ZDelete

USER MANUAL

Ver. 9.0.6

Updated: 21 Apr 2020

Contents

Legal Statement

LSOFT TECHNOLOGIES INC. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of LSOFT TECHNOLOGIES INC. to provide notification of such revision or change.

LSOFT TECHNOLOGIES INC. provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. LSOFT may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

All technical data and computer software is commercial in nature and developed solely at private expense. As the User, or Installer/Administrator of this software, you agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

`Active@ ZDelete`, the `Active@ ZDelete` logo and `ZDelete` are trademarks of LSOFT TECHNOLOGIES INC.

LSOFT.NET logo is a trademark of LSOFT TECHNOLOGIES INC.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

End-User License Agreement

`Active@ ZDelete 9`

Copyright(c) 1999-2020 LSoft Technologies Inc. All Rights Reserved.

END-USER LICENSE AGREEMENT

IMPORTANT! READ CAREFULLY: This *End-User License Agreement* ("EULA") is a legal agreement between you (either an individual or a single entity) and *LSoft Technologies Inc*. for the `ZDelete` later referred to as '*SOFTWARE*'. By installing, copying, or otherwise using the *SOFTWARE*, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the *SOFTWARE*.

LSoft Technologies Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

SOFTWARE LICENSE

Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the *SOFTWARE*. The *SOFTWARE* is licensed, not sold.

1. GRANT OF LICENSE. This **EULA** grants you the right to install and use one copy of the *SOFTWARE* or any prior version on a single computer; a license for the *SOFTWARE* may not be shared or used concurrently on different computers.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on reverse engineering, recompilation, disassembly, modify, translate *SOFTWARE*, make any attempt to discover the source code of the *SOFTWARE*.

3. RENTAL. You may not rent, lease, or lend the *SOFTWARE*.

4. DISCLAIMER OF WARRANTY. This *SOFTWARE* and the accompanying files are provided "as is" and without warranties as to performance or merchantability or any other warranties whether expressed or implied. You use the *SOFTWARE* at your own risk. No liability for consequential damages. To the maximum extent permitted by applicable law, in no event shall the *Lsoft Technologies Inc*. or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this *SOFTWARE*, even if *Lsoft Technologies Inc*. Has been advised of the possibility of such damages. In any case, the *Lsoft Technologies inc.* entire liability under any provision of this **EULA** shall be limited exclusively to product replacement.

Lsoft Technologies Inc. reserves all rights not expressly granted here.

Introduction

An overwhelming majority of people, businesses and organizations do not understand the importance of security in digital data storage. An average hard drive stores thousands of files written on it and many of them contain sensitive information. Over the course of a hard drives lifetime the likelihood for *recoverable* remnants of sensitive information left on a drive at its end of life is very high.

Advanced Data Recovery Systems

Advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped and disassembled. Security agencies use advanced applications to find cybercrime related evidence. Also there are established industrial spy agencies using sophisticated channel coding techniques such as *PRML* (*Partial Response Maximum Likelihood*), a technique used to reconstruct the data on magnetic disks. Other methods include the use of magnetic force microscopy and recovery of data based on patterns in erase bands.

Although there are very sophisticated data recovery systems available at a high price. Almost all the data can also be easily restored with an off-the-shelf data recovery utility like Active@ File Recovery, making your erased confidential data quite accessible.

Using `ZDelete` all files on your hard drive or removable device can be destroyed without the possibility of future recovery. After using `ZDelete` the process of disposal, recycling, selling or donating your storage device can be done with peace of mind.

Related information

Using ZDelete on page 9

Erase Disk Concepts on page 19

Erasing Confidential Data

Modern methods of data encryption are deterring network attackers from extracting sensitive data from stored database files.

Attackers (who want to retrieve confidential data) become more resourceful and look for places where data might be stored temporarily. For example, the Windows **DELETE** command merely changes the files attributes and location so that the operating system will not look for the file. The situation with *NTFS* is similar.

One avenue of attack is the recovery of data from residual data on a discarded hard drive. When deleting confidential data from hard drives, removable disks or USB devices, it is important to extract all traces of the data so that recovery is not possible.

Most official guidelines regarding the disposal of confidential magnetic data do not take into account the depth of today's recording densities nor the methods used by the OS when removing data.

Removal of confidential personal information or company trade secrets in the past might have been performed using the **FORMAT** command or the **FDISK** command. Using these procedures gives users a sense of confidence that the data has been completely removed.

When using the **FORMAT** command Windows displays a message like this:

```
Important: Formatting a disk removes all information from the disk.
```

The **FORMAT** utility actually creates new *FAT* and *ROOT* tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced *FAT* and *ROOT* tables is stored so that the **UNFORMAT** command can be used to restore them.

FDISK merely cleans the Partition Table (located in the drive's first sector) and does not touch anything else.

Related tasks

Erase Files on page 9

Related information

Erase Disk Concepts on page 19

Wiping Confidential Data

You may have some confidential data on your hard drive in spaces where the data is stored temporarily. You may also have deleted files by using the *Windows Recycle Bin* and then emptying it. While you are still using your local hard drive there may be confidential information available in these unoccupied spaces.

Note: Wiping the logical drive's deleted data does not delete existing files and folders. It processes all unoccupied drive space so that recovery of previously deleted files becomes impossible. Installed applications and existing data are not touched by this process.

`ZDelete` wipes unused data residue from file slack space, unused sectors and unused space in MTF records or directory records.

Wiping drive space can take a long time, so do this when the system is not being actively used. For example, this can be done overnight.

Related tasks

Wipe Drive on page 12

Related information

Wipe Disk Concepts on page 20

International Standards in Data Destruction

`ZDelete` works with more than **20** international standards for clearing and sanitizing data including the US DoD 5220.22-M standard. You can be sure that once you erase a disk with `ZDelete` all the sensitive information is destroyed forever.

Related information

Erase & Wipe Methods (Sanitation Standards) on page 23

ZDelete Overview

Active@ ZDelete

ZDelete is a data cleanup and erase utility that can delete selected folders and groups of files without any possibility of data recovery afterward. Access to the drive's data is made on the physical level via **BIOS** (*Basic Input-Output Subsystem*) bypassing the operating system's logical drive structure organization.

ZDelete is designed to help protect your privacy by deleting files in such a way as to prevent other people from recovering your private data after deletion. Its integrated Disk Wipe can clear out all free space on a hard disk so that recovery of deleted files becomes impossible. It is a powerful and flexible data shredder for information that must be permanently directed away from the hard drive.

ZDelete is a powerful software that delivers the following main features:

- Destroy data permanently with a choice of **20+** international disk sanitizing standards including US DoD 5220.22-M
- Sanitize external disks (USB drives, external HDD/SSD) connected to both USB 2.0 and 3.1 ports
- Wipe out unused clusters and metadata on live volumes, leaving existing data intact, cleaning up free and slack space according to the concepts
- Windows *Drag-and-Drop* functionality
- Graphical User Interface integrated with Windows Explorer
- Functions reside in context command menus
- ZDelete Bin - familiar, comfortable and reliable erasure mechanism

Related information

Erase & Wipe Methods (Sanitation Standards) on page 23

System Requirements

`ZDelete` is designed to run on Windows operating system with the following minimum requirements:

Workstation

- IBM PC compatible machine
- Intel Pentium or higher
- 2 Gb of RAM
- 50Mb of free disk space

Video

- VGA (1024x768) resolution or better

Operating Systems

- Windows XP or higher

Drive Storage

Disk types supported:

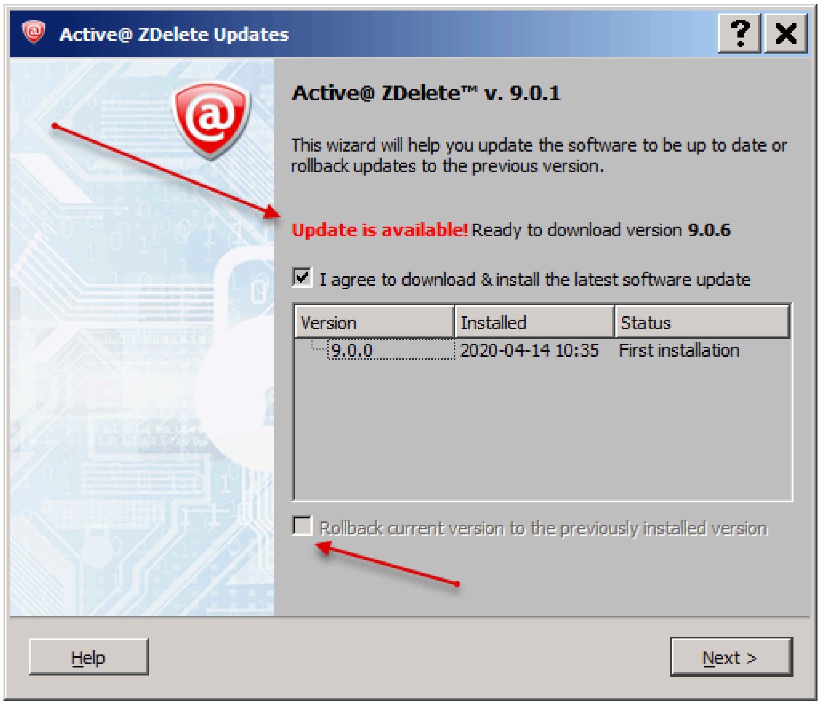
- HDD via IDE, ATA, SATA I, SATA II, SATA III, SAS
- SSD via SATA I, SATA II, SATA III, SAS
- External eSATA & USB disks
- SCSI & iSCSI devices
- Onboard NVMe M.2 (SATA & PCI-E types)
- Removable media (USB drive, MemoryStick, SD card, Compact Flash, Floppy Disk, Zip Drive)

Related tasks

Installation and setup on page 8

Software Updates

`ZDelete` has a built-in update client to ensure you always have an access to the latest version of the application, with the option to roll back to older versions if needed. To update, use the file menu bar to navigate to **Help** > **Updates**



Active@ ZDelete Updates

Active@ ZDelete™ v. 9.0.1

This wizard will help you update the software to be up to date or rollback updates to the previous version.

