Reversing Malware with Debugging Tools

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

Demo

Static or Dynamic first?

Reversing Malware Dynamically

Tools and Techniques

Demo

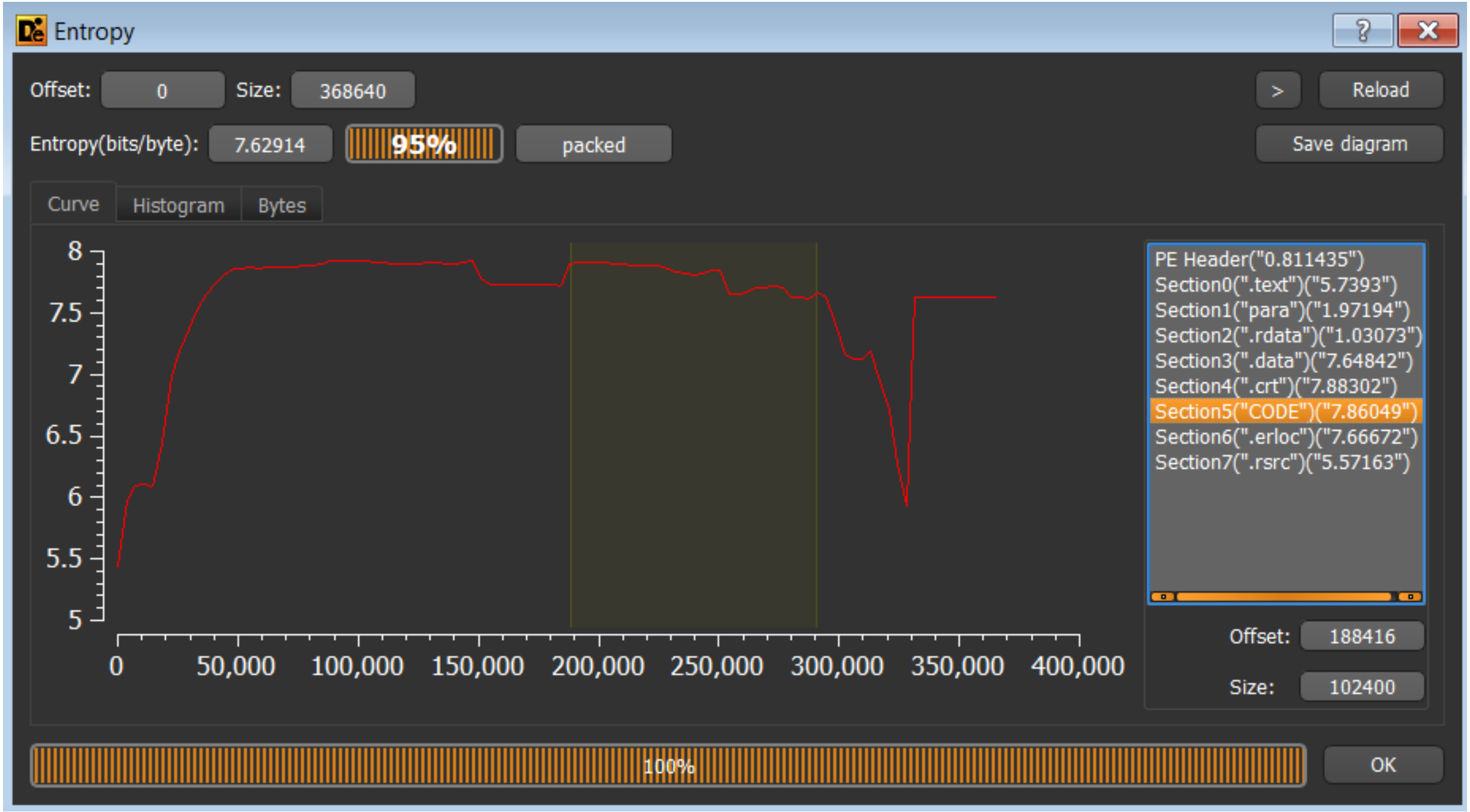
Unpacking Malware Dynamically

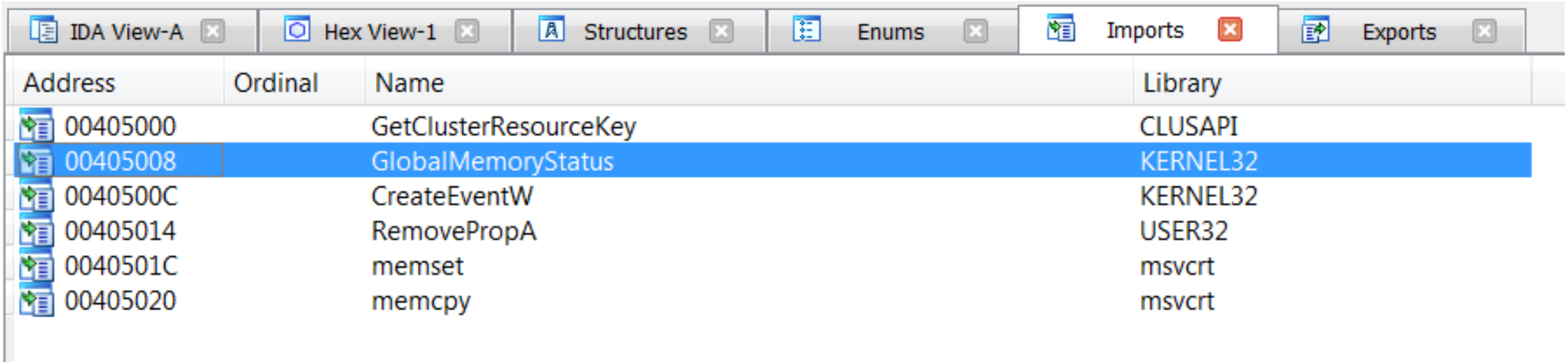
https://malwarecookbook.googlecode.com/svn/trunk/3/8/pescanner.py

```
#!/usr/bin/python
# Copyright (C) 2010 Michael Ligh
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.
#
# [NOTES] ---------------------------------------------------------
# 1) Tested on Linux (Ubuntu), Windows XP/7, and Mac OS X
# 2) The only requirement is pefile, other modules just add extra info
# 3) There are various versions of python-magic and pyssdeep - we try to support both
#-----------------------------------------------------------------
import hashlib
import time
import binascii
import string
import os, sys
import commands

try:
    import pefile
    import peutils
except ImportError:
    print 'pefile not installed, see http://code.google.com/p/pefile/'
    sys.exit()

try:
    import magic
except ImportError:
    print 'python-magic is not installed, file types will not be available'

try:
    import yara
except ImportError:
    print 'yara-python is not installed, see http://code.google.com/p/yara-project/'
```

exe\vdespohcfeyy.exe	Value	Value	Value	Value	Value
.rdata	.data	.crt	CODE	.erloc	.rsrc
0x0000031F (799)	0x000523D0 (3368...	0x000186B5 (10002...	0x000186B8 (10002...	0x00009C47 (40007)	0x00008960 (35168)
0x00005000	0x00006000	0x00059000	0x00072000	0x0008B000	0x00095000
0x00001000 (4096)	0x0000F000 (61440)	0x00019000 (10240...	0x00019000 (10240...	0x0000A000 (40960)	0x00009000 (36864)
0x00005000	0x00006000	0x00015000	0x0002E000	0x00047000	0x00051000
0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
-	-	-	-	-	-
A144F7E064CC427...	69ED26DA8A749B...	49B2C8966BEAEA3...	1195EBA20B42432...	0CA4263ADE3890...	6A633497F8B7626...
0x00000CE1 (3297)	0x00000000 (0)	0x0000094B (2379)	0x00000948 (2376)	0x000003B9 (953)	0x000006A0 (1696)
-	-	-	-	-	-
-	-	x	-	x	-
x	x	x	x	x	x
-	x	x	x	x	-
x	-	-	-	-	-
-	-	-	-	-	-

```
CODE:00472000 CODE            segment para public 'DATA' use32
CODE:00472000                 assume cs:CODE
CODE:00472000                 ;org 472000h
CODE:00472000                 db  40h ; @
CODE:00472001                 db 0D4h ; +
CODE:00472002                 db  96h ; û
CODE:00472003                 db  76h ; v
CODE:00472004                 db  64h ; d
CODE:00472005                 db  93h ; ô
CODE:00472006                 db 0EAh ; O
CODE:00472007                 db 0D6h ; +
CODE:00472008                 db 0C9h ; +
CODE:00472009                 db  97h ; ù
CODE:0047200A                 db 0BDh ; +
CODE:0047200B                 db 0E4h ; S
CODE:0047200C                 db 0AEh ; «
CODE:0047200D                 db 0A2h ; ó
CODE:0047200E                 db  40h ; @
CODE:0047200F                 db  44h ; D
CODE:00472010                 db  67h ; g
CODE:00472011                 db  9Bh ; ¢
CODE:00472012                 db 0CDh ; -
CODE:00472013                 db 0DCh ; _
CODE:00472014                 db 0B9h ; ¦
CODE:00472015                 db    1
CODE:00472016                 db  5Eh ; ^
CODE:00472017                 db  48h ; H
CODE:00472018                 db 0AAh ; ¬
CODE:00472019                 db 0D8h ; +
CODE:0047201A                 db  47h ; G
CODE:0047201B                 db  6Dh ; m
```


Entropy
Offset:
0
Size:
368640
>
Reload
Entropy(bits/byte):
7.62914
95%
packed
Save diagram
Curve
Histogram
Bytes
8
7.5
7
6.5
6
5.5
5
0
50,000
100,000
150,000
200,000
250,000
300,000
350,000
400,000
PE Header("0.811435")
Section0(".text")("5.7393")
Section1("para")("1.97194")
Section2(".rdata")("1.03073")
Section3(".data")("7.64842")
Section4(".crt")("7.88302")
Section5("CODE")("7.86049")
Section6(".erloc")("7.66672")
Section7(".rsrc")("5.57163")
Offset:
188416
Size:
102400
100%
OK

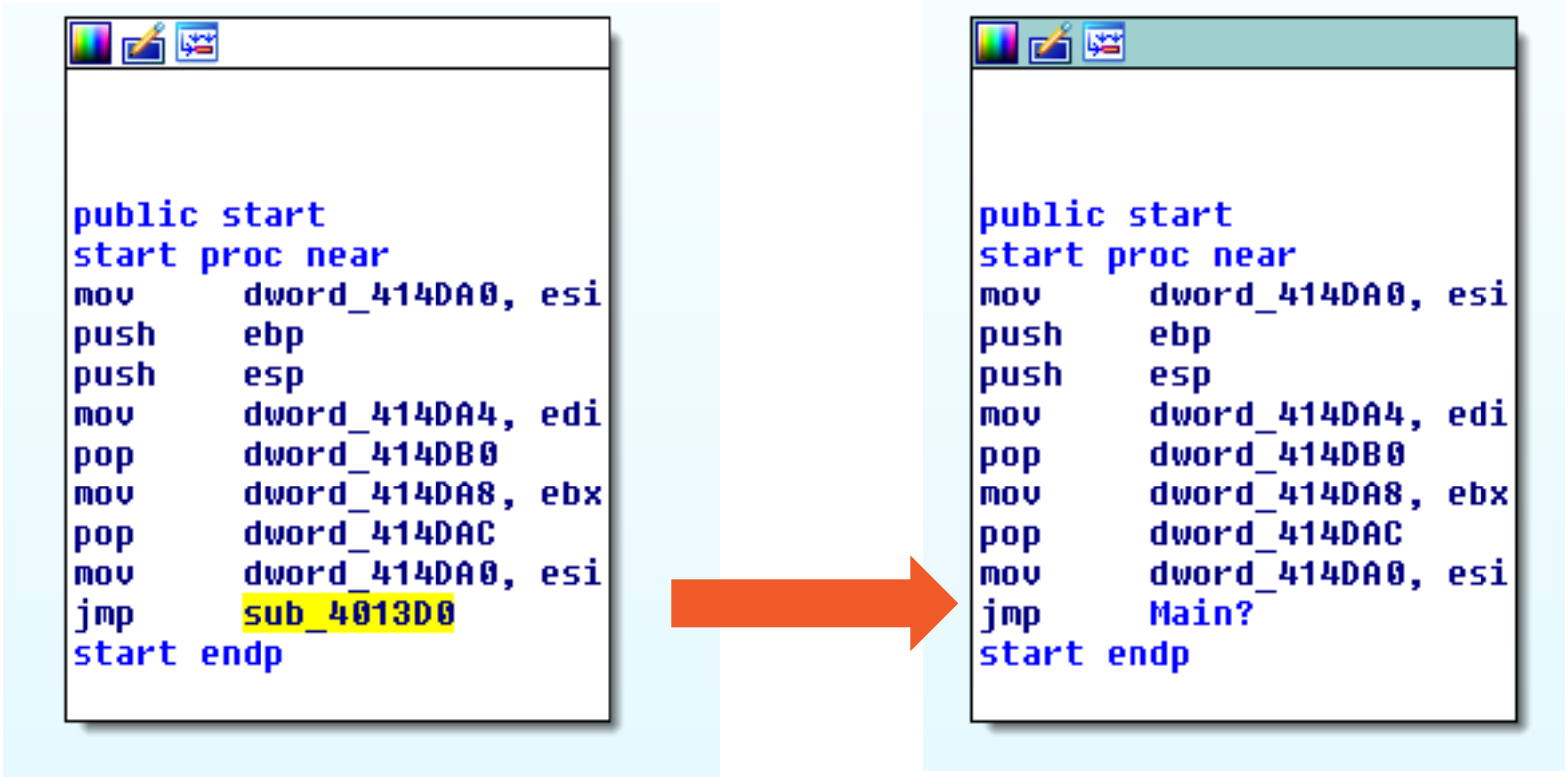

IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Address
Ordinal
Name
Library
00405000 GetClusterResourceKey CLUSAPI
00405008 GlobalMemoryStatus KERNEL32
0040500C CreateEventW KERNEL32
00405014 RemovePropA USER32
0040501C memset msvcrt
00405020 memcpy msvcrt

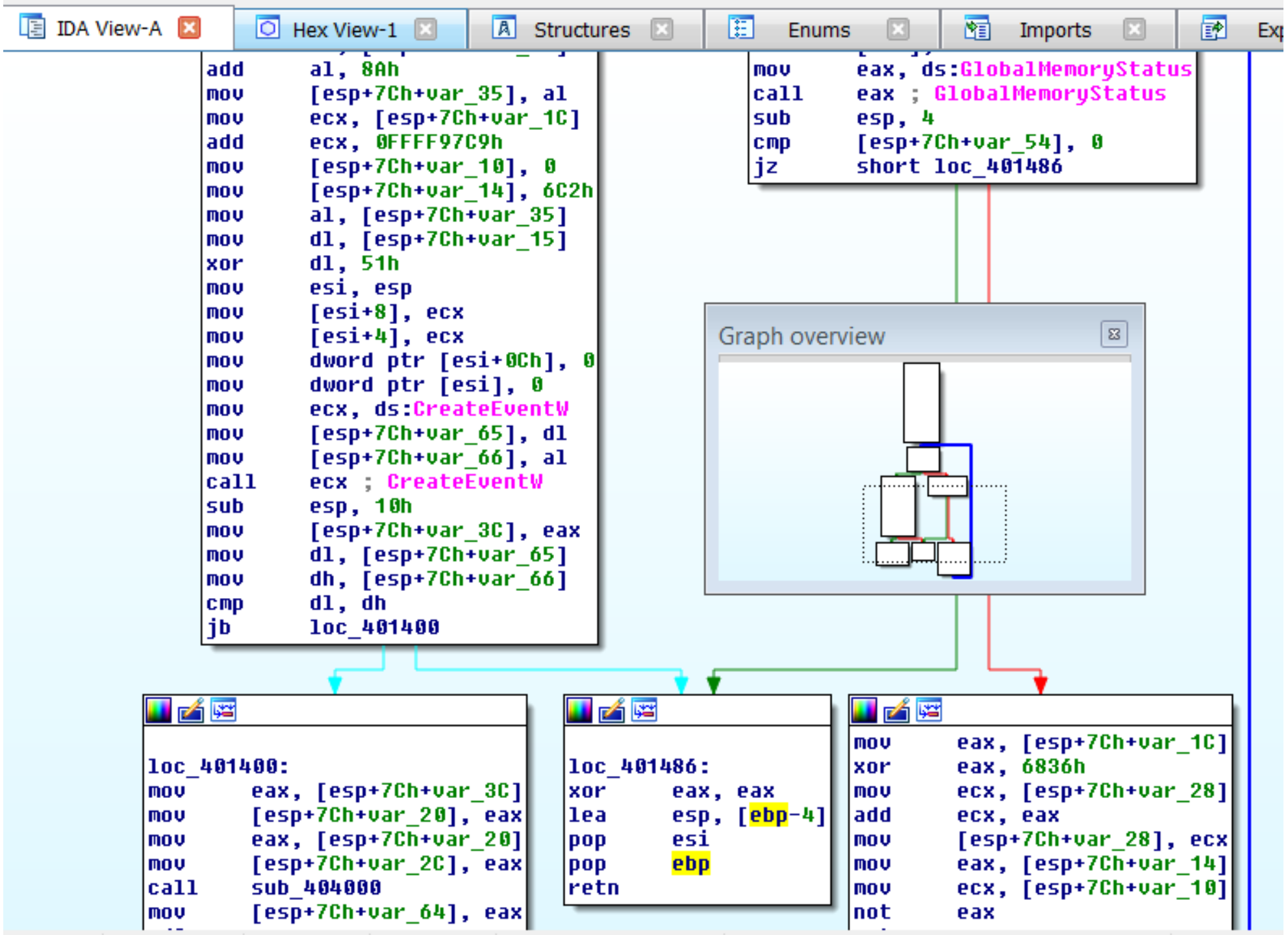
Type	Size	Secti...	Blacklisted (15)	Item (3786)
ascii	4	?:0x0...	x	.crt
ascii	6	?:0x0...	x	.erloc
ascii	5	?:0x0...	x	.rsrc
ascii	12	para:...	x	VirtualAlloc
ascii	11	.rdata...	x	CLUSAPI.dll
ascii	10	.rdata...	x	msvcrt.dll
ascii	11	.rdata...	x	CreateEvent
ascii	18	.rdata...	x	GlobalMemoryStatus
ascii	12	.rdata...	x	KERNEL32.dll
ascii	10	.rdata...	x	USER32.dll
ascii	31	.rdata...	x	E:\Tools\aolfed\release\osc.pdb
unicode	9	.rdata...	x	ntdll.dll
unicode	12	.rdata...	x	kernel32.dll
unicode	11	.crt:0x...	x	control.ini
unicode	9	.crt:0x...	x	nbvgg.hlp
ascii	40	?:0x0...	-	!This program cannot be run in DOS mode.
ascii	4	?:0x0...	-	Rich
ascii	5	?:0x0...	-	.text
ascii	5	?:0x0...	-	`para
ascii	7	?:0x0...	-	`.rdata
ascii	6	?:0x0...	-	`.data
ascii	4	?:0x0...	-	CODE
ascii	4	?:0x0...	-	5ZP@
ascii	4	.text:0...	-	=LP@
ascii	4	.text:0...	-	^_[]

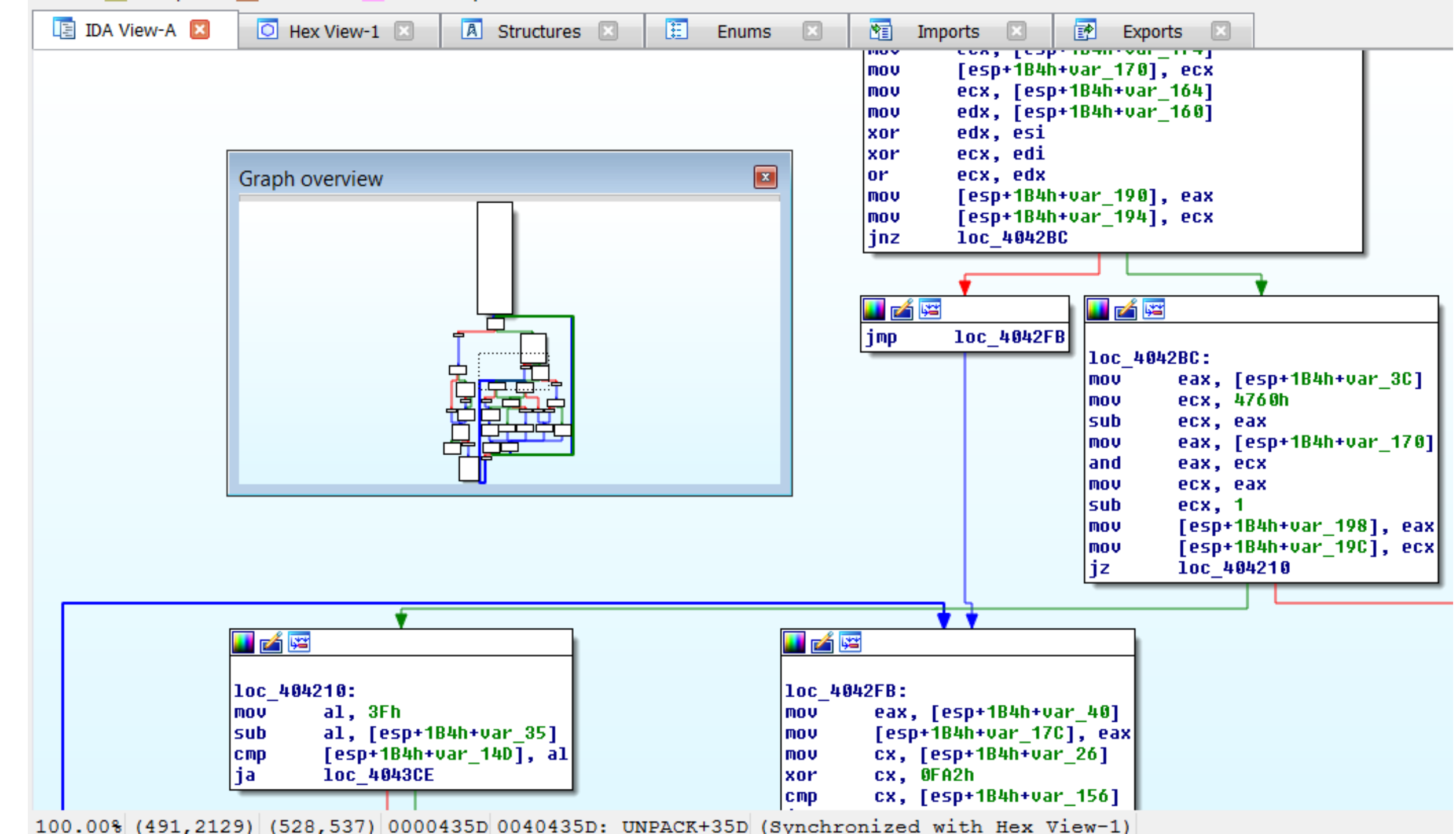
ContextEdit

Control which items are displayed on your context menu by using this user-friendly and straightforward software solution that supports numerous formats

The Windows context menu may become choked by numerous entries in case you install lots of new applications and since sometimes the removal process isn't quite efficient, you might end up with many invalid entries.

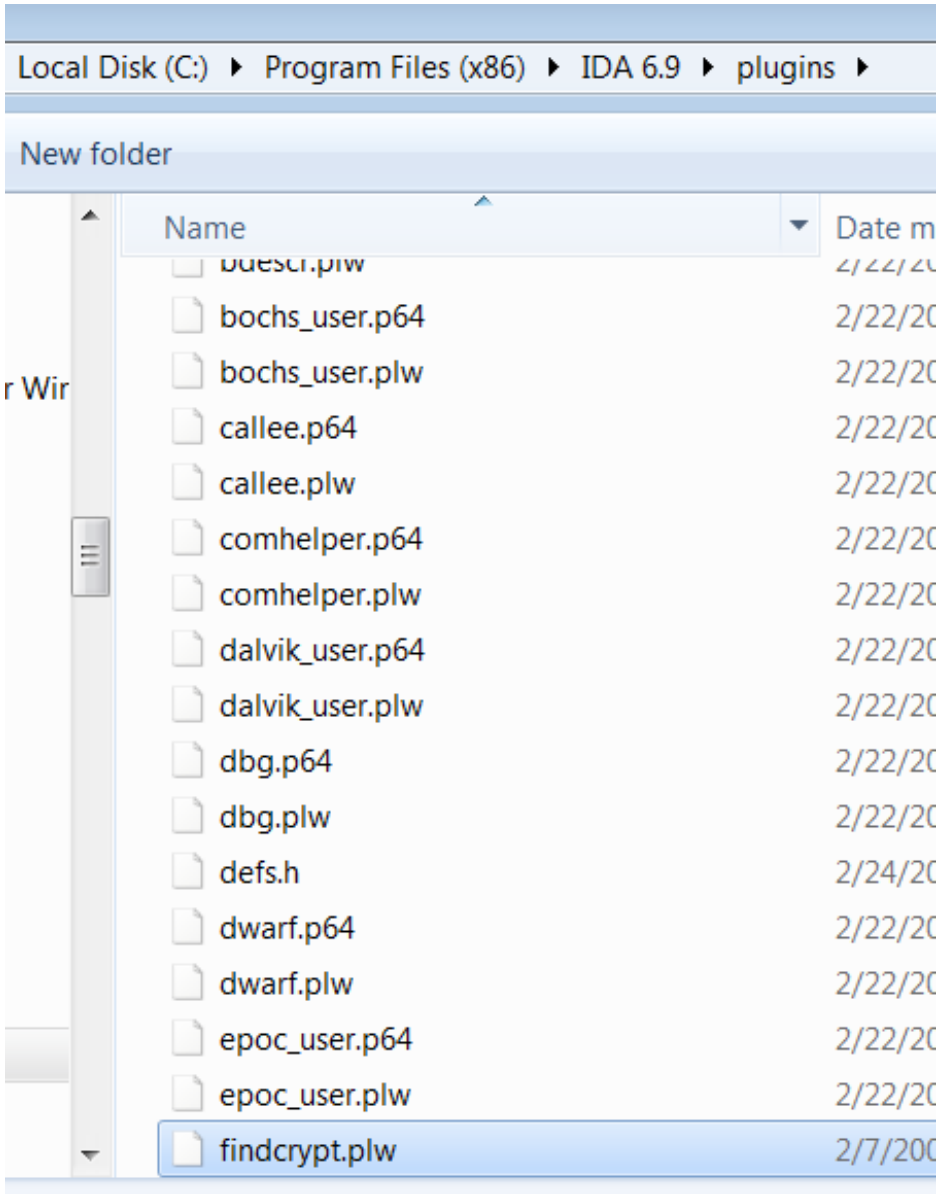

public start
start proc near
mov dword_414DA0, esi
push ebp
push esp
mov dword_414DA4, edi
pop dword_414DB0
mov dword_414DA8, ebx
pop dword_414DAC
mov dword_414DA0, esi
jmp sub_4013D0
start endp
public start
start proc near
mov dword_414DA0, esi
push ebp
push esp
mov dword_414DA4, edi
pop dword_414DB0
mov dword_414DA8, ebx
pop dword_414DAC
mov dword_414DA0, esi
jmp Main?
start endp

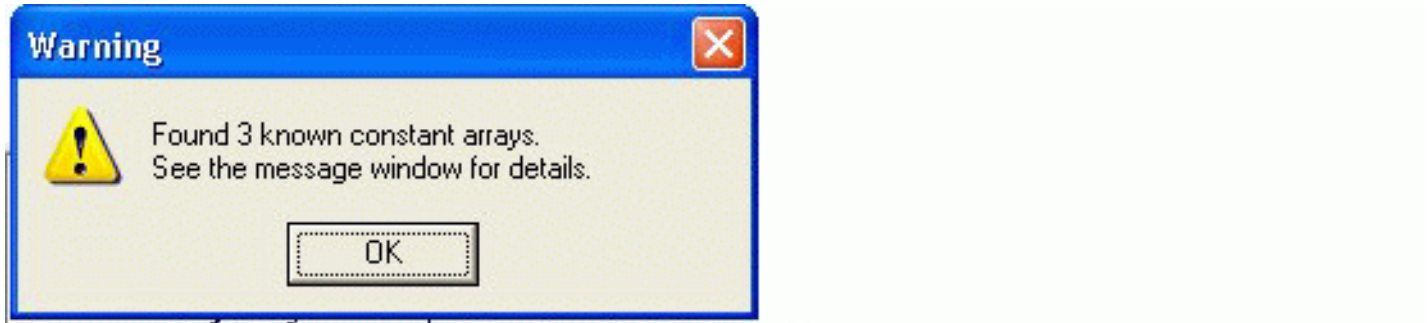

IDA View-A
Hex View-1
Structures
Enums
Imports
add al, 8Ah
mov [esp+7Ch+var_35], al
mov ecx, [esp+7Ch+var_1C]
add ecx, 0FFFF97C9h
mov [esp+7Ch+var_10], 0
mov [esp+7Ch+var_14], 6C2h
mov al, [esp+7Ch+var_35]
mov dl, [esp+7Ch+var_15]
xor dl, 51h
mov esi, esp
mov [esi+8], ecx
mov [esi+4], ecx
mov dword ptr [esi+0Ch], 0
mov dword ptr [esi], 0
mov ecx, ds:CreateEventW
mov [esp+7Ch+var_65], dl
mov [esp+7Ch+var_66], al
call ecx ; CreateEventW
sub esp, 10h
mov [esp+7Ch+var_3C], eax
mov dl, [esp+7Ch+var_65]
mov dh, [esp+7Ch+var_66]
cmp dl, dh
jb loc_401400
mov eax, ds:GlobalMemoryStatus
call eax ; GlobalMemoryStatus
sub esp, 4
cmp [esp+7Ch+var_54], 0
jz short loc_401486
Graph overview
loc_401400:
mov eax, [esp+7Ch+var_3C]
mov [esp+7Ch+var_20], eax
mov eax, [esp+7Ch+var_20]
mov [esp+7Ch+var_2C], eax
call sub_404000
mov [esp+7Ch+var_64], eax
loc_401486:
xor eax, eax
lea esp, [ebp-4]
pop esi
pop ebp
retn
mov eax, [esp+7Ch+var_1C]
xor eax, 6836h
mov ecx, [esp+7Ch+var_28]
add ecx, eax
mov [esp+7Ch+var_28], ecx
mov eax, [esp+7Ch+var_14]
mov ecx, [esp+7Ch+var_10]
not eax

