

X-Ways Software Technology AG

WinHex

Clearing Computer Media

Instructions

1 Introduction

This paper discusses how to clear or sanitize magnetic storage media using the WinHex software (<http://www.winhex.com/winhex/>) and how to be sure of the procedure's effectiveness.

Clearing (or wiping) is the secure removal of all data from a media. Media are cleared to shred private and confidential data, e.g. because they are to be passed to other users. After clearing, the data cannot be recovered using any common software (including WinHex itself), conceivably only by highly sophisticated laboratory techniques. Clearing can also be used to prepare a forensically sound mirror drive before cloning, to ensure that no data is left from a previous examination.

Sanitizing (also purging) is even more secure. In general, laboratory techniques cannot retrieve data that has been sanitized. According to the U.S. Department of Defense (DoD), media have to be sanitized before they are released from usage or reused in an environment that does not provide an acceptable level of protection for the data that was on the media.

According to the Clearing and Sanitization Matrix, the standard outlined in the DoD 5220.22-M operating manual, method "c", a hard disk or floppy disk can be *cleared* by overwriting (once) all addressable locations with a single character. This is usually the hexadecimal value 0x00, but can be any other value. To *sanitize* hard disks according to method "d", overwrite all addressable locations with a character, its complement, then a random character, and verify. (This method is not approved by the DoD for sanitizing media that contain *top secret* information.)

Example how to sanitize your media (clear more than once):

- Overwrite first with a certain byte value (e.g. 01010101 = 0x55), then with its complement (10101010 = 0xAA), and finally with random byte values. Consistent with DoD 5220.22-M.

Alternatively,

- Overwrite with random byte values first, then with binary zeroes (00000000 = 0x00), and finally binary ones (11111111 = 0xFF).

2 How to Clear using WinHex

1. Attach the media to a computer with Windows 95, 98, Me, NT, 2000, or XP and a full version of WinHex installed.
2. Close any application that may write to the media.
3. Run WinHex.
4. Select Tools | Disk Editor from the menu (or press F9).
5. Select the media to clear. It must be listed as a physical disk. Click OK.

You will see the hexadecimal and ASCII representation of the media's first sector, usually a system area. Floppy disk: boot sector. Hard disk: master boot record.

6. Select Edit | Fill Disk Sectors from the menu.

In case you select a part of the media as a block before, the menu command will be labelled "Fill Block", and clearing will apply to the block only

7. Select either "Fill with ... hex values" and specify a byte value in hexadecimal notation (without the preceding "0x") or "Fill with random bytes" and specify a range of allowed byte values in decimal notation (usually 0 to 255). Click OK.

In case of large media, the program will warn you that changes will be written immediately to the disk. Remember, you are clearing the media, and any data will be lost. In case of small media like floppy disks, WinHex will buffer the changes and flush them only when closing the edit window, after prompting you to do so.

