Do Current Erasure Programs Remove Evidence of BitTorrent Activity?

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

Craig Valli
School of Computer and Information Science, Edith Cowan University Australia

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Do Current Erasure Programs Remove Evidence of BitTorrent Activity?

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

Craig Valli
School of Computer and Information Science
Edith Cowan University
Australia
a.woodward@ecu.edu.au

ABSTRACT

This research in progress aims to evaluate the effectiveness of commercial programs to erase traces of the use of BitTorrent software. The erasure programs MaxErase, P2PDoctor, 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 then searched for torrent files. 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 MaxErase, P2PDoctor, Window Washer and Privacy Suite claimed to erase evidence of P2P activity, but 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

1. INTRODUCTION

The most common method of obtaining information in the form of multimedia files on the internet has been and continues to be through file sharing software (Karagiannis et al 2003), often referred to as P2P software. This type of software allows users to search for and obtain images, video files, software and music, be they legal or illicit. Music files, or MP3 as they are more commonly known, are of particular concern to some file sharers as various organisations seek to protect their intellectual property through legal action (Broucek and Turner 2004). In the case of illegal activity, individuals seek to remove evidence of their activities, and this is usually done through the use of commercial erasure software. Whilst these programs may remove the files themselves, and even evidence from internet browser programs, the introduction of third party software to perform the downloading creates other avenues for investigators to collect evidence. Use of file sharing software itself creates information in areas of the system, such as the registry and in user's hidden folders that these erasure programs may not be written to deal with (Woodward 2005). However, these tags that are left behind can give vital information to anyone interrogating a seized computer, possibly revealing what file was downloaded and when.

One form of file sharing software that has been around since 2001, known as BitTorrent, is now the most popular means of downloading files from the internet, with data from as far back as November 2004 showing BitTorrent accounting for 35% of all internet traffic (Pasick 2004). There is evidence that usage of this software is increasing in some countries, and is the dominant software for use to download material from the internet in others (BBC 2005). BitTorrent is similar to its contemporary P2P software 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. These fragments are normally stored as hashed segments on machines within the BitTorrent network. 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 such as the distribution of software.

Previous studies have examined commercial erasure tools to examine their effectiveness at removing traces of internet activity, and found that these programs still left traces of various activities (Jones and Meyler, 2004). While some of these software products claim to remove traces of P2P activity by programs such as E-donkey, another P2P file sharing system, it is unknown whether this software is effective at removing traces of BitTorrent activities. Five 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), MaxErase (Maxion Software, 2005), P2PDoctor (P2PDoctor, 2005) and Privacy Suite (CyberScrub, 2005). This research in progress paper examined the ability of these programs to remove evidence of torrent activity.

2. 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 not 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 overwrites 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.

(Webroot, 2005)

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 Gernerating 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.

(CyberScrub, 2005)

Max Eraser – Version 4.2

This product is created by Maxion Software and the following claims are made about its abilities in relation to P2P activity:

Peer to Peer History Eraser

Peer to peer Programs Supported:

- Kazaa Media Desktop
- Morpheus
- iMesh
- Bearshare
- Peer to Peer Histories erased
- Location Bar History
- Search history
- Cache files
- Cookies

(Maxion Software, 2005)

P2P Doctor – Version

This product is designed specifically to remove traces of P2P activity. The manufacturer, MadZ software, made the following claims:

MadZ P2P Doctor 2.0 removes all adware, spyware, popup ads, banner ads, and other third party software from the popular Peer To Peer (P2P) file sharing programs Kazaa Media Desktop, Morpheus, iMesh, Bearshare, Limewire, and Warez P2P without rendering the software unusable. In fact, P2P Doctor will scan your system for thousands of types adware, spyware, etc., and remove it if it is found. Now you can use these programs without the annoying third party software they install on your system. P2P Doctor also corrects any problems created in your Windows registry by this third party software.

Other features include a stealth option to protect against unauthorized access to P2P Doctor by third party applications that may try to disable it, a P2P history cleaner to remove all remnants of P2P activity from your system, a backup before remove option to allow you to restore items removed by P2P Doctor, and a built in download accelerator. This makes P2P searches faster and improves results. You even get automatic regular updates of P2P Doctor so you can keep your system cleaned of any new adware, spyware, or malware that may get added to the file sharing programs.

(P2PDoctor 2005)

3. METHODOLOGY

PC setup and Torrent Software

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.

Torrent files used for this research

In order to make sure that no intellectual property or copyright laws were violated, torrent files were obtained that are covered under the creative commons license. These are files can be freely downloaded and exchanged, so long as no fees or monies are charged.

Details of the files used to perform the BitTorrent downloads were 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.

Procedure

The first step was to install one of the erasure programs, use it to erase Internet and downloading activities with its default settings. Additionally, the files themselves were deleted and the recycle bin forensically erased. 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. The registry of the source machine was examined to determine whether there were traces of BitTorrent activity still remaining. The Windows search utility was used to search for the file names of the programs downloaded using Azureus to find information. It was set to look for hidden files and folders under the advanced settings.

At this point, the hard drive was securely erased, and the image containing torrent software and torrent activity was reinstalled on the PC, and a different erasure program was used. The examination process was also repeated.

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.

4. RESULTS

R-Clean and Wipe

This program did not remove any traces of torrent activity from the test machine. 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.
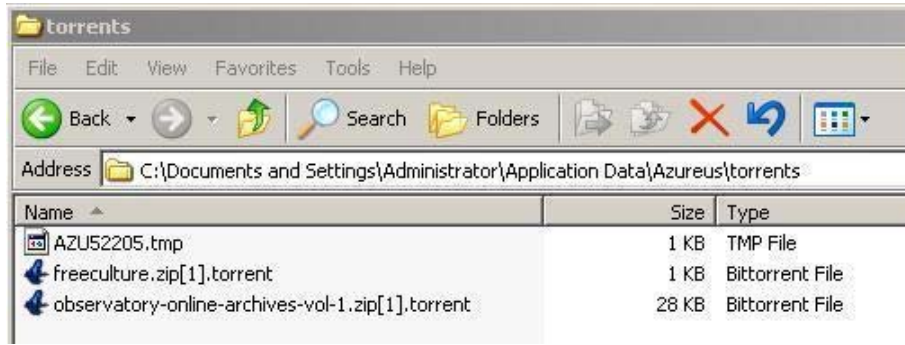
Figure 1 – The torrent file linked to the download still remained after "erasure"

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).
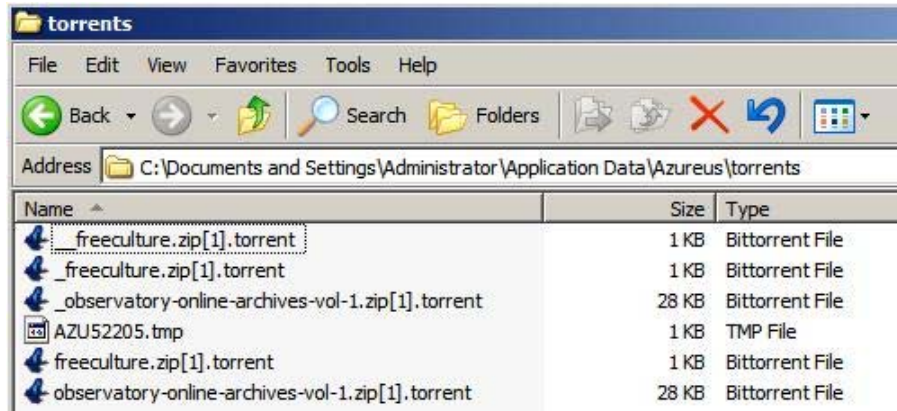

Figure 3: The torrent files used to download the test files were still found on the hard drive, without the need for forensic analysis
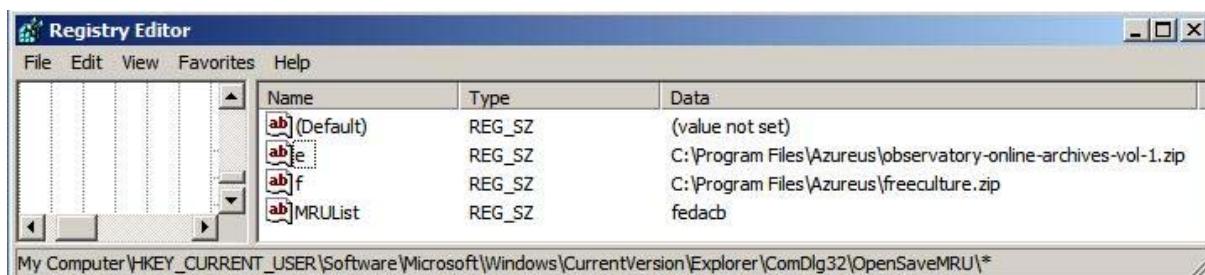
Figure 4: Evidence of torrent activity found in the registry after using Window Washer

