Counter-Forensic Privacy Tools

A Forensic Evaluation

Matthew Geiger, Lorrie Faith Cranor
June 2005

CMU-ISRI-05-119

Institute for Software Research, International, Carnegie Mellon University

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Abstract

Modern operating systems and the applications that run on them generate copious amounts of data about their users' activity. Users are increasingly aware of their privacy exposure from these records and from digital artifacts that linger after files are "deleted" on computers they use. Efforts to redress this privacy exposure have spawned a range of counter-forensic privacy tools – software designed to irretrievably eliminate records of computer system usage and other sensitive data.

In this paper, we use forensic tools and techniques to evaluate the effectiveness of six counter-forensic software packages. The results highlight some significant shortfalls in the implementation and approach of these tools, leading to privacy concerns about the exposure of sensitive data. The findings also raise questions about the level of privacy protection that is realistic to expect from these tools, and others that take a similar approach.

TABLE OF CONTENTS

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 the focus of investigation in legal and personal disputes, as well as a risk to privacy and security in shared computer environments. At the same time, user awareness is growing that "deleting" files doesn't mean obliterating the information they contain – an awareness heightened by such newsworthy events as the 1986 resurrection of erased Iran-Contra records from Oliver North's computer to the recovery of files and e-mail communications in the Enron Corp investigation.

Concern about recovering privacy-sensitive data from computer systems takes on greater significance in light of recent trends in computer use. Employees use company computers for personal e-mail, shopping and banking. When companies provide employees with laptops to work at home, other family members often use these computers too. As a result, company computers may contain sensitive, personal information that individuals want to keep private, as well as records that companies have a legitimate interest in protecting and examining.

Monitoring of employee activity on computers is increasingly commonplace (EPIC 2004). Companies' interest in tracking computer use is underscored by surveys that show insiders are responsible for about half of computer crimes and related misconduct (Gordon et al, 2004). Companies also monitor employees' online activity to comply with legal obligations to provide a harassment-free working environment, or to enforce company policy. Others block access from the corporate network to Web sites critical of the company or that contain other objectionable content. It's not just network traffic that is monitored; companies also routinely examine the contents of storage media, like computers' hard drives, sometimes using forensic tools to recover deleted material. Nearly one in four companies searches employees' e-mail and computer files for key words and phrases, according to an American Management Association survey on workplace monitoring (2001).

These colliding interests have spawned a market for specialized software designed to guard users' privacy. Users have access to an array of commercial tools that claim to remove all traces of privacy-sensitive information about their computer usage, including documents they've created, records of websites they've visited, images they've viewed, files downloaded and programs installed and executed. User concerns about this data range from eliminating information that exposes them to financial loss, such as online banking credentials, to ensuring purely personal information is kept private. Counter-forensic privacy tools locate activity records scattered across the computer filesystem and seek to erase them irretrievably.

The technical challenge of finding and eliminating this sensitive data is far from trivial given the complexity of modern computer operating systems, designed to preserve data rather than shed it. Yet rigorous testing and evaluation of these privacy tools is lacking. Online resources that offer consumer-oriented advice about commercial privacy tools consist of comparisons of advertised features, usability and support, rather than evaluations of the tools' performance. Software reviews published in the technology press have included only cursory assessments of performance (see http://privacy-software-review.com and Appendix D for examples). We were unable to find a published evaluation of the comprehensive data protection performance of the tools selected for this report.

Our research attempts to bridge the knowledge gap about how much privacy protection these tools offer. Employing accepted forensic tools and methods, we examine the performance of six commercial privacy tools. We evaluate the tools' abilities to purge a range of activity records and other data representative of real-world privacy sensitivities. The evaluation's methodology and findings are intended to be reproducible and extensible. Our analysis of the tools' performance identifies shortfalls and challenges in their approach to sanitizing data – and discusses how future privacy tools could more reliably address these concerns, along with alternative methods to protect sensitive user data.

To flesh out the challenge faced by these privacy tools, we first review filesystem and operating system behavior and existing research in the secure deletion of data. Our preparation of a test system and of the tool evaluations follows, along with some background on the companies behind the software. The subsequent performance analysis of the privacy tools' performance highlights some serious concerns and discusses the issues that limit the tools' effectiveness.

Background

Deletion Process

Almost all data written to a computer hard drive or other forms of digital storage remain there until overwritten. Contrary to popular belief, even the act of reformatting most hard disks will not remove the bulk of the resident data. When a user deletes a file or directory of files, what typically happens is the filesystem's reference to that data, comparable to an index card in a library, is marked as 'erased'. The data itself is left on the media, whether it is a hard disk, floppy diskette, zip drive, flash memory key, etc. Returning to the library analogy, the book stays on the shelf even after the index file pointing to it is removed. A typical hard drive is littered with such files or remnants of them.

With the correct tools and techniques, this data can be recovered, in some cases in its entirety along with the original 'index card' information about the file. Even fragments of critical data can contain privacy-sensitive information and can be used to reconstruct files and events on the system.

Although different filesystems may use varying methods to handle the task of deleting files, no mainstream filesystem provides a built-in mechanism to "wipe," or overwrite, deleted data by default. There's good reason for this. For most users and operating system developers, speed and reliability are the two primary concerns for a filesystem. Overwriting deleted data areas to make them unrecoverable would impose a huge performance penalty.

Privacy Risks

Other researchers have provided stark demonstrations of the privacy risks of latent data on hard disks. In a 2002 study, Simson Garfinkel and Abhi Shelat recovered a plethora of private information, ranging from medical correspondence to banking transaction records, from 158 second-hand hard drives they purchased. Of the 129 functioning drives they examined, only 12 had been properly wiped of data (Garfinkel et al, 2003).

More recently, a research team at Britain's Glamorgan University analyzed 101 used disks. They reported that more than half still contained personal or proprietary information, ranging from crop research by a U.S. agrochemical conglomerate to evidence of a married woman's affair and detailed biographical information about children. The data recovery was made more significant because the institutions and corporations that discarded many of the drives were violating the U.K.'s Data Protection Act by failing to protect the information (Hoyle 2005).

Destroying Data

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, Peter Gutmann published detailed 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 such 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, who 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, digital investigations 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). Even when eradication programs are more assiduously used, some accounts indicate probative data can be missed by these tools (Leyden 2002; Seifried 2002).

Research has identified two broad factors that complicate the task of selectively eliminating traces of computer usage. One is the creation of arbitrary temporary files and cached data streams by common user applications, such as the Microsoft 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, which significantly increases the difficulty of finding the data subsequently in order to securely wipe them (Thomas 2003).

At the same time, modern file systems 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 data structures to allow filesystem records to be rebuilt more swiftly and consistently after a system crash (shred manual pages, 2003).

For these reasons, the U.S. Department of Defense standard advocates overwriting the entire device (hard disk) or partition (C: drive), instead of file-by-file wiping, for eradicating sensitive information. For truly secret information, the standard is complete physical destruction of the disk.

Still, using a power drill or sledgehammer to destroy the hard drive is not a practical solution for computer users who are seeking to eliminate particular records but retain the rest of their data. For the same reason, overwriting the entire hard drive or partition with NULL characters isn't a useful option, unless the disk or machine is being sold. The privacy tools tested seek to provide an alternative to these drastic steps that can be used routinely to guard against the disclosure of sensitive information.

Testing Methodology

The test system

The testing platform was a 466 MHz Celeron Pentium-powered desktop machine with 128MB of RAM. Windows XP Professional was 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 ensures that previous artifacts present on the media won't be mistaken for data in deleted space on the test system.

The operating system was configured as a default, non-domain installation. All security updates and patches were installed, with the exception of Service Pack 2 because it was uncertain whether SP2 would interfere 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 under 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 activated. IE was configured to retain its browsing history records for just three days. This was intentionally shorter than the intended usage cycle for the test system to gauge the privacy 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.

Internet browsing and related activity

Browsing activity comprised a mixture of arbitrary navigation to a variety of websites and specific activity designed to test privacy-protecting features of the tools. This specific activity included:

- registering user accounts at a variety of websites, including the New York Times, Hotmail and Napster
- posting comments to online forums
- saving web pages and related components
- conducting Windows Messenger chats
- retrieving and composing e-mail both from a Hotmail webmail 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 documents including all 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 on the system.

Discretionary file creation and manipulation occurred as far as possible in the test user's My Documents directory and its sub-directories (see Appendix E for a tree listing of the directory contents). 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 operating system feature. Most of the documents and some interactive Web activity were seeded with phrases, such as "secret stuff" and "world domination," that we used to help target subsequent searches for the material.

Napster Client

The Napster Light digital music retrieval 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 truncated song 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 the forensic environment without mounting the filesystem on the hard drive. A bit-for-bit duplicate image of the 2.5GB NTFS test partition was made, using the Linux utility dd. After the imaging process, a checksum (employing the MD5 hashing algorithm) of the imaged partition was compared to a checksum calculated from the original partition prior to the image process. They matched, demonstrating that the image was a faithful copy of all the data, including files and unallocated space, on the partition. This image preserves the baseline configuration and activity record of the system before the installation of the tested privacy tools.

Privacy tool testing

Configuration and use

We tested six privacy 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. Most are only available for the Microsoft Windows operating system, the most common desktop platform, although versions of two tools were marketed for other platforms. Listed prices for the tools ranged from about $29 to $100.

Each tool was installed into an identical operating environment based on the described test computer system and baseline filesystem image. This allows the performance of each tool to be tested in the same environment with identical data and activity records. The privacy software was configured and run to eradicate targeted records, rebooting if recommended to complete the process. The system was then shut down normally and booted into the same 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 privacy software followed a consistent approach. (Details of each tool's configuration are contained in Appendix C).

- We configured each tool to overwrite 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

pseudo-random characters before deleting the file record. This step is designed to prevent the disclosure of the names and types of files deleted because filesystem records about a deleted file can be retrieved even if the file contents are wiped. For example, a file named "cancer-information.doc" might be renamed to something like "sdfFF443asajsa.csa" before deleting. This option was selected for each tool for which it was available.

- The tools were configured to eradicate standard Windows activity records such as the Internet Explorer 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 securely delete the contents of the My Documents directory and subdirectories, as well as 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 tested.
- 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) wasn't 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 didn't always turn on overwriting of areas to be deleted, although the tools' documentation typically notes that wiping is necessary to ensure that erased records aren't recoverable. Similarly, wiping of unallocated space isn't always selected by default. Using default settings that don't activate wiping would severely degrade these tools' abilities to protect the users' privacy. The disclosure of privacy sensitive information in these cases would be significantly greater than reflected in our testing.

Analysis platform and tools

The main platform for analyzing the performance of the privacy tools was the Forensic Tool Kit (FTK), versions 1.50a-1.51, from AccessData, a commercial package optimized for analyzing Windows platforms. 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 records still exist for deleted files (because they haven't been overwritten or reallocated to new files), FTK can parse the information these "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 signatures and text content – and builds an index for later searching.

If a file has been conventionally deleted and the filesystem record and file data haven't been overwritten by new data, then recovering the file entails simply identifying the deleted filesystem record, the "index card," and examining the space it points to on the disk. Tools such as FTK do this automatically. When the filesystem record has been obliterated, recovering data from the disk becomes more challenging, depending on how the data was stored. 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. Some more complicated file formats, such as .jpg or .gif images or Zip archives, contain consistent sequences of code, or signatures, that allow the contents of the files to be rebuilt, under certain conditions, from unallocated disk space. This process is termed "data carving."

FTK and similar tools include data-carving features. "Foremost," an open-source tool created by the U.S. Air Force Office of Special Investigations, for example, performs data carving for custom-specified signatures, allowing the recovery of files with any format for which a signature can be identified.

Analysis Results

All the privacy tools failed to eradicate some sensitive information. Some shortfalls were more serious than others. In one case, the tool failed to wipe any of the records it deleted.

The following table summarizes the areas of weakness and the degree of privacy exposure. More footprint icons indicate greater exposure. This classification is subjective; the subsequent discussion of the analysis offers more details. We treat the two versions of Window Washer tested as separate tools in the analysis. Tool-by-tool results are presented in Appendix B.

Table 1: *Evaluation of privacy tools.*
(Footprints reflect level of privacy exposure)

Privacy Issue	Window Wash-1	Window Wash-2	Privacy Expert	Secure Clean	Internet Cleaner	Evidence Eliminator	Cyber Scrub
Incomplete wiping of unallocated space							
Failures erasing targeted user and system files							
Registry usage records missed							
Registry archive recoverable from system restore point							
Data recoverable from special filesystem structures							
Tool discloses its configuration, activity record							

Case Study: Window Washer

Our testing experience with Window Washer underscores the importance of reliable performance evaluations for privacy tools.

Among the features highlighted by Window Washer's producer, Webroot Software Inc., is the tool's ability to securely wipe data with its "Bleach" function.

> **Bleach for Extra Security**
> Completely overwrite files with random characters making them unrecoverable by undelete or unerase utilities - a security feature which exceeds the tough standards of the Department of Defense and the National Security Agency (Webroot Product Information).

However, the first test version of Window Washer (build #5.5.1.19) failed to implement its data-wiping feature. Window Washer left file contents intact and recoverable on the disk.

In researching the failure, we contacted Webroot in November 2004 to verify that the trial version of the tool being tested was fully functional, which the company confirmed. Searching for reports of the data-wiping bug we found an April 2004 entry in Webroot's online knowledge base entitled: "Why does my new version of Window Washer run faster than my old version?" The answer, according to Webroot's support staff, is that the tool runs much faster because of a "bug in our code" that causes it to skip wiping files. Webroot suggested a workaround: setting a user-defined number of wiping passes for the "bleaching" process. The workaround made no difference in our testing, however.

The flaw would not be apparent to a typical user because, while the files are not wiped, they are deleted and so don't appear in file listings. The trials performed in published reviews of privacy software also wouldn't have revealed the problem. No other notice about this privacy-critical bug could be found on the Webroot web site.

In January 2005, we obtained and tested a version of Window Washer in which this bug had been fixed. Still, as with other tools tested, performance shortfalls persisted – shortfalls that aren't apparent or easy to discover for users.

The privacy implications for Larry

As we discuss the privacy tools' shortfalls, we'll examine their significance from the point of view of an individual we'll call Larry. Larry wants to expunge sensitive material from his work-owned Windows XP computer.

Let's assume Larry receives the results of a medical test that was attached as a Word document in an e-mail sent by his doctor's office to his private Webmail account. Larry browses to his Webmail provider to check his mail, sees the message and – although he's aware that his Internet activity may be monitored at the workplace – doesn't want to wait to review the document. He downloads the document to his My Documents folder. He opens and reads the document: *biopsy-results.doc*. After adding some comments to the top of the report, Larry forwards it to his wife – using his personal Webmail account.

At this point, Larry could just erase the document and purge it from his Windows Recycle Bin. But Larry is conscious that material deleted by the operating system remains recoverable, and he's keen to keep the report private. So, instead of deleting the file, he downloads a privacy tool and configures it to wipe both his medical report file and the activity records of his browser, which would contain his Webmail visit. (In order to do this, Larry needs administrative rights on his computer, not always the case in a corporate setting.) Larry feels much better … but should he?

The answer, from our testing: probably not.

Failure areas

Incomplete wiping of unallocated space

Searches of unallocated disk space – areas of the disk registered as unused in the disk 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 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 occupied by the files it is set to wipe, it still doesn't have a feature 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, which is why wiping unallocated space is a critical component of securing data privacy. 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 his e-mail account. Part of a viewed page from the test user's Hotmail account was also recovered.

If the privacy tool Larry used didn't wipe so-called unallocated, or free, space on the disk, the entire medical report is most likely still recoverable. That's because the document that selected to wipe wasn't the only copy of the report created on his computer's disk. When Larry edited the document before sending it to his wife, Word created at least one temporary copy of the file to record changes in case the application crashes or if Larry needs to undo his editing. That copy was automatically deleted when Larry closed his Word document – but because the deletion operation only affects the file's index record, what this really means is there's 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 the company's virus scanning software.

Let's say Larry's privacy tool is configured by default to wipe unallocated space, and Larry proceeds with the time-consuming process of overwriting the "unused" space on his disk with arbitrary data. Incomplete wiping of unallocated space or the disk cache file or filesystem journal may leave enough of the text of the medical report on the disk to compromise Larry's privacy.

Failures in erasing targeted user and system files

All the tools missed some records created by the operating system or user applications that contained sensitive information. Six of the seven tools failed to completely wipe the data contained in targeted user or system files, most often because of implementation flaws. In the case of WW-1, this was the result of its already noted failure to conduct wiping despite having the wiping feature enabled in its configuration. WW-1 also missed Window's shortcut files that provided data about Office documents the user last worked with, and – significantly – 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 to the user's

My Documents folder, although it was configured to wipe the entire directory tree.

Evidence Eliminator didn't 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 didn't clean up a temporary directory, named *__eetemp*, in the filesystem root that contained copies of the IE 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 filename and directory listings similar to those recovered from the Windows prefetch folder (see the following comments), and a directory containing Windows "shortcuts" to recently used Office files.

Privacy Expert doesn't rename files or obfuscate file metadata (such as creation times 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 contain 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.

Perhaps Larry selected a tool that does not scramble the names of the files it wipes. It's likely that Larry wouldn't want it known that he had wiped a document called *biopsy-results.doc*. This is also a problem if privacy tools miss one of the other places Windows and applications record filenames and other data. Every tool tested missed some place this information was stored, including – ironically – the activity logs of some of the tools tested.

Then there's the data trail left by Larry's Webmail session. Some tools that

successfully wiped other data missed some or all of the Internet Explorer cache. The information in this cache could include the contents of the e-mail from Larry's doctor. The cache ordinarily wouldn't include Larry's e-mail to his wife, except that he attached the lab report – a process that in Webmail systems commonly causes the e-mail composition page to be re-displayed (to show the attached file). This reloading of the page placed it in the cache, which would reveal what Larry wrote to his wife.

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 privacy 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 the 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 of a large, special file structure, and wiping this space proved problematic for the privacy tools.

Similar small files and fragments were 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 privacy tools, although Windows XP offers a built-in option to overwrite the

pagefile on system shutdown.

The filesystem also employs special files to record additional directory data 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 recoverable

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.

