SWGDE Best Practices for Handling Damaged Hard Drives

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 Handling Damaged Hard Drives

Table of Contents

1. Purpose **4**

2. Scope **4**

3. Limitations **4**

4. Evidence Collection of Known Damaged Magnetic Media **4**

4.1 Water Damage 5
4.2 Dropped 5
4.3 Fire Damage 5
4.4 Unknown Drive Failure 5
4.5 Broken Pieces 6

5. Qualifications for a Technician Performing for Media Recovery **6**

6. Evidence Packaging /Transport **6**

7. Additional Guidance **6**

8. References **7**

1. Purpose

The purpose of this document is to describe the best practices for handling magnetic media hard drives when the data cannot be accessed via the guidelines provided in the *SWGDE Best Practices for Computer Forensics*.

2. Scope

This document provides basic information on the handling of damaged magnetic media and the expectations of the technician responsible for media recovery. The intended audience is examiners in a cleanroom lab setting and personnel who collect digital evidence in the field.

This document is not intended to be used as a step-by-step guide for conducting data recovery on magnetic media nor should it be construed as legal advice.

3. Limitations

This document does not cover all digital devices that may contain electronically stored information (e.g., solid-state drives, flash media, and optical media).

This document only discusses those devices currently available at the time of writing. Emerging technologies will be addressed in future revisions.

Hard drive data recovery techniques should only be conducted by properly trained personnel. Performing traditional computer forensic imaging techniques on a failed or failing hard drive may cause evidentiary data to be destroyed. Traditional computer forensic examiners should never open the drive chassis cover or attempt to disassemble the original evidence.

4. Evidence Collection of Known Damaged Magnetic Media

General guidelines concerning the collection and handling of known damaged magnetic media is provided below. For all damaged media consider the following:

- The technician responsible for media recovery should consult with the investigator to determine the details of the case and potential scenarios where recovery services are required. With any evidence being submitted for recovery service, include a cover sheet indicating the type of damage (if known). This is imperative so once the recovery examiner accepts the exhibit, immediate actions are taken to mitigate possible continuing damage.
- Occasionally, there may be a need to conduct traditional forensic processes on media, e.g. DNA, latent prints, etc. The processes are case dependent and should be discussed with the investigator to determine the need for such processing as well as the order in which the processes should be performed.

4.1 Water Damage

If a hard drive was recovered from water or other liquids, DO NOT attempt to power.

Shipping of water damaged media:

- If the drive is known to have been submerged for 24 hours or less at a depth of 2 feet or less, DO NOT package it in the original liquid. Package the drive in an anti-static bag with desiccant gel packs and ensure the drive is protected on all sides by at least 3 inches of padding.
- If the drive has been submerged for more than 24 hours and/or at a depth of greater than 2 feet, DO package the drive in the same liquid in which it was found (unless it was a bio-hazard or dangerous substance).
- Water damaged items need to be shipped to the recovery service immediately. Additionally, a notification should be made to the technician responsible for media recovery. If restrictions and/or regulations prevent shipping in the manner described above, contact the recovery examiner for other options.

4.2 Dropped

If a hard drive was dropped or known to have fallen, DO NOT power-on the drive. With any dropped evidence being submitted for recovery service, include a cover sheet indicating that the drive has been dropped and whether or not the drive was known to have been powered on at the time of the drop.

4.3 Fire Damage

If a hard drive was in a fire that was extinguished with water, package the drive in anti-static bag with silica gel packs and ensure the drive is protected on all sides by at least 3 inches of padding. Once the exhibit is packaged, ship as soon as possible and notify the technician responsible for media recovery.

If a hard drive was in a fire that was extinguished on its own and/or reached a temperature of 150° Fahrenheit or more then DO NOT power-on the drive.

4.4 Unknown Drive Failure

Certain circumstances may arise when a drive is collected into evidence and shows no physical signs of damage. However, once powered on, the drive starts clicking or makes a musical type tone. These are indications of drive failure and the drive should be immediately powered-off and sent to the technician responsible for media recovery.

If the drive fails to power-on, or there are burn marks on the PCB, then the drive should be sent to the technician responsible for media recovery.

4.5 Broken Pieces

If the hard drive has any pieces broken, attempt to recover as many pieces as possible and send all recovered pieces with the drive to the technician responsible for media recovery.

- It is especially important to recover any electronic components that belong to the PCB.
- Attempt to recover and keep intact any labels or other components with identification markings.

5. Qualifications for a Technician Performing for Media Recovery

The following are basic qualifications for a technician performing media recovery:

- Meets *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.
- A technician performing media recovery should have experience and/or training that culminate in a competency in all of the following areas:
    - Advanced imaging techniques applicable to the recovery of data hard drives with problematic sectors.
    - Advanced soldering techniques applicable to hard drive circuitry, e.g. Surface Mount Technology (SMT).
    - Cleaning, repairing, and replacing of hard drive internals to include the head stack assembly (HSA), the spindle motor, and the transplanting of platters.
    - Accessing, manipulating, and correcting hard drive firmware.
    - Disk imaging on failed or failing media and data reconstruction with accordance to the *SWGDE Best Practices for Computer Forensics*.

6. Evidence Packaging /Transport

- Magnetic media damaged from water, fire, and/or blunt force impact should be packaged in accordance to the recommendations outlined in Section 5 of this document.
- Refer to *SWGDE Best Practices for Computer Forensics*.
- External drives should be packaged with all components (power supply, PCB boards, special connectors, etc.).

7. Additional Guidance

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

8. References

The following SWGDE documents are referenced in this document:

- SWGDE Data Integrity within Computer Forensics
- SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence

Access the most current version of these documents at www.swgde.org.

SWGDE Best Practices for Handling Damaged Hard Drives

History

Revision	Issue Date	Section	History
1.0	01/16/2014	All	Original working draft created
1.0	02/06/2014	All	Formatting and technical edit.
1.0	06/06/2014	All	Voted for release as a Draft for Public Comment.
1.0	06/11/2014	All	Formatting and technical edit completed for release as a Draft for Public Comment.
1.0	08/28/2014	None	No changes made; voted to publish as an Approved document.
1.0	09/05/2014	All	Section 3 (Definitions) removed from document and added to Glossary. Formatting and technical edit performed for release as an Approved document.
N/A	N/A	All	Replaced the term, “Data Recovery Examiner,” with the description, “technician responsible for/performing media recovery,” throughout the document. No content changes. (01/15/2015)