## Contents

**Legal Statement** ................................................................. 4

**Introduction** ............................................................................ 5
  - Advanced Data Recovery Systems .............................................. 5
  - Erasing Confidential Data ......................................................... 5
  - International Standards in Data Destruction ............................... 6

**KillDisk Overview** ............................................................... 7
  - Software Licensing ................................................................. 8
  - Software Updates ................................................................. 8
  - System Requirements ............................................................ 9
  - Security Hardware ............................................................... 9
  - New in version 2.0 ............................................................... 10

**Getting Started with KillDisk** .............................................. 14
  - KillDisk Installation and Distribution ......................................... 14
  - Launching and initial Configuration .......................................... 14
  - Navigating Killdisk .............................................................. 15
  - Disk Layout Overview .......................................................... 16
    - Create a new Disk Bay Layout ............................................. 17
    - Export and Import of Disk Bay Layouts ................................. 20
    - Formatting Disk Bay Layout ................................................ 21
    - Layouts Advanced Features ................................................. 21
  - Disk Explorer ........................................................................ 23
    - Disk Bays View .............................................................. 23
    - My Computer View .......................................................... 24
    - Local Devices View ......................................................... 25

**Using KillDisk** ...................................................................... 27
  - Disk Erase ........................................................................... 27
  - Disk Wipe ............................................................................ 31
  - Examine Disk Physical Integrity ............................................. 32
  - Disk Cloning ....................................................................... 34
    - Mount Disk Image .......................................................... 35
  - Processing Summary .......................................................... 35
  - Certificates, Labels and Reports ............................................ 36
    - Erase Certificates ........................................................... 37
    - Erase Reports ................................................................. 39
    - Erase Labels .................................................................... 40
  - Additional Options and Features ........................................... 44
    - Mapping Network Shares .................................................. 44
    - Changing Disk Serial Number ............................................ 44
    - Reset Hidden Areas .......................................................... 45
    - Property Views ............................................................... 46
    - Dynamic Disks: LDM, LVM and WSS ................................. 48
Copyright © 2018, LSOFT TECHNOLOGIES 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 LSOFT TECHNOLOGIES INC.

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

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

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

Active@ KillDisk, the Active@ KillDisk logo, KillDisk, KillDisk for Industrial Systems, KillDisk Desktop and Erasers Software are trademarks of LSOFT TECHNOLOGIES INC.

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

Other brand and product names may be registered trademarks or trademarks of their respective holders.
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 74 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 74 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.

**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 for Industrial Systems

This edition of KillDisk is designed to provide a software solution for industrial workstations, configured to service disks in high volumes. KillDisk for Industrial Systems is distributed as a software package that may be installed on a disk erase workstation and used to examine, erase and even write images to individual or batches of disks. Highly customizable, the software is able to conform to any company standards - erasure standards, examination type, reporting, error handling are only a subset of the configurable settings KillDisk supports. All elements of KillDisk's operations may be documented in XML reports, PDF certificates, or even printable labels for erased hard drives. Versatile, easy to navigate and rich in features, KillDisk for Industrial Systems is the ideal KillDisk solution for recyclers and corporations to securely erase hard drives - simply and efficiently.

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

• Erase data on the entire hard disk drive surface, supports parallel erasing of large numbers of disks (hardware-limited);
• Destroy data permanently with a choice of dozens of international disk sanitizing standards, including DoD 5220.22-M;
• Sanitize external disks (USB drives, external HDD/SSD) connected to both USB 2.0 and 3.0 ports;
• Examine disk integrity and overall stability, disk verification and detect bad sectors;
• Auto-erase mode sanitizes disks and prints certificates without of any user interaction;
• Hot-swap operations are fully supported, erase could be auto-initiated upon HDD plug-in;
• Browse file systems on disk volumes and inspect particular sectors Hex Viewer on a low level;
• Issue customizable certificates and detailed reports for disk erase and examination;
• Print different types of labels to be attached to hard disks after erase completion;
• Provides enhanced information about disks and their attributes including S.M.A.R.T. Monitoring;
• Export local erase history to the external databases;
• Wipe out unused clusters and metadata on live volumes, leaving existing data intact;
• and more...

KillDisk maintains the highest standards in disk erasure, and with that, provides extensive documentation options for its' operations through Reports and printable Erase Certificates on page 37 and Erase Labels on page 40.
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.

KillDisk Industrial is supplied with a security USB key that contains number of licenses being purchased (one license is required per slot where HDD/SSD is plugged into).

![Security USB key containing licenses](image1.png)

**Figure 1: Security USB key containing licenses**

This key must be inserted into any USB slot on the PC before running KillDisk software, otherwise authorization error appears.

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**.

![Check for updates](image2.png)

**Figure 2: 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.

### System Requirements

KillDisk Industrial is design to run on Linux and Windows operating systems with the following minimum requirements:

**Workstation:**
- IBM PC compatible machine
- Intel Pentium or higher
- 2 Gb of RAM
- 100Mb of free disk space

**Video:**
- VGA (1024x768) resolution or better

**Operating System:**
- Windows XP or higher
- Linux Kernel 2.x or higher

**Drive Storage:**
- Disk types supported:
  - IDE
  - ATA
  - SSD
  - SATA
  - eSATA
  - SCSI
  - Removable media (memory stick, SD card, compact flash...)
- KillDisk Industrial supports all drives supported by the Operating System with read/write access

### Security Hardware

KillDisk authorization is provided by an external or internal removable USB key with license and user information. This USB key must be inserted all the times to make KillDisk software operable.
New in version 2.0

New functionality: Wipe

Now, KillDisk Industrial has the ability to sanitize free space on the hard drive with **Wipe**, leaving existing files intact. Careful not to confuse it with **Erase** which erases everything!

Advanced views

- Added an ability to toggle a view with complete partition information of your connected disks in the **Disk Explorer View**
• Revamped the local disks view to show more details, including partition information for all connected disks:

![Disk View](image1)

• ...and a new work flow view for managing your disk processes efficiently:

![Workflow View](image2)

**Erase History, Database Integrations and Email Notifications**

KillDisk Industrial version 2.0 adds a number of features to simplify auditing and management pains, with the addition of:

• The **Erase History** menu, allowing users to see the history of operations, with easy access to certificates from within the KillDisk application interface:
• ...these reports can now easily be connected and exported into your SQL database!

