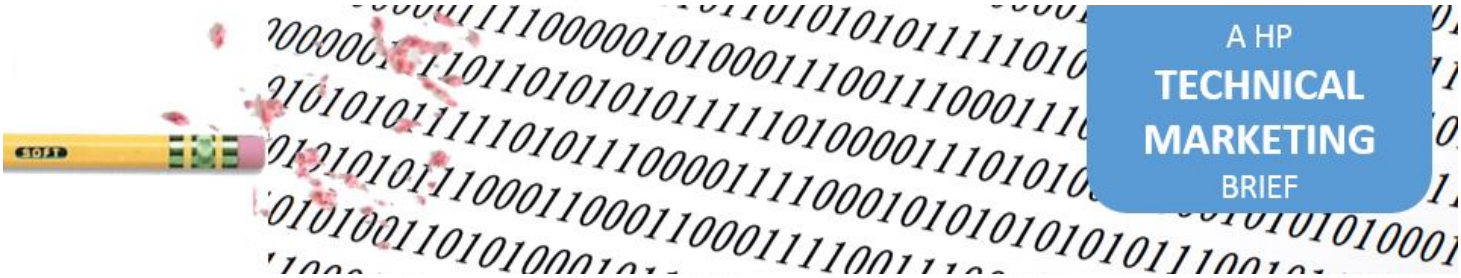


HP Secure Erase: Securely Erasing SSDs

Joe Marenin, Senior EliteBook Product Manager

Introduction

In an era where protecting sensitive information is so important, the ability to ensure that user data is securely erased from a data storage device is critical. HP has implemented a disk erase feature built-in the BIOS of the HP ELITEBOOK AND PROBOOK SERIES NOTEBOOK which meets the NIST SP800-88r1 "Clear" level requirements for the cleaning of disk media. This paper describes this capability and related information.

Erasing SSDs vs. HDDs

With magnetic media (e.g., HDDs), data can be overwritten using a data removal algorithm that writes multiple patterns on every sector, cluster, bit of the hard drive (see table below) that is documented in the Department of Defense (DOD) 5220.22-M Chapter 8 specification[1].

Table: Data written to the drive on each cycle

Disk Sanitizer Cycle	Data written to drive
First cycle	00000000 (all zeros)
Second cycle	11111111 (all ones)
Third cycle	random writes of 1 or 0 and verify
Fourth cycle	00000000 (all zeros)

Overwrite-based tools are effective for only hard disk drives. Writing a predetermined data pattern to a NAND Flash-based SSD does not result in an empty drive. Instead, it results in a full drive with data that must be erased before new user data can be written and massively shortens the service life.

To securely erase all user data from an SSD and restore the drive to a fresh-out-of-box (FOB) performance state, the National Institute of Standards Technology (NIST) supports the "SECURITY ERASE UNIT" command that meets the minimum sanitization guideline for media sanitization of SSDs (NIST SP800-88 Rev. 1).

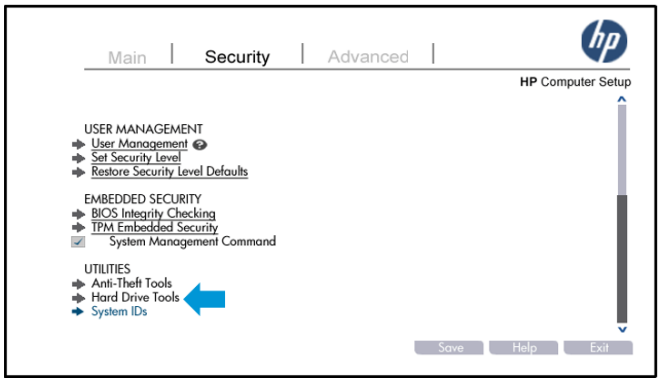
Secure Erase relies on an ATA command called "Security Erase Unit" that is defined in the American National Standards Institute (ANSI) ATA and SCSI disk drive interface specification which meets NIST 800-88r1 "Clear" guidelines. This command does not actually write anything to the drive. Instead it causes the SSD to apply a voltage spike to all available NAND in unison, resetting every available block of space in one operation forcing the drive to "forget" all stored data which cannot be recovered by even advanced data recovery services. By doing this, you will use one whole program-erase cycle for your drive and is completed in less than two minutes which is a quantum leap ahead of a similar operation in HDDs, which can take hours to securely eliminate user data.

What Data Is Not Erased?

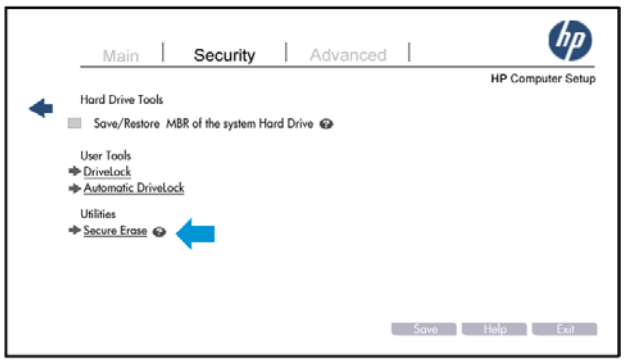
All data in the user space is completely and irretrievably erased, and every block in the user space is ready to accept new host-written data, which moves the drive to its highest performance state (FOB). However, some data must be left in place; this includes data required for normal drive operation: SSD firmware copies that reside in the NAND, all SMART data, and retired NAND block mapping tables.

How to enable HP Secure Erase?

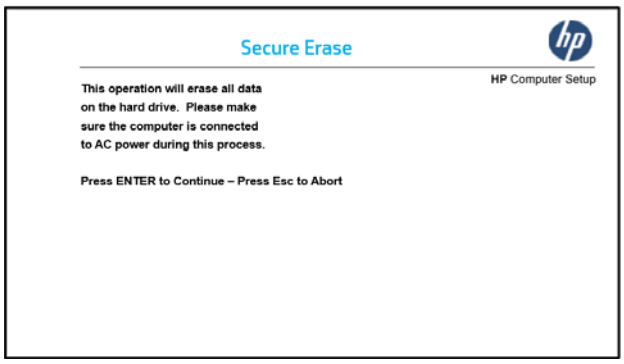
1. Turn-on or re-boot the system and press F10 to enter the BIOS setup.



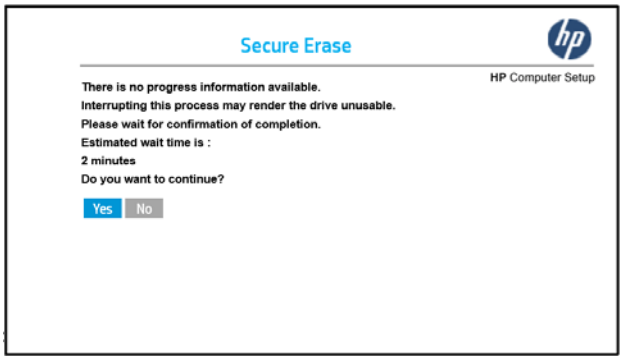
2. Select "HARD DRIVE TOOLS".



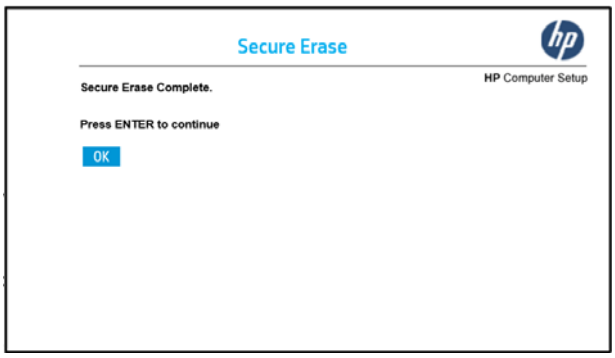
3. Select “SECURE ERASE”.



4. Press “ENTER” to continue.



5. Select “YES”



6. HP Secure Erase is complete.

Conclusion

Writing or overwriting data to drive is the accepted practice of securely eliminating data from a HDD. However, in the case of NAND Flash-based SSDs, overwriting is redundant, unnecessary, and a potentially insecure method of eliminating data. NAND Flash is properly erased using the “SECURITY ERASE UNIT” command that is available with the HP SECURE ERASE built-in the HP Notebook BIOS.

By using HP SECURE ERASE, you will be able to erase all user data from a SSD meeting the minimum sanitization guideline for media sanitization of SSDs (NIST SP800-88 Rev. 1 Clear Level).

[1]Please note that the 5220.22-M no longer exists. Today, The DoD has decided that secure information that must retain secure must be destroyed. NIST has restated in clear terms that a two person rule (read human verification) shall be implemented, but no guidelines as to what method of sanitization (it could be a single wipe with dual human verification, or a single destruction with the same.)

May 2016 / Document Version: 1