ERASER
user guide

Table of Contents

Overview

Eraser is an advanced security tool which allows you to completely remove sensitive data from your disk drives by overwriting it several times with carefully selected patterns. You can drag and drop files and folders to the program, setting arbitrarily complex schedules and any number of targets, or use the convenient Windows Explorer shell extension.

All the patterns used for overwriting are based on published standards by either researchers or government agencies and they are selected to effectively remove the magnetic remnants from the hard disk making it impossible to recover the data. These methods include

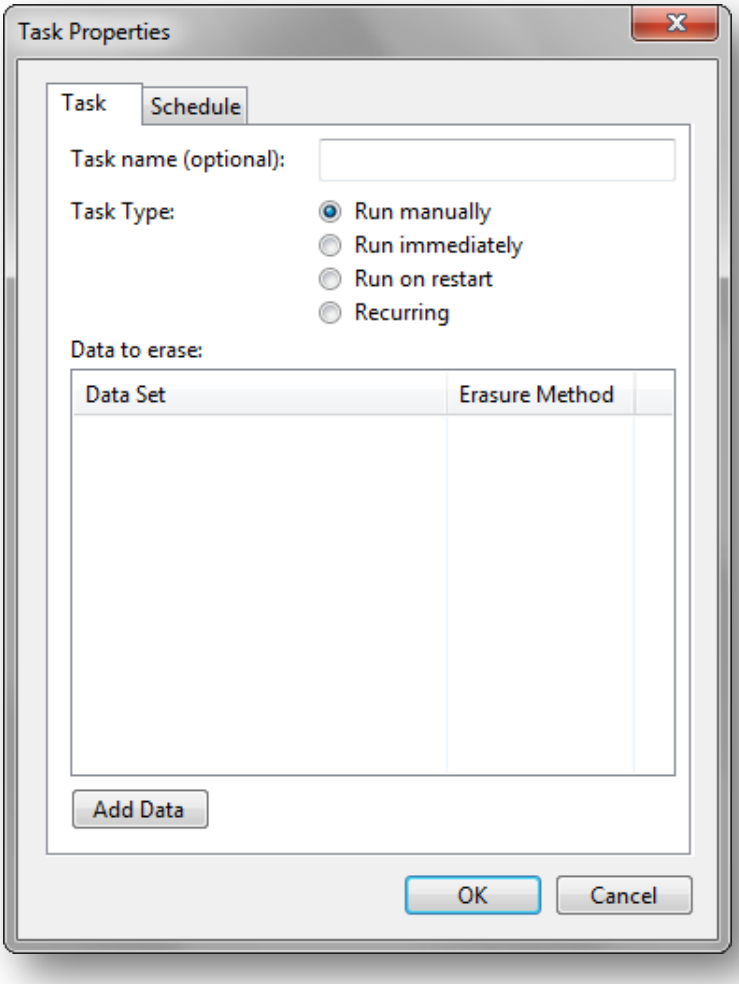
- Peter Gutmann's paper **Secure Deletion of Data from Magnetic and Solid-State Memory**
- National Industrial Security Program Operating Manual of the US Department of Defense
- Simple pseudorandom data

Using Eraser

Eraser, although being designed as an advanced security tool, has a user-friendly interface for users to design, schedule and execute tasks. The interface is therefore an integral part of the user's workflow and in this chapter we demonstrate the common tasks users expect of such a program.

Creating Tasks

The fundamental unit of operation in Eraser 6 is the Task. The task represents one unit of work that will be executed. A task has a schedule as well as a set of TARGETS: the schedule defines the time and date that a task will run and the targets define what data needs to be erased. Tasks can be defined by selecting the *Erase Schedule* drop-down menu, then selecting **New Task** (or press Ctrl+N). You will then be presented with the Task Properties Dialog.



The **Task** tab allows you to define the the Task Name, Task Type as well as the data to erase (erasure targets).

The Task Name is a user-defined text which is displayed to you in the scheduler as well as in task notifications. It is otherwise not used by the program at all – it only serves as a reference point for you as a user to know which task the program is referring to. If this is left blank, a program-generated name from the list of erasure targets is used.

The Task Type defines when and how the task will be run:

- If the task is set to Run Manually, then the task is run only when you explicitly request a task to run.
- If the task is set to **Run Immediately**, after the Task Dialog is closed, the task will run (after all running tasks complete.) Tasks set to Run Immediately will be deleted if AUTOMATICALLY REMOVE TASKS WHICH RUN IMMEDIATELY AND COMPLETED SUCCESSFULLY is checked in the **Eraser Settings** page. Tasks set to Run Immediately will be reset to Run Manually upon completion of the task; if the task was aborted in the process of execution (e.g. by an application crash) the task will automatically be run again upon program restart.

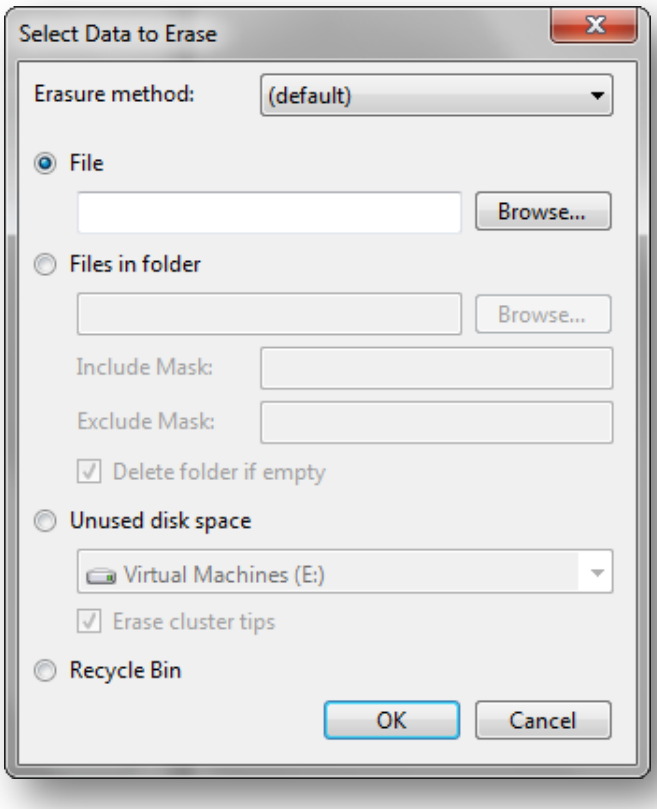
- If the task is set to **Run at Restart**, the task will be run when the computer is next restarted. This is useful for erasing files which are currently in use. Tasks set to Run at Restart will be reset to Run Manually upon completion of the task.

