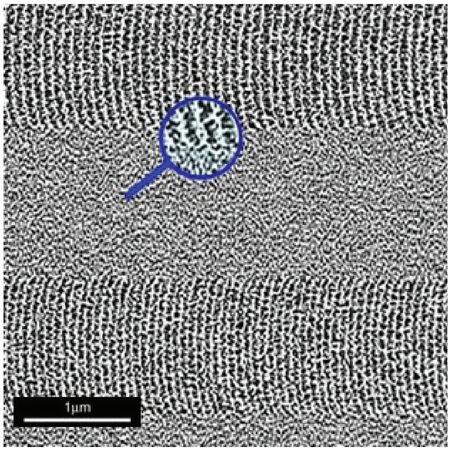
WHITE CANYON™
SOFTWARE

Are Multiple Overwrite Passes Necessary?

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

THE ORIGIN OF MULTIPLE PASSES

Many current and past government standards including DoD 5220.22-M, HMG, BSI require data be overwritten multiple times to insure that the information cannot be recovered. The idea that multiple wipe passes are required to effectively erase data originates in part with a 1996 study published by Peter Gutmann. He suggested that data should be wiped up to 35 times in order to be considered irrecoverable. He proposed that data could be recovered using magnetic force microscopy (MFM) and scanning tunneling microscopy (STM) techniques.



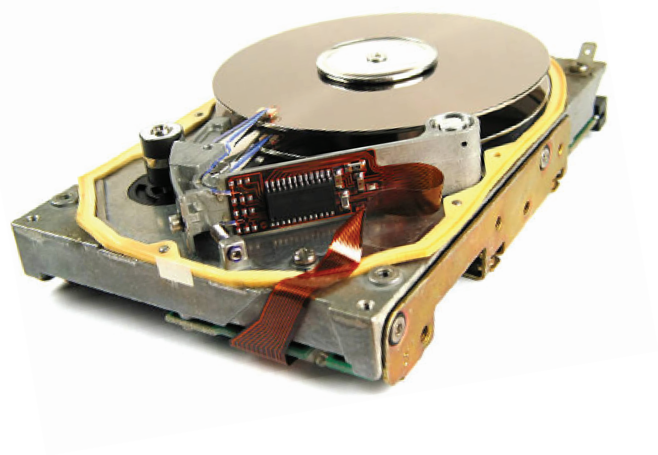
Bit Shadows

If viewed under an atomic microscope, hard drives built during the late 90's and very early 2000's would show "Bit Shadows". These shadows could reveal what information was previously written in that location. To eliminate this possibility Gutmann recommended multiple overwrites.

DATED GOVERNMENT STANDARDS

Because of these concerns various domestic and international government standards such as the DoD 5220.22-M (February 2006) and the NSA 130-2 (Pre 2011) have required multiple passes when sanitizing data storage. Many organizations are required to comply with these standards as a matter of policy and data erased using these standards is certainly irrecoverable. These older standards were created for older technologies. Over the last 15 years drive technology has advanced to the point where the MFM and STM techniques have become obsolete. Specifically, part of Gutmann's claim was that the head positioning system in hard drives was not precise enough to overwrite new data on top of the exact position of the old data, thus creating the possibility that the old data would remain intact. Today's hard drive technologies are very precise and have eliminated this possibility.

Peter Gutmann has since advised, "If you're using a drive which uses encoding technology X, you only need to perform the passes specific to X, and you never need to perform all 35 passes."



A NEW STANDARD

Due to the evolution of hard drive technology and the introduction of Solid State Drives (SSD) newer and more efficient standards have been developed. In recent years, the NIST standard has become the industry standard and the Department of Defense has since adopted the NIST standard for data erasure. Former DOD CIO Teri Takai said, “While in fact this may seem like a dramatic shift, we don’t see it so much as a dramatic shift as an evolution of where we want to go.” (April 2, 2014 at Intel’s Security Through Innovation Summit in Washington.) To confirm that multiple overwrites are no longer necessary, the National Institute of Standards and Technology (NIST) states in SP 800-88r1: “Guidelines for Media Sanitization (December 2014)” that the “NSA has researched that one overwrite is good enough to sanitize most drives.”

DATA WIPING RECOMMENDATION

WhiteCanyon Software recommends the NIST 880-88r1 standard for data removal on hard drives and solid state drives. NIST 880-88r1 wipe specification was made for current technologies and treats different storage types accordingly. This process significantly reduces the wipe time while still ensuring that the data is irrecoverable. As the NIST standard has been adopted as industry standard, the data removal process has been sped up significantly. The NIST standard states that changing the encryption key on self-encrypting drives is sufficient. WipeDrive takes it a step further by changing the encryption key then overwriting the entire drive. This process ensures that the data is irrecoverable beyond industry standard.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Performing multiple wipes as part of a multi-pass overwrite pattern is unnecessary to completely erase data. WhiteCanyon Software only recommends using multiple passes if required as part of your organization’s policy or for special use cases where multiple redundancies are desired.