- 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  $\rightarrow$  Symbol File  $\rightarrow$  Symbol File Path"

Edit View Peleg   Open Gurce File Ctrl-R   Open Case Current Window Ctrl-R   Open Secutable Ctrl-R   Open Cash Dump Ctrl-R   Open Cash Dump Ctrl-R   Somet Files Ctrl-R   Symbol File Path Ctrl-R   Open Workspace Ctrl-R   Doren et File Heile   Save Workspace Ctrl-R   Diconnet File Heile   Save Workspace Ctrl-R   Diconnet Network Drive Reart Files   Bater Files Image	nDbg:6.8.0004.0														> C
Open Source File Ctrl-0   Open Source File Ctrl-F4   Open Executable Ctrl-F4   Open Crash Dump Ctrl-D   Connect to Remote Session Ctrl-R   Connect to Remote Sub Ctrl-R   Connect to Remote Sub Ctrl-F4   Symbol File Path Ctrl-P   Open Workspace Ctrl-I   Open Workspace Ctrl-W   Save Workspace Ctrl-W   Save Workspace File   Open Workspace Ctrl-W   Open Workspace Ctrl-W   Save Workspace In File Save Workspace In File   Save Workspace In File Alt-F4	Edit View Debug Window	v Help	-												
Close Current Window: Ctrl+F4 Open Executable Ctrl+E Attach to a Process F6 Open Crash Dump Ctrl+B Connect to Remote Stab Kernel Debug Ctrl+K Symbol File Path Ctrl+S Symbol File Path Ctrl+D Image File Path Ctrl+1 Open Workspace Ctrl+W Save Workspace As Clear Workspace Delete Workspaces Open Workspace or File Save Workspace or File Save Workspace or File Save Workspace or File Save Workspace or File Etit Alt+F4	Open Source File	Ctrl+0	10 0	2 😡 0	•× 🗆	<b>B</b>		A 1							
Open ExecutableCtrl+EAttach to a ProcessF6Open Cash DumpCtrl-DConnect to Remote SessionCtrl+RSomoor Fine PathCtrl+RSource Fine PathCtrl+PImage File PathCtrl+IOpen WorkspaceCtrl+WSave Workspace AsCtrl+RClear Workspace AsCtrl+RDie Workspace AsCtrl+RDent Workspace TelleMap Network DriveDisconnect Network DriveFileDisconnect Network DriveAlt+F4	Close Current Window	Ctrl+F4													
Attach to a ProcessF6Open Cash DumpCtrl-DConnect to Remote StassionCtrl-RConnect Networe StubCtrl-KSymbol File PathCtrl-SSource File PathCtrl-DOpen WorkspaceCtrl-IOpen WorkspaceCtrl-WSave Workspace AsCtrl-WClear WorkspaceCtrl-WDelete WorkspaceCtrl-WDelete WorkspaceCtrl-WDelete WorkspaceCtrl-WDelete VorkspaceCtrl-WDenet KorkspaceCtrl-WDenet KorkspaceCtrl-WSave WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDeter WorkspaceCtrl-WDisconnect Network DriveCtrl-WDisconnect Network DriveAlt-F4	Open Executable	Ctrl+E													
Open Crash DumpCtrl - DConnect to Remote SessionCtrl - RConnect to Remote StuduCtrl - KSymbol File PathCtrl - PImage File PathCtrl - IOpen WorkspaceCtrl - WSave Workspace AsCtrl - WClear Workspace in FileCtrl - WSave Workspace to FileCtrl - WSave Workspace t	Attach to a Process	F6													
Connect to Remote Session Ctrl+R Connect to Remote Stub Kernel Debug Ctrl+K Symbol File Path Ctrl+S Joure File Path Ctrl+I Image File Path Ctrl+I Image File Path Ctrl+W Save Workspace Cler Workspace As Cler Workspace in File Save Workspace to File Save Workspace to File Save Workspace to File Exit Alt+F4	Open Crash Dump	Ctrl+D													
Kernel DebugCtrl+KSymbol File PathCtrl+PImage File PathCtrl+IOpen WorkspaceCtrl+WSave Workspace AsCtrl+WClear WorkspaceCtrl+IDelete WorkspaceDelete WorkspaceSave Workspace to FileHermite Hermite Hermite Hermite Hermite Hermite HermiteSave Workspace to FileHermite Hermite Hermi	Connect to Remote Session Connect to Remote Stub	Ctrl+R													
Symbol File Path Ctrl+S Source File Path Ctrl+P Image File Path Ctrl+P Mage File Path Ctrl+W Save Workspace Save Workspace As Clear Workspace Delete Workspace Delete Workspace in File Save Workspace to File Map Network Drive Disconnect Network Drive Exit Alt+F4	Kernel Debug	Ctrl+K													
Source File Path Ctrl+P Image File Path Ctrl+I Open Workspace Ctrl+W Save Workspace As Clear Workspace As Clear Workspace Delete Workspace in File Save Workspace to File Save Workspace to File Exit Alt+F4	Symbol File Path	Ctrl+S	2												
Image File Path Ctrl+I Open Workspace Ctrl+W Save Workspace As Clear Workspaces Delete Workspaces Open Workspace to File Save Workspace to File Save Workspace to File Save Workspace to File Exit Alt+F4	Source File Path	Ctrl+P													
Open WorkspaceCtrl+WSave Workspace AsSave Workspace AsClear WorkspaceDelete WorkspaceDelete Workspace in FileSave Workspace in FileSave Workspace to FileSave Workspace to FileBap Network DriveDisconnect Network DriveDisconnect Network DriveAlt+F4	Image File Path	Ctrl+I													
Save Workspace As Clear Workspace Delete Workspace Doen Workspace in File Save Workspace to File Save Workspace to File Disconnect Network Drive Recent Files  Cather Comparison	Open Workspace	Ctrl+W													
Save Workspace As Clear Workspace Delete Workspace in File Save Workspace to File Save Workspace to File Map Network Drive Disconnect Network Drive Recent Files    Katta F4	Save Workspace														
Clear Workspaces   Delete Workspaces   Open Workspace in File   Save Workspace to File   Map Network Drive   Disconnect Network Drive   Exit   Alt+F4	Save Workspace As														
Delete Workspaces   Open Workspace in File   Save Workspace to File     Map Network Drive   Disconnect Network Drive   Exit   Alt+F4	Clear Workspace														
Open Workspace in File   Save Workspace to File   Map Network Drive   Disconnect Network Drive   Recent Files   Exit   Alt+F4	Delete Workspaces														
Save Workspace to File Map Network Drive Disconnect Network Drive Recent Files Leit Alt+F4	Open Workspace in File														
Map Network Drive Disconnect Network Drive Recent Files  Exit Alt+F4	Save Workspace to File														
Disconnect Network Drive Recent Files Exit Alt+F4	Map Network Drive														
Recent Files  Exit Alt+F4	Disconnect Network Drive														
Exit Alt+F4	Recent Files	•													
	Exit	Alt+F4													
In 0. Cold. Sys 0: cNones. Broc 000:0. The d 00:0.0. Aski. OVD. C/	e ormhol search nath								Suctor	200	Proc 000-0	Thed 000-	ASM	OVP	CAP

