Global Information Assurance Certification Paper

Secure File Deletion, Fact or Fiction?

Submitted by

John R. Mallery

GSEC Practical Assignment
Version 1.2e

7/16/01

”In short, the average computer is about as secure as a wet paper bag, and it is one of the last places where you would want to hide valuable data or use to communicate secret or sensitive information.”

Rick Maybury
Bootcamp week 182: Email and PC security
Connect
July 5, 2001

Introduction

Computers have changed the way people communicate and conduct business. Word processors, spreadsheets, e-mail, instant messaging, chat have become part of daily life. With the creation and growth of the Microsoft Windows Operating Systems, the ability to utilize these tools no longer requires college degrees or the ability to program. Application interfaces have become intuitive and once you have mastered one application, other applications perform and operate similarly. From a user’s standpoint, applications create files that are stored on the hard drive or removable media. When the user no longer needs a particular file, the user deletes it and moves on. As far as the user is concerned any information contained in that file is gone forever, unable to be recovered by the user. However, because of the way operating systems and applications work, that file may be recoverable and if that file is not recoverable, the data it contained may be found in other files. The reason for this is that in order to function properly, operating systems and applications create additional files or write data to the hard drive. All of this is done without the user’s knowledge. From a privacy and corporate security standpoint, it is important to know about these additional files. These files may contain remnants of proprietary data, research and development projects, confidential memos, merger and acquisition information, financial data, customer information etc. Although these files may not be viewable or recoverable by the user, they can be recovered utilizing computer forensics tools (or simply viewed using a tool such as Norton’s Disk Edit).

This paper will deal with how and where some of these files are created and how to securely remove them from a system. Microsoft Windows operating systems and associated applications will be the main focus. This paper is divided into two main sections, the first section is designed to be a primer on the types of information that can be found on a hard drive. It is not designed to be a fully detailed data recovery/computer forensics tutorial, but is designed to show security professionals how much information can be found on a hard drive. The second section deals with the concepts behind securely deleting files and associated data from a hard drive.

Files Users Don't Intentionally Create

Windows Swap and Page Files

When Microsoft Windows-based operating systems need additional random access memory, they utilize "virtual memory" by using the hard drive as a memory area. In Windows, Windows 95 and Windows 98, this storage area is called the Swap File. In Windows NT and 2000 this file is called the Page File but functions the same as the Swap File. Swap files can range in size from 20 million bytes to over 200 million bytes and can contain an incredible amount of information. Anything from a Windows session can be contained in a swap file – remnants from any application – word processing, databases, spreadsheets, Internet activity etc. can be found in a Windows Swap File. What makes the Swap File such a dangerous source for losing proprietary information is that it is dynamic, and every time Windows is started, a new swap file is created. Because of this multiple swap files could still exist on a hard drive. This is valuable information for a computer forensics analyst looking for evidence of a crime, but is frightening to a corporate security professional trying to prevent the loss of proprietary data. There are ways to minimize the risk created by Windows Swap and Page Files, these will be covered in the "Ways to Eliminate Proprietary Data" section of this paper.

