BitRaser
Quick Start Guide 1.0

Introduction

What is BitRaser?

BitRaser is a portable and reliable application providing permanent data erasure of storage device. This application erases data in order to prevent recovery of sensitive data that is no more required. Many organizations and users, while formatting their hard drives, still found an open possibility of data being recovered. BitRaser solves this problem efficiently by using powerful algorithms that fill the storage device with useless binary data. This leaves no possibility of data being recovered.

What is disk wiping and how it works?

Disk wiping is the process of permanently deleting data from a hard disk. In it's simplest form, a disk wiping algorithm will write all zeros, but in more advanced algorithms, a combination of filling up a disk with random data (either 1s or 0s) plus multiple passes to ensure the impossibility of retrieving data from a wiped disk.

Key Features of BitRaser

- Option to boot from either a USB dongle or CD/DVD.
- Supports up to 32 hard drives for simultaneous erasure.
- Supports erasure of IDE, SATA, SCSI hard drives SSD, Flash drive, USB drive.
- Displays SMART information of connected IDE and SATA hard drives.
- Software allows you to customize reports and erasure certificate with an option to save reports in PDF, XML or HTML format.
- Equipped with 19 world class wiping algorithms with 3 options of erasure verification (No verification, Random verification and Total verification).
- Support to read and write ATA commands.
- Support for HPA/DCO detection and removal.
- Support to add custom erasure method (upto 5).

- NIST Compatible Certificates.
- Support to provide Pre Report Information and Asset Tag before the erasure process.
- Support for Bad Sector customization.
- Support for Certificates with annexure.
- Auto saving of report and certificate on dongle.
- Various setting like permanent custom images for all session.
- All settings saved for all session on dongle.
- Support to install device driver from external source.

System Requirements

Before you start installing the BitRaser, ensure that your computer meets the following requirements.

Hardware Requirements

- x86 or x64 Processor
- RAM: Minimum 1 GB, recommended 2 GB
- USB PORT 2.0 / 3.0, with an option in the BIOS to boot computer from USB device, if you are using USB to boot your computer.

Requirements to erase a drive on System are listed below

- Bootable CD / USB to erase system media.

How to Prepare Boot CD

If your system does not boot with the hardware lock, you can then boot it from a CD. BitRaser comes as a bootable ISO image which can be downloaded from the download link. This image needs to be written on to a recordable CD in order to use this application. In order to successfully prepare a bootable disc from ISO image you need to make sure that you have a recordable CD, a CD writer drive and CD burning software installed in your computer.

Steps to burn image on to a CD are described below (these steps are generic and may differ from the steps of your CD writing software):

- Insert a blank CD in your system's C-RW or DVD-RW drive.
- Right-click on ISO file and select the option '**Open With**'. Select the CD burning software from the list displayed.
- Select the CD-RW or DVD-RW recorder
- Select writing speed.
- Click CD Burning button of the software.
- The bootable CD created can be used to wipe the desired drive on the client machine.

Note: If you have BitRaser hardware lock, you can directly boot your system with the hardware lock. In this case you don't need to prepare boot CD.

