LSOFT.NET LSOFT TECHNOLOGIES

Active@ KillDisk

User Guide

Version Number 1.1

Contents

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

Using **Active@ KillDisk**, our powerful and compact free 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.

High Standards

Active@ KillDisk Professional conforms to US Department of Defense clearing and sanitizing standard **DoD 5220.22-M**. 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. Thus it does not matter operating systems and file systems located on the machine, it can be DOS, Windows 95/98/ME, Windows NT/2000/XP, Linux, 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 286
- 640Kb 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 Version	Professional Version
Securely overwrites all data on drive	yes	yes
Displays detected drive information	yes	yes
Supports IDE / ATA / SCSI drives	yes	yes
Supports Fixed Disks, Floppies, Zip Drives, Jazz drives	yes	yes
Supports large format (more than 8GB) drives	yes	yes
Operates independent of Operating System and File System	yes	yes
Supports Command Line mode	yes	yes

Feature	Free Version	Professional Version
Operates from bootable floppy	yes	yes
US Department of Defense 5220.22 M compliant		yes
Customized Security Levels		yes
Supports all detected hard disk drives		yes

3 PROCEDURES

This chapter describes how to use the application.

Prepare DOS-Bootable Floppy Disk (Startup Disk)

Active@ KillDisk operates from the floppy drive in a Microsoft DOS environment. For hard drives on PCs with operating systems other than DOS or Windows, you must create a DOS-bootable floppy on a DOS or Windows machine and use it on your alternate-OS machine.

If you have a bootable floppy, skip to the Copy Active@ KillDisk section, below.

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

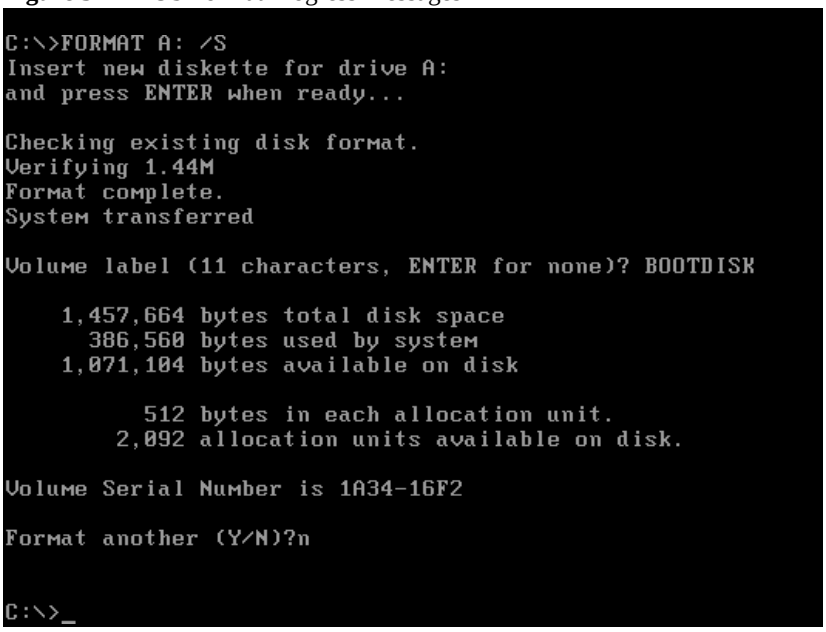
1 From MS-DOS or in Command Prompt mode of Windows 95/98:

a On the screen, type the format command as follows (see Figure 1):

```
FORMAT A: /S
```

b Follow on-screen messages until process is complete.

