Learn about the Write Zero method

Many file shredder and Data Destruction programs support Data Sanitization method based on Write Zero software to overwrite existing data on storage devices such as hard drives.

Many file shredder and Data Destruction programs support Data Sanitization method based on Write Zero software to overwrite existing data on storage devices such as hard drives.

The Data Sanitization Write Zero method may not prevent the most advanced hardware-based recovery methods, extract at least some of the deleted data, but potentially prevent all file recovery methods. based on software that pulls information from the drive.

Note : The Write Zero method is sometimes, and more precisely, called the Single Overwrite method. It can also be called Zero Fill Erase or Zero-fill.

What does Write Zero do?

Some Data Sanitization methods, such as Gutmann and DoD 5220.22-M, will write random characters to existing information on the drive. However, the Data Sanitization Write Zero method (which is not surprising) is usually done in the following way:

1st time: Overwrite with 0

Some implementations of the Write Zero method may include verification after the first time, writing a non-zero character or writing zeros many times, but these are not common practices.

Tip : Most software programs that support Write Zero provide a way for you to customize the character and number of verifications that take place. However, changing these to some extent means you don't really use

Write Zero anymore.

Is Write Zero enough to erase data?

Most likely yes. However, some Data Sanitization methods replace your usual, easy-to-read data with random characters. As mentioned above, Write Zero does the same thing but uses zeros. In a practical sense, if you wipe a hard drive with zero and then throw it away, no matter who holds it it will then also be unable to recover any deleted data.

If that's true, you might be wondering, why other types of data deletion methods still exist. With all available data deletion methods, what is the purpose of the Zero-fill utility? For example, the Random Data method writes random characters to a drive instead of zero, so how is it different from Write Zero or any other method?

On the one hand, it is important not only what characters are written, but also how the method is applied effectively to overwrite data. If only one write is made and the software does not verify that all data has been deleted, the method will not be as effective as what other methods do.

In other words, if you use Write Zero on a drive and verify that all data has been overwritten, then you can be confident that information is less likely to be recovered, compared to the same data. Data is overwritten by the Random Data method, but does not verify that each sector has been replaced with random characters.

However, some characters may also provide better privacy than others. If a file recovery program knows that data is only overwritten with zeros, then screening existing data is significantly easier than the program doesn't know the characters used, as in Schneier method.

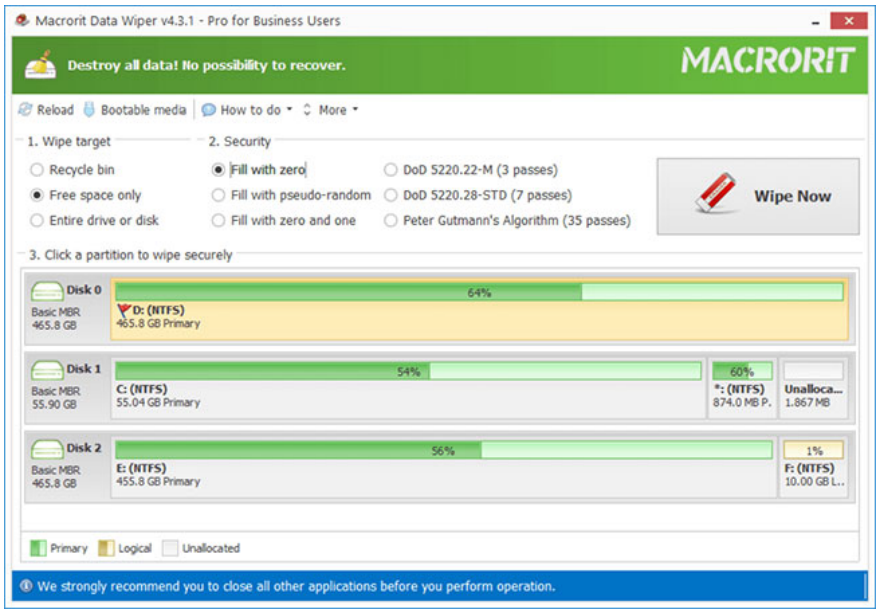
Another reason for all other data deletion methods to persist is that some organizations want to prove that their information is being deleted in a specific way, potentially preventing the recovery, because So they use a certain Data Sanitization method for all their data deletion needs.

The program supports Write Zero

In Windows 10, Windows 8, Windows 7 and Windows Vista, the **format** command is reliable, by default, using the Write Zero method during formatting. You can use that command in the command prompt to write the number 0 to your hard drive without having to download any special software or tools.

See the article: How to use the format command to write 0 to the hard drive for details on how to do this. This is not quite as simple as the name suggests, when you are trying to do this on your main system drive.

There are also third-party programs that support the use of the Write Zero method to erase data, such as DBAN, HDShredder, KillDisk and Macrorit Disk Partition Wiper. Some of these programs can be used to erase the hard drive you're using (like drive C) by running from a disk or flash drive, and programs running in the operating system to delete other drives, like removable drives. dynamic.



Other tools use the Write Zero method to delete specific files instead of everything as the above programs do. A few examples of such tools include WipeFile and BitKiller.

Most data destruction programs support a variety of Data Sanitization methods, in addition to Write Zero, so chances are you'll be able to choose another method (if you're interested), when opening a program.

You finished reading the article "**Learn about the Write Zero method**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.