

# Admissibility of Digital Photographs in Criminal Trials



Keith Hodges, Senior Instructor, [Keith.Hodges@dhs.gov](mailto:Keith.Hodges@dhs.gov)  
Federal Law Enforcement Training Center  
Glynco, GA

Digital Photos - IACP 2008



# What we will discuss

- Digital photos captured by law enforcement.
  - If seized, use your digital forensics folks.
- Focus on smaller departments.
- Legal requirements to admit digital photos.
  - And how officers meet them.
- How the defense attacks our digital photos.
  - And how we meet that challenge.
- Handling digital photos from scene to court.
- Altered and enhanced digital photos.

# Digital Cameras – The Bad

---

- Resolution not quite as good as film.
  - But good enough in most cases.
- New equipment and training costs.
- Judges and prosecutors not digitally literate.
- Mistrust due to the alteration fairy.

# Digital Cameras – The Good

---

- Cheaper than equivalent film cameras.
- Can see results immediately.
- Faster and cheaper to share photos.
- Reduced printing and processing costs.
  - “Film” is free.
- Usually easier to use.

# Are Digital Photos Admissible ?

- **Yes.** No court has held a digital photo is inadmissible just because it is digital.
- “We are aware of **no authority**, and appellant cites none, for the proposition that **the procedure for admitting pictures should be any different when they were taken by a digital camera.**” *Almond v. State*, 274 Ga. 348 (Ga. 2001)
- “ ... we **do not agree** that this court should impose a **higher burden of proof for the admissibility of digital photographs** merely because digital images are easier to manipulate.” *Owens v. State*, 363 Ark. 413, 421 (Ark. 2005)

# This says it all ...

- “When, as here, the .... photograph is generated as a digital image .... the judge must determine whether the image **fairly and accurately presents what it purports to be**, whether it is **relevant**, and whether its **probative value outweighs any prejudice** to the other party.” *Renzi v. Paredes*, 452 Mass. 38, 52 (Mass. 2008)

# Requirements to Admit Digital Photo

- Like *ALL* evidence.
  - **Relevant** (tends to prove something)
    - And probative value does not substantially outweigh prejudicial effect.
  - **Authentic** (a foundation)
  - Meets **Best Evidence** requirements

# Authentication = Foundation

- FRE 901(a).
- The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.
- “This is photo is a fair and accurate portrayal of X.”



# Elements of a Foundation

1. The witness is familiar with the object or scene.
  2. The witness can explain his/her familiarity.
  3. The witness recognizes what is depicted.
  4. **The photo is a fair – accurate – true – good - depiction of the scene.**
- 
5. (No alterations or deletions.)
  6. (Enhancements documented.)

(Imwinkelried, *Evidentiary Foundations*)

# The Foundation Issue

- Claims the photo has been altered.
  - The *alteration fairy* defense.
- Digital photos ....
  - Can be easily altered (accidentally or on purpose).
  - Can be deleted (accidentally or on purpose).
  - The above can be hard to detect.
- Whether realistic unimportant ....
  - Judges and juries believe it so.



# Claims of Alteration

- Party must offer some evidence of alteration.
- “.... we further disagree .... that expert testimony of no alteration was required when there was no indication that the still photographs had been enhanced .... or altered in any way.”  
*Owens v. State*, 363 Ark. 413, 421 (Ark. 2005)
- “The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility.” [Alteration of business data]. *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. Or. 1988)

# “Weight, and not admissibility”

- Possibility of alteration – with no supporting evidence – doesn’t go to admissibility.
- It can go to “weight”.
  - That is, the jury can buy into the alteration fairy.
- Solution: good foundation testimony.
  - I did not alter, and no one else did.
  - “Fair and accurate representation.”

