Identifying Trace Evidence from Target-Specific Data Wiping Application Software

Gregory H. Carlton
California State Polytechnic University
ghcarlton@csupomona.edu

Gary C. Kessler
Gary Kessler Associates
Embry-Riddle Aeronautical University
gck@garykessler.net

ABSTRACT

One area of particular concern for computer forensics examiners involves situations in which someone utilized software applications to destroy evidence. There are products available in the marketplace that are relatively inexpensive and advertised as being able to destroy targeted portions of data stored within a computer system. This study was undertaken to analyze a subset of these tools in order to identify trace evidence, if any, left behind on disk media after executing these applications. We evaluated five Windows 7 compatible software products whose advertised features include the ability for users to wipe targeted files, folders, or evidence of selected activities. We conducted a series of experiments that involved executing each application on systems with identical data, and we then analyzed the results and compared the before and after images for each application. We identified information for each application that is beneficial to forensics examiners when faced with similar situations. This paper describes our application selection process, our application evaluation methodology, and our findings, including the variability of the effects of these tools. Following this, we describe limitations of this study and suggest areas of additional research that will benefit the study of digital forensics.

1. INTRODUCTION

Arguably, one of the most difficult challenges facing computer forensics examiners concerns identifying evidence from digital data in situations where someone has deliberately attempted to destroy information. This challenge is compounded by conflicting perspectives, as individuals that hire computer forensics examiners seem to anticipate that professionals within this field are able to retrieve all relevant evidence, individuals that wipe data do so with the intent that their techniques are sufficiently elaborate enough to prevent information from being recovered, and forensic examiners may be driven by professional pride and the satisfaction of performing their craft well in order to uncover evidence wiped by sophisticated methods. These conflicting goals between those that attempt to

hide evidence and those that seek to submit recovered evidence within the legal system increase the levels of risk and uncertainty facing computer forensics examiners in situations where attempts to destroy data have occurred.

One area of particular concern for computer forensics examiners involves situations in which someone utilized software utilities or applications designed specifically to destroy evidence (R-Tools Technology, 2011). There are a number of products available in the marketplace that are easily available, relatively inexpensive, and advertised as being tools to destroy targeted portions of data stored within a computer system (Hughes, Coughlin, & Commins, 2009). This study was undertaken to identify these tools and analyze them. Our analysis goals focus on identifying trace evidence, if any, left behind on suspect disk media after executing these applications (O & O Software, GmbH, 2011). We found two examples of prior literature that addressed this topic; however, both of them are based on older versions of Windows operating systems. The earlier work evaluated "disk cleaners" on Windows 98 and Windows 2000 based systems (Jones & Meyler, 2004). More recently, a paper discussed "disk scrubbers" on Windows XP based systems, and Jones and Meyler (Geiger, 2006).

We evaluated five Windows 7 compatible software application products whose advertised features include the ability for users to wipe targeted files, folders, or evidence of selected activities (i.e., Internet history, registry keys, etc.) (KremlinEncrypt.com, 2008). Rather than select tools that simply wipe entire storage devices, we chose to evaluate tools that target portions of storage media, as the potential exists to recover data from partially wiped media, especially if the wiping application performed poorly or left trace evidence (Paragon Technologies GmbH, 2011).

After selecting five file wiping applications, we conducted a series of experiments that involved executing each application on systems with identical data. We then analyzed the results and compared the before and after images for each application. While the extent of wiping data differs among the applications, we identified information concerning each application that is beneficial to forensics examiners when faced with obtaining evidence from systems subjected to similar situations.

The following sections describe our application selection process, our application evaluation methodology, and our findings. Following this, we describe limitations of this study and suggest areas of additional research that will benefit the study of digital forensics.

2. APPLICATION SELECTION

The data wiping software products on the market can be divided into two broad categories: those that simply wipe an entire volume or device and those that allow users to target selected files, folders, or data related to certain activities (e.g., Internet history or server log files). The software utilities or applications we chose

to evaluate are those that allow users to wipe targeted files or folders within a specified volume or device, as this set of products provide the potential for suspects to intentionally attempt to conceal their activities while maintaining a useable system. Our objective was to identify trace evidence available on known systems in which the selected applications have been utilized.

In addition to the ability to select specific files or folders within a volume, we chose to focus on the Windows 7 operating system. Our justification for this is that Windows is the most widely used family of operating systems and, at the time of this study, Windows 7 is the most recent version available. Although large numbers of Windows XP and Windows Vista installations are currently in use, Windows 7 is likely to be more widely used as time moves forward.

Table 1 - Initial data wiping applications

Product	**File/Folder Target Wiping**	**Windows 7 Compatible**
Acronis Drive Cleanser	No	No
Active@KillDisk	Yes	Yes
Bodrag Wipe Expert 2	Yes	No
Darik's Boot and Nuke	No	No
Data Wiper Tool	Yes	No
Heidi Eraser	Yes	Yes
Evidence Eliminator	Yes	Yes
Evidence Smart	Yes	Yes
HDDerase	No	No
Iolo DriveScrubber	Yes	Yes
Jetico BCWipe	Yes	Yes
Kremlin Wipe	No	No
O&O Safe Erase	Yes	Yes
Paragon Disk Wiper Personal	No	Yes
R-Wipe & Clean	Yes	Yes
UltraSentry	Yes	Yes
Webroot Window Washer	Yes	Yes
Active@Eraser	Yes	Yes

Our selection process began in March, 2011, by selecting a team of senior, undergraduate Computer Information Systems students at California State Polytechnic University (Cal Poly Pomona) that had successfully completed coursework in Computer Forensics. After describing our objectives to the team of students, we asked them to perform research to identify the data wiping applications that met our criteria. The student team was instructed to use the Internet as a research tool to approximate the procedures we believed typical suspects were likely to follow to learn of these tools. As a result, the student team identified a set of eighteen applications, as listed in Table 1 (EvidenceSmart.com, 2011) (GEEP EDS LLC., 2011) .

We reviewed each of the products identified in Table 1 - Initial data wiping applications using criteria including purchase price, the availability of a fully-functional trial version, customizability, reporting capability, security standards, targeted file/folder wiping, registry wiping, device wiping, partition or volume wiping, graphical user interface (GUI), and logging capability(Acronis Inc, 2011) (Bodrag S.R.L., 2011). We then selected five products for comprehensive analysis from the list, with each of the products meeting our minimum requirements and collectively providing an extensive range of features. Additionally, the five selected data wiping tools ranged in purchase price from free to the most expensive product identified. The products selected for analysis are listed in Table 2 - Selected data wiping applications.

Table 2 - Selected data wiping applications

Product	**Version**	**Purchase Price**	**File/Folder Wiping**	**GUI**
Heidi Eraser	6.0.8	Free	Yes	Yes
Evidence Eliminator	6.0.3	$149.95	Yes	Yes
Jetico BCWipe	5.01.2	$39.95	Yes	Yes
Active@Eraser	4.1.0.5	$29.95	Yes	Yes
Webroot Window Washer	6.6.1.18	$29.95	Yes	Yes

We limited our evaluation to five applications, as we had determined that this was the maximum number of applications we could feasibly test extensively given our limited resources and time constraints. We also felt that this was an adequate number of applications to test, as this was intended as a demonstration of capability rather than an exhaustive study. Each of the selected applications utilized a GUI, as we reasoned that non-technical individuals were more likely to use them instead of command-line products. Finally, all selected applications

allowed targeted file and folder wiping, and they operated on the Windows 7 operating system. A summary of the features of each of these applications is described below:

2.1 Heidi Eraser

Eraser, distributed by Heidi Computers, Ltd., is a freely available data wiping application that is released under the GNU General Public License, including its source code (Heidi Computers, Ltd., 2010). This tool's features include the ability to remove selected files and folders, support for all Windows compatible drives, and use of a customized scheduler (Low, 2010). Additionally, the version of Eraser used in this study (v6.0.8) operates on Windows XP and all existing, subsequent versions of the Windows operating system.

2.2 Evidence Eliminator

Evidence Eliminator is a data wiping application that can, ostensibly, target a large array of files that can be wiped and hidden from forensics analysis. Among the specific items that can targeted for elimination in the test version are swap files, application logs, temporary files, the Recycle Bin, registry backups, Internet Explorer (IE) temporary typed Uniform Resource Locators (URLs), cache and history files, AutoComplete forms and passwords, cookies, and slack space (Robin Hood Software Ltd., 2011).

