Minidump Browser

by

Software Verify

Minidump Browser

Easily inspect Minidump contents.

by Software Verify Limited

Welcome to the Minidump Browser software tool.

Minidump Browser is a software tool that allows you to inspect the contents of minidumps.

We hope you will find this document useful.

MiniDump Browser Help

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: June 2025 in United Kingdom.

Table of Contents

Part I

1 How to get Minidump Browser

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

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

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

Whilst Minidump Browser is free for commercial use, Minidump 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

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 II

2 What does Minidump Browser do?

Minidump Browser allows you to view kernel dumps and minidumps on your machine, or your network.

32 bit and 64 bit

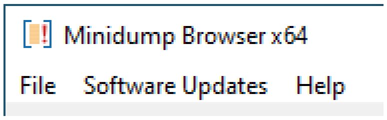
32 bit and 64 bit kernel dumps are supported.

32 bit and 64 bit minidumps are supported.

Part III

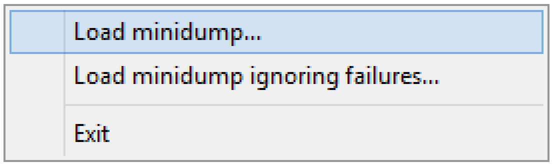
3 Menu

The main menu contains three menus, File, Software Updates and Help.



3.1 File

The File menu controls the scanning and display of minidumps.



File menu > **Load minidump...** > loads a kernel dump or a minidump and displays it.

If the kernel dump or minidump is the wrong bit depth (32 bit when running 64 bit, or vice versa) then the other version of Minidump browser is started to display the minidump.

If any errors occur when trying to load the minidump, the load fails. This means that mindumps from ARM, IA64 and other architectures can't be displayed.

File menu > **Load minidump ignoring failures...** > loads a minidump and displays it.

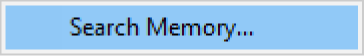
If the minidump is the wrong bit depth (32 bit when running 64 bit, or vice versa) then the other version of Minidump browser is started to display the minidump.

If any errors occur when trying to load the minidump, the load fails to load just the failing part of the minidump and continues with other parts of the minidump.
This means that mindumps from ARM, IA64 and other architectures can be displayed, but may have incomplete information.

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

3.2 Inspect

The Inspect menu allows you to view arbitrary memory, or to search for memory.

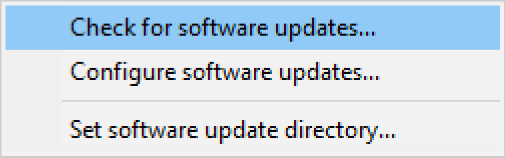


Inspect menu > **Search memory...** > search for a text string or a sequence of bytes. The Search Memory Dialog is displayed.

3.3 Software Updates

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

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

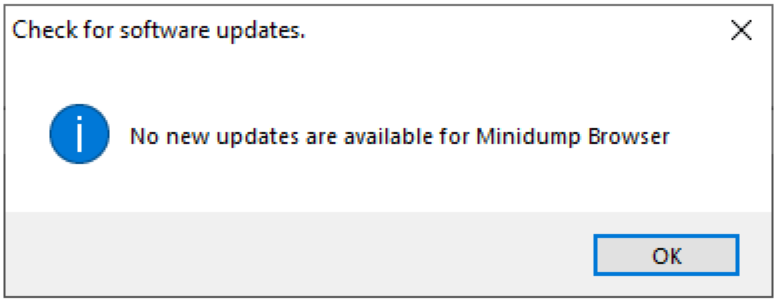

Check for software updates...
Configure software updates...
Set software update directory...

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.

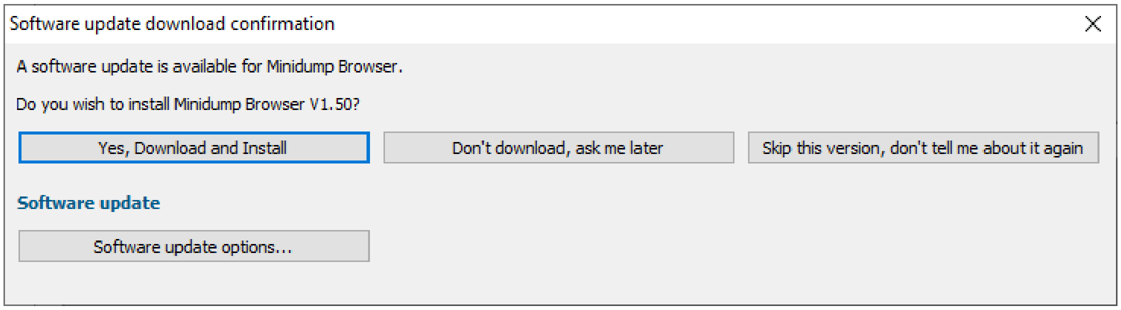
If no updates are available, you'll just see this message:



No new updates are available for Minidump Browser

Software Update dialog

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



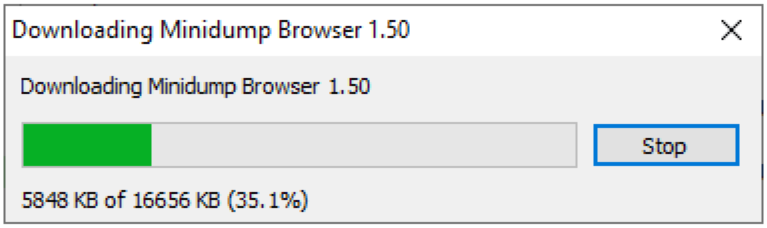
Software update download confirmation

A software update is available for Minidump Browser.

Do you wish to install Minidump Browser V1.50?

Yes, Download and Install
Don't download, ask me later
Skip this version, don't tell me about it again
Software update
Software update options...

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



Downloading Minidump Browser 1.50

Downloading Minidump Browser 1.50

5848 KB of 16656 KB (35.1%)

Once the update has downloaded, Minidump 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 Minidump 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 Minidump Browser as follows:

- Ensure Minidump 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

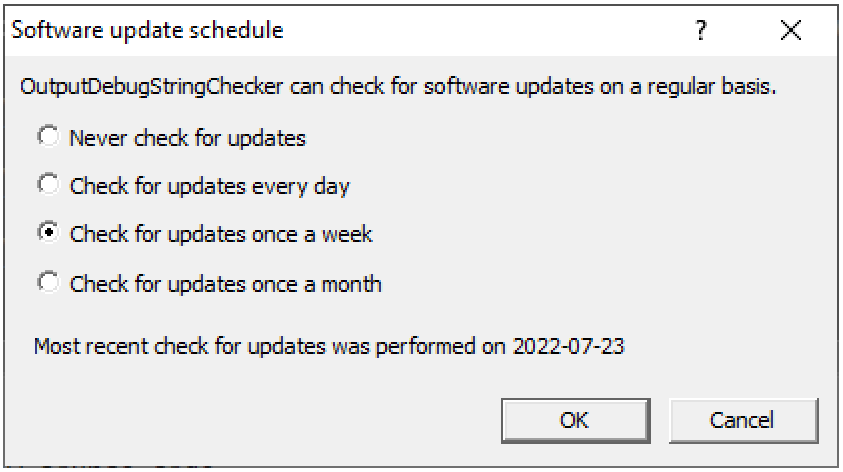
Minidump Browser can automatically check to see if a new version of Minidump Browser is available for downloading.

☰ **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 schedule

OutputDebugStringChecker can check for software updates on a regular basis.

○ Never check for updates

○ Check for updates every day

● Check for updates once a week

○ Check for updates once a month

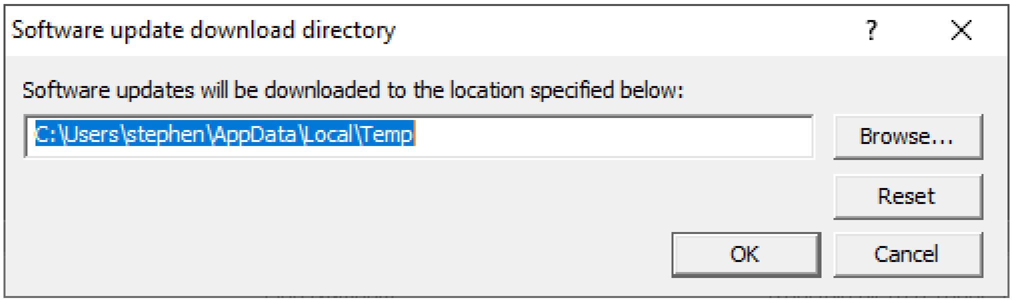
Most recent check for updates was performed on 2022-07-23

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



Software update download directory

Software updates will be downloaded to the location specified below:

C:\Users\stephen\AppData\Local\Temp

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)

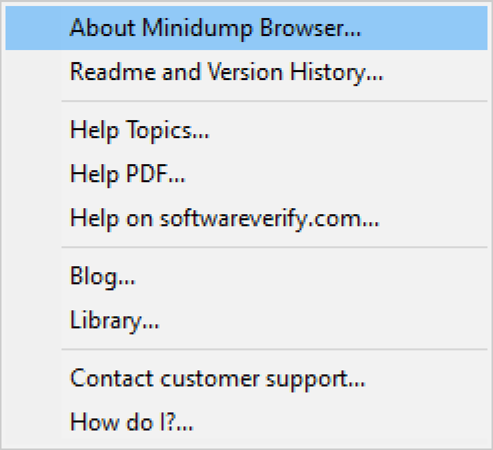
When modifying the download directory, you should ensure the directory will continue to be valid. Updates may no longer occur if the download location is later invalidated.

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

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

3.4 Help

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


About Minidump Browser...
Readme and Version History...
Help Topics...
Help PDF...
Help on softwareverify.com...
Blog...
Library...
Contact customer support...
How do I?...

Help menu › **About Minidump Browser...** › displays information about Minidump Browser.

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

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

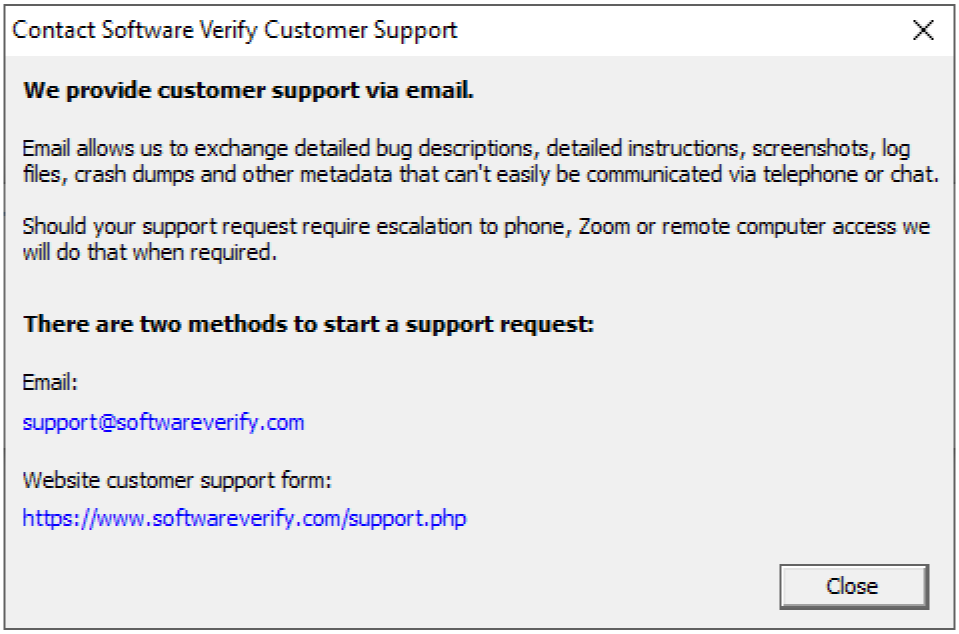
Help menu › **Help PDF...** › displays this help file in PDF format.

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.



Contact Software Verify Customer Support

We provide customer support via email.

Email allows us to exchange detailed bug descriptions, detailed instructions, screenshots, log files, crash dumps and other metadata that can't easily be communicated via telephone or chat.

Should your support request require escalation to phone, Zoom or remote computer access we will do that when required.

