INTERHACK

Interhack
5 E. Long Street, Suite 1001
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Identifying and Protecting Intellectual Property:
A FORENSIC COMPUTING CASE STUDY

SUMMARY

Attorneys must be prepared to protect intellectual property that is stored electronically. From illegally downloading music to sharing digital assets with competitors, intellectual property (IP) theft is on the rise. An experienced forensic computer analyst can identify when IP theft has taken place and present the facts needed to remediate in litigation.

- **Interhack discovered the necessary evidence to support a civil case against an employee accused of stealing proprietary information in electronic form and sharing it with the competition.**
- **As the computer forensic advisor, Interhack's Matthew Curtin put the facts uncovered into context, interpreting what they could mean to counsel.**

Background

Today's technology is making it much easier and less expensive to copy proprietary information – both with and without authorization. For example, an innocuous-looking flash drive, a compact electronic storage device no bigger than one's thumb, can be purchased anywhere and plugged into any computer, making downloading proprietary information simple for even the least technologically savvy employee.

Executives at a financial services company suspected an ex-employee of stealing intellectual property and taking it to his new employer, a competitor. The ex-employee, a financial analyst, had left his position very abruptly. Additionally, many of their customers had recently been solicited by the competitor, which caused the executives to question whether their former employee had taken confidential information with him to the new company.

Customers were aggressively pursued by the competition using solicitation packages. The solicitation packets included forms requesting detailed personal financial information – pre-populated for the convenience of the potential client. The amount of information needed to populate the forms for that number of clients seemed far beyond what any one person could remember, raising the question of whether the financial advisor took his old employer's proprietary customer information with him to his new employer for use in building his practice with the new firm. Remediating the damage caused by the theft of proprietary information through litigation would require proving the theft – a far higher burden of proof than circumstantial evidence.

Objective

The executives at the original firm hired Interhack's founder, Matthew Curtin, as chief forensic scientist to search the ex-employee's computer, which remained at their office. Interhack's objective was to uncover evidence to determine whether or not the ex-employee had stolen intellectual property from his former employer.

Actions

Interhack began by taking a forensic image, an exact copy, of the hard drive of the computer used by the ex-employee while working at his former employer's office.

Curtin found that two spreadsheets containing proprietary information had been transferred to a floppy disk in some of the last actions performed at his former employer's office. In the words of the former employer, those spreadsheets "are my business," including proprietary formulas used to analyze clients' finances.

This analysis led to the court issuing an order for discovery, which granted Interhack access to the ex-employee's own personal computer as well as the new employer's computers and servers.

Although the ex-employee had recently stated in deposition that he did not take anything with him from his former employer, Interhack did in fact find numerous copies of these customer files on the competitor's server, showing the employee had taken them with him from his previous job.

Interhack's findings, presented in a report and admitted into evidence, demonstrated facts contrary to the former employee's testimony. In subsequent depositions, the former employee made significant concessions when confronted with the findings.

Resolution

Through Interhack's process of discovery and analysis, the following was concluded:

- The employee knowingly transferred intellectual property from his previous employer to his new employer and perjured himself in deposition.
- The employee and new employer used the former employer's proprietary information, even after the court issued an injunction against them doing so.

Using both factual evidence and expert opinion, Interhack proved the employee's misconduct and how the data discovered was directly relevant to the critical issues of the litigation.

The Plaintiff would have had nothing more than circumstantial evidence against their ex-employee without Interhack's technical analysis and opinion.

Interhack: Demystifying Computing Technology

As computing technology becomes increasingly important in the practice of law, so does the need for understanding the technology, finding electronic facts and interpreting them in the context of a specific case.

Founded in 2000 by computer and information science researchers in Columbus, Ohio, Interhack is a professional services firm with practices in both Information Assurance and Forensic Computing.

Interhack Forensic Computing serves the legal system by finding facts through collection and analysis of electronic information. Services we provide support adjudication in civil litigation as well as criminal proceedings. Demystifying technology for attorneys, judges, and juries, we use computer science to establish the facts, and provide informed, impartial opinions, allowing the legal process to follow its course.

Aside from acting as undisclosed technology consultants in numerous cases, we have served as testifying experts in cases such as Sony BMG "Rootkit" Litigation, RIAA v. MP3Board.com, Avenue A Privacy Litigation, and the Pharmatrak Privacy Litigation, which led the First Circuit to establish standards for application of Federal wiretap statutes to Web technology.

Interhack Forensic Computing Services

- **Expert Testimony** – Testimony for the court on technical matters.
- **Forensic Consultation & Analysis** – Technical analysis of data or programs for legal argumentation. Explanation of computer or networking technology to attorneys, including assistance in definition of discovery, deposition, and the cross-examination of experts.
- **Data Recovery** – Recovery and reconstruction of data, apparently deleted, damaged or lost.
- **Electronic Discovery** – The routine collection and reporting of electronic documentation in evidence.

When you have a case where technology matters, we'll be happy to talk to you about the issues at stake, how we can help, and offer strategies to answer critical technical questions without breaking the bank.

We have supported even the most high-risk and complex adjudication.

We can do the same for you.

INTERHACK