• Email Notifications for network-connected devices, allowing all certificates/reports/logs to be emailed to a central repository for record-keeping. All you need to do is put in your email address:
Disk Performance Monitoring

• Monitor SMART information throughout the erase operation and set thresholds to eject under-performing drives:

• Set minimum disk Read/Write speed for drives to be evaluated during erase

Batches, redesigned

• New wizard for creating batches
• Batches can be designated for Erase, Wipe, Examination and Clone with common parameters:
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 Industrial distribution overview

KillDisk Industrial is distributed as a software solution, with a DVD-ROM and security USB license. DVD-ROM contains two installations:

- KillDiskIndustrial-Setup.exe - installation for Windows OS
- KillDiskIndustrial.run - installation for the Linux OS

Simply install the application into your data erasure workstation environment and configure it to your system.

Launching and initial Configuration

Note: Before launching KillDisk make sure that security USB stick is plugged into the any USB slot on a workstation running the software.

Upon first launching the application you will encounter the Disk Bay Layout Wizard.

![Figure 4: Disk Bay Layout Wizard](image)

This menu allows you to initialize KillDisk to display your hardware in an intuitive way. To illustrate the purpose of this, read this section on Disk Bay Layouts. This initial configuration can be done in one of three ways:

Load predefined layout

Here you can find one of our predefined layouts that may fit your system. If an appropriate layout is not listed, you may try the next option.
Generate default disk bay layout
Define your systems in terms of a disk array, arranged in a X by Y grid of disks. You may make adjustments to this later, so this may just be a base to start from.

Automatically generate disk bays for all discovered disks
Defines your Disk bay layout based on the disks recognized by your system's device manager. The disks will be placed in their own individual row when the layout is generated.

Create empty layout for manual editing
Defines a blank layout with no disks, so they can be added in the Disk Bay Layout window later.

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 with 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:

- **File menu bar**: The file menu bar contains can be manipulated to perform nearly any operation in KillDisk, such as accessing elements of the program such a settings and help, changing views and what is visible in the dashboard, opening tools, and navigating between KillDisk's windows.

- **Tabbed Windows**: Here, you may move between KillDisk tabbed windows, the main windows being Disk Explorer, Application Log etc..

- **Command Toolbar**: The command toolbar is a dynamic toolbar that allows the user to perform Tabbed Window-specific actions, depending on what window the user is in and what element is selected.
View Selection

Only available in the Disk Explorer View, this View Selection allows you to manipulate how the bays are displayed in the Windowed View, manipulating the type of graphics used to show the bays and the cardinality of the bays in the Disk Bay View.

Windowed view

Contains the window that is currently open.

Output window

Contains the log of operations KillDisk has performed.

Batch control window

The Batch control window is an easily accessible interface to create, delete and manipulate disk batches.

Advanced tool tabs

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

Advanced tool window

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

The purpose of Disk Bay Layouts is to match KillDisk's graphical representation of your disk configuration to your physical hardware configuration, making it easy to manage your disks for Erasure, Examination, Cloning and more. To illustrate this, let's look at an example, using the hardware below:

Figure 6: Example of a generic disk array

In the above example, we have a generic disk array consisting of 16 disks, arranged in a 4x4 grid. The machine using these disks would see the disks similarly to KillDisk's Local Devices view, as depicted in the Figure below:
Now imagine inserting a Hard Disk Drive into the bottom-leftmost bay of the disk array and wanting to perform an operation on it. Even finding the device in a list of 15 other disks would be tedious and not very intuitive. This is where creating a Disk Bay Layout is extremely useful. By creating a 4x4 Disk Bay Layout, we can map the physical ports to their corresponding Bay in KillDisk and visually see our disk array like this:

Assuming that the bays were mapped correctly, finding the correct disk to manipulate now much easier in the Disk Bays view than it would have been in a list view. You can now select the bottom-leftmost disk in the Disk Bays view and perform any necessary actions on it.

Create a new Disk Bay Layout

In the KillDisk toolbar, select Tools > Disk Layout Editor, or shortcut CTRL + M.

Figure 7: Local Devices view

Figure 8: Disk Bays view

Figure 9: Opening the Disk bays layout tab
This will bring you to the **Disk Bays Layout** tab, where you can manipulate, save, import and create Disk Bay Layouts.

**Figure 10: Opening the Disk Bays Layout tab**

Here we are looking to create a new layout, so get rid of the current layout shown by clicking **Layout > New Layout Wizard**.

**Figure 11: Creating a new layout**

This will launch the **Disk Bay Layout Wizard**
This configuration of a new layout can be done in one of three ways:

**Load predefined layout**
Here you can find one of our predefined layouts that may fit your system. If an appropriate layout is not listed, you may try the next option.

**Generate default disk bay layout**
Define your systems in terms of a disk array, arranged in a X by Y grid of disks. You may make adjustments to this later, so this may just be a base to start from.

**Automatically generate disk bays for all discovered disks**
Defines your Disk bay layout based on the disks recognized by your system's device manager. The disks will be placed in their own individual row when the layout is generated.

**Create empty layout for manual editing**
Defines a blank layout with no disks, so they can be added in the Disk Bay Layout window later.

**Warning:** Make sure to save the old layout by selecting Layout > Save Layout before creating the new layout, or your old layout WILL be lost.

With the old layout cleared out, you now have a new layout ready to be configured to your machine.

### Adding and Deleting Rows and/or Bays
Disk bay layout consist of disk bays grouped by row to maximize mocking effect of an actual disk bay mounted in hardware unit. To design bay layout, simply use the Add Row or Add Bay buttons to create additional rows/bays to work with. When a bay is selected, the Delete Bay button can be used to delete the individual bay. When a row is selected, the Delete Row button will delete the row and all the bays contained within it.

### Map disk bays to physical drives
In Disk Layout Editor you can map actual physical bay to its GUI representation (disk bay widgets) in two ways:
- Assign platform name to disk bay widget
- Assign disk port of physical disk controller to disk bay widget
- Assign a bay to a particular batch
Important: Due to different hard disk controller manufacture standards and platform limitations, physical disk port address format may vary.

Note: If both, platform name and disk port, are assigned to disk bay widget then platform name is used for disk bay mapping.

To make and assignment, double click in either Platform Name, Port (BUS) key or Used in batch column in correspondent disk bay line to initiate editing. Enter platform name as text or disk port as masked text. You can use drop down list of all detected physical disk controller ports for immediate port assignment.

You can also edit disk port in disk bay widget from main view by using context menu of disk bay widget.

Saving and Reverting changes

Use the Save Layout button to commit any changes to the layout to the application views.

