

Data Recovery Techniques and the Myths Surrounding Data Wiping Tools

Contributed by Webmaster

By Andrew Frowen

As the use of computer forensics in criminal investigations becomes more commonplace, news reports have made many ordinary computer users aware that deleting a file via the recycle bin does not truly destroy it. Nevertheless, understanding among the public about what constitutes an effective method for permanently deleting data is still poor. This article looks at two of these methods - formatting the hard drive and using data wiping tools - and dispels some of the myths surrounding their use.

Many people believe that the act of formatting a drive permanently wipes all the data contained on it. In fact, the purpose of formatting is to create a file system to manage data, and so all that is lost is the directory entries that index the data on the drive. While this renders data undiscoverable via the operating system, it does not delete or overwrite it. For this reason, most data on a formatted drive can be recovered.

Computer forensic recovery of data after formatting usually involves 'data carving', the act of looking for flags in the raw data which suggest the start and end of a block of data. When a block is identified, analysts then attempt to reassemble the information in between the blocks to make up a single file. Standard data structures can also be searched for. So, for example, if a computer forensics analyst had been asked to identify evidence of images on a formatted drive, they might search for a string of code that is common to all image files in order to narrow down their search. Data carving, which is also used in recovery programs such as 'Encase' and 'AccessData FTK', can prove very successful, so the majority of a drive's contents can usually be recovered.

Until recently, it was widely believed that it was necessary for a hard drive to be written over repeatedly with random binary data (ones and zeros) in order for the data to be permanently wiped. Now, however, it has been accepted that fully writing over the drive just once can render all data completely unrecoverable.

The main reason why experts previously believed that multiple overwrites were necessary is that the head (the part of the hard drive that writes the information) is not always precisely positioned, and so it was feared that the information would not be overwritten precisely enough, byte for byte. However, a study published in December 2008 by Wright, Kleiman and Sundhar revealed that after a single overwrite, there is only a 0.5% chance of successfully recovering a single byte of data and even less chance of recovering more than this. Given that a typical two page Word document has a file size of over 22,000 bytes, the danger of any significant data being recovered is quite negligible.

It seems therefore, that it is not necessary to perform multiple wipes, provided a sufficient method is used to overwrite the entire drive in the first instance, rather than simply formatting. This is, of course, great news for companies wishing to remove client sensitive data from computers before disposing of them, but not such good news for law enforcers tackling increasingly computer savvy criminals.

IntaForensics a BS EN ISO 9001:2000 registered firm providing Computer Forensics, Expert Witness, Mobile Phone Forensics, and Forensic Data Recovery to the Legal Sector, Police Forces, Local Authorities and Commercial organisations internationally. Visit [Computer Forensics](#) for further information.