

# Forensic Times

**Berenfeld, Spritzer, Shechter & Sheer**

CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS

## Introductory Newsletter

### First Four Bits!

Every computer file contains header and footer information that is not easily viewable by the novice user.

This "metadata" contains important programming information that allows the computer to interpret the files and use them appropriately. The first four bits contain information which identify the file type.

So, it's not the name or extension that determines the file type, it's the program used to create it. When in doubt, the first four bits will always tell you the truth.

Welcome to our *Forensic Times* introductory newsletter. Every quarter Berenfeld, Spritzer, Shechter & Sheer's Forensic Technology Group will feature recent developments in computer forensics and provide practical, actionable information on how to manage electronic discovery more effectively.

Our goal is to provide clients the most effective and efficient solutions to their electronic discovery needs. That goal is a moving target, because the needs and challenges of electronic discovery are constantly changing and intensifying. So to pursue our goal—and to best serve our clients—we focus on ways to continuously improve our ability to adapt and respond to changing electronic discovery challenges.

As you read this newsletter, you will see examples of the many ways in which Berenfeld Spritzer's Forensic Technology Group builds upon our most compelling competitive advantages—our "whatever it takes" approach to client service; collective knowledge and experience; dedicated cross-functional team of computer forensic professionals; and exceptional value.

We are thankful for the opportunity to serve our clients in 16 states, 14 countries and over 100 industries, and look forward to the challenges and opportunities ahead.



Robert D. Moody



Robert D. Moody, JD CISM CISA  
Partner, Forensic Technology Group  
Berenfeld, Spritzer, Shechter & Sheer

### Inside this issue

Efforts to Adopt the New Federal Rules on E-Discovery	2
Importance of TCP/ IP Protocol	2
Electronic Discovery: A Smart Five Step Approach	3
Free Computer Virus Finds Willing Victims	3
Sedona Conference Update	4

## Sedona Conference Update

The newly amended Federal Rules of Civil Procedure anticipate that all litigants will be able to identify, preserve, review, and disclose relevant electronically stored information (ESI) quickly and at a cost proportionate to the needs of the case. To effectively accomplish the task, organizations need to design processes and assemble new teams which leverage diverse players and skill-sets (Legal, IT, Records Management).

John Oakley, Principal, in Berenfeld Spritzer's Forensic Technology Group participated in the two-day Sedona Conference and offers advice to help facilitate communication and implement a winning litigation response strategy. See Sedona, Page 4.

## Efforts to Adopt the New Federal Rules on E-Discovery

**Seth Eichenholtz**

*Seichenholtz@forensic-data-svc.com*

### California:

In the summer of 2006 a state Judicial Council committee looking at e-discovery rules deferred proposed amendments to state court rules. Those amendments to California Rule of Court 212 would have required parties to meet and confer on electronic discovery issues during case management conferences (These changes would largely have followed the language of FRCP 16(b) and 26(f) governing pre-trial conferences and the requirements for pre-conference meet and confer discussions amongst the parties).

An important implication of the Judicial Council Committee's decision is that litigants in California Superior Court must

continue to look to other jurisdictions for guidance on electronic discovery issues until the body of case law in California is more fully developed or new rules are adopted.

### Florida:

There have been proposed changes by the Middle District of Florida (Federal Court) regarding Local Rule 3.03(f).

This jurisdiction requires that attorneys use technology to the maximum extent possible in all phases of litigation. The rule offers the example of serving interrogatories on computer disk.

### Illinois:

The Illinois Supreme Court Rules on Civil Proceedings in the Trial Court delineate the law regarding discovery of elec-

tronically stored information.

Rule 201(b)(1) defines "documents" to include "all retrievable information in computer storage" (effective since July 1, 2002).

Rule 214 governs requests for production of "all retrievable information in computer storage" (effective Jan. 1, 1996).

### New York:

There have been a number of decisions in the New York state courts that show a positive movement with respect to electronic discovery and their understanding of the nuances associated with e-discovery, particularly in the areas of cost shifting, review of electronic backup tapes (email and non-email), time periods, and forensic examinations of computer hard-drives.



## Importance of TCP/IP Protocol

**A. James Boote**

*Jboote@bsss-cpa.com*

*"An IP address can provide some supporting evidence that links a suspect to an internet crime."*

At the very heart of the internet lies the TCP/IP protocol. TCP/IP, or the Transmit Control Protocol and Internet Protocol, is the common language spoken by every computer connected to the internet and every backbone on it.

The unique name assigned to every single node connected to the internet is a 32 bit number known as the IP address. Before your browser loads a website from a web server, it provides your IP address in a packet that is sent off to the IP address of the web server. When the server sends the website to you, the data is passed along in a route determined by your IP address.

In cases involving wrongdoing via the internet, often the only clues left behind are IP addresses. When an IP address

is connected to an access log, an e-mail, or a firewall log, there are a few tools that can be applied to gather more data. The tools range from something as simple as a Google or WHOIS Search to something as legally involved as providing a Subpoena to an ISP for subscriber information. While rarely a smoking gun anymore, an IP address can provide some supporting evidence that links a suspect to an internet crime.

IP addresses are regulated by the Internet Assigned Numbers Authority (IANA). For regions across the globe, certain blocks are delegated by IANA to regional registries that hold databases of license information for those blocks.

If one knows how to interpret the registration information, a wealth of information becomes available. Each WHOIS record contains a company or person

who the addresses are assigned to, a global address, a phone number, and a few abuse reporting e-mails.

All of these are channels of communications to continue the trail of investigation. Most companies hold information as to which subscriber or computer is assigned an IP address over time and this information can be subpoenaed by the courts in the case of civil or criminal cases.

