SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence

Disclaimer:
As a condition to the use of this document and the information contained therein, the 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 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 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.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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 the SWGDE cover page containing the disclaimer.
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 create date) of the document and mention 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 forwarded to the Secretary in writing at secretary@swgde.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

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.

Table of Contents

1. Purpose

The purpose of this document is to describe the minimum requirements necessary to achieve quality assurance in regard to completing forensic examinations.

2. Scope

The document proposes minimum requirements regarding training/education, examiner certification, examination requirements and lab requirements. The intended audience includes examiners and laboratories in both small and large agencies and organizations.

3. Education / Training

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 commensurate with the minimum requirements put forth here.

The practitioner's knowledge must reflect what is required for the assigned task. The supporting education and training for this knowledge base should, at the minimum, be reflective of the following requirements.

3.1 Employment Qualifications

Qualifications for practitioners within the field of digital and multimedia evidence (DME) analysis are broad, based on organizational requirements and job description(s). The below qualifications are minimum requirements upon initial employment.

3.1.1 Personal characteristics

An individual must pass a criminal history and background check.

3.1.2 Education

Although a baccalaureate degree is preferred, at a minimum practitioners of digital and multimedia evidence must have a high school diploma or GED equivalent. Additionally, personnel must have requisite training and/or experience within the appropriate sub-discipline as follows:

1. Computer Forensics
    a. Hardware
    b. Networking
    c. Operating systems and file systems structure
    d. Related software
2. Audio Forensics
    a. Acoustic concepts
    b. Audio equipment (hardware/software)
    c. Audio recording, formats, and media
    d. Signal processing
3. Video Analysis
    a. Hardware
    b. Related software
    c. Linear/Non-linear editors
    d. Digital and Analog media
4. Image Analysis
    a. Hardware
    b. Related software

c. Mathematics (Photogrammetry)

Note – The following related prior experience may be used in lieu of educational requirements.

i. An individual mentored by a qualified professional in DME.
ii. Activity in a professional internship related to DME.
iii. One's completion of training certifications in related topics including software applications used within the discipline.
iv. Industry related experience.

3.2 DME Training in Areas Related to Duties

Upon assignment, an individual's knowledge, skills, and abilities shall be assessed to determine the level of training required to achieve competency. A documented training program within the organization's established standards must be provided. This training program should include written elements as well as practical assignments based on a training syllabus. Management of this process should be documented and overseen by a qualified professional in DME.

Minimum training requirements for DME consists of the following:

- Core competencies (see Certification (Sub-Discipline Specific)) within the respective discipline
- Standard Operating Procedures (SOP)
- Quality Assurance
- Legal and Ethics
- Courtroom procedures
- Competency and Proficiency Assessments

3.3 Apprenticeship

New examiners must demonstrate a working competence with a discipline-specific mentor.

3.4 Ongoing Training

A minimum of forty (40) hours of discipline-specific training that concludes in a competency test shall be completed annually. Discipline-specific continuing education opportunities shall be offered annually to strengthen an examiner's skill set.

3.5 Competency and Proficiency Assessments

One's proficiency within their discipline shall be assessed annually to ensure consistency and quality. If proficiency is not achieved, independent casework must cease until proficiency is demonstrated. Additionally, competency tests should be administered regarding new technologies.

3.6 Resources

1. ASTM "*Standard Guide for Education and Training in Digital Forensics"*
2. Training recommendations within the National Research Council Report to Congress "*Strengthening Forensic Science in the United States: A Path Forward*"
3. SWGDE/SWGIT "*Guidelines and Recommendations for Training in Digital and Multimedia Evidence*"
4. Core Competencies in Forensic Audio

4. Certification (Sub-Discipline Specific)

Certification of digital evidence practitioners in all sub disciplines in which they conduct casework is mandatory. Any digital evidence certification shall meet all of the following requirements:

1. The certification must focus on the theory of how digital evidence is created, stored, recovered and analyzed, and must not be based on specific software or tools.
2. The certification must be based upon a defined set of core competencies specific to digital forensics sub-disciplines. Core competencies shall at a minimum address:
    a. Pre-examination procedures and legal issues.
    b. Media assessment and analysis.
    c. Data recovery.
    d. Specific analysis of recovered data.
    e. Documentation and Reporting.
    f. Presentation of findings.
3. There must be recommended training courses and/or a specified number of training hours for the candidate to be eligible for entry level certification. In lieu of the training requirement, a certifying body may consider experience in the field as a suitable substitute. Certifying bodies may submit their certifying standards (core competencies, testing materials), which meet the above listed competencies, for review and acknowledgment of compliance by SWGDE.
4. The candidate must demonstrate an understanding of the core competencies for the particular digital forensic sub-discipline via a comprehensive written exam.
5. The candidate must demonstrate an understanding of the core competencies for the particular digital forensic sub-discipline via one or more practical examinations. The candidate performing the practical examination(s) must be required to follow SWGDE Best Practices where appropriate.
6. All candidates for certification must agree to adhere to a strict Code of Ethics in which the examiner agrees to approach each investigation in a fair and unbiased manner. Violations of the Code of Ethics by the forensic practitioner will result in disciplinary actions to include revocation of the certification by the certifying body.
7. The certification must require periodic recertification that contains:
    a. A practical examination adhering to the core principles;
    b. a recertification must occur at a minimum of every 5 years;
    c. documentation of continued relevant work experience;
    d. a minimum 40 hours of continuing education per year in the discipline; and
    e. an agreement to continue to follow a Code of Ethics.

5. Laboratory Standards

Digital Evidence Laboratories (DEL) must have and follow a written Quality Management System (QMS) that is documented in a Quality Manual (QM). The QMS defines and documents the organizational structure, responsibilities, procedures, processes, and resources for ensuring work product and methodologies are sound and free from error. The following subsections must be addressed in writing.

5.1 Personnel

Roles and responsibilities within the Digital Evidence Unit must be clearly defined. The following must be documented:

1. An organizational chart that shows the organization and management structure of the unit.
2. Defined relationships and responsibilities of management, technical operations, and support services personnel. Individual(s) responsible for monitoring compliance with the QMS must be designated.
3. Written job description for all personnel.
4. Minimum qualifications, training, and education requirements for all personnel.
5. A training program and qualifying procedure(s) for all technical personnel.
6. Minimum continuing professional development requirements for all technical personnel.
7. A written procedure whereby the testimony of each examiner is monitored at least annually. This monitoring can be accomplished by observation, review of transcripts, having a court officer complete an evaluation or telephonic solicitation by a supervisor. In the absence of court testimony during a calendar year, a memorandum must be prepared to document that fact.

5.2 Facility Design

The facility shall provide for adequate safety, security for personnel and operations, and access control. The facility must meet required health and safety standards. The facility must contain adequate space to perform required analytical functions and prevent alteration/damage to evidence. Facilities must be designed to ensure the proper safekeeping of evidence, data, and records to protect from loss, cross-transfer, contamination and/or deleterious change. The facility should be designed to mitigate electrostatic discharge, electrical and magnetic fields to ensure the integrity of the digital evidence.

5.3 Evidence Control

The organizational must maintain records of requests for analysis/service and of the respective items of evidence. A unique identifier must be assigned to each case file, item

of evidence, or record. This file or record must include a request for services and a chain of custody.

5.4 Validation

Validation testing must be applied to all tools, techniques and procedures utilized in the performance of digital forensics. If an organization incorporates another entity's testing results, then the organization must verify that the tool, technique, or procedure functions as expected within that organization's environment. Consideration may be given to the general acceptance of a tool, technique or procedure in its determination of whether validation is required.

5.5 Equipment Performance

Equipment must be maintained to ensure proper performance according to established organizational policy. Only suitable and properly operating equipment shall be employed.

The following documentation must be maintained, where applicable, for each piece of equipment:

1. Manufacturer's manuals
2. Calibration log
3. Performance verification log
4. Maintenance Log

5.6 Examination Procedures

The organization shall have and follow written examination procedures.
Work practices shall be established to prevent contamination of evidence during examination procedures. Written procedures must exist to address deviations from normal operating procedures.

5.7 Examination Review

A written policy must exist to define the organization's administrative and technical/peer review process. A minimum of twenty-percent of cases must be technical/peer reviewed and one-hundred percent of cases administratively reviewed.

