Using SDFI's Negative Invert Filter In Court

Dear Reader,

It is our pleasure to share known and accepted legal information about SDFI's Negative Invert Filter in the following pages. Please use this information to educate other professionals within your fields of excellence including technology, medicine and law.

Filters **CANNOT AND DO NOT** determine intent or cause, consent or non-consent, guilt or innocence, diagnose or analyze or distinguish right from wrong. They simply help you see better.

EXECUTIVE SUMMARY - Digital Photography and Image Enhancement

Digital photography and image enhancement has a history that goes back to circa 1965. Images and image enhancement has been part of the U.S. court system long before forensic photography went digital. Film based forensic photography tools are now hard to come by as film based photography has been replaced by imaging systems like SDFI®- TeleMedicine, a combination of photographic image capture tools, image management and security software and secure File Portal/TeleMedicine communication tools.

SDFI has 15 years of history and use within the industry, yet only now within the last five years are legal professionals showing interest in SDFI's Negative Invert Filter. The number one legal question is "Can the SDFI Negative Invert Filter be used in court" and the answer is a resounding "Yes". Image enhancement is widely accepted and used in court as the following pages will show and prove beyond a reasonable doubt.

Please review the following collection of documents and references to further your knowledge and education on the subject of image enhancement and its use in the legal system.

http://www.sdfi.com/downloads/Using_The_SDFI_Negative_Invert_Filter_In_Court.pdf

Sincerely,

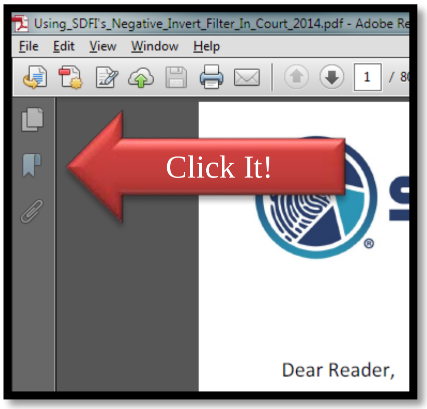
SDFI-TeleMedicine
806 Buchanan Blvd   STE 115-299
Boulder City, Nevada 89005
E-Mail: Support@SDFI.com
Phone: 310-492-5272

Table of Contents

How Best To Use This Document:

Download the document and open it a PDF Reader, press "CTRL-F" and search for a word or phrase. As an example, search for "**Case Law**". If you find it, review the section and then search again. Look for other yellow highlighted areas of interest.

Also, use the built-in bookmarks to find a title or section.


Using_SDFI's_Negative_Invert_Filter_In_Court_2014.pdf - Adobe Re
File
Edit
View
Window
Help
1
/ 8
Click It!
Dear Reader,

If you print, "Print in Color".

Filters ***CANNOT AND DO NOT*** determine intent or cause, consent or non-consent, guilt or innocence, diagnose or analyze or distinguish right from wrong. They simply help you see better.

Forensic Image Processing

An Introduction to Image Enhancement

As technology is brought to bear upon the problem of latent fingerprint recovery, combinations of existing techniques will be joined with new systems to improve the recovery rate on traditionally difficult surfaces. The distinction between Automated Fingerprint Identification Systems (AFIS) and recovery systems will begin to blur. The amount of time necessary to conduct crime scene investigations and recover physical evidence will decrease, while the overall quality of the evidence will continue to increase. The next major advancement in the history of the Science of Fingerprints is about to be recorded. It will be known as digital image enhancement.

Imaging can be divided into three main categories. The first is film based photography. The second is electrical analog or video. The third is digital.

Film based photography uses a lens to focus light onto a chemically treated piece of acetate, which changes in relation to the quantity of light striking it. Colored filters and controlled lighting techniques can be used to effect the way an image is exposed. Once exposed, the acetate, also known as film, must be chemically processed to produce a visible image. This is a lengthy and expensive process requiring two to three hours just to produce a print.

Video images are produced when light is focused through a lens and onto a light sensitive chip called a charged couple device (CCD). The CCD chip converts the light into a series of electrical signals. These electrical signals are then recorded onto a magnetic media, such as video tape, or displayed directly on a video monitor. As with film based photography, lighting techniques can be employed to help control how the image is recorded, but once recorded, only limited image enhancement is possible.

Digital images are made up of a series of numerical values, each representing a specific light intensity and color. Similar to the video process, a CCD chip is usually employed to convert an image to electrical impulses. A converter then translates the electrical signals to numerical values. A picture element (pixel) is used to represent each numerical value so that an image can be displayed on a computer monitor. Pixels are used to control the display of a computer screen in much the same way that light bulbs are used to control the display of reader board type signs. By turning on a row of light bulbs it becomes possible to create letters and shapes. By turning on and varying the color and intensity of a pixel, and then assembling a group of pixels into a mosaic, it becomes possible to create an image on

ALSO INSIDE:

LEGAL ISSUES AND COURT CASES.

a computer screen. By changing the numerical value of a group of pixels, we can change the way the image appears to the viewer.

Images can be recorded for enhancement purposes using a variety of methods, including all of those outlined above. The only prerequisite is that before an image can be introduced into a computer it must be digitized or converted to numbers. There are numerous devices available for doing just that. If you have a photographic negative, a film scanner or, in some cases, a flatbed scanner can perform the operation of turning colors and levels of gray into numerical data. Other equipment is available for converting video images. By far the easiest method is to use a digital camera to capture an image and simultaneously convert it to digital information. The method chosen depends on the specific application and the image quality required.

If you know how to use a photocopy machine or a 35mm camera, you're well on your way to learning the mechanics of recording a digital image. Once an image is digitized, you can exert a great deal of control over how certain elements within the image appear to the human eye. Very small details can be brought out of a dark background without affecting the rest of the image. Specific colors can be identified, isolated and, if necessary, changed or removed.

The human eye is only capable of distinguishing between 30 and 50 different shades of gray. The exact number is dependent upon the person's age and eye sight. A typical digital camera is capable of recording 256 different shades of gray. Much of this subtle information often goes unnoticed by the human observer, because of the eye's inability to distinguish the fine nuances of tone. When an image is recorded in color, the human eye has an even more difficult time trying to distinguish between subtle tonal and color differences found in supposed true color images containing up to 16.7 million different colors. By knowing the limitations of the human eye we can begin to understand why the computer might have an advantage in finding detail in an image that would otherwise elude detection.

A computer sees an image only as a group of numbers. In the case of a gray scale image, absolute black is represented by 0 and absolute white is represented by 255. The image is displayed on a screen in shades of gray only for the convenience of the human operator. What may look like medium gray to the operator (the word medium itself is open to wide interpretation) is seen as an absolute numerical value by the computer. There is no interpretation or subjective opinion involved. By moving a cursor around an image, the computer will display the numerical value for whatever portion of the image the cursor happens to be hovering over. In some cases this can be as small as one or two pixels. To put that in perspective, the FBI's minimum requirement for a digitally captured fingerprint card is 500 pixels per inch. That means that within the space of one square inch we can find 250,000 dots. A fingerprint card is usually 8 inches by 8 inches. That means there are 16,000,000 dots defining that single fingerprint card. For latent fingerprint work, I would recommend capturing images at significantly higher rates, but even at 500 pixels per inch, you begin to fathom just how small a pixel is. A tool that can selectively measure detail that small is something every Forensic Expert should be interested in.

Using the computer to help uncover subtle details in an image that we might otherwise miss is analogous to a person who wears eye glasses to overcome a problem with limited vision.

Computer Issues

What kind of computer do I need?

Image processing can be very taxing on a computer's central processing unit (CPU). A simple sharpening filter operation can require thousands of mathematical calculations per second. This can slow down even the most powerful CPUs. When selecting a computer, specify the most powerful CPU available. Currently, the Intel Pentium series is considered the most powerful on the PC platform.

Digital images tend to be large and as a result use lots of random access memory (RAM). What this means is that you won't be able to use a computer designed for word processing and games to do image enhancement. You will need lots of memory and lots of hard drive storage space.

Minimum memory (RAM) requirements can be based upon the following guideline. Take the size of a typical image and multiply by three. Add four megabytes for your operating system (DOS and Windows) and 6 to 8 more megabytes for the imaging software. The total would represent a practical minimum specification for an imaging computer. Using this example, if we typically work with images that are 4 megabytes in size and we multiply by three, add four and then another 8, we come up with 24 megabytes. This would be a functional minimum. As little as 16 megabytes would probably still work, but would hinder some functionality and productivity would suffer. As with some other things in life, more is better. Get as much RAM as you can afford.

Given the drop in price of hard drives, it doesn't make sense to buy anything less than a 1 gigabyte hard drive for image storage. As with RAM, more is better.

Listed below are some general specifications for a computer that is going to be used for image processing:

Pentium 100 or better processor
32 megabytes of random access memory (more the better)
2 gigabyte hard drive
SVGA video card with 2 megabytes of VRAM (4 megabytes is better)
17" color monitor with a .28 or better dot pitch (21" monitor is really nice)
Tape storage device for backing up hard drive data

Additional features are available, but this would serve as a good platform upon which to build. Various input devices, such as flatbed scanners, digital cameras and film scanners, are also available and selection should be based upon specific needs.

Software Issues

What kind of software do I need?

Imaging software can reasonably be compared to a tool box. There are a variety of hammers available for pounding nails, but each one is designed to accomplish a specific job, such as roofing or framing. Imaging software is a collection of tools designed to manipulate and analyze images on a computer. Software programs generally offer a set of tools. Some tools are unique to a particular program, while others can be found in all programs. The choice of which programs to use is based partly on the application's features and partly on personal preferences. Several questioned document examiners in Oregon prefer the tools found in Micrografx Picture Publisher, while I prefer Adobe's Photoshop for day to day image enhancement. There are numerous other software programs available.

A toolbox that contains a seemingly esoteric array of tools designed for infrequent tasks may seem overly burdened, until the day its owner requires the function of a wrench designed to remove spark plugs from a 1929 Ford. Just as a veteran mechanic reaches confidently for his wrench, the Forensic Imaging Expert grabs a mouse to activate the rarely used pattern removal filter so she can identify a particularly difficult latent print.

The only wisdom I can offer here is: Choose your day to day software for the range of tools it offers, but don't be afraid to collect other software along the way.

Expanding Possibilities

Now that you know how a digital image is created, lets talk about how we can use this capability to make other image related tasks easier and faster. A photo montage used to mean copying an assortment of photos from various sources on Polaroid film so all the images appeared to come from the same source. The results were generally poor and expensive, costing about $1 per print. Using a digital camera or scanner, it is possible to scan each image and then adjust them individually so each more closely matches the rest. Color balance, contrast and image sharpness can all be adjusted easily and quickly. The resulting images can then be printed inexpensively on a laser printer.

One task all latent examiners share in common is the need to prepare court displays of latent fingerprint comparisons. The traditional process of film based photography and manual drafting techniques can take hours. Using a digital camera or scanner and Adobe Photoshop, the whole procedure can be accomplished in an hour. Lines and numbers are drawn on screen in any of up to 16.7 million colors. If a line or number is misplaced, it can be erased and redrawn easily without leaving a trace of the original error. Once completed, the chart can be printed in color or black and white. It can also be printed on acetate for projection on an overhead projector. The savings in time and materials can be significant.

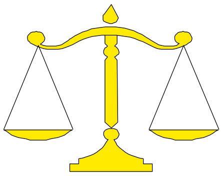
You're not limited to just fingerprint charts. Any application that requires the combining of images, text and line art can be performed using a digital capture device and a computer. DNA and ballistics can both benefit from the speed and quality of digitally prepared exhibits. A little imagination can expand significantly upon the examples presented here.

5

Legal Issues

Chain of Custody and Case Law

Any evidence that is going to be introduced into a legal proceeding brings with it a potential argument over its origin and the inevitable *chain of custody*. With digital imaging there is the added element that the original image cannot be touched or examined directly since unlike traditional photography, a film negative is not produced. Without the proper computer software the digital file sits invisibly on the computer's hard drive or other storage medium. Because of this it is very important to track the history of any digital image captured for evidence purposes. The date and time the image was captured, as



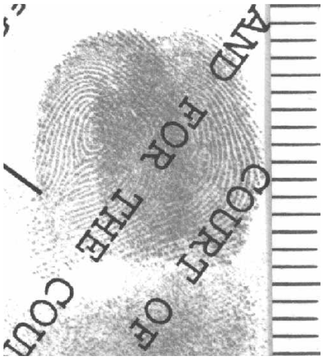
well as who captured it should be kept in a secure location. When the image is enhanced, it is important to record who enhanced it and when. Record the procedures used to enhance the image so that, if it becomes necessary several months or even years later, the procedure can be repeated for the defense and the court. Under no circumstance should the original image be compromised during enhancement procedures. A copy should be made of any original image to be enhanced. Enhancement is then carried out using the copy. By using this procedure, if anything happens to the image, it is always possible to go back to the original image. By maintaining both the original image and the enhanced version it becomes an easy task to satisfy disclosure requirements. It is also relatively easy to demonstrate the entire procedure for the defense or even a jury. By following this simple protocol and limiting access to your images you'll avoid the need to answer a whole series of questions, which can only lead to the eventual suppression of the evidence you worked so hard to recover.

One question you should expect to answer in court , "Is digital image enhancement technology generally accepted by the Forensic Profession?" This question is the basis of a Kelly-Frye Hearing and is normally asked by the defense in an attempt to have the evidence suppressed. In some cases the prosecutor may pose the question first in order to head off the argument. The litmus test : *Is the technology used based upon sound scientific principles that are generally accepted by the profession* ? The answer to this question should be obvious, but the reasons may not be so apparent.

The technology used to enhance a latent fingerprint is the same technology developed by NASA in the early sixties to record galaxies and space missions. At that time imaging was an expensive and time consuming undertaking. The drastic reduction in size and cost of modern computers has enabled the technology to spread. A modern weather satellite produces digital images of the earth every 15 minutes. Commercial and Military aircraft use this information to make navigational choices. Ordinary citizens use the information to plan their fishing and camping trips. The accuracy of the information is well tested.

There have been numerous articles published in both The Journal of Forensic Identification and the Journal of Forensic Sciences documenting both the techniques used in digital image enhancement and the acceptance of the technology by the forensic profession. There are also two precedent setting criminal cases that involved the identification of digitally enhanced latent fingerprints. We'll discuss those cases and how they may affect you a little later.

Explaining the technology in terms a jury can relate to will help fend off attempts by the defense to confuse and misdirect the jury. Another tactic you will see used is the result of ignorance. An allegation will be made that a latent print was changed during the enhancement process, either deliberately or unknowingly, resulting in the misidentification of the defendant. There could also be an allegation that the computer made a change to the image without the expert's knowledge. All of these arguments are pure fantasy. Television creates a mystic about the computer and the general public, without personal knowledge to the contrary, believes it. A computer does only what it is programmed to do. Changing a fingerprint by moving minutia is relatively easy. Moving those minutia, so that the print is identified as someone other than the person who left it and in a manner that would not be easily discovered, would be difficult and very time consuming. If it was attempted and the result introduced as evidence, it would be the result of a criminal act, not a consequence of renegade computer technology.



Applicable Case Law

Cases that establish a precedence for image processing

There are two cases that establish a precedence for the acceptance of digitally enhanced evidence in American criminal proceedings. The first is Commonwealth of Virginia vs. Robert Douglas Knight. This 1991 murder case involved the enhancement of a bloody fingerprint found on a pillow case at the crime scene. A company called Hunter Graphics (no longer in business) was contacted by the Henrico County Police Department to assist in the enhancement process. Experts from Hunter Graphics used a frequency filter known commonly as a Fast Fourier Transform (FFT) to subtract the fabric pattern that interfered with the identification of the fingerprint. The fingerprint was subsequently identified as belonging to Robert Knight. After being charged with the crime, Knight's attorney moved for a a Kelly-Frye Hearing to determine the scientific validity and acceptance of the enhancement process. The determination of the court was that the techniques used were essentially photographic processes. Robert Knight plead guilty and was sentenced to four life terms.

The second case is State of Washington vs. Eric Hayden. This case involved the murder of a young missionary in her apartment. The murder took place in the small bedroom community of Kirkland, WA. The detective in the case requested the assistance of the King County Police (Seattle) to process the crime scene for latent fingerprint evidence. After collecting and later processing a bed sheet found at the crime scene, several faint prints were found. But, because the ridge detail was very faint and the fabric pattern of the sheet interfered with attempts to compare the prints, an identification was not possible. King County contacted the Tacoma Police Department for assistance in enhancing the latent prints. A combination of techniques, including a Fast Fourier Transform, were used to enhance a palm print and two fingerprints that had been developed on the fabric using Amido Black. All three prints were later identified as having been made by Eric Hayden.

