

St. Louis Technology News

THE TECHNOLOGY SPIRIT OF ST. LOUIS™

TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH



Case Closed

Ispirian Computer Forensics' specialist is able to disprove a claim involving improper use of data.

As more and more business is conducted electronically, the legal community has become aware of the need to properly archive data that might be required as evidence in litigation. Computer forensics investigation certainly plays a key role in the electronic discovery process. As Boston attorney Michael J. McHugh recently learned, however, computer forensics specialists like Ispirian's Tom Smith, a forensic scientist and a member of the American College of Forensic Examiners Institute of

Forensic Science, can also aid companies and their legal counsel in addressing claims regarding the improper use or destruction of data.

"We often use IT people for litigation support. Usually it boils down to how you produce electronic files under the new federal rules for electronic discovery," McHugh said. "I had the privilege of working with Tom recently and seeing how he can actually re-create what had occurred inside a computer with a particular set of data over a period of time. This was the first time that the actual inner workings of the computer were relevant to an issue that I had in a case.

"I had a general idea of what takes place inside a computer but I had never had the need to retain someone like Tom who could prepare a report that detailed it step by step."

In electronic discovery, computer

continued on page 2

St. Louis Technology News

PRSR STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

Case Closed

continued from p. 1 ...

forensics ensures that digital evidence isn't corrupted or contaminated from a legal standpoint. However, the same techniques can be used to prove — or, in this case, disprove — that computer devices have been used for improper or illegal activities.

Investigative Techniques

A computer forensics investigation begins with proper “chain of custody” of digital media. The investigator must ensure that no damage is done or change is made to the original media when data is extracted and copied. A computer forensics specialist then makes a bit-stream image of the original media. The hard drive is copied bit-by-bit – adding nothing and omitting nothing – and proves this by the verification of message digests (digital fingerprints) of the original media and the forensic copy.

Once the forensics image is obtained, Smith can analyze it using a variety of tools and techniques to ascertain what data has been modified, copied or deleted. He is also able to identify key evidentiary data that may be hidden or encrypted and perform extraction, analysis and reporting of evidence.

“In this case, Tom’s ultimate challenge was to determine whether or not data was improperly used,” said McHugh. “There was also the issue of spoliation of the data because a long period of time had elapsed before the forensic image was obtained. And the extent to which you can

establish that data has been modified or deleted in the interim has legal relevance. The courts will treat very harshly a party who engages in that type of spoliation.”

Smith was able not only to refute that plaintiff’s claim and to show that spoliation of the data did occur but to prove that the event did not happen.

Strong Evidence

McHugh was impressed with Smith’s technical skills as well as his ability to describe his analysis in layman’s terms. Smith provided a detailed yet comprehensible report that could have been used as evidence had the case gone to trial.

“Tom is very good at what he does,” McHugh said. “He did not need to get into a lot of jargon. The report broke down the analysis and the tools used into understandable pieces. There was a logical progression of how the investigation took place and what a computer does when it processes and stores information. I understood his report and I’m not that computer literate. So I know it had to be generally understandable to lay people.”

With a combination of technical acumen and law enforcement techniques, computer forensics specialists investigate crimes ranging from homicide to identity theft. In the business world, computer forensics is used to aid in electronic discovery, corporate governance and regulatory compliance, and in cases of employee misconduct or data theft. Given the vital role computers play in business, computer forensics specialists like Tom Smith are key assets to the business and legal communities.

THIS DATA IS SPOILED!

The word “spoliate” means to “despoil,” but how can data be spoiled? The answer has to do with legal requirements concerning the preservation of evidence — in this case, electronic data.

“‘Spoliation’ refers to the destruction or material alteration of evidence. or to the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation,” said Ispirian CEO Tom Smith. “The right to impose sanctions for spoliation arises from the court’s inherent power to control the judicial process, and the underlying policy of preservation of the integrity of the judicial process in order to retain confidence that the process works to uncover the truth.”

In addition to the courts, a growing number of regulations require that organizations preserve key data by archiving it on Write Once Read Many (WORM) media, which can be read and appended but not overwritten or reformatted. Some WORM drives can also place an electronic key on the media to ensure data integrity.



“**I had the privilege of working with Tom recently and seeing how he can actually re-create what had occurred inside a computer with a particular set of data over a period of time.**”

**— MICHAEL J. MCHUGH,
attorney**