Evaluating Commercial Counter-Forensic Tools

By

Matthew Geiger

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2005 USA

New Orleans, LA (Aug 17th - 19th)

Evaluating Commercial Counter-Forensic Tools

Matthew Geiger
Carnegie Mellon University
Pittsburgh, PA
mgeiger@cmu.edu

Abstract

Digital forensic analysts may find their task complicated by any of more than a dozen commercial software packages designed to irretrievably erase files and records of computer activity. These counter-forensic tools have been used to eliminate evidence in criminal and civil legal proceedings and represent an area of continuing concern for forensic investigators.

In this paper, we review the performance of six counter-forensic tools and highlight operational shortfalls that could permit the recovery of significant evidentiary data. In addition, each tool creates a distinct operational fingerprint that an analyst may use to identify the application used and, thus, guide the search for residual data. These operational fingerprints may also help demonstrate the use of a tool in cases where such action has legal ramifications.

Introduction

Modern computer operating systems and the applications that run on them generate copious amounts of data about their users' activity. These records increasingly have become valuable sources of evidence and, concomitantly, the focus of investigation and legal discovery.

At the same time, user awareness has grown that "deleting" files does not mean obliterating the information they contain – an awareness heightened by a string of headlines, from the 1986 resurrection of erased Iran-Contra records on Oliver North's computer to the recovery of files and e-mail communications in the Enron Corp investigation. This awareness has spawned demand for counter-forensic software, which developers market as guarding users' privacy and/or protecting them from being penalized for activity on the computer.

The marketplace for counter-forensic software is competitive. Referral-driven Web sites, such as http://www.privacy-software-review.com, list more than 20 such tools. However, a number of these are 're-branded' distributions of the same underlying engine. (For example, Privacy Eraser from PrivacyEraser Computing Inc. and Windows Internet Cleaner from NeoImagic Computing Inc.)

These commercial tools claim to expunge all traces of information about specific computer usage, including documents and other files created, records of websites visited, images viewed and files downloaded. To do this, counter-forensic tools must locate activity records scattered across the filesystem and erase them irretrievably, while leaving the rest of the operating system intact. The technical challenge of finding and eliminating this data is far from trivial, given the complexity of modern computer operating systems, which are designed to preserve data rather than shed it. Yet rigorous testing and evaluation of these counter-forensic tools appears lacking. We were unable to find a comprehensive resource evaluating the performance of the tools covered in this report.

We examined the performance of six commercial counter-forensic tools, evaluating the tools' abilities to purge a range of activity records and other data representative of real-world computer use. 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.

Background

Methods have been developed to effectively destroy data on magnetic media, such as hard disk drives. One of the most frequently referenced standards in this area was produced by the U.S. Department of Defense in 1995 and recommends sanitizing data on magnetic media by overwriting it repeatedly with specific patterns (DoD 5220.22-M). A year later, researcher Peter Gutmann published seminal research on recovering data from magnetic media using specialized tools and magnetic force microscopy. He also proposed a scheme for wiping data to thwart even a well-funded attacker, such as a government (Gutmann 1996).

Gutmann's threat scenario far exceeds the resources typically available at present to most forensic analysts. They rely on software tools to retrieve latent data from disks. Just overwriting the data once presents a major obstacle to recovery in these circumstances. As a result, forensic reviews of digital media often include an assessment of whether or not such counter-forensic tools were used, and it is has been suggested that these tools should be banned by corporate policies (Yasinsac and Manzano, 2001). Indeed, courts have ruled that the use of such software implies intent to conceal evidence (Kucala Enterprises v Auto Wax Co.) and have sanctioned the users.

In other cases, poorly used or improperly functioning data-wiping tools permitted the recovery of critical digital evidence (US v. H. Marc Watzman, 2003; O'Neill 2004). Even when eradication programs are more assiduously used, some accounts indicate probative data can be missed by these tools (Leyden 2002; Seifried 2002).

On modern personal computer systems, two broad factors complicate the task of eliminating user files and activity records. One is the creation of arbitrary temporary files and cached data streams by common user applications, such as Microsoft Corp's Office suite or Internet Explorer web browser. Identifying and locating all the sensitive temporary data written to disk by user applications under varying circumstances is non-trivial. These temporary files are often deleted by the applications that created them, significantly increasing the difficulty of locating the data subsequently in order to securely wipe it.

