Active@ KillDisk for Windows

User Guide

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.

Contents

1 Product Overview

Active@ KillDisk for Windows 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 MTF records or root records.

When you erase data with Active@ KillDisk for Windows, you destroy data permanently, conforming to any one of six international standards or your own custom settings.

Wiping drive space or erasing data can take a long time, so perform these operations when you are prepared to wait. For example, these operations may be run overnight.

1.1 Erasing Confidential Data

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

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

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

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

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

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

1.1.1 Advanced Data Recovery Systems

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

Although there are very sophisticated data recovery systems available at a high price, data can 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 Active@ KillDisk for Windows, our powerful and compact utility, all data on your hard drive or removable device can be destroyed without the possibility of future recovery. After using Active@ KillDisk for Windows, 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 for Windows conforms to four international standards for clearing and sanitizing data. You can be sure that once you erase a disk with Active@ KillDisk for Windows, sensitive information is destroyed forever.

Active@ KillDisk for Windows is a quality security application that destroys data permanently from any computer that can be started using a bootable CD or DVD-ROM. 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 Drive 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 conveniently using the Windows Recycle Bin and then emptying the Recycle Bin. While you are still using your local hard drive, there may be confidential information available in these unoccupied drive spaces.

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.

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 root records.

Wiping drive space can take a long time, so perform this operation at a time when you are prepared to wait. For example, it is a process that can be run overnight.

2 System Requirements

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

Personal Computer

IBM PC/AT compatible CPU

Intel Pentium or higher

300 Mb of RAM

Video must be VGA or better resolution (800 x 600)

Drive Storage System

CD or DVD-ROM drive

USB storage device

Hard Disk Drive type IDE, ATA, SATA or SCSI with controllers (additional drivers can be loaded for RAIDs or non-standard controllers after the system is booted up)

Other Requirements

One blank CD or DVD to burn an ISO image.

2.1 Active@ KillDisk for Windows Version

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

Table 2-1 Differences between Free and Professional Versions

Feature	Free Demo Version	Professional Version
Securely overwrites and destroys all data on physical drive or logical partition	yes	yes
Erases partitions, logical drives and unused disk space	yes	yes
Supports IDE / ATA / SATA / SCSI hard disk drives	yes	yes

Feature	Free Demo Version	Professional Version
Supports fixed disks, floppies, zip drives, USB devices	yes	yes
Supports large-sized drives (more than 128 GB)	yes	yes
Supports Command Line mode (can be run with no user interaction)	yes	yes
Operates from bootable CD/DVD-ROM or bootable USB device	yes	yes
Erases with one-pass zeros	yes	yes
Erases with one-pass random characters		yes
Erases with user-defined number of passes (up to 99) and user-defined pattern		yes
US Department of Defense 5220.22 M compliant		yes
Canadian OPS-II compliant		yes
HMG IS5 Baseline and Enhanced compliant		yes
US Army AR380-19 compliant		yes
US Air Force 5020 compliant		yes
Navso P-5329-26 RL and MFM compliant		yes
NCSC-TG-025 compliant		yes
German VISTR compliant		Yes
Russian GOST p50739-95 compliant		Yes
Bruce Schneier compliant		yes
Gutmann method compliant		yes
Customizable security levels		yes
Supports all detected hard disk drives	yes	yes
Erasing report is created and can be saved as a file	yes	yes

Feature	Free Demo Version	Professional Version
Displays detected drive and partition information	yes	yes
Scans NTFS and FAT 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
Wipes out NTFS, FAT32, FAT16 and FAT12 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 and ROOT system records	yes	yes
Wipes out unused space in any MFT records and compressed clusters	yes	yes

3 Running Active@ KillDisk

After you purchase Active@ KillDisk, you will receive an installation file named KILLDISK-SETUP.EXE. This file contains everything you need to get started.

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

The installed application contains two main applications:

- Active@ KillDisk for Windows—Run this application from your Windows operating system to scan local drives.
- Active@ Boot Disk Creator—Create a bootable CD/DVD or USB device and run Active@ KillDisk for Windows from the device. Using Active@ KillDisk this way allows you to wipe confidential data from the system cache and you can gain exclusive use of a partition because the operating system runs outside the partition that you are securing.

3.1 Active@ Boot Disk Creator

Active@ Boot Disk Creator helps you prepare a bootable CD, DVD 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 for Windows:

1. From the Windows Start menu, click All Programs > Active@ KillDisk Professional > Bootable Disk Creator. The Active@ Boot Disk Creator main page appears.
2. Click KillDisk Boot Disk. The KillDisk Boot Disk page appears.
3. To prepare a bootable USB device, skip ahead to step 8.
4. To prepare a bootable CD or DVD:
    a. Click CD/DVD-R Boot Disk. The CD/DVD-R Boot Disk page appears.
    b. Insert a blank or re-writable CD or DVD into the disk writer.
    c. Click Create!. A progress bar appears.
5. After the ISO has been created, you must write it to the bootable CD or DVD.

   If you have Windows Vista or Server 2003, use Windows Burning Engine, integrated with the operating system to write to the CD.

   If you have Windows XP SP1 operating system or lower, you do not have access to Windows Burning Engine. You may use another disk burning utility to burn the ISO to the disk.

6. If you have Windows XP SP2 or higher, you may use another disk burning utility or you may choose to install Windows Burning Engine update, using the steps below.

   To update the Windows Burning Engine:

   a. Open a connection to the Internet.
   b. From the Windows Start button, choose All Programs > Active@ KillDisk Professional > Windows Burning Engine Update. A new session of your default web browser opens to http://www.ntfs.com/burning_engine_update.htm.
   c. Download the file from the ntfs site and install it on your computer.

7. If you choose not to use Windows Burning Engine, you may use Active@ ISO Burner utility. Continue with the steps below.

   a. In the Active@ ISO Burner main page, in the Step 1 area, the path to the ISO appears. To change this path and use a different ISO, click the ellipsis button (...) and navigate to the ISO.
   b. In the Step 2 area, the disk burning device name appears. To use a different disk burning device, select it from the drop-down list.
   c. To choose a different burning speed, select it from the speed drop-down list.
   d. To change burning settings, click the Settings link and change settings on the dialog box.
   e. Click BURN ISO!. A progress bar appears.
   f. After the CD or DVD has been finalized, the disk ejects and a success message box appears. Click OK.
   g. To burn another CD or DVD, insert a blank disk and click BURN MORE!.

8. To prepare a bootable USB mass storage device:

   a. Insert a blank USB mass storage device into any USB port.
   b. Click USB Flash Boot Disk. The USB Flash Boot Disk page appears.
   c. Select the device in the USB Flash Removable Device list.
   d. Click Create!. A progress bar appears.
   e. After the ISO has been created and copied onto the USB device, you must use Safely Remove Hardware to stop and unplug the device.

3.2 Modes of Operation

Active@ KILLDISK for Windows can be used two ways:

- Interactive Mode
- Command Line 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.

