Dr. Aggarwal

60-564

Report on Spybot-S&D

Submitted By:

Ataul Bari

ID: 100653937

Table of Content

1 Introduction

Spybot Search & Destroy (Spybot S&D) is a tool that can help an Internet user to detect and remove spyware from the user system. Spyware is a general term for a program that surreptitiously monitors an Internet user's actions [1]. It is a technology that assists in gathering information about a person or organization without their knowledge. On the Internet, "spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties"[2]. Now a day, just about every Internet user has had to deal with spyware. It is a serious security and privacy risk. It also degrades system performance by stealing the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection.

There are a number of tools available that can be used to help protecting a system from spyware including Spybot S&D, Ad-Aware SE etc. This report describes spyware protection using Spybot S&D, which is free to download from the Internet. The rest of this report is organized as follows:

Section 2 describes the downloading, installation and running of Spybot S&D. section 3 describes the details of different features and capabilities of Spybot S&D as it is explored for the purpose of this project. The report concludes with a summary in section 4.

2 Spybot S&D

This section describes some features of Spybot-S&D along with the system requirement, downloading and installation of it in windows environment.

2.1 Preview

Spybot - S&D is a tool that can detect and remove different kinds spyware from a computer. It is free and easy to use. A user can use it to see if something snooped into his/her computer.

Spybot-S&D can start in two modes: *easy mode* for new users who want just the basic features, and *advanced mode* for professional users and those who want more control. Both modes are available in the free version. [3]

Feature	Default mode	Advanced mode
Removal of adware and spyware, Removal of dialers Removal of keyloggers Removal of trojans and other baddies Removal of usage tracks	**Yes**	**Yes**
User-extendable database	**Yes**	**Yes**
Save removal of threats by shredding them	**Yes**	**Yes**
Backups of every removed problem	**Yes**	**Yes**
Exclude option to ignore specific problems	**Yes** (1)	**Yes**
Permanent blocking of threatening ActiveX downloads Permanent blocking of known tracking cookies for IE Permanent blocking of threating downloads in IE	**Yes**	**Yes**
Command line parameters to automate tasks	**Yes**	**Yes**
Number of targets	**> 600**	**> 600**
Number of detection files and entries	**> 10000**	**> 10000**
Detailed information about problems found	**Yes**	**Yes**
Strict criteria to define targets	**Yes**	**Yes**
Integrated update function Weekly updates Update notification by mail	**Yes**	**Yes**
Free email & forum support	**Yes**	**Yes**
Settings to automate scan, removal and update	No	**Yes**
System reports to locate even unknown threats	No	**Yes**
Skins to adjust interface to the users liking	No	**Yes**
(1) Can only be undone in advanced mode (2) Planned for the near future		

Table 1 Features of Spybot S&D in easy and advanced mode [3]

2.2 Supported Operating Systems

Following table 2 summarizes the OS requirement for Spybot-S&D.

Operating system	Supported
Windows 95	Winsock update necessary
Windows 98	Fully functional
Windows ME	Fully functional
Windows NT	Some functions need administrator rights
Windows 2000	Some functions need administrator rights
Windows XP	Some functions need administrator rights (XP accounts have those rights by default)
Windows XP AMD64	Some functions need administrator rights (XP accounts have those rights by default) (no problems found, but still in testing)
Windows 2003	Some functions need administrator rights (no problems found, still in testing)
Mac OS	Not supported
Mac OS X	Not supported
Linux/Unix	Not supported

Table 2 Operating Systems supported by Spybot S&D [4]

2.3 Downloading Spybot S&D

The Spybot S&D can be downloaded from using the following link: http://www.safer-networking.org/en/download/index.html. The download is free. For the purpose of this project, Spybot-S&D, version 1.3 has been used.

2.4 Installing Spybot S&D

The downloaded installation file is named as *spybotsd13.exe*. To install Spybot-S&D, this file has to be run. Once started, the installation program first prompts for the selection of setup language (Fig. 1) and upon selection, the set up screen appears (Fig. 2). Clicking on the next button in set up screen (Fig. 2) brings the license agreement screen and upon accepting the agreement, the setup continues with the screen for selecting the location of the installation (Fig. 3) followed by the screen for selecting the components (Fig. 4) for the installation. In the similar way, the set up continues by displaying the screens for selecting the start menu folder and additional tasks options. To use the default values for all these setting, a user can keep on clicking on the “next” button provided with each screen.

Fig. 1 Choosing setup language

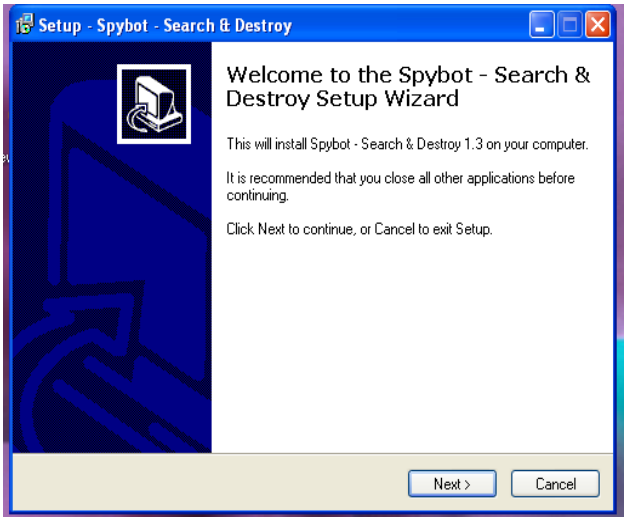


Fig. 2 Set up screen of Spybot S&D

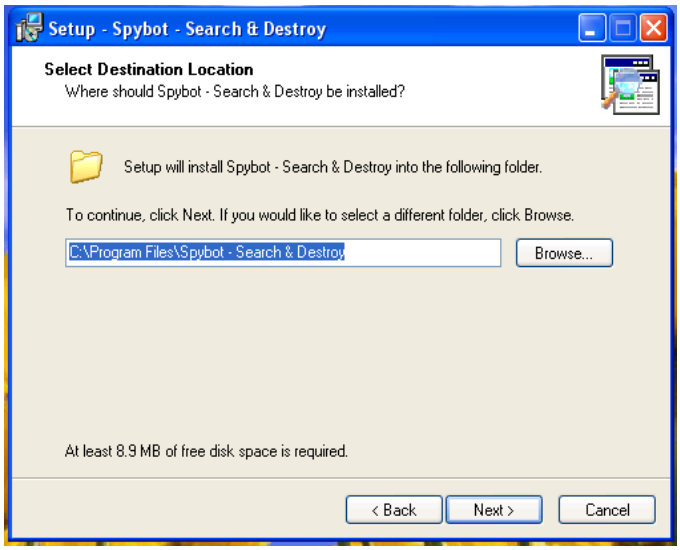


Fig 3 Selecting the location of installation

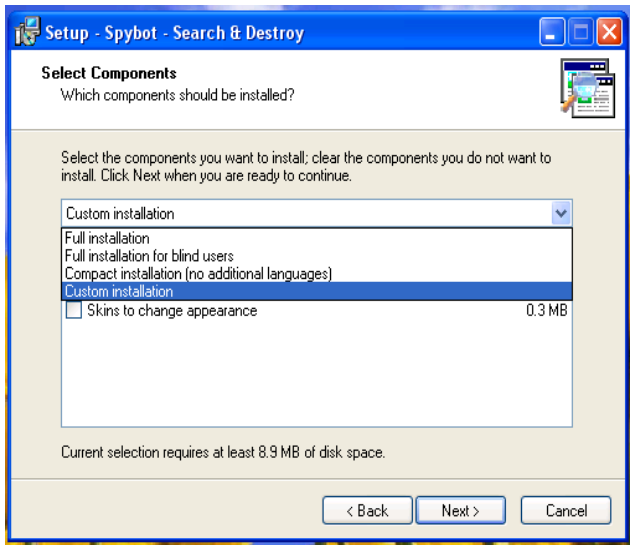


Fig. 4 Selecting Components

Once the setup program finishes gathering all these information, the installation begins and the Spybot-S&D program is installed into the system. After finishing the installation, an icon named *Spybot - Search & Destroy* appears on the desktop and in the start menu. Clicking on this button starts the Spybot-S&D.

2.5 Running Spybot S&D

After installation, the Spybot-S&D can be started by clicking on the icon named as *Spybot - Search & Destroy (by default)* that appears on the desktop. Clicking on the entry with the same name that appears in the program group where the software has been

installed can also start it. While started, the program provides a Graphical User Interface (GUI) that is shown as screenshot in fig. 5. This GUI provides access to the different functionalities of Spybot-S&D as well as to the expert setting of the program.

A tutorial on installation and execution of Spybot-S&D can be found in http://www.safer-networking.org/en/tutorial/index.html.

Fig 5 Spybot-S&D – the start up GUI

3 Exploring Spybot S&D

For the purpose of this project, Spybot-S&D, version 1.3 has been used. The program was explored using a system with Pentium-4 processor and windows platform. During the exploration, the system was connected to the Internet through bell simpatico modem using Ethernet card. All screenshots presented here is the result of the program execution on this system. Some features of the program are described using the content of the help files integrated with it.

3.1 The Running Of Spybot S&D For The First Time

When Spybot S&D is started for the first time in a computer system, it goes through some settings. First it asks the user with an option for creating a back up of the registry so that it can be used to restore the system to the original state, if desired (fig. 6).

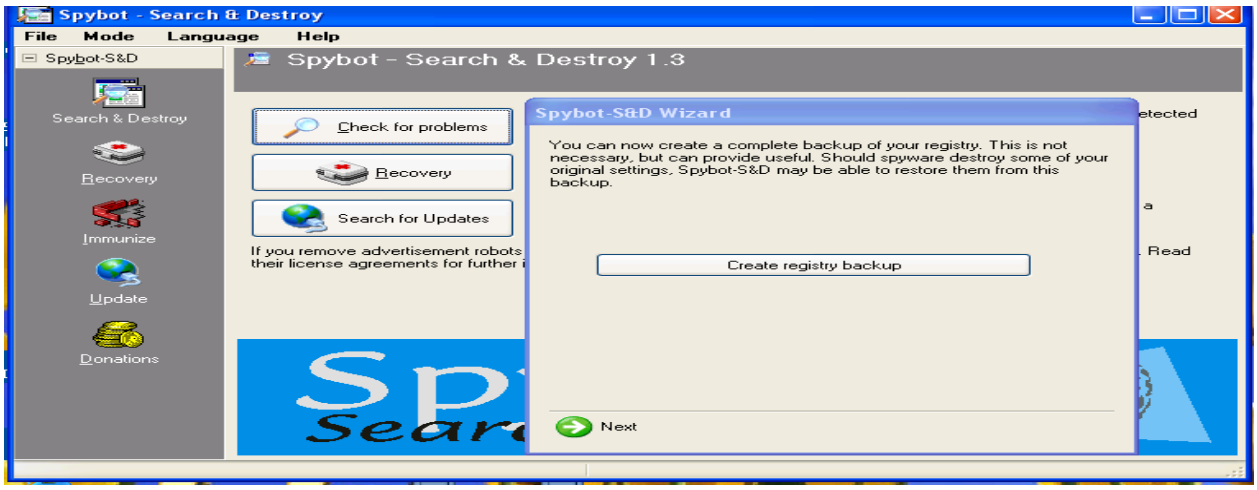


Fig. 6 The first run – Creating Registry Backup

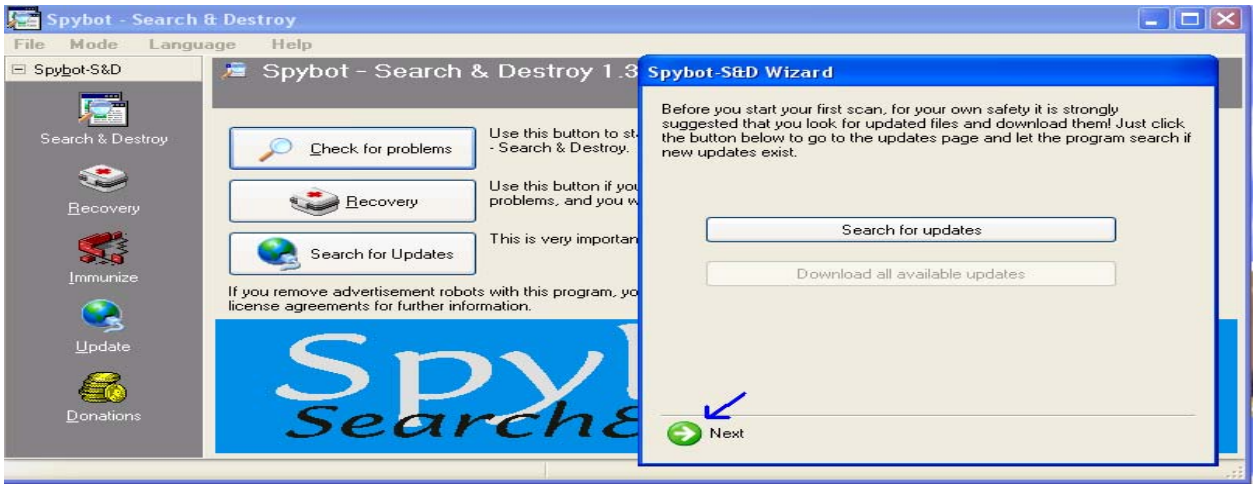


Fig. 7 The first run – Checking for updates

Clicking on “Next” provides the user with an option for checking and downloading updates from the web (fig. 7). Clicking on “Next” in there provides the user with an option for immunization of the system (fig. 8). And another “Next” provides the user with an option for reading the help files, read tutorial or start using the program (fig. 9).

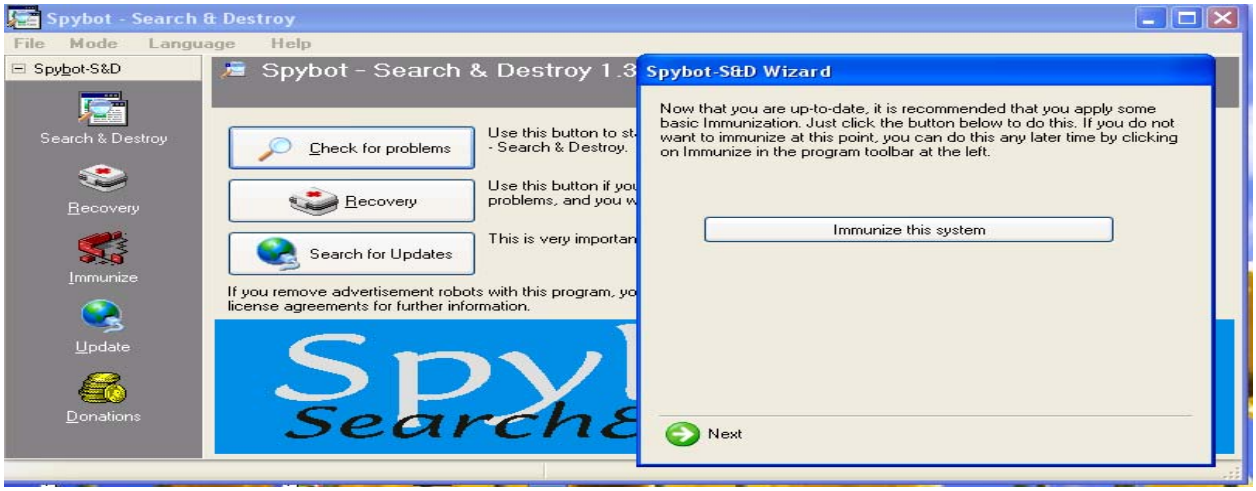


Fig. 8 The first run – Immunize the system

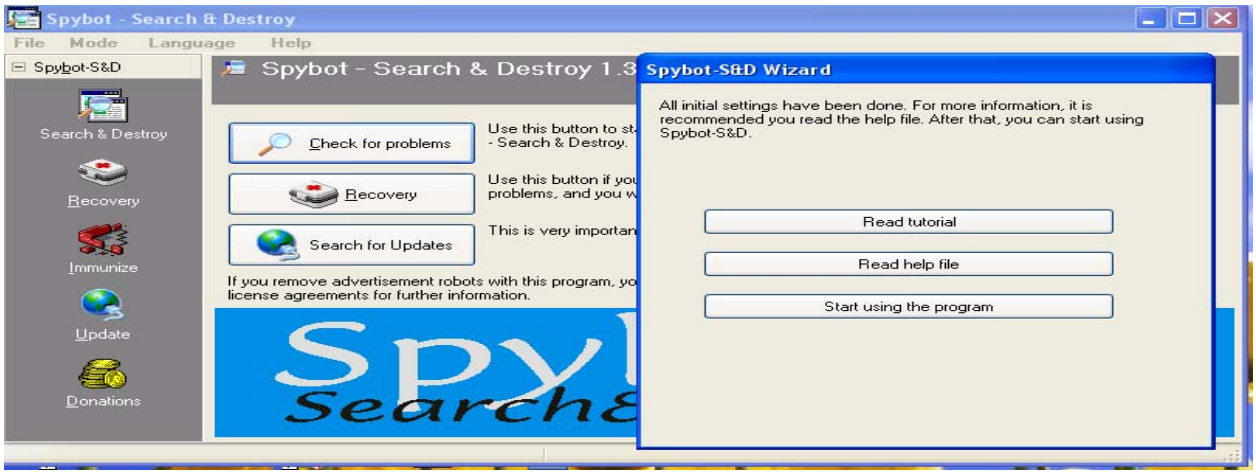


Fig. 9 The first run – option to read help files, tutorial or using the system

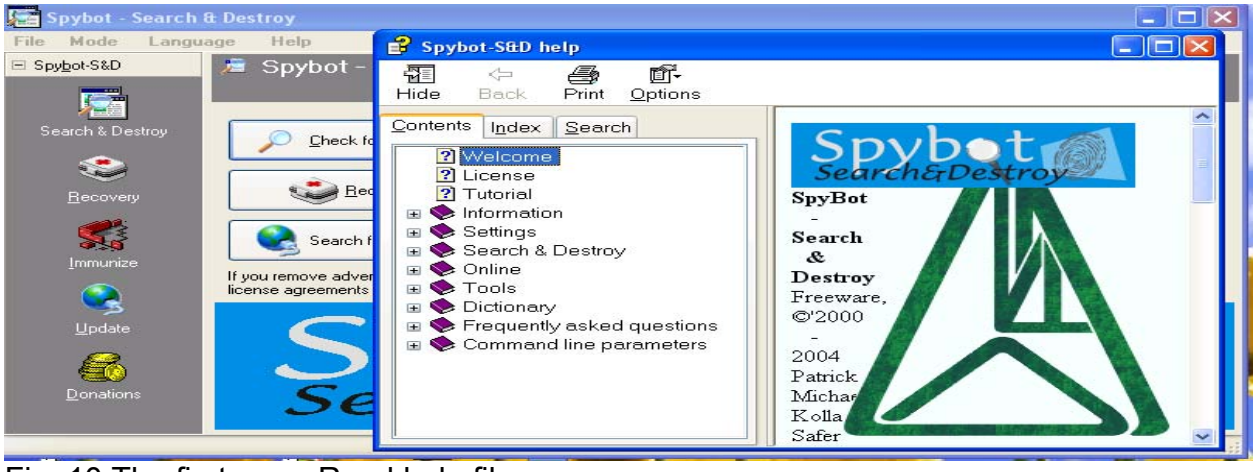


Fig. 10 The first run – Read help file

Clicking on Read tutorial button and Read help file button pop ups respective help pages (Read help is shown in fig. 10). Clicking on “start using the program” button will provide the default GUI for the program as shown in fig. 5.

