varese
SECURE LTD

Telephone. +44(0)1489 854131
Email. sales@varese-secure.co.uk
www.varese-secure.co.uk

Electronic Data - A Process of Elimination

Very few items have such high liability for owners as tape and hard disk storage media. Whether it is company secrets, personal information, medical information, credit card transactions or financial data, information is a hot commodity and the vast majority of it by far is stored on some type of magnetic media. One hard drive could contain more than $10 million in fines for a variety of privacy and ethics laws! Information that is critical to the operation of our infrastructure such as power, traffic and phone could be compromised by simple theft of an inoperable hard drive. Stolen personal information for sale is already a mega billion dollar industry.

If your job is to permanently dispose of data stored on tape or hard drives, how would you do it? The best place to start would be to understand how data is stored on hard drives and tape. 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). Hard disk drives are called by that name because they are rigid. They are organized as a concentric stack of disks or "platters" (Figure 1). 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 in concentric circles on the surfaces known as servo tracks. Corresponding servo 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)(James, 2006)(Figure 2).

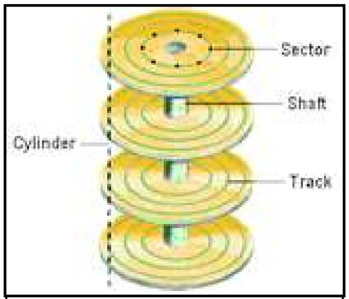

Figure 1. Hard Disk Platters

Early hard drives and tape had sectors that were laid end to end or “Longitudinal”. Later advances allowed manufacturers to stand sectors up or make them “Perpendicular”. As long as the components and above structure exist, there will be data available. This system has proved to be extremely robust.

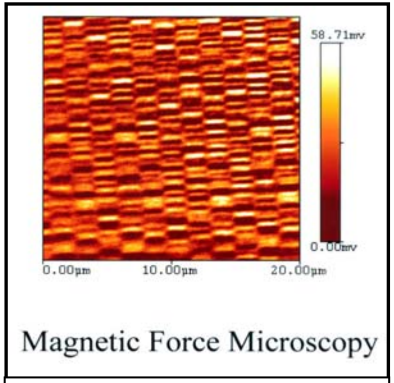

Figure 2. Close up of Sectors from MFM Imagery

Once data is stored with such organization it can be extremely difficult to remove or lose. While the typical computer user might have difficulty recovering lost or damaged data, commercial data recovery companies have established thriving businesses recovering “Lost” or damaged data. *Drivesavers* is one such company and their “Museum of Bizarre Disk-asters” is a veritable gold mine of information on the subject.

The need for storage of complicated files and high resolution images has steadily put pressure on manufacturers to expand the capacity of hard drive and tape. Despite the rapid technological advances in disk and tape storage, many users still utilize outdated modes of data elimination. There are many urban myths and legends about data destruction. File deletion, disk reformat, overwrite/Secure Erase and physical damage are the mainstays held over from the early days of the PC. Many see these methods as a secure way of destroying their high liability or sensitive data but with the exception of overwriting or Secure Erase, they are incorrect (Munro, 2004).

The first two ideas, deleting and reformatting are plausible to keep casual interlopers from viewing your data but a moderately experienced hacker can use free software to access the data easily. Overwriting or Secure Erase are better but not without built in flaws. The U.S. Department of Defense only authorizes clearing/overwriting for items within the same security level. A hard drive cannot contain overwritten "Top Secret" information and be used in an environment that only has authorization for "Secret" or below information (**DoD** 5220.22-M). This is a pretty discriminate regulation as far as data destruction is concerned. The reasoning is that the magnetic surface of the hard drive has residual traces of the data, which, with talent, time and the right tools, can be recovered (Munro, 2004) (Spector, 2003).

Overwriting and Secure Erase are also software based. Is there a line of code in the software that moves the supposed "overwritten" information somewhere else? How much time and wealth is spent on battling software viruses and could those viruses play a part in an over-write? Could there be back-door codes written into the hard drives for government forensics (It might not even be your government)? The disk drive has to be in perfect working order for overwriting or Secure Erase to take place. Is the drive capable of being overwritten? These are the questions that must be asked and answered. Many of them cannot be answered. Overwriting and Secure Erase work on functioning drives if one has the capability and is willing to spend hours and hours.

Many businesses and government agencies still drill holes or damage hard drives with a hammer before disposing of them. In addition to being a hazard to employees tasked with using a drill or hammer to damage a hard drive, the effectiveness in data elimination is marginal in most cases. Damaging the platters certainly makes recovering the data more difficult but as you can see from the above reference to *Drivesavers*, it can be and is often done.

There are two fool-proof ways to eliminate hard disk and tape data, incineration and degaussing. Incineration subjects magnetic media to over 2,000 degrees C which returns the magnetic field to zero and vaporizes much of the drive leaving only raw metals. In the United States, heavy incineration for metals and smelting operations have almost ceased for environmental reasons.

