Recover a corrupted registry that prevents Windows XP from starting

In this case we DID NOT use Tweaking.com's Registry Backup and we have to use our bare hands!
Windows may be unable to boot or just totally unstable. Don't fret, we have a method to restore
the registry even if the client had no foresight to backup anything.

Part 1

1 Put the XP CD in the drive, and restart.
2 Just hit R for RecoverYy Console

3 System should then ask you...
Which Windows Installation would you like to log onto (To cancel, press ENTER)?
Select #1 - > 1: C:WINDOWS

4 Enter your administrator password, and then hit enter. You're in!

Please note that this procedure assumes that Windows XP is installed to the "C:Windows" folder.
Make sure to change "C:Windows" to the whatever your Windows folder's name is if it's different or in a diiferent location.
.

In the following commands, we are simply copying some existing files to a temporary location.
This way, if anything should go wrong down the line, (Do no harm) you will at least still have access to the original files.
These original files are not used again in this tutorial, but you should be aware that you made a backup copy of them.

```
c:\windows\tmp
md c:\windows\tmp
copy c:\windows\system32\config\system c:\windows\tmp\system.bak
copy c:\windows\system32\config\software c:\windows\tmp\software.bak
copy c:\windows\system32\config\sam c:\windows\tmp\sam.bak
copy c:\windows\system32\config\security c:\windows\tmp\security.bak
copy c:\windows\system32\config\default c:\windows\tmp\default.bak
delete c:\windows\system32\config\system
delete c:\windows\system32\config\software
delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\default
```

Important Addendum Note: When attempting the copy operations above, you may encounter an error message saying
"unable to copy". The way arround this is to simply replace the copy (and delete) commands above with the following:

```
cd \windows\system32\config
rename system system.ppp
rename software software.ppp
rename sam sam.ppp
rename security security.ppp
rename default default.ppp
```

I use the extension .ppp becuase windows XP sometimes likes to use the .bak extension itself and unlike the copy
commands above, we are not putting our backup copies in the windows tmp directory, but rather we are leaving
them in thier original directory (but with the .ppp extension, so that windows will ignore them.). As I said before,
these are just backup files, but it is good to know where they are if the repair fails and you ever need them.
Note: The delete is no longer necessary because rename is basically like a "copy and delete" operation in one.

In the following commands, we are simply copying some repair (basically default window install) files so that we can get
windows XP to boot. (It will look awful and none of previous setup and programs will show up, but that is fine.) We simply
need to make windows runnable so that we can do the next parts
(that will retore our full configuration as it was prior to the crash).

```
copy c:\windows\repair\system c:\windows\system32\config\system
copy c:\windows\repair\system\software c:\windows\system32\config\software
copy c:\windows\repair\system\sam c:\windows\system32\config\sam
```

copy c:\windows\repair\system\security c:\windows\system32\config\security
copy c:\windows\repair\system\default c:\windows\system32\config\default

Now what did you just do?
I'll tell you. You first made a temporary directory called "tmp" (md tmp), and then into it, you copied all the files that boot up Windows. Then you deleted all those startup files, one of which is the stinker that got you into this mess in the first place. After that, you copied into that same place fresh startup files from a special repair directory. When you reboot, Windows will look for those files where it always does, and there won't be a stinker in the bunch. *The only thing is, there won't be all your settings for all those applications you run every day, either. But not to worry. Right now, you're sitting in something like a lifeboat -- it's not the original ship, but it'll get you back to where you need to go.* We'll get everything back to that comfortable place, but only after we go through steps 2 and 3.

Now type Exit and watch your computer restart into Windows XP again. Be sure not to tell it to boot from the CD this time. But wait. That's not the way you had XP set up before this disaster struck! That's OK. We're in a lifeboat right now -- this isn't your comfy cruise ship, not just yet. Hang in there. I'm going to show you how to restore your system to the way it was the moment before you told it to install that errant application, or whatever it was you did, so follow along and we'll go to part 2.