The attorney representing Hayden raised a number of issues during a Kelly-Frye hearing held on December 13, 1995 to determine the admissibility of the fingerprint evidence. One issue raised was the *manipulation* of the images and whether or not the prints had been altered to match his client. The manipulation question was answered by first explaining how an image is recorded and then enhanced. To answer the more disturbing question regarding the deliberate changing of an image, so that it will be identified to the wrong person, it was pointed out that in spite of what may appear to be possible, due to the influence of television, it is quite impossible to change a fingerprint in such a way that it will both be identified as having been made by a person other than the person who actually left the print and not be readily detected. In addition, at no time did the person doing the enhancement work ever see inked fingerprint cards of any of the suspects in this case. The argument then shifted to a variation of the original argument, namely, *the computer made changes to the image without the expert noticing.* To neutralize this equally silly argument a demonstration was performed using the actual fingerprint evidence on the bed sheet. An image was captured using a digital camera setup in the court room. The image was then tracked using *PC PROS' MORE HITS Image Tracking System* to maintain an unbroken chain of custody, while changes made to the image were recorded using specific features of the software. This software package pre-empted the defense attorney's remaining questions regarding the unauthorized tampering and changing of images and the protection of the chain of custody.

State of Washington vs. Eric Hayden serves as an affirmation of the conclusion reached in the Commonwealth of Virginia vs. Robert Douglas Knight case. It also imposes the same requirements for digital images as those placed upon other types of evidence. There must be a documented and secure chain of custody maintained for every image introduced into a legal proceeding. Aside from testifying that an image is a fair and accurate representation of the item it depicts, the expert must also be able to document the steps taken to protect the image from tampering by unauthorized persons. Any enhancement techniques used must be reproducible, so that notes about the enhancement process, as well as who did the work, should be maintained.

To those experts who are familiar with the legal requirements of other types of physical evidence, none of the findings in the Hayden case should come as any great surprise. To those who have not been applying the same chain of custody procedures to electronic images, as are applied to other forms of evidence, be forewarned that a continuation of this practice could endanger the success of future prosecutions where image enhancement is used. By establishing secure procedures for the capture and protection from tampering of original images, as well as the recording of enhancement techniques, you will avoid having to answer difficult questions in court. By having a defensible procedure in place the only questions left open to the defense will be where the print was recovered. The goal in imaging should be the same goal all forensic experts strive for: *a stipulation to the facts*.

Other Sources of Information

Books and Periodicals

There are dozens of books covering the subject of digital imaging. Most contain information that is potentially useful to the Forensic Professional. The majority of these books fall into two broad categories. The largest of these is the graphic arts field and all its related disciplines. The other category is a combination of academia and commercial applications. The commercial publishing business has been using electronic imaging for more than 10 years to produce illustrations for books and magazines. Newspapers have been exchanging wire service photographs for publication world wide since 1921 when the first photograph was sent via the Trans-Atlantic Telegraph from a coded tape and printed by a telegraph printer with special type faces. The Associated Press recorded the Winter Games in Lillihammer, Norway using custom built digital cameras. Images were uploaded using laptop computers to a satellite and sent back to New York for distribution and publication in newspapers all over the world.

I have listed several books and periodicals below that contain information useful to the forensic professional who is interested in applying digital imaging technology. Some of these sources are general in scope while others delve deeply into the dark mathematical intricacies of digital image processing.

Periodicals:

Erik Berg, *The Digital Future of Investigations*, Law Enforcement Technology, Aug. 1995, pp. 38 - 40.

Erik Berg, *Latent Image Processing - A changing technology*, The Pacific NW IAI Examiner, April 1994, pp. 12 - 15.

Brian Dalrymple, *Computer Enhancement of Evidence Through Background Noise Suppression*, Journal of Forensic Sciences, Vol. 39 No. 2, pp. 537 - 546.

George Reis, *Digital Cameras Raid California Crime Scenes*, Photo Electronic Imaging, Oct. 1993, pp. 22 - 27.

Norman Tiller, *The Power of Physical Evidence: A Capital Murder Case Study*, Journal of Forensic Identification, Vol. 42 No. 2, pp. 79 - 83.

William Watling, *Using the FFT in Forensic Digital Image Enhancement*, Journal of Forensic Identification, Vol. 43 No. 6, pp. 573 - 583.

Books:

Gary David Bouton and Barbara Bouton, *Inside Adobe Photoshop 3*, New Riders Publishing, New York, 1995.

Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Addison-Wesley Publishing Company, New York, 1993.

Armin Lange, *Computer Aided Text-Reconstruction and Transcription*, J.C.B. Mohr (Paul Siebeck), Tubingen, Germany, 1993.

Wayne Niblack, *Digital Image Processing*, Prentice/Hall, New York, 1986.

Nikon, *Scanning Essentials - The Nikon Guide to Desktop Film Scanning*, Nikon, New York, 1994.

Sid-Ahmed, *Image Processing*, McGraw Hill, New York, 1995.

10

Written by Erik Berg

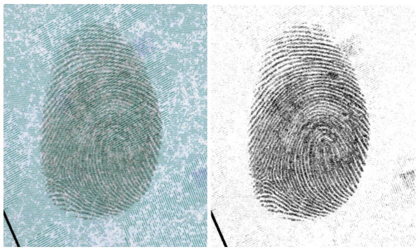
Digital Image Integrity

TABLE OF CONTENTS

The integrity of a digital image is paramount in fields such as forensic, medical imaging, military, and industrial photography. Courts make decisions affecting an individual's liberty based, in part, on images presented as evidence. Physicians and researchers make diagnoses based on imaging—holding people's lives in the balance. Military photographs may be used to determine target locations based on their content and interpretation. Industrial photographs depict defects in materials that could lead to faulty and dangerous consumer products if not discovered.

Because it is frequently necessary to make corrections and adjustments to images (for example, to separate one type of cell from another, or to enhance a fingerprint), it is important to maintain the integrity of images from capture through final usage. To address this issue, the creator of an image can follow best practices that maintain an archive image, restrict access to the archive image, require work to be done only on copies of the archive image, and then provide an audit trail of any adjustments made to the image.

In the case of nonraw file formats, the archive file is the original file itself. In the case of raw files, the DNG format with an embedded raw file is an excellent solution for the archive file—providing an archive of the raw file plus the information associated with any image adjustments made in Adobe® Camera Raw or another raw image processor.



The image on the left shows a fingerprint on a check.
The image on the right shows a fingerprint that has been bleached and altered for clarity.

Viability of digital images

Are digital images intrinsically viable in the above-mentioned fields? Comparing digital imaging to silver-based photography puts many issues into perspective. The question is whether digital imaging technology prevents this medium from use in fields in which image integrity is paramount. If not, what methods must be employed to meet the requirements of the fields?

Silver-based photographic images have been manipulated, altered, and faked for over 150 years. Dino Brugioni's *Photo Fakery* (published by Brassey's Inc., 1999) shows images from the 1850s to the late 20th century in which multiple negatives were used to create scenes that never existed, or were otherwise manipulated. Throughout history silver-based images have been manipulated—often for political reasons.

Digital imaging doesn't create the possibility of image manipulation; it merely provides an additional technology for image manipulation, and for the detection of it. Therefore, the potential of image manipulation is not unique to digital images. With digital-imaging technology and a film original, you can scan a roll of negatives, manipulate the images and output them to a film recorder, and create a new set of negatives. There is no metadata stored with an analog image as there is with a digital photograph. If a digital photograph is altered, the associated metadata will reveal the alteration; any break or inconsistency in the metadata will be a clue to the manipulation, making digital originals more difficult to manipulate than film originals.

Digital imaging is as viable as any other imaging technology and is perhaps even better than analog photography for showing the provenance of an image. In forensic, scientific, military, and industrial applications, those who create and work with images should utilize best practices with all imaging media.

Best practices

Best practices are policies or rules that provide guidelines for procedures and workflow, and should incorporate (and may go beyond) any industry-side standards. You can use best practices to maintain the integrity of a digital imaging workflow.

A typical best-practices policy incorporates maintaining an archive image, only working on copies of the archive image, maintaining an audit trail, and employing only valid image processing procedures.

Archive images

Maintaining an unaltered archive image is essential to the workflow in most technical, medical, forensic, and military applications. A viewer can compare the archive image and the final image to determine if the image content or quality has been altered. Maintaining an archive image also ensures that any user can verify that the procedures used to make adjustments to it are reproducible and valid.

The Federal Bureau of Investigation (FBI) formed the Scientific Working Group on Imaging Technologies (SWGIT) in the mid 1990s to address some of the issues surrounding the use of digital imaging in forensics, among other issues. The SWGIT guidelines (www.fdiai.org/images/SWGIT guidelines.pdf) provide recommendations for photography and digital imaging in forensics. SWGIT recommends maintaining an archive image, and defines the archive image as “Either the primary or original image stored on media suitable for long-term storage.” The primary image is defined as “…the first instance in which an image is recorded onto any media that is a separate, identifiable object or objects. Examples include a digital image recorded on a flash card or a digital image downloaded from the Internet.” In other words, an archive image is an exact copy of what the camera recorded onto its original media.

If the original image was captured as a JPEG or TIFF file, the archive image will be an exact copy of it in the same format. TIFF and JPEG captures have distinct limitations—they are processed within the camera and are limited to 8 bits per channel during their camera processing. In addition, recovering highlights is impossible, and adjustments to color balance, contrast, and brightness can quickly deteriorate the image quality.

If the original was captured in a raw format, it is important to also retain information on any image adjustments made when the raw image is opened or converted. Raw files are, by definition, read-only, and contain unprocessed data from the digital camera that must be processed when opened. Raw files opened with the Camera Raw plug-in may contain a hidden sidecar file, or this information may be placed in a database on the host computer—depending on user preferences. In either case, it is important (but not intuitive) to keep this information with the file when the file is moved or archived. With raw file formats, the archive image includes the raw file plus the sidecar file.

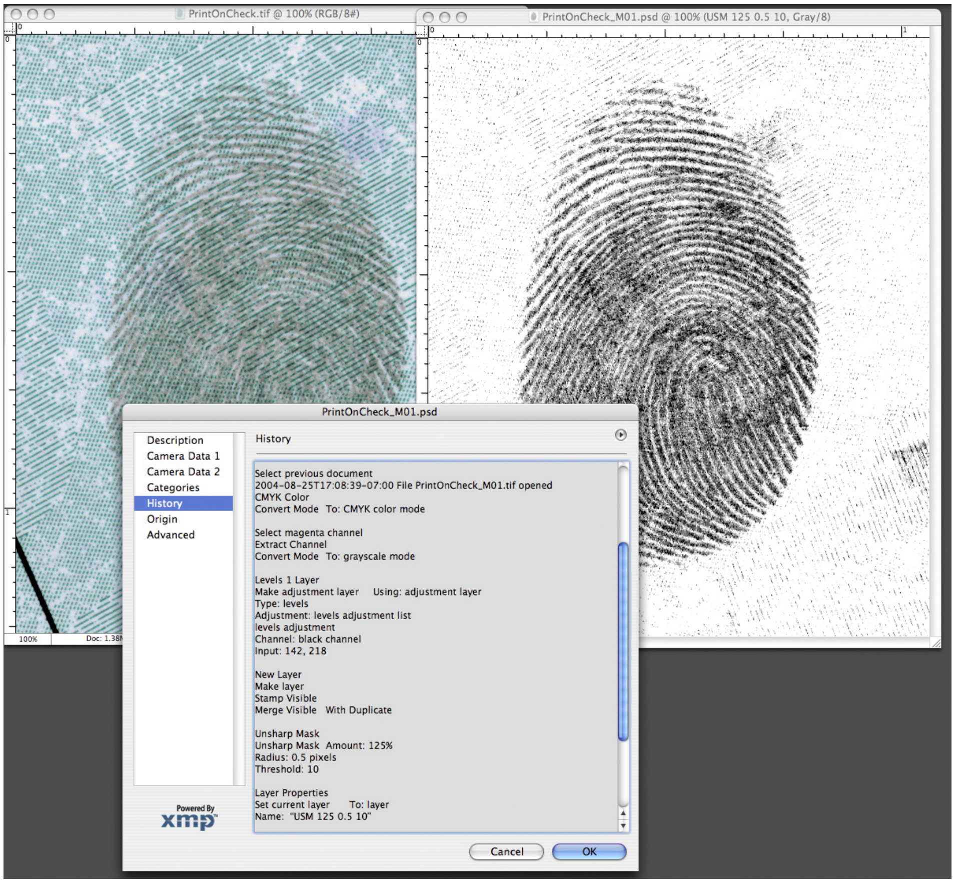
Raw formats can provide images with greater bit depth (10, 12, or more, depending on the camera). When opened using the Camera Raw plug-in, raw images provide many advantages in addition to their higher bit depth, such as color balance, brightness, and contrast adjustments that are nearly lossless.

Taking advantage of raw file formats is essential to getting the best image, and this is where the DNG format comes into play. Without the DNG file format, there is no guarantee that the settings used when opening the file are archived with the raw file. Using the DNG format with the raw file embedded provides the quality improvements of the raw format and the maintenance of the image adjustments as part of a single archive file.

Audit trail

In most fields, it's often necessary to make adjustments to images. For example, an image presented in court or analyzed for medical evaluation may have gone through several adjustments after it was captured. A question may arise as to whether the adjustments made were valid for the application, or if the adjustments resulted in a misrepresentation of the image.

In forensics, an image that was taken under fluorescent lighting may need color correction to eliminate the green cast, or a fingerprint image may benefit from a contrast boost and image sharpening. In medical imaging, applying false colors to the tonal range may help isolate, identify, and quantify a specific type of bacteria. Various methods of image processing used to identify product defects are important tools in industrial photography.

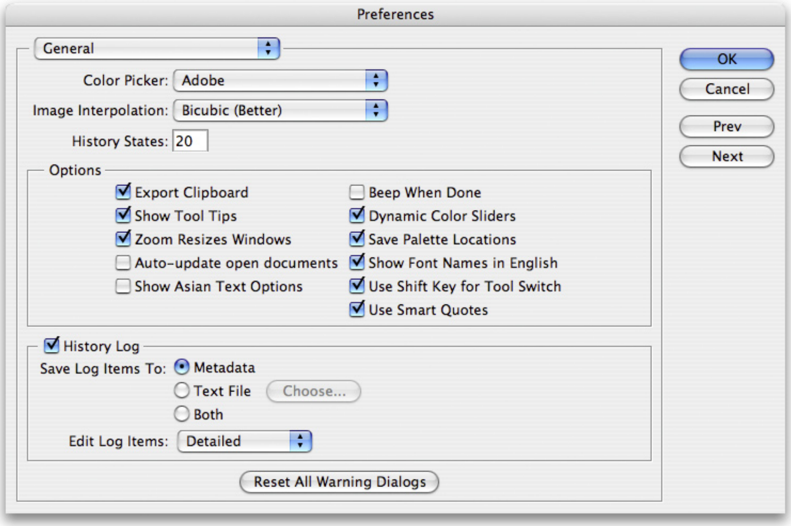


```
Select previous document
2004-08-25T17:08:39-07:00 File PrintOnCheck_M01.tif opened
CMYK Color
Convert Mode  To: CMYK color mode

Select magenta channel
Extract Channel
Convert Mode  To: grayscale mode

Levels 1 Layer
Make adjustment layer    Using: adjustment layer
Type: levels
Adjustment: levels adjustment list
levels adjustment
Channel: black channel
Input: 142, 218

New Layer
Make layer
Stamp Visible
Merge Visible  With Duplicate

Unsharp Mask
Unsharp Mask  Amount: 125%
Radius: 0.5 pixels
Threshold: 10

Layer Properties
Set current layer     To: layer
Name:  "USM 125 0.5 10"
```

This figure shows the history of modification to an image of a fingerprint.

Using a method of tracking changes to create an audit trail shows whether valid procedures were used, how each procedure affected the image, and allows the procedures to be repeated with similar results. In Adobe Photoshop® CS and later, an image creator can automatically record an audit trail by turning on the History Log feature in the Preferences panel. Each tool and feature used can be recorded, along with the parameters used for the given tool, filter, or adjustment. There are some exceptions, however, including the exact shape of Lasso tool selections and the paths of brush strokes of any of the painting or dodging/burning tools.

The History Log can be recorded directly into the image's metadata or as a separate text file, depending on the preference set in the General Preferences panel. If the log is stored in metadata, it can be viewed in the File Info panel, or in the Metadata window in the File Browser.



Preferences

General

Color Picker: Adobe

Image Interpolation: Bicubic (Better)

History States: 20

Options

☑ Export Clipboard
☑ Show Tool Tips
☑ Zoom Resizes Windows
□ Auto-update open documents
□ Show Asian Text Options
□ Beep When Done
☑ Dynamic Color Sliders
☑ Save Palette Locations
☑ Show Font Names in English
☑ Use Shift Key for Tool Switch
☑ Use Smart Quotes

☑ History Log

Save Log Items To: ● Metadata
○ Text File
○ Both

Edit Log Items: Detailed

You can select the History Log in the General Preferences panel.

In earlier versions of Photoshop, recording an audit trail required a plug-in or had to be done manually. To store the audit trail in the file's metadata, the image creator could have typed the information in one of the fields in the File Info panel.

Repeatability of image adjustments

When a technology is challenged in court, a Kelly-Frye or a Daubert hearing may be called to determine if the technology is valid. Digital imaging technology has gone through three such hearings since 1991. In his paper About Forensic Digital Imaging (www.imagingforensics.com/forensic.pdf) Erik Berg states, "State of Washington vs. Eric Hayden serves as an affirmation of the conclusion reached in the Commonwealth of Virginia vs. Robert Douglas Knight case. It also imposes the same requirements for digital images as those placed upon other types of evidence. …Any enhancement techniques must be reproducible, so that notes about the enhancement process, as well as who did the work should be maintained."

The need for image processing techniques to be repeatable and produce similar results is a cornerstone in forensics applications. For any technique to be reproducible, the technique must be performed on the same image or an exact copy of that image. With raw files, it is essential that experts open the images using the same settings in order to have the same starting point. If one expert opens the image in Adobe RGB color space, with a color temperature setting of 5500 in 16-bit mode, and another opens the same raw file in the sRGB color space with a color temperature setting of 4500 in 8-bit mode, it is like starting with two different images.

The DNG format with embedded raw files resolves this problem by creating a single image that contains the raw file along with the information about any adjustments made in the raw file conversion process.

History of tools to address issues of archive images

Since the early 1990s, camera and software companies have created products to provide various sorts of archive images, audit trails, and image authentication systems. Some of these products have provided the basis for the present raw files and audit trails.

Perhaps the earliest attempt to create a proprietary archive image format was the Kodak KDC file format. This format required either Kodak software or a Kodak plug-in to open the image. Like current raw formats, it was an unchangeable format, meaning that you couldn't save an image to KDC format. It also contained some metadata, including camera make and model, shutter speed and f-stop. The drawback to this format was that it wasn't universal and had limited bit depth—but it led the way to more powerful raw file formats.

In 1999, Olympus developed the Image Authentication System for use with two of its point-and-shoot digital cameras. This system required software to be installed in both the camera and the computer. Running the software would verify if an image had been altered.

Canon currently has a Data Verification Kit for the EOS 1Ds and EOS 1D Mark II cameras, which functions much like the Olympus system, but requires a dedicated memory card as well. Canon states that its system will detect any changes to the image, even as small as 1 bit.

Lexar has announced its Locktight security system, which can prevent a memory card from being used in an unauthorized camera or downloaded onto an unauthorized computer.

Most camera manufacturers now offer a raw file format from digital cameras. The benefit of raw formats, as related to digital image integrity, is that they are virtually unalterable. Raw file formats are read-only, which makes them difficult to alter without leaving traces that experts can detect. With the DNG format, one can now take that raw file and embed it, plus any adjustments made to it in a raw file processor, and archive this as a single file. The DNG file format provides an open source format that meets the needs of the forensics, medical, military, and industrial fields for archiving. As more software and hardware manufacturers support the DNG format, it will become the standard for archiving raw files in a secure manner that will meet the needs in fields in which image integrity is essential.

ABOUT THE AUTHOR

George Reis is the owner of Imaging Forensics Inc., which provides consulting and training services in forensic applications of imaging technologies, and image analysis support for court cases. He has testified as an expert in photography and in image analysis in courts in California and Hawaii.

He has been a Crime Scene Investigator, Forensic Photographer, and Fingerprint Technician with the Newport Beach (CA) Police Department from 1989 to 2006 and introduced digital imaging technology to that agency in 1992.

Imaging Forensics has provided training and consulting services to thousands of individuals, and represented hundreds of police and government agencies since 1995. These agencies include the US Secret Service, US Army Crime Lab, Missouri State Crime Lab Supervisors, Arkansas Criminal Justice Institute, Colorado Bureau of Investigation, San Francisco Police Department, Los Angeles Sheriff's Office, St. Louis County Police Department, and numerous state, county, and municipal agencies throughout the country.

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com

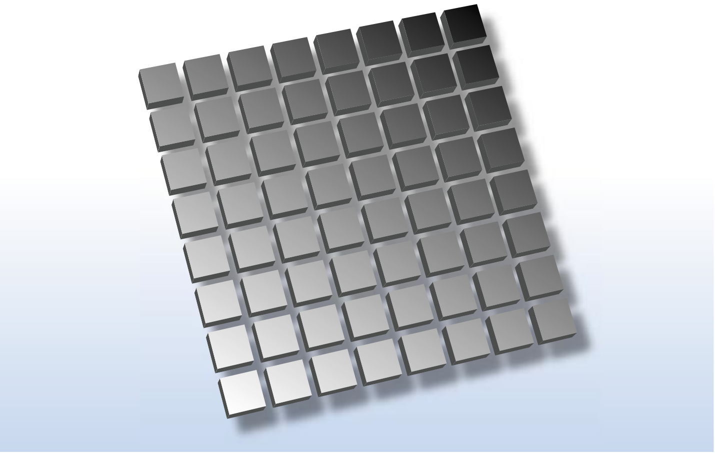
Understanding Digital Raw Capture

TABLE OF CONTENTS

By now, you've probably heard some talk about digital raw capture, but finding a coherent explanation of just what a digital raw capture actually is can be a bit more challenging. Part of the challenge is that raw isn't one single thing. Rather, it's a general term for a variety of proprietary file formats—such as Canon's .CRW and .CR2, Minolta's .MRW, Olympus' .ORF, and the various flavors of Nikon's .NEF, for example—that share important common features. To understand the nature of digital raw captures, you first need to know a bit about how those cameras that shoot raw actually capture images.

A raw file is a record of the data captured by the sensor. While there are many different ways of encoding this raw sensor data into a raw image file, in each case the file records the unprocessed sensor data. So let's consider what the sensor in a digital camera actually captures. A number of different technologies are included in the category of "digital camera," but nearly all of those that shoot raw are of the type known as "mosaic sensor" or "color filter array" (CFA) cameras.

Color filter array cameras use a two-dimensional area array to collect the photons that are recorded in the image. The array is made up of rows and columns of photosensitive detectors—typically using either CCD (charge-coupled device) or CMOS (complementary metal oxide semiconductor) technology—to form the image. In a typical setup, each element of the array contributes one pixel to the final image (see below).

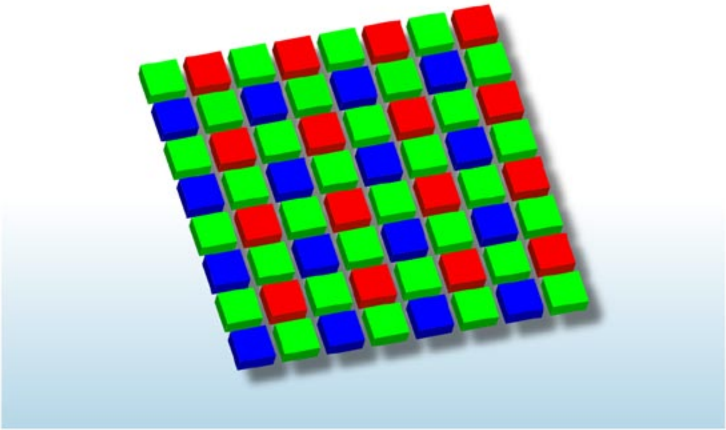


An area array—each photosensor contributes one pixel to the image.

But the sensors simply count photons—they produce a charge that's directly proportional to the amount of light that strikes them. A key point is that raw files from color filter array cameras are grayscale.

Grayscale to color

The role of the color filter array is to create color images from the raw grayscale capture. Each element in the array is covered by a color filter, so that each element captures only red, green, or blue light. Many cameras apply the filters in a Bayer pattern like the one shown below.

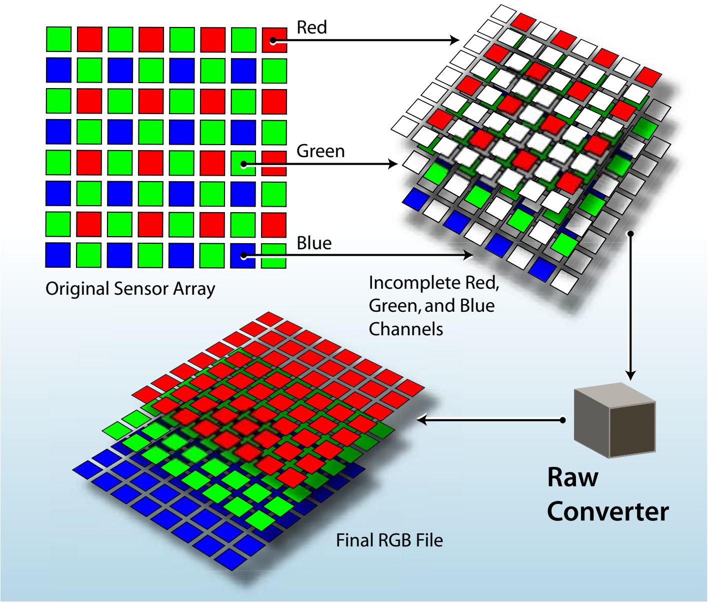


In a Bayer pattern color filter array, each photosensor is filtered so that it captures only a single color of light: red, green, or blue. Twice as many green filters are used as red or blue because our eyes are most sensitive to green light.

Other filter patterns are possible. Some cameras use CMY rather than RGB filters because they transmit more light, while still others may add a fourth color to the mix. The common factor in all color filter array cameras is that, no matter what color filter arrangement is used, each element in the sensor captures only one color. The red-filtered elements produce a grayscale value proportional to the amount of red light reaching the sensor, the green-filtered elements produce a grayscale value proportional to the amount of green light reaching the sensor, and the blue-filtered elements produce a grayscale value proportional to the amount of blue light reaching the sensor.

Raw files contain two different types of information: the image pixels themselves, and the image metadata. Metadata, which literally means "data about data," is generated in the camera for each capture. Both raw and JPEG captures, for example, contain EXIF (Exchangeable Image Format) metadata that records shooting data such as the camera model and serial number, the shutter speed and aperture, the focal length, and whether or not the flash fired. Raw files also include some additional metadata that raw converters need in order to process the raw capture into an RGB image.

In addition to the grayscale values for each pixel, most raw formats include a "decoder ring" in metadata that conveys the arrangement of the color filters on the sensor, so it tells raw converters which color each pixel represents. The raw converter then uses this metadata to convert the grayscale raw capture into a color image by interpolating the "missing" color information for each pixel from its neighbors.



The raw capture is demosaiced and interpreted by a raw converter, using portions of the metadata embedded into the file at the time of capture, as well as algorithms in the conversion software.

This process, known as demosaicing, is one of the key roles a raw converter plays, but it's not the only one. Raw conversion involves the following steps in addition to demosaicing.

- White balance. The white balance setting on the camera has no effect whatsoever on the captured pixels when you shoot raw—it's simply recorded as a metadata tag in the raw file. Some raw converters can read this tag and apply it as the default white balance (which the user can then override if desired), while others may ignore it completely and analyze the image to determine white balance.

- Colorimetric interpretation. Each pixel in the raw file records a luminance value for either red, green, or blue. But red, green, and blue are pretty vague terms—if you take a hundred people and ask them to visualize "red," you'd almost certainly see a hundred different shades of red if you could read their minds.

  Many different filter sets are in use with digital cameras. So the raw converter has to assign the correct, specific color meanings to the "red," "green," and "blue" pixels, usually in a colorimetrically defined color space such as CIE XYZ, which is based directly on human color perception.

- Gamma correction. Digital raw captures have linear gamma (gamma 1.0), a very different tonal response from that of either film or the human eye. So the raw converter applies gamma correction to redistribute the tonal information so that it corresponds more closely to the way our eyes see light and shade. (This property of digital capture has important implications for exposure settings when shooting, which I discuss in a paper called "Raw Capture, Linear Gamma and Exposure".)

- Noise reduction, antialiasing, and sharpening. Problems can arise with very small details in an image. If the detail is only captured on a red-sensing pixel or a blue-sensing pixel, the raw converter may have a hard time figuring out what color that pixel should really be. Simple demosaicing methods also don't do a great job of maintaining edge detail, so most raw converters also perform some combination of edge-detection and antialiasing to avoid color artifacts, noise reduction, and sharpening.

All raw converters perform all of these tasks, but they may use very different algorithms to do so, which is why the same image may look quite different when processed through different raw converters. Some converters will map the tones flatter to provide editing headroom while others will try to achieve a more film-like look by increasing the contrast of the curve.

Generally, there is no one single "correct" interpretation of a given raw format. Vendors make a relatively subjective determination of what the best "look" is, and then adjust their converter to produce that result.

How JPEG differs from raw

When you shoot JPEG, a raw converter built into the camera carries out all the tasks listed earlier to turn the raw capture into a color image, then compresses it using JPEG compression. Some cameras let you set parameters for this conversion—typically, a choice of sRGB or Adobe RGB as color space, a sharpness value, and perhaps a tone curve or contrast setting. Unless your shooting schedule is atypically leisurely, it's difficult to adjust these parameters on an image-by-image basis, so you're locked into the camera's interpretation of the scene.

JPEGs offer fairly limited editing headroom—large moves to tone and color tend to exaggerate the 8-by-8-pixel blocks that form the foundation of JPEG compression—and while JPEG does a decent job of preserving luminance data, it applies heavy compression to the color data, which can lead to issues with skin tones and gentle gradations when you try to edit the JPEG.

When you shoot raw, however, you get unparalleled control over the interpretation of the image through all the aforementioned aspects of the conversion. When you shoot raw, the only on-camera settings that have an effect on the captured pixels are the ISO speed, the shutter speed, and the aperture setting. Everything else is under your control when you convert the raw file—you can reinterpret the white balance, the colorimetric rendering, the tonal response, and the detail rendition (sharpening and noise reduction) with a great deal of freedom. Within limits (which vary from one raw converter to another), you can even reinterpret the exposure compensation.

Almost all cameras that shoot raw capture at least 12 bits, or 4096 shades, of tonal information per pixel. The JPEG format, however, is limited to 8 bits per channel per pixel, so when you shoot JPEG, you're trusting the camera's built-in raw converter to throw away a large amount of the captured data in a way that will hopefully do the image justice. This is exacerbated by the tendency of most camera vendors to impose a fairly steep contrast curve in the raw-to-JPEG conversion in an effort to produce a JPEG that resembles a transparency. In the process, they throw away about a stop of usable dynamic range, and you have essentially no control over what gets discarded.

In some ways, it's tempting to draw the analogy that shooting JPEG is like shooting transparency film while shooting raw is more like shooting negative film. With JPEG, as with transparency film, you need to get everything right in the camera, because there's very little you can do to change it later. Shooting raw provides considerable latitude in determining the tonal rendition, like negatives, and also offers great freedom in interpreting the color balance and saturation. The fact that raw also lets you control detail rendition—noise reduction and sharpening—breaks the analogy but offers a further advantage.

Raw offers one more potential advantage that may be hard to demonstrate but is, I believe, real nevertheless. If you shoot raw, you'll be able to take advantage of future improvements in raw converters. Digital photography may no longer be in its infancy, but it hasn't yet reached adolescence, let alone maturity, and anyone who has spent more than a couple of years working with digital imaging knows that digital imaging software improves with each iteration. JPEGs are relatively inflexible files—we may see improvements in their handling, but any such improvements are likely to be modest. Raw converters, however, have undergone radical improvements in the 10 years or so that color filter array cameras have been around, and there's little reason to think that the next 10 years won't see similar improvements. Shooting raw will allow you to exploit these improvements as and when they happen.

Bruce Fraser
Bruce emigrated from Edinburgh, Scotland where he escaped the dreary Scottish climes only to discover San Francisco's equally challenging weather. Rumor has it this was the inspiration of Bruce's lifelong fascination with all things relating to color. Bruce has made a study of human vision and how it relates to reproducible color in photography and photomechanical reproduction.

Adobe Systems Incorporated • 345 Park Avenue, San Jose, CA 95110-2704 USA • *www.adobe.com*

Digital Imaging: The Technology and the Prosecutor

Penney Azcarate

Article published in The Prosecutor Magazine, vol. 34/number 1 (Jan/Feb 2000).

Technology is rapidly changing every aspect of the criminal justice system as computers make possible the streamlining of many procedures, shortening their time span and increasing their accuracy. Techniques used in the collection, processing and storage of evidence benefit from these recent developments.

Digital imaging, once used primarily for fingerprint comparisons, now is being used effectively in an increasing variety of evidence procedures, including analysis of altered documents, recording crime scenes and traffic crash sites, documenting domestic violence cases and creating video mug shot systems. However, as the use of digital cameras and digital imaging increases as a powerful crime-fighting tool, so do the inevitable challenges to its admissibility in court. Therefore it’s imperative that a prosecutor be familiar with the process and aware of preventative measures to overcome any objections at trial.

