

Why a normal delete is not sufficient

[lus mentis](#)

ABSTRACT: A normal "delete" command does not actually delete files at all. But even with more advanced "file wiping" utilities, some data may remain that is very useful for a forensic investigator. In particular, the magnetic properties of a hard disk can be exploited to recover data.

Paranoia?

It pays to be a little paranoid sometimes. Often the reason for paranoia, is a deeper anxiety over not having absolute information about a thing. Without absolute information, we are always acting somewhat in the dark. Where our personal privacy and security is at stake, a healthy imagination is a good thing. How often do we hear others stating their beliefs as fact (absolutes), which just a short time later, are seen to be far removed from the reality.

Not so long ago, simple system commands were held to be a "secure" method of file deletion. When these were found to offer very little "true" security, utilities became available that were able to overwrite the related disk sectors. It seemed that these would surely be foolproof ; but no ! Of these new deletion utilities, most were considered too weak for their use to be allowed within the UK Civil Service. The question occurs; why were they considered unacceptable for such use ?

The reason is, that the government are well aware of the weaknesses of such programs.

Areas of concern

There are three areas of particular concern.

1. When a file is written to a disk, it has a certain number of sectors or clusters allocated to it. The area of disk space provided, is always larger than the file itself. Deleting a file alone, leaves a space which can contain sensitive data. There are a number of ways in which this sensitive data can be deposited without a user knowing it.
2. It is in the nature of a computer, to always be updating one file or another. Every time a file is updated or "saved", new copies are created and written wherever there is sufficient space. Applications can create huge numbers of such files. When a file is eventually deleted, only the last image is accounted for. All other images appearing as free disk space, unseen, unsuspected. That is until a disk is viewed with the appropriate software; then is all is revealed. Even when partially overwritten, these files can make interesting reading !
3. As if the preceeding were not enough, applications also create "temporary" files as part of their normal execution. That these files are not so "temporary", can now be appreciated.

Precautions

Present file deletion programs, attempt to address the problem of "data remanence", with varying degrees of success. If you work within a graphical "windows" type environment, then these programs may offer little or no security at all. If you work within

a "DOS" environment, they can offer a lot. Much depends on their intended use. As a companion to programs like "PGP", they are excellent. Able to disappear all those "plaintext" files for ever. Great care needs to be exercised in this connection though !

- NEVER EVER "save" an edited plaintext file; use "save as" instead. All versions will then remain available for deletion.
- Choose a deletion program with the ability to perform multiple overwrites. If you wish to deter only casual snoopers, one overwrite may be sufficient. For those who require their disks to withstand the scrutiny of Police forensic services; three times should be the minimum. Those (civil libertarians) who are likely to come into conflict with their government, should overwrite at least six times.

These precautions should not be regarded as excessive. Some would say that there is no chance of recovering data that has been overwritten just once or twice. These individuals are without awareness, of the "true" extent to which "data remanence" has been investigated !

Magnetic media

Deletion by rewrite is never absolute; more of a sliding greyscale. Once magnetic media have been exposed to a structured magnetic field, it is in reality, very difficult to ever totally disguise the fact. This applies especially to present drive heads, and high coercivity media.

When a write function is carried out, magnetic domains are created by the millions for each bit that is written. There is a limit as to how great the write current can be, or adjacent data will be corrupted. Increasing the spacing between adjacent data bit representations, would lower the total capacity of the media. Modern high coercivity magnetic coatings allow much greater data densities, but are more difficult to magnetize.

Consequently, when a rewrite is carried out, a significant number of these tiny molecular domains remain in their original orientation. This orientation is never the exactly the same twice. The precise orientation of the domain would have been influenced by adjacent bit representations. Each precise orientation being individualized like a finger print. With each subsequent rewrite, less of these "permanent" domains remain, and so a molecular history is encoded by a scale of relative molecular domain numbers.

In an age where molecular polarity is such a vital area of science, it should come as no surprise that special techniques exist for it's determination. The obvious value of being able to recover data, is not lost to the intelligence and forensic services of any developed nation.

Governmental approach

So with a knowledge of what methods are available for the analysis of magnetic media, how do governments treat their own data ? In the UK, the Ministry Of Defense has it's own idea of what constitutes the declassifying of magnetic media; hard disks for example. They require that the surface of all hard disk platters be ground off, and the

dust securely stored for twelve years! The dust is still officially classified even after this period.

Things are little different in the United States. A US naval document entitled OPNAVINST 5239.1A states that disks that are "unclassified", can either have their surfaces sanded away, or dissolved by acid !!!

Who's paranoid !!!