



A FORENSIC DISCOVERY NEWSLETTER  
Volume VI, Issue I Spring, 2006

FEATURE ARTICLE

## COMPELLING PRODUCTION OF HARD DRIVES

In today's heyday of electronic discovery, production of computer-generated documents has become more commonplace than it was just a few short years ago. Most major law firms understand that letters, agreements, reports, statistical and financial data may exist electronically, and they are willing to include "documents" created with everyday software programs in their discovery requests and responses. Email has also taken over as the predominant method of business communication and has proven to be a virtual treasure-trove of discoverable information. Typically these documents end up either printed out to paper or converted into an image format compatible with litigation databases such as Summation or Concordance.

Yet there is a wealth of information stored on computers that may not be as readily apparent as your standard Word or Excel file. Computers generate or store data the average user is usually not even aware of, including:

- tracking of printing, CD burning, and internet activity
- connection of removable media devices to a PC, such as USB flash drives
- records of frequently used programs/files
- fragments of documents that no longer exist on the computer
- patterns that indicate files may have been intentionally deleted or otherwise destroyed

The difficulty with this kind of information lies with how to retrieve and present it in the course of litigation. To guarantee both

authenticity and admissibility, a qualified computer forensic expert must be retained to collect the evidence. What's more, the forensic expert must have access to the original computer or hard drive to make a bit-stream copy prior to conducting the analysis and recovery of the data.

The difficulty in securing access to another party's computer or hard drive lies in the numerous objections their attorneys will assert to prevent access to it. Due to the popular myth that producing "actual" or "existing" documents is sufficient to comply with discovery requirements, counsel will typically maintain that imaging the hard drive is unnecessary, unlikely to lead to the discovery of relevant evidence, unduly burdensome, will provide access to privileged or otherwise protected information, and will unfairly disrupt the business activities of their client. In turn, the seeking party is forced to file a motion to compel, and as most judges still have little experience in dealing with e-discovery, they will need some solid reasoning as to why the other side should be forced to comply with the request.

### **Establish Need**

The first step in getting access to the opposing party's hard drive is to set forth why you need it and why you cannot get that information elsewhere. As mentioned above, computer evidence encompasses more than user files or documents, and only a forensic examination can reveal that additional information.

Common instances that warrant a thorough forensic analysis include when a departing employee is suspected of misappropriating trade secrets or when there are significant

### Inside This Issue:

Feature Article:	1
<i>Compelling Production of Hard Drives</i>	
Employee Spotlight:	3
<i>Anthony B. Hernandez</i>	
Busy First Quarter	4
<i>2006 at Forensicon</i>	
ABA Techshow 2006	4

### Welcome New Clients:

- *Ice Miller, LLP*
- *Jakubs, Kritzmire & Wigoda, LLP*
- *Kane, Carbonara & Mendoza, Ltd.*
- *McAndrews, Held & Malloy*
- *Rieck & Crotty, PC*
- *Scott P. Zoppoth, PLLC*
- *Stitt, Klein, Daday, Aretos & Giempietro, LLC*

(Continued on page two...) →

## COMPELLING PRODUCTION

(Continued from page one...)

gaps in an evidence production that indicate evidence may have been intentionally deleted.

In the case of deletion, if you can pinpoint a specific document or email you know exists (from your own production) but hasn't been produced by opposing, you give the judge more reason to suspect foul play. Furthermore, if opposing has shown a pattern of deletion (even in other litigation) or withholding evidence, you will often have an easier time getting to the drive. Counsel should also realize that in such cases, preservation in itself can be a compelling justification to allow for a forensic image to be taken of a hard drive.

### **Tailor the Request**

In order to overcome objections of being overly broad, the request must be sufficiently tailored to lead to the production of the evidence in question. The simplest way to do this is to not ask for every hard drive in the opposing party's possession. The request should pinpoint specific custodians of the data that likely have the information you seek, and should further target specific machines or devices used by those individuals. A manager of a company that left for a competitor may have a home computer with important evidence, but it may be possible to get a significant amount of what you need from his or her primary working computer. By only asking for that one computer first (but reserving the right to further discovery) you are more likely to be accommodated.

Furthermore, it often takes an examination of only one machine to discover enough information that gives cause to investigate others. With a fruitful initial search, one computer can point to other related devices that may have been attached to it, and you can more easily demonstrate the value of further analysis and illustrate how examining other media will further substantiate your claims.

