User's Manual

Version Number 2.0

Active@ KillDisk v 2.0   END-USER LICENSE AGREEMENT

~~~~~~

Copyright (c) 1998-2003 LSoft Techologies Inc., All rights reserved.

~~~~~~

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and The LSoft Techologies for the Active@ KillDisk later referred to as 'SOFTWARE'. By installing, copying, or otherwise using the SOFTWARE you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE.

WE REQUIRE ALL OUR DEALERS TO PROVIDE EACH PURCHASER WITH FREE DEMO OF THE SOFTWARE TO GET A FULL UNDERSTANDING OF THE CAPABILITIES AND THE EASE OF USE OF THE SOFTWARE. OUR DEALERS HAD TO RECOMMEND YOU TO DOWNLOAD DEMO. WE WON'T ISSUE ANY REFUNDS AFTER PURCHASING FULL VERSION OF THE SOFTWARE.

LSoft Techologies may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

SOFTWARE LICENSE

1. The SOFTWARE is licensed, not sold. Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the SOFTWARE.

2. GRANT OF LICENSE.

(a) FREE DEMO COPY. You may use the full featured DEMO SOFTWARE without charge on an evaluation basis to erase floppies and hard disk drives using [One Pass Zeros] data destruction method only. You must pay the license fee and register your copy to get professional version of the product that can erase floppies and HDDs using other data destruction methods, including DoD 5220.22-M, and the most secure Gutmann's method.

(b) REDISTRIBUTION OF DEMO COPY. If you are using DEMO SOFTWARE on an evaluation basis you may make copies of the DEMO SOFTWARE as you wish; give exact copies of the original DEMO SOFTWARE to anyone; and distribute the DEMO SOFTWARE in its unmodified form via electronic means (Internet, BBS's, Shareware distribution libraries, CD-ROMs, etc.). You may not charge any fee for the copy or use of the evaluation DEMO SOFTWARE itself, but you may charge a distribution fee that is reasonably related to any cost you incur distributing the DEMO SOFTWARE (e.g. packaging). You must not represent in any way that you are selling the software itself. Your distribution of the DEMO SOFTWARE will not entitle you to any compensation from LSoft Techologies.

You must distribute a copy of this EULA with any copy of the Software and anyone to whom you distribute the SOFTWARE is subject to this EULA.

(c) REGISTERED COPY. After you have purchased the license for SOFTWARE, and have received SOFTWARE distribution package, you are licensed to copy the SOFTWARE only into the number of floppy disks corresponding to the number of licenses purchased. Under no other circumstances may the SOFTWARE be operated at the same time on more than the number of floppy disks for which you have paid a separate license fee. You may not duplicate the SOFTWARE in whole or in part, except that you may make one copy of the SOFTWARE for backup or archival purposes. You may terminate this license at any time by destroying the original and all copies of the SOFTWARE in whatever form. You may permanently transfer all of your rights under this EULA provided you transfer all copies of the SOFTWARE (including copies of all prior versions if the SOFTWARE is an upgrade) and retain none, and the recipient agrees to the terms of this EULA.

(d) SITE AND ENTERPRISE LICENSES. "Site" license means that you can use SOFTWARE without of any limitations at one company's office (one physical location). "Enterprise" license means that you can use SOFTWARE without of any limitations at all company's offices and branches (worldwide).

3. RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not rent, lease, or lend the SOFTWARE. You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA. You may not use the SOFTWARE to perform any unauthorized transfer of information (e.g. transfer of files in violation of a copyright) or for any illegal purpose.

4. SUPPORT SERVICES. LSoft Techologies may provide you with support services related to the SOFTWARE. Use of Support Services is governed by the LSoft Techologies polices and programs described in the online documentation and web site, and/or other LSoft Techologies-provided materials, as they may be modified from time to time. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE and subject to the terms and conditions of this EULA. With respect to technical information you provide to LSoft Techologies as part of the Support Services, LSoft Techologies may use such information for its business purposes, including for product support and development. LSoft Techologies will not utilize such technical information in a form that personally identifies you.

5. TERMINATION. Without prejudice to any other rights, LSoft Techologies may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE.

