OSAC 2024-N-0011

Standard Guide for Forensic Digital Image Management

Video/Imaging Technology & Analysis Subcommittee
Digital/Multimedia Scientific Area Committee (SAC)
Organization of Scientific Area Committees (OSAC) for Forensic Science

OSAC Proposed Standard

OSAC 2024-N-0011

Standard Guide for Forensic Digital Image Management

Video/Imaging Technology & Analysis Subcommittee

Version: 1.0
April 2024

Disclaimer:

This OSAC Proposed Standard was written by the Video/Imaging Technology & Analysis Subcommittee of the Organization of Scientific Area Committees (OSAC) for Forensic Science following a process that includes an open comment period. This Proposed Standard will be submitted to a standard developing organization and is subject to change.

There may be references in an OSAC Proposed Standard to other publications under development by OSAC. The information in the Proposed Standard, and underlying concepts and methodologies, may be used by the forensic-science community before the completion of such companion publications.

Any identification of commercial equipment, instruments, or materials in the Proposed Standard is not a recommendation or endorsement by the U.S. Government and does not imply that the equipment, instruments, or materials are necessarily the best available for the purpose.

Standard Guide for Forensic Digital Image Management

1. Scope

1.1. This guide outlines best practices for the handling of digital images in a forensic environment to ensure transparency, and the security, integrity, and availability of said images.

1.2. This standard does not instruct on how to capture original images nor how to process images, rather addresses the storage and handling of original and processed images.

1.3. This standard addresses the difference between images captured by a forensic service provider and images obtained from external sources.

1.4. This standard cannot replace knowledge, skills, or abilities acquired through education, training, and experience, and is to be used in conjunction with professional judgment by individuals with such discipline-specific knowledge, skills, and abilities.

1.5. This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.

2. Referenced Documents

2.1. *ASTM Standards:*

ASTM E2916 *Terminology for Digital and Multimedia Evidence*

2.2. *SWGDE Documents:*

Best Practices for Archiving Digital and Multimedia Evidence

3. Terminology

3.1. Definitions

3.1.1. Primary Image — The first instance in which an image is recorded onto any media that is a separate, identifiable object. (ASTM E2916)

3.1.2. Original Image — An accurate and complete replica of the primary image, irrespective of media. (ASTM E2916)

3.1.3. Backup Image — A duplicate copy of any image, typically stored during the processing of the original image, to protect against accidental loss or corruption.

3.1.4. Working Image — a copy of a recording or data that can be used for subsequent processing or analysis or both. (ASTM E2916)

3.1.5. Fixity Checking — The act of verifying, generally through the use of checksum or hash function, that particular information has not changed. (SWGDE)

3.1.6. Image Processing — Any activity that transforms an original input image to an output image. (ASTM E2916)

3.1.7. Processed Image — In image and video analysis, any image that has undergone enhancement, restoration, or other operation. (ASTM E2916)

3.1.8. Integrity Verification — A process of confirming that the data presented is complete and unaltered since time of acquisition.

3.1.9. Archive Image — Any image placed on media that is suitable for long-term storage. (SWGDE)

4. Significance and Use

4.1. This document is intended to guide forensic practitioners in the storage and maintenance of digital images in a manner that ensures their preservation and protection for any potential end use, including admissibility in court.

4.2. This document provides guidelines to assist in the development of training programs and standard operating procedures pertaining to the handling of digital images.

4.3. This document is not intended to address all potential conditions, nor does it supersede requirements of accrediting or certifying bodies.

5. Image Handling, Backup, and Archival

5.1. It is the responsibility of the organization to maintain all images so they are available for all intended purposes.

5.1.1. The organization should be aware of and follow all local, state, and federal laws that regulate the manner, duration, and maintenance of image storage. The designation of images as evidence, records or documentation may impact the legal requirements.

5.1.2. Digital images shall be adequately maintained to prevent loss and degradation.

5.2. Access to images shall be secure and safeguarded with physical or logical barriers to ensure image integrity is maintained. Access to these digital images shall be consistent with organizational confidentiality regulations.

5.2.1. Release of images should be documented according to chain of custody policies.

5.2.2. Access to images should be tracked physically or electronically.

5.2.3. Policies and procedures should be in place to prevent unauthorized access and use of images.

5.3. All images should be retained as part of case documentation. A baseline for image integrity should be established through hashing, or some other form of fixity checking.

5.3.1. Images captured with the photographer's primary camera or any other camera, such as a back-up camera, cell phone camera, or point-and-shoot device, shall be treated as original images from the point of capture.

5.3.2. Images obtained from external sources shall be treated as original images from the point of receipt.

5.4. Original images should not be deleted. All images, including poor quality or unintended images, should remain as part of case documentation. In a controlled, laboratory environment, unintended or poor-quality photographs may be deleted if a proper policy or procedure is in place.

5.5. Original images, processed images, and applicable documentation should be stored in a manner that allows them to be easily retrieved and associated with their relevant case information.

5.6. All images should be archived in more than one physical location and on more than one storage device to ensure a single-system failure never results in the loss of images.

6. Image Processing

6.1. Original images are to be maintained in their native file format and protected at all times.

6.2. Working images should be created and designated as such before any processing steps are performed. Verify the working image is a true copy of the original through hashing, integrity verification, or some other form of fixity checking.

6.3. All steps taken to process working images shall be documented.

6.3.1. Image processing steps should be sufficiently documented to allow a comparably trained person to understand the steps taken, techniques used, and achieve comparable results.

6.3.2. Processing steps that are not included in the final image do not need to be documented.

6.3.3. Minimum requirements for documentation of advanced techniques include identifying the version of the software application, techniques, settings, and parameters used.

6.3.4. Automated processes, such as user-created macros, require thorough documentation of each step contained within. This can be described in an SOP and then only referred to by the process name thereafter.

6.3.5. Documentation can be recorded in a variety of ways including hand-written notes, electronic recording, image metadata, automated logging tools, or incorporated into the final report.

6.4. Processed images should be designated as such and preserved in the same manner as original images.

7. Keywords

7.1. Image Handling

7.2. Image Backup

7.3. Image Archiving

7.4. Image Storage

7.5. Fixity Checking

7.6. Deleted Image