Note: Save Layout will apply current change to the KillDisk session so the changes will be seen in the Disk Bays explorer views and even be loaded in upon future application launch. These changes will not affect the .dbl file, however, so be sure to commit any important changes using the Save Layout command.

Click Layout > Revert Layout to revert any changes you made to the layout.

Export and Import of Disk Bay Layouts

Once a disk bay layout is configured, it can be saved and later used with other KillDisk configurations. This is done with the Export and Import features.

Exporting a Disk Bay Layout

Layouts are saved using the disk bay layout command tool bar's commands. Select Layout, then Export Layout as... in the drop down list of commands. This will open a dialogue where the layout can be configured by setting the Title, description, file name and path to save the layout to. Once these settings are configured, click Save and the layout will be saved as a .dbl file in the specified location.

Figure 13: Export disk bay layout dialog

Title

Enter any label to distinguish newly created disk bay layout to differentiate it among other disk bay layouts.

Description

Describe any specifications, features or particularities of the new disk bay layout.

Layout profile name

Select the name of the file that the disk bay layout will be saved as. File extension should remain as .dbl.
**Importing a Disk Bay Layout**

Saved disk bay layouts are imported into separate KillDisk sessions using the import feature. In the command toolbar, select **Layout** and **Import Layout**. Select the desired disk bay layout (.dbl file) in the file explorer window and click **Open**.

This will import the disk bay layout into the current KillDisk session. Finally, click **Save layout** to update the disks in the **Disk Explorer** and the import should be complete.

**Formatting Disk Bay Layout**

Once a disk bay layout is created, there are a number of actions that can be performed to format or manipulate the layout and appearance of the disks in the KillDisk application.

**Naming Disk Bays**

To make disk bay widgets easier to navigate, they can be renamed by simply double-clicking on the existing bay label and typing in a new name, shown in the Figure below:

![Figure 14: Renaming bays](image)

**Changing Row and Bay positioning**

Configured bay widgets may be moved around to accommodate changes in physical configuration or fix mistakes in creating the layout. This is done quite simply by selecting the bay that needs to be moved, and clicking the **Move Bay Up** and **Move Bay Down** buttons. Similarly, bay rows can be manipulated by selecting the row in question and pressing the **Move Row Up** and **Move Row Down** buttons.

**Adding more Rows and Bays**

Click the **Add/Insert Row** or **Add/Insert Bay** toolbar buttons to add row or bay at current position.

**Deleting Rows and Bays**

Click the **Delete Row** or **Delete Bay** toolbar buttons to remove row or bay at current position.

**Saving and Reverting changes**

Use the **Save Layout** button to commit any changes to the layout to the application views.

**Note:** **Save Layout** will apply current change to the KillDisk session so the changes will be seen in the Disk Bays explorer views and even be loaded in upon future application launch. These changes will not affect the .dbl file, however, so be sure to commit any important changes using the **Save Layout command**.

Click **Layout > Revert Layout** to revert any changes you made to the layout.

**Layouts Advanced Features**

Once a disk bay layout is created, there are a number of actions that can be performed to format or manipulate the layout and appearance of the disks in the KillDisk application.

**Locking Disks**

In order to prevent accidental deletion of important disks, KillDisk supports locking of disks. Once a disk is locked, no write operations are allowed to be performed on the drive. To do this, simply find the disk that needs to be locked and execute **Lock** menu command from the **Edit** menu.
Figure 15: Locking a disk to prevent accidental destruction

**Locking Clone Source**

Disks that are planned to be used as master copy for *Disk Cloning* on page 34 could be marked in disk bay layout by selecting disk bay and clicking *Clone Source* from the *Edit* menu. Thus disks marked this way will be protected from accidental destruction and also will be available in list devices as source for disk cloning.

**Auto Erase**

*Auto Erase* feature designed to speed up disk wiping process in scenario when many disks must be erased with the same erase attributes with less user interaction. When disk is inserted in a bay marked as Auto Erase then disk erase procedure will start without any introduction or confirmation dialogs. However you will see 30 seconds countdown started on disk bay about to be erased and may cancel this action by selecting disk bay widget and clicking *Stop* button in view's toolbar or in context menu.

Figure 16: Enabling Auto Erase

**Caution:** Use this feature with extreme caution — be sure that inserted disk is intended to be erased and appeared in a right bay. You will have 30 seconds to abort disk erasure.

**Saving and Reverting changes**

Use the *Save Layout* button to commit any changes to the layout to the application views.
Note: *Save Layout* will apply current change to the KillDisk session so the changes will be seen in the Disk Bays explorer views and even be loaded in upon future application launch. These changes will not affect the .dbl file, however, so be sure to commit any important changes using the *Save Layout command*.

Click *Layout > Revert Layout* to revert any changes you made to the layout.

## Disk Explorer

The **Disk Explorer** is the main interface for the KillDisk application. Here, disks are visualized, can be selected and manipulated. The status of any procedures performed on the disks can be seen here, new procedures like erasure can be initiated.

![Disk Explorer](image)

**Figure 17: Disk Explorer**

Supplementary toolbar helps to execute frequently performed tasks. It contains the following buttons with drop-down menus:

**View**

The disk explorer supports a range of different views to use when performing KillDisk's actions, each with their own customizable settings for different use cases.

**Customize**

These settings let you customize appearance for better experience for each view. Disk bay positioning and the type of information displayed, such as partition view, can be toggled here.

### Disk Bays View

This view visually displays the disks configured in the **Disk Layout Editor**. The bays are grouped by their row, colored by the batch color, and show the current status of the disk. If any operations are being performed on the disk, the operation and progress are displayed.
Figure 18: Disk Bays view

Customize menu

Show partitions
Show or hide additional layout for partitions and volumes.

Show removable devices
Show or hide additional layout row for removable devices.

Rows as Columns
This setting can be toggled on/off to display the rows (defined by the disk bay layout) as columns in the Disk Bays view.

Vertical Bays
This setting can also be toggled to change the orientation of the bays from horizontal to vertical and backward.

Show Disk Bays in Tree View
Switches Disk Bays view to tree view related to the one configured in Disk Layout Editor.

Disk Layout Editor
Opens Disk Layout Editor in a separate tab for current layout customization or creating a new layout.

My Computer View

The My Computer view presents the disk bay layout in a standard list form, much like the disks would be shown in an explorer. Disk bays are grouped by row and can be colored according to their batch color. Information such as disk status, serial number, partitioning are shown in list form next to their respective disk bays. Properties window at the right side displays attributes of the currently selected object.
Figure 19: My Computer View

Customize menu

Show My Computer

Displays all devices that are detected by the system device manager.

