Acronis DriveCleanser
User's Guide

END-USER LICENSE AGREEMENT

BY ACCEPTING, YOU (ORIGINAL PURCHASER) INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT WISH TO ACCEPT THE PRODUCT UNDER THESE TERMS, YOU CAN CHOOSE NOT TO ACCEPT BY SELECTING "I decline..." AND NOT INSTALLING THE SOFTWARE.

 The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1. The license is to the original purchaser only, and is not transferable without prior written permission from Acronis.
2. The original purchaser can use the software on a single computer. You cannot use the software on more than one machine, even if you own or lease all of them, without the written consent of Acronis.
3. The original purchaser cannot engage in, nor permit third parties to engage in, any of the following:

A. Providing or permitting use of by, or transferring the software to, third parties.

B. Providing use of the software in a computer service business, network, timesharing or multiple user arrangement to users who are not individually licensed by Acronis.

C. Making alterations or copies of any kind in the software (except as specifically permitted above).

D. Attempting to unassemble, decompile or reverse-engineer the software in any way.

E. Granting sublicenses, leases or other rights in the software to others.

F. Making copies, or verbal or media translations, of the users guide.

G. Making telecommunication data transmission of the software.

Acronis has the right to terminate this license if there is a violation of its terms or default by the original purchaser. Upon termination for any reason, all copies of the software must be immediately returned to Acronis, and the original purchaser shall be liable to Acronis for any and all damages suffered as a result of the violation or default.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. ACRONIS DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES

IN NO EVENT SHALL ACRONIS OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ACRONIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

Introduction

About Acronis DriveCleanser

Getting rid of an old PC, upgrading to a new hard drive, returning a leased computer, or redeploying a PC within your company? It is truly imperative to completely destroy all data from the old hard disk.

Acronis DriveCleanser guarantees the complete destruction of data on selected partitions and/or entire disks with extremely simple Windows XP-style interface and straight forward actions.

Confidential information on hard disks: storage and access

Today more and more amount of confidential information is created in the digital form and consigned to stored on computers. Documents that were previously created with the help of printing machines or table database files are now stored on computer hard disk drives.

The enormous amount of personal data, including such important things as personal banking account information, credit card numbers, business application, data-banking, financial, accounting, and industrial – are all stored on hard disks. It is impossible to enumerate all documents and data that in no circumstances should not left behind on a hard disk drive for criminals or rivals to possibly retrieve.

The main feature of these documents is that all of them contain **confidential information**.

Confidential information: destruction

However, information not only has to be **stored** according to specially developed rules, but also be destroyed according to the strict rules to provide confidentiality.

Computers are usually upgraded more than once during their lifetimes. In doing so, very often the computer disk subsystem is upgraded first due to the ever increasing amounts of data stored on the hard disk drive. When a hard disk of larger capacity is installed on the computer, all data from the old disk can be transferred to the new one, but quite often the data also remains on the old disk.

Careless storage of a hard disk that is no longer needed can result in the loss of confidential information. The best solution is to completely **destroy** data on the old disk after it is moved to the new disk. Destroy! Not to erase information, not to delete needless files, but to destroy confidential data! (The difference between file deleting and information destruction will be explained later.)

The following real-life passage illustrations this idea:

Jack V., a computer consultant from Brighton, bought a used notebook computer for $400.00 at the clearance sale of a bankrupt Internet company. It was clear that the hard disk drive contained data about the Internet. This data included social security numbers and salary levels of the company's forty-six employees, plus pay-roll records, strategic company plans, confidential board of directors minutes, and other internal documents.

There have been many cases like this concerning the sales and purchase of used computer.

Data deletion with the means of an operating systems

There is a considerable difference between file deletion with operating systems (with the help of file managers) and data destruction with the help of specialized erasing programs.

The point is that operating systems, such as Windows, do not materially delete anything from a hard disk when **deleting a file**: the name of the deleted file in the File Allocation Table (FAT) is substituted by the name which is not assumed as a correct one by the operating system. The file only becomes invisible for a user and the cluster chain that contains file data is considered to be free. But the information contained within the hard disk sectors stays permanent. It is not very difficult for someone to recover it.

File deletion under the Linux operating system is somewhat more reliable, but even in this case it is possible to obtain software tools to recover any important information.

Neither **partitions deletion** on a disk nor even disk **formatting** solves this problem. When partitions are deleted on a hard disk the information of Partition table (if it is a primary partition) or File Allocation Table are deleted. The information contained within sectors however remains untouched and can be recovered with the help of software tools.

Reliable information destruction on hard disks is possible only while using specially designed programs that implement specially designed erasing algorithms.

Guaranteed destruction of confidential information: standards

The Acronis DriveCleanser application offers the guaranteed destruction of confidential information on hard magnetic disks with the help of special algorithms.

Acronis DriveCleanser algorithms guarantee compliance with most known national standards:

(1) American: U.S. Standard, DoD 5220.22-M;

(2) American: NAVSO P-5239-26 (RLL);

(3) American: NAVSO P-5239-26 (MFM);

(4) German: VSITR;

(5) Russian: GOST P50739-95.

Besides algorithms corresponding to national standards, Acronis DriveCleanser supports predefined algorithms proposed by well-known and authoritative specialists in the field of information security:

(6) Peter Gutmann algorithm – data on hard disk is destroyed with 35 passes;

(7) Bruce Schneier algorithm – data is destroyed with 7 passes.

The Acronis DriveCleanser also supports simple but fast algorithms for information destruction that provide a single hard disk pass with all sectors zeroed.

The major feature of the Acronis DriveCleanser Deluxe version is the opportunity for you to create your own algorithms for **data destruction**.

Detailed information on data destruction standards is given in **Appendix A.** «**Hard Disk Wiping algorithms**» to the current Guide.

Software usage conditions

The conditions for Acronis DriveCleanser software usage are described in the «License agreement», included with this package. The supplied registration card is the confirmation of your legal purchase and usage of Acronis DriveCleanser on your system. Each registration card has its own unique registration number.

Under current legislation the «License agreement» is considered a contract between a user (you) and a software manufacturer (Acronis, Inc.). The contract has legal effect and its violation may entail a court examination.

Illegal use and/or distribution of this software will be prosecuted.

Technical support

Users who have legally purchased and registered their copy of Acronis Disk Director Suite will receive free technical support from Acronis. If you have installation or working problems that you can't solve by yourself using this manual and the readme.txt file, e-mail the technical support team. You will need to provide the serial number of your Acronis Disk Director Suite copy bundled with the program.

Before you do this, you will have to register your copy at:

http://www.acronis.com/homecomputing/my/products/registration/ .

Support URL: http://www.acronis.com/homecomputing/my/support/

Chapter 1. Installing Acronis DriveCleanser and Getting Started

1.1 Acronis DriveCleanser system package

Acronis DriveCleanser system package includes:

- An installation CD,
- This guide,
- License agreement,
- Registration card,
- Advertising materials.

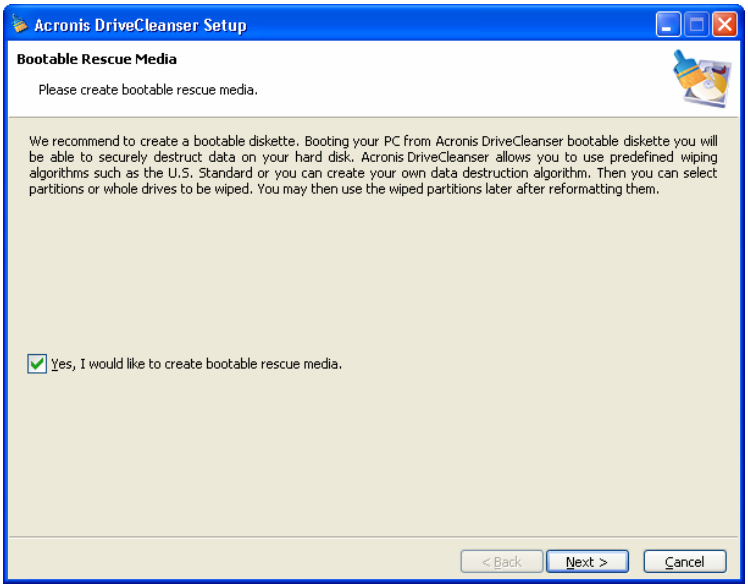
1.2 Installation

To install the Acronis DriveCleanser:

1. Insert the Acronis DriveCleanser installation CD into CD-ROM drive and start the installation procedure.

2. Carefully follow the installation program instructions on the screen.

3. After making your installation choices and copying of Acronis DriveCleanser files onto your hard disk, you will be offered to create a **bootable diskette or CD-R/W** (you may omit this step if you have purchased the boxed product that contains a bootable CD). While DriveCleanser works in Windows, you can also wipe a hard disk with Linux or other PC operating system. If you are not running Windows, you should create bootable media, and re-boot your PC from it, to start a wiping.



After installation of Acronis DriveCleanser is completed, you should restart your computer.

1.3 Repairing/Upgrading Acronis DriveCleanser

In order to upgrade or repair your software, start the DriveCleanser installation program again. It will determine that DriveCleanser was already installed on your computer and will ask you if you want to restore (update) the program or completely remove it from disk.

1.4 Removing the software

To remove the software select **Acronis → DriveCleanser → Uninstall Acronis DriveCleanser** from the Programs menu. You will see a dialog box asking if you really want to remove the software from your PC hard disk. Press `Yes` to confirm removal. Acronis DriveCleanser software will be completely removed.

1.5 User interface

Acronis DriveCleanser software has a Windows-like Wizard-driven graphical user interface and is controlled by the mouse or by `Tab`, `Shift+Tab`, `Left`, `Right`, `Up` , `Down`, `Space`, `Enter` and `Escape` keys.

If you regularly work with Windows, X Window or OS/2 applications, you should not encounter any problems with the Acronis DriveCleanser interface.

While working with Acronis DriveCleanser software, a user deals with a sequence of **dialogs**, in which he/she selects one further action, of several

possible, by setting switches to the necessary position or choosing a value from a list, or marking the necessary partitions or disks for work.

The necessary position (or condition) of the switch is **selected** (or set) with a mouse click or by pressing keys.

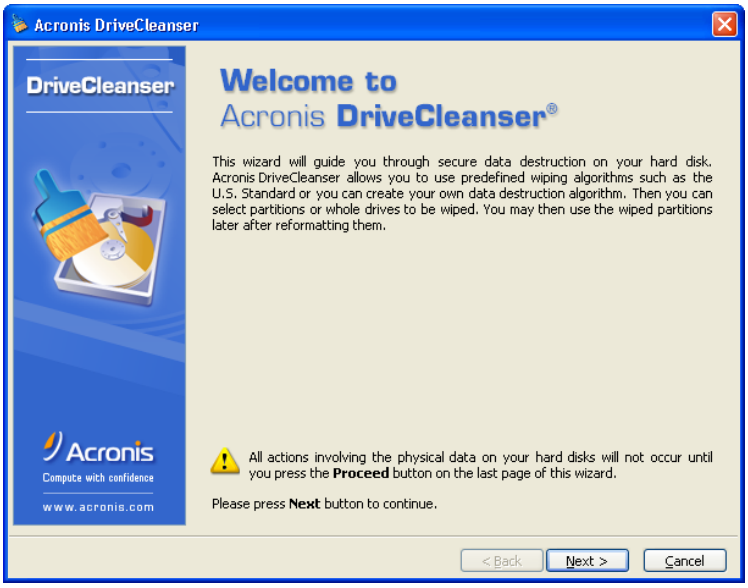
Each dialog contains detailed text comments describing its purpose and the purpose of a list (or switch) located on it. There are also text comments for each element of the list (possible switch conditions).

There is no Help button on Wizard pages. It is unnecessary because on each page there is detailed information about the purpose of the page and its controls. Moreover, there is detailed information about what possibilities you get if you select any of controls in any possible state.