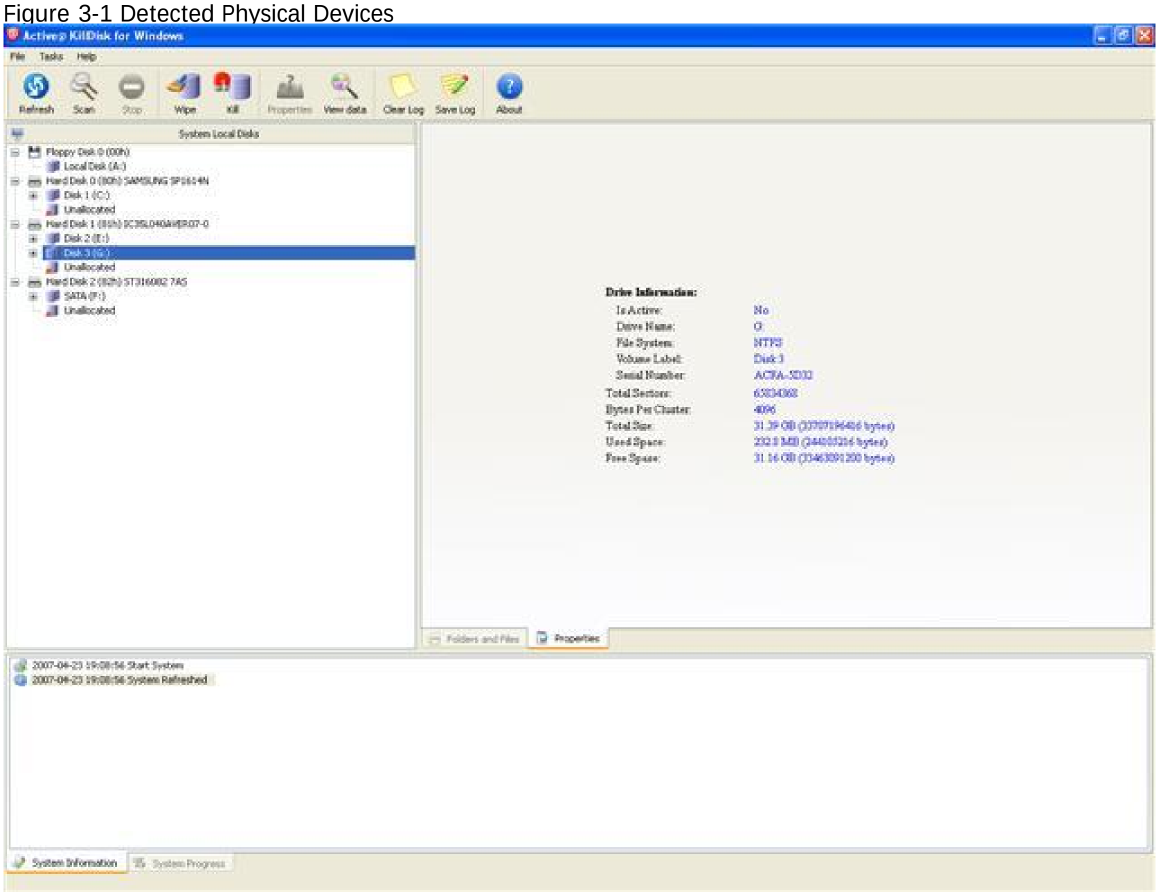
If you are booting from a CD/DVD-ROM drive, check that the drive has boot priority in the BIOS settings of your computer.

Here are the steps for interactive operation:

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

   The Detected Physical Devices screen appears.

Figure 3-1 Detected Physical Devices



```
Floppy Disk 0 (00h)
    Local Disk (A:)
Hard Disk 0 (80h) SAMSUNG SP1614N
    Disk 1 (C:)
    Unallocated
Hard Disk 1 (81h) IC35L040AVER07-0
    Disk 2 (E:)
    Disk 3 (G:)
    Unallocated
Hard Disk 2 (82h) ST316002 7AS
    SATA (F:)
    Unallocated
```

```
Drive Information:
  Is Active:          No
  Drive Name:         G:
  File System:        NTFS
  Volume Label:       Disk 3
  Serial Number:      ACFA-5D32
Total Sectors:        65834368
Bytes Per Cluster:    4096
Total Size:           31.39 GB (33707196416 bytes)
Used Space:           232.8 MB (244105216 bytes)
Free Space:           31.16 GB (33463091200 bytes)
```

```
2007-04-23 19:08:56 Start System
2007-04-23 19:08:56 System Refreshed
```

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

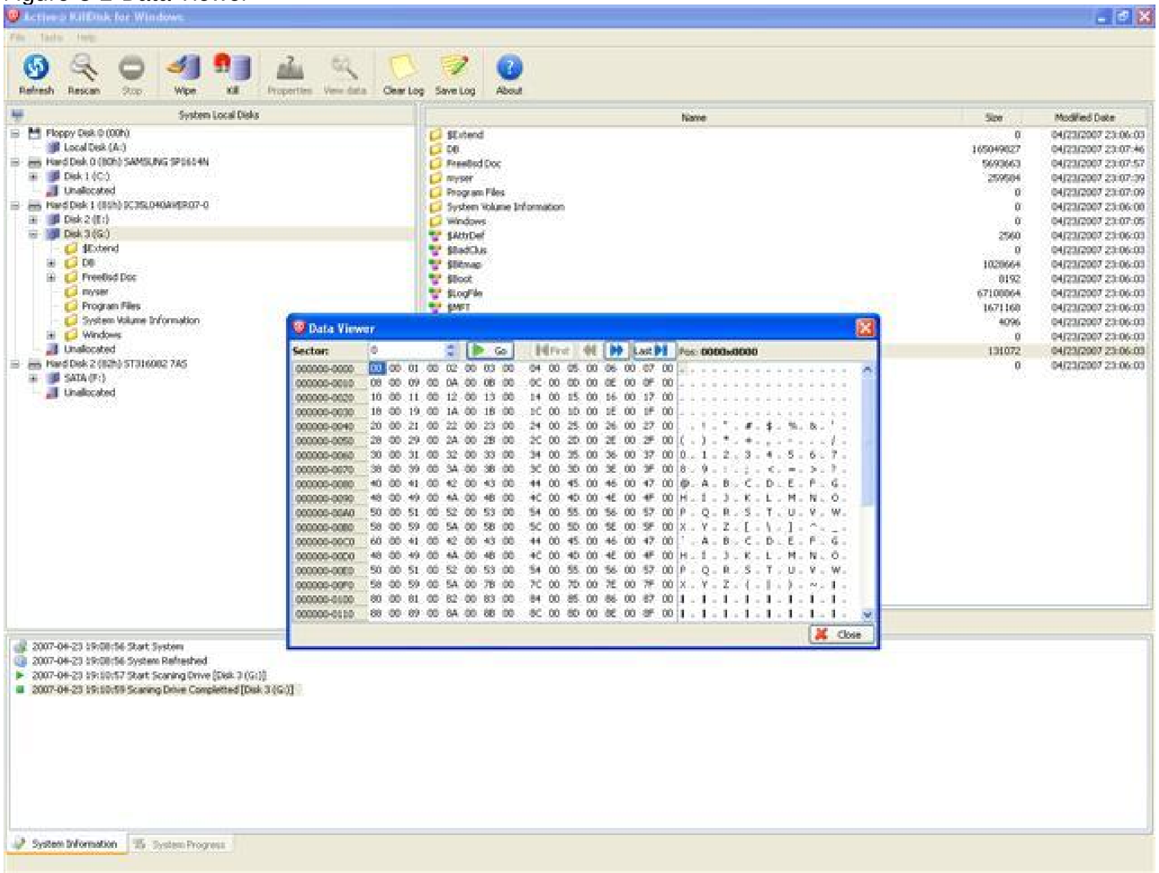
Hard drive devices are numbered by the system BIOS. A system with a single hard drive shows as number 0. Subsequent hard drive devices are numbered consecutively. For example the second device will be shown as Hard Disk 1.

2. Select a device and read the detailed information about the device in the right pane. Below the device, select a logical partition. The information in the right pane changes.

3. Be certain that the drive you are pointing to is the one that you want to erase or the one you want to wipe. If you choose to erase, all data will be permanently erased with no chance for recovery.

