Scientific Working Group on Digital Evidence

SWGDE Best Practices 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 Best Practices for Mobile Phone Forensics

Table of Contents

SWGDE Best Practices for Mobile Phone Forensics

1. Purpose

The purpose of this document is to describe the best practices for mobile phone forensics.

2. Scope

This document provides basic information on the logical and physical acquisition of mobile phones. The intended audience is either examiners in a lab setting or first responders who encounter mobile phones in the field.

These best practices should be followed if hardware or software is used to retrieve data from a phone. This document may not apply for those outside the lab setting whose only interaction with the phone is to manually look at the content of the phone.

This document is not to be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile phones or construed as legal advice.

3. Definitions

Mobile phone forensics is the utilization of scientific methodologies to recover data stored by a mobile phone for legal purposes.

4. Limitations

Mobile phones present a unique challenge to law enforcement due to rapid changes in technology. There are numerous models of mobile phones in use today. New families of mobile phones are typically manufactured every three (3) to six (6) months. Many of these phones use closed operating systems and proprietary interfaces making it difficult for the forensic extraction of digital evidence.

Some limitations encountered are as follows:

- **Incoming and Outgoing Signals** – Attempts should be made to block incoming and outgoing signals of a mobile phone. Common methods include Radio Frequency (RF) blocking container or jamming appliances. Blocking RF signals will drain the battery, may be expensive, are not always successful and may result in the alteration of mobile phone data.
- **Cables** – Data Cables are often unique to a particular phone. Frequently cables are specific to the forensic tool to be used. Data cables often have a wide variety of connections (e.g., RJ-45, USB, or RS-232). This results in a large number of cables being required for forensic analysis of mobile phones.
- **COM Ports** – Some tools may require the use of specific ports. Operating systems may not release control of ports after use.
- **Condition of the Evidence** – Commercially available tools may not provide solutions to deal with physically damaged mobile phones.

- **Destruction of Data** – There are methods to destroy data locally and remotely on a mobile phone.
- **Drivers** – Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with the tool or downloaded from a Web site. Drivers may compete for control for the same resource if more than one forensic product is loaded on the analysis machine.
- **Dynamic Nature of the Data** – Data on active (powered-on) mobile phones is constantly changing. There are no conventional write-blocking methods for mobile phones.
- **Encryption** – Data may be stored in an encrypted state preventing analysis.
- **Equipment** – Equipment used during examinations may not be the most recent version due to agency verification requirements of hardware, firmware and/or software.
- **Field analysis** – First responders should be aware of the risks associated with triaging mobile phones. Triaging mobile phones is not considered a full examination. The phone should be protected for further examination.
- **Hash Values** – Individual data objects (e.g., graphics, audio, and video files) will often maintain consistency between the forensic workstation and the hash value reported by the mobile phone application.[1] Due to the volatility of mobile phone operating systems, overall case file hashes of system files will typically not be consistent due to file system optimization.
- **Industry Standards** – Manufacturers and carriers lack standardized methods of storing data (e.g., closed operating systems and proprietary data connections).
- **Legal Issues** – Unopened emails, unread text messages, and incoming phone calls of seized phones may present non-consensual eavesdropping issues.
- **Loss of Power** – Many mobile phones may lose data or initiate additional security measures once discharged or shut down.
- **Passwords** – Authentication mechanisms can restrict access to a phone and/or data. Traditional password cracking methods can lead to permanent inaccessibility or destruction of data. There are different methods to protect a phone (e.g., Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset protection).
- **Removable Media Cards** – Processing these cards inside the phone poses risks (e.g., not obtaining all data including the deleted data, and altering date/time stamps).
  Identity Module e.g., SIM, USIM, CSIM, RUIM Cards – Lack of or removal of an identity module may prevent the examiner from accessing data stored on the internal memory of a handset. Inserting an identity module from another phone may cause the loss of data.
- **Training** – The individual copying data from a mobile phone should be trained to ensure the integrity of the data.

[1] Refer to NIST Publication: "*Hashing Techniques for Mobile Device Forensics*."

