



User Guide

Table of Contents

1	Product Overview	3
1.1	Erasing Confidential Data.....	3
1.1.1	Advanced Data Recovery Systems.....	3
1.1.2	International Standards in Data Removal.....	3
1.2	Wiping Confidential Data from Unoccupied Drive Space.....	4
2	System Requirements.....	4
2.1	DOS version.....	4
2.1	Personal Computer	4
2.2	Drive Storage System.....	4
2.3	Other Requirements.....	4
2.2	Windows version.....	5
2.1	Personal Computer	5
2.2	Drive Storage System.....	5
2.3	Other Requirements.....	5
3	Running Active@ KillDisk	7
3.1	Preparing a Vista-based Bootable CD (Professional package only).....	7
3.2	Modes of Operation.....	7
3.2.1	Interactive Mode.....	7
3.2.2	Command Line Mode.....	16
3.3	Erasing or Wiping Logical Drives (Partitions).....	18
3.5	Erase or Wipe Operation Complete	19
4	Common Questions.....	19
4.1	How does the licensing work?	19
4.2	How is the data erased?	19
4.3	What is the difference between the Site and Enterprise license?	20
4.4	Which operating systems are supported by Active@ KillDisk?.....	20
4.5	Is Active@ KillDisk compatible with Macintosh computers?	20
4.6	Will I be able to use my Hard Disk Drive after Active@ KillDisk erase operation?	20
4.7	Why I cannot boot the machine from CD/DVD-ROM?.....	20
5	Descriptions of Erase/Wipe Parameters.....	21
5.1	Erase/Wipe Methods	21
5.1.1	One Pass Zeros or One Pass Random.....	21
5.1.2	User Defined	21
5.1.3	US DoD 5220.22-M	21
5.1.4	German VSITR.....	21
5.1.5	Russian GOST p50739-95	21
5.1.6	Gutmann.....	21
5.2	Other Parameters.....	21
5.2.1	Verification	21
5.2.2	Retry Attempts	22
5.2.3	Ignore Errors	22
5.2.4	Clear Log File before Start.....	22
5.2.5	Skip Confirmation	22
5.2.6	Wipe out Deleted/Unused data.....	22
6	Glossary of Terms.....	23

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 (DOS version) or Windows Vista-based bootable CD/DVD (Windows version). Access to the drive's data in DOS 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 either from DOS or drive is being locked under Windows before wiping starts. 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 MFT 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 DOS version

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.

2.2 Windows version

2.1 Personal Computer

IBM PC/AT compatible CPU

Intel Pentium or higher

300 Mb of RAM

Video must be VGA or better resolution (800x600)

2.2 Drive Storage System

CD or DVD-ROM drive

Hard Disk Drive type IDE, ATA, SATA or SCSI with controllers (additional drivers could be loaded for RAID's or non-standard controllers after system booted up)

2.3 Other Requirements

Blank CD or DVD to burn an ISO image.

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	Yes	Yes
Erases partitions, logical drives and unused disk space	Yes	Yes
Supports IDE / ATA / SATA / SCSI hard disk drives	Yes	Yes
Supports fixed disks, floppies, zip drives, FlashMedia drives	Yes	Yes
Supports large-sized drives (more than 128GB)	Yes	Yes
Supports Command Line mode (can be run with no user interaction)	Yes	Yes
Operates from floppy disk or bootable CD-	Yes	Yes

ROM drive		
Erases with one-pass zeros	Yes	Yes
Erases with one-pass random characters		Yes
Erases with user-defined number of passes (up to 99)		Yes
US Department of Defense 5220.22 M compliant		Yes
German VISTR compliant		Yes
Russian GOST p50739-95 compliant		Yes
Gutmann method compliant		Yes
Customizable security levels		Yes
Supports all detected hard disk drives	Yes	Yes
Erasing report is created and can be saved as a file	Yes	Yes
Displays detected drive and partition information	Yes	Yes
Scans NTFS and FAT volumes and displays existing and deleted files and folders	Yes	Yes
Data verification may be performed after erasing is completed		Yes
Disk Viewer allows you to preview any sectors or file clusters on a drive	Yes	Yes
Includes DOS real mode utility, which operates in the most secure and reliable environment	Yes	Yes
Wipes out NTFS, FAT32, FAT16 and FAT12 volumes from areas containing deleted and unused data	Yes	Yes
Wipes out free clusters (unused by file data sectors)	Yes	Yes
Wipes out file slack space (unused bytes in the last cluster occupied by file)	Yes	Yes
Wipes out deleted MFT and ROOT system records	Yes	Yes

Wipes out unused space in any MFT records and compressed clusters	Yes	Yes
---	-----	-----

3 Running Active@ KillDisk

After you purchase Active@ KillDisk, you will receive an installation file named KILLDISK-SETUP.EXE. This file contains everything you need to set up and run the application. Double-click KILLDISK -SETUP.EXE to run installation and follow the instructions.

3.1 Preparing a Vista-based Bootable CD (Professional package only)

This chapter describes how to create a Windows Vista-based-bootable CD/DVD-ROM that contains the Active@ KillDisk application.

3.2 Modes of Operation

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

- Interactive Mode
- Command Line Mode

It is wise to label the CD/DVD-ROM to identify the way you plan to use Active@ KILLDISK for Hard Drives.

3.2.1 Interactive Mode

This section describes how to use the Interactive 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.

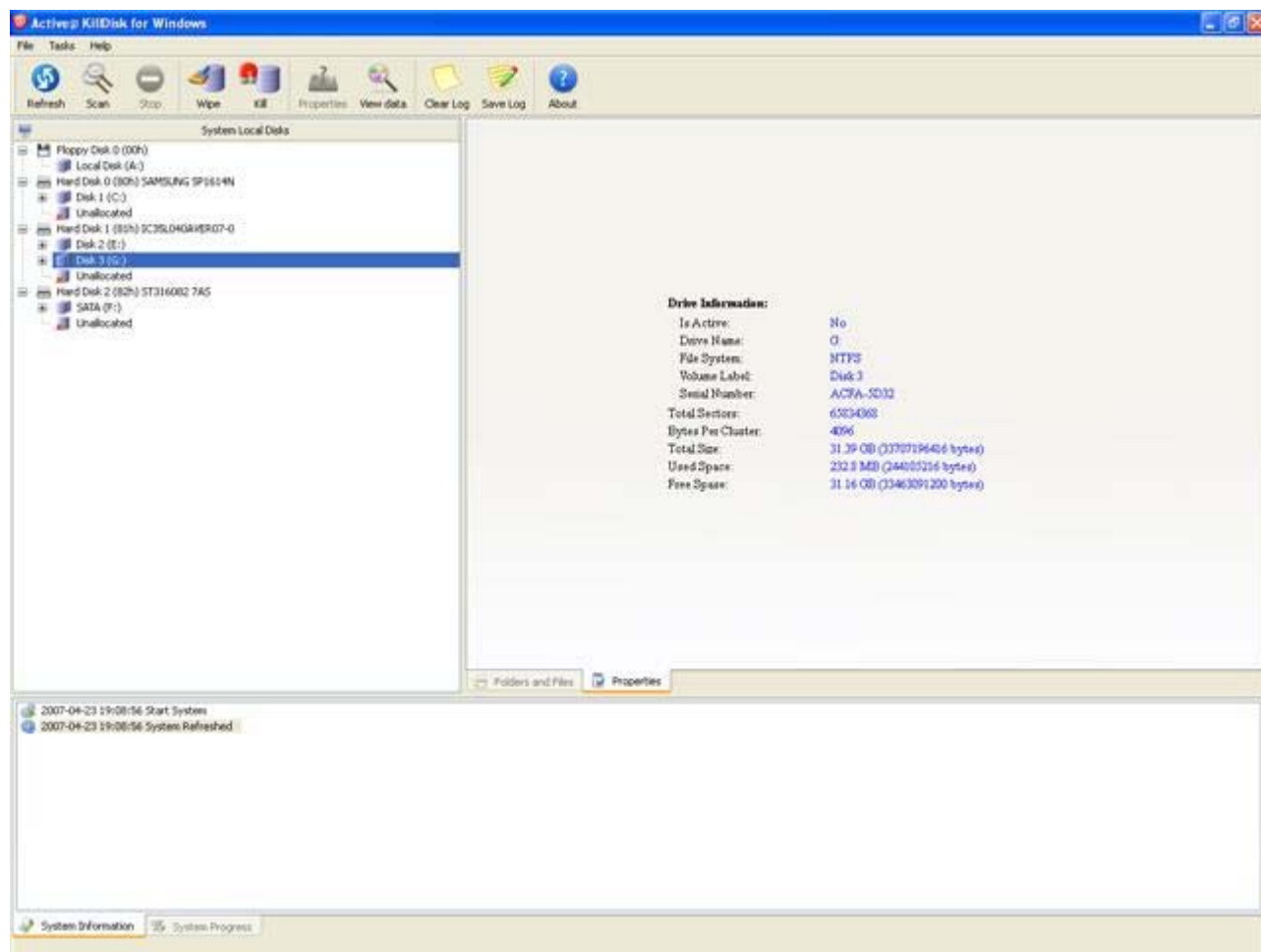
If you are booting from a CD/DVD-ROM drive, check that the CD/DVD drive has boot priority in the BIOS settings of your computer.

Here are the steps for interactive operation:

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

The Detected Physical Devices screen appears.

Figure 3-1 Detected Physical Devices



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

2. Change the position of the cursor in the list using the keyboard **[Down]** and **[Up]** arrow keys, or using the mouse.

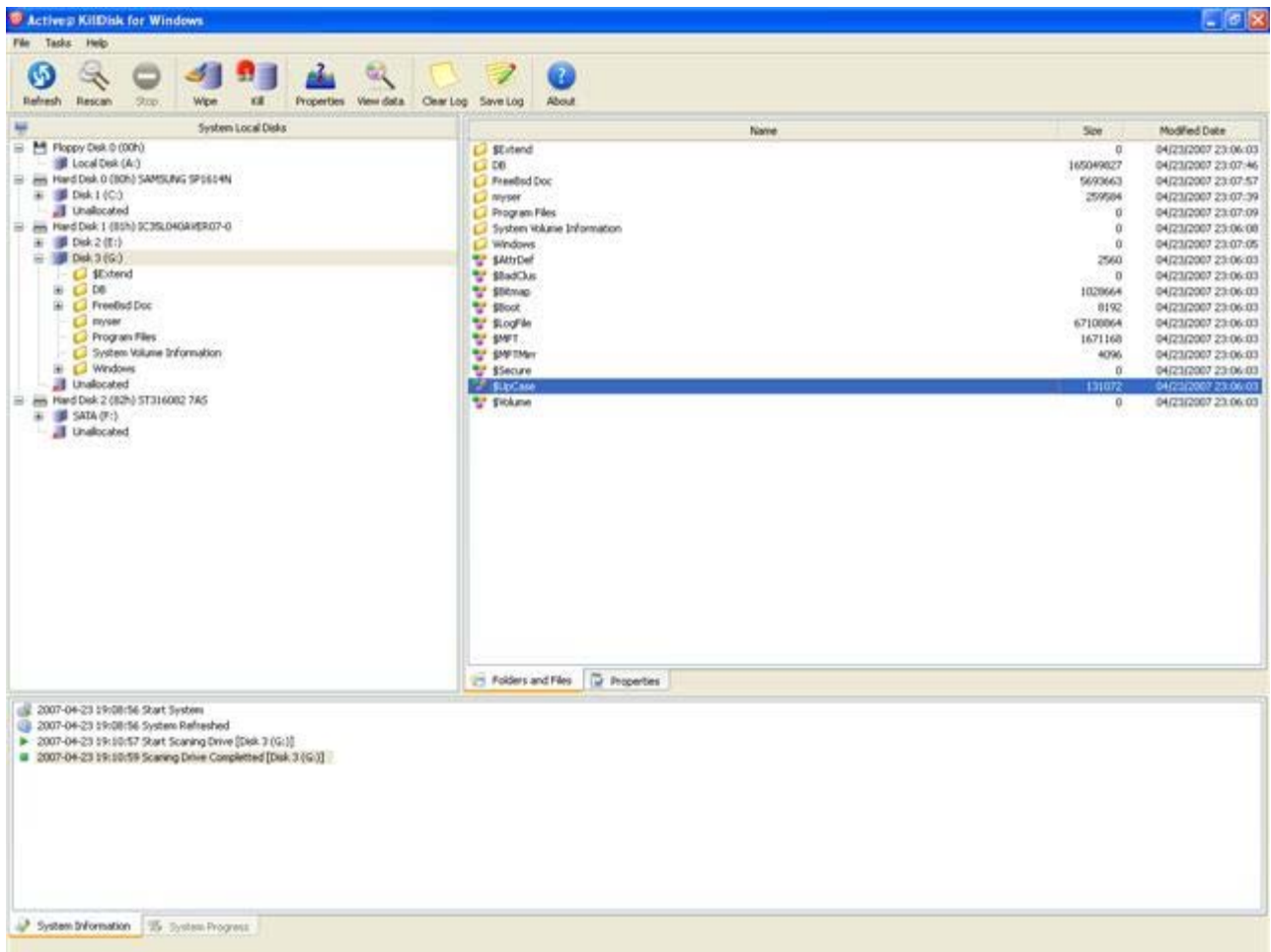
Hard drive devices are numbered by the system BIOS. A system with a single hard drive shows as number 0. Subsequent hard drive devices are numbered consecutively. For example the second device will be shown as **Hard Disk 1**.

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.

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

To preview the sectors in a device, press **[Ctrl + V]** or click **View Data** button on the toolbar. The **Data Viewer** screen appears.

Figure 3-2 Data Viewer



8. Press **[Tab]** to switch between the panels, or use the mouse.

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

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

3.2.1.1 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

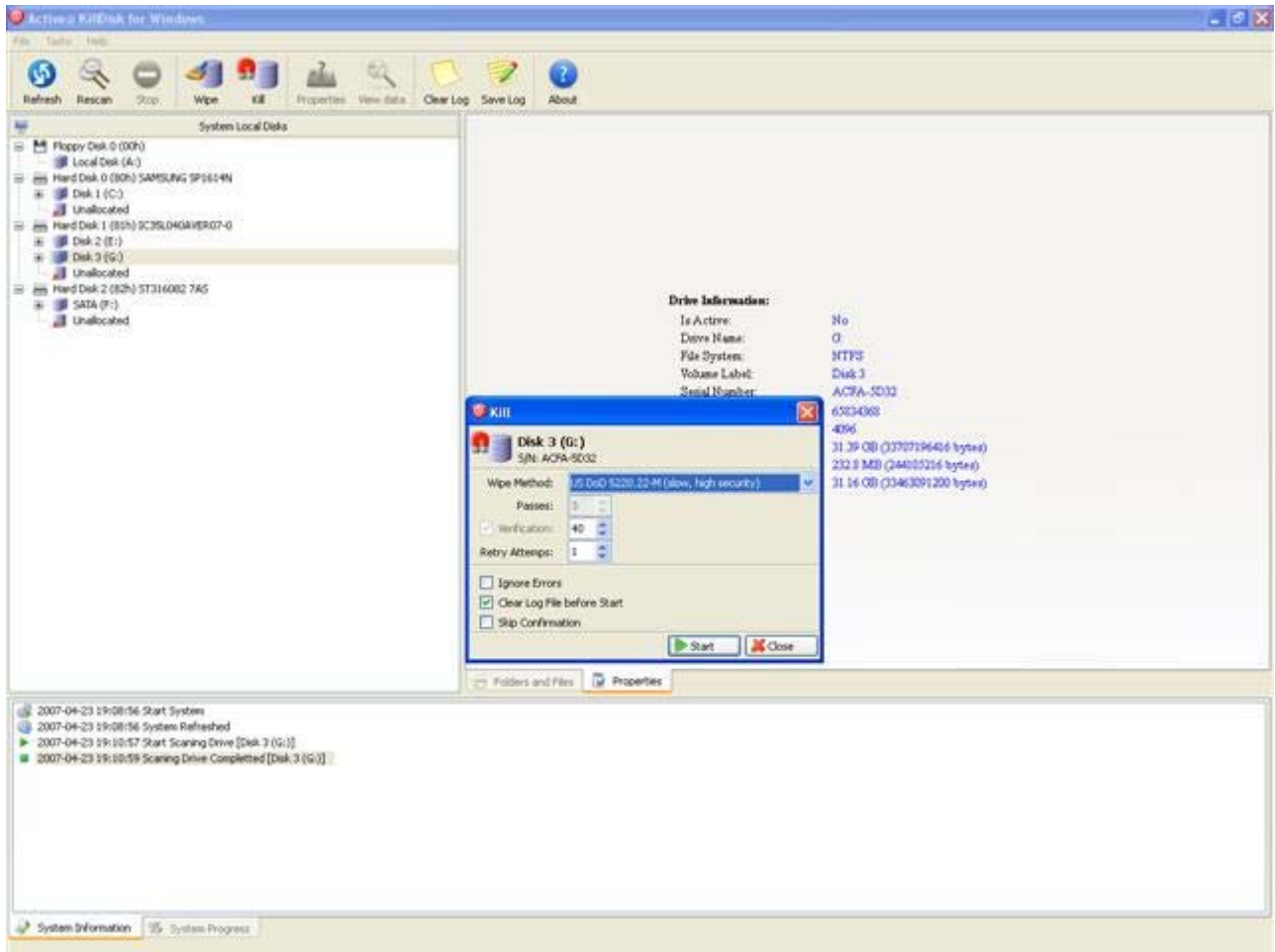
3.2.1.2 Wiping the Data.

