

The Litigator's Guide to Metadata

By Eric R. Harlan

Metadata is a form of electronically stored information that can be used not only to authenticate other electronic evidence but also to challenge the veracity of proffered electronic evidence. However, to be an effective tool for doing either, the metadata itself must be authentic and accurate.

Metadata Basics

Simply put, metadata is “data about data.”¹ The advisory committee note to the 2006 Amendments to Federal Rule of Civil Procedure 26(f) refers to metadata as “information describing the history, tracking, or management of an electronic file.” Examples of such transactional information include “a file’s name, a file’s location (e.g., directory structure or pathname); file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, date of last metadata modification); [and] file permissions (e.g., who can read the data, who can write to it, who can run it).”²

More specifically, metadata could include the type and serial number of the microprocessor of the computer hosting the application (e.g., Microsoft Word or Excel), as well as a Global Unique Identification (GUID). A GUID is:

An electronic fingerprint or serial number placed in the non-printing portions of many documents . . . which identifies the program that created it. It can be used to compare various documents to see if they came from the same source and if that source is positively identified, then the various documents can be potentially authenticated.³

The advisory committee note to Rule 26(f) also speaks of “embedded data” such as draft language, editorial comments, or other deleted material “automatically included in electronic files but not apparent to the creator or to readers.” Unlike transactional metadata, this embedded metadata is generated by the computer user rather than by the machine itself.⁴

Role of Metadata in Litigation

Litigants can utilize metadata to authenticate other forms of electronic evidence, to impeach electronic evidence offered by an opposing party, and as substantive evidence to establish a claim or defense.

For example, with the growing popularity and convenience of digital cameras, photographic

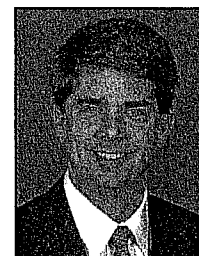
evidence will increasingly take the form of digital images, as opposed to print film images. These photographs may be subject to authenticity challenges given the technology available to manipulate them. In those instances, the image file’s metadata will likely contain information about the camera model used to take the photograph, the original date and time the image was taken, the focal length, and whether any programs were used to enhance or alter the image.⁵ The accuracy of the image can be ascertained with this information.⁶

Metadata analysis can also establish that evidence has been manipulated. In *Plasse v. Tyco Electronics*,⁷ a wrongful discharge suit, Tyco alleged that its discharged employee, Plasse, falsely claimed on his résumé to have earned a Masters of Business Administration (MBA).⁸ Speculating that a recruiter had mistakenly created and provided an inaccurate résumé to Tyco, Plasse denied that his actual résumé contained such credentials, and he produced in discovery a résumé identifying him only as an “MBA candidate.”⁹ On motion, the court ordered Plasse to produce his computers and media storage devices for forensic analysis.¹⁰

Tyco’s computer expert retrieved a deleted résumé from one of Plasse’s floppy disks, identifying Plasse as holding an MBA. Significantly, the file metadata revealed that the résumé was accessed and modified two weeks after Tyco filed its motion to compel, and was deleted before Plasse produced his computer and files a month later.¹¹ Analysis of the security log on Plasse’s laptop computer revealed that two days before Plasse produced the computer for inspection, the system date on the laptop was changed to three specific dates. Coincidentally, file metadata showed that files titled “resume” and “cover letter”—which were no longer accessible—were last accessed on these three dates, suggesting they were accessed and destroyed just two days before production of Plasse’s laptop.¹²

Had the *Plasse* case gone to trial, Tyco could have used the deleted (but retrieved) résumé on Plasse’s floppy disk, together with metadata showing his actions to destroy it, to authenticate the original offending résumé as being authored by Plasse. However, because of Plasse’s blatant manipulation and destruction of evidence, the court, not surprisingly, dismissed Plasse’s suit and provided for sanctions.¹³

In some instances, file manipulation may be so extensive as to prevent metadata from being useful



Eric R. Harlan

Eric R. Harlan is a partner with Shapiro Sher Guinot & Sandler in Baltimore.

Authentication
does not
necessarily
translate into
admissibility.

at all. Such was the case in *Krumwiede v. Brighton Associates, L.L.C.*¹⁴ in which default judgments were entered against the offending party.