Other ways to limit your request include setting date restrictions for the files or user activity in question. However, keep in mind that some data cannot be filtered by date. You can also suggest

keywords to be used during searches for evidence, or even describe the specific tasks to be performed on the evidence, such as examining internet history, recycle bin records, or registry entries. These details should be explicit in your protocol.

### **Have a Protocol**

By far the most important step in getting access to your opponent's hard drive is to spell out the protocol for acquiring and conducting the investigation of the evidence. At a minimum this should include a way to assuage concerns that privileged information may be revealed. Usually this is done by having the forensic expert provide any substantive documents to opposing first for review, then allowing them to designate which files are privileged and should be excluded from the final production. Also, many times a protective order is used to address concerns of privacy.

The protocol should also detail how chain of custody will be maintained, and how the original drive will be preserved through proper forensic imaging techniques. Your forensic expert can help you draft a protocol that both fits your needs and protects the confidentiality and privilege status of the evidence.

### **Presenting the Evidence**

The last major hurdle in dealing with production of forensic evidence lies in how to present the information found. Many times the investigation leads not so much to specific files or documents that can be produced, but rather to evidence of computer usage during certain timeframes. For example, system logs, registry entries, and other tools that show patterns of activity can reveal what a user was doing at a given time or what devices and programs were being utilized, which is not always easily printed out or viewed. The solution is to have your forensic expert prepare a written report of findings, with clear documentation of how the evidence was located and interpretation of what the activity patterns indicate.

*By far the most important step in getting access to your opponent's hard drive is to spell out the protocol for acquiring and conducting the investigation of the evidence...  
Your forensic expert can help you draft a protocol that both fits your needs and protects the confidentiality and privilege status of the evidence.*

(Continued on page three...)



## COMPELLING PRODUCTION

(Continued from page two...)

Computer forensic data and accompanying analysis can be admitted similarly to other scientific evidence under Federal Rule of Evidence 702, provided it can be attested to by a qualified expert and meets the other criteria set forth in *Daubert* (see case law, right). For this reason, examining the expert's credentials and methodology used, along with verifying his or her ability to present oral and written testimony, is a crucial step in the process.

### Costs

While it may be tempting to include an award of costs as part of your motion or in your proposed order, nothing else will cause more contention over your request. Asking for costs invites your opponent to balk even more at your motion and gives the judge more ammunition for denying your request. By being focused solely on getting

access to the drive, you can avoid this confrontation and are more likely to get to the evidence. Once you have located specific substantive information from the examination, you can always follow up with a motion for costs at a later time.

### Conclusion

Very rarely will both parties agree on the types and method of production, particularly when it involves electronic data. In cases where you can come to an agreement, you will certainly have an easier time with discovery, so every effort should be made to compromise whenever possible. When collaborative efforts fail, though, these suggestions should prove to be the basis of successfully gaining access to the opposing party's media.

## EMPLOYEE SPOTLIGHT: ANTHONY B. HERNANDEZ



With over five years of experience in litigation support on both the client and vendor sides, Anthony B. Hernandez joined Forensicon as Senior Electronic Discovery Specialist to lead Forensicon's ever-expanding electronic discovery team.

Mr. Hernandez began his career with Novack and Macey in Chicago after attending Northwestern University. He was the resident consultant for litigation technology and assisted attorneys and paralegals in cases involving electronic discovery or production databases. His role

eventually evolved into the firm's first management-level electronic discovery litigation support position, wherein he expanded his responsibilities to include exploring new ways to integrate technology into the firm's practice.

Mr. Hernandez later went on to join the team of Paragon Legal Technology support where he worked on numerous electronic discovery projects for several law firms. He spent the majority of his time processing digital evidence and educating clients on how to utilize litigation tools to gain a competitive advantage in their cases. As an experienced paralegal, Mr. Hernandez brings a wealth of knowledge in streamlining Forensicon's production process to provide clients with more tailored offerings for production review.

Mr. Hernandez is a Summation Certified Trainer and is certified to support both CaseMap and TimeMap as well. Since joining Forensicon, Mr. Hernandez has attended computer forensic courses and has continued developing his overall electronic discovery and computer forensics knowledge.

In his free time, Anthony is usually busy at home with his two Labrador retrievers and two short-haired cats; he also enjoys playing the piano, role-playing video games and reading fantasy/adventure novels.

