

WIN1038

February 2007

How to Securely Delete Electronic Information in Windows

Author: Deanna Pasternak

Introduction	1
Why Should I Securely Erase?	1
Who Should Securely Erase Hard Drives?	2
Methods of Securely Erasing Files	2
Things to know before you securely erase	2
Applications to erase files and folders	2
Shredding files and folders with Eraser	2
Other options in Eraser	7
Securely erasing the entire hard drive using DBAN	14
Error Messages and Problems	15
More Information	15
Getting Help	16

Introduction

This document explains the importance of securely deleting electronic information, using the tools Eraser and DBAN. Eraser is an application that can be used to ensure the files that you "delete" are actually destroyed. DBAN is a one-time use tool to ensure your hard drive is wiped clean before you dispose of it.

Although ITS recommends securely erasing/deleting sensitive information and has tested the software (Eraser version 5.8 on Windows XP and DBAN version 1.0.7), you are advised to use them with caution and at your own discretion as ITS will not be liable for any damage caused by the use of Erase or DBAN. You should backup your files before using this software, as well as be sure that the files being erased should be permanently removed.

This is not software that is supported on-site by ITS, but this document was written as an aide for those that require secure deletion.

Why Should I Securely Erase?

When you delete a file or folder using the "Recycle Bin" or "Trash" on your computer, the file is not actually deleted from the hard drive. Using the "Recycle Bin" or "Trash" is just like using a trashcan at your house. Someone can pick up the piece of paper out of the trash and retrieve your confidential information. A program that securely erases a file is analogous to paper shredder so that the information is destroyed. Until you write over the area on the hard drive where the file is located, it can be easily retrieved with an undelete utility.

There are many reasons people would use a program like Eraser, one of the most common would be the user of a laptop that travels often and has an increased chance of the laptop being stolen. You would use DBAN if you want to give your computer away, dispose of, or donate it. There are links to both of the software downloads in the sections below.

Any individual that doesn't want their data to be viewed by someone else should securely erase their hard drives before disposing of or giving their computer to another person or department. This procedure is especially important for those who maintain and store sensitive information on their hard drives (e.g. social security numbers, dates of birth, credit card numbers).

Methods of Securely Erasing Files

There are different ways of ensuring that your data cannot be recovered from a hard drive. The ways range from various types of software to physically destroying the drive. There are also ways that you can securely erase information off of other devices such as PDA's or cell phones. More information on these can be found at <u>http://www.wirelessrecycling.com/home/data_eraser/default.asp</u>.

This document will focus on using the software tool Eraser to routinely erase (or shred) your files, and the software tool DBAN for when you want to erase everything on a hard drive.

Things to know before you securely erase

The most important thing to realize is that once you erase your files, they are gone. **There is nothing that ITS can do to help you retrieve your document or folder.** If you are giving away your computer and want to keep your files, you should back up the files to another location before you begin and verify that this backup works. You may also want to create a file that you don't need to save, to practice erasing it before you erase one of your actual documents.

Applications to erase files and folders

There are many different applications that you can install to securely erase your files and folders in Windows. Some of them are freeware, and others you can purchase for a fee. This document covers the application Eraser that can be downloaded for free at <u>http://www.heidi.ie/eraser/download.php</u>. The current version of the application, Eraser 5.82, works on Windows 95, 98, ME, NT 4.0, 2000 and XP. It is not currently supported for Windows Vista.

Shredding files and folders with Eraser

Installing Eraser

- 1. Download the installer from <u>http://www.heidi.ie/eraser/download.php</u>.
- 2. Locate and double-click on the installer to begin installation.
- 3. Follow the on-screen instructions.
- 4. Once you reach the last screen that asks you if you want to restart your computer, you will need to close all open programs and restart the computer for the software to work properly.

Using Eraser

After your computer is rebooted, you will have a new menu option when you right-click on a file or folder. The image below shows that now you have options to **Erase** or **Erase Secure Move** your documents.

Open	
Edit	
New	
Print	
Erase	
Eraser Secure M	love
Scan for Viruses	
Open With	
Send To	•
Cut	
Сору	
Create Shortcut	
Delete	
Rename	
Properties	

When you choose to **Erase** a file or folder using this menu, you will see a prompt similar to the one below asking you to confirm your decision. Clicking the **Yes** button will erase the file, making it unrecoverable.