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).
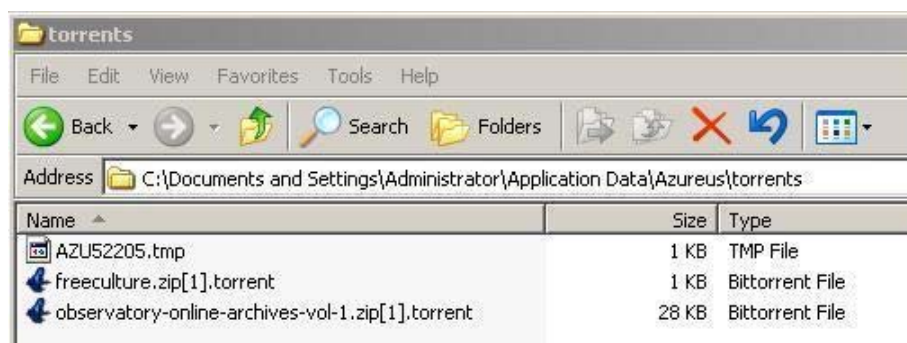

Figure 5: The program Privacy Suite did remove evidence from the registry, but did not remove the torrent files that were used to download the files.

MaxEraser

As for the previous program, Privacy Suite, this software removed the evidence of P2P activity from the registry, but not from the hidden Application data folder. Figure 6 Shows the files downloaded that still remained.
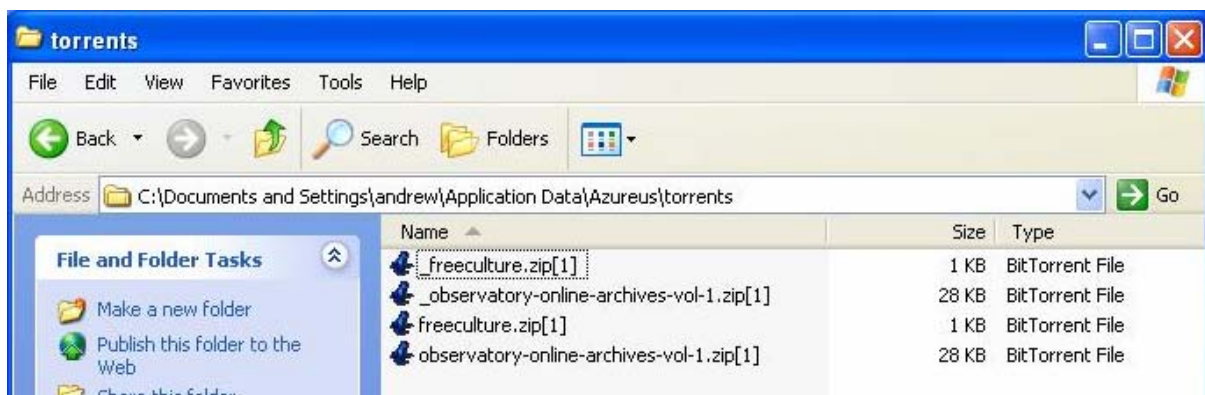

Figure 6: The program MaxEraser did not remove evidence of torrent activity from the Application Data folder

P2PDoctor

As with the previous two utilities, registry evidence was eliminated, but Application data folder torrent files were not (Figure 7). Of greater concern was that this program did not remove the web link that was used to locate and download the files used.

Figure 7: The erasure program P2PDoctor also left both the name of the file, and the web site from where the file was obtained in the Application Data folder

5. DISCUSSION

Removal of Torrent activity

This research in progress found that all five programs were deficient when it came to cleansing the PC of BitTorrent activity. Forensic analysis with Autopsy (SleuthKit 2005) was not deemed necessary as for 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. Further to this, 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.

The only other option open to a user who does not have the technical knowledge to locate these tags and remove them would be to securely erase an entire drive. A recent investigation by Valli and Patak (2005) has shown that the advent of larger hard drives has made this a very time consuming task, and not something that could be done with any expediency should the need arise. Even directed erasure of large Bittorrents such as CD or DVD image files would take several hours in some cases to erase beyond possible forensic recovery.

P2P Specific Programs

None of the programs which claimed to remove evidence of Torrent activity actually removed the torrent link created by Azureus. Of particular concern was that the program P2PDoctor did not even remove the link from where the torrent was obtained. Such information would greatly aid a forensic investigator by providing more information about a file that a user had deleted. It appears that while these programs have settings to remove P2P evidence, they only do so for particular programs, none of which are BitTorrent clients, and some of which have been closed down (Ferguson, 2005). For example, the program MaxEraser will remove evidence of files downloaded with the P2P programs as shown in Figure 8. The software P2PDoctor had a similar list of applications that it will erase. Further, these P2P applications that the programs claim to erase are based on earlier versions of file sharing software such as eDonkey and Kazaa. These programs, while still in use, are not as popular as the BitTorrent clients that now account for a significant amount of the total traffic on the internet (Pasick, 2004). It is surprising that these programs do not cater for BitTorrent applications as they have been in use since 2002 (Schiesel, 2004). They may be other considerations in relation to the functioning of these BitTorrent clients that makes effective removal difficult.

