

Five Apps

Five hard disk cleaning and erasing tools

By [Mark Kaelin](#)

October 10, 2012, 11:36 AM PDT

Takeaway: Brien Posey lists five tools that ensure your personal information is securely removed from all hard disks.

When it comes to disposing of old hard drives, simply erasing your files or reformatting the drive alone is not enough to ensure your privacy. In this age of rampant ID theft, it is more important than ever to ensure that your personal information is securely removed from all hard disks. That being the case, I decided to create a list of five utilities for securely erasing and formatting old hard drives.

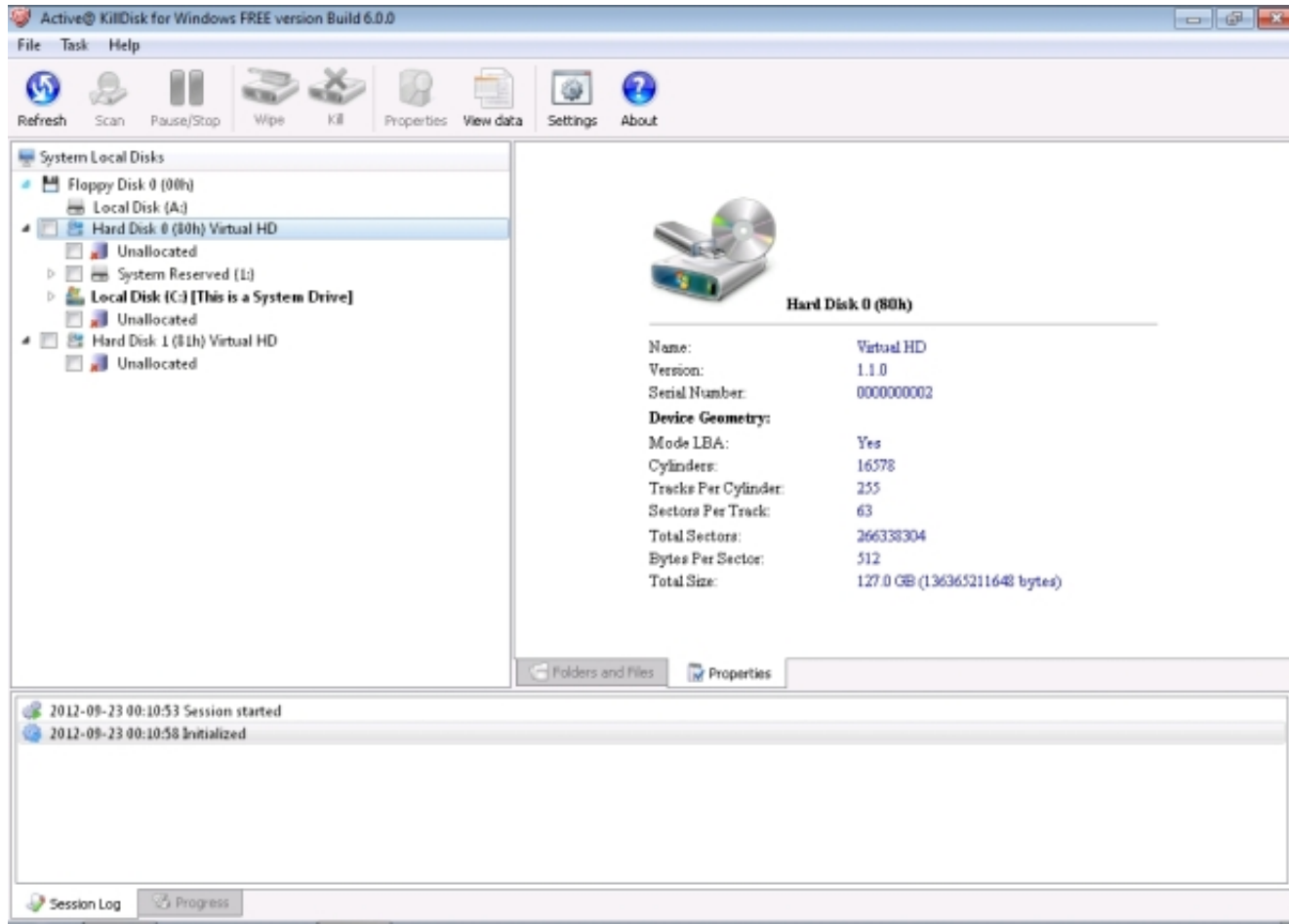
This blog post is also available as a [TechRepublic Photo Gallery](#).