> ***Be careful with the Run at Restart option. Eraser does not currently check to ensure that the file being erased is the same file that erasure was requested. This means that if a file was renamed after the task was created, and a new file created in place, the new file would be erased when the system restarts and this will occur without user confirmation!***

- If the task is set to **Recurring**, go to the **Schedule** to define the frequency of which the task will execute

Erasure targets can be added by clicking on **Add Data**; editing defined targets is accomplished by double-clicking on a task; deleting targets is accomplished by right-clicking on an erasure target, and selecting **Remove from List**.

Selecting Data to Erase



Targets define the files and folders which require erasure. The Select Data to Erase dialog allows you to specify which files or folders require erasure, and which erasure method to apply to destroy those files.

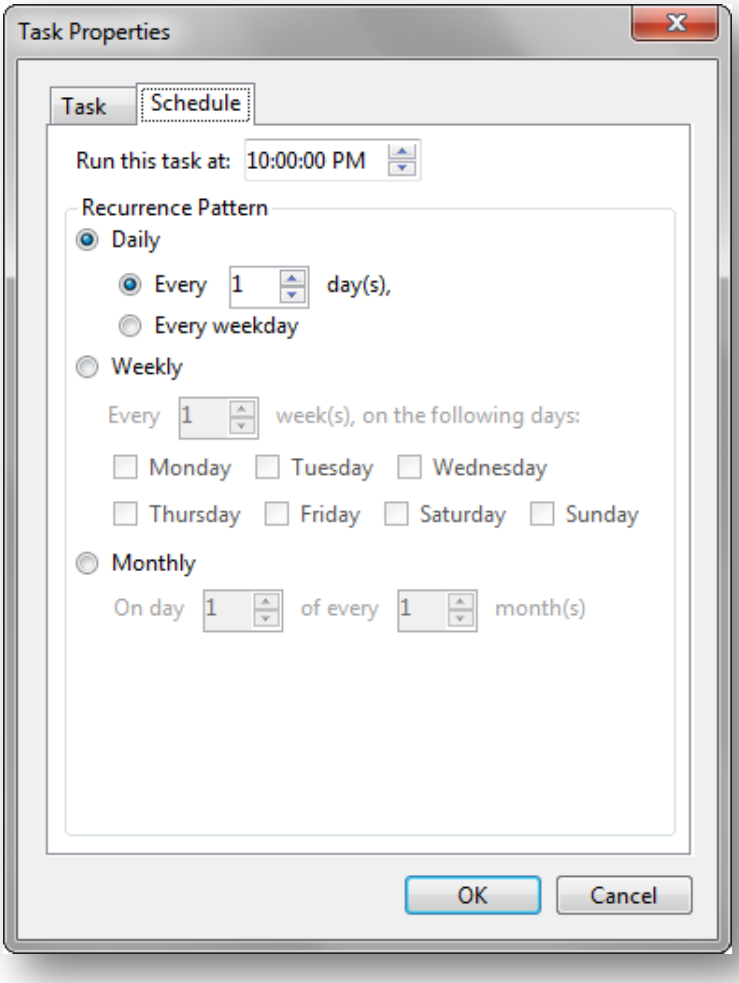
The Erasure method applied defaults to the global default – that is, the erasure method applied will follow the default method specified in the SETTINGS dialog (see the Settings documentation for more information.) You can override the defaults by specifying a different erasure method here. Even when the global defaults change, this setting will be left unmodified; however if this is left to **(default)**, the erasure method will change as the global defaults change.

There are currently four kinds of erasure targets:

- **File** targets specify that file to be erased.

- **Files in Folder** specifies a folder for erasure, and the include mask specifies a WILDCARD EXPRESSION to include files for erasure, and the exclude mask specifies another Wildcard expression to exclude files for erasure.
    - The include mask is applied before the exclude mask; a blank include mask includes all files and a blank exclude mask includes all files.
    - Combinations of the two are supported.
- **Unused disk space** specifies that all unallocated disk space on the selected volume will be overwritten with random data to eliminate the traces of files which were insecurely deleted.
    - Checking the **Erase cluster tips** checkbox will erase the CLUSTER TIPS of files on the specified drive. Symbolic links, hard links and Junctions will not be followed.
    - Starting from Eraser 6.1, mounted network drives (with a drive letter) are also displayed in the drop-down list, allowing the unused space erasure of network drives.

For the unused space erasure of network drives to work properly, knowledge of the NAS is required: only the partition which the drive is mounted on will be erased. Furthermore, if quotas are enforced, Eraser may not be aware of it and the unused space erasure may not work as expected, even if Eraser completes the task successfully.



- **Recycle bin** specifies that all files in the *current user's* recycle bin is erased.

Creating Recurring Tasks

Recurring tasks will run on a schedule – they have a predetermined time for running and will run at regular intervals. To create recurring tasks, select **Recurring** under **Task Type** in the Task Properties dialog. Then, select the **Schedule** tab.

The first thing to specify is the time the task will run: this must be set, and defaults to the current time of the day. There are currently three kinds of schedules:

- Daily schedules run every X days or every weekday.

- Weekly schedules will run every X weeks from the last run, on the selected days of the week.
- Monthly schedules will run on the X'th day of the month, on every Y months. If the X'th day does not exist on the current month, the month will be skipped.

