

CyberBytes™

Straight Talk about Electronic Evidence Discovery in Civil Cases- July 2006

Evidence on The Run

Act One: A client calls to let you know that after hiring three software programmers a few weeks earlier, it has come to their attention that the ex-employer may be planning to file a lawsuit and injunction against them. The client assures you that the new employees did nothing inappropriate.

Act Two: Within a few days, your client becomes a named party in a lawsuit that cites all three ex-employees as having permanently destroyed trade secrets belonging to the plaintiff and that they allegedly conspired to misappropriate electronic information including application source code that was under development in the plaintiff's place of business while the three litigants were still employed by the plaintiff. Further, the plaintiff is seeking injunctive relief due to the fact that your client is a

direct competitor with the plaintiff which implies that the advantage gained by the alleged pirating of source code would result in a severe financial setback to the plaintiff.

Act Three: Your discussions with the client and the three software programmers to make a determination as to what may have taken place is met with complete denials that anything nefarious took place on their part. Instead, the client believes that the plaintiff has invented the entire accusation out of revenge because the three programmers went to work for a major competitor.

Act Four: The plaintiffs file for an emergency hearing to seek permission to have their computer forensic examiner conduct the examination of numerous computers used by the named litigants to locate the misappropriated electronic information and source code alleged to have been taken. Accompanying

this request is an affidavit from the plaintiff's Technology Development V.P. that claims that the unique source code which was under development by the three ex-employees was found missing only days after their sudden resignations. After many exhaustive attempts to recover the missing data, it was determined that commercial "scrubbing" software had been used to permanently erase all traces of the source code.

Act Five: You meet with your client to insist upon the hiring of your own computer forensic expert in order to conduct an internal examination of the three litigant's computers to determine who is not telling the truth before this case goes any further. Within a few days, the forensic examiner presents irrefutable results that clearly implicate the three employees in misappropriating trade secrets (documents and source code belonging to the

plaintiff), computer tampering and the willful destruction of computer information (e-mails and scrubbing software installed on one PC). A rough estimate of the costs involved to conduct the examination of three computers would be \$3K-\$5K at most!

This scenario is all too common for these types of instances in which electronic assets are misappropriated by ex-employees. In Act Five, the attorney's decision to conduct an internal audit of the computers in question is more of a rarity than normal procedure. Whether it is a belief in what the client insists to be the truth, or the attorney's unfamiliarity with computer forensics, the choice not to conduct an internal audit would likely result in the plaintiff's forensic expert finding the evidence eventually. This would leave the defense in a much weaker position as compared to discovering the truth before the plaintiff does.

The utilization of computer forensics is mostly associated with the requesting parties in civil litigation matters. But, the

responding party has just as many compelling reasons to enlist the services of a computer forensics specialist (see our white paper, "Evidence on the Run", by clicking the link at the bottom of this message. Please call us at 847-756-4890 or visit our cyber sites at www.cybercontrols.net.

You are also invited to write to us at cyberinfo@cybercontrols.net.

To download the white paper "Evidence on the Run":
<http://www.cybercontrols.net/common/downloaddoc.asp?docid=1643&id=281911>

Robert Guinaugh

Editor..... Robert Guinaugh
Contributors.....Wolfgang Wilke

This document is neither designed nor intended to provide legal or other professional advice but is intended merely to be a starting point for research and information on the subject of electronic evidence discovery. While every attempt has been made to ensure accuracy of this information, no responsibility can be accepted for errors or omissions.

CyberBytes is a monthly newsletter published by CyberControls, LLC and all contents are copyrighted with all rights reserved. Please submit your requests for distribution and additional copies to cyberinfo@cybercontrols.net
847-756-4890-Office
847-620-2500-Fax