

KillDisk - User Manual



Contents

Legal Statement.....	4
Introduction.....	5
Advanced Data Recovery Systems.....	5
Erasing Confidential Data.....	5
Wiping Confidential Data.....	6
International Standards in Data Destruction.....	6
KillDisk Overview.....	7
System Requirements.....	7
Software Licensing.....	8
Registering the Software (Online).....	8
Registering the Software (Offline).....	10
Deactivating a Registration.....	12
Software Updates.....	12
Getting Started with KillDisk.....	14
KillDisk Installation and Distribution.....	14
Active@ Boot Disk Creator.....	15
Navigating Killdisk.....	17
Disk Explorer.....	19
Using KillDisk.....	20
Disk Erase.....	20
Selecting Disk Area for Erasure & Erasing Partitions.....	23
Disk Wipe.....	24
Processing Summary.....	25
Certificates, Labels and Reports.....	26
Erase Certificates.....	27
Erase Reports.....	28
Erase Labels.....	28
Additional Options and Features.....	31
Mapping Network Shares.....	31
Changing Disk Serial Number.....	32
Reset Hidden Areas.....	33
Property Views.....	33
Dynamic Disks: LDM, LVM and WSS.....	35
Preferences.....	36
General Settings.....	37
Disk Erase Options.....	39
Disk Wipe Options.....	41
Certificate Options.....	41
Report Options.....	43
Labels Options.....	45
Disk Viewer Options.....	49

Error Handling Options.....	49
Email Notification Options.....	50
Command Line and Batch Modes.....	52
Command Line Mode.....	52
Batch Mode.....	55
Advanced Tools.....	57
File Browser.....	57
Disk Viewer.....	58
Application Settings.....	63
Troubleshooting and System Recovery.....	68
Common Troubleshooting Tips.....	68
Application Log.....	68
Hardware Diagnostic File.....	70
Appendix.....	71
Glossary.....	71
Erase Disk Concepts.....	72
Wipe Disk Concepts.....	74
Erase Methods / Sanitation Standards.....	78
Using KillDisk in PXE environment.....	80
File Name Tags.....	86
Disk Hidden Zones (HPA/DCO).....	88

Legal Statement

Copyright © 2019, LSOFTECHNOLOGIES INC. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from LSOFTECHNOLOGIES INC.

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

LSOFTECHNOLOGIES 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. LSOFTECHNOLOGIES INC. 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@ KillDisk, the Active@ KillDisk logo, KillDisk, KillDisk for Industrial Systems, KillDisk Desktop are trademarks of LSOFTECHNOLOGIES INC.

LSOFTECHNOLOGIES.NET logo is a trademark of LSOFTECHNOLOGIES INC.

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

Introduction

As a relatively new technology, an overwhelming majority of people, businesses and organizations do not understand the importance of security in digital data storage. The average hard drive sees thousands of files written to it, many of which contain sensitive information. Over the course of a hard drive's lifetime, the likelihood for **recoverable** remnants of sensitive information left on a hard drive at its' end of life is very high. To see this firsthand, simply try out KillDisk's *File Browser* on page 57 on your system drive. You'll be surprised to see what you find!



Note: Additionally, try formatting a USB drive with files on it and browse it with KillDisk's *File Browser* on page 57 as well. Data breaches are not limited to hard drives!

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 adopting 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, data can also be easily restored with the help of an off-the-shelf data recovery utility like Active@ File Recovery (<http://www.file-recovery.com>), making your erased confidential data quite accessible.

Using KillDisk, 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 KillDisk, disposal, recycling, selling or donating your storage device can be done with peace of mind.

Erasing Confidential Data

Modern methods of data encryption are deterring unwanted network attackers from extracting sensitive data from stored database files. Attackers who want to retrieve confidential data are becoming more resourceful by looking into places where data might be stored temporarily. A hard drive on a local network node, for example, can be a prime target for such a search. One avenue of attack is the recovery of data from residual data on a discarded hard disk drive. When deleting confidential data from hard drives, removable floppies or USB devices, it is important to extract all traces of the data so that recovery is not possible.

Most official guidelines around disposing of confidential magnetic data do not take into account the depth of today's recording densities, nor the methods used by the operating system when removing data. For example, the Windows DELETE command merely changes the file name so that the operating system will not look for the file. The situation with NTFS is similar.

Removal of confidential personal information or company trade secrets in the past might have used the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures give users a sense of confidence that the data has been completely removed.

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

```
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 are stored, so that the UNFORMAT command can be used to restore them.

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

Moreover, most of hard disks contain hidden zones (disk areas that cannot be accessed and addressed on a logical access level). KillDisk is able to detect and reset these zones, cleaning up the information inside.

Wiping Confidential Data

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.

KillDisk wipes unused data residue from file slack space, unused sectors, and unused space in MFT 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.

International Standards in Data Destruction

KillDisk conforms to dozens of 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 KillDisk, sensitive information is destroyed forever.

KillDisk is a quality security application that destroys data permanently from any computer that can be started using a bootable USB or CD/DVD. Access to the drive's data is made on the physical level via the BIOS (Basic Input-Output Subsystem), bypassing the operating system's logical drive structure organization. Regardless of the operating system, file systems or type of machine, this utility can destroy all data on all storage devices. It does not matter which operating systems or file systems are located on the machine.

KillDisk Overview

KillDisk 12

KillDisk 12 is the most powerful consumer edition released to date. With the development and release of KillDisk Industrial, KillDisk 12 benefits from industrial stability, improved disk handling, interface layout and several new features including:

- Redesigned and improved user interface
- Enhanced visualization of physical disks and erase processes
- Improved handling of disks with controller malfunctions
- Stable handling of hot-swappable and dynamic disks
- Sound notifications for completed erase jobs with different results
- Auto hibernate or shutdown the system after all jobs are completed
- Enhanced certificates and reports for disk erase and wipe
- Advanced Disk Viewer with flexible Search for low-level disk inspection
- Customizable file names for certificates & XML reports
- Unique Computer ID can be displayed in certificates/reports
- Disk health - S.M.A.R.T. information can be displayed and monitored
- Customizable look & feel: four different application styles included
- ATA Secure Erase command - available in Ultimate package

New features for version 12 include:

- Customizable Printable Labels
- Customizable Sound Notifications
- Redesigned and improved printable Certificates and Reports
- Disk Serial Number can be properly detected for most scenarios, including disks connected via USB
- Many other enhancements and stability improvements while working with unstable disks

This release is available as an executable to run in your desktop environment, or in a bootable format with the help of the Active@ Boot Disk Creator - the bootable disk creation tool included in the installation package.

System Requirements

KillDisk runs on Linux and Windows operating systems with the following minimum requirements:

Workstation:

- PC: x64 (64-bit) or x86 (32-bit)
- CPU: Intel or AMD
- RAM: 512 Mb (Windows), 1 Gb (Linux)
- Disk: 100Mb of disk space

Video:

- VGA (800x600) or better resolution

Operating System:

- Windows XP to Windows 10, Server 2003 to 2016 (Windows version)
- Linux Kernel 2.x and higher (Linux version)

Drive Storage:

- CD/DVD/Blu-Ray optical drive (for applicable boot disk features)
- USB 1.0 / 2.0 / 3.0 storage device (for applicable boot disk features)
- 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)
- KillDisk supports all drives seen by the Operating System with read/write access, additional drivers can be loaded onto the boot disk for drivers not included by default in the bootable environment

Software Licensing

KillDisk is licensed **per concurrent use of the software** and **for each concurrent disk being erased or wiped**, outlined in the EULA. The maximum number of disks erased in parallel corresponds to the number of purchased licenses.

One Corporate license grants you the ability to run the software on one machine and erase one disk at any given time. **To run on several machines in an office or multiple drives concurrently on one machine, you require the corresponding number of licenses.**

Site and Enterprise licenses grant the license holder *unlimited* use of the software in a geographical location and worldwide respectively.

This licensing is maintained through software registration and activation. Once the full version of KillDisk is purchased, the license holder will receive an email with their **Registered Name** and **Registration Key**. Any machine that needs to use the full version of the software needs to be activated with this key.

Activations are limited to the number of licenses held. To transfer from one machine to another, they must be deactivated from decommissioned hardware first.

For boot disks to be created, the Active@ Boot Disk Creator must be registered with an active registration key.

Registering the Software (Online)

For this task you require an active internet connection on the machine you wish to register the product on.

After installation, Active@ KillDisk still starts as FREE version (unregistered), you need to register it first to have all professional features activated. To register the software with an active internet connection:

1. Select **Register or Upgrade Software** in the initial Registration & Licensing dialog launched on application start up, or click **Registration...** from the Help menu to access it from the application.

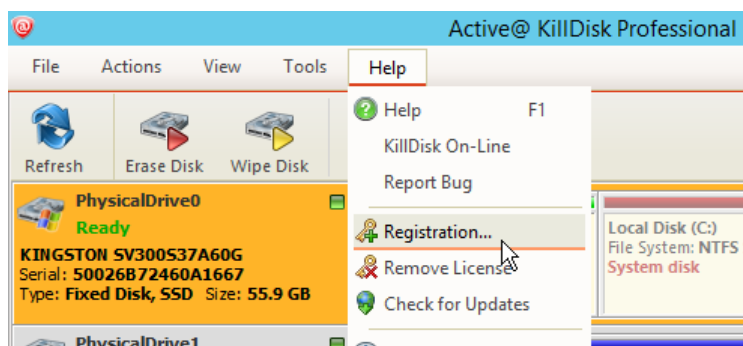


Figure 1: Accessing the registration window

2. Select the **Register or Upgrade Software** radio button
3. Read the License agreement and activate the check box to agree to the terms of the license
4. Click **Next** to proceed with the registration



Figure 2: Registration window

5. Copy & Paste your 30-digit registration key into the field called **Registration Key**:
6. You should receive a response that the software has been registered. The registration is now complete. You may click **Next** and exit the registration window

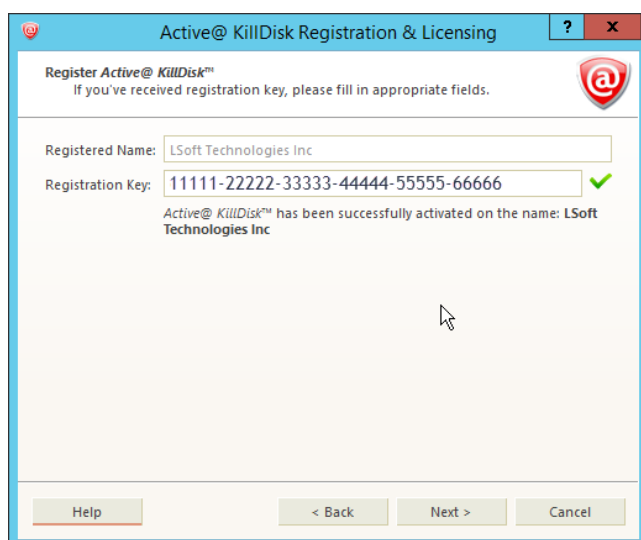


Figure 3: Completed registration

You now have access to the full features of the application.



Note: If your registration key is too long, you are using the key for an earlier version. Ensure you update to the latest version by making sure your support and updates are active and use the key to this latest version. This can be done through your client profile.



Note: You can also load registration information from a text file, (either INI or TXT type) where the first line is the name and second line is the key.

Registering the Software (Offline)

For this method of activation, you need any computer with a web browser and active internet connection and a USB. **Use this method only if the computer you are activating does not have internet access.**

In some cases, such as security or lack of access, you may not have access to an internet connection on the machine you wish to install the software on. For offline activation:

1. Select **Register or Upgrade Software** in the initial Registration & Licensing dialog launched on application start up, or click **Registration...** from the Help menu to access it from the application.
2. Select the **Register or Upgrade Software** radio button
3. Read the license agreement and activate the check box to agree to the terms of the license
4. Click **Next** to proceed with the registration
5. Copy & Paste your 30-digit registration key into the **Registration Key:** field. The Activation Request and Activation Response boxes will appear

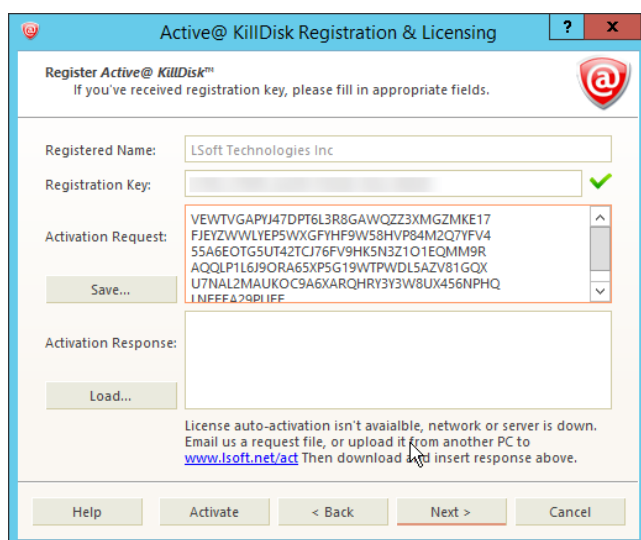


Figure 4: Offline activation boxes appearing

6. Click **Save...** to generate a registration request file. Copy this file to a USB.
7. Bring the USB to a computer with an active internet connection
8. Open the web browser and navigate to lsoft.net/act
9. Import the request file using the **Choose File** button and click **Load**
10. Click **Process!** to generate the Activation Response
11. Save the response to your USB by clicking **Save to *.licenseActivated**

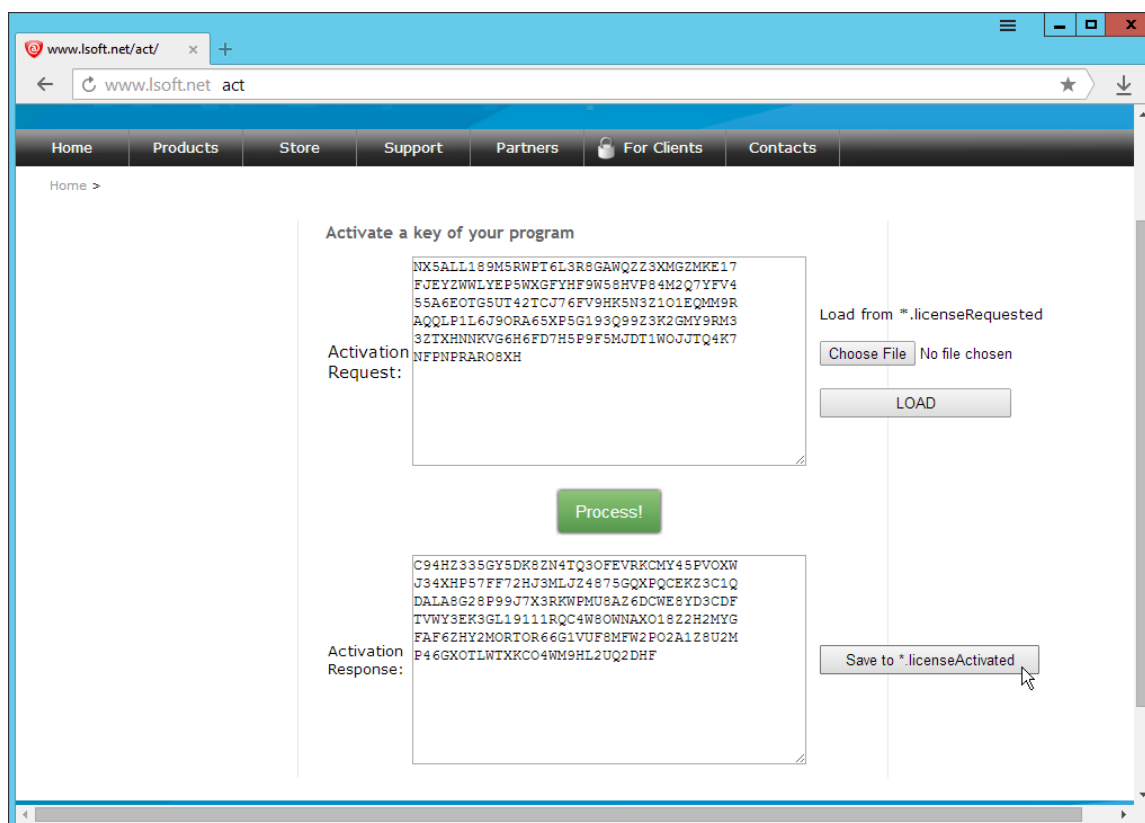


Figure 5: Generating an offline activation

12. Bring the USB to the machine with KillDisk installed
13. Import the activation response in the registration window and click **Activate**

You have now activated the software on your offline machine.

Deactivating a Registration

To transfer licenses from one machine to another, you will need to free up your activation on the licensed machine. You may do this by deactivating the registration from within the KillDisk application:

1. Click **Help > Remove License** in the file menu bar
2. Click **Deactivate Registration** in the pop-up licensing window

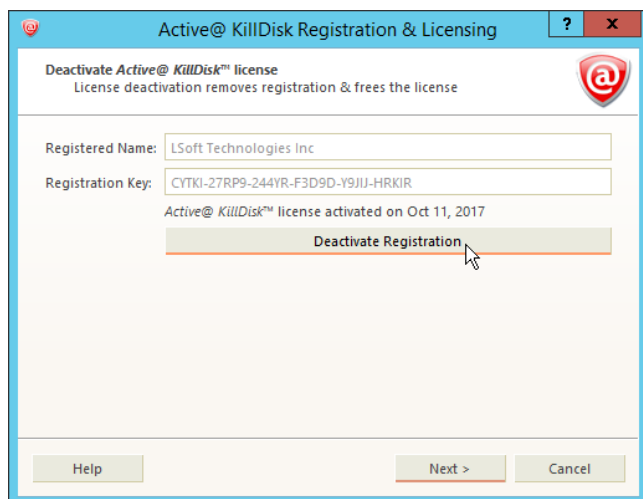


Figure 6: Deactivating a registration

Your active license is now revoked from your machine and may be used to activate a different computer.



Note: Uninstalling the application from the computer using the uninstaller will also deactivate your license from the machine, provided the machine has an active internet connection

Software Updates

KillDisk has a built-in update client to ensure you always have access to the latest version of the application. To update, use the file menu bar to navigate to **Help > Check for Updates**



Figure 7: Checking for updates

Update dialog contains history of previously installed versions and updates.

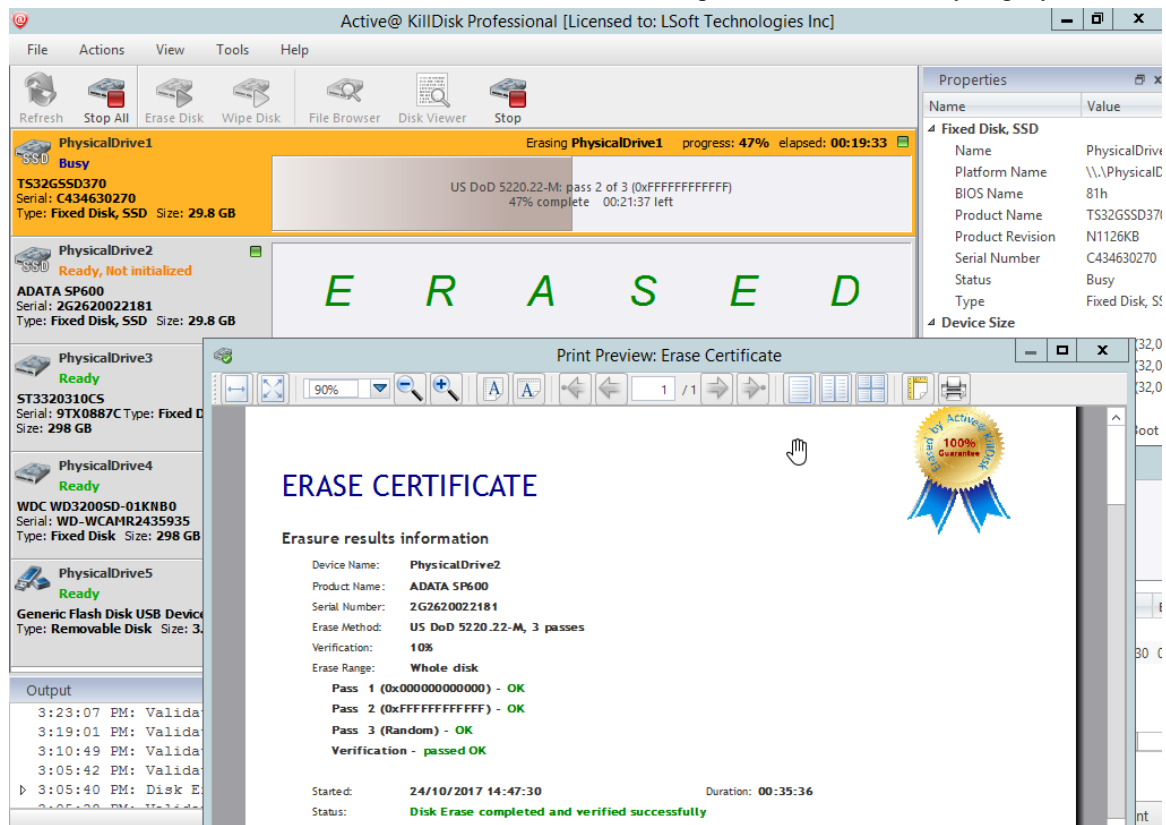
If a new version or update is detected, it can be downloaded and installed on the next wizard steps.



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

Getting Started with KillDisk

This section outlines the essential features of KillDisk and explains basic functionality to get you started.



KillDisk Installation and Distribution

KillDisk distribution overview

After purchasing Active@ KillDisk a registration key will be emailed to you, as well as a download link to installation package named KILLDISK-<VERSION>-SETUP.EXE . This file contains everything you need to get started - just double click on the file and installation wizard will take you through the setup process.

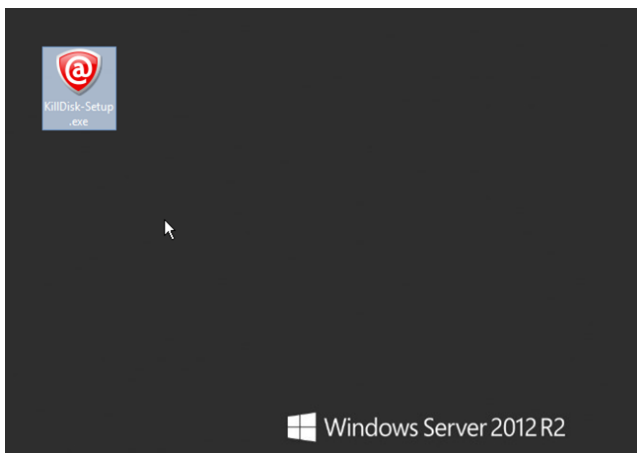


Figure 8: Installation file



Note: If you purchased the Ultimate version, you will receive installation executable file to run on Windows. To access the Linux installation files, install KillDisk on your Windows machine and navigate to the application directory. In Linux subfolder you will find the Linux installation files. The path to the linux application will look something like: C:\Program Files\LSoft Technologies\Active@ KillDisk Ultimate 11\Linux\KillDisk_Linux_Installer.tar.gz

After installation Active@ KillDisk still starts as a FREE (unregistered) version. You need to register it first to have all professional features activated.

Windows or Ultimate versions:

To install the application, double-click KILLDISK-SETUP.EXE and follow the instructions in the installation wizard.

The installed application contains two main applications:

- Active@ KillDisk for Windows (KillDisk.exe) — Run this application from your Windows operating system to inspect local disks and erase/wipe your data.
- Active@ Boot Disk Creator (BootDiskCreator.exe) — Create a bootable WinPE-based CD/DVD/BD or USB disk to boot from and run Active@ KillDisk for Windows. Using Active@ KillDisk this way allow you to wipe out confidential data from the system volumes while gaining exclusive use to partitions because the operating system runs outside the partition that you are securing.

Linux versions:

To install KillDisk on Linux, make sure you found the Linux file, as mentioned in the note above. Double-click **KillDisk_Linux_Installer.tar.gz** in your Linux environment and unpack the archive to a proper location. To install, simply run the following command in the directory where the archive was unpacked:

