your right to be forgotten

Youwipe

Erasure Standards

Erasure Tool 4

Overwriting Standards (HDD, SSD, USB and SD cards)

HMG Infosec Low	(1 time overwrite)
Overwrite	0x0
3% Verification[1]	Function

HMG Infosec High	(3 times overwrite)
Overwrite	0xAA
Overwrite	0x55
Overwrite	Random
10% Verification	Function

DoD 5220.22-M	(3 times overwrite)
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
10% Verification	Function

DoD 5220.22-M ECE	(7 times overwrite)
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
Overwrite	Full random
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
10% Verification	Function

SSD/ATA Baseline	(2 times overwrite + secure erase)
Overwrite	Random
Secure Erase[2]	Function
Overvwrite	0x55
10% Verification	Function

SSD/ATA Enhanced	(3 times overwrite + enhance secure erase)
Overwrite	Full random
Overwrite	Full random
Enhance Secure Erase [3]	Function
Overwrite	0x55
10% Verification	Function

NIST SP 800/ATA Clear	(1 time overwrite + enhance secure erase)
Overwrite	0xFF
10% Verification	Function

[1] YouWipe has a default verification of 10% (unless it is the NIST standard where it is 25%) of the whole drive to verify if the last algoritm is written as it should be according to the standard the user has chosen. This 10% is always and random. It will be done on different sectors per drive and per verification. YouWipe can tailor the verification percentage to other levels, if the user wishes so, e.g. 100%.

[2] Secure Erase is the name given to a set of commands available from the firmware on PATA and SATA based hard drives. So basicly it is a firmware command that command the firmware to do an erasure.

[3] The enhanced version of the secure erasure does the same, but uses a more secure algorithm than it will use in the secure erase version.

NIST SP 800/ATA Purge	(3 time overwrite + enhance secure erase)
Overwrite	0x55
Overwrite	Random
Overwrite	0xAA
10% Verification	Function

Ext. HMG Infosec Low	(1 time overwrite + enhance secure erase)
DCO Restoration[4]	Function
HPA Expansion[5]	Function
Enhance Secure Erase	Function
Overwrite	0x0
3% Verification	Function

Ext. HMG Infosec High[6]	(3 times overwrite + enhance secure erase)
DCO Restoration	Function
HPA Expansion	Function
Enhance Secure Erase	Function
Overwrite	0xAA
Overwrite	0x55
Overwrite	Random [7]
10% Verification	Function

Ext. DoD 5220.22-M	(3 times overwrite + enhance secure erase)
DCO Restoration	Function
HPA Expansion	Function
Enhance Secure Erase	Function
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
10% Verification	Function

Ext. DoD 5220.22-M ECE	(7 times overwrite + enhance secure erase)
DCO Restoration	Function
HPA Expansion	Function
Enhance Secure Erase	Function
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
Overwrite	Full random
Overwrite	0x55
Overwrite	0xAA
Overwrite	Random
10% Verification	Function

[4] DCO is an abbreviation for Device Configuration Overlay which is a hidden area on many of the HDD's we are using today. The DCO is mainly used to resize the number of sectors shown in the BIOS and OS (Operating System)

[5] HPA is an abbreviation for Host Protected Area, which is a hidden area that for example is used by computer manufacturers to preload an OS for installation and recovery. In that case they do not need to provide a CD or DVD with the software.

[6] This erasure standard is certified based on the requirements of BSPA certification scheme and Common Criteria (CC) scheme

[7] last random overwrite is with a byte different from AA and 55 (NCSC requirement)

Ext. NIST SP 800/ATA Clear	(1 time overwrite + enhance secure erase)
HPA Expansion	Function
DCO Restoration	Function
Enhance Secure Erase	Function
Overwrite	0xFF
10% Verification	Function

Ext. NIST SP 800/ATA Purge	(3 time overwrite + enhance secure erase)
HPA Expansion	Function
DCO Restoration	Function
Enhance Secure Erase	Function
Overwrite	0x55
Overwrite	Random
Overwrite	0xAA
10% Verification	Function

Overwriting Standards (iPhone, iPads, Android Devices)

Erasure method	Description
iOS (confirming US **NIST** guidelines and recommendation, **Crypto** Erasure, page 28)	
Cryptographic sanitization[8]	Cryptographic erasure. Operating system reset and update to the latest. The erasure process overwrites the encryption key making the user data on the device inaccessible. The latest iOS operating system version is downloaded from the Apple servers and new encryption keys generated to the device during the erasure process. Overwriting is not necessary.
Android	
Factory reset	Android device built-in factory reset.
Infosec Low	Remove applications and writable files from the device flash memory. Overwrite the free space of the device's unprotected flash memory space two (2) times with random bytes. Perform Android device built-in factory reset.
Infosec High[9]	Remove applications and writable files from the device flash memory. Overwrite the free space of the device's unprotected flash memory space three (3) times with random bytes. Perform Android device built-in factory reset.

[8] This erasure standard is certified based on the requirements of BSPA certification scheme and Common Criteria (CC) scheme