

Contents

General Information About W32Dasm Demo Version 6.x Series

W32Dasm Information

HOW TO ORDER THE LATEST FULL W32DASM VERSION

Price: \$45.00 US Dollars (Email UUENCODED Delivery)

\$50.00 US Dollars (Snail Mail Delivery on 3.5 Floppy)

Prices valid until 12/31/96

Means: US cash or,

Check or International Money Order made payable to: P J Urbanik

No Credit cards or EuroChecks Accepted.

For Canadian Checks please add \$3.00 US Bank processing fee.

Send To: URSoft
44 Sachem Dr.
Glastonbury, Connecticut 06033
USA

Include: Your Name
Mailing Address
Email Address

Commands

File Menu
Text Search Menu
Goto Menu
Execute Menu
Functions Menu
HexData Menu
Reference Menu
Print Menu
Font Menu
Help Menu

Toolbar

Toolbar Commands

Procedures

Exiting
Printing

For information on how to use Help, press F1 or select Using Help from the Help menu.

W32Dasm Demo Version 6.x Series General Information:

This is the **Demo Version 6.x** Series of W32Dasm. It is **not** to be **copied** for distribution or **downloaded** as shareware.

NOTE: This demo version limits the number of operations that can be performed per session. The Text file save and print functions are also disabled. See the help contents on how to obtain the full functional version.

Comments, Questions, & Problems:

If you have any Comments (Good & Bad), Questions About or Problems with W32Dasm Ver 6.x, send them to me via Email. (urbie@msn.com)

If you encounter a problem, please provide as much detail as you can about your computer system, file you were disassembling, operation you were performing, etc. in your description of the problem.

W32Dasm Ver 6.x Series

Version 6.x includes new functionality, and fixes to known anomalies in Versions 1.x , 2.x, 3.x ,4.x and 5.x.

VERSION 6.x SERIES NEW FUNCTIONALITY:

* W32Dasm now has a Text Highlight Bar which focuses on the active disassembled text. All executable jumps and calls that are placed in the Text Highlight Bar will cause the bar to turn from CYAN to GREEN indicating that a jump or call can be made by clicking the appropriate menu button or pressing the Right Arrow key. The Text Highlight Bar may be repositioned on the screen by double clicking any line of text or by holding the SHIFT key while pressing the UP or DOWN Arrow keys. The results of all import, export, data, and text searches end up in the Text Highlight Bar.

* Current System memory Statistics are now available from the help menu.

* Menu Resource and Dialog Resource Information are now available.

* Printing can now be done for selected lines of text in addition to selected pages.

* Disassembly methods have been improved to distinguish code from string and numerical data.

Windows 32 Bit PE Format Files:

W32Dasm Version 6.x will disassemble 32 Bit Windows programs that are in the Portable Executable (PE) Format.

For valid Windows 32 Bit PE formats, an assembly code listing will be produced that has header information describing all Imported and Exported functions in the file. **Exported Functions, Imported Functions** and **String Data** references are **color** coded on the screen listing.

Search functions are available to aide in finding text, functions, code, string data, etc.

Imported Functions, Exported Functions, Menu References, Dialog References and String Data References are listed alphabetically in special List Boxes with a search feature.

See:

[Imports](#)
[Exports](#)
[Menu Reference](#)
[Dialog Reference](#)
[String Data Reference](#)

A [Goto Program Entry Point](#) command is available to quickly find the program starting point. (Starting points for windows programs are not necessarily at the start of the code listing).

A [Goto Code Location](#) command is available to quickly goto any valid code location reference.

Commands for [Execute Jump](#), [Execute Call](#), [Return From Last Jump](#), and [Return From Call](#) are also available.

Windows 16 Bit NE Format Files:

W32Dasm Version 6.x will disassemble 16 Bit Windows programs that are in the New Executable (NE) Format.

For valid Windows 16 Bit NE formats, an assembly code listing will be produced that has header information describing all Imported and Exported functions in the file. **Exported Functions, Imported Functions** and **String Data** references are **color** coded on the screen listing.

Search functions are available to aide in finding text, functions, code, string data, etc.

Imported Functions, Exported Functions and **String Data References** are listed alphabetically in special List Boxes with a search feature.

See:

[Imports](#)
[Exports](#)
[String Data Reference](#)

A [Goto Program Entry Point](#) command is available to quickly find the program starting point. (Starting points for windows programs are not necessarily at the start of the code listing).

