# Dr Solomon's Anti-Virus

Main Screen:

Other Topics:

## Main Screen

The Main Screen is the interface from which you select the drives you want to scan, the type of scan you want to perform, and view the Virus Encyclopedia.

In the Drives list click on an unselected drive to select it, click on a selected drive to deselect it.

After selecting drives click on the appropriate scan button or select the scan from the Scan menu.

The types of scan are:

Quick scan - this is a fast scan which provides most of the protection you need on a daily basis. It scans executable and document files for all known viruses.

Deep scan - this provides a more thorough check than Quick scan. It is slower than Quick scan, so you should only use it occasionally, perhaps if Quick scan has already reported a virus. Deep scan checks for all known viruses in all files, and also uses Advanced Heuristic Analysis. Deep scan also checks files that are archived in such formats as .ZIP, .ARJ etc.

Repair - this finds and removes virus infections. Like Deep scan, Repair scans all files, including archived ones, so it is slower than Quick scan. You should use Repair after Quick scan has already reported an infection.

Click on the Encyclopedia button to access an up-to-date database of viruses which can be detected, with detailed information on their characteristics.

Back to Overview

## Scan Menu

The Scan menu provides alternatives to the buttons of the Main Screen. Instead of selecting a button you can select its equivalent item from the Scan menu.

Back to Overview

## Quick scan

The Quick scan virus check is faster, but less secure than Deep scan.

As only executable files and data files containing macro code can be infected by viruses, Quick scan only checks files with the extensions: APP, BAT, BIN, CMD, COM, DEV, DLL, DOC, DOT, EXE, QV?, QLB, SYS, XTP, 001, 002.

In addition Quick scan also searches boot sectors and partition sectors.

Back to: Main Screen

## Deep scan

The Deep scan virus check is slower, but more secure than Quick scan.

Additionally to the Quick scan check, Deep scan checks all files (rather than just executables and document files), it searches heuristically, and it recursively scans inside compressed and archived files.

The compressed file formats supported are: PKZip, ARJ, LZH, ARC, PKLite, LZExe, Diet, Cryptcom Microsoft Expand, and ICE.

Even files compressed with the PKLite Pro -E switch (described as unextractable) can be scanned for viruses.

Back to: Main Screen

## Repair viruses

This removes virus infections. The virus code is then overwritten with zeroes to ensure that it is completely removed.

Where a virus cannot be removed from a file you are given the option to rename it (so that it cannot be run accidentally), or to delete it. The file is overwritten with zeroes before it is deleted to ensure that it cannot be undeleted.

Repair can also remove viruses from boot sectors and partition sectors.

Back to: Main Menu

## Virus Encyclopedia

For each virus, the Encyclopedia gives the following information:

How common is it?
How infectious is it?
How much damage does it do?
What is infected, and how much do files grow by?
What memory-resident capabilities does it have?
Does it use stealth?
Is it encrypted?
Is it polymorphic?
What other effect does it have?
What other names are used for this virus?
How many variants are there?
Can it be repaired?

On the right of the dialog there is a list of the viruses. A virus can be selected from the list by clicking on it with the mouse. If a virus has a number of similar variants, their names can be displayed by pressing the Variants button.

Below the virus list there is a search box. As a virus name is entered in the box the Encyclopedia performs an incremental search through its database. Often it is unnecessary to type the full name before the Encyclopedia finds the correct entry.

Pressing the Repair button gives instructions on handling and removing different types of viruses.

Back to: Scan Menu

## Daily Scanning

There is a launch program - 'FVLAUNCH.EXE' - to implement daily virus scanning.

To activate FVLAUNCH move it to the StartUp folder. To de-activate FVLAUNCH remove it from the StartUp folder.

Each time you boot up the computer FVLAUNCH checks whether a virus scan has already been performed that day. If a scan has not been performed FVLAUNCH starts a scan, which checks the local drives.

Before the scan starts you may see the licence agreement prompt. If you do see this prompt you can check the 'Don't show again' box. If you check this box the licence agreement prompt will not be shown again.

