Analysis of Memory Dump file (* .dmp)

When trying to open any * .dmp file created by Windows Debugging Tools, you will find the language used in it extremely strange. Sometimes you are curious to know exactly what information inside it is?

You may or may not be familiar with the word 'memory dump'. But, you should know that it is a very important thing. This article talks about how to create a memory dump / minidump file, read it and analyze it. Also, you will know why it is so important.

Users who were faced with a dead blue screen error, may have heard about memory dump. But, most other people don't know about it. So, before going to the main points, you should have some basic knowledge about the dump file on Windows.

Analysis of Memory Dump file (* .dmp)

What is Dump memory in Windows?

When a system or application crashes, it stores and displays content in a file. This process is called memory dump. When a system failure or a blue screen error occurs, Windows stores information related to the problem on a file. It is like a log file. After that, the user or expert can analyze the dump file to determine the real reasons for the system error. In Windows, there are several types of memory dump files, including:

1. Complete Memory Dump

It is the largest dump file in Windows. It contains all memory related information. Complete Memory Dump has many advantages. But, sometimes, it can occupy a considerable amount of drive space.

2. Kernel Memory Dump

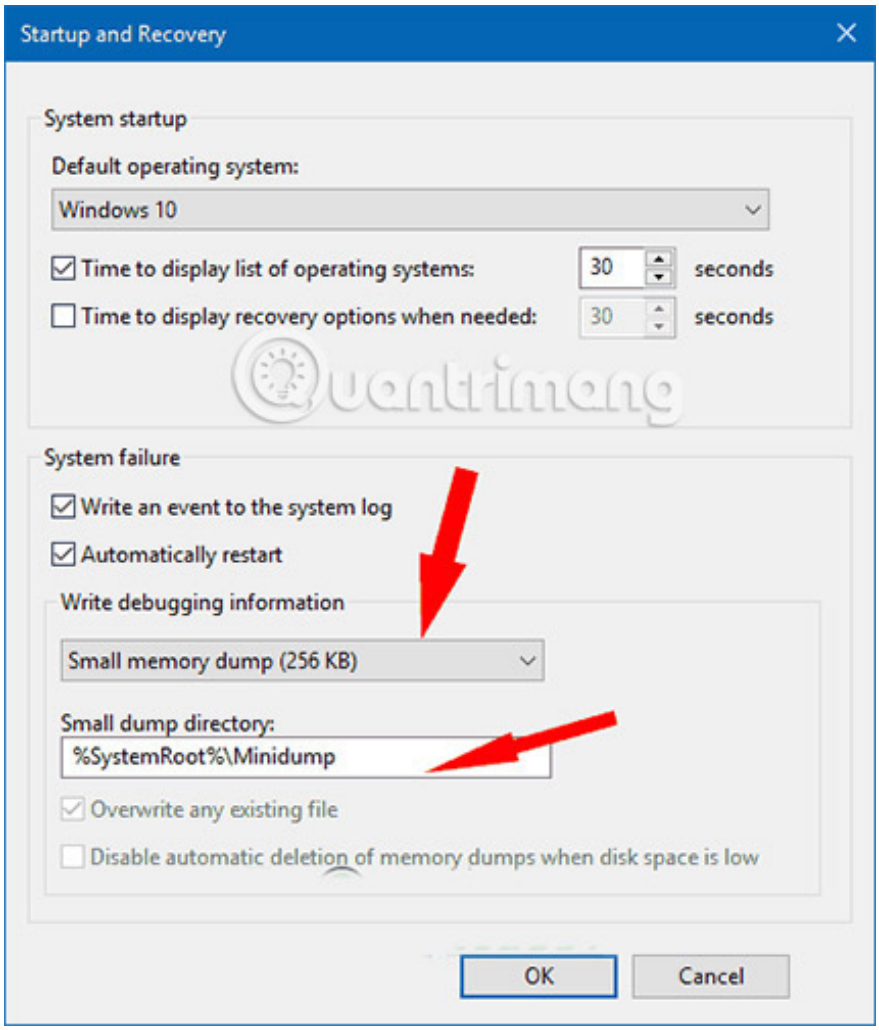
It is much smaller than Complete Memory Dump. It contains all information about the memory usage of the kernel at the time the system is broken or an error occurs.

3. Small memory dump

Small memory dump is the smallest size. It contains some basic information about drivers, kernel, etc. In general, its size is usually 128 or 256KB. It helps identify driver-related errors, like a dead blue screen error.

How to create Small Memory Dump / Minidump file

Technically, you will not have to create a Small Memory Dump file. Windows will do it automatically. You only need to configure Windows so that it creates Small Memory Dump or Minidump files. The following is a guide on how to do it.



1. First, open the **Start** menu **,** type **sysdm.cpl** and press **Enter.** Then, the **System Properties** window will open.
2. Now, go to the **Advanced** tab and click **Settings** in the **Startup and Recovery section.**

3. Then, click the drop-down option in the **Write debugging information section** . Select **Small Memory Dump (256KB)** .
4. Then, click **OK.**

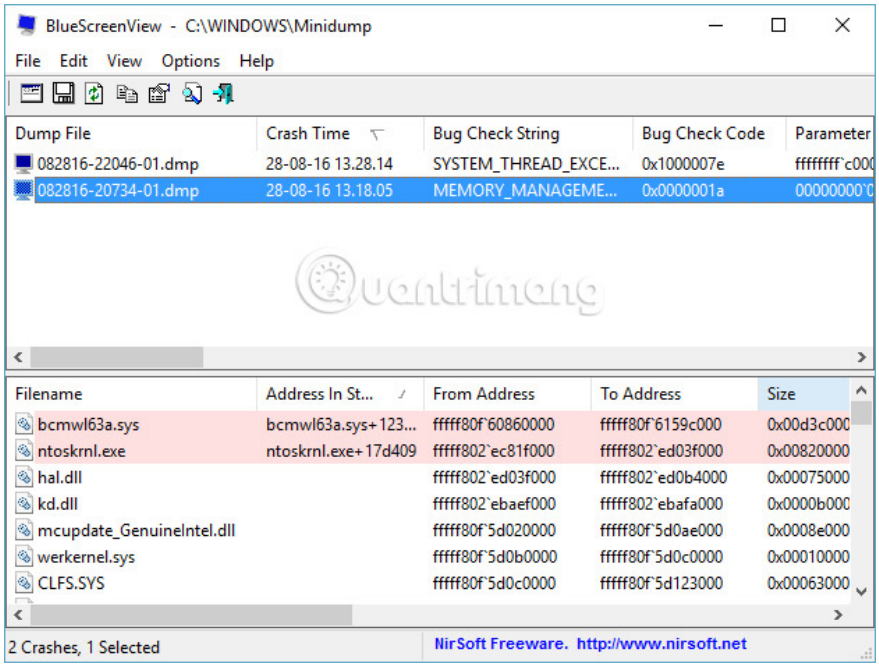
In general, the location of the minidump file is usually **% SystemRoot% Minidump** by default. That means you can find the dump file in **C: WindowsMinidump.** But, you can change this if you want.

How to read and analyze Minidump files

You have just configured your PC to create Small Memory Dump file. Therefore, it will store all memory-related information on a single file when you encounter a dead blue screen error. But, then, what will you do? How can you read it? How do you know what is causing the problem? This is really a very easy process.

Use BlueScreen Viewer

NirSoft has created a simple program called "BlueScreen Viewer", which can read and analyze Small Memory Dump file. You can download it from: **http://www.nirsoft.net/utils/blue_screen_view.html#DownloadLinks.** Then, unzip and open it on your computer. Next, just browse the minidump file and read it.



When you have a minidump file in BlueScreen Viewer, it will show you a series of basic data. You will find problematic files that have caused the latest blue screen death error to be marked.

Find related drivers

The problem is that when you analyze the dump file, it will highlight the **.sys** file name **.** It really involves a driver on your computer. For example, **bcmwl63a.sys** is related to the Wireless Broadcom WiFi driver. But, How do you understand it? There are two easy ways you can do the following:

1. First, go to **C: WindowsSystem32drivers.**
2. You will see a list of .sys files. Just find one of the highlighted files in Bluescreen Viewer.
3. Then, right click on it and go to its properties section.
4. Then, click the **Details** tab **.**
5. You will see information about the driver in the description.

If you don't like this way, you can search on Google .sys driver name. It will help find the exact name of the problem driver.

Surely, you understand that a Minidump file is very important in determining the reason for causing a Windows error. After finding a problem driver, you can update it, restore or uninstall to solve your problem.

Hope this article will help you create Small Memory Dump file easily. It will also help identify and fix various system problems on Windows.

Good luck!

See more:

1. Use the WinDBG debugger to fix the blue screen error
2. Trick to fix 'blank' windows error
3. Use the RecoverServer switch to restore Exchange 2007