Update is available! Ready to download version **9.0.6**

☑ I agree to download & install the latest software update

Version	Installed	Status
9.0.0	2020-04-14 10:35	First installation

☐ Rollback current version to the previously installed version

Figure 1: Checking for updates

Update dialog contains history of previously installed versions and updates.

If there is an available update, this window will notify and help you to install the latest version. If you've upgraded from an older version, you may also roll back to the older version using the **Rollback current version to the previously installed version** feature by selecting the checkbox.

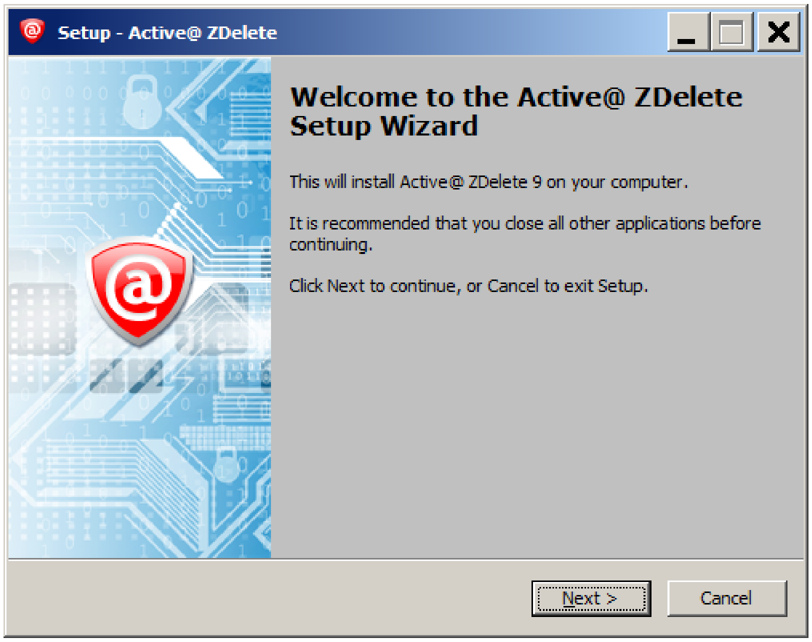
Note: `ZDelete` stores your previously installed versions so you may roll back to any of your older versions at any time.

Installation and setup

In order to install `ZDelete` follow the steps below.

1. Download `ZDeleteSetup.exe` from our website: https://www.zdelete.com
2. Run `ZDeleteSetup.exe` as an administrator

3. Follow the *Setup Wizard* steps to successfully install the software



Welcome to the Active@ ZDelete Setup Wizard

This will install Active@ ZDelete 9 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 2: ZDelete Setup Wizard

Using ZDelete

`ZDelete` is a powerful tool to provide disk erasure solutions for personal use. This guide will help you to get started with configuring `ZDelete` for your system and using it to the full potential. `ZDelete` allows you to launch any of its actions from a graphical user interface:

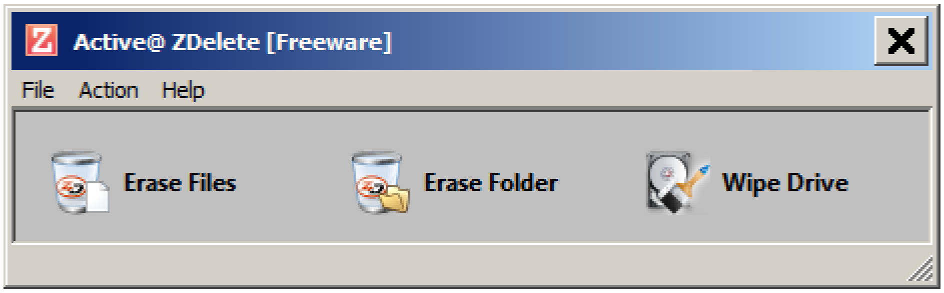


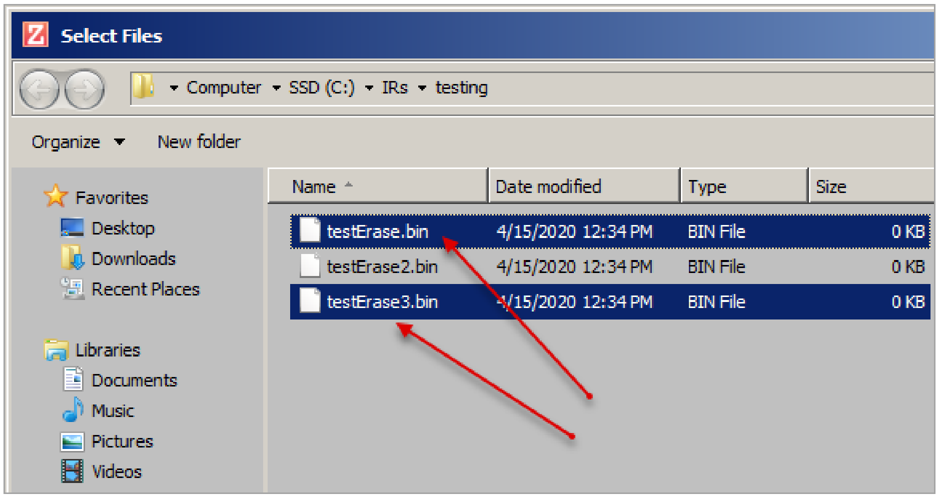
Figure 3: Main View

Erase Files

`ZDelete` is an extremely powerful tool for file erasure. Individual files can be erased according to any desired standard with just a few clicks. The process to achieve this is described below.

1. Select files for erasure

   Use **Erase Files** button or main menu **Action** > **Erase Files** to select 1 or more files. For multiple selection use **Ctrl+Left Mouse** click

   Select Files

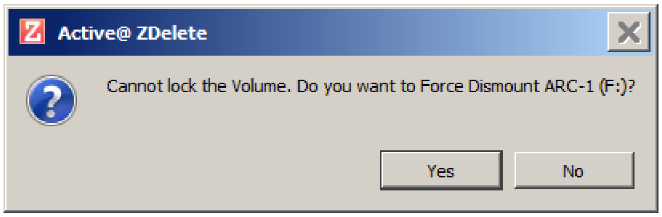
   Computer ▸ SSD (C:) ▸ IRs ▸ testing

   Organize ▾ New folder

Name	Date modified	Type	Size
testErase.bin	4/15/2020 12:34 PM	BIN File	0 KB
testErase2.bin	4/15/2020 12:34 PM	BIN File	0 KB
testErase3.bin	4/15/2020 12:34 PM	BIN File	0 KB

   Figure 4: Files' multiple selection

   Note: If the selected drive/volume can not be locked exclusively by `ZDelete` the process of forcing dismount could be initiated:

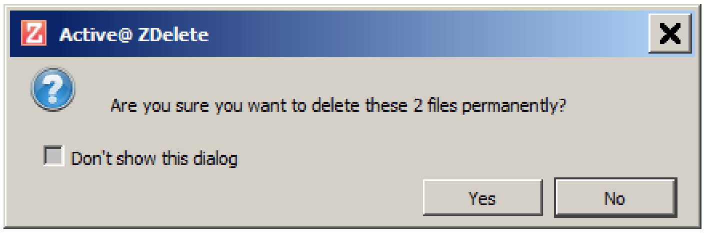
   

   Active@ ZDelete

   Cannot lock the Volume. Do you want to Force Dismount ARC-1 (F:)?

   Figure 5: Force Dismount

2. Confirm erasure in the dialog

   Active@ ZDelete

   Are you sure you want to delete these 2 files permanently?

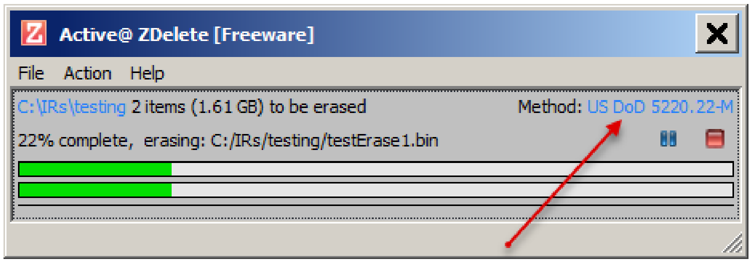
   □ Don't show this dialog

   Figure 6: Initiating the Erase operation

   The erasure procedure starts

3. Observe erase process

   When the *Erase* procedure begins you see the disk area representation as a progress bar as well as a chosen erase method. The progress bar represents the percentage of file(s) space processed. As the procedure progresses the percentage increases and estimated time is recalculated. You are able to **STOP** or **PAUSE** the process at any time.

