



API Function Spy

(c)1992 by Mark Gamber



Overview



Warnings



Starting Spy



Stopping Spy



Function Addresses



Break



Saving the Display



Printing



Exit



Options



Registration



If this is the first time you have run this application, you should at least read the "Warning" section of this help file as it has the potential to wreak all sorts of havoc on the system and Windows!



Using Break:

If you started the program under Codeview or another compatible debugger, selecting the "**Break**" menu item calls the **DebugBreak()** function, returning control to the debugger. You may use this in conjunction with the "Proc. Addr." menu item to set debug points in Windows code.



Printing the Listbox Contents:

You may print the contents of the listbox by selecting "**Print...**" in the "**File**" menu. This menu item cannot be accessed while spying is in progress. Select the printer you want to use from the dialog box displayed and the contents of the listbox are printed.

If you only want to initialize the printer for printing, select the "**Printer Setup...**" menu item in the "**File**" menu. This menu item may be selected at any time.

See also: [Save!](#), [Stop!](#)



Function Addresses:

When running a debugger such as Codeview, it is possible and often quite handy to be able to set a breakpoint in the Windows code itself. To do so, you enter the full 32 bit address in the dialog box provided by Codeview. To get the address of the function in question, you come here. Simply enter the function name in the edit box provided and press the "**Get Address**" button or Enter. If the function is found, the address is displayed with the module it was found in. Otherwise, there is no display whatsoever.



Modules searched may include the GDI, USER, KERNEL, MMSYSTEM, SHELL and COMMDLG modules unless deselected.



Use the scrollbar to display more items in the listbox.

Version 1.2 Rev. 6/9/92



Press OK to make changes specified.



Press cancel to close the dialog box without any changes.



Select item from the listbox and press OK or double-click the listbox item to select it and close.



API Function Spy



(c)1992 by Mark Gamber
Rev. 6/9/92



Changes from Version 1.1:

Help system added.

Function Address Lookup

More functions available.

Hooks handled through DPML.

Improved function translation.

Print, save listbox contents.



More information:

Several books are available for Windows programming and the Win32 help file is available from a number of sources, including **America Online**. This program does not document the Windows API functions.



Overview:

Windows is comprised of a number of Dynamic Link Libraries, or DLLs. All Windows applications at some point or another call functions in these DLLs, passing parameters back and forth as needed. API Function Spy hooks into the DLL code itself, trapping the function calls and displaying the function and parameters. You may print the results of trapping or save the display to a disk file.

Codeview allows you to set breakpoints in Windows code if you know the address of the function to set the breakpoint in. You may look up the function and module the function is located in.

API Function Spy comes in four parts:

APISPY.EXE - The executable you run from within Windows.

APILIB.EXE - Hook code called in place of function.

APISPY.HLP - Help file.

XSTATIC.DLL - Custom control used by API Function Spy.

These files must be in the same directory, a directory in your DOS path or in the Windows directory.



Examples of Dynamic Link Libraries are COMMDLG.DLL, and MMSYSTEM.DLL. The DLL files searched by API Function Spy are USER, GDI and KERNEL.



Warning:

This program hooks directly into Windows code and alters it slightly on the fly. Because of this, it can be a very dangerous program. It is not recommended the program run under a heavy load and, should the program, system or another application mysteriously terminate or seize, close Windows and, if needed, reboot your system as soon as possible.



Windows 3.1 allows you to reboot a program rather than the entire machine. When recovering from an error caused by API Function Spy, you should reboot the machine, not just a local window!



Start Spying:

Select the **"Start"** menu item to display a list of functions available to spy upon. You may type a function in the edit box or click on a function in the list box to select it. Press **"OK"**, Enter or double-click a list box item to close the dialog box, selecting the function or **"Cancel"** to close the dialog box with no change.

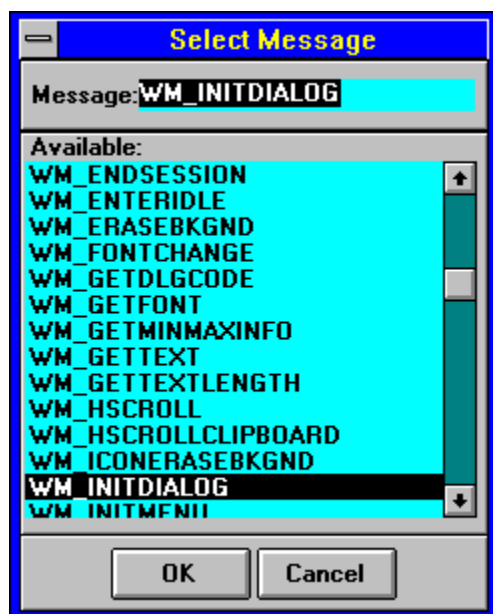
If a function is selected, the function name is displayed in the title bar of the window with "API Function Spy". **"Start!"**, **"Save"**, **"Exit"**, **"Close"** and Windows shutdown are disabled while spying is in progress. You must select **"Stop!"** to end the process and enable those items.

SendMessage is so heavily used, you must select a message to watch as well as the function itself. Selecting **SendMessage** in the function list box displays a second list box displaying the messages available. Select a message the same way as a function.

See also: Stop!, Exit!, Save!



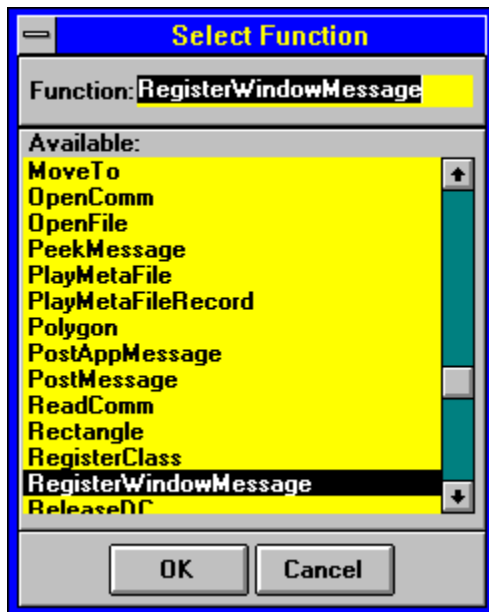
Message Listbox:



See also: [Function Listbox](#)



Function Listbox:



See also: [Message Listbox](#)



Functions chosen pass parameters according to a set standard. Functions which deviate from that convention cannot be hooked into.



As a function is typed in the edit box, the list box is searched for a match. If an unsupported function is typed, the closest match in the list box is used.



Stop Spying:

Once spying is started, you cannot close the program or Windows itself without stopping the program. In addition, the "**Save**" feature is disabled while spying. Selecting this menu item enables all the above features and deletes the function name from the title bar of the program.

See also: Start!, Exit!, Save!



Saving the List box Display:

You may save the current contents of the list box to a disk file by selecting "**Save**" in the "**File**" menu. The feature is disabled while spying is in progress. Selecting the item displays a dialog box where you may enter a filename. If the file entered already exists, it is overwritten.

See also: Stop!



Save Dialog Box:

Save Listbox Contents

File Name:
*.txt

Directories:
c:\windev\bin\windows

Save File as Type:
Text File

Drives:
c:

☐ Read Only

OK
Cancel

The dialog box contains a listbox showing the directory structure: c:\, windev, bin, windows, cdk, and dll. The 'windows' directory is selected.



Exiting the application:

The application must **not** be in spy mode to exit. If not currently active, selecting "**Exit**" from the "**File**" menu or "**Close**" from the System menu will close the application properly. You may not exit Windows while the application is running, either.

See also: [Stop!](#), [Start!](#)



Options:

Text and background display colors may be changed by their respective menu items. The font used in the listbox may also be changed by selecting a new font. Finally, "**Max. Items**" sets the maximum number of items kept in the listbox. It may be set from **50** to **500**. Heavily used functions may slow the system and updating a large listbox will slow it even more. Keep the number low if spying on an often used function.

All changes made are saved from session to session.



Max Item Dialog:

Listbox Control

Items: 100

OK Cancel



Font Dialog Box:

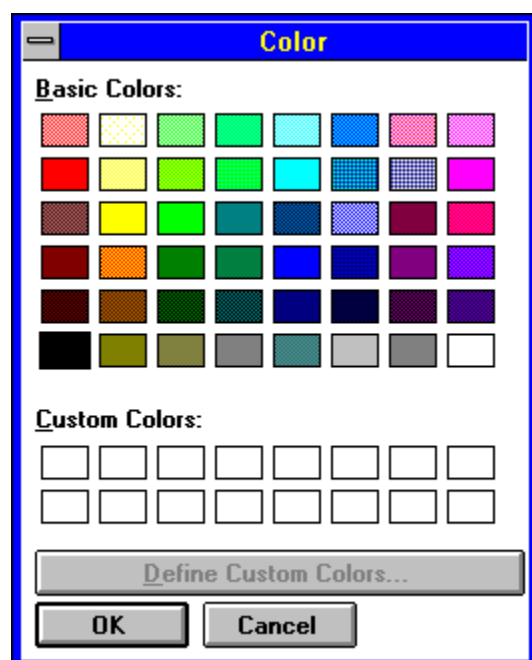
The dialog box is titled "Font" in yellow text on a blue background. It contains three main sections for font selection: "Font:", "Font Style:", and "Size:". Each section has a list box with up and down arrows. The "Font:" list includes "MS Sans Serif", "MS Serif", "Roman", "Small Fonts", and "Symbol". The "Font Style:" list includes "Regular", "Italic", "Bold", and "Bold Italic". The "Size:" list includes "8", "10", "12", "14", and "18". To the right of these lists are "OK" and "Cancel" buttons. Below the lists is a "Sample" text area containing the text "AaBbYyZz".

Font:	Font Style:	Size:
MS Sans Serif	Regular	8
MS Sans Serif	Regular	8
MS Serif	Italic	10
Roman	Bold	12
Small Fonts	Bold Italic	14
Symbol		18

Sample: AaBbYyZz



Color Dialog Box:





Registering this Program:

Sorry, but this program is not free. It took a lot of effort to get the program this far. If you find the program to be useful and intend to continue using it, the author requests a fee of **\$20** in check or money order form. In return, you will receive a registration number to make the box go away as well as notification of updates. The author may be reached at:

Mark Gamber
18 Village Dr.
Lancaster, Pa 17601

America Online E-Mail: **PCA MarkG**
Internet E-Mail: **pcamarkg@aol.com**