   To preview the sectors in a device, press CTRL + V or click View Data on the toolbar. The Data Viewer screen appears.

Figure 3-2 Data Viewer



- Floppy Disk 0 (00h)
  - Local Disk (A:)
- Hard Disk 0 (80h) SAMSUNG SP1614N
  - Disk 1 (C:)
  - Unallocated
- Hard Disk 1 (81h) IC35L040AVER07-0
  - Disk 2 (E:)
  - Disk 3 (G:)
    - $Extend
    - DB
    - FreeBsd Doc
    - myser
    - Program Files
    - System Volume Information
    - Windows
  - Unallocated
- Hard Disk 2 (82h) ST316002 7AS
  - SATA (F:)
  - Unallocated

Name	Size	Modified Date
$Extend	0	04/23/2007 23:06:03
DB	165049027	04/23/2007 23:07:46
FreeBsd Doc	5693663	04/23/2007 23:07:57
myser	259584	04/23/2007 23:07:39
Program Files	0	04/23/2007 23:07:09
System Volume Information	0	04/23/2007 23:06:08
Windows	0	04/23/2007 23:07:05
$AttrDef	2560	04/23/2007 23:06:03
$BadClus	0	04/23/2007 23:06:03
$Bitmap	1028664	04/23/2007 23:06:03
$Boot	8192	04/23/2007 23:06:03
$LogFile	67108864	04/23/2007 23:06:03
$MFT	1671168	04/23/2007 23:06:03
	4096	04/23/2007 23:06:03
	0	04/23/2007 23:06:03
	131072	04/23/2007 23:06:03
	0	04/23/2007 23:06:03

```
Sector: 0                                                 Pos: 0000x0000
000000-0000  00 00 01 00 02 00 03 00  04 00 05 00 06 00 07 00  ................
000000-0010  08 00 09 00 0A 00 0B 00  0C 00 0D 00 0E 00 0F 00  ................
000000-0020  10 00 11 00 12 00 13 00  14 00 15 00 16 00 17 00  ................
000000-0030  18 00 19 00 1A 00 1B 00  1C 00 1D 00 1E 00 1F 00  ................
000000-0040  20 00 21 00 22 00 23 00  24 00 25 00 26 00 27 00  . . ! . " . # . $ . % . & . ' .
000000-0050  28 00 29 00 2A 00 2B 00  2C 00 2D 00 2E 00 2F 00  ( . ) . * . + . , . - . . . / .
000000-0060  30 00 31 00 32 00 33 00  34 00 35 00 36 00 37 00  0 . 1 . 2 . 3 . 4 . 5 . 6 . 7 .
000000-0070  38 00 39 00 3A 00 3B 00  3C 00 3D 00 3E 00 3F 00  8 . 9 . : . ; . < . = . > . ? .
000000-0080  40 00 41 00 42 00 43 00  44 00 45 00 46 00 47 00  @ . A . B . C . D . E . F . G .
000000-0090  48 00 49 00 4A 00 4B 00  4C 00 4D 00 4E 00 4F 00  H . I . J . K . L . M . N . O .
000000-00A0  50 00 51 00 52 00 53 00  54 00 55 00 56 00 57 00  P . Q . R . S . T . U . V . W .
000000-00B0  58 00 59 00 5A 00 5B 00  5C 00 5D 00 5E 00 5F 00  X . Y . Z . [ . \ . ] . ^ . _ .
000000-00C0  60 00 41 00 42 00 43 00  44 00 45 00 46 00 47 00  ` . A . B . C . D . E . F . G .
000000-00D0  48 00 49 00 4A 00 4B 00  4C 00 4D 00 4E 00 4F 00  H . I . J . K . L . M . N . O .
000000-00E0  50 00 51 00 52 00 53 00  54 00 55 00 56 00 57 00  P . Q . R . S . T . U . V . W .
000000-00F0  58 00 59 00 5A 00 7B 00  7C 00 7D 00 7E 00 7F 00  X . Y . Z . { . | . } . ~ . ▌ .
000000-0100  80 00 81 00 82 00 83 00  84 00 85 00 86 00 87 00  ▌ . ▌ . ▌ . ▌ . ▌ . ▌ . ▌ . ▌ .
000000-0110  88 00 89 00 8A 00 8B 00  8C 00 8D 00 8E 00 8F 00  ▌ . ▌ . ▌ . ▌ . ▌ . ▌ . ▌ . ▌ .
```

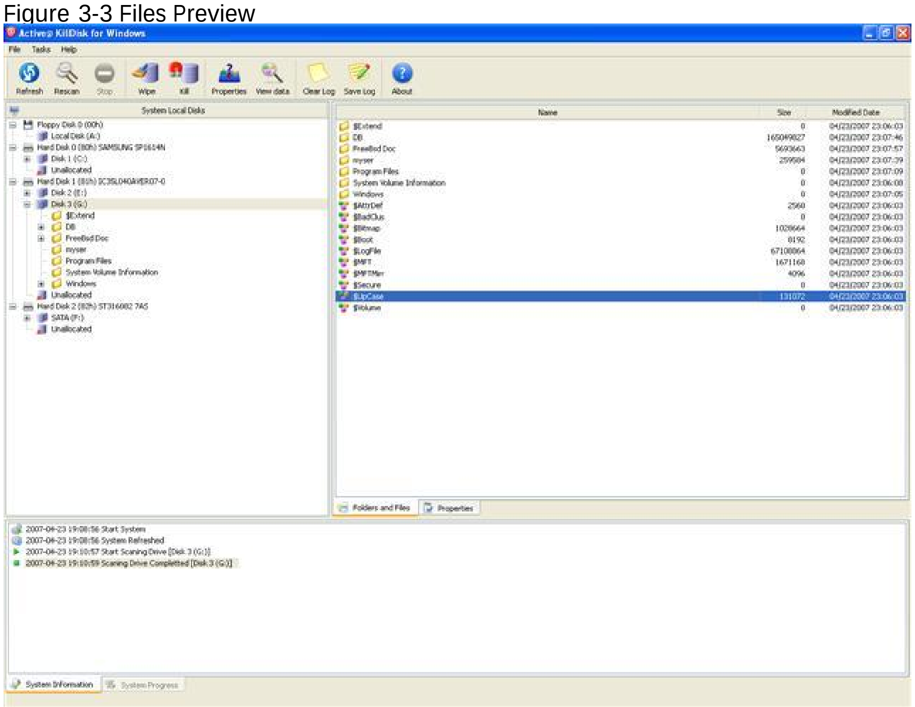
```
2007-04-23 19:08:56 Start System
2007-04-23 19:08:56 System Refreshed
2007-04-23 19:10:57 Start Scaning Drive [Disk 3 (G:)]
2007-04-23 19:10:59 Scaning Drive Completted [Disk 3 (G:)]
```

4. To scroll up and down, use the keyboard arrow keys, PAGE UP, PAGE DOWN, HOME and END navigation keys, or use the related buttons on the toolbar.

5. To jump to a specific sector, in the Sector box, type the sector number and press ENTER or click Go on the toolbar.

6. When you are satisfied with the identification of the device, press ESC to close this screen.
7. To preview the files in a logical partition, select the partition and press ENTER. KillDisk scans the MFT records for the partition. The Folders and Files screen appears.