# How 'bout this ??

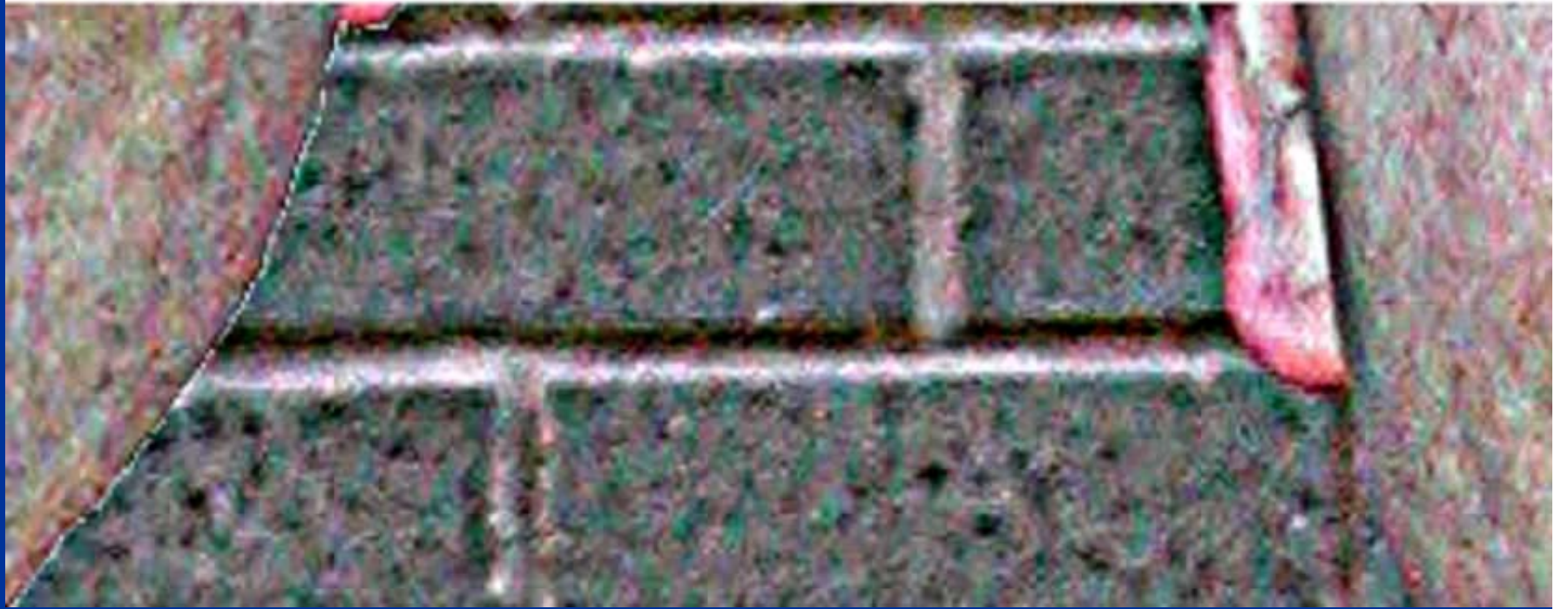
- “... a mere claim that photographs may be altered should not bar their admission. The proponent is not required to prove a negative.” *United States v. Harris*, 55 M.J. 433, 440 (C.A.A.F. 2001)