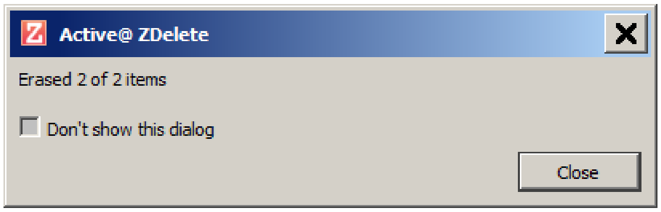


C:\IRs\testing 2 items (1.61 GB) to be erased Method: US DoD 5220.22-M

22% complete, erasing: C:/IRs/testing/testErase1.bin

Figure 7: File(s) Erasure Progress

A confirmation dialog appears at the end of successful erase:



Erased 2 of 2 items

□ Don't show this dialog

Note: You may disable this dialogue from appearing every time. Simply check the box reading **Don't show this dialog**

When erase is completed user is able to check the Log file.

Related information

Erase & Wipe Methods (Sanitation Standards) on page 23

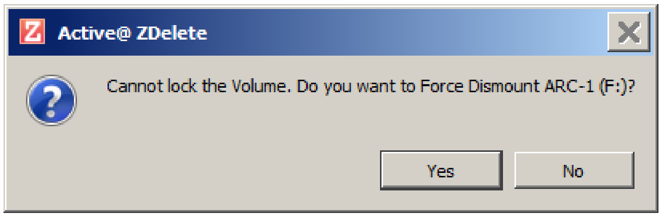
Erase Folder

In addition to files erase an individual folder (with all the files) can be erased according to any desired standard. The process to achieve this is described below.

1. Select folder to erase

Use **Erase Folder** button or main menu **Action** > **Erase Folder** to select a folder to erase.

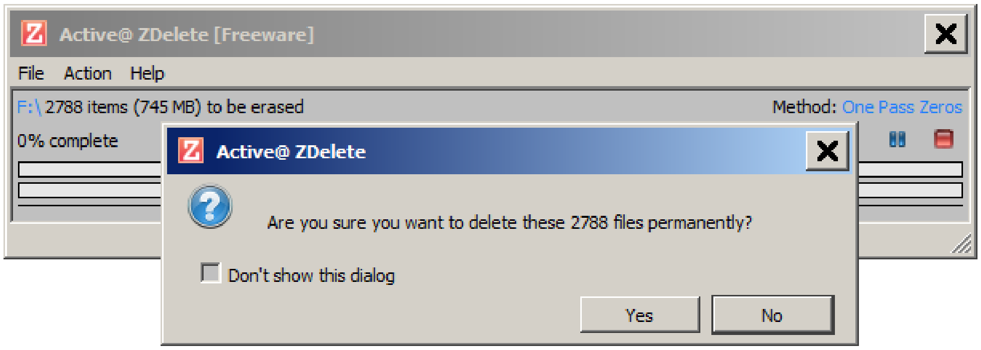
Note: If the selected drive/volume can not be locked exclusively by `ZDelete` the process of forcing dismount could be initiated:



Cannot lock the Volume. Do you want to Force Dismount ARC-1 (F:)?

Figure 8: Force Dismount

2. Confirm erasure in the dialog



F:\ 2788 items (745 MB) to be erased

Method: One Pass Zeros

0% complete

Are you sure you want to delete these 2788 files permanently?

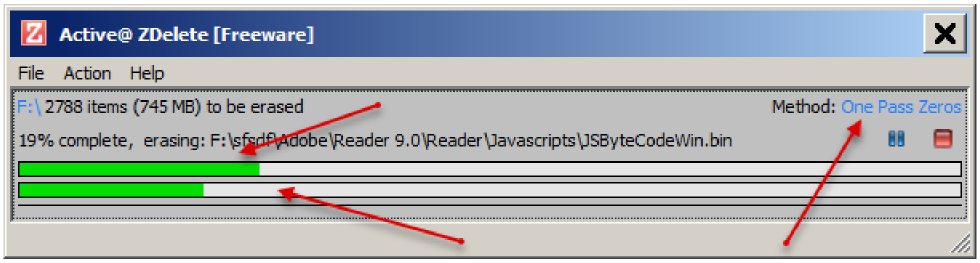
□ Don't show this dialog

Figure 9: Initiating the Folder Erase operation

The erasure procedure starts

3. Observe erase process

When the *Erase* procedure begins you see the 2 progress bars represent the percentage of folder file(s) processed as well as a chosen erase method. As the procedure progresses the percentage increases and estimated time is recalculated. You are able to **STOP** or **PAUSE** the process at any time.



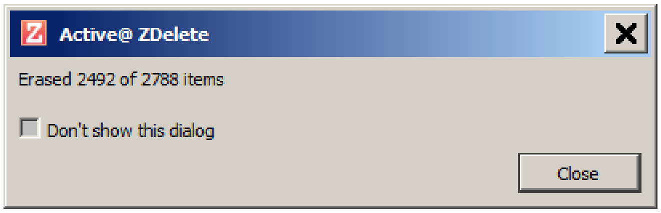
F:\ 2788 items (745 MB) to be erased

Method: One Pass Zeros

19% complete, erasing: F:\sfsdf\Adobe\Reader 9.0\Reader\Javascripts\JSByteCodeWin.bin

Figure 10: Folder Erasure Progress

A confirmation dialog appears at the end of successful erase:



Erased 2492 of 2788 items

□ Don't show this dialog

Note: You may disable this dialogue from appearing every time. Simply check the box reading **Don't show this dialog**

When erase is completed user is able to check the Log file.

Related information

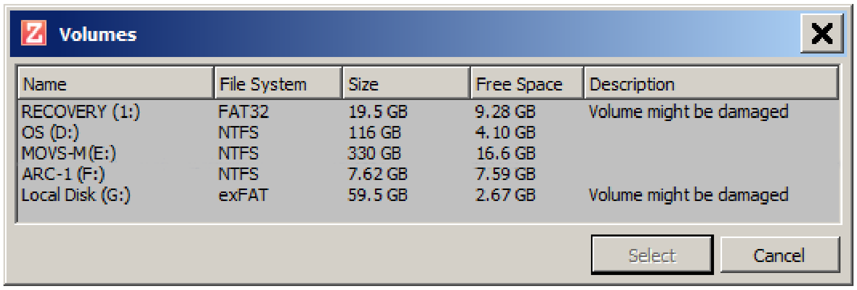
Erase & Wipe Methods (Sanitation Standards) on page 23

Wipe Drive

In addition to files erase and Erase Folder on page 11 a powerful process of wiping can be applied to a drive/volume according to any desired standard. The process to achieve this is described below.

1. Select a drive to wipe

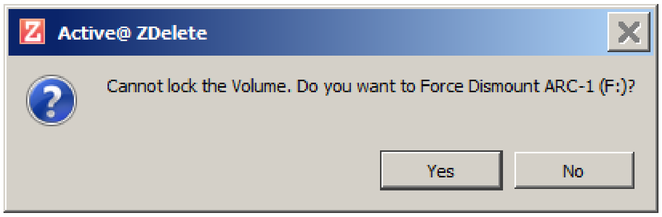
   Use **Wipe Drive** Wipe Drive or main menu **Action** > **Wipe Drive** to select a drive to wipe.



Name	File System	Size	Free Space	Description
RECOVERY (1:)	FAT32	19.5 GB	9.28 GB	Volume might be damaged
OS (D:)	NTFS	116 GB	4.10 GB	
MOVS-M (E:)	NTFS	330 GB	16.6 GB	
ARC-1 (F:)	NTFS	7.62 GB	7.59 GB	
Local Disk (G:)	exFAT	59.5 GB	2.67 GB	Volume might be damaged

Figure 11: Drive/Volume Selection

Note: If the selected drive/volume can not be locked exclusively by `ZDelete` the process of forcing dismount could be initiated:

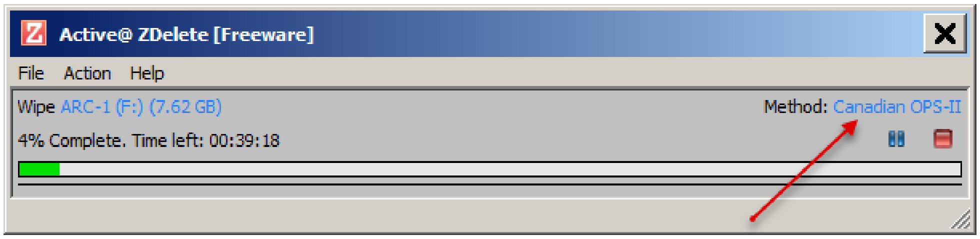


Cannot lock the Volume. Do you want to Force Dismount ARC-1 (F:)?

Figure 12: Force Dismount

2. Observe erase process

   When the *Wipe* procedure begins you see the disk area representation as a progress bar as well as a chosen erase method. The progress bar represents the percentage of drive space processed. As the procedure progresses the percentage increases and estimated time recalculated. You are able to **STOP** or **PAUSE** the process at any time.