Show System Disk

Displays the disk containing the Operating System. This is 'off' by default to prevent accidental erasure of the system.

Show Unallocated Partitions

Displays partitions that may not yet be formatted.

Show Devices

Switches between display of devices (physical disks containing volumes) and just volumes display.

Show Removable Disks

Displays removable media storage (USB Flash Disk, External USB,...).

Show Not Ready Devices

Displays devices that may not yet be initialized and accessible by the OS.

Navigator Pane

Toggle Navigator Pane (are on the left hand side of device view)

Local Devices View

Local Devices view shows all disks recognized by the system and available for application in a list view:
Figure 20: Local Devices View

Customize menu

Show System Devices
Displays the disk where Operating System installed.

Show Not Ready Devices
Displays devices not yet initialized and usable by the OS.

Show Removable Devices
Displays all removable disks, such as USB's and externally connected disks.

Compact View
Cleans up the disk view by hiding all partition information and only displaying key points of information about the disks.
Using KillDisk

KillDisk Industrial is a powerful industrial tool to provide disk erasure solutions for large workstations with many disks. The features in the KillDisk Industrial software are built with this goal in mind. This section outlines the key features of KillDisk and how they are used to erase single disks to large batches. 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.

Note:

It is important to properly set up your KillDisk layout before using any of the features, so read and follow the steps to do this in the Disk Layout Editor section, if you have not already.

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 23 to select disk bays.

2. Open Erase disks dialog 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
   - Click Run Batch > Named batch command from toolbar or from Actions main menu to erase disks in predefined disk batch.

   ![Figure 21: Initiating the Erase operation](image)

3. Confirm erasure options

   Disk Erase options dialog pops up:
Figure 22: Disk Erase Options

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

- **Disk Examination Options** on page 54 [optional in Industrial & Desktop only]
- **Disk Erase Options** on page 52
- **Certificate Options** on page 56
- **Report Options** on page 58
- **Email Notification Options** on page 65
- **Labels Options** on page 60
- **Error Handling Options** on page 63

Use **Disk Examination Options** on page 54 page in application preferences to specify disk grading attributes if necessary.

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

![Erase Disk - Area Selection](image)

**Figure 23: 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:

![Confirm action (as superuser)](image)

**Figure 24: Disk Erase Confirmation**

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

4. **Observe erase process**

   If **Disk Examination Options** on page 54 was selected then disk examination will started first. Depending on examination outcome at second stage - disk erase begins.

   Once the Erase procedure begins, you will see the disk bay represented 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:

![Erase progress](image)

**Figure 25: Disk Erase Progress**
If Disk Clone Options on page 56 was selected then after erase the final stage of this task begins - clone data from source to all successfully erased disks.

When erasing completes you can review results and print an Erase Certificates on page 37 and Erase Labels on page 40 for processed disks.
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 27.

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** button is disabled. If you select a device and the **Wipe** button is disabled, select individual partitions (drives) and wipe them separately.

1. Switch to **Local Devices** view
2. Select the device or a volume to wipe in the disk explorer view. You may select multiple devices/volumes to be wiped out simultaneously
3. 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, or use the context menu

![Figure 29: Initiating the Wipe operation](image)

4. Confirm Wipe options
   Use tabbed views to adjust disk wipe options if necessary. Available options:
   - **Examine Disk Physical Integrity** on page 32
   - **Disk Wipe Options** on page 53
   - **Certificate Options** on page 56
   - **Email Notification Options** on page 65
   - **Labels Options** on page 60
   - **Error Handling Options** on page 63
   - **Report Options** on page 58
Figure 30: Selecting an an erase algorithm for the wipe

5. Select the areas of the disks to be wiped. With individual disks you may select individual partitions.

6. Click **Start** to advance to the final step before erasing data. 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 37

   **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.

---

**Examine Disk Physical Integrity**

The disk examination feature is designed to scan the physical integrity of the disks selected for this operation. **Disk Examine step** can be the preliminary step to **Disk Erase**, **Disk Wipe** and **Disk Clone** procedures.

To examine disks:

1. Select disks or volumes for examination

   Use **Disk Explorer** on page 23 to select one or more physical disks or logical volumes.

2. Open **Examine Disk** configuration dialog using one of the following:

   • Click the **Examine Disk** command in the action toolbar
   • Click **Actions > Examine Disk** command from main menu
- Click **Examine Disk** command from context menu
- Click **Run Bach > Named batch** command from toolbar or from **Actions** main menu to examine disks in predefined disk batch.

**Figure 31: Examine Disk Options**

3. Confirm examination options

   Use tabbed views to adjust examination options if necessary. Available options:
   - **Disk Examination Options** on page 54
   - **Error Handling Options** on page 63
   - **Report Options** on page 58

   Use **Disk Examination Options** on page 54 in application preferences to specify disk grading attributes if necessary.

   **Note:**

   If only one disk was selected for examination than you can specify boundaries of examined area for selected disk.

   Click **Start** button to begin examination process.

4. Observe examination process

   In the **Disk Explorer** on page 23, you will see the progress of the examination in the slot of the drive being operated on. The progress will be shown as a progress bar, seen below:
Figure 32: Disk examination progress

As seen in the image above, the green progress bar will fill the virtual drive slot in the KillDisk application. The percentage of the examination completed and the estimated completion time will also be shown in the slot. Once this process completes, the word **EXAMINED** will flash in the slot space.

When erasing completes you can review results for the processed disks.

**Disk Cloning**

In addition to securely erasing hard drives, KillDisk also allows you to write an image or copy a Master Disk to newly erased hard drives with its' cloning feature.

To clone a disk or image to a disk after the erase procedure is completed, navigate to the **Disk Clone** tab when you edit existing or create a new **Batch**, and check the **Use Disk Clone** box, as shown below.

An existing disk image, or physical hard drive can be used as the **Master Copy** to be cloned to the newly erased drive. For additional preferences and configuration see **Disk Clone Options** on page 55.
To configure a source image/disk for **Disk Clone** operation:

1. Navigate to the Disk Clone tab in the Batch settings, and check the Use Disk Clone checkbox
2. Select the disk image source from either image file or physical disk.
3. Specify which sector to start the copy to. If unsure, leave as '0'.

Disk cloning is now configured so that when an Erase operation has completed, the source image/disk will be cloned to the newly erased drive.

