I need my data back, or someone else's!

Kevin Caldwell - The Computer Doctors

You've deleted a file and you've looked in your recycle bin – it isn't there. Emotions such as frustration and anger, and feelings of helplessness set in. But wait, it's still not deleted! Unbeknownst to most mere mortals of the IT world, lawyers included, there is often a way to get your data back.

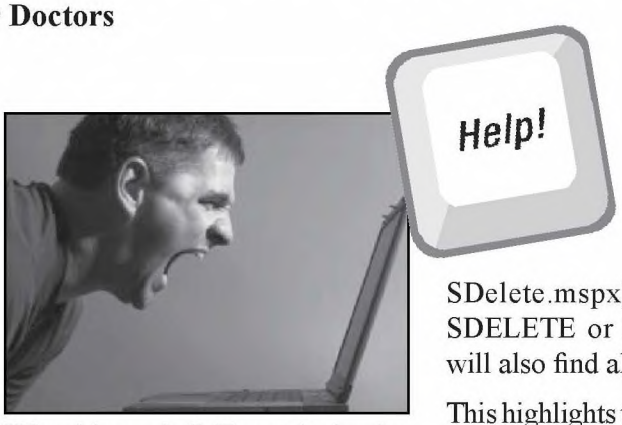
First port of call – backups

So, you've established that it isn't in the recycle bin, possibly because it has been deleted from a network drive off a server. This leaves you with backups as your first port of call. If you don't have a backup regime in place, this is the time you wished you had. Get one in place, quick smart. Types of backup include external hard drive, USB memory stick, DVD or burnt CDs, Internet/network based backup, or a tape backup.

If you do have a backup regime in place, restore it from your back up.

No backup?

All is not lost. If the data is stored on your local hard disk and it is not clicking or thudding, in most cases you can use an undelete utility to get your data back. The freeware Restoration.exe is downloadable from SnapFiles (http://www.snapfiles.com/get/restoration.html). There are more functional and easy to use commercial utilities such as Active@ Undelete, but Restoration is a great place to start. It is relatively easy to use, fast, free, and doesn't need to be installed – it can just be run once you download it. Other undelete utilities such as Active@ Partition Recovery will allow you to undelete whole partitions should your drive have been formatted.



Why this works? To put it simply, each file on your computer has a record like an address in an address book. When a file is deleted, the record in the address book says that space previously occupied by the file is now free space to be written to. It is only when another file is written, such as saving a document, that the space might be overwritten.

Undelete utilities sometimes can only retrieve parts of a file, because some of the space may have been overwritten. Using an undelete utility as soon as possible after the delete occurred is key to getting the data back.

It's good to know that this method usually works on USB memory sticks, MP3 players and memory cards commonly used in cameras and mobile phones.

"Confidentiality!" I hear you worry. Well, yes, it is a concern. If you dispose of a computer or other portable storage device which may have contained sensitive data, make sure it is sanitised first using a program that will destroy the data previously on the device. Good programs for this are BCWipe and GDISK. There are utilities to assist with secure file deletion (also known as file shredding) by file level such as SDELETE (http://www.microsoft.com/technet/sysinternals/Security/SDelete.mspx). If you Google SDELETE or File Shredder you will also find alternatives.

This highlights the need for security awareness. Portable storage devices such as laptops and USB memory sticks are most easily compromised. They can be easily lost or stolen, and if they have been used to view confidential documents or even email attachments that were deleted, they may be able to be undeleted. Internal policy surrounding the handling of sensitive data should mandate either not storing the sensitive data on portable devices or ensuring it is encrypted. You may find it worthwhile seeking professional advice on this subject.

Clean Lab Data Recovery – your last port of call. Even if your hard disk or storage device is physically damaged, there may be a chance of getting it back. There are companies in major capital cities that have specialised dust free clean rooms to open up hard drives, and carefully separate the components and retrieve the data off the disk platters. Get in touch with a local IT company first as this step is expensive and may not be necessary.

I hope that this article has cleared up misconceptions and opened your mind up to a whole world of possibilities with data recovery and forensic computing, including legal related processes such as electronic evidence and electronic discovery.