Handling Digital Photographs for Use in Criminal Trials
V2, March 2008

This is a DRAFT guide that may, once fully developed, be used by law enforcement to help ensure that digital photographs are admissible in court. This DRAFT has not been adopted or approved by any agency, department, or entity.

I solicit your comments, similar guides, forms and views so we can develop a workable guide for this needed process. keith.hodges@dhs.gov. (912) 554-5757. FAX: (912) 261-3635

The scope of this DRAFT is limited to still, digital photographs taken by first responder law enforcement and some crime scene personnel. It presumes that the digital camera uses media cards to store the images.

This guide does not address:

- Audio or video files.
- Evidence seized by law enforcement at a crime scene such as digital images – or other electronic data - in the defendant's possession.
- Images taken and worked on by laboratory personnel who, in that instance, should follow their lab procedures.

Digital photographs must be handled to anticipate their being challenged in court. Among those challenges is the assertion - often without any basis - that a photograph taken by the officer might have been altered either intentionally or accidentally. A gap in the number sequencing of photos might also prompt the defense to claim that the missing photo contained defense-favorable information.

The use of verification or encryption software, camera firmware, watermarking, and other methods were considered for inclusion, but were not included for a variety of reasons. Most law enforcement officers serve in small departments that may not be able to afford the software, equipment, or trained personnel. (This DRAFT was designed to combine simple procedures that anyone with rudimentary computer skills can execute.) In addition, water-marking, encryption, and other processes applied to a captured image is, technically, an alteration that most departments may not have the expertise to explain in court. Watermarking software could potentially obliterate an important part of the image.

This guide was developed through research by many and advice from those in the field. Many of the materials consulted along with this draft in several file formats, can be found at: http://www.khodges.com/digitalphoto/. Future drafts will also be posted there.

Keith Hodges, Senior Instructor, Legal Division, Federal Law Enforcement Training Center

Best Practices for Handling Digital Photographs Taken by Law Enforcement

This is a DRAFT guide and has not been fully peer-reviewed or approved by any government agency.

Please send comments or suggestions to Keith.Hodges@dhs.gov

Best Practices for Handling Digital Photographs Taken by Law Enforcement

Introduction

I. Purpose of this guide. Any evidence offered in court must have a foundation and be authenticated. The authenticity of the evidence is subject to challenge, and a common objection can be that the handling and the processing of the photos was such that they were altered – accidentally or intentionally – or that photos were deleted. Following the recommendations in this guide will assist in laying a foundation, showing a photograph's authenticity, and responding to objections by opposing counsel. Following this guide is not required to have photos admitted in court; that is a decision made by the trial judge. If this guide is not followed, a trial judge should still admit photos that meet foundational and authenticity requirements.

II. Who might use this guide. This guide was designed for first responders, accident scene investigators, photos taken during the execution of arrest or search warrants, and basic crime scene work. This guide is not recommended for:

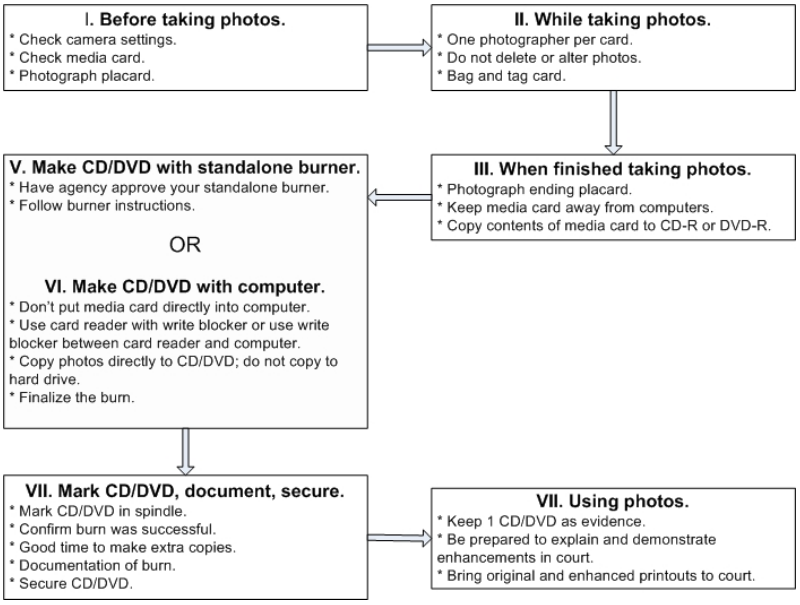
- Audio or video files because those issues can present technological issues beyond the scope of this DRAFT.
- Laboratory and crime scene personnel who have their own laboratory procedures to follow.
- Seizing electronic evidence (data, to include digital photos) that might be used in court. In such cases, law enforcement should follow guidelines developed by Seized Computer Evidence Recovery Specialists (SCERS), FBI standards (Scientific Working Group on Digital Evidence (SWGDE) and Computer Analysis Response Teams), and other federal and state entitles.

III. File formats and compression.

- Those who are familiar and know how to use proprietary RAW data files should capture digital images in that format.
- If RAW is not used, but enhancement or manipulation might be necessary, TIFF should be used to capture the images.
- JPEG can be used, and should be, if the person handling the images is not familiar with RAW and TIFF. Special caution is required when handling JPEG files because whenever the file is saved or "SavedAs," the file will be compressed unless special precautions are taken. Compression will degrade the quality of the JPEG file.

IV. Concept of these best practices.

- Camera settings are confirmed before shooting.
- No photos are deleted.
- No photos are altered.
- One photographer per media card.
- All the photos are moved directly from the media card to a CD-R or DVD-R.
- Document the process.



Suggested Best Practices

I. Before taking photos.

I-1. Check camera settings.

I-1-A: Confirm date stamp is correct.

I-1-B. Set date stamp so that it does NOT appear in the image and obliterate important information.

I-1-C. Turn red-eye reduction ON so that photos of people appear more normal.

I-1-D. Select file format (RAW, TIFF, or JPG). (See Part III of the introduction.)

I-1-E. Select size of the image the camera will generate. The larger the image selected, the more detail in the photo.

I-1-F. Check battery and if necessary, availability of spare batteries.

I-2. Check media card.

I-2-A. Use a blank or formatted media card whenever possible.

I-2-B. If images on the card cannot be safely deleted, photograph a placard as the first photo. (See I-3).

I-3. Photograph Placard.

I-3-A. Photograph a placard before taking the first photograph.

I-3-B. The placard can be a photo with handwritten information indicating the date and the case/case number, the scene being photographed or other information which identifies the nature of the photos being taken. (See Attachment 1.)

II- While taking photos.

II-1. Use only one photographer per media card to ensure no photos are deleted. If this is not possible, each photographer should use his/her own media card. If only one media card is available, photograph a placard when changing photographers.

II-2. Do not delete any photos taken no matter how bad the quality may be.

II-3. Do not alter any images by using camera features, rotating photos, or changing photo numbers, date, or the like.

II-4. If the contents of a media card will fit on a CD or DVD, photograph a placard after the last photograph. Bag and tag the card. Details of the tag need not be as detailed as crime scene evidence might be. (See Attachment 5.)

II-5. If the number of photos exceeds capacity of media card.

II-5-A. Photograph an end of session placard before the card becomes full. Do NOT delete existing photos just to make room for the placard.

II-5-B. Bag and tag the card.

II-5-C. Using the new blank media, photograph placard indicating “Card 2.”

II-5-D. If media card has a serial number, indicate that on the evidence tag.

III. When finished taking photos.

III-1. Photograph end of session placard.

III-2. Do not put the media card into any device that has the ability to delete or alter data.

III-3. Make a copy of all images on the media card onto a CD-R or DVD-R following the recommendations in section IV, and then either V or VI below.

IV. Prepare to make a copy of photos on the media card.

IV-1. This step, and steps V or VI, involve placing the contents of the media card(s) onto a CD-R or DVD-R.

IV-2. Use quality (sometimes called “evidence grade”) CDs or DVDs. Use Write Once, Read Many discs (-R). Do not use -RW (rewriteable) discs.

IV-3. Ensure ALL images on the media card are copied. If the media card capacity is larger than the CD/DVD capacity, you may have to use more than one disc. If so, mark the discs accordingly. (See VII.)

IV-4. Some media cards have tabs that can be set to prevent deletion of the card's contents (read only). If so, engage the tab to the "read only" position. (See Attachment 2.)

V. Copy photos to CD-R or DVD-R: *Option 1, Standalone burners*.

V-1. A standalone burner is one that is NOT connected to a computer. Standalone burners should be first vetted with your agency and ideally have only the ability to read from the media card, and not to write to it.

V-2. Use standalone burner to copy ALL the images to a CD-R or DVD-R.

V-3. Use instructions with the standalone burner to confirm a good burn.

V-4. If the standalone burner does not have a confirmation function, check the CD/DVD in a computer to see if the number of images is the same as the card and file sizes are consistent.

V-5. Go to VII.

VI. Copy photos to CD-R or DVD-R: *Option 2, Using a computer.*

VI-1. Do not put the media card directly into a computer. Put the media card into a separate media card reader.

VI-2. Unless the card reader has a write-block feature that prevents deleting or changing the media card's contents, do not connect the card reader directly a computer. Connect the card reader to a separate write blocker, and connect the write blocker to the computer. (See Attachment 3.)

VI-2-A. A write blocker is not necessary if caution is taken to ensure that none of the data on the media card is altered or deleted until the copying process is complete.

VI-3. Copy the contents of the media card directly to a CD-R or DVD-R. Do not copy the media card contents to the computer hard drive. (This would enable users to accidentally delete or alter files.)

VI-4. When making the CD or DVD, ensure you select the "finalize" option so data cannot be added or deleted.

VI-5. Go to VII.

VII. Mark CD/DVD, document the process, secure CD/DVD as evidence.

VII-1. Mark the CD/DVD with a soft tip, permanent marker. Mark in the spindle area. If that is not possible, mark along the outer edge. (See Attachment 4.) (It is best to mark before the below steps are taken to ensure the marking process did not damage the CD/DVD.)

VII-2: Confirm that the creation of the CD/DVD was done correctly by:

VII-2-A. Viewing the CD/DVD.

VII-2-B. Comparing the number and appearance of the images on the CD/DVD and the images on the media card.

VII-2-C. (Optional). Attempt to write or change/save a file to the CD/DVD you just created. If it is possible to write a file to the CD/DVD, the media was not finalized. Destroy the media just made and create another following the above procedures.

VII-3. This is a good time to make extra copies of the photographs. Properly made copies are legally "duplicates" and are the evidentiary equivalent to the first CD/DVD made.

VII-4. Document the process to make the CD/DVD, and place at least one CD/DVD into evidence. (See Attachment 5.)

VIII. Using the photographs.

VIII-1. Keep at least one of the CD/DVDs as evidence.

VIII-2. Make copies of the CD/DVD for those that need them.

VIII-3. If photographs are manipulated or enhanced, be prepared to replicate the steps taken. For the courtroom, be prepared with printouts of the original, un-enhanced photographs as well as the enhanced ones.

IX. Recycling the media card.

IX-1. Check with your prosecutors if they want the original media card preserved as evidence.

IX-2. Considerations.

IX-2-A. A properly made CD/DVD of the contents of the card is the evidentiary equivalent of the contents of the media card.

IX-2-B. Media cards are much more easily lost or damaged than a CD/DVD.

IX-2-C. Data on a media card is less stable than that on a CD/DVD and is subject to data corruption through heat, shock, magnetic, and other factors.

IX-2-D. Media cards are expensive.

"Digital Evidence Custodians"

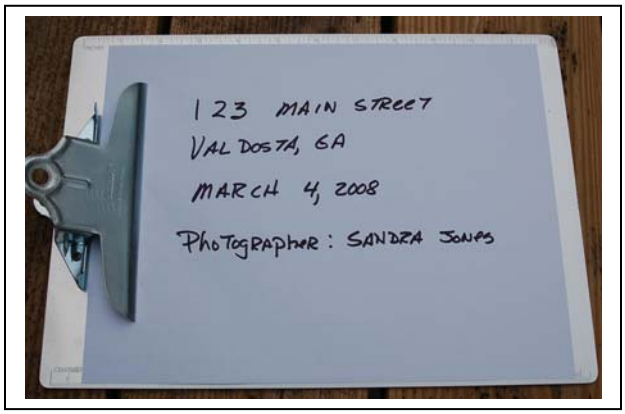
1. Some departments may wish for the officer who takes the digital photo to be the one to create the CD/DVD. In other departments, because of the level of computer skills of officers, the officer who takes the photos may turn over the camera or the media card to another for the making of the CD/DVD.

2. In those instances where a person other than the one who took the digital photos makes the CD/DVD, that person might be designated a "Digital Evidence Custodian." (The designee does not have to be the regular evidence custodian.) This Custodian would have the time and expertise to copy the digital photos from media card to the CD/DVD.

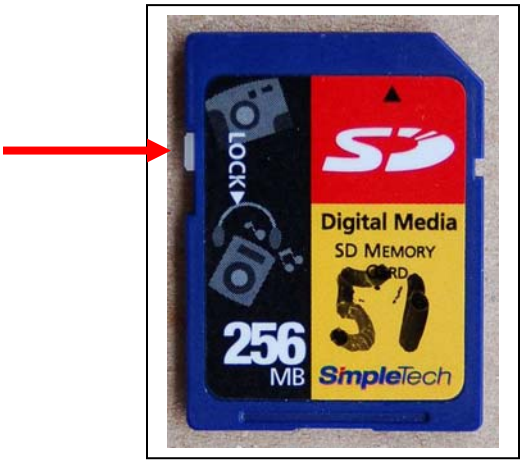
3. When using a Digital Evidence Custodian, that Custodian should document from whom, and when and where, the flash card was received. This step will help demonstrate in court that the digital photos were not altered.