### Mount Disk Image

To use file as a source of write a physical copy of file contents to one or several disks

1. To open the Mount Disk Image dialog, do one of the following:

   ![Mount Disk Image dialog](image)

   **File name**
   
   Full path to the disk image file

   **Caption**
   
   Enter any label to distinguish newly opened (mounted) disk image among other devices and disks.

   **Figure 34: Mount Disk Image dialog**

2. Confirm and open disk image

   Click **OK** to mount a Disk Image.

If disk image opens successfully then disk image node appears in **Disk Explorer** view and will be available as clone source in **Disk Clone Options** on page 55 tab and in drop-down list of clone sources in task dialog.

### Processing Summary

Once **KillDisk**'s finishes processing any task, such as disk erasure or disk examination, 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.
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.

**Disk Examination Status**

Specifications of the examination procedure are listed and the status of the examination is reported.

**Disk Examination Report**

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

**Disk Grade Assignment Status**

Confirms the inclusion of the disk grade assignment operation, based on disk integrity examination results.

**Erasure Status**

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

**Disk Erasure 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 Erasure 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.

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 36: Disk Erase - Batch Certificate - First Page
For group operations like **Batches** KillDisk can create both Batch Summary certificate as well as particular certificates for each disk in the Batch.

**Figure 38: Disk Wipe Certificate**
### 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**, **Erasure** and **Wipe**. These reports contain all the information pertaining to the KillDisk procedure. The contents of the report are outlined below.

<table>
<thead>
<tr>
<th>Company Information</th>
<th>Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Name</td>
<td>- Device Size</td>
</tr>
<tr>
<td>- License</td>
<td>- Device Type</td>
</tr>
<tr>
<td>- Location</td>
<td>- Serial Number</td>
</tr>
<tr>
<td>- Phone</td>
<td>- Revision</td>
</tr>
<tr>
<td>- Disclaimer</td>
<td>- Product Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technician Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Name</td>
<td></td>
</tr>
<tr>
<td>- Comments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System &amp; Hardware Info</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- OS version</td>
<td></td>
</tr>
<tr>
<td>- Architecture</td>
<td></td>
</tr>
<tr>
<td>- Kernel</td>
<td></td>
</tr>
<tr>
<td>- Processors</td>
<td></td>
</tr>
<tr>
<td>- Manufacturer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Erase Attributes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Erase verify</td>
<td></td>
</tr>
<tr>
<td>- Passes</td>
<td></td>
</tr>
<tr>
<td>- Method</td>
<td></td>
</tr>
<tr>
<td>- Verification passes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Batches</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Name</td>
<td></td>
</tr>
<tr>
<td>- Disks</td>
<td></td>
</tr>
<tr>
<td>- Time</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Attributes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Fingerprint Information</td>
<td></td>
</tr>
<tr>
<td>- Initialization</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Erase Result</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Bay</td>
<td></td>
</tr>
<tr>
<td>- Time and Date Started</td>
<td></td>
</tr>
<tr>
<td>- Disk Information</td>
<td></td>
</tr>
</tbody>
</table>
Error Handling Attributes

- Errors terminate
- Skip interval
- Number of Retries
- Source Lock
- Ignore Write Error
- Ignore Read Error
- Ignore Lock Error

| 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. 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 39: 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 Label Preview window on the left side. The right side of the dialog has the styling and template configuration options.
Figure 40: Print Label Dialog

**Page template options**

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.

**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 41: Template Editor

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.

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

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.
**Label Style and options**

These options allow you to change the styling on the labels with the following options:

**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.

**Add signature line**
- Toggling this on places a line at the bottom of the label for the technician to sign off upon completion of the wipe.

**Add certificate logo**
- Includes the logo used in the certificate as a watermark background of the label.

**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.

![Print Preview](image)

*Figure 42: Example of a Print Preview*
Additional Options and Features

KillDisk also has a number of supporting 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

![Map Network Share](image)

Figure 43: 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

3. 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 in question and select Set Serial Number... in the context menu.
Figure 44: 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 45: Resetting Hidden Areas
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

Figure 46: 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.
Figure 47: 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
Figure 48: 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 49: Virtual drive being erased in conjunction with a Windows Storage Spaces striped array

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 File > Preferences... or
- Use F10 keyboard shortcut at any time

Preferences dialog could be open from other task dialogs to change related settings.
Preferences allow users to configure all the global settings for the application.

When **Wipe** or **Erase** are 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 controls disk bay layout behavior in main **Disk Explorer** on page 23

**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 KillDisk’s location directory.

**Application log detail**

Manipulate the amount of detail included in the logs. Values 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)

![Small icons no text](image1)

**Figure 51: Small icons no text**

![Large icons no text](image2)

**Figure 52: Large icons no text**

![Large icons with text](image3)

**Figure 53: 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.

**Use sound effects on errors and notifications**

Toggles sound tones being used for notifying the user of the completion of a task, errors and notification during an operation.
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, erase labels etc.

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

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

Any attached USB's will have the certificates and logs written to them upon completion

Disk Erase Options

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

The same erase options for each batch could be set through Edit Batch Attributes on page 71 dialog

Figure 54: Erase 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 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 after erase

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

Write fingerprint

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

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

![Sensitive action confirmation dialog](Figure 55: 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.

**Disk Examination Options**

KillDisk offers different **Disk Examination Options**, depending on user needs. Each examination type has its own strengths and weaknesses, mainly tradeoffs between time and thoroughness. Any of the examination types can be performed on an entire disk, or a selected segment.

Examination options are required for disk integrity examination and optional for disk erasure but can be used to sort away faulty disk from following processing in sequence.

To examine disk integrity the following three algorithms are used:

**Partial Examination**
Examines a percentage of the disk, equally segmented in a selected area

**Partial Random Examination**
Examines a set number of randomly distributed sections of the disk within the selected area

**Read Each Sector in Selected Area**
Examines the entirety of a selected area, set for examination. Because this reads every sector in the selected area, this is the most lengthy, but thorough of the disk examination procedures.

**Disk Grading**

Based on examination results disks could be "graded" depending on amount of failed sectors. Specific grade attributes can be set on **Disk Examination Grades** page of application preferences. Further **Disk Erase** command can be executed or canceled based on current disk's grade.

For each grade, you may select the Green, Yellow, or Red to represent the disk grade visually. Multiple grades may share the same color.

![Examine Disks (as superuser)](image)

**Figure 56: Disk Examination Grades**

**Limits for errors**

Defined under the second grade disks section, the maximum read errors settings allows the user to define the maximum read error tolerance before a disk is categorized as a third grade disk. Third grade disks are the worst grade level, and are considered unreliable for use.
Exclude unstable disks from further processing

If this option is turned on, all disks having any type of errors will be automatically excluded from further batch operations.

