Integrating WinDbg and IDA for Improved Code Flow Analysis

IDA is hands down the best tool for static analysis. Its debugger on the other hand, when compared to the power of WinDbg is certainly lacking, IMHO. As such, I find myself wasting too much time switching between windows and manually highlighting and commenting instructions in IDA as I trace through them in WinDbg. Fortunately, the power of IDApython can be unleashed to reduce this tedium.

I was reading an older TippingPoint MindshaRE article from Cody Pierce entitled “Hit Tracing in WinDbg[1]” and was inspired by his ideas to implement my own IDApython script to better integrate WinDbg with IDA. While, I may be recreating many of his efforts, my primary intent was to get better at scripting in IDApython while improving upon my static/dynamic analysis workflow.

The purpose of my script is to parse WinDbg log files for module base addresses, instruction addresses, references to register values, and pointer dereferences. Then, for every instruction you hit in your debug session, the corresponding instructions will be colored and commented accordingly and in a module base address-agnostic fashion.

To get started, your WinDbg log file will need to display the following:

• Disassembly of current instruction

• Effective address for current instruction

• Register state

• Listing of loaded modules (optional, but highly recommended)

The first three items should be enabled by default but can be re-enabled with the ‘.prompt\_allow’ command. Your output should look like the following:

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000001

eip=00491469 esp=0020e348 ebp=0020e388 iopl=0 nv up ei pl zr na pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246

calc!CCalcEngine::DoOperation+0x6be:

00491469 e8074efeff call calc!divrat (00476275)

The reason it is ideal to include module base addresses in your log file is so that effective addresses can be calculated as offsets then added to the base address of the module in IDA. This helps because the module base address in WinDbg is often different than the base address in IDA. Also, this avoids having to modify the dumpfile to match IDA or rebase the addresses in IDA – both, a pain and unnecessary. My script parses the output of ‘lmp’ in WinDbg which outputs the base addresses of loaded modules minus symbol information.

To continue riding Cody’s coattails, I’ll be analyzing the DoOperation function (0x00495001-0x00495051) in calc.exe as he did. I determined the beginning and ending addresses of the function with the following commands:

0:000> X calc!\*DoOperation\*

00495001 calc!CCalcEngine::DoOperation =

0:000> BP 00495001

0:000> g

Entering in 1000 / 4 in calc

Breakpoint 0 hit

eax=00439220 ebx=0069c420 ecx=0069c278 edx=00000000 esi=0069c278 edi=00000000

eip=00495001 esp=0032e95c ebp=0032ea4c iopl=0 nv up ei pl nz na pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206

calc!CCalcEngine::DoOperation:

00495001 6a1c push 1Ch

Step through function until return instruction

0:000> PT

eax=00000000 ebx=0069c420 ecx=00495051 edx=00445310 esi=0069c278 edi=00000000

eip=00495051 esp=0032e95c ebp=0032ea4c iopl=0 nv up ei pl zr na pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246

calc!CCalcEngine::DoOperation+0xfa:

00495051 c20c00 ret 0Ch

0:000> g

0:004> .logopen "calc.log"

The following dump is the result of the operation 1000/4 in the function without stepping into calls (using the PA command):

Opened log file 'calc.log'

