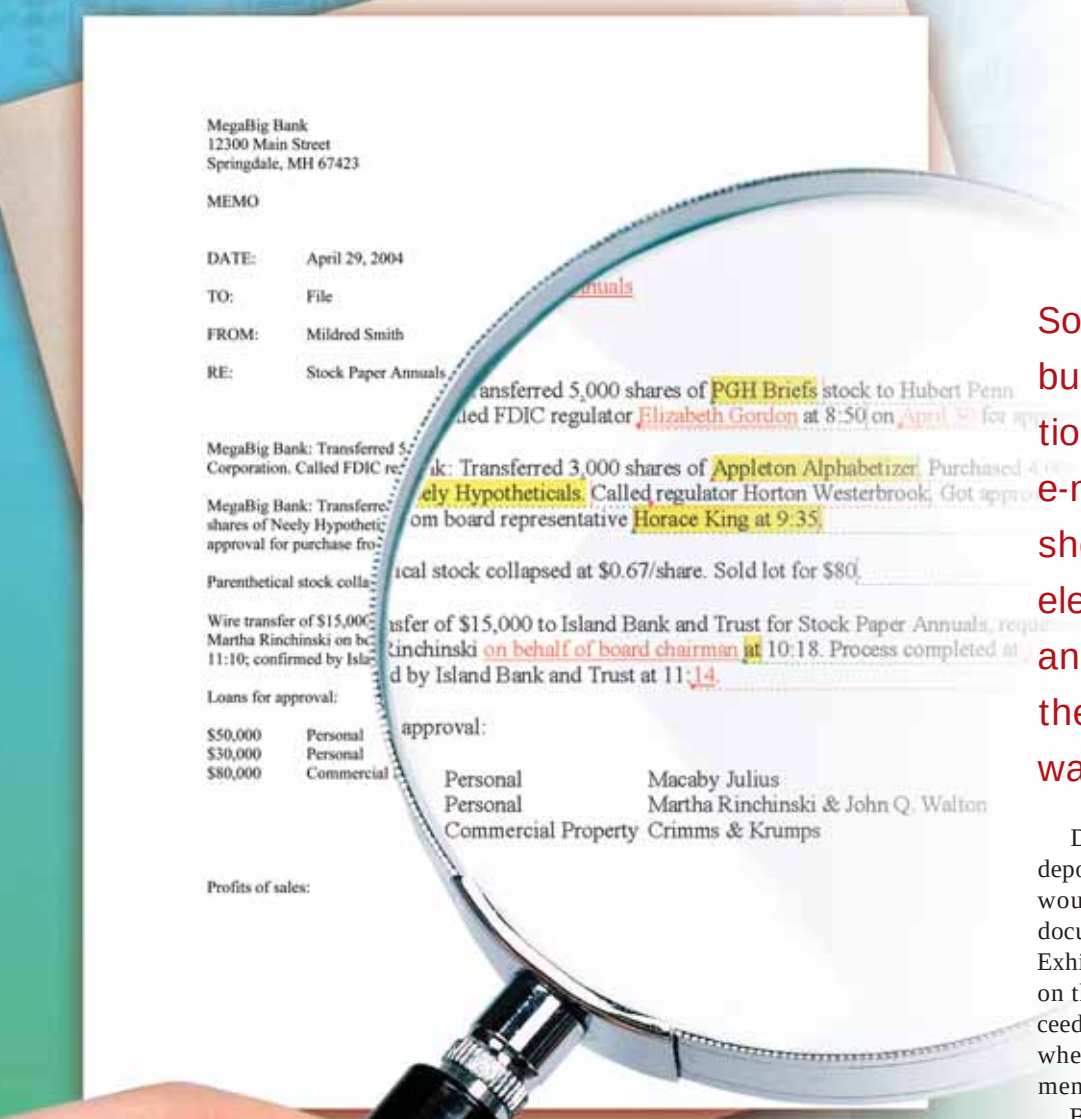
BY NANCY J.