If you want to erase data on selected logical drives, follow the steps in 3.3 *Erasing or Wiping Logical Drives (Partitions)*.

To erase the data:

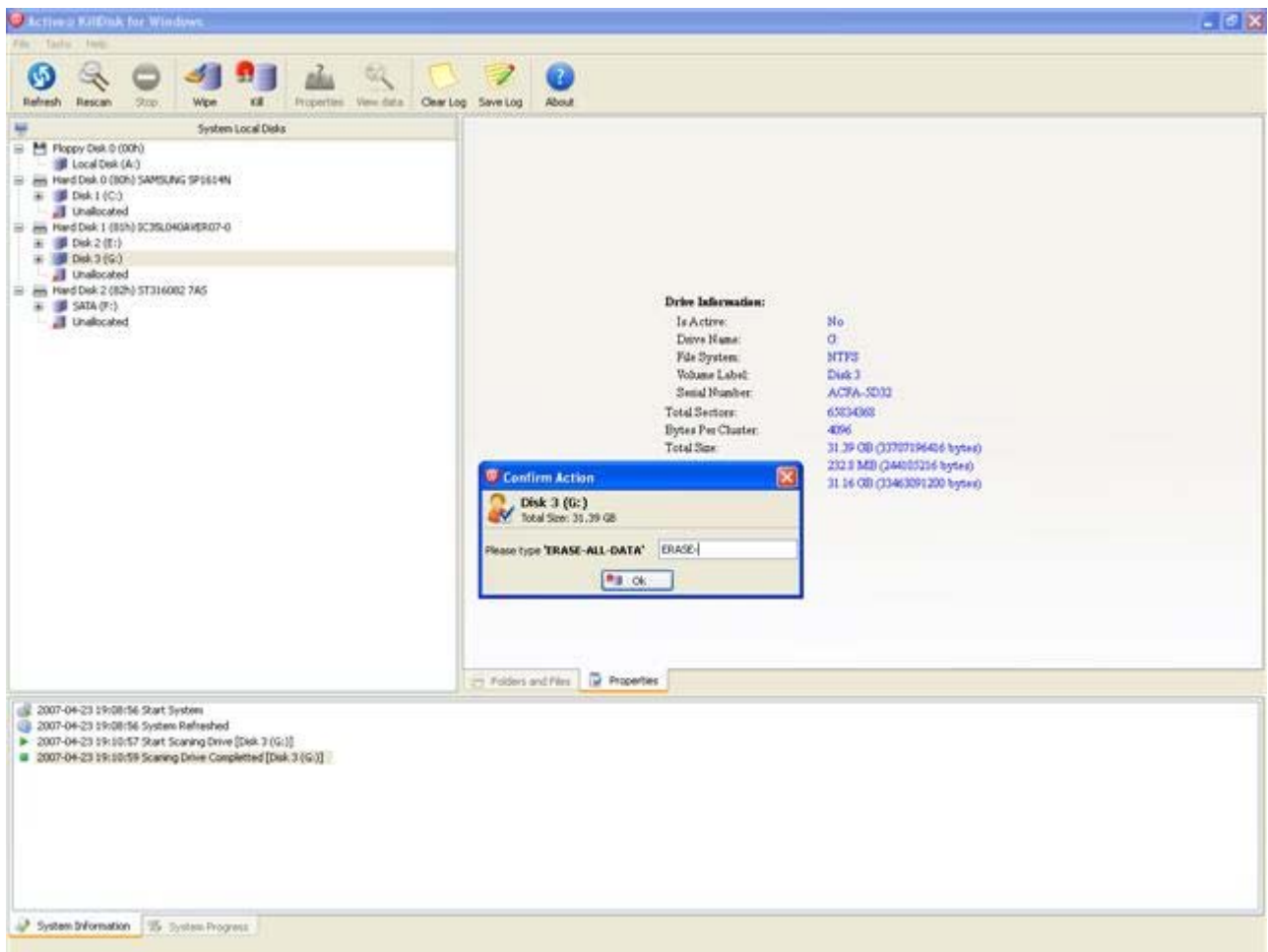
1. Be certain that the drive you are pointing to is the one that you want to erase. All data will be permanently erased with no chance for recovery.
2. When you have selected the device to erase, move the cursor to that device. To permanently erase all data on the selected partition, press **[F10]** or click **Kill** button on the toolbar. The **Erase Method** screen appears.

