east-tec Eraser 2013
User Manual

Table of Contents

1 Introduction

1.1 The Need for Secure Data Destruction

1.1.1 "Delete" does not mean "Erase"

"Delete" does not mean "Erase"

Today more and more people have sensitive information that they would like to protect from falling into the wrong hands. If your hard disk contains valuable corporate trade secrets, business plans, personal files or confidential letters, you must know that the delete function does not erase, wipe or overwrite the information beyond recovery.

When you delete a file, the operating system does not destroy the file contents from the disk - it only deletes some "references" on the file from some system tables. The file contents remains on disk until another file happens to overwrite it. Any software recovery tool can restore the data if it hasn't been overwritten or thoroughly erased. Hardware recovery tools may even restore overwritten files by analyzing latent magnetic traces.

As a result, your confidential information may be lying unprotected on your disk (not wiped, overwritten or erased) and it is almost impossible to prevent it from falling into the wrong hands.

Sensitive files on your PC

You have just decided to move some sensitive files (business plans, password files, financial reports, etc.) from your hard disk to your floppy disk to make sure you are the only one that can access them. Moving the files to the floppy disk means copying them and then deleting them from the hard disk. But normal deletion is not secure - it does not really erase, overwrite and wipe the information beyond recovery. The result is that the contents of your sensitive files will remain exactly where you didn't want them: on the hard disk!

Looking for email privacy?

You have just accessed your mail account from your office. You've got some private messages that you decide to take home on a floppy disk. After copying the messages on the floppy disk, you delete the messages from the computer hard disk, as other people have access to your office computer and you don't want them to see your mail.

Bad news! The mail programs don't erase information to make sure the messages you delete are really gone. They simply ask Windows to perform the deletion. And Windows leaves the contents of deleted files on disk! This data must be securely wiped, overwritten and erased. Someone will eventually run a recovery tool on your office computer and find your deleted mail messages.

Dangerous Web surfing

You have just visited some compromising Web sites. You are aware of the fact that your Web browser has stored text and images from those sites in a special folder for quick viewing later (Internet Explorer's Temporary Internet Files or Netscape Navigator's cache). To hide your tracks, you use the Web browser's option to delete any temporary Internet files (or the cache) stored on your computer.

Do you think you got rid of those compromising files? Think again! They are still on disk! Disk tools like Norton Utilities can easily recover those deleted files! You'd better start thinking: How am I going to explain to my boss (or worse: my wife) why I visited those sites? It is of the utmost importance to thoroughly wipe, overwrite and erase data to ensure secure deletion.

1.1.2 Disk areas filled with sensitive information

- **The unused (free) disk space.** When a file is deleted, the area (or the space) previously used by the file is marked as unused (free) and it becomes available for other files. However, the area is not cleared so the content of the deleted file continues to be stored there until the operating system allocates the area for another file. That's why the unused (free) disk space is a warehouse of sensitive information and previously 'deleted' data.

- **The Windows swap file.** The Windows Swap file is the system file used for virtual memory support. The size of this file changes dynamically, and it can temporarily store the parts of files or other information.

- **The Windows Recycle Bin.** When you delete files Windows usually moves them to the Recycle Bin instead of removing them from disk. These files can be retrieved using recovery methods.

- **Configuration and data files and the Windows registry.** Windows and a lot of programs (such as your Web browser – Internet Explorer or Netscape Navigator) store a lot of sensitive information in configuration and data files on your hard disk or in the Windows registry. Most of the information is stored without your knowledge or approval.

- **The slack portion of files.** The file slack is usually filled with random information that comes from your computer. The information can be a listing of a directory, a part of a password file or other sensitive data from your computer.

- **File/Folder names and properties.** After deleting files and folders on FAT or NTFS drives, recovery utilities may still be able to find the names and properties of the files and folders you have deleted, even if they are not able to recover any information from their contents. This may reveal very sensitive information.

1.2 Overview of East-Tec Eraser 2013

1.2.1 Introducing East-Tec Eraser 2013 ("Eraser" in short)

East-Tec Eraser 2013 ("Eraser" in short) is an advanced security application designed to help you completely eliminate sensitive data from your computer and protect your computer and Internet privacy.

Erasing a file now means wiping its contents beyond recovery, scrambling its name and dates and finally removing it from disk. When you want to get rid of sensitive files or folders beyond recovery, add them to the Eraser list of doomed files and ask Eraser to do the job. Eraser offers tight integration with the Windows shell, so you can drag files and folders from Explorer and drop them in Eraser, or you can erase them directly from Explorer by selecting 'Erase beyond recovery' from the context menu.

Eraser is also able to completely destroy any data from previously deleted files that might still be accessible on your disk, in the Recycle Bin or in unused disk areas. Eraser can also remove sensitive information stored without your knowledge or approval (evidence of your computer activities, texts and pictures from sites visited on the Internet, the contents of deleted e-mail messages, etc.)

Eraser can also completely destroy entire drives, using its integrated Entire Drive Wiper. When you give your co-worker or friend a file or a program on a disk (floppy, CD/DVD-RW, USB flash drive, ZIP, Jaz, or any other type of disk), or give him access to your hard disk, you may actually give him access to the information that the disk used to contain. Backup copies of your financial records or business plans, your private files and e-mail messages, and all your other sensitive documents can easily fall into the wrong hands. The Entire Drive Wiper feature from Eraser, in addition to formatting a drive, securely wipes the data in order to eliminate all sensitive information beyond recovery.

The extensive erasing capabilities of Eraser make sure that not even a trace remains after erasing data. Eraser has a lot of erasing (wipe) methods, differing in speed and security. The fastest ones offer normal security and can stop software recovery tools. The slower ones match and exceed the specifications of the U.S. Department of Defense and can stop even the most sophisticated hardware recovery tools. If you are not satisfied with the existing wipe methods, you can even define your own wipe methods. Advanced features like verifying each wipe pass and each disk operation allow Eraser to intercept any failures and inform you if data is not successfully erased.

With Eraser you can also erase entire folder structures (folders with all their subfolders and files) and even entire drives. Features like the possibility of collecting multiple file specifications (e.g. *.tmp) turn Eraser into a clean-up utility. The command-line parameters allow you to use Eraser from BAT files or from scheduling software.

Additional features include password protection, optional confirmation, logging support, data retention policies, critical folder protection, and more.

Eraser has a very intuitive interface and it is very easy to use. Offers tight integration with the Windows shell (drag and drop and integration via the Explorer context menu).

1.2.2 How can Eraser help me get rid of sensitive information?

Erasing very sensitive files with Eraser

Existing files can be easily destroyed with Eraser. All you have to do is ask Eraser to erase them beyond recovery. This is a very secure way to get rid of sensitive files: after Eraser has finished erasing them, you can be sure they are gone for good.

Erasing sensitive information stored without your knowledge or approval

Eraser can remove sensitive information the Windows operating system has stored on your computer without your knowledge or approval. You can clear sensitive information from the swap file, delete temporary files created by applications, destroy evidence of your previous activities, etc.

Eliminating evidence of your Internet activities

Your computer documents not only your web browsing activity (sites visited, etc.) but retains any picture or graphic previously viewed for easy and fast retrieval. Eraser can remove all traces of your Internet activity: history, cookies, text, pictures and sounds.

Destroying the contents of previously deleted files

Deleting a file using the Windows operating system does not remove the file contents from your hard drive. It simply prevents you from accessing the file. As a result, sensitive and private information can be easily retrieved by almost anyone. Eraser can help you ensure that previously deleted files are removed from your computer beyond recovery.

This feature allows you to continue to delete data using the methods offered by the applications you use (delete files with Explorer or other file managers, delete mail messages with your mail application, delete cache files / temporary Internet files with your Web browser, etc.). Then you should use Eraser to ensure the data and files you delete are really destroyed beyond recovery.

Eliminating deleted email

When you delete an email message from Outlook Express, Netscape Messenger or other mail programs, the message is moved to a special folder called "Deleted Items" or "Trash" and is not removed from disk. Even if you empty the "Deleted Items" or "Trash" folders, part of the original message may still remain stored on disk. Eraser is able to thoroughly rid your disk of discarded email.

Erasing entire disk drives (hard drive partitions, floppy, CD/DVD-RW, USB flash drive, etc.)

When you give your co-worker or friend a file or a program on a disk (floppy, CD/DVD-RW, USB flash drive, ZIP, Jaz, or any other type of disk), or give him access to your hard disk, you may actually give him access to the information that the disk used to contain. Backup copies of your financial records or business plans, your private files and e-mail messages, and all your other sensitive documents can easily fall into the wrong hands. The Entire Drive Wiper feature from Eraser, in addition to formatting a drive, securely wipes the data in order to eliminate all sensitive information beyond recovery.

