USER MANUAL

Ver. 5.0.0

Updated: 20 Oct 2020

Contents

Legal Statement

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

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

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

Active@ KillDisk, the **Active@ KillDisk** logo, **KillDisk**, **KillDisk for Industrial Systems**, **KillDisk Desktop** 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 stores thousands of files written on it and many of them contain sensitive information. Over the course of a hard drives lifetime the likelihood for recoverable remnants of sensitive information left on a hard drive at its end of life is very high. To see this just try out **KillDisk**'s File Browser on page 82 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 82 as well. Data leakages are not limited to hard drives!

Related information

File Browser on page 82

Data Recovery

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

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

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

Related information

Getting Started on page 10

Usage Scenarios on page 28

Erase Disk Concepts on page 143

Erasing Confidential Data

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

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

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

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

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

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

Important:

Formatting a disk removes all information from the disk.

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

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

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.

Related tasks

Disk Erase

Related information

Disk Erase on page 103

Erase Disk Concepts on page 143

Disk Hidden Zones (HPA/DCO) on page 155

Wiping Confidential Data

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

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 on the system disk, the process must be run under operating system booted from CD/DVD/USB disk. 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 system records or directory records.

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

Related tasks

Disk Wipe on page 35

Related information

Disk Wipe on page 106

Wipe Disk Concepts on page 146

International Standards in Data Destruction

KillDisk works with dozens of international standards for clearing and sanitizing data including the US DoD 5220.22-M and NIST 800-88 standards. You can be sure that once you erase a disk with **KillDisk** all the sensitive information is destroyed forever.

KillDisk is a professional security application that destroys data permanently from any computer that can be started using a boot 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 machine types, 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.

Related information

Erase Methods (Sanitation Standards) on page 151

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:

- Fast 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 US DoD 5220.22-M
- Sanitize external disks (USB drives, external HDD/SSD) connected to both USB 2.0 and 3.1 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 external databases or CSV-file
- Wipe out unused clusters and meta-data on live volumes, leaving existing data intact
- Provides fast low-level Secure Erase feature for your SSD
- 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
- And more...

KillDisk maintains the highest standards in disk erasure and provides extensive documentation options for its operations through Reports and printable Erase Certificates on page 54 and Disk Labels on page 61.

Related information

Disk Batches on page 74

Erase Methods (Sanitation Standards) on page 151

System Requirements

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

Workstation

- PC compatible computer
- Intel Pentium or higher
- 2 GB of RAM
- 100 MB of free disk space

Video

- VGA (1024x768) resolution or better

Operating Systems

- Windows XP or higher
- Linux Kernel 2.x or higher

Drive Storage

Disk types supported:

- IDE / ATA
- HDD / SSD
- SATA / mSATA / eSATA
- SCSI / SAS
- M.2 / NVMe
- USB / SD

KillDisk Industrial works with all drives supported by the Operating System with read/write access.

Related information

Installation and Distribution on page 10

Security Hardware on page 10

Software Licensing

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).

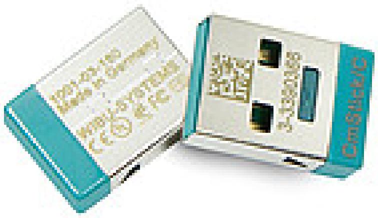
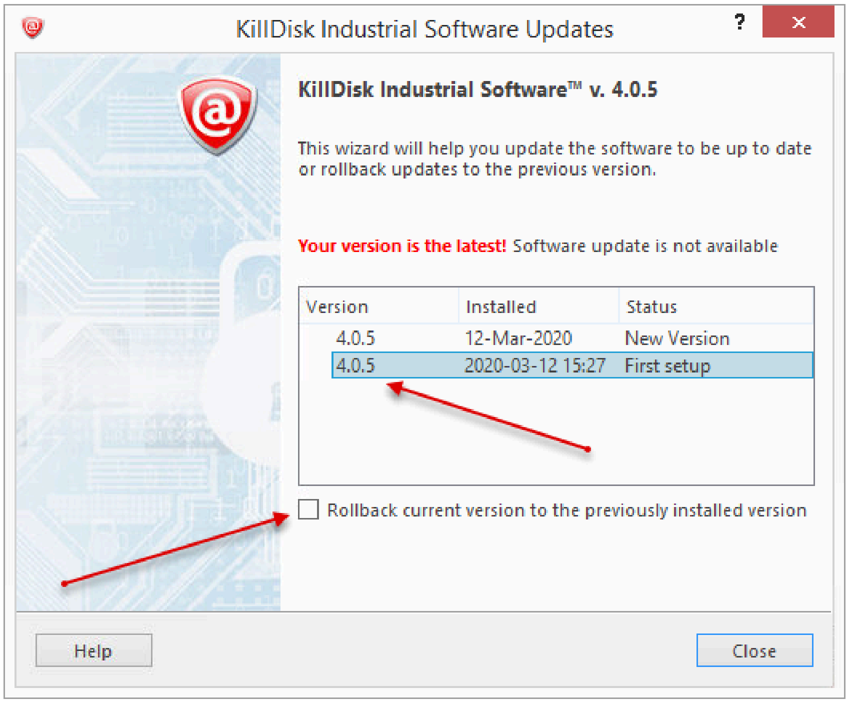


Figure 1: Security USB license key

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 an access to the latest version of the application. To check for update, use the file menu bar to navigate to **Help** > **Check for Updates**



KillDisk Industrial Software™ v. 4.0.5

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

Your version is the latest! Software update is not available

Version	Installed	Status
4.0.5	12-Mar-2020	New Version
4.0.5	2020-03-12 15:27	First setup

☐ Rollback current version to the previously installed version

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.

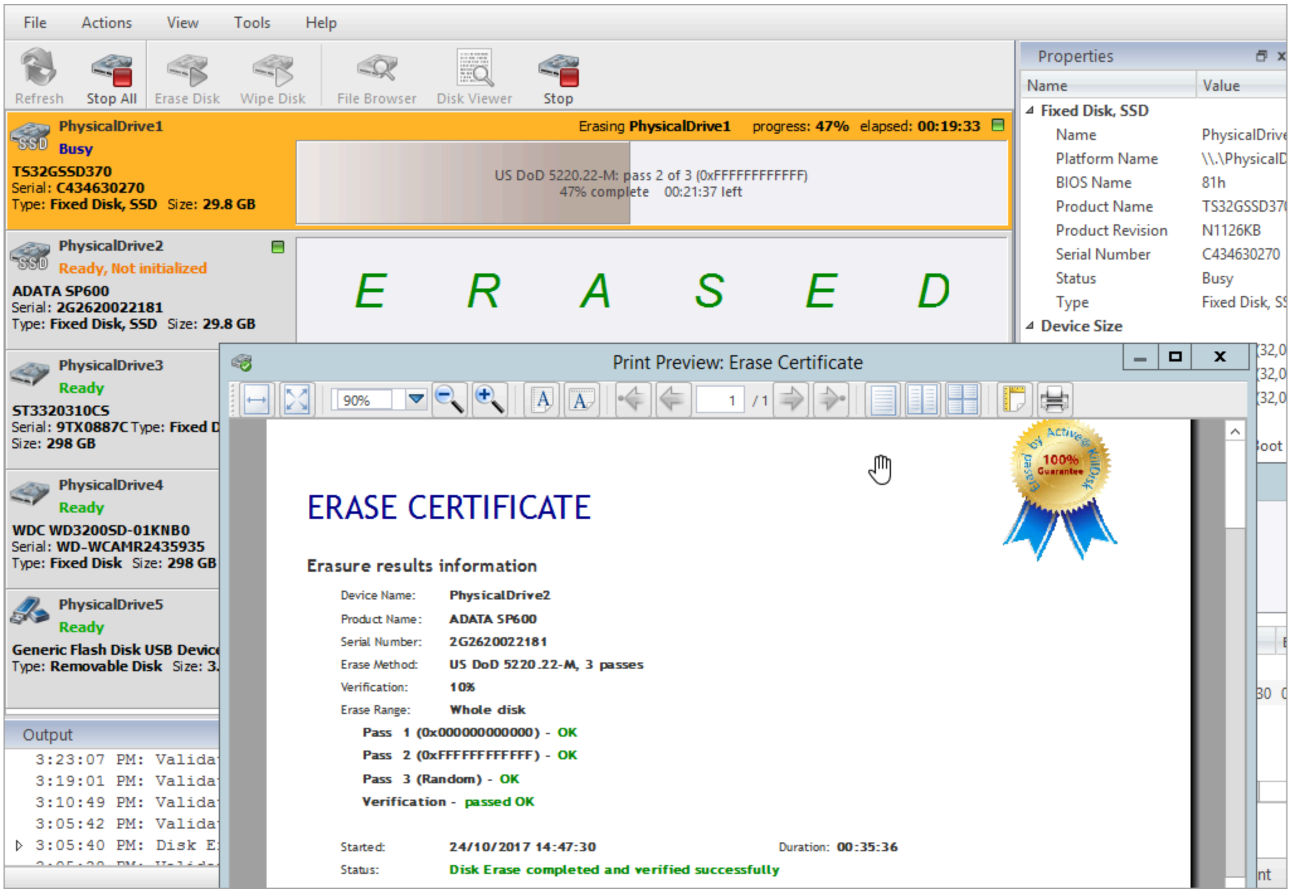
Security Hardware

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.

Figure 3: Hardware activation dongle

Getting Started

This section describes the key features of **KillDisk** and explains basic functionality.



PhysicalDrive1
Busy
TS32GSSD370
Serial: C434630270
Type: Fixed Disk, SSD Size: 29.8 GB

Erasing PhysicalDrive1 progress: 47% elapsed: 00:19:33

US DoD 5220.22-M: pass 2 of 3 (0xFFFFFFFFFFFF)
47% complete 00:21:37 left

PhysicalDrive2
Ready, Not initialized
ADATA SP600
Serial: 2G2620022181
Type: Fixed Disk, SSD Size: 29.8 GB

PhysicalDrive3
Ready
ST3320310CS
Serial: 9TX0887C Type: Fixed D
Size: 298 GB

PhysicalDrive4
Ready
WDC WD3200SD-01KNB0
Serial: WD-WCAMR2435935
Type: Fixed Disk Size: 298 GB

PhysicalDrive5
Ready
Generic Flash Disk USB Devic
Type: Removable Disk Size: 3.

```
3:23:07 PM: Valida
3:19:01 PM: Valida
3:10:49 PM: Valida
3:05:42 PM: Valida
3:05:40 PM: Disk E
```

Name	Value
Fixed Disk, SSD	
Name	PhysicalDrive
Platform Name	\\.\PhysicalD
BIOS Name	81h
Product Name	TS32GSSD37
Product Revision	N1126KB
Serial Number	C434630270
Status	Busy
Type	Fixed Disk, S
Device Size	

Print Preview: Erase Certificate

ERASE CERTIFICATE

Erasure results information

Device Name: PhysicalDrive2
Product Name: ADATA SP600
Serial Number: 2G2620022181
Erase Method: US DoD 5220.22-M, 3 passes
Verification: 10%
Erase Range: Whole disk
Pass 1 (0x000000000000) - OK
Pass 2 (0xFFFFFFFFFFFF) - OK
Pass 3 (Random) - OK
Verification - passed OK

Started: 24/10/2017 14:47:30 Duration: 00:35:36
Status: Disk Erase completed and verified successfully

Installation and Distribution

KillDisk Industrial is distributed as a software solution on DVD media plus security license on USB dongle.

DVD media contains two files:

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

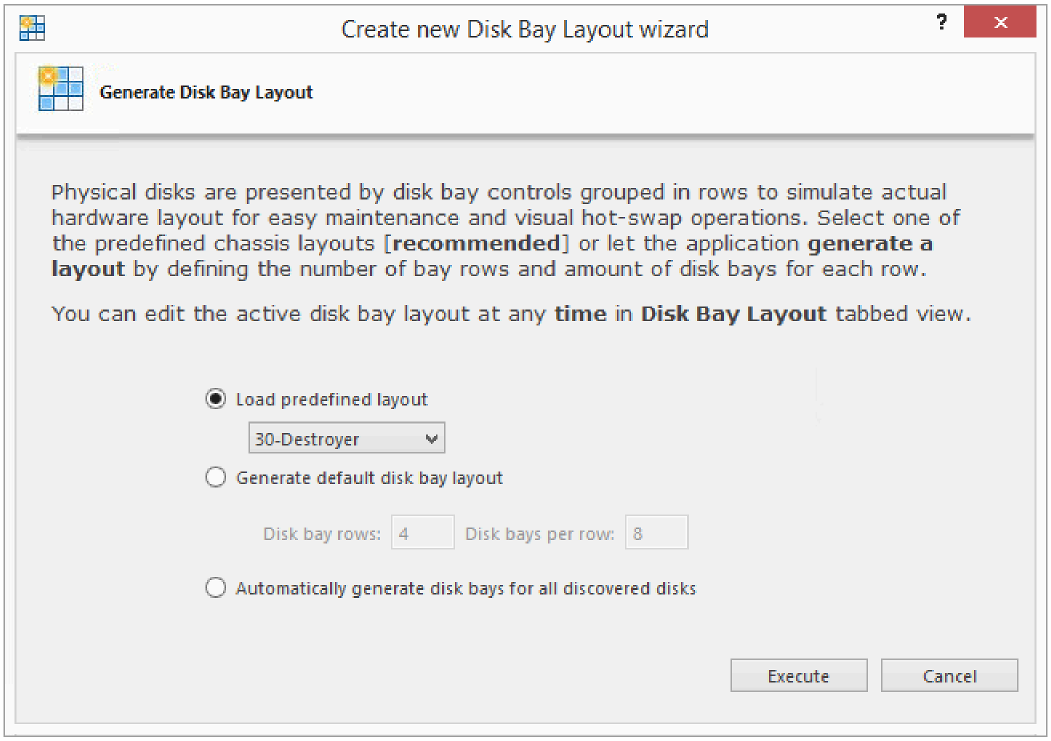
Double-click the installation package to install the application into your data erasure workstation, then configure it.

Launching and Configuration

Note:

Before launching the software make sure the security USB dongle is plugged into the workstation's USB slot.

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



Create new Disk Bay Layout wizard

Generate Disk Bay Layout

Physical disks are presented by disk bay controls grouped in rows to simulate actual hardware layout for easy maintenance and visual hot-swap operations. Select one of the predefined chassis layouts [**recommended**] or let the application **generate a layout** by defining the number of bay rows and amount of disk bays for each row.

You can edit the active disk bay layout at any **time** in **Disk Bay Layout** tabbed view.

● Load predefined layout

30-Destroyer

○ Generate default disk bay layout

Disk bay rows: 4 Disk bays per row: 8

○ Automatically generate disk bays for all discovered disks

Figure 4: Disk Bay Layout Wizard

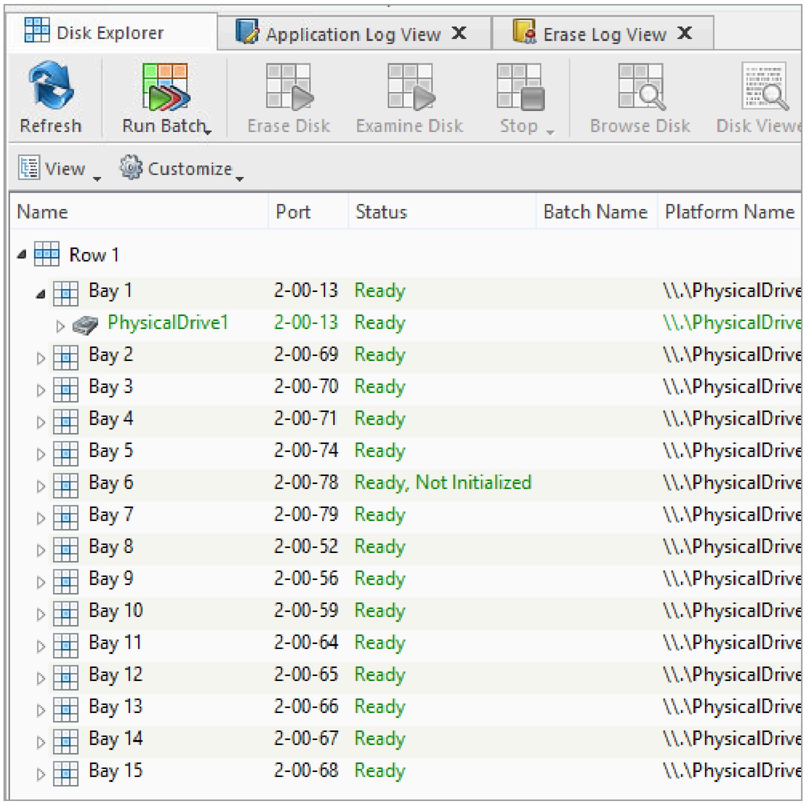
This menu allows you to initialize **KillDisk** to display your hardware in an intuitive way. To illustrate the purpose of this read this section on Disk Bay Layouts. This initial configuration can be done in one of three ways:

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 hardware 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 template 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. The result could be looking as the following:



Name	Port	Status	Batch Name	Platform Name
Row 1				
Bay 1	2-00-13	Ready		\\.\PhysicalDrive
PhysicalDrive1	2-00-13	Ready		\\.\PhysicalDrive
Bay 2	2-00-69	Ready		\\.\PhysicalDrive
Bay 3	2-00-70	Ready		\\.\PhysicalDrive
Bay 4	2-00-71	Ready		\\.\PhysicalDrive
Bay 5	2-00-74	Ready		\\.\PhysicalDrive
Bay 6	2-00-78	Ready, Not Initialized		\\.\PhysicalDrive
Bay 7	2-00-79	Ready		\\.\PhysicalDrive
Bay 8	2-00-52	Ready		\\.\PhysicalDrive
Bay 9	2-00-56	Ready		\\.\PhysicalDrive
Bay 10	2-00-59	Ready		\\.\PhysicalDrive
Bay 11	2-00-64	Ready		\\.\PhysicalDrive
Bay 12	2-00-65	Ready		\\.\PhysicalDrive
Bay 13	2-00-66	Ready		\\.\PhysicalDrive
Bay 14	2-00-67	Ready		\\.\PhysicalDrive
Bay 15	2-00-68	Ready		\\.\PhysicalDrive

Figure 5: Disk Bay View (automatically generated)

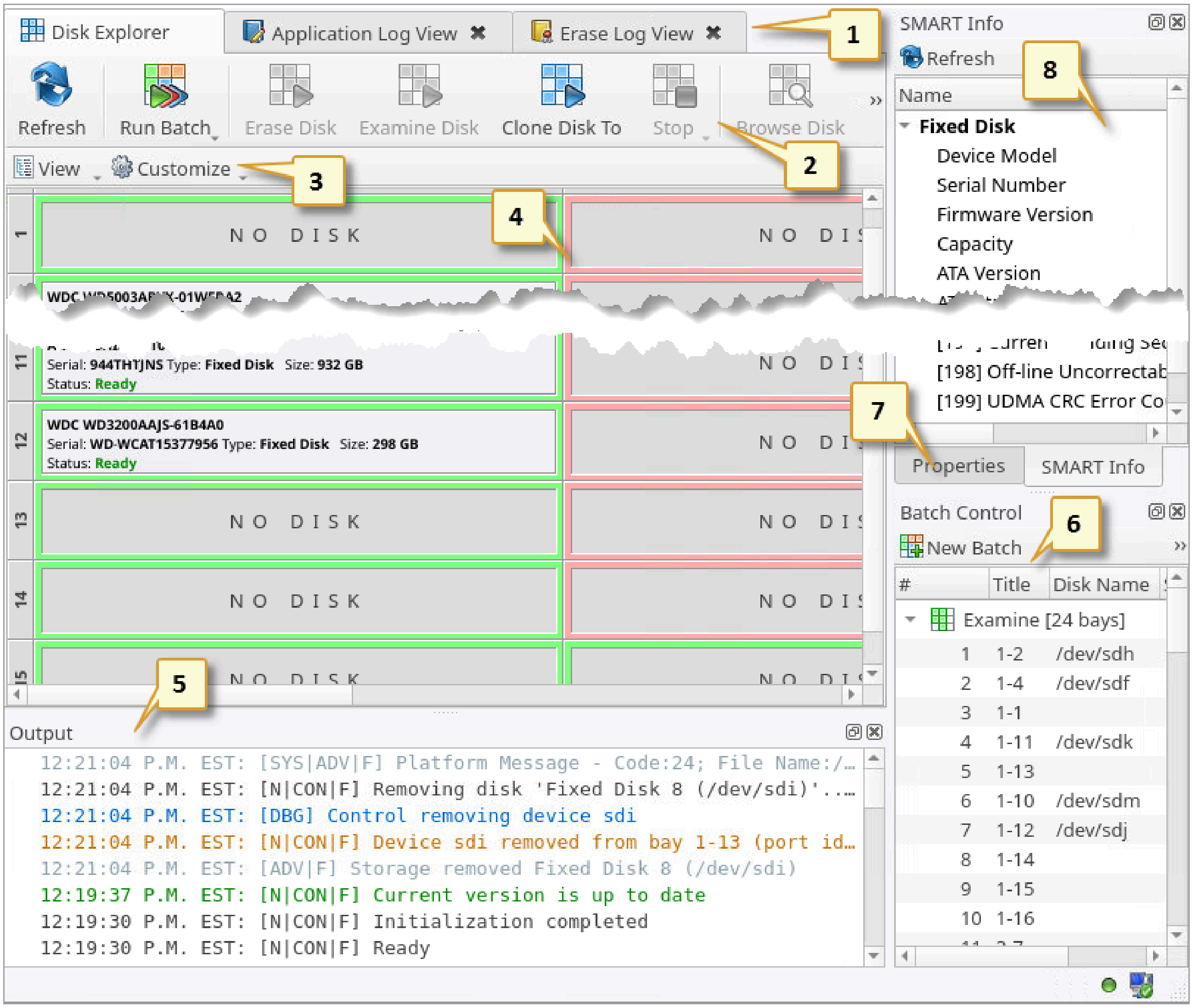
Related information

Security Hardware on page 10

Disk Layout Overview on page 21

Navigating

Once the **KillDisk** application is launched the main application's dashboard appears. From here you can use any of **KillDisk**'s tools on your system. This section describes the main components of the application. The full functionality and features of these components are discussed in their corresponding sections later.



WDC WD3200AAJS-61B4A0
Serial: WD-WCAT15377956 Type: Fixed Disk Size: 298 GB
Status: Ready

Serial: 944THTJNS Type: Fixed Disk Size: 932 GB
Status: Ready

#	Title	Disk Name
Examine [24 bays]		
1	1-2	/dev/sdh
2	1-4	/dev/sdf
3	1-1	
4	1-11	/dev/sdk
5	1-13	
6	1-10	/dev/sdm
7	1-12	/dev/sdj
8	1-14	
9	1-15	
10	1-16	

```
12:21:04 P.M. EST: [SYS|ADV|F] Platform Message - Code:24; File Name:/…
12:21:04 P.M. EST: [N|CON|F] Removing disk 'Fixed Disk 8 (/dev/sdi)'.…
12:21:04 P.M. EST: [DBG] Control removing device sdi
12:21:04 P.M. EST: [N|CON|F] Device sdi removed from bay 1-13 (port id…
12:21:04 P.M. EST: [ADV|F] Storage removed Fixed Disk 8 (/dev/sdi)
12:19:37 P.M. EST: [N|CON|F] Current version is up to date
12:19:30 P.M. EST: [N|CON|F] Initialization completed
12:19:30 P.M. EST: [N|CON|F] Ready
```

Figure 6: KillDisk Industrial application dashboard

Where:

1 - Tabbed Windows
Here you can navigate between **KillDisk** tabbed windows such as Disk Explorer, Application Log etc..

2 - Command Toolbar
The command toolbar is a dynamic toolbar that allows the user to perform Tabbed Window-specific actions (depending on the context).

3 - View Selection
This *View Selection* (only available in **Disk Explorer View**) allows you to manipulate how the *Bays* are displayed in the **Windowed View** as well as manipulating with type of graphics used to show the *Bays* in **Disk Bay View**.

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

5 - Output window
Contains the log of operations **KillDisk** has performed.

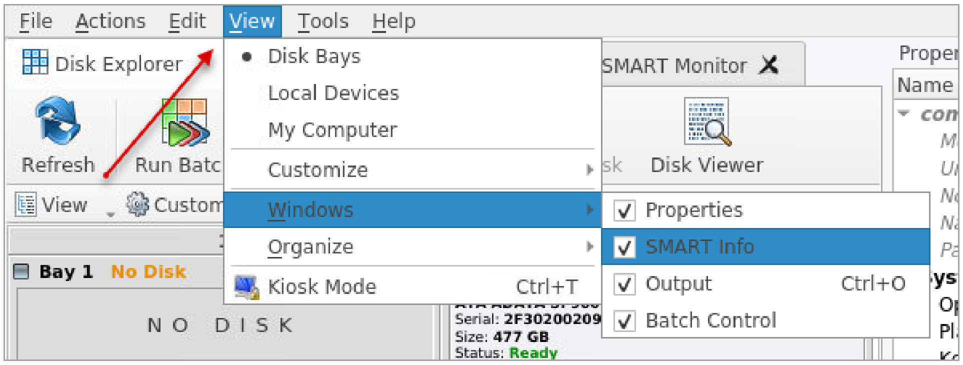
6 - Batch control window
The *Batch control* window is an easily accessible interface to create, delete and manipulate disk batches.

7 - Advanced tool tabs
These tabs allow to navigate between the different *Advanced Tool* windows.

8 - 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 open any closed View just 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.

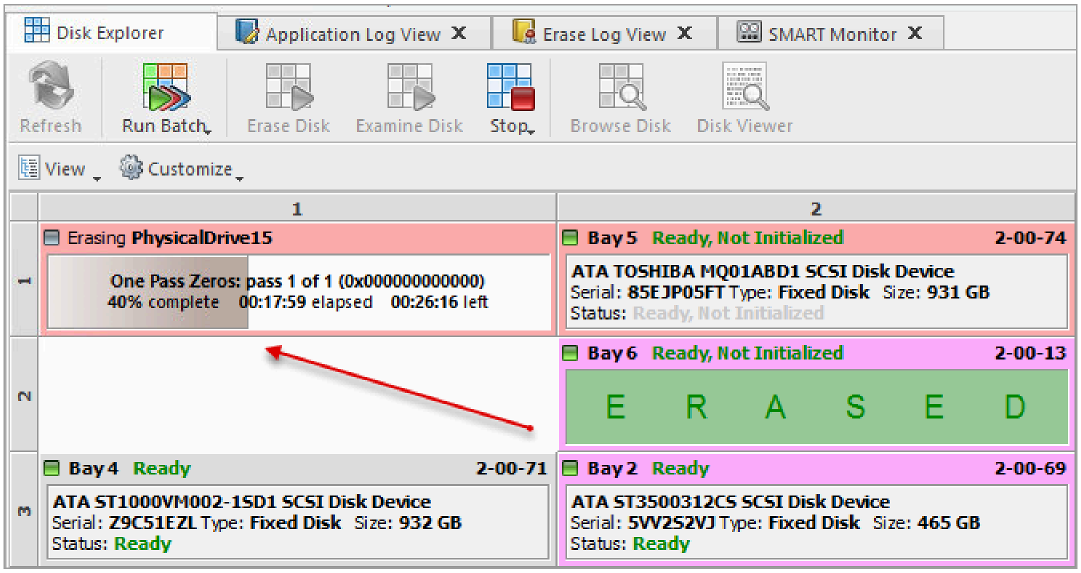
Related information

Usage Scenarios on page 28

Property Views on page 71

Disk Explorer

The Disk Explorer is a default View for the **KillDisk** application. All the attached *HDD/SSD/USB* disks are visualized can be selected and manipulated here. New procedures like erasure can be initiated from here as well as displaying statuses and progress for actions performed with disks. There are three available main Views: Disk Bays View on page 15, Local Devices View on page 18 and My Computer View on page 20



Erasing PhysicalDrive15
One Pass Zeros: pass 1 of 1 (0x000000000000)
40% complete 00:17:59 elapsed 00:26:16 left

Bay 5 Ready, Not Initialized 2-00-74
ATA TOSHIBA MQ01ABD1 SCSI Disk Device
Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB
Status: Ready, Not Initialized

Bay 6 Ready, Not Initialized 2-00-13
E R A S E D

Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: Z9C51EZL Type: Fixed Disk Size: 932 GB
Status: Ready

Bay 2 Ready 2-00-69
ATA ST3500312CS SCSI Disk Device
Serial: 5VV2S2VJ Type: Fixed Disk Size: 465 GB
Status: Ready

Figure 7: Disk Explorer Views

An additional 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** actions, each with their own customizable settings for different use cases.

Customize

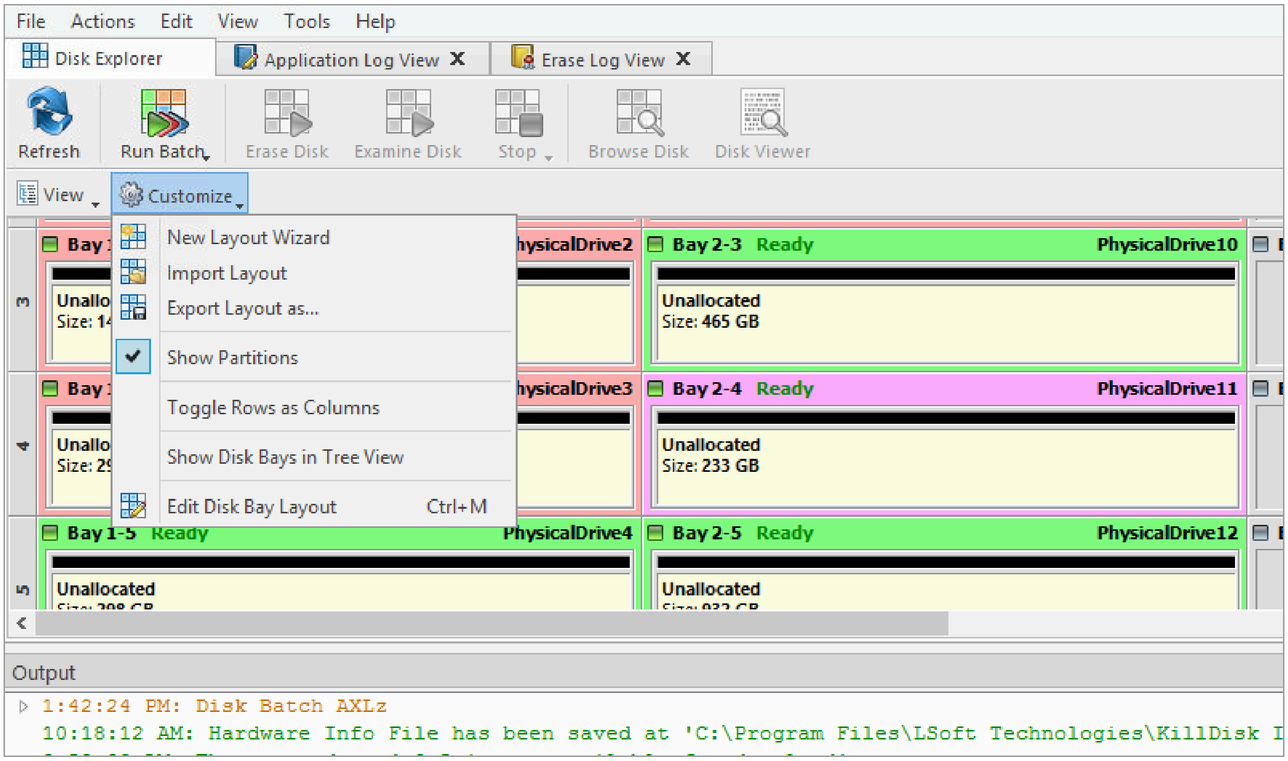
These settings (different for each View) let you customize appearance for better experience for each View.

Related information

Preferences on page 99
Disk Bays View on page 15
Local Devices View on page 18
My Computer View on page 20

Disk Bays View

This View 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 status and progress are displayed.



```
1:42:24 PM: Disk Batch AXLz
10:18:12 AM: Hardware Info File has been saved at 'C:\Program Files\LSoft Technologies\KillDisk I
```

Figure 8: Disk Bays View

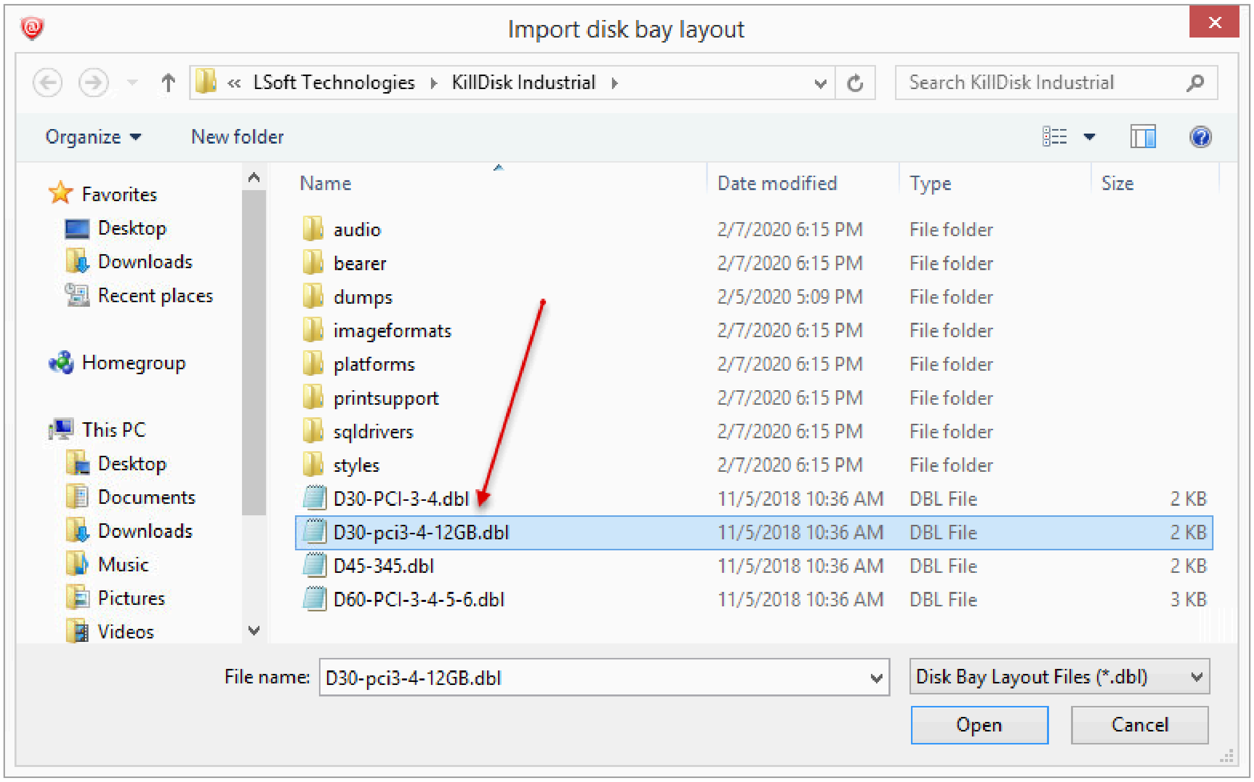
Customize menu

New Layout Wizard

Launches the Disk Bay Layout Wizard

Import Layout

Imports saved (exported) layout (*.dbl)



Name	Date modified	Type	Size
audio	2/7/2020 6:15 PM	File folder	
bearer	2/7/2020 6:15 PM	File folder	
dumps	2/5/2020 5:09 PM	File folder	
imageformats	2/7/2020 6:15 PM	File folder	
platforms	2/7/2020 6:15 PM	File folder	
printsupport	2/7/2020 6:15 PM	File folder	
sqldrivers	2/7/2020 6:15 PM	File folder	
styles	2/7/2020 6:15 PM	File folder	
D30-PCI-3-4.dbl	11/5/2018 10:36 AM	DBL File	2 KB
D30-pci3-4-12GB.dbl	11/5/2018 10:36 AM	DBL File	2 KB
D45-345.dbl	11/5/2018 10:36 AM	DBL File	2 KB
D60-PCI-3-4-5-6.dbl	11/5/2018 10:36 AM	DBL File	3 KB

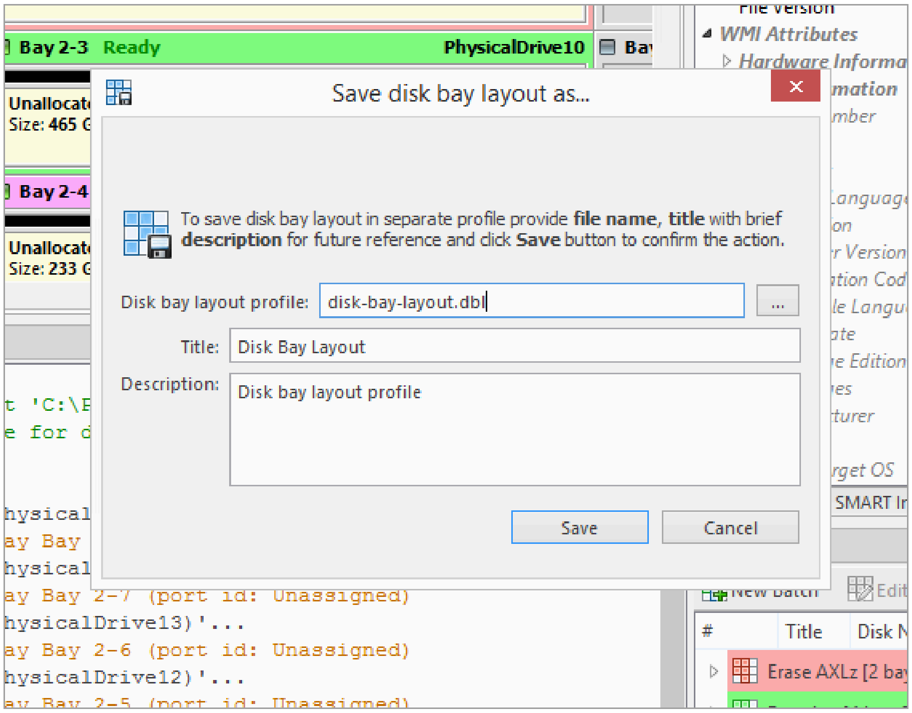
File name: D30-pci3-4-12GB.dbl

Disk Bay Layout Files (*.dbl)

Figure 9: Disk Bay Layout Import

Export Layout as..

Exports custom (built) layout (*.dbl)



Save disk bay layout as...

To save disk bay layout in separate profile provide **file name**, **title** with brief **description** for future reference and click **Save** button to confirm the action.

Disk bay layout profile: disk-bay-layout.dbl

Title: Disk Bay Layout

Description: Disk bay layout profile

Figure 10: Disk Bay Layout Export

Show Partitions

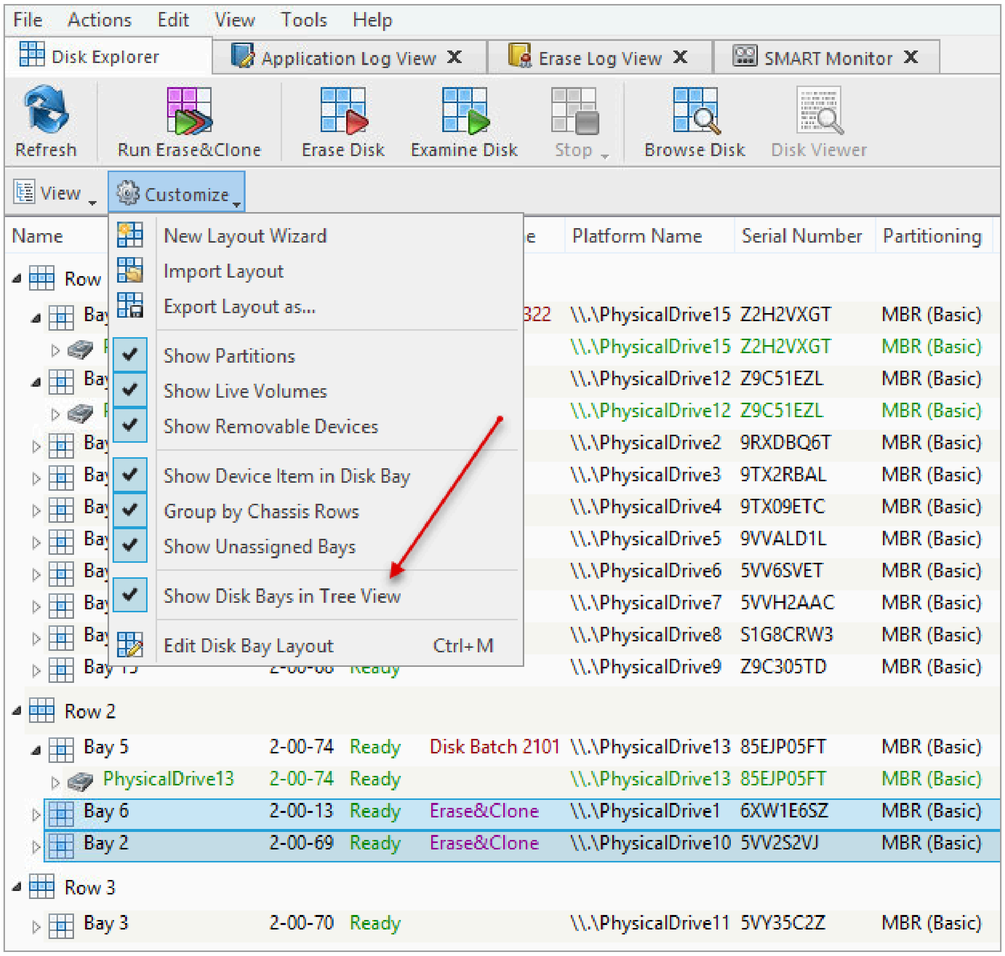
Show or hide additional layout for partitions and volumes

Toggle 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

Show Disk Bays in Tree View

Switches **Disk Bays** View to Tree View for user convenience and customization related to the one configured in Disk Layout Editor



Name			e	Platform Name	Serial Number	Partitioning
Row						
Bay			322	\\.\PhysicalDrive15	Z2H2VXGT	MBR (Basic)
				\\.\PhysicalDrive15	Z2H2VXGT	MBR (Basic)
Bay				\\.\PhysicalDrive12	Z9C51EZL	MBR (Basic)
				\\.\PhysicalDrive12	Z9C51EZL	MBR (Basic)
Bay				\\.\PhysicalDrive2	9RXDBQ6T	MBR (Basic)
Bay				\\.\PhysicalDrive3	9TX2RBAL	MBR (Basic)
Bay				\\.\PhysicalDrive4	9TX09ETC	MBR (Basic)
Bay				\\.\PhysicalDrive5	9VVALD1L	MBR (Basic)
Bay				\\.\PhysicalDrive6	5VV6SVET	MBR (Basic)
Bay				\\.\PhysicalDrive7	5VVH2AAC	MBR (Basic)
Bay				\\.\PhysicalDrive8	S1G8CRW3	MBR (Basic)
Bay				\\.\PhysicalDrive9	Z9C305TD	MBR (Basic)
Row 2						
Bay 5	2-00-74	Ready	Disk Batch 2101	\\.\PhysicalDrive13	85EJP05FT	MBR (Basic)
PhysicalDrive13	2-00-74	Ready		\\.\PhysicalDrive13	85EJP05FT	MBR (Basic)
Bay 6	2-00-13	Ready	Erase&Clone	\\.\PhysicalDrive1	6XW1E6SZ	MBR (Basic)
Bay 2	2-00-69	Ready	Erase&Clone	\\.\PhysicalDrive10	5VV2S2VJ	MBR (Basic)
Row 3						
Bay 3	2-00-70	Ready		\\.\PhysicalDrive11	5VY35C2Z	MBR (Basic)

Figure 11: Tree View Layout

Edit Disk Bay Layout

Opens Disk Layout Editor for current layout customization or creating a new layout

Related information

Disk Explorer on page 14

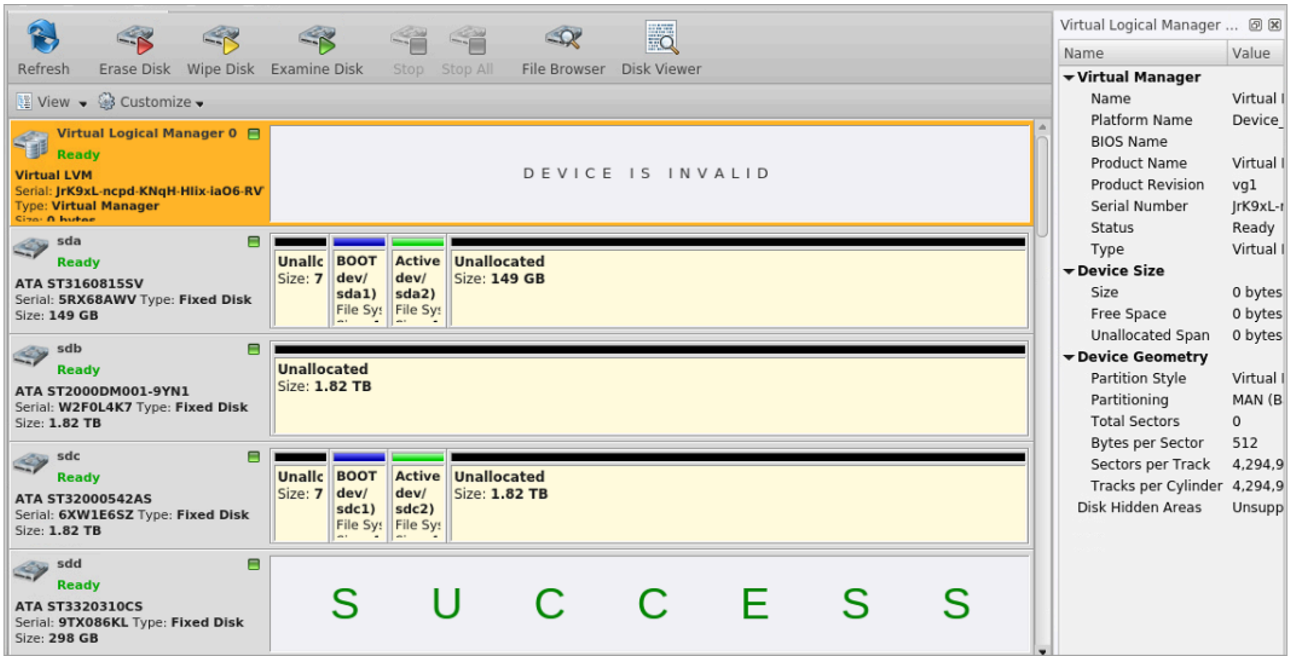
Local Devices View on page 18

My Computer View on page 20

Disk Layout Overview on page 21

Local Devices View

Local Devices View shows all disks recognized by OS and available for application in a List View:



Virtual Logical Manager 0
Ready
Virtual LVM
Serial: JrK9xL-ncpd-KNqH-Hlix-ia06-RV
Type: Virtual Manager
Size: 0 bytes

sda
Ready
ATA ST3160815SV
Serial: 5RX68AWV Type: Fixed Disk
Size: 149 GB

Unallc Size: 7	BOOT dev/ sda1) File Sys	Active dev/ sda2) File Sys	Unallocated Size: 149 GB

sdb
Ready
ATA ST2000DM001-9YN1
Serial: W2F0L4K7 Type: Fixed Disk
Size: 1.82 TB

Unallocated
Size: 1.82 TB

sdc
Ready
ATA ST32000542AS
Serial: 6XW1E6SZ Type: Fixed Disk
Size: 1.82 TB

Unallc Size: 7	BOOT dev/ sdc1) File Sys	Active dev/ sdc2) File Sys	Unallocated Size: 1.82 TB

sdd
Ready
ATA ST3320310CS
Serial: 9TX086KL Type: Fixed Disk
Size: 298 GB

Virtual Logical Manager ...

Name	Value
Virtual Manager	
Name	Virtual I
Platform Name	Device_
BIOS Name	
Product Name	Virtual I
Product Revision	vg1
Serial Number	JrK9xL-r
Status	Ready
Type	Virtual I
Device Size	
Size	0 bytes
Free Space	0 bytes
Unallocated Span	0 bytes
Device Geometry	
Partition Style	Virtual I
Partitioning	MAN (B
Total Sectors	0
Bytes per Sector	512
Sectors per Track	4,294,9
Tracks per Cylinder	4,294,9
Disk Hidden Areas	Unsupp

Figure 12: Local Devices View

Customize menu

Show System Devices

Displays the disk where OS installed

Show Not Ready Devices

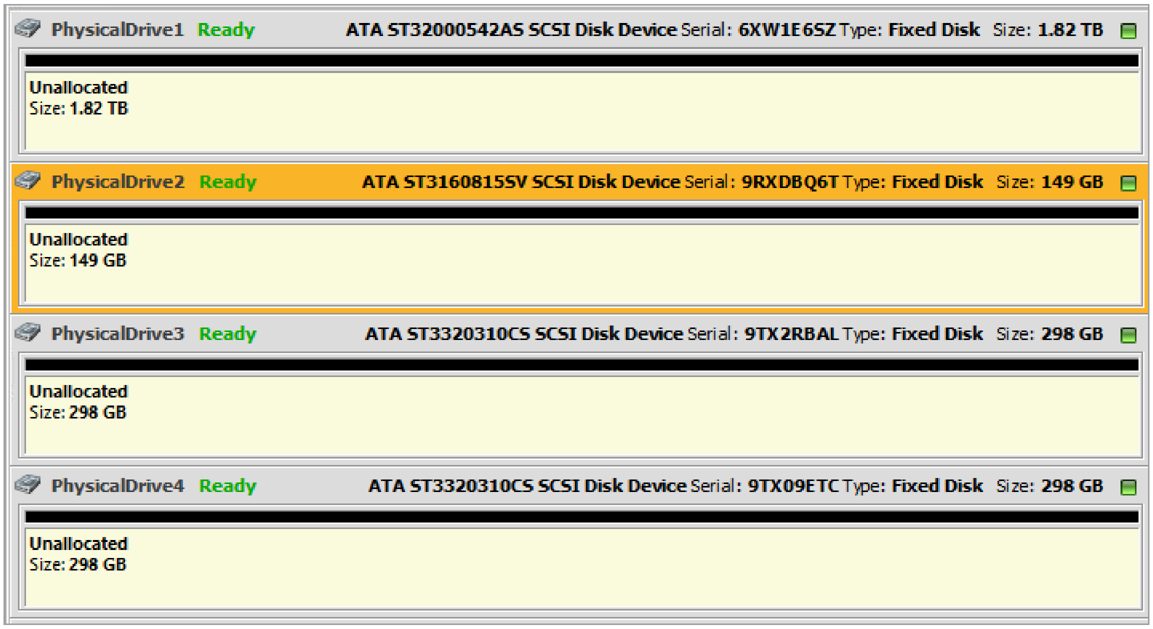
Displays devices not yet initialized and used by OS

Show Removable Devices

Displays all removable and externally connected disks (such as *USB*'s)

Compact View

Changes the layout of the Disk View from display block to inline block orientation



PhysicalDrive1 Ready ATA ST32000542AS SCSI Disk Device Serial: 6XW1E6SZ Type: Fixed Disk Size: 1.82 TB

Unallocated
Size: 1.82 TB

PhysicalDrive2 Ready ATA ST3160815SV SCSI Disk Device Serial: 9RXDBQ6T Type: Fixed Disk Size: 149 GB

Unallocated
Size: 149 GB

PhysicalDrive3 Ready ATA ST3320310CS SCSI Disk Device Serial: 9TX2RBAL Type: Fixed Disk Size: 298 GB

Unallocated
Size: 298 GB

PhysicalDrive4 Ready ATA ST3320310CS SCSI Disk Device Serial: 9TX09ETC Type: Fixed Disk Size: 298 GB

Unallocated
Size: 298 GB

Related information

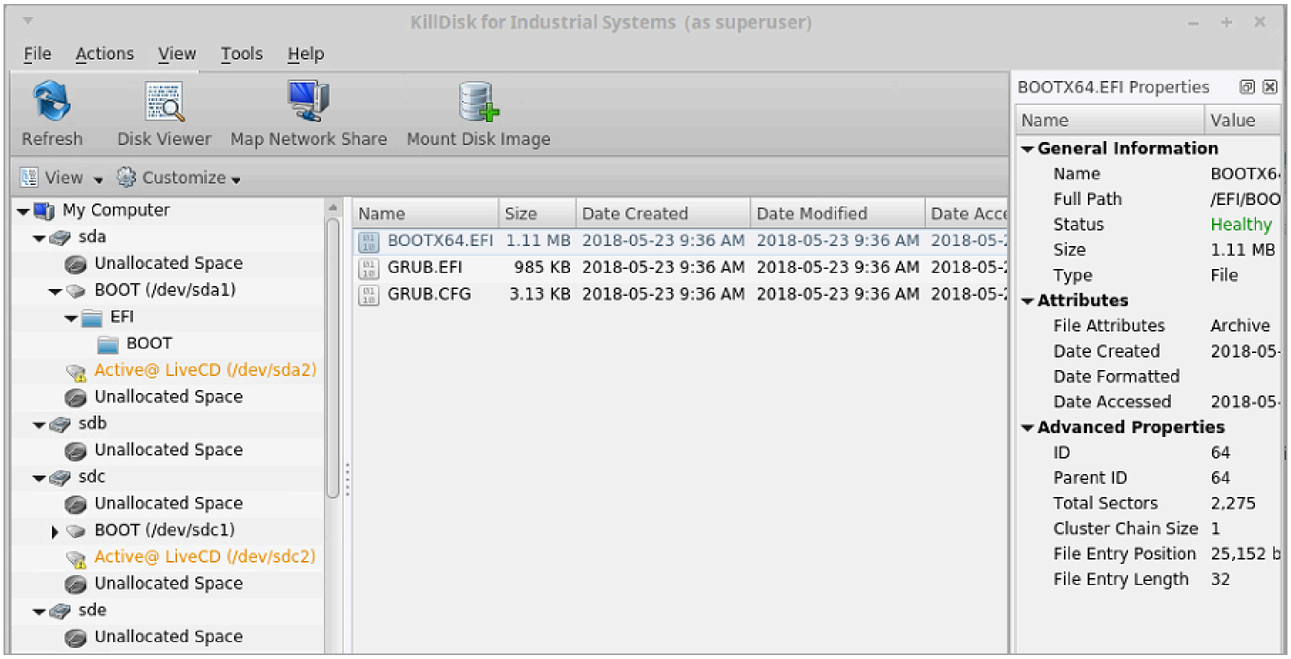
Disk Explorer on page 14

Disk Bays View on page 15

My Computer View on page 20

My Computer View

My Computer View presents the Disk Bay Layout in a standard list form, much like the disks in *Windows 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.



- My Computer
  - sda
    - Unallocated Space
    - BOOT (/dev/sda1)
      - EFI
        - BOOT
    - Active@ LiveCD (/dev/sda2)
    - Unallocated Space
  - sdb
    - Unallocated Space
  - sdc
    - Unallocated Space
    - BOOT (/dev/sdc1)
    - Active@ LiveCD (/dev/sdc2)
    - Unallocated Space
  - sde
    - Unallocated Space

Name	Size	Date Created	Date Modified	Date Acc
BOOTX64.EFI	1.11 MB	2018-05-23 9:36 AM	2018-05-23 9:36 AM	2018-05-
GRUB.EFI	985 KB	2018-05-23 9:36 AM	2018-05-23 9:36 AM	2018-05-
GRUB.CFG	3.13 KB	2018-05-23 9:36 AM	2018-05-23 9:36 AM	2018-05-

BOOTX64.EFI Properties

Name	Value
General Information	
Name	BOOTX6
Full Path	/EFI/BOO
Status	Healthy
Size	1.11 MB
Type	File
Attributes	
File Attributes	Archive
Date Created	2018-05-
Date Formatted	
Date Accessed	2018-05-
Advanced Properties	
ID	64
Parent ID	64
Total Sectors	2,275
Cluster Chain Size	1
File Entry Position	25,152 b
File Entry Length	32

Figure 13: 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 been formatted

Show Devices

Switches between display of devices (physical disks containing volumes) and "volumes only" display

Show Removable Disks

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

Show Not Ready Devices

Displays devices that may not yet been initialized and accessed by the OS

Navigator Pane

Shows/hides **Navigator Pane** (on the right side of the View)

Related information

Disk Explorer on page 14
Disk Bays View on page 15
Local Devices View on page 18

Disk Layout Overview

The purpose of **Disk Bay Layouts** is to match **KillDisk** 's graphical disks' representation to your actual hardware configuration making it easy to manage disks for erasure, examination, cloning and more. To illustrate this let's look at the example, using the hardware below:

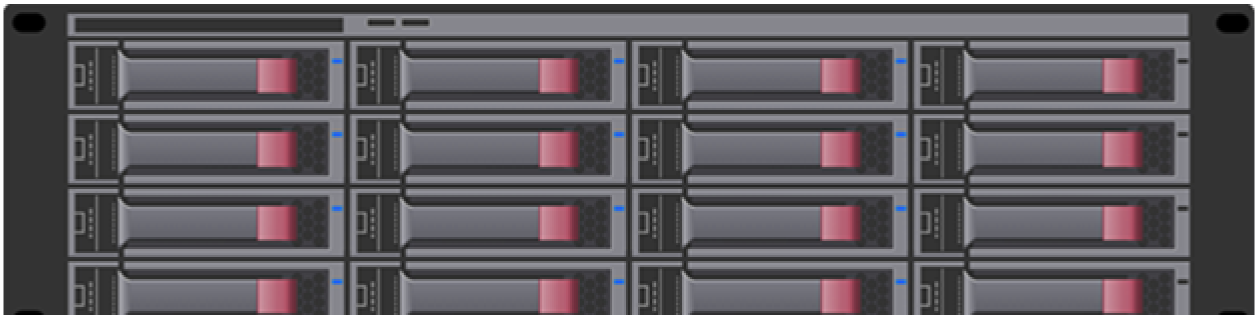
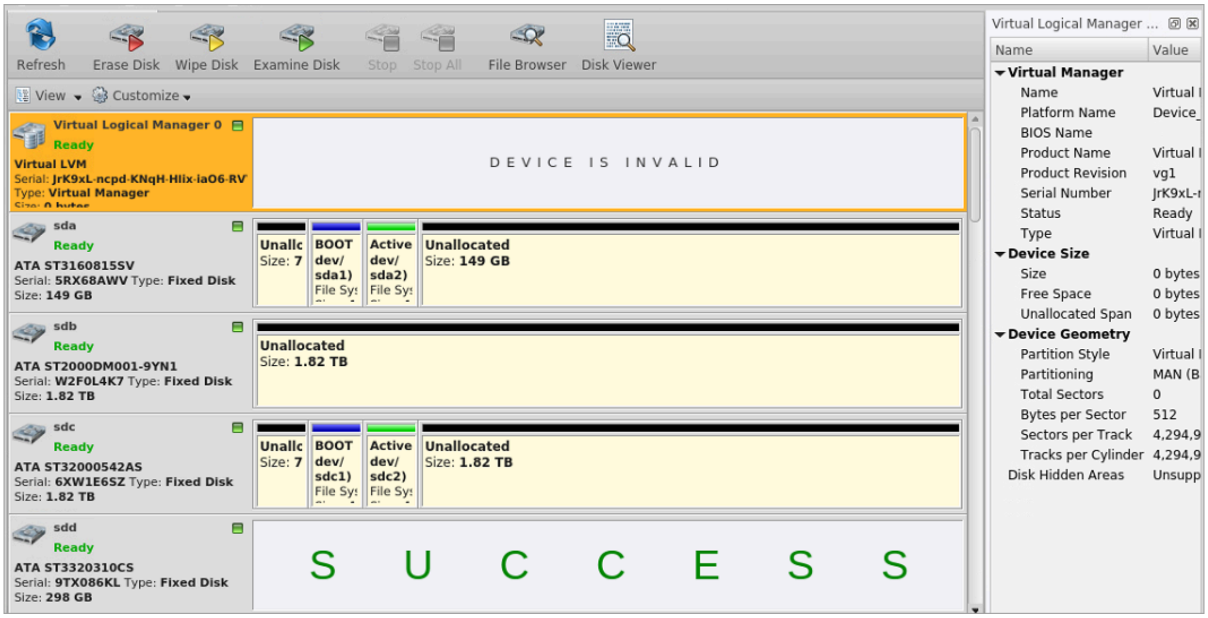


Figure 14: Example of a generic disk array

In the example above 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:



Virtual Logical Manager 0
Ready
Virtual LVM
Serial: JrK9xL-ncpd-KNqH-Hlix-iaO6-RV
Type: Virtual Manager
Size: 0 bytes

DEVICE IS INVALID

sda
Ready
ATA ST3160815SV
Serial: 5RX68AWV Type: Fixed Disk
Size: 149 GB

Unallc Size: 7 | BOOT dev/ sda1) File Sys | Active dev/ sda2) File Sys | Unallocated Size: 149 GB

sdb
Ready
ATA ST2000DM001-9YN1
Serial: W2F0L4K7 Type: Fixed Disk
Size: 1.82 TB

Unallocated Size: 1.82 TB

sdc
Ready
ATA ST32000542AS
Serial: 6XW1E6SZ Type: Fixed Disk
Size: 1.82 TB

Unallc Size: 7 | BOOT dev/ sdc1) File Sys | Active dev/ sdc2) File Sys | Unallocated Size: 1.82 TB

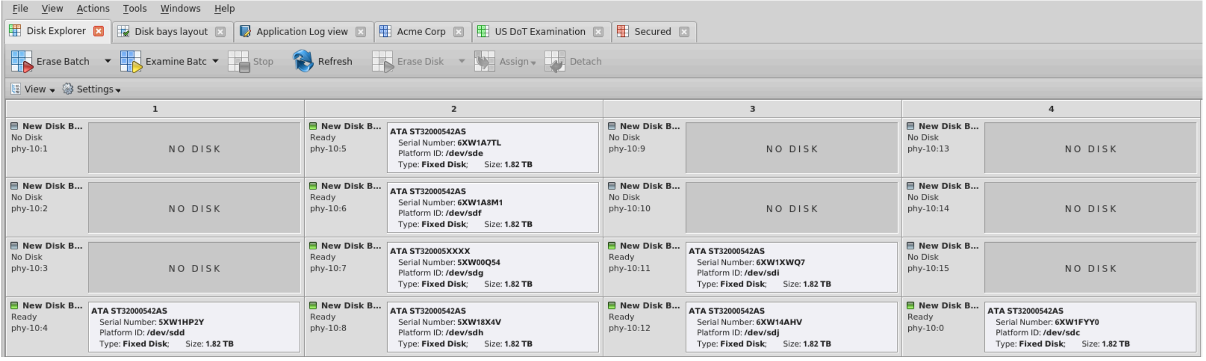
sdd
Ready
ATA ST3320310CS
Serial: 9TX086KL Type: Fixed Disk
Size: 298 GB

SUCCESS

Name	Value
Virtual Manager	
Name	Virtual I
Platform Name	Device_
BIOS Name	
Product Name	Virtual I
Product Revision	vg1
Serial Number	JrK9xL-r
Status	Ready
Type	Virtual I
Device Size	
Size	0 bytes
Free Space	0 bytes
Unallocated Span	0 bytes
Device Geometry	
Partition Style	Virtual I
Partitioning	MAN (B
Total Sectors	0
Bytes per Sector	512
Sectors per Track	4,294,9
Tracks per Cylinder	4,294,9
Disk Hidden Areas	Unsupp

Figure 15: Local Devices View

Now imagine inserting a HDD into the bottom-leftmost Bay of the disk array. Even finding the device in a list of 15 other disks would be tedious and not very intuitive. This is when 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:



1	2	3	4
New Disk B... No Disk phy-10:1 NO DISK	New Disk B... Ready phy-10:5 ATA ST32000542AS Serial Number: 6XW1A7TL Platform ID: /dev/sde Type: Fixed Disk; Size: 1.82 TB	New Disk B... No Disk phy-10:9 NO DISK	New Disk B... No Disk phy-10:13 NO DISK
New Disk B... No Disk phy-10:2 NO DISK	New Disk B... Ready phy-10:6 ATA ST32000542AS Serial Number: 6XW1A8M1 Platform ID: /dev/sdf Type: Fixed Disk; Size: 1.82 TB	New Disk B... No Disk phy-10:10 NO DISK	New Disk B... No Disk phy-10:14 NO DISK
New Disk B... No Disk phy-10:3 NO DISK	New Disk B... Ready phy-10:7 ATA ST320005XXXX Serial Number: 5XW00Q54 Platform ID: /dev/sdg Type: Fixed Disk; Size: 1.82 TB	New Disk B... Ready phy-10:11 ATA ST32000542AS Serial Number: 6XW1XWQ7 Platform ID: /dev/sdi Type: Fixed Disk; Size: 1.82 TB	New Disk B... No Disk phy-10:15 NO DISK
New Disk B... Ready phy-10:4 ATA ST32000542AS Serial Number: 5XW1HP2Y Platform ID: /dev/sdd Type: Fixed Disk; Size: 1.82 TB	New Disk B... Ready phy-10:8 ATA ST32000542AS Serial Number: 5XW18X4V Platform ID: /dev/sdh Type: Fixed Disk; Size: 1.82 TB	New Disk B... Ready phy-10:12 ATA ST32000542AS Serial Number: 6XW14AHV Platform ID: /dev/sdj Type: Fixed Disk; Size: 1.82 TB	New Disk B... Ready phy-10:0 ATA ST32000542AS Serial Number: 6XW1FYY0 Platform ID: /dev/sdc Type: Fixed Disk; Size: 1.82 TB

Figure 16: Disk Bays View

Assuming that the Bays were mapped correctly finding the correct disk to manipulate with is now much easier in the **Disk Bays** View than it would have been Local Devices View on page 18. You can now select the bottom-leftmost disk in the **Disk Bays** View and perform any necessary actions on it.

Related information

Editing Disk Bay Layouts on page 22
Layouts Export and Import on page 25
Layouts Advanced Features on page 26

Editing Disk Bay Layouts

To create or edit current Disk Bay Layout select **Edit** > **Edit Disk Layout** in the menu or use a shortcut **CTRL + M**.

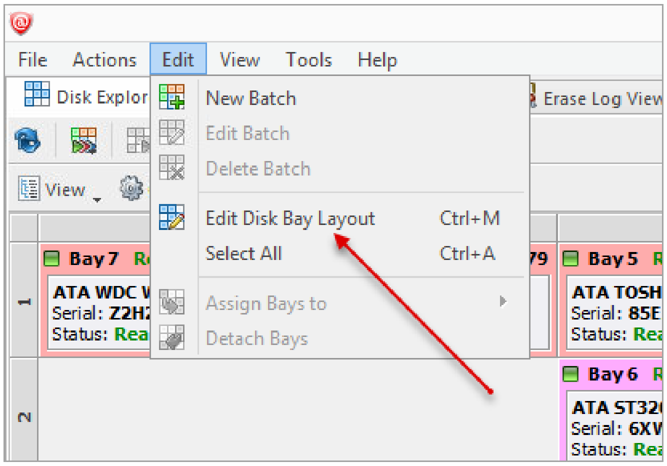


Figure 17: Opening the Disk Bay Layout View

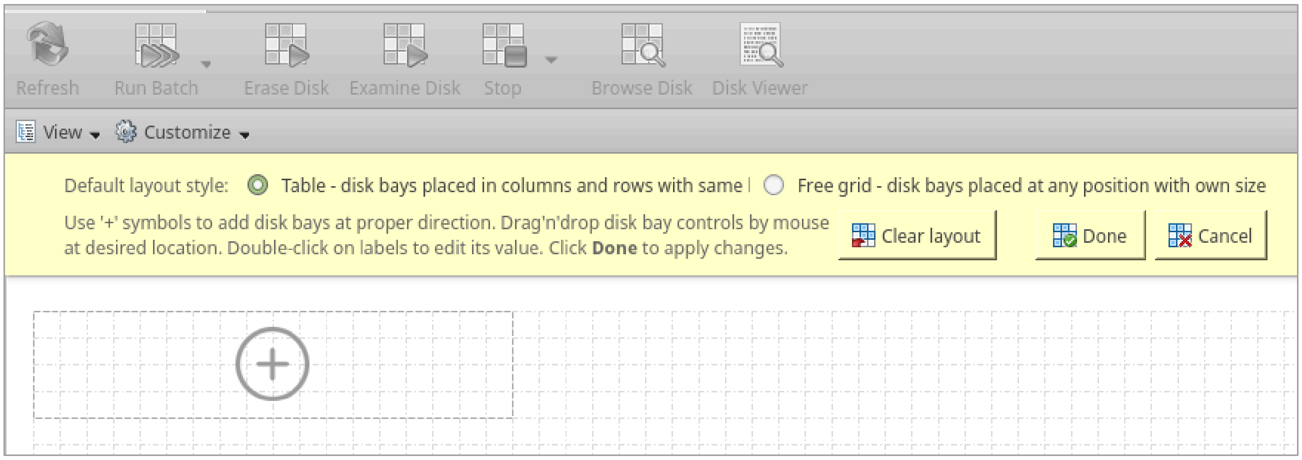
This will bring you to the **Disk Bays Layout** View where you can manipulate, save, import and create Disk Bay Layouts.

