



# FORENSICON

computer forensics & electronic discovery specialists

An electronic discovery newsletter

Volume V, Issue I

Spring, 2005

## We're moving—again!

Forensicon continues growth trend

*Moving "Foreword" by Lee Neubecker, President & Founder*

In the beginning of 2004, we had just moved to a space that was double the size of our office in 2003. Now, well into 2005, we find ourselves moving again to a space almost five times the size of our current office suite. Our new office space includes numerous offices, a conference room, a state-of-the-art computer forensics lab, plus secure access storage for our client's electronic evidence and equipment.

The rapid growth of our client base, as well as the many additions to our staff has necessitated our move to a much larger facility. The new suite will allow us to expand our offering of services to address many legacy computer processing projects, tape conversion work, as well as more complex data recovery projects. We have been fortunate to have clients that recognize and value our unique talents.

(Continued on page four...) →

## Getting your Money's Worth

FEATURE ARTICLE

### —Deliverables to Request from your Computer Forensic Examiner

A vast majority of corporations utilize high technology to conduct everyday business. Because of the widespread use and adoption of technological innovations by these companies, electronic information has become ever more crucial to resolving litigation disputes.

Since electronic evidence may contain the smoking gun, you really should be equipped with the knowledge of just how many ways you can obtain the information you need (and be sure to exhaust every possibility). Deciding on a reputable forensic expert is of course the first step in finding the proverbial smoking gun without spoliation of evidence.

To preserve electronic evidence, an expert forensically images the suspect electronic media or hard drive, which is a process that involves creating a bit stream copy of the original media device. This copy is authenticated as genuine by generating and comparing something known as a hash value for both the original and copy. Once your expert has an exact copy to work with, the original drive can be stored and sealed while the expert performs all search and recov-

ery functions on the copy. This will reduce the risk of evidence spoliation.

Assuming the forensic copy has been made, the next step is equally essential—knowing what to ask from your expert. Having a printout of ALL of the data on the computer is one way to go, but do you really have the time to sift through possibly millions of pages of information? With the right requests, the production can be quite manageable and much less daunting. For example, if you're investigating an employee who's suspected of downloading pornography, perhaps asking for every file on the computer may not be the most effective method in locating these incriminating pictures. What would make more sense is to target the Internet history of the computer user, which resembles a spreadsheet list of all websites visited showing the relevant dates and times of access.

The following is a list of some of the deliverables you can request from your computer forensics expert:

(Continued on page two...) →

### Inside This Issue:

<i>Forensicon Expands to a Larger Location</i>	1
<i>Getting Your Money's Worth—What to Request from your Computer Forensic Examiner</i>	1
<i>Forensicon Celebrates Five Years in Business</i>	3
<i>Employee Spotlight: Gregg Kiriazes</i>	3

### Welcome New Clients:

- *Brooks, Adams & Tarulis*
- *Esposito & Schramm*
- *Gentry, Locke, Rakes & Moore, LLP*
- *Leydig, Voit & Mayer*
- *Mirabella & Kincaid, PC*
- *Schiff Hardin, LLP*
- *Smith, Gambrell & Russell, LLP*

## Deliverables...

(Continued from page one...)

### 1. Recover erased / deleted partitions and files:

If there is suspicious activity, chances are, they will not be found in the obvious places like the Desktop or the user's personal folder. More than likely, incriminating activities will be deleted. Therefore, having your expert recover deleted partitions and files is the most logical first step. From here, you can have a list of all deleted activity, as well as all deleted files burnt to CD, and you just might be able to find the company's intellectual property that never should have been on the computer in the first place.

