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.org and Chair@swgit.org

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.

Requests for Modification:

SWGDE/SWGIT encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded in writing to secretary@swgde.org and Chair@swgit.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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 change

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

Preface

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.

1.0 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.
- Implement a program for continual assessment of employees' skills.

2.0 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:

2.1 Categories of Training

2.1.1 **Awareness:** Training designed to provide the student with a general knowledge of the major elements of digital and multimedia evidence (i.e. video analysis, forensic audio, image analysis and computer forensics) including the capabilities and limitations of hardware and software.

2.1.2 **Skills and Techniques:** Training designed to provide the student with the ability to competently use specific tools and procedures.

2.1.3 **Knowledge of Processes:** Training designed to provide the student with an understanding of digital and multimedia evidence procedures and how to apply that understanding given various situations and sub-disciplines.

2.1.4 **Skills Development for Legal Proceedings:**

- **Witness Testimony:** Training designed to provide the student with the ability to present clear and non-technical digital and multimedia evidence-based testimony in court.
- **Forensic Results Preparation:** Training designed to provide the student with the ability to prepare accurate and reliable documentation and/or visual aids (i.e. notes, reports, printouts, audio recordings).

2.1.5 **Continuing Education:** Training designed to provide personnel with the ability to obtain the skills and knowledge of evolving technology in digital and multimedia evidence.

2.1.6 **Specialized Applications and Technologies:** Training in specific sub-disciplines or in specialized areas (i.e. cell phones, image comparison, audio authentication, video optimization).

2.2 **Job categories**

2.2.1 **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 digital and multimedia evidence. *(See Section 3.1 for training goals)*

2.2.2 **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. *(See Section 3.2 for training goals)*

2.2.3 **Technician:** Includes personnel whose primary responsibility is to collect and/or prepare digital and multimedia evidence for examination and analysis. *(See Section 3.3 for training goals)*

2.2.4 **First Responder:** Includes personnel who are the first to secure, preserve and/or collect digital and multimedia evidence at the crime scene. *(See Section 3.4 for training goals)*

3.0 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.

3.1 **Managers, Commanders/Supervisors**

3.1.1 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.

3.1.2 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).

3.1.3 Quality Assurance and Controls

3.1.4 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.

3.1.5 Strategic Alternatives

- Contact procedure for technical support.
- References/information sources.

3.2 Examiner/Analyst

All Examiners/Analysts should be able to 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. They must understand their agency procedure for handling physical evidence and receive the following general training:

3.2.1 Safety issues

- Blood borne pathogen training
- Electrical and fire safety
- Contaminants

3.2.2 Maintain data integrity

Preventing data modification is preferred but some changes may become necessary. All modifications to data should be technically and scientifically sound and thoroughly documented.

3.2.3 Ethics

3.2.4 General forensic principles and practices

3.2.5 Evidence handling and chain of custody.

3.2.6 Court testimony skills.

3.2.7 Legal issues as related to the profession.

3.2.8 Quality assurance (consistency within the forensic community).

3.2.9 Basic crime scene management (understanding scene and evidence complexity).

3.2.10 Technical writing and note taking skills.

3.2.11 "Best Practices" (i.e., technical procedures).

3.2.12 Standard Operating Procedures (SOP's).

3.2.13 Demonstration of competency (written or practical exam)

3.2.14 Discipline specific

Position specific training relevant to the specific sub-discipline should include the following:

3.2.14.1 Computer Forensics

- Scientific foundations
  - Fundamentals of binary and hexadecimal based numbers
  - Understanding of file structures
  - Fundamentals of computer programming
  - Fundamentals of data communications (parallel, serial, com, etc.)
  - Fundamentals of file systems

- Technical foundations
  - Data interface technology
  - Operating system fundamentals
  - Installation, configuration, and upgrading
  - Diagnosing and troubleshooting

- Equipment
  - PC preventive maintenance, safety, and environmental issues
  - Motherboard, processors, memory, etc.
  - Internal/external devices
  - Duplicators
  - Write blockers

- Networking
  - Network topology
  - Network operating systems
  - Network security
  - Internet infrastructure and protocols
  - Network specific hardware devices

- Software
  - Forensic and non-forensic applications
  - File identification
  - Operating systems
  - Malicious code recognition

- Storage
  - Logical
  - Physical
  - Media types
  - Networked
  - Remote (ex: wireless)

- Computer forensic analysis procedures

3.2.14.2 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
  - Forensic and non-forensic applications
  - File identification
  - Optimization

- Forensic Audio Analysis Procedures

3.2.14.3 Image Analysis

- Scientific Foundations
  - Image science and technology
  - Photographic theory (traditional and digital)
  - Basic video theory
  - Image comparison theory (ACE-V)

- Technical Foundations
  - Optics
  - Image processing (traditional and digital)
  - Photogrammetry
  - Data integrity and imaging artifacts
  - Compression artifacts
  - Specific domain knowledge for content analysis
  - Statistics
  - Image types and formats

- Equipment
  - Capture/input/output devices
  - Processing system (traditional and digital)
  - Digital storage devices and media

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

- Image Analysis Procedures

3.2.14.4 Video Analysis

- Scientific Foundations
  - Theory and history of television
  - Basic computer theory and application to video processing
  - Basic digital theory
  - Imaging science to include optics and cameras
  - Frequency fundamentals

- Technical Foundations
  - Image processing (traditional and digital)
  - Compression artifacts
  - Video signal standards
  - 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
  - Video formats, standards, and file identification

- Equipment
  - Recording and playback devices
  - Monitors and other output devices
  - Tools for duplication, conversion, processing and analysis
  - Media types
  - Calibration and maintenance
  - Video signal measuring devices

- Software Applications
  - File identification
  - Processing and enhancement of video/images
  - Metadata determination
  - Diagnostic
  - Calibration
  - Recovery of corrupted video files
  - Non-linear editing

- Video Analysis Procedures

3.3 **Technician**

3.3.1 Safety and security issues

3.3.2 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

3.3.3 Contact procedure for technical support (i.e., whom to call)

3.3.4 Identification of digital and multimedia evidence

3.3.5 Media types and remain current of new media formats technologies

3.3.6 Evidence handling (to preserve integrity of evidence)

3.3.7 Use of tools for media acquisition (hardware and software)

3.3.8 Maintenance of the chain of custody

3.3.9 SOP's

3.3.10 Demonstration of competency (written or practical exam)

3.3.11 Ethics and legal issues

3.3.12 General forensic principles and practices

3.3.13 Quality assurance (consistency within the forensic community)

3.3.14 Documentation and note taking

3.4 **First Responders**

3.4.1 Safety and security issues

3.4.2 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.

3.4.3 Contact procedure for technical support (whom to call)

3.4.4 Recognize the presence of digital and multimedia evidence at the crime scene

3.4.5 Proper collection and preservation techniques

3.4.6 Creation and maintenance of the chain of custody

3.4.7 SOP's

3.4.8 Demonstration of competency (written or practical exam)

3.4.9 Ethics and legal issues

3.4.10 General forensic principles and practices

3.4.11 Documentation and note taking

4.0 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.

4.1 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.

4.2 Continuing Education

Continuing education should be obtained annually from training conferences, trade shows, professional organizational memberships, professional publications, 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

4.3 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

4.4 Certifications

Certifications can be comprehensive or topic specific and can be an added tool in verifying technical skills and abilities. Certifications available through certifying bodies generally require training to be completed and a minimum amount of experience in the discipline. These certifications can be beneficial and should be pursued, if relevant. Certification attainment

requires testing. Certification retention may include retesting and specific continuing education requirements.

4.5 Higher Education

The possession and type of a degree may be dictated by the forensic discipline, the accreditation status of the agency, or the requirements of the agency.

4.6 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.

The retention of training documentation is left to the discretion of the agency.

5.0 Competency and Proficiency

Competency testing is designed to verify that an individual is able to conduct a specific task prior to its use in independent casework. Forensic community consensus should be leveraged to determine which skills are required for competency within each discipline.

Proficiency testing is the continual evaluation of agency personnel in the performance of tasks relating to their discipline.

5.1 Competency Testing

Competency testing can be conducted either at the end of training or in a modular format throughout the course of training. At any point that an examiner/analyst learns a new technique, process and/or software to perform their duties, one's competency in that area should be tested.

- Required levels of skill and knowledge for a job category should be identified by the agency. These levels should be driven by the requirements established in the forensic community for the specific tasks to be accomplished.
- A curriculum should be designed by the agency to provide the skills and information necessary for the agency's personnel to attain competency in those skills.

5.2 Proficiency Testing

The accumulation of successfully completed competency tests in all training milestones should demonstrate that one is proficient in a discipline. Annual discipline specific proficiency testing is a means to confirm that a trained examiner/analyst is qualified to continue performing their assigned duties and is recommended regardless of accreditation status.

- This should be documented and confirmed with annual proficiency testing in the relevant subject matter.
- Discipline and job specific topics should be included in proficiency tests.
- There should be a mechanism for remediation if proficiency is not demonstrated at any time.

6.0 References

"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

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

Revision	Issue Date	Section	History
1.0	11/15/04		Original Release
2.0	02/01/10		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.