Figure 3-3 Files Preview



Name	Size	Modified Date
$Extend	0	04/23/2007 23:06:03
DB	165049827	04/23/2007 23:07:46
FreeBsd Doc	5693663	04/23/2007 23:07:57
myser	259584	04/23/2007 23:07:39
Program Files	0	04/23/2007 23:07:09
System Volume Information	0	04/23/2007 23:06:08
Windows	0	04/23/2007 23:07:05
$AttrDef	2560	04/23/2007 23:06:03
$BadClus	0	04/23/2007 23:06:03
$Bitmap	1028664	04/23/2007 23:06:03
$Boot	8192	04/23/2007 23:06:03
$LogFile	67108864	04/23/2007 23:06:03
$MFT	1671168	04/23/2007 23:06:03
$MFTMirr	4096	04/23/2007 23:06:03
$Secure	0	04/23/2007 23:06:03
$UpCase	131072	04/23/2007 23:06:03
$Volume	0	04/23/2007 23:06:03

```
2007-04-23 19:08:56 Start System
2007-04-23 19:08:56 System Refreshed
2007-04-23 19:10:57 Start Scanning Drive [Disk 3 (G:)]
2007-04-23 19:10:59 Scanning Drive Completed [Disk 3 (G:)]
```

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 MFT records for this folder. The files in the folder appear in the right panel. Existing files and folders marked by yellow icons and deleted files and folders marked by gray icons. If you are wiping data from unoccupied areas, the gray-coloured file names are removed after the wiping process completes. You may use Data Viewer to inspect the work done by the wiping process. After wiping, the data in these areas and the place these files hold in the root records or MFT records are gone.

3.2.1.1 Erase Data from a Device

When you select a physical device (for example, Hard Disk 0), the erase command processes partitions no matter what condition they are in. Everything must be destroyed.

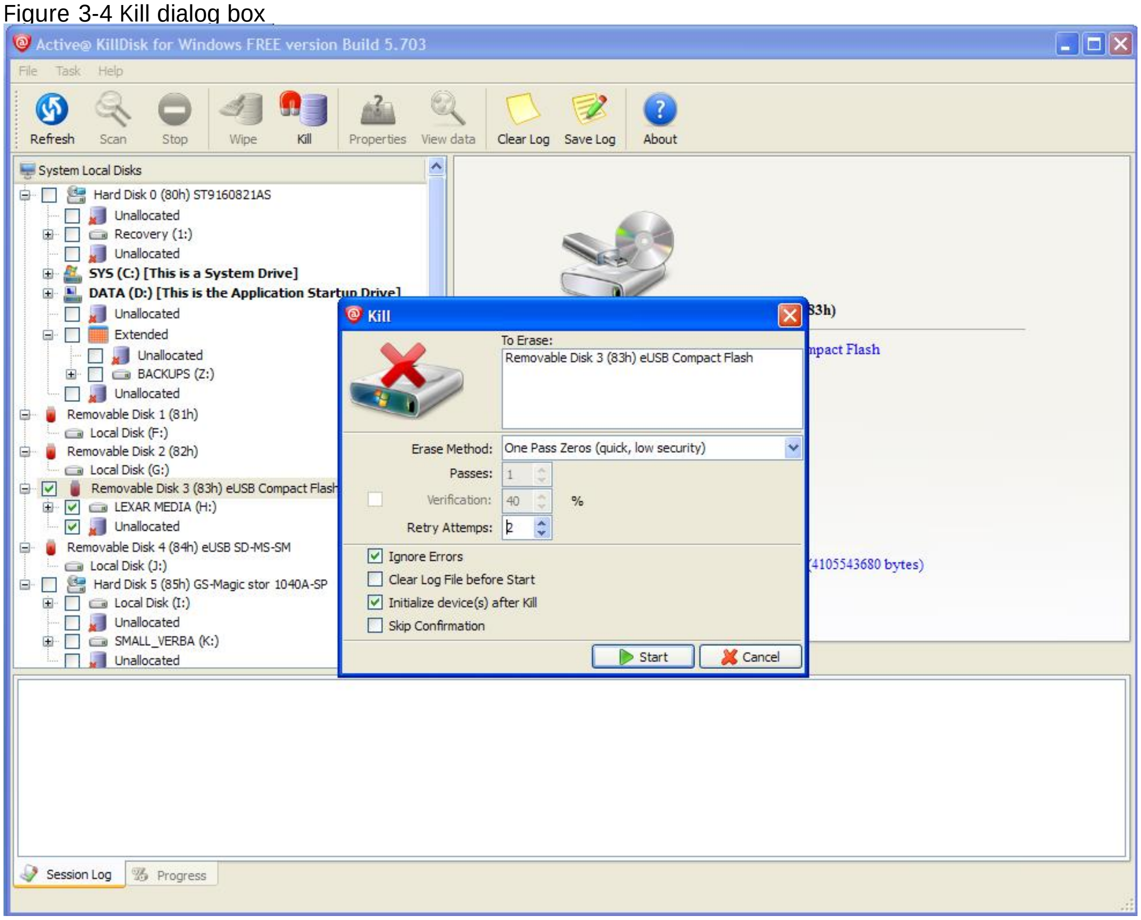
NOTE Because of the BIOS restrictions of some manufacturers, a hard disk device that is larger than 300 MB must have an MBR (Master Boot Record) in sector zero. If you erase sector zero and fill it with zeros or random characters, you might find that you cannot use the hard drive after erasing the data.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

If you want to erase data on selected logical drives, follow the steps in 3.2.3 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.
2. When you have selected the device to erase, select the checkbox for this hard drive. To permanently erase all data on the selected partition, press F10 or click Kill on the toolbar. The Kill dialog box appears.

Figure 3-4 Kill dialog box



System Local Disks

- □ Hard Disk 0 (80h) ST9160821AS
  - □ Unallocated
  - □ Recovery (1:)
  - □ Unallocated
  - SYS (C:) [This is a System Drive]
  - DATA (D:) [This is the Application Startup Drive]
  - □ Unallocated
  - □ Extended
    - □ Unallocated
    - □ BACKUPS (Z:)
  - □ Unallocated
- Removable Disk 1 (81h)
  - Local Disk (F:)
- Removable Disk 2 (82h)
  - Local Disk (G:)
- ☑ Removable Disk 3 (83h) eUSB Compact Flash
  - ☑ LEXAR MEDIA (H:)
  - ☑ Unallocated
- Removable Disk 4 (84h) eUSB SD-MS-SM
  - Local Disk (J:)
- □ Hard Disk 5 (85h) GS-Magic stor 1040A-SP
  - □ Local Disk (I:)
  - □ Unallocated
  - □ SMALL_VERBA (K:)
  - □ Unallocated

83h)

mpact Flash

(4105543680 bytes)

Kill

To Erase: Removable Disk 3 (83h) eUSB Compact Flash

Erase Method: One Pass Zeros (quick, low security)

