Minidump Browser

by

Software Verify

Copyright Software Verify Limited (c) 2020 - 2021

softwareverify

Smarter tools for better software

Minidump Browser

Easily inspect Minidump contents.

by Software Verify

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

Copyright © 2020-2021 Software Verify Limited

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

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 2021 in United Kingdom.

Table of Contents

Foreword 1

Part I How to get Minidump Browser 2

Part II What does Minidump Browser do? 4

Part III Menu 6

1 File ... 7
2 Help ... 7

Part IV The user interface 9

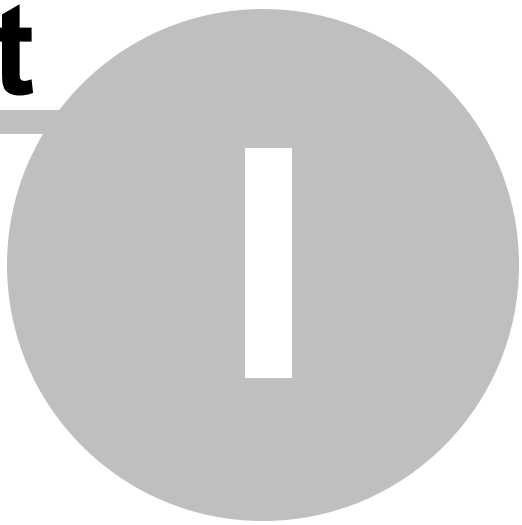
1 Summary ... 10
2 Comments ... 11
3 Exception ... 12
4 Handles ... 13
5 Handle Operation ... 14
6 Memory ... 15
7 Memory Info ... 16
8 Misc Info ... 16
9 Modules ... 17
10 Tokens ... 18
11 Threads ... 18
12 Thread Info ... 19
13 Thread Names ... 19
14 System Info ... 20
15 System Memory Info ... 21
16 Unloaded Modules ... 21
17 VM Counters ... 22

Index 0

Copyright © 2020-2021 Software Verify Limited

Copyright © 2020-2021 Software Verify Limited

Part



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.

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 Software Verify at:

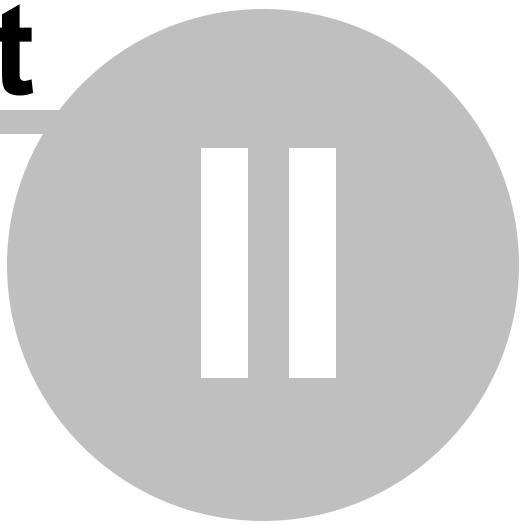
Software Verify Limited
Suffolk Business Park
Eldo House
Kempson Way
Bury Saint Edmunds
IP32 7AR
United Kingdom

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.

Copyright © 2020-2021 Software Verify Limited

Part



2 What does Minidump Browser do?

Minidump Browser allows you to manage and identify minidumps on your machine, or your network.

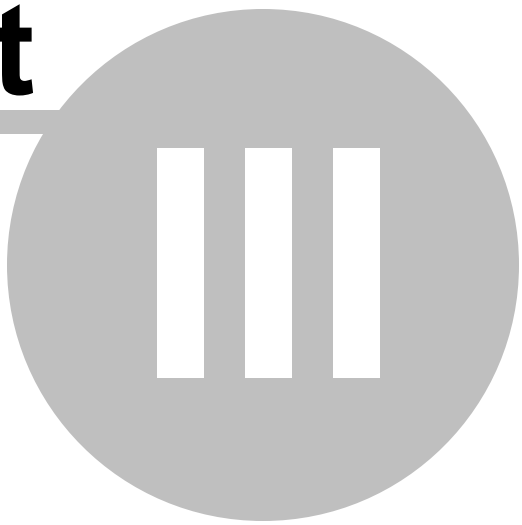
Options are provided for advanced filtering of minidumps and to launch debuggers and minidump visualisation tools.

32 bit and 64 bit

32 bit and 64 bit miniDumps are supported.

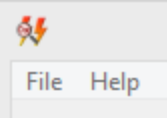
Copyright © 2020-2021 Software Verify Limited

Part



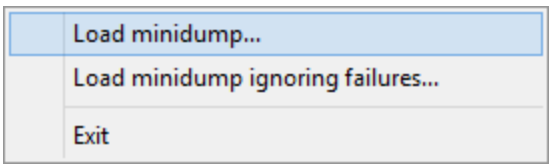
3 Menu

The main menu contains two menus, File, and Help.



3.1 File

The File menu controls the scanning and display of minidumps.



File > Load minidump...
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. This means that mindumps from ARM, IA64 and other architectures can't be displayed.

File > 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.

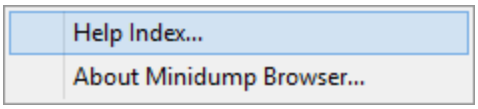
If any errors occur when trying to load the minidump, the load fails to load just the failing part of the minidump and continues with other parts of the minidump.
This means that mindumps from ARM, IA64 and other architectures can be displayed, but may have incomplete information.