Wipe ARC-1 (F:) (7.62 GB)

Method: Canadian OPS-II

4% Complete. Time left: 00:39:18

Figure 13: Wipe Drive Progress

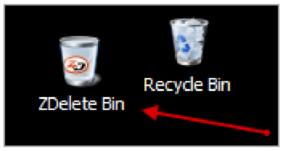
Related information

Erase & Wipe Methods (Sanitation Standards) on page 23

Wipe Disk Concepts on page 20

ZDelete Bin

ZDelete Bin is a convenient method for secure erasing files and folders according to international security standards while maintaining the comfort of having a *Recycle Bin* to drag these files into.



Note: Once files are deleted using the **ZDelete Bin**, they are **unrecoverable** by any file recovery software or data recovery laboratory.

In order to delete files/folders with **ZDelete Bin** mechanism do the following:

- Drag the selected file(s)/folder(s) into the **ZDelete Bin** desktop icon:

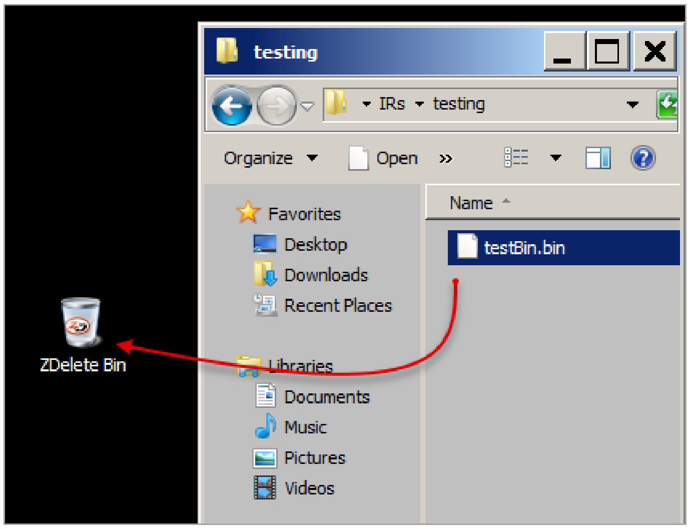


Figure 14: Drag and drop a selected file to the Bin

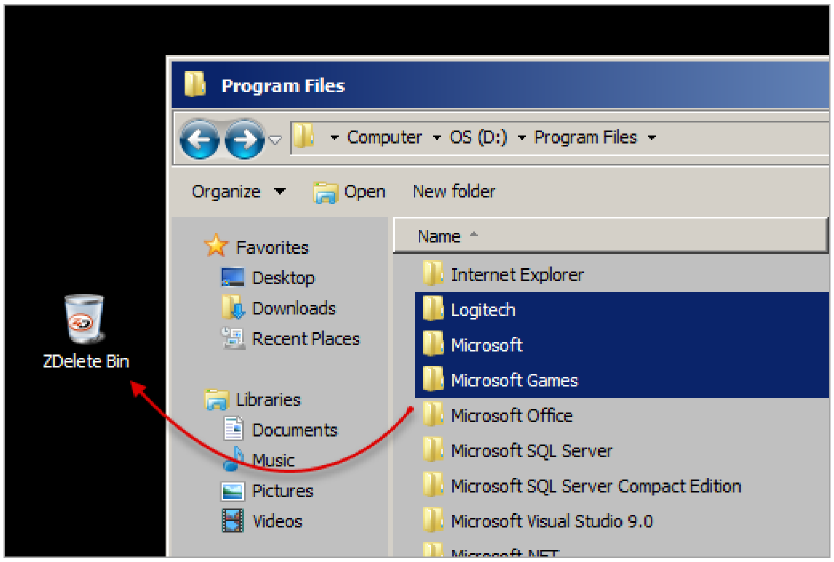


Figure 15: Drag and drop selected folders to the Bin

- Confirm erasure in the dialog for files(s) or folder(s) and proceed with the procedures

Note: Make sure the file(s) is not currently open or being used. This may prevent the erasure process from initiating.

ZDelete Context Menu Features

There is an option to use a Windows Explorer's context menu for file(s), folders and drives selection for the process of erasing or wiping.

For erasing a file(s) **Right Mouse Click** on selected file(s) in *Windows Explorer* and choose an option of **ZDelete Item(s)** in pop-up context menu:

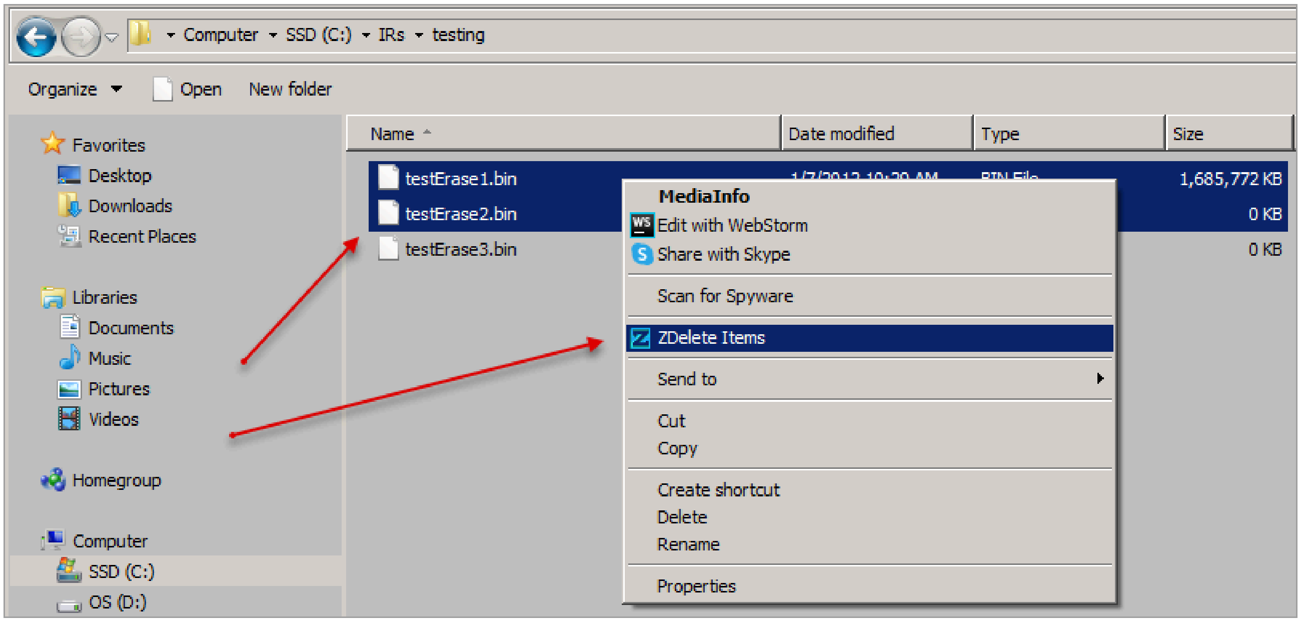


Figure 16: Multiple selection of files to erase

For wiping a drive simply **Right Mouse Click** the desired drive in *Windows Explorer* and proceed with the option of **ZDelete Disk Wiper**:

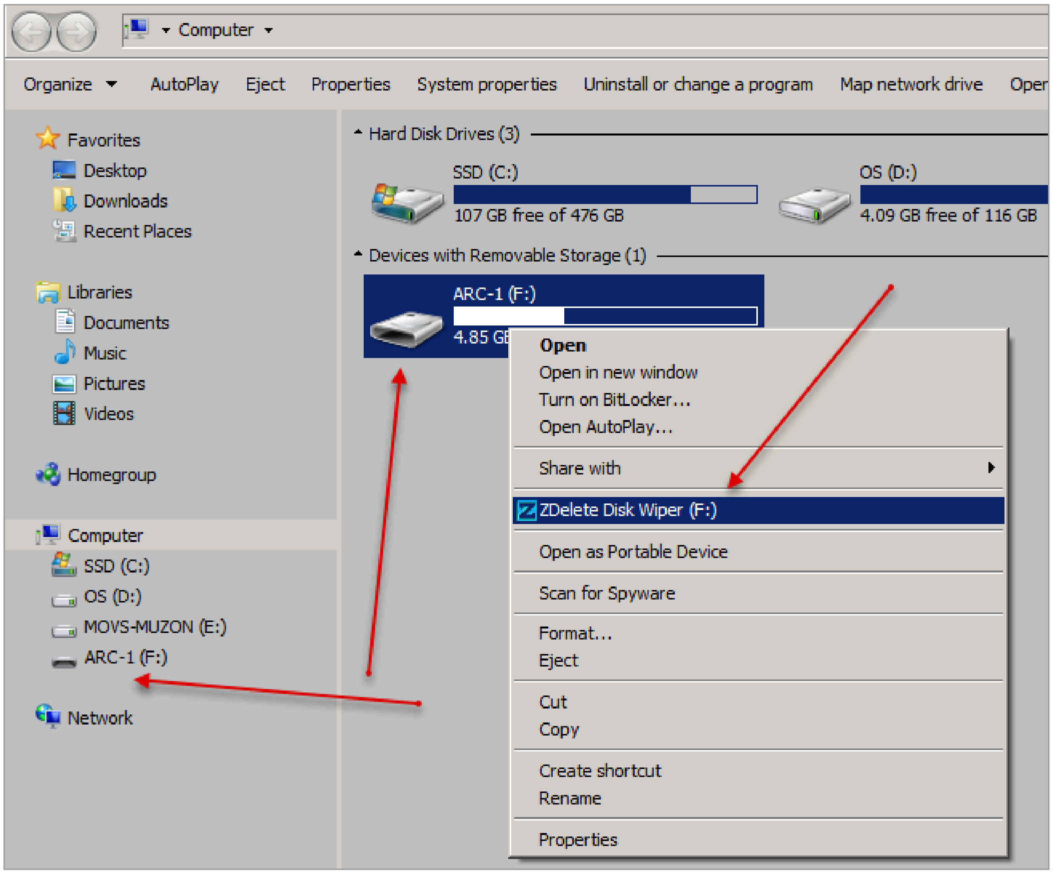


Figure 17: Drive selection for wiping

Related tasks

Erase Files on page 9

Wipe Drive on page 12

Additional Options and Features

`ZDelete` also has a number of extra features to ensure the most complete sanitation operations, flexibility to meet the most strict requirements and compatibility with a wide range of systems. This section outlines these features.

