



# Scientific Working Group on Digital Evidence

---

## Best Practices for Data Destruction Media Sterilization and Sanitization

SWGDE F-24-001-1.0

**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.**

### 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](mailto: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](mailto:secretary@swgde.org). The following information is required as a part of any suggested modification:



# Scientific Working Group on Digital Evidence

---

- 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 Data Destruction Media Sterilization and Sanitization

### Table of Contents

1. Purpose.....	2
2. Scope.....	2
3. Limitations.....	2
4. Definitions.....	2
5. Considerations.....	4
6. Categories and Levels of Sanitization .....	4
6.1 Level 0 - Retention .....	5
6.2 Level 1 - Logical Deletion/Weak Erase .....	5
6.3 Level 2 - Quick Format.....	5
6.4 Level 3 - Obfuscation/Full Disk Encryption - Secure Erase/Cryptographic Erase	5
6.5 Level 4 - Low Level Format/Single Pass Wipe/Block Erase/Secure Erase.....	5
6.6 Level 5 - Multipass Wipe/Enhanced Secure Erase .....	5
6.7 Level 6 - Physical Destruction.....	5
7. Verification .....	6
8. Initialization, Dissemination, Recirculation, and Reuse of Devices .....	6
9. Additional Resources.....	6
10. History.....	7



# Scientific Working Group on Digital Evidence

---

## 1. Purpose

The purpose of this document is to provide essential information on data handling and best practices for data sterilization and sanitization in digital environments. This ensures that sensitive media remains within privileged hands, maintaining confidentiality.

## 2. Scope

This document does not cover every type of storage medium or every tool or method for data sterilization and sanitization. Instead, it focuses on those most commonly used, or recommended, in digital forensic applications. The intended audience is digital forensic examiners.

For the purposes of this document, the term “examiner” refers to any practitioner performing technical tasks related to digital forensic applications.

## 3. Limitations

New technologies are constantly emerging, which may include new types of storage mediums, interfaces, protocols, and standards for data handling and destruction. The ideas, concepts, and technical aspects discussed herein are strictly related to what is available at the time this document was created.

This document is not intended to be a training manual, nor to replace organizational policy or standard operating procedures, nor should it be construed as legal advice. This document is not intended to set forth specific operating procedures, nor is it all-inclusive and does not contain information relative to specific commercial products. Examiners dealing with technology, tools, or methodologies that are outside of their area of expertise, experience, and/or training should consult with an appropriate specialist.

## 4. Definitions

- **Sterilization:** The removal of all data from the media with verification.
- **Verification:** The process of confirming, through testing or inspection, that data sanitization has been successfully performed and the data is irrecoverable.
- **Format:** The process of preparing a hard disk and/or removable media for data storage. This is not a replacement for a forensic wipe.
- **Quick Format:** The deletion of files from the file system by removing the journal making the data inaccessible.
- **Low Level Format:** All files are completely deleted along with a scan for bad sectors. Additionally, the partition table is overwritten, and a new file system is written.
- **Media Sanitization:** The process of permanently wiping data from any media. This process renders access to data infeasible, either by making it unreadable or by destroying



# Scientific Working Group on Digital Evidence

it, thereby ensuring it is sufficiently unrecoverable as appropriate for the data type, sensitivity, media type, and established standards.

- **Target Data:** data that is selected by the user on any media source. This also may refer to specific data identified for sanitization.
- **Wiping:** a verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value.
- **Obfuscation:** The process of rendering data unreadable without physically removing it (such as through cryptographic erasure) by securely deleting encryption keys, making the data permanently inaccessible and indecipherable.
- **File Level Deletion: Also called weak Erase.** The logical deletion of files through the file system, typically by removing the file's name and location from the file system index and marking the sectors the file occupied as unallocated. This leaves the data intact and recoverable using basic forensic tools and is not adequate for secure sanitization.
- **Block Erase:** The complete replacement of target data with another set of known data, but at the drive logical level. This data is written to the storage medium from an external source and often consists of zeroes or ones or a similar repeating pattern. This may consist of any data that can be verified afterwards to ensure that the replacement is complete and successful.
- **Secure Erase:** A firmware-implemented method (as defined by ATA, SCSI, or NVMe standards) that overwrites all user-addressable storage locations, making data unrecoverable.
- **Enhanced Secure Erase:** A firmware-based method that securely overwrites all accessible and hidden areas, including sectors that have been remapped or reserved.
- **Physical Destruction:** the actual breaking and/or removal of the disks and/or chips to become indecipherable.
- **Full Disk Encryption-Secure Erase (FDE-SE):** A variant of Enhanced Secure Erase in which encrypted data is rendered inaccessible by securely deleting the cryptographic keys used to protect it before the data is overwritten.
- **Clear:** a logical technique to sanitize data in all user-addressable storage locations for protection against simple recovery techniques by rewriting with a new value or using a menu option to reset the device to the factory state.
- **Purge:** a physical or logical technique that renders Target Data recovery infeasible.
- **Destroy:** to render Target Data recovery infeasible, resulting in the inability to use the media for storage of data.