This oversight leaves Larry vulnerable even if his privacy tool thoroughly wipes targeted files, purges sensitive activity data from system records and every relevant nook in the Windows Registry and expunges trace data from unallocated space on his hard drive. In fact, the installation of the privacy tool Larry downloaded could well have prompted Windows to back up key configuration files, including a copy of his registry hive, with much of the activity data he's about to try to eliminate.

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 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*.

Given the precedent in Kucala Enterprises v Auto Wax Co., the discovery of such signatures might have legal ramifications for the user.

Outdated coverage of applications

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

Lessons from failure

Although the review identified some technical issues that repeatedly proved troublesome for the privacy tools' developers, the overarching problems aren't wholly technical. If they were, it's unlikely a solution would be elusive for long. Instead, it's 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. The first problem area points to a need for more rigorous testing, better research and design, and associated improvements in quality control. Solving the second problem involves considerably more effort 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 identify 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 privacy tools tested used dozens (in some cases more than 100) "plug-ins" to specifically target data generated by such third-party applications.

Complexity also increases along another axis: time. Some of the tested privacy 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 the XP restore point function) – requires sustained resources and effort.

Vendor notification

The vendor of each tool tested was contacted by e-mail and provided an opportunity to make comments on a draft of this report. Only one, CyberScrub LLC, the vendor of the eponymous tool, responded. Bill Adler, CyberScrub's chief executive, noted that a number of the issues raised in our tests have been addressed with a recently released version of the privacy tool, CyberScrub Privacy Suite Professional Edition 4.0. The issues addressed include scrambling the names of files in the IE cache folder, overlooked file metadata in the Registry and Microsoft Office shortcuts, and wiping of e-mail from Outlook Express. We were unable to test Cyberscrub's latest version prior to publication of this report but look forward to doing so.

Other vendors have released updated versions of their privacy tools since we completed our testing. These include: Acronis Privacy Expert Suite 8, Windows & Internet Cleaner Pro v. 4 and Window Washer v. 6 from Webroot, which now can be configured to wipe unallocated space.

A market comparison

To understand the resources required to track these changes, a comparison with virus-scanner software development may be helpful. While major anti-virus vendors identify and respond to new virus variants every day, updating scanning software usually involves the straightforward addition of new virus signatures. Privacy tool developers would face less frequent update requirements, but each update would entail greater development efforts. Anti-virus vendors can spread the associated costs over a user base that numbers from tens of thousands to millions each, depending on the vendor. The market for privacy tools is undoubtedly much smaller. If the comparison is valid, it calls into question whether sufficient demand exists to provide economic justification for rigorously tested, frequently updated privacy tools that address the shortcomings we discovered.

Norman ASA, a Norwegian anti-virus company that made about 80% of its US$36 million in sales last year to small and mid-sized businesses in Europe and America, spent about US$4.6 million on research and development. According to its Chief Financial Officer Tom Nøttveit, that was substantially all due to the cost of maintaining its anti-virus products. McAfee, one of the largest anti-virus vendors in the consumer and corporate markets worldwide,

spent about US$180 million on R&D in 2003 and employs about 1,000 people in research. However, McAfee's R&D activities encompass a wide range of products and services beyond their virus-scanner software. McAfee, Symantec and other major vendors contacted didn't provide detailed breakdowns of their R&D costs.

In comparison, Evidence Eliminator, one of the most heavily advertised counter-forensic products on the Web, is produced by Robin Hood Software Ltd., a privately held British company based in Nottingham, England. The company submitted unaudited accounts for the 2004 financial year that indicate net profit of around US$346,000. If we can use Robin Hood's accounts as a rough gauge and estimate its net profit margin at between 20% and 45%, sales would range from US$769,000 to US$1.7 million. At an estimated average price of about US$100 per copy of Evidence Eliminator, that implies annual sales of between 7,700 and 17,300 copies for the company that has been described as the market leader in a number of publications.

Without sufficient market scale, privacy software vendors may find it difficult to dedicate resources to surmount the challenges identified in this research. Our test results suggest those resources aren't being applied now – either in detecting bugs that compromise the effectiveness of the privacy tools or in keeping plug-ins up to date with the latest versions of software they are designed to handle.

Search for standards

For market forces to work to encourage improvement in these privacy tools, consumers need reliable, relevant information about the tools' performance. One way to achieve this is through the development of standards and independent testing. Some suitable frameworks for such standards already exist, such as the Common Criteria family used by NIST, the largest standards and testing arm of the US government.

In terms of developing criteria suitable to design test measures of these privacy tools' effectiveness, some parallels can be drawn with existing elements of the Common Criteria. Indeed, the Common Criteria include some components for evaluating privacy protection. And Kai Rannenberg and Giovanni Iachello have applied these specific Protection Profiles to the area of privacy-protecting e-mail systems and noted problems that arose when they attempted to express security objectives outside of the existing Criteria components (2000).

This obstacle to applying the Criteria is starker in the case of the tested privacy tools. The specified Protection Profiles that involve privacy focus on the way software or devices incorporate protections for privacy into their initial operations and processes. It's the absence (or paucity) of such measures within mainstream operating systems and applications that places

privacy sensitive data on the computer system. The functionality and standards for software that has to subsequently eliminate this data is not specifically considered in the privacy family of Protection Profiles.

Extending or adding families to include operational criteria for counter-forensic privacy tools may provide the basis for creating an independent and well-articulated standard for their performance. Some guidance in this approach may eventually come from the efforts of Ontario's Information and Privacy Commissioner, who has launched a Privacy Enhancing Technology Testing & Evaluation Project.

An alternative is for privacy tool vendors to submit to private testing to build consumer trust. Again there is precedent in the computer security field. For example, ICSA Labs, an arm of TruSecure Corp, performs independent performance reviews and validation for a range of security-related software, implementations and devices. The labs have performance tested hundreds of products such as anti-virus software, firewalls, intrusion detection systems and wireless networking devices. Testing follows published criteria and is repeated throughout a product family life cycle.

Users would have a much clearer notion of the limits of their protection if they were alerted by the privacy tools when installed versions of applications don’t match those that the tool has been designed handle. In addition to a list of covered software, privacy tools could maintain a database of privacy-benign applications and then alert users when encountering any installed software not on either list.

Still, attempts to retrofit privacy into current computer operating environments face challenges that parallel those confronting the security community as it grapples with protocols and architectures conceived with little regard to security. A high degree of confidence in privacy protection will be elusive unless the environment is engineered with privacy in mind. Meanwhile, the exposure of privacy-sensitive data is likely to escalate with the wider deployment of networked storage systems.

Privacy-protective alternatives

Other approaches may prove to be more privacy protective than the tools we tested. One method is the use of encryption to protect private data so that sensitive information is never written to disk in unencrypted form. Common approaches either encrypt each file individually (as does the Encrypting File System, or EFS, native to recent Windows operating systems) or encrypt an entire filesystem (PGP Corp.’s PGPDisk, Jetico Inc.’s BestCrypt and Apple Computer Inc.’s Mac OS X FileVault).

Under EFS, individual files and directories on NTFS volumes are tagged for encryption. When a directory is selected, EFS by default attempts to encrypt all new files created in the folder. However, EFS refuses to encipher system

files and any files under the system root directory (typically, C:\Windows). The system files that EFS will not encrypt include Registry files, some locally stored application data and contents of the Internet Explorer browser cache and the index databases to those files and history records. Because EFS encryption is performed file-by-file, some of these "exempt" files can exist in plaintext form within a directory that is tagged as encrypted. In addition, Microsoft advises against encrypting directories used to store temporary files for third-party applications, saying doing so can cause problems.

In comparison, PGPDisk and BestCrypt create a self-contained, encrypted filesystem in a container that – when it's encrypted – looks just like any other file to Windows. A user who supplies the correct password or key, however, can decrypt the container and mount its contents like a Windows volume, assigning it an unused drive letter.

Part of the reason EFS refuses to encrypt so many privacy-sensitive areas is a chicken-and-egg issue that also affects the other encryption strategies for Windows. The problem is that Windows offers no built-in way for users to decrypt their files before logging in, and the process of logging in requires access to some of the very files that users would want to encrypt to protect their privacy, such as their Registry database and other system files. The problem is compounded by other Windows user activity files, such as the Explorer History file and IE's cookie store, that don't offer relocation alternatives, by third-party applications that may save usage records in unexpected locations, and by data that's leaked through other OS operations, such as the RAM swap file. BestCrypt offers a swap-file encrypting option to address this last concern, and a slightly different approach has been outlined by Neils Provos for OpenBSD systems (2000).

In response to this conundrum, some vendors have developed whole-disk encryption systems, which use a small program invoked during the boot-up process, before the operating system, to decrypt the disk's contents. Hard drive manufacturer Seagate Technology LLC recently introduced a line of laptop hard disks with in-built encryption.

Encrypting user activity records under some Unix-based operating systems, including many Linux distributions and Apple's Mac OS X, proves easier because of available mechanisms to decrypt user directories in a just-in-time fashion for login. The approach taken by the Linux encrypted loopback filesystem, OS X's FileVault and BestCrypt for Linux is similar. All create an encrypted container that looks like a large file to the operating system, except when it is decrypted and mounted as a filesystem.

One drawback undercuts the usefulness of all the encryption approaches in a corporate setting. It's unlikely that most companies would allow users of their computers to encrypt arbitrary files so that they can't be decrypted by the company. In fact, Windows' EFS and other encryption systems that target the corporate market allow for the creation of master keys that can

decrypt any encrypted file.

Another consideration in evaluating encryption schemes is how they protect their keys. To eliminate the need for multiple passwords, some approaches, such as Windows EFS and Mac OS' FileVault, can employ the user's logon credentials to protect the keys. The advantage is usability and convenience. In addition, because there's just one password to remember, this "single sign-on" approach may help reduce weak passwords or passwords written on a Post-it® note stuck to the monitor. The disadvantage is that the key is only as safe as the login credentials – which may be more poorly protected than users expect. For example, Windows XP systems and earlier, by default, store user passwords in both strongly and weakly encrypted forms for backward compatibility. Even Microsoft describes the weak form as "prone to fast brute force attack" (Microsoft Knowledge Base Article ID 299656).

Implications and Future Work

As our research underscores, selectively purging the average computer system of sensitive data is a challenging task. Although most of the tools examined eliminate the majority of targeted data, all missed some records that – depending on the context – would be privacy sensitive. In some cases, the tools offered little more protection than simply deleting the files. Yet, it seems likely that the tools' users have a false sense of security about their privacy protection. This misplaced confidence is fostered by consumer-oriented reviews of these tools that do not adequately evaluate their performance, and a lack of independent testing and performance standards.

Even for tools that are relatively free of implementation mistakes and bugs, the results of these tests suggest the challenge of locating and sanitizing in place all sensitive data on a working operating system is far from trivial. It's clear that a privacy tool capable of meeting this challenge will require intensive, sustained development effort on a higher level than currently evident.

Although this review focused on the tools' flaws, it's important to note that all the tools eliminate potentially sensitive information; most irretrievably erase the vast majority of targeted data. From the point of view of a forensic reconstruction of activity or the recovery of data, their use represents a significant, easily fatal, obstacle. At the same time, all these tools leave enough sensitive data that an individual deeply concerned about the recovery of specific information cannot be confident of its elimination. The tools' effectiveness is not equivalent, even in a broad sense, to the privacy garnered by wiping the entire storage medium – the Department of Defense recommendation. In addition, because of the operational signatures generated by the tools, they might incur separate risk for some users in specific legal settings.

As a resource for the digital forensics community, we propose to extend testing to similar privacy tools (and other versions of tested tools) to build a catalog of their operational signatures. This catalog could be used to identify the use of a tool by the signature and other artifacts on the media wiped. This identification could then point an examiner to known areas of operational weakness in that tool.

Acknowledgments

The authors would like to extend our sincere thanks to Simson L. Garfinkel and Chuck Cranor for valuable advice and criticism.

References

American Management Association. "Workplace Monitoring & Surveillance: Policies and Practices." AMA, New York, 2001. From the Summary of Key Findings, http://www.amanet.org/research/pdfs/emsfu_short.pdf

Electronic Privacy Information Center. "Workplace Privacy." An online resource published at http://www.epic.org/privacy/workplace/. Updated Aug. 3, 2004. Viewed Nov. 14, 2004.

Gordon, Lawrence A. et al. "CSI/FBI Computer Crime and Security Survey." Computer Security Institute, San Francisco, 2004. Available from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

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. Retrieved from http://www.guidancesoftware.com/support/resources/kucalavautowax.shtm on Oct. 1 2004.

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/

Provos, Niels. "Encrypting Virtual Memory." Published in the 9th USENIX Security Symposium proceedings, Denver, Colorado, Aug. 13-17, 2000. http://www.usenix.org/events/sec2000/full_papers/provos/provos_html/index.html

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

Rannenberg, Kai and Iachello, Giovanni. "Protection profiles for remailer mixes - Do the new evaluation criteria help?" 16th Annual Computer Security Applications Conference, December 2000.
http://www.ipc.on.ca/docs/PPPP025.pdf

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

(For more information about the Windows XP prefetch directory)
Windows XP Driver Development Kit. "Memory Management Enhancements." Microsoft Developer Network.
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/appendix/hh/appendix/enhancements5_0eecebea-e58b-4c95-8520-9b1dc2bc6196.xml.asp

APPENDIX A – About the privacy tools analyzed

Window Washer 5.5

Two sub-versions of Window Washer 5.5 (build # 5.5.1.19 and build # 5.5.1.240) were reviewed. The fully functional, 30-day trial package was downloaded from the website of its producer, Webroot Software Inc. at http://www.webroot.com. No error messages or alerts were generated during the installation process, and Window Washer reported its installation as successful.
Webroot describes Window Washer as a tool to protect the privacy of computer users. The company's list of software features includes:

- Simply, safely and easily wipe clean your online and offline tracks for complete privacy
- Shred function includes bleach to completely wipe out data
- Free plug-ins instantly detect and clean up more than 60 popular programs (Webroot Product Information).

Instead of simply deleting these records, Window Washer says it securely eradicates them so that they cannot be recovered.

> **Bleach for Extra Security**
> Completely overwrite files with random characters making them unrecoverable by undelete or unerase utilities - a security feature which exceeds the tough standards of the Department of Defense and the National Security Agency (Webroot Product Information).

Webroot is a privately held company based in Boulder, Colorado and has been operating since 1997. Most of Webroot's other software offerings relate to privacy issues. They include anti-spam, anti-phishing and anti-spyware applications – the last also marketed to enterprises. Webroot also sells a personal firewall and an anonymizing proxy for web browsing privacy.

In September 2004, the company announced that Michael Irwin, the former chief financial officer of anti-spam technology developer Brightmail Inc., had joined Webroot as CFO to help prepare the company for a public stock offering. http://www.webroot.com/company/pressreleases/20040914-finance/

Windows & Internet Cleaner

A fully functional, 15-day trial version of Windows & Internet Cleaner Professional 3.60 was retrieved from the website of NeoImagic Computing Inc (http://www.neoimagic.com). Some internal configuration displays and menus referred to the software as Privacy Eraser Pro, and checking screenshots of that package available on the http://www.privacyeraser.com

website suggests Windows & Internet Cleaner is a re-branded edition of Privacy Eraser. Whether there are any functional differences isn't clear, but configuration options appear the same. Windows & Internet Cleaner installed cleanly with no reported errors.

The company offers a range of software products that include applications for screensaver creation and managing and sharing digital images. The company doesn't provide a physical address on the website; the domain is registered to an entity in LiuZhou, China.

CyberScrub Pro

A 15-day trial package of CyberScrub Pro 3.5 was downloaded from the company website (http://www.cyberscrub.com). The program installed without errors.

CyberScrub LLC is based in Alpharetta, Georgia, near Atlanta. It also makes an anti-virus product. CyberScrub lists among its clients the U.S. Air Force and Army, the Departments of the Interior and Defense and other federal, state and municipal agencies. The company has received a purchasing schedule from the U.S. government's General Services Administration (GSA). "Other clients include the United Nations, major healthcare providers and Fortune 100 companies," according to its website.

CyberScrub sends periodic e-mails to those who registered to try its privacy tools, containing tips on the tool's use and reminders about the privacy exposure of using computers:

> Remember, "Delete" doesn't mean "Erase". Files and data may come back to haunt you. All your Internet tracks are recorded as well, and every picture you view is written to your hard drive." (CyberScrub e-mail)

Evidence Eliminator

No trial version of the latest Evidence Eliminator product was available. Previous versions for which trials are available caution that functionality is limited on Windows NTFS filesystems. So, a fully licensed version was tested. The software reported its version as 5.058, build 9. No errors were reported on installation. However, an alert box directed the user to consult help documentation for Windows NT systems because "certain configurations are required" for Evidence Eliminator's operation in this version of Windows.

Evidence Eliminator is produced by Robin Hood Software Ltd., a privately held British company based in Nottingham, England. The company says it specializes "in providing complete, one-click anti-forensic software solutions

for end-user Microsoft Windows installations." According to documents Robin Hood filed in July 2004 with the UK's Registrar of Companies, two individuals – Andrew S. Churchill and Robert H. Ride – each own one of the company's two shares and are its sole directors. Both list their occupations as "sales."

Evidence Eliminator is one of the most heavily advertised counter-forensic products on the web. Robin Hood has drawn criticism of its marketing tactics, exemplified by the warning from Evidence Eliminator's home page (http://www.evidence-eliminator.com/product.d2w) excerpted below.

> Do you surf the internet and send **E-mail** at work? Your work PC will be **full of evidence**. It is becoming common in the workplace for companies to copy and investigate the contents of workers computers out of hours - without your consent or knowledge. This is perfectly legal and it is happening **now**! Your job could be at risk, what would happen to you if you **lost your job**? People like you are losing their jobs right now because of their Internet activities … .

The company's mission statement reads, in part:

> As technology advances and people find new ways of sharing information, snoops use the same technology to find new ways of intruding in people's lives.
> Our highly-motivated development team takes pride and satisfaction in being the first in the world to offer convenient, fully tested and verified protection against forensic analysis of hard disk drives.