Figure 3-1 DOS Format Progress Messages



2 From the Windows 95/98/ME screen:

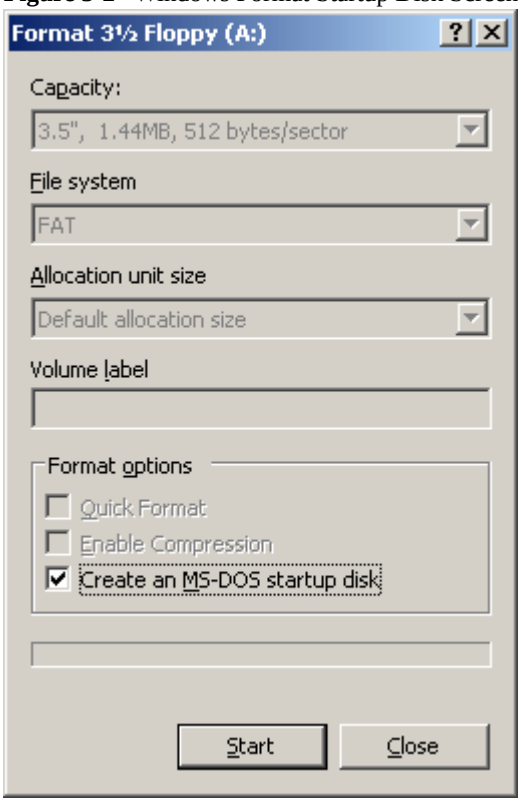
a Click the **Start** button and click **Settings**, **Control Panel**.

b From the **Control Panel** screen, click **Add/Remove Programs**.

c In the **Add/Remove Programs** screen, click the **Startup Disk** tab.

d Click the **Startup Disk...** button and follow the screen instructions until the process is complete.

Figure 3-2 Windows Format Startup Disk Screen



3 From the Windows XP screen:

a Right-click **A: drive**.

b From the drop-down menu, click **Format...**

c Enable the checkbox beside **Create an MS-DOS startup disk**.

d Click the **Start** button and follow the screen instructions until the process is complete.

Copy Active@ KillDisk

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.

Label the Disk

Active@ KillDisk can be used two ways:

- DOS Interactive mode
- Command Line mode

If you plan to use **Active@ KillDisk** in DOS Interactive mode, label the disk as follows:

```
Active@ KillDisk
Data Eraser Utility
```

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.

Boot to DOS (Interactive Mode)

This section describes using **Active@ KillDisk** using the DOS Interactive screens. For "hands-off" operation, please see the next section, below.

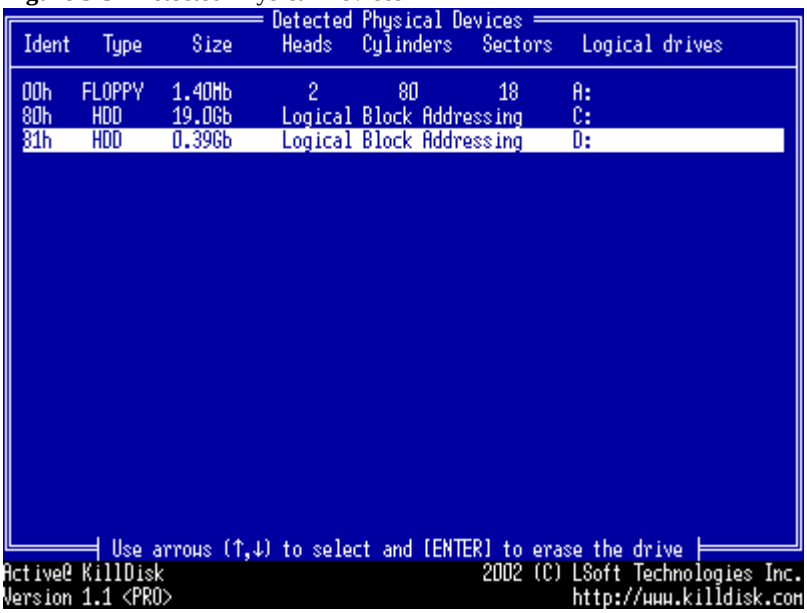
Here are the steps:

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, run **Active@ KillDisk** by typing:

   ```
   KILLDISK.EXE
   ```

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

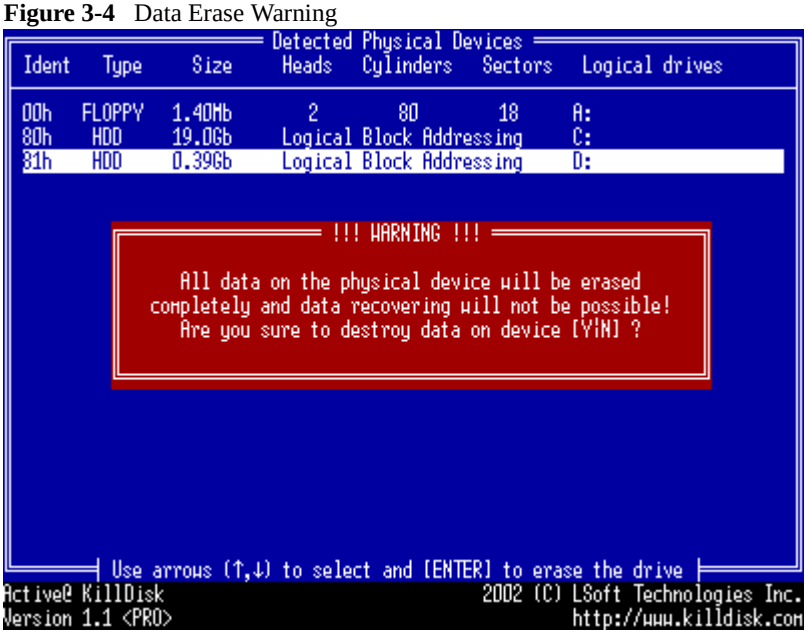
Figure 3-3 Detected Physical Devices



All system hard drives will be displayed along with their system information.

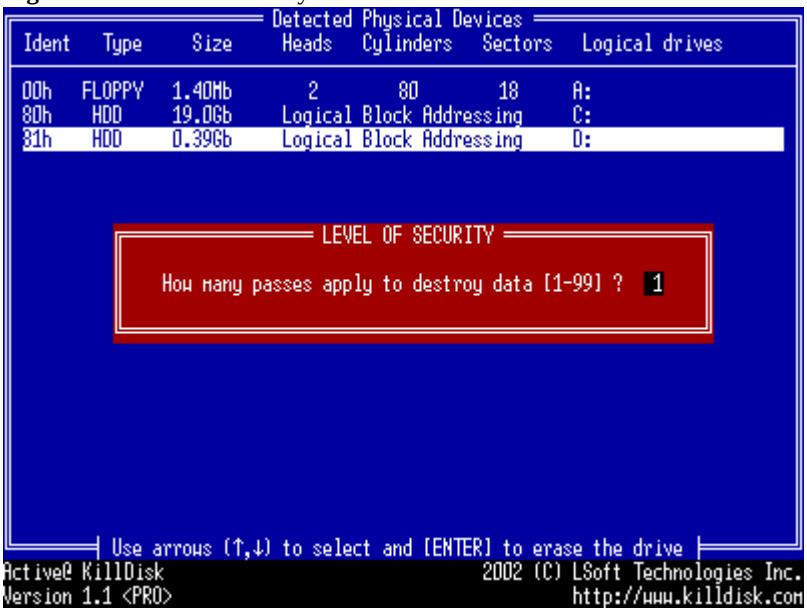
4 Using the keyboard arrow keys, select the drive you want to erase. Press **[Enter]**. The **Data Erase Warning** screen appears.

Figure 3-4 Data Erase Warning



5 Confirm your choice to erase data on selected drive by pressing the letter [**Y**] on the keyboard. The **Level of Security** screen appears.