If you have previously checked the 'Don't show again' box the scan starts immediately.

You see an indication of the progress of the scan in the Task Bar. A report screen is displayed when the scan has completed.

## Check Memory

Memory is automatically checked for known stealth, common, and fast-spreading viruses on start up.

# Index

## About Viruses

A virus is a program that copies itself without the knowledge of the computer user. Typically, a virus spreads from one computer to another by adding itself to an existing piece of executable code so that it is executed when its host code is run.

Viruses can be classified by their method of concealment. Some are called stealth viruses because of the way that they hide themselves, or polymorphic because of the way they change themselves to avoid scanners.

The most common classification, however, relates to the sort of executable code which the virus attaches itself to. These are:

Partition Viruses
Boot Sector Viruses
File Viruses
Macro Viruses

As well as replicating, a virus may carry a Damage routine.

There is also a set of programs that are related to viruses by virtue of their intentions, appearances, or users likely reactions:

Droppers
Failed viruses
Packagers
Trojans
Jokes
Test files

## Stealth Viruses

If a stealth virus is in memory, any program attempting to read the file (or sector) containing the virus is fooled into believing that the virus is not there. The virus in memory filters out its own bytes, and only shows the original bytes to the program.

There are three ways to deal with this:

1. Cold Boot from a clean DOS floppy, and make sure that nothing on the hard disk is executed. Run any anti-virus software from floppy disk. This method is foolproof but you will have to upgrade to the full Dr Solomons Anti Virus Toolkit to obtain a diskette version.

2. Search for known viruses in memory. Dr Solomon's Anti-Virus does this when it is run.

3. Use advanced programming techniques to penetrate the fog that the virus throws up.
Dr Solomon's Anti-Virus uses "Anti-Stealth Methodology" for this.

See also: About Viruses

## Polymorphic Viruses

A polymorphic virus is one that is encrypted, and the decryptor/loader for the rest of the virus is very variable. With a polymorphic virus, two instances of the virus have no sequence of bytes in common. This makes it more difficult for scanners to detect them.

Dr Solomon's Anti Virus uses "Fuzzy Logic" techniques and the 'Generic Decryption Engine' to detect these viruses.

See also: About Viruses

## The Partition and Partition Sector Viruses

The partition sector is the first sector on a hard disk. It contains information about the disk such as the number of sectors in each partition and where the DOS partition starts, plus a small program. The partition sector is also called the "Master Boot Record" (MBR).

When a PC starts up, it reads the partition sector and executes the code it finds there. Viruses that use the partition sector modify this code.

The Repair option removes virus code from partition sectors.

Since the partition sector is not part of the normal data storage part of a disk, utilities such as DEBUG will not allow access to it.

Floppy disks do not have a partition sector.

## The Boot Sector and Boot Sector Viruses

The boot sector is the first sector on a floppy disk. On a hard disk it is the first sector of a partition. It contains information about the disk or partition, such as the number of sectors, plus a small program.

A boot sector virus replaces this sector with its own code and moves the original elsewhere on the disk.

When the PC starts up, it attempts to read the boot sector of a disk in the A: drive. If this fails because there is no disk, it reads the boot sector of the C: drive.

Even a non-bootable floppy disk has executable code in its boot sector. This displays the "not bootable" message when the computer attempts to boot from the disk. Viruses can use this mechanism to infect the PC.

See also: About Viruses

## File Viruses

File viruses append or insert themselves into executable files, typically .COM and .EXE programs.

A direct-action file virus infects another executable file on disk when its 'host' executable file is run.

An indirect-action (or TSR) file virus installs itself into memory when its 'host' is executed, and infects other files when they are subsequently accessed.

See also: About Viruses

## Macro Viruses

Macro Viruses infect executable macro code in documents. An example is the Concept virus which infects Word 6 document files.

See also: About Viruses

## Droppers

Droppers are programs that have been written to perform some apparently useful job but, while doing so, write a virus out to the disk. In some cases, all that they do is install the virus (or viruses).