Acronis Privacy Expert

A trial version of the Acronis Privacy Expert 7.0 tool was tested. During installation, the software (which was tagged as build# 7.0.0.541) stated that it was a fully functional version limited to 15 days of use. The Privacy Expert package also offers tools to combat spyware and control Web browser pop-ups. These tools weren't installed where the option to not do so was available, and the features installed weren't employed during the testing phase.

Headquartered in San Francisco, Acronis has offices in the United States, Europe and Asia and sells its products through resellers and directly on the Web. The company was founded by Russian entrepreneur Serguei Beloussovis, who heads the SWSoft group (http://www.sw-soft.com/en/company/team/).

According to the company's website, Acronis produces a range of software, including "disaster recovery, backup and restore, partitioning, boot management, privacy, data migration, and other storage management products for enterprises, corporations and consumers of any qualification."

SecureClean

A time-limited trial version of SecureClean 4 was tested; it reported its build number as 04.08.25.0. The software is distributed by White Canyon Inc. of Utah, which also produces tools to completely wipe digital storage media and a secure password storage application.

White Canyon markets SecureClean to both individuals and organizations. In the latter case, SecureClean is framed as a compliance tool to help avoid inadvertent data exposure by organizations. White Canyon bills SecureClean as using Department of Defense-approved technology, apparently a reference to following the DoD 5220.22-M standard.

Over the past six years, SecureClean has become an accepted and well proven means of secure document retirement. The SecureClean Administrator was created to help system administrators install and maintain SecureClean on medium to large computer networks.

SecureClean uses the same disk sanitizing methods developed by the U.S. Department of Defense! Please contact sales for support documentation.

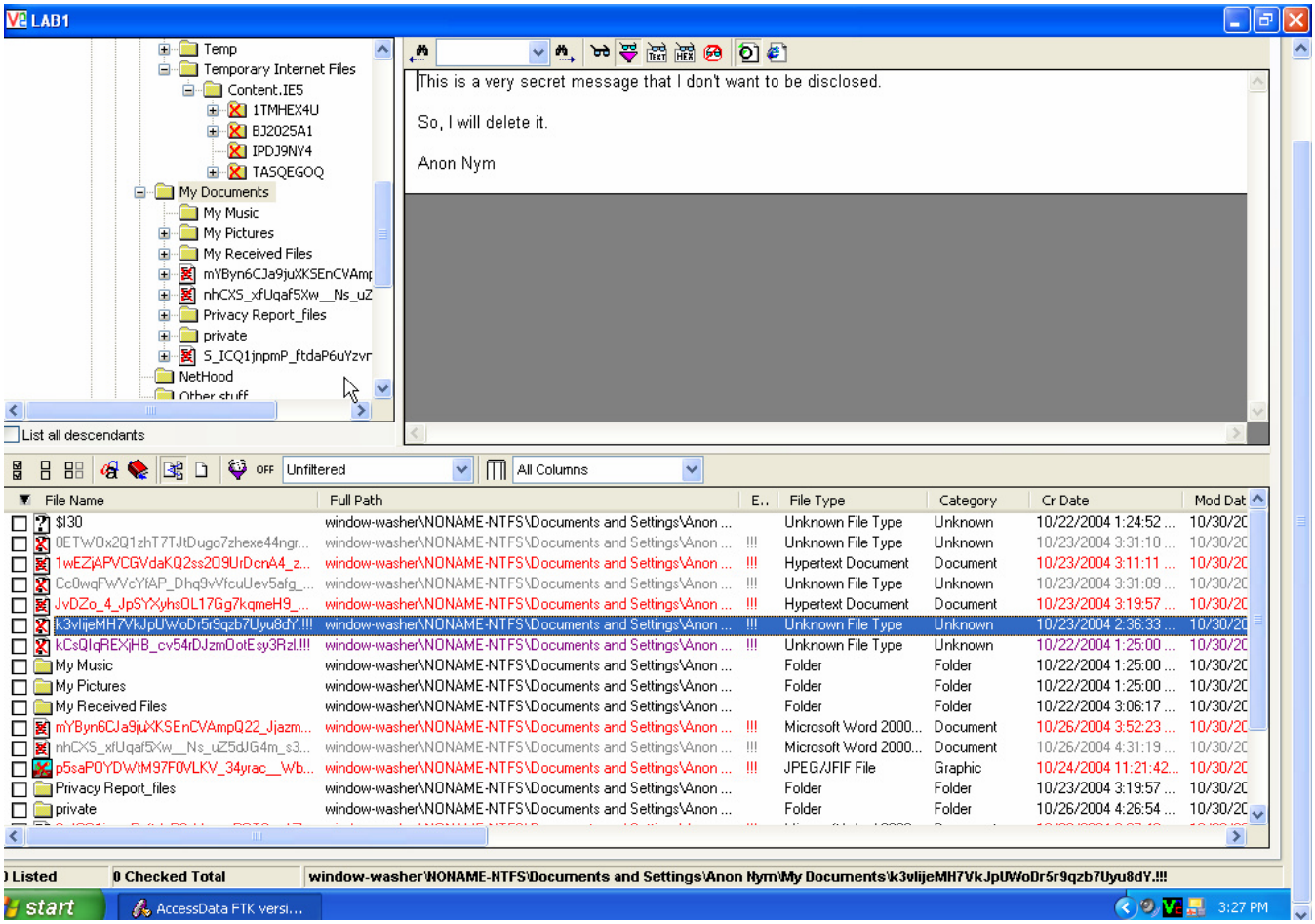
APPENDIX B – Individual tools' test results

Window Washer

WW-1

Window Washer proved largely ineffective at privacy protection, demonstrating several critical implementation errors. The major underlying flaw was that it did not, contrary to its claim, overwrite the data stored in files that it deleted. Instead, Window Washer simply renamed the targeted file and marked it as deleted in the filesystem. When the filesystem data is viewed with low-level tools, the pattern of deleted files is apparent and distinctive. In addition, although the pattern overwriting the filenames is pseudo-random, the file suffix created by Window Washer is always ".!!!", which greatly simplifies isolating the records of Window Washer-deleted files. This draws attention to precisely that material that the user wanted to keep private.

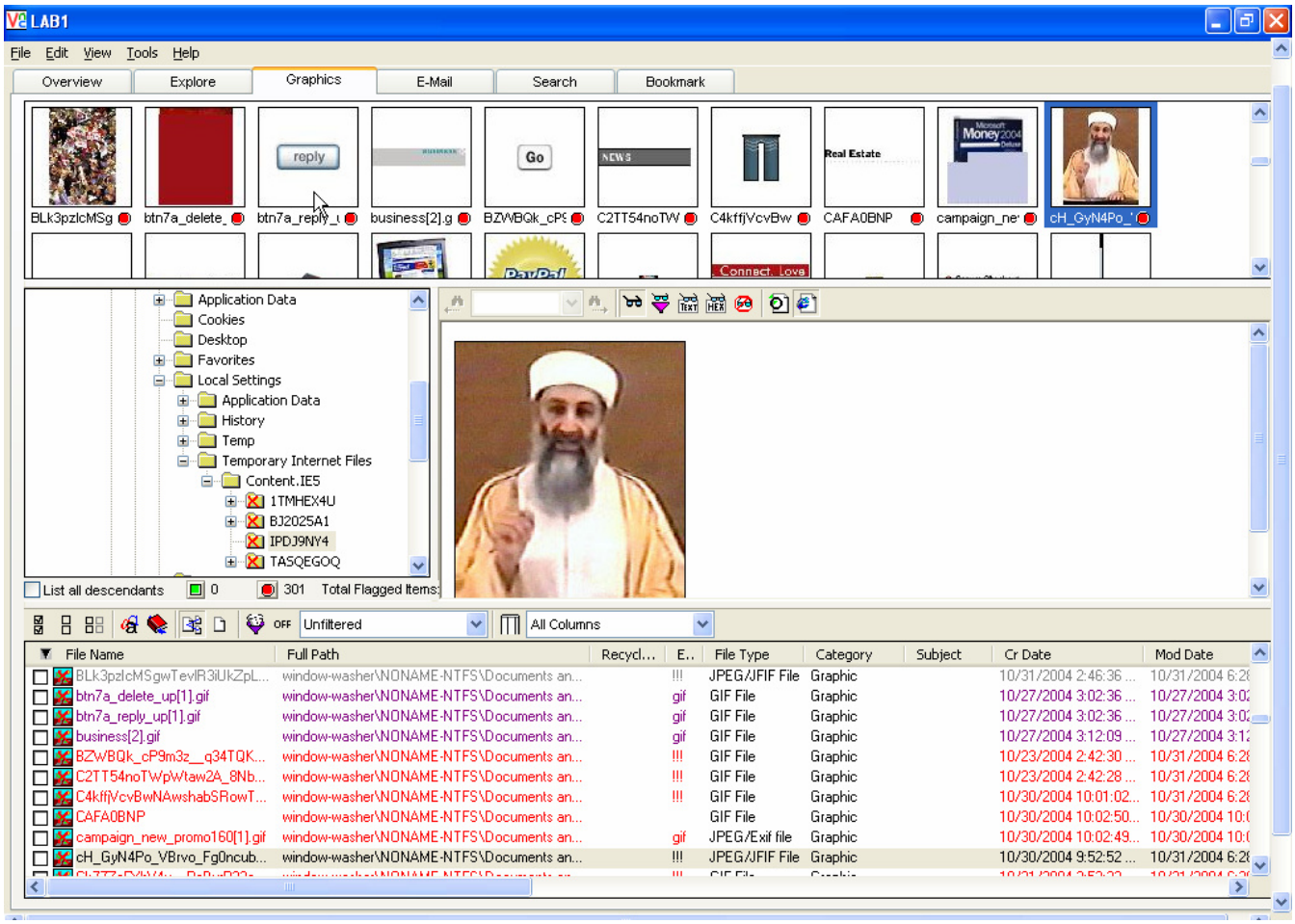
The following screenshot shows the listing of "deleted" files in the My Documents directory as viewed in the FTK forensic application. Note the scrambled filenames. The highlighted file's content appears in the upper right panel.



Viewing contents of deleted files in FTK

Comparing the content and directory structure of the My Documents folder after Window Washer shows that almost all of the files originally available on the test system (see Appendix E) can be recovered.

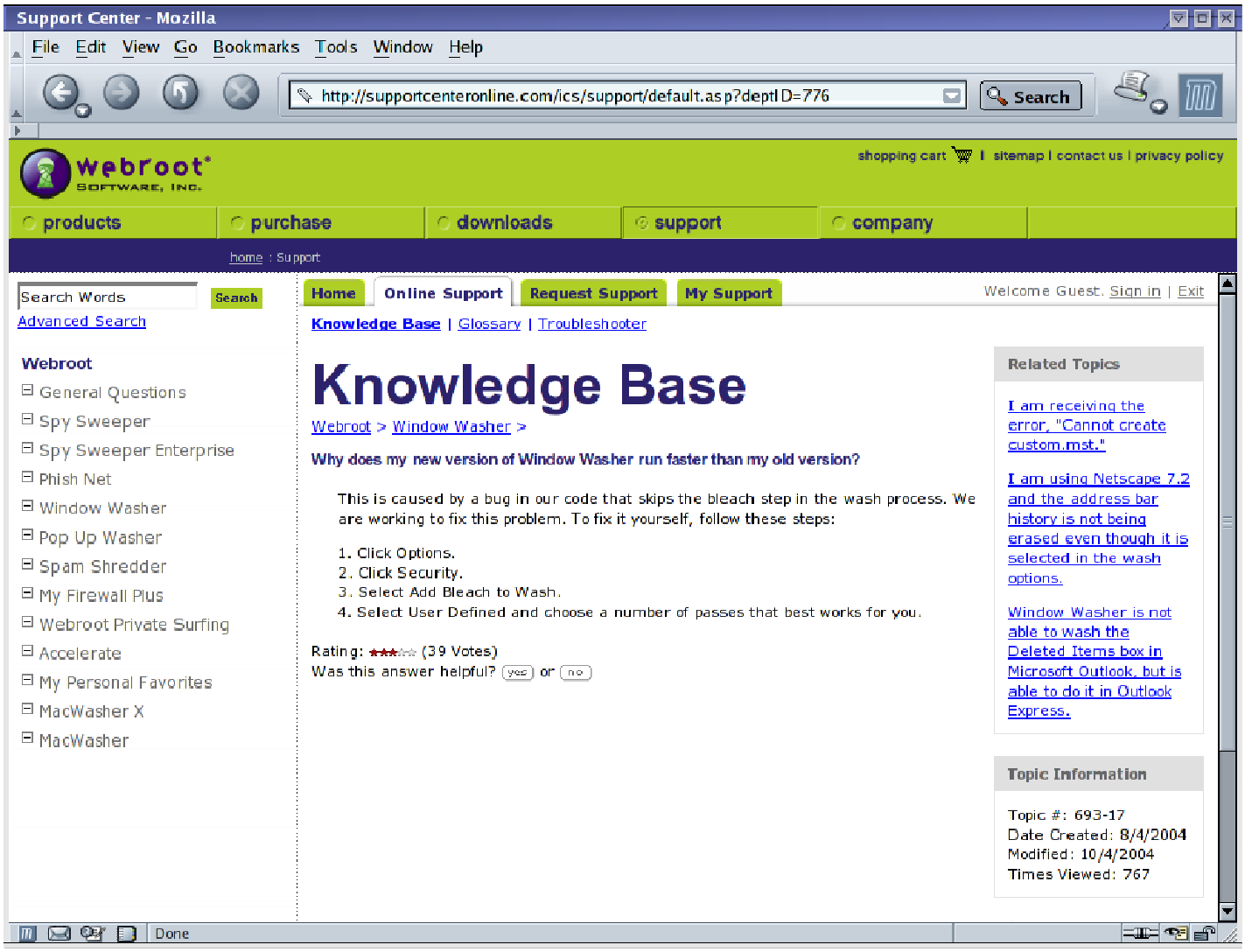
The same "washing process" leaves files cached from Internet browsing sessions recoverable. FTK is displaying the recoverable graphic content from one of the Temporary Internet Files subdirectory in the following screenshot:



Recovering cached browsing files

Window Washer takes a similar approach to the deletion of e-mail records from Outlook Express, renaming the selected database files and then marking them deleted – but not overwriting their content.

(See the preceding Case Study: Window Washer, for a narration about this failure and the steps leading to the testing of a second version.)



Window Washer statement about wiping bug

The WW-1 testing process was repeated with a suggested workaround: setting user-defined wiping passes to one for the "bleaching" process (see above). However, the tool again failed to wipe the targeted files after employing the suggested workaround. No other notification of this privacy-critical bug could be found on the Webroot site.

Also recoverable because they had not been overwritten were:
Cookies; shortcuts to recently used files in a directory that Windows creates to keep track of this on a per-user basis; temporary files created in the user's Windows "/temp" directory.

Because Window Washer didn't attempt to wipe unallocated space on the disk, it was possible to recover intact (along with file metadata, such as original name and creation time) files that had been previously deleted by the operating system or applications, such as temporary files created by Word and the Internet Explorer History file deleted after three days by

Windows.

Deleting and attempting to wipe the files under the My Document tree required creating a Window Washer "plug-in" to specify the action. Window Washer provides simple, step-by-step prompts to create the plug-in. However, the program also creates a list of the files to be deleted by the plug-in and stores them in a plain-text file with an ".mst" suffix in a subdirectory called "plugins" in the Window Washer program directory. This reveals not only the names and path structure of the deleted files, but also discloses that they were selected for "wiping" by the user.

Window Washer completely missed some categories of sensitive data, including: Windows shortcuts under the test user's "\Application Data\Microsoft\Office\Recent\" directory, which provide data about Office documents the user last worked with; the Internet Explorer history file, which was undeleted and intact.

As for sensitive data in the registry, Window Washer deleted the form data stored in Internet Explorer's auto-form-completion scheme and the list of typed URLs. However, it left untouched information about files the test user had worked with, which is stored in subkeys under the user hive's Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 branch.

Window Washer left untouched backup copies of the test user's registry created by Windows XP's system restore function, which allowed the full recovery of form data, typedURLs and other data from activity up to the most recent restore point.

WW-2

The second test version of Window Washer remedied its failure to overwrite files. It also improved its performance in other areas, such as adopting a less predictable file renaming schema. However, we encountered another significant operational glitch, and the tool overall still allowed substantial privacy exposure. The main contribution to this exposure was the absence of a mechanism to wipe unallocated disk space. As noted in the previous test, this permitted the retrieval of a wide range of potentially sensitive data, including material cached during web browsing sessions, images and documents.

Window Washer incompletely wiped some files in the web browser cache directory, allowing for the recovery of much of the original content of some viewed HTML pages including several from Webmail browsing sessions. A bigger bug apparently stopped WW-2 from deleting the subdirectories to the user's My Documents folder, although it was configured to wipe the entire directory tree. As a result, the subdirectories and their contents were left untouched.

WW-2 more thoroughly wiped the registry of user activity data. However, path and file name information about deleted files and directories was recoverable from the Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell key and related keys under the user's registry hive. WW-2 failed to remove files from the Windows system prefetch folder that contained information about the names and path of deleted files.

WW-2 also left untouched backup copies of the test user's registry created by Windows XP's system restore function, creating the same exposure in this regard as present in WW-1.

In terms of operational signature, WW-2 reduced its footprint from WW-1. Wiped files were renamed with an assortment of lowercase letters used for both the filename and a three-letter extension, such as "fpubhmrwbgkpuydin.ydh." The length of the filename also varied. The characters used to overwrite the data area varied from file to file, but always consisted of the same character repeated for the full size of the file overwritten.

Windows & Internet Cleaner Professional

W&I Cleaner fell short of its claimed performance in a few key areas, and contained further implementation oversights that disclosed some sensitive information. The program did perform wiping on unallocated space and targeted files, but missed some areas.

W&I Cleaner also can "scramble" file names before wiping them to remove suggestions about the files types and what they contained. However, like Window Washer, it uses a predictable pattern of pseudo-random characters that leaves a "signature" record that may be used to infer what tool was used and how many files were wiped and from where. W&I Cleaner renames its files with sets of hexadecimal values, separated by hyphens, in the pattern xxxx-xx-xx-xx-xxxxxx. The file suffix was always ".tmp"

Searching for phrases known to be contained in the original sensitive files revealed areas of unallocated space that had not been completely wiped. This omission was sufficient to allow the recovery of the following types of information: substantially complete text contents from Word documents, cached HTML from views of the users Hotmail account, and metadata contained within MS Office documents. Why wiping failed in some unallocated space wasn't immediately apparent, but it appears that at least some latent data may have existed in a Windows pagefile. It's possible that the pagefile was at some point deleted or truncated but not completely wiped.

Like Window Washer, W&I Cleaner didn't erase the back-up registry files

created for the test user by Windows XP's system restore function. These contained completed usage records up to the restore point.

W&I Cleaner failed to delete e-mail in Outlook Express' deleted mail folder, which had been designated for deletion and wiping. It also failed to wipe two Internet Explorer history files, which were deleted but recoverable intact.

Some of the special files that contain listings of directory contents under the NTFS filesystem were also recoverable, revealing the names of files and directories within a few of the wiped directories. A number of other tiny files, mainly GIF images but including a few text and HTML snippets, were retrievable from the Master File Table.

Similarly, some small gif images and fragments of HTML pages were recoverable from the NTFS journal log, a file used to store partial changes to the filesystem to make recovering from a crash simpler and faster.

Analysis of the Windows Registry indicates the privacy program deleted most of the targeted data from this repository. However, W&I Cleaner stores most of its own configuration settings in the user registry, allowing easy analysis of what the application had been set to wipe. In addition, the privacy tool missed the records of recently saved Word documents, stored in the test user's registry hive under the "Software\Microsoft\Office\9.0\Common\Open Find\Microsoft Word\Settings\Save As\File Name MRU" key.

CyberScrub Professional

CyberScrub showed fewer implementation weaknesses and privacy disclosures than most of the tools tested. However, it also missed sensitive information and didn't completely obliterate metadata about files targeted for wiping.

CyberScrub also renames files it wipes to eliminate information about the files types and what they contained. Its renaming scheme creates names of varying lengths of pseudo-random combinations of capital letters. File suffixes are three-letter combinations of capitals. Wiped file lengths are set to zero. The lack of a more consistent pattern to the file renaming scheme makes searching for the records of wiped files slightly harder and is a less clear signature of the tool's use. However, records of a deleted file called "D889D1C1.wip" were left in the root directory. This file appears to be an artifact created by Cyber scrub's unallocated-space-wiping process and may provide a more consistent signature of the use of the tool. (This seems to be confirmed by a CyberScrub registry entry for the ".wip" file suffix.)

CyberScrub didn't apply the file-renaming approach to the contents of the Internet Explorer cache directory. So, although the contents of the files in the directory was overwritten, the file names, file sizes, and information

about when the files were created, accessed, etc were available. The same sort of information was recoverable for the contents of the user's Windows temporary directory.

Searching for phrases known to be contained in the original sensitive files revealed areas of unallocated space that had not been completely wiped. The information recoverable from these areas was highly fragmented and didn't include substantial portions of sensitive text or similar content. Some cached HTML snippets and file name information was recoverable.

CyberScrub didn't offer the option of wiping e-mail stored in Outlook Express archives.

The program also failed to delete Microsoft Office's records of files the user worked with recently. This data was in the form of shortcut files (links) that contain metadata about the Office files opened, edited, printed and saved by the user.

Some of the special files that contain listings of directory contents under the NTFS filesystem were also recoverable, revealing the names of files and directories within a few of the wiped directories. A number of other tiny files, mainly GIF images but including a few text and HTML snippets, were retrievable from the Master File Table. Likewise, the names of some files deleted before CyberScrub was used were recoverable, along with other data, as long as their slot in the MFT index records had not been reused.

More file names, including the full path of many of the files in the test user's My Documents directory, were recoverable from a pre-fetch file used by Windows to speed the loading of certain programs.

Some small gif images and fragments of HTML pages were recoverable from the NTFS journal log, a file used to store partial changes to the filesystem to make recovering from a crash more reliable and faster.

Analysis of the Windows Registry indicates the privacy program missed a principal listing of files worked with, stored in the test user's registry hive under the Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs entry. It also missed records of recently saved Word documents, stored under the "Software\Microsoft\Office\9.0\Common\Open Find\Microsoft Word\Settings\Save As\File Name MRU" key. CyberScrub stores configuration settings in the user registry, allowing easy analysis of what the application was set to wipe.

Evidence Eliminator

While Evidence Eliminator was among the more effective tools in scope and thoroughness of eradicating targeted records and wiping unallocated space

on the disk. However, the program exhibited a significant implementation flaw that allowed the recovery of sensitive information from some targeted records. These were copied to a temporary directory that EE subsequently failed to delete.

EE sanitizes metadata about the files it wipes by overwriting file names, filesystem timestamps and truncating the reported file length to zero. Its renaming scheme creates names of 243 characters, with no filename extensions (or suffixes). 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 that is wiped and renamed. The following is an example:

```
0000002825wtkdvjiiugvwgveodruvlmdptxgpgfyrqnxpxyjajkqrienrnebnzhoshuyfzhdvzvvv
veszlikswlhqpwbetowmznlvzquveyvhkrkcidsmpgpjrxjgpzaxcffvdxynlxiikdnhgachijkuajmdf
dcvxbupesrwdyykqfckndbqwittwnyfmtcesftoxtyrnfdwwoblkpcvzwseokhydmcvtvodbrwyvv
mewuoge
```

EE stores a series of files in the "\Program Files\Evidence Eliminator\Data" directory that contain plaintext configuration entries for the program, including information about some files and directories targeted for wiping and what plug-ins are active.

EE, alone amongst the privacy tools, wiped the Windows-created prefetch files that contained, among other information, the full path and names of many of the files targeted for deletion.

Searches for phrases seeded in the test system's files recovered no significant portions of relevant data from unallocated space or, with the exceptions noted below, from files targeted for deletion. However, EE missed files that contained user activity data created by the Napster application and Macromedia's Flash player, despite data-erasure plug-ins for both being selected.

Some of the special files that contain listings of directory contents under the NTFS filesystem were recoverable, revealing the names of files and directories within a couple of the wiped directories. A number of other tiny files, mainly GIF images but including a few text and HTML snippets, were retrievable from the "resident data" records of the Master File Table.

Analysis of the Windows Registry indicates the privacy program missed a few key entries that provided information about the directories and files previously existing under the My Documents tree. An example of is the "Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell" key, which contained the names of many of the files and folders in the My Documents directory.

The most significant information leak occurred when EE copied a number of Windows-maintained files – including the index files to the Internet Explorer

browser cache and cookie records, as well as the browser history file – to a temporary directory, named __eetemp. These files were renamed but otherwise intact. Some of the other files in the folder appeared to have originated from the Windows\prefetch folder. According to EE's documentation, the contents of this directory should be wiped once the computer is rebooted.

> Locked files: Evidence Eliminator™ can delete "Locked" system files like the index.dat cache files of Internet Explorer. These files are renamed to .TMP files in the __eetemp\ folder on each drive and cleaned during the reboot procedure. Locked files can only be cleaned by running the full Safe Shutdown/Safe Restart of Evidence Eliminator™. They cannot be cleaned by right-clicking them in Windows Explorer.

However, EE failed to wipe the directory and its contents after a Safe Shutdown and Restart cycle. This left recoverable Explorer history information (which includes some files viewed or manipulated with the Windows Explorer file browser), such as the following:

URL	http://www.nytimes.com/2004/10/29/politics/campaign/29CND-CAMP.html?hp&ex=1099108800&en=cf32ca365ccac49d&ei=5094&partner=homepage
User name	Anon Nym
Page title	The New York Times > Washington > Campaign 2004 > Bush and Kerry Offer Competing Visions of the Future
Last Accessed (UTC)	10/30/2004 2:02:51 AM
Last Modified (UTC)	10/30/2004 2:02:51 AM
Last Checked (UTC)	10/30/2004 2:02:52 AM
Expires (UTC)	11/8/2004 1:55:42 AM
Hits	2

URL	file:///C:/Documents%20and%20Settings/Anon%20Nym/My%20Documents/Privacy%20Report.htm
User name	Anon Nym
Last Accessed (UTC)	10/30/2004 2:07:58 AM
Last Modified (UTC)	10/30/2004 2:07:58 AM
Last Checked (UTC)	10/30/2004 2:08:00 AM

Acronis Privacy Expert

Privacy Expert allowed some significant information leaks through implementation and design shortfalls. While data-wiping was used both for targeted files and unallocated space, Privacy Expert left metadata information about the files erased and left some data recoverable from unallocated space. The program, as most of the others tested, also missed entirely some repositories of sensitive information.

Privacy Expert does not "scramble" file names by renaming files before wiping them. It also doesn't overwrite other metadata about the files wiped, such as their size, date of creation and modification, and other attributes. This may allow insight into the type of files erased and hint at their contents.

Searching for phrases known to be contained in files created for the test benchmark system revealed areas of unallocated space that had not been wiped. They included fragmentary registry data that contained e-mail account information and file and directory names that had been wiped. Part of an HTML page viewed during a Hotmail session was also recoverable.

Privacy Expert missed the index files Windows uses to keep track of the contents of the Recycle Bin and the Internet Explorer cache directories. So, while the contents of both were wiped, information about the files in each location was available. For example, for a file cleansed from the Recycle Bin, the following information is stored in the bin's index:

Filename	Dc3.txt
Original Name	C:\Documents and Settings\Anon Nym\My Documents\Copy (11) of secret.txt
Date Recycled	10/23/2004 2:31:22 PM
Removed from Bin	Yes

Like most of the other privacy tools, Privacy Expert 7.0 didn't erase the back-up registry files created for the test user by Windows XP's system restore function. These contained completed usage records up to the restore point. It also didn't purge Windows' prefetch folder, which contained files that mapped out the full path and name of wiped files and directories. In addition, Privacy Expert left untouched shortcut files created by Microsoft Office that provide information about recently used Office documents. For example:

Link target information	
Local Path	C:\Documents and Settings\Anon Nym\My Documents\Privacy Report.htm
Volume Type	Fixed Disk
Volume Serial Number	68B0-7704
File size	104149

Creation time (UTC)	10/23/2004 7:19:57 PM
Last write time (UTC)	10/30/2004 1:33:27 AM
Last access time (UTC)	10/30/2004 1:33:30 AM
File attributes	
Archive	
Optional fields	
Relative Path	..\..\..\..\My Documents\Privacy Report.htm
Target system information	
NetBIOS name	test1
MAC address	00-00-e8-8b-93-dd

Acronis successfully wiped mail records from two folders selected in Outlook Express. However, like all of the other programs, Acronis encountered difficulties wiping data residing in the NTFS Master File Table. The tiny files recoverable included two cookies from website visits.

Analysis of the Windows Registry revealed the privacy program missed some records of user activity. These included the "Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs" key and sub-keys, which revealed documents and similar files recently used. The privacy tool missed the records of recently saved Word documents, stored in the test user's registry hive under the "Software\Microsoft\Office\9.0\Common\Open Find\Microsoft Word\Settings\Save As\File Name MRU" key.

Acronis Privacy Expert kept plain-text logs of its activity that showed the classes of data it was set to delete but didn't reveal granular information, such as the specific files targeted.

SecureClean

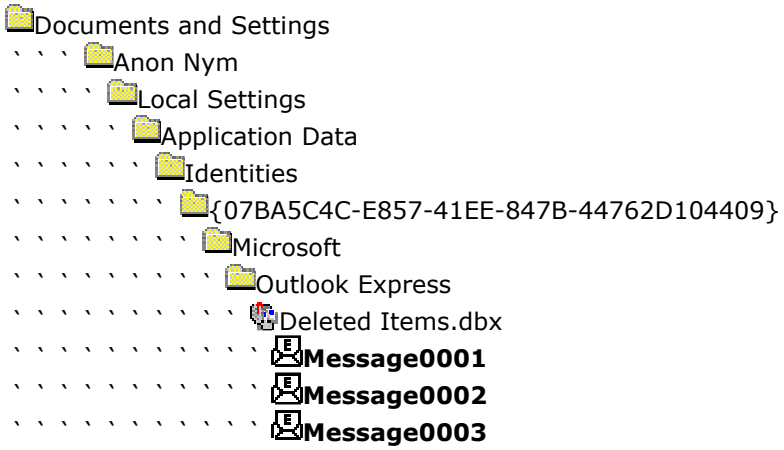
SecureClean's wiping of targeted files and unallocated disk space was relatively thorough. However, the tool missed a number of sensitive records and created detailed logs that recorded the full path and name of every file deleted. It also failed to wipe e-mail messages that it was configured to eliminate.

SecureClean renames files it wipes to obscure the filesystem records about the wiped files' names and types. It uses a predictable renaming scheme that

creates new file names by appending a six-digit number to the capital letters SC. The number is incremented by one for each new file name and all the files are give the suffix T~P, as in SC000135.T~P. Wiped file lengths are set to zero. This scheme represents a clear signature of the tool's use, and conveys information about the number of files wiped in the numbering scheme used to rename files.

However, the full file path and name of wiped files was stored in plain text form in an activity log created by SecureClean and named "\Program Files\WhiteCanyon\SecureClean 4\SCDebug.dat." Similar information about wiped files was also recoverable from files in Windows' start-up accelerating prefetch folder, which SecureClean neglected.

SecureClean didn't wipe the contents of the Outlook Express deleted e-mail folder, although it had been configured to do so. The deleted mail was untouched and viewable from within the mail client.



The Windows Registry retained a few entries that provided the names of files and directories previously existing under the My Documents tree. For example, "Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\3" contained file and directory names.

Other file names and associated data were recoverable from the NTFS journal log, a file used to store partial changes to the filesystem to make recovering from a crash more reliable and faster. This data was in the format used by the MFT.

MFT-format data recovered from the filesystem journal

```
Copy of secret document.doc
FILE0
MYPROG~1.DOC
my program.doc
FILE0
e2RCRD(
POKERS~1.DOCeio
poker secrets.doc
FILE0
f2xl
f2RCRD(
300X25~1.GIF2ts
300x250_1.gifts
FILE0
BINLAD~1.184ets
binladen.1842ts
FILE0
g2RCRD(
COPYOF~1.DOCets
Copy of secret document.doc
FILE0
h2RCRD(
MYPROG~1.DOCets
my program.docs
FILE0
PARTIA~1.DOCets
Partial secrets.doc
```

APPENDIX C – Privacy tool configuration details

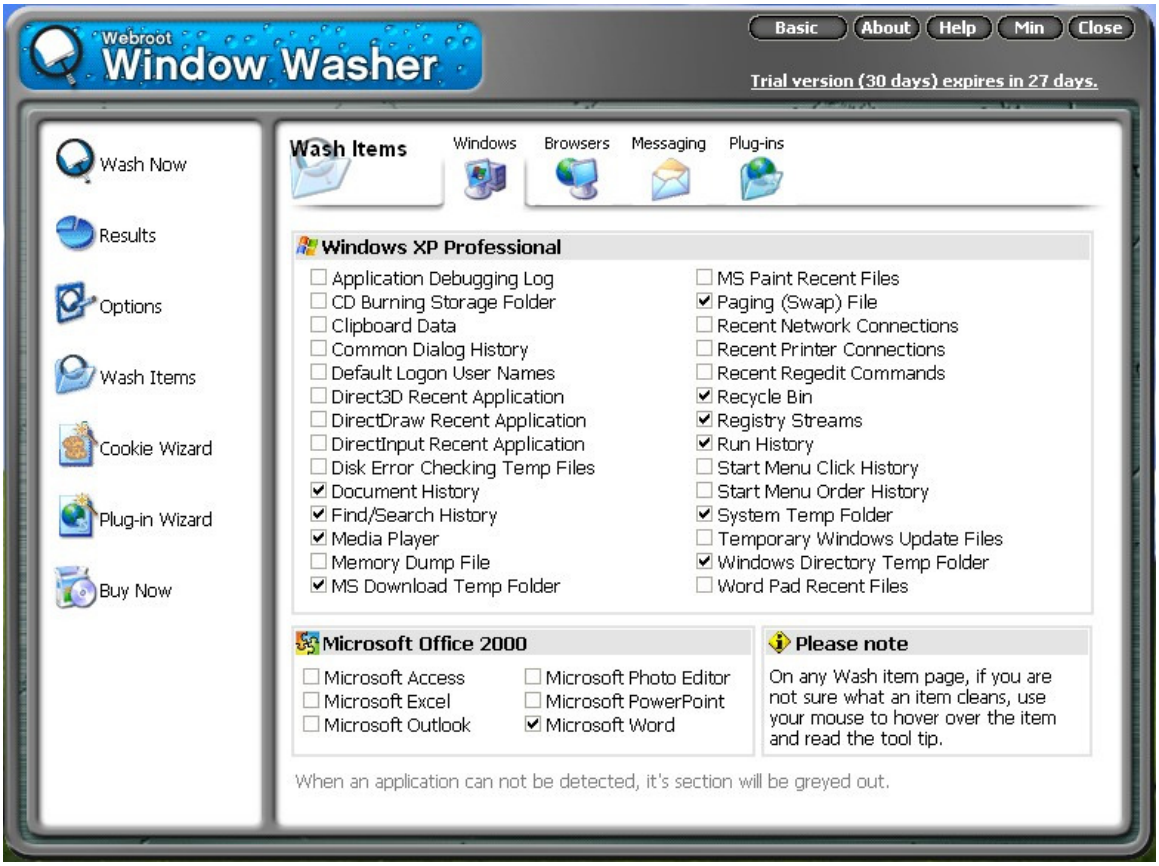
Window Washer 1 & 2 configuration

Both versions of Window Washer tested were configured similarly, using the advanced user interface.

In addition, a separate "plug-in" was created to wipe files in the test user's My Documents folder and all its sub-folders.