This article addresses questions prosecutors may be asking in this ever-changing technological field. What is digital imaging? Should my jurisdiction buy a digital camera? What are the advantages and disadvantages? Do new evidence rules apply? What impact does digital imaging have on courtroom presentations?

What are defense challenges to digital imaging and how do I overcome these challenges?

As these issues are addressed, it is important to keep in mind that digital imaging is the latest in a long line of technology used by law enforcement to collect and document evidence. In the not so distant future, digital cameras and digital imaging will be of such quality and price that regular film processing may become archaic and uneconomical. Any doubts or challenges to digital imaging will then be silenced. Until that day, prosecutors need to walk into a courtroom with an underlying knowledge of digital imaging to keep this issue from circumventing the substantive issues of the case.

WHAT IS DIGITAL IMAGING?

The Basics

Digital images are pictures processed through a computer. The images can be created several ways. The most obvious way is with a digital camera which creates images that are eventually downloaded and stored on a computer. Another popular way is to scan a photograph directly into a computer. Scanning converts original film photographs into digital images which can be stored, e-mailed, or enhanced.

To get a better understanding of digital images and digital cameras, one must first grasp a few basic terms and procedures. Computers understand and read coded numbers. In order for a computer to process pictures, the information must be converted to a series of numbers or digits, hence the name "digital". These number sequences consist of bits and bytes that the computer reads.

A binary digit (**bit**) is the smallest unit of information a computer can process. Its value is always "0" or "1" which the computer reads as an on/off electrical sequence.[1] Eight bits make a **byte**. A picture element (**pixel**) is a code consisting of bits of information representing a specific color, intensity and location. Pictures are made up of many different pixels. This digital representation of a photograph is stored in the computer on a rectangular grid called a **bitmap.**[2] The more pixels per inch (ppi), the sharper and clearer the final photograph will appear.

Digital Cameras

To acquire photographs, a digital camera uses the same principles as traditional film. Instead of using light-sensitive film to record images, most digital cameras use a light-sensitive chip called a charged coupled device (CCD) to record the image electronically. This is the same image sensor used in most video cameras. The light sensors on the CCD capture and store the image as red, green, and blue pixels.[3]

The electrical output of the CCD is sent to a converter which changes the image to a digital output. The data is then stored in the camera as a computer data file with each file representing a different photograph. Some digital cameras have the ability to display the resulting images on a view screen, others require a computer to view the images.

Scanners

Scanners allow a user to scan in documents or pictures into a computer. As stated earlier, traditional film pictures and negatives can be scanned to create a digital image on the computer. Because film has more information per inch than an image captured from a digital camera, more computer storage space will be used.[4] The quality of the scanned image depends on the resolution of the optical system in the scanner.[5]

Enhancements

The enhanced digital imaging process evolved from the NASA space program over twenty years ago. The technology was developed by the jet propulsion laboratories to isolate galaxies and receive signals from satellites in the late 1960's.[6]

After a file is downloaded or scanned into a computer, an image can be enlarged or enhanced by using one of several software programs available. By using software, poor quality or obscured details in photographs can be enhanced in an attempt to bring out fine points that are not visible to the unaided eye.[7]

In explaining this process, it is important to distinguish between enhancement and manipulation. The software enhances photographs by improving sharpness and image contrast; nothing is added to the image. It makes what is there more usable. Enhanced pictures are not changed or cut and pasted to create new images. For example, pattern and color isolation filters can contribute to the enhancement process by removing interfering colors and background patterns.[8] In this context, enhancement is comparable to adjusting a television's picture[9] or tuning into a radio station.

Manipulation, on the other hand, is defined as "to change by artful or unfair means so as to serve one's purpose."[10] Certainly, one could manipulate an image to create a fraudulent portrayal of a scene. For example, a segment of one picture could be cut and pasted into another picture creating a false representation. However, manipulation did not originate with digital images. Some form of manipulation can be done with any generated piece of evidence to include videotapes, negatives, sound recordings, or traditional photographs. Where there is a will, there is a way.

Technology is catching up to the possibilities of manipulation in digital imaging. Currently, there are several software packages and digital cameras available on the market preventing the user from adding to, changing or destroying the original image. The original files are saved as a special type of file format that makes it impossible for the user to alter the original file in any form. An original picture must be saved as a different type of file format in order to enhance the image which leaves the original file unchanged. In addition, some software programs limit accessibility to the images through passwords and encryption while maintaining a log of user access. Regardless of these safeguards, if a prosecutor focuses on the enhancement process and the credibility of the witness, manipulation arguments will not carry much weight with the factfinder.

ADVANTAGES v. DISADVANTAGES

Digital imaging offers the user convenient and efficient means of collecting and cataloging evidence. Images can be delivered via e-mail, saved on disks and CDs, or added to a searchable database. If a digital camera is used to capture the images, there is no need for a chemical lab to develop film. Another advantage to digital cameras is photographs can be accessed on the scene. Viewing the pictures at the scene ensures superior picture quality and that all key aspects of the area are captured. Any poor quality pictures can be deleted and shot again before the scene is destroyed. In addition, the digital camera, in conjunction with a laptop, allows an officer the ability to electronically transmit photographs from the scene.[11]

High resolution digital cameras can capture approximately 16 million different colors and can differentiate between 256 shades of gray.[12] This is not to say digital cameras are faultless. As with any relatively new electronic device, there are drawbacks. Traditional film still provides the highest resolution images and gives the operator more control over the picture taking process. For example, low light situations may introduce electronic "noise" in digital images but an operator with film could increase exposure time to compensate for the lighting conditions. As the technology involved with digital cameras becomes more advanced and inexpensive, these drawbacks should disappear.

FACING A CHALLENGE

Manipulation/Tampering

Skeptics view the enhancement ability of digital imaging as a possible means to invalidate the technology in the courtroom. An unbiased expert would agree that any media can be manipulated whether in a dark room or in a computer. The International Association for Identification (IAI) has formally recognized digital imaging as a "scientifically valid and proven technology for recording, enhancing, and printing images".[13] Manipulation arguments are not new and, as always, can be overcome through the credible testimony of your expert witness.

A preventative measure to counter these arguments is to ensure your law enforcement agency has a standard operating procedure for taking and handling digital images. As discussed later, these procedures should be in a written format and cover all aspects of the digital imaging process. The police photographer at trial should be able to articulate these procedures and state that these procedures were followed in preparing images in this case. If any enhancements were done to the original, a witness must be able to explain how the adjustments or enhancements were accomplished. As the prosecutor, you may want to demonstrate the same enhancements on sample images in the courtroom or view the actual enhancement process conducted in the case one image at a time. This demonstration will allow the jury to see the exact procedures and clear up any of their misconceptions of digital imaging.

As the technology advances, manipulation arguments may become moot. Digital imaging continues to evolve into a more secure tamper-resistant process. As stated earlier, recent technological advances utilize software that authenticates and encrypts images, tracks the chain of custody and restricts access to authorized personnel.[14]

Chain of Custody

Standard operating procedures should control the way images are captured, handled, archived and secured. Many law enforcement agencies have established such procedures for digital imaging. Although, these procedures vary depending on the use and type of the equipment involved, there are some core elements that should be incorporated.

First, original images should be recorded in an unalterable form as soon as possible.[15] Some digital cameras and software programs automatically create a data file attached to the image which can not be changed. However, the original should be saved on a Writable CD if possible. Once data is written to a Writable CD (CD-R), it cannot be removed or altered and any enhancement of the image must take place on a copy of the original. Writable CDs are the best solution today. However, as technology advances, the issue of archiving images should be re-addressed to insure the best available source is being used for storing images. For example, a new type of Writable CD (CD-RW) on the market allows a user to reuse the CD and delete files. Consequently, this type of Writable CD should not be used for archival purposes.

Second, every enhancement to an image should be saved as a separate photograph so the complete trail from original to final photograph is captured.[16] This process should be tracked and preserved either by using a manual log or a software program.

Third, custody control and access limitations must be established. Access to the computer and the original image should be limited.[17] The original image is equivalent to a negative and should be treated as such.[18]

Witness Testimony

The witness or witnesses should be able to explain how the image was acquired, whether the original is a fair representation, the process involved in enhancing the image, and the chain of custody. This explanation must be a clear and articulate description of the process. An officer trained in presenting digital imaging evidence lends to his or her credibility and dispels suspicions of impropriety.

Legal Authority

Several jurisdictions have used digital imaging for years without any challenges to its admissibility. Many other jurisdictions are just getting the digital systems and have yet to face any challenges. Consequently, case law on challenges to digital imaging is limited. Cases involving digitally-enhanced photographs have survived *Frye* hearings in California, Ohio, Virginia and Washington. Only one of these cases, *State v. Hayden* (Washington)[19] resulted in a published appellate opinion and, therefore, is worth further comment.

State v. Hayden

A woman was found raped and strangled in her apartment. Investigators found bloody hand prints on a bed sheet where the victim was discovered. The sheet was taken to the County's latent print examiner who put it through a chemical process to set the prints but the contrasts were too subtle to make a positive identification.[20]

The examiner took the sheet to Erik Berg, a forensic specialist and digital imaging expert at the Tacoma Police Department. Mr. Berg photographed digital images of the sheet and enhanced the images by filtering out background patterns and colors.[21] The print examiner was then able to find over forty comparison points on a palm print from an enhanced photograph.[22]

The trial court held a *Frye* hearing on the admissibility of the enhanced photographs. The court held the *Frye* test was inapplicable.[23] Moreover, the court continued stating even if *Frye* applied, the process passed the test.[24]

On appeal, the prosecuting attorney for King County, Norman K. Maleng, assigned the case to assistant prosecutor, Todd Bergstrom. Mr. Bergstrom argued that the digital enhancement process was not novel scientific evidence and, therefore, the *Frye* test was not necessary. In addition, Mr. Bergstrom argued that if the court found the process to be new or novel, enhanced digital imaging is accepted in the relevant scientific community.

The appellate court agreed that the process was not novel but since the issue was one of first impression, the court went on to decide the admissibility of the process under *Frye*.[25] Finding the enhanced digital imaging was generally accepted in the relevant scientific community, the court found the process passed the *Frye* test.[26]

Since the outcome of the Hayden case, Mr. Bergstrom has been involved with an FBI working group developing guidelines for the use of digital imaging in law enforcement. The Scientific Working Group on Imaging Technologies(SWGIT)has published a draft guidelines document, *Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System*, which can be viewed at "http://www.fbi.gov/programs/lab/fsc/backissu/april1999/swgit1.htm". SWGIT is interested in receiving feedback on this draft from anyone in the criminal justice field.

Mr. Bergstrom believes new challenges to digital imaging may be more technical and warns, "Although the *Hayden* case was unique because the sole evidence was the palm print, a prosecutor facing any challenge to digital imaging needs to know the science underlying the process."

CONCLUSION

Digital imaging is now available and affordable to the home user. The exposure to the techniques involved with the process will eventually clear up any misconceptions surrounding digital imaging and enhancement. Until then, prosecutors need to be familiar with the procedures used in their jurisdiction to capture and store digital images. In addition, prosecutors must be familiar with the technology incorporated in digital imaging to defend against any potential attacks.

At trial, prosecutors should focus on the image and the witness: not the technology unless challenged. Does the photograph depict a fair representation of the scene? Can the chain of custody be established? Going beyond standard questions used to admit traditional photographs may initially confuse the factfinder. Presenting the photograph in a fair and professional manner adds to the credibility of your witness and will serve as a solid foundation with the jury if the witness is needed later to refute any defense challenges.

Word Count: 2598

[1] Eastman Kodak Company, *Digital Learning Center:Frequently Asked Questions*, faq1006 (last modified January 1999) <http://www.kodak.com/US/en/digital/dlc/book4/chapter1/index.shtml>.

[2] *Id.*

[3] *Id.*

[4] Eastman Kodak Company, *Kodak Professional: Managing Image Records* (visited August 5, 1999) <http://www.kodak.com/global/en/professional/hub/law/filmdig/manage.shtml>.

[5] Erik Berg, *Legal Ramifications of Digital Imaging*, p.2, Presented at the International Association for Identification's International Educational Conference in Boston, Massachussetts (1997).

[6] Redflex Traffic Systems Pty. LTD, *Digital Imaging For Secure Primary Evidence*, 586-007-1v0 (1998).

[7] Erik Berg, *The Digital Future of Investigations*, p. 38, Law Enforcement Technology (August 1995).

[8] *Id.*

[9] Berg, *supra*, note 5, at 11.

[10] Merriam-Webster, Incorporated, **Merriam-Webster's Collegiate Dictionary**, Tenth Edition (1998).

[11] Eastman Kodak Company, *Kodak Professional: About Digital* (visited July 15, 1999) <http://www.kodak.com/global/en/professional/hub/law/filmdig/digital.shtml>.

[12] *State v. Hayden*, 950 P.2d 1024, 1028 (Wash. Ct. App. 1998).

[13] International Association for Identification, *Resolution 97-9* (August 1, 1997).

[14] Berg, *supra*, note 5, at 8.

[15] Richard Kammen and Herbert Blitzer, *Ensure Admissibility of Digital Images*, The Indiana Lawyer, vol. 6 no. 15 (November 1995).

[16] Berg, *supra*, note 5, at 5.

[17] Kammen and Blitzer, *supra*, note 15.

[18] Berg, *supra*, note 5, at 5.

[19] *State v. Hayden*, 950 P.2d 1024 (Wash. Ct. App. 1998).

[20] *Hayden*, 950 P.2d at 1025.

[21] *Id.*

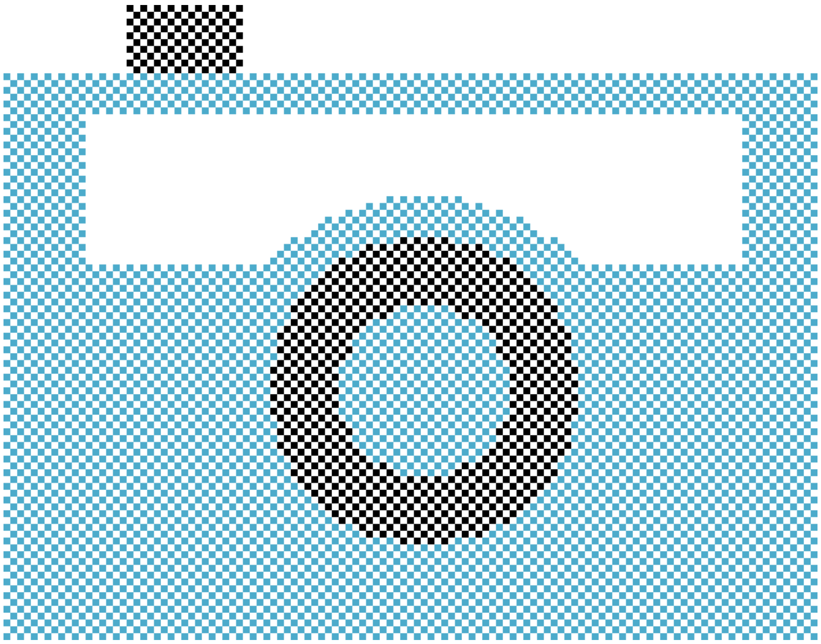
[22] *Id.*

[23] *Id.* at 3.

[24] *Id.*

[25] *Id.* at 4.

[26] *Id.* at 5.



A Simplified Guide To Crime Scene Photography

Introduction

Anyone who has seen the movie **MY COUSIN VINNY** (1992) knows how a snapshot can save the day. In the film, inexperienced New York lawyer Vincent LaGuardia "Vinny" Gambini travels to a small southern town with his fiancée, Mona Lisa Vito, to represent his cousin in a murder case. Mona Lisa's incessant picture taking with a cheap pocket camera causes frustration throughout the film, but eventually produces a photograph that holds the key to the case.

Photography of everything from landscapes to historical events has preserved and illustrated history for the past 200 years. When a photograph of a forged document was presented and allowed as courtroom evidence in 1851[1], photography as a forensic tool was born and soon became a boon to cases of identification and scene analysis. Crime scene photography became cutting edge in the 1870s and new technologies have expanded its use ever since.

In this discussion, photographs are not evidence in and of themselves, but provide visual documentation of the scene and locations of evidence within the scene. Photographs taken at a crime scene allow investigators to recreate that scene for later analysis, or for use in the courtroom. If the crime scene photography does not thoroughly and accurately document the entire scene, it could be detrimental to the investigation and potentially damaging during a criminal trial.

Principles of Crime Scene Photography

There is no prescribed length of time it takes to photographically document a crime scene. The amount of time spent depends on the size and

[1] *Luco vs U.S.*, 64 U.S (23 How.) 515, 162, L. Ed 545 (1859)

complication in the crime scene, how much there is to document and environmental factors like weather or danger to the investigative team. It can consist of thousands of photographs and hours of work.