At the same time, modern filesystems and the operating systems that govern them employ redundancy and performance-enhancing techniques that can propagate sensitive data onto arbitrary areas of storage media. These techniques include "swapping" data from RAM to a temporary file on the disk to better manage system memory usage, and creating a file to store the contents of RAM and system state information to support a hibernate function. Journaling file systems such as NTFS, ext3 and Reiser also record fractional changes to files in separate journal structures to allow filesystem records to be rebuilt more swiftly and consistently after a system crash.

Testing Methodology

The test system

The testing platform was a desktop machine with 128MB of RAM and Windows XP Professional installed on a 2.5GB partition. Prior to the operating system's installation, the Maxtor 91080-DS hard disk was prepared by overwriting the partition space with zeros before an NTFS filesystem was created. Zeroing out the disk space helps ensure that previous artifacts on the media will not be mistaken for data on the test system.

All security updates and patches available at the time were installed, with the exception of Service Pack 2 because it was uncertain how SP2 would interact with the tools to be tested. After the initial installation, configuration and updates, the operating system reported total space on the NTFS volume as 2.33 GB, with 573MB of that unused. A principle user account was created with administrative privileges, and given the name Anon Nym. This account was used for all subsequent activity on the system.

In Windows Internet Explorer (IE), the privacy settings slider was dropped to its lowest setting to accelerate the collection of cookies, and form auto-completion was turned on. IE was set to delete browsing history records after three days. This was

intentionally shorter than the intended usage cycle for the test system to gauge the counter-forensic tools' abilities to eradicate history information that IE had already attempted to delete. The size for IE's temporary cache of web pages, images and objects viewed was set to 15MB.

Activity record

Test activity on the system breaks down into two general categories: browsing and document creation and management. The activity covered a span of eight days.

Internet browsing and related activity

Browsing activity comprised a mixture of arbitrary navigation to a variety of websites and activity designed to test specific data-eliminating features of the tools. The activity included:

- registering user accounts at a variety of websites, such as the New York Times, Hotmail and Napster
- posting comments to online forums
- saving HTML pages and linked components
- conducting instant messaging sessions
- retrieving and composing e-mail both from a browser-based account and from a POP3 e-mail account via Outlook Express
- using online search engines

Documents

Using the standard Windows Notepad plain text editor and Microsoft's Word 2000 word processor, we created or copied and edited several dozen documents. The document editing process in Word was made lengthy enough to trigger the application's auto-save feature. This feature, which enables the recovery of "unsaved" work in the event of a power failure or application crash, saves a version of the document including changes to a temporary file that is deleted by Word if the document is subsequently closed normally. Images in various formats, principally JPG and GIF, were also saved or copied.

Discretionary file creation and manipulation occurred as far as possible in the test user's My Documents directory and its sub-directories. In all, some 80 files were created in these directories – a few were moved to the Recycle Bin to test erasure of files from this directory. The documents and interactive Web activity were seeded with key words and phrases to help target subsequent searches for latent data.

Napster Client

The Napster Light digital music client, the latest version as of the time of the test, was also installed and a user account registered. The client was used several times, recording registration information and playing music trials.

Baseline filesystem image

At the end of the test activity period, the computer was shut down normally. Using Helix v1.5, a bootable CD-ROM Linux distribution customized for forensic examinations, the computer was booted into a self-contained environment without mounting the hard drive's filesystems. A bit-for-bit image of the 2.5GB NTFS test partition was made, using the Linux utility dd. After the imaging process, a checksum (using the MD5 hashing algorithm) of the imaged partition was compared to a checksum calculated from the original partition immediately prior to the image process to verify that it was a faithful copy of all data, including deleted files and unallocated space. This image preserved the baseline configuration and activity record of the system before the installation of the counter-forensic tools to be tested.

Counter-Forensic Tool Testing

Configuration and use

We tested six software packages: Window Washer 5.5 (a second version of this tool was tested, after a serious flaw was discovered in the first), Windows & Internet Cleaner Professional 3.60, CyberScrub Professional 3.5, SecureClean 4, Evidence Eliminator 5.0 and Acronis Privacy Expert 7.0. All were installed on the Microsoft Windows operating system, the most common desktop platform, although versions of at least two tools were available for other platforms. Where the latest version was available under a fully functional trial license, this was used. Otherwise a license was purchased.

