

CyberBytes



Subject: New Year's Resolution for E-Discovery Requests

In the past year, we all witnessed a significant surge of state and federal cases in which digital forensics as an integral part of e-discovery requests was implemented by trial attorneys. For some counselors, this strategy was a continuation of past experiences with computer forensics in pursuing relevant evidence in behalf of their clients' claims. An even higher percentage of digital forensic requests however, were initiated by attorneys who for the first time were willing to take the plunge into the world of digital bits and bytes. For most of these new adopters, discovery will never be the same. This is not because a "smoking gun" was always recovered, but because in most situations, the storyline's missing pieces were located which solidified the claimant's position.

We want to suggest that you consider not letting one more year or one more important case go by without seriously considering strengthening your e-discovery request by stipulating in your motion both the inclusion of accessible (active data) and inaccessible (deleted data) electronic information.

In the absence of such a stipulation, the responding party's evidence production will always be limited to their search being focused only on accessible "active" or "live" data files. This limited discovery approach to locating and processing electronic information and e-mails for privilege review before it is delivered to the requesting party while the norm for most production requests is exactly what your opponents are counting on.

The inclusion of computer forensics in a commercial litigation matter has become an essential necessity when you consider the massive amounts of data that an average business amasses on a daily basis. Consider UC Berkeley's School of Information Management and Systems 2003 survey shows that over 93% of all commercial business information is created on computers. It further reports that over 87% of all written business communications are e-mails.

Your client's awareness of the increase in computer forensics in criminal matters has been heightened since the terrorist attack in Manhattan on September 11th. Those same clients look to you for your legal prowess and resourcefulness in using effective means to win or successfully defend their interests.

How will you be able to explain the absence of digital evidence discovery and analysis in a case after an unfavorable verdict has been passed to your client?

Attorneys who are reluctant to engage computer forensic examiners early on in commercial litigation matters need to consider familiarizing themselves with the successful strategies and tactics being utilized by their enlightened colleagues and adversaries.

CyberControls, LLC provides legal professionals with an array of educational tools to quickly acquire the basics on how and when to employ computer forensics in litigation matters.

CyberControls, LLC is prepared to assist you today. You don't have to have a degree in computer science to pursue digital forensics in your discovery efforts. Our staff of forensic examiners is prepared to be a member for your litigation team.

Take the first step in contacting Cybercontrols so that you can quickly assess how a computer forensics strategy might be appropriate to include in your client's case. Our firm is staffed with seasoned professionals who are prepared to conduct a discreet conversation about practical steps and costs involved in incorporating computer forensics consulting and services for the case you are working on.

Our examiners are available to discuss your specific needs at 847-756-4890.