SWGDE Core Competencies for Mobile Phone 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 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.

SWGDE Core Competencies for Mobile Phone Forensics

Table of Contents

1. Purpose **4**

2. Scope **4**

3. Core Competencies **4**

3.1 Core Competencies for First Responders (Level 1) 5
3.2 Core Competencies for First Responders (Level 2) 5
3.3 Core Competencies for Lab Personnel 6

SWGDE Core Competencies for Mobile Phone Forensics

1. Purpose

This document provides an outline of the knowledge and abilities all practitioners of mobile phone 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 mobile phones. It applies to both first responders and lab personnel. Different levels of cell phone analysis are discussed as well as the basic skills required at each of these levels. This document does not address core competencies for chip-off or micro-read analysis.

Refer to the "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence" for general training requirements of forensic practitioners.

3. Core Competencies

First Responders are defined as individuals that may be responsible for the collection and minimal examination of a mobile phone. There are two levels of First Responders. Level 1 First Responders are individuals that collect and/or manually examine mobile phones. Level 2 First Responders are individuals that utilize a tool or software to extract data from the mobile phone. The use of any tool to download/extract data from a mobile phone necessitates that proper training be completed by the individual using that tool.

The mobile phone forensics field continues to be dynamic and shares some aspects of traditional computer forensics. A practitioner should have an overall understanding of mobile forensics analysis and can remain current by reading trade journals, taking classes, participating in professional organizations, taking 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."

An examiner may be assigned casework that falls within one or more of the following levels and should therefore have the appropriate level of training to perform the examination.

Levels of analysis - The level of analysis is dependent on the request and the specifics of the investigation. Higher levels of analysis require a more comprehensive examination, additional

skills and may not be applicable or possible for every device or situation. The levels are as follows:

1. Manual – A process that involves the manual operation of the keypad and handset display to document data present in the mobile phone's internal memory.
2. Logical – A process that provides access to the user accessible files. This process will not generally provide access to deleted data.
3. Hex dump – A process that provides a physical acquisition of a mobile phone's data. This may provide access to deleted data that has not been overwritten.
4. Chip-Off – A process that involves the removal of a memory chip to conduct analysis.
5. MicroRead – A process that involves the use of a high-power microscope to provide a physical view of the electronic circuitry of memory. This would typically be used when acquiring data from physically damaged memory chips.

3.1 Core Competencies for First Responders (Level 1)

Competencies listed below outline the minimum requirements for a First Responder manually analyzing a mobile phone in the field without the use of an examination tool. *An example of a Level 1 First Responder would be a patrol officer/case agent who encounters a mobile phone during the course of an investigation.*

Three examples of manual examinations include: 1) browsing through a mobile phone's handset to view the data stored in the phone, 2) photographing or videotaping the data found on the screen or 3) manually transcribing the data viewed on the screen to a spreadsheet.

3.1.1 Understand proper evidence handling, labeling, preservation and seizure (e.g., obtain PIN or pattern lock codes prior to seizure).
3.1.2 Understand the possible damage that can be caused to mobile devices by fluids (bodily or other) and proper decontamination procedures.
3.1.3 Understand the consequences and risks associated with manipulating the mobile phone to be examined.
3.1.4 Understand that placing SIM or memory cards in different computers or mobile phones may modify data.
3.1.5 Understand that removal and replacement of a battery may cause the phone to restart.
3.1.6 Understand applicable legal authority and case law.
3.1.7 Understand the importance of proper documentation.
3.1.8 Understand the need to verify the data extracted from the mobile phone.
3.1.9 Understand the importance of creating a report of their findings.

3.2 Core Competencies for First Responders (Level 2)

Level-2 (Includes all Level 1 competencies plus the following):

Competencies listed below outline the minimum requirements for a First Responder that uses an examination tool to analyze a mobile phone. *An example of a Level 2 First Responder would be*

a properly trained patrol officer/case agent who uses software or a hardware device to download data from a mobile phone.

Examples of logical and file system examinations include using software or a hardware device to acquire user accessible data such as contacts, call history, text messages (SMS/MMS), pictures, video, audio, voicemail, e-mail, application data, Web history, device information, calendar, notes, etc., stored on the mobile phone.

3.2.1 Define important acronyms used to describe cell phone components and their functions.
3.2.2 Identify the following types of cell Phones: GSM, CDMA and iDEN.
3.2.3 Identify what information can be stored in a handset.
3.2.4 Identify what information can be stored on a SIM card.
3.2.5 Identify other locations where information can be stored.
3.2.6 Understand the legal issues associated with mobile phones (e.g., scope of warrant, consent, case law, licensing by state, and certification requirements)
3.2.7 Ability to isolate a cell phone from provider signal by powering off the phone, using RF shielding or disabling all radio communications.
3.2.8 Ability to explain the advantages and disadvantages of powering off the mobile phone.
3.2.9 Describe methods and tools for processing mobile phones.
3.2.10 Knowledge of tool functionality, their limitations and the possible need for additional examination (e.g., logical dumps of data may not retrieve deleted data from the handset, SIM card or memory cards).
3.2.11 Understand the need to perform tool testing, maintenance and validation.
3.2.12 Understand the "Best Practices for Mobile Phone Examinations."
3.2.13 Understand the difference between read vs. unread messages and how processing a mobile phone can alter them.
3.2.14 Understand the legal implications of opening unopened voicemail.
3.2.15 Understand that data from media cards may not be extracted using some software or hardware devices.
3.2.16 Ability to defend in court the use of utilized tools.