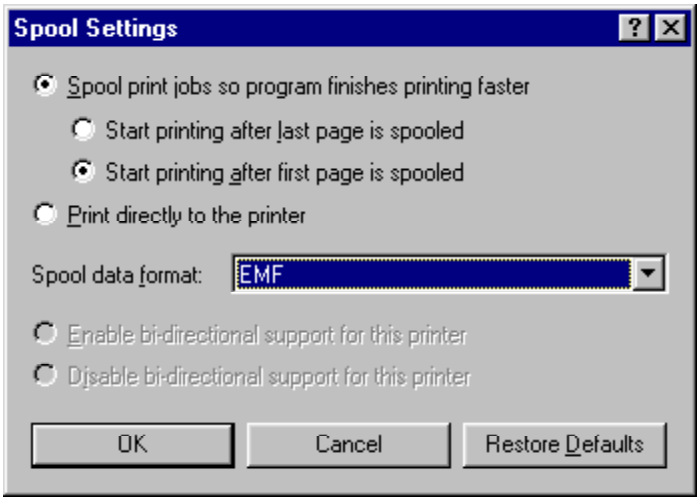
Temporary Files

In an effort to improve performance and efficiency, many applications create temporary files. Microsoft Knowledge Base Article Q211632 accurately describes temporary files, " A temporary file is a file that is created to temporarily store information in order to free memory for other purposes, or to act as a safety net to prevent data loss when a program performs certain functions." These temporary files remain open as long as the application needs them. When the application is shut down, these files are deleted, but the data they contained still remains on the hard drive. How many temporary files are created by an application? This depends on the application but Microsoft states that both Word 97 and Word 2000 create 15 temporary files during use.[1] An important concept to remember about temporary files is that the data they contain remains on the hard drive (until it is overwritten), even if the original file (document, spreadsheet, etc.) is not saved to the drive.

Printer Spool Files

In Microsoft Windows the default setting for printers is to "Spool print jobs so program finishes printing faster." (see screen shot on next page)

[1] Microsoft Knowledge Base Articles Q89247 and Q211632



Spool is an acronym and stands for "simultaneous peripheral operations online". The significance of spooling is that the application sends the file to the hard drive first and then to the printer. Because the file is copied to the hard drive, the data it contains will remain on the drive until it is overwritten. A key security concept to remember is that even if the file is never saved, but only printed, it may be possible to recover the data in the original document. These files can be recovered using forensics tools and then viewed using an image viewer that supports enhanced metafiles (notice the data format in the screen shot).

Metadata

Metadata can be described simply as "data about data". Although metadata is not a separate file, the data it contains is created automatically by Microsoft Office products. Understanding what is contained in metadata provides another reason to verify that sensitive files are completely removed from a drive. From a security standpoint, metadata may contain information that should not be shared outside of an organization. What can be found within Metadata? According to Microsoft Knowledge Base article Q223790 the following are examples of metadata that can be stored in documents:

- Your name
- Your initials
- Your company or organization name
- The name of your computer
- The name of the network server or hard disk where you saved the document
- Other file properties and summary information
- Non visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions
- Document versions

- Template information
- Hidden Text
- Comments

If metadata is not controlled, sensitive internal information can be disseminated outside of an organization. The previously mentioned Knowledge Base article, Q223790, mentions steps used to minimize metadata. The Payne Consulting Group of Seattle, Washington has a product, "Metadata Assistant" that claims to "identify, display and remove" metadata contained in Word 97, 2000 and 2002 documents. (The product was not reviewed for this paper, additional information can be found at: http://www.payneconsulting.com/public/products/ProductDetail.asp?nProductID=7)

Deleted Files

It has become common knowledge that "delete does not mean delete", however, what really happens when a file is deleted? When a file is created, a directory entry for that file is also created. When a file is deleted and not sent to the recycle bin, the first letter of the filename in the directory entry is changed to a special character (Hexadecimal E5). All entries for that file in the File Allocation Table are then cleared. The data contained in the file remains on the hard drive until it is overwritten. Theoretically, this data could remain on the hard drive forever.

Finding Deleted Files

It has been established that the data contained in deleted files remains on the hard drive. Where are they located? How can they be viewed? How can they be recovered? All the data on the drive can be viewed using a tool such as Norton Utilities Disk Edit. From an "oops" I would like to get that file back standpoint undelete tools exist that may be able to retrieve a deleted file. Software Shelf International's File Rescue 2.5, Que Tek Consulting's File Scavenger 1.4 and CC Technology International's Recover NT 3.5 are stand alone utilities that claim to be able to recover deleted files. Directory Snoop from Briggs Software has an unerase feature and Symantec's Norton Utilities and On Track's System Suite 2000 include undelete tools. It is important to remember that files can be recovered only if they have not been overwritten.

