Scientific Working Group on Digital Evidence

Core Competencies for Digital Forensics

12-F-006-2.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

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 email 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

Core Competencies for Digital Forensics

Table of Contents

1. Purpose

This document provides an outline of the knowledge, skills, and abilities practitioners of digital forensics should possess. The following elements provide a basis for training and testing programs. This basis is suitable for certification, competency, and proficiency testing.

2. Scope

This document identifies the core competencies necessary for identifying, handling, collecting, seizing, examining, acquiring, and analyzing digital evidence such as computer systems and mobile devices and their electronically stored information. This document applies to anyone involved in these tasks. For the purposes of this document, the term "examiner" refers to individuals who have specialized training, knowledge, skills, and abilities that allow them to handle a wide range of technical issues related to digital forensics, and who may be performing technical tasks to include collection, acquisition, analysis, and reporting.

Not all core competencies will be relevant to every practitioner's role in a forensic services organization. These organizations must determine which core competencies are within the scope of their organization and examiners. Lack of competence in one component may not invalidate overall competency.

There is a spectrum of capabilities within core competencies. It is not expected that an examiner has to be proficient in every capability to be considered competent. Examiners should exhibit competence pertinent to the examination being undertaken.

An examiner should apply all principles as defined in *SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*.

3. Limitations

This document is not all-inclusive, does not contain information relative to or in support of specific commercial products, and is not intended to be a training manual or to specify operating procedures.

4. General Considerations

Examiners engaging in digital forensics activities should be confirmed by their organization to meet criteria such as capabilities, education, training history, certification, competency assessment(s), and final authorization determined by the organization to carry out examinations.

5. Digital Forensics Core Competencies

A digital forensic examiner must be able to recognize circumstances beyond their expertise. If an examiner is dealing with technology outside their area of expertise, they should consult with an appropriate specialist. The categories of core competencies are as follows:

- Legal Considerations and Ethical Standards
- Preparation
- Search and Identification
- Collection, Seizure, and Preservation
- Data Acquisition
- Examination and Analysis
- Documentation
- Presentation and Testimony

5.1 Legal Considerations and Ethical Standards

- Sufficient training to understand and apply authorization to conduct a search and seizure of digital devices, (e.g., the ability to read a search warrant and determine scope including what places may be searched and what data may be seized)
- Awareness and understanding of applicable laws and policies relevant to handling digital evidence or computer-related crimes
- Understanding of search authority as it applies to seized devices and searching or analyzing data contained within seized devices
- Understanding jurisdictional differences, informed by local, state, and federal guidelines
- Adherence to ethical guidelines and professional standards to ensure impartiality, proportionality, confidentiality, and legal compliance in the collection, analysis, and reporting of digital evidence
- Balancing the need to review relevant evidence while minimizing intrusion into privacy

See *SWGDE Considerations for Required Minimization of Digital Evidence Seizure*.

5.2 Preparation

- Knowledge of how and when to use Personal Protective Equipment (PPE)
- Knowledge of what equipment could be needed for onsite exams (cables, drives, camera, software, etc.)
- Knowledge of organizational policies, procedures, and best practices
- Understanding the concepts of testing and validating forensic tools
- Ability to properly sanitize media and prepare a forensic workstation for use during forensic examinations

5.3 Search and Identification

- Ability to identify digital devices including computers, mobile devices, peripheral devices, storage media, input/output (I/O) interfaces, processing components, and other non-traditional media that may assist investigations
- Ability to recognize volatile data and the access-state of various devices (on/off/locked/unlocked) and respond according to best practices for data access and integrity
- Understanding of the functionalities of these devices and their dependencies

5.4 Collection, Seizure, and Preservation

- Understand the possible need to process media for other traditional forensic evidence prior to extracting its data (e.g., fingerprints/DNA/blood/trace evidence issues)
- Ability to establish and maintain chain of custody for seized items and follow established procedures for evidence handling
- Ability to practice general collection safety and determine the best method of collection to preserve maximum information relevant to the incident or case
- Ability to execute a planned collection process and maintain quality control in the evidence collection process
- Understanding of procedures for performing on-scene collections and acquisitions without contaminating the scene or collected evidence
- Ability to preserve a device in its most data recoverable state
- Ability to gather intelligence including interviewing individuals regarding digital evidence, and to successfully obtain passwords, hardware authentication keys, and encryption keys
- Awareness of digital evidence packaging, such as protecting evidence against environmental threats
- Understanding the differences between static and volatile data sources
- Understanding how to preserve volatile data sources
- Ability to recognize commonly utilized encryption methods
- Ability to maintain data integrity

For additional information, see *SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition*, and *Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices*.

5.5 Acquisition

- Understand the advantages and disadvantages of different types of acquisitions

- Understand the role of hashing in forensic examinations
- Ability to properly acquire and validate data from a variety of digital sources
- Ability to recognize and acquire data from various commonly utilized file system formats
- Ability to troubleshoot physical hardware to the extent required for acquisition and processing
- Understand the differences between feature phones, smartphones, and tablets
- Ability to identify mobile devices that contain removable media
- Ability to identify appropriate tool requirements for acquisition of data and devices and also conduct risk assessments for issues that may arise when using these tools

For additional information, *see SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition* and *Best Practices for Computer Forensic Acquisitions*.

5.6 Examination and Analysis

- Knowledge of how to verify data integrity
- Basic recognition and understanding of various operating systems
- Ability to evaluate what evidence could be recovered based on specific media
- Ability to determine the appropriate tool(s) for the forensic task being performed
- Ability to understand the concepts of reading and converting binary data
- Understanding of foundational forensic concepts including:
    - Basic computer architecture, data storage, and operating system concepts
    - Numbering systems relevant to computing, e.g., hexadecimal, binary
    - Types of physical storage media and their characteristics
    - Wiping/sterilization of media
    - Disk geometry/partitioning, volume management, sectors, clusters, fragmentation, slack
    - Processes such as partitioning, formatting, file writing, deletion, wiping
    - File systems, including metadata, timestamps, attributes, permissions
    - Compound files
    - Encoding/Decoding
    - File signatures
    - Carving
    - Parsing
    - Metadata
    - Keyword searching and search expressions
    - Encryption/Decryption
    - Common databases technologies

- Operating system artifacts
- Configuration and registry files
- User activity artifacts
- Log file analysis
- Networking
- Memory acquisition and analysis
- Cloud computing
- Virtualization and container technologies
- Use of hash algorithms

For additional information, see *SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition*, *Best Practices for Computer Forensic Acquisitions*, and *Best Practices for Computer Forensic Examinations*.

5.7 Documentation

- Ability to record contemporaneous notes while conducting the examination to ensure repeatability and reproducibility
- Ability to write report(s) containing all relevant information in a clear and concise manner to include unique identifiers of digital device(s)
- Ability to have general photography skills may be required to document physical condition, manual analysis, and evidence on site or on the target media

For additional information, see *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics.*

5.8 Presentation and Testimony

- Ability to develop demonstrative exhibits for legal proceedings
- Ability to present technical findings clearly and concisely to a non-technical audience

For additional information, see *SWGDE Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings and Introduction to Testimony in Digital and Multimedia Forensics.*

6. History

Revision	Issue Date	History
1.0	9/20/2012	Draft and release of document.
2.0 DRAFT	9/21/2023	Draft of document with major revisions. Release for public comment.
2.0 DRAFT	1/10/2024	Addressed public comments and minor editorial changes. Submitted for publication.
2.0 DRAFT	5/16/2024	Addressed public comments and major editorial changes based on those comments and comments within the Forensic committee.
2.0 DRAFT	7/3/2024	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.