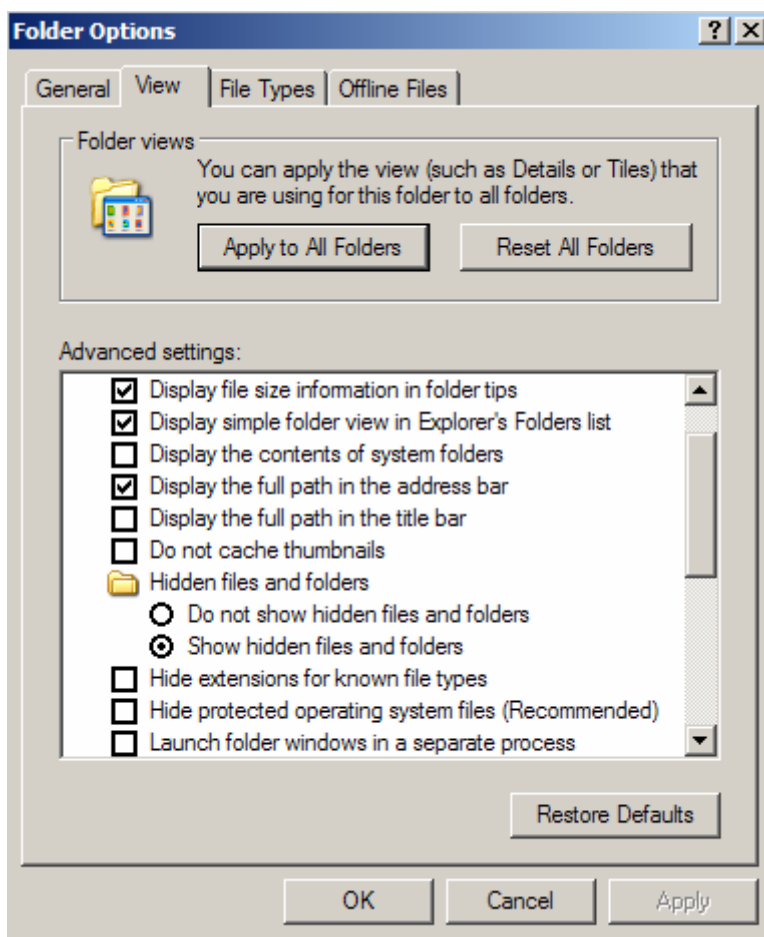
## Retrieve a previous version of the five files from the System Volume Information Folder and save them in c:\windows\tmp

*Note: All of these instructions are for XP Pro with SP2. There may be slight differences with XP Home. See <http://support.microsoft.com/kb/309531/> for Microsoft's instructions regarding gaining access to this folder.*


Double-click on My Computer

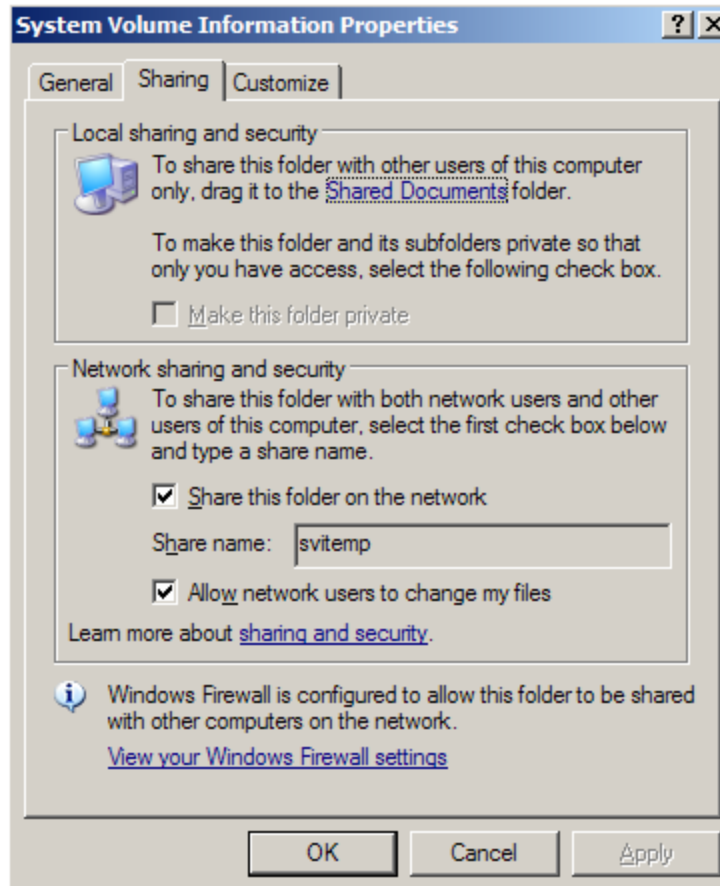
Double-click on drive C: (if that's where your Windows files are, which for most people they will be)