There are two methods to start a support request:

Email:

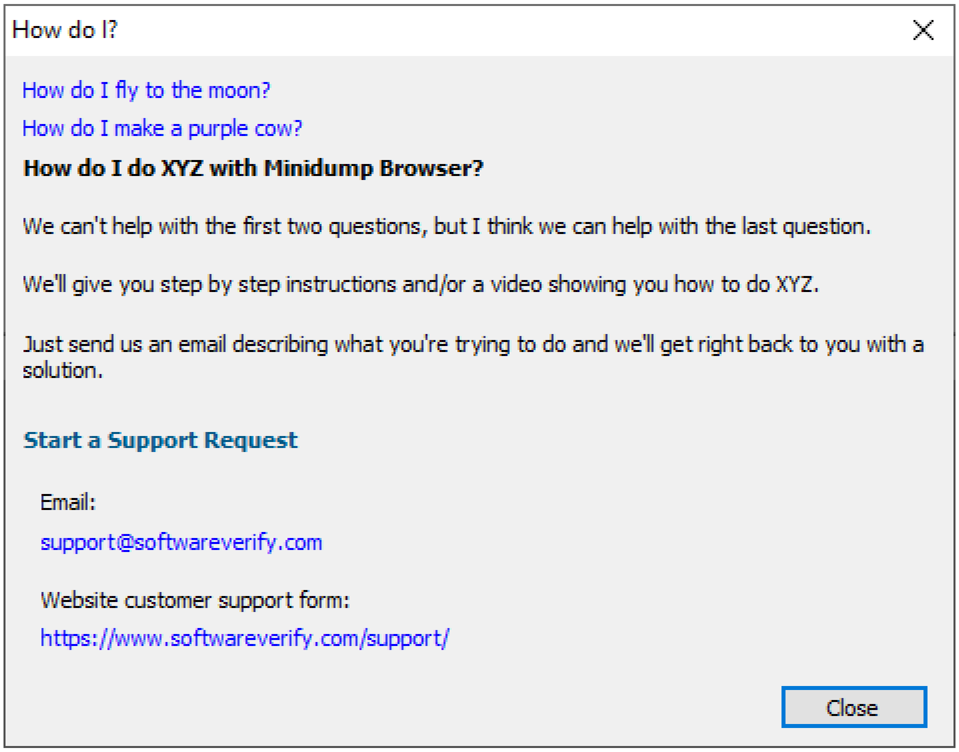
support@softwareverify.com

Website customer support form:

https://www.softwareverify.com/support.php

Click a link to contact customer support.

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



How do I fly to the moon?

How do I make a purple cow?

How do I do XYZ with Minidump Browser?

We can't help with the first two questions, but I think we can help with the last question.

We'll give you step by step instructions and/or a video showing you how to do XYZ.

Just send us an email describing what you're trying to do and we'll get right back to you with a solution.

Start a Support Request

Email:
support@softwareverify.com

Website customer support form:
https://www.softwareverify.com/support/

Part IV

4 The user interface

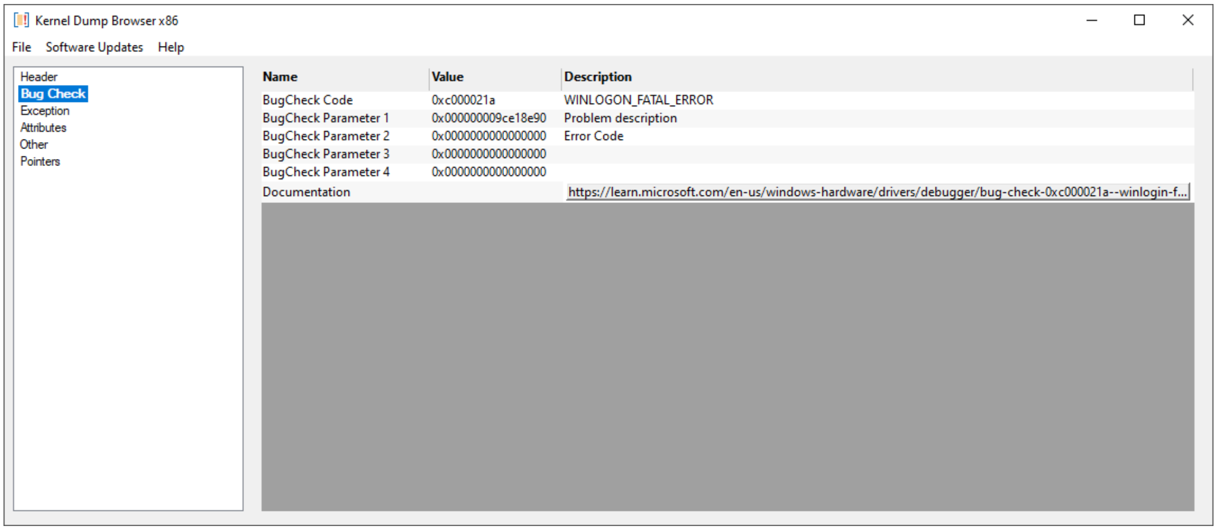
Enter topic text here.

4.1 Kernel dumps (Blue Screen of Death)

The Kernel Dump Browser user interface is shown below.

When a kernel dump contains an exception the exception display will be automatically selected as the first display to show you information.

Not all information in a kernel dump is valid. Information that isn't valid has the same value as the signature field: 0x45474150.



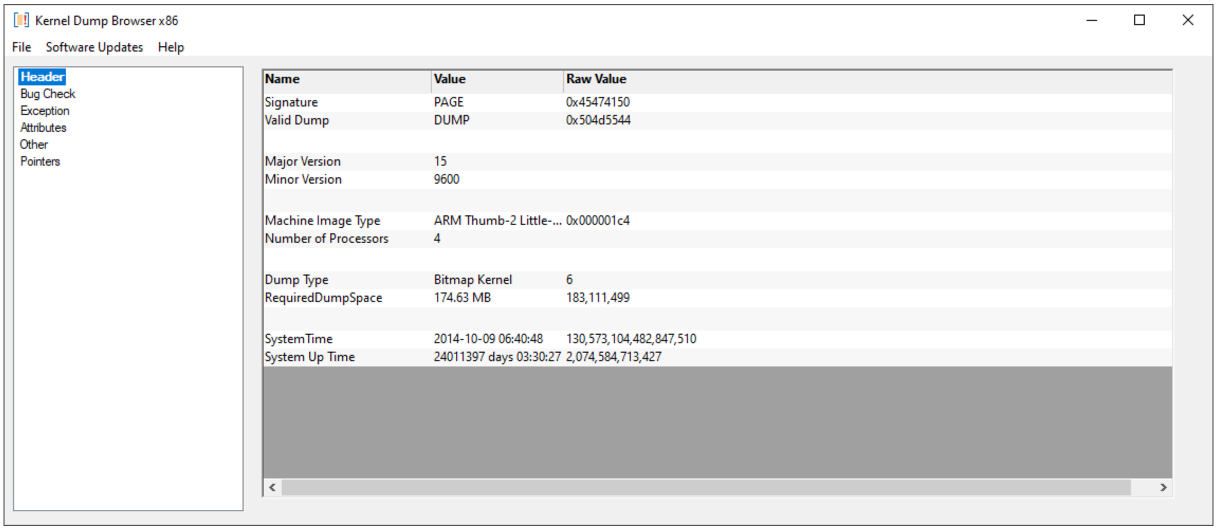
Name	Value	Description
BugCheck Code	0xc000021a	WINLOGON_FATAL_ERROR
BugCheck Parameter 1	0x000000009ce18e90	Problem description
BugCheck Parameter 2	0x0000000000000000	Error Code
BugCheck Parameter 3	0x0000000000000000	
BugCheck Parameter 4	0x0000000000000000	
Documentation		https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0xc000021a--winlogin-f...

The display shows six pages of data about the kernel dump.

Each page is listed on the left hand side. Selecting that entry displays the page on the right hand side.

4.1.1 Header

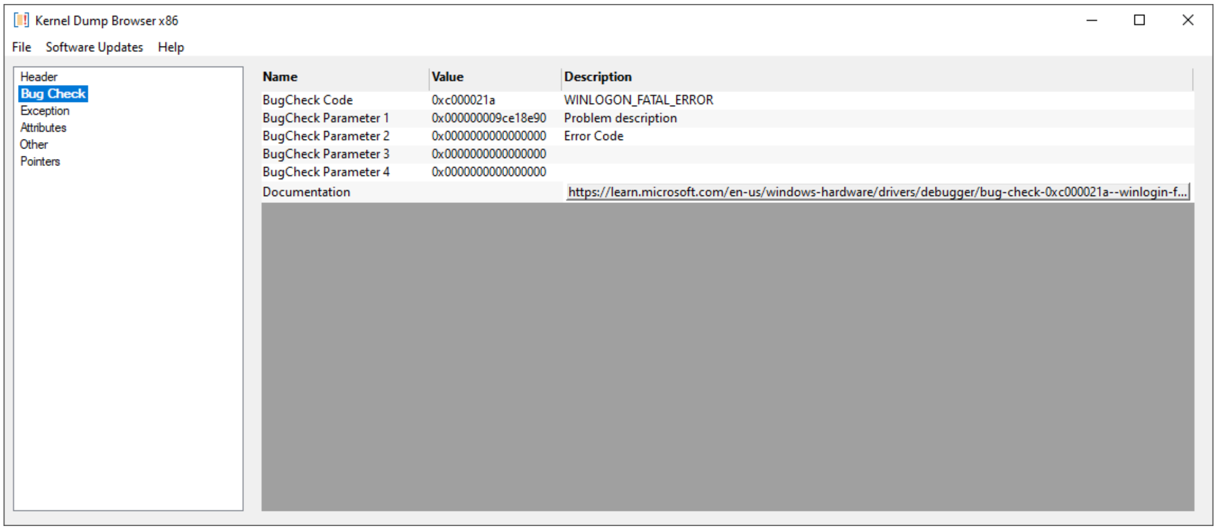
The Header page displays general information about the kernel dump.



Name	Value	Raw Value
Signature	PAGE	0x45474150
Valid Dump	DUMP	0x504d5544
Major Version	15	
Minor Version	9600	
Machine Image Type	ARM Thumb-2 Little-...	0x000001c4
Number of Processors	4	
Dump Type	Bitmap Kernel	6
RequiredDumpSpace	174.63 MB	183,111,499
SystemTime	2014-10-09 06:40:48	130,573,104,482,847,510
System Up Time	24011397 days 03:30:27	2,074,584,713,427

4.1.2 Bug Check

The Bug Check page displays exception information from the kernel dump.

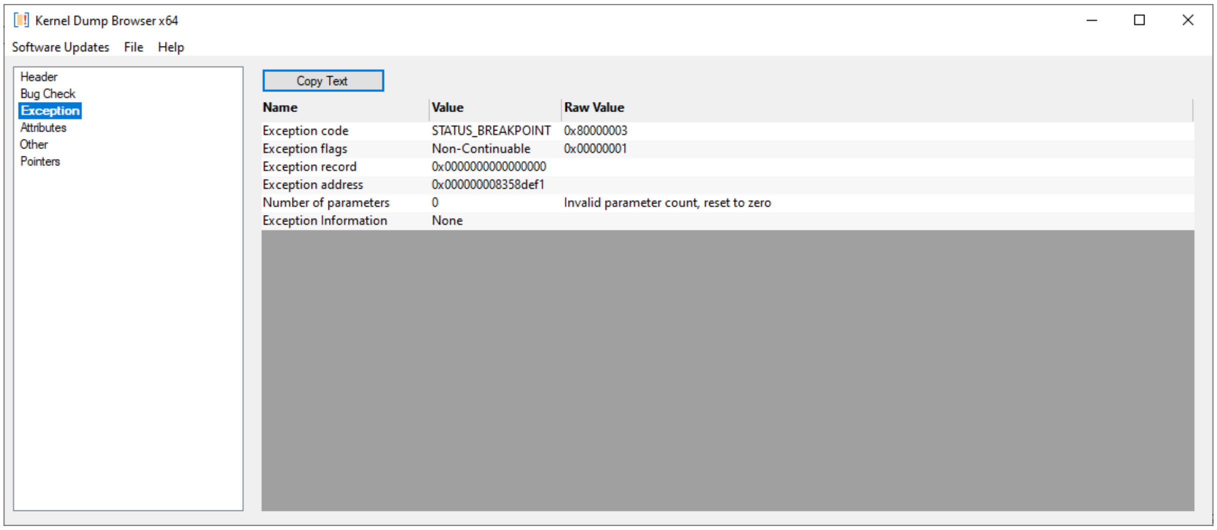


Name	Value	Description
BugCheck Code	0xc000021a	WINLOGON_FATAL_ERROR
BugCheck Parameter 1	0x000000009ce18e90	Problem description
BugCheck Parameter 2	0x0000000000000000	Error Code
BugCheck Parameter 3	0x0000000000000000	
BugCheck Parameter 4	0x0000000000000000	
Documentation		https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0xc000021a--winlogin-f...

For each BugCheck code we provide a link to the official Microsoft documentation for the BugCheck. Clicking the link will open the default web browser.