**Disk Clone Options**

This preferences tab allows you to select a master-copy disk to use for cloning on other disks after they have been erased.

![Disk Clone Options](image)

**Figure 57: Disk Clone Options**

### Selecting a Disk for cloning

Any disk recognized by KillDisk may be used as a master-copy for Cloning. Simply find the disk under the "Available Disks" column and check the box next to the desired Disk Bay. This disk will be locked and read/write operations will be restricted from the disk until the cloning operation is complete.

### Selecting a Disk Image for cloning

Additionally to cloning from a disk, cloning can be done from a mounted disk image. This is done using the following procedure in the Disk Clone preferences tab:

1. At the bottom of the dialog, click **Mount Disk Image**
2. To the right of the "Disk Image file name field" click the ... button
3. Find the desired disk image in the file explorer and click **Open**.
4. Fill in the "Display name" text box with a desired name for the image and click **OK**.
5. The mounted disk image should appear under "Disk Images" in the Master-copy sources window. Check the box next to it and

   **Note:** To avoid repeating steps 1-4 above every time the application is launched, check the "Autoload mounted Disk Images at every application start" box. This will complete the mounting process automatically in the future.

   **Note:** Cloning is only available as an operation when working with a Batch of disks, as an option after erasure.

**Disk Clone Options**

   **Note:** This feature is only available when working with a Disk Batch, after an erase. Operations on single disks will not be able to use these option.

**Copy disk image**

When selected, this enables the copy feature. This will copy a disk image from a selected source to all disks that were erased in the batch.

**Use file image**

Allows you to specify a disk image file to write to the other disks.

**Use physical disk**

Allows you to specify one disk from the batch to act as the "master disk". This disk will not be erased, but rather be cloned to the other disks in the batch after they are erased.

**Start copy to sector**

You can specify which sector the copy starts from on the source disks. If you don't know what this is for, leave as 0.

**Certificate Options**

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

![Certificate Options](image)

**Figure 58: 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

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

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:**

<table>
<thead>
<tr>
<th>Available file name element:</th>
<th>Tag:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial ID</td>
<td>{Serial ID}</td>
</tr>
<tr>
<td>Erasure Status</td>
<td>{Status}</td>
</tr>
<tr>
<td>Date of Erasure</td>
<td>{Date(YYYY-MM-DD)}</td>
</tr>
<tr>
<td>Time of Erasure</td>
<td>{Time(HH-mm-ss)}</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Specific data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company Information</strong></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>License</td>
</tr>
<tr>
<td></td>
<td>Location</td>
</tr>
<tr>
<td></td>
<td>Phone</td>
</tr>
<tr>
<td></td>
<td>Disclaimer</td>
</tr>
<tr>
<td><strong>Technician Information</strong></td>
<td>Operator Name</td>
</tr>
<tr>
<td>Type of Information</td>
<td>Specific data</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>Comments</td>
</tr>
<tr>
<td>System Information</td>
<td>OS version</td>
</tr>
<tr>
<td></td>
<td>Platform</td>
</tr>
<tr>
<td></td>
<td>Kernel</td>
</tr>
<tr>
<td>Hardware Information</td>
<td>Motherboard Manufacturer</td>
</tr>
<tr>
<td></td>
<td>Motherboard Description</td>
</tr>
<tr>
<td></td>
<td>Number of Processors</td>
</tr>
<tr>
<td>Erase Attributes</td>
<td>Erase Verify</td>
</tr>
<tr>
<td></td>
<td>Passes</td>
</tr>
<tr>
<td></td>
<td>Method</td>
</tr>
<tr>
<td></td>
<td>Verification Passes</td>
</tr>
<tr>
<td>Error Handling Attributes</td>
<td>Errors Terminate</td>
</tr>
<tr>
<td></td>
<td>Skip interval</td>
</tr>
<tr>
<td></td>
<td>Number of Retries</td>
</tr>
<tr>
<td></td>
<td>Lock</td>
</tr>
<tr>
<td></td>
<td>Source?</td>
</tr>
<tr>
<td></td>
<td>Ignore Write?</td>
</tr>
<tr>
<td></td>
<td>Read?</td>
</tr>
<tr>
<td></td>
<td>Lock?</td>
</tr>
<tr>
<td>Disks</td>
<td>Device Size</td>
</tr>
<tr>
<td></td>
<td>Device Type</td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
</tr>
<tr>
<td></td>
<td>Revision</td>
</tr>
<tr>
<td></td>
<td>Product Number</td>
</tr>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Geometric Information</td>
</tr>
<tr>
<td></td>
<td>Partitioning Scheme</td>
</tr>
<tr>
<td>Additional Report Attributes</td>
<td>Fingerprint Information</td>
</tr>
<tr>
<td></td>
<td>Initialize disk?</td>
</tr>
<tr>
<td>Result</td>
<td>Bay</td>
</tr>
<tr>
<td></td>
<td>Time and Date Started</td>
</tr>
<tr>
<td></td>
<td>Disk Information</td>
</tr>
<tr>
<td></td>
<td>Status</td>
</tr>
<tr>
<td></td>
<td>Result</td>
</tr>
<tr>
<td>Type of Information</td>
<td>Specific data</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Time Elapsed</td>
<td></td>
</tr>
<tr>
<td>Errors</td>
<td></td>
</tr>
<tr>
<td>Name of operation</td>
<td></td>
</tr>
</tbody>
</table>

**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 59: Label Options**

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

**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.
Creating a new template

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

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 in entered in one measurement and the unit size is changed, the appropriate conversion will take place.

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.

Label Style and options
These option allow you to change the styling on the labels with the following options:

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

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

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

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.
Database Export Options

KillDisk Industrial's Export feature allows to send out all current logs, certificates and reports from locally stored database over the network to the external SQL database. Both local Erase History and all future transactions can be exported after connection to database is established.

