LSOFT.NET LSOFT TECHNOLOGIES

Active@ KillDisk

User Guide

Version Number 3.0

Contents

OVERVIEW

SYSTEM REQUIREMENTS

RUNNING ACTIVE@ KILLDISK

COMMON QUESTIONS

ERASING PARAMETERS

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 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 or button indicated and left-click that icon.
Letter "i" in the left margin	***i***	Information worthy of noting.
Exclamation mark in the left margin	***!***	Important information that may cause the utility to behave incorrectly and may damage data as a result.

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 Microsoft DOS **del** 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.

The **format** utility actually creates new **FAT** and **ROOT** tables, leaving all previous data on the disk untouched.

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

When you use **Active@ KillDisk**, you can scan drives and view all files on them - including files that have been deleted using the Microsoft DOS **del** command.

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 Minimum Requirements

- 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 Active@ KillDisk

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		✓
Customized Security Levels	✓	✓
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	✓	✓
Lightweight installation (only about 1MB)	✓	✓
Disk Viewer allows previewing of any sectors on a drive	✓	✓
Scans drives and previews files before erasing on FAT, FAT32 and NTFS file systems	✓	✓

What's New in Version 3.0

- When the cursor is positioned on the logical drive, pressing **[Enter]** scans the drive, allowing you to preview all files and folders. In this way, you can check one last time - to be certain you have selected the correct drive - before erasing data permanently.
- Scans and previews files in all major file systems (FAT, FAT32, NTFS, NTFS5)

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 **Copying 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**.

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** starts 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.

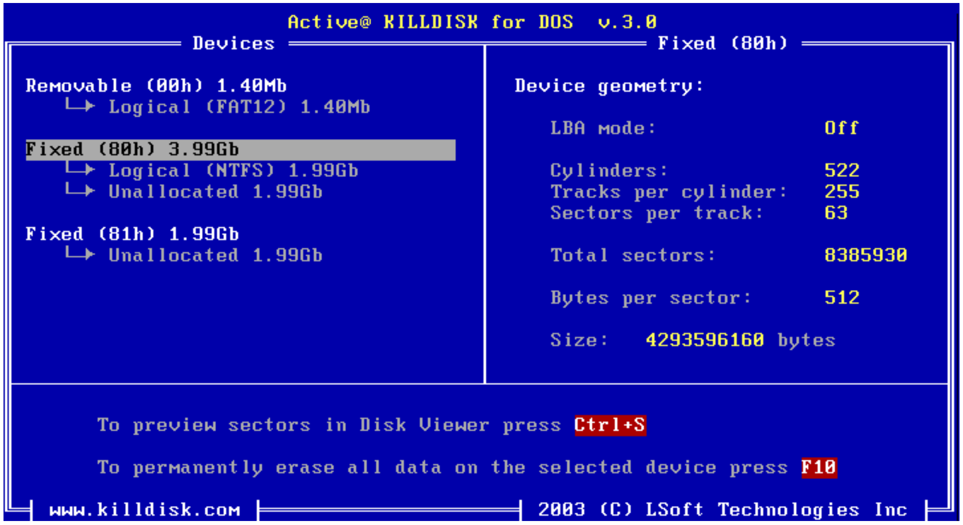
Here are the steps for interactive operation:

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 displays 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



```
                      Active@ KILLDISK for DOS  v.3.0
 ═══════════ Devices ══════════════════════════ Fixed (80h) ══════════
 Removable (00h) 1.40Mb                  Device geometry:
    └→ Logical (FAT12) 1.40Mb
                                            LBA mode:              Off
 Fixed (80h) 3.99Gb
    └→ Logical (NTFS) 1.99Gb                Cylinders:             522
    └→ Unallocated 1.99Gb                   Tracks per cylinder:   255
                                            Sectors per track:     63
 Fixed (81h) 1.99Gb
    └→ Unallocated 1.99Gb                   Total sectors:         8385930

                                            Bytes per sector:      512

                                            Size:   4293596160 bytes

        To preview sectors in Disk Viewer press Ctrl+S

        To permanently erase all data on the selected device press F10

   www.killdisk.com                        2003 (C) LSoft Technologies Inc
```

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

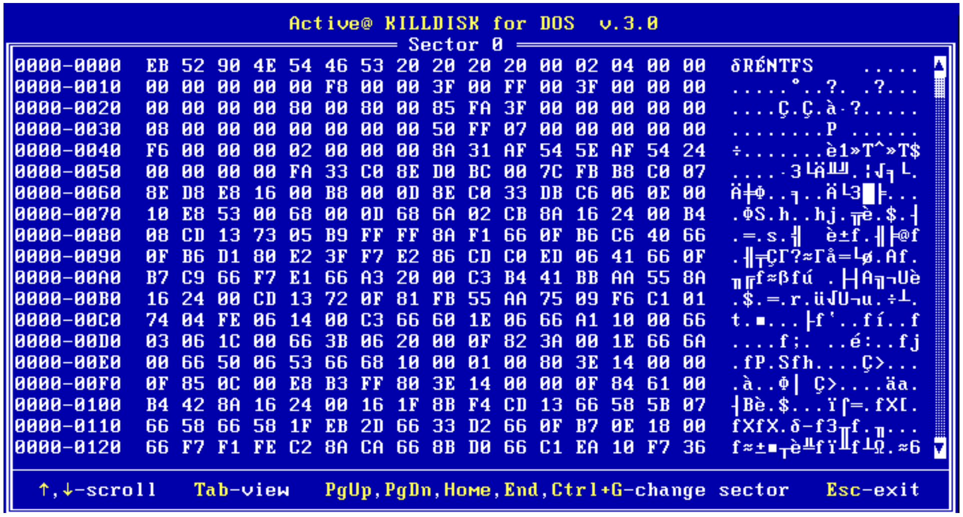
4. Change the position cursor using the keyboard **[Down]** and **[Up]** arrow keys. Information in the right pane changes according to the structure of the detected devices.

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

5. Be certain that the drive you are pointing to is the one that you want to erase. All data is 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

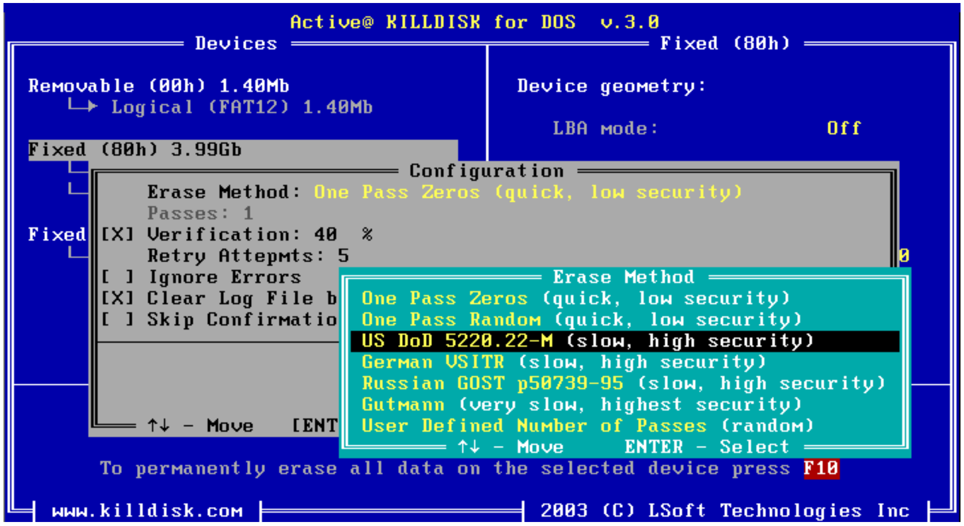


```
                     Active@ KILLDISK for DOS  v.3.0
                                Sector 0
0000-0000  EB 52 90 4E 54 46 53 20 20 20 20 00 02 04 00 00  δRÉNTFS     .....
0000-0010  00 00 00 00 00 F8 00 00 3F 00 FF 00 3F 00 00 00  .....°..?. .?...
0000-0020  00 00 00 00 80 00 80 00 85 FA 3F 00 00 00 00 00  ....Ç.Ç.à·?.....
0000-0030  08 00 00 00 00 00 00 00 50 FF 07 00 00 00 00 00  ........P ......
0000-0040  F6 00 00 00 02 00 00 00 8A 31 AF 54 5E AF 54 24  ÷.......è1»T^»T$
0000-0050  00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07  ....·3└Ä╨╝.¦√╕└.
0000-0060  8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00  Ä╪Φ..╕..Ä└3█╞...
0000-0070  10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4  .ΦS.h..hj.╦è.$.┤
0000-0080  08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66  .═.s.╣  è±f.╢╞@f
0000-0090  0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F  .╢╤ÇΓ?≈Γå═└φ.Af.
0000-00A0  B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A  ╖╔f≈ßfú .├┤A╗¬Uè
0000-00B0  16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01  .$.═.r.ü√U¬u.÷┴.
0000-00C0  74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66  t.■...├f`..fí..f
0000-00D0  03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6A  ....f;. ..é:..fj
0000-00E0  00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00  .fP.Sfh....Ç>...
0000-00F0  0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00  .à..Φ│ Ç>....äa.
0000-0100  B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07  ┤Bè.$...ï⌠═.fX[.
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╩fï╨f┴Ω.≈6

 ↑,↓-scroll   Tab-view   PgUp,PgDn,Home,End,Ctrl+G-change sector   Esc-exit
```