THE ELECTRONIC



So many of today's business communications — letters, e-mails, and spreadsheets — start as electronic documents, and lawyers are using these exhibits in new ways. Are you ready?

During the course of a deposition, deposing counsel asks, "Miss Reporter, would you please mark this original document," a printout of an e-mail, "as Exhibit 1." You place an exhibit sticker on the document, and the attorney proceeds to question the witness regarding when the e-mail was sent, what attachments it bore, and so forth.

But wait a minute. The paper bearing the exhibit sticker is not actually the "original document." In this particular case, Exhibit 1 began life as a Microsoft Outlook electronic e-mail message.

JCR *Contributing Editor Nancy J. Hopp, RDR, CRR, serves as court reporter liaison for Summation Legal Technologies, Inc., a litigation-support software company. Samantha L. Miller, Esq., a former practicing attorney, is Summation's marketing manager.*

EVOLUTION OF EVIDENCE

The fact that nowadays so many business communications have their origins in electronic format — and, indeed, may ultimately never exist on paper — is leading the legal world to rethink its definition of the word *document.* Although not obsolete, the paper paradigm of producing and using hard-copy exhibits is morphing into an electronic model by changing the way attorneys practice law and affecting the products and services offered by reporters.

The e-mail file cited above is an example of *electronic evidence*. Such files contain properties called *metadata* that are generated by software and are not visible on hard-copy printouts. For instance, Outlook e-mail messages contain underlying information disclosing the following:

- Author
- Recipients, including those copied and blind carbon copied
- Subject
- E-mail message
- Date created
- Date saved
- Date and time sent
- Date and time received
- Attachments

Similarly, a Microsoft Excel spreadsheet can be viewed electronically in Excel to reveal the underlying formula of a given cell, information that would not otherwise be visible in hard copy. Microsoft Word documents contain metadata that may reveal a document's author, revision number, date created, date last saved, who last saved the file, how many revisions took place, which program (and which version of that program) was used to create the file, and total editing time, among other things. You can view a Word file's metadata by clicking **File** > **Properties** while viewing or editing the document. (See Figure 1.)

Figure 1

Figure 1: Properties screen of a Word document, showing dates, times, and other statistics

Now imagine how knowledge of this metadata would enable a techno-savvy attorney to probe and impeach a witness's testimony regarding a document's creation and distribution. When you consider the ubiquity of computer-generated documents, can the proliferation of electronic evidence usage at deposition and trial be far behind? In fact, several states have already revised their rules of civil procedure to incorporate electronic evidence as a medium distinct from paper.[1]

WHAT CONSTITUTES ELECTRONIC EVIDENCE?

Several acronyms and terms exist for electronic evidence, such as EDD (Electronic Data Discovery or Electronic Document Discovery), EED (Electronic Evidence Discovery), or e-Evidence. Because electronic evidence is a relatively new topic in litigation, the industry has not yet settled on a common term to describe it. But labels aside, what exactly is electronic evidence?

The most common forms of electronic evidence are file types that people work with each day in their business and personal environments, such as Word documents, e-mails, and Excel spreadsheets. However, electronic evidence can conceivably include digital audio, video or photographs, program codes, database records, voice mail, instant messages, or even global positioning system information.

Writings created, exchanged, or electronically exchanged constitute electronic documents, but a document's existence in electronic format does not necessarily make it electronic evidence. A rudimentary knowledge of computer file formats can aid in understanding this distinction.

TABLE 1. OTHER FORMS OF FILE EXTENSIONS

Native File Format Extension	Originating Application
PST	Microsoft Outlook
NSF	IBM Lotus Notes
XLS	Microsoft Excel spreadsheet
PPT	Microsoft PowerPoint

TABLE 2. CONVERSION METHODS FOR IMAGE FILE FORMATS

Image File Format Extension	Conversion Method
TIFF	Scanner
PDF	Scanner or Adobe Acrobat

Native file format vs. image file format

A document's *native file format* is the format in which it originated. For example, a Word document in its native file format would have a DOC *extension* (e.g., "Hopp complaint.doc"). Table 1 gives other examples of native file format extensions.

