

Re: EFS – Please help to unsecure data

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/10769.html>

From: Galen (galennews_at_gmail.com)

Date: 02/07/05

Date: Mon, 7 Feb 2005 10:34:50 -0500

In news:e14963ODFHA.1188@tk2msftngp13.phx.gbl,
– 781 <lets@have.org> had this to say:

> *I will buy and try all*
> *that's available, and will keep you posted if I had gotten anything*
> *from those tools. Thank you again, and thank you much.*
> *G*

I have the OS installed at this point on a box sitting on the desk to my left. Before you buy the software there's a few other options. There are professionals who can deal with this and if you're really certain that you've no other backups of your data you might want to look to them for help. Each continued use of your computer lessens your chance of recovering data from an earlier installation. While this software might help you nobody seems to know for certain if it will or not and my GUESS is that this is to be mostly based on your chances of recovering your lost keys.

I should know before the end of the day today if I'm even able to recover the data after a fresh installation and generating some random drive activity. Even if I'm able to recover the data and then use the application to open the encrypted files it doesn't mean that you will certainly be able to. The sectors holding your key information may very well have been over-written.

Your original post says you reformatted your drive. I'm wondering if you used the same user name for your account or not. I'd like to mimik your actions as much as possible for this. I don't suppose you did a quick format and/or a repair installation and still have your old user accounts in the C:\Documents and Settings*****\ folder? Where ***** is your old user name... In order to see them you have to be logged on as an admin and you will probably have to open My Computer, click on the C: drive (or your root drive) and then click tools > folder options > view > and select show hidden files and folders. Might want to click to show the hidden protected operating system files as well but that might not be required... I suppose that's a slim hope and that you probably don't have them anymore or you'd have already tried that but I guess it's worth asking.

I'd also not let me give you false hope... I'm trying the experiment based on what I have seen here and what I've been reading. While I'm trying to make it as close to your particular case as possible it's not certain that the cases will be the same or even close enough to matter. My goal is just to see if I can recover the keys after a re-installation with forensic tools and then to see if the keys recovered will be enough to open any or all of the six files that I have encrypted. (Just so you know it's two plain text files, two executable files, and two compressed files that I'm trying this with.) Even if I'm able to recover the keys AND the software works to decrypt the material the same may not be true in your case.

A good idea would be to try the solution offered by R. McCarty (converting to FAT32 to remove the encryption.) As odd a solution as that is it just might work. I've been looking around on the 'net and this is what I came across:

<http://weblogs.asp.net/paranoidmike/archive/2005/01/24/359390.aspx>

That says this:

"By default, encrypted data on NTFS will be decrypted when copied/moved to non-NTFS media. We want a solution so that EFS encrypted data cannot be copied to non-NTFS removable media."

I would definitely try that. It can't hurt and it just might be the answer you're looking for.

Galen

--

"My mind rebels at stagnation. Give me problems, give me work, give me the most abstruse cryptogram or the most intricate analysis, and I am in my own proper atmosphere. I can dispense then with artificial stimulants. But I abhor the dull routine of existence. I crave for mental exaltation." -- Sherlock Holmes