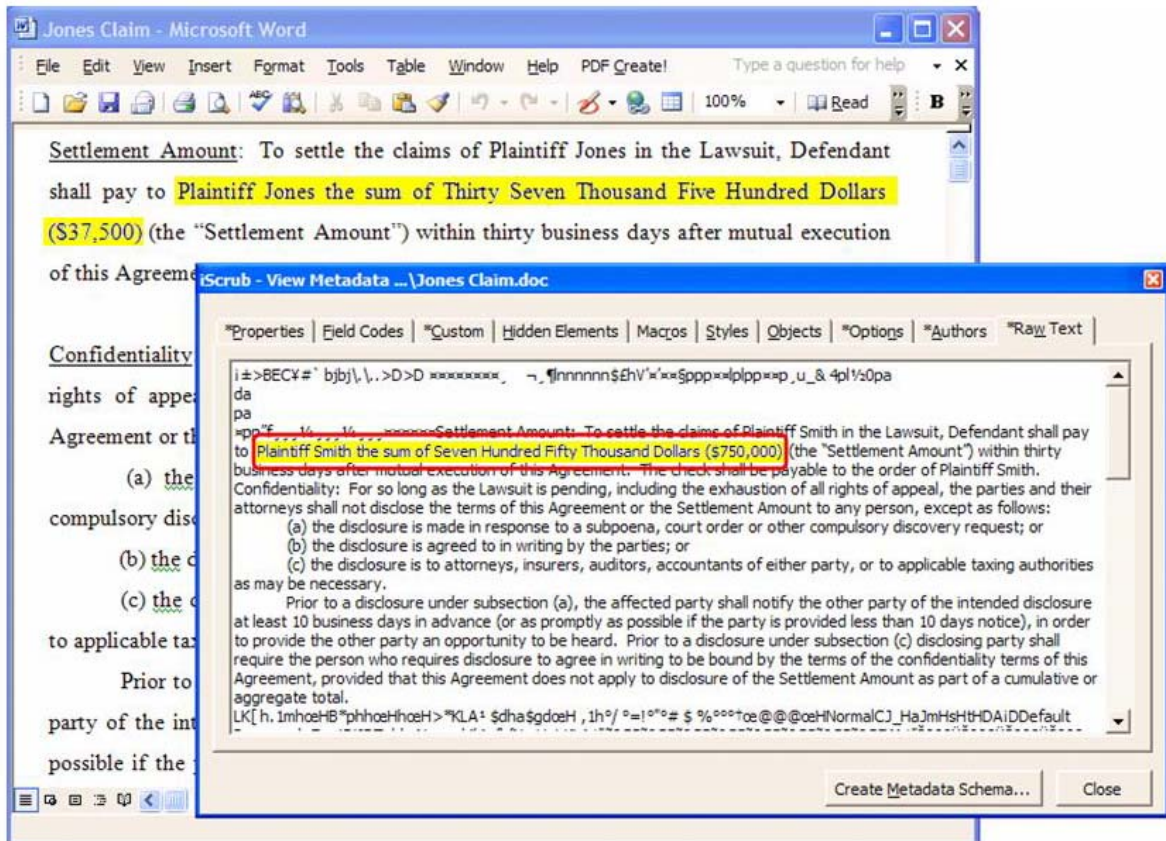




## Example: Meta Data

So let us see what meta data looks like:



© 2006 Ixio Corporation/WBTT

The Word document in the background was created using the "Open File – Save As" method. The original document was drafted for Plaintiff Smith, who earlier settled with Defendant for \$750,000. Defendant later is seeking to settle with Plaintiff Jones for much less money. You can see in the foreground with the iScrub viewer application "stuff" (*i.e.*, meta data) that cannot be seen using the Word application, such as deleted and revised text, which is highlighted. Meta data also includes other information, such as the author and the date of the revised document (not shown above).

