DWARF Browser

by

Software Verify

Software Verify
Troubleshoot your software

DWARF Browser

DWARF Symbols inspector

by Software Verify Limited

Welcome to the DWARF Browser software tool. DWARF Browser is a software tool that allows you to inspect DWARF debugging information stored in executable files.

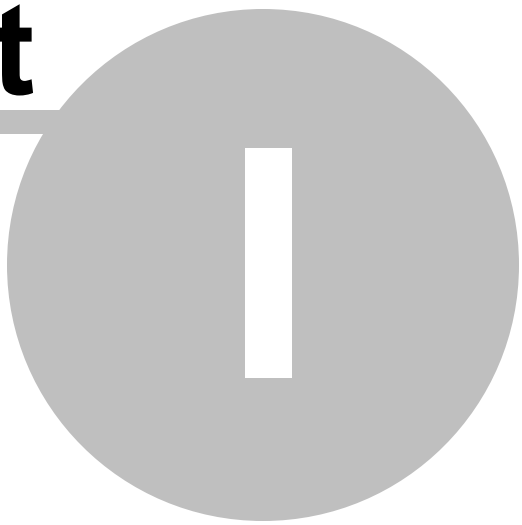
We hope you will find this document useful.

DWARF Browser Help

Printed: December 2023 in United Kingdom.

Table of Contents

Part



1 How to get DWARF Browser

DWARF Browser is free for commercial use. DWARF Browser can be downloaded for Software Verify's website at https://www.softwareverify.com/product/dwarf-browser/.

This help manual is available in Compiled HTML Help (Windows Help files), PDF, and online.

Windows Help	https://www.softwareverify.com/documentation/chm/dwarfBrowser.chm
PDF	https://www.softwareverify.com/documentation/pdfs/dwarfBrowser.pdf
Online	https://www.softwareverify.com/documentation/html/dwarfBrowser/index.html

Whilst DWARF Browser is free for commercial use, DWARF Browser is copyrighted software and is not in the public domain.

You are free to use the software at your own risk.

You are not allowed to distribute the software in any form, or to sell the software, or to host the software on a website.

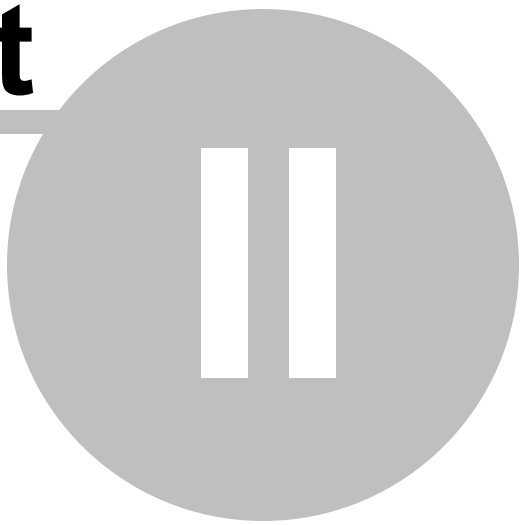
Contact Software Verify at:

Software Verify Limited
Suffolk Business Park
Eldo House
Kempson Way
Bury Saint Edmunds
IP32 7AR
United Kingdom

email	sales@softwareverify.com
web	https://www.softwareverify.com
blog	https://www.softwareverify.com/blog
twitter	http://twitter.com/softwareverify

Visit our blog to read our articles on debugging techniques and tools.
Follow us on twitter to keep track of the latest software tools and updates.

Part



2 What does DWARF Browser do?

DWARF Browser allows you to inspect the DWARF symbols in an executable file.

You can sort the data, filter the data by name or by type of data.

You can also query the data by address which can be useful for identifying what function is at a given address if all you have is a crash address and nothing else.

Query by address is supported three ways:
- Query by absolute address.
- Query by address offset from a DLL load address.
- Query by address offset from a symbol.
- Query using Windows event log XML crash data.

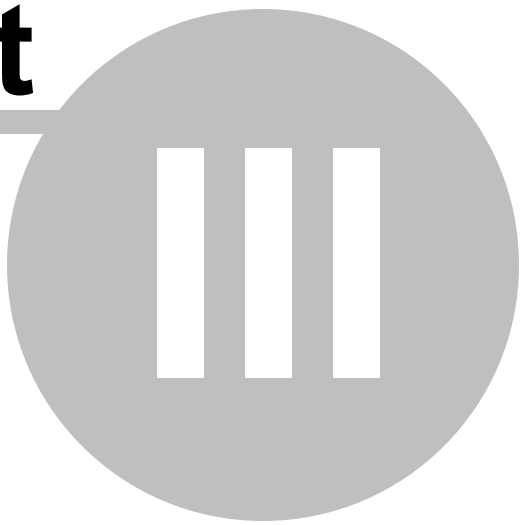
32 bit and 64 bit

DWARF data embedded in 32 bit executables and 64 bit executables are supported.

History

DWARF Browser has been an internal tool at Software Verify for many years. We recently decided to make it a bit more user friendly and to make it available for public use.

Part



3 What is a module?

A module is a contained block of executable code and data. For example, a DLL or EXE.

Some software vendors name their DLLs with different file extensions, for example .BPL, .ARX.

When you call LoadLibrary to load a module, you are returned a HMODULE, which is an opaque handle to a module. The HMODULE is most often the same as the module load address, but not always.
The lower few bits of the HMODULE can get OR'd with some flags to create a HMODULE value that is not the same as the module load address.

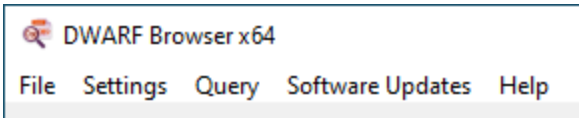
You can get the load address of a module from it's HMODULE by masking out the lower 16 bits of the HMODULE value then casting to a DWORD_PTR.

In this documentation when you read EXE or DLL or module, we are effectively referring to the same thing. It's easier to read and write "DLLs" rather than "DLLs or EXE".

Part IV

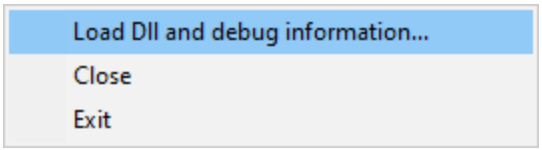
4 Menu

The main menu contains five menus, File, Settings, Query, Software Updates and Help.



4.1 File

The File menu controls loading of DLLs and debug information, clearing the display and exiting the program.



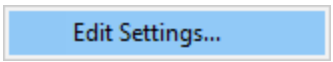
File menu > **Load Dll and debug information...** > loads a DLL and the debug information and displays it.

File menu > **Close** > clear all results, unloads the DLL and debug information.

File menu > **Exit** > closes DWARF Browser.

4.2 Settings

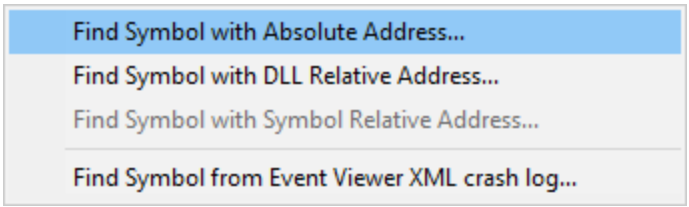
The Settings menu controls editing of the settings controlling Exception Tracer



Settings menu > **Edit Settings...** > displays the settings dialog.

4.3 Query

The Query menu controls searching for symbols.



Query menu > **Find Symbol with Absolute Address...** > use this option to turn an absolute address in a process into a symbol, filename and line number.

See Decoding an absolute crash address for more details.

Query menu > **Find Symbol with DLL Relative Address...** > use this option to turn a relative address inside a DLL into a symbol, filename and line number.

See Decoding a relative crash address for more details.

Query menu > **Find Symbol with Symbol Relative Address...** > use this option to turn an address that is relative to a symbol inside a DLL into a symbol, filename and line number.

See Decoding a symbol relative crash address for more details.

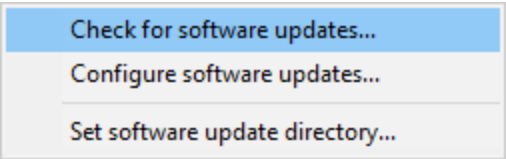
Query menu > **Find Symbol from Event Viewer XML crash log...** > use this option to turn an XML crash log from the Microsoft Event Viewer to a symbol inside a DLL into a symbol, filename and line number.

See Decoding an Event Viewer XML crash log for more details.

4.4 Software Updates

The Software Updates menu controls how often software updates are downloaded.

If you've been notified of a new software release to DWARF Browser or just want to see if there's a new version, this feature makes it easy to update.

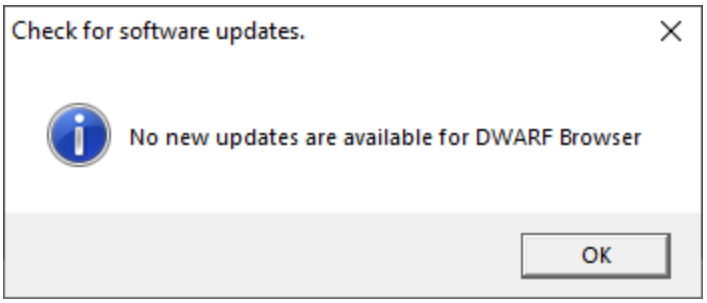


Software Updates menu > **Check for software updates** > checks for updates and shows the software update dialog if any exist

An internet connection is needed to be able to make contact with our servers.

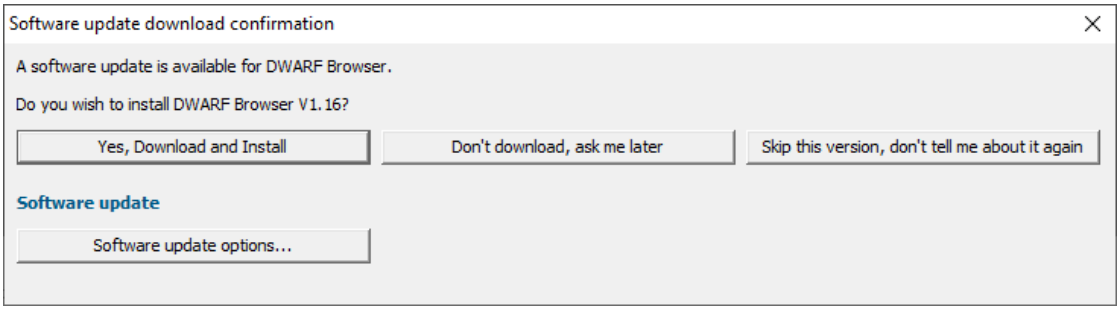
Before updating the software, close the help manual, and end any active session by closing target programs.