Scheduled tasks which are missed (for example, because the computer was shut down, or if Eraser was not running) have two methods for returning to the schedule. This will be discussed in SCHEDULER SETTINGS

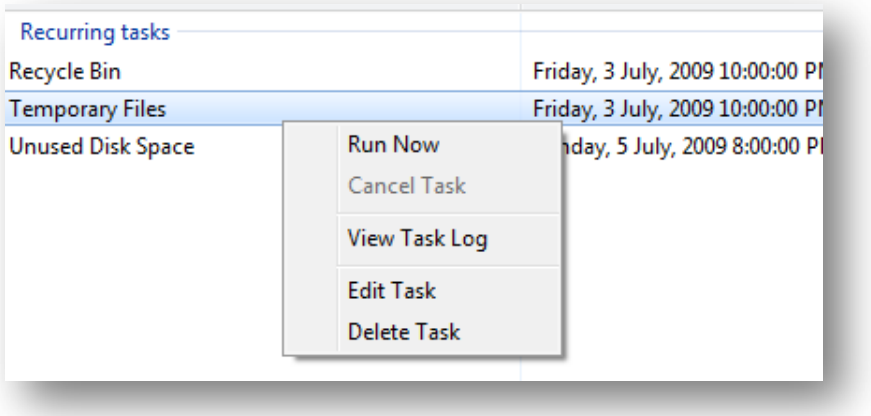
Importing/Exporting Tasks

Task lists can be exported and imported from Eraser. This is accomplished by going to **Erase Schedule** | **Export/Import Task List**. Below is a matrix containing the list of compatible task list versions.

Reading\Writing	5.x	6.0.x	6.1.x/6.2.x
5.x	Yes	No	No
6.0.x	No	Yes	No
6.1.x/6.2.x	No	No	Yes

Running Tasks

Tasks can be run on-demand by selecting the relevant tasks in the **Erase Schedule**, right-clicking on them and selecting **Run Now**.



> ***Hint: click and drag to select, or select one and press shift to select multiple tasks in a sequence, or select and press control while selecting other tasks to cherry-pick.)***

It is also through the context menu that you can cancel running tasks, view the task log, edit the task as well as delete the task. Tasks can also be edited by double-clicking on the task in the schedule.

Behaviour toward encrypted, sparse or compressed files

IF you are using Windows 2000 or later, as well as having an NTFS file system, you have the option of encrypting and/or compressing your files. Also, programs are able to set files as "sparse", which

means that long stretches of data which are absent will occupy zero disk space. Because encrypted files, compressed files and sparse behave differently when applying the standard erasure procedure, Eraser will not erase such files when they are encountered and will instead log an error.

Behaviour toward reparse points

Symbolic links, NTFS junctions are special kinds of files where they reference another file, folder or drive.

Symbolic links are basically Windows shortcuts – but unlike Windows shortcuts they work without any application support. The difference is mainly to programmers as typical Shortcuts appear as files containing garbage data when opened with a program not designed to handle shortcuts; whereas symbolic links always appear as the file it points to regardless of the program. Symbolic links can reference files and folders, as well as files and folders from outside the current drive.

Directory junctions are like symbolic links for folders.

Collectively, these are known as reparse points. Eraser treats reparse points specially to avoid data loss.

Firstly, when erasing the free space of a drive, when Eraser meets a reparse point file cluster tips are not erased as the file which the reparse point refers to may be on a slow link (e.g. network connection) and cluster tip semantics may differ from local erasures successfully. This also prevents network saturation (for network files). Reparse points referring to folders are completely ignored as the folder can be accessed by another path and it may not be the intent of the user to erase that folder as well.

Next, when erasing folders, files and subfolders which are reparse points are ignored so as to prevent data loss. To erase such files, specifically tell Eraser to erase the file the reparse point refers to.

NTFS hard links are treated differently. Hard links are like symbolic links, except that they can only reference files on the same drive as the drive containing the hard link and that hard links work differently. They basically allow two file names to share the same data, thus they are indistinguishable from normal files. Hard links are transparent to Eraser and they will be erased; however, since hard links point to data which is referred to by more than one file, the other references will now point to invalid (erased) data. There is currently no workaround for this – you will need to erase the other hard links in the normal way before all references to the garbage data are removed.

Behaviour toward Saved HTML files

Eraser handles files differently from Windows. One such difference is regarding the use of HTML files: When saving a web page from a browser, the file is saved and a folder (containing the file name appended with **_files**, hereafter termed the *associated folder*) is created to store the linked files. If you wish to simply delete a downloaded webpage and its associated folder on your hard drive you will just delete the saved file. Windows will then move the HTML file and its associated folder to the Recycle Bin. After you are certain that you no longer require the HTML file and folder you can right click the Recycle Bin and select **Empty Recycle Bin**. Windows will then mark the file and folder as free space and remove it from the recycle bin.

Obviously, the file and folder are still actually on your hard drive within the free space, but they are inaccessible to the user without specialist recovery software. You may want to employ Eraser and its privacy capabilities to permanently and immediately erase your downloaded HTML files and folders.

