

# SYSTEM Scrutiny

## Operating Instructions

Advanced search facility developed by Russell Kempley  
Designed for use with centrally stored user data on a computer network

Development version 2.00

## Licence Information, copy of text file Licence.txt

This is a development version of 'System Scrutiny'

The term 'software' in this context includes the three executable programs which form the 'System Scrutiny' package

The content of this publication is subject to change without notice and does not represent a commitment on the part of Russell Kempley or Aquinet Systems

All files are supplied solely for the purpose of testing the software with the intention of finding errors or problems that occur when the software is used.

Neither Russell Kempley nor Aquinet Systems can be held responsible for any adverse effects, including but not limited to loss of data, which occurs as a consequence or otherwise of running the software on a host computer system.

Some components of the software are redistributable controls owned but licensed by Microsoft Corporation. Microsoft can not be held responsible for the use of these controls in conjunction with this software. The controls may not be further distributed.

All software, documentation, code and information supplied (with the exception of the Microsoft redistributable controls) are the intellectual property of Russell Kempley and Aquinet Systems. Copyright has been secured.

## Details of files supplied with Development Version 2.00

### SCRUTINY.EXE

Main program for physically performing search process. A search profile is defined specifying the directories or user sub-directories to be searched by sets of given criteria. See main section 1.2.4

Data File extension - SPF

Command line - Profile Data, Results File, Auto-Run Flag (/r)

### SSRESULT.EXE

Decodes and displays search results and messages generated by the search process. Stores deleted file data and lists root directories searched.

Data File extension - SRT

Command line - Results File

### SCHEDULE.EXE

Runs defined searched on a 24hr repeat. Designed to be used for overnight operation.

Data File extension - SCD

### SCRUTINY.DAT

Contains reference information for the three programmes (components) to enable the internal shell link function to operate correctly. A copy of the file is required in each directory which also contains one of the components. The file contains three lines which should be relative directory paths to each of the three components in the above order.

### COMCTL32.OCX, TABCTL32.OCX, COMDLG32.OCX

Microsoft redistributable files. These should be moved to the Windows System directory of the host computer system. It should not be necessary to overwrite existing copies of these files, doing so may disable other software running on the host computer

### LICENCE.TXT, README.TXT

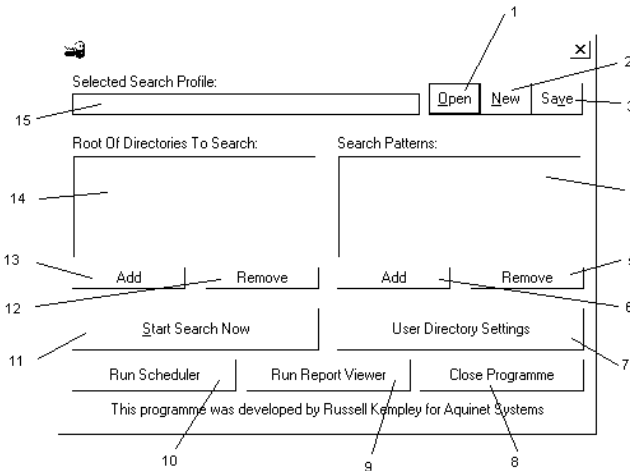
Textual information and documentation

# Documentation Contents

1. Use of SCRUTINY.EXE
  - 1.1. Opening and saving search profiles
  - 1.2. Managing search items
    - 1.2.1. Adding search item
    - 1.2.2. Search item criteria
    - 1.2.3. Loading criteria from example file
    - 1.2.4. Finding disguised files
    - 1.2.5. Removing search items
  - 1.3. Managing directory items
    - 1.3.1. Adding directory item
    - 1.3.2. Accessing network drives
    - 1.3.3. Searching user directories
    - 1.3.4. Removing directory items
  - 1.4. User directory identification settings
    - 1.4.1. Identifier files
    - 1.4.2. Manually creating identifier files
    - 1.4.3. User Work Files
  - 1.5. Shell functions
  - 1.5. Running Search
2. Use of SSRESULT.EXE
  - 2.1. Opening of results file
  - 2.2. Results display lists
  - 2.3. Sorting the results list
  - 2.4. Managing search results
  - 2.5. Interpretation of messages
  - 2.6. Forced termination of results program
3. Use of SCHEDULE.EXE
  - 3.1. Opening and saving schedules
  - 3.2. Managing schedules
    - 3.2.1. Adding schedule item
    - 3.2.2. Removing schedule item
  - 3.3. Viewing results

# 1. Use of SCRUTINY.EXE

This program is used to define and run search profiles. A profile contains a list of the criteria to be used to select files and the root directories to be searched for files matching those criteria. The search can be restricted to examine only user sub-directories of a given root.