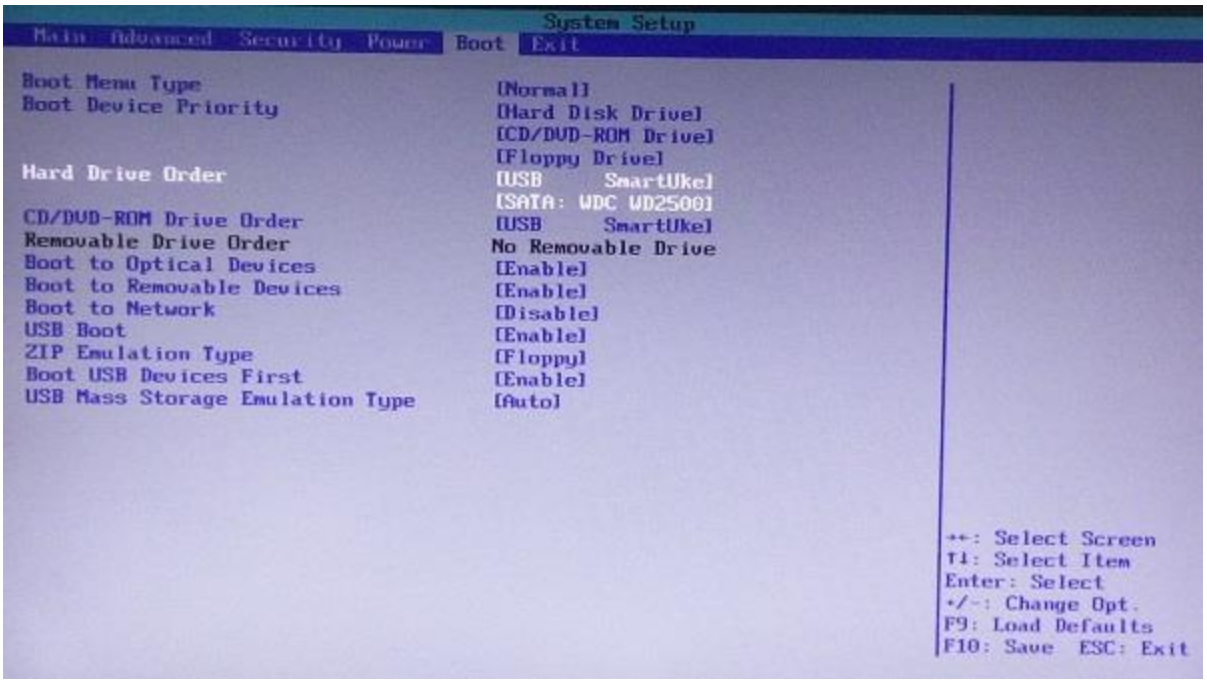
How to Boot From BitRaser Device?

BitRaser device is a complete solution to wipe data from multiple hard drives simultaneously. It comprises of 2 partitions. The first partition is a virtual CD that has a bootable image to boot your computer and second partition is a bootable USB thumb drive. You can choose either of the options to boot your computer.

