

FORENSICON

Computer forensics

An electronic discovery newsletter

Electronic discovery

Volume IV, Issue III

Summer I, 2004

ASK OUR EXPERT :

What can computer forensics do for you?

The following are frequently asked questions pertaining to computer forensics and answers from our resident expert, Lee Neubecker.

What do you recommend as a best practice for preserving electronic data on a computer?

One of the most important things that companies need to do is to make sure that they do not spoil the evidence by looking to see what the employee was doing. In many cases, right after someone departs, the manager or someone from IT will look through the computer to see what files were recently accessed. The problem with that is the employee may have downloaded files to CDs to take with them. If someone surfs through a computer to see what was stolen, they are altering the file metadata (see "metadata" on page three), such as the date the file was last accessed. It may cause a file that was burned to CD along with other collection of files to have its last access date altered. In computer forensics, we often look for clustering of files with similar dates and times. For instance, if someone burns a number of files to CD, the last accessed time may be a second apart on files that were recently burned to CD. Frequently, we can figure out what was burned to CD by looking at the access dates because when the

computer reads the file to write it to CD, it alters access dates. The manager who accesses the computer to look around has just caused the access dates to be modified, so it makes it more difficult for forensic experts to piece evidentiary information together.



The most important step is first to make sure the evidence does not get altered, and in most situations (e.g. Windows operating systems), simply pulling the plug from the computer works. Pulling the plug prevents evidence spoliation and preserves relevant last accessed dates. Exceptions to that are Linux, servers and other more complex file structures that do not recover well from a power loss.

If someone needs to reuse the computer, they should remove the hard drive in question and buy a new hard drive for the computer. That way the evidence is reasonably preserved. They can keep the evidence hard drive in an envelope sealed by a signature and clear tape, and that way any evidence alteration can be detected by tampering of the package.

(Continued on page two...) →

LEE NEUBECKER'S CLE SEMINAR AT THE CHICAGO BAR ASSOCIATION

CHICAGO, May 6—Lee Neubecker, President and CEO of Forensicon, a computer forensics and electronic discovery firm in Chicago, presented "Computer Forensics for Lawyers" to the members of the Chicago Bar Association and the legal community. This

Continuing Legal Education (CLE) seminar emphasized the technology behind computer forensics, illuminating legal experts on details they should target when facing an electronic discovery case.

(Continued on page four...) →

Inside This Issue:

ASK OUR EXPERT: What Can Computer Forensics Do For You?	1
Lee Neubecker's CLE Seminar at the Chicago Bar Association	1
TECH SPEAK: Helpful Computer Terminology	3
Employee Spotlight: Scott R. Jones	3
Forensicon Seminar: "Resolving Intellectual Property Theft with Computer Forensics" Wednesday, June 16	4

Welcome New Clients:

- Greenberg Traurig
- Mayer, Brown, Rowe & Maw
- Sidley, Austin, Brown & Wood

What can computer forensics do for you?

(Continued from page one...)

What is the most effective method of authenticating evidence?

The first step in authenticating evidence is that you need to preserve the original evidence by removing it from normal use and sealing it from possible tampering. Once you preserve the evidence, it needs to be forensically copied in a way that does not alter the original (see *"forensic hard drive imaging"* on next page). The copy is then used by experts to perform their analysis. Before performing the analysis, the evidence needs to be authenticated. To authenticate the evidence, in essence, is to certify that the copy is exactly the same as the original.

In our profession, a hash value is used to authenticate evidence. A hash value is generated when you apply a hash algorithm against a collection of 0's and 1's that exist as data on a hard drive or any other type of storage media (see *"storage media"* on the next page). That value is such that altering a single character in a Word document, for example, changing an upper case S to a lower case s, would cause the collection of 0's and 1's on the storage media to be altered. This would then cause the hash value generated to be something totally different. Therefore, when we copy data, we are copying all the 0's and 1's on the most micro level of the storage media. We are applying the hash algorithm, and as an end result, we are getting a unique hash value, which is much like a digital fingerprint. After copying, we apply that same algorithm to the copy, for the same number of sectors. If the hash values match, we know we have a perfect copy. Once we have copied the evidence and authenticated it, then we are ready to work with the data.

If the judge allows electronic discovery without limitations, is it advisable to ask for a printout of all files on the computer?

Before doing a print production, it makes a lot of sense to apply technology to eliminate a lot of

the unnecessary information. Unique to computer forensics is the ability first to tell what is on the hard drive—files that exist on the hard drive, deleted or not, when they were accessed and created, how large they are, etc. That is a great starting point because it allows you to assess, if you were to print the files, how many pages would result and what the universe of data is. Once we know what is on the hard drive, we can perform a hash analysis whereby we analyze every individual file's hash value and compare the fingerprint of the individual file against the NIST (National Institute of Science and Technology) database, which publishes a database with the hash values or fingerprints of all known files that exist. The NIST hash database contains files that appear on operating system CDs and software applications. After analyzing and comparing all the files on the subject hard drive against this database, we can eliminate gigabytes of information that are in no way pertinent to that user's created data. We can remove those files from the list, which eliminates useless help text files and other files that come with your computer. That saves the client a lot of time, as well as money.