3.2 Scanning The System With Spybot-S&D

The scan screen of Spybot-S&D is shown in fig. 11. If not present, clicking on Search & Destroy button on the left frame will make the scan screen to appear on the right frame.

Clicking on “Check for problems” button (fig. 11) starts scanning the system for possible threats. Clicking on this button changes the appearance of the scan screen; and the new appearance is shown in fig. 12. At the bottom of this window, the status bar indicates the progress of the scan process [12-1]. User can stop the scan at any point by pressing the “Stop check” button (fig. 12-2), which causes the program to abort the scan and displays the message (fig. 13).

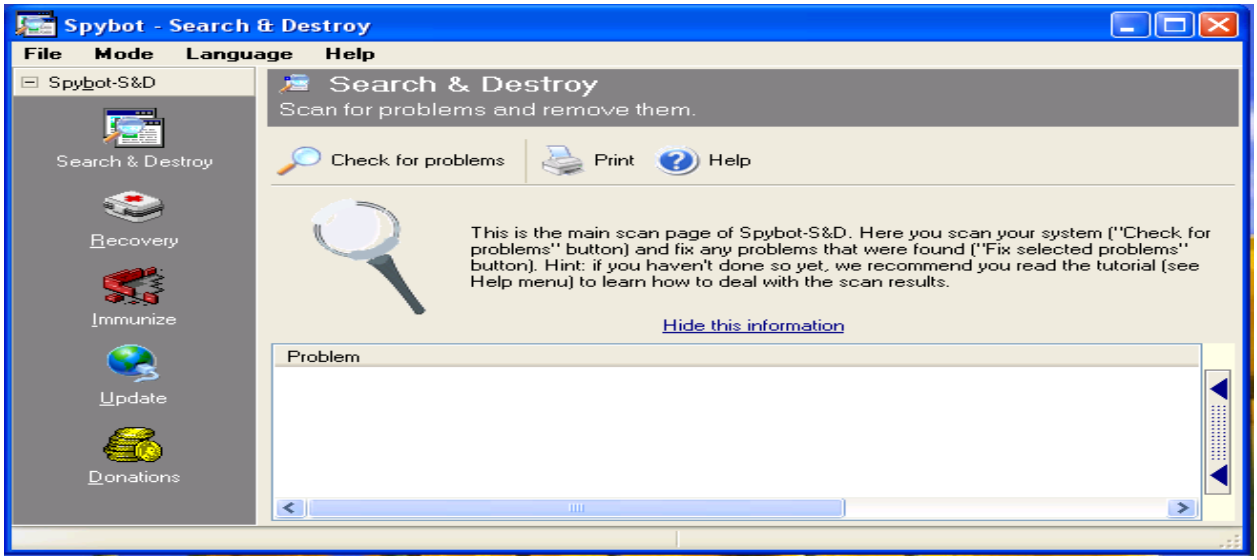


Fig. 11 The scan screen

If the scan has found something, it will be shown in a list (fig. 12-3). Different colors are used in the list to indicate different types of risks:

- Red entries indicate spyware.
- Black entries are system internals.
- Green entries indicate usage tracks.

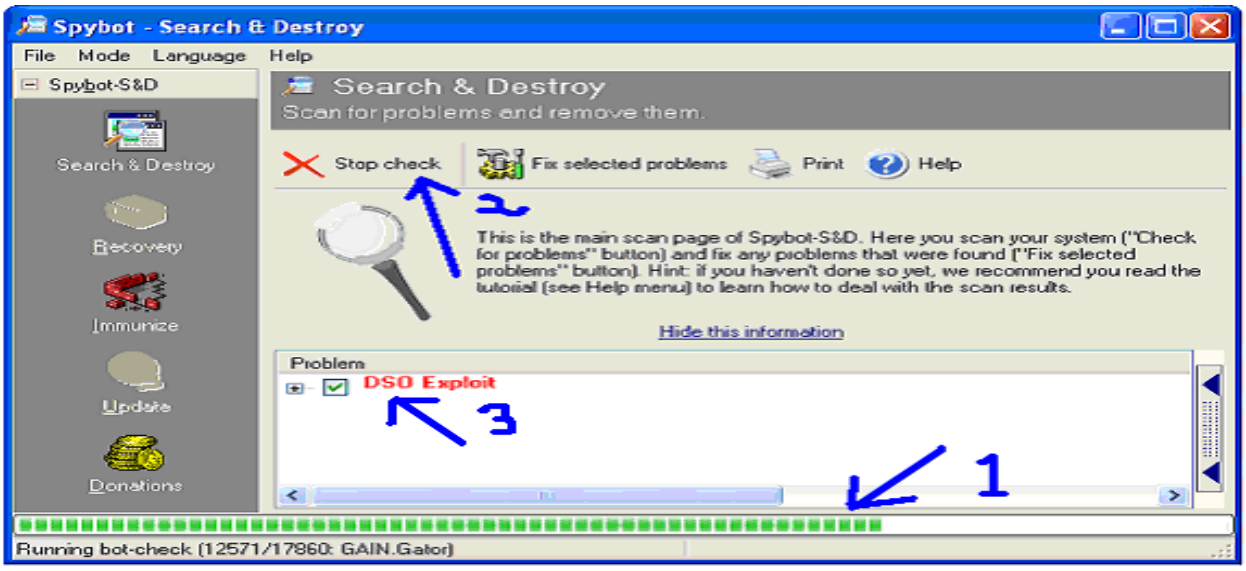


Fig. 12 Scanning the system

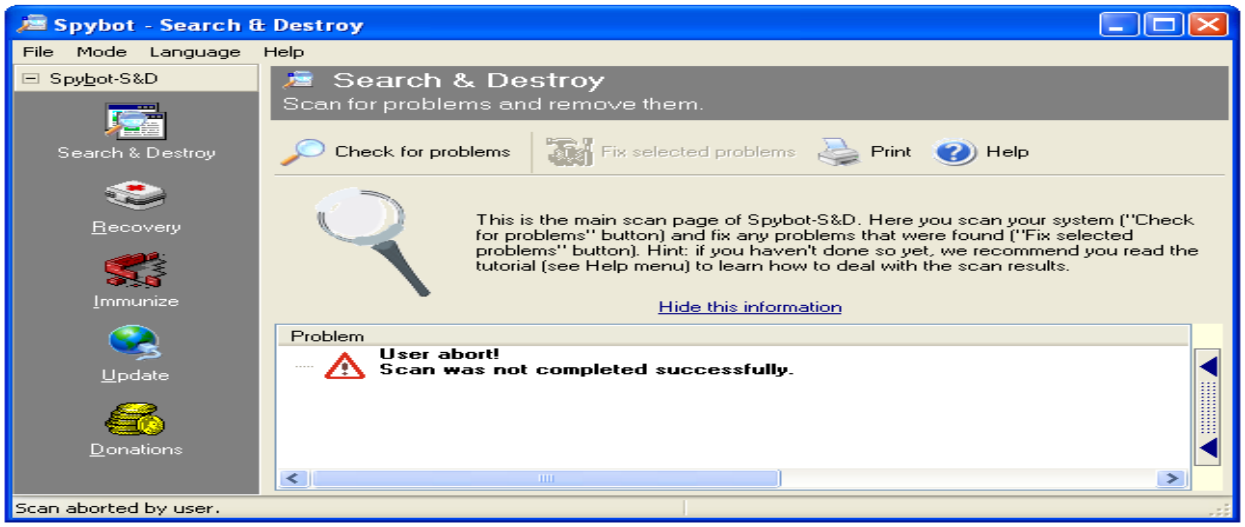


Fig. 13 User aborted the scan

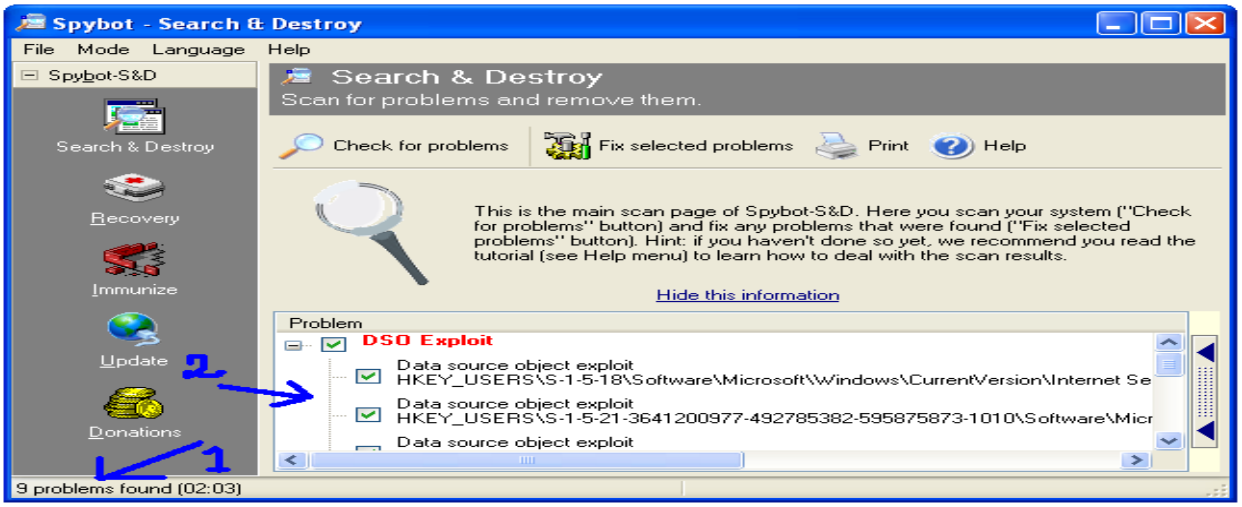


Fig. 14 Viewing the list

Clicking on the group in the list displays all entries found by the scan (fig. 14-2). The total number of problem found is also displayed at the bottom of the screen (fig. 14-1). Selecting an item from the list (fig. 15-1) displays a description of that product (fig. 15-2).

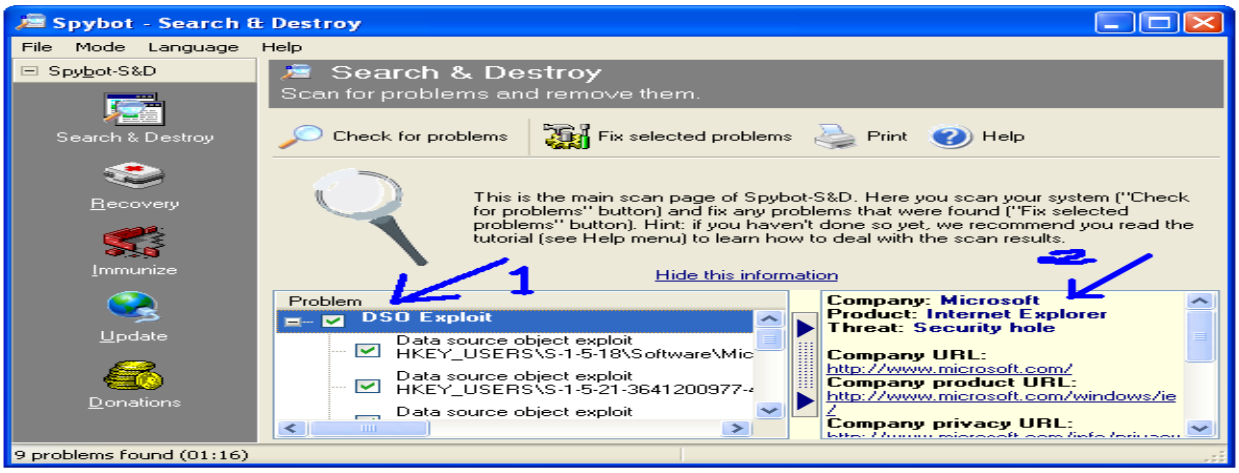


Fig. 15 Description of product

The problems that a user wants to fix are selected by clicking the checkbox before it. More selection options are available in the context menu that appears when a user right clicks on a problem (fig. 16). The context menu also allows a user to exclude single problems or whole products from further scans.

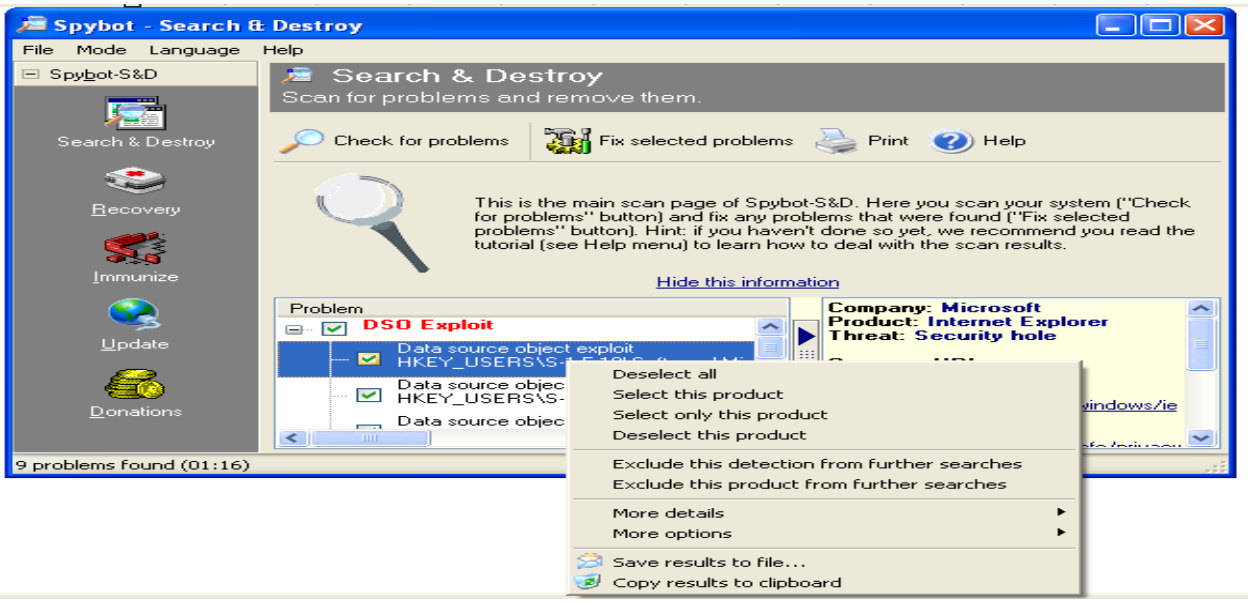


Fig. 16 Context menu

The results of the scan can be saved in a log file by selecting “Save results to file…” option in the context menu (fig. 16). This will pops up the save option window as shown in fig. 17. User can choose the location and file name to save the results.

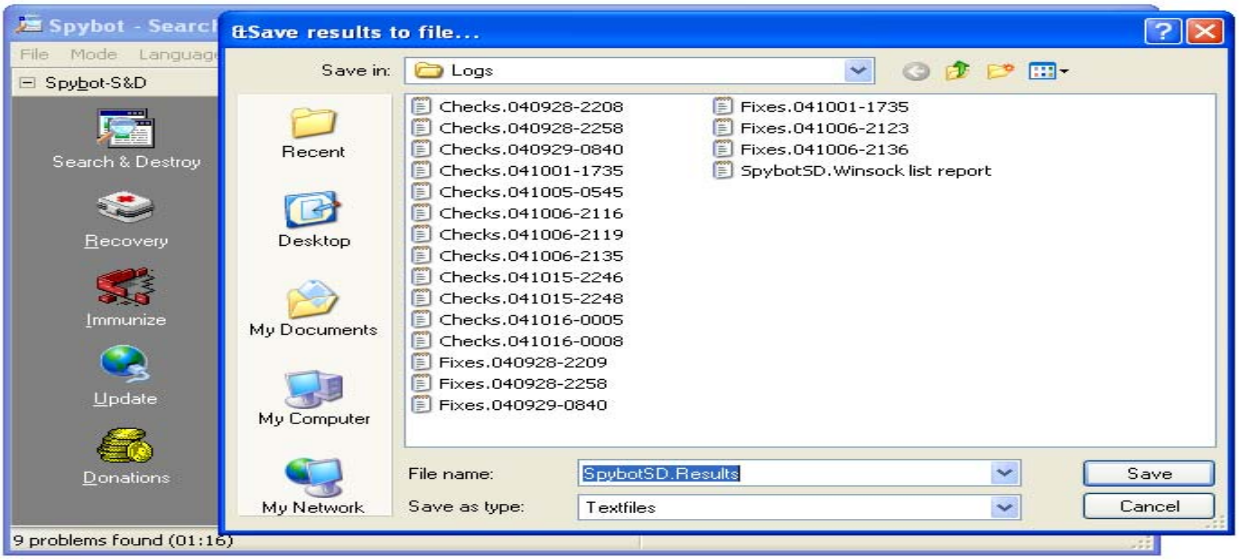


Fig. 17 Saving scan results in file.

```
DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-21-3641200977-492785382-595875873-1010\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-21-3641200977-492785382-595875873-1009\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-21-3641200977-492785382-595875873-1008\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-21-3641200977-492785382-595875873-1007\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-21-3641200977-492785382-595875873-1005\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

DSO Exploit: Data source object exploit (Registry change, nothing done)
  HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

--- Spybot - Search && Destroy version: 1.3  ---
2004-08-11 Includes\Cookies.sbi
2004-09-30 Includes\Dialer.sbi
2004-09-30 Includes\Hijackers.sbi
2004-09-30 Includes\Keyloggers.sbi
2004-05-12 Includes\LSP.sbi
2004-09-30 Includes\Malware.sbi
2004-08-11 Includes\plugin-ignore.ini
2004-08-12 Includes\Revision.sbi
2004-09-16 Includes\Security.sbi
2004-09-30 Includes\Spybots.sbi
2004-08-30 Includes\Tracks.uti
2004-09-30 Includes\Trojans.sbi
```

Fig 18 Copy results to clipboard and paste in a document

The user can also copy the results in the clipboard by selecting the “Copy results to clipboard” option in the context menu (fig. 16). This causes the results to be copied to the clipboard and allows user to paste it into some text files or word documents. Fig. 18 shows the results of a scan after it had been copied to the clipboard and that pasted in a word document.

After the user done with the selection for the problems to be removed from the computer system, he/she presses the “Fix selected problems” button to execute it (fig. 19-1). A confirmation window appears (fig. 19-2), and upon confirmation by the user, selected problems are removed. The bottom status bar shows the progress of the removal process. Prior to this removal, Spybot-S&D creates a backup of selected entries so that the system can be recovered to the original state, if required.

