

CHSSTS Documentation

Ad-Aware SE

James Schwar

version 0.2
Summer 2006

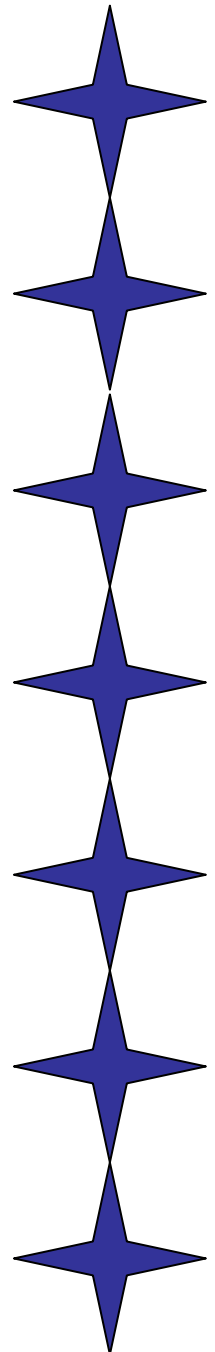


Table of Contents

1. Introduction.....	2
1.1 Purpose of this document	2
1.2 Scope of this document	2
1.3 Reference	2
1.4 Document Legend	2
2. General Description.....	3
2.1 Product Functions.....	3
2.2 Similar System Information.....	3
2.3 User Characteristics.....	3
2.4 User Problem Statement.....	3
3. Installation	4
3.1 Download the Installation Package	4
3.2 License Agreement.....	4
3.3 Choose a Destination for the Installation	5
3.4 Choose Who Can Use the Program.....	6
3.5 Accept Settings and Install Program	6
4. Updating the Definitions File.....	8
4.1 Why should I update the definitions?	8
4.2 Start the Program	8
4.3 Connect to Server.....	8
4.4 Get the New Definitions.....	9
4.5 Finish the Update	9
5. Scanning the Computer.....	10
5.1 Open the program.....	10
5.2 Preparing a Scan	11
5.3 System Scan	11
5.4 Remove Found Items	12

1. Introduction

1.1 Purpose of this document

This document was created to assist an average computer user with the task of installing, configuring, and using Lavasoft's Ad-aware. The document is intended to be a walk through of the basic functions of the application.

1.2 Scope of this document

This document will only cover the core of Ad-aware Personal, the free version. The document will cover how to detect and remove spyware, but will not cover what to do if the software inadvertently messes up your computer.

1.3 Reference

<http://www.lavasoft.de/software/adaware/>

<http://www.microsoft.com/athome/security/spyware/spywarewhat.msp>

1.4 Document Legend

Items in *italics* indicate an action to be performed by a user

Items in **bold** indicate an item within a screen to perform an action on

2. General Description

2.1 Product Functions

Ad-aware removes two (2) types of malware known as spyware and adware. Spyware collects information about you and your computer, such as credit card numbers, user accounts, etc... Adware provides advertisements on your computer, this most often comes in the form of annoying pop-ups that seem to come from nowhere.

2.2 Similar Product Information

There are many products on the market today that provide similar functions to Ad-aware. No one product is 100% effective against malware so I suggest a combination of some of the better free products. Personally I use a combination of Ad-aware, Spybot Search and Destroy (<http://www.safer-networking.org/>), and Microsoft's Window's Defender (<http://www.microsoft.com/athome/security/spyware/software/default.mspx>). Spybot Search and Destroy has an immunize function that allows you to stop certain problems before they start. Window's Defender has real-time scanning, which will check for malware actions as you are working with the machine.

2.3 User Characteristics

We make the assumption that the users of this document are of the Do It Yourself type. The users may have a busy schedule and may not have time to bring their machines to technicians for maintenance. Also the users may not wish to have their computers infected with anything that they did not intentionally place there.

2.4 User Problem Statement

The user has a machine that is beginning to run slower, has annoying pop-up messages, or they just want to do their best to prevent anything from going wrong.