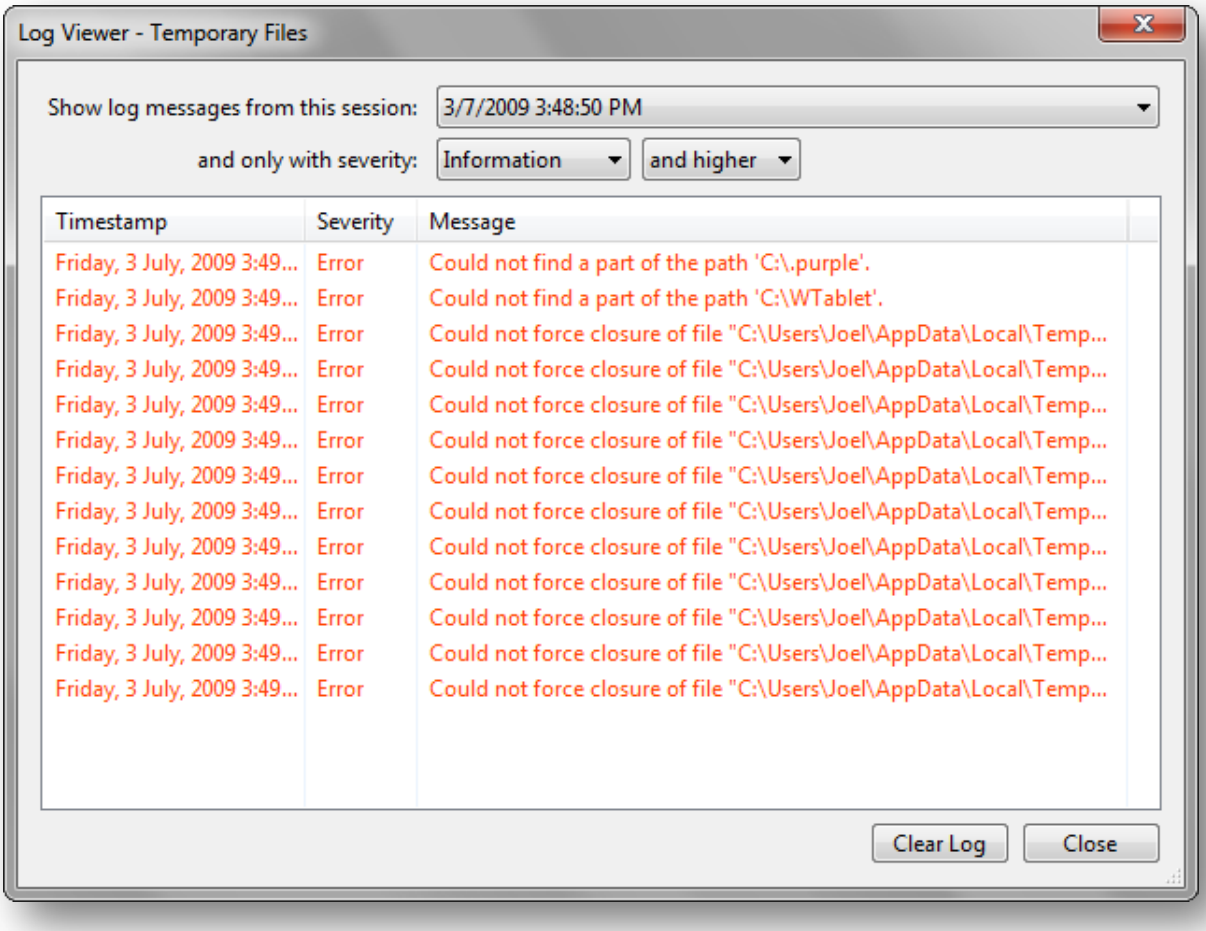
However, because the erasure process is irreversible, when the main file is selected, only the file is erased, the associated folder is left alone. Although this removes some of the convenience to the user as they now have to manually select both the HTML file and associated folder before instructing Eraser to erase them, it is safer as it removes the risk of accidental erasure.

If you happen to have many downloaded web pages on your hard drive, selecting both the HTML file and associated folder would be time consuming and tedious. You may wish to be able to quickly sort which files and folders you want to delete with the expediency of Windows' ability to associate HTML files and folders but also require the security Eraser provides. There is fortunately a workaround for this: use the Windows delete option as described above, but stop before emptying the Recycle Bin. This will send both the HTML file and its associated folder to your Recycle Bin for review.

You now have all the HTML files and folders you selected within the Recycle Bin. This gives you the option to wait or double check you have not deleted something you would rather not have done. When you are absolutely certain you have not removed a folder with data you require in it you can proceed to SECURELY ERASE THE RECYCLE BIN'S CONTENTS.

Viewing the Results of an Erasure

After an erase is complete, the task scheduler will display the result in the Status column. If it displays **Completed with Errors**, the erase was unsuccessful and you should determine the cause so as to ensure no privacy leaks occur. Once again, you will right-click on the affected task and select **View Task Log**. This will bring up the Log Viewer which displays tasks from a given erase session.



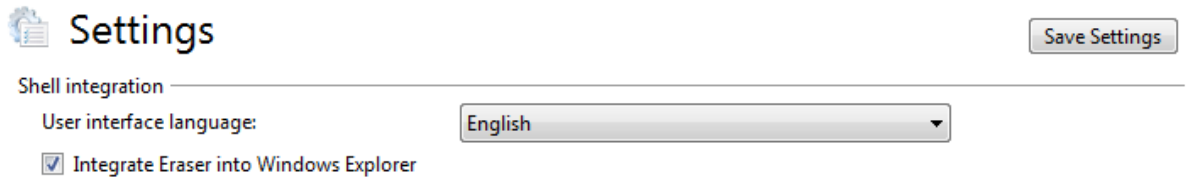
You can select the log messages from which session (if you see errors, you should select the latest session), and you can filter down the log messages to only those of desired severity. This is helpful when running an Unused Space erasure with cluster tip erasure enabled as there will be many informational messages stating that access is denied to a particular file or that the file is a protected system file and thus left untouched.

Eraser Settings

Eraser is a customisable program which allows you to change settings that fit your threat model. Nonetheless, the default settings that come with Eraser out-of-the-box are relatively safe for the majority of users.