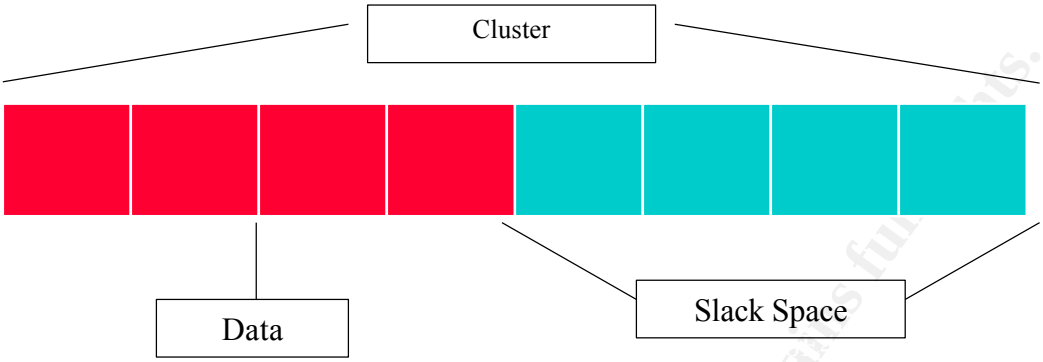
Finding Data

It has been established that there is a large amount of data on a hard drive that a user does not create. It may not be visible through standard interfaces, but can be found in several locations, including ***slack space*** and ***unallocated space.*** It is important to understand these terms, since overwriting data in these areas is one of the keys to preventing data from being recovered.

Slack Space

Windows operating systems use fixed sized clusters to store data. An entire cluster is used even if

the data being stored does not fill the cluster. The space between the end of the file and the end of the cluster is called slack space. A visual representation might look like this:



Using this concept, if a cluster is filled with data, and then the cluster is only partly overwritten, the data in slack space is recoverable. It can be viewed and recovered using a tool such as Norton Utilities DiskEdit, but is more efficiently recovered using forensics' tools such as NTI's GetSlack and Guidance Software's EnCase.

Unallocated Space

Unallocated space (more accurately, unallocated clusters) can be defined as clusters that are not currently allocated by the Operating System or File Allocation Table. Essentially, unallocated space contains all of the deleted files (among other types of files) on the drive that have not yet been overwritten. Once again, this data can easily be recovered using forensics' tools such as EnCase and NTI's GetFree.

Now that it has been established that a computer hard drive can contain a wealth of information, how can a security professional insure that corporate laptops are not leaving with unprotected proprietary information, donated computers are free from confidential records and that no documents, e-mails, memos can be uncovered and used against a corporation in a lawsuit? The next section will contain the steps to reduce the risk of loss of proprietary information.

Securely Deleting Files

It has been established that deleted files can be recovered. Is it possible to delete a file (and its associated files, temporary, spooler, etc.) so that it cannot be recovered? There are rumors that government agencies have the capabilities to recover data that has been overwritten as many as 21 times. From a corporate perspective, an individual will have to determine the value of his data and determine the steps that can be considered "reasonable and practical" to prevent proprietary data from being stolen or recovered by competitors or groups intent on corporate espionage. The main premise for preventing data from being recovered is to overwrite it. The question becomes how many times should it be overwritten? There are individuals that believe that overwriting data only one time is sufficient to prevent the recovery of deleted files. However, the more the data is overwritten, the less likely it becomes recoverable by any means. For a drive currently in use, it is necessary to overwrite slack space and unallocated space. There are a variety of tools available to

perform this task (some of which will be described later). These tools use one of three overwrite methods:

Single Pass – data area is overwritten once with either 1's, 0's or pseudorandom data

