Legility

Case Study

Digital Forensics – Using Metadata to Prove a Case

Challenge

Forensically collect and investigate digital files for a complex employment case with noncompete covenants and trade secrets at stake.

Solution

Legility's detailed forensic analysis of data and its metadata produced the "smoking gun" – metadata properties revealing points of origin and information about file transfers and revisions. This critical evidence was used in court, and verified by Legility's expert witness, to help win the case.

> **We helped develop a forensic protocol to outline what information would be collected, how to ensure it was done correctly and how to make sure privileged information would not be exposed accidentally.**

By definition, metadata is data about data. For computer files, it includes file name, file type, date last opened, date last edited and more. In addition to that kind of file information, which most people can see, there are many more metadata fields that are hidden to typical users. When a file is created or revised, details may be embedded about who created or changed the document, when, on what computer, at what company, what was changed and more. This information can be valuable for a court case, and it goes beyond standard electronic discovery data collection: it must be gathered and analyzed by a digital forensics specialist.

Background

In this case, a health company acquired another health company, creating Company A. After the acquisition was complete, some employees from the acquired company left Company A to start a competitor, Company B. Company A sued Company B for taking trade secrets and proprietary documents to their new company and using it against Company A. The companies compete on an employee level as well, and the plaintiff, Company A, accused Company B of poaching employees who would take with them stolen customer lists, contracts and more.

Company A sought $8 million in damages for the loss of reputation and data. Thanks to Legility's investigation into the metadata, they were awarded $7 million, including attorneys' fees and expenses.

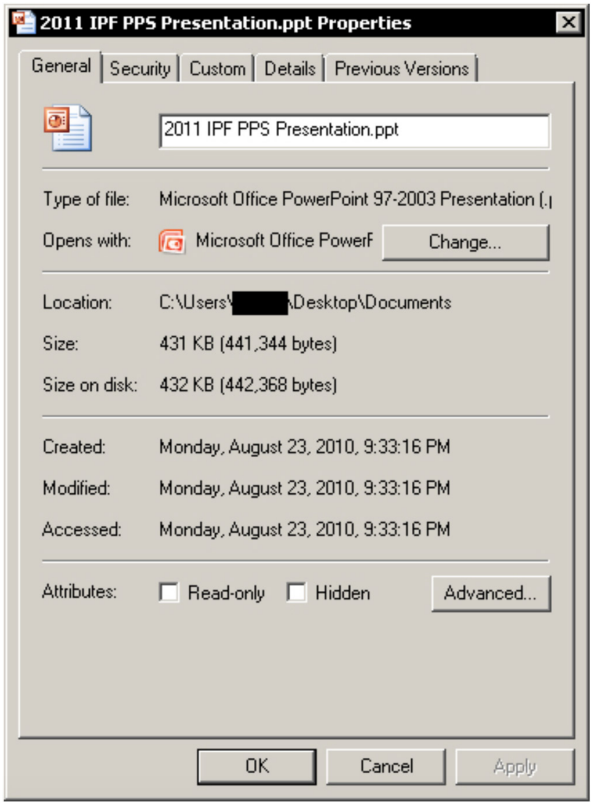
Collection & Analysis

The plaintiff did not have faith that the defendants would perform collections in a reasonable manner so the court approved access to the defendants' computers. Legility helped develop a forensic protocol to outline what information would be collected, how to ensure it was done correctly and how to make sure privileged information would not be exposed accidentally.

Legility sent a forensic evidence specialist across the country to collect data from four defendants' corporate and personal devices, including their phones, laptops and desktop computers. The data was brought back to Legility for in-depth analysis.

The forensic investigation began with a general look at the data and a goal of proving that certain files originated with Company A. Legility created file listings of everything on the devices, including emails, communications, Internet history, fileshare sites, connections/removals of other media (flash drives, etc.), and more.

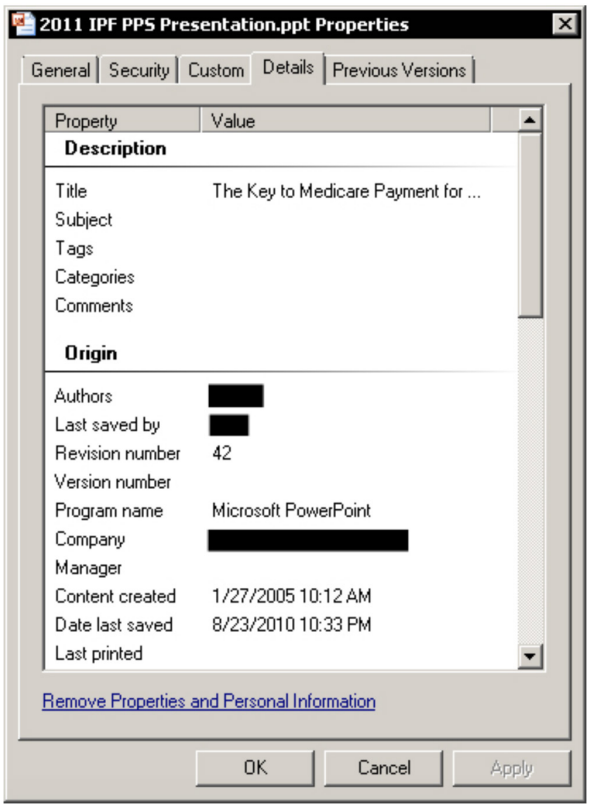
As Legility's forensic analysts drilled down into the data, they found proof of what was taken, copied, transferred, deleted and when. The image at right shows what kind of metadata is viewable to any user (confidential information has been blacked out).



