What are File Headers? (Signatures)

August 12th, 2008

Many file types can be identified by using what's known as a file header. A file header is a 'signature' placed at the beginning of a file, so the operating system and other software know what to do with the following contents.

Many electronic discovery applications will use the file header as a means to verify file types. The common fear is if a custodian changes a files extension or the file wasn't named using an applications default naming convention, that file will be missed during electronic discovery processing. For example, if I create a Microsoft Word document and name it 'myfile.001', instead of 'myfile.doc' and then attempt to locate all Microsoft Word files at a later date, I would miss the file if I were looking for all files ending in '.doc'. There are specific file extensions associated with the native application.

During a computer forensic investigation file headers are extremely valuable because they allow us to locate the contents of deleted files, user activity logs, registry entries, and other relevant artifacts. For example, if I'm investigating a custodian hard drive for evidence that they were working for a competing company I would want to recover their file activity records. A large number of custodian activity records are often already purged or deleted. By scanning a computers hard drive for the signature related to user activity records we often recover relevant artifacts (file access records) up to several years after they were deleted.