Graphic 1.1. - main system scrutiny search dialog

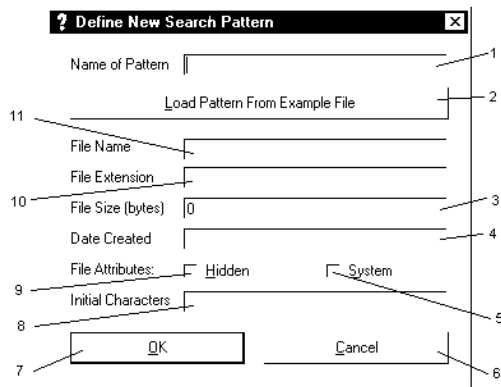
## 1.1. Opening and saving search profiles

The lists of criteria and root directories which form the search profile can be stored in a csv (comma separated variable) file with specific and multi field definition. This file is given, by default, the extension SPF.

Search profiles can be Opened and Saved using buttons G1.1.1 (graphic 1.1. item 1) and G1.1.3 respectively. Selecting these activate standard windows Open and Save dialog boxes. The filename of the currently open search profile is displayed in the text box G1.1.15. A new search profile can be started by selecting the button G1.1.2. If NEW, OPEN or CLOSE buttons are selected whilst a search profile is in use, a prompt will display with the option of saving the profile.

## 1.2. Managing search items

The list G1.1.4 displays a list of the sets of search criteria which will be applied to the files in the directories to be examined. A file needs only to be selected by one criteria to be listed in the results, implied logic OR. Each set of criteria is called a search 'item'. These items can be managed by using the ADD and REMOVE buttons, G1.1.6 and G1.1.5 respectively. Selecting the ADD button will launch the define new search item dialog.



Graphic 1.2. - define new search item dialog

### 1.2.1. Adding search item

A new search item is created by entering data into the fields in dialog G1.2. The criteria are combined using the logical AND operator, thus a file must satisfy all the criteria to be selected by the search process. An explanation of the criteria is given in the next section.

Once entry is complete select the OK button, G1.2.7 to add commit the search item to the profile. The list on dialog G1.1. is also updated with this new search item. To stop the addition of a new search item select the CANCEL button, G1.2.6

## 1.2.2. Search item criteria

Six criteria are available for selecting files during a search. These, and the associated dialog control, are: file name G1.2.11, file extension G1.2.10, date created G1.2.4, file size G1.2.3, file attributes G1.2.5 and G1.2.9, and the initial characters of the file G1.2.8.

The file name and extension are similar to standard search facilities, although this version of SCRUTINY.EXE does not support the use of wild cards.

The date created and size options are used to find known files on a system when those files have had their name and /or extension changed. This is particularly useful, and was designed, for administration of networks where all user data is stored on a central server. The facility enables the detection of files which have been disguised by users, and might for example be used to find games such as solitaire or mine sweeper, where the use of these games is not permitted - see section 1.2.4. The date is specified with the format dd/mm/yy hh:mm:ss and the size is measured in bytes. The information for both of these fields can be found from the properties dialog for a file selected in windows explorer.