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.

6 When you have selected the device to erase, move the cursor to that device and press **[F10]** on the keyboard. The **Configuration** screen appears.

Figure 3-3 Configuration Screen



```
                     Active@ KILLDISK for DOS  v.3.0
              Devices                              Fixed (80h)

 Removable (00h) 1.40Mb                  Device geometry:
     └→ Logical (FAT12) 1.40Mb
                                            LBA mode:            Off
 Fixed (80h) 3.99Gb
     └                     Configuration
     └        Erase Method: One Pass Zeros (quick, low security)
              Passes: 1
 Fixed    [X] Verification: 40  %
     └        Retry Attempts: 5                                        0
          [ ] Ignore Errors            Erase Method
          [X] Clear Log File b  One Pass Zeros (quick, low security)
          [ ] Skip Confirmatio  One Pass Random (quick, low security)
                                US DoD 5220.22-M (slow, high security)
                                German VSITR (slow, high security)
                                Russian GOST p50739-95 (slow, high security)
                                Gutmann (very slow, highest security)
              ↑↓ - Move    [ENT User Defined Number of Passes (random)
                                      ↑↓ - Move     ENTER - Select
        To permanently erase all data on the selected device press F10

   www.killdisk.com                        2003 (C) LSoft Technologies Inc
```

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

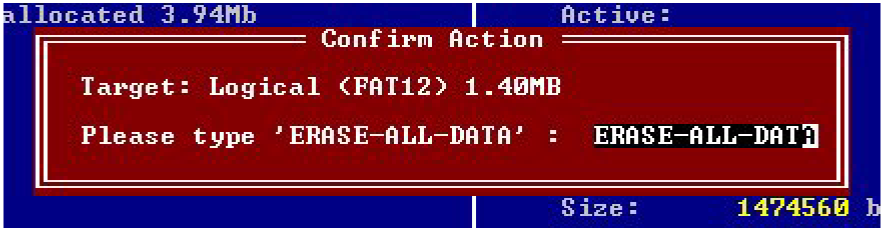
To assist with options presented in this screen, please refer to the table on the following page.

