HP Disk Sanitizer, External Edition

Providing permanent erasure of data on the hard drive for select HP Compaq dc series business desktops
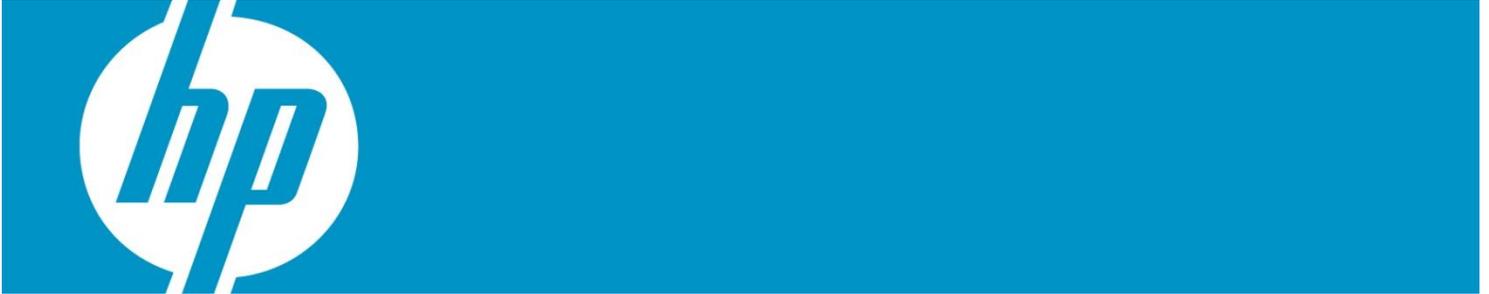
Executive Summary

Did you know deleted files aren't really wiped clean from your hard drive? Simply deleting files from the hard drive is not a secure method to erase data. Anyone with a basic knowledge of data recovery can "undelete" them. To protect your business and comply with industry/governmental regulations, it is important that all data be effectively eliminated from the hard drive prior to recommissioning or retiring assets through recycling or returning equipment at the end of a lease period.

HP Disk Sanitizer, External Edition was designed to completely empty the hard drive for the use cases outlined in the DOD 5220.22-M Supplement for complete disk data erasure. To minimize the ability to recover following erasure, the U.S. government has issued standards that this application attempts to follow as closely as possible. HP Disk Sanitizer, External Edition performs multiple write passes across the drive, writing different patterns of data to ensure all data is permanently erased. The application is flexible, allowing you to select the number of write passes applied to the entire hard drive. Permanent erasure of data is important when passing computers on to different users or resetting hard drives back to factory settings.

This document explains how HP Disk Sanitizer, External Edition works and how to use it.

Benefits

HP Disk Sanitizer, External Edition is available at no charge on www.hp.com. You can save the software either to a CD or to a USB drive for easy use. Whether you are using Microsoft Vista, Microsoft Windows XP, or any other operating system software, HP Disk Sanitizer, External Edition will erase the data permanently from the hard drive.

Overview

HP Disk Sanitizer, External Edition was written using a U.S. Department of Defense algorithm[*] erasure method that writes zeros, then ones, then random bytes to the drive. You will be able to select the number of disk write passes you would like to employ in the disk sanitizing process (from a single write for speed purposes or up to 15 write passes on the entire hard drive for improved security).

After the selected number of passes has been completed, the software writes the completion date/time of the last erase and number of passes to sector 1 of the target hard drive so you will have the information you need to ensure the hard drive is devoid of confidential data.

---

[*] For the use cases outlined in the Department of Defense 5220.22-M supplement.

Instructions

This utility runs only on 2005 and later HP Compaq business desktop dc series systems. The software will validate the HP system, and will prompt you to enter a choice from the main menu (see Figure 1).

Figure 1: Main Menu of HP Disk Sanitizer, External Edition Software

***************DiskSan**************

HP Disk Sanitizer, External Edition, Version 1.00

Copyright (c) 2008 Hewlett-Packard

Please make a choice from the following list:

1: Erase Hard Drive

2: Quick Verify Hard Drive

3: Full Verify Hard Drive

4: DiskSan Help

Q: Exit DiskSan

If you select the Erase, Quick Verify, or Full Verify option, you will be prompted to identify the drive to be erased (see Figure 2). The information displayed on the screen will vary, depending on how many drives are connected.