A [Goto Code Location](#) command is available to quickly goto any valid code location reference.

Commands for [Execute Jump](#), [Execute Call](#), [Return From Last Jump](#), and [Return From Call](#) are also available.

NOTE: W32Dasm Ver 6.x will automatically find **Imported Function Names** if the import

DLL files exist either in the **Windows System Directory** or the **Current Directory** of the file being disassembled. If the Import DLL file is **not found** or does **not contain function names**, only the Imported Function **Ordinal** will be displayed.

Windows 32 Bit LE Format Files:

W32Dasm Version 6.x will disassemble 32 Bit Windows programs that are in the Linear Executable (LE) Format. (ie: Vxd files and others).

For valid Windows 32Bit LE formats, an assembly code listing will be produced that has header information describing the file and its objects. Limited Search functions are available. Commands for execution of jump, return from jump, call, and return from call instructions are also available.

Other File Formats:

W32Dasm Version 6.x can also disassemble the byte data in any any file. If the file opened for disassembly is not in the Windows 32Bit PE, 32Bit LE, or 16Bit NE format, the user will be given the option to disassemble the opened file from a user specified starting byte offset into the file.

NOTE: The user has a choice of treating the data in the file as 32 bit assembly code or 16 bit assembly code when disassembling via a checkbox on the popup dialog box that appears when raw disassembly is the option.

NOTE: W32Dasm automatically detects .COM files and sets the 16 bit option and first code location value to :0001.0100.

NOTE: Disassemblies of files (Other than .COM files disassembled as 16 bit) not in the Windows 32Bit PE, 32Bit LE, or 16Bit NE format will not have Data references.

NOTE: Disassemblies of files not in the Windows 32Bit PE, 32Bit LE, or 16Bit NE format will not have Import or Export references.

File Menu

The File menu provides commands for opening files for disassembly, saving disassembler text to an ASCII file, printing disassembler text, and exiting the application.

Open Opens an existing file for disassembly.

To enable the selection of any file extension for opening, select All Files(*.*) from the List Files of Type list box in the Open File Dialog Box.

Save Saves the disassembler text to a ASCII file. The default filename is the original filename with an .alf (Assembly List File) extension.

Exit Exits the W32Dasm application.

Text Search Menu

The Text Search menu provides commands to find and mark selected text.

Find Finds a pattern of text and marks in red on the screen display. This is useful for finding specific functions in the disassembly text. All code location begin with a semicolon (ie :004123CB (32 Bit) or :0004.345D (16 Bit)) to uniquely identify them in searches. Searches can be performed up or down from the current screen location by selecting the appropriate button in the Find Dialog Box. The text Case Match is defaulted OFF but may also be activated in the Find Dialog Box.

Next Repeats search of last find operation. The F3 key or toolbar button can also be used for Find Next operations.

Goto Menu

Goto Code Start Sets Disassembled text to the start of the Code Listing. The F7 or Toolbar Button can also be used for this function.

Goto Program Entry Point Sets Disassembled text to Program Entry Point Code. The F8 or Toolbar Button can also be used for this function.

Goto Page Sets Disassembled text to the Page Selected from the Goto Page Dialog Box. The F9 or Toolbar Button can also be used for this function.

Goto Code Location Sets Disassembled text to the Code Location Offset Selected (32 Bit) or Code Location Segment.Offset (16 Bit) from the Goto Code Location Dialog Box. The F10 or Toolbar Button can also be used for this function.

Functions Menu

The Functions Menu provides access to the Import and Export Function List Boxes.

Imports Displays the Imported Functions List Box.

Exports Displays the Exported Functions List Box.

Execute Menu

The Execute Menu provides access to the generic jump, call, and return from jump/call commands.

Execute Jump Sets listing to the location specified by the jump instruction that is in the Text Highlight Bar of the screen display.

Return From Last Jump Sets the Highlight Text Bar listing to the location of the last executed jump instruction. **NOTE: All jumps executed between a Execute Call and Return From Call are eliminated from the stack of return jumps when the Return From Call command is executed. All jump returns prior to a Execute Call command remain valid.**

Execute Call Sets the text listing to the location specified by the call instruction that is in the Text Highlight Bar line of the screen display.

Return From Call Returns the Highlight Text Bar listing to the location of the most recently executed call (See Execute Call).

HexData Menu

The HexData menu provides access to the Code Object and Data Object/Segments Hex Display.

