Troubleshooting and analyzing Blue Screens of Death

How to troubleshoot and analyze the crash dump file that is the direct result of the infamous Blue Screen of Death in Windows 2000, Windows XP, Windows Vista and Server 2003 or 2008 and also Windows 7 and Windows Server 2008 R2 operating systems.

About 80 percent of all BSODs occur because of bad drivers. Hardware problems such as corrupt memory modules or a broken hard drive generally also produce a BSOD every now and then.

Stop the computer from restarting automatically
The standard setting for when a crash occurs is that Windows restarts automatically, which means you cannot read the error message in the actual blue screen before the computer restarts. You can adjust this setting in
System > Advanced system settings > Startup and recovery settings and uncheck automatically restart.
But even if you then have the chance to read the error message on the blue screen it does not necessarily mean that you can understand it and find the cause of the problem. That's where this guide comes in handy.

Install the necessary software go get started
We will be working with the Microsoft tool Windows Debugging Tools which can be downloaded fir free from Microsoft, http://www.microsoft.com/whdc/devtools/debugging/default.mspx

Depending on which platform you are running you must choose the appropriate debugger for x86, x64 or the ia64 platform. Install the application with the standard settings and then start it from the Start menu, it's called WinDbg. To be able to get a result from the debugging you will need the symbol files. These can be downloaded as one package but it is much more convenient to setup Windows Debugging Tools to download files as necessary. To set this up go to Open and choose Symbol file path. Now type a path to a directory on the hard drive, for example:
SRV*C:\symbolfiles*http://msdl.microsoft.com/download/symbols

Load and analyze the crash dump file
When your computer crashes a snapshot of the memory is dumped to a file on your computer. This is the file that contains the key to the crash and to analyze it first open it by going to Open and then choosing Open Crash Dump. Usually the crash dump file is named MEMORY.DMP and is located in the root of the WINDOWS (or WINNT) folder. There can also be mini dumps in the ?minidumps? folder in WINDOWS which can be used if there are no MEMORY.DMP files available.
Browse to the DMP file and choose to load it and if you get a question if you want to save the workspace you choose Yes. The necessary symbol files will now be downloaded from Microsoft. When that part is done the crash dump file will be analyzed but to find out more details about the crash you have to type:

```
!analyze -V
```

and then press Enter. An analysis is now done and you will get information about which files and drivers are involved in the crash, or if there is faulty hardware that is likely causing the crashes.
I usually pay close attention to the Bit Bucket error!

Summary
You can with the above information at least find out what the cause of the crash is and most times the crashes happen due to bad drivers. Which driver is causing the crash can be found out by either the driver name or by using your favorite search engine to lookup the file name mention in the analysis. For example nv4_disp.sys is related to Nvidia and ati2dvag.sys is related to ATI. If you learn that a specific driver is causing the crash immediately go to the hardware vendor's site and see if there is an updated driver available, if not submit a bug report with the hardware vendor or computer manufacturer.

Other ways to analyze BSOD mini dumps is with
BlueScreen View
MS DART