Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure File Deletion: Fact or Fiction?

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 fou...

Copyright SANS Institute
Author Retains Full Rights

AD

Secure File Deletion: Fact or Fiction?

John R. Mallery
7/16/01, Updated 6/12/06

GSEC Practical Assignment, Version 1.2e

"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

Preface

This paper covers various aspects and details of secure file deletion. If you'd like to learn more about how to secure or delete your data permanently as well as other computer security topics, we recommend taking the SANS SEC401 Security Essentials Course.

Introduction

Computers have changed the way people communicate and conduct business. Word processors, spreadsheets, e-mail, instant messaging, and 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 knowing how to program. Application interfaces have become intuitive; 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 creates 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

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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 rather 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 That 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, 2000, and XP 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. How to minimize the risk created by Windows Swap and Page Files will be covered in "Ways to Eliminate Proprietary Data".

Temporary Files

In an effort to improve performance and efficiency, many applications create temporary files. Microsoft Knowledge Base Article 211632 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 remain on the hard drive (until it is overwritten), even if the original file (document, spreadsheet, etc.) is not saved to the drive.

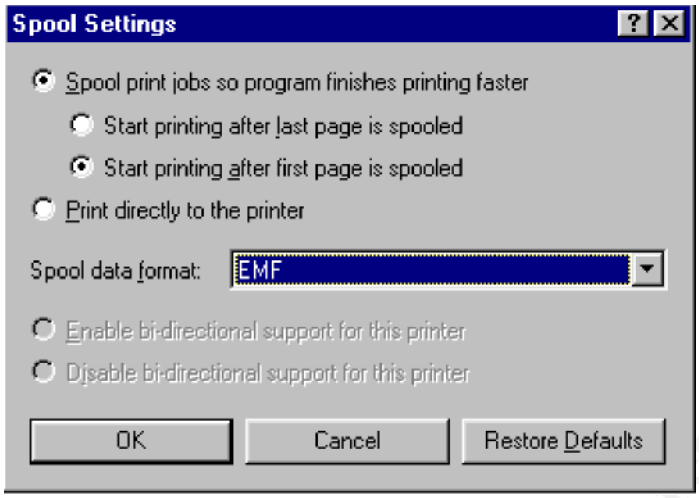
---

[1] "Description of how Word creates Temporary Files - http://support.microsoft.com/kb/211632/EN-US/

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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)



Spool is an acronym that 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 is 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 article 223396[2] 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

[2] "How to minimize metadata in Office Documents - http://support.microsoft.com/default.aspx?scid=kb;en-us;223396

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- 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. Knowledge Base article 22396 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 documents (the product was not reviewed for this paper. Additional information can be found at: http://www.payneconsulting.com/products/).

Another popular metadata removal tool is iScrub from Esquire Innovations, Inc., http://www.esqinc.com/products_iscrub.asp. Metadata has become such a significant concern that Microsoft has created the Remove Hidden Data Add-In for Office 2003/XP which can be downloaded from http://tinyurl.com/3u5tw. To understand the significance and impact of metadata, one should read Judge Waxse's memorandum and order in the *Williams v. Sprint* case, where a party used iScrub to remove metadata against a judge's order.[3]

Deleted Files

While it has become common knowledge that "delete does not mean delete", 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 remain on the hard drive. Where are they located? How can they be viewed? How can they be recovered? All the data

---

[3] *Williams v. Sprint*, September 29, 2005 Memorandum and Order - http://www.ksd.uscourts.gov/opinions/032200JWLDJW-3333.pdf.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

on the drive can be viewed using a tool such as Norton Utilities Disk Edit or any Hex Editor. From an "oops, I would like to get that file back" standpoint, numerous undelete tools exist that may be able to retrieve a deleted file. Several free computer forensics related tools will allow you to recover deleted files. WinHex,[4] which is actually a hex editor on "steroids," will allow you to recover deleted files as well as ProDiscover Basic[5] from Technology Pathways; Directory Snoop[6] from Briggs Software has an unerase feature and Symantec's Norton Utilities and Ontrack's EasyRecovery include undelete tools. Another popular tool is Recover My Files from GetData. It is important to remember that files can be recovered only if they have not been overwritten. A screenshot of Ontrack's EasyRecovery DataRecovery tool can be seen below.

