Scientific Working Group on Digital Evidence

Best Practices for Digital Video Authentication

23-V-001-1.2

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 Digital Video Authentication

Table of Contents

1. Purpose

Authentication is defined as the process of substantiating that the data is an accurate representation of what it purports to be. When examining digital video files for authentication, an examiner seeks to determine if the file's video content, context, and structure align with the information provided about the file. The purpose of this document is to provide the background, technical considerations, and potential criteria to conduct forensic authentication examinations of digital video in order to assess a file's provenance, content, and integrity.

2. Scope

This document will iterate the possible categorical outcomes of video authentication examinations (e.g., contextualization, source identification, content authentication). The document will outline the categories of data inherent in digital video files that can be exploited during an authentication examination. Finally, the document will identify the available techniques used to examine specific categories of data in digital video files.

3. Limitations

This document exclusively addresses digital video files and does not address the authentication of analog recordings/media nor digital tape, or non-file-based media (e.g., live broadcast, streaming media).

While this document covers several methods to identify potential authentication issues, it does not cover context-based authentication. The methods discussed can identify where the video recording is an accurate original or altered, but it cannot determine if the events depicted within the file are authentic. For example, a video file may be a camera original file, but the scenes were scripted and reenacted.

If the questioned media is a multimedia file, which contains both audio and video streams, an authentication of the audio should be completed. This document does not address audio authentication and recommends that examiners refer to the guidance articulated in that document. The authentication of audio content is addressed in *SWGDE 15-A-001-1.3 Best Practices for Digital Audio Authentication*.

Still images are a component of a digital video file. As a result, individual images are discussed in the context of video authentication. To better understand the methodology for the authentication of individual digital images, please refer to *SWGDE 18-I-001-1.0 Best Practices for Image Authentication*.

This document is not intended to be a training manual or a specific operating procedure. This document is not all-inclusive and does not contain information relative to specific commercial products. If dealing with technology outside your area of expertise, consult an appropriate specialist. For recommendations on forensic video training, refer to *SWGDE 15-M-001-1.2 Training Guidelines for Video Analysis, Image Analysis, and Photography*.

Regarding specific techniques for examinations, there may be limitations to their individual effectiveness in specific scenarios. For this reason, it is useful to examine digital video files

using multiple examination methods whenever possible. The examination process should be designed to mitigate the potential effects of bias.

4. General Concepts

When conducting forensic examinations to determine authenticity, the methodology to authenticate/identify a video's source may differ from the methodology to authenticate whether or not the video content has been altered. Commonly asked questions that drive authentication examinations include but are not limited to the following:

- How did a file come to be in its present state?
- What type, brand, or model of camera generated the file?
- Is the file a camera-original file?
- Has the file been re-encoded?
- Has the content of a file been altered/modified beyond what it is purported to be?

To answer these types of questions, an authentication examination may be interested in one or all of the analyses below. Each approach may require a specific set of examinations (listed in section 5 of this document) The examiner must choose the appropriate techniques and apply them effectively to complete the authentication examination. A known (sample video) from the alleged original device or one that reflects the alleged generational history of the file being questioned should be obtained, if possible, for the examination.

4.1 Contextualization

Contextualization as it relates to video authentication is the examination of digital video evidence to determine the provenance or the history with which the digital video file was created. This evaluation typically discerns the software or type of software that last interacted with a video file. The encoding structure and metadata within a file can assist with this type of examination.

4.2 Source Identification

Source identification as it relates to video authentication, is the examination of digital video evidence to identify the type of equipment or camera that originally created the video file. This is most effective through a comparative analysis between a questioned and reference multimedia sample.

Outcomes often include identifying the make, model, and software version that the equipment or camera used when encoding the video. Encoding structure, in conjunction with technical attributes, can be used to identify camera brands and models [1]. These attributes can be used to identify camera brands and models, provided the user has knowledge of what the camera brand and model structure should present as.

4.3 Content Authentication

Content authentication, as it relates to video authentication, is the examination of digital video evidence to determine potential visual changes to the encoded streams within the digital video file container. This analysis reviews the decoded image and audio samples stored within the file at the global and local levels. Metadata and structural analysis can assist in determining what changes the recorded audio/video streams underwent.

Outcomes of the analysis may include, but are not limited to, the following:

- Video data content has been recompressed.
- Color space has been affected.
- Content is missing.
- Content has been added.
- Apparent image alterations.
- Changes to the timing of the playback.

5. Technical Considerations

When examining digital video files for an authentication examination, there are specific elements to be evaluated. These elements are described further in this section, including the type of video format (i.e., the container), the arrangement of the components within the container (i.e., the structure), the attributes and embedded information (i.e., metadata) defined within the container, and the image and audio samples themselves (i.e., content).

5.1 Container

A video container (referred to in this document as a container) is a digital file format that is used as a wrapper for data files. The specifics of containers have been covered in a previous document, *SWGDE 17-V-001-1.3 Technical Overview of Digital Video Files* [2]. When evaluating a container, an initial consideration is whether the container is proprietary (i.e., the encoding specifications for the container are not known outside of the private entity that authored the specification) or open file format (i.e., the encoding specifications for the container are publicly available, either freely or for a fee).

Knowing the type of container informs which techniques can be employed during an authentication exam.

5.1.1 Considerations for Proprietary Format

The following are examinations that are applicable to proprietary camera/recording systems, devices, and files:

- If a recording system has a built-in security or validation feature, document the state of those features. When possible, obtain documentation from the manufacturer of the embedded security features and include it in case notes.

- If a recording system uses a file naming convention, document the filename and its relationship to the naming convention.
- Research the system to determine:
    - Are specific applications or codecs required on the lab system to decode or playback the video or audio?
    - What is the impact of transcoding the file into an open file format?
        - How will metadata be preserved or changed?
    - How is the file format structured?
    - How are the data streams structured?
    - Are there peripheral (e.g., hidden, inaudible) data streams or other data present (e.g., timecode, data block numbering) within the video file or in separate files produced as part of the recording process?
    - Are there additional unrelated files present at the time of creation?
    - Can recordings and administrative files deleted from the device be recovered?
- Due to the proprietary nature of the format, editing any data and encoding the resultant file in the same proprietary format is almost impossible.

Other analyses may require that proprietary files be exported to an open file format.

5.1.2 Considerations for Open File Formats

Open file formats, such as ISO Base Media File Formats (e.g., MOV, MP4, M4V, 3GP, 3G2), the Advanced Systems Format (ASF) (e.g., WMV), Matroska (e.g., WebM, MKV), and the Resource Interchange File Format (RIFF) (e.g., AVI), all of which adhere to published specifications and are compatible with most playback and editing software. Video editing software may modify a file's metadata fields and internal binary structures. It may also change the order of internal binary structures, alter their information, add new structures, and/or delete them entirely. The possibility exists that a video may be altered using an external editor and placed back onto a device prior to submission and extraction. Therefore, when encountering these formats, consider a comparison with an exemplar file from the same make/model of device as the questioned file; or even the original recording device, if possible.

5.2 Structure

Regardless of the format (e.g., open file or proprietary), the structure of digital video files is complex. The format specification for a given container will include a definition of how internal functional and non-functional components are stored within the binary stream. These internal components have structural integrity that can be documented through binary analysis.

Techniques described in Section 5 of this document examine these internal components to identify the camera or software that last encoded the file that is being evaluated.

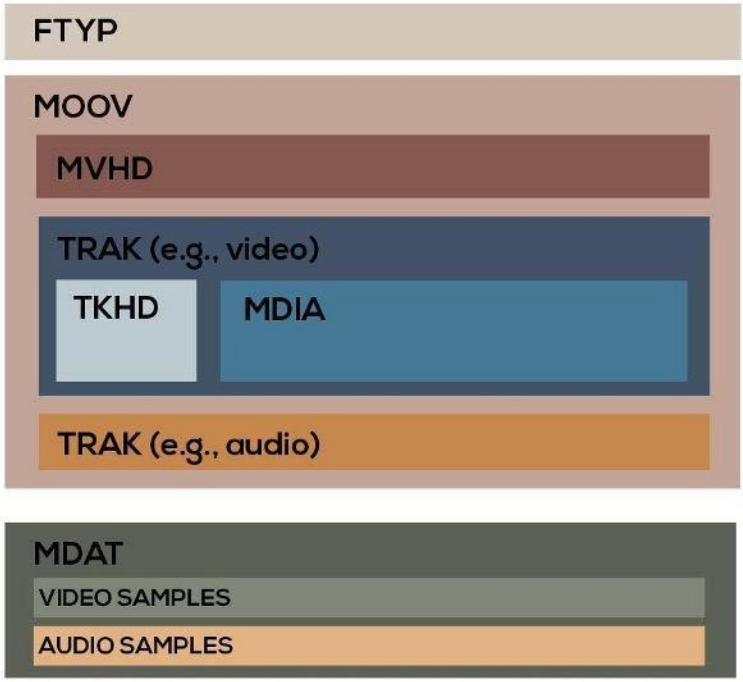

Figure 1. An illustration of some of the components that constitute an ISO Base Media File Format (e.g., MP4, MOV, 3GP) video file structure. (Image Credit: SWGDE)

5.3 Attributes

The attributes of a video file are often referred to as a type of metadata about the file itself. Metadata about digital video files can be embedded within the file but can also be calculated by tools that read the internal content. Common technical attributes of interest include but are not limited to, the date and time of the recording, spatial resolution, frame timing (X) (sample rate), bits per sample, color space, number and types of sample sets contained within the file, and bit rate.

Non-technical attributes of interest can include, but are not limited to, software used to encode the video, camera brand and/or model that created the video, modification timestamps, and GPS data.

There is no metadata standard for digital video files in the same way that EXIF exists for digital still images. Metadata is susceptible to alteration without affecting the playback of the file. Metadata cannot be relied upon in isolation and should be used in conjunction with other elements of the file when possible.

When performing an attribute analysis, the metadata extraction tool should be validated. Multiple metadata tools should be used to verify the interpreted results as well as the accuracy of the encoded attributes of the file. See *SWGDE 18-Q-001-2.0 Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics* for additional information.

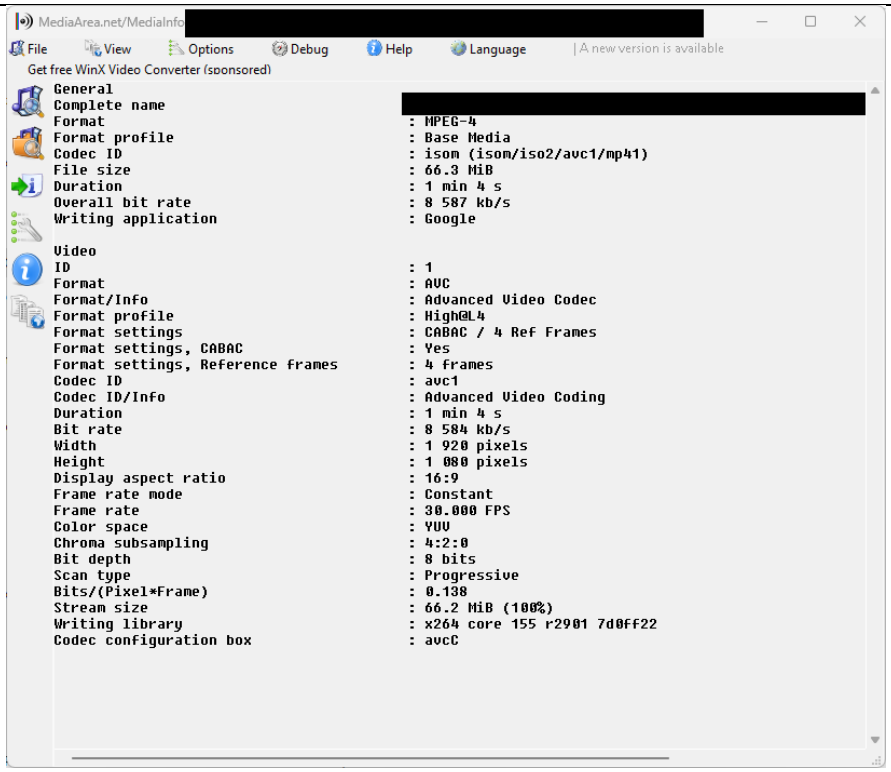

Figure 2. An example of the output of Media Info when extracting metadata from an MP4 video (Image Credit: SWGDE)

5.4 Video Content

The purpose of the video container is to be able to deliver recorded samples of moving images and/or sound on a timeline. These samples are often referred to as the content of the video file. *SWGDE 17-V-001-1.3 Technical Overview of Digital Video Files* [2] describes the ways digital video content is encoded, stored, and reconstructed for playback.

An analysis of the content within a digital video file can be carried out on global and local elements to determine whether the recorded images and/or the timing of playback has been altered from what has been purported about the file being examined.

6. Prior to Examination

When the digital video file is submitted, the requestor should include a clear statement of the work desired. Care should be taken to avoid any potential examiner bias by obtaining only the necessary amount of case information.

Files submitted in a manner that leaves questions to the chain of custody should be evaluated for their originality prior to additional analyses. This includes videos submitted through a public portal or not directly acquired by a submitting organization. More information on the collection of videos from third-party sources is available in *SWGDE 20-V-002-1.0 Guidelines for Video Evidence Canvassing and Collection*.

6.1 Clarify The Request

Before the authentication examination can begin, there must be a clear understanding of the request. Some questions to consider may include:

- What is the legal authority to operate on the submitted video file?
- What is the purported chain of custody of the submitted video file?
- What is the purported date and time the video was made?
    - Determine if the authentication request extends to the authentication of the time/date of file creation (or modification).
- What is the purported original camera, recording system, device, and storage media?
- Is the recording device accessible for testing?
- Are there other examples from the same device available for evaluation?
- What are the specific questions or issues raised related to the questioned video's authenticity?
    - Determine if the authentication request extends to the context of the events recorded within the questioned video.
    - What file, video encoding, and audio encoding formats are supported by the purported original recording system?
    - What physical media type can be used in the device?
    - Can the device transmit or receive video electronically?
    - Are there embedded security features to prevent alterations?

6.2 Assess the Request

Once an examiner has evaluated the request, they should determine if an authentication examination is suitable to answer the requestor's questions. In some cases, there may be multiple types of authentication examinations needed in order to address the request. If no suitable examination is able to address the request, inform the requestor of the findings. The requestor can then modify the request, or a request for a different examination can be made.

6.3 Prepare for Testing

Once a determination of which questions about the authenticity of the video can be made, the examiner should then develop a plan, obtain reference videos, and prepare the questioned video for analysis. Assess and document the technical attributes of the video.

6.3.1 Develop a Plan

Follow your evidence handling standard operating procedures in the event it is necessary to test an evidence device.

NOTE: Some digital/network recording systems have the capability to export configuration parameters to retain the state of the evidence device's configuration.

6.3.2 Generate Exemplars

If device classification or identification is the primary objective, exemplar files may need to be generated for comparison. Video samples produced by the testing equipment may have various export and acquisition methods available. Evaluation of all possibilities including double encoding, direct downloading, sharing, or other acquisition methods from these devices will ensure the most accurate results.

6.3.3 Prepare Files for Video Stream Analysis

While the original questioned file should be preserved, there may be times when an audio or video stream needs to be isolated or prepared as an independent media file (e.g., separating the audio and video streams into bifurcated channels.). When isolating the audio or video streams, the preferred method for analysis is to copy the media stream from the original file (e.g., stream copy). In circumstances where this is not possible, each stream may be transcoded into a lossless or uncompressed codec.

Should an individual still image be needed from a video stream, exports should also be conducted in a lossless or uncompressed format. One method to verify the streams have not been altered in the conversion process is to use a method called stream hashing, which can be calculated on the questioned file prior to transcoding and compared with the duplicated file's stream to verify there is a decoded value match. For more information on conversion and stream hashing, see SWGDE Technical Notes on FFmpeg.

7. Examination Techniques

The following describes a generalized workflow for the authentication of video evidence. These recommendations represent specific considerations to be addressed by the examiner. The exact sequence will be dependent upon the evidence submitted and the required examinations.

The digital video authentication examination is a process that leads to a conclusion based on the interpretation of global and local testing results and shall be comprised of a clearly defined set of analyses. As with any scientific examination, the process shall be systematic, objective, and repeatable. Test results should be reproducible using only validated tools and methodologies widely accepted in the scientific community. The analyses and conclusions submitted by the examiner shall be peer-reviewed by an examiner of similar qualifications.

7.1 Types of Analyses

Analyses can be classified as observation-based or measurement-based. For example, techniques that express the format or extract embedded metadata can be considered observational analysis and Techniques that calculate duration or quantify similarity are categorized as measurement-based analysis. Measurement uncertainty or measurement error applies to measurement-based analyses only. See *SWGDE 12-Q-001-2.0 Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis* for more information.

Additionally, when evaluating elements of digital video files, techniques can target the entirety of the file (global) or smaller segments of content within the file (local):

- Global Analysis: Global analyses are conducted on the file as a whole and produce results relevant to a video's authenticity without regard to specific areas or portions of a video.
- Local Analysis: Local analyses are conducted on specific areas or portions of a video and provide results relevant to a video's authenticity.

Not all tests will be applicable in each case, nor shall any single analysis be individually relied upon. All applicable tests available to the examiner should be conducted. By conducting multiple tests, the results from each can be cross-verified, thereby increasing confidence in the conclusion.

- Visual Analysis: A thorough and detailed examination should be carried out at both the local and global levels to carefully assess the visual consistency of the scene content. This examination should adhere to a consistent and systematic methodology, which may involve the use of a standardized form or checklist, ensuring that the examination is conducted in a scientific manner.
    - During the examination, various attributes should be observed, such as: consistency of textures, adherence to physical laws and principles, e.g. the consistency of object-to- object relationships, uniformity in lighting conditions, accurate depiction of shadows, adherence to gravity, and realistic representation of fluid dynamics, among others. By thoroughly evaluating these elements, a comprehensive understanding of the content's visual coherence can be achieved.
    - Note: Any inconsistency observed in these scene attributes may or may not indicate intentional tampering.
- File Format Analysis: A type of global analysis in which an examiner uses applications capable of reading and decoding video file metadata to document metadata fields in the file and their associated values. Alternatively, this work can be done manually using an examiner's knowledge of file formats and a hex editor.
- File Structure Analysis: A global analysis of the internal components that constitute the digital file. This analysis can be used to describe the internal binary components of the file being examined or can be used to compare to an exemplar from the same device class, if not the same device.
- File Structure Comparison: File structure comparison involves comparing the file format and hexadecimal data in the questioned file with data from exemplars of known cameras created using all variations of the camera's settings. The file structure comparison may also involve a comparison of the questioned file with known device library/databases and core software library/databases. The comparison analysis looks for artifacts indicative of alterations or tampering as compared with the original camera's file structure artifacts [2].

- Pixel Level Analysis: A combination of local and global processes used in digital video authentication to examine the individual pixels of a video frame in order to identify any signs of manipulation. This type of analysis can be used to detect a wide range of video manipulation techniques (e.g., adding or removing objects, altering the background, or changing the lighting/color of the scene).
    - Frequency Analysis: The combination of local and global processes of looking for high- frequency details through tools such as a Fourier filter. The filter's output is then reviewed by correlating the surrounding frames for irregularities.
    - Color Space Analysis: A global analysis process that examines the values within a color space to evaluate potential exaggerations to a color space. In a video with altered values, there will be peaks within the color space.
    - Histogram Equalization/Color Channel Analysis: A local analysis that allows examiners to utilize filters to visually inspect a video frame through individual color channels, equalization of multiple channels, and their luminance levels.
- Double Compression Analysis: A global analysis process that utilizes the fundamentals of spatial encoding within videos (more information available in Section 6 of *SWGDE 17-V-001-1.3 Technical Overview of Digital Video Files* [2]). Examiners ensure that the total block types for each frame type are consistent with the stated GOP structure.
- Correlation Analysis: A local process that evaluates the decoded values of a frame and compares them to the decoded values of a corresponding frame to determine if a frame or portion of the frame is copied, moved, or cloned.
- Image Sensor Analysis: A global or local analysis of a video that involves extraction of sensor pattern noise of each video frame by subtracting the original frame scene content from its noise-free version (frequently using a wavelet denoising filter) to obtain a noise-free frame. One common implementation of this is Photo Response Non-Uniformity (PRNU).
- PRNU: A sensor pattern noise created in processing variations where not all pixels demonstrate the same sensitivity to light. A local analysis may subsequently partition each video frame into non-overlapping blocks of the same size (e.g., N x N). Analysis of the statistical properties of block-level PRNU correlation may reveal tampered blocks between frames.

There are limitations where PRNU may not be a viable approach to identify the source of a submitted video file. Illumination and resolution are critical factors in successfully extracting a reliable PRNU signature from the source video.

It is recommended to test an exemplar device of the same make and model as the capture device used for the questioned video. It's important to note that pattern noise is typically

consistent with a compression scheme and possibly the make/model of the device, rather than the actual device itself.

8. Reporting

The results shall be communicated to the requestor and if deemed necessary, a written report prepared. Details typically included in a report regarding the authenticity of a recording will vary based on the analyses conducted and may include the following components:

- A list of all related observations, noting the significance of each.
    - Note: If attributes are observed that may be to the contrary of the opinion, they should be explained.
- A formulation of an opinion based on an interpretation of the results with accompanying technical explanations.
- The opinion should address the requested analysis.
    - Opinions must be properly supported and address the limitations of the methodology and research.
    - Care should be taken to not overstate the opinion.
- The strength of the opinion. It is possible for the results of an examination to be:
    - Consistent with an original
    - Inconsistent with an original
    - Inconclusive
    - Note: In examinations where a statistical result is made, the statistical model should be reported.

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.

Note: Refer to your agency's standard operating procedures for independent reviewing processes.

Language implying absolute certainty should be avoided unless discussing known alterations or deletions. *SWGDE 18-Q-002-1.0 Requirements for Report Writing in Digital and Multimedia Forensics* should be followed [3].

9. References

[1] Gloe, Thomas, et al., “Forensic Analysis of Video File Formats.” *Digital Investigation*, vol 11, 2014, pp.S68-S76. https://doi.org/10.1016/j.diin.2014.03.009.

[2] Scientific Working Group on Digital Evidence. *Technical Overview of Digital Video Files*. SWGDE 17-V-001-1.3. *SWGDE*, 5 Aug. 2024, https://www.swgde.org/17-v-001/.

[3] 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/.

10. Additional Resources

- Al-Athamneh, Mohammad et al. "Digital video source identification based on green-channel photo response non-uniformity (G-PRNU)." *Computer Science & Information Technology*, vol. 6, no 11, 2016, pp. 47-57. https://doi.org/10.5121/csit.2016.61105.
- Johnson, Micah K., and Hany Farid editors. "Exposing digital forgeries by detecting inconsistencies in lighting." *Proceedings of the 7th ACM Multimedia and Security Workshop*, Association for Computing Machinery, 2005, pp. 1-10. https://doi.org/10.1145/1073170.1073171.
- Li, Quan et al. "An Inter-Frame Forgery Detection Algorithm for Surveillance Video," *Information*, vol. 9, no. 12, 2018, p. 301. https://doi.org/10.3390/info9120301.
- Lukas, J, et al. "Digital camera identification from sensor pattern noise." *IEEE Transactions on Information Forensics and Security*, vol 1, no. 2 2006, pp. 205-214. https://doi.org/10.1109/TIFS.2006.873602.
- Popescu, A.C., and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, 2005, pp. 3948-3959. https://doi.org/10.1109/TSP.2005.855406.
- Scientific Working Group on Digital Evidence. *Best Practices for Digital Audio Authentication.* SWGDE 15-A-001-1.3. *SWGDE,* 20 Sept. 2018, https://www.swgde.org/15-a-001/.
- Scientific Working Group on Digital Evidence. *Best Practices for Image Authentication.* SWGDE 18-I-001-1.0. *SWGDE,* 11 July 2018, https://www.swgde.org/18-i-001/.
- Scientific Working Group on Digital Evidence. *Training Guidelines for Video Analysis, Image Analysis, and Photography.* SWGDE 15-M-001-1.2. *SWGDE,* 8 Feb. 2016, https://www.swgde.org/15-m-001/.
- Scientific Working Group on Digital Evidence. *Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics.* SWGDE 18-Q-001-2.1. *SWGDE,* 7 Mar. 2024, https://www.swgde.org/18-q-001-2/.
- Scientific Working Group on Digital Evidence. *Guidelines for Video Evidence Canvassing and Collection.* SWGDE 20-V-002-1.0. *SWGDE,* 14 Jan. 2021, https://www.swgde.org/20-v-002/.
- Scientific Working Group on Digital Evidence. *Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis*. SWGDE 12-Q-001-2.0. *SWGDE,* 20 Nov 2018, https://www.swgde.org/12-q-001/.

- Scientific Working Group on Digital Evidence. *Best Practices for Frame Timing Analysis of Video Stored in ISO Base Media File Formats*. SWGDE 19-V-005-1.1. *SWGDE,* 9 June 2022, https://www.swgde.org/19-v-005/.
- 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/.
- Van Houten Wiger, and Zeno Geradts. "Source video camera identification for multiply compressed videos originating from YouTube." *Digital Investigation*, vol 6, no.1-2, 2009, pp.48-60. https://doi.org/10.1016/j.diin.2009.05.003.
- Wales, Gregory S. *Proposed Framework for Digital Video Authentication*. 2019. University of Colorado at Denver. Master's Thesis. https://digital.auraria.edu/work/sc/11334ca6-d007-42b1-9fc3-20f30387b35d
- Wang, Weihong, and Hany Farid. "Exposing digital forgeries in video by detecting double MPEG compression." *Proceedings of the 8th ACM Multimedia and Security Workshop*, Association for Computing Machinery, 2006, pp. 37-47. https://doi.org/10.1145/1161366.1161375.
- Wang, Weihong, and Hany Farid. "Exposing digital forgeries in video by detecting duplication." *Proceedings of the 9th ACM Multimedia and Security Workshop*, Association for Computing Machinery, 2007, pp. 35-42. https://doi.org/10.1145/1288869.1288876.
- Wang, Weihong, Hany Farid. "Exposing digital forgeries in interlaced and deinterlaced video." *IEEE Transactions on Information Forensics and Security*, Vol. 2, no. 3, 2007, pp. 438-449. https://doi.org/10.1109/TIFS.2007.902661.
- Wang, Weihong and Hany Farid. "Exposing digital forgeries in video by detecting double quantization." *Proceedings of the 11th ACM Multimedia and Security Workshop*, Association for Computing Machinery, 2009, pp. 39-48. https://doi.org/10.1145/1597817.1597826.

11. History

Revision	Issue Date	History
1.0 DRAFT	9/14/2020	Initial draft created
1.0 DRAFT	9/19/2022	Content organized, formatted in new SWGDE template.
1.0 DRAFT	1/11/2023	Further formatted, sections re-arranged, detailed information about testing methods reduced and simplified. New content generated about source identification content authentication, technical considerations, and conclusions.
1.1 DRAFT	6/14/2023	Various layout and grammatical errors addressed and corrected. References to the evaluation of audio information when digital multi-media files present audio during a video investigation was revised
1.1 DRAFT	9/20/2023	Conclusion language revised to opinion based. Discussed further comments from other committees regarding local analysis methodology and relevancy. Substantive changes made to document.
1.2 DRAFT	2/29/2024	SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
1.2	11/6/2024	SWGDE voted to approve as Final Approved Document. Formatted for release as a Final Approved Document.