You will also notice an **Options** button on this screen. If you click this button it will open up the following screen.

#	Description	Passes	New
1	Gutmann	35	
2	US DoD 5220.22-M (8-306. / E, C and E)	7	Edit
3	US DoD 5220.22-M (8-306. / E)	3	-
4	Pseudorandom Data	1	Delete
5			
Select verwr IZ C IZ F	sted: Gutmann (35 passes) ite iluster Tip Area ile Names (File Names will always be cleared on NT	/XP and above)	

When you securely erase a file or folder, Eraser overwrites your file with random data. The more overwrite passes, the more securely your data is deleted. However, the more times you write over an area, the longer it will take. Passing over an area three times, which is the US DoD 5220.22-M (8-306. /E) standard, should be sufficient for deleting confidential information. The default is the Gutmann erase, which uses 35 passes, making it take a considerable amount of time.

Once you decide how many times you wish to overwrite the file or folder and select **Yes** to delete the file, the file or folder is now gone; it does not go to the "Recycle Bin."

Clicking on **Erase Secure Move** will move your file to a new location on your hard drive and securely erase the source location. When you click **Erase Secure Move**, you will see the following screen, which will allow you to browse for the location to move the file.

Browse For Folder	? 🛛
Select target folder	
Desktop	^
E 🛅 My Documents	
🚵 🤐 Adobe	
😬 My Pictures	
🗄 🥅 SnagIt Catalog	
B S My Network Places	~
n Li Mu Documento	
Folder:	<u> </u>
Make New Folder OK	Cancel

Once you choose the location and click **OK**, you will then get the following box to confirm the move.

Confirm	n Secure Move		X
\square	Are you sure you want to move 'C:\ to 'C:\Documents and Settings\De	\Desktop\New B anna Pasternak\My	itmap Image.bmp' Documents'?
Opti	ons	Yes	No

Clicking **Yes** here will move the file to the chosen location, and the source location will be erased. This would be most useful when moving data to another hard disk or to external media.

If you want to securely empty items that are already in your "Recycle Bin," you can right click on it to reveal the **Erase Recycle Bin** option. Once it is done erasing you will see a status window similar to the one below, verifying the erase is complete.

Erasing Report		×
Task completed.		
Information:		
Statistics: Erased area Cluster tips Data written Write time Write speed	= 520 kB = 6144 bytes = 18200 kB = 16.06 s = 1133 kB/s	×
Failures: # Item		
	Save As	Close

Other options in Eraser

Erase has a number of other options. If you go to Start > Programs > Eraser and open the Eraser program you will see the following screen:

Eraser [On-	Demand]				
File Edit Task	View Help				
	× 8 №				
Eraser	🗅 Name	Size	Туре	Modified	Attributes
On-Demand					
Scheduler					
Explorer					
For Help, press F1					0 Items

This screen gives you the ability to securely erase all the free space on your hard drive, and also to schedule the program to automatically erase the free space or certain areas on your hard drive.

To erase the free space on your hard drive, click on File > New Task. You should now see this window.

Task Properties	
Data Schedule	
Unused space on drive	
Second Disk (C:)	•
C Files on folder	
Subfolders Remove folder(s) Gelu subfolders	
C File	
I Use wildcards	
When finished	
None	
OK Cancel	Help

You can either select the unused space on a specified drive, or specific files and folders (such as your temp directory). If you choose to erase the unused space on your drive, files will not actually be touched unless they have previously been deleted. You can also choose to have it do nothing, reboot your computer, or shut it down when it is complete. Make sure you have the correct drive selected, as you cannot retrieve anything that is erased from the specified space.

Note: Eraser does not support erasing unused space on network drives.

You will see it cycle through you files; do not be alarmed, your files are not being deleted. Eraser is just searching the areas around them for empty space.

Erasing:	Unused disk space Cluster Tips	
ltem: Pass:	C:\\HP\Digital Imaging\bin\en\hpqpanos.resource	s.dll
		32%
Total:		
		8%

You can also securely erase the free space on your hard drive by right clicking on your C:\ drive in the "My Computer" window. The process is the same except that the first screen is the one below.