Figure 3-4 Erase Method



3. To select a different erase method, use arrows or mouse to choose it from a combobox. Erase methods are described in *Chapter 5 Descriptions of Erase/Wipe Parameters* in this guide
4. To change another parameter, use the arrow keys, or mouse to move the cursor to the parameter. For information on these parameters, see *Chapter 5 Descriptions of Erase/Wipe Parameters* in this guide.
5. After parameters have been set,
6. After parameters have been set, to advance to the final step before erasing data, After parameters have been set. The **Confirm Action** screen appears.

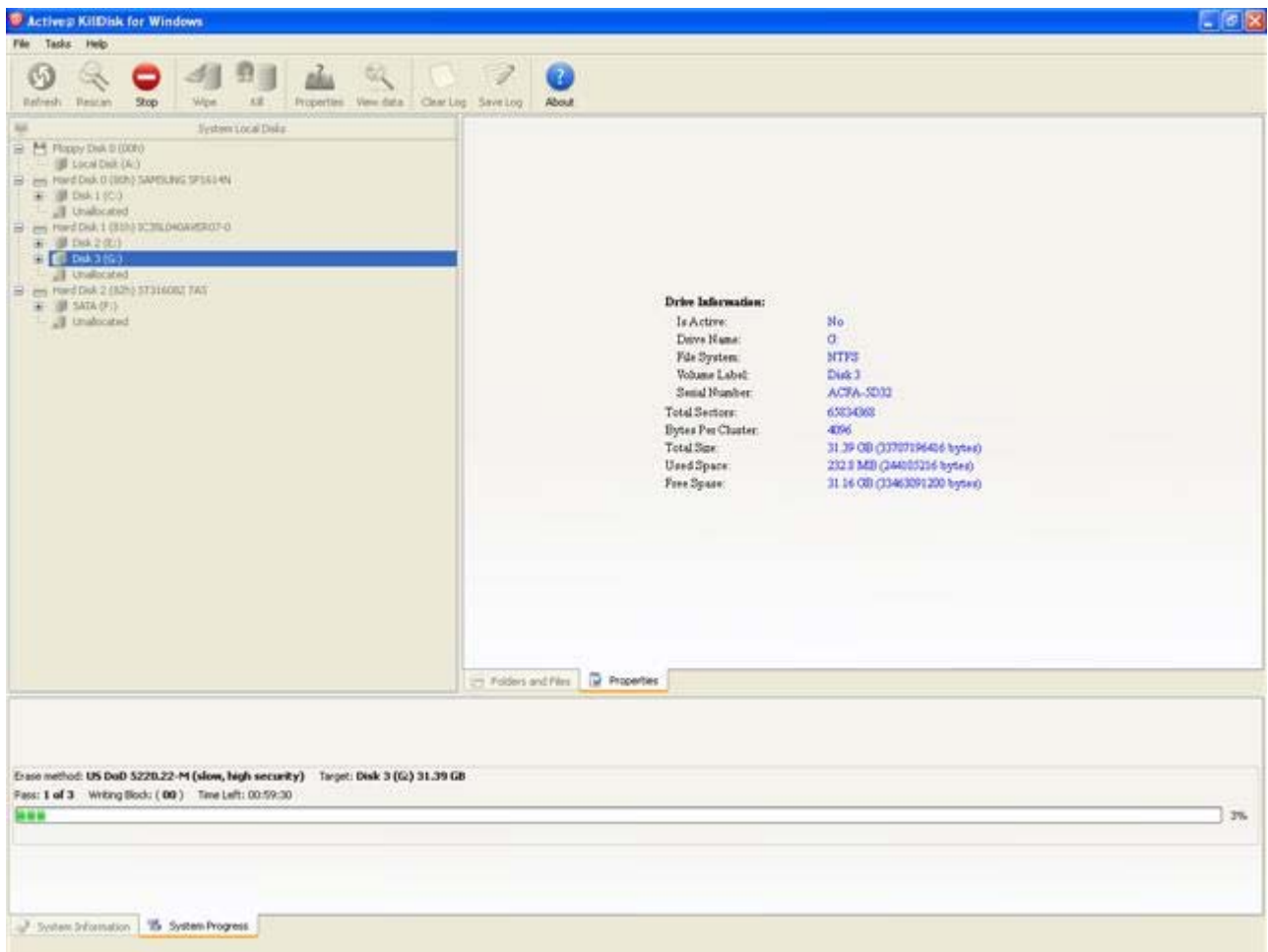
Figure 3-5 Confirm Action



7. 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]** or click **OK** button. 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



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

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

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

3.2.1.2 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.

