SWGDE Core Competencies for Embedded Device Forensics

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 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 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.

SWGDE Core Competencies for Embedded Device Forensics

Table of Contents

1. Purpose

This document provides an outline of the knowledge and abilities examiners of embedded electronic device 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 the handling and forensic processing of embedded electronic devices, which can include, but is not limited to, devices categorized as the Internet of Things (IoT), magnetic card readers, and medical equipment. Refer to *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence* for general training requirements of forensic examiners.

3. Core Competencies

The embedded electronic devices forensic field is dynamic but shares some aspects with traditional computer forensics. An examiner should have a solid understanding of digital forensic analysis and remain current by reading trade journals, participating in professional organizations, continuing education, on the job training and hands-on experience.

An examiner must adhere to:

- All appropriate standard operating procedures and policies.
- A code of ethics including neutrality in the scientific processes.

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

3.1 Identification of Devices

3.1.1 Ability to identify an embedded electronic device to include basic functionality.

3.1.2 Ability to recognize physically damaged embedded electronic devices.

3.1.3 Ability to properly seize an embedded electronic device.

3.2 Electronics Knowledge

3.2.1 Knowledge of basic electronics concepts, theory, and troubleshooting.

3.2.2 Ability to identify common embedded electronic device components.

3.2.3 Knowledge of the function and operation of embedded electronic devices.

3.3 Disassembly and Repair

3.3.1 Ability to disassemble and repair electronic devices to the extent required for acquisition.

3.3.2 Ability to research and identify chips, e.g., manufacturer information, pinout, and architecture.

3.3.3 Ability to solder, desolder, and test connections.

3.3.4 Ability to remove a flash memory chip from a printed circuit board (PCB).

- Ability to identify flash memory and memory controller chips;
- Understand the differences in chip packages;
- Familiarity with rework stations and processes; and
- Understand the procedures for removing chips.

3.4 Acquiring Data

3.4.1 Ability to properly acquire data from an embedded device.

3.4.2 Ability to properly connect to a wireless module, e.g. Bluetooth, and acquire artifacts.

3.4.3 Ability to process physically damaged embedded electronic devices.

3.4.4 Ability to acquire data from a flash memory chip.

- Ability to reball or prepare chips to be read; and
- Understand the procedures for reading chips with a flash programmer.

3.4.5 Ability to connect to a printed circuit board

- Ability to conduct boundary scanning;
- Ability to identify test access points through probing;
- Ability to test circuits; and
- Ability to use an alternate power supply.

3.5 Data Processing

3.5.1 Ability to validate software tools used for automated processing in the examination of embedded devices.

3.5.2 Ability to examine a microcontroller to identify the format of stored data.

3.5.3 Ability to convert data acquired from an electronic embedded device to a readable format.

3.6 Documentation

3.6.1 Ability to record examination notes that document how exhibits were handled and what processes were performed with enough detail to allow a comparably trained examiner to explain the results or derive similar conclusions.

3.6.2 Ability to write a report containing all of the relevant information in a clear and concise manner using standardized terminology.

3.6.3 Ability to present technical data in a clear and concise manner.

SWGDE Core Competencies for Embedded Device Forensics
History

Revision	Issue Date	Section	History
1.0 DRAFT	2019-09-19	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	2019-09-29	--	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0	2020-09-17		Voted for release for final publication