

Deciphering the Blue Screen of Death

Brien M. Posey

I'll never forget the first time I ever encountered the infamous Blue Screen of Death (BSOD). Although my experience with Windows was very limited at the time, I was absolutely positive of two things:

1. Something bad had happened.
2. All of those hieroglyphics on the screen contained useful information, if I could just figure out how to read them.

In retrospect, both of those assumptions turned out to be true. A Blue Screen of Death is Windows' way of telling you that an unrecoverable, kernel mode error has occurred. There are a number of different things that can cause a BSOD error, so the BSOD gives you information that is designed to help you figure out what went wrong. In this article, I will show you how to make sense of these rather cryptic screens.

BSOD has changed over time

Before I get started, I want to point out that the BSOD has evolved over the years. In Figure A, you can see a Windows NT style BSOD that I captured back in 1999. Figure B shows a Windows XP BSOD. Although there are some major differences between those two screens, there are also some similarities.

```
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFFD4,0xC0000000)
BAD_POOL_HEADER

CPUID: GenuineIntel 5.2.c irq1:1f SYSVER 0xf0000565

Dll Base DateStmp - Name Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe 80010000 31ee6c52 - hal.dll
80001000 31ed06b4 - atapi.sys 80006000 31ec6c74 - SCSIPTORT.SYS
802c6000 31ed06bf - aic78xx.sys 802cd000 31ed237c - Disk.sys
802d1000 31ec6c7a - CLASS2.SYS 8037c000 31eed0a7 - Ntfs.sys
fc698000 31ec6c7d - Floppy.SYS fc6a8000 31ec6ca1 - Cdrom.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS fc9c9000 31ec6c99 - Null.SYS
fc864000 31ed868b - KSecDD.SYS fc9ca000 31ec6c78 - Beep.SYS
fc6d8000 31ec6c90 - i8042prt.sys fc86c000 31ec6c97 - mouclass.sys
fc874000 31ec6c94 - kbdclass.sys fc6f0000 31f50722 - UIDEOPORT.SYS
feffa000 31ec6c62 - mga_mil.sys fc890000 31ec6c6d - vga.sys
fc708000 31ec6ccb - Msfs.SYS fc4b0000 31ec6cc7 - Npfs.SYS
fefbc000 31eed262 - NDIS.SYS a0000000 31f954f7 - win32k.sys
feffa4000 31f91a51 - mga.dll fec31000 31eedd07 - Fastfat.SYS
feb8c000 31ec6e6c - TDI.SYS feaf0000 31ed0754 - nbf.sys
feacf000 31f130a7 - tcpip.sys feab3000 31f50a65 - netbt.sys
fc550000 31601a30 - e159x.sys fc560000 31f8f864 - afd.sys
fc718000 31ec6e7a - netbios.sys fc858000 31ec6c9b - Parport.sys
fc870000 31ec6c9b - Parallel.SYS fc954000 31ec6c9d - ParUdm.SYS
fc5b0000 31ec6cb1 - Serial.SYS fea4c000 31f5003b - rdrv.sys
fea3b000 31f7a1ba - mup.sys fe9da000 32031abe - srv.sys

Address dword dump Build [1381] - Name
fec32d84 80143e00 80143e00 80144000 ffdff000 00070b02 - KSecDD.SYS
801471c8 80144000 80144000 ffdff000 c03000b0 00000001 - ntoskrnl.exe
801471dc 80122000 f0003fe0 f030eee0 e133c4b4 e133c4d0 - ntoskrnl.exe
80147304 803023f0 0000023c 00000034 00000000 00000000 - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.
```

Figure A

This is a Windows NT style BSOD

Deciphering the Blue Screen of Death

Brien M. Posey

```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)
A problem has been detected and Windows has been shut down to prevent damage
to your computer
DRIVER_IRQL_NOT_LESS_OR_EQUAL
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.
*** ABCD.SYS - Address F73120AE base at C0000000, DateStamp 36B072A3
Kernel Debugger Using: COM2 (Port 0x2F8, Baud Rate 19200)
Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

Figure B

This is a Windows XP style BSOD

For the purposes of this article series, I will be examining the Windows XP style BSOD (which is also used in Windows Server 2003). If you happen to be running another version of Windows, you can still use the information in this series of articles to help figure out what's going on with your system, but you won't be able to follow along step by step.

The anatomy of a stop message

The text that is displayed on the BSOD is known in Microsoft circles as a stop message. The stop message is broken into four different parts, each of which has its own purpose. The parts of a stop message include bug check information, recommended user action, driver information and debug port and status information. Figure C shows the same stop message that's displayed in Figure B, but also shows the stop message's various parts.

Deciphering the Blue Screen of Death

Brien M. Posey

Bug Check Information

```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)
A problem has been detected and Windows has been shut down to prevent damage
to your computer
```

Recommended User Action

```
DRIVER_IRQL_NOT_LESS_OR_EQUAL

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.
```

Driver Information

```
*** ABCD.SYS - Address F73120AE base at C0000000, DateStamp 36B072A3
```

Debug Port and Dump Status Information

```
Kernel1 Debugger Using: COM2 (Port 0x2F8, Baud Rate 19200)
Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

Figure C

These are the components of a stop message

The Bug Check Information section

The Bug Check Information is made up of a stop error number and four additional parameters that are listed in parentheses immediately following the stop error number.

Here is where I need to stop for a quick reality check. Each of these five numbers has its own significance, as does everything else on the screen. If you happen to be a software developer, and a software component that you created is causing the stop error, then each of these five numbers is going to be critically important to you. From an administrator's standpoint, though, the four numbers found in parentheses are almost always unimportant.

Over the years, I have fixed more blue screen errors than I care to think about, and only on extremely rare occasions has the diagnostic process required me to look at the individual parameters. Typically, knowing the stop error code is sufficient. I will be talking about the stop error code in depth later in this series.

The Recommended User Action section

The second part of the stop message is the Recommended User Action. Figure C shows that the

Deciphering the Blue Screen of Death

Brien M. Posey

recommended user action is usually a generic message that tells you to try disabling or removing whatever hardware or software was recently installed. While this is good advice, it won't always fix the problem.

By far the most important part of the recommended user action is the very first line. In Figure C, this is the line that reads:

```
DRIVER_IRQL_NOT_LESS_OR_EQUAL
```

This line directly corresponds to the stop error number. Using this bit of text in conjunction with the stop error number gives you a lot of insight into the problem.

The Driver Information section

The Driver Information section provides the third important piece of information. It tells you which file triggered the stop error. By looking at the driver listed in this section and the information provided in the Bug Check Information section and the Recommended User Action section, you can usually gain a fairly clear picture of what happened.

The Debug Port and Dump Status Information section

The Debug Port and Dump Status Information section tells you two main things. The first is which COM port is being used by the debugger and at what speed the COM port is running. You can ignore this bit of information. In the old days, you could connect a serial cable between a functional machine and a machine that had crashed, and use a debugger on the functional machine to figure out what had happened to the machine that had crashed. Today, though, computers are not even equipped with serial ports, so this information is irrelevant.

The other thing this section tells you is that a dump file was created. Essentially this means that the entire contents of the system's memory were written to a file and placed on the hard drive. Some administrators like to use this file as a tool for debugging the problem. But as I mentioned earlier, it is usually possible to fix the problem without delving into that level of complexity.

Memory dumps can come in a few different forms. You can use registry settings to control whether Windows performs a complete memory dump, a kernel memory dump or a small memory dump. In addition, there is a setting you can use to control whether or not the dump file is overwritten should a subsequent crash occur. I will discuss the dump file and the various configuration options in a lot more detail later on in this series.

Some final advice

I will delve much deeper into the information that is within the stop message in part two and beyond in this series of articles.

I realize, however, that some of you may need to correct a stop error now, and may not have time to wait for me to write part two. That being the case, here is a final piece of advice based on my own experience:

In most cases, stop errors occur immediately after installing a piece of hardware or software or changing some aspect of the system's configuration. If you notice this type of cause and effect pattern, you can usually boot the system into Safe Mode, and then correct whatever action it was that caused the problem (or remove the new hardware).

Deciphering the Blue Screen of Death

Brien M. Posey

If the problem starts happening for no apparent reason, look for these two things: file corruption and memory problems. Try reinstalling the latest Windows service pack (to refresh the system files) and download the latest versions of all of the device drivers that are used by the system. If that doesn't work, then try removing the computer's memory and replacing it with known good memory. Nine times out of ten this will fix the problem.