# Scientific Working Group on Digital Evidence

## 5. Considerations

The following considerations are not intended to be all-inclusive but should serve as a guide for circumstances where the examiner is considering whether or not to sanitize media and at what level that sanitization should occur.

- Origin of the device: depending on how the device will be used, a device that comes from an outside source, including devices removed from manufacturer's original packaging may need to be sanitized prior to use to confirm that no prior data will be present.
- Function of the device: a device that is being used to store a forensic clone should be sanitized to a higher standard than a device that is being used to store containerized files as there is less risk of evidence contamination. In cases where prior resident data may confound analysis, that prior resident data should be removed through the appropriate sanitization process.
- Access to the physical device: a device that will not leave the hands of the owner/examiner may not need the same level of sanitization as one that will be provided to an outside agency.
- Sensitivity of data: a device containing contraband data such as CSAM, PII, or privilege material should be handled with the utmost care and afforded the highest level of sanitization before the device is recirculated.
- Type of device: the type of device may determine if or how it should be sanitized such as in the case of solid-state media, write-only media, or volatile media. NAND or Flash memory or other forms of memory devices that use sophisticated memory control units may block off existing data from being overwritten. In these situations, where software is not available to address this data, physical destruction may be necessary depending on the sensitivity of the data resident on the device.

## 6. Categories and Levels of Sanitization

There are three standard categories of sanitization based on the methodology and the recoverability of data:

- Cleared: a device is considered cleared if it is overwritten.
- Purged: a device is considered purged if it is overwritten in a manner that prevents recovery by state-of-the-art laboratories or proficient adversaries, or if the device is made physically unrecoverable.
- Destroyed: a device is considered destroyed if it is physically destroyed in a manner that prevents any future data recovery or use.

For examples of how these tasks may be completed, refer to the charts in *NIST SP 800-88r2 Guidelines for Media Sanitation*.

Within this framework, levels of sanitization can help examiners assess if a sanitization method complies with the established standards.

### Best Practices for Data Destruction Media Sterilization and Sanitization

SWGDE F-24-001-1.0

Version: 1.1 (10/23/2025)

This document includes a cover page with the SWGDE disclaimer.



# Scientific Working Group on Digital Evidence

## 6.1 Level 0 - Retention

An examiner may retain data if it does not meet criteria to be sanitized or does not pose a threat if confidentiality is lost. This does not meet a standard of sanitization.

## 6.2 Level 1 - Logical Deletion/Weak Erase

Data that is logically deleted using an operating system's native deletion method may be considered sanitized if that data is of low enough sensitivity and/or the device will not be in the possession of an adversary who could recover or exploit that data. This does not meet a standard of sanitization.

## 6.3 Level 2 - Quick Format

Reinitializes the file system by removing metadata, leaving the actual data intact and recoverable. Removing a volume's pointers or journals to the location of sensitive data on that device may be considered sufficient sanitization if the device is not leaving the possession of the examiner or those who would otherwise have access to that level of confidentiality to that data. This does not meet a standard of sanitization.

## 6.4 Level 3 - Obfuscation/Full Disk Encryption - Secure Erase/Cryptographic Erase

Media containing data that is properly encrypted may be considered sanitized once the encryption keys are deleted if the data is of lower sensitivity and/or the device will not be in the possession of an adversary who could recover or exploit that data. This level would meet the standard of clearing data.

## 6.5 Level 4 - Low Level Format/Single Pass Wipe/Block Erase/Secure Erase

The overwrite of a volume's file table and a write of all zeros to the device is sufficient to consider most devices or volumes sanitized in all except the most sensitive of data. A write of pseudorandom data is not sufficient to be considered a single pass wipe. An examiner should write hexadecimal zeros to the device to facilitate verification of the sanitization, unless another reliable method can be used. This level would meet the standard of purging data. Additionally, it is important to note that this is generally a manufacturer-performed process that establishes the physical geometry of storage media (tracks, sectors, etc.) prior to shipping and use. It is distinct from any user-accessible formatting method.

## 6.6 Level 5 - Multipass Wipe/Enhanced Secure Erase

In cases where the data to be sanitized is of the highest sensitivity, or it is expected that a highly skilled adversary may attempt to obtain that data and the device cannot be destroyed, multiple passes should be employed, and efforts should be made to ensure that areas protected by a memory management unit are also sanitized. This level would meet the standard of purging data.

## 6.7 Level 6 - Physical Destruction

This is the most secure sanitization method since the data is physically destroyed through the use of physical methods such as degaussing, crushing, shredding, or incineration.



# Scientific Working Group on Digital Evidence

## 7. Verification

After sanitizing the media, verification of that wipe should be performed. Manually scrolling through a large data partition with the use of a hex editor and looking at the contents of the device does not properly satisfy this verification. An examiner may use a validated tool for this process or may verify the sanitization through the use of scripts.

## 8. Initialization, Dissemination, Recirculation, and Reuse of Devices

An agency may place more restrictive policies regarding the sanitization and confidentiality than the best practices outlined in this paper. An examiner required by their agency to perform more rigorous sanitization methods should defer to those policies.

It should not be assumed that any device entering an organization has arrived in sanitized condition. If a drive is intended for dissemination or may at any time be disseminated, it should be sanitized prior to use.

No device that previously contained sensitive data should be disseminated to anyone outside of the authorization of that confidential data without the device having been properly sanitized. In this case, devices should be sanitized to the highest level of the previously resident data before being written with the data to be disseminated.

Similarly, no device that previously contained sensitive data should be recirculated without sanitization in the assumption that anyone who receives that device may not have authorization to view data that was previously stored on that device. In this case, devices should be sanitized to the highest level applicable to the previously resident data before recirculation.

A drive may be reused by an examiner if it was sanitized at lower levels or not sanitized at all provided the examiner will maintain control of the device and/or that other considerations do not apply.

## 9. Additional Resources

- Hughes, Gordon, and Tom Coughlin. "Tutorial on Disk Drive Data Sanitization." *Coughlin Associates*, Sept. 2006, <https://tomcoughlin.com/Coughlin/Techpapers/DataSanitizeTutorial121206b.pdf>. Accessed 9 Oct. 2025.
- Chandramouli, Ramaswamy, Eric A. Hibbard. *Guidelines for Media Sanitation*. NIST SP 800-88r2. *NIST*, 2025, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf>. Accessed 9 Oct. 2025.
- Greer, Christopher, et al. *Cyber-Physical Systems and Internet of Things*. NIST.SP.1900-202. *NIST*, Mar. 2019, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf>.



# Scientific Working Group on Digital Evidence

- Scientific Working Group on Digital Evidence. *Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices*. SWGDE 22-F-001-1.0. SWGDE, 2022, <https://www.swgde.org/22-f-001/>.
- Scientific Working Group on Digital Evidence. *Best Practices for the Acquisition of Data from Novel Digital Devices*. SWGDE 16-F-003-1.0. SWGDE, 2017, <https://www.swgde.org/16-f-003/>.

## 10. History

Revision	Issue Date	History
1.0 DRAFT	1/12/2023	Initial draft created.
1.0 DRAFT	11/6/2024	SWGDE voted for release as a Draft for Public Comment; formatted for release for public comment.
1.0 DRAFT	9/18/2025	Addressed public comments and updated sections 4, 6.3, 6.5, and 6.7.
1.0 DRAFT	10/9/2025	Reference to <i>Guidelines for Media Sanitation</i> updated: NIST SP 800-88r1 (archived) replaced with NIST SP 800-88r2.
1.0 DRAFT	10/9/2025	Formatting and technical edit performed for re-release as a Draft for Public Comment.