



# Scientific Working Groups on Digital Evidence and Imaging Technology



## SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence

### **Disclaimer:**

As a condition to the use of this document and the information contained therein, the SWGDE/SWGIT request 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 any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE/SWGIT as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to: [secretary@swgde.us](mailto:secretary@swgde.us) and [SWGIT@yahoogroups.com](mailto:SWGIT@yahoogroups.com)

### **Redistribution Policy:**

SWGDE/SWGIT grant permission for redistribution and use of all publicly posted documents created by SWGDE/SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGDE/SWGIT cover page containing the disclaimer.
2. Neither the name of SWGDE/SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE/SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

# SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence

There are many topics to include in forensic digital and multimedia training. There are also many vehicles to provide training, such as in-service and out-service training and distance learning. The purpose of this document is to provide guidelines and recommendations to assist with designing a proper training program.

It should be recognized that some agencies might choose to provide training other than what is recommended in this section. In such circumstances, those agencies should demonstrate and document that the training selected is adequate to meet their anticipated needs.

## 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 process should be aware of the procedures commonly followed within the forensic community and should strive to meet or exceed these recommendations. They should also endeavor to maintain awareness of new 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 continuing education courses in digital and multimedia evidence technology.
- Maintain awareness of legal developments relating to digital and multimedia evidence.
- Maintain awareness of technological advancements.

## Definitions of Categories

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

- **Categories of training**
  - **Awareness:** Training designed to provide the student with a general knowledge of the major elements of digital and multimedia evidence including the capabilities and limitations of hardware and software
  - **Skills and techniques:** Training designed to provide the student with the ability to competently use specific tools and procedures
  - **Knowledge of processes and relationships:** Training designed to provide the student with an understanding of digital and multimedia evidence and when to apply that understanding given various situations
  - **Court procedures:**
    - **Witness testimony:** Training designed to provide the student with the ability to present reliable digital and multimedia evidence-based testimony in court
    - **Case preparation:** Training designed to provide the student with the ability to prepare accurate and reliable exhibits
  - **Continuing education:** Training designed to provide personnel with ongoing training in digital and multimedia evidence
  - **Specialized applications and technologies:** Training in specific subdisciplines or in specialized areas
  - **Competency:** A competency-testing program incorporates a number of components:
    - Required levels of skill and knowledge for a job category should be identified by the agency. These levels should be driven by the requirements of the specific tasks to be accomplished
    - Course(s) should be designed or identified by the agency or its agent to provide the skills and information necessary for the agency's personnel to attain competency in those skills

- If determined to be necessary by the agency, a competency test should be developed and administered to test these skills
  - Different types of competency tests may be developed depending on the various skills required
- **Job categories**
  - **Management:** Includes personnel who are responsible for setting agency policies and/or making budget decisions
  - **Command/Supervision:** Includes personnel who supervise and/or direct personnel engaged in the field of digital and multimedia evidence
  - **Examiner/Analyst:** Includes personnel for whom examination, analysis and/or recovery of digital and multimedia evidence is a major component of their routine duties. The personnel may also be responsible for the collection of digital and multimedia evidence.
  - **Technician:** Includes personnel whose primary responsibility is to collect and/or prepare digital and multimedia evidence for examination and analysis
  - **First Responder:** Includes personnel who are the first to secure, preserve and/or collect digital and multimedia evidence at the crime scene

### **Topical areas for focused training**

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

### **Managers, commanders/supervisors**

- Status of digital and multimedia evidence technology
  - Legal issues
  - Industry, market and user trends for new and emerging technologies

- Sources of digital and multimedia evidence used in criminal activity
- Current life cycle-cost comparisons and limitations of hardware and software
- Description of core technologies
  - Basic forensic science
  - Basic digital and multimedia evidence technology
    - Strengths and limitations in forensic processes
    - Strengths and limitations of digital and multimedia forensic tools (e.g. hardware and software)
- Quality Assurance and controls
- Personnel Management
  - Strengths and limitations of personnel capabilities
  - Competency and continuing education with respect to current digital and multimedia evidence technology
  - Psychological stress
  - Time management and staffing requirements
- Strategic alternatives
  - Contact procedure for technical support
  - References/information sources

### **Examiner/Analyst**

- Recognize the presence of other forms of physical evidence not related to digital and multimedia evidence such as fingerprints and/or other types of biological evidence
- Understand agency procedure for handling physical evidence
- General training

- Safety issues
- Maintain chain of custody and data integrity
- Ethics
- General forensic principles and practices
- Evidence handling (to preserve integrity of evidence)
- Court testimony skills
- Legal Issues as related to the profession
- Quality assurance (consistency within the forensic community)
- Basic crime scene management (understanding scene and evidence complexity)
- Technical writing and note taking skills
- “Best Practices” (i.e., technical procedures)
- SOP’s
- Demonstration of competency (written or practical exam)
- Position specific training relevant to the specific sub-discipline should include the following:

### **Computer Forensics**

- Scientific and technical foundations
  - Data interface technology
  - History
  - Operating system technologies
    - Operating system fundamentals
    - Installation, configuration, and upgrading

- Diagnosing and troubleshooting
- Core hardware objectives
  - Installation, configuration, and upgrading
  - Diagnosing and troubleshooting
  - PC preventive maintenance, safety, and environmental issues
  - Motherboard, processors, and memory
- Networking
  - Network topology
  - NOS types
  - Network security
  - Internet infrastructure and protocols
- Software
  - Applications
  - File identification
  - Operating systems
  - Malicious code recognition
- Storage
  - Logical
  - Physical
  - Partitioning
  - File systems
  - Media types
- Forensic analysis procedures

## **Forensic Audio**

- Scientific Foundations
  - Sound and Acoustics
  - Speech and Hearing
  - Frequency Fundamentals
  - Basic Digital Theory
  - Audio Engineering

- Electronics
- Technical Foundations
  - Principles of Audio Recording
  - Noise / Enhancement principles
  - Data / Signal Analysis
  - Reconstruction / Recovery
  - Playback optimization / Head alignment
- Equipment
  - Audio formats, standards, and file identification
  - Recording and playback devices
  - Microphones and speakers
  - Tools for duplication, conversion, processing and analysis
  - Media types
  - Calibration and maintenance
  - Software applications

## **Image Analysis**

- Scientific and Technical Foundations
  - Image Science and Technology
  - Optics
  - Photographic Theory (traditional and digital)
  - Image processing (traditional and digital)
  - Photogrammetry
  - Basic video theory
  - Data integrity and imaging artifacts
  - Compression artifacts
  - Specific domain knowledge for content analysis
  - Image comparison theory (ACE-V)
  - Statistics
- Equipment
  - Capture/Input/Output devices
  - Processing system (traditional and digital)
  - Digital storage devices and media
  - Image types and formats

➤ Software

- Applications
  - ▶ Analytical Software (i.e., Photogrammetry)
  - ▶ Processing and enhancement of images
  - ▶ Meta data determination
  - ▶ Documentation
- File Identification
- Diagnostic Software
- Calibration Software
- Restoration of corrupted files

## Video Analysis

➤ Scientific and Technical Foundations

- Theory and history of television
- Image processing (traditional and digital)
- Compression artifacts
- Basic computer theory and application to video processing
- Video signal standards
- Imaging Science to include optics and cameras
- Frequency Fundamentals
- Basic Digital Theory
- Basic Audio Principles
- Electronics
- Principles of Video Recording (analog and digital)
- Video Enhancement
- Video Editing
- Signal Analysis
- Video Media Reconstruction
- Video Data Recovery
- Playback optimization / Head alignment
- Analog and digital CCTV concepts

➤ Equipment

- Video formats, standards, and file identification
- Recording and playback devices
- Monitors and other output devices

- Tools for duplication, conversion, processing and analysis
- Basic media types
- Calibration and maintenance
- Video signal measuring devices

## **Technician**

- Safety and security issues
- 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
- Contact procedure for technical support (i.e., whom to call)
- Identification of digital and multimedia evidence
- Media types and remain current of new media formats technologies
- Evidence handling (to preserve integrity of evidence)
- Use of tools for media acquisition (hardware and software)
- Maintenance of the chain of custody
- SOP's
- Demonstration of competency (written or practical exam)
- Ethics and legal issues
- General forensic principles and practices
- Quality assurance (consistency within the forensic community)
- Documentation and note taking

## **First Responders**

- Safety and security issues
- 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

- Contact procedure for technical support (whom to call)
- Recognize the presence of digital and multimedia evidence at the crime scene
- Proper collection and preservation techniques
- Creation and maintenance of the chain of custody
- SOP's
- Demonstration of competency (written or practical exam)
- Ethics and legal issues
- General forensic principles and practices
- Documentation and note taking

### **Issues 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 providers and addressing continuing education and testimony training needs.

- **On the Job Training**

Experience is a critical training tool. Personnel who train under a competent practitioner gain valuable experience, as well as, knowledge and improved skills.

- **Continuing education**

Continuing education can be obtained from training conferences, trade shows, professional organizational memberships, professional and current literature, and specialized courses. This training should address updates and the use of new technologies as it relates to:

- Hardware and Equipment
- Software
- Techniques, procedures and methods

- **Testimony training**

This training should address the use of digital and multimedia evidence in court using techniques such as:

- Lecture-type presentation relevant to court testimony
- Moot court
- Court monitoring

- **Training documentation**

To demonstrate compliance with training, conduct the following:

- Develop a written training program
- Provide a training syllabus
- Document performance
- Establish a formal means of recognition of successful completion of the training such as a certificate, letter, or memorandum.

**History:**  
**SWGDE/SWGIT Guidelines and Recommendations for Training in  
Digital and Multimedia Evidence**

<b>Revision</b>	<b>Issue Date</b>	<b>Section</b>	<b>History</b>
1.0	11/15/04		Original Release
			Review of this document by the SWGDE Training Committee was conducted and no changes recommended. Version # will not be changed.