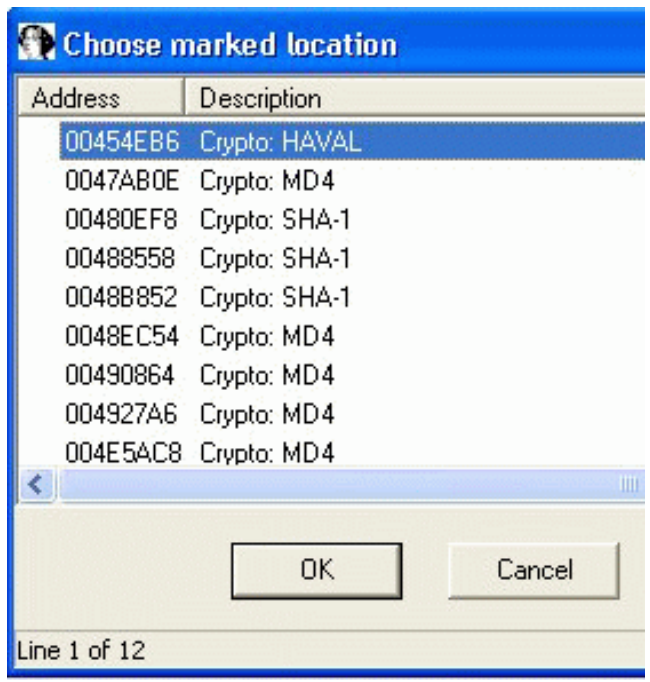

IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
mov [esp+1B4h+var_170], ecx
mov ecx, [esp+1B4h+var_164]
mov edx, [esp+1B4h+var_160]
xor edx, esi
xor ecx, edi
or ecx, edx
mov [esp+1B4h+var_190], eax
mov [esp+1B4h+var_194], ecx
jnz loc_4042BC
jmp loc_4042FB
loc_4042BC:
mov eax, [esp+1B4h+var_3C]
mov ecx, 4760h
sub ecx, eax
mov eax, [esp+1B4h+var_170]
and eax, ecx
mov ecx, eax
sub ecx, 1
mov [esp+1B4h+var_198], eax
mov [esp+1B4h+var_19C], ecx
jz loc_404210
loc_404210:
mov al, 3Fh
sub al, [esp+1B4h+var_35]
cmp [esp+1B4h+var_14D], al
ja loc_4043CE
loc_4042FB:
mov eax, [esp+1B4h+var_40]
mov [esp+1B4h+var_17C], eax
mov cx, [esp+1B4h+var_26]
xor cx, 0FA2h
cmp cx, [esp+1B4h+var_156]
100.00% (491,2129) (528,537) 0000435D 0040435D: UNPACK+35D (Synchronized with Hex View-1)

Finding Crypto Statically

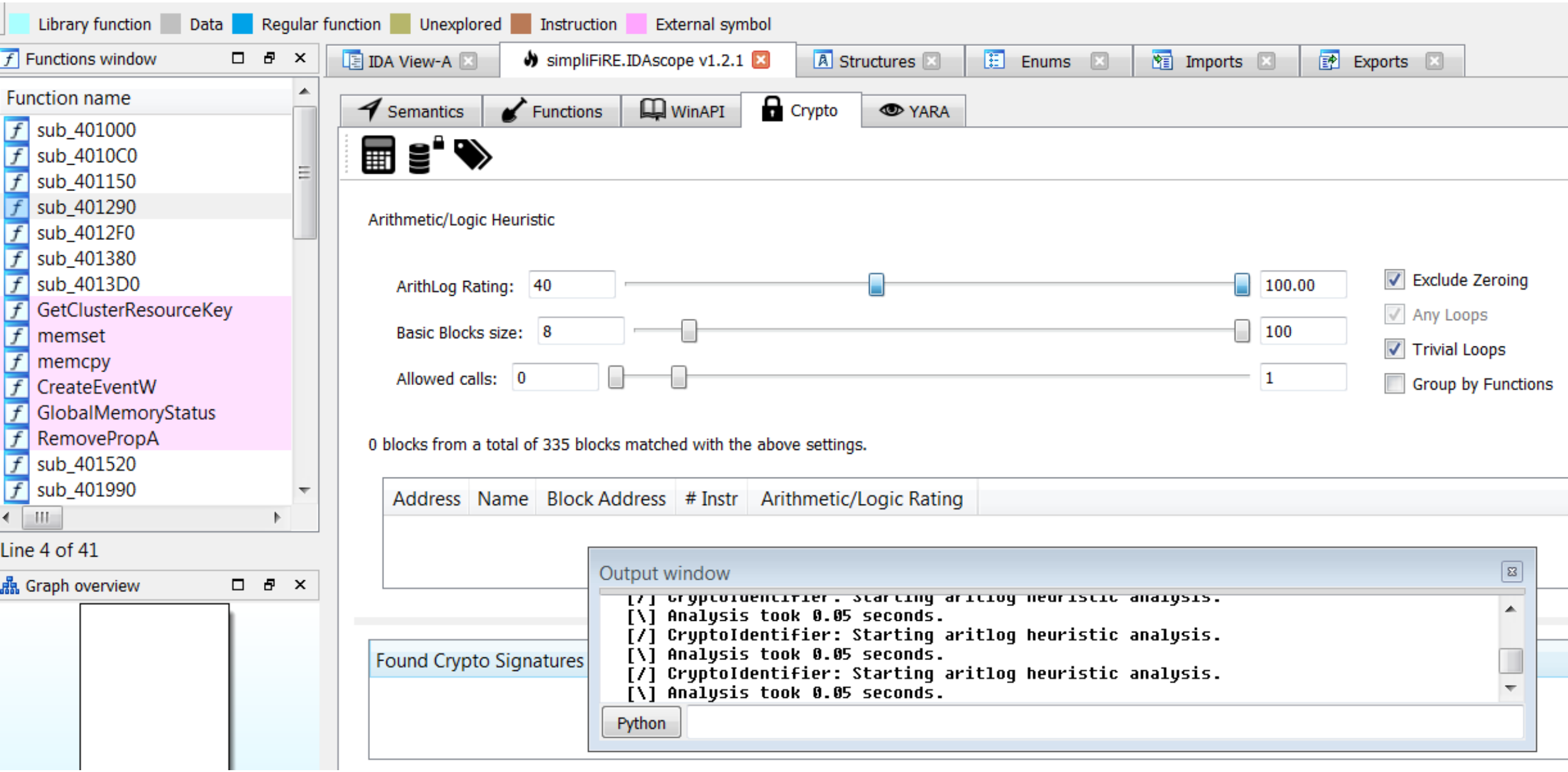
- FindCrypt2
- IDAscope
- Manually

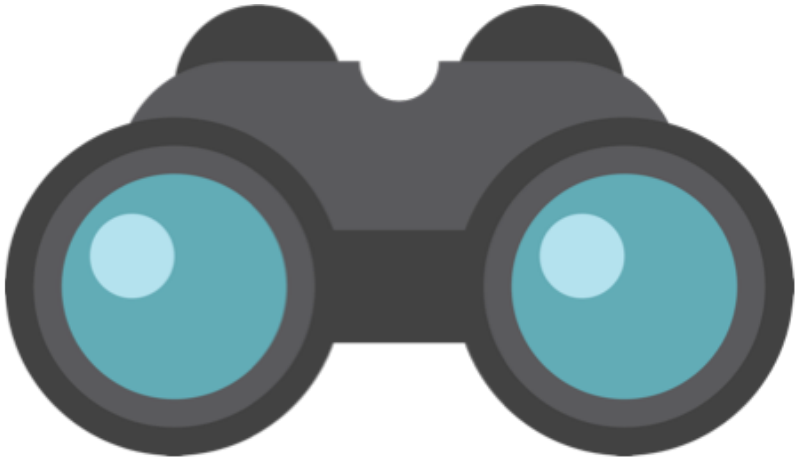

Local Disk (C:) ▸ Program Files (x86) ▸ IDA 6.9 ▸ plugins ▸
New folder
Name
Date m
bochs_user.p64
bochs_user.plw
callee.p64
callee.plw
comhelper.p64
comhelper.plw
dalvik_user.p64
dalvik_user.plw
dbg.p64
dbg.plw
defs.h
dwarf.p64
dwarf.plw
epoc_user.p64
epoc_user.plw
findcrypt.plw


Warning
Found 3 known constant arrays.
See the message window for details.
OK
You may start to explore the input file right now.
100FC9D8: found const array CRC32_m_tab (used in CRC32)
100FF65C: found const array zinflate_lengthExtraBits (used in zlib)
100FF6D0: found const array zinflate_distanceExtraBits (used in zlib)


Choose marked location
Address
Description
00454EB6 Crypto: HAVAL
0047AB0E Crypto: MD4
00480EF8 Crypto: SHA-1
00488558 Crypto: SHA-1
0048B852 Crypto: SHA-1
0048EC54 Crypto: MD4
00490864 Crypto: MD4
004927A6 Crypto: MD4
004E5AC8 Crypto: MD4
OK
Cancel
Line 1 of 12

https://bitbucket.org/daniel_plohmann/simplifire.idascope





Dynamic

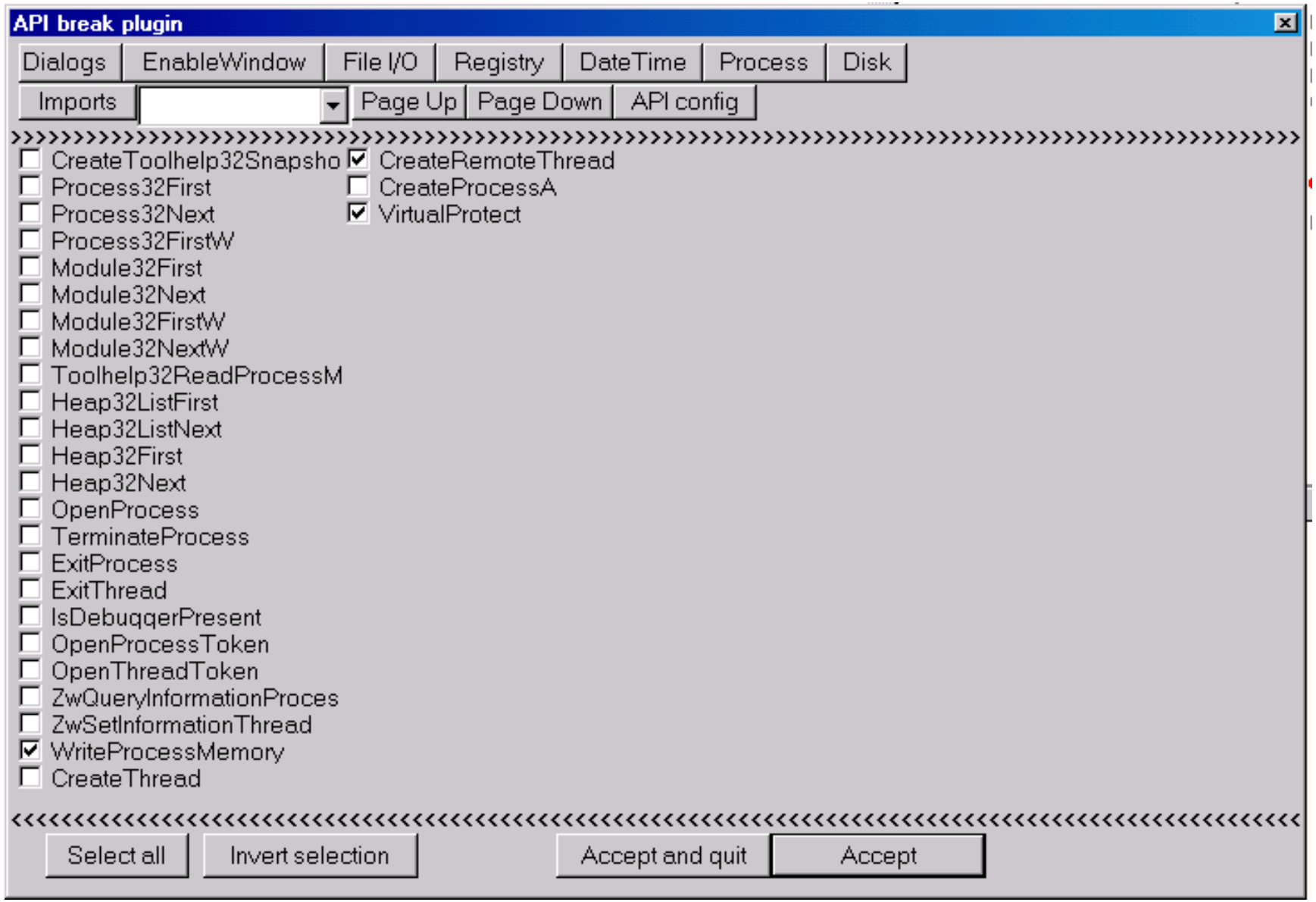
- Locate original entry point
  - Use breakpoints
- Dump process to disk
- Reconstruct binary
  - Repair import table

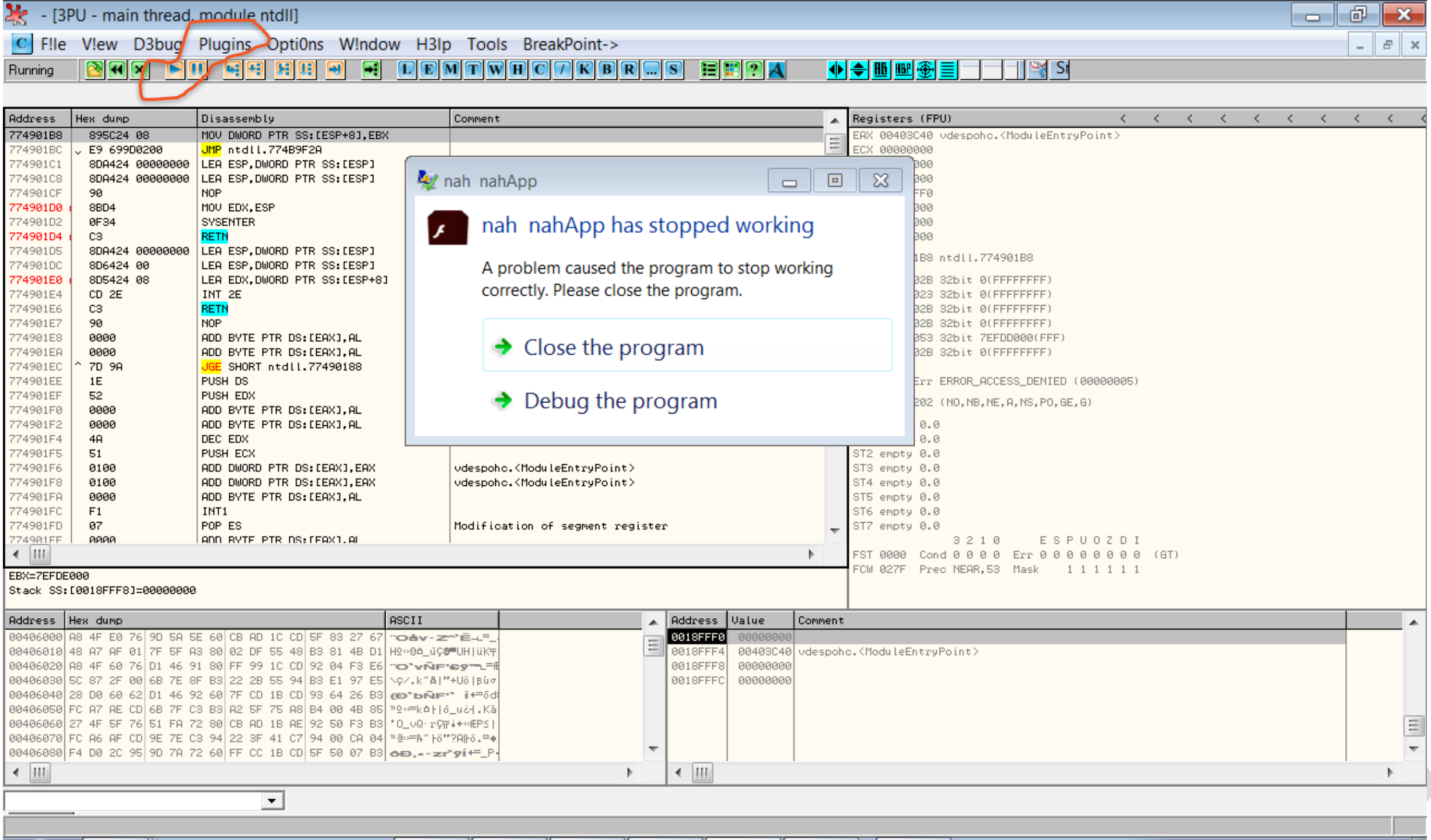
OllyDbg Engines / Modifications [Find the original OllyDbg and custom / modified engines here...]

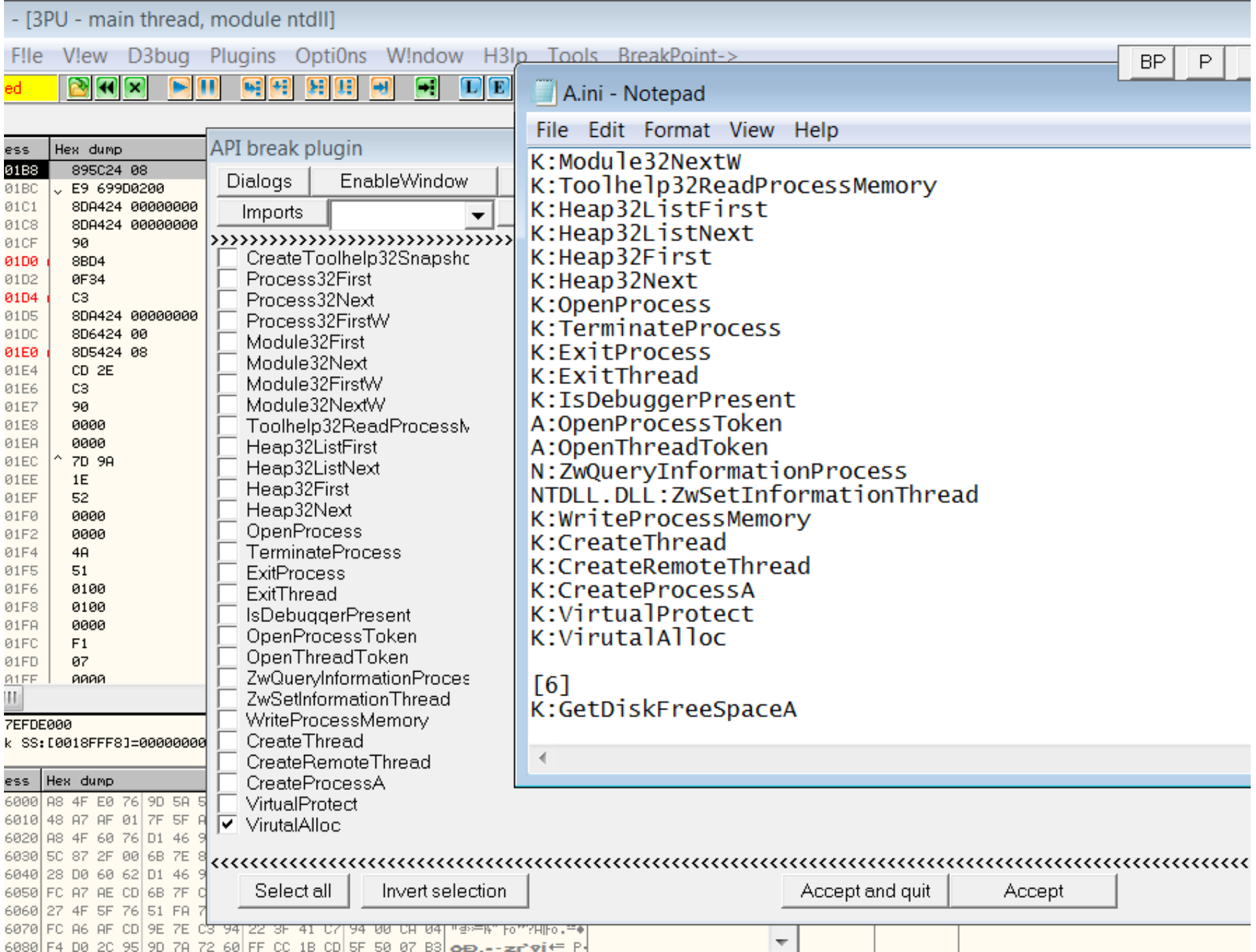
OllyDbg - UST_2bg

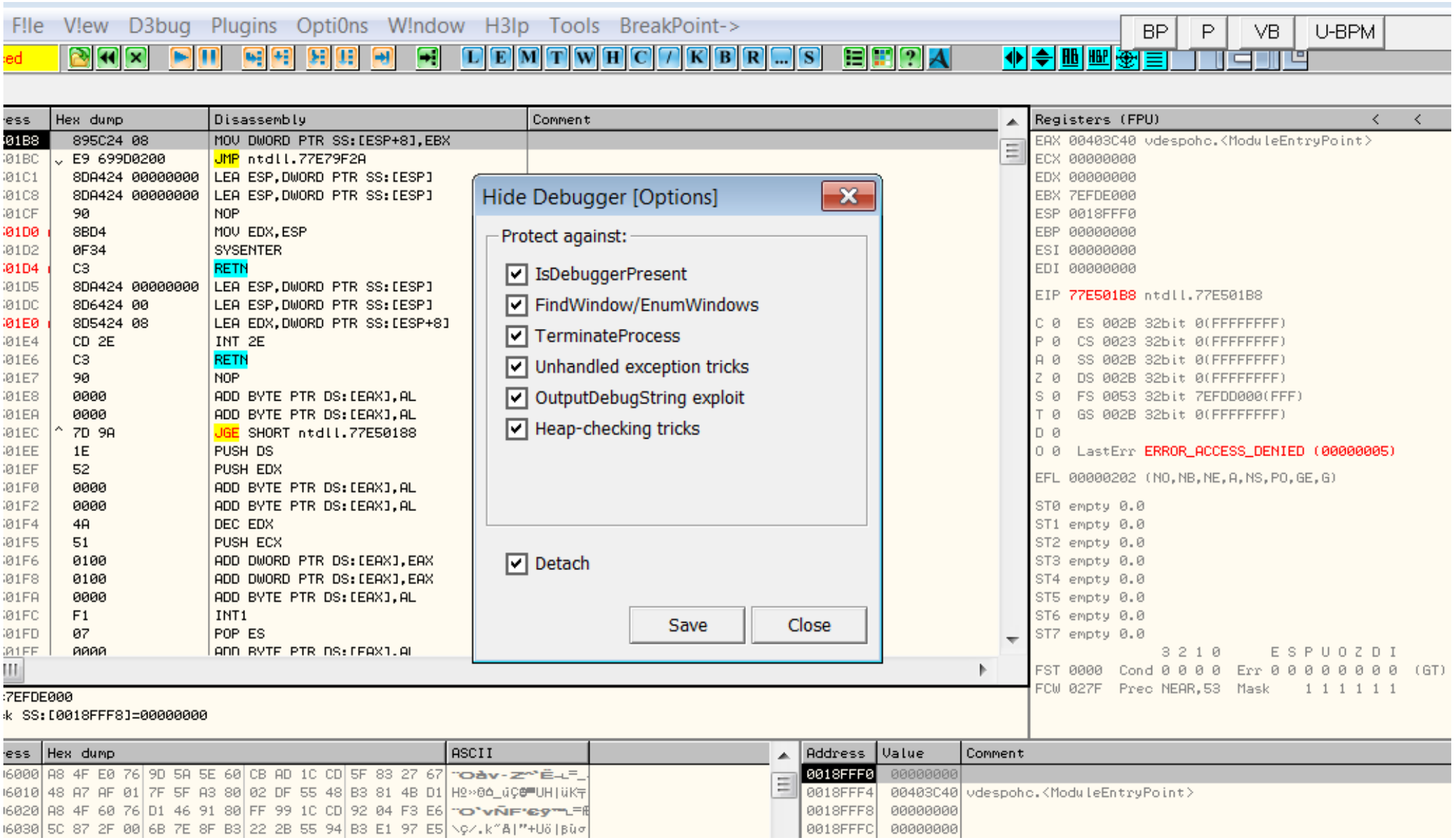
Author	AnTiCDLoCK
Author website	http://forum.tuts4you.com/index.php?showforum=46
Description	A nice modification of the original OllyDbg 1.10 engine. Contains; a quick breakpoint feature, common and popular plugins, toolbar, extra features and slight visual changes.
Image	no image available
Filesize	2.94 MB
Date	Sunday 04 October 2009 - 09:40:37
Downloads	6803
Download	
Rating	Not rated

<< Previous [OllyDbg 2.01 Final] Back to list [OllyDbg - EvO_DBG] Next >>


API break plugin
Dialogs
EnableWindow
File I/O
Registry
DateTime
Process
Disk
Imports
Page Up
Page Down
API config
CreateToolhelp32Snapsho
Process32First
Process32Next
Process32FirstW
Module32First
Module32Next
Module32FirstW
Module32NextW
ToolhelpReadProcessM
Heap32ListFirst
Heap32ListNext
Heap32First
Heap32Next
OpenProcess
TerminateProcess
ExitProcess
ExitThread
IsDebuqqerPresent
OpenProcessToken
OpenThreadToken
ZwQueryInformationProces
ZwSetInformationThread
WriteProcessMemory
CreateThread
CreateRemoteThread
CreateProcessA
VirtualProtect
Select all
Invert selection
Accept and quit
Accept


- [3PU - main thread, module ntdll]
F!le V!ew D3bug Plugins Opti0ns W!ndow H3lp Tools BreakPoint->
Running
Address Hex dump Disassembly Comment
774901B8 895C24 08 MOV DWORD PTR SS:[ESP+8],EBX
774901BC E9 699D0200 JMP ntdll.774B9F2A
774901C1 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
774901C8 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
774901CF 90 NOP
774901D0 8BD4 MOV EDX,ESP
774901D2 0F34 SYSENTER
774901D4 C3 RETN
774901D5 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
774901DC 8D6424 00 LEA ESP,DWORD PTR SS:[ESP]
774901E0 8D5424 08 LEA EDX,DWORD PTR SS:[ESP+8]
774901E4 CD 2E INT 2E
774901E6 C3 RETN
774901E7 90 NOP
774901E8 0000 ADD BYTE PTR DS:[EAX],AL
774901EA 0000 ADD BYTE PTR DS:[EAX],AL
774901EC 7D 9A JGE SHORT ntdll.77490188
774901EE 1E PUSH DS
774901EF 52 PUSH EDX
774901F0 0000 ADD BYTE PTR DS:[EAX],AL
774901F2 0000 ADD BYTE PTR DS:[EAX],AL
774901F4 4A DEC EDX
774901F5 51 PUSH ECX
774901F6 0100 ADD DWORD PTR DS:[EAX],EAX vdespohc.<ModuleEntryPoint>
774901F8 0100 ADD DWORD PTR DS:[EAX],EAX vdespohc.<ModuleEntryPoint>
774901FA 0000 ADD BYTE PTR DS:[EAX],AL
774901FC F1 INT1
774901FD 07 POP ES Modification of segment register
Registers (FPU)
EAX 00403C40 vdespohc.<ModuleEntryPoint>
ECX 00000000
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
nah nahApp
nah nahApp has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Debug the program
EBX=7EFDE000
Stack SS:[0018FFF8]=00000000
Address Hex dump ASCII
00406000 A8 4F E0 76 9D 5A 5E 60 CB AD 1C CD 5F 83 27 67
00406010 48 A7 AF 01 7F 5F A3 80 02 DF 55 48 B3 81 4B D1
00406020 A8 4F 60 76 D1 46 91 80 FF 99 1C CD 92 04 F3 E6
00406030 5C 87 2F 00 6B 7E 8F B3 22 2B 55 94 B3 E1 97 E5
00406040 28 D0 60 62 D1 46 92 60 7F CD 1B CD 93 64 26 B3
00406050 FC A7 AE CD 6B 7F C3 B3 A2 5F 75 A8 B4 00 4B 85
00406060 27 4F 5F 76 51 FA 72 80 CB AD 1B AE 92 50 F3 B3
00406070 FC A6 AF CD 9E 7E C3 94 22 3F 41 C7 94 00 CA 04
00406080 F4 D0 2C 95 9D 7A 72 60 FF CC 1B CD 5F 50 07 B3
Address Value Comment
0018FFF0 00000000
0018FFF4 00403C40 vdespohc.<ModuleEntryPoint>
0018FFF8 00000000
0018FFFC 00000000