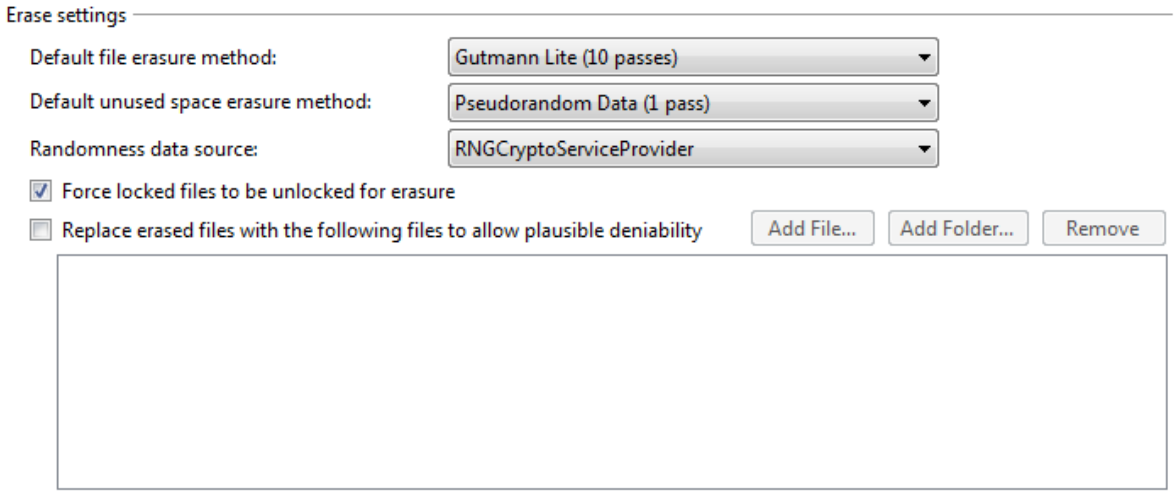
Note that for settings to take effect, you need to select the Save Settings button at the top-right of the settings page. Some settings also require a restart to take effect.

Shell Integration



- **User interface language** specifies the translation of Eraser you wish to use.
- When **Integrate Eraser into Windows Explorer** is checked, the Eraser context menu will appear when right-clicking supported items in Windows Explorer.

Erase Settings

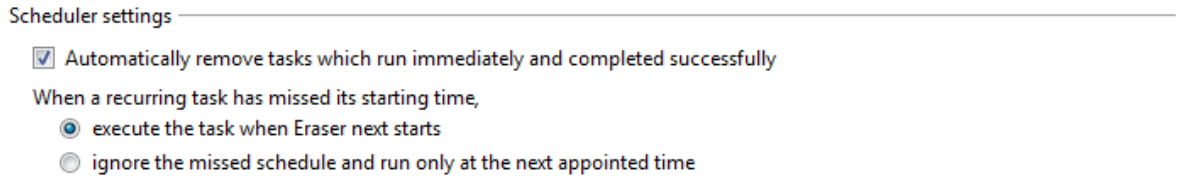


The Erase settings group allows you to specify the behaviour of Eraser when erasing files.

- The **Default file erasure method** and **Default unused space erasure method** will be used when task targets specify **(default)** as their erasure method.
- The **Randomness data source** specifies where to get random data from for use in random data passes during erasure.
- When **Force locked files to be unlocked for erasure** is checked, when Eraser tries to erase a file but it is locked by a program, Eraser will attempt to forcibly unlock the file for erasure; if this is unchecked, the file will be ignored by Eraser and reported as an error.
- **Replace erased files with the following files to allow plausible deniability** specifies a list of files to use to replace the erased files' space on the drive after deleting to give the

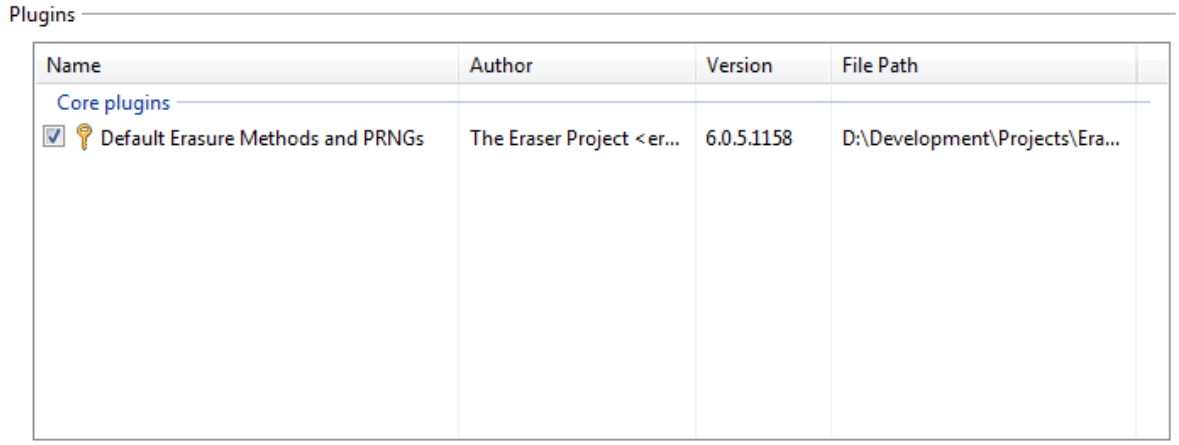
impression that no files were erased, except other files which were deleted before (hence plausible deniability.)

Scheduler Settings



- When **Automatically remove tasks which run immediately and completed successfully** is checked, tasks scheduled to run immediately and completed without errors are automatically removed from the Erase Schedule.
- The next two radio buttons specify the behaviour when the run-time of recurring tasks are missed:
    - **Execute the task when Eraser next starts** will cause the task to run the next time Eraser starts.
    - **Ignore the missed schedule and run only at the next appointed time** will cause the task to be rescheduled as if the task ran as expected.

Plugins



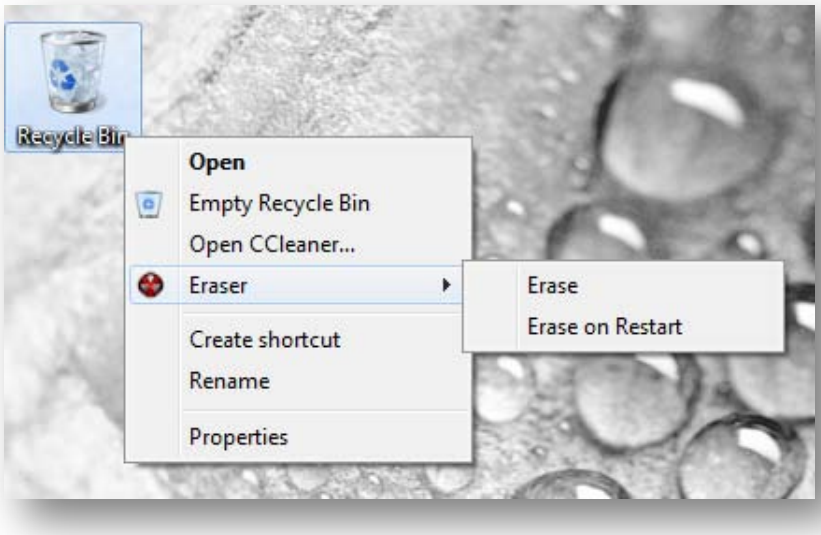
The Plugins section contains a list of plugins which are loaded into Eraser.

