

## **DRAFTING ELECTRONIC EVIDENCE PROTOCOLS: STAYING OUT OF THE BRIAR PATCH**

By Sharon D. Nelson, Esq. and John W. Simek  
© 2004 Sensei Enterprises, Inc.

Discovery holds many a thorny briar patch and one of the thorniest is how to handle electronic evidence. Opposing counsel may not permit a harmonious resolution of all issues relating to electronic evidence, but giving it your best shot will hold costs down while hopefully producing the desired results. Of course, in the event of a stalemate, a judge will always be happy to dictate a protocol, but that is rarely in anyone's best interests, not only because of cost but because so many judges lack the technical skills to draft an appropriate electronic evidence protocol. Leaving such protocols in the hands of the court is often like spinning a roulette wheel – and with the same odds of success.

In a world where 95% of all documents are electronic and most will never be converted to paper, it is important for the legal profession to come up to speed on the methodology of computer forensics. While most attorneys will never become technologists, it is important that they at least grasp the fundamentals of electronic evidence in order to serve their clients well.

What issues does an electronic evidence protocol address? Here are some of the basics.

### **DESIGNATION OF FORENSIC EXPERT FOR ACQUISITION**

Generally, there is no need for multiple acquisitions, one for each side. So long as you have a true computer forensic expert, the acquisition will be handled professionally. Once a forensic image is made, another image can be produced so both sides can have their own expert do analysis, if needed. So how do you know if you have a real expert? Generally, the two best indicators are certifications (currently the EnCE – Encase Certified Forensic Examiner - is the most prestigious of the private certifications) and the expert's CV, which should indicate a host of other technical certifications, years of computer forensics experience, and the number of courts in which the expert has qualified. Generally, the designation will call for the expert to sign a confidentiality agreement so that privileged or proprietary information revealed during the evidence analysis will be protected.

### **ACQUISITION SCHEDULE.**

Make the time period reasonable and assume Murphy's law will always be a factor. Making a bit by bit image is not the same as copying or "Ghosting" a hard drive. The process is much slower. The best alternative, where feasible, is to have the computers in issue delivered to the expert's lab. In a lab setting, the expert can set up the case, kick off the acquisition, and go do other billable work while the acquisition proceeds. In the event there is some sort of complication, the expert has all his/her hardware, software, and reference materials close at hand to solve the problem.

Sometimes, the acquisition will have to be done on site, either to minimize business impact or because the other side will not agree to any other kind of acquisition. This can be economically painful because the expert must “babysit” the acquisition irrespective of time consumed. As an example, it may take 12-36 hours to acquire a single server. It is possible to run multiple acquisitions simultaneously, which will help cut costs, but often the scenario is that it is only a single server that needs to be acquired. Clients tend to be very impatient with the costs of onsite acquisition, but it simply takes as long as it takes – there is no acceleration process. Be sure to specify if the work is to be done after hours or on weekends, extending the time period for acquisition as needed to accommodate the slower pace.

## **PREVIEWS OF THE EVIDENCE**

If the parties do not agree to a full-scale acquisition, they can sometimes agree to a preview of the evidence. In fact, courts seem increasingly amenable to previews in cases where one side adamantly insists there is no relevant evidence on their computers. What is a forensic preview? A preview allows you to look at the evidence in a “read-only” mode without the need to acquire it. The expert can generate a report of this examination, but it is not repeatable because it represents a “point in time” and there is no frozen image of the data.

However, previews can have their uses, depending on the facts of the case. In one recent case, plaintiff had charged defendant with appropriating its proprietary database. Defendant insisted that it had not. Plaintiff’s expert made a set of hash values (mathematical algorithms which digitally “fingerprint” a file) representing the files that made up the database. A preview of defendant’s computers showed over 900 files matching the database files. Given that report, defendants had no further interest in discussing a full-scale forensic examination and promptly settled the case.

## **ANALYSIS SCHEDULE**

Frequently, there is only one expert working to analyze the evidence, with the results to be turned over the party charged with producing the evidence. That party then screens for privileged documents or proprietary information that it will seek to protect before turning the resulting evidence over to the other side.