- **Unallocated Data / Deleted Data** – Many mobile phone forensic tools may only provide the logical acquisition[2] of data. Deleted data may only be recoverable from a physical acquisition[3].

5. Evidence Collection

General guidelines concerning the collection of evidence are provided as follows:

- Consult with the investigator to determine the necessary equipment to take to the scene.
- Review the legal authority to collect the evidence, ensuring any restrictions are noted. If necessary during the collection, obtain additional authority for evidence outside the original scope.
- All individuals not involved in the collection process should be removed from the proximity of the mobile phone to prevent modifications to the data.
- Solicit information from mobile phone user to determine the phone number, pass codes, pattern locks or PINs.
- If the phone is unable to be processed immediately, turn off phone, remove battery if practical, and do not turn it back on.
    - The benefits of turning off the phone include:
        - Preserving call logs and last cell tower location information (LOCI).
        - Preventing overwriting deleted data.
        - Preventing data destruction signals from reaching the mobile phone.
        - Preventing improper mobile phone handling (i.e., placing calls, sending messages, taking photos or deleting files).
    - The risks of turning off the mobile phone include possibly engaging authentication mechanisms (e.g., passwords, PINs, etc). Exigency may dictate that the mobile phone remains on for immediate processing. If the mobile phone must be left on, isolate it from its network while maintaining power.
        - Radio Frequency (RF) shielding – Mobile phones communicate with cell towers. Allowing this communication will change data on the phone.
        - Many mobile phones can be placed in "Airplane" mode limiting access to cell towers (e.g., 911 calls still available). This requires user input on the handset.
        - Disable Wi-Fi, Bluetooth, RFID and IrDA communications if practical
- Searchers should be able to recognize different types of mobile phone evidence.
- The scene should be searched systematically and thoroughly for evidence. Document the scene according to policy. Collect associated chargers, cables, peripherals, and manuals.

[2] Logical acquisition implies a copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).
[3] Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip)

5.1 Handling Evidence

- Evidence should be handled according to policy while maintaining a chain of custody.
- Network isolation of the mobile phone should be maintained.
- Additional forensic analysis – Occasionally, there may be a need to conduct traditional forensic processes on a mobile phone (e.g., DNA and latent prints). These are case dependent and should be discussed with the investigator about the need for such evidence as well as the order in which they should be performed. Contact appropriate lab personnel for guidance on processing order to avoid the destruction of forensic evidence.
- Biological contaminants and physical destruction provide unique challenges to the recovery of data. Universal precautions should be utilized to protect the health and safety of the examiner.

5.2 Equipment Preparation

"Equipment" in this section refers to the non-evidentiary hardware and software the examiner utilizes to conduct data extraction and analysis of the evidence.

- Equipment and software applications should be verified[4] to ensure proper performance.
- Current information (e.g., user's manual) describing the manufacturer's software/hardware and other relevant documentation should be recently reviewed and accessible.
- The site http://www.cftt.nist.gov/ provides NIST validation reports illustrating the capabilities and limitations of specific mobile phone tools.

5.3 Data Acquisition

Mobile Forensics Pyramid – The level of extraction and analysis required depends on the request and the specifics of the investigation. Higher levels require a more comprehensive examination, additional skills and may not be applicable or possible for every phone or situation. Each level of the Mobile Forensics Pyramid has its own corresponding skill set. The levels are:

1. **Manual** – A process that involves the manual operation of the keypad and handset display to document data present in the phone's internal memory.
2. **Logical** – A process that extracts a portion of the file system.
3. **File System** - A process that provides access to the file system.
4. **Physical (Non-Invasive)** – A process that provides physical acquisition of a phone's data without requiring opening the case of the phone.
5. **Physical (Invasive)** – A process that provides physical acquisition of a phone's data requiring disassembly of the phone providing access to the circuit board. (e.g., JTAG)

[4] The validation process is discussed in the document titled "*SWGDE Recommended Guidelines for Validation Testing*."

