MediaClone, Inc. 6900 Canby Ave, 107, Reseda, CA 91335 email: info@media-clone.com, web: www.media-clone.net

White Paper MediaClone on Data Erase Tools 2021 – how to select the right vendor and the right erase tools

Erasing data from a digital storage is essential to secure sensitive information stored on it before the storage device is discarded or recycled for reselling purposes. For example, if you are a healthcare provider, the data needs to be erased with no possibility of retrieving even a single bit of information by the data privacy law established by the government.

On the surface, it seems like a simple task to erase the data, but it is much more involved.

Here are several points to consider when you need to erase a storage medium and are searching for data erasing tools and solutions:

- Software vs. Hardware Solution
- OS – select the right one
- Hard Disk Drives vs. Solid State Drives (SSD), the main difference when it comes to erase
- Erase Protocols – most solutions support multiple protocols, which one to select?
- Hardware Configuration and Media Storage Support – cover as many as possible
- Reporting Capabilities – NIST guidelines
- R.2 requirements for electronic recycling centers
- Bad Sectors Handling – trapped sensitive information
- Dealing with Special Storages – Netapp
- Selecting and Optimization of the hardware – get the maximum out of your investment
- Application and Ease of Use – use untrained, low-cost workforce
- Support – Advantage of local US
- Quality and Reputation

Software vs. Hardware Solution:

There are many available software solutions in the market; some are even free. It makes sense to use those solutions when you need to erase just a few drives. In general, any software solution needs to interface with a physical drive and will need some hardware. That hardware can be your

PC, Laptop that you might have to customize to connect those drives – so it can be a messy situation.

Alternatively, you can build your drive array server using erase software with a licensing scheme charged per erased drive. Usually, those drive arrays are not easy to operate and are not built for many drive insertions daily. The erase licensing can also be very costly, and large corporations can pay $50-100k per year.

To get consistent results, the most efficient economical solution geared to erase a large number of drives simultaneously, you may want to look at a standalone hardware solution that supports the latest storage technologies.

The Erase Standalone Hardware Solutions are very secure since they do not have to connect to a network or internet. Look at those solutions that are very efficient with running multiple erase sessions simultaneously, making it economical and flexible to accommodate different types of data storage drives, various form factors, and various digital storage technologies.

Remember that some of the standalone erase solutions use an embedded processor to lower the cost. Those usually cannot give a good erase performance and compete with the latest processors in the market. In addition, look for a solution that is flexible to adapt to new technologies. With the embedded solution, everything is hardcoded in a very rigid design.

OS:

One of the most efficient OS with very little overhead is Linux – so avoid erase units that running Windows.

Hard Disk Drives vs Solid State Drives

Hard Disk Drives: built from mechanical magnetized platters to store the data. It contains a spinning platter with a thin magnetic coating. A "head" moves over the platter, writing 0's and 1's on tiny areas of the magnetic platter. They have been very successful in large capacity, but they exhibit a few challenges. They have limited access speed because of the magnetic head's mechanical movement and therefore limited erase speed (max erase speed of 11 Gb/s). When it comes to data erasing, there is always a chance that some bit of data was not fully de-magnetized ("bad" sector), and therefore multiple erases passes over the drive are needed - which means more time to erase to make sure no bit is left behind. Also, for some of those drives, the only erase method available is rewriting the media, which can take a long time.

So there are challenges in erasing a Hard Disk Drive. For example, DoD developed some extensive guidelines on how to erase those drives, it involves rewriting the hard disk drives seven times, each

time with a different pattern of filling data to ensure that data is scrambled even in the weak/"bad" sector. DoD Erase is a very long process that is not necessarily the most optimized but is typical for hard disk drives (see below for other methods).

SSD are "logical" drives, built with solid-state technology, they store information on flash memory chips, so they contain no mechanical moving parts, and therefore memory access speed is much higher. The most efficient way to erase data from an SSD is to let the internal firmware of the SSD do the job. The erase speed is very high. SSDs have become very popular in the market place, but their main disadvantages are higher cost, limited capacity and lifespan.

There are four main kinds of SSDs: SATA, NVME, USB, and SAS. The challenges to erase an SSD are different. Now a “bit” of data is just logical gates (there is no area around the physical bit like in hard disk drives that pose issues), so turning a bit on and off is a 100% success. If there are “bits” that are not functioning, the f/w of the SSD remaps them, and they become not available to the user. The Erase is very quick and erase methods can be rewriting the media – not efficient, security erase – very efficient, or encrypt the data and throwing the encryption key away.

Erase protocols:

There are many erase protocols to be used, and a good erase solution does support many of them! In general some erase protocols are tailored to the media.

For example NVMe tools are designed to deal with NVMe media; Sanitize is designed to deal with SAS SSDs, Secure Erase and Enhance Secure Erase are designed to deal with SATA drives.

The methods that use the capabilities of the drive firmware to do the erase are fast and most efficient.

Beside that, there are the DoD and DoD Lite erase protocols that erase the media by overwriting it multiple times. This method is essential for erasing older SCSI/FC/SATA drives where no other options are available.

Some companies or agencies have guideline/restrictions to use only the DoD erase protocols because they support deep cleaning (7 passes over the drive) of Hard disk Drive with magnetic platters to ensure that every single bit of data is completely erased.

NIST: Advocates for Security Erase OEM erase protocols. In general the NIST guideline is that does not matter how you are going to erase the data, just make sure to run one pass of erase verification over the drive. That is needed because the erase application can send a command to write zero to a certain bit on the drive, but if that particular bit is weak or not magnetized, the “zero” will not be written and there will be no indication for it, unless the application reads that status of bit back in

verification pass. As for the erase protocols that use a drive's internal firmware to erase the drive, the read verification can be important if something happened to the hardware that erases the drives! So the bottom line is that you can use any erase protocol you wish or instructed to, just make sure that you do select to run one pass of verification.
To select erase protocols, the best practice is first to understand the media you are trying to erase, and which protocols are supported by it. For example USB flash drives do not support Security Erase and the only methods to erase them are DoD, DoD Lite, or User Defined erase modes.
User Erase mode: Can be used when the user just wants to erase the media by overwriting, and to be qualified for the NIST800-88 certificate the user will need one pass of erase with any pattern and one pass of verification.

Hardware configuration:

Have a look at erase solutions that support or can support as many different kinds of storage devices and can adapt to new ones.
The primary digital storage devices that are in use today are:
SAS, SATA, USB, NVMe
The legacy storage devices:
SCSI, FC, 1394, IDE
For Apple: Have a look for erasing solution that are able to connect to a laptop via 1394A/B and Thunderbolt 2.0 and 3.0
Technologies: Hard Disk Drives, SSDs & flash drives
Form Factors: 3.5", 2.5", M.2 (different length and different technologies SATA / NVMe), ZIFF, MSATA, MicroSATA, Apple NGFF, PCIE memory cards, U.2 (NVMe)

(**NVMe** comes in 3 types: PCIE Memory card – needs a special adapter to connect to a U.2 port or plug directly to a PCIE slot, M.2 type with M.2 to PCIE, or M.2 to U.2 adapter, U.2 68 pin SFF-8639 port – look like 2.5")

Standalone Erase Hardware Solution with many ports gives the user ability to run multiple drives simultaneously, so the more ports you have the better. But usually, the erase speed reduces when you run too many concurrent sessions. So there is an optimum.

Reporting capabilities:

Have a look at erase solutions that enable you to customize the NIST 800-88 certificate by adding detailed info on the erase job and the erase media.
In addition, see if the solution provides a detailed log with information on the drive, the erase session, and the S.M.A.R.T diagnostics quick health test of the drive.

Bad sector handling:

Have a look at erase solutions that enable you to select which method to use when the erase application encounters bad sectors (areas) on the drive.
It is a crucial point if you intend to erase data for security reasons. It mostly applies to Hard Disk Drives, where some magnetized areas on the platter are not readable anymore. The drive will try to relocate the bad sectors, and the user will not be able to access them anymore. When the reallocation sector count increases significantly, it is usually a sign that the drive will fail soon.
Some erase applications allow the user to control the bad sector handling by skipping the "bad" areas and continue with the erase operation (taking a risk that some data remains) or by aborting the erase operation (assuming that after that the user will physically destroy the drive).

R.2 requirements for recycling centers:

Occasionally there is some confusion between the erase products and the facility that uses them. R.2 and other recycling centers certification bodies require the electronic recycling facility to be certified and audited. The erase tools need to support self-calibration and they need to be calibrated every year.

Dealing with special media:

Have a look at erasing solutions that support erasing non-standard media.

Netapp drives use proprietary firmware to secure their storage solutions. They also format the drive with 520 bytes per sector (the standard is 512), and they use special storage controllers to communicate with these drives.

Erasing those drives poses a significant challenge. A standard Windows-based PC will not recognize those drives. Some advanced techniques are needed. Even if the user tries to formats the drives back to 512, the drives might become unusable because of its special f/w. For some drive model, the

special f/w can be replaced with an OEM version, but that is risky and has only a small % of success (provided the OEM firmware is available)

Selecting and optimizing of the hardware

How to select the right products:
What erase protocol you would like or must use (DoD, or proprietary OEM f/w erase method)
Type of storage: Make sure your erase machine supports the media that you intended to erase. Some storage devices need additional adapters, so make sure you have the right one.
Also, the main unit's USB ports can be converted to SATA ports in order to maximize the usage of the hardware solution.
Be aware that NVMe SSDs require special built-in hardware.
Volume – How many drives do you need to erase per month (take into account the erase protocols that you are going to use and the erase speed, like NVMe, erase tools are extremely fast. So even if you have a large number of drives, it is not going to take long to erase them and you might need less NVMe ports).

Select an application that is easy to use

How to select the right product – application aspect:

- An application that is intuitive and easy to use.
- An application that uses touchscreen icons.
- An application that even an untrained person can comprehend and use and can be up and running in a few minutes.
- An application that allows the user to run a continued erase operation with no downtime. Each port acts as independent of others, and when the erase operation is completed on a port, the user can plug a new drive and start a new erase operation.
- An application that allows the user to run multiple erase sessions simultaneously utilizes every available port.

Supports

Read customer reviews about the company's tech support.
Are they local or overseas? Are they a low cost solution?
USA local support gives the user a better chance to solve issues quickly, whether it is a hardware or software issue. There is a saying "things happen", but it all depends on how they are handled.

For the OEM to be local is a huge advantage since it avoids language barriers, time zones and supports concepts.

Check the Quality and Reputation:

Check the quality of products:
What is the customer experience using it and interacting with the OEM?
How long does the product last in the field?
What is the product failure rate?

I hope that is helping you to evaluate a vendor and its erase tools and help you to select the right solution for you

Ezra Kohavi
MediaClone, Inc.