The one true solution is to degauss. A degausser applies a magnetic force far greater than the read/write heads to eliminate magnetic data. The degausser is not a new tool, it has evolved and kept up with the technological advances of magnetic media. It was used mostly in the early days to recycle expensive tape for re-use. The only non-destructive method for erasing "Top Secret" data is degaussing. Because of this, it has also withstood the test of time forensically. No government, corporation or individual has breached this form of disposal.

A degausser with sufficient strength and field orientation will eliminate all of the magnetic domains of the drive or tape resulting in a disk platter that is void of the deepest magnetic patterns, the servo tracks. However, all degaussers are not created equal and the strength of the degausser should not be judged on the highest power but the power that is maintained consistently within the degaussing chamber. Orientation of the drive or tape in relation to the path of the magnetic erasure field is also important. A drive passing inside of a directed magnetic field is going to have better erasure results than a drive passing over a magnetic field. The goal is to remove all of the data and as much of the underlying structure as possible from the hard drive or tape not just part of it (Figure 3).

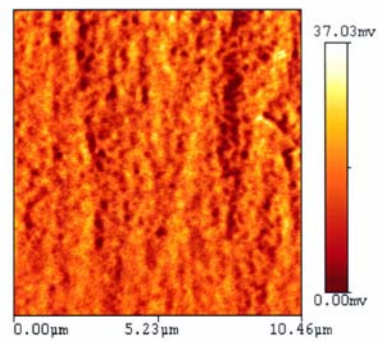

Figure 3. MFM Imagery of a degaussed drive.

The one drawback to degaussing hard drives and some of the newer data tapes is that the drive or tape is not reusable. Compared to hours long overwrite or Secure Erase sessions to re-use older drives, degaussing and replacing with a new drive is still far more cost effective. Also, computer hard drives do fail with great regularity and in the future the rate will increase as manufacturers lower pricing and computers enter the market in the $200.00 price range. Hard drive failures cannot be overwritten.

To conclude, the only sure way to avoid the liability of stored data, other than environmentally unfriendly incineration, is to eliminate it permanently by degaussing. All other forms of sanitation have serious security drawbacks with today's technology. Tomorrow's technology might relegate Secure Erase, certain types of destruction and overwriting to the level of what the "delete" and "format" is today. Only degaussing has withstood the test of time.

References:

James, Daniel, (2006). *Forensically Unrecoverable Hard Drive Data Destruction* Retrieved on August 4, 2009, from http://www.infosecwriters.com/text_resources/pdf/Hard_Drive_DJames.pdf

HIPAA Privacy and Security, (2002). *Examples of Privacy Violations from Health and Human Services*. Retrieved on July 28, 2009, from http://er.hipaaps.com/examples.html

Internet World Stats (2006). *World Internet Usage and Population Statistics*. Retrieved July 29, 2009, 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 August 4, 2009, from http://www.pcguide.com/ref/hdd/geom/tracks.htm

Munro, Jay, (April 20, 2004). *Wipe Data from Old PC's for Good.* Retrieved July 27, 2009from http://www.pcmag.com/article2/0,1895,1838698,00.asp Forensically Unrecoverable Hard Drive Data Destruction 9

Spector, Lincoln, (April 30, 2003). *Answer Line: Wipe Your Drive Clean of All Its Sensitive Data.* Retrieved August 4, 2009 from http://www.pcworld.com/article/id,110338-page,1/article.html

The following is information on how to get data back from a re-formatted drive from *RUNTIME.*

Runtime Software--A drive can be considered "dead", if it is not accessible by any software means, e.g. the BIOS, Windows' Disk Management or disk utilities such as Runtime Software's GetDataBack. A dead drive often shows additional symptoms. It does not spin or it "clicks" or it makes other kinds of strange noises.

Theses drives might have a damaged electronic board, damaged read heads, a damaged motor or damaged magnetic media. Data recovery companies with clean room facilities can often resurrect the drive by exchanging the damaged parts. They will then image the drive and perform a logical file reconstruction.

This approach is sometimes successful and then well worth the cost of several hundred or even thousands of dollars; however, sometimes it is not successful.

Data Recovery After Formatting In FAT, formatting a volume clears both file allocation tables and deletes the root directory. All data is still there, but you have lost:

- All entries in the root directory. Files can only be recovered as "lost files". Sub directories of the first level will have only numbers instead of their original name. Sub directories of deeper levels show their original name.
- The file allocation tables. This will cause the "fragmentation problem" as discussed in the chapter "Logical reconstruction with GetDataBack for FAT".

Within the limitations above, you will get a "fair" data recovery. Most files should be uncorrupted. You will need to look for your files in the numbered directories. Fragmented files, such as Outlook email files or databases, will be corrupted and probably unusable.

In NTFS, formatting a volume creates a new MFT. However, this affects only the first 25 or so entries. It usually does not touch the MFT entries of previous user files. That means you can expect a "good" data recovery. Almost all files should be correctly retrieved. Your results will be even better when you formatted a drive that was previously FAT-formatted with NTFS or vice versa. In this case the original FAT or MFT will probably not be damaged because these structures are located at different areas on the drive.