2010

An Investigation into the Efficacy of Three Erasure Tools under Windows 7

Cheng Toy Chiang
Edith Cowan University

Kelvin Triton
Edith Cowan University

Andrew Woodward
Edith Cowan University

DOI: 10.4225/75/57b2b5b740ce4
Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

An Investigation into the Efficacy of Three Erasure Tools under Windows 7

Cheng Toh Chiang Kelvin Triton and Andrew Woodward
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

Abstract

This paper examined three erasure software tools aimed at removing evidence of online and other activity, and was investigated using the Windows 7 operating system as the test platform. The tools in question were Anti-Tracks, Free Internet Eraser and Free Internet Window Washer. The findings included each of the tested software's ability to completely erase target data on the drive. It also included examined whether the data was erased or merely the link to the data was deleted, making the file recoverable. It was found that the Anti-Tracks program did not erase any of the information targeted by the researchers. The Free Internet Window Washer software was able to erase Internet Explorer browser history, and recent document activity for the operating system, but not any other activity or information was erased. The last tool, Free Internet Eraser was able to erase all information apart from MSN Messenger chat history, and the temporary internet files. The conclusion is that end users should be careful in selecting or using such erasure tools as they may behave differently under different operating systems, and may not always remove beyond recovery all information.

Keywords

Erasure tools, internet activity, digital forensics, anti-forensics

INTRODUCTION

Organisations and individuals who have employed the use of erasure software have no reason to doubt that the data on the hard drive is securely erased. However, this is not necessarily the case, as there is residual data which is the remainder of the original data left on the disk. This is partly due to the storage principles and magnetic force properties (Dong *et al.*, 2009). Another possibility of having residual data remain on the hard disk is because data can be written on any part of a hard disk as files are created, deleted and re-written. If the hard drive is 40GB, some of the content can be written on the 20th GB sector. If an individual uses a trial version of erasure software and the erasure software only erases the first 5 GB of the hard drive, this means that the content is still on the hard drive (Author 2007). Along with this process, other operating system functions such as virtual memory and block usage on the disk itself also result in file and system slack space occurring on the drive (Garfinkel & Shelat, 2003).

Information can also be leaked through different types of media such as email and chat program. Some employees may choose to reveal sensitive information through a chat program and later use erasure software to cover their tracks. There are many erasure software tools available for download from the World Wide Web. Many software claims to perform the tasks of browser cleaning, window cleaning among the many other features available. Some of these tools are free, some have trial periods, while others have to be purchased.

Since the operating system delete function is unable to remove data thoroughly, as pointed out by Dong, Kun and Yu (2009), users need to make use of software that removes all data remnants in the hard drive prior to disposal. If sensitive information still resides in the hard drive, it could lead to undesirable consequences. Erasure software plays an important role prior to disposing a hard drive, as regardless of whether the information belongs to a home user, or the director of a multi-national Organisation, mismanagement of personal details can have adverse consequences (Watson, 2009). It is therefore important that users know how effective the erasure software is and what limitations it has, if any.

This paper examined the efficacy of three software based data erasure tools in terms of their claims to destroy data. A range of different data types were examined, with the focus on the functionality of the following three erasure software tools: Anti-Tracks, Free Internet Eraser, Free Internet Window Washer.

MATERIALS AND METHODS

To ensure that the tests were carried out in a forensically sound manner, the operating system and software should be installed on a forensically erased hard drive for each test. To achieve this in a manageable timeframe, a virtual machine was created on an existing hard drive. The operating system, Windows 7, was then installed on this virtual machine, and relevant software was then installed. This was followed by performing various tasks such as internet banking, surfing web sites, downloading files and performing chat activities.

Different web browsers such as Internet Explorer, Flock, Mozilla and Netscape Navigator were installed to test how well the erasure software performed on each of the browsers. Different types of activities were carried out through the web browsers such as internet banking, searching and normal surfing activities. Different download programs were also installed to test the functionality of the erasure software. Windows messenger is installed as it is one of the many chat programs many users use to communicate. The various erasure software and software recovery tool is then installed.

After all the software installations, the instance is cloned three times. This is to ensure consistency and in an event where the process of erasure and retrieving erased files, it can be reproduced with the same consistencies. This will also allow all the erasure software to be tested on a common platform.

Erasure Software

Anti Tracks

Anti Tracks software is a shareware program by Giant Matrix. The features it claims to perform can be found from its website (Giant Matrix, 2010). Anti Tracks shows what files it attempts to delete. It does not have an option to delete other browser surfing history, and download programs' history. However, it does have plug-in MSN messenger and yahoo messenger. The website claims it is able to securely erase tracks and unwanted files so that they are gone forever (Giant Matrix, 2010).

Free Internet Eraser

Free Internet Eraser is a paid software by Privacy Eraser. This software is chosen because it claims to support Microsoft Windows' platform ranging from FAT to FAT32 to NTFS file system. It also claims that it exceeds the US Department of Defense DOD 5520.22-M and NSA clearing and sanitizing standards. It also claims that with this software, the data once erased cannot be recovered (Privacy Eraser, 2010).

Free Internet Window Washer

Free Internet Window Washer is a free erasure software tool by Eusing Software. The features it claims to perform can be found from its website (Eusing Software, 2010). There are several options that can be set using this software. The program can clean Internet Explorer, Netscape and Mozilla among others. It can also clean the history in messenger.

Target Locations and Information

Different erasure software removes many different areas of traces of information on the hard drive. These software lists down what type of information are erased. For this paper, four main area of interest were targeted.

The common areas of interest were:

- Windows operating system recent access document history
- Browsers' surfing history
    - Flock
    - Internet Explorer
    - Mozilla
    - Netscape
- Chat programs' history
    - Windows Messenger
- Downloading Programs' history
    - BitTorrent
    - LimeWire

The recent access document history is of interest because it is an area which records what files the user has access recently. An employee of an Organisation would want to remove traces found in recent document history if the files accessed are not allowed. The employee may attempt to use erasure software to delete the history found.

The surfing history under the web browser is another major concern especially if sensitive information has been input. It has to be tested against different browsers because different users have different browsers.

Another program which is of concern to security investigators will be a chat program history. The history can reveal if any sensitive data has been transmitted between the sender and receiver. The sensitive data may include company trade secrets, clients' details or statistical figures.

For digital forensics investigators, the ability to trace what programs what programs and files were download is another way to find if any malicious software have been downloaded. This can be performed by disgruntled employees.

The primarily goal of this project is to determine if the software in the market is able to erase files from the system securely. This is very important because many Organisations need to dispose their hard drives which contain sensitive information properly. If the erasure software does not erase the files securely, this will mean that information from the hard drive may be retrieved.

Procedure

A base image is created first and subsequently cloned. This is to ensure that the software that is going to be tested has a common platform with same data set to be performed on.

a) Install Virtual Machine. By installing this software, it allows a secondary operating system to be installed within Windows XP which is the base operating system.

b) Create Base Image. The purpose of creating a base image is to allow duplication of the same test environment for the different erasure software. This will allow a consistent set of variables to be tested. The process is as follows:

- Install Windows 7 (Operating System)
- Install Windows Live Messenger (Chat Program)
- Install LimeWire (Download Music, Files, Program Software)
- Install BitTorrent (Download Music, Files, Program Software)
- Install Flock (Web Browser)
- Install Mozilla Firefox (Web Browser)
- Install Netscape Navigator (Web Browser)
- Install Anti-Tracks (Erasure Software)
- Install Free Internet Eraser (Erasure Software)
- Install Window Washer (Erasure Software)
- Install Regshot (Compare Registry Prior and After Task is Performed)
- Install Recovery Software (Easeus)
- Perform Task – Chatting on Windows Live Messenger
- Perform Task – Download Music, Files, Program Software on LimeWire and BitTorrent
- Perform Task – Surfing, Internet Banking, Google Search on Flock, IE, Firefox, Navigator

c) Clone Image. The objective is to have the same test environment for the different erasure software to be tested. This will allow comparison between the effectiveness of the software. The 1st Regshot is taken to record the variables prior to erasure software being run. The 2nd Regshot is taken to record the changes after the erasure software was run, allowing for comparison of the changes before and after. The 3rd

Regshot was taken to allow comparison with the 4th Regshot where the recovery software is run between them. The procedure is then repeated for each of the other two tools.

- Run Regshot and take 1st shot
- Run Erasure tool
- Run Regshot and take 2nd shot
- Run Regshot and Compare the difference between 1st and 2nd shot
- Run Regshot and take 3rd shot
- Run Recovery Software
- Run Regshot and take 4th shot
- Run Regshot and Compare the difference between 3rd and 4th shot
- Run EASEUS recovery software

RESULTS

A summary of the findings for all three tools can be found in Table 1. Individual results for each tool are explained below.

Table 1: Results of an investigation into internet erasure activity software. Three tools were examined for their ability to delete software as claimed

	Anti Tracks	Free Internet Window Washer	Free Internet Eraser
Browser History			
Flock	N	N	Y
IE	N	Y	Y
Mozilla	N	N	Y
Netscape	N	N	Y
Chat Program			
Messenger	N	N	N
Download Program			
LimeWire	N	N	Y
BitTorrent	N	N	Y
OS Recent Document History	N	Y	Y
Temporary Files Directory	N	N	N

Anti Tracks

There were eight keys deleted through the comparison between prior and after to executing anti-tracks programs. There are four keys that were added (recovered). It is noticed that it deletes only the recent documents (RecentDocs) folder. The browsers' surfing history were not deleted. The chat program's message history is also not deleted as well. The various downloading software history were also not deleted. After anti tracks program was run, the recovery software (EASEUS) is immediately executed to see if it can recover any of the deleted files. It was noticed that the recovery software managed to recover some of the contents that was deleted in the recent document (RecentDocs) folder. When Anti-Tracks software is run again, it is noticed that it can still locate files in windows temp folder, recent documents history, Internet Explorer cookies, Internet Explorer Cache and Internet Explorer browser history. This means that despite its claims to delete the files in concern, it is still able to locate the files in the drive. This is further supported by Easeus Data Recovery software showing that it can still restore the files. Web browser programs such as Mozilla and Netscape also indicates that its browser history is still intact. By input a previous partial visited URL, the full URL will appear for completion shows that the surfing history was not deleted by the anti-tracks erasure software. Chat programs such as Windows Live Messenger and LimeWire also indicated that the chat history and download history were not deleted.

The Anti-tracks software behaved as claimed on the manufacturer's website in that it was able to delete browsing history, windows temp files and recent document history. However, it did not appear to have the ability to delete information for other browser software such as Mozilla and Netscape. Even when the files were said to be deleted, it can still be recovered. The tool (Anti-Tracks) has likely unlinked the files but will not wipe the data from the disk. This is because the files can be recovered using the EASEUS recovery software.

Free Internet Eraser

The regshot program was executed before and after free internet eraser was run to capture the various files and keys that were deleted. It was observed that there were thirty-six values being deleted and four values were added (restored). Free Internet Eraser software was unable to erase LimeWire download history, Messenger chat history, Mozilla and Netscape browser history. It however was able to delete Internet Explorer. It however was able to retrieve the RecentDocs history files.

Free Internet Eraser performs most of its claims on the website. These include clearing the chat history of messenger, Google web browser history, IE web browser history and Mozilla web browser history. A search for index.dat in Windows 7 yields no returns. This software can be classified under the alternate hypothesis (H1) as Free Internet Eraser can be relied upon removing all traces of Internet activity. It has unlinked the files and wiped data from the disk. It has also modified the registry and wiped the old registry file. The majority of the registries (thirty-six) were modified and four were retrieved.

Free Internet Window Washer

After running Free Internet Washer, a list of items found deleted through regshot which compared what were changed before and after Free Internet Washer program is run. There were thirteen keys that were deleted through regshot program and three keys were recovered.

After the erasure software is run, EASUS recovery software is launched to attempt to find if any files that were deleted can be retrieved. It is noticed that it still managed to retrieve some files from the Recent Document folders. When Netscape was run again after executing Free Internet Washer, the browsing history was still not deleted. It was also unable to clear Flock browsing history. However, it was able to clear the Google and Mozilla browsers' history. It was also able to clear the message history of Messenger.

DISCUSSION

As criminals resort to erasure software to remove incriminating evidence, it is important to know the functionality of erasure software because forensic examiners need to retrieve data based on date and time as evidence is a fundamental part of forensic computing examinations (Boyd & Forster, 2004, p. 18). Erasure software such as anti-tracks and free internet window washer did not managed to delete most of the browsing history, chat history coincides with the 2005 report which Geiger pointed out that not all erasure software functions properly (Geiger, 2005, p. 2). All three tested erasure software were unable to delete Windows Messenger chat history. The chat history allows forensic examiners to gain an insight of the user's messenger activities (van Dongen, 2007, pp. 86-87).

Besides forensic examiners who want to know the functionality of erasure software, criminals will be interested to know also. This is because they want to remove traces of evidence to prevent forensic examiner who would use recovery software such as EASEUS to retrieve erased files. In the testing procedure, internet banking transaction was performed as it is one of the many common activities perform by internet users. When these users dispose of their computers, they did not pause to think that that such sensitive information is still stored on the computer (James, p. 2).

If they had use one of the unreliable erasure programs such as anti-tracks, it would have given the user false impression that the sensitive has been erased which is not the case or it can be recovered using recovery software. In an event when a user believes that the data has been erased and dispose it through thrift shop or leave it just next to a rubbish bin, someone can easily get hold of them and run recovery software to retrieve sensitive data and used it for illegal activities including identity theft and fraud (Author, 2007).

It is therefore important to use software such as Free Internet Eraser that uses DoD 500.28 standard to perform erasure tasks. This software is different from its predecessor DoD5220.22 in that it runs seven passes rather than three and employs the use of more random data in erasure data (Innes, 2005, p. 24).

Even when the erasure program indicates that the data has been removed, it may mean that the original data still sits in the sector of the hard drive. If one knows the record structure of a file system, it is possible to reconstruct the information that does not exist in the HASH table. (Jones, 2003, p. 28) One of the possible ways to ensure that it is completely removed is to grind the platters of the hard drive till the shine is gone or by drilling holes into the drive (Verducci, 2007). Either method will result in a hard drive which is physically destroyed, and unlikely to be recovered short of heroic effort by a state actor.

There can be undesirable consequences should individuals and Organisations that use the software that were supposed to erase the data but did not perform these tasks. If after performing the erasure tasks the user was to dispose of the machine, and there is sensitive information that can be retrieved, it can have adverse effects on the Organisation and the owner of the hard disk. The information can compromise the integrity and security of the Organisation and individual in concern.

Among the three erasure software tools examined in this research, Free Internet Eraser erased the greatest amount of data by type. However, there were some elements which were not erased by this software. In order to completely There is HDE-1 Hard Drive Eraser which totally and completely destroys magnetic encoding on a hard drive including all the factory pre-encoded data, rendering the drive unusable (Anderson, 2006, p. 39). However, this software is reasonably expensive, and while a corporation would certainly have no issue with using such software, a private individual is unlikely to pay this cost; it is more likely that they will use software such as one of the three tested here. The issue being that not all data is erased beyond recoverability with this software, as has been demonstrated in this research.

CONCLUSION

Of the three software tools tested here, the Free Internet Eraser performed the best as it deleted the majority of the internet activities' history. The data that were erased included chat history in messenger, the browsing history of the browsers, and the traces of downloaded programs. This tool also included the option to erase to DoD erasure standards.

Anti Tracks and Free Internet Window Washer showed that data were deleted but most was recoverable. It is therefore important to know the strengths and limitations of the erasure software so that individuals and organisations can handle sensitive data in an appropriate manner. Besides using reliable and robust erasure software, procedures to erase data must be followed especially for sensitive information.

There is a need to understand that data remnants do exist on hard drives and data disposal must be treated with the same degree of care as for other information security practices and procedures. Studies carried out show that many people believed that the data has been erased but it was not the case. Some organisations may have security policies to ensure that the drives are to be sanitised prior to disposal but is the process being audited? Further research will aim to expand the scope of this trial to include a greater variety of tools, and also to look for additional remnants in terms of data type in order to determine whether this software meets the manufacturer's claims. Additional research could also be carried out to determine whether people are aware of the consequences of not erasing their data on a hard drive prior to disposal.

Organisations that rely on insecure erasure software risk loss of confidential data, which could potentially lead to financial loss, embarrassment, legal action, and maybe even have national security implications. Criminals who rely on the insecure erasure software risk being apprehended by the authorities. End users of such tools are advised to perform due diligence, and not just depend on what the software manufacturer claims.

REFERENCES

Anderson, J. D. (2006). Destroying/erasing your hard drive. *Accounting & Tax Periodicals, 16*(7), 39.

Boyd, C., & Forster, P. (2004). Time and date issues in forensic computing--a case study. *Digital Investigation, 1*(1), 18-23. doi: DOI: 10.1016/j.diin.2004.01.002

Dong, H., Kun, S., & Yu, C. (2009). *Research on secure destruction of digital information*. Paper presented at the Apperceiving Computing and Intelligence Analysis, 2009. ICACIA 2009. International Conference on

Eusing Software. (2010). Internet Eraser Feature, from http://www.eusing.com/Window_Washer/Internet_Eraser_Features.htm

Garfinkel, S.L. & Shelat, A. (2003). Remembrance of data passed: a study of disk sanitization practices. *Security & Privacy, IEEE*, **1(1):** pp 17-27

Geiger, M. (2005). Evaluating Commercial Counter-Forensic Tools *2005 Digital Forensic Research Workshop (DFRWS)*. New Orleans, LA.

Giant Matrix. (2010). Why Anti Tracks Retrieved 07 September 2010, from http://www.giantmatrix.com/products/anti-tracks/

Innes, S. (2005). *Secure deletion and the effectiveness of evidence elimination software*. Paper presented at the Proceedings of 3rd Australian Computer, Network & Information Forensics Conference, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.

James, D. G. Forensically unrecoverable hard drive data destruction.

Jones, K. J. (2003). Forensic Analysis of Internet Explorer Activity Files. Retrieved 14 June 2010 http://ftp2.uk.freebsd.org/sites/download.sourceforge.net/pub/sourceforge/o/project/od/odessa/ODESSA/White%20Papers/IE_Internet_Activity_Reconstruction.pdf

Martinez-Cabrera, A. (2010). Erasing all digital footprints 'impossible', *The San Francisco Chronicle,* p. 3.

Privacy Eraser. (2010). Internet Eraser Pro - Erase internet history & protect your privacy! , 2010, from http://www.privacyeraser.com/index.html

Valli, C., & Jones, A. (2005). *A UK and Australian Study of Hard Disk Disposal.* Paper presented at the In Proceedings of the 3rd Australian Computer, Information and Network Forensics Conference, Edith Cowan University, Perth, Western Australia.

Author. (2007). *Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks.* Paper presented at the Proceedings of The 5th Australian Digital Forensics Conference, Edith Cowan University - Mount Lawley Campus.

van Dongen, W. S. (2007). Forensic artefacts left by Windows Live Messenger 8.0. *Digital Investigation, 4*(2), 73-87. doi: DOI: 10.1016/j.diin.2007.06.019

Verducci, A. (2007). How to absolutely, positively destroy your data: DIY tech Retrieved 10 June 2010, from http://www.popularmechanics.com/technology/how-to/computer-security/4212242