[Automatically sign up for TechRepublic's Five Apps newsletter!](#)

Active@Kill Disk - Hard Drive Eraser

[Active@ Kill Disk - Hard Drive Eraser](#) is a free utility for securely erasing a hard drive. More importantly, this utility adheres to United States Department of Defense standards (DoD 5220.22M) for hard disk data removal.

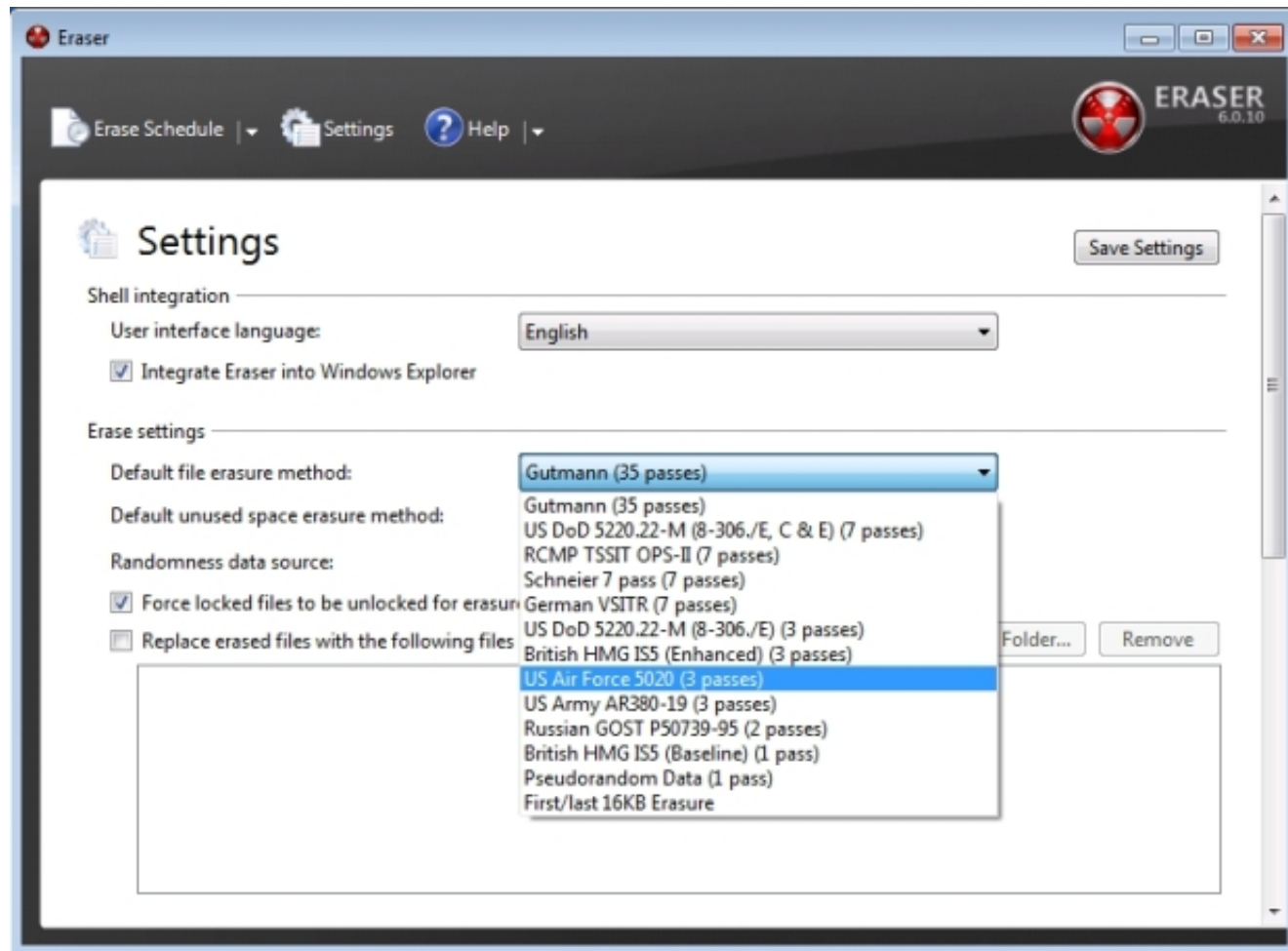
Although some might consider it to be hokey, I especially liked the certificate feature. When a hard disk has been erased, the software generates a certificate that you can print as a way of proving that the disk has been securely erased.



