

# CyberBytes™

*Straight Talk about Electronic Evidence Discovery in Civil Cases- May 2006*

## Beyond the Smoking Gun

With dozens of recent high-profile commercial litigation cases covered in the news media that involved the discovery of 'smoking gun' like evidence such as; pivotal e-mails or deleted electronic documents, is it any wonder why most litigators are holding out for similar results in their electronic discovery efforts?

To be sure, electronic discovery and digital forensic examinations are conducted to identify and recover all pertinent and relevant evidentiary items that might be stored on various storage media. Sometimes the results of such efforts will yield very damning evidence or exculpatory evidence that can be used to effect an immediate settlement. The rest of the time, in the absence of recovering a 'smoking gun' item, many litigators are prone to conclude (incorrectly) that

further pursuit of electronic evidence is a waste of time and money.

As with all things of importance and value, the investment of effort should be commensurate with the results being sought. When it comes to computer forensics, there are a multitude of specific areas in which a seasoned forensics examiner can conduct an analysis in order to locate essential pieces of the puzzle to unveil the otherwise hidden actions and intentions of specific computer users identified in the litigation matter. In fact, it is with these categories of lesser known forensic evidence when reconstructed, can become the 'smoking gun'.

With this in mind, it is incumbent upon today's requesting parties to be much more intentional and specific with their reasons to conduct an examination of those computers of interest in a lawsuit. Otherwise, you may

run the risk of being duped into an arrangement that would severely limit the scope of an inspection and examination of those subject computers. CyberControls has published a brief description of numerous areas of a computer forensics analysis that should be considered and possibly listed as specific items of interest in an e-discovery request or computer examination request ("Beyond the Smoking Gun").

<http://www.cybercontrols.net/common/downloaddoc.asp?docid=1641&id=272232>

Finally, the recent adoption of numerous amendments to the F.R.C.P. rules that specifically deal with electronic discovery issues will require both parties in a litigation matter to more openly dialog with one another about e-evidence discovery and production in a pre-trial conference. Now that a pre-trial conference is stipulated in Rule 26(f), both parties will be required

to cover three primary aspects:

1. Preservation of all discoverable data compilations
2. The format in which the producing party should deliver all discoverable materials
3. Provisions for inadvertent disclosure

To learn more about CyberControls and the digital forensic services and pre-trial litigation consultancy support, please call us at 847-756-4890 or visit our cyber sites at [www.cybercontrols.net](http://www.cybercontrols.net). You are also invited to write to us at

[cyberinfo@cybercontrols.net](mailto:cyberinfo@cybercontrols.net)

To download the white paper "Beyond the Smoking Gun":  
<http://www.cybercontrols.net/common/downloadaddoc.asp?docid=1641&id=272232>

*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](mailto:cyberinfo@cybercontrols.net)  
847-756-4890-Office  
847-620-2500-Fax