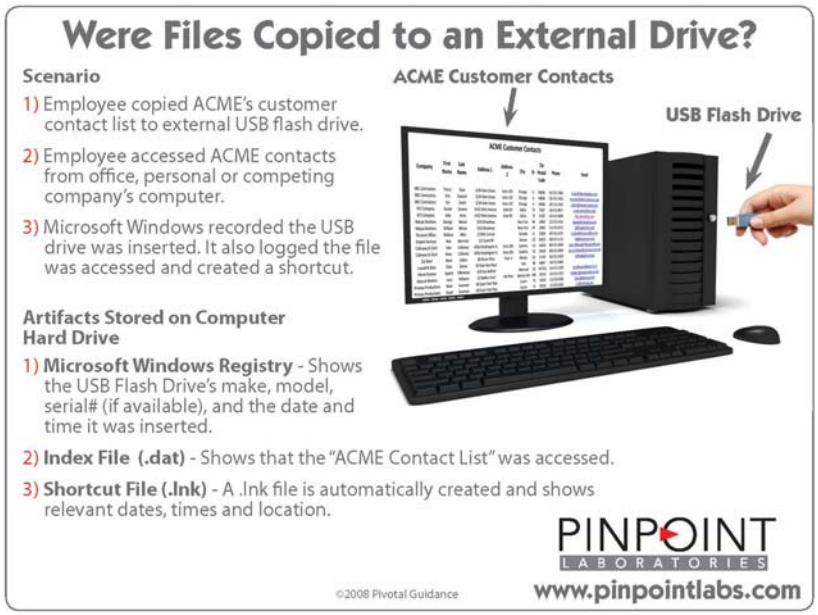
Secretly Copying Files To An External USB Drive

Posted By Jon Rowe On November 21, 2008 @ 10:41 pm In Collection, Computer Investigations, Data Recovery, Metadata, Software, Tips & Tricks, file recovery | No Comments

Copying corporate data and using it at a competing company (intellectual property/corporate asset theft) is a common and serious concern for companies and their legal counsel. When employees leave companies, there are often questions about the security of the information they previously accessed. Will they use the contacts, forms, or product details as a competitive advantage in their new job?

I had previously written about how to use the file activity records located in the index.dat file to identify when files were accessed. This can help determine if files were copied from a corporate file server. I want to expand on a couple of additional artifacts that can be used and then provide an illustration. There are three primary artifacts that can be used to help determine if someone accesses and copies specific files using an external drive, CD/DVD, flash device, or other storage media.



[1]

1) USBStor Registry Entry – Microsoft Windows uses its registry to track information about the computer's users, operating system, hardware, applications, security, and other relevant information. When USB devices are plugged into a computer, several key artifacts are captured including the make, model, serial number (if available), and when the device was plugged in.

2) Index.dat Access Record – Microsoft Windows uses the index.dat file to track website activity in Internet Explorer. It also contains when and from where files were accessed. We often have to recover deleted or purged activity using programs like NetAnalysis to do a thorough analysis. NetAnalysis can often recover hundreds of thousands of records that are no longer available in the index.dat files on the system.

3) Link File (.lnk shortcut) – Shortcuts can be created by a user and are commonly stored on the desktop. Microsoft Windows also automatically creates shortcuts for files that are accessed in .lnk files. These files store a wealth of information about the source document, including the path, date and time created, written, last accessed, size, volume serial, and several others. This information is encoded and requires special software to display it in a format that is useful.

By using the above artifacts, it is possible to determine that files located on a company server or client machine were copied or accessed after a specific date and time. Note that this doesn't provide the contents of the file and a thorough review would be necessary to make sure it is the same file. However, if the file name and other relevant metadata is a match, it does appear suspicious and may be enough to construct a solid argument that the employee did copy or burn files, access the contents, or used the information. This may lead to criminal and civil charges around possibly benefiting a future employer or a new company that the employee decided to start.