THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 16

Article 1

July 2021

An Economical Method for Securely Disintegrating Solid-State Drives Using Blenders

Brandon J. Hopkins PhD
Akamai Technologies Inc., brandon.j.hopkins@gmail.com

Kevin A. Riggle
Akamai Technologies Inc., kevinr@free-dissociation.com

Follow this and additional works at: https://commons.erau.edu/jdfsl

Part of the Computer Law Commons, Electro-Mechanical Systems Commons, Information Security Commons, and the Manufacturing Commons

Recommended Citation

Hopkins, Brandon J. PhD and Riggle, Kevin A. (2021) "An Economical Method for Securely Disintegrating Solid-State Drives Using Blenders," *Journal of Digital Forensics, Security and Law*: Vol. 16 , Article 1.
Available at: https://commons.erau.edu/jdfsl/vol16/iss2/1

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University.
DAYTONA BEACH, FLORIDA

PURDUE
UNIVERSITY

(c)ADFSL

An Economical Method for Securely Disintegrating Solid-State Drives Using Blenders

Cover Page Footnote

B.J.H. and K.A.R. are inventors on a patent related to solid-state drive pulverization: Patent No. US 10,589,286 B2.

This article is available in Journal of Digital Forensics, Security and Law: https://commons.erau.edu/jdfsl/vol16/iss2/1

AN ECONOMICAL METHOD FOR SECURELY DISINTEGRATING SOLID-STATE DRIVES USING BLENDERS

Brandon J. Hopkins[1], Kevin A. Riggle[2]
Akamai Technologies, 145 Broadway, Cambridge, MA 02142
bhopki31@ford.com,
kevinr@free-dissociation.com

ABSTRACT

Pulverizing solid-state drives (SSDs) down to particles no larger than 2 mm is required by the United States National Security Agency (NSA) to ensure the highest level of data security, but commercial disintegrators that achieve this standard are large, heavy, costly, and often difficult to access globally. Here, we present a portable, inexpensive, and accessible method of pulverizing SSDs using a household blender and other readily available materials. We verify this approach by pulverizing SSDs with a variety of household blenders for fixed periods of time and sieve the resulting powder to ensure appropriate particle size. Among the 6 household blenders tested, sharp-blade blenders with high peak power (1,380 W) and high blade speed (28,000 RPM) properly disintegrate 2.5-inch SSDs in less than 20 min. This method is useful for pulverizing small numbers of SSDs that contain secret information when on-site conventional disintegrators are not available or practical.

Keywords: solid-state drives, destructive sanitization, information security, blender, National Security Agency guidelines

1. INTRODUCTION

At Akamai Technologies Inc., a company providing a content distribution network which at the time delivered about a quarter of the traffic on the web, solid-state drives (SSDs) started to fail that contained sensitive secrets at data centers located far from the main office. These failures were due to the expected, natural aging of SSDs (Arakelyan et al., 2017). While Akamai had a robust program for disposing magnetic platter-based hard disk drives (HDDs) containing secrets, the company had no similar protocol for disposing SSDs. Unlike HDDs, SSDs cannot be sanitized by degaussing (Kissel, Regenscheid, School, Stine, 2014). Ensuring proper SSD sanitization is critical as improper practices can result in substantial legal punishment (Blyth Mellings, 2014; G. Hughes Coughlin, 2006), not to mention the cost of losing data to an adversary. For example, data breaches related to health care issues covered by the Health Insurance Portability and Accountability Act (HIPAA) can result in fines of $50,000 United States dollars (USD) and imprisonment (Murphy, Angelini, Shwartz, 2018). The National Security Agency (NSA) recommends the sanitization of SSDs that contain information ranging from unclassified to top secret by disintegration "into particles that are nominally 2 millimeter edge length in size (Taflan, 2014)." In general, researchers regard physical destruction of data storage devices as the most secure method of sanitization (Garfinkel Shelat, 2003; G. F. Hughes, Coughlin, Commins, 2009). Even if non-destructive methods can effectively delete SSD data (Kumar, Neyaz, Shashidhar, 2020; Wei, Grupp, Spada, Swanson, 2011), these strategies are more difficult to verify than destructive methods. For example, a non-destructively sanitized SSD looks the same as it did before data deletion, while a pulverized SSD—a small pile of powder—cannot be mistaken with its original intact state. The authors have not attempted to extract data from 2-mm pieces of SSD nor are they aware of successful attempts. However, even if the NSA-disintegration metric is overly conservative, certain organizations still want this high level of assurance. For common users, proper use of software full-disk encryption is sufficient to make personal data unrecoverable from SSDs.

Purchasing typical commercial disintegrators for all of Akamai's data centers is expensive and excessive. These disintegrators that pulverize SSDs in accordance with NSA standards are large (1 m^3), heavy (450 kg), and costly ($52,000) (SEM, 2020). In addition, only a small number of SSDs need to be disposed of in this rigorous manner annually. As a second option, the NSA recommends incineration: "[m]aterial must be reduced to ash (Taflan, 2014)." Unfortunately, this strategy creates hazardous gases, which is illegal to generate in some data-center locations (Leung, Duzgoren-Aydin, Cheung, Wong, 2008).

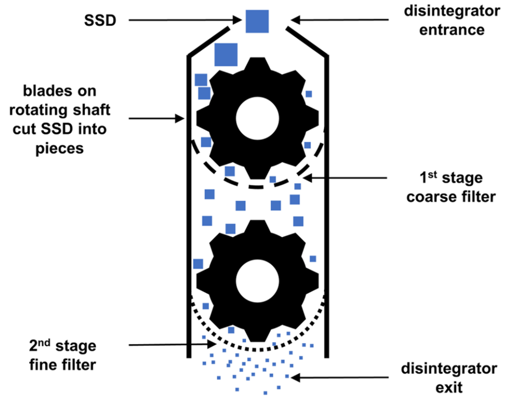

Figure 1. Schematic of conventional disintegrator.

If SSDs cannot be disposed of on-site, they must be taken to disintegration facilities, which are often expensive, far from data centers, and provide minimal sanitization verification. Moving the SSD from the data center requires travel that increases the likelihood that a well-funded adversary could steal the SSD. Sanitization verification is challenging because of how commercial disintegrators are designed. Disintegrators commonly use two-stage destruction processes often involving hammer mill technology, which consists of blades on rotating shafts that cut SSDs into pieces (Figure 1).

Operators feed SSDs into a steel-encased destruction chamber, and particles fall out of a sieve into a collection bin. SSD owners cannot easily verify that the outgoing particles are from their inserted SSD because the destruction chamber is opaque. An adversary could easily design a machine that collects whole SSDs and outputs spurious powder. Even if the disintegrator owner lets the SSD owner look inside the machine, the SSD owner will have difficulty determining whether the machine properly disintegrated the whole SSD. Particles slightly larger than 2 mm, could still be in the big machine filled with small crevices and coated in powder from previously ground SSDs. Based on the authors' calculation, the total cost of disintegration in accordance with NSA standards including personnel cost and travel is expensive, at least $2,000 per SSD. In summary, outsourcing SSD pulverization is expensive, increases the likelihood of adversarial interception, and offers a poor level of sanitization verification.

With no conventional, commercial options to meet Akamai's requirements, Akamai needed a new solution to achieve NSA standards for on-site sanitization that allows for appropriate verification. Based on Akamai's experience using commercial disintegrators, the authors outline key needs for a better option (Table 1). Equation 1 estimates device power assuming an SSD is machined.

$$P \approx n \times u_s \times \frac{V_{SSD}}{t} \qquad (1)$$

The variable P is the motor power. The authors use a factor of safety n (no units) equal to 5. They select this value, assuming that a significant amount of energy is dissipated via sound and heat, to size the motor large enough so that it will not stall. The variable u_s is the specific energy of the SSD material. While an SSD is made of many materials, the authors use the specific energy of copper (Kalpakjian Schmid, 2014), 3 J mm^3, for approximation. The variable V_{SSD} represents the volume of the SSD, approximately 20,500 mm^3, and t is the time required to disintegrate the SSD. Time ranging from 1–20 min results in an inversely proportional power range from 5,000 W down to 250 W, respectively.

Commercial disintegrators in comparison pulverize SSDs in seconds. For Akamai's low-volume application, trading disintegration speed for portability and low cost is acceptable. While a custom-made line of machines meeting these requirements (Table 1) could be made, creating a new pulverizing device is costly and time consuming. Using an off-the-shelf product for the job decreases cost and increases implementation speed.

Using the power requirements derived from equation 1, the authors find that some off-the-shelf food processing technologies fall within the necessary power-capability range. Blenders stand out as a good off-the-shelf candidate because they can pulverize a volume of 1,000,000 mm^3 into particles near 1 mm^3 in one step. In contrast, grain grinders, meat processors, and nut-and-spice grinders require several steps to achieve similar size reduction. Blenders are also easily cleaned, which decreases the likelihood of overlooking a large piece of SSD caught in the grinding chamber. Blender jars are transparent, so the pulverization process can be easily videotaped for sanitization verification (Hopkins Riggle, 2020).

With these insights, the authors test the following hypothesis: if a household blender with sufficient blade sharpness and motor power is turned on at its highest speed for up to 20 min with an SSD printed circuit board (PCB) inside the blender jar, the PCB will be pulverized into particles that are all smaller than 2 mm in edge length. Among the 6 tested household blenders, the authors find that sharp-blade blenders with high peak power (1,380 W) and blade speed (28,000 RPM) properly disintegrate 2.5-inch SSDs in less than 20 min.

2. TESTING PROTOCOL

The authors create this testing protocol (Figure 2) to identify characteristics of blenders that properly disintegrate a 2.5" SSD in less than 20 min. In summary, the PCB from the SSD is removed, cut into pieces, and then blended. The authors check particle size by sieving every minute after 5 min of initial blending. If any particle is larger than 2 mm, the authors pour all the particles back into the blender and continue blending for additional 1-min intervals followed by particle verification. Blenders that fail to appropriately pulverize an SSD PCB after 20 min of total blending time are inadequate.

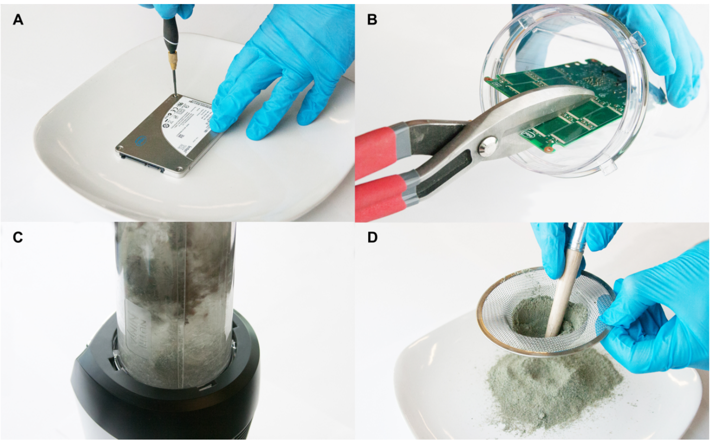

Figure 2. SSD pulverization process. (A) Unscrew SSD from casing. (B) Cut PCB into blending container. (C) Blend the SSD PCB. (D) Sieve the resulting powder.

1. Remove the screws and casing from the PCB of the SSD (Figure 2A). The case and screws store no data and therefore do not need to be disintegrated.

2. Remove all stickers from the SSD PCB. Stickers inhibit disintegration and cause jamming in the sieve during the size verification step.

3. With the PCB positioned so that the side of the PCB with microchips on it is facing downward into the blender jar, use shears to cut the SSD PCB into pieces that are approximately 9 cm^2 in size (Figure 2B). If the microchips shatter during cutting, they will shatter into the blender jar not out of it. Avoid cutting the microchips. If the SSD PCB is not precut, the SSD PCB can get jammed in the top of the blender jar, resulting in prolonged or ineffective pulverization.

4. Place the SSD PCB pieces into the selected blender and turn on the blender's highest speed (Figure 2C).

5. After 5 min of blending, pour the contents through a sieve with pores smaller than 2 mm positioned over a large white plate (Figure 2D). The white plate allows the operator to clearly see particles during the sieving process. Use a brush to wipe down surfaces on the inside of the blender jar to ensure that no large particles miss entering the sieve.

6. If the largest SSD particles pass through the sieve, the SSD is disintegrated properly. If some particles are too large, replace all particles back into the blender using the brush and white plate. Continue blending for one minute and recheck the particle sizes using the sieve until all particles are appropriately sized. In general, the longer the particles are blended, the smaller they become.

The authors use this protocol to collect the data shown in Table 2. Near the end of the processing time for each SSD, the authors check the particle sizes in 1-min intervals to ensure that processing times fell within –61 s to +1 s of their listed times in Table 2. If one of any five 2.5" SSDs, from a variety of manufacturers and data storages sizes, do not appropriately disintegrate within 20 min, the authors stop testing that blender. The authors determine the processing time of five 2.5" SSDs for blenders that yield processing

Key Needs	Metrics	Values	Units
1. Resulting powder meets NSA guidelines	Longest particle dimension	< 2	mm
2. Disintegration can be visually recorded and verified	Light transmission of disintegration chamber	> 70	%
3. Appropriate operation time	Disintegration time of one SSD	< 20	min
4. Disintegration cost is low	Cost of destruction per SSD	< 2,000	USD
5. Fits into carry-on suitcase for airplane travel	Rectangular volume of device	< 55 < 35 < 23	cm
6. Health of operator and bystanders are maintained	Lead exposure concentration averaged over 8-h period (OSHA, 2020)	< 50	$\mu g\ m^{-3}$
7. Nonthreatening	Absence of explosives	binary	unitless

Table 1. Key design requirements.

Blender	Time [min]	Max. power [W]	Max. speed [RPM]	Cost [USD]
Oster® 10-Speed	> 20	450	11,000	45
Nutri Ninja® Pro	> 20	1000	21,000	125
Vitamix® Turbo-Blend Two Speed	9,13, 15, 19, 19	1380	29,000	480
Oster® Versa®	12, 13, 14, 16, 17	1400	28,000	300
Ninja® Ultima	> 20	1500	24,000	160
Blendtec® Classic 575	> 20	1575	29,500	330

Table 2. Blender specifications and 2.5” SSD processing times.

times under 20 min. Even with a sample size of 5, there is a 93.75% chance that the smallest and largest processing times bound the median processing time of 2.5" SSDs assuming the authors randomly selected these SSDs (Hubbard, 2010). Note that processing times do not increase sequentially as shown in Table 2. Instead, the authors organize data so that minimum and maximum values can be easily read.

3. RESULTS DISCUSSION

The authors demonstrate that certain household blenders appropriately disintegrate SSDs in less than 20 min. Among the blenders tested, blenders with peak powers greater than or equal to 1,380 W and with blade speeds greater than or equal to 28,000 RPM can disintegrate SSDs in less than 20 min except for the Blendtec® Classic blender. One explanation for this observation is that the Blendtec® is designed with large, blunt clean-safe blades. To compensate for blunt blades, the Blendtec® uses a higher power motor than most blenders. For the given application, however, the Blendtec® motor may need more power to appropriately disintegrate an SSD within the allotted time. Higher power but more costly Blendtec® blenders are available. In contrast, the sharp blades used by the Oster® Versa® and Vitamix® allow for appropriate pulverization times while using lower-power motors. The authors note that the Ninja® Ultima and Vitamix® used for testing are preowned, and therefore the blades may have been originally sharper, which would allow for faster processing times.

Distributors sell blenders that successfully disintegrated SSDs in less than 20 min for $300 or more. The authors, however, find refurbished, used, or discounted blenders of the same models for less than $200. An additional issue is that all the blender jars become progressively clouded or less transparent with each blending cycle due to internal surface-finish marring from the PCB pieces. SSD owners may therefore need to purchase new blending jars, which can cost about $100, to maintain blender jar transparency and blade sharpness. Blades usually come with blender jars. Purchasing a new blender for every SSD sanitization is still an order of magnitude lower in cost than outsourcing sanitization.

The authors note that some SSDs contain heavy metals such as lead and other potentially harmful substances (Fu et al., 2008; Leung et al., 2008). The authors therefore pulverize SSDs with a blender inside a Spilfyter® Hands-in-Bag® Disposable Artificial Atmospheric Chamber, a type of low-cost, portable, disposable glove bag, to mitigate dust exposure. During testing, the authors observe that generated dust appears to be fully contained in the sealed glove bag. The authors also measure the temperature of all tested blenders using an infrared thermometer. None of the measured blenders' surface temperatures reached higher than 50 °C, which is less than half the average melting temperature of the polyethylene glove bags.

The authors note that the reported testing protocol has limitations. For example, during sieving, an SSD piece can pass through even if one of its dimensions is greater than 2 mm such as a fiber-shaped piece with a diameter less than 2 mm but with a length greater than 2 mm. However, this limitation is universal to sieving methods that are already used in NSA-approved commercial disintegrators.

4. CONCLUSIONS

Solid-state drive pulverization in accordance with NSA standards is critical for information security. Conventional pulverization methods, however, can be costly and inconvenient.

Outsourcing SSD sanitization can cost $2,000 per SSD, and commercial SSD disintegrators can cost more than $50,000. In addition, some users of commercial SSD disintegrators find sanitization verification challenging because of how existing machines are designed. The authors therefore create an accessible, portable SSD disintegration method using off-the-shelf products that altogether can cost less than $300. This method uses a household blender that makes sanitization verification simple and less prone to adversarial manipulation. The proposed method requires less than 20 min to properly pulverize an SSD in accordance with NSA standards.

REFERENCES

[1] Arakelyan, S., Lee, H., Jeong, Y., Babajanyan, A., Friedman, B., Lee, K. (2017). Direct imaging of the SSD and USB memory drives heating by thermoelastic optical indicator microscopy. Case Studies in Thermal Engineering, 10, 407–412.

[2] Blyth, A., Mellings, S. (2014). Managing End of Life Risk For Solid State Devices (SSD). Retrieved from `http://www.btc.co.uk/newsletter/ADISA\_SSD.pdf`

[3] Fu, J., Zhou, Q., Liu, J., Liu, W., Wang, T., Zhang, Q., Jiang, G. (2008). High levels of heavy metals in rice (Oryza sativa L.) from a typical E-waste recycling area in southeast China and its potential risk to human health. Chemosphere, 71(7), 1269–1275. `https://doi.org/10.1016/j.chemosphere.2007.11.065`

[4] Garfinkel, S. L., Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. IEEE Security and Privacy, 1(1), 17–27. `https://doi.org/10.1109/MSECP.2003.1176992`

[5] Hopkins, B. J., Riggle, K. A. (2020). Efficiently sanitizing a solid state drive (SSD). Retrieved from `https://patentimages.storage.googleapis.com/18/68/44/cb61beb066f6cf/US10589286.pdf`

[6] Hubbard, D. W. (2010). How to Measure Anything: Finding the Value of "Intangibles" in Business (2nd ed.). Hoboken, New Jersey: John Wiley Sons, Inc. Hughes, G., Coughlin, T. (2006). Tutorial on Disk Drive Data Sanitization. Retrieved from `https://www.researchgate.net/publication/229003088\_Tutorial\_on\_Disk\_Drive\_Data\_Sanitization`

[7] Hughes, G. F., Coughlin, T., Commins, D. M. (2009). Disposal of disk and tape data by secure sanitization. IEEE Security and Privacy, 7(4), 29–34. `https://doi.org/10.1109/MSP.2009.89`

[8] Kalpakjian, S., Schmid, S. (2014). Manufacturing Engineering and Technology (7th ed.). Upper Saddle River, New Jersey, 07458: Pearson Education, Inc.

[9] Kissel, R., Regenscheid, A., School, M., Stine, K. (2014). Guidelines for Media Sanitization. NIST Special Publication 800-88. `https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-88r1`

[10] Kumar, A., Neyaz, A., Shashidhar, N. (2020). A Survey On Solid-State Drive Forensic Analysis Techniques. International Journal of Computer Science and Security, 14(2), 13–21.

[11] Leung, A. O. W., Duzgoren-Aydin, N. S., Cheung, K. C., Wong, M. H. (2008). Heavy metals concentrations of surface

dust from e-waste recycling and its human health implications in southeast China. Environmental Science and Technology, 42(7), 2674–2680. https://doi.org/10.1021/es071873x

[12] Murphy, A. M., Angelini, L. B., Shwartz, J. (2018). Criminal prosecution for violating HIPAA: an emerging threat to health care professionals. Stat News. Retrieved from https://www.statnews.com/2018/07/02/criminal-prosecution-violating-hipaa/#:~:text= The penalties for criminal violations,to one year in prison.

[13] OSHA. (2020). Occupational Safety and Health Standards Lead Exposure Policies. Retrieved from https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=10030

[14] SEM. (2020). Model 2SSD Solid State Drive Disintegrator - ENTERPRISE. Retrieved October 19, 2020, from https://www.semshred.com/product/model-2ssd-solid-state-drive-disintegrator-enterprise/

[15] Taflan, J. (2014). NSA/CSS Storage Device Sanitization Manual. Retrieved from https://patentimages.storage.googleapis.com/18/68/44/cb61beb066f6cf/US10589286.pdf

[16] Wei, M., Grupp, L. M., Spada, F. E., Swanson, S. (2011). Reliably Erasing Data from Flash-Based Solid State Drives. FAST, 11.