```
sudo ./KillDisk_Linux_Installer.run
```

Active@ Boot Disk Creator

Active@ Boot Disk Creator helps you prepare a bootable CD, DVD, Blu-ray or USB mass storage device that you may use to start a machine and repair security access issues or destroy all data on the hard drives.

To prepare a bootable device:

1. Run **Bootable Disk Creator** from the Windows Start menu (Windows platform). The Active@ Boot Disk Creator wizard will appear.

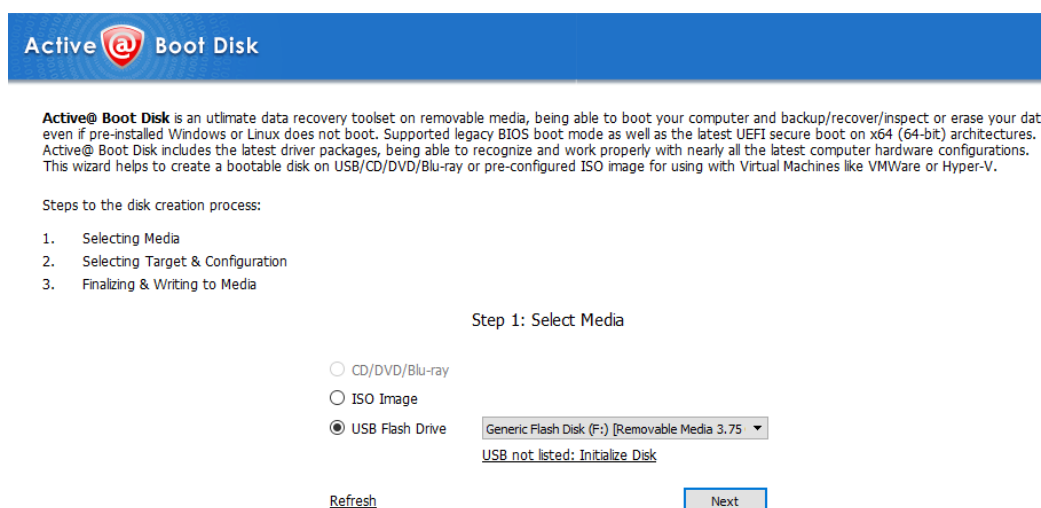


Figure 9: Bootable Bisk Creator

2. If Active@ KillDisk has not been registered yet, you need to register software first by clicking **Register** in the bottom-right corner and [Registering the Software](#)
3. In the Active@ Boot Disk Creator main page, select the desired bootable media: a **CD/DVD/Blu-ray**, a **USB Flash Drive** or an **ISO Image file** to be burned later on. If several media drives are inserted, click the ellipsis button (...) and choose a particular device. Click **Next**.



Note: If your USB bootable disk does not appear in the drop-down list, click **Initialize Disk**. You should be able to find the device in the setup menu and initialize it to be compatible with the application. This process **will** erase all data on the selected device.

4. Select the target platform for booting up. Depending on Active@ KillDisk version you purchased, one or more target platforms will be available for selection (Windows-based, Linux-based or Console).

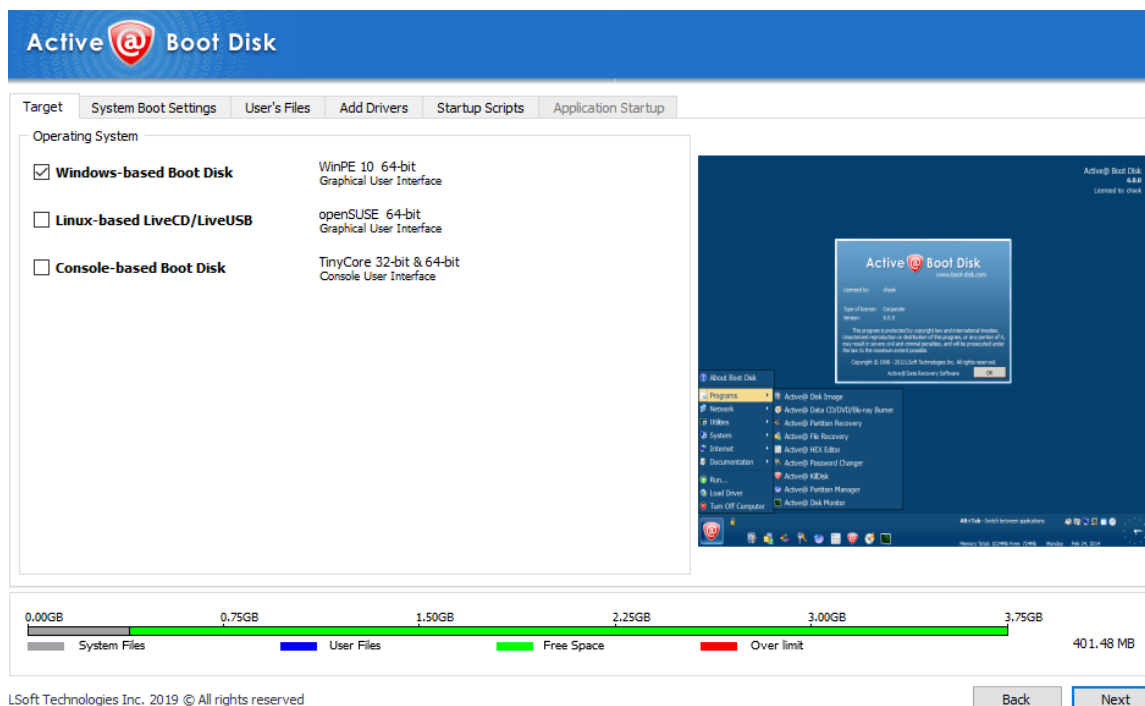





Figure 10: Creating Windows-based boot disk

5. At this step you can specify additional boot disk options:

- a) To customize boot options, click the **System Boot Settings** tab. You can change the default settings to be used: Time Zone, Additional Language Support, Default Application Start and Auto-Start Delay. You can also change these options in the Active@ Boot Disk initialization screen while booting (Windows version). Additional Network and Security sub-tabs allow to configure static IP & Firewall settings, as well as to protect your Boot Disk with a password at boot time.
 - b) To add your custom files to the bootable media, click the **User's Files** tab. Add files or folders using the related buttons at the right side. Added items will be placed in the User_Files root folder
 - c) To add specific drivers to be loaded automatically, click the **Add Drivers** tab. Add all files for the particular driver (*.INF, *.SYS, ...). Added items will be placed in the BootDisk_Drivers root folder. At boot time all *.INF files located in this folder will be installed.
 - d) To add specific scripts to be launched after Active@ Boot Disk is loaded, click the **Add Scripts** tab. Add your scripts (*.CMD files). Added files will be placed in the BootDisk_Scripts root folder. At boot time all *.CMD files located in this folder will be executed.
 - e) To add command line parameters for KillDisk startup after the boot, click **Application Startup** tab and type desired parameters. This tab is available only if Default Application Start option is turned ON on the **System Boot Settings** tab
6. Click **Next**. Verify the selected media, sizes and boot up environment.
 7. Click **Create**. A progress bar appears while the media is being prepared.
-  **Note:** Not all additional boot disk options are accessible for all platforms. For example, Add Drivers section applies only to Windows Operating System, and is available for Windows target only.
 -  **Note:** A USB Drive or blank CD/DVD/BD must be inserted and explicitly chosen on the first step before you can proceed further.
 -  **Note:** If you've created an ISO Image file, you can burn it to a disk later on using either our free Active@ ISO Burner utility (www.ntfs.com/isoburning.htm) or a utility of your choice.

Navigating Killdisk

Once the KillDisk application is launched, you will be presented with the main KillDisk application dashboard. From here you can use any of KillDisk's tools on your system. This section will outline the main components of the application. The full functionality and features of these components are discussed in their corresponding sections later in this documentation:

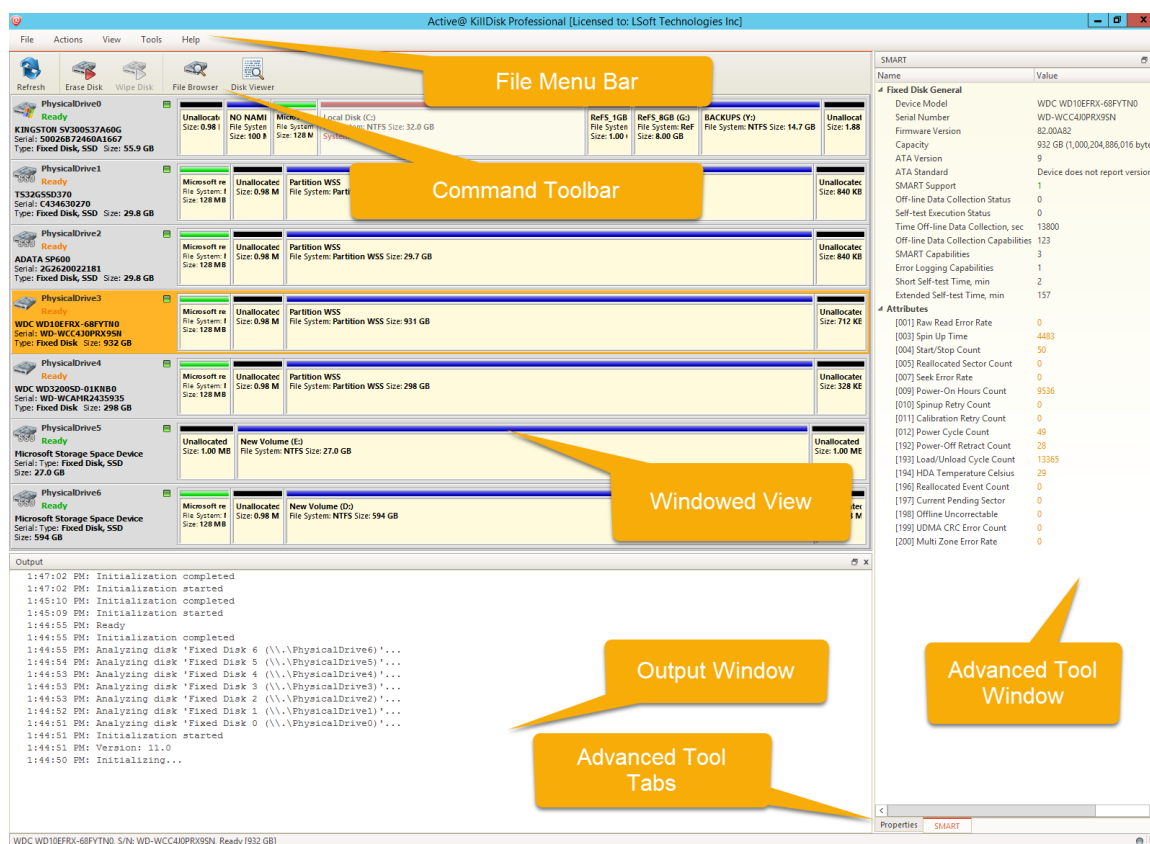


Figure 11: Navigating the KillDisk application

File menu bar

The file menu bar contains actions to perform nearly any operation in KillDisk, such as accessing settings and help, changing views and what is visible in the dashboard, opening tools, and navigating between KillDisk's windows.

Command Toolbar

The command toolbar is a dynamic toolbar that allows the user to perform Tabbed Window-specific actions, depending on the context.

Windowed view

Contains the window that is currently active. By default you can see here all HDD/SSD/USB disks attached to the workstation.

Output window

Contains the log of operations KillDisk has performed.

Advanced tool window

This window shows the data for the Advanced tool selected. The window can be moved, popped out and re-sized.

Advanced tool tabs

These tabs allow for navigation between the different advanced tool windows.

To browse through each of these views, click on the appropriate tab. You may also open a view from the **View** menu.

To close the current view at any time, press **CTRL+F4**. To open any closed view, select it from the **View** menu.

The status bar, at the bottom of the workspace shows the current status of the application or status of the activity in progress.

Disk Explorer

The **Disk Explorer** is a default view and interface for the KillDisk application. All attached HDD/SSD/USB disks are visualized, can be selected and manipulated here. New procedures like erasure can be initiated here, as well as displayed the status and progress for actions performed with disks.

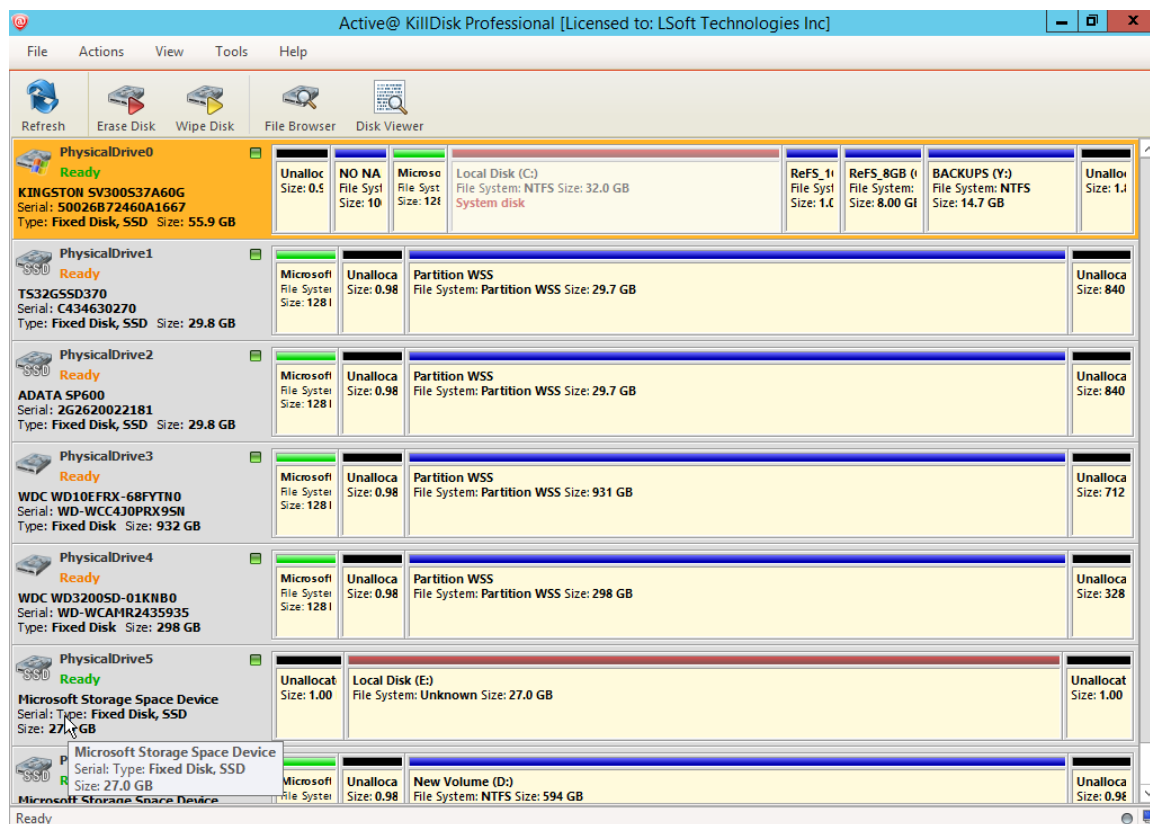


Figure 12: Disk Explorer

Using KillDisk

KillDisk is a powerful tool to provide disk erasure solutions for personal and corporate use. This section outlines the key features of KillDisk and how to use this software's many features. Much of the software is highly customizable and this guide will help get you started with configuring KillDisk for your particular system, and using KillDisk to its' full potential.

Disk Erase

KillDisk is an extremely powerful tool for secure disk erasure. Individual disks or batches of disks can be erased to any desired standard with just a few clicks. The process to achieve this is outlined in this section.

1. Select a disks for erasure

Use [Disk Explorer](#) on page 19 to select proper disks.

2. Open **Erase disks** dialog using one of the following methods:

- Click the **Erase** command in the action toolbar
- Click **Actions > Erase Disk** command from main menu
- Click **Erase Disk** command from context menu
- Press **F10** key

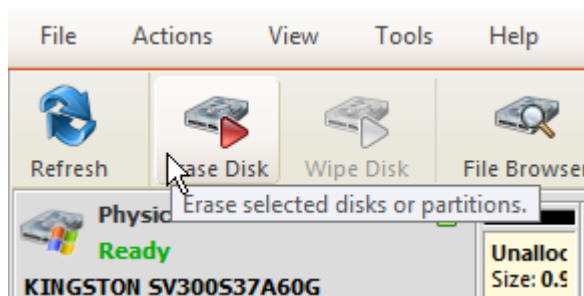


Figure 13: Initiating the Erase operation

3. Confirm erasure options

Disk Erase options dialog pops up:

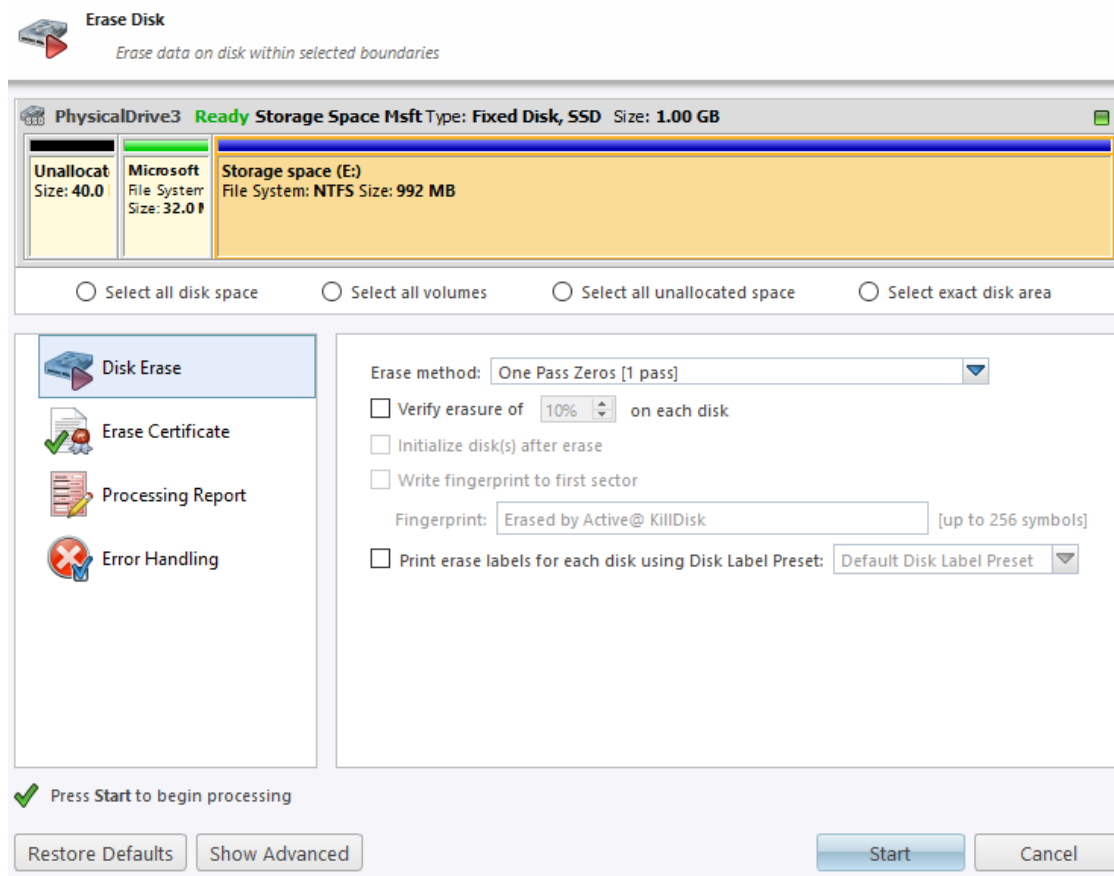


Figure 14: Disk Erase Options

Use tabbed views to adjust disk erasure options if necessary. Available options:

- [Disk Erase Options](#) on page 39
- [Certificate Options](#) on page 41
- [Report Options](#) on page 43
- [Error Handling Options](#) on page 49

Note:

If only one disk was selected for erasure than you can specify boundaries of erased area for selected disk by clicking **Select exact disk area**. Here you may select sector ranges, or select individual partitions.

If single disk is selected for the **Erase Disk** command, disk area to be erase can be specified:

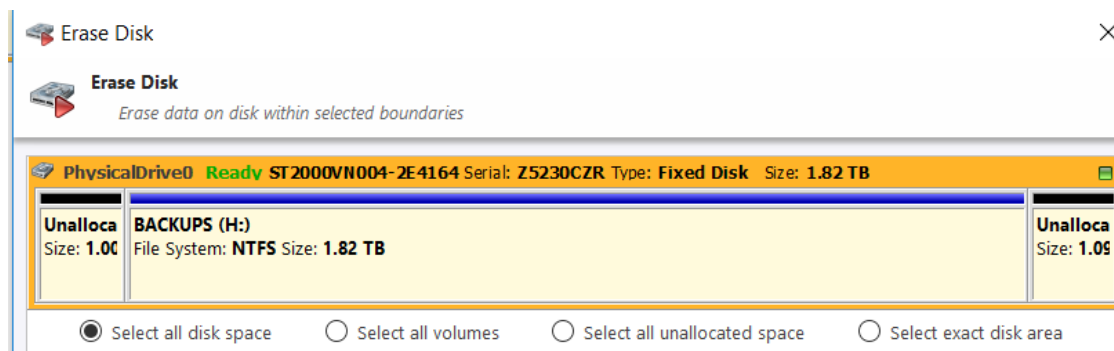


Figure 15: Erase Disk - Area Selection

Select all disk space

Entire surface of the disk will be erased

Select all volumes

Select for erase the only disk's space where live volumes located

Select all unallocated space

Select for erase the only disk's unallocated area, the space where no live volumes exist

Select exact disk area

Allows you to use the sliders on the visualization of your disk to select a particular range of sectors for erasure.

You may also click on individual partitions and the selected individual partitions will be erased.

Click **Start** button to go to the final confirmation dialog:

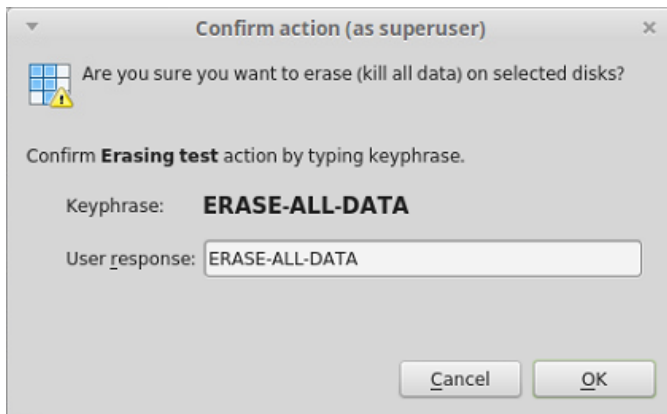


Figure 16: Disk Erase Confirmation

Click **OK** button to begin disk erase process.

4. Observe erase process

Once the Erase procedure begins, you will see the disk area representing as a progress bar and it will show the erase method and progress of that disk operation. The progress bar represents the percentage of data left to erase on the drive, with the corresponding percentage shown. As the procedure progresses, the percentage will decrease, and the red bar will get smaller.

The remaining time will also be seen and progress in the operation will be displayed, as shown below:

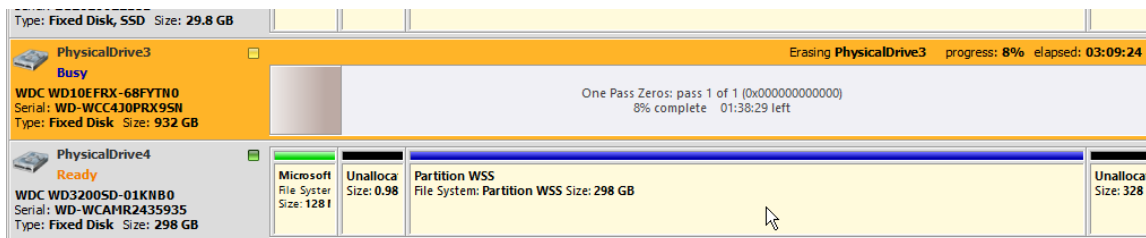


Figure 17: Disk Erase Progress

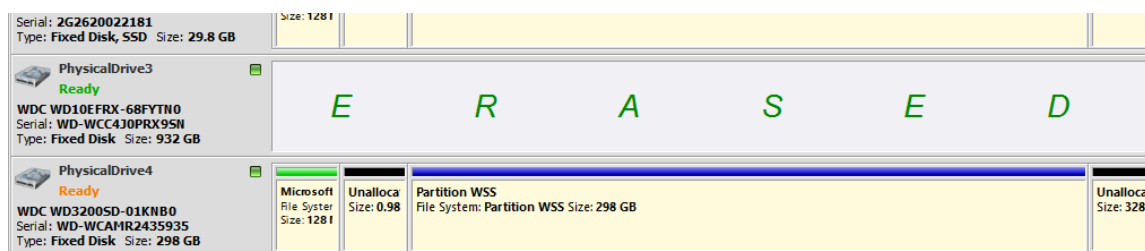


Figure 18: Disk Erase Completed

When erasing completed you can review results and print an [Erase Certificates](#) on page 27 and [Erase Labels](#) on page 28 for processed disks.

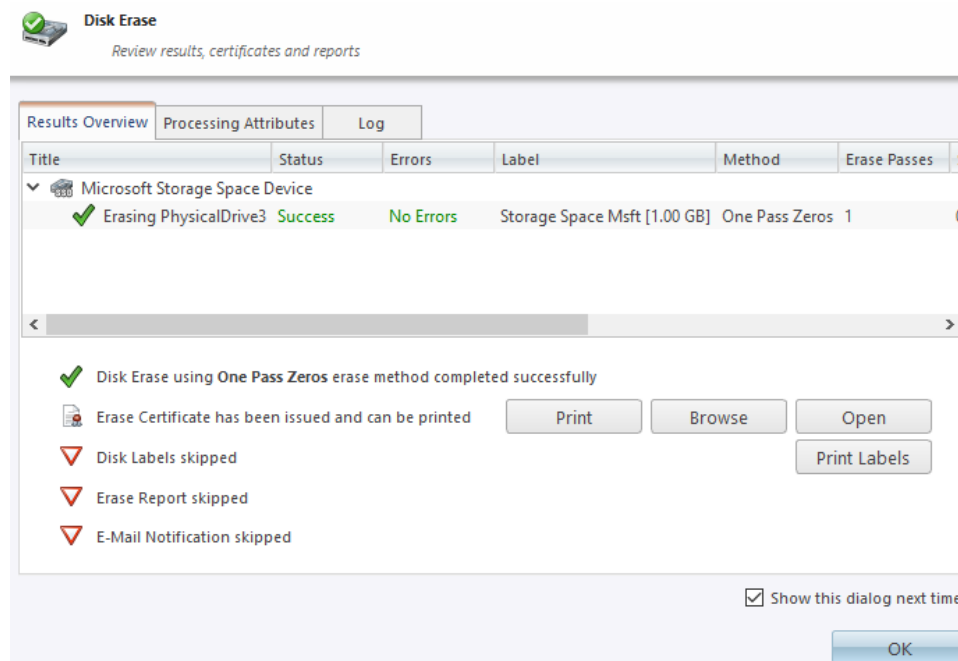


Figure 19: Disk Erase Summary

Selecting Disk Area for Erasure & Erasing Partitions

In **KillDisk**, you have the option to specify the area on the disk to erase. To access this feature, you must select the disk first. From **Actions** menu, initiate the **Erase Disk** operation. The default option is **Select all disk space**, which will apply the selected operation on the entire disk selected.

If you're interested in specific areas of the disk (specific partitions, for example), you may use the **Select exact disk area** option. This will allow you to use the sliders on the visualization of your disk to select a particular range of sectors. You may also click on individual partitions and the individual partitions will be selected for erasure.

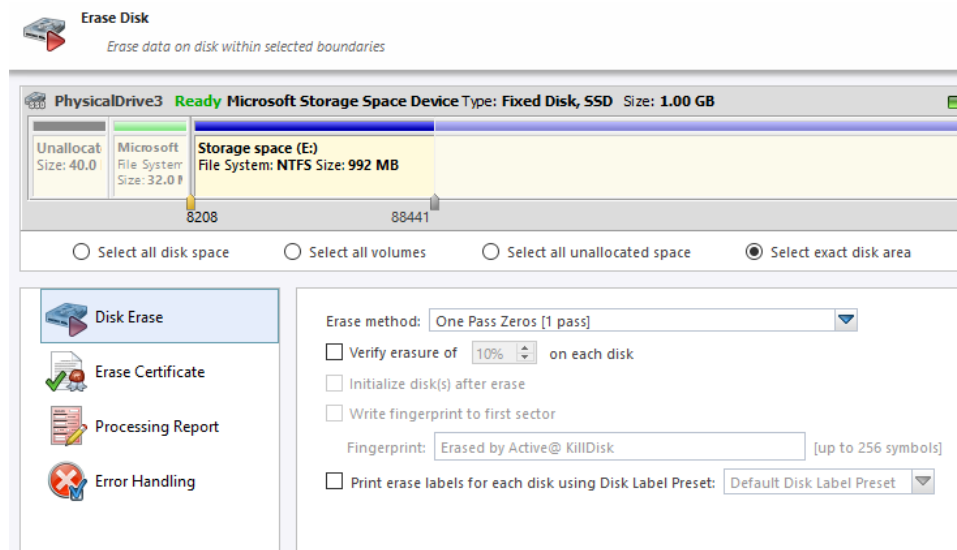


Figure 20: Erasing a specific partition

Disk Wipe

When you select a physical device, the **Wipe** command processes all logical drives consecutively, erasing the only data in unoccupied areas (free clusters and system areas), leaving existing data intact. *Unallocated space* (where no partition exists) has been erased as well.

Note: If you want to erase all data (existing and deleted) from the hard drive device permanently, see [Disk Erase](#) on page 20.

If KillDisk detects that a partition has been damaged or that it is not safe to proceed, KillDisk does not wipe data in that area. The reason it does not proceed is that a damaged partition might contain important data.

There are some cases where partitions on a device cannot be wiped. Some examples are an unknown or unsupported file system, a system volume, or an application start up drive. In these cases the **Wipe** command is disabled. If you select a device and the **Wipe** button is disabled, select individual partitions (drives) and wipe them separately.

To Wipe out a disk or volume:

1. Select a disk or volume to wipe out in the disk explorer. You may select multiple disks/volumes to be wiped out simultaneously
2. Click the **Wipe** toolbar button to wipe out all data in unoccupied sectors on the disk or one of its' partitions. Alternatively you can execute **Wipe** command from **Actions** menu, use the context menu or press **F9**

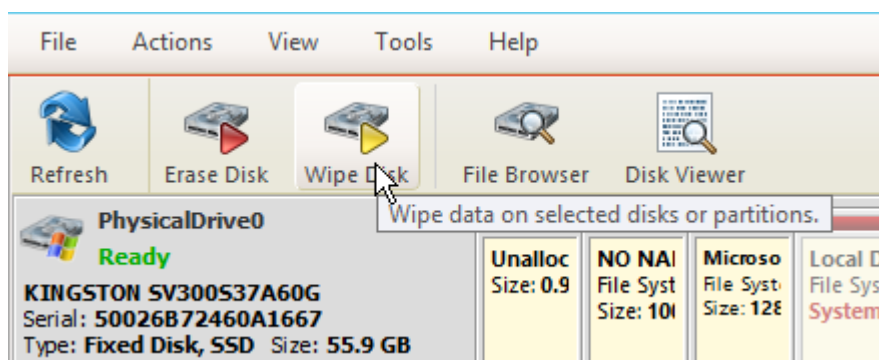


Figure 21: Initiating the Wipe operation

3. Confirm Wipe Options

Use tabbed views to adjust disk wipe options if necessary. Available options:

- [Disk Wipe Options](#) on page 41
- [Certificate Options](#) on page 41
- [Report Options](#) on page 43
- [Error Handling Options](#) on page 49

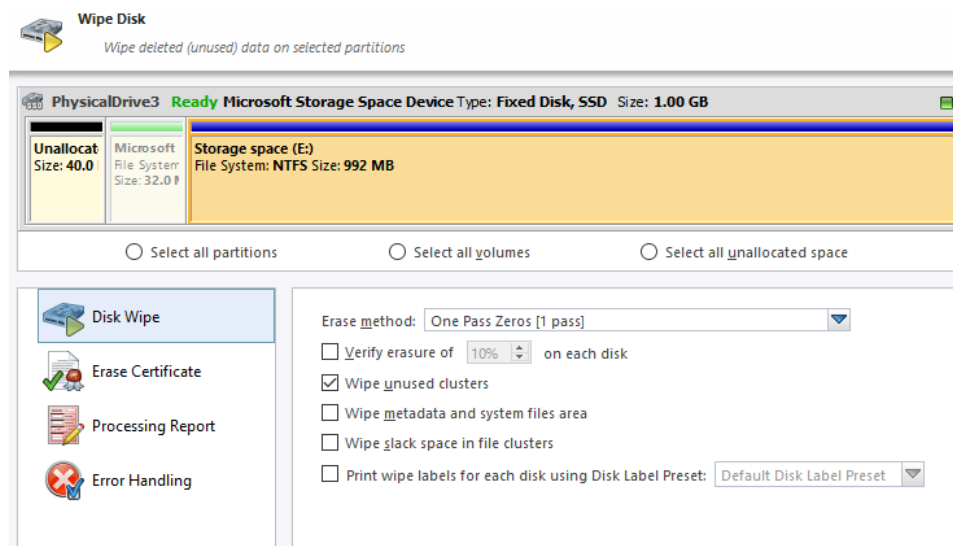


Figure 22: Selecting erase method for the wipe

4. Select the areas of the disks to be wiped. With individual disks you may select individual partitions.
5. Click **Start** to advance to the final step before erasing data. Confirm **Wipe** action and process starts.
6. The progress of the wiping procedure will be monitored in the Disk Wiping screen.

