

CyberBytes™

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

Managing Digital Forensic Evidence in Litigation

Despite the stereotypical mischaracterization of attorneys as being technology-challenged, an increased awareness of the importance and value of electronic evidence in commercial litigation is readily apparent just by the 23% increase in court rulings and opinions in year 2004 over the prior year with particularity to electronic evidence and related issues. Digital forensics discovery and the corresponding production of e-evidence can be a costly and complicated endeavor, especially if there is the absence of an effective and repeatable process to manage such efforts.

While every case has an abundance of unique facts and circumstances to make things interesting, the justification for employing digital forensics are relatively straightforward:

Requesting Party

- Recovery of deleted electronic evidence
- Recovery of deleted e-mail voice mail
- Recovery of metadata to authenticate evidentiary documents
- To determine custodianship and authorship of relevant evidence

Producing Party

- Recovery of lost or deleted exculpatory evidence
- Used to preserve electronic data (active/deleted) for preservation hold
- Used to provide counsel with preliminary review of questionable data files previously deleted by client
- Production of responsive, deleted electronic evidence

Too little involvement on the part of the litigator when retaining the services of a digital forensics provider can often result in overlooking critical

locations in which essential electronic evidence may still reside. It is recommended that before you contact the digital forensics provider, you determine whether you require a forensics consultant or an expert. In a consultancy arrangement, an attorney enjoys the advantages of work-product privilege, which permits greater information flow between attorney and consultant. A retained forensics expert on the other hand is by design an objective observer whose interaction with the litigation attorney is minimized. Savvy e-discovery attorneys are now retaining the services of both forensic computer consultants and independent experts in order to gain benefits from each.

And yes, there is also a thing called too much involvement or control over the digital forensics process by attorneys. Sometimes the urge to over-control the situation is the result of a

missing scope of work description coming from the service provider with sufficient details of the work to be performed accompanied with a cost estimates. If the service provider is reluctant to furnish sufficient documentation in this area, you may be talking to the wrong outfit. If on the other hand, the service provider demonstrates a firm grasp of the objectives with a detailed timeline of the tasks and associated costs to perform the work, the need for you to micro-manage the project may not be necessary.

Most digital forensic services providers are adept communicators, so you shouldn't experience much resistance in having them accommodate your need for timely updates on their work progress in your behalf. Remember that the timely exchange of follow-up information works both ways so don't delay in getting back to your service provider with any follow-up information you owe them.

At the end of the engagement, consider taking the time to initiate a wrap-up discussion with your service provider to

go over what steps worked and which didn't. Some aspects of the engagement may never be employed on another case, but the odds are that many of those steps will be used again, so it's worth the time investment to improve upon those steps that worked for you.

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