SWGDE Best Practices for Collection of Damaged Mobile Devices

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 Collection of Damaged Mobile Devices

Table of Contents

1. Purpose 4
2. Scope 4
3. Limitations........ 4
4. Collection of Damaged Mobile Devices 4
  4.1 Liquid Damage........ 4
  4.2 Structural damage........ 5
  4.3 Thermal Damage 5
5. Evidence Packaging /Transport........ 5
6. Additional Guidance........ 6

1. Purpose

The purpose of this document is to describe the best practices for the collection of damaged mobile devices (e.g., smart phones, tablets, feature phones).

2. Scope

This document provides basic information on the handling of mobile devices damaged by liquid, structural damage, or thermal exposure. The intended audience is first responders and/or others involved in the collection of damaged mobile devices.

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.

This document does not address the forensic processing of recovered devices.

3. Limitations

This document discusses techniques currently in practice within the forensic community. Emerging technologies will be addressed in future revisions. At the time of the publication of this document, there is limited scientific research published on this topic.

This information is intended to be used as a guideline and the procedures implemented will vary depending on a wide variety of circumstances.

4. Collection of Damaged Mobile Devices

General guidelines concerning the collection and handling of damaged mobile devices are provided below. The following should be taken into consideration for damaged mobile devices:

- Applying power may cause additional damage and the device should not be connected to any power source (i.e., battery or power adapter).
- Physical damage is not always indicative of device inoperability or the impossibility of data recovery.
- The type of damage (if known) should always be documented and communicated to the examiner.
- The need to conduct additional forensic processes on mobile devices (e.g., DNA, latent prints) should be discussed prior to any cleaning efforts. Discussions with lab personnel will help determine the order in which those processes should be performed.

4.1 Liquid Damage

When collecting liquid damaged devices, a key objective is to get the device before a properly trained examiner as soon as possible. If a mobile device was *previously submerged* in liquid, the battery should be removed at the time of collection (if possible). Attempts to power on the device may result in additional damage.

If a mobile device was *previously submerged* in liquid and the battery is inaccessible, the device should be powered off. The collector should be aware that removing power from the device may result in an inability to access the data on the device due to encryption/authentication.

Devices *previously submerged*, but no longer in liquid, should be submitted to mobile forensics trained personnel for immediate processing.

Devices *discovered submerged* in liquid should be collected in a watertight container along with sufficient liquid to keep the device submerged. The device should then be immediately transported to the lab for processing. Devices found submerged in flammable, caustic, or bio-hazardous liquids require remediation on-scene before transporting to the lab.

Individuals collecting damaged devices should notify the lab of any known liquid damage or exposure at the time of laboratory submission.

Liquid damaged devices should be transported to the lab as soon as possible.

As soon as possible, the collector should attempt to obtain authentication information (e.g., passwords, swipe patterns) from the user of the device and provide it to the lab.

4.2 Structural damage

If an inoperable mobile device is suspected to have been subjected to some form of structural damage (e.g., dropped, cracked screens, broken into pieces), the device should be submitted to mobile forensics trained personnel for processing.

When a device is submitted for processing, 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.

- Recover peripheral accessories, such as cables and chargers.
- Recover available documentation to aid in further identification (e.g., make, model).

4.3 Thermal Damage

Mobile devices exposed to excessive heat may have sustained 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 or chassis will frequently undergo severe cosmetic damage possibly making the phone unrecognizable while the interior components are left undamaged. Such devices should be submitted for processing regardless of their external appearance.

In the event the mobile device was exposed to water or chemicals used to extinguish the fire, follow the guidelines as listed above in **Section 4.1 Liquid Damage**.

5. Evidence Packaging /Transport

Contact the lab for direction on preparing the device for transport or shipping.

Evidence should be handled according to policy, while maintaining a chain of custody.

Additional Forensic Analysis – Occasionally, there may be a need to conduct traditional forensic processes on a mobile device (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 the 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.

6. Additional Guidance

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

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

History

Revision	Issue Date	Section	History
1.0	08/28/2014	All	Original draft created, titled SWGDE Best Practices for Handling Damaged Hard Drives. Voted for release as a Draft for Public Comment.
1.0	09/23/2014	All	Formatting and technical edit performed for release as a Draft for Public Comment.
--	06/01/2015	All	Committee voted to remove the draft from public comment pending additional research and rewriting.
1.1	09/17/2015	Title; All	Committee revised the document and retitled it, SWGDE Best Practices for Collection of Damaged Mobile Devices. Voted by SWGDE to re-release as a new Draft for Public Comment.
1.1	09/29/2015	All	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.1	01/14/2016	N/A	Voted by SWGDE for release as an Approved Document.
1.1	02/08/2016	All	Formatting and technical edit performed for release as an Approved Document.