



In This Issue

- Evidence Preservation
- Standing Committee Approves Proposed Amendments to Federal Rules of Civil Procedure
- Jury Raises Morgan Stanley Damages to \$1.45 Billion
- Digital Evidence Trail Crucial in Murder Conviction

Mentioned Links

[Norton Ghost Switches U.S. Courts Guidance Software](#)
[Martin K. Miller Trial](#)

Legal Links

[Federal Rules of Evidence](#)
[Ron Perelman v. Morgan Stanley](#)

Contact Us

<http://SusquehannaDigitalForensics.Com>
Examiner@SusquehannaDigitalForensics.Com

1-717-704-0067

Evidence Preservation

You suspect that an employee is engaged in activity that violates your corporate Acceptable Use Policy for company computers. John was recently transferred out of the marketing department, to the mail room at the request of his supervisor. A co-worker in the new department found a document on the workgroup printer that contained client data that should not be available to employees in the mail department. A second document, a request for supplies, was also found in the printer tray. This document had John's name listed as the requestor. You believe that he may be collecting confidential marketing material and company customer lists.

You request your Information Technology department to investigate John's computer to determine if in fact he is engaging in the suspected behavior. One of the first things they do is to check John's access privileges on the confidential data. They discover that his access privileges weren't revoked when he was transferred, so they immediately revoke them. The Domain Administrator then remotely connects to John's computer through the Administrative Share and looks in John's My Document's folder. He finds a document called customers.doc, opens it and finds that it is the same document that the mailroom employee discovered on the printer.

You decided that it would be wise to preserve a copy of John's hard drive in case the incident leads to personnel action so you direct your staff to obtain a copy of the entire hard drive. The IT staff removes the hard disk from John's computer, and uses Norton Ghost in its standard configuration to preserve the disk.

The employee is terminated, and since you have an image of his computer, the original is wiped of all data and placed back into service. Eighteen months later you are served with a wrongful termination lawsuit. Ex-employee John claims that the document in question was placed on his computer while he was employed in the marketing department, and that he never printed customer information when he was in the mailroom. John's attorney files a discovery motion and gain access to the Ghost image you have obtained. A digital forensic expert conducts an examination with the following results.

- The Ghost image was created incorrectly. In the standard configuration, Ghost only copies the file structure and files. Your staff failed to use specialized switches that would have preserved deleted data and data found in unallocated disk space. Printer image files can reside in unallocated space for long periods of time, but since they

Editor

Robert L. Maley, CIFI, EnCE,
CISSP, MCSE

were not preserved there is no direct evidence that John actually printed the document.

- When your IT staff connected to John's computer via the Administrative share and began viewing the disk contents, file access dates were changed. They also opened the suspect document, further changing its properties. Since John had legitimate reason to have that document when he was in the Marketing Department, the file accessed times can not be used to prove he printed the document while in the mail room.

The only evidence that you are left with is the printed document, which happened to be with a document with John's name it. Can you still prevail in defending the suit? The answer may be yes, but it would have been better to prevent the suit entirely.

This scenario is rather simplistic, and in the real world there are many other factors, but it points out how important the preservation of evidence can be. A proper investigation could have found raw printer image files showing that the document was actually printed. Printer job files can also be recovered showing when and to what printer the document was sent. File access times can show when someone viewed or modified the file.

Even though employee actions may never see a criminal or civil court, evidence collection and preservation protocols should mirror what Law Enforcement uses. Properly collected and preserved evidence can prevent situations like John's law suit.

You can also use digital forensics in a proactive stance in cases of termination, transfer or promotion. Obtaining a qualified forensic duplicate of the employee's hard drive on any of these occasions may give you the ability to easily investigate matters that may arise at some future time.

In any event, develop sound policy and procedures for the forensic acquisition and preservation of digital evidence in your enterprise.

Standing Committee Approves Proposed Amendments to Federal Rules of Civil Procedure

On June 16, 2005, the Standing Committee on Rules of Practice and Procedure approved the amendments submitted by the Civil Rules Advisory Committee addressing discovery of electronically stored information.

The proposed text of each rule was approved without change; some changes were made to the committee notes. The package will be considered at the Judicial Conference in the Fall of 2005, after which the Supreme Court is expected to consider the package for promulgation before May 1, 2006.

The Rules are expected to go into effect December 1, 2006.

Jury Raises Morgan Stanley Damages to \$1.45 Billion

May 18, 2005, the jury in the Ron Perlman vs. Morgan Stanley case awarded Perlman \$850 million in punitive damages in addition to the previously awarded \$604.3 million in compensation.

The trial judge ruled that Perelman deserved an "adverse inference" because of bad faith actions by Morgan Stanley in the production of emails during the discovery phase. Judge Elizabeth T. Maass told the jury it should simply assume the firm helped defraud Mr. Perelman, sanctions for what Judge Maass determined had been egregious behavior by the defendant.

Digital Paper Trail Crucial in Murder Conviction

Martin K. Miller of Douglas County, KS, never realized that something he typed on his computer in 2002 would be used as evidence to help convict him of murdering his wife. In 2002 he made entries into a personal journal on his computer detailing the ways his wife wasn't meeting his needs. That evidence was found by police investigators and helped to establish motive in the case.

Miller also claimed he was sleeping when his wife was strangled, however his daughter told detectives that she heard him booting the computer shortly after midnight. A forensic analysis found that the computer was used at that time to conduct Internet searches. When confronted with the information, Miller changed his story and admitted being awake and conducting the searches.

"It's becoming increasingly common that any time you have a serious criminal investigation, that law enforcement is seeking the seizure of computers as a source of evidence that's going to contain information," Dist. Atty. Charles Branson said. "It's the modern digital paper trail."

Susquehanna Digital Forensics

- ▶ The company principal has a 29 year background in law enforcement, court testimony, computer systems, information systems security and forensic investigations.
 - ▶ EnCE - Encase® Certified Examiner
 - ▶ CIFI - Certified Information Forensics Investigator
 - ▶ CISSP - Certified Information Systems Security Professional
 - ▶ SSCP - Security Systems Certified Practitioner
 - ▶ MCSE - Microsoft Certified Systems Engineer
 - ▶ MCSA - Microsoft Certified Systems Administrator
 - ▶ IISFA - Member International Information Systems Forensic Association
- ▶ ISSA - Member of the Information Systems Security Association, Vice President of the Central PA Chapter
 - ▶ InfraGard - Member Central Pennsylvania Chapter