Crime scene photography should not just focus on the obvious. The purpose of crime scene photography is to document what is there and where it is in relationship to the scene, whether it is obviously connected to the crime or not. For example, a photographer in Florida shot the inside of every cabinet and the refrigerator at a homicide scene in a home, just as a matter of procedure. It was later discovered that the victim had a receipt for a six-pack of beer, matching the beer shown in the photograph of the refrigerator. Relatives noted that the victim did not drink beer. Further investigation led the team to the convenience store where the beer was purchased and the surveillance tape showed the victim with an unknown person purchasing the beer. It turns out that the victim had picked up a hitchhiker, purchased beer for that person and come back to the house. The photograph of the refrigerator contents had created the link enabling the investigators to find the suspect.

Capturing the Scene

Photography, or "writing or drawing with light", is defined as the process or art of producing images of objects on sensitized surfaces by the chemical action of light or of other forms of radiant energy, such as X-rays, gamma rays or cosmic rays. Fixing an image permanently has been possible since the 1820s in a variety of ways from the daguerreotype, to silver plates, to film and now digitally.

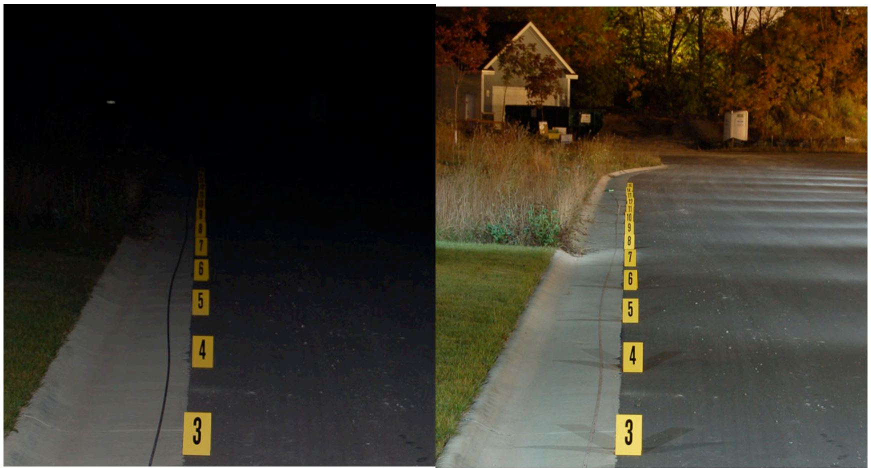
Some may consider photography more of an art than a science, but well-taken crime scene photographs can aid scientists, investigators and members of the court in their search for the truth. This makes photography a critical first responder skill. Larger agencies may have specially trained and certified crime scene photographers with high-end cameras and lighting to document crime scenes and evidence, but more often the first responder needs to do what they can with equipment assigned to them. That said, many of today's digital point-and-shoot cameras have a variety of settings that, with some basic operator training, allow for proper documentation.

Controlling the Light

Photographers use several means to tell the camera how to capture the image including aperture, shutter speed, depth of field and white balance. Aperture refers to the size of the opening that lets light into the camera and shutter speed is how long that opening, or shutter, remains open. Depth of field is the amount of area in front of (foreground) and behind (background) an object that remains in focus. Lastly, white balance allows the camera to record the proper temperature of light, resulting in an accurate representation of the color tones of objects in the photograph.

Brightening the Darkness

Experienced photographers often use a technique called “painting with light” to expose image details in dark or near-dark conditions. In this technique, the shutter is held open for seconds or minutes and the photographer walks through the scene adding light from sources such as a flashlight or detached camera flash.



Crime scene at night & after using the painting with light technique. (Courtesy of Scott Campbell)

However the photographer chooses to capture the image, the main reason for crime scene photography is to thoroughly document the entire scene, the evidence, and any areas of special significance to the investigation.

Why and when is crime scene photography used?

Photography should be used as part of the documentation for all physical crime scenes, including traffic collisions, burglaries, homicides, or any number of crimes against people or property. Photographs, however, can be misleading and confusing to the viewer. Therefore, crime scene photographers must ensure their work is both ethical and honest while capturing as much accurate information and detail as possible. Documenting all elements of a crime scene is a major stepping stone when trying to piece together what happened, how it happened and who did it.

Crime scenes are typically full of activity and often unpredictable, with first responders assisting victims and investigators beginning their work. Even in the most ideal situation, capturing photographic evidence can be challenging. An experienced photographer will know to take photos at all stages of the investigation and that it is better to have too many than not enough images.

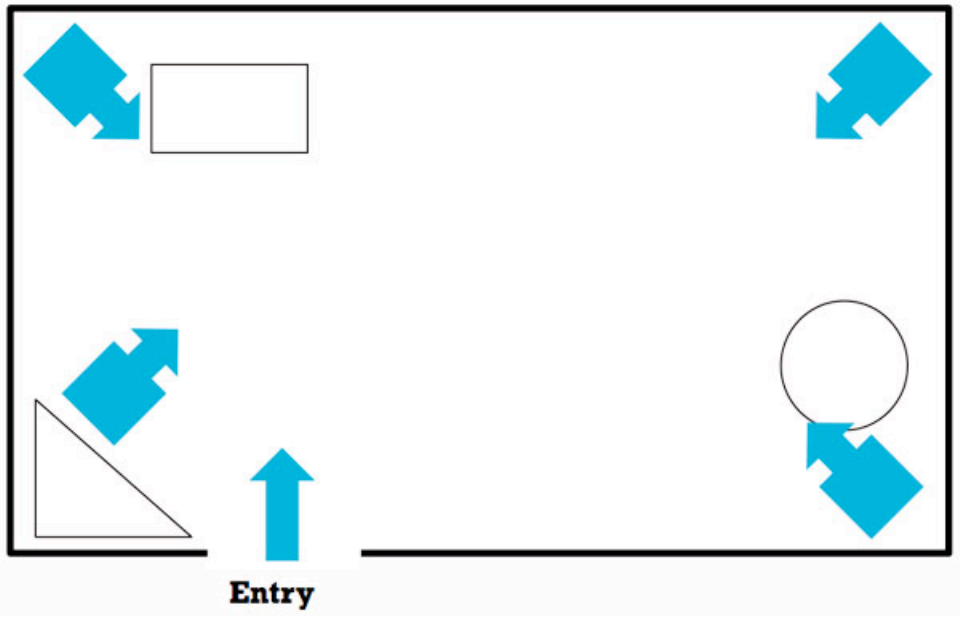
The following steps are taken to ensure proper photographic documentation:

1. **Secure the scene:** In all forensic investigations, the first step is to secure the crime scene.

2. **Evaluate conditions:** Next, the photographer should evaluate the available light and weather conditions and adjust camera settings appropriately. Crime scenes can be indoors, outside or both; they can be vehicles, include multiple rooms, or any combination of locations, therefore no single camera setting will work for all crime scenes.

3. **Shoot the scene:** The photographer should take photographs before anything is disturbed, progressively working through the scene from outside to close-up pictures. Many shots should be taken, from the entire scene, to medium shots to show the relationship of evidence to the overall scene.

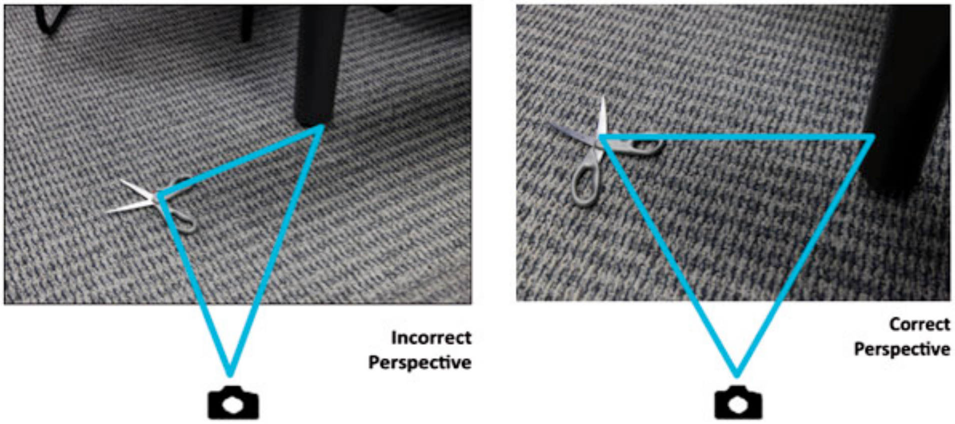
   Just like a television program will show the viewer the outside of a building to establish where the characters are going, the crime scene photographer should capture the whole scene first using wide-angle shots covering the entire scene from the approach and through every area. Close-up images of evidence can be taken out of context, so establishing the scene first with wide and medium shots is critical.



In addition, photographs should be taken looking up from the scene to capture evidence or environmental factors that may be above the scene.

4. Photograph the victims: The next series of shots should include victims (if present) to show locations, injuries and condition.

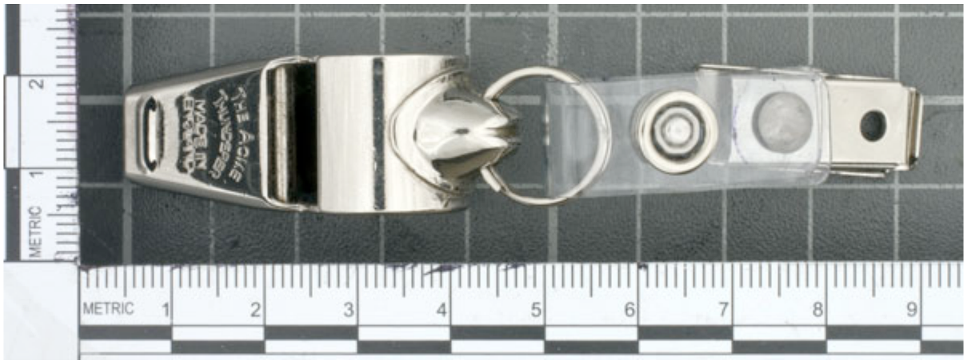
5. Photograph the evidence: Then each piece of evidence should be photographed to illustrate where it was found. This establishes the relationships of the evidence to the victim, the victim to the room and so on. These photographs should be taken from straight above or straight on at right angles, eliminating potential distance distortions. Each piece of evidence should be photographed with a scale to indicate size and without a scale.



(Courtesy of Daniel Nichols, NFSTC)

6. Evidence markers: Photographs should be taken before evidence markers are placed, then again after. These initial shots are important to prove that no one has tampered with the crime scene.

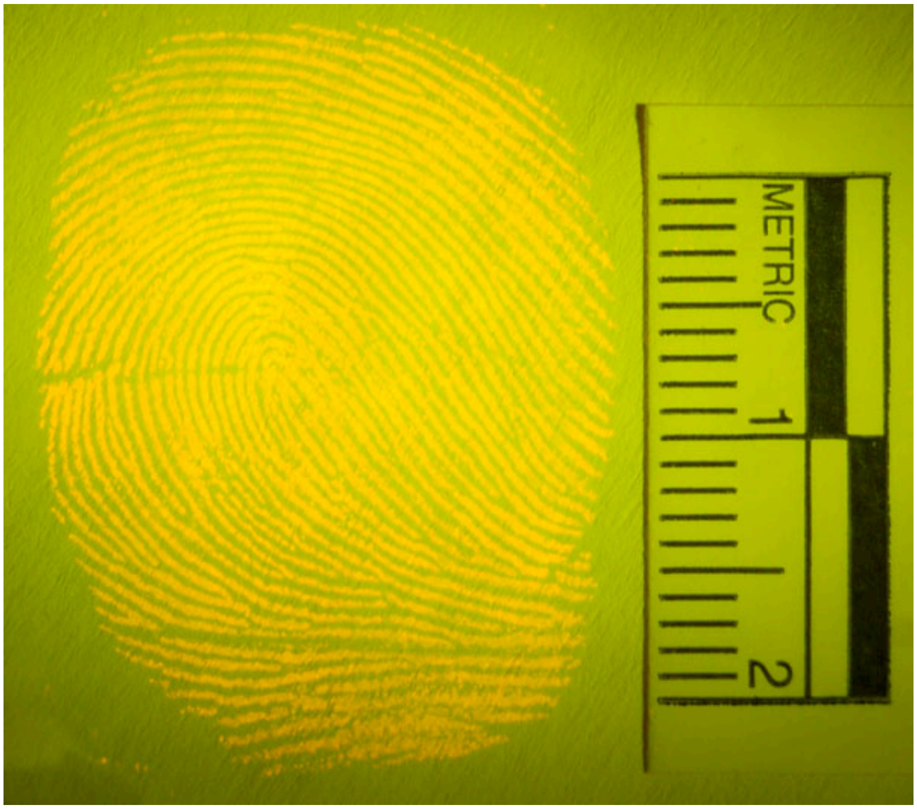
7. Re-shoot for new evidence: If investigators mark new evidence, the whole series of shots should be repeated, including all evidence shots. These photos should include the entire piece of evidence and a scale to indicate size.



(Courtesy of Becky Carter, CEP, NFSTC)

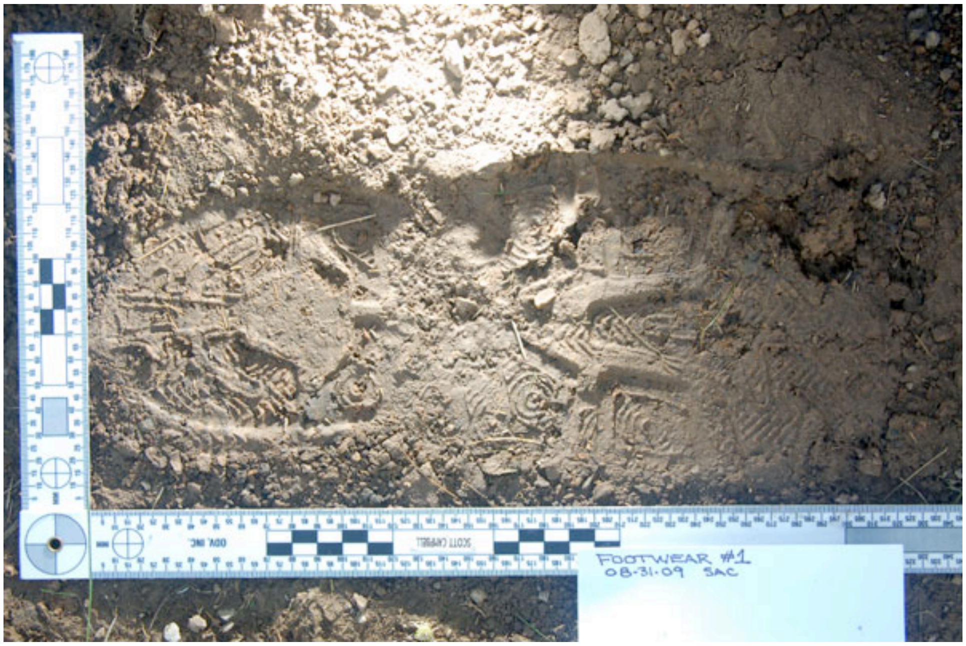
Special imaging techniques and lighting should be used to capture things like fingerprints, indentations, shoe and tire track impressions, vehicle identification numbers (VIN) and very small pieces of evidence. Techniques may include:

- **Alternate light sources (ALS)** – such as lasers, blue or green lights and colored filters that help detect processed latent fingerprints or other hidden evidence and illuminate for photographing



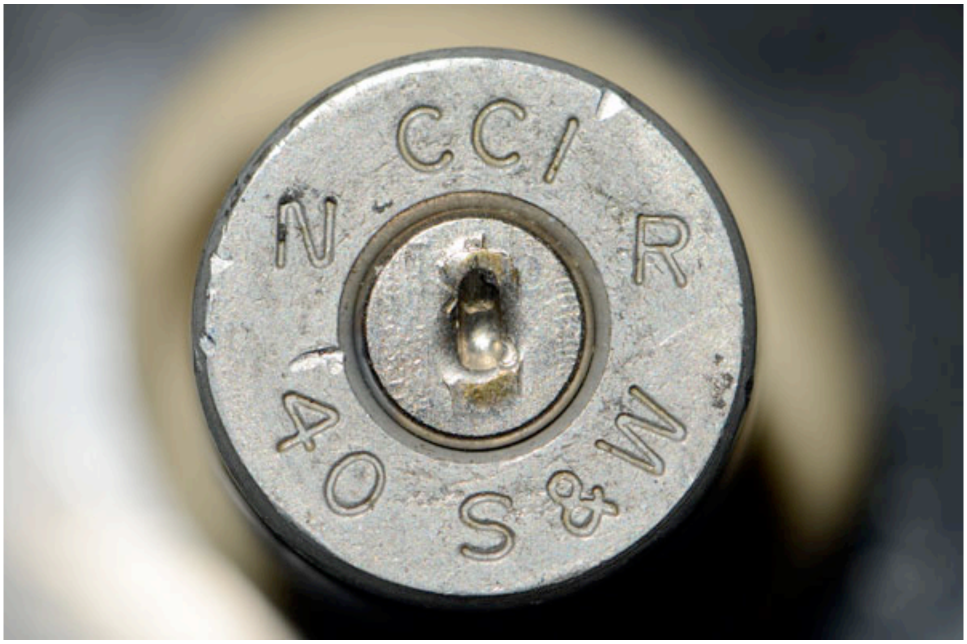
Green light used to illuminate a latent fingerprint. (Courtesy of Scott Campbell)

- **Oblique angle lighting -** using a flashlight, camera flash or ALS at a very low angle to cast shadows that allow an imprint or impression to be photographed



Oblique light used to add contrast to a footprint. (Courtesy of Scott Campbell)

- **Macro lenses -** can take very close-up images (1:1 or 1:2) of small items such as tool marks or trace evidence



Cartridge case details captured with macro lens. (Courtesy of Scott Campbell)

Photographs should accurately document the lighting conditions at the scene. After those photos are taken, if necessary, a photographer will add artificial light, like a flash, to compensate for a camera's limitations in capturing the visible range of light under certain conditions.

