

RezSearch 1.0b © 1988

by Wade Blomgren
UC San Diego Academic Computing
Mail Code B-028
La Jolla, CA 92093
wade@sdacs.ucsd.edu

This software is provided "as is", with no warranties. Use it at your own risk. Regardless, the author takes responsibility for the existence of this software, and in particular the University of California bears no responsibility for the content or performance of the software. You may freely redistribute the program under the following conditions: This document must be included. The distribution must not be for profit. This document and the software must not be altered in any way. Please submit suggestions or bug reports to the author at the above address or via email.

Introduction:

RezSearch examines all files in an HFS volume or subdirectory, searching for resources of a specified type. Additionally, a resource ID number and size may be specified. All files which contain resources of that type, (as well as the ID# and/or size if specified) are displayed by name on the screen and optionally listed in a text file. The program is known to work on Macintosh 512E, Plus, SE, and II computers.

One possible use for RezSearch is to determine whether a disk volume has files which contain resource types known to harbor "virus" code, such as the "nVIR" resource, or the various INIT and other resources used by the SCORES virus. Although the program attempts to search for the nVIR resource type by default, any resource type code can be used for the search. By default the program will search the entire HFS volume from which it is launched. If you uncheck the Search Entire Disk box in the configuration dialog, you will be asked to specify a particular folder to search. This can be useful if you load a new group of Public Domain, Freeware, or Shareware programs onto your disk into a particular folder, and would like to examine just that folder for particular resource types (such as nVIR) without rechecking your entire hard disk. The report file created by the program is a plain text file which can be read with any text editing DA or word processor. If you attempt to run RezSearch from a non-HFS system it should complain gently and quit.

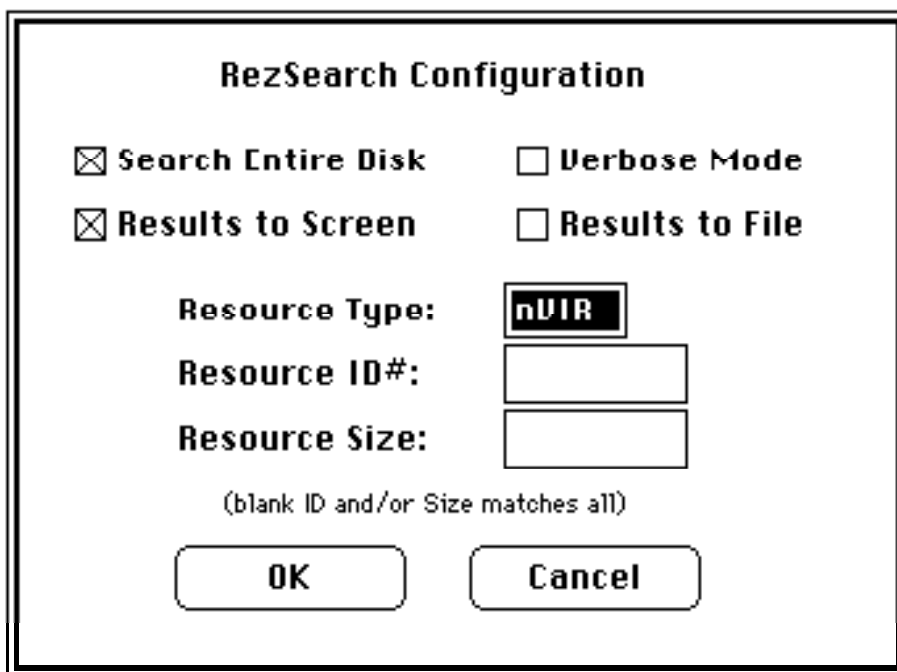
Methods for removing nVIR, SCORES, "peace", and other types of viruses have been documented in various periodicals like MacWeek and MacTutor, as well as in articles placed on Usenet, Genie, etc. Also, programs such as Vaccine from CE Software may be useful for detecting attempts at infection. In any case, methods for preventing and removing known types of viruses are beyond the scope of this program and this document. As an example of the potential complexity of virus removal, note that simply removing nVIR resources from an infected file will in general cause that application to become permanently unusable.

Using uniquely numbered or sized resources is by no means a method all virus perpetrators will use. If, however, new viruses using unique resources do surface, the characteristics of those resources will be well publicized, and you will be prepared to search for those resources. If RezSearch finds suspect resources on your disk, and you are unfamiliar with methods for dealing with those resources, please contact a knowledgeable friend or business associate for advice on how to proceed.

RezSearch may in fact be useful for tasks other than "virus hunting". For instance, you can find all files which contain FONTS or DRVRs, search for duplicate signature resources, files containing ICONs or PICTs, etc.

Instructions for use:

Copy RezSearch to the disk you want to search. Note that RezSearch may not give accurate results if it is used while MultiFinder™ is running! Double click on the RezSearch icon. A short description and Copyright notice will be displayed. Click the OK button or type return. The configuration dialog will appear. Default settings are for a complete search, with results displayed on the screen. If you want the results to be saved in a file, check the Results to File box. If you want to see each filename and directory name displayed as it is examined, check the Verbose Mode box. Enter the resource type (normally a 4 letter sequence) in the Resource Type field. You may tab to the next field or click in it. If you are searching for a specific resource ID or size, fill in the appropriate field. If you want to look for all ID numbers and/or all sizes, leave the appropriate field blank. Click the OK button or type return to proceed. (Click Cancel if you wish to abort the search and terminate the program).



RezSearch Configuration

Search Entire Disk Verbose Mode

Results to Screen Results to File

Resource Type:

Resource ID#:

Resource Size:

(blank ID and/or Size matches all)

If you have checked the Results to File box, a dialog box will be presented allowing you to specify an output file. The default file name is "RezSearch report". Specify an output file and click Save. Click Cancel to avoid saving results in a file. Note that when you specify the same output file name a second time, and tell the program to replace the existing version, the original file is overwritten, not appended to.

If you have **un**checked the Search Entire Disk box, a dialog will be presented which allows you to choose the specific folder you wish to search. Navigate through the dialog as though you were looking for a file to open from the Standard File Dialog. When you have selected the folder to search by highlighting it, click Search. If you click Cancel, the entire disk volume currently displayed will be searched by default. This is an inelegant way to search a disk other than the one RezSearch is installed on. (Use the Drive button to choose the disk you want to search, then click Cancel).

Once the search is underway, you may click the Pause button in the search results window to suspend the search, or the Stop button to abort the current search. Once the search has completed normally or been stopped, you may scroll around in the results window, Reconfigure or Quit. Reconfigure lets you alter the settings in the configuration dialog and run another search, and Quit terminates the program.

The search will make an attempt to open the resource fork of every file on the disk (or in the target folder). If the resource fork cannot be opened, and the reason is something other than the fact that no resource fork for the file exists, the error will be displayed in the results window. If you choose the verbose mode, each successive level in the directory hierarchy will be indented in the results listing, which may help you find the files which have matching resources, but the non-verbose mode is faster.