What is Secure Erase?

Secure Erase is the name given to a group of commands available from the firmware on hard drives based on SATA and PATA. The Secure Erase commands are used as a Data Sanitization method to completely overwrite all data on the hard drive.

Secure Erase is the name given to a group of commands available from the firmware on hard drives based on SATA and PATA. The Secure Erase commands are used as a Data Sanitization method to completely overwrite all data on the hard drive.

Once the hard drive has been erased using a program that uses the Secure Erase firmware commands, no other file recovery program, partition or other data recovery method can extract data from the drive anymore.

Note : Secure Erase or any Data Sanitization method is not the same as sending files to the computer's Recycle Bin or Recycle Bin. Using Secure Erase will permanently "delete" the files.

Method of erasing Secure Erase

The Secure Erase method is implemented in the following way:

1. Overwrite data with number 0 or number 1

Method of erasing Secure Erase

There is no need to verify the overwriting using the Secure Erase method, since the overwriting takes place from within the drive, meaning that detecting a drive's write error will prevent any errors. This makes Secure Erase

much faster and more efficient than other Data Sanitization methods.

This method differs from other Data Sanitization methods such as CSEC ITSG-06, RCMP TSSIT OPS-II and NAVSO P-5239-26, usually performing verification after the first or last override and / or any recording. override any other.

Some specific Secure Erase commands include **SECURITY ERASE PREPARE** and **SECURITY ERASE UNIT** .

Some other information about Secure Erase

1. Some free hard drive erasing programs work through the Secure Erase command.
2. Secure Erase is not available as a method of deleting data when destroying individual files or folders.
3. Using Secure Erase to erase data from a hard drive is often considered the best method because the action is taken from the drive itself, with the hardware writing the data in the first place.
4. The only Data Sanitation method based on software is the method of using Secure Erase commands.
5. HDDErase is a free data destruction software program that works by executing Secure Erase commands.
6. Secure Erase is not available on SCSI hard drives.
7. Security Erase can be considered as Secure Erase, but probably not very often.
8. You cannot run firmware commands on your hard drive as if you were running Windows commands from the Command Prompt.

Secure Erase and securely erase your hard drive are no different

Some file shredder programs and data destruction software have the word 'secure erase' in their names or ads that they delete data safely from the hard drive. However, unless they specifically note that Secure Erase commands will be used, otherwise all is just an advertisement.

These programs call their deletion methods 'safe' because they overwrite the data with 0, 1 or random data to make it harder for someone to detect what has been deleted from the drive.

In other words, while all data deletion methods may be secure, not all options use the Secure Erase method.

So be careful before deciding to use a program. For example Secure Eraser and SDelete (Secure Delete) may look similar to Secure Erase support but are not. MHDD, CopyWipe and hdparm are some examples of free data destruction programs that use Secure Erase.