To stop the process for any reason, click the stop button for a particular disk. Click the stop all button to cancel wiping for all selected disks. Note that all existing applications and data will not be touched. Data that has been wiped from unoccupied sectors is not recoverable.

7. Optional: Select the wiped partition click **File Browser** toolbar button to inspect the work that has been done.

KillDisk scans the system records or the root records of the partition. The **Browser** tab appears. Existing file names and folder names appear with a multi-colored icon and deleted file names and folder names appear with a gray-colored icon. If the wiping process completed correctly, the data residue in these deleted file clusters and the place these files hold in the directory records or system records has been removed. You should not see any grey-colored file names or folder names in the wiped partition.

You will see a confirmation dialog when the process is complete, where you may and print an [Erase Certificates](#) on page 27



Note: If there are any errors, for example due to bad clusters, they will be reported on the Interactive screen and in the Log. If such a message appears, you may cancel the operation or continue wiping data.

Processing Summary

Once KillDisk's finishes processing any task, such as disk erasure or disk wipe, a task complete dialog will appear with a summary of the task, containing all of the information pertaining to the operation. For example, this includes information like disks operated on, status of erasure and all associated certificates and reports.

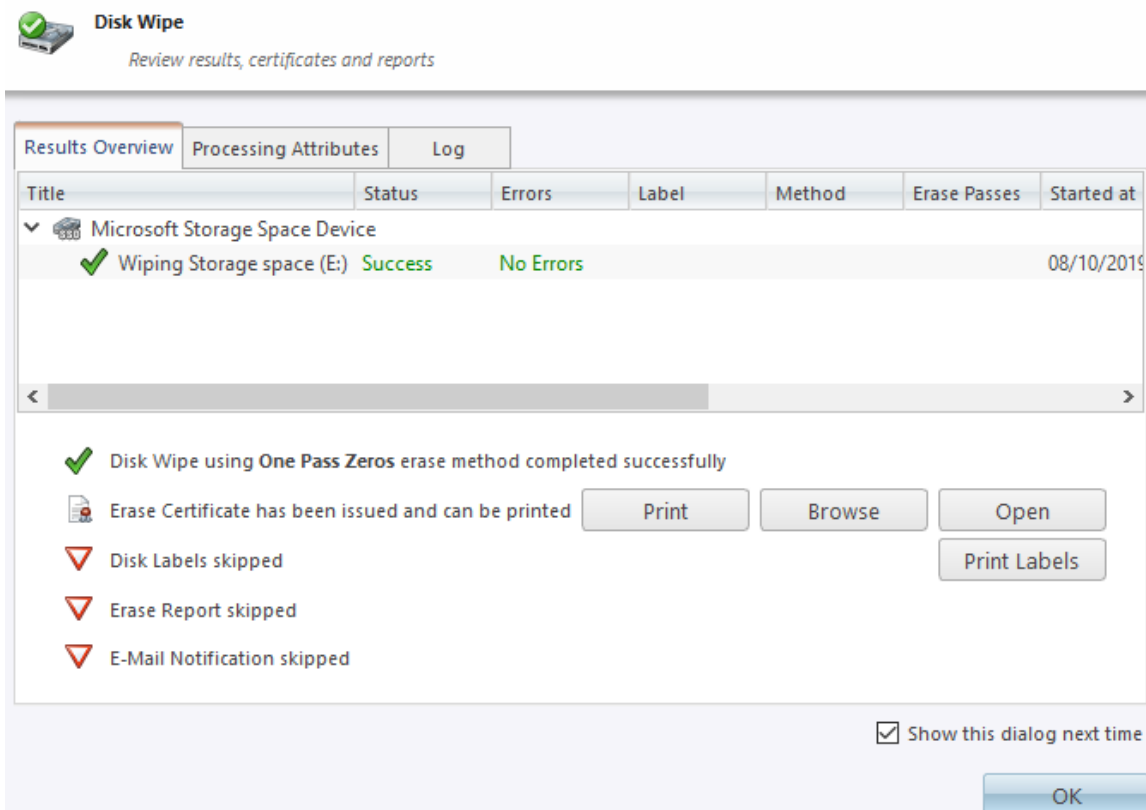


Figure 23: Example of task complete dialog

The successful erasure window contains the features of the successful erasure, discussed further in this section.

Devices

All devices erased are displayed with their erasure status in list format at the top of the notification.

Erase Status

Details the status of the disk erase operation showing the erasure specifications and status with which the erasure was completed.

Disk Certificate

Verifies that the erasure PDF certificate has been saved and specifies the path to the saved report. Allows user to examine the certificate by pressing the **Open** button.

Disk Report

Verifies that the erasure report has been saved and specifies the path to the saved report. Allows user to examine the .xml erasure report by pressing the **Browse** button.

Print Labels

Allows user to examine, customize, change options and print labels by pressing the **Print Labels** button.



Note: The Wipe operation will produce a similar processing summary for the disk wipe

Certificates, Labels and Reports

KillDisk maintains the highest standards in disk erasure, and with that, provides extensive documentation options for its' operations through [Reports](#) , [Labels](#) and [Certificates](#). This section will discuss these features in length.

Erase Certificates

Overview

KillDisk provides PDF certificates of erasure upon the completion of data erase operations. These certificates may be customized to include company-specific information and notes specific to the particular procedure. Configuring these custom settings is outlined in the [Certificate Preferences](#) section of this guide. A sample of the certificate is shown below:

Figure 24: Disk Erase - Batch Certificate - First Page

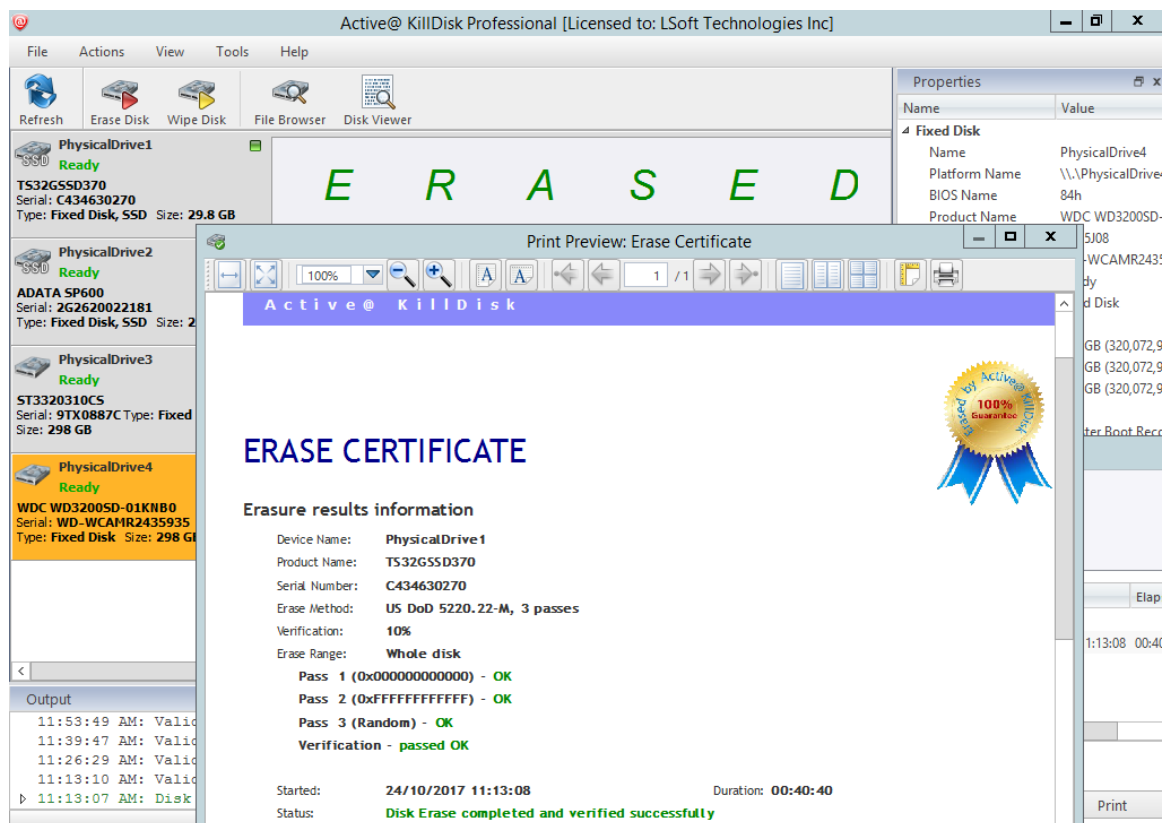


Figure 25: Disk Erase - Batch Certificate - Second Page

Certificate Elements

Company Logo

Custom company's logo can be placed to the certificate instead of the default KillDisk's logo at the top right corner

Company Information

Displays all company information provided in the preferences. The user in the above example only provided their business name, but other company information may also be included in the certificate

Technician Information

Displays the technician information provided in the preferences. Namely, this section is for the name of the operator and any notes they may want to include in the certificate report

Erasure Results Information

Displays information pertaining to the erasure procedure conducted on the hard drive(s). Type of erasure algorithm, custom settings, date and time started and duration of the erasure are all listed here

Disk

Uniquely identifies the disk that was operated on by the KillDisk application. Includes information like Name, Serial Number, Size and Partitioning Scheme

System Information

Provides details on the system used to run KillDisk, such as the Operating System and architecture.



Note: The system information here only applies to the system running KillDisk, not the system that was erased by the application! Provided KillDisk remains on one workstation, this information will stay consistent with all systems that the workstation erases.

Erase Reports

KillDisk gives you the option to save XML reports for any major operation it performs on a disk, such as **Examination**, **Erase** and **Wipe**. These reports contain all the information pertaining to the KillDisk procedure. The contents of the report are outlined below.

<p>Company Information</p> <ul style="list-style-type: none"> • Name • License • Location • Phone • Disclaimer <p>Technician Information</p> <ul style="list-style-type: none"> • Name • Comments <p>System & Hardware Info</p> <ul style="list-style-type: none"> • OS version • Architecture • Kernel • Processors • Manufacturer <p>Erase Attributes</p> <ul style="list-style-type: none"> • Erase verify • Passes • Method • Verification passes <p>Error Handling Attributes</p> <ul style="list-style-type: none"> • Errors terminate • Skip interval • Number of Retries • Source Lock • Ignore Write Error • Ignore Read Error • Ignore Lock Error 	<p>Disks</p> <ul style="list-style-type: none"> • Device Size • Device Type • Serial Number • Revision • Product Number • Name • Geometric Information • Partitioning Scheme <p>Batches</p> <ul style="list-style-type: none"> • Name • Disks • Time <p>Additional Attributes</p> <ul style="list-style-type: none"> • Fingerprint Information • Initialization <p>Erase Result</p> <ul style="list-style-type: none"> • Bay • Time and Date Started • Disk Information • Status • Result • Time Elapsed • Errors • Name of operation
---	--

Erase Labels

Along with the PDF certificate, KillDisk allows you to print labels to place on erased disks with its Print Label features. Disk Labels with process results and essential disk information could be issues for any disk processing, such

as Disk Erase, Disk Wipe, Disk Examination and Disk Clone (for Industrial edition). These labels may be completely customizable to print on any sized sheet with any dimension. Simply specify the parameters and KillDisk will prepare the printable labels for you. The procedure is outlined in this section.

Accessing the Print Labels Option

Upon the completion of a major KillDisk operation, you will see a report dialog. In the list of completed tasks, you will see the **Print Labels** button, depicted below. Click it to enter the **Print Label Dialog**.

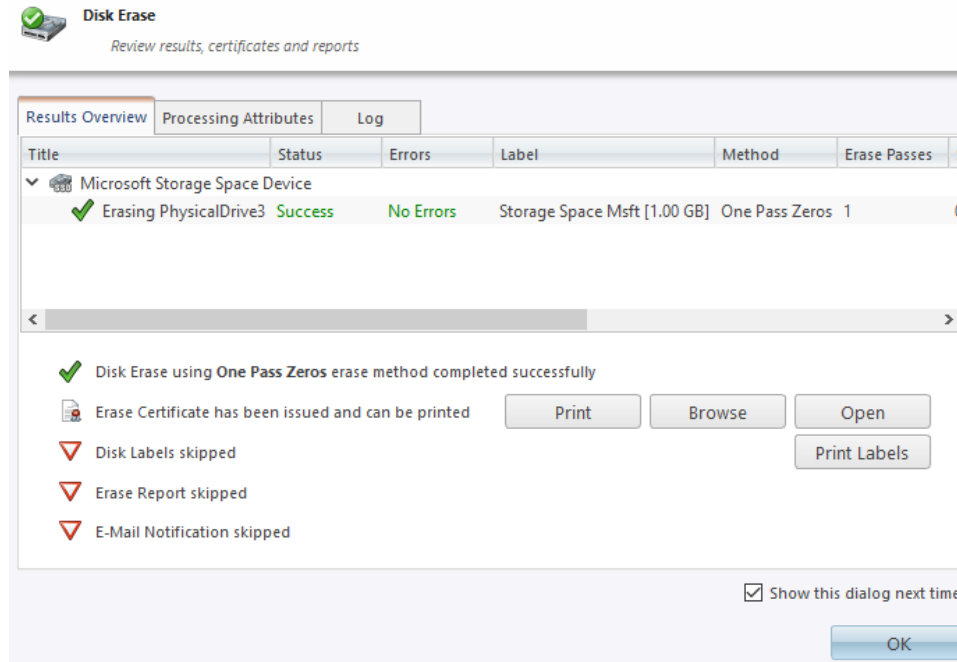


Figure 26: Opening Print Label Dialog

Print Label Dialog

This dialog will allow you to configure the labels and prepare them for printing. The top of the dialog will show you a list of the drives that will have labels generated for them. At any point in the operation, a sample of the label is shown in the **Preview** window on the left side. The right side of the dialog has the styling and template configuration options.

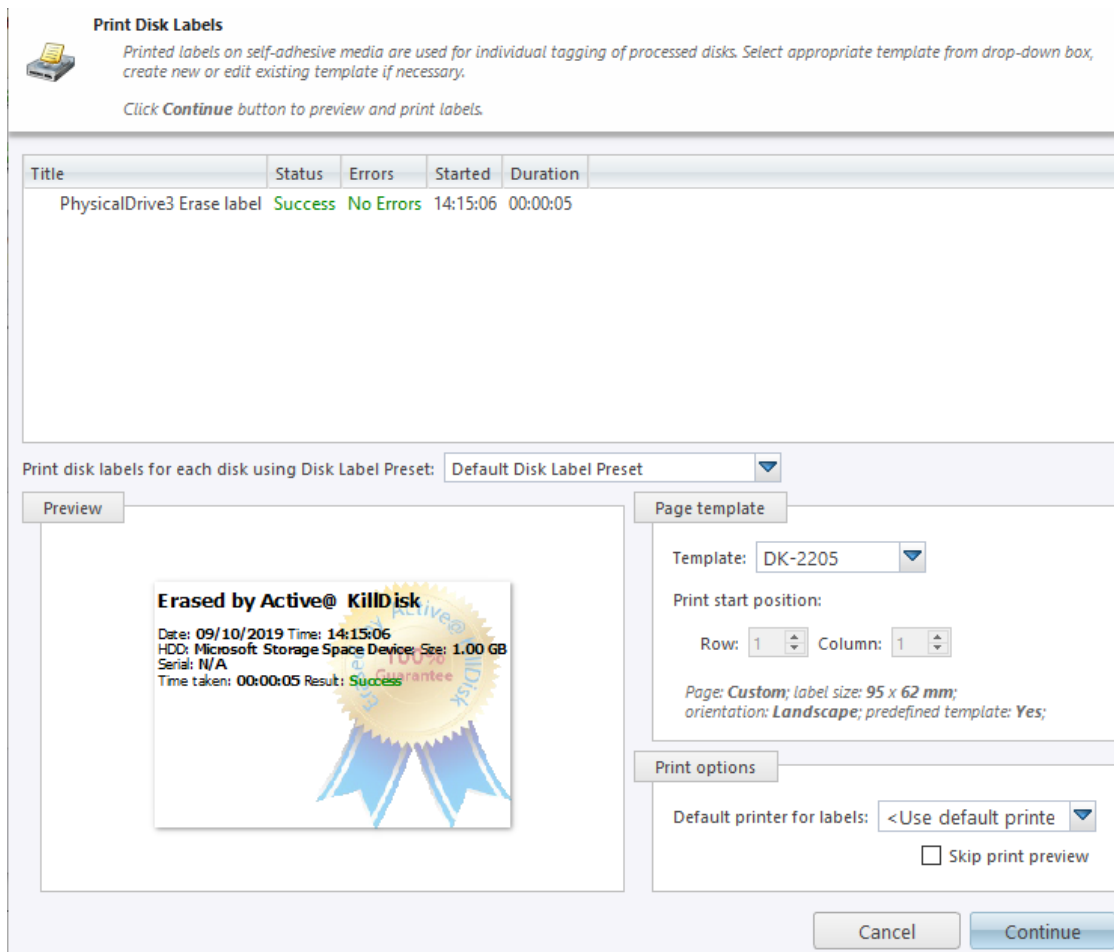


Figure 27: Print Label Dialog

Page template options

The print label dialog gives you access to a number of predefined standard presets and any custom templates you may create. These template may be easily selected without opening any additional dialogs and the details of the selected template will be displayed below the selection box

Print Start Position

The print start position section of the dialogue allows you to select what label on the page the labels start printing from. As you use labels, the labels won't always start from the 1x1 position, so you can adjust this setting accordingly.

Print Preview and Printing

Once all the settings are configured, you may see the print preview by clicking the **Continue** button. The preview displays what the print is going to look like and from here the print job can be sent to a printer that is configured with the system.

Skip print preview

Disable in-build system print preview dialog and print labels immediately when requested.

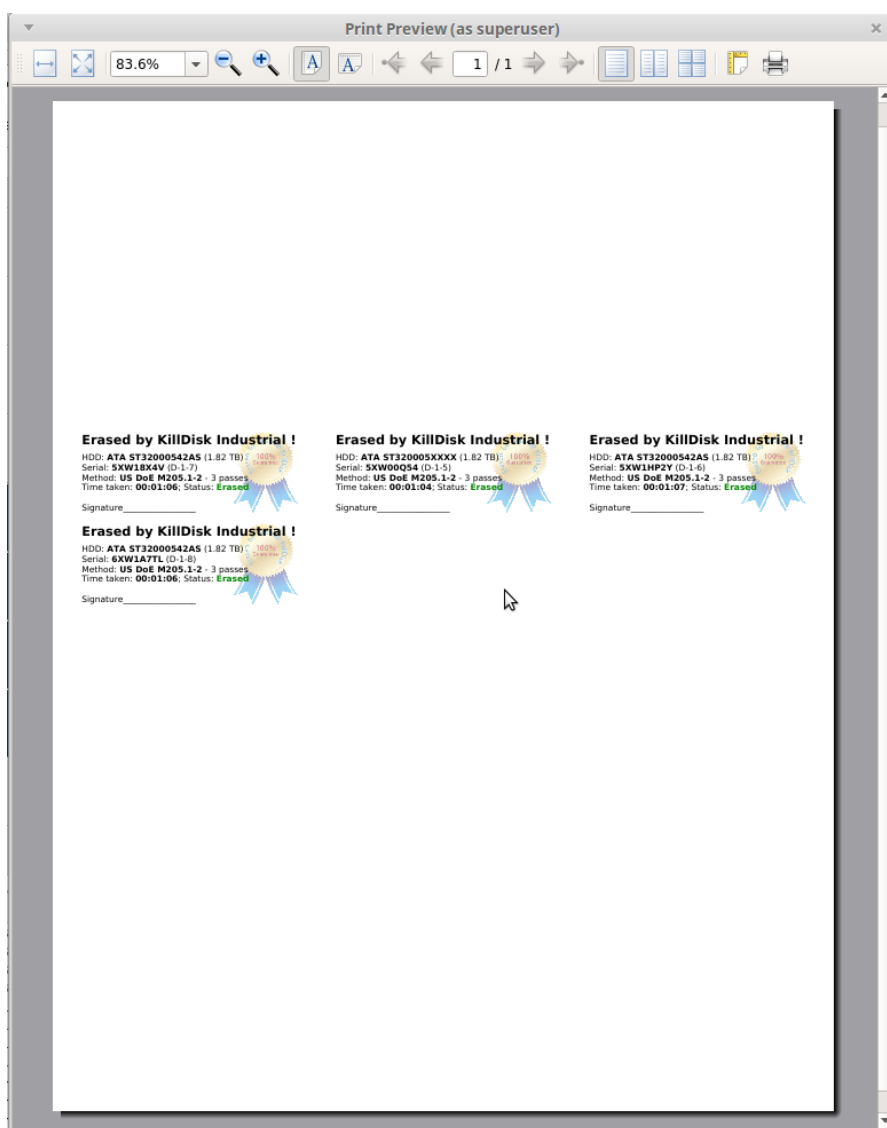


Figure 28: Example of a Print Preview

Additional Options and Features

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

Mapping Network Shares

Mapping Network Shares is very useful, especially when booting from a boot disk and running the application in batch mode. It guarantees a specific drive letter to save logs and certificates to, as well as provides a central location for erase reports to be stored.

To map a network share:

1. In the menu bar, navigate to **File > Map Network Share...**
2. Configure your network drive and assign a letter to it, then press **OK**

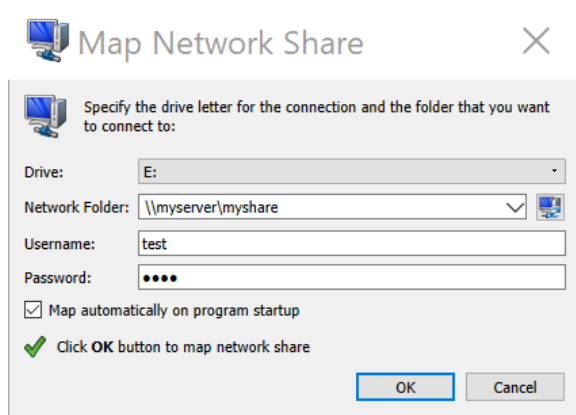


Figure 29: Mapping a network drive

Note: KillDisk will identify all connected network drives, so you may use the drop-down list to select the one you'd like to use

- Now that your network drive is configured, you may select it as a destination for certificates and reports in the [Preferences](#)

Changing Disk Serial Number

In case you notice a disk serial number does not match the number on the disk, KillDisk supports several methods of detecting disk serial numbers, where it pulls it from various sources. To access this feature, right-click the disk and select **Set Serial Number..** from the context menu.

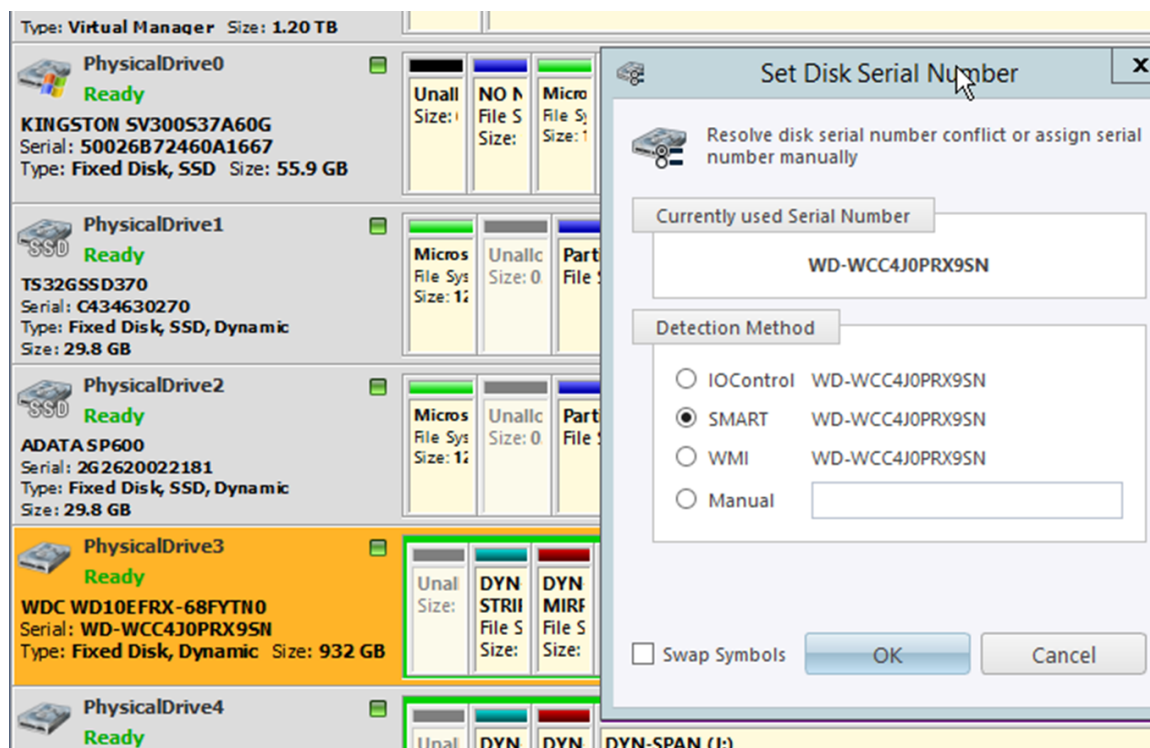


Figure 30: Setting the Disk Serial number

Note: If you don't see your serial number in any of the detection methods, try checking the **Swap Symbols** check box. If this doesn't help, input the serial number manually using the last option. The serial number you are looking for does not match the serial number stored by the disk (i.e. the sticker does not match the drive).

Reset Hidden Areas

KillDisk supports erasing hidden areas of the disk: **HPA** and **DCO**.

To perform this task on its' own, right click on the disk and select **Reset Hidden Areas...**

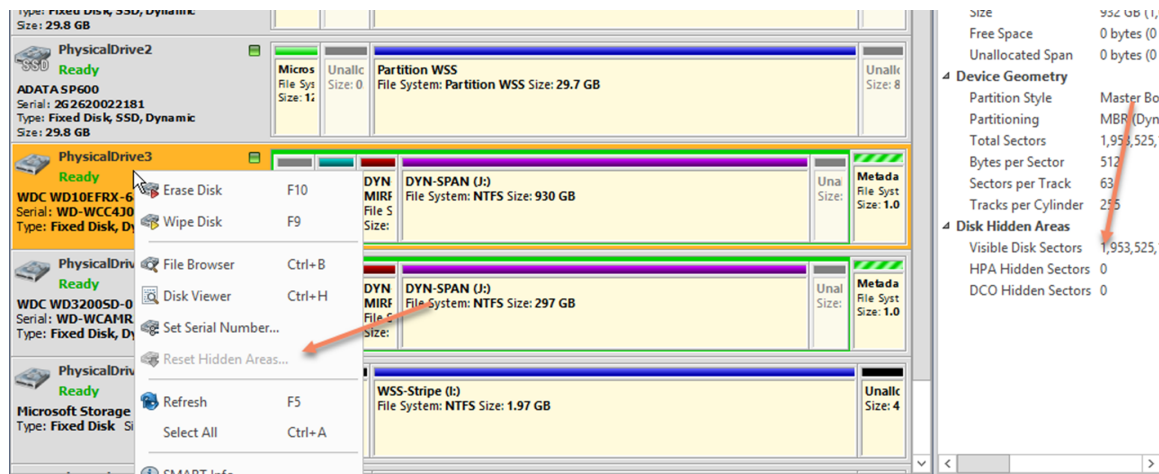


Figure 31: Resetting Hidden Areas

If related context menu item is disabled, there are no hidden areas on the disk has been detected, so nothing to reset.

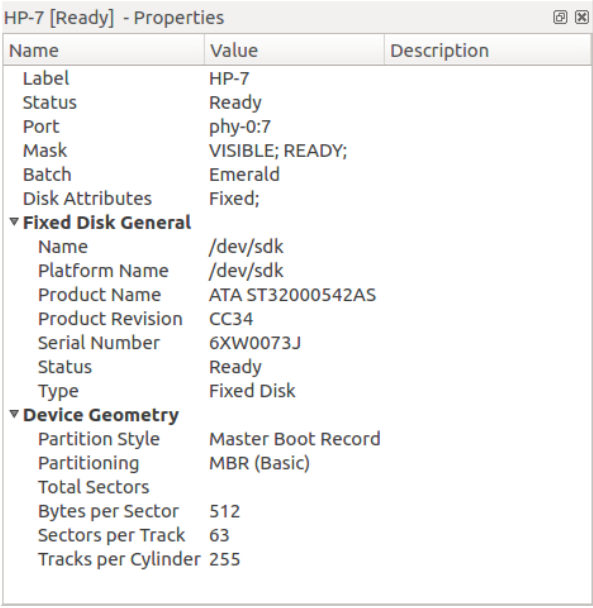
Property Views

To show detailed information about any subject of an application, such as disk, partition, volume, file etc., KillDisk uses information views. When open, they follow selected changes and show information about the selected item automatically.

Property view

To show property view for selected item do one of the following:

- Click **View > Windows > Properties**
- Click **F4** keyboard short cut or
- Use context menu command **Properties** for the same effect



Name	Value	Description
Label	HP-7	
Status	Ready	
Port	phy-0:7	
Mask	VISIBLE; READY;	
Batch	Emerald	
Disk Attributes	Fixed;	
▼ Fixed Disk General		
Name	/dev/sdk	
Platform Name	/dev/sdk	
Product Name	ATA ST32000542AS	
Product Revision	CC34	
Serial Number	6XW0073J	
Status	Ready	
Type	Fixed Disk	
▼ Device Geometry		
Partition Style	Master Boot Record	
Partitioning	MBR (Basic)	
Total Sectors		
Bytes per Sector	512	
Sectors per Track	63	
Tracks per Cylinder	255	

Figure 32: Property view example

Besides only displaying valuable data, they also allow you to copy that information onto a clipboard by using context menu commands.

Copy Value

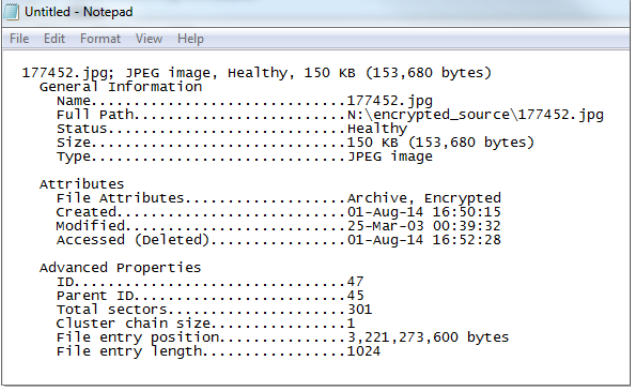
Copy only value of selected field in the information view.

Copy Field

Copy formatted name and value field pair.

Copy All

Copy all information as formatted set of name and value pairs.