6. COPYRIGHT. The SOFTWARE is protected by copyright law and international treaty provisions. You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. You further acknowledge that title and full ownership rights to the SOFTWARE will remain the exclusive property of LSoft Techologies and you will not acquire any rights to the SOFTWARE except as expressly set forth in this license. You agree that any copies of the SOFTWARE will contain the same proprietary notices which appear on and in the SOFTWARE.

7. DISCLAIMER OF WARRANTY. LSoft Techologies expressly disclaims any warranty for the SOFTWARE. THE SOFTWARE AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

8. LIMITATION OF LIABILITY. IN NO EVENT SHALL ACTIVE DATA RECOVERY SOFTWARE OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE, OR USE OF THE SOFTWARE, EVEN IF LSOFT TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY EVENT, ACTIVE DATA RECOVERY SOFTWARE'S ENTIRE LIABILITY UNDER ANY PROVOSION OF THIS EULA SHALL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT.

LSoft Techologies reserves all rights not expressly granted here.

Contents

Standards Used in This Guide

The following standards are used to provide more concise documentation:

Table 0-1 User Input

Description	Example	Action
Bold text within square brackets.	Press **[Enter]**. Press **[Y].**	Press the key on the keyboard that corresponds to the message within square brackets.
Bold text and operand within square brackets.	Press **[Ctrl + B]**	Together, press the combination of keys within the square brackets.
Bold text.	Click **OK**	With the mouse pointer, find the icon, tab or button indicated and left-click that icon.

1 OVERVIEW

This chapter gives an overview of **Active@ KillDisk** application.

Deleting Confidential Data

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

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** (www.file-recovery.net) or **Active@ UNERASER** (www.uneraser.com), making your erased confidential data quite accessible.

Using **Active@ KillDisk**, 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**, disposal, recycling, selling or donating your storage device can be done with peace of mind.

International Standards in Data Removal

Active@ KillDisk conforms to four international standards for clearing and sanitizing data. You can be sure that once you wipe a disk with **Active@ KillDisk**, sensitive information is destroyed forever.

Active@ KillDisk 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.

2 SYSTEM REQUIREMENTS

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

Personal Computer	• IBM PC/AT compatible CPU ◦ Operates with processors as old as Intel 486 • 4 Mb of RAM • Video must be EGA or better resolution
Drive Storage System	• 1.44 Mb floppy diskette drive • Hard Disk Drive type IDE, ATA or SCSI with controllers
Other	• One blank 3.5-inch or 5.25-inch floppy disk suitable for formatting • Alternately use a Windows 95/98/ME Startup Disk

Active@ KillDisk Version

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

Table 2-1 Differences Between Free and Professional Versions

Feature	FREE DEMO Version	Professional Version
Securely overwrites and destroys all data on physical drive or logical partition	✔	✔
Supports IDE / ATA / SCSI drives	✔	✔
Supports Fixed Disks, Floppies, Zip Drives, FlashMedia drives	✔	✔
Supports large format drives (more than 8GB)	✔	✔
Supports Command Line mode (can be run with no user interaction)	✔	✔
Operates from a floppy disk	✔	✔
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		✔
Supports all detected hard disk drives	✔	✔
Erasing report is created and can be saved as a file	✔	✔
Displays detected drive and partition information	✔	✔
Data verification performed after erasing is completed		✔
Disk Viewer allows previewing of any sectors on a drive	✔	✔

3 RUNNING ACTIVE@ KILLDISK

This chapter describes how to use the application. The chapter's sections are:

- Preparing a DOS-bootable Floppy Disk
- Modes of Operation:
  - DOS Interactive Mode
  - DOS Command Line Mode
  - DOS Autoexecute Mode

Preparing a DOS-Bootable Floppy Disk

Active@ KillDisk 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.

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

Copying Active@ KillDisk to a Floppy

Copy the **Active@ KillDisk** file (KillDisk.EXE) to the bootable floppy disk or startup disk in drive a:.

If you don't have the **Active@ KillDisk** 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** 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.

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.

Modes of Operation

Active@ KillDisk 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**.

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** will start immediately upon completion of the bootstrap startup (depending on the automatic settings).

DOS Interactive Mode

This section describes using the DOS Interactive screens. For “hands-off” operation, please see the next section, below.