## **Electronic Discovery: A Tiger About to Roar**

Those who believe that electronic discovery is just hype or a sleeping monster are in grave danger. Craig Ball, a leading national expert in electronic discovery, makes the following observation:

It's the Stirring Monster. E-discovery's been slow to take hold in everyday practice, but everyone uses computers and nearly all documentary evidence is born digitally. Lawyers can't walk away from 2/3rds of the evidence or turn a blind eye to its metadata. Judges are starting to "get it," too. Intelligently and aggressively pursued, e-discovery lets you eat your opponents for breakfast.

<http://www.abanet.org/lpm/lpt/articles/ptr07041.html>

It is unacceptable to continue to turn a blind eye to electronic discovery. Tom Mighell, an expert on legal technology and a well known legal blogger, cites the following statistics:

According to the ABA's Legal Technology Resource Center's 2004-2005 report, 73% have never received a request for electronic discovery, while 11% receive two or less per year, 9% receive 3-11 requests per year, and 6% receive them monthly. ([http://www.discoveryresources.org/04\\_om\\_thinkingED\\_0510.html](http://www.discoveryresources.org/04_om_thinkingED_0510.html))

Past practices no longer will work: "Lawyers have tended to avoid filing e-discovery requests, primarily out of fear. If they file a request, the other side may retaliate with a last-minute barrage of requests on the eve of trial. John Tredennick, chief executive of Catalyst Repository Systems, Inc., calls this 'mutually assured destruction.'" (<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1159866329787>)

And there is plenty of information out there to inform and educate members of the Bar about electronic discovery. (See, e.g., <http://www.wsba.org/media/publications/barnews/june06-medved.htm>)

### **Attorney Duties and Ethical Rules**

The American Bar Association and the Washington State Bar Association have adopted the following ethical rule:

A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

Attorneys are under ethical requirements to preserve client confidences and not waive privileged information. As electronic discovery takes hold, it is now critical to control the collection, review and production of all electronic information. Furthermore, this responsibility should not be delegated to a non-attorney that is unfamiliar with the case and legal principles at stake. "Lawyers can outsource many services or hire technical support to operate electronic systems, but they retain a duty to supervise staff, outside vendors, and independent contractors in the performance of their professional responsibilities." (<http://www.abanet.org/genpractice/magazine/2003/jun/judgment.html>)

### **Start Now – Plan and Prepare**

A smart approach to this problem is to be proactive, and begin to plan before any problem arises. This approach will enable you to control the timing of your tasks without having externally imposed pressures, such as discovery deadlines, affecting your work.

Before starting, it is important to make sure everyone is educated. You should ask each participant (including legal staff, outside counsel, IT staff, records management staff, and senior management) the following questions:

- Have you ever seen meta data before?
- Do you know where electronic information is stored?

If they are unable to answer these questions, they should first read this paper before starting.

#### **1. Organize and Protect Your Electronic Information**

Step 1: Send all third party email attachments as Adobe .pdf files (<http://www.adobe.com/products/acrobat/readstep2.html>).

Step 2: Digitize your existing hard copy documents, such as your signed original contracts. These digitized documents should be converted into a non-editable format, such as Adobe .pdf files, and stored in a secure location within your system (such as your document management system). They should be organized so you or anyone can find them quickly and easily. If they contain confidential information, they should be protected from internal public view to the extent possible.

There are many companies today that provide document scanning services. Most of them are now regionally based, and local law firms will have a good idea of which companies will do the best job for the best price.

