Designation: E3046 – 15

Standard Guide for
Core Competencies for Mobile Phone Forensics[1]

This standard is issued under the fixed designation E3046; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide identifies the core competencies necessary for the handling and forensic processing of mobile cellular (cell) telephones (phones). It applies to both first responders and laboratory personnel.

1.2 Different levels of cell phone analysis are discussed as well as the basic skills required at each of these levels.

1.3 This guide does not address core competencies for chip-off or MicroRead extraction methods.

1.4 Refer to the Scientific Working Group on Digital Evidence (SWGDE) Guidelines and Recommendations for Training in Digital and Multimedia Evidence for general training requirements of forensic practitioners.

1.5 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *2.1 SWGDE Documents:*[2]

SWGDE Guidelines and Recommendations for Training in Digital and Multimedia Evidence

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

SWGDE's Best Practices for Mobile Phone Forensics

SWGDE Best Practices for Examining Mobile Phones Using JTAG

2.2 *NIST Documents:*[3]

NIST Special Publication 800-101 Revision 1—Guidelines on Mobile Device Forensics

3. Significance and Use

3.1 This guide provides an outline of the knowledge, skills, and abilities all practitioners of mobile phone forensics should possess. The core competencies provide a basis for training and testing programs. This basis is suitable for certification, competency, and proficiency testing.

4. Core Competencies Overview

4.1 First responders are defined as individuals that might 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 or manually examine mobile phones or both. Level 2 first responders are individuals that use a tool or software to extract data from the mobile phone. Laboratory personnel are defined as individuals that might be responsible for the collection and extensive examination of a mobile phone in a laboratory environment and their competencies are outlined in Section 7 below. 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.

4.2 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.

4.3 An examiner shall adhere to:

4.3.1 All appropriate standard operating procedures, and policies and

4.3.2 A code of ethics including neutrality in the scientific processes.

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

4.5 An examiner might 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.

4.6 The concept of levels of extraction for mobile devices is not new to the mobile forensics field, but, it is important that

[1] This guide is under the jurisdiction of ASTM Committee E30 on Forensic Sciences and is the direct responsibility of Subcommittee E30.12 on Digital and Multimedia Evidence.

Current edition approved Dec. 1, 2015. Published February 2016. DOI: 10.1520/E3046-15.

[2] Available from the Scientific Working Group on Digital Evidence (SWGDE), https://www.swgde.org.

[3] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

the reader have a basic understanding of this concept to best comprehend the technical aspects of this document.[4] The level of extraction technique used will be dependent on the request and the specifics of the investigation. Higher levels of analysis require a more comprehensive examination, additional skills, and might not be applicable nor possible for every device or situation. The levels are:

4.6.1 *Manual*—A process that involves the manual manipulation of the keypad and handset display to document data present in the mobile phone's internal memory.

4.6.2 *Logical*—A process that provides access to the user accessible files. This process will not generally provide access to deleted data. This includes file system extractions.

4.6.3 *Hex Dumping/Joint Test Action Group (JTAG)*—A process that provides the forensic examiner more direct access to the raw information stored in flash memory of a mobile phone's data. This might provide access to deleted data that has not been overwritten.

4.6.4 *Chip-Off*—A process that involves the direct reading and extraction of data as contained within a memory chip (generally requiring removal) to then conduct analysis on the data extracted. This includes In-System Programming (ISP).

4.6.5 *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.

5. Core Competencies for First Responders (Level 1)

5.1 The 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.

5.2 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 as viewed on the screen of a device.

5.3 The Level 1 first responder shall understand:

5.3.1 Proper evidence handling, labeling, preservation, and seizure (for example, obtain the personal identification number (PIN) or pattern lock codes before seizure);

5.3.2 Possible damage that can be caused to mobile devices by exposure to fluids (bodily or other) as well as the proper evidence preservation and decontamination procedures based on the substance(s) involved;

5.3.3 Consequences and risks associated with manipulating the mobile phone to be examined;

5.3.4 Placing a foreign subscriber identification module (SIM) or memory cards in different computers or mobile phones might modify data;

5.3.5 Removal and replacement of a battery might cause the phone to restart;

5.3.6 Applicable legal authority and case law;

5.3.7 Importance of proper documentation;

5.3.8 Need to verify the data as recorded from the mobile phone;

5.3.9 Importance of creating a report of their findings; and

5.3.10 Understand the possible need to prioritize processing a phone for other traditional forensic evidence (for example, fingerprints/deoxyribonucleic acid (DNA)/blood/trace evidence issues) as well for data extraction.

6. Core Competencies for First Responders (Level 2)

6.1 Level 2 includes all Level 1 competencies plus the following competencies. Examples of these types of examinations include: extraction and analysis of data call log information, multimedia data file carving and timeline creation of timestamp and other file system metadata.

6.2 The competencies listed in 6.3 give 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 a software or hardware device to conduct logical and file system examinations and download data (for example, contacts, call history, text messages (short message service/multimedia messaging service (SMS/MMS)), pictures, video, audio, voicemail, e-mail, application data, website history, device information, calendar, notes, etc.) from a mobile phone.

6.3 The Level 2 first responder shall:

6.3.1 Define important acronyms used to describe cell phone components and their functions;

6.3.2 Identify the following types of cell phones: global system for mobile communications (GSM), code division multiple access (CDMA), and integrated digital enhanced network (iDEN);

6.3.3 Identify what information can be stored in a handset;

6.3.4 Identify what information can be stored on a SIM card;

6.3.5 Identify other locations where information can be stored;

6.3.6 Understand the legal issues associated with mobile phones (for example, scope of warrant, consent, case law, licensing by state, opening unopened voicemail, and certification requirements);

6.3.7 Have the ability to isolate a cell phone from the provider signal by powering off the phone, using radiofrequency (RF) shielding, or disabling all radio communications;

6.3.8 Have the ability to explain the advantages and disadvantages of powering off the mobile phone;

6.3.9 Describe methods and tools for processing mobile phones as outlined in NIST Special Publication 800–101, Revision 1, Section 3.1;

6.3.10 Understanding the importance of the use of a compatible extraction cable and any required device driver and the implications of using incompatible cables or drivers for data extraction;

6.3.11 Have knowledge of tool functionality, their limitations, and the possible need for additional examination (for example, logical dumps of data may not retrieve deleted data from the handset, SIM card, or memory cards);

[4] Please see NIST Special Publication 800–101, Revision 1, Section 3.1, for additional information.

6.3.12 Understand the need to perform tool testing, maintenance, and validation;

6.3.13 Understand SWGDE's Best Practices for Mobile Phone Forensics;

6.3.14 Understand the difference between read versus unread messages and how processing a mobile phone can alter them;

6.3.15 Understand that data from media cards might not be extracted using some software or hardware devices; and

6.3.16 Have the ability to explain in court the use of utilized tools.

7. Core Competencies for Laboratory Personnel

7.1 The competencies listed in 7.2 – 7.6 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 laboratory setting and includes all competencies as previously identified in Levels 1 and 2.

7.2 *Universal Integrated Circuit Card (UICC)/Subscriber Identity Module (SIM) Processing*—Laboratory personnel shall have knowledge of:

7.2.1 Various types of identity cards (for example, SIM, universal subscriber identity module (USIM), CDMA subscriber identity module (CSIM), and removable user identity module (RUIM)).