Chapter 2. Wiping Hard Disks with Acronis DriveCleanser

Working with Acronis DriveCleanser starts with the welcome screen. The screen informs you about the basic features of the software; they are:

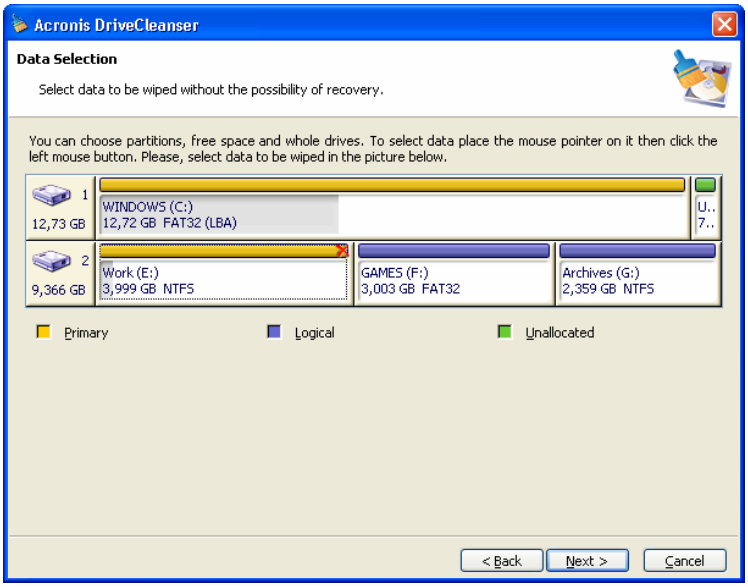
1. Wiping selected partitions of a hard disk (disks) with one of the predefined wiping algorithms;
2. Creating and using custom wiping algorithms.



The Acronis DriveCleanser welcome window

All actions on hard disks are performed on the basis of **scripts** created during the dialogue with the user. No data destruction occurs, until you execute the created script. You may return to a previous stage of script creation, from any stage of working with the software, and select other partitions and/or disks to wipe or to change the wiping algorithm.

The following window will contain the list of hard disks connected to your computer, and their partitions with main parameters (disk capacities and partition sizes, file systems and labels).



The list of computer's hard disks (with partitions)

Next you will need to select the partitions on hard disks to be designated for data destruction.

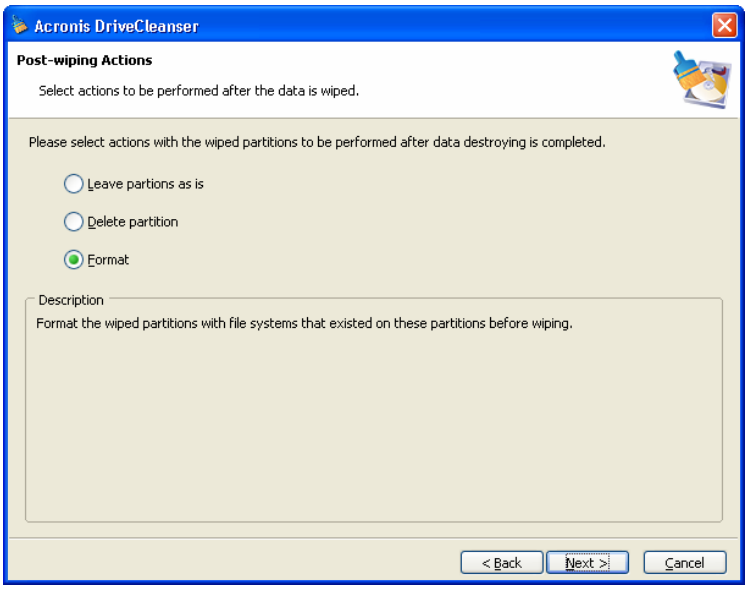
Mouse-click the rectangle representing the hard disk partition. The red cross will appear in the top right corner of the rectangle. It means that the partition is selected for data destruction.

You may choose to destroy data on the entire disk (or several disks). For this purpose mouse-click the rectangle representing the hard disk (with device icon, disk number and its capacity).

You may simultaneously select several partitions located on different disks, or several disks.

In the **Post-wiping actions** window you may choose what to do with partition that is the subject of data destruction. Acronis DriveCleanser offers you three opportunities:

- **Leave partition as is** – that is just to destroy data according to the algorithm which you will select later;
- **Delete partition** – to destroy data and remove partition;
- **Format** – to destroy data and format partition (default).

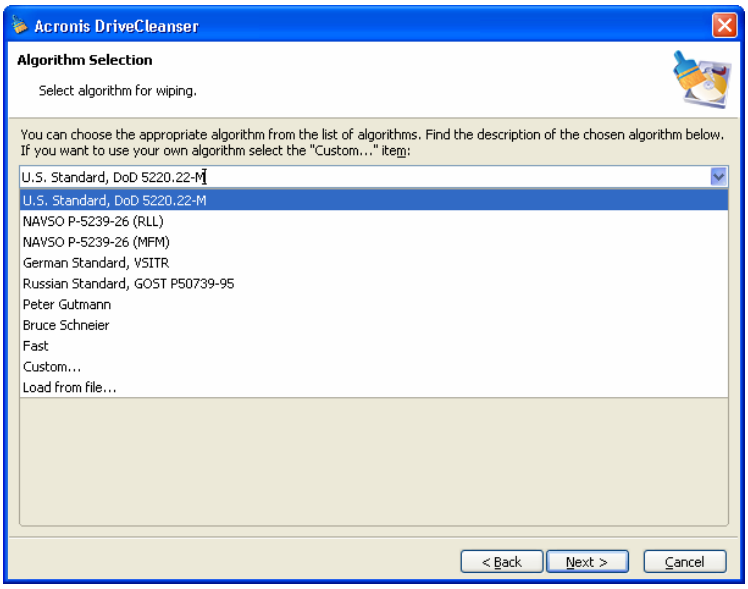


The Post-wiping actions window

In the example below it is supposed that the switch is set to the **Leave partitions as is** position. This will allow you to see the results of the data destruction itself (without partition formatting or removal).