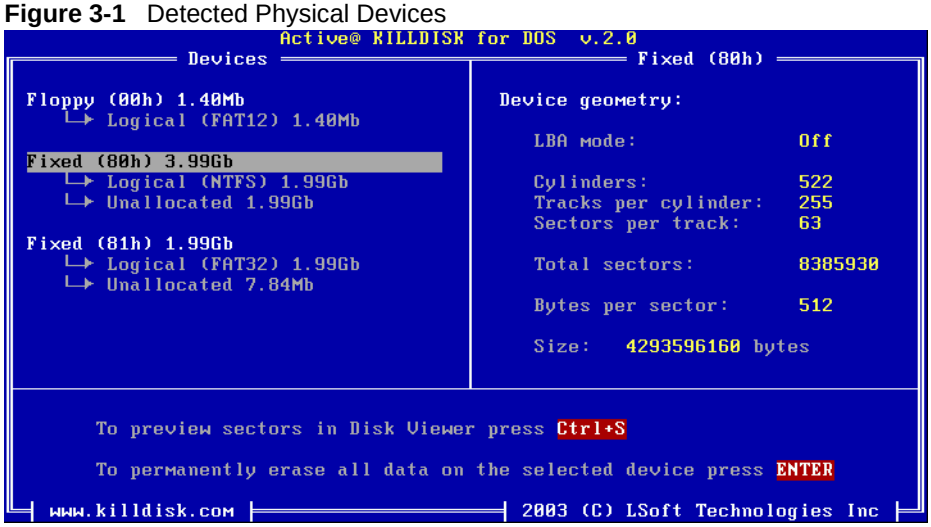
Here are the steps for DOS interactive operation:

1. With the PC power off, insert the **Active@ KillDisk** 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, run **Active@ KillDisk** by typing:

```
KillDisk.EXE
```

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

Figure 3-1 Detected Physical Devices



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

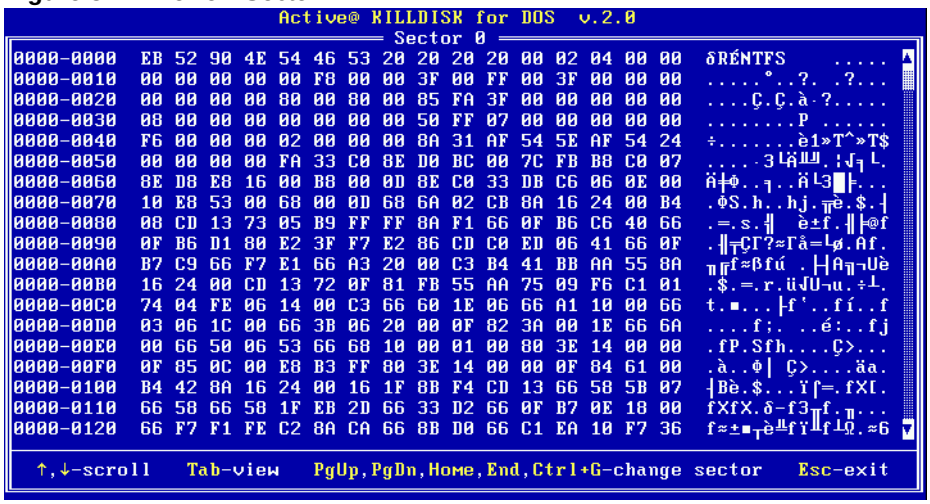
4. Change the position cursor using the keyboard **[Down]** and **[Up]** arrow keys. Information in the right pane will change according to the structure of the detected devices.

   Hard drive devices are numbered by the system BIOS. A system with a single hard drive will show it as number 80h. Subsequent hard drive devices will be numbered consecutively. For example the second device will be shown as 81h.

5. 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.

