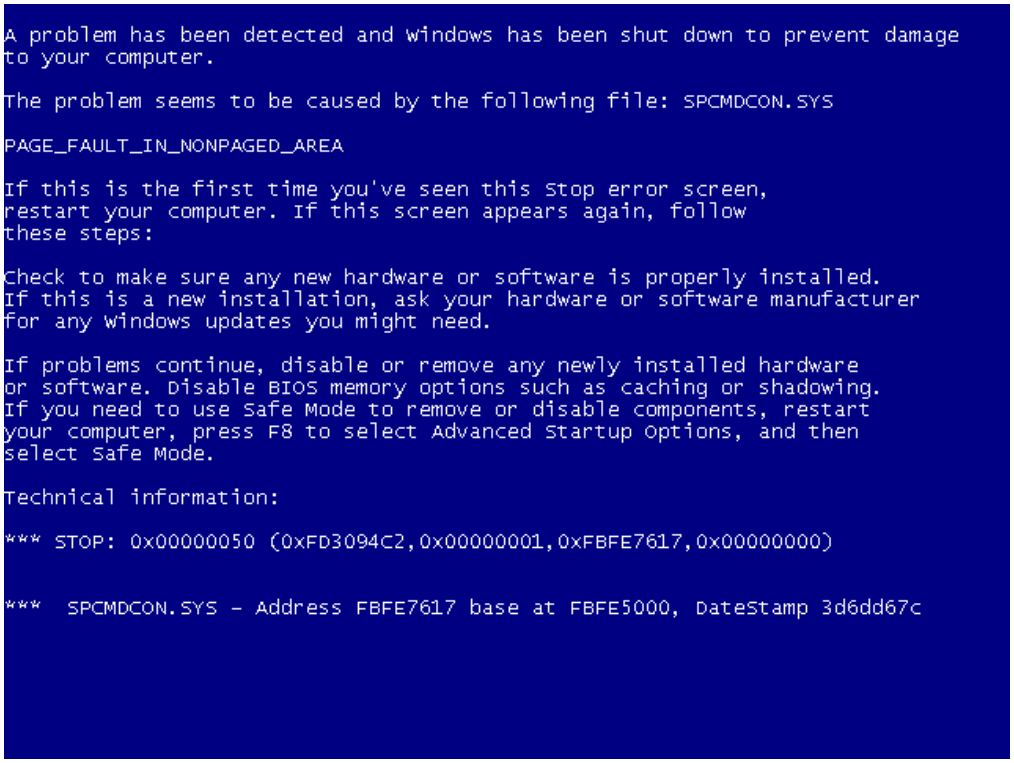
How To Diagnose A Windows BSOD

For many computer owners, getting the infamous Blue Screen of Death (or BSOD) can be a frustrating experience, and for most, one that doesn't lead anywhere, since there is no clear indication as to what to do next. But it doesn't need to be this way. With the right tools, the cause of a BSOD can quickly be determined, or at least we can be pointed in the right direction, saving us hours of blind troubleshooting.

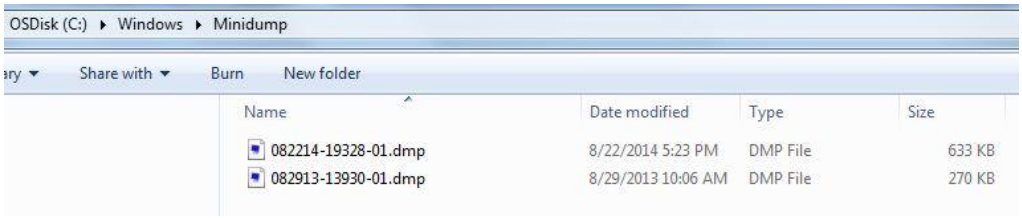


Enter the Small Memory Dump

Windows has the capability of--upon a system crash--dumping certain information from memory onto a file stored in your computer's hard drive. Some of the tidbits Windows writes to this dump file include the following:

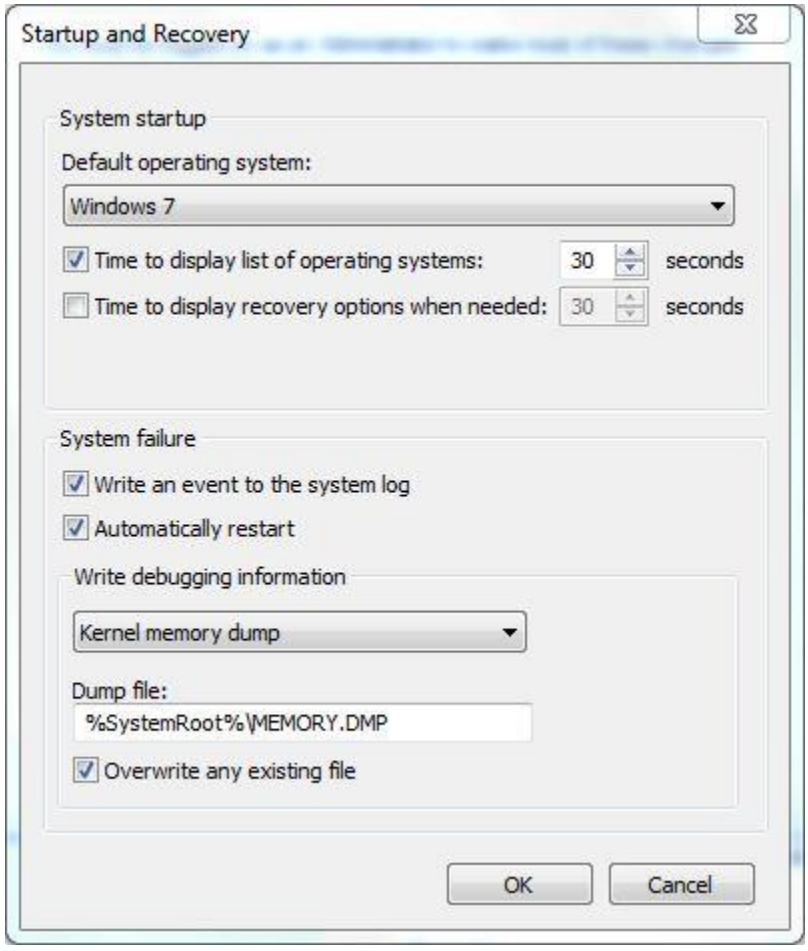
- The Stop message (such as KMODE_EXCEPTION_NOT_HANDLED or IRQ_NOT_LESS_OR_EQUAL).
- A list of drivers in use when the crash occurred.
- Information on what the CPU was doing when the crash occurred.
- What processes were running at the time.

This information is written to a file with a DMP extension (for example, 082214-19328-01.dmp) and stored in **C:\Windows\Minidump**.



If you can't find the **Minidump** folder it means the feature that writes debugging information is not enabled. To enable it you'll need to do the following:

1. Click on the **Start** button, and then click **Control Panel**.
2. Click on **System**, and then click **Advanced system settings**.
3. Click the **Advanced** tab, and then click **Settings** under **Startup and Recovery**.
4. In the **Write debugging information** list, click **Small memory dump**



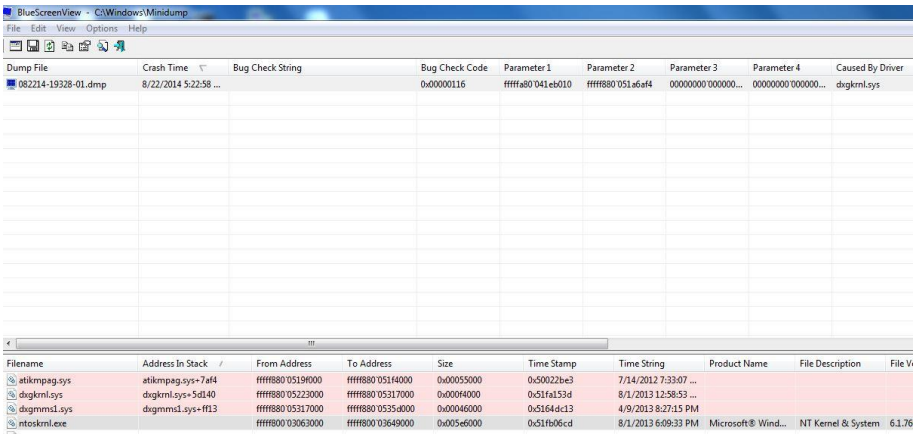
The next time Windows crashes navigate to the **C:\Windows\Minidump** folder; a new DMP file should have been created. But what do we do with this file?

Debugging tools

Microsoft has several debugging tools that can be used to view DMP files, such as the **Dump Check Utility** or **Windows Debugger**, but I prefer a freeware tool called **BlueScreenView** (http://www.nirsoft.net/utils/blue_screen_view.html). As opposed to **Dump Check Utility** and **Windows Debugger**, which are command-line programs, **BlueScreenView** is a GUI-based tool that is very user-friendly.

When you open a DMP file using **BlueScreenView** the program shows you the Stop message and which driver caused the crash. It also shows you a complete list of drivers that were in use at the time of the incident, and highlights the drivers that may have suffered a conflict.

For example, while checking a DMP file on your PC, **BlueScreenView** points to dxgkrnl.sys as the driver that caused the crash. Looking at the list of drivers that were in use at the time you see that the program has highlighted the same dxgkrnl.sys file along with dxgmms1.sys and atikmpag.sys. Googling the file names you find that the first two files are related to DirectX while the third one is related to the ATI video card driver. Knowing this you can probably go to the ATI website and look for an updated driver for your video card. Running the DirectX Diagnostic Tool to see if this software has a problem would also be a good option.



By using **BlueScreenView** to examine Windows' Small Memory Dumps you're able to narrow down the list of possible culprits, instead of blindly swapping memory modules, purchasing a new hard drive, reinstalling Windows or doing a number of things that may result in a waste of time and money.