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 13

Best Practices for Maintaining the Integrity of Digital Images and Digital Video

Introduction

Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. Files which are copied from storage and processed result in new files. These files must also have their integrity maintained.

Integrity differs significantly from authentication. Authentication is the process of substantiating that the content is an accurate representation of what it purports to be. For example, authentication of a digital image of a gun on a table could be authenticated by a person at the scene stating the picture fairly and accurately represents the gun on the table. The integrity of the image can be established by methods covered in this document. For further information on image authentication, see SWGIT document *"Best Practices for Image Authentication"*.

This document is designed to cover the issues that can affect the integrity of digital media files. Extraction of digital media files from devices is not covered in this document.

Integrity of a digital image or video file is best demonstrated through a combination of methods. This document will discuss specific methods and provide examples of how those methods can be applied. Maintaining integrity requires both documentation and security of the files throughout the workflow. A standard operating procedure (SOP) should describe the workflow.

MAINTAINING AND DEMONSTRATING INTEGRITY

When working with digital image and video files, one needs to maintain integrity of the files and also demonstrate that the steps taken were effective. Maintaining integrity requires security of the files during transport and storage. Demonstrating integrity uses methods to show that the file has not changed.

When a digital image or video file is obtained, a reference is created for future demonstration of integrity. The reference can be accomplished in a variety of ways. The file is then transported to a storage device or location. When it is removed from storage for use, the integrity is demonstrated by the method used to create the reference.

Figure 1 shows a generic workflow of methods for maintaining, referencing and demonstrating integrity. The arrows and the boxes indicate where security measures need to be implemented to protect file integrity. The circles indicate methods used to demonstrate integrity has been maintained.

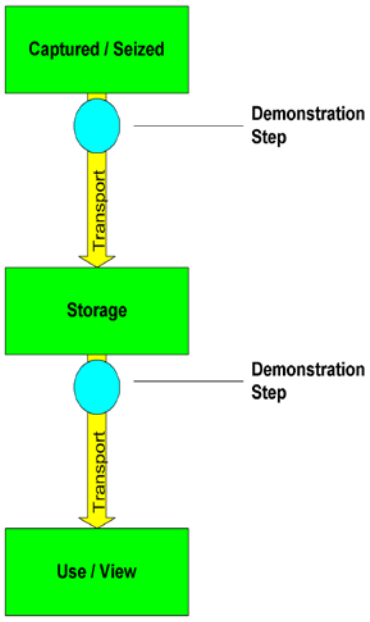


Figure 1 - Overall Maintainance with Demonstration Steps

METHODS FOR MAINTAINING INTEGRITY

The following is a list of some of the more common methods of maintaining integrity and is not exhaustive.

- Written Documentation: SOP documenting the steps required to properly maintain security. This documentation may include chain of custody, if required by agency policy.

- Physical Security / Environment: Mechanical or physical systems for preventing unauthorized access to data or loss of data, e.g. door locks, security guards, personal control, fire suppression systems, isolated computer systems.

- Redundant Physical Copies: Duplicates of files kept in an alternate location to prevent loss of files in the case of disaster.

- Logical Security (WAN / LAN): Operating system or software-based devices to prevent access to files, e.g. password protection, firewalls.

- Third-Party Escrowing: This requires transferring files to third parties, which relinquishes control. Although it may be appropriate under certain circumstances, the agency must have a viable method for demonstrating integrity that is independent of the vendor, and an appropriate contract that clarifies the vendor's obligations should be in place before any files are transferred.

METHODS FOR DEMONSTRATING INTEGRITY

The following is a list of some of the more common methods of demonstrating integrity and is not exhaustive.

- Hashing Function: An established mathematical calculation that generates a numerical value based on input data. This numerical value is referred to as the hash or hash value. Hashing computes a number using a complex formula and is very sensitive to changes in the input values.

- Visual Verification: The process of confirming the accuracy of an image through visual inspection.

- Digital Signature: 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 a digital file can be attributed to an individual.

- Written Documentation: Notes/narrative written by the operator at various steps to document the workflow.

- Checksums / Cyclical Redundancy Check (CRC): Checksums are often used in file transfer to verify that the data transfer was successful. Some checksums are as powerful as hashes. It is recommended that those checksums which are not, be used in concert with other methods (such as hashing or visual verification) to the degree possible.

- Encryption: This process modifies the content of the files and does not in and of itself demonstrate that the file has not been altered. Encryption can be used in concert with other methods.

- Watermarks: This process modifies the content of the files and can persist as a part of the file. This method is not recommended.

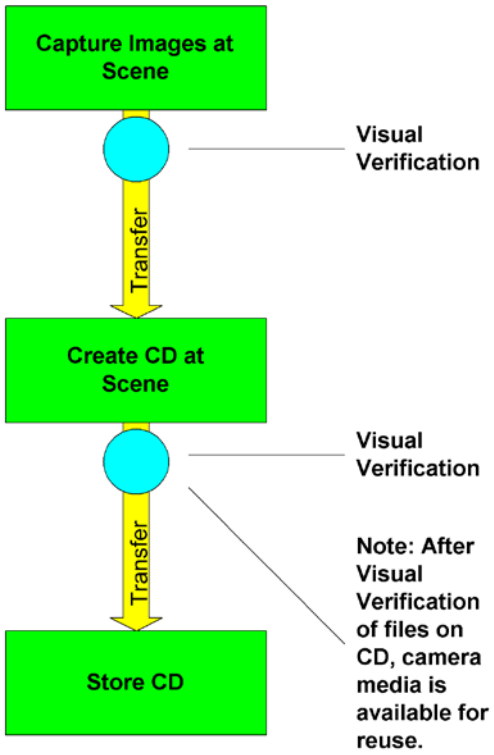
- Proprietary Methods: Methods offered for sale or license where a vendor controls the source code may not be independently verifiable. Likewise, it may not be possible to validate the methodology independently. Therefore, this method is not recommended.

EXAMPLE WORKFLOWS

The following is a list of specific workflow examples. The list is not exhaustive as each situation requires tailoring a specific process that should be outlined in an organization's SOPs.

Example #1

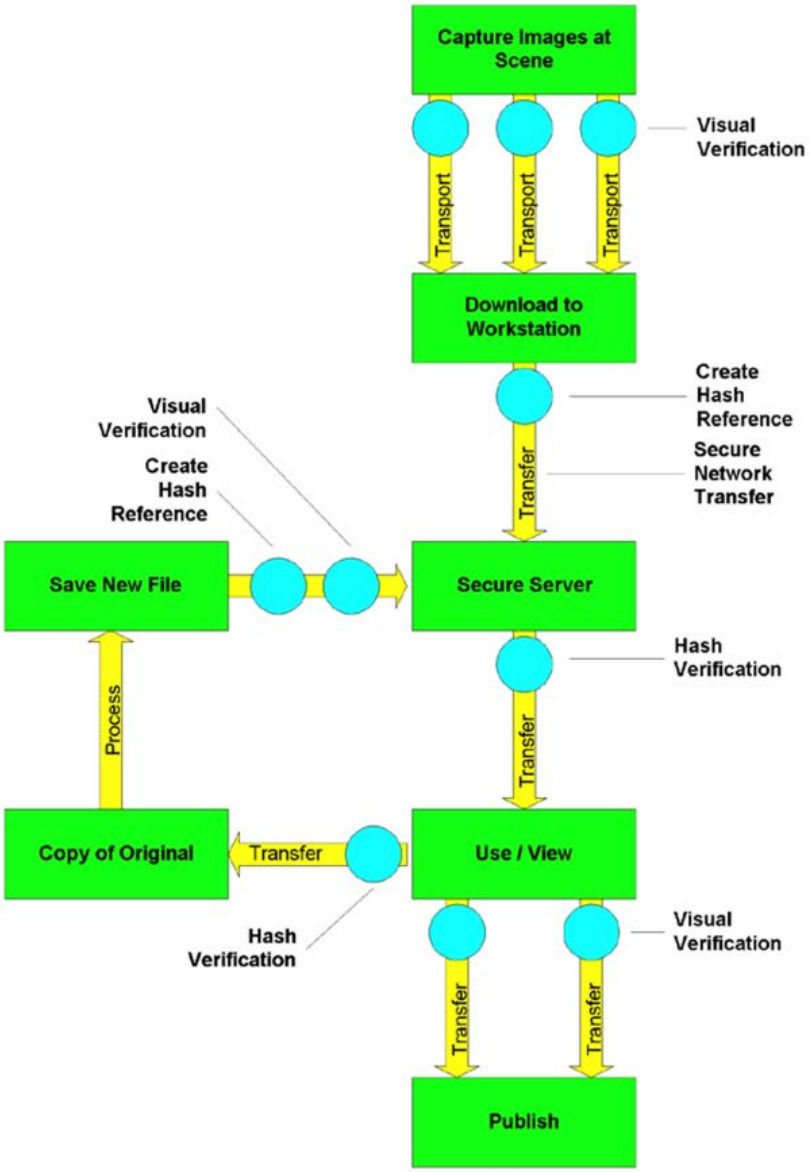
A series of digital still pictures are taken at a scene and are visually verified on the camera. The memory card is removed and placed in a self-contained CD writer, which creates two read-only copies of the pictures on CDs. The CDs are labeled with the photographer's name, the date, case number, and signature. Until the files are stored, they are in the hands of the photographer. The files on the CDs are visually verified, and then the CDs are stored in separate secure locations. At that point the memory cards are wiped and reused. In preparation for court, one CD is removed from storage; the signature on the CD is verified, and the files are visually verified. Then prints are prepared for court.



Example #2

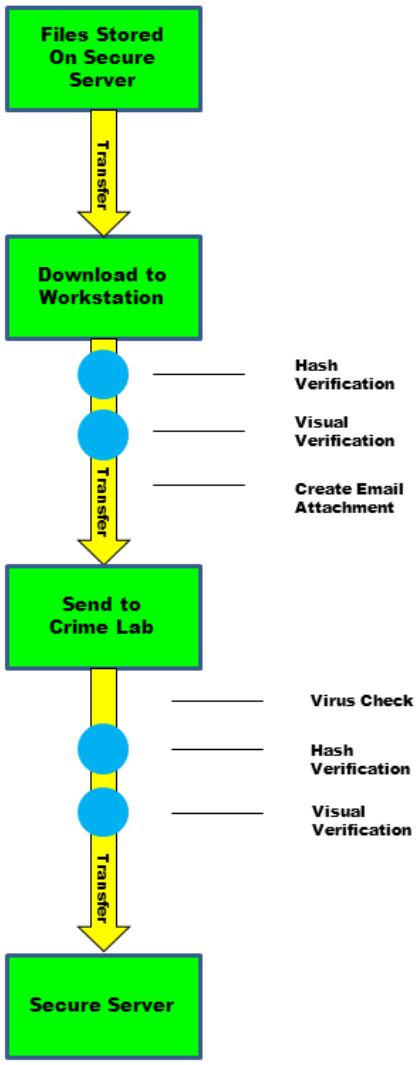
A series of digital still pictures are taken using multiple flash cards at a scene and are visually verified on the camera. Each flash card is sealed in an envelope with the name of the photographer, case number, case details, and the signature of the photographer. The flash cards are transported to another site and the person transporting them provides physical security. They are logged in at the other secure facility and placed in a locked box. Another worker removes the cards and signs the log. The files are downloaded from the memory cards to a workstation and a hash reference is created. The data is transferred to a secure network server. The hash numbers are then verified.

Later the photographer creates working copies of the files from the server, checks the hash references, and visually verifies them. The files are printed for court and some are used for further processing. The processing results in new files which are saved at the processing workstation. Visual and hash references are created. The processed files and hash references are then saved to the secure network server.



Example #3

A processed file is sent to the crime lab via electronic transfer (e.g. E-mail, FTP, etc.) for analysis. The submitting agency prepares an evidence submission form or equivalent with appropriate case information, hash value and analysis request. The sender verifies the hash reference and forwards the file to the forensic laboratory as an E-mail attachment. The forensic laboratory receives the E-mail, enters case information into the laboratory information management system, detaches the file, runs an anti-virus program, verifies the hash value and stores the file on a secure server pending analysis. The laboratory sends a response acknowledging receipt.



Example #4

In the course of an investigation, a digital video camera is seized. The Mini DV tape is removed and the write protection tab is engaged. The cassette is placed in an evidence envelope and sealed and then an entry on an inventory log is completed. The envelope is transported to and stored in a physically protected facility. When the material is removed for use or viewing, the write protect, signature, and inventory information is verified.