

Re: XP Logging on then immediately logging off

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2008-07/msg00468.html>

- *From:* "Pegasus \ (MVP)" <I.can@xxxxxxxxxxx>
 - *Date:* Wed, 2 Jul 2008 22:24:39 +0200
-

Backing up the System registry file is extremely simple: You locate it with Windows Explorer, then copy it to some safe location. Exporting it to the desktop will not do the job – you won't be able to import it in case you need to.

As I said before, I am by no means sure that your drive letters are incorrect. If the problem machine was networked then it would be a one-minute job to find out. Since your machine is not, it's considerably more complicated. Here is a way that I believe should work. While the problem disk is connected as a slave disk, do this:

1. Click Start / Run / cmd {OK}
 2. Type this command: mountvol {Enter}
- You will get a number of lines such as this one:
- ```
\\?\Volume{5b21c8e0-b18f-11dc-afb6-806d6172696f}
H:\
```
3. Pick the line above drive letter H: (which you previously reported to carry the folder c:\Windows) and jot down the stuff between the curly brackets.
  4. Run regedit and load the System hive of the problem disk, as previously described.
  5. Navigate to HKLM\SYSTEM\MountedDevices of the problem hive.
  6. On the right side of the screen, under the word "Default", locate the string you jotted down in Step 3.
  7. Jot down the hex data on the far right side. It is of the form  
4a ac 4a 8c . . . .
  8. Scroll down to the bunch of DosDevices\ values.
  9. Locate the hex data you jotted down in Step 7.  
Which is the drive letter that uses this data?

I'm aware that this is getting quite complex. It might help if you stepped back and considered your options:

- a) Persist with your repair effort.
- b) Ask a computer-savvy friend to help.
- c) Take the machine to a computer shop.
- d) Forget it and reload Windows from scratch.

Re: XP Logging on then immediately logging off

"RipperT @nOsPaM.nEt" <<RiPpErT> wrote in message  
[news:OBFIj1G3IHA.2424@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OBFIj1G3IHA.2424@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Following your instructions, I've accessed ProblemPC and  
H:\Windows\system32\config\system shows entries for \DosDevices\A:  
as well as C: thru K:. Since C: already exists, it seems I should not  
rename the D: to C: Is this correct? Also, I am unsure how to backup the  
System Registry file. After loading the system hive of the problem disk  
per your instructions, I exported the whole reg file to the desktop of the  
host machine as a backup. Is this correct? I'm fumbling in the dark here  
more than you know and I appreciate your help very much.

Thanks,

Rip

"Pegasus (MVP)" <I.can@xxxxxxxx> wrote in message  
[news:uWENVG02IHA.2336@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uWENVG02IHA.2336@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I don't know if or why the drive letter might have changed – it's  
not my machine and I don't know anything about the events that  
led up to the problem.

When slaving the disk to another machine then you don't know  
anything about the original drive letters. The drive letters you see  
are assigned by the other machine and are irrelevant for the  
normal operation.

When you wish to edit the System hive of the problem disk  
then you can do it with regedit.exe like so:

1. Click HKLM.
2. Click File / Load Hive.
3. When prompted, type H:\windows\system32\config\system to  
load the System hive of the problem disk.
4. When prompted for a key name, type ProblemPC.
5. Double-click the key ProblemPC and navigate to MountedDevices.
6. Check the values DosDevices\...

You can now rename any of these values. Unfortunately you're  
groping in the dark: You don't know if these values are correct  
or not unless you can access the problem machine via a networked  
PC. This is why it is essential to create a backup copy of the System  
registry file so that you can restore it if things go wrong.

When finished, click the key ProblemPC, then File/Unload Hive.

"RipperT @nOsPaM.nEt" <<RiPpErT> wrote in message  
[news:Oo4EWFx2IHA.2524@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:Oo4EWFx2IHA.2524@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Thank you for taking the time to respond. I would like to  
understand the  
why of this solution before I do it. How is the drive letter

Re: XP Logging on then immediately logging off

Re: XP Logging on then immediately logging off

incorrect?

Slaving the drive to another machine shows that it has two logical

drives: G and H. How could it be set up this way if it is incorrect?

Please explain. Also, I have already attempted to edit the registry of

this H drive using a host machine. I searched the H drive for the

Regedit.exe program, double clicked it and I navigated to HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\.

Upon viewing the entries in the right hand pane, I see my name and the name of the host machine. Does this not mean

I am editing the registry of my host machine and not the H drive? Thanks

again,

Rip

"Pegasus (MVP)" <I.can@xxxxxxxxxx> wrote in message [news:%23hoUKwu2IHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23hoUKwu2IHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

See below.

"RipperT @nOsPaM.nEt" <<RiPpErT>

wrote in message

[news:%233rV%23Uu2IHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%233rV%23Uu2IHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I have an HP Pavillion desktop w/ XP (don't know if it's Home or Pro) that logs off as soon as it logs on. I get welcome screen, logon screen, desktop wallpaper, then logoff. This happens with the only account on the machine, the same account in safe mode and the admin account in safe mode. My research points to a corrupt userinit.exe file in Windows\system32.

\*\*\* It's rare that this file gets corrupted. In most cases Windows

\*\*\* is simply unable to locate it.

Re: XP Logging on then immediately logging off

I removed the HDD to another computer and replaced the userinit.exe file with a known good one, then returned the drive to its host machine, but no change.

\*\*\* This is entirely expected.

Further research suggests that a registry key may still point to a wrong userinit.exe file or wrong path, and I would like to check the registry to see if this is true. The key is supposed to be:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

\*\*\* It is actually  
HKLM/Software/Microsoft/Windows  
NT/Current  
Version/Winlogon/Userinit

The value is supposed to be  
(on a machine with  
Windows installed to  
C):  
C:\WINDOWS\system32\userinit.exe,

\*\*\* Yes.

This computer is not on my network, so I can't connect to it's registry via the network. I've booted into recovery console and it asks me to choose between these two installs:

Re: XP Logging on then immediately logging off

Re: XP Logging on then immediately logging off

1. H:\MiniNT
2. H:\I386

I am confused by this because I think there is usually a C:\Windows option here, or in this case, an H:\Windows.

\*\*\* Here is your answer: The system drive letter is incorrect, hence  
\*\*\* Windows cannot find userinit.exe.

Looking at this drive's folder structure on another computer, it has a G:\ drive and an H:\ drive. The H drive has a Windows folder with an I386 folder inside that. The G drive I believe is the recovery partition and has the MiniNT folder and an I386 folder at it's root. No Windows folder.

I don't know which installation to select and I don't know what commands to enter to open or check the registry values to see if the key is correct. The HP recovery utility says that I will have to reinstall all apps that didn't come with the machine if I use it and I'd like to avoid that. Can anyone help?  
Many thanks,

Rip

Editing the registry from the Recovery Console, if at all possible, would be painful. It's much easier to connect the problem disk

Re: XP Logging on then immediately logging off

temporarily as a slave disk to another  
WinXP PC, then to edit  
the "System" registry file with regedit.exe on  
that machine.

Simply rename

HKLM\SYSTEM\MountedDevices\H: to

HKLM\SYSTEM\MountedDevices\C: