Scientific Working Group on Digital Evidence

SWGDE Best Practices for Maintaining the Integrity of Imagery

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous 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) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Best Practices for Maintaining the Integrity of Imagery

Table of Contents

1. Introduction

The integrity of digital imagery plays an important role in the process of forensic investigation. In the current legal system, there are standards and expectations for proving that digital imagery has been maintained in a forensically sound manner. In the absence of integrity, the evidence may be inadmissible or deemed unreliable. With the preservation of integrity, the evidence is shown as accurate and consistent without requiring testimony from all personnel who had custody of the imagery. Additionally, when the reexamination of imagery is required, integrity provides a method to ensure the original evidence is available and admissible.

2. Purpose

The purpose of this document is to provide personnel with guidance regarding maintaining and evaluating the integrity of imagery.

3. Scope

For the purposes of this document, the word "imagery" refers to an imitation or representation of a subject or object derived from digital images or video.

Integrity of digital imagery is best demonstrated through a combination of methods. This document will provide information on the issues that can affect integrity, specific methods for maintaining integrity, and methods for evaluating the integrity of digital imagery.

This document is not intended to be used as a step-by-step guide for conducting a proper forensic examination or reaching a conclusion. This document should not be construed as legal advice.

4. Definitions

Imagery Integrity – An assurance the imagery in question and/or work product is complete and unaltered, from the time of acquisition or generation through the life of the imagery.

Integrity Verification – The process of confirming that the imagery presented is complete and unaltered since the time of acquisition or generation.

Authentication – The process of substantiating the content of imagery is an accurate representation of what it purports to be, or the process of substantiating the origin of the imagery.

Provenance (Origin) – The time, place, and manner of image creation.

5. Limitations

This document is not intended to be a training manual or a standard operating procedure.

Personnel using this document should be sufficiently trained in the procedures discussed. For further information, refer to *SWGDE Training Guidelines for Image Analysis, Video Analysis and Photography*.

This document is not all-inclusive, and does not contain information related to specific products. This document should not be construed as legal advice. This document does not address archival policy or retention policy of evidence.

6. Issues Affecting Integrity

A number of factors may affect imagery integrity. Failure to address these issues adequately may result in the inadmissibility of the imagery or the inability to reexamine the evidence.

6.1 Compression for storage (save as, resave jpg, opened file)

While compression is useful for image storage, multiple aspects of imagery can be lost or altered when images are re-compressed. These aspects can include both the visual content and associated metadata. Images should be stored in an unaltered state, and any subsequent review or processing should be completed on a copy of the original evidence. In addition, any processed imagery should then be considered derivative evidence, and the integrity of this evidence should then be assured.

6.2 Loss/change of metadata

Metadata can be an important portion of imagery, particularly for integrity verification. Metadata can help establish the provenance of imagery; however, it may be edited, intentionally or unintentionally, or lost. This can impact the ability to establish the provenance of imagery after the fact.

6.3 Improper documentation at generation/acquisition

Whether evidence is created as a derivative or received for examination for the first time, integrity needs to start at the time of generation/acquisition. Additionally, the policies of the agency should be followed to ensure that the integrity of digital imagery is preserved, whether it is through a chain of custody, a hash value, a visual inspection, or some other means.

6.4 Legacy software/devices

When software and devices become outdated, they may have produced imagery in nonstandard formats or formats incompatible with updated software or equipment, preventing integrity verification. To address this issue, new software or equipment should be backwards compatible, or a plan should be in place to maintain usability of the evidence.

6.5 Proprietary nature of software

Programs that are for sale or license where a vendor controls the source code implementing storage of the imagery may not be independently verifiable. Likewise, vendors may not exist indefinitely. Therefore, using proprietary software to verify integrity is not recommended.

6.6 Data access

To aid in ensuring integrity, access to imagery should be limited to appropriate personnel. This mitigates tampering by personnel with an ulterior motive or negligent behavior.

7. Methods for Maintaining Integrity

There are several methods for maintaining the integrity of digital imagery. These methods include, but are not limited to, the following:

7.1 Written documentation

Standard operating procedure for documenting the steps taken to secure the evidence properly. This documentation should include a chain of custody.

7.2 Physical security/environment

Mechanical or Physical systems for preventing, unauthorized access to data or loss of data, e.g. secure access, personnel control, fire suppression systems, non-networked computer systems.

7.3 Redundant physical copies

Duplicates of files kept in an alternate location to prevent loss of files.

7.4 Logical security (WAN/LAN)

Operating system or software-based devices to prevent access to files (e.g., password protection, firewalls).

7.5 Third-party storage

This requires transferring files to third parties, which relinquishes control of the integrity process. Although third party storage may be appropriate under certain circumstances, there should be a viable method for documenting access to the files and demonstrating integrity that is independent of the vendor. Additionally, an appropriate contract that clarifies the vendor's obligations should be in place before any files are transferred.

7.6 Digital signatures

This process is used along with a hash process. The resulting hash is encrypted with a specific private key. File integrity can be verified using the hash value and the source of the signature is validated using the public key. The advantage of a digital signature is that the source of the digital file can be attributed to an individual.

7.7 Watermarking

This process modifies the content of the files and can persist as part of the file. This method can obscure the visual content and is therefore not recommended.

7.8 Encryption

The process encodes the content of the files to limit access, and does not demonstrate the files integrity. Encryption can be used in concert with other methods for integrity verification.

8. Methods for Evaluating Integrity

8.1 Hash verification

An established mathematical calculation that generates a numerical value based on input data. This numerical value is referred to as the hash or the hash value. Hashing computes a number using a complex formula and is very sensitive to changes in input values. Hashing should be performed prior to and subsequent to a copy function.

8.2 Visual verification

The process of confirming the accuracy of imagery through visual inspection. This involves viewing both the original imagery and the questioned imagery and verifying they contain identical visual information. Image processing tools (e.g. subtract function) may be useful in determining if regions of the imagery are altered.

8.3 Evaluation of factors listed in Section 7

These factors may or may not provide additional verification capabilities depending on integrity procedures implemented.

9. Workflow Examples

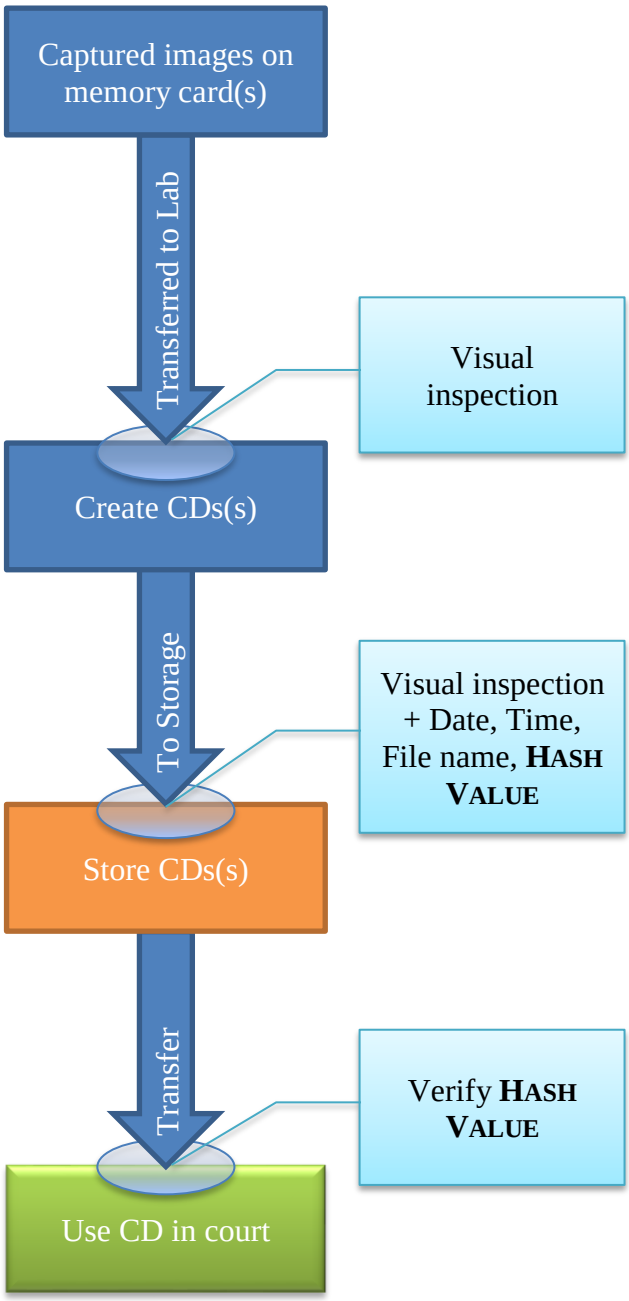
9.1 Example #1

A series of digital images are captured at a crime scene. The photographer transports the camera and memory card to a laboratory environment, where the memory card is removed and placed in a self-contained CD writer, which creates two read-only copies of the pictures on CDs. The CDs are labeled with the photographer's name, the date, the case number, and the signature of the photographer, and chain of custody documents are initiated. The files on the CDs are reviewed for completeness (i.e., all files have transferred), hash values generated, and the CDs are stored securely. The memory cards are wiped for reuse. In preparation for court, one CD is removed from storage. The photographer's signature on the CD is verified, and hash values for the files are calculated, compared to the values of the original files, and found to match. Prints are then prepared for court.

Flowchart from Example #1

NOTE:

It is important to document chain of custody throughout the lifecycle of the evidence. In this case, the chain of custody is initiated and maintained by the appropriate personnel.

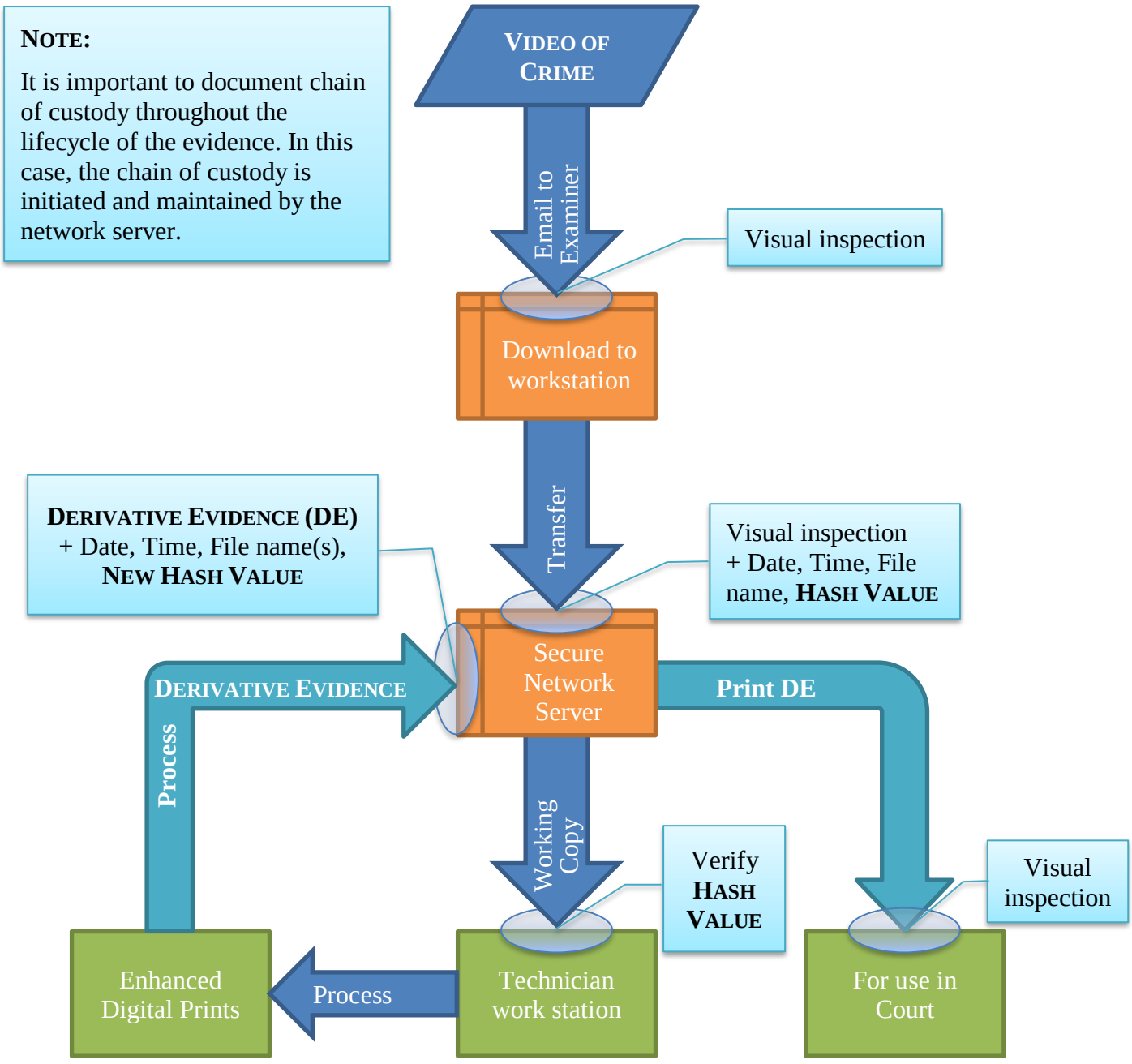


9.2 Example #2

A video is submitted to an agency via email. The sender includes a description of the video content, and the recipient reviews the video to determine that the video matches the included description. The recipient downloads the video file to a secure network server, and visually verifies that the content of the video on the email appears to match that of the downloaded video. The network server automatically logs the input video, including the date, time, file name, and a hash value for the file. The recipient inputs the associated case number, and digitally signs the server's log to indicate initial custody of the video.

An agency technician is tasked to create enhanced still images from the video. The technician signs into the network server, and downloads a working copy of the video, which is logged by the server. The technician calculates a hash value and compares it to the original to ensure the copy is the same as the original. The technician processes the working copy of the video, resulting in thirteen processed images. The processed images are uploaded to the folder for the associated case number on the secure server, with identifiers including the date, time, file name, and associated hash values. The technician digitally signs the server's log to indicate custody of the derivative evidence. The technician then prints copies of the digital stills for use in court, and visually verifies that the content of the prints matches that of the digital files.

Flowchart from Example #2



SWGDE Best Practices for Maintaining the Integrity of Imagery

History

Revision	Issue Date	Section	History
1.0 DRAFT	2017-01-12	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	2017-02-21	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2017-06-22	6.4	Clarified section in response to public comments. SWGDE voted to publish as an Approved document.
1.0	2017-07-18	--	Formatted and published as Approved version 1.0.