Figure 2: Drive selection for HP Disk Sanitizer, External Edition

Choose a drive to erase from the following list:

1: Drive 0x80 <> 2.0 GB

2: Drive 0x81 <> 80.0 GB

3: Drive 0x82 <> 160.0 GB

A: Erase All Drives

M: Return To Main Menu

If you have selected the Erase Hard Drive option and have selected a drive, you will then select the number of passes to be executed (see Figure 3).

Figure 3: Selections offered for Write Sequence for HP Disk Sanitizer, External Edition

How would you like to erase Drive 0x82?

1: Single Pass Erase

2: 3 Pass Erase (DoD 5220.22-M Supplement method)

3: 5 Pass Erase

4: 10 Pass Erase

5: 15 Pass Erase

M: Return to Main Menu

Erase Methods

Each erase method follows basically the same formula which is described in more detail below (See Figure 4). Note: Estimated times are based on an 80GB hard drive.

Figure 4: Write Patterns for HP Disk Sanitizer, External Edition

Write Patterns for HP Disk Sanitizer, External Edition

Pass Erase Cycles	Estimated Time*	Description
Single	22 minutes	Writes zeros to the entire hard drive.
3	68 minutes	Writes zeros, then ones, then random hexadecimal digits to the entire hard drive.
5	115 minutes	Writes zeros, then ones, followed by two passes of random hexadecimal digits, then single pass of zeros.
10	230 Minutes	Writes zeros, then ones, followed by seven passes of random hexadecimal digits, then a single pass of zeros.
15	348 minutes	Writes zeros, then ones, followed by twelve passes of random hexadecimal digits, then a single pass of zeros.

Once you choose a secure erase method, you will be prompted to confirm the deletion of data from the hard drive. The utility will then begin erasing the drive.

NOTE

If, at any time, an input error occurs (such as typing an "M" rather than an "N", the application will print an error message. You will then be asked to input a correct selection. The only correct input to be entered is menu selections such as 1, 2, 3, "Y" or "N".

Multiple Drives

Prior to running HP Disk Sanitizer, External Edition, make sure you have correctly identified the drive to be erased. If running in interactive mode, there is a confirmation of the drive to be erased and opportunity to cancel the erase cycle before inadvertently destroying data.

If this application is booted from a USB drive, the USB drive will be detected as hard drive 0x80. **Use caution when choosing which drive to delete.** The best way to proceed is to disconnect all other drives except the drive to be erased in order to ensure that another drive is not accidentally erased.

Please note that when choosing the "Erase All Drives" option, the software will automatically detect which disk is being booted from. If a user boots from a CD, all internal and external (USB) drives will be erased. However, if a user boots from a USB drive key, the first drive to be erased will be Drive 0x81. This is to ensure that the bootable USB drive key is not erased.

RAID Configuration

HP Disk Sanitizer, External Edition supports RAID configuration.

- If two 80GB hard drives are used in mirrored mode (**Raid 1**), one 80GB hard drive will be detected, but both drives will be erased.

- If two 80GB hard drives are used in striped mode (**Raid 0**), one 160GB hard drive will be detected, and both drives will be erased. In all cases, a small section of non-personal metadata used by the RAID controllers will remain on the hard drives.

Maximum Speed

It is important to keep in mind that no matter how quickly and efficiently the code can execute, the speed of writing to the hard drive is restricted by physical and mechanical limitations of the read and write heads. Even in the future, the CPU will be able to process and execute the application faster than the hard drive will ever be able to move the heads. So essentially, as soon as the program fills up the hard drive's write buffer, the speed at which the drive is written to will remain constant.

Furthermore, this application performs one disk erase or verify at a time, providing status as the write or verification pass progresses across the drive. While multiple drives can be erased, each will increase the erasure time required.

Preventing Data Loss

When erasing a disk, HP strongly recommends that you disconnect all other hard drives from the system in order to prevent accidental loss of data.

- If you boot the Disk Sanitizer utility from a USB drive, the USB drive will be detected as drive 0x80. Use caution when selecting which drive to delete and take note of the drive size displayed to avoid erasing the wrong drive. USB drives are typically less than 5GB.
- If you use RAID mode, HP recommends that you change to IDE mode before running this utility.

If you run this utility in RAID mode, there will be a small section of RAID metadata that will not be erased from the hard drive. This RAID metadata does not contain user data.