Active@ KillDisk

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

This chapter gives an overview of Active@ KillDisk for Hard Drives application.

1.1 Erasing Confidential Data

Although modern methods of data encryption are deterring unwanted network attackers from extracting sensitive data from stored database files, attackers wishing 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 supposedly-erased data from a discarded hard disk drive. When deleting confidential data from hard drives or removable floppies, 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. 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 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 are 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 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 Partial Response Maximum Likelihood (PRML), a technique used to reconstruct the data on magnetic disks. Other methods include the use of magnetic force microscopy and recovery of data based on patterns in erase bands.

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

Using Active@ KillDisk for Hard Drives, our powerful and compact utility, all data on your hard drive or removable floppy drive can be destroyed without the possibility of future recovery. After using Active@ KillDisk for Hard Drives, 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 Hard Drives conforms to four international standards for clearing and sanitizing data. You can be sure that once you erase a disk with Active@ KillDisk for Hard Drives, sensitive information is destroyed forever.

Active@ KillDisk for Hard Drives is a quality security application that destroys data permanently from any computer that can be started using a DOS floppy disk. Access to the drive's data is made on the physical level via the Basic Input-Output Subsystem (BIOS), 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, it can be DOS, Windows 95/98/ME, Windows NT/2000/XP, Linux or UNIX for PC.

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 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 Microsoft DOS. As a result, the process does not depend on Windows system caching and 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 Hard Drives.

2.1 Personal Computer

IBM PC/AT compatible CPU

Operates with processors as old as Intel 286

640 Kb of RAM

Video must be EGA or better resolution

2.2 Drive Storage System

1.44 Mb floppy diskette drive or CD-ROM drive

Hard Disk Drive type IDE, ATA, SATA or SCSI with controllers

2.3 Other Requirements

One blank 3.5-inch or 5.25-inch floppy disk suitable for formatting or a blank CD-ROM to burn an ISO image.

Alternately use a Windows 95/98/ME Startup Disk.

2.4 Active@ KillDisk for Hard Drives Version

The performance of Active@ KillDisk for Hard Drives 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	✓	✓
Erases partitions, logical drives and unused disk space	✓	✓
Supports IDE / ATA / SATA / SCSI hard disk drives	✓	✓
Supports fixed disks, floppies, zip drives, FlashMedia drives	✓	✓

Feature	Free Demo Version	Professional Version
Supports large-sized drives (more than 128GB)	✓	✓
Supports Command Line mode (can be run with no user interaction)	✓	✓
Operates from floppy disk or bootable CD-ROM drive	✓	✓
Erases with one-pass zeros	✓	✓
Erases with one-pass random characters		✓
Erases with user-defined number of passes (up to 99)		✓
US Department of Defense 5220.22 M compliant		✓
German VISTR compliant		✓
Russian GOST p50739-95 compliant		✓
Gutmann method compliant		✓
Customizable security levels		✓
Supports all detected hard disk drives	✓	✓
Erasing report is created and can be saved as a file	✓	✓
Includes Console Application to run and erase data under Windows	✓	✓
Displays detected drive and partition information	✓	✓
Scans NTFS and FAT volumes and displays existing and deleted files and folders	✓	✓
Data verification may be performed after erasing is completed		✓
Disk Viewer allows you to preview any sectors or file clusters on a drive	✓	✓

Feature	Free Demo Version	Professional Version
Operates in DOS real mode, the most secure and reliable environment	✓	✓
Wipes out NTFS, FAT32, FAT16 and FAT12 volumes from areas containing deleted and unused data	✓	✓
Wipes out free clusters (unused by file data sectors)	✓	✓
Wipes out file slack space (unused bytes in the last cluster occupied by file)	✓	✓
Wipes out deleted MFT and ROOT system records	✓	✓
Wipes out unused space in any MFT records and compressed clusters	✓	✓

3 Running Active@ KillDisk

After you purchase Active@ KillDisk, you will receive a self-extracting file named KD-SETUP.EXE. This file contains everything you need to set up and run the application. Double-click KD-SETUP.EXE to extract a list of files. Use these files while following the steps to prepare a bootable disk.

3.1 Preparing a DOS-Bootable Floppy Disk

Active@ KillDisk for Hard Drives is a powerful utility with a small footprint. It is small enough to operate from a single floppy drive in a Microsoft DOS environment. This can be useful in a number of situations. For example, a computer technician who is assigned to erase the data on PCs with hard drives containing Windows operating systems or operating systems other than DOS or Windows can use a single DOS-bootable floppy to erase all data.

This chapter describes the steps to create a DOS-bootable floppy (a startup disk) and run the utility. If you have a bootable floppy, skip to the Copy Active@ KillDisk to a Floppy section, below.

If you want to create a bootable CD ROM, follow instructions in 3.2 Preparing a Bootable CD.

3.1.1 System Formatting

To prepare a bootable floppy from MS-DOS, Windows 95/98/ME/XP, put a blank 3.5-inch floppy in the floppy drive (drive A:) and follow the appropriate instructions below.

Windows 95/98 MS-DOS or Command Prompt Mode

1. On the screen, type the format command as follows:

```
FORMAT A: /S
```

2. Follow on-screen messages until process is complete.

Windows 95/98/ME Operating System

1. Click the **Start** button and click **Settings** > **Control Panel**.
2. From the **Control Panel** screen, click **Add/Remove Programs**.
3. In the **Add/Remove Programs** screen, click the **Startup Disk** tab.
4. Click **Startup Disk...** and follow the screen instructions until the process is complete.

Windows XP Operating System

1. Right-click A: drive.
2. From the drop-down menu, click **Format**...
3. Select the check box beside **Create an MS-DOS startup disk**.
4. Click the **Start** button and follow the screen instructions until the process is complete.

3.1.2 Copying KILLDISK.EXE, DOS4GW.EXE Files to a Floppy

Copy the Active@ KillDisk for Hard Drives file (KILLDISK.EXE) and DOS-extender file (DOS4GW.EXE) to the bootable floppy disk or startup disk in drive A:.

If you don't have the Active@ KillDisk for Hard Drives file, download it from http://www.killdisk.com/downloadfree.htm.

After copying the file onto the floppy disk, remove it from the floppy drive.