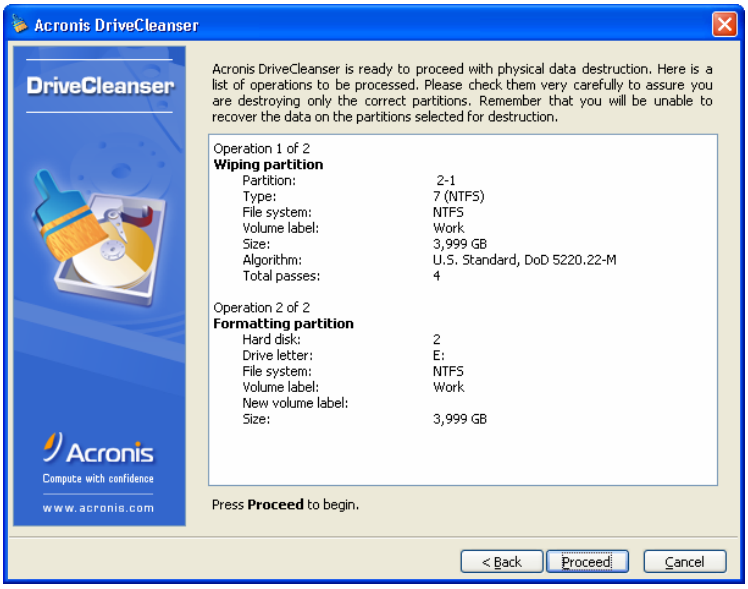
2.1 Using predefined wiping algorithms

Now you need to select one of the predefined wiping algorithms from the list in the Algorithm selection window.



The list of predefined wiping algorithms

The next window represents the created script for wiping the hard disk partitions.



The window of the hard disk wiping script

The Acronis DriveCleanser software is now ready to perform the wiping procedure.

Click the Proceed button to execute the script for wiping the hard disk partitions.

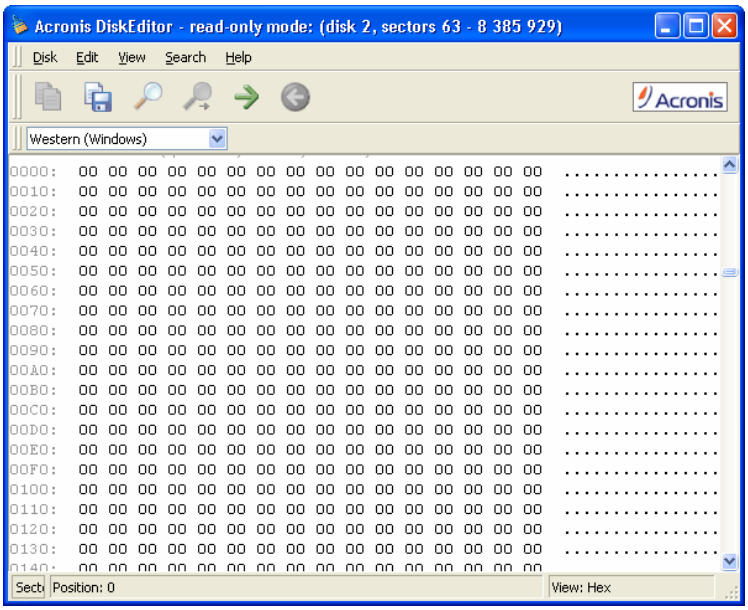
After pressing Proceed DriveCleanser takes care of everything automatically. To complete the execution of all processes, DriveCleanser will reboot your system after you have pressed the Proceed button.

Upon completion of the data destruction execution, you will receive a message reporting the successful completion of the disk wiping procedure.

The successful completion of the wiping procedure window

Acronis DriveCleanser software gives you another method to review the results of partition and/or hard disk wiping. Acronis DriveCleanser has a built-in DiskViewer utility for viewing the hard disk contents.

The algorithms described above offer different variants for data destruction. Thus, the picture you may see on a partition and/or a disk depends on the selected data destruction algorithm.



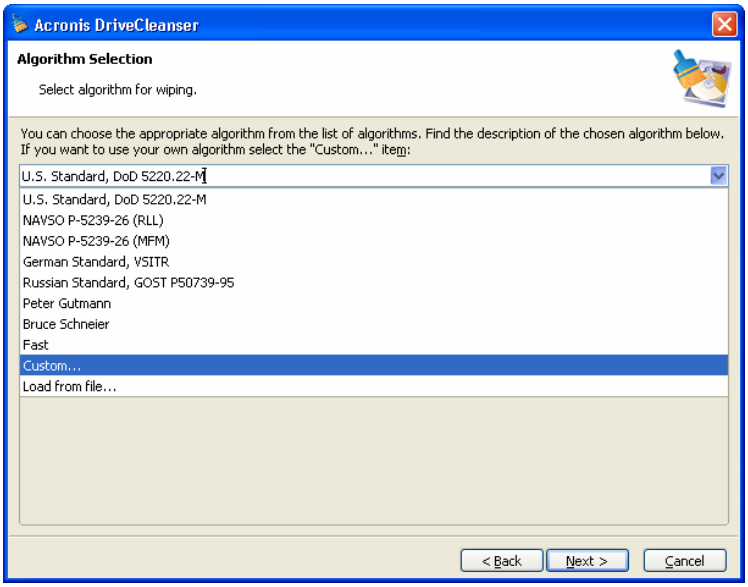
The sector of the disk partition after the fast algorithm execution

2.2 Creating custom algorithms of data destruction

Acronis DriveCleanser software gives you an opportunity to create your own algorithms for wiping hard disks. In spite of the fact that the software includes algorithms of all classes, you may choose your own algorithms.

2.2.1 Creating custom algorithms

To create a custom algorithm of hard disk wiping, select and mouse-click the «Custom...» line from the drop-down list in the **Algorithm selection** window. Please pay close attention to the load algorithm option in the same drop-down list.

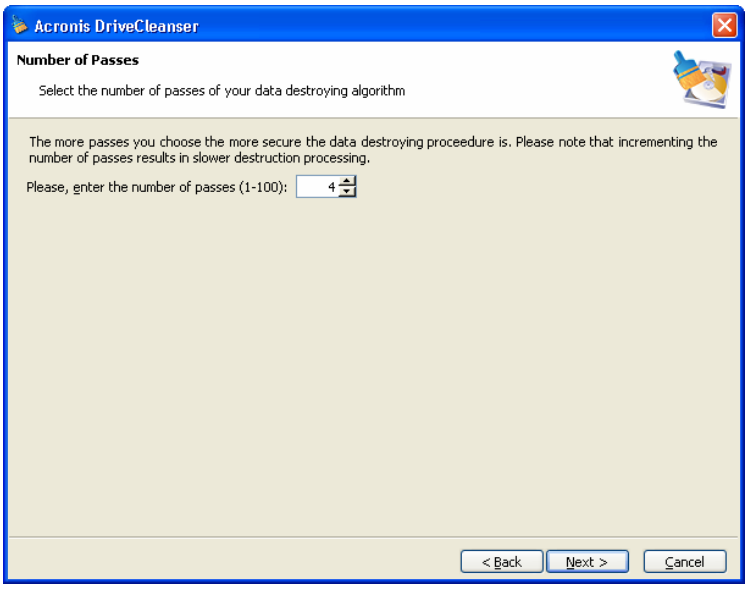


The selection of custom algorithm creation

Click the Next button to continue.

The window with the script for wiping a hard disk partition (partition and/or hard disk was selected on one of the previous steps) shows after the selection of one of the predefined wiping algorithms. This time the Custom algorithm wizard will be started and you will see the **Number of passes** window.

As an example let's create a simple custom algorithm similar to the American standard. As you may remember, the American standard assumes three passes for a hard disk during which different symbols are written to it, and one more pass for verification – i.e. 4 passes in total.



The window with number of passes of the custom algorithm

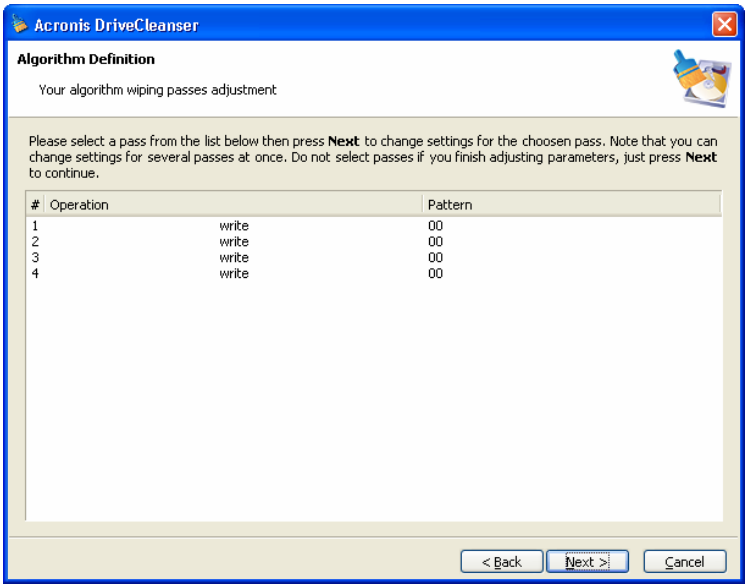
Let us remind you that the predefined wiping algorithms perform from 1 (fast algorithm, the Russian standard) up to 35 passes (Peter Gutmann algorithm).

You may enter any value into the spinner field of the Wizard window with keyboard or mouse. For our example enter 4 into this field.

Click the Next button to continue.

2.2.2 Algorithm definition: template

The **Algorithm definition** window shows you a template of the future algorithm: the list contains as many elements, including the defined algorithm at the previous stage.



The algorithm definition window

The window has the following legend: The first column of the list contains the number of passes for a disk; the second contains the type of operation on a disk (there are just two such operations: to write a symbol to disk, «writing», and to verify written, «verification»); the third column contains the pattern of data to be written to disk.

The pattern to be written to disk is always a hexadecimal value, for example, the value of this kind: 0x00, 0xAA, or 0xCD, etc. These values are 1 byte long, but they may be up to 512 bytes long. Except for such values you may enter a random hexadecimal value of any length (up to 512 bytes). Your algorithm may also include one more value for writing that is designated as the «complementary value» – the value that is complementary to the one written to disk during the previous pass.

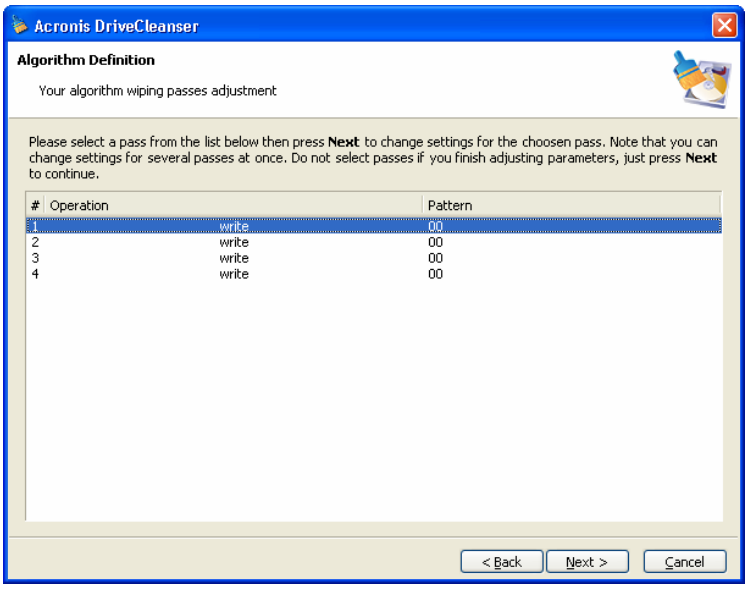
We shall remind that if the binary value is represented by 10001010 (0x8A) sequence then the complementary binary value will be represented by 01110101 (0x75) sequence.

Thus you may include the following values in algorithm:

- Any hexadecimal value 1 – 512 bytes long;
- Random hexadecimal values 1 – 512 bytes long;
- Hexadecimal values, complementary to those written to hard disk during the previous pass.

The **Algorithm definition** window offers you the template for the algorithm only. you should define what exactly the software should write to disk to destroy the confidential data according to your algorithm.