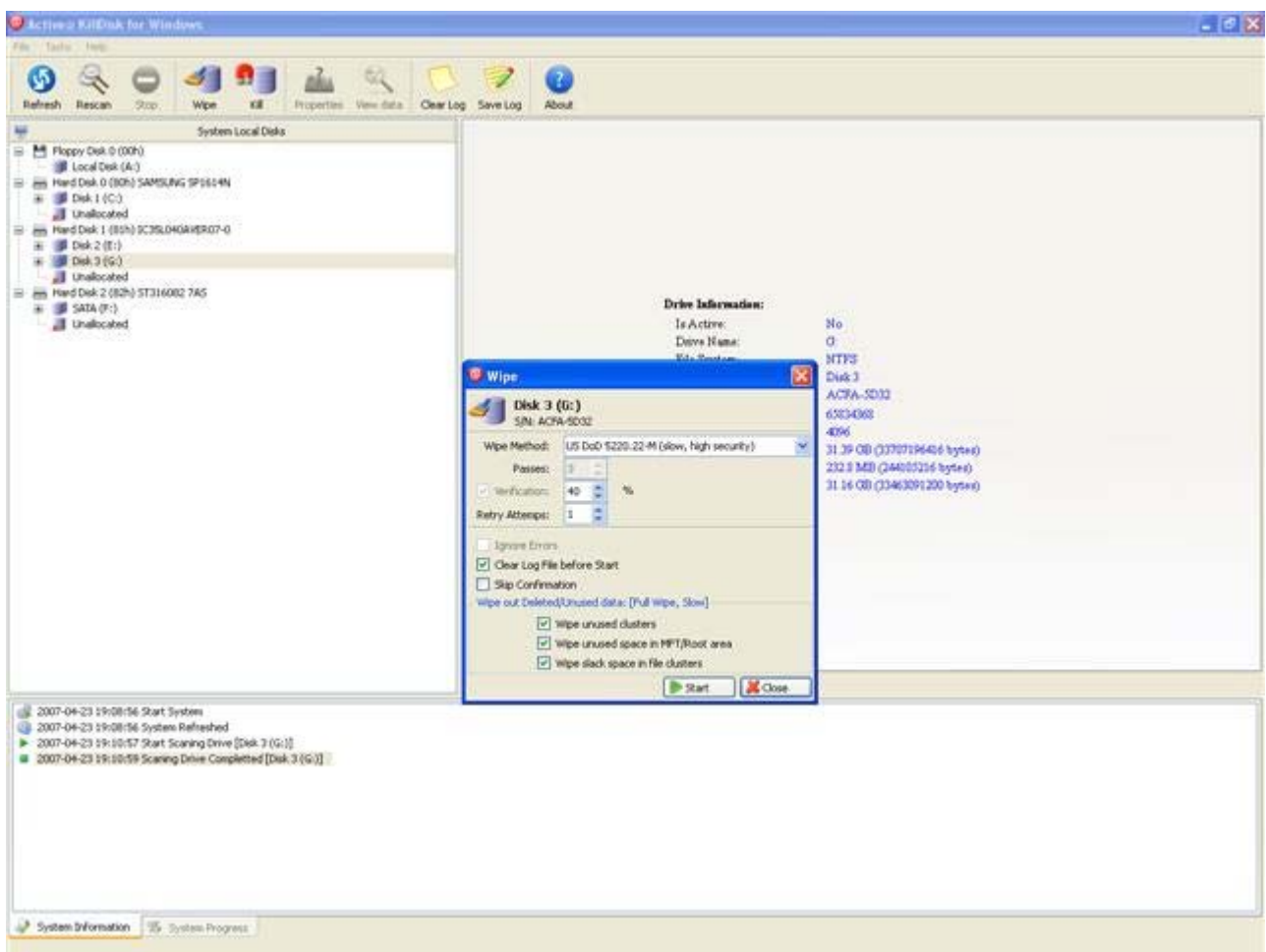
If you want to erase data from the hard drive device permanently, see *3.2.1.1 Erasing the Data*.

If you want to wipe data in unoccupied areas on selected logical drives, follow the steps in *3.3 Erasing or Wiping Logical Drives (Partitions)*.

To wipe data:

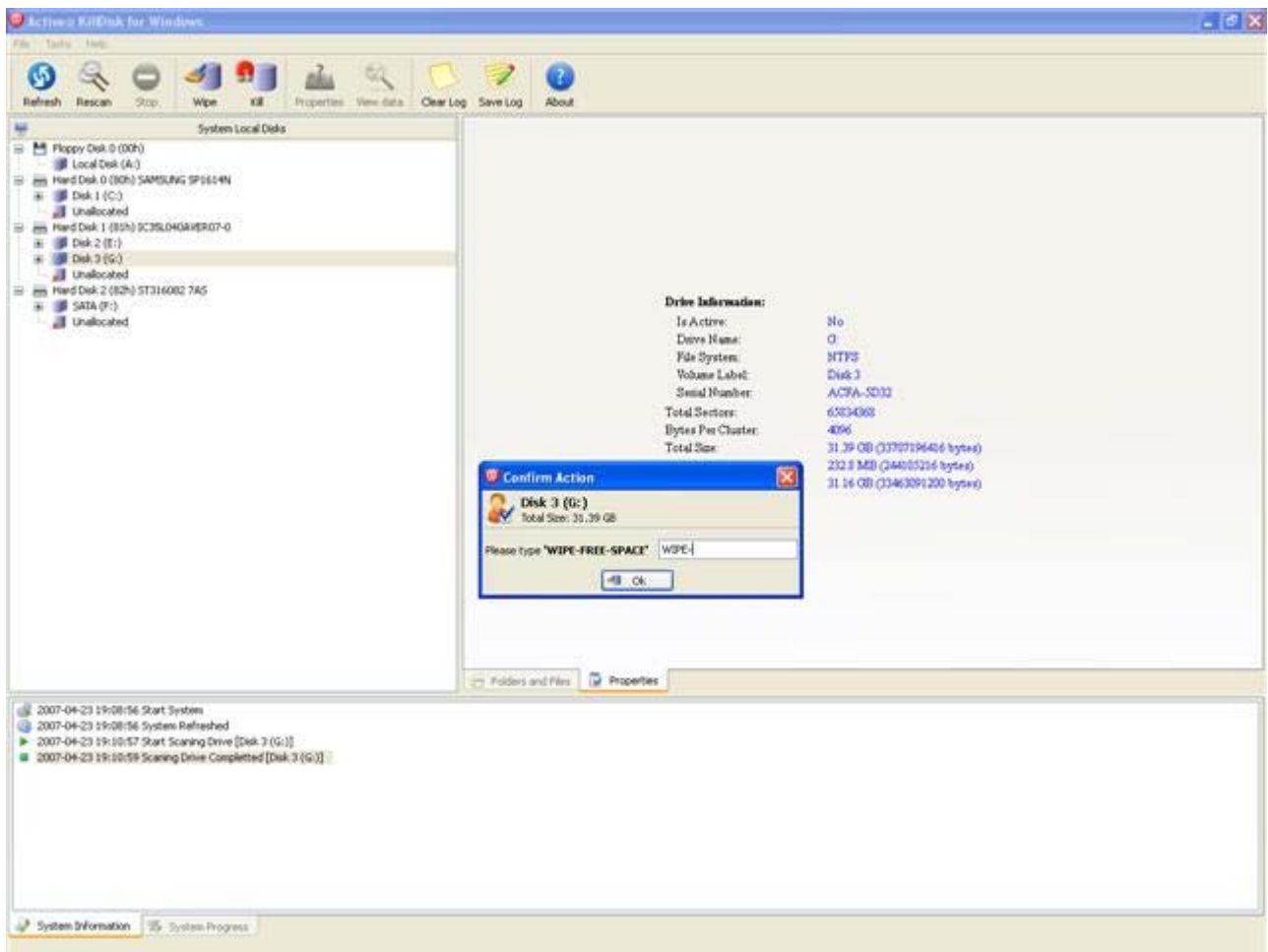
1. When you have selected the device to wipe, move the cursor to that device. To wipe all data in unoccupied sectors on the selected partition, and press **[F9]** or click the **Wipe** button on the toolbar. The Wipe Method screen appears.
2. To select a different wipe method, choose it from the combobox. Wipe methods are described in *Chapter 5 Descriptions of Erase/Wipe Parameters* in this guide.
3. To change another parameter, use the arrow keys, or mouse to move the cursor to the parameter. For information on these parameters, see *Chapter 5 Descriptions of Erase/Wipe Parameters* in this guide.

Figure 3-7 Wipe Options Screen



4. After parameters have been set, to advance to the final step before erasing data, click **START** button. The Confirm Action screen appears.

Figure 3-8 Confirm Action



5. 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]** or click **OK** button. Progress of the wiping procedure will be monitored in the **Disk Wiping** screen.

6. 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.

7. 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.

8. 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 Data Viewer screen appears.

Existing file names and folder names appear with yellow icon and deleted file names and folder names appear with gray icon. If the wiping process completed correctly, the data residue in these deleted file clusters and the place these files hold in the root records or

MFT records has been removed and you should not see any gray-coloured icons for files or folders in the wiped partition.

3.2.2 Command Line Mode

To run Active@ KillDisk in command line mode, at Command prompt, display Active@ KillDisk for Hard Drives parameters by typing:

```
KILLDISK.EXE -?
```

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.
-ignoreerrors	-ie	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?
-beep	-bp	Beep after erasing is complete.
-wipeallhdds	-wa	Wipe all hard drives.
-wipehdd = [80h-8Fh] -test	-wh=	Name the hard drive to be wiped. 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.

Key the command and parameters into the Command Prompt. Here is an example:

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

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

Here is an example with the wipe disk command:

```
killdisk.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 Command Prompt when complete.

Press **[Enter]** to complete the command and start the process.

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

3.3 Erasing or Wiping Logical Drives (Partitions)

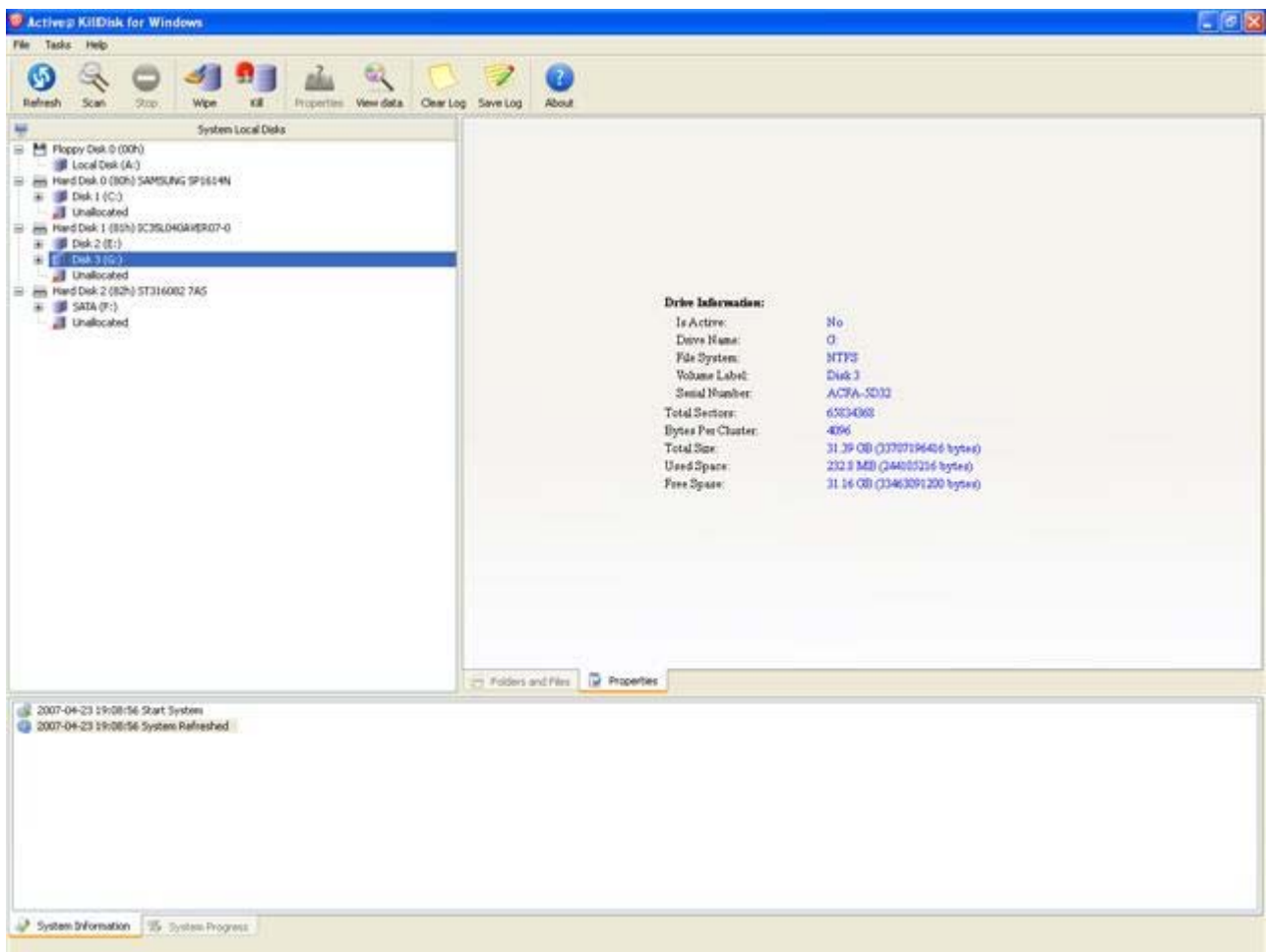
In all previous examples in this chapter, the process has erased data or wiped data from a physical drive. Using a similar method, you can erase or wipe logical disks and partitions, and even “Unallocated” areas where partitions used to exist and the area was damaged, or the area is not visible by the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

Erase Data From a Logical Drive

To erase data from a logical drive, run KillDisk and follow the steps below.

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

Figure 3-9 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.

Position the cursor over the logical disk or on the Unallocated area.

Press **[F10]** or click Kill button 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.

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.

Position the cursor over the logical drive.

Press **[F9]** or click **Wipe** button on the toolbar 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 or the mouse to scroll through the report.

To save the log file, press **[F2]** or execute **Save Log** command from the File menu. Details of this report are saved to a log file.

4 Common Questions

4.1 How does the licensing work?

The software is licensed on a per CD/DVD basis. Each license allows you to use the program from a separate CD/DVD. If you want to use the program to wipe 5 computers concurrently, you would need 5 CD/DVDs (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 hardware device directly. To erase data it overwrites all addressable locations on the drive with zeros (FREE version). Active@ KillDisk Professional version suggests several methods for data destruction. For example, in US DoD 5220.22-M method it overwrites all addressable storage and indexing locations on the drive three

times: with zeros (0x00), complement (0xFF) and random characters; and then verifies all writing procedures. This complies with the US DoD 5220.22-M security standard.

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

Site License means an unlimited usage of the program in one location, Enterprise License - in any location.

4.4 Which operating systems are supported by Active@ KillDisk?

Active@ KillDisk for DOS 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.

Active@ KillDisk for DOS runs in any Windows environment: Windows XP, Vista, Server 2003, etc..

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 utility like FDISK.
- Reformat partitions using a standard utility like FORMAT.
- Reinstall the Operating System using a bootable CD-ROM.

4.7 Why I cannot boot the machine from CD/DVD-ROM?

Machine has boot priority for Hard Disk Drives, or another device set higher than for CD/DVD 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, F2, F10 or Escape on the keyboard during PC startup.
2. 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. 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.

Copyright © 2007, LSOFT TECHNOLOGIES INC. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from LSOFT TECHNOLOGIES INC.

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

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

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

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

LSOFT.NET logo is a trademark of LSOFT TECHNOLOGIES INC.

Other brand and product names may be registered trademarks or trademarks of their respective holders.