Update: 1/1/2016

SuperWiper® units erase data from digital storage media for reuse

"Digital" media today often store highly sensitive and confidential information. Once the information is no longer needed, the media must be erased in a manner that insures that all traces of information are completely removed and the data is no longer susceptible to viewing by sophisticated Forensic applications or electronics device.

There are several laws and regulations in the United States that require the sanitization of media even when the device is not intended for reuse. Examples of these laws and regulations include:

- Health Information Portability and Accountability Act (HIPAA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- FICA
- California Senate Bill 1386
- Sarbanes-Oxley Act (SBA)
- SEC Rule 17a

MediaClone's SuperWiper addresses the following two critical aspects of the sanitizing process:

- Overwriting the data multiple times utilizing different patterns.
- A Security Erase protocol, which utilizes specific hard drive OEM erase, commands to completely erase the data from the drives.

MediaClone's Erase Media Unit and solution supports the two main storage technologies (2 main classes):

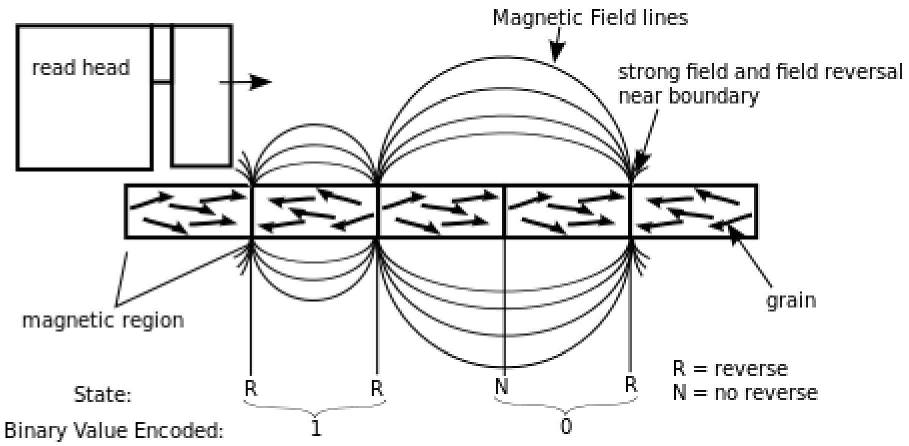
1) Hard Disk Drive (HDD)

These devices are used to store and retrieve "digital" information through use of very fast rotating disks (platters) which are coated with magnetic material. Data is stored to the HDD by magnetizing a small area on the platters (each area is known as a "bit"), which are described as "0" and "1". A group of bits is a bite and a group of bites is a block.

Data on the HDD is read with the use of magnetized heads arranged on a moving actuator arm which operates in a random-access manner, which means that individual blocks of data can be stored or retrieved in any order, not just sequentially. The HDD also has an internal controller and firmware (code) that controls the platters, the magnetic heads, and the physical action of reading and writing data to the HDD. Data is written onto the HDD when the “bit” area is magnetized with the magnetic headers. Data is then read by viewing the magnetized “bit” area.

Data stored to the HDD is not necessarily contained on a precise bit, but can overflow to more than one bit or to the area between two bits.

Data stored to the HDD can be captured with some electronic devices.



Hard Disk Drives come with different kinds of interfaces and communication protocols, including IDE, SCSI, SATA, SAS, FC (1394 with the use of a bridge 1394).

2) Multi Media Cards, PCIE memory cards, USB storage devices, Solid State Drives (all of which are based on NAND technology). There is a supplementary article written by a few experts in the area of Computer Forensic with SSD drives, that reader might find useful to read.

Two main eraser techniques exist today:

The first, Security Erase, is the best and fastest of the two techniques and can be used on all hard drives that support this OEM specific erase commands. Security Erase is not supported by SAS and not by USB protocols, adapters, devices. This technique is especially recommended for SSD drives. In the past, some “old” SSD had some issues with the internal firmware that was not performing internal erase very well, but all those issues have been resolved by SSD manufacturers.

The second eraser technique follows the DOD 5220-22M specs and employs a very long and tedious process that does not guarantee eraser on Class 2 media (SSD, etc.) when reallocation of the blocks results in data being hidden from the OS.

For magnetic media, like hard disk drives, a complete eraser of the data is also not guaranteed by rewriting the media multiple times, particularly where the reading magnetic heads of the rotating disks continue reading and writing to the same physical location of a single bit. But after 7 iteration of re-writing the media none of the residue of portion of a bit is really usable information. There are some that suggesting to run 32 iteration to really have a complete erase, but that can take forever.

Delete File: This process in the OS deletes an entry in a file from the File Allocation Table (different OS call the Allocation Table by different names) and indicates that the area is un-allocated and the location of the deleted file is ready to be reused. This process does not result in complete eraser of the data. Instead, the data remains on the disk until it is overwritten by another file. Until then, the data remains still accessible, even if a new file is written on the same area because slacks of information remain between the files that can be recovered.

Formatting Drives: The process only deletes the Partition Table that tells the drive controller and the OS where file are located on the disk. Formatting a disc does not erase the data, it is still there.