1.2.3 Why use Eraser and its data destruction capabilities?

EVERYONE has sensitive information to protect from falling into the wrong hands. Normal deletion is not secure, you need the Eraser to make ensure your deleted data is not recoverable.

Suppose you have sensitive files on your computer (personal letters, financial reports, health records, etc.) and want to move them to a floppy disk to make ensure only you can access them. Moving the files to the floppy disk will mean copying them and then deleting them from the hard drive. But normal deletion is not secure! The result is that the contents of your sensitive files will remain exactly where you didn't want them: on the hard drive. If you copy the files to the floppy disk and then destroy them using the Eraser, you have accomplished your task. The files are now only on your floppy disk!

Privacy and security are important - you need East-Tec Eraser and its data destruction capabilities.

2 Using Eraser

2.1 Quick start

4 easy ways to erase files with East-Tec Eraser 2013

Using the 'Erase beyond recovery' context menu entry

1. In My Computer or Windows Explorer, select one or more files and/or folders.
2. Click the right mouse button to open the context menu.
3. Run the 'Erase beyond recovery' command from the context menu.

Using 'Send To'

1. In My Computer or Windows Explorer, select one or more files and/or folders.
2. Click the right mouse button to open the context menu.
3. Select the 'Send To' menu item and click on Eraser.

Dropping items on the East-Tec Eraser 2013 desktop icon

1. In My Computer or Windows Explorer, select one or more files and/or folders.
2. While holding down the left mouse button, drag (move) the mouse pointer over the East-Tec Eraser 2013 icon on the desktop.
3. Release the mouse button to drop the file(s) and/or folder(s).

Running East-Tec Eraser 2013 in interactive mode

1. Start East-Tec Eraser 2013 (from the East-Tec Eraser 2013 program folder or by clicking the Eraser desktop icon).
2. Drag one or more files and/or folders from My Computer or Windows Explorer to the Eraser window. If you've minimized Eraser, you can drag the files and folders to the minimized icon.
3. Click on the 'Erase Files & Folders' toolbar button (or select the 'Erase Files & Folders' menu item from the Erase menu).

The easy way to protect your computer and Internet privacy

1. Start East-Tec Eraser 2013 (from the East-Tec Eraser 2013 program folder or by clicking the East-Tec Eraser 2013 desktop icon).
2. Click on the 'Privacy Guard' toolbar button (or select the 'Privacy Guard' menu item from the Erase menu).

2 easy ways to destroy the contents of previously deleted files

Using the 'Wipe deleted data' context menu entry

1. In My Computer or Windows Explorer, select one or more drives.
2. Click the right mouse button to open the context menu.
3. Run the 'Wipe deleted data' command from the context menu.

Running East-Tec Eraser 2013 in interactive mode

1. Start East-Tec Eraser 2013 (from the East-Tec Eraser 2013 program folder or by clicking the East-Tec Eraser 2013 desktop icon).
2. Click on the 'Erase Deleted Data' toolbar button (or select the 'Erase Deleted Data' menu item from the Erase menu).

2 easy ways to destroy the files in the Recycle Bin

Using the 'Erase beyond recovery' entry from the Recycle Bin context menu

1. Select the Recycle Bin icon
2. Click the right mouse button to open the context menu.
3. Run the 'Erase beyond recovery' command from the context menu.

Running East-Tec Eraser 2013 in interactive mode

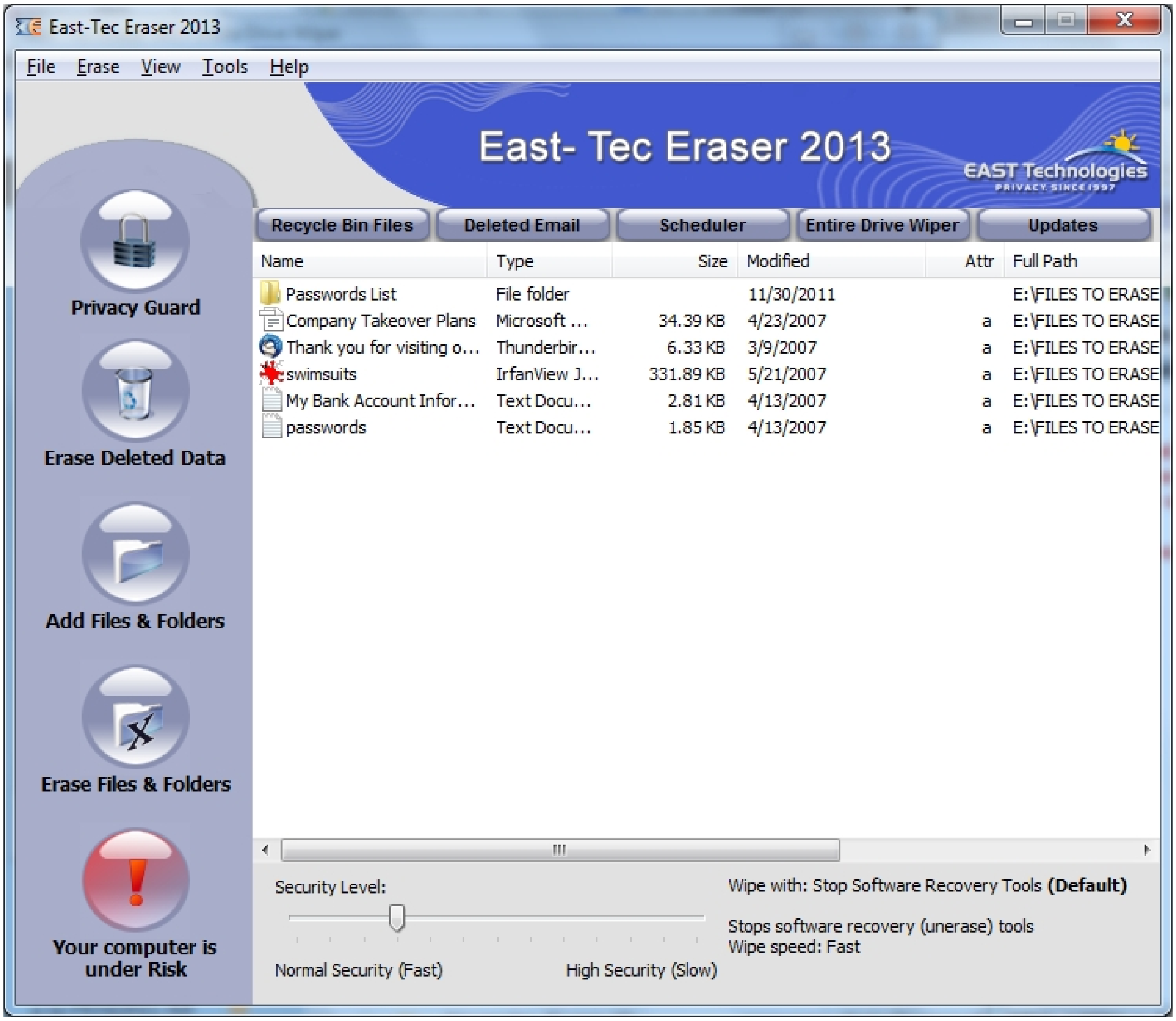
1. Start Eraser (from the Eraser program folder or by clicking the Eraser desktop icon).
2. Click on the '(Eliminate) Recycle Bin Files' toolbar button (or open the Erase menu, select 'Eliminate' and click on the 'Recycle Bin Files' menu item).

The easy way to erase entire disk drives beyond recovery

1. Start East-Tec Eraser 2013 (from the East-Tec Eraser 2013 program folder or by clicking the East-Tec Eraser 2013 desktop icon).
2. Open the Tools menu, select 'Entire Drive Wiper', choose the disk drives you want to erase entirely, and follow the instructions from the screen.

2.2 The Eraser Interface

Here is a snapshot of the Eraser main window:



Name	Type	Size	Modified	Attr	Full Path
Passwords List	File folder		11/30/2011		E:\FILES TO ERASE
Company Takeover Plans	Microsoft ...	34.39 KB	4/23/2007	a	E:\FILES TO ERASE
Thank you for visiting o...	Thunderbir...	6.33 KB	3/9/2007	a	E:\FILES TO ERASE
swimsuits	IrfanView J...	331.89 KB	5/21/2007	a	E:\FILES TO ERASE
My Bank Account Infor...	Text Docu...	2.81 KB	4/13/2007	a	E:\FILES TO ERASE
passwords	Text Docu...	1.85 KB	4/13/2007	a	E:\FILES TO ERASE

Security Level:

Wipe with: Stop Software Recovery Tools **(Default)**

Stops software recovery (unerase) tools
Wipe speed: Fast

2.3 Erasing File and Folders

2.3.1 Erasing files and folders with Eraser

Step 1. Select the files and folders you want to erase and add them to the Eraser window

To add files and folders using drag and drop:

1. In My Computer or Windows Explorer, select any number of files and folders.
2. While holding down the mouse button, drag (move) the mouse pointer to the Eraser window. If you've minimized Eraser, you can drag the files and folders to the minimized icon.
3. Release the mouse button to drop the files and folders.