Connection to SQL Databases supported:

- Microsoft SQL Server
- ORACLE
- PostgreSQL
- MySQL

To connect to the external SQL database do one of:

1. Navigate to File > Preferences or press F10. Then click Database Export tab on the left
2. Database Export dialog appears:

![Database Export Dialog](image)

**Figure 60: Database Export Dialog**

3. Select Driver for the particular database you want to connect to from the list of databases
4. Type in the Database Name on the remote end
5. Type in the database Username for the connection
6. Type in the database password for the selected user
7. Type in the Hostname (which can be IP address or local Network Server Name)
8. Select a TCP/IP Port to use, if it is different from the default value for the particular database
9. Set check marks, if needed, for the additional export options:
   - Export certificates and reports for batches
   - Export certificates and reports for particular disks
   - Export existing erase history (can be done the only once per a new connection)
10. Click **OK** to test connection and store connection parameters in settings for future use

Once a connection to the external SQL database established, KillDisk Industrial starts exporting all information related to the current operations automatically.

**Note:**

For the database export to be successful you need to provide a database user with privileges enough for creation two tables (**DISKS** and **BATCHES**) and populating these tables with current operation's parameters.

### Disk Viewer Options

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

![Disk Viewer Options](image)

**Figure 61: 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 62: 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.

**Rely upon disk performance**
- Set a minimum acceptable read/write speed in megabytes per second for disks to flag underperforming drives.
SMART Diagnostics

SMART attributes may also be used in error handling, so threshold limits may be set on some or all of the disks SMART parameters. This may speed up processing by immediately terminating operations with unusable drives.

Note: Query execution for SMART attributes is very time and resource consuming operation. It can pause disk erasure procedure for several seconds. Thus it is recommended to validate these attributes not very frequently.

Email Notification Options

Email Notifications

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

![Figure 65: SMTP Settings](image)

**Account Type**

*KillDisk* offers you a free SMTP account located on [www.smtp-server.com](http://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.
Disk Batches

Disk Batches are used to organize disks into groups, depending on what the disks are being used for, type of disk, or the desired operation to be performed on them: Examine, Erase, Wipe, Clone and combinations. The user has complete freedom to use disk batches however is most convenient for their particular use case. Disks can be added or removed from a particular batch at any time.

Figure 66: Disk Batches distinguished by color

Once disks are batched together, they may be treated as a group and similar settings may be set for this batch. Likewise, operations may be performed on these batches — initiating the operation on a batch will perform the operation on all the disks belonging to the batch.

Create Batches

Create a Disk Batch

Disk batches are created using the Batch Control toolbox.

Note:

If you can't find the Batch Control toolbox when you run KillDisk, make sure that you have the view activated. To do this, navigate to the file menu bar, click View > Windows > Batch Control There should be a check mark next to the Batch Control view.

In the Batch Control toolbox, click New batch. This will open the Create a New Batch configuration wizard. After configuring batch settings, click Finish and the new batch will appear in the batch control window.
Adding disks to a disk batch

Disk bays can be added to batches in several ways:

- From Disk Bays view
- From Edit menu

Read *Add Disks to Batches* for more information.

Removing disks from a disk batch

Disks are removed from a batch in a very similar way to the way they are attached. Follow the same steps as with Adding Disks, only select bays that are attached to batches and select the Detach command.

Deleting batches

Batches can be deleted by selecting the batch in the Batch Control toolbar and selecting the Delete command.

Edit batch attributes

Batch attributes can be edited at any time after batch created. See: *Edit Batch Attributes* on page 71

Note:

Disk batch attributes changed every time if altered in confirmation dialog before executed.

Add Disk Bays to Batches

Disk Bays can be assigned to existing disk batches in order to apply same batch attributes for selected tasks (disk examination, erasure, etc).

Note:

Single disk bay can only belong to the one batch.

Once a new batch is created, a new message will appear at the top of the Disk Bays view of the Disk Explorer window, prompting you to add disks to the new batch.
Click on disks to select them and/or click on selected disk to remove them from the batch disk selection. Once the desired disks are selected, click **Done** in the message toolbar and the selected disks will be added to the new batch.

Alternatively, disks can be added to a batch in one of several ways:

**From Disk Bays view**

1. In the disk bays view, select the disk(s) that you'd like to place in a batch.
2. Right-click on the disk.
3. Hover over the **Assign bays to** option to see a list of available batches.
4. Select the desired batch from the list to place the selected disk into.
From Edit menu

Figure 70: Assign Disk through the Edit menu bar

1. In the Disk Explorer, select the disk bay(s) that needs to be assigned
2. Click Edit menu bar
3. Hover over the Assign bays to action to see a complete list of available batches
4. Click on the desired batch. The selected bay(s) will be assigned to that batch.

Edit Batch Attributes

When you create a new disk batch, you will encounter the Edit Batch window, where disk batch settings may be set. For existing disk batches, you may access this window by selecting the desired batch in the Batch Control toolbox and clicking Edit Batch toolbar button.

Batch Attributes

These are General Settings for the batch, such as Title, Color, how the batch is displayed, and more.
Figure 71: Batch Editor - General Settings

**Disk Examination**
These settings allow you to configure the optional Disk Examination feature, toggling it on/off, method of examination, setting disk integrity thresholds and how these reports are saved.

Read *Disk Examination Options* on page 54 for description of each attribute.

**Disk Erase**
These settings configure the disk erase settings for the batch. Erase methods, verification, and report settings can be changed here. Additional options can be individually configured here by clicking *Show Advanced* button.

Read *Disk Erase Options* on page 52 for description of each attribute.

**Disk Wipe**
These settings configure the disk wipe settings for the batch. Erase methods, verification, and report settings can be changed here.

Read *Disk Wipe Options* on page 53 for description of each attribute.

**Disk Clone**
This feature allows the user to configure either a disk or disk image to write to all the disks in the batch.

Read *Disk Clone Options* on page 55 for description of each attribute.

**Batch Certificate**
These settings give you the option to toggle whether or not to issue an erasure certificate upon erase and configure the options to include, like name, destination, details and comments. Options for printing and issuing individual certificates for the particular disk in the batch can be configured.

Read *Certificate Options* on page 56 for description of each attribute.
Batch Report
These settings give you the option to toggle whether or not to issue an erasure XML report upon erase and configure the options to include, like name, destination, SMART details. Options for issuing individual XML reports for the particular disks in the batch can be configured.
Read Report Options on page 58 for description of each attribute.

Email Notifications
User can turn on email notifications for batch operations and attach a Certificate, XML Report and Erase Log to the email.
Read Email Notification Options on page 65 for description of each attribute and SMTP settings configuration.

Disk Labels
User can turn on displaying and printing disk labels after batch operation completion, as well as configure default printer and customizing label templates.
ReadLabels Options on page 60 for description of each attribute.

Error Handling
For each batch error handling attributes can be set individually.
Read Error Handling Options on page 63 for description of each attribute.
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 gives 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 well 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
- SMART monitor
- Erase History and Export to Database

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 from the Disk Bay layout view, simply select the desired disk and click Browse Disk in the action toolbar or select related command from the context menu.

Figure 72: Launching the File Browser

This will launch the file browser window, seen below.
The file browser window displays the disk selected. The file explorer windowed view may also be manipulated by navigating to the Customize button at the top. Here, you can you have options to manipulate the elements below.

**Show System Files**
- Toggles advanced disk information (system files) being shown

**Show Unallocated Partitions**
- Toggles the unallocated disk partitions being shown

**Navigator Pane**
- Toggles the Navigator Pane view on and off.

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 75: 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.

Figure 76: NTFS Boot Sector Template
Figure 77: 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 78: 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.
SMART Monitor

KillDisk supports displaying SMART information pertaining to the disks it sees. This is done simply by navigating to the file menu bar and selecting Tools > SMART Monitor. This will open the SMART Monitor window shown below.

SMART Information

The SMART Monitor displays a list of all discovered disks and shows the SMART information next to them in table format. The following SMART information is shown as separate columns:

- Display Name
- Device Model
• Serial Number
• Firmware Version
• Read Error Rate
• Reallocated Sectors Count
• Spin-up Retries
• Command Timeout
• Reallocated Event Count
• Current Pending Sectors
• Reported Uncorrectable Errors
• Soft Read Error Rate
• Read Error Retry Rate

Configurable Settings
In the Settings drop-down menu on a toolbar, these are the parameters that can be configured:

Monitored disks
Here you have the option to either display All Disks seen by the system, or only the Active (processing) disks.

Refresh Rate
This specifies the interval in seconds between updates to the SMART information displayed when the SMART Monitor is running.

Running the SMART Monitor
The SMART monitor can either be refreshed manually or run to keep the information current. To run the SMART monitor, simply click the Start button in the action toolbar. To pause or stop auto-refreshing sequence click Pause or Stop buttons in view's toolbar respectively.

Note:
SMART Monitoring is a process that requires a lot of resources. It can slow down erase/wipe/examine process significantly. We advise you to avoid querying SMART information very often.

Erase History Log
Erase History is a feature that allows you to oversee all your operations from within KillDisk Industrial. Once any KillDisk Industrial operation completes, the results of this operation are added to the Erase History log stored in the local database, and are available to use with any of the features explained below.

To access the Erase History do one of:
1. In the file menu bar, navigate to Tools > Erase History or
2. Press CTRL + L
**Figure 81: Erase History Log View**

**Action Toolbar Options**

**Connect**
Allows you to connect to your external database to export erase logs. After providing credentials to log into the database, KillDisk Industrial will be able to export certificates and reports, as well as erase history to the external SQL database.

**Disconnect**
Disconnects and stops exporting to the external SQL database, however Erase History still kept and accumulating in the local database.

**Refresh**
Refreshes the erase history to reflect any recently completed operations.

**Show Certificate**
Shows the corresponding PDF erase certificate for the selected erase operation.

**Show Report**
Shows the corresponding erase report for the selected erase operation.

**Clear**
Clears the erase history.

**Additional Options**

**Show Batches View**
Rather than showing history for each individual disk, batches are displayed together.

**Filter**
Filter the operations displayed by success rate, batching, or display all.

For the individual disk history, completed processes can be viewed and sorted by important attributes like Serial Number, size, date and more:
Export Log to SQL Database

KillDisk Industrial's Export feature allows to send out all current logs, certificates and reports from locally stored database over the network to the external SQL database. Both local Erase History and all future transactions can be exported after connection to database is established.

Connection to SQL Databases supported:

- Microsoft SQL Server
- ORACLE
- PostgreSQL
- MySQL

To connect to the external SQL database do one of:

1. Navigate to **File > Preferences** or press **F10**. Then click **Database Export** tab on the left
2. Alternatively, on the file menu bar, navigate to **Tools > Erase History** or press **CTRL + L**. Then click **Connect** toolbar button
3. Database Export dialog appears:
4. Select Driver for the particular database you want to connect to from the list of databases
5. Type in the Database Name on the remote end
6. Type in the database Username for the connection
7. Type in the database password for the selected user
8. Type in the Hostname (which can be IP address or local Network Server Name)
9. Select a TCP/IP Port to use, if it is different from the default value for the particular database
10. Set check marks, if needed, for the additional export options:
    • Export certificates and reports for batches
    • Export certificates and reports for particular disks
    • Export existing erase history (can be done the only once per a new connection)
11. Click **OK** to test connection and store connection parameters in settings for future use

Once a connection to the external SQL database established, KillDisk Industrial starts exporting all information related to the current operations automatically.

**Note:**

For the database export to be successful you need to provide a database user with privileges enough for creation two tables (**DISKS** and **BATCHES**) and populating these tables with current operation's parameters.
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@ 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 83: 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/DVD-ROM 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 cybersecurity-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 MTF records or directory records.

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

Wipe Algorithms

The process of deleting files does not eliminate them from the hard drive. Unwanted information may still be left available for recovery on the computer. A majority of software that advertises itself as performing reliable deletions simply wipes out free clusters. Deleted information may be kept in additional areas of a drive. 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 84: 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.
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 85: Disk free space and allocated clusters

Figure 86: Compressed file structure

The MFT (Master File Table) Area

Wiping the system information:

The SMFT 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.
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.

Figure 88: This is how Directory Area looks before Wiping, red rectangles display deleted records
Figure 89: 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 90: 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.
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.

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/~pgut001/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.

**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)}
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.

![Diagram of HPA creation](image)

**Figure 93: 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. \textit{SET MAX ADDRESS} reduces the reported size of the hard drive. \textit{READ NATIVE MAX ADDRESS} returns the true size of the hard drive. An HPA has been created.

3. \textit{IDENTIFY DEVICE} returns the now fake size of the hard drive. \textit{READ NATIVE MAX ADDRESS} returns the true size of the hard drive, the HPA is in existence.

\textbf{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 \textit{Boot Engineering Extension Record (BEER)} and \textit{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 \textit{READ NATIVE MAX ADDRESS} and \textit{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.

\textbf{DCO - Device configuration overlay}

\textbf{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 \textit{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 \textit{DEVICE_CONFIGURATION_IDENTIFY} command is used, and the output of this command can be compared to the output of \textit{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 \textit{DEVICE_CONFIGURATION_RESET} command. This permanently alters the disk, unlike with the (HPA), which can be temporarily removed for a power cycle.

\textbf{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.