DoD Method – the data area is overwritten with 0's, then 1's and then once with psuedorandom data. Many tools use variations of this, overwriting as many as seven times, using three alternating passes of 0's and 1's following by one pass of psuedorandom data. This is based on standards outlined in the Department of Defense Manual 5220.22 M, also known as the National Industrial Security Program Operating Manual or NISPOM. This manual outlines the steps to both "clear" and "sanitize" a "rigid non-removable disk". To clear a disk it states that you must "overwrite all addressable locations with a single character." To "sanitize" a disk you must do one of the following:

- Degauss with a Type I degausser (degaussing exposes the drive to an electromagnetic field)
- Degauss with a Type II degausser
- Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS TOP SECRET INFORMATION.
- Destroy - Disintegrate, incinerate, pulverize, shred, or smelt.[2]

Guttman Method – the data area is overwritten 35 times. This method uses psuedorandom data to overwrite the drive and overwrites the drive taking into account the different encoding algorithms used by various hard drive manufacturers, RLL (run length limited), MFM (modified frequency modulation), PRML (partial-response, maximum-likelihood). This method of overwriting data was created by Peter Guttman, and is described in his paper, "Secure Deletion of Data from Magnetic and Solid State Memory."

It is important to note that the consensus is that overwriting the data only reduces the likelihood of data being recovered. The more times data is overwritten, the more expensive and time consuming it becomes to recover the data. In fact Peter Guttman states "…it is effectively impossible to sanitise storage locations by simple overwriting them, no matter how many overwrite passes are made or what data patterns are written."[3] Overwritten data can be recovered using magnetic force microscopy, which deals with imaging magnetization patterns on the platters of the hard disk. The actual details of how this is accomplished are beyond the scope of this paper.

Disk Wiping Utilities

There are numerous disk-wiping utilities available. Sarah Dean's web site, "Disk and File Shredders: A Comparison," lists 34 utilities, and the list is not comprehensive. Some security sites recommend using a "file shredding" utility which overwrites the file when it is deleted. This only prevents the original file from being recovered, as has been described earlier, the data the

[2] NISPOM, pages 77-78 (pdf file)
[3] Guttman, p. 13

original file contained can be recovered elsewhere. Instead of using a file shredding utility, it is recommended that the file be deleted by bypassing the recycle bin (by hitting "shift + delete" instead of just "delete") and then overwrite slack space and unallocated space on a regular basis. Details on the actual steps for securely removing data will be outlined later.

The author had the opportunity to examine several disk-wiping utilities, they all appeared to function the same way. The tools that seemed the easiest to use, understand and had the most features include Eraser and WipePro+ (both are freeware, with a small fee charged for commercial use). They both offer single pass, DoD and Guttman wiping options. They also include a tool for wiping the swap file (The swap file can only be overwritten from within DOS, not a DOS window. Some wiping utilities claim to be able to wipe the swap file from within Windows, but it is very difficult, if not impossible to overwrite a file that is in use.). WipePro+ also includes an "Information Center" which is an excellent source of information on disk wiping concepts. Another useful tool is Msweep from computer forensics experts, NTI. This is a DOS based tool and is very efficient. It allows you to overwrite slack space and unallocated space and includes information on how to create a script file that will delete temp files and clean slack space before overwriting begins. For additional information on these tools visit the following sites:

Eraser - http://www.tolvanen.com/eraser/
WipePro+ - http://www.marcompress.com/AboutWipePro.htm
Msweep - http://www.secure-data.com/ms.html

For a list of additional wiping utilities see Appendix A.

Windows Swap and Page Files

Because so much information can be found in the Windows swap and page files, it is important to overwrite these areas as well. In Windows NT and 2000 it is possible to edit the registry to allow the page file to be cleared at shutdown. To clear the page file at shutdown, complete the following steps:

- Start Registry Editor (Regedt32.exe)
- Change the data value of the ClearPageFileAtShutdown value in the following registry key to a value of 1:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ Memory Management

  If the value does not exist, add the following value:

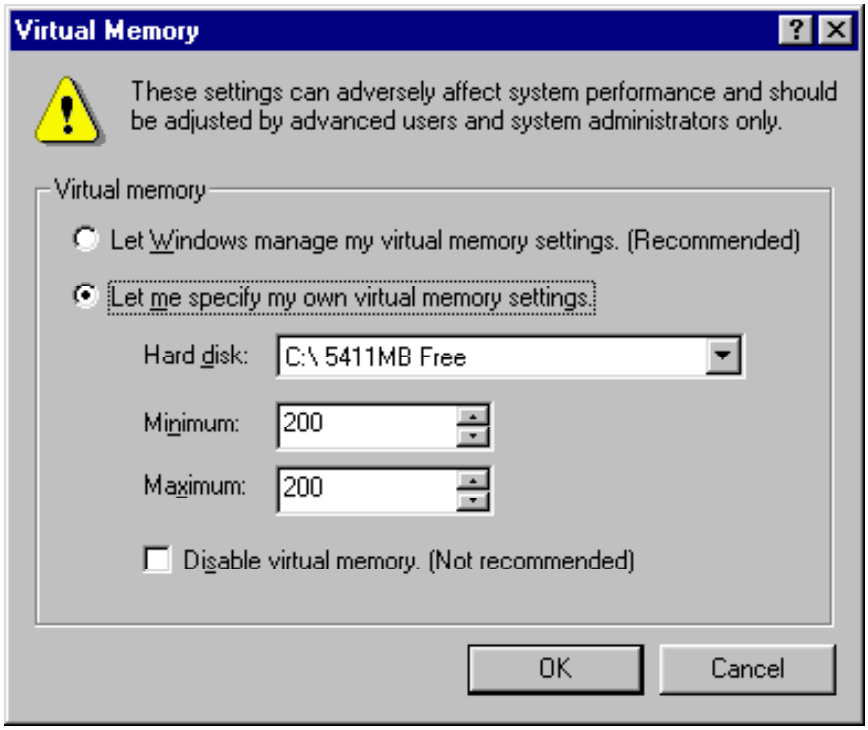
  Value Name: ClearPageFileAtShutdown Value Type: REG_DWORD Value: 1

This change does not take effect until you restart the computer.[4]

With Windows 9x there is no automated method to clean the swap file. Several things must be completed before the swap file can simply and easily be cleaned. The default setting for Windows 9x systems is to let the operating system control the size and location of the swap file, Win386.swp. With this setting the swap file is dynamic, it's size and location changes depending

[4] Microsoft Knowledge Base, Q182086

on the needs of the system. To be able to securely overwrite the swap file, you must specify a specific size for the swap file. This will keep it in the same location, so multiple copies of the swap file do not exist on the drive. In order to do this you should go to "Control Panel", "System", click on the "Performance" tab and then "Virtual Memory" You will see the following screen:



Select the "Let me specify my own virtual memory settings" option. Then set the Minimum and Maximum options to be the same. There is some question as to the appropriate size for the swap file, a good starting point would be 64MB. If system performance is poor or you constantly receive out of memory messages, you can gradually increase the size of the swap file. You will be asked to restart your computer after making changes.

Once you have set a fixed size to the swap file, you can then boot to DOS and run a swap file wiping utility. Using a DOS boot disk with the utility installed will work as well. Eraser, WipePro+, BCWipe all include swap file overwriting tools.

Steps to Securely Remove Files and Associated Data from a hard drive

1. Delete files.
2. Delete all temporary files.
3. Defrag hard disk
4. Run File wiping utility to overwrite slack and free space.
5. Defrag hard disk
6. Run swap file utility.

Thoughts and Considerations

The steps outlined above make the process look fairly simple. But there are some issues to consider. With the large disk drives in use today, this process can be exceptionally time consuming. The biggest consideration is which file wiping method will be used, Single Pass, DoD or Guttman. The more overwrites, the longer the process. Running Msweep set to overwrite slack and free space once on a system with 7GB of free space, takes approximately 30 minutes. Running Gregory Braun's Disk CleanUp 2000 set to the NSA option (Guttman) takes over 10 hours.

