Erasure Methods

With the advent of advanced drive erasure technologies, simple overwrites are no longer preferred, and yet with multiple competing erasure possibilities, knowing which methods are usable on any given drive to accomplish the task would take a lot of trial and error. Fortunately, the drives tell us what methods that they support so that the software can make good choices on how to proceed for each drive on an individual basis.

The NIST 800-88 revision 1 specification recognizes that there are many possible ways to accomplish the goal of erasing a hard drive that will do an adequate job. The specification breaks them down into two levels: Purge and Clear. Details can be downloaded and read from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf on document pages 32/33 for Hard Disk Drives (HDD), and pages 36/37 for Solid State Drives (SSD.)

The NIST 800-88 revision 1 Purge specification essentially covers all drive self-erasure methods that are guaranteed to erase all customer data, even if not accessible to the user. The valid Purge methods include the T10 and T13 Sanitize specifications of Block Erase, Cryptographic Scramble, and Overwrite as well as the much more complicated Trusted Computing Group standards of Opal and higher which also implement these features but in an End-To-End trust chain.

The NIST 800-88 revision 1 Clear specification covers less rigorous methods, but which should, at minimum, overwrite all user accessible data. These methods include Secure Erase/SCSI Format as well as manually overwriting all areas of the media at least one time. Optionally, multiple passes can be used and with more complicated patterns than a solid block, which means that a NIST 800-88 revision 1 Clear encompasses the older DoD M5220 Santize specification (3x alternating patterns + random), for example.

Erasure Process

Initially in Xerase, the user will assign a given Erasure Method to each sort of drives, classified by the language they speak (ATA or SCSI) and the type of device (HDD or SSD.) If the method selected is a simple overwrite method, the software will simply follow the instructions for that erasure method which dictates the number of passes, the patterns, and so on in accordance with applicable governmental standards and/or user-defined patterns.
However, if the user chooses certain erasure methods, such are Secure Auto, NIST 800-88 rev1 Purge or NIST 800-88 rev1 Clear, the software will intend to make an intelligent guess as how to best implement an erasure that conforms to that guideline. We shall refer to these as Dynamic Erasure Methods from now on.

Secure Auto is our oldest Dynamic method, and simply selects between Secure Erase/Format if available, or the HDD erasure method if it is not. Generally, this is only configured on SSD drives.

NIST 800-88 rev1 Purge is the most rigorous Dynamic method available and the most flexible. Assuming that it has been configured appropriately, it should handle any drive inserted. First, the program determines if the drive supports Sanitize Block Erase, Cryptographic Scramble or Overwrite and if the drive is allowed to execute it by not being in a Sanitize Freeze-Lock state. If so, then an appropriate supported method is chosen (See Purge Adjustments below) and the erasure begins. If no such commands are available, then the program will attempt to evaluate whether it is possible to erase the drive with the NIST 800-88 rev1 Clear method instead.

NIST 800-88 rev1 Clear will choose between Secure Erase/Format depending on drive support of the command and whether the drive is in a Secure Freeze-Lock state. As with Purge above, several adjustments to the choice algorithm are possible (See Clear Adjustments below), but the default operation is as follows. If the drive is an SSD and Secure Erase/Format is possible, then a Secure Erase/Format is initiated. If the drive is an SSD and Secure Erase/Format is not available, then a 3x manual overwrite will be attempted. The additional two passes beyond the minimum required provides a better chance of erasing all previous user-level data even if in currently unmapped sectors due to Wear Levelling features. If a drive is an HDD, then the minimum 1x manual overwrite will occur.

New Dynamic Erasure Methods may get added over time if other governmental bodies require similar logic.

**Purge Adjustments**

It is possible for a drive to support multiple valid erasure methods, or none at all, and the software allows the user some input on the decision-making flow.

Cryptographic Scramble is the fastest method available, as it accomplishes its erasure by simply changing the encryption key on the drive. The data that is stored on the media itself is unreadable without the key. Reading the SSD media “raw” using laboratory attack methods can not retrieve data. Similarly, after changing the key, valid data on the drive is random gibberish when re-read through the controller interface.
However, in theory someone could know the encryption key and restore it, or somehow brute force it with a lengthy iterative attack to make the data readable again. In practice, this is probably not a concern, but it is the primary reason that we normally choose Block Erase instead of Cryptographic Scramble if both are available. Should the user prefer to use Crypto as the preferred method, this can be set in the software via menu Customize->Interface->NIST Settings->Purge: Prioritize Cryptographic Erasure.