Once it is finished erasing your free space, you will see an erasing report. Any reported failures that you see could be a file that is in use or being locked by another program. It is best to close all programs or files when erasing the free space on your drive.

ntormation:		
Statistics: Erased area Cluster tips	= 31738 MB = 63415 kB	^
Data written Write time Write speed	= 31738 MB = 4679.65 s = 6945 kB/s	2
<	2	
Failures:		
# Item		~
1 Failed: C:\5f071c05 2 Failed: C:\Documen 3 Failed: C:\Documen 4 Failed: C:\Documen	8edd0b504504d37ad0df0fe8\msxml4-KB92 ts and Settings\All Users\Application Data\ ts and Settings\All Users\Application Data\ ts and Settings\All Users\Application Data\	
5 Failed: C:\Documen	ts and Settings\All Users\Application Data\	× .

The **Schedule** tab gives you the ability to schedule your task to happen at a later time.

Task Propert	ies	×
Data Sched	dule	
Schedule tasi	k to be processed	
Every	Day 💌	
At	12:00 FM	
	OK Cancel	Help

If you schedule Eraser to run on your C:\ drive every Monday at 12:00PM, your scheduler window would look similar to the window below:

Eraser [Sch	eduler]					
File Edit Task	View Help					
	► × ? N	?				
Eraser	🗋 Name	Туре	Last Run	Next Run	🖗 Schedule	
	Sec:\	Local Disk		2/26/2007 12	Every Monday	
onDeilland						
20						
Scheduler						
Explorer						
For Help, press F1	11	L.		ES.	1	1 Task

The last feature that Eraser offers is the ability to Erase Verify. If you go to Start > Programs > Eraser > Eraser Verify you will see this screen.

Eraser:	Verify 🛛 🔀
믔	This program uses the Eraser library to securely overwrite a file using the predefined settings. After each overwriting pass, you are shown the contents of the file so you can verify that the operation was successful.
	0. Select the overwriting method you want to use.
	1. Select the file you want to erase. Browse
	2. Start overwriting by pressing "Erase". Erase
	3. Follow the overwriting process.
	Close

You can select the file you want to erase and choose **Erase**. After each overwrite pass, you will see a log of how the file looks after that pass of the shredder. In the example below you can see how the file structure becomes more unreadable the more times it is written over.

File Before Shred

: (Docu Ixplore)luster)000:)010:)020: 1030:	ments and ar 7 DRAFT : 0 (4096) 205B2525 73694420	1.log (138) bytes, off 646F7250	bytes) set: 0 byt	cernak (Des	KCO]	p\Getting Started w	ith Internet
luster 000: 010: 020: 030:	: 0 (4096) 205B2525 73694420	bytes, off 646 F 7250	set: 0 byt	10000 L 4			
luster 000: 010: 020: 030:	0 (4096 . 205B2525 73694420	bytes, off 646F7250	set: 0 byt	100001-000			
000: 010: 020: 030:	205B2525 73694420	646 F 7250		es):			
010: 020: 030:	73694420		4E746375	3A656D61	-	%%[.ProductName:	
020:		6C6C6974	5D207265	0A0D2525	:	.Distiller.]%%	
030:	505B2525	3A656761	255D3120	250A0D25		%%[Page:.1]%%%	
	61505B25	203A6567	25255D32	25250A0D	-	%[Page:.2]%%%%	
040:	6761505B	33203A65	0D25255D	5B25250A	:	[Page:.3]%%%%[
050:	65676150	5D34203A	0A0D2525	505B2525	:	Page:.4]%%%%[P	
060:	3A656761	255D3520	250A0D25	61505B25	:	age:.5]%%%%[Pa	
070:	203A6567	25255D36	25250A0D	73614C5B	-	ge:.6]%%%%[Las	
:080	67615074	25255D65	00000A0D	00000000	1	tPage]%%	