Passes: 1

□ Verification: 40 %

Retry Attemps: 2

☑ Ignore Errors

□ Clear Log File before Start

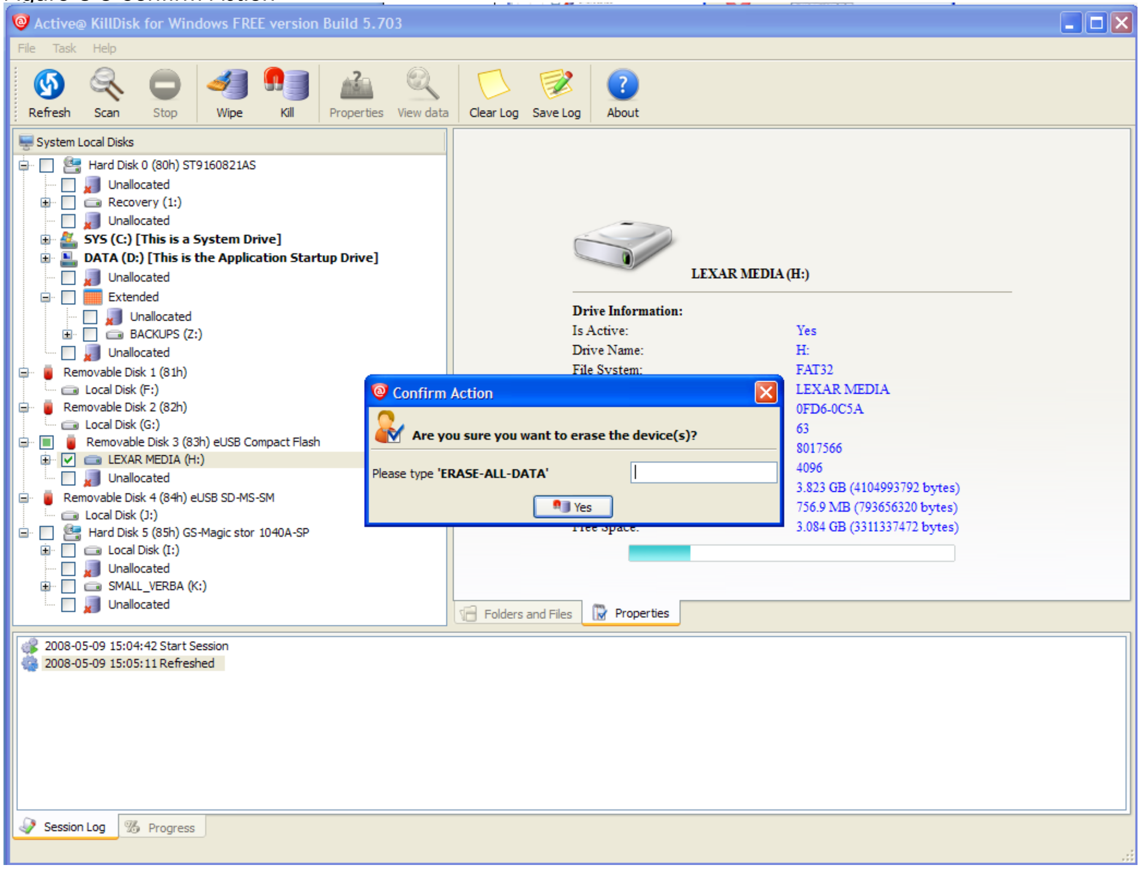
☑ Initialize device(s) after Kill

□ Skip Confirmation

3. To choose an erase method, select one from the drop-down list. Erase methods are described in Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.

4. Set other parameters for erasing. For information on these parameters, see Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.
5. Click Start.
   - If the Skip Confirmation check box is clear, the Confirm Action dialog box appears.

Figure 3-5 Confirm Action



LEXAR MEDIA (H:)

Drive Information:

Is Active:	Yes
Drive Name:	H:
File System:	FAT32
	LEXAR MEDIA
	0FD6-0C5A
	63
	8017566
	4096
	3.823 GB (4104993792 bytes)
	756.9 MB (793656320 bytes)
Free Space:	3.084 GB (3311337472 bytes)

Confirm Action

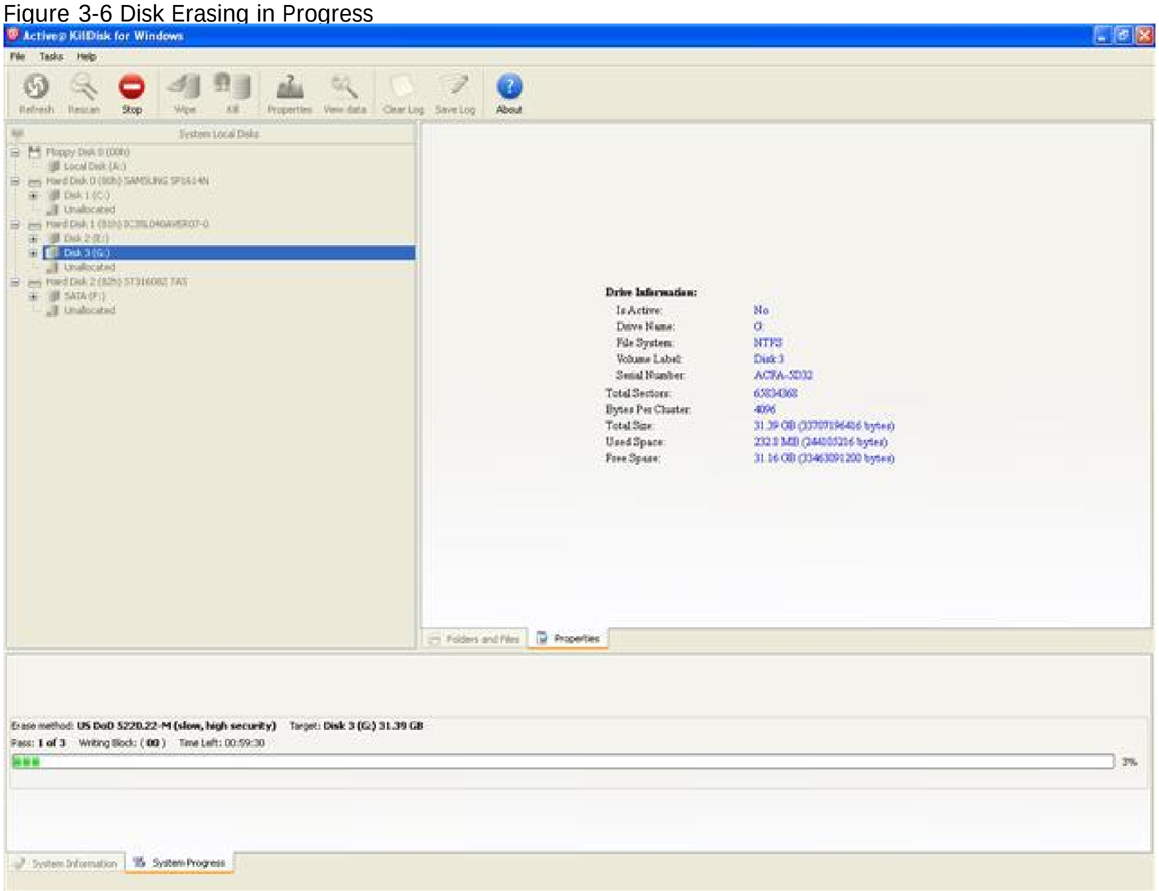
Are you sure you want to erase the device(s)?

Please type 'ERASE-ALL-DATA'

```
2008-05-09 15:04:42 Start Session
2008-05-09 15:05:11 Refreshed
```

6. This is the final step before removing data from the selected drive for ever. Type ERASE-ALL-DATA in the text box and press ENTER or click YES. The Progress bar appears.
7. To stop the process at any time, press ESC. Please note, however that data that has already been erased will not be recoverable.

Figure 3-6 Disk Erasing in Progress



Drive Information:

Is Active:	No
Drive Name:	G:
File System:	NTFS
Volume Label:	Disk 3
Serial Number:	ACFA-3D32
Total Sectors:	65834368
Bytes Per Cluster:	4096
Total Size:	31.39 GB (33707196416 bytes)
Used Space:	232.0 MB (244005216 bytes)
Free Space:	31.16 GB (33463091200 bytes)

Erase method: **US DoD 5220.22-M (slow, high security)** Target: **Disk 3 (G:) 31.39 GB**

Pass: **1 of 3** Writing Block: (**00**) Time Left: 00:59:30

3%

8. There is nothing more to do until the end of the disk erasing process. The application will operate on its own.

   If there are any errors, for example due to bad clusters, they will be reported on the Interactive screen. If such a message appears, you may cancel the operation (by pressing ESC), or you may continue erasing data.

