

# EFS + unbootable HDD help ...

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2006-02/msg03572.htm](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-02/msg03572.htm)

---

- *From:* [andersen\\_mikael@xxxxxxxxxxxx](mailto:andersen_mikael@xxxxxxxxxxxx)
  - *Date:* 22 Feb 2006 12:57:51 -0800
- 

Here's the deal:

- 1) HDD crashes, making it unbootable
- 2) It contains EFS encrypted files and I didn't backup keys

Yes, I know ... I'm a moron ... but not all hope is out and I'd like any help ...

My hope is that:

- 1) I did make weekly backups and thus have the encrypted files available.
- 2) Using Stellar's recovery tool I was (and still am) able to recover virtually \*all\* files from the NTFS drive (haven't located a defect file yet!!!) – accessing it from Explorer, makes the HDD make 'funny' noises – like "I can't read anything", until it gives up and suggests me to format :)

However recovering EFS encrypted files using Stellar is not possible (they just contain garbage) and is not access controlled (thus not marked green) – anyone knows of any tools that can recover EFS encrypted files from a damaged disk??? (I've tried some different tools, which all fails in scanning the HDD – only Stellar succeeded incl. Active Undelete, File Scavenger)

Now on to my recovery attempts ...

I first tried following the description at <http://www.beginningtoseethelight.org/efsrecovery/index.php> by changing the SID (the "blue text" description, but no luck – still access denied).

Then it came to me ... at least I thought ... I'll simply recreate my OS. Since I could recover all files:

- 1) I simply took an old HDD, made it primary drive, installed XP on it (until first reboot).
- 2) I then made my (newly bought) replacement disc primary again and booted on it (leaving the newly formatted disc as sec. disc).
- 3) Copied all recovered files to the just installed HDD (I first delete

## EFS + unbootable HDD help ...

the newly installed XP – both windows + docs. and settings folder and then copied). I copied docs and settings + windows folder + selected "program files" folders – made that HDD primary again and booted ...

And voila ... sign on dialog, logging in ... everything looks like before – GREAT (was now able to easily export outlook express accounts too, great!). But decrypt wont work ... still access denied (ownership of files was claimed).

So I tried to encrypt a random file while watching the C:\Documents and Settings\\Application Data\Microsoft\Crypto\RSA\S-1-5-21-1957994488-179605362-725345543-1003 folder (and protect) – and immed. after the encrypt, a new file was generated ... I'm baffled ... it's like it can't see the file(s) already present – how/why can't it see the files already present?????

Then I noted that the files from the recovery didn't have the same attributes set (wasn't marked as system file and wasn't hidden – which file created in protect folder was when created), so perhaps Stellar didn't recover them "correctly" ??

Can anyone help ? I seem to be stuck ...

1) Since I completely replaced the new XP installation with the recovered one – and even running on the same physical machine – I can't see how this could fail ... unless the key-files wasn't recovered correctly by Stellar ... making the XP installation not recognize them??

That'll put me back to my above question, about a (even better) tool, which can extract both the latest versions of my encrypted files, along with the correct EFS key files ?!

2) Did I miss someting in "restoring" my OS, which would make this approach fail?

looking forward to your help ....

Sincerly

Mikael Andersen

.