# Is this altered? (Expert required)



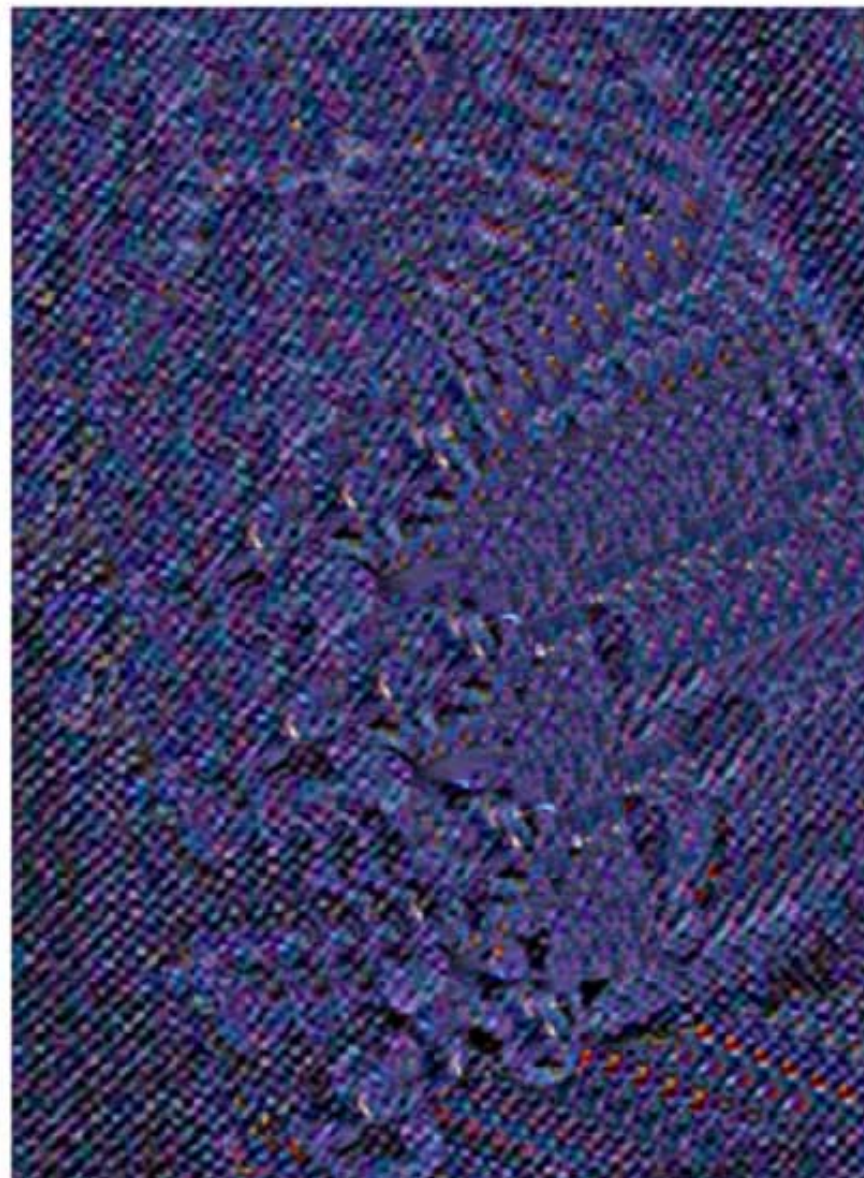


Digital Photos - IACP 2008





# Missing Patch - Unsharp Mask



# Defeating the Defense



- **Reduce opportunities** for alteration or deletion (accidental or intentional).
- Establish a **SIMPLE procedure** to handle digital photos.
  - And follow it.

# Opportunities to Alter or Delete

- Staged scene before photo taken.
- When photo taken (cropping, lighting, angle, etc.)

---

- Right after photo taken
  - Deletion from camera media.
  - Alteration of original media in a camera or computer.
- While transferring images from camera media to other media.
- While photo is in later possession of law enforcement
  - Evidence room.
  - On a computer (and LAN).
  - In officer's possession.

Credibility

Credibility

+

Procedure

# Handling Overview

- **GOAL:** Move images to stable, unalterable media ASAP, by:
  - Limiting access to the flash media.
  - Not deleting or altering images.
  - Keeping media away from electronic devices.
  - Burning all images to CD-R/DVD-R.
  - Confirming burn.
  - Documentation.

# Recommendation 1

One photographer handles the camera.

(or at least, keep media cards separate)

- So, the witness can testify:
  - “I had the camera, and I never altered or deleted any photos.”

## Recommendation 2

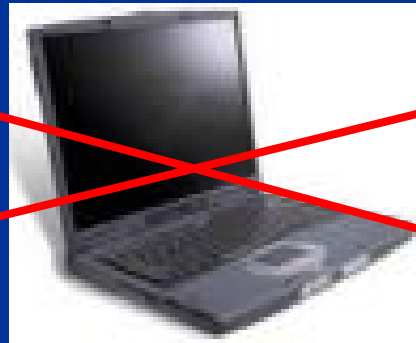
Do not delete, alter, or print photos at any time before duplication.

(Rotating photo in camera can be an alteration)

- So, the witness can testify:
  - “All the pictures I took, good and bad, are right here.”
  - “I did not delete or alter any photos.”

## Recommendation 3

Keep media away from devices that can alter it  
(until duplication is finished.)



## Recommendation 4

Immediately burn to quality CD-R / DVD-R directly from media using a write blocker.

- Putting on hard drive first creates alteration opportunities.
- Write blocker prevents alteration.
- Finalized CD-R / DVD-R can't be altered.





Card read with built in  
Write-Block



Card read with no  
Write-Block



## Recommendation 5

**Before reformatting media card,  
confirm burn.**

**(Visual plus CRC or hash)**

- Not recommended:
  - Encryption software.
  - Watermarking software.
- See SWGIT guidelines: [www.theiai.org](http://www.theiai.org)

## Recommendation 6

Make working copies *now* from either media card or the CD / DVD.

(Burn and confirm).