Labeling the Disk

If you plan to use Active@ KillDisk for Hard Drives in Command Line mode, please skip the next section and read Boot to DOS (Command Line Mode). Once preparation of the bootable 3.5-inch floppy disk is complete, you are ready to begin removing data.

3.1.3 One-Step Method

Combine all the above steps into one by navigating to our Web site.

Download and run Bootable Floppy Disk Creator for Active@ KillDisk.

Once you have installed Active@ KillDisk on the floppy, you are ready to boot from the floppy and use the software for disk erasing.

3.2 Preparing a Bootable CD

This chapter describes how to create a DOS-bootable CD-ROM that contains the Active@ KillDisk application.

After you have uncompressed KD-SETUP.EXE, find the ISO file: KILLDISK.ISO. This file contains everything you need to boot and launch Active@ KillDisk from a CD.

There is a similar ISO file available for the free version of KillDisk. The file name in the free version is BOOT-DSK.ISO and you may download it from this link: Download Bootable ISO Image of Active@ KillDisk to burn CD.

Burn KILLDISK.ISO to a blank CD and you are ready to use Active@ KillDisk.

Most CD-R writing software includes a feature to write the contents of an ISO file to a CD. Below are instructions for some popular applications.

ISO Recorder Power Toy (Freeware)

ISO Recorder is a Windows XP freeware utility that uses native Windows XP functions to write images to a CD. You can download this utility from the author's Web page. When the program is installed, it is automatically associated with the ISO file extension in Windows Explorer.

For more information about this utility, visit the author's Web page at http://isorecorder.alexfeinman.com/isorecorder.htm

To create a CD using ISO Recorder Power Toy:

1. Insert a blank CD in your CD-RW drive.
2. Start **Windows Explorer**.
3. Locate the ISO file. Right-click the file name and then click **Copy image to CD**. The **ISO Recorder Wizard** appears.
4. Follow the steps in the wizard to write the image to the CD.

Another alternate method:

1. In Microsoft Explorer, right-click your CD drive and choose **Copy Image to CD**.
2. In the new window browse to the ISO file and click **Next**.

Nero - Burning ROM (Ahead Software)

You can use Nero Burning ROM to record a CD from an ISO file. For more information about this program, visit the Ahead Software Web site at: http://www.ahead.de

To create a CD if you have installed Nero - Burning ROM:

1. Insert a blank CD in your CD-RW drive.
2. Start **Nero Burning**.
3. Follow the wizard steps to burn a **Disk Image**.
4. In the **Open** dialog box, select the ISO file, and then click **Open**.
5. In the wizard, click **Burn** to write the image to the CD.

EasyCD Creator (Roxio)

You can use EasyCD Creator to create a CD from an ISO file. When the program is installed, it is automatically associated with the ISO file extension in Windows Explorer. For more information about this program, visit the Roxio Web site at: http://www.roxio.com

Steps to create a CD if you have installed EasyCD Creator:

1. Insert a blank CD in your CD-RW drive.
2. Start **Windows Explorer**.

3. Locate the ISO file. Right-click the file name, and then click **Open** to start EasyCD.
4. In the **Write Method** section of the **CD Creation Setup** dialog box, click **Disk at Once** for optimum recording performance.
5. To write the image to the CD, click **OK**.

WinISO

WinISO is a CD-ROM image file utility that can convert binary files to ISO, extract/edit/create ISO files directly, make bootable CDs and act as a BIN/ISO converter/extractor/editor. For more information, visit http://www.winiso.com.

UltraISO

This tool allows you to create, edit, convert and burn CD and DVD images. Files and folders can be extracted from ISO/BIN files, and you can make ISO from your DVD or CD-ROM or hard disk. For more information, visit http://www.tucows.com/preview/306129.

3.3 Modes of Operation

Active@ KILLDISK for Hard Drives can be used three ways:

- DOS Interactive Mode
- Command Line Mode
- Autoexecute Mode

It is wise to label the floppy disk to identify the way you plan to use Active@ KILLDISK for Hard Drives.

DOS Interactive Mode and Command Line Mode are similar in that you can control what happens after the utility has started. In Autoexecute Mode, however, Active@ KILLDISK for Hard Drives will start immediately upon completion of the bootstrap startup (depending on the automatic settings).

3.3.1 DOS Interactive Mode

This section describes how to use the DOS Interactive screens. For “hands-off” operation, see 3.3.3 Autoexecute Mode.

The steps for erasing data and wiping data are similar. Follow steps 1 through 13 and then click the link to complete either the erasing process or the wiping process.

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

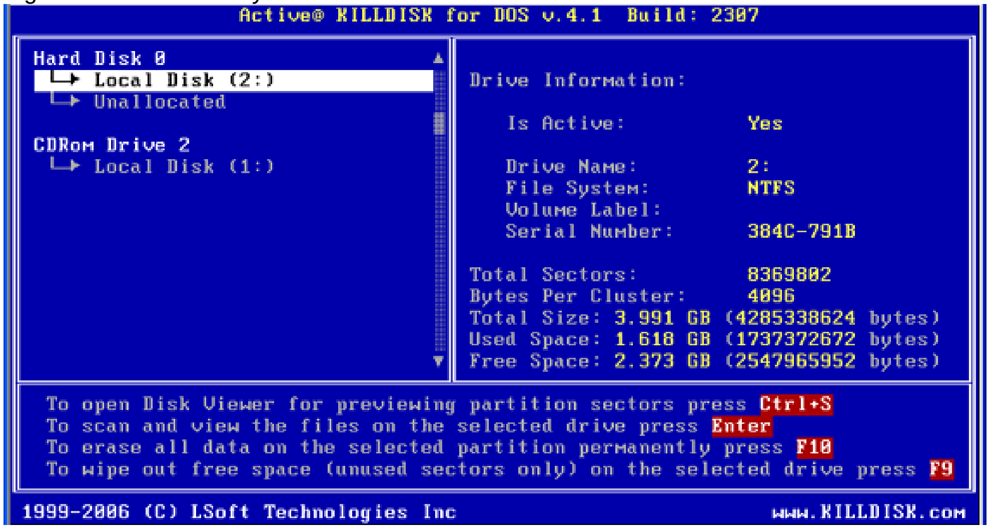
Here are the steps for interactive operation:

1. With the PC power off, insert either the Active@ KILLDISK bootable floppy disk into drive A: or the Active@ KILLDISK bootable CD into your CD-ROM drive.
2. Start the PC by turning on the power. The screen will display the Microsoft DOS prompt.
3. At the DOS prompt, run Active@ KILLDISK for Hard Drives by typing:

   KILLDISK.EXE

   The Detected Physical Devices screen appears.

Figure 3-1 Detected Physical Devices



```
Active@ KILLDISK for DOS v.4.1  Build: 2307

Hard Disk 0                          Drive Information:
 └→ Local Disk (2:)
 └→ Unallocated                        Is Active:          Yes

CDRom Drive 2                          Drive Name:         2:
 └→ Local Disk (1:)                    File System:        NTFS
                                       Volume Label:
                                       Serial Number:      384C-791B

                                     Total Sectors:        8369802
                                     Bytes Per Cluster:    4096
                                     Total Size: 3.991 GB (4285338624 bytes)
                                     Used Space: 1.618 GB (1737372672 bytes)
                                     Free Space: 2.373 GB (2547965952 bytes)

  To open Disk Viewer for previewing partition sectors press Ctrl+S
  To scan and view the files on the selected drive press Enter
  To erase all data on the selected partition permanently press F10
  To wipe out free space (unused sectors only) on the selected drive press F9

1999-2006 (C) LSoft Technologies Inc                        www.KILLDISK.com
```

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

4. Change the position of the cursor in the list using the keyboard **[Down]** and **[Up]** arrow keys. A list of commands is displayed below the device list.

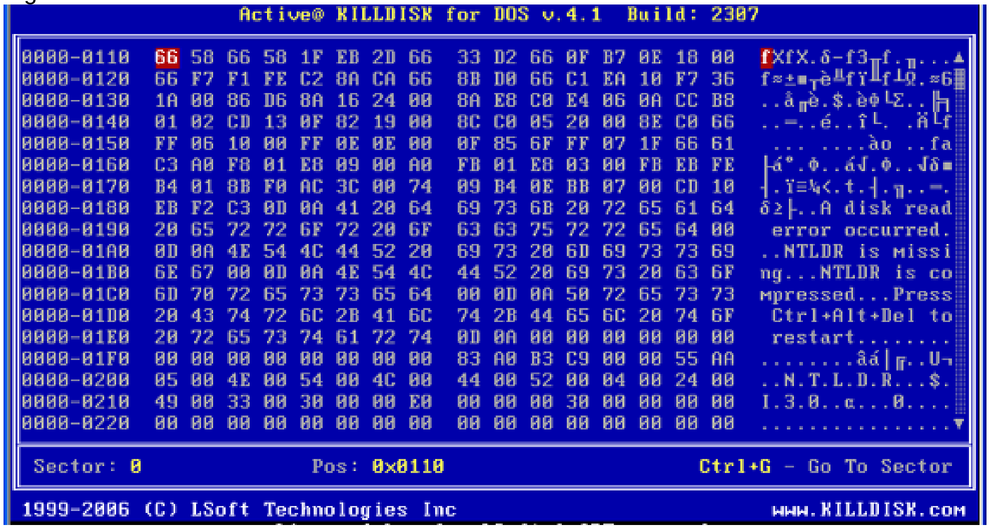
   Hard drive devices are numbered by the system BIOS. A system with a single hard drive shows as number 0. Subsequent hard drive devices are numbered consecutively. For example the second device will be shown as **Hard Disk 1**.

   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. As well, the list of commands changes.

5. 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 + S]**. The **Preview Sector** screen appears.

Figure 3-2 Preview Sector



```
                 Active@ KILLDISK for DOS v.4.1  Build: 2307

0000-0110  66 58 66 58 1F EB 2D 66  33 D2 66 0F B7 0E 18 00  fXfX.δ-f3╥f.╖...
0000-0120  66 F7 F1 FE C2 8A CA 66  8B D0 66 C1 EA 10 F7 36  f≈±■┬è╨fÿ╨f┴Ω.≈6
0000-0130  1A 00 86 D6 8A 16 24 00  8A E8 C0 E4 06 0A CC B8  ..å╓è.$.èΦ└Σ..╠
0000-0140  01 02 CD 13 0F 82 19 00  8C C0 05 20 00 8E C0 66  ..═..é..î└. .Ä└f
0000-0150  FF 06 10 00 FF 0E 0E 00  0F 85 6F FF 07 1F 66 61   ... ....ào ..fa
0000-0160  C3 A0 F8 01 E8 09 00 A0  FB 01 E8 03 00 FB EB FE  ├á°.Φ..á√.Φ..√δ■
0000-0170  B4 01 8B F0 AC 3C 00 74  09 B4 0E BB 07 00 CD 10  ┤.ï≡¼<.t.┤.╖..═.
0000-0180  EB F2 C3 0D 0A 41 20 64  69 73 6B 20 72 65 61 64  δ≥├..A disk read
0000-0190  20 65 72 72 6F 72 20 6F  63 63 75 72 72 65 64 00   error occurred.
0000-01A0  0D 0A 4E 54 4C 44 52 20  69 73 20 6D 69 73 73 69  ..NTLDR is missi
0000-01B0  6E 67 00 0D 0A 4E 54 4C  44 52 20 69 73 20 63 6F  ng...NTLDR is co
0000-01C0  6D 70 72 65 73 73 65 64  00 0D 0A 50 72 65 73 73  mpressed...Press
0000-01D0  20 43 74 72 6C 2B 41 6C  74 2B 44 65 6C 20 74 6F   Ctrl+Alt+Del to
0000-01E0  20 72 65 73 74 61 72 74  0D 0A 00 00 00 00 00 00   restart........
0000-01F0  00 00 00 00 00 00 00 00  83 A0 B3 C9 00 00 55 AA  ........âá│╔..U¬
0000-0200  05 00 4E 00 54 00 4C 00  44 00 52 00 04 00 24 00  ..N.T.L.D.R...$.
0000-0210  49 00 33 00 30 00 00 E0  00 00 00 30 00 00 00 00  I.3.0..α...0....
0000-0220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................

 Sector: 0                 Pos: 0x0110                Ctrl+G - Go To Sector

1999-2006 (C) LSoft Technologies Inc                          www.KILLDISK.com
```

