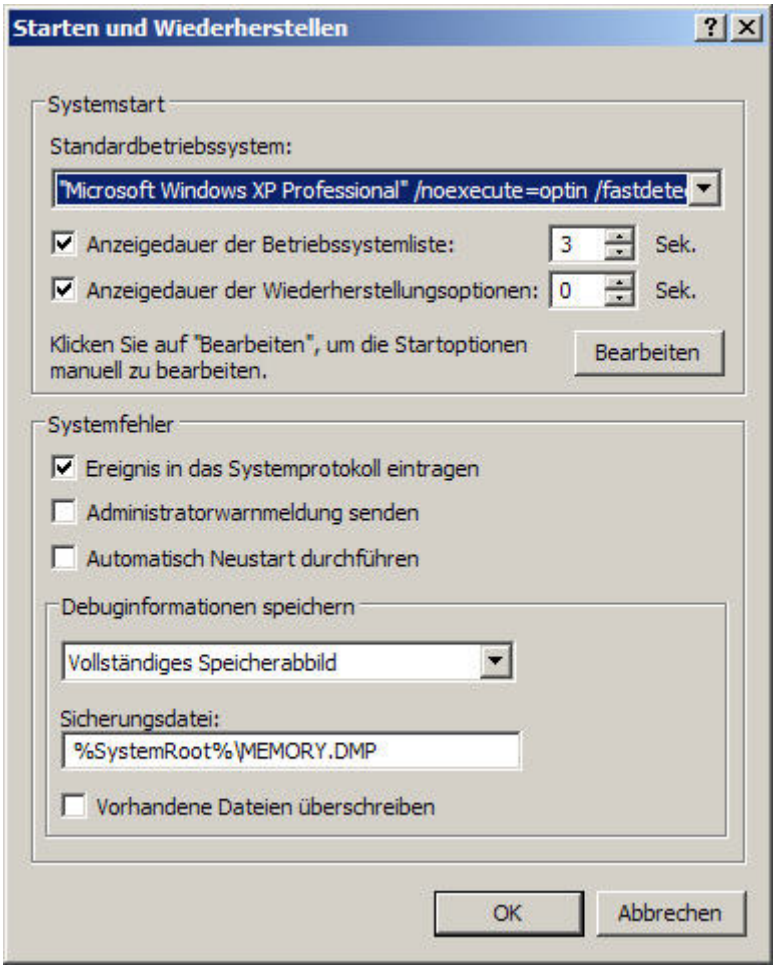
Bluescreen- Analyse

Verabschiedet sich das System mit einem Bluescreen, ist das meist ein ziemlicher Schock. Man sollte die Meldung genau lesen und zuerst einmal nachschauen, was einem in DreiTeufelsNamen gesagt werden soll. Zuerst mal hier nachschauen:
http://www.jasik.de/Shutdown/stop_fehler.htm
– in der Hoffnung, eine bekannte Meldung zu finden um auf die Ursache schließen zu können.
Reicht das nicht aus oder fehlt eine solche Meldung, kann man weiterhin versuchen, ein Speicherabbild zu erzeugen und dies auszuwerten.

Vorbereitung:

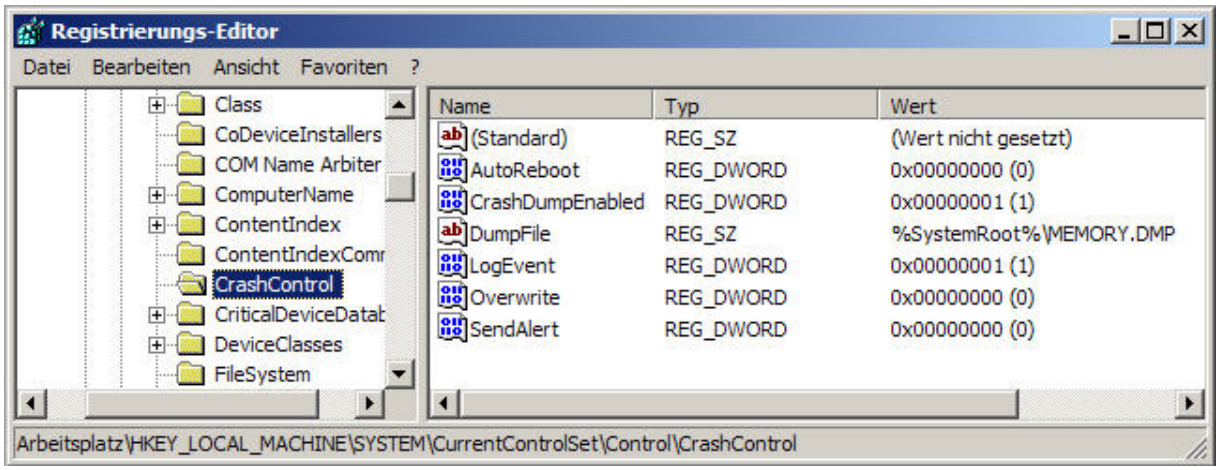
Eine Crash- Datei "MEMORY.DMP" muß erzeugt werden. Dies macht man, indem man die entsprechenden Einstellungen (unten) erzeugt.
Die Auslageungsdatei soll hierfür mindestens so groß bemessen werden, wie der eingesetzte RAM.
In Systemeigenschaften > Erweitert > Starten und Wiederherstellen diese Einstellungen vornehmen:



Die Größe der Auslagerungsdatei sollte mindestens dem RAM entsprechen. Dessen (flüchtiges) Abbild wird ja in die Auslagerungsdatei auf der Festplatte geschrieben.

Neu booten!

Danach sollten die entsprechenden Registry- Einträge im Pfad
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]



stehen.
Bei einem Absturz, der einen Bluescreen verursacht, wird nun automatisch der Inhalt des RAM in die Auslagerungsdatei geschrieben.
Das dauert einige Minuten!
Nach dem Neustart hat man eine Datei "MEMORY.DMP", welche alls Informationen des RAM beinhaltet.
Diese muß nun ausgewertet werden.

Ich benötigen also ein Tool, welches uns diese Dateien erstellt und analysiert. Das lade ich mir von Microsoft von dieser Seite herunter:

http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx

Direktdownload:
http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.6.07.5.exe

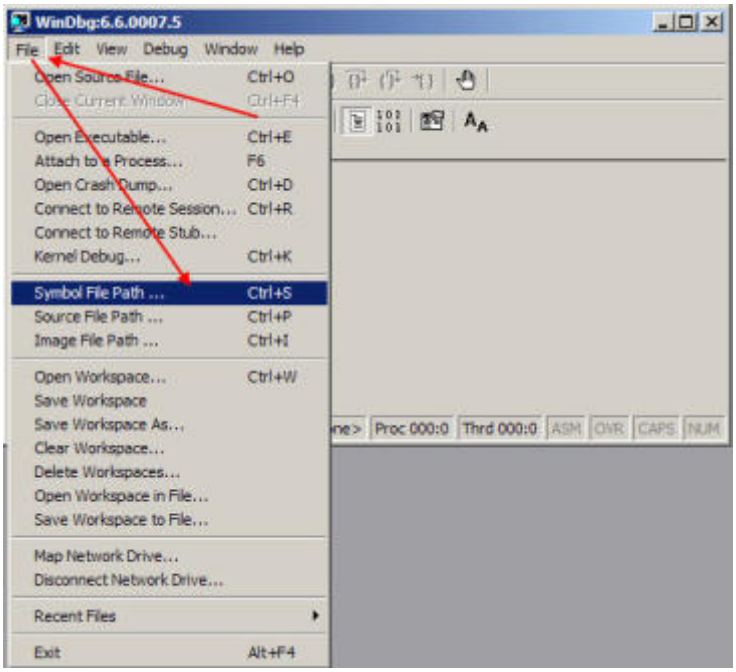
Downloaden und installieren.

Einen Ordner "**symbols**" in "C" anlegen:
C:\symbols

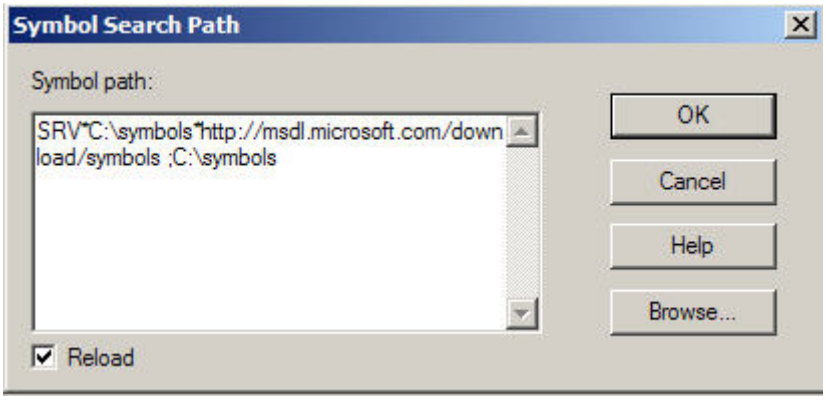
So, nun hat sich der PC mit einem Bluescreen verabschiedet und ein Speicherabbild erstellt. das kann dauern! Er, der PC vermeldet das mit
"Speicherabbild wurde erstellt"
 Nun neu booten und WinDbg.exe starten

WinDbg benötigt Informations-Dateien – diese befinden sich im Kernel-Dump.
Diese Daten müssen natürlich zu installierten Windows passen. Das wird automatisch erledigt:

Im Menu 'File' >Symbol File Path< auswählen:



und eingeben:
SRV*C:\symbols*http://msdl.microsoft.com/download/symbols :



Haken bei "Reload" rein, ok.

Nun im "File- Menü" den Befehl "Open Crash Dump" auswählen.
Dort auf die erzeugte "MEMORY.DMP" verweisen.
Nunl lädt die Kernel-Dump Datei, die sich in dem oben angegebenen Pfad – "C:\symbols" befindet.
WinDbg lädt jetzt damit die Dump-Datei und die ebenfalls passenden Symboldateien vom Microsoft-Server.
Jetzt füllt sich das Fenster von WinDbg mit Daten, die meisten dürften unverständlich sein.

Ich gehe unten in das Kommandozeilen-Fenster von WinDbg und tippe den Befehl ein:

!analyze –v > und Enter.

WinDbg beginnt nun mit der Analyse des Dump. Wiederum werden alle möglichen und dabei wiederum meist vollkommen unverständliche Informationen angezeigt.
Stehen da aber solche oder ähnliche Meldung da: (Beispiele!)

Probably caused by :xxxDriver.sys (xxxDriver+xxxx)
oder
Followup: memory_corruption

- haben wir schon einen Erfolg erzielt. Denn
>>**xxxDriver**<<
ist nun mit hoher Wahrscheinlichkleit der Name eines fehlerhaften Treibers, der für den Bluescreen verantwortlich war.
Und
>>**memory_corruption**<<
deutet auf einen fehlerhaften RAM hin.
Weitere Gründe für einen Bluescreen, zum Beispiel Fehler im Dateisystem können ebenfalls aus den Meldungen "erraten" werden.

Ich habe in meinen Notizen noch etwas gefunden – Autor "Hajo Schulz".
Leider hab ich den Link nicht mit aufgeschrieben:

Man kann das durchaus erst einmal als "Trockenübung" testen – dazu bietet Windows die Möglichkeit. Navigiere in der Registry zum Schlüssel

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters

und lege dort einen neuen DWORD-Eintrag

CrashOnCtrlScroll

an, dem Du den Wert eine 1 zuweist.
Nach einem Windows-Neustart kannst Du einen Bluescreen auslösen künstlich, indem Du die rechte Strg-Taste gedrückt hältst und zweimal auf "Rollen" drückst.

Diese Tastenkombination zu aktivieren kann selbst dann sinnvoll sein, auch wenn man überhaupt nicht die Absicht hat, mit Bluescreens und dem Debugger zu experimentieren. Gerade auf Notebooks, denen eine Reset-Taste fehlt und die auch das Ziehen des Netzsteckers keinen Erfolg bringt, kann sie eine letzte Rettung sein. Wenn der Rechner sich mal komplett aufgehängt hat. Auch wenn der Mauszeiger sich nicht mehr bewegt und selbst ein Druck auf Strg-Alt-Entf (Affengriff) keine Reaktion zeigt.
Die am Anfang beschriebene Option "Automatischer Neustart" des Rechners nach einem Systemfehler sollte für diesen Zweck allerdings aktiviert sein.

(Diese Angelegenheit hat bei mir allerdings nicht zuverlässig geklappt!)

Jürgen Kirsten

Ich würde mich sehr über Rückmeldungen und Erfahrungen freuen, um diese mit einbauen zu können!