Steps to boot your computer using this BitRaser device, either from the CD or USB device:

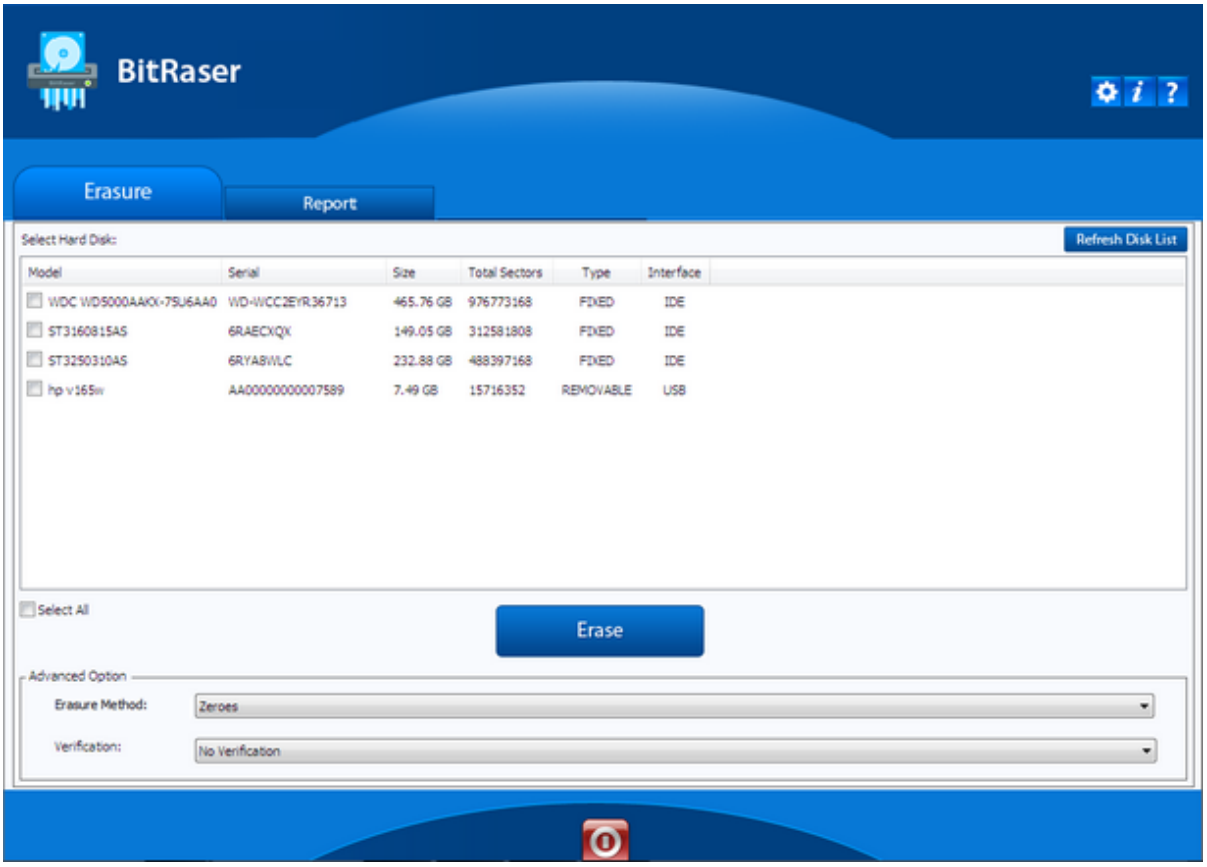
1. Restart your computer and wait for the first screen that shows up when you boot. At the lower right position of your screen you will see the key you need to press in order to enter either the Boot Menu or BIOS Settings.