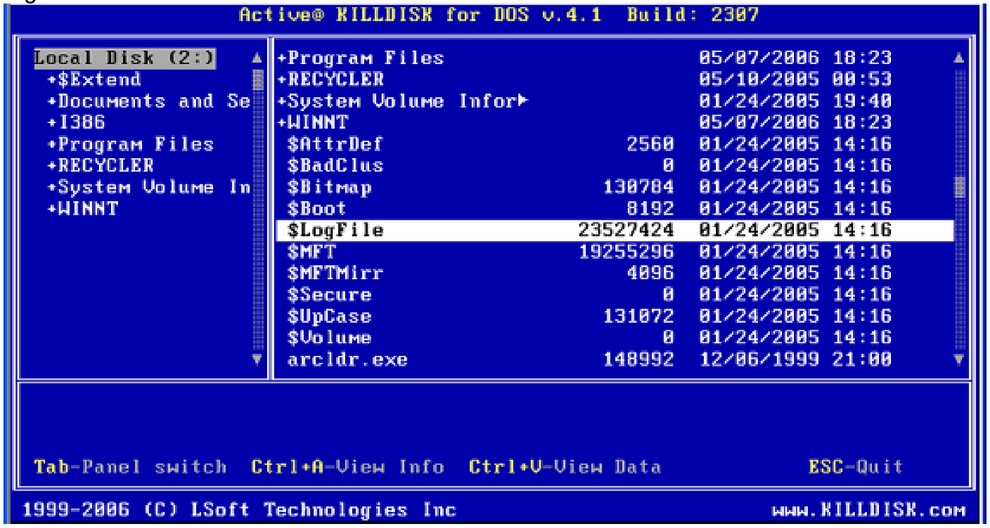
6. To scroll up and down, use the keyboard arrow keys, **[Page Up], [Page Down], [Home]** and **[End]** navigation keys.

7. To jump to a specific sector, press **[Ctrl + G]**.

8. When you are satisfied with the identification of the device, press **[Esc]** to exit this screen.

9. To preview the files in a logical partition, select the partition and press **[Enter]**. KillDisk scans the MFT records for the partition. The Files Preview screen appears.

Figure 3-3 Files Preview



```
                 Active@ KILLDISK for DOS v.4.1  Build: 2307

 Local Disk (2:)      +Program Files                    05/07/2006 18:23
  +$Extend            +RECYCLER                         05/10/2005 00:53
  +Documents and Se   +System Volume Infor►             01/24/2005 19:40
  +I386               +WINNT                            05/07/2006 18:23
  +Program Files       $AttrDef                  2560   01/24/2005 14:16
  +RECYCLER            $BadClus                     0   01/24/2005 14:16
  +System Volume In    $Bitmap                 130784   01/24/2005 14:16
  +WINNT               $Boot                     8192   01/24/2005 14:16
                       $LogFile              23527424   01/24/2005 14:16
                       $MFT                  19255296   01/24/2005 14:16
                       $MFTMirr                  4096   01/24/2005 14:16
                       $Secure                      0   01/24/2005 14:16
                       $UpCase                 131072   01/24/2005 14:16
                       $Volume                      0   01/24/2005 14:16
                       arcldr.exe              148992   12/06/1999 21:00


 Tab-Panel switch  Ctrl+A-View Info  Ctrl+V-View Data           ESC-Quit

1999-2006 (C) LSoft Technologies Inc                          www.KILLDISK.com
```

10. Press **[Tab]** to switch to the right panel.

11. To see items in the list, use **[Page Down], [Page Up]** or the up or down arrow keys.

12. To open a folder, move the cursor to the folder and press **[Enter]**. KillDisk scans the MFT records for this folder. The files in the folder appear in the

right panel. Existing file names and folder names appear in white colour and deleted file names and folder names appear in gray colour. If you are wiping data from unoccupied areas, the gray-coloured file names are removed after the wiping process completes. You may use Files Preview 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.

13. Press **[Esc]** to close this screen and return to Detected Physical Devices.

3.3.1.1 Erasing the Data

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.

If you want to wipe data residue from unoccupied drive space, see

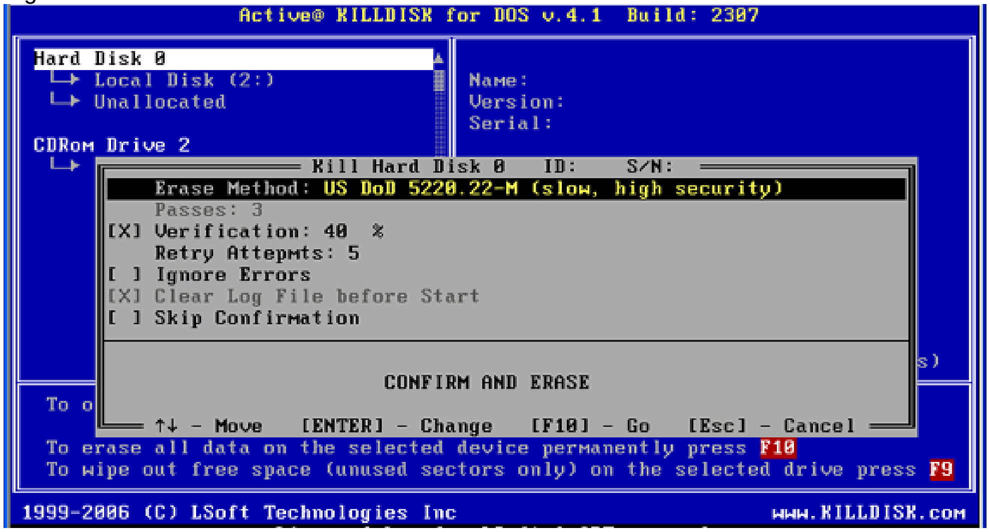
3.3.1.2 Wiping the Data.

If you want to erase data on selected logical drives, follow the steps in 3.4 Erasing or Wiping 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, move the cursor to that device. To permanently erase all data on the selected partition, press **[F10]**. The **Erase Method** screen appears.

