Antivirus System AVG 4.1 for Windows - Index

Informative Functions

Test Functions

Program Settings

Service Functions

General Information

Desktop

The AVG window is full size only and contains the following:

Menu bar
Standard menu bar to access AVG's functions.

Icons
Quick start of Scan test, Comparative test, Heuristic analysis,   Memory test and Exit.

Current settings
These are for information only - use menu Settings to change values.

About AVG

Displays information about the AVG version you are using, including subversion, date of release for distribution and information on language versions.

The serial number and the name of the licensee are important. They are written into the AVG program during installation and cannot be changed later.

The information about the AVI and AVF files is important. These files influence the range and capability of the tests, i.e. two programs of the same version but with different data files will differ in their capabilities.

If the user employs his own files for user validation and/or his own description of external viruses, the appropriate information is displayed in the window.

About Viruses

Displays basic data on viruses detected by your installation of AVG (the number of detected viruses depends on which version you have installed and on the AVI/AVF files).It should be pointed out that the information given here has been abbreviated considerably, i.e. it contains only the name of the virus and type of attack (file/system area).

AVG contains a detailed description of the commonest viruses, it is not available for all viruses contained in the virus databank.

System information

Displays information on the working environment - type and version of the operating system, memory controls, processor mode, size of base and XMS memory etc.

Heuristic analysis flags

Lists flags with their meaning in alphabetical order.

Selection of devices

Before the test - scan test, heuristic analysis or comparative test - the device/directory to be tested must be selected.

A dialog box is displayed containing all available drives. Next to each is also displayed the type - eg. local, network etc - and whether or not a Comparative database exists (existence is not tested on diskettes or network drives).

Any number of drives can be selected for a test. A particular directory can also be selected, all subdirectories of which will be tested.

The selection of drives is as follows:

Testing one device
Highlight the device to be tested and choose Start test.

Testing one directory
Highlight the appropriate drive and choose Directories... In the displayed directory tree highlight directory to test. Click Select to confirm selection. Chosen directory will appear next to selected device. To test this directory select Start test.

Testing more than one drive/directory
To test more than one drive/directory at the same time, selection Add must be used. Select required drive/directory as described above and instead of starting the test, click on Add. Selected drives/directories will be listed in the bottom part of the dialog box. Repeat until the list is complete, then click Start test.

Clearing the list
If you want to clear the list of drives/directories, click on Clear.

Double click with mouse
To simplify the selection of drives a double click of the left mouse button can be used. Double click can be setup in Settings - General settings. The default setting for a double click is Start test. Other possible settings are Selection of directory, Add to list or double click is ignored.

Scan test

The Scan-test in AVG consists of three independent techniques which appear as one compact test. We shall deal with the three parts separately.

Standard search

The standard way to detect known viruses is to search for virus identifiers (sequence of symbols characteristic of a given virus).

Individual algorithms

Individual algorithms are for detecting some known mutation viruses of the Tremor, MtE, TPE etc. type. Each file tested is checked to see if it contains a coding algorithm characteristic of a known type of mutation virus.

Fast heuristic analysis

The principle of this technique consists in analysing the code of the file being tested and in understanding the meaning of the instructions. The analysis can reveal suspicious activities. In contrast to full heuristic analysis (analysis with code emulation), which is a separate test, fast heuristic analysis does not carry out consistent pseudo-operation of the instructions. It is not able to detect new mutation viruses protected by an as yet unknown encryption routine.

Fast heuristic analysis can be switched off in Scan-test settings. If active, the ‘bullet’ is green, otherwise it is grey.

During the Scan-test the above techniques appear to the user as one compact test. The advantage of this is that the file being tested is checked thoroughly and the test can thus detect both known and also the great majority of unknown viruses.

Virus Detected

If Scan-test or Heuristic analysis detects a virus the user is alerted and offered choices for the next action.

Menu options depend on whether the virus was found in the system region or in a file.

Virus in system region:

Continue
Continues testing system regions or starts testing files. The virus is left in the infected area.

Information
Gives detailed information about viruses found.