4.1.3 Exception

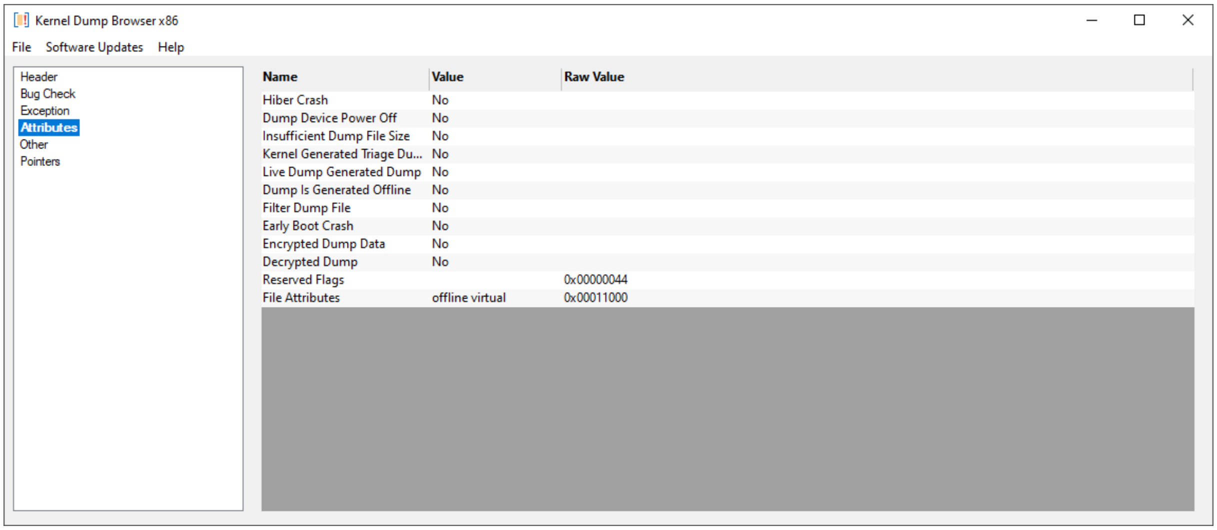
The Exception page displays exception information from the kernel dump.



Name	Value	Raw Value
Exception code	STATUS_BREAKPOINT	0x80000003
Exception flags	Non-Continuable	0x00000001
Exception record	0x0000000000000000	
Exception address	0x000000008358def1	
Number of parameters	0	Invalid parameter count, reset to zero
Exception Information	None	

4.1.4 Attributes

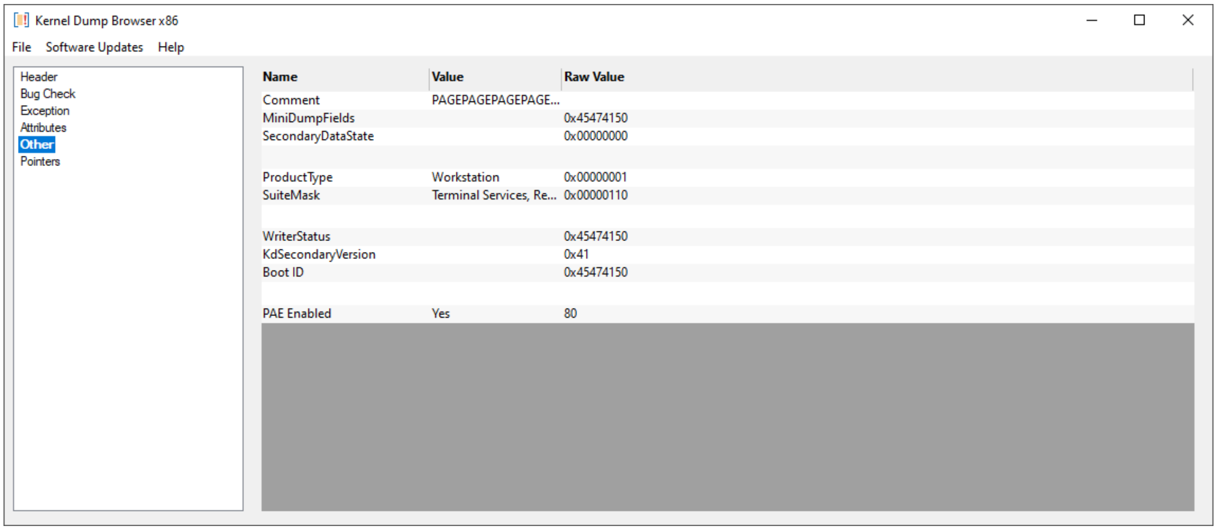
The Attributes page displays the kernel dump attributes.



Name	Value	Raw Value
Hiber Crash	No	
Dump Device Power Off	No	
Insufficient Dump File Size	No	
Kernel Generated Triage Du...	No	
Live Dump Generated Dump	No	
Dump Is Generated Offline	No	
Filter Dump File	No	
Early Boot Crash	No	
Encrypted Dump Data	No	
Decrypted Dump	No	
Reserved Flags		0x00000044
File Attributes	offline virtual	0x00011000

4.1.5 Other

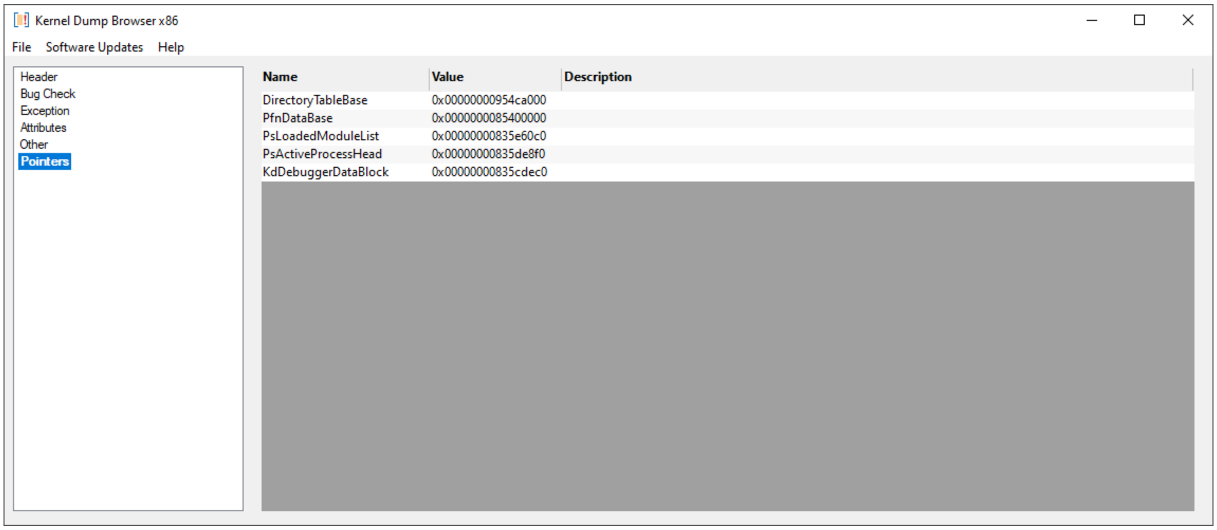
The Header page displays general information about the kernel dump.



Name	Value	Raw Value
Comment	PAGEPAGEPAGEPAGE...	
MiniDumpFields		0x45474150
SecondaryDataState		0x00000000
ProductType	Workstation	0x00000001
SuiteMask	Terminal Services, Re...	0x00000110
WriterStatus		0x45474150
KdSecondaryVersion		0x41
Boot ID		0x45474150
PAE Enabled	Yes	80

4.1.6 Pointers

The Pointers page displays the pointers in the kernel dump.

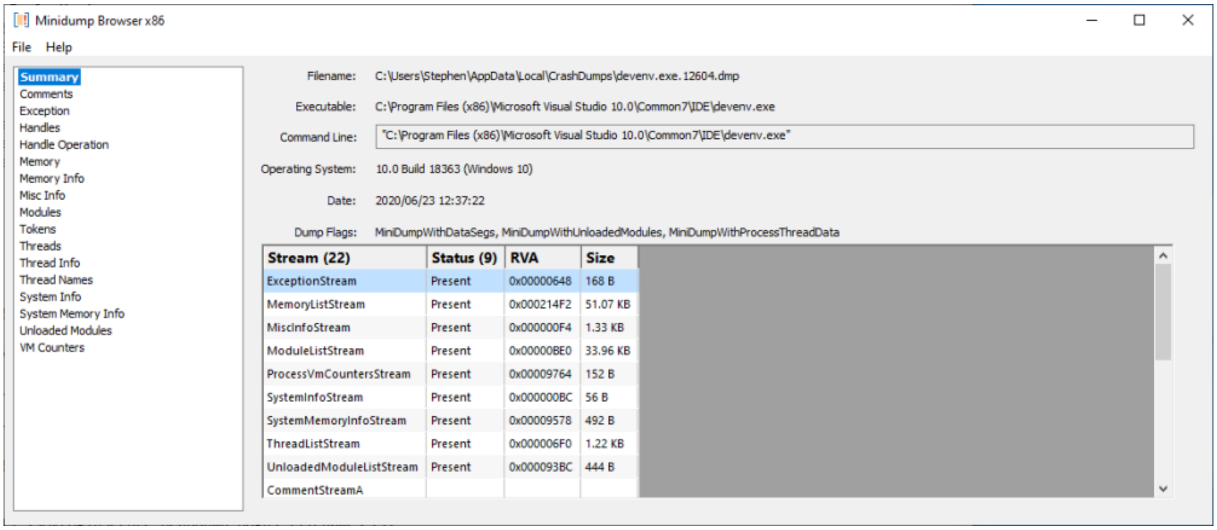


Name	Value	Description
DirectoryTableBase	0x00000000954ca000	
PfnDataBase	0x0000000085400000	
PsLoadedModuleList	0x00000000835e60c0	
PsActiveProcessHead	0x00000000835de8f0	
KdDebuggerDataBlock	0x00000000835cdec0	

4.2 Minidumps

The Minidump Browser user interface is shown below.

When a minidump contains an exception the exception display will be automatically selected as the first display to show you information.



Filename: C:\Users\Stephen\AppData\Local\CrashDumps\devenv.exe.12604.dmp

Executable: C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\devenv.exe

Command Line: "C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\devenv.exe"

Operating System: 10.0 Build 18363 (Windows 10)

Date: 2020/06/23 12:37:22

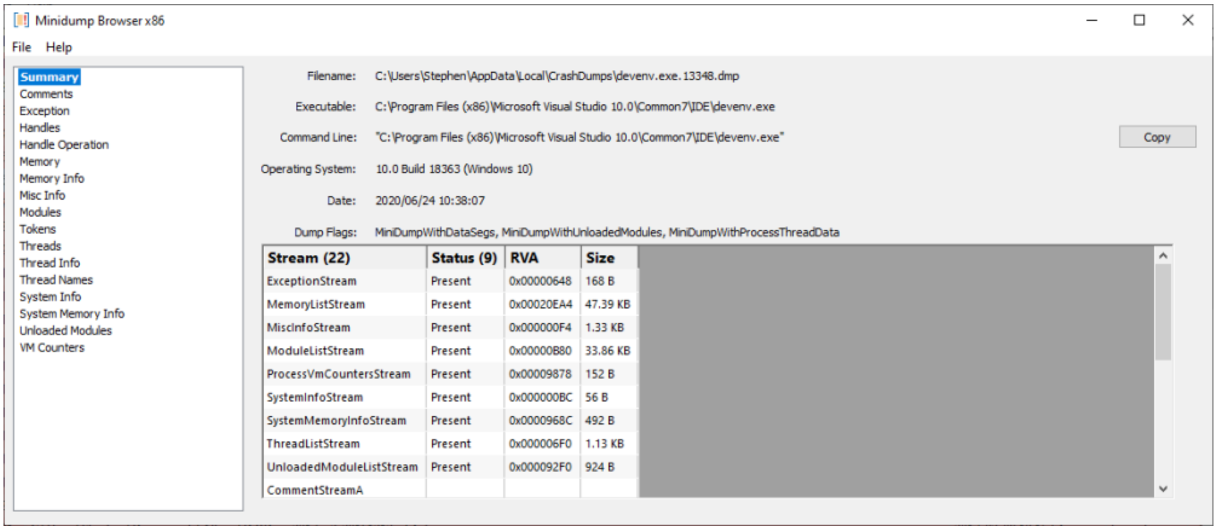
Dump Flags: MiniDumpWithDataSegs, MiniDumpWithUnloadedModules, MiniDumpWithProcessThreadData

Stream (22)	Status (9)	RVA	Size
ExceptionStream	Present	0x00000648	168 B
MemoryListStream	Present	0x000214F2	51.07 KB
MiscInfoStream	Present	0x000000F4	1.33 KB
ModuleListStream	Present	0x00000BE0	33.96 KB
ProcessVmCountersStream	Present	0x00009764	152 B
SystemInfoStream	Present	0x000000BC	56 B
SystemMemoryInfoStream	Present	0x00009578	492 B
ThreadListStream	Present	0x000006F0	1.22 KB
UnloadedModuleListStream	Present	0x000093BC	444 B
CommentStreamA			

The display shows a summary page and then one page per logical group of data in the minidump. This means that some discrete sections in the minidump have been coalesced - for example ThreadListStream and ThreadExListStream are both represented in the Threads page. Each page is listed on the left hand side. Selecting that entry displays the page on the right hand side. The summary page lists each stream so that you can see which streams are present in the minidump and which are absent. Few minidumps (if any) contain all streams.

4.2.1 Summary

The Summary page displays general information about the minidump, plus a list of all possible streams and data about streams that are present.