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

---

4 WinHex - http://www.x-ways.net/winhex/index-m.html

5 ProDiscover Basic – http://www.techpathways.com

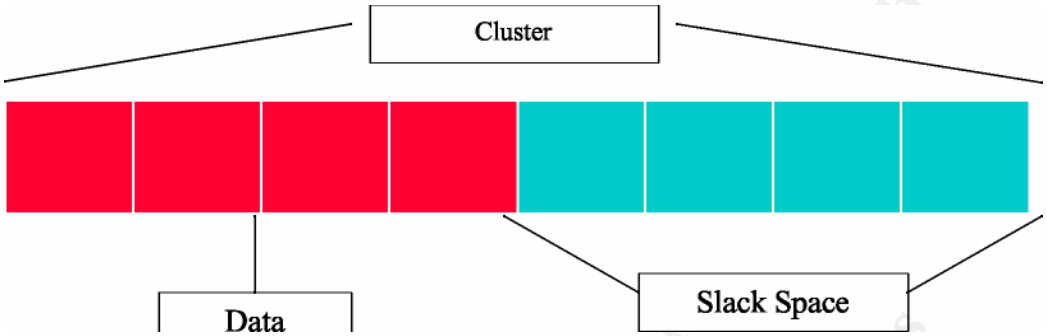
6 Directory Snoop - http://www.briggsoft.com/dsnoop.htm

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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 forensic tools such as NTI's GetSlack[7] and Guidance Software's EnCase.[8]

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 forensic tools such as EnCase, WinHex, NTI's GetFree[9] and DataLifter File Extractor Pro.[10]

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 describe the steps to reduce the risk of loss of proprietary information.

---

7 GetSlack - http://www.forensics-intl.com/getslack.html

8 EnCase – http://www.guidancesoftware.com

9 GetFree - http://www.forensics-intl.com/getfree.html

10 DataLifter File Extractor Pro - http://www.datalifter.com/products.htm

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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 capability 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 who 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 several overwrite methods:

Single Pass – data area is overwritten once with either 1's, 0's or pseudo-random data.

DoD Method – the data area is overwritten with 0's, then 1's and then once with pseudo-random data. Many tools use variations of this, overwriting as many as seven times, using three alternating passes of 0's and 1's and following by one pass of pseudo-random 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.[11] 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 CONTAIN TOP SECRET INFORMATION.
- Destroy –Disintegrate, incinerate, pulverize, shred or smelt.

Royal Canadian Mounted Police Technical Security Standard for Information Technology, Appendix OPS-II – Media Sanitization. This standard, normally abbreviated as RCMP TSSIT OPS-II, states that "One approved method used to declassify media is to write over every addressable location first with one pattern, usually binary "one" digits, and then with the complementary pattern, in this case, binary "zero" digits. This cycle of overwrite

[11] NISPOM - http://www.usaid.gov/policy/ads/500/d522022m.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

is then repeated alternately for a minimum of three cycles. After the overwrite has been accomplished, unclassified random data should be written in all data locations on all tracks of the disk and left there."[12]

NAVSO P5239-26. The Department of the Navy Remanence Security Guidebook states that for "Some magnetic data storage media may be purged by overwriting all data storage locations first with a data pattern, then with the data pattern's complement, then with a random pattern which will be subsequently verified (per DoD 5200.28-M). The procedure should force the magnetic fields at every addressable location on the data storage media to both polarities. The overwrite program should write to file allocation tables, directories, block maps, active and inactive (unused) file space, and to the space between the end of a file and the end of the sector or block where it resides. It should write to bad and spare sectors and tracks (including those removed from standard addressing). CAUTION: Ensure the read/write device hardware is functioning properly before beginning this procedure."[13] This is essentially the Navy's interpretation of the Department of Defense standards. Both the Army and Air Force have similar documents, AR380-19 and AFSSI-5020 respectively.

Pseudo-random Number Generator (PRNG). This is a method of generating a stream of pseudo-random numbers that are used to fill the target hard drive. The term pseudo-random is used because there are mathematicians who believe that a true random pattern generator does not exist. To learn more about PRNG visit http://en.wikipedia.org/wiki/Pseudo-random_number_generator.

Guttman Method. The data area is overwritten 35 times. This method uses pseudo-random 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."[14]

It is important to note the consensus 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 sanitize storage locations by simple overwriting them, no matter how many overwrite passes are made or what data patterns are

---

12 RCMP TSSIT OPS-II -http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/tssit97_e.pdf.

13 NAVSO P5239-26 - http://tinyurl.com/h7fbc

14 "Secure Deletion of Data from Magnetic and Solid State Memory" - http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Disk Wiping Utilities

When this paper was initially submitted and published, there were probably several dozen well-known wiping utilities. But as more and more stories appeared in the media about supposedly deleted data being recovered causing embarrassment and legal issues, even more wiping utilities have been created. Many very useful wiping utilities are now available for free. In fact Microsoft has included the ability to wipe data with their command line tool cipher.exe as far back as June of 2001. Cipher.exe is used to manage the Encrypted File System and is available with Windows 2000 Service Pack 3 or later and Windows 2000 Security Rollup Package 1 (SRP1) and Windows XP Professional.

