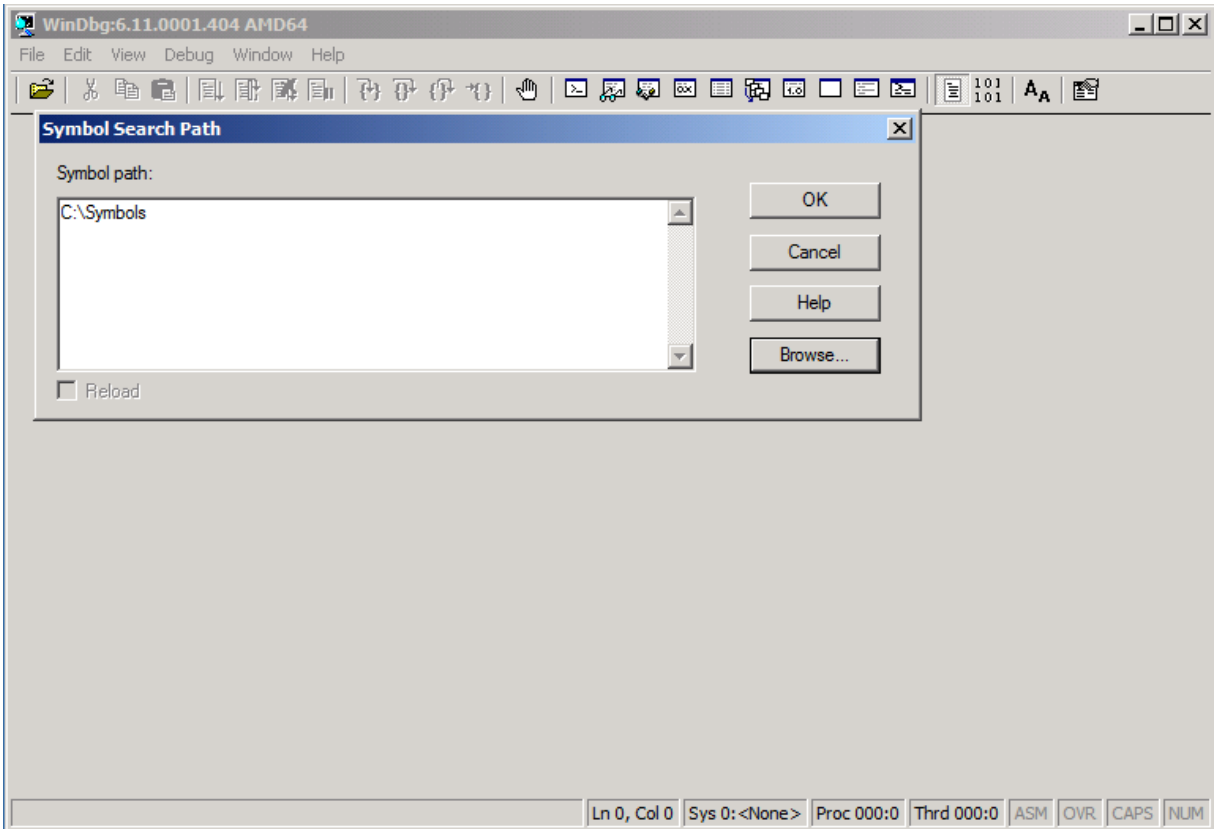
Forefront TMG BSOD in FWENG.SYS

Grundlagen

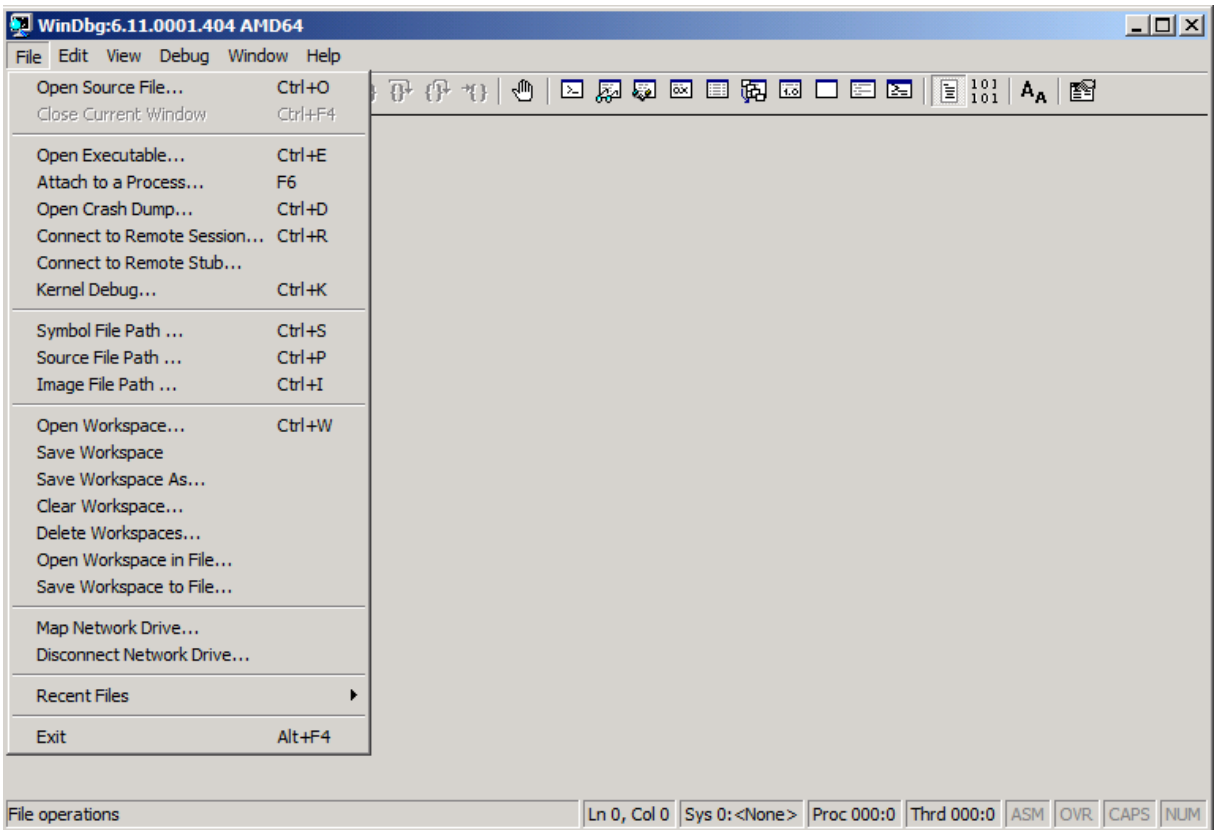
http://support.microsoft.com/kb/315263
http://www.microsoft.com/whdc/devtools/debugging/default.mspx
http://support.microsoft.com/kb/254649/