If no updates are available, you'll just see this message:

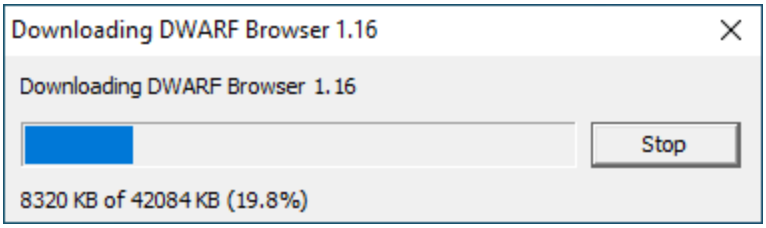


Software Update dialog

If a software update is available for DWARF Browser you'll see the software update dialog.



- **Download and install** > downloads the update, showing progress



  Once the update has downloaded, DWARF Browser will close, run the installer, and restart.

  You can stop the download at any time, if necessary.

- **Don't download...** > Doesn't download, but you'll be prompted for it again next time you start DWARF Browser
- **Skip this version...** > Doesn't download the update and doesn't bother you again until there's an even newer update
- **Software update options...** > edit the software update schedule

Problems downloading or installing?

If for whatever reason, automatic download and installation fails to complete:

- Download the latest installer manually from the software verify website.

Make some checks for possible scenarios where files may be locked by DWARF Browser as follows:

- Ensure DWARF Browser and its help manual is also closed
- Ensure any error dialogs from the previous installation are closed

You should now be ready to run the new version.

Software update schedule

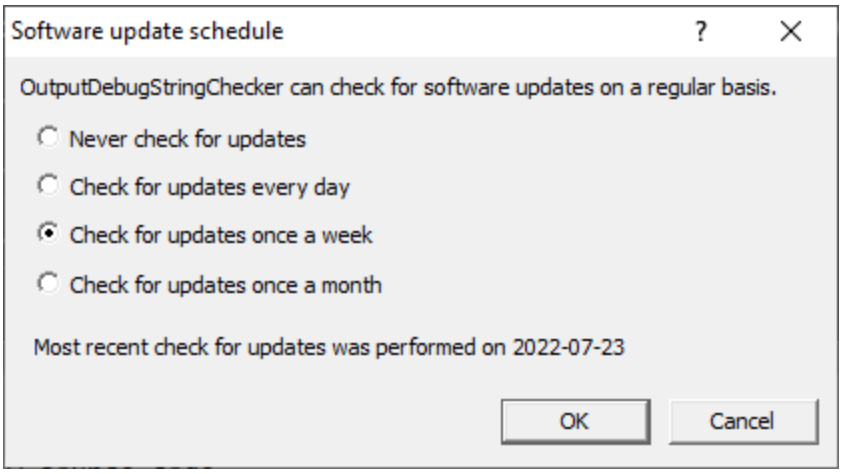
DWARF Browser can automatically check to see if a new version of DWARF Browser is available for downloading.

Software Updates menu > **Configure software updates** > shows the software update schedule dialog

The update options are:

- never check for updates
- check daily (the default)
- check weekly
- check monthly

The most recent check for updates is shown at the bottom.

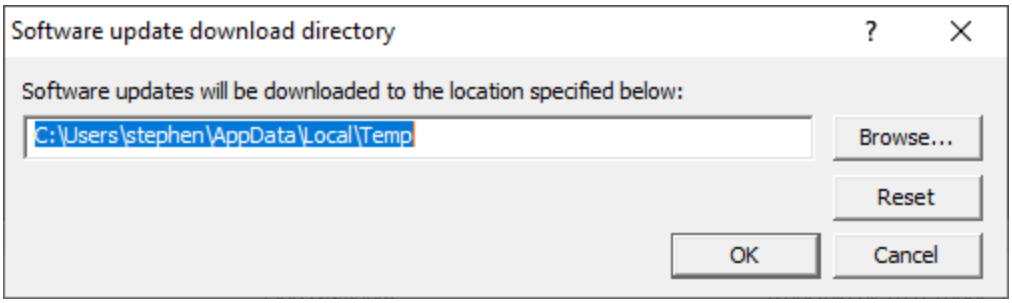


Software update directory

It's important to be able to specify where software updates are downloaded to because of potential security risks that may arise from allowing the `TMP` directory to be executable. For example, to counteract security threats it's possible that account ownership permissions or antivirus software blocks program execution directly from the `TMP` directory.

The `TMP` directory is the default location but if for whatever reason you're not comfortable with that, you can specify your preferred download directory. This allows you to set permissions for `TMP` to deny execute privileges if you wish.

Software Updates menu › **Set software update directory** › shows the Software update download directory dialog



An invalid directory will show the path in red and will not be accepted until a valid folder is entered.

Example reasons for invalid directories include:

- the directory doesn't exist
- the directory doesn't have write privilege (update can't be downloaded)
- the directory doesn't have execute privilege (downloaded update can't be run)

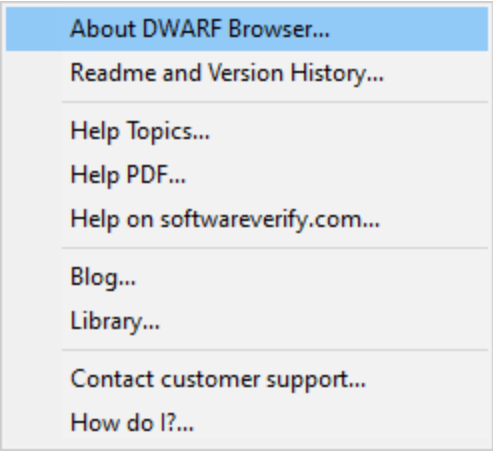
When modifying the download directory, you should ensure the directory will continue to be valid. Updates may no longer occur if the download location is later invalidated.

- **Reset** › reverts the download location to the user's `TMP` directory

  The default location is `c:\users\[username]\AppData\Local\Temp`

4.5 Help

The Help menu controls displaying this help document and displaying information about DWARF Browser.



Help menu > **About DWARF Browser...** > displays information about DWARF Browser.

Help menu > **Readme and Version History...** > displays the readme and version history.

Help menu > **Help Topics...** > displays this help file.

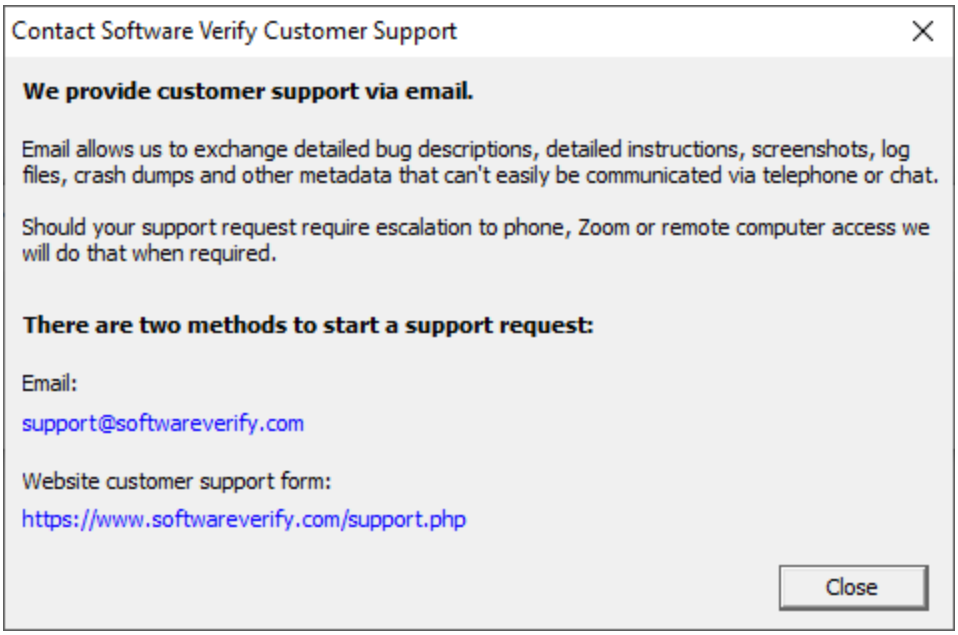
Help menu > **Help PDF...** > displays this help file in PDF format.

Help menu > **Help on softwareverify.com...** > display the Software Verify documentation web page where you can view online documentation or download compiled HTML Help and PDF help documents.

Help menu > **Blog...** > display the Software Verify blog.

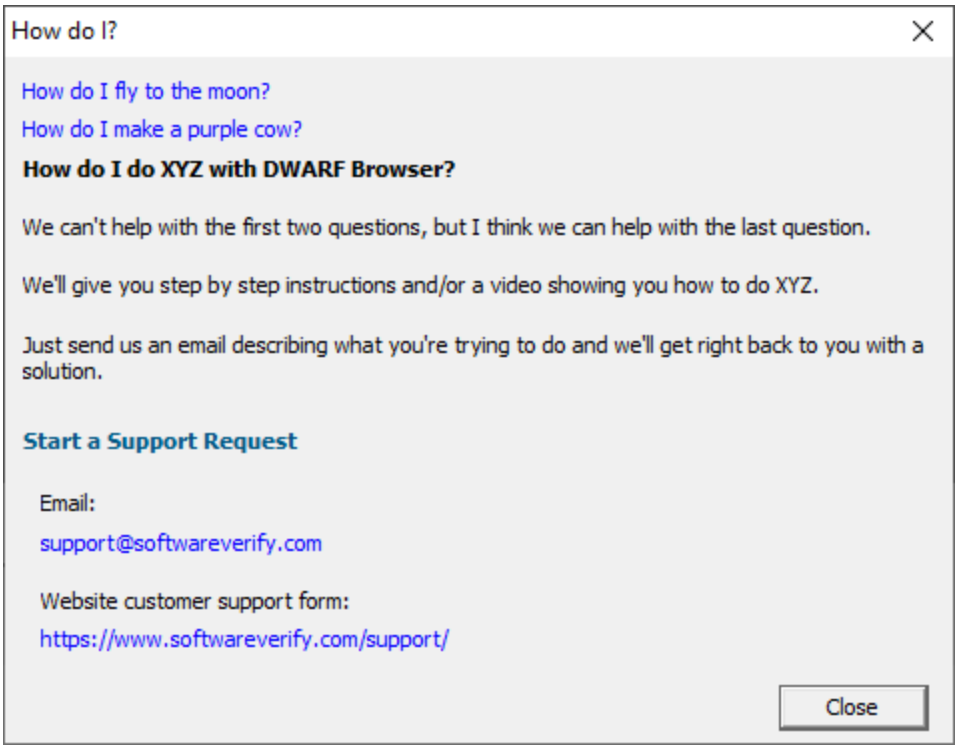
Help menu > **Library...** > display the Software Verify library - our best blog articles grouped by related topics.

Help menu > **Contact customer support...** > displays the options for contacting customer support.



Click a link to contact customer support.