Figure 3-4 Erase Method



```
Active@ KILLDISK for DOS v.4.1  Build: 2307

Hard Disk 0                                 Name:
  └→ Local Disk (2:)                        Version:
  └→ Unallocated                            Serial:

CDRom Drive 2
  └→    ═══════ Kill Hard Disk 0   ID:    S/N:   ═══════
        Erase Method: US DoD 5220.22-M (slow, high security)
        Passes: 3
    [X] Verification: 40  %
        Retry Attepmts: 5
    [ ] Ignore Errors
    [X] Clear Log File before Start
    [ ] Skip Confirmation
                                                          s)
                       CONFIRM AND ERASE
  To o
    ═══ ↑↓ - Move   [ENTER] - Change   [F10] - Go   [Esc] - Cancel ═══
  To erase all data on the selected device permanently press F10
  To wipe out free space (unused sectors only) on the selected drive press F9

1999-2006 (C) LSoft Technologies Inc                    www.KILLDISK.com
```

3. To select a different erase method, press **[Enter]**. Erase methods are described in Chapter 5 Descriptions of Erase/Wipe Parameters in this guide. Use the keyboard arrow keys to select the erase method that you want to use. Press **[Enter]** to use the selected method.

4. To change another parameter, use the arrow keys to move the cursor to the parameter. For information on these parameters, see Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.

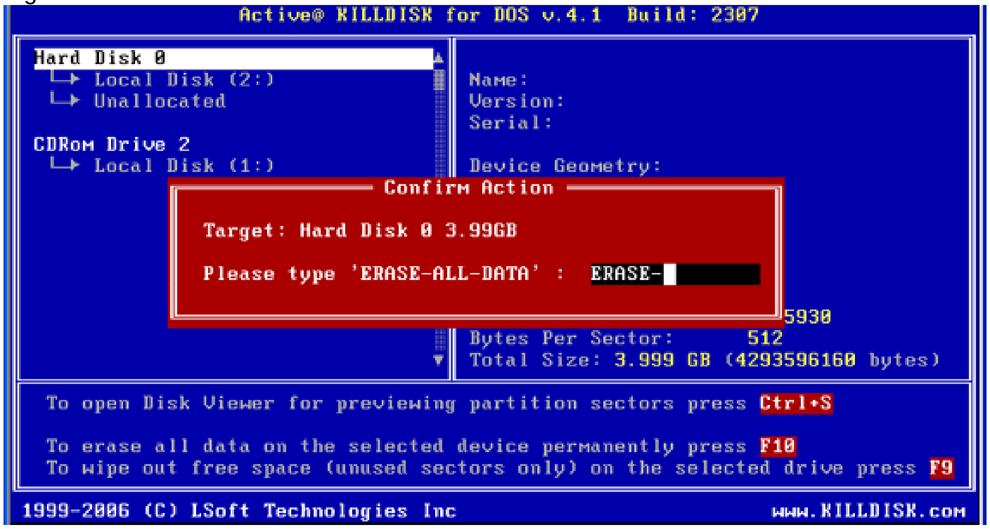
5. The square brackets represent a check box. To clear the check box if it is selected, select the parameter and press the spacebar. Similarly, to select the check box if it is clear, select the parameter and press the spacebar.

6. To change a number in a parameter, select the parameter and press **[Enter]**. Type a number and press **[Enter]** to accept the number.

7. After parameters have been set, move the cursor down to **CONFIRM AND ERASE**.

8. To advance to the final step before erasing data, press **[Enter]**. The **Confirm Action** screen appears.

Figure 3-5 Confirm Action

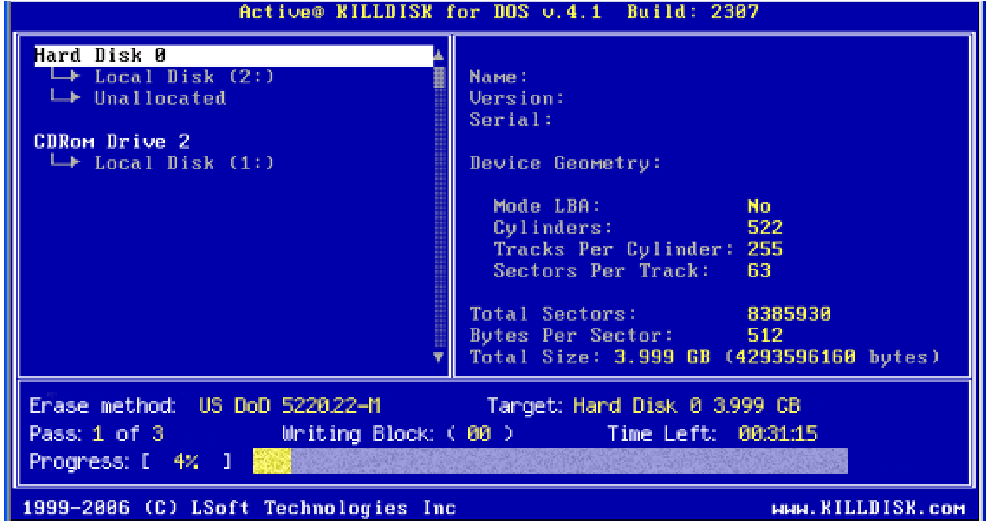


```
              Active@ KILLDISK for DOS v.4.1  Build: 2307

Hard Disk 0
  └→ Local Disk (2:)               Name:
  └→ Unallocated                   Version:
                                   Serial:
CDRom Drive 2
  └→ Local Disk (1:)               Device Geometry:
                    Confirm Action

          Target: Hard Disk 0 3.99GB

          Please type 'ERASE-ALL-DATA' :  ERASE-

                                                         5930
                                   Bytes Per Sector:      512
                                   Total Size: 3.999 GB (4293596160 bytes)

  To open Disk Viewer for previewing partition sectors press Ctrl+S

  To erase all data on the selected device permanently press F10
  To wipe out free space (unused sectors only) on the selected drive press F9

1999-2006 (C) LSoft Technologies Inc                    www.KILLDISK.com
```

9. This is the final step before removing data from the selected drive for ever. After the process has started, you may stop it by pressing the **[Esc]** key.

   Type **ERASE-ALL-DATA** and press **[Enter]**. Progress of the erasing procedure will be monitored in the Disk Erasing screen, similar to the one below.

