Scientific Working Group on Digital Evidence

Best Practices for Digital Forensic Video Analysis

18-V-001-1.1

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 suggested best practices, practical guidance, technical positions, and educational information 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 e-mail 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, 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

Unauthorized use of the SWGDE logo or documents 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 Forensic Video Analysis

Table of Contents

1. Introduction 2
2. Limitations 2
3. General Tasks 2
   - 3.1 Technical Preparation 2
   - 3.2 Examination 3
   - 3.3 Interpretation 4
4. Workflow 4
   - 4.1 Review Request for Analysis 4
   - 4.2 Technical Preparation 5
   - 4.3 Examination 7
   - 4.4 Interpretation 9
5. Delivery of Examination Results 10
   - 5.1 Storage Media 10
   - 5.2 Printouts 10
   - 5.3 Verification 11
6. Archiving 11
7. Additional Considerations 11
   - 7.1 Standard Operating Procedures 11
   - 7.2 Infrastructure 12
   - 7.3 Validation/Confirmation Testing of Tools 12
   - 7.4 Documentation 12
   - 7.5 Training, Competency, and Proficiency 13
8. References 14
9. History 17

1. Introduction

Forensic Video Analysis (FVA) is defined as the scientific examination, comparison, and/or evaluation of video in legal matters. Organizations may utilize different titles for the personnel who perform FVA (e.g., analyst, examiner, practitioner, scientist). For the purpose of this document, personnel performing FVA will be referred to as an "analyst."

The purpose of this document is to provide forensic video analysts with recommendations on the handling and examination of video evidence to successfully introduce such evidence in a court of law. These guidelines may also be used to assist organizations when developing standard operating procedures (SOPs) for the processing of video evidence. Organizations should align the best practices in this document to ensure they adhere to governmental and local laws, regulations, and SOPs.

For the purposes of this document, the word "image" refers to a representation of a subject or object derived from video or still photography.

2. Limitations

This document is not a training manual, nor a step-by-step methodology.

This document is intended for use by forensic science service providers working in a forensic environment. While many of the practices and processing techniques relate, it is not intended to be used for the processing of video files as part of criminal investigations strictly for use as an "investigative lead" (e.g., BOLO, wanted poster). For the purpose of this document, an investigative lead is any piece of information that should not be used as a sole source of charging decision or submission in court.

This document does not address the acquisition of digital and multimedia evidence. For more information on data acquisition from DVRs, see SWGDE Best Practices for Data Acquisition from Digital Video Recorders [1]. For more information on data acquisition from cloud storage, see SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage [2].

This document does not address the analysis of analog media.

3. General Tasks

The process of FVA can involve several different tasks, regardless of the type of analysis performed. These tasks fall into three categories: technical preparation, examination, and interpretation. The general principles and procedures used in these tasks are the same regardless of the format in which the images/videos are recorded.

3.1 Technical Preparation

Technical preparation is the performance of tasks in advance of examination, analysis, or output. There are a multitude of technical decisions within the various tasks. Technical preparation will affect further stages of the analysis. Tasks may include the following: creating working copies, integrity verification, write protection, organization of files, and playback optimization.

3.2 Examination

Examination is the application of imaging and computer science expertise to extract technical information from video. Examples may include the following: metadata collection, structural analysis, macroblock analysis, format conversion, timeline sequence reconstruction, and pattern or video frame information analysis. Examination tasks also include image and video clarification, frame averaging, video stabilization, synchronization, and other video processing activities intended to improve the visual appearance of features in a video.

3.2.1 Types of Examinations

- **Metadata and structural analysis**: The use of software tools to decode or calculate embedded and structural data contained in video files.
- **Format conversion**: The use of software to convert the video file's container or codec to facilitate examination, analysis, and/or playback.
- **Timeline sequence reconstruction**: The process of relating video, still images, audio, or other data to one another in a chronologically ordered succession. Analysts should be aware that synchronizing multimedia files with different video properties, if not properly accounted for, may result in a drift in synchronization. Additionally, analysts should be cognizant of different pixel dimensions between still images and videos to ensure that the aspect ratio is presented and scaled incorrectly.
- **Speed or motion analysis**: The determination of an object's speed and/or direction using frame information from the recorded video.
- **Pattern or video frame information analysis**: The use of a video's visual cues and/or metadata to examine specific information relative to individual frames of video (e.g., display order, display timing, identification of key frames).
- **Macroblock analysis**: The understanding and/or visualization of original video data and predicted information contained within individual video frames.
- **Frame difference**: The calculated difference between successive frames of video. This can be used to visualize and identify new and copied pixels.
- **Video frame extraction**: Accurately producing individual, or a group of, still images from recorded video while maintaining technical attributes as well as visual content.
- **Video clarification**: The use of techniques and adjustments to provide insight and information related to the visual data of a video frame. This can include pattern or noise removal, frame averaging, levels adjustments, stabilization, interpolation, and edge sharpening.
- **Comparison**: The analysis of video to extract individual frames and prepare images for comparison. This type of examination can be applied to objects or persons for identification purposes. It requires proper training and a comparison methodology. For

more information, refer to SWGDE Best Practices for Photographic Comparison for All Disciplines [4].

- **Video File Repair**: The applied knowledge of video file, codec, and frame information to repair or reconstruct video not available through traditional means.
- **Video Authentication**: An examination to determine if the file's video content, context, and structure align with the information provided about the file. Refer to SWGDE Best Practices for Digital Video Authentication [11].
- **Video Recovery**: The acquisition of video and audio evidence from digital video recorders. Refer to SWGDE Best Practices for Data Acquisition from Digital Video Recorders [1].

3.3 Interpretation

For purposes of this document, interpretation in video analysis is the application of specific subject matter expertise to develop opinions about video recordings or the content of those recordings produced in the examination. Content-based interpretations fall under the discipline of Image Analysis as applied to video images. For further information on Image Analysis, refer to SWGDE Guidelines for Forensic Image Analysis [5]. Interpretation can include statements pertaining to video attributes observed during the examination (e.g., reliability of images seen in temporally compressed frames).

NOTE: "Technical preparation," "Examination," and "Interpretation" are tasks, not job descriptions or roles. An individual may perform part of one task or a combination of multiple tasks within the organizational structure of any given activity. Additionally, not all requests require the use of all three tasks. Each of these tasks requires its own training and qualifications.

4. Workflow

The following describes a generalized workflow for the analysis of video evidence. These recommendations represent specific considerations to be addressed by the analyst. The exact sequence will be dependent upon the evidence submitted and the required examination(s).

4.1 Review Request for Analysis

- A submission form should be completed for every case the analyst receives, regardless of what type of examination or service the requestor is seeking. See Appendix A for an example.
- In exigent circumstances, it may be acceptable to obtain a verbal request for examination or service; however, a formal request should be completed prior to any final examination results being reported.
- Review the request for analysis and ensure the organization is able to fulfill the request. i) The organization must verify that it has the necessary equipment, materials, and resources needed to conduct the requested analysis.

- The organization must ensure the requestor has submitted all items needed to support the requested analysis or examination.
- Note: In some cases, it may be necessary for the organization to obtain additional items or information before the analysis can be started/completed. This may require the submission of additional items or an in-person meeting or phone conference.
- Efforts should be made to obtain pertinent information regarding the recording device, if not previously provided by the requestor (e.g., manufacturer, make, model).
- The request for analysis must be assigned to the appropriate personnel.
- Ensure that no other prior examination is required. In situations where video evidence requires additional forensic analyses, the video analyst should consult with qualified examiners (e.g., latent prints, DNA) to determine the proper sequence of examinations to maximize the evidentiary value of the submitted evidence. Analysts should follow organizational policy to minimize cross-contamination or destruction of physical evidence.
- Depending on the organization's SOPs, if a prior analysis on the same evidence has been performed, there may be a specialized process for submitting a request for the additional analysis.

4.2 Technical Preparation

4.2.1 Physical Inspection of the Submitted Media

- The evidence submitted with the request should be inspected prior to analysis to ensure that the physical items match those described on the submission form. Care should be taken based on any safety precautions or special handling identified in the request for analysis (e.g., use of gloves, presence of bodily fluids, exposed wires).
- Document and photograph the physical condition of the evidence.
- Inspect the items for physical damage that may impact the proper function of the media or device.
- If damaged, document and photograph the condition in which the item was received (e.g., scratches and cracks on optical media, the presence of
- contaminants, water damage).
- Follow organizational policies and procedures for documentation and repair processes.
- The integrity of all collected media should be verified or authenticated as needed. The scope of this examination is dependent on the acquisition methodology.
- Electronically submitted cloud-based evidence should be downloaded immediately and transferred to a more permanent means of storage. Refer to SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage for additional guidance [2].

4.2.2 Evidence Labeling

- Evidence should be labeled per organizational policy. Labeling may include initials, case number, item number, or any other identifying information required by the analyst's organization.
- Any identifying information (e.g., brand, storage capacity, serial numbers) should be documented.
- Labeling should not cover any identifying information, integral components, or existing labels.

4.2.2.1 Optical Media

- The ideal method for labeling optical media (e.g., BD-R, DVD-R, CD-R) is with a non-solvent-based felt-tip permanent marker designed to mark optical media.
  - Labeling should be made on the clamping ring, which is the clear inner portion, as no data information is recorded in that area. Inappropriate labeling methods may affect playback and could potentially damage the evidence.
  - Never use a ballpoint pen, pencil, or other sharp writing instrument when marking optical media.
  - Do not use adhesive labels on optical media as the label could delaminate over time and impede disc drive operation.

4.2.2.2 Hard disk drives and Flash Media

- Label the physical media directly, when possible.
- If the media is too small for labeling (e.g., microSD card, flash drive), the media should be placed in an appropriate packaging with the information required by the analyst's organization displayed.

4.2.3 Write Protection

- Digital media must be treated in such a manner to prevent modification of the content.
- The use of write blockers, either hardware or software based, should be utilized for flash media and hard disk drives (HDD). Digital media should be accessed as read-only or utilizing write-protecting mechanisms to ensure that data cannot be altered.
  - If the device is accessed as read-write, the reason shall be documented.
- When utilizing hardware write protection, the analyst should be aware that the flash media serial number displayed may be the serial number of the write protection hardware and not the flash media itself.

4.2.4 Creation of a Working Copy and Verification

- Create a working copy of the original submitted evidence.
- Steps should be taken to ensure the integrity of the data acquired; this should include computing a hashing algorithm on the original submitted evidence and the working copy. Compare the two hash results to ensure that they are identical and that no changes have occurred during the copy process.

4.2.5 Verify Proprietary Player Operability

- If a proprietary player is required to view the video, ensure operating system compatibility and codec functionality.

4.3 Examination

4.3.1 Media Interrogation

Media interrogation involves the examination of the technical aspects of a multimedia file to ascertain its attributes (e.g., display resolution, pixel aspect ratio, frame rate, codec).

- Interrogate the file to determine recording properties.
- There are several open source and commercial tools available for file analysis. A comparison of file interrogation results from multiple sources is recommended. Any discrepancies in the reported results should be documented and evaluated.
- Compare these results to those documented when the video files were acquired, if available. See SWGDE Best Practices for Data Acquisition from Digital Video Recorders for additional information [1].

4.3.2 Review

- The video files submitted for analysis should be reviewed to ensure that the file is an accurate representation of the video described in the request for examination. Any observed discrepancies with the information in the submitted request should be documented.
- If the submitted recording was not submitted in its native file format, then the limitations of the analysis (e.g., missing metadata, frame timing, resolution) should be communicated to the requestor. If the native file format is available, an attempt should be made to recover the most original version and document the status. If the native file format is not available, the format of what was recoverable should be verified and documented. Note: Considerations should be made to verify native file information, as necessary.
- A preliminary determination should be made with respect to the feasibility of the requested task(s) (e.g., clarification, comparison, conversion).
- When identifying the area of interest for analysis, the following should be considered:

- Whether there is information outside the area of interest that provides additional details relevant to the analysis. Note: Consider consulting with the requester to possibly expand the scope of the request.
- Whether any details about the incident not directly related to the request may be present. These include:
  - Images which could verify the time and/or place of the incident, such as clocks, street signs, scoreboards, and dispatch time when responding units arrive.
  - Potential witnesses or bystanders.
  - If the digital video file contains audio, examination should be considered. See SWGDE Best Practices for Forensic Audio

Note: Care should be given to information that could create a cognitive bias for the analyst.

4.3.3 Processing, Clarification, and Examination

- Any processing performed on the video files should be completed on the working copy and sufficiently documented so that the methods can be reproduced and independently evaluated. This documentation should include the order and settings in which the processes were applied to ensure the integrity and the reproducibility of the results.
- If possible, the video files should be imported into any processing, clarification, and/or examination tool in the native format. See SWGDE Technical Overview of Digital Video Files for more information [6].
  - Importing video files into software may require a conversion. Steps to preserve the original video codec should be taken, such as changing the file container while keeping the original video codec. Note: While the video frame information may stay intact, additional file metadata will be lost by changing the file container.
  - Should changing the container not produce a file for processing, steps can be made to transcode to a lossless codec. See SWGDE Technical Notes for FFmpeg for a list of processes [7]. Transcoding could affect the content of a video file by changing its visual appearance, however small. Avoid degradation of the video by limiting unnecessary conversions.
  - If no other option is available or appropriate, capturing the output of a proprietary player into an open file for processing is possible (sometimes referred to as screen capture). Care should be taken to ensure the resultant file stays consistent with the source material's recording properties (e.g., frame rate, frame count, resolution, aspect ratio).
- Identify the appropriate tool(s) to clarify the recording/image. The process of selecting tools should be done by looking for technical concerns within the video that can be corrected.

- Initial corrections should be those that account for the input file structure as it was recorded. These would include corrections for aspect ratio, understanding of compression artifacts, noise as it relates to chroma subsampling, frame rate, and file resolution. An understanding of these aspects can be found in SWGDE's Technical Overview of Digital Video Files [6].
- The analyst should then make corrections regarding the camera the video was recorded with. These can include issues with focus, luminance, focal length, and camera location.
- Once the technical concerns within the recording are resolved regarding the file structure and the camera, the analyst can address specific details within the area of interest. These can include noise removal (e.g., frame averaging, Fourier pattern removal), sharpening, and local adjustments.
- Specific information and additional recommendations related to video/image clarifications may be found in the SWGIT document Best Practices for Documenting Image Enhancement [8].

- Assess the clarified file and determine if it yielded the best result(s).

4.4 Interpretation

4.4.1 Opinions

The analyst may be asked to render an opinion regarding the evidence based on the scope of the request. The opinion should answer the question posed by the requestor as it relates to the evidence or results of the analysis. In instances where the opinion cannot definitively answer the question being asked, an answer of "inconclusive" may be the only appropriate response. In instances where a quantitative response is required, a margin of error may be expected, based on the frame information and compression of the images. The results of any FVA, regardless of scope, should be included in an analyst's report.

4.4.2 Reporting

- Results should be properly reported in accordance with an organization's SOPs. i) Reports should include the requestor, items of evidence, case number(s), results, and opinions, if applicable.

4.4.3 Technical and Administrative Review

4.4.3.1 Technical Review

- Efforts should be made to have a comparably trained analyst independently review the results of the analysis, including opinions rendered.

- Organizational SOPs should include the scope, frequency, and method of documentation for technical reviews. SOPs should also address the qualifications of the technical reviewer.
- An organization's SOPs should include a course of action if an analyst and the technical reviewer do not agree.

4.4.3.2 Administrative Review

- An organization's SOPs should include protocols for administrative review.
- The administrative review may be a supervisor, the technical reviewer, or a third party.

5. Delivery of Examination Results

The type of output (clarified video, still images, charts, or a combination of these outputs) is dependent on what best illustrates the content, quality, and events to be depicted in the final product. Consider the intended use of examination results and the quality of the output for playback and courtroom presentation.

Analysts should choose a format that preserves the quality of the clarified recording and meets the needs of the requestor. Consider using an uncompressed format, when applicable. If a compressed format is requested or required, it should be noted in the documentation and the consequences of that choice should be explained to the requestor.

Any labeling added to the output media, such as agency logos, text, case information, or analyst initials should not obscure the pertinent area(s).

5.1 Storage Media

- Examination results should be output to write-once media, where appropriate, (e.g., BD R, DVD-R, CD-R). Rewritable optical media (e.g., DVD-RW, CD-RW) should not be used.
- In situations where the analyst is responsible for the acquisition, preservation, processing, and analysis of video evidence it may be appropriate to store the original and resultant multimedia evidence onto one storage device.
- A hard disk drive or other media may be utilized in accordance with the organization's SOPs.
- A hashing function should be performed on the results media and stored with the case file.

5.2 Printouts

- Durability, longevity, and quality of printed images produced should be considered. Whenever possible, the printer manufacturer's recommendation for ink, paper, storage, maintenance, and settings should be followed.
- The most important aspect of printing is that the printed still image file remains a true and accurate representation of the original event. For this reason, considerations should be

made to ensure aspect ratios, resolution, and color balance is consistent between digital and printed images.

- Some clarified results may be best displayed digitally instead of in a printed format and should be documented when this is the case.
  - Printed reports may lose interactions that the analyst intended (e.g., embedded video, hyperlinks).

Note: For more information when resizing imagery and documentation, see SWGDE Fundamentals of Resizing Imagery and Considerations for Legal Proceedings [12]

5.3 Verification

Examination results should be verified to check that all content was transferred successfully, and that the quality of the output accurately reflects the results of the analysis.

- A post-examination hash value should be generated and documentation of the examination results to aid in verifying data integrity at a future point.
- The analyst should be aware that there may be compatibility issues between the examination results and the ability to play video files in the future.
- After verification, the original media and all examination results should be properly labeled, packaged, and sealed in accordance with an organization's SOPs.

6. Archiving

Case files, including examination results, should be archived in accordance with an organization's SOPs.

7. Additional Considerations

7.1 Standard Operating Procedures

Organizations should have SOPs for the handling, transportation, documentation, and storage of evidence for the analysis being performed. The SOPs should be organization specific, reflect the workflow, and be general enough to permit flexibility for the required tasks.

7.1.1 Evidence Management

Organizations should ensure that the evidence is safely stored, maintained, transferred, etc. to guarantee that the integrity of the evidence remains unchanged.

7.1.2 Quality Control and Quality Assurance

Organizational SOPs should provide planned and systematic actions necessary to provide sufficient confidence that the organization's product or service will satisfy given requirements for quality. These should include technical review, administrative reviews, validations, performance verifications, etc.

7.1.3 Security

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

7.1.4 Virus Scan

- Virus scanning should be performed in accordance with organizational policies and procedures.
- The specific methods and software applications used for virus scanning, and remedial actions if a virus is found, will be determined by individual organizations. This should be documented within an organization's SOPs.
- Considerations should be made for utilizing a virtual machine for any executable files or those that could make any changes or alter the local workstation. A virtual machine can serve to protect the host system from any potential malware or inadvertent system changes that can affect other casework.

7.1.5 Chain of Custody

- The chain of custody is the chronological documentation of the movement, location, possession, and disposition of evidence.
- Organizations should have chain of custody procedures in place throughout the entire FVA process and should follow these procedures to ensure the integrity, and authentication of the data.

7.2 Infrastructure

Organizations should have sufficient space, equipment, privacy, security, and facilities to adequately support the required quality and volume of work.

7.3 Validation/Confirmation Testing of Tools

Organizations should have SOPs that address validation and/or verification of software and hardware. Hardware used should meet the developers' minimum specifications. Consideration should be given to archiving previous software versions, builds, and operating systems for processing video evidence from legacy digital video recorder systems and other sources of video. For more information see SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics.

7.4 Documentation

- Notes should be contemporaneous with the examination process to document how evidence was handled and what processes were performed.

- The application of analytical techniques in a given case should be recorded to the degree that a similarly trained analyst would be able to replicate the techniques and reach a comparable analytical conclusion.
- Documentation may be accomplished through handwritten or electronically generated notes, photographs, photocopies, screenshots, and automated tool reports.

7.5 Training, Competency, and Proficiency

Organizations and Forensic Video Analysts are encouraged to review SWGDE Training Guidelines for Video Analysis, Image Analysis and Photography and SWGDE Proficiency Test Guidelines [9] [10].

7.5.1 Training

- Analysts should have sufficient training in their knowledge domain and associated forensic discipline. Sufficient training can be determined by a certifying body or an analyst's organization.
- Certification is one method to evaluate competency. 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 a specific amount of training, documented experience in the discipline, and the successful completion of an examination. Certifications can be beneficial and should be considered when appropriate.
  - In order to maintain most certifications, additional training is required for certification renewal.

7.5.2 Competency and Proficiency

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. Analysts should maintain competency through continuing education, training, successful proficiency testing, and peer review of examinations. Organizations and analysts should document training, competency, proficiency, and continuing education.

Analysts should demonstrate:

- An understanding of the scope of work and how it will be applied in the forensic environment.
- Subject matter knowledge and competence.
  - Knowledge of image and/or video processing and evaluation techniques.
  - Knowledge of image and/or video compression standards and technologies.
- Knowledge of applications and tools utilized in the specific organization.
  - Knowledge of SWGDE and SWGIT guidelines for capturing, storing, and processing image/video, including topics such as data integrity and compression artifacts.

- Understanding of legal precedent for the use of specific image and/or video processing techniques.
- Knowledge of appropriate case work documentation and ability to follow organizational SOPs.

- Analysts should 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, or internal/external validations.

8. References

[1] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Data Acquisition from Digital Video Recorders (DVRs)," 2023. [Online]. https://www.swgde.org/documents

[2] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Digital and Multimedia Evidence Video Acquisition from Cloud Storage," 2018. [Online]. https://www.swgde.org/documents

[3] Scientific Working Group on Imaging Technology, "Section 7: Best Practices for Forensic Video Analysis," 2009. [Online]. https://www.swgde.org/documents/swgit-document-archive

[4] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Photographic Comparison for All Disciplines," 2017. [Online]. https://www.swgde.org/documents

[5] Scientific Working Group on Digital Evidence, "SWGDE Guidelines for Forensic Image Analysis," 2017. [Online]. https://www.swgde.org/documents

[6] Scientific Working Group on Digital Evidence, "SWGDE Technical Overview of Digital Video Files," 2017. [Online]. https://www.swgde.org/documents

[7] Scientific Working Group on Digital Evidence, "SWGDE Technical Notes on FFmpeg," 2017. [Online]. https://www.swgde.org/documents

[8] Scientific Working Group on Imaging Technology, "Section 11: Best Practices for Documenting Image Enhancement,". [Online].]. https://www.swgde.org/documents/swgit-document-archive

[9] Scientific Working Group on Digital Evidence, "SWGDE Training Guidelines for Video Analysis, Image Analysis and Photography," 2016. [Online]. https://www.swgde.org/documents

[10] Scientific Working Group on Digital Evidence, "SWGDE Proficiency Test Guidelines," 2015. [Online]. https://www.swgde.org/documents

[11] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Digital Video Authentication" 2023. [Online]. https://www.swgde.org/documents

[12] Scientific Working Group on Digital Evidence, " SWGDE Fundamentals of Resizing Imagery and Considerations for Legal Proceedings (22-V-001-1.1) " 2022. [Online]. https://www.swgde.org/documents

Appendix A: Sample Forensic Video Analysis Submission Form

Organization Use Only

Forensic Case #: Item(s) #:

Received by: Date:

Forensic Video Analysis Submission Form

Submitting Agency: Submitter Name:

Agency Case Number: Submitter Email:

Offense: Submitter Phone Number:

Date of Offense: Submitter Division:

Offense Location: Submitter Address:

Evidence Submitted:

#	Item #	Description of Item	Recovery Location

Request:

☐ Video Enhancement ☐ Still Images ☐ Media Release ☐ Video Segments ☐ DVR Analysis

☐ Format Conversion ☐ Other:

Dates/Times of Export and/or Enhancements (if applicable):

Additional Details (if applicable):

Submitter Signature Printed Name/Employee Number Released to (Signature) if

applicable Printed Name/Employee Number

9. History

Revision	Issue Date	History
1.0 DRAFT	7/10/2018	Initial draft created and distributed for SWGDE voting.
1.0 DRAFT	7/25/2018	Voted by SWGDE for release as a Draft for Public Comment. Formatting and technical edit performed for release as a Draft for Public Comment.
1.0	9/20/2018	Comments from committees and public addressed. SWGDE voted to publish as an Approved document.
1.0	11/20/2018	Formatted and published as Approved version 1.0.
1.1	9/20/2023	Evaluated comments from committee members, and added new examination methods
1.1	3/22/2024	SWGDE voted to approve as Final Approved Document. Formatted for release as a Final Approved Document.