### 2. Generate file hash values:

In essence, hash values are electronic fingerprints. Without going into the nitty gritty of the MD5 hash, know that there are two constants: a good computer forensic expert will know what a hash value is and that these hash values can be used to uniquely identify electronic files. When hash values are generated using a computer forensic software, you can de-duplicate files (eliminating redundancies, hence minimizing costs) and find matching files in other computer media. For example, if a hash value is generated for a file containing proprietary blueprints that are confidential, the expert can use this value to find a match in the suspect hard drive. If there is a match, it is evident that the file was saved to the computer in an unaltered state. Proprietary information that is suspected to be misappropriated can be burnt to a CD, then all files on the CD can have their hash values calculated and added to a hash set. A hash set is very similar to the federal government's known felons fingerprint database, only the hash set uniquely identifies electronic files. These hash sets help to quickly find files on a computer that has been forensically imaged.

### 3. Request file listing inventory:

Having a list of everything you need to know about a file (e.g. name, file extension, physical location, access date, create date, etc.) will help narrow your focus. For example, if you know an employee's last day of employment is the 6th of August, 2004, you will want to start your search with all files accessed/modified/deleted the two

weeks prior to that to monitor any suspicious/ anomalous activities that might occur just before the employee's departure.

### 4. Request DAT file report for Internet history:

A review of the Internet history of a user can help you and your examiner quickly focus a search on the computer user's personal web mail account. Additionally, a review of the Internet history may help you to determine if the user was accessing pornography, researching how to erase a hard drive of all activities, searching for how to successfully commit a fraud, or sending proprietary information to a competitor. This step should be taken prior to a general keyword search of the media imaged.

5. After reviewing all of the above, most often referred to by our staff as the "round one production," you can begin to target specifics:

- a. Key files of interest
- b. Relevant time frame files were created, modified, deleted
- c. Key individual organizations involved
- d. Generate keyword list for filtering of files (key addresses, web mail accounts, key terms, etc.)

### 6. Image files (.jpg, .gif, etc.) that tell a story:

Once you visit a website, most of the data that appears on your screen has likely been saved somewhere on your computer's hard drive, even if you didn't deliberately save it onto your hard drive. A review of image files can be very revealing and will often indicate what programs were recently installed or used on the computer.

### 7. Search the unallocated space and native files:

For most investigations, we find that focusing on the unallocated or empty part of the hard drive yields the best information. Because the computer will cache much of what is displayed on your computer screen to the hard drive in the unallocated portion of the hard drive, a review of

*A review of the Internet history of a user can help you and your examiner quickly focus a search on the computer user's personal web mail account. Additionally, a review of the Internet history may help you to determine if the user was accessing pornography, researching how to erase a hard drive of all activities, searching for how to successfully commit a fraud, or sending proprietary information to a competitor.*

(Continued on page three...)



## For ensicon celebrates five great years in business! (And Looking Back with President and Founder, Lee Neubecker)

Forensicon celebrated its five-year anniversary with a cocktail reception at the Union League Club of Chicago. Amongst those in attendance were clients, vendors, employees (past and present) and channel partners. Despite the blustery and wintry conditions, many braved the elements to attend the event.

As one of the few computer forensic and electronic discovery firms in Chicago, Forensicon's primary focus is the preservation, recovery and analysis of electronic information. As specialists in computer forensics, Forensicon's experts are highly trained to concentrate on receiving, imaging, tracking, processing and managing electronic evidence.

Forensicon was founded in January of 2000 but was originally named BuzzBoltMEDIA. Formerly a web management company, BuzzBoltMEDIA rode the wave of the dot com boom. However, as with many high technology companies at the turn of the century, it also saw the economy fizzle after 9/11. While many businesses failed, Mr. Neubecker had a brand new vision for his company, as most ingenious entrepreneurs do.



He revitalized the business by transforming its core focus to a growing industry—computer forensics.

At the time, Chicago was sorely lacking in computer forensics experts. Mr. Neubecker's formative training (MBA, with a focus on Technology, BBA Finance) and vocational background as an accountant and product manager for Lycos.com provided him the experience he needed in the computer forensic industry. While at Lycos, Mr. Neubecker led the discovery responses to law enforcement. Using his innate technological skills, Mr. Neubecker was able to facilitate the progress of the business and utilize his experience to elevate the company to the successful computer forensic firm it is today. Forensicon has since developed into a steady corporation with a national clientele that includes major law firms and corporations.

As Mr. Neubecker succinctly put it during his speech at the anniversary party: "We wouldn't be here today if it weren't for our clients, employees and all of the good people who refer us to their colleagues and associates."

## deliverables...

(Continued from page two...)

this area is more likely to yield a smoking gun. Electronic discovery vendors routinely neglect to search this portion of a hard drive. Only computer forensics allows you to search the unallocated space. A search of the native files that exist on the computer is also important and crucial to a search but deceptive activities are often found only in unallocated space. When deception is involved, always insist on searching the unallocated space.

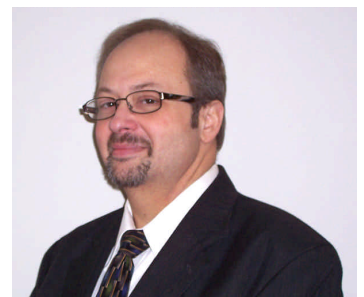
8. Every program leaves a trace. Look for .lnk files:

Most programs and documents leave link files or shortcuts throughout the hard drive. These link files can help establish when a file was last used on the computer and if it still exists. Even if scrub software was used and uninstalled, a link file may still be resident on the computer that can prove it was once there.

## EMPLOYEE SPOTLIGHT: Gregg Kiriazes

Gregg Kiriazes joined Forensicon in January, 2005 as a Systems Engineer. He brought with him more than 24 years of experience in the information technology field, ranging from data center management to his in-depth knowledge of legacy equipment migration and infrastructure.

Previously, Gregg was a consultant at Baxter Healthcare Corporation. There, he was the lead data security architect for the enterprise manufacturing and distribution systems applications. Before Baxter, Gregg was an independent systems consultant whose focus was security, backup and recovery, disaster recovery, technical support, system and network performance and configuration. In his role as systems consultant at First Chicago/NBD (now Bank One), Gregg served as the technical and management lead for the internal audit compliance project. Prior to First Chicago, Gregg was the assistant data center manager at Budget Car Rental, performing the full spectrum of data center operations.



Gregg is a lifelong Chicago resident who is passionate about his community. He is involved in community organization issues, such as Wrigley Field campus and night game expansion, business development, zoning and land use, affordable housing, charitable giving, lakefront revetment, social service availability, commercial and residential development and coexistence.

# FORENSICON

An electronic discovery  
newsletter

226 South Wabash Avenue  
Suite 300  
Chicago, IL 60604

Phone: 312-427-5667  
Fax: 312-427-5668  
Email: info@forensicon.com

---

WWW.FORENSICON.COM

---

**Computer Forensics &  
Electronic Discovery Services**

Page 4

## New Location...

(Continued from page one...)

Our new facility in the Chicago Loop will make us the largest commercial computer forensics lab in the area. It will also house a state-of-the-art secured computer forensics lab second in Chicago only to the Federal Government's Chicago Regional Computer Forensic Laboratory.

With almost 4,000 square feet in commercial space, we have the ability to stock numerous legacy computer systems that uniquely position us to be able to turn around e-Discovery data acquisition from archaic computer systems on short notice. We will continue to expand our offering of legacy tape conversion services to enable us to handle a variety of media types with faster turnaround capabilities.

These are exciting times for us. I am proud to say that the success of Forensicon is owed not only to its clients but also to our top notch team of employees that are dedicated to responding to client needs.

Again, I want to thank all of you for helping to propel us to growth and success!

**Lee Neubecker**  
**President**

**Please note our new address  
effective immediately:**

**226 South Wabash Avenue  
Suite 300  
Chicago, Illinois 60604**

### 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.

© 2005 FORENSICON, Inc. All rights reserved. Please send article reproduction requests to publications@forensicon.com.