# Recommendation 7

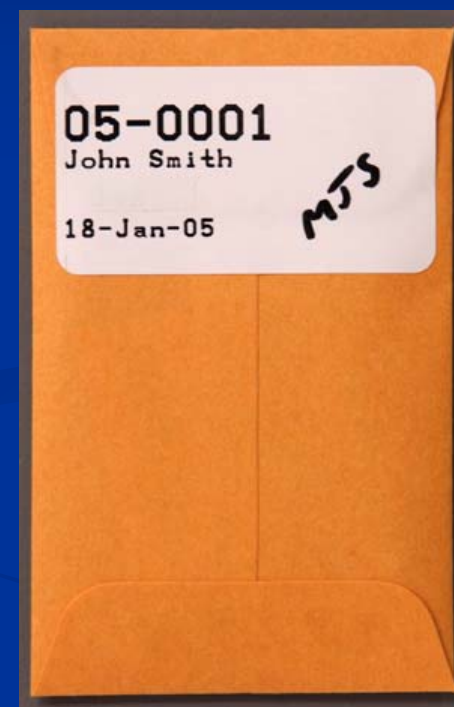
Label the CD / DVD and document what you did.

- Don't use ball point.
- Use "Sharpie" type of soft tip, permanent marker.
- Mark in spindle area.



# “Digital Evidence Custodians”

- Not all are computer literate.
- Designate “digital evidence custodian.” (DEC)
  - Bag and tag flash media for DEC.
  - DEC makes the CD / DVD.
  - Simple chain of custody.
- Not a full time job.



# Current Issues

- Are CDs and DVDs suitable for archiving?
  - Use secure, RAID servers instead?
- CDs and DVDs can be damaged.
- Why not an automated process?

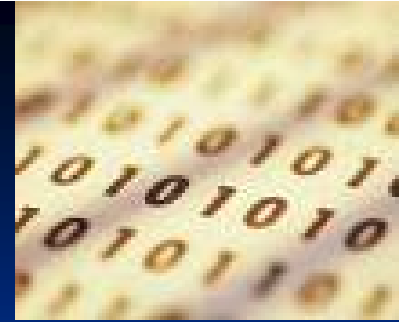


# Best Evidence Rule (FRE 1001)

---

- Bad name – it doesn't mean what it says.
  - *Original* recording / writing rule.
  - *Original* photo rule.
  - *Original* data rule.
- To prove the contents of a writing, recording, **photo** or data, we must have the “**original**.”
  - Some exceptions.

# What is an “original”



- Legal definition is not always the same as the technical.
- **Photo**: the negative or print there from.
- **Data**: “any printout or other output readable by sight shown to reflect the data accurately.”
- **Prints** are “originals.”
  - But think of data as the negative.
  - So, preserve the data (CD or DVD).

# Duplicate = Original

- Duplicate = original, unless:
  - Genuine question as to the original, or
  - “Unfair.”
- Properly made copies of data equivalent to an original.
  - That produced by mechanical or electronic re-recording, or by chemical reproduction, or other equivalent techniques which accurately reproduces the original.

# Alteration versus Enhancement

- Alteration: When the content of the photo is changed.
  - We don't alter.
- Enhancement:
  - No alteration.
  - What is in the image is made easier to see.
  - Still a “fair and accurate portrayal.”
  - Traditional versus non-traditional enhancements.

# Enhancements

- Image enhancement is any process **intended to improve the visual appearance of an image**. This includes processes that have a **direct counterpart in the conventional silver-based photographic** laboratory and those that can be accomplished only by using a computer.
- *SWGIT Guidelines, Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System.*

# “Traditional Enhancements”

**Traditional enhancement techniques** have direct counterparts in traditional darkrooms. They include:

- brightness and contrast adjustment,
- color balancing,
- cropping, and dodging and burning.

These traditional and acceptable forensic techniques are used to achieve an accurate recording of an event or object.

- *SWGIT Guidelines, Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System*

# Enhanced Images in Court

- Always have unenhanced image available.
  - Be prepared to replicate the enhancement process.
  - When possible, use software that records the enhancement process.
- 
- *United States v. Seifert*, 351 F. Supp. 2d 926, 927 (D. Minn. 2005), *aff'd* 445 F.3d 1043 (8th Cir. Minn. 2006) (*dicta*)

# Non-Traditional Enhancements (Experts only !!)

- Removing noise or clutter.
- Other filtering.
  - Sharpening, edge enhancement, etc.
- Certain color balancing.
- Need to be able to replicate the enhancement.
  - SWGIT (FBI Scientific Working Group on Imaging Technology.) [www.theiai.org](http://www.theiai.org)



# Admissibility of Digital Photographs in Criminal Trials



Keith Hodges, Senior Instructor, [Keith.Hodges@dhs.gov](mailto:Keith.Hodges@dhs.gov)

**Federal Law Enforcement Training Center**

**Glynco, GA**

Digital Photos - IACP 2008