An *image file format*, as the term is used here, is more akin to a snapshot of a native file. Two common image formats are *TIFF* (Tagged Image File Format) and *PDF* (Portable Document Format).[2] You may already be familiar with these formats if you currently scan paper exhibits for your clients. Documents in TIFF or PDF format most likely existed as paper or in a native file format before being converted into an image file using a scanner or PDF-conversion software, typically Adobe Acrobat. (See Table 2.) This conversion process is known as *petrification*.

For purposes of this discussion, the term *electronic evidence* refers to documents saved in their native file formats, not image files such as TIFFs or PDFs. Once a document — or spreadsheet or e-mail — has been petrified, it is no longer in its native format, and, therefore, its original metadata cannot be viewed.

Advantages and Disadvantages

Much like beauty, the benefits or drawbacks of presenting evidence in a native versus a petrified format are in the eyes of the beholder. On the basis of cost and recent case law, the current trend is for the techno-savvy litigator to obtain native files in discovery and then to convert relevant native files into images only if redaction is required or the document is being introduced at trial. By initially obtaining and working with native files, the litigator can minimize scanning and copying costs, thus saving money for the client. Given this trend, it seems likely that (1) more evidence will be presented at depositions in native format, while the litigator is still trying to gauge a document's relevance and use the metadata to his advantage and (2) the majority of evidence will still be presented at trial in an image format, given the benefits outlined next.

Image files permit annotations (e.g., redactions, notes, highlighting, and other forms of marking) and are most commonly used in the courtroom with trial presentation software programs. However, when electronic evidence is converted to TIFF or PDF format and becomes an image file, the metadata that was once associated with that document is usually no longer available. This change can be good if you are producing that information, or bad if you are seeking it.

In contrast, native files reveal metadata usually not found in image files or hard-copy documents. This metadata can be used in a case to reveal prior document drafts, which is handy for breach-of-contract cases, and timelines (e.g., when did Smith actually open and read