2. Press the noted key on your keyboard and wait for setup to start.
3. If case you have selected BIOS, you will be prompted to a System Setup screen. Among all the available tabs, select Boot tab.



4. In '**Boot Device Priority**' set **USB SmartUke** as first priority to boot and hit <**F10**> function key to save changes and exit BIOS.
5. After saving your changes, Exit out of your BIOS and reboot your computer. Make sure that BitRaser device is attached to your computer.
6. Once you are done with rebooting process, your computer will start booting from your preferred device. Following screen appears:

7. And finally, after the system booting gets completed, you will see the BitRaser running on your screen as shown below:


BitRaser
Erasure
Report
Select Hard Disk:
Refresh Disk List
Model
Serial
Size
Total Sectors
Type
Interface
WDC WD5000AAKX-75U6AA0
WD-WCC2EYR36713
465.76 GB
976773168
FIXED
IDE
ST3160815AS
6RAECXQX
149.05 GB
312581808
FIXED
IDE
ST3250310AS
6RYA8WLC
232.88 GB
488397168
FIXED
IDE
hp v165w
AA000000000007589
7.49 GB
15716352
REMOVABLE
USB
Select All
Erase
Advanced Option
Erasure Method:
Zeroes
Verification:
No Verification

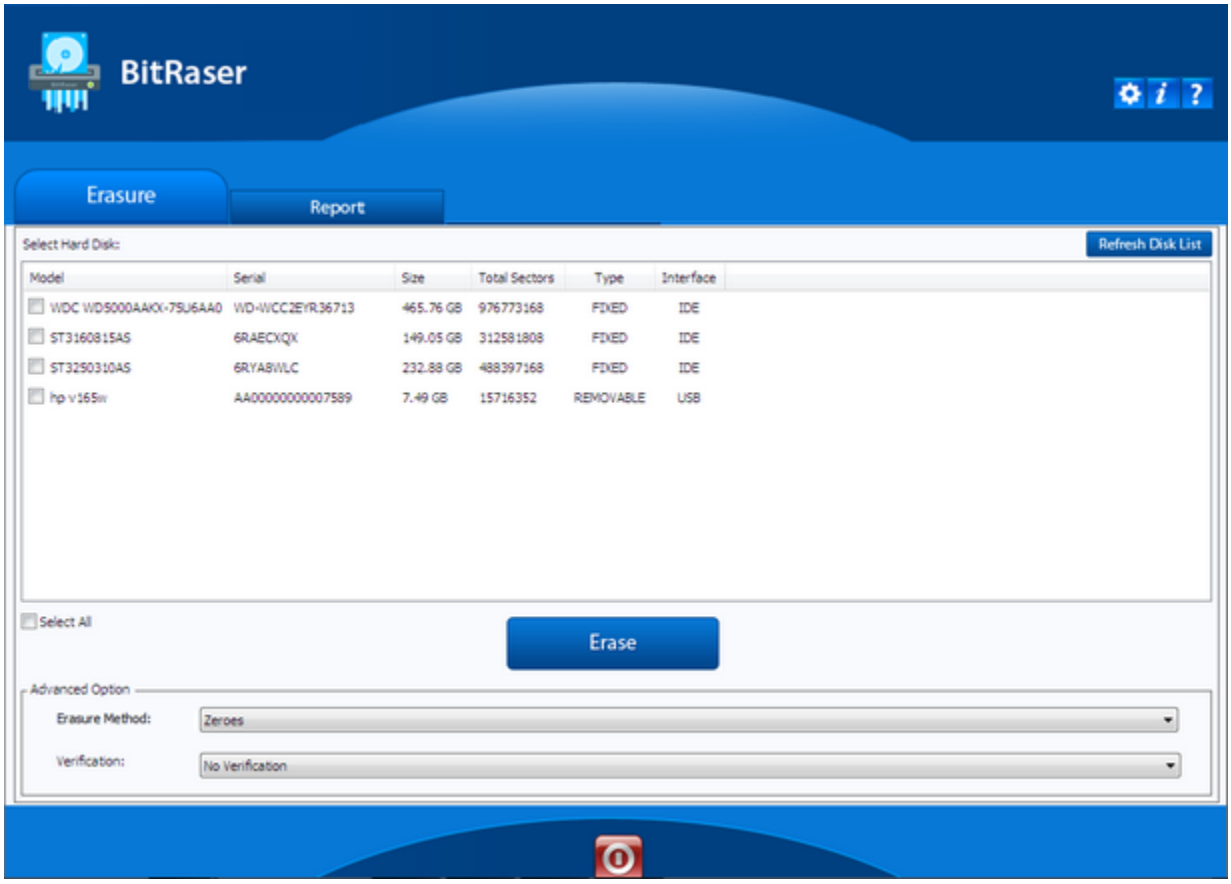
How to Erase?

You can securely wipe data from your hard drive / pen drive by using erasure feature of BitRaser. You can choose a wiping algorithm from a list of 19 data wiping algorithms. Selection of wiping algorithm is available under Advanced Options section. Also, 3 verification options are available to you in order to verify that the data has been wiped permanently and is no longer recoverable.

Note *You can wipe up to 32 hard drives simultaneously using BitRaser.*

To erase / wipe data using BitRaser:

1. Run BitRaser. The Erasure tab (which is selected by default) will list all the attached storage devices.

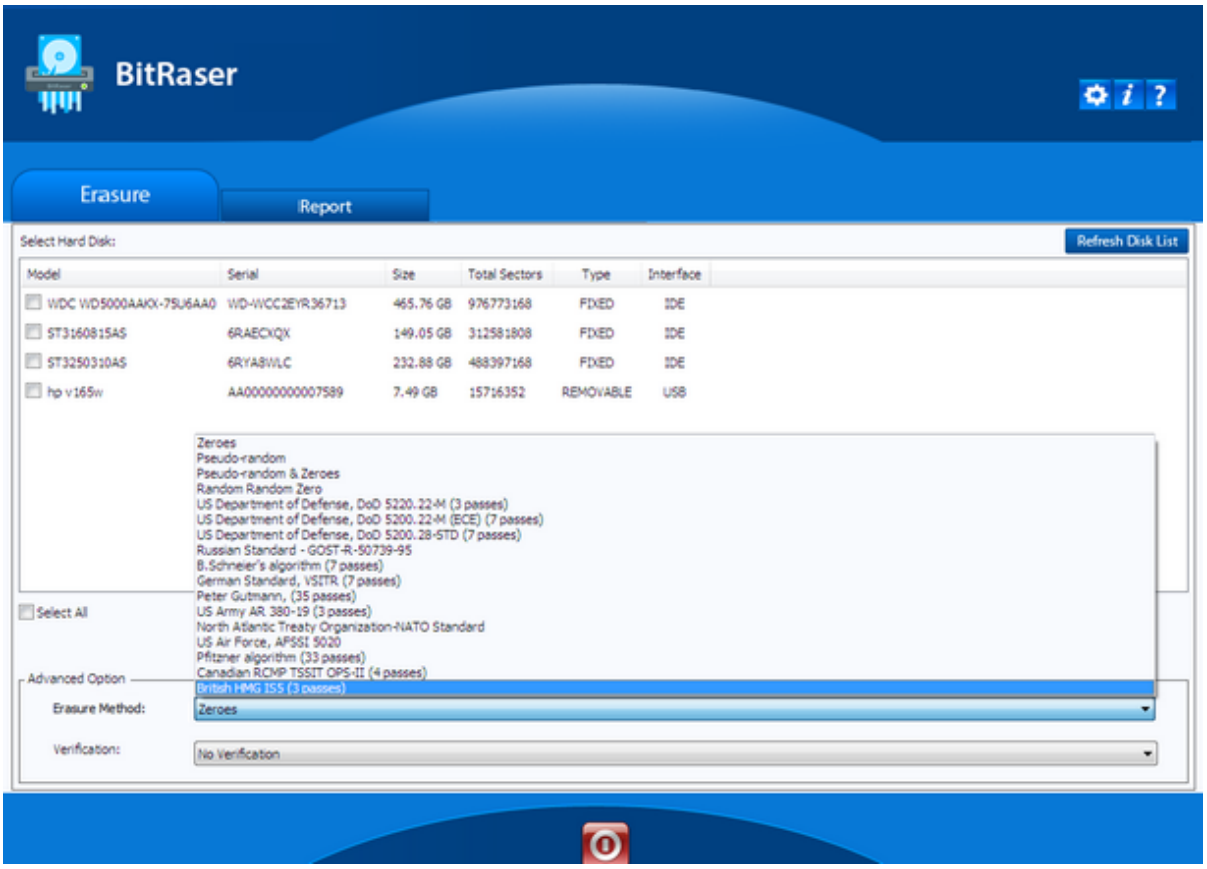


2. All storage devices along with their information like model number, serial number, storage capacity, total sectors, type and interface are displayed.
3. Select storage devices you want to wipe by marking the check box before every storage device.