- **Core plugins** are plugins which *cannot* be disabled.
- A key beside the name of the plugin represents a **signed plugin.**
    - Signed plugins are automatically allowed to run after it is installed.
    - Unsigned plugins must be explicitly checked by the user.
- The checkbox beside the name represents whether the plugin will be loaded in future (unchecking disables the plugin.)
- Right-clicking on a plugin displays a context menu with Settings if the plugin can be configured.

Using the Windows Explorer Extension

If you have selected the Windows Explorer extension during setup, Eraser will install a context menu entry when right-clicking the following items:

- Files and/or folders
- Disk Drives in the Computer folder
- Recycle Bin



Hovering over the Eraser menu will show a submenu containing the items **Erase** and **Erase on Restart**. If you right-clicked a drive, you also have the option of **Erasing Free Space** from the context menu. If there are no files in the Recycle Bin, the Eraser context menu will be greyed out.

Selecting any of the Erase options will send a new Task to the running Eraser program (or it will be started if it is not running) and notifications will appear in the system notification area when tasks complete.

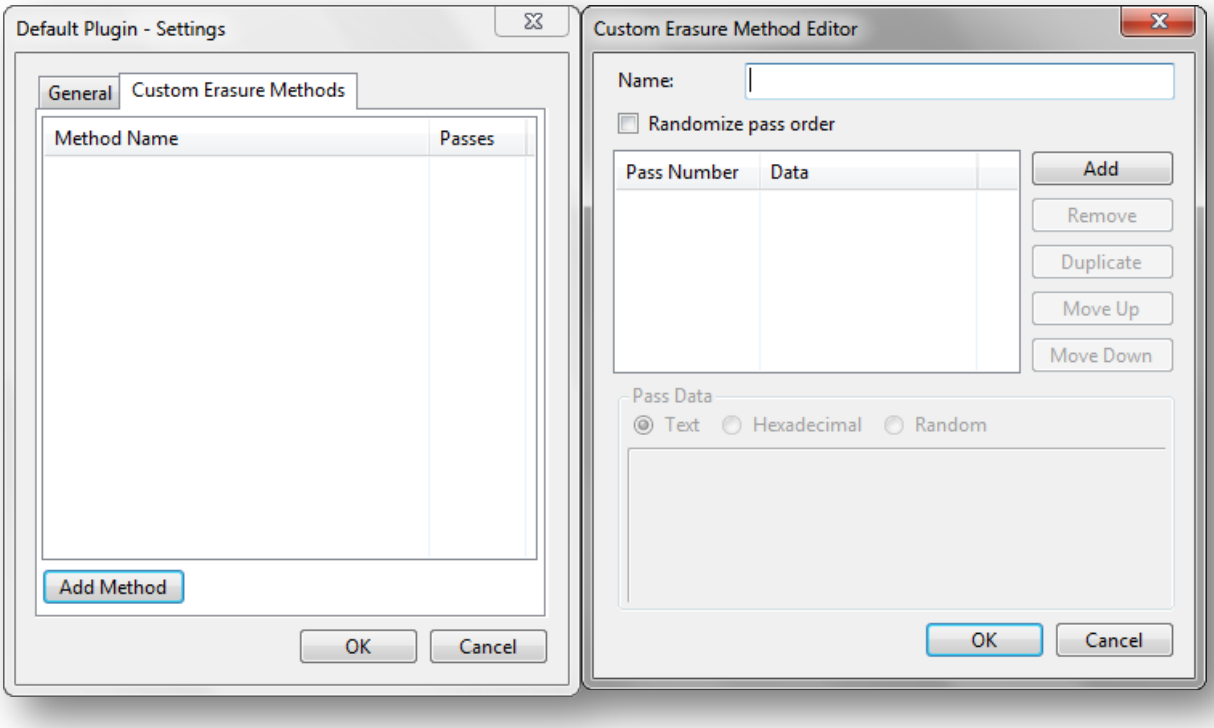
Advanced Topics

Using the Eraser Command Line

TBD.

Creating Custom Erasure Methods

Eraser comes with the ability for you to create your own erasure methods for file overwriting. This is accomplished by right-clicking the **Default Erasure Methods and PRNGs** plugin in the **Settings** page, then selecting **Custom Erasure Methods**. You will be presented with the Custom Erasure Method Editor.



Provide a Name for the erasure method, as that is how you will identify it in the list of methods, then add any arbitrary number of passes.

- **Randomize pass order** will cause the passes to be jumbled every time the erasure is run.
- **Add**, **Remove**, **Duplicate**, **Move Up**, **Move Down** will operate on the currently selected pass in the pass list
- **Pass Data** allows you to specify the data for the pass:
    - **Text/Hexadecimal** will be for your own data. Text will be treated as normal input (UTF-8) and hexadecimal will be used for raw data. The data will be repeated for all parts of the file/unused space until erasure is complete. The interconversion between Hexadecimal and Text may not be lossless (especially if the hexadecimal number translates to a non-Unicode codepoint)
    - **Random** will erase the file/unused space with random data

Eraser How To's

Erase Browser Caches

Surfing the internet leaves traces of your activity in the form of cookies, the history as well as a browser cache. These browser data files should be erased if privacy is a concern.

Mozilla Firefox

Mozilla stores the saved files to the folder "Cache", which you can find under the profile folder (%LOCALAPPDATA%\Mozilla\Firefox\Profiles\<profile name>\). You can safely erase that folder when Firefox is *not* running.

You will also need to erase the history file called places.sqlite, which can be found in the profile folder (%APPDATA%\Mozilla\Firefox\Profiles\<profile name>\). The cookie file may also reveal information so cookies.sqlite which is in the same place as the history file should be erased as well.