To add files and folders using the Eraser Add options:

1. Click on the 'Add Files & Folders' toolbar button or open the Erase menu and select 'Add Files...' or 'Add Folders...'.
2. Select 'Add Files' to add one or more files; select 'Add Folders' to add a folder; select Search for Files to search for the items you want to erase or to add a large number of files using wildcards.

Step 2. Use the Erase Files & Folders option to erase the selected items

WARNING: Before starting to erase, please ensure that you have selected only the files and folders you really want to destroy beyond recovery. If you erase a file by mistake with Eraser, you will not be able to recover it!

To erase the files and folders you have selected and added to the Eraser window, click on the 'Erase Files & Folders' toolbar button or open the Erase menu and select 'Erase Files & Folders'.

When the erase process is completed, the files and folders that were successfully erased are automatically removed from the main list box.

2.4 Protecting your computer and Internet privacy

2.4.1 The Privacy Guard feature

The Privacy Guard will seek out and destroy (Erase Beyond Recovery) the contents of folders that monitor and track your Internet usage and habits. It will also rid your computer of Windows "hidden" files and other data stored without your knowledge. Furthermore, you may also customize this feature to target specific files or folders that may contain sensitive or embarrassing information.

To open the Privacy Guard dialog box, click on the 'Privacy Guard' toolbar button from the Main window or select the 'Privacy Guard' command from the Erase menu. The Privacy Guard has a Wizard intuitive interface.

The Privacy Guard dialog box lets you choose between running the **Basic** or the **Advanced** mode.

Note: When opening the Privacy Guard feature, there is a button called 'Autodetect installed programs', by clicking on this button, all programs installed on your computer will be considered when wiping traces of your activity.

The **Basic** mode will run all the pre-configured defaults. This option is recommended for most users. The **Advanced** mode allows you to choose your own options for the Privacy Guard. It contains the following major components:

Windows Sensitive Areas

Select this option to remove sensitive information the Windows operating system has stored on your computer without your knowledge or approval. You can clear sensitive information from the swap file, delete temporary files created by applications, destroy evidence of your previous activities, delete Thumbs.db files etc. This will allow you to protect your computer privacy.

NOTE: The Windows Sensitive Areas page also has an option that allows you to find and erase files that contain alternate data streams on NTFS. The NTFS file system provides applications the ability to create alternate data streams for each stored file/folder. Although these streams are not visible to the average users, they can be easily found on the disk even after the actual file that they belong to are deleted. The streams contain any kind of sensitive information since they have the same format as normal files do.

Browsers Sensitive Areas

Your computer documents not only your web browsing activity (sites visited, etc.) but retains any picture or graphic previously viewed for easy and fast retrieval. Select this option to remove all traces of your Internet activity: history, cookies, text, pictures and sounds from the popular browsers installed on your computer (Opera 9, Mozilla Firefox, Internet Explorer 6 and 7, etc).

This area protects your Internet privacy.

Applications Sensitive Areas

Use this option to remove sensitive information from the popular applications and programs installed on your computer (e.g. Yahoo Messenger, Windows Media Player, RealPlayer, Divx Player, Adobe Photoshop and many more). The available applications and programs are displayed in the Applications Areas, in the Privacy Guard.

Peer2Peer Sensitive Areas

Use this option to remove sensitive information from the popular Peer2Peer applications and programs installed on your computer (e.g. Kazaa, Kazaa Lite, iMesh, Limewire, Napster, Morpheus, Direct Connect, Edonkey, Shareaza, SoulSeek and many more). The available Peer2Peer applications and programs are displayed in the Peer2Peer Sensitive Areas, in the Privacy Guard.

NOTE: You should check only the applications and programs that are installed on your computer. A warning message will appear once you select an application or program that is not installed.

After selecting an application (already installed on your computer), the 'Properties' button will allow user to set his own erasing options for that application.

News and Email Readers

Use this option to remove traces of newsgroup activities (messages, binaries, etc.) and deleted email messages from popular news and email programs (Outlook Express, Mozilla Thunderbird, Agent Newsreader, Eudora etc.). The available news and email programs are displayed in the News & Email Readers area, in the Privacy Guard.

Custom Sensitive Areas

The Privacy Guard also allows you to target specific files and folders to Erase Beyond Recovery. You can use this special feature to destroy files and folders that usually contain sensitive data (such as password files, business plans, trade secrets, financial records, etc.). You can also eliminate data from registry entries that may contain sensitive information. If you want to find out how to create new custom sensitive areas, please read the Creating Custom Sensitive Areas section.

Press the Start button to erase the selected sensitive information. The data will be destroyed in accordance with the specified erase setting.

NOTE: After running the Privacy Guard you will be prompted to restart your computer. This step is necessary to delete certain "locked" Windows files.

Don't forget to read the Important facts about the Privacy Guard feature 10 topic.

2.4.2 Important facts about the Privacy Guard feature

Scramble files and folders properties in Privacy Guard

This option is not required when running the Privacy Guard feature. This is because only the contents of files are sensitive, whereas the filenames are not sensitive information. The names of files erased using the Privacy Guard feature are usually standard names given by the application itself and do not contain sensitive information about your activity.

For advanced security reasons, you also have the possibility to select this option, however the overall performance of the computer will be slowed down during the wiping process as the disk space will temporarily fall to zero bytes.

Sometimes Windows will warn you that you are running out of disk space on the drive where Eraser is scrambling the file properties. You should ignore this error, because Eraser will free up the disk space after it finishes wiping.

Cookies to protect

Cookies are usually a major privacy concern, as they can be used to gather valuable information on your habits or interests. The Privacy Guard feature protects your privacy by deleting these cookies. However you may wish to retain specific cookies that make your Internet browsing convenient.

To protect the cookies for sites you visit frequently, just open the Privacy Guard and in the Browsers section select any of the browsers installed on your computer, click the Properties button and in the window that appears select Protect Cookies, then check the cookies you want to protect.

Windows and Internet Explorer "Locked" files

After running the Privacy Guard you will be prompted to restart your computer. This step is necessary to delete certain "locked" Windows files. These are files that are used by Windows or by Internet Explorer and can only be erased while Windows starts. One of these files may be the Windows swap file, a file that may contain sensitive information collected without your knowledge or approval. The Internet Explorer history or cookies index files are also "locked" while Windows is running.

Not found application warning
In the Application Sensitive Areas section there is a list containing all the available applications you may select. If you want to check an application not installed on your computer, a warning message will appear prompting you that application does not exist on your PC.

Note: When opening the Privacy Guard feature, there is a button called 'Autodetect installed programs', by clicking on this button, all programs installed on your computer will be considered when wiping traces of your activity.

The Privacy Guard feature 9

2.5 Destroying previously deleted files beyond recovery

2.5.1 The Erase Deleted Data feature

Deleting a file using the Windows operating system does not remove the file contents from your hard drive. It simply prevents you from accessing the file. As a result, sensitive and private information can be easily retrieved by almost anyone.

The Erase Deleted Data feature ensures that previously deleted files are removed from your computer beyond recovery.

Please note that running the Erase Deleted Data feature on large drives can take a long time. However, this disadvantage can be overcome by scheduling the erasing process at times when the computer is not used or only at the end of the day (or of the week).

To find out more about the Scheduler feature read The Scheduler 22 page.

Contents:

2.5.2 Overview

Previously deleted information and files are usually stored in the following locations on disk:

1. **The Recycle Bin**: When you delete a file, Windows usually moves it to the Recycle Bin instead of removing it from disk. The files stored in the Recycle Bin are removed from disk when you empty the Recycle Bin.

2. **The disk free space**: The free space on disk usually contains the contents of the files that were previously deleted using standard operating system commands. Some of them were temporary files used by applications; these temporary files were created and deleted without your knowledge. Let's also take into account the Windows Swap file, the system file used for the virtual memory support. The size of this file changes dynamically, and it can temporarily store the parts of files or other information. You see now that the disk free space is not at all "empty": it may contain passwords, financial records, personal files, etc. In a word, it contains sensitive data that can be restored using any disk utility.

3. **The file slack**: The file slack is usually filled with random information that comes from your computer. The information can be a listing of a directory, a part of a password file or other sensitive data from your computer. This information is an easy target for hackers as they can restore it using any disk utility.

4. **File/Folder names and properties.** After deleting files and folders on FAT or NTFS drives, recovery utilities may still be able to find the names and properties of the files and folders you have deleted, even if they are not able to recover any information from their contents. This way, the identity of the erased files and folders can be revealed.