How to Use Cipher.exe

To overwrite the deallocated data:

1. Quit all programs.
2. Click Start, click Run, and type cmd, and then press ENTER.
3. Type cipher /w:'folder', and then press ENTER, where folder is optional and can be any folder in a local volume that you want to clean. For example, the cipher /w:c:\test command causes the deallocated space on drive C: to be overwritten. If c:\test is a mount point or points to a folder in another volume, deallocated space on that volume will be cleaned."[15]

Another popular, free, command line tool is sdelete[16] from SysInternals. "In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk."

While cipher and sdelete allow you to "cleanse free space" they do not provide the ability to wipe "slack space." A free tool (donations accepted) that is very robust and allows you to wipe free space (more accurately called "unallocated clusters") as well as slack space (also called "cluster tips") is Eraser.[17] In addition, it includes the ability to configure your system to wipe the page file at shutdown. It includes a scheduler to allow you to schedule how frequently you would like the program to run. It is a well-designed and easy to use application.

Commercial tools

There are very few stand-alone wiping tools. WipePro+[18] is one of the few straight wiping tools available. It includes a tool to wipe the Windows 9x swap file, but appears

---

15 Microsoft Support article 298009, "Cipher.exe Security Tool for the Encrypting File System," http://support.microsoft.com/default.aspx?scid=kb;en-us;298009&sd=tech

16 s-delete - http://www.sysinternals.com/Utilities/SDelete.html

17 Eraser - http://www.heidi.ie/eraser/

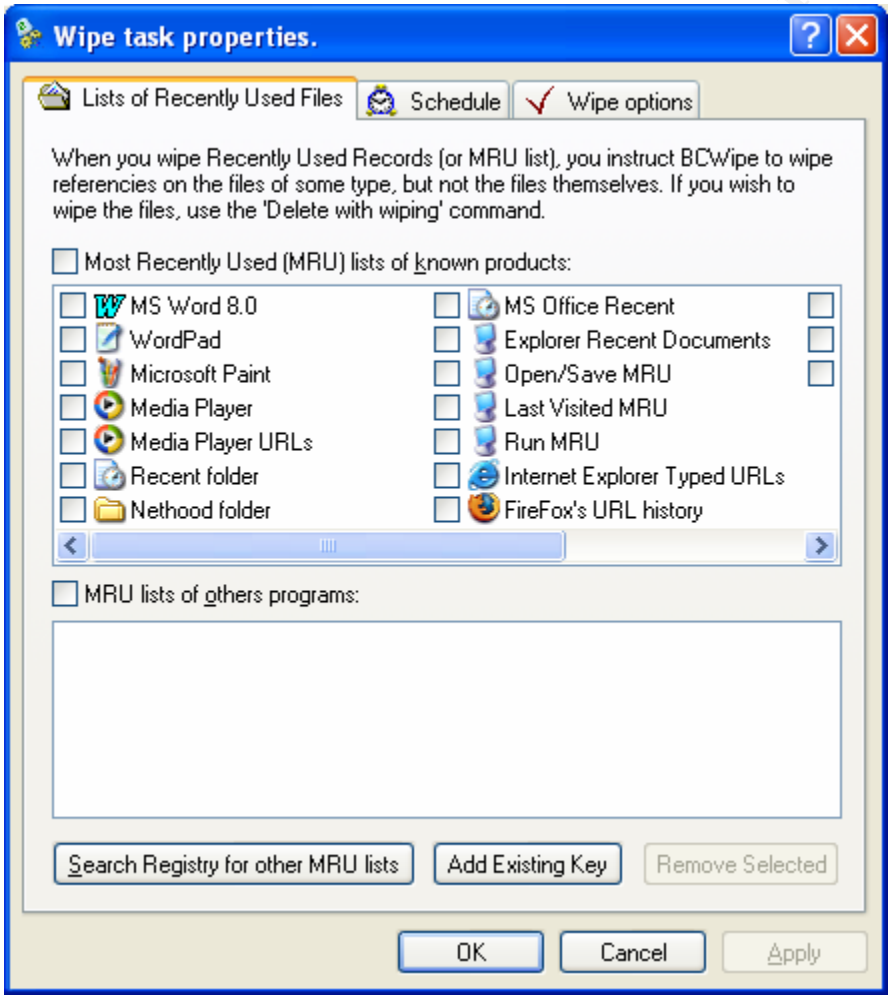
18 WipePro+ - http://www.marcompress.com/AboutWipePro4.htm

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

to only wipe free space, not slack space. WipePro+ also includes an "Information Center" which is an excellent source of information on disk wiping concepts.
A very good command line tool that will wipe slack space and free space is Rm written by Dan Mares.[19]

Disk wiping is now a part of most, if not all "Privacy Tools," which are designed to not only wipe free space and slack space, but also to remove evidence of a variety of computer activities. BCWipe[20] now provides the ability to remove references to a wide range of "Most Recently Used" (MRU) files as well as browser history as seen in the screenshot below.

It also includes a tool, "Cryptoswap" which is "…intended to encrypt Windows Swap File."



[19] Rm - http://www.maresware.com

[20] BCWipe – http://www.jetico.com

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The Cyberscrub Privacy Suite[21] (formerly Cyberscrub Professional Suite) includes what they call a "Privacy Guard" which provides the ability to remove a wide range of computer activities including Internet activity, MRU listings, Newsgroup activity and Peer to Peer activity.

Physical Disk Wiping

The tools mentioned above are designed to be used on computers that are actively in use. But what tools should be used if a computer or hard drive is going to be discarded, donated or sold, and you want to remove all data, including the operating system and the applications? There are tools available that will "wipe" the entire physical drive. This will remove all data including the partitions. As with the previously mentioned disk wiping tools there are several free tools that are commonly used.

One of the most well known tools for physical disk wiping is the tool "dd" which is a standard command line tool in Unix and Linux. The basic command to wipe a drive is:

```
dd if=/dev/zero of=/dev/hda
```

This will fill the target drive with zeros. In personal communications with Thomas Rude (better known as Farmerdude), he explained that using this particular syntax would utilize the default block size of 512 bytes, which would make the process extremely slow, he recommends trying a block size of 8192 as a good starting point (you can try different block sizes, as long as they are a multiple of 512). So this would make the syntax:

```
dd if=/dev/zero bs=8192 of=/dev/hda
```

To make the process even more efficient, add the flag, "conv=noerror" so that dd will keep going despite any I/O errors. This would make the complete syntax:

```
dd if=/dev/zero bs=8192 conv=noerror of=/dev/had
```

If you would like to fill the drive with random characters you can use `if=/dev/random.`

While dd is available in all distributions of Linux, it is important to recognize that it can be found on many Linux boot CD distributions. While these boot CD's are free, they can be "buggy." For this paper a random sampling of ISO's for five Linux boot CD's were downloaded. One of the ISO's could not be burned to CD. Three others would not boot into a usable environment. Only one, Frenzy,[22] booted successfully. "Frenzy is a "portable system administrator toolkit," LiveCD based on FreeBSD. It generally contains software for hardware tests, file system check, security check and network setup and

---

[21] Cyberscrub Privacy Suite - http://www.cyberscrub.com/products/privacysuite/index.php

[22] Frenzy - http://frenzy.org.ua/eng/

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

analysis. Size of ISO-image is 200 MBytes (3" CD)." If you would like to try to find a Linux boot CD that meets your needs and will work on your system, visit FrozenTech's LiveCD list which lists 309 Live CD/DVDs.[23] If you would like to take some of the guesswork out of the process it may be worth trying a commercially available boot CD, such as the Farmer's Boot CD.[24]

An extremely popular physical disk wiping tool is Darik's Boot and Nuke which is a self-contained boot floppy that provides multiple options for wiping a physical disk. It comes with the wiping tool previously mentioned, Eraser, or it can be downloaded from http://sourceforge.net/projects/dban. It is a SYSLINUX based boot floppy.

Sterilize[25] is another free wiping tool that was designed to sterilize computer media in preparation for use in computer forensics examinations. It is a DOS based tool and is designed to run from a DOS boot floppy.

Because computer forensics examiners must create forensically sound media for their examinations, all computer forensics tools provide the ability to wipe an entire physical drive. While nearly all computer forensics tools are available for a fee, there is one that is free and includes disk-wiping functionality. The tool is ProDiscover Basic and can be downloaded from the Technology Pathways website.[26]

Commercial Physical Disk Wiping Tools

There are several commercially available physical disk-wiping tools. As mentioned earlier, all computer forensics tools include drive wiping functionality. AccessData, the developers of the Forensic Tool Kit, has a utility called WipeDrive.[27] Maresware has the tool, Declasfy.[28] Ontrack DataRecovery has the tool DataEraser.[29] An excellent tool that is reasonably priced and fairly fast (depending on the system on which it is used), is Wiper,[30] from Key Computer Service, Inc. It is a DOS based tool and runs from a boot floppy. It is extremely simple to use and meets many of the specifications mentioned earlier.

