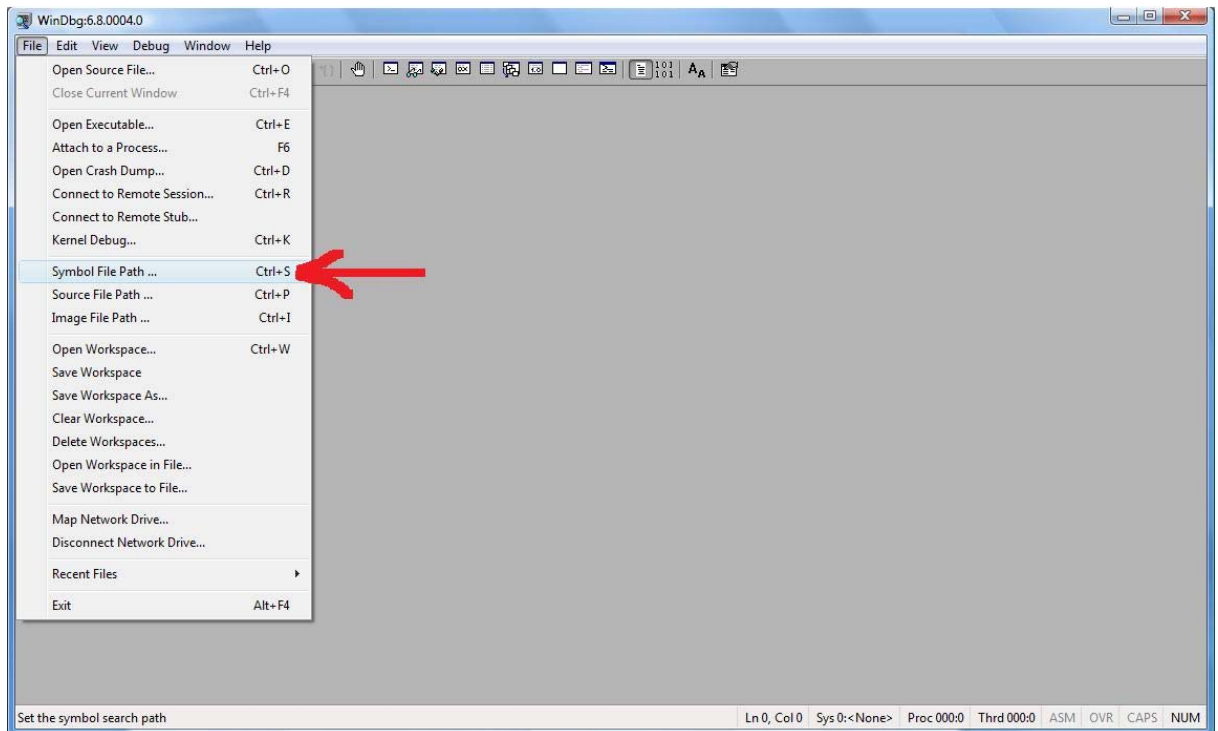
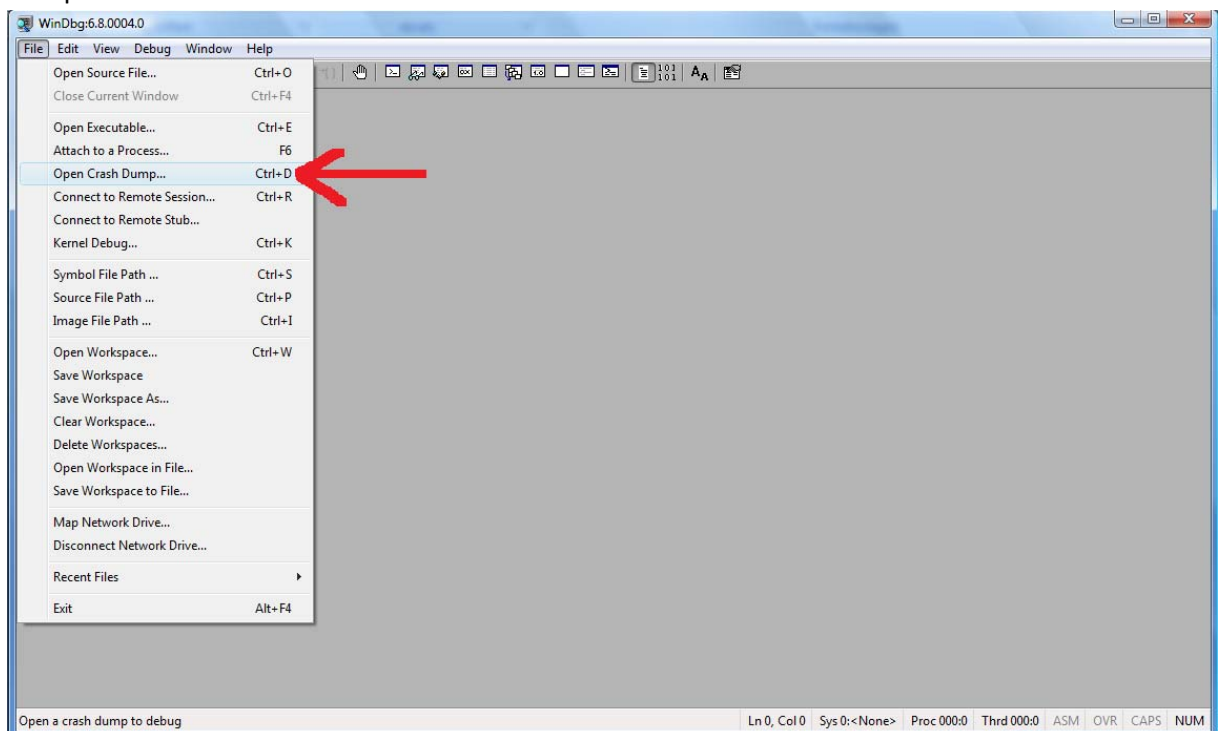


1. Programm herunterladen [Download](#) und als Admin installieren
2. Du startest das Tool als Admin (weil wenn du das nicht als Admin startest geht es nicht^^)
3. Du gehst in „File→Symbol File → Symbol File Path“



4. Dort gibst du dann folgendes ein (ohne Anführungszeichen Bitte!!):  
 „SRV\*c:\windows\symbols\*http://msdl.microsoft.com/download/symbols“
  5. So... dann machst du das Programm erst mal kurz zu, und wenn er fragt, Save Informations for Workspace auf ja klicken.... (sonst musst du immer den File Pfad neu eintragen^^)
  6. Das Programm als Administrator neu starten
  7. So... dann gehst du unter „File→Open Crash Dump“
- Dump“



8. Dann kommst du in ein Auswahlfeld, wo du erst mal nichts findest (du suchst nach \*.dmp Dateien)... dort gehst du in „C:\Windows“ dort sollte, wenn du ganz nach unten scrollst eine Datei „\*.dmp“ (der Stern, weil ich keine abstürze hatte^^ und damit nicht weiß wie die Datei genau heißt) da klickst du drauf und dann auf öffnen.
9. Dann erscheint ein Feld, wo erst mal alle möglichen Informationen angezeigt werden. Dort ist jetzt ganz unten eine Zeile (ab hier sind die Bilder aus dem Internet, da ich keine File da habe um das bei mir zu zeigen^^, und habe auch keine Lust meinen PC deswegen zu killen... die Bilder aus dem Internet tun's auch)

The screenshot shows the WinDbg 6.8.0004.0 interface. The 'Command' window displays a list of loaded modules with their base addresses and file paths. Below the list, a break instruction exception is shown with register values (eax, ebx, ecx, edx, esi, edi, eip, esp, ebp, iopl, cs, ss, ds, es, fs, gs, efl) and a message: '\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols for C:\WINDOWS\ntdll!DbgBreakPoint:'. At the bottom, the command line shows '0:039>'. A red arrow points to the command line.

```

Command
ModLoad: 76dc0000 76de8000 C:\WINDOWS\system32\adslldpc.dll
ModLoad: 76b80000 76bae000 C:\WINDOWS\system32\credui.dll
ModLoad: 76a80000 76a98000 C:\WINDOWS\system32\ATL.DLL
ModLoad: 712d0000 712fe000 C:\WINDOWS\system32\adslldp.dll
ModLoad: 75da0000 75e5d000 C:\WINDOWS\system32\SXS.DLL
ModLoad: 766f0000 76704000 C:\WINDOWS\system32\NTDSAPI.DLL
ModLoad: 71ca0000 71cf8000 C:\WINDOWS\system32\kerberos.dll
ModLoad: 766e0000 766ec000 C:\WINDOWS\system32\cryptdll.dll
ModLoad: 15a30000 15a4a000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15a10000 15a18000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15a70000 15a7a000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15a90000 15a9a000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15ab0000 15ab8000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15ad0000 15ad8000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15af0000 15af8000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15b10000 15b18000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15b30000 15b3a000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15b50000 15b58000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15b70000 15b78000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15bc0000 15bc8000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
ModLoad: 15bd0000 15bd8000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary A
(a0.2a0): Break instruction exception - code 80000003 (first chance)
eax=7ffdf000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c81a3e1 esp=1581ffcc ebp=1581fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\WINDOWS
ntdll!DbgBreakPoint:
7c81a3e1 cc                int     3
0:039>

```

und dort gibst du jetzt (wieder ohne Anführungszeichen):

„!analyze -v“ ein und drückst Enter (wichtig ist hier die Leertaste vor dem Bindestrich !)

10. So... damit nimm das Programm jetzt alle Informationen sorgfältig auseinander. Jetzt, wenn er alles geladen hat, drückst du „STRG+F“ um ein Suchfenster zu öffnen. In das Suchfenster gibst du jetzt (wieder ohne Anführungszeichen): „MODULE\_NAME“ ein und drückst Enter. Falls nichts gefunden wird, ändere einfach die Suchrichtung in „nach oben“.
11. Jetzt ist dort Angegeben, welches Modul/Programm/Treiber etc. für den Absturz verantwortlich ist. Zusätzlich wird eine Zeile darunter neben „IMAGE\_NAME“ der Name des Treibers. Das Modul neben „MODULE\_NAME“ ist blau unterlegt, wenn du dort drauf klickst, bekommst du noch mehr Informationen zum Modul des Absturzes, meistens reicht aber der bloße Name aus, um bei Google was passendes zu finden um das Problem zu lösen.
12. Google öffnen, Module Name eintragen und vorher noch „Blue Screen“ und dann wird geholfen. (wenn man Glück hat, findet man einen Link auf die Microsoft Support Seite)

So noch was: Dieses Tool wird offiziell von Microsoft herausgegeben um sich selbst zu helfen.

Es ist NICHT die Lösung aller Probleme, aber man bekommt wenigstens Informationen.

Ich hoffe dass ich damit helfen konnte.