Figure 3-6 Disk Erasing in Progress



```
                 Active@ KILLDISK for DOS v.4.1  Build: 2307

 Hard Disk 0
   └→ Local Disk (2:)           Name:
   └→ Unallocated               Version:
                                Serial:
 CDRom Drive 2
   └→ Local Disk (1:)           Device Geometry:

                                  Mode LBA:               No
                                  Cylinders:              522
                                  Tracks Per Cylinder:    255
                                  Sectors Per Track:      63

                                Total Sectors:            8385930
                                Bytes Per Sector:         512
                                Total Size: 3.999 GB (4293596160 bytes)

 Erase method:  US DoD 5220.22-M          Target: Hard Disk 0 3.999 GB
 Pass: 1 of 3        Writing Block: ( 00 )        Time Left:  00:31:15
 Progress: [  4%  ]

 1999-2006 (C) LSoft Technologies Inc                    www.KILLDISK.com
```

10. To stop the process for any reason, press the **[Esc]** key. Please note, however that data that has already been erased will not be recoverable.

11. There is nothing more to do until the end of the disk erasing process. The application will operate on its own without user intervention.

    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.

3.3.1.2 Wiping the Data

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. It does not proceed in case it is a damaged partition with important data.

If you want to erase data from the hard drive device permanently, see 3.3.1.1 Erasing the Data.

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

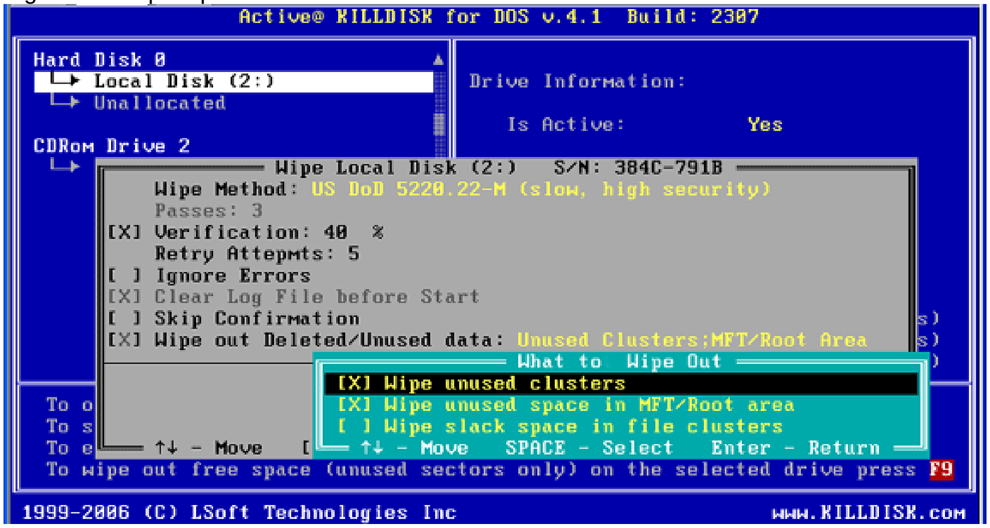
To wipe data:

1. When you have selected the device to wipe, move the cursor to that device. To wipe all data in unoccupied sectors on the selected partition, press **[F9]**. The Wipe Method screen appears.

2. To select a different wipe method, press **[Enter]**. Wipe methods are described in Chapter 5 Descriptions of Erase/Wipe Parameters in this guide. Use the keyboard arrow keys to select the wipe method that you want to use. Press **[Enter]** to use the selected method.

3. To change another parameter, use the arrow keys to move the cursor to the parameter. For information on these parameters, see Chapter 5 Descriptions of Erase/Wipe Parameters in this guide.
4. The square brackets represent a check box. To clear the check box if it is selected, select the parameter and press the spacebar. Similarly, to select the check box if it is clear, select the parameter and press the spacebar.
5. To change a number in a parameter, select the parameter and press **[Enter]**. Type a number and press **[Enter]** to accept the number.

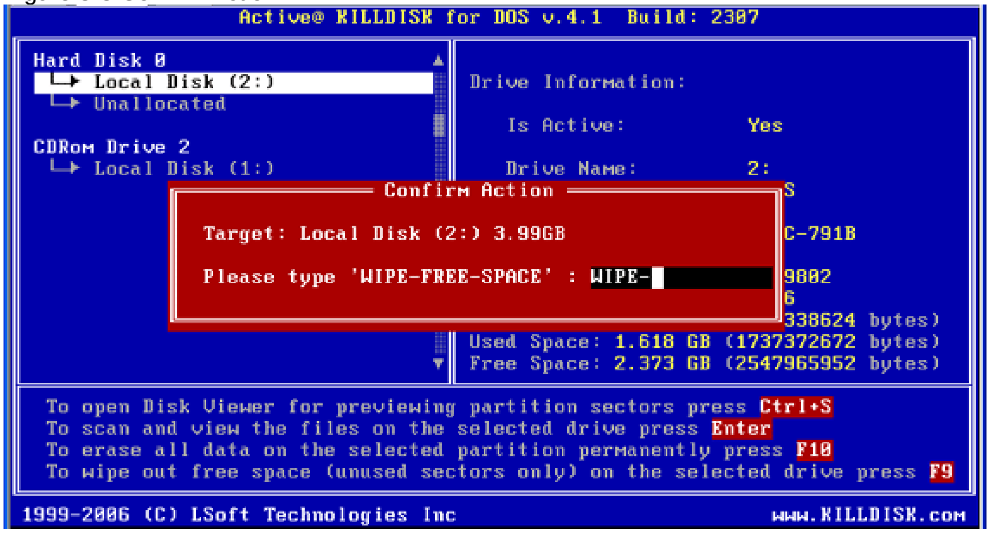
Figure 3-7 Wipe Options Screen



```
              Active@ KILLDISK for DOS v.4.1  Build: 2307
 Hard Disk 0                                 
  └→ Local Disk (2:)                         Drive Information:
  └→ Unallocated
                                               Is Active:          Yes
 CDRom Drive 2
  └→           Wipe Local Disk (2:)   S/N: 384C-791B
        Wipe Method: US DoD 5220.22-M (slow, high security)
        Passes: 3
    [X] Verification: 40  %
        Retry Attepmts: 5
    [ ] Ignore Errors
    [X] Clear Log File before Start
    [ ] Skip Confirmation                                              s)
    [X] Wipe out Deleted/Unused data: Unused Clusters;MFT/Root Area   s)
                                  What to  Wipe Out                    )
                          [X] Wipe unused clusters
   To o                   [X] Wipe unused space in MFT/Root area
   To s                   [ ] Wipe slack space in file clusters
   To e   ↑↓ - Move    [  ↑↓ - Move    SPACE - Select    Enter - Return
   To wipe out free space (unused sectors only) on the selected drive press F9

 1999-2006 (C) LSoft Technologies Inc                        www.KILLDISK.com
```