---

23 Frozen Tech's LiveCD List - http://www.frozentech.com/content/livecd.php

24 Farmers Boot CD - http://www.forensicbootcd.com/

25 Sterilize - http://www.cybersecurityinstitute.biz/software/

26 ProDiscover Basic - http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14

27 WipeDrive - http://www.accessdata.com/products/wipe/

28 Declasfy - http://www.maresware.com/maresware/df.htm#DECLASFY

29 DataEraser - http://www.ontrack.com/dataeraser/

30 Wiper - http://www.keycomputer.net/soft-hard.htm?

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Verification

There are numerous disk-wiping tools available, and many of them will securely remove data from a hard drive or other storage medium so that it is irretrievable. Regardless of what tool you are going to use, it is important to verify that it performs as promised. Many of these tools are marketed based on people's paranoia and lack of understanding of technology. A marketing pitch from the Evidence Eliminator Web site[31] requests that you, "Protect Your Job, Property, Family, Car, Friends and Your Reputation - Before It's Too Late!" (car? friends?). Testing the tool can be done by running the tool and then examining your system using the hex editor of your choice. Win-Hex is a good choice. If you are wiping an entire hard drive, simply specify a specific character with which to wipe the drive, then after the wiping is complete, use a hex editor and search for all characters other than the one you specified. If nothing is found, the tool performs as promised. It is important to validate your tool with a secondary source. Many wiping tools include the capability to verify that it performed correctly, but it is a best practice to test with a tool other than the one used to conduct the wiping. Although the site is a little out of date, Sarah Dean's web site, "Disk and File Shredders: A Comparison"[32] discusses some options for comparing various tools.

A listing of wiping tools can be found in 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, 2000 and XP, 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:

1. Start Registry Editor (Regedt32.exe)

2. 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
3. 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.[33]

---

31 Evidence-Eliminator – http://www.evidence-eliminator.com

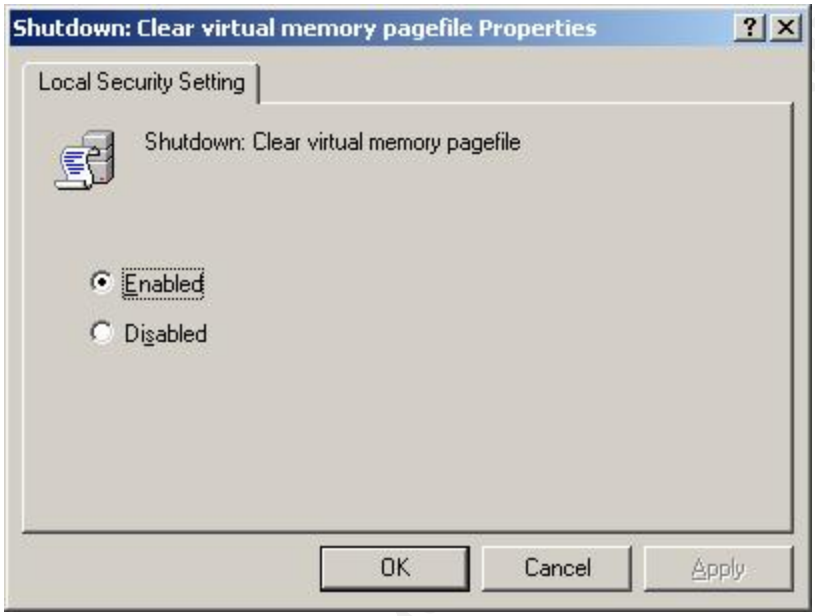
32 "Disk and File Shredders: A Comparison" - http://www.sdean12.org/Comparison_Shredders.htm

33 Microsoft Support Article 314834, "How to Clear the Windows Paging File at Shutdown," - http://support.microsoft.com/?kbid=314834

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

In Microsoft Windows XP Professional you can configure the system to clear the page file at shutdown by configuring the local security policy. This can be accomplished by going to:

Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Options | Shutdown: Clear virtual memory Page File | Select Enabled



Note: Setting the system to clear the page file at shutdown significantly increases the time it takes for the system to shutdown.

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 -- its size and location change depending 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

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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.