While an IP address helps a browser find a website, it may not always help an investigator find a culprit. Once the suspect is found, however, the IP address may provide evidence of involvement that fills in another piece of the whole puzzle. There is quite a bit of information that can be found in thirty-two ones and zeroes.



## Electronic Discovery: A Smart Five-Step Approach

**Robert Moody**

Rmoody@bsss-cpa.com

When you hear the term “electronic discovery,” do you have the urge to bury your head in the sand?

Sorry. Not an option. These days, every lawsuit – from a divorce to a complex litigation – can involve records that are stored electronically. Furthermore, judges have become more educated in this area. Once considered secondary information, electronic data is now a primary source.

When requesting electronically stored data, how can you be sure you’ve captured it all? Too narrow a request can cause you to miss essential information. But the “give me everything” approach doesn’t work either.

Here’s a cost-effective method for zeroing in on the data required in a discovery action.

1. Make a roadmap. First, draw the topography of the IT infrastructure – including servers and other data stores;

workstations; mobile and remote devices; software, Internet and intranet applications; and the connections between them all. You need the complete picture this will provide.

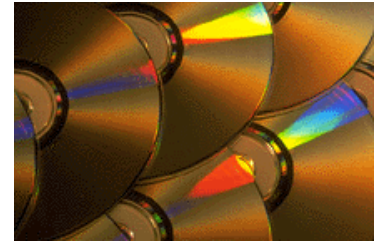
2. Track the data flow between all systems. The systems a company uses evolve over time. For instance, an IT department frequently upgrades its company’s servers. Understanding how information moved from server A to B is essential. It’s possible that non-current data was stored rather than transferred. As a result, information critical to your case may not be on the company’s servers.

3. Understand the relevant date. Examine a discovery request to determine exactly what you’re looking for. Narrow the environment to the issues involved in the suit. Identify which employees are related to the issue. For instance, in a case of fraud, you would request data, spreadsheets, and memos from the accounting department. You wouldn’t be concerned with manufacturing.

4. Find out who does what. Interview employees and document their responsibilities. By doing so, you’ll discover which people are likely to “touch” the relevant data in the course of their duties. Understand the way data flows between employees. Which software programs do they use? Where are the caches of information related to their departments?

5. Put it all together. Overlay the request for production onto your topography, data flow and knowledge of the systems. You’ll more easily pinpoint the repositories where you should look for relevant data.

Finally, get started early. This allows you to be more targeted in your request and better informed about the evidence that exists. Take time to ask the right questions, and you’ll save money and minimize the time you spend poring through irrelevant data.



*When requesting electronically stored data, how can you be sure you’ve captured it all?*

## Free Computer Virus Finds Willing Victims

**Justin Tait**

Jtait@bsss-cpa.com

Security and antivirus concerns are pressing issues for companies and individuals. A recent ad campaign on Google demonstrates that not all users exert the proper caution when downloading software.

Over 400 users clicked on an ad that offered free infection of their PCs. Didier Stevens, a

computer specialist, conducted the experiment to reveal the harmful nature of many online advertisements and the potentially damaging impact the software could have on a user’s system.

While the test advertisement actually contained no harmful programs, it did demonstrate the passivity and potential carelessness of some internet

users. According to Reuters, Mikko Hypponen, head of research at F-Secure, a data security firm, said “Some of them must have clicked on it by mistake. Some must have been curious or stupid.”

The test underscores the care firms and individuals should exhibit when clicking on various links on the Internet.



## **Berenfeld, Spritzer, Shechter & Sheer**

CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS

1551 Sawgrass Corporate Parkway, Suite 130  
Sunrise, Florida 33323  
www.bsss-cpa.com

Phone: 954-854-6004  
E-mail: Rmoody@bsss-cpa.com

**“We make sense of your data.”**

Ralph MacNamara, Editor  
Rmacnamara@bsss-cpa.com

**Berenfeld, Spritzer, Shechter & Sheer**  
Copyright © 2007  
All Rights Reserved

*In January 2006, Berenfeld Spritzer expanded the firm’s service line to establish the Forensic Technology Group through the acquisition of a practice led by Robert Moody, a computer forensic expert who was formerly with a national accounting firm.*

*Today, the 20-person forensic services team assists law firms, companies and government in conducting technology investigations on issues ranging from human resource violations to embezzlement and fraud.*

*The firm has built a state-of-the-art forensic laboratory that is capable of processing data 24 hours a day, seven days a week and can remotely connect clients to their data from anywhere in the world.*

## **Sedona Conference Update**

### **John Oakley**

Joakley@bsss-cpa.com

With 150 attendees and panelists comprised of judges, attorneys, record managers, information technologists, and computer forensic experts, the Sedona Conference represented a who’s who in electronic discovery.

While there is so much to share from this conference, one underutilized tool that can help facilitate communication and implement a winning litigation response strategy is the “Meet and Confer.”

Panelists agreed that in almost 95% of cases, parties are not even meeting, and when they do, there is little to no value.

In an effort to have a more effective meet and confer session, request that communication be transparent and “off the record”.

“Agree” or “agree not to agree”, but hashing out the issues in the meeting will ultimately reduce costs for the client. Create a checklist outlining the topics you plan to cover and send it to opposing counsel before the meet and confer.

In addition, your team should include a forensic expert and an IT representative from your client to discuss the often complex technical issues with opposing counsel’s technical team, who should also be at the meeting.

*About the Sedona Conference:*

*The Sedona Conference brings together the brightest minds for focused discussion in a think-tank setting with the goal of creating practical solutions and recommendations.*

[www.sedonaconference.org](http://www.sedonaconference.org)