```

Untitled - Notepad
File Edit Format View Help

177452.jpg; JPEG image, Healthy, 150 KB (153,680 bytes)
General Information
Name.....177452.jpg
Full Path.....N:\encrypted_source\177452.jpg
Status.....Healthy
Size.....150 KB (153,680 bytes)
Type.....JPEG image

Attributes
File Attributes.....Archive, Encrypted
Created.....01-Aug-14 16:50:15
Modified.....25-Mar-03 00:39:32
Accessed (Deleted).....01-Aug-14 16:52:28

Advanced Properties
ID.....47
Parent ID.....45
Total sectors.....301
cluster chain size.....1
File entry position.....3,221,273,600 bytes
File entry length.....1024
  
```

Figure 33: Example of Copied Information

S.M.A.R.T. Information

This is another information view, displaying SMART (Self-Monitoring, Analysis and Reporting Technology) data of the selected hard drive, if the device supports it. To show this view:

- Click **View > Windows > SMART Info**
- Use context menu command **SMART Info** for the same effect

Fixed Disk: /dev/sdk - S.M.A.R.T. Information	
Refresh	
Name	Value
▼ Fixed Disk General	
Device Model	ST320005XXXX
Serial Number	6XW01CTW
Firmware Version	CC34
Capacity	2000398934016
ATA Version	8
ATA Standard	Device does not report versi
SMART Support	1
Off-line data collection status	130
Self-test execution status	0
Time Off-line data collection, sec	633
Off-line data collection capabilities	123
SMART capabilities	3
Error logging capabilities	1
Short self-test time, min	1
Extended self-test time, min	255
▼ Attributes	
[001] Raw Read Error Rate	15788906
[003] Spin Up Time	0
[004] Start/Stop Count	269
[005] Reallocated Sector Count	0
[007] Seek Error Rate	9525169451
[009] Power-On Hours Count	33165
[010] Spinup Retry Count	0
[012] Power Cycle Count	267
[183] Runtime Bad Block	0
[184] End-to-End Error	0
[187] Reported Uncorrect	0
[188] Command Timeout	4295032835
[189] High Fly Writes	25
[190] Airflow Temperature Celsius	26
[194] HDA Temperature Celsius	26
[195] Hardware ECC Recovered	15788906
[197] Current Pending Sector	0
[198] Offline Uncorrectable	0
[199] UDMA CRC Error Count	0
[240] Head Flying Hours	33560
[241] Total LBAs Written	2826716440
[242] Total LBAs Read	110146536

Figure 34: SMART information for physical device example

SMART data can be used to diagnose disks by showing important information such as Power-on Hours, Reallocated Sectors and Current Pending Sectors



Note: If the Current Pending Sectors parameter is not 0, the disk has bad sectors that will cause problems in the future. Dispose of these disks as soon as possible.

Dynamic Disks: LDM, LVM and WSS

Dynamic Disks - virtual disks being used by:

- **Logical Disk Manager** (LDM on Windows)
- **Logical Volume Manager** (LVM on Linux)
- **Windows Storage Spaces** (WSS on Windows)

Dynamic Disks are virtual operating system devices handling other physical disks and emulating different types of RAID not on a hardware level, but on an operating system level. These virtual devices are fully supported with

KillDisk. These disks will appear in the disk view as any other disks would, along with their component disks. When you launch an erase operation on the virtual disk, you will see it reflected on the components disks as well.

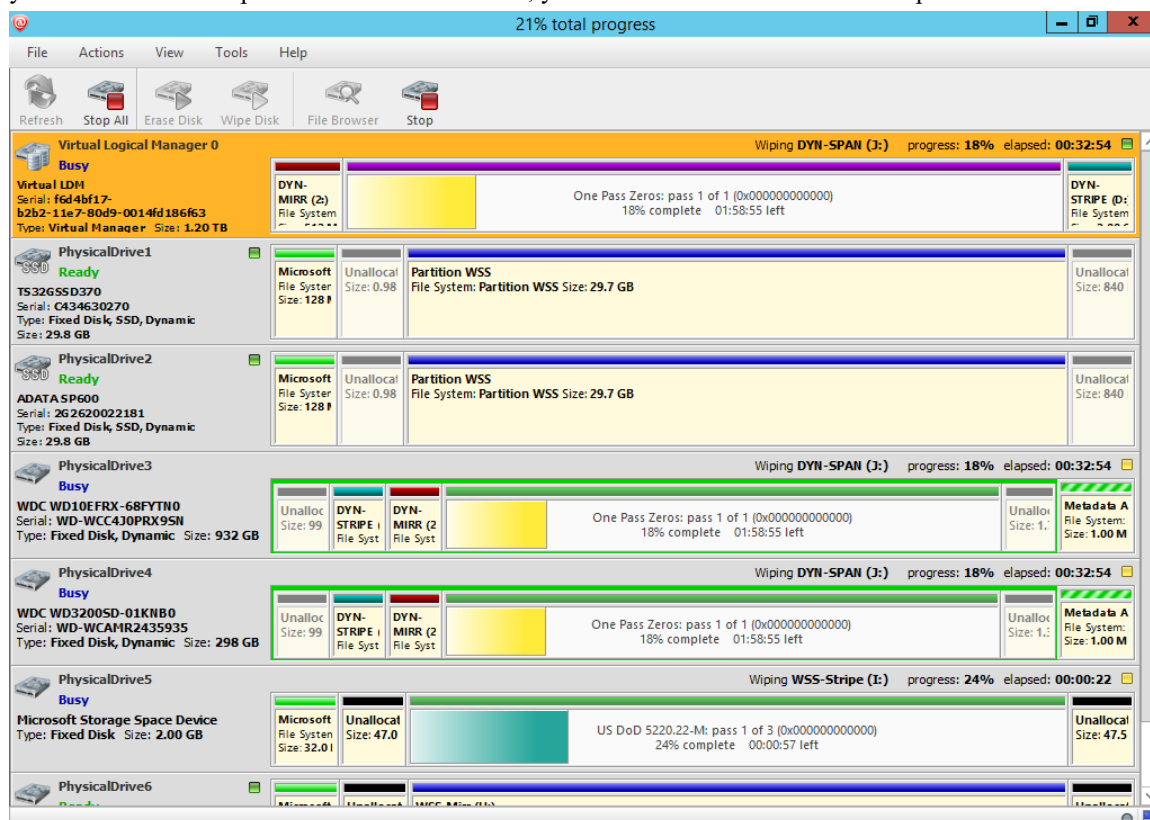


Figure 35: Virtual drive (Striped Disk Array) being erased in Windows Storage Spaces

Preferences

KillDisk **Preferences** window is the central location where KillDisk features can be configured. These features are split up into several tabs.

To open **Preferences** dialog:

- From main menu choose **Tools > Preferences...** or
- Use **F2** keyboard shortcut at any time

Preferences dialog could be open from other task dialogs to change related settings.

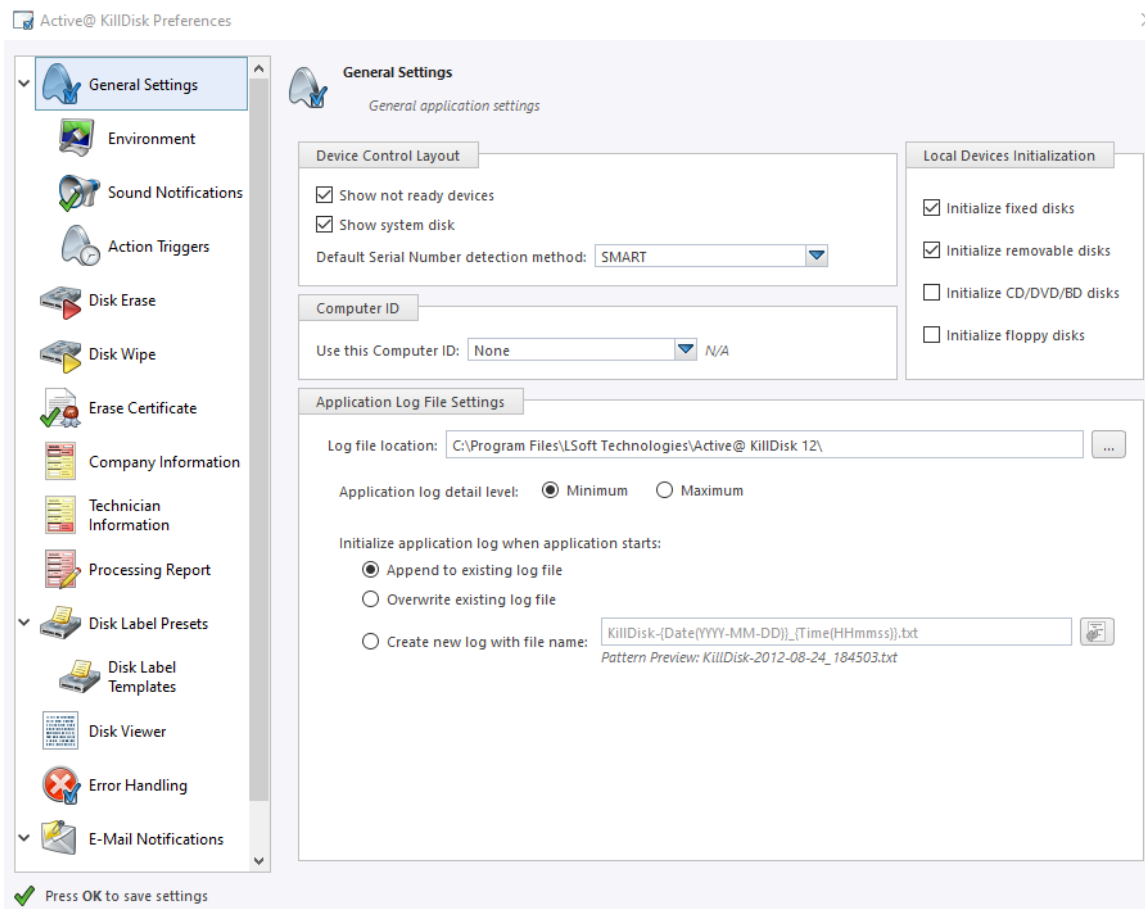


Figure 36: KillDisk Preferences dialog

Preferences allow users to configure all the global settings for the application.

When **Erase** or **Wipe** command initiated, smaller subset of these settings is available to modify, however global settings may be kept, pertinent to the particular job.

The functionality of the **Preferences** will be outlined in this section.

General Settings

The **General Settings** allow the user to configure general application settings, as well as the visual aspects of the application.

General Settings

These are configurable options pertaining to the applications functionality.

Device Control Layout

These settings control visual disk behavior in [Disk Explorer](#) on page 19 and allow to Show or Hide system disk and devices which are not ready (offline)

Default Serial Number detection method

Select how KillDisk retrieves the disk serial number by default. Values are: **SMART**, **IOControl** & **WMI**

Local Devices Initialization

Select which types of devices appear in KillDisk by default: **Fixed disks**, **Removable disks**, **CD/DVD/BD** and **Floppies**

Computer ID

Configure how the KillDisk workstation is identified in logs & reports. Values are: **None**, **BIOS Serial Number**, **Motherboard Serial Number**

Application Log File Settings

These settings apply to the log file automatically generated by the application. Not to be confused with the erasure report or certificate. All operations performed in a KillDisk session will be saved in this log.

Log file location

Allows the user to specify where the application log file is saved. By default this is set to a KillDisk's location directory

Application log detail

Manipulate the amount of details included in the logs. Options are: **Minimum** and **Maximum**

Initialize application log when application starts

This setting configures whether KillDisk generates a new log file for every session (erasing the log of the previous session), or appends new sessions to one log file. Moreover, logs can be placed to the files being named using naming pattern specified here

Environment

These are configurable options pertaining to the applications user interface and user experience.

Application style

Configures the color scheme used in the application. Values are : **None**, **Silver**, **Olive** and **Blue**

Toolbar style

Configures how icons are shown in the toolbar (shown below)

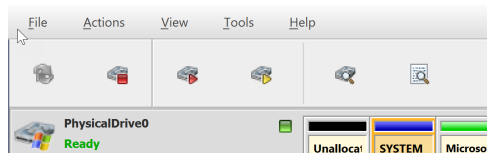


Figure 37: Small icons no text

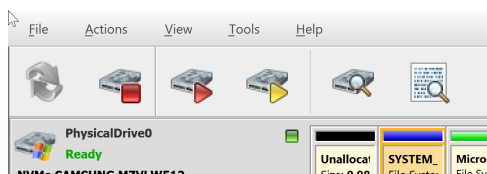


Figure 38: Large icons no text

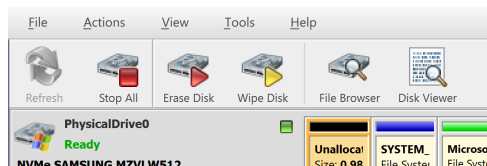


Figure 39: Large icons with text

Default help source

If available, user can select help documentation source to be addressed when requested. Values are: **PDF**, **CHM** and **Online web help**

Show notification dialog after process complete

Process complete dialog will be shown at the end of single or multiple disk processing, letting user print certificate, labels etc.

Sound Notifications

These are configurable options related to application sounds: you can use either predefined values or assign your own sounds.

Use Sound Notifications

Toggles sound tones being used for notifying the user of the completion of a task, errors and notification during an operation: **Success, Warnings, Errors, Failures**

Action Triggers

Configure actions performed while application is running

Automatically check for software updates

If this option set, application will check for a new updates during every start up

Action after all processes complete

Select either **None, Hibernate, Shutdown** or **Restart** system after all processes have been finished



Caution: You will have 30 seconds to abort system hibernation, restart or shutdown.

Export erase certificates and application log to all detected removable media

Upon erase completion all certificates and logs will be automatically exported to attached USB disks (removable media)

Disk Erase Options

The **Disk Erase Options** tab allows for users to configure settings for the KillDisk erase procedures.

Figure 40: Erase Options

Disk Erase
Define default disk erase attributes and options

Erase method: One Pass Zeros [1 pass]

☐ Verify erasure of 10% on each disk

☒ Initialize disk(s) after erase

☐ Write fingerprint to first sector

Fingerprint: Erased by Active@ KillDisk [up to 256 symbols]

☐ Print erase labels for each disk using Disk Label Preset: Default Disk Label Preset

Erase Confirmation

☒ Use keyphrase to confirm erase

Keyphrase: ERASE-ALL-DATA

☐ Use randomly generated keyphrases to confirm erase

☐ No keyphrase confirmation

Erase method

One of 20+ sanitizing methods, including many international standards and custom patterns *supported by KillDisk*

Erase verification

Percentage of disk to be verified after disk erasure



Note: In some erase methods such as the US DoD 5220.22-M, this option is mandatory. After the erase operation has completed, this option will scan the entire drive evenly and verify the integrity of the erase operation. The percentage indicates the percent of the sectors that are checked, spread across the disk. Most standards specify 10% as an accurate sample size for the verification.

Initialize disk(s) after erase

Initializes the first disk's sector (MBR) after erasure, for the disk to be visible and accessible by Operating System

Write fingerprint to first sector

This feature will write the specified fingerprint to the first sector of the erased drive. If erased disk is plugged into the system and system boots from this disk, the user will see this fingerprint as a message on the screen

Print erase labels

This feature will print erase label automatically after erase completion using specific Disk Label Preset configuration

Erase confirmation

As a safety precaution to prevent accidental destruction of hard drives, KillDisk has the user type a key phrase before the erase procedure is initiated (figure below). By default this precaution is set with the key phrase **ERASE-ALL-DATA**. This key phrase can be modified, set as a randomly generated set of characters, or disabled in these settings

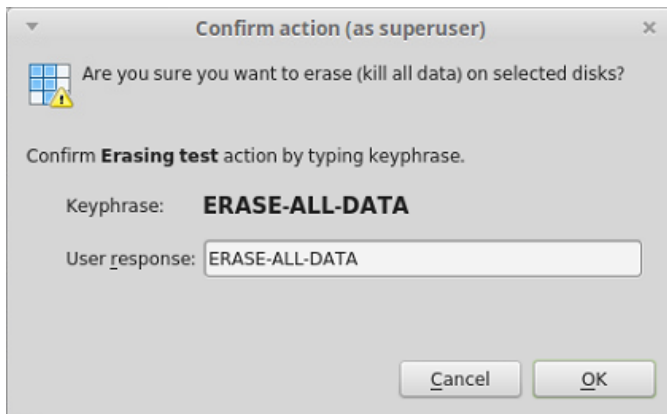


Figure 41: Sensitive action confirmation dialog

Disk Wipe Options

The **Wipe Disk** procedure, like with the erase procedure, allows you to specify the erase method used, as well as a few additional wipe-specific options.

Erase method

One of 20+ sanitizing methods, including many international standards and custom patterns *supported by KillDisk*

Erase verification

Percentage of disk to be verified after wiping out unused clusters

Wipe unused clusters

Erase areas of the hard drive that are not formatted and not currently used by the operating system (data has not been recently written there unless this is a recently deleted partition)

Wipe metadata and system files area

Erase areas of the disk containing information about previous files on the volume and prevents recovery of files using past records of them

Wipe slack space in file clusters

Erase slack space within files. Files are allocated a set amount of space by the OS, in certain increments (depending on the file system). Because files are usually never *exactly* the size of the space allocated to them, there may be unused space within a file that may contain traces of data. This algorithm wipes this space to remove these data traces.

Print wipe labels

This feature will print wipe label automatically after wipe completion using specific Disk Label Preset configuration

Certificate Options

These preferences allow the user to customize the erasure certificates with company specific information, technician information, and additional certificate options.

Figure 42: Certificate Options

Certificate location

Use this option to save erase certificate as file in PDF format to selected location

File name template

Here you may specify the name template for the erase certificate. To see additional file name tags available, see the [File name tags section](#) in the Appendix

Include company information

Use this option to include all company's information (see section below)

Include technician information

Use this option to include all technician's information (see section below)

Include system info

Ensures that the Operating System-specific information is saved, such as:

- Operating system
- Kernel version
- Architecture

Include hardware info

Ensures that the Chassis-specific information is saved, such as:

- Motherboard manufacturer
- Motherboard description
- Number of processors

Include disk SMART information

Use this option to include SMART information for the disk

Show KillDisk logo on certificate

Displays "Erased by Active@ KillDisk" logo in the certificate at top-right corner

Use Computer ID on certificate

This option includes the Hardware ID of the machine being erased on the certificate. It may be taken from the BIOS or the Motherboard (these values may differ from each other).

Print Options

Always print certificate after disk erase

Prints erase certificate after erase completion automatically

Skip print preview

Prints erase certificate skipping certificate preview step

Default printer

Select a default printer for printing erase certificates

Company information

This section allows for the user to customize company features like:

- Licensed to
- Business name
- Location
- Phone
- Disclaimer
- Signature field for a company supervisor (optional)

Additionally, custom logos can be added by clicking **Set** and selecting an logo through the file explorer. The logo will be previewed in the Company logo space above. Most image formats are supported: JPEG, TIFF, BMP, PNG, etc.



Tip: It is recommended for better results to use company logo with resolution suitable for printing (300dpi) with a side not exceeding 300px.

Technician Information

This section allows for the user to customize technician information:

- Operator name
- Comments
- Signature field for a technician (operator)

Report Options

These settings allow you to configure the XML reports generated by different KillDisk commands.

Report Location

User may configure where XML erasure reports are saved

File name template

Here you may specify the name template for the XML reports. Because every erase operation will generate a separate report, KillDisk saves the date and time in the default settings to keep reports. The main tags available are:

Table 1: Default file name template tags:

Available file name element:	Tag:
Serial ID	{Serial ID}
Erase Status	{Status}
Date of Erasure	{Date(YYYY-MM-DD)}
Time of Erasure	{Time(HH-mm-ss)}

To see additional file name tags available, see the [File name tags section](#) in the Appendix

Include system and hardware info

Ensures that the system-specific information is saved in the XML report, such as:

- Operating system
- Kernel version
- Motherboard manufacturer
- Motherboard description
- Processors count
- Architecture (x86, x64)

Include company and technician information

Optionally place the technician information (defined in the [Certificate Preferences](#)) into the XML erasure report

Include SMART information for each disk

Additional information about particular disk health based on SMART attributes can be placed to XML.

The KillDisk XML report contains the following parameters:

Table 2: XML Report Parameters

Type of Information	Specific data
Company Information	<i>Name</i>
	<i>License</i>
	<i>Location</i>
	<i>Phone</i>
	<i>Disclaimer</i>
Technician Information	<i>Operator Name</i>
	<i>Comments</i>
System Information	<i>OS version</i>
	<i>Platform</i>
	<i>Kernel</i>
Hardware Information	<i>Motherboard Manufacturer</i>
	<i>Motherboard Description</i>
	<i>Number of Processors</i>
Erase Attributes	<i>Erase Verify</i>
	<i>Passes</i>
	<i>Method</i>
	<i>Verification Passes</i>
Error Handling Attributes	<i>Errors Terminate</i>
	<i>Skip interval</i>
	<i>Number of Retries</i>
	<i>Lock</i>
	<i>Source?</i>

Type of Information	Specific data
	<i>Ignore Write?</i>
	<i>Read?</i>
	<i>Lock?</i>
Disks	<i>Device Size</i>
	<i>Device Type</i>
	<i>Serial Number</i>
	<i>Revision</i>
	<i>Product Number</i>
	<i>Name</i>
	<i>Geometric Information</i>
	<i>Partitioning Scheme</i>
Additional Report Attributes	<i>Fingerprint Information</i>
	<i>Initialize disk?</i>
Result	<i>Bay</i>
	<i>Time and Date Started</i>
	<i>Disk Information</i>
	<i>Status</i>
	<i>Result</i>
	<i>Time Elapsed</i>
	<i>Errors</i>
	<i>Name of operation</i>

Labels Options

These preferences help you globally adjust label settings for the KillDisk system. These labels may be configured to any printer, page or label type using KillDisk's highly customizable labels features.

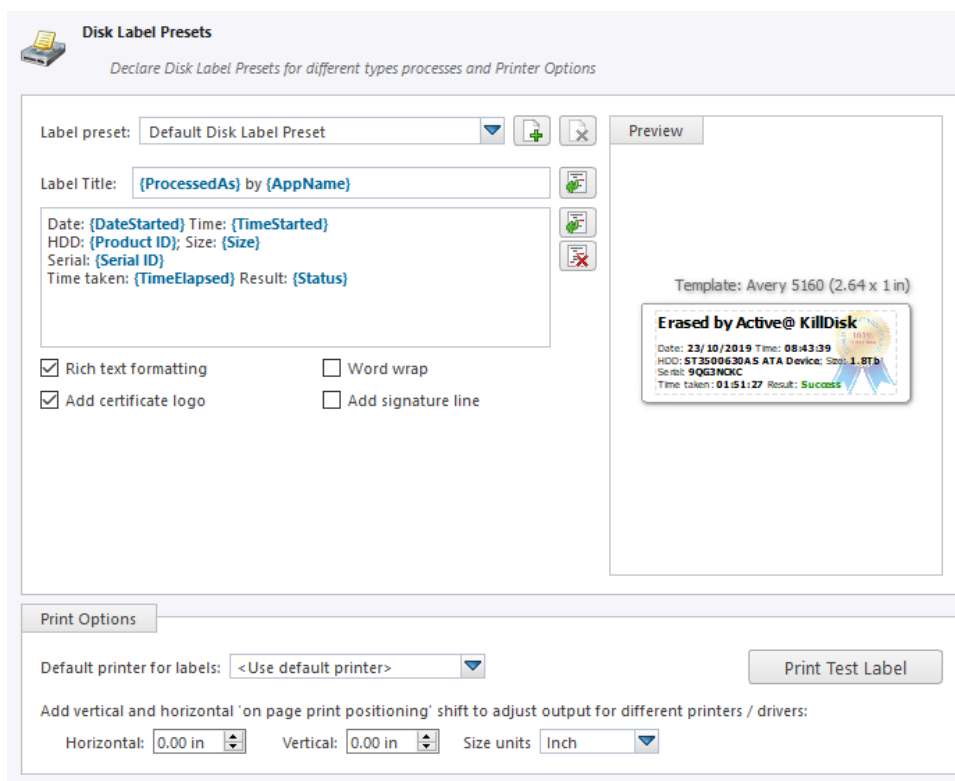





Figure 43: Disk Label Presets

Label preset


Displays and let you select a default Label Preset or create a new one. **Add New Label Preset** button  allows you to create a custom label preset with your own specifications. Delete button  deletes the selected label preset

Label title

Allows you to set a title to be printed in bold at the top of the labels. This can be company name, batch name or any other descriptors you may consider useful to identify the operation. Static text can be typed in or any dynamic

attributes (tags) can be inserted at current cursor's position. Click **Insert Name Tag** button  to insert predefined tag from the drop-down list

Label Area

Form the Label's content for the preset. Static text can be typed in or any dynamic attributes (tags) can be inserted at current cursor's position. Click **Insert Name Tag** button  to insert predefined tag from the drop-down list. Click **Clear Pattern** button to empty all label's area

Label Attributes

You can use **RTF formatting** and set **Word Wrapping** behavior using related check boxes

Add signature line

Toggling this on places a line at the bottom of the label for the technician to sign off on upon completion of the wipe

Add certificate logo

Includes the logo used in the certificate as a watermark background of the label

Label preview

Displays a preview of one label, given the current inputted settings. Refreshes as adjustments are made to the settings.

Print options

Define options for erase label printing, including special label printers line Brother QL-570 and others:

Default printer

Select printer to be used exclusively to print erase labels from the list of installed printers

Print output adjustments

The print output adjustments section of the dialogue allows you to **vertically** or **horizontally** displace the position measured in specific **units** of the print to adjust to different printers.

Print test label command will let you print erase label sample to verify your settings and selected layout attributes.

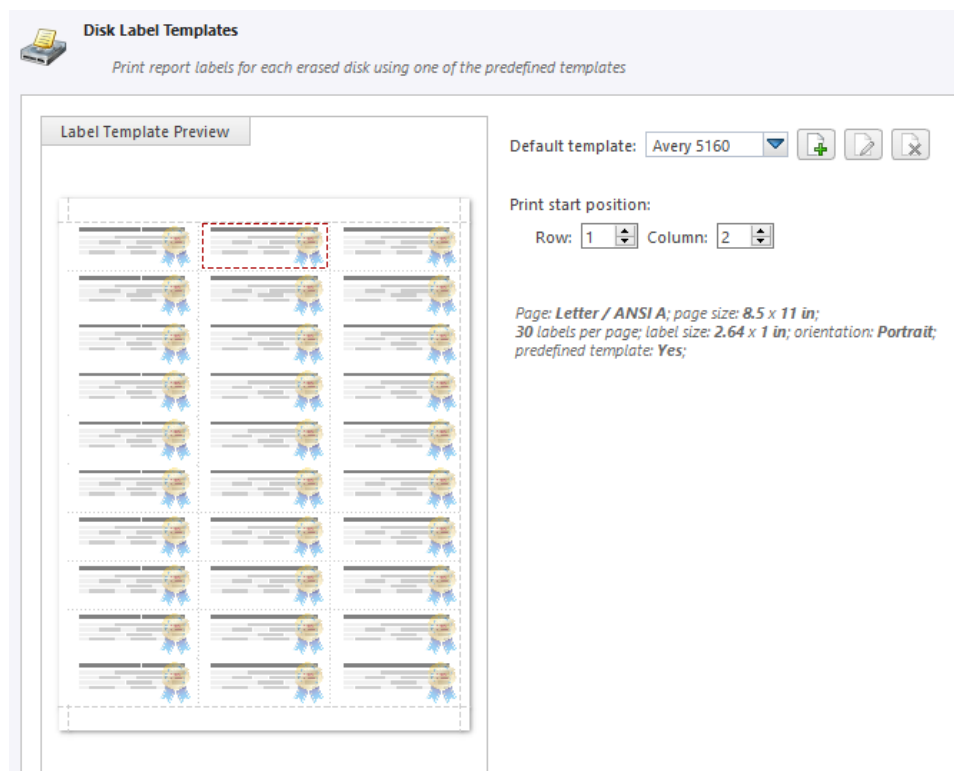





Figure 44: Disk Label Templates

Page template

The print label dialog gives you access to a number of predefined standard templates and any custom templates you may create. These template may be easily selected without opening any additional dialogs and the details of the selected template will be displayed below the selection box. If your specific labels differ from any of the templates


available, the  button allows you to create a custom template with your own specifications. Additionally, the 

button allows you to modify an existing template and the  button deletes the selected template.

Print Start Position

The print start position section of the dialogue allows you to select what label on the page the labels start printing from. As you use labels, the labels won't always start from the 1x1 position, so you can adjust this setting accordingly.

Creating a new template

Upon clicking the  button, the following template editor window will appear. Descriptions of the template editor options are listed below.

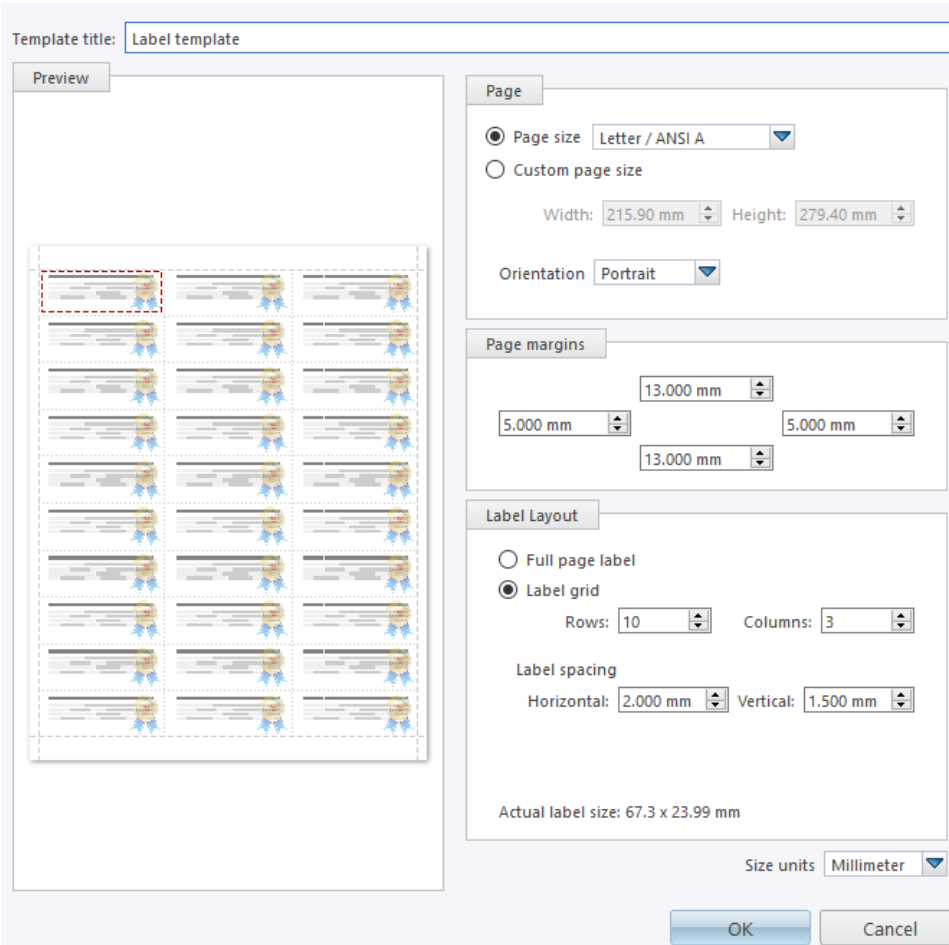


Figure 45: Create a New Disk Label Template

Template Title

Here you may create a custom title for your template. This is the name that will reference this template when selecting it in the Print Label dialog.

Page

Here you may specify the dimensions of the page used to print the labels. This may be selected from the list of standard sizes, or defined using exact measurements.

Page margins

Here, page margins are defined for the top, bottom, left and right sides of the page.

Label Layout

These settings define how the labels appear on the page. You may define the spacing in between labels on the page and the dimensions of the label grid. Once you've put in the proper measurements, KillDisk will take care of the formatting.

Size units

The units of measurement may be manipulated between millimeters, inches, pixels and points. If a value is entered in one measurement and the unit size is changed, the appropriate conversion will take place.

Disk Viewer Options

These settings allow user to set hexadecimal view settings, font and interaction.

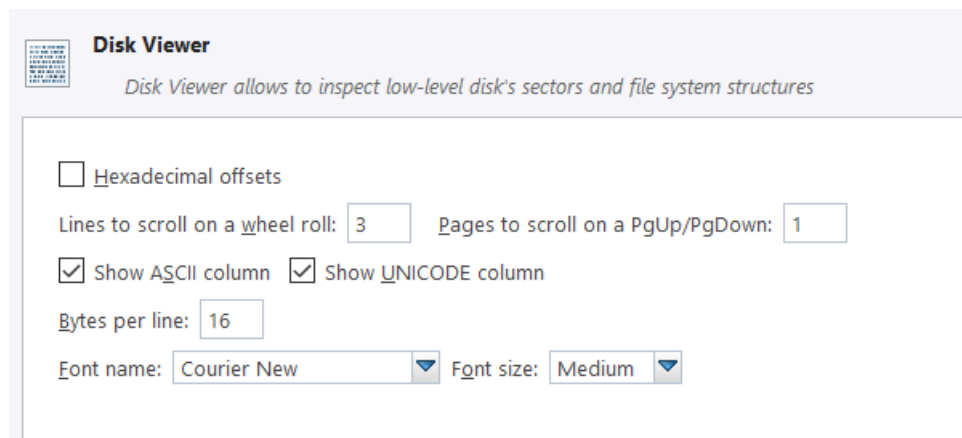


Figure 46: Disk Viewer Options

Hexadecimal offsets

Toggles offset format between decimal and hexadecimal.

Show ASCII column

Toggles display content in ASCII format

Show UNICODE column

Toggles display content in UNICODE format

Lines to scroll

Number of lines to scroll for a single mouse wheel sweep

Pages to scroll

Number of pages to skip for a single **PageUp** or **PageDown** click

Bytes per line

Defines amount of bytes per line in binary display

Font name

Select any monospace font available for better experience

Font size

Font size to be used in binary view

Error Handling Options

KillDisk has a broad capabilities to handle errors encountered during continuous disk processing. This is an advanced preference that allows for the configuration of KillDisk's error handling of continuous processes.

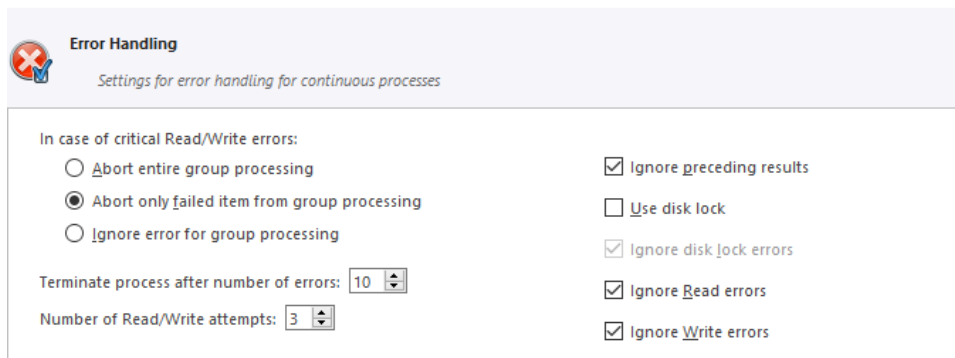


Figure 47: Error Handling Options

Error handling attributes

KillDisk allows you to select one of three ways to handle Read/Write Errors:

Abort entire disk group processing

This means that if you're running a batch erase and one of the disks has errors, the erase process for ALL the disks in the batch will be terminated

Abort only failed disk from group processing

This is the suggested setting. Failed disks will return an error and terminate the erase process, but other disks in the batch will not be interrupted from completing the erase operation

Ignore error for disk grouping

Ignores the read/write error and continues erasing wherever is possible on the disk. No active or forth going operations are terminated

Terminate process after number of errors

Sets the error threshold to a certain amount before the disk operation is terminated and deemed unsuccessful

Number of Read/Write attempts

Sets the number of attempts KillDisk make to perform an operation when an error is encountered before it stops command execution

Use disk lock

Locks disks from being used by any other applications

Ignore disk lock errors

Errors encountered with KillDisk not being able to access locked disks are ignored

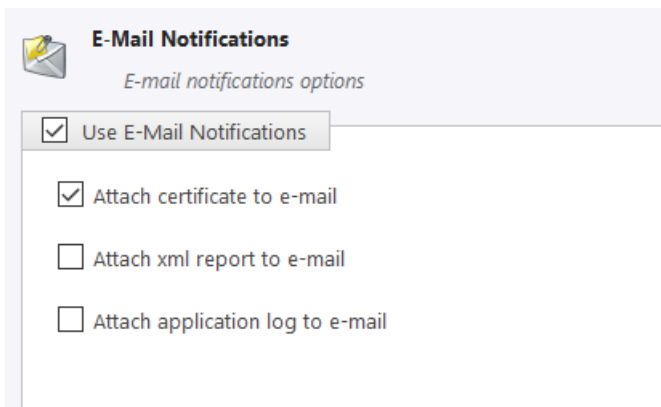
Ignore read/write errors

Toggle whether errors should appear for read and/or write errors

Email Notification Options

Email Notifications

KillDisk can deliver results of its sanitation process by e-mail.



E-Mail Notifications
E-mail notifications options

☒ Use E-Mail Notifications

☒ Attach certificate to e-mail

☐ Attach xml report to e-mail

☐ Attach application log to e-mail

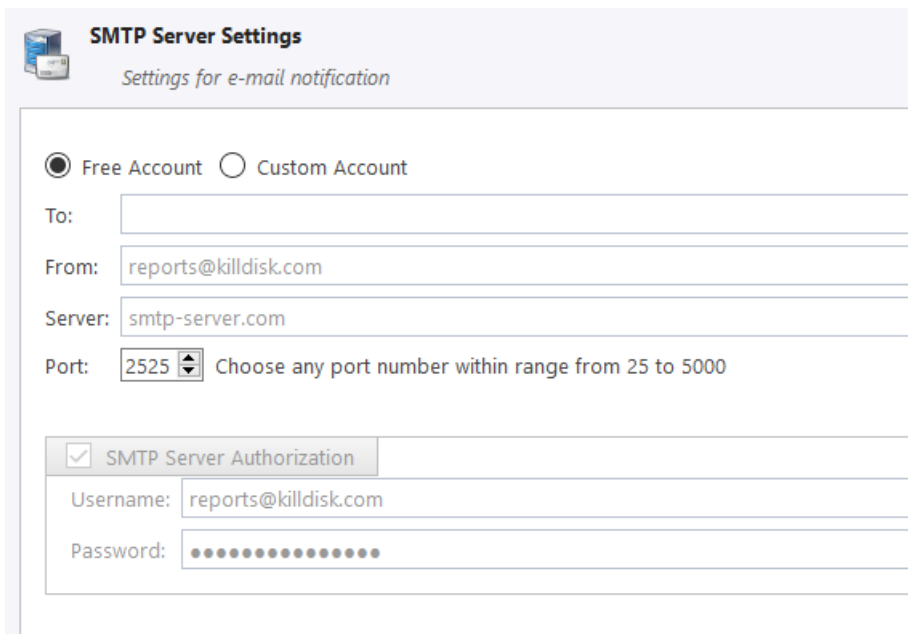
Figure 48: Email Notification Options

Certificate, XML Report or Application Log can be emailed to the client, just check the related option.

When you check **Use E-Mail Notifications** option, the next set of options: **SMTP Server Settings** will be available for configuration.

SMTP Server Settings

These settings allow configuring mailer settings for delivering erasing/wiping reports to your mailbox. Simple Mail Transport Protocol (SMTP) is responsible for transmitting e-mail messages and needs to be configured properly.



SMTP Server Settings
Settings for e-mail notification

☒ Free Account ☐ Custom Account

To:

From:

Server:

Port: Choose any port number within range from 25 to 5000

☒ SMTP Server Authorization

Username:

Password:

Figure 49: SMTP Settings

These options can be configured in the Freeware version, but will be used in the Professional version only.

Account Type

KillDisk offers you a free SMTP account located on www.smtp-server.com that can be used for sending out reports. By default all required parameters are pre-filled and configured properly. The only field you need to type in is the e-mail address where reports will be sent to. If your corporate policy does not allow using services other than its own, you need to switch this option to Custom Account and configure all settings manually. Ask your system/network administrator to get these parameters.

To

Type the e-mail address where erasing/wiping reports will be sent to

From

Type the e-mail address which you expect these reports to come from

SMTP Server

KillDisk offers you the use of smtp-server.com for a free SMTP account. This account is pre-configured for KillDisk users. Ask your system/network administrator to get the SMTP server name to be used in the Custom Account

SMTP Port

For the free SMTP account, KillDisk allows you to use smtp-server.com on port 80. This is a standard WWW port being used by all web browsers to access the internet. This port most likely will be kept open on a corporate or home network. Other ports can be filtered by and closed on a network firewall. Ask your system/network administrator to set proper SMTP port for the related SMTP server.

SMTP Server requests authorization

To avoid spam and other security issues, some SMTP servers require each user to be authorized before allow sending e-mails. In this case a proper user name and password are required. Ask your system/network administrator to get proper configuration settings.

Command Line and Batch Modes

KillDisk can be executed with some settings pre-defined when started from a command prompt with specific command line parameters.

KillDisk can be also launched in fully automated mode (batch mode) which requires no user interaction.

KillDisk execution behavior depends on either command line parameters (highest priority), settings configured in interactive mode and stored in the KILLDISK.INI file (lower priority), or default values (lowest priority).

Command Line Mode

To run KillDisk in command line mode, open a command prompt and go to installation directory.

At the command prompt, start KillDisk for Windows by typing:

```
KILLDISK.EXE -?
```

In Linux environment, type:

```
./KillDisk -?
```

A list of parameters appears. You can find explanations of them in the table below.

Table 3: Command Line Parameters

Parameter	Short	Default	Options
no parameter			With no parameter, Interactive screen will appear
-erasemethod=[0-23]	-em=	2	0 - One pass zeros (quick, low security)
			1 - One pass random (quick, low security)
			2 - US DoD 5220.22-M (slow, high security)
			3 - US DoD 5220.22-M (ECE) (slow, high security)
			4 - Canadian OPS-II (slow, high security)

Parameter	Short	Default	Options
			5 - British HMG IS5 Baseline (1 pass, quick)
			6 - British HMG IS5 Enhanced (slow, high security)
			7 - Russian GOST p50739-95(slow, high security)
			8 - US Army AR380-19 (slow, high security)
			9 - US Air Force 5020 (slow, high security)
			10 - Navso P-5329-26 RL (slow, high security)
			11 - Navso P-5329-26 MFM (slow, high security)
			12 - NCSC-TG-025 (slow, high security)
			13 - NSA 130-2 (slow, high security)
			14 - German VSITR (slow, high security)
			15 - Bruce Schneier (slow, high security)
			16 - Gutmann (very slow, highest security)
			17 - User Defined Method. Number of passes and Overwrite pattern supplied separately
			18 - NIST 800-88 (1 pass zeroes, quick)
			19 - NIST 800-88 (1 pass random, quick)
			20 - NIST 800-88 (3 pass zeroes, slow, high security)
			21 - Canadian CSEC ITSG-06 (3 passes, verify, slow, high security)
			22 - US DoE M205.1-2 (3 passes, verify)
			23 - Australian ISM-6.2.93 (1 pass random, quick)
-passes=[1 - 99]	-p=	3	Number of times the write heads will pass over a disk area to overwrite data with User Defined Pattern. Valid for User Defined Method only
-verification=[1 - 100]	-v=	10	Set the amount of area the utility reads to verify that the actions performed by the write head comply with the chosen erase method (reading 10% of the areaby default). Verification is a long process. Set the verification to the level that works best for you
-retryattempts=[1 - 99]	-ra=	2	Set the number of times that the utility will try to rewrite in the sector when the drive write head encounters an error
-erasehdd=[0,1..63]	-ch=		Number in BIOS of the disk to be erased. First physical disk has a zero number. In Linux first disk usually named /dev/sda. In Windows Disk Manager first disk is usually named Disk 0. On older systems (DOS, Windows 9x) first disk is usually named 80h (obsolete syntax is still supported in the parameter)
-eraseallhdds	-ea		Erase all detected disks
-excluderemovable	-xr		Exclude all removable disks from erasing when erase all disks selected

Parameter	Short	Default	Options
-excludefixed	-xf		Exclude all fixed disks from erasing when erase all disks option selected
-excludedisk=[0,1..63]	-xd=		Exclude disk from erasing when erase all disks option selected
-ignoreerrors	-ie		Do not stop erasing each time a disk error is encountered. When you use this parameter, all errors are ignored and just placed to the application log
-initdisk	-id		Initialize disk(s) after erase
-fingerprint	-fp		Initialize disk(s) and write fingerprint to the disk's first sector
-computerid	-ci		1 - Display BIOS ID on the certificate
			2 - Display Motherboard ID on the certificate
-clearlog	-cl		Use this parameter to clear the log file before recording new activity. When a drive is erased, a log file is kept. By default, new data is appended to this log for each erasing process. By default the log file is stored in the same folder where the software is located
-exportlog	-el		Export a log file as XML report
-logpath=["fullpath"]	-lp=		Path to save application log file. Can be either directory name or full file name. Use quotes if full path contains spaces
-certpath=["fullpath"]	-cp=		Path to save erase/wipe certificate. Can be either directory name or full file name. Use quotes if full path contains spaces
-inipath=["fullpath"]	-ip=		Path to the configuration file (KILLDISK.INI) for loading the advanced settings. See table below
-noconfirmation	-nc		Skip confirmation steps before erasing starts. By default, confirmation steps will appear in command line mode for each hard drive as follows: Are you sure?
-beep	-bp		Beep after erasing is complete
-wipeallhdds	-wa		Wipe out unallocated space on all recognized volumes located on all detected disks
-wipehdd = [0,1...63]	-wh=		Wipe out unallocated space on the disk specified by BIOS number
-test=["fullpath"]			If you are having difficulty with Active@ KillDisk, use this parameter to create a hardware information file to be sent to our technical support specialists. You must specify the name of the file where to store technical information
-batchmode	-bm		Execute in batch mode based on command line parameters and INI file settings (without user interaction, all operations being stored to log file)
-userpattern=["fullpath"]	-u		File to get user-defined pattern from. Applied to User Defined erase method. Each line in the file corresponds to the particular pass pattern
-shutdown	-sd		Save log file and shutdown PC after completion
-nostop	-ns		Prevent erase/wipe stop action

Parameter	Short	Default	Options
-help or -?			Display this list of parameters



Note: Parameters -test and -help must be used alone. They cannot be used with other parameters.



Note: Commands -erasehdd, -eraseallhdds, -wipehdd and -wipeallhdds cannot be combined.

Type the command and parameters into the command prompt console screen at the prompt. Here is a Windows example:

```
killdisk.exe -eh=80h -bm
```

The same in Linux:

```
./KillDisk -eh=0 -bm
```

In the example above, data on device 80h will be erased using the default method (US DoD 5220.22-M) without confirmation and returning to the command prompt screen when complete.

Here is another Windows example:

```
killdisk.exe -eh=80h -nc -em=2
```

The same in Linux:

```
./KillDisk -eh=0 -nc -em=2
```

In this example, all data on the first detected disk (which has Zero number or 80h) will be erased using US DoD 5220.22-M method without confirmation and showing a report at the end of the process.



Note: In Linux environment, to detect and work with physical disks properly, Active@ KillDisk must be launched under Super User account, so, if you are not a Super User, you should type a prefix **sudo**, or **su** (for different linux versions) before each command.

After you have typed KillDisk and added command line parameters, press ENTER to complete the command and start the process.

Information on how drives have been erased is displayed on the screen when the operation has completed successfully. KillDisk execution behavior depends on either command line parameters (highest priority), settings configured in interactive mode and stored in the KILLDISK.INI file (lower priority), or default values (lowest priority).

Batch Mode



Note: This feature is intended for advanced users only

Batch mode allows KillDisk to be executed in fully automated mode without any user interaction. All events and errors (if any) will be placed to the log file. This allows system administrators and technicians to automate erase/wipe tasks by creating scripts (*.CMD, *.BAT files) for different scenarios that can be executed later on in different environments.

To start KillDisk in batch mode, add the -bm (or -batchmode) command line parameter to the other parameters and execute KillDisk either from the command prompt or by running a script.

Here is an example of batch mode execution with the wipe command:

```
KillDisk -wa -bm -em=16
```

This command will wipe all deleted data and unused clusters on all attached physical disks without any confirmations using most secure Gutman's method and returning to the command prompt when complete.

If `-ns` (`-nostop`) command line parameter is specified, no user interaction is possible after erase/wipe action started, so user cannot cancel the command being executed.

After execution, application returns exit codes to the operating system environment: 0 (`zero`) if all disks being erased successfully, 1 (`one`) if errors occurred or nothing erased/wiped, and 2 (`two`) if minor warnings occurred.

Advanced Tools

KillDisk offers a number of advanced tools to work in conjunction with the software to make operations easier to perform and the disks easier to navigate. KillDisk give you the power to browse through disks on both a file level and a low, hexadecimal (HEX) level. Disk health analysis with its' SMART monitor as weell as logs/reports export to the external databases fully supported in KillDisk Industrial version. This section describes each of these features at length:

- [File Browser](#)
- [Hexadecimal Viewer](#)

File Browser

KillDisk also includes a built-in file browser for examining the contents of disks for verification purposes of the procedure and that correct hard drives are being selected, and validation that erased files have been overwritten after erase and wipe. Details on using this feature will be discussed in this section.



Note: KillDisk **will** detect existing files, as well as files that have been deleted, but **not** sanitized. They will appear grey and indicate deleted files with a high probability of being recovered with file recovery tools.

Opening the Browsing View

To browse the contents of a specific disk, simply select the disk and click **File Browser** in toolbar button or select related command from the context menu.

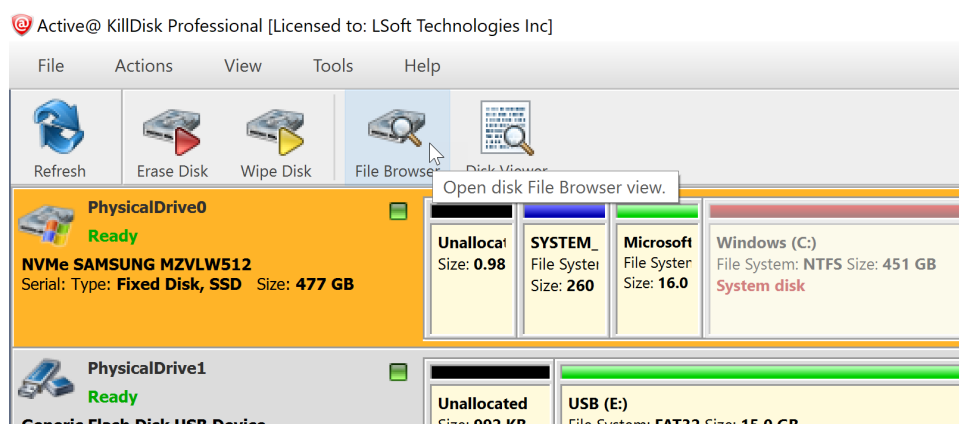


Figure 50: Launching the File Browser

This will launch the file browser window, seen below.

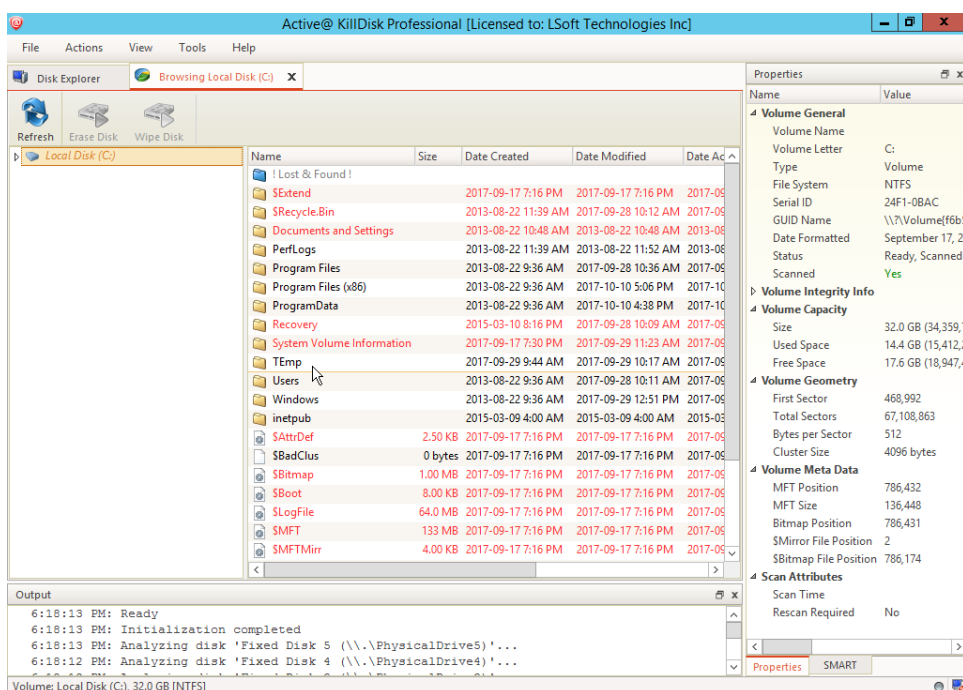


Figure 51: File Browser Window

The file browser window displays files and folders on the disk being selected.

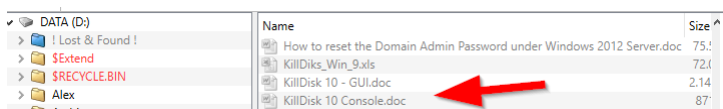


Figure 52: Deleted Files in the File Browser

Grey files indicate deleted files that have not been sanitized. These files are recoverable. Running KillDisk's *Wipe* operation will ensure these files are unrecoverable and make these grey files disappear from the file browser.



Note: Found deleted files will appear in their original directory (before they were deleted). The **! Lost & Found !** folder a virtual directory created for found deleted files where the directory information is not discovered by the application.

Disk Viewer

KillDisk's Disk Viewer allows users to view the contents of connected drives on a sector's level in a hexadecimal view. To launch it, select a disk to be inspected and click **Browse Disk** toolbar button.

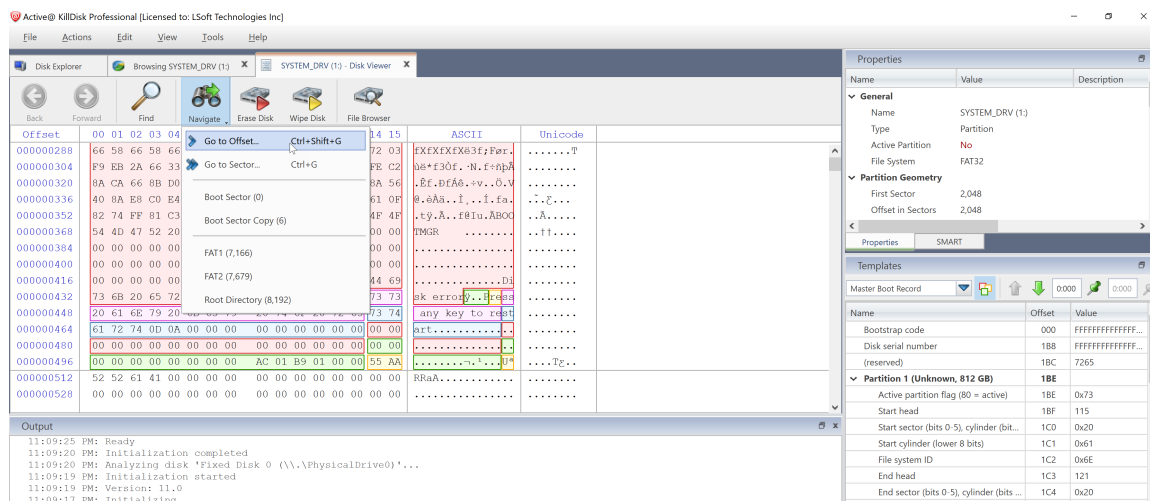


Figure 53: Disk Viewer with the MBR Template

To make it easier to navigate the Hex Editor view, KillDisk also offers a list of templates to help display the organization of the sectors on the disk by colored sections. The above uses the MBR template, below is a template for NTFS file system boot sector.

Templates			
NTFS Boot Sector			
Name	Offset	Value	Copy Value
JMP instruction	000	FFFFFFFF...	FFFFFFFF...
OEM ID	003	NTFS	NTFS
BIOS Parameter Block	00B		
Bytes per sector	00B	512	512
Sectors per cluster	00D	8	8
Reserved sectors	00E	0	0
(always zero)	010	000	000
(unused)	013	00	00
Media descriptor	015	248	248
(unused)	016	00	00
Sectors per track	018	63	63
Number of heads	01A	255	255
Hidden sectors	01C	567,296	567,296
(unused)	020	0000	0000
Signature	024	FFFFFFFF...	FFFFFFFF...
Total sectors	028	272,629,759	272,629,759
\$MFT cluster number	030	725,343	725,343
\$MFTMirr cluster number	038	2	2
Clusters per File Record Se...	040	246	246
Clusters per Index Block	044	1	1
Volume serial number	048	6B6FFFFFFFF...	6B6FFFFFFFF...
Checksum	050	0	0
Bootstrap code	054	FFFFFFFF...	FFFFFFFF...
Signature (55 AA)	1FE	55FFFFFFFF...	55FFFFFFFF...

Figure 54: NTFS Boot Sector Template

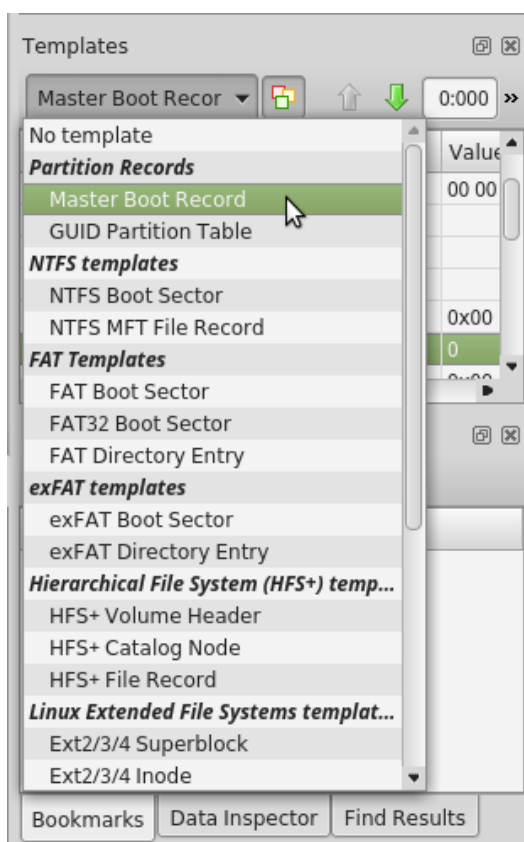


Figure 55: Disk Viewer Templates

The Disk Viewer also includes a **Find** feature, for locating specific data in the low-level disk view

Find what

Input the characters you are searching for in ANSI, Hex or Unicode

Search Direction

If you have an idea of where the data may be located, specify where to search

Not

Search for characters that do not correspond to the **Find what** parameter

Ignore case

Disables case-sensitivity in the search

Use

Select between **Regular Expressions** and **Wildcards**

Per block search

To speed up the search process, if you are familiar with the position of the data in the data block, you may specify a search with an offset or beginning of the object

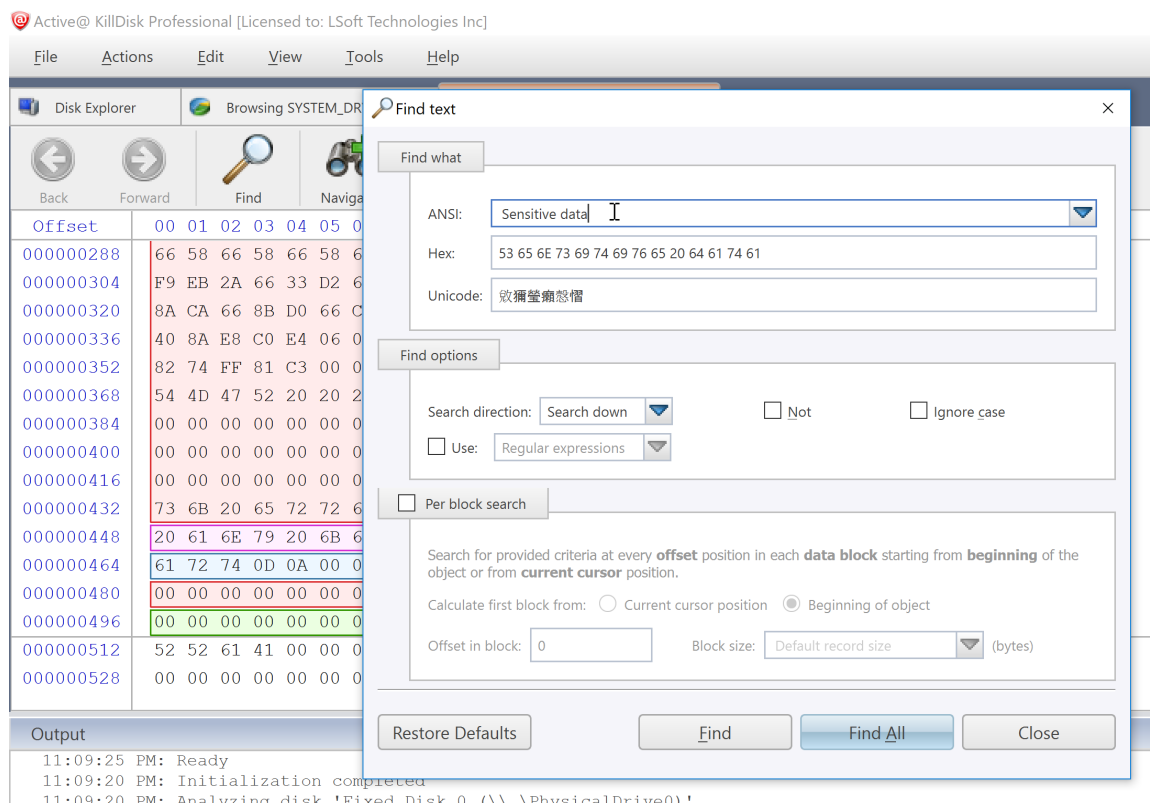


Figure 56: Finding Data

Disk Viewer's **Navigate** feature, located on toolbar allows:

Go to Offset

Jumps to the particular offset that needs to be entered manually in a decimal or hexadecimal form

Go to Sector

Jumps to the particular sector or cluster on the disk

Partition Table

Jumps to the sector where partition table is located, for example to the first sector on MBR disks

Partition Table

Jumps to the sector where partition table is located, for example to the first sector on MBR disks

Particular Partition

Lists all partitions and allows to jump to the boot sectors, to the beginning and to the end of any available partition.

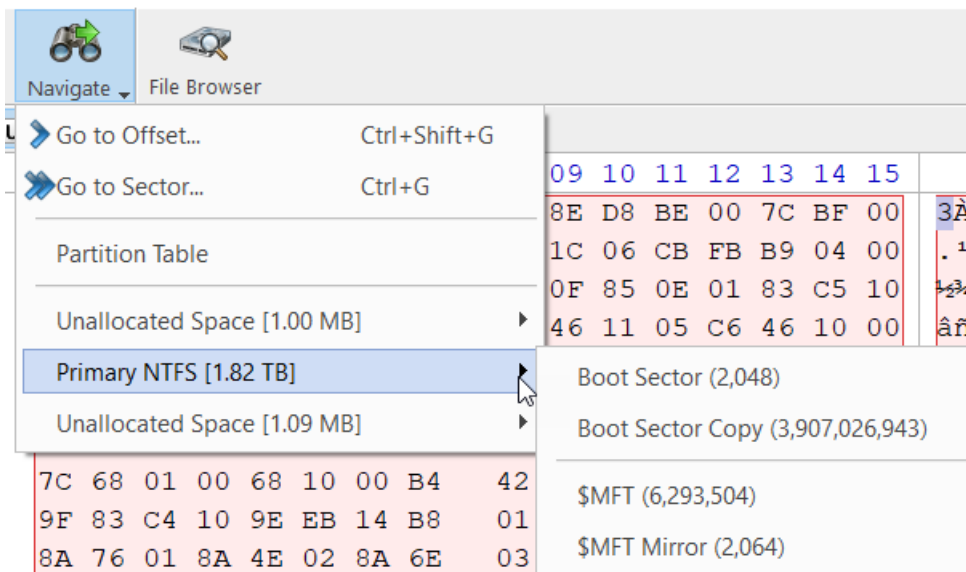


Figure 57: Disk Viewer Navigation Options

Application Settings

When you start `KillDisk`, change its settings (erase method, certificate options, etc...) and close the application, all current settings are saved to the **KILLDISK.INI** file in the location of the `KillDisk` executable. These settings will be used as default values the next time `KillDisk` is run.

KILLDISK.INI is a standard text file possessing sections, parameter names and values. All `KillDisk` settings are stored in the [General] section.

For parameter storage the syntax being used is:

Parameter=value

Here is an example of an INI file:

```
[General]
excludeSystemDisk=false
initHD=true
initRD=true
initCD=false
initFD=false
defaultSerialDetectionMethod=2
clearLog=false
logPath=C:\\Program Files\\LSoft Technologies\\Active@ KillDisk
Ultimate 11\\
logName=killdisk.log
logging=0
shutDown=false
saveToRemovable=false
showCert=true
killMethod=0
killVerification=false
killVerificationPercent=10
initDevice=true
fingerPrint=false
autoEject=false
skipConfirmation=false
wipeMethod=0
wipeVerification=false
wipeVerificationPercent=10
wipeUnusedCluster=true
wipeUnusedBlocks=false
```