- [3PU - main thread, module ntdll]
F!le V!ew D3bug Plugins Opti0ns W!ndow H3lp Tools BreakPoint->
BP
P
A.ini - Notepad
File Edit Format View Help
K:Module32NextW
K:Toolhelp32ReadProcessMemory
K:Heap32ListFirst
K:Heap32ListNext
K:Heap32First
K:Heap32Next
K:OpenProcess
K:TerminateProcess
K:ExitProcess
K:ExitThread
K:IsDebuggerPresent
A:OpenProcessToken
A:OpenThreadToken
N:ZwQueryInformationProcess
NTDLL.DLL:ZwSetInformationThread
K:WriteProcessMemory
K:CreateThread
K:CreateRemoteThread
K:CreateProcessA
K:VirtualProtect
K:VirutalAlloc
[6]
K:GetDiskFreeSpaceA
API break plugin
Dialogs
EnableWindow
Imports
CreateToolhelp32Snapshc
Process32First
Process32Next
Process32FirstW
Module32First
Module32Next
Module32FirstW
Module32NextW
ToolhelpReadProcessM
Heap32ListFirst
Heap32ListNext
Heap32First
Heap32Next
OpenProcess
TerminateProcess
ExitProcess
ExitThread
IsDebuqqerPresent
OpenProcessToken
OpenThreadToken
ZwQueryInformationProces
ZwSetInformationThread
WriteProcessMemory
CreateThread
CreateRemoteThread
CreateProcessA
VirtualProtect
VirutalAlloc
Select all
Invert selection
Accept and quit
Accept
Hex dump
01B8 895C24 08
01BC E9 699D0200
01C1 8DA424 00000000
01C8 8DA424 00000000
01CF 90
01D0 8BD4
01D2 0F34
01D4 C3
01D5 8DA424 00000000
01DC 8D6424 00
01E0 8D5424 08
01E4 CD 2E
01E6 C3
01E7 90
01E8 0000
01EA 0000
01EC 7D 9A
01EE 1E
01EF 52
01F0 0000
01F2 0000
01F4 4A
01F5 51
01F6 0100
01F8 0100
01FA 0000
01FC F1
01FD 07
7EFDE000
SS:[0018FFF8]=00000000


F!le V!ew D3bug Plugins Opti0ns W!ndow H3lp Tools BreakPoint->
BP P VB U-BPM
Hide Debugger [Options]
Protect against:
IsDebuggerPresent
FindWindow/EnumWindows
TerminateProcess
Unhandled exception tricks
OutputDebugString exploit
Heap-checking tricks
Detach
Save
Close
Registers (FPU)

NtQuery / Scylla

Imports Reconstructor

206 commits 1 branch 8 releases 3 contributors

Branch: master New pull request New file Upload files Find file HTTPS https://github.com/NtQuer Download ZIP

NtQuery Merge pull request #35 from mrexodia/fix_leaks ... Latest commit 0ca2c1a 24 days ago

Plugins	readme update	a year ago
Scylla	Merge pull request #35 from mrexodia/fix_leaks	24 days ago
ScyllaDllTest	dll tester	2 years ago
WTL	README for tinyxml + generic WTL directory (+ readme) + added gitigno…	a year ago
diStorm	distorm update	11 months ago
tinyxml	README for tinyxml + generic WTL directory (+ readme) + added gitigno…	a year ago
.gitignore	include distorm	11 months ago
COMPILING	README for tinyxml + generic WTL directory (+ readme) + added gitigno…	a year ago
LICENSE	new readme and license file	5 years ago

https://tuts4you.com/download.php?view.415

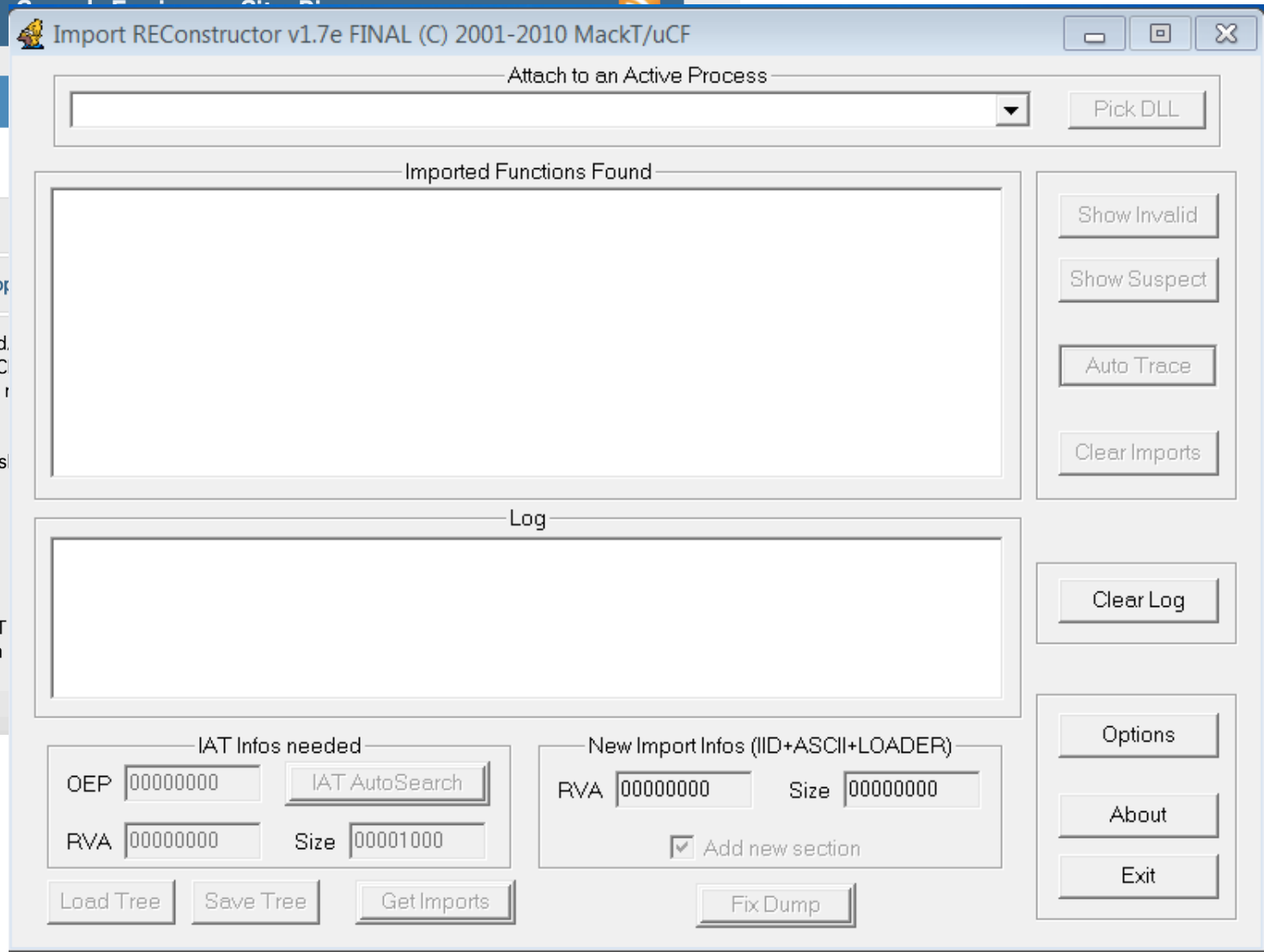
TUTS4YOU

Latest Downloads Forums Blogs Submissions

IAT / PE Rebuilding [IAT and portable executable rebuilding...]

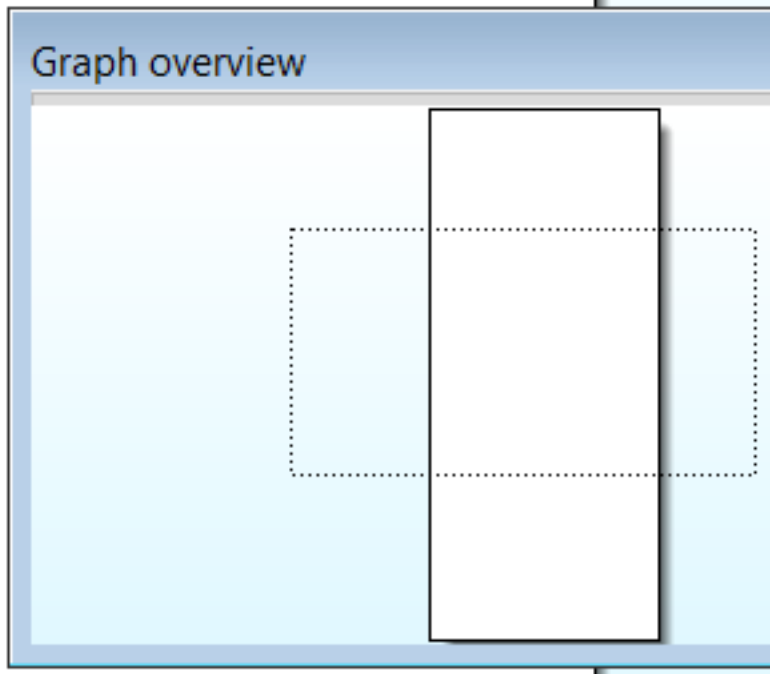
Import REConstructor 1.7e FINAL

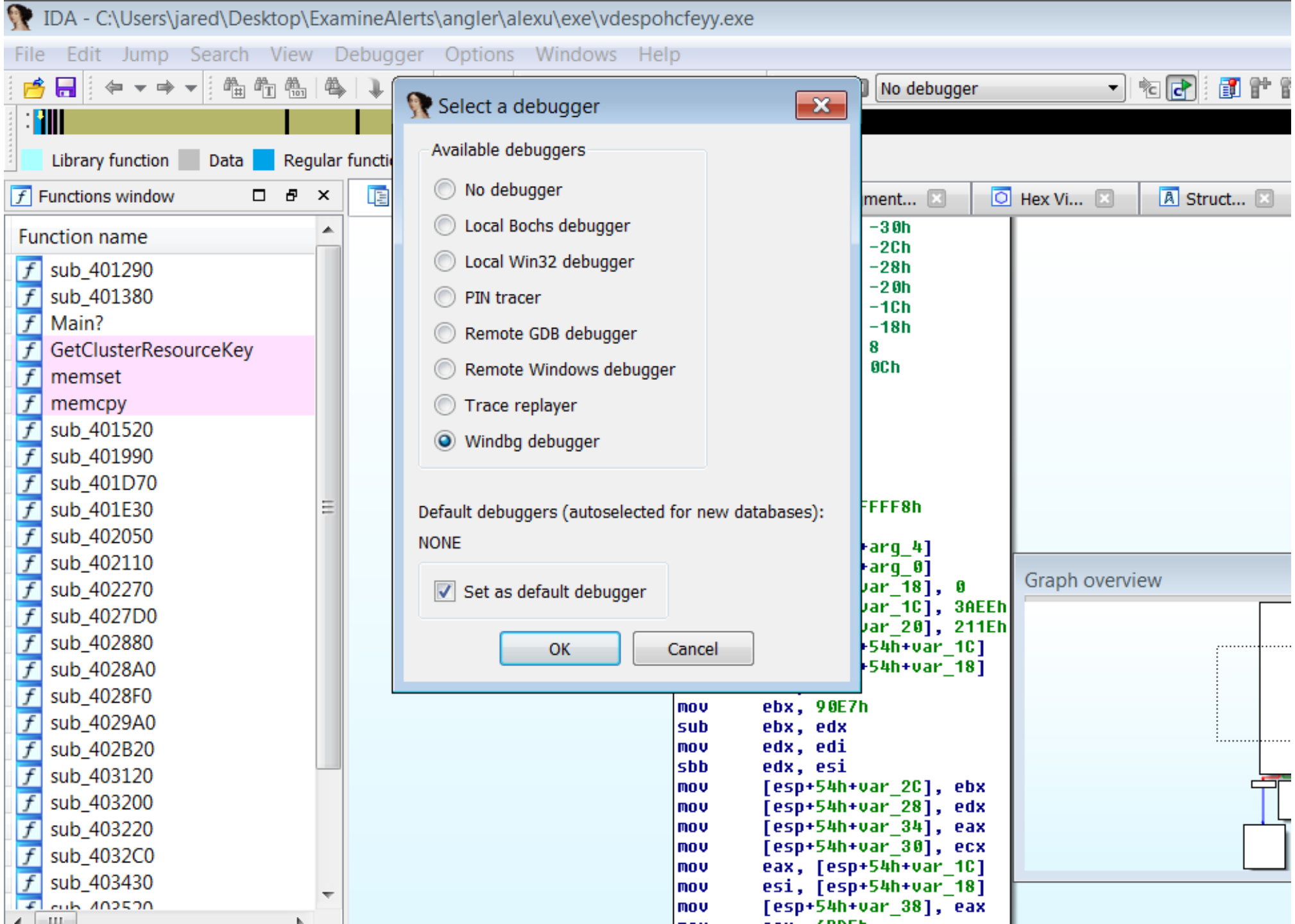
Author	MackT
Author website	http://www.tuts4you.com/forum/index.php?showtop
Description	This tool is designed to rebuild imports for protected Descriptor (IID), Import Array Table (IAT) and all ASC executable, a loader which is able to fill the IAT with r useful against emulated API in a thunk). Sorry but this tool is not designed for newbies, you s easy to find on internet). Features: - Imports - An original tree view - 2 different methods to find original imports (by IAT - A *FULL* complete rebuilder (including a new fresh - Loader - An analyzer and ripper of redirected API code