In addition, if our client provides us with the universe of intellectual property data (e.g. CAD drawings, price books and customer directories) on a CD, we can generate the hash values for each of the individual files. These values are then used to compare with that of all the files that exist on the subject hard drive we imaged. If there is a match, it is evident that our client's intellectual property exists on the subject computer. At that point, we can begin to explore how it got there, when it got there, what other places the file was stored and other critical information.

Hash analysis is by far the most powerful tool in proving theft of intellectual property. None of this analysis is possible when receiving evidence as printouts only.

Best Practices for Using Electronic Evidence:

1. *Create forensic copy of evidence*
2. *Authenticate evidence*
3. *Manage chain of custody*
4. *Conduct your search*
5. *Trim the dataset*

TECH SPEAK :

Helpful computer terminology

Forensic Hard Drive Imaging: Bit stream copy of all data on a hard drive. Not all hard drive copying utilities produce a true forensic copy. When making a forensic copy of a hard drive, every sector of the hard drive is copied exactly onto another hard drive that is equal in size or larger than the subject drive. The drive can also be imaged into a compressed format which allows the drive image to be stored on media such as CDs, DVDs and smaller hard drives. Once a forensic copy has been made, an expert may use the copy to reconstruct the entire contents of the hard drive and detail recent activities performed on the computer. As opposed to regular file copying, hard drive forensic imaging captures file slack, unallocated clusters, and unused drive space, where much evidence usually resides. A true forensic copy enables an expert to recover data even after data on a drive has been erased, FDISK'd and reformatted.

Metadata: Data about data. Metadata can provide information about a specific file or document. For example, filename, size, when created, last modified, last accessed and total document editing time are all considered valuable metadata. Sometimes individuals

make an effort to alter metadata. When a person tries to cover their tracks by tampering with metadata, inconsistencies across various metadata points can sometimes reveal clues of evidence tampering. Only an expert skilled in forensic examinations has the necessary skills and experience to testify credibly in a court of law relating to computer evidence tampering.

Storage Media: Storage media are devices that store application and user information. The primary storage media for a computer is usually the internal hard drive. Most internal drives are regular IDE hard drives that come with the computer. A removable drive is another popular storage device that is usually connected by firewire, USB, or parallel port (e.g. portable Zip drives, Jaz drives, or CD/DVD drives). Newer forms of external storage include USB thumb drives and camera storage media. Most external drives enable flexible data transfer from one computer to another. A computer that has had external drives connected to it usually has evidence in the computer's registry of using the subject device. When performing a forensic examination during discovery proceedings for litigation, determining if external drives were connected to the computer may help in obtaining additional evidence for discovery.

Once a forensic copy has been made, an expert may use the copy to reconstruct the entire contents of the hard drive and detail recent activities performed on the computer...A true forensic copy enables an expert to recover data even after a drive has been erased, FDISK'd and reformatted.

EMPLOYEE SPOTLIGHT: Scott R. Jones

Scott R. Jones joined Forensicon in March of 2004 as an associate whose primary functions involve computer forensic work. Scott's educational background includes two undergraduate degrees—one in Administrative Management and the other in Computer Science.

Prior to joining Forensicon, Scott was an Inventory Support Specialist at Sprint PCS. His duties entailed overseeing all aspects of inventory control, including creating weekly and monthly reports, and serving as the on-site computer technician. Scott also provided over-the-phone troubleshooting, programming, and debugging services for Sprint's clients. Scott honed his technical skills in his previous role as Senior Computer Repair Technician, repairing and maintaining customer PCs that run various Windows OS platforms, installing computer peripherals in client computers and training part-time technicians in new technologies and procedures for computer repair and software troubleshooting. His skills earned him a "Tech Bench MVP" title for customer service and technical leadership.



When Scott isn't at the computer, don't be surprised to find him playing his violin as he has a minor in music. He also enjoys movies and reading about military history.

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

WWW.FORENSICON.COM

**Computer Forensics &
Electronic Discovery Services**

Chicago bar association SEMINAR...

(Continued from page one...)

Neubecker gave an in-depth illustration of what happens to deleted files—where the missing information resides within the computer—and how computer forensics can trace intellectual property theft, IP addresses, evidence tampering and internet activities. He also shared industry best practices when managing a case that involves electronic evidence.

Next, he addressed one of the more challenging scenarios in computer forensics that attorneys encounter, which is a suspect's use of evidence-elimination software to hide traces of unlawful activity. Neubecker shed new light on the varying degrees of evidence removal using these sometimes effective software packages, and explained to the audience that even if a program is effective in wiping out relevant information, hiding the traces of the software itself proves to be a task that is beyond most people's capability. Computer forensics can usually prove existence of such programs in a suspect's machine; hence, possibly proving that evidence tampering is involved in a case.

The presentation, which was also webcast live on the Internet, was an hour and a half long, and the audience had a ten-minute Q&A session with Neubecker to wrap up the seminar.

Due to the positive response, Neubecker has been invited to be a regular CLE faculty member for the Chicago Bar Association.

MARK YOUR CALENDAR!

Wednesday, June 16th, 2004, 12 noon - 1:00 pm

Forensicon seminar:

**“Resolving intellectual property theft with
computer forensics”**

Seminar at 53 W. Jackson Blvd., Suite 826

Cost of Seminar: \$20, includes lunch

Participants will learn how computer forensics can prove misappropriation of trade secrets with electronic evidence, track movement of intellectual property across electronic media and how hash analysis can be used to quickly locate intellectual property.

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.