Filename: C:\Users\Stephen\AppData\Local\CrashDumps\devenv.exe.13348.dmp

Executable: C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\devenv.exe

Command Line: "C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\devenv.exe"

Operating System: 10.0 Build 18363 (Windows 10)

Date: 2020/06/24 10:38:07

Dump Flags: MiniDumpWithDataSegs, MiniDumpWithUnloadedModules, MiniDumpWithProcessThreadData

Stream (22)	Status (9)	RVA	Size
ExceptionStream	Present	0x00000648	168 B
MemoryListStream	Present	0x00020EA4	47.39 KB
MiscInfoStream	Present	0x000000F4	1.33 KB
ModuleListStream	Present	0x00000B80	33.86 KB
ProcessVmCountersStream	Present	0x00009878	152 B
SystemInfoStream	Present	0x000000BC	56 B
SystemMemoryInfoStream	Present	0x0000968C	492 B
ThreadListStream	Present	0x000006F0	1.13 KB
UnloadedModuleListStream	Present	0x000092F0	924 B
CommentStreamA			

For each stream that is listed we indicate if the stream is present, the RVA (the offset from the start of the minidump) to the stream and the size of the stream.

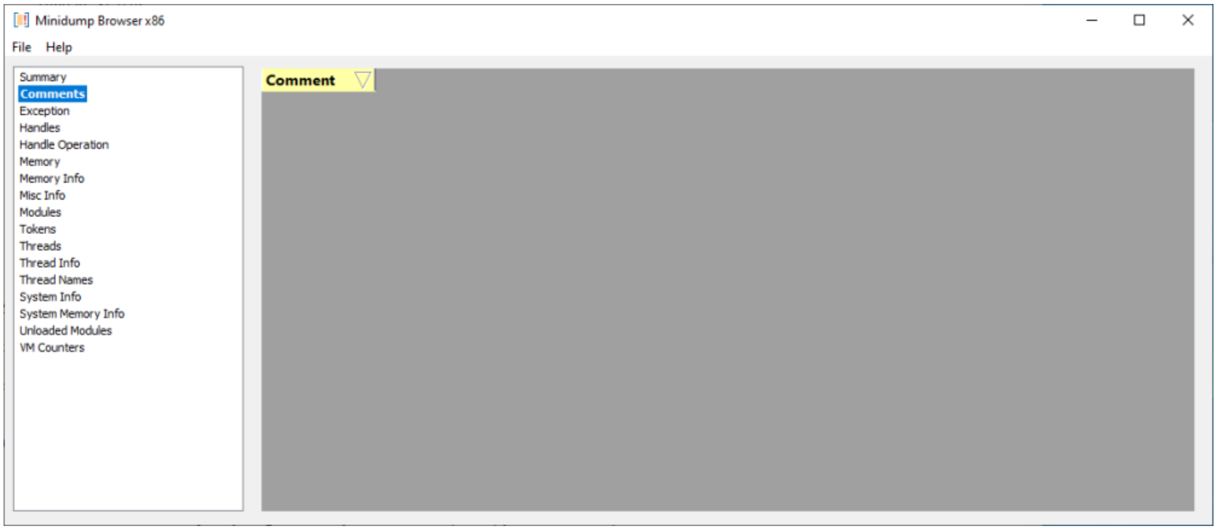
If you want to see the complete command line (for the cases when it's too long to display) use the **Copy** button to copy the command line to the clipboard.

Command Line

To display the command line the minidump must contain Thread Info and memory data. The Thread Info is used to locate the Thread Environment Block, which is then used to locate the Process Environment Block, which is then used to read the command line.

4.2.2 Comments

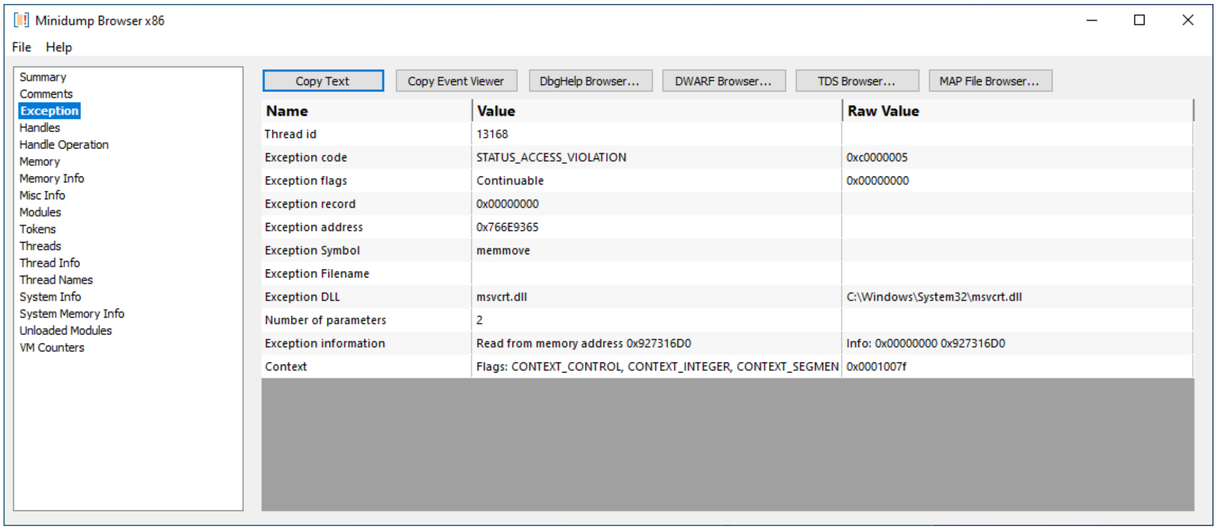
The Comments page displays the contents of the CommentStreamA and CommentStreamW minidump streams.



4.2.3 Exception

The Exception page displays the contents of the ExceptionStream minidump stream.

A few extra fields are displayed to provide additional information: Exception Symbol, Exception Filename, Exception DLL.



Name	Value	Raw Value
Thread id	13168	
Exception code	STATUS_ACCESS_VIOLATION	0xc0000005
Exception flags	Continuable	0x00000000
Exception record	0x00000000	
Exception address	0x766E9365	
Exception Symbol	memmove	
Exception Filename		
Exception DLL	msvcrt.dll	C:\Windows\System32\msvcrt.dll
Number of parameters	2	
Exception information	Read from memory address 0x927316D0	Info: 0x00000000 0x927316D0
Context	Flags: CONTEXT_CONTROL, CONTEXT_INTEGER, CONTEXT_SEGMEN	0x0001007f

Copy Text

Copy Text copies the text from the grid to the clipboard.

Each column is separated with a comma. Each line is separated by "\r\n".

Copy Event Viewer

Copy Event Viewer copies the exception data to the clipboard in the same format as the Windows Event Viewer. You can paste this data into some of our other tools (Minidump Browser, MapFile Browser, TDS Browser).

An example of the data is shown below for an Access Violation at 0x0c18459c in devenv.exe.

```
<Event>
  <System>
    <Provider Name="Windows Error Reporting">
  </System>
  <EventData>
    <Data></Data>
    <Data></Data>
    <Data>APPCRASH</Data>
    <Data></Data>
    <Data></Data>
    <Data>C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\devenv.exe</Data>
    <Data></Data>
    <Data></Data>
    <Data></Data>
    <Data></Data>
    <Data></Data>
    <Data>0xc0000005</Data>
    <Data>0x0c18459c</Data>
    <Data></Data>
    <Data></Data>
    <Data>STATUS_ACCESS_VIOLATION</Data>
    <Data>OK</Data>
    <Data></Data>
  </EventData>
</Event>
```

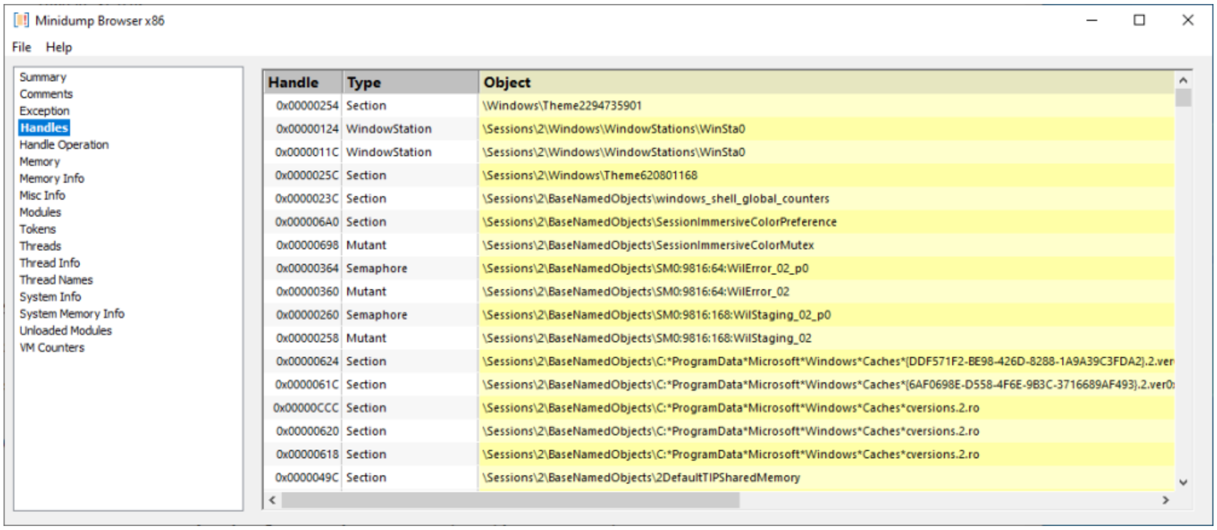
Tools

If you have installed Minidump Browser, DWARF Browser, TDS Browser, MAP File Browser, the appropriate button to launch this tool will be enabled.

Launching the tool will attempt to load the appropriate PDB, DWARF, TDS, MAP data and then locate the symbol that matches the exception crash address.

4.2.4 Handles

The Handles page displays the contents of the HandleDataStream minidump stream.



Handle	Type	Object
0x00000254	Section	\Windows\Theme2294735901
0x00000124	WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
0x0000011C	WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
0x0000025C	Section	\Sessions\2\Windows\Theme620801168
0x0000023C	Section	\Sessions\2\BaseNamedObjects\windows_shell_global_counters
0x000006A0	Section	\Sessions\2\BaseNamedObjects\SessionImmersiveColorPreference
0x00000698	Mutant	\Sessions\2\BaseNamedObjects\SessionImmersiveColorMutex
0x00000364	Semaphore	\Sessions\2\BaseNamedObjects\SM0:9816:64:WilError_02_p0
0x00000360	Mutant	\Sessions\2\BaseNamedObjects\SM0:9816:64:WilError_02
0x00000260	Semaphore	\Sessions\2\BaseNamedObjects\SM0:9816:168:WilStaging_02_p0
0x00000258	Mutant	\Sessions\2\BaseNamedObjects\SM0:9816:168:WilStaging_02
0x00000624	Section	\Sessions\2\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver
0x0000061C	Section	\Sessions\2\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0:
0x00000CCC	Section	\Sessions\2\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
0x00000620	Section	\Sessions\2\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
0x00000618	Section	\Sessions\2\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
0x0000049C	Section	\Sessions\2\BaseNamedObjects\2DefaultTIPSharedMemory

For each handle that is present in the dump the following information is displayed:

Handle
The handle value.

Type
The handle type.

Object
The name of the object referenced by the handle.

Attributes
The attributes of the handle.

Granted Access
Access rights to the handle.

Handle Count
Number of references to the handle.

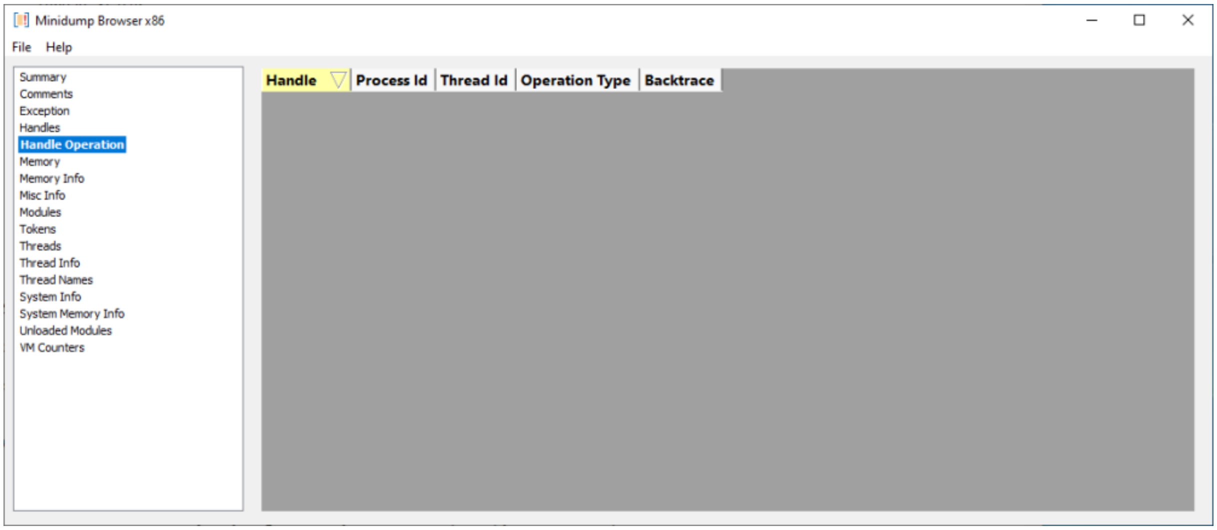
Pointer Count
Object specific count.

Object Info
Extra information about the object.

Reserved0

4.2.5 Handle Operation

The Handle Operation page displays the contents of the HandleOperationListStream minidump stream.



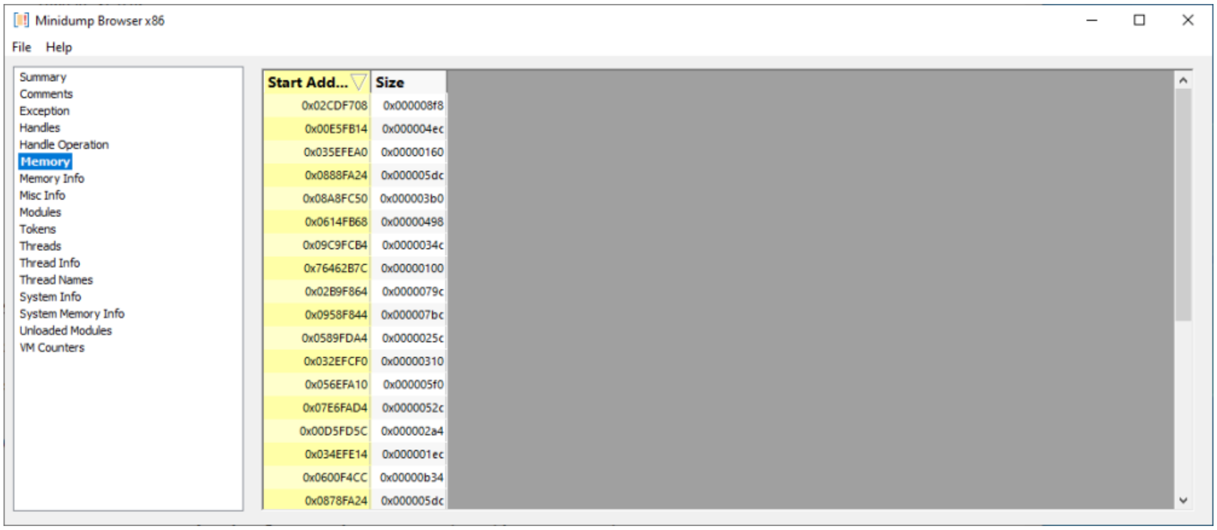
Handle	Process Id	Thread Id	Operation Type	Backtrace

Handle operation information relates to information collected by Application Verifier.

More information here: https://docs.microsoft.com/en-gb/windows/win32/api/minidumpapiset/ns-minidumpapiset-minidump_handle_operation_list

4.2.6 Memory

The Memory page displays the contents of the MemoryListStream and the Memory64ListStream minidump streams.

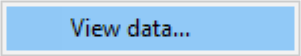


Start Add...	Size
0x02CDF708	0x000008f8
0x00E5FB14	0x000004ec
0x035EFEA0	0x00000160
0x0888FA24	0x000005dc
0x08A8FC50	0x000003b0
0x0614FB68	0x00000498
0x09C9FCB4	0x0000034c
0x76462B7C	0x00000100
0x02B9F864	0x0000079c
0x0958F844	0x000007bc
0x0589FDA4	0x0000025c
0x032EFCF0	0x00000310
0x056EFA10	0x000005f0
0x07E6FAD4	0x0000052c
0x00D5FD5C	0x000002a4
0x034EFE14	0x000001ec
0x0600F4CC	0x00000b34
0x0878FA24	0x000005dc

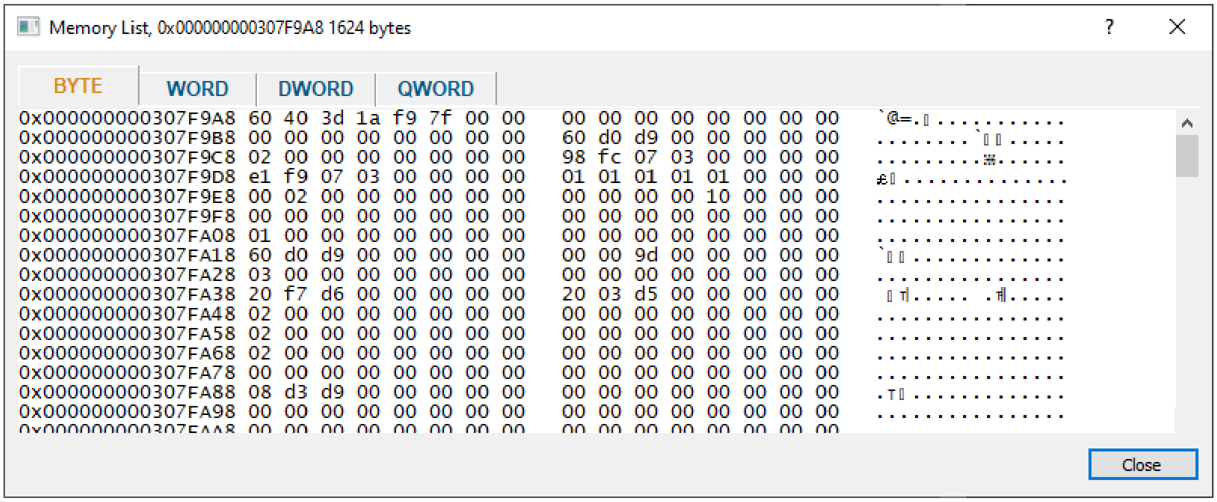
The information presented here is a list of memory start addresses and the size of the memory at that address.

Context Menu

A context menu provides a single option:



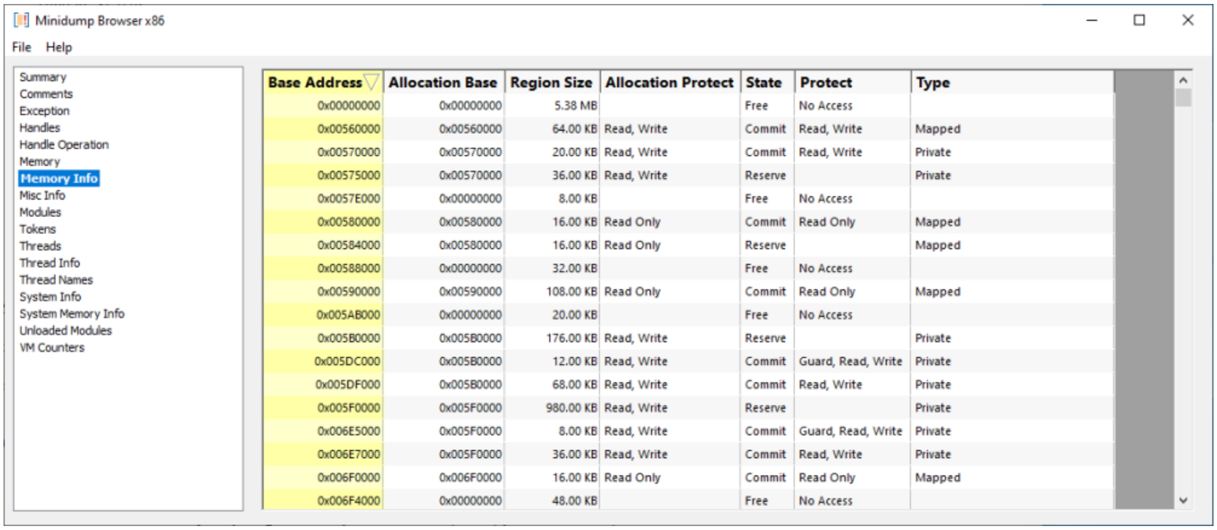
Clicking **View data...** opens a memory inspection dialog, allowing you to view the memory as BYTEs, WORDs, DWORDs or QWORDs. For executable code a disassembly view is provided.



```
0x000000000307F9A8 60 40 3d 1a f9 7f 00 00   00 00 00 00 00 00 00 00   `@=.▯...........
0x000000000307F9B8 00 00 00 00 00 00 00 00   60 d0 d9 00 00 00 00 00   ........`▯▯.....
0x000000000307F9C8 02 00 00 00 00 00 00 00   98 fc 07 03 00 00 00 00   .........▯......
0x000000000307F9D8 e1 f9 07 03 00 00 00 00   01 01 01 01 01 00 00 00   £▯..............
0x000000000307F9E8 00 02 00 00 00 00 00 00   00 00 00 00 10 00 00 00   ................
0x000000000307F9F8 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA08 01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA18 60 d0 d9 00 00 00 00 00   00 00 9d 00 00 00 00 00   `▯▯.............
0x000000000307FA28 03 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA38 20 f7 d6 00 00 00 00 00   20 03 d5 00 00 00 00 00    ▯╥.....  .╫.....
0x000000000307FA48 02 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA58 02 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA68 02 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA78 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FA88 08 d3 d9 00 00 00 00 00   00 00 00 00 00 00 00 00   .╙▯.............
0x000000000307FA98 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
0x000000000307FAA8 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
```

4.2.7 Memory Info

The Memory Info page displays the contents of the MemoryInfoListStream minidump stream.



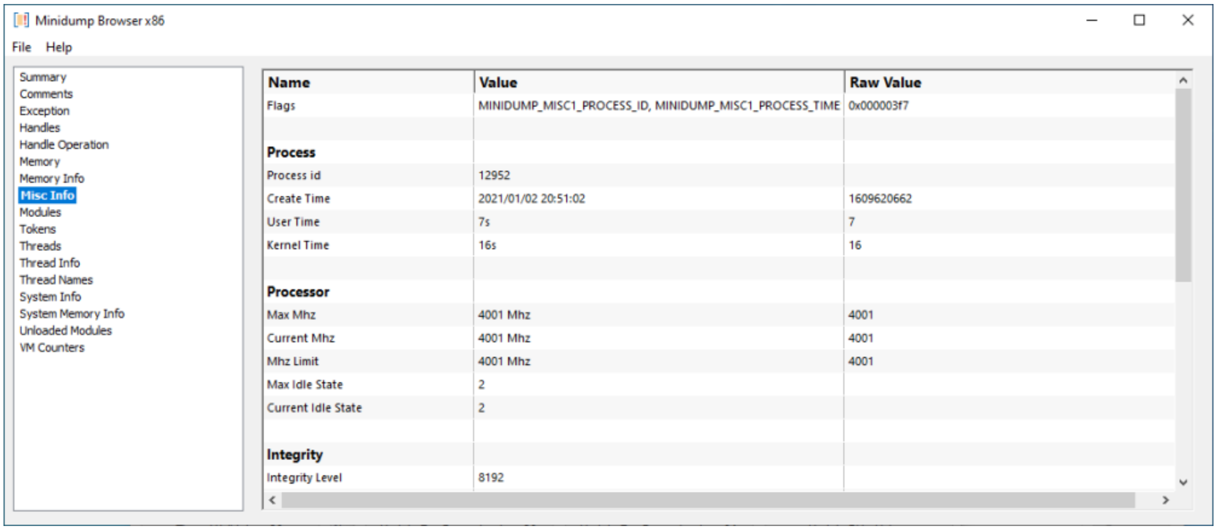
Base Address	Allocation Base	Region Size	Allocation Protect	State	Protect	Type
0x00000000	0x00000000	5.38 MB		Free	No Access	
0x00560000	0x00560000	64.00 KB	Read, Write	Commit	Read, Write	Mapped
0x00570000	0x00570000	20.00 KB	Read, Write	Commit	Read, Write	Private
0x00575000	0x00570000	36.00 KB	Read, Write	Reserve		Private
0x0057E000	0x00000000	8.00 KB		Free	No Access	
0x00580000	0x00580000	16.00 KB	Read Only	Commit	Read Only	Mapped
0x00584000	0x00580000	16.00 KB	Read Only	Reserve		Mapped
0x00588000	0x00000000	32.00 KB		Free	No Access	
0x00590000	0x00590000	108.00 KB	Read Only	Commit	Read Only	Mapped
0x005AB000	0x00000000	20.00 KB		Free	No Access	
0x005B0000	0x005B0000	176.00 KB	Read, Write	Reserve		Private
0x005DC000	0x005B0000	12.00 KB	Read, Write	Commit	Guard, Read, Write	Private
0x005DF000	0x005B0000	68.00 KB	Read, Write	Commit	Read, Write	Private
0x005F0000	0x005F0000	980.00 KB	Read, Write	Reserve		Private
0x006E5000	0x005F0000	8.00 KB	Read, Write	Commit	Guard, Read, Write	Private
0x006E7000	0x005F0000	36.00 KB	Read, Write	Commit	Read, Write	Private
0x006F0000	0x006F0000	16.00 KB	Read Only	Commit	Read Only	Mapped
0x006F4000	0x00000000	48.00 KB		Free	No Access	

The information here allows you to inspect the memory protection status of areas of memory in the minidump.

If you'd like to view this information in graphical form you can also use VM Validator. VM Validator views memory data in live processes and minidumps.

4.2.8 Misc Info

The Misc Info page displays the contents of the MiscInfoStream minidump stream.

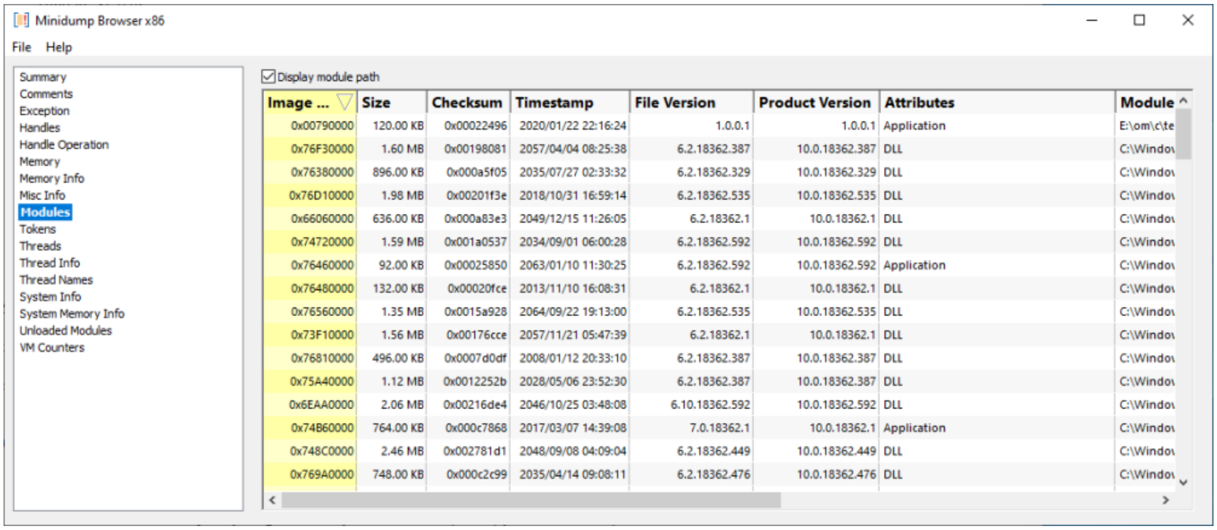


Name	Value	Raw Value
Flags	MINIDUMP_MISC1_PROCESS_ID, MINIDUMP_MISC1_PROCESS_TIME	0x000003f7
Process		
Process id	12952	
Create Time	2021/01/02 20:51:02	1609620662
User Time	7s	7
Kernel Time	16s	16
Processor		
Max Mhz	4001 Mhz	4001
Current Mhz	4001 Mhz	4001
Mhz Limit	4001 Mhz	4001
Max Idle State	2	
Current Idle State	2	
Integrity		
Integrity Level	8192	

This section provides miscellaneous information about the minidump application.

4.2.9 Modules

The Modules page displays the contents of the ModuleListStream minidump stream.



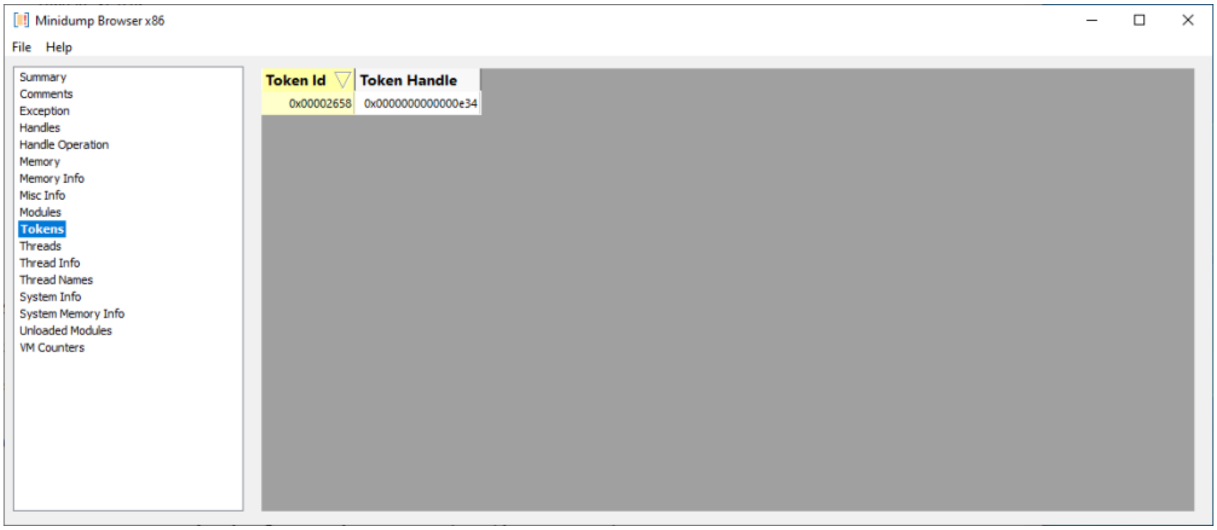
☑ Display module path

Image ...	Size	Checksum	Timestamp	File Version	Product Version	Attributes	Module
0x00790000	120.00 KB	0x00022496	2020/01/22 22:16:24	1.0.0.1	1.0.0.1	Application	E:\om\c\te
0x76F30000	1.60 MB	0x00198081	2057/04/04 08:25:38	6.2.18362.387	10.0.18362.387	DLL	C:\Windo
0x76380000	896.00 KB	0x000a5f05	2035/07/27 02:33:32	6.2.18362.329	10.0.18362.329	DLL	C:\Windo
0x76D10000	1.98 MB	0x00201f3e	2018/10/31 16:59:14	6.2.18362.535	10.0.18362.535	DLL	C:\Windo
0x66060000	636.00 KB	0x000a83e3	2049/12/15 11:26:05	6.2.18362.1	10.0.18362.1	DLL	C:\Windo
0x74720000	1.59 MB	0x001a0537	2034/09/01 06:00:28	6.2.18362.592	10.0.18362.592	DLL	C:\Windo
0x76460000	92.00 KB	0x00025850	2063/01/10 11:30:25	6.2.18362.592	10.0.18362.592	Application	C:\Windo
0x76480000	132.00 KB	0x00020fce	2013/11/10 16:08:31	6.2.18362.1	10.0.18362.1	DLL	C:\Windo
0x76560000	1.35 MB	0x0015a928	2064/09/22 19:13:00	6.2.18362.535	10.0.18362.535	DLL	C:\Windo
0x73F10000	1.56 MB	0x00176cce	2057/11/21 05:47:39	6.2.18362.1	10.0.18362.1	DLL	C:\Windo
0x76810000	496.00 KB	0x0007d0df	2008/01/12 20:33:10	6.2.18362.387	10.0.18362.387	DLL	C:\Windo
0x75A40000	1.12 MB	0x0012252b	2028/05/06 23:52:30	6.2.18362.387	10.0.18362.387	DLL	C:\Windo
0x6EAA0000	2.06 MB	0x00216de4	2046/10/25 03:48:08	6.10.18362.592	10.0.18362.592	DLL	C:\Windo
0x74B60000	764.00 KB	0x000c7868	2017/03/07 14:39:08	7.0.18362.1	10.0.18362.1	Application	C:\Windo
0x748C0000	2.46 MB	0x002781d1	2048/09/08 04:09:04	6.2.18362.449	10.0.18362.449	DLL	C:\Windo
0x769A0000	748.00 KB	0x000c2c99	2035/04/14 09:08:11	6.2.18362.476	10.0.18362.476	DLL	C:\Windo

For each module in the minidump this page displays the following information, dll load address (image base), size, checksum, timestamp, file version, product version, application attributes and module name (with optional path).

4.2.10 Tokens

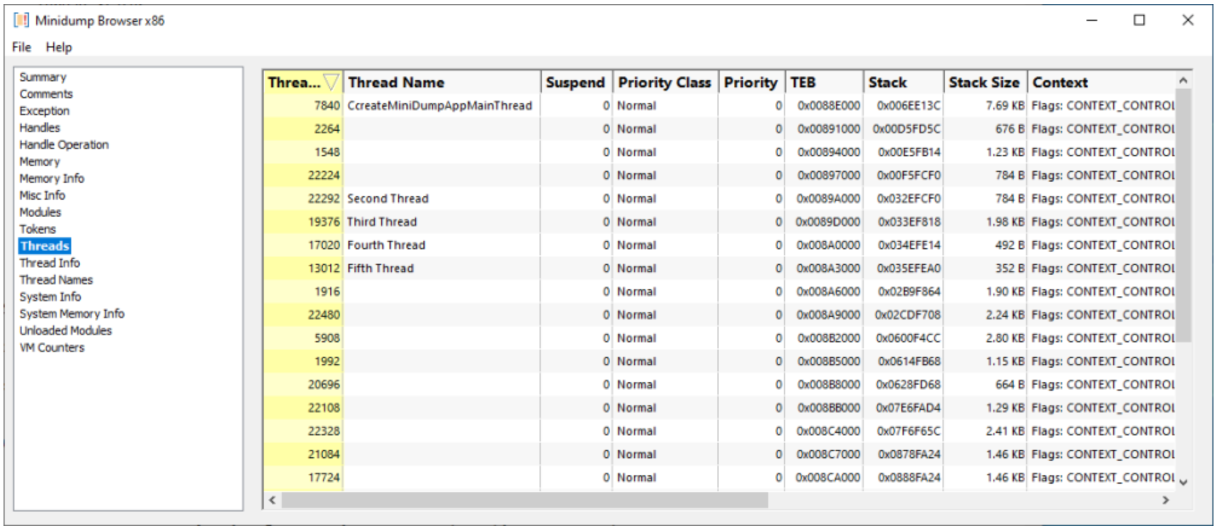
The Tokens page displays the contents of the TokenStream minidump stream.



Token Id	Token Handle
0x00002658	0x0000000000000e34

4.2.11 Threads

The Threads page displays the contents of the ThreadListStream and ThreadExListStream minidump streams.

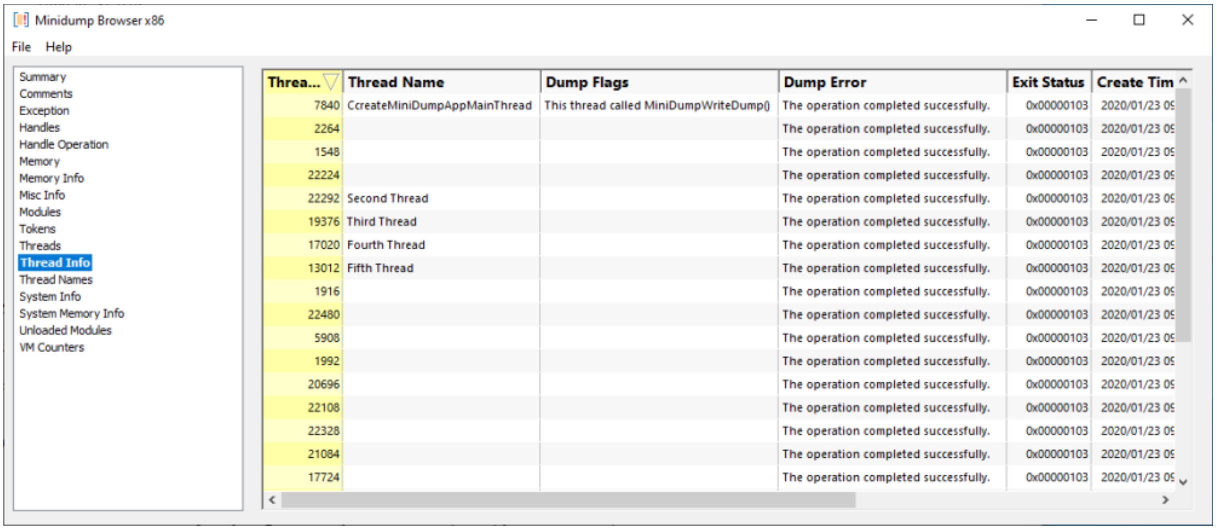


Threa...	Thread Name	Suspend	Priority Class	Priority	TEB	Stack	Stack Size	Context
7840	CcreateMiniDumpAppMainThread	0	Normal	0	0x0088E000	0x006EE13C	7.69 KB	Flags: CONTEXT_CONTROL
2264		0	Normal	0	0x00891000	0x00D5FD5C	676 B	Flags: CONTEXT_CONTROL
1548		0	Normal	0	0x00894000	0x00E5FB14	1.23 KB	Flags: CONTEXT_CONTROL
22224		0	Normal	0	0x00897000	0x00F5FCF0	784 B	Flags: CONTEXT_CONTROL
22292	Second Thread	0	Normal	0	0x0089A000	0x032EFCF0	784 B	Flags: CONTEXT_CONTROL
19376	Third Thread	0	Normal	0	0x0089D000	0x033EF818	1.98 KB	Flags: CONTEXT_CONTROL
17020	Fourth Thread	0	Normal	0	0x008A0000	0x034EFE14	492 B	Flags: CONTEXT_CONTROL
13012	Fifth Thread	0	Normal	0	0x008A3000	0x035EFEA0	352 B	Flags: CONTEXT_CONTROL
1916		0	Normal	0	0x008A6000	0x02B9F864	1.90 KB	Flags: CONTEXT_CONTROL
22480		0	Normal	0	0x008A9000	0x02CDF708	2.24 KB	Flags: CONTEXT_CONTROL
5908		0	Normal	0	0x008B2000	0x0600F4CC	2.80 KB	Flags: CONTEXT_CONTROL
1992		0	Normal	0	0x008B5000	0x0614FB68	1.15 KB	Flags: CONTEXT_CONTROL
20696		0	Normal	0	0x008B8000	0x0628FD68	664 B	Flags: CONTEXT_CONTROL
22108		0	Normal	0	0x008BB000	0x07E6FAD4	1.29 KB	Flags: CONTEXT_CONTROL
22328		0	Normal	0	0x008C4000	0x07F6F65C	2.41 KB	Flags: CONTEXT_CONTROL
21084		0	Normal	0	0x008C7000	0x0878FA24	1.46 KB	Flags: CONTEXT_CONTROL
17724		0	Normal	0	0x008CA000	0x0888FA24	1.46 KB	Flags: CONTEXT_CONTROL

For each thread the following information is displayed: thread id, thread name, if the thread is suspended, it's priority class, it's priority level, the thread environment block (TEB) address, the stack location and size and the flags used to create the thread context, plus a dump of some thread context members (processor registers etc).

4.2.12 Thread Info

The Thread Info page displays the contents of the ThreadInfoListStream minidump stream.

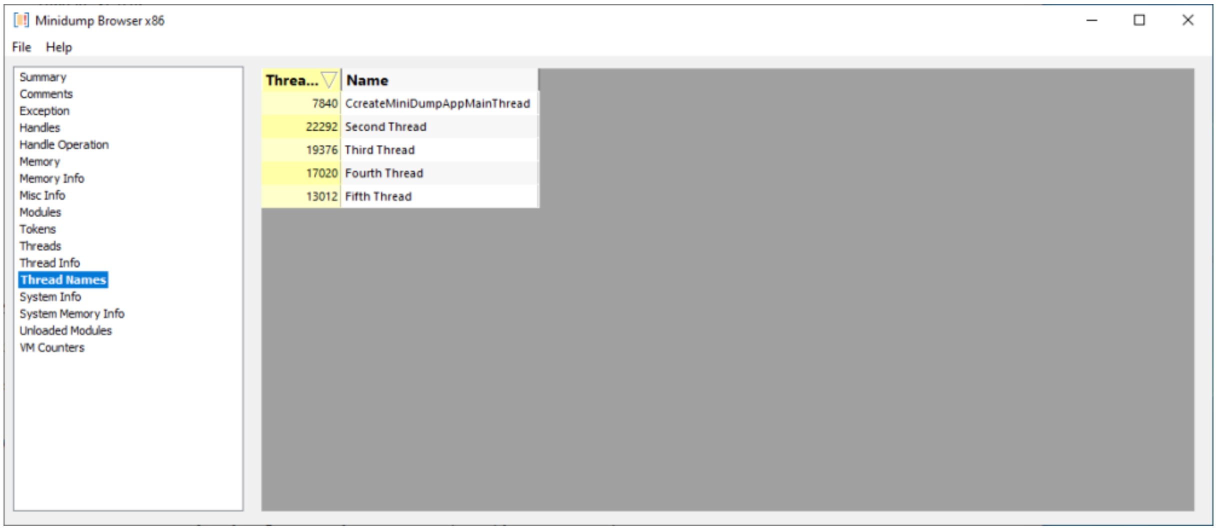


Threa...	Thread Name	Dump Flags	Dump Error	Exit Status	Create Tim
7840	CcreateMiniDumpAppMainThread	This thread called MiniDumpWriteDump()	The operation completed successfully.	0x00000103	2020/01/23 0
2264			The operation completed successfully.	0x00000103	2020/01/23 0
1548			The operation completed successfully.	0x00000103	2020/01/23 0
22224			The operation completed successfully.	0x00000103	2020/01/23 0
22292	Second Thread		The operation completed successfully.	0x00000103	2020/01/23 0
19376	Third Thread		The operation completed successfully.	0x00000103	2020/01/23 0
17020	Fourth Thread		The operation completed successfully.	0x00000103	2020/01/23 0
13012	Fifth Thread		The operation completed successfully.	0x00000103	2020/01/23 0
1916			The operation completed successfully.	0x00000103	2020/01/23 0
22480			The operation completed successfully.	0x00000103	2020/01/23 0
5908			The operation completed successfully.	0x00000103	2020/01/23 0
1992			The operation completed successfully.	0x00000103	2020/01/23 0
20696			The operation completed successfully.	0x00000103	2020/01/23 0
22108			The operation completed successfully.	0x00000103	2020/01/23 0
22328			The operation completed successfully.	0x00000103	2020/01/23 0
21084			The operation completed successfully.	0x00000103	2020/01/23 0
17724			The operation completed successfully.	0x00000103	2020/01/23 0

For each thread the following information is displayed: thread id, thread name, dump flags, dump error status, thread exit status, thread creation time, exit time, kernel time, user time, thread start address and thread processor affinity.

4.2.13 Thread Names

The Thread Names page displays the contents of the ThreadNamesStream minidump stream.

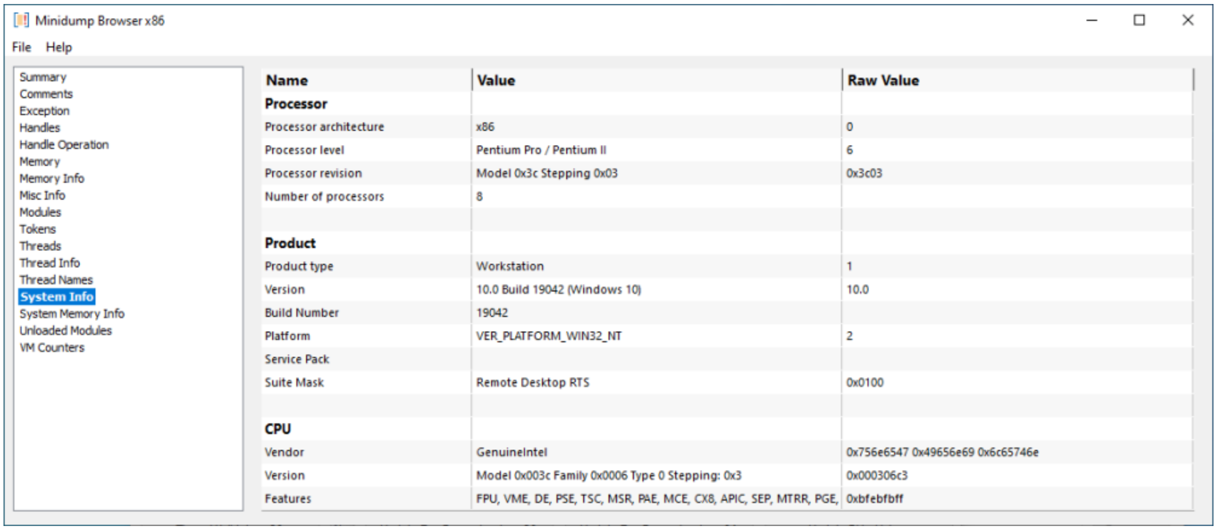


Threa...	Name
7840	CcreateMiniDumpAppMainThread
22292	Second Thread
19376	Third Thread
17020	Fourth Thread
13012	Fifth Thread

For each thread the thread id and thread name is listed. We use this information to provide thread names on appropriate other minidump displays.

4.2.14 System Info

The System Info page displays the contents of the SystemInfoStream minidump stream.

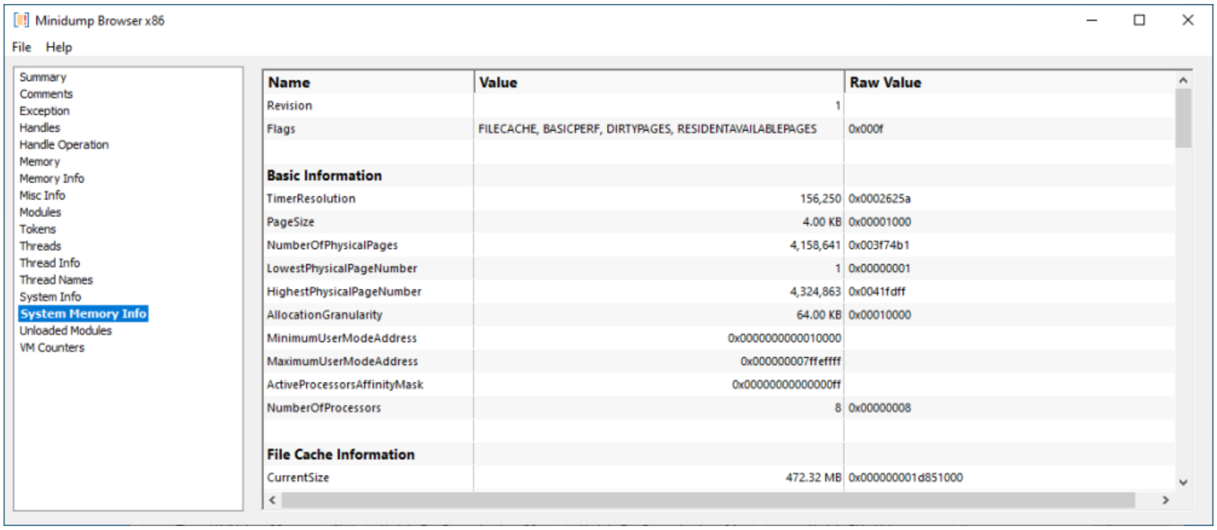


Name	Value	Raw Value
Processor		
Processor architecture	x86	0
Processor level	Pentium Pro / Pentium II	6
Processor revision	Model 0x3c Stepping 0x03	0x3c03
Number of processors	8	
Product		
Product type	Workstation	1
Version	10.0 Build 19042 (Windows 10)	10.0
Build Number	19042	
Platform	VER_PLATFORM_WIN32_NT	2
Service Pack		
Suite Mask	Remote Desktop RTS	0x0100
CPU		
Vendor	GenuineIntel	0x756e6547 0x49656e69 0x6c65746e
Version	Model 0x003c Family 0x0006 Type 0 Stepping: 0x3	0x000306c3
Features	FPU, VME, DE, PSE, TSC, MSR, PAE, MCE, CX8, APIC, SEP, MTRR, PGE,	0xbfebfbff

This page provides information about the computer hardware and the operating system you are using.

4.2.15 System Memory Info

The System Memory Info page displays the contents of the SystemMemoryInfoStream minidump stream.

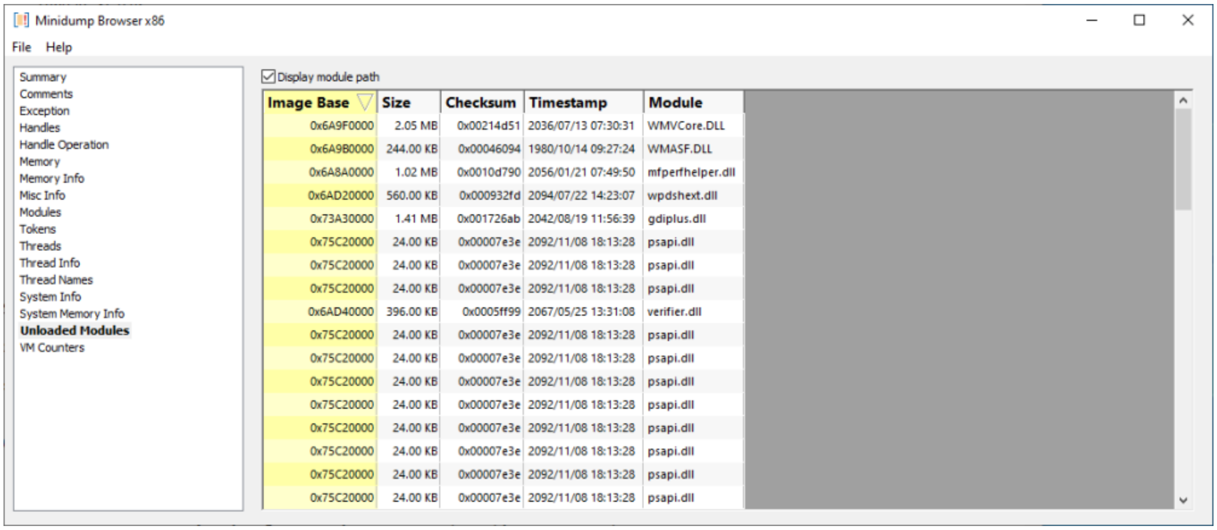


Name	Value	Raw Value
Revision	1	
Flags	FILECACHE, BASICPERF, DIRTYPAGES, RESIDENTAVAILABLEPAGES	0x000f
Basic Information		
TimerResolution	156,250	0x0002625a
PageSize	4.00 KB	0x00001000
NumberOfPhysicalPages	4,158,641	0x003f74b1
LowestPhysicalPageNumber	1	0x00000001
HighestPhysicalPageNumber	4,324,863	0x0041fdff
AllocationGranularity	64.00 KB	0x00010000
MinimumUserModeAddress	0x0000000000010000	
MaximumUserModeAddress	0x000000007ffeffff	
ActiveProcessorsAffinityMask	0x00000000000000ff	
NumberOfProcessors	8	0x00000008
File Cache Information		
CurrentSize	472.32 MB	0x000000001d851000

This page provides detailed information about the memory state of the system.

4.2.16 Unloaded Modules

The Unloaded Modules page displays the contents of the UnloadedModuleListStream minidump stream.



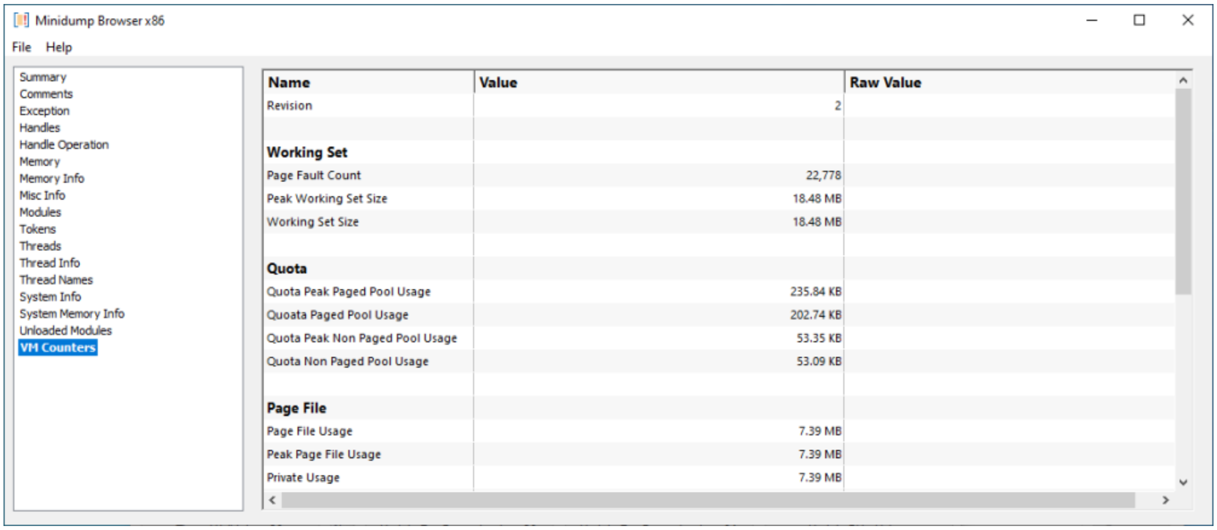
☑ Display module path

Image Base	Size	Checksum	Timestamp	Module
0x6A9F0000	2.05 MB	0x00214d51	2036/07/13 07:30:31	WMVCore.DLL
0x6A9B0000	244.00 KB	0x00046094	1980/10/14 09:27:24	WMASF.DLL
0x6A8A0000	1.02 MB	0x0010d790	2056/01/21 07:49:50	mfperfhelper.dll
0x6AD20000	560.00 KB	0x000932fd	2094/07/22 14:23:07	wpdshext.dll
0x73A30000	1.41 MB	0x001726ab	2042/08/19 11:56:39	gdiplus.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x6AD40000	396.00 KB	0x0005ff99	2067/05/25 13:31:08	verifier.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll
0x75C20000	24.00 KB	0x00007e3e	2092/11/08 18:13:28	psapi.dll

For each module in the minidump that has been unloaded this page displays the following information, dll load address (image base), size, checksum, timestamp, module name (with optional path).

4.2.17 VM Counters

The VM Counters page displays the contents of the ProcessVmCountersStream minidump stream.

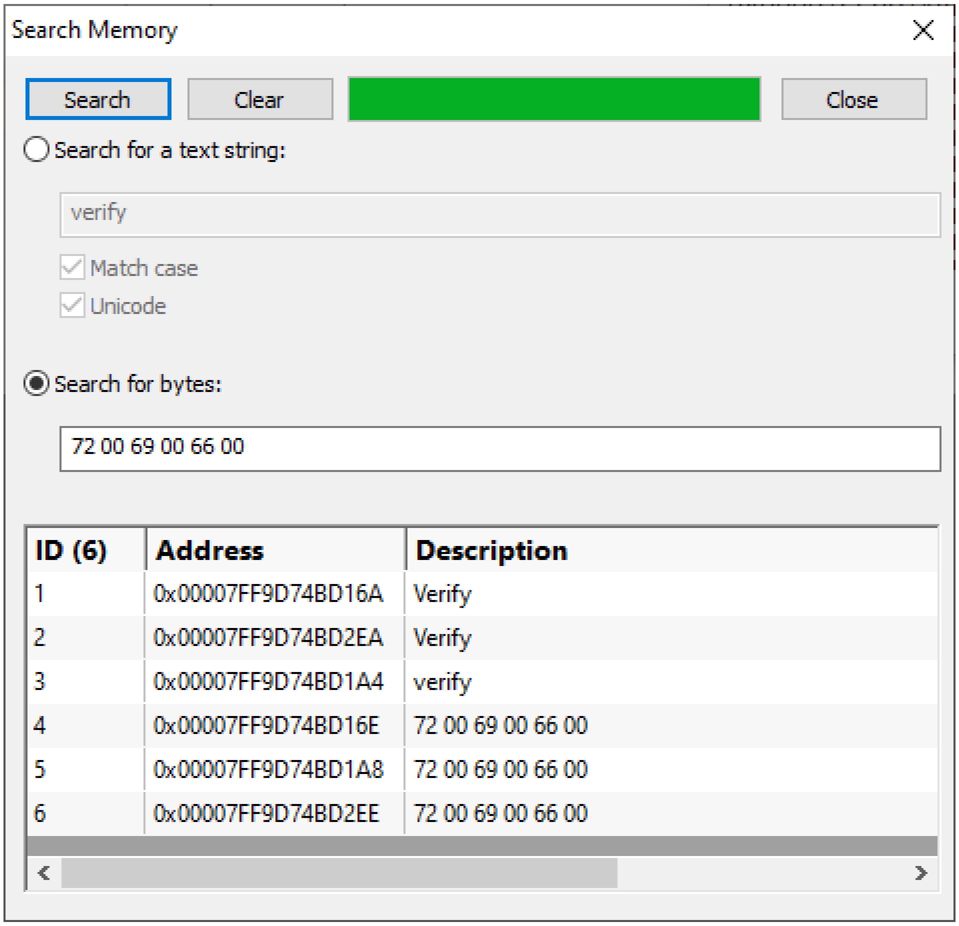


Name	Value	Raw Value
Revision	2	
Working Set		
Page Fault Count	22,778	
Peak Working Set Size	18.48 MB	
Working Set Size	18.48 MB	
Quota		
Quota Peak Paged Pool Usage	235.84 KB	
Quoata Paged Pool Usage	202.74 KB	
Quota Peak Non Paged Pool Usage	53.35 KB	
Quota Non Paged Pool Usage	53.09 KB	
Page File		
Page File Usage	7.39 MB	
Peak Page File Usage	7.39 MB	
Private Usage	7.39 MB	

This page provides detailed information about the virtual memory counters of the system.

4.3 Search Memory Dialog

The Search Memory dialog is shown below.



○ Search for a text string:

verify

☑ Match case

☑ Unicode

● Search for bytes:

72 00 69 00 66 00

ID (6)	Address	Description
1	0x00007FF9D74BD16A	Verify
2	0x00007FF9D74BD2EA	Verify
3	0x00007FF9D74BD1A4	verify
4	0x00007FF9D74BD16E	72 00 69 00 66 00
5	0x00007FF9D74BD1A8	72 00 69 00 66 00
6	0x00007FF9D74BD2EE	72 00 69 00 66 00

You can search for text strings or you can search for byte sequences.

Search for a text string › type the string you wish to search for into the text box

Match case › select the check box if the string match should be case sensitive

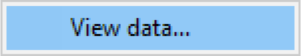
Unicode › select the check box if the string match should be Unicode. If the check box is not selected the string match is ANSI

Search for bytes › type the bytes you wish to search for into the text box. A byte should be specified as a two digit hex value. Separate bytes with spaces

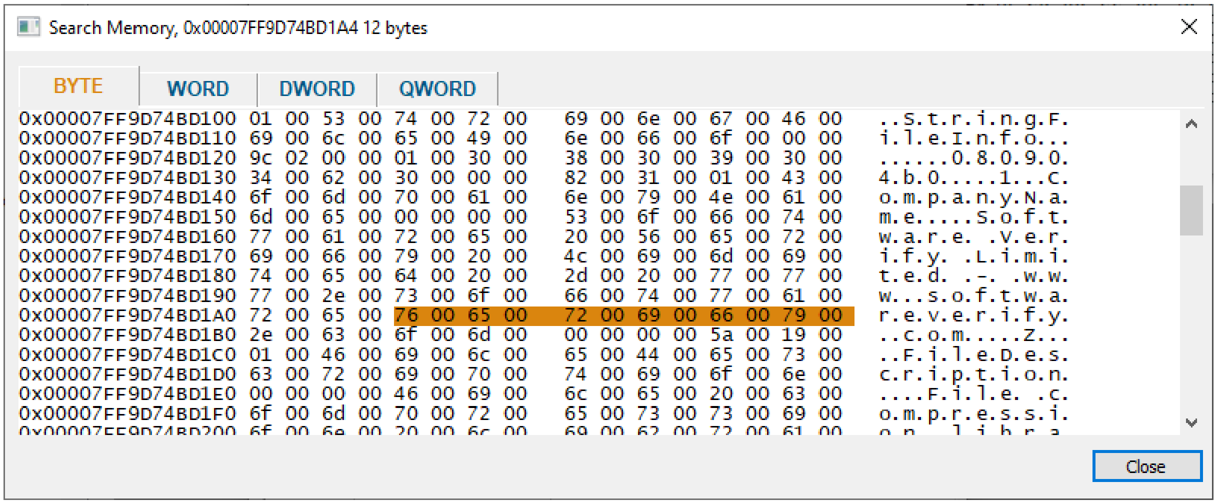
Search › perform the search. The progress of the search is shown on the progress bar, any matching search results are shown in the list.

Clear › clear the search results

A context menu on the search results provides a single option:



Clicking **View data...** opens a memory inspection dialog, allowing you to view the search results memory as BYTEs, WORDs, DWORDs or QWORDs.



```
0x00007FF9D74BD100 01 00 53 00 74 00 72 00   69 00 6e 00 67 00 46 00   ..S.t.r.i.n.g.F.
0x00007FF9D74BD110 69 00 6c 00 65 00 49 00   6e 00 66 00 6f 00 00 00   i.l.e.I.n.f.o...
0x00007FF9D74BD120 9c 02 00 00 01 00 30 00   38 00 30 00 39 00 30 00   ......0.8.0.9.0.
0x00007FF9D74BD130 34 00 62 00 30 00 00 00   82 00 31 00 01 00 43 00   4.b.0.....1...C.
0x00007FF9D74BD140 6f 00 6d 00 70 00 61 00   6e 00 79 00 4e 00 61 00   o.m.p.a.n.y.N.a.
0x00007FF9D74BD150 6d 00 65 00 00 00 00 00   53 00 6f 00 66 00 74 00   m.e.....S.o.f.t.
0x00007FF9D74BD160 77 00 61 00 72 00 65 00   20 00 56 00 65 00 72 00   w.a.r.e. .V.e.r.
0x00007FF9D74BD170 69 00 66 00 79 00 20 00   4c 00 69 00 6d 00 69 00   i.f.y. .L.i.m.i.
0x00007FF9D74BD180 74 00 65 00 64 00 20 00   2d 00 20 00 77 00 77 00   t.e.d. .-. .w.w.
0x00007FF9D74BD190 77 00 2e 00 73 00 6f 00   66 00 74 00 77 00 61 00   w...s.o.f.t.w.a.
0x00007FF9D74BD1A0 72 00 65 00 76 00 65 00   72 00 69 00 66 00 79 00   r.e.v.e.r.i.f.y.
0x00007FF9D74BD1B0 2e 00 63 00 6f 00 6d 00   00 00 00 00 5a 00 19 00   ..c.o.m.....Z...
0x00007FF9D74BD1C0 01 00 46 00 69 00 6c 00   65 00 44 00 65 00 73 00   ..F.i.l.e.D.e.s.
0x00007FF9D74BD1D0 63 00 72 00 69 00 70 00   74 00 69 00 6f 00 6e 00   c.r.i.p.t.i.o.n.
0x00007FF9D74BD1E0 00 00 00 00 46 00 69 00   6c 00 65 00 20 00 63 00   ....F.i.l.e. .c.
0x00007FF9D74BD1F0 6f 00 6d 00 70 00 72 00   65 00 73 00 73 00 69 00   o.m.p.r.e.s.s.i.
0x00007FF9D74BD200 6f 00 6e 00 20 00 6c 00   69 00 62 00 72 00 61 00   o.n. .l.i.b.r.a.
```