Recovering Files From Unallocated Space

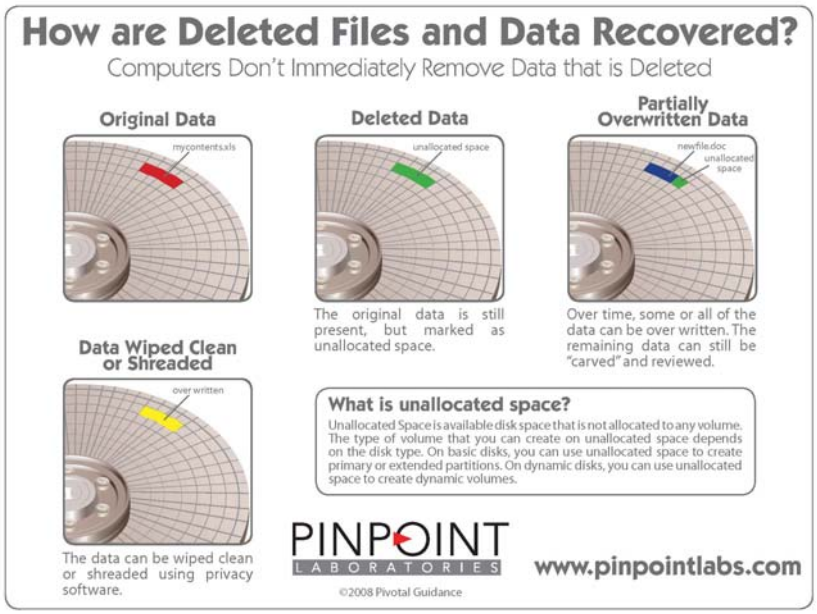
Posted By Jon Rowe On November 19, 2008 @ 11:58 am In Computer Investigations, Data Recovery, electronic discovery | No Comments

Recovering data from a hard drive is one of the most common tasks during a computer investigation. Here are a few of the artifacts which computer investigators may retrieve from unallocated (free) space to assist in a case:

* MS Office documents
* Acrobat files (.pdf)
* Email messages and attachments
* Images in various formats
* Internet history (pages visited, searches)
* Registry files (current and past)
* File access records (when and where files were opened)
* Pre-fetch files (when a specific program was ran)

Many cases revolve around correspondence, work products, whether or not files were stolen or manipulated, and to what length the suspect went to cover up his or her activities. A common misconception among attorneys and litigation support professionals is that all relevant data from a computer hard drive is recovered during electronic discovery processing. The truth is that off-the-shelf electronic discovery software doesn't index or search data that was deleted and resides in unallocated space. A considerable amount of valuable information is available on computer hard drives, but it resides in an area of the hard drive that may not have been collected from or was not searched during a typical electronic discovery project.

I don't believe that every project warrants a complete computer investigation. I just want to clarify that if the computers of certain individuals involved in a lawsuit require a more thorough analysis, then a forensic image or hard drive clone is required. In this case, a computer forensic investigator with the skills and appropriate software tools needs to be hired to search deleted items which aren't typically reviewed during the electronic discovery processing phase.



[1]

What is unallocated space? I have provided an illustration that helps show the different states for the physical area of a file, before it was deleted, and then once it is deleted, the different stages of retrieval possible from unallocated space.