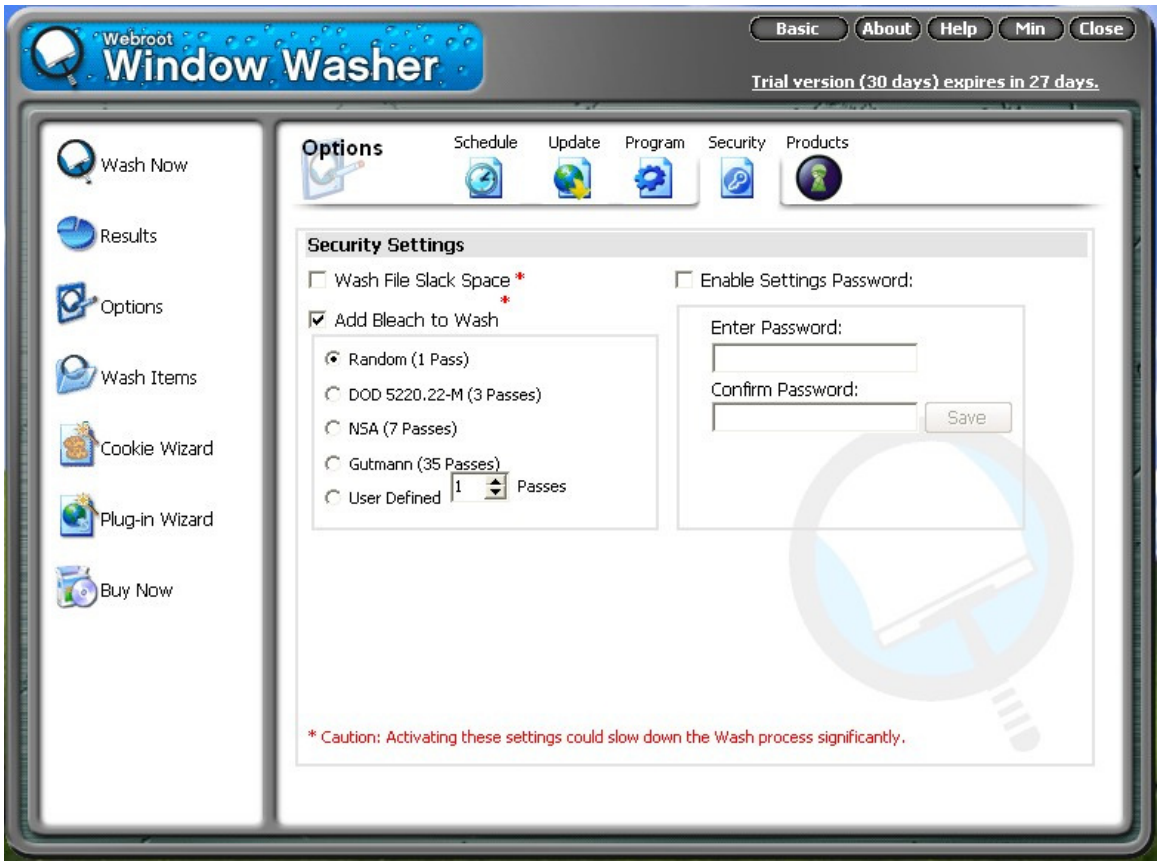
Under Window Washer's terminology, the "Add bleach to wash" option means the selected data is slated to be overwritten with random characters to make it unrecoverable.

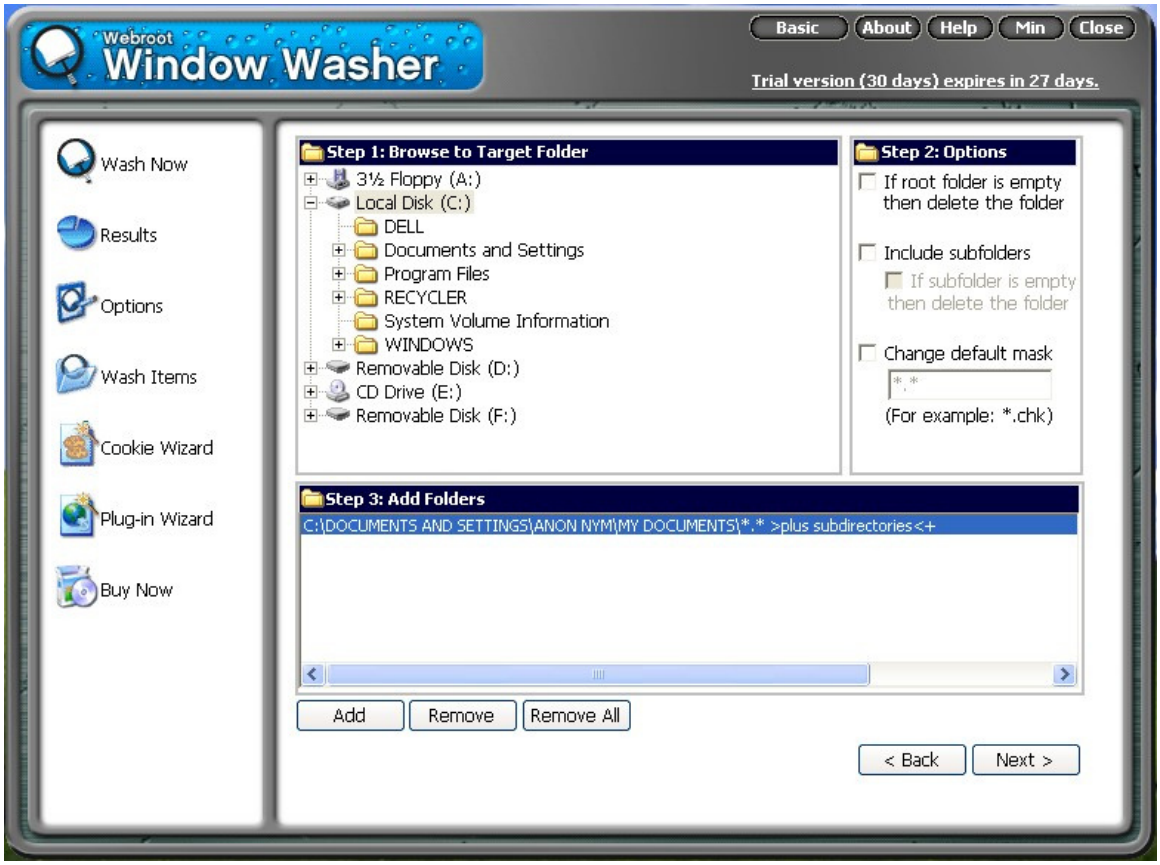
The following screenshots give an overview of the configuration settings.




Webroot
Window Washer
Basic
About
Help
Min
Close
Trial version (30 days) expires in 27 days.
Wash Now
Results
Options
Wash Items
Cookie Wizard
Plug-in Wizard
Buy Now
Wash Items
Windows
Browsers
Messaging
Plug-ins
Internet Explorer 6.0
Address Bar History
AutoComplete Form Data
Bleach Index.dat on Windows Startup
Cookies
Downloaded Folder Memory
History (Visited Sites)
Media Bar (Player) History
Setup Log File
Temporary Internet Files Folder
Netscape
Location Bar History
Form Manager Data
Cookies
Mail Trash
Disk Cache
Preferences
History (Visited Sites)
America Online
Address Bar History
AOL Internet Cache Folder
Additional Browser Options
Detect Running Browser
When an application can not be detected, it's section will be greyed out.

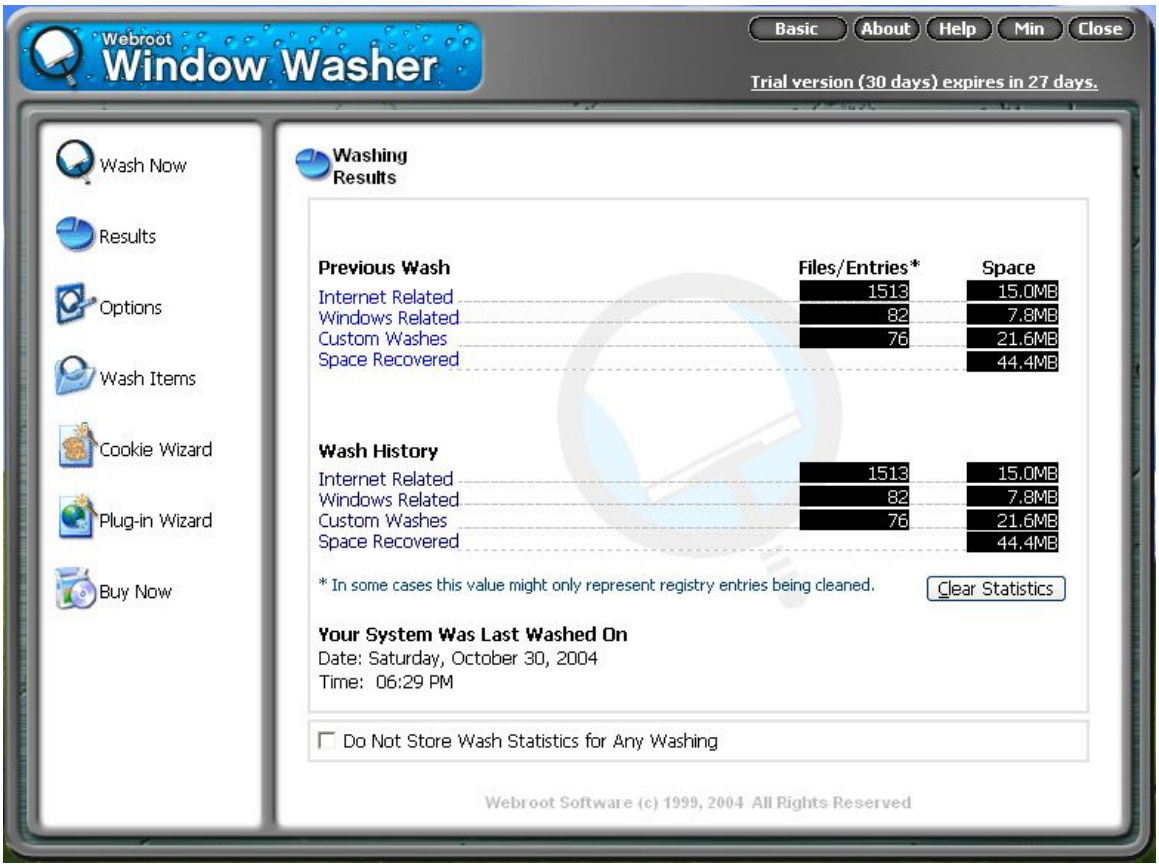

Webroot
Window Washer
Basic
About
Help
Min
Close
Trial version (30 days) expires in 27 days.
Wash Now
Results
Options
Wash Items
Cookie Wizard
Plug-in Wizard
Buy Now
Wash Items
Windows
Browsers
Messaging
Plug-ins
Outlook Express
Deleted Items Folder
Inbox Folder
Outbox Folder
Outlook Express Log File
Sent Items Folder
AOL Instant Messenger
Downloaded Files folder
Recent Screen Names
MSN Messenger
My Chat Log Folder
My Received Files Folder
ICQ
Bookmarks
Browser Cache
Contact Lists
Log Files
Received Files
Recent Chat History
Yahoo Messenger
Clear Pager Settings
Reset Yahoo Profiles
Temporary Internet Files
When an application can not be detected, it's section will be greyed out.


Webroot
Window Washer
Basic
About
Help
Min
Close
Trial version (30 days) expires in 27 days.
Wash Now
Results
Options
Wash Items
Cookie Wizard
Plug-in Wizard
Buy Now
Options
Schedule
Update
Program
Security
Products
Security Settings
Wash File Slack Space *
Add Bleach to Wash
Random (1 Pass)
DOD 5220.22-M (3 Passes)
NSA (7 Passes)
Gutmann (35 Passes)
User Defined
Passes
Enable Settings Password:
Enter Password:
Confirm Password:
Save
* Caution: Activating these settings could slow down the Wash process significantly.


Webroot
Window Washer
Basic
About
Help
Min
Close
Trial version (30 days) expires in 27 days.
Wash Now
Results
Options
Wash Items
Cookie Wizard
Plug-in Wizard
Buy Now
Step 1: Browse to Target Folder
3½ Floppy (A:)
Local Disk (C:)
DELL
Documents and Settings
Program Files
RECYCLER
System Volume Information
WINDOWS
Removable Disk (D:)
CD Drive (E:)
Removable Disk (F:)
Step 2: Options
If root folder is empty then delete the folder
Include subfolders
If subfolder is empty then delete the folder
Change default mask
.
(For example: *.chk)
Step 3: Add Folders
C:\DOCUMENTS AND SETTINGS\ANON NYM\MY DOCUMENTS*.* >plus subdirectories<+
Add
Remove
Remove All
< Back
Next >

Although Window Washer offered prepackaged plug-ins to clean up activity records for a number of after-market Windows applications – such as the Adobe Acrobat Reader for portable document format files, the WinZip compressed archive utility and the Gator online form filler – there was no plug-in for Napster.

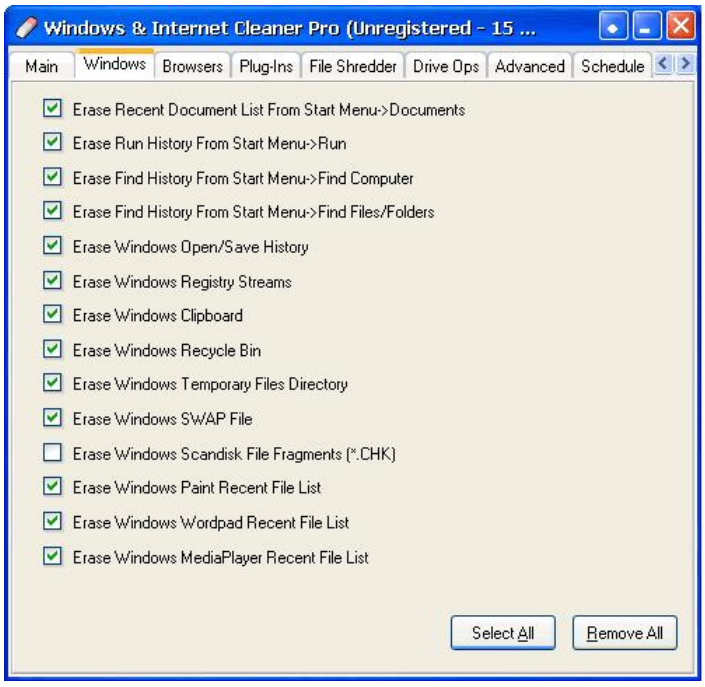
After configuration was completed and checked, the clean-up process was initiated and reported that it had completed after approximately one minute. The results screen reported "washing" 1,513 Internet-related files, 82 Windows system files and 76 files designated by the custom plug-in for deletion. No errors were reported.

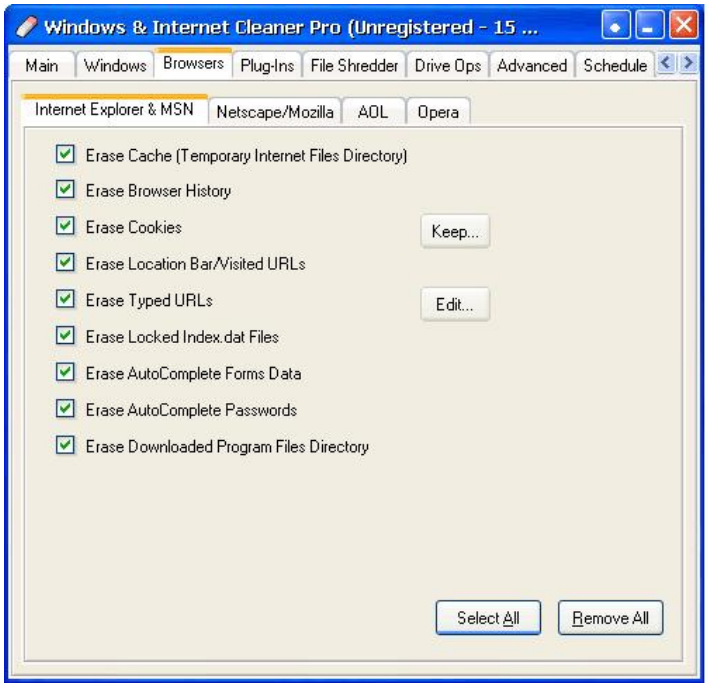


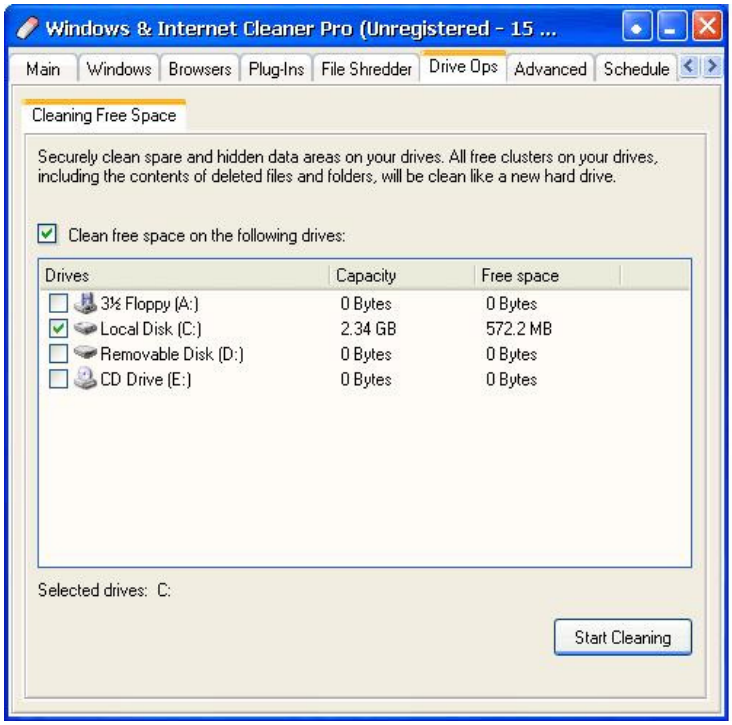
Windows & Internet Cleaner Professional configuration

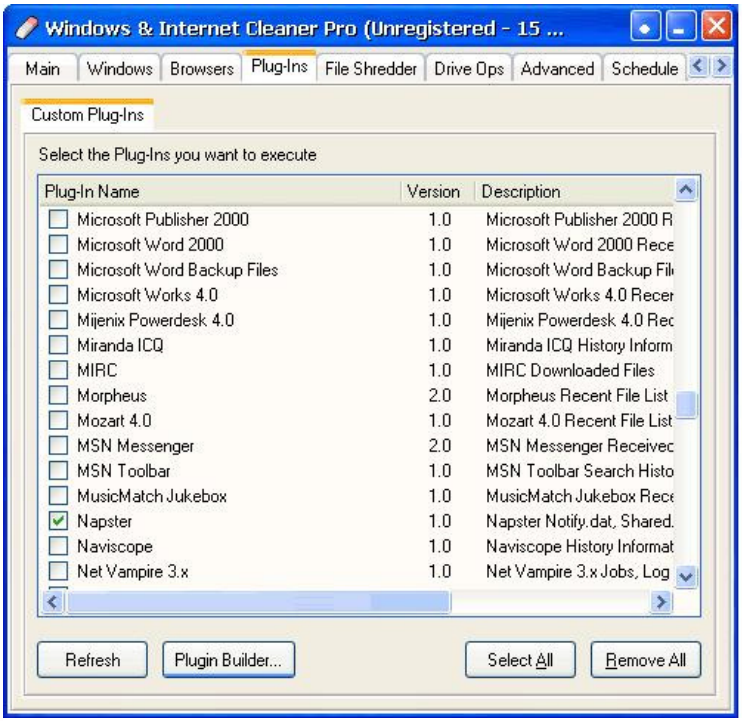
Options similar to those chosen for Window Washer were selected for Windows & Internet Cleaner, with the additional specification to wipe "free" or unallocated space on the disk.