2.3 Jetico BCWipe

Jetico Inc's BCWipe, like the products above, can target user-specified files and directories, or classes of files such as Internet history, swap file, file slack space, Master File Table (MFT) records and directory entries (Jetco Inc., 2011). In addition, BCWipe can be installed as part of the Windows Explorer content-sensitive menus.

2.4 Active@ ERASER

Active Data Security Solutions' Active@ ERASER has similar features to the other test software, including the ability to reside within the Windows Explorer's menus. Active@ Eraser's features also include the ability to remove specified files and folders, as well as Internet and local activity history files created by several browsers (Active Data Security Solutions, 2011).

2.5 Webroot Window Washer

Webroot Software, Inc.'s Window Washer is a broad-featured application that claims to "wash" many types of files in order to enhance a user's privacy protection. In addition to erasing Internet activity (supporting a number of browsers), wiping files and free space, and "shredding" files and directories, Window Washer can also clean up files associated with a variety of applications, such as Microsoft Office, iTunes, Adobe Flash Player, and Adobe Acrobat (Webroot Software, Inc., 2011).

3. EVALUATION METHODOLOGY

After selecting the five wiping applications described in Section 2, we proceeded to design and conduct a series of experiments using each application. This section describes the methodology we used to prepare test data and conduct our experiments.

Our primary research objectives was to provide information useful for digital forensics examiners in identifying trace evidence left on suspect media after the execution of data wiping application software targeting selected data. To that end, we constructed a pre-experiment, personal computer system that would represent a consistent starting point prior to conducting our experiments. Using the pre-experiment data image as a starting point, we then performed a set of tasks for each selected data wiping software product. After performing the tasks, we compared the post-experiment data images to the pre-experiment data image. In the following sections, we describe our preparation of evaluation data, the experiments we conducted, and our analysis of the data after conducting the experiments.

Our secondary objective was to create a framework by which additional wiping applications could be tested and compared. Because new products are being introduced into this application space and the versions of existing products change frequently, we wanted to have a methodology that could be expanded to other, similar applications.

3.1 Preparation of evaluation data

Prior to conducting the experiments, we established an initial disk drive with which we could measure the changes caused by running each application. Our initial configuration consisted of a personal computer workstation in which we had installed a known set of data files. We installed each data wiping application onto a separate instance of the known initial configuration.

The workstation used for this study had a single Seagate Barracuda 7200 160 GB internal hard disk drive as the only storage medium. To ensure that no data contamination existed on the physical disk drive, we used EnCase Law Enforcement (v6.11.2.2) to wipe the drive prior to using it. We selected null characters (i.e., 0x00) to be written to every byte of the physical disk using the EnCase disk wiping procedure. We verified that the wiping procedure completed successfully in two ways. First, EnCase provided a dialog box that indicated that the wiping process completed successfully. Second, we performed a global regular expression (grep) search for any non-null character on the physical disk using EnCase, and found none. Subsequently, we created a single 25 GB NTFS bootable partition on the hard disk drive and installed the Windows 7 operating system.

After installing the operating system, we placed sample data onto the disk drive to provide a basis from which we could evaluate the thoroughness of the selected wiping tools. Our sample data consisted of 57 data files organized within nine folders, as listed in Table 3 - Evidence data files. Most of the data files were downloaded directly from the Internet, including all of the data files stored in the *Desktop*, *Desktop\images idea*, *Desktop\ images Italian food*, *Downloads*, *Downloads\Midi*, and *Downloads\pdf* folders. The data files stored in the *Pictures\2011-04020 Building98* folder consisted of still and video images taken with a Canon PowerShot SD960 camera, transferred directly from the camera's Secure Digital (SD) card using Windows Explorer and a Universal Serial Bus (USB) connection.

Within the *Pictures* folder, we created four PNG files by using the Print Screen key to take screen shots, pasting the screen shots into Paint application data files, and saving them as .png files. This operation also provided data for the Windows clipboard function whereby we were able to later measure the extent to which the data wiping tools destroyed this data.

We placed 13 data files within the *Desktop\Culinary Documents* folder consisting of Microsoft Word documents, Microsoft Excel spreadsheets, and Portable Document Format (PDF) files. All of these files were created on another workstation using MS Office 2007, and subsequently transferred onto the test system from a USB flash drive. Once these files were placed onto our test system, we performed some additional tasks on a subset of these files, as described below.

After the *Chips.docx* file was transferred onto our test system from the flash drive, we used Microsoft Windows Skydrive document editor to modify the file. We added one sentence consisting of "I love Hot Cheetos with Limon!" as the first sentence after the heading at the beginning of the document, and we then downloaded the modified version of the file back onto the test system replacing the original version of the file.

Similarly, after we transferred the *peanut butter.docx* file onto our test system from the flash drive, we again used Microsoft Windows Skydrive document editor to modify the file by deleting the last paragraph from the document. After this deletion, we downloaded the modified version of the file back onto the test system replacing the original version of the file.

We performed a similar modification using a different editing tool to modify the *Brownies.xls* spreadsheet after we transferred the file onto our test system from the flash drive. For this file, we used Google Docs spreadsheet editor to add the text "Red Velvet Cake" into the cell in column C, row 9. After adding the text, we downloaded the modified file back onto the test system replacing the original version of the file.

The last file we modified within this folder was the *Cheesecake.xls* spreadsheet. Again, we used Google Docs spreadsheet editor to modify the file after we had

transferred it onto our test system. Our modification of this file consisted of deleting the contents of the cell located at column B, row 3 and three cells from the F column of the spreadsheet, namely rows 3, 4, and 6. After modifying this file, we downloaded it back onto our test system replacing the original version of the file.

The modifications made to the four documents described above provide us with a sample of files that were originally placed within the folder and subsequently modified by one of two different editing tools. This provides us with samples from Microsoft Word documents in versions 2003 and 2007, and Microsoft Excel spreadsheets. Also, both the Word documents and the Excel spreadsheets include one file with additions and one file with deletions. Text from the additions and deletions are included in keyword searches we performed during our analysis of the post-test data described section 3.3 of this paper.

Table 3 - Evidence data files

Logical path and file name	Physical locaton
C:\Users\Forensics Prof\Desktop\Culinary Documents\	
Tiramasu.xlsx	6993864-6993895
Chips.docx	22163504-22163535
Grape Jelly.docx	22163536-22163567
peanut butter.docx	6104032-6104055
Bread.pdf	28562392-28562439
Chips.pdf	21451968-21452023
Grape Jelly.pdf	21418712-21418767
Peanut butter.pdf	21452024-21452063
Brownies.xls	21418768-21418799
Cheesecake.xls	21418856-21418879
Cookies.xls	22044688-22044759
Tirmasu.xls	22045928-22046215
Bread.docx	28562440-28562471
C:\Users\Forensics Prof\Desktop\images idea\	
Light-Bulb-Idea-Hand.jpg	28399184-28399223
gatsby-idea!.jpg	9523776-9523847
light_bulb.png	229728-229759
idea.jpg	20154632-20154743
C:\Users\Forensics Prof\Desktop\images italian food\	
italian-food.jpg	6979096-6979207
italian_food2.jpg	6978368-6978511
italian_food_recession.jpg	4622608-4622903
italian-food-cuisine-pizza.jpg	20864888-20864983
italian-food2.jpg	20718728-20718879
C:\Users\Forensics Prof\Desktop\	
bbsps.jpg	27122824-27122983
Firefox Setup 4.0.exe	20426720-20451295
HazcomManual.doc	26836808-26839999
Loto.doc	20146400-20147343
Rubric2009.doc	6941616-6941815
wrar400.exe	20778592-20781423