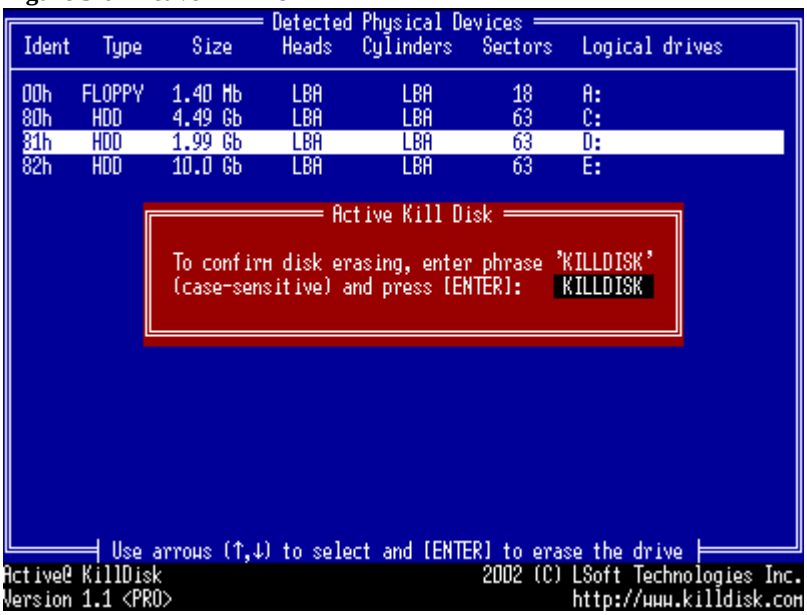
Figure 3-5 Level of Security



6 Each number between 1 and 99 indicates three disk write head passes, as described in the DoD standard specifications. A higher number of passes will ensure a higher level of security. Each time the write head passes over the disk surface, more of the residual data charge will be removed from the disk surface.

Key in the level of security by number between 1 and 99 and press **[Enter]**. (**Active@ KillDisk Professional** version only). The **Active Kill Disk** screen appears.

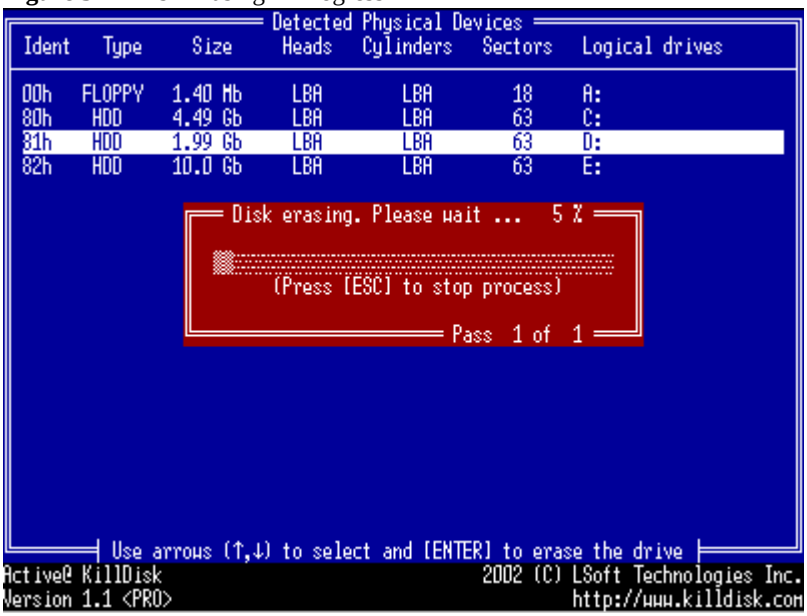
Figure 3-6 Active Kill Disk



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 **KILLDISK** and press **[ENTER]**. Progress of the erasing procedure will be monitored in the **Disk Erasing** screen, similar to the one below:

Figure 3-7 Disk Erasing in Progress



8 If, for any reason you wish to stop the process 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 human 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, it will be possible to cancel the operation (by pressing **[Esc]**), or continue erasing data.

Boot to DOS (Command Line Mode)

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

1. With the PC power off, insert the **Active@ KillDisk** Interactive mode 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. An explanation follows:

Table 3-1 Command Line Parameter Descriptions

Parameter	Description	Note
	No parameter	With no parameter, the DOS Interactive screens will appear.
-?	Question mark	The table of parameters will appear.
-noconfirmation	Skip confirmation steps before erasing starts	By default, confirmation steps will appear in command line mode for each hard drive or floppy: Are you sure? Number of passes? 'KILLDISK' This gives you an opportunity to check the level of security.
-passes:[1-99]	number of passes to overwrite data on disk (1 to 99)	Available only with **Active@ KillDisk Professional** version. Default value is 1.
-ignoreerrors	Do not display error messages (if any)	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.
-killalldrives	Automatically wipe all detected drives and floppies	Caution: All drive devices attached to the system will be erased, including floppy drives, Zip drives and Jazz drives.
-killallfloppies	Automatically wipe all detected floppy drives	If the system supports two floppy drives, insert floppies in both drives.
-killallhdds	Automatically wipe all detected fixed disk drives	Caution: Data from all detected fixed disk drives will be erased.