6. After parameters have been set, move the cursor down to **CONFIRM AND WIPE**.
7. To advance to the final step before erasing data, press **[Enter]**. The Confirm Action screen appears.

Figure 3-8 Confirm Action



```
              Active@ KILLDISK for DOS v.4.1  Build: 2307
 Hard Disk 0
  └→ Local Disk (2:)                         Drive Information:
  └→ Unallocated
                                               Is Active:          Yes
 CDRom Drive 2
  └→ Local Disk (1:)                           Drive Name:         2:
                        Confirm Action                             S

        Target: Local Disk (2:) 3.99GB                             C-791B

        Please type 'WIPE-FREE-SPACE' : WIPE-                      9802
                                                                   6
                                                                   338624 bytes)
                                             Used Space: 1.618 GB (1737372672 bytes)
                                             Free Space: 2.373 GB (2547965952 bytes)

   To open Disk Viewer for previewing partition sectors press Ctrl+S
   To scan and view the files on the selected drive press Enter
   To erase all data on the selected partition permanently press F10
   To wipe out free space (unused sectors only) on the selected drive press F9

 1999-2006 (C) LSoft Technologies Inc                        www.KILLDISK.com
```

8. 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.

   Type **WIPE-FREE-SPACE** and press **[Enter]**. Progress of the wiping procedure will be monitored in the **Disk Wiping** screen.

9. 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 will not be recoverable.

10. There is nothing more to do until the end of the disk erasing process. The application operates on its own without user intervention.

    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.

11. 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 Files Preview screen appears.

    Existing file names and folder names appear in white colour and deleted file names and folder names appear in gray colour. 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.

3.3.2 DOS Command Line Mode

To run Active@ KillDisk in command line mode:

1. With the PC power off, insert the Active@ KillDisk for Hard Drives floppy disk into drive A:

2. Start the PC by turning on the power. The screen will display the Microsoft DOS prompt.

3. At the DOS prompt, display Active@ KillDisk for Hard Drives parameters by typing:

   ```
   A:\>KILLDISK -?
   ```

   A list of parameters will be displayed. Explanations of the parameters can be found in the table below.

Table 3-2 Command Line Parameters

Parameter	Short	Default	Options
no parameter			With no parameter, the DOS Interactive screens will appear.
-erasemethod=[0-6]	-em=	0	0 - One pass zeros (quick, low security) 1 - One pass random (quick, low security) 2 - US DoD 5220.22-M (slow, high security) 3 - German VSITR (slow, high security) 4 - Russian GOST p50739-95 (slow, high security) 5 - Gutmann (very slow, highest security) 6 - User Defined Number of Passes (random)
-passes=[1 - 99]	-p=	3	Number of times the write heads will pass over a disk area to overwrite data. Valid only if -erasemethod = 6.
-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.

Parameter	Short	Default	Options
-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 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			If you are having difficulty with Active@ KillDisk for Hard Drives, 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.
-help or -?			Display this list of parameters.

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

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

```
A:\>killdisk.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:

```
A:\>killdisk.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:

```
A:\>killdisk.exe -wa -bm -em=5 -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.

5. 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.

3.3.3 Autoexecute Mode

You may start Active@ KillDisk for Hard Drives with a DOS auto-executable batch file. The command line contains the command to execute the program along with chosen parameters.

To run Active@ KillDisk from an auto-executable batch file:

1. In the Microsoft DOS screen, open a new autoexec.bat file or edit an existing one with the following command:

   ```
   A:\>edit autoexec.bat
   ```

   The Microsoft DOS file edit screen appears.

2. Enter the command line and parameters as needed. Here is an example:

   ```
   killdisk -erasehdd=80h -erasemethod=6 -passes=1 -
   ignoreerrors
   ```

   In the example above, the first detected hard disk will be erased in one pass. Confirmations will be encountered and errors will be ignored.

3. Save the autoexec.bat file in the root directory of the system floppy disk and exit the edit utility.

4. Remove the floppy from this floppy drive.

5. The floppy is now ready for automatic data erasing. To erase data using Autoexecute Mode, follow these steps:

   - Go to the machine that requires data erasing
   - With the PC power off, insert the Active@ KillDisk for Hard Drives Automatic Mode floppy disk into drive A:
   - Start the PC by turning on the power.
   - The PC will indicate booting into DOS. The data erase process will begin.

3.4 Erasing or Wiping Logical Drives (Partitions)

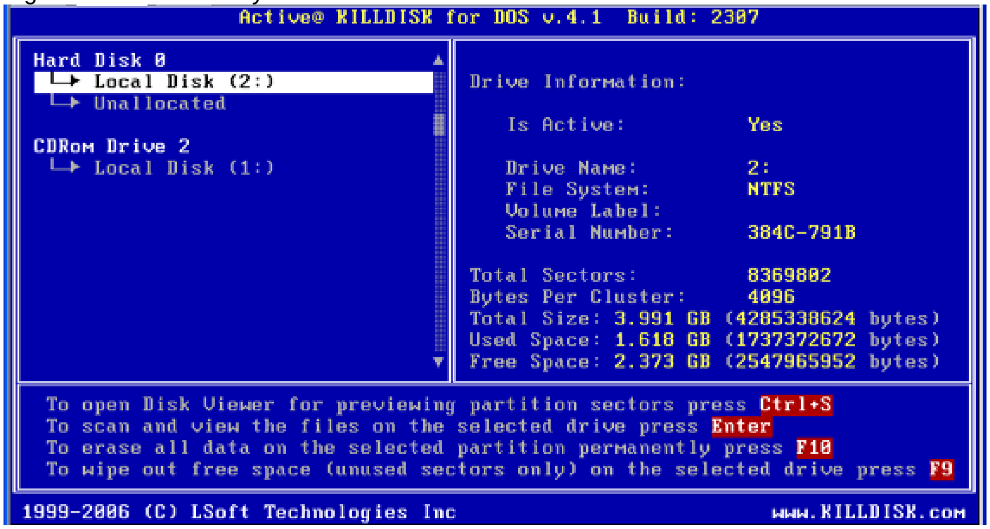
In all previous examples in this chapter, the process has erased data or wiped data from a physical drive. Using a similar method, you can erase or wipe logical disks and partitions, and even “Unallocated” areas where partitions used to exist and the area was damaged, or the area is not visible by the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

Erase Data From a Logical Drive

To erase data from a logical drive, open the DOS Interactive Mode screen and follow the steps below.

1. The **Detected Physical Devices** screen appears as below:

Figure 3-9 Detected Physical Devices