A typical example is a utility that formats a floppy disk, complete with Stoned virus installed on the boot sector.

See also: About Viruses

## Failed Viruses

Sometimes a file is found that contains a 'failed virus'. This is the result of either a corrupted 'real' virus or simply a result of bad programming on the part of an aspiring virus writer. The virus does not work - it hangs when run, or fails to infect.

Many viruses have severe bugs that prevent their design goals - some will not reproduce successfully or will fail to perform their intended final actions (such as corrupting the hard disk).

Many virus authors are very poor programmers.

See also: About Viruses

## Packagers

Packagers are programs that in some way wrap something around the original program. This could be as an anti-virus precaution, or for file compression. Packagers can mask the existence of a virus inside.

See also: About Viruses

## Trojans and Jokes

A Trojan is a program that deliberately does unpleasant things, as well as (or instead of) its declared function. They are not capable of spreading themselves and rely on users copying them.

A Joke is a harmless program that does amusing things, perhaps unexpectedly. We include the detection of a few jokes in Dr Solomon's Anti-Virus, where people have found particular jokes that give concern or offense.

See also: About Viruses

## Test files

Test files, in the context of viruses, are used to test and demonstrate anti-virus software. They are not viruses - simply small files that are recognized by the software and cause it to simulate what would happen if it had found a virus. This allows users to see what happens when it is triggered, without needing a live virus.

A test file for Dr Solomon's Anti-Virus can be made by creating a small text file, at least 50 characters long, which has the following sequence of characters at the very beginning:

ZQZXJVBVT

Note that the test file should have an executable extension (.COM or .EXE) for this to work correctly.

Back to About Viruses

## Virus Protection

Protecting a floppy disk
Protecting a hard disk

Back to About Viruses

## How to protect a floppy disk

To protect a clean floppy disk against viruses, use the write-protect notch.

If a diskette is write-protected, it cannot be written to by any software, including a virus.

The write protect notch uses a hardware mechanism, so it cannot be overridden by software.

See also: Virus Protection

## How to protect a hard disk

It is possible to write-protect a hard disk, either in software or in hardware.

However, write-protecting a hard disk generally limits its usefulness too much for most applications.

The alternative is to use software to actively detect virus activity.

Dr Solomons Anti-Virus finds known viruses and can be set up to run daily.

See also: Virus Protection

## Upgrades

The full Dr Solomon's toolkit is supported by monthly or quarterly updates to keep up with the appearance of new viruses.

To upgrade to the full Dr. Solomon's Anti Virus Toolkit print, fill out and send the order form to your local distributer.

# Upgrade Order Form

See Upgrades for an introduction to this form.
----------------------------------------------------------------------------------------------------

To: ______________________________________ C/E056

______________________________________

______________________________________

______________________________________

Name ____________________________________

Company ____________________________________

Department ____________________________________

Street ____________________________________

City, State, Zip/Country ____________________________________

____________________________________

Please complete the following:

Please send me the Dr Solomon's AntiVirus Toolkit
for (please check one operating system)

Windows 95 .___
Windows 3.x ___
Windows NT ___
Netware ___

1. Registration fee.....................................____________

Please contact your local distributor
for the current price

2. Shipping..................................................____________

3. Sales tax, if applicable..........................____________

TOTAL of 1, 2 and 3.................................____________

Please indicate payment method:

Check/M.O. ___ Credit card ___

Credit Card No.__________________________ Expires ___________

Signature______________________________ Date ___________

Check here ____ if you require 5.25" media.

We accept corporate purchase orders--please call your local distributor for details.

In the USA, you can telephone your order to 800-310-9078 or fax this form to 617-238-0851.

Dr Solomon's Software can be contacted by email

| | |
|---|---|
| North America | info@us.drsolomon.com |
| United Kingdom | info@uk.drsolomon.com |
| Germany | info@de.drsolomon.com |

or on the World Wide Web http:/www.drsolomon.com/
or Compuserve Go Drsolomon

Back to Overview

## How to do a Cold (Power-off) Boot

1. Switch off the computer.
2. Wait for 10 seconds for the power supply to reset.
3. Put a known clean bootable DOS diskette in drive A.
4. Switch the computer back on again.

