

# FORENSICON

Computer forensics

An electronic discovery newsletter

Electronic discovery

Volume IV, Issue II

Spring I, 2004

FEATURE ARTICLE:

## FORENSIC HARD DRIVE IMAGING

**W**hen a computer is identified as possibly containing electronic evidence, it is imperative to follow a strict set of procedures to ensure a proper (i.e. admissible) extraction of any evidence that may exist on the subject computer. The first thing to remember is the “golden rule of electronic evidence”—never, in any way, modify the original media if at all possible. Thus, before any data analysis occurs, it usually makes sense to create an exact, bit stream copy of the original storage media that exists on the subject computer. This may include a single or multiple hard drives, floppy disk(s), CD(s), Zip drive (s) or DVD(s), plus many other types of storage media that now exist. Imaging the subject media by making a bit-for-bit copy of all sectors on the media is a well-established process that is commonly performed on the hard drive level, hence often referred to as hard drive imaging.

The creation of a true forensic hard drive image is a highly detailed process. If you do not have it performed by a trained professional, you may severely compromise your chances of obtaining admissible evidence as a result of your discovery efforts. Also, to avoid accusations of evidence tampering or spoliation, it is a recommended best practice that imaging be per-

formed by an objective third party. Suggested protocols for hard drive imaging can be found within guidelines standardized by institutions and organizations like the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST).

As you hire a computer forensics expert, know that he or she can choose among a large number of software and hardware to obtain a forensic image. What is important is that you qualify the expert's experience and that you ensure a rigid process by asking the right questions. A good start is to always make sure that the integrity of all evidence is maintained, chain of custody is established, and all relevant hash values are documented.

Once imaging is completed, any good tool should generate a digital fingerprint of the acquired media, otherwise known as a hash. A hash generation process involves examining all of the 0's and 1's that exist across the sectors examined. Altering a single 0 to a 1 will cause the resulting hash value to be different. Both the original and copy of the evidence are analyzed to generate a source and target hash. Assuming they both match, we can be confi-

(Continued on page three...) ➡

## LEE NEUBECKER SPEAKS AT THE LAW

### BULLETIN E-DISCOVERY SEMINAR IN APRIL

Forensicon's President and CEO, Lee Neubecker, will be speaking at Law Bulletin Publishing Company's Electronic Discovery seminar on April 27, 2004. You can register for the seminar at the Law Bulletin's website: [www.lawbulletin.com/lb\\_seminars.cfm](http://www.lawbulletin.com/lb_seminars.cfm). The seminar is part of a series organized by Law Bulletin annually, exploring the latest issues and hottest trends in the legal industry.

“Companies involved in litigation today have learned that if you don't seek electronic information, especially raw data that can reveal evidence tampering, you are not getting all the facts. Just ask Martha!” – Lee Neubecker, President of Forensicon.

Neubecker will lend his expertise in the

(Continued on page four ...) ➡

### Inside This Issue:

<i>Feature Article:</i> <i>Forensic Hard Drive Imaging</i>	1
<i>Lee Neubecker Speaks at the Law Bulletin E-Discovery Seminar</i>	1
<i>Effective Preservation Letters for Electronic Evidence</i>	2
<i>Employee Spotlight: Justine Tan Goldsberry</i>	3
<i>Forensicon Seminar: "How to Formulate Your Discovery Request for Electronic Evidence" Thursday, March 25</i>	4

### Welcome New Clients:

- Bartlit, Beck, Herman, Palenchar & Scott
- Weaver A. Denison, Ltd.
- Spence, Moriarty & Shockey
- Johnson & Bell
- Kalcheim, Schatz & Berger

## EFFECTIVE PRESERVATION LETTERS FOR ELECTRONIC EVIDENCE

Since 90% of the world's information is stored as computer generated data, electronic discovery has become an imperative part of litigation. Billions of e-mails are being sent each day and more information is primarily (and sometimes only) stored electronically. When litigation occurs, evidence is most likely found hidden between the bits and bytes of electronic information. But the flexibility in today's computerized information era can just as easily work against you; data can easily be overwritten and purged. Time is of the essence when it comes to protecting short-lived log files that may be overwritten on a daily basis. You should send a preservation letter to the opposing party as soon as you expect litigation so that you can maximize the available information to help you prove your case.