Logical path and file name	Physical locaton
C:\Users\Forensics Prof\Downloads\Midi	
Another_One_Bites_the_Dust.mid	5158080-5158119
Crawling.mid	5158120-5158191
ISawHerStandingThere.mid	26783320-26783383
C:\Users\Forensics Prof\Downloads\pdf	
Ds_Tetris_Ds.pdf	20714712-20717727
lindamanual.pdf	20782480-20782543
mcm996.pdf	20865208-20865271
C:\Users\Forensics Prof\Downloads	
eraser-demo.exe	18428288-18432615
mseinstall.exe	19929976-19930943
winzip150.exe	2919888-2920199
yahoomailuploader.exe	28047064-28047127
C:\Users\Forensics Prof\Pictures\	
Search chickenpasta.png	20853416-20853695
Search applepie images.png	26650944-26653655
Download idea images.png	28389000-28391175
Download italian food images.png	20865640-20865783
C:\Users\Forensics Prof\Pictures\2011-04-20 Building98\	
Building98 001.MOV	21423544-21423551
Building98 001.THM	28046392-28046399
Building98 002.MOV	21423592-21423599
Building98 002.THM	21447272-21447287
Building98 003.MOV	6942120-6942127
Building98 003.THM	21986256-21986279
Building98 004.JPG	28578376-28578415
Building98 005.JPG	22337800-22338055
Building98 006.JPG	28583240-28584263
Building98 007.JPG	21556472-21557807
Building98 008.JPG	22187512-22194799
Building98 009.JPG	22216120-22223215
Building98 010.JPG	22227384-22231183
Building98 011.JPG	22235320-22239343
Building98 012.JPG	22250808-22255855

Overall, the sample user data we generated consisted of 57 data files including Microsoft Word documents, Microsoft Excel spreadsheets, PDF files, executable program files, and multimedia files representing audio, video, and picture content. We also included Internet activity, consisting of searches, download history, browsing data, and activity from three web-based e-mail applications. To provide additional variety with Internet activity files, we installed Mozilla Firefox in addition to Microsoft Internet Explorer. Additionally, to represent the actions a typical user would perform to delete files, we deliberately deleted files using the Windows 7 GUI to ensure that entries were created in the Windows Recycle Bin folder. A listing of the data file names is provided in Table 3 - Evidence data files.

Once we completed the installation of the sample user data on the computer workstation, we performed a static data acquisition of the physical device; with the computer workstation powered off, we removed the Seagate Barracuda hard disk drive, attached it to a Tableau Model T5 write blocking device *via* an IDE ribbon cable, and connected the write blocking device to our Mac Pro forensic workstation using a FireWire 800 connection. We used EnCase running under Windows XP Professional in native mode on a Mac Pro using BootCamp to perform the data acquisition from the physical device of the Seagate Barracuda hard disk. We saved the image in an E01 file, and we validated the integrity of the data acquisition with Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) hash values.

We analyzed the image created from this static data acquisition and identified the physical sector location of each data file we had stored (Table 3 - Evidence data files) and used this image as the starting point from which we installed each of the data wiping products. After installing each data wiping application, we acquired another image of the physical device. This resulted in six forensic images, one without any wiping application installed and five consisting of the data contained on the initial image plus one data wiping application; these latter five images served as pre-experiment images from which we compared in the post-wipe analysis.

3.2 Data wiping application tasks

After preparing data images for evaluation, we performed various data wiping tasks on each pre-experiment image. The tasks targeted specific items on the volume and are described below:

3.2.1 Active@ Eraser

Upon launching the Active@ Eraser application, we used its GUI to locate and select each of the files within their respective paths listed in Table 3 - Evidence data files. We then expanded the Internet & Local Activities option and selected each of the following items:

- My Internet Auto-Complete (Forms & Passwords)
- My Internet Cookies
- My Internet History
- My Internet Temporary Files
- My Recently Used List
- My Recycle Bin
- My Run History
- My Temporary Files

Once all of the files and Internet and local activities had been selected, we clicked the "Erase" button and employed the "One Pass Zeros (quick, low security)" option. We unselected the "Verify" option and kept the default option to "Ignore Errors" (Figure 1 - Screenshot of Active@ ERASER).

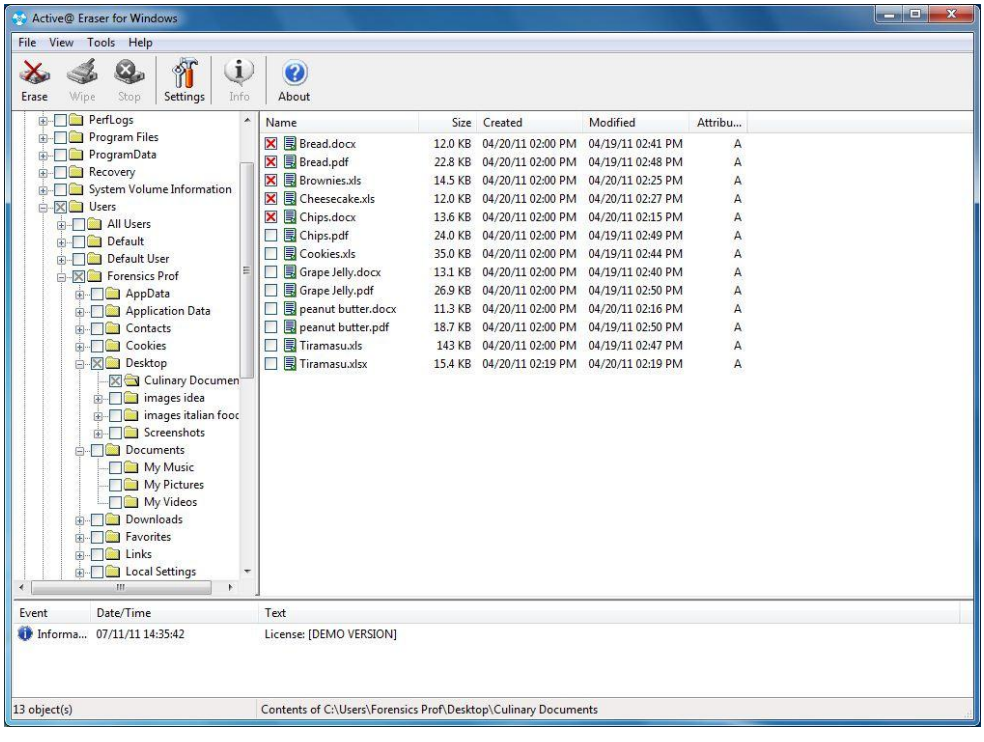

Figure 1 - Screenshot of Active@ ERASER

After the process completed successfully, we exited the application and shut down the personal computer workstation using the standard Windows 7 shutdown function. We then extracted the hard disk drive and acquired a forensic image of the entire physical device.

3.2.2 Window Washer

Upon launching the Window Washer application, we clicked on the "Wash Setup" option and selected the "Custom Wash Items" choice. Within the "Custom Wash Items" selection, we selected the individual file names and folders indicated in Table 3 - Evidence data files, and we chose the option to add all of the files in the preselected file paths. The program indicated that a total of 58 files were selected for washing.

We chose to accept all of the default options for the other settings. The Internet items that are selected by default for Internet Explorer are: address bar history, cookies, temporary Internet files folder (i.e., cache), history (i.e., visited sites), Index.dat, and Auto-Complete form data. The default setting for the Index.dat file includes the non-technical user description, "wash with bleach on Windows startup."

Similarly, the Internet items that are selected by default for Mozilla Firefox are Internet cache, cookies, and URL history. Also included by default are Windows start menu and desktop items, including the Recycle Bin, document history, Run history, and "find and search history." Additional Windows system items included by default include the Windows temp folder and the system temp folder. Other items selected by default include recent activity (i.e., Most Recently Used, or MRU) for disk error checking and media player recent file list.

After making the selections indicated above, we selected the "Home" button and clicked on the button to "Wash My Computer Now." After the application completed its tasks, we selected the "Finish" option, exited the application program, and performed the Windows shutdown process. As above, we then made a forensic image of the disk drive.

3.2.3 Jetico BCWipe

The BCWipe application was a bit more straight-forward than the two previous applications; we merely selected the files to be wiped and selected the option to "delete with wiping." After the operation completed successfully, we exited the BCWipe application, and performed the Windows shutdown procedure.

As with the other applications, after the personal computer workstation was powered off, we imaged the hard drive.

