TECH TRENDS: Disk Imaging

By Roy Atkinson

First, let's define *disk imaging*. Disk imaging produces a sector-by-sector copy of the original disk, keeping all the data intact. Backups often concentrate solely on user data and, therefore, don't capture all the information that exists on the original disk.

Why Image?

There are many reasons to image hard disk drives—surely as many reasons as there are organizations—but probably the most common one is to capture the data and configuration information from a computer as part of the process of hardware replacement. I could, for example, take an image of your current, aging laptop (which has been painfully upgraded to Windows 7), and put that image onto the drive of your spiffy new laptop. If all goes according to plan, your new laptop will function just the same way as your old one (only much faster, one hopes), with all of your shortcuts, dictionary entries, and half-completed projects intact.

Another reason would be to create a custom configuration for a group of computers, including all of the applications needed for a specific task, or for a specific department. We could, for example, create an image of a "sales department" computer with browser home pages set to Salesforce.com's login page, or "finance department" machines homed on the company's Oracle login, with all the data analysis tools already enabled in the new installation of Excel.

But there's another reason we don't like to talk about, and that is forensic analysis. Unfortunately, it sometimes becomes necessary to do a thorough examination of all the data on an individual's hard drive, whether we're engaged in a legal action or searching for evidence of a breach of company policy. In such cases, the forensic investigator, whether a law enforcement officer or a desktop support manager, should *never work on the original evidence.*[1]

Removable media, such as flash drives and SD cards, or optical media, such as CDs and DVDs, can be imaged as well, and moved to either physical or virtual disks. This can allow for easier backup and deployment of the contents of the disks. It's also possible to image optical disks to USB flash or SD media for easier distribution and use. As part of your department's marketing initiatives, for example, you may wish to distribute a video and some self-service information on flash drives. You could set up one drive just as you want it, and then copy that image to the drives you'll be giving away.

Finding the Right Tool

There is a variety of disk imaging software available for enterprises, for small businesses, and for personal use. Their capabilities may vary, but they all share the ability to make sector-by-sector copies of existing data. Use the HDI Buyer's Guide as the starting point for your disk imaging tool search.

[1] Madihah Mohd, "Section 5.1: An Overview of Disk Imaging Tool in Computer Forensics," SANS Institute (2001), www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643.