File after one pass of shredder

C:\Doc	ruments and	l Settings\	Deanna Pas	ternak\Des]	stoj	p\Getting Started with	^
Intern	het Explore	r 7 DRAFT1	.log (4096	bytes)			
Juste	er U (4096	bytes, orr	set: U byt	es):			
010.	00000000	00000000	00000000	000000000			
020-	00000000	000000000	00000000	000000000			
020.	00000000	00000000	00000000	000000000	3		
040-	00000000	00000000	00000000	00000000			
050-	00000000	000000000	000000000	000000000	-		
060-	00000000	000000000	00000000	000000000	÷.		
070-	00000000	00000000	00000000	000000000	3		
0.80-	00000000	000000000	000000000	000000000	-		
000.	00000000	000000000	00000000	000000000	-		
030-	00000000	000000000	00000000	000000000	0		
ORO-	00000000	000000000	00000000	000000000	3		
000.	00000000	000000000	000000000	000000000	-		
0000.	00000000	000000000	000000000	000000000	1		
OFO-	00000000	000000000	00000000	00000000	2		
OFO-	000000000	000000000	00000000	000000000	3		
100-	00000000	00000000	000000000	000000000	-		
1110-	00000000	000000000	000000000	000000000			
120-	00000000	00000000	00000000	00000000	2		
130:	00000000	00000000	00000000	00000000	- 3		
140:	00000000	00000000	00000000	00000000			
150:	00000000	00000000	00000000	00000000	- 2		
160:	00000000	00000000	00000000	00000000	- 2		
170:	00000000	00000000	00000000	00000000	- 2		
180:	00000000	00000000	00000000	00000000	-		
190:	00000000	00000000	00000000	00000000	- 2		
1A0:	00000000	00000000	00000000	00000000		1999 1999 1997 1997 1997 1997 1997 1997	~

File after two passes of shredder

:\Doc	uments and	Settings\	Deanna Pas	ternak\Desl	ktop\Getting Started with 🦻 🦻
Intern	et Explore	r 7 DRAFT1	.log (4096	bytes)	
Cluste	r O (4096	bytes, off	set: 0 byt	es):	
0000:	FCI5396B	IDSUE2B7	12#45005	KA331D33	: K9P
0010:	KB6B44AZ	BDZIA965	C790DDB3	BA327BAB	: .Jk.e.!
0020:	48211EA6	A7C948Z3	D99D2118	0739D639	:!H#H!9.9.
0030:	F009517C	724F19FF	D1C6A4B9	ZF84B1BA	: 10/
0040:	BAB8FA42	FF334FAE	EAOA5FD9	E1710DEF	: BQ3q.
0050:	5485ZZ3B	394A9A71	D990K791	B49BCF5F	: ;".Tq.J9
0060:	D580EA47	793B7FFF	8AFB4F1B	9ZA77559	: G;y.OYu
0070:	OD7B2B12	2127A7CA	21B0255B	C7C81806	: .+{'![%.!
0080:	012BB508	6B69D91A	01ED5A82	E9948336	:+ik.Z6
0090:	766B4149	00AC1A20	84DB085A	18099C32	: IAkv22
)0A0:	E4822A05	A0773F8F	A49B2327	E873003D	: .*?w.'#=.s.
DOBO:	ED1B3BE1	53B3AD94	FCB62533	246691C2	: .;\$3%f\$
DOC0:	B5A67A33	SEBDFE3D	FOCB2F05	C07389C4	: 3z=/s.
DODO:	F9837FE6	D1BEE7D9	7DB8C7D5	D2A31EA6	:
DOE0:	1B024300	9301C56 E	B9841300	F3D5D14E	: .CnN
DOFO:	73C6936E	EEDB1F7D	F90B8FF4	6688A63A	: ns}f
0100:	SCC56D1D	053A61F1	67E4EEC8	66BAFA87	: .m.\.a:gf
0110:	60FE29F5	790B0AD5	OB06F3D1	01FAC153	: .).`yS
0120:	2B21ED30	61E15BE9	332594FF	3620A00E	: 0.!+.[.a%36
0130:	6155F134	D6BB3D80	EOACE475	9AE08411	: 4.Va.=u
0140:	CFEC081A	C4A25BBD	F26F0949	21BEF4C8	:[I.o!
0150:	93FC08E3	26FF6843	BC4E4BE5	C5438100	:Ch.&.KNC.
0160:	8BF43B25	644F030F	50F5C3C1	FB916A3F	: %;OdP?j
0170:	D5967679	A1C1FFE4	500B1155	A134403F	: yvUP?@4.
0180:	9C2FF2FF	6BC37391	7CED81AB	7FC9DD2B	:/s.k +
0190:	22D57973	0582CF95	85D9AED8	20614434	: sy."4Da.
01A0:	5B6EF227	6CD3B799	C344F099	97E6BF65	: '.n[1D.e 🔉

File Shredder is Complete

	This program uses the Eraser library to securely overwrite a file using the predefined settings. After each overwriting pass, you are shown the contents of the file so you c verify that the operation was successful.
	0. Select the overwriting method you want to use.
	1. Select the file you want to erase. Browse
	2. Start overwriting by pressing "Erase".
	3. Follow the overwriting process. Stop Erasing completed.

Securely erasing the entire hard drive using DBAN

DBAN is a program that will erase your entire hard drive when you wish to dispose of it. When you install the Eraser program, it also installs the most recent version of a program that you can use to create a DBAN floppy disk or USB drive.

You can find it by going to Start > Programs > Eraser > Create Nuke Boot disk. If you do not wish to use Eraser to run DBAN, you can download this software for free at <u>http://dban.sourceforge.net/</u>. If you download the executable from this web site, you should choose "Save As" and save the executable to your computer.

Creating a DBAN image

If you create the Nuke Boot disk from either Eraser or by double-clicking on the DBAN executable, you will see the following screen.

WinImage Self Extractor	
Install DBAN to this floppy disk or USB flash device:	About WinImage
Darik's Boot and Nuke (dban-1.0.7_i386) http://www.dban.org/ README.TXT Contents 	

You can install the image on either a floppy disk or a USB flash device. Creating this image will erase all information on your floppy or USB device.

Once you install the image on the floppy or USB device, you will need to reboot your computer. It would also be a good idea to remove any external storage drives to ensure those do not get erased accidentally. The computer will boot off of the device that contains the image and it will boot up to a blue screen at a **boot:** prompt. You will have the following options.

Press the F2 key to learn more about DBAN. This will give you information on what kinds of media can and cannot be wiped with DBAN.

Press the **F3** key for a list of quick commands. This screen will give you the list of commands you can type in. You can also change the method of wipe that DBAN users. By default it will use the short DoD 5220.22-M method (recommended).

Press the **F4** key for troubleshooting hints.

Press **ENTER** key to start DBAN in interactive mode.

Type in **autonuke** at this prompt to start DBAN in automatic mode (recommended). **WARNING:** When you type in **autonuke** and hit enter, DBAN will begin to erase your drive, and anything on it will be unrecoverable. Even if you attempt to stop this process by rebooting, your data could be permanently destroyed. This process can take a considerable amount of time, depending on the size of your hard drive.

Error Messages and Problems

If you cannot get DBAN to install on either a floppy disk or a USB drive, you may contact the ITS Help Desk for "best effort" assistance.

If you install the DBAN image on a USB drive, and the computer boots straight into Windows, you should make sure that your computer BIOS is set to enable your computer to boot from a USB device. Most computer manufacturers have different settings and ways of entering the BIOS. You may need to contact your computer's manufacturer for instructions on how to access the BIOS, or to find the proper settings.

More Information

For more information on securely erasing your hard drive:

ITS kb article on Securely Deleting Electronic Information

http://www.hawaii.edu/askus/706

Eraser Quick Start Guide

https://www.heidi.ie/eraser/quickstart.php You may need to copy and paste this link in your browser

DBAN Readme File

http://DBAN.sourceforge.net/download/readme.txt

Getting Help

Click on the **Help** link (usually in the upper right hand corner of the window) for on-line help. There is extensive on-line help available. Please refer to this on-line help first for any questions not answered by this document.

For additional assistance, please phone the ITS Help Desk at (808) 956-8883, send e-mail to **help@hawaii.edu**, or fax (808) 956-2108. The Help Desk's toll-free phone number is (800) 558-2669.

```
Or visit the ITS Help Desk home page at http://www.hawaii.edu/help
```

The ITS Help Desk functions are located in Keller 105, Keller 213, ITS Hamilton Lab (2nd Floor Addition) and CLIC Lab (Sinclair Lib, 1st Floor) on the UH Mānoa Campus.

The University of Hawai'i is an equal opportunity/affirmative action institution.