8. **Shoot fast:** Sometimes environmental factors such as rain, snow or traffic can make conditions difficult for photography. The photographer must work quickly to capture as much visual documentation as possible from a deteriorating scene.

9. **Photograph the victim later:** If a victim must be moved or requires treatment, the photographer can go back to document the victim's injuries. Various techniques using special lighting and colored filters can highlight injuries (bruising, scarring) and healing status.

How It's Done

Who Conducts the Photographic Analysis and Enhancements

Once working copies of all the photographs have been created, investigators can select images for analysis and enhancement. This is normally done by the photographer or, if available, within the audio/visual department in the laboratory. As with all evidence, detailed records should be kept regarding who accesses or works with the files and what techniques were used to enhance or otherwise modify the files.

The International Association for Identification (IAI) has a Certified Forensic Photographer (CFPH) (http://www.theiai.org/certifications/imaging/index.php) program, established in 2001. The CFPH process is accredited by the Forensic Specialties Accreditation Board. This program requires specific training or coursework and testing that includes both written and practical assessments. Evidence Photographers International Council (EPIC) (http://www.evidencephotographers.com/) formerly provided specific certification for evidence photographers.

Many times, the images are taken by a member of the investigative team that is responsible for many crime scene duties that also incorporates photography. Depending on the size of the agency and support from their local laboratory, more experienced photographers may be available for major cases.

How and Where Evidence Photographs are Processed

All photographs taken are saved as originally captured, entered into evidence inventory and tracked. Selected photographs of particular evidence or parts of a scene may need additional enhancement. This can be done within the department if the appropriate software is available or may be sent to a regional specialist. The most common enhancements include cropping, brightness and contrast adjustments and color processing.

Potential photographic enhancements follow the same rules as news journalism. An image may be lightened and darkened, cropped or the color enhanced. The white balance can be adjusted, but adding or removing information is unacceptable. When submitted for courtroom use, the original photograph must be available for comparison and the technician or examiner must be able to show and describe any enhancements that were done, and why.

When images are presented, they must be clearly identified as a working and/or enhanced version. The original camera sequential numbering system should be retained to show that images are in order and none have been removed. The working images should not be renamed until identified or selected for use, and original files should not be renamed at all.

Type of Equipment Used

Investigators and technicians photographing a crime scene should have access to a good quality camera that is capable of manual override and has interchangeable lenses, off-camera flash, cable release, and a tripod mount. With these tools and a widely attainable level of training and practice, good quality photographs can be taken in a broad range of scenarios including low light, highly reflective surfaces and tight spaces.

That said, many first responders are equipped with basic, consumer-level point-and-shoot cameras. Since they may be in the best position to capture important evidence, basic knowledge of how to capture an image and use the camera they have is very important. Even with simple equipment, a first responder with introductory photography training can produce images of sufficient quality to support an investigation.

Cell phones and other personal electronic devices with integrated cameras are not recommended unless their use is an operational necessity. An example would be if a muddy shoe print is found near a crime scene but it is raining. The shoe print may disappear quickly, so if a cell phone camera is the only camera available, then it would be operationally necessary to use it.

FAQs

What are the limitations of crime scene photography?

The majority of evidence photography is now done using digital cameras and equipment. Limitations in photography are twofold: limitation of the camera in general and lack of experience or training of the photographer.

Cameras cannot produce the same view that the human eye sees; it is the photographer’s use of the camera settings that can affect what can or cannot be seen in a photograph. A trained photographer will recognize difficult lighting situations and adjust the camera settings accordingly. Often, more than one photo will be taken of the same view, in order to properly expose for widely varying conditions in a single view.

The use of digital cameras allows a crime scene photographer to instantly review their photos and make changes to the camera settings if needed to capture the best possible image while still on the scene. Critical thinking skills and analysis are constantly applied during the scene documentation process. An inexperienced photographer will often forgo the review process, relying on their camera to “make the right decisions” for settings.

How is quality control and assurance performed?

To ensure the most accurate capture, processing and analysis of crime scene photographs, the management of criminal justice agencies and forensic laboratories puts in place policies and procedures that govern facilities and equipment, methods and procedures, and personnel qualifications and training. These Standard Operating Procedures (SOPs) are intended to maintain and demonstrate the integrity of the images and information captured at a crime scene and its admissibility in court. Crime scene photography SOPs ensure uniform processes are used by photographers and the information represented in the images accurately represents objects and conditions at the scene as they are found.

The Scientific Working Group on Imaging Technology (SWGIT) works to set quality guidelines for the capture, storage, processing, analysis, transmission, output and archiving of images. These guidelines provide good general practice standards for crime scene photographers and other individuals performing photography within the criminal justice system. SWGIT guidelines are available (**https://www.swgit.org/documents**).

Is there anything else about crime scene photography that would be important to the non-scientist, or any common misconceptions regarding this topic?

A common misconception is that digital images can be changed more easily than film prints and done to mislead the court. Photographs created in a darkroom from film can also be altered by a skilled photographer using a wide variety of techniques, so they are not necessarily more accurate than digital images. While digital software exists that can make drastic changes to a digital image, a comparison of the altered image with the original makes any changes obvious. This is why proper chain-of-custody procedure and workflow is necessary.

According to the SWGIT guidelines: "Documenting image enhancement steps should be sufficient to permit a comparably trained person to understand the steps taken, the techniques used, and to extract comparable information from the image."

Similar to scientific research being documented to allow other scientists to perform the same steps and get the same results, image enhancement documentation should be specific and in order. The SWGIT guidelines include examples of documentation and draft SOPs (**https://www.swgit.org/pdf/Recommended Guidelines for Developing Standard Operating Procedures?docID=59**)(PDF download) for agencies to customize.

Another misconception may be reinforced by television crime dramas, and that is the idea that every crime scene unit and/or investigator has high-end camera equipment and is thoroughly trained in crime scene photography. Though many are, it should be clarified that equipment, training and procedures vary widely among agencies.

Common Terms

Terminology in photography has changed slightly since the rise of professional digital cameras to include information on digital equipment such as light sensors, as well as techniques for using computer software to enhance images. The definitions below represent common terms used in general and crime scene photography. For additional glossary terms see the SWGDE and SWGIT Digital & Multimedia Evidence Glossary (**https://www.swgit.org/pdf/SWGDE and SWGIT Digital and Multimedia Evidence Glossary?docID=60**) or the All Things Photography (**http://www.all-things-photography.com/digital-dictionary.html**) website.

Ambient Light - Light already existing in an indoor or outdoor setting that is not caused by any illumination supplied by the photographer.

Aperture - opening in the camera that lets in the light.

Aspect Ratio - The ratio of width to height in photographic prints; a ratio of 2:3 in 35 mm pictures produces photographs most commonly measuring 3.5 × 5 inches or 4 × 6 inches.

Camera Angles - Various positions of the camera (high, medium, or low; and left, right, or straight on) with respect to the subject, each giving a different viewpoint, perspective or visual effect.

Capture - The process of recording data, such as an image, video sequence, or audio stream.

Color Correction - To correct or enhance the colors within an image.

Contrast - The difference in darkness or density between one tone or another.

Cropping - Removing portions of an image that are outside the area of interest.

Depth of Field - The area between the nearest and farthest points from the camera that are acceptably sharp in the focused image.

Evidence Quality Photos - Images of sufficient size and quality to allow comparison and examination by a qualified forensic expert.

Exposure - The quantity of light allowed to act on photographic material; a product of the intensity (controlled by the lens opening) and the duration (controlled by the shutter speed) of light striking the film or sensor.

F-stop - Lens setting number indicating the size of the aperture that allows light into the camera. It is an inversely proportionate number, so that f/1.8 indicates a larger opening than f/5.6.

Filter - A colored piece of glass or other transparent material used over the lens to emphasize, eliminate, or change the color or density of the entire scene or certain areas within a scene.

ISO Speed - The sensitivity of a given film or sensor to light, indicated by a number such as ISO 200. The higher the number, the more sensitive or faster the film or sensor.

Lens Speed - The largest lens opening at which a lens can be set. A fast lens transmits more light and has a larger opening than a slow lens. For example, f/1.8 would set a larger opening than f/5.6 and would, therefore, be a faster lens.

Raw File - The data captured by a digital camera sensor before it is converted into an image file by software, either inside the camera or on a stand-alone computer.

Resolution - In a digital photograph, the number of pixels which make up the image.

Scale - The relative size of an object as compared to other objects in general proximity. Also refers to a measuring device or set of marks to indicate object size in a photograph.

Shutter - Blades, a curtain, plate, or some other movable cover in a camera that controls the time during which light reaches the film.

Working Copy - A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis.

Additional Resources

You can learn more about this topic at the websites and publications listed below.

Resources

Evidence Photographers International Council (EPIC)
http://www.evidencephotographers.com/

Scientific Working Group on Imaging Technology (SWGIT)
http://www.swgit.org

Professional Photographers Association (PPA) **http://www.ppa.com**

Stanford University Depth of Field
(**http://graphics.stanford.edu/courses/cs178-10/applets/dof.html**)

Stanford University Variables That Affect Exposure
(**http://graphics.stanford.edu/courses/cs178-11/applets/exposure.html**)

Crime Scene Resources Crime Scene and Evidence Photography
(**http://www.crime-scene-investigator.net/csi-photo.html**)

References

Robinson, E. **CRIME SCENE PHOTOGRAPHY, SECOND EDITION**, Elsevier Academic Press, Burlington, MA (2010).

Law Enforcement & Emergency Services Video Association (LEVA)(accessed June 27, 2012). **http://www.leva.org**

National Center for Audio & Video Forensics (NCAVF) (accessed June 27, 2012). **http://www.ncavf.com**

DSLR Camera Simulator CameraSim, SLR Photography Demystified. (accessed June 27, 2012) **http://camerasim.com/camera-simulator/**

Levoy, Marc; Adams, Andrew; Dektar, Katie; Willett, Nora. Variables that Affect Exposure, 2011. Flash applets on some technical aspects of photography (Stanford University CS 179 - Digital Photography). (accessed June 27, 2012) **http://graphics.stanford.edu/courses/cs178-11/applets/exposure.html**

McHugh, Sean. Understanding Depth of Field. Cambridge in Color. (accessed June 27, 2012) **http://www.cambridgeincolour.com/tutorials/depth-of-field.htm** (accessed June 27, 2012)

Acknowledgments

The authors wish to thank the following for their invaluable contributions to this forensic guide:

Becky Carter, CEP, National Forensic Science Technology Center

Denise Weigand, *Forensic Investigator*, Pasco County Sheriff's Department

Danny Nichols, National Forensic Science Technology Center

Forensic Evidence Admissibility and Expert Witnesses

How or why some scientific evidence or expert witnesses are allowed to be presented in court and some are not can be confusing to the casual observer or a layperson reading about a case in the media. However, there is significant precedent that guides the way these decisions are made. Our discussion here will briefly outline the three major sources that currently guide evidence and testimony admissibility.

The *Frye* Standard – Scientific Evidence and the Principle of General Acceptance

In 1923, in *Frye v. United States*[1], the District of Columbia Court rejected the scientific validity of the lie detector (polygraph) because the technology did not have significant general acceptance at that time. The court gave a guideline for determining the admissibility of scientific examinations:

> *Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while the courts will go a long way in admitting experimental testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be* **sufficiently established to have gained general acceptance** *in the particular field in which it belongs.*

Essentially, to apply the "*Frye* Standard" a court had to decide if the procedure, technique or principles in question were generally accepted by a meaningful proportion of the relevant scientific community. This standard prevailed in the federal courts and some states for many years.

Federal Rules of Evidence, Rule 702

In 1975, more than a half-century after *Frye* was decided, the Federal Rules of Evidence were adopted for litigation in federal courts. They included rules on expert testimony. Their alternative to the *Frye* Standard came to be used more broadly because it did not strictly require general acceptance and was seen to be more flexible.

[1] 293 Fed. 1013 (1923)

The first version of Federal Rule of Evidence 702 provided that a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

a. the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
b. the testimony is based on sufficient facts or data;
c. the testimony is the product of reliable principles and methods; and
d. the expert has reliably applied the principles and methods to the facts of the case.

While the states are allowed to adopt their own rules, most have adopted or modified the Federal rules, including those covering expert testimony.

In a 1993 case, *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* the United States Supreme Court held that the Federal Rules of Evidence, and in particular Fed. R. Evid. 702, superseded *Frye's* "general acceptance" test.

The *Daubert* Standard – Court Acceptance of Expert Testimony

In *Daubert* and later cases[2], the Court explained that the federal standard includes general acceptance, but also looks at the science and its application. Trial judges are the final arbiter or "gatekeeper" on admissibility of evidence and acceptance of a witness as an expert within their own courtrooms.

In deciding if the science and the expert in question should be permitted, the judge should consider:

- What is the basic theory and has it been tested?
- Are there standards controlling the technique?
- Has the theory or technique been subjected to peer review and publication?
- What is the known or potential error rate?
- Is there general acceptance of the theory?
- Has the expert adequately accounted for alternative explanations?
- Has the expert unjustifiably extrapolated from an accepted premise to an unfounded conclusion?

The *Daubert* Court also observed that concerns over shaky evidence could be handled through vigorous cross-examination, presentation of contrary evidence and careful instruction on the burden of proof.

[2] The "Daubert Trilogy" of cases is: **DAUBERT V. MERRELL DOW PHARMACEUTICALS**, **GENERAL ELECTRIC CO. V. JOINER** and **KUMHO TIRE CO. V. CARMICHAEL**.

In many states, scientific expert testimony is now subject to this *Daubert* standard. But some states still use a modification of the *Frye* standard.

Who can serve as an expert forensic science witness at court?

Over the years, evidence presented at trial has grown increasingly difficult for the average juror to understand. By calling on an expert witness who can discuss complex evidence or testing in an easy-to-understand manner, trial lawyers can better present their cases and jurors can be better equipped to weigh the evidence. But this brings up additional difficult questions. How does the court define whether a person is an expert? What qualifications must they meet to provide their opinion in a court of law?

These questions, too, are addressed in **Fed. R. Evid. 702**. It only allows experts "qualified … by knowledge, skill, experience, training, or education." To be considered a true expert in any field generally requires a significant level of training and experience. The various forensic disciplines follow different training plans, but most include in-house training, assessments and practical exams, and continuing education. Oral presentation practice, including moot court experience (simulated courtroom proceeding), is very helpful in preparing examiners for questioning in a trial.

Normally, the individual that issued the laboratory report would serve as the expert at court. By issuing a report, that individual takes responsibility for the analysis. This person could be a supervisor or technical leader, but doesn't necessarily need to be the one who did the analysis. The opposition may also call in experts to refute this testimony, and both witnesses are subject to the standard in use by that court (*Frye, Daubert*, Fed. R. Evid 702) regarding their expertise.

Each court can accept any person as an expert, and there have been instances where individuals who lack proper training and background have been declared experts. When necessary, the opponent can question potential witnesses in an attempt to show that they do not have applicable expertise and are not qualified to testify on the topic. The admissibility decision is left to the judge.

Additional Resources

Publications:

Saferstein, Richard. **CRIMINALISTICS: AN INTRODUCTION TO FORENSIC SCIENCE**, Pearson Education, Inc., Upper Saddle River, NJ (2007).

McClure, David. Report: Focus Group on Scientific and Forensic Evidence in the Courtroom (online), 2007,

https://www.ncjrs.gov/pdffiles1/nij/grants/220692.pdf (accessed July 19, 2012)

Acknowledgements

The authors wish to thank the following for their invaluable contributions to this guide:

Robin Whitley, *Chief Deputy*, Appellate Division, Denver District Attorney's Office, Second Judicial District

Debra Figarelli, *DNA Technical Manager*, National Forensic Science Technology Center, Inc.