Attachments

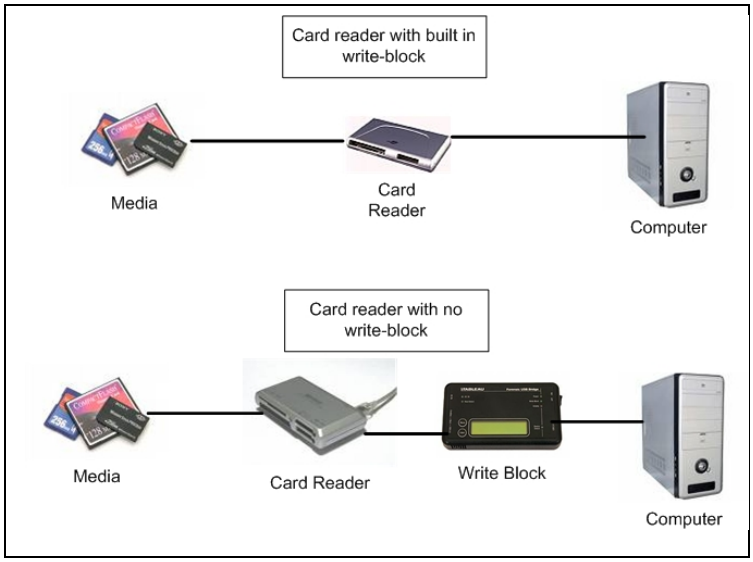
1: Sample placard.



2. SD type media card showing read-only (lock) tab.

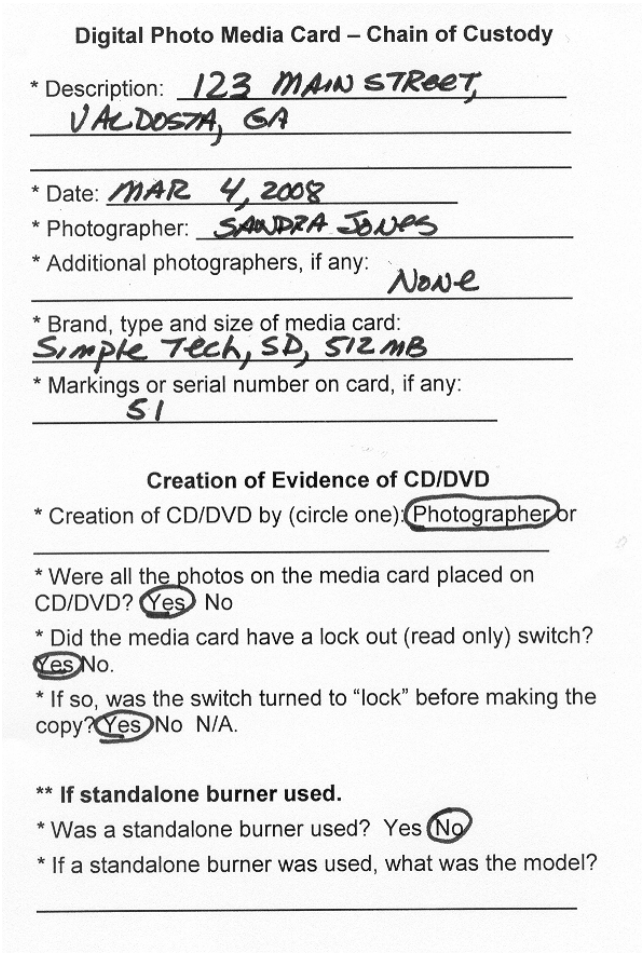


3. Cabling to make CD/DVD.



4. CD/DVD – Mark in Spindle.

5. Evidence tag and Chain of Custody.



Digital Photo Media Card – Chain of Custody

* Description: 123 MAIN STREET, VALDOSTA, GA
* Date: MAR 4, 2008
* Photographer: SANDRA JONES
* Additional photographers, if any: NONE
* Brand, type and size of media card: Simple Tech, SD, 512 MB
* Markings or serial number on card, if any: S1

Creation of Evidence of CD/DVD

* Creation of CD/DVD by (circle one): (Photographer) or

* Were all the photos on the media card placed on CD/DVD? (Yes) No
* Did the media card have a lock out (read only) switch? (Yes) No.
* If so, was the switch turned to "lock" before making the copy? (Yes) No N/A.

**** If standalone burner used.**

* Was a standalone burner used? Yes (No)
* If a standalone burner was used, what was the model?

** **Computer used to make CD/DVD.**

* Did the media card reader have a write blocker?

Yes (No)

* If the media card reader did not have a built in write blocker, was a write blocker used? (Yes) No N/A

Marking of CD/DVDs

The contents of the media card were copied to:

* 1 CDs marked CASE 623-08

* ~~0~~ DVDs marked _____

* If the CDs or DVDs had serial numbers, note them here:

NONE

Safekeeping of CD/DVD.

The CDs or DVDs as listed above were placed into evidence as follows:

Location: COUNTY EVID LOCKER

Marking: CASE 623-08, VOL.4