There are two types of layouts:

- **Free Grid Layout** allows user to place Disk Bay widget at any position, change Bay widget size and its alignment (vertically or horizontally) individually for each Bay. Hence, user can create relatively accurate mocking layout of actual (physical) disk Bay slots located on hardware chassis
- **Table Layout** is similar to Disk Bay Layout from previous versions. However, now user can re-size or select Disk Bay widgets by using row and column headers

Creating a New Layout

To create a new layout select either **Free Grid** or **Table** layout option and start adding Disk Bays using circled "+" symbols.



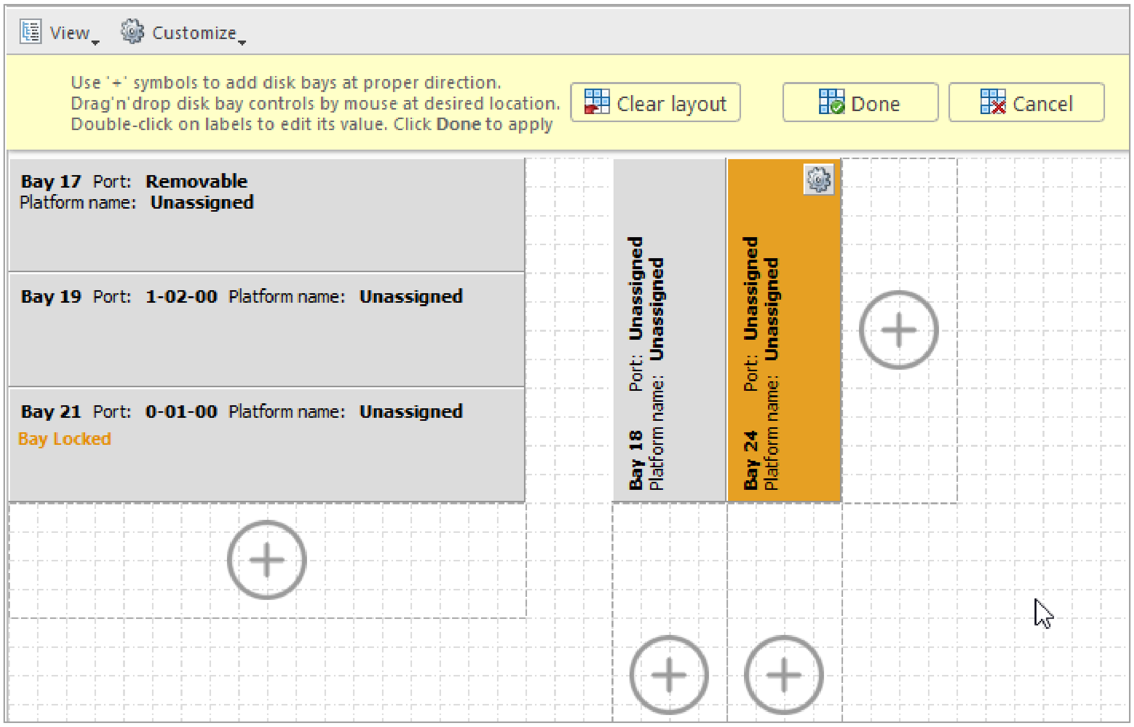
Default layout style: ● Table - disk bays placed in columns and rows with same ○ Free grid - disk bays placed at any position with own size

Use '+' symbols to add disk bays at proper direction. Drag'n'drop disk bay controls by mouse at desired location. Double-click on labels to edit its value. Click **Done** to apply changes.

Figure 18: New Layout View

If predefined layout already exists click **Clear Layout** to remove it and create a new one.

Editing Disk Bay Layout



Use '+' symbols to add disk bays at proper direction.
Drag'n'drop disk bay controls by mouse at desired location.
Double-click on labels to edit its value. Click **Done** to apply

Bay 17 Port: **Removable**
Platform name: **Unassigned**

Bay 19 Port: **1-02-00** Platform name: **Unassigned**

Bay 21 Port: **0-01-00** Platform name: **Unassigned**
Bay Locked

Bay 18 Port: **Unassigned**
Platform name: **Unassigned**

Bay 24 Port: **Unassigned**
Platform name: **Unassigned**

Figure 19: Editing Disk Bay Layout

- Click on circled **"+"** signs to add new Disk Bay widget on a side of existing one. New Disk Bay widget size will be corresponded to adjusted *Disk Bay*
- To re-size Disk Bay use mouse to drag it's right side or bottom
- To set Disk Bay vertically-oriented use mouse to drag it's right side to shrink it until it changes to vertical state.
- To delete Bay(s) select it and press **Delete** keyboard key or use service menu by clicking "gear" icon on left upper corner
- Use mouse to drag-n-drop selected Disk Bay widgets to new location. If hovered location is invalid Disk Bay widgets will be highlighted with crossed sign
- To change disk label or port, click on corresponded labels on disk widget to start editing
- To change Disk Bay attributes use menu by clicking on "gear" sign on selected *Bay*

Important:

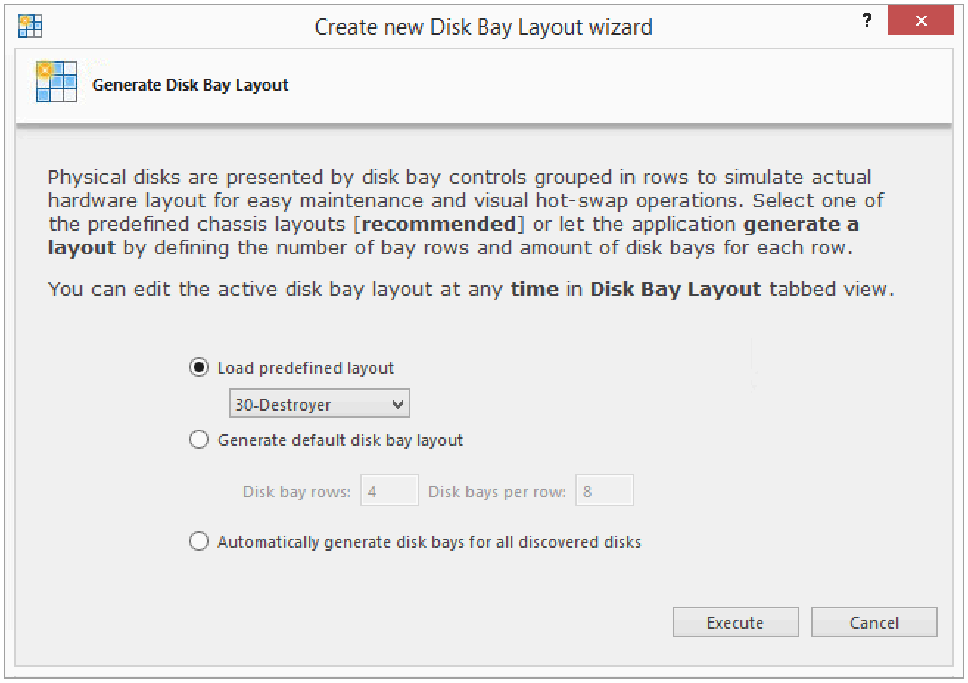
Due to different hard disk controller manufacture standards and platform limitations physical disk port address format may vary.

Note:

If both platform name and disk port are assigned to Disk Bay widget then platform name is used for Disk Bay mapping.

Disk Bay Layout Wizard

To create a new layout using the wizard click **Customize** > **New Layout Wizard**. This will launch the **Disk Bay Layout Wizard**



Physical disks are presented by disk bay controls grouped in rows to simulate actual hardware layout for easy maintenance and visual hot-swap operations. Select one of the predefined chassis layouts [**recommended**] or let the application **generate a layout** by defining the number of bay rows and amount of disk bays for each row.

You can edit the active disk bay layout at any **time** in **Disk Bay Layout** tabbed view.

● Load predefined layout

30-Destroyer

○ Generate default disk bay layout

Disk bay rows: 4 Disk bays per row: 8

○ Automatically generate disk bays for all discovered disks

Figure 20: 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 hardware in terms of a disk array arranged in a *X* by *Y* grid of disks. You can make adjustments to this later so this may just be a template to start from. Table-style layout will be created.

Automatically generate *Disk Bays* for all available physical ports
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.

Warning:

Make sure to save the layout by clicking **Done** otherwise your layout WILL be lost.

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

Saving and Reverting changes

Click **Done** button to commit any changes to the application View layout.

Note:

Done will apply current change to the application session so the changes will be seen in the *Disk Bays* View and even be loaded in future application launch. These changes will not affect the .dbl file.

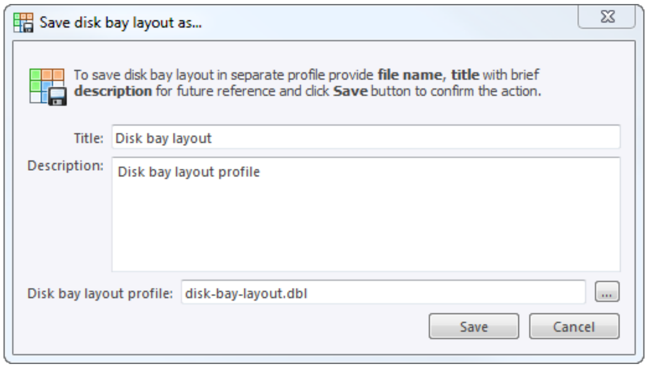
Click **Cancel** to revert any changes you made to the layout.

Layouts Export and Import

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 **Customize** 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.



Save disk bay layout as...

To save disk bay layout in separate profile provide **file name**, **title** with brief **description** for future reference and click **Save** button to confirm the action.

Title: Disk bay layout

Description: Disk bay layout profile

Disk bay layout profile: disk-bay-layout.dbl

Figure 21: Layout Export Dialog

Title

Enter any label to distinguish newly created Disk Bay Layout to differentiate it among other Disk Bay Layouts.

Description

Describe all the specs and features 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 application sessions using the **Import** feature. In the command tool bar select **Customize** 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 application session. Finally, click **Done** to update the disks in the **Disk Explorer** and the import should be complete.

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 **Bay Locked** menu command from the **Change disk bay attributes** drop down menu:

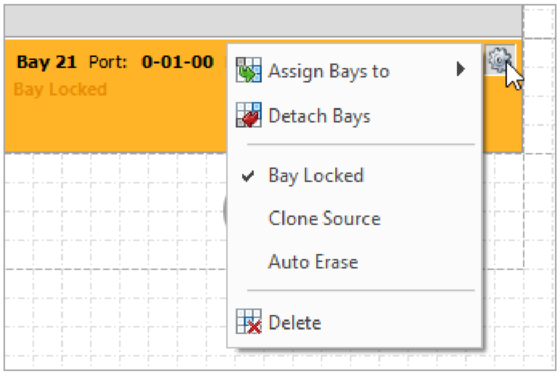


Figure 22: Locking a disk to prevent erasing

Locking Clone Source

Disks that are planned to be used as master copy for Disk Clone on page 44 could be marked in Disk Bay Layout by selecting Disk Bay and clicking **Clone Source** from the **Change disk bay attributes** drop down menu. Hence, disks marked this way will be protected from accidental destruction and also will be available in devices' list as source for disk cloning.

Auto Erase

Auto Erase feature is designed to speed up disk wiping process in scenario when many disks must be erased with the same erase attributes with minimum 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 and may cancel this action by selecting Disk Bay widget and clicking **Stop** button in View's toolbar or in context menu.

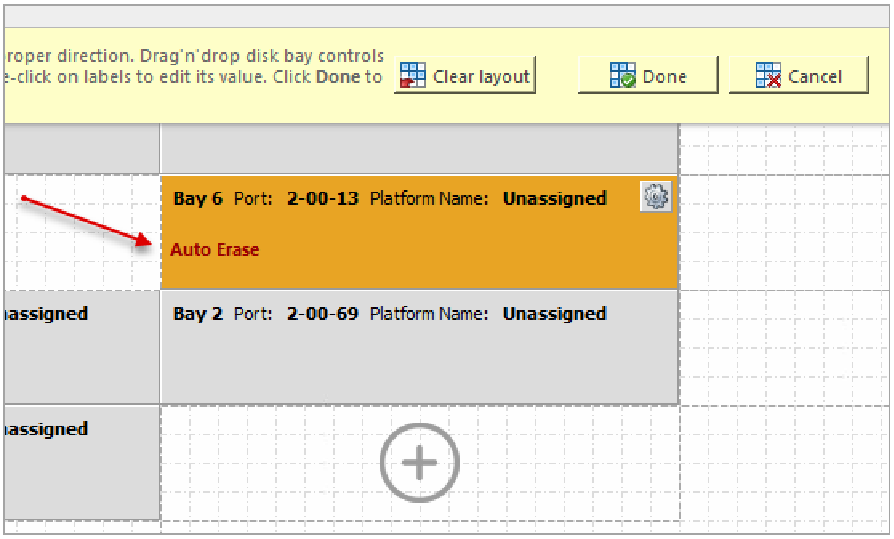

roper direction. Drag'n'drop disk bay controls
-click on labels to edit its value. Click Done to
Clear layout
Done
Cancel
Bay 6 Port: 2-00-13 Platform Name: Unassigned
Auto Erase
Bay 2 Port: 2-00-69 Platform Name: Unassigned
ıassigned
ıassigned

Figure 23: Enabling Auto Erase

CAUTION:

Use this feature with extreme caution - make sure the 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

Click **Done** button to commit any changes to the application View layout.

Note:

Done will apply current change to the application session so the changes will be seen in the Disk Bays View and even be loaded in future application launch. These changes will not affect the *.dbl* file.

Click **Cancel** to revert any changes you made to the layout.

Usage Scenarios

KillDisk Industrial is a powerful industrial tool to provide disk erasure solutions for large workstations being able to erase large volumes of disks. The features in the **KillDisk Industrial** software are built with this goal in mind. This section describes the key features of the software and how they are used to erase single disks to large batches. The software is highly customizable and this guide will help get you started with configuring **KillDisk Industrial** for your system and using it to the full potential.

Note:

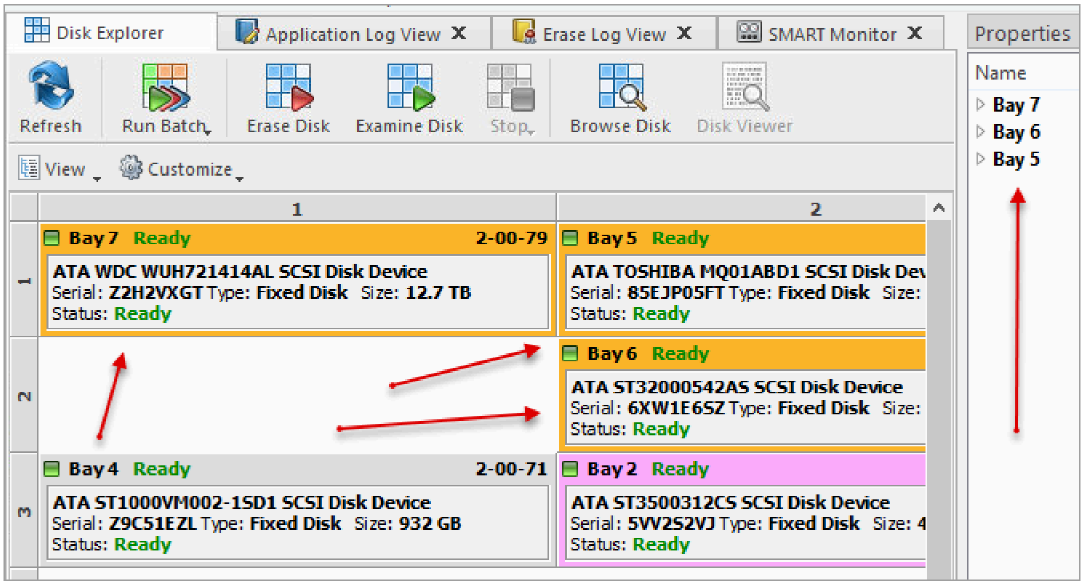
It is important to properly set up your **KillDisk** layout before using any of the features so read and follow the steps to do this in Disk Layout Editor section.

Disk Erase

KillDisk is an extremely powerful tool for disk erasure. Individual disks or batches of disks can be erased according to any desired standard with just a few clicks. The process is described below.

1. Select disks for erasure

   Use Disk Explorer on page 14 to select one or more physical disks or logical volumes. For multiple selection use **Ctrl+Left Mouse** click



Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: **Z2H2VXGT** Type: **Fixed Disk** Size: **12.7 TB**
Status: **Ready**

Bay 5 Ready
ATA TOSHIBA MQ01ABD1 SCSI Disk Dev
Serial: **85EJP05FT** Type: **Fixed Disk** Size:
Status: **Ready**

Bay 6 Ready
ATA ST32000542AS SCSI Disk Device
Serial: **6XW1E6SZ** Type: **Fixed Disk** Size:
Status: **Ready**

Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: **Z9C51EZL** Type: **Fixed Disk** Size: **932 GB**
Status: **Ready**

Bay 2 Ready
ATA ST3500312CS SCSI Disk Device
Serial: **5VV2S2VJ** Type: **Fixed Disk** Size: 4
Status: **Ready**

Figure 24: Multiple bay selection

2. Open Disk Erase dialog using one of the following methods:
   - Click **Erase Disk** command on 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

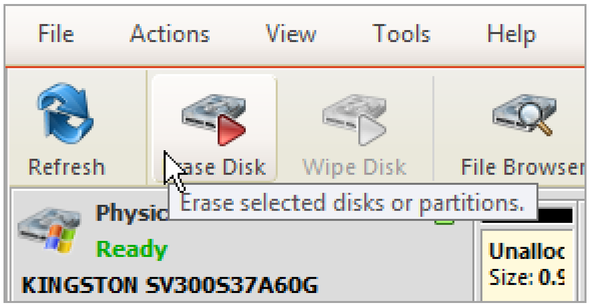
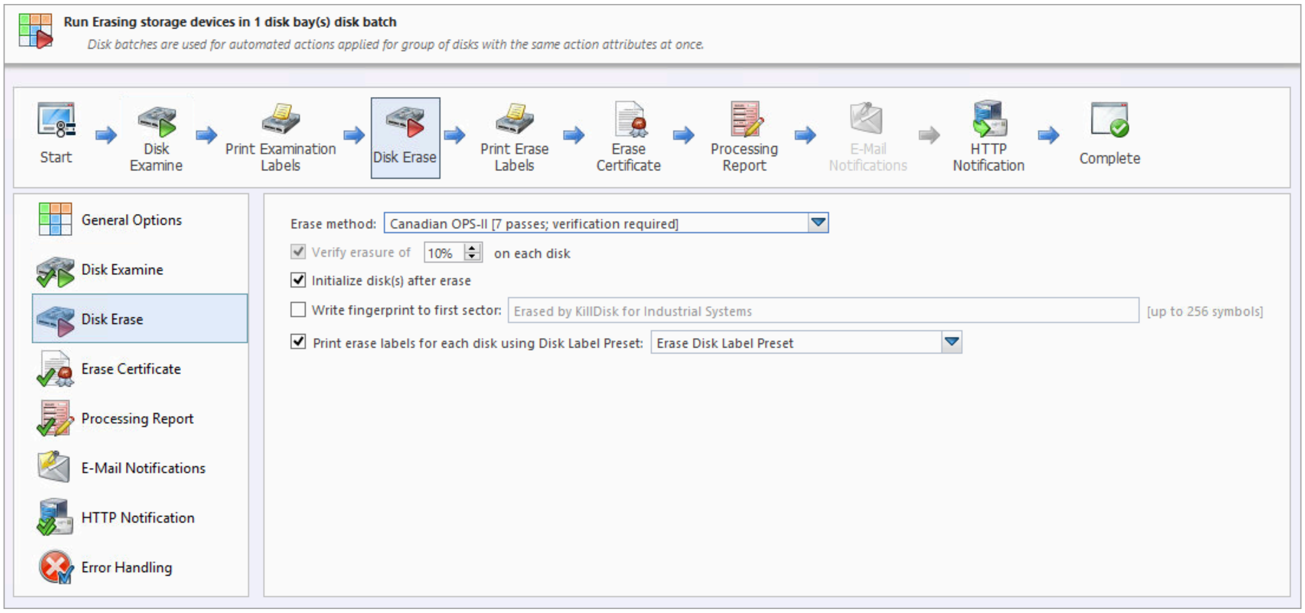


Figure 25: Initiating the Erase operation

3. Confirm erasure options

Disk Erase options dialog pops up:



Run Erasing storage devices in 1 disk bay(s) disk batch

Disk batches are used for automated actions applied for group of disks with the same action attributes at once.

Erase method: Canadian OPS-II [7 passes; verification required]

☑ Verify erasure of 10% on each disk

☑ Initialize disk(s) after erase

☐ Write fingerprint to first sector: Erased by KillDisk for Industrial Systems [up to 256 symbols]

☑ Print erase labels for each disk using Disk Label Preset: Erase Disk Label Preset

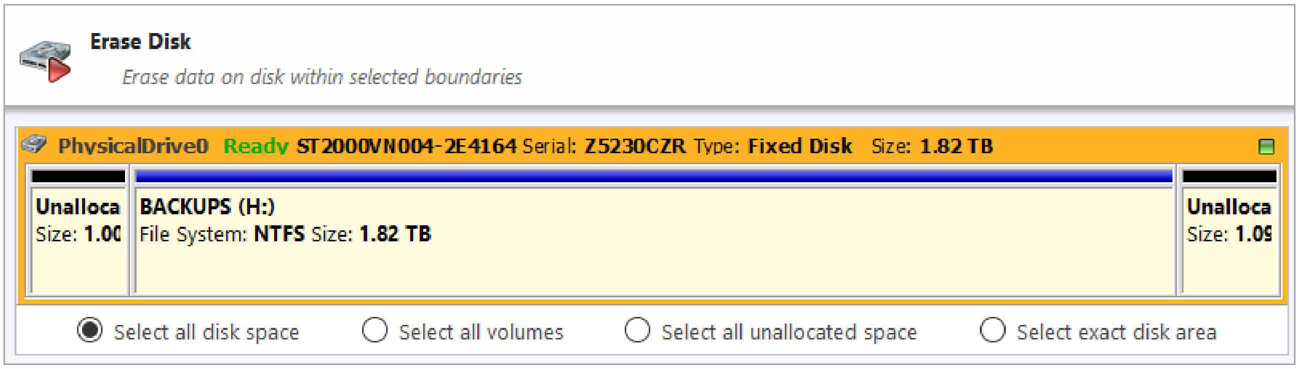
Figure 26: Disk Erase Options

Use tabbed Views to adjust disk erasure options if necessary. Options available are:

- General Settings on page 99
- Disk Examine on page 107
- Disk Erase on page 103
- Erase Certificate on page 111
- Processing Report on page 115
- E-mail Notifications on page 126
- HTTP Notifications on page 128
- Disk Label Presets on page 119
- Error Handling on page 125

Use Disk Examine on page 107 page in application preferences to specify disk grading attributes if necessary.

If single disk is selected by **Erase Disk** command a disk area to be erased can be specified:



Erase Disk

Erase data on disk within selected boundaries

PhysicalDrive0 Ready ST2000VN004-2E4164 Serial: Z5230CZR Type: Fixed Disk Size: 1.82 TB

Unalloca Size: 1.00

BACKUPS (H:) File System: NTFS Size: 1.82 TB

Unalloca Size: 1.09

● Select all disk space ○ Select all volumes ○ Select all unallocated space ○ Select exact disk area

Figure 27: 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 space where the live volumes located

Select all unallocated space

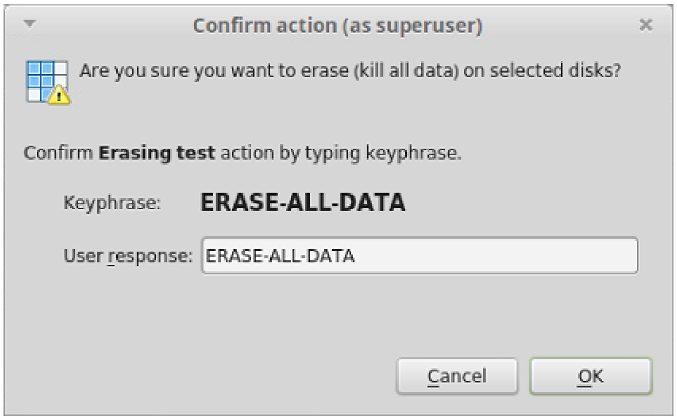
Select for erase the only disk unallocated area (the space where no live volumes exist)

Select exact disk area

Allows you to use 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 partitions will be erased.

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



Confirm action (as superuser)

Are you sure you want to erase (kill all data) on selected disks?

Confirm **Erasing test** action by typing keyphrase.

Keyphrase: **ERASE-ALL-DATA**

User response: ERASE-ALL-DATA

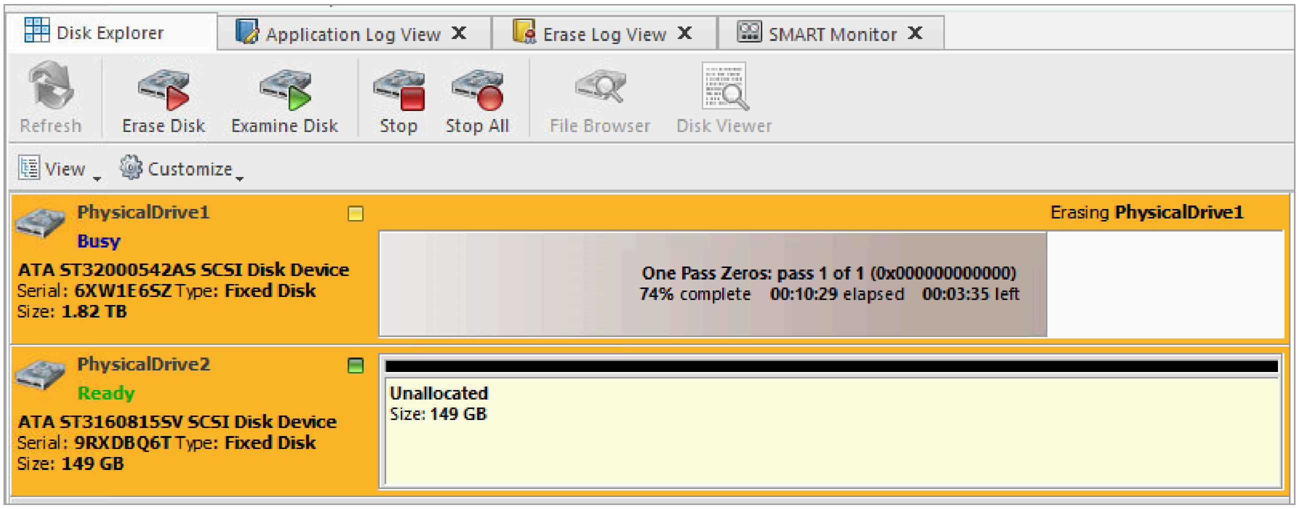
Figure 28: Disk Erase Confirmation

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

4. Observe erase process

   If Disk Examine on page 107 was selected then a disk examination will start first. Depending on examination at the second stage - disk erase begins.

   When the *Erase Disk* procedure begins you see the disk area representation as a progress bar as well as an erase method and its progress. The progress bar represents the percentage of disk space processed. As the procedure progresses the percentage increases and estimated time recalculated.



PhysicalDrive1
Busy
ATA ST32000542AS SCSI Disk Device
Serial: 6XW1E6SZ Type: Fixed Disk
Size: 1.82 TB

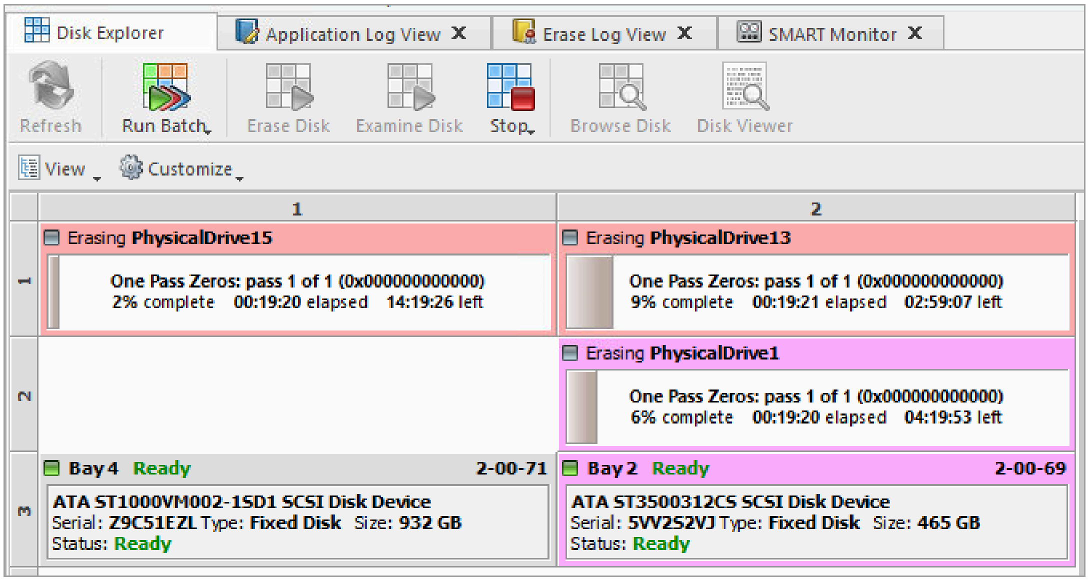
Erasing PhysicalDrive1

One Pass Zeros: pass 1 of 1 (0x000000000000)
74% complete 00:10:29 elapsed 00:03:35 left

PhysicalDrive2
Ready
ATA ST3160815SV SCSI Disk Device
Serial: 9RXDBQ6T Type: Fixed Disk
Size: 149 GB

Unallocated
Size: 149 GB

Figure 29: Disk Erase Progress (Local Devices View)



Erasing PhysicalDrive15
One Pass Zeros: pass 1 of 1 (0x000000000000)
2% complete 00:19:20 elapsed 14:19:26 left

Erasing PhysicalDrive13
One Pass Zeros: pass 1 of 1 (0x000000000000)
9% complete 00:19:21 elapsed 02:59:07 left

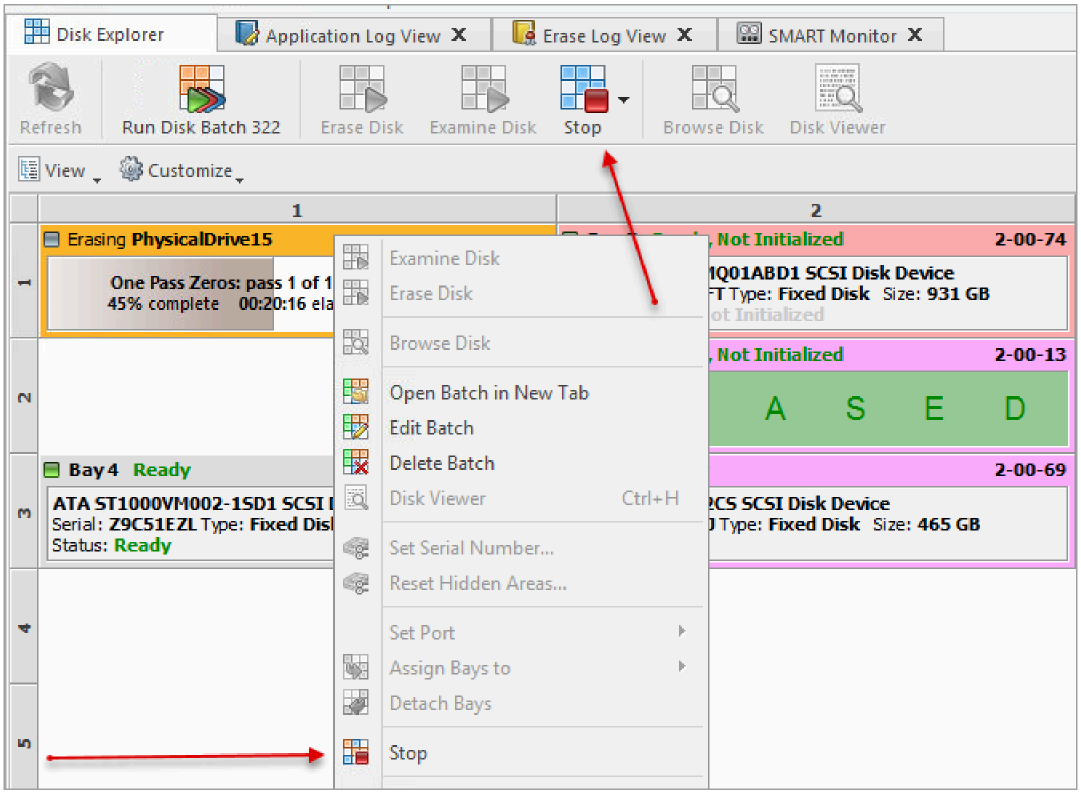
Erasing PhysicalDrive1
One Pass Zeros: pass 1 of 1 (0x000000000000)
6% complete 00:19:20 elapsed 04:19:53 left

Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: Z9C51EZL Type: Fixed Disk Size: 932 GB
Status: Ready

Bay 2 Ready 2-00-69
ATA ST3500312CS SCSI Disk Device
Serial: 5VV2S2VJ Type: Fixed Disk Size: 465 GB
Status: Ready

Figure 30: Disk Erase Progress (Disk Bays View)

User can **Stop** erase process at any time (via action toolbar, main menu or context menu) :



Erasing PhysicalDrive15

One Pass Zeros: pass 1 of 1
45% complete 00:20:16 ela

Bay 4 Ready

ATA ST1000VM002-1SD1 SCSI I
Serial: Z9C51EZL Type: Fixed Disl
Status: Ready

, Not Initialized 2-00-74

1Q01ABD1 SCSI Disk Device
FT Type: Fixed Disk Size: 931 GB
ot Initialized

, Not Initialized 2-00-13

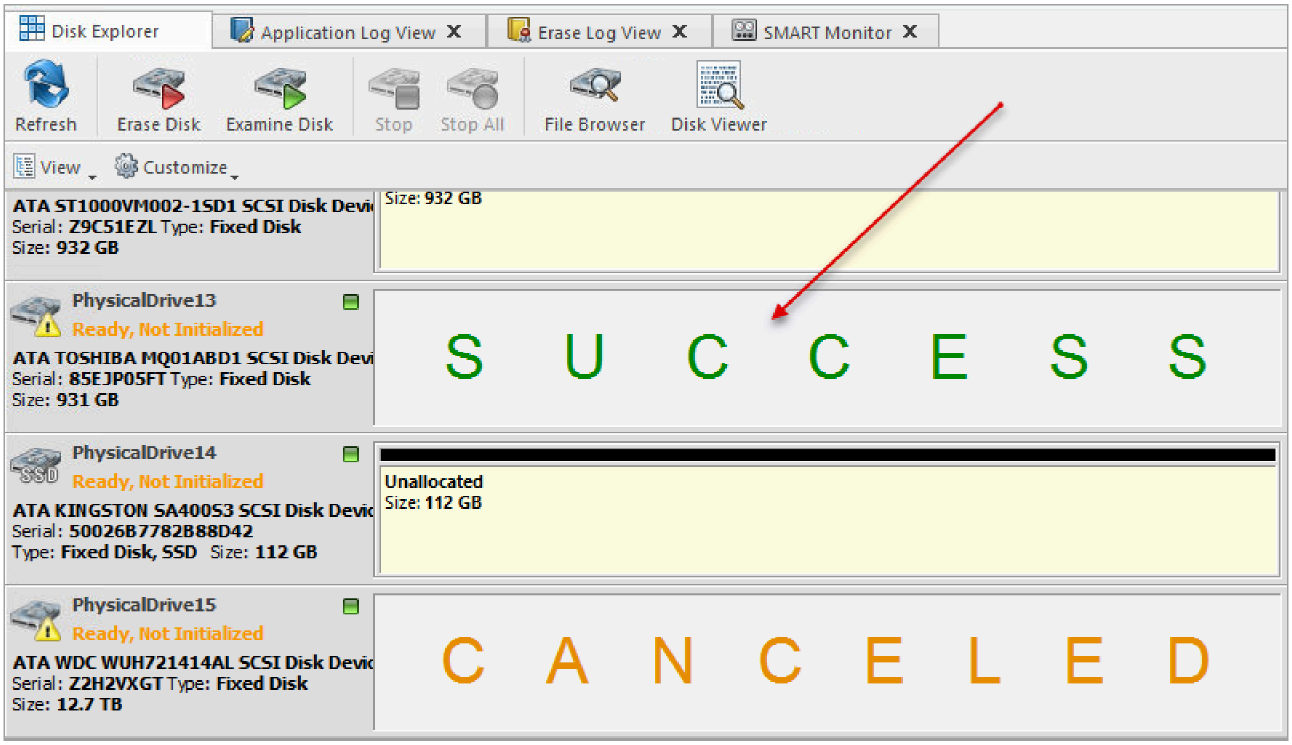
A S E D

2-00-69

2CS SCSI Disk Device
J Type: Fixed Disk Size: 465 GB

Figure 31: Stopping Erase

After Erase is complete for the particular disk, its status is displayed on Disk Bays:



ATA ST1000VM002-1SD1 SCSI Disk Devi
Serial: Z9C51EZL Type: Fixed Disk
Size: 932 GB

Size: 932 GB

PhysicalDrive13
Ready, Not Initialized
ATA TOSHIBA MQ01ABD1 SCSI Disk Devi
Serial: 85EJP05FT Type: Fixed Disk
Size: 931 GB

S U C C E S S

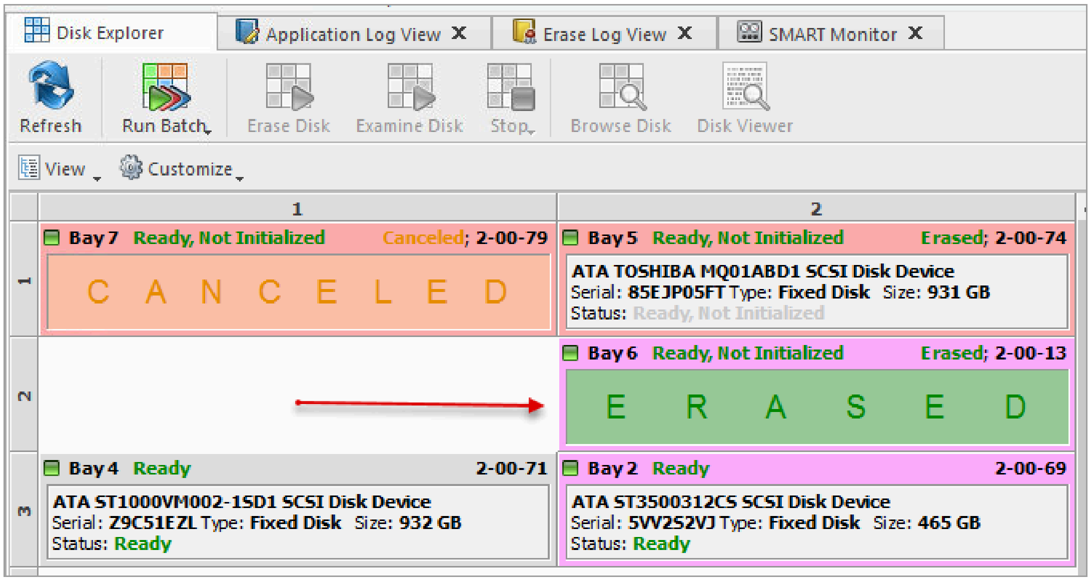
PhysicalDrive14
Ready, Not Initialized
ATA KINGSTON SA400S3 SCSI Disk Devic
Serial: 50026B7782B88D42
Type: Fixed Disk, SSD Size: 112 GB

Unallocated
Size: 112 GB

PhysicalDrive15
Ready, Not Initialized
ATA WDC WUH721414AL SCSI Disk Devic
Serial: Z2H2VXGT Type: Fixed Disk
Size: 12.7 TB

C A N C E L E D

Figure 32: Erase Completed (Local Devices View)

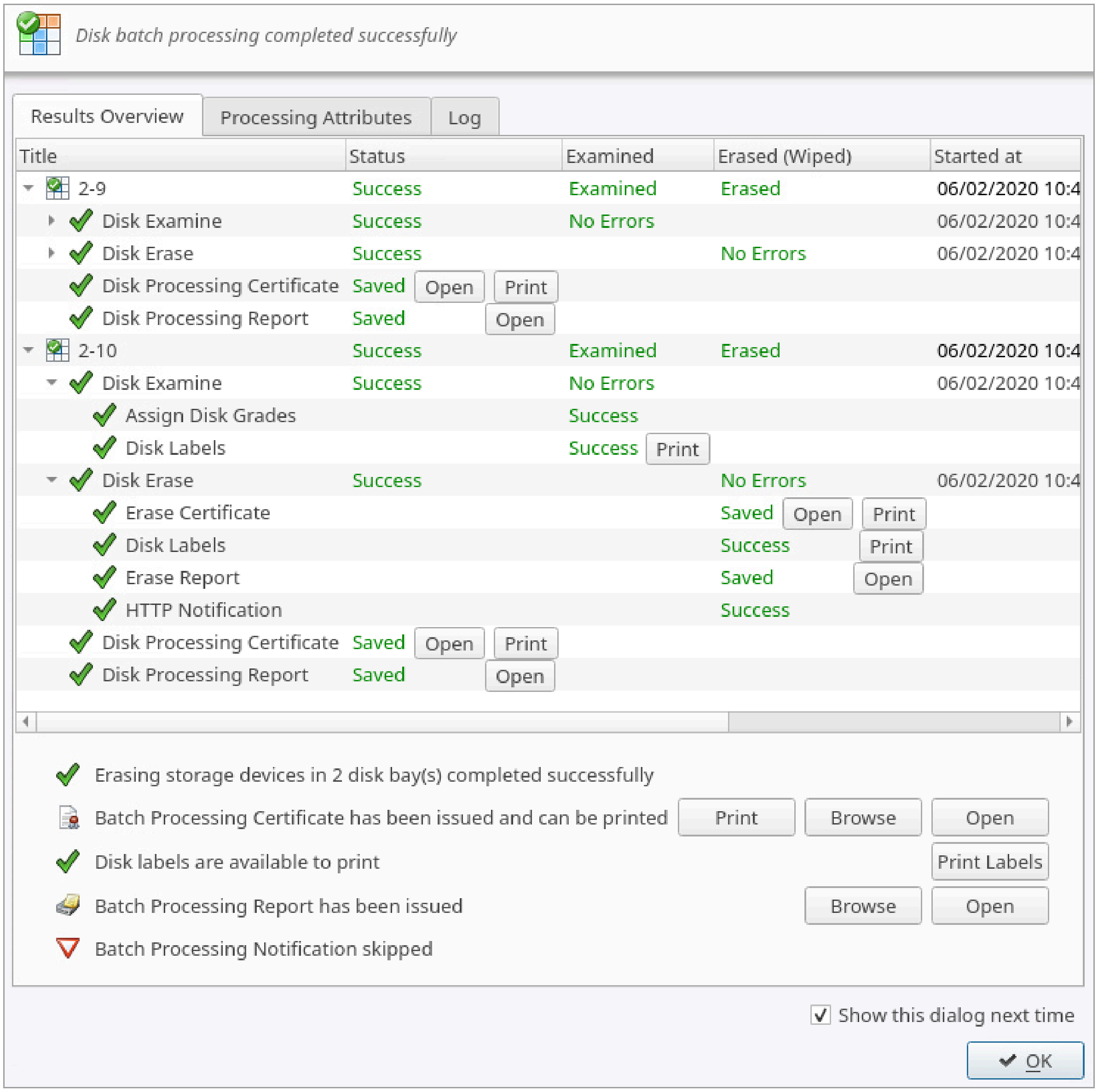


	1	2
1	Bay 7 Ready, Not Initialized Canceled; 2-00-79 CANCELED	Bay 5 Ready, Not Initialized Erased; 2-00-74 ATA TOSHIBA MQ01ABD1 SCSI Disk Device Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB Status: Ready, Not Initialized
2		Bay 6 Ready, Not Initialized Erased; 2-00-13 ERASED
3	Bay 4 Ready 2-00-71 ATA ST1000VM002-1SD1 SCSI Disk Device Serial: Z9C51EZL Type: Fixed Disk Size: 932 GB Status: Ready	Bay 2 Ready 2-00-69 ATA ST3500312CS SCSI Disk Device Serial: 5VV2S2VJ Type: Fixed Disk Size: 465 GB Status: Ready

Figure 33: Erase Completed (Disk Bays Views)

If Disk Clone on page 44 was selected then after erasing the final stage begins: data cloning from source to all the successfully erased disks.

When erase is completed user is able to review results (logs, processing reports and attributes), print Erase Certificates and Disk Labels for processed disks.



Disk batch processing completed successfully

Title	Status	Examined	Erased (Wiped)	Started at
2-9	Success	Examined	Erased	06/02/2020 10:4
Disk Examine	Success	No Errors		06/02/2020 10:4
Disk Erase	Success		No Errors	06/02/2020 10:4
Disk Processing Certificate	Saved Open Print			
Disk Processing Report	Saved Open			
2-10	Success	Examined	Erased	06/02/2020 10:4
Disk Examine	Success	No Errors		06/02/2020 10:4
Assign Disk Grades		Success		
Disk Labels		Success Print		
Disk Erase	Success		No Errors	06/02/2020 10:4
Erase Certificate			Saved Open Print	
Disk Labels			Success Print	
Erase Report			Saved Open	
HTTP Notification			Success	
Disk Processing Certificate	Saved Open Print			
Disk Processing Report	Saved Open			

✓ Erasing storage devices in 2 disk bay(s) completed successfully

Batch Processing Certificate has been issued and can be printed

✓ Disk labels are available to print

Batch Processing Report has been issued

Batch Processing Notification skipped

☑ Show this dialog next time

Figure 34: Erase Summary

Related information

Erase Methods (Sanitation Standards) on page 151

Processing Summary on page 51

Certificates, Labels and Reports on page 54

Disk Wipe

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

Note:

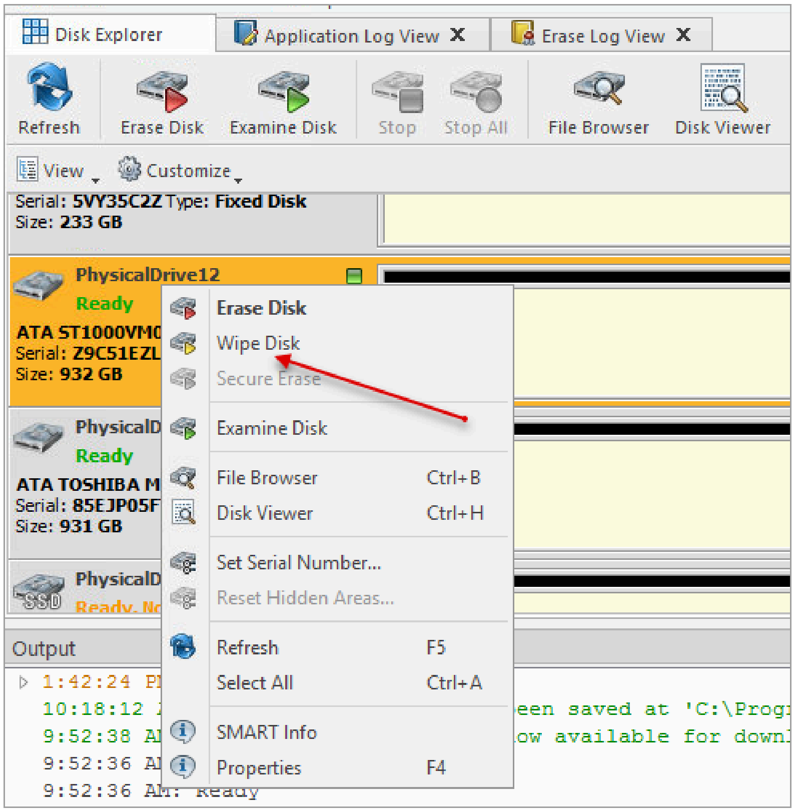
If you want to erase ALL data (existing and deleted) from the hard drive device permanently, see Disk Erase on page 28.

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

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

1. Select a disk or volume to wipe out in **Disk Explorer** > **Local Devices View**

   You may select multiple disks/volumes to be wiped out simultaneously.
2. Execute **Wipe Disk** command from **Actions** menu (or use the context menu)



Serial: **5VY35C2Z** Type: **Fixed Disk**
Size: **233 GB**

PhysicalDrive12
Ready
ATA ST1000VM0
Serial: **Z9C51EZL**
Size: **932 GB**

PhysicalD
Ready
ATA TOSHIBA M
Serial: **85EJP05F**
Size: **931 GB**

PhysicalD
Ready, No

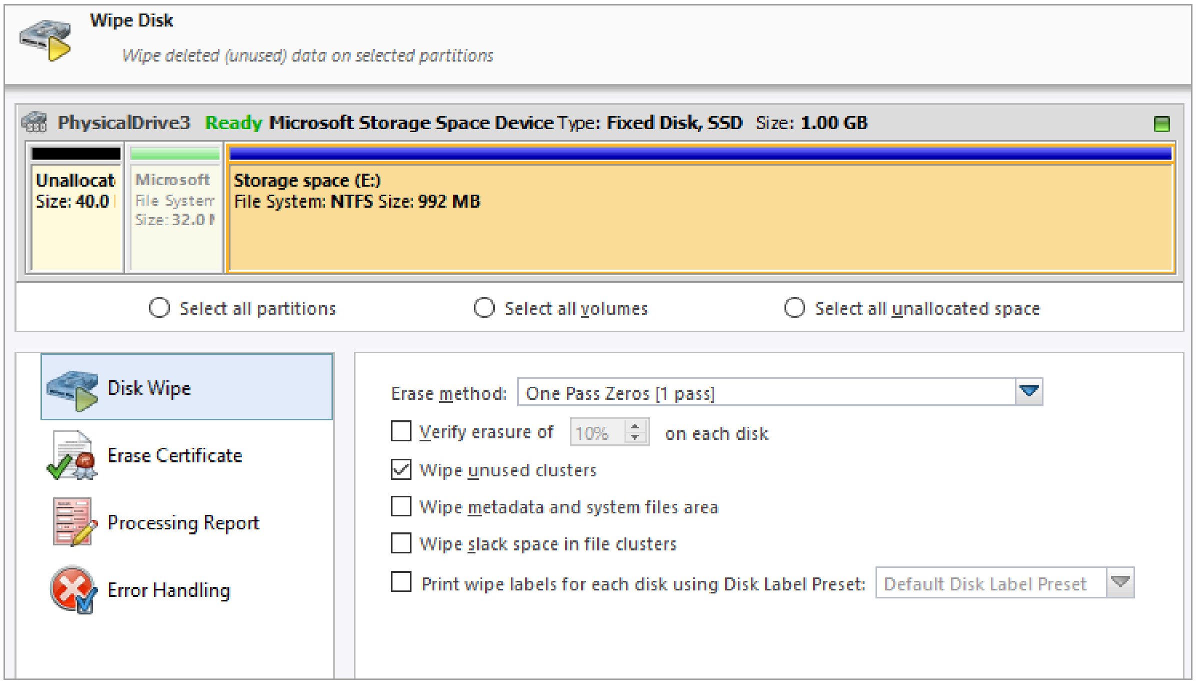
```
▷ 1:42:24 PI
  10:18:12 /                                   een saved at 'C:\Prog
  9:52:38 AI                                   ow available for downl
  9:52:36 AI
  9:52:36 AM: Ready
```

Figure 35: Initiating the Wipe operation

3. Confirm Wipe Options

Use tabbed views to adjust Disk Wipe options if necessary. Available options are:

- Examine Disk Physical Integrity on page 39
- Disk Wipe on page 106
- Erase Certificate on page 111
- Processing Report on page 115
- E-mail Notifications on page 126
- Disk Label Presets on page 119
- Error Handling on page 125



Wipe Disk

Wipe deleted (unused) data on selected partitions

PhysicalDrive3 Ready Microsoft Storage Space Device Type: Fixed Disk, SSD Size: 1.00 GB

Unallocat Size: 40.0 | Microsoft File Systen Size: 32.0 | Storage space (E:) File System: NTFS Size: 992 MB

○ Select all partitions ○ Select all volumes ○ Select all unallocated space

Erase method: One Pass Zeros [1 pass]

□ Verify erasure of 10% on each disk

☑ Wipe unused clusters

□ Wipe metadata and system files area

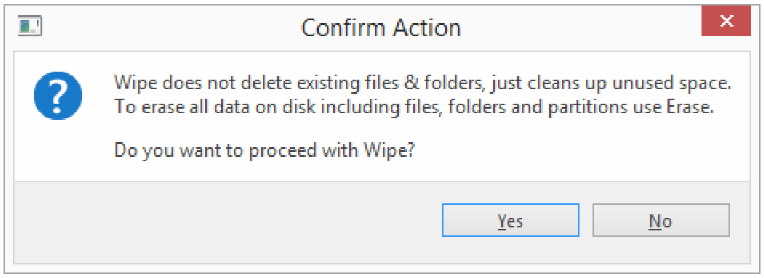
□ Wipe slack space in file clusters

□ Print wipe labels for each disk using Disk Label Preset: Default Disk Label Preset

Figure 36: Selecting erase method

4. Select the areas of the disks to be wiped. For each disk you can select individual partitions.

5. Click **Start** to reach the final step before erasing data. Confirm **Wipe** action and process starts.



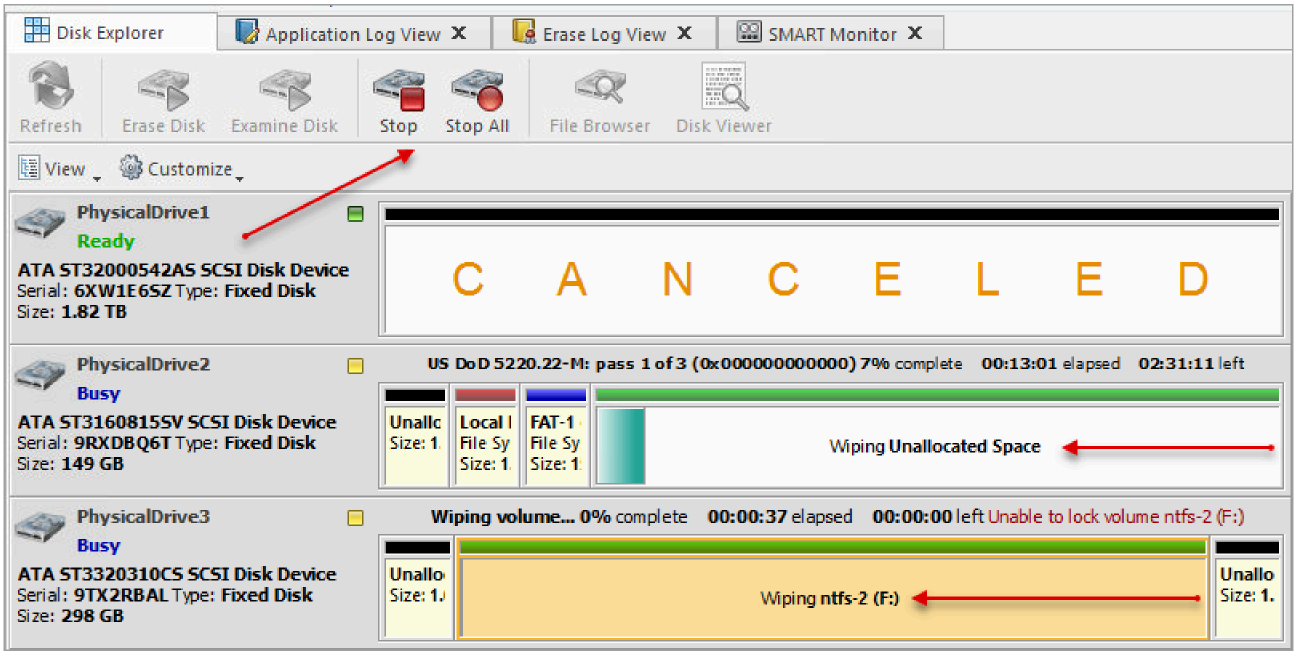
Confirm Action

Wipe does not delete existing files & folders, just cleans up unused space.
To erase all data on disk including files, folders and partitions use Erase.

Do you want to proceed with Wipe?

6. The progress of the wiping procedure will be monitored.

To stop the process at any time click the **Stop** button for a particular disk. Click the **Stop All** button to cancel wiping for all selected disks. Please note that all the existing applications and data will not be touched. The data that has been wiped from unoccupied sectors is not recoverable.

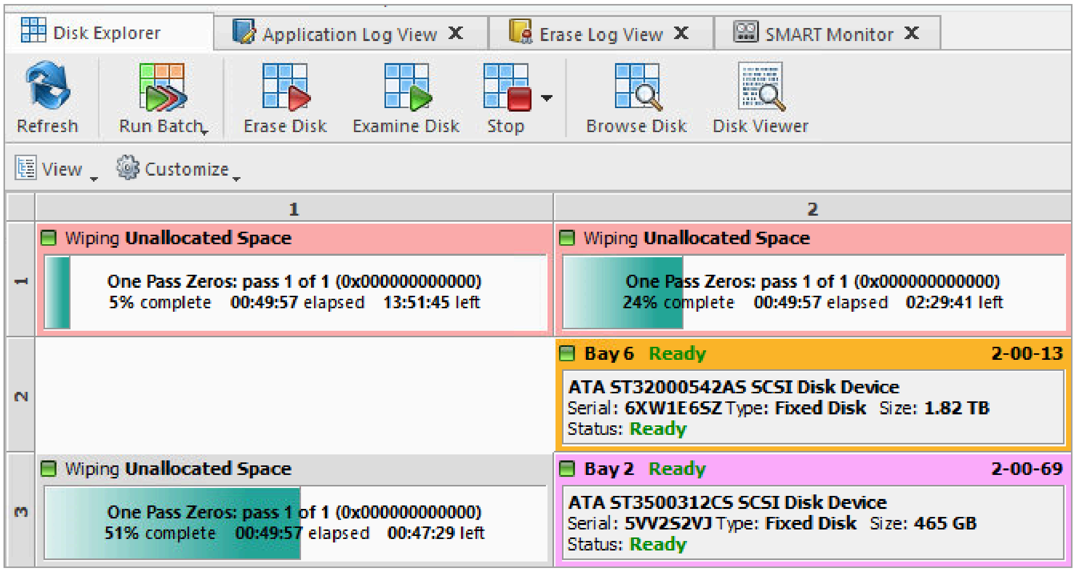


PhysicalDrive1
Ready
ATA ST32000542AS SCSI Disk Device
Serial: 6XW1E6SZ Type: Fixed Disk
Size: 1.82 TB
C A N C E L E D

PhysicalDrive2
Busy
ATA ST3160815SV SCSI Disk Device
Serial: 9RXDBQ6T Type: Fixed Disk
Size: 149 GB
US DoD 5220.22-M: pass 1 of 3 (0x000000000000) 7% complete 00:13:01 elapsed 02:31:11 left
Unallc Size: 1.
Local I File Sy Size: 1.
FAT-1 File Sy Size: 1.
Wiping Unallocated Space

PhysicalDrive3
Busy
ATA ST3320310CS SCSI Disk Device
Serial: 9TX2RBAL Type: Fixed Disk
Size: 298 GB
Wiping volume... 0% complete 00:00:37 elapsed 00:00:00 left Unable to lock volume ntfs-2 (F:)
Unallo Size: 1.
Wiping ntfs-2 (F:)
Unallo Size: 1.

Figure 37: Disk Wipe Progress (Local Devices View)



Wiping Unallocated Space
One Pass Zeros: pass 1 of 1 (0x000000000000)
5% complete 00:49:57 elapsed 13:51:45 left

Wiping Unallocated Space
One Pass Zeros: pass 1 of 1 (0x000000000000)
24% complete 00:49:57 elapsed 02:29:41 left

Bay 6 Ready 2-00-13
ATA ST32000542AS SCSI Disk Device
Serial: 6XW1E6SZ Type: Fixed Disk Size: 1.82 TB
Status: Ready

Wiping Unallocated Space
One Pass Zeros: pass 1 of 1 (0x000000000000)
51% complete 00:49:57 elapsed 00:47:29 left

Bay 2 Ready 2-00-69
ATA ST3500312CS SCSI Disk Device
Serial: 5VV2S2VJ Type: Fixed Disk Size: 465 GB
Status: Ready

Figure 38: Disk Wipe Progress (Disk Bays View)

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

KillDisk scans the system/root records of the partition. The **Browser** tab appears. Existing file/folder names appear with a multicolor icon and deleted file/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/system records has been removed. You should not see any gray-colored file names or folder names in the wiped partition.

You will see a confirmation dialog when the process is complete. Now you may print Erase Certificates on page 54.

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.

Related information

Disk Wipe on page 106

Processing Summary on page 51

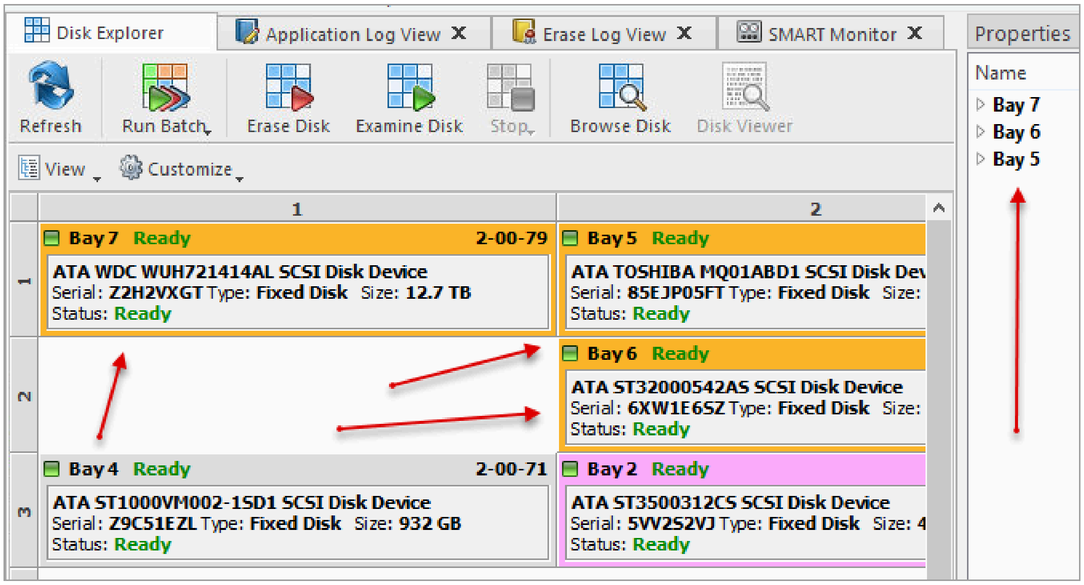
Certificates, Labels and Reports on page 54

Examine Disk Physical Integrity

Disk examination feature is designed to scan the physical integrity of the disks. **Disk Examine** step can be the preliminary step to **Disk Erase**, **Disk Wipe** or **Disk Clone** procedures.

1. Select disks or volumes for examination

Use Disk Explorer on page 14 to select one or more physical disks or logical volumes. For multiple selection use **Ctrl+Left Mouse** click



Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed Disk Size: 12.7 TB
Status: Ready

Bay 5 Ready
ATA TOSHIBA MQ01ABD1 SCSI Disk Dev
Serial: 85EJP05FT Type: Fixed Disk Size:
Status: Ready

Bay 6 Ready
ATA ST32000542AS SCSI Disk Device
Serial: 6XW1E6SZ Type: Fixed Disk Size:
Status: Ready

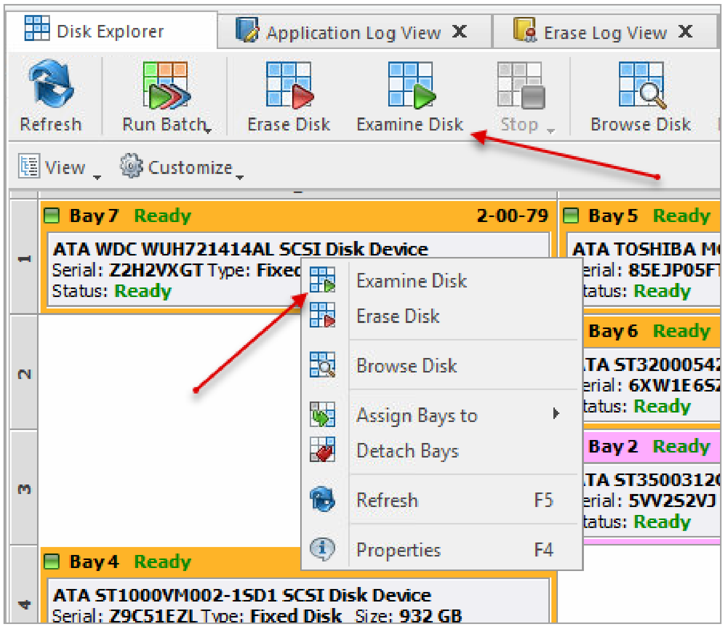
Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: Z9C51EZL Type: Fixed Disk Size: 932 GB
Status: Ready

Bay 2 Ready
ATA ST3500312CS SCSI Disk Device
Serial: 5VV2S2VJ Type: Fixed Disk Size: 4
Status: Ready

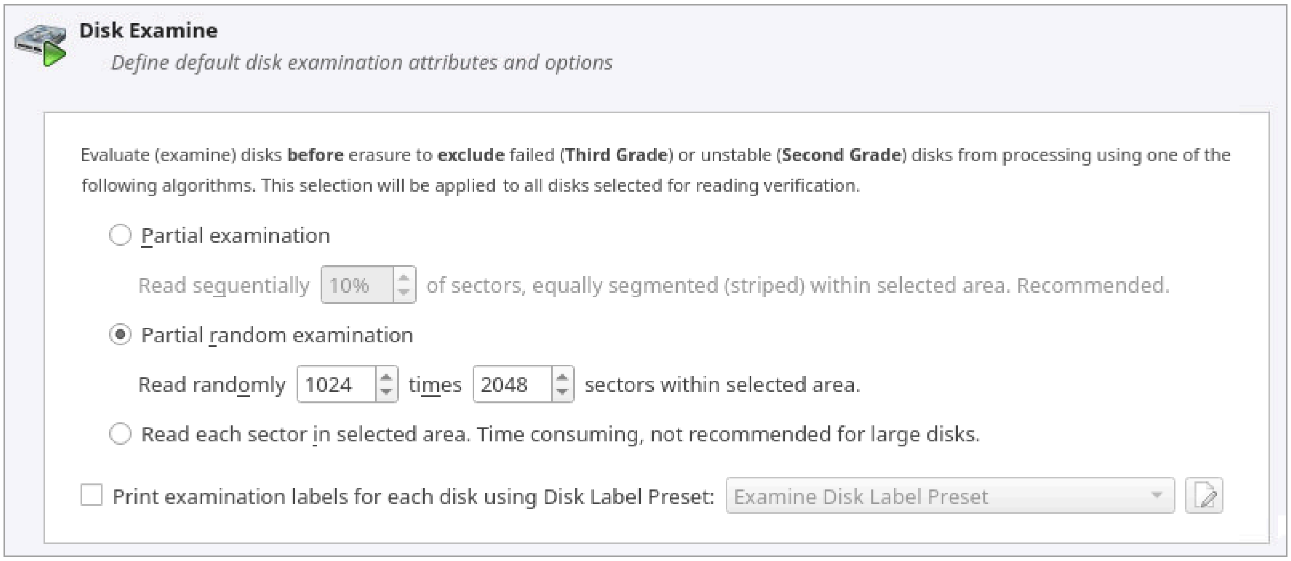
Figure 39: Multiple bay selection

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

   - Click the **Examine Disk** command on the action toolbar
   - Click **Actions** > **Examine Disk** command from main menu
   - Click **Examine Disk** command from context menu



   - Click **Run Batch** > **Named Batch** command from toolbar or from **Actions** main menu to examine disks in predefined disk batch



Disk Examine

Define default disk examination attributes and options

Evaluate (examine) disks **before** erasure to **exclude** failed (**Third Grade**) or unstable (**Second Grade**) disks from processing using one of the following algorithms. This selection will be applied to all disks selected for reading verification.

○ Partial examination

Read sequentially 10% of sectors, equally segmented (striped) within selected area. Recommended.

● Partial random examination

Read randomly 1024 times 2048 sectors within selected area.

○ Read each sector in selected area. Time consuming, not recommended for large disks.