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 that—on hard drives larger than 300 MB—KillDisk creates an empty partition table and writes a typical MBR in sector zero.

3.2.1.2 Wipe Data from a Device

When you select a physical device (for example, Hard Disk 0), the wipe command processes all logical drives consecutively, deleting data in unoccupied areas. Unallocated space is not touched. 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; for example, if there is an unknown file system, or if the disk contains unallocated space. 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 out separately.

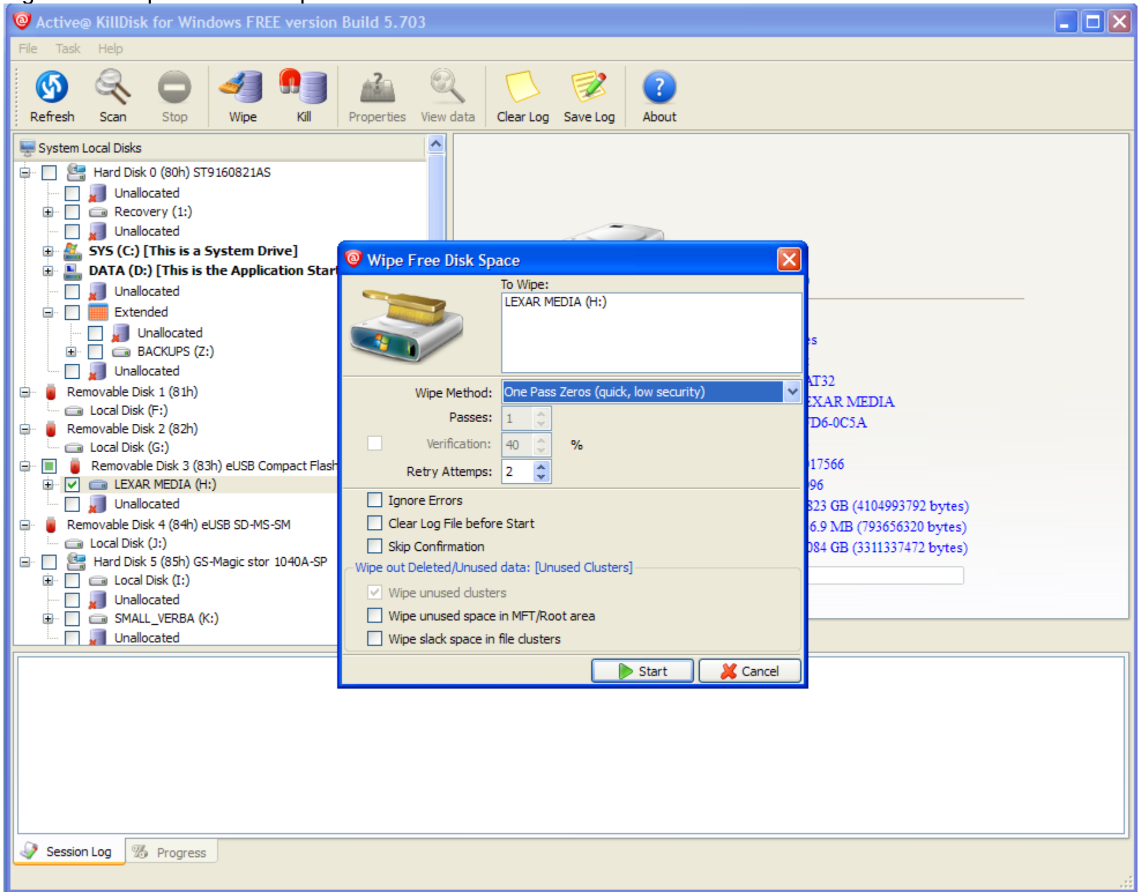
If you want to erase data from the hard drive device permanently, see 3.2.1.1 Erase Data.

If you want to wipe data in unoccupied areas on selected logical drives, follow the steps in 3.2.3 Erase or Wipe Logical Drives (Partitions).

To wipe 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.
2. To wipe all data in unoccupied sectors on the selected partitions, press F9 or click Wipe. The Wipe Free Disk Space dialog box appears.

Figure 3-7 Wipe Free Disk Space



To Wipe: LEXAR MEDIA (H:)

Wipe Method: One Pass Zeros (quick, low security)

Passes: 1

□ Verification: 40 %

Retry Attemps: 2

□ Ignore Errors

□ Clear Log File before Start

□ Skip Confirmation

Wipe out Deleted/Unused data: [Unused Clusters]

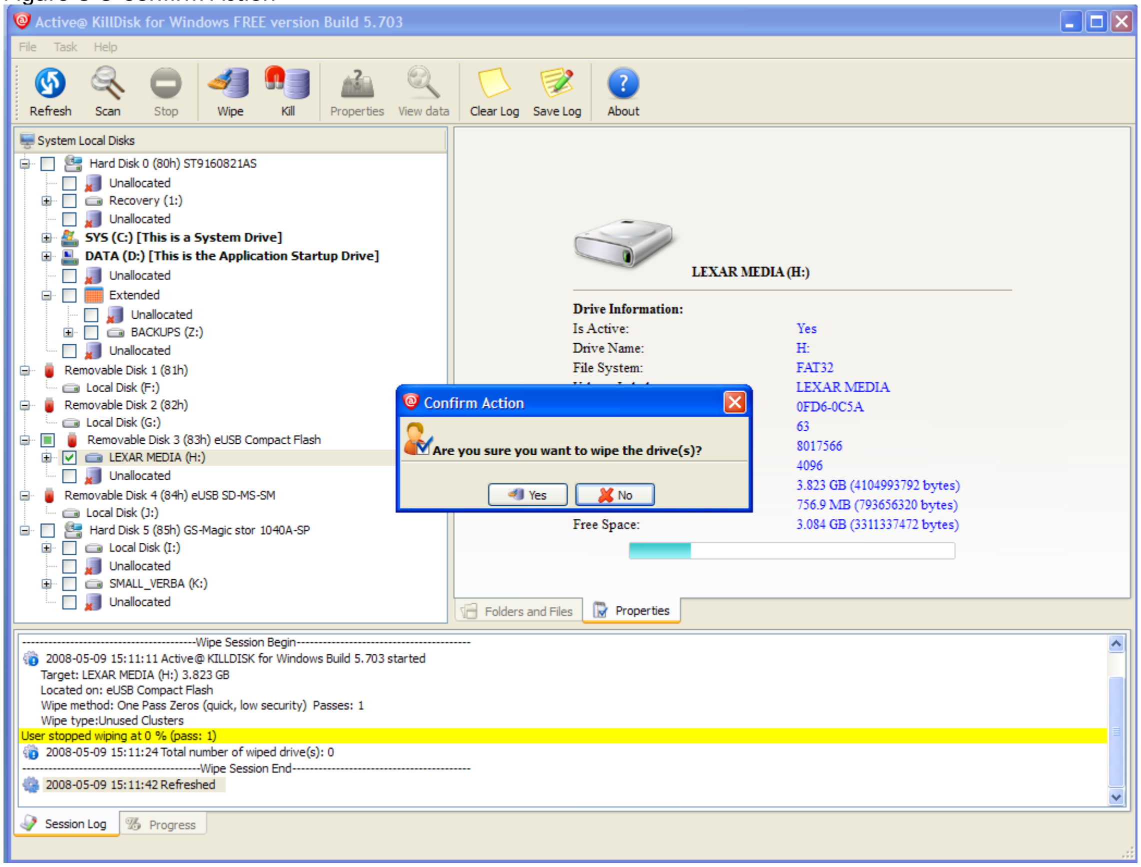
☑ Wipe unused clusters

□ Wipe unused space in MFT/Root area

□ Wipe slack space in file clusters

3. To select a wipe method, choose a method from the Wipe Method drop-down list. Wipe methods are described in Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.
4. You may change other parameters in this dialog box. For information on these parameters, see Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.
5. 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



Are you sure you want to wipe the drive(s)?

