Device-Aware Data Sanitization: An Empirical Evaluation of Overwriting Standards Across HDD, SATA SSD, and NVMe Media

Yashan Namal Priyadarshana
yashannp@gmail.com

Abstract

Widely used data sanitization standards, including the Gutmann 35-pass overwrite method, continue to be applied uniformly across storage media despite fundamental architectural differences between magnetic hard disk drives (HDDs) and NAND-flash-based solid-state drives (SSDs and NVMe devices). This study presents an empirical, device-aware evaluation of five sanitization methods simple deletion, operating-system formatting, NIST 800-88 (single-pass), DoD 5220.22-M (three-pass), and Gutmann (35-pass) applied across six physical storage devices (four HDDs, one SATA SSD, one NVMe SSD) using a standardized 44-file test set. Forensic recoverability was verified using Autopsy, Recuva, and Pandora Recovery, while S.M.A.R.T. telemetry was used to assess hardware impact before and after wiping. Results show that NIST single-pass overwriting already reduces HDD recoverability to 0%, a result reconfirmed by DoD three-pass overwriting, indicating that the additional 32 passes performed by the Gutmann method provide no measurable security benefit on modern HDD hardware. For SSD and NVMe devices, a standard OS format alone achieved 0% recoverability due to automatic TRIM invocation, while additional overwrite passes measurably increased NAND wear without improving security outcomes. These findings support a proportionate, device-aware sanitization strategy DoD three-pass for HDDs and OS-level formatting for SSD/NVMe media implemented in this study as a prototype framework, DataSanitix.

Keywords: *data sanitization; digital forensics; disk wiping; solid-state drives; NAND wear; S.M.A.R.T.; DoD 5220.22-M; Gutmann method; TRIM; data security*

I. Introduction

Improperly sanitized storage media continue to pose a demonstrated data security risk. Devices resold through second-hand electronics markets have been found to retain forensically recoverable personal data despite having been “deleted” or “formatted” by their previous owners, and documented incidents of sensitive data exposure from improperly disposed devices remain a recurring concern in both organisational and governmental contexts [1]. A persistent assumption underlying much of this risk is that all storage media respond identically to a given sanitization method an assumption this study directly tests.

Legacy multi-pass overwriting standards, most notably Peter Gutmann's 35-pass method, were originally designed in 1996 for the encoding schemes used by contemporaneous magnetic storage technology [2]. Modern HDDs use substantially different encoding, and modern SSD and NVMe devices do not use magnetic storage at all, relying instead on NAND flash cells with a finite Program/Erase (P/E) cycle lifespan. Despite this, the Gutmann method continues to be popularly regarded as a maximal-security standard applicable across device types. This study empirically tests that assumption using controlled, device-specific experiments across both HDD and flash-based media.

II. Related Work

Gutmann's original work [2] proposed multiple overwrite passes to counter magnetic force microscopy-based data recovery on the drive encoding schemes prevalent at the time, but Gutmann himself later noted

that these techniques are largely inapplicable to modern drive technology. Wright, Kleiman, and Sundhar [3] provided one of the first empirical challenges to multi-pass overwriting, demonstrating that a single overwrite pass was sufficient to prevent data recovery on modern HDDs using standard forensic tools, a finding this study independently reconfirms with a broader device sample. Garfinkel and Shelat [1] examined disk sanitization practices in used and resold drives and found that inadequate sanitization was widespread in real-world secondary markets, motivating the practical framing adopted in this study. NIST Special Publication 800-88 Revision 1 [4] formally recommends single-pass overwriting ("Clear") as sufficient for most magnetic media and recommends cryptographic erase or vendor-specific commands for flash-based media, a device-differentiated position that this study provides direct experimental support for, and this position is echoed in the international storage security guidance of ISO/IEC 27040 [6]. Existing literature, however, offers limited controlled, cross-device empirical comparison of legacy multi-pass standards against modern NIST and DoD [5] guidance on the same physical hardware — the gap this study addresses.

III. Methodology

Six physical storage devices were tested under controlled conditions: four HDDs (WDC WD5000AAKX-75U6AA0, Hitachi HTE543232A7A384, HITACHI HTS543232A7A384, and Seagate ST500LM012 HN-M500MBB), one SATA SSD (Samsung MZ7LN256HCHP-000L7), and one NVMe SSD (WDS250G3X0C-00SJG0). Devices with substantial prior usage histories (ranging from approximately 5,800 to over 58,000 power-on hours) were deliberately selected to reflect realistic secondary-market and enterprise disposal conditions rather than idealized new hardware.

A standardized test set of 44 files (99.7 MB) was written to a 2GB test partition on each device prior to each sanitization run. Five conditions were evaluated per device where applicable: simple file deletion, standard operating-system quick format, NIST 800-88 Clear (single-pass overwrite), DoD 5220.22-M (three-pass overwrite), and the Gutmann method (35-pass overwrite). Forensic recoverability following each condition was assessed using Autopsy [7], Recuva, and Pandora Recovery. S.M.A.R.T. telemetry (including temperature, reallocated sector count, and, for SSD/NVMe devices, wear-levelling and Percentage-Used/Life-Left attributes) was recorded immediately before and after each experimental cycle using CrystalDiskInfo and DiskGenius.

Gutmann 35-pass completion was not independently re-verified for every device. Given that DoD three-pass overwriting had already produced 0% forensic recoverability, and considering the substantially longer runtime the full 35-pass method requires at scale, Gutmann outcomes for most devices are reported as inferred rather than independently forensically re-scanned; this decision is disclosed here for methodological transparency and is itself consistent with this study's central finding, discussed in Section V.

IV. Results

A. HDD Recoverability

Table I summaries forensic recovery rates across the four HDD devices. Simple deletion left 100% of test data recoverable in every case, as only file-system metadata is affected. Standard formatting produced inconsistent results across devices (77–100% recovery), depending on file-system conversion behaviour,

and therefore cannot be relied upon as a sanitization method for magnetic media. Both NIST single-pass and DoD three-pass overwriting achieved 0% recoverability across every HDD tested.

HDD Device	Simple Delete	Windows Format	NIST / DoD	Gutmann
WDC WD5000AAKX-75U6AA0	100%	77%	0%	0%
Hitachi HTE543232A7A384	100%	100%	0%	0%
HITACHI HTS543232A7A384	100%	n/a*	0%	0%*
ST500LM012 HN-M500MBB	100%	n/a*	0%	0%*

*TABLE I. HDD Recovery Rate by Sanitization Method (*Gutmann testing deemed redundant for HDD media following confirmed 0% recovery at 3-pass; see Section III.)*

B. SSD and NVMe Recoverability

Table II summarizes results for the SATA SSD and NVMe devices. In both cases, a standard OS-level format without any multi-pass overwriting was sufficient to reduce forensic recoverability to 0%. This outcome is attributable to automatic TRIM command invocation during formatting [9], which instructs the flash controller to invalidate previously mapped data pages independently of any overwrite operation.

SSD / NVMe Device	Simple Delete	OS Format (TRIM)	DoD 3-Pass
Samsung MZ7LN256HCHP (SATA)	100%	0%	0%
WDS250G3X0C-00SJG0 (NVMe)	100%	0%	0%

TABLE II. SSD / NVMe Recovery Rate by Sanitization Method

C. Wiping Duration and Hardware Impact

Table III summarizes average wiping durations across device classes for a 2GB test partition. HDD devices required substantially longer durations for multi-pass methods (1.97–2.30 minutes for DoD three-pass) than SSD or NVMe devices (0.75 minutes), reflecting the higher sequential write throughput of flash-based interfaces. S.M.A.R.T. telemetry showed minimal change on HDD devices across the full experimental cycle. On the SATA SSD, the wear-levelling and Percentage-Used attributes showed a measurable increase following repeated multi-pass overwrite cycles, directly evidencing NAND wear accumulation. The NVMe device recorded a modest temperature increase (43–45°C) during sustained wiping, remaining well within the manufacturer's safe operating threshold (85°C critical limit).

Device Class	NIST (1-pass)	DoD (3-pass)	Gutmann (35-pass)
HDD (avg., 2GB partition)	0.34–0.38 min	1.97–2.30 min	2.29–2.45 min†
SATA SSD (2GB partition)	—	0.75 min	0.77–1.5 min†
NVMe SSD (2GB partition)	—	0.75 min	0.85 min†

TABLE III. Average Wiping Duration by Device Class and Method († Gutmann durations for most devices are tool-projected or inferred rather than independently timed to completion; see Section III.)

V. Discussion

The central finding of this study is that, once forensic recoverability has been reduced to 0% a threshold this study found HDD media reach after a single NIST-standard overwrite pass, and flash media reach after

a standard TRIM-invoking format there is no residual data for additional overwrite passes to act upon. Continued overwriting beyond this point does not provide additional data security; it instead consumes finite hardware resources for no corresponding benefit. On HDDs, this manifests as unnecessary mechanical cycling. On SSD and NVMe media, it is more consequential: NAND flash cells are governed by a finite Program/Erase cycle lifespan (measured in Terabytes Written, TBW) [8], and every additional overwrite pass performed after data is already unrecoverable directly consumes a portion of that finite endurance.

This effect scales with deployment size. For an individual device, the additional wear, thermal stress, and time cost of legacy multi-pass methods are modest. At enterprise or data-center scale, where sanitization may be performed across thousands of devices, the cumulative cost in electricity consumption, processing time, hardware wear, and reduced device resale or reuse value becomes substantial. This is not an argument against sanitization the risks of leaving data unwiped are well documented and are not in dispute but an argument for proportionate, device-aware sanitization: this study found that a DoD three-pass wipe, completed in approximately two minutes per 2GB partition on HDD media, achieved the same 0% recoverability outcome as the 35-pass Gutmann method, without its additional wear, thermal stress, time cost, and energy expenditure.

Given the limited device sample (n = 4–6 per device class), inferential statistical testing was considered but is not presented as the primary basis for these conclusions. A supplementary Wilcoxon signed-rank comparison of recovery counts between simple deletion and DoD three-pass overwriting across the tested HDDs approached but did not reach conventional statistical significance ($p \approx 0.06$), consistent with the small sample size rather than a weak underlying effect DoD achieved deterministic 0% recovery in every tested case. This deterministic, consistent outcome across all tested devices is treated here as the primary evidence for the study's conclusions.

VI. Limitations and Future Work

This study's device sample, while broader than a single-device pilot, remains limited to six physical units and cannot fully capture variation across all manufacturers, models, and capacities in current use. Testing was conducted on 2GB partitions rather than full device capacity; wiping durations reported here should be understood as indicative rather than directly representative of full-disk sanitization timescales, which would scale considerably at full capacity. This research was limited to software-based sanitization methods; physical destruction techniques such as degaussing and shredding were outside its scope, as were hardware-level encryption-based erasure methods (e.g., Instant Secure Erase on self-encrypting drives), which represent a promising direction for future SSD-specific research. Future work should also examine the effectiveness of emerging AI-assisted forensic recovery techniques against the sanitization methods evaluated here, and should evaluate the proposed device-aware framework at enterprise scale.

VII. Conclusion

This study provides controlled, empirical evidence that legacy multi-pass overwriting standards, exemplified by the Gutmann 35-pass method, offer no measurable security advantage over NIST single-pass or DoD three-pass overwriting on modern HDD media, while measurably degrading SSD and NVMe device health when unnecessarily applied. A device-aware sanitization strategy DoD three-pass overwriting for HDDs and standard OS-level formatting for SSD/NVMe media is shown to achieve equivalent forensic security outcomes in substantially less time and with substantially less hardware cost.

These findings are implemented as a prototype framework, DataSanitix, intended to apply proportionate, verified sanitization automatically based on detected storage media type.

References

[1] S. L. Garfinkel and A. Shelat, "Remembrance of data passed: A study of disk sanitization practices," IEEE Security & Privacy, vol. 1, no. 1, pp. 17–27, 2003.

[2] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in Proc. 6th USENIX Security Symp., San Jose, CA, USA, 1996.

[3] C. Wright, D. Kleiman, and S. Sundhar R. S., "Overwriting hard drive data: The great wiping controversy," in Information Systems Security, Lecture Notes in Computer Science, vol. 5352, Springer, 2008, pp. 243–257.

[4] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, "Guidelines for media sanitization," NIST Special Publication 800-88, Revision 1, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2014.

[5] U.S. Department of Defense, "National Industrial Security Program Operating Manual," DoD 5220.22-M, U.S. Department of Defense, Washington, DC, USA, 2006.

[6] International Organization for Standardization, "Information technology — Security techniques — Storage security," ISO/IEC 27040:2015, ISO, Geneva, Switzerland, 2015.

[7] B. Carrier, File System Forensic Analysis. Boston, MA, USA: Addison-Wesley, 2005.

[8] S. Boboila and P. Desnoyers, "Write endurance in flash drives: Measurements and analysis," in Proc. 8th USENIX Conf. on File and Storage Technologies (FAST), San Jose, CA, USA, 2010, pp. 115–128.

[9] T-13 Technical Committee, "ATA/ATAPI Command Set (ACS-3): Data Set Management Command (TRIM)," INCITS, 2013.

Appendix

1. Decision Matrix for Sale

Situation	Recommended Method	Why
Selling an HDD	DoD 5220.22-M (3-pass)	Eliminates recoverable data with acceptable time
Selling an SSD	Windows Format (TRIM)	0% recovery with minimal NAND wear
Selling an NVMe SSD	Windows Format (TRIM)	Fastest method with no additional overwrite required
Highly confidential HDD	DoD 3-pass	Good balance between security and time
Enterprise reuse	Device-aware DataSanitix	Automatically selects the correct method

Table vi Decision Matrix for Sale

2. Cost–Benefit Analysis

Method	Security	Time	Hardware Wear	Overall Rating
Delete	Low	Excellent	None	★
Format	Medium	Excellent	None / some count in SSD	★★★
NIST	High	Good	Low	★★★★
DoD	Very High	Good	Medium	★★★★★
Gutmann	Very High	Very Poor	Very High	★★

Table V Cost–Benefit Analysis

3. Format 2 GB space

Method	Average Time
Delete	2 seconds
Format	5 seconds
NIST	20 seconds
DoD	2 minutes
Gutmann	Much longer

Table VI Format 2 GB space

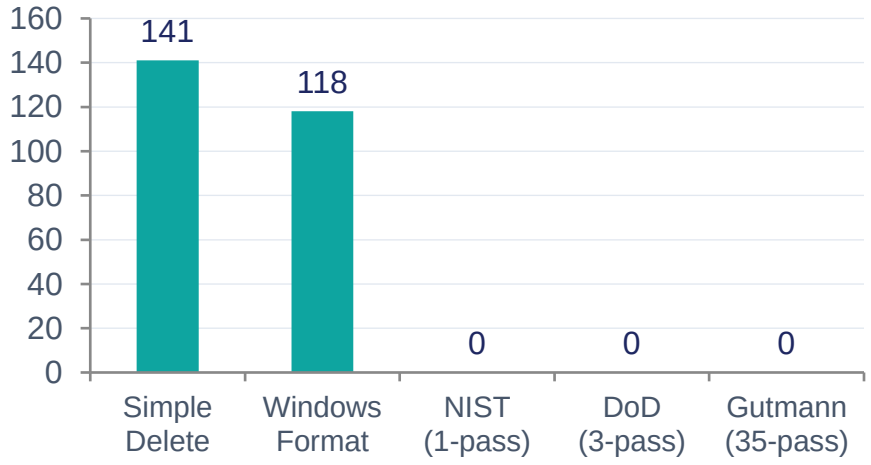


Figure 1 Amount of file recovery by after format Different method