```
wipeFileSlackSpace=false
wipeInHex=false
wipeUserPattern=Erased by Active@ KillDisk
wipeUserPasses=3
eraseInHex=false
killUserPattern=Erased by Active@ KillDisk
killUserPasses=3
accessDeniedCount=10
retryAtt=3
ignoreErrors=true
saveCert=true
certPath=C:\\Users\\Mikhail\\certificates\\
hideDefaultLogo=false
computerIDSource=0
showLogo=false
logoFile=
clientName=
companyName=
companyAddress=
companyPhone=
logComments=I hereby state that the data erasure has been
carried out in accordance with the instructions given by software
provider.
technicianName=Technician
sendSMTP=false
attachCert=true
useDefaultAccount=true
fromSMTP=
toSMTP=
nameSMTP=
portSMTP=2525
authorizeSMTP=false
usernameSMTP= password
SMTP=
mapName=
mapPath=
mapUser=
mapPass=
```


When KillDisk is running in interactive mode, all these parameters can be configured from a settings dialog accessed by clicking the “Settings” toolbar button. They also can be changed manually by editing the **KILLDISK.INI** file in any text editor such as Notepad.

Here is an explanation of all settings:

Table 4: KillDisk's Settings.ini Parameters

Parameter	Default	Options
defaultSerialDetectionMethod=	2	1 - use operating system's DeviceIOControl method
		2 - use S.M.A.R.T information, if device supports it
		3 - use Windows Management Instrumentation (WMI), if operating system supports it
showCert=	true	true/false – option of displaying the Erase/Wipe Certificate for printing after completion
saveCert=	false	true/false – option of saving the Erase/Wipe Certificate after completion
certPath=		Full path to the location where Erase/Wipe Certificate will be saved. This is a directory name
logPath=		Full path to the location where log file will be saved. This is a directory name
logName=		Name of the log file where event log will be saved to
skipConfirmation=	false	true/false – whether to display or skip Erase/Wipe confirmation dialog, or not
ignoreErrors=	false	true/false – whether to display disk writing errors (bad sectors), or ignore them (just place them to the log file)
clearLog=	false	true/false – whether to truncate log file content before writing new sessions, or not (append to existing content)
initDevice=	true	true/false – whether to initialize disks after erasing complete, or not
fingerPrint=	false	true/false – whether to initialize disk(s) and write fingerprint to the disk's first sector, or not
hideDefaultLogo	false	true/false – whether to hide default KillDisk logo at the top-left corner of the certificate, or not
computerIDSource=	0	0 - Disables showing the computer ID on the certificate
		1 - Shows BIOS ID in the certificate
		2 - Shows Motherboard ID in the certificate
shutDown=	false	true/false – whether to shutdown PC after Erase/Wipe execution complete, or not
sendSMTP=	false	true/false – to send e-mail report by email via SMTP
attachCert=	false	true/false – to attach a PDF certificate to e-mail report being sent
useDefaultAccount=	true	true/false – use pre-defined Free SMTP account for sending e-mail reports
fromSMTP=		E-mail address you'll get a report from, for example: reports@killdisk.com

Parameter	Default	Options
toSMTP=		E-mail address the report will be sent to
nameSMTP=		SMTP server (relay service) being used for sending e-mail reports, for example: www.smtp-server.com
portSMTP=	25	TCP/IP port SMTP service will be connected on. The standard SMTP port is 25, however some internet providers block it on a firewall
authorizeSMTP=	false	true/false – use SMTP authorization for sending e-mail reports (Username and Password must be defined as well)
usernameSMTP=		In case if SMTP service requires authorization, this is SMTP Username
passwordSMTP=		In case if SMTP service requires authorization, this is SMTP Password
showLogo=	false	true/false – whether to display custom Logo (image) on a Certificate, or not
logoFile=		Full path to the file location where Logo image is stored
clientName=		Client Name - custom text to be displayed on a Certificate
technicianName=		Technician Name - custom text to be displayed on a Certificate
companyName=		Company Name - custom text to be displayed on a Certificate
companyAddress=		Company Address - custom text to be displayed on a Certificate
companyPhone=		Company Phone - custom text to be displayed on a Certificate
logComments=		Any Comments - custom text to be displayed on a Certificate
killMethod=	2	[0-23] – Erase method to use for disk/volume erasing. See table of Erase Methods available. DoD 5220.22-M by default
killVerification=	true	true/false – whether to use data verification after erase, or not
killVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
killUserPattern=		ASCII text to be used for User Defined erase method as a custom pattern
killUserPasses=		[1-99] – number of overwrites to be used for User Defined erase method
wipeMethod=	2	[0-23] – Wipe method to use for volume wiping. See table of Erase Methods available. DoD 5220.22-M by default
wipeVerification=	true	true/false – whether to use data verification after wipe, or not
wipeVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
wipeUserPattern=		ASCII text to be used for User Defined wipe method as a custom pattern
wipeUserPasses=		[1-99] – number of overwrites to be used for User Defined wipe method
wipeUnusedCluster=	True	true/false – whether to wipe out all unused clusters on a volume, or not
wipeUnusedBlocks=	False	true/false – whether to wipe out all unused blocks in system records, or not
wipeFileSlackSpace=	False	true/false – whether to wipe out all file slack space (in last file cluster), or not

When you start **KillDisk** with or without command line parameters, its execution behavior depends on either command line settings (highest priority), settings configured in interactive mode and stored in the **KILLDISK.INI** file (lower priority), or default values (lowest priority).

Default value means that if the **KILLDISK.INI** file is absent, or exists but contains no required parameter, the pre-defined (default) value will be used.

The latest version of **KillDisk 12** still supports settings stored by previous versions in INI file, however when first run, it exports all settings to **SETTINGS.XML** file and work with this file thereafter.

Troubleshooting and System Recovery

In the event that you encounter technical difficulties with KillDisk, you may choose to either troubleshoot the system yourself with the files describe or, if you have active support and updates (you receive 1 year free with your purchase), contact our support team and attach your application log and hardware configuration file.

Common Troubleshooting Tips

Active@ Boot Disk Creator Troubleshooting:

All the OS options are greyed out

Ensure you have the Boot Disk Creator activated. You should see your registered name in the application.

Image file not found

You have activated the freeware that does not have the boot disk image you wish to create. Download your complete version using the link provided in your email and reinstall the software.

Issues formatting USB drive

This may happen occasionally when the file system causes conflicts in Windows. Launch the KillDisk application and erase the first few megabytes of the USB drive you wish to use. This will solve the problem.

Issues booting from the boot disk

Ensure the boot disk device is set at the top of your boot priority in the BIOS

Ensure your system time in the BIOS is accurate

Ensure you are not booting a 64-bit boot disk on a 32-bit system. In these cases, create a Console boot disk

Active@ KillDisk Troubleshooting:

Disk data will not erase

Ensure you are not erasing the system disk from the application. Use the boot disk to erase system disks

Data still found after a 'Wipe' operation

The Wipe operation will only sanitize data that has already been deleted in the OS. To sanitize all the data, including the operating system, use the 'Kill' operation

Erased the wrong disk

Stop the operation as soon as possible. Once data is sanitized by KillDisk, it will no longer be accessible. Use a tool like Active@ File Recovery to recover any data that has not been sanitized

Application Log

This log view monitors each action taken by the application and displays messages, notifications and other service information. Use the messages in this screen to observe and further understand the flow of the recovery process.

To open and activate Application log view do one of the following:

- From main menu choose **Tools > Application Log** or
- Use **F8** keyboard shortcut at any time

It is best to save the log file to a physical disk that is different from the disk that holds the deleted data. By doing this, you reduce the risk of writing over the data that you are trying to recover.

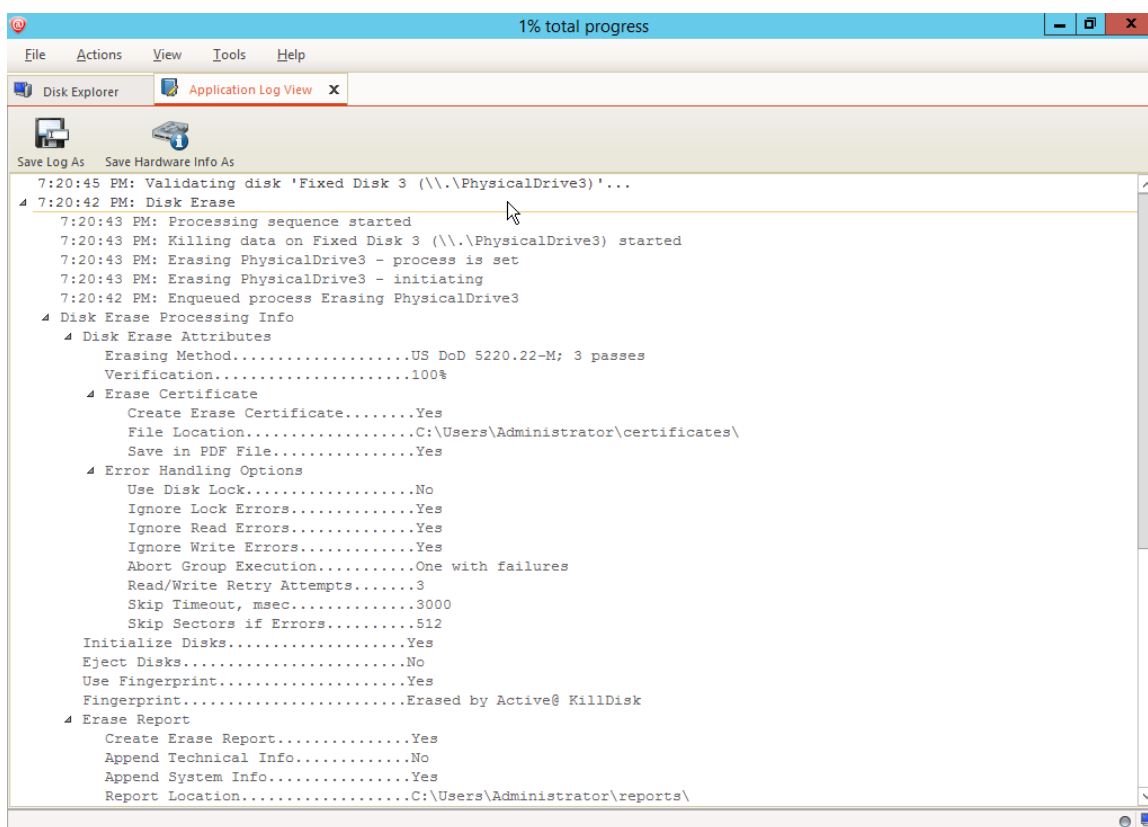


Figure 58: Viewing the application log

Log filter

Show or hide specific entry types in log view:

Show warning entries

Show non-critical warning entries

Show advanced entries

Show advanced entries related to application behavior and data analysis

Show console entries

Duplicate console entries into main log view

Show system entries

Show entries related to operating system activity and state

Font size

Change size of mono-space font used in log view for better experience

Write log on Disk

Writes log entries in dedicated file on disk, located in application directory. **Off** by default.

Expand and Collapse

Expand or collapse all log entries respectively

Clear

Clear log for current application sessions



Tip: We recommend that you attach a copy of the log file to all requests made to our technical support group. The entries in this file will help us resolve certain issues.

Hardware Diagnostic File

If you want to contact our technical support staff for help, a file that contains a summary of your local devices is helpful.

KillDisk allows you to create a summary listing file in XML format. This data format is “human-readable” and can help our technical support staff analyze your computer configuration or point out disk failures or abnormal behavior.

Create a hardware diagnostic file from the **File** menu by clicking the **Save Hardware Info as...** command.



Note: To save time when contacting our technical support staff, we highly recommend that you provide us with a hardware diagnostic file.

Appendix

Glossary

BIOS settings

Basic Input Output Subsystem. This programmable chip controls how information is passed to various devices in the computer system. A typical method to access the BIOS settings screen is to press F1, F2, F8, F10 or ESC during the boot sequence.

boot priority

BIOS settings allow you to run a boot sequence from a floppy drive, a hard drive, a CD/DVD-ROM drive or a USB device. You may configure the order that your computer searches these physical devices for the boot sequence. The first device in the order list has the first boot priority. For example, to boot from a CD/DVD-ROM drive instead of a hard drive, place the CD/DVDROM drive ahead of the hard drive in priority.

compressed cluster

When you set a file or folder property to compress data, the file or folder uses less disk space. While the size of the file is smaller, it must use a whole cluster in order to exist on the hard drive. As a result, compressed clusters contain "file slack space". This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data without touching the existing data.

cluster

A logical group of disk sectors, managed by the operating system, for storing files. Each cluster is assigned a unique number when it is used. The operating system keeps track of clusters in the hard disk's root records or MFT records. (See lost cluster).

file slack space

The smallest file (and even an empty folder) takes up an entire cluster. A 10- byte file will take up 2,048 bytes if that is the cluster size. File slack space is the unused portion of a cluster. This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data without touching the existing data.

free cluster

A cluster that is not occupied by a file. This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data.

deleted boot records

All disks start with a boot sector. In a damaged disk, if the location of the boot records is known, the partition table can be reconstructed. The boot record contains a file system identifier.

ISO

An International Organization for Standardization ISO-9660 file system is a standard CD-ROM file system that allows you to read the same CD-ROM whether you're on a PC, Mac, or other major computer platform. Disk images of ISO-9660 file systems (ISO images) are a common way to electronically transfer the contents of CD-ROMs. They often have the filename extension .ISO (though not necessarily), and are commonly referred to as "ISOs".

lost cluster

A cluster that has an assigned number in the file allocation table, even though it is not assigned to any file. You can free up disk space by reassigning lost clusters. In DOS and Windows, you can find lost clusters with the ScanDisk utility.

MFT records

Master File Table. A file that contains the records of every other file and directory in an NTFS-formatted hard disk drive. The operating system needs this information to access the files.

PXE

Preboot Execution Environment - In computing, the Preboot eXecution Environment specification describes a standardized client-server environment that boots a software assembly, retrieved from a network, on PXE-enabled clients. On the client side it requires only a PXE-capable network interface controller, and uses a small set of industry-standard network protocols such as DHCP and TFTP.

root records

File Allocation Table. A file that contains the records of every other file and directory in a FAT-formatted hard disk drive. The operating system needs this information to access the files. There are FAT32, FAT16 and FAT versions.

sector

The smallest unit that can be accessed on a disk. Tracks are concentric circles around the disk and the sectors are segments within each circle.

unallocated space

Space on a hard disk where no partition exists. A partition may have been deleted or damaged or a partition may not have been created.

unused space in MFT records

The performance of the computer system depends a lot on the performance of the MFT. When you delete files, the MFT entry for that file is not deleted, it is marked as deleted. This is called unused space in the MFT. If unused space is not removed from the MFT, the size of the table could grow to a point where it becomes fragmented, affecting the performance of the MFT and possibly the performance of the computer. This space may also contain residual confidential data (file names, file attributes, resident file data) from the files that previously occupied these spaces. KillDisk can wipe out the residual data without touching the existing data.

Windows system caching

Windows reserves a specified amount of volatile memory for file system operations. This is done in RAM because it is the quickest way to do these repetitive tasks.

Windows system records

The Windows registry keeps track of almost everything that happens in windows. This enhances performance of the computer when doing repetitive tasks. Over time, these records can take up a lot of space.

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 are becoming more resourceful by looking into 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 operating system 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. Ordinarily, 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.

Moreover, most of hard disks contain hidden zones (disk areas that cannot be accessed and addressed on a logical access level). **KillDisk** is able to detect and reset these zones, cleaning up the information inside.

Advanced Data Recovery Systems

Advances in data recovery have been made such that in many cases data can be reclaimed from hard drives that have been wiped and disassembled.

Security agencies use advanced applications to find cybercrime-related evidence. There also are established industrial spy agencies adopting sophisticated channel coding techniques such as **Partial Response Maximum Likelihood (PRML)**, 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, data can easily be restored with the help of an off-the-shelf data recovery utility like [Active@ File Recovery](#), making your erased confidential data quite accessible.

Using our powerful and compact **Active@ KillDisk** utility, all data on your Hard Disk Drive/Solid State Disk or removable USB drive can be destroyed without the possibility of future recovery.

After using **Active@ KillDisk**, disposal, recycling, selling or donating your storage device can be done with peace of mind.

International Standards in Data Removal

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

Active@ KillDisk is a quality 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 Subsystem), bypassing the operating system's logical drive structure organization. Regardless of the operating system, file systems, or type of machine, this utility can destroy all data on all storage devices. It does not matter which operating systems or file systems are located on the machine.

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.

KillDisk wipes unused data residue from file slack space, unused sectors, and unused space in MFT 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. KillDisk 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. KillDisk supports more than 20 international data sanitizing standards, including US DoD 5220.22M and the most secure Gutmann's method overwriting with 35 passes.

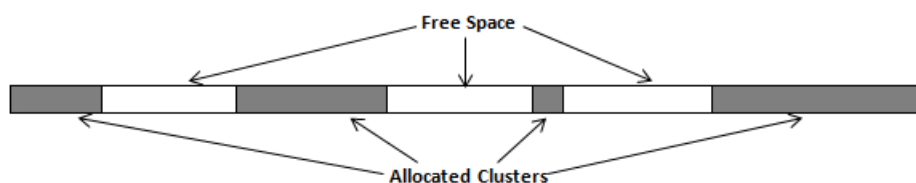


Figure 59: Disk free space and allocated clusters

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 4KB increments and thus have slack space at their end.

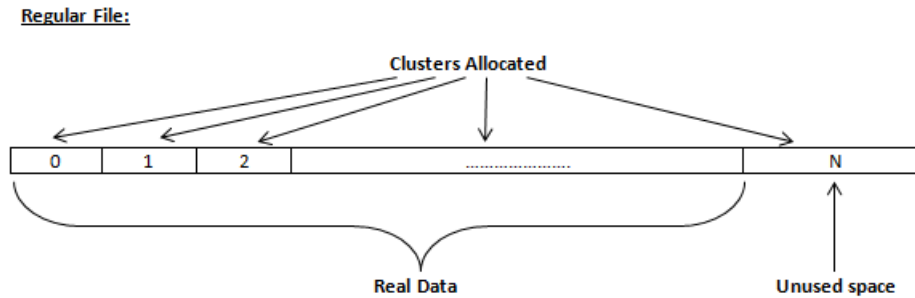


Figure 60: Disk free space and allocated clusters

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 64KB 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.

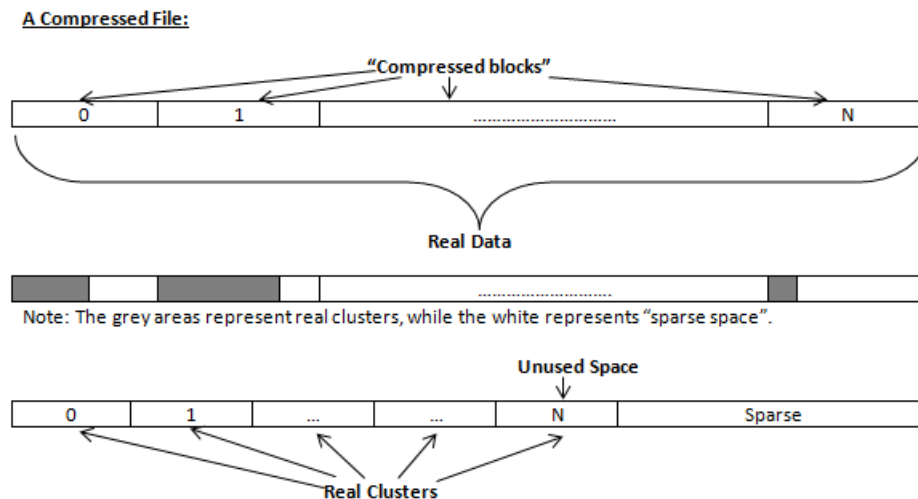


Figure 61: Compressed file structure

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 KillDisk wipes all of the unused information out of the MFT records and wipes the unusable space, making a recovery process impossible.

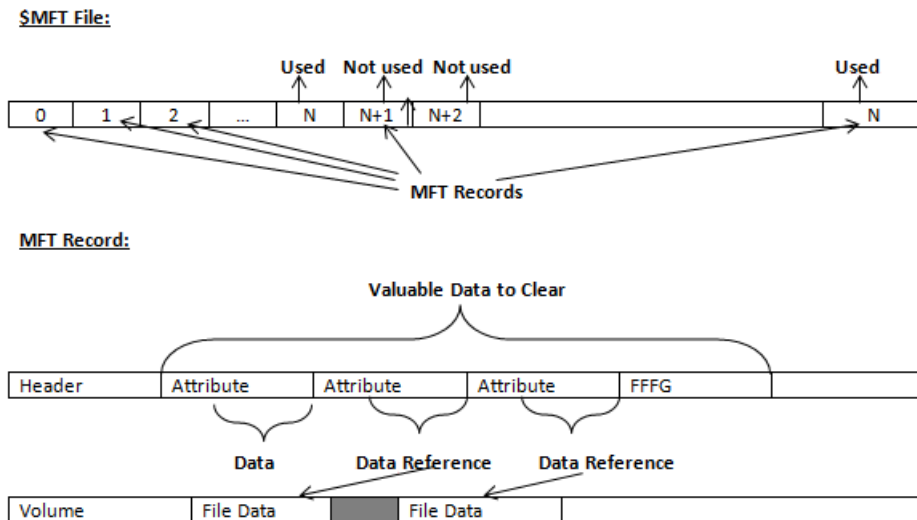


Figure 62: MFT structure

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@ KillDisk makes data recovery impossible by using an algorithm that wipes out all unused information from directory descriptors. Active@ KillDisk 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 UAA
00000030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	AAAAAAAAAAAA AAAA
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	ÿÿÿÿ \$ÿÿ@
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 AA AAAA
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	ÿÿÿÿ 'ÿÿÿH"
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	ÿÿÿÿ wÿÿ@>>
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	ÿÿ A -ÿÿ@«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	ÿÿÿÿ 5ÿÿ@1H
00000140	24	52	45	43	59	43	4C	45	42	49	4E	16	00	26	6A	32	\$RECYCLEBIN 5j2
00000150	A2	40	A2	40	0A	00	6B	32	A2	40	C5	01	00	00	00	00	ÿÿÿÿ k2ÿÿ@E
00000160	4C	44	4D	20	20	20	20	20	54	58	54	20	10	A8	87	21	LDM TXT E+!
00000170	D5	40	D5	40	09	00	8A	B3	D5	40	07	1F	CF	11	00	00	X0X0 5iX0 0 0
00000180	E5	52	43	48	49	56	45	20	5A	49	50	20	00	7A	D9	B5	eRCHIVE ZIP zllp
00000190	A2	40	A2	40	20	00	00	2E	00	70	00	0F	00	3C	61	00	ÿÿÿÿ . 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	

Figure 63: 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	08	00	00	00	00	00	WORK	Record 0: Valid Volume Label "WORK"
00000010	00	00	00	00	00	24	27	A2	40	00	00	00	00	00	00	00	\$'ÿ@	Records 1-2 (before wipe - 6-7): Normal Folder "Documentation" (begins with a cluster #301886)
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	ÿ@ÿ@ w&ÿ@>>	
00000060	50	52	4F	4A	45	43	54	53	20	20	20	10	00	24	6B	28	PROJECTS \$k (Record 3 (before wipe - 8): Normal Folder "PROJECTS" (begins with a cluster #621227)
00000070	A2	40	1E	41	09	00	AD	26	A2	40	AB	7A	00	00	00	00	ÿ@ A -&ÿ@«z	
00000080	24	52	45	43	59	43	4C	45	42	49	4E	16	00	26	6A	32	\$RECYCLEBIN &j2	Record 4 (before wipe - 10): Normal Folder "\$RECYCLE.BIN" (begins with a cluster #653813)
00000090	A2	40	A2	40	0A	00	6B	32	A2	40	C5	01	00	00	00	00	ÿ@ÿ@ k2ÿ@E	
000000A0	4C	44	4D	20	20	20	20	20	54	58	54	20	10	A8	87	21	LDM TXT E+I	Record 5 (before wipe - 11): Normal File "LDM.TXT" (begins with a cluster #597767 and has the size 4559 bytes)
000000B0	D5	40	D5	40	09	00	8A	B3	D5	40	07	1F	CF	11	00	00	X@X@ .iX@ Π	
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		

Figure 64: Directory Area after Wiping: all deleted records removed, root defragmented

Specifics of Wiping Apple HFS+ File System

HFS+ B-tree

A B-tree file is divided up into fixed-size nodes, each of which contains records consisting of a key and some data.

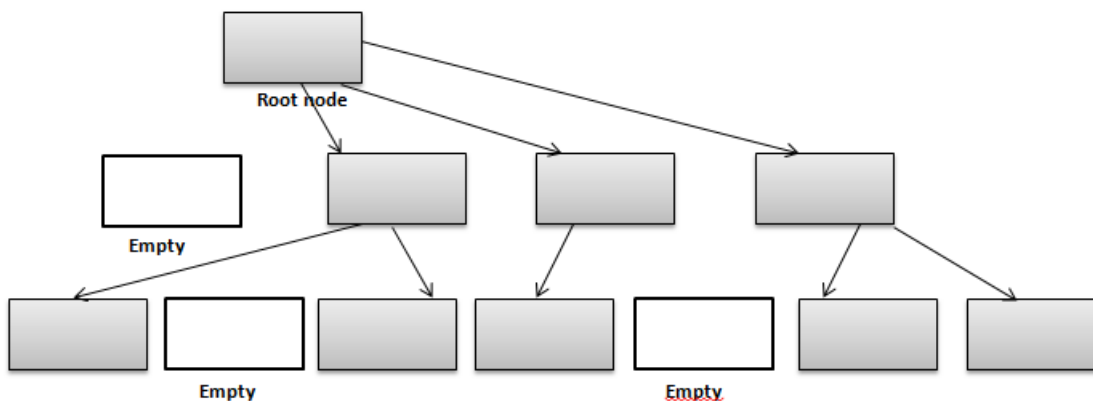


Figure 65: B-tree structure

In the event of the deletion of a file or folder, there is a possibility of recovering the metadata of the file, (such as its name and attributes), as well as the actual data that the file consists of. KillDisk's Wipe method clears out all of this free space in the system files.

Node Description
Record II 0
Record II 1
.....
Record #N
Free Space
Records' offsets

Figure 66: HFS+ system table

Specifics of Wiping Linux Ext2/Ext3/Ext4 File Systems

A Linux Ext file system (Ext2/Ext3/Ext4) volume has a global descriptors table. Descriptors table records are called group descriptors and describe each blocks group. Each blocks group has an equal number of data blocks.

A data block is the smallest allocation unit: size vary from 1024 bytes to 4096 bytes. Each group descriptor has a blocks allocation bitmap. Each bit of the bitmap shows whether the block is allocated (1) or available (0). KillDisk software enumerates all groups, and for each and every block within the group on the volume checks the related bitmap to define its availability. If the Block is available, KillDisk wipes it using the method supplied by the user.

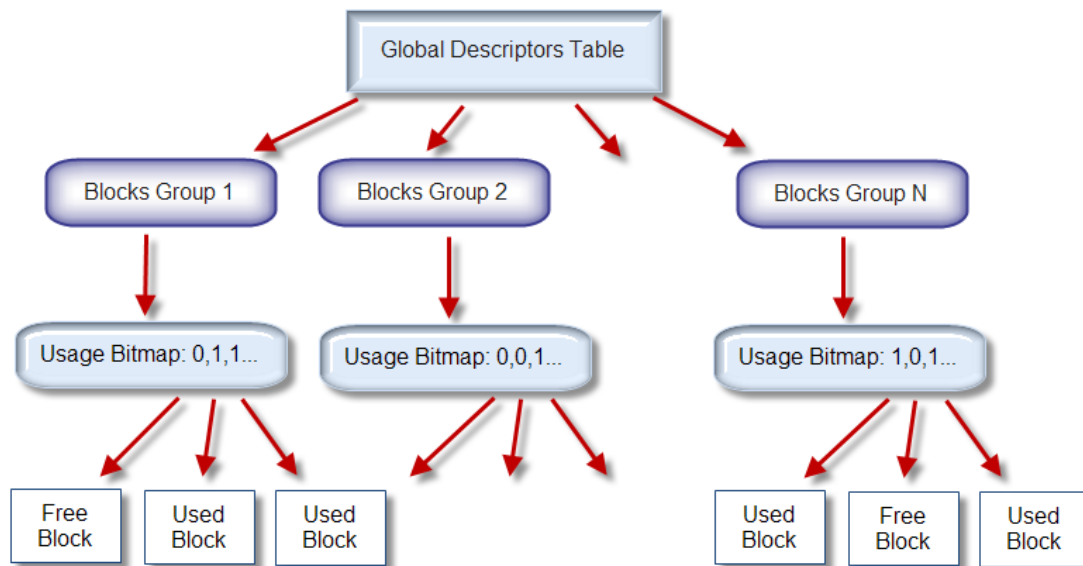


Figure 67: Ext2/Ext3/Ext4 descriptors table

Erase 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 sanitization 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.

User Defined

User indicates the number of times the write head passes over each sector. Each overwriting pass is performed with a buffer containing random characters. Enables user to define any disk erase algorithm.

Using KillDisk in PXE environment

How to place a registered Active@ KillDisk into a Windows PE image for use in a network PXE boot environment



Note: To modify Windows PE image (WIM) you need to have [Windows ADK](#) installed.

Start the Active@ Boot Disk Creator and make bootable media.

Let's assume that the Active@ Boot Disk media has an **F:** letter in our environment:

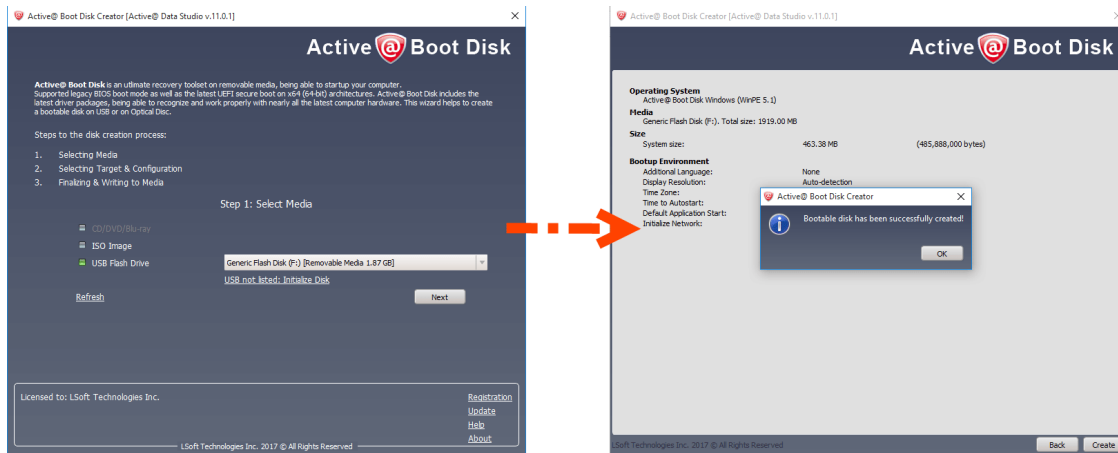


Figure 68: Creating Active@ KillDisk bootable media

Using the Windows Search Bar, find and run Command Prompt as an Administrator:

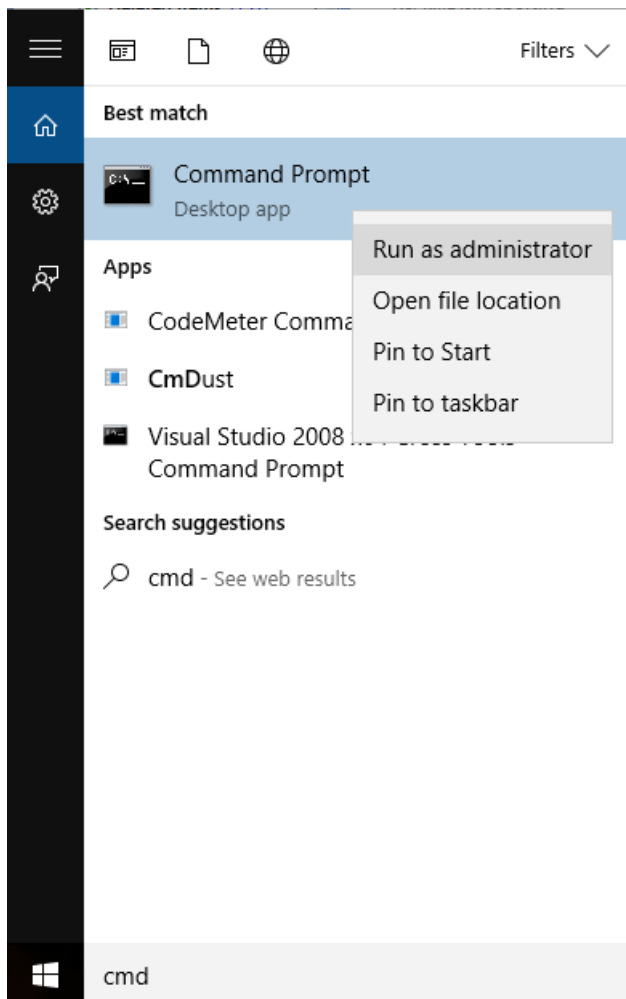


Figure 69: Run Command Prompt as Administrator

Create an empty directory **C:\MOUNT** and mount **BOOT.WIM** file to it using the DISM tool:

```
Command: Dism /mount-image /imagefile:F:\sources\boot.wim /index:1 /
mountdir:C:\mount
```

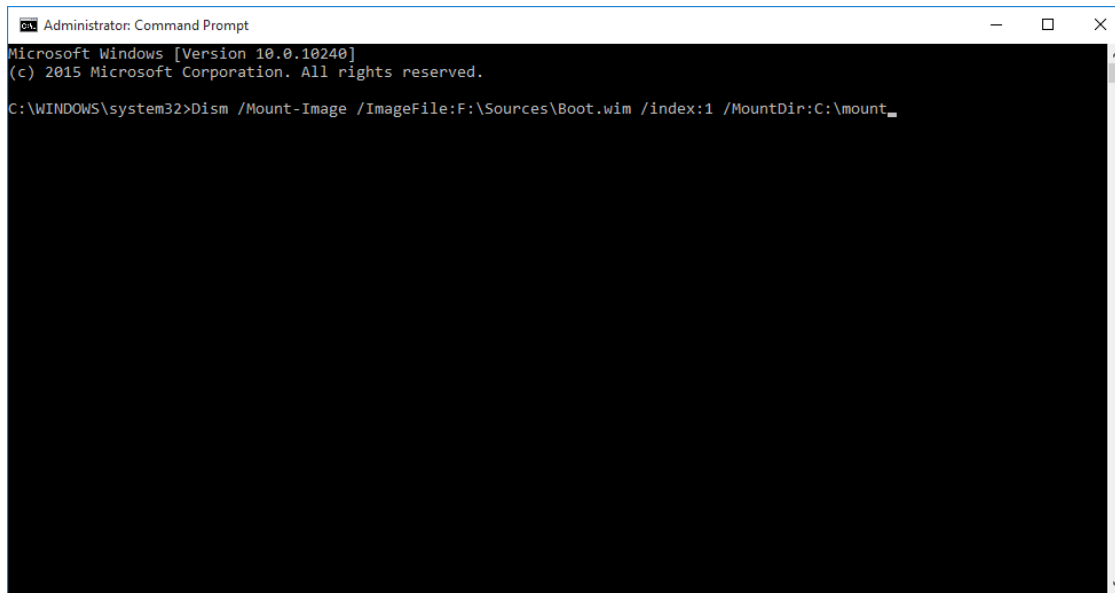


Figure 70: Mounting BOOT.WIM

Replace **BOOTDISK.KEY** in **C:\MOUNT** directory with **BOOTDISK.KEY** located at the root of Active@ Boot Disk media (F:\BOOTDISK.KEY). This file contains user's registration information.

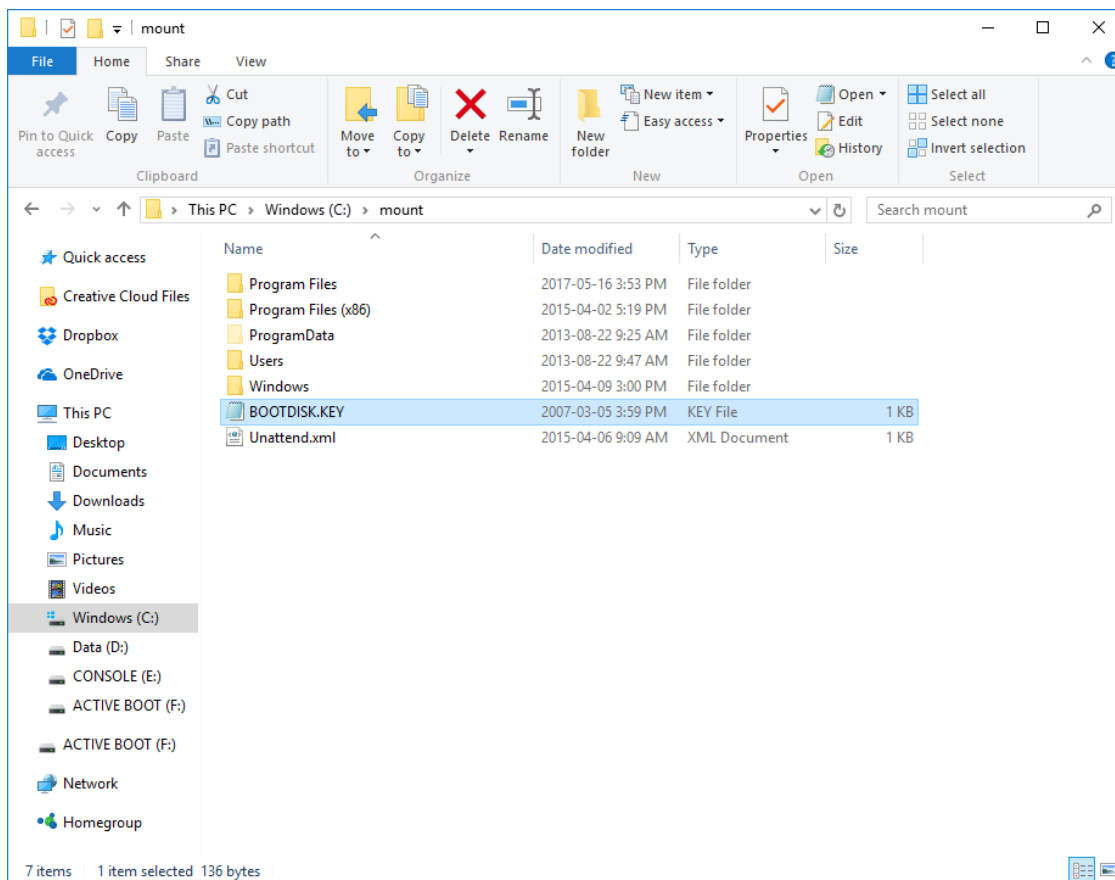


Figure 71: Replacing BOOTDISK.KEY in BOOT.WIM

Dismount the **BOOT.WIM** image, committing the changes you applied:

Command: `Dism /Unmount-Image /MountDir:C:\mount /commit`

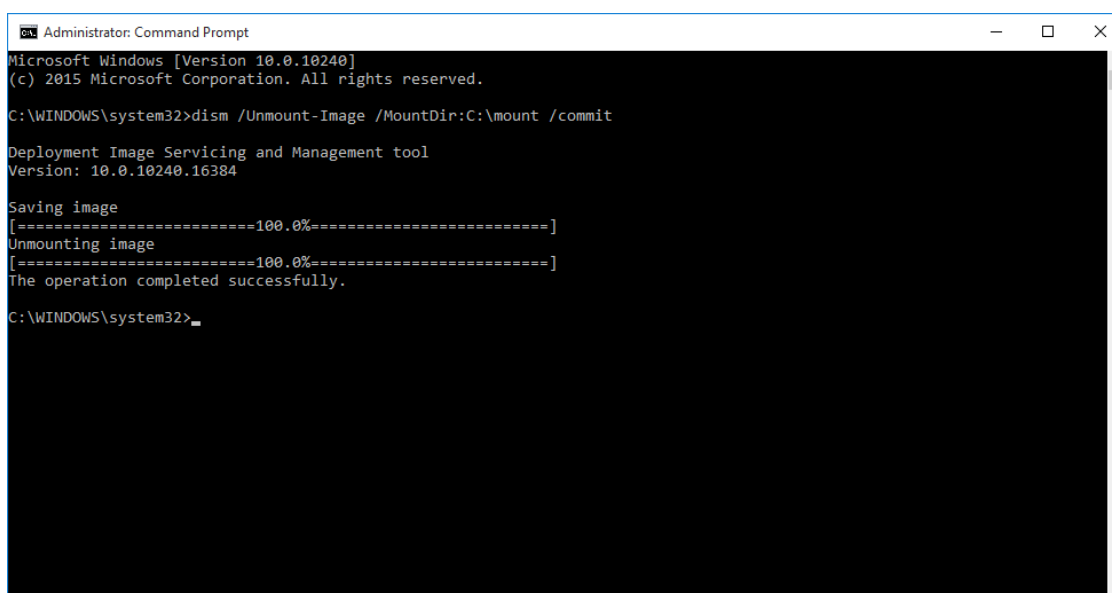


Figure 72: Dismounting BOOT.WIM

Use **F:\SOURCES\BOOT.WIM** for network PXE boot environment

How to load Active@ KillDisk over the network via PXE environment on Windows Server platform

- Add roles Windows Deployment Services
- Configure the WDS server, but don't add images in WDS Configuration Wizard
- Add Windows PE image with Active@ KillDisk software Boot.wim in Boot Images on WDS server
- In properties of WDS server in Boot tab add our image as default boot image for x64 architecture
- Configure the DHCP server for work with WDS server

For more detailed instructions, read [Microsoft TechNet](#) official documentation.

How to load Active@ KillDisk over the network via PXE environment on a Windows 10 computer

There are several steps required to do this: configuring the WinPE WIM, Boot Manager and PXE Server.

For the configuration steps, let's assume that inserted Active@ Boot Disk has a F: letter in our configuration environment.

Step 1: Copy WinPE Source Files onto the PXE Server

- Map a network connection to the root TFTP directory on the PXE/TFTP server and create a **\BOOT** folder there. We will assign this network drive the **Y:** letter

 **Note:** You can the 'Easy access' feature in the Windows Explorer to do this

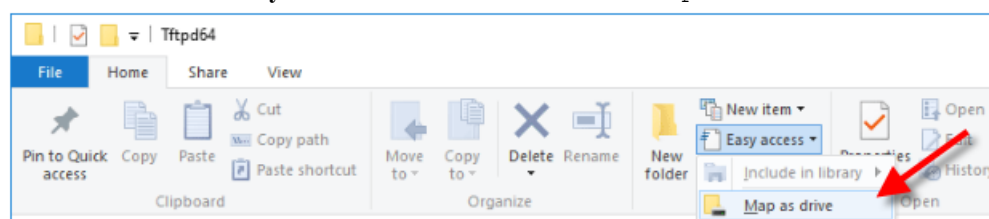


Figure 73: Mapping drive in Windows Explorer

Make sure to enable read/write permissions in the sharing and folder options

- Copy the PXE boot files from the mounted **\BOOT** folder of the Active@ Boot Disk *boot.wim* to the **\BOOT** folder on PXE/TFTP server. For example:

```
copy C:\mount\windows\boot\pxe\*. * y:\boot
```



Note: To mount/dismount the *boot.wim* file, see section “*How to place a registered Active@ KillDisk into a Windows PE image for use in a network PXE boot environment*”

- After dismounting the *boot.wim*, copy the bootable Windows PE image (F:\Sources\boot.wim) to the \BOOT folder on PXE/TFTP server
- Copy the file boot.sdi (F:\Boot\boot.sdi) to the \BOOT folder on PXE/TFTP server

Step 2: Configure boot configuration

- On a Windows 10 computer or in a Windows PE environment, create a BCD store using the BCDEdit tool
- In the BCD store, configure the **RAMDISK**, **BOOTMGR** and **OSLoader** settings for the Windows PE image
- Copy the BCD file to the \BOOT folder on PXE/TFTP server
- Configure your PXE/TFTP server and DHCP server to point PXE clients to download **PXEBoot.com** or **PXEBoot.n12**

These are a few of the files that were copied over to the server in **Step 1**

For more details, see “*Creating a BCD file for PXE boot*” below.

Step 3: Deployment process

Boot the client machine through PXE, connected to the network. After pressing initializing the PXE boot, the system should handle the rest. Here’s what will happen:

- The client is directed (by using DHCP Options or the PXE Server response) to download **PXEBoot.com**
- **PXEBoot.com** downloads **Bootmgr.exe** and the BCD store. The BCD store must reside in a \BOOT directory in the TFTP root folder. Additionally, the BCD store must be called **BCD**
- **Bootmgr.exe** reads the BCD operating system entries and downloads **boot.sdi** and the Windows PE image
- **Bootmgr.exe** begins booting Windows PE by running **Winload.exe** within the Windows PE image

For more detailed instructions, read the Microsoft TechNet official documentation.

Configuring a PXE Server

Configuring a TFTP server is made simple with a tool called *Serva*. You can download it [here](#).

This tool is an “*Automated PXE Server Solution Accelerator*” that supports a variety of server protocols. The ones we will be configuring are TFTP and DHCP.

- Click the logo in the top left to access the Settings
- Configure your DHCP settings. You may copy the ones below, just make sure the address it binds to is a static IP address from your router. Under IP Pool 1st addr, input the first available IP address in your routers IP pool settings.

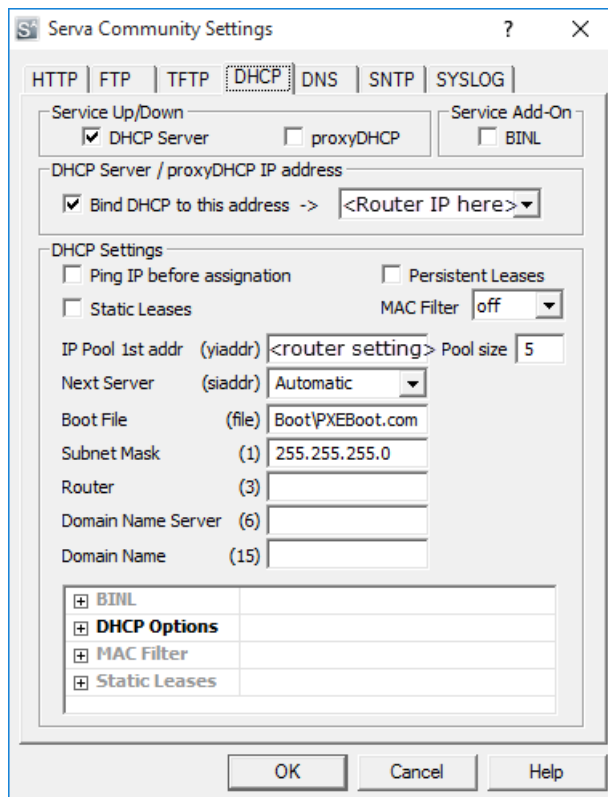


Figure 74: DHCP configuration

- Configure your TFTP settings. You may also copy the setting below. Again, make sure the IP address is your router's static IP and the TFTP server root directory is the one you configured in Step 1.

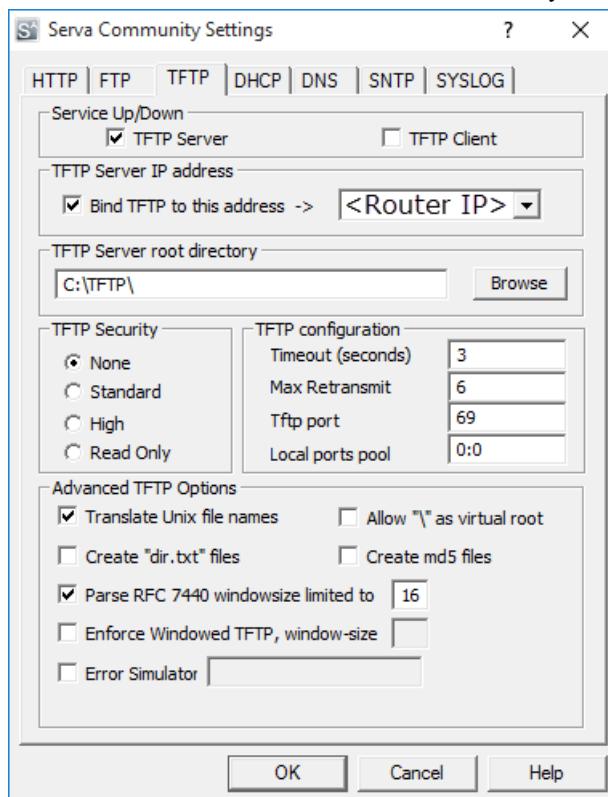


Figure 75: TFTP configuration

Once the settings are configured, reset the application and your PXE server should be fully operational!

Creating a BCD file for PXE boot:

This entire process is done in Windows Command Prompt. Be sure to run it as **Administrator**.

1. Create a BCD store using `bcdedit.exe`:

```
bcdedit /createstore c:\BCD
```

2. Configure **RAMDISK** settings:

```
bcdedit /store c:\BCD /create {ramdiskoptions} /d "Ramdisk options"
bcdedit /store c:\BCD /set {ramdiskoptions} ramdisksdidevice boot
bcdedit /store c:\BCD /set {ramdiskoptions} ramdisksdipath \boot\boot.sdi
bcdedit /store c:\BCD /create /d "winpe boot image" /application osloader
```

The last command will return a GUID, for example:

The entry { bb254249-93e9-11e7-84cb-6c71d9da760e } was successfully created.

Copy this GUID for use in the next set of commands. In each command shown, replace "GUID1" with your GUID.

3. Create a new boot application entry for the Windows PE image:

```
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} device ramdisk=[boot]\Boot\boot.wim,{ramdiskoptions}
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} path \windows\system32\winload.exe
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} osdevice ramdisk=[boot]\Boot\boot.wim,{ramdiskoptions}
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} systemroot \windows
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} detecthal Yes
bcdedit /store c:\BCD /set {bb254249-93e9-11e7-84cb-6c71d9da760e} winpe Yes
```

4. Configure **BOOTMGR** settings (remember to replace GUID1 in the third command with your GUID):

```
bcdedit /store c:\BCD /create {bootmgr} /d "boot manager"
bcdedit /store c:\BCD /set {bootmgr} timeout 30
bcdedit /store c:\BCD -displayorder {bb254249-93e9-11e7-84cb-6c71d9da760e} -addlast
```

5. Copy the BCD file to your TFTP server:

```
copy c:\BCD \\PXE-1\TFTP\Boot\BCD
```

Your PXE/TFTP server is now configured. You can view the BCD settings that have been configured using the command:

```
bcdedit /store <BCD file location> /enum all
```

See the following example below.



Note: Your GUID will be different than the one shown below.

```
C:\>bcdedit /store C:\BCD /enum all
Windows Boot Manager
-----
identifier                {bootmgr}
description                boot manager
displayorder              {bb254249-93e9-11e7-84cb-6c71d9da760e}
timeout                   30

Windows Boot Loader
-----
identifier                {bb254249-93e9-11e7-84cb-6c71d9da760e}
device                    ramdisk=[boot]\boot\boot.wim,{ramdiskoptions}
description                winpe boot image
osdevice                  ramdisk=[boot]\boot\boot.wim,{ramdiskoptions}
systemroot                \Windows
detecthal                 Yes
winpe                     Yes

Setup Ramdisk Options
-----
identifier                {ramdiskoptions}
description                ramdisk options
ramdisksdidevice          boot
ramdisksdipath            \boot\boot.sdi
```

File Name Tags

Sequence number

Sequential number, used for group (batch) processing.

{Sequence #}

{Sequence 0#}

{Sequence 00#}

{Sequence 000#}

Date

Date file name tag uses current date in most cases in different formats:

{Date(YYYYMMDD)}

{Date(YYYY-MM-DD)}

{Date(YYMMDD)}

{Date(YYYY)}

{Date(YY)}

{Date(Month)}

{Date(MM)}

{Date(DD)}

Time name tags

{Time(HHmmss)}

{Time(HH-mm-ss)}

{Time(HH)}

{Time(mm)}

{Time(ss)}

Disk name tags

Values for these name tags retrieved from context device:

{Serial ID}

Disk serial number, retrieved from OS or from SMART attributes

{Platform ID}

Disk platform identification (may be vary due to OS format);

{Product ID}

Disk manufacturer id

{Model}

Disk model name (if available);

{Size}

Disk size in gigabytes

{Sectors}

Disk size in sectors

Processing attributes

Disk processing attributes based on execution conditions:

{BatchName}

Batch name, if part of a batch processing.

{BayName}

Label of disk bay (slot).

{Status}

Overall completion status for group processing or separate disk processing status.

Disk Hidden Zones (HPA/DCO)

Active@ KillDisk is able to detect and reset disk's hidden zones: HPA and DCO.

HPA - Host protected area

The **host protected area (HPA)** is an area of a hard drive or solid-state drive that is not normally visible to an operating system. It was first introduced in the ATA-4 standard CXV (T13) in 2001.

How it works

The IDE controller has registers that contain data that can be queried using ATA commands. The data returned gives information about the drive attached to the controller. There are three ATA commands involved in creating and using a host protected area. The commands are:

- IDENTIFY DEVICE
- SET MAX ADDRESS
- READ NATIVE MAX ADDRESS

Operating systems use the IDENTIFY DEVICE command to find out the addressable space of a hard drive. The IDENTIFY DEVICE command queries a particular register on the IDE controller to establish the size of a drive.

This register however can be changed using the SET MAX ADDRESS ATA command. If the value in the register is set to less than the actual hard drive size then effectively a host protected area is created. It is protected because the OS will work with only the value in the register that is returned by the IDENTIFY DEVICE command and thus will normally be unable to address the parts of the drive that lie within the HPA.

The HPA is useful only if other software or firmware (e.g. BIOS) is able to use it. Software and firmware that are able to use the HPA are referred to as 'HPA aware'. The ATA command that these entities use is called READ NATIVE MAX ADDRESS. This command accesses a register that contains the true size of the hard drive. To use the area, the controlling HPA-aware program changes the value of the register read by IDENTIFY DEVICE to that found in the register read by READ NATIVE MAX ADDRESS. When its operations are complete, the register read by IDENTIFY DEVICE is returned to its original fake value.

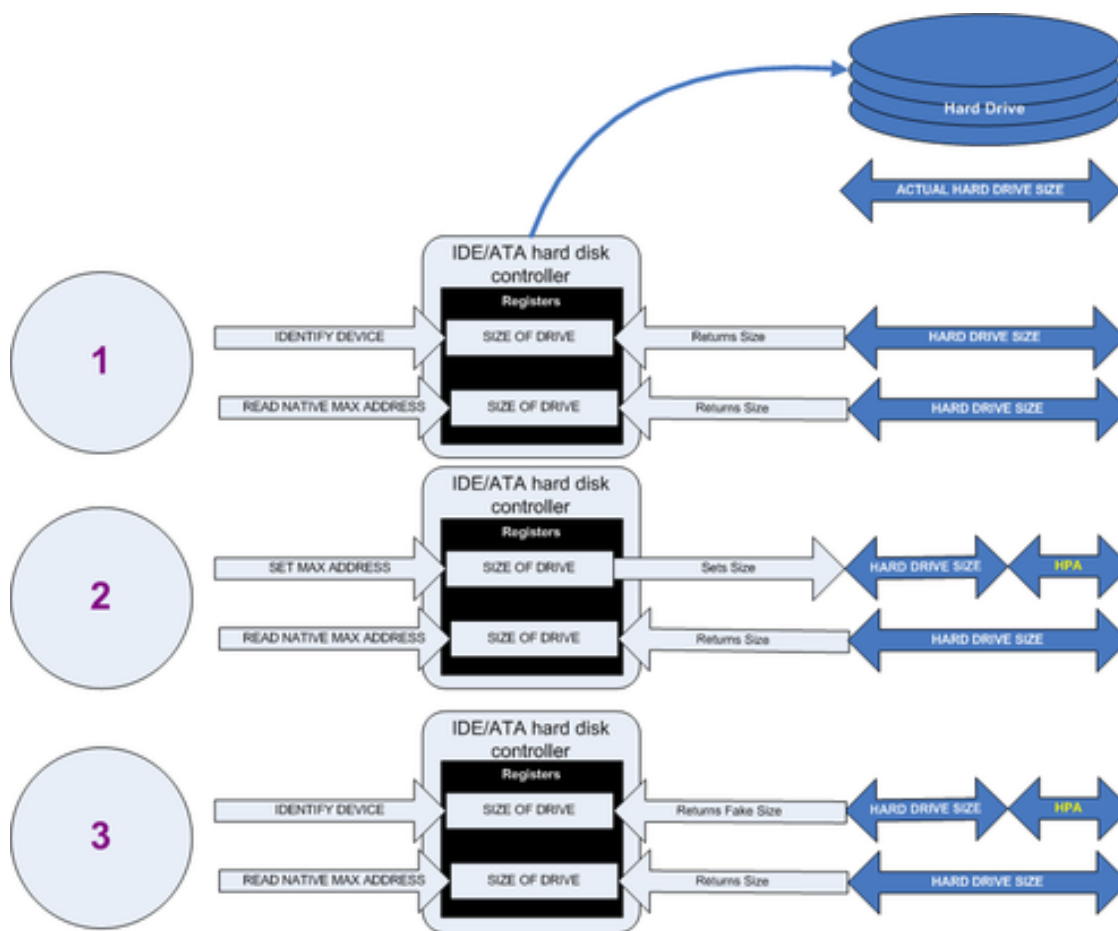


Figure 76: Creation of an HPA

The diagram shows how a host protected area (HPA) is created:

1. **IDENTIFY DEVICE** returns the true size of the hard drive. **READ NATIVE MAX ADDRESS** returns the true size of the hard drive.
2. **SET MAX ADDRESS** reduces the reported size of the hard drive. **READ NATIVE MAX ADDRESS** returns the true size of the hard drive. An HPA has been created.
3. **IDENTIFY DEVICE** returns the now fake size of the hard drive. **READ NATIVE MAX ADDRESS** returns the true size of the hard drive, the HPA is in existence.

Usage

- At the time HPA was first implemented on hard-disk firmware, some BIOS had difficulty booting with large hard disks. An initial HPA could then be set (by some jumpers on the hard disk) to limit the number of cylinder to 4095 or 4096 so that older BIOS would start. It was then the job of the bootloader to reset the HPA so that the operating system would see the full hard-disk storage space.
- HPA can be used by various booting and diagnostic utilities, normally in conjunction with the BIOS. An example of this implementation is the Phoenix FirstBIOS, which uses **Boot Engineering Extension Record (BEER)** and **Protected Area Run Time Interface Extension Services (PARTIES)**. Another example is the Gujin installer which can install the bootloader in BEER, naming that pseudo-partition `/dev/hda0` or `/dev/sdb0`; then only cold boots (from power-down) will succeed because warm boots (from Control-Alt-Delete) will not be able to read the HPA.
- Computer manufacturers may use the area to contain a preloaded OS for install and recovery purposes (instead of providing DVD or CD media).
- Dell notebooks hide Dell MediaDirect utility in HPA. IBM ThinkPad and LG notebooks hide system restore software in HPA.

- HPA is also used by various theft recovery and monitoring service vendors. For example, the laptop security firm Computrace use the HPA to load software that reports to their servers whenever the machine is booted on a network. HPA is useful to them because even when a stolen laptop has its hard drive formatted the HPA remains untouched.
- HPA can also be used to store data that is deemed illegal and is thus of interest to government and police
- Some vendor-specific external drive enclosures (Maxtor) are known to use HPA to limit the capacity of unknown replacement hard drives installed into the enclosure. When this occurs, the drive may appear to be limited in size (e.g. 128 GB), which can look like a BIOS or dynamic drive overlay (DDO) problem. In this case, one must use software utilities (see below) that use READ NATIVE MAX ADDRESS and SET MAX ADDRESS to change the drive's reported size back to its native size, and avoid using the external enclosure again with the affected drive.
- Some rootkits hide in the HPA to avoid being detected by anti-rootkit and antivirus software.
- Some NSA exploits use the HPA for application persistence.

DCO - Device configuration overlay

Device configuration overlay (DCO) is a hidden area on many of today's hard disk drives (HDDs). Usually when information is stored in either the DCO or host protected area (HPA), it is not accessible by the BIOS, OS, or the user. However, certain tools can be used to modify the HPA or DCO. The system uses the IDENTIFY_DEVICE command to determine the supported features of a given hard drive, but the DCO can report to this command that supported features are nonexistent or that the drive is smaller than it actually is. To determine the actual size and features of a disk, the DEVICE_CONFIGURATION_IDENTIFY command is used, and the output of this command can be compared to the output of IDENTIFY_DEVICE to see if a DCO is present on a given hard drive. Most major tools will remove the DCO in order to fully image a hard drive, using the DEVICE_CONFIGURATION_RESET command. This permanently alters the disk, unlike with the (HPA), which can be temporarily removed for a power cycle.

Usage

The Device Configuration Overlay (DCO), which was first introduced in the ATA-6 standard, "allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. An example of this would be using DCO to make an 80-gigabyte HDD appear as a 60-gigabyte HDD to both the (OS) and the BIOS.... Given the potential to place data in these hidden areas, this is an area of concern for computer forensics investigators. An additional issue for forensic investigators is imaging the HDD that has the HPA and/or DCO on it. While certain vendors claim that their tools are able to both properly detect and image the HPA, they are either silent on the handling of the DCO or indicate that this is beyond the capabilities of their tool.