

# MediaWiper User Manual

1. Introduction.....	2
2. System Requirements.....	2
3. Getting Started with MediaWiper.....	2
a. Installing / Uninstalling MediaWiper.....	2
b. Launching MediaWiper.....	2
4. Wipe Media.....	3
a. Select a Drive to be Wiped.....	4
b. Select Drive Format.....	4
1. FAT.....	4
2. NTFS.....	4
c. Select Drive Label.....	4
d. Select Security Level.....	4
1. 1 Overwrite.....	5
2. 3 Overwrite.....	5
3. 7 Overwrite.....	5
4. 12 Overwrite.....	5
e. Wipe Media Selection.....	5
5. Verify Media.....	6
a. Verify.....	6
b. Quick Verify.....	7
6. View Media Sectors.....	7
7. MediaWiper Tools.....	8
a. Configure Report Log.....	8
b. Check for Updates.....	9
8. Help File.....	9
a. Online Help.....	9
b. Help File.....	9
9. Department of Defense Standards.....	9
10. Similar Products.....	9
a. WipeDrive.....	9
b. SecureClean.....	9
11. More Help and Contact Information.....	10

## 1. Introduction-----

Simply deleting a file DOES NOT erase your data! Files can be recovered from your PC after they have been deleted. MediaWiper will completely erase all data on a selected drive rendering that data irretrievable. MediaWiper allows you to choose which drives you wish to wipe prior to reuse or disposal. In addition MediaWiper will reformat your drive so that new data can be saved to it.


## 2. System Requirements-----


Supported Operating Systems:

- Windows 98 SE
- Windows Me
- Windows 2000
- Windows XP

## 3. Getting Started with MediaWiper-----

### 3.a. Installing / Uninstalling MediaWiper

1. Browse to the MediaWiper CDROM and double click the “setup” icon  Follow the prompts. Upon installation, MediaWiper will create a folder which will include a Help file and Uninstall feature. During the installation process you will be prompted to browse to the directory where you wish the folder to be created in.

2. Once MediaWiper is installed, a shortcut will appear on the desktop with the icon 
3. To uninstall MediaWiper you must browse to the MediaWiper folder and click on the “Uninstall” option located in this folder. Follow the prompts.

### 3.b. Launching MediaWiper

When you first begin MediaWiper you will be prompted to register your software online.



This is an important step in using your software; registering MediaWiper will ensure your future eligibility for technical support and free version upgrades. This step takes only a few minutes. Click on “Register” to go to the WhiteCanyon registration page and fill out the short questionnaire.

Note: If you purchased MediaWiper directly from the WhiteCanyon website your software is already registered. If you have already registered your software, click on “Skip” to enter MediaWiper.

When you first enter, MediaWiper will automatically check for updates. If there is a new version available online, MediaWiper will offer to take you to the WhiteCanyon website where you can download the latest version. You can disable the automatic update check by clicking on “Tools” option in the upper left corner of the MediaWiper main menu screen and disabling this option.

Opening MediaWiper will bring up the main menu screen where you can choose to Wipe, Verify, or View the data on a disk:



## 4. Wipe Media-----

There are four steps you must perform prior to wiping a disk:

1. Select drive to be wiped
2. Select drive format
3. Select a drive label
4. Select a security level

#### 4.a. Selecting a Drive to be Wiped

Click on the down arrow of the drive list and select which drive you wish to wipe. MediaWiper will completely erase everything on that selected drive.

**Important:** *When you wipe a drive, all the information on it is gone forever! Make sure you have backed up your important files before you proceed.*

Once you have selected a drive, click “Next” to choose a drive format.

#### 4.b. Selecting a Drive Format

After performing a wipe, MediaWiper will reformat your drive for reuse. You can choose between two drive formats:

##### 4.b.1 FAT file system

FAT will work for all versions of Windows. If you are not sure which format to use, choose FAT. Always select FAT for removable media such as diskettes, zip disks, flash memory cards, etc.

##### 4.b.2. NTFS

Disks formatted with NTFS can only be accessed using Windows NT, 2000, or XP. Therefore, we recommend that you choose NTFS only if you are formatting a Windows NT, 2000, or XP hard drive.