```
                 Active@ KILLDISK for DOS v.4.1  Build: 2307

 Hard Disk 0
  └→ Local Disk (2:)                    Drive Information:
  └→ Unallocated
                                           Is Active:            Yes
 CDRom Drive 2
  └→ Local Disk (1:)                       Drive Name:           2:
                                           File System:          NTFS
                                           Volume Label:
                                           Serial Number:        384C-791B

                                        Total Sectors:           8369802
                                        Bytes Per Cluster:       4096
                                        Total Size: 3.991 GB (4285338624 bytes)
                                        Used Space: 1.618 GB (1737372672 bytes)
                                        Free Space: 2.373 GB (2547965952 bytes)

   To open Disk Viewer for previewing partition sectors press Ctrl+S
   To scan and view the files on the selected drive press Enter
   To erase all data on the selected partition permanently press F10
   To wipe out free space (unused sectors only) on the selected drive press F9

 1999-2006 (C) LSoft Technologies Inc                          www.KILLDISK.com
```

All system hard drives and floppy drives will be displayed in the left pane along with their system information in the right pane.

2. Position the cursor over the logical disk or on the Unallocated area.
3. Press **[F10]** to securely remove data. Follow directions to set up erase parameters.

Wipe Data From a Logical Drive

To wipe data from a logical drive, open the DOS Interactive Mode screen and follow the steps below.

1. 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.

2. Position the cursor over the logical drive.
3. Press **[F9]** to wipe data from unoccupied areas. Follow directions to set up wipe parameters.

3.5 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 started at: Thu Feb 20 11:56:51 2006

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 floppy from which you started Active@ KillDisk.

4 Common Questions

4.1 How does the licensing work?

The software is licensed on a per floppy or CD basis. Each license allows you to use the program from a separate floppy or CD. If you want to use the program to wipe 5 computers concurrently, you would need 5 floppies or CDs (or combination of the two not exceeding five), and therefore need a 5 user license.

4.2 How is the data erased?

Active@ KillDisk communicates with the system board Basic Input-Output Subsystem (BIOS) functions to access hardware directly. It uses Logical Block Addressing (LBA) access if necessary to clean FAT32 drives more than 8 GB in size. 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 runs in any DOS environment. It can be MS-DOS, PC-DOS, FreeDOS, DR-DOS, etc. As it can be installed easily onto a bootable floppy disk or a bootable CD-ROM, it does not matter which operating system is installed on the machine hard drive. If you can boot in DOS mode from the boot diskette or boot CD-ROM, you can detect and erase any drives independent of the installed Operating System.

4.5 Is Active@ KillDisk compatible with Macintosh computers?

No, it is not.

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 What to do if I cannot boot from a floppy?

There are many possible reasons that you cannot boot from a floppy. Please consult this troubleshooting chart:

Table 4-3 Troubleshooting Floppy Disk Problems

Problem	Solution
Error message "bad command or file name"	You can use our KillDisk Bootable Floppy Creator to make a bootable floppy: http://www.killdisk.com/downloadfree.htm To use KillDisk floppy creator: 1. From the link, save "killdiskfloppysetup.exe" file to your Desktop. 2. Insert an empty floppy disk in the floppy drive. 3. On your Desktop, double-click killdiskfloppysetup.exe and follow all instructions. 4. When you purchase Active@ KillDisk Professional version, you receive the file "kd-setup.exe". Double-click this file and copy all the extracted flies to the floppy disk. Make sure that you overwrite the file "killdisk.exe" with the registered version. 5. Restart your PC using the bootable floppy.
Floppy disk is not bootable or damaged.	With the floppy in drive A:, verify whether or not system files (COMMAND.COM, etc.) are located on floppy. If the disk directory can be read and system files appear by name, some files on the floppy may be damaged, or the surface of the floppy may be damaged. On a DOS or Windows PC, run SCANDISK.EXE to check for damaged areas on the floppy surface. Alternately, prepare and test another bootable floppy disk. For more instructions, see Chapter 3, Running Active@ KillDisk.
Machine has boot priority for Hard Disk Drives, or another device set higher than for Floppy Drives.	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 Escape on the keyboard during PC

Problem	Solution
	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 ROM drives, Floppy Drives and Network Boot option. 3. If the floppy device has been disabled, enable it (provided you have a floppy disk installed). The priority should indicate that the floppy device is the number one device the BIOS consults when searching for boot instructions. If Floppy Drives 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

5.1.1 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.

5.1.2 User Defined

You indicate the number of times the write head passes over each sector. Each overwriting pass is performed with a buffer containing random characters.

5.1.3 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.

5.1.4 German VSITR

The write head passes over each sector seven times.

5.1.5 Russian GOST p50739-95

The write head passes over each sector five times.

5.1.6 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 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.

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 Skip Confirmation

The confirmation screen is the final step before either erasing or wiping data. In this red-colored screen, you type ERASE-ALL-DATA or WIPE-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.

5.2.6 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 or F10 during the boot sequence.

boot priority

BIOS settings allow you to run a boot sequence from a floppy drive, a hard drive or a CD-ROM drive. 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-ROM drive instead of a hard drive, place the CD-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.