

Forensically Unrecoverable Hard Drive Data Destruction

Daniel G. James

Forensically Unrecoverable Hard Drive Data Destruction

Preface

You have probably heard someone make the statement, “once it is has been deleted it is gone forever!” This statement is simply just not true. Deleted files can actually be recovered if effort to do so is made shortly after deletion. Another common misconception is that formatting a data storage device will erase all data beyond recovery. This scenario is also not true. It is possible to restore partition tables on a drive and recover the entire contents! So, how can anyone be sure their data has been destroyed beyond recovery? The solution is overwriting the data with random or consecutive patterns. This can be done with a number of freeware and retail products.

Introduction

Data destruction is not a new concept as it has been practiced by the DoD (Department of Defense) for years. However, there are many people who still do not understand the personal risk involved when throwing out their used computers. It is estimated that 1,086,250,903 people worldwide use the Internet, which is a 200% increase in usage since the year 2000 (Internet World Stats, 2006). In today’s world it is common place to make purchases over the Internet or be involved in some form of online banking. Most users never stop to think that their credit card, bank account number, or social security number may be stored somewhere on their computer before they dispose of it at the local thrift shop, flea market, or family yard sale. Sure, there is a possibility that someone will purchase the computer and destroy the residual data. There is also an equal possibility that it could fall into the hands of a criminal looking to steal a persons identity.

So, how can data be protected? How about selecting all of the sensitive files and pressing the delete key? How about formatting the hard drive? The truth is that many people see these methods as a secure way to destroy their valuable data, but they are wrong (Munro, 2004)! It is very easy for even a novice user to recover some deleted files with freeware products available for download on the Internet. Formatting and using the recovery disks are effective deterrents for casual data snoops, but a determined hacker can dig into the guts of the hard drive and carve out old data. The magnetic surface of the hard drive has residual traces of the data, which, with perseverance and the right tools, can be recovered (Munro, 2004) (Spector, 2003) (Hines, 2005). The only secure ways to permanently destroy your unwanted data is to overwrite it or to physically destroy the hard drive to render it unusable (Hines, 2005).

The Concept of Data Wiping

Several definitions are essential to fully understand the concept of data destruction. The data destruction process is often referred to as “data wiping”, “data cleansing”, or “data scrubbing”. The goal of data wiping is simply to destroy all data on a given drive, beyond recovery. A hard drive stores data in a logical formation known as a cluster. These clusters are formed by several smaller data units known as sectors. A sector is the smallest addressable memory unit on a hard drive (Kozierok, 2001). Because it is the smallest addressable unit this will be the logical starting point of the drive wiping software. Overwriting is simply to record (new data) on top of already stored data, thus destroying the old data. This may sound like a daunting task, but it is easier than you think and can be done by novice computer users!

Disk Drive Technology

Hard disk drives are called by that name because they are not floppy (as in floppy disk drives). They are organized as a concentric stack of disks or "platters". Each platter has two surfaces (although in practice the outer surfaces on the top and bottom of the stack are often unused because of physical space considerations), and each has its own read/write head (which reads and writes data magnetically on the surface). The data is stored on concentric circles on the surfaces known as tracks. Corresponding tracks on all surfaces on a drive, when taken together, make up a cylinder. Since an individual data block is one sector of a track blocks can be addressed by specifying the cylinder, head and sector numbers of the block ("CHS"). A sector is the smallest addressable unit of storage space on a hard drive which holds 512 bytes of data (Koehler, 2002).

Since a sector is the smallest addressable unit on a hard drive the goal of permanently deleting data will logically start here. The sectors on a drive are each numbered 0 – n. The drive wiping software will start with the first sector on the drive and overwrite the data contained there with a random pattern of data. This is continued for every sector on the hard drive until the overwriting process has completely written over all data in every sector. Once this operation has completed it is referred to as a “single pass”. For government security usage, the US DoD 5220.22 specification dictates a drive (or file) must be over written with all binary ones, all binary zeros, and then random characters. This is repeated a minimum of three times. When repeated a certain number of times, the data is effectively removed from deepest recesses of the drive (Munro, 2004). With some drive wiping programs you can then go back over the drive

and “spot check” or search every sector of data to insure that the process worked effectively.

If you are still not convinced it worked you can use an imaging tool to make a forensic bit for bit image of the drive and then analyze the image with a hex editor. The hex editor will reveal if all sectors on the target hard drive have been successfully overwritten. If you chose to overwrite the data with all zeros then you should see them in the hex editor located in every sector of the hard drive.

