SWGDE Best Practices for Handling Damaged Mobile Devices

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

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

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.

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 Handling Damaged Mobile Devices

Table of Contents

1. Purpose

The purpose of this document is to describe the best practices for handling damaged mobile devices (e.g., smart phones, tablets, and feature phones) when the data cannot be accessed via the guidelines provided in the document *SWGDE Best Practices for Mobile Phone Forensics* [1].

2. Scope

This document provides basic information on the handling of damaged mobile devices and the expectations of forensic data recovery examiners. The intended audience is first responders or individuals proficient in data acquisition Levels 3-4[1] and mobile device repair on failed or failing mobile devices (hereafter be referred to as an Advanced Mobile Forensics Examiner).

This document is not intended as a step-by-step guide for conducting data recovery for damaged mobile devices nor should it be construed as legal advice.

3. Definitions

(Note: These definitions will be added to the joint glossary as part of the Approved document publication process.)

- Desiccant – Substances that absorb moisture. Typical commercial desiccants include calcium oxide or silica gel; silica gel being the preferred substance for mobile device recovery operations as calcium oxide is caustic.
- JTAG extraction – Joint Test Access Group (JTAG): A data acquisition method (Level 3) involving connecting to Test Access Ports (TAPs) on a device then instructing the processor to transfer data to collection media.
- Chip-Off extraction (Level 4) – A data acquisition method requiring physical removal of chips from a device's Printed Circuit Board (PCB) then transferring the resident data to collection media.
- Feature Phone - A mobile device that primarily provides users with simple voice and text messaging services.

4. Limitations

This document discusses techniques currently in practice within the forensic community. Emerging technologies will be addressed in future revisions.

Those individuals performing the recovery procedures mentioned below require advanced training and a working knowledge of electrical engineering concepts, file system forensics, and reverse engineering. Performing mobile device acquisitions on a damaged device may cause evidentiary data to be altered or destroyed.

[1] The data acquisition levels used in this document refer to NIST's mobile device tool classification system [2].

It is recommended that an individual experienced with data recovery from mobile devices be consulted prior to performing any of the processes listed below. This information is intended to be used as a guideline and the procedures implemented will vary depending on a wide variety of circumstances.

5. Collection of Known Damaged Mobile Devices

General guidelines concerning the collection and handling of known damaged mobile devices are provided below. For all damaged devices, the following should be considered:

- Applying power may cause additional damage and the device should not be connected to a power source (battery or power adapter).
- Physical damage is not always indicative of device inoperability or the impossibility of data recovery. Some devices may show no visible sign of damage yet may be inoperable. This may be an indication of device or component failure; yet, the mobile device data may still be recoverable using techniques from Level 3 or 4 [2].
- The mobile forensic examiner should consult with the investigator to determine the details of the case and the need for advanced recovery processes. With any device being submitted for recovery service, the type of damage (if known) should be documented. This is imperative so once the mobile forensic examiner accepts the device, immediate actions are taken to mitigate possible further damage.
- The need to conduct additional forensic processes on mobile devices (e.g. DNA, latent prints, etc.) should be discussed prior to any cleaning efforts. Discussions with lab personnel will help determine the order in which those processes should be performed.

5.1 Liquid Damage

If a mobile device has been exposed to any liquids, the battery should be removed immediately (if possible) and/or the device powered off. Attempts to power on the device may result in additional damage.

If available, compressed air may be used to help dry the device. A hair drier should NOT be used to remove liquid from a damaged device. Any liquid damaged device should be thoroughly dried before packaging. Devices should remain in an unpowered state until thoroughly dried.