5. **Systems log file (NTFS drives).** Or the file named $LogFile, that contains a list of transaction steps used for NTFS recoverability. The log file size depends on the volume size and can be as large as 4 MB. It is used by Windows NT/2000/XP to restore consistency to NTFS after a system failure, and it contains very sensitive information about all transactions you make in your system (such as temporary data of all files you are working with).

The **Erase Deleted Data** feature was designed to help you get rid of any sensitive information stored in these three areas of your disks:

- It destroys the contents of the files stored in the Recycle Bin and then removes them from disk.
- It wipes the free space on drives. This ensures that the content of previously deleted files is destroyed beyond recovery. The existing files on drive are not modified.
- It wipes the files slack without modifying the files themselves. This ensures that any sensitive information that happens to be located in the slack portion of a file is now gone forever.
- It removes any file attributes that might reveal the identity of the erased files or folders by destroying (scrambling) files and folders properties (name, date, size, etc.). This ensures that the files and folders properties on FAT or NTFS drives are properly destroyed and cannot be recovered.
- It erases the system transactions log file (NTFS drives), ensuring that information about the transactions you make in your system, are deleted.

Using the Erase Deleted Data feature 13

2.5.3 Using the Erase Deleted Data feature

First open the Erase Deleted Data dialog box, by clicking on the 'Erase Deleted Data' toolbar button or by selecting the 'Erase Deleted Data' command from the Erase menu.

If you want to destroy the contents of all the files stored in the Recycle Bin and then remove them from disk, select the 'Destroy all files from the Recycle Bin beyond recovery' option.

Then select one or more drives from the drives list box and click on the Start button to start destroying the deleted information from the selected drives. For maximum security, you should select to wipe both the disk free space and the slack portion of existing files.

If you want to remove any file attributes that may reveal the identity of the erased file or folder, select the 'Scramble files and folders properties (name, data, size ...)' option. When this option is enabled, the files and folders properties are destroyed (scrambled).

Select 'Scramble system transactions log file (on NTFS)' to clear the file named $LogFile, that contains a list of transaction steps used for NTFS recoverability. The log file size depends on the volume size and can be as large as 4 MB. It is used by Windows NT/2000/XP to restore consistency to NTFS after a system failure, and it contains very sensitive information about all transactions you make in your system (such as temporary data of all files you are working with).

IMPORTANT: Before running the "Erase Deleted Data" feature it is recommended to close all running applications (programs). Running applications sometimes create temporary files that may store sensitive data. Eraser cannot destroy the contents of these sensitive files if the applications that created them are currently running. Running applications also store data in the Windows swap file (the file used for virtual memory support). That part of the swap file cannot be wiped while those applications are running.

Overview of the Erase Deleted Data feature 12

2.5.4 Important facts

The Erase Deleted Data feature is a slow process on large drives

Please note that running the Erase Deleted Data feature on large drives can take a longer time. However, this disadvantage can be overcome by scheduling the erasing process at times when the computer is not used or only at the end of the day (or of the week).

Wiping the unused disk space will temporary modify the amount of disk free space

When wiping the unused disk space on a drive, Eraser creates a series of temporary files (.WIP files) in a folder placed in the root of the disk drive and fills them until there is no free space left on drive. Then it removes them from disk, thus freeing up the disk space. Each temporary file has up to 2 GB in size (if your drive has 3 GB of free space, Eraser will create two temporary files, one of 2GB and one of 1GB, it will fill them and then remove them from disk). This high-level method is the most secure method to wipe the disk free space, because there is no danger for existing files to get modified or deleted.

Sometimes Windows will warn you that you are running out of disk space on the drive where Eraser is wiping the disk free space. You should ignore this error, because Eraser will free up the disk space after it finishes wiping.

Question: My system crashed while Eraser was wiping the disk free space and all of my available hard drive space disappeared. How do I get it back?
Answer: Run Eraser again and it will automatically delete all the temporary files that remained on your

drive(s) after wiping the free space.

Scramble files and folders properties option

After wiping the free space on a drive, recovery utilities may still report previously deleted files as being available for recovery. This is because wiping the free space on a drive does not destroy the names of the deleted files. However, they will NOT be able to recover any data from their contents.

To remove any file attribute that may reveal the identity of the erased files and folders, check the 'Scramble files and folders properties (name, data, size ...)' option when running the Erase Deleted Data feature.

NOTE: Using this method may slow down the wiping process, especially on large hard drives containing substantial amount of information (files and folders).

The Windows swap file

To wipe any sensitive information from the Windows swap file (the file used for virtual memory support), please run the Privacy Guard 9 feature.

2.6 Eliminating deleted Email

2.6.1 Eliminating deleted Email with Eraser

When you delete an email message from Outlook Express, Microsoft Outlook, Netscape Mail or other mail programs, the message is moved to a special folder called "Deleted Items" or "Trash" and is not removed from disk. Even if you empty the "Deleted Items" or "Trash" folders, part of the original message may still remain stored on disk.

Eraser is able to thoroughly rid your disk of discarded email.

To access this feature, click on the Deleted Email toolbar button, or open the Erase menu, choose Eliminate and click on the Deleted Email menu command.

2.6.2 Instructions for other email programs

Eraser helps you get rid of deleted email messages with Outlook Express, Microsoft Outlook, Netscape Mail, Eudora, Yahoo, Gmail, etc.

This help topic contains instructions for other popular email programs.

First of all, delete the email message(s) you want to get rid of from your email program.

Then:

Outlook Express users:

Step 1: Open the Outlook Express Edit menu and select 'Empty the Deleted Items Folder'.
Step 2: Open the Outlook Express File menu and select 'Folder', then 'Compact all folders'.
Step 3: Run the Erase Deleted Data feature from Eraser 13.

Microsoft Outlook users:

Step 1: Open the Outlook Tools menu and select 'Empty the Deleted Items Folder'.
Step 2: Open the Outlook File menu and select 'Data File Management' . Select the data file to compact, and then click Settings. Now click 'Compact Now'.
Step 3: Run the Erase Deleted Data feature from Eraser 13.

Netscape Mail users:

Step 1: Open the Netscape Mail File menu and select 'Empty Trash'.
Step 2: Select the Trash folder. Open the Netscape Mail File menu and select 'Compact this folder'.
Step 3: Run the Erase Deleted Data feature from Eraser 13.

Eudora users:

For Eudora, please go to the Privacy Guard - News and Email Readers.

IncrediMail users:

Step 1: Open the IncrediMail Edit Menu and select Empty 'Deleted Items' Folder.
Step 2: Close IncrediMail.
Step 3: Run the Erase Deleted Data feature from Eraser 13.

Pegasus Mail users:

Step 1:Close Pegasus Mail.
Step 2: Run the Erase Deleted Data feature from Eraser 13.

Opera Mail users:

Step 1: Open the Opera Mail Panel, right click 'Trash' and select 'Emtpy Trash'.
Step 2: Close Opera.
Step 3: Run the Erase Deleted Data feature from Eraser 13.

Web-based Email (Hotmail, Yahoo, Gmail, etc) users:

Step 1: From your web browser, access your web-based email account and empty the Trash or Deleted Items folder.
Step 2: Run the Privacy Guard feature from Eraser 9.

2.7 Erasing entire disk drives

2.7.1 Erasing entire disk drives

To erase entire disk drives, please click the Entire Drive Wiper toolbar button, or select the Entire Drive Wiper option from the Tools menu of East-Tec Eraser 2013.

Step 1: Selecting the drives/devices to wipe

East-Tec Eraser 2013 will first open an Introductory Screen that displays information about what it means to usually format a drive using the Windows Format option. Selecting the Next button in this Introductory Screen, East-Tec Eraser 2013 will let you select the drives you want to wipe. You will have the possibility to select one or more hard disk drives and also one or more devices with removable storage connected to your computer.

After selecting the drive(s)/device(s) you want to wipe, click the Next button to go to the following step: Selecting the wipe method.

Note: With the Disk Viewer, you can see the data that exists in the sectors of a disk drive. The Disk Viewer can help you better observe the wipe process and verify that all the original disk data is destroyed beyond recovery.

You can choose the Disk Viewer feature in Step 1: Selecting the drives/devices to wipe when you select the drive(s)/device(s) to be wiped, or after the wipe process for a drive has been finished.

Step 2: Selecting the wipe method

After selecting the drive(s)/device(s) you want to wipe, East-Tec Eraser 2013 will now let you select the wipe method you want to use. In this screen you will see the list of available wipe methods. When you select a method name in the list, the method description is displayed in the lower part of the screen.

NOTE: To learn more about the wipe methods, please read the Wiping Methods/Algorithms 22 topic.

After choosing the wiping method, click the Next button to go step 3.

Step 3: Selecting the wipe options

East-Tec Eraser 2013 will now let you select various wipe options. In this window you will see the list of available wipe options.

NOTE: To learn more about the wipe options, please read the Entire Drive Wiper Options 16 topic.