Make sure that nothing on the diskette runs any software on the hard disk. For example, there might be the command "C:\KEYB ..." in the AUTOEXEC.BAT.

If you do a warm boot, using Ctrl+Alt+Del, that might not reboot the computer. Joshi virus, for example, fakes a reboot if you do a Ctrl+Alt+Del.

Some computers have a Reset button which appears to do a cold boot, and some programs can also do a cold boot. However, what really happens when these features are used depends on how the manufacturer implemented them. A power-off boot always clears memory.

## Damage

Damage is defined as something that you would prefer not to have happened. It is measured by the amount of time it takes to reverse the damage.

Trivial damage happens when all you have to do is get rid of the virus. There may be some audio or visual effect; often there is no effect at all.

Minor damage occurs when you have to replace some or all of your executable files from clean backups, or by re-installing. Remember to run Dr Solomon's Anti-Virus again afterwards.

Moderate damage is done when a virus trashes the hard disk, scrambles the FAT, or low-level formats the drive. This is recoverable from your last backup. If you take backups every day you lose, on average, half a day's work.

Major damage is done by a virus that gradually corrupts data files, so that you are unaware of what is happening. When you discover the problem, these corrupted files are also backed up, and you might have to restore a very old backup to get valid data.

Severe damage is done by a virus that gradually corrupts data files, but you cannot see the corruption (there is no simple way of knowing whether the data is good or bad). And, of course, your backups have the same problem.

Unlimited damage is done by a virus that gives a third party access to your network, by stealing the supervisor password. The damage is then done by the third party, who has control of the network.

See also: Virus Encyclopedia and About Viruses

## File Allocation Table (FAT)

The FAT is the area on the disk that contains the information about what part of the disk belongs to which file. If the FAT is zeroed or corrupted, then the hard disk is like the pages of a book, without any binding, in a random order, and no page numbers.

A number of viruses zero, overwrite, or (much worse) make small changes to the FAT.

See also: Damage

## Distributors

Dr Solomon's Anit Virus is available from a number of sources. If your country does not appear on this list, please contact Dr Solomon's in the United Kingdom, in the USA or in Germany.

North America
Argentina
Australia
Austria
Bahrain
Baltic Republics
Bangladesh
Belgium
Belorussia
Bolivia
Brazil
Canada
Central America
Chile
China
Colombia
Cyprus
Czech Republic
Denmark
Egypt
Ecuador
Estonia
Ethiopia
Finland
France
Germany
Ghana
Greece
Guatamala
Honduras
Hong Kong
India
Indonesia
Iran
Ireland
Isreal
Italy
Ivory Coast
Japan
Kenya
Korea
Kuwait
Latvia
Luxembourg
Malaysia
Malta
Mexico
Nepal
Netherlands

New Zealand
Nicaragua
Nigeria
Norway
Oman
Peru
Poland
Portugal
Qatar
Russia
Saudi Arabia
Sierra Leone
Singapore
Slovakia
South Africa
Soviet Block
Spain
Sri Lanka
Sweden
Switzerland
Taiwan
Thailand
Trinidad
Turkey
UAE
United Kingdom
USA
Venezuela
West Indies
Zimbabwe

If you have any problems contacting your local distributor, call Dr Solomon's Software on +44 (0)1296 318700, or fax us on +44 (0)1296 318777.

