Truly Deleting Files[1,2]

Lorrin R. Garson

NOTE: Thoughtful caution should be exercised before downloading, installing and running any software… perhaps extra caution with programs that purport to over-write files and/or "clean up" the Registry. Only download software from trusted sources and seek independent reviews of software before attempting to use. *The author of this document has not tested any of the software cited, does not endorse any of these products and services and accepts no responsibility for their use*.

Background:

When a file is deleted from a disk drive, even deleted from the Recycle Bin, data in that file remain on the disk drive. The deleted file is marked as "deleted" in the master file table (MFT) and clusters allocated to the deleted file are marked as "free" in the file $BitMap (each cluster being nominally 4 KB). Until these clusters are over-written by another file or process the data are recoverable in part or whole. Thus "deleted" personal or sensitive information may be accessible to those with less than honorable intentions.

There are numerous programs and services available to recover "lost" data; for example, **BringBack** (see http://www.toolsthatwork.com/bringback.htm), **Recuva** (see http://www.piriform.com/recuva), **R-Studio** (see http://www.data-recovery-software.net/), **Ontrack Data Recovery** (see http://www.ontrackdatarecovery.com/), **Data Recovery Services** (see http://www.datarecovery.net/), and **ABC Data Recovery** (see http://www.abcdatarecovered.com/)[3]. Of course these tools and services can also be used by individuals seeking to acquire personal information for nefarious purposes.

Baring completely overwriting a disk drive [for example **Darik's Boot and Nuke**, see http://www.dban.org/; **Shredit**, see http://www.mireth.com/pub/siwe.html; and **cyberCide Data Destruction**, see http://www.cyberscrub.com/en/]—and/or physically destroying the drive—how can a user be reasonably assured that sensitive information has been truly deleted?

Below are listed 11 programs that offer secure "cleansing" of deleted files.

Specific Software:

1. See http://www.piriform.com/ for **CCleaner**. For a description and review, also see http://www.brighthub.com/computing/smb-security/reviews/32036.aspx. To quote from this latter site:

   "The most important feature in CCleaner is the option to securely delete the files using different method (sic) and one of the welcome additions in CCleaner's features was

---

[1] © 2010 Lorrin R. Garson.

[2] This discussion pertains only to the Windows operating system.

[3] See http://www.datarecoverycompanies.com/softwareandservices.html for a list of data recovery services and software.

provided earlier this year is the ability to wipe the free disk space in the hard-drive. Such feature is often found in commercial tools only!

"When you first install CCleaner, the program automatically configures to wipe the free disk space of the system drive (Drive C). If you have more than one hard-drive or partition, you should allow CCleaner to wipe also the free disk space of the non-system drives."

See the following for more information:

a. http://answers.yahoo.com/question/index?qid=20100310202948AAPe03D

b. http://www.dooyoo.co.uk/utilities/ccleaner/1040998/

2. See http://www.fileshredder.org/ for **File Shredder**. The following information is from http://www.fileshredder.org/fileshredder-help.php.

> **"Shred Free Disk Space -** This option will shred unused or free disk space across the whole disk volume. For instance, this option is very useful if you haven't shred your unwanted files regularly but instead you used regular windows delete command and now you want your previously deleted files unretrievable (sic). Those files now cannot be shredded by picking them since they are already deleted. This option will enforce shredding of everything you have deleted once using the regular delete command, whether it was yesterday or months ago."

3. See http://www.quickwiper.com/ for **QuickWiper**. To quote from this site:

> "QuickWiper is a disk and file wipe utility that allows you to wipe sensitive files in handy manner (sic). QuickWiper provides you with wipe free disk space function to wipe all previously deleted files, temporary files created by MS Office and other (sic). QuickWiper includes System Clearer that clears in one click Internet Explorer's cookies, history, cache records and typed URLs, temporary and recent files. QuickWiper has several security modes. You can use simple windows deletion, wipe files with single pass wiping or use most secure NSA erasure algorithm."

4. See http://www.cezeo.com/products/disk-redactor/ for **Disk Redactor**. To quote from this site:

> "The functions that Disk Redactor performs are wiping all free unused space on your disks, and writing a big file with zeros to overwrite all old (deleted) files on your drive. After using Disk Redactor, all old data will be erased completely without any chances for its recovery.
>
> "Use Disk Redactor every time you delete files contain your confidential and sensitive data, otherwise this data can be easily recovered."

5. See http://eraser.heidi.ie/ for **Eraser 6.0.7**. To quote from this site:

> "Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Eraser is currently supported under Windows XP (with Service Pack 3), Windows Server 2003 (with Service Pack 2), Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008 R2.

"Eraser is free software and its source code is released under GNU General Public License."