Table 3-1 Erase Parameters Configuration

Feature	Default	Options
Erase Method	US DoD 5220.22M	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 ANOTHER PLACE, below.)
Passes	3	If **User Defined Number of Passes** is selected in the line above, this number may be changed. Otherwise this line displays 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 of times the operation repeats before displaying an error message. Repeating the operation sometimes helps to overcome IO problems.
Ignore Errors	Disabled	Enabled: Each time the read heads encounter a read-write error, a message appears that requires confirmation by the user. Disabled: Error messages are not displayed.
Clear Log File before Start	Enabled	
Skip Confirmation	Disabled	Next step confirmation screen does not appear.

The **Confirm Action** screen appears.

Figure 3-4 Confirm Action

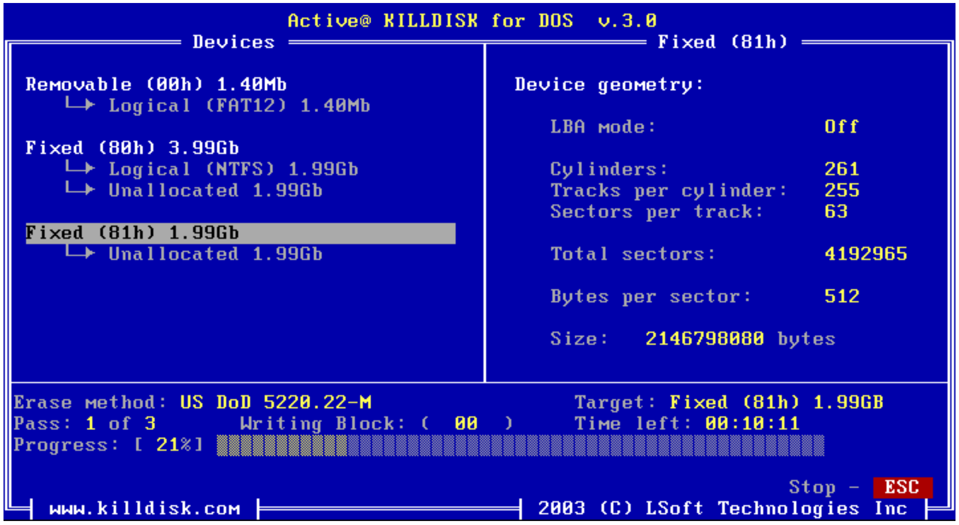


```
allocated 3.94Mb                  Active:
                 Confirm Action

   Target: Logical (FAT12) 1.40MB

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

                                  Size:      1474560 b
```

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 is monitored in the **Disk Erasing** screen, similar to the one below:

Figure 3-5 Disk Erasing in Progress



```
                     Active@ KILLDISK for DOS  v.3.0
 ================== Devices ============================ Fixed (81h) ====
  Removable (00h) 1.40Mb                  Device geometry:
     └→ Logical (FAT12) 1.40Mb
                                             LBA mode:                Off
  Fixed (80h) 3.99Gb
     └→ Logical (NTFS) 1.99Gb                Cylinders:               261
     └→ Unallocated 1.99Gb                   Tracks per cylinder:     255
                                             Sectors per track:       63
  Fixed (81h) 1.99Gb
     └→ Unallocated 1.99Gb                   Total sectors:           4192965

                                             Bytes per sector:        512

                                             Size:    2146798080 bytes

 Erase method: US DoD 5220.22-M               Target: Fixed (81h) 1.99GB
 Pass: 1 of 3       Writing Block: (  00  )   Time left: 00:10:11
 Progress: [ 21%] ▓▓▓▓▓▓▓▓▓▓▓░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░

                                                              Stop - ESC
 ─┤ www.killdisk.com ├──────────────────────┤ 2003 (C) LSoft Technologies Inc ├─
```

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 is not recoverable.

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 are reported on the Interactive screen. If such a message appears, it is 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 displays the Microsoft DOS prompt.

3 At the DOS prompt, display **Active@ KillDisk** parameters by typing:

```
A:\>killdisk -?
```

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

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 is erased in seven passes without user confirmation.

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.