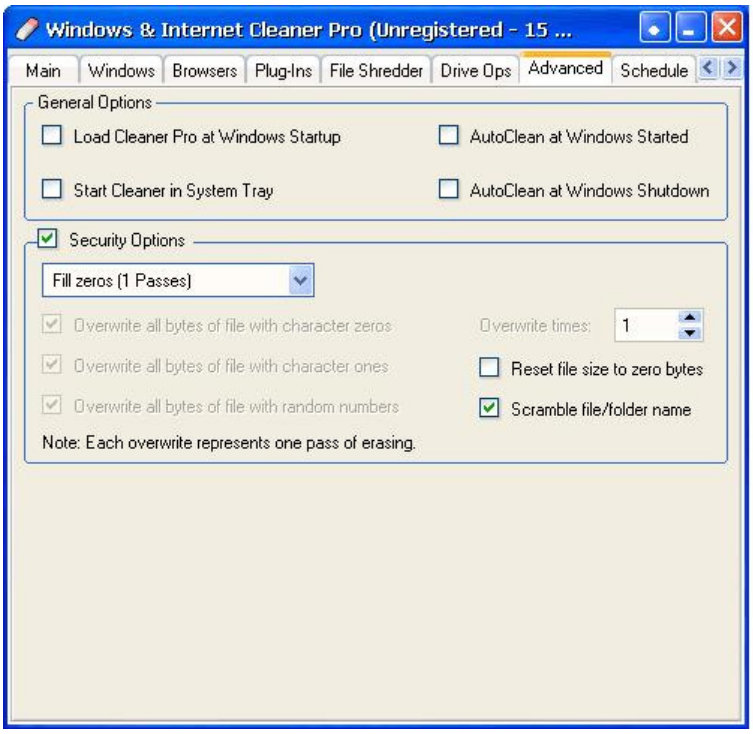
The following screenshots detail the configuration options selected:







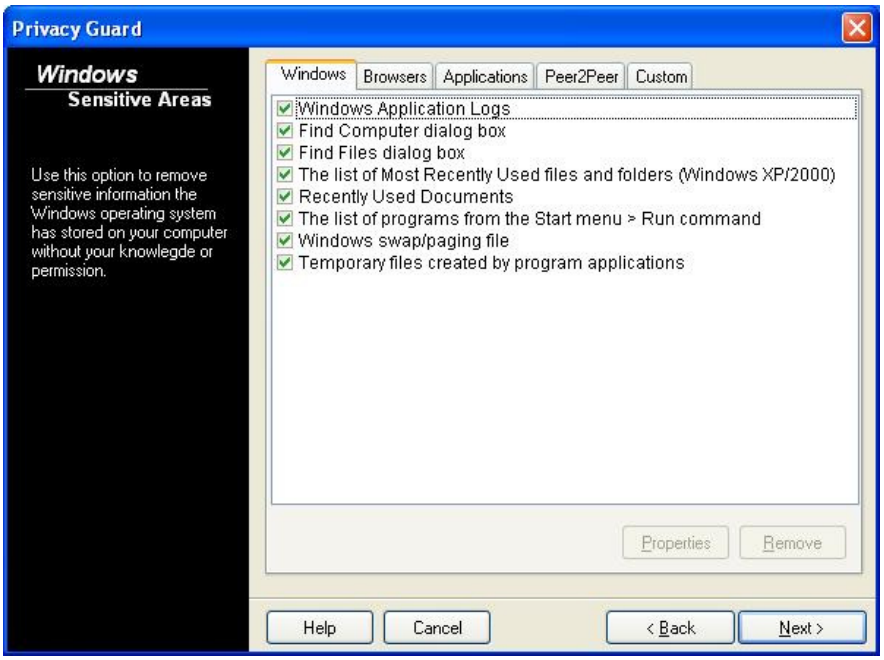


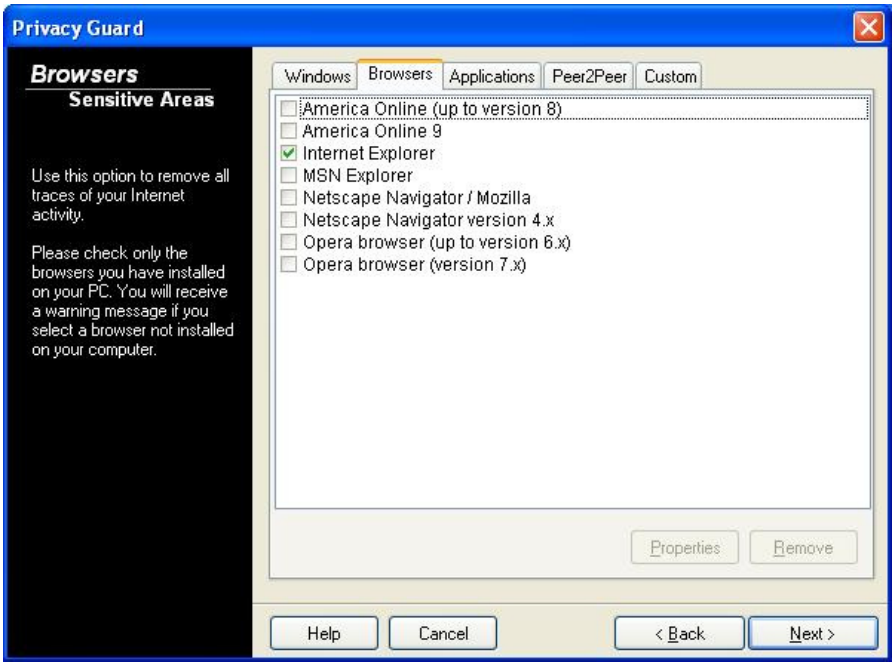

Windows & Internet Cleaner Pro (Unregistered - 15 ...
Main
Windows
Browsers
Plug-Ins
File Shredder
Drive Ops
Advanced
Schedule
General Options
Load Cleaner Pro at Windows Startup
AutoClean at Windows Started
Start Cleaner in System Tray
AutoClean at Windows Shutdown
Security Options
Fill zeros (1 Passes)
Overwrite all bytes of file with character zeros
Overwrite times:
1
Overwrite all bytes of file with character ones
Reset file size to zero bytes
Overwrite all bytes of file with random numbers
Scramble file/folder name
Note: Each overwrite represents one pass of erasing.

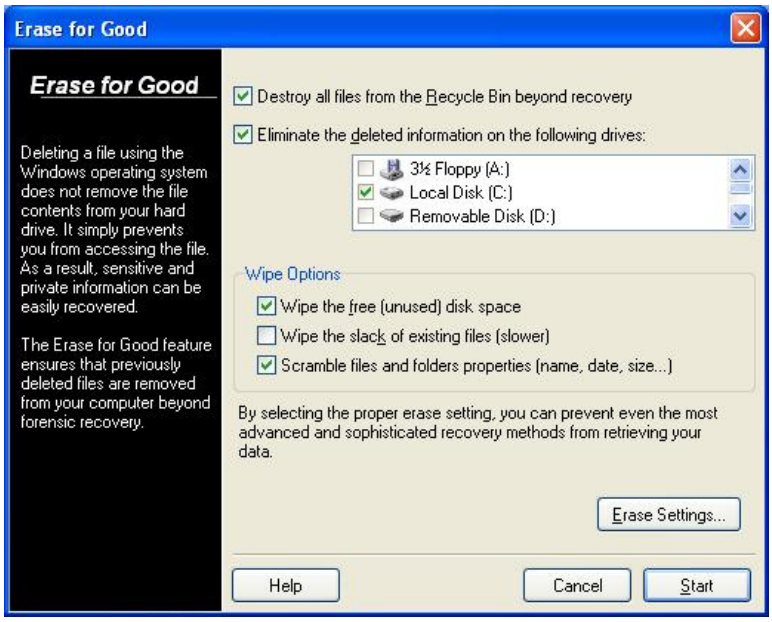
CyberScrub Professional configuration

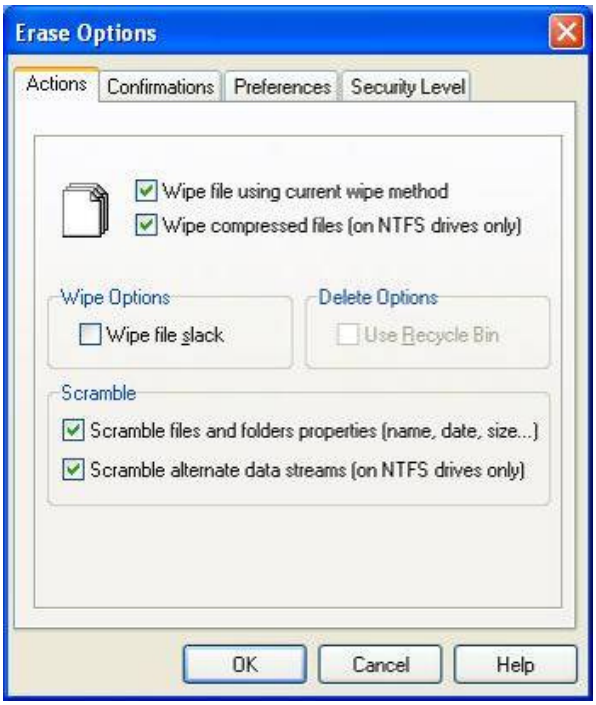
Options selected for CyberScrub Pro were consistent with those for the other privacy tools, and included the specification to wipe "free" or unallocated space on the disk.

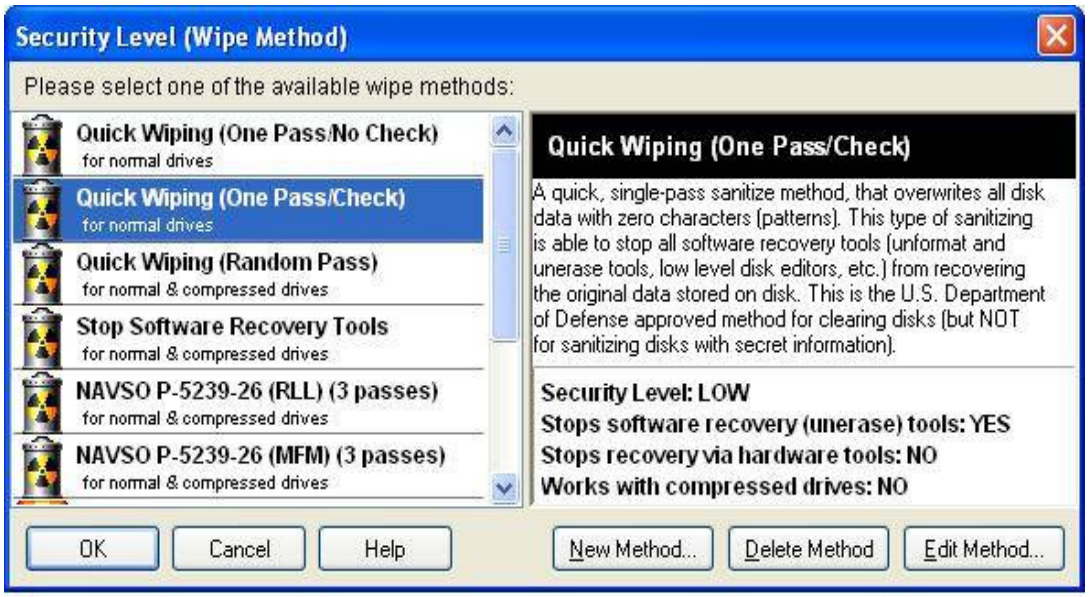
The following screenshots detail the configuration options selected:






Erase for Good
Erase for Good
Deleting a file using the Windows operating system does not remove the file contents from your hard drive. It simply prevents you from accessing the file. As a result, sensitive and private information can be easily recovered.
The Erase for Good feature ensures that previously deleted files are removed from your computer beyond forensic recovery.
Destroy all files from the Recycle Bin beyond recovery
Eliminate the deleted information on the following drives:
3½ Floppy (A:)
Local Disk (C:)
Removable Disk (D:)
Wipe Options
Wipe the free (unused) disk space
Wipe the slack of existing files (slower)
Scramble files and folders properties (name, date, size...)
By selecting the proper erase setting, you can prevent even the most advanced and sophisticated recovery methods from retrieving your data.
Erase Settings...
Help
Cancel
Start

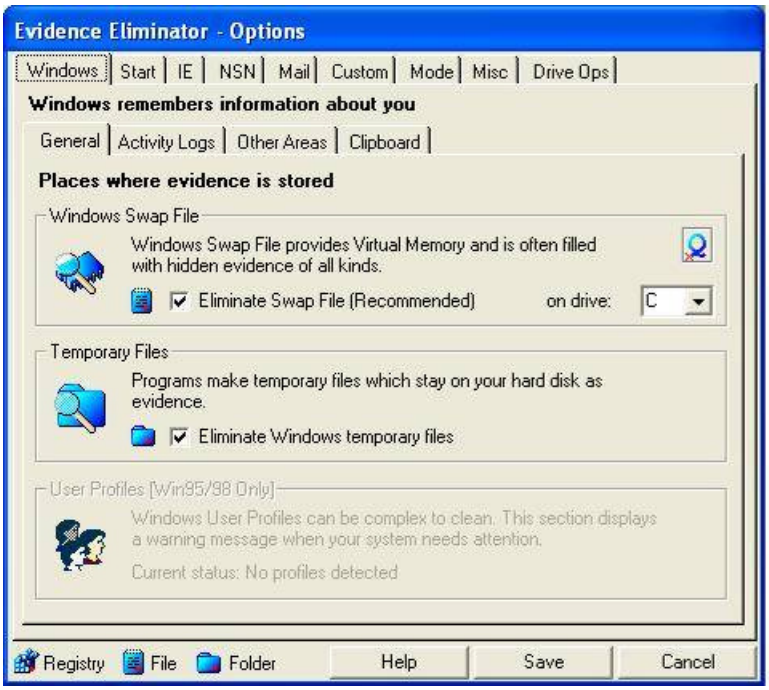

Erase Options
Actions
Confirmations
Preferences
Security Level
Wipe file using current wipe method
Wipe compressed files (on NTFS drives only)
Wipe Options
Wipe file slack
Delete Options
Use Recycle Bin
Scramble
Scramble files and folders properties (name, date, size...)
Scramble alternate data streams (on NTFS drives only)
OK
Cancel
Help

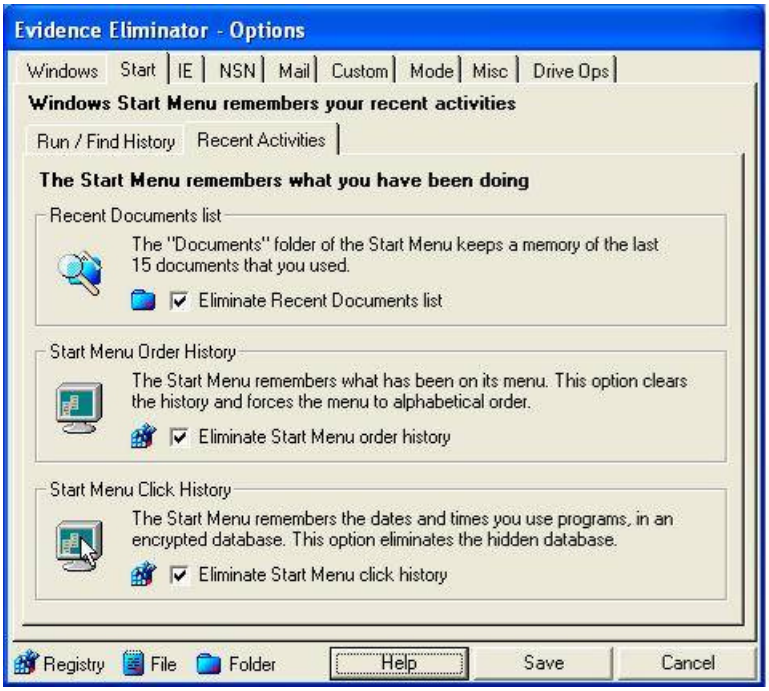

Security Level (Wipe Method)
Please select one of the available wipe methods:
Quick Wiping (One Pass/No Check)
for normal drives
Quick Wiping (One Pass/Check)
for normal drives
Quick Wiping (Random Pass)
for normal & compressed drives
Stop Software Recovery Tools
for normal & compressed drives
NAVSO P-5239-26 (RLL) (3 passes)
for normal & compressed drives
NAVSO P-5239-26 (MFM) (3 passes)
for normal & compressed drives
Quick Wiping (One Pass/Check)
A quick, single-pass sanitize method, that overwrites all disk data with zero characters (patterns). This type of sanitizing is able to stop all software recovery tools (unformat and unerase tools, low level disk editors, etc.) from recovering the original data stored on disk. This is the U.S. Department of Defense approved method for clearing disks (but NOT for sanitizing disks with secret information).
Security Level: LOW
Stops software recovery (unerase) tools: YES
Stops recovery via hardware tools: NO
Works with compressed drives: NO
OK
Cancel
Help
New Method...
Delete Method
Edit Method...