Log Files

User is able to reach the log records (history) via main menu **File** > **View Log**

Right Mouse Click on Log window for **Save Log** and **Clear Log** options.

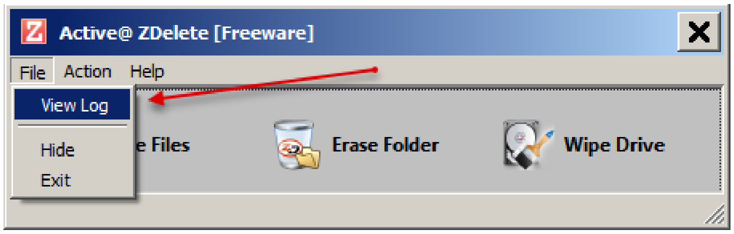
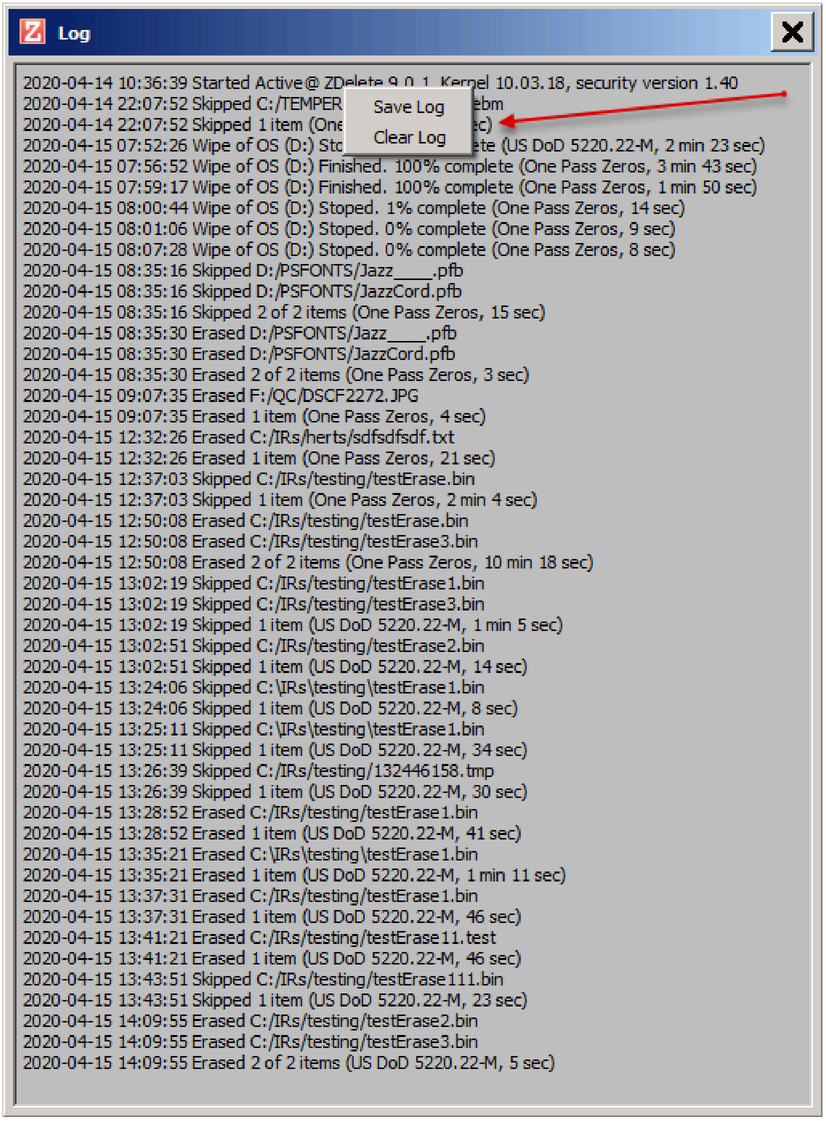


Figure 18: Main menu



```
2020-04-14 10:36:39 Started Active@ ZDelete 9.0.1 Kernel 10.03.18, security version 1.40
2020-04-14 22:07:52 Skipped C:/TEMPER               ebm
2020-04-14 22:07:52 Skipped 1 item (One             c)
2020-04-15 07:52:26 Wipe of OS (D:) Sto            ete (US DoD 5220.22-M, 2 min 23 sec)
2020-04-15 07:56:52 Wipe of OS (D:) Finished. 100% complete (One Pass Zeros, 3 min 43 sec)
2020-04-15 07:59:17 Wipe of OS (D:) Finished. 100% complete (One Pass Zeros, 1 min 50 sec)
2020-04-15 08:00:44 Wipe of OS (D:) Stoped. 1% complete (One Pass Zeros, 14 sec)
2020-04-15 08:01:06 Wipe of OS (D:) Stoped. 0% complete (One Pass Zeros, 9 sec)
2020-04-15 08:07:28 Wipe of OS (D:) Stoped. 0% complete (One Pass Zeros, 8 sec)
2020-04-15 08:35:16 Skipped D:/PSFONTS/Jazz____.pfb
2020-04-15 08:35:16 Skipped D:/PSFONTS/JazzCord.pfb
2020-04-15 08:35:16 Skipped 2 of 2 items (One Pass Zeros, 15 sec)
2020-04-15 08:35:30 Erased D:/PSFONTS/Jazz____.pfb
2020-04-15 08:35:30 Erased D:/PSFONTS/JazzCord.pfb
2020-04-15 08:35:30 Erased 2 of 2 items (One Pass Zeros, 3 sec)
2020-04-15 09:07:35 Erased F:/QC/DSCF2272.JPG
2020-04-15 09:07:35 Erased 1 item (One Pass Zeros, 4 sec)
2020-04-15 12:32:26 Erased C:/IRs/herts/sdfsdfsdf.txt
2020-04-15 12:32:26 Erased 1 item (One Pass Zeros, 21 sec)
2020-04-15 12:37:03 Skipped C:/IRs/testing/testErase.bin
2020-04-15 12:37:03 Skipped 1 item (One Pass Zeros, 2 min 4 sec)
2020-04-15 12:50:08 Erased C:/IRs/testing/testErase.bin
2020-04-15 12:50:08 Erased C:/IRs/testing/testErase3.bin
2020-04-15 12:50:08 Erased 2 of 2 items (One Pass Zeros, 10 min 18 sec)
2020-04-15 13:02:19 Skipped C:/IRs/testing/testErase1.bin
2020-04-15 13:02:19 Skipped C:/IRs/testing/testErase3.bin
2020-04-15 13:02:19 Skipped 1 item (US DoD 5220.22-M, 1 min 5 sec)
2020-04-15 13:02:51 Skipped C:/IRs/testing/testErase2.bin
2020-04-15 13:02:51 Skipped 1 item (US DoD 5220.22-M, 14 sec)
2020-04-15 13:24:06 Skipped C:\IRs\testing\testErase1.bin
2020-04-15 13:24:06 Skipped 1 item (US DoD 5220.22-M, 8 sec)
2020-04-15 13:25:11 Skipped C:\IRs\testing\testErase1.bin
2020-04-15 13:25:11 Skipped 1 item (US DoD 5220.22-M, 34 sec)
2020-04-15 13:26:39 Skipped C:/IRs/testing/132446158.tmp
2020-04-15 13:26:39 Skipped 1 item (US DoD 5220.22-M, 30 sec)
2020-04-15 13:28:52 Erased C:/IRs/testing/testErase1.bin
2020-04-15 13:28:52 Erased 1 item (US DoD 5220.22-M, 41 sec)
2020-04-15 13:35:21 Erased C:\IRs\testing\testErase1.bin
2020-04-15 13:35:21 Erased 1 item (US DoD 5220.22-M, 1 min 11 sec)
2020-04-15 13:37:31 Erased C:/IRs/testing/testErase1.bin
2020-04-15 13:37:31 Erased 1 item (US DoD 5220.22-M, 46 sec)
2020-04-15 13:41:21 Erased C:/IRs/testing/testErase11.test
2020-04-15 13:41:21 Erased 1 item (US DoD 5220.22-M, 46 sec)
2020-04-15 13:43:51 Skipped C:/IRs/testing/testErase111.bin
2020-04-15 13:43:51 Skipped 1 item (US DoD 5220.22-M, 23 sec)
2020-04-15 14:09:55 Erased C:/IRs/testing/testErase2.bin
2020-04-15 14:09:55 Erased C:/IRs/testing/testErase3.bin
2020-04-15 14:09:55 Erased 2 of 2 items (US DoD 5220.22-M, 5 sec)
```

Figure 19: Log file sample

System Tray

User is able to minimize `ZDelete` to *System Tray* (hide) via main menu **File** > **Hide** or simply by pressing a **Close** button.

