

## **DECODING COMPUTER INVESTIGATION VENDORS: HOW TO AVOID MISTAKES AND HEADACHES**

by Sharon Nelson, John Simek and Mike Maschke

© 2009 Sensei Enterprises, Inc.

When you need someone to assist with computer forensics or electronic discovery, it's usually not a happy day – or a cheap one.

E-discovery is an overwhelming subject for most attorneys. Some can hardly bear to think about it. Many have faced challenges and unforeseen problems during the e-discovery process. Since the Federal Rules of Civil Procedure were revised in 2006, attorneys have had to adapt to the new rules for e-discovery, sometimes unwillingly, and many have said it is almost akin to learning a foreign language. E-discovery is here, and is the future. All lawyers will have to learn about it. It's no longer a choice, it's the law. Just thinking back a few years ago, what lawyer knew that they would have to learn the differences between computer forensics and e-discovery, and how the two fields overlap?

Perhaps worse, incompetence in this area is so rampant that it approaches malpractice – and many commentators have suggested we will see a lot of malpractice actions in this area. We are already seeing judges handing out sanctions like Pez candy, impatiently telling lawyers, “hey, we came up to speed on this – we took classes and learned it – there has been enough time for you to get educated too.”

Technology is a moving target. Almost immediately after the rules went into effect, the technology addressed by the rules was outdated. Most attorneys believe it's impossible to keep up with the changes. When they make an effort to learn, and the technology morphs again, they feel like they are drowning. The paper world they knew so well is gone – forever. They are resistant to the electronic world, but have slowly come to realize that “resistance is futile.” A lawyer who can't play in this world can't litigate – and can't even advise clients properly.

*Understand your case before you start shopping around. Do you need a forensic expert or simply an EDD vendor? You need to understand the difference from the outset. How much ESI are you dealing with? You don't always need one of the big players, but in the right case they may be your best option. The smaller the collection, the less likely it is you need the more expensive big EDD company. Do you want online hosting? It may be the most cost effective option depending on your IT infrastructure. In making your choice you need to pick the best tool for your needs."*

- Bruce Olson  
Davis Kuelthau, <http://www.dkattorneys.com>

Production of electronic documents and data during the litigation process often will require the assistance of third-party vendors to help guide you through the process. Vendors are usually the ones responsible for the collection of the electronic data or documents, conducting the investigation, and providing the data to you in a reviewable format. In some instances, the vendors may also be asked to draft expert reports and provide expert testimony in court. With the need for e-discovery services expanding rapidly over the past few years, there are hordes of vendors vying for your business. In the current economic climate, some are almost histrionic in their entreaties.

*Early case assessment and diligence are crucial in determining whether a particular electronic discovery or computer forensics vendor is the right fit. You have to know the basics of the case, the discovery issues you may face, and the vendor's capabilities. In short, do your homework before you decide.*

- Jon Talotta  
Hogan & Hartson, <http://www.hhlaw.com>

Now the tough part for you, weeding through all the spin to figure out which vendor is right for the job.

The process of selecting a computer investigation vendor is not simple, and often can be overwhelming. However, whether choosing a computer forensics or an electronic discovery vendor, there are a number of significant questions that need to be asked before making a selection.

First and foremost, what is the vendor's knowledge of the law? Do they understand both the state and Federal laws that impact their service? You might be surprised at the number of computer forensics vendors who are willing to violate the law in order to please a customer, such as often is the case when vendors are willing to bypass password-protected information to access restricted e-mail accounts or financial information. Their illegal acts, even if committed in ignorance, can jeopardize your case. A vendor should be well balanced in both the legal aspects and the technical expertise that impact their field of business. Some follow up questions you should consider:

- (1) Does the company have any attorneys on staff?
- (2) How does the company stay up-to-date with the changes in e-discovery law?
- (3) Is the company aware of any state(s) that require a Private Investigators (PI) license to perform e-discovery services? If so, do they maintain a PI license for those states?

The answers to these questions will help you to determine if the vendor has the necessary legal knowledge to help, rather than to become a liability.

After the legal competence of the vendor is examined, the capabilities of the vendor should be explored to determine if they offer the necessary services to assist in your matter. Primarily, what services does the vendor offer within the Electronic Discovery Reference Model (EDRM), and which services do they consider their

strengths? It's common to find vendors who are well suited to complete such tasks as data identification, collection, analysis and expert testimony but lack the training and experience in other areas of the EDRM model such as data processing, review and production. Be wary of vendors who claim they can do it all. To get a better understanding of the vendor's capabilities, here are some additional questions that should be asked:

- (1) What tools does the vendor use? Have these tools been validated in court? Be cautious of vendors who use proprietary systems. Their systems may work, but will they stand up to a Daubert challenge? You don't want to risk having your evidence not admitted.
- (2) What abilities does the vendor have for incident response, in the event a client has a network security breach? Can they respond in a timely fashion, to preserve the data before its integrity is compromised? Having a vendor who is prompt and can respond at the drop of the dime is vital in some cases, especially in matters involving network security breaches, data theft and destruction. Be prepared to pay a premium for work involving a fast turn-around – the emergency nature of the beast requires moving quickly, and that comes at a premium cost.
- (3) Does the vendor have the staff in place capable of handling your project? Or is the vendor going to outsource some of the work to other companies? Will they be able to meet your deadlines and timetable? Everyone wants a vendor that is a one-stop shop. While simpler, sometimes that's neither feasible nor the best solution. In most instances, multiple vendors will be needed to perform both computer forensic and e-discovery services, depending on the requirements of your project. Can the vendor supply expert testimony if needed? Be sure to request the CVs of all their testifying experts. And review CVs with skepticism – there is a great deal of puffery in some of the CVs we've seen. Do they have a true certification or just a certification of attendance at some course?
- (4) What security systems and measures does the vendor have in place to protect your data? A secure vendor is the preferred vendor. If the vendor offers online hosting, a whole new set of security issues emerges. How does the vendor manage client confidentiality? Is all data encrypted point to point as it moves? Stored encrypted? Who has the keys? What kind of physical security is there? Is all activity logged? The vendor should have the necessary security policies and procedures in place to keep your data confidential and protected.
- (5) What types of data can the vendor handle? You will want a vendor that can handle electronic data from all types of computer systems, Windows, Macintosh and even Linux. There's no need to engage multiple vendors just to handle the different systems. Any reputable vendor should be able to handle each of them, although how they do so can vary.

- (6) Do you have a case involving foreign languages? Can the vendor handle that?
- (7) If the case involves data from abroad, is the vendor familiar, as a for instance, with European privacy laws? Have they certified their compliance with the U.S.-E.U. Safe Harbor Framework?
- (8) Can the vendor handle and process all types of e-mail? How do they deal with attachments? Do they remain with the base message or are they separated out? How do they deal with image (pictures) and sound (voicemail) files? How does the vendor handle deleted data? Deleted information may be important to your case, so ensuring that the vendor can handle and process this type of information may be vital. Remember that computer forensics is a true science – you don't want “wannabes” or amateurs here.
- (9) How do they de-duplicate the information? Do they hash the data throughout each phase of the processing? What is considered to be a duplicate? Can they process near-duplicate data?
- (10) What searching methodologies does the vendor employ? What are their search capabilities? Do they support contextual searching? Can they search through compound files such as Zip files?
- (11) How does the vendor process electronic data? Be sure to get the details down to the smallest item. You will need to know how your data is being manipulated and converted. Are they going to be able to produce the data in a format that you will be able to review?
- (12) If they're going to testify, are they credible? Can they explain complicated technical issues in plain English to juries (or judges) who have no technology knowledge?

