Scientific Working Group on Digital Evidence

Guidelines for Forensic Image Analysis

16-I-002-2.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should 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; and 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 the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

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 this SWGDE cover page containing the Disclaimer Regarding Use.
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 creation date) of the document and also indicate 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 submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE 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 suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, 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.

Scientific Working Group on Digital Evidence

Guidelines for Forensic Image Analysis

Table of Contents

1. Objective

The purpose of this document is to offer the forensic examiner clear guidance on best practices for conducting a range of analytic tasks involving images.

2. SWGDE Position on Forensic Image Analysis

Forensic image analysis is a forensic science. It has been practiced since the early days of photography, dating at least to 1851 when Marcus A. Root conducted the first documented example of Forensic Image Authentication. Through microscopic examination, Root revealed that the color daguerreotype "process" promoted by Reverend Levi Hill was actually the product of hand coloring, not a breakthrough in photographic science [1]. In addition to being an accepted scientific practice in the forensic community, image analysis is also recognized in other disciplines including medicine, intelligence, geology, astronomy, agriculture, and others.

3. Introduction

Forensic Image Analysis involves the utilization of image science and specialized knowledge to evaluate the content of an image and/or the image itself in legal matters. Major sub-disciplines of Forensic Image Analysis with law enforcement applications include: Photogrammetry, Photographic Comparison, Content Analysis, and Image Authentication.

The process of Forensic Image Analysis can involve several different tasks, regardless of the type of image analysis performed. These tasks fall into three categories: Technical Preparation, Examination, and Evaluation. These tasks are described below. The general principles and procedures used in these tasks are the same regardless of the format or media in which the images are recorded. For the purposes of this document, the word "image" refers to an imitation or representation of a subject or object derived from photography or video.

4. Forensic Image Analysis – General Tasks

4.1 Technical Preparation

Technical preparation refers to the preliminary tasks, such as: calibration, function checking, creating working copies, or generating output. Note the type of tasks are dictated by the requirements set forth in the laboratory's operating procedures.

4.2 Examination

Examination refers to the skilled application of image science to the extraction of information from images, the characterization of image features, and the interpretation of image structure. Examples include, but are not limited to: compression effects, metadata collection, feature detection, extraction of Photo Response Non-Uniformity signature, image alteration evaluation, and the development of case-specific image exploration strategies. Additionally, activities such

as image enhancement, restoration, and other image processing techniques aimed at improving the visual appearance of image features are all part of the examination process.

4.3 Evaluation

Evaluation, as used here, is the application of specific subject matter expertise to draw opinions about subjects or objects depicted in images. Examples include, but are not limited to: patterned injury analysis, source determination, object classification, photogrammetry, and image authentication.

4.4 Reporting

Results of examinations, including opinions or the inability to form opinions, should be documented and reported. For further information, see SWGDE 18-Q-002-1.0 and SWGDE 10-Q-002-3.0.

5. Forensic Image Analysis – Specific Areas of Analysis

5.1 Photogrammetry

"Photogrammetry is the art, science, and technology of obtaining reliable information about physical objects and the environment through the processes of recording, measuring, and interpreting photographic images and patterns of electromagnetic radiant energy and other phenomena." [3] In forensic applications, photogrammetry (sometimes called "mensuration") is most commonly used to extract dimensional information from images, such as the height of subjects depicted in surveillance images and accident/crime scene reconstruction. Other forensic photogrammetric applications include speed determination and subject/camera perspective.

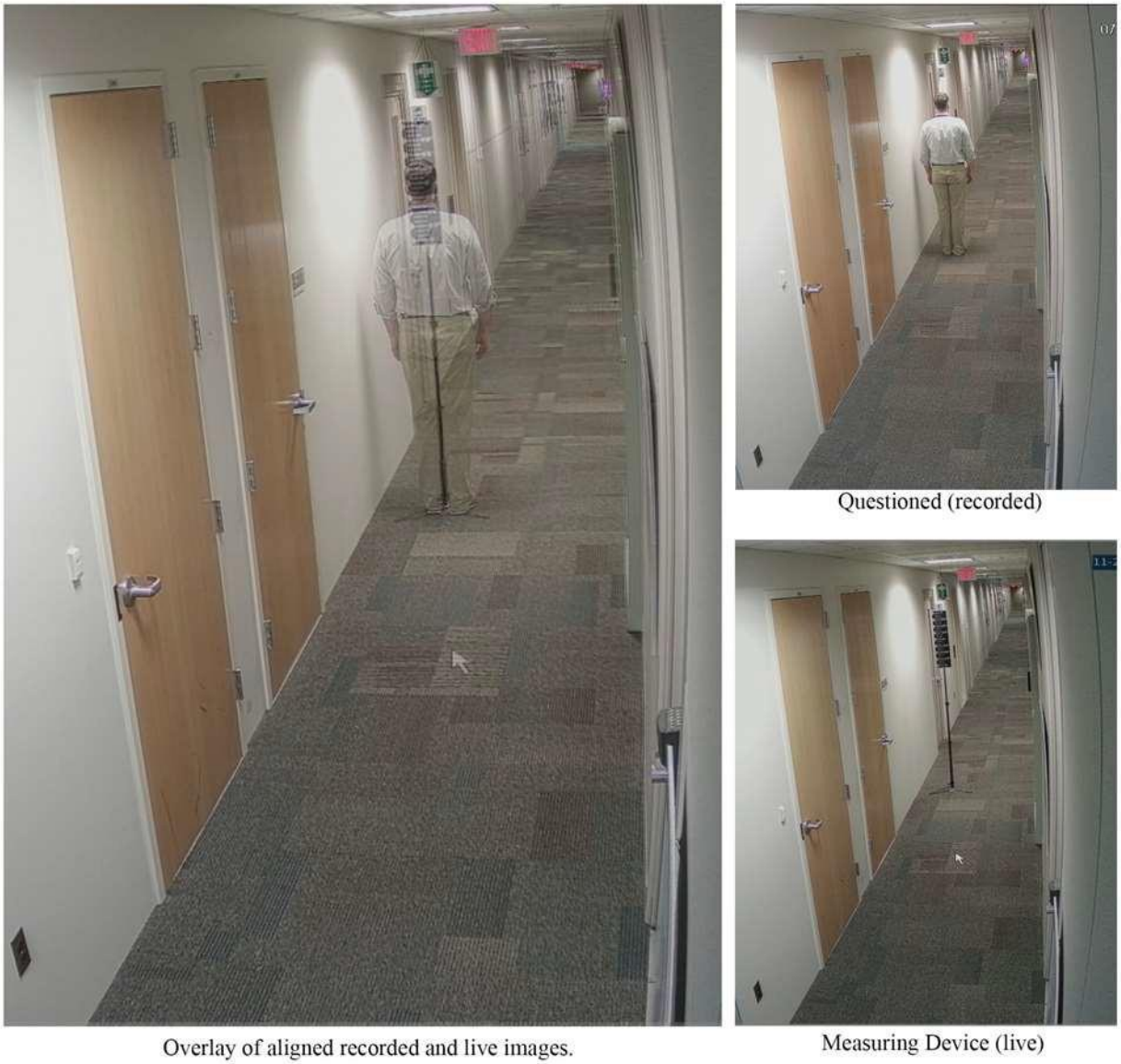

Figure 1. An example of a photogrammetric analysis (Reverse Projection) conducted to determine the height of a subject depicted in a surveillance photograph, Photo Credit: SWGDE, 2024.

5.2 Photographic Comparisons

Photographic comparison is the process of comparing object(s) or person(s) when at least one of the items in question is captured in imagery, and making an assessment of the correspondence between features of the captured imagery for rendering an opinion (as opposed to a demonstrative exhibit). Examples of photographic comparisons include, but are not limited to:

- A facial comparison between an unknown subject depicted in a surveillance image with a known subject; for further information, see ASTM E3149-18 as well as multiple guidelines offered by the Facial Identification Scientific Working Group (FISWG).
- The comparison of objects such as vehicles depicted in surveillance images with those recovered in an investigation; for further information, see SWGDE 18-I-003-1.0.

Photographic comparisons are frequently referred to as "side-by-side" comparisons since they usually involve a comparison of class and individualizing characteristics in imagery. Any methodology applied to photographic comparison should incorporate an analysis of the imagery, a comparison of individual features, an evaluation of the significance of the comparison, and a verification of the comparison. The repeatability of the procedure and documentation of the workflow is of paramount importance. For further information, see SWGDE 18-I-003-1.0 and SWGDE 15-I-002-1.1.

Figure 2. This figure is a simplified example of a demonstrative exhibit, commonly used for facial comparison. For further information, please see FISWG Facial Image Comparison Best Practices for Markups and Annotations. Photo Credit: SWGDE, 2024.

Figure 3. A demonstrative exhibit from a clothing comparison examination, with support for the proposition that the plaid shirt is not the same one in both images. The red arrows in the images indicate areas of inconsistency between the questioned and known shirts.

5.3 Content Analysis

Content analysis, within the field of forensic image analysis, involves drawing opinions and extracting meaningful information from an image. The targets of content analysis encompass a wide range of elements, including but are not limited to:

- understanding the circumstances or process involved in capturing or creating the image
- analyzing the physical aspects of the scene, including events or activities depicted classifying objects within an image
- determining the location or setting represented in the image

Examples of content analysis include but are not limited to:

- interpreting license plate information from an image

- determining the image orientation (e.g., upright or rotated)
- assessing the presence or absence of specific objects within the image
- analyzing and identifying logos or trademarks present in an image

Through content analysis, examiners can extract valuable information from images to aid in investigations and provide critical evidence.

5.4 Image Authentication

Image Authentication is the process of verifying the content and accuracy of data, ensuring that it truly represents what it purports to be. With the rise of deepfakes, it is essential to be aware of the potential for manipulated content. Authentication can be performed either by the data collector, relying on first-hand knowledge, or by an examiner in the lab.

The criteria for image authentication typically involve assessing the interpretability of the data, focusing on changes that genuinely impact the meaning or content.

Examples include:

- assessing the degradation of a transmitted image to identify any tampering
- differentiating between an original recording and an edited version in videos
- evaluating the degree of information loss in an image saved using lossy compression
- identifying feature-based modifications in images, such as the addition or removal of elements (e.g., adding bruises to a face), which may indicate manipulation

It is important to note that image authentication differs from integrity verification, which confirms the completeness and unaltered state of data since the time of acquisition. Ensuring data integrity can involve measures such as maintaining a chain of custody, utilizing evidence preservation techniques, and/or generating hash values to establish that the data has remained unchanged.

Video is composed of still images. As a result, image authentication is applicable to video, however, to better understand the methodology for the authentication of digital video, reference SWGDE 23-V-001-1.0.

6. Best Practices

The following guidelines outline the SWGDE recommended best practices for conducting forensic image analysis.

6.1 Evidence Management

Agencies should have documented procedures for the handling, transportation, storage, and documentation of evidence (chain of custody/hashing) to ensure the integrity of the data.

6.2 Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and administrative reviews are integral components of quality control.

6.3 Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis-related materials. For example, archived case-related materials should be stored in a manner that limits access. The degree of access will be agency-specific.

6.4 Documentation

The application of analytic techniques in a given case should be recorded to the degree that a similarly trained professional could repeat the steps taken. Agencies should establish standards for information included in, and the format for, reporting results.

The examiner should also have available documentation that describes and justifies the use of any method involved in the analysis. Such documentation can include peer-reviewed journal articles, scientific conference proceedings, reference books, internal white papers, training documents, or the results of empirical studies.

6.5 Training to Competency and Demonstrating Proficiency

Agencies employing forensic image examiners should follow SWGDE 15-M-001-1.2 and SWGDE 15-Q-001-1.0.

Certification is one method to evaluate personnel. Certifications can be comprehensive, tool based, or topic specific, and can be an additional tool in verifying technical skills and abilities. Comprehensive certifications generally require training to be completed, as well as a specified amount of experience in the discipline, and the successful completion of an examination. Certifications can be beneficial and should be considered when appropriate and available.

Examiners should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. In addition, analysts should demonstrate proficiency and maintain continuing education activities. Agencies should document the competency, proficiency, and continuing education of each examiner.

The examiner should demonstrate:

- understanding of the scope of work and how it will be applied in the forensic environment

- subject matter knowledge and competence
- working knowledge of the potential image processing and evaluation techniques
- working knowledge of applications and tools utilized in the specific agency
- working knowledge of SWGDE guidelines for capturing, storing, and processing of imagery, including issues relating to topics such as data integrity and compression artifacts
- understanding of legal precedent for the use of specific image processing techniques
- knowledge of the techniques necessary to document the opinions

6.6 Standard Operating Procedures (SOPs)

There should be Standard Operating Procedures (SOPs) for the tasks being performed. These SOPs should reflect the work flow and be general enough to permit flexibility for the required tasks. SOPs should also address workload limitations, so as to avoid cognitive fatigue and errors stemming from employee overload. SOPs should also recognize the effect examinations may have on employee well-being, and attempt to include ways to mitigate effects and steps to take when employee well-being suffers.

6.7 Workflow

The following describes a generalized sequence of actions involved in the analysis of an image and recommendations for their performance. The exact sequence will be agency specific.

1. Review of request for analysis.
    a. The agency must confirm that it performs the requested analysis.
    b. The agency must ensure the requestor has submitted all items needed to support the requested analysis or examination. In some cases, it may be necessary for the agency to obtain additional items before the analysis can be completed.
    c. The agency must confirm that it has the necessary equipment, materials, and resources needed to conduct the requested analysis.
    d. The agency must assign the analysis request to the appropriate personnel.
2. Acquisition of imagery. The image acquisition step is where the integrity of the primary or original data is initially established. Most often, subsequent steps are performed utilizing working copies, but in all cases, the integrity of the primary or original image(s) must be maintained.
    a. If possible, the original or primary image, or a bit-for-bit duplicate, should be available for analysis.
    b. Triage imagery
        i. The examiner must determine if the submitted material is suitable for analysis.

ii. The examiner must determine if all of the submitted material, or only a subset of the material, is to be subjected to analysis.

3. Production of working copies. Produce working copies of images to be subjected to analysis. This may require conversion from other media.
4. Processing of images to be analyzed, which may include enhancement for better visualization of details in the imagery. (For further information, refer to SWGDE 15-M-002-1.0.)
    a. Design an image processing strategy. This is the application of domain knowledge to choose which processes to apply to the image to extract the information necessary for drawing an opinion. The strategy should be justifiable. No single processing strategy is appropriate for all cases. This should be reflected in the organizational SOPs.
    b. Identify the appropriate tools to implement the strategy. There should be some references/documentation that the selected tools are capable of implementing the strategy.
    c. Implement the designed image processing strategy.
    d. Assess results. Determine that the image processing strategy yielded results suitable for analysis.
        i. If the results are suitable for analysis, then proceed to the analysis (5). Otherwise, repeat the process of designing an image processing strategy until suitable results are achieved (4a). Exploratory strategies that are not incorporated into the final work flow pathway need not be documented in case notes. Agencies may wish to document this fact in their SOPs.
5. Analyze processed data.
    a. Determine if criteria necessary for reaching an opinion are present in the processed image.
        i. Specific criteria for reaching an opinion should be identified, and
        ii. In some cases, the criteria will reflect the subjective experience of the examiner.
    b. Reach an opinion.
6. Report the opinion.
    a. The basis for, and uncertainty of, any opinion should be reflected in the reporting.
    b. When a statistical basis for an opinion can be made based on validated probability models, the opinion should be quantitatively reported.
    c. When statistical criteria do not exist, the opinion should be reported in terms of the kind of features discerned. If no appropriate statistical model is available, a

clear indication of the strength of an opinion should be reported. This will necessarily be a descriptive statement and not a numerical probability, as probability should not be implied where none exists. When facing statistical limitations in image examinations or lacking a suitable model, these constraints should be acknowledged. For further information on describing the relative level of support provided by the data, see OSAC 2022-S-0001. For additional information on statistical models in forensics, consult the American Statistical Association's (ASA) "Position on Statistical Statements for Forensic Evidence."

d. When opinions are a mix of both quantitative and qualitative results, reports must reflect the findings clearly and indicate the basis for each finding.
e. The report format and contents should follow agency standards.

7. Independent verification of opinions should be obtained. To avoid confirmation bias, verifiers should not know the results obtained by the original practitioner.
8. Ensure accurate archival of all imagery used for analysis. This may include original imagery, working copies, and processed imagery, as required by agency SOPs.

7. Conclusion

In summary, this document serves as a resource for forensic examiners seeking guidance in the field of forensic image analysis. It offers an overview of key tasks and specific domains within forensic image analysis, emphasizing best practices and presenting a structured workflow.

8. References

[1] Davis, Phil. *Photography*. Madison: Brown & Benchmark, 1995.

9. Additional Resources

American Statistical Association. "Position on Statistical Statements for Forensic Evidence." *American Statistical Association*, 2 Jan. 2019, www.amstat.org/asa/files/pdfs/POLForensicScience.pdf.

American Society for Testing and Materials. *Standard Guide for Facial Image Comparison Feature List for Morphological Analysis.* ASTM E3149-18, *ASTM*, 2018.

Organization of Scientific Area Committees for Forensic Science. Standard Guide for Image Comparison Opinions OSAC 2022-S-0001, *OSAC*, 2022. https://www.nist.gov/system/files/documents/2023/07/27/OSAC%202022-S-0001%20Standard%20Guide%20for%20Image%20Comparison%20Opinions_REGISTRY%20VERSION.pdf

Scientific Working Group on Digital Evidence. *Training Guidelines for Video Analysis, Image Analysis, and Photography.* SWGDE 15-M-001-1.2. *SWGDE*, 31 Mar. 2023, https://www.swgde.org/15-m-001/

Scientific Working Group on Digital Evidence. *Proficiency Test Guidelines*. SWGDE 15-Q-001-1.0. *SWGDE*, 29 Sept. 2015, https://www.swgde.org/proficiency-testing-guidelines/

Scientific Working Group on Digital Evidence. *Image Processing Guidelines.* SWGDE 15-M-002-1.0. *SWGDE*, 8 Feb. 2016, https://www.swgde.org/15-m-002/

Scientific Working Group on Digital Evidence. *Technical Overview for Forensic Image Comparison*. SWGDE 18-I-003-1.0. *SWGDE*,16 July 2019, https://www.swgde.org/18-i-003/

Scientific Working Group on Digital Evidence. *Best Practices for Photographic Comparison for All Disciplines. SWGDE* 15-I-002-1.1. *SWGDE*, 17 July 2017, https://www.swgde.org/15-i-002/

Scientific Working Group on Digital Evidence. *Requirements for Report Writing in Digital and Multimedia Forensics.* SWGDE 18-Q-002-1.0. *SWGDE*, 20 Nov. 2018, https://www.swgde.org/18-q-002/

Scientific Working Group on Digital Evidence. *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. SWGDE 10- Q-002-3.0. *SWGDE*, 15 May 2010, https://www.swgde.org/10-q-001/

10. History

Revision	Issue Date	History
1.0 DRAFT	9/15/2016	Initial draft created by updating SWGIT Section 12 – Best Practices for Forensic Image Analysis. SWGDE voted to release it as a Draft for Public Comment.
1.0 DRAFT	11/7/2016	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	1/12/2017	Following the period of Public Comment, no feedback was received and no edits were made. SWGDE voted to publish it as an Approved document (Version 1.0).
1.0	2/21/2017	Formatted and published as Approved Version 1.0.
1.1	6/14/2023	Began reviewing this document to update content.
1.1	5/14/2024	Review completed. Publish as draft for public comment.
2.0	9/16/2024	Updated Figures 1-3. Addressed public comments received by updating wording throughout. Re-publish as draft for public comment.
2.0	11/20/2024	SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.