File > Exit
Closes Minidump Browser.

3.2 Help

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

Copyright © 2020-2021 Software Verify Limited



Help > Help Index...
Displays this help file.

Help > About Minidump Browser...
Displays information about Minidump Browser.

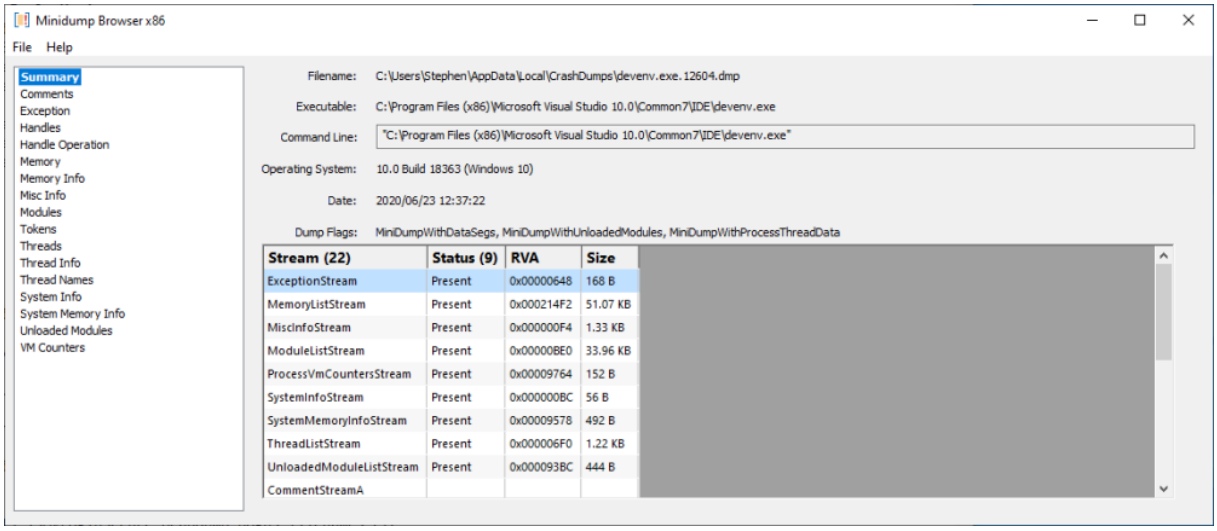
Copyright © 2020-2021 Software Verify Limited

Part IV

4 The user interface

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.

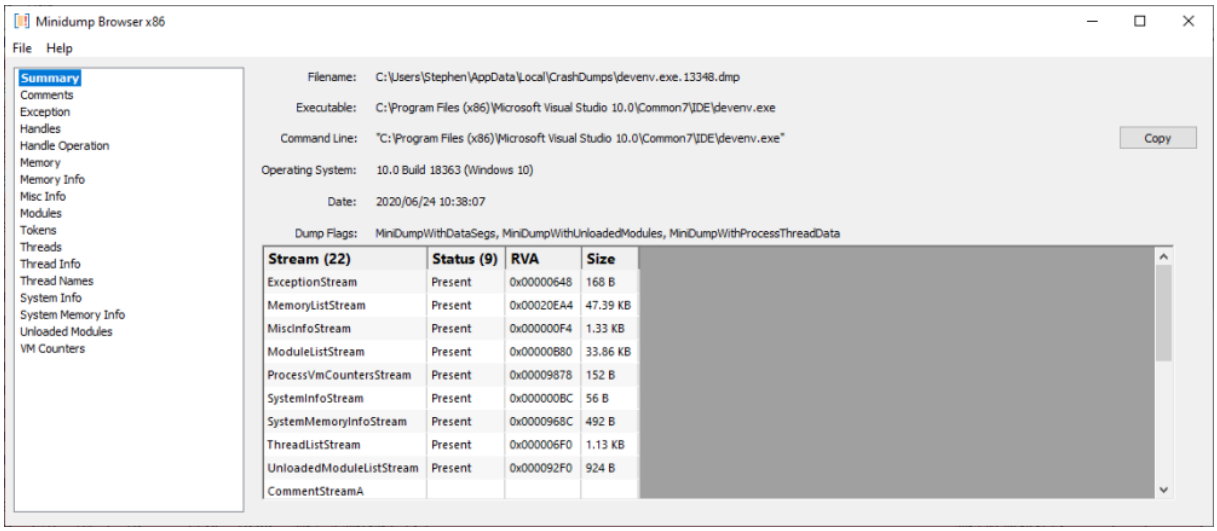


The display shows a summary page and then one page per logical group of data in the minidump. This means that some discrete sections in the minidump have been coalesced - for example ThreadListStream and ThreadExListStream are both represented in the Threads page. Each page is listed on the left hand 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.

