Metadata Analysis - “Fabricated” Documents

September 16th, 2008

One of the common requests we receive is to help a client determine when a document was created, or if it existed at a specific date and time, and when it was last modified. For example, an employment dispute may involve one of the following circumstances:

1. A memo was handed to an employee during a meeting but the employee denies s/he received the document. The document is presented but it is believed to have been created after the fact. Could the document have existed at the time of the meeting?
2. An employee produces a document that s/he claims was received from the manager, but management denies the allegations. Did the employee create the file? Can metadata provide any answers?
3. Bob, the sales manager for Acme Widgets Inc., was working for a competitor during his employment. How long did this go on? What does the metadata of the recovered files tell us? Can it help us track down files he potentially stole from the company?

Here are a few facts that should help to clear up many similar questions:

1. All metadata and timestamps can be altered. Don’t base your case on the ‘Date Created’ field of a Microsoft Word document alone. Free utilities can be downloaded that can alter this and other metadata fields.
2. If metadata was altered, it may conflict with other metadata or timestamps within the file, and such discrepancies could raise a strong suspicion.
3. Analysis of other areas of the computer that could support or deny a claim is often required. For example, in Microsoft Windows, the index.dat files contain records of when the user opens a document. Recovering and analyzing the file access activity in the index.dat could help support claims or metadata (file access dates/times) that suggests the file was created or revised at a specific date and time.

Feel free to download the Pinpoint Labs MetaViewer or MetaDiscoversoftware and review the ‘No-Nonsense Metadata’ white paper. If you need assistance with an investigation, please email examiner@pinpointlabs.com.