After choosing the wipe options, click the Next button to go to the following step: Starting the wipe process.

Step 4: Starting the wipe process

Before starting to wipe the selected drive(s) and/or device(s) using the selected wipe method and options, East-Tec Eraser 2013 will open a "safety" screen that warns you that you are about to destroy the data from one or more drives beyond recovery.

To start the wipe process, all you have to do is click the Next button. The next screen will display the progress bar showing the evolution of the wipe process.

Step 5: The Wipe Process

During the wipe process, East-Tec Eraser 2013 will display a progress bar showing the evolution of the wipe process, the name of the drive wiped in that moment and the name of the method used to wipe that drive. If the option 'Allow the user to abort the wiping process' was selected before, the user may also choose to pause or to abort the wipe process.

2.7.2 Entire Drive Wiper Options

Displays the Wipe Options dialog box, allowing you to change various erase and security level settings. Please see below:

Allow the user to abort the wiping process

If this option is selected, the user will be allowed to abort the wiping process during the execution. Otherwise, the process will be executed and the user will not be able to stop it.

DEFAULT VALUE: (on)

Wipe without requiring user intervention

If this option is selected, the wiping process will not require user intervention. After a drive/device has been wiped, East-Tec Eraser will automatically start to wipe the next selected drive. When an error occurs, it will not be displayed to the user and the wiping process will automatically continue.

DEFAULT VALUE: (off)

NOTES: This option allows you to wipe one or more drives without requiring user intervention or input. After selecting the drives to wipe and the wipe method and options, the user can leave the product to do its job and continue his work elsewhere.

Use ISAAC pseudo random number generating algorithm

If this option is selected, East-Tec Eraser will use ISAAC pseudo random number generation algorithm for random data generating. This ensures a high security level but slows down the wiping process.

DEFAULT VALUE: (off)

No buffering/caching

When this option is enabled, data is written to disk without intermediate buffering or caching. This provides performance gains in many situations. When this option is disabled, data is written using the standard buffered/cached method and disk buffers are flushed at the end of each wipe pass. (Note: If you disable this option, other applications will run slower while East-Tec Eraser is wiping)

Overwrite buffer: This option allows you to select the size of the buffer used to wipe data. Larger buffer sizes should substantially speed up the wiping process. You may want to experiment with different buffer sizes in order to determine where you get the best performance (the recommended buffer size is 512 KB).

DEFAULT VALUE: (on)

Quick Wipe CD/DVD-RW drives

When this option is enabled, East-Tec Eraser will erase the disc quickly (between 1 and 2 minutes depending on the recorder speed), but the program area will still contain user data.

The quick erase option is recommended for routine use, when you want to prepare the disc for another burning but do not need to ensure that the data is erased beyond recovery.

DEFAULT VALUE: (off)

Format the disk drive in addition to wiping all data

When this option is selected, a quick format of the drive will be also executed at the end of the wipe process. This step will remove all traces of the destruction process.

DEFAULT VALUE: (on)

Ask after every wipe

If this option is selected, the wipe process will require user intervention after a drive/device has been wiped.The user can choose to continue, to abort or to view the disk.

DEFAULT VALUE: (off)

Generate report file

If this option is selected, East-Tec Eraser will generate a wipe report file for each drive that is wiped. The log will contain information about the drive, the time and date of wiping, any errors that occur while wiping, etc. The user can choose the name and the place where the report file will be generated.

DEFAULT VALUE: (off)

Use Department of Defense log style for generating log file

If this option is selected, East-tec Eraser will also log extra information required by U.S. Dept. of Defense standards (such as the name of the person performing the wiping process). The log file will also contain the exact contents of any sector that could not been wiped. This helps the user determine if the data that remained on disk is too sensitive to permit the release of the media.

DEFAULT VALUE: (off)

Append log file

This option must be selected if you want to keep the current contents of the log file, and add new entries at the end of the file.

2.7.3 Command-line parameters

You may run Entire Drive Wiper from the command line prompt. This feature allows you to automatically erase entire disk drives from BAT files or from scheduling software.

Use the following syntax:
ETDRIVEWIPER disk1 [disk2 …] [erase options]

disk1, disk2, …
The disk drives to be completely erased. You will be prompted for confirmation before erasing them according to the current options.

erase options
See the erase options below:

/M<methodID>
Use a specific wipe method to perform the actions specified in the command-line. MethodID can be 0 (the first wipe method as it appears in the wipe method list), 2 (the second), and so on.

/U
If this parameter is used, the user will be allowed to abort the wiping process during the execution. Otherwise, the process will be executed and the user will not be able to stop it.

/W
If this parameter is used, the wiping process will not require user intervention. After a drive/device has been wiped, Entire Drive Wiper will automatically start to wipe the next selected drive. When an error occurs, it will not be displayed to the user and the wiping process will automatically continue.

/I
If this parameter is used, the process will use ISAAC pseudo random number generation algorithm for random data generating. This ensures a high security level but slows down the wiping process.

/N
If this parameter is used, data is written to disk without intermediate buffering or caching. This provides performance gains in many situations.

/Q
If this parameter is used, Entire Drive Wiper will erase the disc quickly (between 1 and 2 minutes depending on the recorder speed), but the program area will still contain user data. The quick erase option is recommended for routine use, when you want to prepare the disc for another burning but do

not need to ensure that the data is erased beyond recovery.

/F
If this parameter is used, a quick format of the drive will be also executed at the end of the wipe process. This step will remove all traces of the destruction process.

/K
If this parameter is used, the wipe process will require user intervention after a drive/device has been wiped.The user can choose to continue, to abort or to view the disk.

/R
If this parameter is used, the wipe process will generate a wipe report file for each drive that is wiped. The log will contain information about the drive, the time and date of wiping, any errors that occur while wiping, etc. The user can choose the name and the place where the report file will be generated.

/D
If this parameter is used, the process will also log extra information required by U.S. Dept. of Defense standards (such as the name of the person performing the wiping process). The log file will also contain the exact contents of any sector that could not been wiped. This helps the user determine if the data that remained on disk is too sensitive to permit the release of the media.

/A
This parameter must be used if you want to keep the current contents of the log file, and add new entries at the end of the file (append).

Example

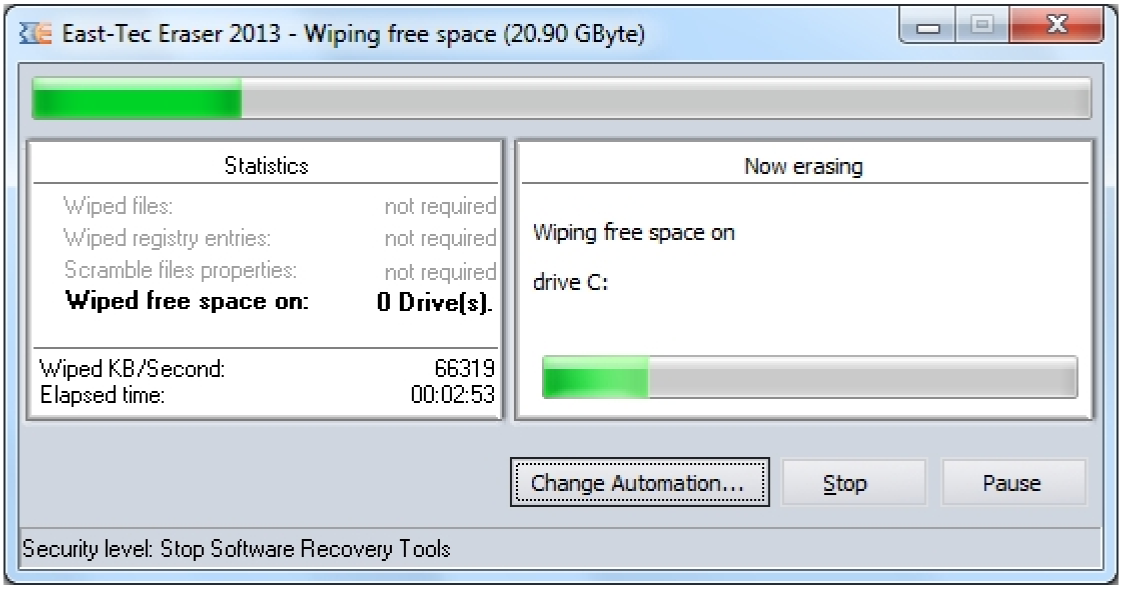
```
"C:\Program Files\East-Tec Eraser 2013\etdrivewiper.exe" E /M5 /R
"C:\Users\admin\AppData\Roaming\EAST Technologies\East-Tec Eraser\report.txt"
```

This command will completely erase partition E using method number 5 and it will generate a log file (report.txt) at "C:\Users\admin\AppData\Roaming\EAST Technologies\East-Tec Eraser".

