

# In Search Of Lost Assets: Using Computer Forensics In Intellectual Property and Trade Secret Theft Investigations

Jerry F. Barbanel  
and Bruce W. Pixley

AON CONSULTING

Theft of intellectual property results in American corporations losing more than \$250 billion annually.<sup>1</sup> The perpetrators of such crimes range from hackers and disgruntled employees trying to make some extra money to former employees who take highly guarded intellectual property and trade secrets to their new companies.

With the significant role that computers often play in intellectual property and trade secret thefts, computer forensics has become a critical component in piecing together the facts needed for a successful investigation or potential litigation. When a company suspects that its intellectual property or trade secrets have been stolen, the primary concern should be ensuring proper collection and preservation of evidence. In such situations, companies need to retain a computer forensic specialist familiar with the latest techniques used to analyze digital evidence and experienced in providing expert testimony.

Understanding what actions to take when allegations of intellectual property or trade secret theft arise can drastically impact the outcome of a matter. For instance, when a former employee is suspected of misappropriating intellectual property by copying electronic data, a search of this person's computer by someone other than a qualified computer forensic specialist can alter or potentially destroy relevant evidence. These innocent actions can result in spoliation issues.

When concerns of wrongdoing arise, the suspected employee's computer should be turned off immediately and secured until a computer forensic expert can properly image the hard drive. This specialist will create a forensic image of the hard drive, which will provide a mirror copy of the hard drive's contents. An analysis of the image will then be conducted – not the original image... Depending on the nature and sensitivity of the matter, the original hard drive will either be secured or placed back into service for future use.

It is prudent to consider retaining an independent third-party computer forensic expert to conduct the analysis of any computers that may have been used in the crime. Using an impartial expert helps maintain objectivity and independence, which will work to counsel's advantage if the matter results in litigation.

*Jerry F. Barbanel is the Executive Vice President in charge of IT Risk and Litigation Consulting for the Financial Advisory and Litigation Consulting Services practice at Aon Consulting. Mr. Barbanel can be reached at (201) 966-3494 or jerry\_barbanel@aon.com. Bruce W. Pixley is a Senior Director in charge of the West Coast Computer Forensics group at Aon Consulting. Mr. Pixley can be reached at (805) 298-0031 or bruce\_pixley@aon.com.*

**Please email the authors at [jerry\\_barbanel@aon.com](mailto:jerry_barbanel@aon.com) or [bruce\\_pixley@aon.com](mailto:bruce_pixley@aon.com) with questions about this article.**

tion and requires expert testimony.

Theft of trade secrets often involves former employees engaged in surreptitious acts designed to avoid detection by their companies. Individuals committing such crimes use a range of tools to obtain information, including external storage devices, online storage services, web-based e-mail and after hours access as well as burning data to optical media.

External storage devices such as USB thumb drives and external hard drives are being used with more frequency in computer crimes. When an external storage device is connected to a company computer, the operating system will record the date and time as well as the manufacturer, model and serial number of the device that is being used. However, the operating system does not track the data being copied to or from the storage device.

In thefts in which external hard drives or thumb drives are used, conducting a date and time analysis of the entire hard drive may aid in identifying copied files. For example, when an employee copies multiple files from a company computer to an external storage device, the rapid and successive access of those files can help establish what was copied to the external storage drive. Should the user open a file on the external storage device while connected to the computer, the operating system will create a short cut to that file. The short cut will contain embedded data that provides a range of information, including file name, date/time stamps, file size and additional information about the drive, such as volume label and serial number.

With online storage services such as AOL's Xdrive and Yahoo! Briefcase, users can upload files to a server that can be accessed from any computer by using an Internet browser. Evidence of this activity can be recovered from the user's hard drive in the form of Internet history, cookies and cached web pages.

Because most intellectual property and trade secret thefts involve a lot of preplanning, it is rare to find an employee who sends an e-mail containing a company's intellectual property using the corporate e-mail server. Instead, perpetrators might resort to web-based e-mail, which many believe is unmonitored and undetected. In reality, this activity is captured in the user's Internet history and cached web pages. Even if the user deletes the Internet history and cached web pages, the information can still be recovered using sophisticated forensic software. Because of this, many companies have taken efforts to block access to web-based e-mail.

Companies that issue laptops are at risk of employees taking their computers off-site and copying data from their company laptop to another computer. By examining the laptop's operating system, such as the registry, a forensic examiner can identify this type of activity.

Data can also be misappropriated by accessing the company's network after hours using a VPN connection. In such instances, a user will gain access through

their assigned user name and password or by unauthorized use of another employee's name and password. Activity is logged on a company's VPN. The type of information logged is dependent on the existing VPN set up. These logs can prove to be extremely valuable in investigations.

Optical media recorders installed on company computers, which enable employees to burn data to a CD-ROM or DVD disk also give users the opportunity to copy proprietary information. The forensic evidence that may be available on these is dependent on the type of burning software being used. Some programs create a temporary log of all files that were burned to the disk. However, these temporary logs are usually deleted once the process is completed. If the logs are not overwritten, then they can be recovered using forensic software. Additionally, date and time analysis of all of the files on the hard drive may also help to determine what was copied to disks. If

one or more of the files on the disk is accessed while using a company computer, the same type of short cuts will be created, as described earlier with reference to the external storage devices.

When entering into an intellectual property or trade secret theft investigation, counsel should be prepared that the investigation will often start with a single computer or device, but will likely escalate into a situation where multiple computers and/or devices must be analyzed to tie all of the relevant evidence together to prove the case. More importantly, there are many techniques that perpetrators will use in an attempt to cover their tracks. Although these investigations can be time and labor intensive, by taking action companies can recoup potential losses and further protect their intellectual capital.

<sup>1</sup> Progress Report of the Department of Justice's Task Force on Intellectual Property, *The Department of Justice*, June 2006, p. 29.

## Corporate Counsel Organization Highlights

### Suffolk Law School Schedules Seminar On Licensing Opportunities

The Suffolk University Law School is planning a CLE seminar titled Licensing: Seizing Opportunities and Mitigating Risks.

The program will take place on Friday, November 9 from 9 a.m. to 4:45 p.m. at the Suffolk University Law School, 120 Tremont Street, Boston.

Viewing licensing pragmatically, this conference focuses on recent changes that are most likely to affect business practices. Changes in the law that could impact licensing relationships will be explained from both a legal and business

perspective. Consideration of these topics will cross international borders and even physical borders, covering issues related to both international licensing and licensing in the virtual world.

Program co-chairs are Steven J. Henry and Edmund J. Walsh, Wolf, Greenfield & Sacks, P.C.

For details on registration fees, see the Bulletin Board on *The Metropolitan Corporate Counsel* website at [www.metrocorpocounsel.com](http://www.metrocorpocounsel.com).

To register for the seminar, visit [www.law.suffolk.edu/academic/als](http://www.law.suffolk.edu/academic/als).

### Boston Bar Names Public Interest Leaders

Reaffirming the Boston Bar Association's commitment to developing the next generation of civic leaders, BBA President Tony Doniger has named 15 lawyers as the newest members of the BBA's prestigious Public Interest Leadership Program.

The leadership training program, now in its fifth year, is for lawyers who have practiced law for fewer than 10 years, and fosters the professional relationships that are essential to success. Participants of the 12-month program become part of a growing alumni network, where both new and old members can benefit from the experience and leadership of their predecessors. The program was expanded this year due to overwhelming demand.

This year's Public Interest Leadership Program participants graduated from eight different law schools and represent 11 law firms, eight of which are new to the program this year. Members of the group also come from legal services agencies, the Massachusetts Legislature, and include a solo practitioner.

The 2007-2008 Public Interest Leaders will be provided with an insider's view of a large scope of civic and chari-

table opportunities in Greater Boston. Participants will spend approximately 200 hours in meetings and workshops throughout the year, learning from prominent community leaders and Public Interest Leadership alumni, developing insight into local organizations, and inspiring their peers to become more active in the civic arena.

The Public Interest leaders are: Claire Bishop Abely, Foley & Lardner LLP; Aaron J. Agulnek, Massachusetts State Senate; Jennifer A. Cardello, Foley Hoag LLP; Bryan S. Conley, Wilmer Cutler Pickering Hale and Dorr LLP; Sherry E. Cruz, Greater Boston Legal Services; Kate Grennan, AIDS Action Committee of MA; Dara Z. Kesselheim, Choate, Hall & Stewart LLP; Rachel A. Lipton, Brown Rudnick Berlack Israels LLP; Bonnie Schroeder McGuire, Ropes & Gray LLP; Jennifer M. Ryan, Dwyer & Collora, LLP; Noah C. Shaw, Mintz Levin Cohn Ferris Glovsky & Popeo, P.C.; Heidsha Sheldon, Seyfarth Shaw LLP; Stephen D. Silveri, Law Office of Stephen D. Silveri; Christopher D. Strang, Corwin & Corwin LLP, and Suleyken D. Walker, Meehan, Boyle, Black & Bogdanow.