Click on Tools>Folder Options>View then under "Hidden Files" click on "Show Hidden Files and Folders" and Uncheck "Hide protected operating system files."




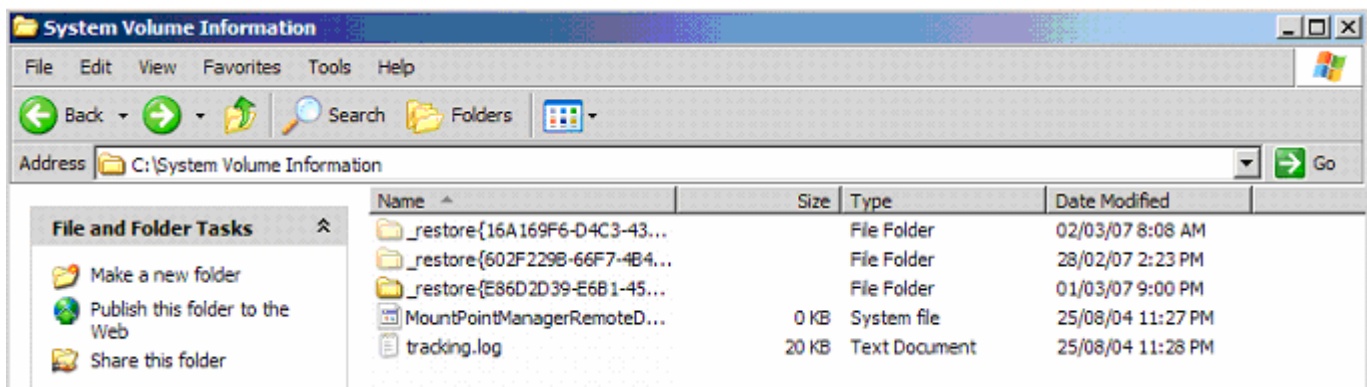
**Folder Options [View Tab]**

Now go back to the listing of folders on drive C:, right click the dim folder  **System Volume Information** click on “Sharing and Security” and under Network Sharing and Security click on “Share this folder on the network” (use share name of “svitemp”) and click on “Allow network users to change my files.” You may or may not have to also click on “Allow network users to change my files.” Note that when you’re done the recovery process you’ll want to go back and undo all of the changes you just made. Sometimes I’ve found that you don’t want to click on “Allow network users to change my files,” and sometimes you do. Experiment.



