Scientific Working Group on Digital Evidence

Best Practices for Handling Damaged Digital Storage Devices

14-F-002-2.0

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should 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; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

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 this SWGDE cover page containing the Disclaimer Regarding Use.
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 creation date) of the document and also indicate 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 submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE 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 suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, 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.

Scientific Working Group on Digital Evidence

Best Practices for Handling Damaged Digital Storage Devices

Table of Contents

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 17-F-002-2.0 Best Practices for Computer Forensic Acquisitions* [1].

2. Scope

This document provides basic information on the handling of damaged digital storage devices. While there are many digital devices that store data, this document is only addressing spinning disk hard drives (HDD), solid state drives (SSD), NVMe and NAND-based thumb drives or cards (SD, MicroSD, etc.), 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 digital media nor should it be construed as legal advice.

3. Limitations

This document only discusses those devices currently available at the time of writing and does not exhaustively cover all media types (e.g., optical media, magnetic tape, mobile devices). 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 unless they have been properly trained and in an approved environment.

4. Evidence Collection of Known Damaged Digital Media

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

- The technician responsible for damaged media recovery should consult with the investigator to determine the details of the case and potential scenarios where recovery services are required. When possible and allowed by an organization's documentation requirements, any evidence being submitted for recovery service should include a cover sheet indicating the type of damage (if known). The recovery technician can utilize that knowledge to take immediate actions to mitigate possible continuing damage. The cover sheet should also include what steps, if any, have been taken to recover the drive by the submitting agency or a commercial recovery service.
- Occasionally, there may be a need to conduct traditional forensic processes on media (e.g., DNA, latent prints). 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 Liquid Damage

If a hard drive was recovered from water or other liquids, **do not** attempt to power.

Shipping or transporting of liquid damaged media:

- If the drive is known to have been submerged in any non-flammable liquid, **do not** package it in the original liquid. Utilize a vacuum sealer to remove the air from the packaging containing the drive and seal. This process will draw the moisture from the drives chassis and limit the air in the package to reduce further oxidation. Ensure the drive is protected on all sides by at least three inches of padding.
- If the drive is known to have been submerged in any dangerous substance great care should be taken during packaging and additional safety requirements should be utilized to protect the packager and device from injury and damage from the volatile substance.
- Liquid 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 on the cover sheet (see Section 4) that the drive has been dropped and whether or not the drive was known to have been powered on after the drive had been dropped.

4.3 Fire Damage

Any spinning disks that are known to have been subjected to a fire or extreme heat should not be powered on even if the external chassis and printed circuit board (PCB) appears in pristine condition. Temperatures above 150° Fahrenheit can melt or deform internal plastics in the drive and cause catastrophic damage if the drive is powered. Solid state devices should also be inspected by a qualified technician before powering to ensure that soldered contacts were not melted or chips deformed.

If a hard drive was in a fire that was extinguished with water, package the drive in an anti-static bag and utilize a vacuum sealer to remove the air then seal the package and ensure the drive is protected on all sides by at least three inches of padding. Once the exhibit is packaged, ship as soon as possible and notify the technician responsible for media recovery.

4.4 Unknown Drive Failure

Certain circumstances may arise when a drive is collected into evidence and shows no physical signs of damage. An indication of drive failure is typically experienced when the drive is powered on and emits unanticipated audible sounds while also being non-addressable by host. The drive should then be immediately powered-off and sent to the technician responsible for damaged digital 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 damaged media recovery.

4.5 Broken Pieces

If a piece of media has any pieces broken, attempt to collect as many pieces as possible and send all pieces with the media to the technician responsible for damaged media recovery.

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

5. Qualifications for a Technician Performing Damaged Media Recovery

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

- Meets *SWGDE 10-Q-002-3.0 Guidelines & Recommendations for Training in Digital & Multimedia Evidence* [2].
- 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 media with problematic sectors.
    - Advanced soldering techniques applicable to circuits (e.g., Surface Mount Technology (SMT)).
    - Cleaning, repairing, and replacing of media components to include the head stack assembly (HSA), the spindle motor, and the transplanting of platters for HDDs.
    - Accessing, manipulating, and correcting digital media firmware.
    - Imaging on failed or failing media and data reconstruction with accordance to the *SWGDE 17-F-002-2.0 Best Practices for Computer Forensic Acquisition* [1].

6. Evidence Packaging /Transport

- Digital media damaged from water, fire, and/or blunt force impact should be handled and packaged in accordance with the recommendations outlined in Section 4 and Section 5 of this document.
- Refer to *SWGDE 17-F-002-2.0 Best Practices for Computer Forensic Acquisitions* [1].

- External drives should be packaged with all components (power supply, PCB boards, special connectors, etc.). Each item should be individually wrapped with at least 3" of padding used to separate the items from each other and the exterior of the packaging.

For additional guidance on equipment preparation, analysis, documentation, and reporting, refer to *SWGDE 17-F-002-2.0 Best Practices for Computer Forensic Acquisitions* [1].

7. References

[1] Scientific Working Group on Digital Evidence. *Best Practices for Computer Forensic Acquisitions*. SWGDE 17-F-002-2.0. *SWGDE*, 2017, https://www.swgde.org/17-f-002/.

[2] Scientific Working Group on Digital Evidence. *Guidelines & Recommendations for Training in Digital & Multimedia Evidence*. SWGDE 10-Q-002-3.0. *SWGDE*, 2010, https://www.swgde.org/10-q-002/

8. Additional Resources

- Scientific Working Group on Digital Evidence. *Data Integrity Within Computer Forensics*. SWGDE 06-F-001-1.0. *SWGDE*, 2006, https://www.swgde.org/06-f-001/.

9. History

Revision	Issue Date	History
1.0 DRAFT	1/16/2014	Initial draft created.
1.0 DRAFT	2/6/2014	Formatting and technical edits made.
1.0 DRAFT	6/6/2014	SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
1.0 DRAFT	8/28/2014	No changes made. SWGDE voted to approve as a Final Approved Document.
1.0	9/5/2014	Removed section 3 (Definitions) added to the Glossary. Formatted for release as a Final Approved Document.
1.0	1/15/2015	Replaced the term “Data Recovery Examiner” with the description, “technician responsible for/performing media recovery,” throughout the document. No content changes.
2.0 DRAFT	9/18/2024	Grammatical updates made throughout the document. Included updated storage devices (e.g., NVMe, SSD, NAND). Overall update in the process of shipping and packaging procedures. Changed name of document from “Best Practices for Handling Digital Hard Drives” to “Best Practices for Handling Damaged Digital Storage Devices” to reflect other digital storage devices rather than just hard drives. SWGDE voted to approve as a Draft for Public Comment.
2.0 DRAFT	11/6/2024	Formatted for release as a Draft for Public Comment.
2.0	2/21/2025	No comments received. SWGDE voted to approve as a Final Approved Document.
2.0	3/3/2025	Formatted for release as a Final Approved Document.