

Re: Can I access a decrypted file if I have all the files backed u

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-07/msg00171.html

- *From:* Rojo26 <Rojo26@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 13 Jul 2007 20:12:03 -0700
-

OK, I think I can do it. It turns out that I still have all the system restore point folders in my System Volume Information folder. The last day I modified the encrypted file was June 23, 2007. I have a restore point from June 24. All I should have to do is follow the instructions in KB307545 (<http://support.microsoft.com/kb/307545/>) for modifying the registry so that I would be able to run System Restore to restore back to that restore point. The registry file from the restore point should include the user SID, the certificate info, and the key info, thereby replicating exactly (except for the hard drive) the conditions under which I could read the file.

I envision doing this on a borrowed, used hard drive on which I would restore all the files from the backup. As long as I don't have a problem that requires me to activate Windows, I think this would work. Any opinions?

Rojo26

"Rojo26" wrote:

You seem to be thinking just like me. I got into this situation by trying to clone the drive in the first place. I needed more disk space and a better performing drive, so I was trying to clone the 40GB drive with a 2MB cache to a 250GB drive with a 16MB cache. That failed over and over again even though the source drive was still able to boot. But then I ran a drive restoration program on it. That program is well known to save drives with problems. But after I used it, I was not only unable to clone it, but I was unable to boot it as well. So now that it is in much worse condition than it was then, I am certainly not going to be able to clone it.

As an A+ tech, I have run repair installs before. I don't believe they affect user account SIDs, and I know that they leave the folder and file attributes intact.

By the way, all my data was backed up; I just never tried to open the one text file that was encrypted—it contains all of my passwords and similar information. I don't remember the circumstances in which I created that file, but it is in a real oddball folder. It is in Docs & Settings\All

Re: Can I access a decrypted file if I have all the files backed u

Users.WINDOWS\Documents. I have no idea how that "user account" ever got created. I have a perfectly good All Users folder, but the All Users.WINDOWS folder is a real oddity. Consequently, I almost never saw the file in its folder—I accessed it from a shortcut.

Something else that is interesting: everyone has been saying that EFS is so effective, but today, I discovered a copy of the file that I made last August. I had copied the file over the network to my laptop, and the copy is not encrypted. I have made quite a few changes and additions to it in the last 11 months, but that copy might solve most of my problems. As of now, it's too early to tell.

I want to try one more thing, although I give it almost no chance of working. I want to format a healthy drive as NTFS and use a second computer to restore all the files from the affected hard drive to it from my Windows backup file. Although that drive won't be created from an image (sounds almost Biblical, doesn't it?), it will have ntdetect.com, boot.ini, ntlldr, and all the Windows, program, registry, and user account files. It seems to me that it should at least boot, especially if I use Windows Disk Management to make it active. Whether it will have valid user accounts is another story, and whether I'll be able to copy the file over the network again is another story also.

I was thinking of using Partition Magic to change the drive format to FAT32 in hopes that it would remove encryption, but my guess is that I'd be able to open the file only to see encrypted data that I won't be able to read. After all, without the cert and key, it shouldn't be able to be decrypted. But somehow when I copied it over the network, it lost its encryption. But when I did the Windows backup over the network, the encryption stayed.

Joel

"Shenan Stanley" wrote:

Rojo26 wrote:

If I had, certainly after reading those articles, I wouldn't have made that post. Windows gave no message at all saying that encryption even involved certificates or keys.

What I need to know is if there is any possibility that I can retrieve the certificate and key from the hard drive.

While there may be some possibility – it is slim. I am sorry you did not learn about encryption and the best practices for using it before diving into it – as it may have sealed the fate of any encrypted files you have on the unbootable hard disk drive.

One of the things encrypting your files was meant to protect against is booting from something other than the system and copying/accessing the files

Re: Can I access a decrypted file if I have all the files backed u

contained within the actual drive with the interesting data. Although your predicament does not exactly match that scenario (you are reportedly trying to access your own data because of a hard disk failure or something else that made said system non-accessible by the means you were used to) – it does bear a striking resemblance to "booting from something other than the system and copying/accessing the files contained within the actual drive with the interesting data..." :-(

I am unsure what attempting a repair install might do (or even attempting to image/clone the defunct system from the dying drive to a new drive and then performing a repair install) and it COULD make things worse. However – if it was me and this data was unbelievably important (and for some reason – not backed up) – I would likely make a clone of the drive and try a repair install on the cloned drive to get it back up and running to see if I could access the data within. After that – you'd likely have to go with non-microsoft products/services and spend a good hunk of money to try and get the files decrypted.

For the future – if you plan on continuing to utilize EFS...

How to back up the recovery agent Encrypting File System (EFS) private key in Windows Server 2003, in Windows 2000, and in Windows XP
<http://support.microsoft.com/kb/241201>

--

Shenan Stanley
MS-MVP

--

How To Ask Questions The Smart Way
<http://www.catb.org/~esr/faqs/smart-questions.html>