5.8 Documentation and Reporting

All examination processes must be fully documented in case notes to allow for repeatability and all examinations must culminate in a report. All reports of examination must address at a minimum:

1. evidence examined,
2. examinations requested, and
3. results of examination.

5.9 Competency and Proficiency Testing

Examiners must successfully pass a comprehensive competency test before the performance of independent casework. Competency testing is the evaluation of a person's ability to perform work in any functional area. This is normally conducted upon completion of a training program.

Examiners must successfully pass an annual discipline-specific proficiency test. A proficiency test is used to evaluate practitioners, technical support personnel and the quality performance of an organization. The test must be realistically designed to reflect analytical concerns in forensic case work as closely as possible.

5.10 Audits

Audits of the QMS must be conducted annually. Records of each audit must be maintained and should include the scope, date of the audit, name of the person(s) conducting the audit, findings, and corrective action(s) taken, if necessary.

5.11 Deficiencies

The organization must have a written policy to address procedural, operational, and physical plant deficiencies. This must include the documentation of the deficiency and any corrective actions taken.

5.12 Health and Safety

All personnel must receive appropriate health and safety training, operate in accordance with organizational policy, and comply with any relevant statutory regulations. The organization must have a documented health and safety program in place to meet the needs of the unit and the manual(s) shall be readily available to all personnel.

5.13 Customer Complaints

The organization must have a policy in place to address customer complaints. The organization must document all customer complaints and their resolutions.

5.14 Document Control

The organization must have a policy on the approval and archiving of current and superseded policies and procedures. Documents must be reviewed annually during the quality audit. The organization must have a policy to ensure that superseded policies and procedures are not being used by practitioners.

5.15 Disclosure of Information

The organization must have a policy detailing how case related information is released.

6. Examination Requirements

6.1 Equipment Preparation

Hardware and software must be configured to prevent cross contamination. In reference to audio and video forensic examinations, system required controls shall be run through signal paths to confirm that they perform as expected.

6.2 Examination Request

All examinations must have a request. A request for forensic services will include:

1. The type of examinations requested and necessary legal authority. Attention should be paid to whether the request requires examinations by other disciplines.
2. Any known safety hazards (e.g., chemical, blood borne pathogens, etc.).
3. The identity of the party requesting the services and the date of the request.

Communicate with requestor to determine the focus and parameters of the examination.

6.3 Evidence Preservation

Digital Evidence submitted for examination must be maintained in such a way that the integrity of the data is preserved. Evidence must be handled in a manner preventing cross contamination. If other forensic processing will be conducted, consult with examiners in the appropriate disciplines.

6.4 Examination

Conduct examinations pursuant to the request and additional identified exams as necessary pending appropriate legal authority. At a minimum, an examination must consist of:

1. **Visual Inspection** – Determine the type of evidence, its condition and relevant information to conduct the examination.
2. **Forensic Duplication** – Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic duplicates or forensic image files.
3. **Media Examination** – Examination of the media should be completed in a logical and systematic manner.
4. **Evidence Return** – Exhibit(s) are returned to appropriate location.

6.5 Documentation

While documentation may vary, the following items must be included:

6.5.1 Request

The examination request must be included.

6.5.2 Chain of Custody

The chain of custody must include a description of the evidence and a documented history of each evidence transfer.

6.5.3 Notes

Notes stemming from the examination shall include at a minimum:

1. Examiner communications regarding the case.
2. Review of legal authority (if necessary)
3. Procedural steps of the examination (with date(s)) in sufficient detail to allow another forensic examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently.
4. If multiple examiners, initials of examiner performing procedural step.

6.5.4 Examination Report

The report is to provide the reader with all the relevant information in a clear and concise manner using standardized terminology. The examiner is responsible for reporting the results of the examination.

Reports issued by the examiner must address the requestor's needs and contain the following items:

1. Identity of the reporting organization.
2. Case identifier or submission number.
3. Identity of the submitter.
4. Date of receipt.
5. Date of report.
6. Descriptive list of items submitted for examination.
7. Identity and signature of the examiner.
8. Description of examination.
9. Results/conclusions/derived items.

History
SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence

Revision	Issue Date	Section	History
1	June 2010		Original Release for Public Comment
1	May 2010		Original Release as Approved
1			Updated document per current SWGDE Policy with: new disclaimer. No changes to content and no version/ publication date change. (9/27/2014)