2.8 The Progress Box

2.8.1 The Progress box

While Eraser erases files and folders, or runs Privacy Guard or Erase Deleted Data, the following dialog box is displayed:



East-Tec Eraser 2013 - Wiping free space (20.90 GByte)

Statistics

Wiped files:	not required
Wiped registry entries:	not required
Scramble files properties:	not required
Wiped free space on:	**0 Drive(s).**
Wiped KB/Second:	66319
Elapsed time:	00:02:53

Now erasing

Wiping free space on

drive C:

Security level: Stop Software Recovery Tools

The Preferences page of the Erase Options dialog box contains a few options that control the progress box.

3 Menu Reference

3.1 File Menu

Exit
Exits the program.

3.2 Erase Menu

Add Files & Folders 8
Contains commands that help you select the files and folders you want to erase beyond recovery.

Erase Files & Folders 8
Starts erasing the selected files and folders.

Privacy Guard 9
Protects your computer and Internet privacy by removing sensitive data stored without your knowledge.

Erase Deleted Data 11
Helps you ensure that no one will recover your deleted information.

Erase Options
Displays the Erase Options dialog box, allowing you to change various erase and security level settings.

Eliminate
Helps you get rid of Recycle Bin files or Deleted Emails.

3.3 View Menu

Large Icons
Displays large icons in the item list.

Small Icons
Displays small icons in the item list.

List
Displays the items in a list

Details
Displays details in the item list.

Sort
Changes the sort order in the list of items to be erased.

3.4 Tools Menu

Scheduler 22
Opens the Scheduler window to allow you to define your erasing tasks.

Entire Drive Wiper 15
Opens the Entire Drive Wiper feature allowing you to erase entire drives.

Volume Shadow Copy Manager 25
Opens the Shadow Copy Manager window allowing you to manage shadow copies. This option is available in Windows Vista and Windows 7 only.

3.5 Help Menu

Help Topics
Opens program Help.

Support
Displays technical support 32 information.

East-Tec Eraser 2013 on the Web
Opens the EAST-TEC Internet Page

User Survey Form
Displays a survey form that allows you to submit your comments and responses. This allows us to continually improve the program.

Enter Key
Opens a window that allows you to enter the name and the key so that you can convert the trial into the licensed version.

About
Displays program information, version and copyright.

4 Advanced Topics

4.1 Wiping Capabilities

4.1.1 The Erasing Security Level: Wipe Methods

Have you tried any of the erasing utilities on the market? If you have, then you must have noticed that most of them do not offer a real control over the wiping process. They usually offer only two types of destroying (wiping) information: a normal (one or two pass) wiping and a special U.S. DoD seven pass wiping. You may find that in some cases none of the above two options is appropriate for you. What can you do in this case?

Eraser does not have only built-in wipe methods. It also offers an easy way **to define** (create) wipe methods. Defining a wipe method means specifying the number of passes and the overwriting pattern for each pass.

The **number of passes** specifies how many times to overwrite the data. One pass is sufficient to stop software recovery tools. Several passes might be needed to stop hardware recovery tools such as electron-tunneling microscopes. These tools can recover faint magnetic residue from previous writes.

The **overwriting pattern** (or the wiping pattern) is the pattern used to overwrite the file data. You can choose between:
- a fixed byte pattern (e.g. 0, FF, etc.)
- a text pattern (e.g. "Censored by Me!")
- a random data stream

The **Shuffle passes option** is used to mix the order of the passes indicated by the interval defined by the two values. To use this option, you need to select at least 2 wipe passes.

A **very powerful security feature** is the possibility of verifying whether the wiping patterns are written correctly to disk over the file's original data. This is accomplished by re-reading the data from file after each pass and comparing it with the wiping patterns.

IMPORTANT: If you want to wipe a file located on a compressed drive, the selected wipe method must have at least one pass that uses a random data stream. A random data stream cannot be compressed, therefore you are assured that the entire file is properly overwritten.

See Also

Security Level (Wipe Method) dialog box, Edit Wipe Method dialog box

4.2 Tools

4.2.1 The Scheduler

4.2.1.1 The Scheduler Window

Use the **Scheduler** feature to run East-Tec Eraser 2013 at a specified time/event or when the computer has been idle for a number of minutes.

The Scheduler allows for better management of system resources while keeping your computer secure. You may, for example, run East-Tec Eraser 2013 at times when the computer is not in use, or when it has been idle for a number of minutes.

The Scheduler window allows you to view and control created tasks using the buttons on the buttom of the screen.

New Task opens the windows which will guide you step by step in creating a new task.
Delete will delete the selected tasks.
Properties will display the properties of the selected task, and allow you to change them.
Create Shortcut will create a shortcut.
Run will start the selected task.

4.2.1.2 How to define a task

1. The first window will ask you to enter the name of the task you are about to define. You have the possibility to *Disable* the task (meaning that the task will not run at the scheduled time), or to *Add to Scheduler Tray icon menu (*adding it to the system tray icon menu*).* Checking the *Close all windows* box and entering a *Hotkey* will create the perfect "Anti-Surprise (Anti-Boss or Panic) Key 23".

For example:
Define a task that A) runs the Privacy Guard feature, then B) check the Close all window box, and C) define a hotkey.
Now you can surf at will, without the fear of the discovery if intruded. By simply using your newly created Panic Key all windows will close and the Privacy Guard will begin to run, eliminating traces of your activity.

2. The second window allows you to schedule the previously named task. The task can run daily, weekly, monthly, once, at startup, at logon or when idle. For each of these options the start time and specific details can be defined.

For example:

You can schedule the program to run every 5 days, every two weeks, on Tuesdays, the third Friday in July and August, etc.

3. The 'What to Erase' window gives allows you to actually define the actions the new task will perform. You can choose to delete files or folders using the *Erase Files* feature, destroy the content of folders monitoring your computer and Internet activity by using the *Privacy Guard* feature, or ensure that the sensitive content of previously "deleted" files is actually erased, using the *Erase Deleted Data* feature.

4.Before completing your task specifications, you are allowed to set the required options to execute the task according to your needs. You have access to the Erase Options and Automation Options.

4.2.1.3 Anti-Boss (Panic) Key

The Anti-Surprise (Anti-Boss or Panic) Key, helps you hide what you are doing by just using a combination of keys from your keyboard. This allows you to close all open windows and immediately run East-Tec Eraser 2013 with preselected options (e.g. erase your Internet traces in stealth mode) with just a combination of keys.

All you have to do is define a new task. Select a name for your task, check the *Close all windows* box and define your hotkey (the desired key combination). Proceed to specify what your task will do, and create it.
Now you can continue your activities feeling safe, because in case of emergency all you have to do is press the defined Panic Key, and all open windows will close, while Eraser starts with the specified task, eliminating all traces of your previous acitivty.

4.2.1.4 How to choose what to erase

The What to Erase panel offers three categories of actions to ensure the security of your computer.

1. Erase Files

Use this option to delete specific files and/or folders. Please see Erase Files 8 for more information.

2. Privacy Guard

Use this option to destroy data from Windows (swap/paging file, Recent/Run/Find lists) or Internet activity (cookies, history, pictures, etc.) that has been placed on your computer without your knowledge or permission.   Please see Privacy Guard 9 for more information.

3. Erase Deleted Data

Use this option to erase the contents of previously "deleted data", ensuring that sensitive information is not recoverable. Go to Erase Deleted Data 11 for more information.

4.2.1.5 Task Settings

East-Tec Eraser 2013 allows you to customize task options.

You can choose between the **Erase Options:**

- Actions
- Confirmations
- Vista Shadow Copies
- Policies
- Preferences
- Security Level
- Import/Export

and the Automation Options**,**

which together, allow you to be in control of every aspect of the task to be performed.

4.2.2 Vista Shadow Copies

4.2.2.1 Overview

About the Vista Shadow Copies

Shadow Copy is a useful innovation of the Windows Vista operating system to help the users protect their data in case they have not backed up their files or in case of accidental deletions. This feature automatically creates point-in-time copies of files as you work, allowing you to restore previous versions of the files/folders you have accidentally deleted or modified.

To restore a previous version of a certain file, right click the file and select "Restore previous versions". This allows you to go back in time, see all previous versions of that file and restore the version you need in the original directory or any other location from the computer. This also works for an entire folder. When restoring an entire previous version of a folder, users can browse the folder hierarchy as it was in a previous point in time.

For more information about the Vista Shadow Copy feature, please refer to the Microsoft website at

http://www.microsoft.com/windows/products/windowsvista/features/details/shadowcopy.mspx

Privacy issues regarding Shadow Copies

By default, Windows Vista stores previous versions (also called shadow copies) of all your files, for backup purposes. For your private files, you may not want this to happen, because someone could discover these previous versions. If you are concerned about your privacy, use East-Tec Eraser when you want to get rid of your private files.