About This Project

This project was developed and designed by the National Forensic Science Technology Center (NFSTC) under a cooperative agreement from the Bureau of Justice Assistance (BJA), award #2009-D1-BX-K028. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse, the contents herein.

National Forensic Science Technology Center®
NFSTC *Science Serving Justice*®
7881 114th Avenue North
Largo, Florida 33773
(727) 549-6067
info@nfstc.org

SWGIT

Scientific Working Group
Imaging Technology

Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: Chair@ swgit.org

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 1

Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System

*** Released previously as "Guidelines for the Use of Imaging Technologies in the Criminal Justice System* and "*Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System" ***

1. Introduction

Although digital imaging technologies have been used in a variety of scientific fields for decades, their application in the criminal justice system is more recent. Consequently, there has been a need to gather and disseminate accurate information regarding the proper application of this and other imaging technologies (including silver-based film and video) in the criminal justice system.

1.1 Mission Statement

The mission of the Scientific Working Group on Imaging Technology (SWGIT) is to facilitate the integration of imaging technologies and systems within the criminal justice system (CJS) by providing definitions and recommendations for the capture, storage, processing, analysis, transmission, and output of images.

1.2 SWGIT Membership

The Technical Working Group on Imaging Technology was formed by the Federal Bureau of Investigation in December of 1997. In 1999, the name of the group was changed to the Scientific Working Group on Imaging Technology (SWGIT). From the beginning the group has been comprised of individuals from federal, state, and local law enforcement agencies, the American military, academia, foreign law enforcement agencies, and other researchers. Those selected for membership in the group are experienced professionals working in the field of imaging technology or a related field and demonstrate the willingness to participate by consulting on the release of best practices and guidelines for the use of imaging technology in the Criminal Justice System. All SWGIT documents represent the consensus opinion of this membership and should not be construed as the official policy of any of the represented agencies.

1.3 Purpose of this Document

This document will familiarize the reader with important considerations in the capture, preservation, processing, and handling of images, whether the images are in digital, analog, or film format. This document will also refer the reader to other SWGIT documents for more complete details and guidelines.

1.4 Admissibility of Digital Images

Digital imaging is an accepted practice in forensic science, law enforcement, and the courts. Relevant, properly authenticated digital images that accurately portray a scene or object are admissible in court. Digital images that have been enhanced are admissible when the enhancement can be explained by qualified personnel.

1.5 Other SWGIT Documents

A complete list of documents that have been published by the SWGIT is attached.

2. Image Capture

"Capture" is the process of recording data such as an image or video sequence. The taking of photographs with a digital, film, or video camera is an example of capture. Digitizing images, documents, or objects with a scanner is another example of capture. When images are captured by those law enforcement or forensic laboratory personnel who are charged with the responsibility for processing or analyzing images, it is possible to control the equipment, methods, and techniques used. This may not be possible when images are captured by others and are submitted for processing or analysis. The handling of this evidence differs dependent on the source.

2.1 Image Capture Equipment

Image capture devices should be capable of rendering an accurate representation of the item or items of interest. Different applications will dictate different standards of accuracy. At a minimum, the following should be considered when selecting appropriate devices:

- Resolution requirements which are in turn driven by the intended use of the image (first responder, crime scene work, preserve impressions, etc.)
- Characteristics (size, movement, location, etc.) of the scene, item, or items of interest
- Lighting of the items of interest
- Dynamic range of the scene
- Time constraints
- Required end product(s)

Specific information and additional SWGIT recommendations relating to different law enforcement field applications may be found in the SWGIT document "*Field Photography Equipment and Supporting Infrastructure.*"

2.2 Image Compression

Compression is the process of reducing a digital file's size. Compression may be lossy or lossless. The decision to use lossy or lossless compression will be dictated by the intended use of the image. When lossy compression is used, critical image information can be lost and unwanted artifacts introduced as a result. Repeatedly saving a file using lossy compression may exacerbate the loss of image information. Therefore, if an image is to be subjected to scientific analysis and compression is necessary, lossless compression is strongly recommended. Likewise, due to the fact that the end use of an image cannot always be predicted, it is recommended that original images be recorded using no compression or lossless compression. If lossy compression must be used, then the lowest level of compression should be used.

Specific information and additional SWGIT recommendations relating to image compression may be found in the following SWGIT documents: "*Issues Relating to Digital Image Compression and File Formats*", "*Guidelines for Image Processing*", *"General Guidelines for Capturing Latent Impressions Using a Digital Camera", "General Guidelines for Photographing Tire Impressions", and "General Guidelines for Photographing Footwear Impressions".*

3. Image Integrity

A legal prerequisite to the admissibility of any evidence is that the evidence being offered in court can be authenticated. An exhibit is authenticated when there is sufficient evidence that the exhibit is what the proponent claims it to be. In the case of images the authentication requirement is usually satisfied when a witness can testify that the image accurately portrays the scene or objects that were captured. If authenticity is challenged, the proponent must be prepared to show that the image (or data) has not been altered.

In the case of images processed using advanced enhancement techniques, qualified witnesses must be able to testify concerning the process used.

3.1 Identifying and Handling the Original Image

A primary image refers to the first instance in which an image is recorded onto any media that is a separate identifiable object. An original image is an accurate and complete replica of the primary image, irrespective of media. See the SWGDE/SWGIT document "*SWGDE and SWGIT Digital & Multimedia Evidence Glossary*".

3.2 Preserving Original Images

The original image should be stored and maintained in an unaltered state. This includes maintaining original digital images in their native file format. To preserve the original image when processing is required SWGIT recommends:

- Film-based media originals may be processed if the processing is non-destructive.
- With analog video, minimal playback of the original is recommended to avoid degradation of signal.
- Original digital images should not be altered. Processing should be performed on working images only.

3.3 Archiving

Care must be taken to ensure that archival media is maintained in such a manner that the information contained thereon may be retrieved in the future (within statutory and agency guidelines).

Specific information and additional SWGIT recommendations relating to archiving may be found in the SWGIT document *"Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System"*.

4. Image Processing and Analysis

Image processing is any activity that transforms an input image to an output image. Image analysis, on the other hand, involves the application of image science and domain expertise to examine and interpret the content of an image and/or the image itself in legal matters.

Specific information and additional SWGIT recommendations relating to image processing and analysis may be found in the SWGIT documents "*Guidelines for Image Processing*" and "*Best Practices for Forensic Image Analysis*".

4.1 Documenting Image Enhancement

The intended use of the image dictates the level to which the enhancements are documented. Any processed image subjected to image analysis should be documented with an image processing log. An image not subjected to image analysis does not need an image processing log.

Specific information and additional SWGIT recommendations relating to image enhancement may be found in the SWGIT document "*Best Practices for Documenting Image Enhancement*".

4.2 Software

Software used in processing and analyzing digital images should produce consistent results, permitting comparably trained personnel to achieve comparable analytical results.

LEGAL NOTE: Manufacturers of software used for image processing may be required to make the software source code available to litigants, subject to an appropriate protective order designed to protect the manufacturer's proprietary interests. Failure on the part of the manufacturer to provide this information to litigants could result in the exclusion of imaging evidence in court proceedings. This should be considered when selecting software.

5. Outputting Images

An output device should be capable of producing an accurate representation of the input image. The following should be considered in the selection of output devices:

- Final use of image
- Time constraints
- Longevity/permanence of output image
- Spatial resolution required
- Range of colors and brightness to be produced

6. Distributing Images

Received images should accurately reflect the distributed images. The following should be considered in the selection of distribution methods and transmission devices:

- Final use of image
- Time constraints
- File size
- Security of transmission
- Integrity of transmission
- Hardware and software compatibility of transmitters and receivers
- File format compatibility

7. Quality Assurance

Personnel utilizing images and imaging technology in the criminal justice system should implement quality assurance programs to ensure that results achieved are repeatable and valid. As part of these programs, performance checks and corrective actions should be documented.

7.1 Equipment

Where applicable, equipment utilized in imaging should be checked regularly for proper performance and calibration, and findings documented. Where applicable, an end-to-end system check for consistency within specified system parameters should be performed on a regular basis and whenever modifications are made to the system. All equipment should be maintained according to the manufacturers' specifications and recommendations as contained in the operating manuals.

When a piece of equipment or a system falls outside the specifications and recommendations, the equipment or system should be taken out of service until it has been corrected. Evaluation of equipment and system checks should be documented to include corrective actions.

7.2 Software

If software errors that significantly affect the results of a processing step are detected, then corrective actions should be taken. If the manufacturer identifies software errors and provides corrective remedies for them, the remedies should be implemented before the software is used again. Once corrective actions have been taken, an end-to-end system check should be performed prior to putting the system back into operation.

7.3 Personnel and Training

All personnel utilizing imaging technologies shall be trained and competent in the operation of the relevant imaging technologies.

Issues relating to personnel and training in imaging technology are addressed in the SWGIT documents, “*Guidelines and Recommendations for Training in Imaging Technology in the Criminal Justice System*”, “*SWGDE/SWGIT Guidelines and Recommendations for Training in Digital and Multimedia Evidence*” and “*SWGDE/SWGIT Proficiency Test Program Guidelines*”.

7.4 Standard Operation Procedures (SOPs)

Personnel engaged in the capture, storage, processing, analysis, transmission, or output of imagery in the criminal justice system should ensure that their use of images and imaging technology are governed by documented policies and procedures.

For issues relating to SOPs see SWGDE/SWGIT “*Recommended Guidelines for Developing Standard Operating Procedures*”.

SWGIT

Scientific Working Group
Imaging Technology

Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: Chair@swgit.org

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 11

Best Practices for Documenting Image Enhancement

INTRODUCTION

A fundamental goal of this and other Scientific Working Group on Imaging Technology documents is to ensure the production of quality forensic imagery for use as evidence in a court of law. The specific purpose of this document is to describe best practices for documenting image enhancement used in the criminal justice system and to provide laboratory personnel with instruction regarding the level of documentation that is appropriate when performing a variety of enhancement operations on still images, regardless of the tools and devices used to perform the enhancement.

Accurate documentation is necessary to satisfy the legal requirements for introducing forensic images as evidence in a court of law and to allow other professionals to understand the enhancement and produce comparable results.

The general principles and procedures used are the same regardless of the format or media in which the images are recorded. Therefore, in this document the word *image* refers to any image recorded on any media (e.g., conventional photographic, electronic, magnetic, or optical media, etc.).

Note: The Best Practices described below are predicated on the assumption that an original file/image that has been subjected to processing be preserved.

IMAGE ENHANCEMENT POSITION

Image enhancement has been used in forensic applications since the 1840s and is an accepted practice in forensic science, regardless of whether it is performed in a traditional wet chemistry darkroom or in a laboratory equipped only with electronic devices, such as computers, scanners, and/or video capture systems.

IMAGE CATEGORIES

The degree to which procedures used in image enhancement should be documented will depend on the intended end use of the image. Furthermore, the nature of such documentation will depend on the procedures used.

The Scientific Working Group on Imaging Technology recognizes two fundamental end uses for images encountered in the legal system.

Category 1

Category One images are used to demonstrate what the photographer or recording device witnessed but are not analyzed by subject matter experts. These can include, but are not limited, to the following:

- General crime scene or investigative images

- Surveillance images
- Autopsy images
- Documentation of items of evidence in a laboratory
- Arrest photographs, such as mug shots

Category 2

Subject matter experts use Category Two images for scientific analysis. These can include, but are not limited, to the following:

- Latent prints
- Questioned documents
- Impression evidence
- Patterned evidence
- Category 1 images to be subjected to analysis

ENHANCEMENT TECHNIQUES

Basic

Basic image enhancement techniques are those used to improve the overall appearance of the image. When one visually compares an original image to that same image after basic enhancement, a trained professional should be able to produce comparable results even in the absence of documentation of specific parameterization or software settings. These techniques can be applied over an entire image and in localized areas in an image. They include, but are not limited to, the following:

- Brightness and contrast adjustment, including dodging and burning
- Resizing (file interpolation)
- Cropping
- Positive to negative inversion
- Image rotation/inversion
- Conversion to grayscale
- White balance
- Color balancing and/or color correction
- Basic image sharpening and blurring (pixel averaging)

- De-interlacing

There can, of course, be both simple and complex ways of doing certain task. For example, there may be many ways to create grayscale representations of color images ("conversion to grayscale"). When complex techniques are used, they should no longer be considered "basic".

Advanced

While advanced image enhancement techniques may also be applied to improve the overall appearance, they are often also used to extract specific information contained in the image. These techniques which are not easily approximated by a trained professional without documentation of specific parameterization or software settings. The techniques include, but are not limited, to the following:

- Frame averaging
- Fourier Analysis (including the use of FFT)
- Deblur
- Noise reduction
- Image restoration
- Color channel selection and subtraction
- Perspective control and/or geometric correction
- Advanced sharpening tools, such as unsharp mask

DOCUMENTATION – What is needed

Category 1 Images

When enhancing Category One images, one need only document the techniques with a standard operating procedure that describes the typical enhancement processes. If an original image previously treated as a Category One image is to be subjected to scientific analysis, it becomes a Category Two image.

Category 2 Images

The use and sequence of any enhancement techniques in Category Two images should be documented in every case.

Documenting image enhancement steps should be sufficient to permit a comparably trained person to understand the steps taken, the techniques used, and to extract comparable information from the image. Documenting every change in every pixel value is discouraged because it adds nothing of value to the analysis.

Exploratory enhancement operations not incorporated in the final image do not need to be documented. Test prints and/or intermediate images resulting from a variety of techniques not incorporated into the final image should be discarded.

Minimum requirements for documentation of advanced techniques include identifying the software application and/or techniques as well as the settings and parameters used. Automated processes, such as running user-defined macros, require only documenting usage if the process is defined in the agency documentation.

DOCUMENTATION – How to do it

Documentation can be recorded in a variety of ways including hand-written notes, electronic recording, or through the use of automated logging tools, or incorporated into the final report.

The following examples are intended to represent the documentation level appropriate for Category Two images. Following these recommendations will help fulfill the requirements for the admissibility of images in a court of law. In addition to the examples below, a sample SOP which includes the use of automated logging is provided in the appendix.

Examples:

Brightness and contrast and/or contrast adjustment

> *I printed the Q5 image using Kodabromide II grade 4 RC paper. The tread area was burned in to increase detail.*

Unsharp mask (strength, distance, threshold)

> *In software application X, version N, I used unsharp mask at strength = 100%, with distance = 1.5 pixels, and threshold of 3 levels.*

Multiple image averaging (number of images used, which images used, individual image weights)

> *I averaged 4 images (Q1_01.tif; Q1_02.tif; Q1_03.tif; and Q1_04.tif) with equal weighting*

Fourier Analysis (Fast Fourier Transform – FFT) (Identify region of interest, and edits performed on spectrum, such as spike cut, spike boost, low pass filter and high pass filter)

> *Selected the region of interest to include the vehicle, performed a forward FFT operation, edited the spectrum, using spike cut on the repetitive signal, then performed the inverse Fourier transform.*

Noise reduction (Type, such as despeckle, Gaussian blur)

I reduced noise in the image by applying an IIR Gaussian blur.

Color channel selection and removal

I removed the red channel by deleting it.

Perspective control and/or geometric correction (scale, rotation or degree, perspective, skew)

I rotated the image 90 degrees clockwise.

User-defined macro (macro name)

In Adobe Photoshop Version 7.0, I used Action Video Process 1 (defined in agency documentation).

Appendix

SAMPLE
STANDARD OPERATING PROCEDURE

Title: Latent Print Image Processing **Approval Date _________**

____
Reviewer Signature

____________________________ __________________________________
Technical Leader Signature **Forensic Services Director Signature**

Purpose: To establish a list of actions to enhance latent print images requested by latent print analysts.

Procedures:

1. Log into the agency-approved software application for processing latent prints.

2. Select the case containing the images to be processed.

3. On the menu bar, click Image, Enhance. The program will make a copy (working image) of the original image and import the copy and the enhanced image history into the agency-approved enhancement software application.

4. Process the working image using enhancement techniques. All processes applied to the working image are recorded using the enhanced image history tool. Approved processing techniques for use on working images are those that have direct counterparts in traditional darkrooms including brightness and contrast adjustment, dodging and burning, and color balancing. The tools include Brightness/Contrast, Levels, Curves, Color Balance, Hue/Saturation, and Invert. Using Mode, Channels, and Fast Fourier Transform filters (FFT) are acceptable. The following tools are prohibited: Rubber Stamp, Airbrush, Paintbrush, Paint Bucket, Eraser, and Blur.

5. After the working image is processed and the processes are recorded, save the changes to the processed working image. Import the processed working image back into the latent print processing application.

6. The operator may now process additional images, export a processed image for printing, or exit the application.

Safety Considerations: None.

Limitations: Based on existing equipment and technology.

