

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.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

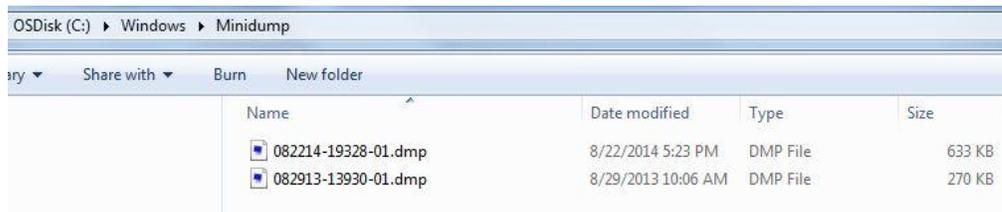
*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

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:

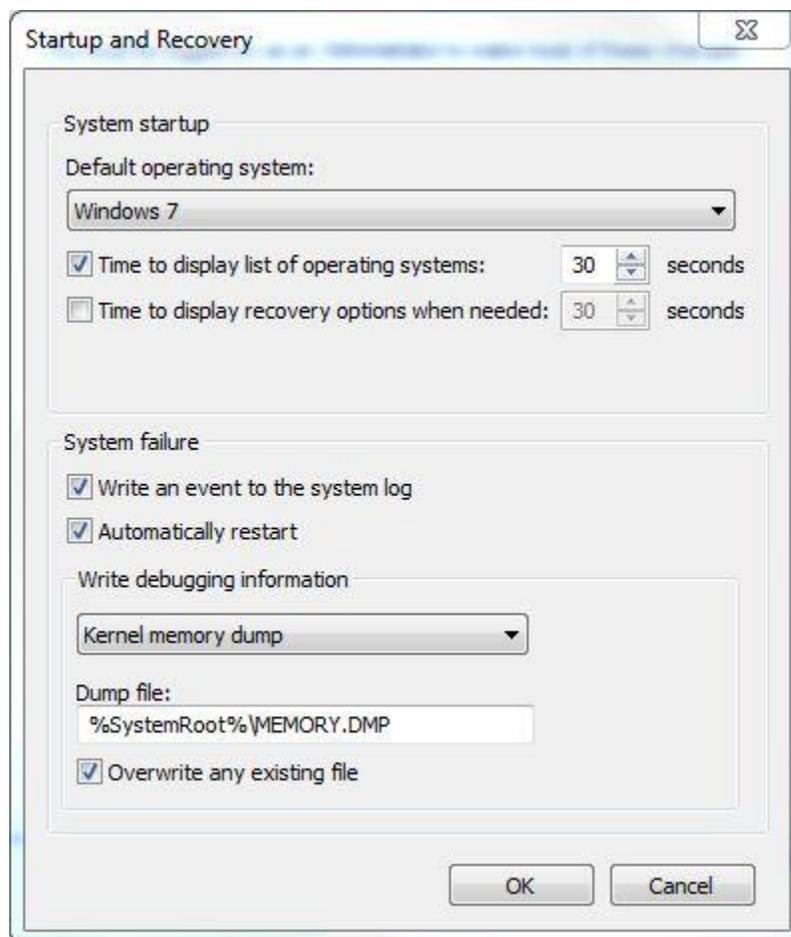
- The Stop message (such as `KMODE_EXCEPTION_NOT_HANDLED` or `IRQ_NOT_LESS_OR_EQUAL`).
- A list of drivers in use when the crash occurred.
- Information on what the CPU was doing when the crash occurred.
- What processes were running at the time.

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**



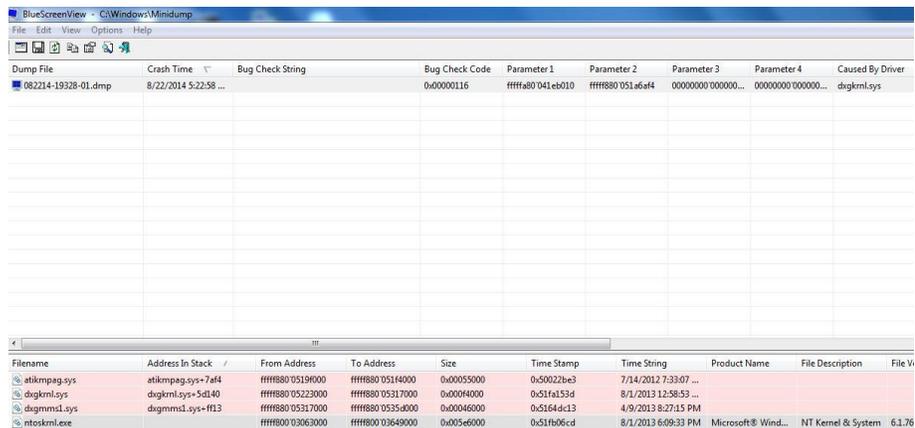
The next time Windows crashes navigate to the **C:\Windows\Minidump** folder; a new DMP file should have been created. But what do we do with this file?

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 dxgmmms1.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.



The screenshot shows the BlueScreenView application window. The main table displays crash information for a dump file named '082214-19328-01.dmp'. The crash occurred on 8/22/2014 at 5:22:58. The bug check code is 0x00000116. The driver that caused the crash is dxgkrnl.sys. Below this, a list of files in use is shown, with dxgkrnl.sys, dxgmmms1.sys, and atikmpag.sys highlighted in red to indicate they were involved in the crash.

Dump File	Crash Time	Bug Check String	Bug Check Code	Parameter 1	Parameter 2	Parameter 3	Parameter 4	Caused By Driver
082214-19328-01.dmp	8/22/2014 5:22:58 ...		0x00000116	ffffa80 041e6010	ffff880 051e6af4	00000000 00000000...	00000000 00000000...	dxgkrnl.sys

Filename	Address In Stack	From Address	To Address	Size	Time Stamp	Time String	Product Name	File Description	File V
atikmpag.sys	atikmpag.sys+7af4	ffff880 05199000	ffff880 051f4000	0x00055000	0x50022be3	7/14/2012 7:33:07 ...			
dxgkrnl.sys	dxgkrnl.sys+5d140	ffff880 05322000	ffff880 05317000	0x00040000	0x51fa1534	8/1/2013 12:58:53 ...			
dxgmmms1.sys	dxgmmms1.sys+ff13	ffff880 05317000	ffff880 0535a000	0x00046000	0x5164d13	4/9/2013 8:27:15 PM			
ntoskrnl.exe		ffff800 03063000	ffff800 03649000	0x005e6000	0x51fb06cd	8/1/2013 6:09:33 PM	Microsoft® Wind...	NT Kernel & System	6.1.76

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.

