Resurrecting the Dead:
Recovering Wiped Files Using Windows Search

It's an electronic discovery nightmare. After months of fighting to gain access to the other side's ESI, you learn that the key evidence you've been hoping to find was deleted. Worse yet, the data was wiped—rendering it unrecoverable by normal forensic techniques. What can be done? If you're lucky, a handy little Microsoft feature called Windows Search could save the day.

I was recently involved in a case just like this. The user of the computer in question was fairly savvy with technology, and he wiped all documents, email, and other user files from his computer before handing it over for discovery. He made a giant mistake, though. He failed to wipe an innocuous looking file called "Windows.edb". This little file happened to be the key to the case.

So what is this "Windows.edb"? It is the core of Windows Search, a piece of Windows that allows you to search your entire computer instantly. Type in a word, and Windows Search will immediately show you every document, email, and media file that contain that term.

In order to make the search instantaneous, Windows works in the background to create a gigantic list of every user-generated file on your computer and the contents of that file. This gigantic list is called an "index", and it is stored in "Windows.edb". In essence, this one file contains the text of every single user file on your computer.

Even though our tech-savvy user had successfully wiped all his files from the computer, it was possible to rebuild almost everything from the "Windows.edb" file he had failed to delete. Using a special set of tools, over 50,000 documents and emails were extracted. Even better, the tools extracted metadata—timestamps, author information, and more.

When it comes to getting evidence from Windows Search, however, speed is of the essence. Windows Search continually re-examines your computer and updates "Windows.edb". When files and emails are deleted from the computer, they are eventually also removed from the index. Thus, if a computer is left in use, evidentiary gems maintained by Windows Search will simply vanish.

If you believe that key evidentiary information has been deleted from your ESI, don't panic—think preservation. If the computer is powered off, make sure it stays that way. If you have control of the computer, sequester it so that no one will be tempted to turn it on. If the computer is still in the hands of the other side, draft a preservation demand that dictates the machine may not be turned on.

Even after wiping, Windows Search might still contain critical evidence for your case. With proper preservation and the right tools, this evidence can be brought back to life.