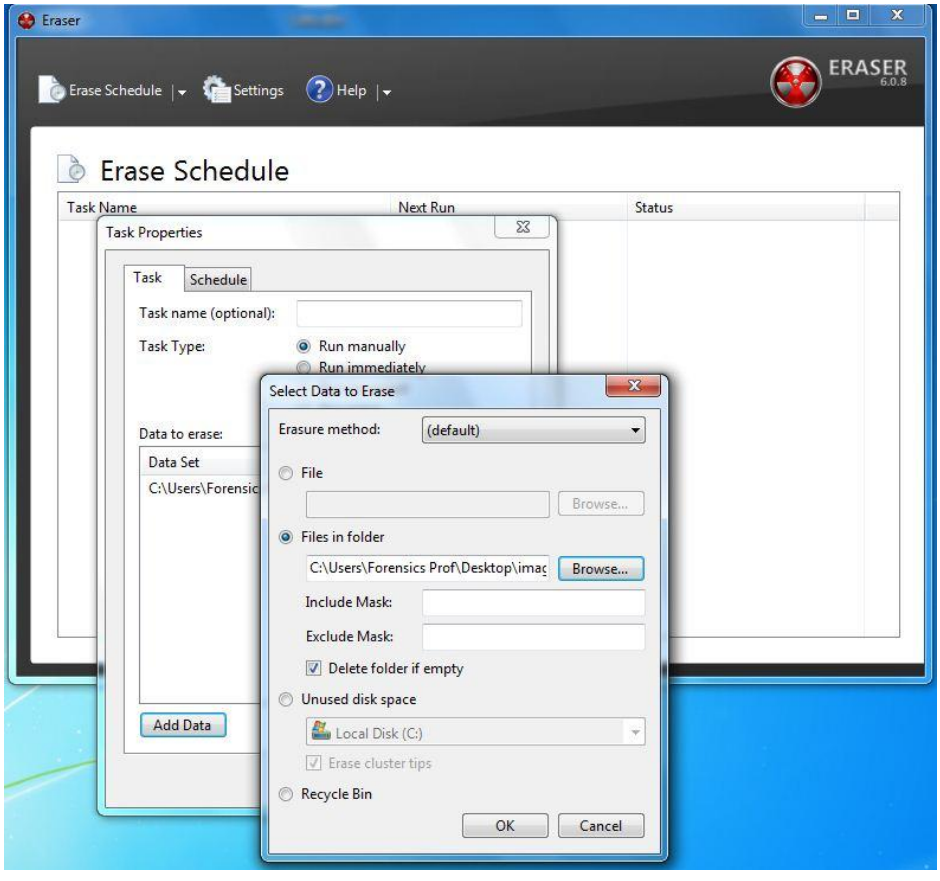

Figure 2 - Screenshot of Heidi Eraser

3.2.4 Heidi Eraser

Eraser's wipe function is largely controlled via the "Erase Schedule" function; files to be wiped are selected using the "Add Data" option and "Data to erase" list (Figure 2 - Screenshot of Heidi Eraser). We verified that the process ran to completion, exited the Eraser application, shut down the computer, and made a forensic image of the hard drive.

3.2.5 Evidence Eliminator

Evidence Eliminator required a fair amount of configuration. From the Windows tab, we selected the "Eliminate Swap File" option, and under the Activity Logs sub-tab, we selected the options to eliminate Registry Streams (e.g., MRU) and Windows application logs. Next, we ensured that all of the options were unchecked under the sub-tab for "Other Areas" and then selected the option to

eliminate all contents of clipboard memory (Figure 3 - Screenshot of Evidence Eliminator).

Our next step was to check all three items under the Start tab, namely "Eliminate 'Run' history," "Eliminate 'Find Computer' history," and "Eliminate 'Find Files' history." Similarly, under the Recent Activities tab, we selected the options to eliminate the recent documents list, start menu order history, and start menu click history.

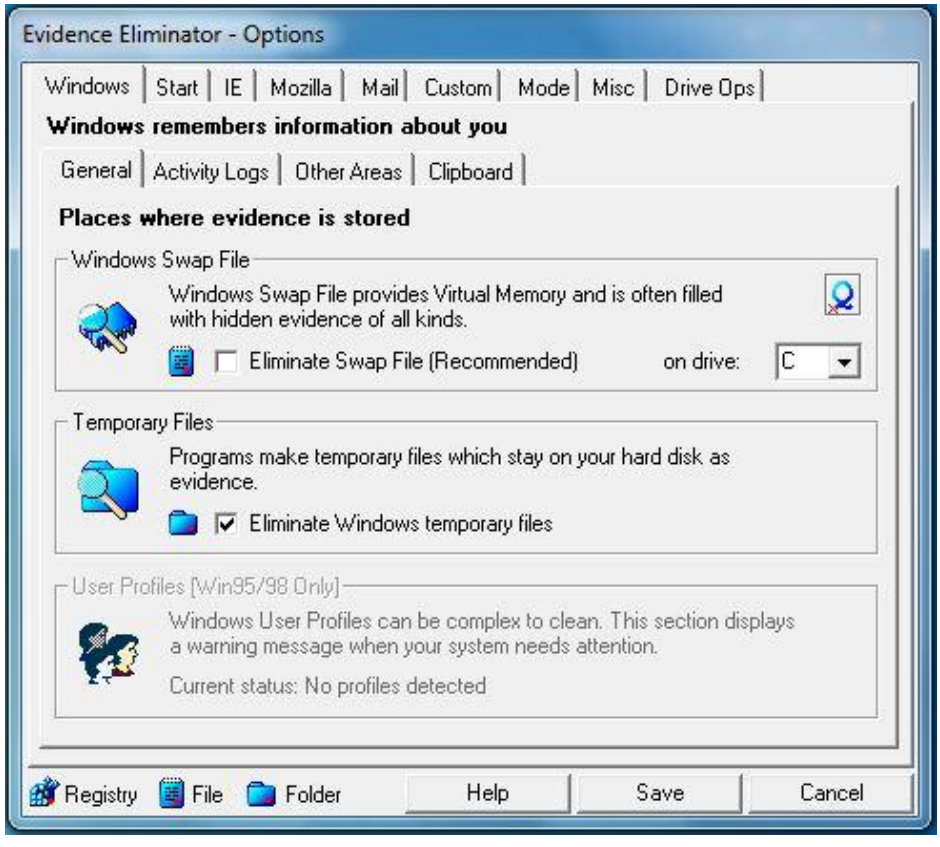

Figure 3 - Screenshot of Evidence Eliminator

Evidence Eliminator provided tabs for Internet Explorer and Mozilla Firefox, and we selected options under each of these categories to remove their respective components, as indicated below.

To remove evidence concerning Internet Explorer, under the IE tab, we checked the options to eliminate:

- History of typed URLs in the Internet Explorer address bar
- Auto-Complete history of typed form data, URLs and passwords
- Download folder memory
- Error logs
- C:\users\forensics prof\AppData\Local\Microsoft\Windows\Temporary Internet Files\
- C:\Windows\Local Settings\Temporary Internet Files\
- Internet Explorer Favorites (URL Bookmarks)
- C:\Users\Forensics Prof\Favorites\
- C:\Users\Forensics Prof\AppData\Local\Microsoft\Windows\History\

Under the Cookies sub-tab, we selected the option to eliminate cookies in the C:\Users\Forensics Prof\AppData\Roaming\Microsoft\Windows\Cookies\ folder. From the Downloaded Components sub-tab, we selected the option to eliminate components in the C:\Windows\Downloaded Program Files\ folder.

From the Mozilla tab, we selected the following items to wipe:

- Cache Folder: C:\Users\Forensics Prof\AppData\Local\Mozilla\Firefox\Profiles\dkvfbgyw.default\Cache
- Offline Cache: C:\Users\Forensics Prof\AppData\Local\Mozilla\Firefox\Profiles\dkvfbgyw.default\OfflineCache
- History: C:\Users\Forensics Prof\AppData\Roaming\Mozilla\Firefox\Profiles\dkvfbgyw.default\places.sqlite
- URL memories in JavaScript prefs file C:\Users\Forensics Prof\AppData\Roaming\Mozilla\Firefox\Profiles\dkvfbgyw.default\

Under the Cookies sub-tab for Mozilla, we selected the option to eliminate Cookies in C:\Users\Forensics Prof\AppData\Roaming\Mozilla\Firefox\Profiles\dkvfbgyw.default\cookies.sqlite. From the "More Options" sub-tab, we selected the option to eliminate the following three items:

- Downloads: C:\Users\Forensics Prof\AppData\Roaming\Mozilla\Firefox\Profiles\dkvfbgyw.default\downloads.sqlite
- Form History: formhistory.sqlite
- Session Store sessionstore.js

We then selected the option to eliminate the folder containing Stored Backups for Mozilla Bookmarks, "Bookmarkbackups."

We accepted the default settings under the "Mail" tab, and under the "Custom Files" sub-tab of the "Custom" tab, added the files indicated in Table 3 - Evidence data files, and selected the option to eliminate all files included in the list. Also, from the "Custom" tab, we selected the option to eliminate all contents of these folders, including sub-folder trees.

We selected the recommended option for maximum speed under the Windows sub-tab of the Mode tab, and we selected the option for extra security to rename and zero sizes when wiping files. We accepted all of the other default settings, and we then saved our selected options. Lastly, from the Evidence Eliminator main window, we selected the "Safe Shutdown" to remove the data and exit the application.

As with the other scenarios, we verified that the process ran to completion, exited the application, shut down the computer, and imaged the hard drive.

3.3 Post-wipe analysis

After completing the experiments for each data wiping application, we compared each post-experiment image against its corresponding pre-experiment image using a commercially available, validated digital forensics tools, including Guidance Software's EnCase Law Enforcement (v 6.11.2.2) and AccessData's FTK (v1.81). As we compared each pair of images, we focused on identifying any persistent markers or trace evidence produced by the wiping process; if present, these traces have the potential to yield valuable information to a digital forensics examiner concerning the activities that have occurred on the computer system.

Our procedures to analyze the results of the data wiping experiments involved seven steps:

1. We located the physical sector of each evidence file in the pre-experiment image, as shown in Table 3 - Evidence data files. For each post-experiment image, we used EnCase to navigate to the physical sector locations of the selected files to determine the data contents at the locations.

2. We generated a list of 99 keywords that were included in the evidence files and performed a search on the pre-experiment image of these keywords and on each of the post-experiment images.
3. Based on the pre-experiment image, we created a hash set that included the MD5 hash values for all 57 evidence files. Using EnCase, we performed a hash analysis on each of the post-experiment images.
4. Using the pre-experiment image, we performed a search for Internet history by using the EnCase search function. Similarly, we performed the same search on each of the post-experiment images.
5. Using the pre-experiment image, we used EnCase to show all of the contents of the device and sorted the contents by file creation date. We then performed the same analysis function on each of the post-experiment images. The primary purpose for looking at file creation date is to identify any items created by the data wiping applications, such as placeholder files.
6. We used AccessData's Registry Viewer (v1.5.4.44) to analyze registry keys contained within the pre-experiment image and each of the post-experiment images. Alghafli, Jones, and Martin (2010) provided additional reassurance that our registry analysis should focus on eight different registry folders within the NTUSER.DAT file.
7. We used Regshot (v1.8.2) to analyze changes to the Windows Registry (Geeknet, Inc., 2009). We used Regshot to take a snapshot of the pre-experiment image and each of the post-experiment images, and compared the differences between the different post-experiment for each data wiping application.

4. FINDINGS

4.1 Physical sector analysis

Our first step in analyzing each of the data wiping applications was to examine the physical locations of each of the files listed in Table 3 - Evidence data files on the post-experiment images to determine if any remnants existed. Four of the five applications we tested successfully wiped the selected files. Window Washer deleted the files, but failed to wipe them from the physical location on the disk drive.

4.2 Keyword search analysis

We performed a keyword search analysis with EnCase using the 99 keywords described in section 3.3. The raw numbers of keyword search hits for each data wiping application are provided in Table 4 - Keyword search analysis. Based on

the keyword search results, Evidence Eliminator was the most thorough at removing instances of the keywords from the disk image while Window Washer allowed the largest number of keywords to remain on the disk image. The majority of items located through the keyword search were from Microsoft Word (.doc) and Excel (.xls) files found in unallocated clusters within the NTFS volume of the post-experiment images. Other instances of the keywords were found in the pagefile and system volume.

Table 4 - Keyword search analysis

Data Wiping Application	**Total Number of Keyword Search Hits**
Active@ ERASER	34,768
Heidi Eraser	36,031
Evidence Eliminator	26.748
Jetico BCWipe	36,557
Webroot Window Washer	39,635

4.3 MD5 hash analysis

We performed an MD5 hash analysis using the hash set of the files identified in Table 3 - Evidence data files; a summary of the results is presented in Table 5 - MD5 hash analysis. Again, Window Washer only deleted the files rather than wiping them; therefore, the hash analysis uncovered all of the evidence files. Discounting the results from Window Washer, we found two patterns from our review of the MD5 hash analysis results that we considered noteworthy. With the exception of the single match from Evidence Eliminator, all of the matches from the MD5 hash analysis were images, and the majority of those images were downloaded through Mozilla Firefox.

Table 5 - MD5 hash analysis

Data Wiping Application	**Total Number of MD5 Hash Value Hits**
Active@ ERASER	12 matches found, all from Mozilla Firefox
Heidi Eraser	11 matches found, most from Mozilla Firefox
Evidence Eliminator	1 match found
Jetico BCWipe	11 matches found, most from Mozilla Firefox
Webroot Window Washer	100% matches found

4.4 Internet search analysis

We used the comprehensive search function of EnCase to analyze the Internet history of the post-experiment images for each of the data wiping applications. We found that each tool produced different results and none of them completely removed all evidence of Internet activity. We examined the contents of the Internet history folders associated with Internet Explorer and Firefox using EnCase to determine whether there was any indication of Internet activity in the post-wipe images.

Table 6 - Internet search evidence comparison

Browser	Prior to Wiping	Active@ ERASER	Webroot Window Washer	Jetico BCWipe	Heidi Eraser	Evidence Eliminator
Internet Explorer:						
Completely Erased	N/A	No	No	No	No	No
Bookmarks	78	90	89	101	97	39
Typed URLs	11	12	0	11	11	0
Daily	340	356	360	455	605	188
Weekly	N/A	241	241	134	134	134
Visited Link	633	799	868	820	1031	314
Cache Total	5915	6515	6438	7904	7540	4755
Code	1499	1494	1859	2154	2118	653
Image	3188	3170	3836	4614	4546	1393
HTML	258	256	320	374	368	119
XML	28	28	32	37	35	11
Text	36	35	48	49	48	15
Cookies After	522	223	672	633	633	113
Mozilla Firefox:						
Completely Erased	N/A	No	No	No	No	Yes
Cache Total	1735	1735	61	1751	1749	0
Code	312	312	11	314	313	0
Image	848	848	30	856	862	0
HTML	241	241	6	243	244	0
XML	17	17	0	17	17	0
Text	21	21	0	21	21	0

We found that that some files and folders were wiped while others were only deleted from the Master File Table and labeled as unallocated clusters; however, the contents were still detected by EnCase. Table 6 - Internet search evidence comparison provides a tabular comparison of the five wiping applications organized by Internet activity attributes for the two browsers. The values shown in the table indicate the number of records detected in the corresponding folder for each browser prior to installing a wiping tool and after using an installed wiping tool. Notice that the prior-to-wiping values for some measurements, such as Internet Explorer's Bookmarks, are smaller than the after-wiping values for several wiping tools. This is a result of the technique we used to install each of the wiping tools. The prior-to-wiping measure is based on an image of the data prior to installing a wiping tool. After this image was created, using restored copies of the image, we accessed the Internet and used a browser to locate and download the installation file for each wiping tool. This technique added data to the disk that was not on the prior-to-wiping image.

4.4.1 Analysis of the Internet Explorer browser

Two of the wiping applications, Window Washer and Evidence Eliminator, completely removed all entries from the "Typed URL" folder; however, all of the applications left other relevant data, including the cache, visited history, and cookies.

BCWipe removed the fewest number of records from the cache, with 7,904 records remaining after its execution. Evidence Eliminator removed the most records, leaving 4,755 records in the cache folder. Evidence Eliminator also left the fewest records in the "Visited Link" and "Cookies" folder with 314 and 113 records left, respectively. Heidi Eraser left the most records in the "Visited Link" folder with 1,031 records remaining. For the "Cookies" folder, Window Washer left the most records 672. Interestingly, Active@ ERASER somehow increased the number of records in the bookmarks folder from 86 records prior to execution to 90 records after execution.

4.4.2. Analysis of the Mozilla Firefox browser

Only Evidence Eliminator removed all detectable Internet history data elements using EnCase's Internet history search. All of the other wiping applications left relevant data in Firefox's Internet history. Eraser left the most traces of evidence in the "Cache" folder with 1,749 records left. Window Washer also removed all of the records from the XML and text folders, and it removed the second largest number of records from the other Firefox folders (after Evidence Eliminator).

4.5 Analysis of newly created files

We examined each of the post-experiment images to determine the extent with which any new files were created on the image after the image's data wiping application was executed. We found that all of the applications we studied created either log files or placeholder files, and some of them created both. We think

these findings are significant, as the data created by these applications provide valuable information that is useful for digital forensics examiners in determining the extent in which wiping activities were implemented. Specific findings from each application are provided below.

4.5.1 Files created by Active@ ERASER

Active@ ERASER created two types of files that are noteworthy. The first is an INI file that details which files the tool attempted to wipe (Figure 4 - Active@ Eraser INI File). The second type of file is a placeholder file with a .tmp extension. These .tmp files were created by Active@ ERASER to replace the files that were wiped and located under the same file paths of the original files. Two examples of the placeholder files are provided in Figure 5 - Placeholder files created by Active@ ERASER.

```
Last Accessed          04/25/11 04:21:52PM
File Created           04/25/11 04:21:52PM
Last Written           04/25/11 08:56:09PM
Physical Size          4,096
Physical Location      106,270,720
Hash Value             8ef4b1ad9fb88d7f2252d32ec3be5a09
Full Path              SPS2011 WT1b\Wiping Tool 1b\D\Program Files\Active Data Security Solutions
                       \Active Eraser Demo\EraserD.ini
[GeneralSettings]
StartupRun=1
RunMinimized=0
ConfirmManualErase=1
ConfirmScheduleErase=0
ErasingMethod=2
KeyExit=88
KeyCleanup=67
KeySetting=83
[StartPlacement]
Width=785
Height=560
TreeRight=250
[ScheduleSettings]
StartOptions=0
[CheckedFiles]
0=C:\Users\Forensics Prof\Pictures\2011-04-20 Building98
1=C:\Users\Forensics Prof\Pictures\Search chickenpasta.png
2=C:\Users\Forensics Prof\Pictures\Search applepie images.png
3=C:\Users\Forensics Prof\Pictures\Download italian food images.png
4=C:\Users\Forensics Prof\Pictures\Download idea images.png
5=C:\Users\Forensics Prof\Desktop\images italian food\italian_food_recession.jpg
6=C:\Users\Forensics Prof\Desktop\images italian food\italian_food2.jpg
7=C:\Users\Forensics Prof\Desktop\images italian food\italian-food2.jpg
8=C:\Users\Forensics Prof\Desktop\images italian food\italian-food.jpg
9=C:\Users\Forensics Prof\Desktop\images italian food\italian-food-cuisine-pizza.jpg
10=C:\Users\Forensics Prof\Desktop\images idea\light_bulb.png
11=C:\Users\Forensics Prof\Desktop\images idea\Light-Bulb-Idea-Hand.jpg
12=C:\Users\Forensics Prof\Desktop\images idea\idea.jpg
13=C:\Users\Forensics Prof\Desktop\images idea\gatsby-idea!.jpg
14=C:\Users\Forensics Prof\Downloads\pdf
15=C:\Users\Forensics Prof\Downloads\midi
16=C:\Users\Forensics Prof\Desktop\Culinary Documents
17=C:\Users\Forensics Prof\Downloads\yahoomailuploader_0.5.exe
```

Figure 4 - Active@ Eraser INI File

4.5.2 Files created by Window Washer

During our analysis of the Window Washer post-experiment image, we identified a log file named *Custom.mst* that was created by the application. This log file provides details of the files selected for wiping (Figure 6 - Log File Created by Window Washer).

Name	Z8518.tmp
Signature	Match
Last Accessed	04/19/11 12:36:18PM
File Created	04/25/11 08:53:11PM
Last Written	04/25/11 08:53:11PM
Physical Location	10,458,480,640
Physical Sector	20,426,720
Hash Value	52ed7cd2a664bc45274e8e1eded33718
Full Path	SPS2011 WT1b\Wiping Tool 1b\D\Users\Forensics Prof\Desktop\Z8518.tmp
Name	Z85C6.tmp
Signature	Match
Last Accessed	04/19/11 12:58:57PM
File Created	04/25/11 08:53:11PM
Last Written	04/25/11 08:53:11PM
Physical Location	13,886,885,888
Physical Sector	27,122,824
Hash Value	249e1be6d20f3da440dc421b69ff5a64
Full Path	SPS2011 WT1b\Wiping Tool 1b\D\Users\Forensics Prof\Desktop\Z85C6.tmp

Figure 5 - Placeholder files created by Active@ ERASER

4.5.3 Files created by BCWipe

From our analysis of the BCWipe post-experiment image, we found that this application also creates placeholder files within their respective folders to replace the files that were wiped. The majority of the filenames of the placeholder files appear to be random characters, and some of them include file extensions. Table 7 - BCWipe Placeholder files contains a listing of the placeholder files names within their respective folders.

4.5.4 Files created by Eraser

Our analysis of the Eraser post-experiment image yielded only one relevant file that was created after running the application, namely a log file named Task List.esrx. This log files appears to contain much metadata; however, for formatting purposes, we are omitting a copy of it from this paper due to its length and extensive quantity non-printable characters. However, it seems likely that additional, valuable content might be available if one were to become aware of the formatting structure of this log file, as many of the unprintable characters may contain important metadata, such as dates and time or binary values.

Name	Custom.mst
File Ext	mst
Signature	Unknown
File Created	04/26/11 02:03:03PM
Last Accessed	04/26/11 02:03:03PM
Last Written	04/26/11 02:03:03PM
Entry Modified	04/26/11 02:03:03PM
Physical Location	1,015,377,920
Physical Sector	1,983,160
Hash Value	584237ae2bb271be9e5e96eee0dcf0e0
Full Path	WPT2b\Window Washer\D\Users\ForensicsProf\AppData\Roaming\Webroot\Washer\Plugins\Custom.mst

```
[Desktop]
FileCount=58
File00=C:\Users\Forensics Prof\Desktop\bbsps.jpg
File01=C:\Users\Forensics Prof\Desktop\Downloads.lnk
File02=C:\Users\Forensics Prof\Desktop\Firefox Setup 4.0.exe
File03=C:\Users\Forensics Prof\Desktop\HazcomManual.doc
File04=C:\Users\Forensics Prof\Desktop\Loto.doc
File05=C:\Users\Forensics Prof\Desktop\rubric2009.doc
File06=C:\Users\Forensics Prof\Desktop\wrar400.exe
File07=C:\Users\Forensics Prof\Desktop\Culinary Documents\Bread.docx
File08=C:\Users\Forensics Prof\Desktop\Culinary Documents\Bread.pdf
File09=C:\Users\Forensics Prof\Desktop\Culinary Documents\Brownies.xls
File10=C:\Users\Forensics Prof\Desktop\Culinary Documents\Cheesecake.xls
File11=C:\Users\Forensics Prof\Desktop\Culinary Documents\Chips.docx
File12=C:\Users\Forensics Prof\Desktop\Culinary Documents\Chips.pdf
File13=C:\Users\Forensics Prof\Desktop\Culinary Documents\Cookies.xls
File14=C:\Users\Forensics Prof\Desktop\Culinary Documents\Grape Jelly.docx
File15=C:\Users\Forensics Prof\Desktop\Culinary Documents\Grape Jelly.pdf
File16=C:\Users\Forensics Prof\Desktop\Culinary Documents\peanut butter.docx
File17=C:\Users\Forensics Prof\Desktop\Culinary Documents\peanut butter.pdf
File18=C:\Users\Forensics Prof\Desktop\Culinary Documents\Tiramasu.xls
File19=C:\Users\Forensics Prof\Desktop\Culinary Documents\Tiramasu.xlsx
File20=C:\Users\Forensics Prof\Desktop\images idea\gatsby-idea!.jpg
File21=C:\Users\Forensics Prof\Desktop\images idea\idea.jpg
File22=C:\Users\Forensics Prof\Desktop\images idea\light_bulb.png
File23=C:\Users\Forensics Prof\Desktop\images idea\Light-Bulb-Idea-Hand.jpg
File24=C:\Users\Forensics Prof\Desktop\images italian food\italian_food_recession.jpg
File25=C:\Users\Forensics Prof\Desktop\images italian food\italian_food2.jpg
File26=C:\Users\Forensics Prof\Desktop\images italian food\italian-food.jpg
```

Figure 6 - Log File Created by Window Washer

4.5.5 Files created by Evidence Eliminator

As in our analysis of the Eraser post-experiment image, we found that the Evidence Eliminator post-experiment image contained only one newly created file of significant value, and it, too, was a log file. The Evidence Eliminator log file is named *Files.dat* and it lists the pathnames of files wiped by the application. The metadata associated with this log file and its visual contents are shown in Figure 7 - Evidence Eliminator log file.

