

Active@ KillDisk
User Guide

Copyright © 1999-2014, LSOFT TECHNOLOGIES INC. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from LSOFT TECHNOLOGIES INC.

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

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

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

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

The 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.

Contents

1. Product Overview.....	4
1.1 Erasing Confidential Data.....	4
1.2 Wiping Confidential Data from Unoccupied Disk's Space	6
2 System Requirements	12
2.1 Active@ KillDisk Version	12
3 Running Active@ KillDisk	16
3.1 Active@ Boot Disk Creator.....	17
3.2 Interactive, Command Line and Batch Modes.....	19
3.3 Application settings (KILLDISK.INI file).....	32
3.4 Erase or Wipe Logical Drives (Partitions)	36
3.5 Completed Erase or Wipe Operation Information.....	38
4 Common Questions.....	40
5 Erase/Wipe Parameters and Application Settings.....	43
6 Glossary of Terms.....	51

1 Product Overview

Active@ KillDisk is a powerful utility that will:

- Wipe confidential data from unused space on your hard drive.
- Erase data from partitions or from an entire hard disk.
- Destroy data permanently.

Wiping the logical drive's deleted data does not delete existing files and folders. It processes all unoccupied drive space so that data recovery of previously deleted files becomes impossible. Installed applications and existing data are not touched by this process. Active@ KillDisk wipes unused data residue from file slack space, unused sectors, and unused space in system records or directory records.

When you erase data with Active@ KillDisk, you destroy data permanently by conforming to any one of more than twenty international data sanitizing standards or using your own custom settings.

Wiping drive space or erasing data can take a long time, so perform these operations when the system is not being otherwise utilized. For example, these operations may be run overnight. If you have several physical hard disk drives attached to the machine, KillDisk can erase or wipe them simultaneously (in multi-threaded mode), thus saving you time and work costs.

After erase or wipe actions are completed, KillDisk offers you the options of initializing erased disks, shutting down your computer, saving a log file and the certificate (XML or PDF), and even sending log files via e-mail to your mailbox. Custom erase or wipe certificates can be created using your company logo and attributes.

KillDisk supports command line parameters (what to erase, which method to use, etc...) and executable exit codes. Application can be run in batch mode, which is fully automated and requires no user interaction.

1.1 Erasing Confidential Data

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

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

Windows DELETE command merely changes the file name so that the operating system will not look for the file. The situation with NTFS is similar.

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

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

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

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

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

1.1.1 Advanced Data Recovery Systems

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

Although there are very sophisticated data recovery systems available at a high price, data can easily be restored with the help of an off-the-shelf data recovery utility like [Active@ File Recovery](#), making your erased confidential data quite accessible.

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

1.1.2 International Standards in Data Removal

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

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

1.2 Wiping Confidential Data from Unoccupied Disk's Space

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

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

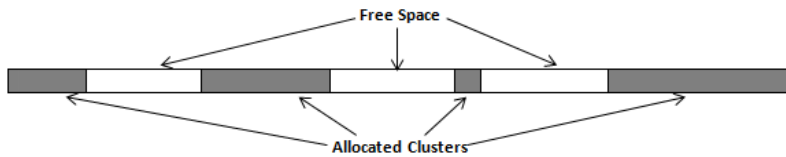
When you wipe unoccupied drive space, the process is run from the bootable CD/DVD operating system. As a result, the wipe or erase process uses an operating system that is outside the local hard drive and is not impeded by Windows system caching. This means that deleted Windows system records can be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

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

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

1.2.1 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 extra steps to ensure secure deletion.



1.2.2 Specifics of Wiping for Different File Systems

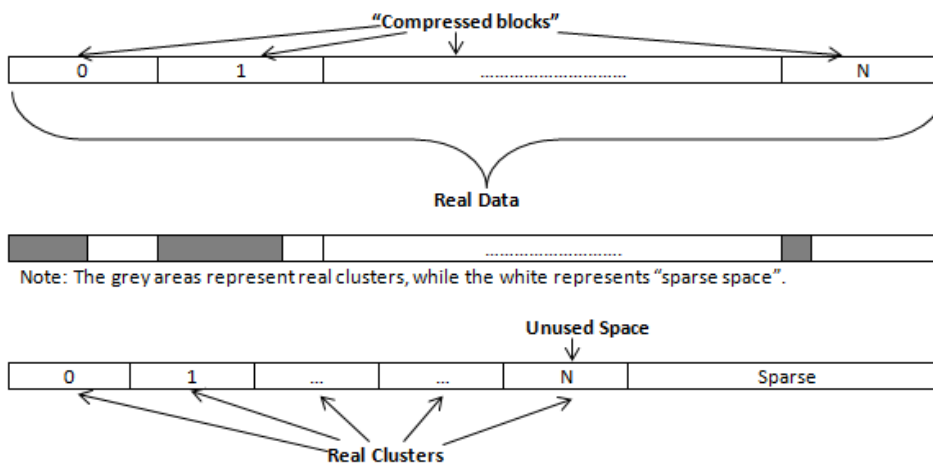
1.2.2.1 NTFS File System

NTFS Compressed Files

Wiping free space inside a file:

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

A Compressed File:

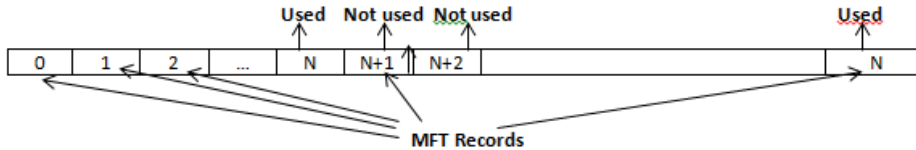


The MFT (Master File Table) Area

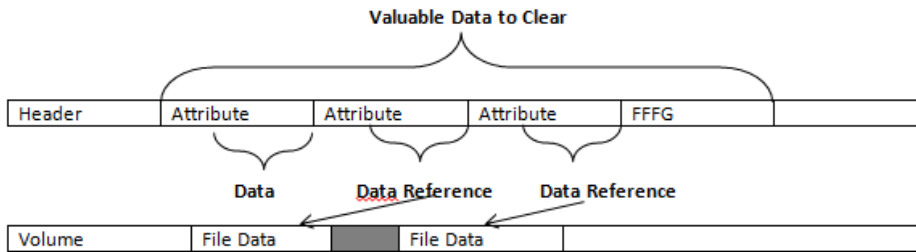
Wiping the system information:

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.

\$MFT File:



MFT Record:



1.2.2.2 FAT/FAT32/exFAT 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 an item is 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.

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	57	4F	52	4B	20	20	20	20	20	20	08	00	00	00	00	00	WORK	Record 0: Valid Volume Label "WORK"
00000010	00	00	00	00	00	00	24	27	A2	40	00	00	00	00	00	00	\$'ÿ@	Records 1-3: Deleted Folder "Photos & Videos" (begins with a cluster #25)
00000020	E5	64	00	65	00	6F	00	73	00	00	00	0F	00	55	FF	FF	ed e o s Уяя	
00000030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	яяяяяяяяя 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	ÿ@ÿ@ \$&ÿ@	
00000080	E5	42	00	75	00	73	00	73	00	69	00	0F	00	02	6E	00	eB u s s i n	Records 4-5: Deleted Folder "Bussiness" (begins with a cluster #300104)
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	ÿ@ç@ ' &ÿ@H"	
000000C0	41	44	00	6F	00	63	00	75	00	6D	00	0F	00	4A	65	00	AD o c u m Je	Records 6-7: Normal Folder "Documentation" (begins with a cluster #301886)
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	ÿ@ÿ@ w&ÿ@>>	
00000100	50	52	4F	4A	45	43	54	53	20	20	20	10	00	24	6B	28	PROJECTS \$k(Record 8: Normal Folder "PROJECTS" (begins with a cluster #621227)
00000110	A2	40	1E	41	09	00	AD	26	A2	40	AB	7A	00	00	00	00	ÿ@ A -&ÿ@«z	
00000120	E5	4D	4F	4B	49	4E	47	20	20	20	20	10	00	35	72	28	eMOKING 5r(Record 9: Deleted Folder "SMOKING" (begins with a cluster #629868)
00000130	A2	40	A2	40	09	00	B6	26	A2	40	6C	9C	00	00	00	00	ÿ@ÿ@ ¶&ÿ@L#	
00000140	24	52	45	43	59	43	4C	45	42	49	4E	16	00	26	6A	32	\$RECYCLEBIN &j2	Record 10: Normal Folder "RECYCLE.BIN" (begins with a cluster #655813)
00000150	A2	40	A2	40	0A	00	6B	32	A2	40	C5	01	00	00	00	00	ÿ@ÿ@ k2ÿ@E	
00000160	4C	44	4D	20	20	20	20	20	54	58	54	20	10	A8	87	21	LDM TXT È#!	Record 11: Normal File "LDM.TXT" (begins with a cluster #597767 and has the size 4559 bytes)
00000170	D5	40	D5	40	09	00	8A	B3	D5	40	07	1F	CF	11	00	00	X@X@ Ìix@ П	
00000180	E5	52	43	48	49	56	45	20	5A	49	50	20	00	7A	D9	B5	eRCHIVE ZIP злп	Record 12: Deleted File "_RCHIVE.ZIP" (begins with a cluster #2100992 and has the size 6372352 bytes)
00000190	A2	40	A2	40	20	00	00	2E	00	70	00	0F	00	3C	61	00	ÿ@ÿ@ . 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		

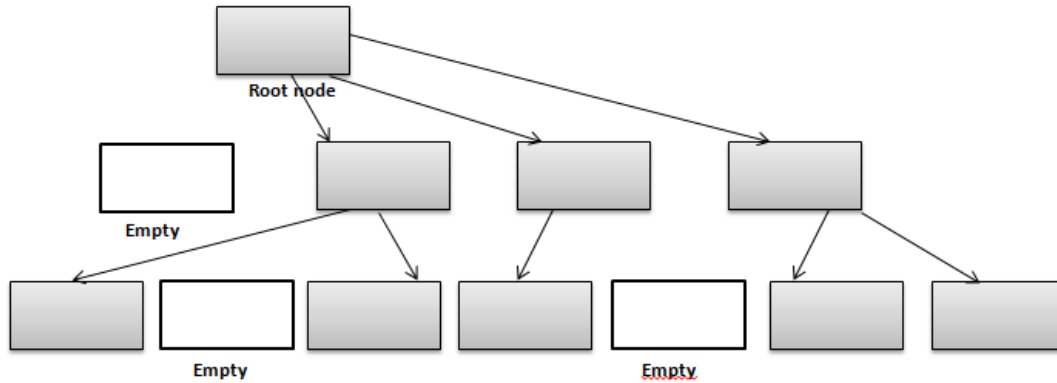
This is how Directory Area looks after Wiping: all deleted records removed, root defragmented:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	57	4F	52	4B	20	20	20	20	20	20	08	00	00	00	00	00	WORK	Record 0: Valid Volume Label "WORK"
00000010	00	00	00	00	00	00	24	27	A2	40	00	00	00	00	00	00	\$'ÿ@	Records 1-2 (before wipe - 6-7): Normal Folder "Documentation" (begins with a cluster #301886)
00000020	41	44	00	6F	00	63	00	75	00	6D	00	0F	00	4A	65	00	AD o c u m Je	
00000030	6E	00	74	00	61	00	74	00	69	00	00	00	6F	00	6E	00	n t a t i o n	
00000040	44	4F	43	55	4D	45	7E	31	20	20	20	10	00	2B	0B	28	DOCUME~1 + (
00000050	A2	40	A2	40	04	00	77	26	A2	40	3E	9B	00	00	00	00	ÿ@ÿ@ w&ÿ@>>	
00000060	50	52	4F	4A	45	43	54	53	20	20	20	10	00	24	6B	28	PROJECTS \$k(Record 3 (before wipe - 8): Normal Folder "PROJECTS" (begins with a cluster #621227)
00000070	A2	40	1E	41	09	00	AD	26	A2	40	AB	7A	00	00	00	00	ÿ@ A -&ÿ@«z	
00000080	24	52	45	43	59	43	4C	45	42	49	4E	16	00	26	6A	32	\$RECYCLEBIN &j2	Record 4 (before wipe - 10): Normal Folder "RECYCLE.BIN" (begins with a cluster #655813)
00000090	A2	40	A2	40	0A	00	6B	32	A2	40	C5	01	00	00	00	00	ÿ@ÿ@ k2ÿ@E	
000000A0	4C	44	4D	20	20	20	20	20	54	58	54	20	10	A8	87	21	LDM TXT È#!	Record 5 (before wipe - 11): Normal File "LDM.TXT" (begins with a cluster #597767 and has the size 4559 bytes)
000000B0	D5	40	D5	40	09	00	8A	B3	D5	40	07	1F	CF	11	00	00	X@X@ Ìix@ 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		

1.2.2.3 Wipe HFS+

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.

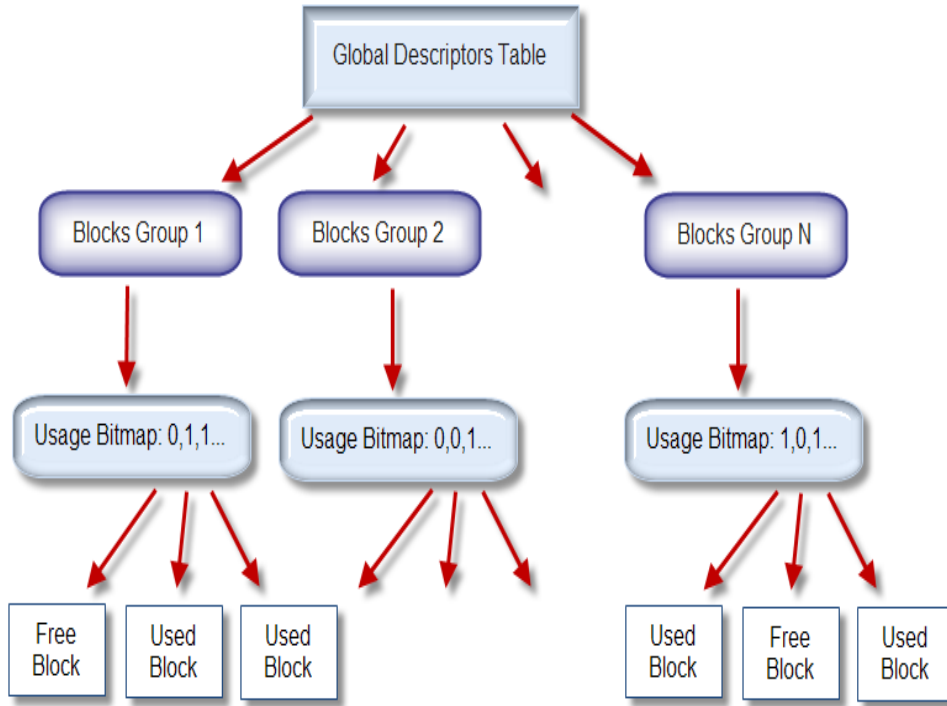


In the event of the deletion of a file or folder, there is a possibility of recovering the metadata of the file (such as its name and attributes), as well as the actual data that the file consists of. KillDisk's Wipe method clears out all of this free space in the system files.

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

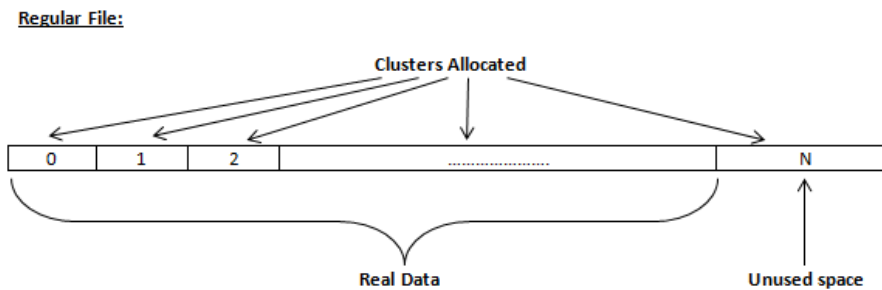
1.2.2.4 Wiping Ext2fs/Ext3fs/Ext4fs

A Linux ExtFs (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; sizes 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.



1.2.3 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 of more or less than 4KB and thus have slack space at their end.



2 System Requirements

This chapter outlines the minimum requirements for PCs using Active@ KillDisk.

Personal Computer

IBM PC compatible machine

Intel Pentium or higher

512 Mb of RAM (Windows version)

1 Gb of RAM (Linux GUI version) Video: VGA resolution (800 x 600) or better

Operating System:

- Windows XP or higher (Windows version)
- Linux Kernel 2.x or high (Linux version)

Drive Storage System

CD/DVD-ROM or Blu-Ray optical drive

USB 2.0 or USB 3.0 storage device (USB flash disk or external USB disk)

Removable media (memory stick, SD card, compact flash, floppy disk)

Hard Disk Drive types: IDE, ATA, SSD, SATA, eSATA or SCSI with controllers. Additional drivers can be loaded for RAIDs or non-standard controllers after the system is booted up.

Other Requirements

A blank CD/DVD/BD disc for burning an ISO image, or a USB flash card to prepare a bootable USB disk.

2.1 Active@ KillDisk Version

The performance of Active@ KillDisk depends on the version of the application as displayed in the table below.

Table 2-1 Differences between Freeware and Professional Versions

Feature	Freeware Version	Professional Version
Securely overwrites and destroys all data on	yes	yes

Feature	Freeware Version	Professional Version
physical drive or logical partition		
Erases partitions, volumes and unused disk space	yes	yes
Supports IDE / ATA / SATA / eSATA / SSD / SCSI hard disk drives, LUN / RAID Disk Arrays	yes	yes
Supports parallel erasing/wiping: two or more HDDs can be cleaned up simultaneously	yes	yes
Supports fixed disks, floppies, zip drives, USB Flash Cards and USB/USB3 external devices	yes	yes
Supports large-sized drives (more than 2 TB)	yes	yes
Supports Command Line parameters	yes	yes
Supports Batch Mode (can be run without of any user interaction)		yes
Operates from bootable CD/DVD/BD Disc or USB disk	yes	yes
Erases with one-pass zeros	yes	yes
Erases with one-pass random characters		yes
Erases with user-defined number of passes		yes
US Department of Defense 5220.22 M compliant		yes
US Department of Energy M205.1-2		yes
US Army AR380-19 compliant		yes
US Air Force 5020 compliant		yes
German VISTR compliant		yes
Russian GOST p50739-95 compliant		yes
Canadian OPS-II compliant		yes
British HMG IS5 Baseline/Enhanced compliant		yes
Navso P-5329-26 (RL/MFM) compliant		yes
NCSC-TG-025 & NSA 130-2 compliant		yes

2 System Requirements

Feature	Freeware Version	Professional Version
NIST 800-88 compliant		yes
Peter Gutmann's method compliant		yes
Bruce Schneier's method compliant		yes
User defined erase method allows to specify custom pattern for each pass		yes
Supports erasing of all detected HDDs and USBs	yes	yes
Erasing report created and can be saved in file	yes	yes
Erasing report can be exported in XML file		yes
Erasing report can be sent out by e-mail via SMTP after erasing/wiping completed		yes
Displays detected drive and partition information	yes	yes
Scans NTFS/EFS, FAT/FAT32/exFAT, HFS+, Ext2/Ext3/Ext4fs volumes and displays existing and deleted files and folders	yes	yes
Data verification may be performed after erasing is completed		yes
Disk Viewer allows you to preview any sectors or file clusters on a drive	yes	yes
Displays Erase/Wipe certificate for printing	yes	yes
Saves Erase/Wipe certificate to PDF file	yes	yes
PDF Certificate can be customized, technician info and company logo can be inserted		yes
Wipes out NTFS, FAT/exFAT, HFS+ volumes from areas containing deleted and unused data	yes	yes
Wipes out free clusters (unused by file data sectors)	yes	yes
Wipes out file slack space (unused bytes in the last cluster occupied by file)	yes	yes
Wipes out deleted MFT records on NTFS and Directory system records on FAT/exFAT	yes	yes

Feature	Freeware Version	Professional Version
Wipes out unused space in any MFT records and compressed clusters on NTFS	yes	yes
Boot Disk Creator prepares bootable CD/DVD/BD or USB disk and configures KillDisk auto-launch with command line parameters		yes

3 Running Active@ KillDisk

After purchasing Active@ KillDisk license, you will receive a registration key and an installation file named KILLDISK-SETUP.EXE (Windows or Ultimate versions) or KILLDISK-SETUP.TAR.GZ (Linux versions). This file contains everything you need to get started.

After installation, Active@ KillDisk still starts as FREE version (unregistered), you need to register it first to have all professional features activated. To register the software, click Enter Registration Key button on the Welcome screen, or click Enter Registration Key... from the Help menu. In the Registration dialog, type (or copy and paste) your name (or company name for corporate licenses) and a registration key being sent to you, and click OK button. You can also load registration information from a text file, (either INI or TXT type) where first line is a name, and second line is a key.

Windows or Ultimate versions

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

The installed application contains two main applications:

- Active@ KillDisk for Windows (KillDisk.exe) — Run this application from your Windows operating system to inspect local disks and erase/wipe your data. KillDisk.exe is a 32-bit application, and KillDisk64.exe is a 64-bit application.
- Active@ Boot Disk Creator (BootDiskCreator.exe) — Create a bootable Windows PE CD/DVD/BD or USB disk to boot from it and run Active@ KillDisk for Windows. Using Active@ KillDisk this way allows you to wipe confidential data from the system volumes while gaining exclusive use of a partition because the operating system runs outside the partition that you are securing.

Linux versions

To setup the application, double-click KILLDISK-SETUP.TAR.GZ under Linux environment and unpack the archive to a proper location. Read ReadMe.txt file for list of supplied files and configuration instructions.

The archive contains two main applications:

- Active@ KillDisk for Linux (KillDisk)— Run this application from your Linux operating system to inspect local disks and erase/wipe your data. File named "KillDisk" is an executable (linux/elf386 format), however it on a clean Linux machine, Qt4 supporting libraries (not supplied) needs to be downloaded and installed using standard Linux Software Manager (like Apper or YaST).
- Active@ Boot Disk Creator (BootDiskCreator)— Create a bootable Linux OpenSUSE-based GUI environment on CD/DVD/BD or USB disk to boot from it and run Active@ KillDisk for Linux at startup. Prepared bootable

disk contains Linux GUI environment with Active@ KillDisk executable with all required dependencies (Qt libraries).

3.1 Active@ Boot Disk Creator

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

To prepare a bootable device:

1. Run Bootable Disk Creator from the Windows Start menu (Windows platform), or launch BootDiskCreator executable under SuperUser account (Linux platform). The Active@ Boot Disk Creator main page appears.
2. If Active@ KillDisk has not been registered yet, you need to register software first. Click Registration link, and copy and paste your registration information and a registration key being sent to you. Click OK to verify registration information, and store this information locally (next time you launch an application, won't need to register it again).
3. In the Active@ Boot Disk Creator main page, select the desired bootable media: a CD/DVD/Blu-ray, a USB Flash Drive or an ISO Image file to be burned later. If several media drives are inserted, click the ellipsis button (...) and choose a particular device. Click Next.
4. Select the target platform for booting up. Depending on Active@ KillDisk version you purchased, one or more target platforms will be available (Windows, Linux GUI, Linux Console or DOS).
5. At this step you can specify additional boot disk options:
 - a. To customize boot options, click the System Boot Settings tab. You can change the default settings to be used: Time Zone, Additional Language Support, Default Application Start and Auto-Start Delay. You can also change these options in the Active@ Boot Disk initialization screen while booting (Windows version). Additional Network and Security sub-tabs allow to configure static IP & Firewall settings, as well as to protect your Boot Disk with a password at boot time.
 - b. To add your custom files to the bootable media, click the User's Files tab. Add files or folders using the related buttons at the right side. Added items will be placed in the User_Files root folder.
 - c. To add specific drivers to be loaded automatically, click the Add Drivers tab. Add all files for the particular driver (*.INF, *.SYS, ...). Added items will be placed in the BootDisk_Drivers root folder. At boot time all *.INF files located in this folder will be installed.
 - d. To add specific scripts to be launched after Active@ Boot Disk is loaded, click the Add Scripts tab. Add your scripts (*.CMD files).

Added files will be placed in the BootDisk_Scripts root folder. At boot time all *.CMD files located in this folder will be executed.

- e. To add command line parameters for KillDisk startup after the boot, click Application Startup tab and type desired parameters. This tab is available only if Default Application Start option is turned ON on the System Boot Settings tab
6. Click Next. Verify the selected media, sizes and boot up environment.
7. Click Create. A progress bar appears while the media is being prepared.



Note: Not all additional boot disk options are accessible for all platforms. For example, Add Drivers section applies only to Windows Operating System, and is available for Windows target only.



Note: A USB Drive or blank CD/DVD/BD must be inserted and explicitly chosen on the first step before you can proceed further.



Note: When you prepare a USB Flash Drive bootable media, it will be reformatted and all data on the media will be erased. You will have the choice of creating a NTFS or a FAT32 file system on the media (Windows target). We recommend you to use FAT32 for smaller volumes. Use NTFS for larger media sizes since it supports large volumes (>32GB) and file sizes (>2GB).



Note: If you've created an ISO Image file, you can burn it to a disk later on using either our free Active@ ISO Burner utility (www.ntfs.com/iso-burning.htm) or a utility of your choice.

3.2 Interactive, Command Line and Batch Modes

Active@ KillDisk can be used two ways:

- Interactive Mode
- Command Line and Batch Mode

3.2.1 Interactive Mode

The steps for erasing data and wiping data are similar. Follow steps 1 through 10 and then click the link to complete either the erasing process or the wiping process.

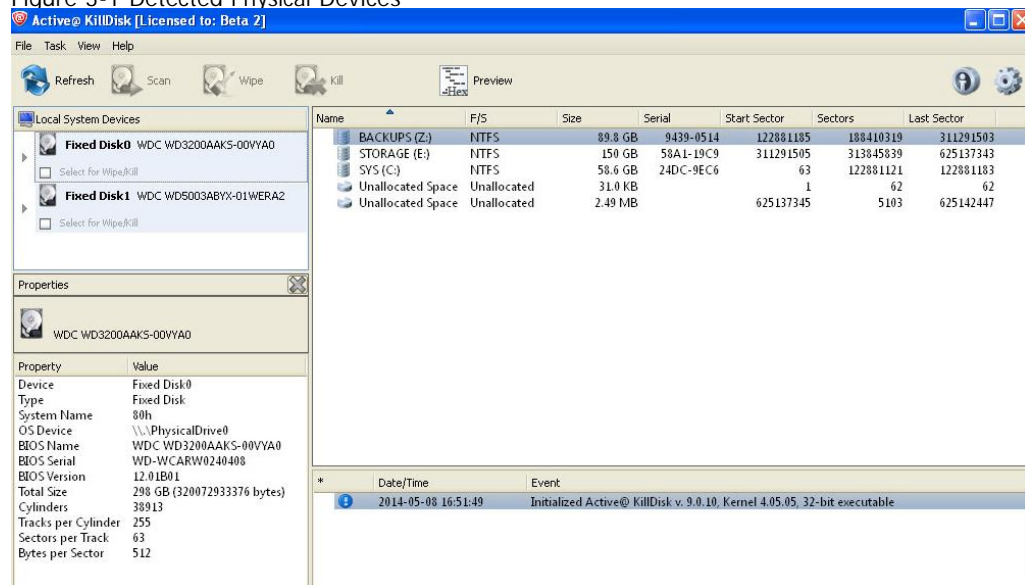
If you are booting from a CD/DVD-ROM drive, check that the drive has boot priority in the BIOS settings of your computer.

Here are the steps for interactive operation:

1. Start Active@ KillDisk either from a bootable CD/DVD, a USB device, or the Programs menu.

The Local System Devices screen appears.

Figure 3-1 Detected Physical Devices



All system physical devices and logical partitions are displayed in a list.

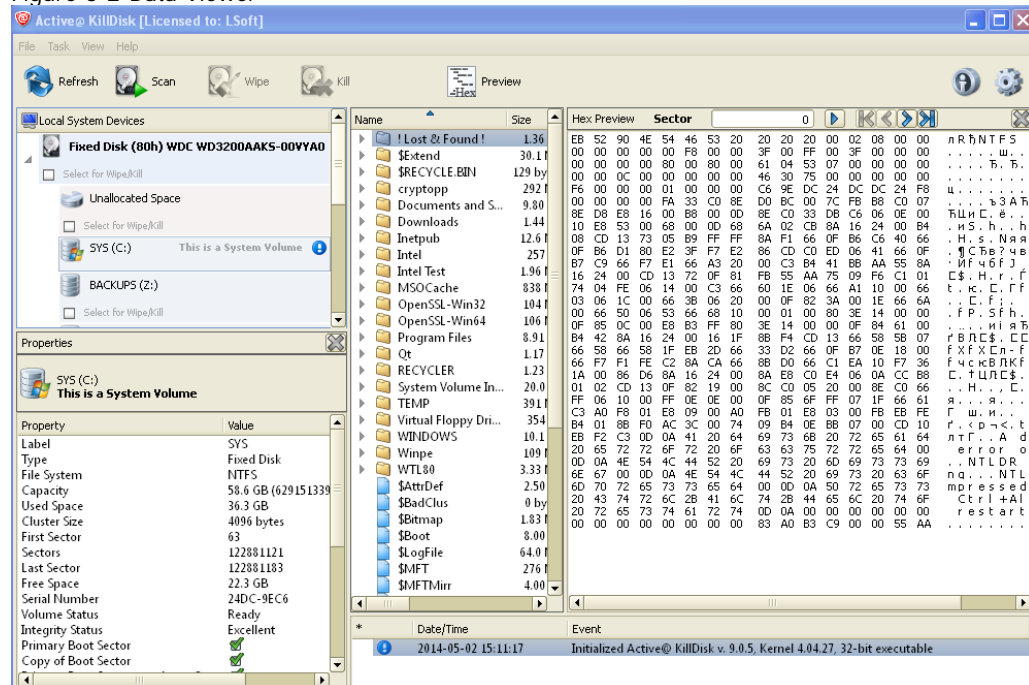
Hard drive devices are numbered by the system BIOS. A system with a single hard drive shows as number 0. Subsequent hard drive devices are numbered consecutively. For example the second device will be shown as Fixed Disk 1.

3 Running Active@ KillDisk

2. Select a device and read the detailed information about the device on the Properties pane. Below the device, select a logical partition. The information in the right pane changes.
3. Be certain that the drive you are selecting is the one that you want to erase or wipe. If you choose to erase, all data will be permanently erased with no chance for recovery.

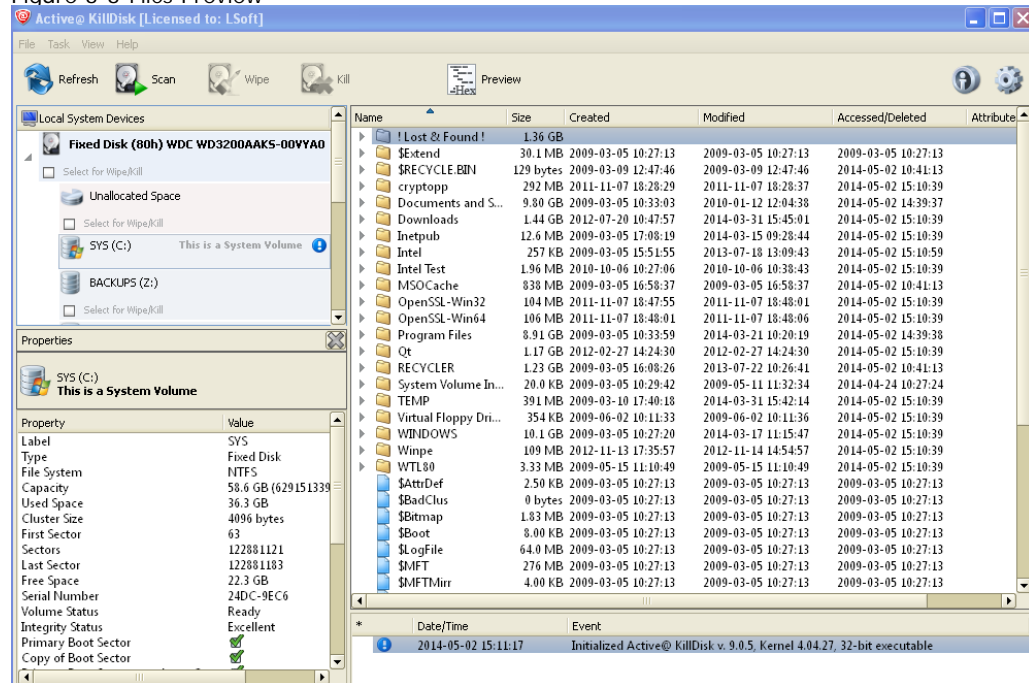
To preview the sectors on a physical disk or on a volume (logical disk), select it and press ALT + P, or click Hex Preview on the toolbar. The Hex Preview panel appears.

Figure 3-2 Data Viewer



4. To scroll up and down, use the keyboard navigation arrow keys PAGE UP, PAGE DOWN, HOME and END, or use the related buttons on the toolbar.
5. To jump to a specific sector, type the sector number in the Sector box and press ENTER or click Go on the toolbar.
6. When you are satisfied with the identification of the device, close the Hex Preview panel (ALT+P).
7. To preview the files in a logical disk, select the volume and press ENTER or double-click it. KillDisk scans the directories for the partition. The Folders and Files screen appears.

Figure 3-3 Files Preview



8. Press TAB to move between panels or choose a panel with the mouse.
9. To select an item in the list, use PAGE DOWN, PAGE UP or the up or down arrow keys or use the mouse.
10. To open a folder, double-click the folder or select it and press ENTER. KillDisk scans the system records for this folder. The files in the folder appear in the right panel. Existing files and folders are marked by yellow icons and deleted files and folders are marked by gray icons. If you are wiping data from unoccupied areas, the gray-colored file names are removed after the wiping process completes. You may use the Hex Preview mode to inspect the work done by the wiping process. After wiping, the data in these areas and the places these files hold in the root records or other system records are gone.

3.2.1.1 Erase Data from a Device

When you select a physical device (for example, Fixed Disk0), the erase command processes partitions no matter what condition they are in. Everything is destroyed.

If you want to erase data on selected logical drives, follow the steps in 3.4 Erase or Wipe Logical Drives (Partitions).

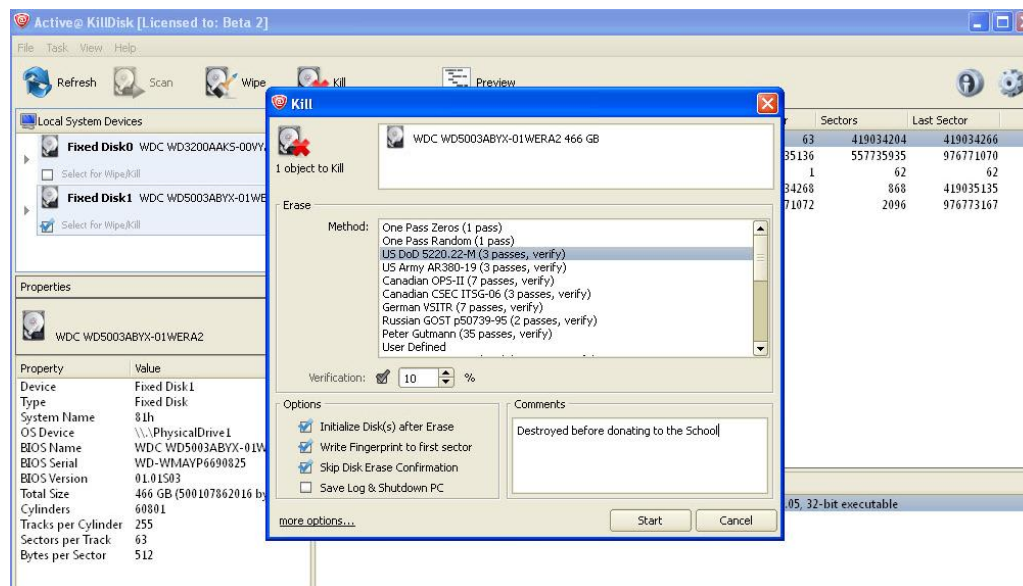
To erase the data:

1. Be certain that the drive you are pointing to is the one that you want to erase. All data will be permanently erased with no chance for recovery.

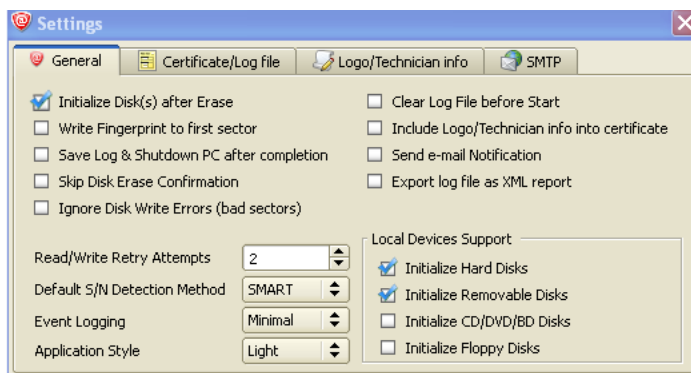
3 Running Active@ KillDisk

- When you have selected the device to erase, select the checkbox for this hard drive. You may select more than one physical disk for the erase action. In this case these disks will be erased simultaneously. To permanently erase all data on the selected disk(s), press F10 or click Kill on the toolbar. The Kill dialog box appears.

Figure 3-4 Kill dialog box



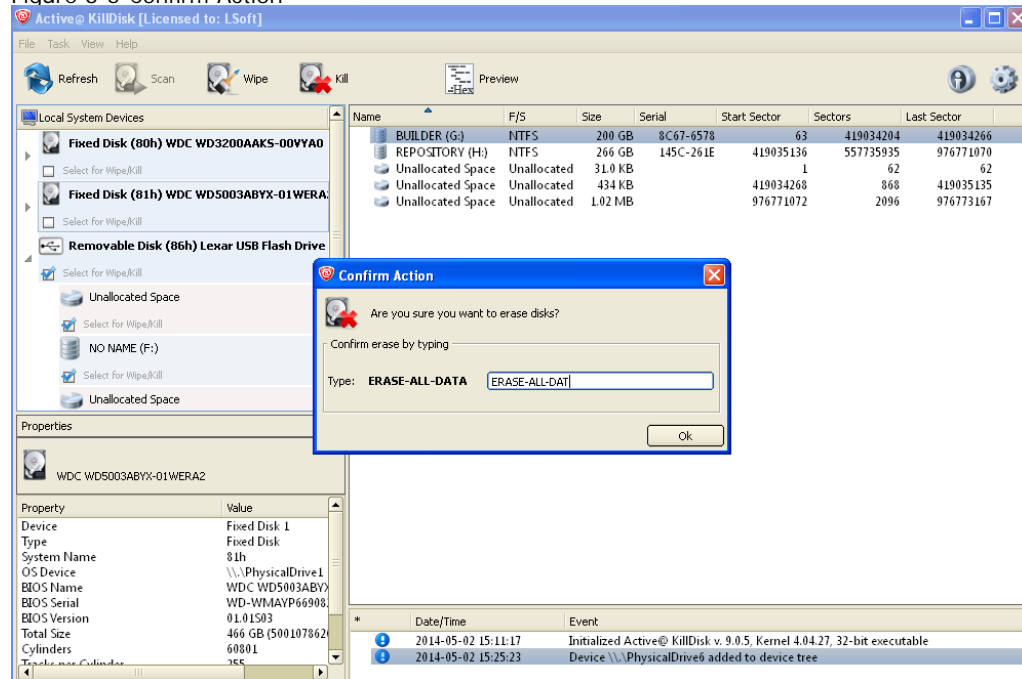
- Select an erase method from the list. Erase methods are described in Chapter 5 Erase/Wipe Parameters in this guide.
- Set other parameters for erasing and add comments for the certificate, if needed. To specify log and certificate file location, e-mail notifications, and other settings, click the [more options...](#) link at the bottom. The settings box will then appear.



For information on these settings, see Chapter 5 in this guide.

- Click Start.
 - If the Skip Disk Erase Confirmation check box is clear, the Confirm Action dialog box appears.

Figure 3-5 Confirm Action





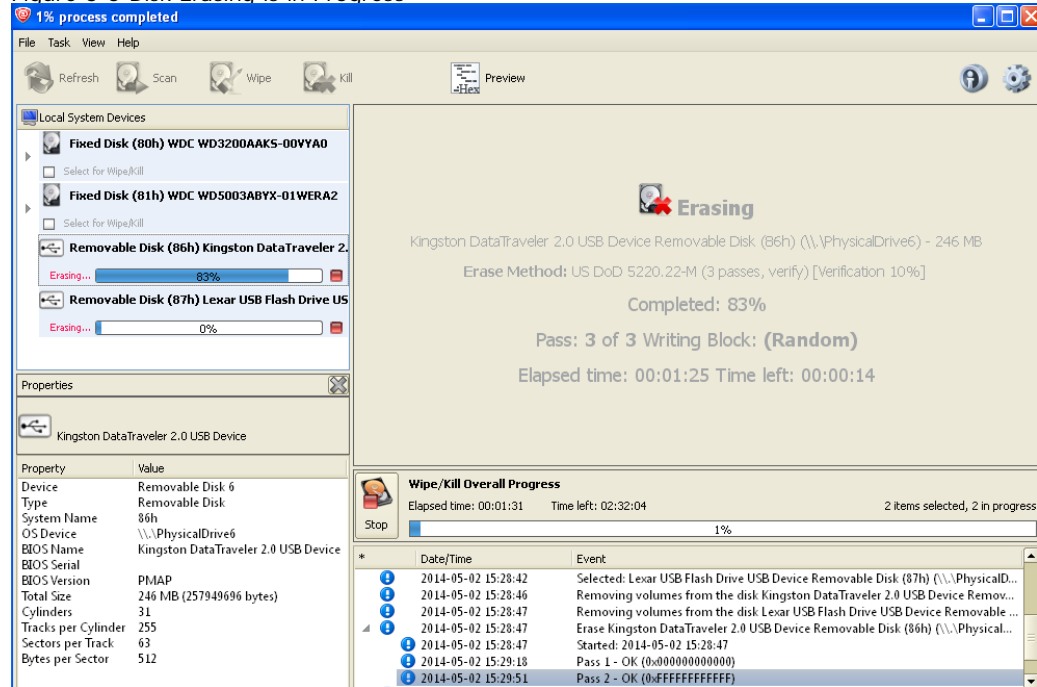
6. This is the final step before removing data from the selected drive forever. Type ERASE-ALL-DATA in the text box and press ENTER or click YES. The Progress bar appears below the disk on the left panel.
7. Overall Wipe/Kill Progress is displayed on the right panel, as well as the detailed command status for the selected disk in the Local System Devices list.
8. To stop the process at any time, click the stop button  for the particular disk. Click the stop all button  left to overall progress to cancel erasing for all disks. Note that data that has already been erased will not be recoverable.

Figure 3-6 Disk Erasing is in Progress



There is nothing more to do until the end of the disk erasing process. The application will operate on its own. However, you can still browse and inspect other disks, scan volumes and launch another Kill or Wipe processes for other objects. KillDisk perfectly erases disks in parallel!

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 (click Abort), or you may continue erasing data (click Ignore or Ignore All).

NOTE: Because of the BIOS restrictions of some manufacturers, a hard disk device that is larger than 300 MB must have an MBR (Master Boot Record) in sector zero. If you erase sector zero and fill it with zeros or random characters, you might find that you cannot use the hard drive after erasing the data. It is for this reason KillDisk creates an empty partition table and writes a typical MBR in sector zero (in case the Initialize disk(s) after Erase option is selected).

3.2.1.2 Wipe Data from a Device

When you select a physical device such as Fixed Disk0, the wipe command processes all logical drives consecutively, deleting data in unoccupied areas. Unallocated space (where no partition exists) has been erased as well. If KillDisk detects that a partition has been damaged or that it is not safe to proceed, KillDisk does not wipe data in that area. The reason it does not proceed is that a damaged partition might contain important data.

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

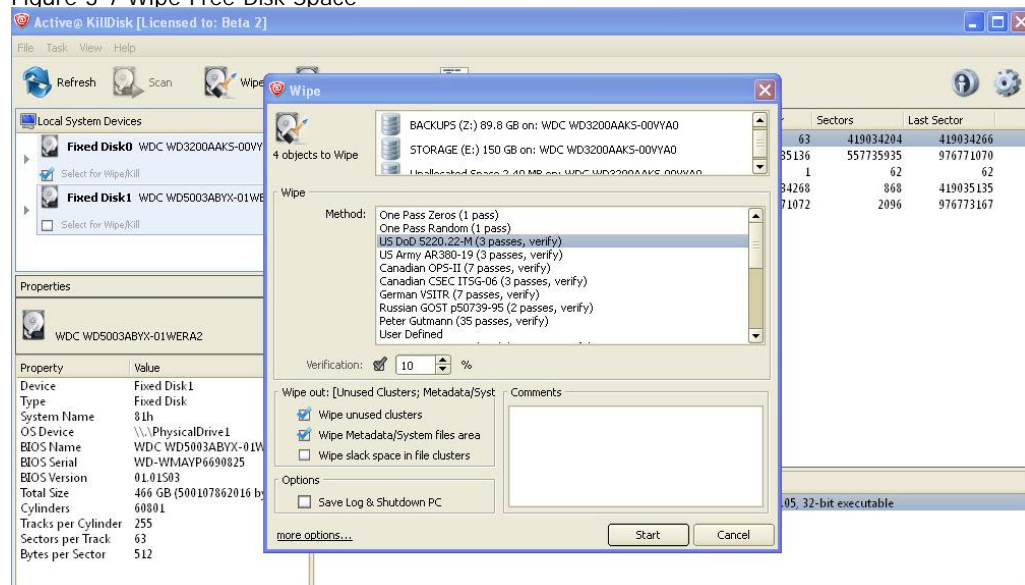
If you want to erase data from the hard drive device permanently, see 3.2.1.1 Erase Data.

If you want to wipe data in unoccupied areas on selected logical drives, follow the steps in 3.4 Erase or Wipe Logical Drives (Partitions).

To wipe deleted data from a device:

1. To choose a device to wipe, select the check box next to the device name. You may select multiple devices. In this case these disks will be wiped out simultaneously
2. To wipe out all data in unoccupied sectors on the selected partitions, press F9 or click the Wipe toolbar button. The Wipe Free Disk Space dialog box appears.

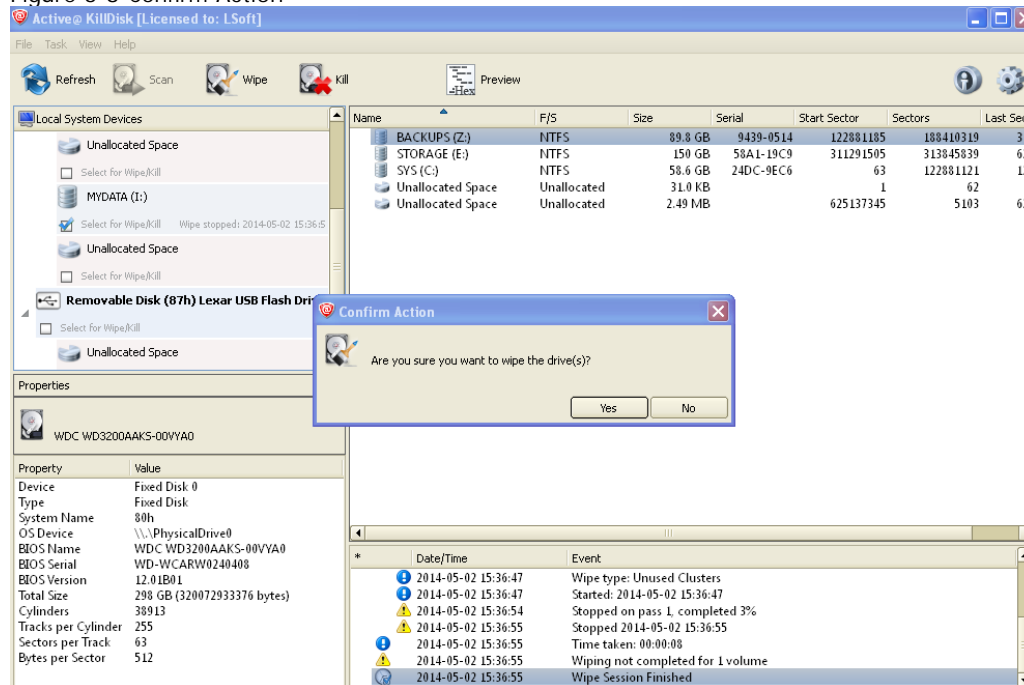
Figure 3-7 Wipe Free Disk Space





3. To select a wipe type, choose a method from the Wipe Method list. Wipe methods are described in [Chapter 5 Erase/Wipe Parameters](#) in this guide.
4. You may change parameters in this dialog box, or click the more options... link at bottom to review and change other options. For information on these parameters, see [Chapter 5 Erase/Wipe Parameters](#) in this guide.

- To advance to the final step before erasing data, click Start. If the Skip Confirmation check box is clear, the Confirm Action dialog box appears.

Figure 3-8 Confirm Action



- This is the final step before wiping data residue from unoccupied space on the selected drive.

To confirm the wipe action, click Yes. The progress of the wiping procedure will be monitored in the Disk Wiping screen.
- To stop the process for any reason, click the stop button  for a particular disk. Click the stop all button () left to the overall progress to cancel wiping for all selected disks. Note that all existing applications and data will not be touched. Data that has been wiped from unoccupied sectors is not recoverable.
- There is nothing more to do until the end of the disk wiping process. The application operates on its own.

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.
- After the wiping process is completed select the wiped partition and press ENTER or double-click it to inspect the work that has been done. KillDisk scans the system records or the root records of the partition. The Folders and Files tab appears.

Existing file names and folder names appear with a multi-colored icon and deleted file names and folder names appear with a gray-colored

icon. If the wiping process completed correctly, the data residue in these deleted file clusters and the place these files hold in the directory records or system records has been removed. You should not see any gray-colored file names or folder names in the wiped partition.

3.2.2 Command Line and Batch Mode

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

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

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

3.2.2.1 Command Line Mode

To run Active@ KillDisk in command line mode, open a command prompt screen.

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

```
> KILLDISK.EXE -?
```

In Linux environment, type:

```
> KillDisk -?
```

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

Table 3-2 Command Line Parameters

Parameter	Short	Default	Options
no parameter			With no parameter, the Interactive screens will appear
-erasemethod=[0 - 22]	-em=	2	0 - One pass zeros (quick, low security) 1 - One pass random (quick, low security) 2 - US DoD 5220.22-M (slow, high security) 3 - US DoD 5220.22-M (ECE) (slow, high security) 4 - Canadian OPS-II (slow, high security) 5 - British HMG IS5 Baseline (slow, high security)

Parameter	Short	Default	Options
			security) 6 - British HMG IS5 Enhanced (slow, high security) 7 - Russian GOST p50739-95 (slow, high security) 8 - US Army AR380-19 (slow, high security) 9 - US Air Force 5020 (slow, high security) 10 - Navso P-5329-26 (RL) (slow, high security) 11 - Navso P-5329-26 (MFM) (slow, high security) 12 - NCSC-TG-025 (slow, high security) 13 - NSA 130-2 (slow, high security) 14 - German VSITR (slow, high security) 15 - Bruce Schneier (slow, high security) 16 - Gutmann (very slow, highest security) 17 - User Defined Method. Number of Passes and Overwrite Pattern supplied separately. 18 - NIST 800-88 (1 pass zeros, quick) 19 - NIST 800-88 (1 pass random, quick) 20 - NIST 800-88 (3 pass zeros, slow, high security) 21 - Canadian CSEC ITSG-06 (3 passes, verify) 22 - US DoE M205.1-2 (3 passes ,verify)
-passes=[1 - 99]	-p=	3	Number of times the write heads will pass over a disk area to overwrite data with User Defined Pattern. Valid for User Defined Method only
-verification=[1 - 100]	-v=	10	Set the amount of area the utility reads to verify that the actions performed by the write head comply with the chosen erase method (reading 10% of the area

Parameter	Short	Default	Options
			by default). Verification is a long process. Set the verification to the level that works for you better
-retryattempts=[1 - 99]	-ra=	2	Set the number of times that the utility will try to rewrite in the sector when the drive write head encounters an error
-erasehdd=[0,1..63]	-eh=		Number in BIOS of the disk to be erased. First physical disk has a zero number. In Linux first disk usually named /dev/sda. In Windows Disk Manager first disk is usually named Disk 0. On older systems (DOS, Windows 9x) first disk is usually named 80h (obsolete syntax is still supported in the parameter)
-eraseallhdds	-ea		Erase all detected disks
-excluderemovable	-xr		Exclude all removable disks from erasing when erase all disks selected
-excludefixed	-xf		Exclude all fixed disks from erasing when erase all disks option selected
-excludedisk=[0,1..63]	-xd=		Exclude disk from erasing when erase all disks option selected
-ignoreerrors	-ie		Do not stop erasing each time a disk error is encountered. When you use this parameter, all errors are ignored and just placed to the application log
-stopaftererrors=[1,2..]	-er=		Stop erasing process after specific number of writing errors encountered
-initdisk	-id		Initialize disk(s) after erase
-fingerprint	-fp		Initialize disk(s) and write fingerprint to the disk's first sector
-clearlog	-cl		Use this parameter to clear the log file before recording new activity. When a drive is erased, a log file is kept. By default, new data is appended to this log for each erasing process. By default the log file is stored in the same folder where the software is located

Parameter	Short	Default	Options
-exportlog	-el		Export a log file as XML report
-logpath=["fullpath"]	-lp=		Path to save application log file. Can be either directory name or full file name. Use quotes if full path contains spaces
-certpath=["fullpath"]	-cp=		Path to save erase/wipe certificate. Can be either directory name or full file name. Use quotes if full path contains spaces
-inipath=["fullpath"]	-ip=		Path to the configuration file (KILLDISK.INI) for loading the advanced settings. See table below
-noconfirmation	-nc		Skip confirmation steps before erasing starts. By default, confirmation steps will appear in command line mode for each hard drive as follows: Are you sure?
-beep	-bp		Beep after erasing is complete
-wipeallhdds	-wa		Wipe out unallocated space on all recognized volumes located on all detected disks
-wipehdd = [0,1...63]	-wh=		Wipe out unallocated space on the disk specified by BIOS number
-test			If you are having difficulty with Active@ KillDisk, use this parameter to create a hardware information file to be sent to our technical support specialists
-batchmode	-bm		Execute in batch mode based on command line parameters and INI file settings (without user interaction, all operations being stored to log file)
-userpattern =["fullpath"]	-u		File to get user-defined pattern from. Applied to User Defined erase method. Each line in the file corresponds to the particular pass pattern
-shutdown	-sd		Save log file and shutdown PC after completion
-nostop	-ns		Prevent erase/wipe stop action

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

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

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

Note: If command line parameter, like full path, contains spaces – it should be by surrounded by double quotation marks.

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

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

The same in Linux:

```
> KillDisk -eh=80h -bm
```

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

Here is another Windows example:

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

The same in Linux:

```
> KillDisk -eh=80h -nc -em=2
```

In this example, all data on the device 80h will be erased using US DoD 5220.22-M method without confirmation and showing a report at the end of the process.

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

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

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

3.2.2.2 Batch Mode

This feature is intended for advanced users.

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

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

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

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

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

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

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

3.3 Application settings (KILLDISK.INI file)

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

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

For parameter storage the syntax being used is:

```
Parameter=value
```


Here is an example of an INI file:

```
[General]
logging=0
showCert=true
saveCert=false
initDevice=true
clearLog=false
ignoreErrors=false
skipConfirmation=true
retryAtt=2
certPath=C:\Program Files\LSOFT Technologies\Active KillDisk\
logPath=C:\Program Files\LSOFT Technologies\Active KillDisk\
logName=killdisk.log
...
```

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

Here is an explanation of all settings:

Table 3-3 KillDisk settings in INI file

Parameter	Default	Options
defaultSerialDetectionMethod=	2	1 - use operating system's DeviceIOControl method 2 - use S.M.A.R.T information, if device supports it 3 - use Windows Management Instrumentation (WMI), if operating system supports it
showCert=	true	true/false – option of displaying the Erase/Wipe Certificate for printing after completion
saveCert=	false	true/false – option of saving the Erase/Wipe Certificate after completion
certPath=		Full path to the location where Erase/Wipe Certificate will be saved. This is a directory name
logPath=		Full path to the location where log file will be saved. This is a directory name

Parameter	Default	Options
logName=		Name of the log file where event log will be saved to
skipConfirmation=	false	true/false – whether to display or skip Erase/Wipe confirmation dialog, or not
ignoreErrors=	false	true/false – whether to display disk writing errors (bad sectors), or ignore them (just place them to the log file)
clearLog=	false	true/false – whether to truncate log file content before writing new sessions, or not (append to existing content)
initDevice=	true	true/false – whether to initialize disks after erasing complete, or not
fingerPrint=	false	true/false – whether to initialize disk(s) and write fingerprint to the disk's first sector, or not
hideDefaultLogo	false	true/false – whether to hide default KillDisk logo at the top-left corner of the certificate, or not
shutDown=	false	true/false – whether to shutdown PC after Erase/Wipe execution complete, or not
sendSMTP=	false	true/false – to send e-mail report by e-mail via SMTP
attachCert=	false	true/false – to attach a PDF certificate to e-mail report being sent
useDefaultAccount=	true	true/false – use pre-defined Free SMTP account for sending e-mail reports
fromSMTP=		E-mail address you'll get a report from, for example: reports@killdisk.com
toSMTP=		E-mail address the report will be sent to
nameSMTP=		SMTP server (relay service) being used for sending e-mail reports, for example: www.smtp-server.com
portSMTP=	25	TCP/IP port SMTP service will be connected on. The standard SMTP port is 25, however some internet providers block it on a firewall

Parameter	Default	Options
authorizeSMTP=	false	true/false – use SMTP authorization for sending e-mail reports (Username and Password must be defined as well)
usernameSMTP=		In case if SMTP service requires authorization, this is SMTP Username
passwordSMTP=		In case if SMTP service requires authorization, this is SMTP Password
showLogo=	false	true/false – whether to display custom Logo (image) on a Certificate, or not
logoFile=		Full path to the file location where Logo image is stored
clientName=		Client Name - custom text to be displayed on a Certificate
technicianName=		Technician Name - custom text to be displayed on a Certificate
companyName=		Company Name - custom text to be displayed on a Certificate
companyAddress=		Company Address - custom text to be displayed on a Certificate
companyPhone=		Company Phone - custom text to be displayed on a Certificate
logComments=		Any Comments - custom text to be displayed on a Certificate
killMethod=	2	[0-20] – Erase method to use for disk/volume erasing. See table of Erase Methods available. DoD 5220.22-M by default
killVerification=	true	true/false – whether to use data verification after erase, or not
killVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
killUserPattern=		ASCII text to be used for User Defined erase method as a custom pattern
killUserPasses=		[1-99] – number of overwrites to be used for User Defined erase method

Parameter	Default	Options
wipeMethod=	2	[0-20] – Wipe method to use for volume wiping. See table of Erase Methods available. DoD 5220.22-M by default
wipeVerification=	true	true/false – whether to use data verification after wipe, or not
wipeVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
wipeUserPattern=		ASCII text to be used for User Defined wipe method as a custom pattern
wipeUserPasses=		[1-99] – number of overwrites to be used for User Defined wipe method
wipeUnusedCluster=	True	true/false – whether to wipe out all unused clusters on a volume, or not
wipeUnusedBlocks=	False	true/false – whether to wipe out all unused blocks in system records, or not
wipeFileSlackSpace=	False	true/false – whether to wipe out all file slack space (in last file cluster), or not

You can find a more detailed explanation of each parameter in Chapter 5 - Erase/Wipe parameters.

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

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

3.4 Erase or Wipe Logical Drives (Partitions)

In all previous examples in this chapter, the process has erased or wiped data from a physical drive. Using a similar method, you can erase or wipe logical disks and partitions. This includes damaged “Unallocated” areas where partitions used to exist and areas not visible to the current operating system.

The Wipe button is disabled when partitions cannot be wiped because of issues such as an unknown or unsupported file system. KillDisk must lock the partition before performing a Wipe or Erase action. A partition cannot be

locked if it is in use by another user or application. In this case a dialog box appears with information that the disk is being used and you need to either skip it, or “force volume dismount”. If you skip it, the wipe or erase operation is canceled for this drive. If you select “force dismount”, some data in the drive’s cache may be lost. This could affect other applications working with the same volume. If, for example, you made changes to a Word document located on D: and haven’t saved the file, a subsequent “forced dismount” for D: would likely result in the loss of the changes. The file’s original version should be unaffected.

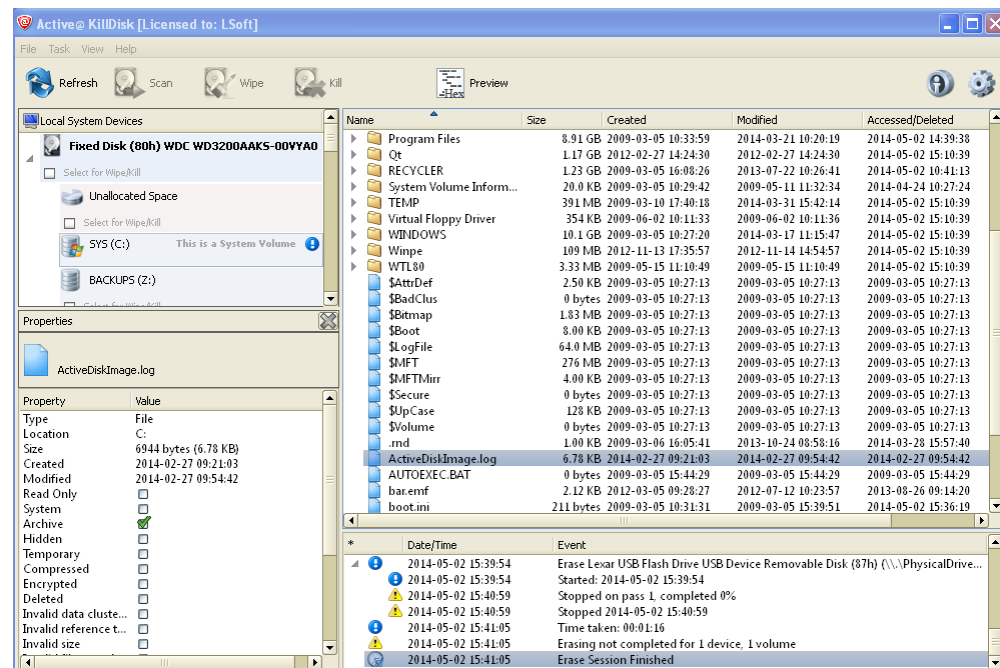
3.4.1 Erase Data from a Logical Drive

To erase data from a logical drive:

1. Start Active@ KillDisk from a bootable device or from the Programs menu.
2. The Local System Devices screen appears.

All system hard drives and removable drives are displayed in the left pane. System information is displayed in the right pane.

Figure 3-9 Local System Devices and Volumes



3. Select the check box of a logical disk/volume or the Unallocated area.
4. Press F10 or click Kill. The Kill dialog box appears.
5. Set the erase method and other parameters for erasing. For information on these parameters, see [Chapter 5 Erase/Wipe Parameters](#) in this guide.
6. Complete the process as you would for other devices.

3.4.2 Wipe Data from a Logical Drive

To wipe data from a logical drive:

1. Start Active@ KillDisk from a bootable device or from the Programs menu.
2. The Local System Devices screen appears.
All system hard drives and removable drives will be displayed in the left pane along with their system information in the right pane.
3. Select the check box of a logical disk/volume or the Unallocated space.
4. Press F9 or click Wipe to wipe data from unoccupied areas. The Wipe Free Disk Space dialog box appears.
5. Select a wipe method and set other parameters for wiping. For information on these parameters, see [Chapter 5 Erase/Wipe Parameters](#) in this guide.
6. Complete the process as you would for other devices.

3.5 Completed Erase or Wipe Operation Information

After an operation is completed successfully, information on how drives have been erased or wiped is displayed in the Event Log at bottom of the screen. The text can be saved in a log file and as a certificate that can be printed or saved as a PDF file for future printing.

An example of an erase session saved in a Log file is displayed below.

```
2012-10-10 11:12:40 Initialized Active@ KillDisk for Windows
-----Erase Session Begin-----
2012-10-10 11:13:59 Active@ KillDisk for Windows started
Erase method: US DoD 5220.22-M (3 passes, verify) Passes: 3 [Verification 10%]
Erase WDC WD1600YD-01NVB1 Fixed Disk (81h) (Serial Number: WD-WMANM1702217) - 153 GB
Started: 2012-10-10 11:13:59
Pass 1 - OK (0x0000000000000000)
Pass 2 - OK (0xFFFFFFFFFFFFFFFF)
Pass 3 - OK (Random)
Verification passed OK
Finished 2012-10-10 13:54:19
2012-10-10 13:54:28 Time taken: 02:40:21
2012-10-10 13:54:28 Erasing completed for 1 device
-----Erase Session End-----
2012-10-10 13:54:28 Rescanned hardware
```

A summary of errors is presented in this report if the process encountered errors from, for example, bad clusters.

Details of this report are saved by default to a log file located in the folder from which you started Active@ KillDisk. Log file location can be changed in Settings.

If XML export option is turned on, log file can be exported, and look like:

```
<?xml version="1.0" encoding="utf-8" ?>
- <killdisk_log>
- <event>
<type>Info</type>
<time>2014-01-02 13:57:22</time>
<text>Initialized Active@ KillDisk for Windows, 32-bit executable</text>
</event>
<type>Info</type>
<time>2014-01-02 14:08:52</time>
<text>DOCS (K:) successfully locked</text>
</event>
- <session>
<action>Wipe</action>
<started>2014-01-02 14:08:52</started>
- <event>
<type>Info</type>
<time>2014-01-02 14:08:52</time>
<text>Wipe method: US DoD 5220.22-M (3 passes, verify) Passes: 3 [Verification 10%]</text>
</event>
- <event>
<type>Info</type>
<time>2014-01-02 14:08:53</time>
<text>Finished 2014-01-02 14:08:53</text>
</event>
- <event>
</killdisk_log>
```

Example of an Erase Certificate that can be printed or saved as a PDF:



4 Common Questions

4.1 How does the licensing work?

The software is licensed on a per CD/DVD or USB media storage device basis. Each license allows you to use the program from a separate CD/DVD or USB device. For example, if you want to use the program to wipe five computers concurrently, you would need five CDs or DVDs or USB devices (or combination of the three not exceeding five), and therefore need a five-user license.

4.2 How is the data erased?

Active@ KillDisk communicates with the system hardware device directly. The Free version erases data by overwriting all addressable locations on the drive with zeros. Active@ KillDisk Professional version suggests several methods for data destruction. For example, in [US DoD 5220.22-M](#) method it overwrites all addressable storage and indexing locations on the drive three times with zeros (0x00), complement (0xFF), and random characters. It then verifies all writing procedures. This complies with the US DoD 5220.22-M security standard.

4.3 What is the difference between the Site and Enterprise license?

Site License means an unlimited usage of the program in one physical location; Enterprise License - in any company's locations.

4.4 Which operating systems are supported by Active@ KillDisk?

Active@ KillDisk for Windows can be launched and work under Windows XP, Windows Vista, Windows 7, Windows 8, Windows 2003, and 2008 Server. Active@ KillDisk for Windows can be also launched from a pre-installed on media storage device operating system (WinPE).

Active@ KillDisk for Linux can be launched and work under different Linux versions (OpenSUSE, Ubuntu, Fedora, Oracle, ...). Required Linux graphical environment: KDE or Gnome, Linux Kernel 2.x or higher, and shared libraries for Qt v.4.x to be installed.

As it can be installed easily onto a bootable CD/DVD or USB card, it does not matter which operating system is installed on the machine's hard drive. If you can boot from the boot CD/DVD/USB, you can detect and erase any drives independent of the installed operating system. This way you can easily erase UNIX, Linux and MacOS X partitions and disks.

4.5 Is Active@ KillDisk compatible with Macintosh computers?

You cannot run Active@ KillDisk in the old Mac OS environment (based on PowerPC architecture). However, the most recent Apple computers (iMac running MacOS X) are based on the Intel architecture. In this case, it is possible to boot from Active@ Boot Disk using a CD, DVD or USB device. To do so, hold the Option key down when starting the computer.

4.6 Will I be able to use my Hard Disk Drive after Active@ KillDisk erase operation?

Yes. To be able to use the HDD again you need to:

- Repartition the hard drive using a standard utility like FDISK.
- Reformat partitions using a standard utility like FORMAT.
- Reinstall the Operating System using a bootable CD/DVD-ROM.

4.7 I cannot boot from the CD/DVD. What should I do next?

Your computer may have boot priority for Hard Disk Drives, or another device set higher than boot priority for CD/DVD device.

Parameters that are set in low-level setup are written to the machine's BIOS.

To change the boot priority:

1. Open the low-level setup utility, usually by pressing F1, F2, F10 or ESC on the keyboard during startup.
2. Use the arrow keys to locate the section about Boot device priority. This section will allow you to set the search order for types of boot devices. When the screen opens, a list of boot devices appears. Typical devices on this list will be hard drives, CD or DVD devices, floppy drives and network boot option.
3. If the CD or DVD device has been disabled, enable it (provided you have a device installed). The priority should indicate that the CD/DVD device is the number one device the BIOS consults when searching for boot instructions. If the CD/DVD device is at the top of the list that is usually the indicator.
4. Save and exit the setup utility.

5 Erase/Wipe Parameters and Application Settings

Whether you choose to erase data from the drive or to wipe data from unoccupied drive space, the methods of overwriting these spaces are the same.

5.1 Erase/Wipe Methods

One Pass Zeros or One Pass Random

When using One Pass Zeros or One Pass Random, the number of passes is fixed and cannot be changed.

When the write head passes through a sector, it writes only zeros or a series of random characters.

User Defined

You indicate the number of times the write head passes over each sector. Each overwriting pass is performed with a buffer containing the pattern you specified (ASCII string).

US DoD 5220.22-M

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

US DoD 5220.22-M (ECE)

The write head passes over each sector seven times (0x00, 0xFF, Random, 0x96, 0x00, 0xFF, Random). There is one final pass to verify random characters by reading.

US DoE M205.1-2

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

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.

Canadian CSEC ITSG-06

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

German VSITR

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

HMG IS5 (Baseline and Enhanced)

Baseline method overwrites disk's surface with just zeros (0x00).

Enhanced method - the write head passes over each sector three times. The first time with zeros (0x00), the second time with 0xFF, and the third time with random characters.

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

Navso P-5329-26 (RL and MFM)

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

MFM method - the write head passes over each sector three times (0x01, 0x7FFFFFFF, Random).

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

NIST 800-88

Supported three NIST 800-88 media sanitization standards:

- The write head passes over each sector one time (0x00)
- The write head passes over each sector one time (Random)
- 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

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.

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.

Gutmann

The write head passes over each sector 35 times. For details about this, the most secure data clearing standard, you can read the original article at the link below:

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

5.2 Erase/Wipe Options

In addition to the erase method, you can specify more options for erasing/wiping.

Verification

After erasing is complete you can direct the software to perform verification of the surface on the drive to be sure that the last overwriting pass was performed properly and data residing on the drive matches the data written by the erasing process.

Because verification is a long process, you may specify a percentage of the surface to be verified. You may also turn the verification off completely.

Wipe out Deleted/Unused data

This parameter appears only when you are wiping data from unused space on the hard drive. The wiping process clears data residue from unoccupied space on the hard drive and does not affect installed applications or existing data. This process contains three options:

- Wipe unused clusters
- Wipe unused space in MFT/Root area
- Wipe slack space in file clusters

You may choose to run only one or two of these options in order to make the process complete more quickly. If you want a thorough wiping of unused space, then include all of the options.

Initialize Disk

Because of the BIOS restrictions of some manufacturers, a hard disk device that is larger than 300 MB must have an MBR (Master Boot Record) in sector zero. If you erase sector zero and fill it with zeros or random characters, you might find that you cannot use the hard drive after erasing the data. It is for this reason KillDisk creates an empty partition table and writes a typical MBR in sector zero. This is called disk initialization.

Write Fingerprint

If fingerprint has been written to the disk's first sector, next time you boot from this disk, you can see disk erase status, like this:

```
Active@ KillDisk for Linux v.9.0 (build 4.04.27)
Copyright (C) 1998-2014 LSoft Technologies Inc.

Sanitation of 000000000000000001 started 2014-05-02 at 16:54:20
Secure erase method: One Pass Zeros
Sanitation completed 2014-05-02 at 16:54:42
Result: SUCCESS
```

In case if errors occurred, or erasing stopped, status will be FAILED and displayed in red color.

5.3 General Settings

General parameters allow you to turn features on or off or change default settings when you are erasing or wiping data from unoccupied space. You can also change the look and feel of the application and its logging options. To view and change settings, press the F2 key, or click the Settings toolbar button.

Read/Write Retry Attempts

If an error such as physical damage on the drive surface is encountered while writing data to the drive, Active@ KillDisk tries to perform the write operation again. You can specify the number of retries to be performed. Sometimes, if the drive surface is not completely destroyed, a damaged sector can be overwritten after several retries.

Ignore Disk Write Errors (bad sectors)

If this option is turned on, error messages will not be displayed while data erasing or verification is in progress. All information about errors is written to the KILLDISK.LOG file. These messages are displayed in the final Erasing report after the process is complete.

Clear Log File before Start

If this option is turned on, the KILLDISK.LOG log file will be truncated before erasing starts. After erasing is completed, the log file will contain information only about the last session.

If this option is turned off, the KILLDISK.LOG log file will not be truncated and information about the last erasing session is appended to the end of the file.

Skip Disk Erase Confirmation

The confirmation screen is the final step before erasing data. In this screen, you type ERASE-ALL-DATA to confirm what is about to happen. If Skip Confirmation is turned on, this final safety request does not appear. This option is typically used with caution by advanced users in order to speed up the process. It is safer to run KillDisk with the default state of Skip Disk Erase Confirmation selected. You may want to use this as a safety buffer to ensure that data from the correct drive location is going to be erased completely with no possibility of future data recovery.

Save Log & Shutdown PC after completion

Erasing can take many hours. You can leave work with KillDisk running and set to turn the computer off when erasing is completed. A log file is saved and can be reviewed later on.

Event Logging

By default KillDisk does a Minimal logging. Information is placed in the Event Log view and saved to the KILLDISK.LOG log file. If more detailed

information is required or execution errors occur, you can specify the Detailed logging option. The problem can then be more effectively analyzed.

Application Style

By default KillDisk has been launched in a "Dark" color scheme. If you are uncomfortable with it, change the Application Style to "Light" mode. An application re-start is required when you change the Application Style.

Include Logo/Technician info into Certificate

After erasing/wiping, KillDisk can produce a certificate PDF file that can be printed later on. This certificate can include custom attributes, such as company logo (graphics) and company info (text). You can configure these parameters in the Logo/Technician Info tab. Turn on this option to include all supplied parameters in the Certificate.

This option is available only in the Professional version.

Hide certificate default logo

After erasing/wiping, KillDisk can produce a certificate HTML file that can be printed later on. This option directs whether to hide default KillDisk logo at the top-left corner of the certificate, or not.

This option is available only in the Professional version.

Send e-mail Notification

After erasing/wiping is complete, KillDisk can deliver the output report (contents of the log file) to your e-mail mailbox. You can configure sending parameters on the SMTP tab. Turn on this option to send out a report after successful job completion or if errors occur.

This option is available in only in the Professional version.

Export log file as XML report

After erasing/wiping is complete and application exited, KillDisk can store the output report (contents of the log file) to XML file at the location of executable. Turn on this option to export report to XML.

This option is available in only in the Professional version.

Local Devices Support

Device initialization takes some time when application starts. For slow-performing devices (floppies, CD/DVD media, USB disks, etc..) this time could be significant. You can save some time by turning off non-important for you device types.

5.4 Certificate and Log File Settings

These settings allow configuration of the storage and display parameters for the certificate and log file.

Certificate options

These parameters allow display of the erase\wipe certificate and setting of its storage location as a PDF file for future printing. If email reports delivery option is specified (on a General tab), PDF certificate can be attached to the notification email.

Log file options

These parameters allow naming the log file and setting its storage location.

5.5 Logo and Technician Info Settings

These settings allow embedding custom information into the standard PDF certificate for printing.

These options can be configured in the Free version, but are useable only in the Professional version.

Logo

You can select a company logo from a graphics file (*.BMP, *.JPG, *.PNG). The image size must be 450 by 200 pixels to be printed properly. The company logo will be placed at the top of the certificate and will be embedded into a PDF file that you can print later on.

Technician Information

You can specify all or some of the fields being displayed on a certificate and embedded into a PDF file:

- Client Name
- Technician Name
- Company Name
- Company Address
- Company Phone
- Comments

5.5 SMTP Settings

These settings allow configuring mailer settings for delivering erasing/wiping reports to your mailbox. Simple Mail Transport Protocol (SMTP) is

responsible for transmitting e-mail messages and needs to be configured properly.

These options can be configured in the Free version, but are useable only in the Professional version.

Account Type

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

To

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

From

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

SMTP Server

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

SMTP Port

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

SMTP Server requests authorization

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

6 Glossary of Terms

BIOS settings

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

boot priority

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

compressed cluster

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

cluster

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

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.

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.

deleted boot records

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

ISO

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

lost cluster

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

MFT records

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

root records

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

sector

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

unallocated space

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

unused space in MFT records

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