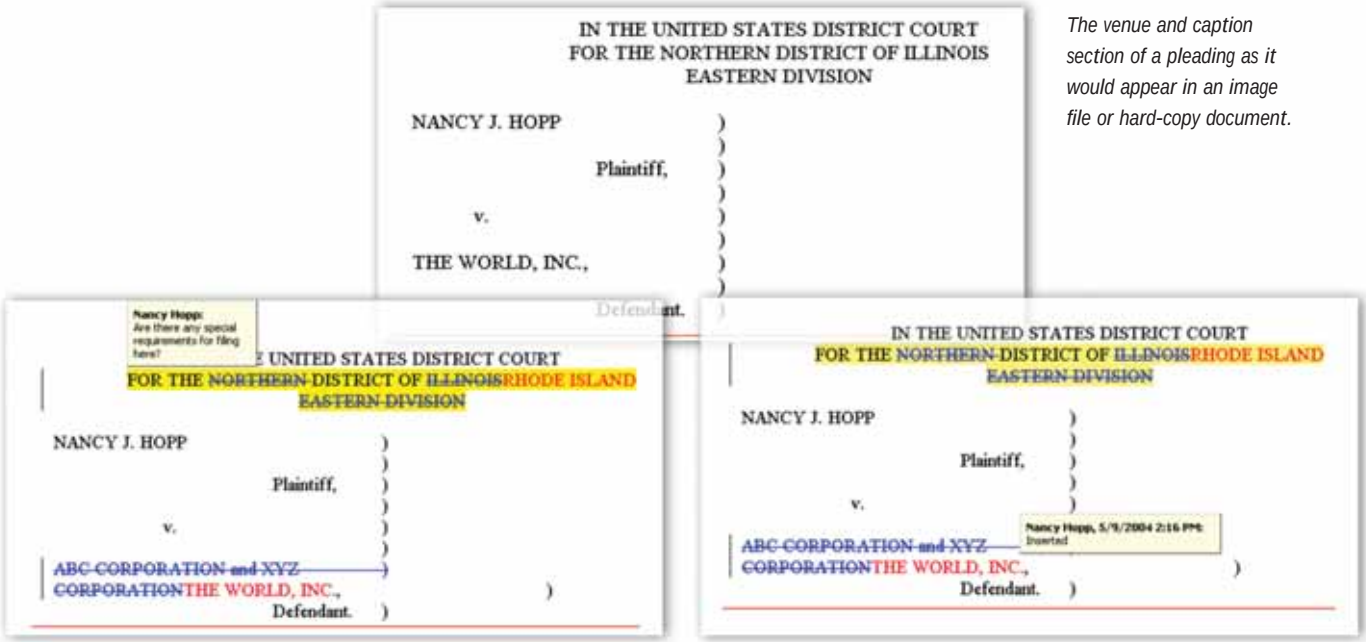
GLOSSARY

electronic evidence — documents originating in a native, or computer-generated, format and containing metadata
extension — a suffix, typically three characters long, following a "." in a filename, which allows computer users and programs to recognize a file's format; e.g., "resume.**doc**"
hidden text — editorial comments or text editing changes electronically concealed from the reader
image file format — a file type for displaying graphics, pictures, or petrified native files
metadata — data about data; descriptive information and statistics embedded in a given computer file
native file format — file format in which a computer file was created
PDF (Portable Document File) — an image format created by Adobe Systems that allows users to view a file with its intended formatting without a need for the program in which the original file was created
petrification — conversion of a file from its original or native format to an image format; also called "tiffification" when converted to a TIFF image
TIFF (Tagged Image File Format) — a common nonproprietary image file format

an e-mail sent by Jones, advising they were doing something unlawful).

In addition, comments and editing changes tracked during the document revision process may be exposed.[3] (For an example, see "An Illustration of Hidden Text" below.) Electronic evidence in native file format is the functional equivalent of capturing each and every marked-up draft of a document, drafts that in a paper-based environment may have been consigned to the shredder. Such *hidden text* is unavailable, however, if the document is printed in hard copy or converted to an image file. Given the option, a safer course for the producing party would be to supply electronic documents in a petrified format.

Bear in mind that in some instances certain metadata can be altered and, thus, rendered unreliable. Also, with the evolution of attendant legal and privacy issues, Microsoft and others have developed software that can remove hidden data from certain files.[4] Nonetheless, electronic evidence is already having an affect on the form in which parties request and produce documents, and many unresolved issues exist regarding its use in litigation.[5] As electronic evidence become more prevalent in litigation, we as court reporters will need to find ways to incorporate it into our work. ■



The venue and caption section of a pleading as it would appear in an image file or hard-copy document.

The same document viewed in its native file format, revealing comments and editing changes, as well as the date, time, and author of such revisions.

ENDNOTES

1. Several Web sites, such as www.kenwithers.com, summarize recent case law and rules regarding electronic evidence.
2. An article titled "Compare and Contrast: PDF versus TIFF," written by Wayne Smith, was published in the December 2002 issue of *Law Technology News*. It is also available online at www.lawtechnews.com.
3. For a real-life example of the perils of producing word processed documents in native file format for the opposing party, see "Hidden test shows SCO prepped lawsuit against BoFA," http://news.com.com/2100-7344-5170073.html.
4. For information on removing metadata and to download a software tool that removes hidden data from various Microsoft files, go to http://office.microsoft.com/home/default.aspx and search "All Office Online" for "metadata" and "remove hidden data."
5. For a discussion of the obligations that could possibly apply to the preservation and production of electronic data and files, see "The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production," www.thesedonaconference.org/miscFiles/SedonaPrinciples200401.