> ***Only erase these files when Firefox is closed, otherwise you may corrupt your Firefox session and/or other files in your drive.***

Windows Internet Explorer

TBD.

Erase the Recycle Bin

Option 1: Using the Windows Explorer Extension

1. Go to your desktop
2. Right-click on the **Recycle Bin**
3. Select **Eraser** | **Erase**

Option 2: Using the Eraser program

1. Go to the **Task Scheduler**
2. Select **New Task** (Ctrl+N)
3. Select **Add Data**
4. Select the **Recycle Bin** radio button
5. Click **OK** until you return to the Scheduler

Erase the Page File

Erasing the Page File needs to be done by Windows though a configuration setting. See the MICROSOFT KNOWLEDGE BASE for instructions.

Encrypt the Page File

1. Start a Command Prompt, elevating it in Vista or later
2. Key in "fsutil behavior set EncryptPagingFile 1"
3. Restart your computer

When do I need to use Eraser?

You should use overwriting every time when removing data from your drive. You do not need to overwrite data which you think is neither secret nor sensitive, but there is no harm in overwriting everything[1].

However, there are some cases where overwriting may not be suitable or may have side effects. These cases are discussed in the following section.

You may also want to erase the unused disk space on your drive regularly to get rid of the remains of temporary files created by applications and other information that may have been stored on your disk. You can use the Scheduler to run the task when the computer is not in use – overnight, for example.

Exceptions

1. Compressed Files/drives
   You cannot erase files compressed at the file system level (file compression requires a file system that supports it such as NTFS). Files compressed with an external application, such as ZIP files, can naturally be erased.
2. Encrypted Files
   You cannot erase files encrypted at the file system level (file ~~compression~~encryption requires a file system that supports it such as NTFS). Files encrypted with an external application, such as Pretty Good Privacy (PGP) or AxCrypt, can however be erased.
   As the data is already stored in unreadable format, erasing is not required, but usually increases security (prevents recovery if the key is compromised, for example)
3. Encrypted Drives
   You may wish to erase the free space of encrypted drives (such as that of TrueCrypt) for the same reasons as those in Encrypted Files. This will work however as the encryption is transparent to Eraser.
4. Network Drives
   Erasing files over the network may work; however it will more likely fail to securely erase your file as data is modified through the network protocol and the semantics required for erasure may not be present. Furthermore, you are very likely to saturate the network, which is very inconsiderate.
5. Floppy Disks
   You can erase data on a floppy disk as if you were erasing a hard disk. However, if you have stored sensitive data on a floppy disk, you may want to consider physically destroying the disk using another method, such as burning it.
6. CD-RW, DVD±RW, solid state drives etc
   These drives have a limited rewrite span and thus you may want to reserve the unused space erasures for emergencies. Also, a single pass is sufficient for eliminating all traces of files as they are not magnetic media. If your media is cheap (e.g. CD-RW) you may consider crushing the disc.

[1] Unless you are writing to media which have limited life span, for example USB keys, CD-RW, DVD±RW, solid state drives etc.

Unintentional Privacy leaks

Some of the most commonly overlooked security holes are discussed below.

1. Page File
   The virtual memory storage of the Windows operating system is called the page file. The operating system may store any information from the memory to the disk whenever it wants. This means that the page file may contain passwords, pieces of documents and other sensitive information.
   Since the operating system locks the paging file while it is running, the file cannot be accessed using standard file operations. There are applications that claim to overwrite the paging file by allocating huge amounts of memory, but this method may freeze your computer and even then the space allocated by applications cannot be accessed and not all the available space on the paging file is necessarily overwritten.
   For information on how to erase the paging file, see Erasing the Page File.
2. Filenames
   Unless you name your files with arbitrary names, the name of a file can reveal information about the file contents. Eraser will overwrite the filename after erasing the file data. Names of the files you have previously deleted may also still be stored in the file system table; Eraser will overwrite them when you erase unused disk space
3. Bad Sectors
   When an area on the disk gets damaged for some reason, the disk electronics mark the area as containing bad sectors. These bad sectors cannot be accessed so the data still stored in them cannot be erased either. Peter Gutmann has discussed this subject further in chapter Further Problems with Magnetic Media of his paper **Secure Deletion of Data from Magnetic and Solid-State Memory**.

More Help

After reading this document, should you have any questions, feel free to post your questions in the Eraser forum: http://bbs.heidi.ie/viewforum.php?f=30. Found a bug? Post a ticket in Trac: http://eraser.heidi.ie/trac/

This section contains the appendices to the documentation which may be of interest for advanced users.

Appendix A: Erasure Methods

Method Name	Number of Passes	Description
Pseudorandom data	1	The fastest wiping scheme. Your data is overwritten with random data[2] (if you use a the data is indistinguishable from random noise.)
British HMG IS5 (Baseline) (1 pass)	1	Your data is overwritten with zeroes.
Russian GOST P50739-95	2	GOST P50739-95 wiping scheme calls for a single pass of zeroes followed by a single pass of random data
British HMG IS5 (Enhanced)	3	British HMG IS5 (Enhanced) is a three pass overwriting algorithm: first pass – with zeroes, second pass – with ones and the last pass with random data.
US Army AR380-19	3	AR380-19 is data wiping scheme specified and published by the U.S. Army. AR380-19 is three pass overwriting algorithm: first pass – with random data, second with a random byte and the third pass with the complement of the 2nd pass
US Department of Defense DoD 5220.22-M (E)	3	DoD 5220.22-M (E) is a three pass overwriting algorithm: first pass – with zeroes, second pass – with ones and the last pass – with random data
US Air Force 5020	3	US Air Force 5020 is a three pass overwriting algorithm with the first pass being that of a random byte, followed by two passes of complement data (shifted 8 and 16 bits right respectively)
US Department of Defense DoD 5220.22-M(ECE)	7	DoD 5220.22-M(ECE) is seven pass overwriting algorithm: first, fourth and fifth pass with a random byte, its 8 right-bit shift complement and 16 right-bit shift complement; second and sixth passes with zeroes, and third and seventh pass with random data
Canadian RCMP TSSIT OPS-II	7	RCMP TSSIT OPS-II is a seven pass overwriting algorithm with three alternating patterns of zeroes and ones and the last pass - with a random byte
German VSITR	7	The German standard calls for data to be overwritten with three alternating patterns of zeroes and ones and in the last pass with random data
Schneier's Algorithm	7	The Bruce Schneier algorithm has seven passes: first pass – with ones, the second pass – with zeroes and then five times with random data

[2] Random Data vs. Random Byte: Random data is continually generated, a random byte is a randomly generated number, and that number is repeated throughout the pass.