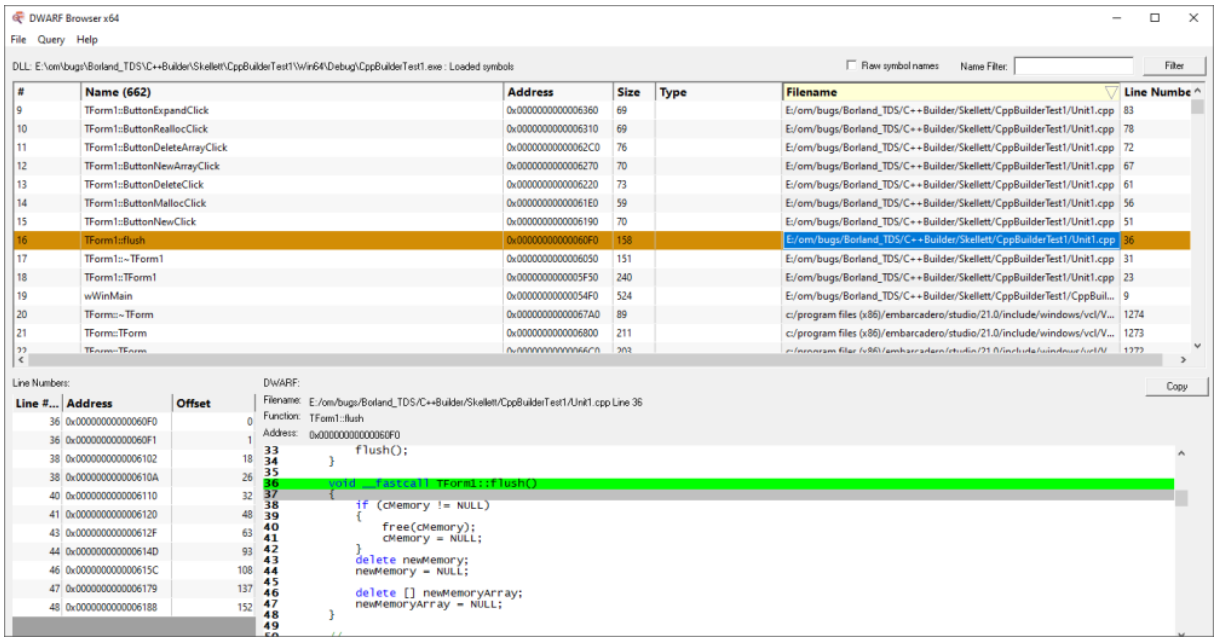
Help menu > **How do I?...** > displays the options for asking us how to do a particular task.



Part V

5 The user interface

The DWARF Browser user interface is shown below.



The user interface consists of a main grid showing all main datatypes and functions in the debug help.

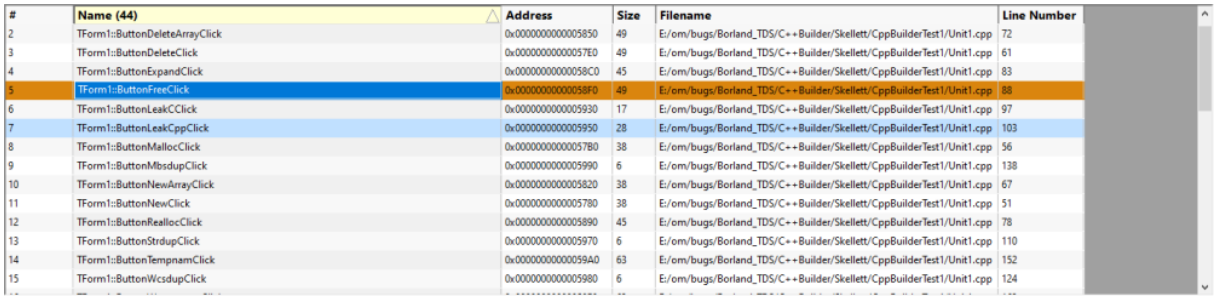
Below is a display for line numbers and a source code display for viewing the source code of any function or variable that is selected.

Selecting any item in the grid populates the lower grid and source code display as appropriate.

Querying any value will select the nearest item in the main grid and populate the other displays as appropriate.

Some basic filtering functionality is also provided.

DWARF Information

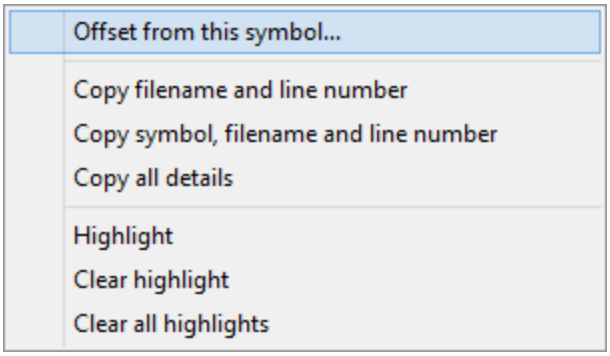


The DWARF information shows you the symbol name, symbol address, symbol size, and the filename and line number for the symbol.

You can sort the data by clicking no the column header and clicking again to reverse the direction of the sort.

If you select any item in the grid the lower grids and source code display are populated with data as appropriate.

If you right click any item a context is displayed which will allow you to perform a symbol relative query.



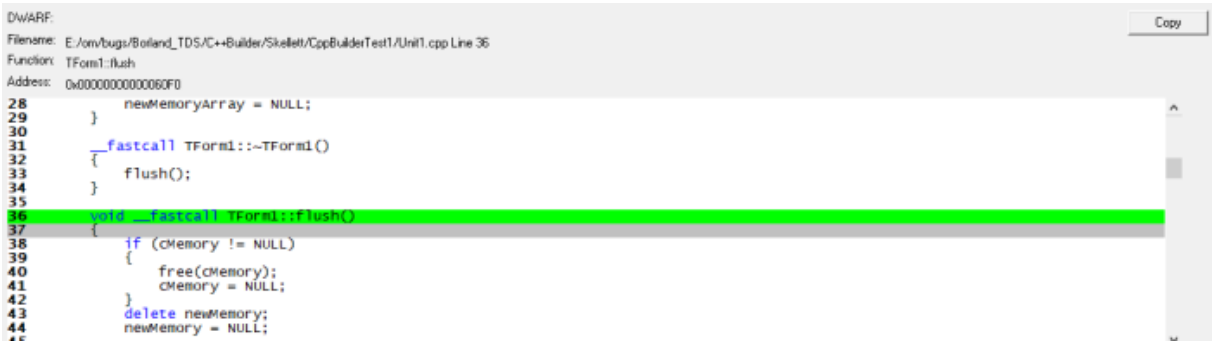
Line Numbers

Line Numbers:

Line #...	Address	Offset
42	0x00052E30	0
43	0x00052E42	1
44	0x00052E4B	2
45	0x00052E58	3
46	0x00052E76	4

The line numbers section lists each line number, the address of that line and the offset of that line from the start of the owning function. Note that offsets can be negative as well as positive depending on how the compiler did it's work.

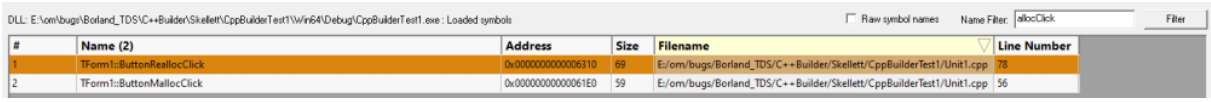
Source Code



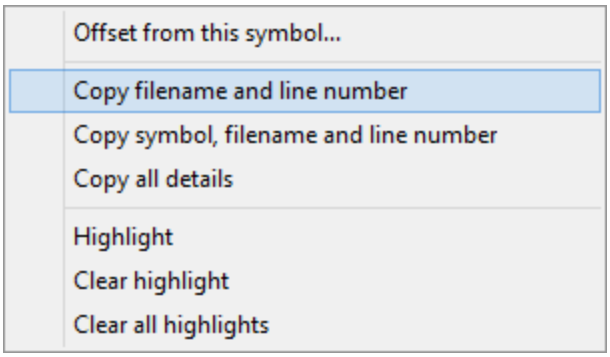
The source code section displays the source code, highlights the selected line and displays information relating to filename, line number, function and address.

Filters

Filtering by symbol name allows you to easily find a particular symbol. This is very useful when wanting to decode a crash address that has been provided as relative to a symbol (symbol + offset).



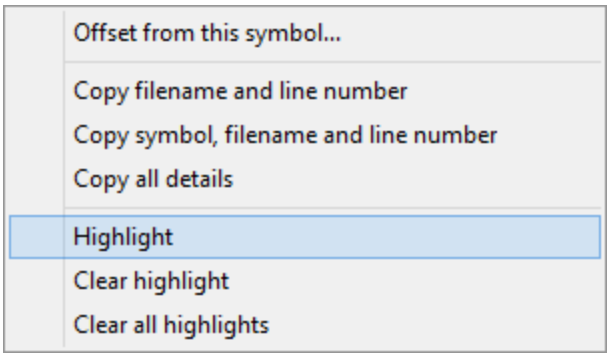
Clipboard



Options on the context menu to allow you to copy the following information to the clipboard:

- Filename and line number. `ThSort.pas 80`
- Symbol, filename and line number. `Thsort.TThreadSortForm.FormCreate ThSort.pas 80`
- All symbol details. `4 Thsort.TThreadSortForm.FormCreate Unknown14 (fast` **`this`**`) 0x002F6B40 16 System.Types ThSort.pas 80`

Highlighting



Options on the context menu allow you to highlight multiple symbols, and to remove highlights.

Highlighting can useful when you want to easily mark a symbol for future reference. Here's an example image showing some symbols that have been highlighted.

#	Name (44)	Address	Size	Filename	Line Number
4	TForm1::ButtonExpandClick	0x00000000000058C0	45	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	83
5	TForm1::ButtonFreeClick	0x00000000000058F0	49	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	88
6	TForm1::ButtonLeakCClick	0x0000000000005930	17	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	97
7	TForm1::ButtonLeakCppClick	0x0000000000005950	28	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	103
8	TForm1::ButtonMallocClick	0x00000000000057B0	38	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	56
9	TForm1::ButtonMbsdupClick	0x0000000000005990	6	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	138
10	TForm1::ButtonNewArrayClick	0x0000000000005820	38	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	67
11	TForm1::ButtonNewClick	0x0000000000005780	38	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	51
12	TForm1::ButtonReallocClick	0x0000000000005890	45	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	78
13	TForm1::ButtonStrdupClick	0x0000000000005970	6	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	110
14	TForm1::ButtonTempnamClick	0x00000000000059A0	63	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	152
15	TForm1::ButtonWcsdupClick	0x0000000000005980	6	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	124
16	TForm1::ButtonWtempnamClick	0x00000000000059E0	63	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	163
17	TForm1::TForm1	0x0000000000005580	203	E:/om/bugs/Borland_TDS/C++Builder/Skellett/CppBuilderTest1/Unit1.cpp	23

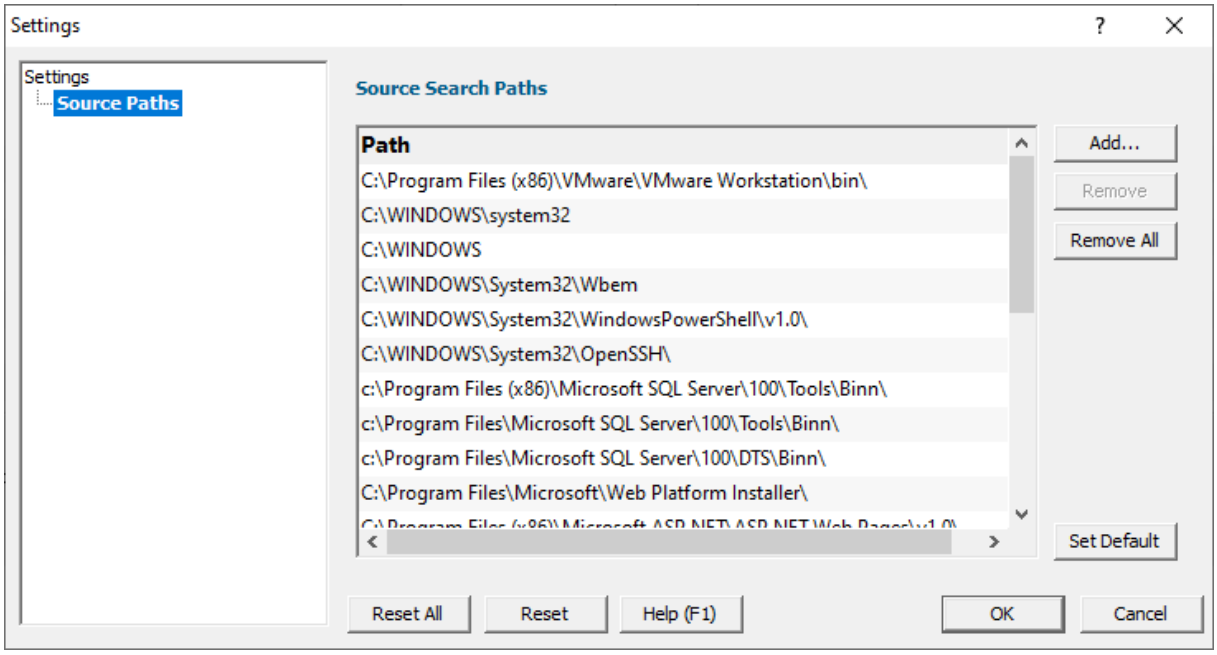
Part VI

6 Settings Dialog

6.1 Source Paths

The Source Paths settings allow you to specify where Dwarf Browser looks for source code files.

The source code paths are used when a filename is incomplete - a filename without a path, a filename with a partial path, or a filename that isn't valid on this machine.



Manually adding path type directories

The Path list shows all the paths that will be searched for source code files.

You can modify the list of files for each path type in the following ways:

- **Add** › appends a row to the directory list › enter the directory path

Edit a directory path by double clicking the entry. The usual controls apply for removing list items:

- **Remove** › removes selected items from the list
- **Remove All** › clears the list
- **Set Default** › adds all valid directories found in the PATH environment variable

Alternatively, press Del to delete selected items, and Ctrl + A to select all items in the list first.

Reset - Resets **all** global settings, not just those on the current page. This includes removing any symbol servers added.

Part VII

7 How to use DWARF Browser

Load DWARF information

To load Debug information you need to have the executable file containing debug information.

Use the **File > Load Dll and debug information...** option to load the appropriate DLL and it's debug information.

The grid displays various attributes of each debugging item. You can sort the grid by clicking the appropriate column header. Click the same header to reverse the sort order.

Select a symbol to see information about the parameters, locals, line numbers and source code.

Filtering

If you wish to only view one type of debugging data, select that datatype using the **Tags** combo.

You can also filter by name by typing the name into the **Name Filter** box and clicking the **Filter** button to perform the filtering.

Viewing function data

As each item in the list is selected the Parameters and Locals grid are populated, the Line Numbers are updated and the source code display updates to show the source code for the function. All lines in the function that contain executable code (as indicated by the debugging information) are coloured grey. The current line for the function is coloured bright green.

Querying data

You can query data by using the two Query fields below the main grid.

Relative query

Type the relative address (also know as address offset) into the Query by Offset field, then click Query. The symbol information is displayed.

The field accepts decimal or hexadecimcal values. Hex values must be prefixed with 0x.

Absolute query

Type the absolute address into the Query by Address field, type the absolute DLL load address into the Alternate Load Address field, then click Query. The symbol information is displayed.

The fields accept decimal or hexadecimcal values. Hex values must be prefixed with 0x.

7.1 Decoding an absolute crash address

Scenario:

A customer has supplied you with a crash report containing a callstack with addresses. The callstack also indicates which module relates to which address.
The customer has also supplied you with a list of module load addresses.

Example Data:

```
Exception code: C0000005 ACCESS_VIOLATION
Fault address:  0x005f5eec (base 0x00400000) C:\Program Files (x86)\Software Verification\
Exception Parameters:
   0: 0x00000000 [Read Error]
   1: 0x035f0034 [Address]

Registers:
   EAX:035F0034
   EBX:00000000
   ECX:FFFDD000
   EDX:00002370
   ESI:006F7D58
   EDI:035F0034
   CS:EIP:0023:005F5EEC
   SS:ESP:002B:0018FE14  EBP:0018FE3C
   DS:002B  ES:002B  FS:0053  GS:002B
   Flags:00010202

StackTrace

C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Windows\syswow64\msvcrt.dll : 0x75D70000 : 0x75D7C3E4
C:\Windows\syswow64\msvcrt.dll : 0x75D70000 : 0x75D836B6
C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Windows\syswow64\kernel32.dll : 0x754D0000 : 0x754E3365
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F6D
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F40
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F40
```

This is data from a real crash a few years ago, from C++ Memory Validator 5.80.

Question:
How do you decode these absolute addresses?

Answer:
In the above data we can see a callstack containing entries for ntdll.dll, msvcrt.dll, and memoryValidator.exe.

All the modules are Microsoft DLLs except for the EXE, which is part of C++ Memory Validator, one of our tools.

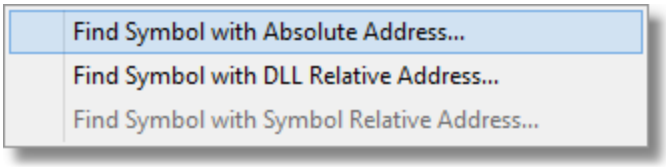
To decode these values, we load memoryValidator.exe into DWARF Browser.exe, then for each symbol we take the following actions.

For our purposes here, we're going to show how to convert one symbol. We're going to use the first symbol from memoryValidator.exe in the example data above.

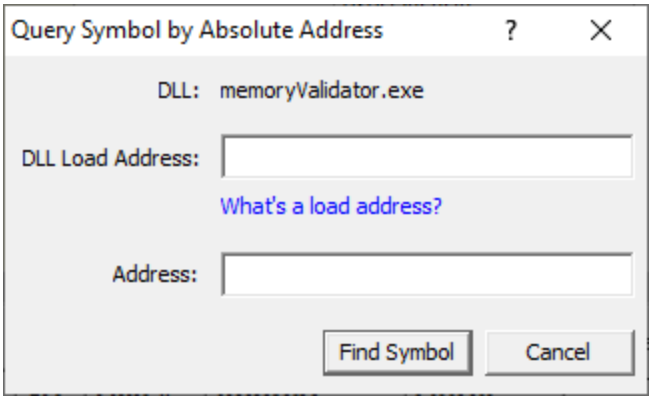
```
0x005f5eec (base 0x00400000)
```

The address is 0x005f5eec. The DLL loaded at 0x00400000. You'll notice the load address for all MemoryValidator.exe entries is 0x00400000.

From the Query menu choose **Find Symbol with Absolute Address...**.



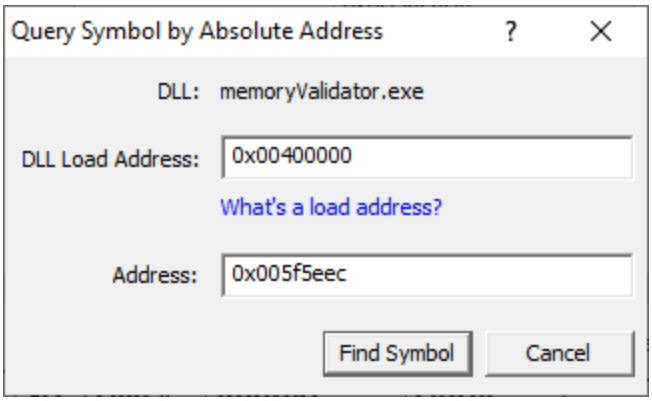
The Query Symbol by Absolute Address dialog is displayed.



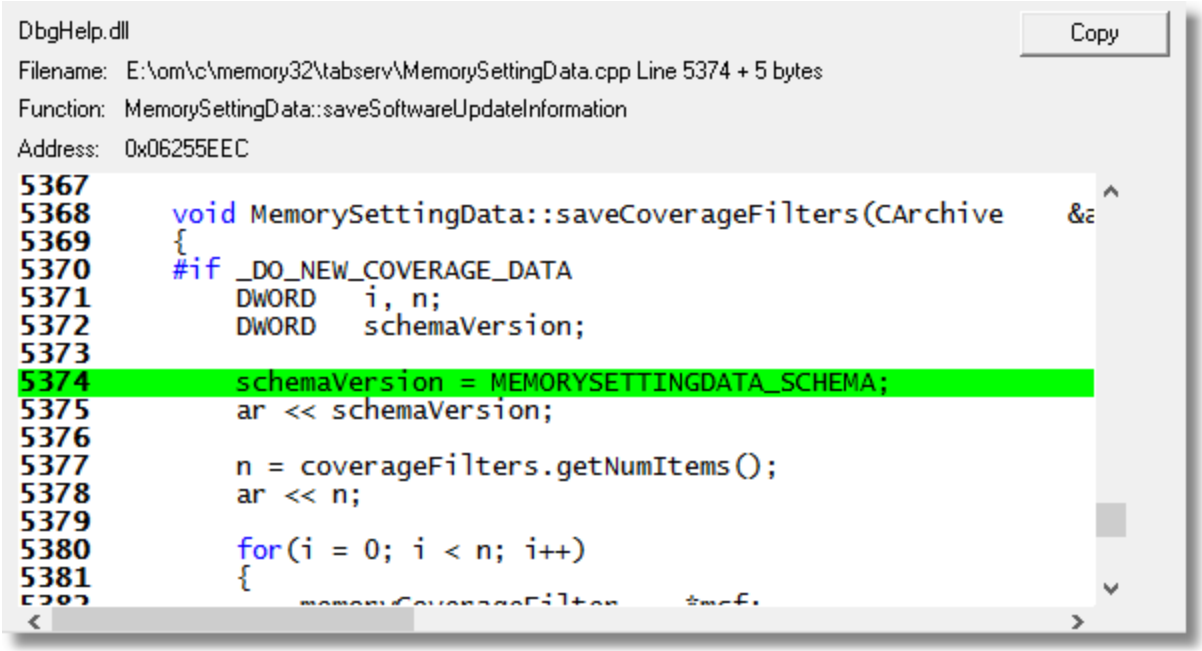
Type the DLL load address into the DLL Load Address field. Prefix any hexadecimal addresses with 0x.

Type the symbol address into the Address field. Prefix any hexadecimal addresses with 0x.

Click the **Find Symbol** button.



The appropriate location in the code is found and displayed.



Results:
Repeating the process for the data shown above resulted in this information.

```
0x005f5eec (base 0x00400000) C:\Program Files (x86)\Software Verification\C++ Memory Valid
C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Windows\syswow64\msvcrt.dll : 0x75D70000 : 0x75D7C3E4
C:\Windows\syswow64\msvcrt.dll : 0x75D70000 : 0x75D836B6
C:\Program Files (x86)\Software Verification\C++ Memory Validator\memoryValidator.exe : 0x
C:\Windows\syswow64\kernel32.dll : 0x754D0000 : 0x754E3365
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F6D
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F40
C:\Windows\SysWOW64\ntdll.dll : 0x77920000 : 0x77959F40
```

Help! I have a crash address but I don't know what the load address is? What do I do?

You need to read about load addresses.

7.2 Decoding a relative crash address

Scenario:

A customer has supplied you with a crash report containing a callstack with relative offsets from DLLs. The callstack also indicates which module relates to which address.

Example Data:

```
Exception code: C0000005 ACCESS_VIOLATION
Fault offset:   0x00036FA3 C:\WINDOWS\system32\MSVCRT.dll
Exception Parameters:
   0: 0x00000000 [Read Error]
   1: 0x5f8f2000 [Address]

Registers:
   EAX:B3BEB6D4
   EBX:5F8CB6C8
   ECX:150BE5B5
   EDX:00000000
   ESI:5F8F2000
   EDI:01B98DEC
   CS:EIP:001B:77C46FA3
   SS:ESP:0023:0012F158  EBP:0012F160
   DS:0023  ES:0023  FS:003B  GS:0000
   Flags:00010212


StackTrace

C:\WINDOWS\system32\MFC42u.DLL : 0x0000270a
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x000db989
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x000db1f8
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00121a83
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00121b7e
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00174ec5
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00175094
C:\WINDOWS\system32\MFC42u.DLL : 0x00013724
C:\WINDOWS\system32\MFC42u.DLL : 0x00014245
C:\WINDOWS\system32\MFC42u.DLL : 0x00001b31
C:\WINDOWS\system32\MFC42u.DLL : 0x0008cba7
```

This is data from a real crash many years ago.

Question:
There are no DLL load addresses and the addresses aren't addresses, but offsets from the start of a DLL. How do you decode these relative offsets?

Answer:
In the above data we can see a callstack containing entries for mfc42u.dll, and memoryValidator.exe.

All the modules are Microsoft DLLs except for the EXE, which is part of C++ Memory Validator, one of our tools.

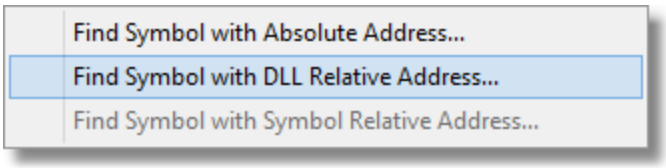
To decode these values, we load memoryValidator.exe into DWARF Browser.exe, then for each symbol we take the following actions.

For our purposes here, we're going to show how to convert one symbol. We're going to use the first symbol from memoryValidator.exe in the example data above.

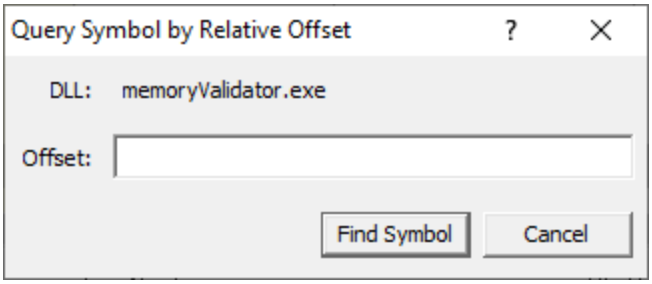
```
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x000db989
```

The relative address (or offset) is 0x000db989. We don't know the DLL load address.

From the Query menu choose **Find Symbol with DLL Relative Address...**.

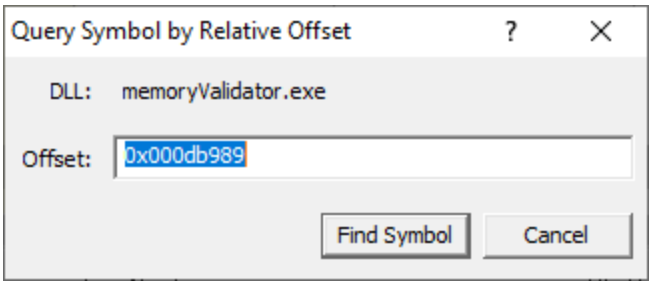


The Query Symbol by Absolute Address dialog is displayed.

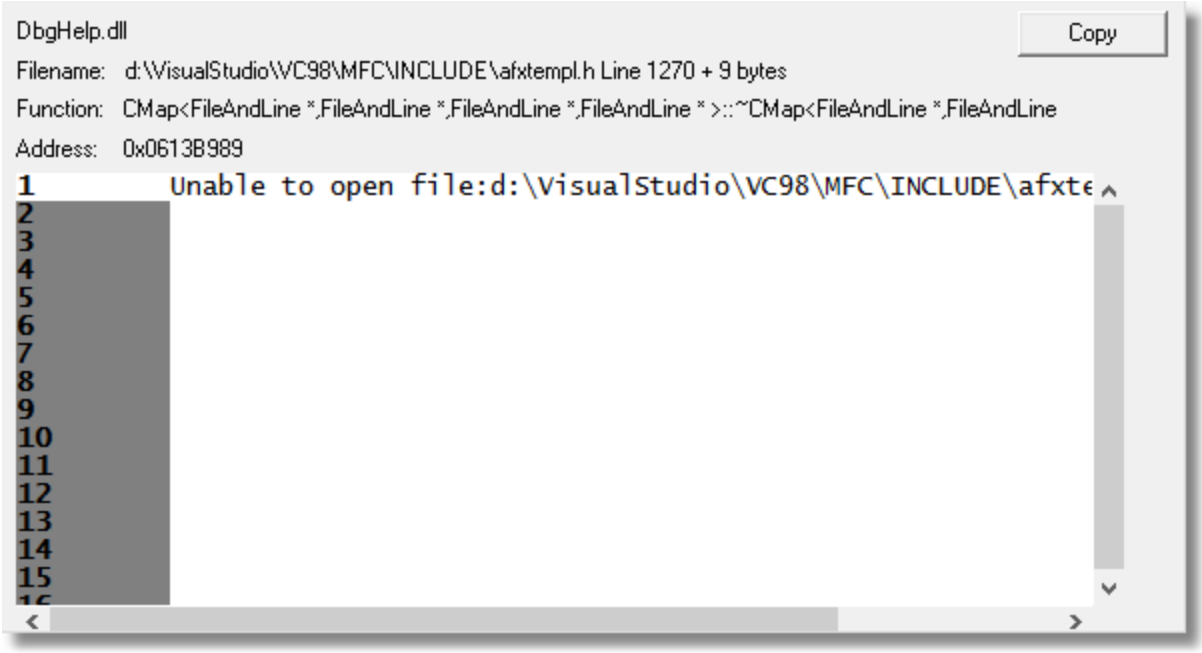


Type the relative address into the Offset field. Prefix any hexadecimal addresses with 0x.

Click the **Find Symbol** button.



The appropriate location in the code is found and displayed. In this example DWARF Browser could not locate the source code (as the file location is not valid on this machine)



Results:
Repeating the process for the data shown above resulted in this information.

```
Exception code: C0000005 ACCESS_VIOLATION
Fault offset:   0x00036FA3 C:\WINDOWS\system32\MSVCRT.dll
Exception Parameters:
   0: 0x00000000 [Read Error]
   1: 0x5f8f2000 [Address]

Registers:
   EAX:B3BEB6D4
   EBX:5F8CB6C8
   ECX:150BE5B5
   EDX:00000000
   ESI:5F8F2000
   EDI:01B98DEC
   CS:EIP:001B:77C46FA3
   SS:ESP:0023:0012F158  EBP:0012F160
   DS:0023  ES:0023  FS:003B  GS:0000
   Flags:00010212


StackTrace

C:\WINDOWS\system32\MFC42u.DLL : 0x0000270a
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x000db989
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x000db1f8
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00121a83
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00121b7e
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00174ec5
C:\Program Files\Software Verification\Memory Validator\memoryValidator.exe : 0x00175094
C:\WINDOWS\system32\MFC42u.DLL : 0x00013724
C:\WINDOWS\system32\MFC42u.DLL : 0x00014245
C:\WINDOWS\system32\MFC42u.DLL : 0x00001b31
C:\WINDOWS\system32\MFC42u.DLL : 0x0008cba7
```

7.3 Decoding a symbol relative crash address

Scenario:

A customer has supplied you with a crash report containing a callstack with symbol relative offsets from DLLs. The callstack also indicates which module relates to which address.

Example Data:

```
ntoskrnl.exe!KeSynchronizeExecution+0x2246
ntoskrnl.exe!KeWaitForMultipleObjects+0x135e
ntoskrnl.exe!KeWaitForMultipleObjects+0xdd9
ntoskrnl.exe!KeWaitForSingleObject+0x373
ntoskrnl.exe!KeStallWhileFrozen+0x1977
ntoskrnl.exe!_misaligned_access+0x13f9
ntoskrnl.exe!KeWaitForMultipleObjects+0x152f
ntoskrnl.exe!KeWaitForMultipleObjects+0xdd9
ntoskrnl.exe!KeWaitForSingleObject+0x373
ntoskrnl.exe!NtWaitForSingleObject+0xb2
ntoskrnl.exe!setjmpex+0x34a3
ntdll.dll!ZwWaitForSingleObject+0xa
KERNELBASE.dll!WaitForSingleObjectEx+0x98
svlcoveragevalidatorstub_x64.dll!sendCommandLineAndStartTimeToGUI+0x2868
svlcoveragevalidatorstub_x64.dll!setValidatorFeedbackHookingComplete+0x1fa6
svlcoveragevalidatorstub_x64.dll!svl_sendMessageRawToUserInterface+0x21837
svlcoveragevalidatorstub_x64.dll!svl_sendMessageRawToUserInterface+0x218cb
KERNEL32.DLL!BaseThreadInitThunk+0x22
ntdll.dll!RtlUserThreadStart+0x34
```

This is real data from a bug at Software Verify Ltd. This is one thread from many in a dump relating to a deadlock bug we were investigating.

Question:
How do you decode these symbol relative offsets?

Answer:
In the above data we can see a callstack containing entries for ntoskrnl.exe, ntdll.dll, kernelbase.dll, kernel32.dll and svlcoveragevalidatorstub_x64.dll.

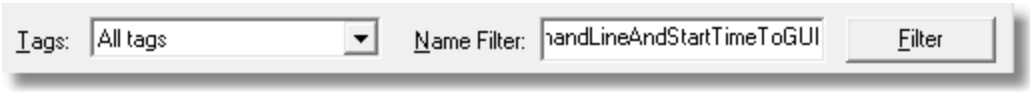
All the modules are Microsoft DLLs except for one DLL, which is part of C++ Coverage Validator, one of our tools.

To decode these values, we load svlCoverageValidatorStub_x64.dll into DWARF Browser.exe (64 bit), then for each symbol we take the following actions.

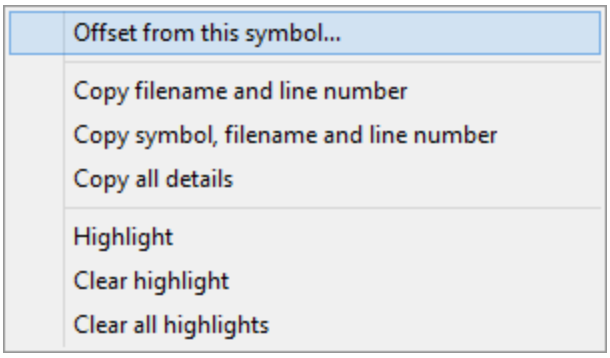
For our purposes here, we're going to show how to convert one symbol. We're going to use the first symbol from svlCoverageValidatorStub_x64.dll in the example data above.

```
svlcoveragevalidatorstub_x64.dll!sendCommandLineAndStartTimeToGUI+0x2868
```

Type the symbol name into the **Name Filter** field, then click **Filter**. This makes it easy to find the symbol we want.

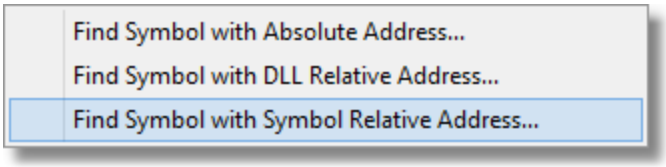


Once we have found the symbol, right click on the symbol to display the context menu and choose **Offset from this symbol...**.

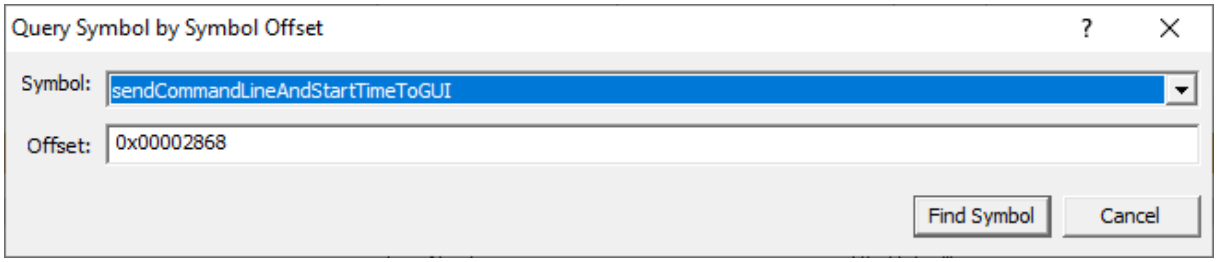


An alternate method is to click on the symbol to select it, then from the Query menu choose **Find Symbol with Symbol Relative Address...**.

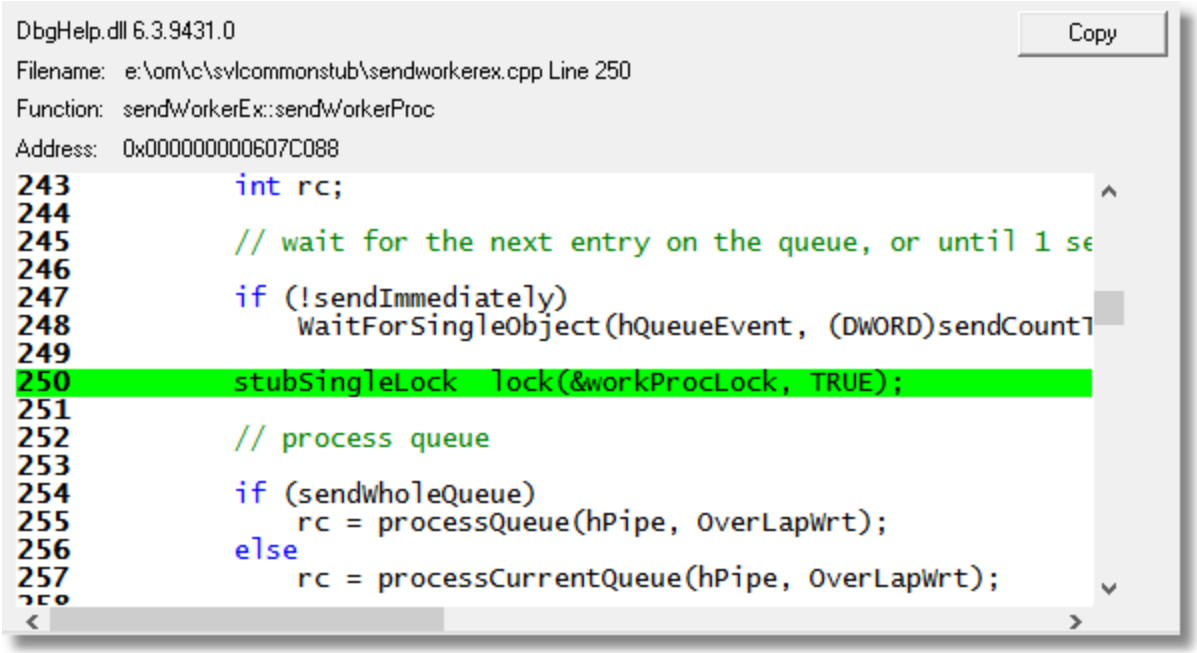
Or, from the Query menu choose **Find Symbol with Symbol Relative Address...** then choose the symbol you want from the combo box.



Type the offset into the dialog (hex values must be prefixed with 0x) and click OK.



The appropriate location in the code is found and displayed.



Results:
Repeating the process for the data shown above resulted in this information.

```
svlcoveragevalidatorstub_x64.dll!sendCommandLineAndStartTimeToGUI+0x2868          sendWorke
svlcoveragevalidatorstub_x64.dll!setValidatorFeedbackHookingComplete+0x1fa6       stubSendC
svlcoveragevalidatorstub_x64.dll!svl_sendMessageRawToUserInterface+0x21837        memcpy
svlcoveragevalidatorstub_x64.dll!svl_sendMessageRawToUserInterface+0x218cb        wcscpy
```

7.4 Decoding an Event Viewer XML crash log

Scenario:

A customer has supplied you with data from Windows Event Viewer about a crash. The log contains XML and you don't know which values are relevant.

The event log data will have a provider name of "Windows Error Reporting" or "Application Error".

The XML data is found on the "Details" tab with the XML View radio box selected.

Example Data:

```xml
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Windows Error Reporting" />
    <EventID Qualifiers="0">1001</EventID>
    <Level>4</Level>
    <Task>0</Task>
    <Keywords>0x80000000000000</Keywords>
    <TimeCreated SystemTime="2020-02-10T17:39:08.000000000Z" />
    <EventRecordID>260219</EventRecordID>
    <Channel>Application</Channel>
    <Computer>hydra</Computer>
    <Security />
  </System>
  <EventData>
    <Data>2023787729086567941</Data>
    <Data>1</Data>
    <Data>APPCRASH</Data>
    <Data>Not available</Data>
    <Data>0</Data>
    <Data>testDeliberateCrash.exe</Data>
    <Data>1.0.0.1</Data>
    <Data>5e419525</Data>
    <Data>testDeliberateCrash.exe</Data>
    <Data>1.0.0.1</Data>
    <Data>5e419525</Data>
    <Data>c0000005</Data>
    <Data>000017b2</Data>
    <Data />
    <Data />
    <Data>C:\Users\stephen\AppData\Local\Temp\WERA14E.tmp.WERInternalMetadata.xml</Data>
    <Data>C:\Users\stephen\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_testDelibera
    <Data />
    <Data>0</Data>
    <Data>3cc45263-4c2c-11ea-83d3-001e4fdb3956</Data>
    <Data>0</Data>
    <Data>54756af49aec84f97c15f03794ffd605</Data>
  </EventData>
</Event>
```

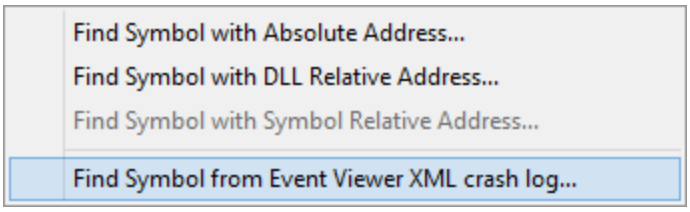

This is data from a test program that is designed to crash.

Question:
There the event log indicates a DLL, but no load address, two different addresses, an exception code and an offset from the start of the DLL. How do you decode this relative offset?

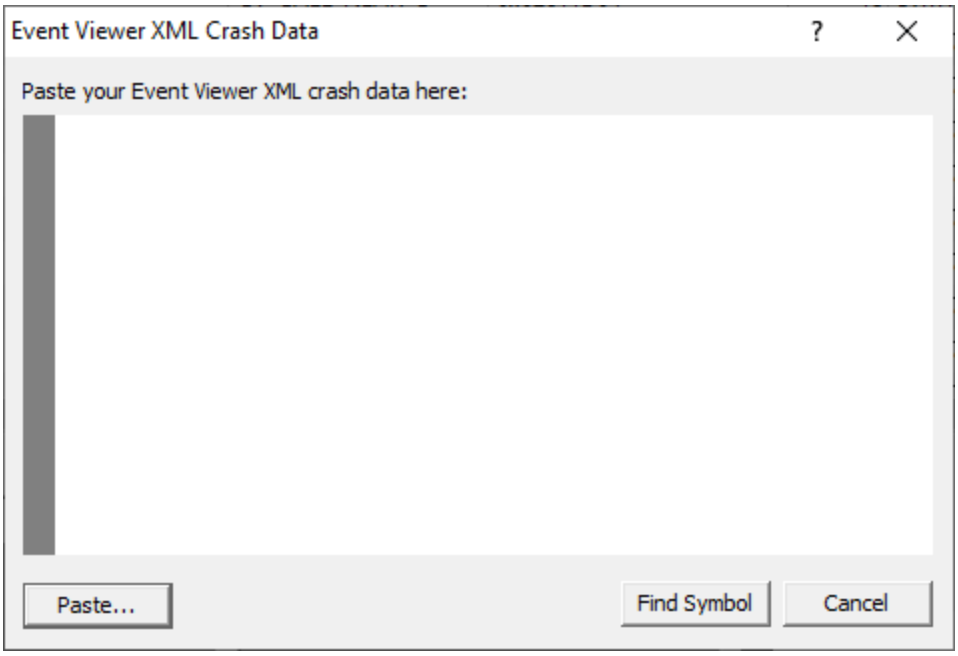
Answer:
DWARF Browser has an option specifically for this occasion.

The XML data indicates the crash happened in **testDeliberateCrash.exe**. Load this into DWARF Browser being sure to load the correct build version so that symbols match the crash addresses.

From the Query menu choose **Find Symbol from Event Viewer XML crash log...**.

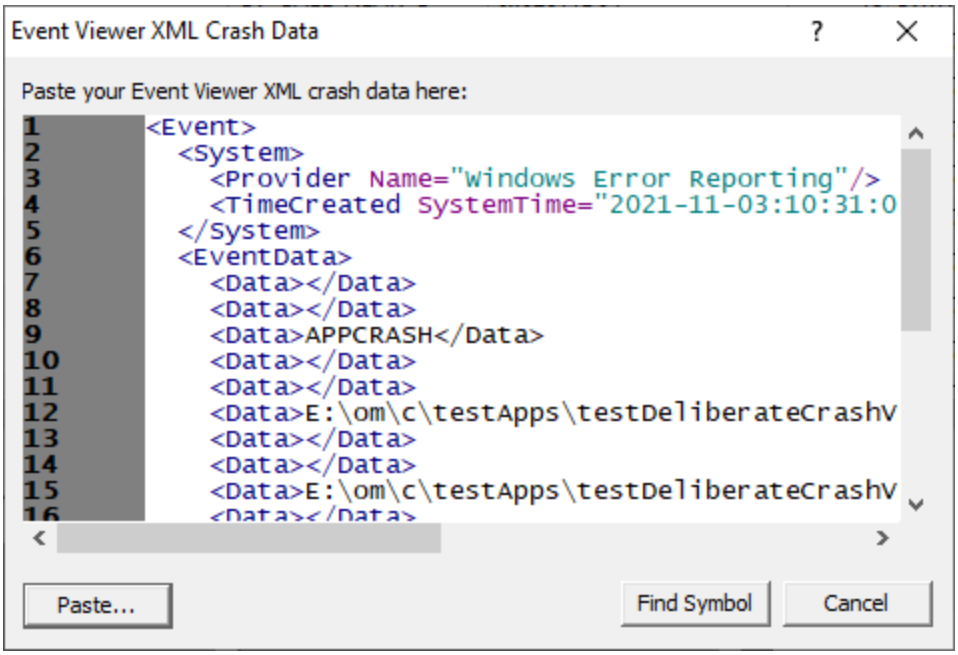


The Query Symbol by Absolute Address dialog is displayed.

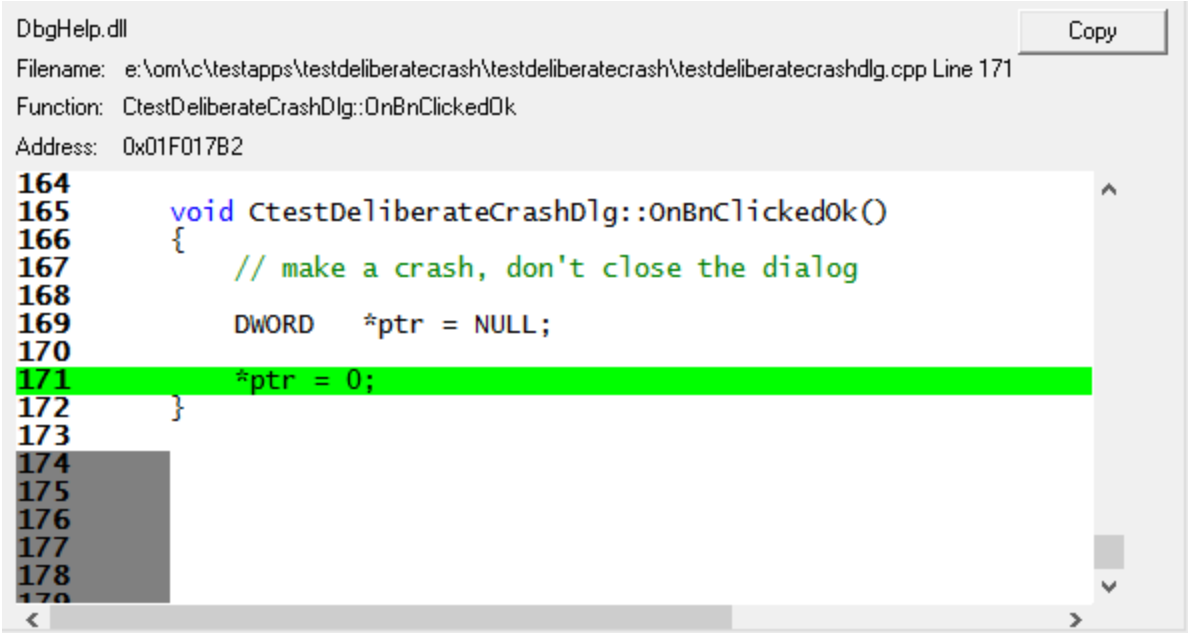


Paste the XML data from the Event Viewer into the text field.

Click the **Find Symbol** button.



The appropriate location in the code is found and displayed.



7.5 What is a load address?

A load address is the address at which a DLL loads.

All versions of Microsoft Windows load modules (.dll, .exe) into address space that is reserved using a call to VirtualAlloc().

The allocation of VirtualAlloc() can be queried by calling Win32 API GetSystemInfo() and examining the value returned in **dwAllocationGranularity**. For all versions of Microsoft Windows this has been 64KB.

Why is the load address important?

The load address is important because without it we can't calculate the offset inside the DLL so that we can obtain a symbol.

That's why a crash address with no DLL Load Address isn't very useful - we don't know which DLL the crash is in, nor do we know where the DLL was loaded.

But I don't have a load address. What can I do?

Depending upon how your module (DLL/EXE) was built we may be able to guess the correct load address.

If the OS you are using is Windows XP or earlier, we can guess the address.

First a brief chat about Address Space Layout Randomisation...

If the OS you are using is Windows Vista or later, we may not be able to guess the load address. The reason this is not precise is because something known as Address Space Layout Randomisation (ASLR) was introduced with Microsoft Vista to improve security against many malicious computer attacks. Any program built with ASLR enabled when run on Vista (or later) will have the load address for all modules (including the .exe) randomised, making guessing the load address a waste of time.

ASLR is enabled by the /DYNAMICBASE in the linker settings of Visual Studio.

If you are using Visual Studio 2005 or earlier this setting is not available, your program is not affected by ASLR.

If you are using Visual Studio 2008 or later you will need to check to see if this option is present. If it is not present, your program is not affected by ASLR.

If you are not using Visual Studio to build your program then you may not be affected by this option, consult your compiler/linker documentation.

If your program is not affected by ASLR...

We can try to guess the load address of your DLL/EXE. We can do this regardless of which compiler/linker you used to build your program. All the programs I mention here are free to download at the time of writing this help file.

VM Validator
https://www.softwareverify.com/cpp-virtual-memory.php

This works for 32 bit and 64 bit programs.

Method 1

- Start your program using VM Validator or attach to your running program with VM Validator.
- On the Summary tab, inspect the DLLs sub tab in the lower half of the display.
- Find the DLL name in the DLL column.
- The load address is the value in the Address column.

DLLs | Page Faults

DLL (133)	Fault Count	Address	Size	Commit	Reserve	CPU
E:\om\c\dbgHelpBrowser\Release\x86\dbgHelpBrowser.exe	0	0x00400000	1176.00 KB	1176.00 KB	0.00 KB	x86
E:\om\c\testApps\testDeliberateCrash\Release\testDeliberateCrash.exe	0	0x00640000	100.00 KB	100.00 KB	0.00 KB	x86
E:\om\c\dbgHelpBrowser\Release\x86\svIPeInfo.dll	0	0x006C0000	172.00 KB	172.00 KB	0.00 KB	x86

Method 2

- Start your program using VM Validator or attach to your running program with VM Validator.
- Go to the Paragraphs tab.
- Find any purple entry, check the DLL name in the Description field.
- The load address is the value in the Address column.

Summary | Virtual | Pages | Paragraphs

Address	Size	Type	Protect	Working Set	Shared	Swap	Description
0x002C0000	64 KB	Private	Read, Write	Read/write.			Commited, Reserved
0x002D0000	152 KB	Private					Reserved, Commited, Reserved
0x00300000	1,024 KB	Private					Reserved
0x00400000	1,176 KB	Image	Read Only	Read-only. Executable and read-only.	Shared: 98		e:\om\c\dbghelpbrowser\release\x86\dbghelpbrowser.exe
0x00530000	796 KB	Mapped	Read Only	Read-only.	Shared: 49		Commited, Free

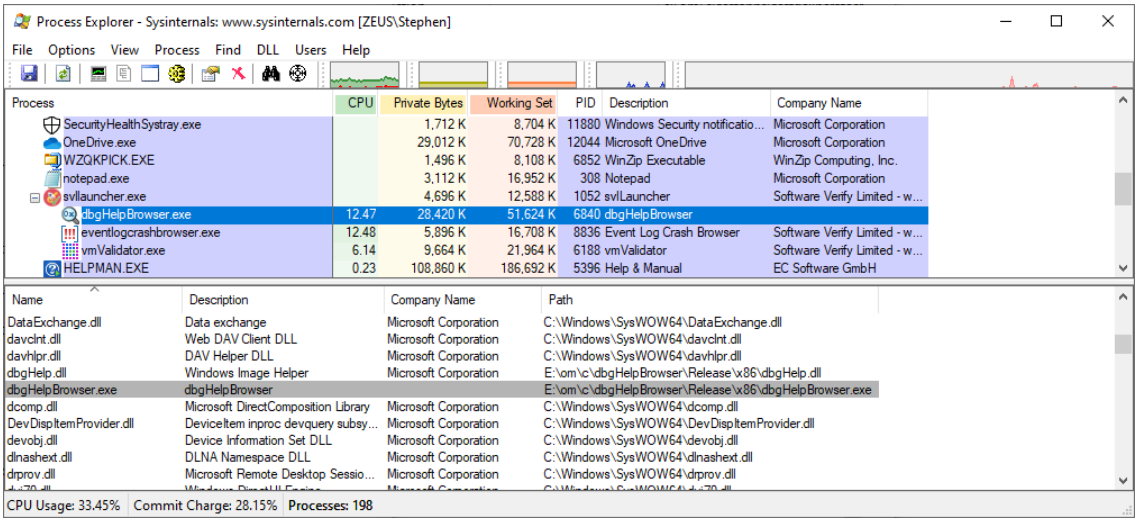
In the example above, for dbgHelpBrowser.exe, the load address is 0x00400000.

Process Explorer
https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx

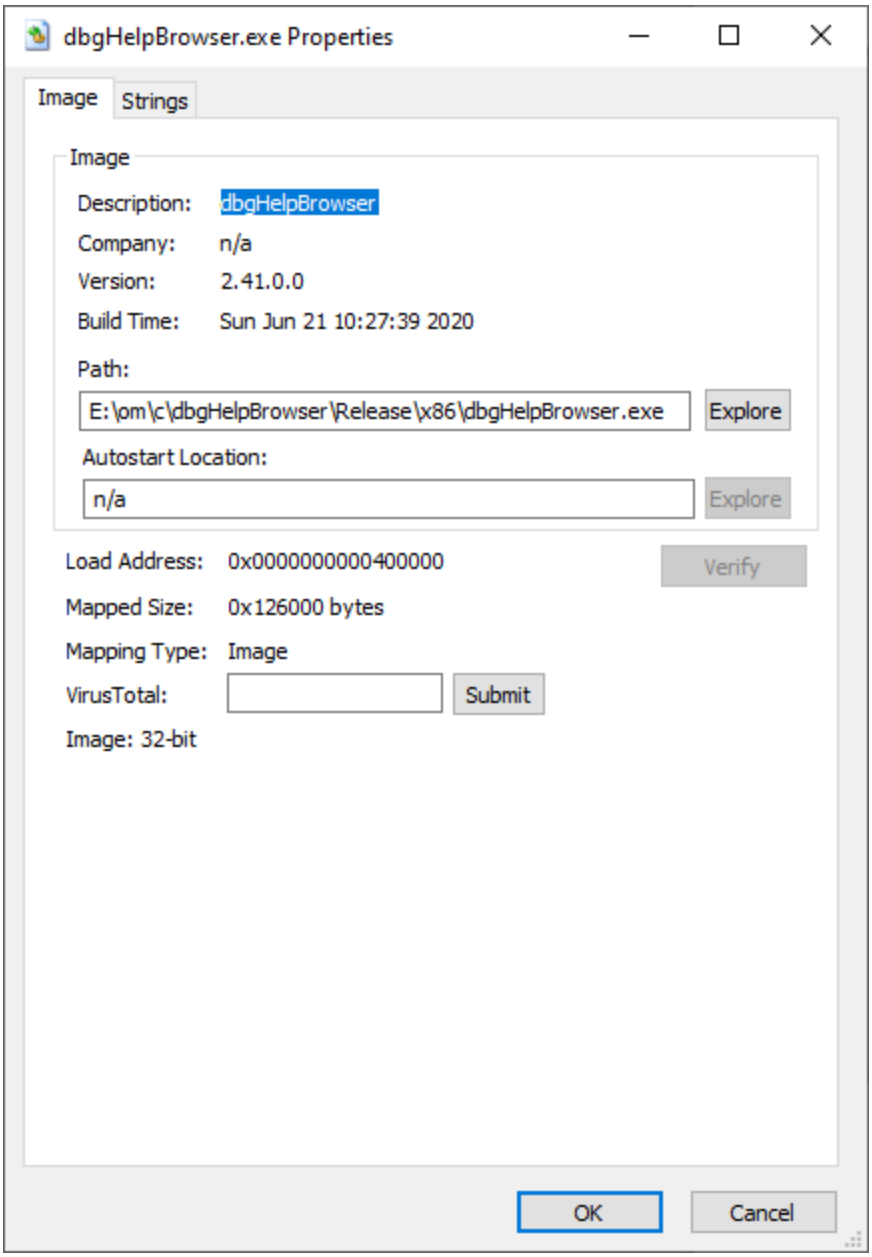
This works for 32 bit and 64 bit programs.

- Start your program
- Start Process Explorer. *If your program is a service or runs as administrator you'll need to start Process Explorer as administrator.*
- In Process Explorer, enable View -> Show Lower Pane. Then for View -> Lower Pane Window, choose DLLs.

- Select your program in the top window.
- Find your DLL in the bottom window. Right click. Choose Properties from the Context menu.



- In the Properties dialog, read the load address.

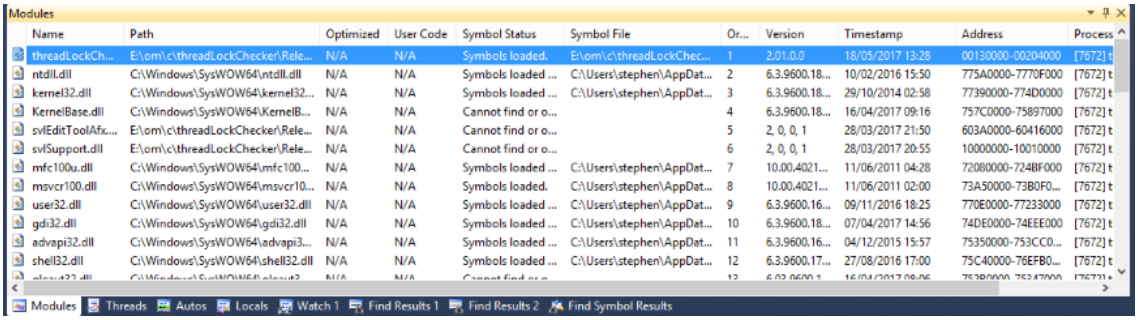


In the example above, for dbgHelpBrowser.exe, the load address is 0x00400000.

Visual Studio (any version)
https://www.visualstudio.com/

- Start Visual Studio.
- From the Project menu, choose File -> Open -> Solution. Choose your executable.
- From the Debug menu, choose Start Debugging.
- From the Debug menu, choose Windows -> Modules.

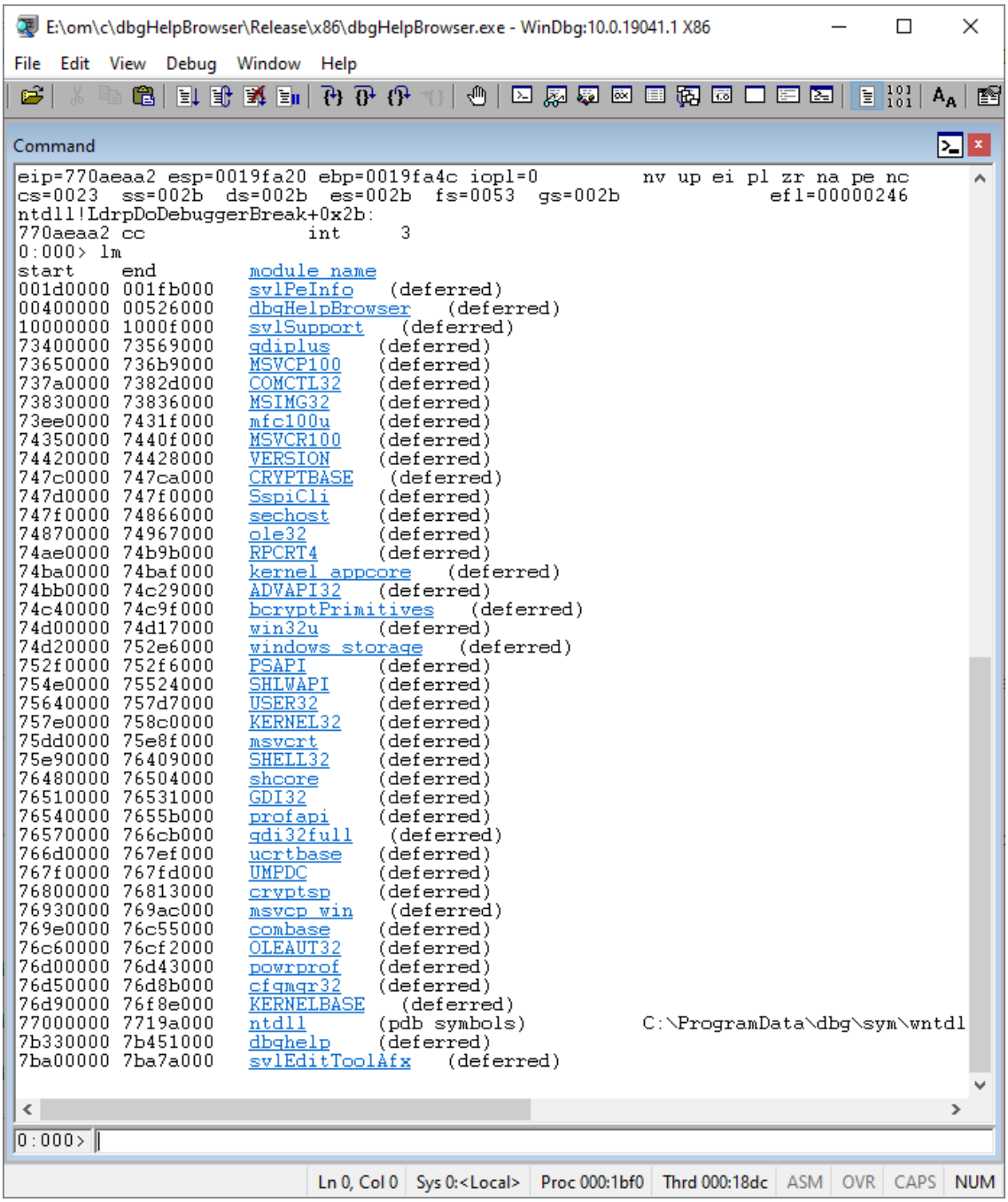
- In the Modules window, find your DLL, then read the Address column.



In the example above, for threadLockChecker.exe, the load address is 0x00130000.

WinDbg
https://msdn.microsoft.com/en-gb/library/windows/hardware/ff551063(v=vs.85).aspx

- Start WinDbg
- From the File menu, choose Open Executable. Choose your executable.
- Type lm, then press return.
- All modules are listed. Find your module. The start address is the load address.



In the example above, for threadLockChecker.exe, the load address is 0x00130000.

Final Comments

OK, you should now know how to find the load address of a DLL or an EXE (or any module type). Remember that a load address obtained this way is only valid for symbol decoding if the executable doesn't have ASLR applied to it.

If your crash reporting code only grabs crash addresses and not DLL load addresses, you need to update your code so that you grab DLL load addresses at the time of the crash. That way you know for sure what the load addresses were and you won't have to guess the load addresses in future.

Part VIII

8 Command Line Interface

DWARF Browser can be used from the command line as well as with the GUI.

The command line options allow you to view DWARF debug information that is embedded in an executable file, and optionally highlight a symbol at a specified offset.

/fileName

Specifies the module to load. This is typically a .exe or a .dll.

/fileName path-to-executable

Example: /fileName e:\om\c\test\release\test.exe

/offset

Specifies an offset inside the executable. DWARF Browser will highlight the symbol that occupies this location.

Typically this offset will be calculated from a crash location.

For example:

If a DLL is loaded at 0x00400000 and a crash happens at 0x00420192, the offset is calculated by subtracting the DLL load address from the crash address.

That is: 0x00420192 - 0x00400000, which gives 0x00020192.

The offset is 0x00020192.

The offset must be specified in hexadecimal with a leading 0x.

/offset value

Example: /offset 0x00020192

Example Command Line

32 bit applications

```
dwarfBrowser.exe /fileName e:\test\release\test.exe /offset 0x00020192
```

64 bit applications

```
dwarfBrowser_x64.exe /fileName e:\test\release\test.exe /offset 0x00020192
```