If there is any doubt about which drive to select, preview the sectors in the device by pressing **[Ctrl + s]**. The screen appears, as below:

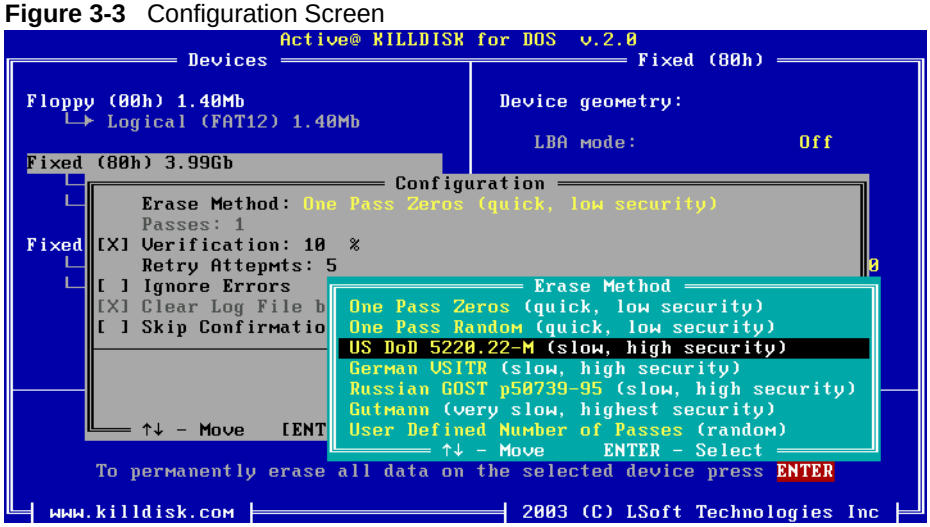
Figure 3-2 Preview Sector



Scroll up and down using the keyboard arrow keys, **[Page Up]**, **[Page Down]**, **[Home]** and **[End]** navigation keys. Jump to a specific sector using **[Ctrl + g]**. When you are satisfied with the identification of the device, press **[Esc]** to exit this screen and return to the **Detected Physical Devices** screen.

6 When you have selected the device to erase, move the cursor to that device and press **[Enter]** on the keyboard. The **Configuration** screen appears.

Figure 3-3 Configuration Screen



Using the keyboard arrow keys, select the feature that you want to configure. Press **[Enter]** to make a change.

To assist with options presented in this screen, please refer to the table on the following page.

Table 3-1 Erase Parameters Configuration

Feature	Default	Options
Erase Method	One pass zeros	One pass zeros One pass random US DoD 5220.22M German VSITR Russian GOST p-50739-95 Gutmann User Defined Number of Passes (For descriptions of these options see Chapter 5 in this guide.)
Passes	3	If **User Defined Number of Passes** is selected in the line above, this number may be changed. Otherwise this line will display the standard number of passes for the selected erase method.
Verification	Enabled / 40%	Enabled: Utility inspects the work done by KillDisk to verify that the attempt was successful. The percentage shown indicates how much of the drive is verified. Disabled: Verification is not performed
Retry Attempts	5	If the process encounters an IO error, the number here shows the number of times the operation will repeat before displaying an error message. Repeating the operation will sometimes help to overcome IO problems.
Ignore Errors	Disabled	Enabled: Error messages are not displayed. Disabled: Each time the read heads encounter a read-write error, a message appears that requires confirmation by the user.
Clear Log File before Start	Enabled	
Skip Confirmation	Disabled	Enabled: Next step requires confirmation by the user. Disabled: Next step confirmation screen does not appear.

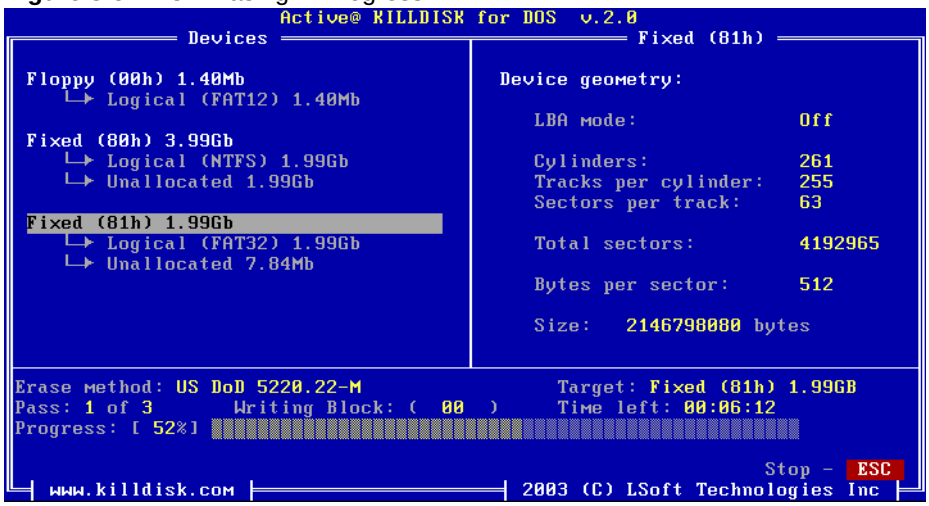
When all configuration settings are complete, press **[Enter]**. The **Confirm Action** screen appears.