WinDbg ausfuehren

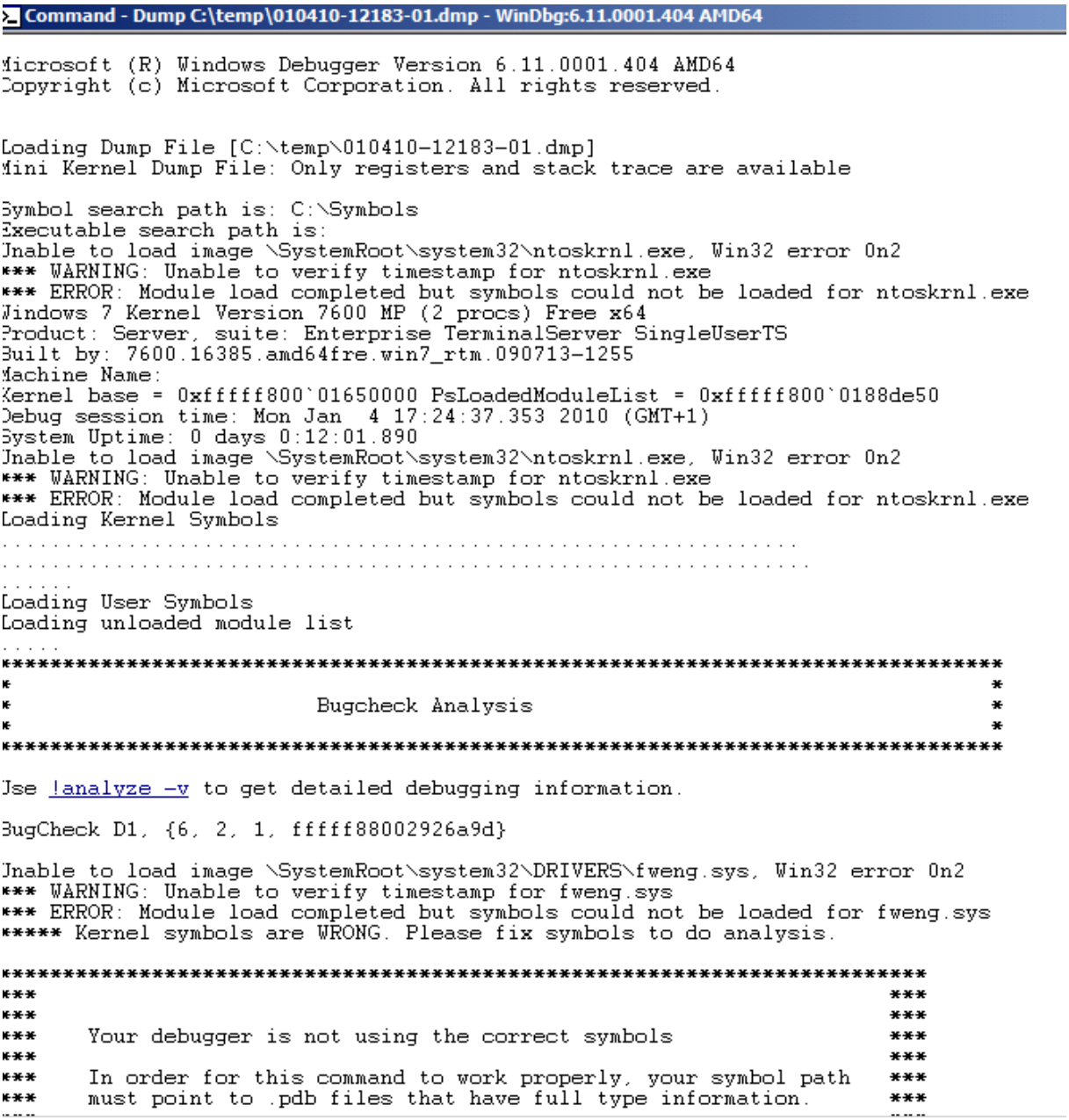
Symbol Path festlegen (Standard Symbole von der MS Webseite)



Open Crash Dump



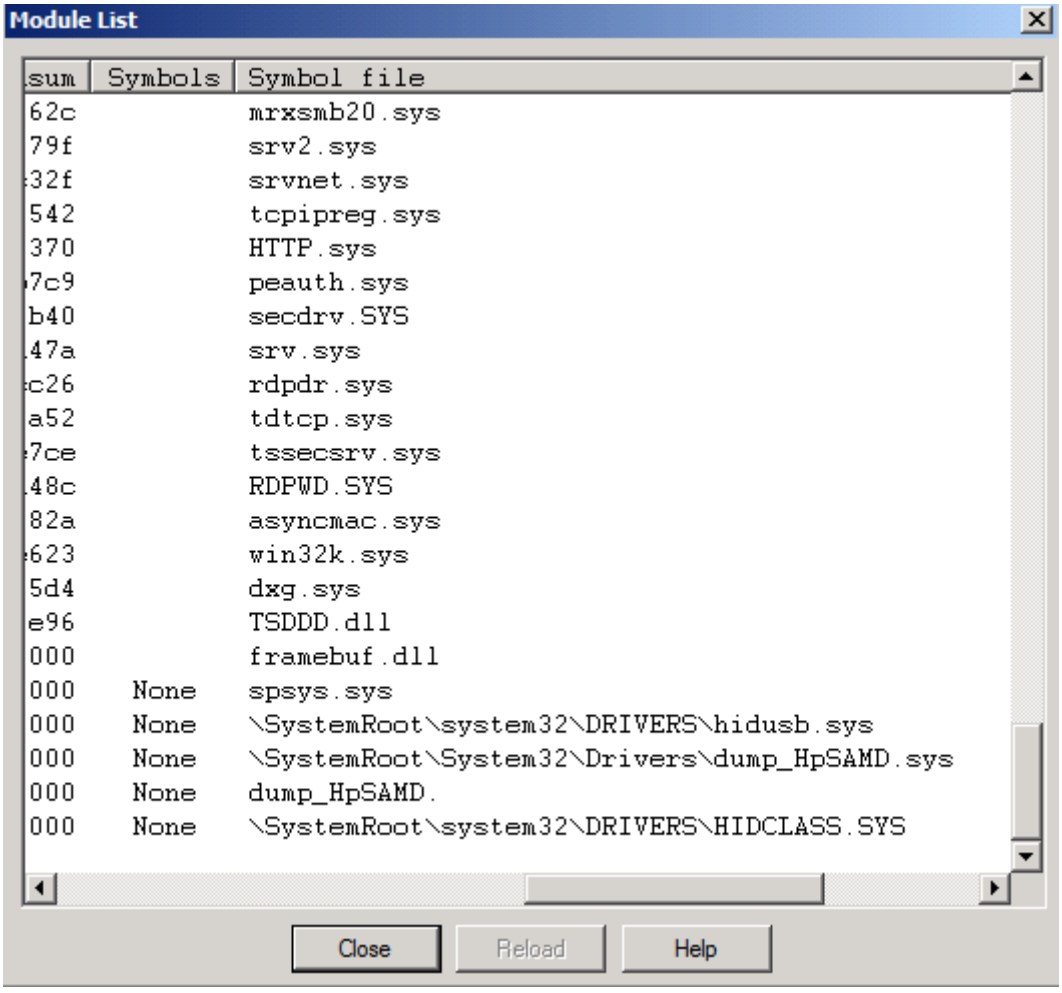
Symbols fuer FWENG.SYS koennen nicht geladen werden



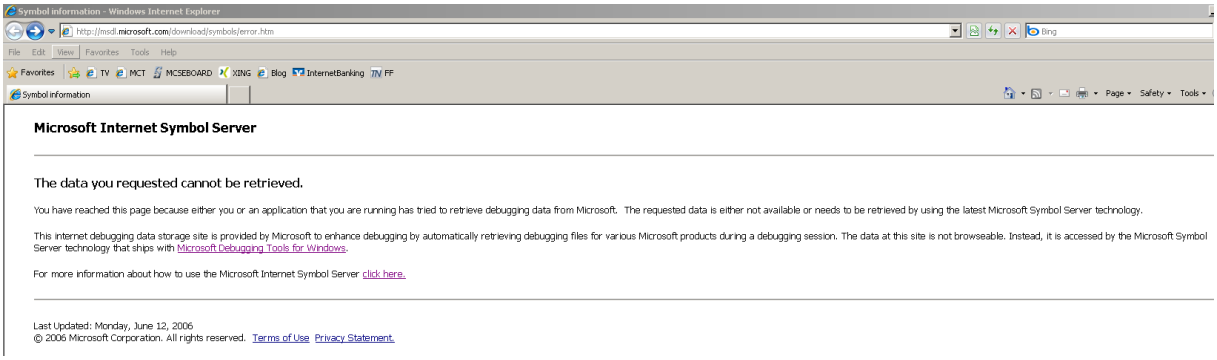
Modulname FWENG

```
ADDITIONAL_DEBUG_TEXT:
Use '!findthebuild' command to search for the target build information.
If the build information is available, run '!findthebuild -s ; .reload' to set symbol path and load symbols.

MODULE_NAME: fweng

FAULTING_MODULE: fffff80001650000 nt

DEBUG_FLR_IMAGE_TIMESTAMP:  4ad4f8bc

WRITE_ADDRESS: unable to get nt!MmSpecialPoolStart
unable to get nt!MmSpecialPoolEnd
unable to get nt!MmPoolCodeStart
unable to get nt!MmPoolCodeEnd
 0000000000000006

CURRENT_IRQL:  0

FAULTING_IP:
fweng+56a9d
fffff880`02926a9d 66891401        mov     word ptr [rcx+rax],dx

CUSTOMER_CRASH_COUNT:  1

DEFAULT_BUCKET_ID:  DRIVER_FAULT_SERVER_MINIDUMP

BUGCHECK_STR:  0xD1

LAST_CONTROL_TRANSFER:  from fffff800016c1469 to fffff800016c1f00

STACK_TEXT:
fffff800`0145cc58 fffff800`016c1469 : 00000000`0000000a 00000000`00000006 00000000`00000002 00000000`00000001 : nt+0x71f00
fffff800`0145cc60 00000000`0000000a : 00000000`00000006 00000000`00000002 00000000`00000001 fffff880`02926a9d : nt+0x71469
fffff800`0145cc68 00000000`00000006 : 00000000`00000002 00000000`00000001 fffff880`02926a9d fffffa80`02b9c3d0 : 0xa
fffff800`0145cc70 00000000`00000002 : 00000000`00000001 fffff880`02926a9d fffffa80`02b9c3d0 00000000`00000000 : 0x6
fffff800`0145cc78 00000000`00000001 : fffff880`02926a9d fffffa80`02b9c3d0 00000000`00000000 00000000`00000000 : 0x2
fffff800`0145cc80 fffff880`02926a9d : fffffa80`02b9c3d0 00000000`00000000 00000000`00000000 00000000`00000000 : 0x1
fffff800`0145cc88 fffffa80`02b9c3d0 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : fweng+0x56a9d
fffff800`0145cc90 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0xfffffa80`02l


STACK_COMMAND:  kb

FOLLOWUP_IP:
fweng+56a9d
fffff880`02926a9d 66891401        mov     word ptr [rcx+rax],dx

SYMBOL_STACK_INDEX:  6

SYMBOL_NAME:  fweng+56a9d
```

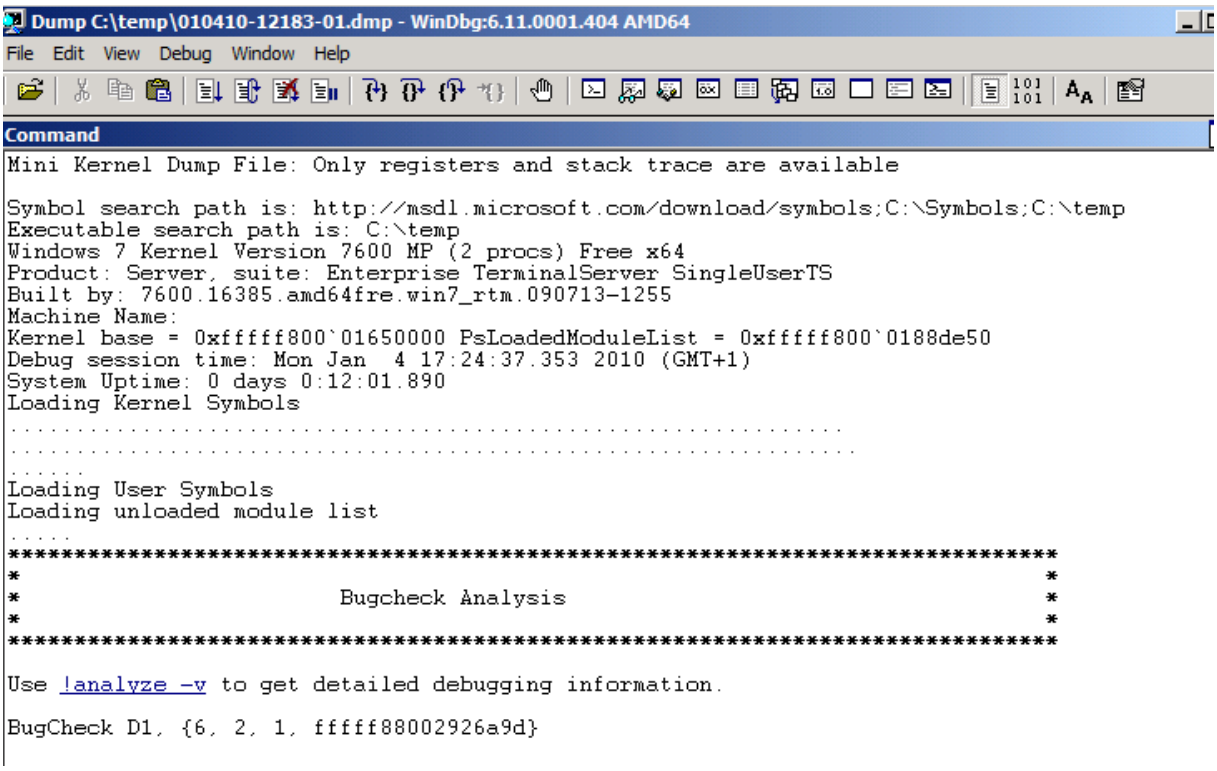
Symbol Files



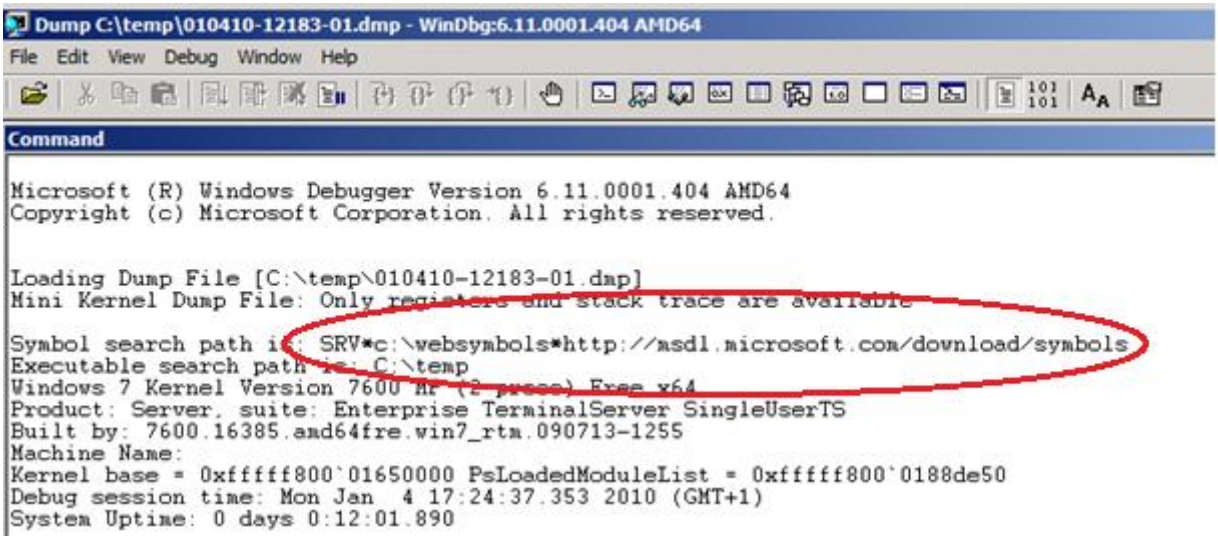
Nichts lokal, also Symbol File Server kontaktieren



Symbol Search Path zum Symbol File Server angeben …



.. oder lokal downloaden (siehe Markierung)



OK, IRQL not less or equal. MSPADMIN.EXE ist auch beteiligt