LEXAR MEDIA (H:)

Drive Information:

Is Active: Yes

Drive Name: H:

File System: FAT32

LEXAR MEDIA

0FD6-0C5A

63

8017566

4096

3.823 GB (4104993792 bytes)

756.9 MB (793656320 bytes)

Free Space: 3.084 GB (3311337472 bytes)

```
--------------------------------------Wipe Session Begin--------------------------------------
2008-05-09 15:11:11 Active@ KILLDISK for Windows Build 5.703 started
   Target: LEXAR MEDIA (H:) 3.823 GB
   Located on: eUSB Compact Flash
   Wipe method: One Pass Zeros (quick, low security)  Passes: 1
   Wipe type:Unused Clusters
User stopped wiping at 0 % (pass: 1)
2008-05-09 15:11:24 Total number of wiped drive(s): 0
--------------------------------------Wipe Session End--------------------------------------
2008-05-09 15:11:42 Refreshed
```

6. This is the final step before wiping data residue from unoccupied space on the selected drive. After the process has started, you may stop it by pressing the ESC key.

   To confirm the wipe action, click Yes. Progress of the wiping procedure will be monitored in the Disk Wiping screen.
7. To stop the process for any reason, press the ESC key. Please note that all existing applications and data will not be touched, however, data that has been wiped from unoccupied sectors is not recoverable.
8. There is nothing more to do until the end of the disk erasing 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. If such a message appears, you may cancel the operation (by pressing ESC), or you may continue wiping data.

9. After the wiping process is completed, to inspect the work that has been done, select the wiped partition and press ENTER. KillDisk scans the MFT records or the root records of the partition. The Folders and Files tab appears.

   Existing file names and folder names appear with a multi-coloured icon and deleted file names and folder names appear with a gray-coloured icon. If the wiping process completed correctly, the data residue in these deleted file clusters and the place these files hold in the root records or MFT records has been removed and you should not see any gray-coloured file names or folder names in the wiped partition.

3.2.2 Command Line Mode

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

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

```
>killdisk_win.exe -?
```

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

Table 3-2 Command Line Parameters

Parameter	Short	Def.	Options
no parameter			With no parameter, the DOS Interactive screens will appear.
-erasemethod=[0-16]	-em=	0	0 - One pass zeros (1 pass) 1 - One pass random (1 pass) 2 - US DoD 5220.22-M (3 passes, verify) 3 - US DoD 5220.22-M ECE (7 passes, verify) 4 - Canadian OPS-II (7 passes, verify) 5 - HMG IS5 Baseline (1 pass, verify) 6 - HMG IS5 Baseline (3 passes, verify) 7 - Russian GOST p50739-95 (2 passes, verify) 8 - US Army AR380-19 (3 passes, verify)

Parameter	Short	Def.	Options
			9 - US Air Force 5020 (3 passes, verify) 10 - Navso P-5329-26 RL (3 passes, verify) 11 - Navso P-5329-26 MFM (3 passes, verify) 12 - NCSC-TG-025 (3 passes, verify) 13 - German VSITR (7 passes, verify) 14 - Bruce Schneier (7 passes, verify) 15 – Peter Gutmann (35 passes, verify) 16 - User Defined Number of Passes (random) and pattern
-passes=[1 - 99]	-p=	3	Number of times the write heads will pass over a disk area to overwrite data. Valid only for User Defined method (-em=16).
-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 erasemethod (reading 10% of the area by default). It is a long process. Set the verification to the level that works for you.
-retryattempts=[1 - 99]	-ra=	5	Set the number of times that the utility will try to rewrite in the sector when the drive write head encounters an error.
-erasehdd=[80h - 8Fh]	-eh=		Name the hard drive to be erased. By default, the utility erases the first logical drive encountered.
-eraseallhdds	-ea		Erase all hard disk drives.
-ignoreerrors	-ie	OFF	Do not stop erasing each time a disk error is encountered. When you use this parameter, all errors are ignored.
-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. The log file is stored in the same folder where the software is located.
-noconfirmation	-nc		Skip confirmation steps before erasing starts. By default, confirmation steps will

Parameter	Short	Def.	Options
			appear in command line mode for each hard drive or floppy as follows: Are you sure?
-log			Save report and error events to a log file.
-beep	-bp		Beep after erasing is complete.
-wipeallhdds	-wa		Wipe all hard drives.
-wipehdd = [80h-8Fh]	-wh=		Name the hard drive to be wiped.
-test=[fullpath]			If you are having difficulty with Active@ KillDisk for Windows, 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 with no user interaction.
-userpattern= [fullpath]	-u		Full path to a file to get user-defined pattern from. Valid only for User Defined method (-em=16).
-help or -?			Display this list of parameters.

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

Type the command and parameters into the DOS screen at the prompt. Here is an example:

```
>killdisk_win.exe -eh=80 -bm
```

In the example above, data on device 80h will be erased using the default method (one pass zeros) without confirmation and return to the DOS prompt when complete.

Here is another example:

```
>killdisk_win.exe -eh=80 -nc -em=2
```

In this example, erase all data on device 80h without confirmations, using US DoD 5220.22-M method, and show a report at the end of the process.

Here is an example with the wipe disk command:

```
>killdisk_win.exe -wa -bm -em=15 -nc
```

Wipe all deleted data and unused clusters on all attached drives without confirmation using Gutman's method and return to the DOS prompt when complete.

Press ENTER to complete the command and start the process.

After operation has completed successfully information on how drives have been erased is displayed on the screen.

3.2.3 Erase or Wipe Logical Drives (Partitions)

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

There are some cases where partitions on a device cannot be wiped; for example, if there is an unknown file system, or if the disk contains unallocated space. In these cases, the Wipe button is disabled.

To perform the Wipe or Erase action you must lock the partition first. If another user or an application is using files on the partition, it cannot be locked. In this case a dialog box appears with information that the disk is being used and you need either skip it, or perform a “hard drive dismount”. If you skip it, the wipe or erase operation is canceled for this drive. If you select “hard dismount”, some data in the drive’s cache may be lost.

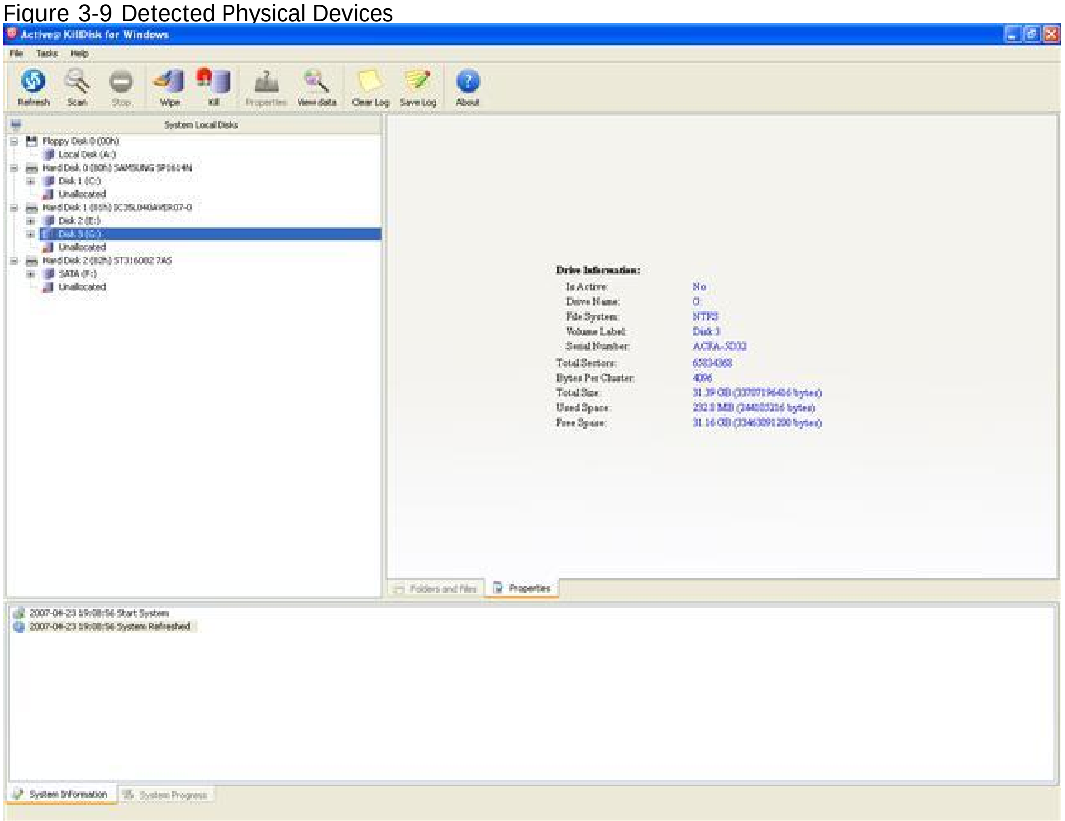
3.2.3.1 Erase Data from a Logical Drive

To erase data from a logical drive:

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

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

Figure 3-9 Detected Physical Devices



Floppy Disk 0 (00h)
Local Disk (A:)
Hard Disk 0 (80h) SAMSUNG SP1614N
Disk 1 (C:)
Unallocated
Hard Disk 1 (81h) IC35L040AVER07-0
Disk 2 (E:)
Disk 3 (G:)
Unallocated
Hard Disk 2 (82h) ST316002 7AS
SATA (F:)
Unallocated

Drive Information:

Is Active:	No
Drive Name:	G:
File System:	NTFS
Volume Label:	Disk 3
Serial Number:	ACFA-3D32
Total Sectors:	65834368
Bytes Per Cluster:	4096
Total Size:	31.39 GB (33707196416 bytes)
Used Space:	232.3 MB (244035216 bytes)
Free Space:	31.16 GB (33463091200 bytes)

```
2007-04-23 19:08:56 Start System
2007-04-23 19:08:56 System Refreshed
```

3. Select the check box of a logical drive or next to the Unallocated area.
4. Press F10 or click Kill. The Kill dialog box appears.
5. Set erase method and set other parameters for erasing. For information on these parameters, see Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.
6. Complete the process, similar to the process for devices.

3.2.3.2 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 Detected Physical Devices screen appears.

   All system hard drives and floppy 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 drive.
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 Descriptions of Erase/Wipe Parameters in this guide.
6. Complete the process, similar to the process for devices.

3.3 Erase or Wipe Operation Complete

After operation is completed successfully, information on how drives have been erased or wiped is displayed. An example of an erase session is displayed below.

```
------------- Erase Session -----------------------

Active@ KillDisk for Windows Build 5.703 started at:
Thu Feb 20 11:56:51 2008

Target: Hard Disk 1

Erase method: US DoD 5220.22-M Passes:3

Verification:40% (completed successfully)

Time taken: 00:01:26

Total number of erased device(s), partition(s): 1
```

If the process encountered errors, for example from bad clusters, a summary of errors is presented in this report. Use the keyboard arrow keys to scroll through the report.

To save the log file, press F2. Details of this report are saved to a log file located in the folder from which you started Active@ KillDisk.

4 Common Questions

4.1 How does the licensing work?

The software is licensed on a per CD/DVD or USB 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. To erase data it overwrites all addressable locations on the drive with zeros (FREE version). 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; and 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 location; Enterprise License - in any location.

4.4 Which operating systems are supported by Active@ KillDisk?

Active@ KillDisk for Windows runs in its own operating system. As it can be installed easily onto a bootable CD/DVD, it does not matter which operating system is installed on the machine hard drive. If you can boot from the boot CD/DVD, you can detect and erase any drives independent of the installed operating system.

4.5 Is Active@ KillDisk for Windows compatible with Macintosh computers?

You cannot run Active@ KillDisk in the MacOS environment. However, the most recent Macintosh computers are based on the Intel architecture. In this case, it is possible to boot from Active@ BootDisk 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?

To be able to use HDD again you need to:

- Repartition the hard drive using a standard DOS utility like FDISK.
- Reformat partitions using a standard DOS utility like FORMAT.
- Reinstall the Operating System using a bootable CD-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 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 Descriptions of Erase/Wipe Parameters

Whether you choose to erase data from the drive or to wipe data from unoccupied drive space, the methods of writing over these spaces is 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 and pattern to be written.

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.

US DoD 5220.22-M (ECE)

The write head passes over each sector seven times. The first time with zeros (0x00), second time with 0xFF and the third time with random characters, the fourth time with 0x96, and then first three passes repeated again. There is one final pass to verify random characters by reading.

German VSITR

The write head passes over each sector seven times, each pass writing the following characters: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.

Russian GOST p50739-95

The write head passes over each sector two times, first pass is zeroes (0x00), the second pass is random characters.

Canadian OPS-II

The write head passes over each sector seven times, each pass writing the following characters: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, Random.

HMG IS5 Baseline

The write head passes over each sector once, writing zeroes (0x00).

HMG IS5 Enhanced

The write head passes over each sector three times, writing zeroes (0x00), then 0xFF, and finally random characters.

US Army AR380-19

The write head passes over each sector three times, first pass writing random characters, then zeroes (0x00), and finally 0xFF.

US Air Force 5020

The write head passes over each sector three times, first pass writing 0xFF, then zeroes (0x00), and finally random characters.

Navso P-5329-26 RL

The write head passes over each sector three times, first pass writing 0x01, then 0x27FFFFFF, and finally random characters.

Navso P-5329-26 MFM

The write head passes over each sector three times, first pass writing 0x01, then 0x7FFFFFFF, and finally random characters.

NCSC-TG-025

The write head passes over each sector three times, first pass writing zeroes 0x00, then 0xFF, and finally random characters.

Bruce Schneier

The write head passes over each sector seven times, each pass writing the following characters: 0xFF, zeroes (0x00), then five passes with random character.

Gutmann

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

```
 http://www.cs.auckland.ac.nz/~pgut001/pubs/se
cure_del.html
```

5.2 Other Parameters

Other parameters allow you to turn features on or off or to change default settings when you are erasing data or wiping data from unoccupied space.

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.

Retry Attempts

If an error is encountered while writing data onto the drive (for example, due to physical damage on the drive's surface), Active@ KillDisk tries to perform the write operation again. You can specify number of retries to be performed.

Sometimes, if the drive surface is not completely damaged, a damaged sector can be overwritten after several retries.

Ignore Errors

If this option is turned on, error messages will not be displayed while data erasing or verification is in progress.

When ignore error messages is turned on, all information about these errors is written to the KILLDISK.LOG file. These messages are displayed after the process is complete in the final Erasing Report.

Clear Log File before Start

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

Skip Confirmation

The confirmation screen is the final step before either erasing or wiping 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 to be used with caution by advanced users in order to speed up the process.

It is safer to run KillDisk with this option selected (default state). 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.

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. Select the parameter and press ENTER to choose from the list of 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.

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. (See lost cluster)

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.

Windows system caching

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

Windows system records

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