MediaClone, Inc. Introduces the SuperWiper™ - Erasure Data - Very Fast and Efficient Erasure from Multiple Storage Devices

MediaClone, Inc. is proud to announce the release of the SuperWiper™ - a Multi-Channel SAS/SATA and USB 3.0 Erase and Format Unit which is a very useful tool for any IT department, Computer Lab, and Computer Forensics Lab when erasure of sensitive data is needed or required by law.

Reseda, CA (PRWEB) August 07, 2014 -- SuperWiper™ - is a Multi-Channel SAS/SATA-3 and USB 3.0 Erase and Format Unit. It built with 8 SAS/SATA and 6 USB 3.0 ports, 8 open insertion drives tray, 8” Touchscreen color LCD display mounted on an elevated display pad that can be adjusted for height and viewing angle, without any network port for security reasons. The unit can erase SAS/SATA drives, USB storage devices, Multi Media Cards, and IDE hard disk drives.

The SuperWiper™ unit performs erase in extremely fast speed with average speed 8.2GB/min for a parallel run of 8 1TB WD Blue hard disk drives.

The SuperWiper™ application runs on Linux OS, which is a very secure environment. It can erase hard disk drives and storage devices following the DOD 5220-22M or ‘Secure Erase’ specifications. The ‘Secure Erase’ is especially recommended for the erasure of Solid State Drives (SSD) and flash drives. The unit’s application allows the user to efficiently run operations with maximum throughput on a number of erasure devices. The user can run a continuous erase mode, where each port operates as a separate and independent operation and with very little downtime, or the user can run a batch erase mode, where all the 8 hard disk drives run simultaneously. The unit also supports formatting of the following file systems: NTFS, FAT32, exFAT, EXT4(Linux), HFS+(Mac).

Data stored on media can contain very sensitive information that many times must be erased completely. The information must be erased without any trace, and without the ability for a smart Forensic application to capture even the smallest portion of information. “Sanitizing” of the media is needed even when the media is not intended on being reused. There are several laws and regulations that relate to data sanitization on data storage devices, including U.S. requirements imposed by the Health Information Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Documents Act (PIPEDA), Gramm-Leach-Bliley Act (GLBA), California Senate Bill 1386, Sarbanes-Oxley Act (SBA), and SEC Rule 17a.

Erase and Sanitize of data is not an easy process. Today’s media has a variety of different technologies, and each needs different handling when it comes to erasing data. From Hard Disk Drives (HDD) with magnetic disks, to Solid State Drives (SSD) with NAND technology, there are many ways to eliminate data from media. One can eliminate data by physical destruction like shredding and degaussing, by software applications that rewrite the media, and by using ‘Secure Erase’ protocols that utilizes special media internal erase commands.

“Data erasure appears to be very simple process, but it is actually pretty complicated and depends on the type of media that need to be erased. The end user needs to be able to rely on a good tool” says Ezra Kohavi, President and CEO of MediaClone Inc. “Our philosophy in designing this erasure unit was to provide the end user with the, most trustworthy unit that employs the highest quality of data erasure. To do this, we did incorporated several new proprietary features in the design of the SuperWiper™”
http://www.media-clone.net/SuperWiper-Erase-and-Format-unit-p/swp-0001-00a.htm

Contact Information
Ezra Kohavi
MediaClone, Inc
http://www.media-clone.net
+1 818-654-6286

Online Web 2.0 Version

You can read the online version of this press release here.