3. Installation

3.1 Download the Installation Package

I have created a local download spot for the file at:

<http://netdrive/~schwarj/software/adaware/aawsepersonal.exe>

You may also wish to get the file directly from the source at:

<http://www.lavasoft.de/support/download/>

You should now have an icon like the one shown in Figure 3.1 somewhere on your machine. *Double-click* on the icon to start the installation.

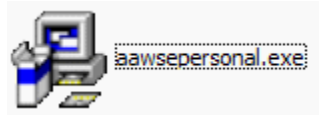


Figure 3.1

Most people won't have a way to verify their downloads, but if you can here is the MD5 sum. If this doesn't make any sense to you then just ignore it.

MD5 Checksum: 6286cf12eeae984d381773f097baf981

3.2 License Agreement

As with most pieces of software these days you will have to agree to a license in order to use the software, see Figure 3.2. I strongly suggest that you read through all of the agreements so that you know exactly what you are getting into when you install a new piece of software. Most people will just *click on the box I accept the License agreement* and then *click Next>*.

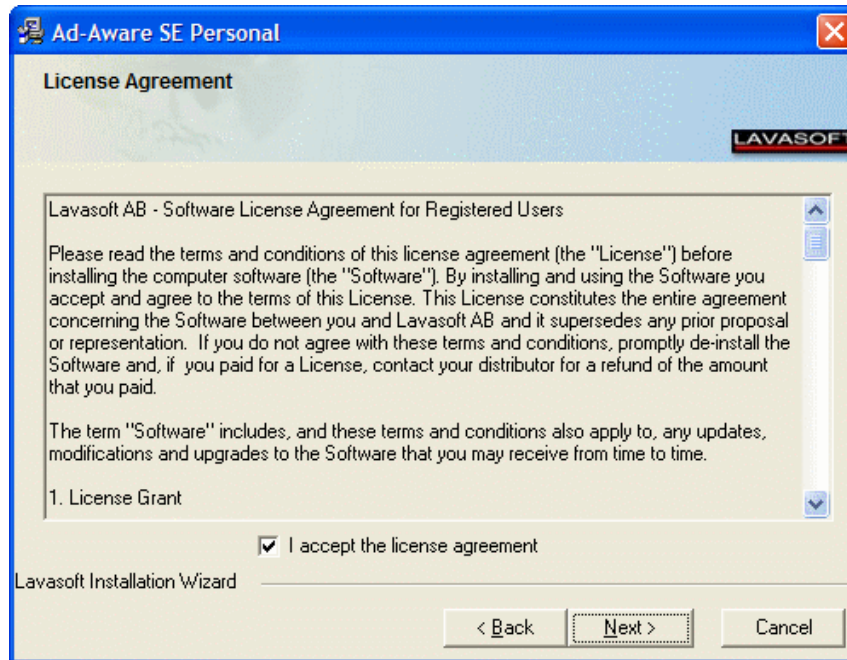


Figure 3.2

3.3 Choose a Destination for the Installation

Now you will need to choose the folder that you want the program installed into. I suggest that you leave the settings at the defaults, and only change them if absolutely necessary. If you leave it at that default setting, just *click* on **Next>** as shown in figure 3.3.