Quality Control: Perform appropriate equipment maintenance to ensure proper capacity and quality performance.

Literature References: User Manual.

SWGIT

Scientific Working Group
Imaging Technology

Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: Chair@swgit.org

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 17

Digital Imaging Technology Issues for the Courts

INTRODUCTION

Digital photography and imaging technology has its background in technology from the 1940s. The first camera designed to create photographs represented by a digital file was developed in the 1960s. Just as color film was a normal progression of the technological evolution from black and white film, electronic/digital imaging is a normal progression of the technological evolution from silver-halide based film.[1] Today, digital imaging technology is regularly encountered in the courts around the world. The goal of this document is to discuss the proper use of digital imaging technology through the dissemination of information to judges and attorneys. This document is designed to present the relevant issues in plain language to maximize the effectiveness of the courts when dealing with this technology.[2]

This document will provide the reader with citations to case law and scientific and technical research articles dealing with digital imaging technology used within the criminal justice system.

This document will also address some of the common myths and misconceptions associated with digital imaging technologies used in the criminal justice system. For additional information readers should become familiar with the basics of digital imaging technology. Information on these basics can be found in several documents released by SWGIT.

DEBUNKING MYTHS AND MISCONCEPTIONS

One of the most challenging issues facing the legal community in dealing with digital imaging technology is separating fact from fiction. “Expert” advice is readily available, but may be inconsistent, impractical, and biased. Despite the misinformation to the contrary, digital imaging technology in the hands of a competent, properly trained practitioner, is appropriate for use in a forensic setting and produces results that are admissible in judicial and similar fact-finding proceedings.

MYTH: “Film is better than digital because film cannot be altered or manipulated.”

FACT: Both film and film-based images can be manipulated. Traditional film and photographs have been manipulated for over 100 years, and the integration of film and digital technologies allows the production of manipulated negatives that can be indistinguishable from the results of traditional film photography. Fortunately, in most cases, manipulation is detectable by those trained to do so. Ultimately, it is the integrity and abilities of the practitioner, established processes, and accepted practices that make film and digital equally valuable in the courtroom.

MYTH: "Because digital images can be manipulated, they should not be admissible."

FACT: The integrity of digital images can be assured. There are methods that demonstrate digital file integrity including hashing functions, visual verification, digital signatures, written documentation, and checksums/cyclical redundancy checks.[3] Additionally, experts may be capable of determining whether a digital image, film photograph, or film negative has been altered. When evidence is produced suggesting an alteration, experts can be used in an attempt to confirm or refute the assertion.[4]

MYTH: "Digitally enhanced images should not be admissible."

FACT: Digitally enhanced images that reveal features that exist in the image but not immediately apparent through visual examination have historically been found to be valid and admissible evidence in courtroom proceedings. Case law supports the admissibility of digitally enhanced images. Both *Frye* and *Daubert* challenges to the use of this technology have been resolved in favor of admission of digitally enhanced images. A digital image or film photograph that has been altered or enhanced that produces an output that does not accurately and fairly depict what was captured does present admissibility issues. For example, if a blue car is the subject of a photograph and the image is changed to make the car appear red, such an image would certainly be subject to objection and explanation. On the other hand, an image that has been enhanced to reveal a fingerprint on a patterned background by removing the background pattern should be admissible because the nature of what the image depicts (a fingerprint) has not been changed. In this respect, one does well to remember that under rules of evidence an "original" of the data (which is what is created when a digital photograph is captured) is not restricted to the data itself, but "any printout or output readable by sight, shown to reflect the data accurately." Federal Rule of Evidence 1001(3).

MYTH**:** "When images are digitally enhanced they must be reproducible, and these reproductions must be "*bit-for-bit*" copies of each other."

FACT: Digitally-enhanced images must be reproducible; however, when images are enhanced the bit values change. Two persons using the same techniques, producing images visually indistinguishable from each other, will get different bit values. This is an expected and normal occurrence that should not affect the admissibility of the image. Reproducibility is judged by obtaining visually comparable results, not identical bit values.

MYTH: "Film always has higher resolution (detail) than digital."

FACT: As digital imaging technology advances, output quality approaches and sometimes surpasses that achieved by traditional photography. Output quality depends upon a number of factors including the camera's optics, sensor or film, method of printing or display, and photographic technique. Any of these can limit the quality of the final product and a digital camera's sensor resolution is often not the limiting factor. In addition, the highest possible resolution is not always necessary to accurately and fairly depict what has been captured with film or a digital camera. Film photographers, for example, do not always find it necessary to use the type of film that has the highest resolution.

MYTH: "Digital cameras do not accurately represent color."

FACT: Digital cameras are neither more nor less accurate in depicting color than film cameras. No imaging technology can exactly reproduce the human visual system. The color rendition of an image is dependent on a number of factors. Although the method used in processing color differs between film and digital imaging technologies, both are capable of producing accurate results.

MYTH: "Localized adjustments such as dodge and burn should never be used in the digital enhancement of images."

FACT: Localized adjustments are appropriate under many circumstances. The dodge and burn technique is one that has its roots in traditional darkroom technology. When the technique is applied appropriately, it can greatly improve the visibility and usefulness of evidence. This processing technique *can* be documented by the practitioner.[5]

MYTH: "Digital enhancement of a fingerprint image can accidentally morph the fingerprint of one person into that of another."

FACT: When digital image enhancement is performed according to accepted guidelines and standards, it is not possible to change one person's fingerprint into another's. The end result of properly enhancing any image is an increase in the visibility of characteristics of interest within the image. Research completed at Indiana University Purdue University Indianapolis (IUPUI), Mathematical Sciences Department, found that the possibility of such an occurrence to be one in 10-to-the-80th power (1 followed by 80 zeroes). This number is approximately equal to the number of atoms in the universe.[6]

MYTH: "All digital images must be electronically authenticated to be admissible."

FACT: A digital image (as well as a film photograph) can be authenticated through testimony or other evidence that the image is a fair and accurate representation of what it purports to depict; electronic authentication is not required. Image integrity must not be confused with the requirement to authenticate evidence as a precondition for admissibility in court.[2,4] Courtroom authentication of an image substantiates that the image is a fair and accurate representation of what it purports to be, whereas integrity verification is the process of confirming that the image presented is complete and unaltered since time of acquisition. The integrity of digital images can be verified through a number of means, some of which are not electronic.

MYTH: "Image files should be left on the camera's removable flash media and the flash media must be available in court as a condition precedent to admissibility of the image."

FACT: Most removable flash media is designed as temporary storage. Flash media cards that are stored for long periods of time are prone to data corruption that leads to loss of images. Excessive heat or cold, shock, and other improper handling and storage techniques can all put flash media at peril of losing data.

MYTH: "Any copy (duplicate) of a digital image made from the camera's media is not an original."

FACT: When the contents of a camera's media is copied to a hard drive, CD, or DVD by a method which accurately reproduces the data on the camera's media, a duplicate of that data is created. Federal Rule of Evidence 1001 (4). Furthermore, "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Federal Rule of Evidence 1003. This legal result is the same as what has happened digitally; the process of correctly copying the data from the camera's media to another media creates identical data. Copying the data from one media to another is analogous to producing multiple original prints from a negative.

MYTH: "Compression of digital images or video is always bad."

FACT: *C*ompression can be appropriate depending on the intended use of the image or video. Compression should be used with care to avoid material degradation of the image. The use of compression, if over applied, can degrade the quality of the image, but it does not change the subject of the image into a different one.[7]

MYTH*:* "Compressed images, such as those captured in JPEG format, are not suitable for comparative or analytical purposes*.*"

FACT: It is preferable to capture images that are intended for comparative or analytical purposes using uncompressed formats; however, lossy compressed formats like JPEG may be used if the examiner determines sufficient detail is present in the image for such analysis.

MYTH: "All digital images must be treated as evidence and tracked with a chain of custody."

FACT: Many digital images do not require a chain of custody. Whether a chain of custody is established for a digital file is determined by the reason for which the file has been created or is being maintained and will vary between jurisdictions. For example, seized evidence almost always requires a chain of custody. Images produced or enhanced in a laboratory setting do not always require a chain of custody.[2]

MYTH: "All digital imaging equipment must be calibrated to be used in a forensic setting."

FACT: The requirement for calibration of equipment is determined by individual agencies and manufacturers, based on the type of equipment and their function. The need for calibration generally exists in equipment that performs quantitative or numerical analysis. When required, visual comparison of digital images can suffice as calibration of digital imaging equipment.

MYTH: "Potential jurors understand how digital imaging is used in a forensic setting."

FACT: Due to the technical and potentially labor intensive nature of forensic imaging, most outside the discipline do not understand the difference between forensic image processing and artistic editing of images. Laypersons exposed to mass media depictions of forensic science such as novels, dramatic cinema, and television programming may not have an accurate understanding of the science and its limitations. The media has a tendency to highlight forensic tools and techniques that pique the audience's interest while often disregarding realism in their application and the time frames required to obtain results. For example, Richard Catalani, writer for the television drama *CSI: Crime Scene Investigatio*ns writes, "*CSI*, admittedly, tends to focus on the more interesting and novel forensic techniques, and not on more realistic, tedious, labor-intensive searches, when no one finds the needle in the haystack."[8]

MYTH: "An expert is required to lay a foundation for any digital images introduced in court."

FACT: When images that have been subjected to processing to reveal information are being offered in court, a subject matter expert will usually be required to explain the process used. On the other hand, when traditional darkroom type adjustments are applied these are easily understood without the need for an expert. For example, an enlargement or brightening.

MYTH: "Watermarking does not change the original image."

FACT: Watermarking is a potentially irreversible process of embedding information into a digital signal. It modifies the content of the files and can persist as a part of the file. This process may change the image content as it was captured by the camera. Watermarking may occur at the time of recording, at the time the video or images are exported from the system, or during post-processing. Watermarking is not recommended.

MYTH: "For the purposes of CCTV recordings, one type of compression is always superior to another."

FACT: CCTV recordings should not be rated solely on the type of compression used, but on the quality and suitability of the entire system. In addition to the type of compression used, other factors within the system affect the quality of CCTV recordings. These include, but are not limited to: lighting, frame size, frame rate, camera quality/optics/placement, environmental factors, and method of collection/output.

MYTH: "The use of cell phone or other electronic devices that have integrated cameras are perfectly acceptable for crime scene documentation."

FACT: Although cell phones and other electronic devices have integrated cameras, the technology has not advanced to the quality necessary for proper crime scene or other forensic purposes. Cellular telephone and other personal electronic devices with digital cameras should not be used unless their use is an operational necessity.

MYTH: "For video to be of evidentiary value, there is a minimum recorded frame rate required."

FACT: NTSC is a common video standard in the US that specifies a frame rate of 29.97 frames per second, referred to as real time. In an effort to reduce hardware requirements (e.g. storage) video is often recorded at a lower frame rate. Lower frame rates may reduce the likelihood of determining activities within a scene but do not negate the value of the video. The evidentiary weight of video should be determined on a case by case basis.

MYTH: "Images should never have their metadata modified or removed as this will invalidate them for forensic use."

FACT: While it is best practice to maintain digital image files in an unaltered state from time of capture, separation of image content from metadata may not invalidate them for forensic use. In the majority of cases, the visual interpretation of an image is not affected by conditions of capture reflected in the metadata. In some cases the presence of metadata is necessary for the analysis of the image.

CASE LAW

Many cases exist in various courts throughout the United States and other countries where digital imaging technology has been challenged and successfully admitted into evidence. This section of the document is designed to provide the reader with case law citations in which issues of admissibility have been addressed.

This list is intended as a starting point for researching such case law.

***ISSUE*: Fair and Accurate Representation of the Scene**

CASE: *Almond v. State*, 553 S.E.2d 803, 805 (Ga. 2001)

***ISSUE*: Digital Manipulation vs. Processing**

CASE: *English v. State, 422 S.E.2d 924 (Ga. Ct. App. 1992)*
CASE: *US v. Mosley, 35 F.3d 573 (9th Cir 1994)*
CASE: *Nooner v. State, 907 S.W. 2d 677 (Ark. 1995)*
CASE: *Washington v. Hayden, 950 P.2d 1024 (Wash. App. 1998)*
CASE: *US v. Beeler, 62 F. Supp. 2d. 136 (D.Me 1999)*
CASE: *Dolan v. State, 743 So. 2d 544 (Fla. App. 1999)*
CASE: *State v. Hartman, 93 Ohio St.3d 274 (Ohio 2001)*
CASE: *Rodd v. Raritan Radiologic Associates, PA et al., 860 A.2d 1003 (N.J. Super. 2004)*
CASE: *Kennedy v. State, 853 So. 2d 571 (Fla. App. 2003)*
CASE: *Hartman v. Bagley, 333 F.Supp. 2d 632 (N.D. Ohio 2004)*
CASE: *State v. Swinton, 847 A.2d 921 (Conn. 2004)*

***ISSUE*: Video**

CASE: *Commonwealth of Pa. v. Auker, 681 A. 2d 1305 (Pa. 1996)*
CASE: *US v. Beeler, 62 F. Supp. 2d. 136 (D.Me 1999)*
CASE: *Dolan v. State, 743 So. 2d 544 (Fla. App. 1999)*

Canadian Case Law

CASE: *R v Mohan (1994)2S.C.R.9*
CASE: *R v Nikolovski (1996) 3 S.C.R. 1197*
CASE: *R v C (P.T.)–(2000) B.C.J.No 446;*
CASE: *R. v. Cooper(2000) B.C.S.C 342;*
CASE: *R v Kucerova(2001) B.C.J. No 358;*
CASE: *R v Mackay(2002)SKQB 316;*
CASE: *R v Penny(2002)N.J. No.70;*
CASE: *R v Pasqua(2008) A.J. No. 184 or ABQB 128.*

United Kingdom Case Law

CASE: R v W & ANTHONY BEST (2006)
CASE: R.v. Birch et al (1992)

SCIENCE AND TECHNICAL PUBLICATIONS

In addition to the cited legal cases, the following references might prove useful to the reader.

Hak JD, Jonathan W., *The Admissibility of Digital Evidence in Criminal Prosecutions*, DOJ- Alberta Canada, 2003
http://www.khodges.com/digitalphoto/hak.pdf

Conviction Through Enhanced Fingerprint Identification, Re-printed in "The Print" 10(2) February 1994, pp1-2
http://www.scafo.org/library/100201.html

Barakat JD., Brian and Miller JD., Bronwyn, *Authentication of Digital Photographs Under the "Pictorial Testimony" Theory: A Response to Critics*, Florida Bar Journal July 2004, pp38
http://www.floridabar.org/DIVCOM/JN/JNJournal01.nsf/76d28aa8f2ee03e185256aa9005d8d9a/1703e6eec2b2a74385256ec100751bda?OpenDocument&Highlight=0,barakat*

Berg, Erik C., *Legal Ramifications of Digital Imaging in Law Enforcement*, Forensic Science Communications October 2000 Volume:2 Number:4, United State Department of Justice, Federal Bureau of Investigation, Washington DC
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm

Nagosky, David P., *The Admissibility of Digital Photographs in Criminal Cases*, FBI Law Enforcement Bulletin, December 2005 Volume:74 Number:12, United State Department of Justice, Federal Bureau of Investigation, Washington DC
http://www.fbi.gov/publications/leb/2005/dec2005/dec05leb.htm

United Kingdom House of Lords, Science and Technology Committee 5th Report, 1997-1998, *Digital Images as Evidence*.
http://www.publications.parliament.uk/pa/ld199798/ldselect/ldsctech/064v/st0501.htm

United Kingdom. Home Office Scientific Development Branch Digital Imaging Procedure. Version 2.1 November 2007. Publication Number 58-07. Crown Copyright 2007, ISBN: 978-1-84726-559-3
http://science.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web).pdf?view=Standard&pubID=555512

Kashi, Joe, Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata, June 2006 Law Practice Today, American Bar Association
http://www.abanet.org/lpm/lpt/articles/tch06061.shtml#bio#bio

Robinson, Edward M. *Crime Scene Photography*, Academic Press, Elsevier, Burlington MA (2007)

Davies, Adrian and Fennessy, Phil. *Digital Imaging for Photographers, 4th ed.*, Focal Press, Elsevier, Burlington MA, (2001)

[1] IAI Resolution 97-9

[2] SWGIT Section 1 *Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System*

[3] SWGIT Section 13 *Best Practices for Maintaining the Integrity of Digital Images and Digital Video*

[4] SWGIT Section 14 *Best Practices for Image Authentication*

[5] SWGIT Section 11 *Best Practices for Documenting Image Enhancement*

[6] Li, Fang. "*Probability of False Positive with an Innocent Image Processing Routine*", Journal of Forensic Identification, V:58, I:5, (2008) Pg:551-561.

[7] SWGIT Section 5 *Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System*

[8] Yale Law Journal, http://yalelawjournal.org/2006/02/catalani.html