Scientific Working Group on Digital Evidence

Guidelines & Recommendations for Training in Digital & Multimedia Evidence

10-Q-002-3.0

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 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.

This project was supported by Grant # 15PJDP-21-GK-03271-MECP awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Scientific Working Group on Digital Evidence

Guidelines & Recommendations for Training in Digital & Multimedia Evidence

Table of Contents

1. Purpose

SWGDE provides many standards and guiding documents to support development of a multi-faceted digital forensic training program. As there are also many vehicles available to provide training, such as internal and external training programs, the purpose of this document is to provide guidelines and recommendations for training requirements for digital and multimedia evidence (DME) Forensic Science Service Provider (FSSP) personnel to assist any agency or activity with development of a proper training program.

2. Scope/Limitation

This document will recommend topics and guidelines for training within all of the DME disciplines. It should be recognized that some agencies might choose to provide training other than what is recommended in this section.

3. Terminology

The following definitions apply to this document. For additional definitions, please refer to the *SWGDE Glossary*.

- *DME*: Digital and multimedia evidence.
- *Education*: The baseline degree(s), previous training, or prior experience of an analyst.
- *Training*: The process of obtaining competency.
- *Continuing Education*: The process of maintaining proficiency, through additional training in evolving technology.

4. Introduction

Personnel that collect, preserve, analyze, and/or examine digital and multimedia evidence (or supervise these functions) must be aware of the capabilities and limitations of specific technologies. Those engaged in the digital and multimedia evidence examination process should be aware of related SWGDE documentation and the best practices and guidelines followed within the forensic community as well as strive to meet or exceed these recommendations. They should also endeavor to maintain awareness of new technical trends and developments.

In support of these goals, the following recommendations are offered:

- Define and employ quality assurance programs to ensure the implementation of valid and reliable procedures for the task.
- Maintain proficiency by pursuing training and continuing education courses in DME technology.
- Maintain awareness of legal developments relating to DME.
- Maintain awareness of technological advancements.
- Implement a program for continual assessment of personnel skills.
- Pursue professional development and establish certification timelines, if appropriate.

5. Categories of Training

Several categories of digital and multimedia evidence training relevant to those who capture, collect, preserve, process, analyze, and/or examine DME (or supervise these functions) are identified and defined as follows:

5.1 Awareness

Training designed to provide personnel with a general knowledge of the major elements of DME (i.e. video analysis, forensic audio, image analysis and computer forensics) including the capabilities and limitations of hardware and software.

5.2 Skills and Techniques

Training designed to provide personnel with the ability to competently use specific tools and procedures.

5.3 Knowledge and Application of Processes

Training designed to provide personnel with an understanding of DME procedures and how to apply that understanding given various situations, and the knowledge of other forensic discipline requirements and their intended uses.

5.4 Skills Development for Legal Proceedings

- *Witness Testimony*: Training designed to provide personnel with the ability to present clear and unbiased DME-based testimony in court. Legal implications for the integrity of collected and/or submitted evidence should be considered (e.g. search and seizure authorization).
- *Forensic Results Preparation*: Training designed to provide personnel with the ability to prepare accurate, clear, and concise documentation of results and/or opinions, and visual aids.

5.5 Continuing Education: Training designed to provide personnel with the ability to obtain the skills and knowledge of evolving technology in DME.

5.6 Specialized Applications and Technologies: Training in specific sub disciplines or in specialized areas (i.e. cell phones, vehicles, drones).

5.7 Job categories: The following job categories are provided as examples. Organizations may have different hierarchies and structures that combine some of the categories below.

- *Manager/Commander/Supervisor:* Includes personnel who are responsible for setting agency policies and/or making budget decisions; supervise and/or direct personnel engaged in the field of DME.

- *First Responder:* Includes personnel who are the first to secure, preserve and/or collect DME at the crime scene. These personnel often have general crime scene evidence collection responsibilities.
- *Crime scene Specialists* include personnel who document and preserve DME evidence outside a laboratory.
- *Technician:* Includes personnel whose primary responsibility is to collect/recover and/or prepare DME for examination and analysis. May include collection, acquisition, and preservation of DME outside of a laboratory environment.
- *Examiner/Analyst:* Includes personnel for whom examination, analysis, and/or advanced recovery of DME is a major component of their routine duties. The personnel may also be responsible for the collection of DME.

6. Topical Areas for Focused Training

The following section delineates specific topical areas in which personnel should receive focused training to fulfill their DME duties. It should be noted that in some instances a single person might occupy multiple job categories.

6.1 Considerations for All Job Categories

- Understanding of relevant standard operating and technical procedures
- Recognize the legal landscape surrounding the identification, preservation, collection, and analysis of DME, both on a digital device and in cloud computing technologies.
- Safety, security, and evidence protection issues such as blood-borne pathogen training, electrical safety, fire safety, and contamination prevention.
- Recognize the possible presence of other forms of physical evidence not related to digital and multimedia evidence such as fingerprints and/or other types of biological evidence.
- Technical support contact procedure for technology that exceeds the scope of tools, training, and experience.
- Recognize the presence of digital and multimedia evidence at the crime scene.
- Understanding of DME collection and preservation best practices
- Creation and maintenance of the chain of custody
- Ethics - Understanding bias and its impact on the digital forensic process.
- Quality assurance - Refer to *SWGDE Minimum Requirements for Quality Assurance in the Processing of DME* and other relevant SWGDE documentation.

6.2 Managers, Supervisors

- Knowledge of DME Process
    - Digital forensic process and its intersection with the identification, examination, admissibility, and legal challenges to digital forensic evidence

  - Digital evidence management, including chain of custody and evidence authentication procedures
  - Reporting of digital forensic findings, in both a a written and digital forensic format
- Knowledge of the Status of DME Technology:
  - Industry, market, and user trends for new and emerging technologies
  - Sources of digital and multimedia evidence used in criminal activities
  - Current life cycle-cost comparisons and limitations of hardware and software
- Understanding of Core Technologies:
  - Basic understanding of forensic science methodologies
  - Basic understanding of DME technologies
  - Strengths and limitations of digital and multimedia forensic tools (e.g. hardware and software)
- Knowledge of Key Legal Issues
  - Evidence and court procedures
  - Search for and seizure of digital evidence
  - Discovery, including the prosecutor's obligations under Brady v. Maryland, 373 U.S. 83 (1963), Giglio v. United States, 405 U.S. 150 (1972)
  - Testimony and exhibits
- Quality Assurance and Quality Management Systems:
  - Basic understanding of Quality Management Systems
  - Understanding of the importance of knowledge about tool performance
  - Understanding of the role of both competency and proficiency testing
  - Peer and Production Review
- Personnel Management:
  - Understanding of organizational strengths, capabilities, and limitations
  - Coordination of programs to address psychological stress and vicarious trauma
  - Time and personnel evaluation and management
- Strategic Alternatives and Planning:
  - Understanding the strengths and limitations of personnel and resources
  - Collaboration with subject matter experts in planning and decision making
  - Management of organizational budget
- Training Considerations:
  - Prioritization and implementation plan for organizational training life cycle
  - Understanding the most effective training delivery methods for organizational budget and personnel

6.3 First Responders

- Identification of DME media and digital devices with a focus on securing potential evidence.
- General DME collection and preservation techniques to avoid compromising the integrity of the digital evidence within the device (e.g., not looking through or performing actions on seized devices such as mobile phones).
- Convey the identification and preservation of DME media and digital devices to Crime Scene Specialists, Technicians, and Forensic Examiners/Analysts
- Photographing/memorializing the scene including potentially DME relevant items such as serial numbers or networking addresses.
- Documentation associated with identification, collection, and preservation of DME

6.4 Crime Scene Specialist

- General forensic principles and practices
- Recognize the presence and exigence of DME at the crime scene
- General DME collection and preservation techniques to avoid compromising the integrity of the digital evidence within the device (e.g., not looking through or performing actions on seized devices such as mobile phones)
- General and detailed photographs of the crime scene, including any devices appearing to be a digital device, for purposes of either the reconstruction of scene for forensic examination or obtaining evidence from a cloud service provider
- Knowledge of the technical resources for specialized collection and extraction of digital evidence that exceeds the resources of the person and/or agency.
- Technical support contact procedure for addressing technology they are unprepared to handle.
- Documentation associated with identification, collection, and preservation of DME

6.5 Technician

- General forensic principles and practices
- Identification of digital and multimedia evidence
- Knowledge of media types and remain current of new media formats technologies
- Understanding and application of evidence handling and preservation
- Use of forensic tools for media acquisition (hardware and software)
- Documentation associated with identification, collection, and preservation of DME

6.6 Examiner/Analyst

- Basic crime scene management

  - Understanding scene and evidence complexity
  - Identifying Collecting, Acquiring and Preserving DME
- Understanding and application of the DME examination process:
  - Identification
  - Collection
  - Preservation
  - Acquisition
  - Examination/Analysis
  - Documentation/Reporting
- Legal issues as related to the profession
  - Respect for the limitations of legal search authority
  - Understanding the legal limitations of DME data retention
- Court testimony skills
  - Refer to *SWGDE Introduction to Testimony in Digital and Multimedia Forensics*
  - Refer to *SWGDE Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings*
- Technical writing skills
  - Refer to *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics* and other relevant SWGDE documentation.
- "Best Practices"
  - Refer to current and relevant SWGDE best practices documentation
  - Refer to current and relevant SWGDE technical procedures documentation
- More discipline specific focused training documentation is available in the following documents:
  - *SWGDE Core Competencies for Digital Forensics*
  - *SWGDE Training Guidelines for Video Analysis, Image Analysis, and Photography*
  - *SWGDE Core Competencies for Forensic Audio*

7. Areas to Consider When Addressing Training Needs

A number of issues should be considered when addressing an agency's training needs. The following section provides guidance for selecting training venues and addressing continuing education and testimony training needs. Training may be internal, taught by competent practitioners on staff, or may be external, utilizing third parties and personnel outside of one's organization. An assessment of an individual's knowledge, skills, and/or abilities, may affect an individual's specific training program and needs.

The quality and structure of educational and training opportunities can vary. It is incumbent on the organization or examiner to manage those opportunities to ensure that the training

accomplishes desired goals. (OSAC Digital Evidence Subcommittee is currently working on a document describing requirements for university DME programs which is anticipated to be published in early 2024. This document will be updated with the reference when it becomes available.)

7.1 Education

- Baseline education can be achieved in a variety of digital and multimedia forensic subdisciplines through a number of ways, including, but not limited to:
    - Training on digital forensics as part of a larger program of education such as police academy training, etc.
    - Vendor-neutral or tool-specific training on digital forensics with specific measurable standards to assure foundational knowledge has been achieved
    - Possession of a degree and documentation of its area of expertise.
    - Dictated by the forensic discipline or the requirements of the agency
- Higher Education: The possession and type of a degree may be dictated by the forensic discipline, accreditation requirements, or other requirements of the organization.

7.2 Continuing Education

- Continuing education should be obtained from a variety of relevant sources and consistent with organizational training policy and workflow.
- Training conferences, trade shows, professional organizational training and education, professional publications, current literature and specialized courses all provide potential opportunities for continuing education.
- Self study can include reading blogs, listservs and other web-based resources with an emphasis on DME as well as performing research in the lab and membership and participation in DME community groups.
- Continuing education should include and address updates, and the use of new technologies as it relates to:
    - Hardware and equipment
    - Software
    - Techniques, procedures and methods
- Continuing education often lends itself well to online on-demand training opportunities that provide flexibility in training.

7.3 On the Job Training

- Makes use of guided experience as a training tool.
- Relies on training under the supervision of experienced and competent personnel.

- Allows organizations to provide targeted training focused on improving specific skill sets.

7.4 Certifications

- Certifications are one method to evaluate personnel and can be either general forensic process related or they can be tool specific.
- General forensic process certifications generally require training to be completed and a minimum amount of experience in the discipline. They also normally require successful completion of both written and practical examinations.
- Tool-based certifications also require training to be completed and are normally issued based on successful completion of course related practical exercises.
- Certifications may be beneficial when testifying in court.
- Certification retention usually requires re-testing and has specific continuing education requirements.

7.5 Testimony Training

Testimony training should address how DME is used in court and may include:

- Organization specific court testimony training
- Moot or mock court exercises
- Courtroom testimony monitoring
- Refer to *SWGDE Introduction to Testimony in Digital and Multimedia Forensics*
- Refer to *SWGDE Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings*

7.6 Training Documentation

Training documentation should include, at a minimum, the following:

- Training syllabus for each training event attended
- Documentation of trainee performance when available
- Documented recognition of successful completion of the training (i.e. certificates, emails, memorandums)
- Training documentation retention in accordance with organizational policy.

8. Categories of Training

Each of the job categories previously mentioned in section 5.7 above may include specific training requirements. Organizations should identify the training that is required by each of the job categories that exist within their organizational structure.

9. References

SWGDE Core Competencies for Training in Digital Forensics

SWGDE Training Guidelines for Video Analysis, Image Analysis, and Photography

SWGDE Core Competencies for Forensic Audio

"Technical Working Group for Education and Training in Digital Forensics" sponsored by National Institute of Justice (NIJ), July 2007

"Education and Training in Forensic Science: A Guide for Forensic Science Laboratories, Educational Institutions and Students" published by NIJ, June 2004

10. History

Revision	Issue Date	History
1.0	11/15/2004	Original Release
2.0	2/1/2010	Review of this document on 10/09/08 by the SWGDE Training Committee was conducted and the following was changed: · Re-format of document · Section 2.2 Job Categories combined: Management and Commander/Supervisor categories and added links to training goals. · Section 3.2.14.1 Computer Forensics: Removed the "History" bullet because this area is covered under the bullet "Scientific and Technical Foundation". · Section 3.2.14.2 Forensic Audio: Revised training guidelines to track with Audio Best Practice Document. Modified on 01/14/2009 by the SWGDE Training Committee was conducted and the following was changed: · Modified Section 3 for consistency · Added Certification and Higher Education in the Science to Section 4. · Added Section 5: Assessment and moved 2.1.1 Competency to this section. Added Proficiency · Added Section 6: References All changes approved by SWGDE and SWGIT on 01/15/10.
2.0	9/27/2014	Admin Change only – Updated document with new SWGDE/SWGIT disclaimer. No changes to content and no version/publication date change.
3.0 DRAFT	9/21/2023	Document updated, reformatted, and rewritten with substantive changes throughout. Moved forward for SWGDE membership vote to be released as a Draft for Public Comment.
3.0 DRAFT	10/15/2023	SWGDE voted to release as a Draft for Public Comment; formatted for release for public comment.
3.0	1/12/2024	No public comments received. Moved forward for SWGDE membership to vote to be released as a Final Approved document.
3.0	3/7/2024	Formatted for posting after SWGDE membership voted to release as a Final Publication.