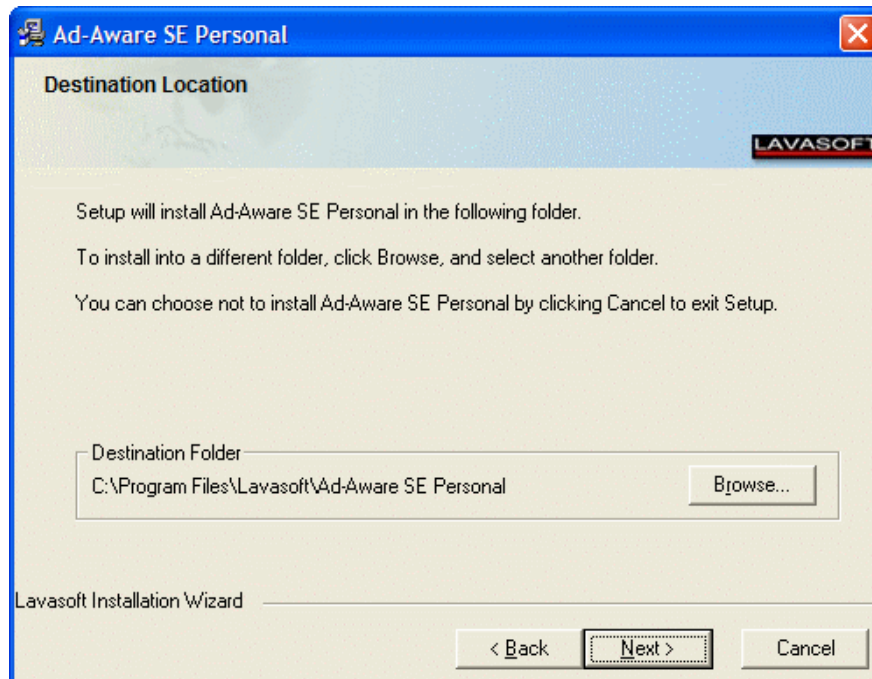


Figure 3.3

3.4 Choose Who Can Use the Program

You can choose to only allow yourself, or to allow everyone access to run the program. The default setting is to allow everyone to run the program. I suggest that you use this setting, if you choose to do so, just *click Next>*. See Figure 3.4.

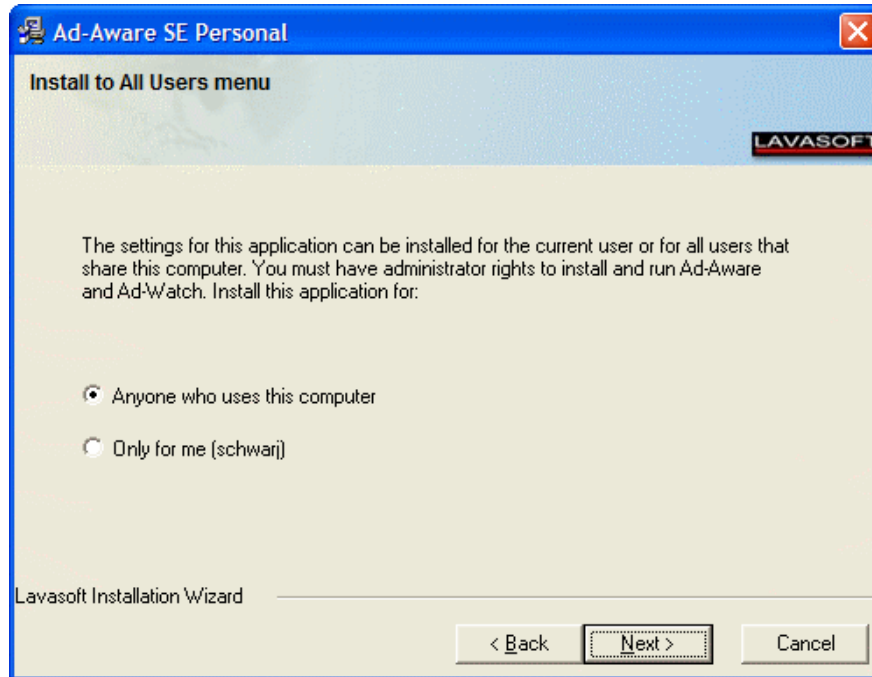


Figure 3.4

3.5 Accept Settings and Install Program

You have hit the point where you have completed choosing the installation settings for the program, see Figure 3.5. You still have the option to go back and change any of the settings or to cancel the installation all together. If you have followed the steps in this guide you can *click* on **Next>**.