Appendix B: Glossary

Cluster

The cluster is the fundamental unit of storage in a file system. It is a collection of sectors on a physical disk.

Cluster Tip

Since the cluster is the fundamental unit of storage in a file system, files which are not sized in a multiple of the cluster size will not fully utilise the clusters allocated to the file. For example, a common cluster size of 4096 bytes. Files using 3000 bytes and 5000 bytes have (4096-3000) = 1096 bytes and (8192-5000) = 3192 bytes of storage allocated to it but left unused. This is the cluster tip.

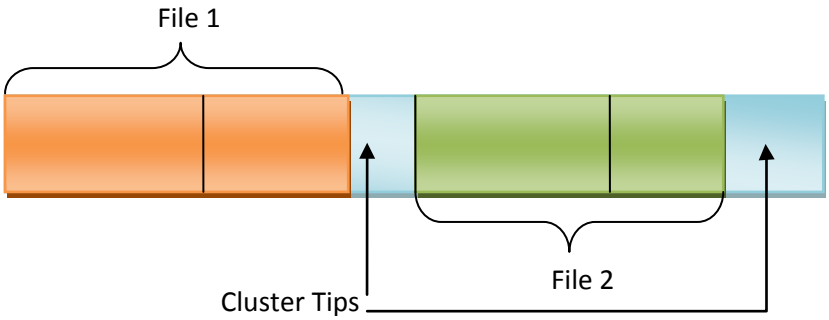


Figure 1: Disk Layout

The cluster tip holds garbage information (previously-present information) from your system memory and may contain sensitive information. Erasing a drive with an Unused Space erase with Cluster Tip erasure enabled will erase these cluster tips.

CSPRNG

This is an acronym for Cryptographically Secure Pseudorandom Number Generator. This is a designation for algorithms which generate random data with patterns indistinguishable from random noise. It is cryptographically secure as it generates “randomness” sufficient for use in salts and key derivation algorithms. It is “Pseudorandom” because the data is generated by a sequence of arithmetic operations.

Erasure Task

The task is the fundamental unit of work that Eraser will complete. A task has associated targets, a schedule, as well as a log to hold errors, warnings and notices encountered during execution.

Erasure Target

The target of an erasure is the set of files or folders which will be erased when the task containing the target is run.

Wildcard expression

A wildcard expression is a specially formed expression which is used to match text. Normal characters appear as-is in a wildcard expression, so these are valid wildcard expressions:

- File
- File2.txt

However, they are not really useful as only files matching those names are selected. Therefore, wildcards include the use of two operators, the question mark (?) and the asterisk (*). The question

mark means that any character may substitute its place; the asterisk means that any number of characters may substitute its place. Below are examples of wildcard expressions and the file names they match/do not match: underlined letters indicate a match, a words with a strikethrough are mismatches.

Expressions	File names matched	File names unmatched
*	All	
Er?se	Erase	~~Erroneous~~ Erase
Er*se	Eraser Erase	
Erase	Any file name will be Erased	

Remember that when using wildcards, most of the time they are applied to file names and file names include the file extension.

Appendix C: Migrating from Eraser 5

Eraser 6 has a huge change in the user experience, favouring a single erasure happening at any one time and using an asynchronous model of erasure execution for a few reasons:

1. Having only one erasure running at a time reduces the amount of time required for multiple erasures to complete. The rate-limiting component in an erasure in modern hard drives is the seek time – writes and reads can complete in the order of the nanoseconds, but seeks require approximately 5 milliseconds (in the ideal case scenario, as of mid-2009)
2. Eraser did not allow users to execute an unused disk space erasure from within the Windows Explorer context menu (in Windows Vista and later with User Account Control enabled)
3. Having all erasures completed in one place allows for easy management of all erasure tasks.
4. Having tasks run asynchronously allows users to do other things when running an erasure. Currently, when an erasure is being run, Windows Explorer cannot be used when erasures are initiated from the context menu and when an erasure is run from the Eraser program, Eraser itself cannot be used.

Migrating to Eraser 6

It is also important to note that all Eraser 5 tasks will not be automatically migrated to Eraser 6 tasks due to the very different nature of erasure tasks. Therefore, when upgrading from Eraser 5, the suggested migration plan is thus:

1. Install Eraser 6
2. Run Eraser 5, manually creating the new tasks in Eraser 6's scheduler
    - On-Demand tasks will be created with a **Run Immediately** schedule
    - Scheduled tasks will be created with a **Recurring** schedule
3. Migrate your custom erasure methods from Eraser 5 to Eraser 6

Terminology Changes

Eraser 6 uses some terminology differently than it was used in Eraser 5. The most notable change will be the use of a "Task". A Task in Eraser 5 only allowed for one schedule and one file, folder or unused space of a drive to erase. In Eraser 6, the objects to erase on a drive are now known as a Target and a single Task can have multiple targets. This allows for easier scheduling of a task, so one schedule can result in multiple targets being erased.

Appendix D: Removing Eraser's Traces

In the event that you wish to remove all traces of Eraser having been installed on the computer, perform the steps below to ensure a more thorough clean up. This assumes that you already have uninstalled Eraser.

1. Delete all registry entries under HKCU\Software\Eraser 6
2. Delete all files under %LOCALAPPDATA%\Eraser 6
3. Repeat steps 1 and 2 for every user on your computer

Of course, simple deletion may not be up to your threat model. If a more thorough clean up is required, do consider erasing your entire drive.