6. **Chip-Off** – A process that involves the removal and reading of a memory chip to conduct analysis.
7. **MicroRead** – A process that involves the use of a high-power microscope to provide a physical view of memory cells.

- The following technologies exist that examiners may encounter:
  - Global System for Mobile (GSM) phones
  - Code Division Multiple Access (CDMA) phones
  - Integrated Digital Enhanced Network (iDEN) phones
  - Satellite phones
  - Identity Module (e.g., SIM, USIM, CSIM, RUIM Cards)
  - Removable media cards

- Care should be taken to prevent cross-contamination of evidence between different phones.
- Document the physical condition of the mobile phone to be examined.
- The examiner should document the method used to acquire the data from the phone (e.g., manually acquired data, cable, IrDA, and Bluetooth).
- Various tools at multiple levels of analysis may be required to provide a holistic view of the data contained within the memory of the mobile phone, identity module, or associated storage media.
- The examiner should verify that the acquired data is an accurate depiction of the data on the phone.
- Levels 4 - 7 may require the use of traditional computer forensic tools to accomplish data carving or data correlation/analysis to display and save the data in a logical view.

5.3.1 Powered-on phones:

- The examiner should take precautions to isolate the mobile phone from its network.
- The examiner should ensure power is maintained to the mobile phone during the entire examination.
- Process the phone as received with the identity module and removable media card in the phone.
- Turn the phone off and follow the procedures for "Powered-off phones"

5.3.2 Powered-off phones:

- Obtain documentation (e.g., user manuals) for the phone to be examined.
- Remove and process identity module and removable media cards separately from the handset.
- Create a Cellular Network Isolation Card (CNIC) for installation into the phone.
- Ensure power is maintained to the mobile phone during the entire examination.
- Acquire the internal memory of the mobile phone.

5.4 Documentation

Documentation should meet the requirements of the organization's policies and should at least contain information on evidence handling, examination information and a report of findings.

- Evidence handling documentation should include but is not limited to:
  - Copy of legal authority.
  - Chain of custody.
  - Detailed description and/or photographs of the phone (e.g., phone number, make, and model).
  - Photographs or documentation of any visible damage.
  - Information regarding the packaging and condition of the phone.
- Examination documentation should be preserved according to policy and include:
  - Sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.
  - Tools and software used in the examination.
  - Documentation of any anomalies in the data acquisition (e.g., acquisition disruptions, faulty cables, and incoming data).
  - Substantive communication notes regarding the case,
- Report of findings:
  - Seek to address case specific requests from the investigator.
  - Identify the scope and/or purpose of the examination.
  - Provide a detailed description of the mobile phone examined (e.g., phone number, carrier, owner, make/model, and OS).
  - Supplement reports related to the examination.
  - Include examiner name and date of exam.
  - Provide the relevant information in a clear and concise manner.
  - Should be reviewed according to organizational policy.

5.5 Archive

Acquisition case files should be archived according to organizational policy and applicable laws.

- Mobile phone acquisitions may capture data using proprietary formats.
- Archiving the tool version used may be required.

6. Reference Sites and Publications

The below listed resources provide information that may prove helpful to the examiner:

- **NIST *SP800-101Guidelines on Cell Phone Forensics***
- www.search.org
- www.nw3c.org
- www.mobileforensicscentral.com
- **ACPO Guidelines**

- www.forensics.nl
- www.phonescoop.com
- www.ssddfj.org
- www.forensicfocus.com

History
Best Practices for Mobile Phone Forensics

Revision	Issue Date	Section	History
V1	5/21/09	All	Initial publication (Best Practices for Mobile Phone Examinations)
Draft V1.1	1/15/12	All	Reformat and update to document
Draft V1.2	6/4/12	All	Formatting – ready for public comment.
V2	9/13/12	All	Updated Publication and title change (Best Practices for Mobile Phone Forensics)
V2	01/13/13	All	Incorporate edits/comments received during public review.
V2	02/11/13	All	Edit/format for publishing as Approved.
V2	--	--	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)