



Debugging.TV

Frame 0x05

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

DumpAnalysis.com

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

OPENTASK

Iterative and Incremental Publishing

Debugging Improvisation 0x02

Topics

- Software breakpoints
- Software breakpoint implementation
- Hardware breakpoints
- Debug registers
- !Ad

Commands

.logopen	bp
kL	u
.reload	bc
~<>s	bl
x	.bpcmds
.symfix	~
.sympath	Ba
rM	uf

Software Breakpoint

0:000> * Debugger View

0:000> U TestWER64!CAboutDlg::CAboutDlg

TestWER64!CAboutDlg::CAboutDlg:

```
00000001`400249d0 48894c2408      mov     qword ptr [rsp+8],rcx
00000001`400249d5 4883ec38        sub     rsp,38h
00000001`400249d9 48c7442420feffff mov     qword ptr [rsp+20h],0FFFFFFFFFFFFFFEh
00000001`400249e2 4533c0         xor     r8d,r8d
00000001`400249e5 ba64000000     mov     edx,64h
00000001`400249ea 488b4c2440     mov     rcx,qword ptr [rsp+40h]
00000001`400249ef e844e9fdff     call   TestWER64!CDialog::CDialog (00000001`40003338)
00000001`400249f4 90            nop
```

0:000> * Another Debugger View

0:000> U TestWER64!CAboutDlg::CAboutDlg

TestWER64!CAboutDlg::CAboutDlg:

```
00000001`400249d0 cc          int     3
00000001`400249d1 894c2408      mov     dword ptr [rsp+8],ecx
00000001`400249d5 4883ec38        sub     rsp,38h
00000001`400249d9 48c7442420feffff mov     qword ptr [rsp+20h],0FFFFFFFFFFFFFFEh
00000001`400249e2 4533c0         xor     r8d,r8d
00000001`400249e5 ba64000000     mov     edx,64h
00000001`400249ea 488b4c2440     mov     rcx,qword ptr [rsp+40h]
00000001`400249ef e844e9fdff     call   TestWER64!CDialog::CDialog (00000001`40003338)
```

Hardware Breakpoint

```
0:000> rM20
```

```
dr0=0000000000000000 dr1=0000000000000000 dr2=0000000000000000  
dr3=0000000000000000 dr6=0000000000000000 dr7=0000000000000000  
USER32!NtUserGetMessage+0xa:  
00000000`774dc92a c3 ret
```

```
0:000> ba e 1 TestWER64!CAboutDlg::CAboutDlg
```

```
0:000> b1
```

```
0 e 00000001`400249d0 e 1 0001 (0001) 0:**** TestWER64!CAboutDlg::CAboutDlg
```

```
0:000> g
```

```
(5e0.140): Break instruction exception - code 80000003 (first chance)
```

```
ntdll!DbgBreakPoint:
```

```
00000000`7760e910 cc int 3
```

```
0:001> rM20
```

```
dr0=00000001400249d0 dr1=0000000000000000 dr2=0000000000000000  
dr3=0000000000000000 dr6=00000000ffff0ff0 dr7=00000000000000401  
ntdll!DbgBreakPoint:  
00000000`7760e910 cc int 3
```

!Ad Hardcore Technical Support Training

December 9, 2011: [Advanced Windows Memory Dump Analysis](#)

January, 2012: [Accelerated Windows Memory Dump Analysis](#)

Training Schedule

Debugging.TV