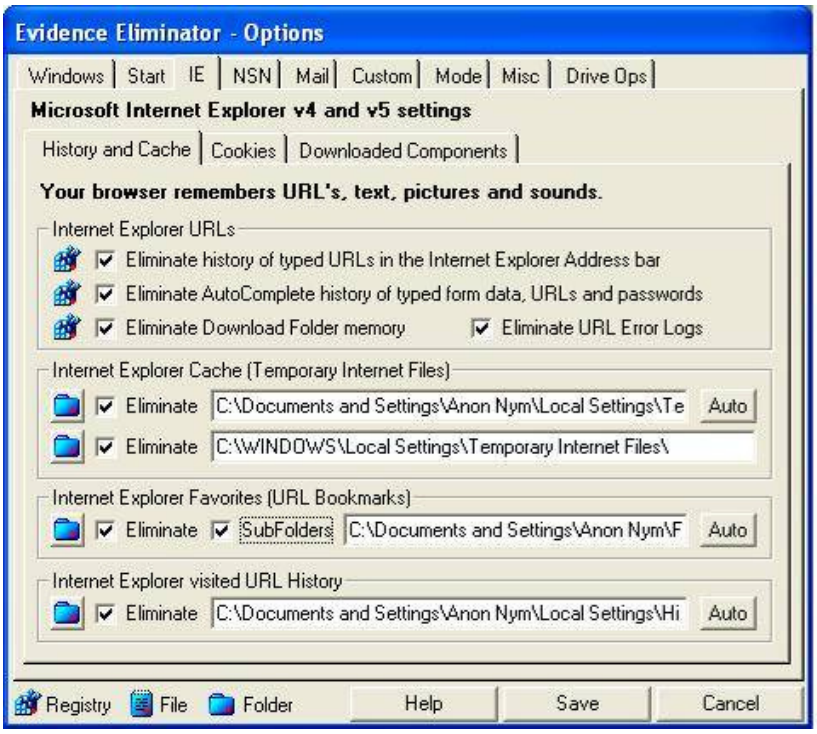
Evidence Eliminator configuration

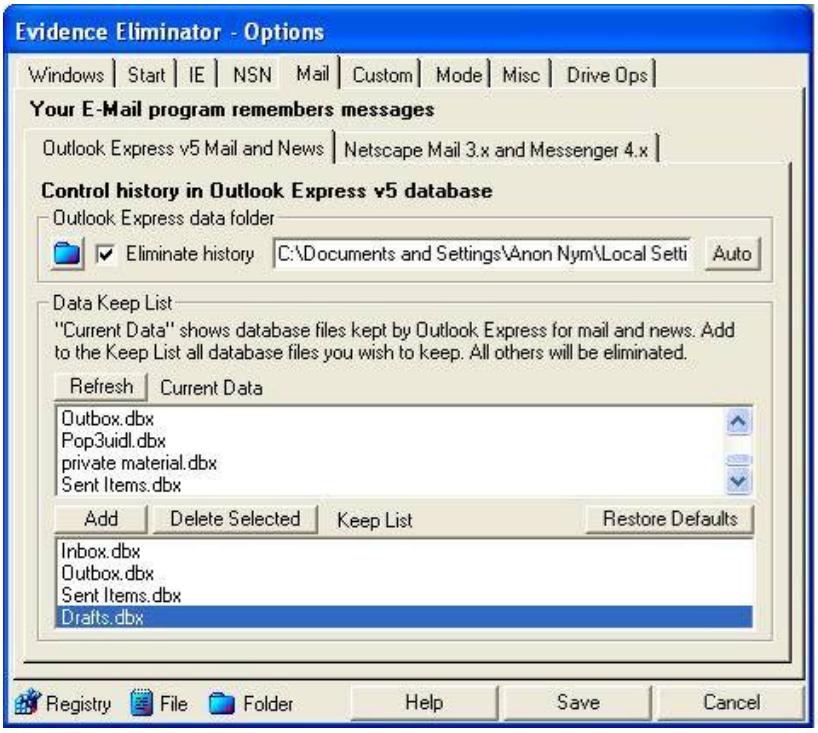
Evidence Eliminator configuration options were consistent with those for other privacy tools tested. Plug-ins for erasing information from a number of Microsoft and third-party applications were selected – Evidence Eliminator proceeds to the next step if a check for the associated files is negative.

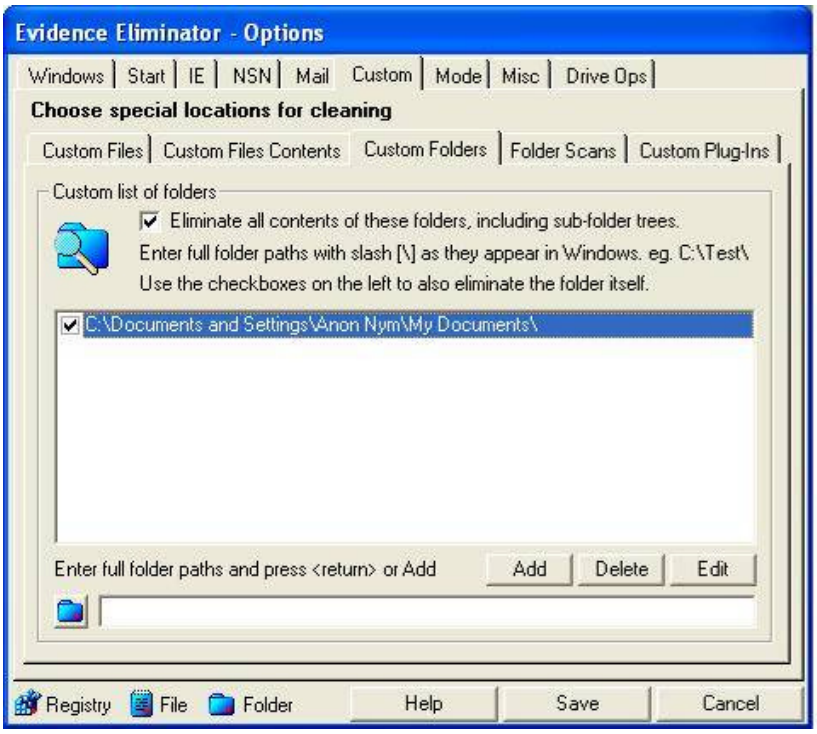
The following screenshots detail the configuration options selected:

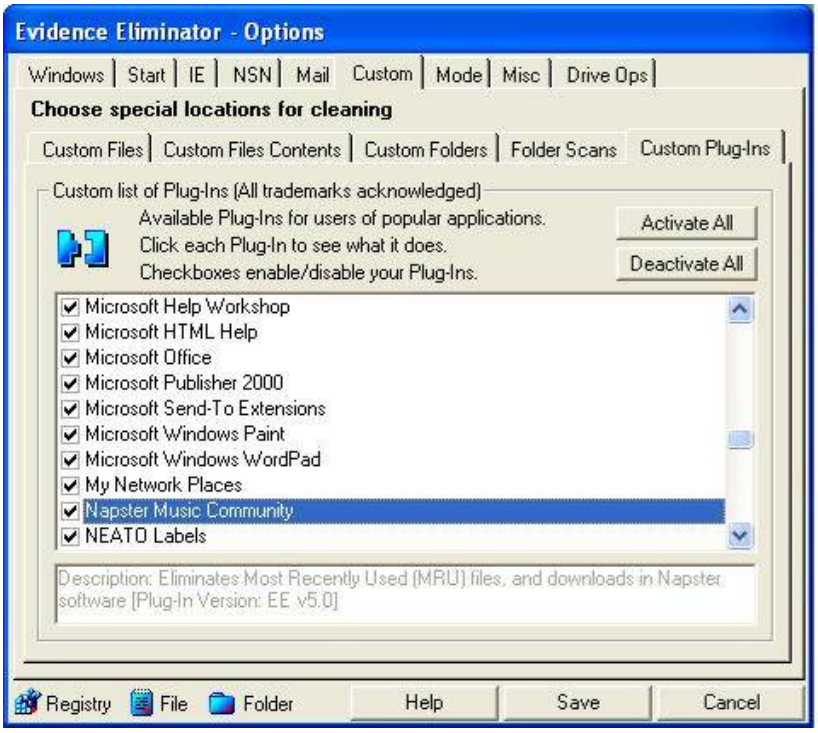


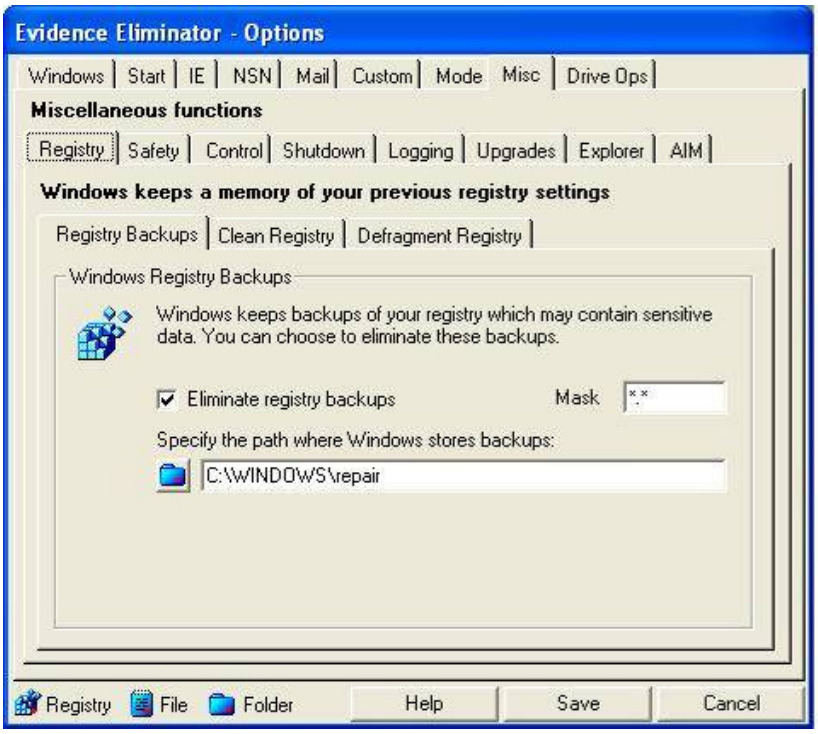



Evidence Eliminator - Options
Windows
Start
IE
NSN
Mail
Custom
Mode
Misc
Drive Ops
Microsoft Internet Explorer v4 and v5 settings
History and Cache
Cookies
Downloaded Components
Your browser remembers URL's, text, pictures and sounds.
Internet Explorer URLs
Eliminate history of typed URLs in the Internet Explorer Address bar
Eliminate AutoComplete history of typed form data, URLs and passwords
Eliminate Download Folder memory
Eliminate URL Error Logs
Internet Explorer Cache (Temporary Internet Files)
Eliminate
C:\Documents and Settings\Anon Nym\Local Settings\Te
Auto
Eliminate
C:\WINDOWS\Local Settings\Temporary Internet Files\
Internet Explorer Favorites (URL Bookmarks)
Eliminate
SubFolders
C:\Documents and Settings\Anon Nym\F
Auto
Internet Explorer visited URL History
Eliminate
C:\Documents and Settings\Anon Nym\Local Settings\Hi
Auto
Registry
File
Folder
Help
Save
Cancel


Evidence Eliminator - Options
Windows
Start
IE
NSN
Mail
Custom
Mode
Misc
Drive Ops
Your E-Mail program remembers messages
Outlook Express v5 Mail and News
Netscape Mail 3.x and Messenger 4.x
Control history in Outlook Express v5 database
Outlook Express data folder
Eliminate history
C:\Documents and Settings\Anon Nym\Local Setti
Auto
Data Keep List
"Current Data" shows database files kept by Outlook Express for mail and news. Add to the Keep List all database files you wish to keep. All others will be eliminated.
Refresh
Current Data
Outbox.dbx
Pop3uidl.dbx
private material.dbx
Sent Items.dbx
Add
Delete Selected
Keep List
Restore Defaults
Inbox.dbx
Outbox.dbx
Sent Items.dbx
Drafts.dbx
Registry
File
Folder
Help
Save
Cancel


Evidence Eliminator - Options
Windows
Start
IE
NSN
Mail
Custom
Mode
Misc
Drive Ops
Choose special locations for cleaning
Custom Files
Custom Files Contents
Custom Folders
Folder Scans
Custom Plug-Ins
Custom list of folders
Eliminate all contents of these folders, including sub-folder trees.
Enter full folder paths with slash [\] as they appear in Windows. eg. C:\Test\
Use the checkboxes on the left to also eliminate the folder itself.
C:\Documents and Settings\Anon Nym\My Documents\
Enter full folder paths and press <return> or Add
Add
Delete
Edit
Registry
File
Folder
Help
Save
Cancel

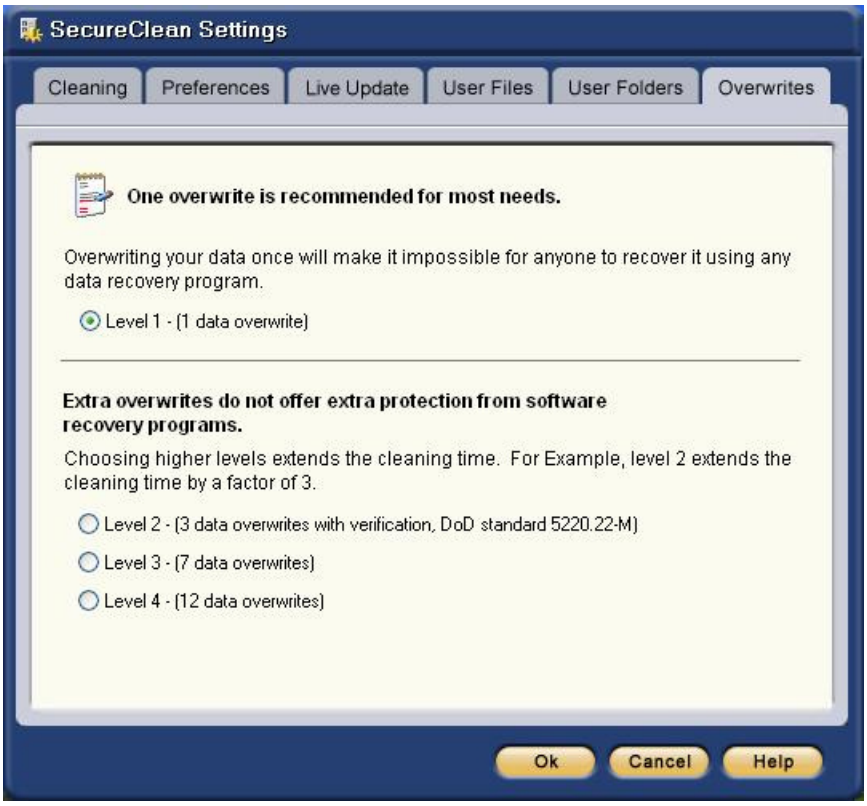

Evidence Eliminator - Options
Windows
Start
IE
NSN
Mail
Custom
Mode
Misc
Drive Ops
Choose special locations for cleaning
Custom Files
Custom Files Contents
Custom Folders
Folder Scans
Custom Plug-Ins
Custom list of Plug-Ins (All trademarks acknowledged)
Available Plug-Ins for users of popular applications.
Click each Plug-In to see what it does.
Checkboxes enable/disable your Plug-Ins.
Activate All
Deactivate All
Microsoft Help Workshop
Microsoft HTML Help
Microsoft Office
Microsoft Publisher 2000
Microsoft Send-To Extensions
Microsoft Windows Paint
Microsoft Windows WordPad
My Network Places
Napster Music Community
NEATO Labels
Description: Eliminates Most Recently Used (MRU) files, and downloads in Napster software [Plug-In Version: EE v5.0]
Registry
File
Folder
Help
Save
Cancel

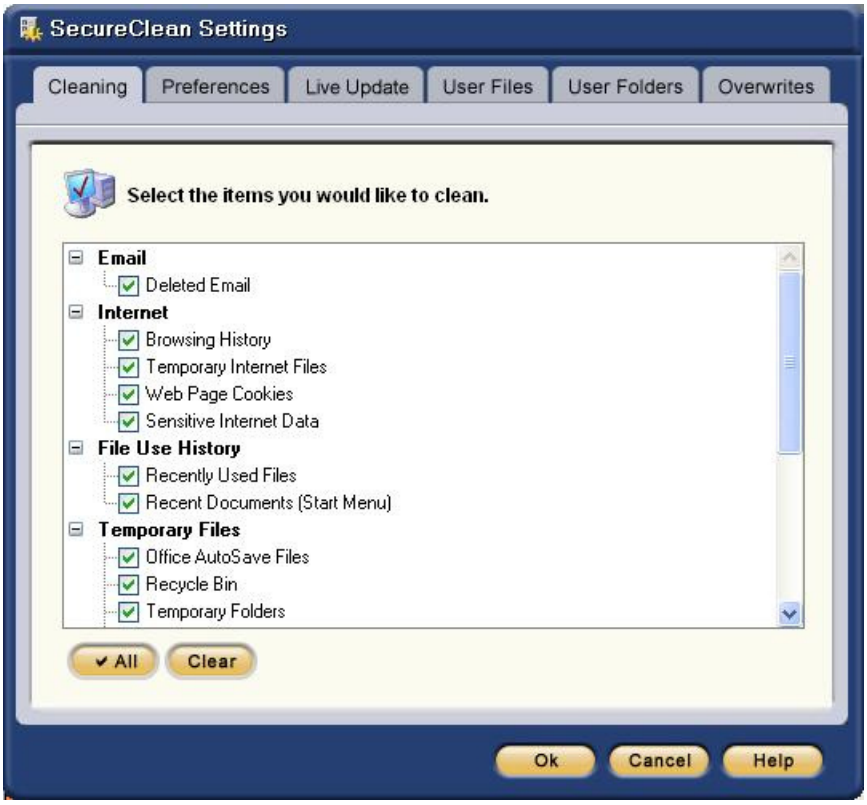

Evidence Eliminator - Options
Windows
Start
IE
NSN
Mail
Custom
Mode
Misc
Drive Ops
Miscellaneous functions
Registry
Safety
Control
Shutdown
Logging
Upgrades
Explorer
AIM
Windows keeps a memory of your previous registry settings
Registry Backups
Clean Registry
Defragment Registry
Windows Registry Backups
Windows keeps backups of your registry which may contain sensitive data. You can choose to eliminate these backups.
Eliminate registry backups
Mask
.
Specify the path where Windows stores backups:
C:\WINDOWS\repair
Registry
File
Folder
Help
Save
Cancel