Handling of liquid damaged mobile devices:

- **Non-Corrosive Liquid** - The mobile device should NOT be packaged in the original substance. The battery should be removed. The device should then be thoroughly dried before being placed in an anti-static bag with desiccant gel packs. The device should be protected on all sides by sufficient packing material.
- **Corrosive Liquid –** Mobile devices known to have been submerged in salt or chlorinated water or other corrosive liquids should be dismantled to the best ability of the responder. Distilled or filtered water is commonly used as a neutralizing agent, because it has very low

conductivity, and should be used to flush salt and other contaminants from a device. Then the device should be immediately placed into a neutralizing agent to inhibit further corrosion (after the power source has been removed). When using neutralizers on corrosive liquids, adhere to proper safety procedures ensuring that the substance is safe for use on micro-electronics. It is important to match the correct neutralizer with the corrosive liquid; if you are unsure what neutralizer to use, an expert should be consulted.

- **Bodily Fluids –** Safety protocols should be employed when handling mobile devices that have been exposed to bodily fluids (e.g., blood, urine, etc.) to ensure pathogens are not transferred to the examiner. Preservation of other evidence (blood, fingerprints, etc.) should be considered before cleaning efforts begin. These fluids can be removed from the device with distilled water and followed by isopropyl alcohol[2].

Liquid damaged devices should be shipped immediately after drying and the mobile forensics examiner notified.

5.2 Blunt Force Impact

If an inoperable mobile device is suspected to have been subjected to blunt force impact, the device should be sent to an examiner trained in advanced repair techniques (e.g., PCB replacement, screen-replacement, etc.). When a device is submitted for repair, the cause and nature of the damage should be indicated.

When collecting a device that is in fragments, the collector should retrieve as many pieces as possible.

- It is particularly important to recover peripheral accessories such as cables and chargers.
- Documentation should be recovered to aid in further identification (i.e., make, model).

5.3 Thermal Damage

Mobile devices exposed to temperatures above the normal operating range (i.e., 5 to 130° F / -15 to 55° C) may sustain thermal damage. Superficial thermal damage is not necessarily indicative of internal damage. For example, in cases when a device is damaged by fire, the casing/chassis will frequently undergo severe cosmetic damage while the interior components are left undamaged.

In the event that water or chemicals were used to extinguish a mobile device, follow the guidelines as listed above in section 5.1.

[2] The isopropyl alcohol should have a purity rating of 99.8% or higher. Isopropyl alcohol is highly flammable and it should be completely evaporated before re-installing the battery or powering the device.

6. Qualifications

Minimum qualifications for forensic examiners conducting repair of damaged mobile devices include:

- Meeting the standards as outlined in *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence* [3].
- Experience and/or training that culminates in a competency in each of the following:
  - Advanced data extraction techniques applicable to the recovery of damaged mobile devices.
  - Soldering techniques applicable to PCB and associated circuitry.
  - Cleaning, repairing, and replacing of mobile device components.

7. Evidence Packaging /Transport

- Prior to shipping liquid-damaged mobile devices, compressed air (if available) should be utilized to remove as much liquid as possible, to mitigate the possibility of further damage, as specified in section 5 above.
- Damaged mobile devices should be packaged in an anti-static bag with desiccant and adequate padding.

8. Additional Guidance

Refer to *SWGDE Best Practices for Computer Forensics* for guidance on equipment preparation, acquisition, analysis, documentation, and reporting [4].

The examiner should conduct all examinations in accordance with *SWGDE Best Practices for Mobile Device Forensics* [1].

9. References

[1] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Mobile Phone Forensics". [Online]. https://www.swgde.org/documents/Current%20Documents

[2] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," *NIST Special Publication 800-101, Revision 1*, May 2014. [Online]. http://dx.doi.org/10.6028/NIST.SP.800-101r1

[3] Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology, "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence". [Online]. https://www.swgde.org/documents/Current%20Documents

[4] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Computer Forensics". [Online]. https://www.swgde.org/documents/Current%20Documents

SWGDE Best Practices for Handling Damaged Mobile Devices

History

Revision	Issue Date	Section	History
1.0	08/28/2014	All	Original working draft created. Voted for release as a Draft for Public Comment.
1.0	09/08/2014	All	Formatting/edit performed for release as a Draft for Public Comment.