Figure 3-4 Confirm Action

7 This is the final step before removing data from the selected drive for ever. Once 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 3-5 Disk Erasing in Progress



8 If you wish to stop the process for any reason after it has begun, press the **[Esc]** key. Please note, however that erased data will not be recoverable.

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 **Ignore Errors** is disabled, a message screen appears each time an error is encountered. If such a message appears, it will be possible to cancel the operation (by pressing **[Esc]**), or continue erasing data.

DOS Command Line Mode

This section describes running **Active@ KillDisk** in Command Line mode.

Follow these steps:

1. With the PC power off, insert the **Active@ KillDisk** 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** parameters by typing:

   ```
   A:\>KillDisk -?
   ```

   A list of parameters will be displayed. Explanations of the parameters can be found in the table on the following page.

Table 3-2 Command Line Parameters

Parameter	Default	Options
no parameter		With no parameter, the DOS Interactive screens will appear, as described in the preceding section.
-erasemethod=[0-6]	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]	1	Number of times the write heads will pass over a disk area to overwrite data. Valid only if erasemethod = 6.
-verification=[1 - 100]	40	After the data erasing process is complete, the utility reads the disk space to verify that the actions performed by the write head comply with the chosen erasemethod (reading 40% of the area by default). It is a long process. Set the verification to the level that works for you.
-retryattempts=[1 - 99]	5	When the drive write head encounters an error in the sector, the utility will retry to write in the sector 5 times by default.
-erasehdd=[80h - 83h]		By default, the utility will erase the first logical drive encountered. Use this parameter to direct the erasing procedure to the correct target.
-ignoreerrors	OFF	By default, the erasing process will stop each time a disk error is encountered. You have the option to continue erasing or to stop the process and deal with the error. When this parameter is used, all errors are ignored.
-clearlog	ON	When a drive is erased, a log file is kept. By default, this log is cleared at the start of the erasing process. The log file is stored in the same folder where the software is located.
-noconfirmation	ON	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?
-test		If you are having difficulty with Active@ KillDisk, use this parameter to create a hardware info file to be sent to our technical support specialists.
-eraseallhdds		Erase all detected hard disk drives
-help or -?		Display this list of parameters.

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

```
A:\>KillDisk -eraseallhdds -erasemethod=6 -passes=7
-noconfirmation
```

In the example above, data on all hard drives will be erased in seven passes without user confirmation. In addition, the process will stop when errors are encountered.

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, similar to the message in **Erase Operation Complete**, below.

Autoexecute Mode

You can start **Active@ KillDisk** with a DOS auto-executable batch file. Include the command line containing call of the program and parameters.

Follow these steps:

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:

1 Go to the machine that requires data erasing

2 With the PC power off, insert the **Active@ KillDisk** Automatic Mode floppy disk into drive A:

3 Start the PC by turning on the power.

4 The PC will indicate booting into DOS. The data erase process will begin.

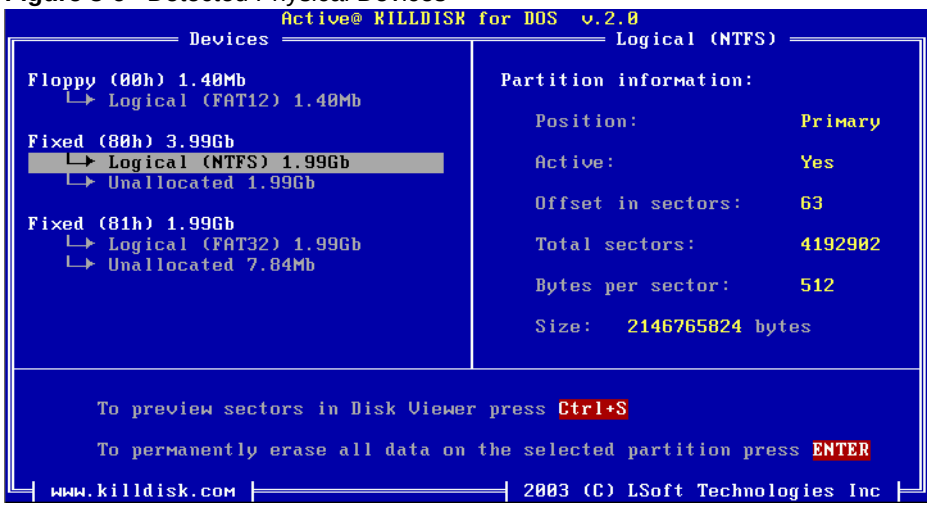
Erasing Logical Drives (Partitions)

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

Open the DOS Interactive Mode screen and follow the steps below.

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

Figure 3-6 Detected Physical Devices



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 [Enter] to securely remove data.

Erase Operation Complete

After operation is completed successfully, information on how drives have been erased is displayed similar to the data below:

```
------------- Erase Session ----------------------
Active@ KillDisk started at: Thu Feb 20 11:56:51 2003
     Target:  Floppy (00h) 1.40MB
 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 would be presented in this report. Use the keyboard arrow keys to scroll through the report.

Details of this report are saved to a log file located in the same order from which you started Active@ KillDisk.

4 COMMON QUESTIONS

I cannot boot the machine from a floppy. What is wrong?

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

Table 4-1 Troubleshooting Floppy Disk Problems

Problem	Solution
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, the disk or some files on the disk may be damaged. On a DOS or Windows PC, run SCANDISK.EXE to check for damaged areas on the disk surface. Alternately, prepare and test another bootable floppy disk.
Machine has boot priority for Hard Disk Drives, or another device set higher than for Floppy Drives.	Open the low-level setup screen, usually by pressing **[F1]** or **[Delete]** on the keyboard during PC startup. These setup parameters build structure in the BIOS. Locate the section about Boot Device Priority, or similar. This section will allow you to set the search order for types of boot devices. When the screen opens, a list of boot devices will appear. Typical devices on this list will be Hard Drives, CD ROM drives, Floppy Drives and Network Boot option. 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.

Which operating systems are supported by Active@ KillDisk?

Active@ KillDisk runs in the Microsoft DOS environment. As it can be installed easily onto a bootable floppy disk, 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, you can detect and erase any drives independent of the installed Operating System.

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 a character or character set defined for a particular method.

For example, to conform to US DoD 5220.22-M security standard, it overwrites locations on the drive three times using the following:

- First time with zeros (0x00)
- Second time with 0xFF
- Third time with random characters

When using **User Defined Number of Passes**, it overwrites each time with random characters.

5 Notes About Erase Methods

This chapter describes the Erase Methods

Number of Passes

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 will write only zeros or a series of random characters.

User Defined

For **User Defined** method, the user can indicate the number of times the write head passes over each sector. Each overwriting pass will be performed with a buffer containing random characters.

US DoD 5220.22-M

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

German VSITR

The write head passes over each sector seven times.

Russian GOST p50739-95

The write head passes over each sector five times.

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/~pgutool/pubs/secure_del.html>

Verification

After erasing is complete you can direct 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 drive matches data written by the erasing process.

Because verification is a long process, you can specify a percentage of the surface to be verified. You can 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 operation again. You can specify number of retries to be performed.

Sometimes a damaged sector can be overwritten if the drive is not completely damaged, 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.

While displaying error messages have been ignored, all information about these errors are written to the KILLDISK.LOG file. They 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 will be appended to the end of the file.

Skip Confirmation

The confirmation step happens when the user types ERASE-ALL-DATA as the final step before the erasing process starts. If **Skip Confirmation** is turned on, the request for confirmation is skipped. This option is typically to be used by advanced users in order to speed up the process.

Turning off this option (default state) is safer because you have one last chance to ensure that data from the correct drive location is going to be erased completely with no possibility of future data recovery.