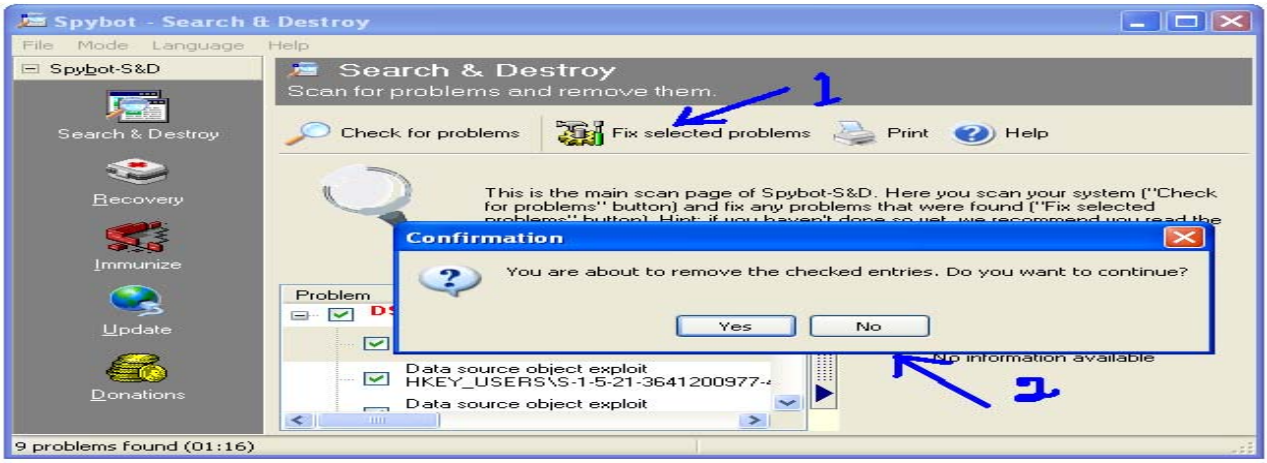


Fig. 19 Fixing problem(s)

Fig. 20 Fixation of problems

After completion of the process, a confirmation window appears that indicates the number of problems that are fixed (fig. 20). If some problems cannot be fixed during this process for some reason (e.g. if they are still loaded and can't be terminated), Spybot-S&D offers to run on next system start, so that the user can check and fix again before that problem get loaded. On the other hand, if the scan does not found any problem, then that information is displayed in the list (fig. 21).

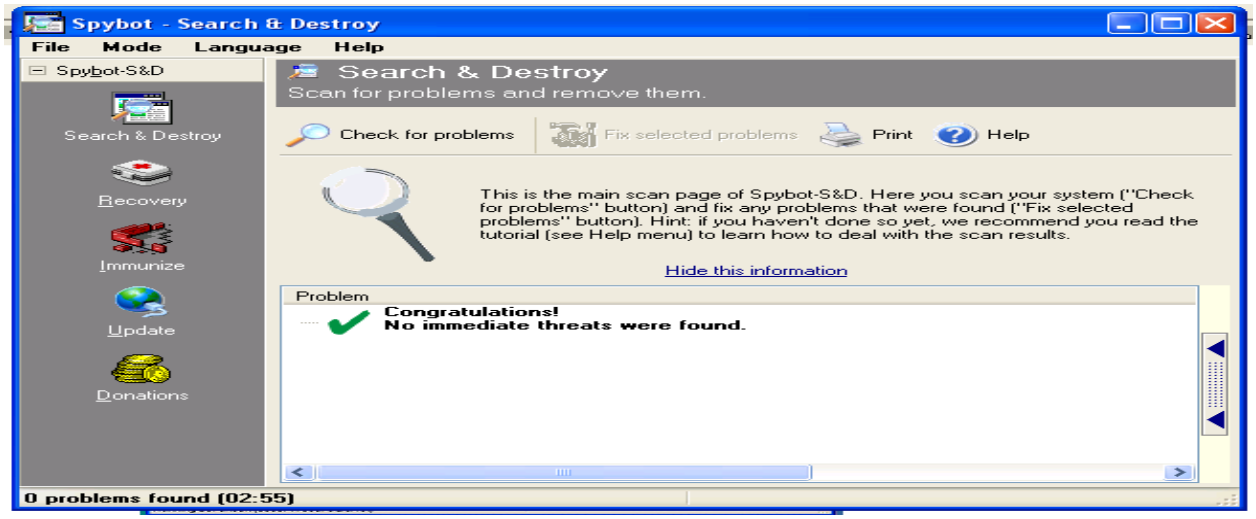


Fig. 21 No problem found

3.3 Recovery

If a user earlier removed something (but not purged) that is required to be restored, it can be done by using the Recovery option provided by Spybot-S&D. The Recovery screen appears at the right side after a user click on “Recovery” button at the left tool bar of the window (fig. 22-1). A list displays all entries that have been previously removed (and not purged or restored) from the system (fig. 22-2).

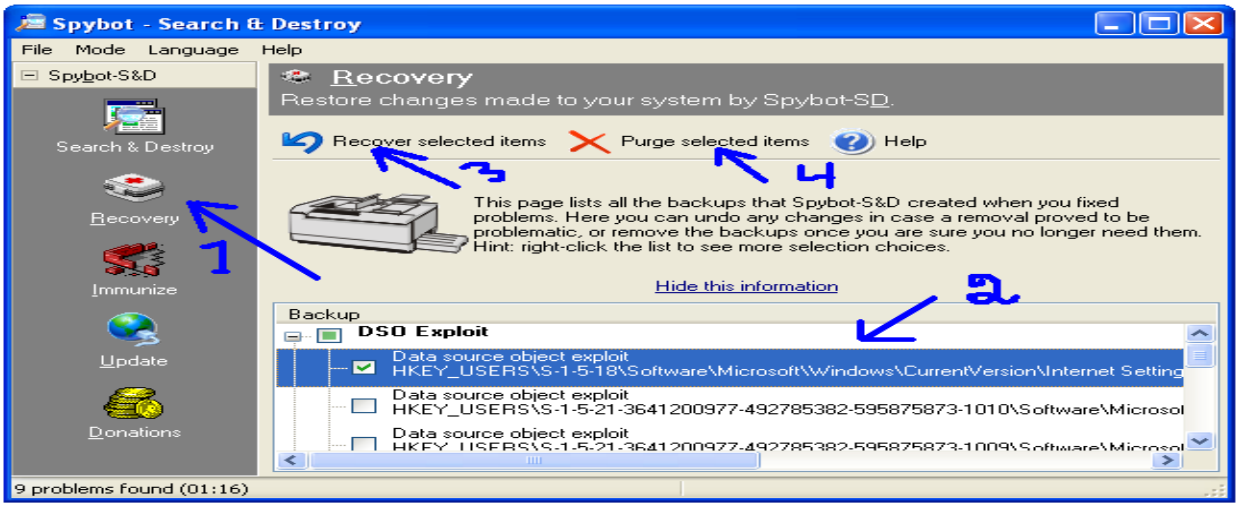


Fig. 22 Recovery screen

The entries that a user wants to restore are selected by clicking the checkbox before it. More selection options are available in the context menu that appears when a user right clicks on an entry (fig. 23). The context menu also allows a user to select a single item or whole products for restoration.

After the selection of the items, clicking on the button named as “Recover selected items” restored them (fig. 22-3). On clicking that button, a confirmation dialogue box appears (fig. 24) and upon confirmation by the user, the selected items are restored.

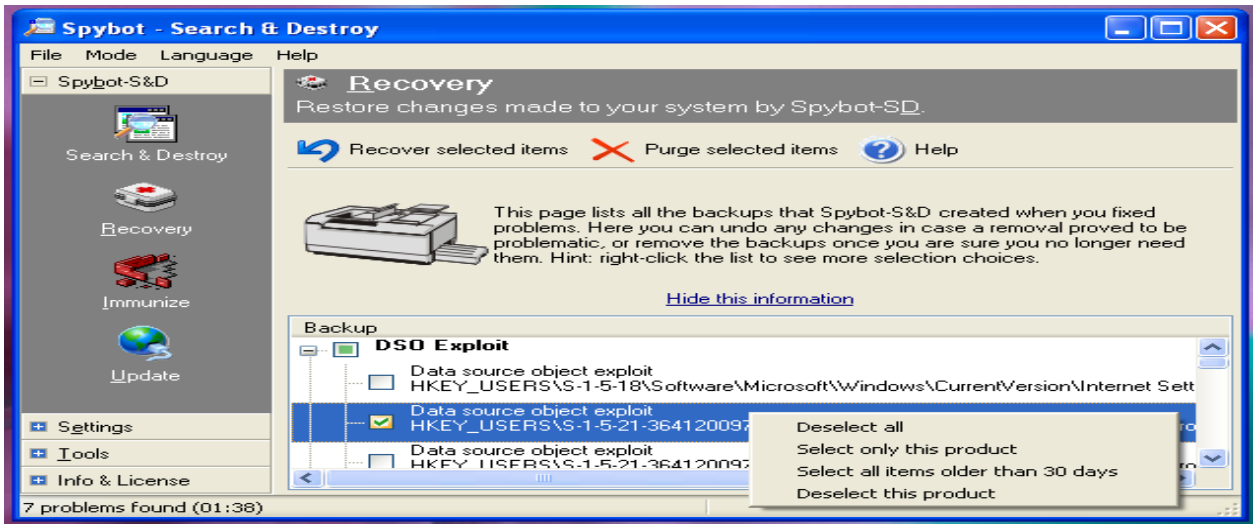


Fig. 23 Recovery context menu

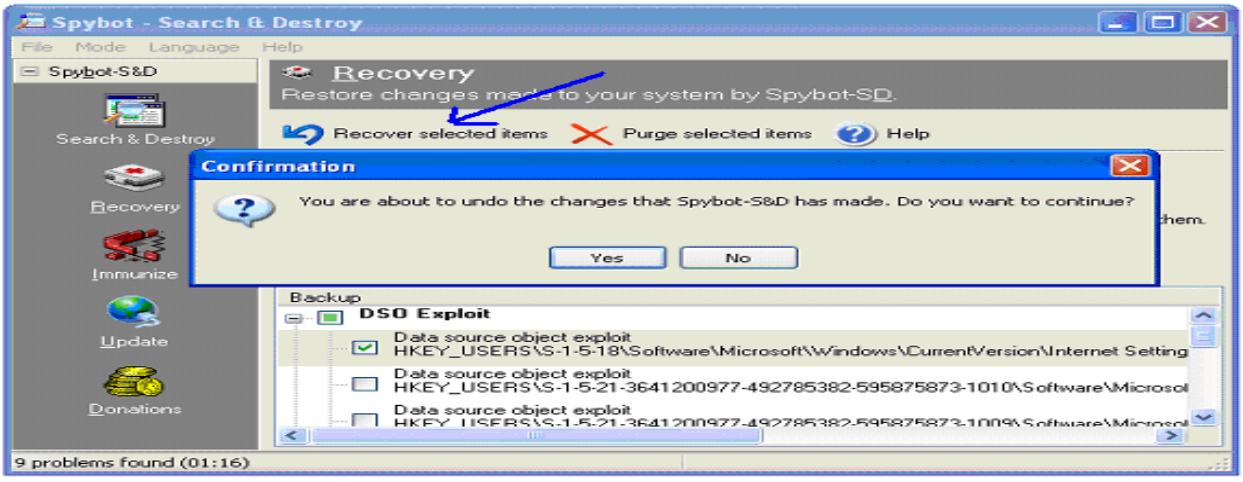


Fig. 24 Confirmation for the restoration of selected items

On the other hand, if the user decides to purge the selected items permanently from the system he/she does it by clicking on the button labeled as “Purge selected items” (fig. 22-4). A similar confirmation dialogue box appears (fig. 25) and upon confirmation from the user, the selected items are permanently purged from the system.

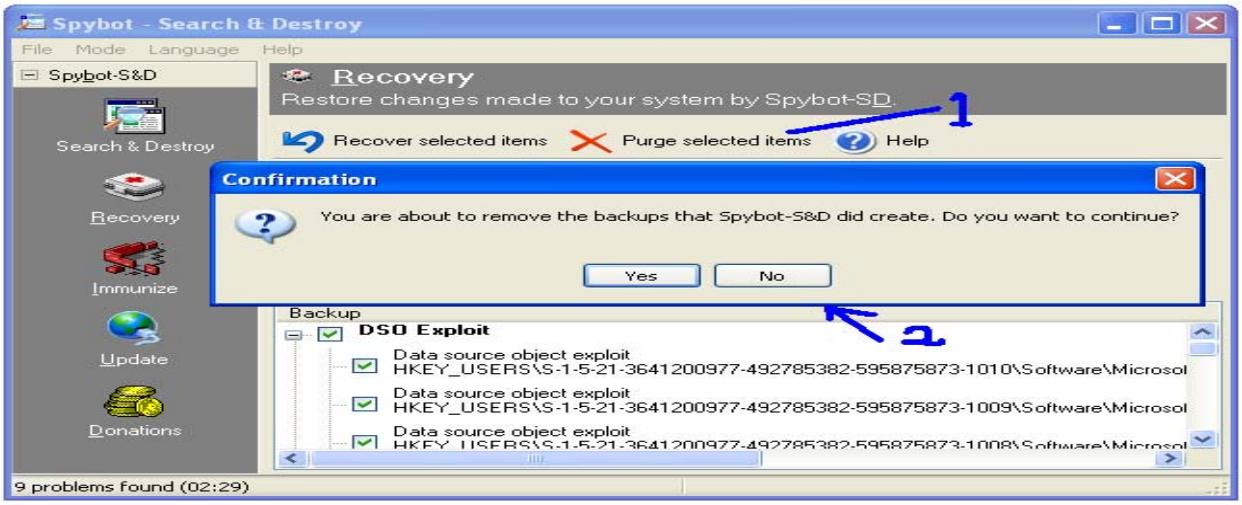


Fig. 25 Confirmation for purging the selected items

3.4 Immunize the system

Spybot-S&D offers for immunization of a computer system. The immunize screen appears at the right side of the window after a user click on “Immunize” button at the left tool bar of it’s window (fig. 26).

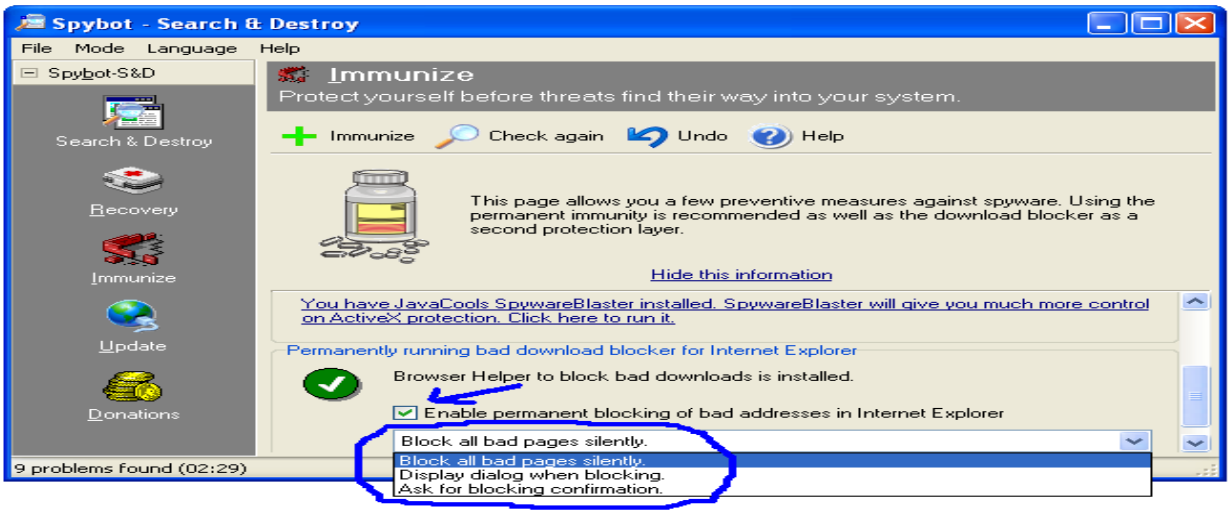


Fig. 26 The immunize screen

A drop down menu allows user to choose the way the program blocks the problem pages (fig. 26). Spybot-S&D, version 1.3 offers three different immunities:

- Permanent Internet Explorer immunity – allows tweaking some internal Internet Explorer settings to block the installation of known spyware installers.
- Permanently running bad download blocker for Internet Explorer - blocks anything that should come through by different aspects.

- Permanent Opera immunity - This list shows all Opera profiles, and the number of the plug-ins that are already blocked in each profile.

Clicking the Immunize button (fig. 27-1) or the “check again” button (fig. 28-1) checks for and shows in a dialogue box the number of bad processes already blocked (fig. 27-2) and the number of additional processes that can be blocked in the system.

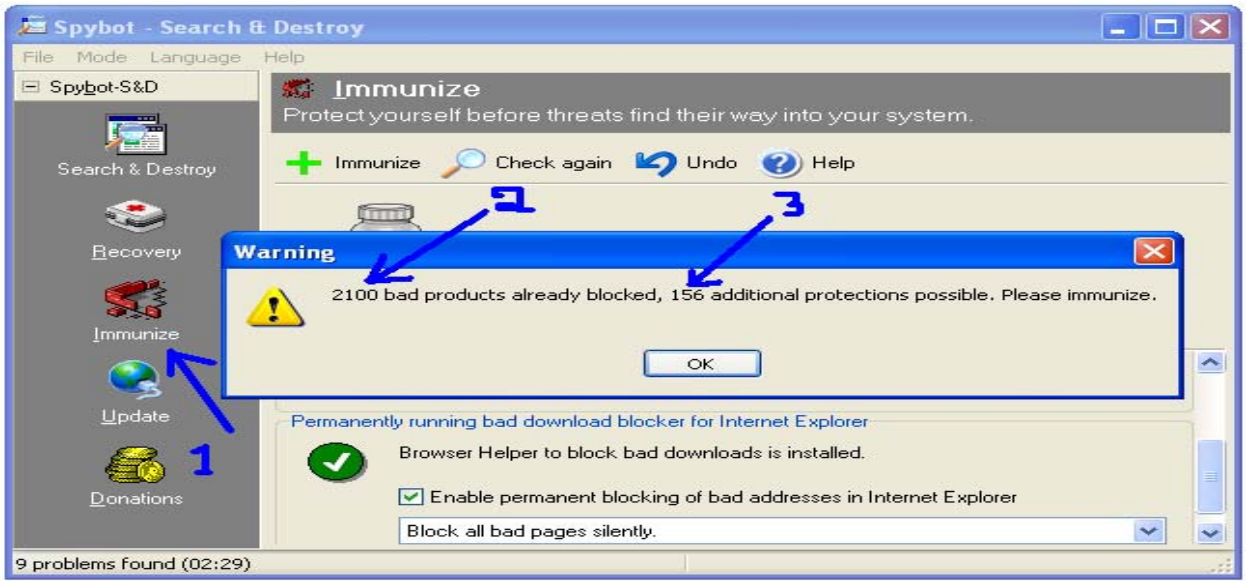


Fig. 27 Immunizing the system

Clicking immunize button (fig. 28-1) immunizes the system by blocking the additional bad processes. If there are no additional processes available to be blocked, clicking on the Immunize button (fig. 27-1) or the “check again” button (fig. 28-1) displays that information trough a dialogue box (fig. 28-3). After blocking, the user can revert it by clicking the “Undo” button (fig. 28-4).

Fig. 28 System immunized

3.5 Downloading and installing Updates

With the presence of an open Internet connection, Spybot downloads include files, newer help files, new languages, updated descriptions etc. using it's integrated update function. The update screen appears at the right side of the window after the user clicks on the "Update" button at the left tool bar of it's window (fig. 29-1) and he/she checks for the updates by clicking on "Search for updates" button (fig. 29-2). Upon clicking on this button, the program first connects to the update server (fig. 30) and downloads a list of updates from a PepiMK Software server.

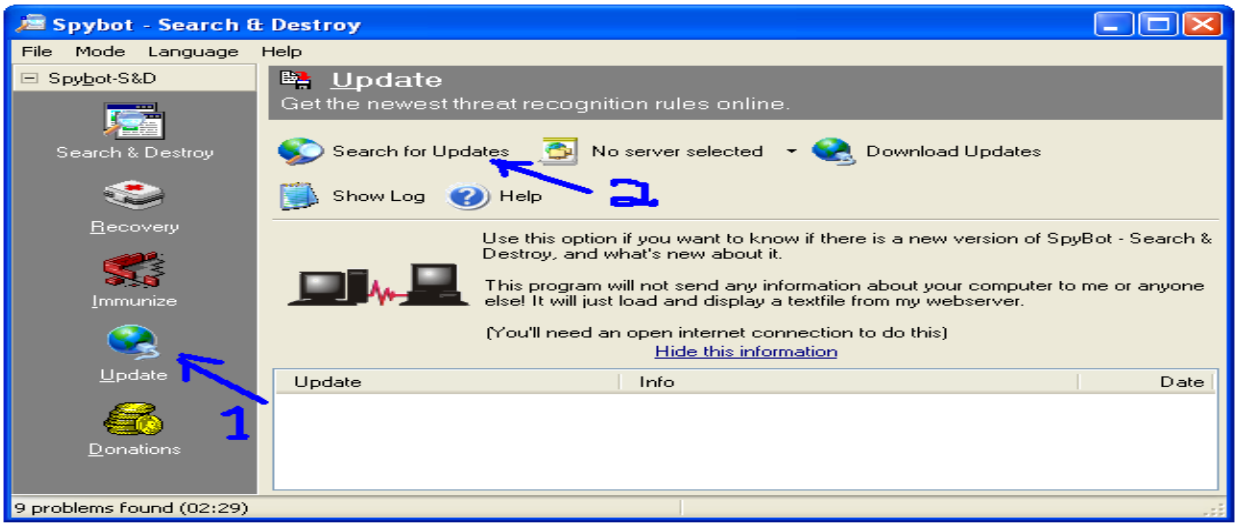


Fig. 29 The Update screen

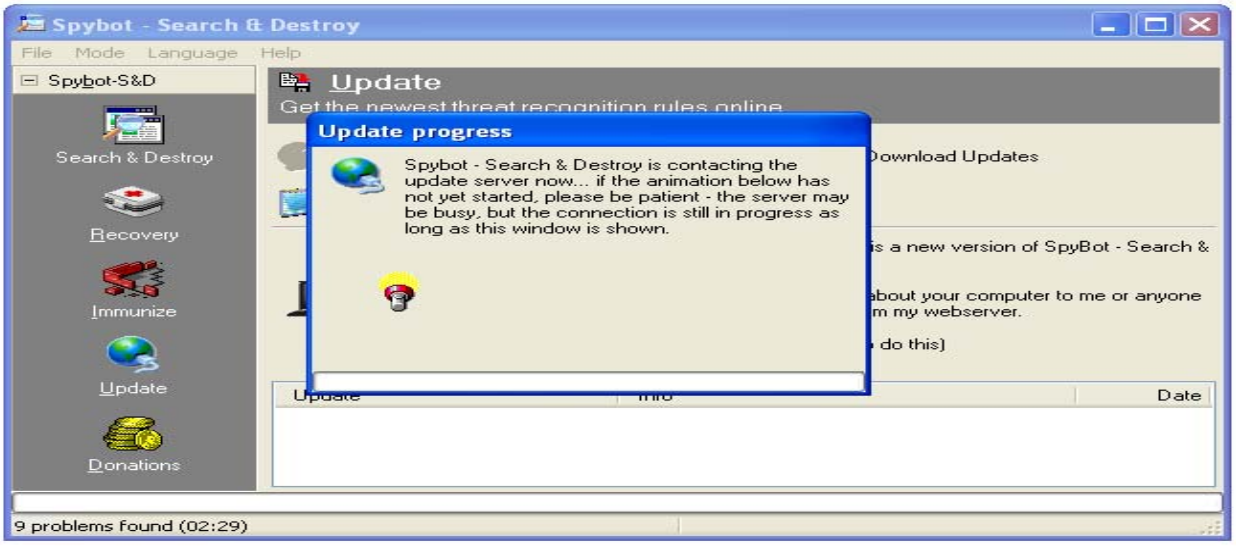


Fig. 30 Connecting the update server

The downloaded items are compared to the files already installed on the system and new files are shown in the list (fig. 31-1). The user selects the items for download by

checking the box before it (fig 31-1). The site from where the user wants to download is selected from the dropdown menu as shown in fig. 31-2. Once these are selected, the user downloads the updates by clicking on “Download updates” button (fig. 31-3). On clicking this button, the downloading begins and the progress is indicated in a dialogue box (fig. 32).

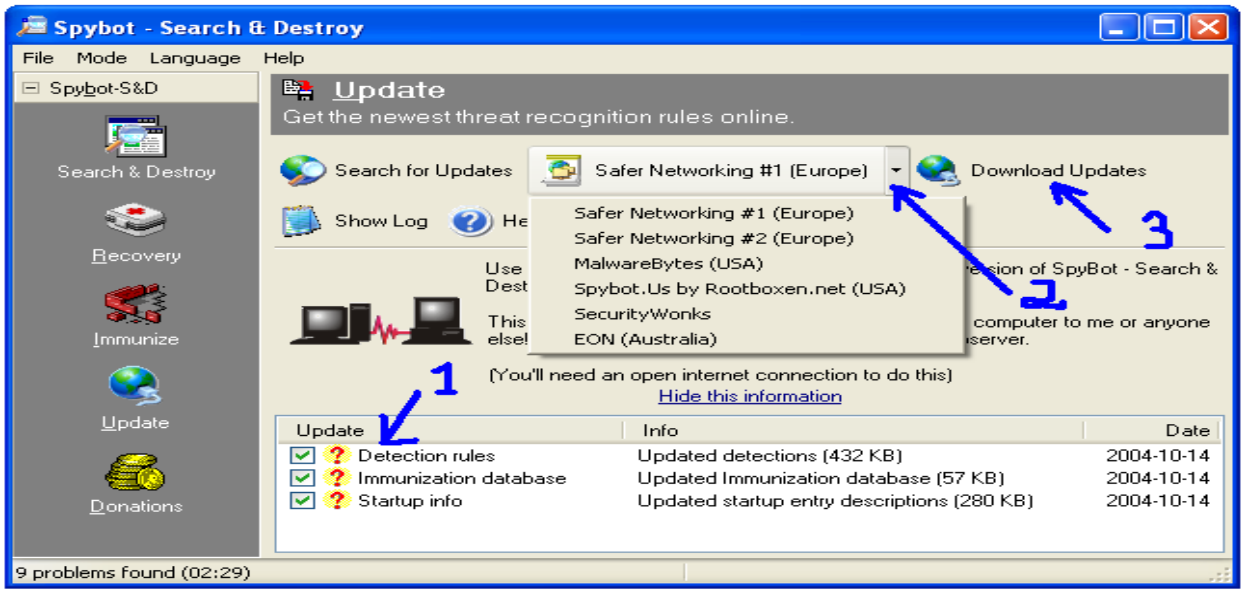


Fig. 31 Updates found

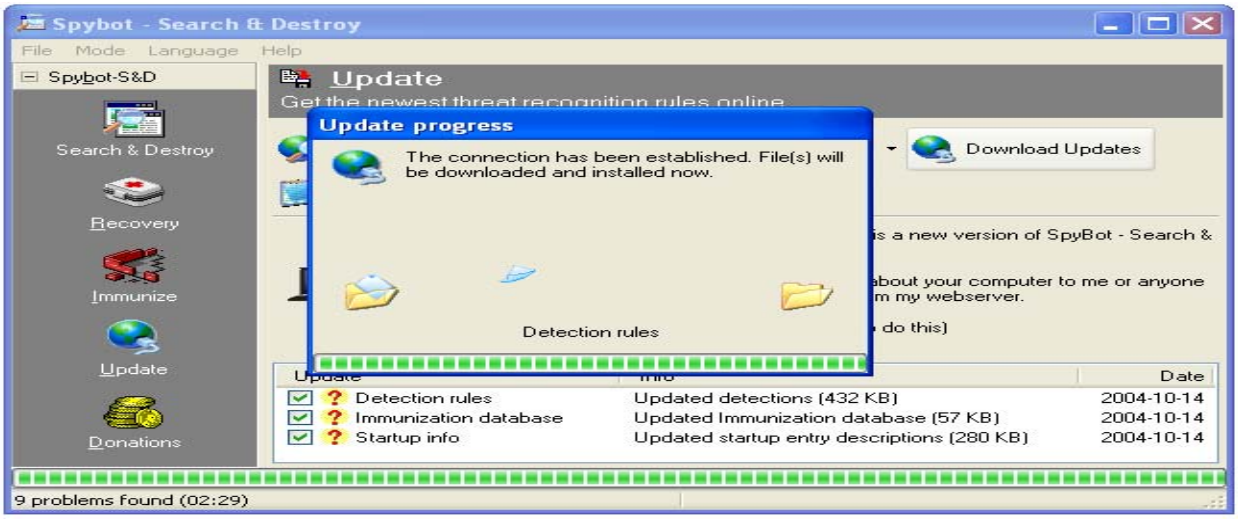


Fig. 32 Downloading updates

During the download, every finished file gets a green check mark (fig. 33). The description of the updates are available in the website of Spybot-S&D for user to read before download, if desired so. After the download, the user can view the update log by clicking on “Show log” button (fig. 33). A typical content of the log is shown in fig. 34.

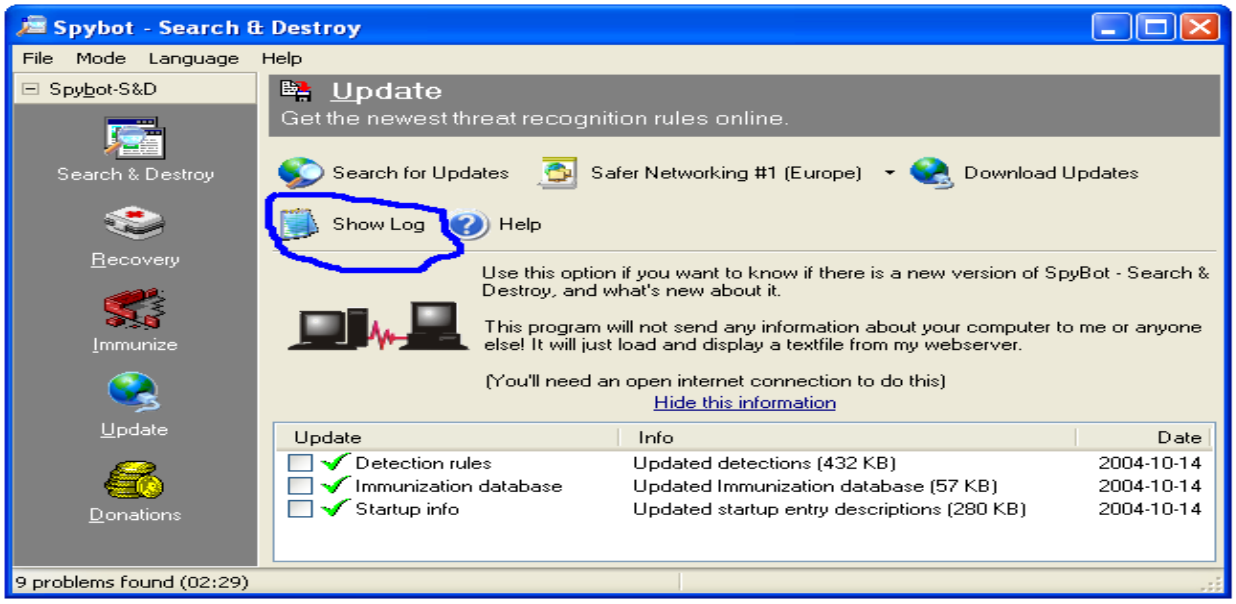


Fig 33 Updates downloaded

```
9/28/2004 10:05:32 PM Downloaded update info file. (http://security.kolla.de/updates/spybotsd.ini)
9/28/2004 10:06:07 PM downloaded update Detection rules
9/28/2004 10:06:07 PM  - URL: http://www.spybotupdates.com/updates/files/includes.zip
9/28/2004 10:06:07 PM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\includes.zip
9/28/2004 10:06:09 PM downloaded update English help
9/28/2004 10:06:09 PM  - URL: http://www.spybotupdates.com/updates/files/help.english.zip
9/28/2004 10:06:09 PM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\help.english.zip
9/28/2004 10:06:10 PM downloaded update English help for TeaTimer
9/28/2004 10:06:10 PM  - URL: http://www.spybotupdates.com/updates/files/helpres.english.zip
9/28/2004 10:06:10 PM  - Local file: C:\Program Files\Spybot - Search &
Destroy\Updates\helpres.english.zip
9/28/2004 10:06:11 PM downloaded update Immunization database
9/28/2004 10:06:11 PM  - URL: http://www.spybotupdates.com/updates/files/clsid.zip
9/28/2004 10:06:11 PM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\clsid.zip
10/5/2004 5:48:59 AM Downloaded update info file. (http://security.kolla.de/updates/spybotsd.ini)
10/5/2004 5:50:16 AM downloaded update Detection rules
10/5/2004 5:50:16 AM  - URL: http://www.spybot.us/~updates/updates/files/includes.zip
10/5/2004 5:50:16 AM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\includes.zip
10/5/2004 5:50:17 AM downloaded update English help
10/5/2004 5:50:17 AM  - URL: http://www.spybot.us/~updates/updates/files/help.english.zip
10/5/2004 5:50:17 AM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\help.english.zip
10/6/2004 9:43:43 PM Downloaded update info file. (http://security.kolla.de/updates/spybotsd.ini)
10/16/2004 1:13:45 AM Downloaded update info file. (http://security.kolla.de/updates/spybotsd.ini)
10/16/2004 1:18:21 AM downloaded update Detection rules
10/16/2004 1:18:21 AM  - URL: http://www.spybotupdates.biz/updates/files/includes.zip
10/16/2004 1:18:21 AM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\includes.zip
10/16/2004 1:18:22 AM downloaded update Immunization database
10/16/2004 1:18:22 AM  - URL: http://www.spybotupdates.biz/updates/files/clsid.zip
10/16/2004 1:18:22 AM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\clsid.zip
10/16/2004 1:18:24 AM downloaded update Startup info
10/16/2004 1:18:24 AM  - URL: http://www.spybotupdates.biz/updates/files/startup.zip
10/16/2004 1:18:24 AM  - Local file: C:\Program Files\Spybot - Search & Destroy\Updates\startup.zip
```

Fig 34 Content of a sample update log

4 The Expert Setting of Spybot-S&D

This section describes the additional options and expert configuration of Spybot-S&D that are available in advanced mode.

4.1 The Advanced Mode

Spybot-S&D offers more options and expert configuration in advance mode, which is activated by selecting the “Advanced mode” option in the mode menu from the top menu bar (fig. 35-1). Upon selection of this mode, three new buttons, labeled as “Setting”, “Tools” and “Info & License”, appear in the left tool bar of the window (fig. 35-2).

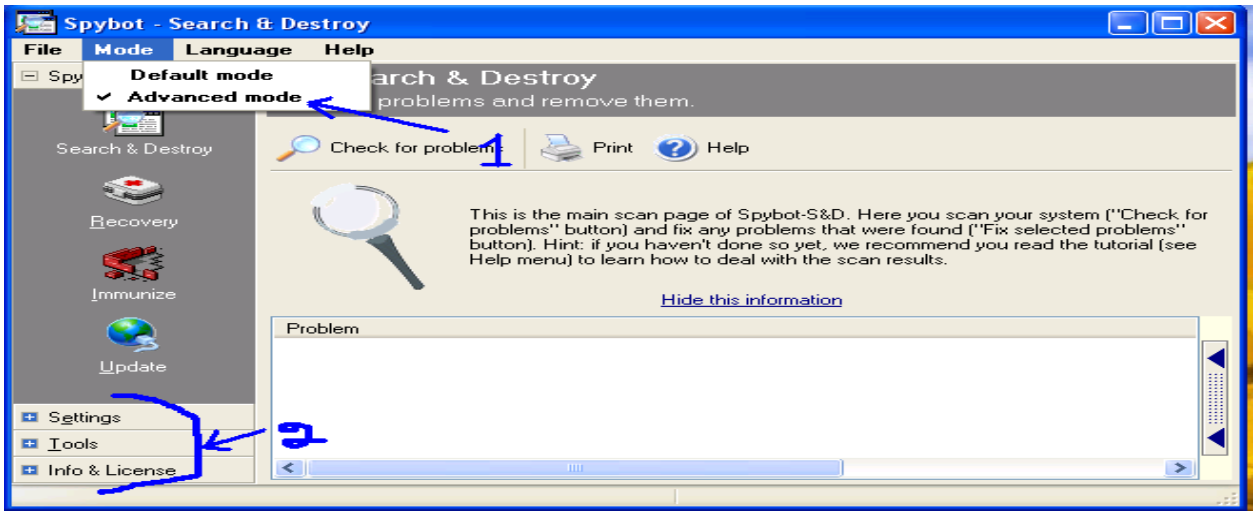


Fig 35 The advanced mode

4.2 The Setting Options

Clicking on setting button (fig. 35) expands it to some other buttons, which provides access to some additional options (fig. 36).

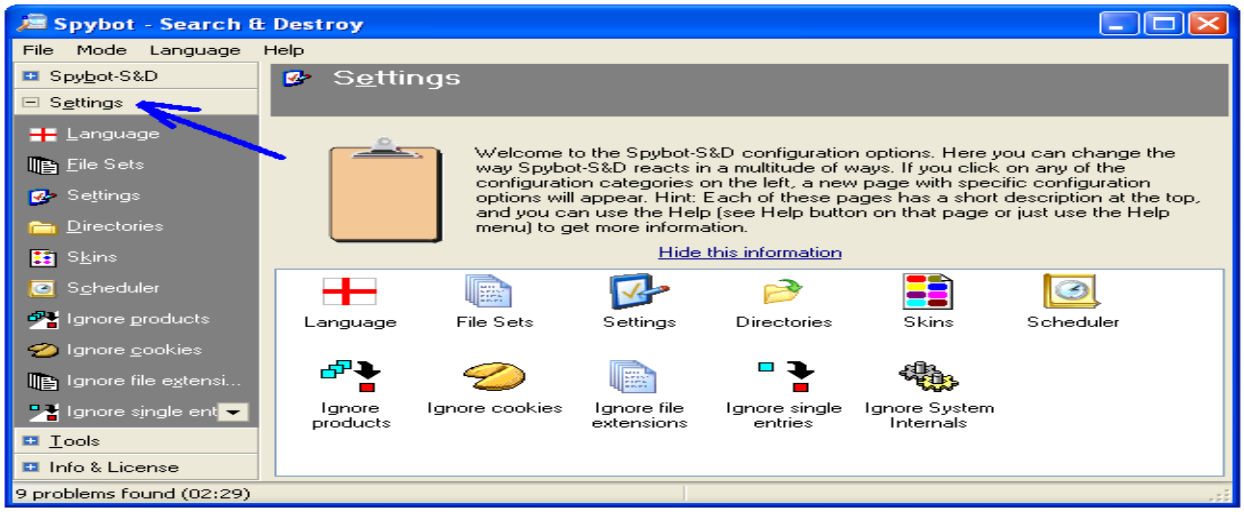


Fig. 36 Expanding the setting button

4.2.1 Languages

Spybot-S&D is available in many languages. User can choose a language by clicking the “Language” button (fig. 37-1) and then selecting a language from the list.

4.2.2 File Sets

File sets include what a user wants to scan. The sets are displayed in the list by clicking the File Sets button (fig. 37-2). Spybot-S&D uses the concept of Include Files where each file containing the description of some problems that Spybot-S&D can detect and fix. These files are divided into categories, so a user can select what he/she wants to target during the scan.

