NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the Office of Justice Programs' National Institute of Justice
From Winter 2007 *TechBeat*
TECH b•e•a•t
Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

EXIF: A Format Is Worth A Thousand Words

The National Center for Missing & Exploited Children revealed in a June 2005 study that 40 percent of arrested child pornography possessors had both sexually victimized children and were in possession of child pornography. Due in part to the increasing prevalence of child exploitation and pornography, the digital photograph has now become a fixture in gathering and examining forensic evidence in such cases.

Investigators who frequently handle child pornography cases usually have (or know where to access) the tools and the knowledge to obtain evidence associated with contraband images. Nevertheless, law enforcement officers who do not handle these cases on a regular basis may be unaware of the important data that can be derived from digital images.

Exchangeable Image File Format, "Exif" for short, defines the file structure and metadata tags used by digital cameras. The Exif standard, originally created to enhance interoperability between photographic imaging devices, can be found in both JPEG and TIFF files.

The Exif standard associates a variety of information with a photograph, such as the date and time the image was taken and the make and model of the digital camera used. It also stores camera settings such as shutter speed, film speed, flash settings, aperture, focal length, and metering mode. A less common feature is the inclusion of global positioning satellite coordinates that provide the exact location where the picture was snapped. Thus, law enforcement can use Exif data to find out when a photograph was taken, tie photos to a specific make and model of camera, or pinpoint the location where an image was created. More advanced techniques can identify the owner of a specific camera by extracting its serial number.

Currently not all digital camera manufacturers support the standard, although makers of many popular brands, such as Nikon, Sony, Canon, Fuji, HP, and Olympus, have adopted it. Many image editing programs (such as Microsoft® Paint) ignore Exif data embedded in a photo if they are used only to open the file. If, however, these programs are used to modify an image, they can destroy the Exif data.

The most important data may be the thumbnail image linked to the photograph. Thumbnails are saved in their own hidden file (a thumbs.db file placed in folders containing images on the computer), and changes to an image may not always transfer to the corresponding thumbnail. If an original image is wiped from a disk using a program such as Secure Clean™ or BCWipe®, the thumbnail may still be available. Officers have encountered situations in which the victim's or perpetrator's face was blurred or concealed in the full image, but the thumbnail depicted an older version that revealed the obscured area.

The Exif standard also supports data called "makernotes." These data fields and their values are unique to each digital camera manufacturer. They can help determine if a suspect has tampered with Exif data in an attempt to prevent linking images to a specific digital camera. For example, encountering an image with the Exif data of a Canon camera and the makernotes of a Nikon would indicate that fields have been modified.

Several tools facilitate the extraction and analysis of Exif data and image thumbnails. Exifer, ThumbsPlus®, Jhead, EXIFextracter, Exif Reader, ExifPro, and IExif® are just a few of the many free or inexpensive tools available on the Internet. Additionally, many commercial forensic applications such as ProDiscover® and DataLifter™ now include Exif data analysis as one of their capabilities.

For more information on Exif data, photo metadata, or image analysis tools, contact Salvatore Paladino, CISSP (Certified Information Systems Security Professional), at the National Law Enforcement and Corrections Technology Center–Northeast in Rome, New York, 888–338–0584 or sal@dolphtech.com. Visit www.missingkids.com for more information about the National Center for Missing & Exploited Children.

This article was reprinted from the Winter 2007 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #2005–MU–CX–K077, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.