There, Brighton claimed that Krumwiede misappropriated a business opportunity and stole trade secrets from it when he went to work for a competitor. Brighton sought production of Krumweide's computer to determine whether its data was used improperly.¹⁵ Forensic analysis revealed that while litigation was pending, Krumweide accessed over 30,000 files and deleted or altered the original file entries.¹⁶ According to Brighton's computer expert, any such file alterations were significant because "the metadata contained in the entry change[d], making it impossible to verify that the file is identical to the original, even if the file's content appears to be unchanged."¹⁷

In sanctioning Krumweide, the court observed that even if the altered or modified documents were not in fact deleted, "the changes to the file metadata call the authenticity of the files into question and make it impossible for Brighton to rely on them."¹⁸

Metadata can also be offered substantively to prove a claim or a defense. For example, in *McClatchey v. Associated Press*,¹⁹ the plaintiff claimed that the Associated Press (AP) removed the copyright notice from her photograph, in violation of the Digital Millennium Copyright Act, before distributing a digital image of the photograph (i.e., a picture of a photo) to its subscribers.

In its motion for summary judgment, the AP contended that the metadata accompanying the digital image stated that the image was a "handout" not created by the AP and further stated "NO SALES, WIDE WORLD PHOTOS OUT."²⁰ Thus, according to the AP, the metadata unambiguously preserved the photograph's copyright protection.²¹

However, in denying the AP's motion, the court pointed out that the same metadata also mistakenly identified the plaintiff photographer as a "stringer," which is a term for a freelance photographer under contract with the AP, and which could lead news outlets to assume that the AP owned the copyright, and not the plaintiff.²²

In another copyright infringement suit, several record companies sued a group of New York University (NYU) students for illegally sharing copyrighted music.²³ In proceedings to compel NYU to disclose the identity of one of the student defendants,²⁴ the record companies relied on metadata obtained from the music files the defendant offered for sharing. This metadata demonstrated that many of the defendant's recordings had been copied from a commercial compact disk to a computer disk (a process called "ripping"), and that the recordings had been ripped by different people using different software.²⁵ The court ruled that

this metadata evidence created a strong inference that the defendant was infringing the plaintiffs' copyrights, which, in part, justified disclosure of the defendant's identity.²⁶

Admissibility of Metadata

Federal Rule of Evidence (FRE) 901(a) states that as condition precedent to admissibility, an item of evidence must be authenticated by "evidence sufficient to support a finding that the matter in question is what its proponent claims." In the case of transactional metadata, authentication can be established, under FRE 901(b)(9), by "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" (i.e. testimony by an authenticating witness [most often a forensic computer expert] that the computer or program's process of creating metadata is functioning as intended); or similarly under FRE 901(b)(1), by testimony of witness with knowledge "that a matter is what it is claimed to be."

Authentication does not necessarily translate into admissibility. Metadata evidence can also be subject to a hearsay challenge. However, the hearsay analysis may be a brief one depending upon whether the metadata in question is transactional or "embedded" substantive data.

Transactional metadata is not hearsay because it is not an out-of-court "statement" under FRE 801(a). It is simply data automatically generated by the computer or program itself in the normal course of use, and thus it is neither an oral or a written assertion, nor is it nonverbal conduct intended by a person as an assertion.

As the Louisiana Supreme Court observed in 1983 regarding a computer log of telephone numbers dialed from a defendant's telephone "[t]he printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants."²⁷


In a 1993 case involving similar computer "phone trace" evidence, The Tennessee Criminal Court of Appeals commented:

[t]he role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.²⁸

By contrast, embedded data input by persons (e.g., prior draft language, comments accompanying

the McClatchey image²⁹) suffice as statements under FRE 801(a), and to the extent they are offered to prove the truth of the matters they assert, must fall under one of the many exceptions to the hearsay rule. Most likely, such evidence would come within the business records exception of FRE 803(6).