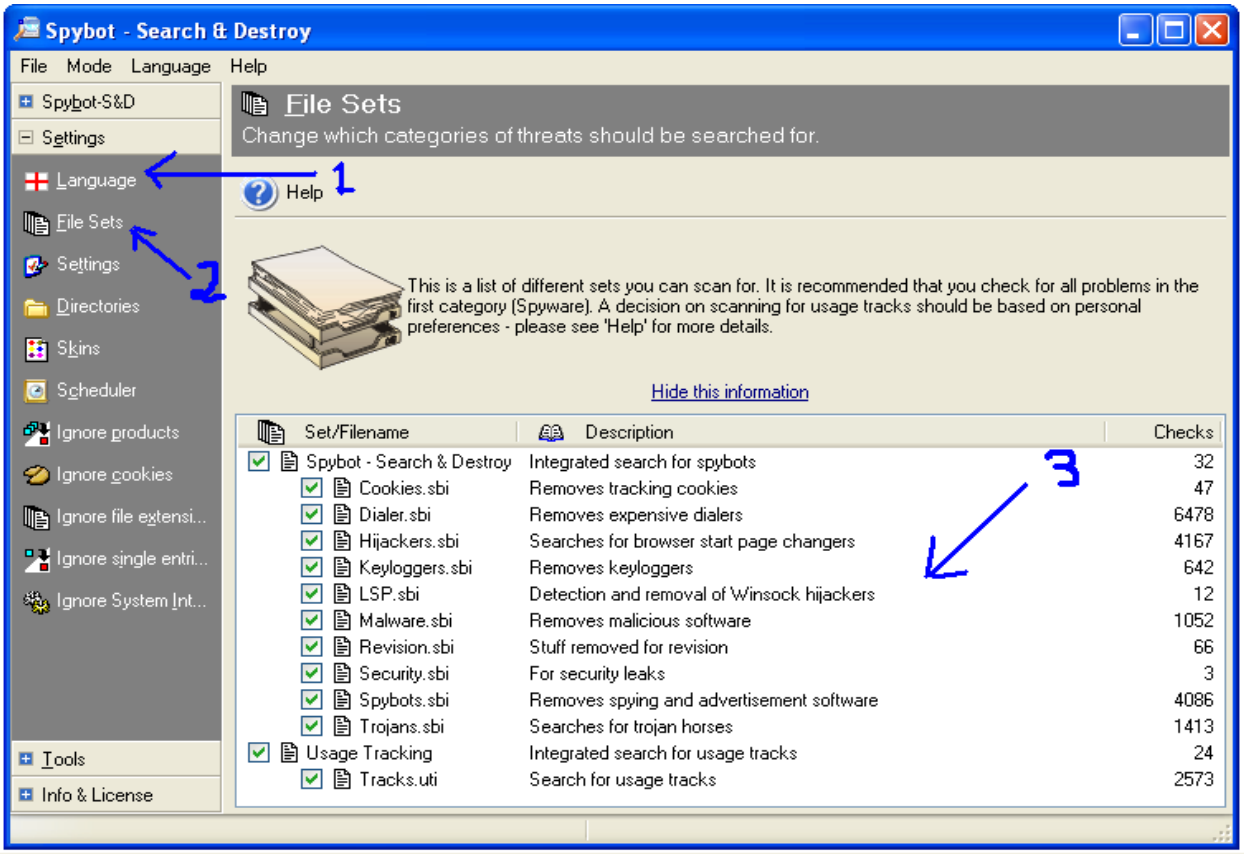


Fig. 37 Language and File sets

The basic categories are "Spybot-Search & Destroy" (contains files for spyware and adware) and usage tracks. For each category, Include Files are shown with a short description on what they do, and the number of files, registry entries and directories that are checked (fig. 37-3). A user can select which Include Files to use for the next scan by toggling the checkbox next to it [5].

4.2.3 Setting the Basic Options

The settings for the basic options are displayed by clicking the “Setting” button in the left tool bar of the program window (fig. 38-1). Important settings are listed in a tree in this section (fig 38-4). Users can select/deselect an option by toggling the checkbox next to it. Default options can be reset by clicking on the “Defaults” button (fig 38-2). Clicking the “Wizard” button (fig 38-3) pop ups the basic setting wizard shown in fig. 6 – 10.

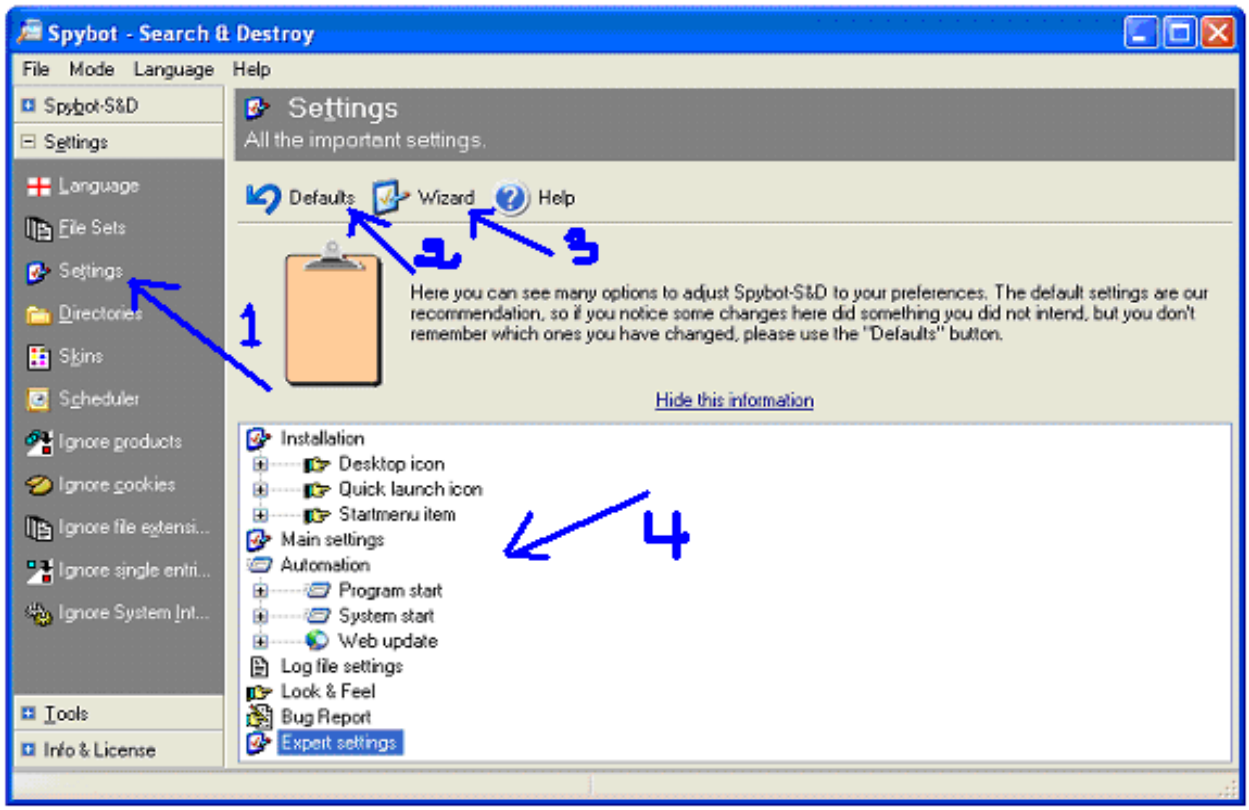
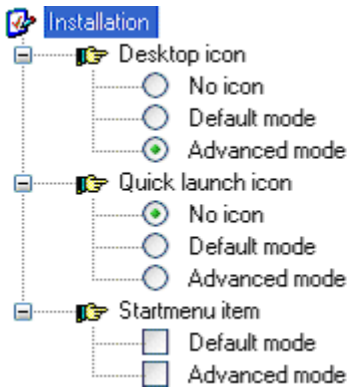
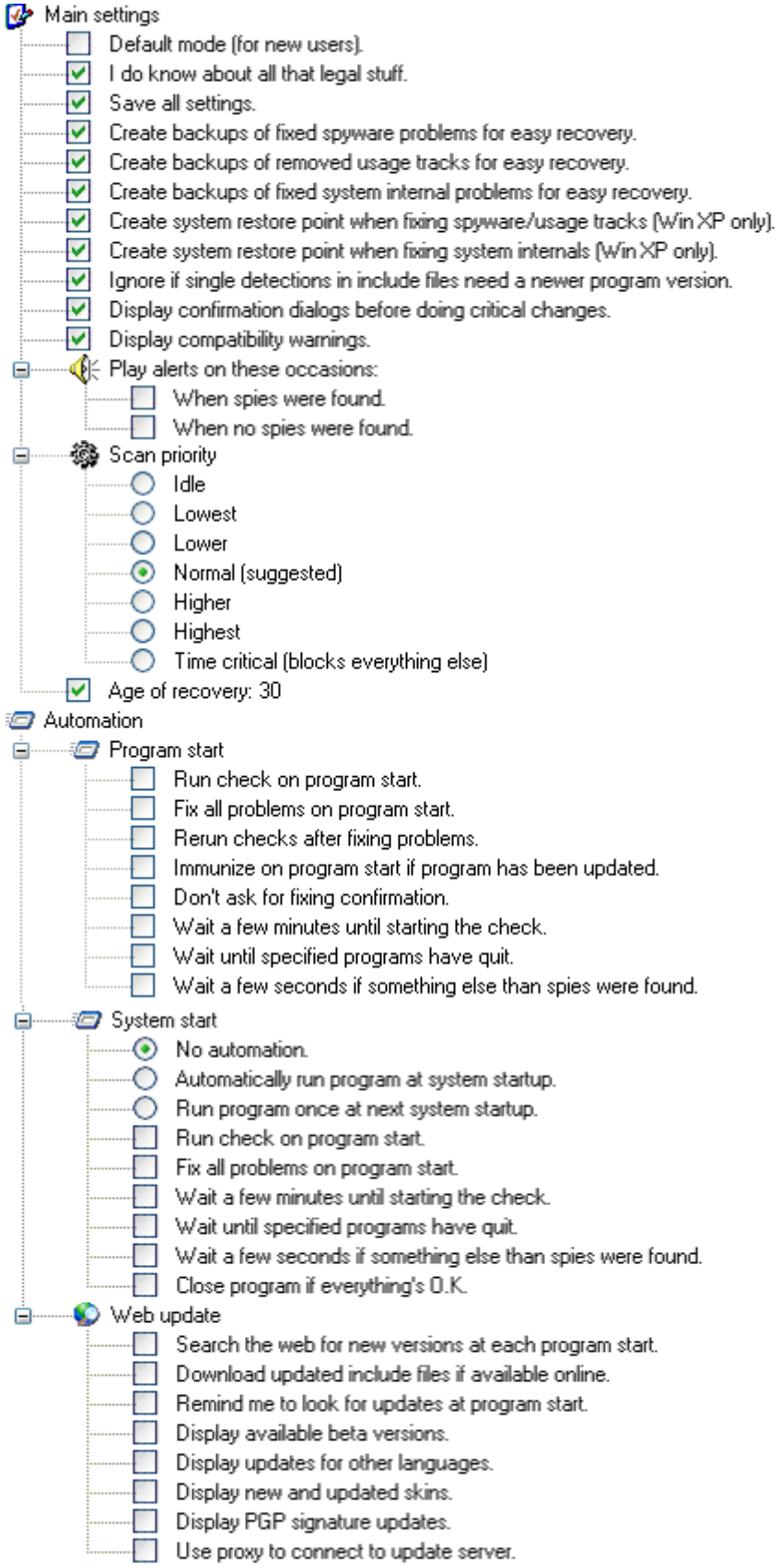
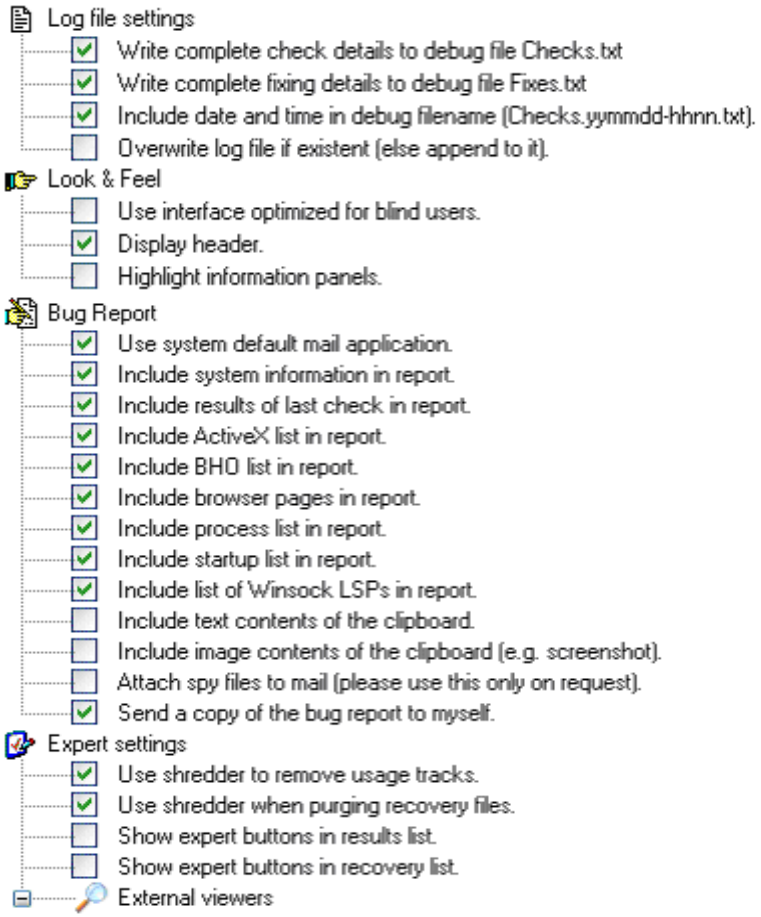


Fig. 38 Setting the basic options

The program provides options for the following settings (copied from the “Settings” screen of the program):




Main settings
Default mode (for new users).
I do know about all that legal stuff.
Save all settings.
Create backups of fixed spyware problems for easy recovery.
Create backups of removed usage tracks for easy recovery.
Create backups of fixed system internal problems for easy recovery.
Create system restore point when fixing spyware/usage tracks (Win XP only).
Create system restore point when fixing system internals (Win XP only).
Ignore if single detections in include files need a newer program version.
Display confirmation dialogs before doing critical changes.
Display compatibility warnings.
Play alerts on these occasions:
When spies were found.
When no spies were found.
Scan priority
Idle
Lowest
Lower
Normal (suggested)
Higher
Highest
Time critical (blocks everything else)
Age of recovery: 30
Automation
Program start
Run check on program start.
Fix all problems on program start.
Rerun checks after fixing problems.
Immunize on program start if program has been updated.
Don't ask for fixing confirmation.
Wait a few minutes until starting the check.
Wait until specified programs have quit.
Wait a few seconds if something else than spies were found.
System start
No automation.
Automatically run program at system startup.
Run program once at next system startup.
Run check on program start.
Fix all problems on program start.
Wait a few minutes until starting the check.
Wait until specified programs have quit.
Wait a few seconds if something else than spies were found.
Close program if everything's O.K.
Web update
Search the web for new versions at each program start.
Download updated include files if available online.
Remind me to look for updates at program start.
Display available beta versions.
Display updates for other languages.
Display new and updated skins.
Display PGP signature updates.
Use proxy to connect to update server.



4.2.4 Setting Downloads Directories

Directories screen appears after a user clicks on the Directories button (fig. 39-1). Download directories can be added by “Drag-and-drop” them from Windows Explorer or by using the context menu (fig. 39-2). Installers that the user must explicitly start downloading will only be scanned for in the directories entered into this list [5].

Fig. 39 Setting download directories

4.2.5 Skins - Setting Color Appearance

The Skins screen appears after a user clicks on the “Skins” button (fig. 40). This screen is used to set the colors in which Spybot-S&D appears.

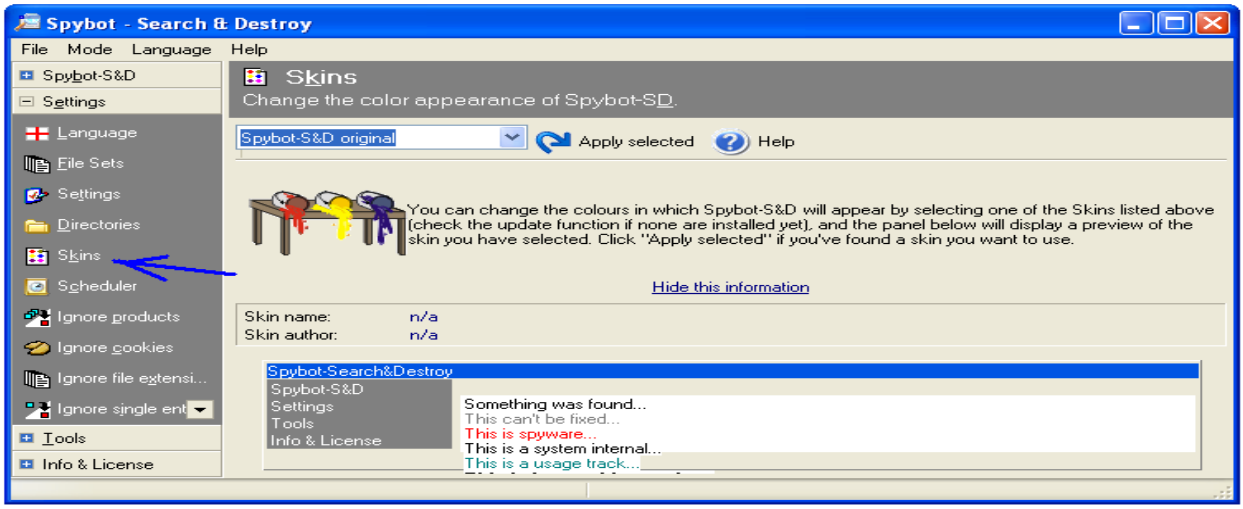


Fig. 40 Skins - Setting Color Appearance

4.2.6 The Scheduler

The Scheduler screen appears after a user clicks on the “Scheduler” button (fig. 41). The Scheduler page allows for adding an entry to automatically run. This is done by first clicking on the Add button, and then by setting the necessary properties (scheduled time etc.) through the Edit button (fig. 41). A task can be removed using the Remove button. Customization options are offered through checkboxes to decide if the user wants to fix problems automatically and to close the program. The Edit button opens the default Windows task properties dialog, so that the user can change the task like any other Windows Scheduler task (fig. 42) [5].

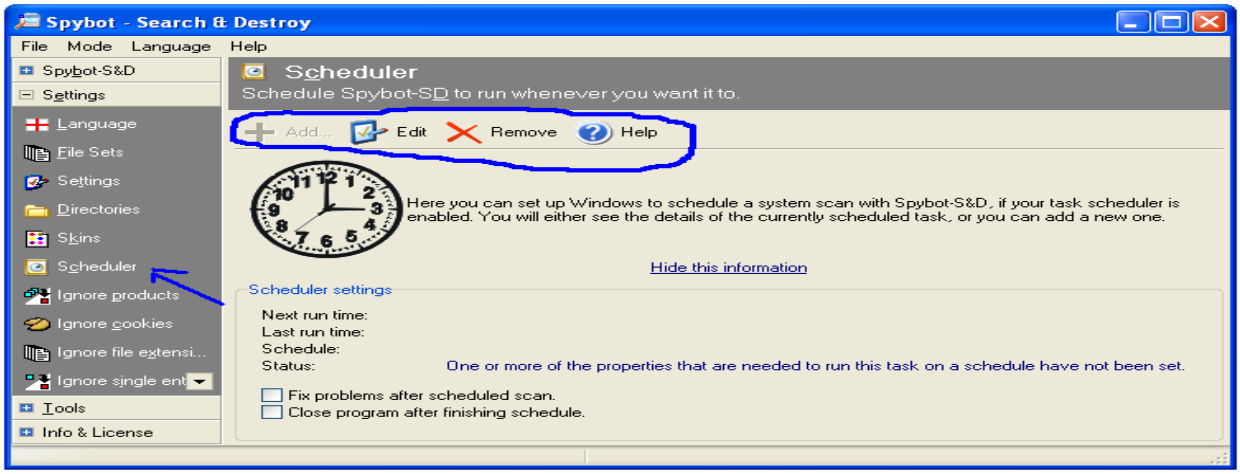


Fig. 41 The Scheduler

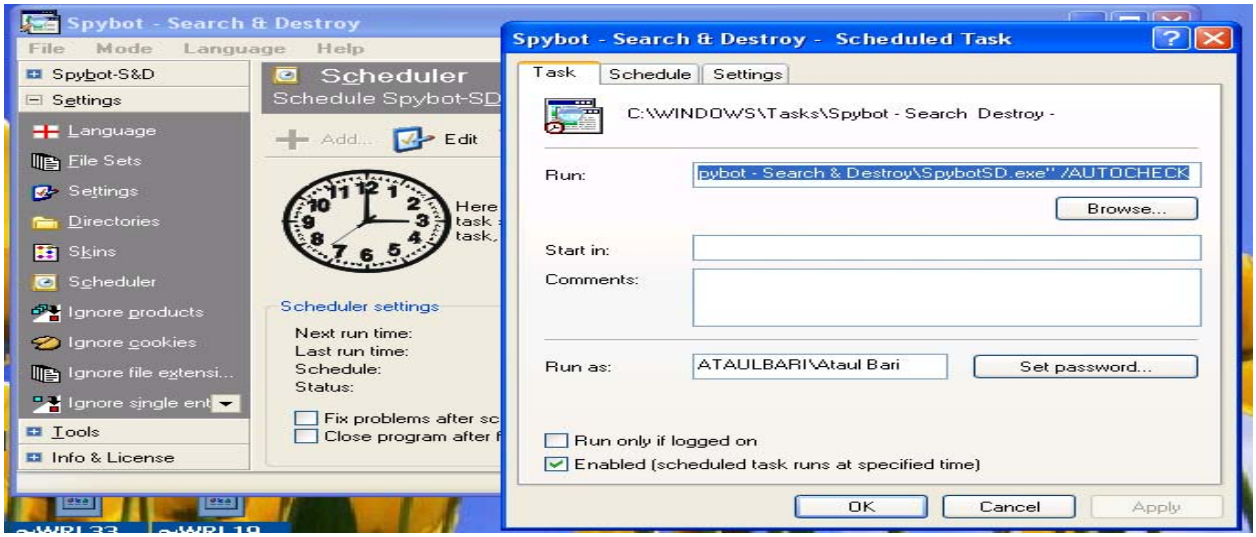


Fig 42 The Scheduler – Edit window

4.2.7 Ignore Products

The Ignore products screen appears after a user clicks on the “Ignore products” button (fig. 43). This section lists all products defined internally and in the external Include Files. If a user wants to exclude a complete product, or include it again, he/she can do it by selecting the file from this section and toggle the checkbox before the product. [5]

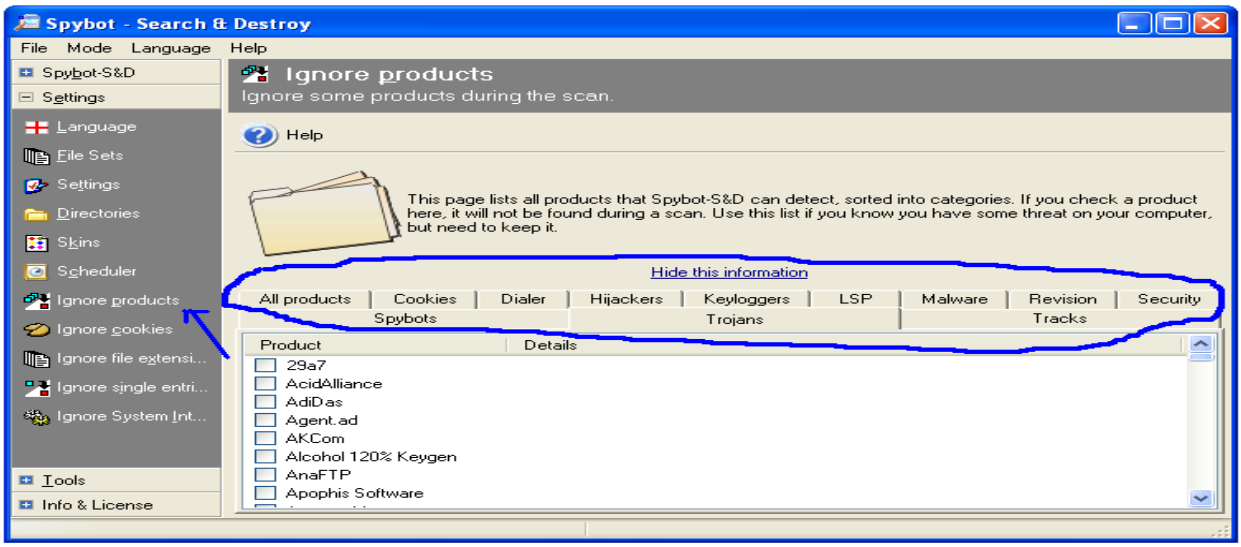


Fig. 43 Ignore Products

4.2.8 Ignore Cookies

The Ignore cookies screen appears after a user clicks on the “Ignore cookies” button (fig. 44). If a user wants to keep some useful cookies, he/she can do so from here as this section lists all cookies currently on system, allowing the user to exclude them from further searches.

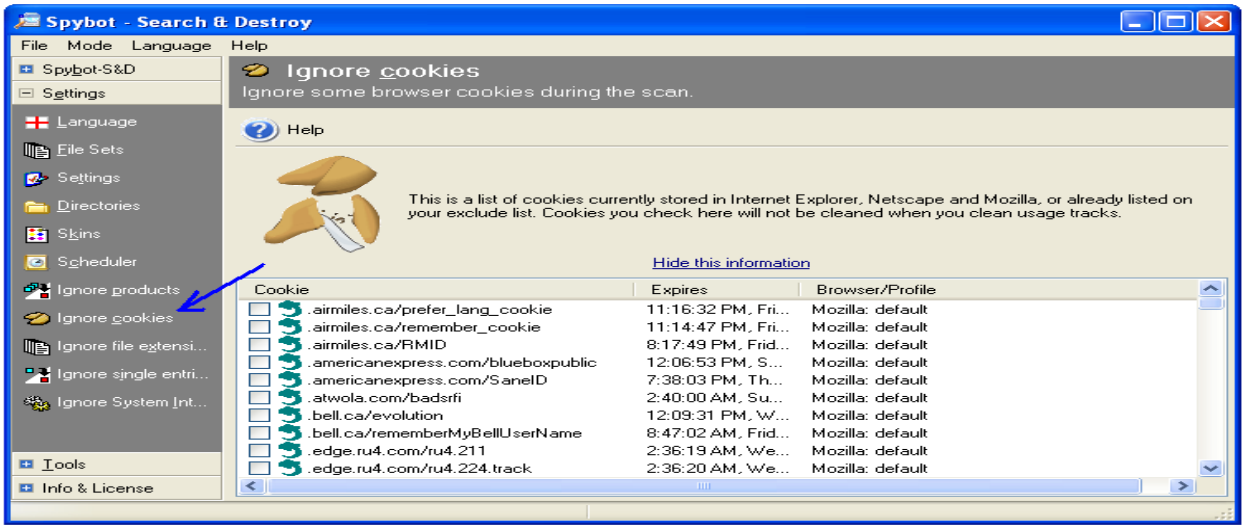


Fig. 44 Ignore cookies

4.2.9 Ignore File Extensions

The Ignore file extensions screen appears after a user clicks on the “Ignore file extensions” button (fig. 45). This section saves lists of opened (and saved) files divided into extensions. For example, if a user does not want to remove common text files, he/she could select *.txt* to be excluded in this section. [5]

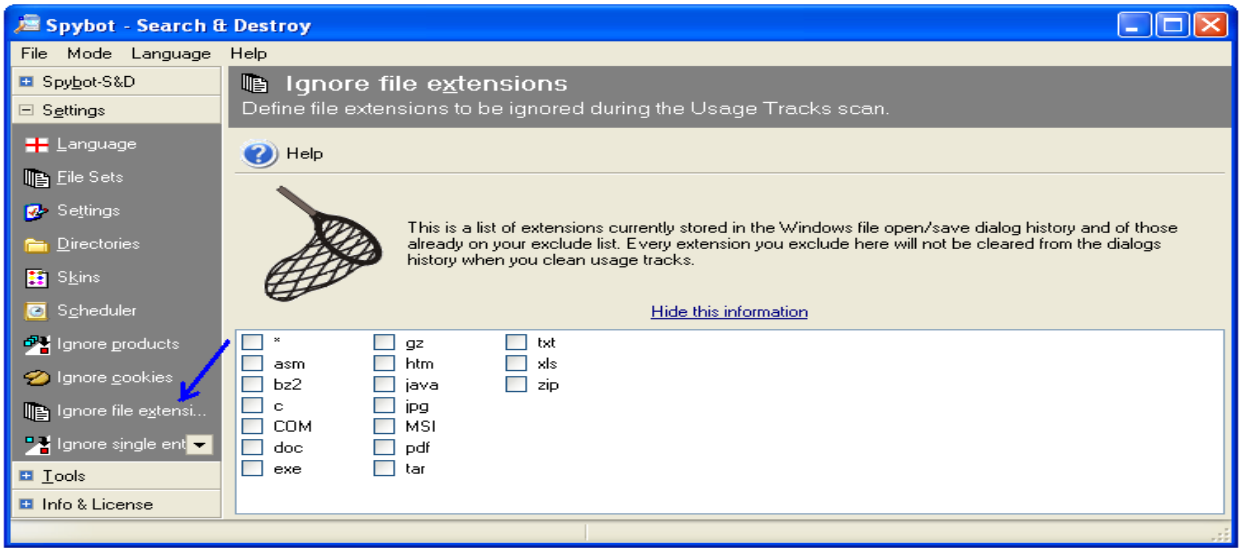


Fig 45 Ignore File Extensions

4.2.10 Ignore Single Entries

The Ignore single entries screen appears after a user clicks on the “Ignore single entries” button (fig. 46). If a user does not want to exclude a complete product, but only a single file or registry setting of it, he/she can select that one from the results list. [5]

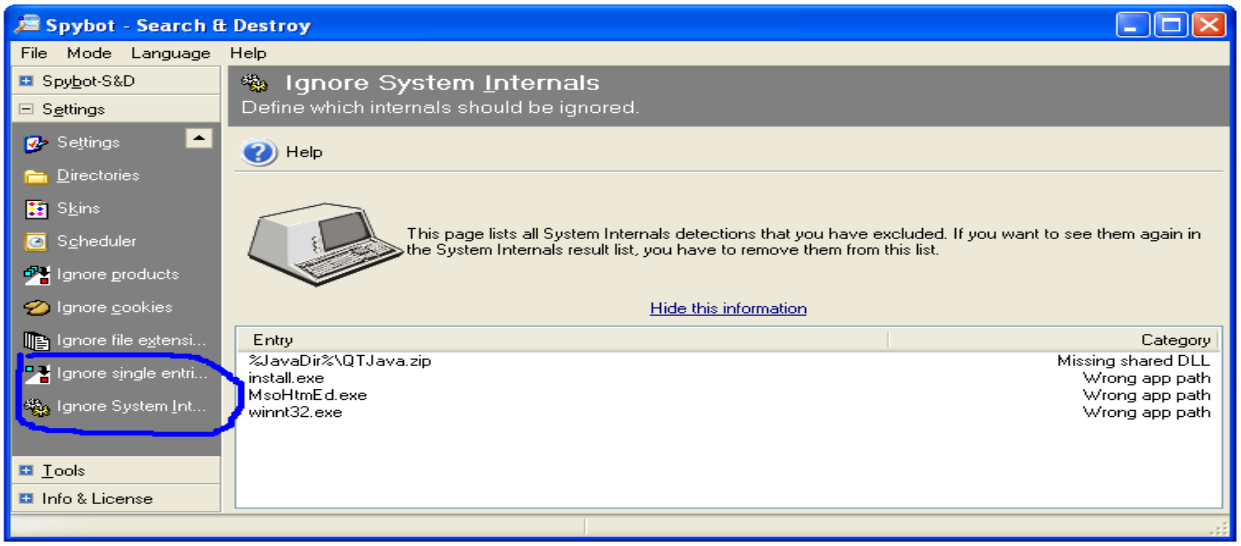


Fig 46 Ignore single entries and System Internals

4.2.11 Ignore Single Entries

The Ignore system internals screen appears after a user clicks on the “Ignore System Internals” button (fig. 46). If a user have put System Internals results on the ignore list, he/she can remove them (from the ignore list) here. [5]

4.3 The Tools Options

Clicking on “Tools” button (fig. 47) expands it to some other buttons, which provides access to some additional options as shown in fig. 47.

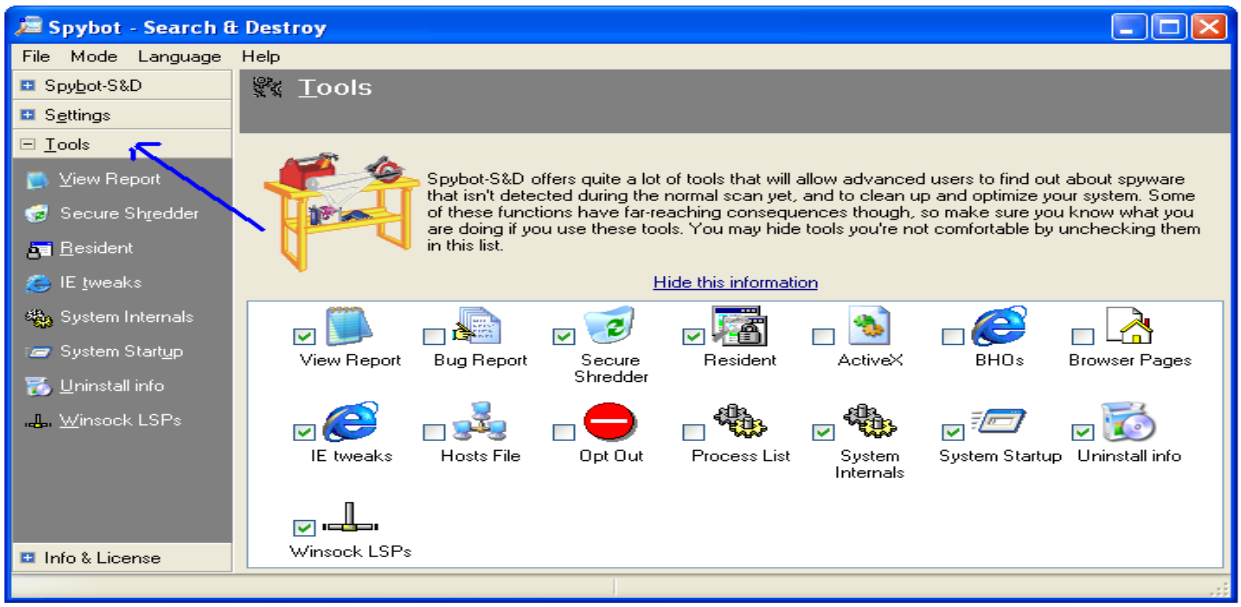


Fig. 47 The tools screen

4.3.1 View Report

The View report screen appears after a user clicks on the “View report” button (fig. 48). This tool allows a user to create a new report including all (or just a selection of the reports that Spybot-S&D can create). The report can be saved into a file for future reference (fig. 49 using export button). The tool also allows a user to view old reports again using the “View previous report” button (fig. 48).

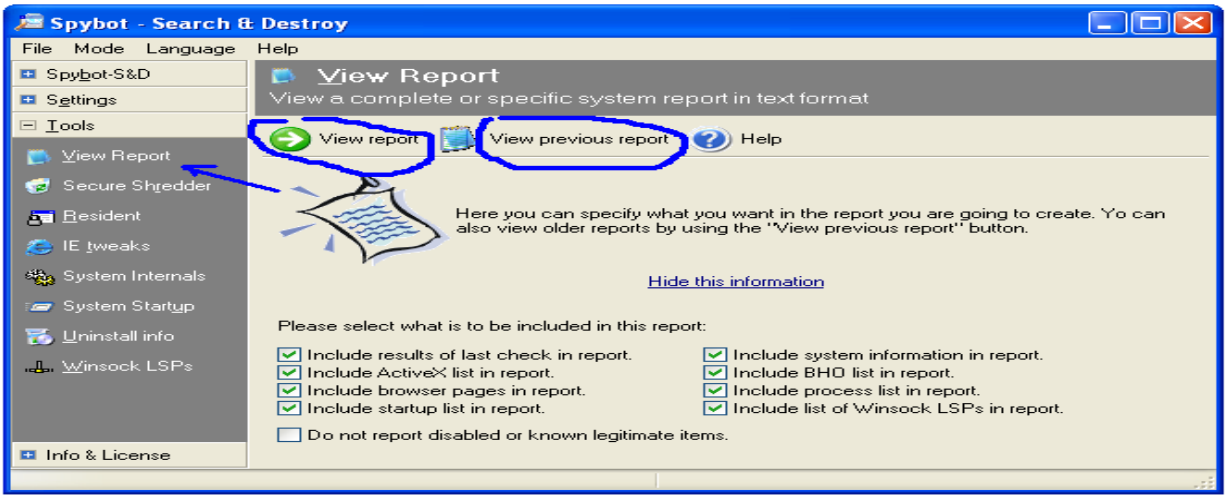


Fig 48 View report

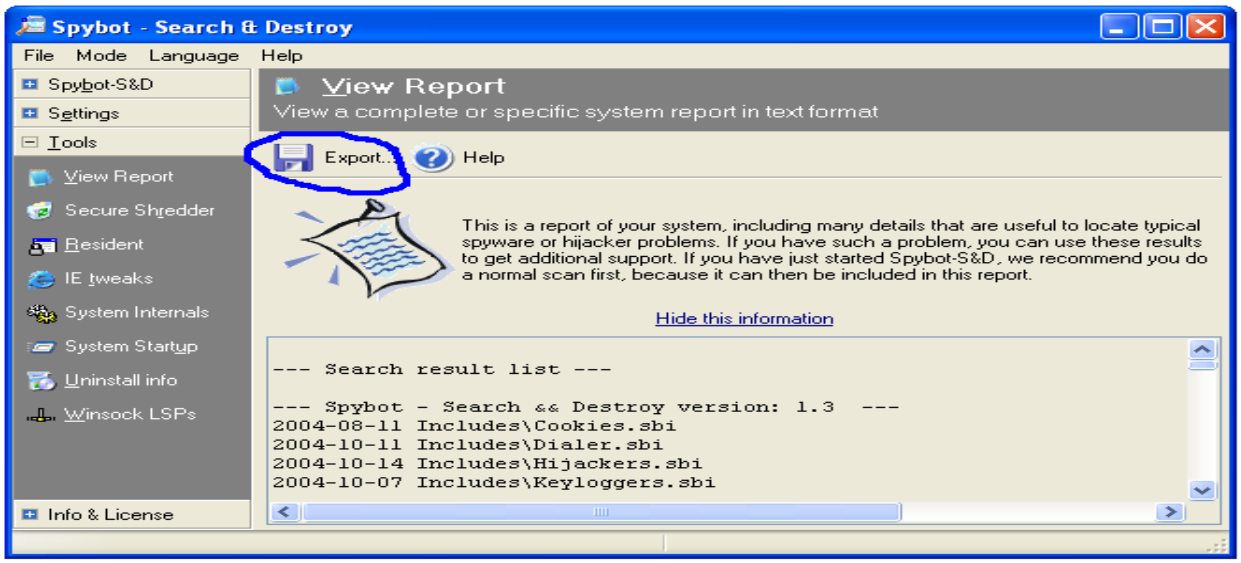


Fig 49 View report – save report

4.3.2 Secure Shredder

The Secure Shredder screen appears after a user clicks on the “Secure Shredder” button (fig. 50-1). It is a tool to get rid of files permanently, without any further possibilities of recovery. Files to be shredded are added in the list (fig. 50-3) using the drop down menu labeled as “Templates” (fig. 50-2). User can also drop some files from the windows

explorer into the list or may use context menu of the list (fig. 50-6). He/she then selects the number of shreds (fig. 50-4) and clicks on “Chop it away button” (fig. 50-5) to shred them.

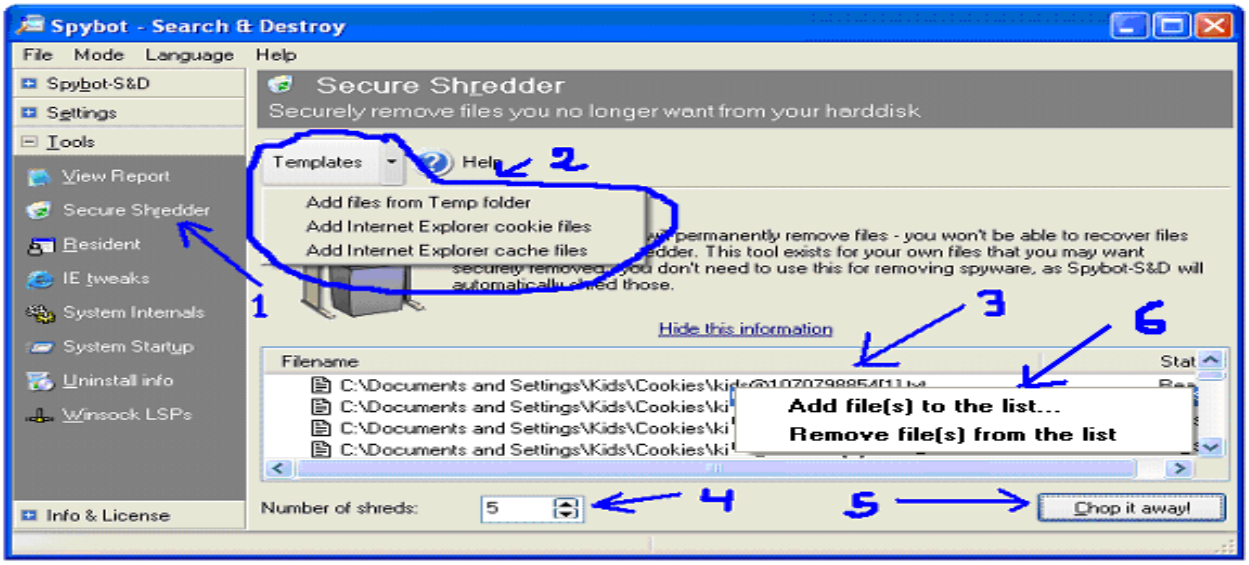


Fig. 50 Secure Shredder

4.3.3 Resident Tool

The Resident screen appears after a user clicks on the “Resident” button (fig. 51). Resident is a permanently running application to protect the system. It consists of a browser helper for Internet Explorer that blocks download of files known as malicious. Fig. 52 a & c and fig. 53 capture some screenshots for Spybot-S&D Resident while in action. The resident icon (fig. 52-b) can be used to get information on the number of blocked processes and the context menu (fig. 52-d) can be used to set options for this tool.

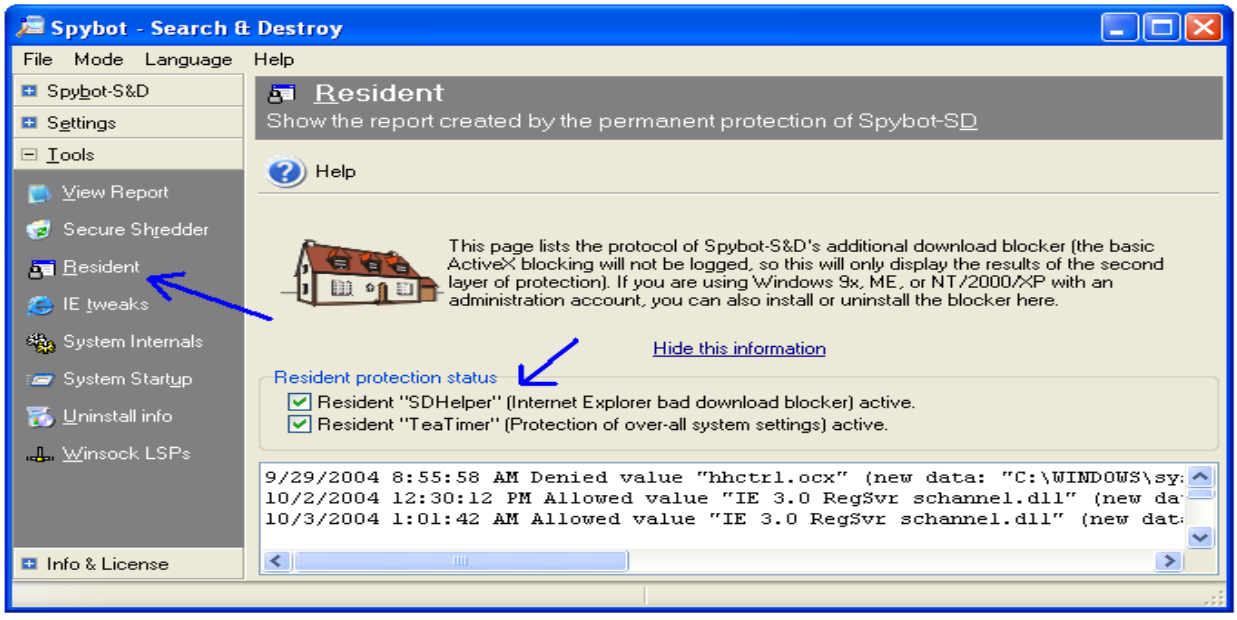


Fig. 51 Resident tool

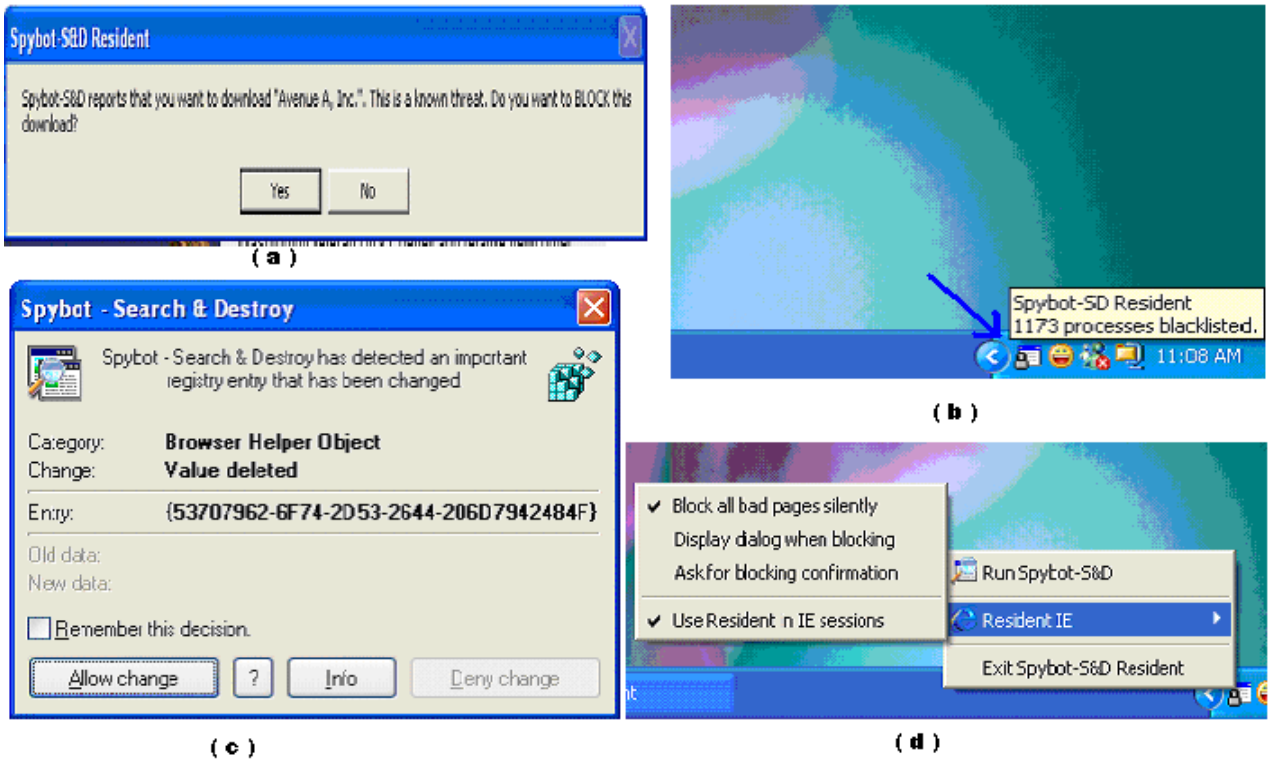


Fig 52 Resident program

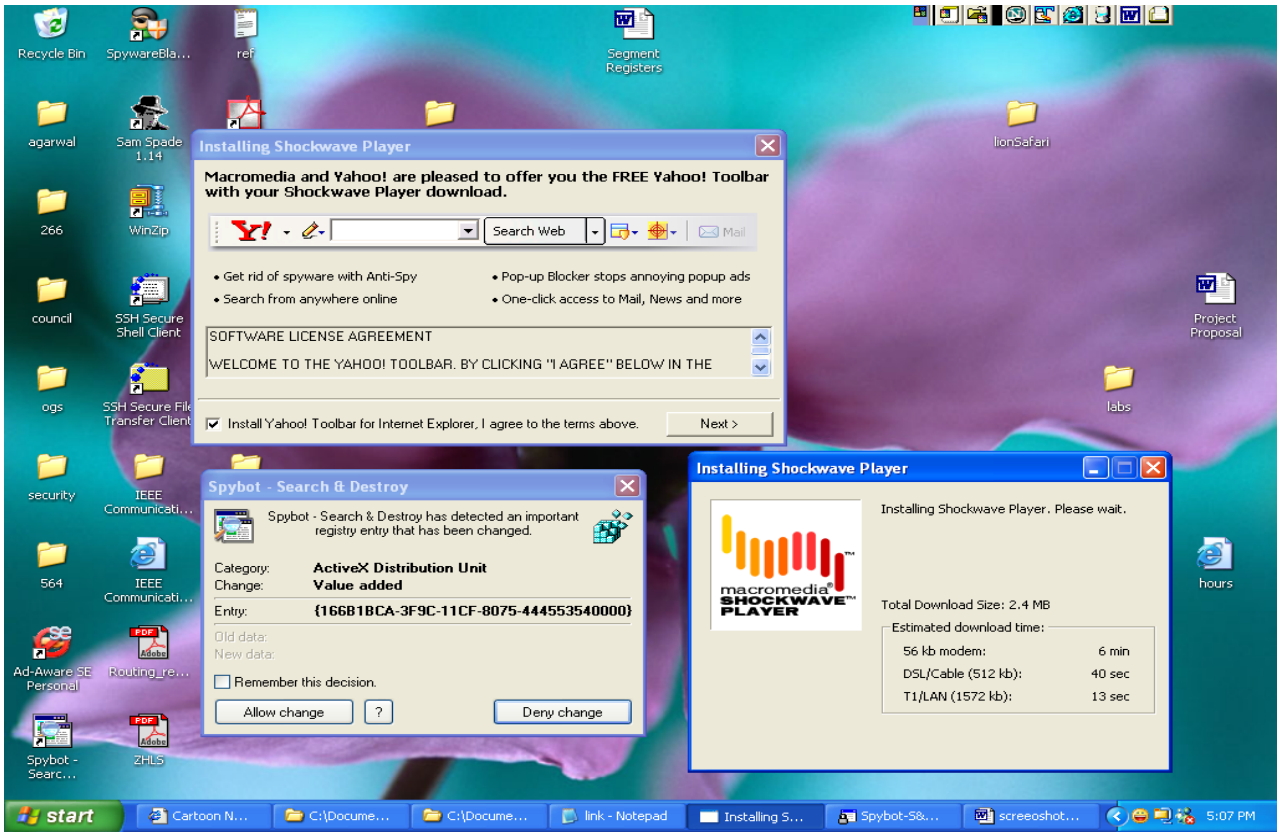


Fig. 53 Resident tool in action

The resident screen allows a user to install/uninstall this helper as well as to view the report on pages that have blocked by the program. The second resident tool is the TeaTimer, a new tool of Spybot-S&D, which perpetually monitors the processes that are called or initiated. It immediately detects known malicious processes wish to start and terminates them. It terminates the process before asking the user as some threats are time critical (e.g. toll dialer), but for the future, it gives user the options on how to deal with these processes:

- Inform when the process tries to start again
- Automatically kill the process, or
- Generally allow the process to run.

Also, there is an option to delete the file associated with this process. In addition to this, TeaTimer detects when something attempts to change some critical registry keys and can protect the user against such changes by giving user an option for "Allow" or "Deny" the change (fig. 52-c).

4.3.4 IE Tweaks Tool

The IE Tweaks screen appears after a user clicks on the “IE Tweaks” button (fig. 54). IE Tweaks are some recommended minor changes that make a system safer and more secure. Locking hosts file prevents most hosts hijackers from doing harm; locking the IE settings prevents other users to change the preferences of a user.

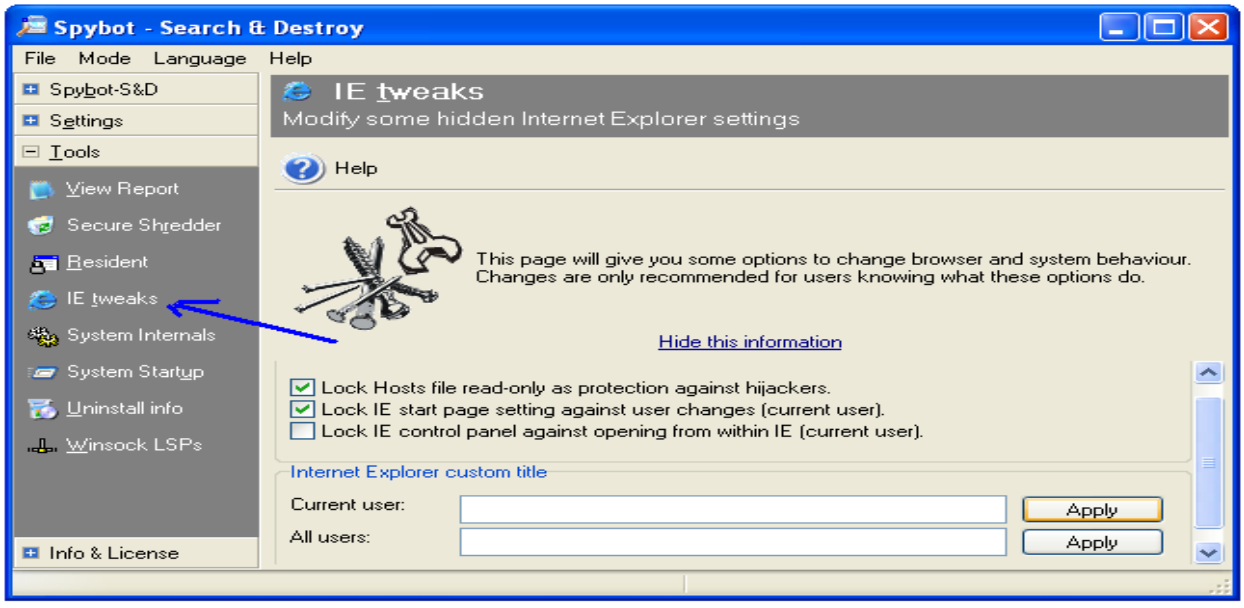


Fig. 54 IE Tweaks screen

4.3.5 System Internals

The system internals screen appears after a user clicks on the “System Internals” button (fig. 55). It is used to search for entries in the registry with incorrect filenames or with non-existent path e.g. missing help files, missing shared DDLs, application paths to non-existent program, wrong uninstall information and broken desktop links. This search is limited to a small number of places and the user are advised to take precaution while changing as it may corrupt the system if the changes are not appropriate for the system. The search is initiated by clicking the “Check” button and the result can be saved using the “Export” button (fig. 55)

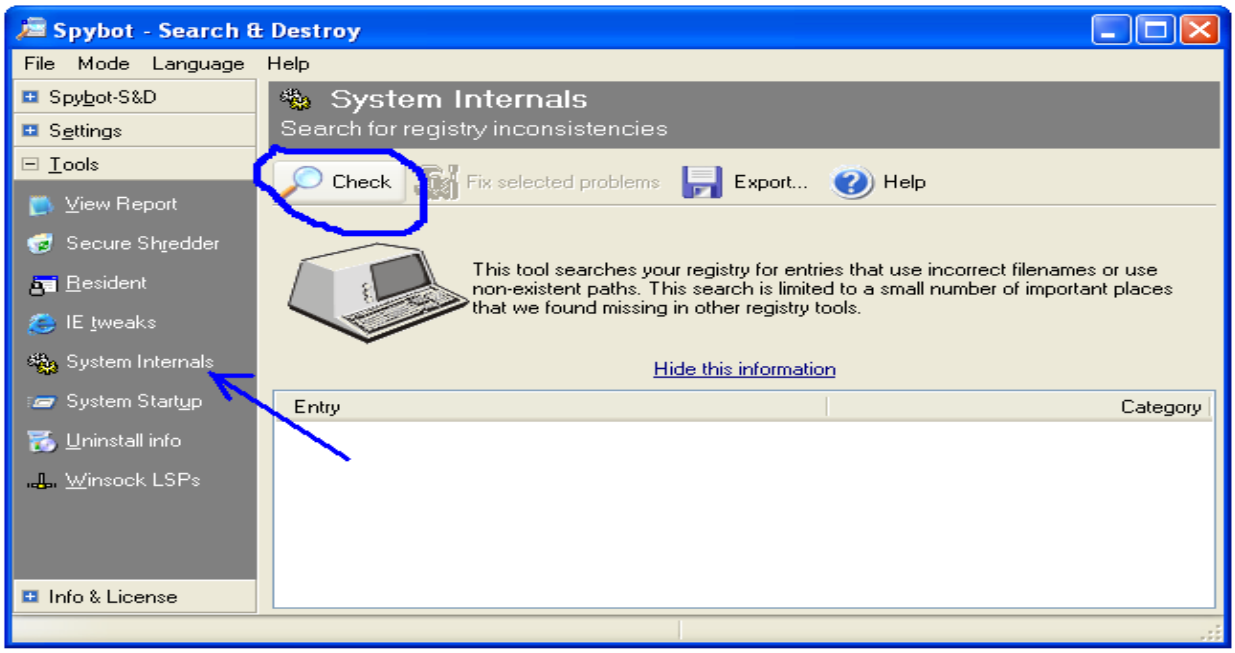


Fig. 55 The system internals screen

4.3.6 System Startup

The System Startup screen appears after a user clicks on the “System Startup” button (fig. 56-3). This tool displays lists all programs (along with some information on the program, if available) that are started at Windows startup (fig. 56). User disables or enables items by un-checking or checking the box besides them, as well as, by selecting an item and then clicking on the Toggle button (fig. 56-4). The Edit, Insert and Delete buttons (fig. 56-4) are used to change an item, insert new items and to delete items respectively. The list can be saved using Export button (fig. 56-4, 56-1). It can also be copied to clipboard using context menu (fig.56-1) that appears with a right click on the list.

The first snapshot is created when Spybot-S&D started in a system for the first time. Afterwards, snapshots are created by right-clicking the list and selecting “Create snapshot” from the context menu item (fig. 56-1). Spybot-S&D displays the entries that have changed since the last snapshot in bold letters (fig. 56-2) [5].

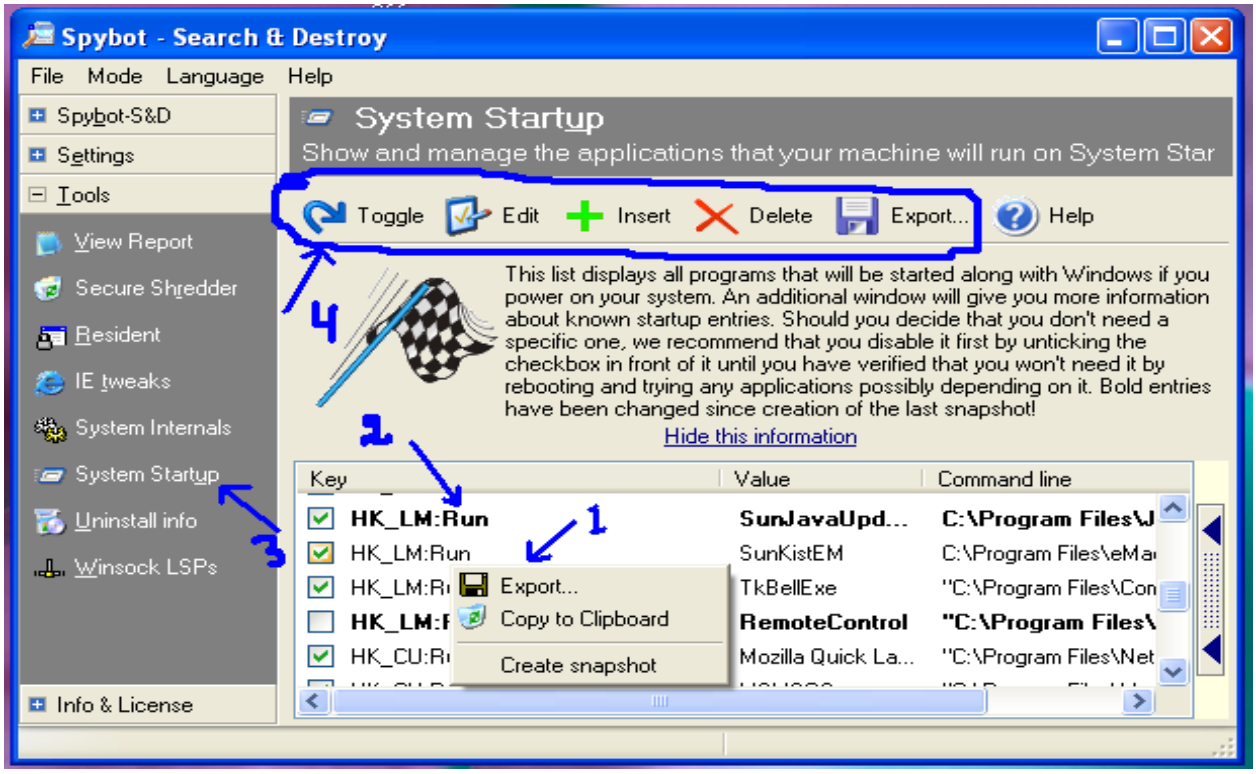


Fig. 56 System Startup

4.3.7 Uninstall Info

The Uninstall Info screen appears after a user clicks on the “Uninstall Info” button (fig. 57-1). This tool lists all programs that have registered some kind of uninstall information with Windows. User can use it to remove the uninstall information of no longer existing programs as well as to simply get an overview [5]. Entries are removed using “Delete” button (fig. 57-2). The list can be saved using Export option (fig. 57-2, 57-3) or copied to clipboard using context menu (fig.57-3).

The first snapshot is created when Spybot-S&D started in a system for the first time. Afterwards, snapshots are created by right-clicking the list and selecting “Create snapshot” from the context menu item (fig. 57-3). Spybot-S&D displays the entries that have changed since the last snapshot in bold letters (fig. 57-4) [5].

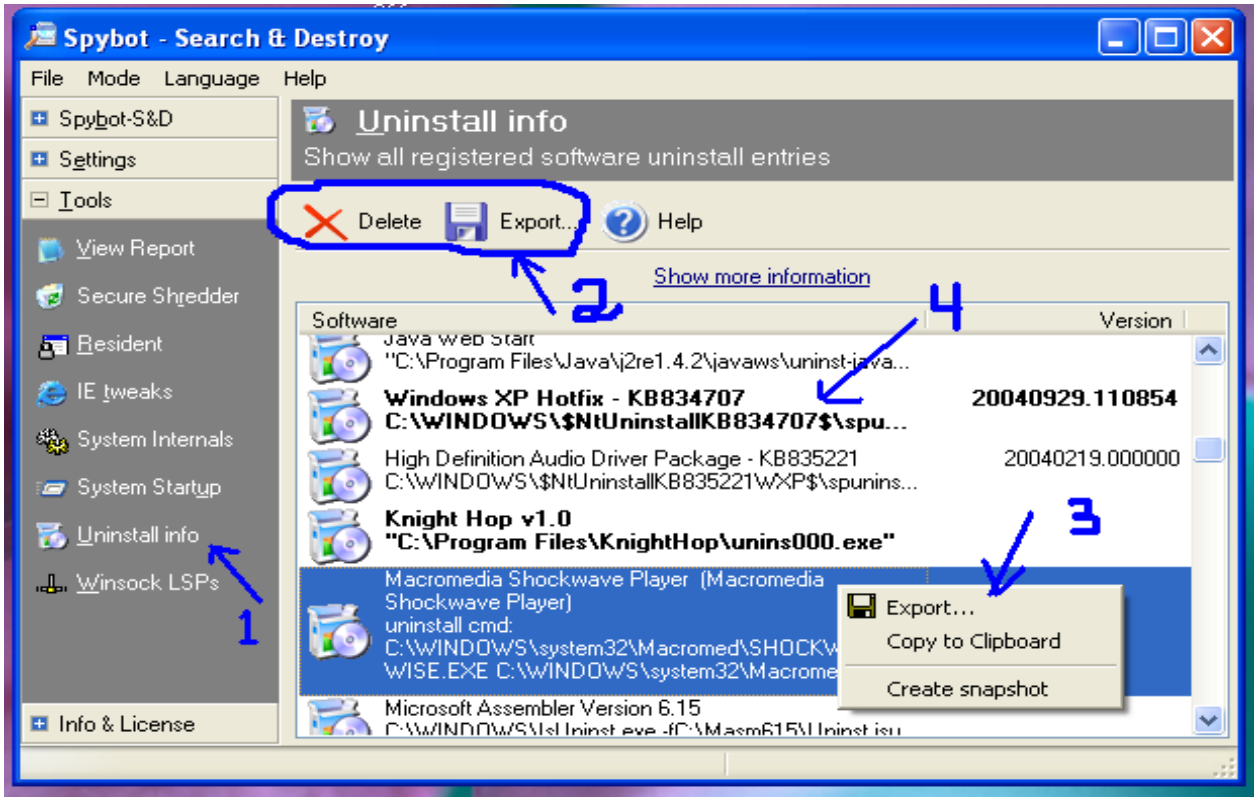


Fig. 57 Uninstall Info

4.3.8 Winsock LSPs

The Winsock LSPs screen appears after a user clicks on the “Winsock LSPs” button (fig. 58). A Layered Service Provider (LSP) is a system driver linked deep into the networking services of Windows. It has access to every data entering and leaving the computer, as well as the ability to modify this data. A few such LSPs are necessary to allow Windows to connect the user to other computers, including the Internet. But Spyware may also install itself as an LSP, thus having access to all the data transmit by a user. Spybot-S&D is able to display a list of installed network drivers as a reference, and allows this list to be exported for future reference [5].

The first snapshot is created when Spybot-S&D started in a system for the first time. Afterwards, snapshots are created by right-clicking the list and selecting “Create snapshot” from the context menu item (fig. 58). Spybot-S&D displays the entries that have changed since the last snapshot in bold letters. The list can be saved using Export option or copied to clipboard using context menu (fig.58) [5].

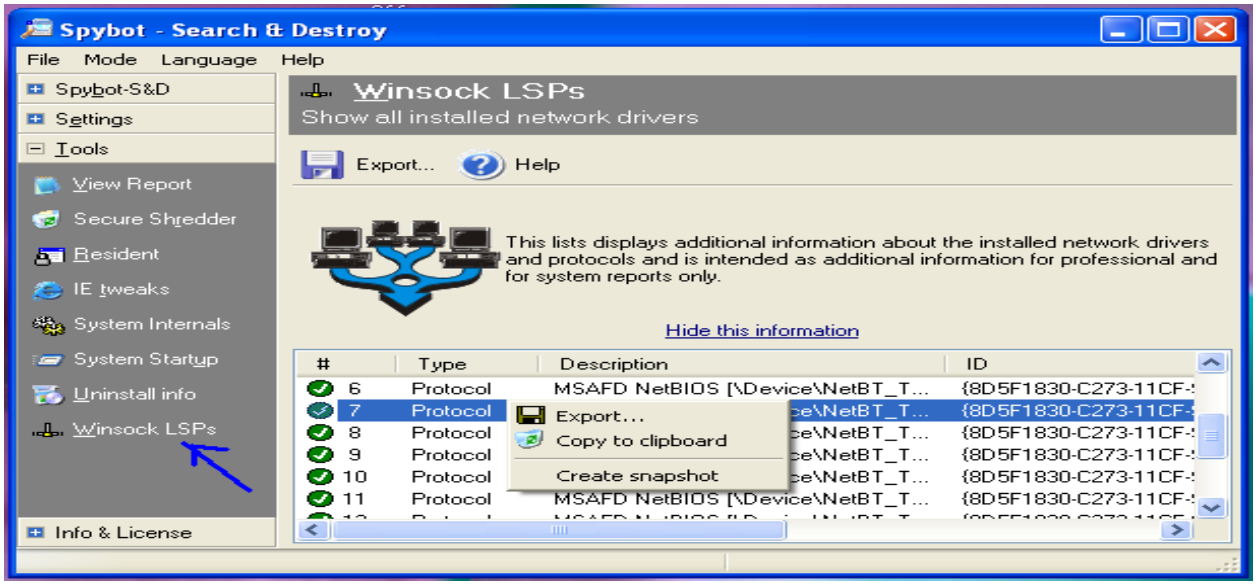


Fig 58 Winsock LSPs

4.4 Info and License

The software version and last update date appears when a user clicks on “Info & License” button (fig. 59). The click also expands the button to four more buttons, labeled as License, Credits, Donations and Statistics.

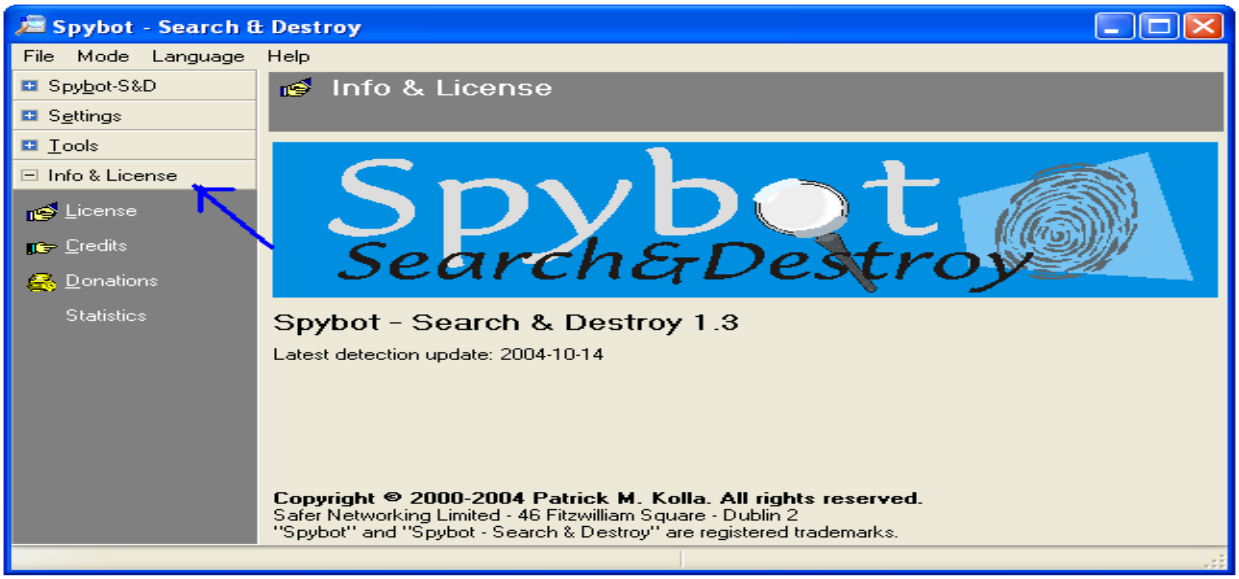


Fig. 59 Info and License

Clicking on each of these four buttons displays the corresponding screen. In brief, the contents of these screens are:

- License: Shows the license agreement for Spybot-S&D (fig. 60-a)
- Credits: List names of persons Spybot-S&D like to offer credits (for their support in reporting bugs, making suggestions, help in testing etc. (fig. 60-b)).

- Donations: A request to donate and a link to the donation site (fig. 60-c).
- Statistics: An overview of threats that the program found and cleared, including number of entries and date (fig. 60-c).

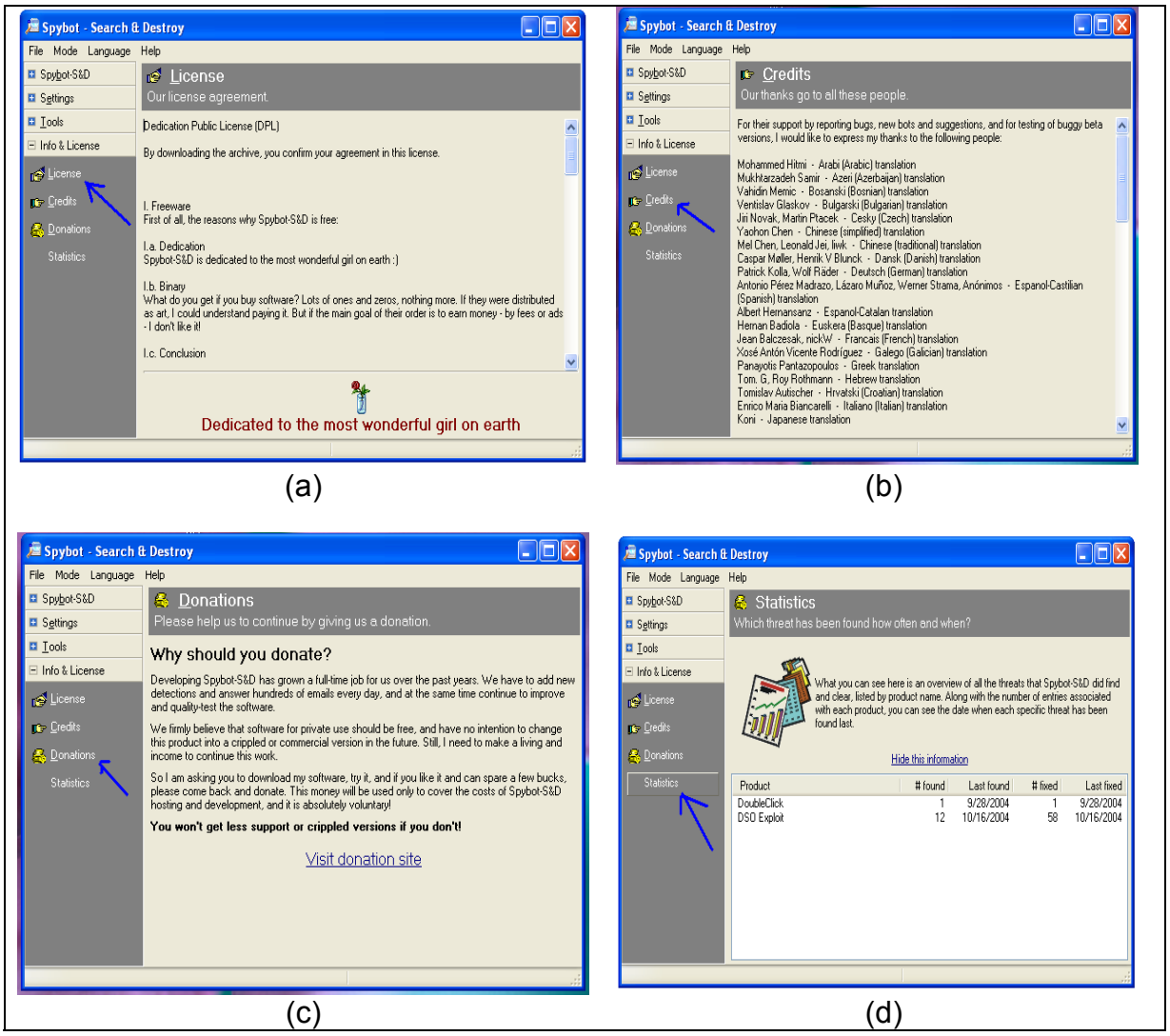


Fig. 60 Info and License – sub-buttons

5 Summary

In the current days, spyware are widespread in the Internet. It is not only a serious security and privacy risk but also degrades system performance by stealing the computer system's resources. There are a number of tools available that can be used to help protecting the system from spyware including Spybot Search & Destroy (Spybot S&D). It is a free tool that can help an Internet user to detect and remove spyware from a computer system.

Spybot S&D provides a convenient GUI to access all of it's functionalities. It allows a user to search and then take appropriate action, including removal, for spyware in a computer system. It also provides the option for recovery so that every changes made by the program can be undone, as long as the user does not delete it from the backup location. In addition, it offers a tool that can stay resident and watch over the system continuously for any type of malicious activities by any program. A variety of custom configuration is also available for the expert user to optimize the performance of the program.

Spybot-S&D works using the hosts' signature. It is important that the definitions are kept up-to-date at all time. The program conveniently provides online update option through an open Internet connection.

Spybot-S&D is a free tool but they accepts donation. Users are encouraged to be generous and visit the donation site located at [6].

5 References

[1] http://www.pluck.com/noadware.aspx

[2] http://www.reach.ucf.edu/~coursdev/cdrom/html/help/glossary.html

[3] http://www.safer-networking.org/en/features/index.html

[4] http://www.safer-networking.org/en/paragraphs/spybotsd_ossupport.html

[5] Spybot-S&D Integrated Help files

[6] http://www.spybot.info/en/donations/index.html