MediaClone’s SuperWiper Application Erase Operation

The SuperWiper application plays a critical role in insuring the complete eraser of data.

HPA/DCO is not set enable and it may leave data in un-allocated spaces of the drives.

Bad Sector handling: Company policies calling for the eraser of data and later disposal or reuse of drives may not realize complete eraser of data, particularly in skip bad sector settings or situations with skip bad blocks, all of which may result on some data remaining on the drive.

Advanced Drive Settings:
On the “Advanced Drive Settings” screen a number of options are shown. First and foremost, the default settings for all drives have the “HPA and DCO Support” box checked.

This is a very important feature that the user must be aware of.

Today's HDDs have built-in features that enable the user to resize the HDD from its native capacity. These features include:

HPA & DCO:

The default settings have the 'HPA & DCO' settings enabled, meaning that the erase operation will always erase the entire HDD ("entire" refers to the native size of the HDD). If the 'DCO/HPA' setting is disabled, the operation will only erase from the areas that were set by the DCO and HPA setting. This is not recommended.

Bad Sector Handling:

In the case of a bad sector or block, the user has the option to abort the drive (which is most recommended and physically destroy it by other methods), skip a sector, or skip a chunk of sectors (this setting is not applicable in Security Erase mode).

Modes of Erase Operation:

- **Full DoD Mode: - 8 passes.**
    - This mode erases data from the HDD with a procedure that meets the U.S. Department of Defense specification DOD 5220-22M
        - The process is performed in three iterations and two individual passes that completely overwrite the HDD. Each of the iterations makes two writes-passes
        - With the first iteration pass, the application writes "1111" (Hex 0xFF).
        - With the second iteration pass, the application writes "0000" (Hex 0x00)
        - After the third iteration pass, the seventh round writes the specific code "246" (Hex 0xF6, which is 11110110)
        - After the eighth iteration pass, the application reads the data back to verify that the pattern matches the last write
        - The DoD operation must run with abort bad sectors enabled

- **User Mode:**
    - If the "User" mode is selected, the user decides on the number of iterations, as well as the final erase pattern. Also the user have the ability to add as a last pass a full erase verification run as required by NIST certification. (Verification pass which is read pass over the drive is very important step, since drives may not

report an error while the application is trying to write data to the drive, but the errors will be discovered while reading the data back)

- User also can select to run a partial verification pass (Random 10%)

- **Security Erase Mode:**
  - This mode is not supported by USB storage devices or by SAS Hard Disk Drive. It only supports SATA hard disk drives
  - It is the best method to erase SSD and SATA drives
  - The 'Security' mode uses the 'Security Erase' protocols, where the unit's 'OS' sends commands directly to the HDD internal controller and to the HDD internal firmware. The OS does not perform any of the HDD erase procedures like in other erase modes where they re-write the tracks of the HDD. The 'OS' sends an erase initialization command to the internal firmware of the HDD, where the erase is done internally. The 'OS' waits to receive acknowledgment that the erase process is complete and will not respond to abort requests by the user in the middle of a 'Security Erase' operation.
  - There are two modes of Security Erase, the regular mode and the **Enhanced mode.** The main difference between the two is that the Security Erase regular mode overwrites all user data areas with binary zeroes, whereas the Security Erase enhanced mode writes pre-determined data patterns (set by the manufacturer) to all user data areas, **including sectors that are no longer in use due to re-allocation.**
  - In the "Erase Setting" screen, under the "Security Erase" option, there is an input box for Security Erase User password. The SuperWiper application sets the entered user password from the dialog box to the drive at the end of the Security Erase operation (That passcode is important if the security erase operation was terminated by a power shut down in the middle of the erase operation, than that passcode can be use later on to detect the drive). In addition if a drive has previously set with a passcode, and the user knows the passcode, he should input the passcode in this dialog box in order for the application to detect the drive.
  - **Security Erase Bad Sectors setting:** The setting as no affect.
  - **Security Erase Multiple drives in one session:** The application will report completion or fail on each drive, regardless of failures of other drives in the session

- **Verification Mode:**

- This mode is just verification that drive been erased by a third party applications of devices. The application compares the pattern from sector zero to the rest of the drive. user can run a full verification or random partial verification

S.M.A.R.T. drive test - Pre Erase operation:

User can use a few kinds of S.M.A.R.T. drive tests (if drives supported S.M.A.R.T. technology) to scan drive prior to erase operation in order to check the drive "health" condition and the failure prediction. Those tests might be very useful for user who intends to re-use drive.

There are 3 tests:

Short test: Can take 2-5 minutes; scan random area of the drive

Full Extended Test: Can take a few hours; scan the entire drive

Conveyance test: Test for drive failure after drive transportation

Erase certification:

NIST 800-88 guidelines are calling for erase and **verification** operation. Both DoD and Security Erase protocols been used by the SuperWiper units are compliance with the erase guidelines. User that use user erase mode with full verification is also in compliance. The SuperWiper application does generates NIST 800-88 recommended format for erase certification

S/W solutions application:

There are many software applications that use today for eraser drives. Most of them are depend on the host unit performances and they are not built to be used for mass erase operation

Compliance:

The SuperWiper units are with compliance with HIPA and other regulations