Debugging.TV

Frame 0x03

Presenter: Dmitry Vostokov

Troubleshooting Symbols

Symbol Problem

```
0:000> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
0018f234 76ce162d ntdll!NtWaitForMultipleObjects+0x15
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsEx+0x8e
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!CheckForReadOnlyResource+0x175
0018f318 76d098f8 kernel32!CheckForReadOnlyResource+0x212
0018f328 76d09875 kernel32!UnhandledExceptionFilter+0x163
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0xe0
0018ffd4 77b89ed5 ntdll!RtlKnownExceptionFilter+0xb7
0018ffec 00000000 ntdll!RtlInitializeExceptionChain+0x36

0:000> .symfix c:\mss

0:000> .reload
.....................
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dll -
```

Bad Trace

```
0:000> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
0018f234 76ce162d ntdll!NtWaitForMultipleObjects+0x15
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsExImplementation+0xe0
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!WerpReportFaultInternal+0x186
0018f318 76d098f8 kernel32!WerpReportFault+0x70
0018f328 76d09875 kernel32!BasepReportFault+0x20
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0x1af
0018ffd4 77b89ed5 ntdll!RtlKnownExceptionFilter+0xb7
0018ffec 00000000 ntdll!RtlInitializeExceptionChain+0x36
```

Symbol Tracing

```
0:000> !sym noisy
noisy mode - symbol prompts on

0:000> .reload
.....................
SYMSRV:  c:\mss\wntdll.pdb\FC9DB05873374DB5985BABAA3F8F734F2\wntdll.pd_
         The file or directory is corrupted and unreadable.
DBGHELP: wntdll.pdb - file not found
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dll -
DBGHELP: ntdll - export symbols
```

Symbol Fix

```
C:\mss\wntdll.pdb\FC9DB05873374DB5985BABAA3F8F734F2>expand wntdll.pd_ wntdll.pdb

Microsoft (R) File Expansion Utility  Version 6.1.7600.16385
Copyright (c) Microsoft Corporation. All rights reserved.

Copying wntdll.pd_ to wntdll.pdb.
wntdll.pd_: 2124800 bytes copied.


C:\mss\wntdll.pdb\FC9DB05873374DB5985BABAA3F8F734F2>
```

```
0:000> .reload
.....................
DBGHELP: ntdll - public symbols
        c:\mss\wntdll.pdb\FC9DB05873374DB5985BABAA3F8F734F2\wntdll.pdb
```

Good Trace

```
0:000> !sym quiet
quiet mode - symbol prompts on

0:000> k
ChildEBP RetAddr
0018f198 75670bdd ntdll!NtWaitForMultipleObjects+0x15
0018f234 76ce162d KERNELBASE!WaitForMultipleObjectsEx+0x100
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsExImplementation+0xe0
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!WerpReportFaultInternal+0x186
0018f318 76d098f8 kernel32!WerpReportFault+0x70
0018f328 76d09875 kernel32!BasepReportFault+0x20
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0x1af
0018f3bc 77bc0cd4 ntdll!__RtlUserThreadStart+0x62
0018f3d0 77bc0b71 ntdll!_EH4_CallFilterFunc+0x12
0018f3f8 77b96ac9 ntdll!_except_handler4+0x8e
0018f41c 77b96a9b ntdll!ExecuteHandler2+0x26
0018f4cc 77b6010f ntdll!ExecuteHandler+0x24
0018f4cc 0041ff21 ntdll!KiUserExceptionDispatcher+0xf
[...]
```

Debugging.TV