Our UK Internet email address is: support@uk.drsolomon.com

Our Internet email address in the USA is: support@us.drsolomon.com

Our Internet email address in Germany is: support@de.drsolomon.com

To access our forum on CompuServe: GO DRSOLOMON

To access us on World-Wide Web: http://www.drsolomon.com/

See also: Upgrades and Overview

## Distribution in: United States of America

Dr Solomon's Software, Inc.
1 New England Executive Park
Burlington   MA 01803
USA

Tel:    +1 617 273-7400
Fax:    +1 617 273-7474
BBS:    +1 617 229-8804

Internet email: support@us.drsolomon.com
CompuServe forum: GO DRSOLOMON

Toll-free technical support: 800-595-9175
Toll-free sales line: 800-701-9648

Back to Distributors

## Distribution in: Argentina & Colombia

Economic Data S.L.
Ponzano, 39-5º I
28003   Madrid
Spain

Tel:    +34 1 442 2800
Fax:    +34 1 442 2294

Internet email: edutaba@edata.es

Back to Distributors

## Distribution in: Australia & New Zealand

Loadplan Australasia Pty Ltd
96-98 South Market Street
South Melbourne
Victoria 3205
Australia

Tel: +61 3 9690 0455
Fax: +61 3 9690 7349

Internet email: loadplan@loadplan.com.au

Back to Distributors

## Distribution in: Germany, Austria & Switzerland

Dr Solomon's Software GmbH
Luisenweg 40
20537 Hamburg
Germany

Tel: +49 40 25 19 54-0
Fax: +49 40 25 19 54-50

CompuServe: 75450,1326
Internet email: support@de.drsolomon.com

Back to Distributors

## Distribution in: Bahrain, Egypt, Kuwait, Oman, Qatar, Saudi Arabia & UAE

LBI International, Inc.
2 Torri Katur
Lourdes Lane
St Julians STJ 02
Malta GC

Tel: +356 344257
Fax: +356 340761

Back to Distributors

## Distribution in: Belgium, Luxembourg & Netherlands

Data Alert International B V
Patrijsweg 80 E
2289 Ex Rijswijk
The Netherlands

Tel:    +31 70 307 7111
Fax:    +31 70 307 7886

Internet email: 100627.2012@compuserve.com

Back to Distributors

## Distribution in: Brazil

PC Software e Consultoria Ltda
R Voluntarios da Patria 45-13º
22270-000   Rio de Janeiro RJ
Brazil

Tel:     +55 21 537 0405
Fax:     +55 21 537 1411

Internet email: pc.software@centroin.ax.apc.org

Back to Distributors

## Distribution in: South East Asia

China, Hong Kong, Indonesia, Korea, Malaysia, Singapore, Taiwan & Thailand

Digitus Computer Systems
11 Dhoby Ghaut
#09-01 Cathay Building
Singapore 229233

Tel: +65 337 1945
Fax: +65 336 9672

Back to Distributors

## Distribution in: Canada

Sensible Security Solutions
Golf Club Road
R.R. #1 Braeside
Ontario
KOA 1GO
Canada

Tel:   +1 613-623-6966
Fax:   +1 613-623-3992

Internet email: secure-1@magi.com

Back to Distributors

**Distribution in: Ecuaodor Chile, Guatamala, Honduras, Nicaragua,**
Peru, Venezuela & Central America

Bysupport Computacion SA
Bernardo Vera y Pintado 2575
Providencia
Santiago
Chile

Tel: +56 2231 0300
+56 2231 0308
Fax: +56 2233 5917

Internet email: bysup@reuna.cl

Back to Distributors

## Distribution in: Cyprus & Greece

A E C Consultants Ltd
PO Box 906
1 G. Afxentiou Avenue
6023 Larnaca
Cyprus

Tel: +357 4 656108/650137/626422
Fax: +357 4 658972

Internet email: aec@zenon.logos.hol.gr

Back to Distributors

## Distribution in: Czech Republic

PCS Software spol. s.r.o.
Na Dvorcích 18
14000 Praha 4
Czech Republic

Tel:   +42 2 42 3962
          +42 2 42 1628
Fax:   +42 2 42 0192

Back to Distributors

## Distribution in: Denmark

Swanholm Distribution A/S
Transformervej 9 D
DK-2730 Herlev
Denmark

Tel: +45 44 92 9393
Fax: +45 44 92 7171

Internet email: support@swanholm.dk

Back to Distributors

**Distribution in: Estonia, Finland, Baltic Republics, Latvia,**
Belorussia, Russia & Soviet Block.

LAN Vision Oy
Sinikalliontie 14
SF-02630 Espoo
Finland

Tel:    +358 0 502 1947
Fax:    +358 0 524 149

Back to Distributors

## Distribution in: France

AB Soft
Parc Burospace 15
91572 Bièvres cedex
France

Tel: +33 1 69 33 70 00
Fax: +33 1 69 33 70 10

CompuServe: 72451,243
Internet email: 72451.243@compuserve.com

Back to Distributors

## Distribution in: Ghana, Nigeria, Ivory Coast and Sierra Leone

Software Marketing Consultancy
House No B26/28, New Achimota
PO Box 8592
Accra North
Ghana

Tel: +233 2755 7506
Fax: +233 2755 2718

Internet email: ghemans@ug.gn.apc.org

Back to Distributors

## Distribution in: India, Bangladesh, Nepal & Sri Lanka

IT Secure
52 Regency Chambers
Near Nandi Cinema
Bandra (West)
Bombay 400 050
India

Tel: +91 22 643 1233/1246
Fax: +91 22 642 2182
Internet email: peter.quantum@axcess.net.in

N&N Systems and Software
105 Om Chambers
123 August Kranti Marg
Bombay 400 036
India

Tel: +91 22 368 0512/0517/0518
Fax: +91 22 368 0513
Internet email: neville.bulsara@lwbom.nandanet.com

Back to Distributors

## Distribution in: Iran

Shabakeh Gostar Corporation
Building Number 10
Palizi Square
North Sohrevardi Avenue
Tehran 15568
Iran

Tel: +98 21 876 7615
Fax: +98 21 876 7615

Back to Distributors

## Distribution in: Ireland

Priority Data Systems Ltd
Priority House
63 Patrick St
Dun Laoghaire
Co Dublin
Ireland

Tel:     +353 1 284 5600
Fax:     +353 1 280 0311

CompuServe: 100143, 575
Internet email: priority@iol.ie

Back to Distributors

## Distribution in: Italy

Siosistemi srl
Via Cefalonia 58
25124   Brescia
Italy

Tel:     +39 30 244 11
Fax:     +39 30 222 249

Back to Distributors

## Distribution in: Japan

Jade Corporation Ltd
3-6-11 Tokiwa-Cho
Shizuoka City
Shizuoka 420
Japan

Tel:   +81 54 252 0085
Fax:   +81 54 221 0282

CompuServe: 100225,3467
Internet email: 100225.3467@compuserve.com

Back to Distributors

## Distribution in: Kenya

Memory Masters
PO Box 70158
Nairobi
Kenya

Tel: +254 2 751916/743934
Fax: +254 2 751916

Internet email: memorymasters@africaonline.co.ke

Back to Distributors

## Distribution in: Malta

Panta Computer Co. Ltd
Panta House
Birkirkara Road
Msida MSD 03
Malta

Tel: +356 492 741
Fax: +356 492 744

Back to Distributors

## Distribution in: Mexico

Grupo ASISA
L.Tequesquinahua No.84 Colonia PIPSA
Tlalnepantla Edo de Mex.
CP 54160 Mexico

Tel: +52 5 392 4155
Fax: +52 5 392 4178

CompuServe: 74174,3053
Internet email: 74174.3053@compuserve.com

Back to Distributors

## Distribution in: Norway

Swanholm Distribution A/S
Wdm Thranesgt 77 (0715)
PO Box 9858, 1LA
0132 Oslo
Norway

Tel:     +47 2 11 6828
Fax:     +47 2 11 6363

Internet email: swanholm@swanholm.no
World-Wide Web: http://www.swanholm.no/

Back to Distributors

## Distribution in: Poland

Dagma sp. z o.o
UL Gen Jankego 15
40-615 Katowice
Poland

Tel:   +48 32 102 11 22
Fax:   +48 32 102 11 22

Internet email: daggps@silter.silesia.ternet.pl

Back to Distributors

## Distribution in: Portugal

RSVP Consultores Associados Lda
Rua Conde de Avranches, 659 - 2 Esq
4200 Porto
Portugal

Tel: +351 2830 0741
Fax: +351 2830 0740

Internet email: rsvp.pt@tpone.telepac.pt

Back to Distributors

## Distribution in: South Africa

BSS (Pty) Ltd
PO Box 811, Gallo Manor
Sandtown 2052
Johannesburg
South Africa

Tel: +27 11 444 8800
Fax: +27 11 444 2959

Internet email: mdanton@bss.co.za

Back to Distributors

## Distribution in: Slovakia

Lynx s.r.o.
Stefanikova 50a
Kosice
Slovakia
040 01

Tel: +42 95 62 27309
+42 95 62 27319
Fax: +42 95 62 26562

Back to Distributors

## Distribution in: Spain

Economic Data S.L.
Ponzano, 39-5º I
28003   Madrid
Spain

Tel:     +34 1 442 2800
Fax:     +34 1 442 2294

Internet email: edutaba@edata.es

Back to Distributors

## Distribution in: Sweden

QA Information Security AB
Box 596
S-175 26 Järfälla
Sweden

Tel:    +46 (0)8-580 100 02
Fax:    +46 (0)8-580 100 05

Internet email: support@qainfo.se

Back to Distributors

## Distribution in: Turkey

Logosoft Yazilim San Tic Ltd
Albay Faik Sozener Cad.
Benson Is Merkezi
21/3 Kadikoy
81300 Istanbul
Turkey

Tel: +90 216 348 1399
+90 216 348 7309
Fax: +90 216 348 1754

Back to Distributors

## Distribution in: United Kingdom

Dr Solomon's Software PLC
Alton House Business Park
Gatehouse Way
Aylesbury
Bucks   HP19 3XU
England

Tel:     +44 (0)1296 318700
Fax:     +44 (0)1296 318777

Support tel: +44 (0)1296 318733
Support fax: +44 (0)1296 318734
Bulletin board: +44 (0)1296 318810

CompuServe forum: GO DRSOLOMON
Internet email: support@uk.drsolomon.com
World-Wide Web: http://www.drsolomon.com/

Back to Distributors

## Distribution in: Trinidad & West Indies

Global Traders Inc Ltd
First Floor   Moller's Plaza
#18 Eastern Main Road
Tunapuna
Trinidad
West Indies

Tel:     +1 809 662 6256
Fax:     +1 809 662 6256

Back to Distributors

## Distribution in: Zimbabwe

RyVal Computers (Private) Limited
PO Box AY 249
AMBY
Harare
Zimbabwe

Tel:   +263 4 487 235
         +263 4 487 239
Fax:   +263 4 486 381
Internet email: ryval@harare.iafrica.com

Ridgehill Investments
15 Lomagundi Road
Avondale
Harare
Zimbabwe

Tel:   +263 4 304 822
Fax:   +263 4 304 822

Back to Distributors

## Compressed and archived files

(Please note this feature is only available on machines with a 386 processor or better).

Use Deep scan to scan archived and compressed files.

You will not need to scan compressed and archived files in normal usage.

Back to Overview

## Advanced Heuristic Analysis (AHA)

Heuristic Analysis is a technique for finding new viruses. It looks inside files for the code combinations necessary for a virus to operate.

You can start a virus scan using heuristics by selecting the Deep scan option.

Back to Overview

## How to contact us

There are a variety of ways of contacting us.   Firstly, you may like to contact your local International distributor of Dr Solomon's anti-virus products.

Other methods:

CompuServe: GO DRSOLOMON
World-Wide Web: http://www.drsolomon.com/

Dr Solomon's Software PLC
Internet email: support@uk.drsolomon.com
Bulletin Board: +44 (0)1296 318810

Dr Solomon's Software, Inc.
Internet email: support@us.drsolomon.com
Bulletin Board: +1 617 229-8804

Dr Solomon's Software GmbH
Internet email: support@de.drsolomon.com
CompuServe: 75450,1326

Back to Overview