Each tool was installed into an identical operating environment created from the baseline filesystem image, allowing the performance of each tool to be tested on the same system and against identical data and activity records. The counter-forensic

software was configured and run, rebooting if recommended to complete the process. The system was then shut down normally and booted into the Helix forensic environment described above. An MD5 hash was calculated for the Windows partition. A bit-for-bit image of the partition contents was created with dd, and the MD5 hash of the image file was compared to the pre-acquisition hash to verify the image was a faithful duplicate. We used a similarly validated copy of this image as a working copy for the analysis process.

Although the configuration details varied somewhat from tool to tool, setting up and using the counter-forensic software followed a consistent approach.

- We configured each tool to wipe all data targeted for deletion. A single overwriting pass was chosen, sufficient to obstruct recovery with standard software-based forensic applications.
- Most tools also offered the option of renaming files to be erased with some pseudo-random characters before deletion. This step is designed to prevent discovery of the names and types of files deleted since filesystem records about the deleted file can be retrieved even if the file contents are wiped. With this approach, a file named "Second Ledger.xls" might be renamed to something like "sdfFF443asajsa.csa" before deleting. This option was selected for each tool.
- The tools were configured to eradicate Windows activity records such as browser history, Microsoft Office document use history, the Internet Explorer file cache, recently used file lists, recent search terms, files in Windows temporary directories and stored cookies. Some of these records are contained in the Windows Registry database, some in other locations in the filesystem.
- Mail in selected Outlook Express folders was targeted for secure deletion when the tool offered this option.
- In tools that offered it, we selected the option of wiping the Windows pagefile, also referred to as the swap file. This contains data written from RAM memory to the hard disk, as the operating system seeks to juggle memory usage and performance.
- Likewise, in tools that offered it, we always chose to wipe unallocated, or free, space not occupied by any active files.
- Each tool was used to wipe the contents of the My Documents directory and subdirectories, and the contents of the Recycle Bin.
- Some tools offered plug-ins to securely erase activity records generated by third-party software – only those for Napster and Macromedia's Flash Player were used.
- The ability to wipe residual data in file slack space (the area between the end of data stored in a sector on the hard disk and the end of the sector) was not evaluated. Tools that offered this feature prominently cautioned that wiping file slack would be time-consuming, which would be likely to dissuade many users. Data recoverable from slack space was ignored.

The default configuration of some tools did not activate overwriting of files to be deleted, although the tools' documentation typically noted that such wiping is necessary to ensure that erased data are not recoverable. Similarly, wiping of unallocated space was not always selected by default. Under these default configurations, the forensic analyst's ability to recover data would greatly exceed what is reflected in our testing.

Analysis platform and tools

The main platform for analyzing the performance of the tools was the Forensic Tool Kit (FTK) versions 1.50a-1.51 from AccessData. Like similar packages, FTK constructs its own map of disk space from the file system records, as distinct from the records that would be presented by the native operating system. Where filesystem metadata still exist for deleted files (because they haven't been overwritten or reallocated to new files), FTK can parse the information these "library index card" records contain about the deleted files, including where on the disk those files' data was stored. FTK also processes unallocated, or "free," space on the disk for file-type signatures and text content – and builds an index for later searching.

When file metadata has been obliterated, recovering data from the disk becomes more challenging, depending on the original data format. For most Microsoft Office documents, for example, much of the content exists in textual format on the disk, and searching for a contained word or phrase can locate the deleted document's content on the disk. Other file formats, such as .jpg

or .gif images or Zip archives, can contain consistent sequences of code, or signatures. Using these location markers, the contents of the files can be reconstructed, under certain conditions, from unallocated disk space. This process is often termed “data carving.”

Analysis Results

All the counter-forensic tools failed to eradicate some potentially sensitive information – either data specifically targeted for wiping by the user or records that contained information the tool was designed to eliminate. Some shortfalls were more serious than others. In one case, the tool failed to wipe, or overwrite, any of the files it deleted.

The following table summarizes the areas of weakness and representative examples of data recovery. These classifications are subjective; the subsequent discussion of the analysis provides greater detail. We treat the two versions of Window Washer tested as separate tools in this presentation.