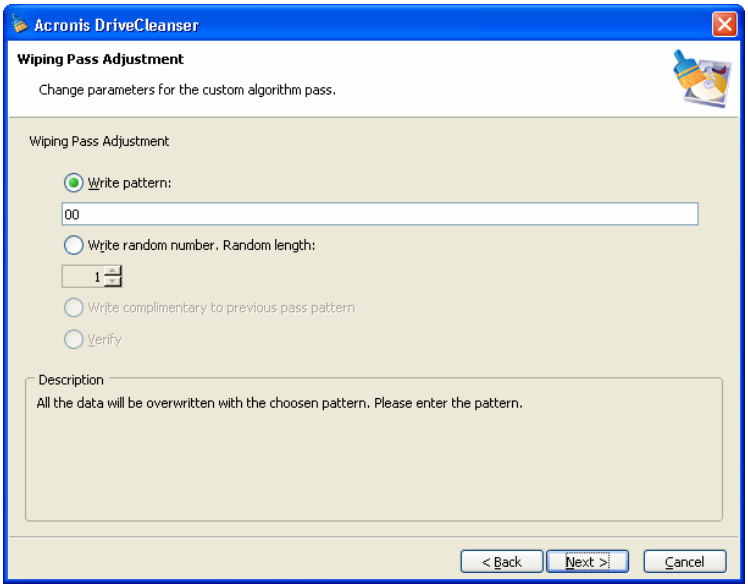
To do this, mouse-click the line representing pass #1.



The selection of the 1-st pass for pattern definition

Click the Next button to continue.

You will see the window that allows you to define the pattern to be written to disk (hexadecimal value).



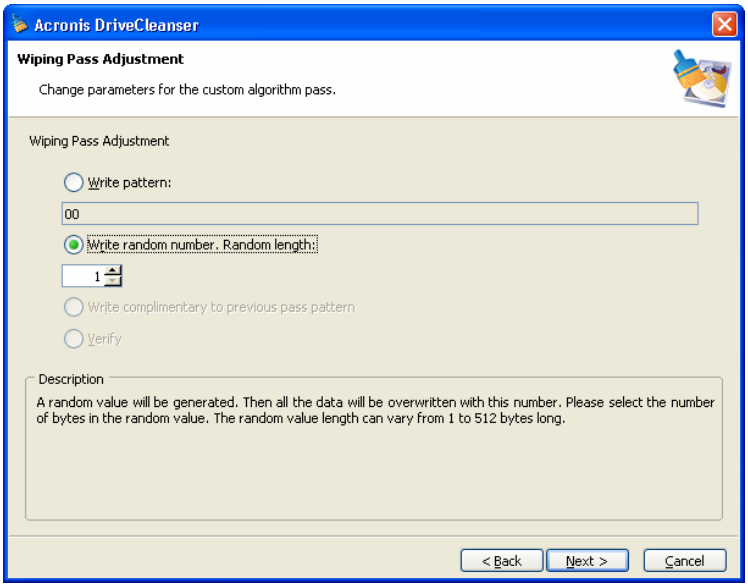
The wiping pass adjustment window for definition of patterns to be written

In this figure the switch is set to **Write a value** position by default, the hexadecimal value 0x00 is entered into the field.

Let us explain the meaning of window control elements. you may enter any hexadecimal value into the field under the **Write a value** switch to write it to a hard disk during any pass (during the 1-st pass in this case).

By setting the switch to **Write a random value** position, you first will select write a random value to disk, and the specify the length of random value in bytes in the spinner field below.

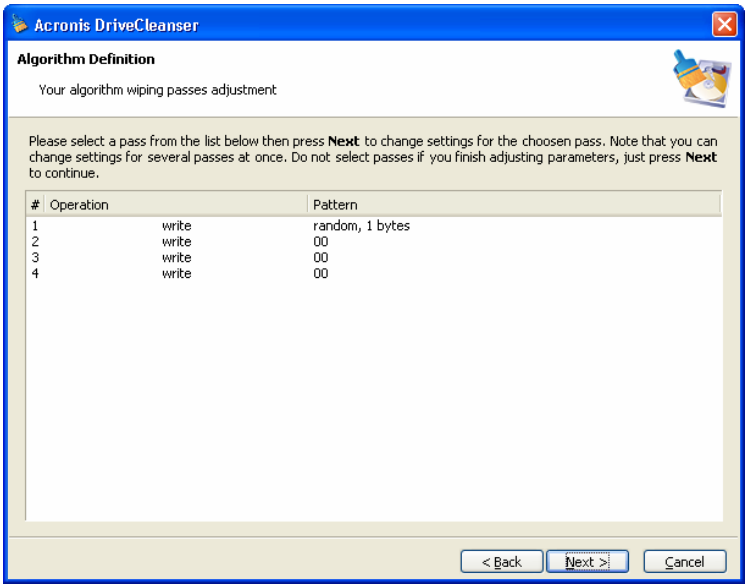
The American national standard provides the writing of random values to each byte of each disk sector during the first pass, so set the switch to **Write a random value** position and to enter 1 into field.



The input of a random 1 byte value as the pattern for writing

Click the Next button to continue.

You will be taken to the algorithm definition window again and will see that the former record (1 – write – 00) was replaced by 1 – write – random value, 1 byte.

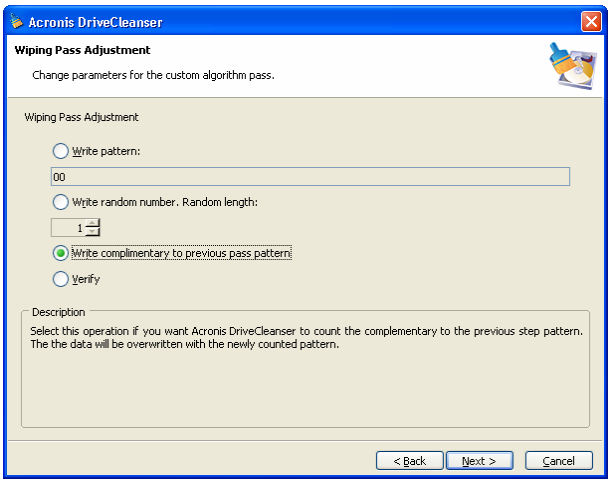


The 1-st pass of the custom algorithm is defined

To define the next pass select the second line of the list and click the Next button.

You will see the already familiar window, but this time there will be more switch positions available: two additional positions will be available for selection:

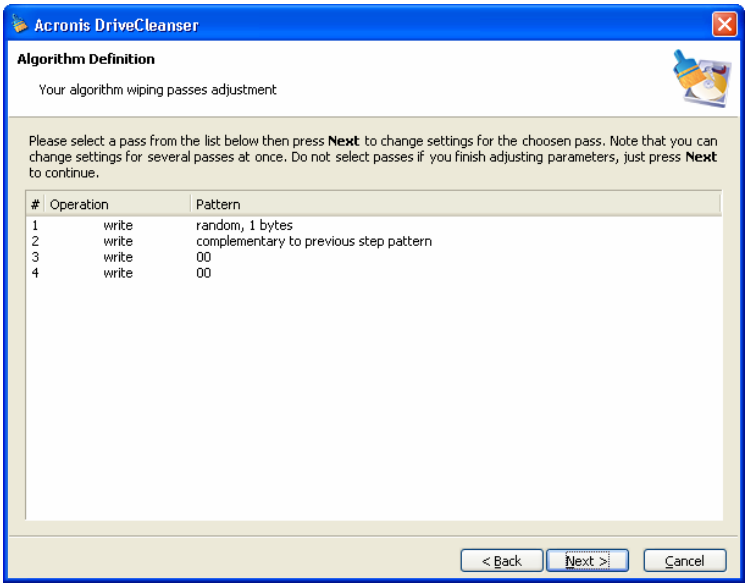
- **Previous step complementary value**,
- **Verify**.



The input of value complementary to the one written during the previous pass

As during the second pass of the American standard each disk sector is filled with hexadecimal values that are complementary to those written during the previous pass. Therefore you should set the switch to the **Previous step complementary value** position and click the Next button.

You will be taken to the algorithm definition window again. In this window the 2-nd record looked like this before: 2 – write – 00, and it was replaced by: 2 – write – previous step complementary value.



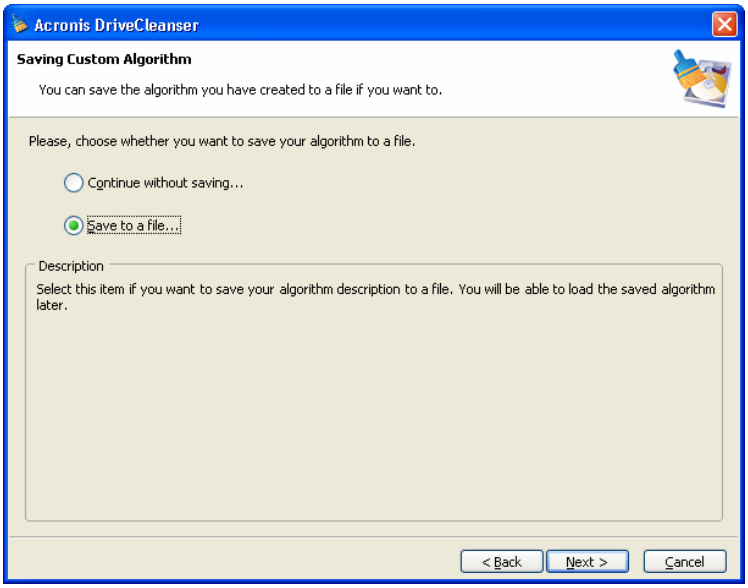
The 2-nd pass of the custom algorithm is defined

Following the U.S. data destruction standard specification, define third and forth data overwriting passes.

In the same way you can create any data destruction algorithm matching your security requirements.

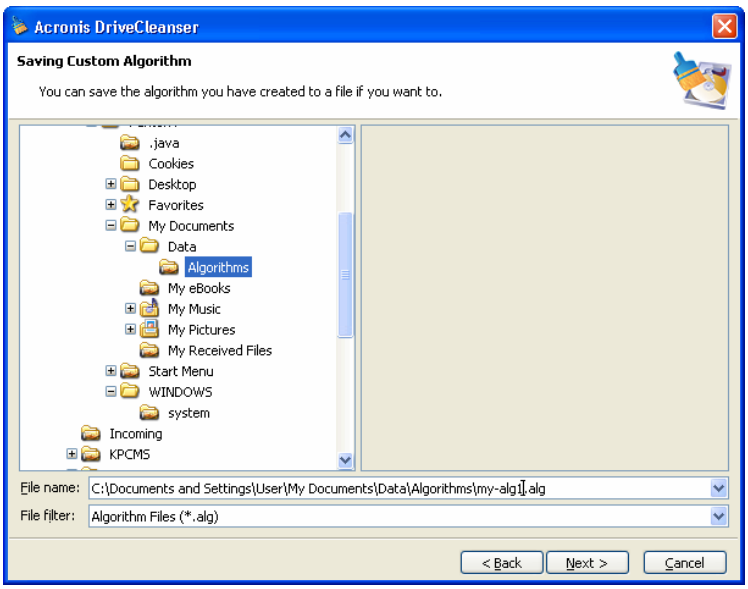
2.2.3 Saving custom algorithm to file

In the next **Saving custom algorithm** window you will be able to save the algorithm you have created. This may be useful if you are going to use this algorithm in future.



The saving custom algorithm window

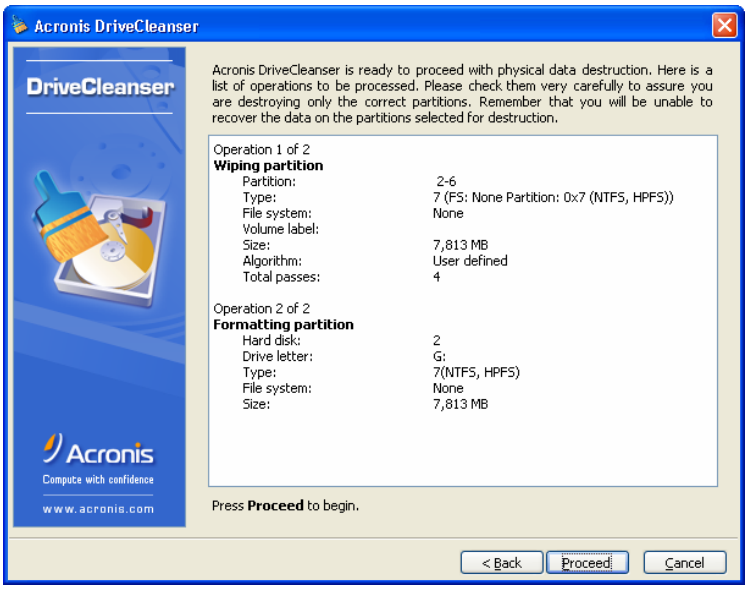
In order do save your algorithm you should define the algorithm filename and the path in the **Select file** field or click the `Browse` button to locate an existing file on the disk. You should also enter the name and a brief description of your algorithm.



The algorithm file name and description window

Each custom algorithm is stored in a separate file with its own name. If you try to write a new algorithm to an already existing file its contents will be erased.

As all passes of your algorithm are defined and the algorithm is saved to file. Clicking the Next button, you will see the window with the generated wiping script based on your custom algorithm.



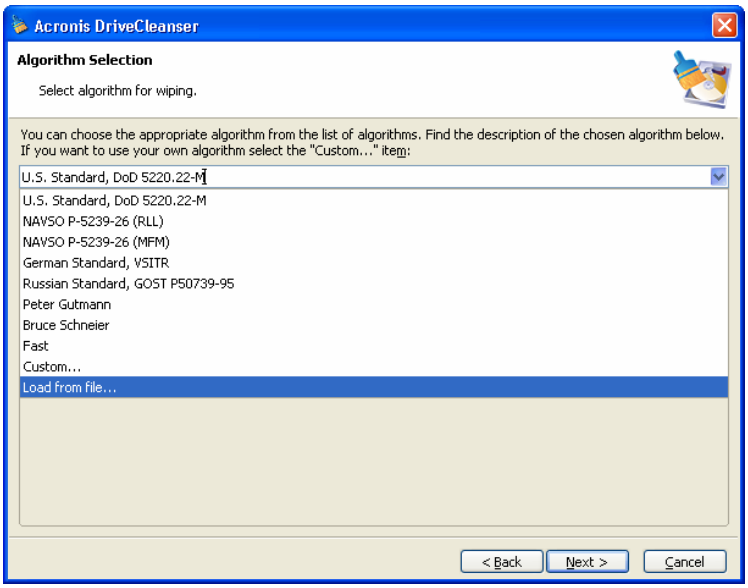
The script of data destruction, based on the custom algorithm

By clicking the Proceed button you will execute the generated script.

If you created and saved your algorithm for data destruction while working with Acronis DriveCleanser software, you may use them in the following way:

2.2.4 Loading algorithm from file

In the **Algorithm selection** window select the «Load from file...» line from the drop-down list.



Algorithm selection: loading from file

Appendix A. Hard Disk Wiping algorithms

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, one may also be able to recover even repeatedly overwritten information. Therefore the problem of guaranteed data wiping is vital as never before.

The **guaranteed wiping of information** from magnetic media (e.g. a hard disk drive) means the impossibility of data recovery by a qualified specialist with the help of any known tools or recovery methods.

This problem can be explained in the following way: Data is stored on a hard disk as a binary sequence of 1 and 0 (ones and zeros), represented by differently magnetized parts of a magnetic disk.

Generally speaking, a 1 written to a hard disk is read as 1 by its controller, and 0 is read as 0. However, of you write 1 over 0, the result is conditionally 0.95 and vice versa – if 1 is written over 1 the result is 1.05. These differences are irrelevant for the controller. However using special equipment, one can easily read the «underlying» sequence of 1 and 0.

It only requires specialized software and inexpensive hardware to read data «deleted» this way by analyzing magnetization of hard disk sectors, residual magnetization of track sides and/or by using current magnetic microscopes.

Writing to magnetic media leads to subtle effects summarized as follows: every track of a magnetic disk stores **an image of every record** ever written to it, but the effect of such record (magnetic layer) becomes more subtle as time passes.

A.1 Information wiping algorithms functioning principles

Physically the complete wiping of information from a hard disk involves the switching of every elementary magnetic area of the recording material as many times as possible by writing specially selected sequences of logical 1 and 0 (also known as samples).

Using logical data encoding methods in current hard disks, you can select **samples** of symbol (or elementary data bit) sequences to be written to sectors in order to **repeatedly and effectively wipe confidential information.**

Algorithms offered by national standards provide (single or triple) recording of random symbols to disk sectors that are **straightforward and arbitrary decision, in general**, but still acceptable in simple situations. The most effective information wiping algorithm based on deep analysis of subtle features of recording data to all

types of hard disks. This knowledge speaks to the necessity of complex multipass algorithms to **guarantee** information wiping.

The detailed theory of guaranteed information wiping is described in an article of Peter Gutmann, please see:

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

A.2 Algorithms used by Acronis DriveCleanser

The table below briefly describes information wiping algorithms used by Acronis DriveCleanser. Each description features the number of hard disk sector passes along with number(s) written to each sector byte.

The description of built-in information wiping algorithms

NN	Algorithm (writing method)	Passes	Record
1.	American: DoD 5220.22-M	4	1st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1st pass; 3 – random symbols again; 4 – writing verification.
2.	American NAVSO P-5239-26 (RLL)	4	1st pass – 0x01 to all sectors, 2 - 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	American NAVSO P-5239-26 (MFM)	4	1st pass – 0x01 to all sectors, 2 - 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1st – 6th – alternate sequences of: 0x00 and 0xFF; 7th - 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6th to 4th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3rd to 1st security level systems.
6.	P. Gutmann's algorithm	35	Peter Gutmann's algorithm is very sophisticated. It's based on his theory of hard disk information wiping (see http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).
7.	B. Schneier's algorithm	7	Bruce Schneier offers seven pass overwriting algorithm in his Applied Cryptography book. 1st pass – 0xFF, 2st pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
8.	Fast	1	Logical zeros (0x00 numbers) to all sectors to wipe.