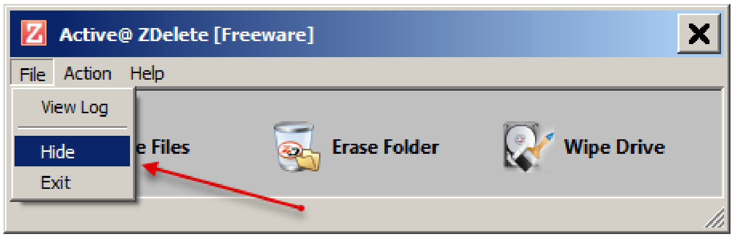


Figure 20: Main menu

Use **Right Mouse Click** > **Show** on *System Tray* `ZDelete` icon for restoring.

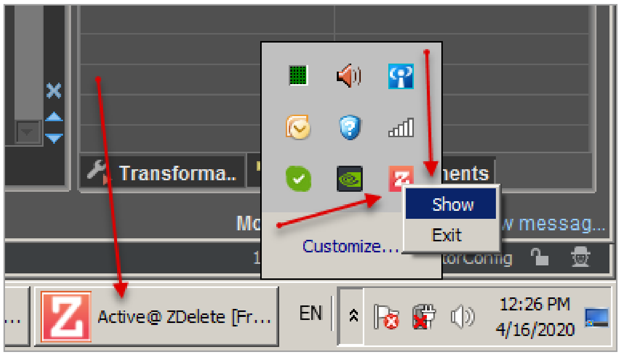
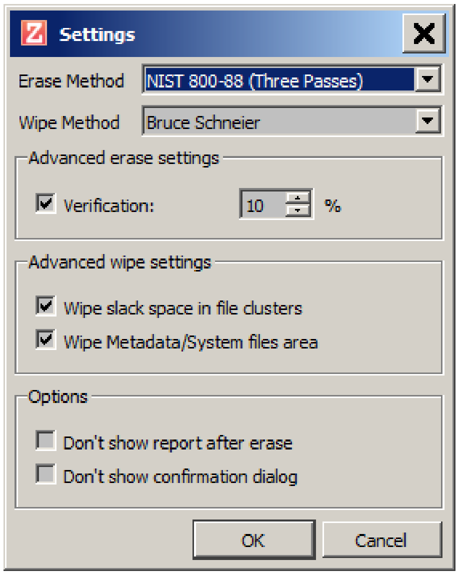


Figure 21: System Tray

Application Settings

ZDelete supports more than 20 international disk sanitation standards and a variety of other customizations to fit a wide range of requirements. These customizations are set in ZDelete main menu **Action** > **Settings**.



Settings

Erase Method: NIST 800-88 (Three Passes)

Wipe Method: Bruce Schneier

Advanced erase settings

☑ Verification: 10 %

Advanced wipe settings

☑ Wipe slack space in file clusters

☑ Wipe Metadata/System files area

Options

☐ Don't show report after erase

☐ Don't show confirmation dialog

Figure 22: Application Settings

- **Erase Method** drop box with selection of all ZDelete available erase methods for files or folders
- **Wipe Method** drop box with selection of all ZDelete available wipe methods for drives.
- **Wipe unused clusters** option to wipe unused clusters according to the concepts
- **Wipe Metadata/System files area** option to wipe metadata and system files according to the concepts
- **Verification** option to run a verification on some of the erase methods. User is able to set a part (in percentage) of erased area to verify
- **Don't show report after erase** option to avoid showing of a report message box
- **Don't show confirmation dialog** option to avoid showing of erase/wipe confirmation dialog

Appendix

Erase Disk Concepts

Erasing Confidential Data

Modern methods of data encryption are deterring network attackers from extracting sensitive data from stored database files.

Attackers (who want to retrieve confidential data) become more resourceful and look for places where data might be stored temporarily. For example, the Windows **DELETE** command merely changes the files attributes and location so that the operating system will not look for the file. The situation with *NTFS* is similar.

One avenue of attack is the recovery of data from residual data on a discarded hard drive. When deleting confidential data from hard drives, removable disks or USB devices, it is important to extract all traces of the data so that recovery is not possible.

Most official guidelines regarding the disposal of confidential magnetic data do not take into account the depth of today's recording densities nor the methods used by the OS when removing data.

Removal of confidential personal information or company trade secrets in the past might have been performed using the **FORMAT** command or the **FDISK** command. Using these procedures gives users a sense of confidence that the data has been completely removed.

When using the **FORMAT** command Windows displays a message like this:

```
Important: Formatting a disk removes all information from the disk.
```

The **FORMAT** utility actually creates new *FAT* and *ROOT* tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced *FAT* and *ROOT* tables is stored so that the **UNFORMAT** command can be used to restore them.

FDISK merely cleans the Partition Table (located in the drive's first sector) and does not touch anything else.

Advanced Data Recovery Systems

Advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped and disassembled. Security agencies use advanced applications to find cybercrime related evidence. Also there are established industrial spy agencies using sophisticated channel coding techniques such as *PRML* (*Partial Response Maximum Likelihood*), a technique used to reconstruct the data on magnetic disks. Other methods include the use of magnetic force microscopy and recovery of data based on patterns in erase bands.

Although there are very sophisticated data recovery systems available at a high price. Almost all the data can also be easily restored with an off-the-shelf data recovery utility like `Active@ File Recovery` (https://www.file-recovery.com), making your erased confidential data quite accessible.

Using `ZDelete`, our powerful and compact utility, all data on your hard drive or removable device can be destroyed without the possibility of future recovery. After using `ZDelete` disposal, recycling, selling or donating your storage device can be done with peace of mind.

International Standards in Data Removal

`Active@ ZDelete` conforms to more than **22** international standards for clearing and sanitizing data (US DoD 5220.22-M, Peter Gutmann etc.). You can be sure that sensitive information is destroyed forever once you erase a disk with `Active@ ZDelete`.

Active@ ZDelete is a professional security application that destroys data permanently on any computer that can be started using a bootable CD/DVD-ROM or USB Flash Disk. Access to the drive's data is made on the physical level via the BIOS (Basic Input-Output System) bypassing the operating system's logical drive structure organization.

Wipe Disk Concepts

Wiping Confidential Data from Unoccupied Disk's Space

You may have confidential data on your hard drive in spaces where data may have been stored temporarily.

You may also have deleted files by using the Windows Recycle Bin and then emptying it. While you are still using your local hard drive, there may be confidential information available in these unoccupied spaces.

Wiping the logical drive's deleted data does not delete existing files and folders. It processes all unoccupied drive space so that recovery of previously deleted files becomes impossible.

Installed applications and existing data are not touched by this process. When you wipe unoccupied drive space, the process is run from the bootable CD/DVD operating system. As a result, the wipe or erase process uses an operating system that is outside the local hard drive and is not impeded by Windows system caching. This means that deleted Windows system records can be wiped clean.

ZDelete wipes unused data residue from file slack space, unused sectors, and unused space in MTF records or directory records.

Wiping drive space can take a long time, so do this when the system is not being otherwise utilized. For example, this can be done overnight.

Wipe Algorithms

The process of deleting files does not eliminate them from the hard drive. Unwanted information may still be left available for recovery on the computer. A majority of software that advertises itself as performing reliable deletions simply wipes out free clusters. Deleted information may be kept in additional areas of a drive. ZDelete therefore offers different wipe algorithms to ensure secure deletion: overwriting with zeros, overwriting with random values, overwriting with multiple passes using different patterns and much more. ZDelete supports more than 20 international data sanitizing standards, including US DoD 5220.22-M and the most secure Gutmann's method overwriting with **35** (!) passes.

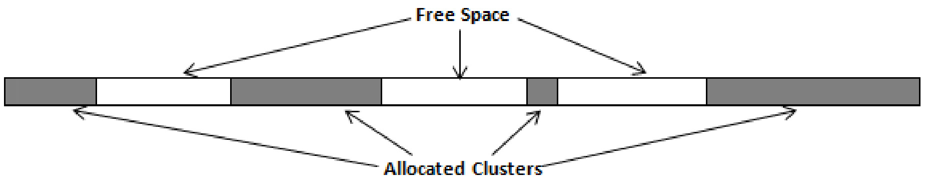


Figure 23: Disk free space and allocated clusters

Wiping File Slack Space

This relates to any regular files located on any file system. Free space to be wiped is found in the "tail" end of a file because disk space is usually allocated in 4 Kb clusters. Most files have sizes that are not 4 Kb increments and thus have *slack space* at their end.