The program will install, after which you will be given the opportunity to update the Definitions File which tells the program what to look for in its search for malware, and you will be given the opportunity to run your first scan, see Figure 3.6. I suggest that you *uncheck these boxes* for now and proceed to sections 4 and 5, which cover updating the definitions file and running scans.

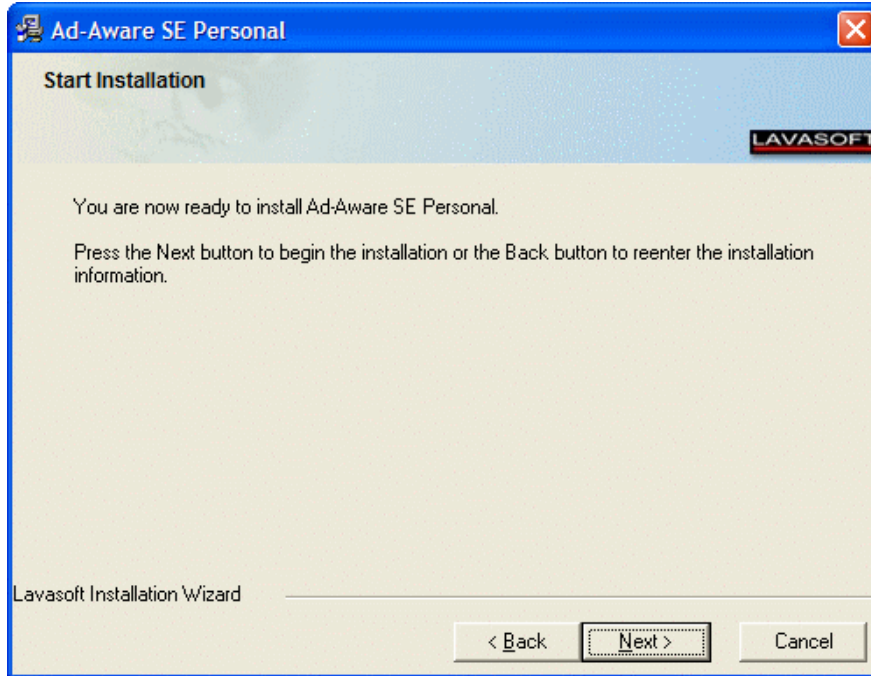


Figure 3.5

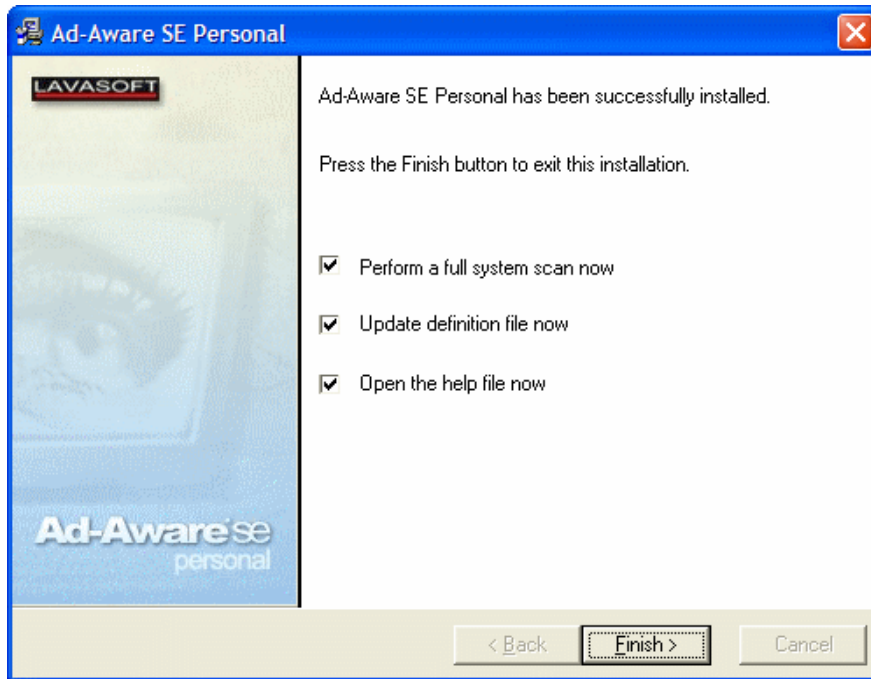


Figure 3.6

4. Updating the Definitions File

4.1 Why should I update the definitions?

Updating the definitions file lets the program know how to detect and remove the latest versions of malware that are out there these days. As the scanners become more advanced and clever in their ways to remove the malware, the malware writers get better at finding new ways to infect machines and hide their software. So it is a never ending battle between the sides, which is why you will definitely want to have every resource available to stop these threats.

4.2 Start the Program

