MSK .NET Meetup #1

# WinDbg сотоварищи

Михаил Щербаков
Independent Consultant

SPB DOT NET

MSK DOT NET

intelli

# Обо мне

- Консультант, Upwork’er,
- Разработчик проекта IntelliDebugger http://intelliegg.com
- Координатор сообществ .NET программистов Москвы и Санкт-Петербурга http://mskdotnet.org/ http://spbdotnet.org
- В прошлом менеджер по продуктам и тимлид в Cezurity, Acronis, Luxoft, Boeing

MVP
Microsoft®
Most Valuable
Professional

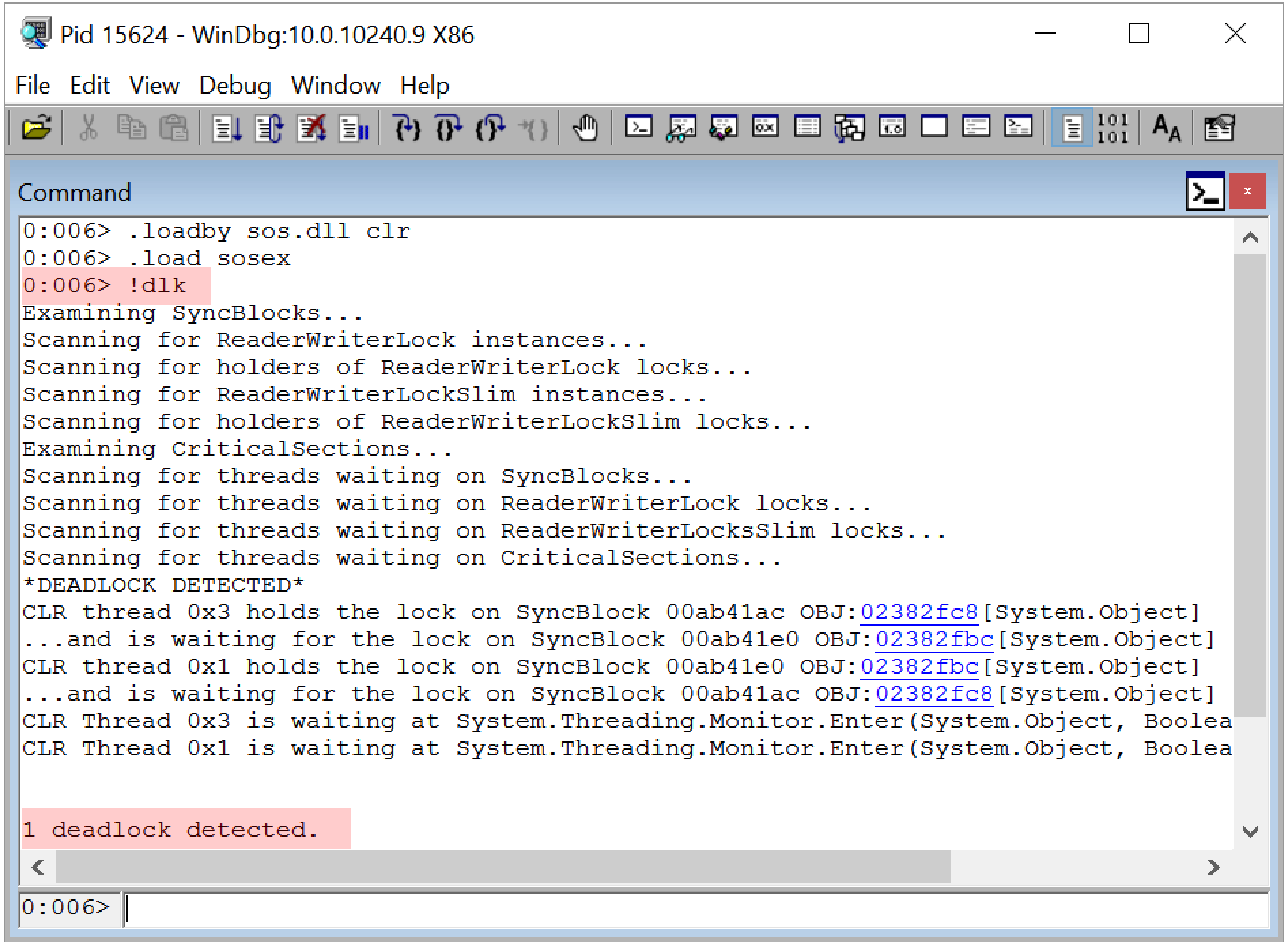
# Зачем WinDbg мне?

Какой отладчик использовать, если нужно отлаживать расширение отладчика Visual Studio, отлаживающего другой процесс?

# Зачем он вам?

- Найти deadlock?
- Легко* с WinDbg

# Зачем он вам?



Pid 15624 - WinDbg:10.0.10240.9 X86
File Edit View Debug Window Help
Command

```
0:006> .loadby sos.dll clr
0:006> .load sosex
0:006> !dlk
Examining SyncBlocks...
Scanning for ReaderWriterLock instances...
Scanning for holders of ReaderWriterLock locks...
Scanning for ReaderWriterLockSlim instances...
Scanning for holders of ReaderWriterLockSlim locks...
Examining CriticalSections...
Scanning for threads waiting on SyncBlocks...
Scanning for threads waiting on ReaderWriterLock locks...
Scanning for threads waiting on ReaderWriterLocksSlim locks...
Scanning for threads waiting on CriticalSections...
*DEADLOCK DETECTED*
CLR thread 0x3 holds the lock on SyncBlock 00ab41ac OBJ:02382fc8[System.Object]
...and is waiting for the lock on SyncBlock 00ab41e0 OBJ:02382fbc[System.Object]
CLR thread 0x1 holds the lock on SyncBlock 00ab41e0 OBJ:02382fbc[System.Object]
...and is waiting for the lock on SyncBlock 00ab41ac OBJ:02382fc8[System.Object]
CLR Thread 0x3 is waiting at System.Threading.Monitor.Enter(System.Object, Boolea
CLR Thread 0x1 is waiting at System.Threading.Monitor.Enter(System.Object, Boolea


1 deadlock detected.
```

```
0:006>
```

# Плюсы WinDbg

- Легкий отладчик, быстро запускается
- Предоставляет больше данных для анализа
- Гибкая и автоматизируемая скриптами отладка кода
- Вменяемый анализ дампов
- Вменяемая отладка смешанного (mixed) кода