Table 7 - BCWipe Placeholder files

\Users\Forensics Prof\Downloads\	\Users\Forensics Prof\Desktop\
moiodwblfgrrvee	xviiijsnertmaf
swsiraumlbmkveqamtejxccx	ffcnwfqquketc
pwsqswva.wey	twgkthep.owl
ohceabbdgtnuequybbnepvwotjqveu	oecjpxuajpbuexbj
lyxlvckrsnybr	ldwaskdaiqofxsnrwt
vacjbeidbbisdp	ufngsqha.hmr
qggkugyl.gmu	iexiyvlm.fqa
rfrsprfdyvnovctm	ycfdkmcbdhaiaev
rfrsprfdyvnovctm	fhthkuxdrwcleucqs
desktop.ini	bijmfhau.urn
pdf	yackamehuvmnir
midi	lxxxojhu.jew
	hjkoyytm.dyj
\Users\Forensics Prof\Pictures\	cudyehux.smb
pikbamjhkbtxwulahv	wwvcuqkoiicplg
eymerktseesfjycwdd	ohceabbdgtnuequybboepvwo
jnvarjoegbprhuotrl	jjrutfhrhlyrfaxb
dwapvgpwbnprouranv	bhkwfcuo.xpk
oedbbbpmvqxwbajldn	astyclxp.dwr
ufmvpgwmfklqkilbcu	qgmmiqsotndovvokgjxmjmgtrpfmyxnlmuwfykcusali
maamiufhrnomehrlha	kbkdyidlcvibbxuy
hcwhoqhpyndlyvqfaj	pftjrgprdprgmehe
tramtucnfiyxjwbhov	pgcjyjlrwhwkmhpov
kfvpbpibhekldukfgbvnelljxacaqnkv	hcbvomvrndmbjeiewxtpbqlwno
wqmxbkrmmmvobiqnlv	rkuappyibbfpekvuiohnwqrrkhksnc
dlbkuoqsmoffpwyhpn	yuxrmnovlmgmneqcc
inqfjfhqoivsexcpgc	kbcmishjtifmtnlcnohxdxbxqn
ntpureeuykmnkukbgf	klywbver.jwo
fgkumsxeqmkaunnibhsenqme	jtsmjnniyfxbfhknmrsem
rujsqrklixgdfgwtnbiwaix	idgqtemk.kif
dkqvodvehoeyjqcujrmbwudcmv	

```
Comment           Evidence Eliminator Log.
Name              Files.dat
Signature         ! Bad signature
File Created      05/02/11 04:48:22PM
Last Accessed     05/02/11 04:48:22PM
Last Written      05/03/11 02:08:10PM
Entry Modified    05/03/11 02:08:10PM
Physical Location 2,385,395,712
Physical Sector   4,658,976
Hash Value        37b663d1364ee98a32b8f6cd8da8bb02
Full Path         WT5b\SPS2011WT5b\D\Program Files\Evidence Eliminator\Data\Files.dat


C:\Users\Forensics Prof\Desktop\bbsps.jpg
C:\Users\Forensics Prof\Desktop\downloads.lnk
C:\Users\Forensics Prof\Desktop\Firefox Setup 4.0.exe
C:\Users\Forensics Prof\Desktop\HazcomManual.doc
C:\Users\Forensics Prof\Desktop\Loto.doc
C:\Users\Forensics Prof\Desktop\Rubric2009.doc
C:\Users\Forensics Prof\Desktop\wrar400.exe
C:\Users\Forensics Prof\Downloads\mseinstall.exe
C:\Users\Forensics Prof\Downloads\winzip150.exe
C:\Users\Forensics Prof\Downloads\yahoomailuploader.exe
C:\Users\Forensics Prof\Pictures\Download idea images.png
C:\Users\Forensics Prof\Pictures\Download italian food images.png
C:\Users\Forensics Prof\Pictures\Search applepie images.png
C:\Users\Forensics Prof\Pictures\Search chickenpasta.png
```

Figure 7 - Evidence Eliminator log file

4.6 Windows registry analysis

Our Windows registry analysis is the first of two methods we used to review the contents of Windows registry data. In this first method, we used AccessData's Registry Viewer to search the contents within the post-experiment images for each of the data wiping applications we studied.

Our Windows registry analysis focused on the *NTUSER.DAT* registry file (i.e., hive) and we evaluated the values for several subdirectories (i.e., keys). The paths we analyzed are listed in

Table 8 - NTUSER.DAT subdirectory analysis.

Table 8 - NTUSER.DAT subdirectory analysis

NTUSER.DAT>Software>Microsoft>	Internet Explorer>TypedURLs		
NTUSER.DAT>Software>Microsoft>	IAM		
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	RecentDocs	
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	RunMRU	
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	ComDlg32>	LastVisitedPidlMRU
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	ComDlg32>	OpenSavePidlMRU
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	ComDlg32>	FirstFolder
NTUSER.DAT>Software>Microsoft>	Windows>CurrentVersion>Explorer>	ComDlg32>	CIDSizeMRU

In analyzing these *NTUSER.DAT* subdirectories, we examined the post-experiment images of each wiping application. As we located traces of evidence pertaining to the files we had planted for wiping or any evidence indicating that a data wiping application had run, we then tracked these findings using the bookmarking feature within Registry Viewer. These bookmarks were subsequently included in reports we generated from Registry Viewer.

Three of the five wiping applications did not remove items from the *NTUSER.DAT* subdirectories. Using AccessData's Registry Viewer, we found entries for typed URLs, Internet accounts, recent documents, and recently used programs in the post-experiment images for Active@ ERASER, BCWipe, and

Eraser. Evidence Eliminator and Window Washer did remove data from their respective *NTUSER.DAT* files with different levels of completeness.

Window Washer removed the typed URLs and a portion of the data regarding recent documents. However, evidence remained that revealed the names of the most recently run programs, Internet accounts, and partial information concerning recent documents.

Of the five applications we analyzed, Evidence Eliminator performed the most thorough cleansing of the *NTUSER.DAT* data. Evidence Eliminator removed the entries in the typed URLs and recent documents subdirectories; however, Internet accounts remained in the *NTUSER.DAT* file, and additional data were present that indicated that the Evidence Eliminator application had been recently used.

All of the applications we analyzed left trace evidence in the *NTUSER.DAT* file. While some of the applications were more successful at removing evidence of previous activity than others, enough data remained to provide valuable information. Based on these findings, we suggest that forensics examiners routinely examine the *NTUSER.DAT* file, especially in cases where there is concern regarding the use of data wiping.

4.7 Regshot analysis

We used the Regshot utility to capture and compare a snapshot of the Windows Registry for the pre-experiment image and each of the post-experiment images. A summary of the changes in registry entries is provided in Table 9 - Regshot comparison summary. This table indicates the number of keys deleted or added from the execution of each data wiping application, as well as, additions, deletions, or modifications of values within the registry. The volume of data provided within the registry snapshots overwhelmed our current personnel resources for analysis; therefore, we were not able to fully examine the extent to which all of the registry entries were impacted by the execution of the data wiping tools. We did find sufficient evidence to justify continuing this evaluation in future studies, and we encourage other researchers to consider this topic.

Table 9 - Regshot comparison summary

	Active@ ERASER	Window Washer	Jetico BCWipe	Heidi Eraser	Evidence Eliminator
Keys Deleted	31	50,960	705	59,811	60,916
Keys Added	38	828	3,135	166	3,253
Values Deleted	63	156,161	1,428	207,899	213,523

Values Added	108	2,855	8,786	1,053	9,908
Values Modified	353	2,316	2,075	429	3,286
Total Changes	593	213,120	16,129	269,358	290,886

5. DISCUSSION OF FINDINGS

While the five data wiping applications we analyzed provide utilities for users to destroy data, we found that all of them leave some trace artifacts that may be valuable to digital forensics examiners. We found that all of the applications created log or other files that detailed their activity and all neglected to remove all relevant data within the Windows 7 Registry. Additionally, these applications left data regarding the usage of the Internet Explorer browser, and all but one of them left data regarding the Firefox browser.

Based on our analysis of these five applications, we suggest that digital forensics examiners routinely analyze the Windows Registry in situations where the examiner is concerned about the use of data wiping applications. For many years we have considered Windows Registry analysis to be among the activities performed during a thorough digital forensic analysis of a Windows-based workstation or server, and we do not think that the specific tasks identified within this paper significantly complicates or prolongs the digital forensic analysis procedure. In our opinions, the potential benefits derived from finding evidence resulting from the Windows Registry analysis outweigh the costs associated with performing the minor additional procedures.

We have also considered the long-term impact of these findings on digital forensic analysis. As this information regarding trace evidence from target-specific data wiping software applications become more disseminated, it is likely that software developers will modify their applications to reduce the amount of trace evidence left after its execution, and the more technically informed users of target-specific data wiping software applications will likely take additional steps to more thoroughly conceal their activities. As a result of these likely future changes, we anticipate that the amount of trace evidence recovered from Windows Registry analysis will decline; however, for the foreseeable future, we consider an analysis of the Windows Registry to be an essential part of a thorough digital forensic analysis of a Windows-based workstation or server.

6. LIMITATIONS

In this study, we analyzed only five data wiping applications that function on Windows 7 based systems. While our methodology of performing measured experiments based on identical data supports generalization, our small sample size does impose significant statistical limitations that make us reluctant to generalize

these findings. Our limited resources, particularly temporal constraints, prohibited us from thoroughly analyzing the extent to which all Windows Registry keys were modified from the data we collected in our Regshot analysis. Nonetheless, the results we obtained are applicable for the experimental conditions, and the methodology that we outlined here was successful in defining a process and procedure with which to carry out additional experiments in more detail and with a broader suite of applications.

We recognize that there are instances whereby users have legitimate reasons for using target-specific data wiping application software. It would be beneficial to provide data concealment information for uses in these instances; however, our focus during this study was directed at a scenario in which a forensic examiner is tasked to recover evidence from a Windows 7 workstation where the user utilized target-specific application software to conceal data or activities. Based on our research focus, we address the forensic examiner's role of identifying trace evidence without regard to normative values.

A potential counterproductive artifact from this study is that the authors of data removal applications may become more aware of the trace evidence that we have exposed and modify their applications to nullify our findings, thus raising the anti-forensics bar. That is, of course, a downside to any research in this space, as those who hide evidence can often stay ahead of those who are tasked with finding it. Nevertheless, the mere existence of wiping software that is "examination-proof" does not mean that users will properly employ it and, therefore, research in this area can still be used to inform the digital forensics community.

7. CALL FOR ADDITIONAL RESEARCH

A more thorough analysis of the Windows Registry modifications might prove to be valuable. Additional research from a larger, scientific sample of data wiping applications might lead to a better understanding of this area, so that generalizations can be recognized.

In addition, as data wiping becomes more commonly available, even built in with operating systems and user applications, computer forensics examiners need to have a more defined approach to detecting when wiping programs have been used and the mechanism employed. To that end, we need to have testing methods in place as new operating systems, applications, and versions of applications become available. Test beds to help detect wiping signatures, including remnants in the registry and other log files, will greatly enhance our ability for this very detection.

8. ACKNOWLEDGEMENTS

The authors would like to take this opportunity to express their appreciation for the work performed by a team of undergraduate students from the Computer Information Systems Department of California State Polytechnic University (Pomona, California) for their attention to detail in conducting and documenting the results from numerous experiments performed within this study. This team of

students consisted of Robert Magzanyan, team leader, Marcus Mehldau, Austin Pham, Justin Pham, Samuel Park, Jason Bresnan, Jason Hoogeveen, and Deanna Maserjian.

9. ABOUT THE AUTHORS

Gregory H. Carlton is Associate Professor in Computer Information Systems and Director of Computer Forensics Programs at California State Polytechnic University (Pomona, California). Greg is also an independent practitioner of computer forensics services, he has been qualified as an expert witness, and he has provided expert testimony. Greg holds a BSBA with concentrations in Information Systems and Marketing, a MBA, and a Ph.D. in Communication and Information Sciences. He is an EnCase Certified Examiner (EnCE) and a member of the High Technology Crime Investigation Association (HTCIA).

Gary C. Kessler is Associate Professor of Homeland Security at Embry-Riddle Aeronautical University (Daytona Beach, Florida), focusing on cybersecurity, and an independent consultant providing training and practitioner services in the areas of computer, network, and mobile device security and forensics. Gary holds a B.A. in Mathematics, an M.S. in Computer Science, and a Ph.D. in Computing Technology in Education, and is a Certified Computer Examiner (CCE) and Certified Information Systems Security Professional (CISSP). Gary is also a member of the Vermont Internet Crimes Against Children (ICAC) Task Force, High Tech Crime Consortium (HTCC), and HTCIA, an Adjunct Associate Professor at Edith Cowan University (Perth, Western Australia), and editor-in-chief of the *Journal of Digital Forensics, Security and Law*.

10. REFERENCES

Acronis Inc. (2011). *Hard disk drive wipe software providing complete disk cleanup*. Retrieved April 2, 2011 from http://www.acronis.com/enterprise/products/drivecleanser/

Active Data Security Solutions. (2011). Retrieved April 14, 2011 from Active@ ERASER: http://www.active-eraser.com/features.htm

Alghafli, K. A., Jones, A., & Martin, T. A. (2010). Forensic Analysis of the Windows 7 Registry. *Journal of Digital Forensics, Security and Law, 5* (4), 5-30.

Bodrag, S.R.L. (2011). *Wipe Expert 2*. Retrieved April 2, 2011, from http://www.bodrag.com/prod/wipe_expert/

EvidenceSmart.com. (2011). *Evidence Smart - Your reliable Privacy Protector*. Retrieved April 2, 2011, from http://www.evidencesmart.com/

Geeknet, Inc. (2009). *SourceForge.net: regshot - Project Web Hosting - Open Source Software*. Retrieved July 12, 2011, from http://regshot.sourceforge.net/

GEEP EDS LLC. (2011). *Darik's Boot and Nuke*. Retrieved April 2, 2011, from http://www.dban.org/about

Geiger, M. (2006). Computer-Forensic Tools: Analysis and Data Recovery. *FIRST.org. 18.* Baltimore: FIRST.org, Inc.

Heidi Computers, Ltd. (2010). *Software Products*. Retrieved July 7, 2011, from http://www.heidi.ie/

Hughes, G. F., Coughlin, T., & Commins, D. M. (2009). Disposal of Disk and Tape Data by Secure Sanitization. *Security and Privacy, 7* (4), 29-34.

IDM Computer Solutions, Inc. (2011). *UltraSentry - secure file delete, Internet history removal, cookie delete, registry cleaner*. Retrieved April 2, 2011, from http://www.ultraedit.com/products/ultrasentry.html

IOLO Technologies, LLC. (2011). *iolo DriveScrubber*. Retrieved April 2, 2011 from, http://www.iolo.com/ds/3/

Jetco Inc. (2011). Retrieved April 14, 2011, from http://www.jetico.com/wiping-bcwipe/

Jones, A., & Meyler, C. (2004). What evidence is left after disk cleaners. *Digital Investigation*, 183-188.

KremlinEncrypt.com. (2008). *Kremlin Wipe*. Retrieved April 5, 2011, from http://www.kremlinencrypt.com/wipe.htm

Low, J. (2010). *Eraser*. Retrieved April 14, 2011, from http://eraser.heidi.ie

O & O Software, GmbH. (2011). *O & O SafeErase 5 Secure Hard Drive Data Erase Software*. Retrieved April 2, 2011, from http://www.oo-software.com/home/en/products/oosafeerase/

Paragon Technologies GmbH. (2011). *Paragon Disk Wiper Personal*. Retrieved April 2, 2011, from http://www.paragon-software.com/home/dw-personal/

Robin Hood Software Ltd. (2011). *Product - Evidence Eliminator*. Retrieved April 14, 2011, from http://www.evidence-eliminator.com/

R-Tools Technology, I. (2011). *Disk Cleaning and Internet Privacy*. Retrieved April 5, 2011, from http://www.r-wipe.com/

Webroot Software, Inc. (2011). *Window Washer, Computer & Internet Privacy Software*. Retrieved April 14, 2011, from http://www.webroot.com/En_US/consumer-products-windowwasher.html