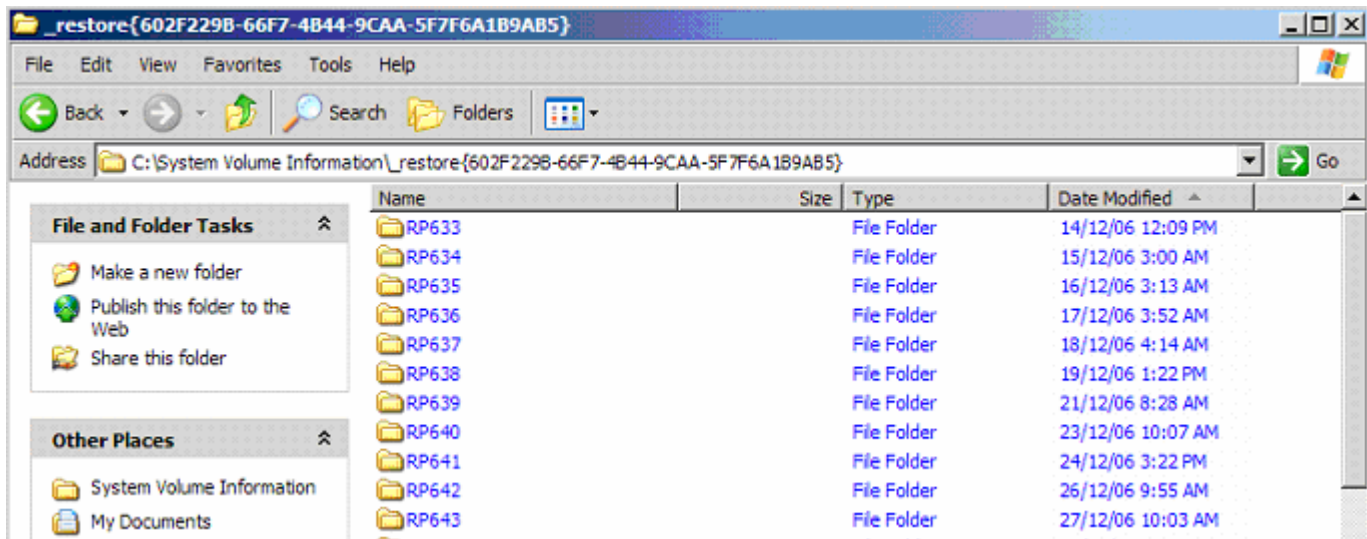
**System Volume Information Properties [Sharing Tab]**

Now double click the “System Volume Information” folder icon, which will now look like , and you’ll see some folders that begin with “\_restore”. Double click on the one with the most recent date that was before your troubles began. In order to see the format as I show below, which includes the date, click on “View” then on “Details”



**c:\System Volume Information**

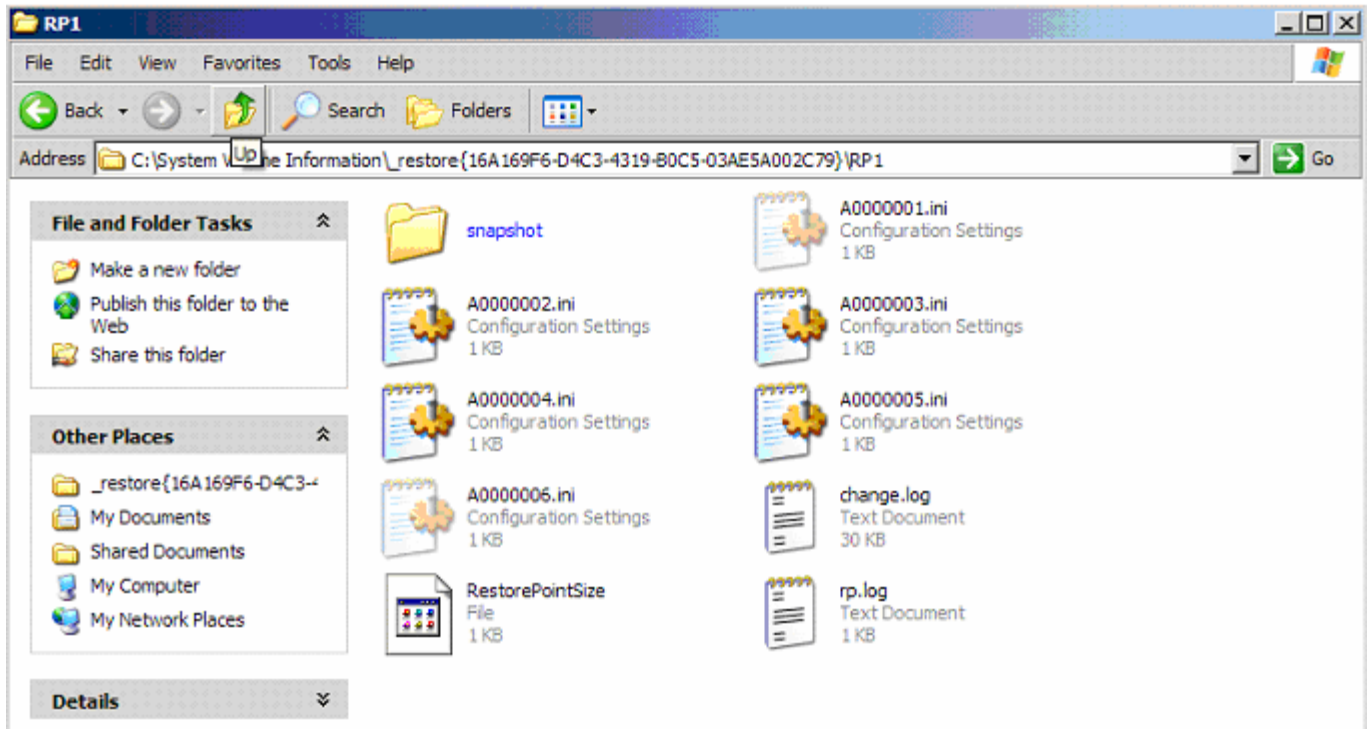
Inside the \_restore folder, you'll see a bunch of folders that begin with "RP".