# Минусы WinDbg

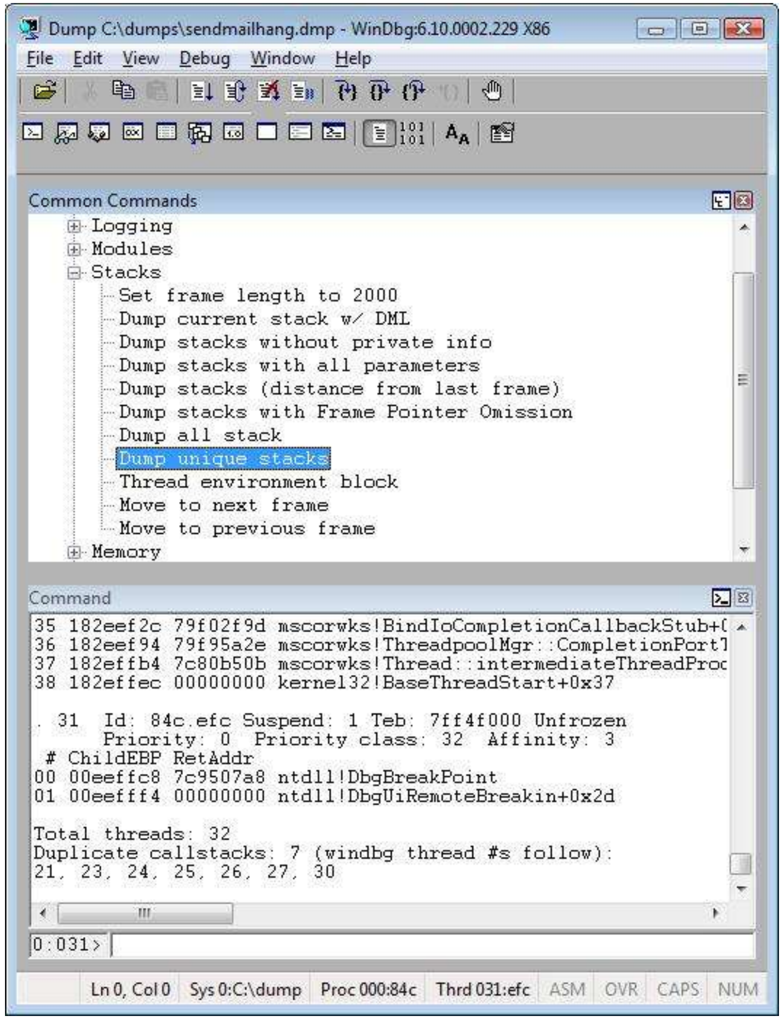
- Командная строка - долго не используешь, быстро забываешь
- Ужасный GUI
- Имеет странности

# Настройка WinDbg

# Командная строка

- Удобно использовать

.cmdtree



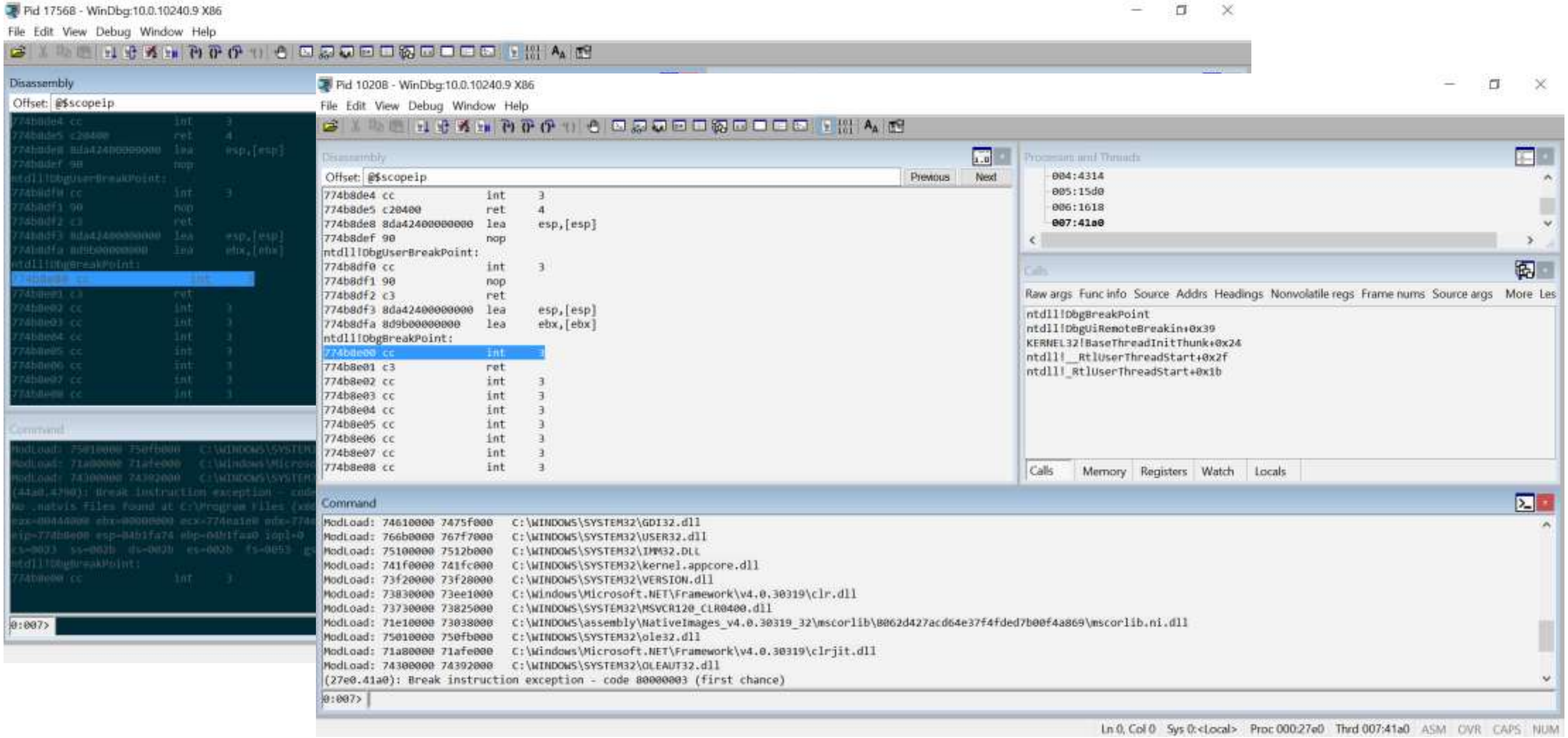
```
⊞ Logging
⊞ Modules
⊟ Stacks
    Set frame length to 2000
    Dump current stack w/ DML
    Dump stacks without private info
    Dump stacks with all parameters
    Dump stacks (distance from last frame)
    Dump stacks with Frame Pointer Omission
    Dump all stack
    Dump unique stacks
    Thread environment block
    Move to next frame
    Move to previous frame
⊞ Memory
```

```
35 182eef2c 79f02f9d mscorwks!BindIoCompletionCallbackStub+(
36 182eef94 79f95a2e mscorwks!ThreadpoolMgr::CompletionPort]
37 182effb4 7c80b50b mscorwks!Thread::intermediateThreadProc
38 182effec 00000000 kernel32!BaseThreadStart+0x37

. 31  Id: 84c.efc Suspend: 1 Teb: 7ff4f000 Unfrozen
      Priority: 0  Priority class: 32  Affinity: 3
 # ChildEBP RetAddr
00 00eeffc8 7c9507a8 ntdll!DbgBreakPoint
01 00eefff4 00000000 ntdll!DbgUiRemoteBreakin+0x2d

Total threads: 32
Duplicate callstacks: 7 (windbg thread #s follow):
21, 23, 24, 25, 26, 27, 30
```

```
0:031>
```