☐ Print examination labels for each disk using Disk Label Preset: Examine Disk Label Preset

Figure 40: Examine Disk Options

3. Confirm examination options

   Use tabbed views to adjust examination options if necessary. Available options are:

   - Disk Examine on page 107
   - Processing Report on page 115
   - Error Handling on page 125

   Use Disk Examine on page 107 in application preferences to specify disk grading attributes if necessary.

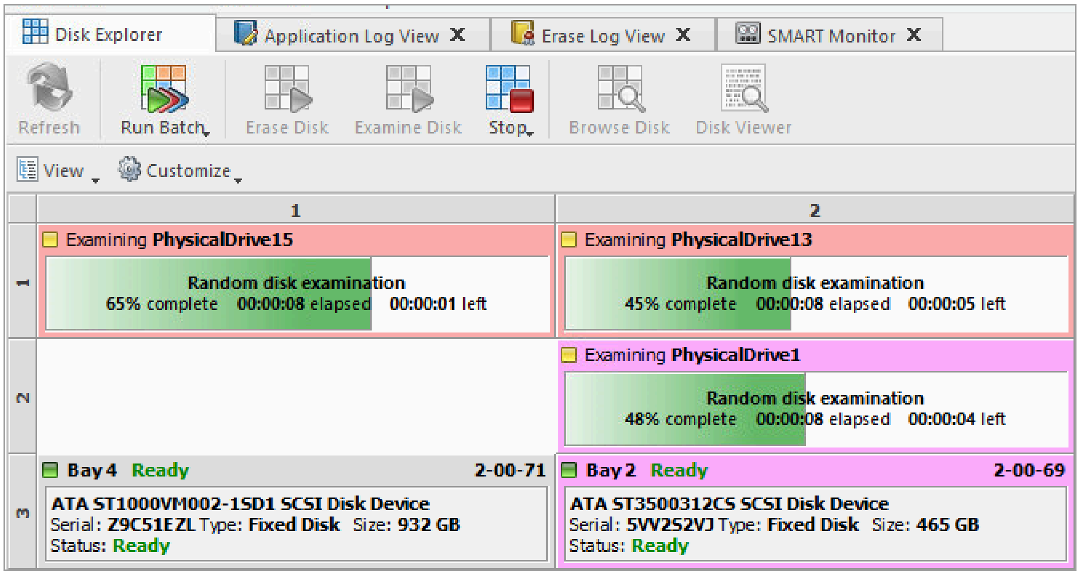
   Note:

   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 14 you will see the progress of the examination in the slot of the drive being operated on. The process will be shown as a progress bar:



Examining **PhysicalDrive15**
Random disk examination
65% complete 00:00:08 elapsed 00:00:01 left

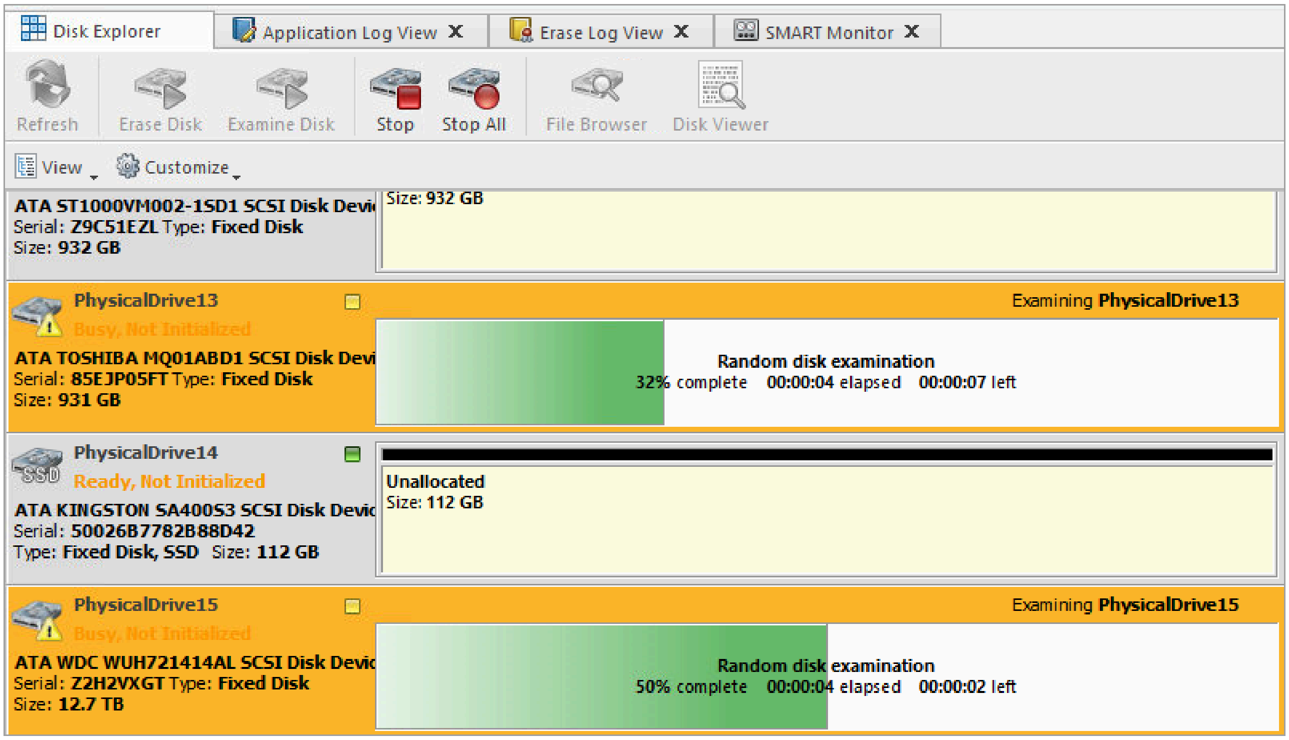
Examining **PhysicalDrive13**
Random disk examination
45% complete 00:00:08 elapsed 00:00:05 left

Examining **PhysicalDrive1**
Random disk examination
48% complete 00:00:08 elapsed 00:00:04 left

Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: **Z9C51EZL** Type: **Fixed Disk** Size: **932 GB**
Status: **Ready**

Bay 2 Ready 2-00-69
ATA ST3500312CS SCSI Disk Device
Serial: **5VV252VJ** Type: **Fixed Disk** Size: **465 GB**
Status: **Ready**

Figure 41: Examination progress (Disk Bays View)



ATA ST1000VM002-1SD1 SCSI Disk Devi
Serial: **Z9C51EZL** Type: **Fixed Disk**
Size: **932 GB**
Size: 932 GB

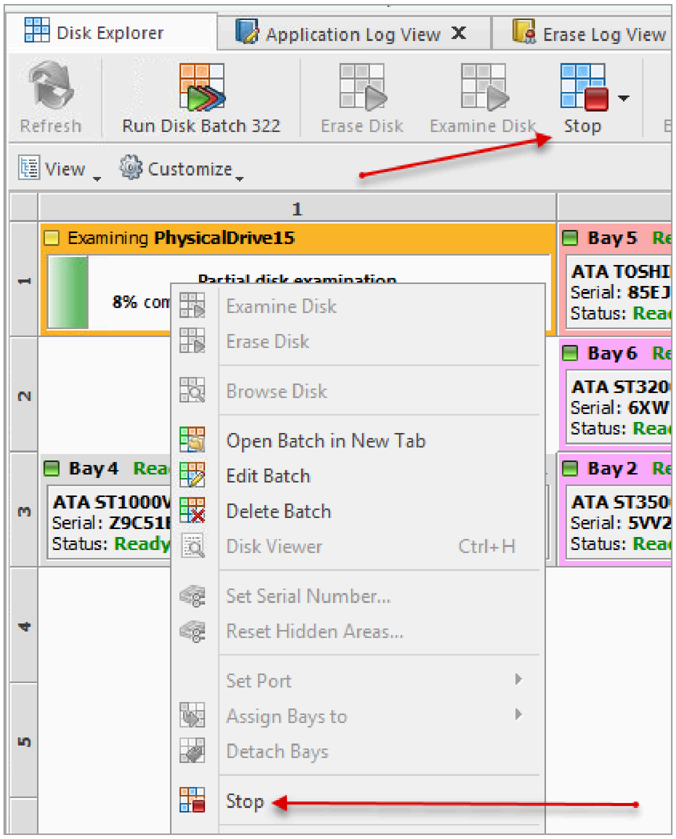
PhysicalDrive13
Busy, Not Initialized
ATA TOSHIBA MQ01ABD1 SCSI Disk Devi
Serial: **85EJP05FT** Type: **Fixed Disk**
Size: **931 GB**
Examining **PhysicalDrive13**
Random disk examination
32% complete 00:00:04 elapsed 00:00:07 left

PhysicalDrive14
Ready, Not Initialized
ATA KINGSTON SA400S3 SCSI Disk Devic
Serial: **50026B7782B88D42**
Type: **Fixed Disk, SSD** Size: **112 GB**
Unallocated
Size: 112 GB

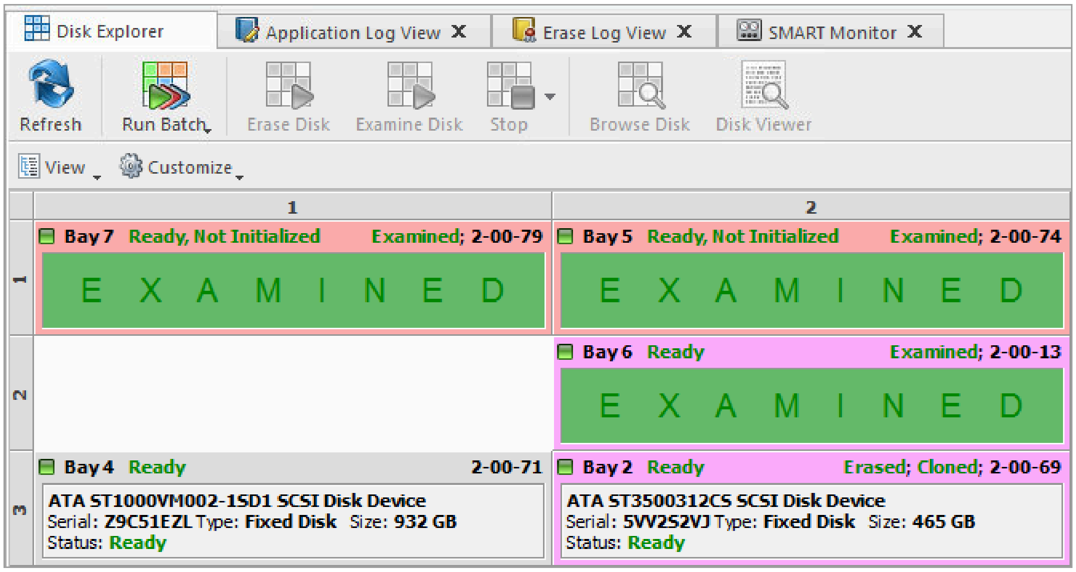
PhysicalDrive15
Busy, Not Initialized
ATA WDC WUH721414AL SCSI Disk Devic
Serial: **Z2H2VXGT** Type: **Fixed Disk**
Size: **12.7 TB**
Examining **PhysicalDrive15**
Random disk examination
50% complete 00:00:04 elapsed 00:00:02 left

Figure 42: Examination progress (Local Devices View)

User is able to **Stop** the process at any time (main menus and context menu) :



As you see the green progress bar fills the virtual drive slot. The percentage of the examination completed and the estimated completion time will also be shown in the slot. Once this process is done the word **EXAMINED** (at Disk Bay View) or **SUCCESS** (at Local Devices View) will flash in the slot space.



Bay 7 Ready, Not Initialized Examined; 2-00-79
EXAMINED

Bay 5 Ready, Not Initialized Examined; 2-00-74
EXAMINED

Bay 6 Ready Examined; 2-00-13
EXAMINED

Bay 4 Ready 2-00-71
ATA ST1000VM002-1SD1 SCSI Disk Device
Serial: Z9C51EZL Type: Fixed Disk Size: 932 GB
Status: Ready

Bay 2 Ready Erased; Cloned; 2-00-69
ATA ST3500312CS SCSI Disk Device
Serial: 5VV2S2VJ Type: Fixed Disk Size: 465 GB
Status: Ready

Figure 43: Examination Completed (Disk Bays View)

When examination is completed user is able to review results (logs, processing reports and attributes) for processed disks and print Disk Labels.

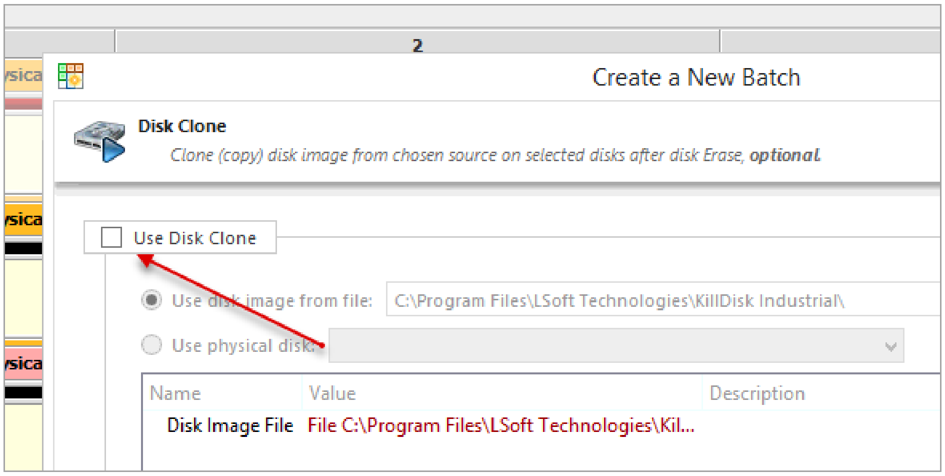
Related information

Disk Examine on page 107

Disk Clone

In addition to 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) navigate to the **Disk Clone** tab when you edit existing Erase Batch or create a new Erase Batch and check the **Use Disk Clone** box, as shown below.



Create a New Batch

Disk Clone

*Clone (copy) disk image from chosen source on selected disks after disk Erase, **optional***

□ Use Disk Clone

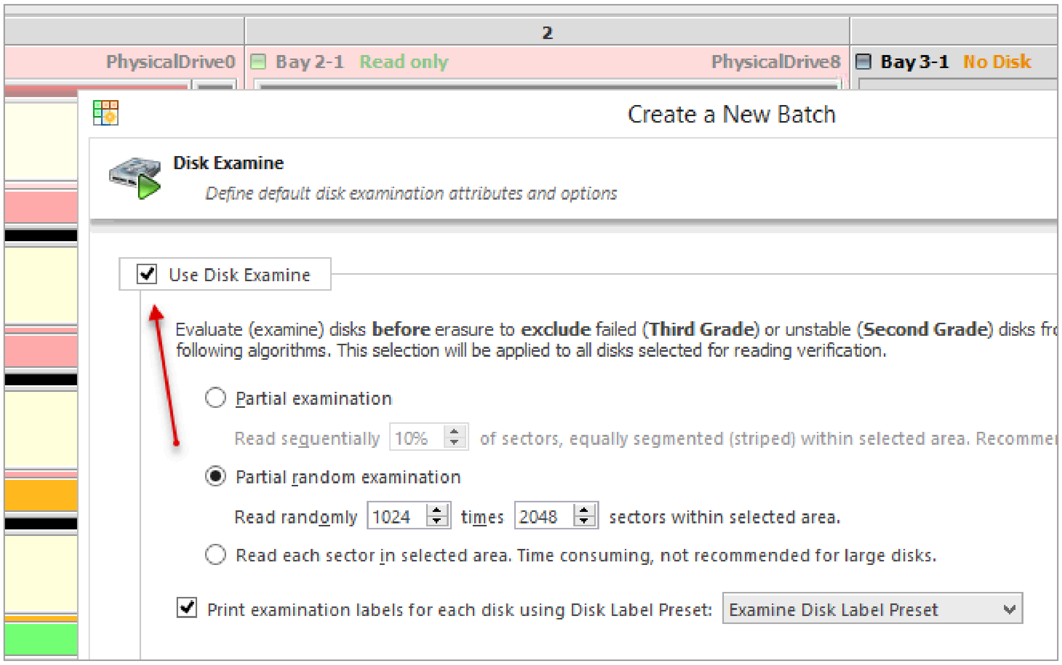
● Use disk image from file: C:\Program Files\LSoft Technologies\KillDisk Industrial\

○ Use physical disk:

Name	Value	Description
Disk Image File	File C:\Program Files\LSoft Technologies\Kil...	

Important:

Make sure the *Use Disk Examine* option is selected on Disk Examine page (as shown below). Otherwise Disk Clone option is avoided in this Wizard as well as in Batch Editing.



Create a New Batch

Disk Examine

Define default disk examination attributes and options

☑ Use Disk Examine

Evaluate (examine) disks **before** erasure to **exclude** failed (**Third Grade**) or unstable (**Second Grade**) disks fr following algorithms. This selection will be applied to all disks selected for reading verification.

○ Partial examination

Read sequentially 10% of sectors, equally segmented (striped) within selected area. Recomme

● Partial random examination

Read randomly 1024 times 2048 sectors within selected area.

○ Read each sector in selected area. Time consuming, not recommended for large disks.

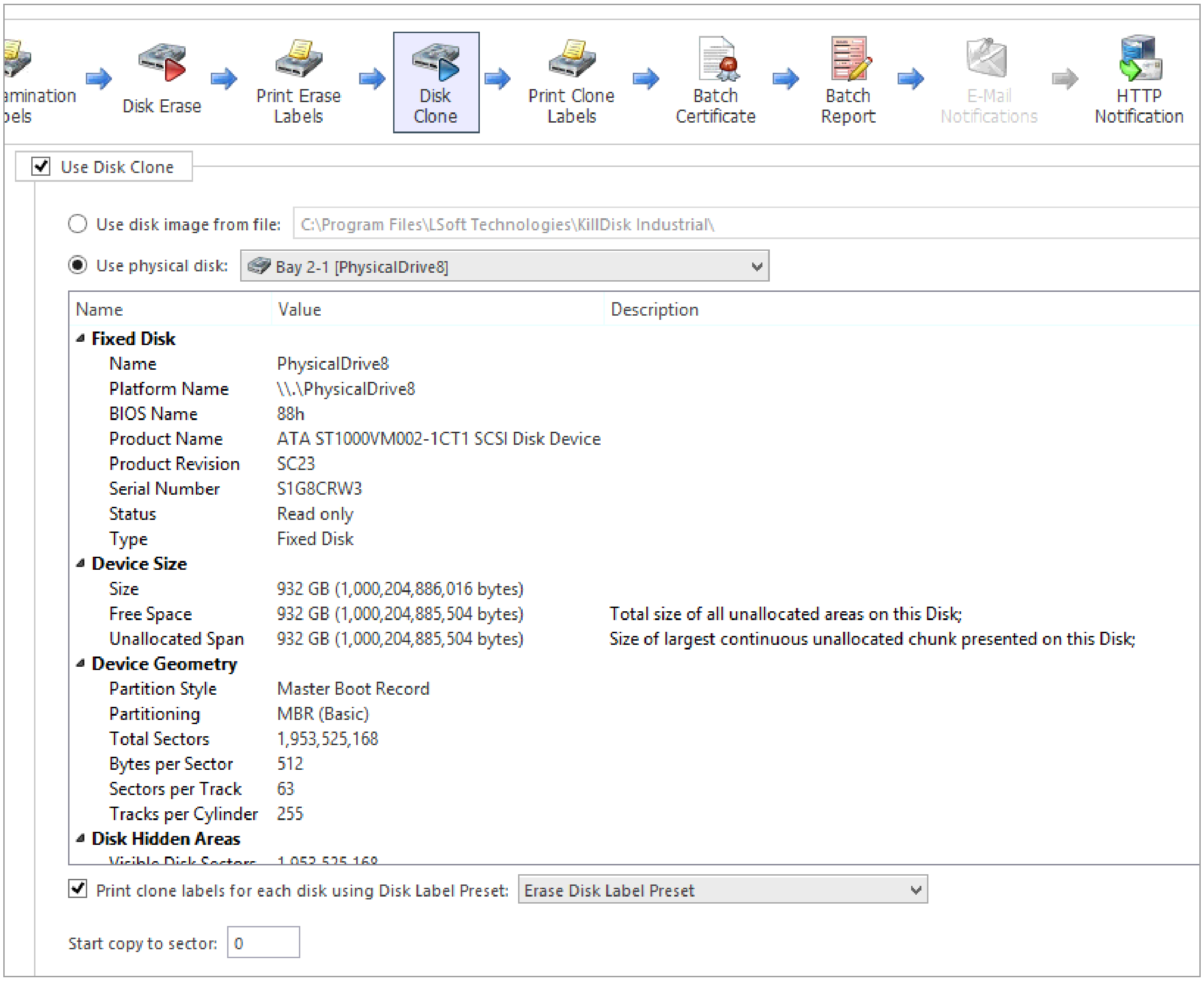
☑ Print examination labels for each disk using Disk Label Preset: Examine Disk Label Preset

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 Clone Sources on page 109.

To configure a source image/disk for **Disk Clone** operation in Erase Batch:

1. Navigate to the Disk Clone tab in the Erase 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 from. If unsure leave as '0'
4. Optional: if you need to print a label, choose a proper Disk Label Preset



☑ Use Disk Clone

○ Use disk image from file: C:\Program Files\LSoft Technologies\KillDisk Industrial\

● Use physical disk: Bay 2-1 [PhysicalDrive8]

Name	Value	Description
Fixed Disk		
Name	PhysicalDrive8	
Platform Name	\\.\PhysicalDrive8	
BIOS Name	88h	
Product Name	ATA ST1000VM002-1CT1 SCSI Disk Device	
Product Revision	SC23	
Serial Number	S1G8CRW3	
Status	Read only	
Type	Fixed Disk	
Device Size		
Size	932 GB (1,000,204,886,016 bytes)	
Free Space	932 GB (1,000,204,885,504 bytes)	Total size of all unallocated areas on this Disk;
Unallocated Span	932 GB (1,000,204,885,504 bytes)	Size of largest continuous unallocated chunk presented on this Disk;
Device Geometry		
Partition Style	Master Boot Record	
Partitioning	MBR (Basic)	
Total Sectors	1,953,525,168	
Bytes per Sector	512	
Sectors per Track	63	
Tracks per Cylinder	255	
Disk Hidden Areas		
Visible Disk Sectors	1,953,525,168	

☑ Print clone labels for each disk using Disk Label Preset: Erase Disk Label Preset

Start copy to sector: 0

Disk Clone is now configured. When an erase operation is completed the source image/disk will be cloned to the newly erased drive.

Related tasks

Mount Disk Image on page 45

Related information

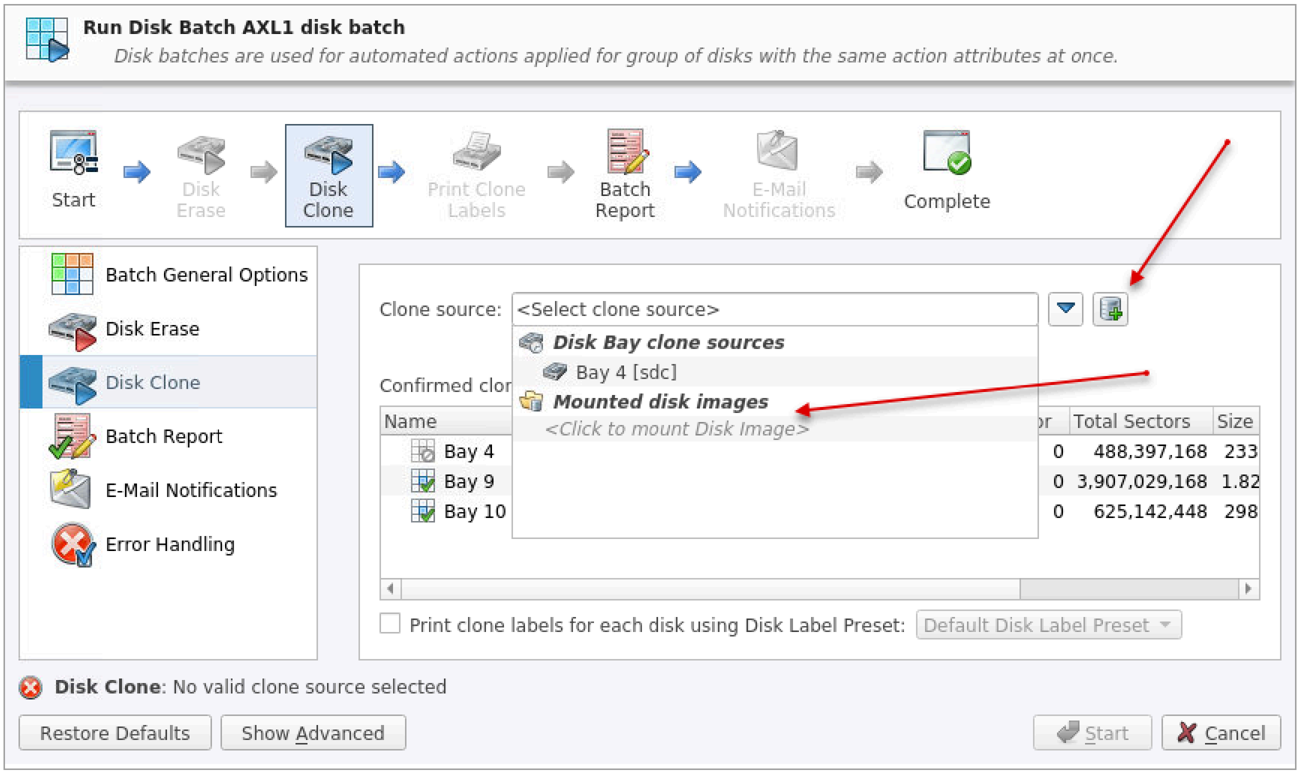
Clone Sources on page 109

Disk Label Presets on page 119

Mount Disk Image

To use a specific disk image file as a data source for cloning:

1. Open the Mount Disk Image dialog in one of ways:



Run Disk Batch AXL1 disk batch

Disk batches are used for automated actions applied for group of disks with the same action attributes at once.

Clone source: <Select clone source>

Disk Bay clone sources

Bay 4 [sdc]

Mounted disk images

<Click to mount Disk Image>

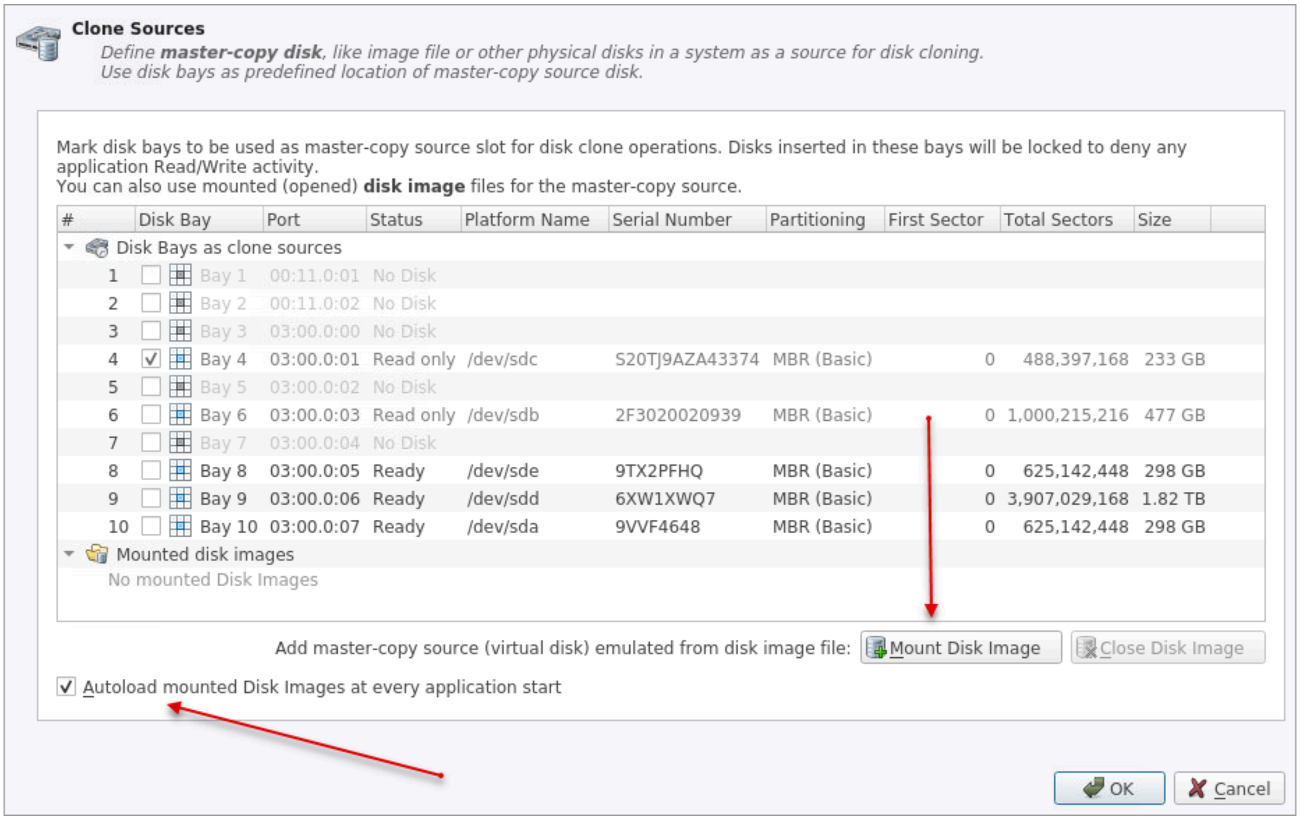
Confirmed clor

Name	or	Total Sectors	Size
Bay 4	0	488,397,168	233
Bay 9	0	3,907,029,168	1.82
Bay 10	0	625,142,448	298

□ Print clone labels for each disk using Disk Label Preset: Default Disk Label Preset

Disk Clone: No valid clone source selected

Figure 44: Mount Disk Image selection



Clone Sources

*Define **master-copy disk**, like image file or other physical disks in a system as a source for disk cloning.*
Use disk bays as predefined location of master-copy source disk.

Mark disk bays to be used as master-copy source slot for disk clone operations. Disks inserted in these bays will be locked to deny any application Read/Write activity.
You can also use mounted (opened) **disk image** files for the master-copy source.

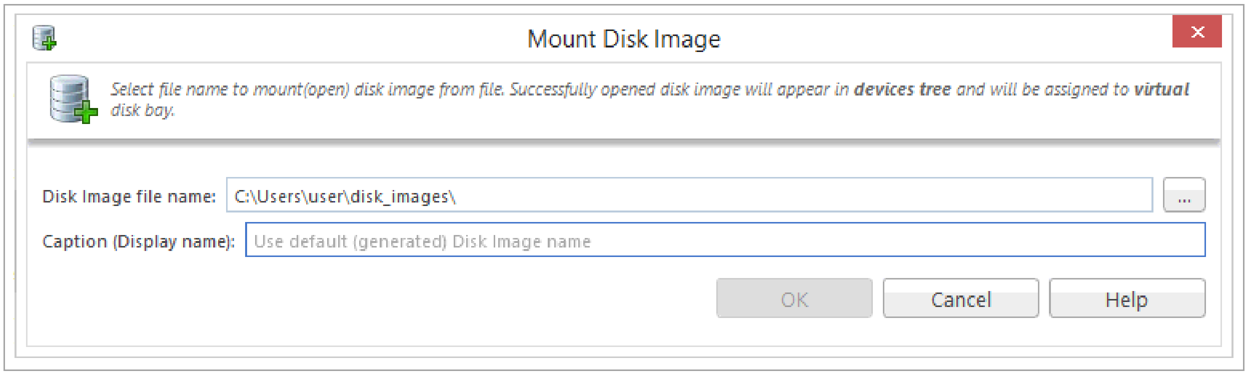
#	Disk Bay	Port	Status	Platform Name	Serial Number	Partitioning	First Sector	Total Sectors	Size
Disk Bays as clone sources									
1	□ Bay 1	00:11.0:01	No Disk						
2	□ Bay 2	00:11.0:02	No Disk						
3	□ Bay 3	03:00.0:00	No Disk						
4	☑ Bay 4	03:00.0:01	Read only	/dev/sdc	S20TJ9AZA43374	MBR (Basic)	0	488,397,168	233 GB
5	□ Bay 5	03:00.0:02	No Disk						
6	□ Bay 6	03:00.0:03	Read only	/dev/sdb	2F3020020939	MBR (Basic)	0	1,000,215,216	477 GB
7	□ Bay 7	03:00.0:04	No Disk						
8	□ Bay 8	03:00.0:05	Ready	/dev/sde	9TX2PFHQ	MBR (Basic)	0	625,142,448	298 GB
9	□ Bay 9	03:00.0:06	Ready	/dev/sdd	6XW1XWQ7	MBR (Basic)	0	3,907,029,168	1.82 TB
10	□ Bay 10	03:00.0:07	Ready	/dev/sda	9VVF4648	MBR (Basic)	0	625,142,448	298 GB
Mounted disk images									
No mounted Disk Images									

Add master-copy source (virtual disk) emulated from disk image file:

☑ Autoload mounted Disk Images at every application start

Figure 45: Mount Disk Image selection (Preferences)

2. Mount Disk Image dialog appears:



*Select file name to mount(open) disk image from file. Successfully opened disk image will appear in **devices tree** and will be assigned to **virtual** disk bay.*

Disk Image file name: C:\Users\user\disk_images\

Caption (Display name): Use default (generated) Disk Image name

Figure 46: Mount Disk Image dialog

Disk Image file name

Full path to the location of disk image file

Caption (Display name)

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

3. 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 a clone source in Clone Sources on page 109 tab and in drop-down list of clone sources in task dialog.

Related tasks

Disk Clone

Resume Stopped or Interrupted Erase

Disk erase can be a time consuming task. Operations with larger disks (10TB+) being erased with sanitizing standards including several overwrite passes could last for hours. If something happened in a middle of erase (user stopped an action, failing disk just turned off, computer re-booted, etc.) user has options:

- Start Erase for the disk all over again
- Resume previous Erase from the point it stopped on a disk (time saving option)

After application start all detected disks being analyzed for previously interrupted erases, and if stopped/ interrupted erases detected on one or more disks, **Resume Erase** button become active. Disks with an erase interrupted are marked with a red label **Interrupted Erase**

Note:

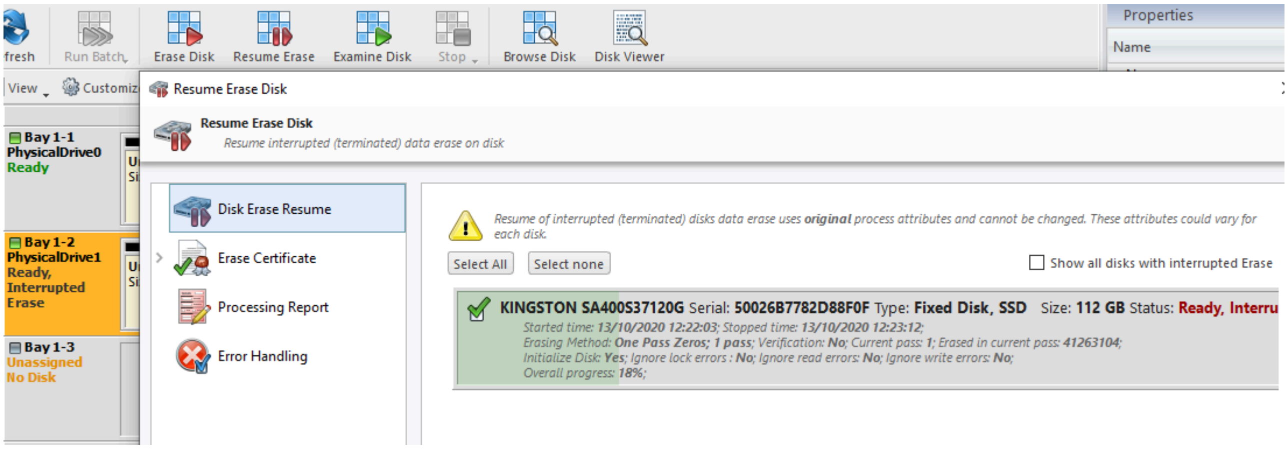
If disks with interrupted erase being detected after program start, pop up dialog appears automatically suggesting you to Resume Erase. You can run Resume Erase from here, or select the only disks you need later on.

To Resume Erase:

1. Select a Disk or group of disks to Resume Erase for

2. Click Resume Erase button on a toolbar

   Resume Erase Disk dialog appears. In the list will be displayed all disks where **Resume Erase** option is available. You can select more disks for resume erase (if any available) or deselect some selected disks



Resume Erase Disk

Resume interrupted (terminated) data erase on disk

*Resume of interrupted (terminated) disks data erase uses **original** process attributes and cannot be changed. These attributes could vary for each disk.*

☐ Show all disks with interrupted Erase

✓ **KINGSTON SA400S37120G** Serial: **50026B7782D88F0F** Type: **Fixed Disk, SSD** Size: **112 GB** Status: **Ready, Interru**

*Started time: **13/10/2020 12:22:03**; Stopped time: **13/10/2020 12:23:12**;*
*Erasing Method: **One Pass Zeros; 1 pass**; Verification: **No**; Current pass: **1**; Erased in current pass: **41263104**;*
*Initialize Disk: **Yes**; Ignore lock errors : **No**; Ignore read errors: **No**; Ignore write errors: **No**;*
*Overall progress: **18%**;*

3. Confirm Resume Erase action

   Verify selected disks, Certificate and Report options and click **Start** button to resume interrupted erase and wait until erase is complete

When resumed erase is completed user is able to review results (logs, processing reports and attributes) for processed disks and print Certificates and Disk Labels.

Secure Erase

Most of Solid State Drives (SSD) support Secure Erase and use it for the physical deletion of all memory blocks on the media. **KillDisk Industrial** is able use SSD **SATA Secure Erase** feature and perform fast unrecoverable erasure. By doing this, you can increase the performance of frequently used SSDs for future use. **All of the data will be lost.** Before using this feature make sure user fully understands the concepts of the feature.

Warning:

100% FATAL DAMAGE GUARANTEED TO MEDIA IF THE PROCESS INTERRUPTED (POWER OUTAGE, UNAUTHORIZED SSD EXTRACTION, ETC.)

Make sure your hardware setup is safe from sudden lost of power.

Do not interrupt the process of *Secure Erase* in any manner.

Note:

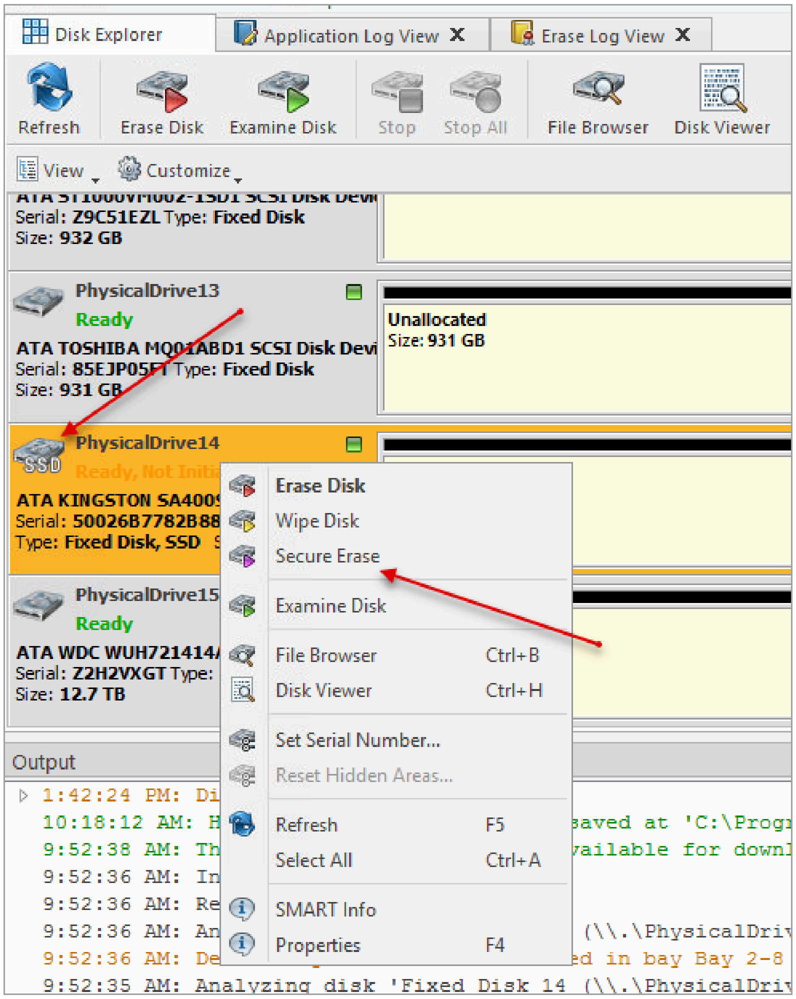
If there is a need to erase ALL data (existing and deleted) from the hard drive device permanently with sanitation standards (US DoD 5220.22-M, Canadian OPS-II, NSA 130-2 etc.), use Disk Erase on page 28 feature.

In order to use **Secure Erase** to erase Solid State Drives:

1. Select a disk for Secure Erase

   Select disks marked as SSD in **Disk Explorer** > **Local Devices** View. You may select multiple disks to be erased simultaneously

2. Execute **Secure Erase** command from **Actions** menu or use context menu:



ATA ST1000VM002-1SD1 SCSI Disk Devi
Serial: Z9C51EZL Type: Fixed Disk
Size: 932 GB

PhysicalDrive13
Ready
ATA TOSHIBA MQ01ABD1 SCSI Disk Devi
Serial: 85EJP05FT Type: Fixed Disk
Size: 931 GB

Unallocated
Size: 931 GB

PhysicalDrive14
Ready, Not Initi
ATA KINGSTON SA400S
Serial: 50026B7782B88
Type: Fixed Disk, SSD

PhysicalDrive15
Ready
ATA WDC WUH721414A
Serial: Z2H2VXGT Type:
Size: 12.7 TB

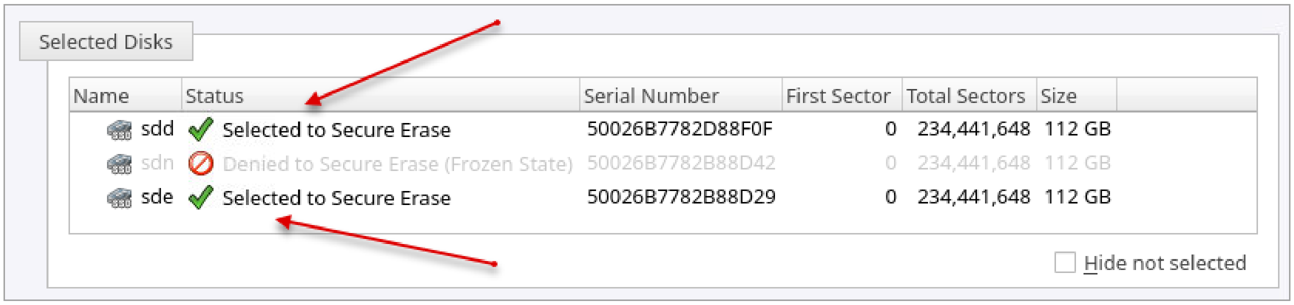
```
1:42:24 PM: Di
10:18:12 AM: H                                      saved at 'C:\Progr
9:52:38 AM: Th                                      vailable for downl
9:52:36 AM: In
9:52:36 AM: Re
9:52:36 AM: An                                       (\\.\PhysicalDriv
9:52:36 AM: De                                      ed in bay Bay 2-8
9:52:35 AM: Analyzing disk 'Fixed Disk 14 (\\.\PhysicalDriv
```

Figure 47: Initiating Secure Erase

3. Confirm *Secure Erase* Options:

Use tabbed views to adjust Secure Erase preferences if necessary. Available options are:

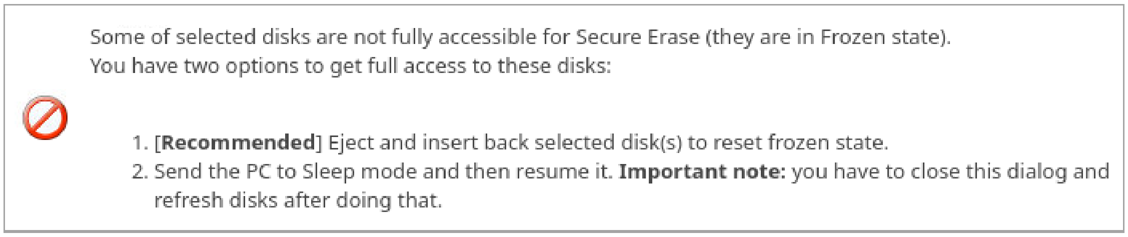
- Secure Erase on page 105
- Erase Certificate on page 111
- Processing Report on page 115
- Error Handling on page 125
- Selected Disks (Disk selection for Secure Erase). Only NOT frozen SSDs can be selected for Secure Erasing



Name	Status	Serial Number	First Sector	Total Sectors	Size
sdd	✓ Selected to Secure Erase	50026B7782D88F0F	0	234,441,648	112 GB
sdn	⊘ Denied to Secure Erase (Frozen State)	50026B7782B88D42	0	234,441,648	112 GB
sde	✓ Selected to Secure Erase	50026B7782B88D29	0	234,441,648	112 GB

Note:

In case of a frozen SSD drive has been selected for erasing the following message appears in Disk Secure Erase tab:



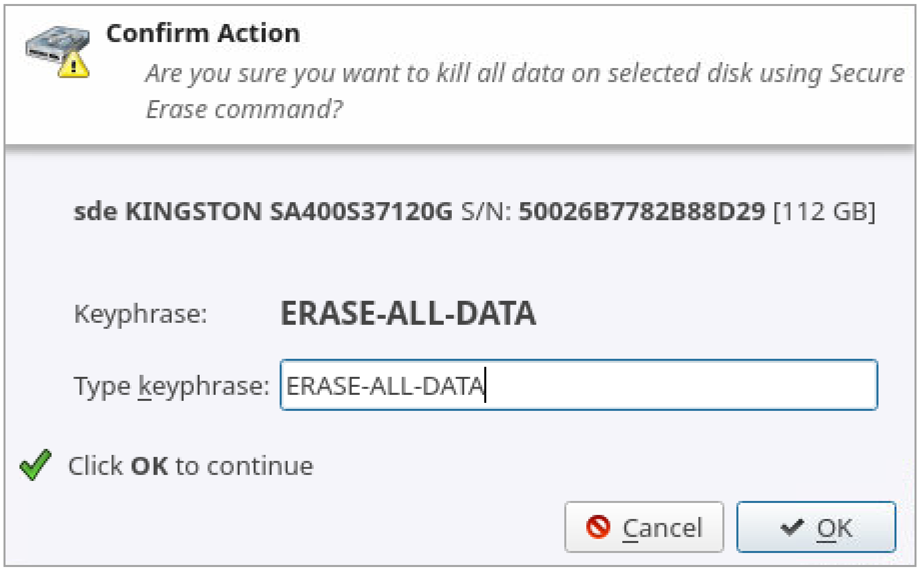
Some of selected disks are not fully accessible for Secure Erase (they are in Frozen state).
You have two options to get full access to these disks:

1. [**Recommended**] Eject and insert back selected disk(s) to reset frozen state.
2. Send the PC to Sleep mode and then resume it. **Important note:** you have to close this dialog and refresh disks after doing that.

Figure 48: Frozen disks

4. Click **Start** to reach the final step before erasing disk data

Confirm **Secure Erase** action by typing a predefined keyphrase and the process starts



Confirm Action

Are you sure you want to kill all data on selected disk using Secure Erase command?

sde KINGSTON SA400S37120G S/N: **50026B7782B88D29** [112 GB]

Keyphrase: **ERASE-ALL-DATA**

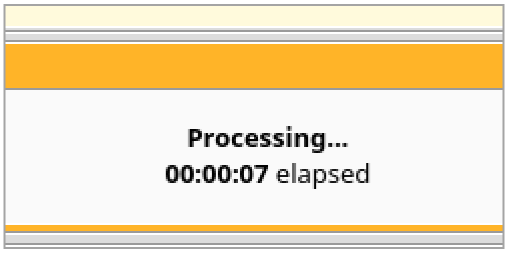
Type keyphrase: ERASE-ALL-DATA

✓ Click **OK** to continue

Figure 49: *Secure Erase* confirmation

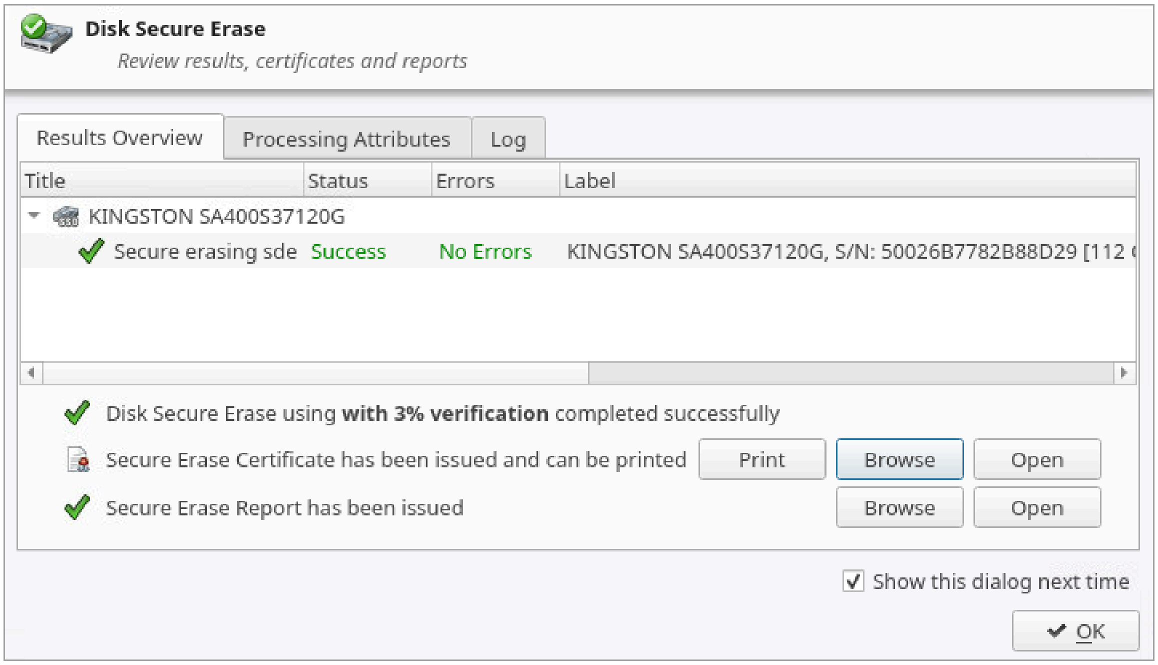
Note:

There is no progress indicator available for Secure Erase. The feature is implemented inside SSD controller. There is only "elapsed" time available:



Processing...
00:00:07 elapsed

After Secure Erase process is completed the Processing Summary on page 51 dialog appears



Disk Secure Erase

Review results, certificates and reports

Title	Status	Errors	Label
KINGSTON SA400S37120G			
✓ Secure erasing sde	Success	No Errors	KINGSTON SA400S37120G, S/N: 50026B7782B88D29 [112

✓ Disk Secure Erase using **with 3% verification** completed successfully

Secure Erase Certificate has been issued and can be printed

✓ Secure Erase Report has been issued

☑ Show this dialog next time

Figure 50: Processing Summary

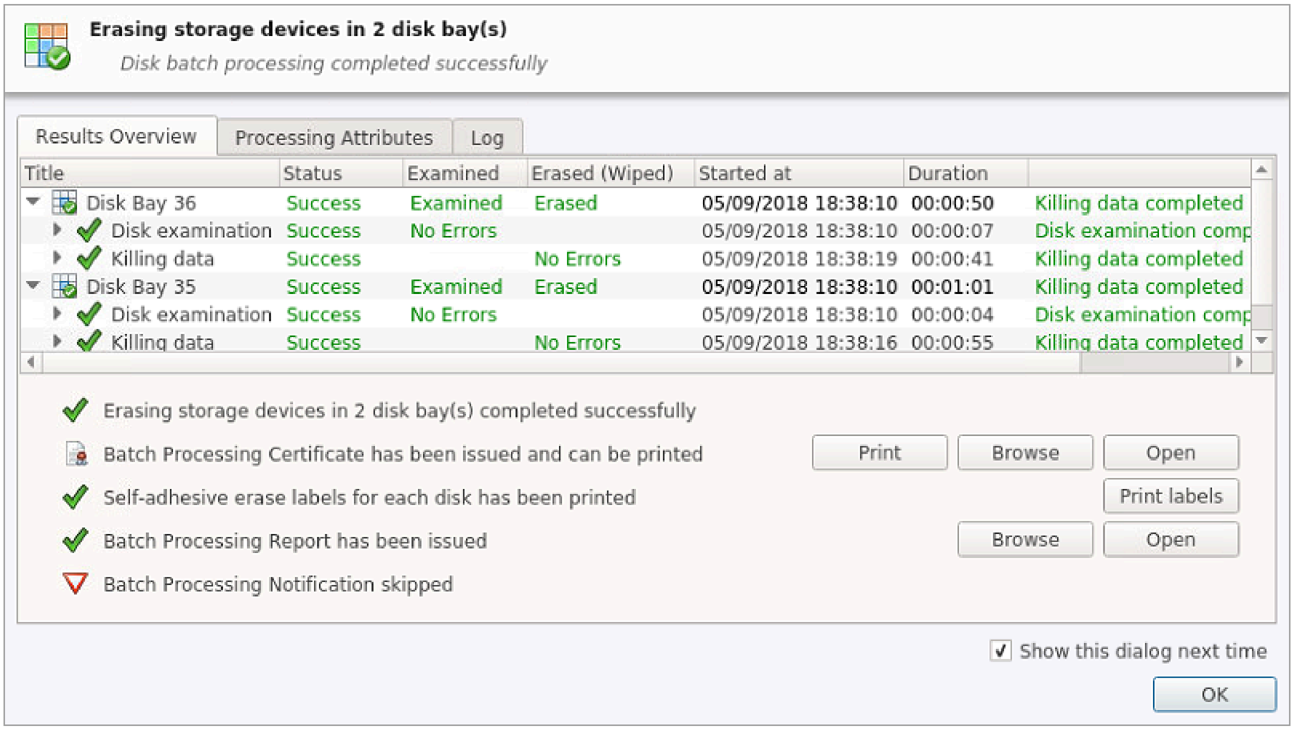
Now you may **Print**, **Browse** or **Open** Secure Erase Certificate and Reports (XML) on page 65. If there are any errors they will be reported on the interactive screen and in Erase History Disk Processing Results.

Related information

Secure Erase on page 105
Processing Summary on page 51
Certificates, Labels and Reports on page 54
Secure Erase (SSD) on page 137
Secure Erase Concepts on page 144
Secure Erase (ANSI ATA, SE) on page 152

Processing Summary

Once **KillDisk** finishes processing any task such as Disk Erase on page 28, Secure Erase on page 48 or Disk Wipe on page 35, a summary dialog appears. It contains all of the information regarding to the operation(s). For example, it includes information like disks operated on, status of erasure, logs and all associated certificates and reports.



Erasing storage devices in 2 disk bay(s)

Disk batch processing completed successfully

Title	Status	Examined	Erased (Wiped)	Started at	Duration	
Disk Bay 36	Success	Examined	Erased	05/09/2018 18:38:10	00:00:50	Killing data completed
✓ Disk examination	Success	No Errors		05/09/2018 18:38:10	00:00:07	Disk examination comp
✓ Killing data	Success		No Errors	05/09/2018 18:38:19	00:00:41	Killing data completed
Disk Bay 35	Success	Examined	Erased	05/09/2018 18:38:10	00:01:01	Killing data completed
✓ Disk examination	Success	No Errors		05/09/2018 18:38:10	00:00:04	Disk examination comp
✓ Killing data	Success		No Errors	05/09/2018 18:38:16	00:00:55	Killing data completed

✓ Erasing storage devices in 2 disk bay(s) completed successfully

Batch Processing Certificate has been issued and can be printed

✓ Self-adhesive erase labels for each disk has been printed

✓ Batch Processing Report has been issued

▽ Batch Processing Notification skipped

☑ Show this dialog next time

Figure 51: Example of processing summary

Results Overview window contains the options for the successful erasure:

Title
All the devices processed are displayed with their success/failure status in a tree list

Status
An actual status (success/fail)

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

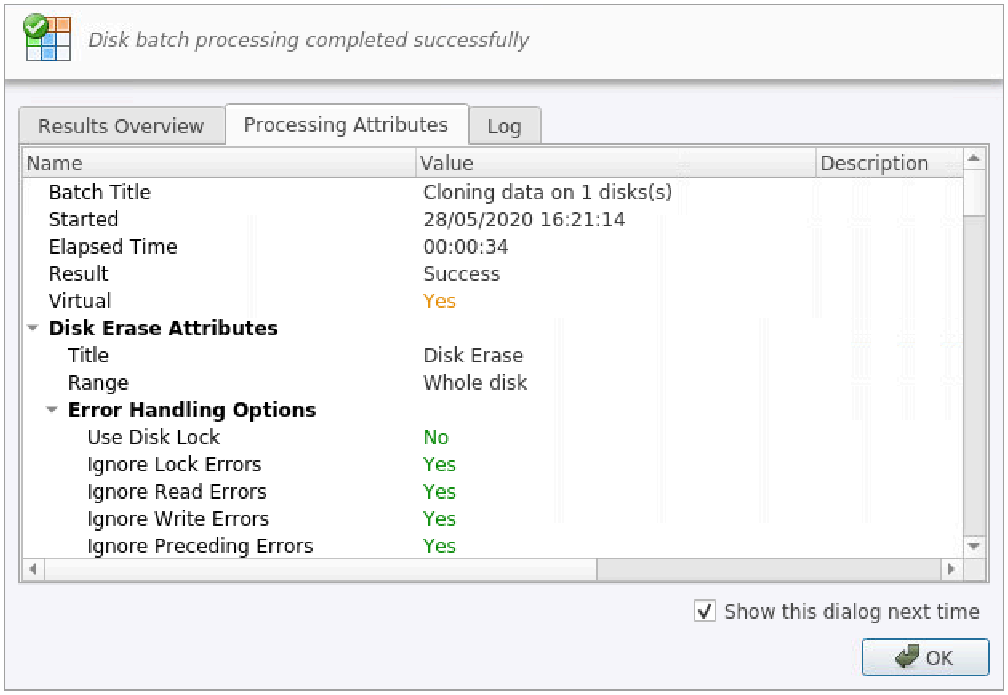
Disk Grade Assignment Status
Confirms the inclusion of the disk grade assignment operation based on disk integrity examination results

Erased
Status of the disk erase operation

Started at
Time & date of operation's start

Duration
Duration of the operation

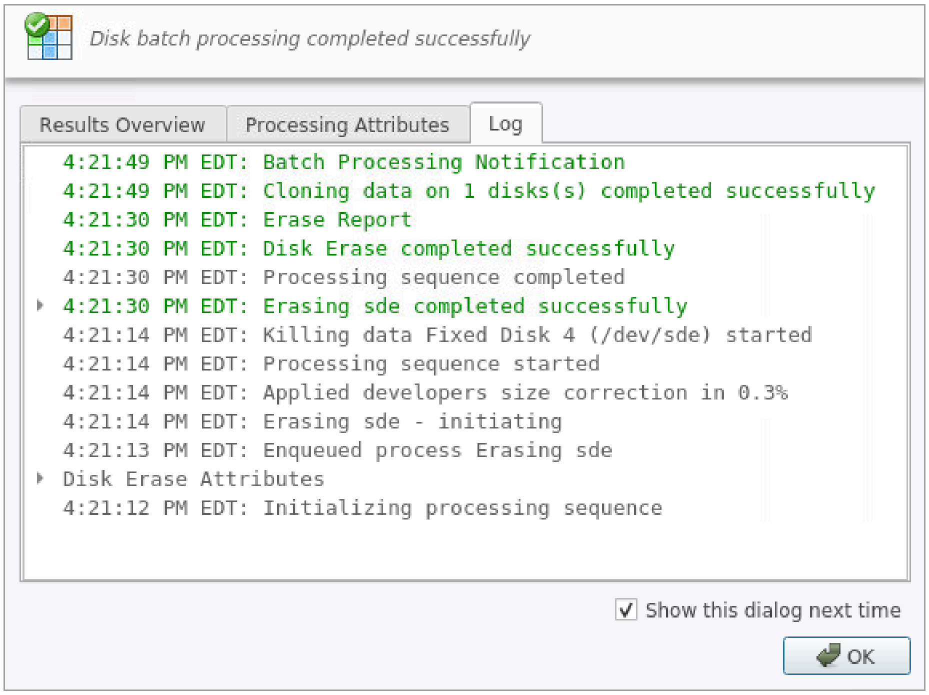
Processing Attributes window contains all the status and attributes of the operations (as more detailed View):


Disk batch processing completed successfully
Results Overview
Processing Attributes
Log
☑ Show this dialog next time
OK

Name	Value	Description
Batch Title	Cloning data on 1 disks(s)	
Started	28/05/2020 16:21:14	
Elapsed Time	00:00:34	
Result	Success	
Virtual	Yes	
Disk Erase Attributes		
Title	Disk Erase	
Range	Whole disk	
Error Handling Options		
Use Disk Lock	No	
Ignore Lock Errors	Yes	
Ignore Read Errors	Yes	
Ignore Write Errors	Yes	
Ignore Preceding Errors	Yes	

Figure 52: Processing Attributes sample

Log window shows an actual Log file:


Disk batch processing completed successfully
Results Overview
Processing Attributes
Log
☑ Show this dialog next time
OK

```
  4:21:49 PM EDT: Batch Processing Notification
  4:21:49 PM EDT: Cloning data on 1 disks(s) completed successfully
  4:21:30 PM EDT: Erase Report
  4:21:30 PM EDT: Disk Erase completed successfully
  4:21:30 PM EDT: Processing sequence completed
▸ 4:21:30 PM EDT: Erasing sde completed successfully
  4:21:14 PM EDT: Killing data Fixed Disk 4 (/dev/sde) started
  4:21:14 PM EDT: Processing sequence started
  4:21:14 PM EDT: Applied developers size correction in 0.3%
  4:21:14 PM EDT: Erasing sde - initiating
  4:21:13 PM EDT: Enqueued process Erasing sde
▸ Disk Erase Attributes
  4:21:12 PM EDT: Initializing processing sequence
```

Figure 53: Log sample

Note:

The Wipe operation will produce a similar processing summary for the Disk Wipe

Additional options are:

Disk Certificate
Specifies the path to the saved erasure PDF certificate. Allows user to examine the certificate by pressing the **Open** button

Print Labels
Allows user to examine, customize, change options and print Disk Labels on page 61 by pressing the **Print Labels** button

Disk Processing Report
Specifies the path to the saved Disk Processing Report. Allows user to examine the *.xml* disk processing report by pressing the **Browse** (to navigate to the containing folder) or **Open** buttons

Related information

Certificates, Labels and Reports on page 54

Certificates, Labels and Reports

KillDisk maintains highest standards of disk erasure implementing most modern sanitation methods and provides extensive options for its operations with Certificates, Reports and Disk Labels with various Barcodes.

Related information

Erase Certificates on page 54

Reports (XML) on page 65

Disk Labels on page 61

Barcode on page 112

Erase Certificates

KillDisk provides PDF-certificates upon the completion of disk Erase, Wipe or Secure Erase operations. These certificates may be customized to include company-specific information and hardware/procedure description. Configuring these custom settings is described in the Certificate Preferences section of this guide.

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

Barcode
A barcode in selected format with encoded tags and attributes for scanning using a barcode scanner

Company Information
Displays all company information provided in the preferences. The user in the sample above only provided a business name. But other company information may also be included in the certificate

Technician Information
Displays the technician information provided in the preferences. 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 Information
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 OS and processor type

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.

Hardware Information

Provides details on the hardware used to run **KillDisk** such as Manufacturer, logical processors etc.

Storing Certificate to PDF

There are options for storing a certificate to file in PDF format as well as encrypting with passwords and digitally signing output PDFs. You can re-print stored to PDF certificates later on as well as you can validate their integrity and validity.

Certificate location

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

File name template

Here user specifies the template for the Erase Certificate. See the tags available in Appendix tags section

Encrypt with password

If password field is not empty, output certificate (PDF) will be encrypted and protected with specified password. This password needs to be typed in any PDF Viewer next time user opens a certificate for printing

Sign Certificate with Digital Signature

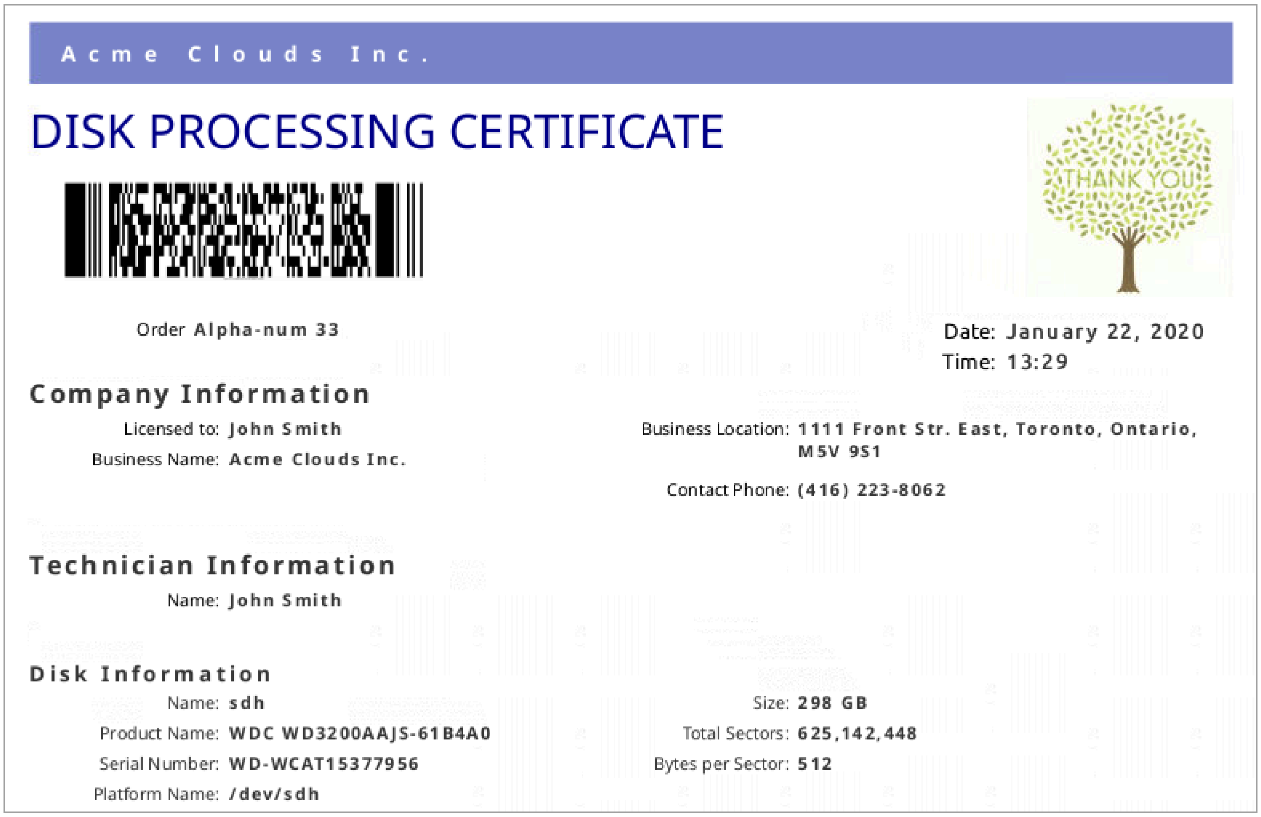
Certificate file (PDF) can be signed with a default Digital Signature (supplied **KillDisk.pfx** certificate) or with your custom Digital Signature (*.PFX) and can be verified later on. If **Adobe Reader** successfully verified PDF document, it is guaranteed that its content hasn't been modified since issue.

If custom Digital Signature is required, please issue a certificate and specify full path to the custom certificate (*.PFX file) as well as its open password in the related fields below (**Digital Signature** and **Use password to open**)

Display Digital Signature

Digital Signature can be displayed as an overlay text on the first page of certificate. After you turn on this option, you can specify overlay text using tags (see tags section), its position on the first page, rectangle dimensions and text size

Sample of Disk Processing Certificate



Acme Clouds Inc.

DISK PROCESSING CERTIFICATE

Order Alpha-num 33

Date: January 22, 2020
Time: 13:29

Company Information

Licensed to: John Smith
Business Name: Acme Clouds Inc.

Business Location: 1111 Front Str. East, Toronto, Ontario, M5V 9S1
Contact Phone: (416) 223-8062

Technician Information

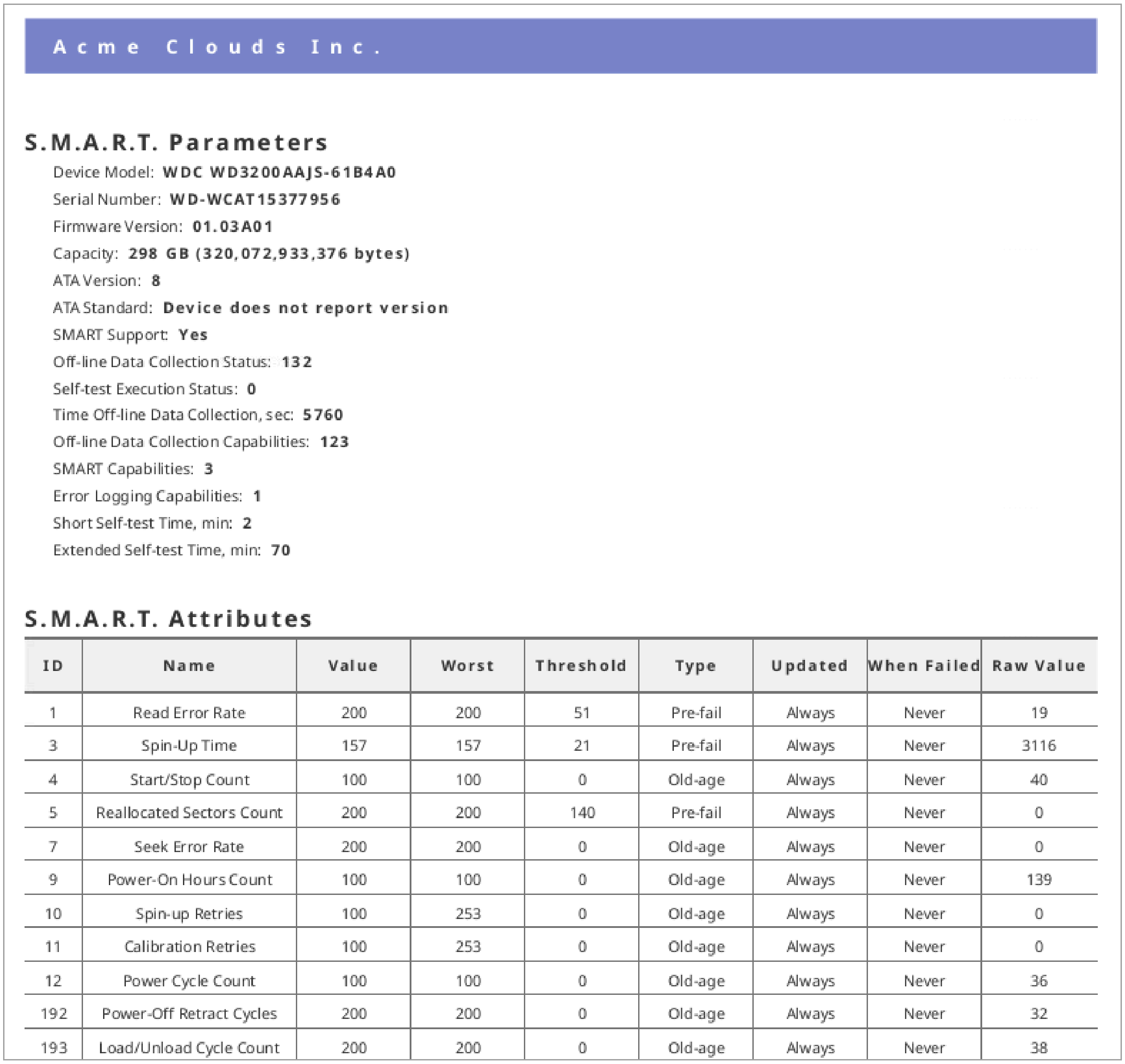
Name: John Smith

Disk Information

Name: sdh
Product Name: WDC WD3200AAJS-61B4A0
Serial Number: WD-WCAT15377956
Platform Name: /dev/sdh

Size: 298 GB
Total Sectors: 625,142,448
Bytes per Sector: 512

Figure 54: Disk Processing Certificate - 1-st Page



Acme Clouds Inc.

S.M.A.R.T. Parameters

Device Model: **WDC WD3200AAJS-61B4A0**

Serial Number: **WD-WCAT15377956**

Firmware Version: **01.03A01**

Capacity: **298 GB (320,072,933,376 bytes)**

ATA Version: **8**

ATA Standard: **Device does not report version**

SMART Support: **Yes**

Off-line Data Collection Status: **132**

Self-test Execution Status: **0**

Time Off-line Data Collection, sec: **5760**

Off-line Data Collection Capabilities: **123**

SMART Capabilities: **3**

Error Logging Capabilities: **1**

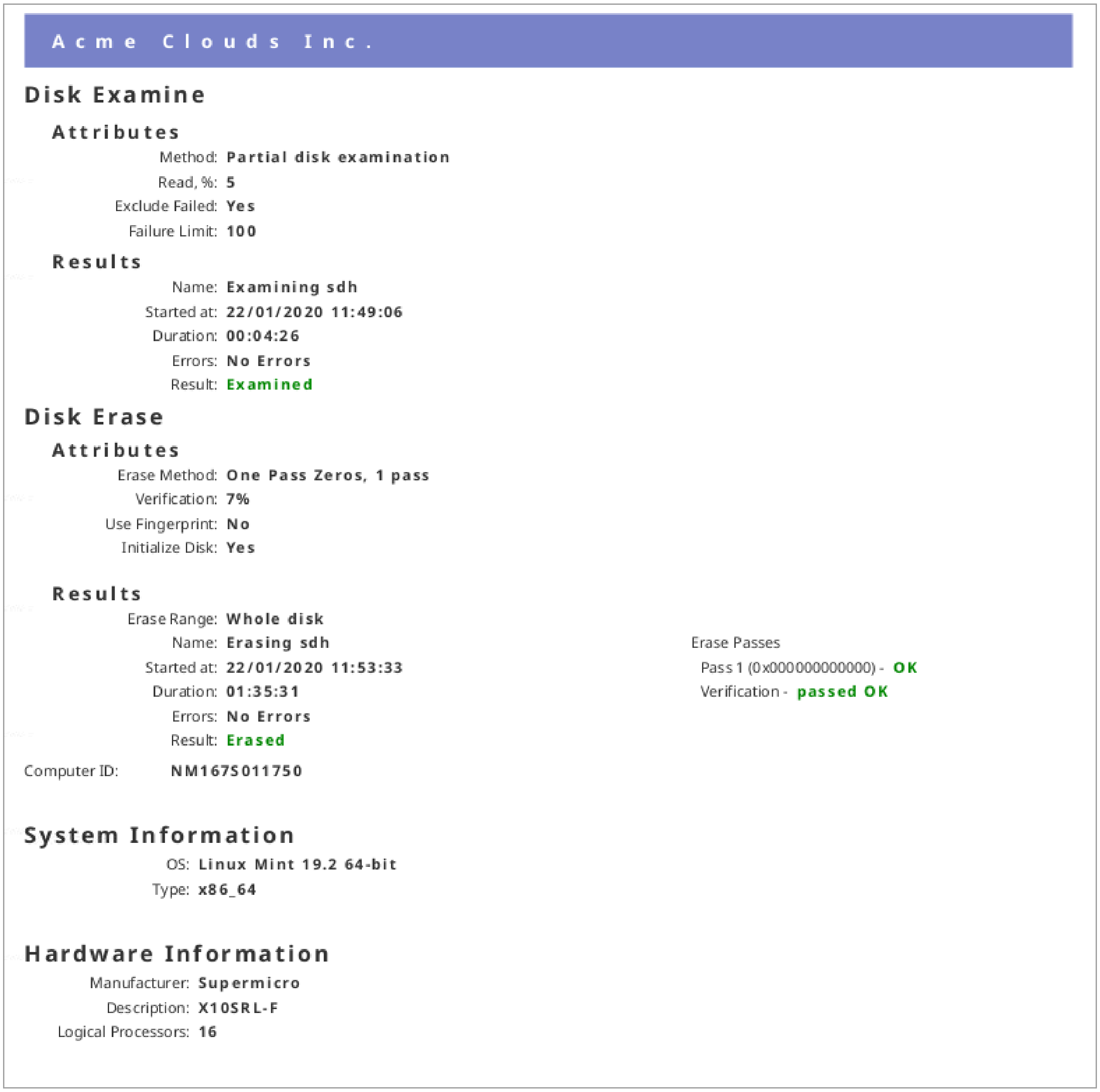
Short Self-test Time, min: **2**

Extended Self-test Time, min: **70**

S.M.A.R.T. Attributes

ID	Name	Value	Worst	Threshold	Type	Updated	When Failed	Raw Value
1	Read Error Rate	200	200	51	Pre-fail	Always	Never	19
3	Spin-Up Time	157	157	21	Pre-fail	Always	Never	3116
4	Start/Stop Count	100	100	0	Old-age	Always	Never	40
5	Reallocated Sectors Count	200	200	140	Pre-fail	Always	Never	0
7	Seek Error Rate	200	200	0	Old-age	Always	Never	0
9	Power-On Hours Count	100	100	0	Old-age	Always	Never	139
10	Spin-up Retries	100	253	0	Old-age	Always	Never	0
11	Calibration Retries	100	253	0	Old-age	Always	Never	0
12	Power Cycle Count	100	100	0	Old-age	Always	Never	36
192	Power-Off Retract Cycles	200	200	0	Old-age	Always	Never	32
193	Load/Unload Cycle Count	200	200	0	Old-age	Always	Never	38

Figure 55: Disk Processing Certificate - 2-nd Page



Acme Clouds Inc.

Disk Examine

Attributes

Method: Partial disk examination
Read, %: 5
Exclude Failed: Yes
Failure Limit: 100

Results

Name: Examining sdh
Started at: 22/01/2020 11:49:06
Duration: 00:04:26
Errors: No Errors
Result: Examined

Disk Erase

Attributes

Erase Method: One Pass Zeros, 1 pass
Verification: 7%
Use Fingerprint: No
Initialize Disk: Yes

Results

Erase Range: Whole disk
Name: Erasing sdh
Started at: 22/01/2020 11:53:33
Duration: 01:35:31
Errors: No Errors
Result: Erased

Erase Passes
Pass 1 (0x000000000000) - OK
Verification - passed OK

Computer ID: NM167S011750

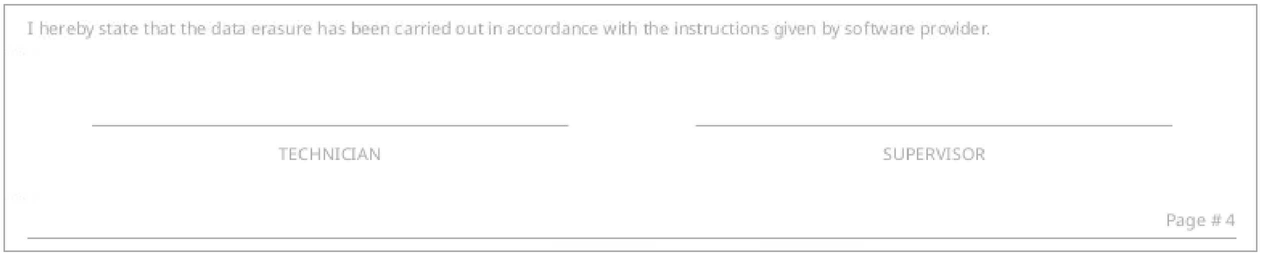
System Information

OS: Linux Mint 19.2 64-bit
Type: x86_64

Hardware Information

Manufacturer: Supermicro
Description: X10SRL-F
Logical Processors: 16

Figure 56: Disk Processing Certificate - 3-rd Page



I hereby state that the data erasure has been carried out in accordance with the instructions given by software provider.

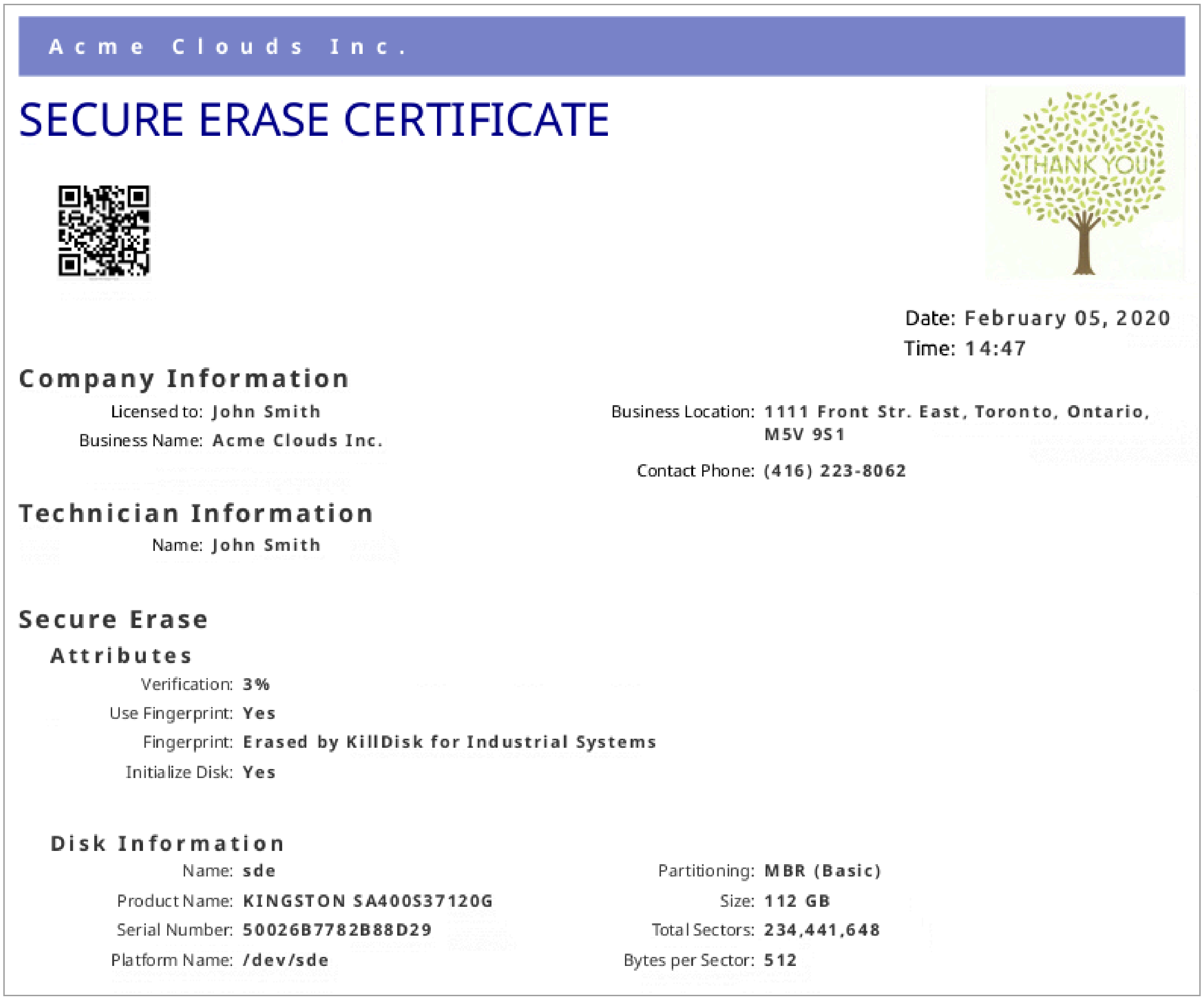
TECHNICIAN

SUPERVISOR

Page # 4

Figure 57: Disk Processing Certificate - Last Page

Sample of Secure Erase Certificate



Acme Clouds Inc.

SECURE ERASE CERTIFICATE

Date: February 05, 2020
Time: 14:47

Company Information

Licensed to: John Smith
Business Name: Acme Clouds Inc.

Business Location: 1111 Front Str. East, Toronto, Ontario, M5V 9S1
Contact Phone: (416) 223-8062

Technician Information

Name: John Smith

Secure Erase

Attributes

Verification: 3%
Use Fingerprint: Yes
Fingerprint: Erased by KillDisk for Industrial Systems
Initialize Disk: Yes

Disk Information

Name: sde
Product Name: KINGSTON SA400S37120G
Serial Number: 50026B7782B88D29
Platform Name: /dev/sde

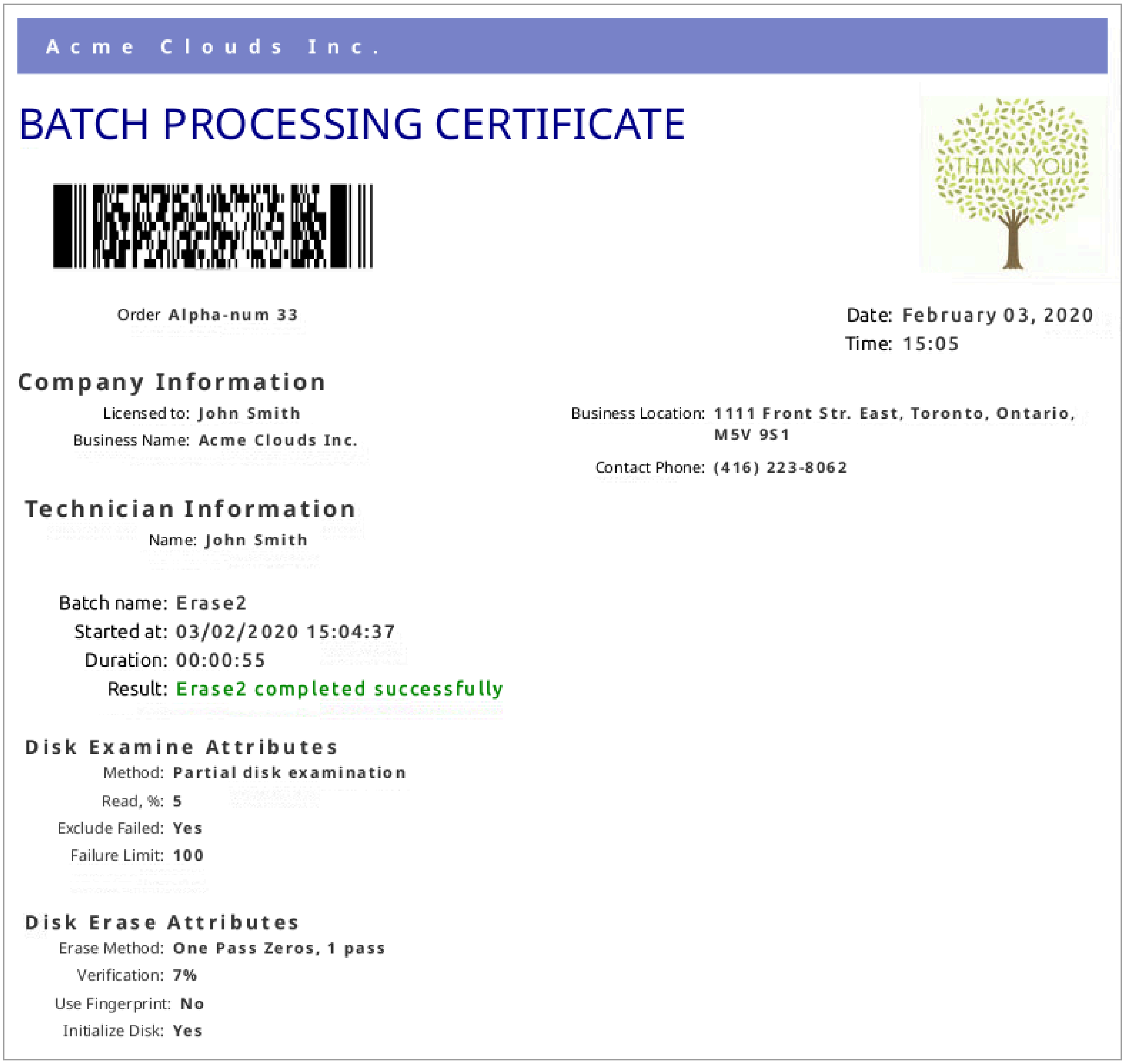
Partitioning: MBR (Basic)
Size: 112 GB
Total Sectors: 234,441,648
Bytes per Sector: 512

Figure 58: Secure Erase Certificate - 1-st Page

Sample of Batch Certificate

Note:

For group operations like Batches KillDisk is able to create both Batch Summary certificate as well as separate certificates for each disk in the Batch.



Acme Clouds Inc.

BATCH PROCESSING CERTIFICATE

Order Alpha-num 33

Date: February 03, 2020
Time: 15:05

Company Information

Licensed to: John Smith
Business Name: Acme Clouds Inc.

Business Location: 1111 Front Str. East, Toronto, Ontario, M5V 9S1
Contact Phone: (416) 223-8062

Technician Information

Name: John Smith

Batch name: Erase2
Started at: 03/02/2020 15:04:37
Duration: 00:00:55
Result: Erase2 completed successfully

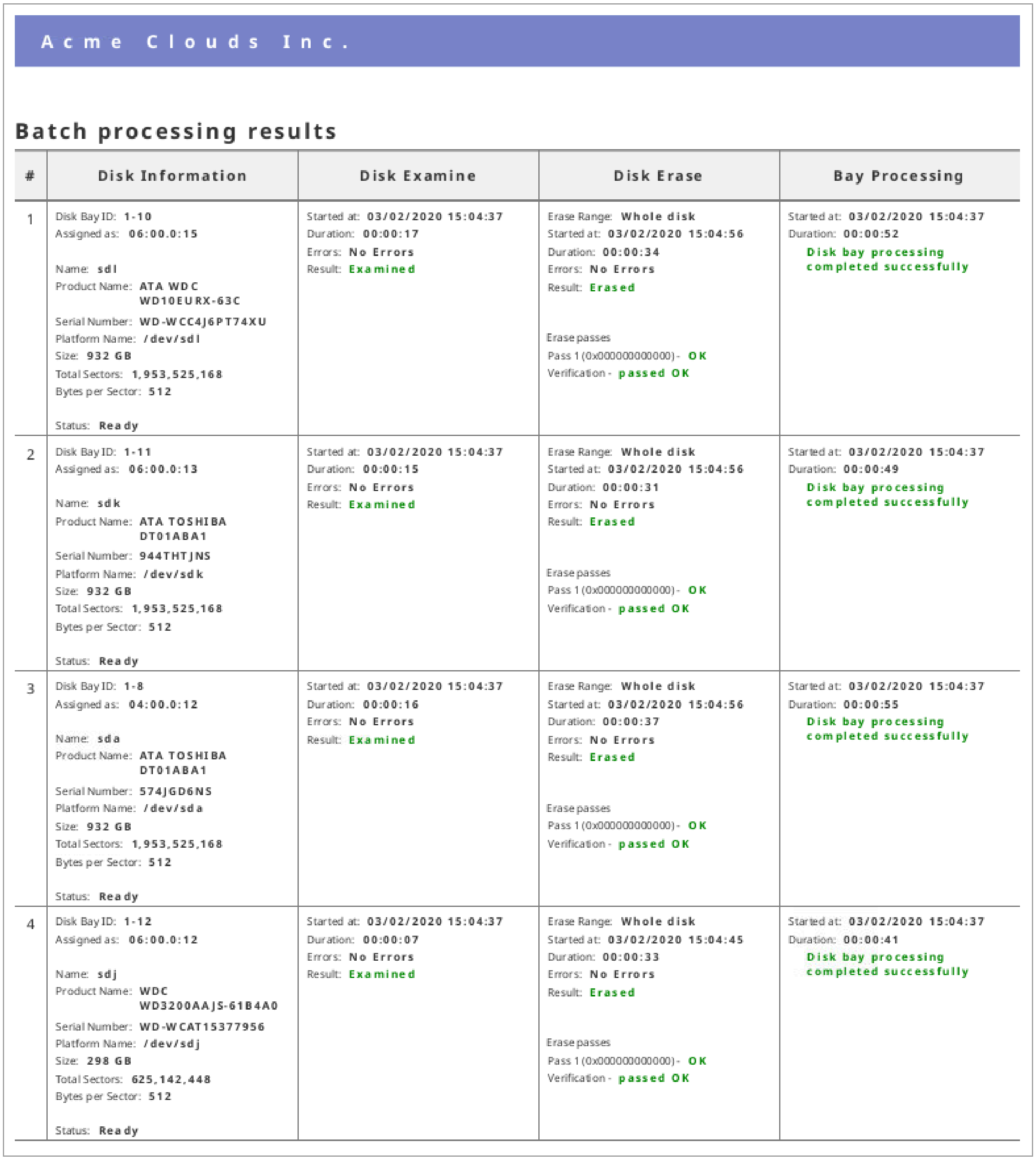
Disk Examine Attributes

Method: Partial disk examination
Read, %: 5
Exclude Failed: Yes
Failure Limit: 100

Disk Erase Attributes

Erase Method: One Pass Zeros, 1 pass
Verification: 7%
Use Fingerprint: No
Initialize Disk: Yes

Figure 59: Disk Erase - Batch Certificate - 1-st Page



Acme Clouds Inc.

Batch processing results

#	Disk Information	Disk Examine	Disk Erase	Bay Processing
1	Disk Bay ID: 1-10 Assigned as: 06:00.0:15 Name: sdl Product Name: ATA WDC WD10EURX-63C Serial Number: WD-WCC4J6PT74XU Platform Name: /dev/sdl Size: 932 GB Total Sectors: 1,953,525,168 Bytes per Sector: 512 Status: Ready	Started at: 03/02/2020 15:04:37 Duration: 00:00:17 Errors: No Errors Result: Examined	Erase Range: Whole disk Started at: 03/02/2020 15:04:56 Duration: 00:00:34 Errors: No Errors Result: Erased Erase passes Pass 1 (0x000000000000) - OK Verification - passed OK	Started at: 03/02/2020 15:04:37 Duration: 00:00:52 Disk bay processing completed successfully
2	Disk Bay ID: 1-11 Assigned as: 06:00.0:13 Name: sdk Product Name: ATA TOSHIBA DT01ABA1 Serial Number: 944THTJNS Platform Name: /dev/sdk Size: 932 GB Total Sectors: 1,953,525,168 Bytes per Sector: 512 Status: Ready	Started at: 03/02/2020 15:04:37 Duration: 00:00:15 Errors: No Errors Result: Examined	Erase Range: Whole disk Started at: 03/02/2020 15:04:56 Duration: 00:00:31 Errors: No Errors Result: Erased Erase passes Pass 1 (0x000000000000) - OK Verification - passed OK	Started at: 03/02/2020 15:04:37 Duration: 00:00:49 Disk bay processing completed successfully
3	Disk Bay ID: 1-8 Assigned as: 04:00.0:12 Name: sda Product Name: ATA TOSHIBA DT01ABA1 Serial Number: 574JGD6NS Platform Name: /dev/sda Size: 932 GB Total Sectors: 1,953,525,168 Bytes per Sector: 512 Status: Ready	Started at: 03/02/2020 15:04:37 Duration: 00:00:16 Errors: No Errors Result: Examined	Erase Range: Whole disk Started at: 03/02/2020 15:04:56 Duration: 00:00:37 Errors: No Errors Result: Erased Erase passes Pass 1 (0x000000000000) - OK Verification - passed OK	Started at: 03/02/2020 15:04:37 Duration: 00:00:55 Disk bay processing completed successfully
4	Disk Bay ID: 1-12 Assigned as: 06:00.0:12 Name: sdj Product Name: WDC WD3200AAJS-61B4A0 Serial Number: WD-WCAT15377956 Platform Name: /dev/sdj Size: 298 GB Total Sectors: 625,142,448 Bytes per Sector: 512 Status: Ready	Started at: 03/02/2020 15:04:37 Duration: 00:00:07 Errors: No Errors Result: Examined	Erase Range: Whole disk Started at: 03/02/2020 15:04:45 Duration: 00:00:33 Errors: No Errors Result: Erased Erase passes Pass 1 (0x000000000000) - OK Verification - passed OK	Started at: 03/02/2020 15:04:37 Duration: 00:00:41 Disk bay processing completed successfully

Figure 60: Disk Erase - Batch Certificate - 2-nd Page

Related information

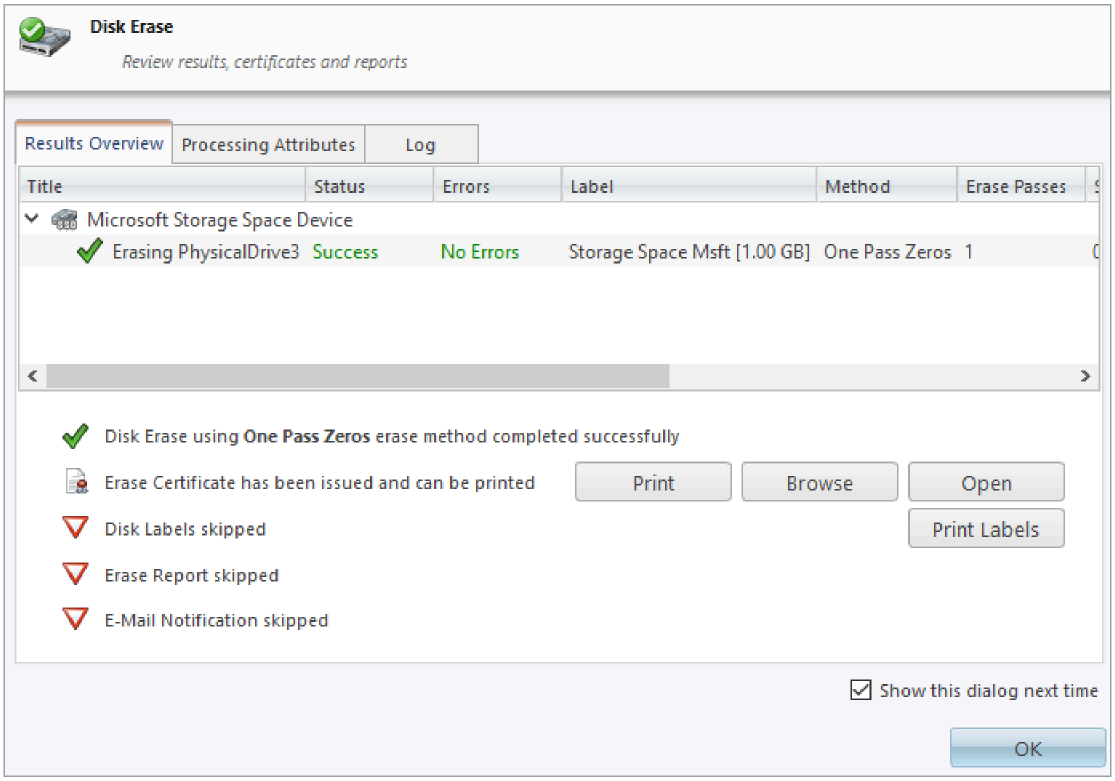
Disk Labels on page 61
Reports (XML) on page 65
Barcode on page 112

Disk Labels

Along with the PDF certificate **KillDisk** allows you to print Disk Labels to place on erased disks with its Print Label features. Disk Labels with process results and essential disk information could be issued for any disk processing (such as Disk Erase, Disk Wipe, Disk Examine or Disk Clone on page 44 and Secure Erase on page 48). 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.

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. Click it to enter the **Print Label Dialog**.



Disk Erase

Review results, certificates and reports

Title	Status	Errors	Label	Method	Erase Passes	S
Microsoft Storage Space Device						
Erasing PhysicalDrive3	Success	No Errors	Storage Space Msft [1.00 GB]	One Pass Zeros	1	(

✓ Disk Erase using **One Pass Zeros** erase method completed successfully

Erase Certificate has been issued and can be printed

Disk Labels skipped

Erase Report skipped

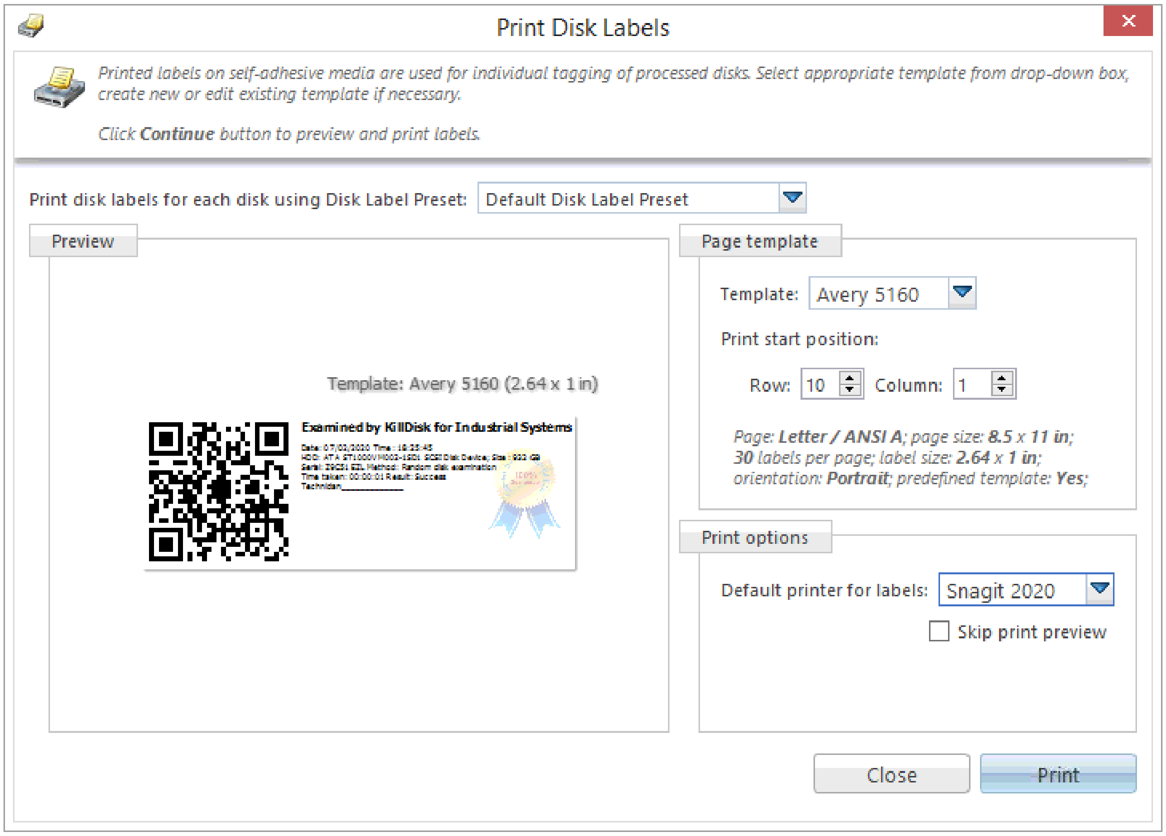
E-Mail Notification skipped

☑ Show this dialog next time

Figure 61: Opening Print Label Dialog

Print Label Dialog

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



Print Disk Labels

Printed labels on self-adhesive media are used for individual tagging of processed disks. Select appropriate template from drop-down box, create new or edit existing template if necessary.

*Click **Continue** button to preview and print labels.*

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

Preview

Template: Avery 5160 (2.64 x 1 in)

Examined by KillDisk for Industrial Systems

Date: 07/03/2020 Time : 16:25:45
HDD: ATA ST1000VM002-1SD1 SCSI Disk Device; Size : 932 GB
Serial: Z9C31 E2L Method: Random disk examination
Time taken: 00:00:01 Result: Success
Technician_______________

Page template

Template: Avery 5160

Print start position:

Row: 10 Column: 1

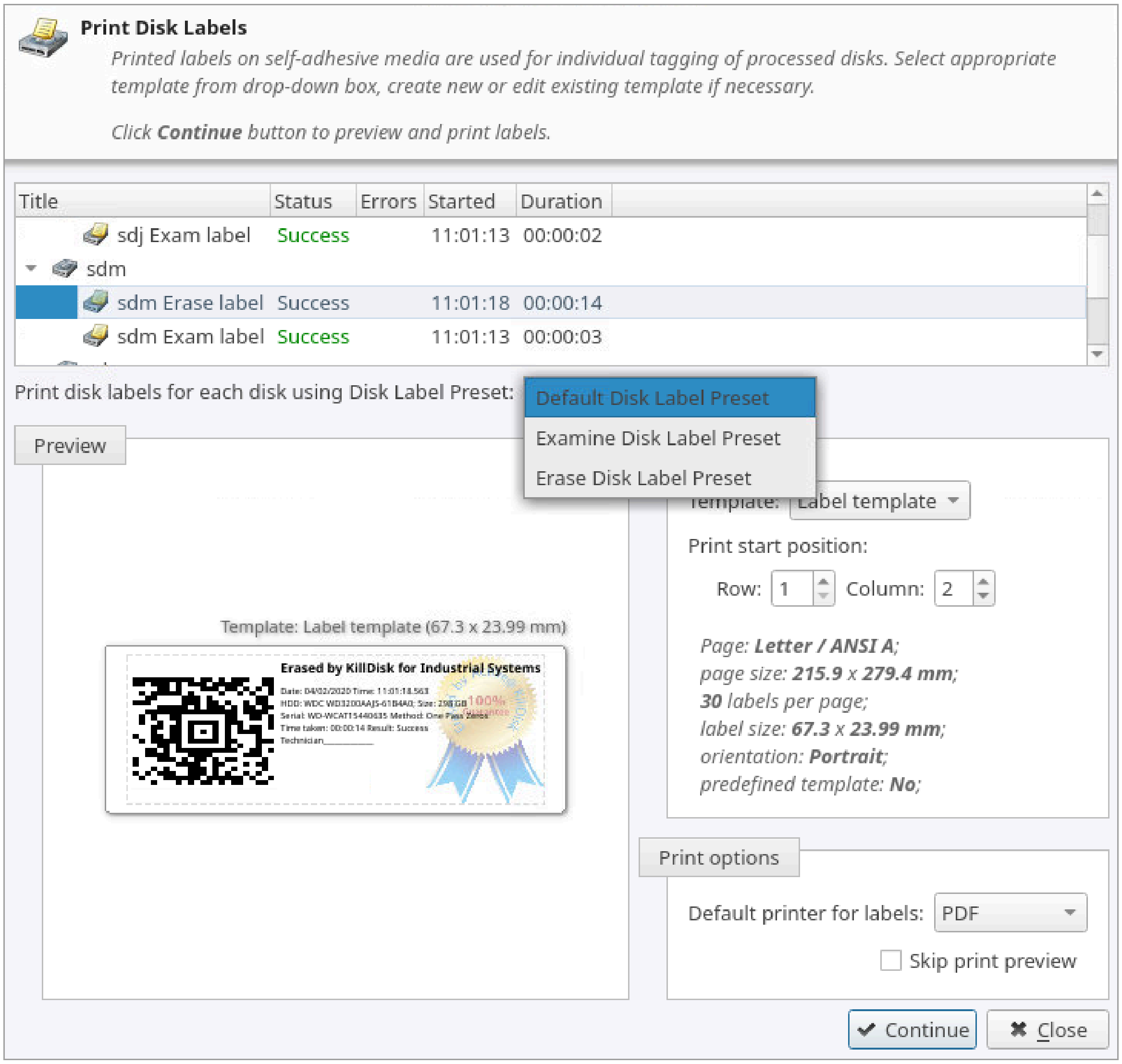
*Page: **Letter / ANSI A**; page size: **8.5** x **11 in**; **30** labels per page; label size: **2.64** x **1 in**; orientation: **Portrait**; predefined template: **Yes**;*

Print options

Default printer for labels: Snagit 2020

□ Skip print preview

Figure 62: Print Label Dialog



Print Disk Labels

Printed labels on self-adhesive media are used for individual tagging of processed disks. Select appropriate template from drop-down box, create new or edit existing template if necessary.

*Click **Continue** button to preview and print labels.*

Title	Status	Errors	Started	Duration
sdj Exam label	Success		11:01:13	00:00:02
sdm				
sdm Erase label	Success		11:01:18	00:00:14
sdm Exam label	Success		11:01:13	00:00:03

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

Template: Label template (67.3 x 23.99 mm)

Erased by KillDisk for Industrial Systems

Date: 04/02/2020 Time: 11:01:18.563
HDD: WDC WD3200AAJS-61B4A0; Size: 298 GB
Serial: WD-WCAT15440635 Method: One Pass Zeros
Time taken: 00:00:14 Result: Success
Technician____________

Template: Label template

Print start position:

Row: 1 Column: 2

*Page: **Letter / ANSI A**;*
*page size: **215.9** x **279.4 mm**;*
***30** labels per page;*
*label size: **67.3** x **23.99 mm**;*
*orientation: **Portrait**;*
*predefined template: **No**;*

Print options

Default printer for labels: PDF

☐ Skip print preview

Figure 63: Print Label Dialog for Batch

Page template options

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

Print Start Position

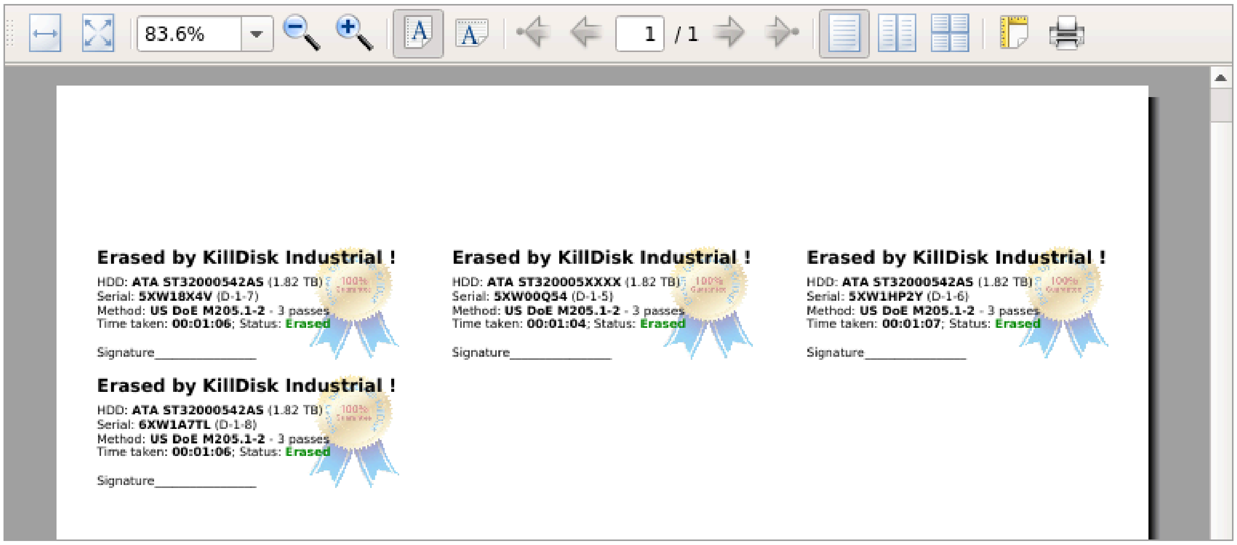
The print start position section of the dialogue allows you to select what label on the page start printing from. The labels won't always start from the 1x1 position so you can adjust this setting accordingly

Print Preview and Printing

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

Skip Print Preview

Disable system Print Preview dialog and print labels immediately



Erased by KillDisk Industrial !
HDD: **ATA ST32000542AS** (1.82 TB)
Serial: **5XW18X4V** (D-1-7)
Method: **US DoE M205.1-2** - 3 passes
Time taken: **00:01:06**; Status: **Erased**

Signature_______________

Erased by KillDisk Industrial !
HDD: **ATA ST320005XXXX** (1.82 TB)
Serial: **5XW00Q54** (D-1-5)
Method: **US DoE M205.1-2** - 3 passes
Time taken: **00:01:04**; Status: **Erased**

Signature_______________

Erased by KillDisk Industrial !
HDD: **ATA ST32000542AS** (1.82 TB)
Serial: **5XW1HP2Y** (D-1-6)
Method: **US DoE M205.1-2** - 3 passes
Time taken: **00:01:07**; Status: **Erased**

Signature_______________

Erased by KillDisk Industrial !
HDD: **ATA ST32000542AS** (1.82 TB)
Serial: **6XW1A7TL** (D-1-8)
Method: **US DoE M205.1-2** - 3 passes
Time taken: **00:01:06**; Status: **Erased**

Signature_______________

Figure 64: Example of Print Preview

Related information

Erase Certificates on page 54

Disk Label Presets on page 119

Reports (XML)

KillDisk gives you the option to save XML reports for any major operation it performs on a disk (such as **Examination**, **Erase**, **Secure Erase** and **Wipe)**. These reports contain all the information regarding to the **KillDisk** procedures, such as:

In order to get the reports generated, simply select and configure them in Processing Report Preferences.

These reports may include (selected by user) all the information regarding to the **KillDisk** procedures, such as:

Company Information

- Name
- License
- Location
- Phone
- Disclaimer

Technician Information

- Name
- Comments

System & Hardware Info

- OS version
- Architecture
- Kernel
- Processors
- Manufacturer

Erase Attributes

- Erase verify
- Passes
- Method
- Verification passes

Error Handling Attributes

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

Disks

- Device Size
- Device Type
- Serial Number
- Revision
- Product Number
- Name
- Geometric Information
- Partitioning Scheme

Batches

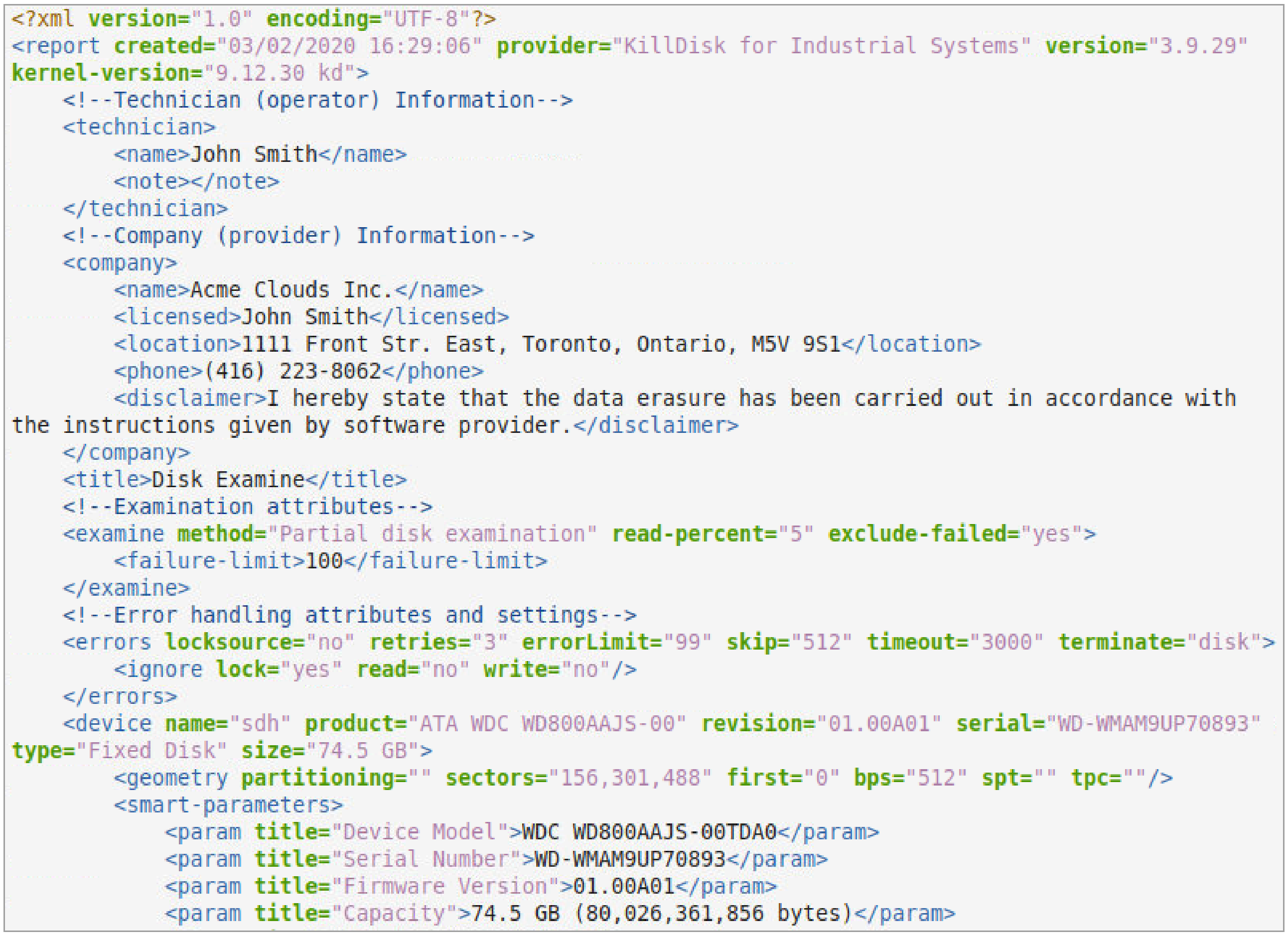
- Name
- Disks
- Time

Additional Attributes

- Fingerprint Information
- Initialization

Erase Result

- Bay
- Time and Date Started
- Disk Information
- Status
- Result
- Time Elapsed
- Errors
- Name of operation



```
<?xml version="1.0" encoding="UTF-8"?>
<report created="03/02/2020 16:29:06" provider="KillDisk for Industrial Systems" version="3.9.29"
kernel-version="9.12.30 kd">
    <!--Technician (operator) Information-->
    <technician>
        <name>John Smith</name>
        <note></note>
    </technician>
    <!--Company (provider) Information-->
    <company>
        <name>Acme Clouds Inc.</name>
        <licensed>John Smith</licensed>
        <location>1111 Front Str. East, Toronto, Ontario, M5V 9S1</location>
        <phone>(416) 223-8062</phone>
        <disclaimer>I hereby state that the data erasure has been carried out in accordance with
the instructions given by software provider.</disclaimer>
    </company>
    <title>Disk Examine</title>
    <!--Examination attributes-->
    <examine method="Partial disk examination" read-percent="5" exclude-failed="yes">
        <failure-limit>100</failure-limit>
    </examine>
    <!--Error handling attributes and settings-->
    <errors locksource="no" retries="3" errorLimit="99" skip="512" timeout="3000" terminate="disk">
        <ignore lock="yes" read="no" write="no"/>
    </errors>
    <device name="sdh" product="ATA WDC WD800AAJS-00" revision="01.00A01" serial="WD-WMAM9UP70893"
type="Fixed Disk" size="74.5 GB">
        <geometry partitioning="" sectors="156,301,488" first="0" bps="512" spt="" tpc=""/>
        <smart-parameters>
            <param title="Device Model">WDC WD800AAJS-00TDA0</param>
            <param title="Serial Number">WD-WMAM9UP70893</param>
            <param title="Firmware Version">01.00A01</param>
            <param title="Capacity">74.5 GB (80,026,361,856 bytes)</param>
```

Figure 65: XML Report Sample

Compact Operating Modes

KillDisk Industrial has advanced operating modes simplifying product usage in the industrial environments.

Touch Mode & Kiosk Mode

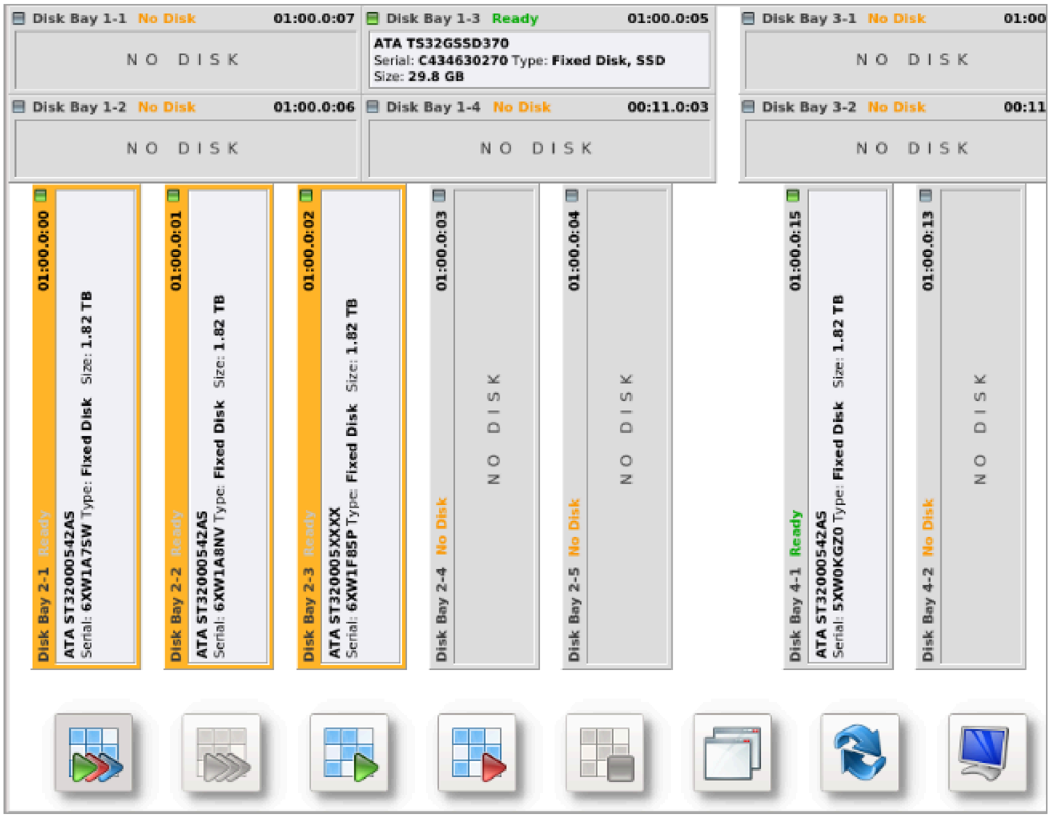
Remember:

These modes are available starting from version 3.0

Compact operating modes added to simplify routing tasks. In these modes user have an access only to the features being used most frequently.

To switch to compact modes, select **Kiosk Mode** (or **Touch Mode**, depending on the product configuration) from the **View** menu. Also, you can press **Ctrl+T** to switch to and return back from compact modes.

All menus, toolbars and other supplementary windows, like Properties and Output will be hidden while operating in compact mode. Access to commands is through floating menu at the bottom left corner of application's main window.



Disk Bay 1-1 No Disk 01:00.0:07
NO DISK

Disk Bay 1-3 Ready 01:00.0:05
ATA TS32GSSD370
Serial: C434630270 Type: Fixed Disk, SSD
Size: 29.8 GB

Disk Bay 3-1 No Disk 01:00
NO DISK

Disk Bay 1-2 No Disk 01:00.0:06
NO DISK

Disk Bay 1-4 No Disk 00:11.0:03
NO DISK

Disk Bay 3-2 No Disk 00:11
NO DISK

Disk Bay 2-1 Ready 01:00.0:00
ATA ST32000542AS
Serial: 6XW1A75W Type: Fixed Disk Size: 1.82 TB

Disk Bay 2-2 Ready 01:00.0:01
ATA ST32000542AS
Serial: 6XW1A8NV Type: Fixed Disk Size: 1.82 TB

Disk Bay 2-3 Ready 01:00.0:02
ATA ST320005XXXX
Serial: 6XW1F85P Type: Fixed Disk Size: 1.82 TB

Disk Bay 2-4 No Disk 01:00.0:03
NO DISK

Disk Bay 2-5 No Disk 01:00.0:04
NO DISK

Disk Bay 4-1 Ready 01:00.0:15
ATA ST32000542AS
Serial: 5XW0KGZ0 Type: Fixed Disk Size: 1.82 TB

Disk Bay 4-2 No Disk 01:00.0:13
NO DISK

There are two compact modes available:

- **Touch Mode** - designed to support portable touch-screen monitors
- **Kiosk Mode** - works similar to previous one but also supports mouse and designed to support commercial grade monitors. It attempts to show as many Disk Bays as possible at once, simplifying visual control and ongoing processes for operator. This mode still supports mouse and giving access to most advanced features. In Kiosk Mode user still have an access to run predefined disk batches, open Erase History View and use other tools.

To switch from compact mode back to windowed operating mode click the most right button (blue computer monitor) at the bottom.

Additional Features

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

Related tasks

Mapping Network Shares on page 68

Related information

Changing Disk Serial Number on page 69

Resetting Hidden Areas on page 70

Property Views on page 71

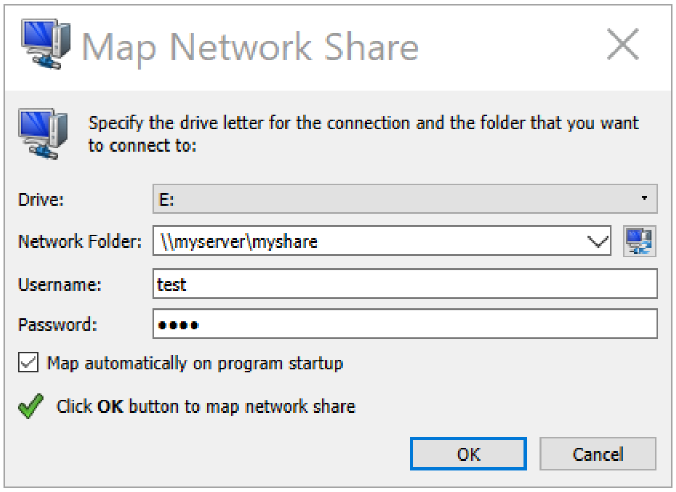
Dynamic Disks: LDM, LVM and WSS on page 73

Mapping Network Shares

This feature provides 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**



Specify the drive letter for the connection and the folder that you want to connect to:

Drive: E:

Network Folder: \\myserver\myshare

Username: test

Password: ●●●●

☑ Map automatically on program startup

✓ Click **OK** button to map network share

Figure 66: Mapping a Network Drive

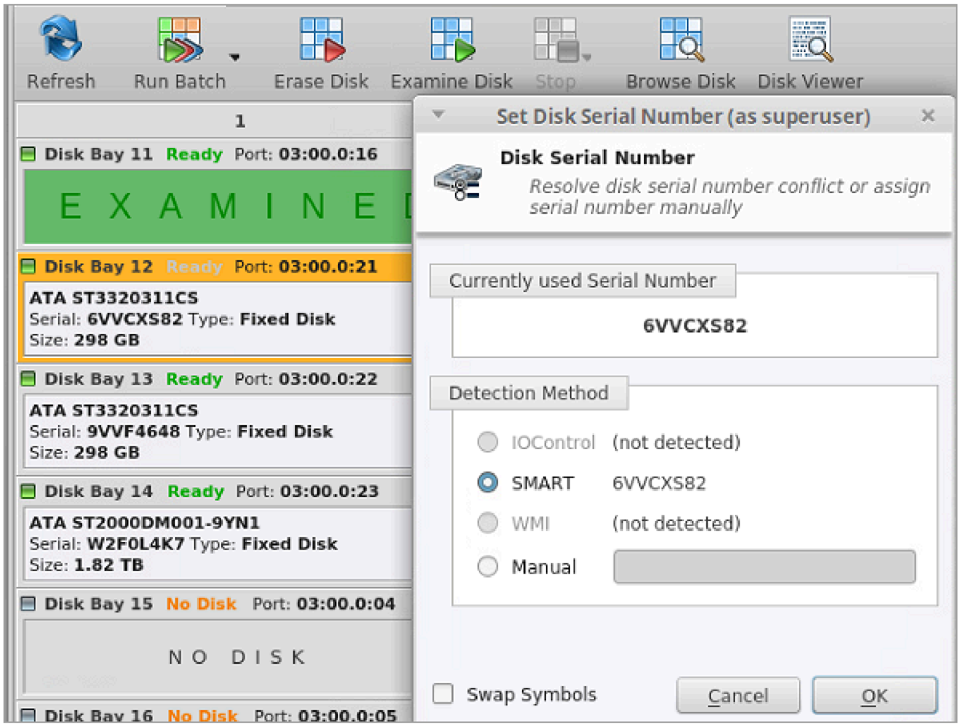
Note:

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. After your network drive is configured, you may select it as a destination for certificates and reports in the Preferences

Changing Disk Serial Number

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



Disk Bay 11 Ready Port: 03:00.0:16

Disk Bay 12 Ready Port: 03:00.0:21
ATA ST3320311CS
Serial: 6VVCXS82 Type: Fixed Disk
Size: 298 GB

Disk Bay 13 Ready Port: 03:00.0:22
ATA ST3320311CS
Serial: 9VVF4648 Type: Fixed Disk
Size: 298 GB

Disk Bay 14 Ready Port: 03:00.0:23
ATA ST2000DM001-9YN1
Serial: W2F0L4K7 Type: Fixed Disk
Size: 1.82 TB

Disk Bay 15 No Disk Port: 03:00.0:04

Disk Bay 16 No Disk Port: 03:00.0:05

Set Disk Serial Number (as superuser)

Disk Serial Number

Resolve disk serial number conflict or assign serial number manually

Currently used Serial Number: 6VVCXS82

Detection Method

○ IOControl (not detected)
● SMART 6VVCXS82
○ WMI (not detected)
○ Manual

□ Swap Symbols

Cancel OK

Figure 67: Setting Disk Serial number

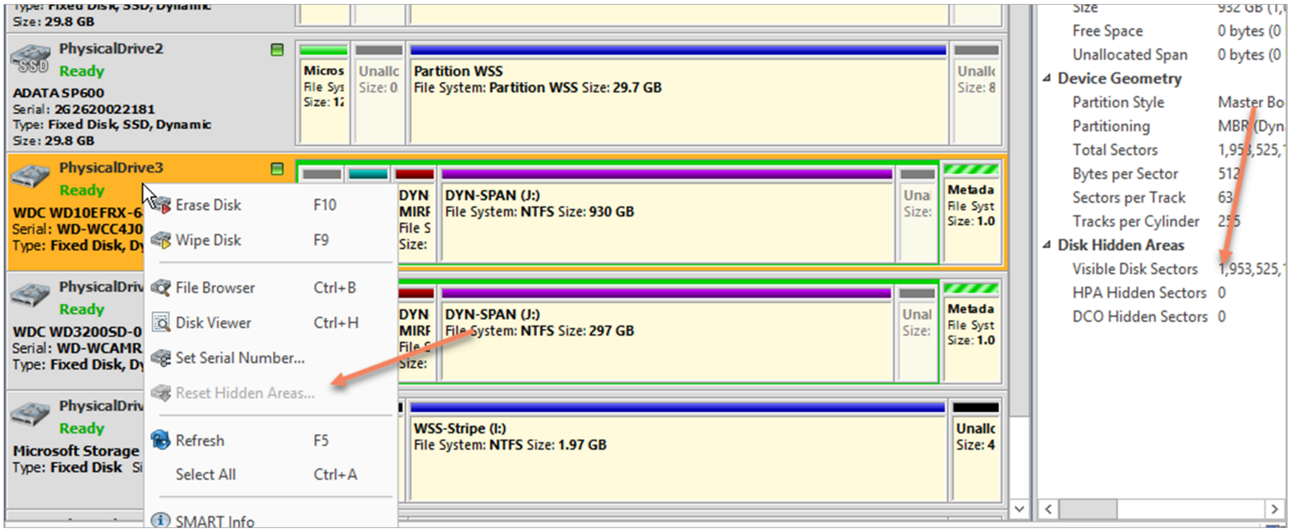
Note:

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).

Resetting Hidden Areas

KillDisk is able to perform erasing of a disk's hidden areas: **HPA** and **DCO**.

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



Type: Fixed Disk, SSD, Dynamic
Size: 29.8 GB

PhysicalDrive2
Ready
ADATA SP600
Serial: 2G2620022181
Type: Fixed Disk, SSD, Dynamic
Size: 29.8 GB

Partition WSS
File System: Partition WSS Size: 29.7 GB

PhysicalDrive3
Ready
WDC WD10EFRX-6
Serial: WD-WCC4J0
Type: Fixed Disk, Dy

DYN-SPAN (J:)
File System: NTFS Size: 930 GB

PhysicalDriv
Ready
WDC WD3200SD-0
Serial: WD-WCAMR
Type: Fixed Disk, Dy

DYN-SPAN (J:)
File System: NTFS Size: 297 GB

PhysicalDriv
Ready
Microsoft Storage
Type: Fixed Disk Si

WSS-Stripe (I:)
File System: NTFS Size: 1.97 GB

Size 932 GB (1,
Free Space 0 bytes (0
Unallocated Span 0 bytes (0

Device Geometry
Partition Style Master Bo
Partitioning MBR (Dyn
Total Sectors 1,953,525,
Bytes per Sector 512
Sectors per Track 63
Tracks per Cylinder 255

Disk Hidden Areas
Visible Disk Sectors 1,953,525,
HPA Hidden Sectors 0
DCO Hidden Sectors 0

Figure 68: Resetting Hidden Areas

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

Related information

Disk Hidden Zones (HPA/DCO) on page 155

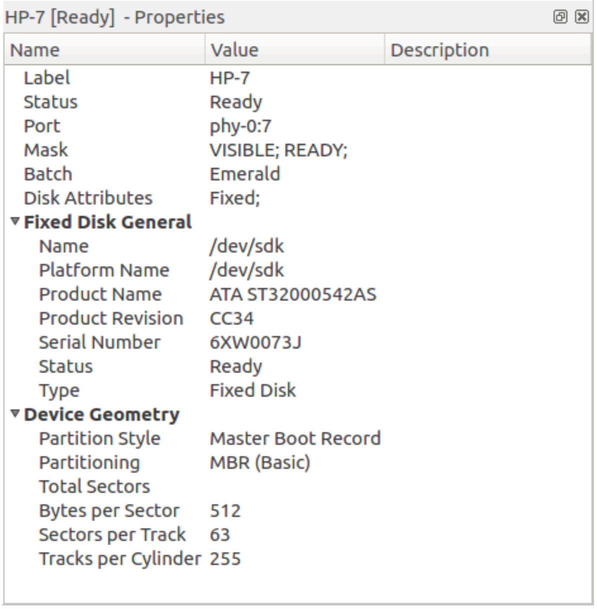
Property Views

To show detailed information about any subject of an application (such as disk, partition, volume, file etc.) **KillDisk** uses information Views. They follow selected changes and show information about the selected item automatically when open.

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**



HP-7 [Ready] - Properties

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

Figure 69: Property View Example

Besides displaying a valuable data it also allows you to copy that information into a clipboard by using context menu commands.

Context menu commands:

Copy Value

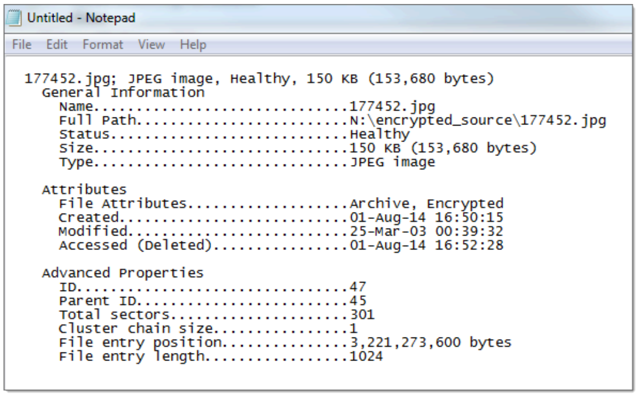
Copy *value* (value only) of selected field in the information View

Copy Field

Copy formatted *name* and *value* pair

Copy All

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



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

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

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

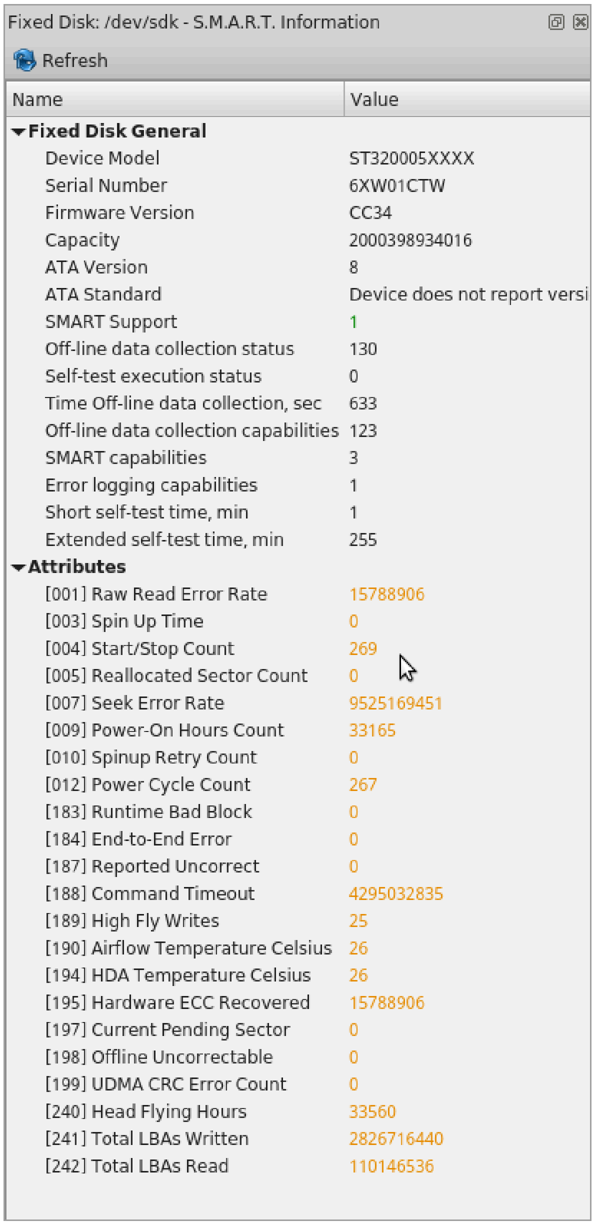
Figure 70: Example of Copied Information

S.M.A.R.T. Information

This is another information View displaying S.M.A.R.T. (*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



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

Figure 71: SMART Information Example

S.M.A.R.T. data can be used to diagnose disks by showing important information such as Power-on Hours, Reallocated Sectors and Current Pending Sectors.

Note:

When Current Pending Sectors parameter differs from zero, this means the disk has bad sectors. It will cause problems in the future. Dispose these disks as soon as possible.

Related information

S.M.A.R.T. Monitor on page 91
Preferences on page 99

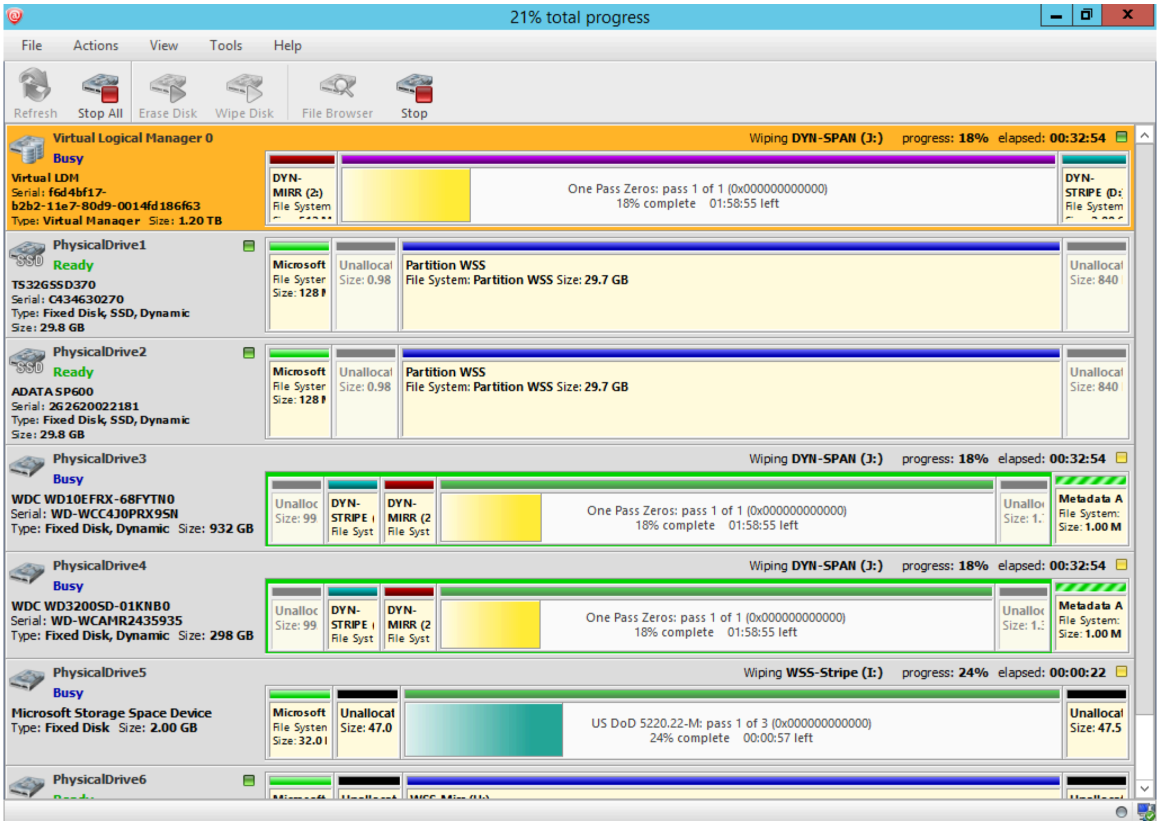
Dynamic Disks: LDM, LVM and WSS

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 see it reflected on the components disks as well.



Virtual Logical Manager 0
Busy
Virtual LDM
Serial: f6d4bf17-b2b2-11e7-80d9-0014fd186f63
Type: Virtual Manager Size: 1.20 TB
Wiping DYN-SPAN (J:) progress: 18% elapsed: 00:32:54
One Pass Zeros: pass 1 of 1 (0x000000000000)
18% complete 01:58:55 left

PhysicalDrive1
Ready
TS32GSSD370
Serial: C434630270
Type: Fixed Disk, SSD, Dynamic
Size: 29.8 GB
Partition WSS
File System: Partition WSS Size: 29.7 GB

PhysicalDrive2
Ready
ADATA SP600
Serial: 2G2620022181
Type: Fixed Disk, SSD, Dynamic
Size: 29.8 GB
Partition WSS
File System: Partition WSS Size: 29.7 GB

PhysicalDrive3
Busy
WDC WD10EFRX-68FYTN0
Serial: WD-WCC4J0PRX9SN
Type: Fixed Disk, Dynamic Size: 932 GB
Wiping DYN-SPAN (J:) progress: 18% elapsed: 00:32:54
One Pass Zeros: pass 1 of 1 (0x000000000000)
18% complete 01:58:55 left

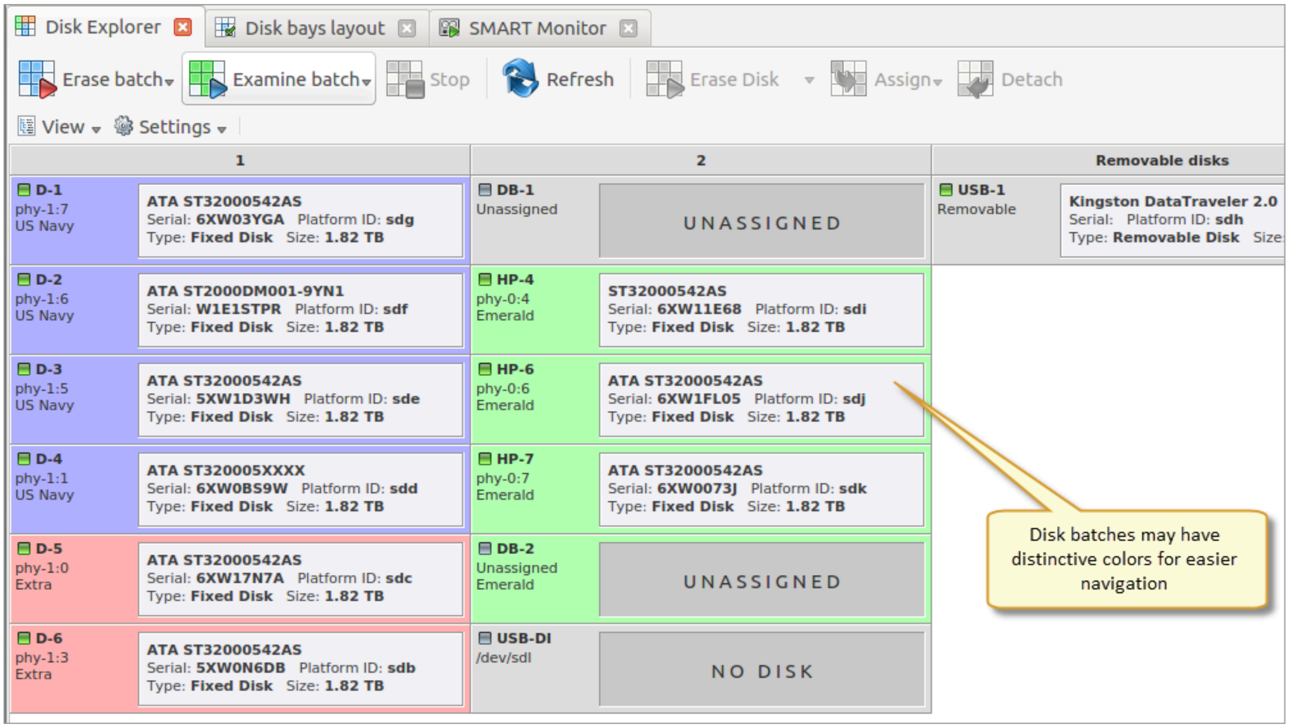
PhysicalDrive4
Busy
WDC WD3200SD-01KNB0
Serial: WD-WCAMR2435935
Type: Fixed Disk, Dynamic Size: 298 GB
Wiping DYN-SPAN (J:) progress: 18% elapsed: 00:32:54
One Pass Zeros: pass 1 of 1 (0x000000000000)
18% complete 01:58:55 left

PhysicalDrive5
Busy
Microsoft Storage Space Device
Type: Fixed Disk Size: 2.00 GB
Wiping WSS-Stripe (I:) progress: 24% elapsed: 00:00:22
US DoD 5220.22-M: pass 1 of 3 (0x000000000000)
24% complete 00:00:57 left

Figure 72: Virtual drive (Striped Disk Array) being erased in Windows Storage Spaces

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. User is free to use disk batches in any manner. Disks can be added or removed from *Batch* at any time.



1		2		Removable disks	
D-1 phy-1:7 US Navy	ATA ST32000542AS Serial: 6XW03YGA Platform ID: sdg Type: Fixed Disk Size: 1.82 TB	DB-1 Unassigned	UNASSIGNED	USB-1 Removable	Kingston DataTraveler 2.0 Serial: Platform ID: sdh Type: Removable Disk Size
D-2 phy-1:6 US Navy	ATA ST2000DM001-9YN1 Serial: W1E1STPR Platform ID: sdf Type: Fixed Disk Size: 1.82 TB	HP-4 phy-0:4 Emerald	ST32000542AS Serial: 6XW11E68 Platform ID: sdi Type: Fixed Disk Size: 1.82 TB		
D-3 phy-1:5 US Navy	ATA ST32000542AS Serial: 5XW1D3WH Platform ID: sde Type: Fixed Disk Size: 1.82 TB	HP-6 phy-0:6 Emerald	ATA ST32000542AS Serial: 6XW1FL05 Platform ID: sdj Type: Fixed Disk Size: 1.82 TB		
D-4 phy-1:1 US Navy	ATA ST320005XXXX Serial: 6XW0BS9W Platform ID: sdd Type: Fixed Disk Size: 1.82 TB	HP-7 phy-0:7 Emerald	ATA ST32000542AS Serial: 6XW0073J Platform ID: sdk Type: Fixed Disk Size: 1.82 TB		
D-5 phy-1:0 Extra	ATA ST32000542AS Serial: 6XW17N7A Platform ID: sdc Type: Fixed Disk Size: 1.82 TB	DB-2 Unassigned Emerald	UNASSIGNED		
D-6 phy-1:3 Extra	ATA ST32000542AS Serial: 5XW0N6DB Platform ID: sdb Type: Fixed Disk Size: 1.82 TB	USB-DI /dev/sdl	NO DISK		

Disk batches may have distinctive colors for easier navigation

Figure 73: 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 performs the operation on all the disks in the batch.

Related tasks

Assign Disk Bays to Batches on page 77

Related information

Create / Delete Batches on page 75

Edit Batch Attributes on page 79

Create / Delete Batches

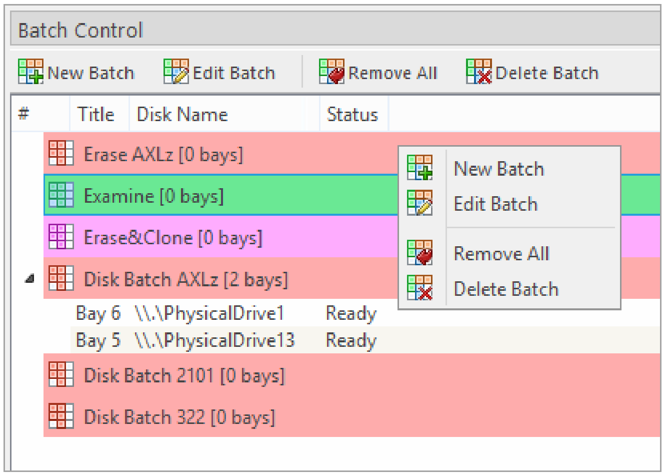
Create a Disk Batch

Disk batches are created using the Batch Control toolbox.

Note:

If you can't find the Batch Control toolbox make sure that you have a proper View activated. To do this navigate to the file menu bar and 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.



#	Title	Disk Name	Status
	Erase AXLz [0 bays]		
	Examine [0 bays]		
	Erase&Clone [0 bays]		
	Disk Batch AXLz [2 bays]		
	Bay 6	\\.\PhysicalDrive1	Ready
	Bay 5	\\.\PhysicalDrive13	Ready
	Disk Batch 2101 [0 bays]		
	Disk Batch 322 [0 bays]		

Figure 74: Batch Control Toolbox

Adding disks to a Disk Batch

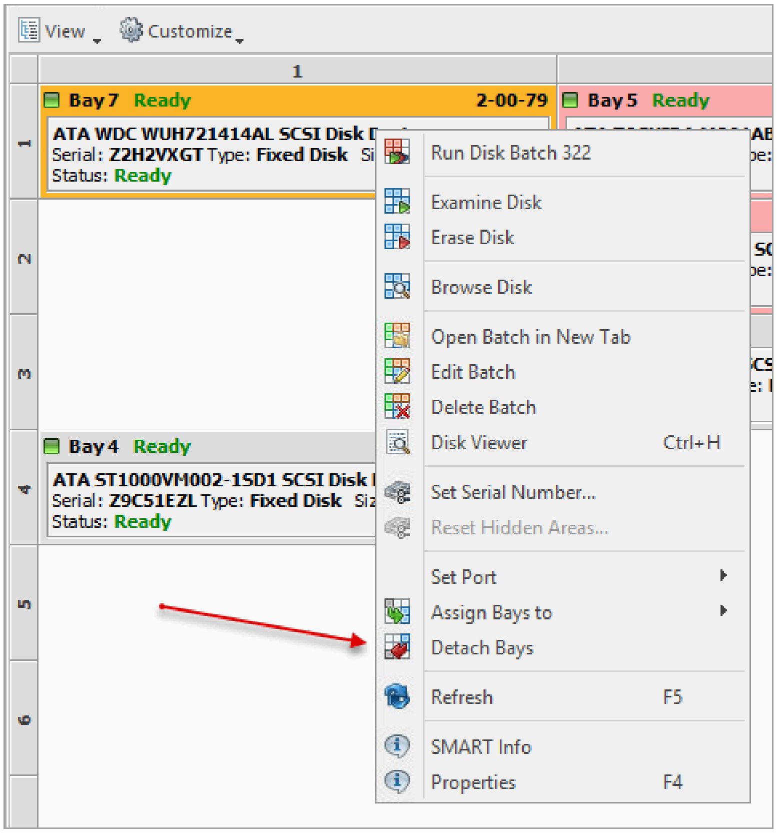
Disk Bays can be added to Batches in several ways:

- 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 but select bays that are attached to batches and choose the **Detach Bays** command.



Deleting Batches

Batches can be deleted by selecting the batch in the Batch Control toolbar and choosing the **Delete Batch** or **Remove All** commands.

Edit Batch attributes

Batch attributes can be edited at any time after batch created. See: Edit Batch Attributes on page 79

Note:

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

Related tasks

Assign Disk Bays to Batches on page 77

Related information

Disk Batches on page 74

Edit Batch Attributes on page 79

Assign Disk Bays to Batches

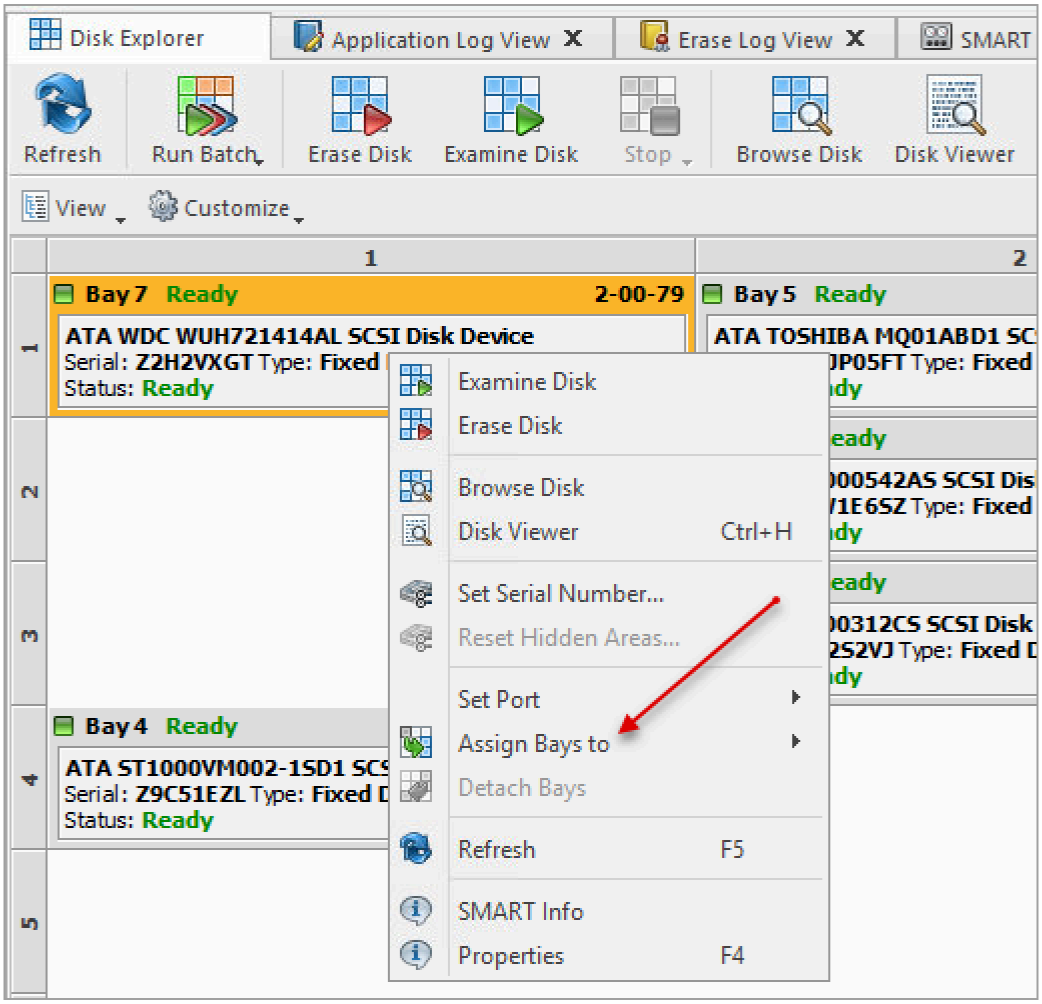
Disk Bays can be assigned to existing Batches in order to apply same batch attributes for selected tasks (disk erase, cloning etc).

Note:

Disk Bay can only belong to one Batch.

Disk Bays are assigned to Batches in one of several ways:

From Disk Bays View



Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed
Status: Ready

Bay 5 Ready
ATA TOSHIBA MQ01ABD1 SC
JP05FT Type: Fixed
dy

eady
000542AS SCSI Dis
/1E6SZ Type: Fixed
dy

eady
00312CS SCSI Disk
2S2VJ Type: Fixed
dy

Bay 4 Ready
ATA ST1000VM002-1SD1 SCS
Serial: Z9C51EZL Type: Fixed
Status: Ready

Figure 75: Assign Disk Bay to Batch in 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 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

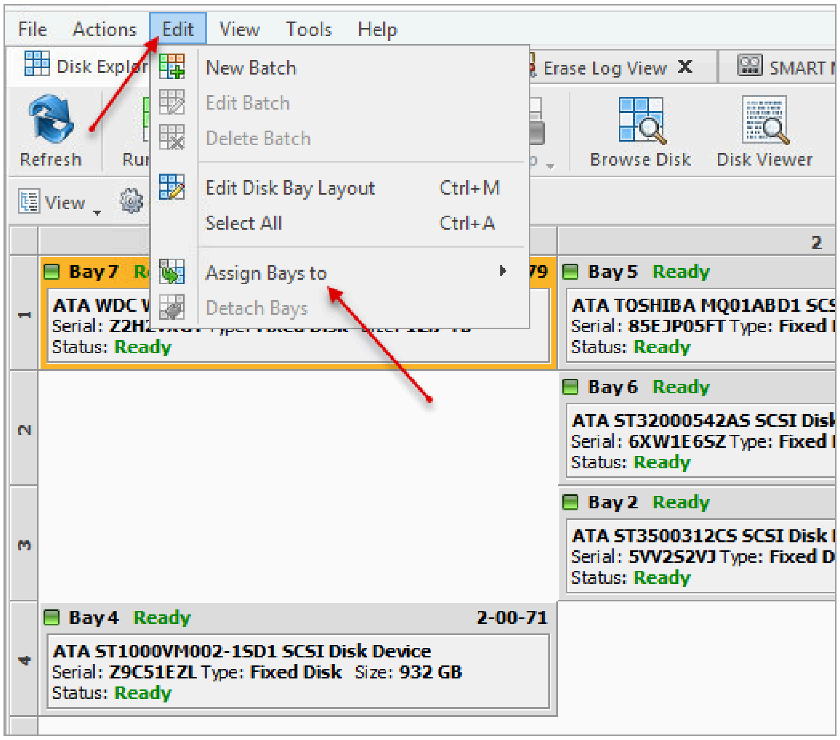


Figure 76: Assign Disk to Batch from Edit menu

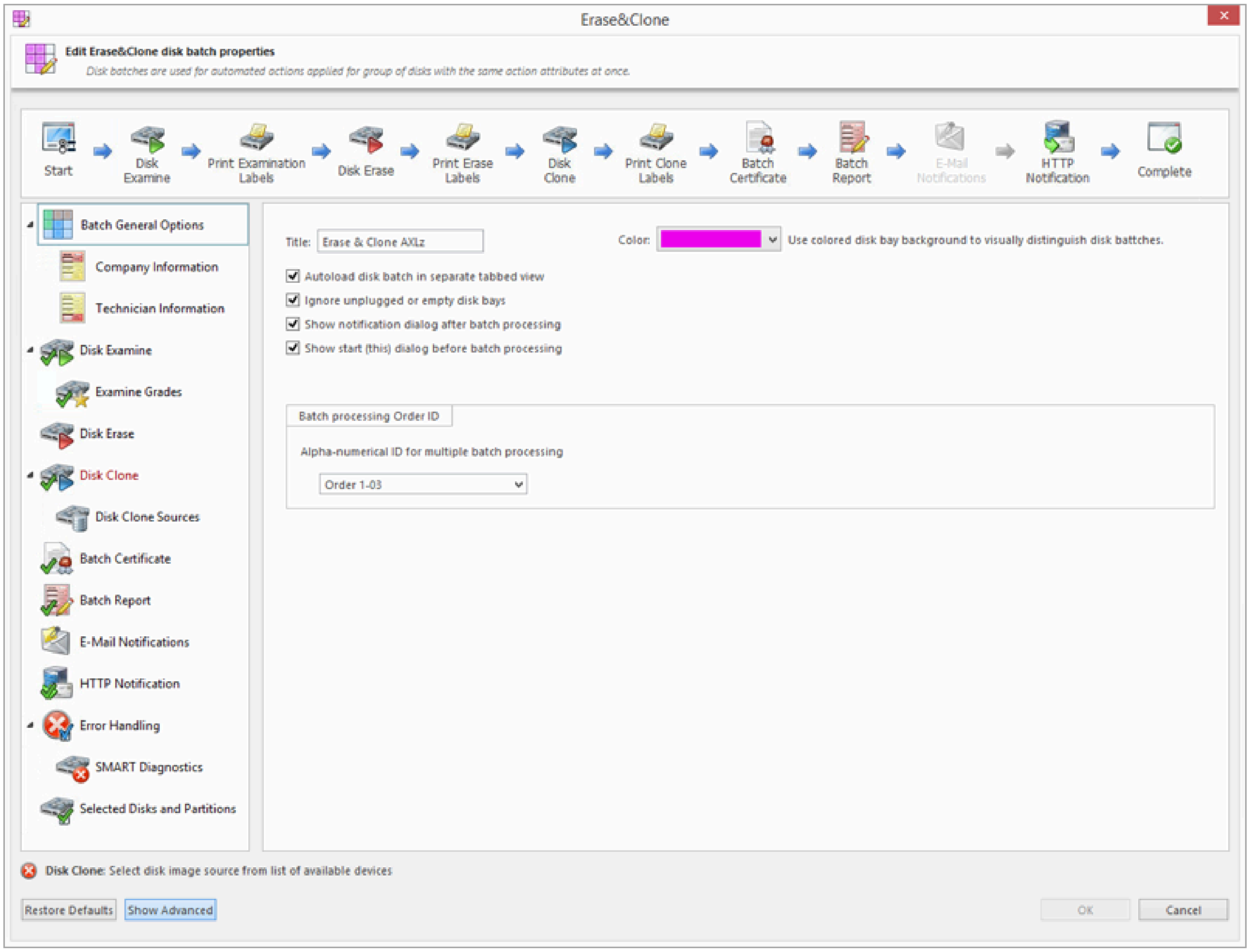
1. In the Disk Explorer: select the Disk Bay(s) that needs to be assigned
2. Click **Edit** menu
3. Hover the **Assign Bays to** action to see a complete list of available Batches
4. Click on the desired Batch. The selected Bay(s) will be assigned to that Batch.

Edit Batch Attributes

After creating a new Disk Batch user is able to work with Edit Batch window where the Batch settings can be changed. For existing Batches it is possible to access this window by selecting the desired Batch in the Batch Control toolbox and clicking **Edit Batch**.

Batch General Settings

These are General Settings for the Batch (such as Title, Color, how the Batch is displayed etc.)



Edit Erase&Clone disk batch properties

Disk batches are used for automated actions applied for group of disks with the same action attributes at once.

Title: Erase & Clone AXLz

Color: Use colored disk bay background to visually distinguish disk battches.

☑ Autoload disk batch in separate tabbed view

☑ Ignore unplugged or empty disk bays

☑ Show notification dialog after batch processing

☑ Show start (this) dialog before batch processing

Batch processing Order ID

Alpha-numerical ID for multiple batch processing

Order 1-03

Disk Clone: Select disk image source from list of available devices

Figure 77: Batch Editor - General Settings

Company Information

These settings allow user to configure Company Information for Erase Certificates and Batch Processing Reports.

It is the same form as in **Preferences** > **Company Information**

Technician Information

This setting allows user to configure Technician Information for Erase Certificates and Batch Processing Reports.

It is the same form as in **Preferences** > **Technician Information**

Disk Examine

These settings configure the disk examine settings for the Batch. Type of examination and Disk Label Presets can be selected here. Examine Grade colors can be individually configured by clicking **Examine Grades** button.

Read Disk Examine on page 107 for description of each attribute.

Disk Erase

These settings configure disk erase settings for the Batch. Erase methods, verification and report settings can be changed here.

Read Disk Erase on page 103 for description of each attribute.

Disk Wipe

These settings configure disk wipe settings for the Batch. Erase methods, verification and report settings can be changed here.

Read Disk Wipe on page 106 for description of each attribute.

Disk Clone

This feature allows user to configure either a disk or disk image for cloning to all the disks in the batch. Available for Erase Batches with examined disks only.

Read Clone Sources on page 109 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 a name, destination, details and comments etc.). Options for printing and issuing individual certificates for the particular disk in the Batch can be configured.

Read Erase Certificate on page 111 for description of each attribute.

Batch Report

These settings give user an option to toggle whether or not to issue an erasure XML report upon erase and configure the options to include (like a name, destination, S.M.A.R.T. details etc.). Options for issuing individual XML reports for the particular disks in the batch can be configured.

Read Processing Report on page 115 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 E-mail Notifications on page 126 for description of each attribute and SMTP settings configuration.

HTTP Notifications

User can turn on HTTP notifications for Batch operations.

Read HTTP Notifications on page 128 and specify server address, port and parameters (name tags) in the URL field.

Disk Labels

User can turn on displaying and printing disk labels after Batch operation is completed. As well as configuring a default printer and customizing label templates.

Read Disk Label Presets on page 119 for description of each attribute.

Error Handling

For each Batch error handling attributes can be set individually. S.M.A.R.T. attributes may also be configured in error handling by clicking **SMART Diagnostics** button.

Read Error Handling on page 125 for description of each attribute.

Related information

Disk Batches on page 74

Create / Delete Batches on page 75

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** makes it possible to browse through disks on both: a file level and a low, hexadecimal (HEX) level. Disk health analysis with its S.M.A.R.T. monitor as well as logs/reports export to the external databases fully supported in **KillDisk Industrial** version. This section describes each of these features:

- File Browser
- Hexadecimal Viewer
- SMART monitor
- Erase History with ability to Export to Database/CSV

File Browser

KillDisk includes a built-in File Browser for examining the contents of disks for verification purposes, for hard drives' selection control or for erased files validation after erase or wipe. Details on using this feature are discussed in this section.

Note:

KillDisk detects existing files as well as files that have been deleted but **not** sanitized. They appear *gray* and indicate deleted files with a high probability of being recovered with a special 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 the related command from the context menu. Shortcut is **Ctrl-B**.

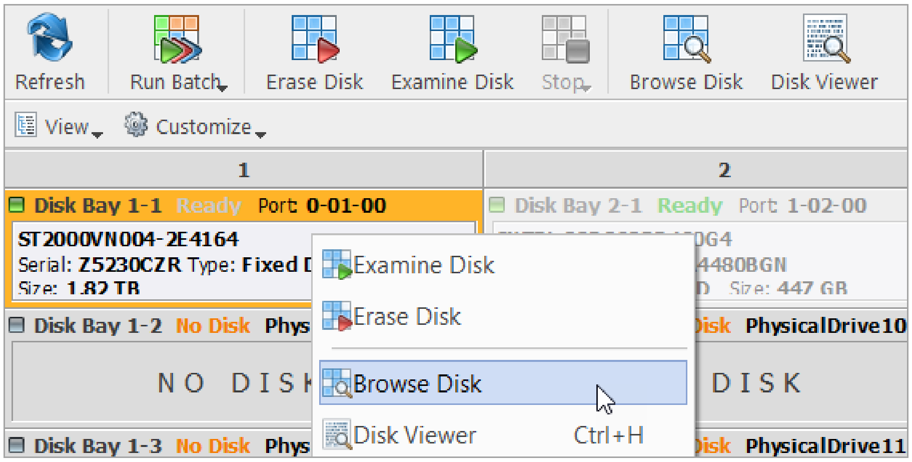
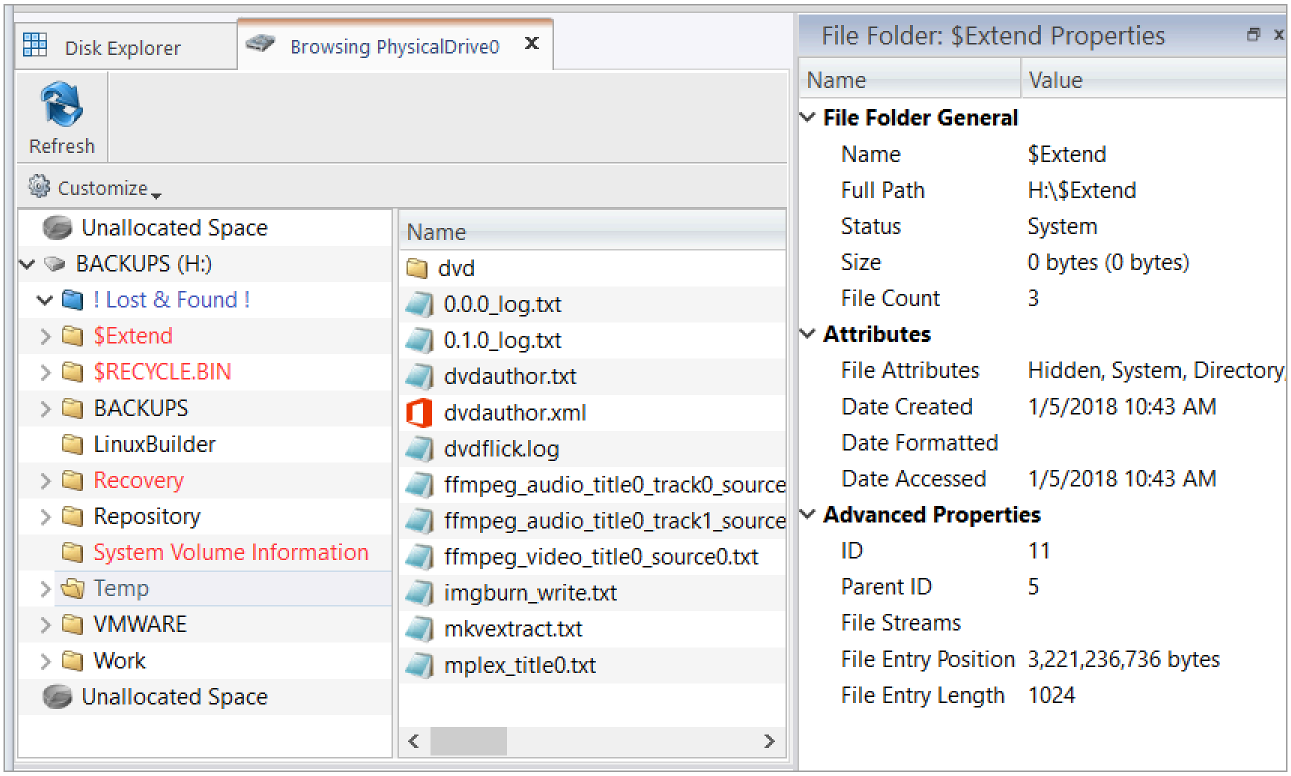


Figure 78: Launching the File Browser

This will open the File Browser tab:



- Unallocated Space
- BACKUPS (H:)
  - ! Lost & Found !
  - $Extend
  - $RECYCLE.BIN
  - BACKUPS
  - LinuxBuilder
  - Recovery
  - Repository
  - System Volume Information
  - Temp
  - VMWARE
  - Work
- Unallocated Space

Name
dvd
0.0.0_log.txt
0.1.0_log.txt
dvdauthor.txt
dvdauthor.xml
dvdflick.log
ffmpeg_audio_title0_track0_source
ffmpeg_audio_title0_track1_source
ffmpeg_video_title0_source0.txt
imgburn_write.txt
mkvextract.txt
mplex_title0.txt

File Folder: $Extend Properties

Name	Value
File Folder General	
Name	$Extend
Full Path	H:\$Extend
Status	System
Size	0 bytes (0 bytes)
File Count	3
Attributes	
File Attributes	Hidden, System, Directory
Date Created	1/5/2018 10:43 AM
Date Formatted	
Date Accessed	1/5/2018 10:43 AM
Advanced Properties	
ID	11
Parent ID	5
File Streams	
File Entry Position	3,221,236,736 bytes
File Entry Length	1024

Figure 79: File Browser Window

The File Browser tab displays files and folders on the disk being selected.

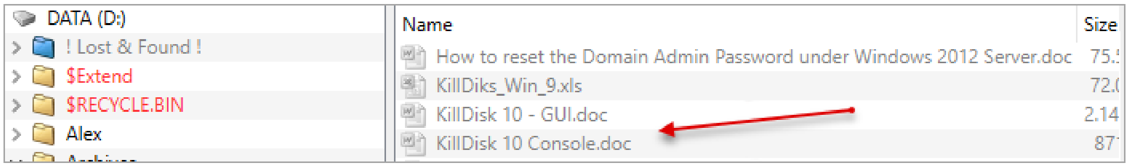
The File Browser tabbed View may also be manipulated by navigating to the **Customize** button at the top.

Here you have options to adjust:

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



- DATA (D:)
  - ! Lost & Found !
  - $Extend
  - $RECYCLE.BIN
  - Alex

Name	Size
How to reset the Domain Admin Password under Windows 2012 Server.doc	75.!
KillDiks_Win_9.xls	72.(
KillDisk 10 - GUI.doc	2.14
KillDisk 10 Console.doc	87

Figure 80: Deleted Files in the File Browser

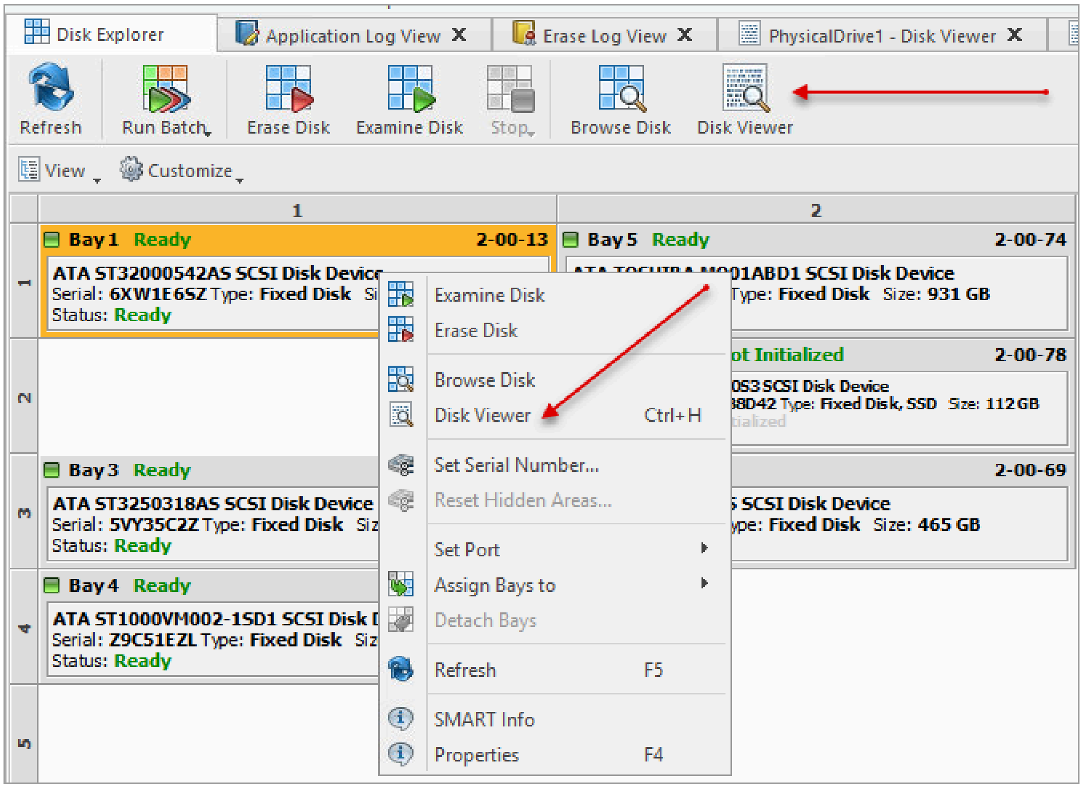
Grey files indicate deleted files have not been sanitized. These files are recoverable. Running **KillDisk**'s Wipe operation ensures these files are unrecoverable and make these gray files disappear from the File Browser.

Note:

Found deleted files appear in their original directory (before they were deleted). The **! Lost & Found !** folder is a virtual directory created for found deleted files with not discovered directory information.

Disk Viewer

Disk Viewer allows users to view the contents of connected drives on a sector's level in a hexadecimal, ASCII and Unicode representations. User is able to launch Disk Viewer from all main Views (**Disk Bays** , **Local Devices** , **My Computer**) as well as through the main menu bar. Shortcut is **Ctrl-H** .



Bay 1 Ready 2-00-13
ATA ST32000542AS SCSI Disk Device
Serial: 6XW1E6SZ Type: Fixed Disk Si
Status: Ready

Bay 5 Ready 2-00-74
ATA TOSHIBA M001ABD1 SCSI Disk Device
Type: Fixed Disk Size: 931 GB

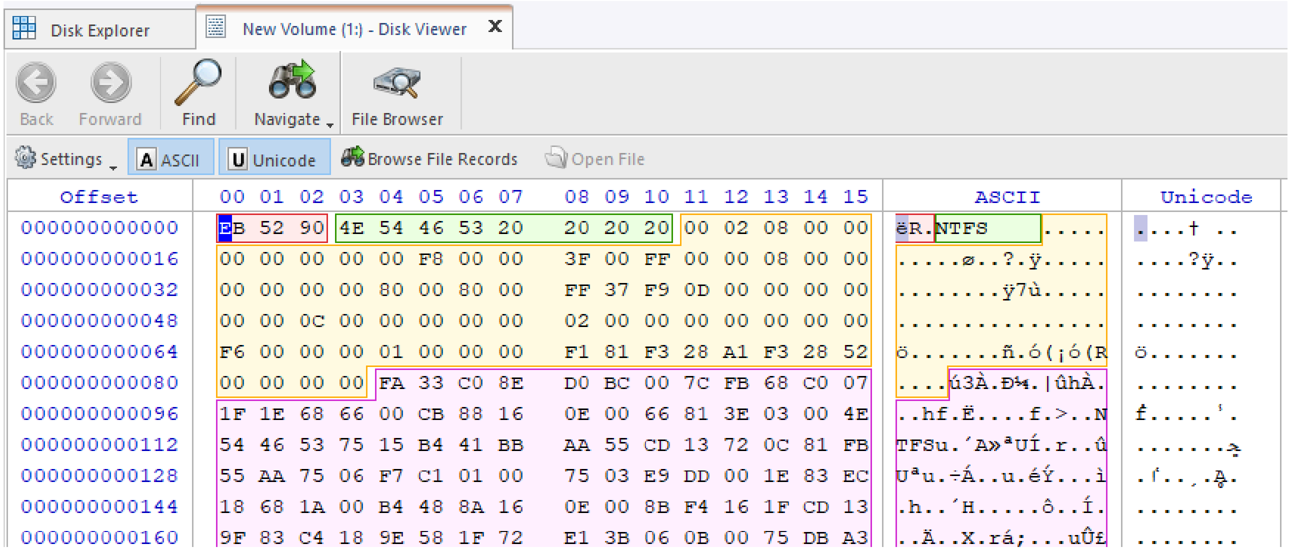
ot Initialized 2-00-78
053 SCSI Disk Device
38D42 Type: Fixed Disk, SSD Size: 112 GB
tialized

Bay 3 Ready
ATA ST3250318AS SCSI Disk Device
Serial: 5VY35C2Z Type: Fixed Disk Siz
Status: Ready

2-00-69
5 SCSI Disk Device
ype: Fixed Disk Size: 465 GB

Bay 4 Ready
ATA ST1000VM002-1SD1 SCSI Disk D
Serial: Z9C51EZL Type: Fixed Disk Siz
Status: Ready

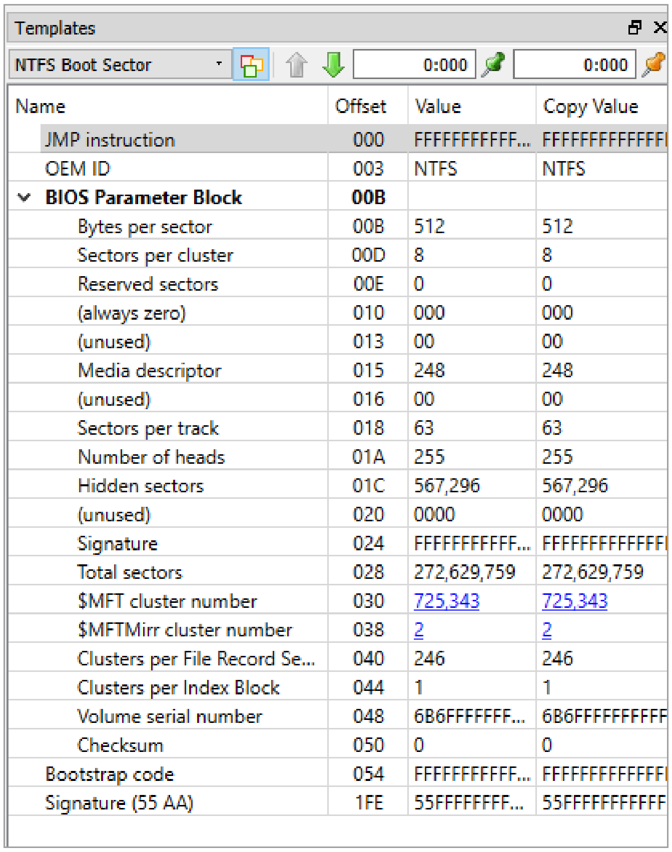
Figure 81: Starting a Disk Viewer



```
Offset          00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15   ASCII              Unicode
000000000000    EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00   ëR.NTFS    .....   ....† ..
000000000016    00 00 00 00 00 F8 00 00  3F 00 FF 00 00 08 00 00   .....ø..?.ÿ.....   ....?ÿ..
000000000032    00 00 00 00 80 00 80 00  FF 37 F9 0D 00 00 00 00   ........ÿ7ù.....   ........
000000000048    00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00   ................   ........
000000000064    F6 00 00 00 01 00 00 00  F1 81 F3 28 A1 F3 28 52   ö.......ñ.ó(¡ó(R   ö.......
000000000080    00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07   ....ú3À.Ð¼.|ûhÀ.   ........
000000000096    1F 1E 68 66 00 CB 88 16  0E 00 66 81 3E 03 00 4E   ..hf.Ë....f.>..N   f.....ˈ.
000000000112    54 46 53 75 15 B4 41 BB  AA 55 CD 13 72 0C 81 FB   TFSu.´A»ªUÍ.r..û   ........
000000000128    55 AA 75 06 F7 C1 01 00  75 03 E9 DD 00 1E 83 EC   Uªu.÷Á..u.éÝ...ì   ........
000000000144    18 68 1A 00 B4 48 8A 16  0E 00 8B F4 16 1F CD 13   .h..´H.....ô..Í.   ........
000000000160    9F 83 C4 18 9E 58 1F 72  E1 3B 06 0B 00 75 DB A3   ..Ä..X.rá;...uÛ£   ........
```

Figure 82: NTFS Volume is opened in Disk Viewer

KillDisk also offers a list of templates to help display the organization of the sectors on the disk by colored sections. Example above displays what happens when NTFS Volume is opened in the Disk Viewer. In this case NTFS Boot Sector template has been attached automatically, and below is NTFS Boot Sector template details in Templates View.



Name	Offset	Value	Copy Value
JMP instruction	000	FFFFFFFFFFF...	FFFFFFFFFFFFF
OEM ID	003	NTFS	NTFS
BIOS Parameter Block	**00B**		
Bytes per sector	00B	512	512
Sectors per cluster	00D	8	8
Reserved sectors	00E	0	0
(always zero)	010	000	000
(unused)	013	00	00
Media descriptor	015	248	248
(unused)	016	00	00
Sectors per track	018	63	63
Number of heads	01A	255	255
Hidden sectors	01C	567,296	567,296
(unused)	020	0000	0000
Signature	024	FFFFFFFFFFF...	FFFFFFFFFFFFF
Total sectors	028	272,629,759	272,629,759
$MFT cluster number	030	725,343	725,343
$MFTMirr cluster number	038	2	2
Clusters per File Record Se...	040	246	246
Clusters per Index Block	044	1	1
Volume serial number	048	6B6FFFFFFF...	6B6FFFFFFFFFF
Checksum	050	0	0
Bootstrap code	054	FFFFFFFFFFF...	FFFFFFFFFFFFF
Signature (55 AA)	1FE	55FFFFFFFF...	55FFFFFFFFFFF

Figure 83: NTFS Boot Sector Template Details

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

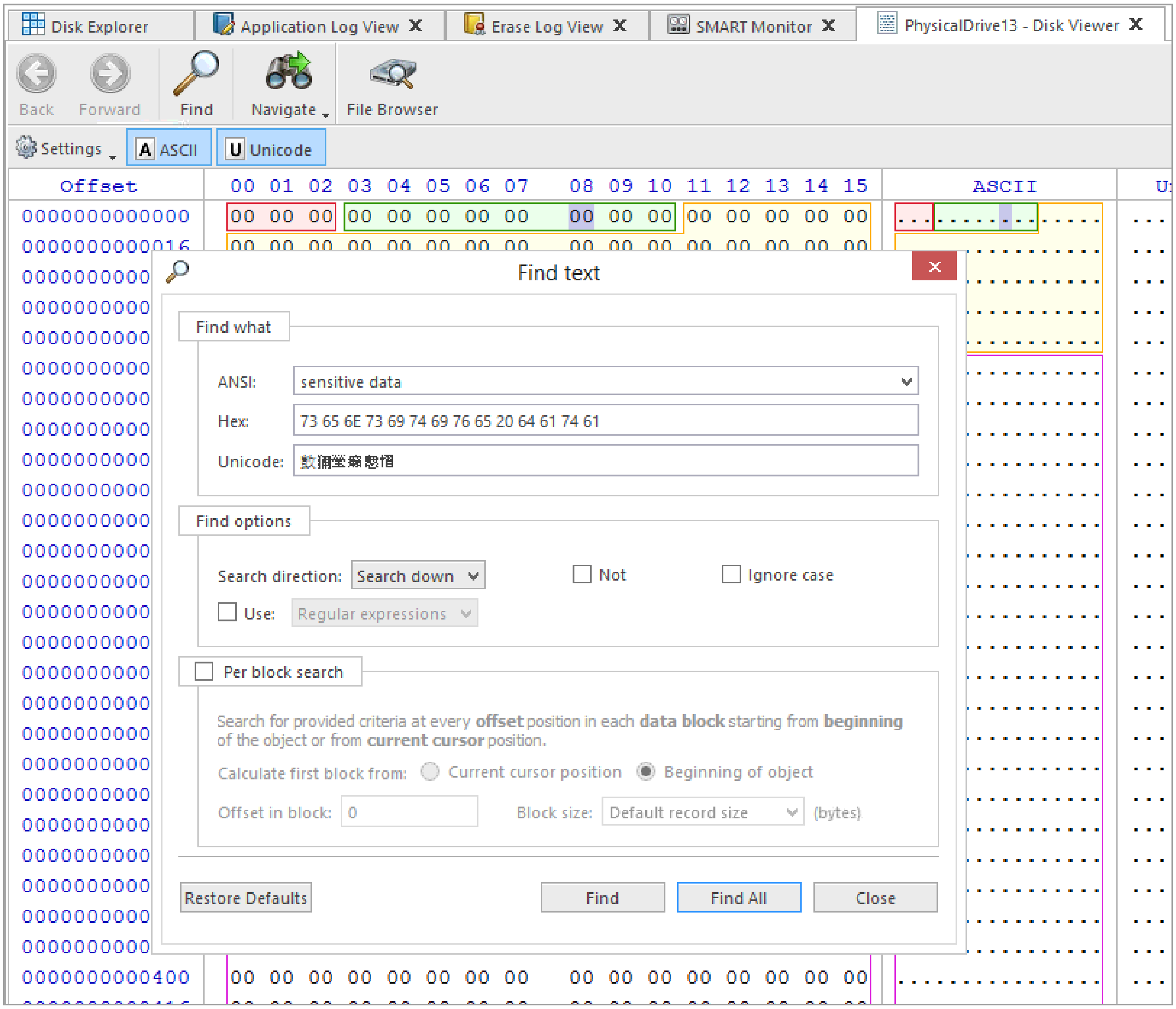
Disables case-sensitivity in the search

Use

Select between *Regular Expressions* and *Wildcards*

Per block search

To speed up the search process (if you are familiar with the location of the data in the data block) you may specify a search with an offset of the object



Find text

Find what

ANSI: sensitive data

Hex: 73 65 6E 73 69 74 69 76 65 20 64 61 74 61

Unicode: 敳湳瑩癩⁥慤慴

Find options

Search direction: Search down

□ Not

□ Ignore case

□ Use: Regular expressions

□ Per block search

Search for provided criteria at every **offset** position in each **data block** starting from **beginning** of the object or from **current cursor** position.

Calculate first block from: ○ Current cursor position ● Beginning of object

Offset in block: 0

Block size: Default record size (bytes)

Figure 84: Finding Data

Disk Viewer's Navigate feature allows:

Go to Offset

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

Go to Sector

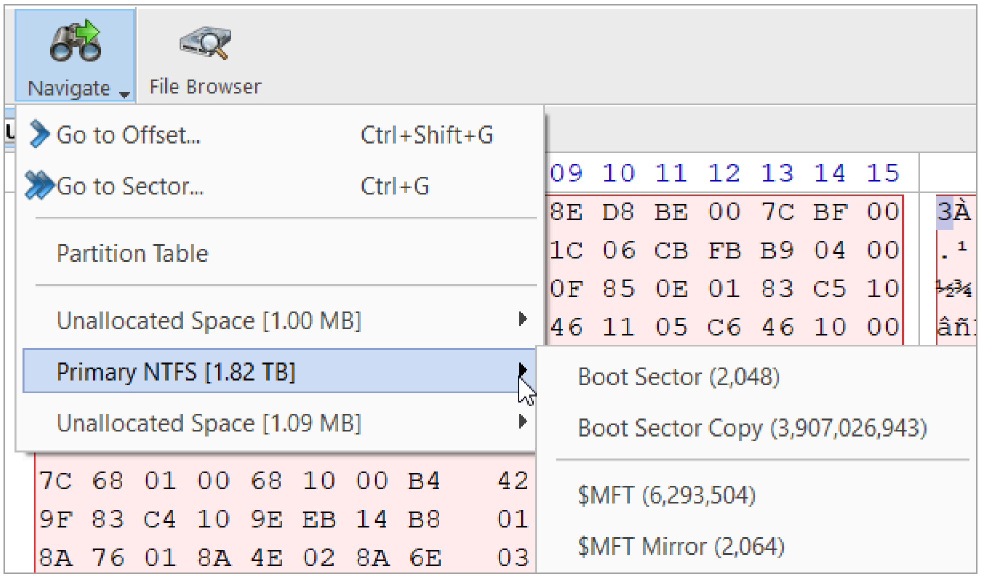
Jumps to the particular sector or cluster on the disk

Partition Table

Jumps to the sector where partition table is located

Particular Partition

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



```
09 10 11 12 13 14 15
8E D8 BE 00 7C BF 00   3À
1C 06 CB FB B9 04 00   . ¹
0F 85 0E 01 83 C5 10   ½¾
46 11 05 C6 46 10 00   âñ
7C 68 01 00 68 10 00 B4   42
9F 83 C4 10 9E EB 14 B8   01
8A 76 01 8A 4E 02 8A 6E   03
```

Figure 85: Disk Viewer Navigation Options

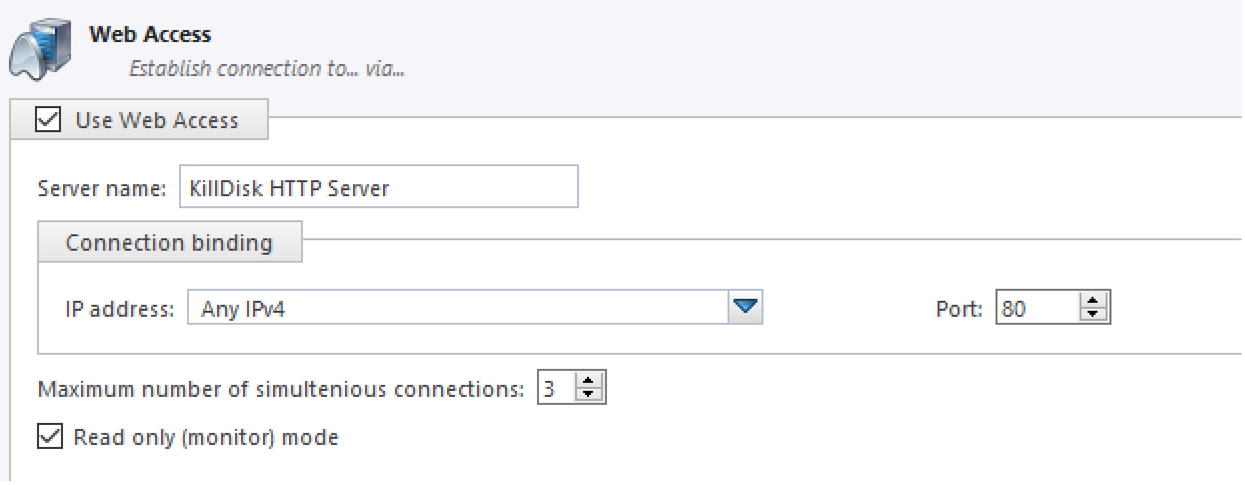
Web Service

KillDisk supports monitoring of workstations state and all running processes from remote computer via standard HTTP protocol in any Web Browser. Just navigate to the menu bar and select **Tools** > **Web Service** > **Start Web Service** to activate build-in Web Server and allow remote web clients to monitor the state of application. Green icon in the status bar will display service status (Started/Stopped, Read Only/Interactive).

In order to start the Web Service properly, connection parameters for the remote host must be configured first.

Web Service Configuration

Navigate **Tools** > **Web Service** > **Settings** or the related tab in **Preferences** to configure remote connection parameters:



Web Access

Establish connection to... via...

☑ Use Web Access

Server name: KillDisk HTTP Server

Connection binding

IP address: Any IPv4   Port: 80

Maximum number of simultenious connections: 3

☑ Read only (monitor) mode

Figure 86: Web Service Settings

Server Name
Type the name of current workstation to be displayed on remote hosts

IP Address
Web Service can be running on all IP addresses (version 4 protocol) assigned to current workstation or on the particular IP. Drop-down list box enumerates all available IP addresses

Port
Web Service can be set up on a default TCP/IP port (80), or any port you like

Important:

Make sure that selected Port is open on the Local firewall for the host to be accessible over the network. Contact you local Network Administrator if you are not sure how to configure Firewall settings.

Maximum Number of Simultaneous Connections
Workstation can serve requests from several web clients, however each connection consumes resources such as CPU, RAM & Network bandwidth. You can limit the number of web clients which can monitor current KillDisk workstation. Default value is 3

Read Only or Interactive Mode
Web Service can be used either for monitoring only or be interactive. In interactive mode user can start Disk Erase, Stop Erase and other commands for Disks and Batches

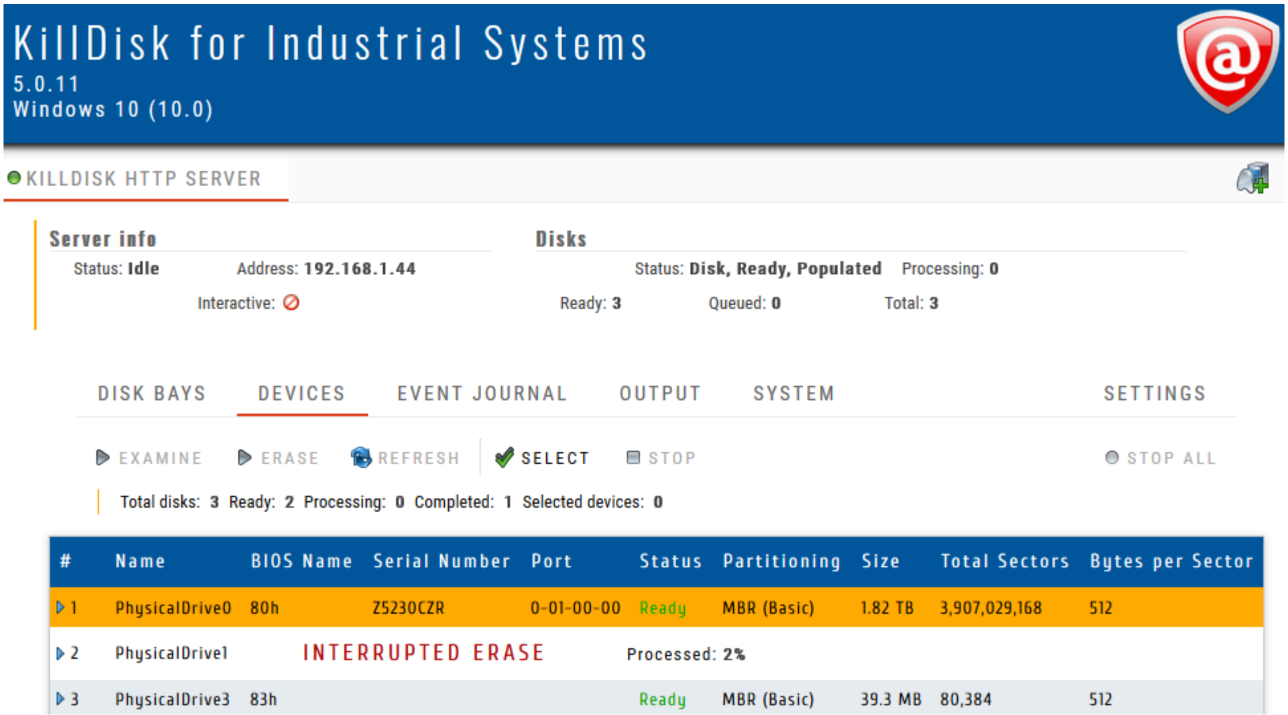
Warning:

Be careful when you clear Read Only check box! In this case any remote client can not only monitor, but start/stop processes on the workstation without physical access to the system and without up-to-date knowledge of disks attached and business needs, so it can interfere with local technicians' work.

Web Service Access

To monitor and control KillDisk workstation remotely, type workstation's IP address in the Address Bar of your favorite Web Browser (supported all modern browsers including Chrome, Firefox, Opera, Edge, Yandex, etc).

If **KillDisk** is up and running in the local network environment and its **Web Service** is configured and started properly, HTTP connection is established and Web Service main screen is displayed:



Server info

Status: **Idle** Address: **192.168.1.44**

Interactive: ⊘

Disks

Status: **Disk, Ready, Populated** Processing: **0**

Ready: **3** Queued: **0** Total: **3**

Total disks: **3** Ready: **2** Processing: **0** Completed: **1** Selected devices: **0**

#	Name	BIOS Name	Serial Number	Port	Status	Partitioning	Size	Total Sectors	Bytes per Sector
▷ 1	PhysicalDrive0	80h	Z5230CZR	0-01-00-00	Ready	MBR (Basic)	1.82 TB	3,907,029,168	512
▷ 2	PhysicalDrive1	INTERRUPTED ERASE			Processed: **2%**				
▷ 3	PhysicalDrive3	83h			Ready	MBR (Basic)	39.3 MB	80,384	512

Figure 87: Devices View

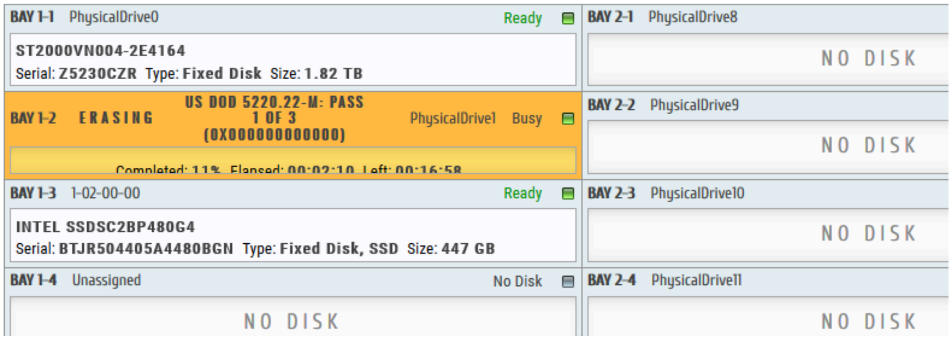
Workstation's name and status shown in the first line. Steady green icon at the left means there is no activities. Blinking green/yellow icon show that some operations are in progress (Erase/Examine/Wipe...).

Server info section below displays basic information about connected workstation (IP Address, Activity Status, Read Only/Interactive mode) and disks connected currently.

Several tabs (default is **DEVICES** tab) allow you to switch current view to obtain more information about server, disks and processes:

Disk Bays

Display Bays the same way as in application's Disk Bays View. Mouse click on the disk selects it. Erase progress can be reflected for the disks being erased



BAY 1-1 PhysicalDrive0 Ready
ST2000VN004-2E4164
Serial: **Z5230CZR** Type: **Fixed Disk** Size: **1.82 TB**

BAY 1-2 ERASING US DOD 5220.22-M: PASS 1 OF 3 (0X000000000000) PhysicalDrive1 Busy
Completed: 11% Elapsed: 00:02:10 Left: 00:16:58

BAY 1-3 1-02-00-00 Ready
INTEL SSDSC2BP480G4
Serial: **BTJR504405A4480BGN** Type: **Fixed Disk, SSD** Size: **447 GB**

BAY 1-4 Unassigned No Disk
NO DISK

BAY 2-1 PhysicalDrive8
NO DISK

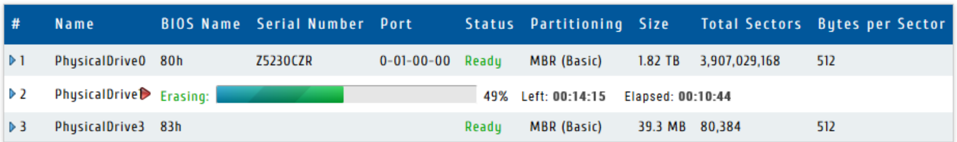
BAY 2-2 PhysicalDrive9
NO DISK

BAY 2-3 PhysicalDrive10
NO DISK

BAY 2-4 PhysicalDrive11
NO DISK

Devices

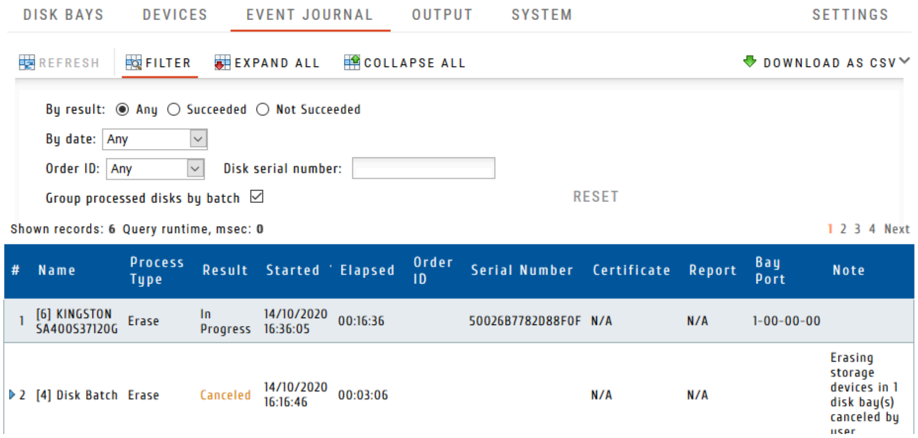
All disks displayed as a flat list. Mouse click on the disk selects it. Double click on the disk expands disk's attributes and S.M.A.R.T parameters. Erase progress can be reflected for the disks being erased



#	Name	BIOS Name	Serial Number	Port	Status	Partitioning	Size	Total Sectors	Bytes per Sector
▷ 1	PhysicalDrive0	80h	Z5230CZR	0-01-00-00	Ready	MBR (Basic)	1.82 TB	3,907,029,168	512
▷ 2	PhysicalDrive	Erasing:		49%	Left: 00:14:15	Elapsed: 00:10:44			
▷ 3	PhysicalDrive3	83h			Ready	MBR (Basic)	39.3 MB	80,384	512

Event Journal

Displays current **Event Journal** as a flat list. User can filter records by Status, Time Frame, Order ID, Disk Serial the same way as in KillDisk application. Grouping by Batches is supported. Resulting record set could be downloaded in CSV format



By result: ● Any ○ Succeeded ○ Not Succeeded

By date: Any

Order ID: Any   Disk serial number:

Group processed disks by batch ☑

Shown records: 6 Query runtime, msec: 0   1 2 3 4 Next

#	Name	Process Type	Result	Started	Elapsed	Order ID	Serial Number	Certificate	Report	Bay Port	Note
1	[6] KINGSTON SA400S37120G	Erase	In Progress	14/10/2020 16:36:05	00:16:36		50026B7782D88F0F	N/A	N/A	1-00-00-00	
▶ 2	[4] Disk Batch	Erase	Canceled	14/10/2020 16:16:46	00:03:06			N/A	N/A		Erasing storage devices in 1 disk bay(s) canceled by user

Output View

Displays Application Log (Output). Log can be downloaded in full as a text file

System View

Displays all information about workstation: Software version, Licensing info, Operating System information and Hardware information. All information can be downloaded in full as a text file

Settings View

Allows to configure General Options (refresh rate) and Event Journal (page size, download options). Settings can be saved for local display or restored to default values

Interacting with a Workstation remotely

Remote Web client is able not only monitor Server's state, but interact with a Workstation remotely, for example, start Disk Erase, start Batch Exam or Stop all current operations.

Note:

To be able to interact with a Workstation remotely , Read Only (Monitor) Mode should be turned off in Workstations' Web Access settings.

To interact with Workstation:

1. Select the disk or group of disks to be Erased/Examined by clicking them in **Bays View** or **Devices View** . Alternatively you can click **SELECT** toolbar button to select all accessible disks
2. Click **EXAMINE** or **ERASE** toolbar button to start the related process

   Warning:

   Be careful! There will be no action confirmation dialog, process will just start automatically. Client must be fully aware of the consequences.

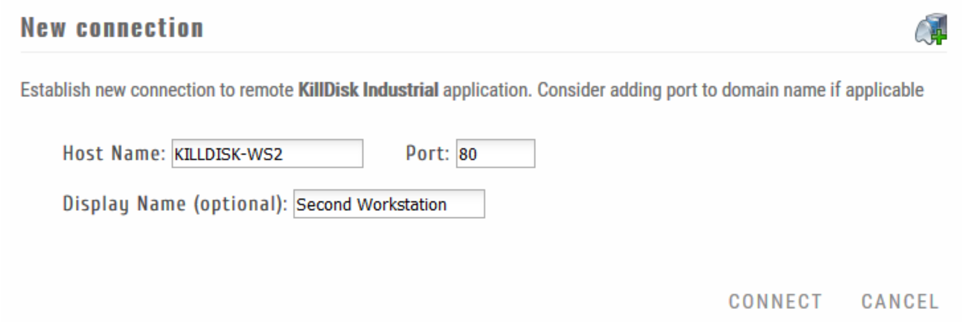
3. Observe the progress which will be displayed on the Disk/Bay. Client can stop any process anytime by selecting the particular disk and clicking **STOP** toolbar button, or stop all running processes by clicking **STOP ALL** toolbar button on the right

Monitoring/Interacting with Several Workstations

Remote Web Client is able not only monitor the single Workstation, but connect to and interact with several Workstations in one place (from the single web page).

To work with several Workstations:

1. Configure all Workstations you want to connect to. On each unit set up IP Address, Port, Firewall, Red Only/Interactive mode properly, start Web Service and check it is up and running
2. Connect to the first Workstation by typing **IP Address:Port** in the Address Bar of the Web Browser
3. Connect other Workstations by clicking icon with Green Plus sign at the right side. **New Connection** dialog appears:



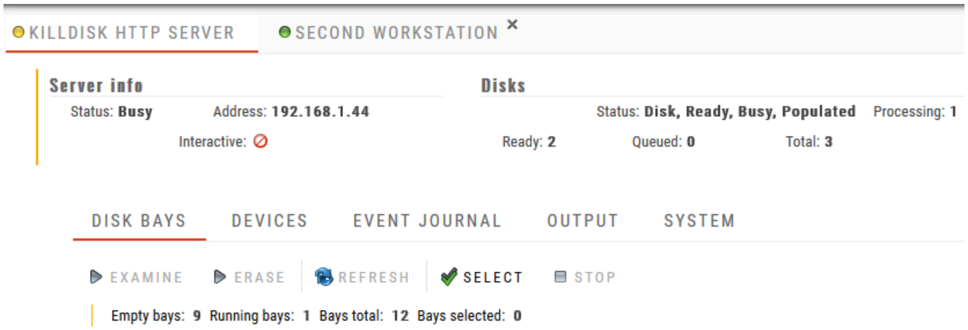
New connection

Establish new connection to remote **KillDisk Industrial** application. Consider adding port to domain name if applicable

Host Name: KILLDISK-WS2 Port: 80

Display Name (optional): Second Workstation

4. Type the Host Name on the Local Network (or related IP Address), Port and Display Name and click **CONNECT** button
5. After connection is established, the second tab appears. Click on another Workstations' Display Name will switch main view to display its information and current processes



Server info

Status: **Busy** Address: **192.168.1.44**

Interactive: ⊘

Disks

Status: **Disk, Ready, Busy, Populated** Processing: **1**

Ready: **2** Queued: **0** Total: **3**

Empty bays: **9** Running bays: **1** Bays total: **12** Bays selected: **0**

If security policy permits (in Interactive mode) you will be able not only monitor, but start Disk Erase/ Exam processes for remote hosts

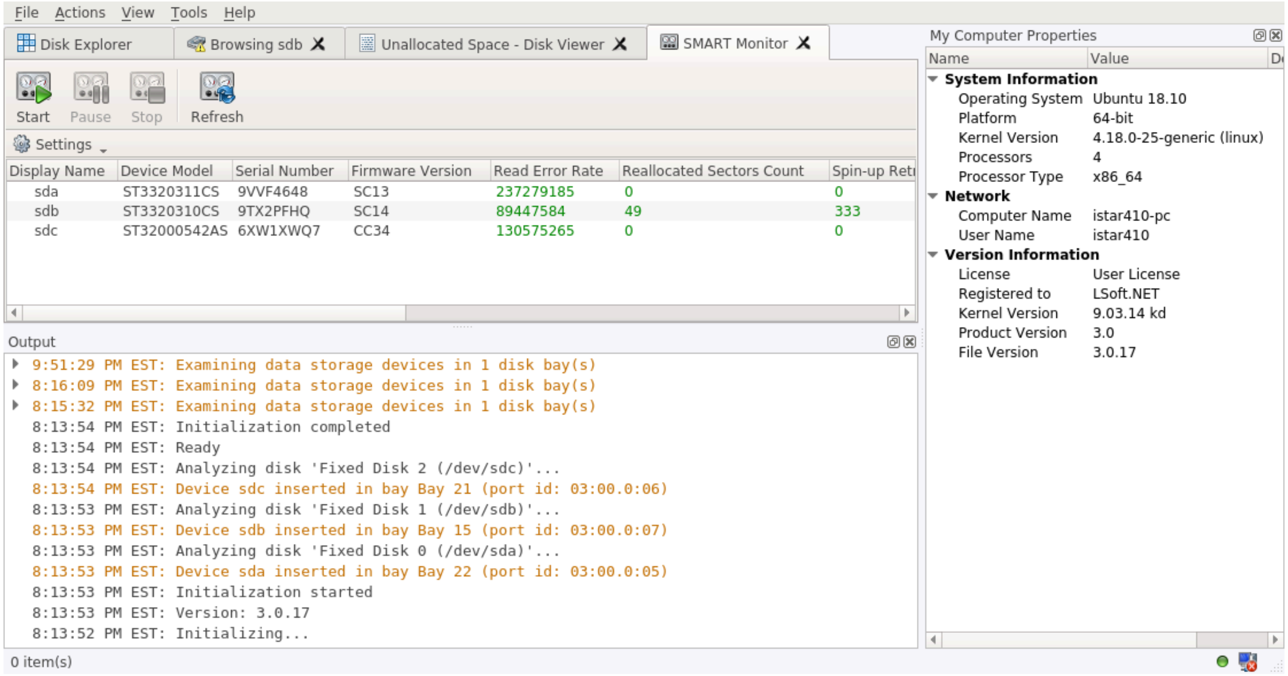
6. Repeat steps 3 and 4 to add more Workstations to monitor and interact with

Important:

Monitoring several workstations from the single location can be very useful to check overall current status (whether something being erased or Workstations are in idle state). In case if any process is running on the Workstation (the Host is busy) - the icon on the left of Workstations' Display Name is blinking (yellow and green). In case if Workstation is in idle mode, the icon is steady green.

S.M.A.R.T. Monitor

KillDisk supports displaying S.M.A.R.T. information. Just navigate to the menu bar and select **Tools** > **SMART Monitor**. It opens the S.M.A.R.T. monitor window shown below:



Display Name	Device Model	Serial Number	Firmware Version	Read Error Rate	Reallocated Sectors Count	Spin-up Retı
sda	ST3320311CS	9VVF4648	SC13	237279185	0	0
sdb	ST3320310CS	9TX2PFHQ	SC14	89447584	49	333
sdc	ST32000542AS	6XW1XWQ7	CC34	130575265	0	0

```
9:51:29 PM EST: Examining data storage devices in 1 disk bay(s)
8:16:09 PM EST: Examining data storage devices in 1 disk bay(s)
8:15:32 PM EST: Examining data storage devices in 1 disk bay(s)
8:13:54 PM EST: Initialization completed
8:13:54 PM EST: Ready
8:13:54 PM EST: Analyzing disk 'Fixed Disk 2 (/dev/sdc)'...
8:13:54 PM EST: Device sdc inserted in bay Bay 21 (port id: 03:00.0:06)
8:13:53 PM EST: Analyzing disk 'Fixed Disk 1 (/dev/sdb)'...
8:13:53 PM EST: Device sdb inserted in bay Bay 15 (port id: 03:00.0:07)
8:13:53 PM EST: Analyzing disk 'Fixed Disk 0 (/dev/sda)'...
8:13:53 PM EST: Device sda inserted in bay Bay 22 (port id: 03:00.0:05)
8:13:53 PM EST: Initialization started
8:13:53 PM EST: Version: 3.0.17
8:13:52 PM EST: Initializing...
```

Name	Value
System Information	
Operating System	Ubuntu 18.10
Platform	64-bit
Kernel Version	4.18.0-25-generic (linux)
Processors	4
Processor Type	x86_64
Network	
Computer Name	istar410-pc
User Name	istar410
Version Information	
License	User License
Registered to	LSoft.NET
Kernel Version	9.03.14 kd
Product Version	3.0
File Version	3.0.17

Figure 88: S.M.A.R.T. Monitor View

S.M.A.R.T. Information

The S.M.A.R.T. monitor displays a list of all discovered disks and shows the S.M.A.R.T. information next to them in table format. The following S.M.A.R.T. 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

These are the parameters to be configured in the **Settings** drop-down menu on a toolbar:

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 S.M.A.R.T. information displayed when the S.M.A.R.T. monitor is running.

Starting the S.M.A.R.T. Monitor

The S.M.A.R.T. monitor can either be refreshed manually or run to keep the information current. To run the S.M.A.R.T. 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 accordingly.

Note:

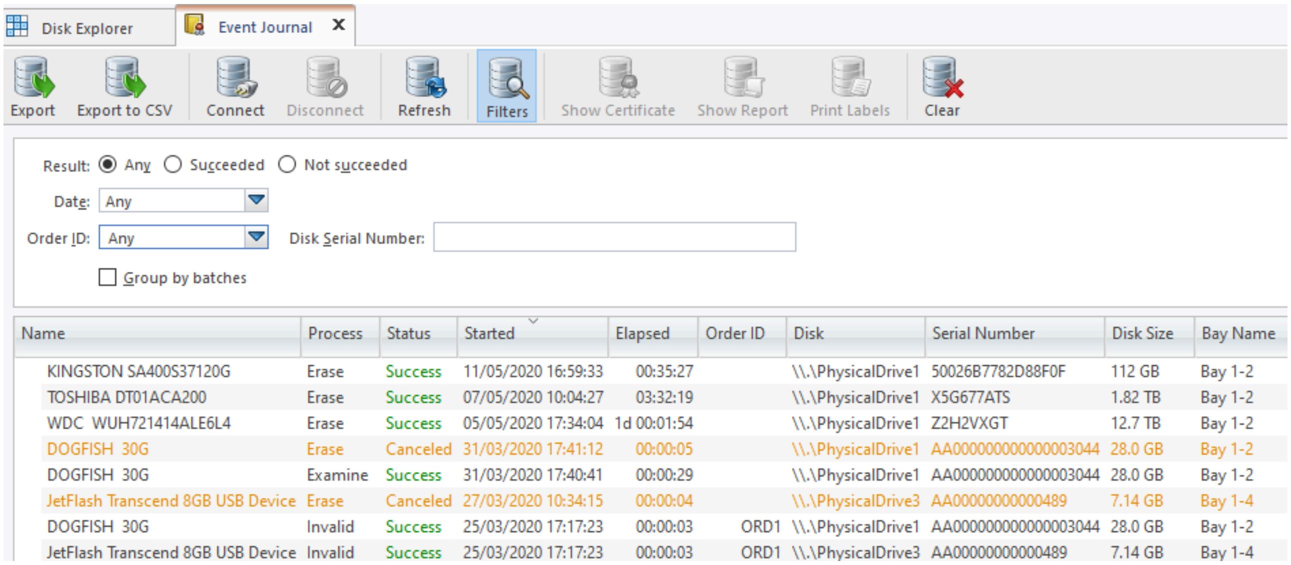
S.M.A.R.T. monitoring is a process that requires a lot of resources. It can slow down erase/wipe/ examine process significantly. We advise you to avoid querying S.M.A.R.T. information very often.

Event Journal

Event Journal is a feature that allows you to collect all your operations' history. Once any **KillDisk Industrial** operation completes the results of this operation are added to the Event Log stored in the local database and are available to use with any of the features explained below.

To access the Event Journal do one of the following:

1. In the file menu bar: navigate to **Tools** > **Event Journal** or
2. Press **CTRL + L**



Result: ● Any ○ Succeeded ○ Not succeeded

Date: Any

Order ID: Any

Disk Serial Number:

□ Group by batches

Name	Process	Status	Started	Elapsed	Order ID	Disk	Serial Number	Disk Size	Bay Name
KINGSTON SA400S37120G	Erase	Success	11/05/2020 16:59:33	00:35:27		\\.\PhysicalDrive1	50026B7782D88F0F	112 GB	Bay 1-2
TOSHIBA DT01ACA200	Erase	Success	07/05/2020 10:04:27	03:32:19		\\.\PhysicalDrive1	X5G677ATS	1.82 TB	Bay 1-2
WDC WUH721414ALE6L4	Erase	Success	05/05/2020 17:34:04	1d 00:01:54		\\.\PhysicalDrive1	Z2H2VXGT	12.7 TB	Bay 1-2
DOGFISH 30G	Erase	Canceled	31/03/2020 17:41:12	00:00:05		\\.\PhysicalDrive1	AA00000000000003044	28.0 GB	Bay 1-2
DOGFISH 30G	Examine	Success	31/03/2020 17:40:41	00:00:29		\\.\PhysicalDrive1	AA00000000000003044	28.0 GB	Bay 1-2
JetFlash Transcend 8GB USB Device	Erase	Canceled	27/03/2020 10:34:15	00:00:04		\\.\PhysicalDrive3	AA0000000000489	7.14 GB	Bay 1-4
DOGFISH 30G	Invalid	Success	25/03/2020 17:17:23	00:00:03	ORD1	\\.\PhysicalDrive1	AA00000000000003044	28.0 GB	Bay 1-2
JetFlash Transcend 8GB USB Device	Invalid	Success	25/03/2020 17:17:23	00:00:03	ORD1	\\.\PhysicalDrive3	AA0000000000489	7.14 GB	Bay 1-4

Figure 89: Event Journal View

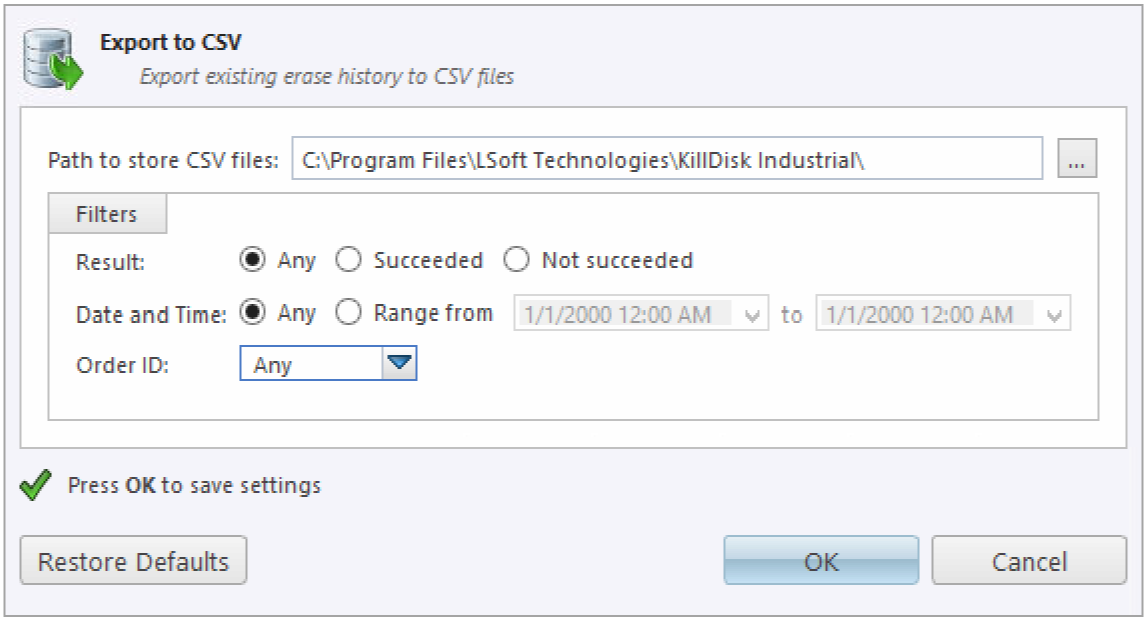
Action Toolbar Options

Export

Exports existing Event Journal or filtered journal records into external database

Export to CSV

Provides export to standard CSV-file (*comma-separated-values* file):



Export to CSV

Export existing erase history to CSV files

Path to store CSV files: C:\Program Files\LSoft Technologies\KillDisk Industrial\

Filters

Result: ● Any ○ Succeeded ○ Not succeeded

Date and Time: ● Any ○ Range from 1/1/2000 12:00 AM to 1/1/2000 12:00 AM

Order ID: Any

✓ Press **OK** to save settings

User should specify the *Path to Store* and the standard filters available.

Connect

Allows user to connect to an external database and export journal records using current database connection. User can specify all the necessary data in this dialog or in Preferences on page 99 section. After providing required credentials and establishing a database connection **KillDisk Industrial** is able to export certificates and reports as well as Event Journal to the external database.

Note:

The button is dimmed when the connection has been established.

Disconnect

Disconnects and stops exporting to the external SQL database. However, *Event Journal* still kept and accumulating in the local database.

Note:

The button is dimmed when there is no connection to external database.

Refresh

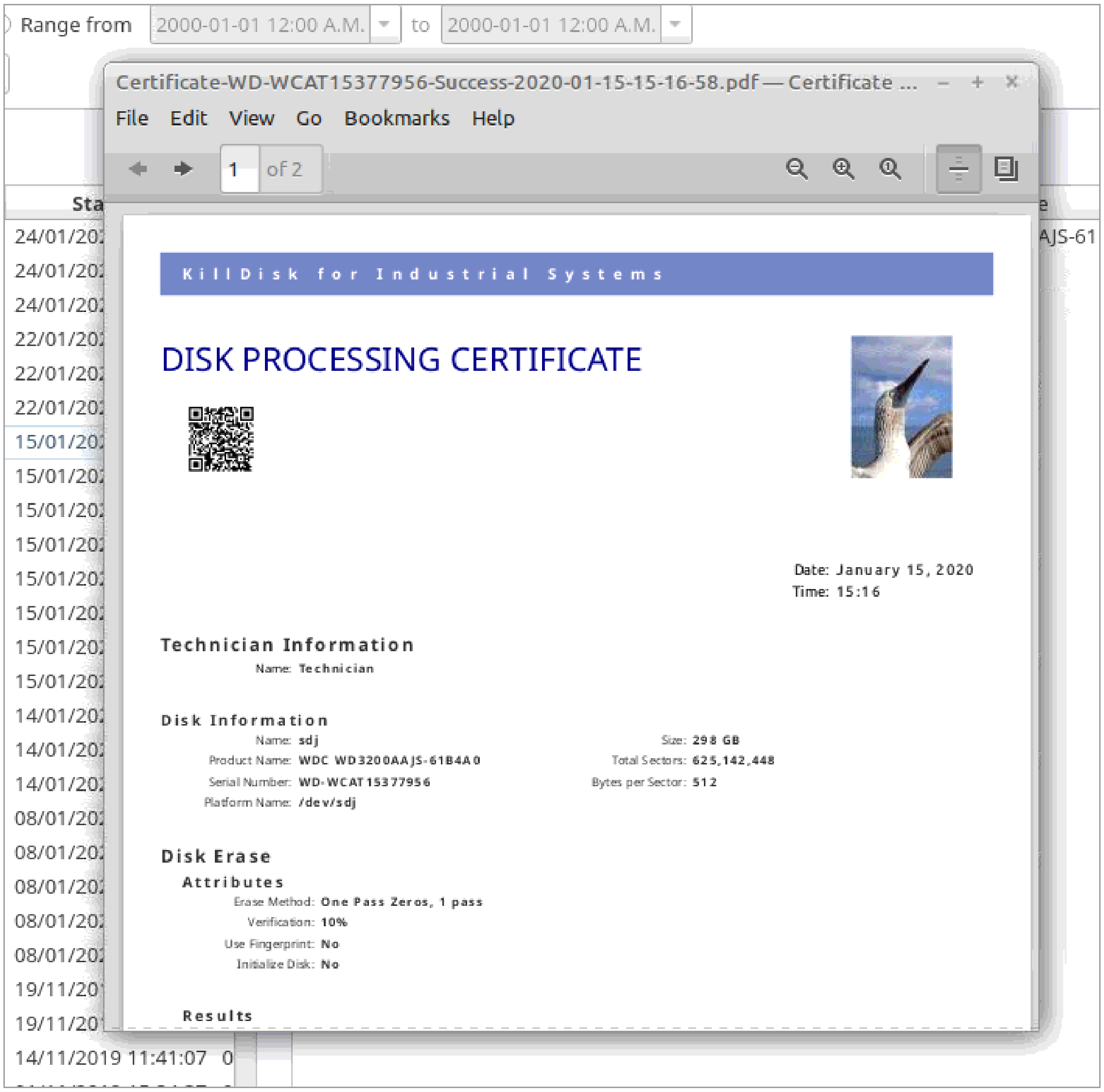
Refreshes the *Event Journal* to reflect any recently completed operations

Filters

Toggles displaying/hiding filtering options

Show Certificate

Shows the corresponding PDF-Certificate with system default PDF-viewer for the selected journal entry:



KillDisk for Industrial Systems

DISK PROCESSING CERTIFICATE

Date: January 15, 2020
Time: 15:16

Technician Information

Name: Technician

Disk Information

Name: sdj
Product Name: WDC WD3200AAJS-61B4A0
Serial Number: WD-WCAT15377956
Platform Name: /dev/sdj

Size: 298 GB
Total Sectors: 625,142,448
Bytes per Sector: 512

Disk Erase

Attributes

Erase Method: One Pass Zeros, 1 pass
Verification: 10%
Use Fingerprint: No
Initialize Disk: No

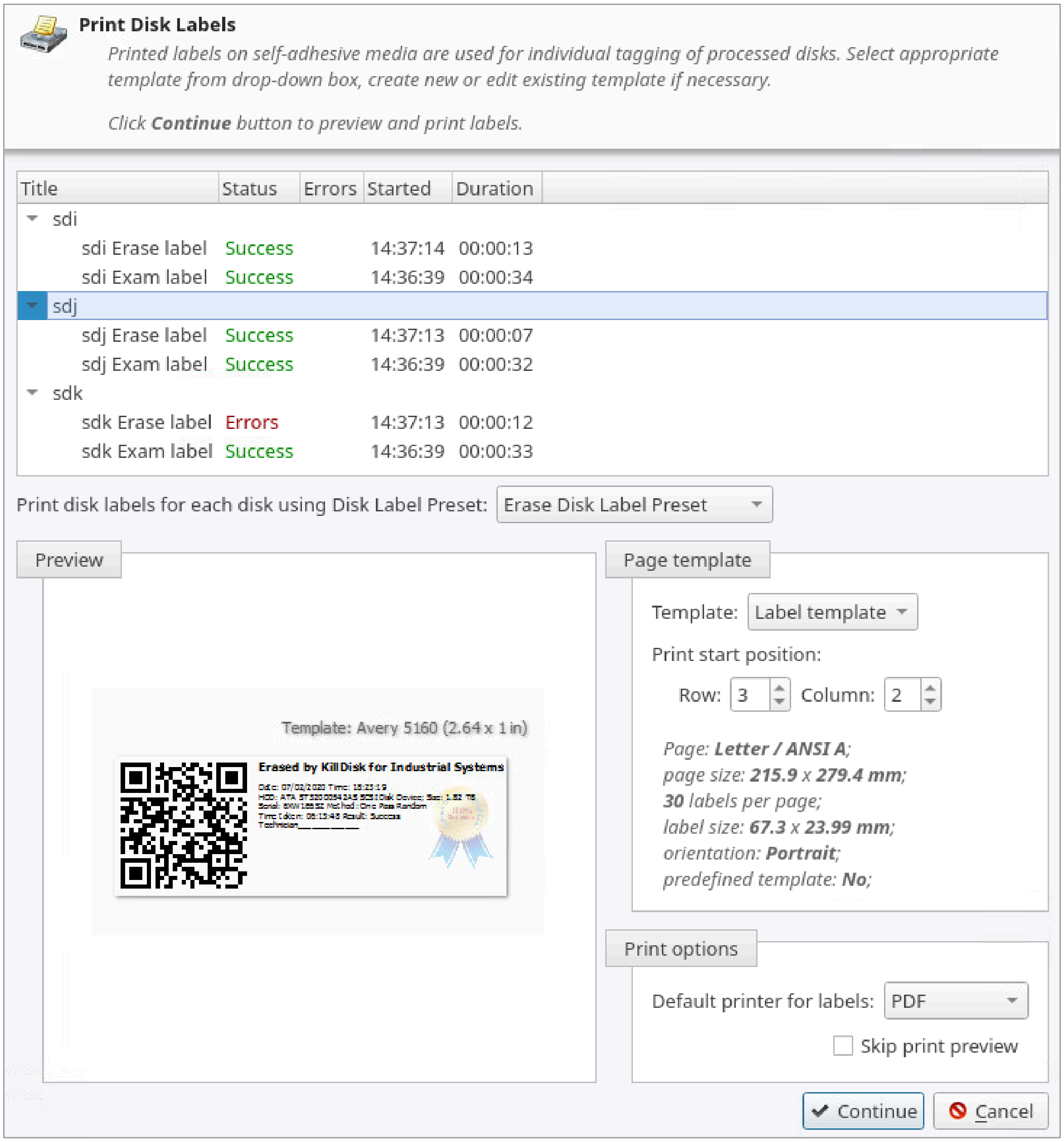
Results

Show Report

Shows the corresponding XML-report with system default XML-viewer for the selected journal entry

Print Labels

Shows a pop-up dialog for printing the corresponding label for the selected journal entry



Print Disk Labels

Printed labels on self-adhesive media are used for individual tagging of processed disks. Select appropriate template from drop-down box, create new or edit existing template if necessary.

*Click **Continue** button to preview and print labels.*

Title	Status	Errors	Started	Duration
sdi				
sdi Erase label	Success		14:37:14	00:00:13
sdi Exam label	Success		14:36:39	00:00:34
sdj				
sdj Erase label	Success		14:37:13	00:00:07
sdj Exam label	Success		14:36:39	00:00:32
sdk				
sdk Erase label	Errors		14:37:13	00:00:12
sdk Exam label	Success		14:36:39	00:00:33

Print disk labels for each disk using Disk Label Preset: Erase Disk Label Preset

Preview

Template: Avery 5160 (2.64 x 1 in)

Erased by KillDisk for Industrial Systems

Date: 07/02/2020 Time: 15:23:19
HDD: ATA ST3200084 2AS SCSI Disk Device; Size: 1.82 TB
Serial: 6XW1B5SE Method: One Pass Random
Time taken: 08:13:48 Result: Success
Technician___________

Page template

Template: Label template

Print start position:

Row: 3 Column: 2

*Page: **Letter / ANSI A**;*
*page size: **215.9** x **279.4 mm**;*
***30** labels per page;*
*label size: **67.3** x **23.99 mm**;*
*orientation: **Portrait**;*
*predefined template: **No**;*

Print options

Default printer for labels: PDF

□ Skip print preview

Clear

Clears the Event Journal

Filtering Options

Result

Display only Succeeded operations, Failed operations, or All events

Date and Time

Display Today's operations or operations from This Week, Month, Year, or within the Custom Range

Order ID

Display all records or only records for the particular Order ID (drop-down list contains all entered Order IDs)

Disk Serial Number

Filters by Disk Serial number. Displays the only record containing typed symbols

Group by Batches

Rather than showing history for each individual disk this option groups operations by Batches and displays Journal in Tree list

For the individual disk history: completed processes can be viewed, filtered with applied standard filters and sorted by attributes like *Name*, *Status*, *Order Id* etc. By **Right Mouse Click** on Results Table Headers user is able to create a custom set of data.

Note:

Export and **Connect** - both features share the same fields/interface for database connection. Generally speaking, user can maintain two modes for Event Journal export : *one-at-a-time* export and *real-time* export modes. **Export** is a *one-at-a-time* transaction. **Connect** establishes and maintains *real-time* connection, so there are two replicas of Event Journal at a time: local and remote.

Related information

Export Journal to External Database on page 97

Export Journal to External Database

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

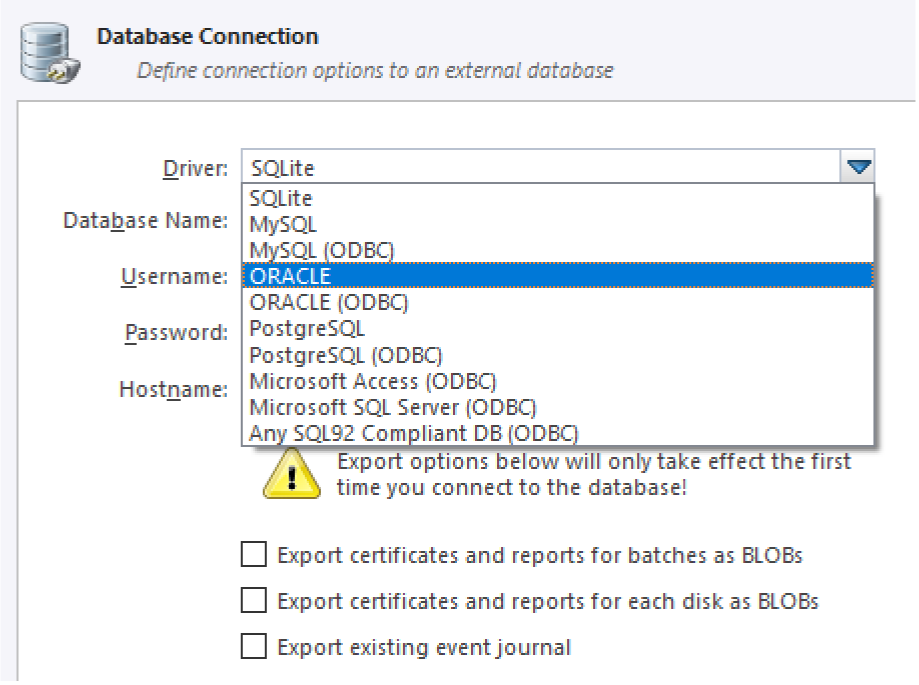
Supported connections to SQL databases:

- Any SQL92 Compliant Database (via ODBC)
- Microsoft Access
- Microsoft SQL Server
- PostgreSQL
- ORACLE
- MySQL
- SQLite

To connect to the external SQL database do one of the following:

1. Navigate to **Tools** > **Preferences** or press **F10**. Then click **Database Connection** tab on the left
2. Alternatively, on the file menu bar navigate to **Tools** > **Event Journal** or press **CTRL + L**. Then click **Connect** toolbar button

3. Database Connection dialog appears:



Database Connection

Define connection options to an external database

Driver: SQLite

- SQLite
- MySQL
- MySQL (ODBC)
- ORACLE
- ORACLE (ODBC)
- PostgreSQL
- PostgreSQL (ODBC)
- Microsoft Access (ODBC)
- Microsoft SQL Server (ODBC)
- Any SQL92 Compliant DB (ODBC)

Database Name:

Username:

Password:

Hostname:

Export options below will only take effect the first time you connect to the database!

□ Export certificates and reports for batches as BLOBs

□ Export certificates and reports for each disk as BLOBs

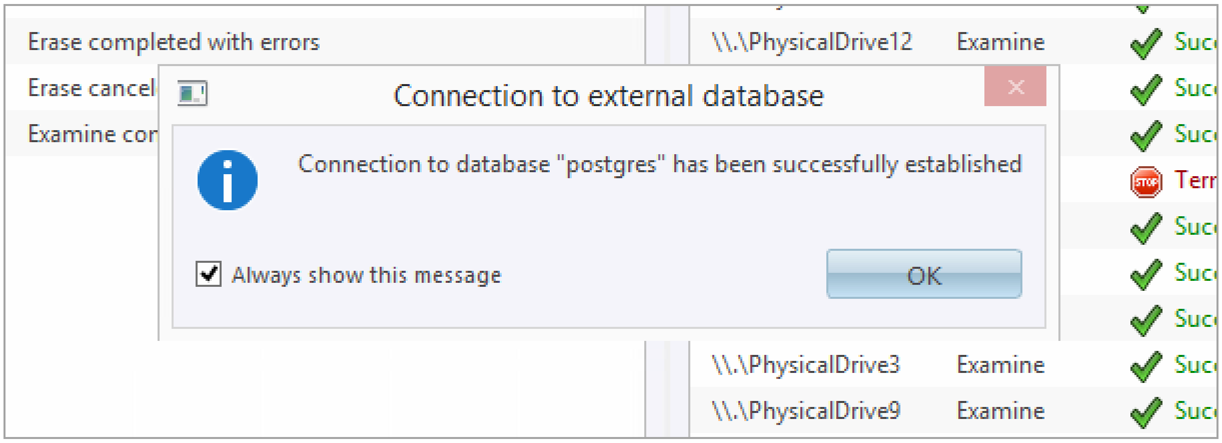
□ Export existing event journal

4. Select a *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
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 event journal (can be done 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 is established **KillDisk Industrial** starts exporting all information related to the current operations automatically.



Erase completed with errors	\\.\PhysicalDrive12	Examine	✓ Suc
Erase cancel			✓ Suc
Examine cor			✓ Suc
			Terr
			✓ Suc
			✓ Suc
			✓ Suc
	\\.\PhysicalDrive3	Examine	✓ Suc
	\\.\PhysicalDrive9	Examine	✓ Suc

Connection to external database

Connection to database "postgres" has been successfully established

☑ Always show this message

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.

Related information

Event Journal on page 93

Preferences

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

To open **Preferences** dialog:

- From main menu choose **Tools** > **Preferences...** or
- Use **F10** keyboard shortcut at any time

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

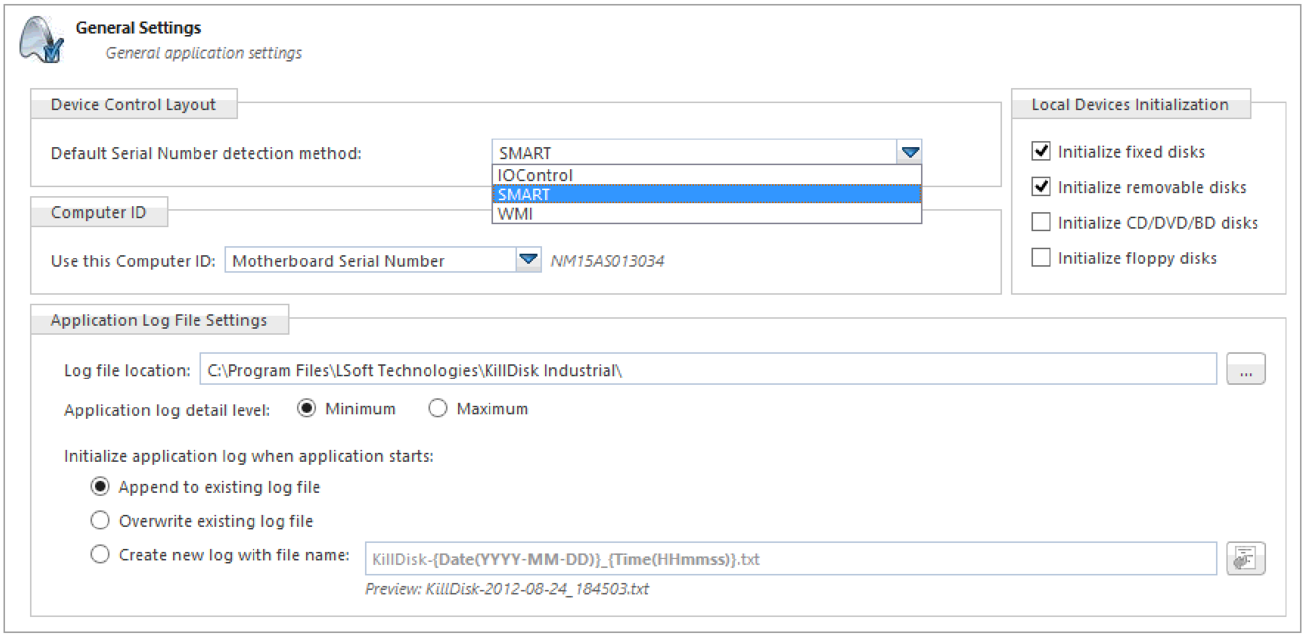
- General Settings on page 99
- Environment
- Sound Notifications
- Action Triggers
- Disk Erase
- Secure Erase
- Disk Wipe
- Disk Examine
- Examine Grades
- Clone Sources
- Erase Certificate
- Company Information
- Technical Information
- Processing Report
- Database Connection
- Disk Label Presets
- Disk Label Templates
- Disk Viewer
- Error Handling
- S.M.A.R.T. Diagnostics
- E-Mail Notifications
- SMTP Server Setting
- Web Service
- HTTP Notification

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

General Settings

The General Settings tab allows to configure general application settings as well as the visual representation.

These are configurable options pertaining to the applications functionality.



General Settings

General application settings

Device Control Layout

Default Serial Number detection method: SMART

IOControl
SMART
WMI

Computer ID

Use this Computer ID: Motherboard Serial Number NM15AS013034

Local Devices Initialization

☑ Initialize fixed disks

☑ Initialize removable disks

□ Initialize CD/DVD/BD disks

□ Initialize floppy disks

Application Log File Settings

Log file location: C:\Program Files\LSoft Technologies\KillDisk Industrial\ ...

Application log detail level: ● Minimum ○ Maximum

Initialize application log when application starts:

● Append to existing log file

○ Overwrite existing log file

○ Create new log with file name: KillDisk-{Date(YYYY-MM-DD)}_{Time(HHmmss)}.txt

Preview: KillDisk-2012-08-24_184503.txt

Device Control Layout

These settings control visual disk behavior in Disk Explorer on page 14 and allow to Show or Hide a System Disk and devices which are not ready (offline)

Default Serial Number detection method

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

Local Devices Initialization

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

Computer ID

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

Application Log File Settings

These settings apply to the log file generated by the application. All operations performed in a **KillDisk** session will be saved in this log.

Log file location

Allows the user to specify where the application log file is saved. By default this is set to a **KillDisk** installation directory

Application log detail level

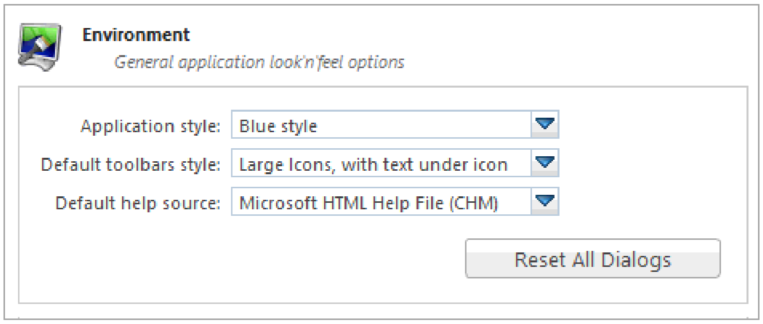
Manipulate the amount of details included in the logs. Options are: **Minimum** and **Maximum**

Initialize application log when application starts

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

Environment

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



Environment

General application look'n'feel options

Application style: Blue style

Default toolbars style: Large Icons, with text under icon

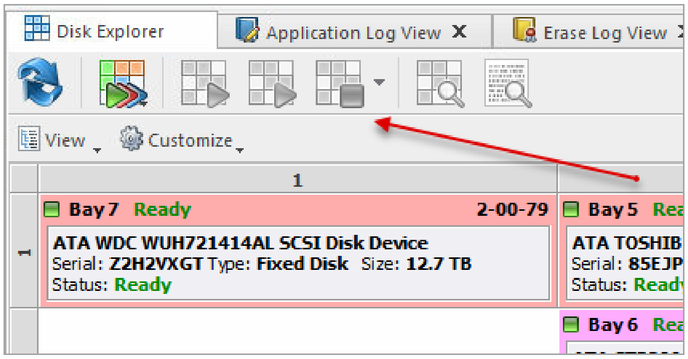
Default help source: Microsoft HTML Help File (CHM)

Application style

Configures the color scheme used in the application. Values are: **Blue** , **Olive** , **None (Use OS default)** and **Silver**

Default toolbars style

Configures how icons are shown in the toolbar. Values are: **Large icons, no text** , **Large icons, with text beside icon** , **Large icons, with text under icon** , **Small icons, with text beside icon** , **Small icons, no text**



Bay 7 Ready 2-00-79

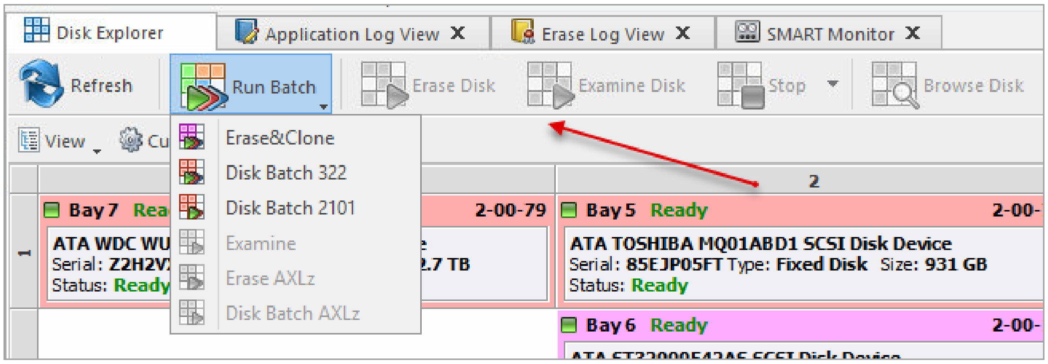
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed Disk Size: 12.7 TB
Status: Ready

Bay 5 Rea

ATA TOSHIB
Serial: 85EJP
Status: Ready

Bay 6 Rea

Figure 90: Large icons, no text



Bay 7 Rea 2-00-79

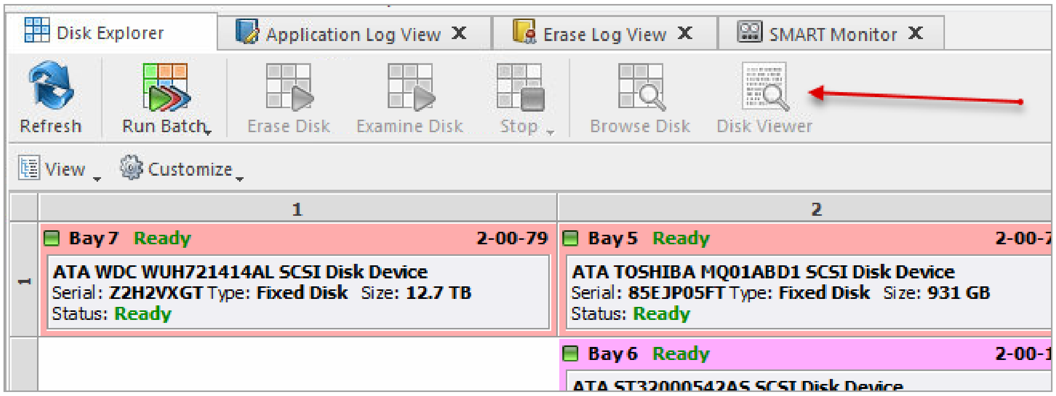
ATA WDC WU
Serial: Z2H2V
Status: Ready

Bay 5 Ready 2-00-

ATA TOSHIBA MQ01ABD1 SCSI Disk Device
Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB
Status: Ready

Bay 6 Ready 2-00-

Figure 91: Large icons, with text beside icon

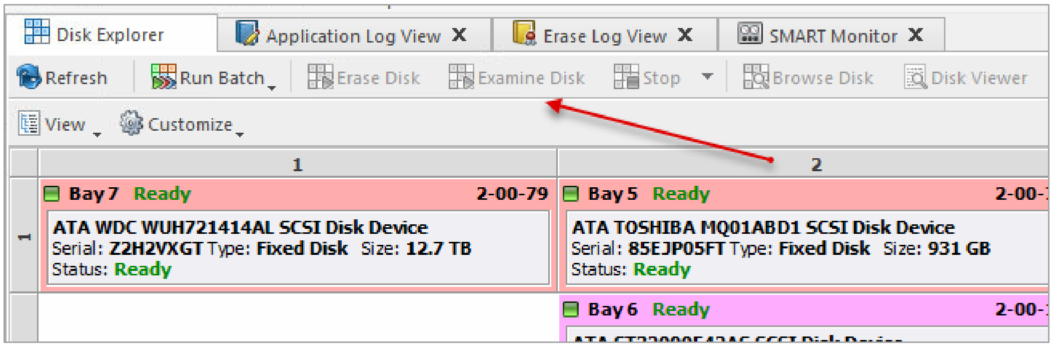


Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed Disk Size: 12.7 TB
Status: Ready

Bay 5 Ready 2-00-7
ATA TOSHIBA MQ01ABD1 SCSI Disk Device
Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB
Status: Ready

Bay 6 Ready 2-00-1
ATA ST32000542AS SCSI Disk Device

Figure 92: Large icons, with text under icon

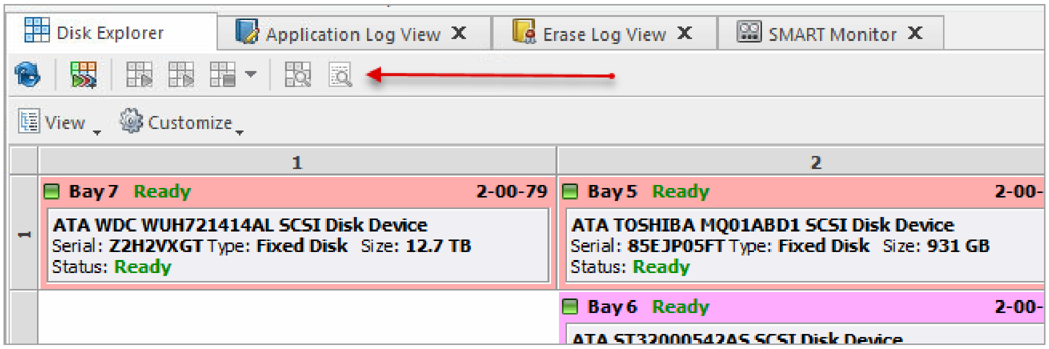


Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed Disk Size: 12.7 TB
Status: Ready

Bay 5 Ready 2-00-
ATA TOSHIBA MQ01ABD1 SCSI Disk Device
Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB
Status: Ready

Bay 6 Ready 2-00-

Figure 93: Small icons, with text beside icon



Bay 7 Ready 2-00-79
ATA WDC WUH721414AL SCSI Disk Device
Serial: Z2H2VXGT Type: Fixed Disk Size: 12.7 TB
Status: Ready

Bay 5 Ready 2-00-
ATA TOSHIBA MQ01ABD1 SCSI Disk Device
Serial: 85EJP05FT Type: Fixed Disk Size: 931 GB
Status: Ready

Bay 6 Ready 2-00-
ATA ST32000542AS SCSI Disk Device

Figure 94: Small icons, no text

Default help source

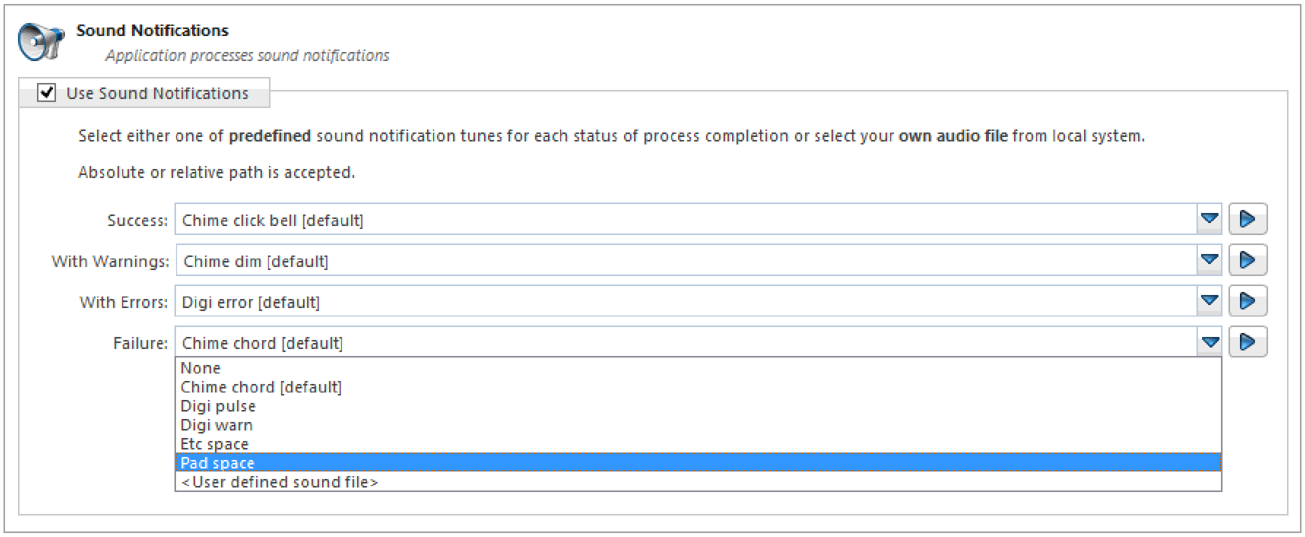
If available, user can select help documentation source to be addressed when requested. Values are: **PDF**, **CHM** and **On-line web help**

Reset All Dialogs

Pressing the button resets all the changes to default state

Sound Notifications

These are configurable options related to application sounds: you can use either predefined values or assign your own sounds (*User defined sound file*)



☑ Use Sound Notifications

Select either one of **predefined** sound notification tunes for each status of process completion or select your **own audio file** from local system.

Absolute or relative path is accepted.

Success: Chime click bell [default]

With Warnings: Chime dim [default]

With Errors: Digi error [default]

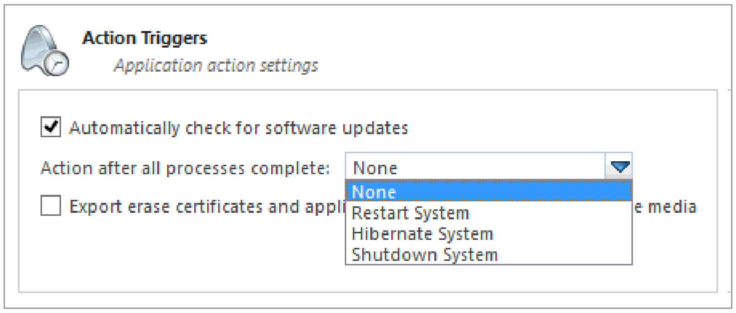
Failure: Chime chord [default]

Use Sound Notifications

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

Action Triggers

Configure actions performed while application is running



☑ Automatically check for software updates

Action after all processes complete: None

□ Export erase certificates and appli e media

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.

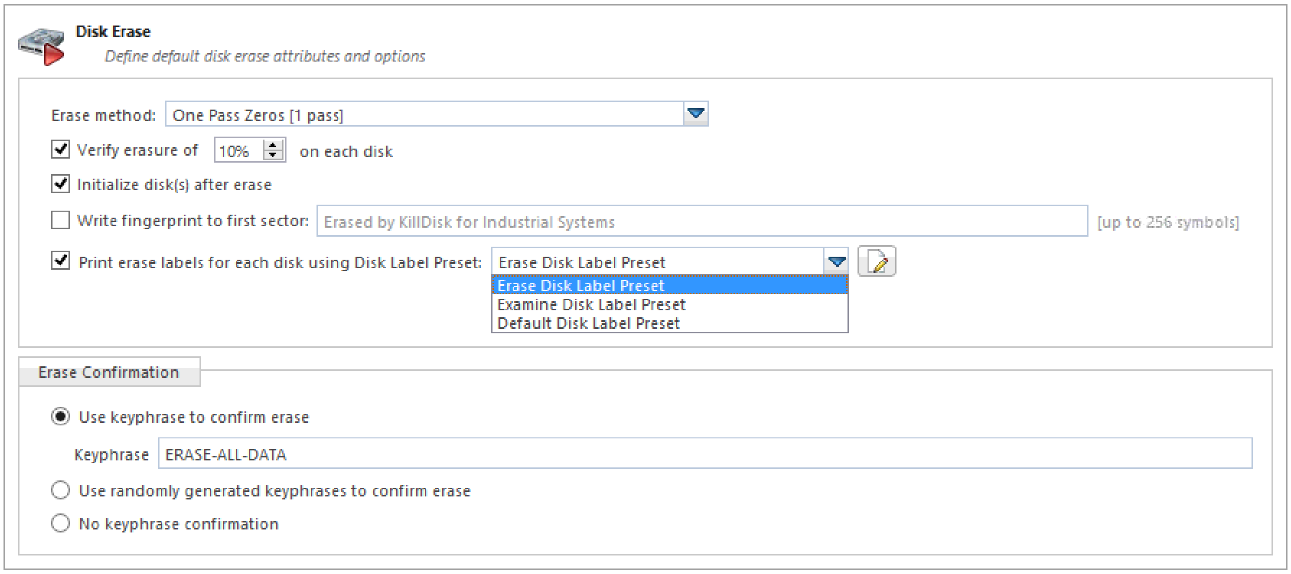
Export erase certificates and application log to all detected removable media

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

Disk Erase

The Disk Erase tab provides settings' configuration for the **KillDisk** erase procedures.

The same erase options for each batch could be set through Edit Batch Attributes on page 79 dialog



Disk Erase

Define default disk erase attributes and options

Erase method: One Pass Zeros [1 pass]

☑ Verify erasure of 10% on each disk

☑ Initialize disk(s) after erase

□ Write fingerprint to first sector: Erased by KillDisk for Industrial Systems [up to 256 symbols]

☑ Print erase labels for each disk using Disk Label Preset: Erase Disk Label Preset

Erase Disk Label Preset
Examine Disk Label Preset
Default Disk Label Preset

Erase Confirmation

● Use keyphrase to confirm erase

Keyphrase ERASE-ALL-DATA

○ Use randomly generated keyphrases to confirm erase

○ No keyphrase confirmation

Erase method

Choose one of more than 20 sanitizing methods including many international standards and custom patterns

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 feature will scan the entire drive evenly and verify the integrity of the erase operation. This option is the percent of the sectors to check across the disk. Most standards specify 10% as an accurate sample size for the verification.

Initialize disk(s) after erase

Writes proper MBR to disk's first sector after erasure complete. This is needed for disk to be visible and accessible by Operating System

Write fingerprint to first sector

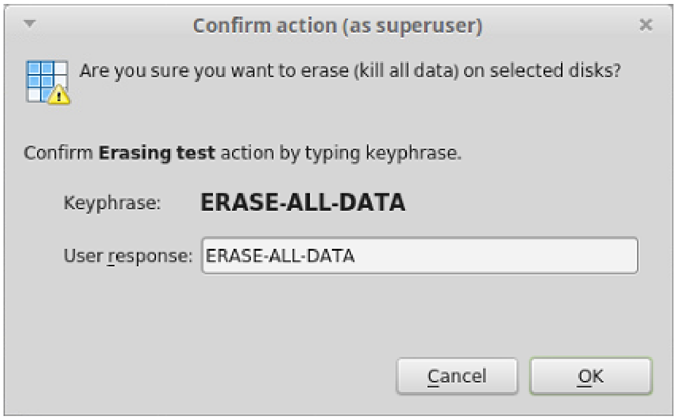
This feature writes the specified fingerprint to the first sector of the erased drive. If erased disk is plugged into the system and system boots from this disk the user will see this fingerprint as a message on the screen

Print Erase Labels

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

Erase confirmation

As a safety precaution to prevent accidental destruction of hard drives **KillDisk** uses the *user-typed keyphrase* mechanism just before the erase procedure is initiated (see below). By default this precaution mechanism is initialized with the key phrase **ERASE-ALL-DATA**. The key phrase can be modified, configured as a randomly generated set of characters or disabled. The keyphrase should be entered correctly in order to start the erase procedure



Confirm action (as superuser)

Are you sure you want to erase (kill all data) on selected disks?

Confirm **Erasing test** action by typing keyphrase.

Keyphrase: **ERASE-ALL-DATA**

User response: ERASE-ALL-DATA

Figure 95: Action confirmation dialog

Related information

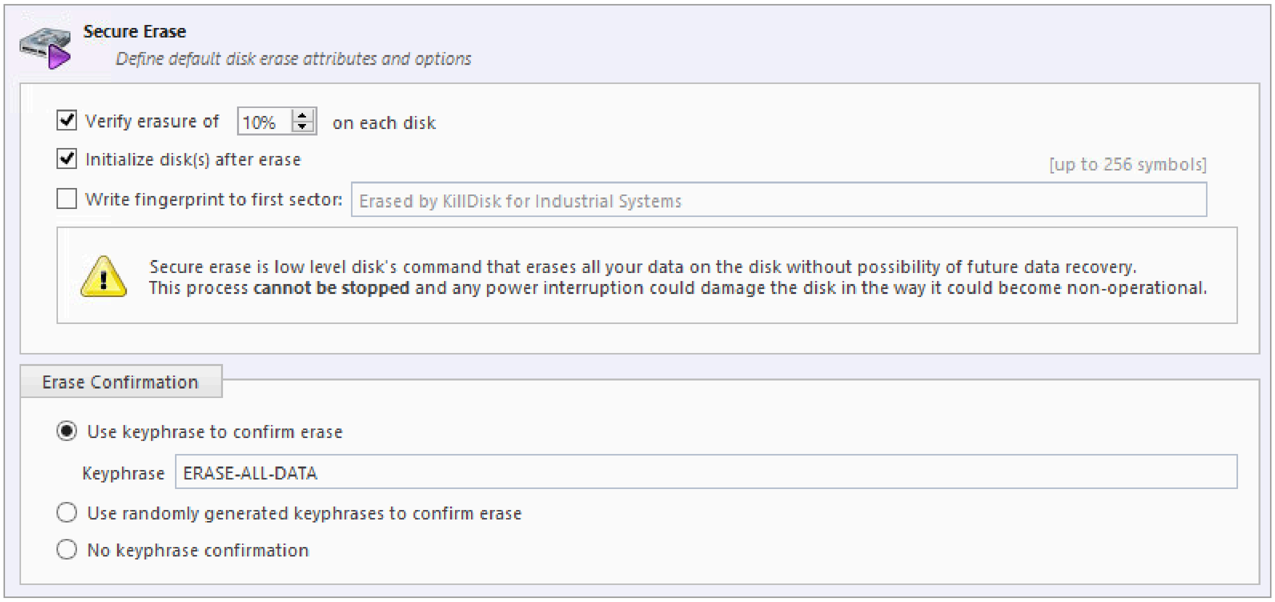
Erase Methods (Sanitation Standards) on page 151

Erase Disk Concepts on page 143

Disk Label Presets on page 119

Secure Erase

The Secure Erase tab provides settings' configuration for the Solid State Drive (SSD) specific erase procedures.



Secure Erase

Define default disk erase attributes and options

☑ Verify erasure of 10% on each disk

☑ Initialize disk(s) after erase

☐ Write fingerprint to first sector: Erased by KillDisk for Industrial Systems [up to 256 symbols]

Secure erase is low level disk's command that erases all your data on the disk without possibility of future data recovery.
This process **cannot be stopped** and any power interruption could damage the disk in the way it could become non-operational.

Erase Confirmation

● Use keyphrase to confirm erase

Keyphrase ERASE-ALL-DATA

○ Use randomly generated keyphrases to confirm erase

○ No keyphrase confirmation

Verify erasure

Percentage of disk to be verified after Secure Erase completes

Initialize disk(s) after erase

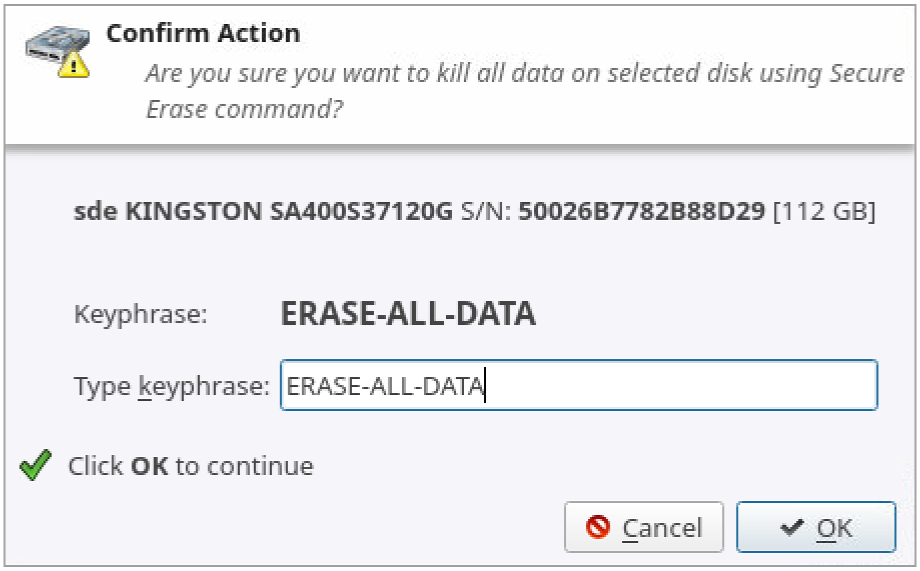
Writes proper MBR to disk's first sector after erasure complete. This is needed for disk to be visible and accessible by Operating System

Write fingerprint to first sector

This feature writes 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 Industrial** uses the *user-typed keyphrase* mechanism just before the erase procedure is initiated (see below). By default this precaution mechanism is initialized with the key phrase **ERASE-ALL-DATA**. The key phrase can be modified, configured as a randomly generated set of characters or disabled. The keyphrase should be entered correctly in order to start the erase procedure.



Confirm Action

Are you sure you want to kill all data on selected disk using Secure Erase command?

sde KINGSTON SA400S37120G S/N: **50026B7782B88D29** [112 GB]

Keyphrase: **ERASE-ALL-DATA**

Type keyphrase: ERASE-ALL-DATA

✓ Click **OK** to continue

Figure 96: Secure Erase confirmation dialog

Related tasks

Secure Erase on page 48

Related information

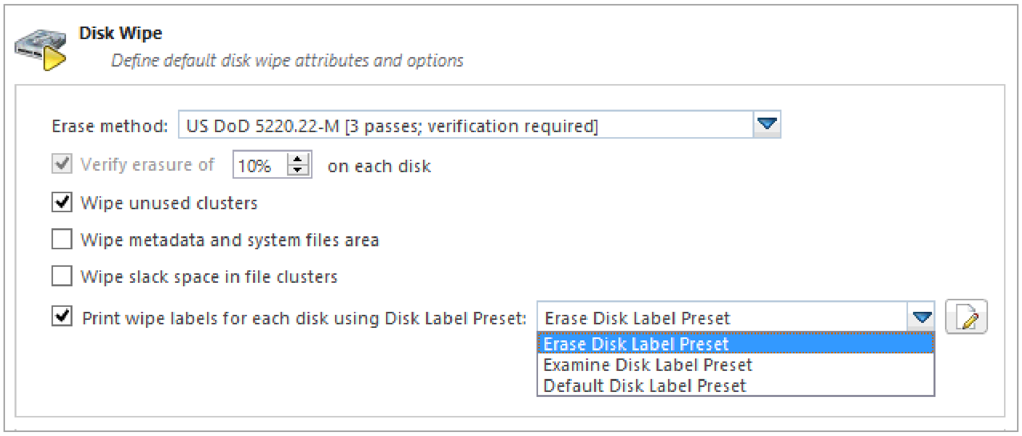
Secure Erase (SSD) on page 137

Secure Erase Concepts on page 144

Secure Erase (ANSI ATA, SE) on page 152

Disk Wipe

The Disk Wipe tab provides settings' configuration for Wipe procedure (like the erase procedure) allows you to specify the erase method to use as well as a few additional wipe-specific options.



Disk Wipe
Define default disk wipe attributes and options

Erase method: US DoD 5220.22-M [3 passes; verification required]

☑ Verify erasure of 10% on each disk

☑ Wipe unused clusters

☐ Wipe metadata and system files area

☐ Wipe slack space in file clusters

☑ Print wipe labels for each disk using Disk Label Preset: Erase Disk Label Preset

Erase method

Choose one of more than 20 sanitizing methods including many international standards and custom patterns

Verify erasure

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 OS (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 their remained records

Wipe slack space in file clusters

Erase slack space within files. 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 that space to remove these data traces

Print wipe labels

This feature prints wipe label automatically after wipe is completed using a specific *Disk Label Preset* configuration

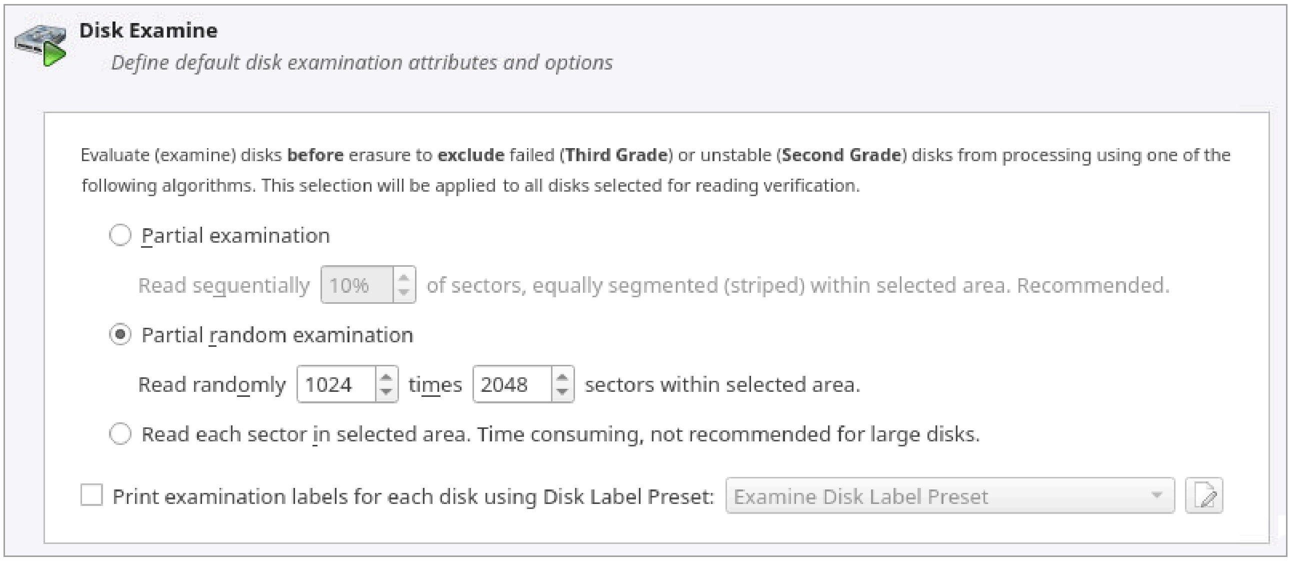
Related information

Erase Methods (Sanitation Standards) on page 151
Wipe Disk Concepts on page 146
Disk Label Presets on page 119

Disk Examine

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 on some 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.



Disk Examine

Define default disk examination attributes and options

Evaluate (examine) disks **before** erasure to **exclude** failed (**Third Grade**) or unstable (**Second Grade**) disks from processing using one of the following algorithms. This selection will be applied to all disks selected for reading verification.

○ Partial examination

Read sequentially 10% of sectors, equally segmented (striped) within selected area. Recommended.

● Partial random examination

Read randomly 1024 times 2048 sectors within selected area.

○ Read each sector in selected area. Time consuming, not recommended for large disks.

□ Print examination labels for each disk using Disk Label Preset: Examine Disk Label Preset

To examine disk integrity the following algorithms being used:

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

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

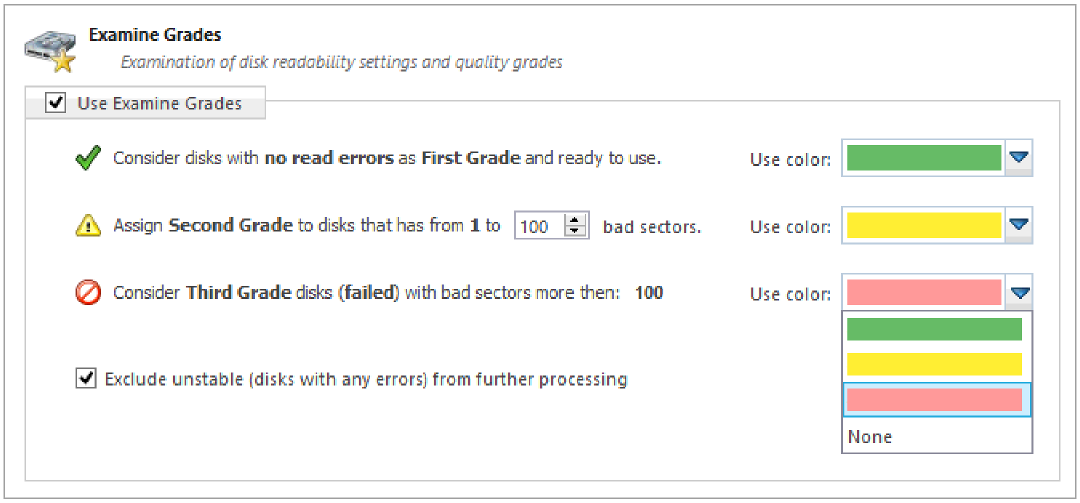
Read Each Sector in Selected Area
Examines entirely all the selected area. Because this reads each sector in the selected area it is the most lengthy, but thorough examination procedure

Print Examination Labels
This feature prints erase label automatically after examination completion using specific Disk Label Preset configuration

Examine Grades

Based on examination results disks could be "graded" depending on amount of failed sectors. Specific grade attributes can be set on **Examine 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* colors in order to represent the disk grade visually. Multiple grades may share the same color:



Examine Grades

Examination of disk readability settings and quality grades

☑ Use Examine Grades

✓ Consider disks with **no read errors** as **First Grade** and ready to use. Use color: 🟩

⚠ Assign **Second Grade** to disks that has from **1** to 100 bad sectors. Use color: 🟨

⊘ Consider **Third Grade** disks **(failed)** with bad sectors more then: **100** Use color: 🟥

☑ Exclude unstable (disks with any errors) from further processing

Limits for errors

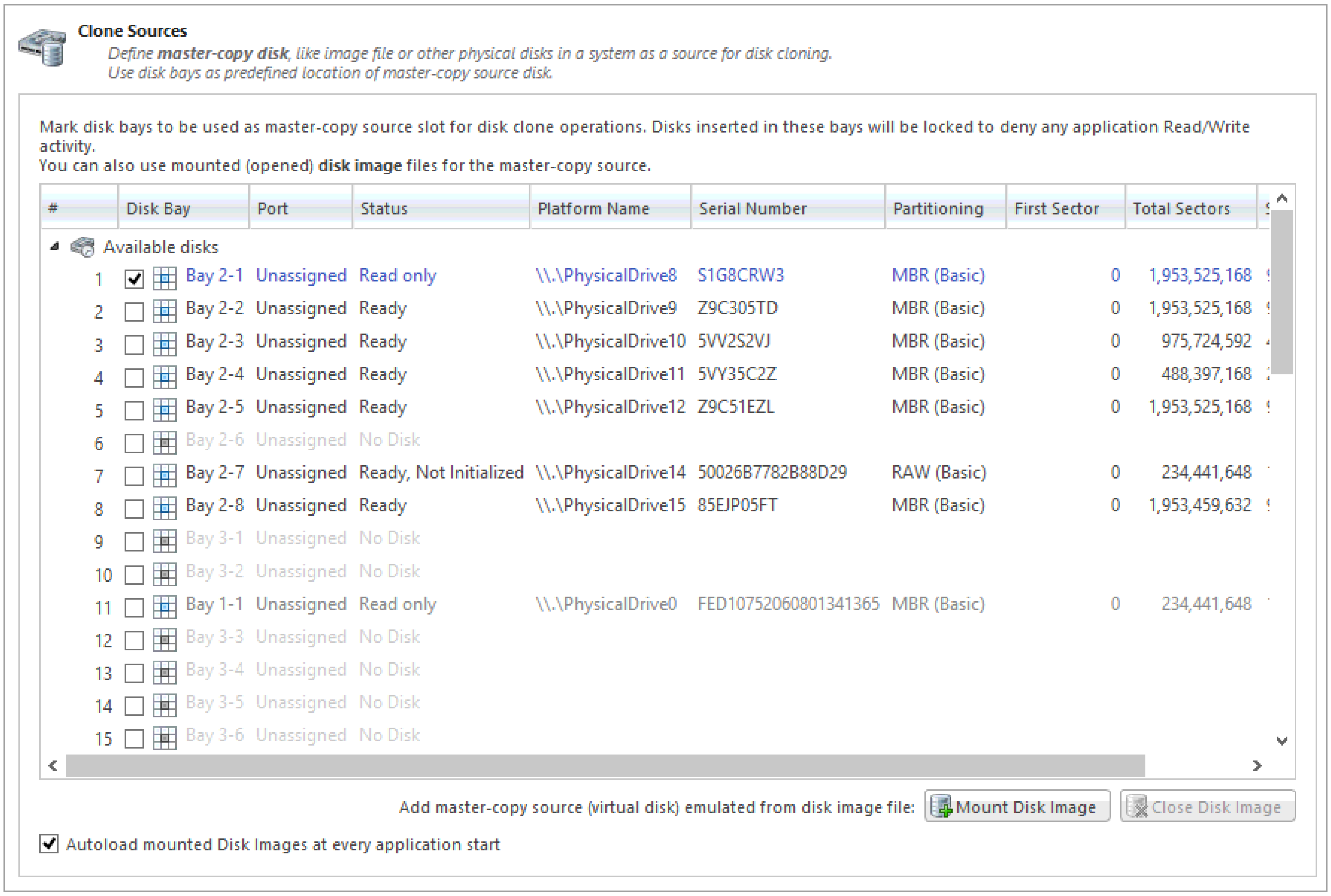
Defined under the second grade disks section, the maximum read errors settings allow the user to define the maximum read error tolerance before a disk is categorized as a 3rd grade disk. Such disks are the worst grade level and are considered as unreliable for use

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

Clone Sources

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



Clone Sources

*Define **master-copy disk**, like image file or other physical disks in a system as a source for disk cloning.*
Use disk bays as predefined location of master-copy source disk.

Mark disk bays to be used as master-copy source slot for disk clone operations. Disks inserted in these bays will be locked to deny any application Read/Write activity.
You can also use mounted (opened) **disk image** files for the master-copy source.

#	Disk Bay	Port	Status	Platform Name	Serial Number	Partitioning	First Sector	Total Sectors
Available disks								
1	☑ Bay 2-1	Unassigned	Read only	\\.\PhysicalDrive8	S1G8CRW3	MBR (Basic)	0	1,953,525,168
2	□ Bay 2-2	Unassigned	Ready	\\.\PhysicalDrive9	Z9C305TD	MBR (Basic)	0	1,953,525,168
3	□ Bay 2-3	Unassigned	Ready	\\.\PhysicalDrive10	5VV2S2VJ	MBR (Basic)	0	975,724,592
4	□ Bay 2-4	Unassigned	Ready	\\.\PhysicalDrive11	5VY35C2Z	MBR (Basic)	0	488,397,168
5	□ Bay 2-5	Unassigned	Ready	\\.\PhysicalDrive12	Z9C51EZL	MBR (Basic)	0	1,953,525,168
6	□ Bay 2-6	Unassigned	No Disk					
7	□ Bay 2-7	Unassigned	Ready, Not Initialized	\\.\PhysicalDrive14	50026B7782B88D29	RAW (Basic)	0	234,441,648
8	□ Bay 2-8	Unassigned	Ready	\\.\PhysicalDrive15	85EJP05FT	MBR (Basic)	0	1,953,459,632
9	□ Bay 3-1	Unassigned	No Disk					
10	□ Bay 3-2	Unassigned	No Disk					
11	□ Bay 1-1	Unassigned	Read only	\\.\PhysicalDrive0	FED10752060801341365	MBR (Basic)	0	234,441,648
12	□ Bay 3-3	Unassigned	No Disk					
13	□ Bay 3-4	Unassigned	No Disk					
14	□ Bay 3-5	Unassigned	No Disk					
15	□ Bay 3-6	Unassigned	No Disk					

Add master-copy source (virtual disk) emulated from disk image file:

☑ Autoload mounted Disk Images at every application start

Selecting a Disk for cloning

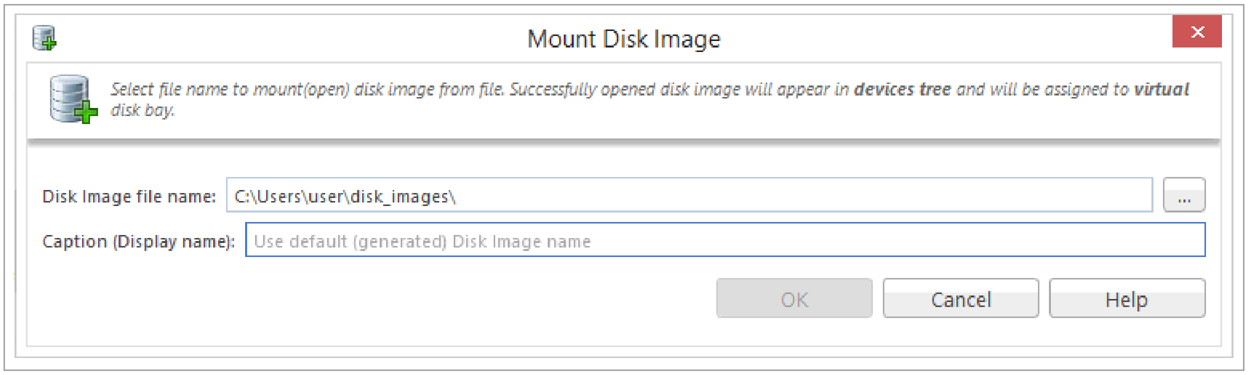
Any recognized disk may be used as a master-copy for Cloning. Simply find the disk under the **Disks Bays as clone sources** and check the box next to the desired Disk Bay. This disk will be locked and read/write operations will be restricted for it until the cloning operation is complete.

Selecting a Disk Image for cloning

Additionally to cloning a disk, cloning can be done from a mounted disk image.

To mount a disk image:

1. At the bottom of the dialog, click **Mount Disk Image**



*Select file name to mount(open) disk image from file. Successfully opened disk image will appear in **devices tree** and will be assigned to **virtual** disk bay.*

Disk Image file name: C:\Users\user\disk_images\

Caption (Display name): Use default (generated) Disk Image name

Figure 97: Mount Disk Image dialog

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

Note:

To avoid repeating steps 1-4 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.

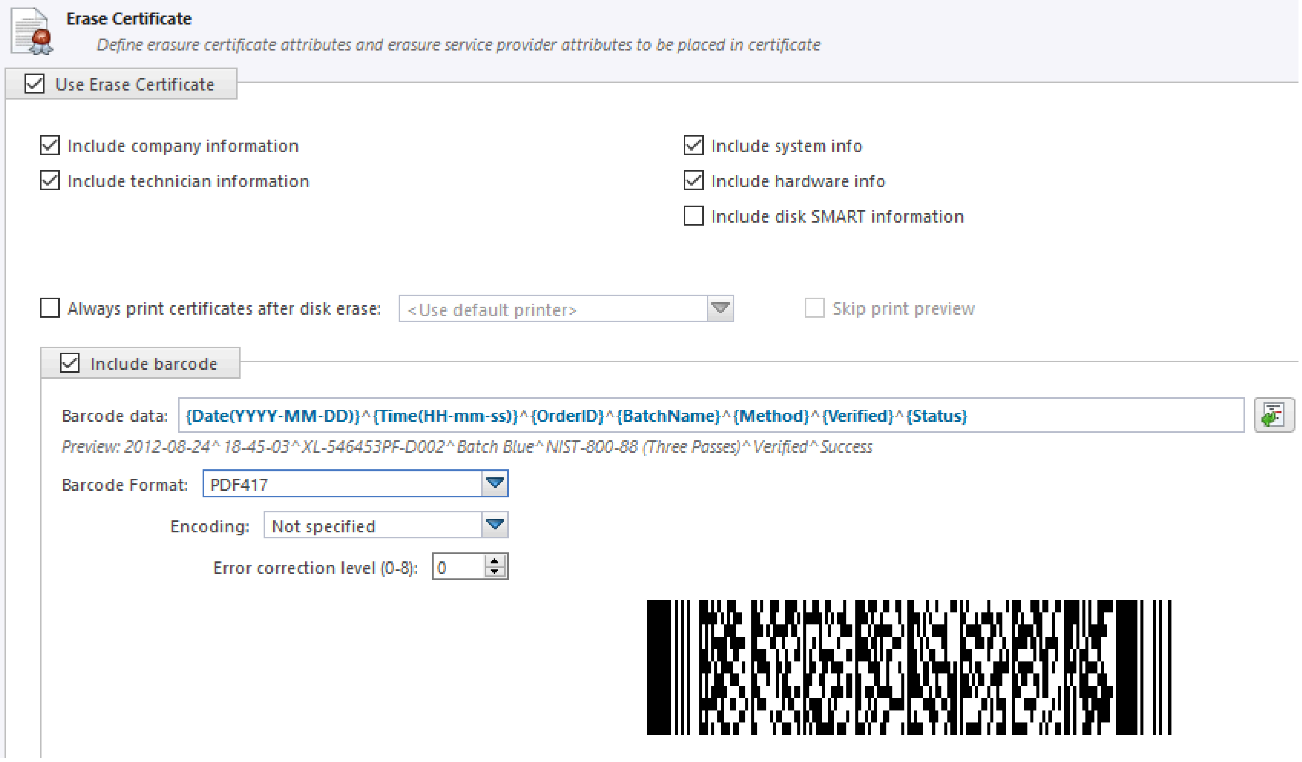
Related tasks

Mount Disk Image on page 45

Disk Clone on page 44

Erase Certificate

By selecting Use Erase Certificate check box the user is able to add and customize the erasure certificates with Company Information on page 114, Technician Information on page 114 and additional certificate options.



Erase Certificate

Define erasure certificate attributes and erasure service provider attributes to be placed in certificate

☑ Use Erase Certificate

☑ Include company information

☑ Include technician information

☑ Include system info

☑ Include hardware info

□ Include disk SMART information

□ Always print certificates after disk erase: <Use default printer>

□ Skip print preview

☑ Include barcode

Barcode data: {Date(YYYY-MM-DD)}^{Time(HH-mm-ss)}^{OrderID}^{BatchName}^{Method}^{Verified}^{Status}

Preview: 2012-08-24^ 18-45-03^XL-546453PF-D002^Batch Blue^NIST-800-88 (Three Passes)^Verified^Success

Barcode Format: PDF417

Encoding: Not specified

Error correction level (0-8): 0

Figure 98: Certificate Options

Include company information

Use this option to include all company's information

Include technician information

Use this option to include all technician's information

Include system info

Ensures that the OS-specific information is saved. Such as:

- Operating system
- Kernel version
- Architecture

Include hardware info

Ensures that the Chassis-specific information is saved. Such as:

- Motherboard manufacturer
- Motherboard description
- Number of processors

Include disk SMART information

Use this option to include S.M.A.R.T. information for the disk

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

Barcode

By selecting **Include Barcode** check box user is able to add a barcode in desired format.

Barcode data

Is a string of available tags and attributes concatenated by **^** (*CARET*) delimiter. User is able to compose a custom string with selected values from drop-down list or by simple typing

Preview

Shows the composed data representation. This data is encoded to the actual barcode

Barcode Format

There is a drop-down list of available barcode formats

Encoding (if available for the Barcode Format selected)

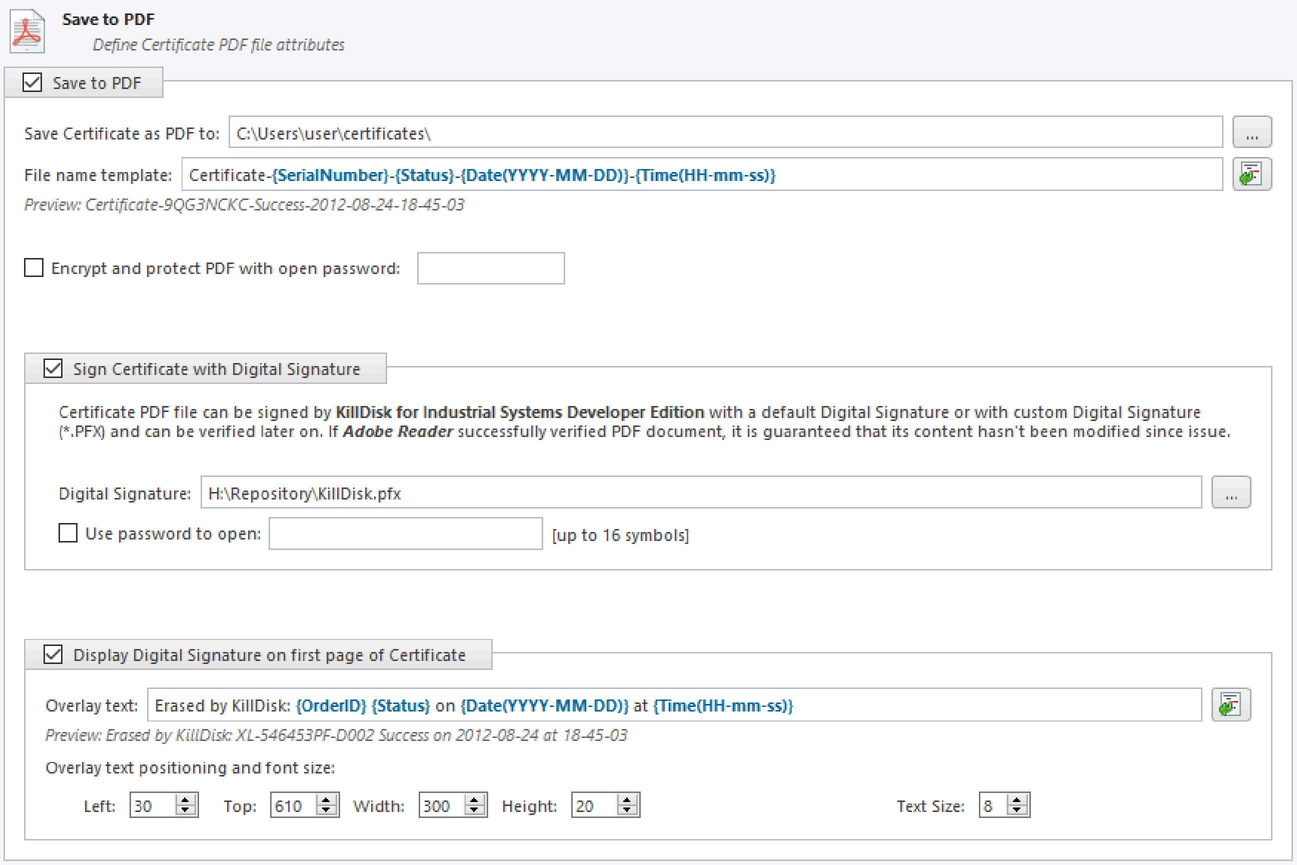
There is a drop-down list with available encoding schemes. The selected one is used to encode the barcode data

Error correction level (0-8) (if available for the Barcode Format selected)

Affects a size of the barcode. Increasing the level value provides a better scanner readability

Save to PDF Options

Sub tab **Save to PDF** offers options for storing a certificate to file in PDF format as well as encrypting with passwords and digitally signing output PDFs.



Save to PDF

Define Certificate PDF file attributes

☑ Save to PDF

Save Certificate as PDF to: C:\Users\user\certificates\ [...]

File name template: Certificate-{SerialNumber}-{Status}-{Date(YYYY-MM-DD)}-{Time(HH-mm-ss)}

Preview: Certificate-9QG3NCKC-Success-2012-08-24-18-45-03

□ Encrypt and protect PDF with open password:

☑ Sign Certificate with Digital Signature

Certificate PDF file can be signed by **KillDisk for Industrial Systems Developer Edition** with a default Digital Signature or with custom Digital Signature (*.PFX) and can be verified later on. If ***Adobe Reader*** successfully verified PDF document, it is guaranteed that its content hasn't been modified since issue.

Digital Signature: H:\Repository\KillDisk.pfx [...]

□ Use password to open: [up to 16 symbols]

☑ Display Digital Signature on first page of Certificate

Overlay text: Erased by KillDisk: {OrderID} {Status} on {Date(YYYY-MM-DD)} at {Time(HH-mm-ss)}

Preview: Erased by KillDisk: XL-546453PF-D002 Success on 2012-08-24 at 18-45-03

Overlay text positioning and font size:

Left: 30 Top: 610 Width: 300 Height: 20 Text Size: 8

Figure 99: Save to PDF Options

Certificate location

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

File name template

Here user specifies the template for the Erase Certificate. See the tags available in Appendix tags section

Encrypt with password

If password field is not empty, output certificate (PDF) will be encrypted and protected with specified password. This password needs to be typed in any PDF Viewer next time user opens a certificate for printing

Sign Certificate with Digital Signature

Certificate file (PDF) can be signed with a default Digital Signature (supplied **KillDisk.pfx** certificate) or with your custom Digital Signature (*.PFX) and can be verified later on. If **Adobe Reader** successfully verified PDF document, it is guaranteed that its content hasn't been modified since issue.

If custom Digital Signature is required, please issue a certificate and specify full path to the custom certificate (*.PFX file) as well as its open password in the related fields below (**Digital Signature** and **Use password to open**)

Display Digital Signature

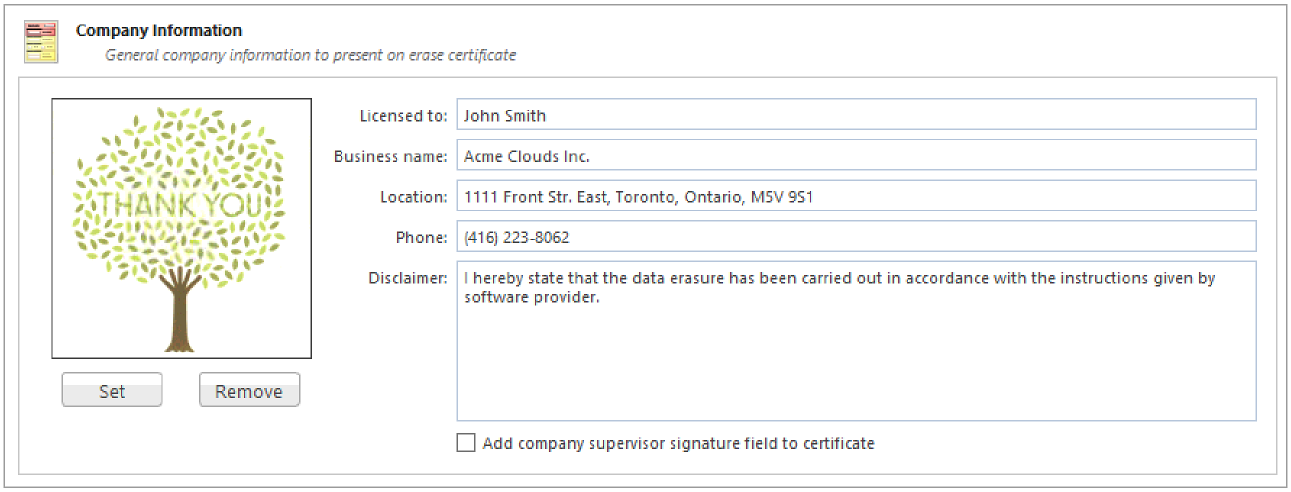
Digital Signature can be displayed as an overlay text on the first page of certificate. After you turn on this option, you can specify overlay text using tags (see tags section), its position on the first page, rectangle dimensions and text size

Related information

Name Tags on page 153

Company Information

These settings allow user to configure Company Information for Erase Certificates, Processing Reports and Disk Labels.



Company Information

General company information to present on erase certificate

Licensed to:	John Smith
Business name:	Acme Clouds Inc.
Location:	1111 Front Str. East, Toronto, Ontario, M5V 9S1
Phone:	(416) 223-8062
Disclaimer:	I hereby state that the data erasure has been carried out in accordance with the instructions given by software provider.

□ Add company supervisor signature field to certificate

To specify a Company Logo image just use the **Set** and **Remove** buttons. It allows you to select a desired image with local *File Explorer*. Most of the image formats are supported: JPEG, TIFF, BMP, PNG etc. The logo will be previewed in the Company Logo space.

Tip:

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

Add all the company information to the related fields.

When the **Add company supervisor signature field to certificate** check box is selected the required field is added to the actual certificate.

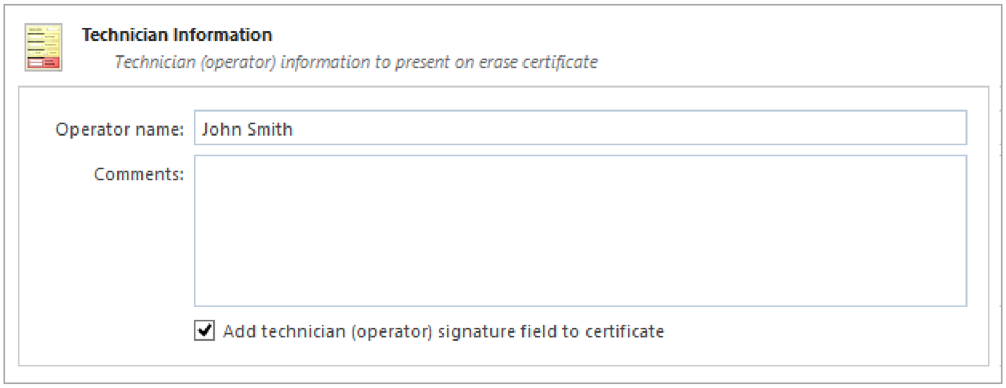
Related information

Erase Certificate on page 111

Processing Report on page 115

Technician Information

These settings allow user to configure Technician Information for Erase Certificates, Processing Reports and Disk Labels.



Technician Information

Technician (operator) information to present on erase certificate

Operator name: John Smith

Comments:

☑ Add technician (operator) signature field to certificate

Add Operator name and Comments to the related fields.

When the **Add technician (operator) signature field to certificate** check box is selected the required field is added to the actual certificate.

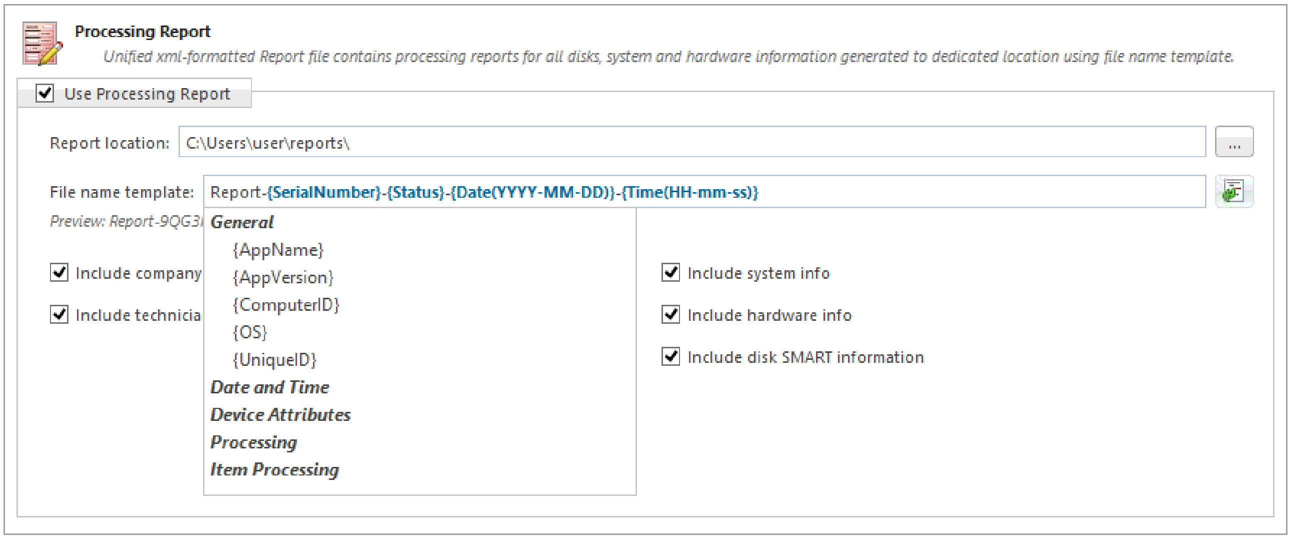
Related information

Erase Certificate on page 111

Processing Report on page 115

Processing Report

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



Processing Report

Unified xml-formatted Report file contains processing reports for all disks, system and hardware information generated to dedicated location using file name template.

☑ Use Processing Report

Report location: C:\Users\user\reports\

File name template: Report-{SerialNumber}-{Status}-{Date(YYYY-MM-DD)}-{Time(HH-mm-ss)}

Preview: Report-9QG3

☑ Include company

☑ Include technicia

☑ Include system info

☑ Include hardware info

☑ Include disk SMART information

Report Location

User may configure where XML erasure reports are saved

File name template

Here you may specify the template for the XML reports. The main tags available are:

Available element:	Tag:
Serial ID	{Serial ID}
Erasure Status	{Status}

Available element:	Tag:
Date of Erasure	{Date(YYYY-MM-DD)}
Time of Erasure	{Time(HH-mm-ss)}

There are additional tags available (see the tags section in Appendix)

Include company information

Optionally adds the company information (defined in Company Information) into the XML erasure report

Include technician information

Optionally adds the technician information (defined in Technician Information) into the XML erasure report

Include system info

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

- Operating system
- Kernel version
- Architecture (x86, x64)

Include hardware info

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

- Motherboard manufacturer
- Motherboard description
- Host (name, domain)
- CPU (logical, physical)
- Memory

Include SMART information for each disk

Optionally adds an additional information about disk health based on S.M.A.R.T. attributes into the XML erasure report.

The **KillDisk** XML report contains the following parts:

Table 1: XML Report Parameters (sample)

Type of Information	Specific data
Technician Information	*Name*
	Note
Company Information	*Name*

Type of Information	Specific data
	Licensed
	Location
	Phone
	Disclaimer
System Information	*OS version*
	Platform
	Kernel
Hardware Information	*Motherboard Manufacturer*
	Motherboard Description
	Number of Processors
Erase Attributes	*Erase Verify*
	Passes
	Method
	Verification Passes
Error Handling Attributes	*Errors Terminate*
	Skip interval
	Number of Retries
	Lock
	Source?
	Ignore Write?
	Read?
	Lock?
Disks	*Device Size*
	Device Type
	Serial Number
	Revision
	Product Number
	Name
	Geometric Information
	Partitioning Scheme
Additional Report Attributes	*Fingerprint Information*
	Initialize disk?
Results	*Bay*
	Time and Date Started

Type of Information	Specific data
	Disk Information
	Status
	Result
	Time Elapsed
	Errors
	Name of operation
Conclusion	*Overall result of the operation*

Note:

If internal tag <task> is present, Results are appeared inside.

Related information

Name Tags on page 153

Database Connection

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

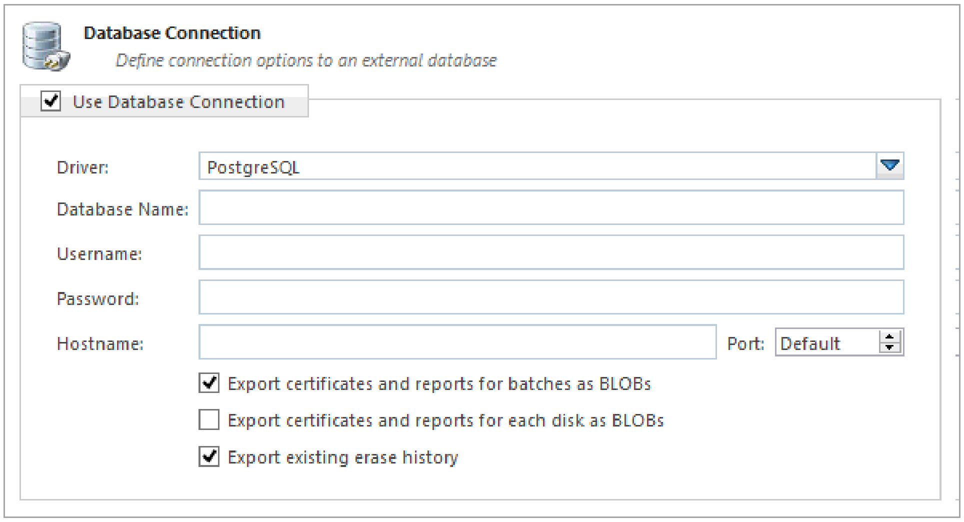
Supported connection to SQL databases:

- Any SQL92 Compliant Database (via ODBC)
- Microsoft SQL Server
- Microsoft Access
- PostgreSQL
- ORACLE
- MySQL
- SQLite

To connect to an external SQL database do one of:

1. Navigate to **Tools** > **Preferences** or press **F10**. Then click **Database Connection** tab on the left

2. Database Connection dialog appears:



Database Connection

Define connection options to an external database

☑ Use Database Connection

Driver: PostgreSQL

Database Name:

Username:

Password:

Hostname: Port: Default

☑ Export certificates and reports for batches as BLOBs

□ Export certificates and reports for each disk as BLOBs

☑ Export existing erase history

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
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 only once per a new connection)

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

Note:

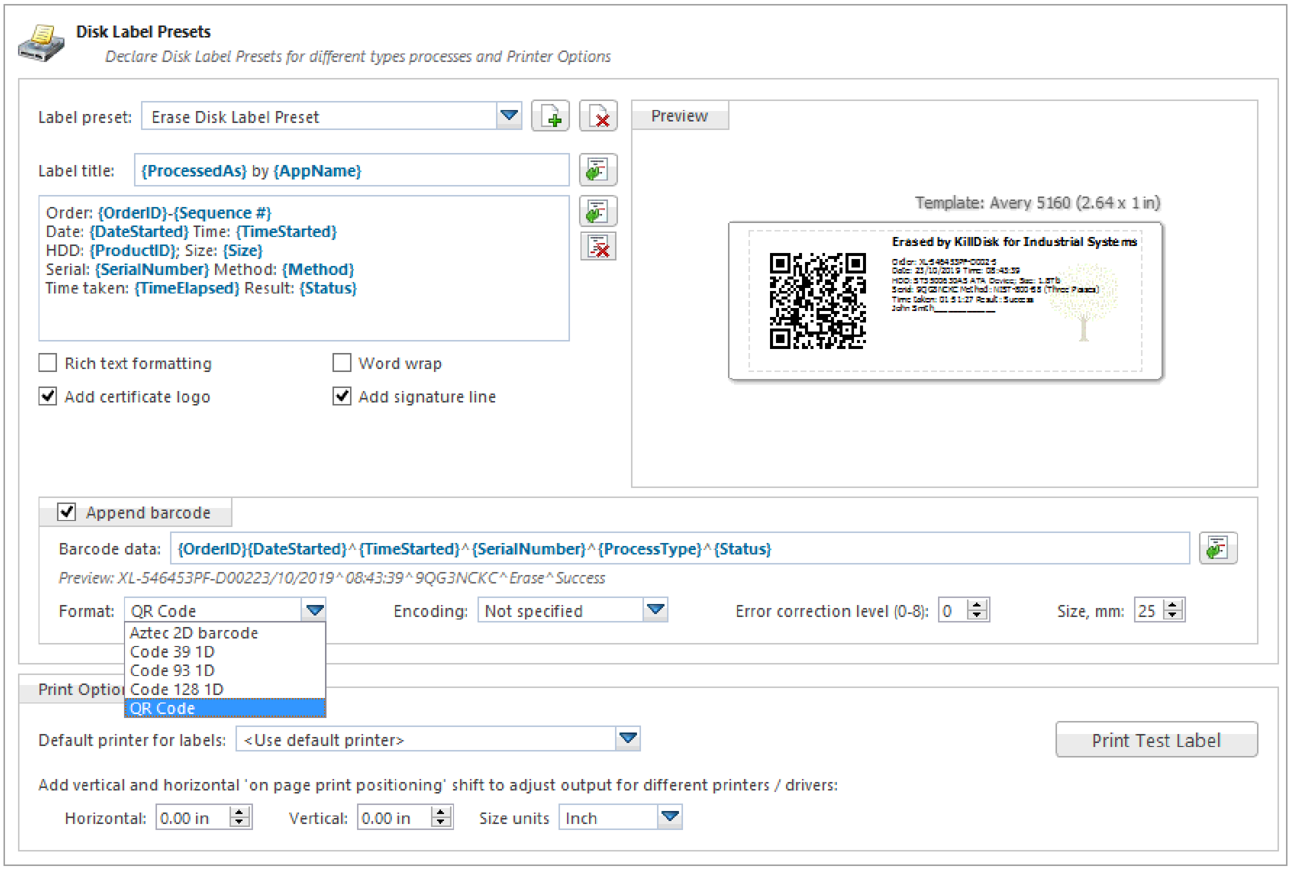
For the database export to be successful you need to provide a database user with privileges enough for creation two tables (**DISKS** and **BATCHES**) and populating these tables.

Related information

Event Journal on page 93

Disk Label Presets

These preferences help to adjust label settings for the **KillDisk** system globally. Labels may be formatted for any printer, page or label type (device) using **KillDisk** highly customizable labels' features.



Disk Label Presets

Declare Disk Label Presets for different types processes and Printer Options

Label preset: Erase Disk Label Preset

Label title: {ProcessedAs} by {AppName}

Order: {OrderID}-{Sequence #}
Date: {DateStarted} Time: {TimeStarted}
HDD: {ProductID}; Size: {Size}
Serial: {SerialNumber} Method: {Method}
Time taken: {TimeElapsed} Result: {Status}

□ Rich text formatting □ Word wrap

☑ Add certificate logo ☑ Add signature line

Preview

Template: Avery 5160 (2.64 x 1 in)

Erased by KillDisk for Industrial Systems

Order: XL-546453PF-D0022-5
Date: 23/10/2019 Time: 08:43:39
HDD: ST3500830AS ATA Device; Size: 1.5TB
Serial: 9QG3NCKC Method: NIST 800-88 (Three Passes)
Time taken: 01:51:27 Result: Success
John Smith____________

☑ Append barcode

Barcode data: {OrderID}{DateStarted}^{TimeStarted}^{SerialNumber}^{ProcessType}^{Status}

Preview: XL-546453PF-D00223/10/2019^08:43:39^9QG3NCKC^Erase^Success

Format: QR Code Encoding: Not specified Error correction level (0-8): 0 Size, mm: 25

Print Optio

Default printer for labels: <Use default printer>

Add vertical and horizontal 'on page print positioning' shift to adjust output for different printers / drivers:

Horizontal: 0.00 in Vertical: 0.00 in Size units Inch

Label preset

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

Label title

Allows you to set a title to be printed (in bold) at the top of the labels. It can be company name, batch name or any other descriptors you may consider useful to identify the operation. Static text can be typed in or any dynamic attributes (tags) can be inserted at current cursor's position. Click **Insert Name Tag** button ▤ to insert predefined tag from the drop-down list

Label Area

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

Label Attributes

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

Add signature line

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

Add certificate logo

Includes the logo used in the certificate as a label's watermark background

Label preview

Displays a preview of one label with the current input settings. Refreshes when any adjustments are made to the settings.

Barcode options

Selecting **Append barcode** check-box will print QR Code or Barcode on the label to be able to be scanned thereafter for third party inventory database

Barcode data

String including essential erase parameters to be encoded and transformed to QR Code or Barcode. Static text can be typed in or any dynamic attributes (tags) can be inserted at current cursor's position. Click **Insert Name Tag** button to insert predefined tag from the drop-down list

Preview

Displays a preview of encoded string with the current input settings. Refreshes when any adjustments are made to the settings.

Format

List of supported QR Code and Barcode formats. Currently supported: **Aztec 2D barcode**, **Code 39 1D**, **Code 93 1D**, **Code 128 1D**, **QR Code**. Note that different types of Barcodes can accept different size of encoded string

Encoding

If barcode string contains symbols other than English letters, you can specify encoding (code page) for the particular language

Error correction level

The lower the error correction level, the less dense the QR code image is, which improves minimum printing size. The higher the error correction level, the more damage it can sustain before it becomes unreadable

Size, mm

Size in millimeters for the Barcode/QR Code to be printed on the label

Print options

Define options for label printing including special label printers (Brother QL-700 etc.):

Default printer

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

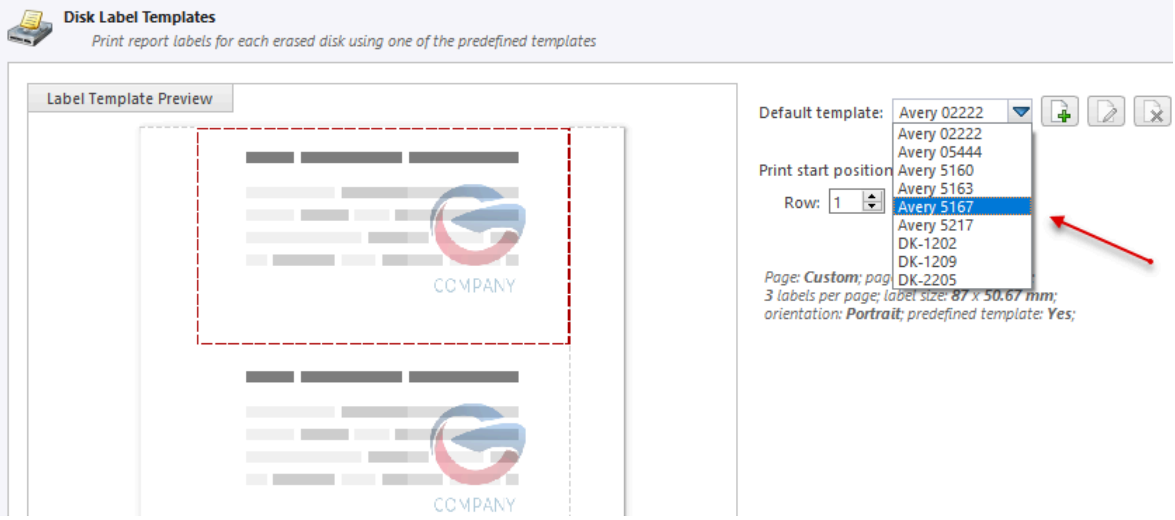
Print output adjustments

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

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

Disk Label Templates

Disk Label Templates tab defines set of predefined label templates for usage with different scenarios.



Disk Label Templates

Print report labels for each erased disk using one of the predefined templates

Default template: Avery 02222

Print start position

Row: 1

*Page: **Custom**; pag*
***3** labels per page; label size: **87 x 50.67 mm**;*
*orientation: **Portrait**; predefined template: **Yes**;*

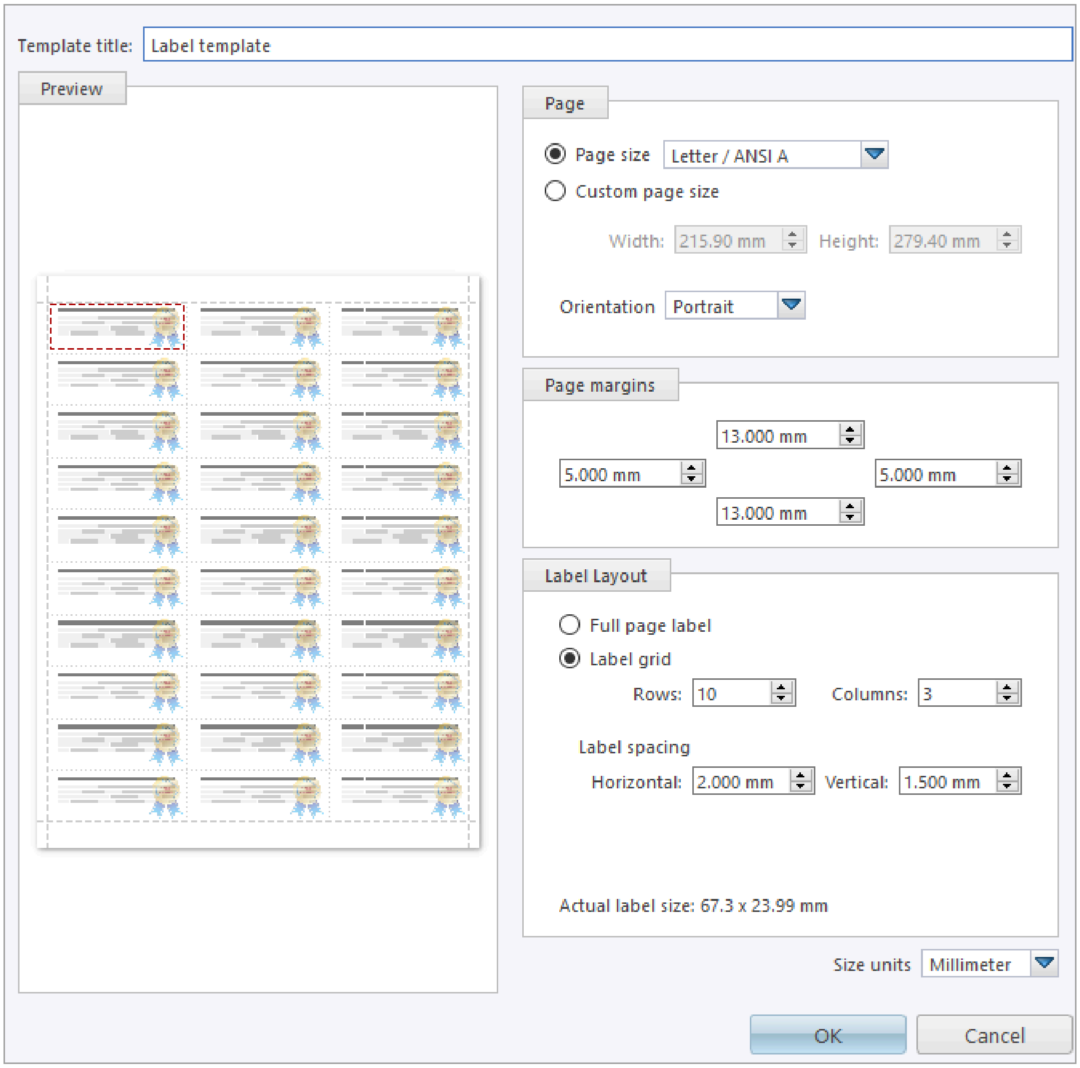
The print label dialog gives you an access to a number of predefined standard templates and to any custom templates you may create. These templates may be easily selected without opening any additional dialogs. The details of the selected template are displayed below the selection box. If your specific labels differ from any of the templates available the button allows you to create a custom template with your own specifications. Additionally, the button allows you to modify an existing template and the button deletes the selected template.

Print Start Position

The Print Start Position section of the dialogue allows you to select what label on the page is the one to start from. The labels won't always start from the 1x1 position, so you can adjust this setting accordingly

Creating a new template

Upon clicking the button the following Template Editor window appears. Descriptions of the Template Editor options are listed below.



Template title: Label template

Page

● Page size Letter / ANSI A

○ Custom page size

Width: 215.90 mm Height: 279.40 mm

Orientation Portrait

Page margins

13.000 mm

5.000 mm 5.000 mm

13.000 mm

Label Layout

○ Full page label

● Label grid

Rows: 10 Columns: 3

Label spacing

Horizontal: 2.000 mm Vertical: 1.500 mm

Actual label size: 67.3 x 23.99 mm

Size units Millimeter

Figure 100: Create a New Disk Label Template

Template Title

Here you may create a custom title for your template. This is the name to refer this template when selecting it in the *Print Label* dialog

Page

Here you can 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

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

Label Layout

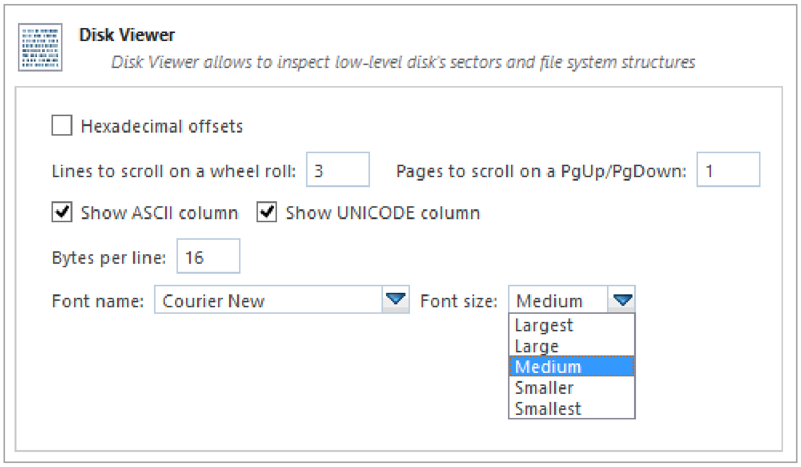
These settings define how the labels appear on the page. You may define the spacing in between labels on the page and the dimensions of the label grid. Once you've enter the proper measurements **KillDisk** will take care of the formatting

Size units

The units of measurement may vary 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

Disk Viewer

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



Disk Viewer

Disk Viewer allows to inspect low-level disk's sectors and file system structures

□ Hexadecimal offsets

Lines to scroll on a wheel roll: 3

Pages to scroll on a PgUp/PgDown: 1

☑ Show ASCII column ☑ Show UNICODE column

Bytes per line: 16

Font name: Courier New

Font size: Medium

Hexadecimal offsets

Toggles offset format between decimal and hexadecimal

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

Show ASCII column

Toggles display content in ASCII format

Show UNICODE column

Toggles display content in UNICODE format

Bytes per line

Defines amount of bytes per line in binary display

Font name

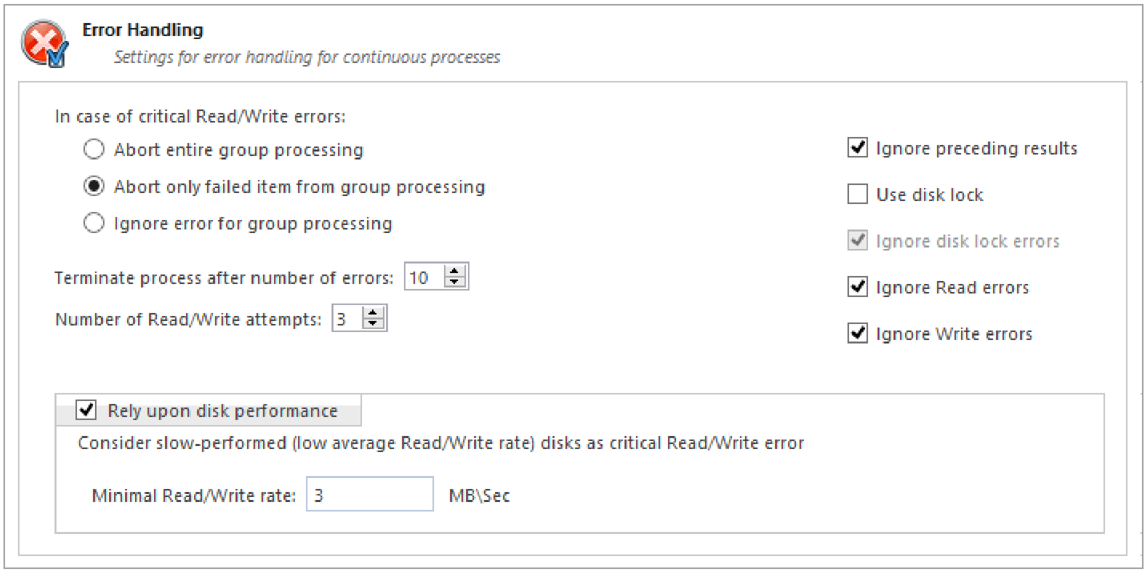
Select any *mono-space* font available for better experience

Font size

Font size to be used in binary view

Error Handling

KillDisk has a wide capabilities to handle errors during continuous disk processing. Those are the advanced settings to configure **KillDisk**'s error handling.



Error Handling

Settings for error handling for continuous processes

In case of critical Read/Write errors:

○ Abort entire group processing

● Abort only failed item from group processing

○ Ignore error for group processing

Terminate process after number of errors: 10

Number of Read/Write attempts: 3

☑ Ignore preceding results

□ Use disk lock

☑ Ignore disk lock errors

☑ Ignore Read errors

☑ Ignore Write errors

☑ Rely upon disk performance

Consider slow-performed (low average Read/Write rate) disks as critical Read/Write error

Minimal Read/Write rate: 3 MB\Sec

Error handling attributes

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

Abort entire disk group processing
This means that if user runs a Batch erase and one of the disks has errors the erase process for ALL the disks in the batch is terminated

Abort only failed disk from group processing
This is the suggested setting. Failed disks return an error and terminate the erase process. But other disks in the batch are not interrupted from 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** makes to perform an operation when an error is encountered before it stops execution

Ignore preceding results
Errors (if any) on previous steps (i.e. *Examination*) are ignored and following steps (i.e. *Erase*, *Clone*) will be performed. If turned off the errors on previous steps will stop all further actions

Use disk lock
Locks disks from being used by any other applications

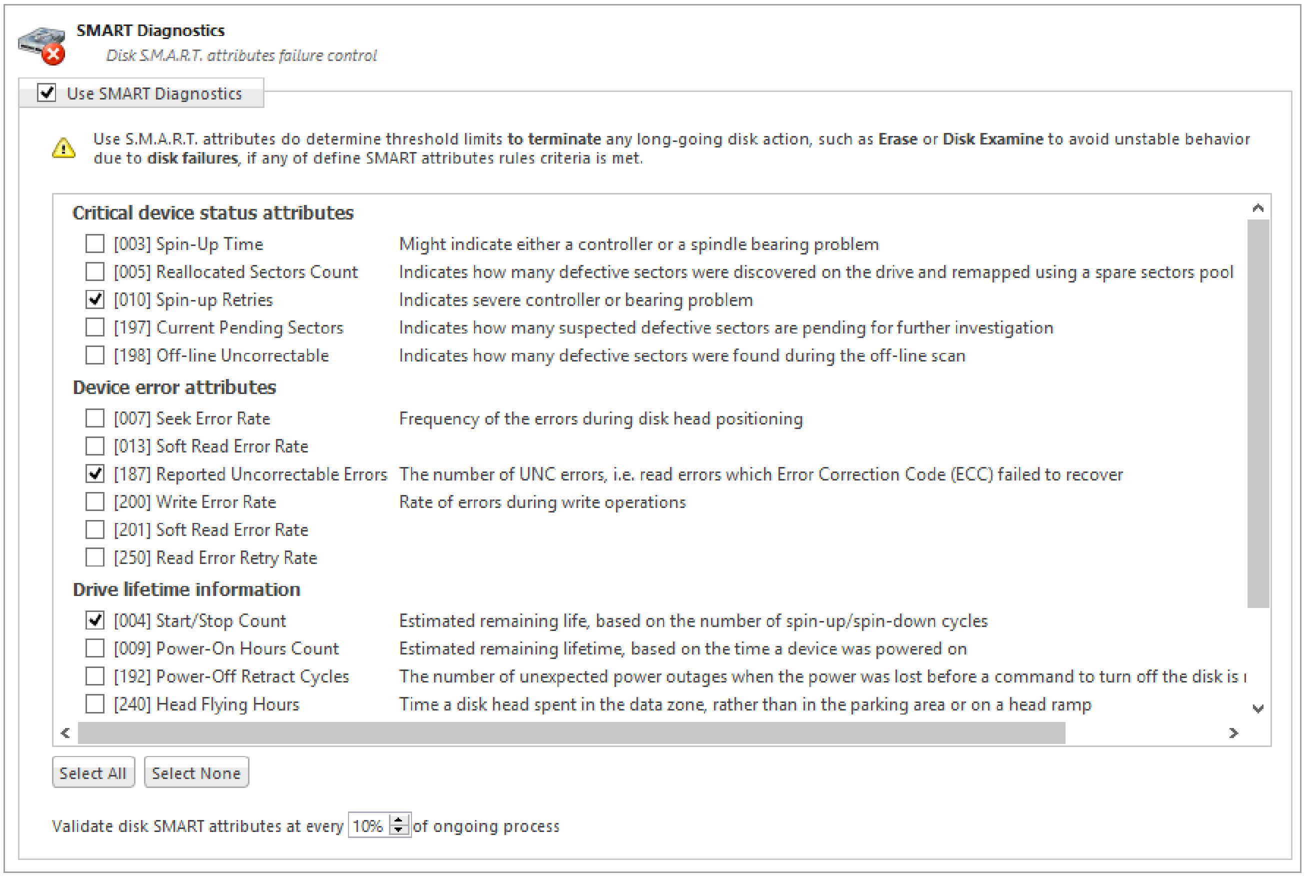
Ignore disk lock errors
Errors encountered with **KillDisk** not being able to access locked disks are ignored

Ignore read/write errors
Toggle whether errors should appear for read/write errors

Rely upon disk performance
Set a minimum acceptable read/write speed in megabytes per second for disks to flag under-performing drives

SMART Diagnostics

S.M.A.R.T. attributes may also be used in error handling. So threshold limits may be set on some or on all of the disks S.M.A.R.T. parameters. This may speed up processing by immediately terminating operations with unusable drives.



SMART Diagnostics

Disk S.M.A.R.T. attributes failure control

☑ Use SMART Diagnostics

⚠ Use S.M.A.R.T. attributes do determine threshold limits **to terminate** any long-going disk action, such as **Erase** or **Disk Examine** to avoid unstable behavior due to **disk failures**, if any of define SMART attributes rules criteria is met.

Critical device status attributes

☐ [003] Spin-Up Time	Might indicate either a controller or a spindle bearing problem
☐ [005] Reallocated Sectors Count	Indicates how many defective sectors were discovered on the drive and remapped using a spare sectors pool
☑ [010] Spin-up Retries	Indicates severe controller or bearing problem
☐ [197] Current Pending Sectors	Indicates how many suspected defective sectors are pending for further investigation
☐ [198] Off-line Uncorrectable	Indicates how many defective sectors were found during the off-line scan

Device error attributes

☐ [007] Seek Error Rate	Frequency of the errors during disk head positioning
☐ [013] Soft Read Error Rate	
☑ [187] Reported Uncorrectable Errors	The number of UNC errors, i.e. read errors which Error Correction Code (ECC) failed to recover
☐ [200] Write Error Rate	Rate of errors during write operations
☐ [201] Soft Read Error Rate	
☐ [250] Read Error Retry Rate	

Drive lifetime information

☑ [004] Start/Stop Count	Estimated remaining life, based on the number of spin-up/spin-down cycles
☐ [009] Power-On Hours Count	Estimated remaining lifetime, based on the time a device was powered on
☐ [192] Power-Off Retract Cycles	The number of unexpected power outages when the power was lost before a command to turn off the disk is
☐ [240] Head Flying Hours	Time a disk head spent in the data zone, rather than in the parking area or on a head ramp

Validate disk SMART attributes at every 10% of ongoing process

Note:

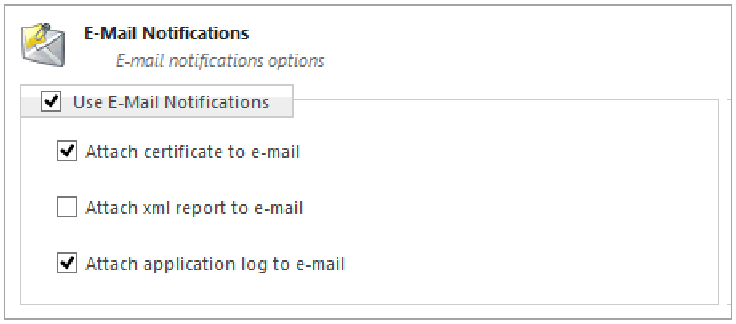
Query execution for S.M.A.R.T. attributes is time and resource consuming operation. It can interrupt disk erasure procedure for several seconds. Thus it is recommended to validate these attributes not very frequently

Related information

S.M.A.R.T. Monitor on page 91

E-mail Notifications

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



E-Mail Notifications

E-mail notifications options

☑ Use E-Mail Notifications

☑ Attach certificate to e-mail

□ Attach xml report to e-mail

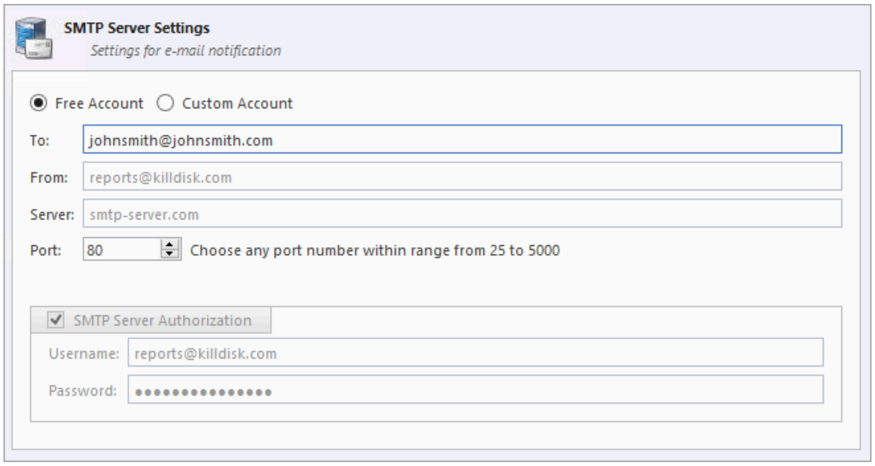
☑ Attach application log to e-mail

Certificate, XML Report or Application Log can be e-mailed 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 user's mailbox. *Simple Mail Transport Protocol* (SMTP) is responsible for transmitting e-mail messages and needs to be configured properly.



SMTP Server Settings

Settings for e-mail notification

● Free Account ○ Custom Account

To: johnsmith@johnsmith.com

From: reports@killdisk.com

Server: smtp-server.com

Port: 80 Choose any port number within range from 25 to 5000

☑ SMTP Server Authorization

Username: reports@killdisk.com

Password: ●●●●●●●●●●●●●●●

Account Type

KillDisk offers you a free SMTP account located on **www.smtp-server.com** that can be used for sending reports out. By default all the required parameters are 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 the settings manually. Ask your system/network administrator to get these parameters

To

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

From

Type an 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

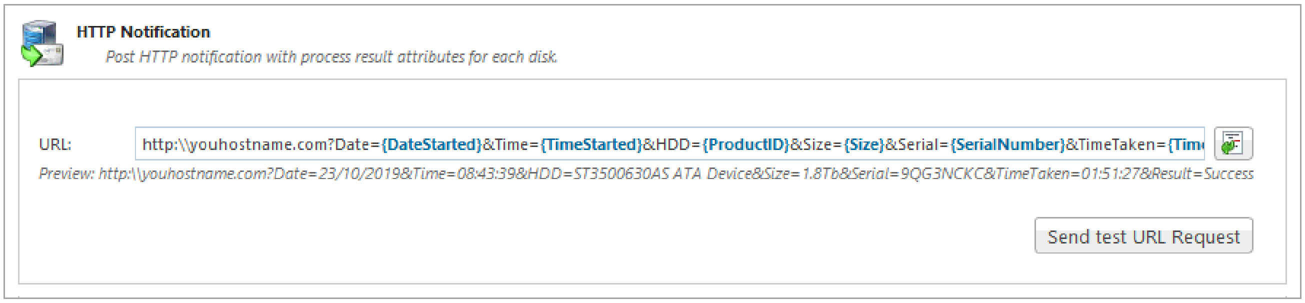
For the free SMTP account **KillDisk** allows you to use smtp-server.com on port 80. This is a standard port being used by all web browsers to access the Internet. This port most likely is open on a corporate and home networks. Other ports can be filtered by and closed by a network firewall. Ask your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

SMTP Server authorization

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

HTTP Notifications

HTTP Notification is a **KillDisk Industrial** feature for collecting and managing application statistics using your own deployed custom HTTP server.



HTTP Notification

Post HTTP notification with process result attributes for each disk.

URL: http:\\youhostname.com?Date={DateStarted}&Time={TimeStarted}&HDD={ProductID}&Size={Size}&Serial={SerialNumber}&TimeTaken={Tim

Preview: http:\\youhostname.com?Date=23/10/2019&Time=08:43:39&HDD=ST3500630AS ATA Device&Size=1.8Tb&Serial=9QG3NCKC&TimeTaken=01:51:27&Result=Success

The server address, port and parameters (attributes) are specified in the URL field. Preview shows the assembled request string. Click the **Send test URL Request** button in order to test the connection. If everything is configured well your server is going to receive a list of desired attributes (described as name tags) after Disk Erase procedure.

Related information

Name Tags on page 153

Troubleshooting

In the event that you experience any technical difficulties with **KillDisk** you may choose to either troubleshoot the system yourself or, if you have an 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 (hardware diagnostic)

Common Troubleshooting Tips

Disk data is not erased

Ensure you are not erasing the system disk from the application. Ensure that disk is fully functional (not physically damages) and is accessible by Operating System.