**c:\System Volume Information\\_restore {15A.....}**

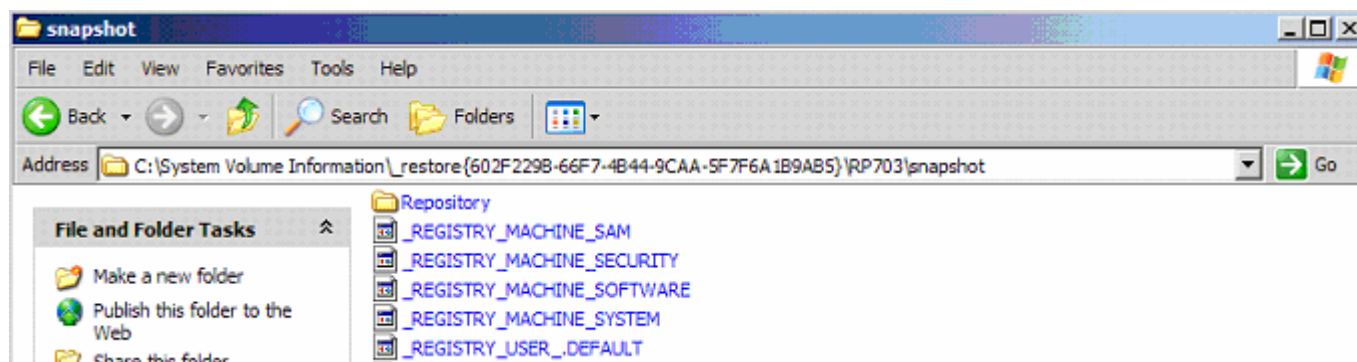
Choose the one with the most recent date that was before your troubles began (you can click on "View" and then "Details" to display the dates, and then you can sort by date).

Open the RP folder, then inside the RP folder you'll see a folder named "Snapshot."



**c:\System Volume Information\\_restore {15A.....}\RP..**

Open the Snapshot folder.

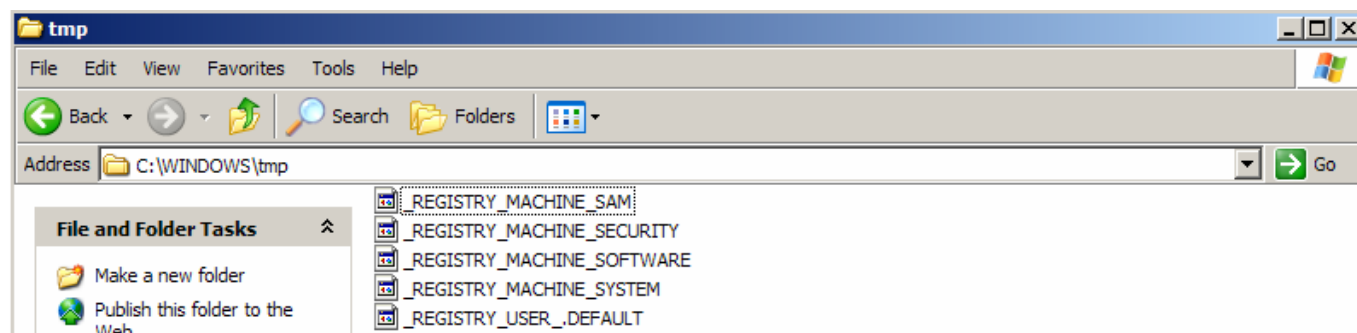


**c:\System Volume Information\\_restore {15A.....}\RP..\snapshot**

Now you'll see the five files you need. They are named:

\_REGISTRY\_MACHINE\_SAM  
\_REGISTRY\_MACHINE\_SECURITY  
\_REGISTRY\_MACHINE\_SOFTWARE  
\_REGISTRY\_MACHINE\_SYSTEM  
\_REGISTRY\_USER\_.DEFAULT

Copy these files over to the temporary folder c:\windows\tmp. Since you're in Windows, you can drag them over to that folder, you don't need to use the command line interface. To open another folder, click on "My Computer" then "Local Disk C:" then "Windows" then "tmp."

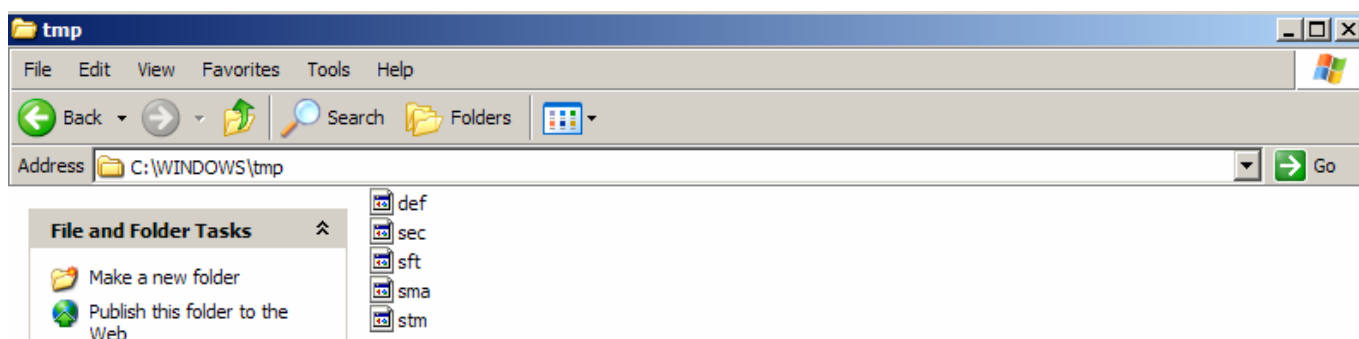


**c:\windows\tmp**

If you're not using batch files, then right click on each file, one at a time, and rename them:

Rename	<u>_REGISTRY_MACHINE_SAM</u>	to	SMA
Rename	<u>_REGISTRY_MACHINE_SECURITY</u>	to	SEC
Rename	<u>_REGISTRY_MACHINE_SOFTWARE</u>	to	SFT
Rename	<u>_REGISTRY_MACHINE_SYSTEM</u>	to	STM
Rename	<u>_REGISTRY_USER_.DEFAULT</u>	to	DEF

This renaming will save you a lot of typing later on. Now the tmp folder should look like the picture below:



**c:\windows\tmp**

*Renaming will save you a lot of typing later. However don't rename them if you're using the batch files I provided because the batch files use the original names.*

