OW Shredder

1) About OW Shredder

1.1 What is OW Shredder?

OW Shredder is an advanced security tool which allows you to completely erase secret data with all drive traces from your hard drives by overwriting it. Individual files, free disk space and entire volumes can by erased. In addition OW Shredder offers various tools to scan, analyze and wipe more drive information and traces. Beside of it OW Shredder supports a desktop widget, a context menu integration and automated recycle bin cleaning. All in all this small and portable application gives private users or even companies the perfect solution to eliminate sensitive data.

1.2 Limitation of OW Shredder

The amount of the files which can be erased are depending on the size of the free random access memory. An intelligent feature of OW Shredder only saves the required data in memory and skips not needed information like files of a folder.

Beside of the system requirements OW Shredder can erase files with up to 8.589.934.591 Gigabyte (9.223.372.036.854.775.807 Bytes).

1.3 Privacy leaks

1.3.1 Page file

Windows creates a page file for virtual memory storage, which is used for storing information from the memory to the disk, which means there is a chance that it contains private data. Erasing the page file is a normally blocked action which usually ends in freezing the system and sometimes blocks the allocated space by other applications.

1.3.2 Dead sectors

When a specific area on the drive gets damaged for some reason it gets technically marked and cannot be accessed anymore even it still contains private data.

1.4 Acknowledgements

In first place we want to thank Shawn Michael Wiebe for the continuous support and help in erasing MFT traces.

We want to thanks AeonHack, Earn and Xertz for the controls design base which gives us the possibility to create a simple yet effective user interface.

The nice icons are made free from Icon8.com.

OW Shredder also uses the awesome Enigma Virtual Box to pack all application files to offer a portable executable on all supported systems.

2) Quick start

2.1 GUI

2.1.1 Control

This tab page gives access to the main functions of OW Shredder. Erasing files, folder, full drives and free drive space including old traces. With the use of a file/folder dialog or a simple drag and drop you can erase all wanted.

2.1.2 Tools

The tools give access to quite interesting drive information like a cluster preview or hardware information about the drives. Beside of it OW Shredder also has a system restore tool and an auto start manager.

2.1.3 Settings

OW Shredders settings allow you to customize the theme of OW Shredder and enable quite handy functions like a desktop widget or a context menu integration.

2.2 Command usage

Unlock file: <OW Shredder path> -U <File path>

Example: D:\OW Shredder.exe –U D:\DeleteMe\Test.txt

Erase File/ Folder

With dialogue: <OW Shredder path> <File/ folder path>

Example: D:\OW Shredder.exe D:\Test.txt

Without dialogue: <OW Shredder path> -Hidden <File/ folder path>

Example: D:\OW Shredder.exe -Hidden D:\Test.txt

Skip admin privileges dialogue: <OW Shredder path> -SkipUAC

Example: D:\OW Shredder.exe -SkipUAC

2.3 Security of the erase algorithms

Quite many people asked why OW Shredder does not offer erase algorithm like Gutmann with 35 passes. The chance of restoring a single byte is 56% when you know the exact location. This means that the chance of restoring a byte overwritten one time is ~0.967%. With only one pass more the chance is ~0.009354%.

This is why OW Shredder does not only offer secure erase algorithms, we also offer the erasure of the drive traces, which destroys all traces and file system entries of the files. The combination of overwriting and erasing the traces results in the maximum security any security software solution can offer. To prevent the use of small restored fragments we always suggest full drive encryption.

But still the only way to reach full security is destroying the drive physically.

Sources: Overwriting Hard Drive Data: The Great Wiping Controversy & Secure Deletion of Data from Magnetic and Solid-State Memory