Role of the Expert

As illustrated in the discussed cases and the Rules of Evidence, the importance of the expert witness cannot be underestimated. Because of the inherently technical nature of the subject matter, litigants must be prepared with a witness with sufficient knowledge and experience to prove that proffered metadata is what it purports to be, or to demonstrate that the program or system that created it functioned as designed and produced an accurate result. Further, the witness must also be able to explain exactly what the metadata shows and why it is important—whether it be focal length metadata from a jpeg image to authenticate a photograph for accident reconstruction,³⁰ or music-ripping software metadata to establish copyright infringement.³¹ 

Endnotes

1. See, e.g., *Netword, LLC v. Centraal Corp.*, 242 F.3d 1347, 1354 (Fed. Cir. 2001) (“Metadata” is a term for data that, in turn, describe other data).

2. *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, App. F n.1 (The Sedona Conference Working Group Series, Sept. 2005 Version), available at http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf.

3. Scott M. Giordano, *Authenticating Electronic Evidence in California and Federal Courts*, Case ‘n Point Newsletter, Issue V.7 (Continuing Education of the Bar—California), available at http://ceb.com/newsletter7/Civ_lit.htm.

4. See, e.g., *Celerity, Inc. v. Ultra Clean Holding, Inc.*, 476 F. Supp. 2d 1159, 2007 WL 632711 (N.D. Cal. 2007) (discussing party seeking to obtain metadata associated with opinion letter, which metadata would contain language of earlier drafts).

5. See Joe Kashi, *Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata*, Law Practice Today (ABA Law Practice Management Section, June 2006), available at <http://www.abanet.org/lpm/lpt/articles/tch06061.shtml>.

6. See *Id.*

7. 448 F. Supp. 2d 302 (D. Mass 2006).

8. *Id.*, at 303.

9. *Id.*, at 304.

10. *Id.*, at 306

11. *Id.*, at 306.

12. *Id.*, at 307.

13. *Id.*, at 311

14. 2006 WL 1308626 (N.D. Ill) (unreported).

15. *Id.*, at * 1.

16. *Id.*, at * 4.

17. *Id.*

18. *Id.*, at * 10.

19. *McClatchey v. Associated Press*, 2007 WL 776103 (W.D. Pa. March 9, 2007).

20. *Id.*, *2.

21. *Id.*, *5.

22. *Id.*, *2 at n.3; *5.

23. *Elektra Entertainment Group, Inc. v. Does 1-9*, 2004 WL 2095581 (S.D.N.Y. September 8, 2004) (unreported).

24. The plaintiff record companies were able to gather certain information about the defendants by logging on to the file sharing networks in which the defendants participated, but were not able to gain identifying information beyond the Internet Protocol (“IP”) address from which each defendant was sharing music files. *Id.*, at *2.

25. *Id.*, at *4.

26. Of course, matters revealed by metadata do not always support a party’s claims. See, e.g., *Michael J., et al v. Derry Township School District*, 2006 WL 148882 (M. D. Pa. 2006) (unreported) (parents argued that metadata contained in school’s Notice of Recommended Educational Placement (NOREP) for their child demonstrated that the school violated procedure because metadata showed that the document that became the NOREP was first created prior to the school’s Individualized Education Plan hearing. The court found that the subject metadata indicated merely that school began formatting the document ahead of time, and that school nonetheless engaged in good faith effort to evaluate child); See also *Turner v. Resort Condominiums International, LLC*, 2006 WL 1990379 (S.D. Ind. 2006) (unreported) (plaintiff claimed unsuccessfully that metadata indicating that one of employer’s reduction in force (RIF) lists was modified after plaintiff filed pregnancy discrimination lawsuit permitted inference she was placed on RIF list only after the employer discovered her pregnancy. The court found that other evidence indicating plaintiff was always on the RIF list negated plaintiff’s metadata argument).

27. *State v. Armstead*, 432 So. 2d 837 (La. 1983).

28. *State v. Meeks*, 867 S.W. 2d 361, 376 (Tenn. Crim. App. 1993).

29. See *McClatchey v. Associated Press, Inc.*, ___ F. Supp. 2d ___, 2007 WL 776103 (W.D. Pa. March 9, 2007), *supra*.

30. See Kashi, *supra*, at n.5.

31. *Elektra Entertainment Group, Inc. v. Does 1-9*, 2004 WL 2095581 (S.D.N.Y. September 8, 2004) (unreported).