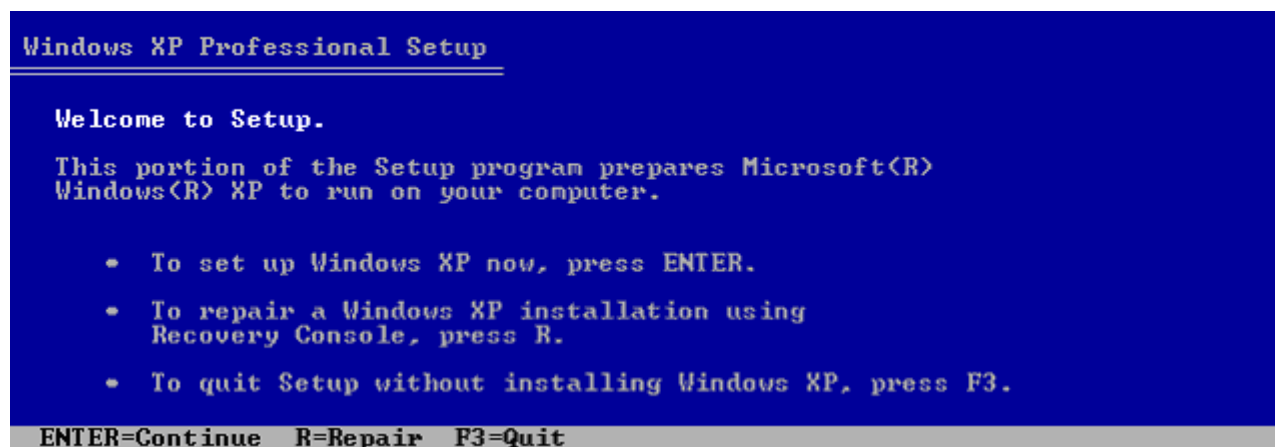
Now, before you do anything else, go back and undo the steps you took to be able to see the System Volume Information. These are unchecking the boxes for "Share this folder on the network" and "Allow network users to change my files," and Click on Tools>Folder Options>View then under "Hidden Files" click on "Do Not Show Hidden Files and Folders" and Check "Hide protected operating system files."

Shut down Windows normally.

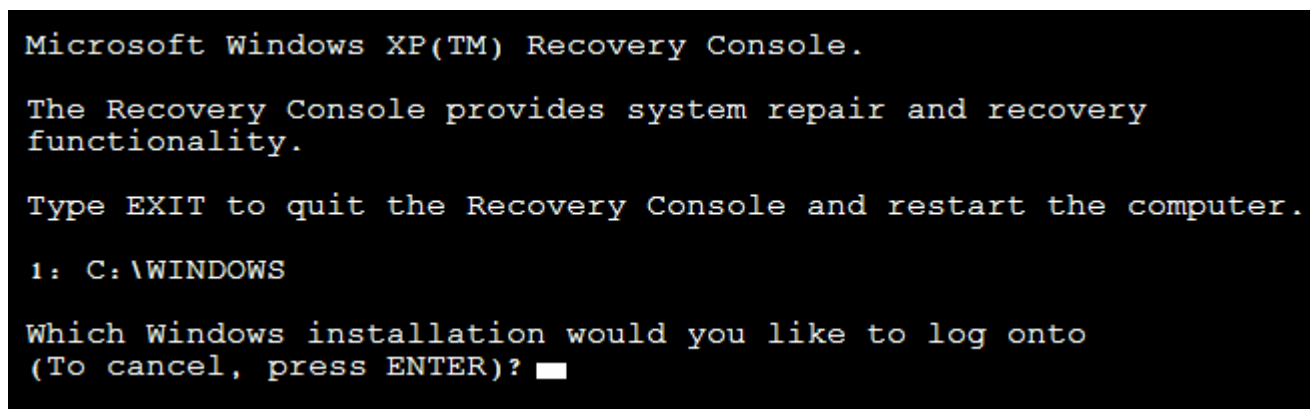
## **Boot the System with recovery CD or floppy diskettes**

Boot the system with the recovery CD or with floppies (six).

The screen will look something like this:



You'll be prompted with several choices. You want to choose "R" for recovery. This will bring up the Recovery Console.



Choose which operating system to recover. For most users there will be only one choice, 1: C:\WINDOWS, So press 1 and then ENTER.

You may be prompted for the Administrator password, enter it and press <ENTER>. However it's possible that the repair file has actually set your Administrator password to nothing, so if it doesn't work when you enter the Administrator password, just try pressing <ENTER> without entering a password.