*For selecting a computer forensics examiner, I look for two things. First, he or she must have technical qualifications and experience. Second, they should be a teacher - able to explain the forensics to a judge or jury.*

*In selecting an e-discovery vendor, prepare a checklist based on the Sedona Best Practices for Selecting Electronic Vendors and check references who have experience with similar datasets.*

- Dave Ries  
Thorp Reed & Armstrong, <http://www.thorpreed.com>

The next logical question is: How much is this going to cost me and my client? There are a few important questions to ask and vendor strategies to be aware of when it comes to pricing.

Some vendors will charge by the hour, by volume or will be flat-fee based. How does the vendor charge? Do they require a retainer payment up front? How did they come up with the pricing structure? Getting an apples-to-apples price comparison between vendors may be hard to do, especially if comparing vendors who use two different pricing methods. As always in life, be wary of the low-ball estimate. It's a common vendor strategy to bid lower upfront on a project than the competition to win the client, and then tack on the charges once the work has started. Many people get burned this way.

To prevent circumstances like these, be upfront with your vendors. Have your vendors lay out a detailed cost estimate, providing details as to the work to be completed, necessary time frame, and the deliverables. Be sure to get full-quote costs up front, even if all the details are uncertain at the current time. Be sure to get this quote in writing. Stay away from oral quotes. This allows you to have an estimate in writing that you can use as a baseline as the project progresses. Do they charge for machine run time? Do they charge for management of the case? Do they charge "set-up" fees? Will they ensure that they do not exceed a pre-determined amount without notifying you in writing and receiving authorization?

*About a year ago, we circulated an RFI fairly widely so that we would have reasonably comprehensive information readily at hand. The litigation support group is responsible for keeping the information current. That is a support function, however. The ultimate decision on which vendor to use in a particular case is between the responsible lawyer and the client.*

*We like to have several choices for a large-scale project. For a meaningful comparison, we try to lay out the likely scope of services in as much detail as possible, bracketing the ranges if there is uncertainty about, e.g., quantities, and doing what we can to make sure we and each vendor are interpreting the terms and requirements the same way. We have standardized "style sheets" for the types of load files we prefer to receive, and we update them to address ambiguities that arise or changed needs.*

*We have yet to see a one-size-fits-all vendor. Size/value of case, size of customer, number and location of sources, and timing are all factors that influence the choice of vendor. Of course, prior performance is a very significant factor.*

- Carl Roberts  
Ballard Spahr Andrews & Ingersoll, LLP  
<http://www.ballardspahr.com>

If after investigating the capabilities and pricing, the vendor looks promising, you should ask the vendor to supply you with a list of references that you can contact. By asking for several references of previous clients with similar types of projects, it will provide you with the opportunity to direct answers and hopefully cut through the "fluff". When speaking with the references, ask questions such as:

- (1) How was your experience with the vendor?
- (2) Were they able to meet all of your deadlines and deliverable requirements?
- (3) Were they responsive and accessible?
- (4) Did they exceed their original cost estimate? If so, did they seek approval prior to doing so?
- (5) Would you use the vendor again?

Checking up with a vendor's references should give you the answer you were looking for. Is this vendor the right one for the job?

Many attorneys report feeling profoundly relieved when they finally find vendors who appear to be competent, honest and fairly-priced. Having someone you trust on tap is certainly comforting. But the road to that point is full of potholes and signs hawking you up the wrong path. Today, the vendors are all touting their "estimators," which inevitably show you how much money you will save if you contract with them. Some are better than others, but it is very difficult to get a true apples-to-apples comparison. As Malcolm Forbes once said, "Beware of geeks bearing formulas." Colleagues who have had good luck decoding the process of selecting a computer investigation vendor acknowledge it is

not simple. But it is well worth investing your time. Clients are extremely appreciative of lawyers who find them quality vendors with fair pricing models. Appreciative clients tend to keep their lawyers!

*The authors are the President, Vice President and Director of Forensics of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone)703-359-8434 (fax) sensei@senseient.com (e-mail), <http://www.senseient.com>*