*Time is of the essence when it comes to protecting short-lived log files that may be overwritten on a daily basis. You should send a preservation letter to the opposing party as soon as you expect litigation so that you can maximize the available information to help you prove your case.*

If a company's document retention policy involves routine destruction of electronic documents, or continued use of pertinent electronic devices, then you need to act as soon as possible. Sending a preservation letter can, and often should, occur even before you file your case. When prompt action is taken, the opposing party will more likely be able to manage the electronic evidence better and make necessary preparations in response to the request for discovery. Rule 26(a)(1)(B) of the Federal Rules of Civil Procedure requires "a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment."

To generate a preservation letter, you have to consider several factors. First, it is important to demonstrate your ability to comprehend how data is created, stored and deleted. Having that advantage would enable you to exhaust all possibilities of extracting electronic evidence in a preservation letter. The extent to which you succeed in your request for preservation depends on the type of electronic information being sought.

Data can be obtained in several forms: active data (currently accessible data from a computer), replicant data (data derived from electronic archives and automatic backups), residual data (deleted or

unallocated data on a computer), and metadata (data about electronic data that includes dates of creation, alteration, deletion, and who accessed the data, and from where, amongst others).

You also have to consider the electronic device that may contain the relevant data, and whether it resides on the home or work desktops, external drives, servers, laptops, backup tapes, etc. Once you identify the location, you should list the individuals that may be involved in the case, identifying them by name and/or capacity.

In addition to listing the location, types of data, and key individuals, the preservation letter should request that the opposing party suspend destruction of all possibly relevant data. This may involve ceasing routine document destruction, recycling of backup tapes, disk defragmentation or compression, and instructing employees to refrain from deleting documents until forensics copies of hard drives can be obtained by hard drive imaging (See feature article on page 1). The letter should also incorporate Rule 16 of the Federal Rules of Civil Procedure that mandates a duty to preserve the requested electronic evidence for discovery, and failure to respond to the request may subject the opposing party to court-ruled sanctions.

In composing the letter, you should anticipate issues that may elicit objections from the opposition. If you ask for "all data" to be preserved, the courts may object to such an overbroad request based on burden or cost. Furthermore, under Rule 26(b)(2) of the Federal Rules of Civil Procedure, the court can limit discovery if the discovery is "unreasonably cumulative...obtainable from some other source that is more convenient, less burdensome, or less expensive" or if "the burden or expense of the proposed discovery outweighs its likely benefit." Therefore, when requesting preservation of data, be specific and identify specific individuals and request that any storage media for those individuals be imaged. This will help focus your search and not encumber the opposing party with an undue burden of finding all data. It is crucial to remember that anything you ask of the opposing party can be asked of you!

(Continued on page three...)



## PRESERVATION LETTERS...

(Continued from page two...)

Finally, deploy a third-party electronic discovery expert early to help you understand the fundamentals of obtaining electronic information. When choosing an expert, consider one who can provide a myriad of services, from composing the

preservation letter to serving as an expert witness during trial. Preparing for electronic discovery may seem a laborious task, but understanding the course of action well and hiring the right experts is certainly a step in the right direction.

## HARD DRIVE IMAGING...

(Continued from page one...)

dent of the authenticity of the copied hard drive or other media.

The industry standard for imaging currently recommends the use of the MD5 algorithm. The creator of the MD5, Ronald L. Rivest of MIT, describes the algorithm as follows:

*[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input... The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.*

Mathematical jargon aside, the above statement simply says that the MD5 is an excellent method of verifying the integrity of data. An MD5 value

obtained from the image of the hard drive should match the value of the original hard drive. Even the smallest modification on a hard drive, for example, adding a comma to a MS Word document, would vastly change the resulting MD5 hash value.

While it may seem plausible to utilize internal IT personnel to render an image of a suspect hard drive, keep in mind the possible consequences. Hiring third-party computer forensics experts will ensure safe handling of evidence. A qualified expert will follow industry standards to avoid spoliation and will help to refute the charge of sabotage by an internal staff member who may know the key individual(s) connected to the case. A third-party expert will also establish a chain of custody that guarantees another layer of protection to the evidence.

*Hiring third-party computer forensics experts will ensure safe-handling of evidence. A qualified expert will follow industry standards to avoid spoliation and will help to refute the charge of sabotage by an internal staff member who may know the key individual(s) connected to the case.*

## EMPLOYEE SPOTLIGHT: JUSTINE TAN GOLDSBERRY

Justine Tan Goldsberry joined Forensicon in October of 2003 as Marketing Communications Associate. Her duties involve leading marketing initiatives for Forensicon, developing seminar series, creating presentation opportunities and providing editorial leadership with the content publishing efforts of the company.

Graduating with Honors with a Master's in English, Justine's vocational experience includes teaching English composition at Robert Morris College and being a General Manager at a high-volume restaurant in Chicago. Justine's corporate experience began with her career as an editor at West Group, a legal publishing company. In less than two years, Justine was promoted to Senior Editor. Her next move was to Hinz, where Justine led marketing and communications initiatives for the company. In this role, Justine managed the company's marketing publications.

In her spare time, Justine loves reading, cooking and entertaining. Not surprisingly, you will find J.R.R. Tolkien's "The Lord of the Rings" trilogy and Nigella Lawson's "How To Eat" cookbook sharing the same shelf in her apartment.



# FORENSICON

An electronic discovery  
newsletter

53 West Jackson Boulevard  
Suite 603  
Chicago, IL 60604

Phone: 312-427-5667

Fax: 312-427-5668

Email: [info@forensicon.com](mailto:info@forensicon.com)

---

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

---

**Computer Forensics &  
Electronic Discovery Services**

## LAW BULLETIN SEMINAR...

(Continued from page one...)

“Electronic Document Collection and Processing” portion of the seminar. His presentation will address the types of media involved in the discovery process, the storage capacity of different types of media and the sources for e-mail collection. Additionally, Neubecker will address how to effectively intake electronic evidence so that it is admissible in court and provide an overview of some of the techniques used by computer forensic examiners to process raw electronic data to find useful information.

Neubecker will be among distinguished peers—computer forensics experts and legal professionals, including Judge David H. Coar (USDC, Northern District Illinois), Judge Nan Nolan (USDC, Northern District of Illinois), Peter Bensigner from the Chicago firm Bartlit, Beck, Palenchar & Scott, and Peter Mierzwa, seminar chairman from the Law Bulletin Publishing Company. The program topics consist of computer forensics, understanding electronic discovery case law, when not to use electronic discovery, electronic document collection and processing, output databases and exhibits plus other topics.



## MARK YOUR CALENDAR!

**Thursday, March 25th, 2004, 7:45 am - 8:45 am**

Forensicon seminar:

### “HOW TO FORMULATE YOUR DISCOVERY REQUEST FOR ELECTRONIC EVIDENCE”

Seminar at 53 W. Jackson Blvd., Suite 826

Cost of Seminar: \$20, includes continental breakfast

Participants will learn the intricacies of drafting preservation letters and generating electronic discovery requests. Important issues will be addressed, including how to select target sources of stored electronic evidence, balance cost of production and discovery vs. scope and magnitude.

To register for this seminar or for more information, please call Forensicon at 312-427-5667.

#### Forensicon's Services:

- Electronic Evidence Preservation & Management
- Computer Forensics
- Data Recovery
- Electronic Discovery
- Expert Reports

---

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.

© 2004 FORENSICON, Inc. All rights reserved. Please send article reproduction requests to [publications@forensicon.com](mailto:publications@forensicon.com).