Table 3-2 Command Line Parameters

Parameter	Default	Options
no parameter		With no parameter, the DOS Interactive screens appear.
-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 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 tries to write in the sector 5 times by default.
-erasehdd=[80h - 83h]		By default, the utility erases the first logical drive encountered. Use this parameter to direct the erasing procedure to the correct target.
-ignoreerrors	ON	By default, the erasing process stops 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 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.

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 is erased in one pass. Confirmations are encountered and errors are 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.

Erasing Data Using Autoexecute

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 indicates booting into DOS. The data erase process begins.

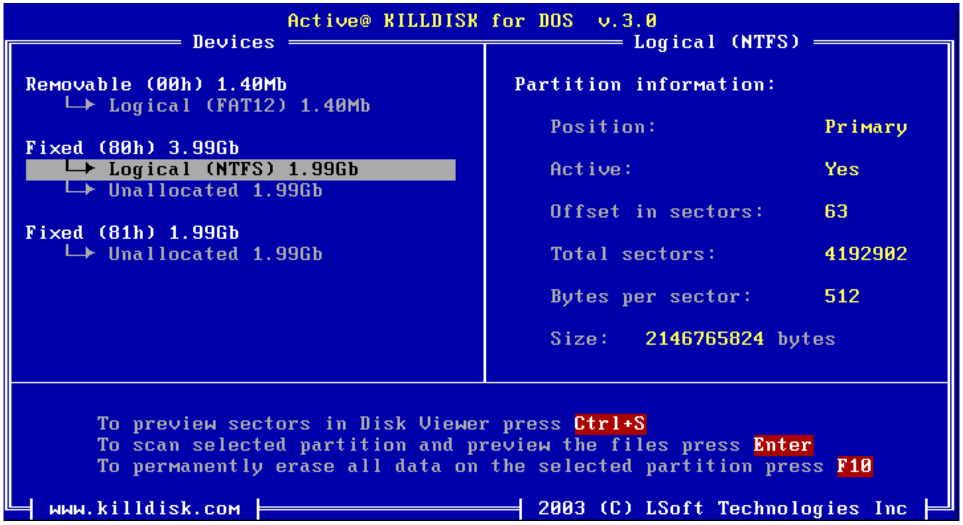
Erasing Logical Drives (Partitions)

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



```
                     Active@ KILLDISK for DOS  v.3.0
 ═══════════════ Devices ════════════════╤════════ Logical (NTFS) ════════
  Removable (00h) 1.40Mb                 │  Partition information:
     └→ Logical (FAT12) 1.40Mb           │
                                         │     Position:            Primary
  Fixed (80h) 3.99Gb                     │
     └→ Logical (NTFS) 1.99Gb            │     Active:              Yes
     └→ Unallocated 1.99Gb               │
                                         │     Offset in sectors:   63
  Fixed (81h) 1.99Gb                     │
     └→ Unallocated 1.99Gb               │     Total sectors:       4192902
                                         │
                                         │     Bytes per sector:    512
                                         │
                                         │     Size:   2146765824 bytes
 ────────────────────────────────────────┴─────────────────────────────────

        To preview sectors in Disk Viewer press Ctrl+S
        To scan selected partition and preview the files press Enter
        To permanently erase all data on the selected partition press F10

 ╡ www.killdisk.com ╞══════════════════════╡ 2003 (C) LSoft Technologies Inc ╞
```