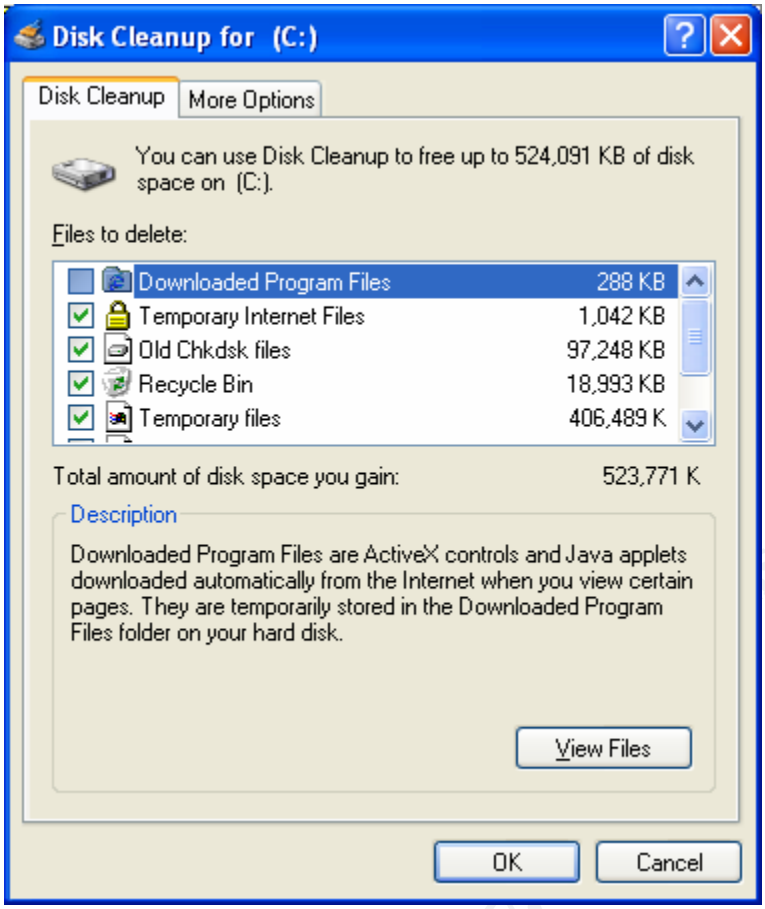
Once you have set a fixed size to the swap file, you can then boot to DOS and run a swap file wiping utility. Using a DOS boot disk with the utility installed will work as well. WipePro+ includes the swap file wiping utility, wipeswap.exe.

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

1. Delete all files you wish removed from the system. When deleting files, use the key combination "Shift + delete" which will immediately delete files, bypassing the recycle bin.
2. Delete all temporary files. This can be accomplished manually, but running Disk Cleanup will help automate the process of removing files. In Windows XP, you can run Disk Cleanup by going to "Start" | "Programs" | "Accessories" | "System Tools" | "Disk Cleanup." Or you can go to "Start" | "Run" and enter "cleanmgr" in the "Open" text box. Windows XP Disk Cleanup screenshot is shown below.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.



3. Defrag hard disk.
4. Run file wiping utility to overwrite slack and free space.
5. Defrag hard disk
6. Run swap file utility. (If necessary for your OS – Windows 9x)

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 to use -- Single Pass, DoD or Guttman, etc. The more overwrites, the longer the process. Determining which method to use can be somewhat simplified if one considers that overwriting data once will defeat all **commercially available** computer forensics tools. This seems like a rather dramatic statement considering all of the standards that have been mentioned in this paper. But computer forensics examiners test their wiping programs with a variety of tools used to conduct computer forensics examinations. I have made this statement publicly from the podium at numerous security and computer forensics related conferences and seminars. I have only been challenged once, and the challenge came from an individual who stated that his agency had been able to recover data that was overwritten three times by using a proprietary piece of software his agency had

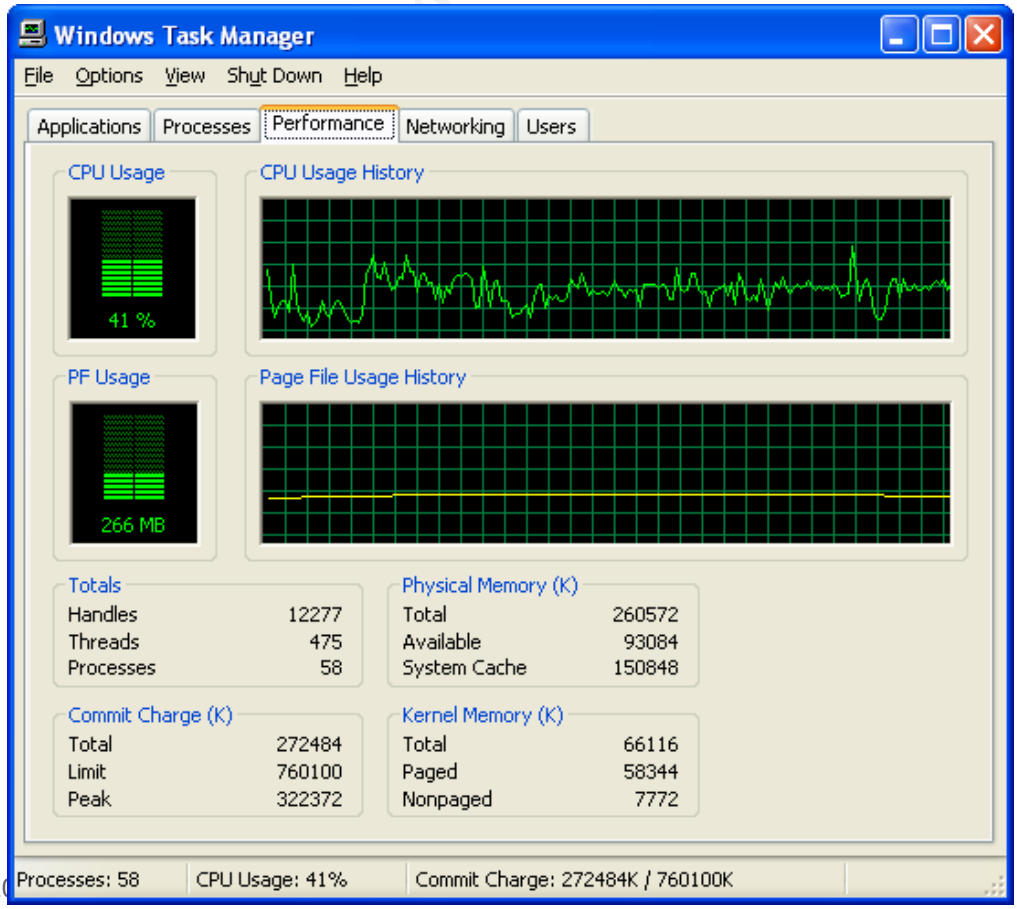
© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

developed and the process was conducted in a vacuum. This certainly goes beyond the scope of the term "commercially available." Despite his claim, I have not been able to confirm whether this is possible or if anyone has ever duplicated his results. I would welcome any information regarding this process.

The value and sensitivity of the information contained on a hard drive will determine the number of overwrites necessary and how often the overwrites are performed. A salesman'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.

I have often been chastised by both security professionals and computer forensics experts for writing this paper. They believe that I have provided instructions to the "bad guys" on how to cover their tracks. While someone could destroy evidence by following the recommendations in this paper, here are several thoughts for security practitioners:

- The fact that deleted files can be recovered is discussed in numerous locations on the Internet. In fact, "Evidence Eliminating Software" posts are made frequently to newsgroups with sexual themes and content.
- The process of wiping a hard drive is time consuming and processor intensive. If an individual wishes to wipe free space and slack space on a computer currently in use, he must essentially give up using the system while the wiping is in process. The process is processor intensive. The following Task Manager screenshot shows CPU



© SANS Institute 20 Author retains full rights.

activity on a system while Eraser is being used to wipe the free space on a drive.

- Many tools do not perform as promised, leaving behind data. For a greater understanding of this, see Matthew Geiger's paper, "Evaluating Commercial Counter-Forensics Tools."[34] He examined the performance of six commercial tools and makes this statement in the paper, "Almost all the tools were capable of wiping data so that it was not recoverable using conventional software-based forensic tools. However, all the tools missed some data they were intended to expunge or had bugs that impaired their performance. In some cases, extensive recovery of targeted data was possible. Further, each tool produced a distinct operational signature that could point to its use, even on media on which no software installation artifacts were present." This paper is extremely interesting and very valuable for computer forensics examiners looking to identify the use of these tools.

- If an individual is actively involved in inappropriate or illegal activities, he will have to use these tools frequently, which can be problematic due to time and processor requirements to accomplish this.

A technologically sophisticated "bad guy" will have greater success in covering his tracks than a white-collar criminal whose technical expertise is limited to word processing and sending email.