## Replace the Repair Version of the Five Files with the Recovered Version

If you're using batch files "batch c:\windows\delconfig.txt" which will delete the repair versions of the configuration files from the c:\windows\system32\config folder (if you're already at the C:\windows prompt then you can just type "batch delconfig.txt"). Otherwise type:

```
cd c:\windows\system32\config (this puts you into the \windows\system32\config folder)
```

Now delete the repair versions of the five files, type:

```
C:\WINDOWS\system32\config> del sam
C:\WINDOWS\system32\config> del security
C:\WINDOWS\system32\config> del software
C:\WINDOWS\system32\config> del default
C:\WINDOWS\system32\config> del system
C:\WINDOWS\system32\config>
```

Now replace the five files with the ones you recovered from the System Volume Information folder

If you made batch files on a floppy (and didn't rename the five files to two letter names), type "batch c:\windows\copysnap.txt" which will copy the recovered versions of the configuration files to the c:\windows\system32\config folder (if you're already at the C:\windows prompt then you can just type "batch copysnap.txt"). Otherwise, type:

```
C:\WINDOWS\system32\config>copy c:\windows\tmp\sma sam
1 file(s) copied.
C:\WINDOWS\system32\config>copy c:\windows\tmp\sec security
1 file(s) copied.
C:\WINDOWS\system32\config>copy c:\windows\tmp\sft software
1 file(s) copied.
C:\WINDOWS\system32\config>copy c:\windows\tmp\stm system
1 file(s) copied.
C:\WINDOWS\system32\config>copy c:\windows\tmp\def default
1 file(s) copied.
C:\WINDOWS\system32\config>
```

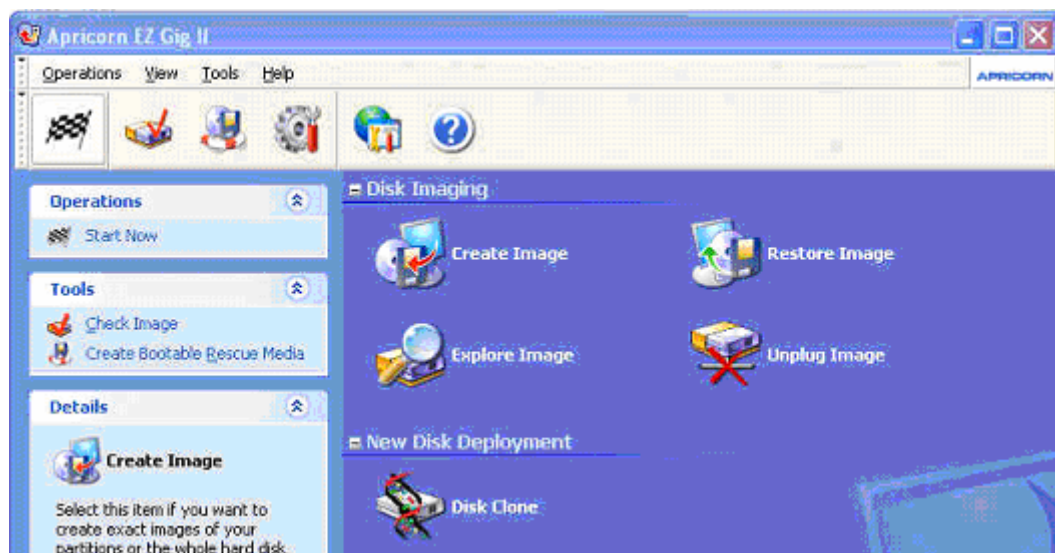
## Eject the CD or Floppy and type “exit” to reboot

Once you boot into Windows XP, you can choose a different restore point if necessary. See <http://support.microsoft.com/kb/306084> for the procedure on doing a system restore.