In order to narrowly target relevant evidence, both sides may agree upon a period of time that is in issue, a list of names or e-mail addresses to search for, or other keywords designed to produce the relevant evidence. Make sure the protocol gives a time limit for both sides to agree upon the search parameters, a time at which the expert is required to turn over the evidence for screening, and a time at which the screening party must produce the evidence to other side.

## **COSTS**

The normal rule of thumb is that the producing party must bear the costs of evidence production. However, it is sometimes smarter for the other side to pick up the costs, especially where it is fairly certain that damning evidence exists. If the proposed discovery is not overbroad and designed to unearth relevant evidence with a minimum of business impact, a judge is not likely

to look with favor upon the other side's claims of hardship where the party requesting discovery agrees to pick up the expenses.

If money is a major issue, it may not be feasible to offer to pick up expenses. However, in accordance with *Zubulake v. UBS Warburg* line of cases, it may be possible to achieve cost shifting depending upon the following (in order of priority):

The extent to which the request is tailored to discover relevant information:

Whether the information is available from other sources;

The cost of production compared to the amount in controversy;

The cost of production compared to each party's resources;

The ability and incentive of each party to control costs;

The importance of the issues at stake; and

The relative benefits to the parties of obtaining the information requested

## **SCOPE OF ACQUISITION**

It is imperative to define the scope of the acquisition. Each workstation or server to be acquired should be specifically identified. Likewise, if backup media is to be restored, generally a more time consuming and costly process, identify which media is in issue. Likewise, if there are digital cameras, digital printers, PDAs, or other peripherals to be acquired, enumerate them. If the case involves loose media (CD-ROMS, DVDs, floppy disks, zip disks, etc.), they too must be specified.

Sometimes, the parties can agree to acquire certain obvious workstations and/or servers and then determine whether any further forensic acquisition and analysis are required after evaluating the results from the initial acquisition and analysis.

## **FORENSIC ACQUISITION**

Here the parties can agree on the type of hardware/software to be used. Commonly, private experts will use FastBloc and EnCase, which has over 12,000 licensed users and has been successfully admitted into evidence in thousands of criminal and civil court cases. There are no known instances of sustained objections to EnCase-based computer evidence on authentication grounds relating to the use of EnCase.

While the acquisitions of any subject media will generally be done using FastBloc write-blocking hardware and EnCase software, there are other forensically sound methods that could be employed in unusual situations and may be referenced in the protocol. The acquisitions will result in a complete bit-by-bit image of the media. Analysis will be done on the imaged drive –

the original media will not be impacted in any way. EnCase acquires the data and saves it into a proprietary evidence format which is constantly hashed and verified for errors and compared against the original at the conclusion of the acquisition to verify that a forensic bit by bit image has been obtained.

Once the evidence is acquired, the protocol should state that the evidence will be kept under lock and key in a secure environment, specifying those who will have access to the evidence. Chain of custody should be maintained in writing throughout the course of the acquisition and analysis. The protocol may also provide that, at the conclusion of the case, the expert will destroy the evidence files upon receipt of written, signed instructions from the parties. Alternatively, the protocol may decree that the evidence is to be returned to the originating party. Generally, the protocol will state that all work on the imaged drive will be documented and included within a forensic report.

## **ANALYSIS AND PRODUCTION**

Once the expert has completed the analysis, the protocol will generally provide that documents and data will be extracted and forwarded to defendant's counsel, who will review them for privilege and proprietary information prior to producing all non-privileged documents to opposing counsel. Any data or documents that are claimed to be privileged will be available to the Judge for an *in camera* inspection upon the appropriate motion by the moving party. The protocol will provide that all data and documents the Judge deems are not confidential or privileged are to be released to opposing counsel, pending the resolution of any and all objections and/or motions from parties.

## **FINAL THOUGHTS**

Careful drafting of an electronic evidence protocol, and working with the other side to achieve a balanced document can avoid many of the preliminary skirmishes that so often are the hallmark of discovery wars. If the other side can't or won't work with you, drafting a responsible and reasonable protocol to be presented to the court will often result in that protocol being adopted wholesale by the court. Remember Brer Rabbit? "Oh please, anything but the briar patch, please don't throw me in the briar patch." The best way to avoid briar patches of electronic discovery is to formulate a well-crafted electronic evidence protocol. With luck, it will be your opponent who is thrown into the briar patch.