Eraser

[Eraser](#) from Heidi Computers, is another free utility for securely erasing data from a hard disk. The most interesting thing about this utility is that it provides several different methods for overwriting data, based on a number of different standards. You can even define your own method for overwriting data.

This utility allows you to securely erase specific files, folders, unused disk space, or even the recycle bin. Furthermore, erase operations can be run manually or scheduled.




Shredit for Windows


[Shredit for Windows](#) is a privacy application that is designed to securely erase individual files, free space, or entire hard drives. The software lets you pick the write pattern and the number of writes. A number of different government standards are supported.

Shredit for Windows costs \$24.95 for the download version or \$34.95 for the CD-ROM version.

ShredIt



There is no way to recover shredded items
Use ShredIt to securely delete a file, a folder, or the free space on a disk.
For online registration go to www.mireth.com



Choose Disk
A: ▼
Shred Freespace

Current Name
Folder:
File:

Shred File
Shred Folder
About
Buy Now
Quit

Progress

00.0%

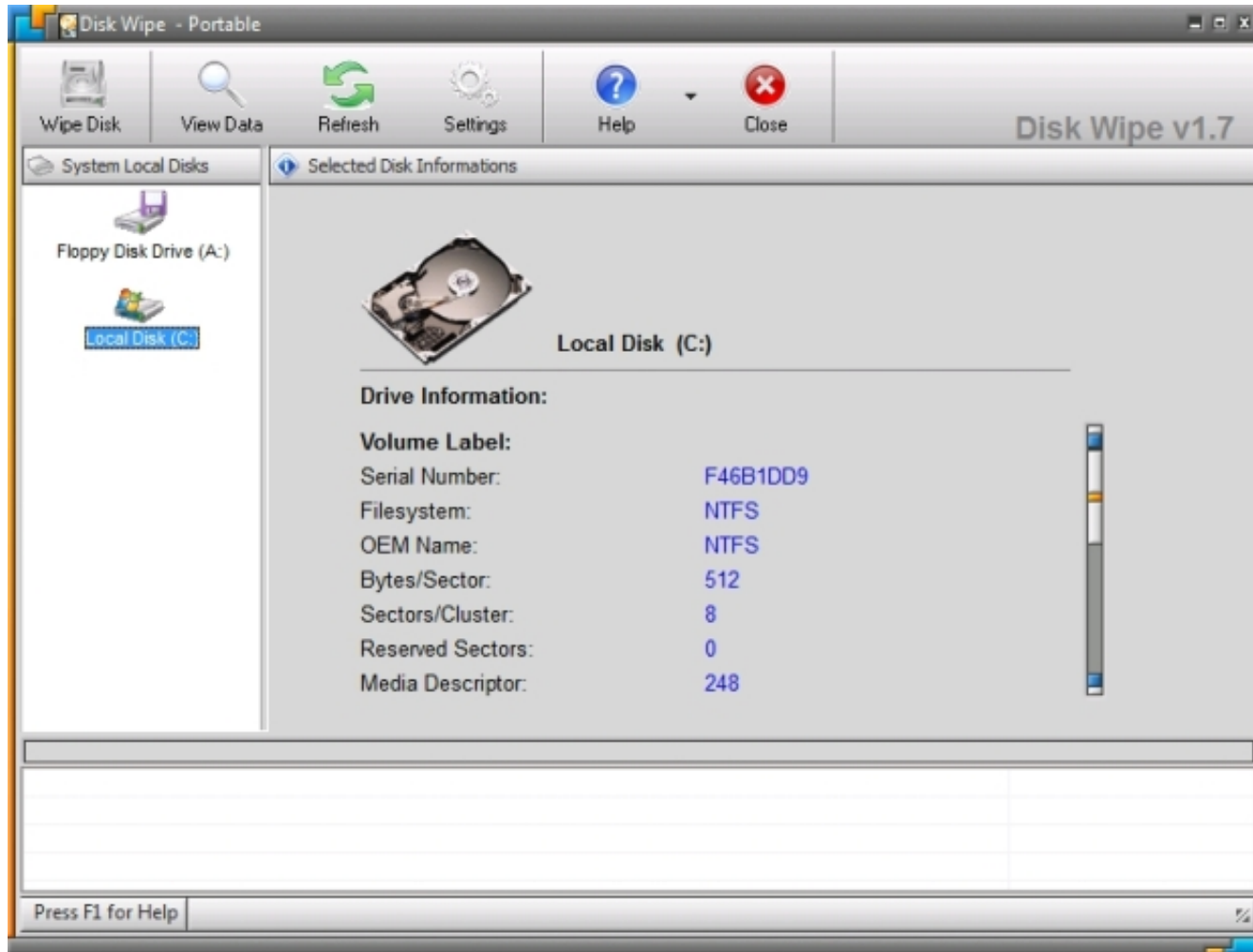
Copyright 1991 - 2009, The Mireth Technology Corporation. All Rights Reserved.