0:004> lmp

start    end        module name

00470000 00530000   calc     <none>

66580000 665bc000   oleacc   <none>

73710000 73742000   WINMM    <none>

739e0000 73adb000   WindowsCodecs <none>

73ae0000 73af3000   dwmapi   <none>

73ca0000 73e30000   gdiplus  <none>

73e30000 73e70000   UxTheme  <none>

73ed0000 7406e000   COMCTL32 <none>

75290000 75299000   VERSION  <none>

75d10000 75d1c000   CRYPTBASE <none>

75f30000 75f7a000   KERNELBASE <none>

76090000 760e7000   SHLWAPI  <none>

760f0000 761c4000   kernel32 <none>

76210000 76293000   CLBCatQ  <none>

762b0000 7637c000   MSCTF    <none>

76380000 763ce000   GDI32    <none>

76460000 76479000   sechost  <none>

76690000 76731000   RPCRT4   <none>

76740000 76809000   USER32   <none>

76810000 768bc000   msvcrt   <none>

768c0000 76a1c000   ole32    <none>

76a20000 76aaf000   OLEAUT32 <none>

76f00000 76f9d000   USP10    <none>

76fa0000 77bea000   SHELL32  <none>

77bf0000 77d2c000   ntdll    <none>

77d30000 77d3a000   LPK      <none>

77d60000 77e00000   ADVAPI32 <none>

77e00000 77e1f000   IMM32    <none>

Unloaded modules:

6d580000 6d59a000   mzvkbd3.dll

77d50000 77d55000   PSAPI.DLL

0:004> g

Breakpoint 0 hit

eax=00384b90 ebx=006cc420 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495001 esp=0020e38c ebp=0020e47c iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation:

00495001 6a1c            push    1Ch

0:000> pa 00495051

eax=00384b90 ebx=006cc420 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495003 esp=0020e388 ebp=0020e47c iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x2:

00495003 b8e1f74b00      mov     eax,offset calc!\_allmul+0x2038 (004bf7e1)

eax=004bf7e1 ebx=006cc420 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495008 esp=0020e388 ebp=0020e47c iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x7:

00495008 e89ed2fdff      call    calc!operator new+0x30 (004722ab)

eax=0020e37c ebx=006cc420 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=0049500d esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286

calc!CCalcEngine::DoOperation+0xc:

0049500d 8bd9            mov     ebx,ecx

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=0049500f esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286

calc!CCalcEngine::DoOperation+0xe:

0049500f 895ddc          mov     dword ptr [ebp-24h],ebx ss:0023:0020e364=00000000

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495012 esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286

calc!CCalcEngine::DoOperation+0x11:

00495012 33ff            xor     edi,edi

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495014 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x13:

00495014 837d0856        cmp     dword ptr [ebp+8],56h ss:0023:0020e390=0000005b

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495018 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x17:

00495018 897dec          mov     dword ptr [ebp-14h],edi ss:0023:0020e374={KERNELBASE!\_except\_handler4 (75f51425)}

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=0049501b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x1a:

0049501b 897dfc          mov     dword ptr [ebp-4],edi ss:0023:0020e384=ffffffff

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=0049501e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x1d:

0049501e 7c0a            jl      calc!CCalcEngine::DoOperation+0xd3 (0049502a) [br=0]

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495020 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x23:

00495020 837d085a        cmp     dword ptr [ebp+8],5Ah ss:0023:0020e390=0000005b

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=00495024 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x27:

00495024 0f8e20f9ffff    jle     calc!CCalcEngine::DoOperation+0x2d (0049494a) [br=0]

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc278 edi=00000000

eip=0049502a esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0xd3:

0049502a 8b750c          mov     esi,dword ptr [ebp+0Ch] ss:0023:0020e394=006cc420

eax=0020e37c ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=0049502d esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0xd6:

0049502d 8b4508          mov     eax,dword ptr [ebp+8] ss:0023:0020e390=0000005b

eax=0000005b ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00495030 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0xd9:

00495030 83c0aa          add     eax,0FFFFFFAAh

eax=00000005 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00495033 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz ac pe cy

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000217

calc!CCalcEngine::DoOperation+0xdc:

00495033 83f80b          cmp     eax,0Bh

eax=00000005 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00495036 esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz ac pe cy

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000297

calc!CCalcEngine::DoOperation+0xdf:

00495036 0f870f050000    ja      calc!CCalcEngine::DoOperation+0x930 (0049554b) [br=0]

eax=00000005 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=0049503c esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz ac pe cy

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000297

calc!CCalcEngine::DoOperation+0xe5:

0049503c ff2485cc4f4900  jmp     dword ptr calc!CCalcEngine::DoOperation+0x96c (00494fcc)[eax\*4] ds:0023:00494fe0=0049132d

eax=00000005 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=0049132d esp=0020e350 ebp=0020e388 iopl=0         nv up ei ng nz ac pe cy

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000297

calc!CCalcEngine::DoOperation+0x517:

0049132d ff75ec          push    dword ptr [ebp-14h]  ss:0023:0020e374=00000000

eax=00000005 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491330 esp=0020e34c ebp=0020e388 iopl=0         nv up ei ng nz ac pe cy

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000297

calc!CCalcEngine::DoOperation+0x51a:

00491330 33c0            xor     eax,eax

eax=00000000 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491332 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x51c:

00491332 40              inc     eax

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491333 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x51d:

00491333 89450c          mov     dword ptr [ebp+0Ch],eax ss:0023:0020e394=006cc420

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491336 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x520:

00491336 8945e8          mov     dword ptr [ebp-18h],eax ss:0023:0020e370=0020ea30

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491339 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x523:

00491339 e8670dfeff      call    calc!\_destroyrat (004720a5)

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=0049133e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x528:

0049133e 33ff            xor     edi,edi

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491340 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x52a:

00491340 897dec          mov     dword ptr [ebp-14h],edi ss:0023:0020e374=00000000

eax=00000001 ebx=006cc278 ecx=006cc278 edx=00000000 esi=006cc420 edi=00000000

eip=00491343 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x52d:

00491343 e83e0dfeff      call    calc!\_createrat (00472086)

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491348 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x532:

00491348 8945ec          mov     dword ptr [ebp-14h],eax ss:0023:0020e374=00000000

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=0049134b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x535:

0049134b ff30            push    dword ptr [eax]      ds:0023:00375548=00000000

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=0049134d esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x537:

0049134d e8870dfeff      call    calc!\_destroynum (004720d9)

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491352 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x53c:

00491352 8b45ec          mov     eax,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491355 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x53f:

00491355 8938            mov     dword ptr [eax],edi  ds:0023:00375548=00000000

eax=00375548 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491357 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x541:

00491357 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491359 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x543:

00491359 8b00            mov     eax,dword ptr [eax]  ds:0023:00379df0=00379d90

eax=00379d90 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=0049135b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x545:

0049135b ff7004          push    dword ptr [eax+4]    ds:0023:00379d94=00000001

eax=00379d90 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=0049135e esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x548:

0049135e e8910dfeff      call    calc!\_createnum (004720f4)

eax=00378300 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=00491363 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x54d:

00491363 8b4dec          mov     ecx,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00378300 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=00491366 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x550:

00491366 8901            mov     dword ptr [ecx],eax  ds:0023:00375548=00000000

eax=00378300 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=00491368 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x552:

00491368 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=0049136a esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x554:

0049136a 8b00            mov     eax,dword ptr [eax]  ds:0023:00379df0=00379d90

eax=00379d90 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=0049136c esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x556:

0049136c 8b4804          mov     ecx,dword ptr [eax+4] ds:0023:00379d94=00000001

eax=00379d90 ebx=006cc278 ecx=00000001 edx=00000000 esi=006cc420 edi=00000000

eip=0049136f esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x559:

0049136f 8d0c8d0c000000  lea     ecx,[ecx\*4+0Ch]

eax=00379d90 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=00491376 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x560:

00491376 51              push    ecx

eax=00379d90 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=00491377 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x561:

00491377 50              push    eax

eax=00379d90 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=00491378 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x562:

00491378 8b45ec          mov     eax,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00375548 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=0049137b esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x565:

0049137b ff30            push    dword ptr [eax]      ds:0023:00375548=00378300

eax=00375548 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=0049137d esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x567:

0049137d e8f90cfeff      call    calc!memcpy (0047207b)

eax=00378300 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491382 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x56c:

00491382 8b45ec          mov     eax,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491385 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x56f:

00491385 83c40c          add     esp,0Ch

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491388 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x572:

00491388 ff7004          push    dword ptr [eax+4]    ds:0023:0037554c=00000000

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=0049138b esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x575:

0049138b e8490dfeff      call    calc!\_destroynum (004720d9)

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491390 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x57a:

00491390 8b45ec          mov     eax,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491393 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x57d:

00491393 897804          mov     dword ptr [eax+4],edi ds:0023:0037554c=00000000

eax=00375548 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491396 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x580:

00491396 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=00491398 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x582:

00491398 8b4004          mov     eax,dword ptr [eax+4] ds:0023:00379df4=003762f8

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=0049139b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x585:

0049139b ff7004          push    dword ptr [eax+4]    ds:0023:003762fc=00000001

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=0049139e esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x588:

0049139e e8510dfeff      call    calc!\_createnum (004720f4)

eax=003770f0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913a3 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x58d:

004913a3 8b4dec          mov     ecx,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=003770f0 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=004913a6 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x590:

004913a6 894104          mov     dword ptr [ecx+4],eax ds:0023:0037554c=00000000

eax=003770f0 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=004913a9 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x593:

004913a9 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=004913ab esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x595:

004913ab 8b4004          mov     eax,dword ptr [eax+4] ds:0023:00379df4=003762f8

eax=003762f8 ebx=006cc278 ecx=00375548 edx=00000000 esi=006cc420 edi=00000000

eip=004913ae esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x598:

004913ae 8b4804          mov     ecx,dword ptr [eax+4] ds:0023:003762fc=00000001

eax=003762f8 ebx=006cc278 ecx=00000001 edx=00000000 esi=006cc420 edi=00000000

eip=004913b1 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x59b:

004913b1 8d0c8d0c000000  lea     ecx,[ecx\*4+0Ch]

eax=003762f8 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=004913b8 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5a2:

004913b8 51              push    ecx

eax=003762f8 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=004913b9 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5a3:

004913b9 50              push    eax

eax=003762f8 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=004913ba esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5a4:

004913ba 8b45ec          mov     eax,dword ptr [ebp-14h] ss:0023:0020e374=00375548

eax=00375548 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=004913bd esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5a7:

004913bd ff7004          push    dword ptr [eax+4]    ds:0023:0037554c=003770f0

eax=00375548 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=00000000

eip=004913c0 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5aa:

004913c0 e8b60cfeff      call    calc!memcpy (0047207b)

eax=003770f0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=004913c5 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5af:

004913c5 83c40c          add     esp,0Ch

eax=003770f0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=004913c8 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x5b2:

004913c8 ff36            push    dword ptr [esi]      ds:0023:006cc420=00379df0

eax=003770f0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000000

eip=004913ca esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x5b4:

004913ca e8d60cfeff      call    calc!\_destroyrat (004720a5)

eax=00000000 ebx=006cc278 ecx=75f376dc edx=00360174 esi=006cc420 edi=00000000

eip=004913cf esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5b9:

004913cf 893e            mov     dword ptr [esi],edi  ds:0023:006cc420=00379df0

eax=00000000 ebx=006cc278 ecx=75f376dc edx=00360174 esi=006cc420 edi=00000000

eip=004913d1 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5bb:

004913d1 e8b00cfeff      call    calc!\_createrat (00472086)

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913d6 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5c0:

004913d6 8906            mov     dword ptr [esi],eax  ds:0023:006cc420=00000000

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913d8 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5c2:

004913d8 ff30            push    dword ptr [eax]      ds:0023:00379df0=00000000

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913da esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5c4:

004913da e8fa0cfeff      call    calc!\_destroynum (004720d9)

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913df esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5c9:

004913df 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913e1 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5cb:

004913e1 2138            and     dword ptr [eax],edi  ds:0023:00379df0=00000000

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=00000000

eip=004913e3 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5cd:

004913e3 8b7d10          mov     edi,dword ptr [ebp+10h] ss:0023:0020e398=0038ffa0

eax=00379df0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913e6 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5d0:

004913e6 8b07            mov     eax,dword ptr [edi]  ds:0023:0038ffa0=0037a1f0

eax=0037a1f0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913e8 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5d2:

004913e8 ff7004          push    dword ptr [eax+4]    ds:0023:0037a1f4=00000001

eax=0037a1f0 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913eb esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x5d5:

004913eb e8040dfeff      call    calc!\_createnum (004720f4)

eax=00379d90 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913f0 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5da:

004913f0 8b0e            mov     ecx,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379d90 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913f2 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5dc:

004913f2 8901            mov     dword ptr [ecx],eax  ds:0023:00379df0=00000000

eax=00379d90 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913f4 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5de:

004913f4 8b07            mov     eax,dword ptr [edi]  ds:0023:0038ffa0=0037a1f0

eax=0037a1f0 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913f6 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5e0:

004913f6 8b4804          mov     ecx,dword ptr [eax+4] ds:0023:0037a1f4=00000001

eax=0037a1f0 ebx=006cc278 ecx=00000001 edx=00000000 esi=006cc420 edi=0038ffa0

eip=004913f9 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5e3:

004913f9 8d0c8d0c000000  lea     ecx,[ecx\*4+0Ch]

eax=0037a1f0 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491400 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5ea:

00491400 51              push    ecx

eax=0037a1f0 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491401 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5eb:

00491401 50              push    eax

eax=0037a1f0 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491402 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5ec:

00491402 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491404 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5ee:

00491404 ff30            push    dword ptr [eax]      ds:0023:00379df0=00379d90

eax=00379df0 ebx=006cc278 ecx=00000010 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491406 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5f0:

00491406 e8700cfeff      call    calc!memcpy (0047207b)

eax=00379d90 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049140b esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5f5:

0049140b 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049140d esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x5f7:

0049140d 83c40c          add     esp,0Ch

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491410 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x5fa:

00491410 ff7004          push    dword ptr [eax+4]    ds:0023:00379df4=00000000

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491413 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x5fd:

00491413 e8c10cfeff      call    calc!\_destroynum (004720d9)

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491418 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x602:

00491418 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049141a esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x604:

0049141a 83600400        and     dword ptr [eax+4],0  ds:0023:00379df4=00000000

eax=00379df0 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049141e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x608:

0049141e 8b4704          mov     eax,dword ptr [edi+4] ds:0023:0038ffa4=00367598

eax=00367598 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491421 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x60b:

00491421 ff7004          push    dword ptr [eax+4]    ds:0023:0036759c=00000001

eax=00367598 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491424 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x60e:

00491424 e8cb0cfeff      call    calc!\_createnum (004720f4)

eax=003762f8 ebx=006cc278 ecx=75f37782 edx=00000000 esi=006cc420 edi=0038ffa0

eip=00491429 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x613:

00491429 8b0e            mov     ecx,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=003762f8 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049142b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x615:

0049142b 894104          mov     dword ptr [ecx+4],eax ds:0023:00379df4=00000000

eax=003762f8 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=0038ffa0

eip=0049142e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x618:

0049142e 8b7f04          mov     edi,dword ptr [edi+4] ds:0023:0038ffa4=00367598

eax=003762f8 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=00491431 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x61b:

00491431 8b4704          mov     eax,dword ptr [edi+4] ds:0023:0036759c=00000001

eax=00000001 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=00491434 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x61e:

00491434 8d04850c000000  lea     eax,[eax\*4+0Ch]

eax=00000010 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=0049143b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x625:

0049143b 50              push    eax

eax=00000010 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=0049143c esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x626:

0049143c 8b06            mov     eax,dword ptr [esi]  ds:0023:006cc420=00379df0

eax=00379df0 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=0049143e esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x628:

0049143e 57              push    edi

eax=00379df0 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=0049143f esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x629:

0049143f ff7004          push    dword ptr [eax+4]    ds:0023:00379df4=003762f8

eax=00379df0 ebx=006cc278 ecx=00379df0 edx=00000000 esi=006cc420 edi=00367598

eip=00491442 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x62c:

00491442 e8340cfeff      call    calc!memcpy (0047207b)

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=00491447 esp=0020e344 ebp=0020e388 iopl=0         nv up ei pl nz na po nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202

calc!CCalcEngine::DoOperation+0x631:

00491447 83c40c          add     esp,0Ch

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=0049144a esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz ac pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216

calc!CCalcEngine::DoOperation+0x634:

0049144a 837b0800        cmp     dword ptr [ebx+8],0  ds:0023:006cc280=00000000

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=0049144e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x638:

0049144e 0f859d390000    jne     calc!CCalcEngine::DoOperation+0x63a (00494df1) [br=0]

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=00491454 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6ad:

00491454 837d085b        cmp     dword ptr [ebp+8],5Bh ss:0023:0020e390=0000005b

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=00491458 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6b1:

00491458 ff75ec          push    dword ptr [ebp-14h]  ss:0023:0020e374=00375548

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=0049145b esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6b4:

0049145b 56              push    esi

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=0049145c esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6b5:

0049145c 0f85fd3b0000    jne     calc!CCalcEngine::DoOperation+0x6c5 (0049505f) [br=0]

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00367598

eip=00491462 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6b7:

00491462 8b7de8          mov     edi,dword ptr [ebp-18h] ss:0023:0020e370=00000001

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000001

eip=00491465 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6ba:

00491465 0faf7d0c        imul    edi,dword ptr [ebp+0Ch] ss:0023:0020e394=00000001

eax=003762f8 ebx=006cc278 ecx=00000004 edx=00000000 esi=006cc420 edi=00000001

eip=00491469 esp=0020e348 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6be:

00491469 e8074efeff      call    calc!divrat (00476275)

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=0049146e esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6cd:

0049146e 837b0800        cmp     dword ptr [ebx+8],0  ds:0023:006cc280=00000000

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=00491472 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x6d1:

00491472 0f84d3400000    je      calc!CCalcEngine::DoOperation+0x930 (0049554b) [br=1]

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=0049554b esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x930:

0049554b 837dec00        cmp     dword ptr [ebp-14h],0 ss:0023:0020e374=00375548

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=0049554f esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x934:

0049554f 0f84f7faffff    je      calc!CCalcEngine::DoOperation+0xf5 (0049504c) [br=0]

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=00495555 esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x93a:

00495555 ff75ec          push    dword ptr [ebp-14h]  ss:0023:0020e374=00375548

eax=00000000 ebx=006cc278 ecx=00000000 edx=00000009 esi=006cc420 edi=00000001

eip=00495558 esp=0020e34c ebp=0020e388 iopl=0         nv up ei pl nz na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206

calc!CCalcEngine::DoOperation+0x93d:

00495558 e848cbfdff      call    calc!\_destroyrat (004720a5)

eax=00000000 ebx=006cc278 ecx=75f376dc edx=00360174 esi=006cc420 edi=00000001

eip=0049555d esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0x942:

0049555d e9eafaffff      jmp     calc!CCalcEngine::DoOperation+0xf5 (0049504c)

eax=00000000 ebx=006cc278 ecx=75f376dc edx=00360174 esi=006cc420 edi=00000001

eip=0049504c esp=0020e350 ebp=0020e388 iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0xf5:

0049504c e81acffdff      call    calc!\_EH\_epilog3 (00471f6b)

eax=00000000 ebx=006cc420 ecx=00495051 edx=00360174 esi=006cc278 edi=00000000

eip=00495051 esp=0020e38c ebp=0020e47c iopl=0         nv up ei pl zr na pe nc

cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246

calc!CCalcEngine::DoOperation+0xfa:

00495051 c20c00          ret     0Ch

0:000> .logclose

Closing open log file calc.log