For more information, see:

a. http://www.snapfiles.com/get/eraser.html
b. http://www.esoft.web.id/utilities/eraser-607-stable-secure-deletion-files-folders-and-empty-space.html

6. See http://ezinearticles.com/?How-to-Permanently-Delete-Files---Using-Windows-Secret-Built-In-Tool&id=1145950 on how to use **Cipher**, a Microsoft Windows utility to permanently delete files (among other functions). See the following for more information
   a. http://support.microsoft.com/kb/315672
   b. http://technet.microsoft.com/en-us/library/dd277319.aspx
   c. http://www.windowsecurity.com/articles/Using-cipherexe.html
7. See http://www.winclear.com/?hop=0 for **Winclear** ($37.00) To quote from this site:

   "Securely cleans spare and hidden data areas on your drives. Completely erase the contents of sensitive files and folders that you specify. Support FAT/FAT32/NTFS file systems."

8. See http://www.sneakyclean.com/ for **SneakyClean** ($67.00) To quote from this site:

   "Sneaky Clean works like an electronic shredder on your PC. Working deep below your Windows operating system, Sneaky Clean employs the exact same sector analysis technology as available in ultra-high-priced tools available only to law-enforcement agencies like the FBI. After identifying and analyzing the unwanted data hidden in your drives, Sneaky Clean destroys it with proven methods of secure disposal similar to US Department of Defense standards for destruction of classified material."

9. See http://www.whitecanyon.com/delete-deleted-file.php for **SecureClean** ($39.95). To quote from this site:

   "In order for hard drive data or a computer file to be permanently deleted, the information must be completely overwritten with a product like SecureClean. With SecureClean you can completely eliminate "deleted" computer files from your computer in a matter of minutes. SecureClean makes protecting yourself safe and easy"

   For more information,

   a. http://www.whitecanyon.com/deleted-files-let-10-2003.php
   b. http://download.cnet.com/WhiteCanyon-SecureClean/3000-2092_4-10205696.html
   c. http://www.softpedia.com/reviews/windows/Secure-Clean-PC-Review-40000.shtml
   d. http://www.softsea.com/review/SecureClean.html

10. See http://www.crisystec.com/ for **Crisystec Sentry 3.0** ($99.95/year). Quoting from this site:

    "Securely delete internet history by overwriting the data to a Standard Defeating US Department of Defense file destroying standards, for destruction of classified data, that can stop both software and hardware tools from recovering data. Once data is destroyed with Crisystec Sentry 3.0, it is gone forever and can never be recovered. Cleaning up the history of your activities can be a time consuming process, having to manually remove each history file or entry - and it actually won't help! You Need Crisystec Sentry 3.0."

11. See http://www.cyberscrub.com/topics/previously_deleted_files.php and http://www.cyberscrub.com/en/ for **CyberScrub Privacy Suite 5.1** ($59.95) and other products.

    "It is necessary to wipe files to ensure that previously "deleted" data is (sic) non-recoverable. You may wipe a file securely using a file wiping utility on its initial erasure. In those instances where there exist multitudes of previously deleted data, it will be necessary to wipe the hard drive free space. This will result in such files being destroyed beyond retrieval or forensic discovery. It is also beneficial to use a software program that will scramble file names and other attributes. By performing this additional action, files are not only non-recoverable, but there is no trace of other sensitive identifying information.

    "Privacy Suite file wiping software allows you to wipe files and folders with methods that exceed standards set by the US Department of Defense (US DoD 5220.22). This program can run from command lines, incorporates powerful scheduling capabilities and produces very detailed log file reports. For a full list of features, please visit the Privacy Suite product page. You can also obtain a free, 15-day fully functional trial of the program for your evaluation."

Other Sources of Information:

1. See http://www.snapfiles.com/freeware/security/fwerase.HTML for a list of freeware for file/document shredders and programs that erase deleted files.
2. See http://3d2f.com/tags/dod/overwrite/program/ for a list of 50 "overwrite programs" from feedback@smartcomputing.com.
3. See http://www.redferret.net/?p=9261 for F.R.E.D. (**F**orensic **R**ecovery of **E**vidence **D**evice), which is software used by law enforcement to recover evidence. Priced at $5,999+.
4. See http://www.guidancesoftware.com/computer-forensics-digital-investigation-law-enforcement.htm? for Guidance Software's forensic tools (enCase). "Technology solution for capturing, analyzing and reporting on digital evidence"

Last printed: 15 July 2010 at 3:00 PM

Last modified (saved): 15 July 2010 at 3:00 PM

C:\Users\Lorrin\Documents\Computer Notes\Sought After Solutions\Truly Deleting Files.docx