- 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"



- 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)

Pia 2000 - Wildburg 8,6,0004.0
Eile Fair New Tepha William Helb
Command 🛛 🛛 🖾
ModLoad: 76dc0000 76de8000 C:\WINDOWS\system32\adsldpc.dll
ModLoad: 76b80000 76bae000 C:\WINDOWS\system32\credui.dll
ModLoad: 76a80000 76a98000 C:\WINDOWS\system32\ATL.DLL
ModLoad: 712d0000 712fe000 C:\WINDOWS\system32\adsldp.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:\WINDOW5\system32\cryptdll.dll
ModLoad: 15a30000 15a4a000 C:\UINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary &
ModLoad: 15a10000 15a18000 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary &
ModLoad: 15a/0000 15a/a000 C: WINDOWS Microsoft.NEI\Framework\v2.0.50/2/\Temporary &
ModLoad: 15a90000 15a9a0000 C:\WINDOWS\Microsoft.NEI\Framework\v2.0.50/2/\lemporary #
ModLoad: ISab0000 ISab0000 C:\WINDOWS\MICFOSOIT.NEI\FFamework\V2.0.50/2/\Temporary #
ModLoad: 15ad0000 15ad0000 C: WINDOWS MICROSOIT. NEL SFAmework V2.0.50/2/\lemporary #
ModLoad: ISAIUUUU ISAIUUUU C: WINDOWS MICROSOIT.NEI FRAmework V2.0.50/2/ Viemporary #
ModLoad: 15D10000 15D10000 C. WINDOWS Microsoft METYFAMEWork V2.0.50727 Temporary &
Modicad: 15b50000 15b50000 C:\WINDOWS\Wicrosoft NET\Framework\v2.0.50727\Temporary &
Modicad: 15b50000 15b50000 C:\WINDOWS\Microsoft NET\Framework\v2.0.50727\Temporary A
Modicad: 15b/0000 15b/0000 C. WINDOWS Microsoft NET Framework/v2.0.50727 Temporary /
ModLoad: 15bd0000 15bd8000 C:\WINDOWS\Microsoft NET\Framework\v2.0.50727\Temporary
(af0 2a0): Break instruction exception - code 80000003 (first chance)
eax=7ffdf000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
ein=7c81a3e1 esn=1581ffcc ebn=1581fff4 ion1=0 ny un ei nl zr na ne nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 ef1=00000246
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\WINDOWS
ntdll!DbgBreakPoint:
7c81a3e1 cc int 3
0:039>
In D. Col D. Svs D: <local> Proc 000:af0 Thrd 039:2a0 ASM_OVR_ICAPS_NUM</local>

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.