Metadata in Digital Photos – Should You Care?

by Sharon D. Nelson, Esq. and John W. Simek

We are hopeful that you are familiar with metadata, especially as it exists in e-mail messages and word processing files. If not, then a brief refresher is in order. There are a couple of different types of metadata, but most regard the common definition to be data that is stored internal to the file (you can't see it without knowing how to look at it) and is not explicitly defined by the user. The application (e.g. word processor) inserts data within the file such as the author, last time printed, fonts used or creation date. But what about image files such as those taken with digital cameras? What metadata do those files contain?

Digital photos can be an electronic evidence heaven. Digital image files typically contain information about the date and time the photo was taken, camera settings such as aperture and shutter speed, manufacturer make and model (and often the serial number) and in the case of smartphones, the GPS coordinates of where the photo was taken (pure evidentiary gold in many cases). This metadata is called Exif (Exchangeable image file format) and is a standard that specifies formats for files recorded by digital cameras. None of this information is added by the user at the time of file creation. As you can see, the information could be extremely valuable, especially in litigation.

Since we've established that metadata does exist in digital image files, should you care? It depends on whether you are the originator or the recipient of the information. The metadata could be extremely dangerous if revealed through social media channels, especially if the user is unaware of the consequences. Here's a real world example. Adam Savage is one of the hosts of the popular science program, MythBusters, on the Discovery Channel. He posted a picture of his automobile parked in front of his house on Twitter. Even though Adam is a "science" guy, he apparently didn't know or simply forgot that his photo revealed more information than the fact that he drives a Toyota Land Cruiser.

Embedded in the picture was a geotag, which provided the latitude and longitude of where the photo was taken. Since he announced that "Now it's off to work," a burglar would know that he was not at home and the geotag would also pinpoint where he lived. Adam certainly dodged a bullet.

Then there's the famous story of the leaked *Harry Potter and The Deathly Hallows* book. Someone took a digital photo of each and every page and posted the entire book on BitTorrent networks such as Pirate Bay. Lucky for the photographer that they haven't been caught, but they sure left behind a lot of electronic breadcrumbs. The metadata tells us that the camera he (we suspect a he since part of their hand and fingers are in many of the photos) used a Canon EOS Digital Rebel 300D camera running firmware version 1.0.2. The camera serial number is 0560151117. Canon identified the camera as being three years old and it had never been serviced. We're sure that the camera is at the bottom of some river by now since it could lead the authorities to the owner.

Probably the most famous Exif story is that of John McAfee. While on the run from authorities in Belize in connection with a murder investigation, he allowed a journalist from a shady website to take a photo

of him, which was then posted on the website complete with its Exif data. Turned out he was in Guatemala, where he was promptly detained and later deported to the U.S.

For those of you who care to know (and it seems everyone does), photos that are posted to Facebook or Twitter currently are stripped of their Exif metadata. On the other hand, Google+ preserves it.

We have many more metadata stories, but you get the picture [bad pun]. Digital image metadata is not readily viewable by the casual viewer. Perhaps that is the reason why we still find a plethora of metadata in the electronic evidence that we analyze for our cases. So how do you identify what metadata exists in the electronic file and is there a way to clear it out?

Viewing the metadata requires that you open the digital image in a piece of software that can readily show you the metadata values. You probably don't even need to spend any money to do so. You can use the included Windows Live Photo Gallery or Windows Photo Viewer if you are running Windows 7. Once the file is open, just go to File, Properties to see a lot of the metadata values, including GPS location information if it exists.

But what if you don't want to distribute the Exif data with the file? How do you get rid of it or at least change it? The function to modify the data as well as remove it is included in your Windows environment. If you right click on a file and select properties then the details tab, you have the opportunity to change or delete much of the embedded metadata. There is even a link at the bottom of the panel that will "Remove Properties and Personal Information." You can use this hyperlink for an individual file or for all files in a folder. Once you click on the hyperlink, you can create a copy with all possible properties removed or selectively remove specific properties. There is also a free Windows utility called QuickFix (http://www.metabilitysoftware.com/products/metability-quickfix.html) that will strip GPS and other metadata from the image file. Give it a try, especially since it's free and supports drag and drop. Finally, you can install a product like Litera's Metadact-e, which will clean metadata from document files as well as image files.

No matter what approach you take, don't just focus on the metadata in your word processing and spreadsheet files. Those digital photographs can hold valuable nuggets as well. Just ask John McAfee.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com