Remove
Removes virus from system area using one of the two following techniques:

Repair
Treats the infected system area using the general technique based on the fact that practically all viruses of this type use the same principal to spread.

Reconstruction
With hard disks this replaces the infected system area by the previously created backup copy (see Backup of system area in Utilities menu). With diskettes the infected boot sector is replaced by a generally valid structure.

As the system areas are of key importance, it is possible to make an UNDO disk before running Repair or Reconstruction. If switched on in Settings, a name and path for the UNDO file must be entered when prompted. This file can be used at any time later (see Complete Reconstruction in Utilities menu) to restore the area to the state it was in before running Repair or Reconstruction.

File Virus:

Continue
Calls up the menu with the option to continue until another infection is found or to continue non-stop.

Information
Displays more detailed information about the tested file.

Remove
Calls up a menu with the following items:

Repair
This, if successful, removes the virus from the infected file and returns the file to its original state. AVG contains two treatment techniques:

Heuristic treatment

Heuristic treatment is not available in the scan-test. To remove a virus we recommend that full heuristic analysis is used as this has a greater success rate than scan-test treatment.

Reconstruction

File reconstruction uses data from the comparative database (see chapter Comparative test) to restore the infected file to its original state. We recommend that the infected file is backed-up prior to treatment (see Settings - Common settings for all tests - Create backup file).

Rename

Renames an infected file. Suitable for situations where the infected files are to be preserved on the device without being changed but also without the danger of their being executed unintentionally.

Erase

Deletes the infected file so that it cannot be restored.

Repair all

Repair all is the same as Repair except that the program automatically tests the remainder of the device and tries to repair all the infected files it finds - best for treating devices with many infected files. However, the device must be tested again to ensure that all viruses have been removed.

Abort test

Ends Scan-test prematurely.

Heuristic analysis

Principle of heuristic analysis

Heuristic analysis, unlike the Scan-test, does not look for anything specific in the objects being tested. Rather, it examines the code in the file, i.e. it follows the instructions and analyses their practical meaning. It is able to pick up dubious activities of a program (e.g. taking control over the operating system or a non-standard method of becoming memory resident). Each incorrect activity is characterised by a "flag" - a letter from A to Z or a to z. Each flag has a different value - not every symbol has the same weight. During the heuristic analysis the virus database is continuously checked for a known virus. When the total weight reaches a critical limit and no match is found in the virus database, the virus is declared unknown.

The system areas of the device are tested first (AVG determines the type of device and how the system areas will therefore be tested). For hard disks this means the partition table and the boot sector. For diskettes it is only the boot sector. With network devices or with some pseudo-devices the test of the system area is omitted since these areas are under the control of the network operating system.

If the system areas are in order, the program continues testing files, otherwise, the user is alerted.

After testing the system areas Heuristic analysis continues testing files. During the test, AVG displays the tested file/directory and any important information is reported in the lower part of the window. This gives not only information on infected but also on non-standard files. Reporting non-standard files can be suppressed in the menu Settings - Heuristic analysis settings - Report non-standard files.
If an infected file is found the type and name of the virus is displayed, if known. Options for removing the virus are offered - see Virus detected.

After carrying out a test, a summary is displayed - the number of files tested, the number of viruses found and files treated etc.

Comparative test

Each infection changes its victim - files in their size and contents, sometimes also the date and time is changed, system areas merely in their contents. This fact is used by the Comparative Test, which creates and maintains a database (called the comparative database) by means of which it can determine what has changed.

Before the test, the device to be tested must be selected - see Selection of devices.

The course of the comparative test depends on whether the comparative database exists for the selected drive.

If there is no comparative database on a device to be tested the user is informed and the option to create one is offered. The default name for this file is AVG.GRS and can be changed in the menu Settings - Comparative test settings.

If a comparative database already exists on a tested device, the comparative test follows - comparing data from the database with data on the drive. The comparative test is fully automated and information about the currently tested directory and file is shown, a brief description of any changes is also displayed. When the test is completed, all detected changes are again displayed together with a detailed description. The comparative test detects these types of change:

<u>Change in system area</u>
This change should be taken seriously. Unless a new operating system, some system software or new hardware (new hard disk, etc.) has been installed since the last test this change is a strong indication of a virus attack. A change in the system area (boot sector) of pseudo-devices (e.g. compressed disks - Stacker, DoubleSpace...) may not be caused by a virus.

<u>Change in file</u>
The comparative test has found a discrepancy between the file and its record in the database. If there is no known reason for the file to have changed since last tested (e.g. replaced by a new version), this discrepancy may signal virus infiltration. It is important to know what has changed - a change in the file attributes or in the time of creation is not as important as a change in the content of the file and/or its length.

<u>File deleted</u>
A file recorded in the database was not found. It has probably been deleted, renamed or moved to another directory.

<u>File is new A file exists on the device but has no record in the database.</u>

<u>Evaluating changes</u>
When testing is over, the changes are listed. It is up to the user to mark changes which are considered correct, and record them in the database as a standard for future tests.

The new and/or deleted files can be updated automatically according to the settings - see menu Settings - Comparative test settings.

Comparative Test Results

When Comparative Test is finished, a list of changes is displayed. The following types of changes are distinguished:

Change in system area
This change should be taken seriously. Unless a new operating system, some system software or new hardware (new hard disk, etc.) has been installed since the last test this change is a strong indication of a virus attack. A change in the system area (boot sector) of pseudo-devices (e.g. compressed disks - Stacker, DoubleSpace...) may not be caused by a virus.

Change in file
The comparative test has found a discrepancy between the file and its record in the database. If there is no known reason for the file to have changed since last tested (e.g. replaced by a new version), this discrepancy may signal virus infiltration. It is important to know what has changed - a change in the file attributes or in the time of creation is not as important as a change in the content of the file and/or its length.

File deleted
A file recorded in the database was not found. It has probably been deleted, renamed or moved to another directory.

File is new
A file exists on the device but has no record in the database.

Evaluating changes
When testing is over, the changes are listed. It is up to the user to mark changes which are considered correct, and record them in the database as a standard for future tests.

The new and/or deleted files can be updated automatically according to the settings - see menu Settings - Comparative test settings.

Mouse click selects/deselects a changed file.

To select/deselect groups of files, choose from the following:

Select all
Deselect all
Select changed
Deselect changed
Select erased
Deselect erased
Select new
Deselect new
Other choices are:

Information - gives more detailed information on a change found.

Exit without update - ends the comparative test without updating the database.

Update database - ends the comparative test and updates the database with all selected changes.

The last screen displayed by the Comparative test is a window containing the test results.

This window is common to all tests and only items relevant to the type of test run are highlighted.

RAM test

This tests memory for the presence of a virus. It is run automatically when AVG is started unless suppressed in Settings - Common settings for all tests or by using the parameter /NOMEM. Note that AVGSYSW.EXE must be loaded before running Windows.

Scheduler

Allows a time interval (in days) for a scheduled test to be defined. Whenever AVG is run the date is checked and the user is prompted when the time has come to run the test.

Particular directories can be selected - see Selection of device and General settings (Use last list)

Macros

Macros are a useful way of carrying out frequent tests.

A macro file is a text file containing AVG commands which can have any name but its extension must be MAK.

AVG checks for MAK files on start-up.

A list of macros is evoked by clicking on the macro icon (camera).

The following commands can be used in a macro:

SCAN - activates Scan-test. The full syntax is:

```
SCAN <DEVICE:<\DIRECTORY<\FILE>> <:number of days>
```

DEVICE:\DIRECTORY\FILE - device and/or directory, or a particular file which is to be tested.

:number of days - time interval between tests run from command file. If omitted or set to 0, the command is always executed.

Example

```
SCAN C: D:\MYDIR:7
```

Runs Scan-test, if more than 7 days have passed since the last test, on the whole of C: drive but on D: only directory \MYDIR is tested.

COMP - activates comparative test. The syntax is the same as for the SCAN command.
HEUR - activates heuristic analysis. Syntax is the same as for the SCAN command.

/SUBDIR<+/->
Turns on/off testing of subdirectories.

/ANALYSIS<+/->
Turns on/off fast heuristic analysis.

/REPORTfilename
Defines the name of the file to which the results of the tests are to be logged.

DOS/FASTREAD<+/->
Turns on/off fast reading.

/XMS<+/->
Turns on/off XMS memory usage.

/STEALTH<+/->
Turns on/off anti-Stealth technology.

More detailed information on the parameters /FASTREAD, /STEALTH and /XMS can be found in the chapter Settings.

Scan-test settings

The following parameters can be set for Scan-test:

Extension
Extension box contains the following:

Default - this group cannot be changed

Other - user definable list of extensions is used

Extensions... - to customise a list of extensions

It should be noted that files like *.TXT, *.DBF are not important as far as viruses are concerned. Only program files (*.EXE, *.COM *.OVL etc.) and some document files (*.DOC) should be tested. Testing, for example, text files could lead to false alarms.

Report non-standard files
Determines whether non-standard files (PKLITE, DIET, LZEXE, immunised programs etc.) will be reported.

Quick analysis
Determines whether fast heuristic analysis will be used during a scan-test - see chapter Scan-test.

Test without messages
By default messages are displayed during testing when an infected or a suspicious file is found. Testing is suspended and continues only after user intervention.
If Test without messages is set to YES, then scan-test will run non-stop until all files have been tested and action can be taken when finished.

Scheduler
Allows a time interval (in days) for a scheduled test to be defined. Whenever AVG is run the date is checked and the user prompted when the time has come to run the test.

Heuristic analysis settings

The following parameters can be set for heuristic analysis:

Extension
Extension box contains the following:

Default - this group cannot be changed

Other - user definable list of extensions is used

Extensions... - to customise a list of extensions

It should be noted that files like *.TXT, *.DBF are not important as far as viruses are concerned. Only program files (*.EXE, *.COM *.OVL etc.) and some document files (*.DOC) should be tested. Testing, for example, text files could lead to false alarms.

Report non-standard files
Determines whether non-standard files (PKLITE, DIET, LZEXE, immunised programs etc.) will be reported.

Export suspicious files
Determines whether heuristic analysis will save a sample of a suspicious file to _GRISOFT.VIR

Test without messages
By default messages are displayed during testing when an infected or a suspicious file is found. Testing is suspended and continues only after user intervention.

Scheduler
Allows a time interval (in days) for a scheduled test to be defined. Whenever AVG is run the date is checked and the user prompted when the time has come to run the test.

Advanced
Contains the following options:

Time limit
Limits the time spent on testing each file. The default is ten seconds. It is important to realise that for the great majority of files this limit is not reached.

Depth and Maximum number of instructions
These two parameters influence the number of instructions tested by heuristic analysis. They have a very similar function but differ in one important fact. The parameter ‘Max. number of instructions’ sets the number of instructions to be tested. Depth of test determines how far down the program listing analysis should penetrate.
The difference between the two parameters is best shown by the following example. Imagine that there are repeating cycles in the code of the program under test. In repeatedly passing through these cycles the number of instructions counted continually rises but the depth of penetration ignores this repetition and increases only as the analysis penetrates deeper into the file.
The default values are 400 for the depth and 1,000,000 for the maximum number of instructions.
Significantly faster execution of heuristic analysis can be achieved by decreasing these parameters but at the risk of not detecting complex polymorphic viruses.

Analyse non-standard files

Files with non-standard structure - those produced by PKLITE, DIET, LZEXE etc. take longer to analyse. Although heuristic analysis recognises these files their analysis is usually unnecessary.

Sensitive cycle detection

Analysis can detect the occurrence of loops in a program and pass through them quickly. With high sensitivity even complex and fragmented viruses can be detected. Low sensitivity speeds up the test at the cost of the potential to detect complex polymorphic viruses.

Alternative addresses

Examines the code reached by a conditional jump. Using this feature makes information about the possibility of a virus in a file more complete but could lead to a false alarm.

Special mode (for treatment)

Heuristic treatment is based on the fact that the most modern viruses can preserve their host in an executable state - the virus temporarily returns the host (infected file) to its original uninfected state so that it can be run. A certain guide to the possibility of heuristic treatment is given by the flag {B} - return to entry point. If this flag appears amongst those found by the analysis, heuristic treatment will probably be successful.
Special mode of heuristic analysis can help to remove some very complex polymorphic viruses when flag {B} is not shown.

Emulate instruction queue

The effort to speed up execution of instructions led Intel to use instruction queues. The processor reads instructions from memory, which it anticipates will be needed, into a queue. If a program changes an instruction in memory which is already in the queue, the CPU may not know this and process the original instruction. Manipulating instructions in this way is a relatively common technique used by viruses as a defence against being tracked or analysed. Instruction queues did not exist on 8086 processors, and although the Pentium has them it can recognise any mismatch and re-read the instruction. AVG sets this parameter to a value corresponding to the processor it is running on. With an 80286, 80386 or 80486 it is on, with an 8086 or a Pentium emulation is off.

Show

Updates the graph to show the effect of any changes.

Comparative test settings

The following parameters can be set for Comparative test:

Extension
Extension box contains the following:

Default - this group cannot be changed

Other - user definable list of extensions is used

Extensions... - to customise a list of extensions

It should be noted that files like *.TXT, *.DBF often change and are unimportant as far as viruses are concerned. Only program files - *.EXE, *.COM *.OVL etc. should be tested.

New and Erased files
The comparative test detects and reports not only changed files, but also new files (their checksum is not in the database) and erased files (their checksum is in the database but the files are no longer on the drive). These changes are usually not of great value and the user can therefore set the update to automatic - that means that new and erased file checksums will automatically be updated in the database and user confirmation is not required.
It should be noted that, to a certain extent, automatic updating reduces control over some types and changes and should be chosen only in justifiable cases.

Database name
Sets the name of the comparative database - default is AVG.GRS.

Scheduler
Allows a time interval (in days) for a scheduled test to be defined. Whenever AVG is run the date is checked and the user prompted when the time has come to run the test.

General settings

Settings common to all tests.

Test RAM Upper Memory
Determines whether Memory RAM test will test memory in the region 640KB-1MB.

Create backup file
AVG can create a backup of an infected file before each attempt to repair. This copy can be useful if repair is unsuccessful -   the infected file has been unrecoverably damaged. A functional, although infected, copy of the file is retained. The extension of the backup is altered - e.g. COMMAND.COM becomes COMMAND.C##.

Memory test on start
Determines whether memory is tested on starting AVG.

Double Click with Mouse
To simplify the selection of devices, a double click of the left mouse button can be used. The default setting for double click is Start test. Other possible settings are Directory selection, Add to list or Not used.

Start test - starts test.

Directory selection - selects directory to be tested.

Add to list - adds a selected device/directory to the list of areas to be tested.

Not used - double clicking has no effect.

List of tested areas
Determines whether the list of tested areas is to be cleared or preserved from the last test.

Environment settings

Contains the following:

Sound
Determines whether AVG uses sound effects on detecting an important event.

Report
Sets the name of a report file, into which AVG will write extra information about tests.

Save configuration
Configuration changes can be saved automatically to AVG.CFG on exit. AVG creates a configuration file with the name AVG.CFG. AVG for WINDOWS creates a configuration file with the name AVGW.CFG. Thus the two programs may have different configurations saved.

Password
AVG contains privileged functions accessible only after a valid password has been entered. The standard generally valid password cannot be changed and is located in the {PWD} file on the installation diskette.
Apart from this password it is possible to define a user password and use it in day to day work. The use of such a password is possible only if a valid password has been entered in the current session.

Font
The font in the menu information line can be changed. AVG must be re-started for this to take effect.

Save configuration
Unless changes to settings are saved, they will apply only for the current session. To save the configuration automatically on exit check the box.

Network communication

In a Novell Netware environment it is possible to use the Network communication feature, but in the DOS version only. If enabled and the user/group is valid, then a message will be sent if scan-test or heuristic analysis finds a virus on your computer.

If network messaging is set to YES, the name of the user to whom messages should be sent must be entered. The file to which the messages are sent must be specified - in case the recipient is not accessible.

The network administrator must ensure that the AVG user has the necessary rights to create the log file in the given directory.

Save settings to disk

Unless changes to settings are saved, they will apply only for the current session.
A configuration can also be saved automatically - see Settings - Environment settings.

If in the current session the password to access privileged functions was entered, saving of configuration file is linked to it. If a password is not entered in later sessions, changed configuration cannot be saved so that a user not knowing the password cannot overwrite the configuration created by system administrator - configuration can be changed for current session only.

Default setting

Default settings
Restores settings to default values. This feature is privileged and is available only after entering a valid password in Utilities.

Password

A password protects those features of AVG which are considered as privileged. These features are not accessible as standard (they are coloured differently in the Menu) and must first be activated with the password.

Default password
This password, which is always valid, is stored in the file {PWD} on the installation diskette. This file is not copied to the hard disk during installation.

Users password
Apart from default password it is possible to define another password - see Environment settings.

Backup system areas

The system areas of disks and diskettes carry information vital to the correct running of a computer and are the prime targets of some viruses.

Removal of viruses from these regions is a very sensitive procedure entailing the possibility of a system crash. The simplest and most reliable method is to back them up. If system regions are infected and/or damaged then they can be restored to their original condition.

All important system areas are stored in one file from which they can be retrieved. In AVG the following areas are backed up:

Partition table
Extended partition tables
Boot sectors of hard disks
CMOS memory.

Devices which DOS views as ‘networked’ cannot be backed-up.

The first step is to name the backup file. The default name is A:\SYSTAB.GRS. Both name and path can be changed.

Do not save backup copies to the hard drive as they will be inaccessible if the system crashes - save them on a diskette.

Backup follows entry of a file name. If this file already exists, the user is warned and must confirm that the file be over-written. AVG also checks that backup copies are not infected - in this case the program refuses to create a backup.

Restoring system areas

The menu item Restore system areas opens a dialogue box from which the selection is made.

Restore partition table and Restore boot sector
A list of devices is displayed. The file containing the backup must be selected. AVG will accept only a file with the correct structure and restore only after further confirmation.

Restore CMOS memory
The date and time will not be restored.

Single Step

This feature is for advanced users only and makes full heuristic analysis accessible in the form of a debugger. It allows selected code to be tested instruction by instruction. It is intended for users with   advanced knowledge of the system and assembler so that they can judge whether code is correct or not.

With this tool you can test:

Selected files
Partition table
Boot sectors

For Single step the following parameters can be set:

Cycle detection - jumps to repeating addresses are detected
EXE re-location - recalculation of relocations in EXE files is made.
Log file - creates single step report file

Updating AVG

In view of rapid developments in the virus world, the AVG antivirus system is being developed continuously. There are two ways in which GRISOFT(c) SOFTWARE keeps its customers up to date:

New versions of AVG
These are issued regularly (approx. once a year). The new versions involve considerable qualitative changes, i.e. improved techniques for searching for viruses, new functions, and so on. All registered users are notified by the manufacturer and can purchase the Upgrade at a discount.

Updating AVG
Updates are released every month. These include new virus information and minor changes to the program. All files are in one self-extracting archive and can be downloaded from the Internet free of charge (WWW: http://www.anet.cz/grisoft). A postal diskette service is available at a nominal cost.

The distribution file has the following format: xxyyyAVG.EXE, where

xx - year in which updated program was created, e.g. 95
yyy - number of the day of the year in which the program was updated (e.g. 046 = 15 February).

If an incorrect registration number is entered when AVG is installed your copy will be unregistered and the program cannot be updated. In this case we recommend installing the AVG system again and paying greater attention to the serial number.

How to contact us

International contact:

GRISOFT (UK) Ltd.
P.O.BOX 296
Sevenoaks
Kent

E-mail: grisoft@pcshop.ftech.co.uk