### Helpful case law to get you started with your motion:

*Daubert v. Merrell Dow Pharmaceuticals, Inc.*,  
509 US 579 (1993)

*Gates Rubber Co. v. Bando Chem. Ind.*,  
167 F.R.D. 90 (D. Colo. 1996)

*Liebert Corp. v. Mazur* \*  
2005 WL 762954 (Ill. Ct. App. Apr. 5, 2005)

*Northwest Airlines, Inc. v. Local 2000, Int'l Bhd. of Teamsters*  
No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000)

*Playboy Enters., Inc. v. Welles*  
60 F.Supp.2d 1050 (S.D. Cal. 1999)

*Rowe Entm't, Inc. v. William Morris Agency, Inc.*  
205 F.R.D. 421 (S.D.N.Y. 2002),  
aff'd, 98 Civ. 8272, 2002 U.S. Dist. LEXIS 8308 (S.D.N.Y. May 9, 2002)

*Simon Property Group v. mySimon, Inc.*  
194 F.R.D. 639 (S.D. Ind. 2000)

*Tulip Computers Int'l v. Dell Computer Corp.*,  
52 Fed. R.Serv. 3d 1420 (D. Del. 2002)

*United States v. Triumph Capital Group*  
211 F.R.D. 31 (D.Conn. 2002)

\* For the complete published opinion by Justice Warren D. Wolfson on *Liebert Corp. v. Mazur*, which references Lee Neubecker's (President of Forensicon) testimony, please go to:

<http://www.state.il.us/court/Opinions/AppellateCourt/2005/1stDistrict/April/Html/1042794.htm>



CHICAGO OFFICE (HQ):  
226 South Wabash Avenue, Suite 300  
Chicago, IL 60604  
p: 312-427-5667 f: 312-427-5668

MILWAUKEE OFFICE:  
250 East Wisconsin Avenue, Suite 1800  
Milwaukee, WI 53202  
p: 414-390-6180 f: 414-390-6181

e: [contact@forensicon.com](mailto:contact@forensicon.com)

---

[WWW.FORENSICON.COM](http://WWW.FORENSICON.COM)

---

## BUSY FIRST QUARTER 2006 AT FORENSICON

Forensicon started its seventh year in business with its first foray into the largest LegalTech tradeshow in the nation, which was held at the end of January in New York City. The 25th Anniversary show saw thousands of legal professionals, and those of related industries, learn about emerging trends in legal technology and services.



(Pictured from left: Peter Mierzwa, Law Bulletin Publishing, Cameron Nelson, Greenberg Traurig and Lee Neubecker, Forensicon)

In February, Lee Neubecker, the President and CEO, presented a workshop, "Using Computer Forensics to Conduct Investigations," to the Chicago chapter of the Association of Certified Fraud Examiners together with attorneys from Johnson & Bell, Joseph Marconi and Kathryn Hoying. Later that month, he also spoke at the Chicago Bar Association's Chicago Law & Technology Conference alongside Cameron Nelson from Greenberg Traurig (see picture).

It has been a demanding first quarter, and the following quarter is starting to look the same, with the ABA Techshow, as well as several speaking engagements, lined up for Mr. Neubecker. It seems like 2006 may be another promising year for Forensicon if things continue to be as busy as it was in the first quarter.

## COME VISIT OUR BOOTH AT THE ABA TECHSHOW 2006

**April 20-21, 2006, 8:30am – 5:30 pm**

**Sheraton Chicago Hotel and Towers**

For more information, please call Forensicon at 312-427-5667 or visit

[http://www.abanet.org/techshow/ABA%20TECHSHOW%202006\\_12-Page%20Brochure.pdf](http://www.abanet.org/techshow/ABA%20TECHSHOW%202006_12-Page%20Brochure.pdf)

**Stop by Booth 410 for a complimentary giveaway!**

### Forensicon's Computer Forensics Services:

- Trade Secrets
- Employment Litigation
- Internal Investigations

Contained herein are the opinions and observations of Forensicon, Inc., derived from our experience and research in the subject topics. The content enclosed is not intended to impart definitive professional or legal counsel.

© 2006 FORENSICON, Inc. All rights reserved. Please send article reproduction requests to [publications@forensicon.com](mailto:publications@forensicon.com).