Now, what's happening if the Shadow Copy feature was enabled on the disk drive where you erase files from? The result is that previous copies of those files may still be available on your disk and anyone may retrieve them easily.

Erasing shadow copies in East-Tec Eraser 2013

When erasing files with East-Tec Eraser 2013, just before starting the erasure process, you will be informed if the files you are going to erase have previous versions stored in Shadow Copies. If yes, you will have to confirm if you want to erase the entire Volume Shadow Copies that contain that file. It is recommended that you select to erase the shadow copies.

Note:
- Because erasing shadow copies of individual files is not possible in Vista, the entire Volume Shadow Copies that contain them must be erased. This may erase copies of other files you don't want to erase, but the original files are left intact.

Private files you create from now on, may have previous versions on your computer. You can exclude certain files and/or folders from this process. To do this, use the Volume Shadow Copy Manager by going to the Tools menu -> Volume Shadow Copy Manager. The user also has the ability to manage (delete and explore) all Volume Shadow Copies from his system. For more information, please click here 25.

4.2.2.2 The Vista Shadow Copy Manager Window

Use the Shadow Copy Manager to manage (delete or explore) the Volume Shadow Copies or to exclude different paths from the shadow copies:

1. Manage Volume Shadow Copies

By default, Windows Vista keeps previous versions (shadow copies) of your files for backup purposes. You can explore the Volume Shadow Copies to see which of them contain copies of your private files and delete them.

2. Exclude from Volume Shadow Copies

You can define a list of files and/or file masks that you want to be excluded from shadow copies. These can be private files or data for which you don't want to have shadow copies created.

You may add your own files and/or folders to be excluded. Wildcards (*) are also accepted to define any group of characters in the path. For more information about path definitions, click here.

Click here to read more about Vista Shadow Copies... 24

4.2.3 Risk Monitor

4.2.3.1 Overview

Risk Monitor is a useful feature which monitors all wiping actions run by East-Tec Eraser 2013 on your system.

In case you did not use a certain feature for a long time, it informs you that you are at risk and there is a chance your data may be recovered. All you need to do is use the 'Fix' button that will automatically start the wiping process related to that risk, and you will be sure that you system is protected by East-Tec Eraser 2013.

You can also choose the number of days you want to be alerted about risks, from the Settings dialog box. This applies only to risks related to Erase Deleted Data, Recycle Bin and Privacy Guard.

See also:

Risks you are protected against 26
Risk Monitor settings 27

4.2.3.2 Risks

The Risk Monitor is protecting you against the following risks:

Privacy Guard
If you did not wipe Internet tracks, application data, Windows system files or other Windows sensitive information that your system stores without your knowledge or approval for a long time, this means that you are at risk, because anyone can recover this information. In this case, you will be notified to run Privacy Guard.

Erase Deleted Data
If you did not wipe your previously "deleted" files for a long time, this means that you are at risk because this information can be easily recovered. You will be notified about this and recommended to run Erase Deleted Data.

Recycle Bin
If you did not erase files from the Recycle Bin for a long time, you be notified that you are at risk and you can choose to destroy these files from the Recycle Bin for good.

Get New Upgrades
The system will notify you that you are at risk because you don't have the latest updates for Privacy Guard applications (sensitive areas) and it will prompt you to download the latest files.

Restart Later
This may happen in the following situation: you run Privacy Guard, but the program needs to restart the system to finalize the wiping process. If you don't restart the system to finish erasing the protected files beyond recovery, someone may recover your files.

Using a Trial Version
If you are using a trial version, Risk Monitor alerts you about this and how you can get the full version.

Buy with Special Offer
Sometimes we offer special prices to buy the full version and you are informed about this opportunity. This is available only in the trial version.

Subscription about to expire
This is displayed when your upgrade subscription is about to expire. After the subscription expires, you will no longer receive free updates and upgrades.

Subscription has expired
This is displayed when your upgrade subscription has expired. To continue to receive free updates and upgrades, you will have to renew your subscription.

4.2.3.3 Settings

You have the following options/settings for Risk Monitor:

Notify me to run Erase Deleted Data every X days
If this option is checked, you will be notified if you haven't run the Erase Deleted Data feature for X days.

Notify me to securely empty Recycle Bin every X days
If this option is checked, you will be notified if you haven't securely emptied the Recycle Bin for X days.

Notify me to run Privacy Guard every X days
If this option is checked, you will be notified if you haven't run the Privacy Guard feature for X days.

Check for updates every X days
If this option is checked, the program will check if there are new versions, every X days. If there is a new version, you will be informed how to obtain it.

4.3 Running in Stealth Mode

The Stealth mode setting will allow the erasure process to proceed in the background, undetectable and transparently. The Progress Indicator (which displays the erasure status) will not appear, however other additional windows and messages may be displayed (and possibly compromise your intention to execute the task covertly).

You may enhance the Stealth process by making a few additional modifications.

From the Erase > Erase Options menu please access:

Confirmations, and uncheck "Confirm once for all files", "Confirm for each individual file" and "Confirm before wiping free space". This will ensure that no confirmation windows are displayed (requiring user interaction).

Next, access:

Automation.

In the first section of this screen make sure you do not select: "Show Restart dialog". Any other option in this section will be acceptable not expose the erasure task.

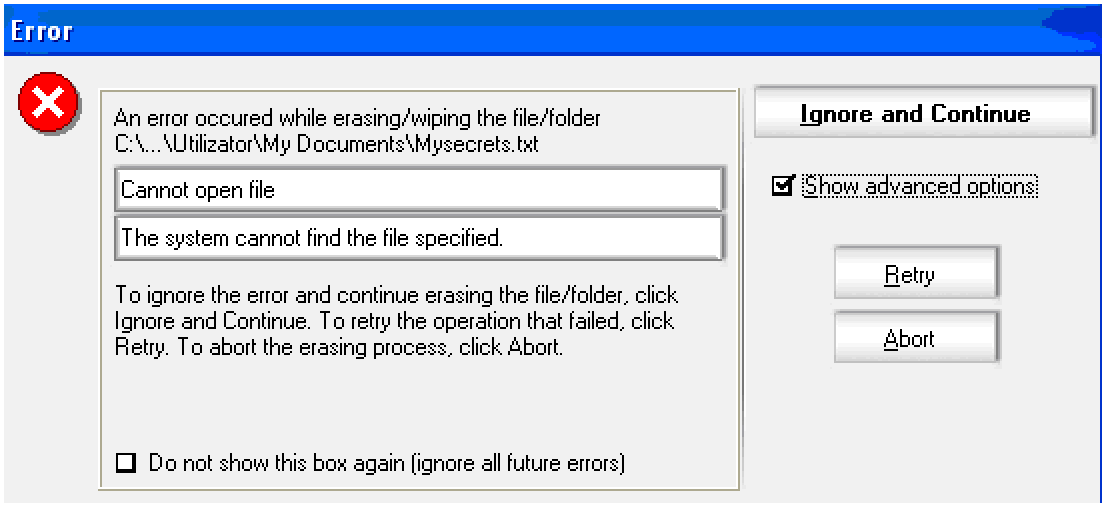
In the second section, any selection is acceptable; however "Don't shut down, just close the progress box" is not applicable because the "progress box" (Progress Indicator) has been disabled by your activation of the Stealth mode setting.

4.4 Error Handling and Logging

4.4.1 Handling errors

Eraser verifies the result of each disk read/write operation and it is able to inform you if any errors occur.

When an error occurs, the following dialog box is displayed (click any control to get more information):



An error occured while erasing/wiping the file/folder C:\...\Utilizator\My Documents\Mysecrets.txt

Cannot open file

The system cannot find the file specified.

To ignore the error and continue erasing the file/folder, click Ignore and Continue. To retry the operation that failed, click Retry. To abort the erasing process, click Abort.

☐ Do not show this box again (ignore all future errors)

You may also instruct Eraser to ignore all errors by selecting the appropriate settings in the Preferences page of the Erase Options dialog box.

4.4.2 Using a log file

A useful feature offered by Eraser is the possibility of maintaining a log file. A log file records all the erasing/wiping operations, the date and time when they started, and the erasing/wiping settings. Any errors that occur are also logged.

Note: File slack wiping operations are not logged in detail (for performance reasons).

Use the Preferences page of the Erase Options dialog box to specify a log file and other logging settings.

Note: You have the option to see the log file directly from the program by using the 'View Log File...' button and to erase it after you have analyzed it by using the 'Clear Log File' option.

4.5 Miscellaneous

4.5.1 Password protection

Eraser is an advanced erasing utility containing features that used improperly could damage your data. An entry password can restrict unauthorized users from accessing it. Eraser will prompt for the entry password each time it is run. If you forget your password, you will have to re-install the program.

Use the Password page of the Configuration dialog box to specify an entry password.