Performance Summary

Failure Area	Window Washer-1	Window Washer-2	Privacy Expert	Secure Clean	Internet Cleaner	Evidence Eliminator	Cyber Scrub
Incomplete wiping of unallocated space	Unallocated space not overwritten	Unallocated space not overwritten	File fragments remaining in unallocated space	-	File fragments remaining in unallocated space	-	-
Failure to wipe targeted user and system files	Complete failure to wipe data; did not delete Office shortcuts and IE history file	Recursive wiping failed for user-selected files; some IE cache files not removed	Filesystem metadata intact; missed IE cache index, Office shortcuts, Recycle bin index, e-mail	Missed OE e-mail	Did not erase e-mail; failed to wipe IE history files	Missed some application user records; other activity records recoverable from EE temp folder	Missed Office shortcuts
Registry usage records overlooked	Missed "Explorer\ComDlg32" branch of recently used files	Missed "Windows\ ShellNoRoam\ Bags\" data on directory structure	Missed MS Office "save as/MRU" values; and "Explorer\RecentDocs"	Missed "Windows\ ShellNoRoam\ Bags\" data on directory structure	Missed MS Office "save as/MRU" values	Missed "Windows\ ShellNoRoam\ Bags\" data on directory structure	Missed MS Office "save as/MRU" values; and "Explorer\RecentDocs"
System Restore points and prefetch folder	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	-	Wiped files and directory tree referenced in prefetch files
Data recoverable from special filesystem structures	Small files, fragments recoverable from MFT, NTFS journal, pagefile	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal, pagefile	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal
Detailed activity logs, configuration files contain sensitive information	Tool stores details about wiping configuration; logs list deleted file names, paths	Tool stores details about wiping configuration	Tool stores details about wiping configuration	Tool stores details about wiping configuration; logs list deleted file names, paths	Tool stores details about wiping configuration	Tool stores details about wiping configuration	Tool stores details about wiping configuration

Failure areas

Incomplete wiping of unallocated space

Searches of unallocated disk space – areas of the disk registered as unused in the filesystem index – recovered sensitive data from four of the seven tools tested. In the case of the first test version of Window Washer (build #5.5.1.19), which completely failed to implement its data-wiping feature, the information recovery was extensive. (We refer to build #5.5.1.19 as WW-1 and the second tested version of Window Washer, build #5.5.1.240, as WW-2.) With WW-1, the files were renamed and marked as deleted, but their contents were not overwritten. Text content of a few targeted Office documents and cached HTML from views of the user's Hotmail account also remained in unallocated space after wiping by Windows & Internet Cleaner.

Although WW-2 correctly overwrites the disk space of the files it is set to wipe, it could not be configured to overwrite unallocated "free" space on the disk. This permits *extensive* information recovery from files that were previously deleted by the user, applications or the OS.

Acronis Privacy Expert failed to completely purge data from unallocated space. Searches recovered data from an old copy of the test user's registry file, including deleted file names and directories and the name of an e-mail account. Part of a viewed page from the test user's Hotmail account was also recovered.

Because the operating system and many applications routinely create and delete temporary files that may contain critical content, tools that incompletely wipe the resulting unallocated space provide a significant scope for recovery of latent data. Microsoft Word, for example, creates temporary copies of documents to record uncommitted changes to aid in recovering from a crash. The copy is automatically deleted when the Word document is closed normally – but because the deletion operation only affects the file's index record, what this really means is there is no longer a convenient way to locate the document contents on the disk in order to overwrite it. Forensic tools designed to find exactly such orphaned information on the disk can still rebuild the document. Other deleted copies of the data may have been scattered elsewhere on the disk, created as temporary copies during the download process or by virus-scanning software.

Failure to erase targeted user, system files

All the tools missed some records created by the operating system or user applications that contained sensitive information. In addition, six of the seven tools failed to completely wipe the data contained in user or system files they had targeted. In the case of WW-1, this was the result of its already noted failure to implement wiping despite having the wiping feature enabled. WW-1 also missed Window's shortcut files that provided data about Office documents the user last worked with, and it also missed the latest version of the Internet Explorer history file, which was undeleted and intact. Windows & Internet Cleaner failed to wipe "history" files that record Internet Explorer activity. The files were marked as deleted in the filesystem but recoverable intact because they had not been overwritten. Windows & Internet Cleaner failed to erase mail in Outlook Express' deleted mail folder, which the tool had been configured to eradicate. CyberScrub also missed the shortcuts created for recently used Microsoft Office files. These shortcuts provide name, file size, file editing and access dates, location and other data about the documents.

WW-2 missed a few of the temporary files created by Internet Explorer, allowing the reconstruction of some Hotmail e-mail pages. More critically, a bug apparently stopped WW-2 from deleting the subdirectories in the user's My Documents folder, although it was configured to wipe the entire directory tree.

