



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: SWGIT@yahoogroups.com

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: Compression 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: "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 Investigations* 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 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.

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. Auken*, 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.khodes.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](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>

REFERENCE LIST

SWGIT and SWGIT/SWGDE documents can be found at:

<http://www.theiai.org/swgit/index.html>

<i>Section</i>	<i>Title</i>
Section 1	Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System
Section 2	Considerations for Managers Migrating to Digital Imaging Technology
Section 3	Guidelines for Field Applications of Imaging Technologies in the Criminal Justice System
Section 4	Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions
Section 5	Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System
Section 6	Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System
Section 7	Best Practices for Forensic Video Analysis
Section 8	General Guidelines for Capturing Latent Impressions Using a Digital Camera
Section 9	General Guidelines for Photographing Tire Impressions
Section 10	General Guidelines for Photographing Footwear Impressions
Section 11	Best Practices for Documenting Image Enhancement
Section 12	Best Practices for Forensic Image Analysis
Section 13	Best Practices for Maintaining the Integrity of Digital Images and Digital Video
Section 14	Best Practices for Image Authentication
Section 15	Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System
Section 16	Best Practices for Forensic Photographic Comparison
Section 17	Digital Imaging Technology Issues for the Courts
SWGIT/SWGDE	Proficiency Test Program Guidelines
SWGIT/SWGDE	Guidelines and Recommendations for Training in Digital and Multimedia Evidence
SWGIT/SWGDE	Recommended Guidelines for Developing Standard Operating Procedures
SWGIT/SWGDE	Glossary of Terms