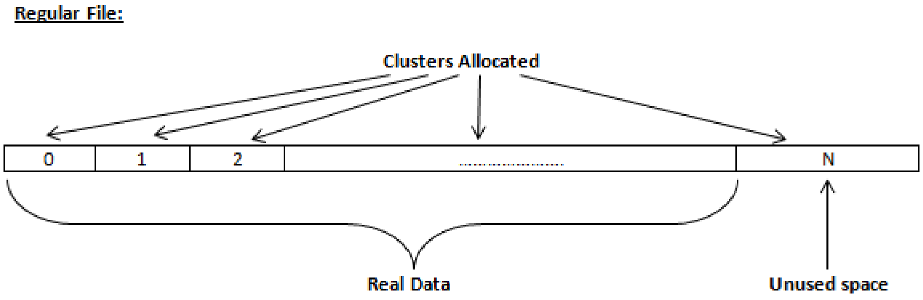


Figure 24: Disk free space and allocated clusters

Specifics of Wiping Microsoft NTFS File System

NTFS Compressed Files

Wiping free space inside a file: The algorithm NTFS uses to "compress" a file operates by separating the file into compressed blocks (usually 64 Kb long). After it is processed, each of these blocks has been allocated a certain amount of space on the volume. If the compressed information takes up less space than the source file, then the rest of the space is labeled as sparse space and no space on the volume is allocated to it. Because the compressed data often doesn't have a size exactly that of the cluster, the end of each of these blocks stays as unusable space of significant size. Our algorithm goes through each of these blocks in a compressed file and wipes the unusable space, erasing previously deleted information that was kept in those areas.

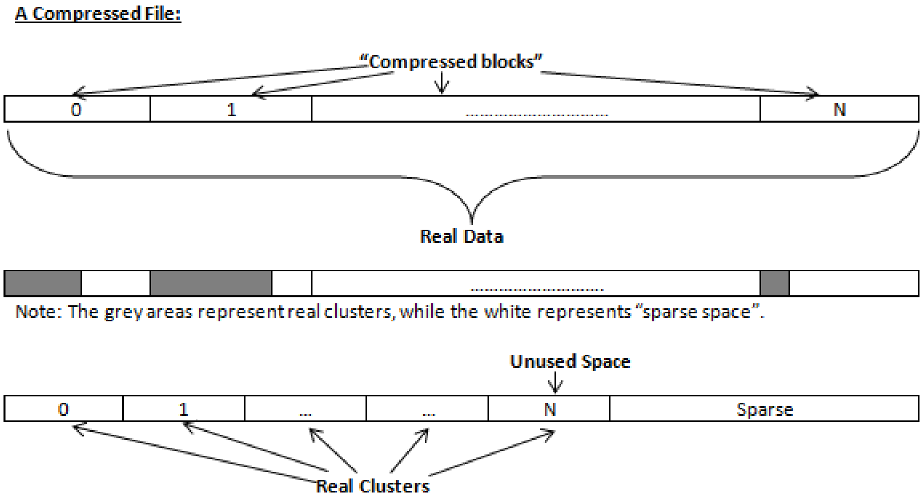


Figure 25: Compressed file structure

The MFT (Master File Table) Area

Wiping the system information:

The MFT file contains records, describing every file on the volume. During the deletion of these files, the records of their deletion are left untouched - they are simply recorded as "deleted". Therefore file recovery software can use this information to recover anything from the name of the file and the structure of the deleted directories down to files smaller than 1Kb that are able to be saved in the MFT directly. The algorithm used by `ZDelete` wipes all of the unused information out of the MFT records and wipes the unusable space, making a recovery process impossible.

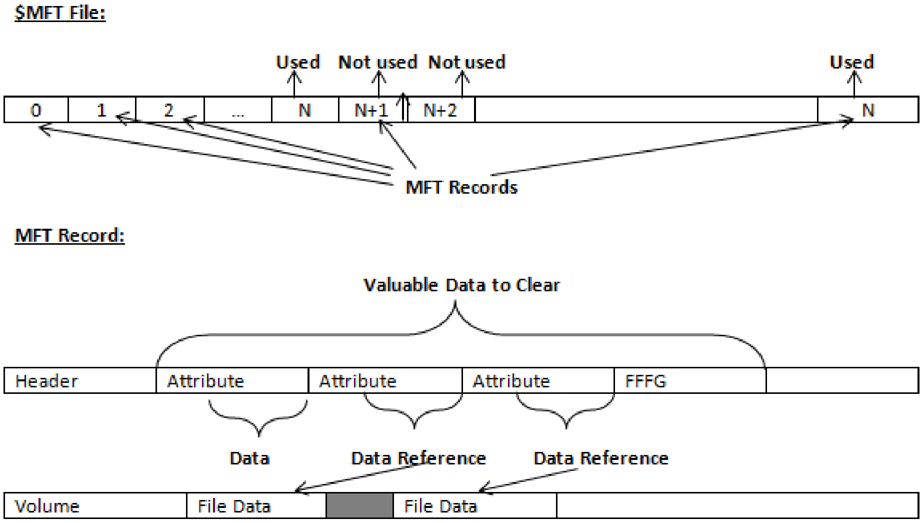


Figure 26: MFT structure

Specifics of Wiping Microsoft FAT File System

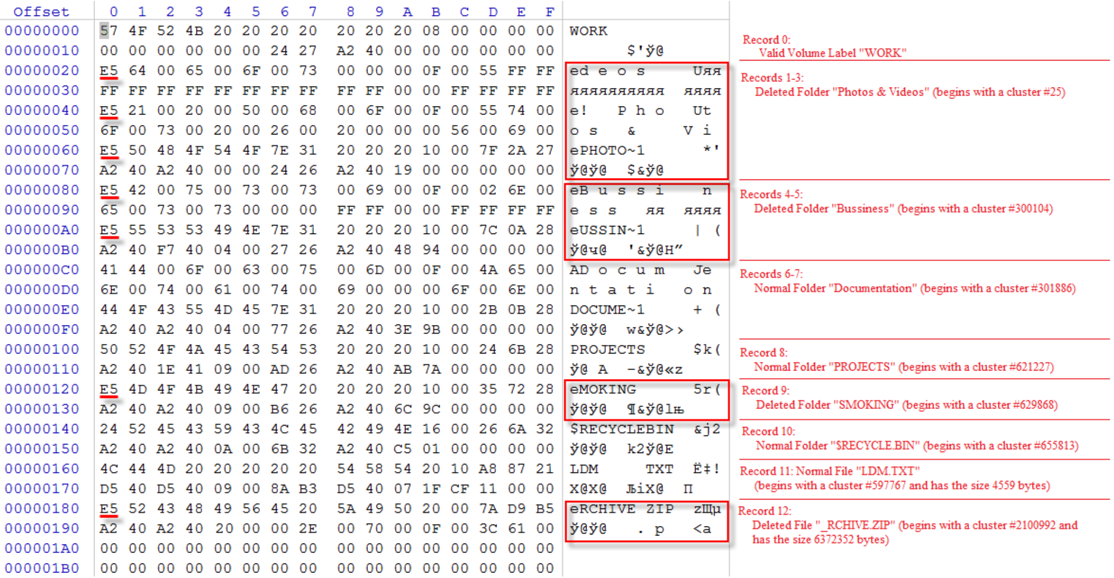
Wiping Directory Areas

Each directory on a FAT/FAT32 or an exFAT volume can be considered as a specific file, describing the contents of the directory. Inside this descriptor there are many 32-byte records, describing every file and other inner folders.

When you delete files this data is not being fully erased. It is just marked as deleted (hex symbol **0xE5**). That's why data recovery software can detect and use these records to restore file names and full directory structures.

In some cases dependent on whether a space where item located has been overwritten yet or not, files and folders can be fully or partially recovered..