Options
Confirm Shredding: ☒ Files ☒ Folders
Write Pattern: Mireth Standard ▼ Number of Writes: Mireth Standard ▼
Activity Log: ☐ Enabled ☐ Include Original Filenames In Log
Log Filename: c:\ShredItLog.txt Browse... Show Log
Government Standards: ☒ DoD 5220 Clear ☒ DoD 5220 Sanitize ☒ NSA
☒ DoE Final DoE Pattern: Zeros ▼

Serial Number (Registration Key)
Enter to Unlock: DEMO Version - Try Before You Buy.

Disk Wipe

Disk Wipe is a free utility for wiping data from a hard disk in a secure manner. Like Eraser, Disk Wipe includes a number of different algorithms, including DoD 5220-22.M, and Peter Guttman. The really nice thing about this utility is that it is portable, so you don't have to install it to be able to use it. Furthermore, Disk Wipe works on more than just hard drives. It can also be used to securely wipe USB flash drives and SD cards.



Darik's Boot and Nuke

[Darik's Boot and Nuke](#) is a free, open source utility for securely erasing hard drives. Although this utility is designed to be secure and effective, the author does not explicitly guarantee that data is completely unrecoverable and there is no support for this application.

Darik's Boot and Nuke

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

- * Press the F2 key to learn about DBAN.
- * Press the F3 key for a list of quick commands.
- * Press the F4 key to read the RAID disclaimer.
- * Press the ENTER key to start DBAN in interactive mode.
- * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _

Also read:

- [Video: How to wipe a hard disk with DBAN](#)
- [Three methods for erasing data securely from an iOS device](#)
- [Five apps to wipe data from your Android phone](#)

You May Also Like

- [Five fast Windows desktop search utilities](#)TechRepublic
- [Five Lovecraft movie adaptations that will make you feel deeply unloved](#)TechRepublic
- [How Windows 8 Apps Stack Up](#)Qualcomm
- [Stock Prices and Corporate Profits: The Divergence Explained](#)Profit Confidential

[about these links](#)