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 OS use the **Erase Disk** operation

Erased the wrong disk

Stop the operation as soon as possible. Once data is sanitized by erase features it will no longer be accessible. Use a tool like **Active@ File Recovery** (https://www.file-recovery.com) to recover any data that has not been sanitized yet

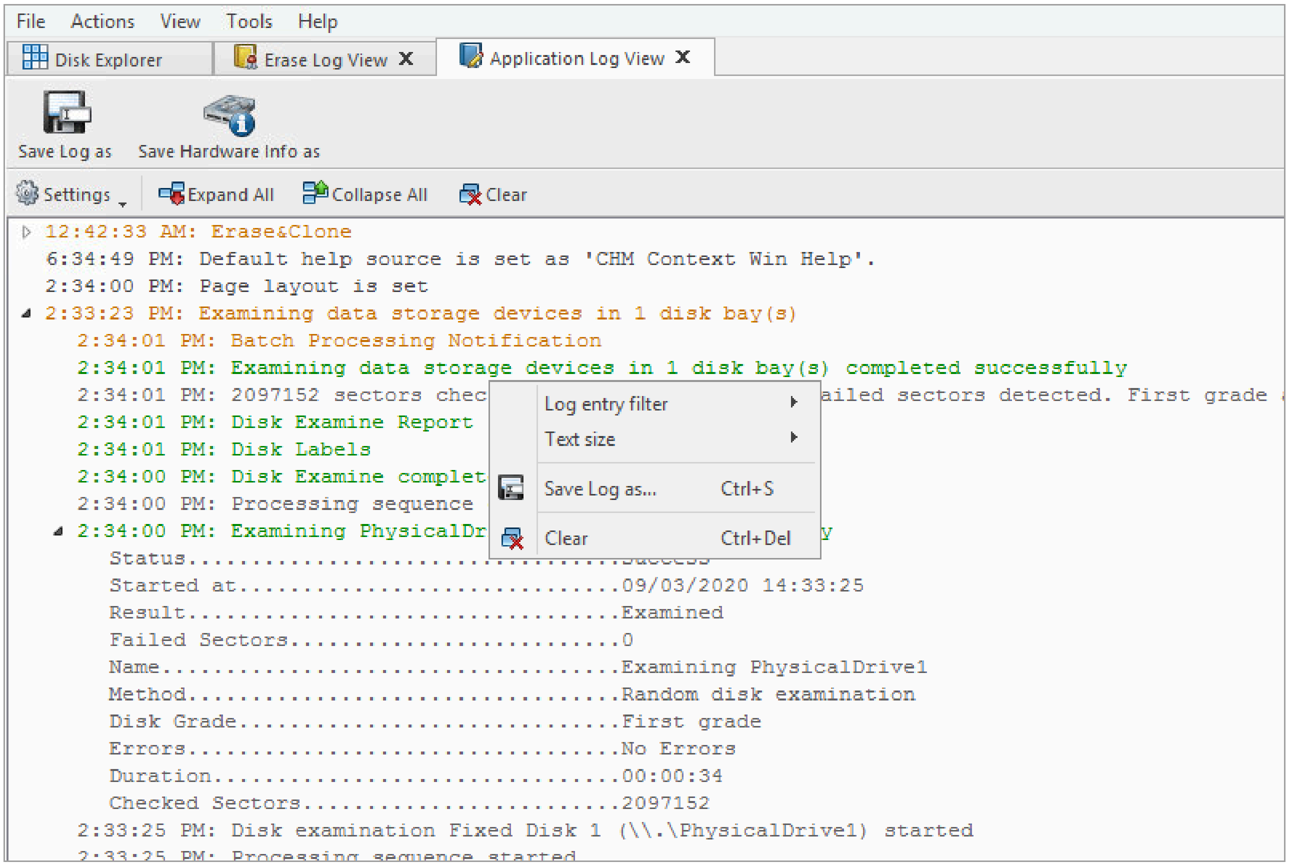
Application Log

Application Log View reflects every action taken by the application and displays messages, notifications and other service information. Use the messages in this screen to observe and further analysis 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 (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.



```
▷ 12:42:33 AM: Erase&Clone
  6:34:49 PM: Default help source is set as 'CHM Context Win Help'.
  2:34:00 PM: Page layout is set
◢ 2:33:23 PM: Examining data storage devices in 1 disk bay(s)
    2:34:01 PM: Batch Processing Notification
    2:34:01 PM: Examining data storage devices in 1 disk bay(s) completed successfully
    2:34:01 PM: 2097152 sectors chec                     ailed sectors detected. First grade
    2:34:01 PM: Disk Examine Report
    2:34:01 PM: Disk Labels
    2:34:00 PM: Disk Examine complet
    2:34:00 PM: Processing sequence
  ◢ 2:34:00 PM: Examining PhysicalDr                     y
      Status.................................Success
      Started at.............................09/03/2020 14:33:25
      Result.................................Examined
      Failed Sectors.........................0
      Name...................................Examining PhysicalDrive1
      Method.................................Random disk examination
      Disk Grade.............................First grade
      Errors.................................No Errors
      Duration...............................00:00:34
      Checked Sectors........................2097152
    2:33:25 PM: Disk examination Fixed Disk 1 (\\.\PhysicalDrive1) started
    2:33:25 PM: Processing sequence started
```

Figure 101: Application Log View

Save Log As

Opens a standard **save as** dialog. Save the actual application log file to the local disk (default extension is *.log*)

Save Hardware Info as

Opens a standard **save as** dialog. Save the *disk diagnostic file* to the local disk (default extension is *.xml*)

With sub-menu the following items are available:

Log entry filter

Shows or hides specific entry types in Log View:

Minimum details

Shows non-critical warning entries

Maximum details

Shows advanced entries related to the application behavior and data analysis

Text size

Changes text size to **Large**, **Normal** or **Small**

Expand All

Expands a tree log data if available

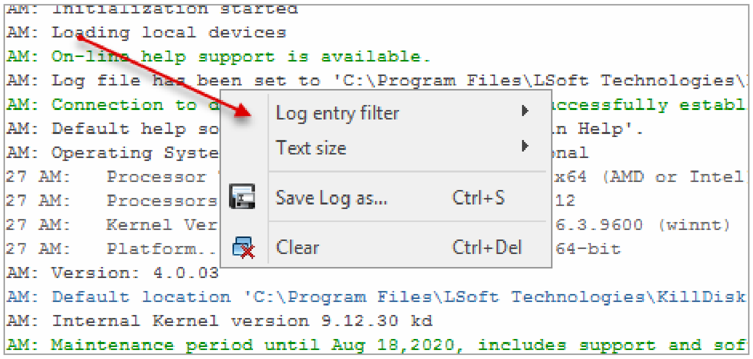
Collapse All

Collapses a tree log data if available

Clear

Clear log for current application sessions

It is possible to go through the options with the context menu (right mouse click).



```
AM: Initialization started
AM: Loading local devices
AM: On-line help support is available.
AM: Log file has been set to 'C:\Program Files\LSoft Technologies\
AM: Connection to d                                   uccessfully establ
AM: Default help so                                   n Help'.
AM: Operating Syste                                   nal
27 AM:    Processor                                   x64 (AMD or Intel
27 AM:    Processors                                  12
27 AM:    Kernel Ver                                  6.3.9600 (winnt)
27 AM:    Platform..                                  64-bit
AM: Version: 4.0.03
AM: Default location 'C:\Program Files\LSoft Technologies\KillDisk
AM: Internal Kernel version 9.12.30 kd
AM: Maintenance period until Aug 18,2020, includes support and sof
```

Figure 102: Context menu

Tip:

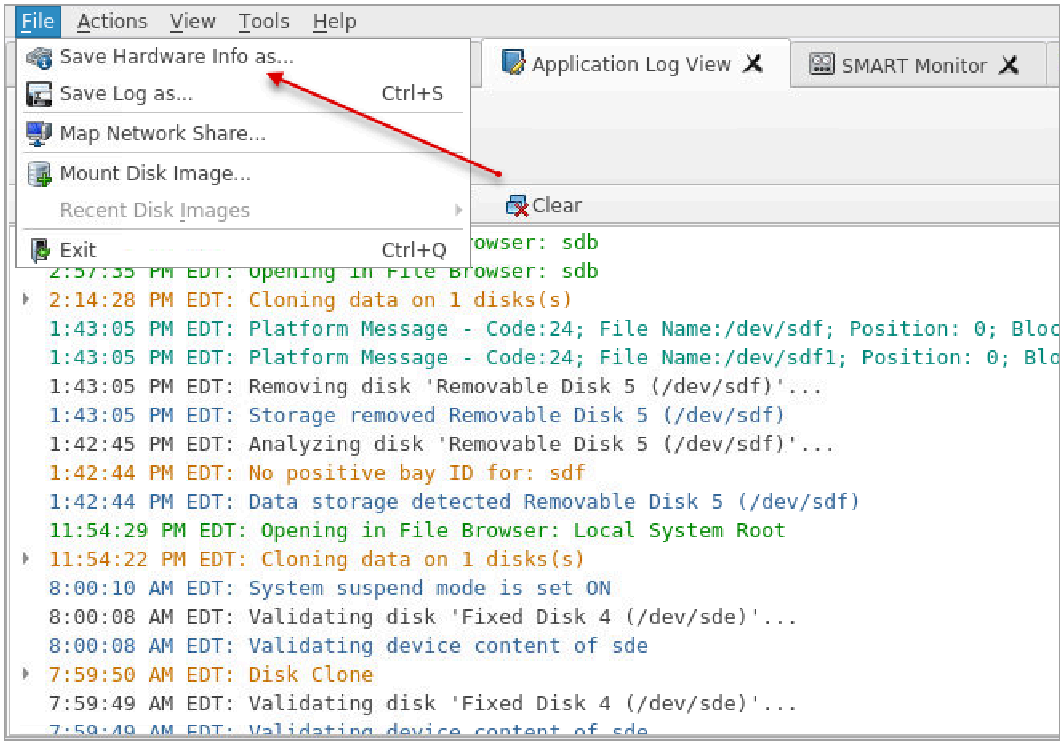
We recommend that you attach a copy of the log file to all requests made to our technical support group. The entries in this file will help us to resolve certain issues.

Hardware Diagnostic File

If you want to contact our technical support 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 to 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...** button.



```
                                 owser: sdb
  2:57:35 PM EDT: Opening in File Browser: sdb
▸ 2:14:28 PM EDT: Cloning data on 1 disks(s)
  1:43:05 PM EDT: Platform Message - Code:24; File Name:/dev/sdf; Position: 0; Bloc
  1:43:05 PM EDT: Platform Message - Code:24; File Name:/dev/sdf1; Position: 0; Blo
  1:43:05 PM EDT: Removing disk 'Removable Disk 5 (/dev/sdf)'...
  1:43:05 PM EDT: Storage removed Removable Disk 5 (/dev/sdf)
  1:42:45 PM EDT: Analyzing disk 'Removable Disk 5 (/dev/sdf)'...
  1:42:44 PM EDT: No positive bay ID for: sdf
  1:42:44 PM EDT: Data storage detected Removable Disk 5 (/dev/sdf)
  11:54:29 PM EDT: Opening in File Browser: Local System Root
▸ 11:54:22 PM EDT: Cloning data on 1 disks(s)
  8:00:10 AM EDT: System suspend mode is set ON
  8:00:08 AM EDT: Validating disk 'Fixed Disk 4 (/dev/sde)'...
  8:00:08 AM EDT: Validating device content of sde
▸ 7:59:50 AM EDT: Disk Clone
  7:59:49 AM EDT: Validating disk 'Fixed Disk 4 (/dev/sde)'...
  7:59:49 AM EDT: Validating device content of sde
```

Note:

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

Related information

Application Log on page 129

Appendix

Glossary

BIOS Settings

Basic **I**nput **O**utput **S**ubsystem is the program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse and printer. A typical method to access the BIOS settings screen is to press **Delete** / **F1** / **F2** / **F8** / **F10** or **Esc** during the boot sequence

BCD

Boot **C**onfiguration **D**ata. Firmware-independent database for boot-time configuration data. It is used by *Microsoft*'s new *Windows Boot Manager* and replaces the *boot.ini* that was used by NTLDR

Boot Priority

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

Boot Record

See MBR

Boot Sector

The boot sector continues the process of loading the operating system into computer memory. It can be either the Glossary on page 131MBR or the Glossary on page 131partition boot sector (see partition boot sector, below)

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

CSV-file

A *comma-separated values* (**CSV**) file is a delimited text file that uses a comma to separate values. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. The use of the comma as a field separator is the source of the name for this file format. A *CSV-file* typically stores tabular data (numbers and text) in plain text, in which case each line will have the same number of fields

Data Cluster

A cluster or *allocation unit* is a unit of disk space allocation for files and directories. To reduce the overhead of managing on-disk data structures, the file system does not allocate individual disk sectors by default, but contiguous groups of sectors, called clusters. A cluster is the smallest logical amount of disk space that can be allocated to hold a file. Storing small files on a file system with large clusters will therefore waste disk space; such wasted disk space is called slack space. For cluster sizes which are small versus the average file size, the wasted space per file will be statistically about half of the cluster size; for large cluster sizes, the wasted space will become greater. However, a larger cluster size reduces bookkeeping overhead and fragmentation, which may improve reading and writing speed overall. Typical cluster sizes range from 1 sector (512 B) to 128 sectors (64 Kb). The operating system keeps track of clusters in the hard disk's root records or MFT records (See Lost Cluster)

Device Node

In the **Local System Devices** list, a physical device containing logical drives. The first physical device is named *80h*

Exclusive Access

Lock that is applied to a partition for exclusive writing access. For example, while recovering deleted or damaged files or folders. The recovery operation must have exclusive access to the target partition while recovering files. If another application or the operating system are using the target partition, user/process must close all applications or system processes that may be using the target partition before locking it

FAT

File **A**llocation **T**able. File (dump) 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. *FAT* file systems are still commonly found on floppy disks, flash and other solid-state memory cards and modules (including USB flash drives), as well as many portable and embedded devices. *FAT* is the standard file system for digital cameras per the *DCF* specification

FTP

File **T**ransfer **P**rotocol. This is a standard network protocol used for the transfer of computer files between a *Client* and *Server* on a computer network. *FTP* is built on a client-server model architecture using separate control and data connections between the client and the server. *FTP* users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, *FTP* is often secured with *SSL/TLS (FTPS)* or replaced with *SSH File Transfer Protocol (SFTP)*. The first *FTP* client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most *Windows*, *Unix*, and *Linux* operating systems. Many *FTP* clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and *FTP* has been incorporated into productivity applications, such as *HTML* editors

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

FreeDOS

A free operating system for IBM PC compatible computers. It intends to provide a complete *DOS*-compatible environment for running legacy software and supporting embedded systems. *FreeDOS* can be booted from a floppy disk or USB flash drive. It is designed to run well under virtualization or *x86* emulation. Unlike most versions of *MS-DOS*, *FreeDOS* is composed of free and open-source software, licensed under the terms of the *GNU General Public License*

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

iSCSI

Internet **S**mall **C**omputer **S**ystems **I**nterface. *iSCSI* is a transport layer protocol that works on top of the *Transport Control Protocol (TCP)*. It enables block-level *SCSI* data transport between the *iSCSI* initiator and the storage target over *TCP/IP* networks

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 file name extension .ISO (though not necessarily), and are commonly referred to as "ISOs"

Logical Drive

A partition is a logical drive because it does not affect the physical hard disk other than the defined space that it occupies, yet it behaves like a separate disk drive

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

MBR

Master **B**oot **R**ecord. All disks start with a boot sector. When you start the computer, the code in the MBR executes before the operating system is started. The location of the MBR is always track (cylinder) 0, side (head) 0, and sector 1. The MBR contains a file system identifier

MFT records

Master **F**ile **T**able. 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

Named Streams

NTFS supports multiple data streams where the stream name identifies a new data attribute on the file. A handle can be opened to each data stream. A data stream, then, is a unique set of file attributes. Streams have separate opportunistic locks, file locks, and sizes, but common permissions

NTFS

NT file system, **N**ew **T**echnology **F**ile **S**ystem (developed by Microsoft) is the file system that the *Windows NT* operating system uses for storing and retrieving files on a hard disk. *NTFS* is the *Windows NT* equivalent of the *Windows 95* file allocation table (FAT) and the OS/2 High Performance File System (HPFS)

NTLDR

Aka *NT loader* is the boot loader for all releases of *Windows NT* operating system up to and including *Windows XP* and *Windows Server 2003*. *NTLDR* is typically run from the primary hard disk drive, but it can also run from portable storage devices such as a CD-ROM, USB flash drive, or floppy disk

openSUSE

A *Linux* distribution. It is widely used throughout the world. The focus of its development is creating usable open-source tools for software developers and system administrators, while providing a user-friendly desktop and feature-rich server environment

Partition

A section of memory or hard disk isolated for a specific purpose. Each partition can behave like a separate disk drive

Partition Boot Sector

On NTFS or FAT file systems, the partition boot sector is a small program that is executed when the operating system tries to access a particular partition. On personal computers, the Master Boot Record uses the partition boot sector on the system partition to determine file system type, cluster size, etc. and to load the operating system kernel files. Partition boot sector is the first sector of the partition

Physical Device

A piece of hardware that is attached to your computer by screws or wires. A hard disk drive is a physical device. It is also referred to as a *physical drive*

RAID

RAID ("**R**edundant **A**rray of **I**nexpensive **D**isks" or "**R**edundant **A**rray of **I**ndependent **D**isks") is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. Data is distributed across the drives in one of several ways, referred to as *RAID* levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are named by the word "*RAID*" followed by a number, for example *RAID **0*** or *RAID **1***. Each scheme, or *RAID* level, provides a different balance among the key goals: reliability, availability, performance, and capacity. *RAID* levels greater than *RAID 0* provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives.

RAID 0

RAID 0 consists of striping, but no mirroring or parity. Compared to a spanned volume, the capacity of a *RAID 0* volume is the same; it is the sum of the capacities of the drives in the set. But because striping distributes the contents of each file among all drives in the set, the failure of any drive causes the entire *RAID 0* volume and all files to be lost. In comparison, a spanned volume preserves the files on the unfailing drives. The benefit of *RAID 0* is that the throughput of read and write operations to any file is multiplied by the number of drives because, unlike spanned volumes, reads and writes are done concurrently. The cost is increased vulnerability to drive failures—since any drive in a *RAID 0* setup failing causes the entire volume to be lost, the average failure rate of the volume rises with the number of attached drives

RAID 1

RAID 1 consists of data mirroring, without parity or striping. Data is written identically to two or more drives, thereby producing a "mirrored set" of drives. Thus, any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first (depending on its seek time and rotational latency), improving performance. Sustained read throughput, if the controller or software is optimized for it, approaches the sum of throughputs of every drive in the set, just as for *RAID 0*. Actual read throughput of most *RAID 1* implementations is slower than the fastest drive. Write throughput is always slower because every drive must be updated, and the slowest drive limits the write performance. The array continues to operate as long as at least one drive is functioning

RAID 2

RAID 2 consists of bit-level striping with dedicated Hamming-code parity. All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive. This level is of historical significance only; although it was used on some early machines (for example, the Thinking Machines *CM-2*), as of 2014 it is not used by any commercially available system

RAID 3

RAID 3 consists of byte-level striping with dedicated parity. All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive. Parity is calculated across corresponding bytes and stored on a dedicated parity drive. Although implementations exist, *RAID 3* is not commonly used in practice

RAID 4

RAID 4 consists of block-level striping with dedicated parity. This level was previously used by NetApp, but has now been largely replaced by a proprietary implementation of *RAID 4* with two parity disks, called RAID-DP. The main advantage of *RAID 4* over *RAID 2* and *3* is I/O parallelism: in *RAID 2* and *3*, a single read I/O operation requires reading the whole group of data drives, while in *RAID 4* one I/O read operation does not have to spread across all data drives. As a result, more I/O operations can be executed in parallel, improving the performance of small transfers

RAID 5

RAID 5 consists of block-level striping with distributed parity. Unlike *RAID 4*, parity information is distributed among the drives, requiring all drives but one to be present to operate. Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. *RAID 5* requires at least three disks. Like all single-parity concepts, large *RAID 5* implementations are susceptible to system failures because of trends regarding array rebuild time and the chance of drive failure during rebuild. Rebuilding an array requires reading all data from all disks, opening a chance for a second drive failure and the loss of the entire array

RAID 6

RAID 6 consists of block-level striping with double distributed parity. Double parity provides fault tolerance up to two failed drives. This makes larger *RAID* groups more practical, especially for high-availability systems, as large-capacity drives take longer to restore. *RAID 6* requires a minimum of four disks. As with *RAID 5*, a single drive failure results in reduced performance of the entire array until the failed drive has been replaced. With a *RAID 6* array, using drives from multiple sources and manufacturers, it is possible to mitigate most of the problems associated with *RAID 5*. The larger the drive capacities and the larger the array size, the more important it becomes to choose *RAID 6* instead of *RAID 5*. *RAID 10* (see Nested RAID levels) also minimizes these problems

PXE

Preboot E**X**ecution **E**nvironment. 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*

RAS

Remote **A**ccess **S**ervice. Is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

A remote access service connects a client to a host computer, known as a remote access server. The most common approach to this service is remote control of a computer by using another device which needs internet or any other network connection.

Here are the connection steps:

1. User dials into a PC at the office.
2. Then the office PC logs into a file server where the needed information is stored.
3. The remote PC takes control of the office PC's monitor and keyboard, allowing the remote user to view and manipulate information, execute commands, and exchange files.

Many computer manufacturers and large businesses' help desks use this service widely for technical troubleshooting of their customers' problems. Therefore you can find various professional first-party, third-party, open source, and freeware **remote desktop applications.** Which some of those are cross-platform across various versions of *Windows*, *MacOS*, *UNIX*, and *Linux*. Remote desktop programs may include *LogMeIn* or *TeamViewer*.

To use *RAS* from a remote node, a *RAS* client program is needed, or any PPP client software. Most remote control programs work with *RAS*. *PPP* is a set of industry standard framing and authentication protocols that enable remote access.

Microsoft Remote Access Server (*RAS*) is the predecessor to *Microsoft Routing* and *Remote Access Server (RRAS)*. *RRAS* is a *Microsoft Windows Server* feature that allows *Microsoft Windows* clients to remotely access a *Microsoft Windows* network.

Registry Hive

Highest level of organization in the *Windows* registry. It is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when *Windows* is started or an user logs in

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

SAM

Security **A**ccount **M**anager. Database file that stores users' passwords in a hashed format. Since a hash function is one-way, this provides some measure of security for the storage of the passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory authenticates remote users.

Sector

The smallest unit that can be accessed on a disk. Typically sector size is 512 or 4096 bytes

SCSI

Small **C**omputer **S**ystem **I**nterface. A set of standards for physically connecting and transferring data between computers and peripheral devices. The *SCSI* standards define commands, protocols, electrical, optical and logical interfaces. *SCSI* is most commonly used for hard disk drives and tape drives, but it can connect a wide range of other devices, including scanners and CD drives, although not all controllers can handle all devices. The *SCSI* standard defines command sets for specific peripheral device types; the presence of "unknown" as one of these types means that in theory it can be used as an interface to almost any device, but the standard is highly pragmatic and addressed toward commercial requirements

Secure Erase (SSD)

The *ATA Secure Erase* command is designed to remove all user data from a drive. With an SSD without integrated encryption, this command will put the drive back to its original out-of-box state. This will initially restore its performance to the highest possible level and the best (lowest number) possible write amplification, but as soon as the drive starts garbage collecting again the performance and write amplification will start returning to the former levels. Drives which encrypt all writes on the fly can implement *ATA Secure Erase* in another way. They simply *zeroize* and generate a new random encryption key each time a secure erase is done. In this way the old data cannot be read anymore, as it cannot be decrypted. Some drives with an integrated encryption will physically clear all blocks after that as well, while other drives may require a *TRIM* command to be sent to the drive to put the drive back to its original out-of-box state (as otherwise their performance may not be maximized)

Secure Erase (Security Frozen State)

SSD disk is blocked (frozen) by BIOS. The reasons can differ. Modern ATA hard drives and SSDs offer security options that help user to control access and reliably destroy data if necessary. Brand new HDD or SSD from a store have all the security features initially disabled... BIOSes of many motherboards run the *SECURITY_FREEZE_LOCK* ATA command when booting to provide protection against manipulation

Signature Files

File types are recognized by specific patterns that may serve as a reference for file recovery. When a file header is damaged, the type of file may be determined by examining patterns in the damaged file and comparing these patterns to known file type templates

Span Array

A series of dynamic drives linked together to make one contiguous spanned volume

S.M.A.R.T.

S.M.A.R.T. (*Self-Monitoring, Analysis and Reporting Technology*; often written as *SMART*) is a monitoring system included in computer hard disk drives (*HDDs*), solid-state drives (*SSDs*) and *embedded MultiMediaCards (eMMC*) drives. Its primary function is to detect and report various indicators of drive reliability with the intent of anticipating imminent hardware failures. When **S.M.A.R.T.** data indicates a possible imminent drive failure, software running on the host system may notify the user so preventative action can be taken to prevent data loss and the failing drive can be replaced and data integrity maintained

Templates (patterns)

File types are recognized by specific patterns that may serve as a reference for file recovery. When a file header is damaged, the type of file may be determined by examining patterns in the damaged file and comparing these patterns to known file type templates. This same pattern-matching process can be applied to deleted or damaged partitions. Using FAT or NTFS templates, recovery software can assume that a particular sector is a FAT or NTFS boot sector because parts of it match a known pattern

Tiny Core Linux

A minimal *Linux* kernel based operating system focusing on providing a base system functionality. The distribution is notable for its small size (11 to 16 MB) and minimalism; additional functions are provided by extensions. *Tiny Core Linux* is free and open source software and is licensed under the *GNU General Public License version 2*

Track

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

UEFI

Unified **E**xtensible **F**irmware **I**nterface is a specification for a software program that connects a computer's firmware to its operating system (OS). *UEFI* is expected to eventually replace *BIOS*. Like *BIOS*, *UEFI* is installed at the time of manufacturing and is the first program that runs when a computer is turned on

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

Volume

A fixed amount of storage on a hard disk. A physical device may contain a number of volumes. It is also possible for a single volume to span a number of physical devices

Volume Shadow Copy

Shadow Copy (also known as *Volume Snapshot Service*, *Volume Shadow Copy Service* or **VSS**) is a technology included in *Microsoft Windows* that can create backup copies or snapshots of computer files or volumes, even when they are in use. It is implemented as a *Windows* service called the *Volume Shadow Copy* service

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* OS. This enhances performance of the computer when doing repetitive tasks. Over time, these records can take up a lot of space

Windows PE

Windows PE (**WinPE**) for *Windows* 10 is a small operating system used as a recovery environment to install, deploy, and repair *Windows* 10 for Desktop Editions, *Windows Server*, and other *Windows* operating systems. After boot to *Windows PE*, user can:

- Set up a hard drive before installing *Windows*.
- Install *Windows* by using apps or scripts from a network or a local drive.
- Capture and apply *Windows* images.
- Modify the *Windows* operating system while it's not running.
- Set up automatic recovery tools.
- Recover data from unbootable devices.
- Add a custom shell or GUI to automate these kinds of tasks

How Fast Erasing Occurs?

An actual speed depends on many factors:

- HDD speed: RPM and *SATA/SCSI/SAS* type - the most important factors
- Disk Controller speed: *SAS* (6 Gbps/12 Gbps), *SATA III* (6Gbps), *SATA II* (3 Gbps), *SATA I* (1.5 Gbps)
- Computer overall performance (CPU + RAM)

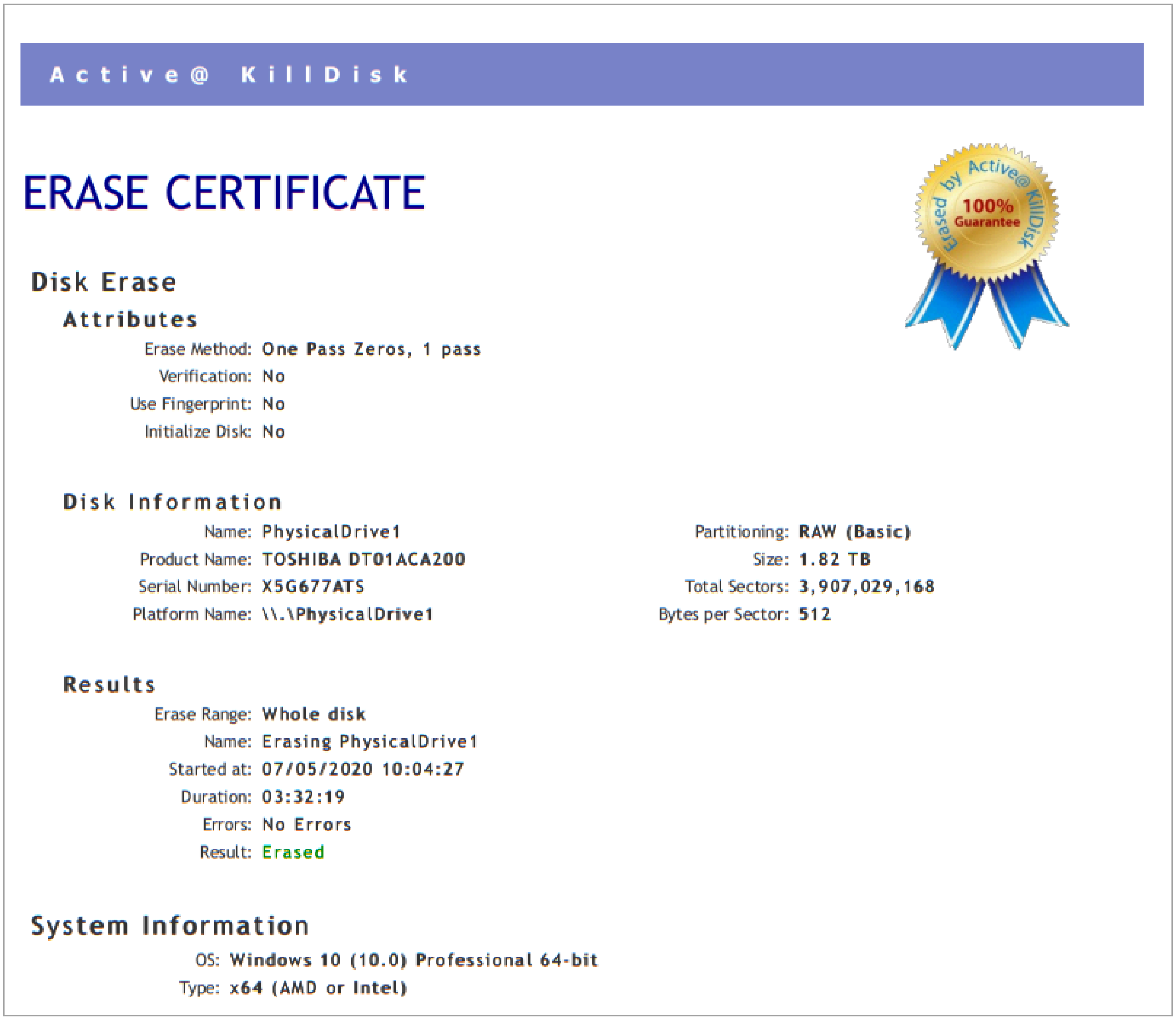
For most modern computers and disks (manufactured last years) *SATA III* standard is supported, so erase speed is limited by HDD throughput (disk write speed) only.

Our tests give the results: **10 GB per minute (in average) per pass** with decent computer configuration and disks with age of up to 5 years old.

For example, 2 TB *Toshiba* disk has been erased on Windows platform with one pass within 3 hours and 32 minutes, 14 TB *Western Digital* disk - within 18 hours 53 minutes.

The following snapshots are real-test certificates for erasing of:

1) **2 TB** *Toshiba* (manufactured in 2015) *SATA III* (6 GBps) 7200 rpm disk with One Pass Zeros and US DoD 5220.22-M (3 passes + verification) showing the average speed of **9** GB/min per pass



Erased by Active@ KillDisk
100%
Guarantee

Active@ KillDisk

ERASE CERTIFICATE

Disk Erase

Attributes

Erase Method:	One Pass Zeros, 1 pass
Verification:	No
Use Fingerprint:	No
Initialize Disk:	No

Disk Information

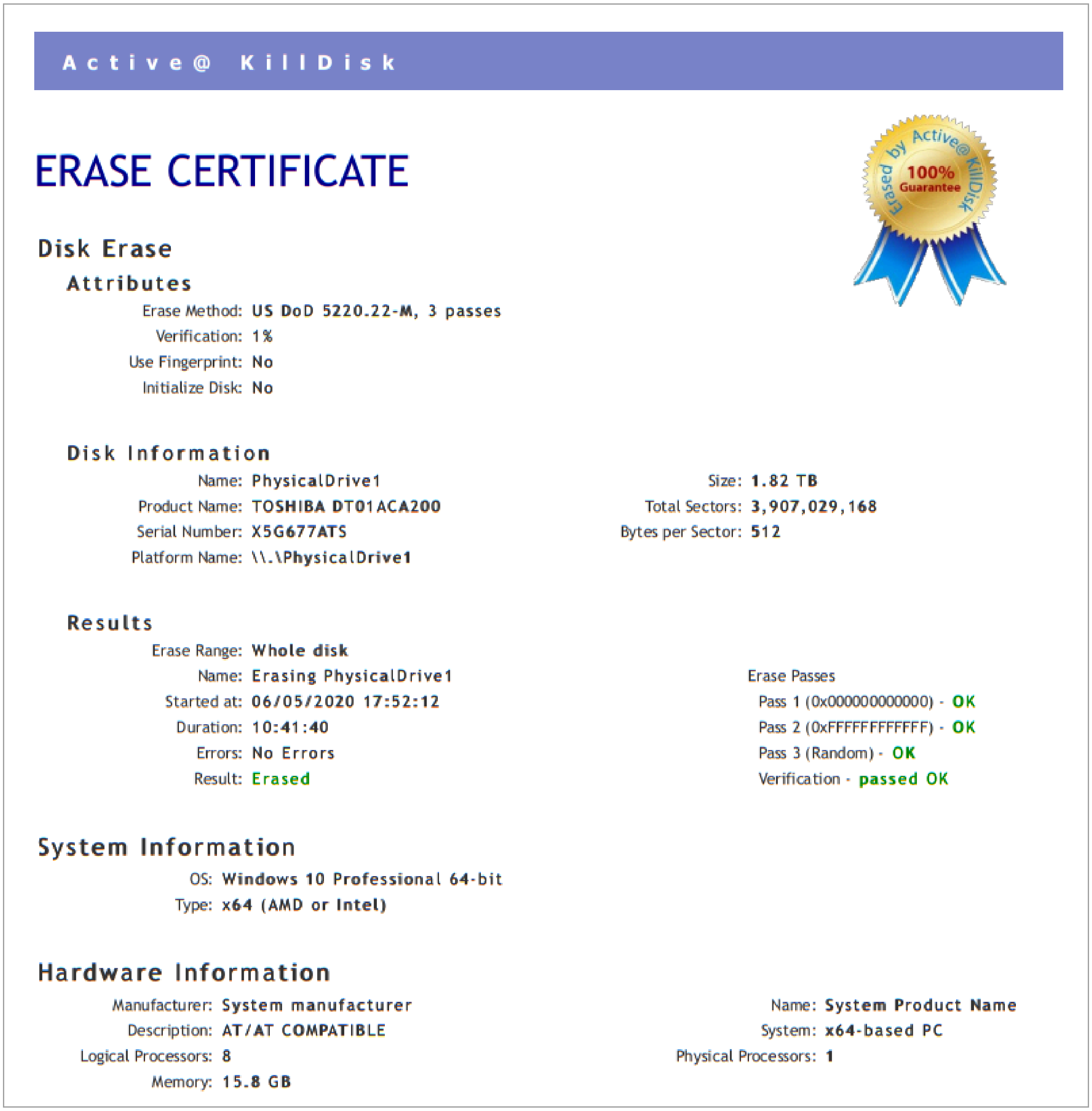
Name:	PhysicalDrive1	Partitioning:	RAW (Basic)
Product Name:	TOSHIBA DT01ACA200	Size:	1.82 TB
Serial Number:	X5G677ATS	Total Sectors:	3,907,029,168
Platform Name:	\\.\PhysicalDrive1	Bytes per Sector:	512

Results

Erase Range:	Whole disk
Name:	Erasing PhysicalDrive1
Started at:	07/05/2020 10:04:27
Duration:	03:32:19
Errors:	No Errors
Result:	Erased

System Information

OS:	Windows 10 (10.0) Professional 64-bit
Type:	x64 (AMD or Intel)


Erased by Active@ KillDisk
100%
Guarantee

Active@ KillDisk

ERASE CERTIFICATE

Disk Erase

Attributes

Erase Method: US DoD 5220.22-M, 3 passes
Verification: 1%
Use Fingerprint: No
Initialize Disk: No

Disk Information

Name: PhysicalDrive1
Product Name: TOSHIBA DT01ACA200
Serial Number: X5G677ATS
Platform Name: \\.\PhysicalDrive1

Size: 1.82 TB
Total Sectors: 3,907,029,168
Bytes per Sector: 512

Results

Erase Range: Whole disk
Name: Erasing PhysicalDrive1
Started at: 06/05/2020 17:52:12
Duration: 10:41:40
Errors: No Errors
Result: Erased

Erase Passes
Pass 1 (0x000000000000) - OK
Pass 2 (0xFFFFFFFFFFFF) - OK
Pass 3 (Random) - OK
Verification - passed OK

System Information

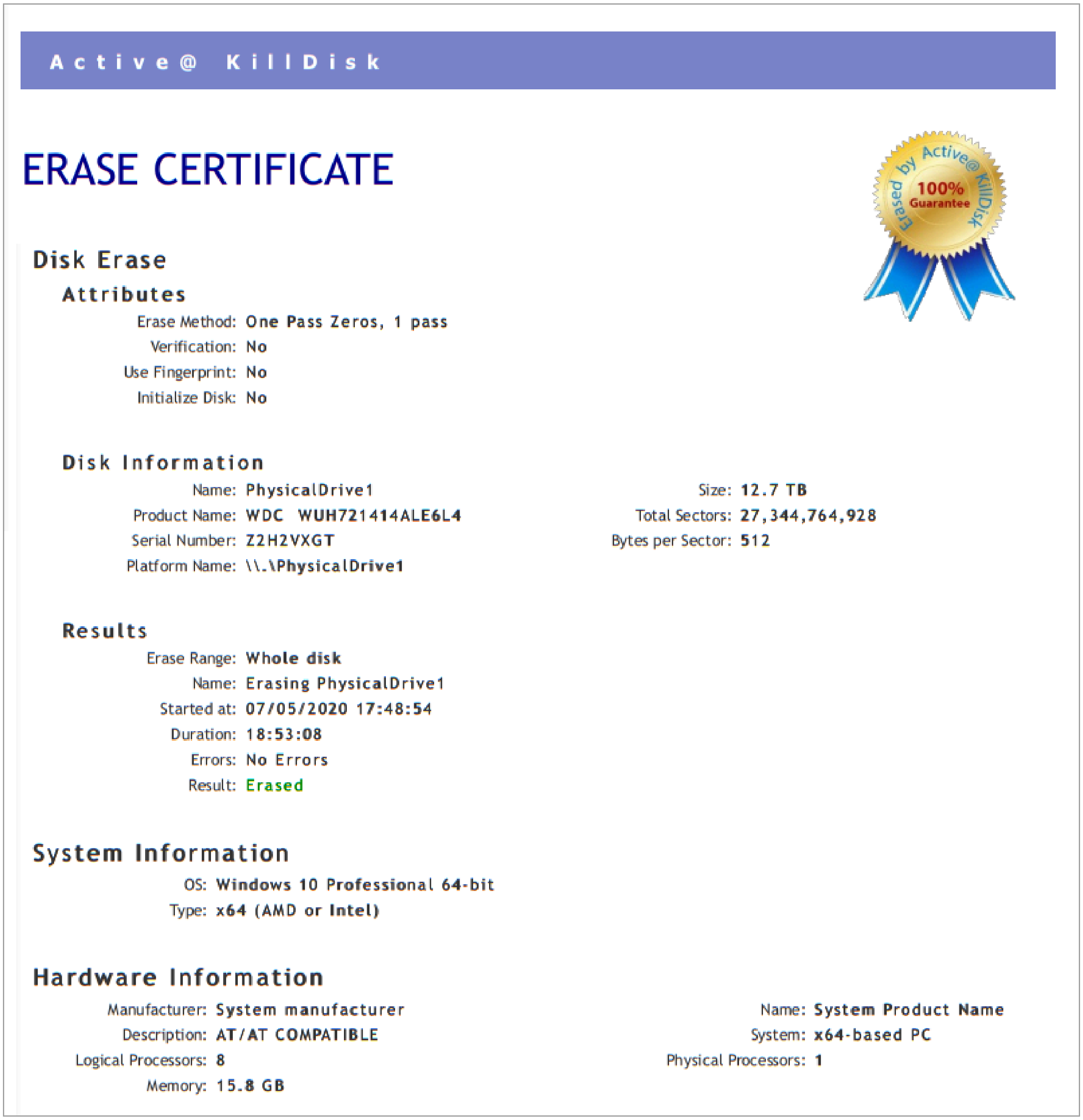
OS: Windows 10 Professional 64-bit
Type: x64 (AMD or Intel)

Hardware Information

Manufacturer: System manufacturer
Description: AT/AT COMPATIBLE
Logical Processors: 8
Memory: 15.8 GB

Name: System Product Name
System: x64-based PC
Physical Processors: 1

2) **14 TB** *Western Digital* (manufactured in 2019) SATA III (6 Gbps) 7200 rpm disk with One Pass Zeros and US DoD 5220.22-M (3 passes + 10% verification) showing the average speed of **12** GB/min per pass



Active@ KillDisk

ERASE CERTIFICATE

Erased by Active@ KillDisk
100%
Guarantee

Disk Erase

Attributes

Erase Method: One Pass Zeros, 1 pass

Verification: No

Use Fingerprint: No

Initialize Disk: No

Disk Information

Name: PhysicalDrive1

Product Name: WDC WUH721414ALE6L4

Serial Number: Z2H2VXGT

Platform Name: \\.\PhysicalDrive1

Size: 12.7 TB

Total Sectors: 27,344,764,928

Bytes per Sector: 512

Results

Erase Range: Whole disk

Name: Erasing PhysicalDrive1

Started at: 07/05/2020 17:48:54

Duration: 18:53:08

Errors: No Errors

Result: Erased

System Information

OS: Windows 10 Professional 64-bit

Type: x64 (AMD or Intel)

Hardware Information

Manufacturer: System manufacturer

Description: AT/AT COMPATIBLE

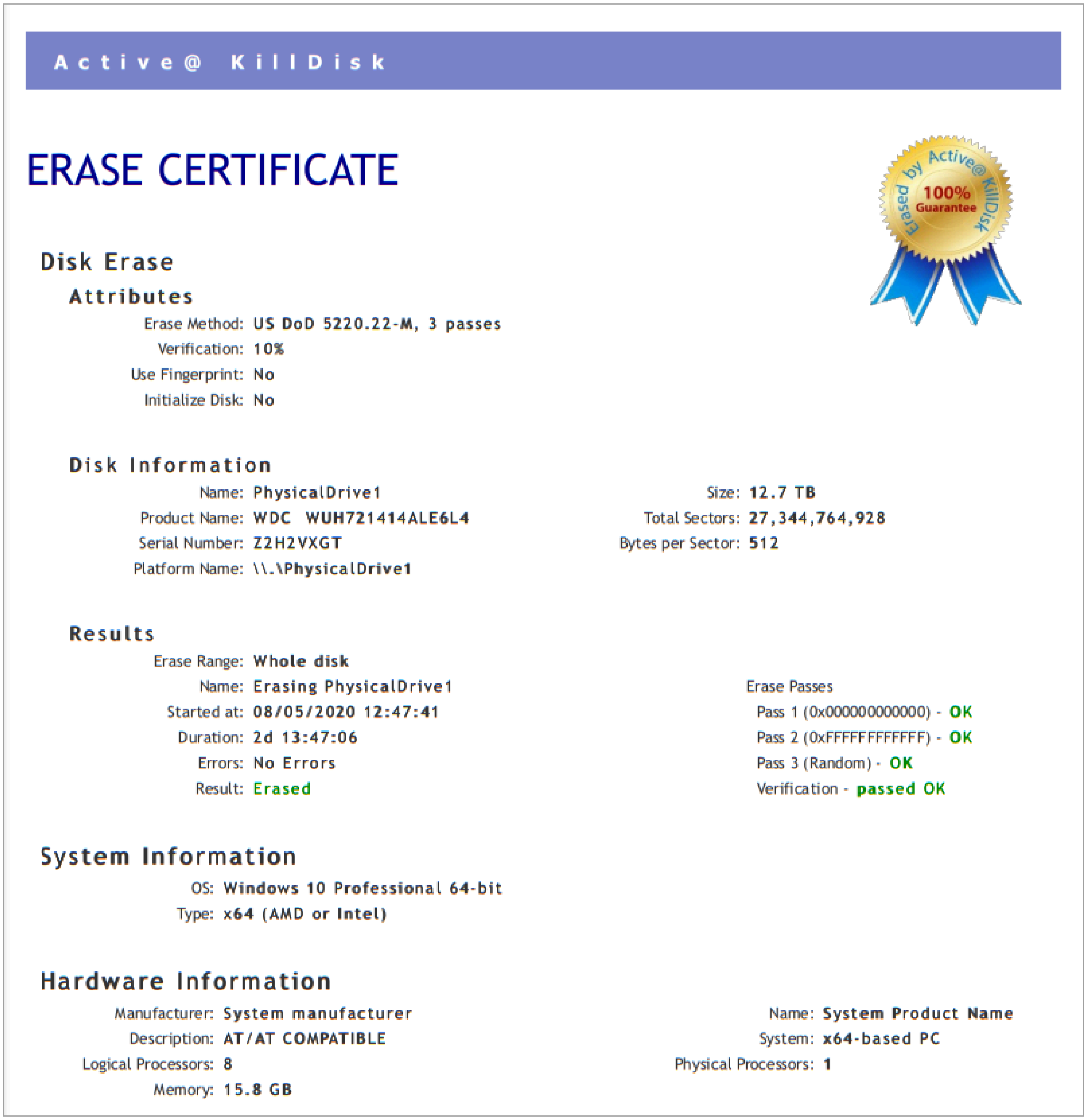
Logical Processors: 8

Memory: 15.8 GB

Name: System Product Name

System: x64-based PC

Physical Processors: 1



Active@ KillDisk

ERASE CERTIFICATE

Erased by Active@ KillDisk
100%
Guarantee

Disk Erase

Attributes

Erase Method: US DoD 5220.22-M, 3 passes
Verification: 10%
Use Fingerprint: No
Initialize Disk: No

Disk Information

Name: PhysicalDrive1
Product Name: WDC WUH721414ALE6L4
Serial Number: Z2H2VXGT
Platform Name: \\.\PhysicalDrive1

Size: 12.7 TB
Total Sectors: 27,344,764,928
Bytes per Sector: 512

Results

Erase Range: Whole disk
Name: Erasing PhysicalDrive1
Started at: 08/05/2020 12:47:41
Duration: 2d 13:47:06
Errors: No Errors
Result: Erased

Erase Passes
Pass 1 (0x000000000000) - OK
Pass 2 (0xFFFFFFFFFFFF) - OK
Pass 3 (Random) - OK
Verification - passed OK

System Information

OS: Windows 10 Professional 64-bit
Type: x64 (AMD or Intel)

Hardware Information

Manufacturer: System manufacturer
Description: AT/AT COMPATIBLE
Logical Processors: 8
Memory: 15.8 GB

Name: System Product Name
System: x64-based PC
Physical Processors: 1

Erase Disk Concepts

Erasing Confidential Data

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

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

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

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

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

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

! **Important:**

Formatting a disk removes all information from the disk.

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

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

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

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

Using **KillDisk** all data on your hard drive or removable device can be destroyed without the possibility of future recovery. After using **KillDisk** the process of 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 20 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 professional security application that destroys data permanently on any computer that can be started using a bootable CD/DVD/BD or USB Flash Disk. Access to the drive's data is made on the physical level via the BIOS (Basic Input-Output System) bypassing the operating system’s logical drive structure organization. Regardless of the operating system, file systems, or type of machine, this utility can destroy all the data on all storage devices. It does not matter which operating systems or file systems are located on the machine.

Secure Erase Concepts

Secure Erase for SSD is used to permanently delete data from the media and to restore the drive’s speed if it starts to drop to noticeably lower performance than stated (at the same time, we don’t consider *SLC-caching* and other "official" reasons for speed reduction since it’s hardware drive features).

The essence of the problem that *Secure Erase* can solve: drive began to work slowly (writing and reading data). There can be a lot of reasons, some of them are related to the hardware component and some to the software component. SSDs are very different in service from classic HDDs, therefore, simply deleting data or formatting the drive does not really mean resetting the cell - you need to clear it before recording, which slows down the process of recording new data. In theory, there shouldn’t be such problems, because *TRIM* exists - a command to clear the data marked for deletion in cells. This command only works with *2.5″* and *M.2 SATA* drives. For drives connected to the *PCIe* bus (M.2 or PCIe on the motherboard) there is an analogue - *Deallocate*. But it happens that these functions are disabled for some reason - an OS error, a user error in setting up a disk through third-party software, or the use of non-standard OS assemblies with unknown software components. So, the disk starts to work noticeably slower and it is quite noticeable without any benchmark performance measurements.

SSDs use a number of mapping layers that hide the physical layout of the flash-based memory, as well as help in managing how flash memory data integrity and lifetime are managed. Collectively, these layers are referred to as the *Flash Translation Layer* (FTL).

SSDs are also over-provisioned: they contain a bit more flash memory than what they’re rated for. This extra memory is used internally by the *FTL* as empty data blocks, used when data needs to be rewritten, and as out-of-band sections for use in the logical to physical mapping.

The mapping layers, and how the flash controller manages memory allocation, pretty much ensure that either erasing or performing a conventional hard drive type of secure erase won’t ensure all data is overwritten, or even erased at all.

One example of how data gets left behind intact is due to how data is managed in an SSD. When you edit a document and save the changes, the saved changes don’t overwrite the original data (an in-place update). Instead, SSDs write the new content to an empty data block and then update the logical to physical map to point to the new location. This leaves the space the original data occupied on the SSD marked as free, but the actual data is left intact. In time, the data marked as free will be reclaimed by the SSD’s garbage collection system, but until then, the data could be recovered.

A conventional *Secure Erase*, as used with hard drives, is unable to access all of the SSD’s memory location, due to the *FTL* and how an SSD actually writes data, which could lead to intact data being left behind.

SSD manufacturers understand the need for an easy way to sanitize an SSD, and most have implemented the ATA command, *Secure Erase Unit* (used with SATA-based SSDs), or the *NVMe* command, *Format NVM* (used with PCIe-based SSDs) as a fast and effective method of securely erasing an SSD.

So, SSD drives have a non-trivial system of work, therefore, the scheme for the complete destruction of data should also not be the easiest. But in reality, this is not so at all. Any SSD has a controller that is the "brain" of the drive. He not only tells the system where to write data, but also encrypts the information passing through it and stores the key with himself. If you remove (or rather replace) a given key, then all the information will turn into a random set of 1 and 0 - it will be impossible to decrypt it in any way. Just one simple action by the user can solve the problem of safe data erasure. This method is the fastest and most effective.

Note:

To protect information that is critical, both for serious organizations that are concerned about the safety of data and for public sector enterprises working with information classified as state secrets, information systems should usually use certified sanitation algorithms (US DoD 5220.22-M, Canadian OPS-II, NSA 130-2 etc.).

If you combine these two methods (replacing the key and resetting the cells), you get the perfect algorithm for obtaining a completely sterile disk in the state of its maximum performance. This, firstly, solves the problem that we raised at the very beginning, and, secondly, it can help us answer the question about the degree of drive wear.

It is important to note that some drives with built-in encryption can receive only one algorithm upon receipt of a safe erase command - it depends on the controller settings by the manufacturer. If you "reset" your SSD and compare the actual performance with the declared one, you will get the answer to this question. This procedure does not affect disk wear (which is very important). Note that these actions are designed specifically for analyzing the state of the disk, but it will not be possible to achieve a long-term increase in the read/write speed due to the peculiarities of the operation of SSD disks - the situation may depend on both the drive model and the controller firmware. And it must be noted that not all drives support encryption. In this case, the controller simply resets the cells.

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.

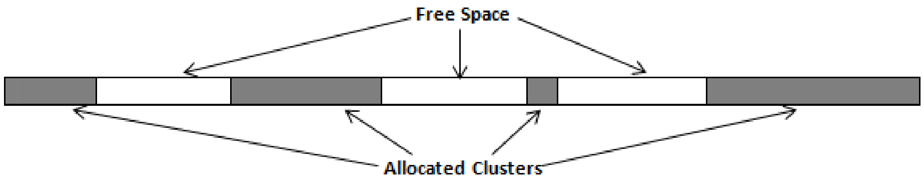


Figure 103: Disk free space and allocated clusters

Wiping File Slack Space

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

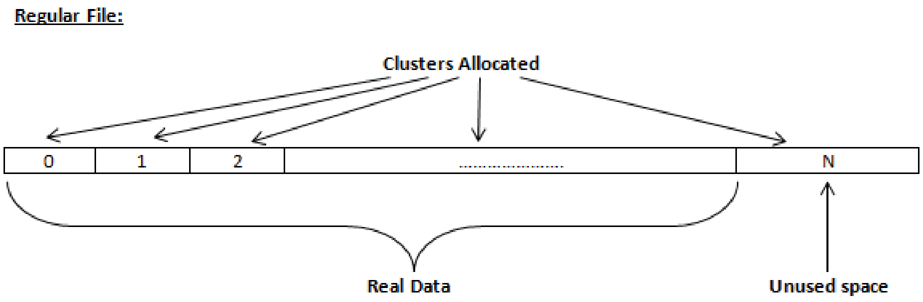


Figure 104: Disk free space and allocated clusters

Specifics of Wiping Microsoft NTFS File System

NTFS Compressed Files

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

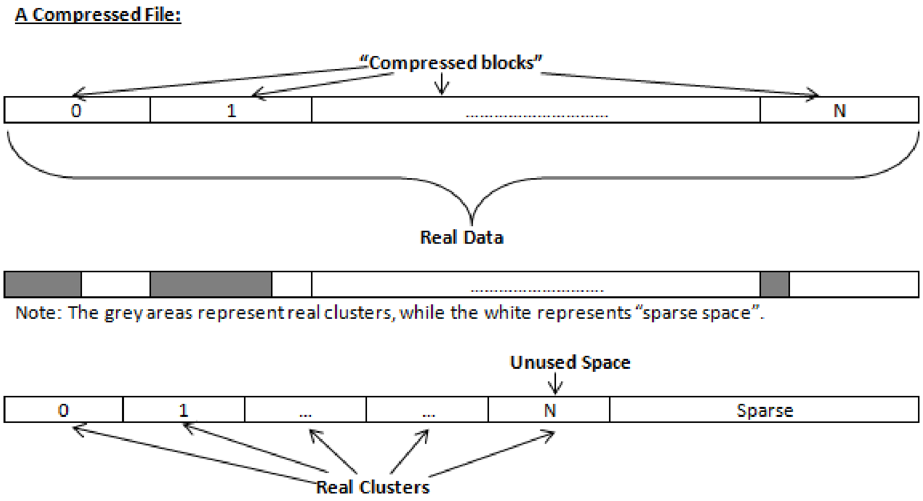


Figure 105: Compressed file structure

The MFT (Master File Table) Area

Wiping the system information:

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

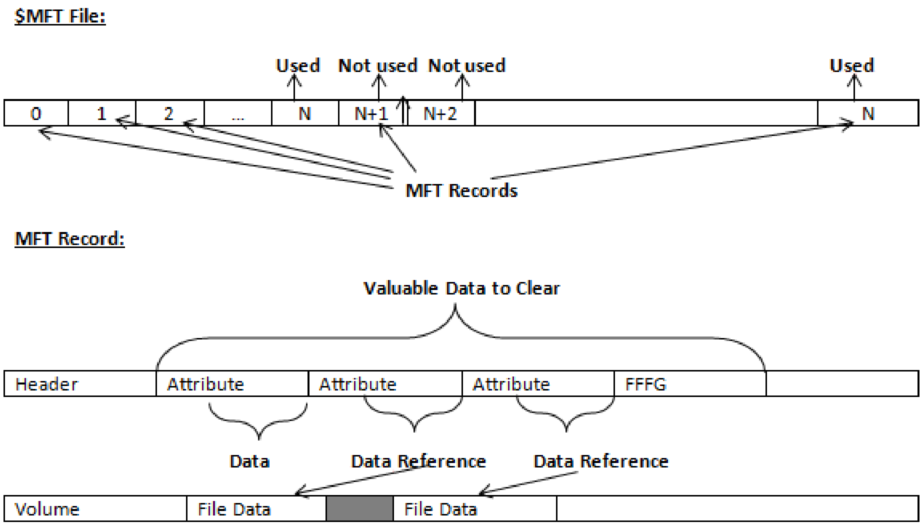


Figure 106: MFT structure

Specifics of Wiping Microsoft FAT File System

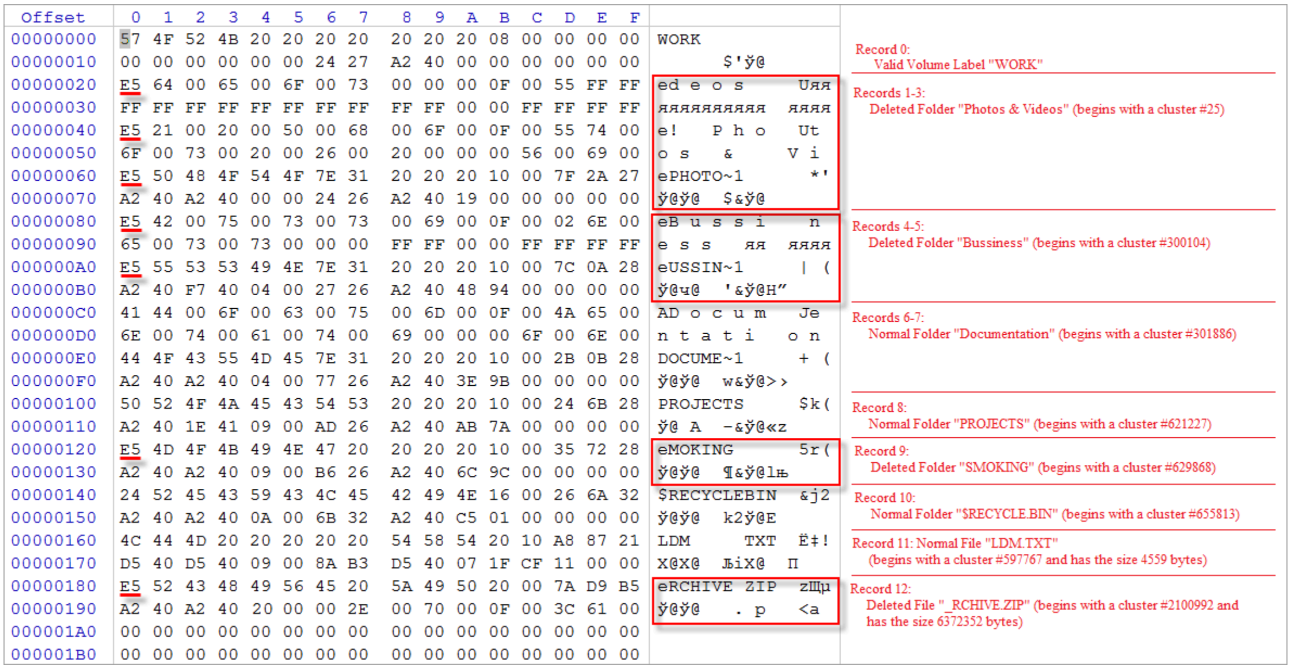
Wiping Directory Areas

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

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

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

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



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

Record 0:
Valid Volume Label "WORK"

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

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

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

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

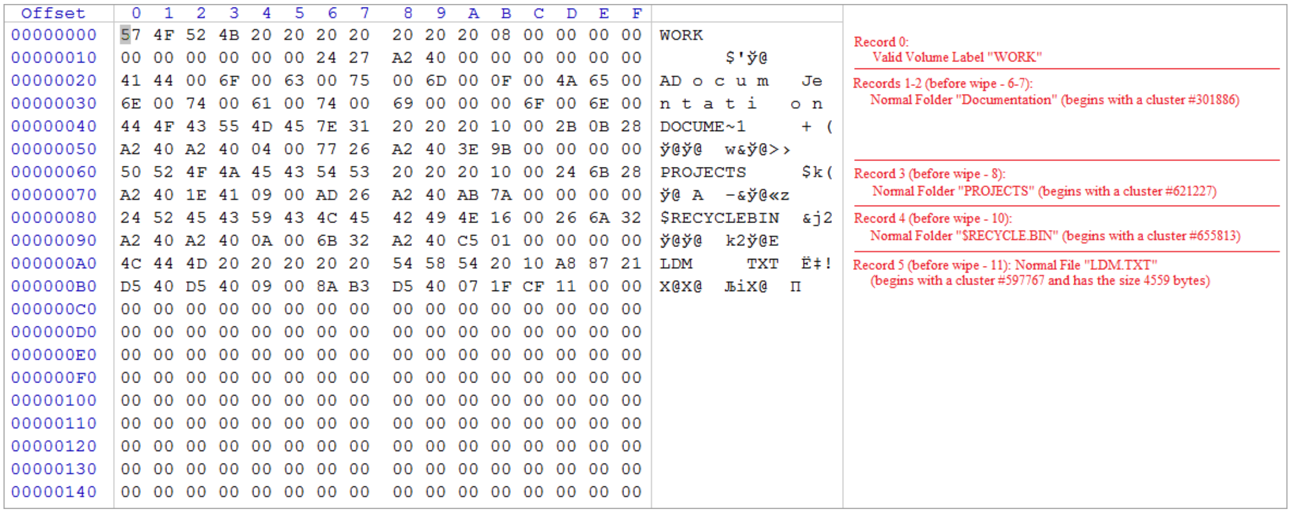
Record 9:
Deleted Folder "SMOKING" (begins with a cluster #629868)

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

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

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

Figure 107: This is how Directory Area looks before Wiping, red rectangles display deleted records



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

Record 0:
Valid Volume Label "WORK"

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

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

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

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

Figure 108: 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.

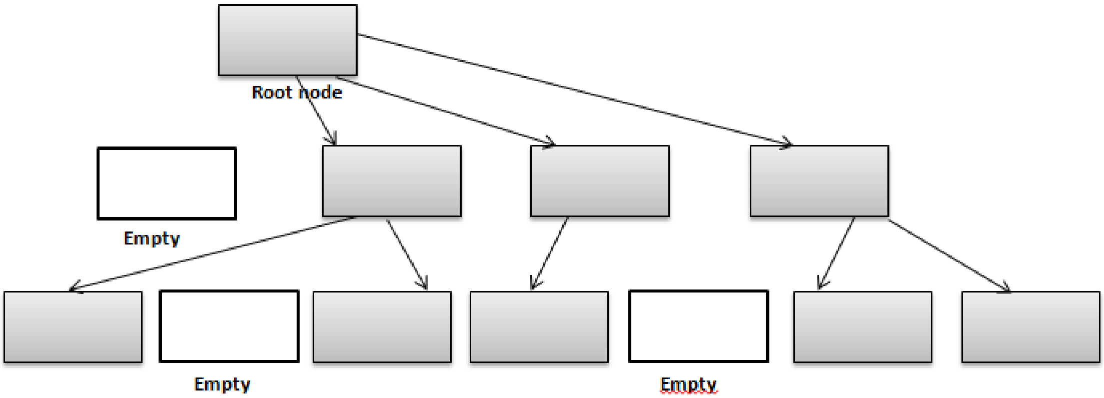
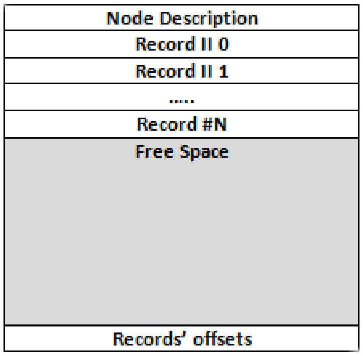


Figure 109: B-tree structure

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



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

Figure 110: HFS+ system table

Specifics of Wiping Linux Ext2/Ext3/Ext4 File Systems

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

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

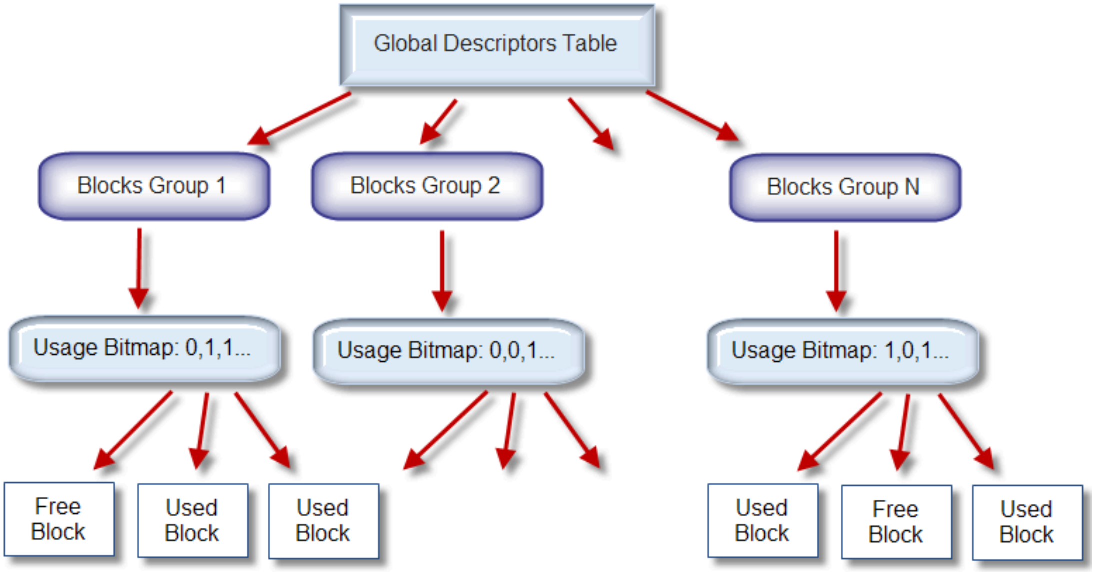


Figure 111: Ext2/Ext3/Ext4 descriptors table

Erase Methods (Sanitation Standards)

One Pass Zeros or One Pass Random

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

US DoD 5220.22-M

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

Canadian CSEC ITSG-06

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

Canadian OPS-II

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

British HMG IS5 Baseline

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

British HMG IS5 Enhanced

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

Russian GOST p50739-95

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

US Army AR380-19

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

US Air Force 5020

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

NAVSO P-5329-26 RL

RL method - the write head passes over each sector three times (*0x01, 0x27FFFFFF, Random*). There is one final pass to verify random characters by reading

NCSC-TG-025

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

NSA 130-2

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

NIST 800-88

Supported three NIST 800-88 media sanitation standards:

- 1. The write head passes over each sector one time (*0x00*).
- 2. The write head passes over each sector one time (*Random*).
- 3. The write head passes over each sector three times (*0x00, 0xFF, Random*).

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

German VSITR

The write head passes over each sector seven times

Bruce Schneier

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

Peter Gutmann

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

Australian ISM-6.2.93

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

Secure Erase (ANSI ATA, SE)

According to *National Institute of Standards and Technology* (NIST) Special Publication 800-88: Guidelines for Media Sanitation, *Secure Erase* is "*An overwrite technology using firmware based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure.*" The guidelines also state that "*degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.*" *ATA Secure Erase (SE)* is designed for SSD controllers. The SSD controller resets all memory cells making them empty. In fact, this method restores the SSD to the factory state, not only deleting data but also returning the original performance. When implemented correctly, this standard processes all memory, including service areas and protected sectors

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

Name Tags

General

{Computer ID}
Workstation (computer) ID
{OS}
Operating System name
{AppName}
Application name
{AppVersion}
Application full version
{KernelVersion}
Kernel version
{UniqueID}
Generated unique 8 symbols ID

Date & Time

Tags to represent current date in different formats:

{Date(YYYYMMDD)}
Complete date in full form without delimiters
{Date(YYYY-MM-DD)}
Complete date in full form with delimiters
{Date(YYMMDD)}
Complete date in short form without delimiters
{Date(YYYY)}
Year in full form
{Date(YY)}
Year in short form
{Date(Month)}
Full month name as literal
{Date(MM)}
Month as digital with leading zero
{Date(DD)}
Day of month with leading zero
{Time(HHmmss)}
Time with hours, minutes and seconds without delimiters
{Time(HH-mm-ss)}
Time with hours, minutes and seconds with delimiters
{Time(HH)}
Hours with leading zero
{Time(mm)}
Minutes with leading zero
{Time(ss)}
Seconds with leading zero

Disk

Values for these name tags retrieved from context device:

{Serial ID}
Disk serial number, retrieved from OS or from S.M.A.R.T. 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:

{ExamGrade}
Disk examination result grade
{BatchName}
Batch name (if a part of a batch processing)
{DiskCount}
Quantity of disk processed in batch
{DiskBayID}
Disk Bay label
{Method}
Erase method
{Passes}
Erases passes description
{Verified}
Verification attribute
{DateStarted}
Process start date
{TimeStarted}
Process start time
{TimeElapsed}
Process elapsed time
{Status}
Overall completion status for group processing or separate disk processing status.
{StatusCode}
Overall process result digital code

Item processing attributes

Item processing attributes based on execution conditions:

{Sequence #} ... {Sequence 000#}
Sequential number. Used for group (batch) processing.
{ProcessType}
Process type name
{ProcessedAs}
Process short name
{Range}
Processed disk range

Disk Hidden Zones (HPA/DCO)

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

HPA - Host protected area

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

How it works:

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

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

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

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

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

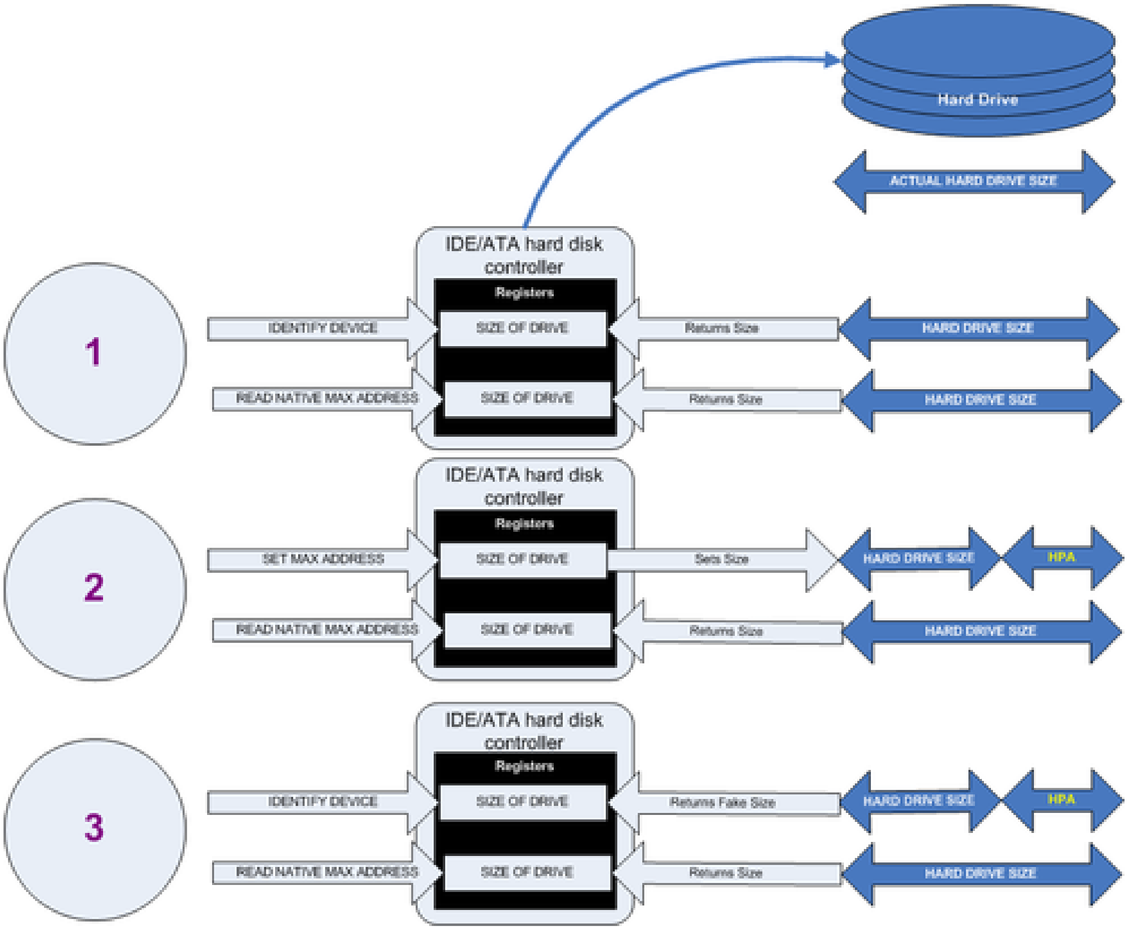


Figure 112: Creation of an HPA

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

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

Usage:

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

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

DCO - Device Configuration Overlay

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

Usage:

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