VirusDetective® Help
Main Window

PREVENTION IS THE BEST CURE !
– that is our motto.

VirusDetective, our main anti-virus product, is a desk accessory for the Macintosh that unearths and sniffs out viruses, Trojan Horses and worms BEFORE the HTDs get a chance to get at your disks and unleash their havoc. VirusDetective may be considered a “DETECTION TOOL”. First you have to find ‘em before you can get rid of ‘em – AND find them before it’s too late and you have an infected Macintosh on your hands. Shulman Software excels in the ‘finding’ part which means finding viruses BEFORE any damage is done, not ‘after the fact’.

TABLE OF CONTENTS…

---

i) PREFACE… DEFINITIONS…

Before you get into this Main Window Help file in any depth, a couple of definitions and explanations are in order:

DEFINITION: “Hexually-transmitted disease” (HTD for short): any virus, Trojan Horse or worm; a file that has an HTD is an “infected” file.

DEFINITION: “A search string has matched the contents of a file”: this is technical jargon for when VirusDetective has found an HTD (virus, Trojan Horse, or worm). In technical terms, a file on the Macintosh is made up of either a resource part (called the resource fork) or a data part (called the data fork), or both. (NOTE: the majority of viruses infect the resource fork.) As a non-technical VirusDetective user, you need NOT know about resource forks and data forks.

Whenever you see something like “A search string matched the resource part of a file or data part of a file” or simply “A search string matched a resource”, know that VirusDetective has found an infected file. It is the same as saying “A search string found an infected file”.

In the event that a search string matches a file but it turns out NOT to actually be an HTD, it is a “false alarm” (a “ false positive”). Statistically, false positives cannot be prevented – they happen occasionally no matter what you do to prevent them.

A) STATUS BOX (THE BOX WITH THE FANCY BORDER) [ON COLOR MONITORS, THIS BORDER IS

IN COLOR]…
This is the “Status box”. The Status Box shows you what’s happening while it’s scanning. The Status box is divided into three sections: the SCANNING section (the first line), the PROGRESS BAR (the second line; the progress bar is invisible unless you are doing a full disk scan), and the MATCHED section (the third and fourth lines).

A.1 The “Scanning” Section (the first line)…
As VirusDetective is performing a scan (a scan is the same as a search), the SCANNING section shows you exactly what files and disks are being scanned as the scanning is happening. Also, whenever VirusDetective is performing a scan, VirusDetective’s four-diamond cursor will be evident.

Without having VirusBlockade installed, VirusDetective scans only when YOU manually start a scan, with one exception. This exception is when you click the Automatically scan floppy disks when VirusDetective is open checkbox; when you click this checkbox, you are telling VirusDetective you want it to scan floppy disks automatically while VirusDetective is in either the ACTIVE mode or the INACTIVE (background, deselected) mode.

You can control whether VirusDetective ejects the floppy disk (or not) after it finishes a scan. After VirusDetective does a scan: 1) if it doesn’t find an HTD, and it IS the active window, it EJECTS the floppy disk; 2) if it doesn’t find an HTD, and it is NOT the active window, it doesn’t EJECT the floppy disk.

When VirusDetective begins scanning when it is an active window, and then you deselect it and place it in the background: 1) under System 6.x, VirusDetective halts scanning until you make VirusDetective the active window again; and 2) under System 7.x, VirusDetective continues scanning.

A.2 The “Progress Bar” (the second line)…
The PROGRESS BAR appears in the second line only when VirusDetective is in the midst of a full disk scan; otherwise, the Progress Bar does not show up at all. The Progress Bar (on color monitors, the Progress Bar is blue) tells you how far along the disk scan is. As progress continues, the names of files show up in the SCANNING section, sometimes so fast that the files’ names flash by at a rapid clip.

A.3 The “Matched” Section (the third and fourth lines)…
When a search string finds an HTD, VirusDetective pauses. VirusDetective pauses to tell you that it found something and what it was that it found. During the pause, the SCANNING section shows you what the infected file’s “pathname” is (the pathname is where to find the file, specifically, what disk the file is on, what folders the file is in, etc.). If the pathname is too long for the space allotted for it, it’ll show just the beginning and tail end of the pathname. The MATCHED section also shows which search string it was that found the infected file so that you have an idea of what you are up against.

After VirusDetective finishes a scan, it shows the number of infected files in the SCANNING section; the total number of files scanned shows up in the MATCHED section.

B) “SCAN FOLDER/DISK” TO “HELP” (THE SET OF BUTTONS THAT LETS YOU CONTROL THE CONDITIONS UNDER WHICH VIRUSDETECTIVE SCANS)…

B.1 “Scan Folder/Disk” button…
When you click the Scan Folder/Disk button, VirusDetective presents a directory dialog box that lets you search various folders’ or disks’ contents. You cannot scan individual files using this button – to scan individual files, click the Scan One File button.

When you press the Option key and the Scan Folder/Disk button, the button changes to Scan All Disks.

If you want a written log of the scanned or matched files, see the Log File Options in the Options dialog box.