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

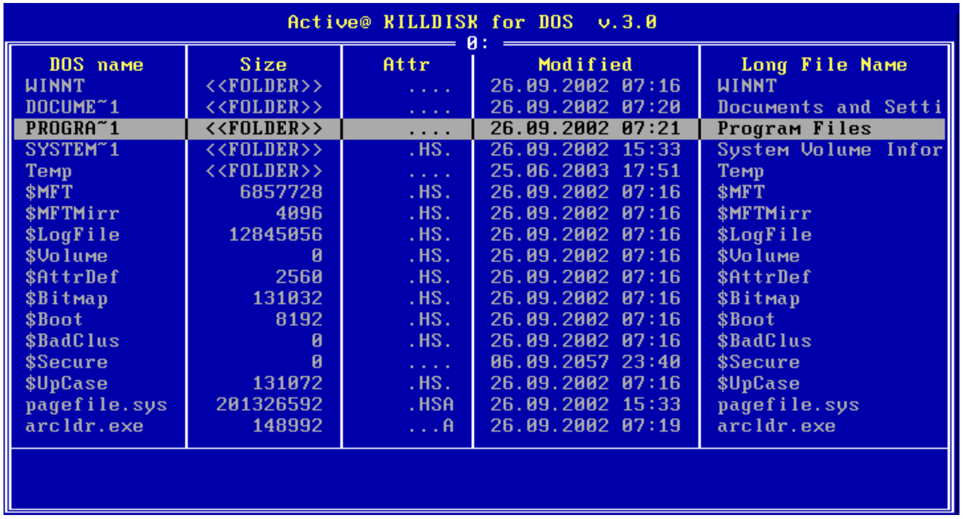
2 Position the cursor over a logical disk or an Unallocated area. A set of options appears in the lower pane of this window.

3 Press **[Ctrl + S]** to open **Disk Viewer** and preview all sectors of this drive

4 When positioned on a logical drive, press **[Enter]** to scan the drive and preview files and folders on the drive. This option allows you to thoroughly check the drive’s folders, hidden and visible files and previously deleted files before erasing data.

When you press **[Enter]**, an activity bar appears while the drive contents are scanned. After the scan has completed, the contents of the drive are displayed similar to the figure below:

Figure 3-7 Scan Results Display



```
                       Active@ KILLDISK for DOS  v.3.0
                                      0:
  DOS name    |    Size     |  Attr  |     Modified      |  Long File Name
WINNT         | <<FOLDER>>  |   .... | 26.09.2002 07:16  | WINNT
DOCUME~1      | <<FOLDER>>  |   .... | 26.09.2002 07:20  | Documents and Setti
PROGRA~1      | <<FOLDER>>  |   .... | 26.09.2002 07:21  | Program Files
SYSTEM~1      | <<FOLDER>>  |   .HS. | 26.09.2002 15:33  | System Volume Infor
Temp          | <<FOLDER>>  |   .... | 25.06.2003 17:51  | Temp
$MFT          |    6857728  |   .HS. | 26.09.2002 07:16  | $MFT
$MFTMirr      |       4096  |   .HS. | 26.09.2002 07:16  | $MFTMirr
$LogFile      |   12845056  |   .HS. | 26.09.2002 07:16  | $LogFile
$Volume       |          0  |   .HS. | 26.09.2002 07:16  | $Volume
$AttrDef      |       2560  |   .HS. | 26.09.2002 07:16  | $AttrDef
$Bitmap       |     131032  |   .HS. | 26.09.2002 07:16  | $Bitmap
$Boot         |       8192  |   .HS. | 26.09.2002 07:16  | $Boot
$BadClus      |          0  |   .HS. | 26.09.2002 07:16  | $BadClus
$Secure       |          0  |   .... | 06.09.2057 23:40  | $Secure
$UpCase       |     131072  |   .HS. | 26.09.2002 07:16  | $UpCase
pagefile.sys  |  201326592  |   .HSA | 26.09.2002 15:33  | pagefile.sys
arcldr.exe    |     148992  |   ...A | 26.09.2002 07:19  | arcldr.exe
```

Navigate up and down the displayed list using up and down arrows or Page Up and Page Down keys. Press **[Enter]** to open a folder and view the contents. Similarly, press **[Enter]** to open Disk Viewer and view the contents of a file.

Press **[Esc]** when finished viewing to return to the **Detected Physical Devices** window.

5 In the Detected Physical Devices window, press **[F10]** 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 allows 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 are 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 ERASING PARAMETERS

This chapter describes the parameters used with various erasing 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 writes 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 is 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 truncates before erasing starts. After erasing is completed, the log file contains 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 appends 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.