Scientific Working Group on Digital Evidence

Best Practices for Image Authentication

18-I-001-2.0

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

Best Practices for Image Authentication

Table of Contents

1. Purpose

The purpose of this document is to provide best practices for forensic practitioners when examining images for authentication. For the purposes of this document, "imagery" can refer to a series of images depicting the same subject or a video.

2. Scope

This document provides basic information and best practices on the evidentiary value, methodology, range of results, and limitations when conducting image authentication as a part of forensic image analysis. The intended audience is examiners in a lab setting.

Image authentication is used to determine whether the imagery is a true and accurate representation of subjects and events. Authentication of image or video is typically aimed at examinations where there are questions on the content of the scene contained in the media. One of the questions this exam seeks to answer is to determine if the scene content is "true" or virtual or altered in a visually consistent manner. Conversely, image authentication does not answer specific questions about the subject(s), object(s), or event(s) within an image, such as "Is a specific object present?" "What happened?" or "Where is the scene depicted?" These are all examples of questions answered through image content analysis.

Image authentication must not be confused with the requirement to demonstrate the integrity of the evidence as a precondition to admissibility in court. Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. For example, the use of a hash function can verify that a copy of a digital image file is identical to the file from which it was copied, but it cannot demonstrate the veracity of the scene depicted in the image.

Image authentication and image content analysis may be performed in conjunction, depending on the use of the imagery.

3. Definitions

- **Alteration**: The changing of image features through artistic means.
- **Compositing**: The duplication and combination of elements from one or more images, including, but not limited to, techniques of cloning and cut-and-paste.
- **Computer Generated Imagery (CGI)**: The creation of still or animated content with imaging software or Artificial Intelligence (AI) based generators.
- **Image Authentication**: The application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria, and/or the determination of the original source of the image.
- **Image Content**: Visual information within an image, such as subjects/objects, artifacts (due to compression and/or capture), and physical aspects of the scene.

- **Image Generation**: The creation of image content through any number of means. One example is the creation of virtual humans using 3-D modeling software (e.g., computer-generated).
- **Image Structure**: Non-visual information about the image itself, such as file type, file compression, metadata, or the origin of the image.
- **Manipulation**: The process of altering the visual appearance of an image or specific features within an image resulting in misrepresentation or erroneous interpretation.
- **Morphing**: The automated transformation of components of one image onto those of another, involving a sequence of intermediate images demonstrating incremental change. Morphing is a combination of alteration and compositing.
- **Staging**: The physical alteration of a scene prior to image acquisition.

4. Limitations

This document will not describe discipline-specific analytical techniques outside of image analysis or the limitations associated with them, only the process for performing image authentication and the general manner used to formulate an opinion.

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, please refer to *SWGDE 23-V-001-1.2 Best Practices for Video Authentication*.

This document is not intended to be a training manual or a specific operating procedure. Practitioners performing image authentication should have sufficient training and experience in image science to allow the formation of an opinion. For further information, refer to *SWGDE 15-M-001-1.1 Training Guidelines for Image Analysis, Video Analysis, and Photography*.

The state of the art in digital imagery is such that in a single image, manipulations can be performed which a trained forensic practitioner may not adequately detect. Therefore, image authentication should be performed on a series of images depicting the same or similar subjects, or on video.

The detection of staging, the physical alteration of the scene prior to acquisition, may require coordination with scene investigators, correlation of image features with the real features at the scene, or comparison with other images of the scene or subject.

This document is not all-inclusive and does not contain information related to specific products. This document should not be construed as legal advice.

5. Background Information on Digital Manipulations

As noted above, it is technically feasible to manipulate an image, particularly a single still image, in a manner that may not be detectable by subsequent analysis using currently available tools and techniques. This process is becoming easier, as software applications are introduced specifically

for this purpose. However, multiple issues are presented and should be considered as a part of any examination of imagery for the purposes of authentication. Task-relevant issues include:

- Does another party have access to the imagery?
- Does another party have the skill level necessary to perform the manipulations?
- Does another party have the time necessary to perform the suspected manipulations?
- Does another party have the hardware and software necessary to perform the suspected manipulations?
- Does the imagery have fine detail, which ultimately requires a higher level of skill to manipulate undetectably?
- Is the image content complex, including physical interactions of people with one another, as well as the environment?

All these questions as well as others relevant to the analysis may be taken into consideration when practitioners examine evidence for the purposes of authentication. For instance, changing the color of a simple object in an image may be easy to achieve, but it would present a greater artistic and technical challenge to alter an image of an adult to appear to be a young child through traditional image alteration techniques. Complex manipulations of this nature would be more likely to leave features indicating the imagery has been manipulated.

In addition, practitioners of authentication techniques must be knowledgeable not only in photographic and analytical techniques but should be equally knowledgeable about techniques used to manipulate or create imagery. Some common manipulation techniques include alteration, compositing, morphing, and image generation.

The detection of computer-generated imagery is established through an examination of the characteristics of humans depicted. Human characteristics can be challenging to reproduce via computer generation or other artistic means, including, but not limited to, skin-to-skin contact (including at the knee and arm joints), skin-to-object contact, fine detail (such as hair and skin creases), translucent qualities in the skin, skin textures (such as pores and blemishes), and the quantity or quality of anatomical features (such as fingers and ears). The forensic practitioner should also be aware of the potential for computer generation to be masked through changes in luminance (e.g., artificially lowering light levels in a scene).

6. Evidence Preparation

General guidelines concerning the preparation of evidence for image authentication are provided as follows:

1. Review the request for examination to determine the subject matter of the image authentication. Information regarding the suspected tampering may be considered, however, task-irrelevant information should be limited (see section 9). To that end, case managers may utilize a worksheet or re-frame the written request to mitigate the effects of task-irrelevant information based on agency policy, prior to assigning an examiner.

2. Based on the request, propositions should be formulated. In the case of image authentication, an example of propositions are:
    a. Proposition 1: The image is authentic.
    b. Proposition 2: The image is not authentic.
3. Based on the request, determine if the image quantity and/or quality will have an effect on the degree to which an examination can be completed.
    a. If the specified quantity and/or quality criteria are not met, determine if it is possible to obtain additional images. If additional images cannot be obtained, this may preclude the practitioner from conducting an examination, or the results of the examination may be limited.
4. Identify the submitted imagery relevant to the analysis.

7. Method

There is no one specific methodology for image authentication, as the methods used will depend on the requested examination. However, any methodology applied to image authentication should incorporate both image content and image structure.

The repeatability of the procedure and documentation of the workflow is of paramount importance. Documentation should be performed contemporaneously.

Image authentication examinations should include the examination of both image (scene) content and image structure (non-scene content) as indicated by the following flowchart:

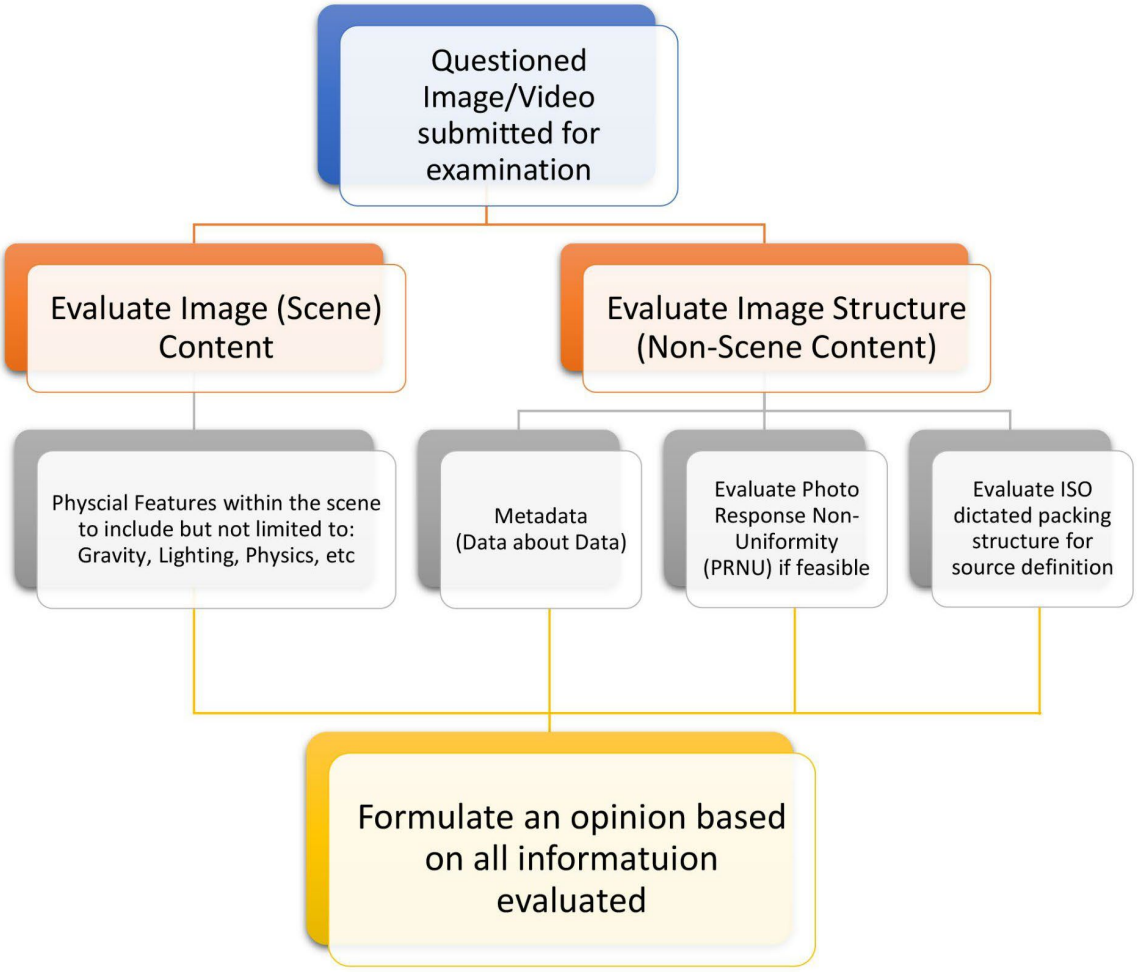

Figure 11. Flowchart on image authentication examinations (Chart Credit: SWGDE, 2018).

- The original imagery shall be preserved. Any processing should be applied only to a working copy of the imagery.
- Assess the image structure to determine whether factors are present that can answer the examination request. Image structure examinations may include, but are not limited to:
    - An examination of the file format of the imagery.
    - An examination of the metadata of the imagery. Metadata may be useful in identifying the source and processing history of the file, but can be limited, absent, or altered. Metadata may include:

        - Camera make/model/serial number
        - Date/time of creation or alteration
        - Camera settings
        - Resolution and image size
        - Global Positioning System (GPS) coordinates/elevation
        - Processing/image history
        - Original file name
        - Lens or flash information
        - Frame rate
        - Thumbnail information
    - An examination of the imagery file packaging (container analysis). This analysis may include but is not limited to:
        - Hex level header, footer, or other information about the file
        - Exchangeable image file format (EXIF) information
        - Bit level analysis of the file structure
    - An examination of noise within the image. This analysis may include but is not limited to:
        - Photo-Response Non-Uniformity (PRNU), this noise signature can be used to correlate images from the same source.
        - Stochastic noise evaluation can be used to show consistency between images from the same sensor manufacturer.
- Assess the image content to determine whether factors are present that can answer the examination request. Image content examinations may include, but are not limited to a review of the following:
    - Artifact features
        - Chromatic aberrations
        - Breaks in compression blocking or patterns
        - Mapping of motion vectors
    - Physical aspects of the scene
        - Lighting, contrast
        - Scale
        - Composition
        - Physics
        - Temporal or geographic inconsistencies
    - Human characteristics
        - Hair detail
        - Scars, bruises, or blemishes
        - Creases

        - Vein patterns
        - Skin contact
        - Movement
    - Evidence of staging
    - Photographic conditions
        - Focus
        - Depth of field
        - Sharpness/blur
        - Perspective
        - Grain structure
        - Noise
        - Lens distortion
- All observations in regard to image structure and image content should be documented. The use of a form (see Appendix C) is recommended to aid in consistency.

8. Results

While, by definition, it is impossible to prove a negative result, it is possible, through a thorough examination, to determine that it is unlikely the imagery has been manipulated or digitally created. Conversely, if alterations are detected, the forensic practitioner may reach the conclusion that the imagery is not authentic.

The provenance or source of an image may be determined as a result of the examination as detailed above. However, the lack of information in support of camera source identification does not preclude the possibility the imagery was captured by the camera in question.

While this examination is subjective, specifically the scene content portion, image authentication is a rigorous process. This process dictates that there is a standardized method of examining the material. The use of forms (see Appendix C for a sample form), in conjunction with standard operating procedures and guidelines, adds structure and consistency to the examination process. The goal of examining the scene content is to understand if software may have been used to create content or to alter the content, or a portion of the content, in the image or video. It should be noted that at this time it is theoretically possible to generate a single frame of a person that is not detectable as virtual by a human.

8.1 Evaluate Observed Characteristics

Evaluate the importance of each observed characteristic. In the context of image authentication examinations, it is crucial to formulate an opinion based on the results of the analysis of both the observation of image (scene) content and the information derived from the image structure (non-scene content). The formation of an opinion should include the following steps, as shown by the flowchart below:

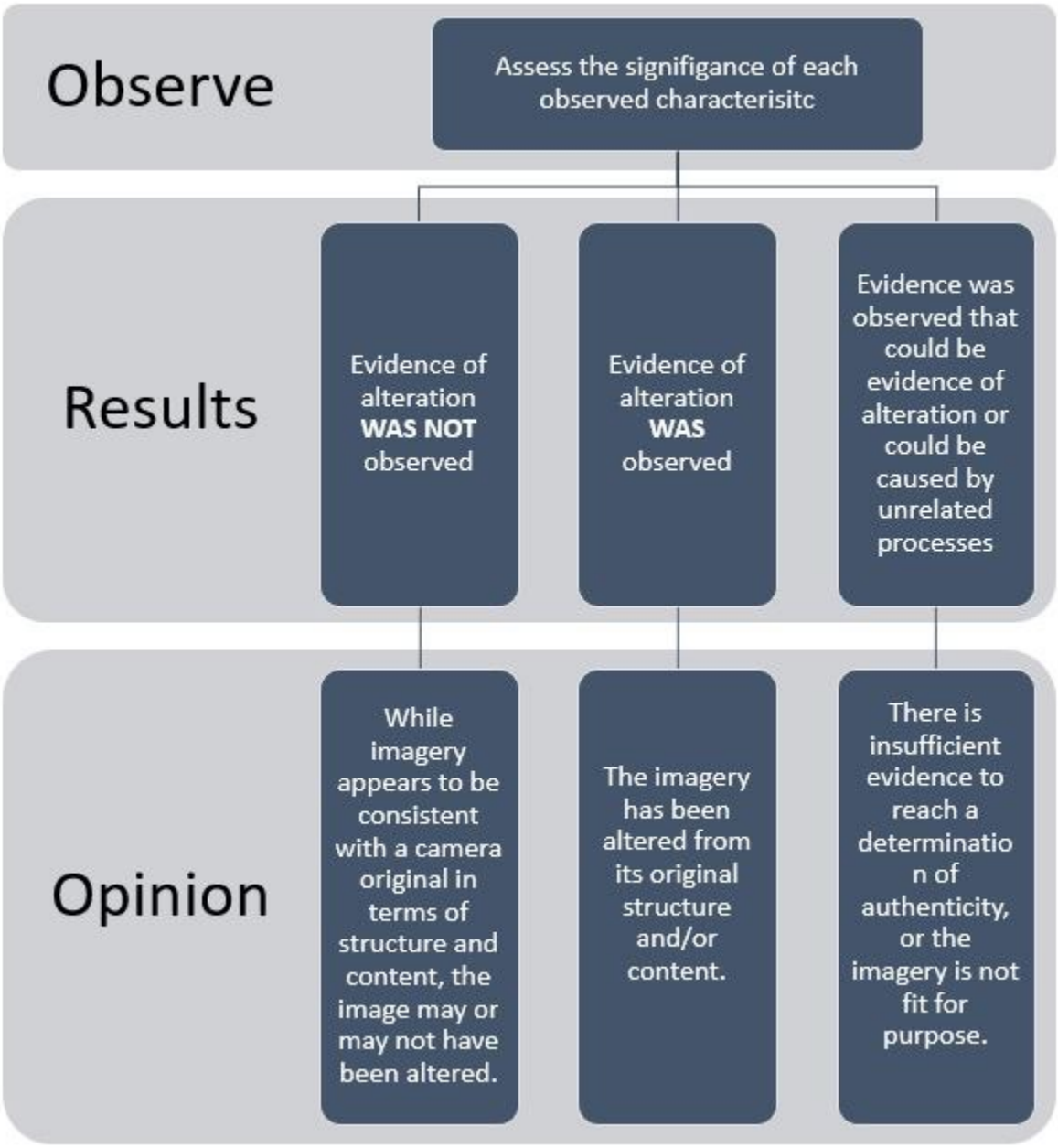

Figure 2. Flowchart on the formation of an opinion (Chart Credit: SWGDE, 2018).

8.2 Report the Results

Report the results, as well as a clear indication of the strength of the opinion (when appropriate).

- Practitioners should report the observed features, including those that support the specified opinion.
- Results should not be reported in terms of numerical probability without a proper scientific foundation and/or related research.
- The results must be properly qualified, address the limitations of the methodology and research, and be evaluated in terms of the propositions developed.

8.3 Review

The results of the examination must undergo independent review by a comparably trained individual. If disputes arise during review, a means for resolution of issues should be in place.

9. Limitations of Methodology

The strength of the results will be limited by the quality of the imagery, the quantity of the imagery, the detection of inconsistent features, and the availability of reference material, as needed. Based on these factors, it is possible the requested examination cannot be fulfilled. Forensic practitioners should take care not to overstate results.

One potential source of uncertainty in any forensic analysis results from cognitive biases (see section 10 for examples that include both confirmation and contextual bias). It is the responsibility of the organization and the practitioner to minimize the effects of bias when conducting examinations and performing reviews. Minimizing the effects of bias can be accomplished through awareness, training, documentation (of any potential sources for bias and the steps taken to minimize), and quality assurance measures, including the limitation of task-irrelevant information and blind verification. For additional information on quality assurance measures in digital and multimedia forensics, see *SWGDE 10-Q-001-1.0 Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*.

10. Additional Resources

- Cooper, Glinda S., and Vanessa Meterko. "Cognitive bias research in forensic science: A systematic review." *Forensic Science International*, vol. 297, no. April 2019, pp. 35-46. *Science Direct*, https://www.sciencedirect.com/science/article/pii/S0379073818304559. Accessed 9 Jan. 2024.
- Curley, Lee J., et al. "Assessing Cognitive Bias in Forensic Decisions: A Review and Outlook." *Journal of Forensic Sciences*, vol. 65, no. 2, 2020, pp. 354-360. *Wiley Online Library*, https://onlinelibrary.wiley.com/doi/abs/10.1111/1556-4029.14220. Accessed 9 Jan. 2024.
- Kunkler, Kimberly S., and Tiffany Roy. "Reducing the Impact of Cognitive Bias in Decision Making: Practical Actions for Forensic Science Practitioners." *Forensic Science International: Synergy*, vol. 7, 2023, https://www.sciencedirect.com/science/article/pii/S2589871X23000281. Accessed on 9 Jan. 2024.
- National Commission on Forensic Science. "Views of the Commission Ensuring That Forensic Analysis Is Based Upon Task-Relevant Information." *U.S. Department of Justice*, https://www.justice.gov/archives/ncfs/file/818196/download. Accessed 9 Jan. 2024.
- Quigley-McBride, A., et al. "A Practical Tool for Information Management in Forensic Decisions: Using Linear Sequential Unmasking-Expanded (LSU-E) in Casework," *Forensic Science International: Synergy*, vol. 4, 2022, https://doi.org/10.1016/j.fsisyn.2022.100216. Accessed 17 Sept. 2024.
- Sunde, Nina, and Itiel E. Dror. "Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward." *Digital Investigation*, vol. 29, 2019, pp. 101-108. https://www.sciencedirect.com/science/article/pii/S1742287619300441. Accessed 8 Jan. 2024.
- Scientific Working Group on Digital Evidence. *Best Practices for Video Authentication*. SWGDE 23-V-001-1.2. *SWGDE*, 2023, https://www.swgde.org/23-v-001/.
- Scientific Working Group on Digital Evidence. *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. SWGDE 10-Q-001-1.0. *SWGDE*, 2010, https://www.swgde.org/10-q-001/.
- Scientific Working Group on Digital Evidence. *Training Guidelines for Image Analysis, Video Analysis, and Photography*. SWGDE 15-M-001-1.1. *SWGDE*, 2015, https://www.swgde.org/15-m-001/.

11. Appendix A: Workflow Example 1

A local police department receives a report of possible child exploitation and downloads imagery from the internet. After retrieval, a compact disc containing images is turned over to a forensic laboratory to determine if the child depicted in the imagery is real, and/or to determine if any manipulations have occurred to the images.

Following the methodology described above, the laboratory proceeds:

1. The request is reviewed, and it is:
    a. determined that this type of analysis is conducted;
    b. determined that all necessary items to support the requested exam have been submitted;
    c. determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and
    d. assigned to an analyst.
2. The analyst acquires the necessary imagery.
    a. The analyst calls the investigating agency/organization and determines that the best quality images have been submitted, and all images have been received.
    b. The analyst reviews the images and selects relevant images for further analysis.
3. The analyst makes copies of the selected imagery for use as working copies and safely stores the received disc.
4. The analyst examines the imagery file structures, to include an examination of the file formats and associated metadata. The analyst determines there is no GPS information, and the file creation dates and file modification dates are the same. The analyst similarly determines the files contain basic camera setting information and thumbnail images are present. This information is documented in the case notes.
5. The analyst determines no image processing software tags exist within the metadata. This information is documented.
6. The analyst examines the content of the imagery. The following inconsistencies were observed and documented:
    a. The majority of the images showed no signs of lossy compression, but one significant portion of an image contained 8x8 jpeg blocking.
    b. The portion of the suspect image appears to have a light source inconsistent with the remainder of the image.
    c. The scale of the subject depicted in the suspect portion is inconsistent with objects in the remainder of the image.
    d. The depth-of-field in the suspect portion is inconsistent with objects in the remainder of the image.

7. The analyst concludes that one image of the submitted series appears to have been manipulated.
8. A comparably trained individual in the laboratory independently reviews the results of the examination.
9. The analyst issues a report. Per the laboratory's standard operating procedures, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the opinion, and the opinion.

12. Appendix B: Workflow Example 2

A local police department receives a report of possible child exploitation and downloads imagery from the internet. After retrieval, the police department develops a suspect and completes a search of the suspect's house pursuant to a search warrant. During the search, two cellular telephones are recovered. The investigating agency/organization contacts their laboratory to determine if the imagery was captured by the recovered cell phones.

Following the methodology described above, the laboratory proceeds:

1. The request is reviewed, and it is:
    a. determined that this type of analysis is conducted;
    b. determined that all necessary items to support the requested exam have been submitted;
    c. determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and
    d. assigned to an analyst.
2. The analyst acquires the necessary materials.
    a. The analyst calls the investigating agency and determines that all imagery and questioned phones have been received.
    b. The analyst reviews the images and selects relevant images for further analysis.
3. The analyst makes copies of the selected imagery for use as working copies and safely stores the received evidence. The analyst also receives permission from the investigating agency to capture images with the questioned phones, thereby changing the data on the phones. The analyst is informed the phones in question have already been thoroughly documented and receives appropriate permissions.
4. The analyst examines the imagery file structure, to include an examination of the file formats and associated metadata. The analyst determines there is no GPS information, and no make, model or serial number captured in the imagery metadata. This information is documented in the case notes.
5. The analyst determines no image processing software tags exist within the metadata. This information is documented.
6. The analyst examines the content of the imagery. The average luminosity is determined to be above the threshold needed for examination.
7. The Photo-Response Non-Uniformity (PRNU) pattern is calculated for each of the relevant images.
8. Exemplar images are captured with the questioned phone cameras.
9. PRNU patterns are calculated for each set of exemplar images.
10. The PRNU patterns are compared between the questioned imagery and the exemplar images. A correlation value is calculated for each comparison.

11. Based on the correlation values calculated, the analyst reaches the opinion that the examined images were captured by one of the questioned phones.
12. A comparably trained individual in the laboratory independently reviews the results of the examination.
13. The analyst issues a report. Per the laboratory's standard operating procedures, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the opinion, and the opinion.

13. Appendix C: Exemplar Image Authentication Form

Scientific Working Group on Digital Evidence — See cover page for SWGDE disclaimer.

EXEMPLAR IMAGE AUTHENTICATION FORM

Examiner: _____ Date: _____

Evidence #: _____ File name: _____

Media Type: ☐ Digital Image or ☐ Printed Still Photo

From: Digital Video OR Analog Video (Type: _____); N/A Other: _____

Mode: _____ Depiction: ____color ____monotone

File size: _____ Resolution: _____

Compression artifacts: ☐ present ☐ not present ☐ unable to determine

Software Tools used (Y/N):

FILE INFO_____ METADATA _____ HEX Reader _____ CODEC Finder _____

Software tags? (Y/N) Details: _____

PRNU Evaluation(Y/N): _____

Image Processing software (Y/N): OBSERVATIONS:

- Levels _____
- Threshold _____
- Equalize _____
- Contrast _____
- Saturation _____
- Hue _____
- Curves _____
- Channels _____
- Brush Strokes (Accented Edges) _____
- Stylize (Find Edges)____(Glowing Edges)____(Trace Contour)____
- Invert _____

Advanced Image Processing (Y/N): _____

- Interactive Channel Selector _____
- Color Safe Levels/Curves _____
- Pattern Remover (FFT) _____
- Edge Enhancer _____
- Adaptive Equalization _____

Open Source Tools (Y/N):

- Process: FFT _____Find Edges_____ Subtract Background _____
- Image Adjust – Threshold _____ Threshold Color _____
- Image Split Channels_____ Image Properties_____ Show Info_____
- Plug-in's / Scripts_____ JAVA Properties _____

Notes: _____

Lab#_____ Case#_____ Page _____ of _____

14. History

Revision	Issue Date	History
1.0 DRAFT	1/11/2018	Initial draft created. SWGDE voted to approve as a Draft for Public Comment.
1.0 DRAFT	4/17/2018	Formatted for release as a Draft for Public Comment.
1.0 DRAFT	6/14/2018	Minor editorial changes based on public comments. Changed the use of "practitioner" or "examiner" to "analyst" throughout the document. SWGDE voted to approve as a Final Approved Document.
1.0	7/11/2019	Formatted for release as a Final Approved Document.
2.0 DRAFT	5/14/2024	Content added for five-year review. SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
2.0 DRAFT	9/19/2024	Added information based on public comments received. SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
2.0	2/21/2025	No comments received. SWGDE voted to approve as a Final Approved Document.
2.0	2/26/2025	Formatted for release as a Final Approved Document.