Step 3: Use a document drafting or document assembly application to create new documents. As the Massachusetts Bar Association recommends:

Avoiding “copy and paste” creation of new documents can help keep sensitive information out of documents. If you use a document assembly program to create your documents, you’re even better off, as each document is created “cleanly” from a template that has no personal information in it. ([http://www.massbar.org/publications/lawyersjournal/article.php?c\\_id=1037515398&vt=2](http://www.massbar.org/publications/lawyersjournal/article.php?c_id=1037515398&vt=2))

Some of the better known document drafting and document assembly applications are as follows:

- Ixio Corporation – Ixio Legal Suite (QShift) (<http://www.ixio.com/>)
- Esquire Innovations – iCreate DA (<http://www.esqinc.com/index.php?p=products&id=13>)
- Lexis-Nexis – HotDocs (<http://www.hotdocs.com/>)

## **2. Develop Written Document Retention/Destruction Policy for Clients**

Step 1: Inventory all electronic devices in the organization. This inventory must include peripherals, such as laptops, Blackberries, cell phones, PDAs, voicemails, home computers, that either belong to the organization, or are connected remotely to the organization’s servers.

Step 2: Develop a diagram (schematic) of all inventoried devices and how they are connected (networked). This also includes how devices, and the entire organization’s network, are backed up for disaster recovery.

Step 3: Inventory all software programs used, including manufacturer, program name and version number. Software programs include operating systems, applications, tools and utilities.

Step 4: Prepare an explanation of how the organization’s database works, and what kinds of reporting capabilities it has. This would include any document management systems, and how those systems are organized (by what variables are documents stored and retrieved).

Step 5: Clearly identify what applications (e.g., emails, disaster recovery tapes) automatically delete and/or overwrite themselves, and by what criteria they are deleted or overwritten (e.g., by dates, or oldest emails, or size of email).

Step 6: Clearly state how the organization's database identifies and protects (a) trade secrets and confidential and proprietary information, and (b) attorney-client privileged communications.

### **3. Develop Litigation Hold Policy for Clients**

Step 1: Immediately when any litigation hold is issued, identify and notify key employees of the hold. Do not allow employees to review or collect the information themselves. Prevent spoliation claims by knowing, as soon as possible, where the data that needs to be preserved is located.

Step 2: Collect the required electronic information without changing or destroying any data. This includes the use of third party forensic experts, if necessary, who can use specially designed technology to collect relevant electronic information. It also includes the ability to collect this information without hindering regular daily operations.

Step 3: Document how the electronic information was collected, stored and accessed so it creates a proper chain of custody. Each person involved in the identification and collection needs to describe how the electronic information was located and collected.

### **4. Form Litigation Hold Team**

The purpose of a litigation hold team is to have knowledgeable personnel available to answer the questions of litigators who do not know what they do not know. This team will be responsible for preserving potentially relevant electronic evidence and prevent spoliation. (See, e.g., Tom O'Connor, e-Discovery & Preservation - Take Control!, [http://www.fiosinc.com/resources/pdfFiles/200510\\_edPreservation.pdf](http://www.fiosinc.com/resources/pdfFiles/200510_edPreservation.pdf))

Step 1: Select team members, including legal department members; outside counsel; paralegal or project manager; records management person; senior management; and IT department member. Consider adding third party forensic experts.

Step 2: Assign team members responsible for culling, filtering and de-duplicating data, which will then be processed in a common format.

Step 3: Review processed data, which includes identifying, indexing, excluding data that is confidential and privileged, and analyzing.

Step 4: Finally, the team must tightly supervise the production of data and post-production management of data.

### **Conclusion**

Electronic discovery is here to stay. Because virtually all documents are "born digital," lawyers must educate themselves to be prepared for this new era in the legal industry. The legal requirements are changing, and therefore so lawyers must change.

Proactive and thoughtful preparation will help you avoid the scenario where, "in this age of electronic discovery, we all – plaintiffs and defendants alike – find ourselves hostage to technology." (<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1159866329787>)

We thank you for this opportunity to share with you our research and experiences on electronic discovery. We would very much appreciate hearing from you about your thoughts and experiences. Let us know at [JYand@staffordfrey.com](mailto:JYand@staffordfrey.com) or [ckobayashi@ixio.com](mailto:ckobayashi@ixio.com).