`Active@ ZDelete` makes data recovery impossible by using an algorithm that wipes out all unused information from directory descriptors. `Active@ ZDelete` not only removes unused information, but also *defragments* Directory Areas, thus speeding up directory access.



```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  57 4F 52 4B 20 20 20 20  20 20 20 08 00 00 00 00  WORK
00000010  00 00 00 00 00 00 24 27  A2 40 00 00 00 00 00 00        $'ÿ@
00000020  E5 64 00 65 00 6F 00 73  00 00 00 0F 00 55 FF FF  ed e o s    Uяя
00000030  FF FF FF FF FF FF FF FF  FF FF 00 00 FF FF FF FF  яяяяяяяяяя  яяяя
00000040  E5 21 00 20 00 50 00 68  00 6F 00 0F 00 55 74 00  e!   P h o   Ut
00000050  6F 00 73 00 20 00 26 00  20 00 00 00 56 00 69 00  o s   &     V i
00000060  E5 50 48 4F 54 4F 7E 31  20 20 20 10 00 7F 2A 27  ePHOTO~1      *'
00000070  A2 40 A2 40 00 00 24 26  A2 40 19 00 00 00 00 00  ў@ў@  $&ў@
00000080  E5 42 00 75 00 73 00 73  00 69 00 0F 00 02 6E 00  eB u s s i     n
00000090  65 00 73 00 73 00 00 00  FF FF 00 00 FF FF FF FF  e s s   яя  яяяя
000000A0  E5 55 53 53 49 4E 7E 31  20 20 20 10 00 7C 0A 28  eUSSIN~1     | (
000000B0  A2 40 F7 40 04 00 27 26  A2 40 48 94 00 00 00 00  ў@ч@  '&ў@H”
000000C0  41 44 00 6F 00 63 00 75  00 6D 00 0F 00 4A 65 00  AD o c u m   Je
000000D0  6E 00 74 00 61 00 74 00  69 00 00 00 6F 00 6E 00  n t a t i   o n
000000E0  44 4F 43 55 4D 45 7E 31  20 20 20 10 00 2B 0B 28  DOCUME~1     + (
000000F0  A2 40 A2 40 04 00 77 26  A2 40 3E 9B 00 00 00 00  ў@ў@  w&ў@>›
00000100  50 52 4F 4A 45 43 54 53  20 20 20 10 00 24 6B 28  PROJECTS     $k(
00000110  A2 40 1E 41 09 00 AD 26  A2 40 AB 7A 00 00 00 00  ў@ A  -&ў@«z
00000120  E5 4D 4F 4B 49 4E 47 20  20 20 20 10 00 35 72 28  eMOKING      5r(
00000130  A2 40 A2 40 09 00 B6 26  A2 40 6C 9C 00 00 00 00  ў@ў@  ¶&ў@lњ
00000140  24 52 45 43 59 43 4C 45  42 49 4E 16 00 26 6A 32  $RECYCLEBIN  &j2
00000150  A2 40 A2 40 0A 00 6B 32  A2 40 C5 01 00 00 00 00  ў@ў@  k2ў@E
00000160  4C 44 4D 20 20 20 20 20  54 58 54 20 10 A8 87 21  LDM     TXT  Ё‡!
00000170  D5 40 D5 40 09 00 8A B3  D5 40 07 1F CF 11 00 00  Х@Х@  Љіх@  П
00000180  E5 52 43 48 49 56 45 20  5A 49 50 20 00 7A D9 B5  eRCHIVE ZIP  zЩµ
00000190  A2 40 A2 40 20 00 00 2E  00 70 00 0F 00 3C 61 00  ў@ў@    . p   <a
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Record 0:
Valid Volume Label "WORK"

Records 1-3:
Deleted Folder "Photos & Videos" (begins with a cluster #25)

Records 4-5:
Deleted Folder "Bussiness" (begins with a cluster #300104)

Records 6-7:
Normal Folder "Documentation" (begins with a cluster #301886)

Record 8:
Normal Folder "PROJECTS" (begins with a cluster #621227)

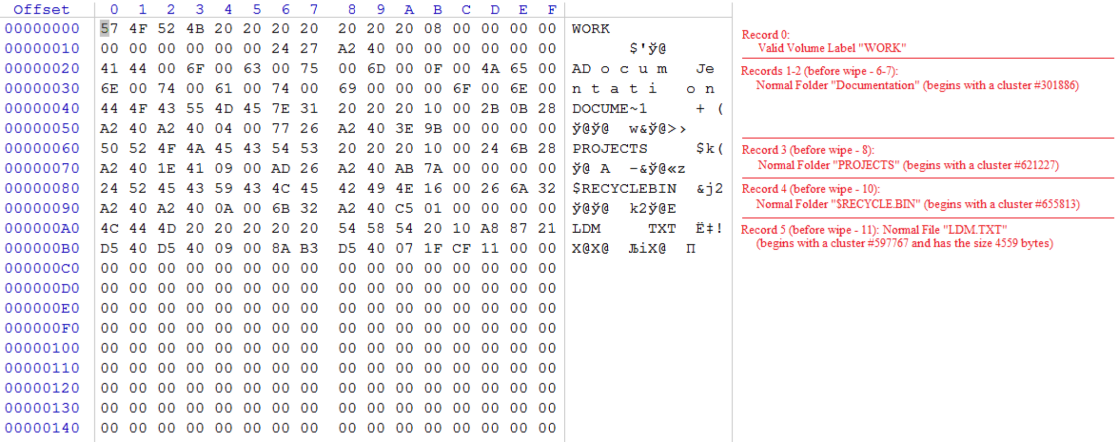
Record 9:
Deleted Folder "SMOKING" (begins with a cluster #629868)

Record 10:
Normal Folder "$RECYCLE.BIN" (begins with a cluster #655813)

Record 11: Normal File "LDM.TXT"
(begins with a cluster #597767 and has the size 4559 bytes)

Record 12:
Deleted File "_RCHIVE.ZIP" (begins with a cluster #2100992 and has the size 6372352 bytes)

Figure 27: This is how Directory Area looks before Wiping, red rectangles display deleted records



```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  57 4F 52 4B 20 20 20 20  20 20 20 08 00 00 00 00  WORK
00000010  00 00 00 00 00 00 24 27  A2 40 00 00 00 00 00 00        $'ў@
00000020  41 44 00 6F 00 63 00 75  00 6D 00 0F 00 4A 65 00  AD o c u m   Je
00000030  6E 00 74 00 61 00 74 00  69 00 00 00 6F 00 6E 00  n t a t i   o n
00000040  44 4F 43 55 4D 45 7E 31  20 20 20 10 00 2B 0B 28  DOCUME~1     + (
00000050  A2 40 A2 40 04 00 77 26  A2 40 3E 9B 00 00 00 00  ў@ў@  w&ў@>›
00000060  50 52 4F 4A 45 43 54 53  20 20 20 10 00 24 6B 28  PROJECTS     $k(
00000070  A2 40 1E 41 09 00 AD 26  A2 40 AB 7A 00 00 00 00  ў@ A  -&ў@«z
00000080  24 52 45 43 59 43 4C 45  42 49 4E 16 00 26 6A 32  $RECYCLEBIN  &j2
00000090  A2 40 A2 40 0A 00 6B 32  A2 40 C5 01 00 00 00 00  ў@ў@  k2ў@E
000000A0  4C 44 4D 20 20 20 20 20  54 58 54 20 10 A8 87 21  LDM     TXT  Ё‡!
000000B0  D5 40 D5 40 09 00 8A B3  D5 40 07 1F CF 11 00 00  Х@Х@  Љіх@  П
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Record 0:
Valid Volume Label "WORK"

Records 1-2 (before wipe - 6-7):
Normal Folder "Documentation" (begins with a cluster #301886)

Record 3 (before wipe - 8):
Normal Folder "PROJECTS" (begins with a cluster #621227)

Record 4 (before wipe - 10):
Normal Folder "$RECYCLE.BIN" (begins with a cluster #655813)

Record 5 (before wipe - 11): Normal File "LDM.TXT"
(begins with a cluster #597767 and has the size 4559 bytes)

Figure 28: Directory Area after Wiping: all deleted records removed, root defragmented

Erase & Wipe Methods (Sanitation Standards)

One Pass Zeros or One Pass Random

When using *One Pass Zeros* or *One Pass Random*, the number of passes is fixed and cannot be changed. When the write head passes through a sector, it writes only zeros or a series of random characters.

US DoD 5220.22-M

The write head passes over each sector three times. The first time with zeros *0x00*, second time with *0xFF* and the third time with random characters. There is one final pass to verify random characters by reading.

Canadian CSEC ITSG-06

The write head passes over each sector, writing a random character. On the next pass, writes the compliment of previously written character. Final pass is random, proceeded by a verify.

Canadian OPS-II

The write head passes over each sector seven times (*0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF*, random). There is one final pass to verify random characters by reading.

British HMG IS5 Baseline

Baseline method overwrites disk's surface with just zeros *0x00*. There is one final pass to verify random characters by reading.

British HMG IS5 Enhanced

Enhanced method - the write head passes over each sector three times. The first time with zeros *0x00*, second time with *0xFF* and the third time with random characters. There is one final pass to verify random characters by reading.

Russian GOST p50739-95

The write head passes over each sector two times. (*0x00*, Random). There is one final pass to verify random characters by reading.

US Army AR380-19

The write head passes over each sector three times. The first time with *0xFF*, second time with zeros *0x00* and the third time with random characters. There is one final pass to verify random characters by reading.

US Air Force 5020

The write head passes over each sector three times. The first time with random characters, second time with zeros *0x00* and the third time with *0xFF*. There is one final pass to verify random characters by reading.

NAVSO P-5329-26 RL

RL method - the write head passes over each sector three times (*0x01, 0x27FFFFFF, Random*).

There is one final pass to verify random characters by reading.

NCSC-TG-025

The write head passes over each sector three times (*0x00, 0xFF, Random*). There is one final pass to verify random characters by reading.

NSA 130-2

The write head passes over each sector two times (*Random, Random*). There is one final pass to verify random characters by reading.

NIST 800-88

Supported three NIST 800-88 media sanitation standards:

1. The write head passes over each sector one time (*0x00*).

2. The write head passes over each sector one time (*Random*).

3. The write head passes over each sector three times (*0x00, 0xFF, Random*).

For details about this,the most secure data clearing standard, you can read the original article at the link below:http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

German VSITR

The write head passes over each sector seven times.

Bruce Schneier

The write head passes over each sector seven times (*0xFF, 0x00, Random, Random, Random, Random, Random*). There is one final pass to verify random characters by reading.

Peter Gutmann

The write head passes over each sector **35** times. For details about this, the most secure data clearing standard, you can read the original article at the link below: http://www.cs.auckland.ac.nz/%7Epgut001/pubs/se%0Acure_del.html

Australian ISM-6.2.93

The write head passes over each sector once with random characters. There is one final pass to verify random characters by reading.