The final two options, attributes and initial character check, form the advanced search tools. System and hidden files are automatically included in searches utilising the other criteria, however by selecting the hidden or system check boxes the search will return only files with those properties. This is useful for creating a list of all files with hidden attributes. The initial character check is the most powerful tool but the definition needs careful attention if the required results are to be returned. This is discussed in the next paragraph:

The maximum number of characters which can be compared is 10. If all 10 characters are used the check is very specific and can be used in conjunction with the size and date functions to ensure exact identification of a known file. The easiest method of obtaining the initial 10 characters is to use the load criteria from example file function, for more information see the next section. If only 2 or 3 characters are defined the

search become much broader and can be used to find files of a specific type. After examining several files of known format similarities between the initial characters will become recognisable. For example all executable files (which include \*.exe \*.dll \*.drv amongst others) start MZ and all zip files start PK. Performing a search for the initial characters MZ will therefore return a list of executable files in user directories even if the extensions have been changed and the file is unknown to administrators.

### 1.2.3. Loading criteria from example file

Selecting button G1.2.2 launches the standard windows open file dialog. Load the file which is to be used to define the criteria for the search. After opening, each of the six criteria fields is updated with information extracted from the file. However this function is designed to be used mainly when the filename and extension of the file in the directories to be searched may have been changed. In these circumstance the contents of the name and extension fields should be deleted. The search will then depend entirely upon matching the remaining criteria.

### 1.2.4. Finding disguised files

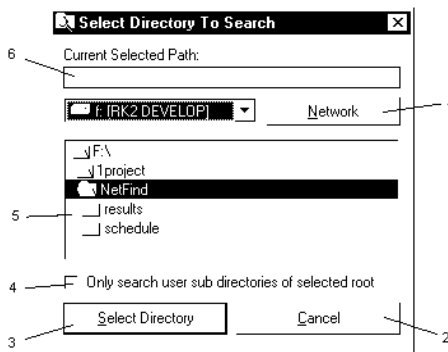
This software was initially developed for network administration purposes in a school environment. Two factors where very important in it's design. Firstly all the user data was stored on a central server so that users (students) could access their personal files from any work station. Secondly students were supposed to only use the computer system for relevant school activities. The use of other applications, such as games, run from the user work area was not permitted. However such files were widely in use, and distribution exacerbated by user access to electronic mail. Students routinely avoided scans by standard search software by changing the name and extension of executable files and screen savers to those of seemingly innocuous word or excel documents. Scrutiny was therefore developed with the intention of finding such files. As discussed in the previous two sections this is achieved by concentrating on criteria other than the name or extension.

## 1.2.5. Removing search items

Search items can be removed from the list G1.1.4 by selecting entries in that list and clicking on the remove button G1.1.5. The list supports multi-selection which can be activated by holding down the SHIFT or CONTROL key on the keyboard when selecting entries.

## 1.3. Managing directory root items

The list G1.1.14 on the main search dialog displays a list of the root directories that will be searched. Roots can be specified as containing user directories which are identified by the settings discussed in section 1.4. Each root directory is called a directory 'item'. These items can be managed by using the ADD and REMOVE buttons, G1.1.13 and G1.1.12 respectively. Selecting the ADD button will launch the select new directory item dialog.



Graphic 1.3. - select new directory item dialog

### 1.3.1. Adding directory item

A new directory item is created by selecting the appropriate path in dialog G1.3. The currently selected path is displayed in the text box G1.3.7 and this can be changed by using the drive and directory controls G1.3.6 and G1.3.5 respectively.

### 1.3.2. Accessing network drives

This search program was designed to be used in a network environment and therefore the facility is provided for accessing network shares. Selecting the NETWORK button G1.3.1 displays a dialog with a single text field. Enter the required network share path in the form \\computer\share and click OK. The directory control now displays the available paths on that share.

### 1.3.3. Searching user directories

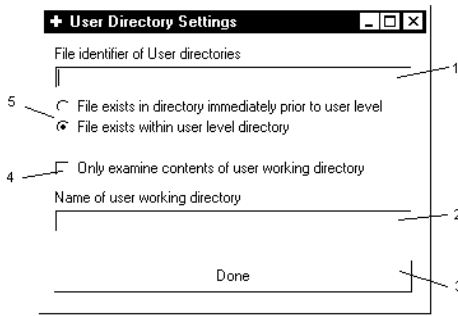
To search only user sub-directories of the current root directory, select the check box G1.3.4. The identification of user directories is dependant upon the settings explained in section 1.4

### 1.3.4. Removing directory items

Directory items can be removed from the list G1.1.14 by selecting entries in that list and clicking on the remove button G1.1.12. The list supports multi-selection which can be activated by holding down the SHIFT or CONTROL key on the keyboard when selecting entries

## 1.4. User directory identification settings

The settings used to identify the presence of user directories are accessed by selecting the button G1.1.7 on the main search dialog. Selecting this button launches the dialog form G1.4. This has fields for the name and location of identifier files, and a facility for further restricting searches to user work directories. When editing of the settings is complete select the DONE button, G1.3.3.



