PINPOINT
LABORATORIES

No-Nonsense Metadata Strategies

Extract, view and identify additional evidence hidden in Microsoft Office metadata

By Jon Rowe, CCE
Certified Computer Examiner
President

Pinpoint Labs
Jon.rowe@pinpointlabs.com
www.pinpointlabs.com

Microsoft Office metadata is routinely reviewed to identify additional evidence and establish document timelines. Whether or not document creation times are fabricated and to what extent documents existed at a specific date a time is a pivotal determinant in many cases.

It's imperative to understand metadata fundamentals related to your firms everyday use. First, you should be aware that all metadata and file timestamps can be altered. This doesn't reduce their importance but requires due diligence to use other sources if needed to confirm whether a file existed or was edited by an individual.

What is Metadata?

Metadata is often defined as 'data about data'. In other words metadata located in Microsoft Office files provides details related to the creation, modification and previous locations. Track changes, document version; privacy information and a number of other attributes is also referred to as metadata.

Microsoft Office files are potential evidence and the timeline of events as well as what happen to the files is important information. Your ability to properly harvest and interpret metadata can mean the difference in winning or losing a case.

Metadata vs. File Timestamps

Before we discuss Microsoft Office metadata it's important to understand there is also file system metadata associated with Microsoft Office documents.

File system metadata which is often referred to as 'timestamps' is independent of the Microsoft Office metadata and is stored in the FAT (File Allocation Table) which is similar to a table of contents for the operating system (i.e. .Microsoft Windows).

When computer files are copied from a custodian computer to another location during a document production file system metadata is often altered. In our last report, No-Nonsense File Collections, we cover how files can be safely copied without altering metadata or file timestamps.

Each Microsoft Office file has two sets of relevant dates. The metadata contained in the file which is created and altered when using Microsoft Office. Generally, these dates are more reliable because file system metadata or timestamps can be easily altered by:

1) Copying to a new location
2) Indexing software
3) Virus scanners
4) Mousing over the file in Windows
5) Burning files to a CD or DVD

Incomplete Search Results

While specifying date range searches extracted from electronic discovery software or provided by a vendor make sure you are using dates from within the file whenever possible. Why? Because many existing processes use file system timestamps which are easily modified and often aren't true to original created date or last accessed time. Incomplete evidence results are a result of using the wrong date field.

MetaDiscover from Pinpoint Labs is a great tool which allows users to quickly extract Microsoft Office metadata. Use MetaDiscover to insure you have access to internal file properties that are relevant to your case.

Where Is the Evidence?

There is a little known secret that can be used to better identify the computers and file shares a custodian accessed. Currently, attorneys who represent the producing party work with their clients and consultants to identify all information relevant to a production request. Unintentionally, relevant computers, backups and file shares are missed due to the lack of current information available.

Using key metadata referred to as 'Last 10 Authors and Locations' which is available in Microsoft Word files can often shed light on additional data sources. Because this information isn't readily available most electronic discovery processes skip it. It may also be identified as privileged information.

MetaDiscover currently helps users display, redact or batch extract Last 10 Authors and Locations from Microsoft Office documents. This information has helped uncover key evidence in many cases.

When was the File Created?

Many cases involve authenticating the created, modified or accessed times of a specific file. Did the commission report exist before an employee was terminated? Was an employee notified of a specific policy or procedure?

These are the kinds of questions attorneys face everyday. As stated earlier it's important to preserve metadata and have access to the most accurate information available. It's equally important to understand metadata can be altered. Using metadata for electronic discovery review where the existing dates and times are accepted is expected.

This article wasn't written to create paranoia or have you question the metadata of all files. Make sure, however, you are harvesting all relevant metadata during processing. Also be mindful that when individual files are investigated its important to remember that experts will argue the metadata of the files in questions can easily be altered – which is true. It may be necessary to examine computer logs, email and other information which can confirm or deny the metadata in question. If you need assistance with a computer investigation the CCE's (Certified Computer Examiners) at Pinpoint Labs can help.

Summary

Microsoft Office metadata plays an important role in both electronic discovery and computer investigations. It's important to understand:

1) There are two sets of timestamps for Microsoft Office files
2) File system (Windows) timestamps are easily altered by many common user actions
3) Microsoft Office metadata timestamps are considered a more reliable source than file system timestamps
4) Many electronic discovery processes don't include all relevant and available metadata
5) Metadata is easily altered
6) If you determine client files should be scrubbed to remove confidential information make sure you discuss with all parties first
7) Last 10 Authors and Locations can provide additional evidence sources

Preserving file metadata and timestamps throughout ESI (Electronically Stored Information) productions is important. Using tools which reveal additional metadata or provide the ability to scrub confidential information will insure your investigations are thorough and protect your clients from producing privileged and confidential information.

Free MetaDiscover Evaluation
(http://www.pinpointlabs.com/software/metadiscover/)

Free SafeCopy Evaluation
(http://www.pinpointlabs.com/software/safecopy2me/)

About Pinpoint Labs
Pinpoint Labs was founded by Jon Rowe and James Beasley, who are Certified Computer Examiners and members of The International Society of Forensic Computer Examiners. Their experience includes 15 years of litigation support and more than two decades in software development.