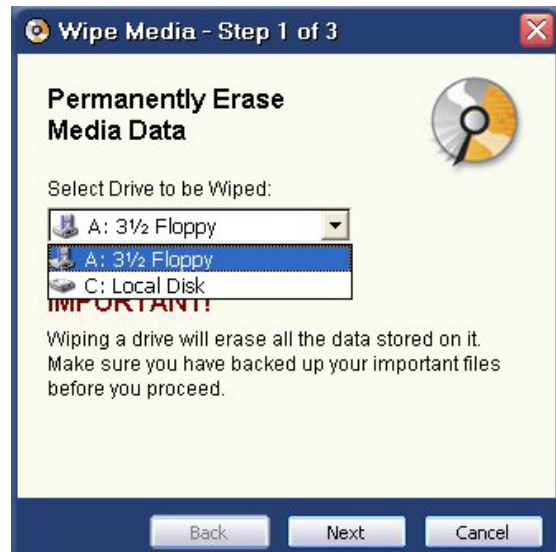
#### 4.c. Selecting a Drive Label

You can choose (up to eleven characters) how you want your drive to be labeled after it is wiped. This feature is optional. This label will be displayed by Windows in Windows File Explorer. The default setting is “CLEANED” and this is what the selected drive will be labeled as automatically if this label is not changed.

#### 4.d. Selecting a Security Level

The final step before wiping your media is choosing a security level. Click on the down arrow of the security level list to select the number of overwrites.

Drive data can be overwritten any number of times. Please note, however, that one overwrite is sufficient for most users. Overwriting data once will make it impossible for anyone to recover your data using a software recovery program.



Recovering data after one overwrite is a very expensive and highly technical operation that is not available to the general public. If you think that someone would go to extreme measures to attempt to recover your data, then you should consider one of the multiple overwrite options. However, please note that increasing the number of overwrites will also increase the time it takes to complete the operation, thus, option two (3 Overwrites [DoD Standard]) will take three times longer than option one (1 Overwrite).

#### 4.d.1. 1 Overwrite

This option is recommended for most users, as one overwrite is sufficient for rendering your data irretrievable using any conventional data recovery software.

#### 4.d.2. 3 Overwrites

This option will overwrite your data three times according to Department of Defense standards, *see* Department of Defense Standards *for more information*. If you think that someone would go to extreme measures to recover your data, you should consider using this option.

#### 4.d.3. 7 Overwrites

This option will overwrite your data seven times in accordance with VSITR standards.

#### 4.d.4. 12 Overwrites

This option will overwrite your data twelve times. Please note, this option will greatly increase the time it will take to overwrite a selected drive.

### 4.e. Wipe Media Selection

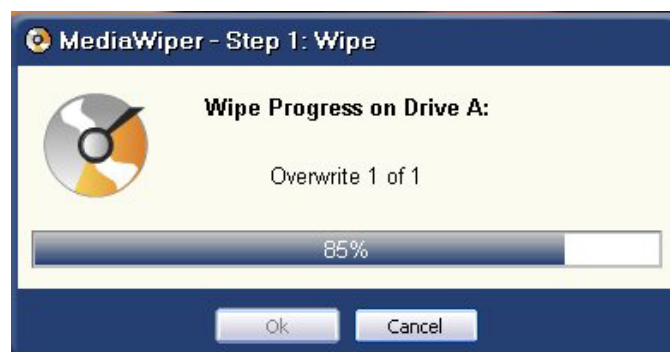
After clicking the “Wipe Media Selection” button, you will be asked twice to confirm that you really want to wipe the selected drive. This is simply extra security, since once you perform a wipe all of the information on your drive will be irretrievable. Select “Yes” to continue the wipe.

Wiping a drive involves 2 steps:

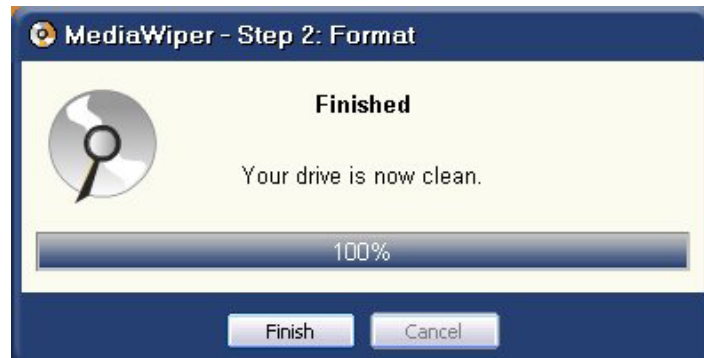
1. Wiping the disk
2. Reformatting the drive

Note: A DoD level wipe (3 Overwrites) involves an additional step: verification.

You may cancel a wipe while it is in progress. However, you will not be able to recover your files intact once the process has begun. If you cancel a wipe, you may still need to reformat your drive before you can use it again.



Once MediaWiper is finished wiping and formatting your drive, click on “Finish” to return to the main menu window.



*Note: MediaWiper cannot erase a drive containing the Windows Operating System. Windows will not allow another program to overwrite it while it is running. To erase your Operating System drive, you will need WipeDrive. For more information on WipeDrive, see Similar Products.*

## 5. Verify Media-----

After you have successfully wiped and reformatted a drive, you may choose to verify that all of the information has indeed been erased.

From the MediaWiper main menu select “Verify Media”. Click the down arrow of the Drive Selection list to choose the drive that you just wiped.

*Note: Drive must be reformatted in order for MediaWiper to perform a verification.*



MediaWiper offers you two verification methods: Verify and Quick Verify.

### 5.a. Verify

This option will check each sector on your drive to see that it has been successfully wiped. Because this option will verify every sector on your drive, it may take a long time depending on the size of your drive.

### 5.b. Quick Verify

“Quick Verify” will spot check your drive for dirty sectors. This option is much quicker than “Verify” because it checks random sectors from the beginning of the drive to the end.

As MediaWiper verifies your drive, the progress will be displayed in the progress bar and in the text under the progress bar.



1. **Drive Status:** The Drive Status will read “Clean” until it detects a dirty sector at which point the Drive Status will read “Uncleaned Sectors Detected”.
2. **Report:** “Report” keeps track of what percent of the drive is not cleaned. When a drive is verified as clean, the Report will read as 0.
3. **Drive Errors:** A drive error occurs when MediaWiper is unable to wipe a section of the drive. If MediaWiper detects any drive errors, the number of errors will be displayed here. If a drive error is detected, it may be useful to attempt another wipe of the drive. However, if the drive is damaged, MediaWiper may not be able to fully wipe that drive. Bad sectors can appear on disks, especially on diskettes. If a sector is bad, it generally means it cannot be written to or read from, thus it results as a drive error. If your disk has a large number of bad sectors on it, you may not want to trust it for future use.
4. **Dirty Sectors:** If MediaWiper finds any dirty sectors during a verification, the number of dirty sectors found will be displayed here. When a drive is verified as clean, “Dirty Sectors” will read as 0.
5. **Drive Type:** MediaWiper automatically formats a drive after a wipe for reuse. You may choose between FAT file system or NTFS file system, prior wiping a drive. See *Wipe Media / Choosing a Drive Format*
6. **Drive Size:**
7. **Drive Label:** The default label setting for a wiped drive is “Cleaned”. You may change this label prior to wiping the drive. See *Wipe Media / Labeling a drive*.
8. **Cluster Size:**

## 6. View Media Sectors-----

Viewing the sectors of a drive is an advanced feature of MediaWiper. If you are not familiar with how data is stored on a drive, this feature may not be very useful to you. However, the more advanced user can use this feature to browse the sectors of a disk.

NOTE: When looking at the individual clusters of a formatted wiped drive, you will notice that the sector view will display quite a bit of data in various sectors. This data is not user data, it is the contents of the drive format and must be in place in order to save files to the disk. MediaWiper can understand this data and test it to make sure that no user data exists in it.

When you select a sector to be viewed, it is displayed in three columns:

Offset	Hexadecimal Representation	Text Equivalent
0x0000:	f0ff ff03 4000 0560 - 0007 8000 09a0 000b	.....@...`.....
0x0010:	c000 0de0 000f 0001 - 1120 0113 4001 1560	..... ..@..`
0x0020:	0117 8001 19a0 011b - c001 1de0 011f 0002	.....
0x0030:	2120 0223 4002 2560 - 0227 8002 29a0 022b	!. #@. % ` ' . . ) . . +
0x0040:	c002 2de0 022f 0003 - 3120 0333 4003 3560	..-./..1 .3@.5`
0x0050:	0337 8003 39a0 033b - c003 3de0 033f 0004	.7..9..;..=..?..
0x0060:	4120 0443 4004 4560 - 0447 8004 49a0 044b	A .C@.E`.G..I..K
0x0070:	c004 4de0 044f 0005 - 5120 0553 4005 5560	..M..O..Q .S@.U`
0x0080:	0557 8005 59a0 055b - c005 5de0 055f 0006	.W..Y..[.]._..
0x0090:	6120 0663 4006 6560 - 0667 8006 69a0 066b	a .c@.e`.g..i..k
0x00A0:	c006 6de0 066f 0007 - 7120 0773 4007 7560	..m..o..q .s@.u`
0x00B0:	0777 8007 79a0 077b - c007 7de0 077f 0008	.w..y..{.}. .@..
0x00C0:	8120 0883 4008 8560 - 0887 8008 89a0 088b	.....@...`.....
0x00D0:	c008 8de0 088f 0009 - 9120 0993 4009 9560	..... ..@..`

The first column, labeled “Offset”, contains the count of bytes displayed up to that point.