Note *Mark Select All option to select every listed device for wiping.*

---

4. From Advanced Option section, select any one of the following wiping algorithms:

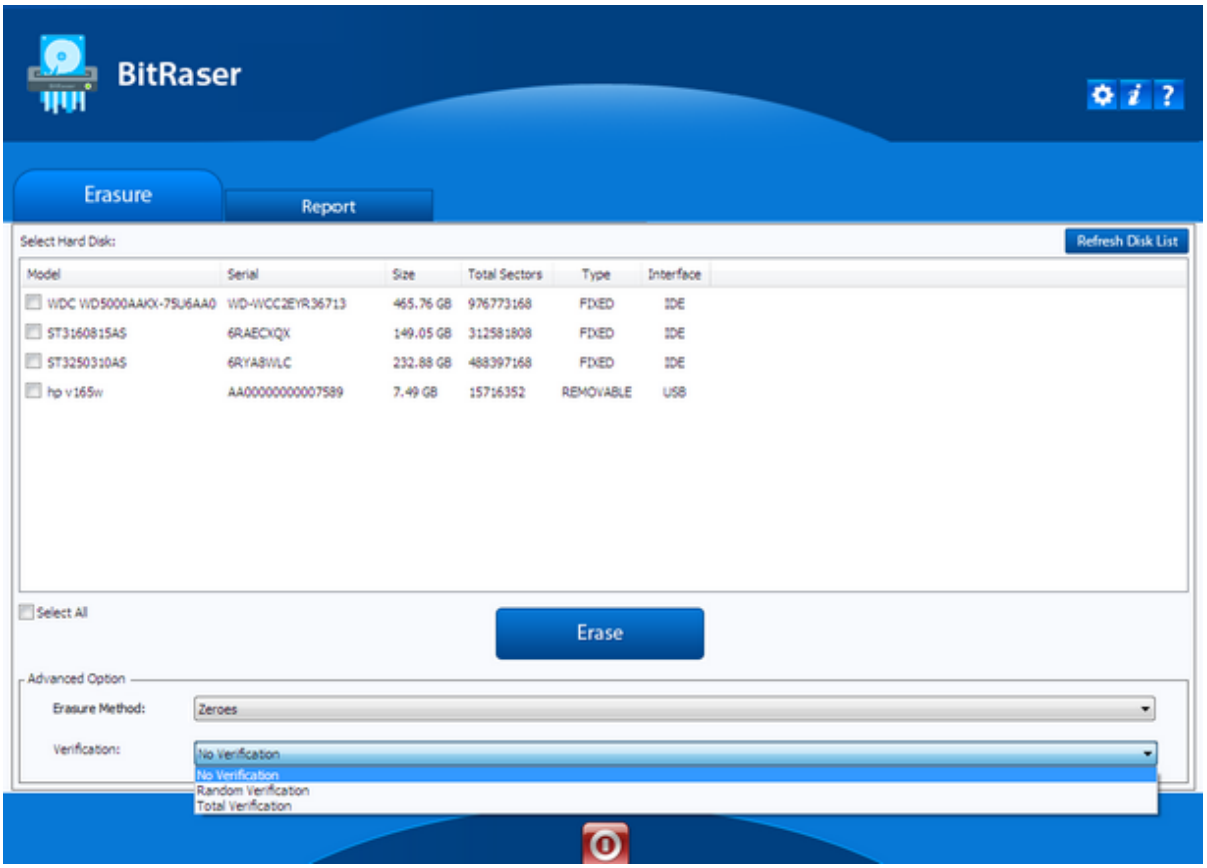


Wiping Algorithm	Description
Zeroes	This algorithm wipes data by overwriting it with zeroes in a single pass. This is the fastest algorithm available to a user.
Pseudo-random	This algorithm wipes data by overwriting an entire hard drive with randomly generated numbers in a single pass.
Pseudo-random & Zeroes	This algorithm wipes data by overwriting the hard drive in two passes. In first pass, it overwrites data with randomly generated numbers and in second pass it overwrites the previously generated data with zeroes.

Random Random Zero	This algorithm wipes data by overwriting a storage media with random characters in a multiple passes.
US Department of Defense, DoD 5220.22-M (3 passes)	This algorithm wipes data by overwriting the hard drive in three passes. In first pass, it overwrites data with zeroes, then in second pass, it overwrites the data with ones and finally in the third pass overwrites the data with randomly generated bytes. This is a U.S. Department of Defense algorithm.
US Department of Defense, DoD 5200.22-M (ECE) (7 passes)	This algorithm wipes data by overwriting the hard drive in seven passes. The first, fourth and fifth pass is overwriting with a random byte, its 8 right-bit shift complement and 16 right-bit shift complement; second and sixth passes are overwriting with zeroes, and third and seventh pass with random data. This is a U.S. Department of Defense algorithm.
US Department of Defense, DoD 5200.28-STD (7 passes)	This algorithm wipes data by overwriting the hard drive in seven passes. In first two passes, it overwrites data with certain bytes and their complements, then in next two passes it overwrites data with random characters. In fifth and sixth passes, it overwrites data with a character and its complements and finally, it overwrites data with random characters. This is a U.S. Department of Defense algorithm.
Russian Standard - GOST-R-50739-95	This algorithm wipes data by overwriting the hard disk with zeroes followed by a single pass of random characters.
B.Schneier's algorithm (7 passes)	This algorithm wipes data in seven passes. In the first two passes, it overwrites the hard disk with ones and then zeroes and in next five passes, it overwrites data with random characters.
German Standard, VSITR (7 passes)	This algorithm wipes data by overwriting data with three alternating patterns of zeroes and ones and then a last pass which overwrites data with random characters.
Peter Gutmann, (35 passes)	This algorithm wipes data by overwriting it 35 times, making recovery of the wiped data by any tool impossible. This algorithm takes more time than other wiping algorithms.
US-Army AR 380-19 (3 passes)	This algorithm wipes data by overwriting the media in three passes. In the first pass, it overwrites data with random bytes, then in second and third pass, it overwrites data with certain bytes and their complements. This is a U.S. Army algorithm.
North Atlantic Treaty Organization-NATO Standard	This algorithm wipes data by overwriting the media in seven passes. From pass one to six, it overwrites the data with a number and its complement alternatively. Then, in the final pass, it overwrites data with random characters.