3.3 Core Competencies for Lab Personnel

Manual/Logical/Hex Dump analysis:

The competencies listed below outline the minimum requirements for an examiner performing analysis on mobile phones in a laboratory environment. This level of analysis is designed for the forensic examiners working in a forensic lab setting and includes all competencies identified in Levels 1 & 2 from the First Responders section above (Sections 3.1 & 3.2)

A Hex dump is the creation of a bit-by-bit copy of the internal memory in a mobile phone. The hex dump provides advantages over logical examinations by providing the examiner access to allocated and unallocated data stored on the mobile phone. Some limitations of the hex dump

are: 1) the difficulty to decode data due to closed file systems, 2) the length of time necessary for the analysis and 3) the need to use multiple tools to process the hex dump may be required.

Identity Card Processing

3.3.1 Knowledge of the various types of identity cards (e.g., SIM, USIM, CSIM, RUIM).
3.3.2 SIM Card Identification (IMSI vs. ICCID).
3.3.3 Knowledge of physical characteristics of various SIM card sizes (e.g., standard, mini, micro and nano).
3.3.4 Knowledge of using Cellular Network Isolation Card (CNIC) for network isolation.
3.3.5 Knowledge of the types and locations of data stored on SIM cards.
- 3.3.5.1 Service related information - ICCID, IMSI, MSISDN, SPN.
- 3.3.5.2 Phonebook and call information – abbreviated and last dialed numbers.
- 3.3.5.3 Messaging information – SMS, EMS.
- 3.3.5.4 Location information – LOCI, GPRSLOCI.

Handset Processing

3.3.6 Understand the possible need to process a phone for other traditional forensic evidence prior to extracting its data – Fingerprints/DNA/Blood/Trace evidence issues.
3.3.7 Understand the differences between feature phones and smart phones (larger memory capacity, available features, applications, password protection and remote wiping).
3.3.8 Ability to identify mobile phones that contain Dual/Tri SIM cards.
3.3.9 Understand the difference between physical and logical analysis and the types of data that can be located.
3.3.10 Understand the different connectivity options (Cable/Bluetooth/IrDA).
3.3.11 Understand the need to use a battery with a sufficient charge capable of completing the data extraction (battery charge 50% or higher).
3.3.12 Ability to power a device when manufacturer power cable is not present or not functioning (variable DC power supply).
3.3.13 Ability to differentiate between handset lock, PIN lock and PUK.

Memory Card Processing

3.3.14 Ability to image and process memory cards using computer forensic tools and best practices.
- a. Understand that processing memory cards while in a mobile phone may not provide deleted data from the memory card.
- b. Understand that processing a memory card while in the device may provide different results than processing it externally.

Damaged Mobile Phones

Mobile phones may be damaged when received in the lab for processing. The type of damage will determine the method to repair the phone for data extraction. Universal precautions should be observed when dealing with damaged phones.

3.3.15 Understand how to recognize and process phones that are physically damaged.
3.3.16 Understand the proper way to decontaminate a mobile phone damaged by fluids (e.g., water and bodily fluids).
3.3.17 Understand how to process a mobile phone that has a damaged screen.
3.3.18 Understand how to repair minor damage to mobile phone system boards.
3.3.19 Understand when a phone is unable to be processed based on the lab's capabilities and when to utilize a higher level of analysis.

Backup Data

Some phone data may not be accessible to the examiner without the use of the backup files. It is important the examiner know the type of backup files used by each Smartphone and where to locate those files on the computer synced to the mobile phone.

3.3.20 Blackberry Devices (.ipd backup files)
3.3.21 Android Based Devices (Gmail account username/password)
3.3.22 iOS Based Devices (iTunes backup files)

History
SWGDE Core Competencies for Mobile Phone Forensics

Rev	Issue Date	Section	History
1.0 Public Draft	06/05/2012	All	Original draft
1.0 Draft 2	01/17/2013	All	Additional comments and changes applied from SWGDE and external sources.
1.0 Approved	02/11/2013	All	Edit/format for publishing as Approved document.
1.0	--	--	Updated document per current SWGDE Policy with: new disclaimer, removed Definitions section, and corrected SWGDE hyperlinks. No changes to content and no version/publication date change. (9/27/2014)