Graphic 1.3. - User directory settings dialog

### 1.4.1. Identifier files

Searching user directories requires the program to identify the parts of roots where these directories are located. This is done by using identifier files. The name of the identifier is entered into the text box G1.4.1. The software was originally designed for use with the RM Connect network system which includes a file called `muser.ini` at the user directory level. In addition the system can be configured to recognise identifier files in the directory immediately prior to user level. Selecting between the two possible locations for the identifier file is done by clicking on the appropriate radio button G1.4.5. Note that the search process is faster if identifier files are placed in the directory immediately prior to user level.

### 1.4.2. Manually creating identifier files

If your network operating system or management software does not automatically create files which can be used as identifiers at the user, or prior user, level directory, then these will have to be introduced manually. This can be achieved by using windows explorer to create a new text file in the first directory where an identifier is required. It is suggested that the name of this file be changed so that it is recognisable as indicating the presence of a user directory, for example `users.dir`. The file should then be copied to every other location where user directories must be identified. It is important that when new users are created the identifier files will enable `SCRUTINY.EXE` to locate them, this may involve further copying.

### 1.4.3. User work directories

The network environment, for which this software was designed, included a variety of preferences and settings stored within the user directory. These files were given read only properties and the users were restricted to working within a further sub-directory called the MyWork folder. This program includes a facility for only searching this work directory which is activated by selecting the check box G1.4.4. The name of the work directory is entered into the text box G1.4.2

### 1.5. Shell functions

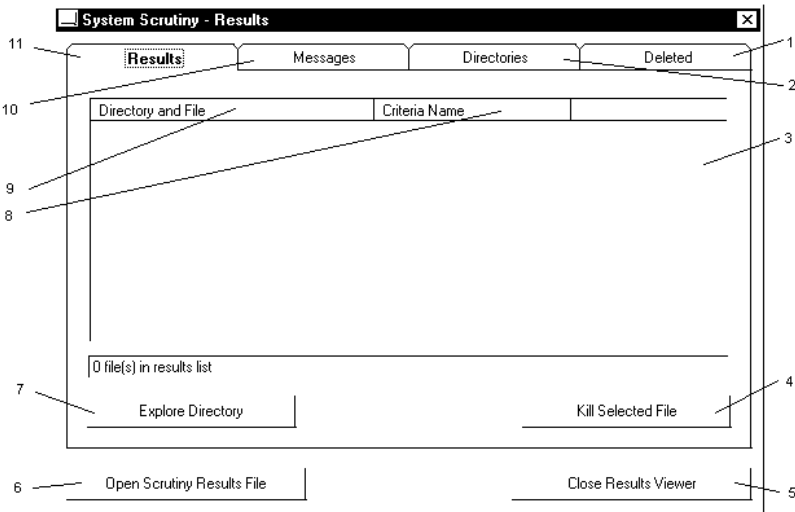
The other software modules SSRESULT.EXE and SCHEDULE.EXE can be run from the main dialog, G1.1, by selecting buttons G1.1.9 and G1.1.10 respectively

### 1.6. Running search

At least one search item and one directory item must be defined before the search will run. To activate the search select the Start Search Now, button G1.1.11. This activates the standard windows save dialog which is used to select the file to which results data is stored. Following the input of a file name, a second dialog box will appear to display the current status of the search. The process will progress through the root directories in the order in which they appear in the list G1.1.14. There is often a short period of apparent inactivity when the program catalogues the available sub-directories of the root being searched.

## 2. Use of SSRResult.exe

This program is used to interpret and display the results files generated by the search process of SCRUTINY.EXE. The original purpose of this software was to enable prohibited files found in user directories to be removed from the system. The main display dialog features four lists containing details of the files found, messages, directories searched and files deleted.



Graphic 2.1. - Results viewer dialog

### 2.1. Opening of results file

The results file contains csv (comma separated variable) data following two header lines. The main portion of the file contains data in three fields, the first is an identifier of the data type, the second and third contain the data itself. The identifier can be ifile, error, dirct or deltd which correspond to the four lists in the order given in section 2. To open a file for viewing the results program can be run with the results file as the command line argument, or the OPEN button G2.1.6 can be selected from the dialog. The OPEN button activates a standard windows dialog. When a results file is opened

the file is locked to prevent simultaneous access which could corrupt the data, especially records of files which had been removed. The results file is given, by default, the extension `SRT`.

## 2.2. Results display lists

The lists of results and information, G2.1.3, can be viewed by selecting the corresponding tab on the results dialog.

Tab G2.1.12 displays the list of files which were detected by the search process. The list has 2 columns, the first contains the file name and path of the detected file, the second displays the search item which caused that file to be detected. Two functions can be performed on selected entries in the list and these are accessed by buttons G2.1.7 and G2.1.4. The first launches windows explorer with the viewed directory set to that of the list entry. The second removes the selected file permanently from the system hard disk, and transfers the list entry to the deleted file list. More information on selecting files is given in section 2.3. The list supports multi selection and the number of files selected is displayed in the status bar G2.1.8

Tab G2.1.11 displays the list of messages that were generated by the search process. The list has 2 columns, the first contains a general statement about the event that occurred, the second provides details about the particular circumstances that caused the message to be generated.

Tab G2.1.2 displays the list of root or user directories that were searched by the process. This can be used to ensure that all user sub-directories were correctly identified. The list has 2 columns, the first contains the path of the root or user directory that was searched, the second states whether that path was a root or user. One function can be performed on selected entries in the list, accessed by button G2.1.7. This launches windows explorer with the viewed directory set to that of the list entry.

Tab G2.1.1. displays the list of files that have been removed from the system by using the delete function of the results list. The deleted file list

has 2 columns, the first contains the path and file name of the deleted file (the same as the original entry in the results list), the second displays the date on which that file was deleted.

### 2.3. Sorting the results list

The main list of results which is displayed by selecting tab G2.1.12 can be sorted in ascending order based on the contents of either column. This is done by clicking on the column header, G2.1.9 or G2.1.10, of the column that is to be used for sorting.

### 2.4. Managing search results

As stated in section 2. this program was developed to detect and remove prohibited files from user directories. The action of the remove function provided is permanent and irreversible, as such care should be taken to ensure the file being removed is not of legitimate origin and required by its owner. In the network environment regular backups were taken of all user files and so this provided a method of restoring files that were inadvertently deleted. It is advised that unknown programs detected on the system should be investigated before deletion. This will provide information about the motive for the file existing (for example there are security implications if a user has attempted to use password cracking applications) and the details of the file could also be added as a separate search item into the relevant search profile for future detection.

### 2.5. Interpretation of messages

This section gives more information about some of the common entries which appear in the messages list:

“No User Directories Were Found” - this message will occur if no instance of the user directory identifier file could be found in the root directory indicated. This may be because a directory which did not contain users was selected or because the settings for the user identifier file were incorrect.

“Failure to load directories” - this message will occur if one of the directory items to be searched does not correspond to a currently existing path. This may be because of file system changes following the creation of the search profile, or because of a network failure if the directory item corresponds to a network drive. The message will also be generated if a network connection is lost whilst analysing user sub-directories of a root. “Failure occurred listing directories” - this message indicates a failure of a network connection or other resource whilst the directories of a particular user or root are being catalogued.

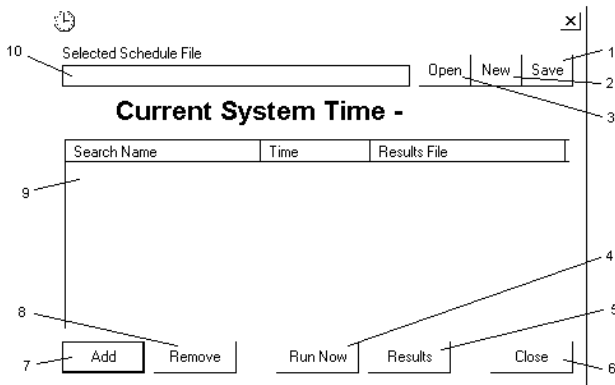
“Error performing initial character check” - because an initial character check requires the file being analysed to be opened this can occasionally cause permission or related file errors. For example some files which are currently opened by the system or a user can not always be simultaneously analysed by an initial character check. If the file name appears to be suspect further investigation may be required.

## 2.6. Forced termination of results program

As indicated by section 2.1, opening a results files causes that file to be locked. This is done by automatically saving the file with the first line “FILE IN USE”. When the results viewer is closed, or another file opened, it is again saved, but this time with the original first line. If the results program terminates abnormally either because of an internal or windows system failure the results file is not released. The results file can not be accessed by the results viewer unless this first line is edited manually, or the search is run again.

### 3. Use of schedule.exe

This program is used to automate the search process by running previously defined search profiles at a set time each day. It stores the name of the results file to create. Prompts and messages in the search program are suppressed for complete automation, and the search program terminates after operation.



Graphic 3.1. - main schedule dialog

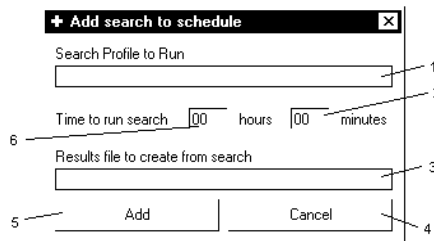
#### 3.1. Opening and saving schedules

The searches, and the time at which searches are to be run, can be stored in a csv (comma separated variable) file with three fields. This file is given, by default, the extension `scd`.

Search schedules can be Opened and Saved using buttons G3.1.3 and G3.1.1 respectively. Selecting these activate standard windows Open and Save dialog boxes. The filename of the currently selected search schedule is displayed in text box G3.1.10. A new search schedule can be started by selecting the button G3.1.2. If NEW, OPEN or CLOSE options are selected whilst a search schedule is in use, a prompt will display with the option of saving the schedule

## 3.2. Managing schedules

The list G3.1.9 displays a list of the currently scheduled searches. The list has 3 columns, the first contains the search profile to be used, the second the time at which the search will be run and the third the results file that is to be created. The three data items correspond to the command line parameters of SCRUTINY.EXE and are known collectively as a schedule item. A search can be forced to run instantaneously by first selecting its entry in the list and then the RUN NOW button, G3.1.x. It is important to note that although several searches can be scheduled to run at the same time, if these searches write to the same results file data corruption will occur. No protection against this eventuality is provided by the software and so care should be taken to ensure that all scheduled searches write to different results files. Schedule items can be managed by using the ADD and REMOVE buttons, G3.1.7 and G3.1.8 respectively. Selecting the ADD button will launch the add search to schedule dialog.



Graphic 3.2 - add new schedule item dialog

### 3.2.1. Adding schedule item

A new schedule item is created by selecting and entering data to fill the fields on dialog G3.2. The search profile to be used is displayed in text box G3.2.1, to select the search profile click on this text box with the left mouse button. This launches a standard windows open dialog. After choosing the search profile text box G3.2.1 is updated. Similarly, the results file to be created is displayed in text box G3.2.3, to select the results file click on this text box with the left mouse button. This launches a standard

windows save dialog. The time at which the search should be run is entered separately as hours and minutes in text boxes G3.2.6 and G3.2.2 respectively. The clock is based on a 24hr format and the acceptable ranges of values are 00-23 for hours and 00-59 for minutes.

### 3.2.2. Removing schedule item

Schedule items can be removed from the list G3.1.9 by selecting the entry in that list and clicking on the REMOVE button G3.1.8

### 3.3. Viewing results

The results files created by the search process are not automatically displayed when the search process finishes. These can be viewed either by opening the results file in SSRESULT.EXE or by selecting the VIEW RESULTS button, G3.1.5, with a schedule item selected in the list G3.1.9.