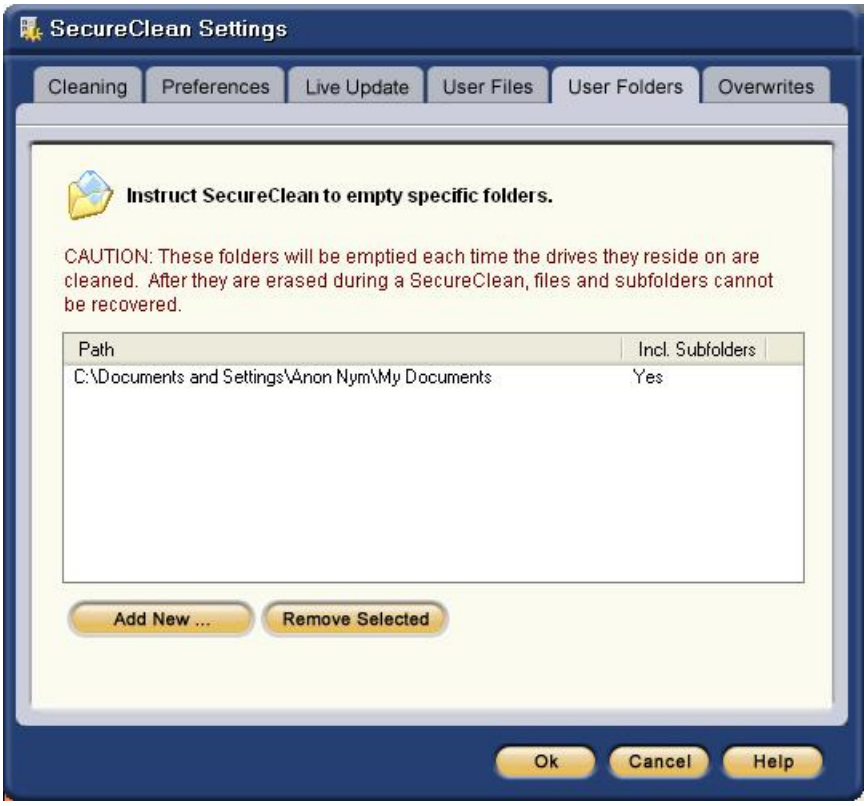
SecureClean configuration

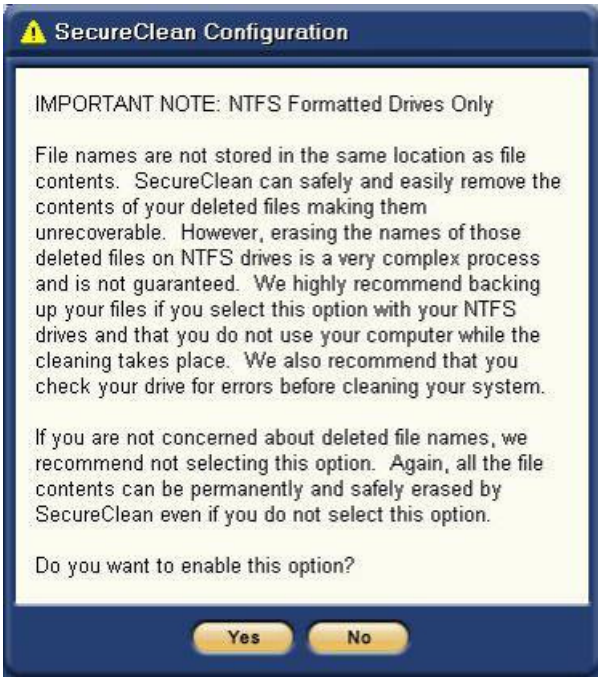
SecureClean's configuration was similar to that of the other privacy tools tested. The tool offers an initial scanning mode that looks for and identifies sensitive data it proposes to eliminate.

The following screenshots detail the configuration options selected:


SecureClean Settings
Cleaning
Preferences
Live Update
User Files
User Folders
Overwrites
One overwrite is recommended for most needs.
Overwriting your data once will make it impossible for anyone to recover it using any data recovery program.
Level 1 - (1 data overwrite)
Extra overwrites do not offer extra protection from software recovery programs.
Choosing higher levels extends the cleaning time. For Example, level 2 extends the cleaning time by a factor of 3.
Level 2 - (3 data overwrites with verification, DoD standard 5220.22-M)
Level 3 - (7 data overwrites)
Level 4 - (12 data overwrites)
Ok
Cancel
Help

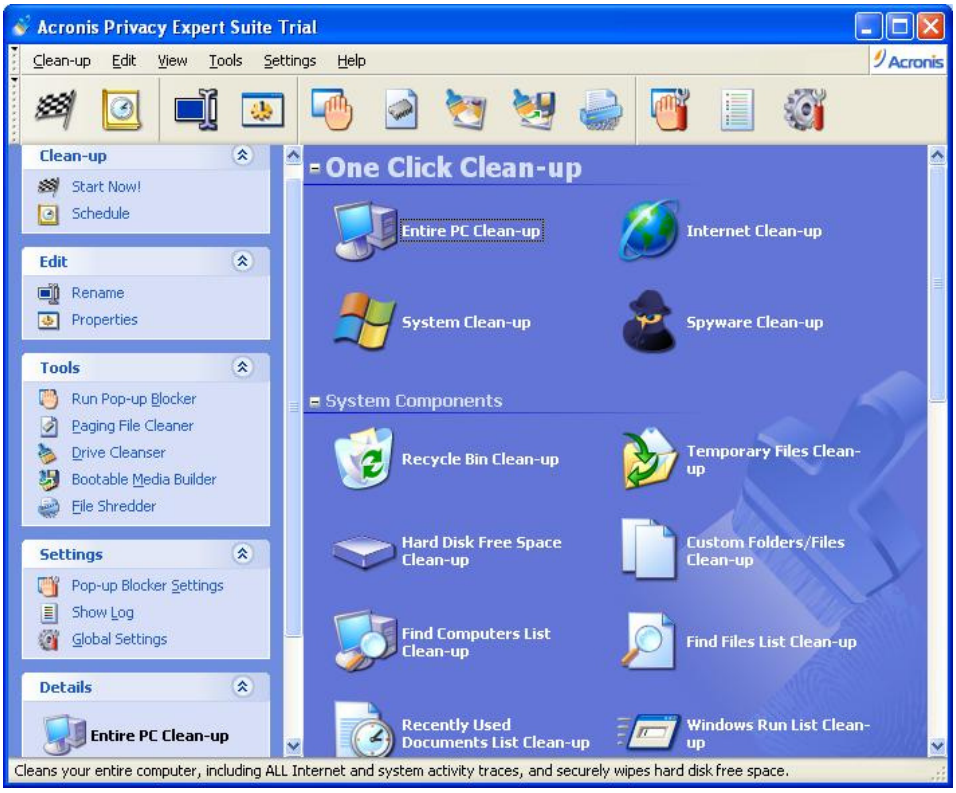

SecureClean Settings
Cleaning
Preferences
Live Update
User Files
User Folders
Overwrites
Select the items you would like to clean.
Email
Deleted Email
Internet
Browsing History
Temporary Internet Files
Web Page Cookies
Sensitive Internet Data
File Use History
Recently Used Files
Recent Documents (Start Menu)
Temporary Files
Office AutoSave Files
Recycle Bin
Temporary Folders
All
Clear
Ok
Cancel
Help


SecureClean Settings
Cleaning
Preferences
Live Update
User Files
User Folders
Overwrites
Instruct SecureClean to empty specific folders.
CAUTION: These folders will be emptied each time the drives they reside on are cleaned. After they are erased during a SecureClean, files and subfolders cannot be recovered.
Path
Incl. Subfolders
C:\Documents and Settings\Anon Nym\My Documents
Yes
Add New ...
Remove Selected
Ok
Cancel
Help

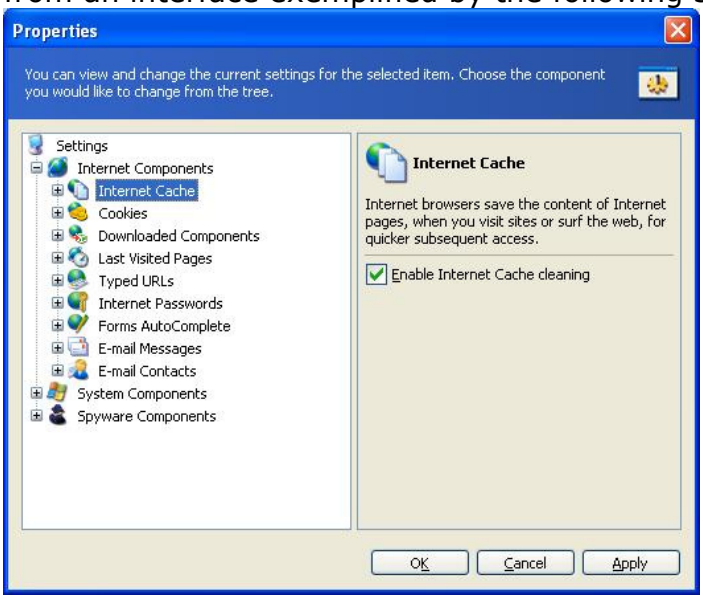

SecureClean Configuration
IMPORTANT NOTE: NTFS Formatted Drives Only
File names are not stored in the same location as file contents. SecureClean can safely and easily remove the contents of your deleted files making them unrecoverable. However, erasing the names of those deleted files on NTFS drives is a very complex process and is not guaranteed. We highly recommend backing up your files if you select this option with your NTFS drives and that you do not use your computer while the cleaning takes place. We also recommend that you check your drive for errors before cleaning your system.
If you are not concerned about deleted file names, we recommend not selecting this option. Again, all the file contents can be permanently and safely erased by SecureClean even if you do not select this option.
Do you want to enable this option?
Yes
No

Acronis Privacy Expert configuration

Privacy Expert offers a number of preset profiles for eliminating activity records, and even spyware. The most comprehensive is the "Entire PC Clean-up" mode highlighted in the following screenshot:



Configuration details and behaviour for these preset profiles can be refined from an interface exemplified by the following screen:



APPENDIX D – Consumer-oriented software reviews

The following are examples of the scope and style of privacy software reviews typically available to consumers on the Internet. They were selected purely as representative samples.

Window Washer

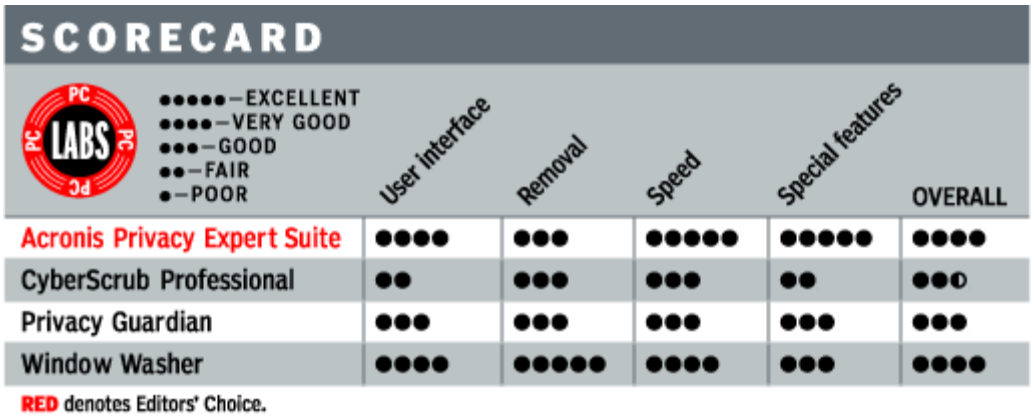
The following review by Download.com, a property of CNET Networks Inc., gives the tool a five-start rating:

This program offers a fast and simple way to protect your privacy by erasing Web browsing and application history. Upon launch, the program automatically scans your PC for supported applications, including such commonplace ones as Adobe Acrobat and RealPlayer. … Clicking the Wash Now button literally leaves your browser's cache, cookies, history, and temporary files list as clear as the day Windows was first installed. … In the final analysis, Webroot Window Washer has very few flaws, making it a fine pick for anyone concerned with privacy issues.
http://www.download.com/Webroot-Window-Washer/3000-2144_4-10289982.html

Privacy-software-review.com, a TopTenREVIEWS, Inc. property, gives the tool an overall 3.5 of four bars rating, and the site's "Silver Award":

Window Washer, from Webroot Software, is an excellent product. … The number of extra plugins dropped from 95 to 22, but many of these plugins are now standard within the product. A plugin is a small piece of interface software that allows your computer to erase information like the history of the last used files within desktop applications like browsers, email, instant messaging, chat, P2P, image viewers, graphical editors, etc.
Privacy Effectiveness: ■■■■
Although Window Washer doesn't have as many options as Evidence Eliminator, it still has all the major features that are required to effectively protect your computer.

PC Magazine published online a review of three of the tools we tested, along with a fourth we didn't, on June 8 2004. The magazine rated their performance in several areas, summarized by the scorecard below.



SCORECARD

●●●●●—EXCELLENT
●●●●—VERY GOOD
●●●—GOOD
●●—FAIR
●—POOR

	User interface	Removal	Speed	Special features	OVERALL
Acronis Privacy Expert Suite	●●●●	●●●	●●●●●	●●●●●	●●●●
CyberScrub Professional	●●	●●●	●●●	●●	●●●
Privacy Guardian	●●●	●●●	●●●	●●●	●●●
Window Washer	●●●●	●●●●●	●●●●	●●●	●●●●

RED denotes Editors' Choice.

The testing didn't include attempts to recover data or validate the wiping process for the programs. Instead, according to the article by Neil J. Rubenking, PC Magazine "set the products to overwrite the files they deleted with a single pass and measured how long the clean-up process took. For those that wipe free disk space, we timed that process separately." From the point of view of consumers concerned about privacy, this review, like the others cited, cannot substitute for rigorous testing of the tools. As demonstrated in the case of Window Washer, the speed of the clean-up process is probably not well correlated with the privacy protection that results.

An evaluation of CyberScrub Pro version 3.0 by Government Computer News in January 2004 also focused on the speed of the software's operation and a subsequent improvement in performance of the test computer.

BOX SCORE **A**

CyberScrub Professional Edition

DATA DELETION SOFTWARE

CyberScrub LLC; Alpharetta, Ga.; tel. 770-951-2080
www.cyberscrub.com
Price: $59.95; $49.95 download

+ Improves PC performance
+ Easy to use
+ Exceeds DOD standards

Real-life requirements:
Any Windows OS

The review employed CyberScrub's own file-scanning feature to validate how well it deleted targeted data and gave the software a "Box Score" of 'A'.

APPENDIX E – Directory and file listing for test system

Starting from the My Documents directory.

```
Folder PATH listing
Volume serial number is 71FAE346 68B0:7704
+---My Documents
|   |   Copy (10) of secret.txt
|   |   Copy (12) of secret.txt
|   |   Copy (26) of secret.txt
|   |   Copy of secret document.doc
|   |   Copy of secret.txt
|   |   I58608-2004Oct24L.txt
|   |   NapsterSetup.exe
|   |   Privacy Guru Interview.htm
|   |   Privacy Report.htm
|   |   secret document.doc
|   |   secret.txt
|   |   Wired 12_05 The Kingmaker.htm
|   |   World Domination Database.doc
|   |
|   +---My Music
|   +---My Pictures
|   |       24africa.large1
|   |       africa184.jpg
|   |       button_5sec.gif
|   |       comiconposter.jpg
|   |       crs_225.gif
|   |       crs_2466.jpg
|   |       crs_368.gif
|   |       dogbert3.jpg
|   |       dsl_bestvalue_girl.gif
|   |       fast.184.1.650
|   |       FF_120_mossberg1_f.jpg
|   |       FF_120_mossberg2_f.jpg
|   |       P1010004.jpg
|   |       P1010008.jpg
|   |       P1010009.jpg
|   |       soxparade-big.jpg
|   |
|   +---My Received Files
|   |       DNC Special Reports Making It Up As He Goes Along How Bush
Failed.txt
|   |       insteelm.exe
|   |       jello.ra
|   |       secret document.doc
|   |       wwsetup1_1769327000.exe
|   |
|   +---Privacy Report_files
|   |       aboutus_off_01.gif
|   |       baccounts_off_04.gif
|   |       back_to_top.gif
|   |       bg.gif
|   |       but_home.gif
|   |       ccards_off_02.gif
|   |       contactus_off_02.gif
|   |       Copy of secret document.doc
|   |       cptrust_off_01.gif
|   |       dlip_off_05.gif
|   |       fnewsletter_off_05.gif
```

```
|   |       fproduct_off_04.gif
|   |       header.gif
|   |       logo.gif
|   |       mdrops_off_03.gif
|   |       menu_starter.gif
|   |       order_off_03.gif
|   |       pixel(1).gif
|   |       pixel.gif
|   |       pledge_off_06.gif
|   |       psso_off_07.gif
|   |       sbodh_off_06.gif
|   |       secret document.doc
|   |       sitemap_off_08.gif
|   |       style.css
|   |       titles_off_07.gif
|   |       ttl_preport.gif
|   |
|   \---private
|       |   2002-epic-annual-report.pdf
|       |   Copy of secret document.doc
|       |   my program.doc
|       |   poker secrets.doc
|       |   World Domination Database.doc
|       |
|       \---super private
|               300x250_1.gif
|               binladen.1842
|               Copy of secret document.doc
|               my program.doc
|               Partial secrets.doc
|               secret
|
+---Other stuff
|       24africa.large1
|       24africa.large2
```