7.2.2 UICC card identification (international mobile subscriber identity (IMSI) versus integrated circuit card identifier (ICCID));

7.2.3 Physical characteristics of various UICC card sizes (for example, standard, mini, micro, and nano);

7.2.4 Creation and correct use of a cellular network isolation card (CNIC) for network isolation;

7.2.5 Types and locations of data stored on UICC cards;

7.2.6 *Cellular Service Related Information*—ICCID, IMSI, and mobile station international subscriber directory number (MSISDN);

7.2.7 *Phonebook and Call Information*—Abbreviated and last dialed numbers;

7.2.8 *Messaging Information*—SMS and enhanced messaging service (EMS); and

7.2.9 Location information (LOCI) and general packet radio service location (GPRSLOCI).

7.3 *Handset Processing*—Laboratory personnel shall:

7.3.1 Understand the differences between feature phones and smartphones;[5] and

7.3.2 Have the ability to identify mobile phones that contain more than one SIM card.

7.4 *7.4 Manual/Logical/Hex Dump/Joint Test Action Group (JTAG) Extraction Techniques:*

7.4.1 Understand the difference between logical (Levels 1 and 2) and physical (Levels 3–5) analysis, the types of data that can be extracted at each level and how each tool's extraction method applies to that tool. Additional information on JTAG extraction best practices can be found in: SWGDE Best Practices for Examining Mobile Phones Using JTAG.

7.4.2 Understand: Chip-off, hex dumping/JTAG (Boundary Scan (that is, physical extractions)) result in the creation of a bit-by-bit copy of the internal memory in a mobile phone. The data extracted provides advantages over logical examinations by providing the examiner access to allocated and unallocated data stored on the mobile phone. Some limitations of the these methods include: (*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 data might be required.

7.4.3 Understand the different connectivity options (cable/Bluetooth[6]/infrared detection and array (IrDA)).

7.4.4 Understand the need to use a battery with a sufficient charge capable of completing the data extraction (battery charge 50 % or higher).

7.4.5 Have the ability to power a device when the manufacturer power cable is not present or not functioning (variable direct current (dc) power supply).

7.4.6 Have the ability to differentiate between various security features including, but not limited to: handset lock, PIN lock, and personal unlocking key (PUK).

7.5 *Memory Card Processing*—Laboratory personnel shall:

7.5.1 Have the ability to image and process memory cards using computer forensic tools and best practices,

7.5.2 Understand that processing memory cards while in a mobile phone might not provide deleted data from the memory card, and

7.5.3 Understand that processing a memory card while in the mobile phone might provide different results than processing it externally.

7.6 *Damaged Mobile Phones*—Mobile phones might be damaged when received in the laboratory for processing. The type of damage will determine the method to repair the phone for data extraction. The examiner should be able to understand:

7.6.1 How to recognize and process phones that are physically damaged,

7.6.2 Proper ways to decontaminate a mobile phone damaged by fluids (for example, water and bodily fluids),

7.6.3 How to process a mobile phone that has a damaged screen,

7.6.4 How to repair minor damage to mobile phone system boards, and

7.6.5 When a phone is unable to be processed based on the laboratory's capabilities and when to use a higher level of analysis.

7.7 *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. Understand the importance of, the type of and the possible location of backup files.

7.7.1 Blackberry[7] devices (.ipd backup files),

[5] See NIST Special Publication 800–101, Revision 1, Section 2.1.

[6] A trademark of Bluetooth SIG, Inc., Kirkland, WA.

[7] A trademark of BlackBerry Limited, Waterloo, Ontario, N2K0A7.

7.7.2 Android[8]-based devices (Google (Gmail)[9] account username/password), and

7.7.3 Internetwork operating system (iOS)-based devices (iTunes[10] backup files).

8. Keywords

8.1 first responder; forensic processing; mobile phone

[8] A trademark of Somasundaram Ramkumar, Madurai, Tamil Nadu, 625002.

[9] A trademark of Google Inc., Mountain View, CA, 94043.

[10] A trademark of Apple Inc., Cupertino, CA, 95014.

ASTM International takes no position respecting the validity of any patent rights asserted in connection with any item mentioned in this standard. Users of this standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard is subject to revision at any time by the responsible technical committee and must be reviewed every five years and if not revised, either reapproved or withdrawn. Your comments are invited either for revision of this standard or for additional standards and should be addressed to ASTM International Headquarters. Your comments will receive careful consideration at a meeting of the responsible technical committee, which you may attend. If you feel that your comments have not received a fair hearing you should make your views known to the ASTM Committee on Standards, at the address shown below.