Collection & Analytics, cont'd

At the same time, the collected data was loaded into Legility's web-based review platform so attorneys could screen for privilege and request forensic analysis of specific documents, which were mostly Microsoft Office documents and emails. For example, one defendant's computer had a folder called "noncompete." Another defendant had a folder explicitly labeled "documents from Company A."

Legility looked at the point of origin for relevant files, and this analysis showed files that definitively originated at Company A. The image at right is an example of the metadata Legility was able to see (confidential information has been blacked out). Legility's investigation also revealed that Company B was using proprietary formulas from Company A on Excel spreadsheets. Additionally, Legility found strong circumstantial evidence of file transfers through thumb drives and record of a mass copy on one defendant's computer.



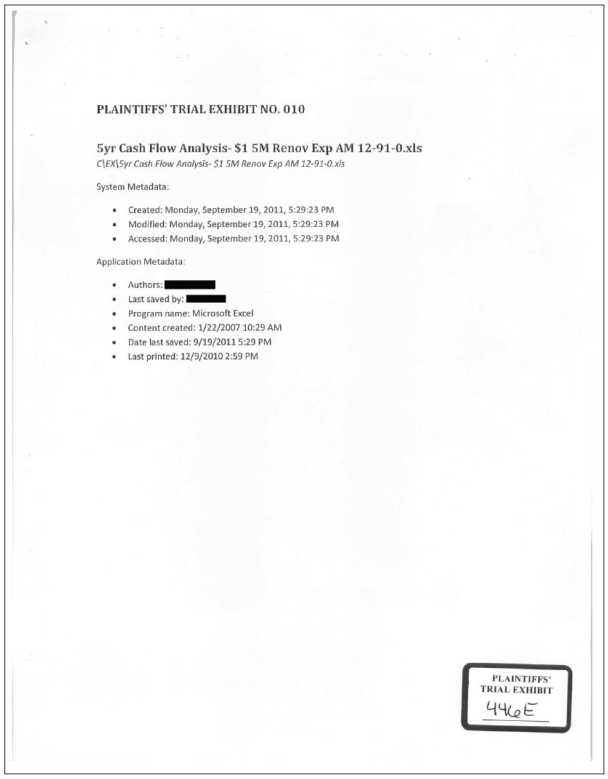
Deleted files also have metadata, and in this case, Legility found documents that the defendants said they did not have on their computers. One defendant had a second computer that he did not initially turn over for collection. His first computer showed backups of the second computer even though the files were deleted from the first computer he provided for collection. The second computer was shipped to Legility to copy and analyze.

Trial

Legility prepared a report on their findings, and a Legility digital forensics analyst testified at the end of the trial. Using the metadata, he showed when, where and by whom documents were created and when and by whom they were last saved. For example, he was able to prove that one document that originated from Company A's server was emailed as an attachment between defendants. The end result was a rebranded version of a proprietary document from Company A. Legility's expert compared the documents from Company A and Company B and explained the metadata to prove the documents were copied.

Trial, cont'd

Legility's forensic analyst also laid out dates to show intent since metadata logs who accessed which documents and when they did so. As a critical witness, Legility's expert testimony included the authors, revisions, who made those changes and when, and the original author, changing the direction of the case and helping with damages.



PLAINTIFFS' TRIAL EXHIBIT NO. 010

5yr Cash Flow Analysis- $1 5M Renov Exp AM 12-91-0.xls

C\EX\5yr Cash Flow Analysis- $1 5M Renov Exp AM 12-91-0.xls

System Metadata:

- Created: Monday, September 19, 2011, 5:29:23 PM
- Modified: Monday, September 19, 2011, 5:29:23 PM
- Accessed: Monday, September 19, 2011, 5:29:23 PM

Application Metadata:

- Authors: [redacted]
- Last saved by: [redacted]
- Program name: Microsoft Excel
- Content created: 1/22/2007 10:29 AM
- Date last saved: 9/19/2011 5:29 PM
- Last printed: 12/9/2010 2:59 PM

PLAINTIFFS' TRIAL EXHIBIT 446E

Conclusion

It's important to note that not every case involving metadata will uncover several smoking guns as this one did. In this case, the metadata proved that the defendants took contact lists, accounting spreadsheets with proprietary formulas, organizational documents and brochures and pamphlets with advertising copy. In addition to taking the proprietary information, the defendants were charged with violating their non-compete agreements.

It is possible to change some of the metadata, such as the title, subject and authors, but the metadata critical to this case, including the date created and computer used to create it, cannot be changed.

The eDiscovery portion of this case was relatively small compared to the digital forensics project involving metadata. Legility's forensic protocol was critical in getting access to the defendants' data. The collection and review phases provided the data that the forensics team needed to uncover the metadata. Through each step of the process, Legility's procedures preserve chain of custody, ensure security and maintain defensibility.

Metadata is being used more and more often in trial. Having at least one certified forensics member on an eDiscovery team is important for these kinds of cases in order to analyze and use metadata in a defensible and forensically sound manner. Legility can perform traditional eDiscovery work from collection through review, including conducting forensic investigations. This digital forensics component can yield significant and compelling evidence, and it ensures a thorough eDiscovery process.

Legility Team

Legility is the independent, global new law company.

We're here to do the best legal work of our lives alongside our innovator clients.

We deliver transformative legal solutions that build business value and set our clients apart. Our global network comprises 20+ offices & 1,500 people, and our legal operations work spans every industry and practice area. We have world-class data, strategy, and talent operations. But everyone and everything is driven by our core values:

- Do the Right Thing.
- Fabled Service.
- Diversity is in our DNA.
- Passion for Innovation.