On System 6.x systems, the directory dialog box contains these buttons (among other buttons): Scan This Fldr, Scan Fldr, Scan Entire Disk and Open Fldr. The Scan This Fldr and Scan Fldr buttons are similar but work somewhat differently. The Scan This Fldr button (above the pop-up menu) scans the current folder (the folder which shows up in the pop-up menu); in contrast, the Scan Fldr button (fifth button down on the right side) scans the highlighted folder. The Scan Entire Disk button (under the directory) scans the current disk in its entirety. The Open Fldr button opens the highlighted folder until you can't open anymore folders.

On System 7.x systems (and later), the directory dialog box contains these buttons (among other buttons): Open Fldr, and Scan Fldr. The Open Fldr button opens the highlighted folder until you can't open anymore folders. The Scan Fldr button scans the highlighted folder. When the Desktop level is showing, these buttons change to Open Disk and Scan Disk which opens and scans the highlighted disk, respectively.

B.2 "Scan One File" button…
When you click the Scan One File button, VirusDetective displays a directory dialog box that lets you scan only one file (the highlighted file) at a time. When you click Open, it starts scanning the highlighted file.

If you want a written log of the scanned or matched files, see the Log File Options in the Options dialog box.

B.3 "Options" button…
When you click the Options button, an Options dialog box appears that lets you choose from various options. These options are: Log File Options (No Log, Log All Files, Log Only Matched Files, Write File/Resource Information to Log File), Create Log File (Separately for Each Disk, Single File), Log/Save Files in the Form of (MacWrite, MacWrite II, TeachText, WriteNow, Word, any other 4-character Creator you choose), No Scan Cancel in VirusBlockade, Unattended Operation, and No Error Msgs., Options Help, Help-> Clipboard, Cancel and Save buttons. The Options dialog box has its own Help file.

B.4 "Password" button…
If you don't want anyone to be able to fiddle with the way you have VirusDetective set up (Options dialog box, Search Strings dialog box or the Automatically scan floppy disks when VirusDetective is open checkbox) as opposed to preset options, then definitely consider using a password. With a password set, once you close VirusDetective, if anyone tries to make any changes, VirusDetective asks the user what the old password is; if that user doesn't know what the old password is, (s)he can cannot make any changes. Any user can still perform scanning while VirusDetective is password-protected.

As you type the password, your password does not show up on the screen, rather – the character • shows up. After you type the password the first time, VirusDetective prompts you to type in the characters of the password a second time (to make sure you got it right). After you input the identical password a second time, the password takes effect after you click the Save button. Passwords must be 255 characters or less.

To clear (get rid of, wipe out) a password: when VirusDetective asks you for the NEW password, don't type anything and click the Save button.

B.5 "Search Strings" button…
When you click the Search Strings button, the Search Strings dialog box appears. The Search String dialog box allows you to add, remove, change and save search strings, plus read from a search string file and write to a search string file. The topmost item is the search string list itself. The second item down is

the input field where you type in your own search strings or change existing search strings. You can copy from a search string and paste it into the input field (you can't cut; use the Remove button). The third set of items are the Add, Remove, Read to File and Write to File buttons. The Search Strings dialog box has its own Help file (the fourth item). The fifth and last set of items is the Help->Clipboard, Cancel and Save buttons.

NOTE: You don't have to understand the search string language (the syntax) for VirusDetective to work. Whenever a new HTD emerges, we furnish you with the new search string that will protect your Macintoshes from that HTD (if you are a registered VirusDetective user, we send you a flyer or postcard; if you are not a registered VirusDetective user, you can get it off the major electronic bulletin boards). All you do is add the new search string to the set of search strings that already resides in your VirusDetective desk accessory. You don't have to devise any of the search strings yourself.

However, you DO have the option of writing your own search strings, but we ask that you do this only if you are motivated to become familiar with how the search string syntax works (see the Search String dialog box Help file). Study the search string syntax first.

B.6 "About" button…
When you click the About button, VirusDetective presents you with the About dialog box. The About dialog box is important to read because it tells you a number of things: the author of VirusDetective, the author's company address, telephone number, electronic addresses, when author is personally available by phone; how to become a registered user, where to send payment, how much, and in what form; when you register, what you we mail you very soon after we receive your registration and payment; technical support and continuing customer service; system requirements; briefly, what VirusDetective and VirusBlockade do; a powerful new VirusBlockade feature called "SUPERFAST FILE SCANNING" (including on file servers); repair and removal by VirusBlockade in the not-too-distant future; a little on search string programability; other major changes in comparison with earlier versions; and where to go for further information.

If you want to copy the contents of the About box to the Clipboard, click the Text->Clipboard button. Paste the contents of the Clipboard wherever you wish (most likely a word processing program).

For more detailed information, read the separate Help files of various dialog boxes.

B.7 "Help" button…
<You are in this file now.> If you want to write the text file to the Clipboard, click the Help->Clipboard button. Paste the contents of the Clipboard wherever you want them (which would probably be in your favorite word processing program). Click the OK button when you want to close the Help file.

C) "NEXT FILE" TO "CANCEL" (THE SET OF BUTTONS THAT IS ONLY AVAILABLE WHEN A SEARCH STRING FINDS AN HTD, EXCEPT THE "CANCEL" BUTTON)…

C.1 "Next File" button…
When you click the Next File button, VirusDetective goes on to search the next file – it skips over the remainder of the current file. It means you are finished with the current file.

C.2 "Next Search String" button…
When you click the Next Search String button, VirusDetective stays in the same file but goes on to the next search string, skipping the current search string. (The same search string can match several different spots in the same file. This would apply if you want to find only the first of those different spots.)

C.3 "Show Info" button…

When you click the Show Info button, VirusDetective divulges detailed technical information about the infected resource or infected file. In actuality, VirusDetective shows you one of two possible information dialog boxes – if a search string matches a resource, the Resource Information dialog box appears; otherwise, the File Information dialog box appears.

The Resource Information dialog box "tells" you specific information regarding the infected file: which search string it was that matched the resource, the File's Name, the last Modification Date, Resource Type, Resource Size, and Data Search Offset; it also lets you "change" the Resource's Name, the Resource's ID, and the Resource's Attributes, as follows:

NOTE: As mentioned above, the "Resource Information" dialog box allows you to change the Resource Name, Resource ID, and Resource Attributes (System heap, purgeable, locked, protected, and preload). ONLY knowledgeable, advanced Macintosh users should consider changing ANY of these selections! If you don't know what you're doing, you can easily render the file permanently non-functional!

When you want to save changes in the Resource Information dialog box, click the Save button. Click the OK button to close the dialog box.

The File Information dialog box shows which search string matched the file, the File Name, File Type, File Creator, Creation Date, last Modification Date, Resource Fork Size, Data Fork Size, and Data Search Offset.

When you want to close the File Information or Resource Information dialog box, click the OK button.

C.4 "Eject" button…
When you click the Eject button, if the infected file is located on a disk that is "ejectable" (such as a floppy disk, compact disc, removable hard disk), given this command, the disk drive ejects the disk. If you attempt to eject your hard disk, be sure to duck!

C.5 "Delete File" button…
When you click the Delete File button, VirusDetective permanently deletes the infected file for you. VirusDetective asks you first to confirm if you REALLY want to delete the file.

C.6 "Remove Resource" button…
When you click the Remove Resource button, VirusDetective removes the matched resource of the infected file. You should almost NEVER use this button – and if you do, you should know EXACTLY what you are doing ! CONSIDER YOURSELF FOREWARNED !

NOTE: MOST VIRUSES ARE NOT STOPPED BY REMOVING ONLY ONE RESOURCE! ONE EXCEPTION TO THIS RULE IS IN REGARD TO "DESKTOP" VIRUSES (WDEF, MDEF AND THE LIKE): IF YOU ARE NOT (I REPEAT) NOT USING MULTIFINDER, IF YOU CLICK THE REMOVE BUTTON, VIRUSDETECTIVE SAFELY RIDS YOUR MACINTOSH OF WDEF AND MDEF (AND OTHER VIRUSES WHICH DAMAGE THE DESKTOP) – THIS IS THE ONLY CLASS OF VIRUSES THE "REMOVE RESOURCES" BUTTON IS DESIGNED TO SUCCESSFULLY REMOVE!

C.7 "Continue" button…
The Continue button becomes active after VirusDetective has paused right after it has found an infected file. When you click the Continue button, VirusDetective resumes where it left off before the pause.

C.8 "Cancel" button…
When you click the Cancel button, it means you don't want the search-in-progress to proceed.

D) “AUTOMATICALLY SCAN FLOPPY DISKS WHEN VIRUSDETECTIVE IS OPEN” CHECKBOX…
This section contains only one item, the Automatically scan floppy disks when VirusDetective is open checkbox. Without having VirusBlockade II 2.0 (or later) installed, this checkbox (if clicked) tells VirusDetective you want to be able to scan floppy disks as you insert them, even if VirusDetective is NOT the active window. This checkbox allows you to either quickly scan a whole bunch of floppy disks one after the other (when VirusDetective IS the active window) or scan floppy disks on a sporadic, as needed, basis (when VirusDetective is NOT the active window).

Whenever VirusDetective IS the active window and finds an infected file, VirusDetective pauses for you to respond, and the floppy disk is NOT ejected.

Whenever VirusDetective: 1) is NOT the active window, 2) IS creating a log file, and 3) finds an infected file, VirusDetective completes the scan, alerts you that it found at least one infected file, and does NOT eject the floppy disk. The log file gives you the “trail” by which to see exactly what HTDs VirusDetective has found and in what quantity.

Whenever VirusDetective: 1) is NOT the active window, 2) is NOT creating a log file, and 3) finds an infected file, VirusDetective stops immediately, alerts you that it found at least one infected file, and does NOT eject the floppy disk. Because you have no log file, you have no “trail” by which to see exactly what HTDs VirusDetective has found and in what quantity.

NOTE: Due to a bug in System 7.0, the floppy disk icon will remain on the Desktop (which it shouldn’t) after the floppy disk is ejected. When Apple corrects this problem, a new version of VirusDetective will be made available. This bug does NOT appear on any System 6.x.

To close VirusDetective, it must be the active window. Then click on the close box or use Command-W.

-the end -