<u>Legal Issues</u>

It is important to note that while these tools are often designed to protect privacy and personal information, they should not be used in response to litigation. If a person is served notice of litigation, he should immediately take steps to preserve all data relevant to the matter. One should not immediately install a privacy- or wiping tool to remove all data on a hard drive. This action can have devastating consequences, the first of which can be financial sanctions levied against the party involved in using these tools. The second issue is that if relevant material is destroyed, the judge can issue what is known as a "spoliation inference." A spoliation inference is presented to the jury and basically states that since no one has been able to review the data that was destroyed, the jury can infer that the material contained evidence supporting the plaintiff's claim. If it is brought out in court that a person has used these tools, it can severely damage his claims. An excellent example of this is Kucala Enterprises v. Auto Wax, where the judge stated that "The Court is not convinced that Kucala did not act willfully and with the purpose of destroying discovery by purchasing and then using Evidence Eliminator on his computer. Any reasonable person can deduce, if not from the name of the product itself, then by reading the website, that Evidence Eliminator is a product used to

[34] Evaluating Commercial Counter Forensic Tools - http://www.dfrws.org/2005/proceedings/geiger_couterforensics.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

circumvent discovery. Especially telling is that the product claims to be able to defeat Encase, the forensic imaging program used by Auto Wax to inspect Kucala's computer. Kukala knew that Auto Wax planned on using EnCase software, and he proceeded to install Evidence Eliminator anyway, even after he was advised by counsel not to use it." The conclusion of the judge's report shows the significance of this activity: "Kucala has engaged in egregious conduct by his flagrant disregard of a court order requiring him to allow the inspection of his computer and his utter lack of respect for the litigation process."[35] Mr. Kucala's actions resulted in the dismissal of his case and the payment of a portion of the defendants' attorney's fees.

Because of the "duty to preserve" data and material during litigation, businesses should think carefully about implementing any type of disk sanitizing or wiping program. If a program is implemented it should be consistent and applied "evenly" throughout the organization. Steps should be put in place to suspend the wiping program if served notice of litigation.

Other Issues

It has been reported that at least one tool had problems accurately wiping drives that utilized a Disk Configuration Overlay (DCO).[36] Additionally not all tools will wipe the Host Protected Area (HPA) of a hard drive.

This paper covers various aspects and details of secure file deletion. If you'd like to learn more about how to secure or delete your data permanently as well as other computer security topics, we recommend taking the SANS SEC401 Security Essentials Course.

© SANS Institute 2007, Author retains full rights.

---

35 Kucala Enterprises v. Auto Wax, May 23, 2003 Report and Recommendation - http://www.guidancesoftware.com/corporate/downloads/whitepapers/KucalaVsAutoWax.pdf

36 ExpertEraser Device Configuration Overlay Disk Wiping Security Issue - http://secunia.com/advisories/15347/

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Appendix A

Utilities

Note: This listing is not comprehensive and it is not meant as an endorsement. This list is provided as a starting point for those interested in finding a tool for their specific situation or for those interested in conducting further research on this topic.

Free Tools

Disk Scrub Utility (Linux) - http://sourceforge.net/projects/diskscrub
Sure Delete - http://www.wizard-industries.com/
Kill Disk - http://killdisk.com/
Darik's Boot and Nuke - http://sourceforge.net/projects/dban
Instructions for Solaris systems -
http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/faqs/purge.xml

Commercial Tools

Wipe Expert - http://www.voodoofiles.com/31452
MediaWiper - http://www.whitecanyon.com/mediawiper-erase-hard-drive.php
Disk Wipe - http://www.dtidata.com/products_disk_wipe.asp
Drive Cleanser - http://www.acronis.com/enterprise/products/drivecleanser/
cyberCide - http://www.cyberscrub.com/cybercide/
M-Sweep Pro - http://www.secure-data.com/ms.html
Declasfy - http://www.maresware.com/maresware/df.htm#DECLASFY
Disk Wiper - http://www.secure-data.com/ms.html
Stellar Wipe - http://www.stellarinfo.com/file-eraser.htm
R-Wipe & Clean - http://www.r-wipe.com/
Quickwiper - http://www.quickwiper.com/
Expert Eraser - http://www.experteraser.com/disk-eraser
Disk Redactor - http:/www.cezeo.com/products/disk-redactor/

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

References

Dean, Sarah. "Disk and File Shredders: A Comparison." URL: http://www.sdean12.org/Comparison_Shredders.htm (5/27/06)

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) http://www.dss.mil/files/pdf/nispom2006-5220.pdf (5/27/06)

Erdelsky, Philip J. "A Description of the DOS File System." 15 January 1993. URL: http://www.alumni.caltech.edu/~pje/dosfiles.html (5/27/06)

Guttman, Peter. "Secure Deletion of Data from Magnetic and Solid-State Memory." URL http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (5/27/06)

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/main.jhtml?xml=/connected/2001/07/05/ecrcomp05.xml

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) http://support.microsoft.com/?kbid=211632 (5/27/06)

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) http://support.microsoft.com/kb/89247/ (5/27/06)

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 (5/27/06)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

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 (5/27/06)

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced