Recovering deleted files

August 5th, 2008

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 files and 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.

It often comes as a shock to attorneys and their staff when they hear that electronic discovery processing doesn't automatically search the entire contents of a custodian's hard drive. So, it's worth stating again for emphasis here. Common electronic discovery applications used by service providers and law firms aren't designed to search the unallocated (swap, free, slack) hard drive space, which is where deleted files and other potentially relevant data will reside.

If you have custodians that need a thorough investigation you may need to dig deeper than the results that EED processing provides. If you suspect that specific custodians may have deleted files or user activity logs, or you need to analyze specific activity taking place on the custodians computer then you'll need to begin a computer forensic investigation to review the computers unallocated space.

I'm not recommending that every custodian hard drive and server willneed to be forensically imaged and analyzed. In fact, the majority of the files identified as being relevant to ESI (Electronically Stored Information) production can be processed and reviewed using off- the-shelf EED software. However, during the course of many cases, an individual or two can be identified as ‘suspects’, requiring a more thorough investigation of the activity on their desktop or laptop computers.

To recover deleted files, user activity logs, Internet history, and other potentially relevant custodian information, a ‘physical’ copy or forensic image of the hard drive or other media is required. Creating a physical copy or forensic image preserves the entire contents of the media, and makes it possible to recover deleted files, user activity and other potentially relevant artifacts. Several hardware and software products specifically designed to capture a physical copy or forensic image are available.

A computer forensic examiner needs access to the ’space’ between the visible files that contains deleted information. This space is referred to as unallocated (slack, free, swap) space and requires a physical copy or forensic image.

Copying files from Windows Explorer skips over the unallocated areas mentioned above. Make sure you request a clone or forensic image of any media where you believe deleted activity and file content might reside. Depending on what remains, your computer forensics examiner will be able to recover the deleted activity.