Recovering deleted files (1 of 3)

Description

In my last post, I pointed out that in the case of the BTK killer in Kansas, investigators recovered a deleted Microsoft Office document that contained evidence crucial to the case. There are still many litigation support professionals who don't thoroughly understand what happens to files and user activity logs once the information is deleted or cleared and why it should be found or how it can be recovered. Recovering user activity, work product and correspondence could be crucial to winning your case.

The reason that a file or other data isn't visible, but can still be recovered is quite simple. If you delete a file, Microsoft Windows removes it from your view; however, at that same point in time, the contents of the file are still stored on your hard drive. In addition to removing the file from your view, Microsoft Windows "flags" the space where the file still resides, as "available". Depending on whether the space is needed for other filesand how much time has passed in the interim determines how much of the original content remains.

One of the primary differences between a computer forensic investigation and electronic discovery processing is the area of the hard drive that is being reviewed for potential evidence. Electronic discovery software will index and search the 'visible' or what is referred to as logical files (those still displayed to the user and available in Windows). Computer forensic investigations, on other hand, will review the current files and **also** the content contained in the deleted information. In order to search through deleted information, however, a forensic image or clone of the suspect media is required. I'll go into more detail in post (3 of 3).

Date
04/25/2025
Date Created
08/05/2008