

Bill Dean

From: Bill Dean [bill.dean@forensicdiscoveries.com]
Sent: Monday, January 07, 2008 1:34 PM
To: bill.dean999@comcast.net
Subject: Knoxville's EDiscovery Newsletter
Attachments: _AVG certification_.txt



~~~~~

## Forensic Discoveries Newsletter

**January 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

[Digital Technology is Where the Evidence is in Divorce](#)

[Nationally Recognized Federal Case Involves Knoxville Company and EDiscovery - Updated](#)

[EDiscovery Case Law](#)

[Courts Now Requiring Computer Forensic Experts-Be Prepared](#)

~~~~~

### Digital Technology is Where the Evidence is in Divorce

Attorneys are well informed of the impact of electronic discovery in large cases such as Zubulake v UBS Warburg and Coleman Holdings Inc. v. Morgan Stanley & Co., Inc., but a large majority of cases that benefit from electronic discovery are not publicized. Statistics from many electronic discovery and computer forensics firms indicate that more than a third of electronic discovery cases are divorce related. Judges have been facilitating this discovery for years. As an example, more than three years ago, [a judge ordered a laptop to be held for discovery](#). Many may be surprised by the high statistic of electronic discovery in divorce, but think about how our society relies on e-mail, instant messaging, or internet chats to communicate. In matters of divorce, these technologies are essential to communicate with their lovers. In today's age of

digital dependency, can an extra marital affair thrive without "secret" digital communications from a computer or cell phone? To potentially raise the stakes of the value of electronic discovery in divorce, many use computers to conduct unknown financial transactions or live a lifestyle that may not be appropriate for child custody.

Today's society uses and relies on digital technology for many aspects of day to day life. What most users of technology do not realize is that digital information is very difficult to destroy. For example, e-mails and instant messaging communications from computers and cellular phones are not destroyed when deleted and can be discovered by attorneys that leverage digital forensics. Assets that were thought to be hidden by performing online financial transactions, secret online purchases, and deleting information of joint assets is also potentially obtainable by attorneys that utilize digital forensics. A digital forensic investigation could also determine a flurry of financial transactions that are of interest to the client.

Electronic discovery can provide crucial information in cases where child custody may be of priority to the client. In these instances, electronic discovery can be a determining factor. One staple of computer users is the assumption of privacy of their actions when using a computer. The utilization of a digital forensics investigation may prove discrepancies in the lifestyle that may have been previously portrayed. Unknown behaviors such as excessive gambling, pornography, and alternative lifestyles can be proven to assist clients in their custody efforts.

Divorce is a common occurrence in today's legal landscape and electronic discovery is serving a critical role. High stake battles over marriage settlements and child custody make an attorney's strategy all the more important. Many divorce lawyers are turning to digital forensics experts to make the difference for their clients. Specialists in digital forensics are capable of finding electronic data on computer systems and cell phones that often reveal smoking gun evidence against an estranged spouse. Information can be found in a myriad of locations such as e-mail, online chat logs, instant messages, financial files, spreadsheets, image files, and internet history logs. In short, digital technology is where the evidence is in divorce.

~~~~~

Nationally Recognized Federal Case Involves Knoxville Company and EDiscovery - updated

Sixth Circuit Stays District Court's Order Allowing Plaintiffs' Computer Expert, Escorted by United States Marshall, to Inspect and Forensically Image Tennessee State Agencies' Computer Systems

John B. v. Goetz, No. 07-6373 (6th Cir. Nov. 26, 2007 and Dec. 7, 2007)

This case is a class action on behalf of roughly 550,000 children seeking to enforce their rights under federal law to various medical services, including early and periodic screenings for their physical well being, and dental and behavioral health needs. Defendants in the case include Tennessee state officials who are in charge of the state programs for these services.

On October 9 and 10, 2007, following a series of conferences and hearings (including a one-week evidentiary hearing on e-discovery issues), the district court issued a 187-

page Memorandum and accompanying Order granting plaintiffs' motion to compel defendants to produce various electronically stored information ("ESI"). The district court's Memorandum and Order addressed search terms, key custodians, claims of undue burden and privilege, spoliation, sanctions and cost-shifting. The district court also sharply criticized the defendants' preservation and production methods, and ordered the production of all metadata and deleted information. Further, the district court ordered that plaintiffs' computer expert "shall be present for the [d]efendants' ESI production and shall provide such other services to the defendants as are necessary to produce the metadata, as ordered by the Court." Additional background on the district court's October 9 and 10 Memorandum and Order, with links to the 187-page Memorandum, is available in a [previous blog entry](#). The district court subsequently appointed a monitor (former United States Magistrate Judge Ronald J. Hedges of the District of New Jersey) to oversee the court-ordered ESI production.

[Continue Reading](#)

~~~~~

## **EDiscovery Case Law**

### **[Court Allows Imaging of Employee's Laptop Hard Drive](#)**

**Sims v. Lakeside School, 2007 WL 2745367 (W.D.Wash. Sept. 20, 2007).**

In this discovery dispute, the defendant made an image of the plaintiff's employer-owned laptop with no objection from the plaintiff. Shortly thereafter, the plaintiff objected, prompting the defendant to file this motion to compel review of the hard drive. The court found the plaintiff had no reasonable expectation of privacy since the laptop was furnished by his employer and clearly articulated in the employee manual. The court granted the defendant's request to review the contents of the plaintiff's hard drive excluding web-based generated e-mails, communications between the plaintiff and his spouse (marital communications privilege) and communications between the plaintiff and his attorney (attorney client privilege). Agreeing with the defendant's proposal as to how the hard drive should be imaged, the court ordered the defendant to provide, at its expense, the parties with a list of files from the plaintiff's computer, allowing the plaintiff a chance to review for any privileged files.

### **[Court Orders Plaintiff to Produce Personal Hard Drive for Limited Inspection](#)**

**Benton v. Dlorah, Inc., 2007 WL 3231431 (D.Kan. Oct. 30, 2007).**

In this employment discrimination suit, the defendants moved to compel the plaintiff to produce documents responsive to their requests for production and the hard drive of the plaintiff's personal computer. The defendants also sought sanctions for the plaintiff's failure to provide complete responses and alleged destruction of evidence. The defendants argued that the plaintiff admittedly deleted and failed to produce relevant e-mail communications with her husband and students. Further, the plaintiff used her personal computer to send and delete hundreds of responsive e-mails, therefore, entitling the defendants to the plaintiff's personal computer hard drive for retrieval of the deleted e-mails. The plaintiff objected, claiming the hard drive contained personal, privileged information beyond the scope of discovery. The court ordered the plaintiff to produce her personal computer for inspection by a forensic

specialist, limited in scope to topics responsive to the production requests, and ordered the plaintiff to pay \$1,000 in sanctions to reimburse the defendants for costs associated with filing of this motion.

**Court Orders Preservation of Images Stored on Cell Phone**

**Smith v. Café Asia, 2007 WL 2849579 (D.D.C. Oct. 2, 2007).**

In this suit alleging sexual discrimination, assault and battery, the defendant, a former employer of the plaintiff, sought images stored on the plaintiff's cell phone to prove the plaintiff invited the treatment that incited the suit. The case was referred to United States Magistrate Judge Facciola for resolution. Judge Facciola stated that Fed. R. Civ. P. 26 is not an "all-or-nothing proposition" and the probative value of the sought-after materials must outweigh their prejudice. After conducting a Rule 26 and Federal Rule of Evidence 412 analysis, Judge Facciola ordered the plaintiff to preserve the stored images. Additionally, Judge Facciola allowed the defendant to designate one attorney to inspect the stored images in order to provide the trial judge with a fully informed debate regarding the images' admissibility.

**Court Imposes Adverse Inference Sanction for Willful Destruction of Evidence**

**Hawaiian Airlines, Inc. v. Mesa Air Group, Inc., 2007 Bankr. LEXIS 3679 (Bankr.D.Haw. Oct. 30, 2007).**

In this trade secret misappropriations claim, the plaintiff motioned the court to sanction the defendant, alleging deliberate destruction of evidence that the defendant had a duty to preserve. Before the complaint was filed, the defendant's top officer installed program deletion software on his home computer and two laptops that permanently eliminated the residue of previously deleted files and changed the system clock. The court found the destruction to be intentional, deliberate, willful and in bad faith. Therefore, the court found spoliation and ordered an adverse inference that the evidence destroyed was unfavorable to the defendant.

~~~~~

Courts Now Requiring Computer Forensic Experts-Be Prepared

From Krollontrack.com

With the changing complexities of technology, it's very important to develop a relationship with a reputable computer forensic expert. Judges are no longer willing to accept the unknown and stop when research becomes too difficult or technologically complex. Judges are basing decisions on answers and testimony from technical experts. Having an effective computer forensic expert on your side can make the difference between a win and loss.

Not only are courts expecting thorough investigations of computer evidence, some have gone as far as to order the use of a computer forensic expert. For example, in *Peskoff v. Faber*, 2007 WL 2416119 (D.D.C. Aug. 27, 2007), the court ordered both sides to solicit bids from computer forensic experts during the ongoing discovery battle. The plaintiff sought what they claimed to be highly relevant e-mails that the

defendant claimed were no longer in existence. Rather than taking the defendant's word for it, the court ordered inspection by a computer forensic expert and required both sides to solicit bids from qualified experts.

In another case, the court allowed one party's computer forensic expert, over objection, to image the other party's hard drives during the evidentiary hearing due to their inability to comply with their discovery obligations. Warner Bros. Records, Inc. v. Souther, 2006 WL 1549689 (W.D.N.C. June 1, 2006). Another court threatened the parties with appointing its own computer forensic expert to get to the truth and threatened to impose sanctions based on the information uncovered from such investigation. Koninklijke Philips Elec. N.V. v. KXD Tech., Inc., 2007 WL 879683 (D. Nev. Mar. 20, 2007).

There are multiple reasons why the knowledge of a computer forensic expert may be required in any given case. The bottom line is that it is recommended to establish a relationship with a reputable expert in advance of needing their services. If your decision comes during litigation, it will be shadowed by the pressures of the case at hand. If you establish a relationship with a reputable expert ahead of time, you will be able to call on their expertise when you require it.

~~~~~

**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
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



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