PID	File Path	Base	Length	Protection	Completion	Count	Source Address	Symbol
2948	C:\Windows\xfjpayxmgocb.exe	1E0000	303104	page read and write	success or wait success or wait	1	4016D6	VirtualAlloc
2948	C:\Windows\xfjpayxmgocb.exe	340000	544768	page execute and read and write	success or wait success or wait	1	401DCB	VirtualAlloc
2948	C:\Windows\xfjpayxmgocb.exe	1280000	544768	page read and write	success or wait success or wait	1	342384	VirtualAlloc
2948	C:\Windows\xfjpayxmgocb.exe	1310000	1638400	page read and write	success or wait success or wait	1	4282B3	HeapCreate
2948	C:\Windows\xfjpayxmgocb.exe	1490000	4096	page read and write	success or wait success or wait	1	4282B3	HeapCreate

```
push    edi
push    esi
sub     esp, 2Ch
mov     eax, [ebp+arg_4]
mov     ecx, [ebp+arg_0]
mov     [ebp+var_14], 249Dh
mov     [ebp+var_1C], eax
mov     [ebp+var_20], ecx
mov     eax, esp
mov     dword ptr [eax], offset aVirtualalloc ; "VirtualAlloc"
call    sub_402050
sub     esp, 4
mov     [ebp+var_24], eax
mov     ecx, [ebp+var_14]
mov     edx, ecx
add     edx, 0FFFFEB63h
mov     esi, ecx
add     esi, 0FFFFDBA3h
add     ecx, 82B63h
mov     edi, esp
mov     [edi+0Ch], esi
mov     [edi+8], edx
mov     [edi+4], ecx
mov     dword ptr [edi], 0
call    eax
sub     esp, 10h
mov     [ebp+var_18], eax
mov     ecx, [ebp+var_1C]
mov     edx, esp
mov     [edx+4], ecx
mov     [edx], eax
call    sub_401E30
```




IDA - C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfeyy.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function
Data
Regular functi
Functions window
Function name
sub_401290
sub_401380
Main?
GetClusterResourceKey
memset
memcpy
sub_401520
sub_401990
sub_401D70
sub_401E30
sub_402050
sub_402110
sub_402270
sub_4027D0
sub_402880
sub_4028A0
sub_4028F0
sub_4029A0
sub_402B20
sub_403120
sub_403200
sub_403220
sub_4032C0
sub_403430
Hex Vi...
Struct...
Select a debugger
Available debuggers
No debugger
Local Bochs debugger
Local Win32 debugger
PIN tracer
Remote GDB debugger
Remote Windows debugger
Trace replayer
Windbg debugger
Default debuggers (autoselected for new databases):
NONE
Set as default debugger
OK
Cancel
-30h
-2Ch
-28h
-20h
-1Ch
-18h
8
0Ch
FFFF8h
+arg_4]
+arg_0]
var_18], 0
var_1C], 3AEEh
var_20], 211Eh
+54h+var_1C]
+54h+var_18]
mov ebx, 90E7h
sub ebx, edx
mov edx, edi
sbb edx, esi
mov [esp+54h+var_2C], ebx
mov [esp+54h+var_28], edx
mov [esp+54h+var_34], eax
mov [esp+54h+var_30], ecx
mov eax, [esp+54h+var_1C]
mov esi, [esp+54h+var_18]
mov [esp+54h+var_38], eax
Graph overview

nihilus / idastealth

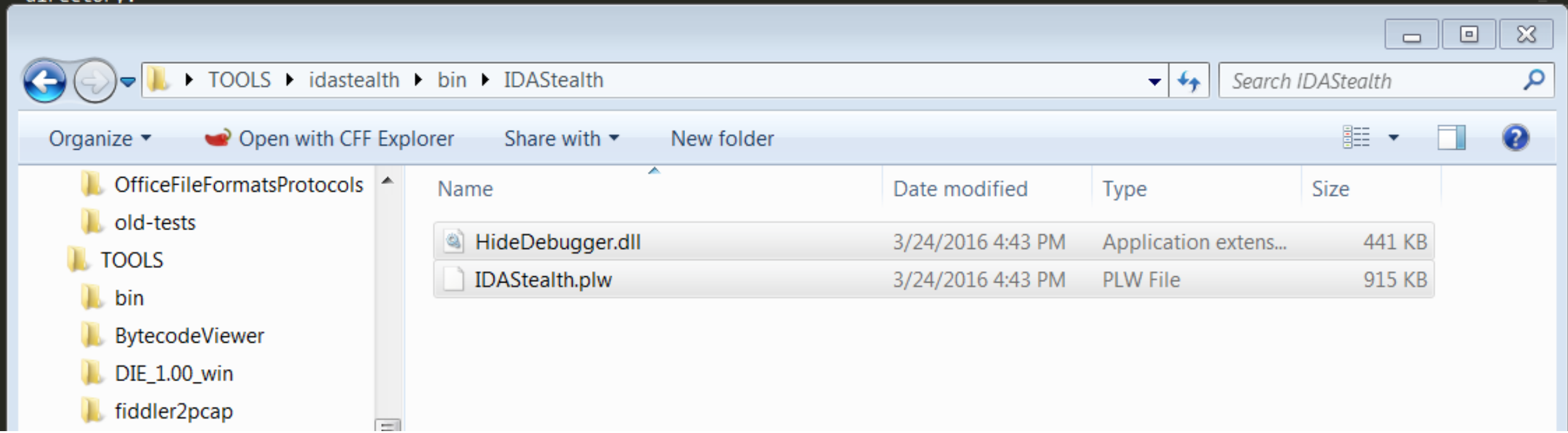
http://newgre.net/idastealth

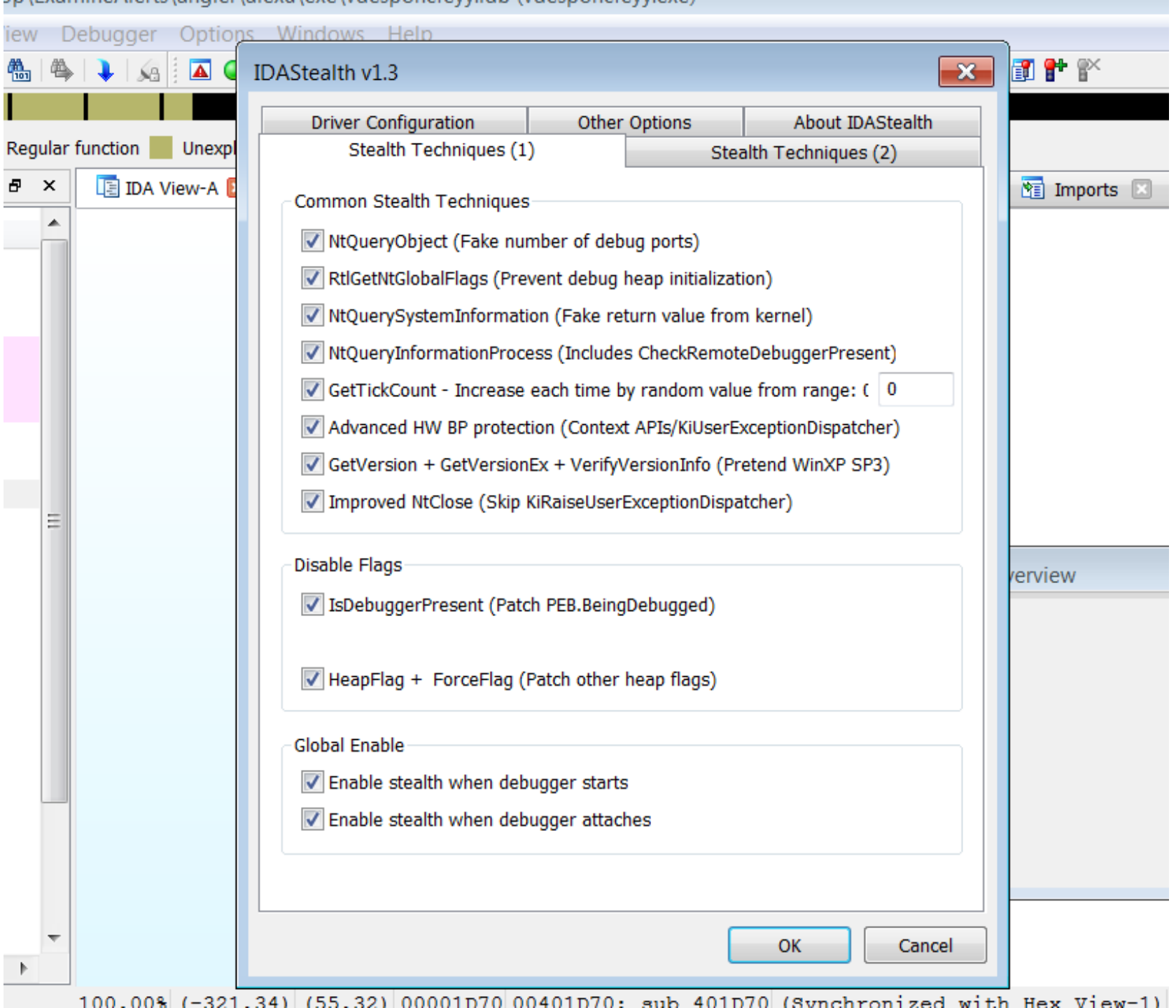
10 commits 1 branch 0 releases 1 contributor

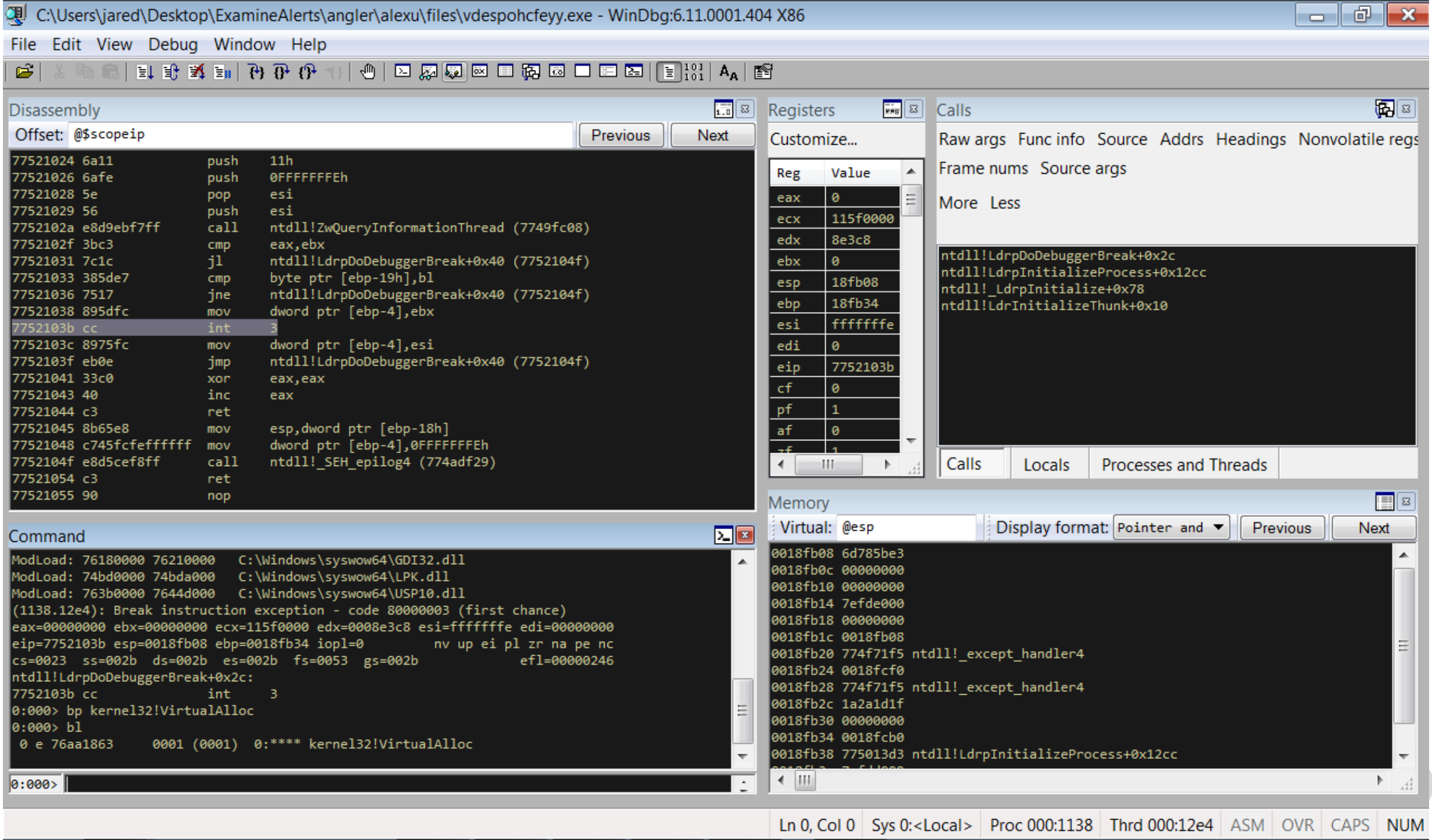
nihilus Fixed bin — Latest commit `88fcf58` on Sep 13, 2014

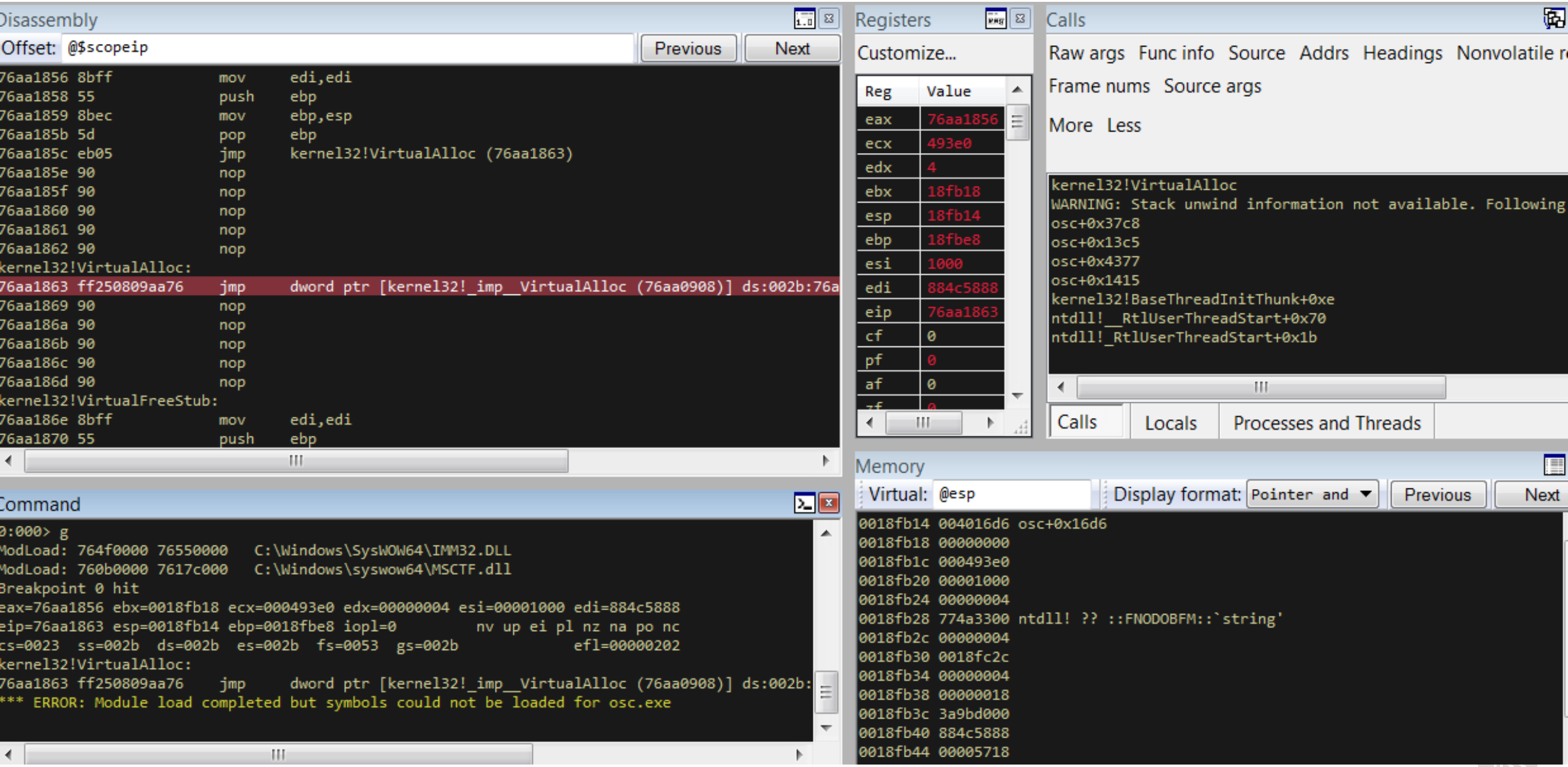
bin	Fixed bin	2 years ago
distorm	Initial ci from rar archive.	2 years ago
sample_config	Initial ci from rar archive.	2 years ago
src	Fixed bin	2 years ago
.gitignore	Added .gitignore files	2 years ago
ddkbuild.cmd	Added .gitignore files	2 years ago

```
14
15  INSTALLATION
16  ------------
17
18  a) IDAStealth
19  Copy both, HideDebugger.dll and IDAStealth.plw to your IDA plugin
20  directory.
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
```