Hex Display of Code Data Displays the current screen code as Hex data.

Hex Display of Data Object/Segments Displays the Data Object/Segments in hexadecimal form.

Reference Menu

The Reference menu provides access to the Menu, Dialog and String Data Reference List/Search Boxes.

Menu Reference Displays the Menu Reference List Box.

Dialog Reference Displays the Dialog Reference List Box.

String Data Reference Displays the String Data Reference List Box.

Print Menu

Print Preview View a sample printout of the current disassembler text.

Print Sends the disassembler text to a printer. User can select specific pages, selected lines, or print the whole listing.

NOTE: To select a specific line of text to print, use the mouse to left click on the far left hand margin of the text . A red dot will appear to the left of the text indicating your selection.

To select a range of text,, after selecting a line as explained above, hold the shift key while left clicking on the far left margin of the other line of the range you wish to print. A series of red dots in the left hand margin will indicate your selection.

Print Setup Set printer characteristics, ie Landscape, Portrait, etc.

Font Menu

Select Font Displays Font Select Dialog from which the user can select fonts.

Save Default Font Sets the currently selected font to the default startup font.

Help Menu

The Help menu provides access to the help system and the about dialog.

Memory Statistics Displays Current Memory Statistics.

Contents Help topic contents.

Context Help Context sensitive help.

About About W32Dasm.

Exiting

To exit W32Dasm, choose File|Exit from the menu. You will be prompted to save any unsaved disassembly text before exiting.

Printing

There are three commands on the File menu which support printing of disassembled text from W32Dasm. File|Print Setup is used to select and configure a printer device. File|Print Preview displays a special preview window which shows how the text will appear when printed. File|Print allows for printing all, selected lines, or selected pages of the current displayed disassembler text.

File Exit Command

The File|Exit command exits W32Dasm. If you've modified documents without saving, you'll be prompted to save before exiting.

File Open Command

The File|Open command displays the Open a File dialog box so you can select a file to disassemble. If the file selected is not in the Windows 32 bit PE format, 32 bit LE format, or Windows 16 bit NE format, an option to interpret and disassemble the file as raw 32 bit assembly code or raw 16 bit assembly code will be enabled. Use the List Files of Type list box to choose the file extensions that will displayed in the file selection box. All Files(*.*) can be chosen to list all files in the selected Directory.

NOTE: The last selected Directory and FileType selected will be the default the next time the File Open Dialog is selected.

Print Print Command

The Print|Print command prints all, selected pages, or selected lines of the disassembler text. Use File|Print Preview to see how the text will be laid out on printer pages. Use File|Print Setup to select a printer, and to set printer options.

NOTE: To select a specific line of text to print, use the mouse to left click on the far left hand margin of the text . A red dot will appear to the left of the text indicating your selection.

To select a range of text,, after selecting a line as explained above, hold the shift key while left clicking on the far left margin of the other line of the range you wish to print. A series of red dots in the left hand margin will indicate your selection.

Print Print Preview Command

Print|Print Preview opens a special window that shows how the disassembled text will appear when printed. The preview window shows one or two pages of the active document as they would be laid out on printer pages. If the Printer is set up for Landscape printing, only one page is available in the print preview window. Controls on the window allow you to page through the pages of the text.

Print Print Setup Command

The Print|Printer Setup command displays the Printer Setup dialog box which allows you to select and configure the printer to be used to print documents in the application.

File Save Command

The File|Save command saves the disassembler text to an ASCII text file. The default name of the saved file will be the original name/path of the disassembled file with an .alf (Assembler List File) extension. This file can be used in a word processor such as MS Word for further editing, searching and formatting. The default filename/path can be overridden by the user.

Text Search Find Command

The Search|Find command searches the disassembled text for a pattern. The command displays the Find dialog which controls the search process. Options in the dialog determine whether the case of characters is significant, and whether the search should be conducted forwards or backwards through the document. As each match is found, it is highlighted in red in on the screen.

NOTE: Text searches on large files may take a long time -- be patient.

Text Search Next Command

The Search|Find Next command repeats the last Find operation.

Goto Goto Code Start Command

The Goto|Goto Code Start Command sets the disassembled text to the start of the code listing. This is not necessarily the start point for the execution of the subject program. (See Goto Program Entry Point)

Goto Goto Program Entry Point Command

The Goto|Goto Program Entry Point Command sets the disassembled text to the program entry point code. This is the start point for the execution of the subject program. When using a debugger program, a breakpoint may be set here to trap beginning of the program execution.

If the code location (ie. :XXXXXXXX or :XXXX.XXXX) of the program entry point is set to the Highlight Text Bar of the display, the status bar at the bottom of the screen will give information as to the hex offset in the program file where this code exists. Patching the code byte of this location with a hex editor to a CC value will place an INT 3 instruction which will cause the program to break automatically when used with a debugger. Of course the original value of the patched byte would then have to be reinstated to continue the debug.

NOTE: Program Entry Points are only valid for 32 bit PE and 16 bit NE files. This command is disabled if no valid PEP exists.

Goto Goto Page Command

The Search|Goto Page Command sets the disassembled text to the page selected from the Goto Page Dialog. The Current Page is displayed when the Dialog is initialized. Page numbers entered that are greater than the total pages available will goto to the last page.

Goto Goto Code Location Command

The Goto|Goto Code Location Command sets the disassembled text to the Code Location Offset (32 Bit) or Code Location Segment.Offset (16 Bit) selected from the Goto Code Location Dialog. The Last Code Location goto point that was entered is displayed when the Dialog is initialized. The initialization value for the first time the Dialog Box is opened after a file is disassembled is the lowest valid Code Location goto Value. Code goto points entered that are greater than or less than the lowest and highest valid values are automatically clamped. Valid in-range values that are entered that are not valid Code Locations in the listing are automatically set to the nearest lowest valid value.

Functions Imports

The Functions|Imports displays a List Box with all the disassembled programs identified Imported Functions listed alphabetically.

Imported Functions are functions that are required to run a program but reside in files other than the subject program file. Imported Functions in the Disassembled Listing, are references to Calls to the function. There can be more than, and usually is, one reference. Imported Functions are usually the result of calls made to Dynamic Link Library files (DLLs).

If there are no Imported Functions identified, the command is disabled. To search for an Imported Function in the disassembled text, Double Click the Left Mouse Button on the desired function in the List Box.

NOTE: If a Imported Reference is not found, it is most likely due to the fact that the disassembler could not properly decode the location of the import reference due to a mixture of data and code in the object being decoded.

NOTE: Files that are not in the Windows NE or PE format will not have Function Import Data.

Functions Exports

The Functions|Exports displays a List Box with all the disassembled programs identified. Exported Functions listed alphabetically.

Exported Functions are functions that are available to other programs. Exported Functions in the Disassembled Code Listing show the actual function code. There should be only one reference in the Code portion of the Disassembler Listing per Exported Function. DLL files usually have many exported functions. Program {exe} files usually have few if any.

If there are no Exported Functions identified, the Command is disabled. To search for an Exported Function in the disassembled text, Double Click the Left Mouse Button on the desired function in the List Box.

NOTE: If a Exported Reference is not found, it is most likely due to the fact that the disassembler could not properly decode the location of the export reference due to a mixture of data and code in the object being decoded.

NOTE: Files that are not in the Windows NE or PE format will not have Export Data.

Execute Execute Jump

The Execute|Execute Jump command sets the screen listing to the location specified by the jump instruction that is in the Highlight Text Bar of the screen listing. All direct jumps to the code object are executed. The command is automatically enabled if a valid jump instruction is in the Highlight Text Bar position. In the case that the jump location is invalid, a message will be posted after a unsuccessful attempt is made. The HOT KEY for this command is the RIGHT Arrow key

Execute Return From Last Jump

The Execute|Return From Last Jump command sets the screen listing to the location of the last executed Jump. The Hot Key for this function is the CTRL- LEFT Arrow Cursor Key. This command is only enabled if a valid jump instruction was executed.

Execute Execute Call

The Execute|Execute Call command sets the screen listing to the location specified by the call instruction that is in the Highlight Text Bar of the screen listing. All direct calls to the code object are executed. The command is automatically enabled if a valid call instruction is in the Highlight Text Bar position. In the case that the call location is invalid, a message will be posted after a unsuccessful attempt is made. After a call command is executed, the Execute|Return command can be used to return to the original call location. Call commands can be stacked, and Return commands will set locations in the order of the calls. The HOT KEY for this command is the RIGHT Arrow key

Execute Return From Call

The Execute|Return From Call command sets the screen listing to the location of the last executed Execute|Execute Call command. Call commands are stacked, and Return commands will set locations in the reverse order of the calls. The command is automatically enabled when valid call commands are executed. The HOT KEY for this command is the LEFT Arrow key.

Data String Data References

The Data|String Data References displays a List Box with all the disassembled programs identified string data references listed alphabetically.

If there is **no** String Data identified, the Command is **disabled**. To **search** for a string data item reference in the disassembled text, **Double Click** the Left Mouse Button on the desired string data text in the List Box.

NOTE: Long String Data References are **abbreviated** in the String Data List Box but are **fully displayed** as wrapped text in the disassembler listing.

NOTE: Only Files that are in the Windows **NE** format, **PE** format, or **.COM** files disassembled as 16 bit, are queried for String Data. This command is **disabled** for all other file types.

Menu References

The Menu References displays a List Box with all the disassembled programs identified Menu references listed alphabetically.

Dialog References

The Dialog References displays a List Box with all the disassembled programs identified Dialog references listed alphabetically.

Data Hex Display of Data Object Command

The Data|Hex Display of Data Object displays a List Box with all the Data Object/Segment data in hexadecimal format. The data is grouped into 1024 byte pages which are selectable from the list box. The number of pages is dependent on the size of the data Object/Segment. This command is enabled after a valid disassembly is executed.

NOTE: If there is more than one Page of data in the Data Object/Segment, the Page Select buttons are automatically enabled.

NOTE: For NE files that have more than one Data Segment, Segment Select buttons are automatically enabled.

Code Hex Display of Code Data Command

The Data|Hex Display of Code Data displays a List Box with the current page code data in hexadecimal format. The starting location is the same as the code location specified at the top line of the screen. This command is disabled if a valid code location is not available on the top line of the screen.

Window Help table of contents

The Help|Contents displays the help contents page.

Memory Statistics

The Memory Statistics Displays the current state of the RAM and Disk memory.

Font Select Font Command

The Font|Select Font Command displays a font selection Dialog Box from which the user may select a text font. W32Dasm uses the **Courier New, Regular** Style, Size **8**, font as a starting default. This default can be changed using the Save Default Font. command.

Font Save Default Font Command

The Font|Save Default Font Command sets the current selected font (See [Select Font](#)) as the program default font. W32Dasm uses the **Courier New, Regular** Style, Size **8**, font as a starting default.

Window Context Sensitive Help























The Help|Context Help creates a cursor that calls up help when clicked over any toolbar or menu item. The context help cursor is automatically deleted upon return from help or it can be canceled by using the right mouse button or pressing the keyboard escape key {Esc}.

Window About W32Dasm

Displays dialog box with information about the W32Dasm Application.

The Toolbar

The Toolbar is a row of buttons at the top of the main window which represent application commands. Clicking one of the buttons is a quick alternative to choosing a command from the menu. Buttons on the toolbar activate and deactivate according to the state of the application.

Button	Action	Menu Equivalent
	Open File to Disassemble.	File <u>O</u> pen
	Save Disassembly to a Text File.	File <u>S</u> ave
	Find Text. Text Search <u>F</u> ind	
	Find Next. Text Search <u>N</u> ext	
	Goto Code Starting Location of Code.	Goto <u>G</u> oto Code Start Point
	Goto Program Entry Point in the Code.	Goto <u>G</u> oto Program Entry Point
	Select and Goto Specified Page .	Goto <u>G</u> oto Page
	Select and Goto Specified Location .	Goto <u>G</u> oto Code Location
	Execute Jump Instruction.	Execute <u>E</u> xecute Jump
	Return From Last Jump.	Execute <u>R</u> eturn From Last Jump
	Execute Call Instruction.	Execute <u>E</u> xecute Call
	Return From Last Call.	Execute <u>R</u> eturn From Last Call
	List Import Functions.	Functions <u>I</u> mports
	List Export Functions.	Functions <u>E</u> xports
	Display of Data Object in Hex Format.	HexData <u>H</u> ex Display of Data Object
	Display of Code Data in Hex Format.	HexData <u>H</u> ex Display of Code Data
	List and Search Menu References.	References <u>M</u> enu References
	List and Search Dialog References.	References <u>D</u> ialog References
	List and Search String Data References.	References <u>S</u> tring Data References
	Print the Disassembler Text.	Print <u>P</u> rint
	Print Preview the Disassembler Text.	Print <u>P</u> rint Preview
	Context Sensitive Help	Help <u>C</u> ontext Help