In theory, a Cryptographic Erasure should result in random gibberish on the drive. However, the NIST specification allows subsequent writing passes to the drive, and some drive firmware follows up a Cryptographic Erasure with a Block Erase. If you want to make sure the drive media is recognizably erased after a Cryptographic Scramble, the software can be instructed to make that happen even if the drive doesn’t do it automatically. This will be done either with Block Erase or a manual overwrite. This can be set in the software via menu Customize->Interface->NIST Settings->Purge: Overwrite if Random Data after Erasure.

By default, if the drive doesn’t support any usable Purge methods, it drops to the NIST Clear. If instead you would prefer that the drive Abort the erasure or Fail, this can be configured via menu Customize->Interface->NIST Settings->Purge: Action if Purge is Not Supported.

**Clear Adjustments**

The Clear specification is fairly relaxed in what is required, so a lot comes down simply to user preferences. Our defaults as described above we feel best take advantage of the software and operating environment vs tradeoffs in security. However, if the user is willing to accept some other the tradeoffs in time and OS responsiveness, other choices can be invoked.

SCSI Format is the primary way to initiate a Secure Erase on SCSI SSD drives. However, you can also perform the Format on SCSI HDDs. This is a low-bandwidth method of erasure, but once initiated the process is largely out of our control and we can merely monitor it. Aborting/Resuming and similar software features aren’t guaranteed to work. The drive will erase until it is complete. Power cycling will interrupt this. If you want to change all SCSI drives to use Format, or disallow even SSD drives from using a SCSI Format, then change Customize->Interface->NIST Settings->Clear: Allow SCSI Format from ‘SSD Only’ to either ‘All Drives’ or ‘Never’ as appropriate.

Like SCSI Format above, the same scenario applies to ATA Secure Erase. Modify the drives allowed to execute a Secure Erase command by changing Customize->Interface->NIST Settings->Clear: Allow ATA Secure Erase from ‘SSD Only’ to either ‘All Drives’ or ‘Never’ as appropriate.
Lastly, if Secure Erase/Format was not chosen/available for a given drive, the software will drop to a manual overwrite pass. A single overwrite pass satisfies the NIST 800-88 rev1 Clear specification, even for SSD drives (with caveats), however we choose to do a 3x overwrite on SSD drives to attempt to eliminate data that currently isn’t mapped into user accessible blocks. If you wish to always implement a 3x overwrite pass on drives then change Customize- >Interface->NIST Settings->Clear: Use a 3x overwrite from ‘SSD only’ to ‘Always’. Conversely, if you wish to only do a 1x overwrite, even on ATA drives, change it to ‘Never.’

**Verification**

For a manual overwrite method, at the end of every pass we log LBA 1 and MaxLBA hashes for documentation of the erasure process, and to be able to fail early if the erasure didn’t result in a change to the media.

For drive self-erasure methods, the software has less knowledge of what actually occurred on the drive, so Xerase implements an additional step prior to the erasure known as Pre-Seeding. In pre-seeding, 100 random blocks are automatically written with a known data pattern (‘EPS ‘ in ASCII format) so that after the erasure we can look back at those blocks specifically and ensure that the data has changed. This gives us a good indication that the erasure process did in fact happen. This helps to confirm that the drive did what it claimed to have done in returning a good erasure status. These blocks are logged for documentation purposes. In addition, 2500 blocks spread over the entire media are automatically compared afterwards to document erasure success or catch failures that are in contrast to the status returned by the drive.

In addition, an extra verification pass is implemented at the end of most erasures. The nature of the verification pass is usually dictated by the setting in Customize->Interface->Erasure Settings->Verification Methods.

The Default verification method is a Spot Verify, logging a user-defined number of blocks randomly scattered over the surface of the disk. A value of 2500 blocks is a good number, but can be increased to 10000 or more if needed. While all blocks are checked, only 80 are logged unless errors are found.

The most thorough verification method is a Full Erasure pass. This reads the entire surface of the media and compares every byte to what is expected to be on the disk. As you would expect, this takes a fair amount of time under the best of circumstances, and if bandwidth limited can be a very lengthy process. We generally would only recommend this for point-to-point connections to the drive with no shared bandwidth such as in our Octane erasure stations.
A middle-ground is available in the form of the NIST Slice Verify method. In this method, the disk is broken up into a large number of slices, and each slice is verified independently in a pair of random sub-regions adding up to a given percentage. By spreading the verification over the entire surface of the disk, and reading a substantial amount from an unpredictable region, it is pretty much impossible to “game” the verification such as might happen if you only verified the first and last 1% of the disk as the status of 98% of the interior would be unknown. The NIST Slice Verify method is documented in the NIST 800-88 rev1 publication http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf beginning on document page 20.

Where verification is impossible (completely random data post Cryptographic Scramble) instead the software verifies that the blocks are all different in a Spot Verify method. True-Random Full-Verify and Slice Verify are not supported.