The second column, labeled “Hexadecimal Representation”, contains 16 bytes from the sector displayed in hexadecimal. Each byte is represented by two digits or letters, and two bytes are always grouped together.

The third column, labeled “Text Equivalent”, contains the same 16 bytes displayed as normal characters. Since not every byte on the drive can be translated into a character, anything that can not be translated is replaced by a period.

The above image is that of a dirty sector. This is what the same sector looks like after it has been wiped by MediaWiper:

Offset	Hexadecimal Representation	Text Equivalent
0x0000:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0010:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0020:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0030:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0040:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0050:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0060:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0070:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0080:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x0090:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x00A0:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x00B0:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x00C0:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....
0x00D0:	0000 0000 0000 0000 - 0000 0000 0000 0000	.....

## 7. MediaWiper Tools-----



### 7.a. Configure Report Log

The report log is a text file that contains a brief report created by the wipe or verify operation. Each successive operation’s report is appended to this file. You can select to disable this feature or view the Report Log by clicking the “Configure Report Log” button.

To view or change the MediaWiper Report Log settings, click on “Configure Report Log”. MediaWiper will automatically save your log report in the MediaWiper file but you may change this location by browsing to a new location.

The Report Log will record the time and date that the wipe was performed as well as the number of overwrites performed and the number of disk errors found, if any.

## **7.b. Check for Updates**

An internet connection is required to check for updates. To check for updates, click on "Tools" in the upper left corner of the MediaWiper main menu and choose "Check for Updates". If there is a new version of MediaWiper available, you will be given the option of connecting to the WhiteCanyon website where you can download the new version.

You can have MediaWiper automatically check for updates once a week. To enable this feature, select the "Enable automat checking for updates" under "Tools".

## **8. Help File-----**

The MediaWiper Help option located at the top of the main menu window provides you with two options:

### **8.a. Online Help**

This is a good place to start. The "Online Help" option will take you to the WhiteCanyon web site where there is a list of Frequently Asked Questions (FAQs).

### **8.b. Help File**

This option will provide you with a detailed explanation of all the features of MediaWiper.

## **9. Department of Defense Standards-----**

The following information is provided for official government use. All government contractors and employees must abide by these set regulations.

WipeDrive can be used to sanitize electronic media, containing non-top secret information, according to the Department of Defense 5220.22-M standard as quoted:

1. "Non-Removable Rigid Disks" or hard drives must be sanitized for reuse by "Overwriting all addressable locations with a character, its complement, then a random character and verify."
2. Removable media such as diskettes should be destroyed. "Destroyed - Disintegrate, incinerate, pulverize, shred, or smelt."

For more details, please refer to the Department of Defense 5220.22-M standard.

## **10. Similar Products-----**

### **10.a. WipeDrive**

Don't give away your personal information with your old PC. Over the past five years, one in four households was victimized by identity theft. If you do not erase your personal information before selling or donating your computer, your personal identity or company trade secrets could be stolen and used against you.

Deleting a file, partitioning a disk, or formatting a hard drive will not erase your data. By using WipeDrive, you can securely overwrite and remove ALL of your information. WipeDrive will wipe everything stored on a hard disk, including partition tables, all file data, boot record information, etc.

### **10.b. SecureClean**

Your files are not erased by Windows when you delete them. SecureClean erases your previously deleted files by overwriting their contents. SecureClean does this while your operating system is running and does not disturb your current files.

Windows often stores unneeded traces of your personal information, including passwords, credit card numbers, and previously deleted data and email, all without you even knowing it. SecureClean isolates and removes this unneeded information, making it impossible for cyber criminals to steal your data. Don't just rely on your firewall to protect you, make SecureClean your second line of defense.

## **11. More Help and Contact Information-----**

### **Email Support**

For more information please email:

[info@WhiteCanyon.com](mailto:info@WhiteCanyon.com) or [support@WhiteCanyon.com](mailto:support@WhiteCanyon.com)

You may visit us online at [www.WhiteCanyon.com](http://www.WhiteCanyon.com)