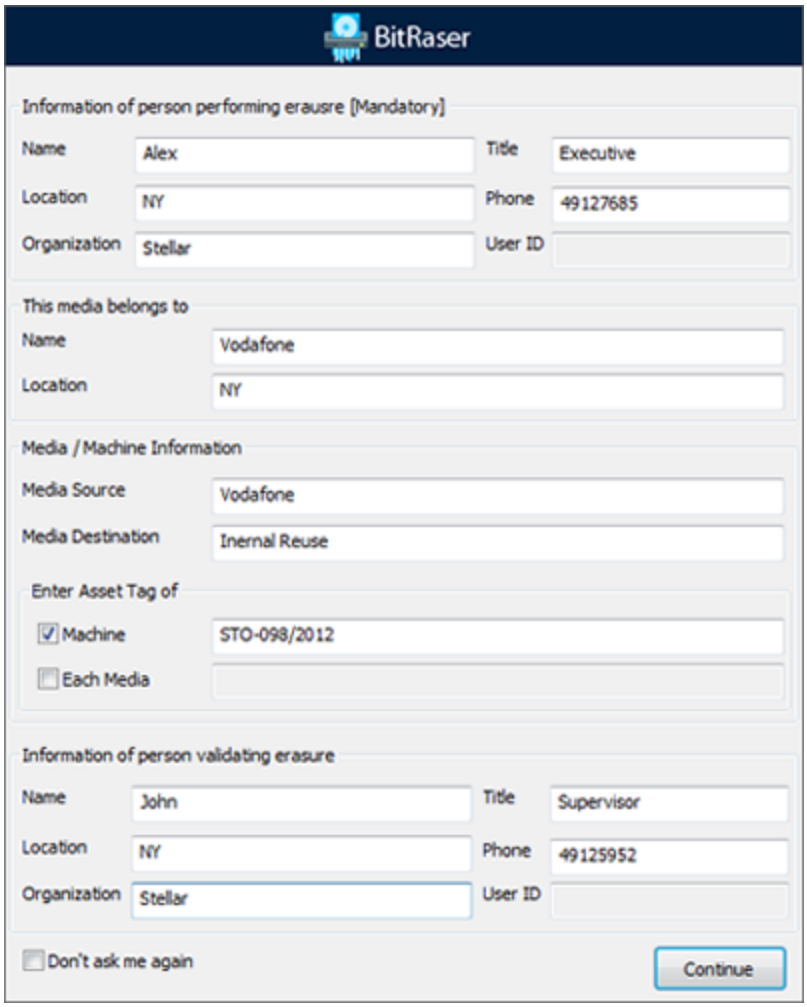
US Air Force, AFSSI 5020	This algorithm wipes data by overwriting the media in three passes. First, it overwrites with zeroes, then with ones and finally with random characters.
Pfitzner algorithm (33 passes)	The Pfitzner algorithm is a used in file shredding and data destruction programs to overwrite existing information on a hard drive or other storage device. All the passes in Pfitzner method consists entirely of random overwriting of data in the storage device.
Canadian RCMP TSSIT OPS-II (4 passes)	This algorithm is a four pass overwriting algorithm with alternating patterns of zeroes and ones and the last pass - with a random byte.
British HMG IS5 (3 passes)	This algorithm is a three pass overwriting algorithm, first pass - with zeroes, second pass &endash; with ones and the last pass with random data.
NIST Clear	This algorithm overwrites media by using organizationally approved and validated overwriting technologies/methods/tools.
NIST ATA Purge	Apply the ATA Secure Erase command. The sanitize command is preferred to Secure Erase when the sanitize command is supported by the device.
Custom Methods	This algorithm is added by the user. User can create upto 5 custom erasure methods.

5. Next from Advanced Option section, select any one of the verification methods:



Verification Methods	Description
No Verification	No verification is done after the media is wiped.
Random Verification	Random verification of the storage device is done after the wiping operation, that is, randomly selected sectors of the storage device are verified after wiping operation.
Total Verification	Total verification verifies all the sectors of the storage device after the wiping operation is completed.

6. Click Erase to start wiping the storage device.
7. An **Asset Tag** menu is displayed as shown below.



8. **Asset Tag** menu contains fields for information about the person performing the erasure, media, machine and person validating the erasure.
9. Checking the **Don't ask me again** field would disable the **Asset Tag** menu when you perform any erasure process thereafter.
10. Enter the required information in the respective fields and click Continue.

Note: The Asset Tag details are saved in the BitRaser hardware lock. If you boot any system with the same lock, the asset details are fetched from the lock automatically.

Note: Information of the person performing erasure is mandatory.