Scientific Working Group on Digital Evidence

SWGDE Core Competencies for Digital Forensics

23-F-007-1.1

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

SWGDE Core Competencies for Digital Forensics

Table of Contents

1. Purpose 2
2. Scope 2
3. Limitations 2
4. General Considerations 2
5. Digital Forensics Core Competencies 3
   - 5.1 Preparation 3
   - 5.2 Search and Identification 3
   - 5.3 Collection, Seizure, and Preservation 3
   - 5.4 Acquisition 4
   - 5.5 Analysis/Examination 5
6. Additional Knowledge, Skills, and Abilities (KSAs) 5
   - 6.1 Tool Testing/Validation 5
   - 6.2 Technical Documentation 5
   - 6.3 Legal Considerations 5
   - 6.4 Presentation and Testimony 5

History 6

1. Purpose

This document provides an outline of the knowledge, skills, and abilities all 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 those identifying, handling, collecting, seizing, acquiring, and analyzing digital devices 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 collections, acquisitions, and/or analysis.

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, is not intended to be a training manual or to specify operating procedures, and the ideas, concepts, and technical aspects referenced are strictly related to what as available at the time this document was created and what were currently the most prominent considerations.

4. General Considerations

Persons engaging in digital forensics activities should be confirmed by their organization to meet the following criteria as appropriate:

- Capable
    - May need to pass a pre-assessment to determine suitability to participate in particular activities. May include signing an agreement to travel, be able to possess appropriate clearances, lift a minimum amount of weight, etc., to conduct tasks.
- Competent/Proficient/Qualified
    - May need to pass an initial test to determine if the current skill set is still adequate. These may include any combination of internally and externally administered tests and evaluations. Regular testing may be needed as well.
- Trained
    - May need to have specific education, training courses, or equivalent.
- Certified

- May be required to have industry standard specific certifications or equivalent and/or vendor specific training/certifications in applicable tools.

- Assigned/Appointed/Authorized
  - Regardless of the amount of expertise, training, background, and other qualifications, must also be assigned/appointed/authorized by organization to conduct digital forensic tasks.

5. Digital Forensics Core Competencies

A digital forensic examiner must be able to recognize situation circumstances beyond their expertise. If an examiner is dealing with technology outside their area of expertise, particularly in an active environment (such as on-scene) where an incident has taken place that is now part of an investigation, they should consult with an appropriate specialist. The basic groupings of core competencies are as follows:

- Preparation
- Search, Identification
- Collection, Seizure, and Preservation
- Data Acquisition
- Examination and Analysis
- Additional Knowledge, Skills, and Abilities (KSAs)

5.1 Preparation

- Knowledge of what Personal Protective Equipment (PPE) to use and when, as well as its appropriate application to the current task.
- Awareness and understanding of laws relevant to handling potential digital evidence and computer-related crimes.
- Knowledge of organizational policies, procedures, and best practices.

5.2 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 information that may assist investigation.
- 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 those devices and their dependencies.

5.3 Collection, Seizure, and Preservation

- Establishing and maintaining chain of custody for seized items and follow established procedures for evidence handling.
- Ability to practice general collection safety, determine the best method of collection to preserve maximum information relevant to the incident or case, execute the planned collection process, and maintain quality control in the evidence collection process.

- Ability to preserve a mobile device in a After First Unlock (AFU) state (device has been unlocked at least once after being powered on) isolate from networks and maintain power).
- Ability to gather intel including interviewing individuals regarding digital evidence, and to successfully obtain passwords, hardware authentication keys, and encryption recovery keys as required. Awareness of digital evidence packaging, protecting evidence against environmental threats, and information assurance.
- Have appropriate training in the preservation of data from digital devices.
- Have an understanding of the order of volatility for data on computers and mobile devices (RAM capture, etc).
- Have an understanding of exigency in preservation of volatile data types (encrypted browsers, etc).
- Understand and creating Chain of Custody.
- Maintain data integrity.

5.4 Acquisition

- Understand the different types of acquisitions (physical, file system and logical) and the pros and cons of each.
- Understanding of the order of volatility as applied to digital data and measures for preserving the integrity of data while minimizing alterations due to the acquisition processes.
- Understanding the applicability and use of hashing in forensic examinations.
- Ability to properly acquire data from a variety of devices, including but not limited to live computer systems, internal storage media, external storage media, and removable device media.
- Ability to recognize and acquire data from various commonly utilized file system formats.
- Ability to disassemble and perform basic troubleshooting to the extent required for acquisition and processing.
- Ability to recognize the presence of commonly utilized encryption methods.
- Ability to properly sanitize media and prepare a forensic workstation for use during forensic examinations.
- Understand the possible need to process a phone for other traditional forensic evidence prior to extracting its data – Fingerprints/DNA/Blood/Trace evidence issues.
- Understand the differences between feature phones and Smart Phones / Tablets (larger memory capacity, available features, applications, password protection and remote wiping).
- 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.

5.5 Analysis/Examination

- Knowledge of how to verify data integrity.
- Ability to evaluate evidence for selection of the appropriate tools and techniques needed for analysis.
- Ability to recognize, understand, and convert between common machine-readable data formats and human-readable data.
- Ability to recognize common forensic artifacts and recover unparsed forensic artifacts.
- Ability to understand and determine a file signature.
- Ability to understand various Operating Systems and inherent artifacts.

6. Additional Knowledge, Skills, and Abilities (KSAs)

6.1 Tool Testing/Validation

- Ability to validate and test tools utilized to conduct computer forensic examinations of digital media.

6.2 Technical Documentation

- Ability to record examination notes documenting handling and processing, as well as any other details required for an examiner with comparable training to explain or replicate results in accordance with best practices and standard operating procedures.
- The ability to document all unique identifiers of the digital devices and its associated parts is also required.
- Ability to write a report containing all relevant information in a clear and concise manner utilizing standardized technology.
- General photography skills may be required to help demonstrate the physical attributes of potential sources of digital evidence, capture some attributes or features of the particular item that may be relevant, or to assist others in understanding the acquired items.

6.3 Legal Considerations

- Sufficient legal training to understand and apply authorization to conduct the search and seizure of digital data, e.g. the ability to read a search warrant and determine scope (what places can be searched and what data can be seized, etc.).
- Understanding jurisdictions.

6.4 Presentation and Testimony

- Ability to present technical findings in a clear and concise manner.
- For additional information, see *SWGDE Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings and Introduction to Testimony in Digital and Multimedia Forensics.*

History

Revision	Issue Date	History
1.0	9/20/2023	Draft and release of document.
DRAFT 1.0	9/21/2023	Draft of document with major revisions. Release for public comment.
DRAFT 1.1	1/10/2024	Addressed public comments and minor editorial changes. Submitted for publication.
1.1	3/5/2024	SWGDE voted to approve as Final Approved Document. Formatted for release as a Final Approved Document.