The value and sensitivity of the information contained on a hard drive will determine the number of overwrites necessary and the frequency that the overwrites are performed. A salesmen's laptop may only need to be "cleaned" once a month, whereas an R&D laptop may need to be "cleaned" everyday. An acceptable level of risk will have to be determined by the corporation.

One way to reduce the time it takes for these procedures is to run Defrag on a regular basis, the more frequently it is run, the less time it takes to run. On a drive that does not contain proprietary or confidential information, step number 3 can be eliminated.

It is important to remember, if a hard drive is being discarded and it contained proprietary information, the only sure way to prevent the data from being recovered is to destroy the drive.

Appendix A

Utilities

Disk Wiping Utilities

BCWipe - http://www.jetico.com/index.htm#/bcwipe.htm
Directory Snoop (includes disk wiping utility) - http://www.briggsoft.com/dsnoop.htm
Disk CleanUp 2000 - http://www.gregorybraun.com/CleanUp.html
Eraser - http://www.tolvanen.com/eraser/
M-Sweep - http://www.securedata.com/ms.html
PGP Wipe (included with PGP) - http://web.mit.edu/network/pgp.html
RMD - http://www.dmares.com/maresware/ps.htm#RM
WipePro+ - http://www.marcompress.com/
Wipe Info (included with Norton Utilities) - http://www.symantec.com
With Out a Trace - http://www.karmadromesoft.com

Undelete Tools

File Rescue - http://www.file-rescue.com/
File Scavenger - http://www.quetek.com/prod01.htm
Recover NT - http://www.lc-tech.com/RecoverNT.asp
Undelete - http://www.executive.com/undelete/undelete.asp

References

Dean, Sarah. “Disk and File Shredders: A Comparison.” 19th May 2001. URL: http://www.fortunecity.com/skyscraper/true/882/Comparison_Shredders.htm

Department of Defense. “National Industrial Security Program Operating Manual” URL: http://www.dss.mil/isec/nispom.htm (http://www.dss.mil/isec/nispom.pdf) (7/10/01)

Erdelsky, Philip J. “A Description of the DOS File System.” 15 January 1993. URL: http://www.alumni.caltech.edu/~pje/dosfiles.html (7/11/01)

Guttman, Peter. “Secure Deletion of Data from Magnetic and Solid-State Memory.” URL http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html. (7/13/01)

Mace, Paul. The Paul Mace Guide to Data Recovery. New York: Brady, 1988. P. 43

Maybury, Rick “Bootcamp week 182: e-mail and PC Security.” Connected. 5 July 2001 http://www.telegraph.co.uk/connected?ac=005455317051464&rtmo=LSGit3Nd&atmo=rrrrrrrq&pg=/et/01/7/5/ecrcomp05.html (7/12/01)

Microsoft, Inc. “WD 2000: How Word for Windows Uses Temporary Files.” URL: http://support.microsoft.com/support/kb/articles/Q211/6/32.ASP (7/10/01)

Microsoft, Inc. “WD 97: How Word for Windows Uses Temporary Files.” URL: http://support.microsoft.com/support/kb/articles/Q89/2/47.ASP (7/10/01)

Microsoft, Inc. “How to Clear the Windows NT Paging File at Shutdown.” URL: http://support.microsoft.com/support/kb/articles/q182/0/86.asp (7/13/01)

New Technologies, Inc. “Windows Swap File Defined.” URL: http://www.forensics-intl.com/def7.html (7/10/01)

Webopedia. “Slack Space” URL: http://webopedia.lycos.com/TERM/S/slack_space.html (7/11/01)

WhatIs.Com. “Simultaneous Peripheral Operations Online” URL: http://whatis.techtarget.com/definition/0,289893,sid9_gci214229,00.html (7/10/01)

ZDNet.com “Create a Swap File” URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2388433-4,00.html (7/13/01)