

FORENSICON

Computer forensics

An electronic discovery newsletter

Electronic discovery

Volume IV, Issue IV

Fall, 2004

FEATURE ARTICLE:

Track former employee's computer activities

(The following is a theoretical scenario staged to help the reader understand the essential role that a computer forensic expert plays in tracing the theft of intellectual property.)

An employee (Jane Doe) preparing to leave ACME for a competitor, NEWCO, wanted to make sure that she could take all of her clients with her to her new place of employment. Ms. Doe thought it would be important to have the customer database, marketing plans and product blueprints from ACME so that when she pitched new proposals at her new job, she would be able to win the deal against ACME by placing NEWCO's price offering just under the price likely to be offered by ACME.

On the week before she left, Ms. Doe began collecting data from numerous sources and saved this information to a removable hard drive she had recently purchased. A few weeks after Ms. Doe left ACME, a long time client called the president of ACME to let him know that Ms. Doe had sent an unsolicited proposal to his company and that Ms. Doe was extolling the benefits of her widgets at NEWCO versus those offered by her former employer.

ACME's management had never thought that Ms. Doe was the type of individual who would do this sort of thing. ACME consulted their lawyers who informed them that they needed to act quickly in

order to preserve the confidentiality of the documents taken by Ms. Doe.

ACME decided to hire a computer forensics firm to conduct an examination of Ms. Doe's work laptop, owned by ACME. Fortunately, the computer had not been used since Ms. Doe's departure. The first step taken was to forensically image the computer used by Jane Doe. Imaging involves making a bitstream copy of a hard drive. It ensures that the computer forensic expert can look at the exact match of the suspect hard drive without having to alter original evidence.

At the end of the imaging process, the copy was authenticated as being a genuine copy of the original by generating a hash value, which is a digital fingerprint meant to uniquely identify a set of data, distinguishing it from other sets of data. This value can be generated for an entire set of data (e.g. the whole universe of data on a hard drive), or an individual file (e.g. a Word document). It is an industry-standard means of authenticating evidence. Should any activity be performed on a computer, whether it be deleting a file or something as simple as changing a single character in a

(Continued on page two...) ➡

Mark your calendar & receive CLE credit!

—Lee Neubecker's seminar on intellectual property at the Chicago Bar association

CHICAGO, October 20—Forensicon's President and CEO, Lee Neubecker, will present "Resolving Intellectual Property Theft with Computer Forensics" to the members of the Chicago Bar Association and the legal community on October 20, 2004. This Continuing Legal Education (CLE) seminar will focus on tracking the movement of intellectual

property across electronic media.

Topics include, targeting specific electronic evidence instead of all data, proving

(Continued on page four ...) ➡



Inside This Issue:

| | |
|---|---|
| Feature Article: <i>Track Former Employee's Computer Activities</i> | 1 |
| CLE seminar on IP by <i>Lee Neubecker at the Chicago Bar Association</i> | 1 |
| Employee Spotlight: <i>Jason L. Gossett</i> | 3 |
| Forensicon Seminar: <i>"Resolving Intellectual Property Theft with Computer Forensics"</i> <i>Wednesday, October 20</i> | 4 |

Welcome New Clients:

- *Babbitt & Melton*
- *Bruggeman, Hurst & Associates*
- *Iwan, Cray, Huber, Horstman & VanAusdal, LLC*
- *Kirkland & Ellis, LLP*
- *Penny, Nathan, Kahan & Associates*
- *Touhy & Touhy, Ltd.*
- *Wessels & Pautsch, PC*

computer activities...

(Continued from page one...)

document (e.g. altering a comma into a colon), the hash value generated would be different. Therefore, if a copy of the original has been made, both should have an identical hash value. To maintain a proper chain-of-custody, the computer forensic expert imaged the original media, documented and validated that the hash value of the original and the copy were the same and kept the original media (suspect drive) sealed while he used the copy (evidence drive) for evidence analysis.

During analysis of the evidence drive, the forensic examiner was able to uncover 20,000 files, including a series of confidential PDF files, that had been deleted from Ms. Doe's computer the day before her departure. These documents were originally on ACME's network in a secure storage area that only the IT manager and VP of Sales had access to.

ACME had many questions to which they wanted answers:

Who accessed these PDF documents at our company besides the IT manager and VP of Sales?

What did Ms. Doe do with these documents?

Has Ms. Doe been using these PDF documents on her new computer at NEWCO?

Did anyone else at NEWCO know of Ms. Doe's actions?

Did they encourage Ms. Doe to share our information with her new employer?

Do any of our files or intellectual property exist or did they ever exist on our competitor's computers?

What else did Ms. Doe do before she left our company?

Did Ms. Doe begin working for NEWCO while she was on our payroll?

To answer these questions, ACME turned to the computer forensics firm, who advised them that they needed the help of the judge to order production of NEWCO's computers for a forensic examination. NEWCO's attorneys objected with the following

arguments:

Our information is confidential.

The cost involved in producing our computers is too great.

This will cause immense disruption to our business and will be too burdensome.

The scope of the search is too broad and isn't focused... seems like a fishing expedition...

ACME overcame these objections by following the computer forensic expert's recommendations below:

- Agree to forensic-imaging by a third party selected by the defendants
 - o Reduces disruptions
 - o Reduces cost for requesting party and all parties involved
 - o Doesn't compromise evidence when using an expert trained in the field of computer forensics
- Perform search of entire hard drive using agreed upon keywords that are focused and likely to generate relevant documents
- Generate hash values of ACME's intellectual property and then compare these hash values against those of all files imaged on NEWCO's computers to see if there's a match
- Agree to allow the responding party to review the hits found by the expert prior to being produced to ACME's attorneys
- Agree to have all parties bound by a protective order
- Consider filtering files by time frame
- Remove known files from the production set (Operating System Files, Application Files, etc...)

During analysis of the evidence drive, the forensic examiner was able to uncover 20,000 files, including a series of confidential PDF files, that had been deleted from Ms. Doe's computer the day before her departure.

(Continued on page three...)



computer activities...

(Continued from page two...)

These suggestions, when performed a step at a time, were all it took to move forward with getting access to NEWCO's computers. A stage-by-stage approach often yields better results than asking for everything at once.

Once both companies agreed to a protocol, ACME first had their forensic analyst perform hash analysis on the files that were deleted from Jane Doe's computer. These files were most likely taken by Jane to her new employer. After this process, NEWCO produced the forensic images of their computers to be examined, and the expert recovered deleted and lost files and documented the hash values that were generated for every file on NEWCO's computers. A forensic expert then compared the hash set of the suspected stolen intellectual property files against that of all files on NEWCO's computers. Any matches of hash values in this comparison quickly established that identical files existed on both companies' computers. (Conversely, if no matches were found, it might indicate that the files never made it to NEWCO's computers.) However, it is possible that a hash analysis could yield a false negative conclusion, especially if scrub software was used on NEWCO's computers to hide the tracks of the files being copied to their computers.

Further analysis to try to find a history of these files

on NEWCO's computers might include:

- Keyword search for the file names taken (Sometimes finds hits of the files as links or in the registry of the computer, despite scrub software being used)
- Examination of archival (i.e., .zip and .tar) files which sometimes contain hidden files
- Examination of the event logs to determine if CD's have been burnt recently or if the log files have been purged
- Search for printer spool files to see what recent print jobs can be reproduced
- Examine file signatures to look for file extension renaming
- Search for encrypted files on the hard drive
- Examination of link files and internet history to determine what the user had been doing recently
- Examination of graphic files on the computer

After performing some of these forensic techniques, ACME was able to retrieve the electronic evidence they needed, and the case was ruled in their favor.

Although every case is different, by adhering to one or

A forensic expert then compared the hash set of the suspected stolen intellectual property files against that of all files on NEWCO's computers. Any matches of hash values in this comparison quickly established that identical files existed on both companies' computers.

EMPLOYEE SPOTLIGHT: Jason L. Gossett

Jason L. Gossett joined Forensicon in August 2004 as a computer forensics associate. His background in Information Technology and Telecommunications enables him to contribute his expertise and skills to further enhance our technical team here at Forensicon.

Before Forensicon, Gossett was with a CPA firm in Northbrook, Illinois. He was responsible for implementing corporate security and managing company network resources. In this role he also oversaw the daily operations of the company's Exchange mail servers.

Gossett graduated Magna cum Laude with a Bachelor of Science in Telecommunications Management from DeVry University. From there, he went on to garner his extensive experience in IT by working at major corporations like GE, Motorola and Allstate Insurance Company.

Between spending time with his infant daughter and working hard on electronic data, Gossett still finds time to golf, play chess, ride motorcycles and rollerblade. It isn't unusual for him to rollerblade 30 miles a week—that's what happens when you sit in front of a computer all day!



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**

CBA SEMINAR...

(Continued from page one...)

inappropriate handling of trade secrets with electronic evidence, locating intellectual property swiftly and working with your computer forensic expert to successfully retrieve electronic evidence.

Even at his busiest, Neubecker finds time to share his knowledge with the legal community. He believes that having the technological know-how in approaching a legal battle involving electronic evidence will highly benefit attorneys who often struggle to navigate around a mountain of data. Neubecker intends to utilize this seminar to show how one can easily filter through all of the irrelevant and nebulous electronic information, hone in on the targeted sources and find the smoking gun, which, essentially, is the crux of every litigation.

Neubecker's computer forensic expertise stems from over twenty years of experience with computer technology. He is the president of a computer forensics and electronic discovery firm in Chicago. Having clients from the top 25 largest law firms in the nation means he has to consistently sharpen his skills and keep up with new technology in this growing field.

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

Get your CLE credit!

Wednesday, October 20th, 2004, 12:00 noon - 1:30 pm

CLE seminar by Lee Neubecker titled:

**"resolving intellectual property theft with
computer forensics"**

Seminar at the Chicago Bar Association, 321 S Plymouth Ct., Chicago, IL 60604

Learn how computer forensic experts can track the movement of IP and find the electronic evidence you need to win your case. You will also discover the virtues of hash analysis and how it can help economize the E-discovery process.

To register for this seminar or for more information, please go to www.chicagobar.org

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.