

The effectiveness of commercial erasure programs on BitTorrent activity

Andrew Woodward
School of Computer and Information Science
Edith Cowan University
a.woodward@ecu.edu.au

Abstract

Recent developments have seen the closure of P2P sites such as Kazaa and Napster due to legal action, and a subsequent rise in the use of alternative file-sharing software, namely BitTorrent. This research in progress aims to evaluate the effectiveness of commercial programs to erase traces of the use of such software. The erasure programs Privacy Suite, Window Washer and R-Clean and Wipe were used on a machine that had used the BitTorrent client Azureus to download two torrent files. The drive was imaged and examined forensically with Autopsy, and the registry was also examined on the source machine. The program R-Clean and Wipe left evidence in both the registry and the image of the name and type of files that had been downloaded with this software. Of greater concern was that the software Window Washer and Privacy Suite claimed to erase evidence of P2P activity, but it did not remove evidence of torrent activity. Current erasure tools do not appear to be effective at removing traces of BitTorrent activity.

Keywords

P2P, BitTorrent, file sharing, erasure software

INTRODUCTION

Perceived losses by various media representative organisations (RIAA, MPAA) has led to the closure of many sites and even software which supported / allowed users to share files with each other. Such software is known as peer-to-peer or more commonly as P2P. The most popular examples of this type of software are eDonkey, Kazaa and Napster. Napster was the original P2P software client, and was closed down some time ago (BBC 2000). Kazaa was a newer incarnation of P2P software, and has also recently had legal action taken against it which will likely see its demise due to the changes being enforced on it (Ferguson 2005). In addition to closing down the organisations that allowed for such file sharing to take place, the various representative bodies have also gone after high volume users of these services or products (MPAA 2005). As a result, a form of file sharing software that had been around since 2001, known as BitTorrent, has become more popular, (BitTorrent 2005). It is similar to its contemporary P2P clients in that it is a decentralised means by which users can exchange information. The difference with torrent exchange, or “streaming” as it is known, is that a file is broken down into much smaller fragments, and it is these fragments that are exchanged between many users. This type of technology is actually a very efficient means of allowing users to download files, and is being used by various organisations (Layman 2005; Linspire 2005) for legitimate purposes. The eDonkey software (MetaMachine 2003) is being used by file sharers as a replacement for the previous two clients, and while there is evidence that usage of this software is increasing in some countries, but in others, it is torrent software that dominates (BBC 2005).

While software exists to remove traces of P2P activity from programs such as E-donkey, it is unknown whether this software is effective at removing traces of BitTorrent activities. Three commercially available erasure tools were selected to determine whether they can remove traces of torrent activity. These were R-Clean and wipe (RRT, 2005), Window Washer (Wenroot, 2005) and Privacy Suite (CyberScrub, 2005). This research in progress paper examined the ability of these programs to remove evidence of torrent activity.

THE ERASURE PROGRAMS

Three different erasure programs varying in both claims and manufacturer were used for testing. Details of each and their claims to their ability to erase various activities are given here.

R-Clean and Wipe - Version 5.1, Build 1169

This erasure software is produced by R-Tools technology and the manufacturer makes the following claims about its software:

R-Wipe & Clean is a complete solution to wipe useless files and keep your computer privacy. Irretrievably deletes private records of your on- and off-line activities, such as temporary internet files, history, cookies, autocomplete forms and passwords, swap files,

recently opened documents list, Explorer MRUs, temporary files, etc. and free up your disk space. The utility wipes files and unused disk space using either fast or secure erase algorithms. All files and folders may be combined in wipe lists to erase them in a single procedure. Supports both the FAT and NTFS file systems. All separate wiping and cleaning tasks can be combined in one or more erasing procedures launched immediately or at predefined times or events as a background task.

(RTT, 2005).

It is worth noting that this software does specifically claim to erase evidence of either P2P or BitTorrent activity.

Window Washer – Version 6, Build 6.0.2.466

This software is produced by the Webroot Company and makes the following claims about its software:

Extensive Wash Areas

Window Washer scrubs hundreds of areas on your PC to remove unnecessary files to ensure your privacy and free up valuable disk space.

Browser Activity Eraser

Window Washer cleans all aspects of your browser activity, including Internet history, address bar, cache, cookies, and more. Mozilla and Firefox users now enjoy the same online privacy protection that users of Internet Explorer, AOL and Netscape already enjoy.

Permanent Bleaching

Bleach, an encryption feature, completely overwrites files with random characters to make them unrecoverable. This feature is so powerful it exceeds the tough standards of the Department of Defense and the National Security Agency.

Free Space Cleaner

Free space on your computer contains portions of old and previously deleted files and documents. Window Washer now cleans this area making the files you deleted earlier permanently unrecoverable.

One-click Shredder

Window Washer lets you simply and conveniently shred a folder and all of its contents, or just a single file, in one step. Just a simple right-click will permanently overwrite these files, making them unrecoverable.

Critical File Protection

Window Washer includes built-in safety features to help prevent you from accidentally removing important files. Alerts prompt you to confirm your request to delete special folders, like system folders, My Documents, My Photos, and others, so they remain safe from unintentional deletions.

Smart Cookie Saver

Window Washer deletes the cookies you don't want and lets you keep and save those you do. That way you maintain your preferred Internet settings and log-ins for all your favorite sites.

Flexible Washes

During a wash, Window Washer automatically cleans the latest versions of your favorite programs such as Real Player, Google Search Toolbar, iTunes, Macromedia Flash Player, Adobe Acrobat and hundreds more, to keep these programs running smoothly.

Automatic Wash Cycles

You can set Window Washer to automatically clean your system at specified intervals, like at shut down or start up. For added security, we recommend setting Window Washer to wash when you close your Internet browser.

Total System Erase

Window Washer can be set to fully erase your hard drive, files, programs and operating system for easy re-formatting. Consider using this feature if you're donating or selling your PC and you don't want your files to be seen by strangers.

Again, while this product states that it erases all history of Internet activity, it makes no specific claims about either P2P or BitTorrent activity.

Privacy Suite – Version 4.0, Build 4.0.0.144

The manufacturer of this software, Cyberscrub, made the following claims about their software:

Key Features

Completely eliminates sensitive data from your computer: valuable corporate trade secrets, business plans, personal files, confidential letters, e-mail messages, Media Player/Real Player history, Web browser tracks, AutoComplete, cookies, Recent Docs, Find/Run data, etc.. Supports Internet Explorer, Netscape, Mozilla and Opera.

Peer2Peer- Erase all evidence from 22 popular applications such as KaZaA, iMesh, Morpheus and more.

Privacy Suite erases data by wiping its contents beyond recovery, destroying its name and dates and finally removing it from disk.

Meets and exceeds the U.S. Department of Defense standards for the permanent erasure of digital information (U.S. DOD 5220.22).

Wipe compressed files on NTFS (allows wiping from the original location of the file).

Scramble file names and folders- destroy file attributes from FAT or MFT partitions.

Offers wipe methods that can stop both software and hardware recovery tools from restoring the erased data.

Stealth mode.

Isaac Random Generating Algorithm.

Completely destroys any data from previously deleted files that might still be accessible on your disk (in the Recycle Bin, in the unused area of the disk or in the slack portion of existing files).

Destruction of file attributes from previously "deleted" files.

Integration with the Windows Recycle Bin: Privacy Suite can destroy the files contained in the Recycle Bin beyond recovery.

Integration with the Windows shell. You can drag files and folders from Explorer and drop them in Privacy Suite, or you can erase them directly from Explorer or My Computer, with a single mouse click.

Eliminate newsgroup binaries (photos) and chat room conversations and Instant Messages that are stored on your computer.

Erases folder structures (folders with all their subfolders and files) and even entire drives.

Delete "locked" Windows files, index.dat, the swap file and "cookies" that track your Internet history .

Cookie management allows you to keep selected cookies.

Privacy Suite can automatically clear the contents of folders that usually contain sensitive data (such as the Web browser cache, Temporary Internet files, the recent document list, the folder designated for temporary files, etc.).

Advanced features like verifying each wipe pass and each disk operation allow Privacy Suite to intercept any failures and inform you if data is not successfully erased.

The command line parameters allow you to insert erasing commands to your BAT files and then run this BAT file automatically using SystemAgent or other scheduling software.

USB flash mini/thumb drives.

Supports FAT12, FAT16, FAT32 and NTFS file systems, floppy, ZIP and Jaz drives.

METHODOLOGY

Step 1

A PC was imaged with Microsoft Windows XP, service pack 2, and the latest Windows updates. The BitTorrent client “Azureus” (version 2.3.0.4), an open source program, was downloaded and installed (Azureus, 2005). As part of this install, the latest Java run-time environment (JRE) version 1.5.0 was also installed (Sun Microsystems, 2005). After successful installation, a download of two legal files was commenced using the Azureus program. At this point, the drive was imaged as the datum so that the three erasure programs could be used. Details of the files used to perform the BitTorrent downloads are as follows:

Observatory Online Archives – Volume 1: <http://www.legaltorrents.com/bit/observatory-online-archives-vol-1.zip.torrent>

Lawrence Lessig – Free culture: <http://www.legaltorrents.com/bit/freeculture.zip.torrent>

The first of these was a collection of MP3 music files, and the second a book title.

Step 2

The next step was to install one of the erasure programs, use it to erase Internet and downloading activities with its default settings. Following this, the drive was imaged using dd on the Helix 1.6 Linux bootable CDROM, and MD5 hashes of both the source drive and image files were created and compared for consistency. If necessary, this image file was then examined using Autopsy (Sleuthkit 2005) to determine whether information had actually been permanently erased. The registry of the source machine was also examined to determine whether there were traces of BitTorrent activity still remaining.

Step 3

Repeat Step 2 using the image containing torrent software and torrent activity that was created in Step 1, but with a different erasure program.

All erasure software was run with its default settings. The reason for this was that the aim of this research was to determine what the programs themselves would erase. By altering settings from the default, the level of knowledge of the researcher would influence what activities the erasure tools removed.

RESULTS

R-Clean and Wipe

This program did not remove any traces of orrent activity from the test machine. The Internet files which contained links leading to the download site were deleted, but this was recoverable with Autopsy. The actual files downloaded and the torrent file itself which pointed to the downloaded files was also not erased (Figure 1). A search of the registry of this machine gave information relating to the exact files that were downloaded (Figure 2). In addition, the torrent files were still available in a hidden folder in documents and settings for the user.

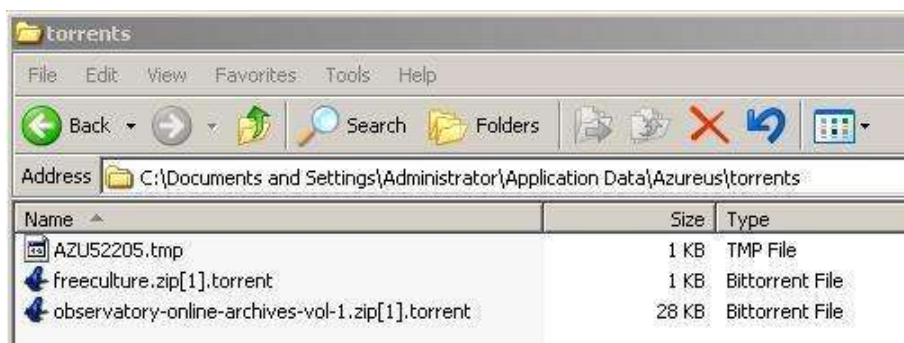


Figure 1 – The torrent file linked to the download still remained after “erasure”

Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	C:\Documents and Settings\Administrator\Desktop\Azureus_2.3.0.4_Win32....
b	REG_SZ	C:\Documents and Settings\Administrator\Desktop\rwc_en_40.exe
c	REG_SZ	C:\Program Files\Azureus\freeculture.zip
d	REG_SZ	C:\Program Files\Azureus\observatory-online-archives-vol-1.zip
e	REG_SZ	C:\Documents and Settings\Administrator\My Documents\My Pictures\rwipe ...
MRUList	REG_SZ	edcba

Figure 2: Evidence of the torrent activity was still found in the registry after using R-wipe and clean.

Window Washer

Whilst this program claims to remove evidence of P2P activity, it did not remove any evidence of the BitTorrent downloading. As with the previous software, R-wipe and clean, evidence still remained in both the files and in the registry of the test machine (Figure 3).

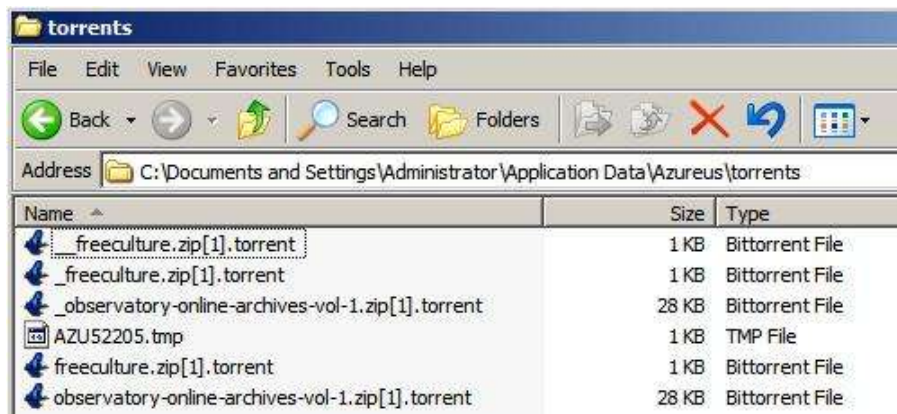


Figure 3: The torrent files used to download the test files were still found on the hard drive, without the need for forensic analysis

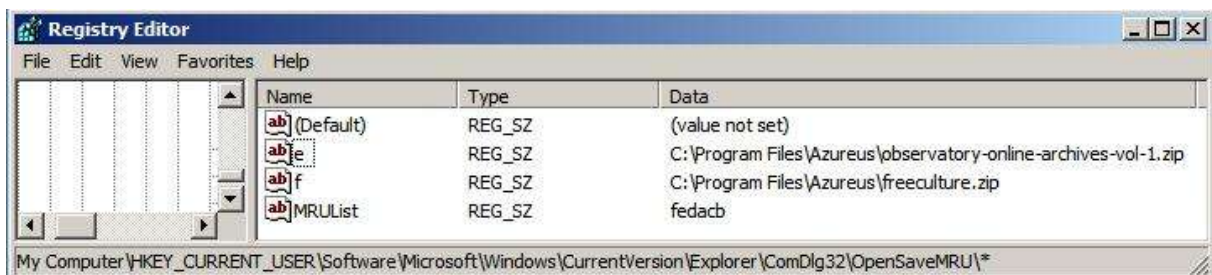


Figure 4: Evidence of torrent activity found in the registry after using Window Washer

Privacy Suite

Another package that listed removal of P2P activity on its web site, but did not remove all traces of torrent activity. Unlike the previous two packages, this program did remove evidence from the registry, but again did not remove the torrent files, or the downloaded files (Figure 5).

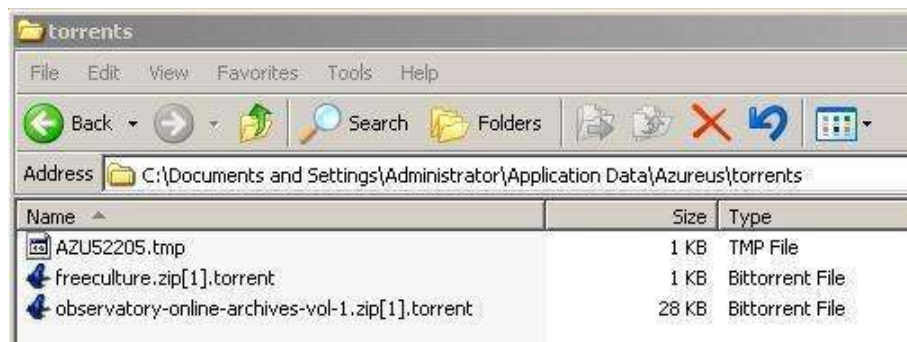


Figure 5: The program Privacy Suite did remove evidence from the registry, but did not remove the torrent files that were used to download the files.

CONCLUSION

This research in progress examined the effectiveness of three commercially available secure erasure programs in removing evidence of BitTorrent activities. All three programs were found deficient when it came to cleansing the PC of BitTorrent activity. Whilst forensic analysis was used with all programs, location of a simple file, and in two cases a simple keyword based registry search, revealed that the computer in question had been used to download files, and further, the names of these files were also recoverable. It is worth pointing out again that these programs were used with their default settings. It is likely that some of them may be configurable to remove traces of torrent activity. However, this would require in depth knowledge of where the files and traces of torrent activity reside on the machine. If a user already knows where this information is, then they would not be resorting to using an erasure program to remove it.

Further research is necessary to determine whether, with modification from the defaults, these programs can be made to remove evidence of torrent activity. There is also scope to examine other erasure software to determine its effectiveness in perform the same task. More in-depth examination of the hard drives using forensics analysis software to find out whether other evidence still exists will be a part of any further research.

REFERENCES:

- BBC (2000). *Napster closure threat*. Retrieved 5/9/05 from <http://news.bbc.co.uk/1/hi/business/789132.stm>
- BBC (2005). *File sharers move from Bit Torrent*. Retrieved 4/9/05 from <http://news.bbc.co.uk/1/hi/technology/4196642.stm>
- BitTorrent (2005). *What is BitTorrent?* Retrieved 4/9/05 from <http://www.bittorrent.com/introduction.html>
- Cyberscrub (2005). *Cyberscrub Privacy Suite 4 – New features*. Retrieved 15/9/05 from http://www.cyberscrub.com/products/privacysuite/features.php?n=new_features_text
- Ferguson, I. (2005). *Kazaa appeal likely in 2006*. Retrieved 9/9/05 from http://www.zdnet.com.au/news/software/soa/Kazaa_appeal_likely_in_2006/0,2000061733,39210189,00.htm
- Layman, J. (2005). *Legitimate use, open source, keep BitTorrent out of court*. Retrieved 5/9/05 from <http://trends.newsforge.com/article.pl?sid=05/03/02/1748210&tid=147&tid=132>
- Linspire (2005). *The worlds easiest desktop Linux*. Retrieved 9/9/05 from <http://www.linspire.com/>
- MetaMachine (2003). *eDonkey v1.4 – the most sophisticated file sharing technology available*. Retrieved 4/7/05 from <http://www.edonkey2000.com/index.html>
- Motion Picture Assiciation of America (2005). *Motion picture industry takes action against Rochester area internet thieves*. Retrieved 4/9/05 from http://www.mpa.org/MPAAPress/2005/2005_07_28.doc
- Rtt (2005). *Disk Cleaning and PC Privacy: R-wipe & clean*. Retrieved 14/09/2005 from <http://www.r-wipe.com/>
- SleuthKit (2005). *Autopsy forensic browser*. Retrieved 9/9/05 from <http://www.sleuthkit.org/autopsy/>
- Webroot (2005). *Window Washer*. Retrieved 14/9/2005 from http://www.webroot.com/consumer/products/windowwasher?rc=266&ac=383&wt.srch=1&wt.mc_id=383

COPYRIGHT

Andrew Woodward ©2005. The author/s assign the School of Computer and Information Science (SCIS) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCIS & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.