

Bill Dean

From: Bill Dean [bill.dean@forensicdiscoveries.com]
Sent: Sunday, March 23, 2008 4:20 PM
To: bill.dean999@comcast.net
Subject: Knoxville's EDiscovery Newsletter
Attachments: _AVG certification_.txt



~~~~~

## Forensic Discoveries Newsletter

### February 2008

~~~~~

Welcome to Knoxville's EDiscovery and Computer Forensics Newsletter. Keeping you and your practice informed of the ever-changing realm and value of Electronic Discovery and Computer Forensics is the purpose of this newsletter. If you have a colleague that may be interested in subscribing, the link to subscribe is <http://www.forensicdiscoveries.com/newsletter.html> or follow the instructions at the bottom of this newsletter. If you choose not to continue receiving this newsletter, follow the directions at the bottom of this newsletter and accept my apologies for intruding.

in this issue

[Computer Forensics Proves Intellectual Property Theft](#)

[Managing Discovery of Electronic Information: A Pocket Guide for Judges](#)

[EDiscovery Case Law - Intellectual Property Theft](#)

Previous Newsletters

Last month's newsletter on the value of Computer Forensics in Divorce received great response and suggestions. Some of you suggested that the newsletters concentrate on the use of Computer Forensics in routine cases that most attorneys deal with frequently. With that suggestion, that will be the focus of the newsletter for the future. This month's installment is "Computer Forensics Proves Intellectual Property Theft" and future newsletters will include topics such as sexual harassment, contract disputes, employment matters, etc.

Below is a review of our previous newsletters:

August 2007 - "[What is Computer Forensics?](#)"

September 2007 - "[Preparing Your Clients for EDiscovery - Part 1](#)"

October 2007 - "[Preparing Your Clients for EDiscovery - Part 2](#)"

November 2007 - "[Preparing for Your Clients' EDiscovery](#)"

December 2007 - "[Why Does My Case Need Electronic Discovery?](#)"

January 2008 - ["Digital Technology is Where the Evidence is in Divorce"](#)

~~~~~

### **Computer Forensics Proves Intellectual Property Theft**

With the continued increase in the value of intellectual property, which now regularly surpasses the value of physical corporate assets, information is the most valued asset to many companies. Confidential processes, financial information, customer lists, business plans, vendor lists, marketing strategies, research data, trade secrets, etc. are vital to the success of a business. When an employee steals this information to take to the competitor that they will soon be working for or to start their own competing business, the result could be devastating to the health of a business. As we have discussed before, somewhere between 95-98% of all information is now in a digital form. When combining the importance of this information to business with the fact that most all of it is stored digitally, intellectual property theft has never been easier. While computers have made the theft of digital information easier, most don't realize that a computer forensic investigation also provides the ability to more easily determine and prove the theft.

There was a point in time when the amount of information that could be stolen was limited to how much could be carried out without being caught. This is no longer the case. Portable media such as USB hard drives, MP3 players, smartphones, and blackberries now have the storage capacity to hold huge amounts of information. Prior to these technologies, one would be a bit suspicious to see an employee that has been offered a position with a competing company carrying out boxes of company files. However, we would think nothing about the same person listening to their iPod that is plugged into their laptop. The advantage from a litigation perspective is that all of these convenient ways used to steal the information leave large amounts of traceable evidence from a computer forensics perspective. For example, each time a portable hard drive of any type (external hard drives, portable thumb drives, iPods, etc.) is plugged into a computer it leaves information such as drive manufacturer, model, and serial number of the device used. In addition, the computer logs the times and dates that the portable storage was used. When a forensic analyst combines this with file access times, creation dates, and file deletion dates, it is possible to create correlation of information that was moved to the media. If the storage media in question can be obtained, with the files more than likely "deleted", computer forensic tools can be used to recover the information to prove the theft and attempts of spoliation. Some prefer to take intellectual property slowly rather than all at once. Many times this is done using e-mail being sent to an outside account that is likely their home computer. Unfortunately, plans to steal intellectual property in this manner are planned and the perpetrator uses webmail (gmail, hotmail, yahoo mail, etc.) to avoid the traces that will be left on the company e-mail server. Unfortunately for them, the history of this activity is available in the computer's Internet history and cached web pages. Even when this information is deleted, the information may still be recovered using sophisticated forensic software. Other methods of intellectual property theft using computers that can be proven are remote access to company systems from home, "burning" the information to CDs, and the use of Internet storage areas.

Companies depend on the intellectual property that is stored digitally on their computer systems for their current and future success. With the significant role that computers often play in intellectual property and trade secret thefts, computer forensics has become a critical component in piecing together the facts needed for a successful investigation or potential litigation. While it may be very enticing for company owners or technical staff to try to determine this theft on their own, I caution

against it. Any review of the potential "smoking gun" information by personnel not trained to handle the information in a forensically sound manner will alter or destroy the information potentially impeding its admissibility and/or degrading its reliability.

~~~~~

[Managing Discovery of Electronic Information: A Pocket Guide for Judges](#)

Posted on January 25, 2008 by [K&L Gates](#)

By Barbara J. Rothstein, Ronald J. Hedges, and Elizabeth C. Wiggins

Federal Judicial Center (2007)

This "[Pocket Guide](#)" identifies problems that recur during the course of electronic discovery, and presents management tools that federal judges may use for responding to them. The [26-page publication](#) may be downloaded from the [Federal Judicial Center's website](#), free of charge.

[Continue Reading...](#)

~~~~~

**EDiscovery Case Law**

**[Appellate Court Finds Preliminary Injunction Warranted Based on Computer Forensic Expert's Findings](#)**

***Liebert Corp. v. Mazur, 827 N.E.2d 909 (Ill. Ct. App. 2005)***. The plaintiffs sought to enjoin several of its former employees from allegedly using electronic "e-commerce" Web sites - containing confidential customer lists, quotations and price books - in a new, competing business. One of the defendants admitted that he downloaded price books from the company's server to his laptop on the day he resigned. The plaintiffs hired a computer forensic expert to examine the laptop, and the expert discovered confidential files were accessed, downloaded and placed in a Zip file. The expert also determined a new Zip folder - containing quote histories and budgets - was created and subsequently copied from the hard drive to a CD-Rom on the same day the defendant was served with the plaintiffs' complaint and preliminary injunction motion. During the copy, the computer automatically placed the files in a "CD burning folder", a folder most computer users are not aware exists. During the next few days, in a "mass wave of deletion," over 12,000 files were deleted from the defendant's computer. The laptop's application log, which tracks programs like the CD-Rom burning program, was also deleted four days after the complaint was served. Despite this evidence, the trial court denied the plaintiff's motion for a preliminary injunction, finding insufficient evidence existed to prove any of the defendants used the price books before they were destroyed. On appeal, the court reversed the decision, determining the trial court

abused its discretion, and ordered the trial court to grant a reasonable preliminary injunction. The appellate court noted, "[b]ecause [the defendant] destroyed this crucial piece of evidence [the application log], we presume it would have showed he successfully copied the price books on a CD."

### **Computer Forensics Expert Uncovers Employee's Attempt to Download Company Confidential Documents**

**LeJeune v. Coin Acceptors, Inc., 2004 849 A.2d 451 (Md. 2004).** In a case involving the violation of a state trade secrets act, an employer alleged that a former employee copied proprietary electronic documents from his work laptop to a compact disc (CD), shortly before he went to work for a competitor. The employee stated that, for the sake of simplicity and because he did not know how to save individual files onto a CD, he had transferred his entire "My Documents" folder, which contained personal files such as his wedding photographs, and inadvertently captured some of his former employer's confidential business documents. The employer's computer forensics expert refuted the employee's claims, testifying that a file, which was not contained in the "My Documents" folder, was also copied to the CD. The expert also determined that the employee had attempted to hide the document transfer by deleting information about the downloads from the laptop. Based on this evidence, the appellate court affirmed the lower court's finding that the evidence supported a finding of trade secret misappropriation.

### **Computer Expert Investigation Leads to Finding of Electronic Document Trade Secret Theft**

**Four Seasons Hotels and Resorts v. Consorcio Barr, 267 F. Supp.2d 1268 (S.D.Fla. 2003).** The plaintiff brought an action against the defendant licensee alleging, among other things, violations of the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Uniform Trade Secrets Act. A computer forensic investigation revealed that the defendant accessed the plaintiff's computer network, downloaded confidential data onto backup tapes, fabricated electronic evidence, and deleted files and overwrote data prior to his computer being turned over for inspection to the plaintiff. The court held that the defendant acquired the plaintiff's confidential customer information through improper means, namely, by theft and by espionage through electronic means. The court issued a judgment for the plaintiff and ordered monetary damages, among other relief.

~~~~~

Quick Links...

[Our Website](#)

[Services](#)

[More About Us](#)

Forensic Discoveries is available to provide onsite presentations or Q&A sessions on topics such as Electronic Discovery, Technical Implications of the updated Federal Rules of Civil Procedure, or Computer Forensics. Forensic Discoveries is also available to you, obligation free, to answer any specific questions pertaining to these topics.

Simply give us a call and we will be glad to answer any questions pertaining to Electronic Discovery and Computer Forensics.

~~~~~

**Contact Information**

~~~~~

Phone: (865)-809-7590

~~~~~

If you have a topic that you would like addressed in the newsletter, please let us know. Either visit <http://www.forensicdiscoveries.com/newsletter.html> and submit your suggestion there or reply to this e-mail with your suggestion.

For previous versions of Forensic Discoveries EDiscovery newsletters, visit <http://www.forensicdiscoveries.com/pastnewsletters.html>

This document does not provide legal or other professional advice and should not be relied upon as anything other than a starting point for research and information on the subject of electronic evidence.

**Forward email**

**✉ SafeUnsubscribe®**

This email was sent to bill.dean999@comcast.net, by [bill.dean@forensicdiscoveries.com](mailto:bill.dean@forensicdiscoveries.com)  
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



Forensic Discoveries | PMB# 124 | 6923 Maynardville Pike | Knoxville | TN | 37918