Evidence Eliminator did not purge user activity data created by the Napster client and Macromedia Flash, despite being configured to do so. On the test system, Evidence Eliminator also created and failed to subsequently eradicate a temporary directory, named *__eetemp*, in the filesystem root that contained copies of the index files for the browser's history records, its cache folder and cookies. So, while the contents of the browser cache folders were deleted, much of the browsing activity could still be reconstructed. Also in this directory were directory listings similar to those recoverable from the Windows prefetch folder (see below), and a directory containing Windows "shortcuts" to recently used Office files.

Privacy Expert does not erase or obfuscate file

metadata (such as name, creation time and length) for the files that it deletes and wipes. So, the original file name and other metadata details were generally recoverable, along with the deleted directory tree structure. This is true both for files selected by the user to be deleted and system activity records targeted for wiping by Privacy Expert. The tool also failed to delete the IE cache index, which keeps track of files stored on the computer by IE while browsing. Together with the metadata in the cache directories, the outlines of browsing activity could be reconstructed even with the contents of the cache files wiped. Privacy Expert also missed shortcuts, created by Microsoft Office, pointing to recently opened Office documents. The links contained a range of metadata about the files they point to, which were deleted. Although files in the Recycle Bin were wiped, Privacy Expert left the index file that describes the files, their original names and where they came from, along with other data. The program also failed to delete designated mail folders in Outlook Express.

SecureClean also failed in this last area, leaving mail in OE's deleted folder that it was supposed to purge.

Most of the tools also missed Windows-created prefetch files that contained, among other information, the full path and names of many of the files in wiped directories. Information in the prefetch folder is used to speed the loading of files frequently accessed by the system or user. Only Evidence Eliminator wiped these files.

Ironically, another occasional repository of the wiped filenames and directories was the tools' own activity logs.

Registry usage records missed

Windows provides a centralized database structure, called the Registry, to hold configuration information, license data and a wide array of other details about the system and installed software. All the counter-forensic tools missed at least a few activity records in the user registry. WW-1 overlooked a registry branch that contained a list of the files of various types the user had recently worked with. Windows & Internet Cleaner missed records of recently saved Word documents in another registry entry, which CyberScrub also missed. In addition, CyberScrub passed over a main registry record of recently used documents and other files. For the other tools, the areas neglected primarily provided insight into the structure of the file tree under the wiped My Documents folder, revealing a small subset of the file and directory names.

Data recoverable from special filesystem structures

All seven test cases encountered problems eradicating sensitive data from special filesystem structures. The operating system usually curtails access to these structures by user applications because they are critical to the filesystem's integrity.

Fragments of user-created files, HTML pages and some complete small .gif images cached from web activity were recoverable from the NTFS Master File Table (MFT). The MFT, the main index to information *about* files on the filesystem, can also contain a file's data if it occupies little enough space, typically less than 1,000 bytes or so. This "resident" data exists as a tiny component within the MFT special file structure, and wiping this space proved problematic for the tools.

Small files and fragments of larger files were similarly recoverable from the NTFS journal after most tools were run. The journal file stores partial changes to files before they are written to the filesystem to make recovering from a crash simpler and faster.

Some fragmented data recovered from unallocated space from the Window Washer and Windows & Internet Cleaner systems may have originally been stored in the pagefile, which all tools were configured to wipe. As another special system file, this might have presented wiping problems for the counter-forensic tools, although Windows XP offers a built-in facility to overwrite the pagefile on system shutdown.

The filesystem also can employ special files to record additional directory metadata outside of the MFT. In the case of Evidence Eliminator and several other tools, files of this type were recoverable and contained information about the structure of the deleted My Documents directory tree.

Archived Registry hives overlooked

How effective the tools were at cleansing the

registry proved moot in five of the seven tool tests. All but Evidence Eliminator and CyberScrub overlooked back-up copies of the user registry stored as part of Windows XP's creation of "restore points" for the system. These restore points, triggered on schedule or by some configuration changes, record system configuration information, often including copies of user registry files. The back-up registry copies contained essentially all the records the tools sought to delete from the current registry.

In fact, the installation of the wiping tools frequently triggered a restore point back-up of key configuration files, including a copy of the user's registry hive just before the use of the tool.