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

   ```
   A:\>killdisk -killallhdds -passes:7 -noconfirmations
   ```

   In the example above, all detected hard disks will be erased in seven passes with no user confirmations.

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 Figure 3-8, above.

Automatic Boot and Execute (autoexec.bat)

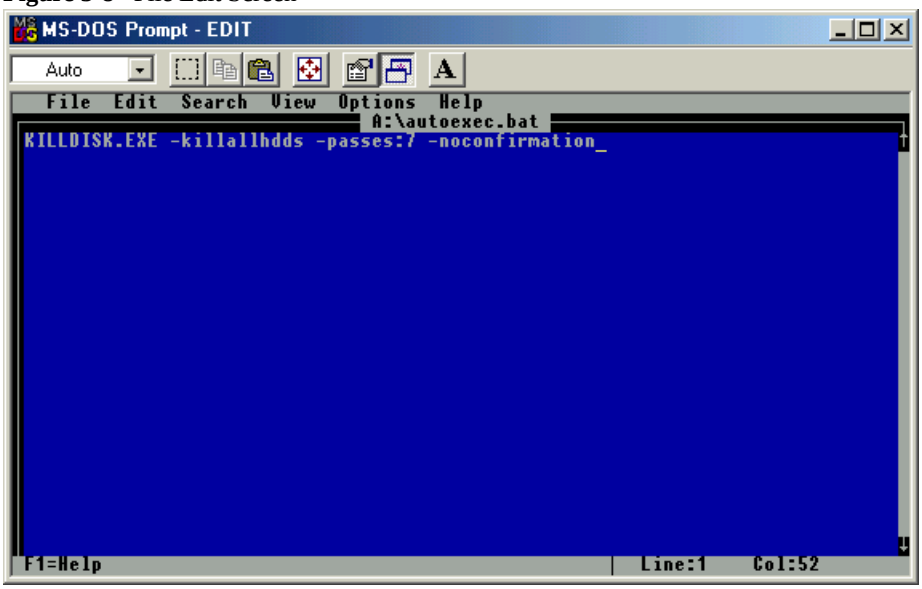
You can use **Active@ KillDisk** in a DOS executable batch file by including a command line containing call of the program and parameters.

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 will appear.

Figure 3-8 File Edit Screen



2 Enter the command line parameters as needed. In the example above, all detected hard disks will be erased in seven passes with no user confirmations.

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

4 Remove the floppy from this floppy drive.

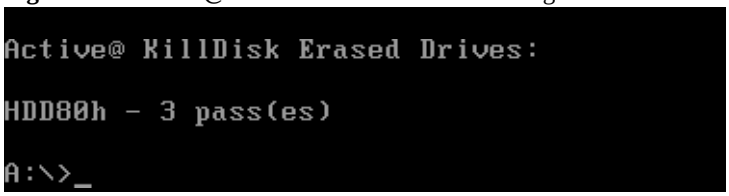
5 The floppy is now ready for automatic data erasing.

6 Turn off power to the PC. Go to the machine that requires data erasing and begin the process as described in Boot to DOS (Command Line Mode), above.

Erase Operation Complete

After operation is completed successfully information on how drives have been erased is displayed as in the screen below:

Figure 3-9 Active@ KillDisk Erased Drives Message



4 COMMON QUESTIONS

What to do I do if I cannot boot the machine from a floppy?

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 (see documentation, beginning with Chapter 3).
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 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 zeros. With each single pass, **Active@ KillDisk Professional** version overwrites all addressable storage and indexing locations on the drive three times with zeros (0x00, 0xFF) and random data. This conforms with the US DoD 5220.22-M security standard.

LSOFT TECHNOLOGIES

LSoft Technologies Inc.
Erasers Software Development Company

http://www.lsoft.net
Phone (416) 893-8796
Fax (905) 785-6735