## Plan for the Future

1. If you had to use floppy diskettes for booting into the recovery console, you should order a recovery CD from the vendor of your PC, even if you have to pay for it (typically less than \$20 including shipping).
2. Make a CD called Ultimate Boot CD for Windows (UBCD). See <http://www.ubcd4win.com/>.
3. Make a Hiren’s CD. See <http://www.hiren.info/pages/bootcd>.
4. Consider doing periodic disk cloning to an external drive. Apricorn makes some kits for notebook drives that are about \$40, not including a drive. You have to buy the kit that matches your drive type (SATA or PATA). Try to buy the same brand and model number of drive as what is in your computer. For desktop drives, you can use a USB enclosure and a product such as DriveClone (<http://www.farstone.com/software/driveclone.htm>). You should periodically clone your drive, i.e. once per week.
  - a. Apricorn PATA for notebook drives (includes software)  
[http://www.apricorn.com/product\\_detail.php?type=reg&id=1023](http://www.apricorn.com/product_detail.php?type=reg&id=1023)
  - b. Apricorn SATA for notebook drives (includes software)  
[http://www.apricorn.com/product\\_detail.php?type=reg&id=1075](http://www.apricorn.com/product_detail.php?type=reg&id=1075)

Note that the Apricorn software does a complete image, including the MBR (master boot record). On my system, which dual boots into Linux with the Grub boot loader, it copied everything and Grub still worked. However the manufacturer told me that it might not automatically work with other Linux boot loaders, and that the boot loader might have to be reloaded.



5. Create the .txt batch files (at the beginning of this document) and place them in the c:\windows folder. This will save you time if you have to do this procedure again.
6. Remember to install an anti-virus program. The free version of Avast is excellent, see <http://www.avast.com/eng/download-avast-home.html> . Try to avoid Norton and Mcafee.
7. Always have an external USB 2.0 hard drive available for emergencies.

## One Page Version for Experienced Users

1. Boot with the Recovery CD or Floppies, then press R for Recovery, then 1 for Windows, enter your administrator password and get to the C:\WINDOWS directory.

```
Type md tmp <ENTER>
Type cd \windows\system32\config <ENTER>
```

2. You're now at c:\windows\system32\config. Rename the five configuration system files to preserve them

```
ren system system.old
ren sam sam.old
ren security security.old
ren default default.old
ren software software.old
```

3. You're still at c:\windows\system32\config. Copy the system configuration files from the repair directory into the \windows\system32\config directory.

```
copy c:\windows\repair\system
copy c:\windows\repair\sam
copy c:\windows\repair\security
copy c:\windows\repair\default
copy c:\windows\repair\software
```

4. Type exit <ENTER>, remove the CD or floppy, type "exit <ENTER>" and boot Windows from the hard disk.

5. Copy the Snapshot versions of the system configuration files from the System Volume Information folder to the \windows\tmp folder. To get to the Snapshot folder do the following:

Double-click on My Computer, double-click on drive C:

Click on Tools>Folder Options>View then under "Hidden Files" click on "Show Hidden Files and Folders" and Uncheck "Hide protected operating system files."

Under drive C:, right click the dim folder "System Volume Information" click on "Sharing and Security" and under Network Sharing and Security click on "Share this folder on the network" (use share name of "svitemp") and click on "Allow network users to change my files." Now open the "System Volume Information" folder. Sometimes you may have to uncheck "Allow network users to change my files."

Open the "\_restore..." folder with the most recent date that was before your troubles began.

Open the RP... folder with the most recent date that was before your troubles began.

Open the "Snapshot" folder.

Drag the five system configuration files over to the \windows\tmp folder. These files are \_REGISTRY\_MACHINE\_SAM, \_REGISTRY\_MACHINE\_SECURITY, REGISTRY\_MACHINE\_SOFTWARE, \_REGISTRY\_MACHINE\_SYSTEM, and \_REGISTRY\_USER\_DEFAULT.

In Windows, in the \windows\tmp folder, rename the five files, sma, sec, sft, stm, and def, respectively (renaming makes for less typing later).

6. Undo the four things you did in order to get to the System Volume Information folder (you don't want to show hidden files and folders, or operating system files, and you don't want to share the System Volume Information folder).

7. Shut down Windows normally, and boot back into the Recovery console (insert CD or floppy)

8. Go to the \windows\system32\config directory and overwrite the repair versions of the system configuration files that you copied in earlier:

```
copy c:\windows\tmp\sma sam
copy c:\windows\tmp\sec security
copy c:\windows\tmp\sft software
copy c:\windows\tmp\stm system
copy c:\windows\tmp\def default
```

9. Type exit <ENTER>, remove the CD or floppy, type and boot Windows from the hard disk.