Information disclosure

Configuration and activity records

All the tools disclosed some information about their configuration, such as what types of information they were set to delete, the timing of their activity, whether wiping was selected, and user registration information. For CyberScrub and Windows & Internet Cleaner, most of this information was stored in the registry unencrypted. Some kept granular records about what specific data was set to be purged. WW-1 stored a complete listing of the filenames and locations in plain text as the configuration file for the "plug-in" created to wipe the files. SecureClean produced a detailed usage log that included the name and full path information for deleted files.

Distinctive operational signature

All the tools also left distinctive signatures of their activity that could be used to postulate the tool's use even if no evidence of the software's installation was recovered. (This could occur, for example, if a tool installed on a separate partition or physical disk is used to delete data on another.) The patterns they created in the filesystem records would not be expected to occur during typical computer operations. For example, WW-1 overwrote filenames with a random-looking pattern of characters but gave each file it wiped a suffix of *!!!*. W&I Cleaner renames its files with sets of hexadecimal values, separated by hyphens, in the pattern xxx-xx-xx-xx-xxxxxx. The file suffix is always *.tmp*. See the accompanying table for a summary of each tool's signature.

Given the precedent discussed above in Kucala Enterprises v Auto Wax Co., the presence of such signatures might have probative value in some cases. The following table outlines signature details for each tool.

Outdated coverage of applications

Windows & Internet Cleaner could be configured to delete Napster's usage records. The Napster version specified was 1, and the tool completely missed the records created by the Napster Light client. Because of the version differences, this was not classified as a tool failure. But it does highlight the difficulty of maintaining the counter-forensic tools' effectiveness given the pace of changes in applications and operating systems. It is likely, for example, that Evidence Eliminator's failure to identify and purge the Napster usage records also stemmed from a version mismatch. However, EE does not notify users about the version of Napster it expects.

Tool Signatures

Counter-Forensic Tool	Operational Signature
Window Washer 1	Targeted files renamed with random characters. But all assigned the same 3-character file extension of exclamation marks. Example: 8wVia7S2B39_nX_Xl9Xfw1DhrhS_Da_j.!!!
Window Washer 2	Targeted files renamed with varying lowercase letters for both the filename and a three-letter extension. Length of filename also varied. Example: fpubhmrwbgkpuydin.ydh. Characters used to overwrite the data area varied from file to file, but this character is repeated for the full space allocated to the file.
Privacy Expert	Filesystem metadata such as name, size and creation date are preserved for targeted files, although data areas are wiped with NULLs.
Secure Clean	Targeted files renamed with a six-digit numerical sequence that appears to be incremented by one for every file wiped. The numbers are preceded by the initials SC. The extension assigned was consistently T~P. Example: SC000043.T~P.
Windows & Internet Cleaner	Targeted files renamed with groups of hexadecimal-format values, separated by hyphens, in the pattern 4-2-2-2-6. The file extension was always ".tmp". Example: 4B282BCB-C34D-4147-ACFA-645F3D524B8D.tmp
Evidence Eliminator	Targeted files are renamed with 243 characters with no filename extensions. All except the first 10 characters are pseudo-random combinations of lowercase letters. The first 10 characters are sequential numerals that appear to increment by one for every file wiped. Example: 0000002825wtkdvjiiugvwgveodruvlmdptxgpgfyrqnxpxyjajkqrienrnebnzhoshuyfzhdvzvvvveszlikswlhqpwbetowmznlvzquveyvhkrkcidsmpgpjrxjgpzaxcffvdxynlxiikdnhgachijkuajmdfdcvxbupesrwdyykqfckndbqwittwnyfmtcesftoxtyrnfdwwoblkpcvzwseokhydmcvtvodbrwyvvmewuoge
Cyber Scrub	Targeted files renamed with pseudo-random combinations of capital letters of varying lengths. File extensions are assorted capital letters also. Example: WEFOPSDFSQ.JKV. A deleted, temporary file with the extension ".wip" was consistently created in the volume's root directory.

Sources of failure

Although the review identified some technical issues that repeatedly proved troublesome for the counter-forensic tools' developers, the overarching challenges are not wholly technical. It is probably more useful to group the tools' shortcomings into two broad categories: implementation flaws (or bugs) and failure to anticipate and track the evolving and complex data interactions on a modern computer system. Solving the second problem may involve considerably more effort than the first because the research, development and testing cycle cannot simply focus on whether the tool works as designed. Instead, a solution must anticipate all the ways interaction between the operating system and applications such as word processors, browsers, e-mail clients and peer-to-peer programs can generate potentially sensitive data and then find all the places this data may be stored.