IDAStealth v1.3
Driver Configuration
Other Options
About IDAStealth
Stealth Techniques (1)
Stealth Techniques (2)
Common Stealth Techniques
NtQueryObject (Fake number of debug ports)
RtlGetNtGlobalFlags (Prevent debug heap initialization)
NtQuerySystemInformation (Fake return value from kernel)
NtQueryInformationProcess (Includes CheckRemoteDebuggerPresent)
GetTickCount - Increase each time by random value from range: (
0
Advanced HW BP protection (Context APIs/KiUserExceptionDispatcher)
GetVersion + GetVersionEx + VerifyVersionInfo (Pretend WinXP SP3)
Improved NtClose (Skip KiRaiseUserExceptionDispatcher)
Disable Flags
IsDebuggerPresent (Patch PEB.BeingDebugged)
HeapFlag + ForceFlag (Patch other heap flags)
Global Enable
Enable stealth when debugger starts
Enable stealth when debugger attaches
OK
Cancel
IDA View-A
Imports
Regular function
Debugger
Options
Windows
Help


C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\files\vdespohcfeyy.exe - WinDbg:6.11.0001.404 X86
File Edit View Debug Window Help
Disassembly
Offset: @$scopeip
Previous
Next
77521024 6a11 push 11h
77521026 6afe push 0FFFFFFFEh
77521028 5e pop esi
77521029 56 push esi
7752102a e8d9ebf7ff call ntdll!ZwQueryInformationThread (7749fc08)
7752102f 3bc3 cmp eax,ebx
77521031 7c1c jl ntdll!LdrpDoDebuggerBreak+0x40 (7752104f)
77521033 385de7 cmp byte ptr [ebp-19h],bl
77521036 7517 jne ntdll!LdrpDoDebuggerBreak+0x40 (7752104f)
77521038 895dfc mov dword ptr [ebp-4],ebx
7752103b cc int 3
7752103c 8975fc mov dword ptr [ebp-4],esi
7752103f eb0e jmp ntdll!LdrpDoDebuggerBreak+0x40 (7752104f)
77521041 33c0 xor eax,eax
77521043 40 inc eax
77521044 c3 ret
77521045 8b65e8 mov esp,dword ptr [ebp-18h]
77521048 c745fcfeffffff mov dword ptr [ebp-4],0FFFFFFFEh
7752104f e8d5cef8ff call ntdll!_SEH_epilog4 (774adf29)
77521054 c3 ret
77521055 90 nop
Registers
Customize...
Reg Value
eax 0
ecx 115f0000
edx 8e3c8
ebx 0
esp 18fb08
ebp 18fb34
esi fffffffe
edi 0
eip 7752103b
cf 0
pf 1
af 0
Calls
Raw args Func info Source Addrs Headings Nonvolatile regs
Frame nums Source args
More Less
ntdll!LdrpDoDebuggerBreak+0x2c
ntdll!LdrpInitializeProcess+0x12cc
ntdll!_LdrpInitialize+0x78
ntdll!LdrInitializeThunk+0x10
Calls
Locals
Processes and Threads
Command
ModLoad: 76180000 76210000 C:\Windows\syswow64\GDI32.dll
ModLoad: 74bd0000 74bda000 C:\Windows\syswow64\LPK.dll
ModLoad: 763b0000 7644d000 C:\Windows\syswow64\USP10.dll
(1138.12e4): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00000000 ecx=115f0000 edx=0008e3c8 esi=fffffffe edi=00000000
eip=7752103b esp=0018fb08 ebp=0018fb34 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2c:
7752103b cc int 3
0:000> bp kernel32!VirtualAlloc
0:000> bl
0 e 76aa1863 0001 (0001) 0:**** kernel32!VirtualAlloc
0:000>
Memory
Virtual: @esp
Display format: Pointer and
Previous
Next
0018fb08 6d785be3
0018fb0c 00000000
0018fb10 00000000
0018fb14 7efde000
0018fb18 00000000
0018fb1c 0018fb08
0018fb20 774f71f5 ntdll!_except_handler4
0018fb24 0018fcf0
0018fb28 774f71f5 ntdll!_except_handler4
0018fb2c 1a2a1d1f
0018fb30 00000000
0018fb34 0018fcb0
0018fb38 775013d3 ntdll!LdrpInitializeProcess+0x12cc
Ln 0, Col 0
Sys 0:<Local>
Proc 000:1138
Thrd 000:12e4
ASM
OVR
CAPS
NUM


Disassembly
Offset: @$scopeip
Previous
Next
76aa1856 8bff mov edi,edi
76aa1858 55 push ebp
76aa1859 8bec mov ebp,esp
76aa185b 5d pop ebp
76aa185c eb05 jmp kernel32!VirtualAlloc (76aa1863)
76aa185e 90 nop
76aa185f 90 nop
76aa1860 90 nop
76aa1861 90 nop
76aa1862 90 nop
kernel32!VirtualAlloc:
76aa1863 ff250809aa76 jmp dword ptr [kernel32!_imp__VirtualAlloc (76aa0908)] ds:002b:76a
76aa1869 90 nop
76aa186a 90 nop
76aa186b 90 nop
76aa186c 90 nop
76aa186d 90 nop
kernel32!VirtualFreeStub:
76aa186e 8bff mov edi,edi
76aa1870 55 push ebp
Command
0:000> g
ModLoad: 764f0000 76550000 C:\Windows\SysWOW64\IMM32.DLL
ModLoad: 760b0000 7617c000 C:\Windows\syswow64\MSCTF.dll
Breakpoint 0 hit
eax=76aa1856 ebx=0018fb18 ecx=000493e0 edx=00000004 esi=00001000 edi=884c5888
eip=76aa1863 esp=0018fb14 ebp=0018fbe8 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000202
kernel32!VirtualAlloc:
76aa1863 ff250809aa76 jmp dword ptr [kernel32!_imp__VirtualAlloc (76aa0908)] ds:002b:
*** ERROR: Module load completed but symbols could not be loaded for osc.exe
Registers
Customize...
Reg Value
eax 76aa1856
ecx 493e0
edx 4
ebx 18fb18
esp 18fb14
ebp 18fbe8
esi 1000
edi 884c5888
eip 76aa1863
cf 0
pf 0
af 0
Calls
Raw args Func info Source Addrs Headings Nonvolatile r
Frame nums Source args
More Less
kernel32!VirtualAlloc
WARNING: Stack unwind information not available. Following
osc+0x37c8
osc+0x13c5
osc+0x4377
osc+0x1415
kernel32!BaseThreadInitThunk+0xe
ntdll!__RtlUserThreadStart+0x70
ntdll!_RtlUserThreadStart+0x1b
Calls
Locals
Processes and Threads
Memory
Virtual: @esp
Display format: Pointer and
Previous
Next
0018fb14 004016d6 osc+0x16d6
0018fb18 00000000
0018fb1c 000493e0
0018fb20 00001000
0018fb24 00000004
0018fb28 774a3300 ntdll! ?? ::FNODOBFM::`string'
0018fb2c 00000004
0018fb30 0018fc2c
0018fb34 00000004
0018fb38 00000018
0018fb3c 3a9bd000
0018fb40 884c5888
0018fb44 00005718

VirtualAlloc function

Reserves, commits, or changes the state of a region of pages in the virtual address space of the calling process. Memory allocated by this function is automatically initialized to zero.

To allocate memory in the address space of another process, use the **VirtualAllocEx** function.

Syntax

C++

```
LPVOID WINAPI VirtualAlloc(
  _In_opt_ LPVOID lpAddress,
  _In_     SIZE_T dwSize,
  _In_     DWORD  flAllocationType,
  _In_     DWORD  flProtect
);
```

Parameters

lpAddress [in, optional]

The starting address of the region to allocate. If the memory is being reserved, the specified address is rounded down to

.childdbg (Debug Child Processes)

The **.childdbg** command controls the debugging of child processes.

```
    .childdbg 0
.childdbg 1
.childdbg
```

Parameters

0

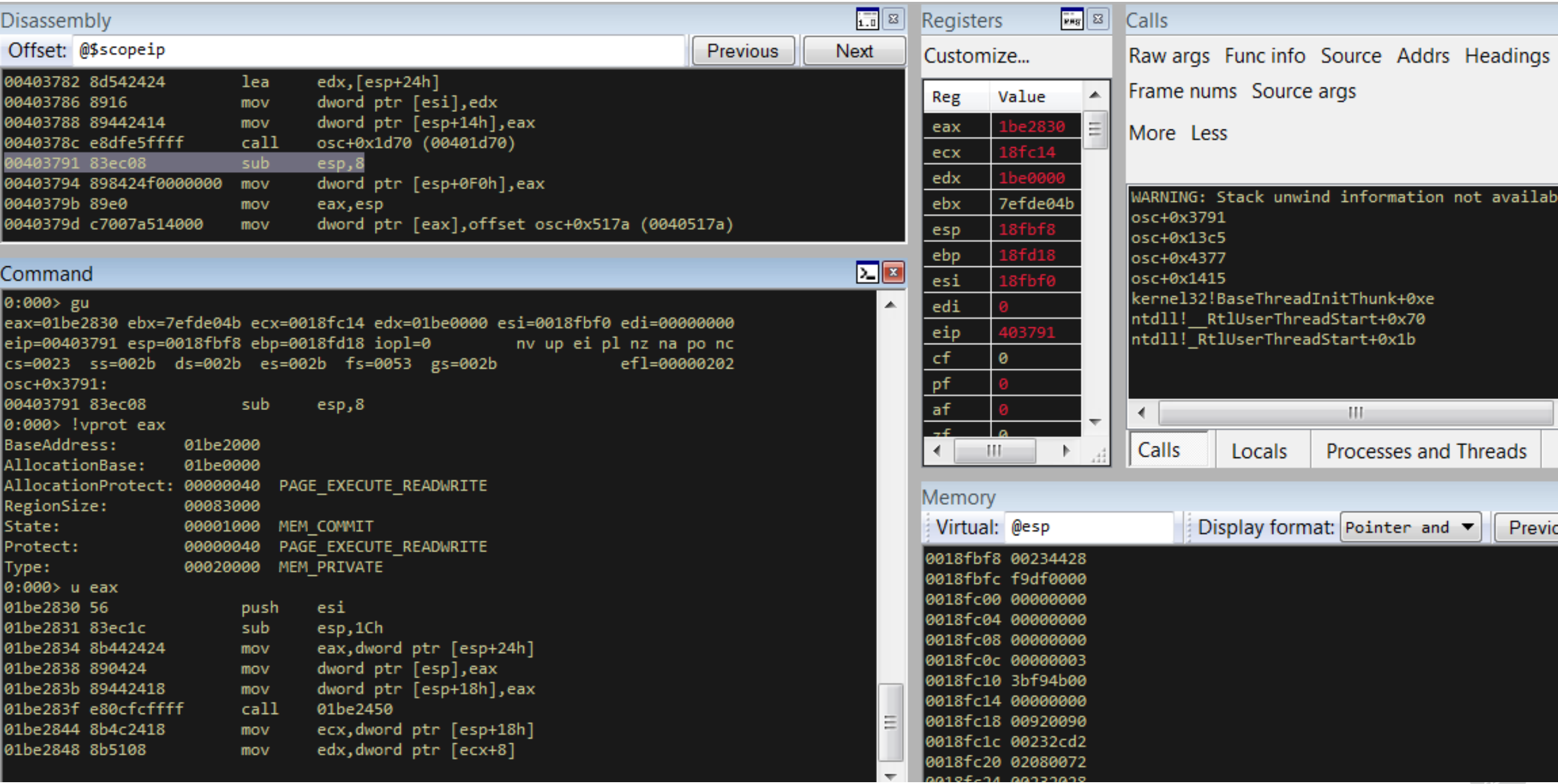
Prevents the debugger from debugging child processes.

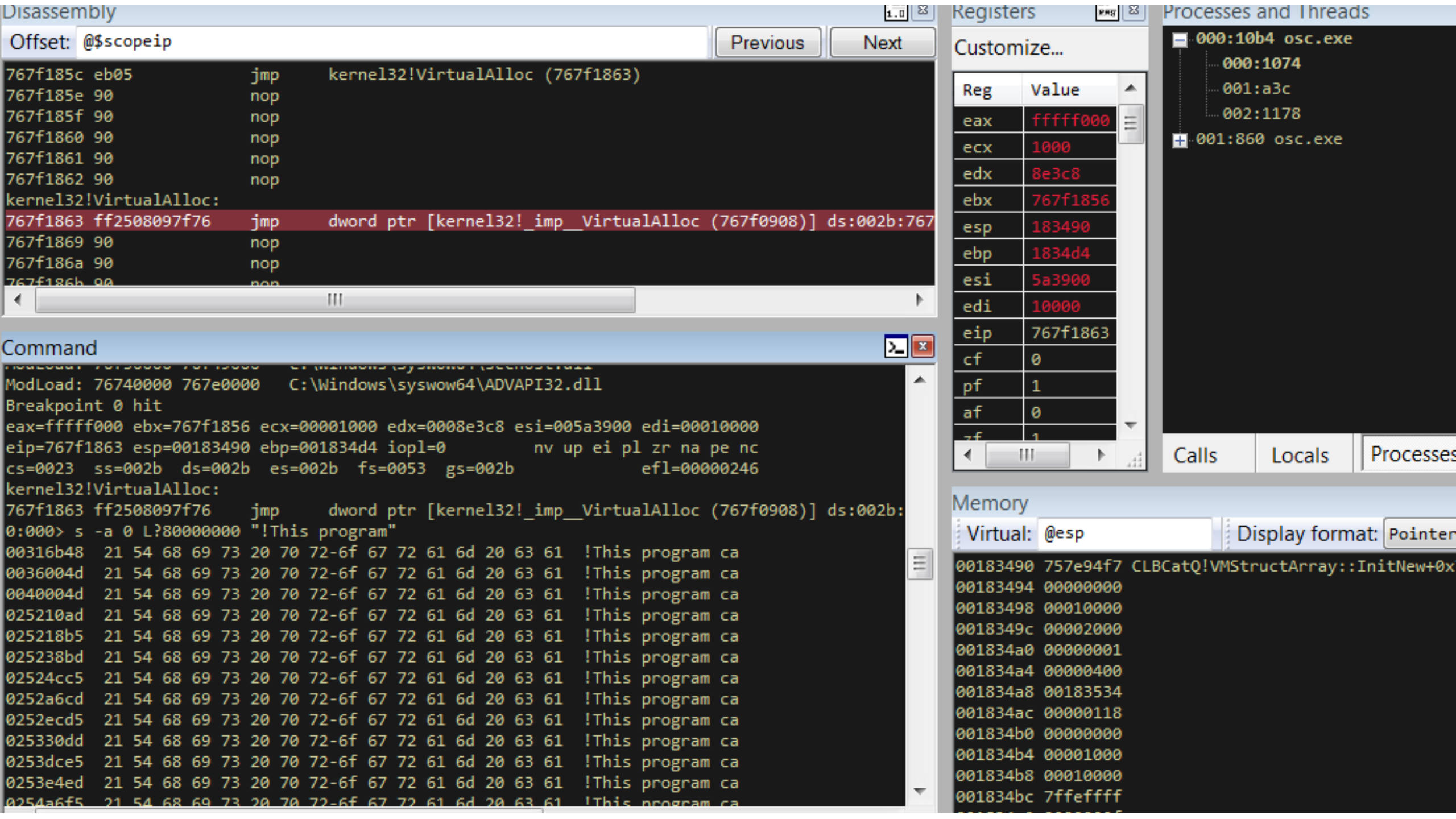
1

Causes the debugger to debug child processes.

Environment

This command is only supported in Windows XP and later versions of Windows.


Disassembly
Offset: @$scopeip
Previous
Next
00403782 8d542424 lea edx,[esp+24h]
00403786 8916 mov dword ptr [esi],edx
00403788 89442414 mov dword ptr [esp+14h],eax
0040378c e8dfe5ffff call osc+0x1d70 (00401d70)
00403791 83ec08 sub esp,8
00403794 898424f0000000 mov dword ptr [esp+0F0h],eax
0040379b 89e0 mov eax,esp
0040379d c7007a514000 mov dword ptr [eax],offset osc+0x517a (0040517a)
Command
0:000> gu
eax=01be2830 ebx=7efde04b ecx=0018fc14 edx=01be0000 esi=0018fbf0 edi=00000000
eip=00403791 esp=0018fbf8 ebp=0018fd18 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000202
osc+0x3791:
00403791 83ec08 sub esp,8
0:000> !vprot eax
BaseAddress: 01be2000
AllocationBase: 01be0000
AllocationProtect: 00000040 PAGE_EXECUTE_READWRITE
RegionSize: 00083000
State: 00001000 MEM_COMMIT
Protect: 00000040 PAGE_EXECUTE_READWRITE
Type: 00020000 MEM_PRIVATE
0:000> u eax
01be2830 56 push esi
01be2831 83ec1c sub esp,1Ch
01be2834 8b442424 mov eax,dword ptr [esp+24h]
01be2838 890424 mov dword ptr [esp],eax
01be283b 89442418 mov dword ptr [esp+18h],eax
01be283f e80cfcffff call 01be2450
01be2844 8b4c2418 mov ecx,dword ptr [esp+18h]
01be2848 8b5108 mov edx,dword ptr [ecx+8]
Registers
Customize...
Reg Value
eax 1be2830
ecx 18fc14
edx 1be0000
ebx 7efde04b
esp 18fbf8
ebp 18fd18
esi 18fbf0
edi 0
eip 403791
cf 0
pf 0
af 0
Calls
Raw args Func info Source Addrs Headings
Frame nums Source args
More Less
WARNING: Stack unwind information not availab
osc+0x3791
osc+0x13c5
osc+0x4377
osc+0x1415
kernel32!BaseThreadInitThunk+0xe
ntdll!__RtlUserThreadStart+0x70
ntdll!_RtlUserThreadStart+0x1b
Calls
Locals
Processes and Threads
Memory
Virtual: @esp
Display format: Pointer and
Previc
0018fbf8 00234428
0018fbfc f9df0000
0018fc00 00000000
0018fc04 00000000
0018fc08 00000000
0018fc0c 00000003
0018fc10 3bf94b00
0018fc14 00000000
0018fc18 00920090
0018fc1c 00232cd2
0018fc20 02080072


Disassembly
Offset: @$scopeip
Previous
Next
767f185c eb05 jmp kernel32!VirtualAlloc (767f1863)
767f185e 90 nop
767f185f 90 nop
767f1860 90 nop
767f1861 90 nop
767f1862 90 nop
kernel32!VirtualAlloc:
767f1863 ff2508097f76 jmp dword ptr [kernel32!_imp__VirtualAlloc (767f0908)] ds:002b:767
767f1869 90 nop
767f186a 90 nop
Registers
Customize...
Reg Value
eax ffff000
ecx 1000
edx 8e3c8
ebx 767f1856
esp 183490
ebp 1834d4
esi 5a3900
edi 10000
eip 767f1863
cf 0
pf 1
af 0
Processes and Threads
000:10b4 osc.exe
000:1074
001:a3c
002:1178
001:860 osc.exe
Calls
Locals
Processes
Command
ModLoad: 76740000 767e0000 C:\Windows\syswow64\ADVAPI32.dll
Breakpoint 0 hit
eax=ffff000 ebx=767f1856 ecx=00001000 edx=0008e3c8 esi=005a3900 edi=00010000
eip=767f1863 esp=00183490 ebp=001834d4 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000246
kernel32!VirtualAlloc:
767f1863 ff2508097f76 jmp dword ptr [kernel32!_imp__VirtualAlloc (767f0908)] ds:002b:
0:000> s -a 0 L?80000000 "!This program"
00316b48 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0036004d 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0040004d 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
025210ad 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
025218b5 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
025238bd 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
02524cc5 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0252a6cd 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0252ecd5 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
025330dd 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0253dce5 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
0253e4ed 21 54 68 69 73 20 70 72-6f 67 72 61 6d 20 63 61 !This program ca
Memory
Virtual: @esp
Display format: Pointer
00183490 757e94f7 CLBCatQ!VMStructArray::InitNew+0x
00183494 00000000
00183498 00010000
0018349c 00002000
001834a0 00000001
001834a4 00000400
001834a8 00183534
001834ac 00000118
001834b0 00000000
001834b4 00001000
001834b8 00010000
001834bc 7ffeffff

processhacker.sourceforge.net/downloads.php

Process Hacker

Overview | **Downloads** | FAQ | About | Forum

The latest stable version of Process Hacker is **2.38.343**.

Download

Installer

Binaries (portable)

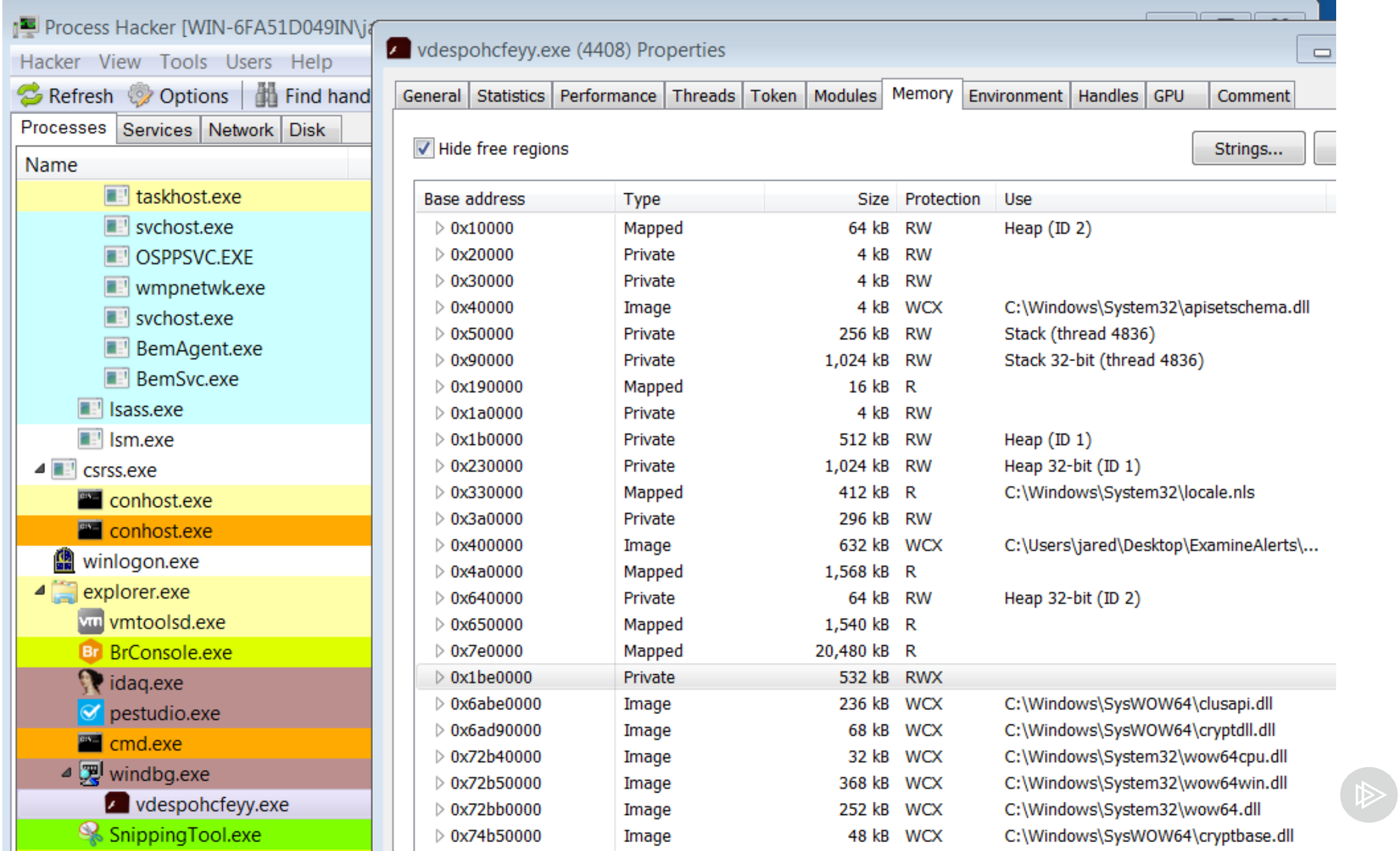
Source code

Mirror
See all downloads

System requirements:

- Windows XP (SP2)/Vista/7/8/10, 32-bit or 64-bit.
- Intel Itanium platforms are not supported.

If you like this software, please **Donate** to show your support!


Process Hacker [WIN-6FA51D049IN\ja
Hacker View Tools Users Help
Refresh Options Find hand
Processes Services Network Disk
Name
taskhost.exe
svchost.exe
OSPPSVC.EXE
wmpnetwk.exe
svchost.exe
BemAgent.exe
BemSvc.exe
lsass.exe
lsm.exe
csrss.exe
conhost.exe
conhost.exe
winlogon.exe
explorer.exe
vmtoolsd.exe
BrConsole.exe
idaq.exe
pestudio.exe
cmd.exe
windbg.exe
vdespohcfeyy.exe
SnippingTool.exe
vdespohcfeyy.exe (4408) Properties
General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment
Hide free regions
Strings...
Base address Type Size Protection Use
0x10000 Mapped 64 kB RW Heap (ID 2)
0x20000 Private 4 kB RW
0x30000 Private 4 kB RW
0x40000 Image 4 kB WCX C:\Windows\System32\apisetschema.dll
0x50000 Private 256 kB RW Stack (thread 4836)
0x90000 Private 1,024 kB RW Stack 32-bit (thread 4836)
0x190000 Mapped 16 kB R
0x1a0000 Private 4 kB RW
0x1b0000 Private 512 kB RW Heap (ID 1)
0x230000 Private 1,024 kB RW Heap 32-bit (ID 1)
0x330000 Mapped 412 kB R C:\Windows\System32\locale.nls
0x3a0000 Private 296 kB RW
0x400000 Image 632 kB WCX C:\Users\jared\Desktop\ExamineAlerts\...
0x4a0000 Mapped 1,568 kB R
0x640000 Private 64 kB RW Heap 32-bit (ID 2)
0x650000 Mapped 1,540 kB R
0x7e0000 Mapped 20,480 kB R
0x1be0000 Private 532 kB RWX
0x6abe0000 Image 236 kB WCX C:\Windows\SysWOW64\clusapi.dll
0x6ad90000 Image 68 kB WCX C:\Windows\SysWOW64\cryptdll.dll
0x72b40000 Image 32 kB WCX C:\Windows\System32\wow64cpu.dll
0x72b50000 Image 368 kB WCX C:\Windows\System32\wow64win.dll
0x72bb0000 Image 252 kB WCX C:\Windows\System32\wow64.dll
0x74b50000 Image 48 kB WCX C:\Windows\SysWOW64\cryptbase.dll

.writemem (Write Memory to File)

The **.writemem** command writes a section of memory to a file.

```
.writemem FileName Range
```

Parameters

FileName
: Specifies the name of the file to be created. You can specify a full path and file name, or just the file name. If the file name contains spaces, *FileName* should be enclosed in quotation marks. If no path is specified, the current directory is used.

Range
: Specifies the memory range to be written to the file. For syntax details, see Address and Address Range Syntax.

Environment

Summary

First look statically

Debugging Malware

Assignment