4.5.2 Command-line parameters

You may run Eraser from the command line prompt. This feature allows you to automatically erase sensitive data from BAT files or from scheduling software.

Erasing files and folders from the command-line

Use the following syntax:

```
ETERASER item1 [item2 …] [erase options] [/K]
```

Item1, item2, …
The files and/or folders to be erased. You will be prompted for confirmation before erasing them according to the current options.

You can use wildcards (e.g. *.tmp, *.bak). Include a '-' character before the file specifications if you want to look for files only in the specified folder and not in its subfolders. By default, Eraser looks for files in the specified folder and in all its subfolders. If you want to erase a larger number of files, use the **/A<textfile>** option. Textfile must be a text file that contains on separate lines the names of the files you want to erase.

erase options
See the erase options below.

/K
(The 'killer' mode) Erase all the files/folders from the command-line, WITHOUT asking any additional confirmation. Be careful to run the utility this way!

Running Privacy Guard from the command-line

Use the following syntax:

ETERASER actions [erase options] [/K]

Actions:

/P[S]
Run the Privacy Guard feature and specify which erase actions to perform.
S - scramble files and folders properties

erase options
See the erase options section below.

/K
(The 'killer' mode) The Privacy Guard will erase all sensitive files WITHOUT asking any additional confirmation.

Running Erase Deleted Data from the command-line

Use the following syntax:

ETERASER actions [erase options]

Actions:

/G
Run the Erase Deleted Data feature with the default options currently selected in the program interface.

/G[R][FSP=<drive(s)>]
Run the Erase Deleted Data feature and specify which erase actions to perform.
R - destroy the files from the Recycle Bin
F - wipe the disk free space on <drive(s)>
S - wipe the slack portion of all files on <drive(s)>
P - scramble files and folders properties on <drive(s)> (note: this option only works together with F)

erase options
See the erase options section below.

Setting erasing options from the command-line

The erase/wipe actions will be performed using the current options (wiping with the current wipe method, erasing using the current erase options, etc.). The current options may be changed in the Erase Options dialog box. You may also change a few options using the following command-line parameters:

/W
Automatically restart Windows to erase "locked" files (files that cannot be accessed while Windows is running).

/L
Schedule "locked" files to be erased the next time Windows is started, but do not automatically restart Windows (restart later).

/U
Do not schedule "locked" files (files in use by Windows that cannot be accessed) to be erased the next time Windows is started (just skip them and continue).

/I
Ignore all errors encountered while performing the actions specified in the command-line.

/M<methodID>
Use a specific wipe method to perform the actions specified in the command-line. MethodID can be 1 (the first wipe method as it appears in the wipe method list), 2 (the second), and so on.

/B
Enable batch mode. Use it when you want Eraser to automatically perform erase actions from batch files, scheduled with SystemAgent. When batch mode is enabled, the progress dialog box will automatically close after each erase action, so Eraser can automatically start the next erase action. In the end, after completing all the actions specified in the command-line, Eraser will automatically close.

/H
Enable minimized mode. Use it to automatically minimize the Progress dialog box. Use with /B (batch mode), /W (automatically restart Windows to erase "locked" files), /K (killer mode) and /I (ignore all errors) to get an automatic erase mode that will not display any windows and that will automatically close Eraser after completing all the actions. For a more powerful hidden mode (invisible mode) see the /V parameter below.

/V
Enable invisible mode. Eraser will run in the background, completely invisible to the user (no main window, no dialog boxes, not visible in the taskbar, etc.). Use with /B (batch mode), /W (automatically restart Windows to erase "locked" files), /K (killer mode) and /I (ignore all errors) to get an automatic erase mode that will be completely invisible and that will automatically close Eraser after completing all the actions.

/S
Scramble files and folders properties. Use this option to remove any file attribute that may reveal the identity of the erased files and folders (name, data, size ...). It may slow down the erase process, especially on larger hard drives containing large amounts of information (files/folders), but this is the only method that ensures that the files and folders properties are properly destroyed and cannot be recovered.

Additional command-line options

Use the **/NC** (no configuration) command-line parameter to prevent Eraser from loading the settings saved in previous sessions and use the default settings. You can use this parameter both in interactive and command-line mode.

Use the **/KV** (kill invisible mode) command-line parameter to kill any stealth mode (invisible mode) process that is currently running in the background (or it is scheduled to run after reboot). If any stealth mode process is detected it will be killed and a message will confirm that the stealth mode wiping process was killed.

Examples

```
> ETERASER c:\*.tmp c:\*.bak /B
```
This will collect the temporary and backup files from drive C and then will start to erase them. You will be prompted for confirmation before erasing them according to the current options. After erasing the files, Eraser will automatically close.

```
> ETERASER –c:\*.zip /K
```
This will collect all the zip archives from the c:folder (but not from its subfolders). The files will be erased without asking any additional confirmation (the 'killer' mode). After completing the erasing process, Eraser will remain open.

```
> ETERASER /P /K /B /W
```
This will run the Privacy Guard feature without any additional confirmation and without requiring your intervention. When the Privacy Guard completes, Eraser will restart your computer to erase the files that were "locked" by Windows or by other running software.

```
> ETERASER /GF=CD
```
This will wipe the disk free space on drives C and D. After completing the wiping process, Eraser will remain open.

```
> ETERASER /GR
```
This will destroy the files from the Recycle Bin. After completing the erasing process, Eraser will remain open.

```
> ETERASER c:\*.tmp /K /GFS=C /I /B
```
This will collect all the temporary files from drive C and will erase them without asking any additional confirmation (the 'killer' mode). Then Eraser will wipe the free space on drive C and the slack of all files from drive C. Any error that occurs will be ignored and the wiping process will continue (the /I option). Because Eraser will run in batch mode (the /B option), these erase actions will be performed without interruption and without requiring your intervention. After erasing the files, Eraser will automatically close.

4.5.3 Protecting your Restore Points

System Restore is a component of Windows that you can use to restore your computer to a previous state, if a problem occurs, without losing your personal data files (such as Microsoft Word documents, browsing history, drawings, favorites, or e-mail). System Restore monitors changes to the system and some application files, and it automatically creates easily identified Restore Points. These Restore Points allow you to revert the system to a previous time. They are created daily and at the time of significant system events (such as when an application or driver is installed).

As Microsoft also documents, Windows automatically removes the Restore Points from your computer when the free space falls below 50 MB on any drives. As a consequence, because some wiping operations (such as the scrambling of file properties - name, date, size, etc.; or the wiping of the free disk space) result in the temporary reduction of the free disk space to zero bytes, the Restore Points will be removed from your system.

Eraser can help you protect your Restore Points from being deleted by Windows in the situations described above. All you have to do is make sure you select *Protect my Restore Points* from the Options dialog box, the Preferences tab.

5 Support

5.1 Getting More Help

EAST-TEC is committed to providing customers with high quality support and assistance. If you encounter a problem, or have a question, or need any other help with our products and solutions, here are a few ways to get an answer or find a solution:

- Consult the product documentation (this help file and/or any other documentation items that come with the product).

- Visit the East-Tec Eraser 2013 Online Area at http://www.east-tec.com/consumer/eraser/index.htm for updated documentation and other information resources.

- Some problems may be solved by updating to the latest version of East-Tec Eraser 2013. Visit EAST-TEC Online at http://www.east-tec.com for more information.

- Visit our online support area at http://www.east-tec.com/support to contact our support team online or learn more about our range of support services (online, e-mail, phone, fax).

- For a fast, efficient and free answer to any of your technical queries and problems, use the EAST-TEC E-Mail Support Service by writing to http://www.east-tec.com/support The support team is available 24 hours a day, 7 days a week and you should expect an answer in less than 24 hours.

Note: To provide the answers you need quickly and efficiently, the EAST-TEC support staff needs some information about your computer and your software. Please include the following information when you request support: program name and version number, computer brand and model, any additional hardware or peripherals connected to your computer, operating system type and version numbers, network information, relevant browsers or applications and their version numbers (where applicable). Please also include information on how to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions.

5.2 More Information and Feedback

To get more information on new product releases and new developments and to make sure you are using the latest and most advanced solutions available, please visit EAST-TEC Online at http://www.east-tec.com.

How to Send Suggestions

EAST-TEC welcomes your comments and suggestions.

We really need your help to learn how to serve you better. Let us know how we can improve our products, solutions and support. Please visit http://www.east-tec.com/support and use the Interactive Support Center to send us your comments and suggestions.

5.3 Acknowledgments

Some of the graphical interface elements in the product are used with the permission of VistaICO.com. Their website address is http://www.vistaico.com/

5.4 Contacting EAST-TEC

Please visit our Interactive Support Center at:
http://www.east-tec.com/support

World Wide Web
http://www.east-tec.com

Send correspondence to:

EAST-TEC European Offices
Str. Balogh Istvan Nr.17
Oradea 410238
Romania
European Union