http://www.wintellect.com/devcenter/jrobbins/a-cool-windbg-sos-hidden-feature

# Графический интерфейс


Pid 17568 - WinDbg:10.0.10240.9 X86
File Edit View Debug Window Help
Disassembly
Offset: @$scopeip
Command
0:007>
Pid 10208 - WinDbg:10.0.10240.9 X86
File Edit View Debug Window Help
Disassembly
Offset: @$scopeip
Previous
Next
Processes and Threads
Calls
Raw args Func info Source Addrs Headings Nonvolatile regs Frame nums Source args More Les
Calls Memory Registers Watch Locals
Command
Ln 0, Col 0 Sys 0:<Local> Proc 000:27e0 Thrd 007:41a0 ASM OVR CAPS NUM

```
774b8de4 cc              int     3
774b8de5 c20400          ret     4
774b8de8 8da42400000000  lea     esp,[esp]
774b8def 90              nop
ntdll!DbgUserBreakPoint:
774b8df0 cc              int     3
774b8df1 90              nop
774b8df2 c3              ret
774b8df3 8da42400000000  lea     esp,[esp]
774b8dfa 8d9b00000000    lea     ebx,[ebx]
ntdll!DbgBreakPoint:
774b8e00 cc              int     3
774b8e01 c3              ret
774b8e02 cc              int     3
774b8e03 cc              int     3
774b8e04 cc              int     3
774b8e05 cc              int     3
774b8e06 cc              int     3
774b8e07 cc              int     3
774b8e08 cc              int     3
```

```
004:4314
005:15d0
006:1618
007:41a0
```

```
ntdll!DbgBreakPoint
ntdll!DbgUiRemoteBreakin+0x39
KERNEL32!BaseThreadInitThunk+0x24
ntdll!__RtlUserThreadStart+0x2f
ntdll!_RtlUserThreadStart+0x1b
```

```
ModLoad: 74610000 7475f000   C:\WINDOWS\SYSTEM32\GDI32.dll
ModLoad: 766b0000 767f7000   C:\WINDOWS\SYSTEM32\USER32.dll
ModLoad: 75100000 7512b000   C:\WINDOWS\SYSTEM32\IMM32.DLL
ModLoad: 741f0000 741fc000   C:\WINDOWS\SYSTEM32\kernel.appcore.dll
ModLoad: 73f20000 73f28000   C:\WINDOWS\SYSTEM32\VERSION.dll
ModLoad: 73830000 73ee1000   C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
ModLoad: 73730000 73825000   C:\WINDOWS\SYSTEM32\MSVCR120_CLR0400.dll
ModLoad: 71e10000 73038000   C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\mscorlib\8062d427acd64e37f4fded7b00f4a869\mscorlib.ni.dll
ModLoad: 75010000 750fb000   C:\WINDOWS\SYSTEM32\ole32.dll
ModLoad: 71a80000 71afe000   C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
ModLoad: 74300000 74392000   C:\WINDOWS\SYSTEM32\OLEAUT32.dll
(27e0.41a0): Break instruction exception - code 80000003 (first chance)
0:007>
```

https://github.com/yuske/DotNextMsk2015

# Отладочные символы

```
0:000> .sympath
Symbol search path is: <empty>
```

# Отладочные символы

```
0:000> .sympath+ c:\mysymbols
Symbol search path is: c:\mysymbols
0:000> .reload
Reloading current modules
....
*** ERROR: Symbol file could not be found. Defaulted
to export symbols for ntdll.dll
0:000> .symfix
```

# Отладочные символы

```
> setx _NT_SYMBOL_PATH cache*C:\symbols;SRV*C:\symbols*http://msdl.microsoft.com/download/symbols;\\host\bulds\last /m
```

```
> set _NT_ALT_SYMBOL_PATH <path>
```

https://msdn.microsoft.com/en-us/library/windows/hardware/ff558829(v=vs.85).aspx

# Отображение переменных

```
0:000> dx /?
DX [-r[#]] <expr> - display C++ expression using extension model (e.g.: NatVis)
DX [-r[#]] <expr>[,<FormatSpecifier>] - display C++ expression using extension model (e.g.: NatVis) in a specified format
```

[https://msdn.microsoft.com/en-us/library/windows/hardware/dn936815(v=vs.85).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/dn936815(v=vs.85).aspx)

# Отображение переменных

```
> cd "C:\Program Files (x86)\Windows Kits\10\
Debuggers\x86"
```

```
> mklink /d Visualizers "C:\Program Files (x86)\
Microsoft Visual Studio 14.0\Common7\Packages\
Debugger\Visualizers“
```

# Расширения для отладки .NET кода

- SOS    http://bit.ly/1PUofK9
- SOSEX    http://www.stevestechspot.com/
- NetExt    http://netext.codeplex.com/
- PSSCOR2/PSSCOR4    http://bit.ly/1kOJLEV; http://bit.ly/1NKan0G
- SDbgExt2    https://github.com/steveniemitz/SDbgExt2

# Сценарии отладки

# Загрузка расширений

```
0:000> .loadby sos.dll clr
0:000> .load sosex
0:000> .load netext
0:000> .load psscor4
0:000> .load spt
```

# Исследование метаданных

- Type Handle
- Sync Block Table
- Method Table
- Method Descriptors
- Modules
- Metadata Tokens
- EEClass

# Исследование метаданных

```
!DumpDomain [<domain address>]
!DumpModule [-mt] <Module address>
!DumpAssembly <assembly address>
!DumpClass <EEClass address>
!DumpMT [-MD] <MethodTable address>
!IP2MD <code address>
!DumpMD <MethodDesc address>
!Name2EE <type name>
```

# Исследование метаданных

```
0:000> !mx Demo!*Thread*
AppDomain 724c6770 (Shared Domain)
----------------------------------------------------
AppDomain 0085dc28 (Demo.exe)
----------------------------------------------------
module: Demo
  class: Demo.Program
    StartThreadA()
    StartThreadB()
```

# Управление точками останова

```
0:004> !name2ee Bar.exe Bar.App.Foo
Module: 00112d8c (Bar.exe)
Token: 0x06000002
MethodDesc: 00113178
Name: Bar.App.Foo(Int32, Int32)
JITTED Code Address: 003e0178
0:004> bp 003e0178
```

# Управление точками останова

```
0:004> !name2ee Bar.exe Bar.App.Foo
Module: 00112d8c (Bar.exe)
Token: 0x06000002
MethodDesc: 00113178
Name: Bar.App.Foo(Int32, Int32)
Not JITTED yet. Use !bpmd -md 00113178 to break on run.
0:004> !bpmd –md 00113178
MethodDesc = 00113178
Adding pending breakpoints...
```

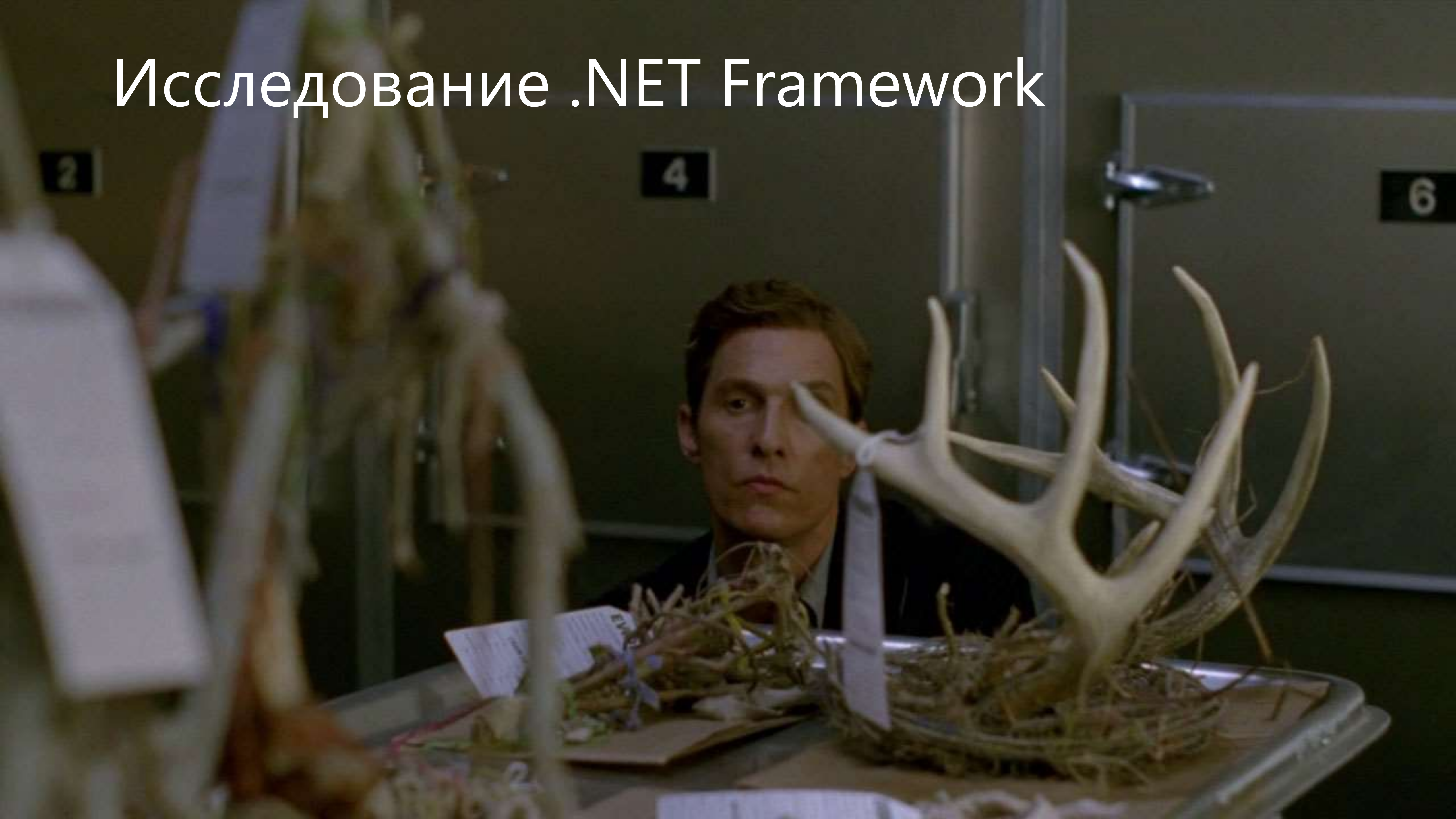
# Управление точками останова

```
0:004> !bpmd Bar.exe Bar.Comparer`1.GreaterThan
Found 1 methods...
MethodDesc = 001a3188
Adding pending breakpoints...
```

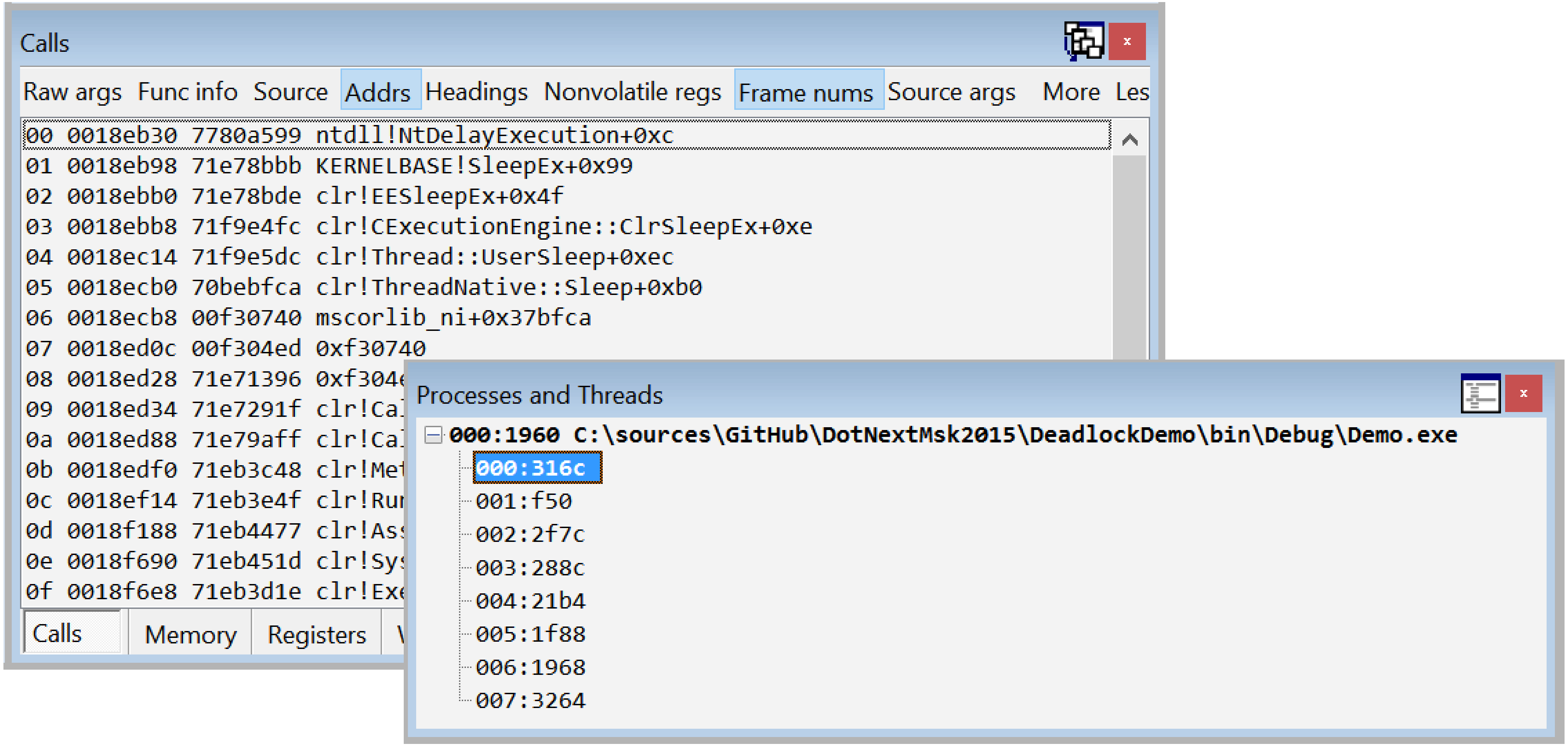
# Управление точками останова

```
!mbm <Type/Method Filter> [ILOffset] [Options]
!mbp <SourceFile> <nLineNum> [ColNum] [Options]
```

# Исследование .NET Framework



# Операции с потоками



```
00 0018eb30 7780a599 ntdll!NtDelayExecution+0xc
01 0018eb98 71e78bbb KERNELBASE!SleepEx+0x99
02 0018ebb0 71e78bde clr!EESleepEx+0x4f
03 0018ebb8 71f9e4fc clr!CExecutionEngine::ClrSleepEx+0xe
04 0018ec14 71f9e5dc clr!Thread::UserSleep+0xec
05 0018ecb0 70bebfca clr!ThreadNative::Sleep+0xb0
06 0018ecb8 00f30740 mscorlib_ni+0x37bfca
07 0018ed0c 00f304ed 0xf30740
08 0018ed28 71e71396 0xf304e
09 0018ed34 71e7291f clr!Ca
0a 0018ed88 71e79aff clr!Ca
0b 0018edf0 71eb3c48 clr!Met
0c 0018ef14 71eb3e4f clr!Rur
0d 0018f188 71eb4477 clr!As
0e 0018f690 71eb451d clr!Sys
0f 0018f6e8 71eb3d1e clr!Exe
```

```
⊟ 000:1960 C:\sources\GitHub\DotNextMsk2015\DeadlockDemo\bin\Debug\Demo.exe
    000:316c
    001:f50
    002:2f7c
    003:288c
    004:21b4
    005:1f88
    006:1968
    007:3264
```

# Операции с потоками

```
0:004> !threads
ThreadCount:      3
UnstartedThread:  0
BackgroundThread: 1
...
       ID OSID ThreadOBJ    State ... Apt Exception
   0    1 316c 0109b6e0   202a020     MTA
   5    2 1f88 010a8e98     2b220     MTA (Finalizer)
   6    3 1968 010c8960   202b020     MTA
```

# Операции с потоками

```
0:004> !ClrStack
OS Thread Id: 0x316c (0)
Child SP       IP Call Site
0018ec34 77b96e3c [HelperMethodFrame: 0018ec34]
System.Threading.Thread.SleepInternal(Int32)
0018ecb8 70bebfca System.Threading.Thread.Sleep(Int32)
0018ecc0 00f30740 Demo.Program.SampleB()
[C:\Demo\Program.cs @ 66]
0018ed14 00f304ed Demo.Program.Main(System.String[])
[C:\Demo\Program.cs @ 17]
```

# Операции с потоками

```
!DumpStack [-ee]
!mk [FrameCount] [-l] [-p] [-a]
!EEStack –short [-ee]
```

# Поиск deadlock’ов

# Исследование объектов в памяти

```
0:000> dd 0x01e06bec

01e06bec  001c30b0 00000000 00000000 00000000
01e06bfc  80000000 790fd8c4 00000014 00000013
01e06c0c  003a0078 0030007b 002c007d 00790020
01e06c1c  007b003a 007d0031 0020002c 003a007a
01e06c2c  0032007b 0000007d 00000000 00000000
01e06c3c  00000000 00000000 00000000 00000000
01e06c4c  00000000 00000000 00000000 00000000
01e06c5c  00000000 00000000 00000000 00000000
```

# Исследование объектов в памяти

```
0:000> !DumpObj 0x01c56bec
Name: Bar.App
MethodTable: 002130b0
EEClass: 00211240
Size: 20(0x14) bytes (C:\samples\Bar.exe)
...
```

# Исследование объектов в памяти

**!DumpVC** <MethodTable address> <Address>

**!DumpArray** [-start <startIndex>] [-length <length>] [-details] [-nofields] <Array object address>

# Исследование объектов в памяти

```
0:000>!mdt 02772f90 -r
02772f90 (Demo.Bar)
    array:02772ff8 (System.Int32[], Elements: 4)
    list:02773038 (.List`1[[System.String, mscorlib]])
        _items:0277305c (System.String[], Elements: 4)
        _size:0x2 (System.Int32)
        _version:0x2 (System.Int32)
        _syncRoot:NULL (System.Object)
    <CurrentPoint>k__BackingField:(Demo.Point) VALTYPE
```

# Исследование объектов в памяти

**!DumpHeap** [-stat] [-strings] [-short] [-min <size>] [-max <size>] [-thinlock] [-startAtLowerBound] [-mt <MethodTable address>] [-type <partial type name>][start [end]]

**!DumpRuntimeTypes**

**!strings**

**!EEHeap** [-gc] [-loader]

**!TraverseHeap** [-xml] <filename>

**!VerifyHeap**

# Исследование объектов в памяти

```
0:006> !HeapStat -iu
Heap     Gen0         Gen1         Gen2          LOH
Heap0  188636      6297752    256636732        17592

Free space:
Heap0      12          116         6916           80

Unrooted objects:
Heap0  170476      6297584    256616572            0
```

# Исследование объектов в памяти

**!GCRoot** [-nostacks] <Object address>

**!gcgen** <hexObjectAddr>

**!dumpgen** <intGenNum> [-free] [-stat] [-type <TYPE_NAME>] [-nostrings]

# Анализ memory leak’ов

# Отладка web-приложений

**!whttp** – список HttpContext обектов

**!wservice** – список WCF service обектов

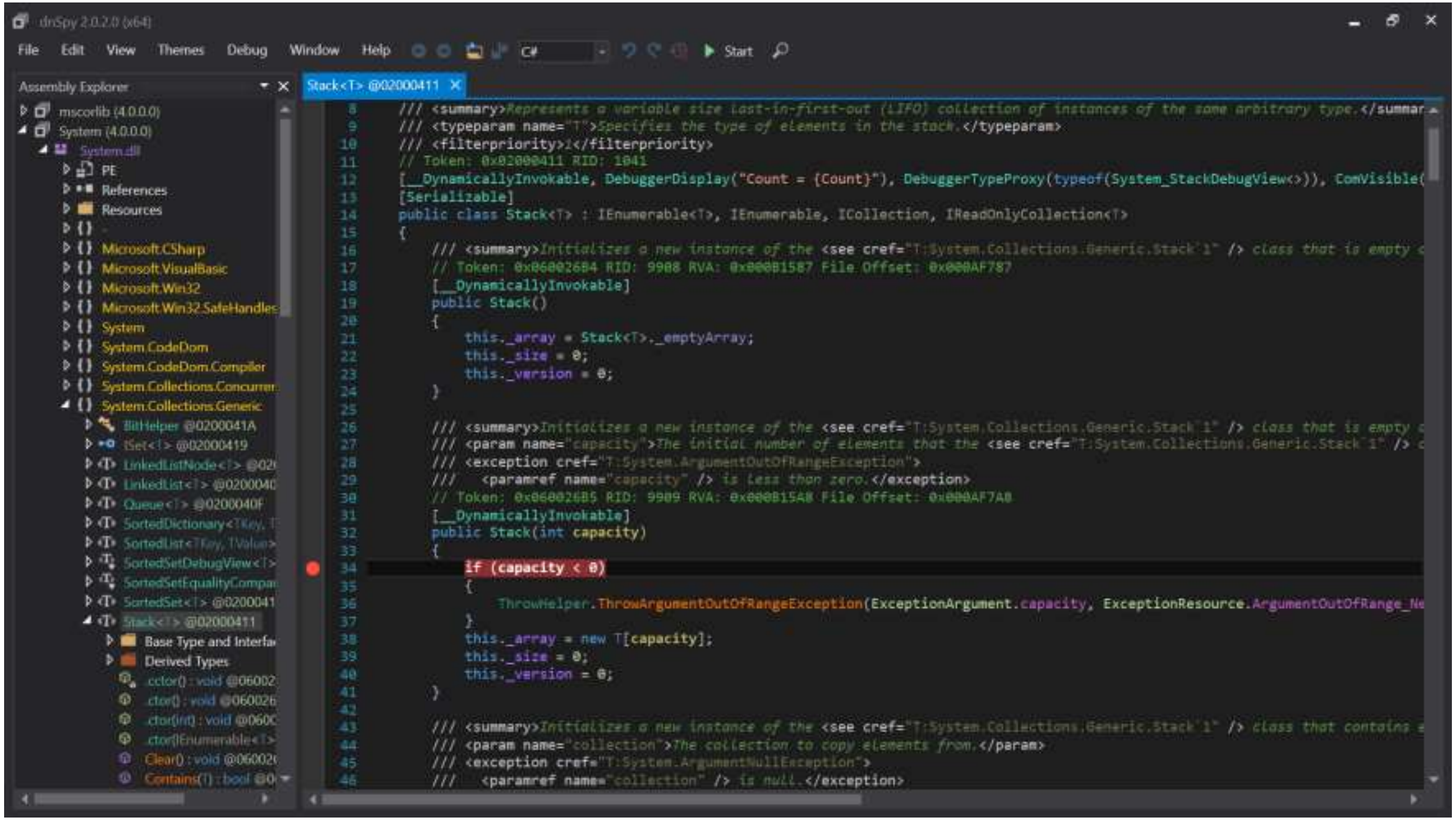
**!wsocket** – информация о сокетах

**!DumpASPNetRequests** – список потоков с HttpContext

**!DumpSqlConnectionPools** – информация о всех Sql connection pools

# Дополнительные инструменты

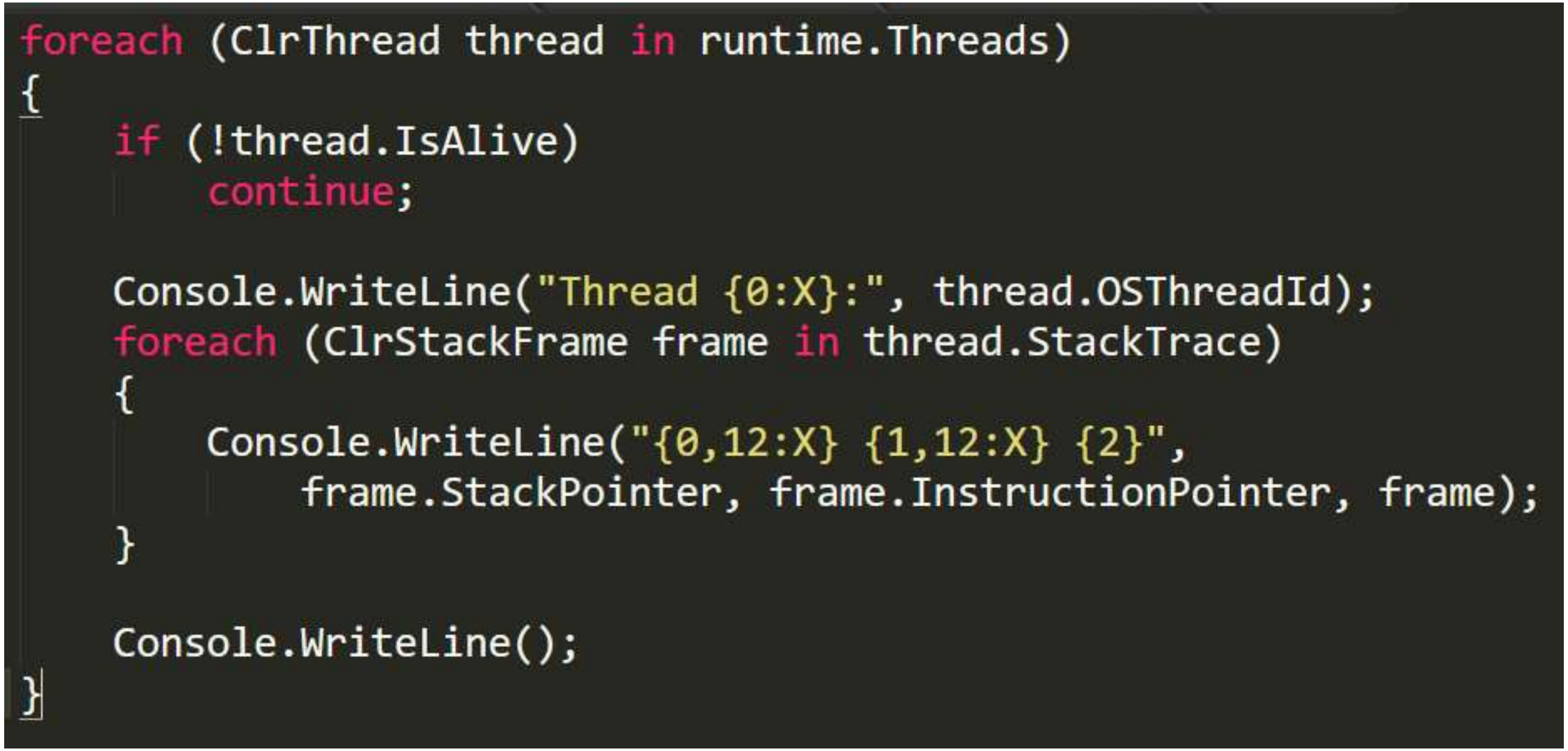
# dnSpy



```
/// <summary>Represents a variable size last-in-first-out (LIFO) collection of instances of the same arbitrary type.</summar
/// <typeparam name="T">Specifies the type of elements in the stack.</typeparam>
/// <filterpriority>1</filterpriority>
// Token: 0x02000411 RID: 1041
[__DynamicallyInvokable, DebuggerDisplay("Count = {Count}"), DebuggerTypeProxy(typeof(System_StackDebugView<>)), ComVisible(
[Serializable]
public class Stack<T> : IEnumerable<T>, IEnumerable, ICollection, IReadOnlyCollection<T>
{
    /// <summary>Initializes a new instance of the <see cref="T:System.Collections.Generic.Stack`1" /> class that is empty c
    // Token: 0x060026B4 RID: 9908 RVA: 0x000B1587 File Offset: 0x000AF787
    [__DynamicallyInvokable]
    public Stack()
    {
        this._array = Stack<T>._emptyArray;
        this._size = 0;
        this._version = 0;
    }

    /// <summary>Initializes a new instance of the <see cref="T:System.Collections.Generic.Stack`1" /> class that is empty c
    /// <param name="capacity">The initial number of elements that the <see cref="T:System.Collections.Generic.Stack`1" /> c
    /// <exception cref="T:System.ArgumentOutOfRangeException">
    ///   <paramref name="capacity" /> is less than zero.</exception>
    // Token: 0x060026B5 RID: 9909 RVA: 0x000B15A8 File Offset: 0x000AF7A8
    [__DynamicallyInvokable]
    public Stack(int capacity)
    {
        if (capacity < 0)
        {
            ThrowHelper.ThrowArgumentOutOfRangeException(ExceptionArgument.capacity, ExceptionResource.ArgumentOutOfRange_Ne
        }
        this._array = new T[capacity];
        this._size = 0;
        this._version = 0;
    }

    /// <summary>Initializes a new instance of the <see cref="T:System.Collections.Generic.Stack`1" /> class that contains e
    /// <param name="collection">The collection to copy elements from.</param>
    /// <exception cref="T:System.ArgumentNullException">
    ///   <paramref name="collection" /> is null.</exception>
```

https://github.com/0xd4d/dnSpy

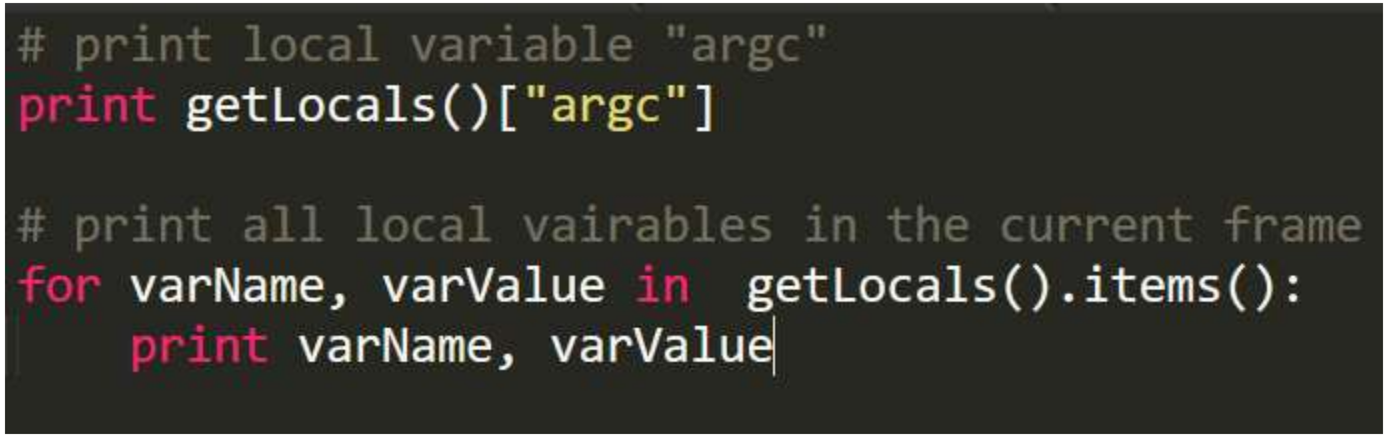
# CLR MD (Microsoft.Diagnostics.Runtime.dll)



```
foreach (ClrThread thread in runtime.Threads)
{
    if (!thread.IsAlive)
        continue;

    Console.WriteLine("Thread {0:X}:", thread.OSThreadId);
    foreach (ClrStackFrame frame in thread.StackTrace)
    {
        Console.WriteLine("{0,12:X} {1,12:X} {2}",
            frame.StackPointer, frame.InstructionPointer, frame);
    }

    Console.WriteLine();
}
```

http://msk2015.dotnext.ru/talks/goldshtein

# PyKd

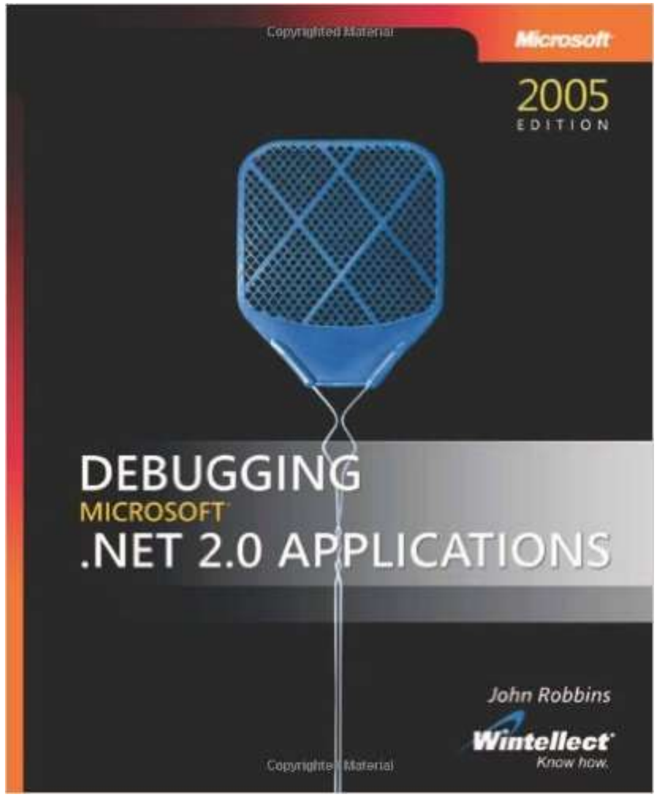


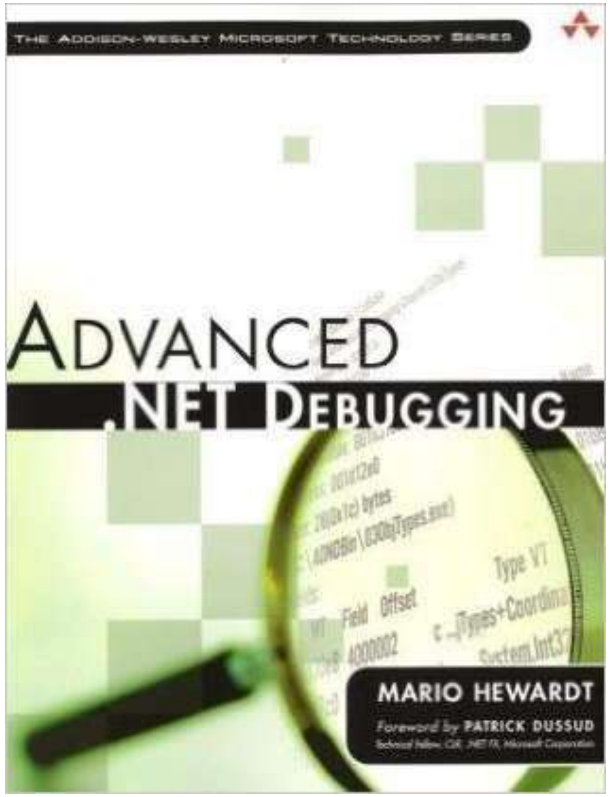
```
# print local variable "argc"
print getLocals()["argc"]

# print all local vairables in the current frame
for varName, varValue in  getLocals().items():
    print varName, varValue
```

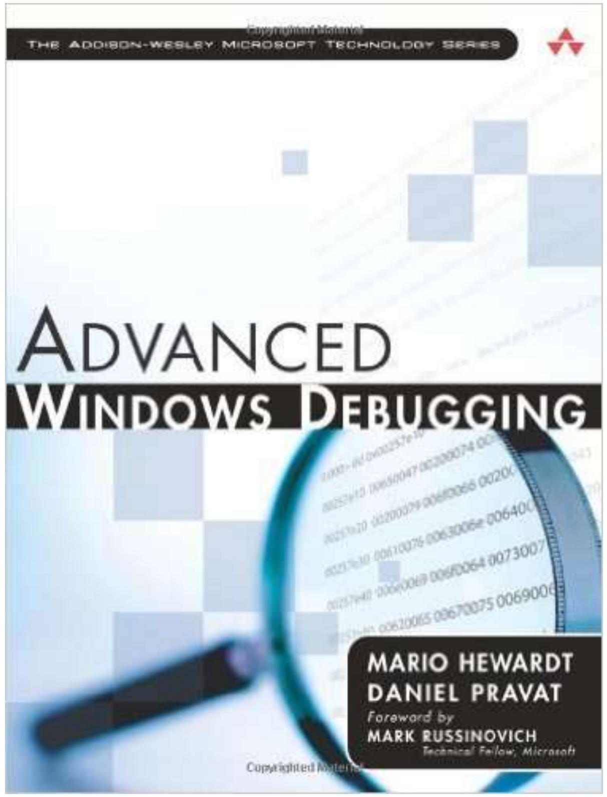
http://2015.phdays.ru/program/40602

# Что дальше?

# Книги




THE ADDISON-WESLEY MICROSOFT TECHNOLOGY SERIES
ADVANCED
.NET DEBUGGING
MARIO HEWARDT
Foreword by PATRICK DUSSUD



http://amzn.to/21TWSWd

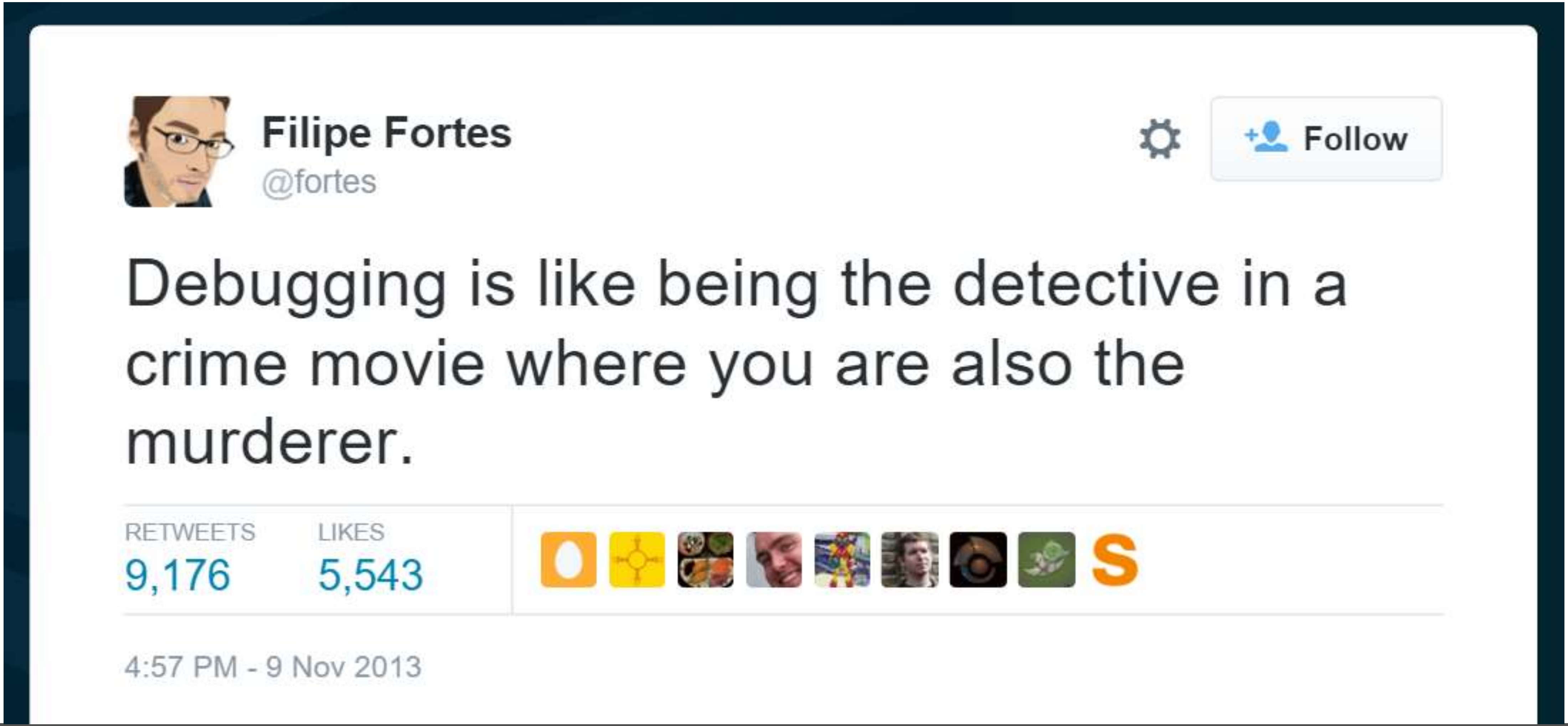
http://amzn.to/1NK2bl0

http://amzn.to/1QzZIdR

# Блоги

- Sasha Goldshtein
  http://blogs.microsoft.co.il/sasha/
- John Robbins
  http://www.wintellect.com/devcenter/jrobbins
- EreTIk's Box
  http://eretik.omegahg.com/WinDbg.html

# *Цитата*



**Filipe Fortes**
@fortes

Debugging is like being the detective in a crime movie where you are also the murderer.

RETWEETS 9,176
LIKES 5,543

4:57 PM - 9 Nov 2013

# Спасибо за внимание!

**Михаил Щербаков**

Independent Consultant

intelliegg.com

spbdotnet.org

github.com/yuske

@yu5k3