4.1 Summary

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

Copyright © 2020-2021 Software Verify Limited



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 Comments

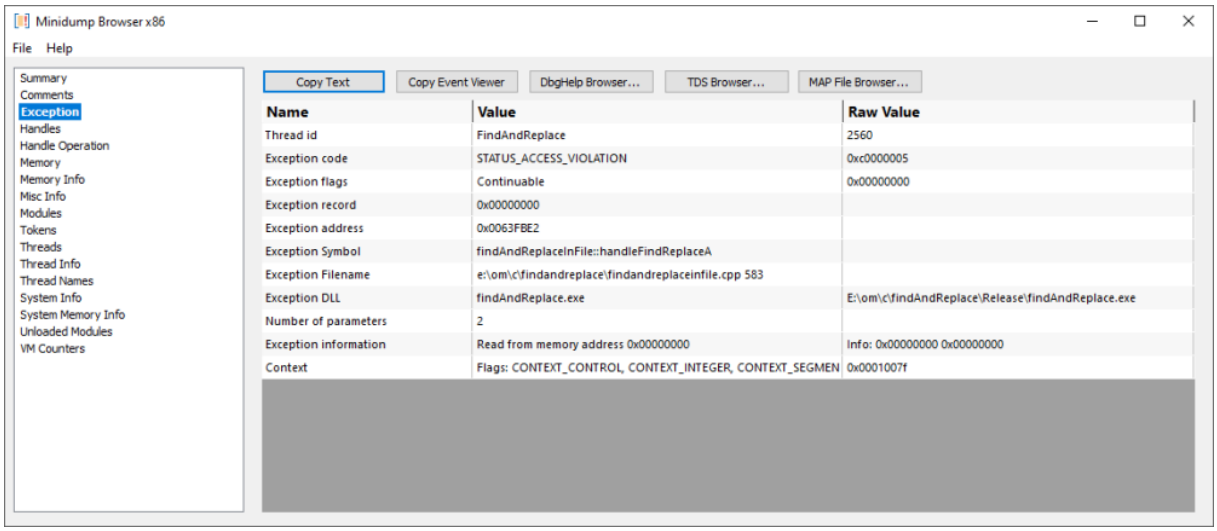
The Comments page displays the contents of the CommentStreamA and CommentStreamW minidump streams.

Copyright © 2020-2021 Software Verify Limited

4.3 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.



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".

Copyright © 2020-2021 Software Verify Limited

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 (DbgHelp 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

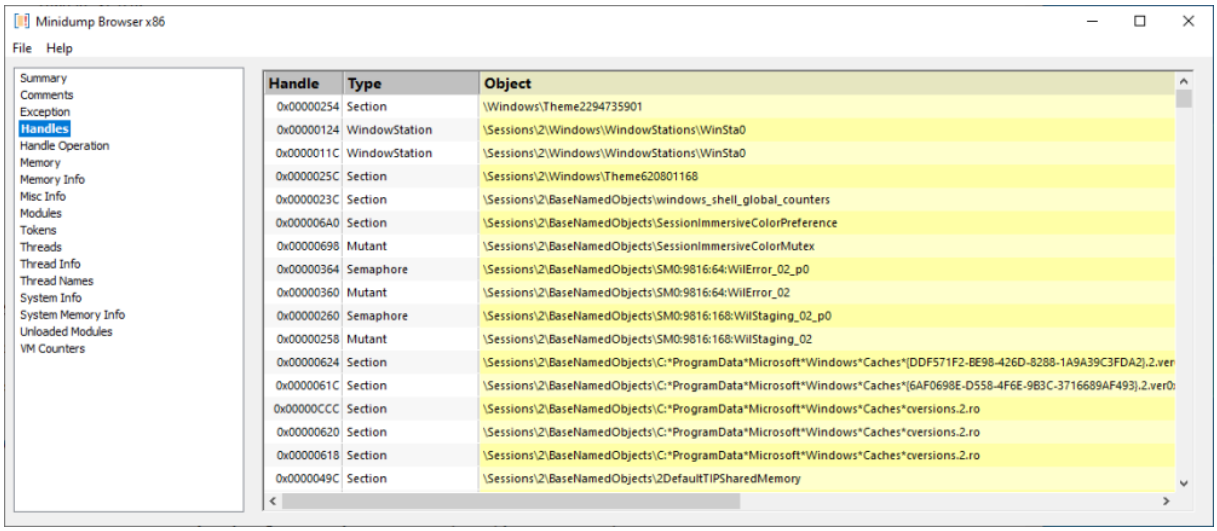
If you have installed DbgHelp Browser, TDS Browser, MAP File Browser, the appropriate button to launch this tool will be enabled.

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

4.4 Handles

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

Copyright © 2020-2021 Software Verify Limited



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.

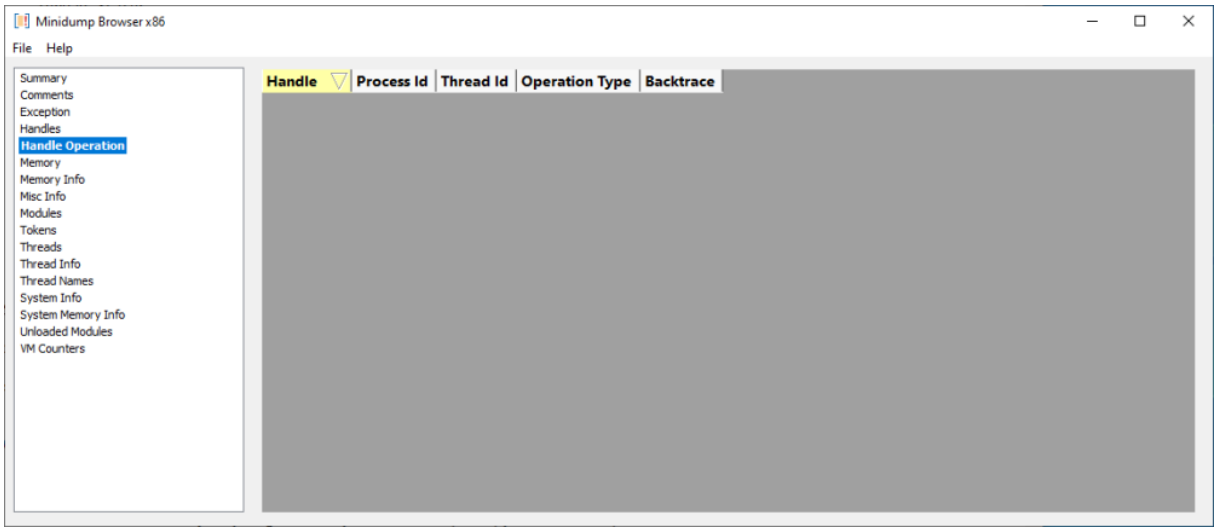
Object Info
Extra information about the object.

Reserved0

4.5 Handle Operation

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

Copyright © 2020-2021 Software Verify Limited



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

4.6 Memory

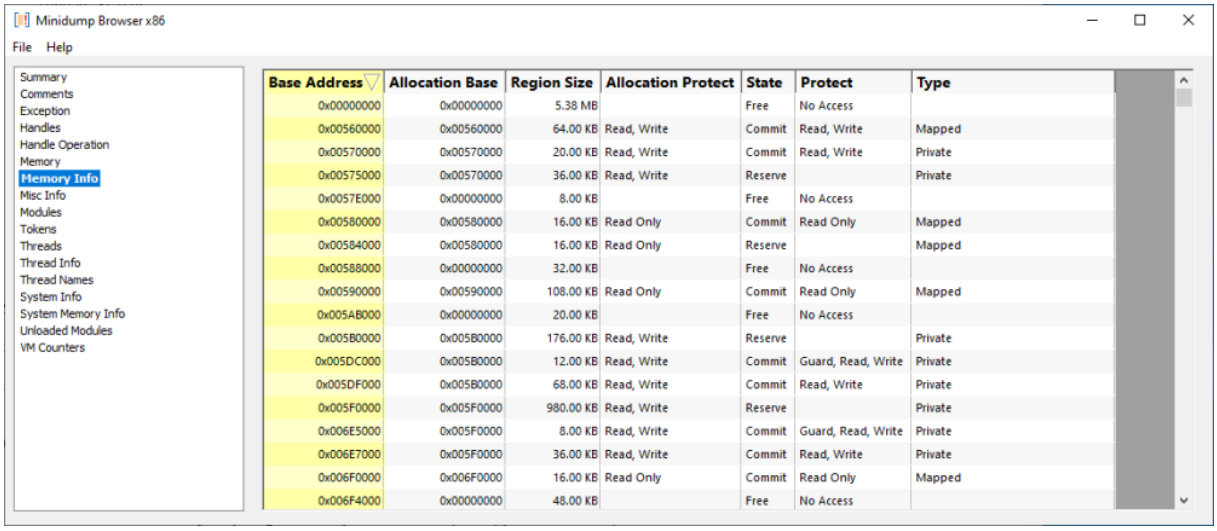
The Memory page displays the contents of the MemoryListStream and the Memory64ListStream minidump streams.

Copyright © 2020-2021 Software Verify Limited

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

4.7 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	

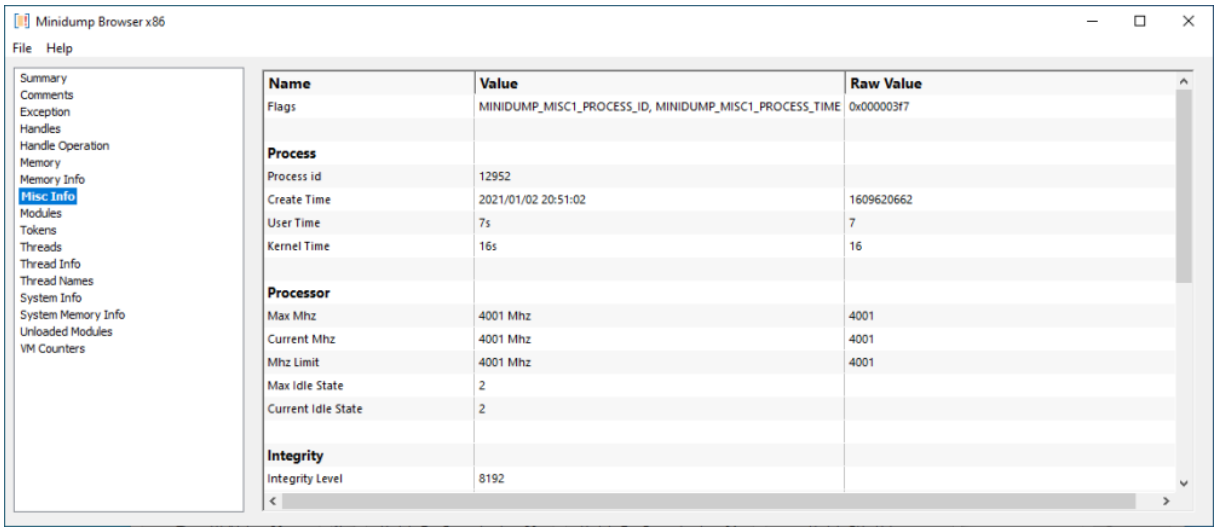
The information here allows you to inspect the memory protection status of areas of memory in the minidump.

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.

4.8 Misc Info

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

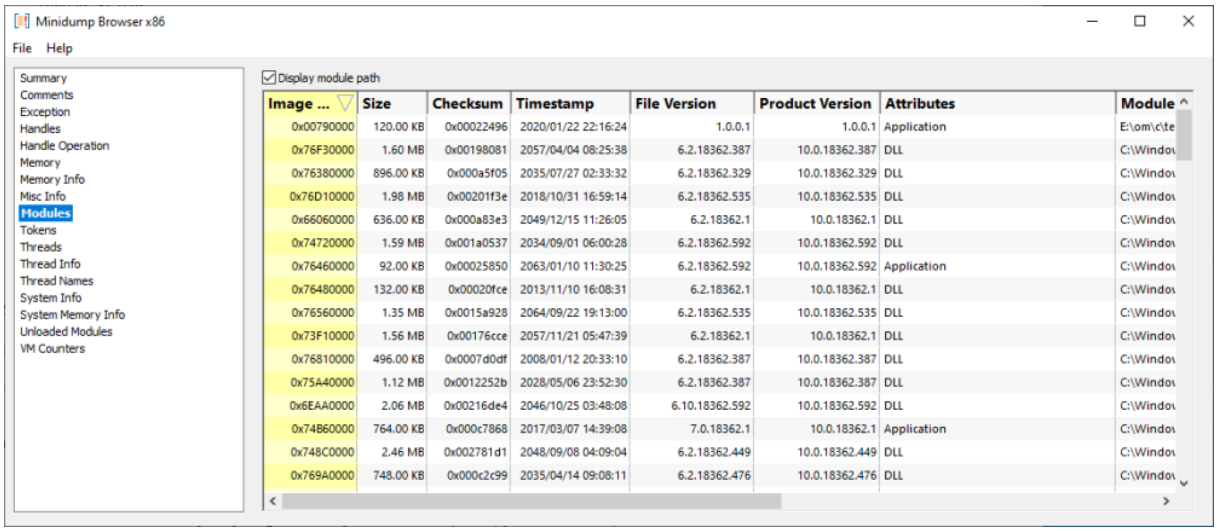
Copyright © 2020-2021 Software Verify Limited



This section provides miscellaneous information about the minidump application.

4.9 Modules

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

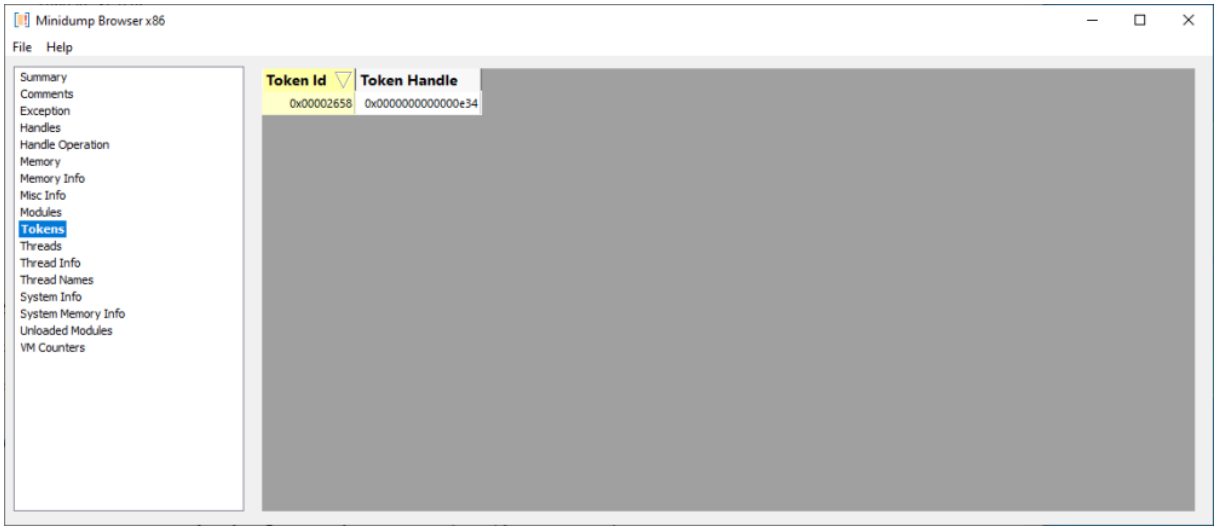


For each module in the minidump this page displays the following information, dll load address (image base), size, checksum, timestamp, file version, product version, application attributes and module name (with optional path).

Copyright © 2020-2021 Software Verify Limited

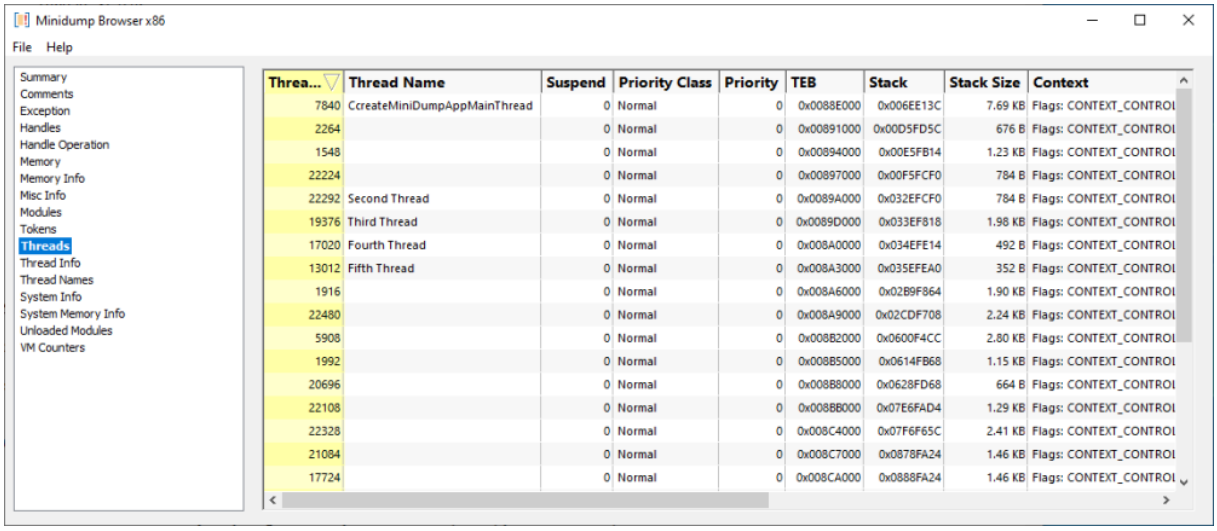
4.10 Tokens

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



4.11 Threads

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



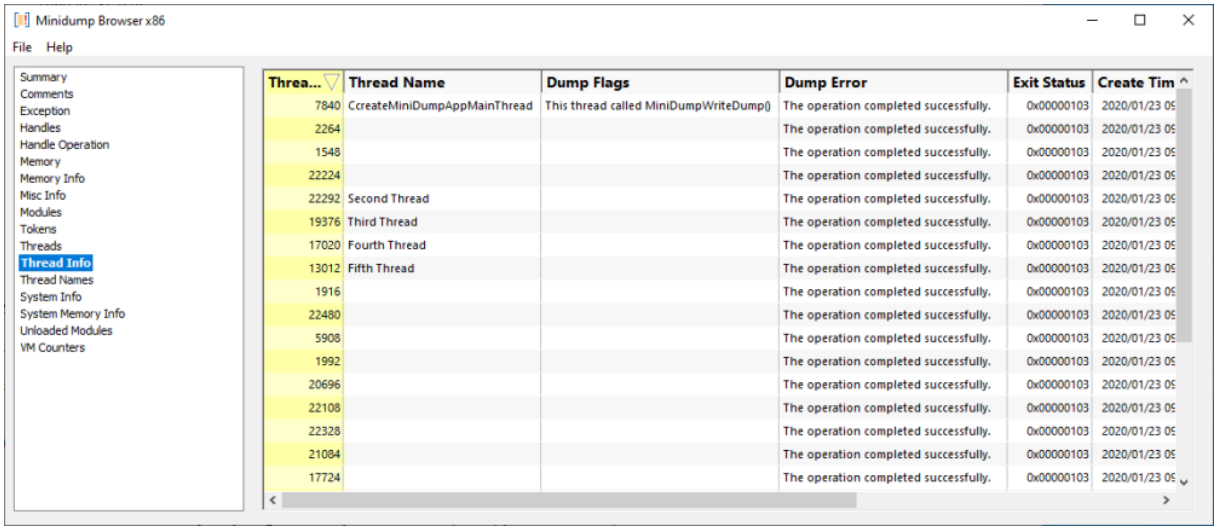
For each thread the following information is displayed: thread id, thread name, if the thread is suspended, it's priority class, it's priority level, the thread environment block (TEB) address, the stack location and

Copyright © 2020-2021 Software Verify Limited

size and the flags used to create the thread context, plus a dump of some thread context members (processor registers etc).

4.12 Thread Info

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



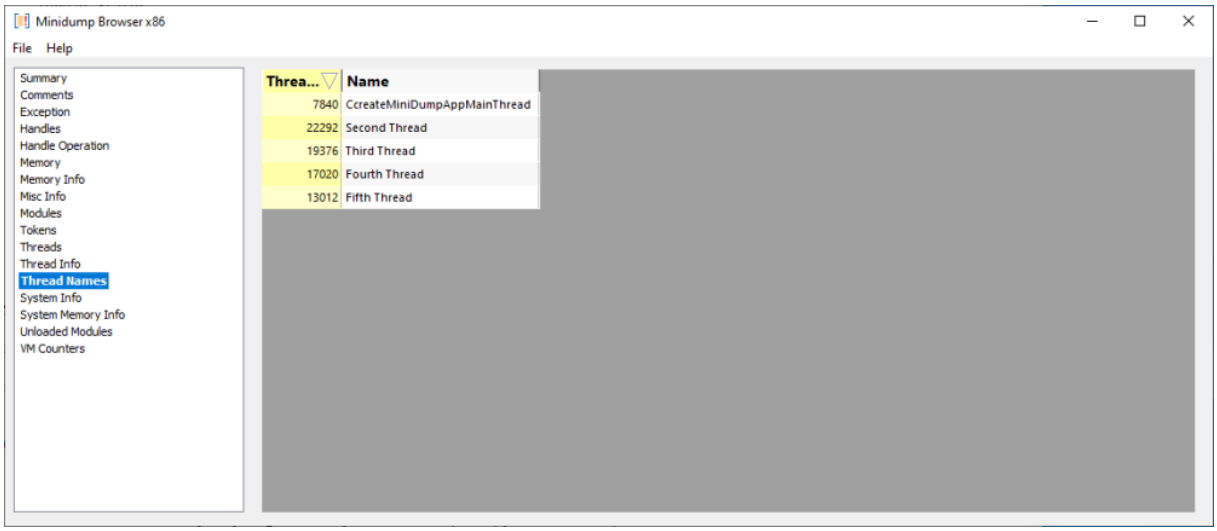
Threa...	Thread Name	Dump Flags	Dump Error	Exit Status	Create Tim
7840	CcreateMiniDumpAppMainThread	This thread called MiniDumpWriteDump()	The operation completed successfully.	0x00000103	2020/01/23 09
2264			The operation completed successfully.	0x00000103	2020/01/23 09
1548			The operation completed successfully.	0x00000103	2020/01/23 09
22224			The operation completed successfully.	0x00000103	2020/01/23 09
22292	Second Thread		The operation completed successfully.	0x00000103	2020/01/23 09
19376	Third Thread		The operation completed successfully.	0x00000103	2020/01/23 09
17020	Fourth Thread		The operation completed successfully.	0x00000103	2020/01/23 09
13012	Fifth Thread		The operation completed successfully.	0x00000103	2020/01/23 09
1916			The operation completed successfully.	0x00000103	2020/01/23 09
22480			The operation completed successfully.	0x00000103	2020/01/23 09
5908			The operation completed successfully.	0x00000103	2020/01/23 09
1992			The operation completed successfully.	0x00000103	2020/01/23 09
20696			The operation completed successfully.	0x00000103	2020/01/23 09
22108			The operation completed successfully.	0x00000103	2020/01/23 09
22328			The operation completed successfully.	0x00000103	2020/01/23 09
21084			The operation completed successfully.	0x00000103	2020/01/23 09
17724			The operation completed successfully.	0x00000103	2020/01/23 09

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.

4.13 Thread Names

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

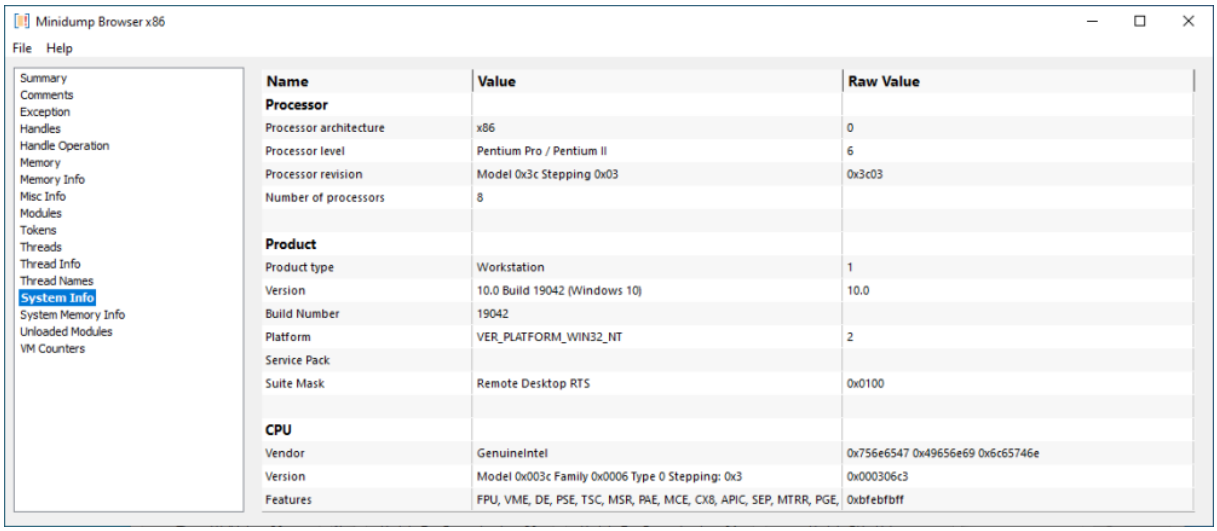
Copyright © 2020-2021 Software Verify Limited



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

4.14 System Info

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

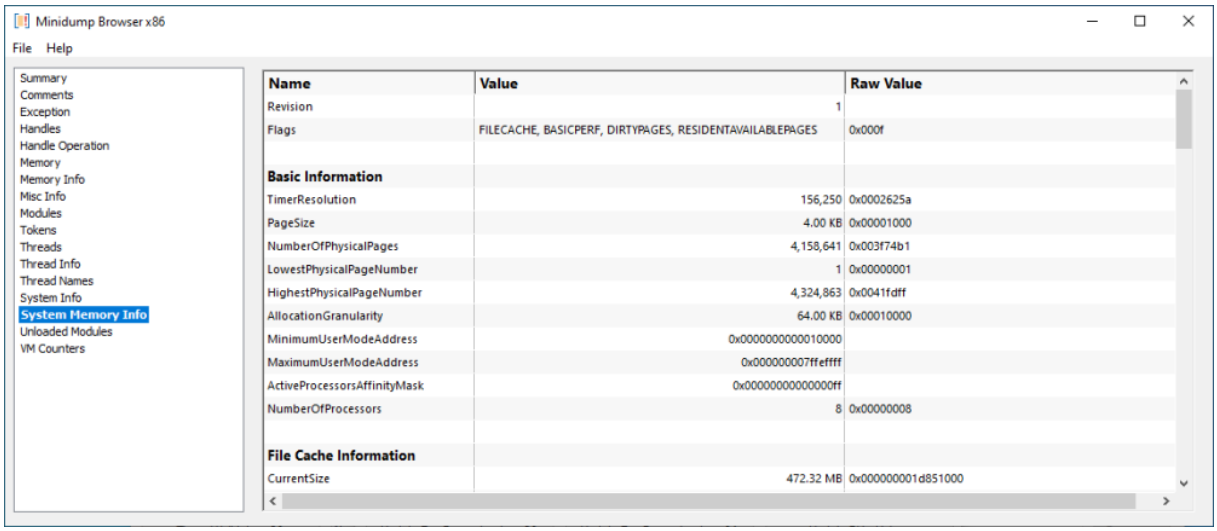


This page provides information about the computer hardware and the operating system you are using.

Copyright © 2020-2021 Software Verify Limited

4.15 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.

4.16 Unloaded Modules

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

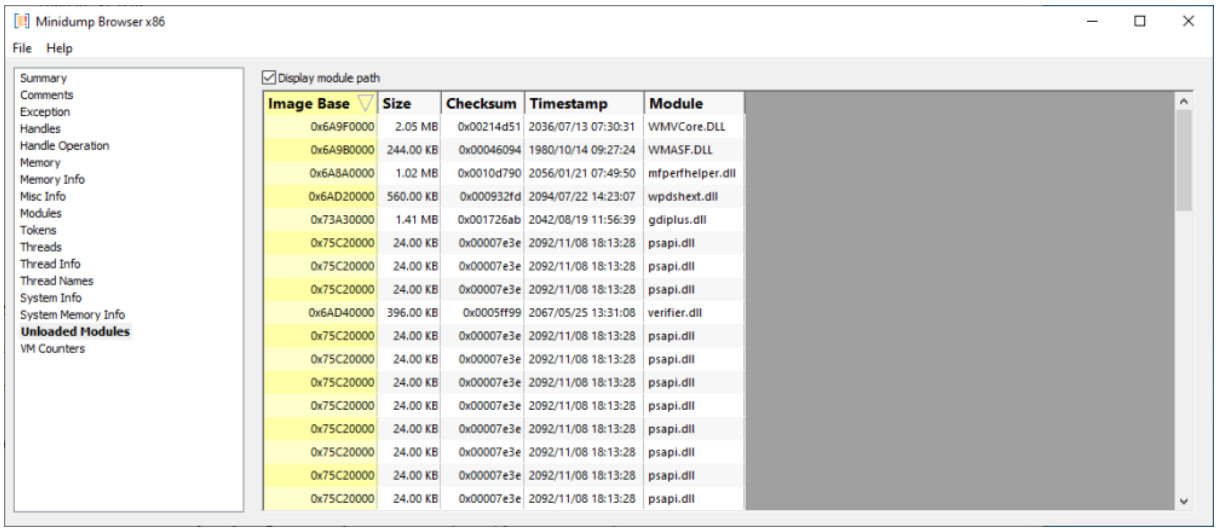


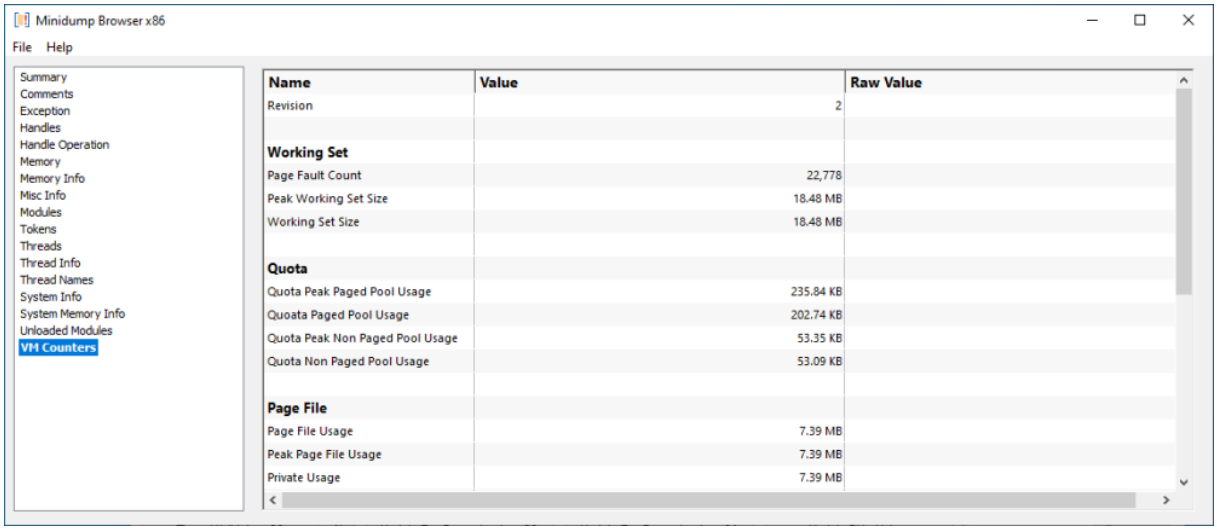
Image Base	Size	Checksum	Timestamp	Module
0x6A9F0000	2.05 MB	0x00214d51	2036/07/13 07:30:31	WMVCore.DLL
0x6A9B0000	244.00 KB	0x00046094	1980/10/14 09:27:24	WMASF.DLL
0x6A8A0000	1.02 MB	0x0010d790	2056/01/21 07:49:50	mfperfhelper.dll
0x6AD20000	560.00 KB	0x000932fd	2094/07/22 14:23:07	wpdshext.dll
0x73A30000	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

Copyright © 2020-2021 Software Verify Limited

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).

4.17 VM Counters

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



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

Copyright © 2020-2021 Software Verify Limited

Copyright © 2020-2021 Software Verify Limited