The complexity of this task multiplies with the number of applications the tool is designed to handle: the Thunderbird e-mail client's format and locations for storing messages are completely different from Outlook Express; varying strategies are used by the Netscape browser and Internet Explorer for caching files and cookies; other applications maintain their own recently used file lists and activity data. The tools tested employed dozens of "plug-ins" (in some cases more than 100) to specifically target data generated by such third-party applications.

Complexity also increases along another axis: time. Some of the tested counter-forensic tools evidently missed sensitive data because a newer version of the targeted application changed where and how it stored the data. Staying on top of all these changes and their behavior under different operating systems – which themselves will be changing over time (recall Windows XP's System Restore points) – would require considerable resources and sustained effort.

Implications and Future Work

As this research underscores, selectively purging sensitive data on a filesystem – as opposed to a blanket wipe of the filesystem – is a challenging task. All of the commercial counter-forensic tools tested left data of potential value to an investigation of activity on the computer system. Still, it would be a mistake to underestimate the ability of these tools to destroy evidence and hinder the forensic analysis of digital storage media. From the point of view of a reconstruction of activity or the recovery of data, their use could represent a significant, easily fatal, obstacle. With a few exceptions, the tools succeeded in wiping the majority of targeted data – the value of the data still recoverable would depend on the goal of the examination.

Research such as this can help analysts understand the behavior of these tools, and help guide their efforts to locate and interpret the records a particular tool fails to eliminate. We propose to extend testing to similar tools (and other versions of tested tools) to extend this catalog of their signatures and areas of operational weaknesses. Of course, tool behavior may vary under different operating systems and configurations, but such a catalog will aid in identifying the use of a tool from artifacts on digital media. This identification could then point an examiner to known areas of operational weakness in that tool. The process of searching for these tools' operational signatures lends itself to automation, suggesting a potential addition to the forensic analyst's software toolkit.

Acknowledgments

The author was able to extend core research and analysis for this paper with the help and support of my faculty advisor Lorrie Faith Cranor, at the Institute of Software Research, International of Carnegie Mellon University. We collaborated on related research that focused on the privacy implications of these findings. For advice and useful criticism, sincere thanks are also due to Simson L. Garfinkel and Chuck Cranor.

References

Gutmann, Peter. "Secure Deletion of Data from Magnetic and Solid-State Memory." First published in the *Sixth USENIX Security Symposium Proceedings*, San Jose, California, July 22-25, 1996. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Hopper, Ian D. "Enron's Electronic Clues: Computer Scientists Seek to Recover 'Deleted' Files." Associated Press, Jan. 16, 2002. Viewed at: http://abcnews.go.com/sections/scitech/DailyNews/enronPCfiles020116_wire.html

Kucala Enterprises v Auto Wax Co. (2003). Judgment in case# 02C1403, United States District Court, Northern District of Illinois. Available as Case No. 1403 - Doc. No. 127 from http://www.ilnd.uscourts.gov/racer2/.

Leyden, John. "Windows wipe utilities fail to shift stubborn data stains." The Register, Jan. 21, 2002. http://www.theregister.co.uk/2002/01/21/windows_wipe_utilities_fail/

O'Neill, Sean. "Court battle on software that destroys cases against paedophiles." The Times of London, Dec. 3, 2004. http://www.timesonline.co.uk/

Seifried, Kurt. "Multiple windows file wiping utilities do not properly wipe data with NTFS file systems." Security advisory published Jan. 21, 2002. http://www.seifried.org/security/advisories/kssa-003.html

Shred manual pages. A component of the Linux coreutils package v 4.5.3, November 2003. Documentation available as part of the coreutils distribution and at http://techpubs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=linux&db=man&fname=/usr/share/catman/man1/shred.1.html&srch=shred

United States v. H. Marc Watzman (2003). Indictment in United States District Court, Northern District of Illinois, Eastern Division. http://www.usdoj.gov/usao/iln/indict/2003/watzman.pdf
See also http://www.kansas.com/mld/kansas/news/7119391.htm for a report of the case.

U.S. Department of Defense "Standard 5220.22-M: National Industrial Security Program Operating Manual" (January 1995), Chapter 8. http://www.dss.mil/isec/chapter8.htm

Yasinsac, Alec and Manzano, Yanet. "Policies to Enhance Computer and Network Forensics." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, New York, 5-6 June, 2001. http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2B3(37).pdf