Figure 8: P2P Applications for which MaxEraser provides erasure facilities

Forensic Analysis

This investigation found sufficient evidence of torrent activity with basic searches. It would be interesting to find out what further information that the forensic analysis utility Autopsy would find. From experimentation, it appears likely that the information that is removed by these programs is simply deleted and not forensically erased and full recovery would be possible.

However, as previously indicated, recovery via forensic analysis software and techniques are moot as the erasure software is defective in the deletion of even a small number of files or registry keys relating to the BitTorrent activities. This research has tested a sparse scenario where a small amount of files have been downloaded onto the client. Forensic recovery techniques could be of some benefit in a typical use scenario where a user may have downloaded several hundred files as none of the erasure software did as specified. To effect proper erasure, at least 3 wipes of the drive area containing the file using a pseudo-random sequence would be needed. This level of erasure is most probably not undertaken by these tools and never will as many BitTorrents are CD or DVD image files that are 0.6 to 4GB in size. These larger sizes mean that a considerable amount of time to effect a forensic erasure would be needed even on today's high speed drive architectures such as SATA (Valli & Patak 2005).

6. CONCLUSION

Currently available internet erasure software, regardless of whether it claims to remove traces of P2P activity or not, does not do so completely. Simple searches of the registry and hard drives found evidence showing what files had been downloaded. Efficacy of different erasure software ranged from no removal of torrent file information, through to removal of some of the evidence. These programs do

not make a distinction between different types of P2P activity, leading to the difference in their erasure abilities.

Further research will be conducted to examine other erasure software to determine its effectiveness in performing the same task. Also, other BitTorrent download client software will be examined to determine what other information may or may not be left behind that could be found by forensics examiners and used as evidence. This research will be used to develop a framework or classification of current BitTorrent clients for use in forensics investigations. There is also scope to determine whether, with modification from the defaults, these programs can be made to remove evidence of torrent activity. 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.

7. REFERENCES:

BBC (2005). File sharers move from Bit Torrent. Retrieved 4/9/05 from http://news.bbc.co.uk/1/hi/technology/4196642.stm

Broucek, V. & Turner, P. (2004). *Computer incident investigations: e-forensic insights on evidence aquisition*. In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8) 18 pages. Copenhagen: EICAR e.V.

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_2006/0,2000061733,39 210189,00.htm

Jones, A. & Meyler, C. (2004). What evidence is left after disk cleaners? *Digital Investigation.* **1:** 183-188

Karagiannis, T., Broido, A., Brownlee, N., Cladffy, K. & Faloutsos, M. (2003). File sharing in the internet: A characterisation of P2P traffic in the backbone. Retrieved 28/1/06 from http://congo.postech.ac.kr/PAPER/MONITORING/IEEE/2003/2003_karagiannis.pdf

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/

Maxion Software (2005). *MaxEraser*. Retrieved 15/11/05 from http://www.maxionsoftware.com/maxeraser.html

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 Assicatioon of America (2005). *Motion picture industry takes action against Rochester area internet thieves*. Retrieved 4/9/05 from http://www.mpaa.org/MPAAPress/2005/2005_07_28.doc

P2PDoctor (2005). *P2PDoctor - Product Details*. Retrieved 4/11/05 from http://www.p2pdoctor.com/whatis.htm

Pasick, A. (2004). Livewire- File sharing network thrives beneath the radar. Retrieved 1/2/06 from http://in.tech.yahoo.com/041103/137/2ho4i.html

Rtt (2005). *Disk Cleaning and PC Privacy: R-wipe & clean*. Retrieved 14/09/2005 from http://www.r-wipe.com/

Schiesel, S. (2004). File Sharing's new face. Retrieved 12/12/05 from http://www.nytimes.com/2004/02/12/technology/circuits/12shar.html?ex=1391922000&en=da

75cefbee224928&ei=5007&partner=Wikipedia

SleuthKit (2005). *Autopsy forensic browser*. Retrieved 9/9/05 from http://www.sleuthkit.org/autopsy/

Valli,C. and P. Patak (2005) An Investigation Into The Efficiency Of Forensic Erasure Tools For Hard Disk Mechanisms, In *Proceedings of the 3rd Australian Computer, Network & Information Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia*, pp.108-114

Woodward, A. (2005). The effectiveness of commercial erasure programs on BitTorrent activity. In *Proceedings of the 3rd Australian Computer, Network & Information Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia*, pp.79-83

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