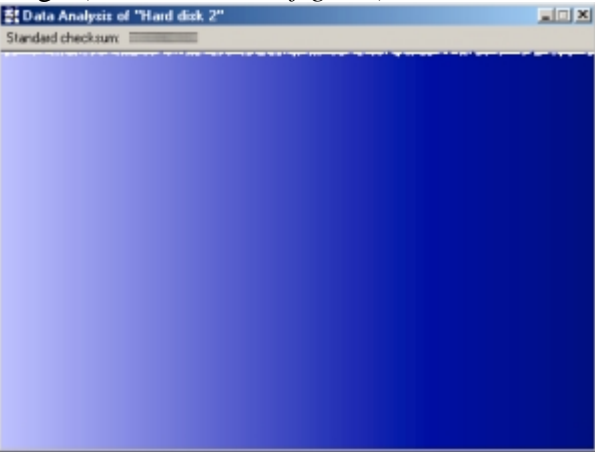
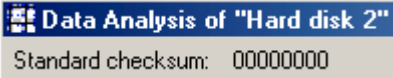
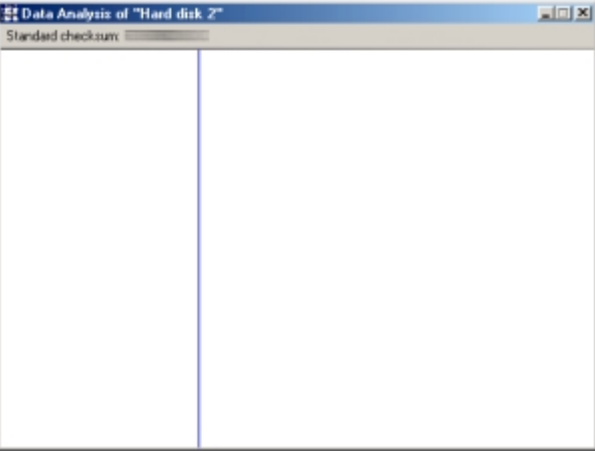
8. A small window will display the progress and an ETA. You may abort at any time by pressing the ESC key or by closing that window.
9. When complete, you may close the edit window and exit WinHex, or repeat the steps 6 and 7 for sanitization (more than one clearing procedure).

3 How to Verify using WinHex

WinHex will warn you during clearing if sectors could not be overwritten (e.g. because of physical damage). If no error messages are displayed, you may assume that clearing was successful. If you wish to further verify that, however, proceed as follows. Note that none of the following verification methods is 100% safe, though.

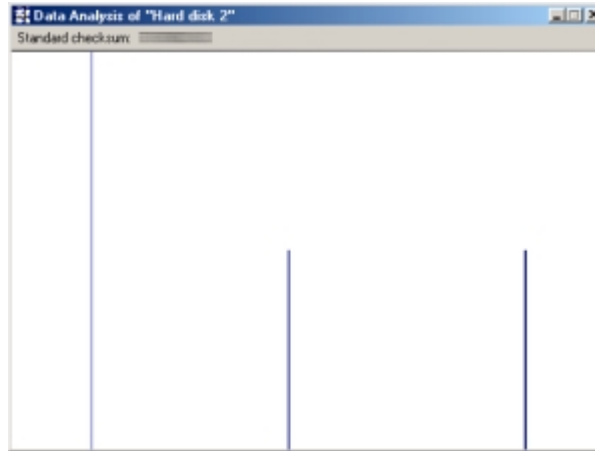
1. When done, close the edit window and open the media again (steps 4 and 5). You will see the chosen byte value pattern (certain hex values or random hex values) throughout the disk. Try scrolling around, press the END key of your keyboard to see the end of the disk, and HOME to return.

2. You may analyze entire media or selected parts thereof using Tools | Analyze Disk or Tools | Analyze Block, respectively.

Type of (last) clearing	Verification by data analysis
Random byte values	<p>Byte values must be almost equally distributed in the selected range. (0 to 255 in this figure.)</p> 
Fixed hex value 0x00	<p>Standard checksum must be 00000000.</p>  <p><i>This criterion is 0.99999998% safe, meaning that there is just a very slight chance that other data than just zero bytes will accumulate to a 32-bit standard checksum of zero.</i></p>
Other fixed hex value	<p>A single vertical bar must be visible only.</p>  <p><i>The vertical bar in this figure represents a hex value of 55 used for overwriting. Verify by moving the mouse cursor over the bar and watching the gray status line.</i></p>

More than one fixed hex value

The same number of vertical bars as hex values specified must be visible.



The figure shows the bars for the hex values 2277DD22. 22 is twice as frequent as 77 and DD, so the corresponding bar is twice as high.

3. You may also try finding known data that formerly existed on the drive, or common text strings (such as “information”, “Windows”, or the name of a person that worked on the media) using Search | Find Text. Short words such as “and” *might* occur accidentally if the disk was overwritten with random data. Aside from that, you shouldn’t find text any more, or else the clearing was incomplete.