

To Cache A Thief

How litigants and lawyers tamper with electronic evidence and why they get caught.

By Eric Friedberg

WHEN I WAS A FEDERAL PROSECUTOR, AN ingenious inmate attempted to break out of prison. Rather than use bed sheet ropes, this would-be escapee employed a fax machine. He had a confederate fax to the prison a forged order reducing his sentence to time served. The plan failed only because of poor research. Among other things, the order did not bear the correct originating fax number, and the type was in an unfamiliar font. For these failures, our less-than-fastidious forger was rewarded with several more years for attempted escape.

His forgery was attempted with a fax. These days, the tool of choice is more often an electronic document or an e-mail. As a partner in a computer forensics and investigations firm, I am increasingly exposed to how clients and lawyers fabricate or alter electronic documents and e-mails in an attempt to gain an advantage in civil and criminal matters. Luckily, there are ways of testing the authenticity of an electronic document or e-mail.

Temptation lurks in the Windows operating system. Most notably, Windows doesn't keep track of a user's changes to a computer's clock. Thus, a user can turn the computer's clock back to 1995, draft and save a Word document, then reset the clock to 2003. In Word, the properties of that document—available by selecting the Files/Properties menu item—would note that it was created in 1995. This deceit is only Windows-deep. Computer forensics experts can discover the actual creation date of a document by delving more deeply into the provenance of the file.

Our firm has seen electronic backdating in a number of cases.

In one, a defendant fabricated and backdated to 1999 a Word document to serve as contemporaneous "proof" of critical oral conversations that he claimed to have had that year. This defendant's lawyers, however, were shrewd enough to test the authenticity of the documents before relying on them in court.

In another case, a defendant sought to improve on the text of an e-mail received from a manufacturing partner, adding confirmatory language to the sender's text so that there would be no statute of frauds issue. E-mail programs have a high degree of security, so it's virtually impossible to modify a piece of mail in an in-box or Sent Items folder. Undeterred, this defendant pasted the text of an e-mail into a Word document, altered the text to his advantage, and then printed the altered text so that it looked like an original e-mail.

The sender, however, had the original on a backup tape, and the manipulation of the e-mail left electronic traces on the forger's computer. When his wrongdoing was uncovered, the forger's attorney dismissed his multimillion-dollar lawsuit with prejudice. Worse yet, because the forger had sworn in an affidavit to the authenticity of his version of the e-mail, the court referred the matter to the U.S. attorney's office for investigation.

Sadly, lawyers, not just litigants, are altering electronic documents. In one instance, a lawyer claimed that before trial he warned his client that he had a potential conflict of interest. In support of his claim, the lawyer proffered to the court contemporaneous electronic time records reflecting that warning. A forensic examination of the lawyer's handheld computer uncovered original copies of his time records that made no reference to the supposed warnings. The same exam identified the exact day that the lawyer altered the entries.

Computer forensics is a complex field, but there are a few basic clues that are left in the wake of electronic document tampering. Here are some of them:

When an electronic document or e-mail is viewed or edited on a computer, the viewed file is often cached, or copied, to a portion of the hard drive called unallocated free space. Forensic tools are capable of finding fragments of this cached material in that space. In the statute of frauds case, many versions of the document were found. As the forger tinkered with the wording of the forged document, he was unknowingly delivering these intermediate versions to his hard drive, where they could later be uncovered.

The authenticity of a document's date can be tested by

examining where it is physically stored on the hard drive. Data is stored in concentric tracks on a hard drive. The tracks are separated into sectors numbered consecutively. Generally, data is written first on low-numbered sectors and then higher-numbered sectors. Under normal circumstances, data saved to a hard drive at similar times will be located in the same general physical area of the drive. An authentic 1999 document should be located in the same disk space with other 1999 documents. But if it rests with 2003 documents, it could be an indication that the user has reset the clock and created a backdated document.

Document tamperers are not normally computer forensic experts. Typically, they are people with tremendous motivation to gain an advantage and low-to-medium computer skills. In the backdating case, the defendant attempted to cover his tracks by using a system performance utility called "disk defragmentation."

A little background is in order: A disk becomes fragmented when, as it fills up, the computer is unable to store new files in contiguous sectors. Instead, parts of files are scattered here and there in faraway sectors. Once there are enough "fragmented" files, computer performance deteriorates.

In the defragmentation process, the computer regroups active files onto contiguous sectors. Defragmentation overwrites unallocated space with active files. Fraudsters use the defragmentation process in the hope that this overwriting process will cover up clues that might reveal their tampering.

The mere use of the defragmentation utility in this particular backdating case was suspicious. The defendant claimed that he had not used the computer since 1998, and that it had sat in a closet since then. What the defendant forgot to do was reset the clock to 1998 before he used the defragmentation utility. Thus, we were able to date his use of the defrag utility to 2003.

What killed his story was that there were 200 temporary files on the computer. (Temporary files are created in the process of opening or viewing a document. They aren't so temporary, however, and can stay on the hard drive until overwritten by newer data.) Nearly all the temporary files were overwritten, mostly by the contiguous block of files created by defragmenting the drive. Only two temporary files were not overwritten.

The temporary files were drafts of the critical 1999 document. There is little to no chance that if those temporary files had actually been created in 1999, they would not have been overwritten by the 2003 defragmentation. Ergo, the temporary files and the critical 1999 document had to have been created after the defragmentation was run in 2003.

At issue in the same case were six other alleged 1997, 1998, and 1999 documents all relating to the same transaction. While allegedly having been created over a three-year time span, all of the documents had create-times between 11:05 and 11:43 A.M. What are the chances that five documents relating to the same transaction would each be separated from the other by only a few minutes? More likely, the defendant forged the documents beginning between 11:05 and 11:43 one morning in 2003, and although he reset

the computer's date when forging and backdating each document, he forgot to reset the hours and minutes.

When individuals alter electronic documents, they often unconsciously import their own stylistic elements. I learned this lesson when I was a prosecutor and my office handled a case in which a bank robber handed the teller a note that read: "This is a hole up." When the robber was later apprehended, he was given a handwriting test and asked to write out the following phrase ten times: "This is a holdup." What did the hapless defendant write? "This is a hole up. This is a hole up. This is a hole up. . . ."

In a case in which one party altered a document in a bid to create a bogus multimillion-dollar real estate commis-

As the forger tinkered with the document, he was also unknowingly making copies to his hard drive.

sion, the suspected forger was the recipient, not the sender, of the original memo. The sender's version had no paragraph referring to the commission, but the recipient's paper version did. The commission paragraph contained certain words that should have had apostrophes but did not. An examination of numerous other documents written by both the sender and recipient showed that the recipient's documents contained many examples of missing apostrophes, but the sender's did not.

There are plenty of tools for testing the authenticity of e-mails and documents, but these investigations also involve technological prowess, an investigative nose, and common sense. The good news is, it's hard to pull off a forgery. The bad news is, people are trying to do so more and more.

Eric Friedberg, a former computer crime prosecutor at the U.S. attorney's office for the Eastern District of New York, is executive vice president at Stroz Friedberg, a computer forensics and investigations firm. E-mail: efriedberg@strozllc.com, Telephone: (212) 981-6536.

This article is reprinted with permission from the January 2004 edition of THE AMERICAN LAWYER. © 2004 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact American Lawyer Media, Reprint Department at 800-888-8300 x6111. #001-01-04-0003

STROZ FRIEDBERG, LLC

15 Maiden Lane, Suite 1208

New York, NY 10038

T: (212) 981-6540

F: (212) 981-6545

www.strozllc.com