



# Debugging.TV

Frame 0x02

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

[DumpAnalysis.com](http://DumpAnalysis.com)

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

**OPENTASK**

Iterative and Incremental Publishing

# Troubleshooting Symbols

# App Version 1

```
0:000> .sympath+ C:\DebuggingTV\DebuggingTV02\x64\Release\Version1
```

```
0:000> .reload
```

```
.....
```

```
0:000> kL
```

Child-SP	RetAddr	Call Site
00000000`001cfb38	00000000`76e7e6fa	user32!ZwUserGetMessage+0xa
00000000`001cfb40	00000001`3fa610d0	user32!GetMessageW+0x34
00000000`001cfb70	00000001`3fa61494	DebuggingTV02!wWinMain+0xd0
00000000`001cfbd0	00000000`76d5cdcd	DebuggingTV02!__tmainCRTStartup+0x154
00000000`001cfc80	00000000`76f7c6e1	kernel32!BaseThreadInitThunk+0xd
00000000`001cfcb0	00000000`00000000	ntdll!RtlUserThreadStart+0x1d

```
0:000> ub 00000001`3fa610d0
```

```
DebuggingTV02!wWinMain+0xac [c:\debuggingtv\debuggingtv02\debuggingtv02\debuggingtv02.cpp @ 50]:  
00000001`3fa610ac call    qword ptr [DebuggingTV02!_imp_TranslateMessage (00000001`3fa66228)]  
00000001`3fa610b2 lea    rcx,[rsp+20h]  
00000001`3fa610b7 call   qword ptr [DebuggingTV02!_imp_DispatchMessageW (00000001`3fa66220)]  
00000001`3fa610bd lea    rcx,[rsp+20h]  
00000001`3fa610c2 xor    r9d,r9d  
00000001`3fa610c5 xor    r8d,r8d  
00000001`3fa610c8 xor    edx,edx  
00000001`3fa610ca call   qword ptr [DebuggingTV02!_imp_GetMessageW (00000001`3fa66238)]
```

# App Version 2

```
0:000> .sympath+ C:\DebuggingTV\DebuggingTV02\x64\Release\Version1
```

```
0:000> .reload
```

```
0:000> kL
```

Child-SP	RetAddr	Call Site
00000000`001dfa88	00000000`76e7e6fa	user32!ZwUserGetMessage+0xa
<b>*** ERROR: Module load completed but symbols could not be loaded for DebuggingTV02.exe</b>		
00000000`001dfa90	00000001`3f3f10d0	user32!GetMessageW+0x34
00000000`001dfac0	00000001`3f3f1494	DebuggingTV02+0x10d0
00000000`001dfb20	00000000`76d5cdcd	DebuggingTV02+0x1494
00000000`001dfbd0	00000000`76f7c6e1	kernel32!BaseThreadInitThunk+0xd
00000000`001dfc00	00000000`00000000	ntdll!RtlUserThreadStart+0x1d

```
0:000> .reload /f /i DebuggingTV02.exe
```

```
0:000> kL
```

Child-SP	RetAddr	Call Site
00000000`001dfa88	00000000`76e7e6fa	user32!ZwUserGetMessage+0xa
00000000`001dfa90	<b>00000001`3f3f10d0</b>	user32!GetMessageW+0x34
00000000`001dfac0	<b>00000001`3f3f1494</b>	<b>DebuggingTV02!wWinMain+0xd0</b>
00000000`001dfb20	00000000`76d5cdcd	<b>DebuggingTV02!__tmainCRTStartup+0x154</b>
00000000`001dfbd0	00000000`76f7c6e1	kernel32!BaseThreadInitThunk+0xd
00000000`001dfc00	00000000`00000000	ntdll!RtlUserThreadStart+0x1d



# ...continue

```
0:000> .asm no_code_bytes
```

```
Assembly options: no_code_bytes
```

```
0:000> ub 00000001`3f3f10d0
```

```
DebuggingTV02!wWinMain+0xac [c:\debuggingtv\debuggingtv02\debuggingtv02\debuggingtv02.cpp @ 50]:
```

```
00000001`3f3f10ac call    qword ptr [DebuggingTV02!_imp_TranslateMessage (00000001`3f3f6228)]
00000001`3f3f10b2 lea    rcx,[rsp+20h]
00000001`3f3f10b7 call    qword ptr [DebuggingTV02!_imp_DispatchMessageW (00000001`3f3f6220)]
00000001`3f3f10bd lea    rcx,[rsp+20h]
00000001`3f3f10c2 xor    r9d,r9d
00000001`3f3f10c5 xor    r8d,r8d
00000001`3f3f10c8 xor    edx,edx
00000001`3f3f10ca call   qword ptr [DebuggingTV02!_imp_GetMessageW (00000001`3f3f6238)]
```

```
0:000> ub 00000001`3f3f1494
```

```
DebuggingTV02!__tmainCRTStartup+0x133 [f:\dd\vctools\crt_bld\self_64_amd64\crt\src\crt0.c @ 275]:
```

```
00000001`3f3f1473 test   byte ptr [rsp+6Ch],1
00000001`3f3f1478 movzx  edx,word ptr [rsp+70h]
00000001`3f3f147d mov    r9d,0Ah
00000001`3f3f1483 cmovne r9d,edx
00000001`3f3f1487 mov    r8,rax
00000001`3f3f148a xor    edx,edx
00000001`3f3f148c mov    rcx,rdi
00000001`3f3f148f call   DebuggingTV02!wWinMain (00000001`3f3f1000)
```

# App Version 4

```
0:000> .sympath+ C:\DebuggingTV\DebuggingTV02\Release\Version1
```

```
0:000> .reload
```

```
0:000> .reload /f /i DebuggingTV02.exe
```

```
0:000> kL
```

```
ChildEBP RetAddr
```

```
001bf968 7675199a ntdll!KiFastSystemCallRet
```

```
001bf96c 767519cd user32!NtUserGetMessage+0xc
```

```
001bf988 003f1045 user32!GetMessageW+0x33
```

```
001bf9a8 003f10f2 DebuggingTV02!wWinMain+0x45
```

```
001bf9ac 031f0197 DebuggingTV02!MyRegisterClass+0x2
```

```
WARNING: Frame IP not in any known module. Following frames may be wrong.
```

```
001bf9d8 003f141d 0x31f0197
```

```
001bfa3c 003f2914 DebuggingTV02!_tmainCRTStartup+0x139
```

```
001bfa68 76573833 DebuggingTV02!__security_init_cookie+0x85
```

```
001bfa74 77c1a9bd kernel32!BaseThreadInitThunk+0xe
```

```
001bfab4 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
0:000> ub 031f0197
```

```
^ Unable to find valid previous instruction for 'ub 031f0197'
```

# ...continue

```
0:000> .sympath+ C:\DebuggingTV\DebuggingTV02\Release\Version4
```

```
0:000> .reload
```

```
0:000> kL
```

```
ChildEBP RetAddr
```

```
001bf968 7675199a ntdll!KiFastSystemCallRet
```

```
001bf96c 767519cd user32!NtUserGetMessage+0xc
```

```
001bf988 003f1045 user32!GetMessageW+0x33
```

```
001bf9a8 003f10f2 DebuggingTV02!MessageLoop+0x45
```

```
001bf9d8 003f141d DebuggingTV02!wWinMain+0xa2
```

```
001bfa68 76573833 DebuggingTV02!__tmainCRTStartup+0x11a
```

```
001bfa74 77c1a9bd kernel32!BaseThreadInitThunk+0xe
```

```
001bfab4 00000000 ntdll!_RtlUserThreadStart+0x23
```

Debugging.TV