Part 2

Here's where you'll copy the saved registry files from their backed up location by using System Restore. This folder is not available in Recovery Console and is normally not visible -- Microsoft is protecting you from yourself by hiding it from you and locking it away from you. But we have the keys. Before you start this procedure, you'll need to change several settings to make that folder visible:

1. Start Windows Explorer.
2. On the Tools menu, click Folder options.
3. Click the View tab.
4. Under Hidden files and folders, click to select Show hidden files and folders, and then click to clear the "Hide protected operating system files (Recommended)" check box.
5. Click Yes when the dialog box is displayed that confirms that you want to display these files.
6. Double-click the drive where you installed Windows XP to get a list of the folders. It's important to click the correct drive.
7. Open the System Volume Information folder. This folder appears dimmed because it is set as a super-hidden folder. If you're using the FAT32 file system, this will be easy. If you're using NTFS, it won't let you open the folder, but here's how to get around that:
8. Right-click on that system volume information folder and select Sharing and Security.
   Then click the Security tab. (No security tab? Goto step 9.)
   Click Add, and then in the box that's labeled "Enter the object names to select," type the name of the user that's at the top of the Start menu -- that's probably you.

Anyway, make sure you type the name the way it's listed there on the Start Menu. I made the mistake of typing my first name only and it wouldn't let me in. Type first and last name if that's how it's written on the top of the Start menu. After you've typed that in, click OK a couple of times and finally that monster will let you in.

9. But what if you don't see a Security tab? Try this:
   Click to select the checkboxes (check BOTH checkboxes) in the "Network sharing and security" area -- one is labeled "Share this folder on the network" and the other is labeled "Allow network users to change my files."
   Change the share name to something short, like sysinfo. Then it'll let you in.

Note: After you're done with this entire rescue operation, you might want to go back and change these back to the way they were before, for maximum security.

Note: If you get an error when you change the name to sysinfo, and hit apply/ok, just try it again...
that happened to me, but it worked on the second try with no problems.

10. This folder contains one or more _restore {GUID} folders such as "_restore{87BD3667-3246-476B-923F-F86E30B3E7F8}".
    Open a folder that was not created at the current time. You may have to click Details on the View menu to see when these folders were created. There may be one or more folders starting with "RP x under this folder.
    These are restore points.

Note: The System Volume is NOT a subdirectory of the windows directory. So if you cannot find it, go up one directory level and look again.

11. Open one of these folders to locate a Snapshot subfolder; the following path is an example of a folder path to the Snapshot folder:
C:System Volume Information_restore{D86480E3-73EF-47BC-A0EB-A81BE6EE3ED8}RP1Snapshot

From the Snapshot folder, copy the following files to the C:WindowsTmp folder (you can use your mouse, you're in Windows now, remember?): Copy and Paste

_registry_user_.default (Notice the period (".") before the word default)
_registry_machine_security
_registry_machine_software
_registry_machine_system
_registry_machine_sam

Part 3

Back into the Recovery Console

In part three, you delete the existing registry files, and then copy the System Restore Registry files to the C:Windows\System32\Config folder:

From within Recovery Console, type the following commands:

Note: Here we are simply replacing those "default" repair files with valid and current restore point files. So we delete the old (default) files and copy in the new files. If get errors when trying to delete, you can simply skip the delete commands and just do the copy (and when prompted to overwrite, type Y (for yes) and hit enter

delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\software
delete c:\windows\system32\config\default
delete c:\windows\system32\config\system

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_machine_sam c:\windows\system32\config\sam
copy c:\windows\tmp_registry_machine_security c:\windows\system32\config\security
copy c:\windows\tmp_registry_user_.default c:\windows\system32\config\default
(Notice the period (".") before the word default in the first parameter)

Now. You're done! Type exit and your computer will reboot into whichever restore file you chose. But wait. If it's not the right one, that's OK, you can now go into your System Restore area and pick a different restore point if you want. There's a whole calendar full of them in there accessible through Windows now.

Here's how to get into that restore area if you're not happy with the current restore point:

1. Click Start, then click All Programs.
2. Click Accessories, and then click System Tools.
3. Click System Restore, and then click Restore to a previous Restore Point.