Can Overwritten Data be Recovered?

It is possible to retrieve meaningful data from a hard drive that has been overwritten to DoD standards. However, the possibility is slight, and debate exists over what is considered “meaningful” data as well as what constitutes reasonable methods to retrieve it (Gutmann, 1996). “Meaningful data” is the term the DoD uses to differentiate between information that could cause harm and data that simply exists in its primitive state of iron particles and requires extensive and expensive recovery methods (Gutmann, 1996).

Magnetic force microscopy (MFM) photography is the most commonly cited technology capable of recovering data from a drive that has been overwritten to DoD standards (Ibid). This technique involves opening the hard drive and examining the platters with a magnetic force microscope, which is used in conjunction with a camera to produce pictures of the drive. MFM then scans the entire surface of the drive, moving from region to region, with each region yielding a picture (Whitehead, 2006).

With the proper equipment, this process seems feasible—until an investigation of the level of effort and expertise required to perform this highly specialized type of data

recovery is done. The process is complex, and any small error in interpretation can result in useless data. As there appear to be no documented and verified private-sector MFM recoveries of meaningful data, it is highly unlikely that it has been performed successfully in the private sector and therefore cannot be considered a threat. Therefore even a single pass overwrite of random data on every sector of a hard drive is the safest way to permanently destroy data beyond forensic recovery with the technology available at the time of this paper's writing.

Conclusion

Is data destruction something that computer owners and users should be concerned about? If a computer is used to record personal financial information or make online purchases, or store sensitive work related files the user should be very concerned about data wiping! Furthermore, if a company maintains records that contain personal identifier information about clients, patients, or customers they may be legally required by the Federal government to insure all data and records are destroyed beyond recovery at the end of life for the data storage device containing the records. For instance healthcare and insurance agencies among others are bound by the Health Insurance Portability and Accountability Act enacted by the Federal government in 1996. HIPAA mandates that due diligence be taken to remove sensitive data from computer disks before the disks are either transferred from one area to another or discarded (Hardwick, 2006). If an institution fails to comply with these federal regulations the company and perhaps individuals in management, depending on the severity of the situation, could be fined hundreds of thousands of dollars and also become the target of multiple civil law suits (HIPAA, 2002). In conclusion, whether a person is concerned for themselves or

places of business always take time to follow the safe and simple procedure of destroying old data before throwing out an old hard drive. There are a multitude of resources available on the Internet about this topic as well as free data wiping software. Take advantage of them and have the piece of mind and assurance that sensitive data is destroyed beyond recovery that only data wiping can offer!

References

- Gutmann, Peter, (July 22-25, 1996) *Secure Deletion of Data From Magnetic and Solid-State Memory*. Retrieved on November 1, 2006, from http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- Hardwick, Steve, (2006). *Secure Removal of Protected Health Information*. Retrieved on November 1, 2006, from http://www.hipaadvisory.com/tech/data_removal.htm
- Hines, Matt, (April 20, 2005). *Skeletons on Your Hard Drive*. Retrieved on November 1, 2006, from http://news.com.com/Skeletons+on+your+hard+drive/2100-1029_3-5676995.html?tag=st.num
- HIPAA Privacy and Security, (2002). *Examples of Privacy Violations from Health and Human Services*. Retrieved on November 8, 2006, from <http://er.hipaaps.com/examples.html>
- Internet World Stats (2006). *World Internet Usage and Population Statistics*. Retrieved November 2, 2006, from <http://www.internetworldstats.com/stats.htm>
- Koehler, Kenneth R., (2002). *Disk Geometry*. Retrieved on November 2, 2006, from <http://www.rwc.uc.edu/koehler/comath/42.html>
- Kozierok, Charles M., (April 17, 2001). *Sector Format and Structure*. Retrieved on November 2, 2006, from <http://www.pcguide.com/ref/hdd/geom/tracks.htm>
- Munro, Jay, (April 20, 2004). *Wipe Data from Old PC's for Good*. Retrieved November 3, 2006, from <http://www.pcmag.com/article2/0,1895,1838698,00.asp>

Spector, Lincoln, (April 30, 2003). *Answer Line: Wipe Your Drive Clean of All Its*

Sensitive Data. Retrieved November 3, 2006, from

<http://www.pcworld.com/article/id,110338-page,1/article.html>

Whitehead, Andrew, (2006) *Physical Data Recovery*. Retrieved on November 4, 2006,

from <http://free-backup.info/physical-data-recovery.html>