To update your malware definitions file you must first go to *Start -> All Programs -> Lavasoft Ad-aware SE Personal -> Ad-aware SE Personal*. When the program starts you will receive a message like the one shown in Figure 4.1 when your definitions file is out of date. If you see the message as shown in Figure 4.1, *click* on the **OK** button to proceed.

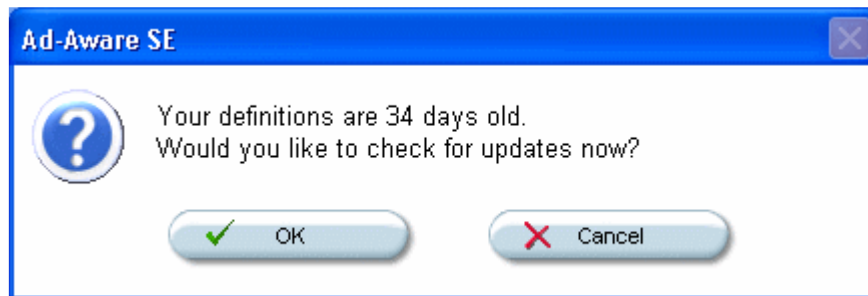


Figure 4.1

4.3 Connect to Server

After you have clicked on the **OK** button in Figure 4.1, you will be presented with the window that is shown in Figure 4.2. Here you will connect to Lavasoft's server and it will determine the proper version of the file for your system. All you will need to do is *click* on the **Connect** button on the bottom right hand corner of the window that is represented by Figure 4.2.

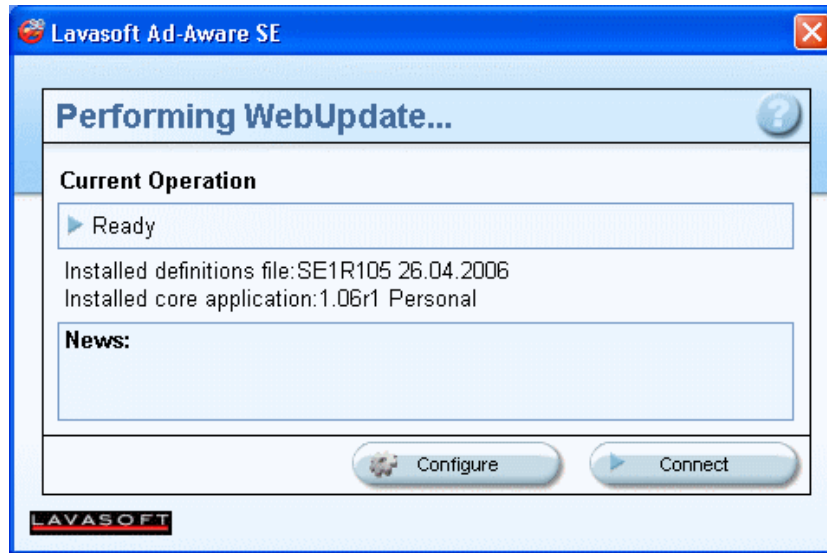


Figure 4.2

4.4 Get the New Definitions

The program will connect to the server and determine the correct definition file for you. When that is done you will be presented with a window like the one shown in Figure 4.3. *Click* on the **OK** button to download and install the update.

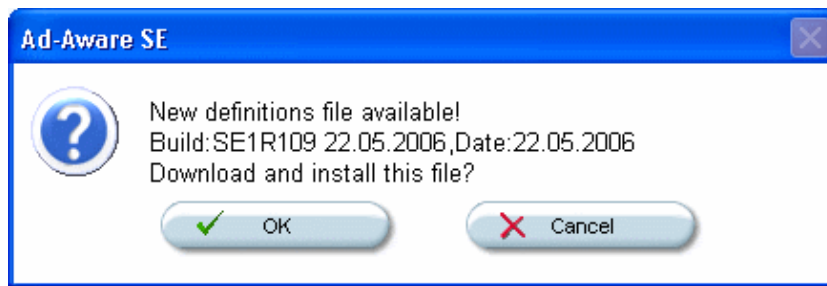


Figure 4.3

4.5 Finish the Update

It should only take a few minutes to update the definitions file. When it has completed the **Finish** button will be highlighted in the bottom right-hand corner of the screen. See Figure 4.4 for a representation of this window. After you have clicked on the **Finish** button you will be brought to the main screen of the program. From there you can run a scan of your computer. See Section 5 of this document to learn more about that.

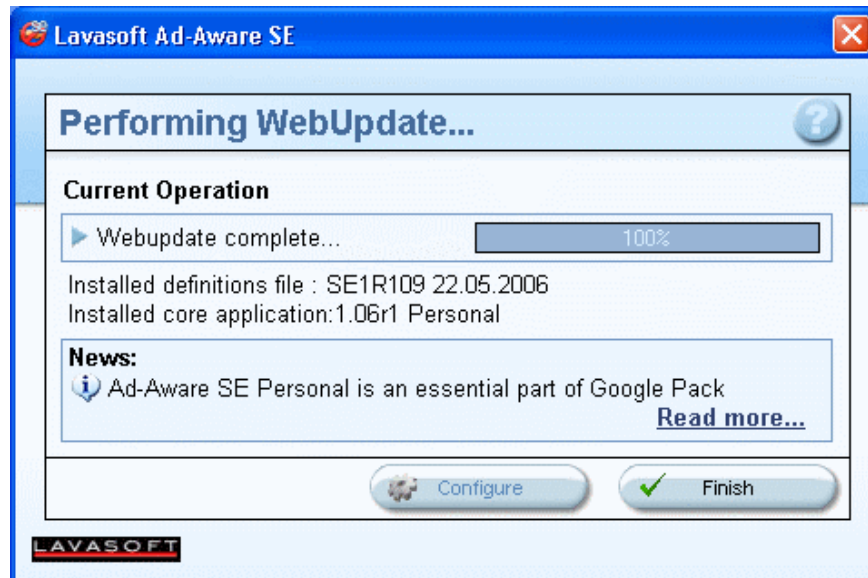


Figure 4.4

5. Scanning the Computer

5.1 Open the program

If you followed the instructions in this guide then you will need to navigate to *Start* → *All Programs* → *Lavasoft Ad-Aware SE Personal* → *Ad-Aware SE Personal* to open the program. If not, you will need to find the link to open the file. Either way, once the program has started you should see the main screen as shown in Figure 5.1. Most of the options here are beyond the scope of this document, so go to the bottom right hand corner of the screen and *click* on the **Start** button.



Figure 5.1

5.2 Preparing a Scan

After you have *clicked* on the **Start** button you will be brought to the screen shown in Figure 5.2. Here you will have a choice of what type of scan to do. I strongly suggest that you *click* on the button for **Perform full system scan** and make sure that the checkmarks for **Search for negligible risk entries** and **Search for low-risk threats** are checked. Once this is done you should *click* on the **Next** button in the bottom right-hand corner.

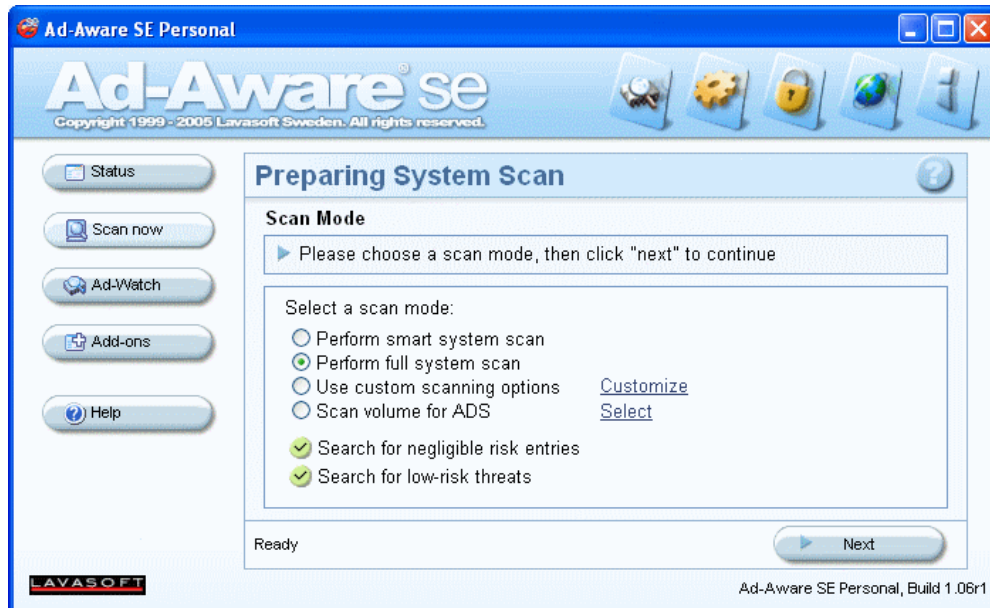


Figure 5.2

5.3 System Scan

If you have *clicked* on the **Next** button as shown in Figure 5.2 the system scan is now in progress. You should see a screen like the one shown in Figure 5.3. Here you can see the progress of the scan and the types of suspicious objects that are found. You have the option to cancelling the operation at any point by *clicking* on the **Cancel** button in the bottom right-hand corner of the screen. I suggest that you wait until the scan has finished and proceed onto the next section. In Figure 5.4 you can see what a finished scan looks like. Notice the red marks indicating that possible malware has been found. *Click* on the button labeled **Next** shown in the bottom right-hand corner of figure 5.4 to proceed.

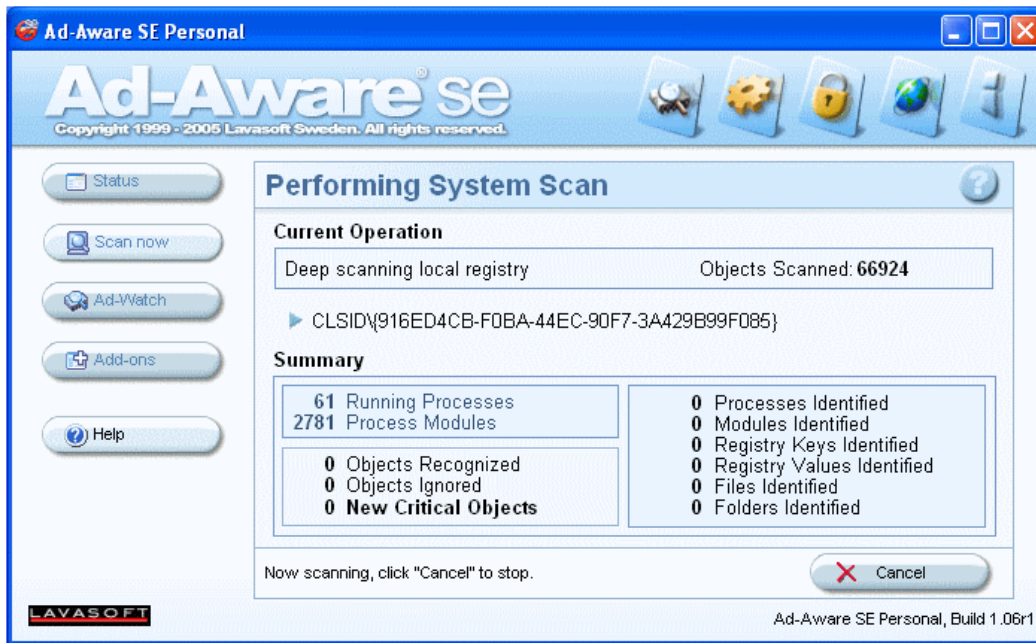


Figure 5.3

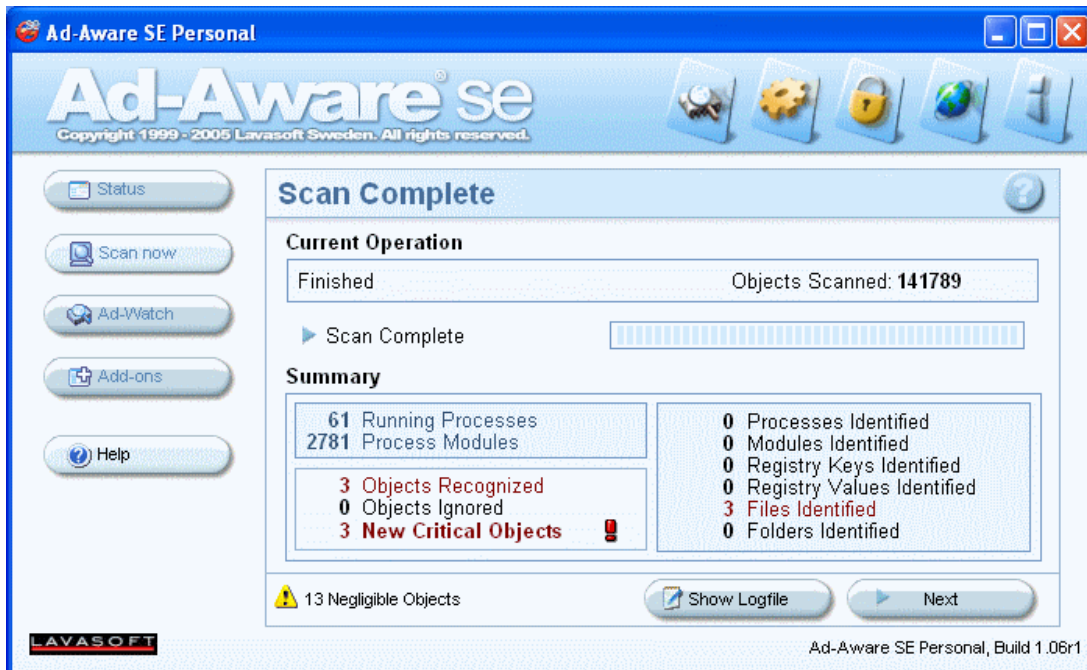


Figure 5.4

5.4 Remove Found Items

At this point you are almost finished. You can *click* on the + signs next to the objects to view more information about them, see Figure 5.5. Also you can *click* on the **!Critical Objects** tab, as shown in Figure 5.6, to see some of the more dangerous objects on your computer. If you *double-click* on an item in Figure 5.6 you can view more information about the object. Most users will just want to make sure that the

items shown in Figure 5.5 have the boxes check marked and then *click Next*. You should now be free of some of the malware on your computer.



Figure 5.5



Figure 5.6