Debugging.TV

Frame 0x18

Presenter: Dmitry Vostokov

Topics

- Visual Studio 2012
- WinDbg (WinDbg.org)
- Stack Frame Navigation w/o source code
- Stack Frame Navigation with source code

Modeling Example

- Modified for crash dump analysis GDB for WinDbg Users
- Compiled for x64 under Visual C++ 2012
- LocalDumps on Windows 7
- WinDbg from Windows SDK for Windows 8

Source Fragment

```
int main()
{
        int   local_0 = 0;
        char *hello = "Hello Crash!";

        g_val_1 = 1;
        g_val_2 = '1';

        func_1(g_val_1, g_val_2, (int *)g_pval_1, (char *)g_pval_2);
        return 0;
}

void func_1(int param_1, char param_2, int *param_3, char *param_4)
{
        int local_1 = 1;

        g_val_1 = 2;
        g_val_2 = '2';

        param_3 = &local_1;

        func_2(g_val_1, g_val_2, param_3, param_4);
}
```

WinDg Log Fragment

```
0:000> knL
 # Child-SP          RetAddr           Call Site
[…]
0c 00000000`0031fb70 00000001`3f9f11a5 FrameNavigation!func_4+0x1f
0d 00000000`0031fbb0 00000001`3f9f1134 FrameNavigation!func_3+0x55
0e 00000000`0031fbf0 00000001`3f9f10b4 FrameNavigation!func_2+0x64
0f 00000000`0031fc30 00000001`3f9f1049 FrameNavigation!func_1+0x64
10 00000000`0031fc70 00000001`3f9f1453 FrameNavigation!main+0x49
[…]

0:000> .frame 10
10 00000000`0031fc70 00000001`3f9f1453 FrameNavigation!main+0x49

0:000> dpa hello L1
00000000`0031fc98  00000001`3f9f21b8 "Hello Crash!“

0:000> .frame f
0f 00000000`0031fc30 00000001`3f9f1049 FrameNavigation!func_1+0x64

0:000> dc local_1 L1
00000000`0031fc50  00000001                                ....

0:000> dp param_3 L1
00000000`0031fc80  00000000`0031fc50

0:000> dpp param_3 L1
00000000`0031fc80  00000000`0031fc50 00000000`00000001
```

Commands

```
.logopen
k
kL
kn
.frame
dv /i /V
.sympath
uf
```

```
!lmi
.sympath
.srcpath
dc
dp
dpa
dp @@c++
dpp
```

!Ad Hardcore Software Support Training

December 7-17, 2012	Accelerated Windows Software Trace Analysis
February 20-25, 2013	Accelerated Windows Memory Dump Analysis
2013	Philosophy of Software Diagnostics (FREE)
January, 2013	Pattern-Based Software Diagnostics (FREE)
2013	Accelerated Windows Malware Analysis
2013	The New Old Debugging

Debugging^3 Coming soon

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV