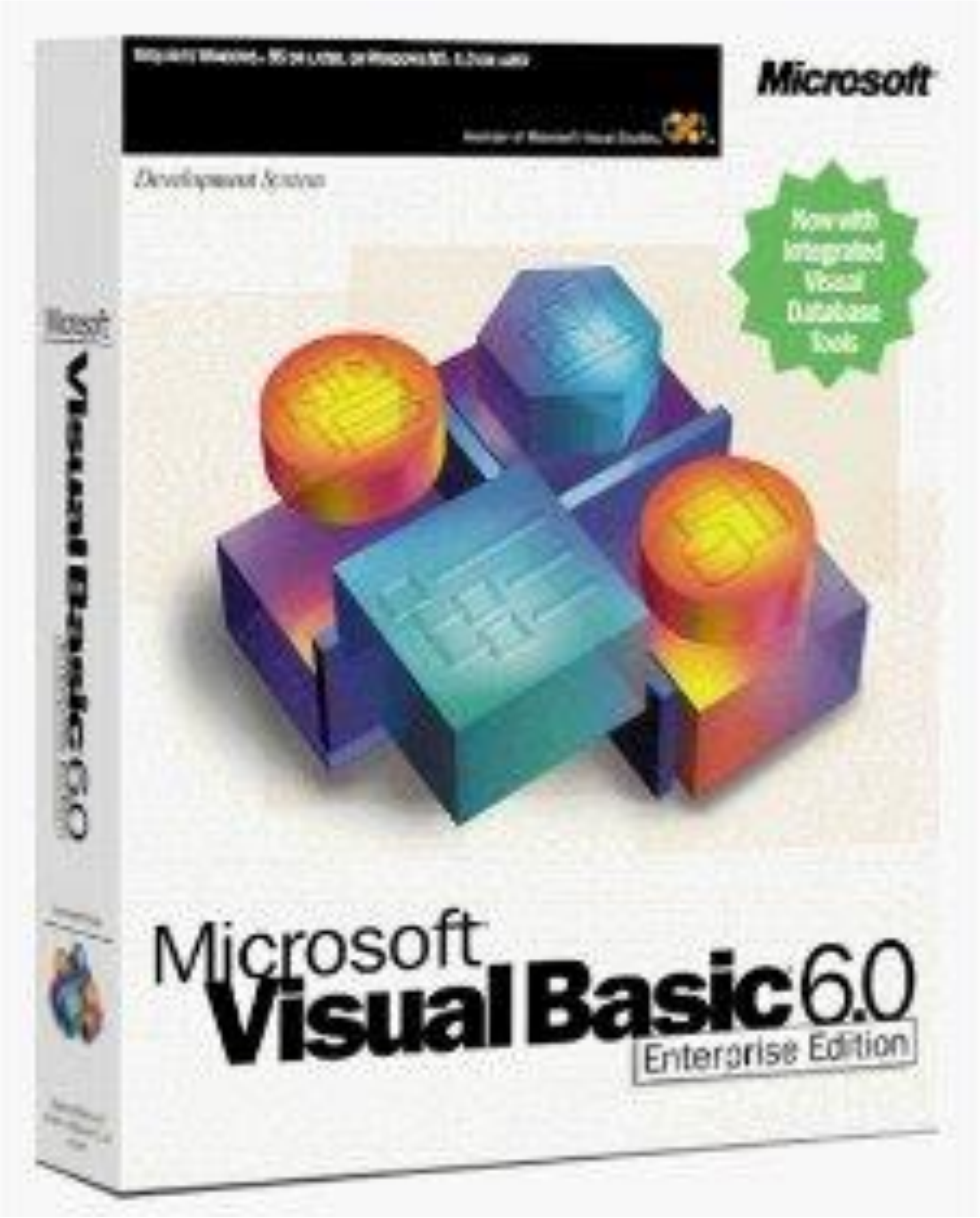
CURING A 15 YEAR OLD DISEASE

Jurriaan Bremer and Marion Marschalek

Area41 Defcon Switzerland - June 2014


Microsoft
Development System
Now with Integrated Visual Database Tools
Microsoft Visual Basic 6.0
Enterprise Edition

The Disease

Form1

Your Researchers Today

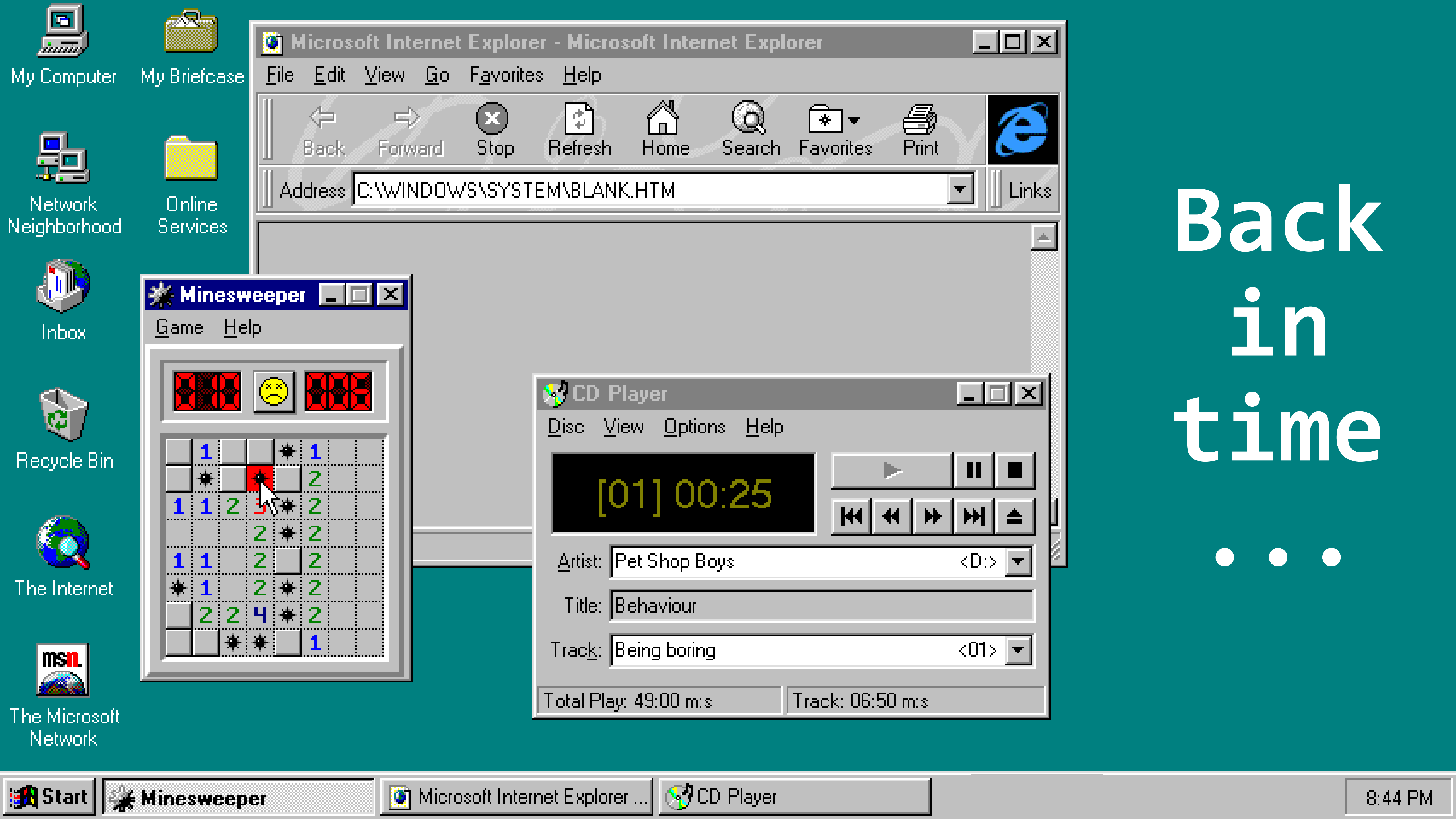
Jurriaan Bremer

Cuckoo Sandbox, Freelancer

Marion Marschalek

Cyphort Inc.

Back in time...



Address C:\WINDOWS\SYSTEM\BLANK.HTM

[01] 00:25

Artist: Pet Shop Boys <D:>

Title: Behaviour

Track: Being boring <01>

Total Play: 49:00 m:s

Track: 06:50 m:s

8:44 PM

Form1

Visual Basic 6.0

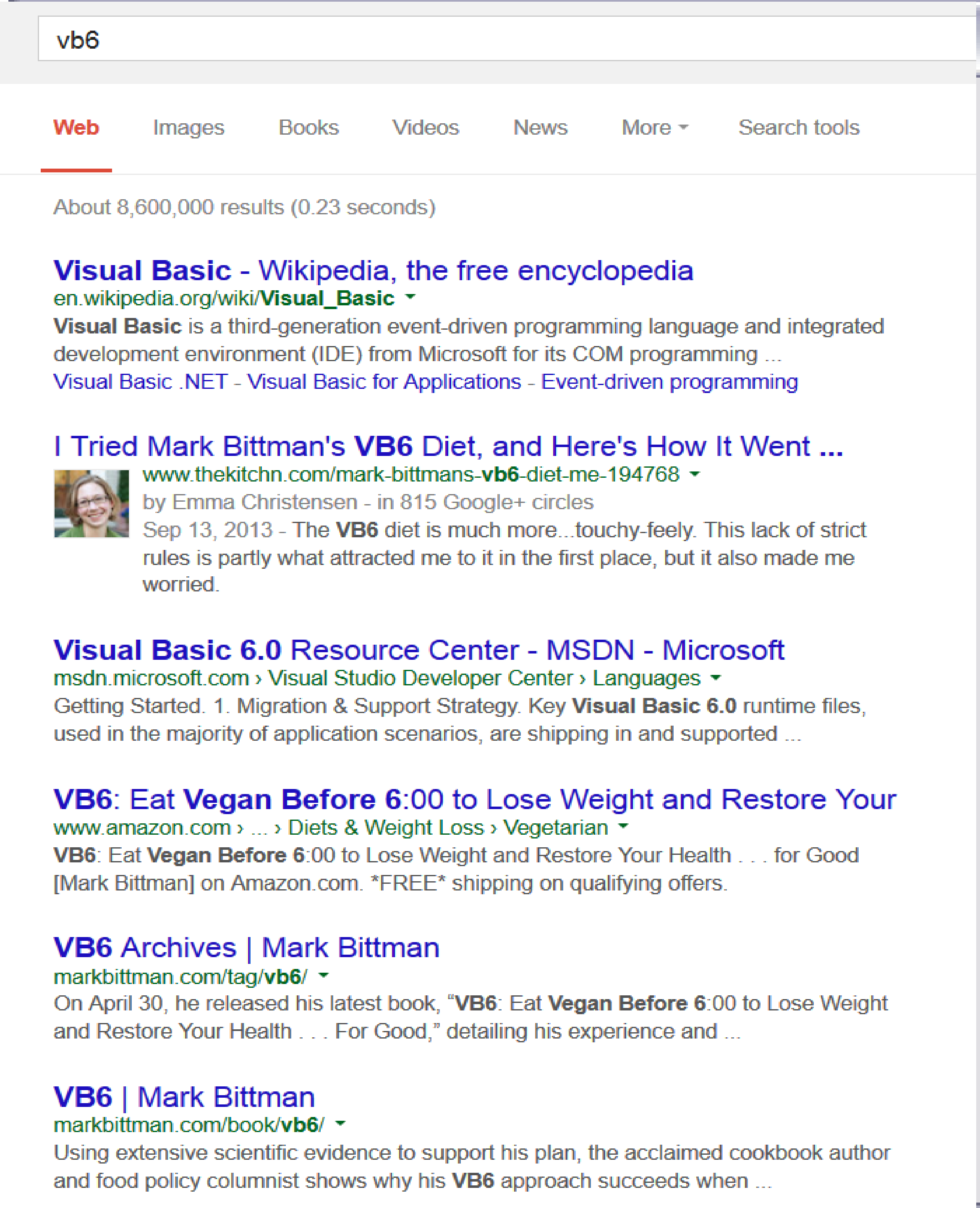
Microsoft, 1998

Object-based / event-driven

Rapid Application Development

Replaced by VB .NET in 2002

End of support in 2008



vb6

About 8,600,000 results (0.23 seconds)

Visual Basic - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/**Visual_Basic**
Visual Basic is a third-generation event-driven programming language and integrated development environment (IDE) from Microsoft for its COM programming ...
Visual Basic .NET - Visual Basic for Applications - Event-driven programming

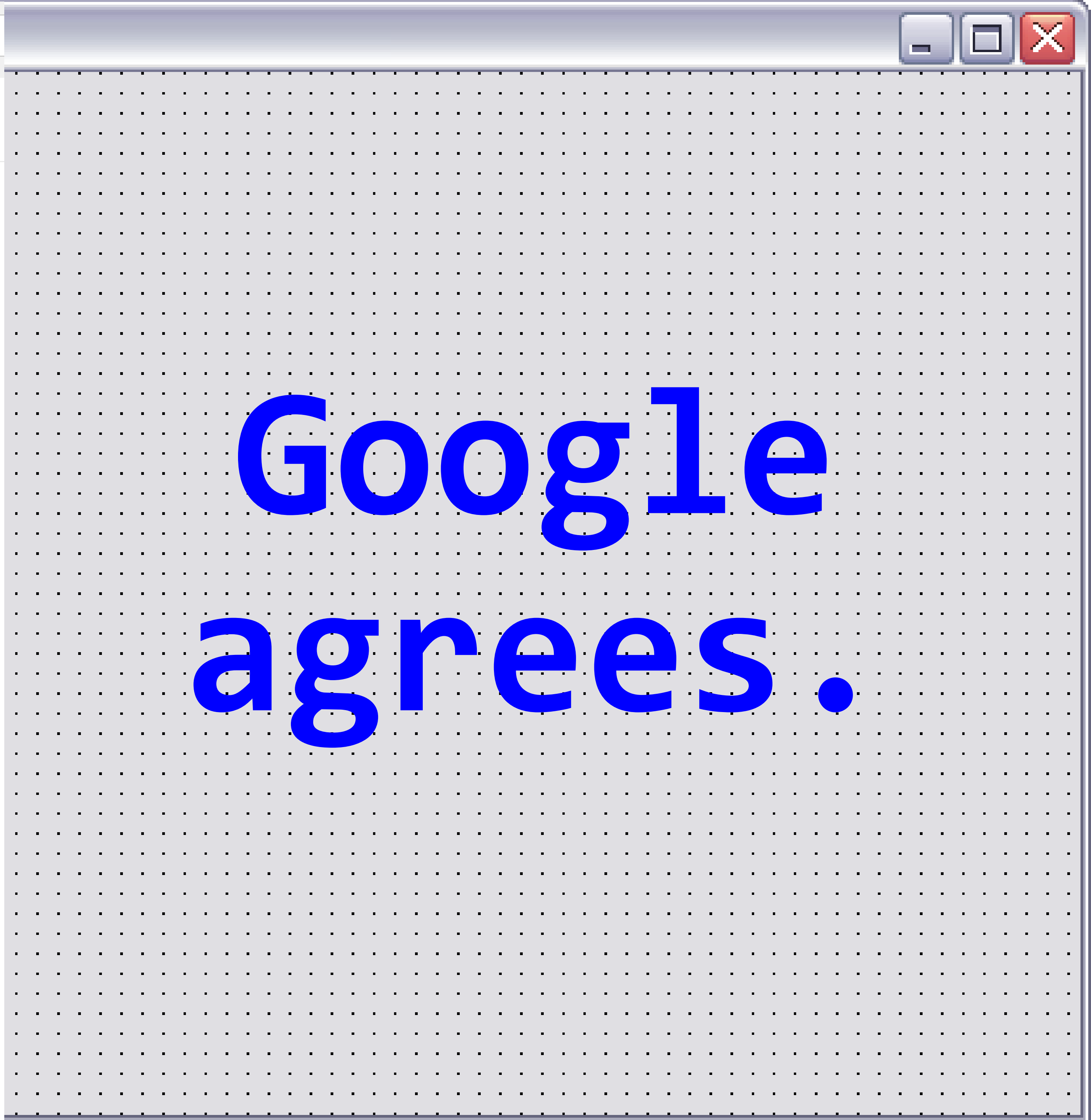
I Tried Mark Bittman's **VB6** Diet, and Here's How It Went ...
www.thekitchn.com/mark-bittmans-**vb6**-diet-me-194768
by Emma Christensen - in 815 Google+ circles
Sep 13, 2013 - The **VB6** diet is much more...touchy-feely. This lack of strict rules is partly what attracted me to it in the first place, but it also made me worried.

Visual Basic 6.0 Resource Center - MSDN - Microsoft
msdn.microsoft.com › Visual Studio Developer Center › Languages
Getting Started. 1. Migration & Support Strategy. Key **Visual Basic 6.0** runtime files, used in the majority of application scenarios, are shipping in and supported ...

VB6: Eat **Vegan Before 6**:00 to Lose Weight and Restore Your
www.amazon.com › ... › Diets & Weight Loss › Vegetarian
VB6: Eat **Vegan Before 6**:00 to Lose Weight and Restore Your Health . . . for Good [Mark Bittman] on Amazon.com. *FREE* shipping on qualifying offers.

VB6 Archives | Mark Bittman
markbittman.com/tag/**vb6**/
On April 30, he released his latest book, "**VB6**: Eat **Vegan Before 6**:00 to Lose Weight and Restore Your Health . . . For Good," detailing his experience and ...

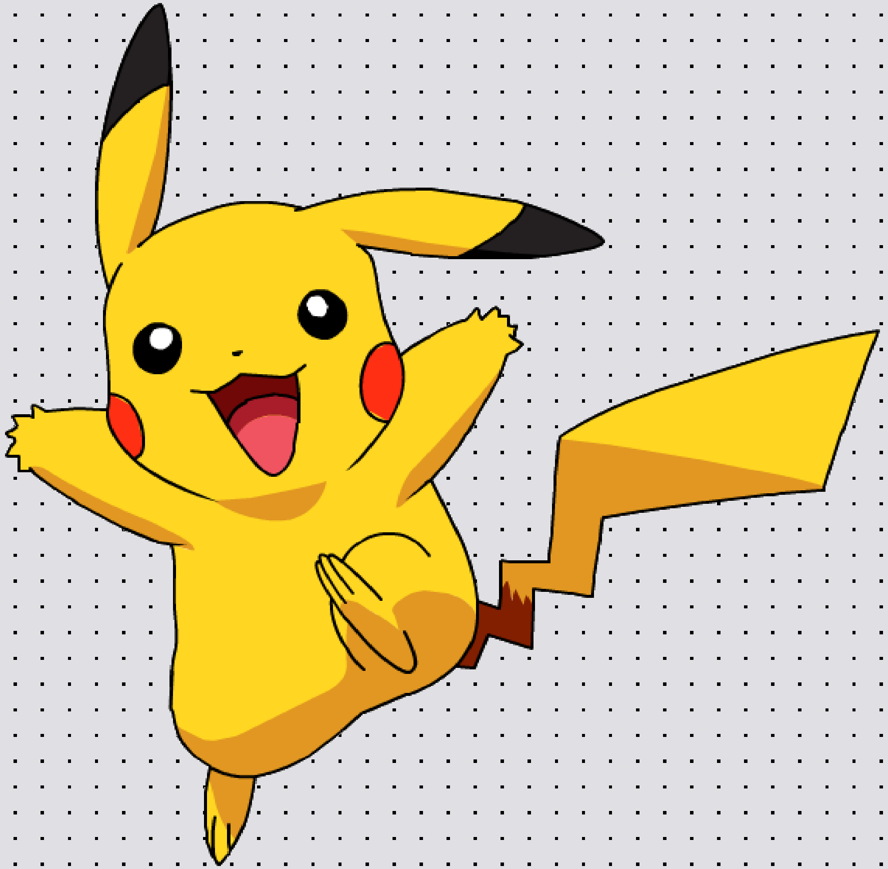
VB6 | Mark Bittman
markbittman.com/book/**vb6**/
Using extensive scientific evidence to support his plan, the acclaimed cookbook author and food policy columnist shows why his **VB6** approach succeeds when ...



Google agrees.

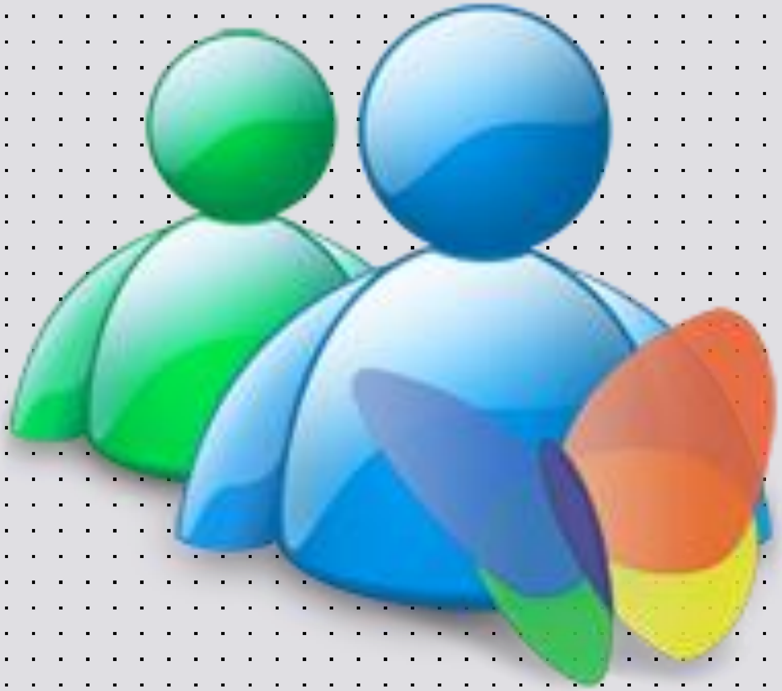
2000: Pikachu Worm

- pikachupokemon.exe – „Pikachu is your friend!“
- Modifies AUTOEXEC.BAT to remove C:\WINDOWS and C:\WINDOBadWS\system32
- Bad coding…



2005: Kelvir Worm

- Spreads through MSN Messenger by *„lol! see it! u'll like it”* message
- Message points to omg.pif on home.earthlink.net
- Spreads further & downloads and executes other malware



Form1

2009: Changeup Worm

- Polymorphic
- Spreads through removable media and shared folders by 'LNK/PIF' Files Automatic File Execution Vulnerability
- Downloads other malware

So... why are we here?

VB6 IS NOT DEAD

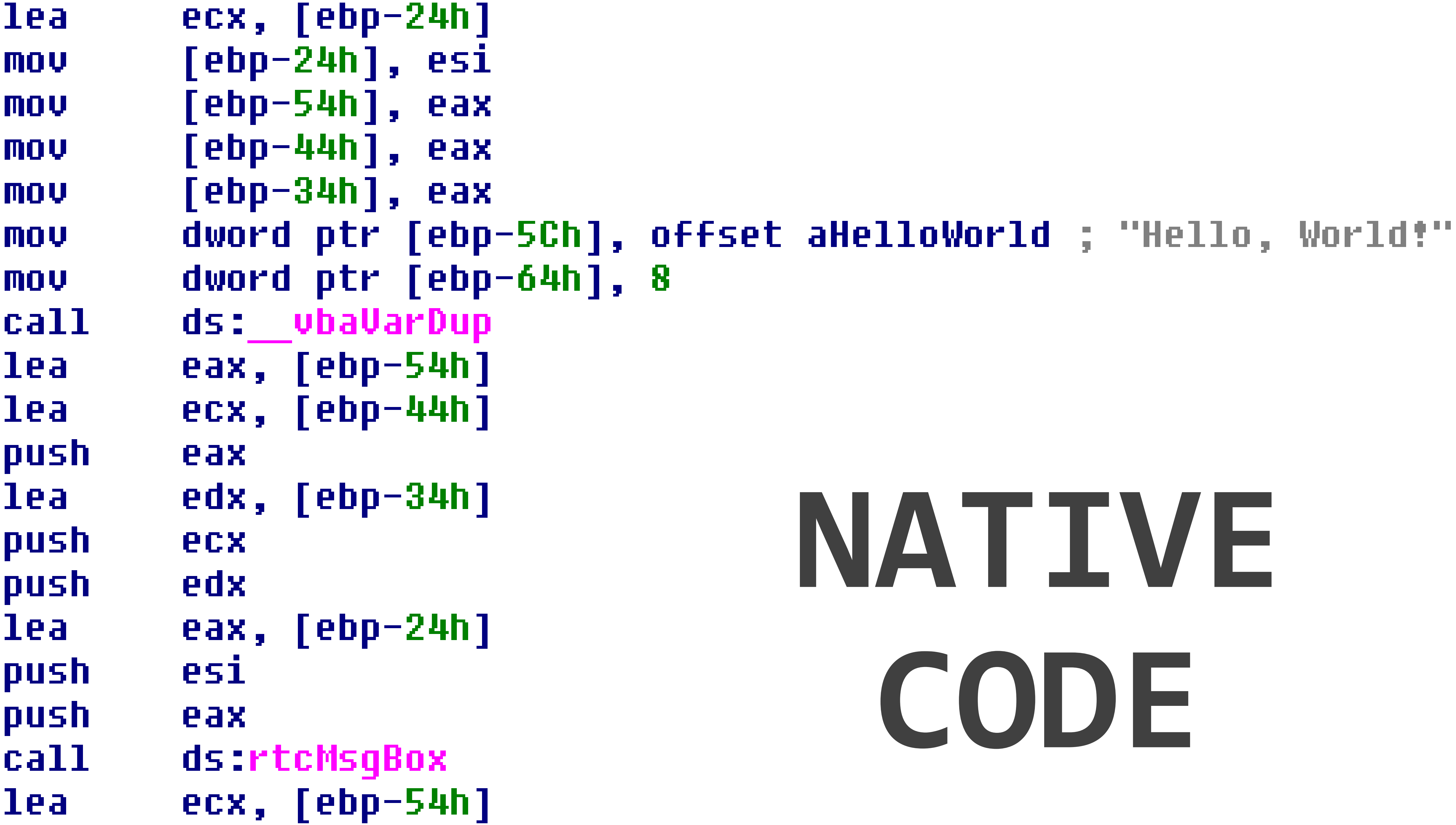
Form1

VB6 101

1991: Visual Basic born

1998: Visual Basic 5.0/6.0 p-code and native code

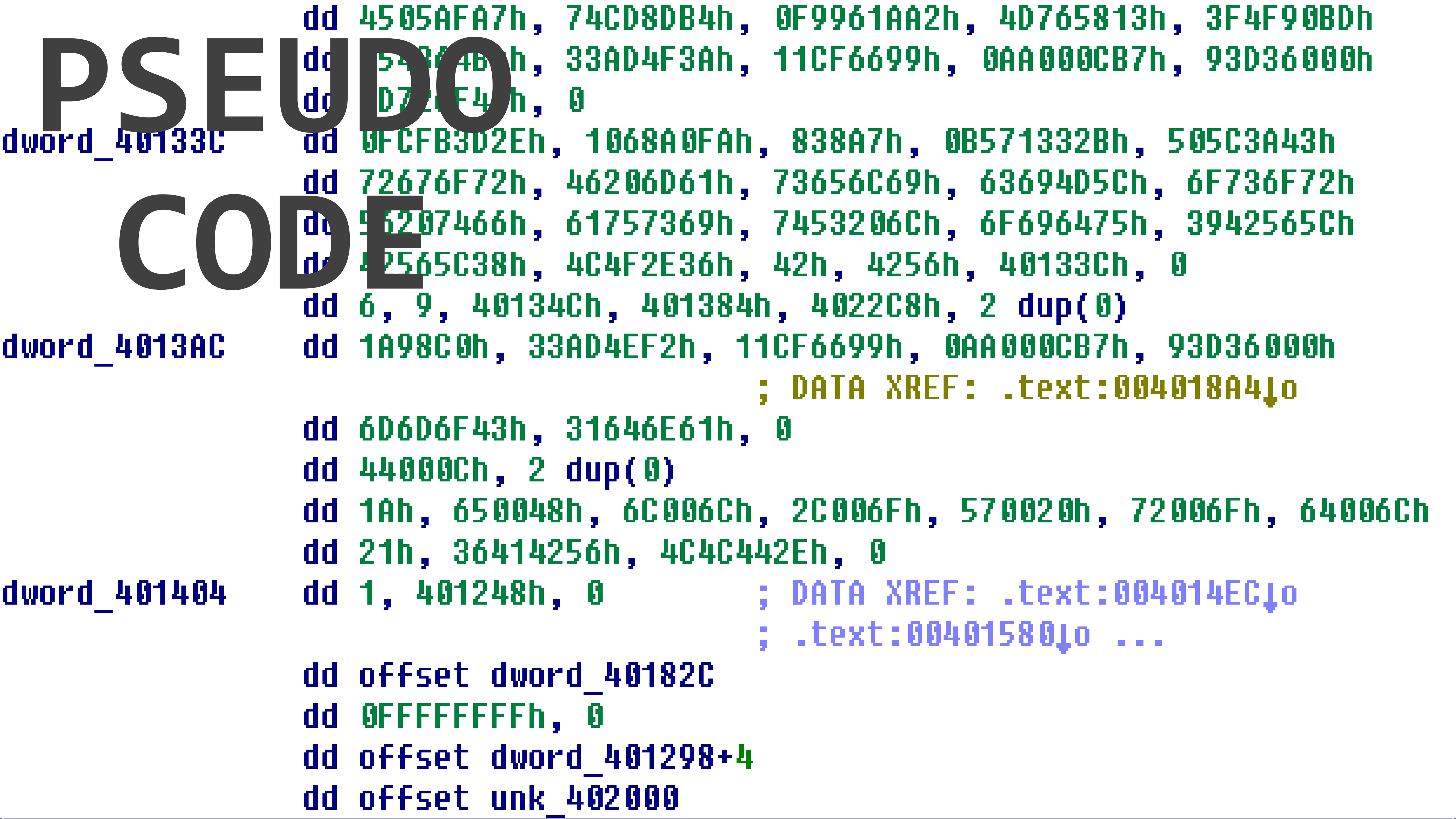
2002: VB.NET and MSIL byte code



```
lea     ecx, [ebp-24h]
mov     [ebp-24h], esi
mov     [ebp-54h], eax
mov     [ebp-44h], eax
mov     [ebp-34h], eax
mov     dword ptr [ebp-5Ch], offset aHelloWorld ; "Hello, World!"
mov     dword ptr [ebp-64h], 8
call    ds:__vbaVarDup
lea     eax, [ebp-54h]
lea     ecx, [ebp-44h]
push    eax
lea     edx, [ebp-34h]
push    ecx
push    edx
lea     eax, [ebp-24h]
push    esi
push    eax
call    ds:rtcMsgBox
lea     ecx, [ebp-54h]
```

NATIVE CODE

PSEUDO CODE



```
                dd 4505AFA7h, 74CD8DB4h, 0F9961AA2h, 4D765813h, 3F4F90BDh
                dd 54[illegible]h, 33AD4F3Ah, 11CF6699h, 0AA000CB7h, 93D36000h
                dd [illegible]D7[illegible]F4[illegible]h, 0
dword_40133C    dd 0FCFB3D2Eh, 1068A0FAh, 838A7h, 0B571332Bh, 505C3A43h
                dd 72676F72h, 46206D61h, 73656C69h, 63694D5Ch, 6F736F72h
                dd 56207466h, 61757369h, 7453206Ch, 6F696475h, 3942565Ch
                dd 42565C38h, 4C4F2E36h, 42h, 4256h, 40133Ch, 0
                dd 6, 9, 40134Ch, 401384h, 4022C8h, 2 dup(0)
dword_4013AC    dd 1A98C0h, 33AD4EF2h, 11CF6699h, 0AA000CB7h, 93D36000h
                                                ; DATA XREF: .text:004018A4↓o
                dd 6D6D6F43h, 31646E61h, 0
                dd 44000Ch, 2 dup(0)
                dd 1Ah, 650048h, 6C006Ch, 2C006Fh, 570020h, 72006Fh, 64006Ch
                dd 21h, 36414256h, 4C4C442Eh, 0
dword_401404    dd 1, 401248h, 0                ; DATA XREF: .text:004014EC↓o
                                                ; .text:00401580↓o ...
                dd offset dword_40182C
                dd 0FFFFFFFFh, 0
                dd offset dword_401298+4
                dd offset unk_402000
```

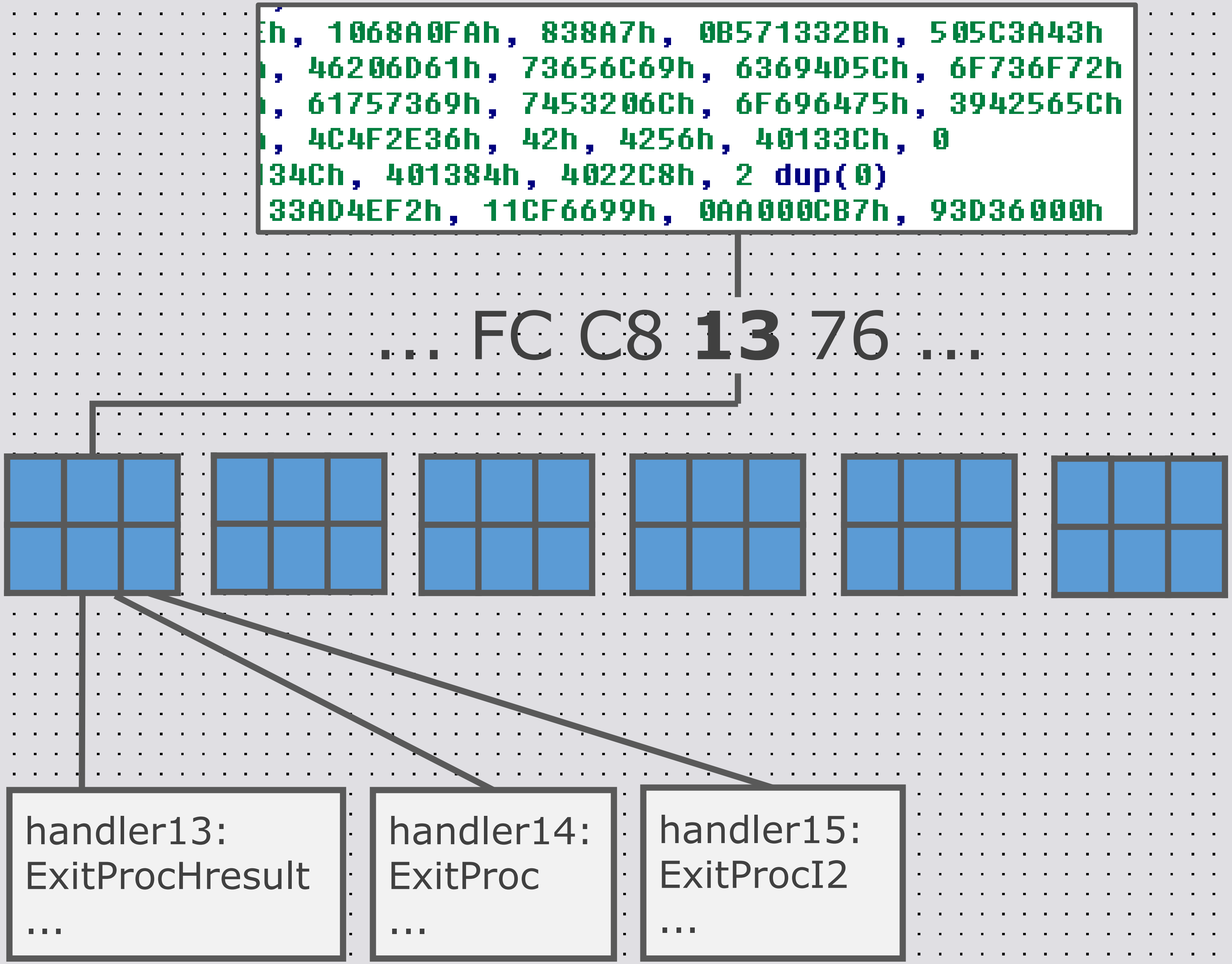
Form1

P-Code Translation

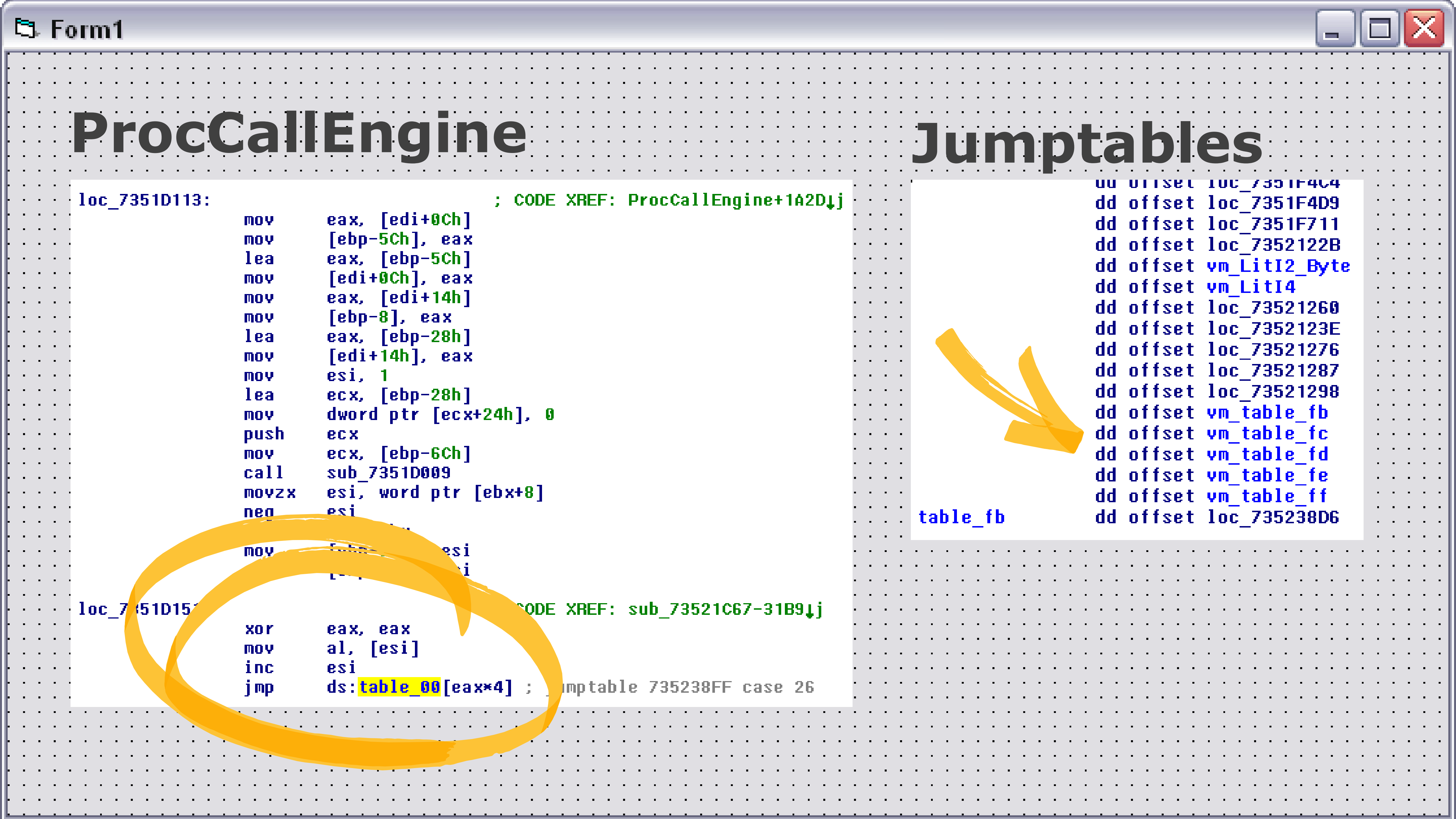
P-code mnemonics

interpreted

by msvbvm60.dll



```
h, 1068A0FAh, 838A7h, 0B571332Bh, 505C3A43h
h, 46206D61h, 73656C69h, 63694D5Ch, 6F736F72h
h, 61757369h, 7453206Ch, 6F696475h, 3942565Ch
h, 4C4F2E36h, 42h, 4256h, 40133Ch, 0
34Ch, 401384h, 4022C8h, 2 dup(0)
33AD4EF2h, 11CF6699h, 0AA000CB7h, 93D36000h
```



ProcCallEngine

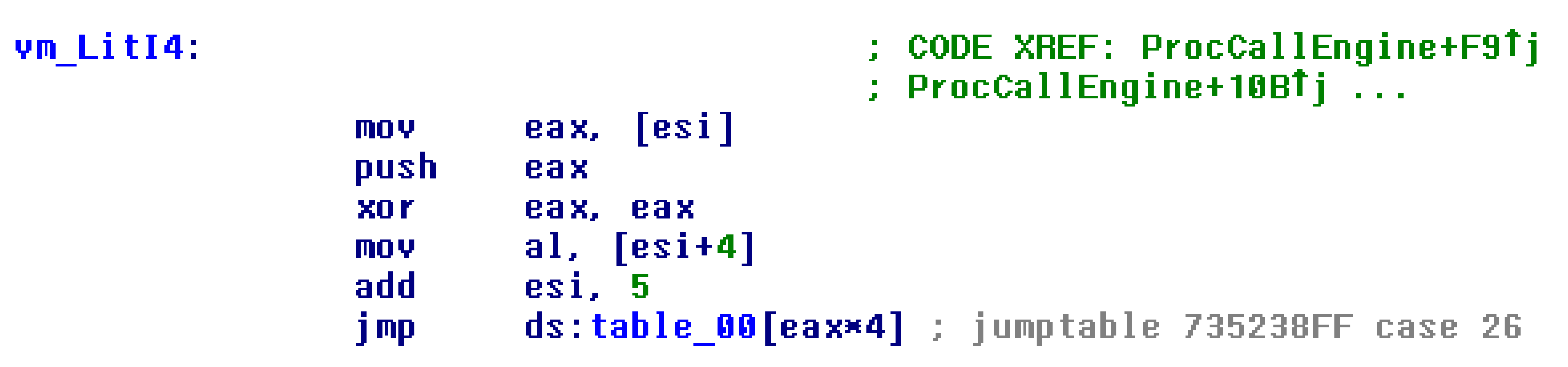
```
loc_7351D113:                           ; CODE XREF: ProcCallEngine+1A2D↓j
                mov     eax, [edi+0Ch]
                mov     [ebp-5Ch], eax
                lea     eax, [ebp-5Ch]
                mov     [edi+0Ch], eax
                mov     eax, [edi+14h]
                mov     [ebp-8], eax
                lea     eax, [ebp-28h]
                mov     [edi+14h], eax
                mov     esi, 1
                lea     ecx, [ebp-28h]
                mov     dword ptr [ecx+24h], 0
                push    ecx
                mov     ecx, [ebp-6Ch]
                call    sub_7351D009
                movzx   esi, word ptr [ebx+8]
                neg     esi
                [illegible]
                mov     [illegible] esi
                        [illegible]i

loc_7[illegible]51D15[illegible]                  ; CODE XREF: sub_73521C67-31B9↓j
                xor     eax, eax
                mov     al, [esi]
                inc     esi
                jmp     ds:table_00[eax*4] ; [illegible]mptable 735238FF case 26
```

Jumptables

```
                dd offset loc_7351F4C4
                dd offset loc_7351F4D9
                dd offset loc_7351F711
                dd offset loc_7352122B
                dd offset vm_LitI2_Byte
                dd offset vm_LitI4
                dd offset loc_73521260
                dd offset loc_7352123E
                dd offset loc_73521276
                dd offset loc_73521287
                dd offset loc_73521298
                dd offset vm_table_fb
                dd offset vm_table_fc
                dd offset vm_table_fd
                dd offset vm_table_fe
                dd offset vm_table_ff
table_fb        dd offset loc_735238D6
```

Instruction Handler

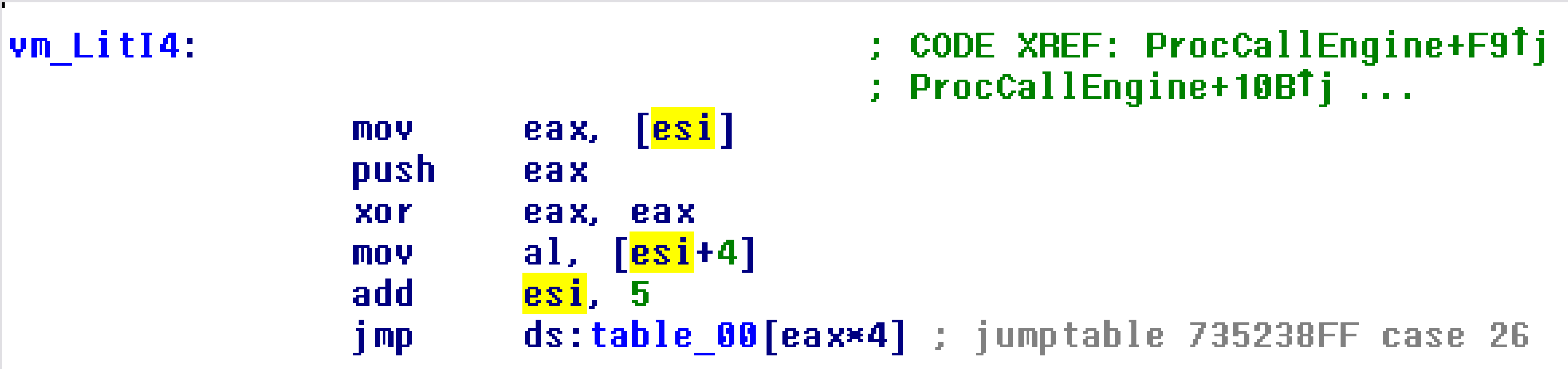


```
vm_LitI4:                                 ; CODE XREF: ProcCallEngine+F9↑j
                                          ; ProcCallEngine+10B↑j ...
                mov     eax, [esi]
                push    eax
                xor     eax, eax
                mov     al, [esi+4]
                add     esi, 5
                jmp     ds:table_00[eax*4] ; jumptable 735238FF case 26
```

pushes integer onto the stack

Form1

Instruction Handler

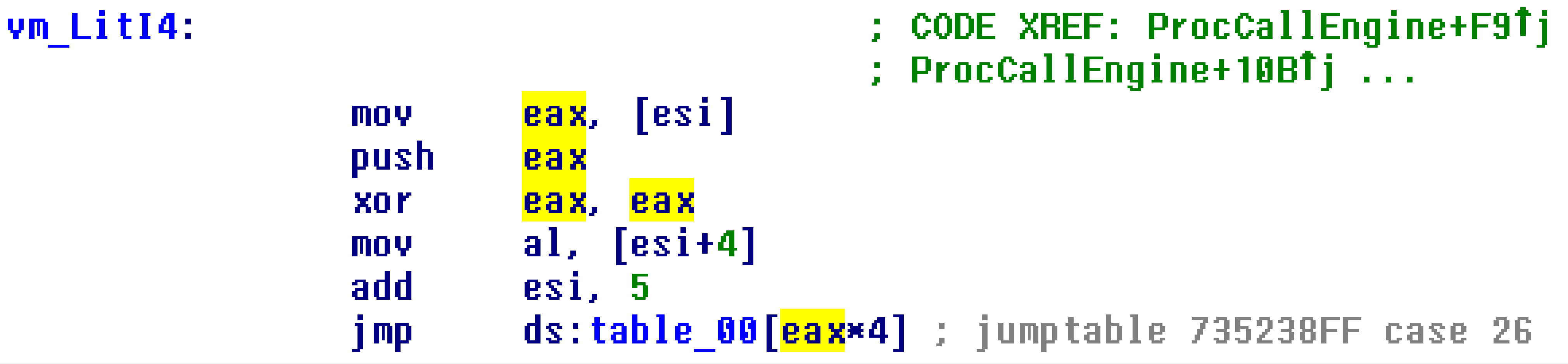


```
vm_LitI4:                                    ; CODE XREF: ProcCallEngine+F9↑j
                                             ; ProcCallEngine+10B↑j ...
                mov     eax, [esi]
                push    eax
                xor     eax, eax
                mov     al, [esi+4]
                add     esi, 5
                jmp     ds:table_00[eax*4] ; jumptable 735238FF case 26
```

pushes integer onto the stack

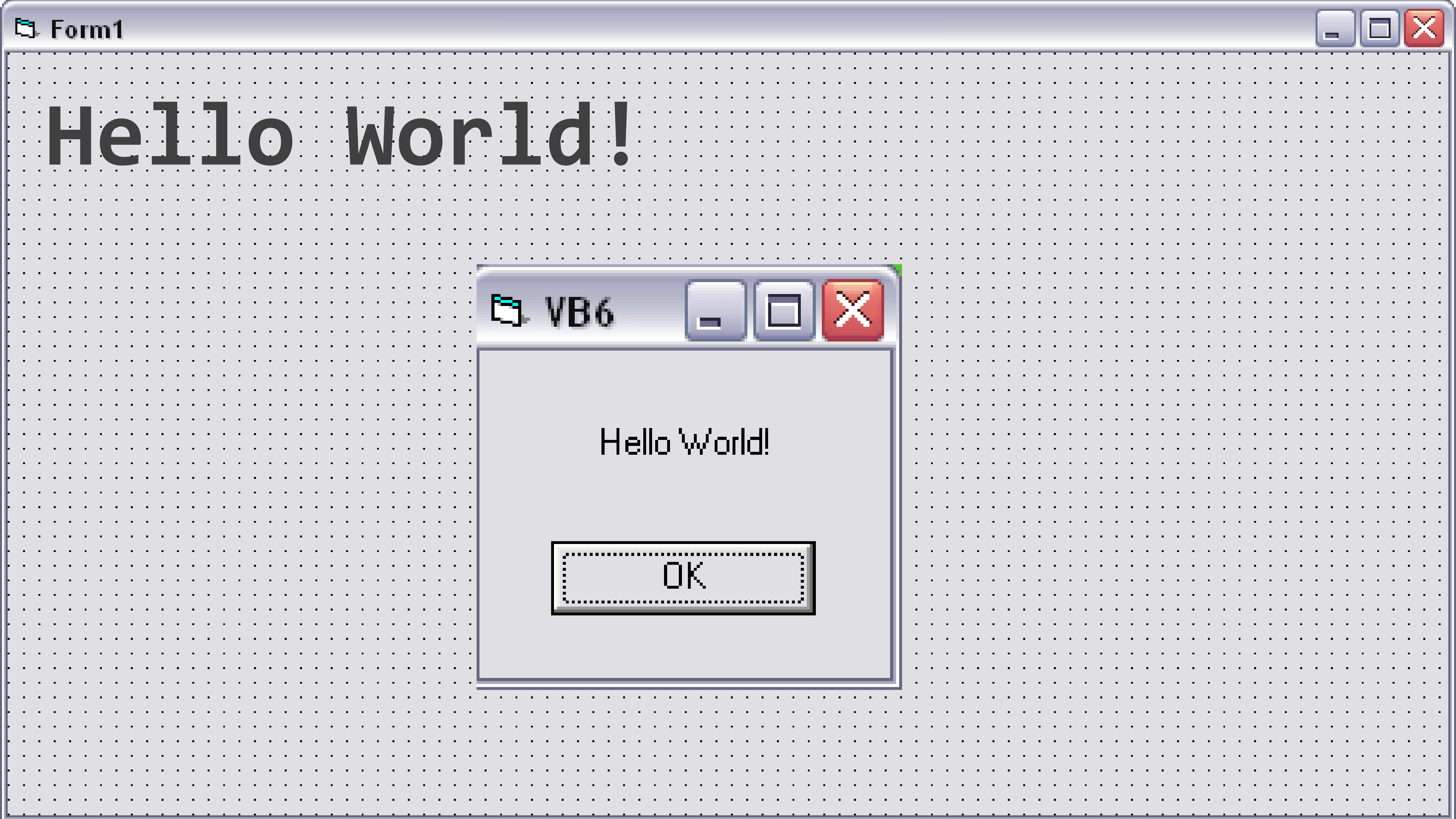
Form1

Instruction Handler



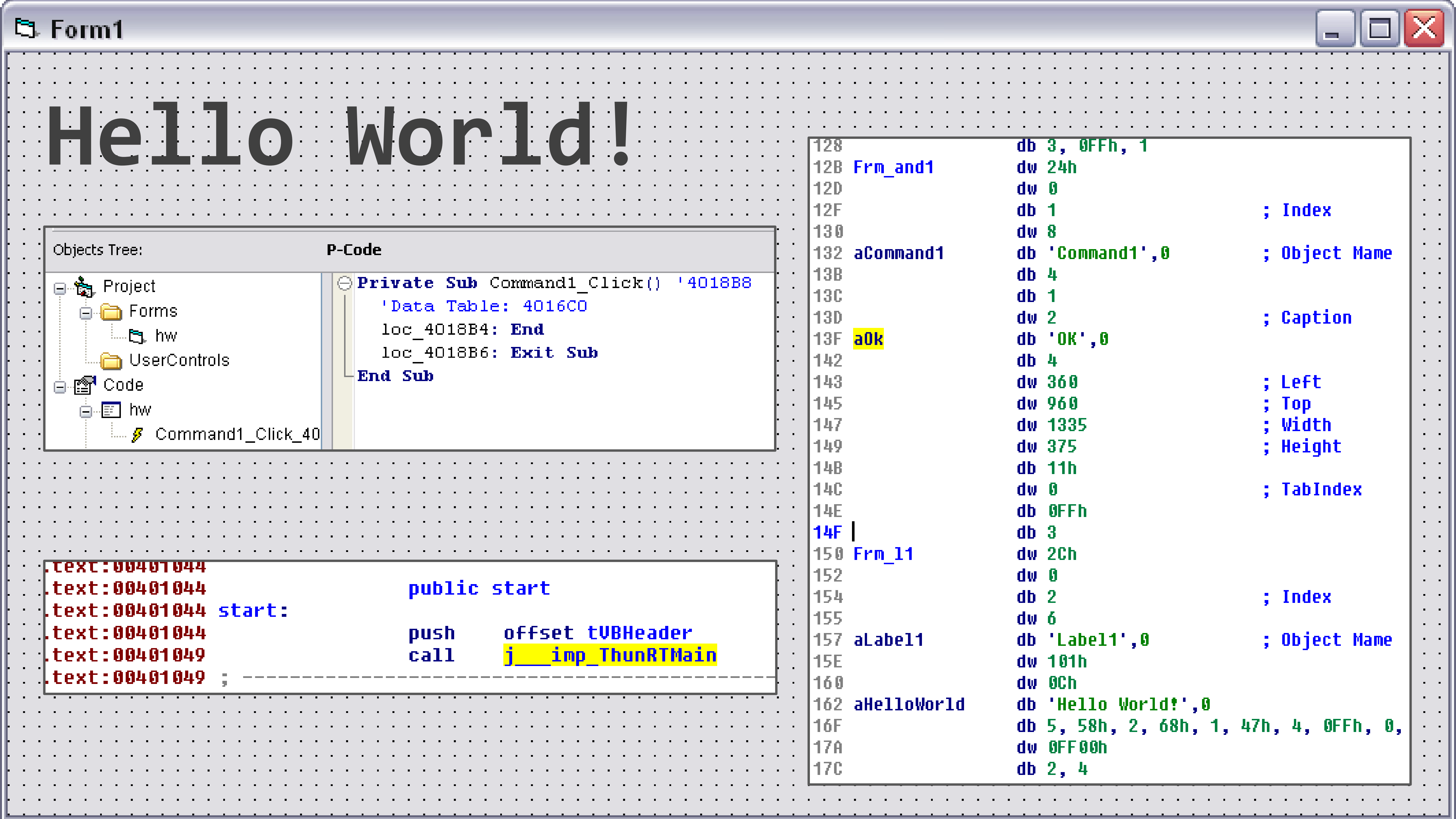
```
vm_LitI4:                                        ; CODE XREF: ProcCallEngine+F9↑j
                                                 ; ProcCallEngine+10B↑j ...
                mov     eax, [esi]
                push    eax
                xor     eax, eax
                mov     al, [esi+4]
                add     esi, 5
                jmp     ds:table_00[eax*4] ; jumptable 735238FF case 26
```

pushes integer onto the stack



Hello World!

Hello World!



Form1

Hello World!

Objects Tree:

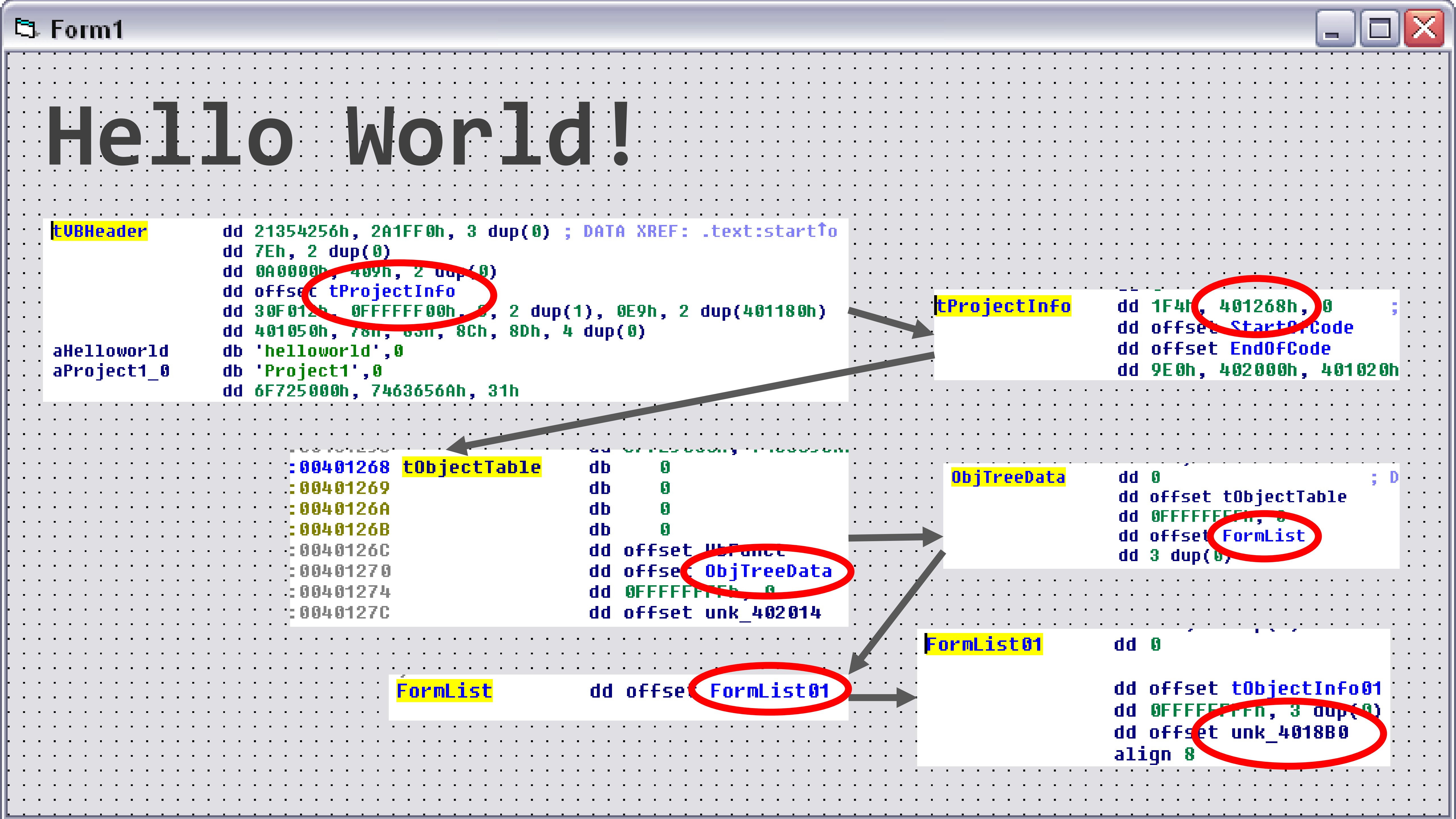
- Project
  - Forms
    - hw
  - UserControls
- Code
  - hw
    - Command1_Click_40

P-Code

```
Private Sub Command1_Click() '4018B8
  'Data Table: 4016C0
  loc_4018B4: End
  loc_4018B6: Exit Sub
End Sub
```

```
.text:00401044
.text:00401044                 public start
.text:00401044 start:
.text:00401044                 push    offset tVBHeader
.text:00401049                 call    j___imp_ThunRTMain
.text:00401049 ; ---------------------------------------------------
```

```
128                  db 3, 0FFh, 1
12B Frm_and1         dw 24h
12D                  dw 0
12F                  db 1                   ; Index
130                  dw 8
132 aCommand1        db 'Command1',0        ; Object Name
13B                  db 4
13C                  db 1
13D                  dw 2                   ; Caption
13F aOk              db 'OK',0
142                  db 4
143                  dw 360                 ; Left
145                  dw 960                 ; Top
147                  dw 1335                ; Width
149                  dw 375                 ; Height
14B                  db 11h
14C                  dw 0                   ; TabIndex
14E                  db 0FFh
14F                  db 3
150 Frm_l1           dw 2Ch
152                  dw 0
154                  db 2                   ; Index
155                  dw 6
157 aLabel1          db 'Label1',0          ; Object Name
15E                  dw 101h
160                  dw 0Ch
162 aHelloWorld      db 'Hello World!',0
16F                  db 5, 58h, 2, 68h, 1, 47h, 4, 0FFh, 0,
17A                  dw 0FF00h
17C                  db 2, 4
```



```
tVBHeader           dd 21354256h, 2A1FF0h, 3 dup(0) ; DATA XREF: .text:start↑o
                    dd 7Eh, 2 dup(0)
                    dd 0A0000h, 409h, 2 dup(0)
                    dd offset tProjectInfo
                    dd 30F012h, 0FFFFFF00h, 0, 2 dup(1), 0E9h, 2 dup(401180h)
                    dd 401050h, 78h, 83h, 8Ch, 8Dh, 4 dup(0)
aHelloworld         db 'helloworld',0
aProject1_0         db 'Project1',0
                    dd 6F725000h, 7463656Ah, 31h
```

```
tProjectInfo        dd 1F4h, 401268h, 0        ;
                    dd offset StartOfCode
                    dd offset EndOfCode
                    dd 9E0h, 402000h, 401020h
```

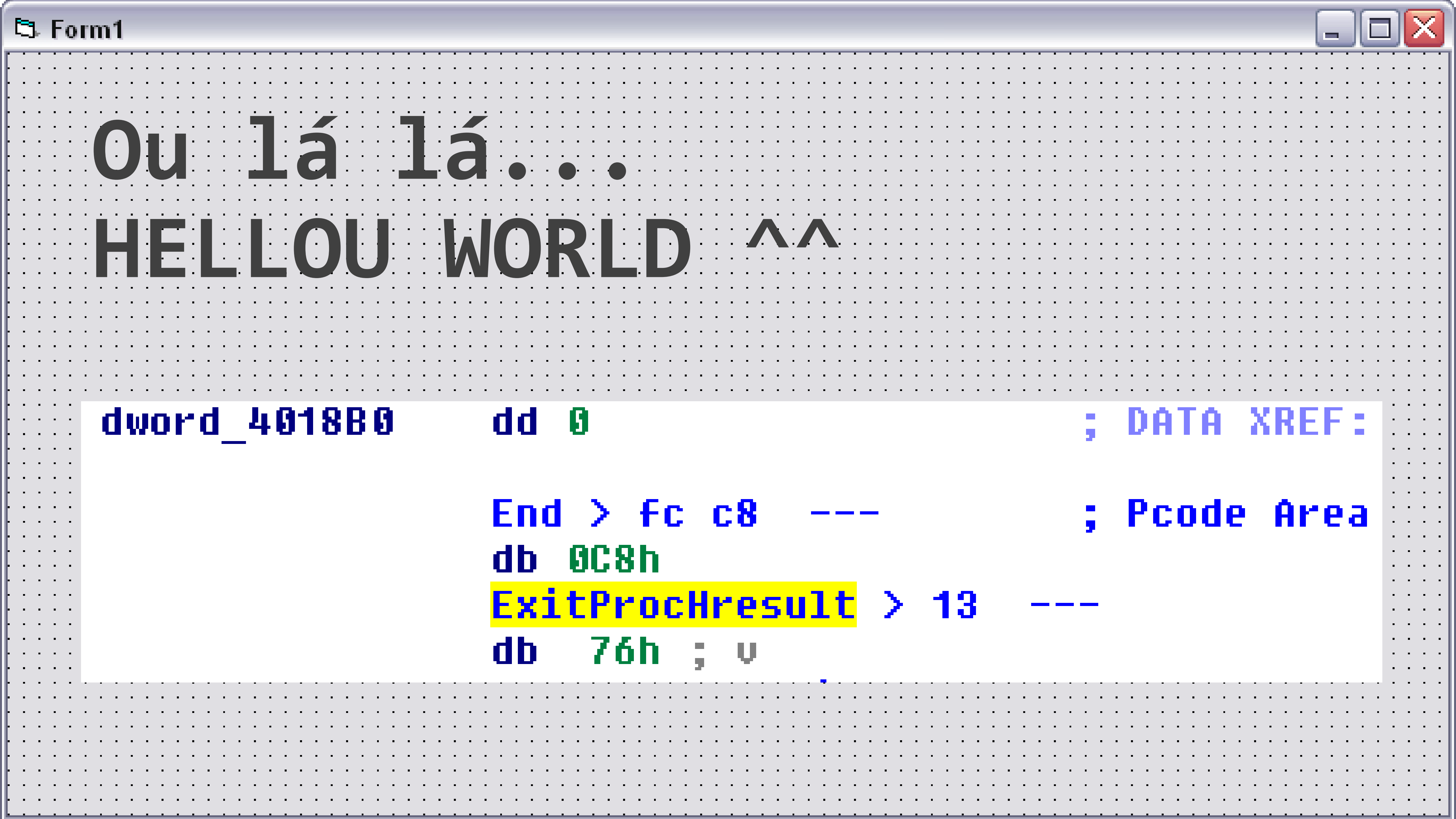
```
:00401268 tObjectTable        db    0
:00401269                     db    0
:0040126A                     db    0
:0040126B                     db    0
:0040126C                     dd offset VbFunct
:00401270                     dd offset ObjTreeData
:00401274                     dd 0FFFFFFFFh, 0
:0040127C                     dd offset unk_402014
```

```
ObjTreeData         dd 0                       ; D
                    dd offset tObjectTable
                    dd 0FFFFFFFFh, 0
                    dd offset FormList
                    dd 3 dup(0)
```

```
FormList            dd offset FormList01
```

```
FormList01          dd 0

                    dd offset tObjectInfo01
                    dd 0FFFFFFFFh, 3 dup(0)
                    dd offset unk_4018B0
                    align 8
```

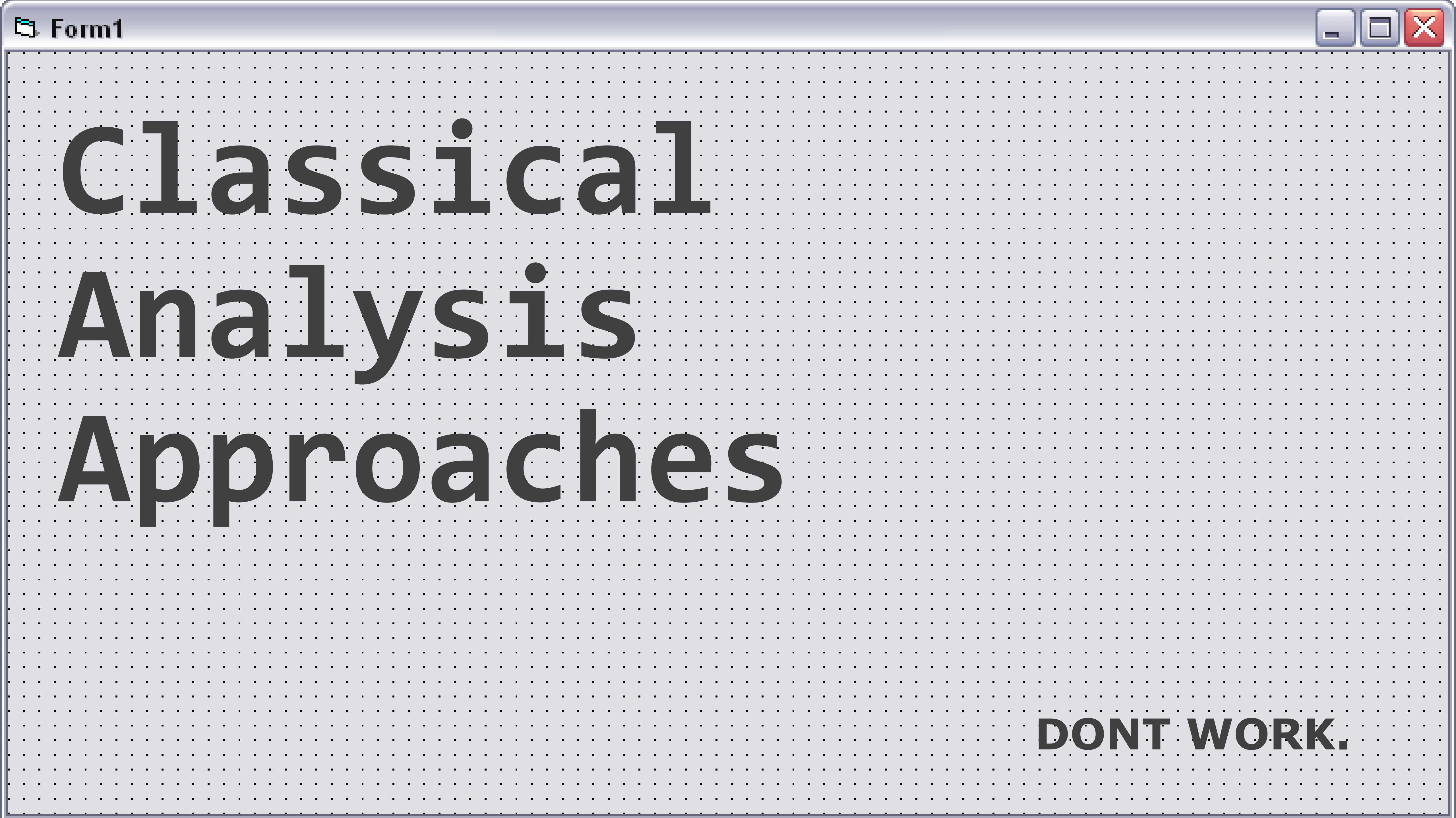


Ou lá lá...

HELLOU WORLD ^^

```
dword_4018B0    dd 0                                 ; DATA XREF:

                End > fc c8  ---                     ; Pcode Area
                db 0C8h
                ExitProcHresult > 13  ---
                db  76h ; v
```



Classical Analysis Approaches

DONT WORK.

Form1

Existing VB Stuff

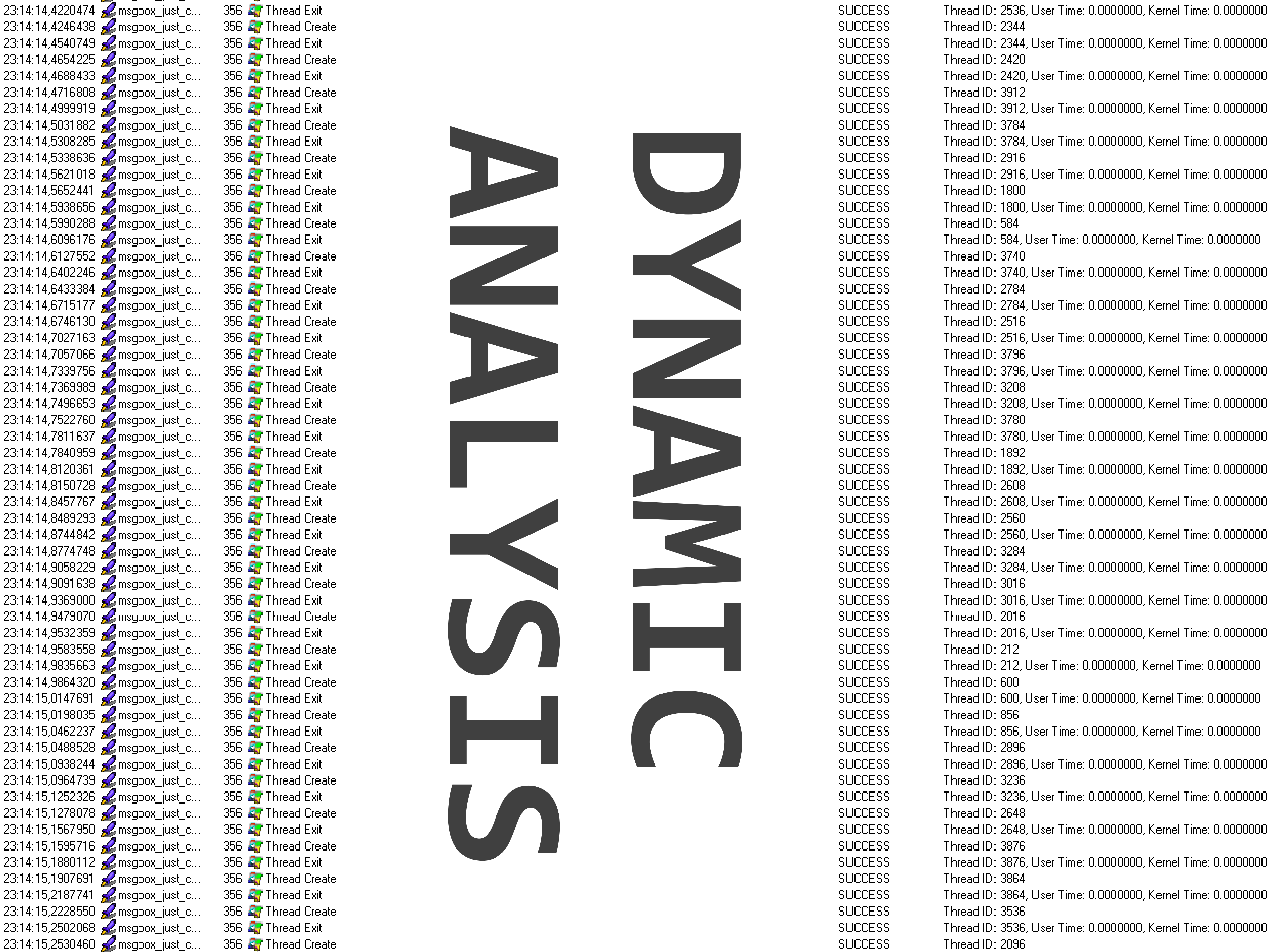
- VB Decompiler
- Tequila Debugger
- IDA Scripts
- Peter Ferrie, Masaki Suenaga

Most Advanced Sophisticated Private Cloud-based Big Data Intelligence Cyber Solution! (tm)

MASPCbBDICS FAIL COMPILATION

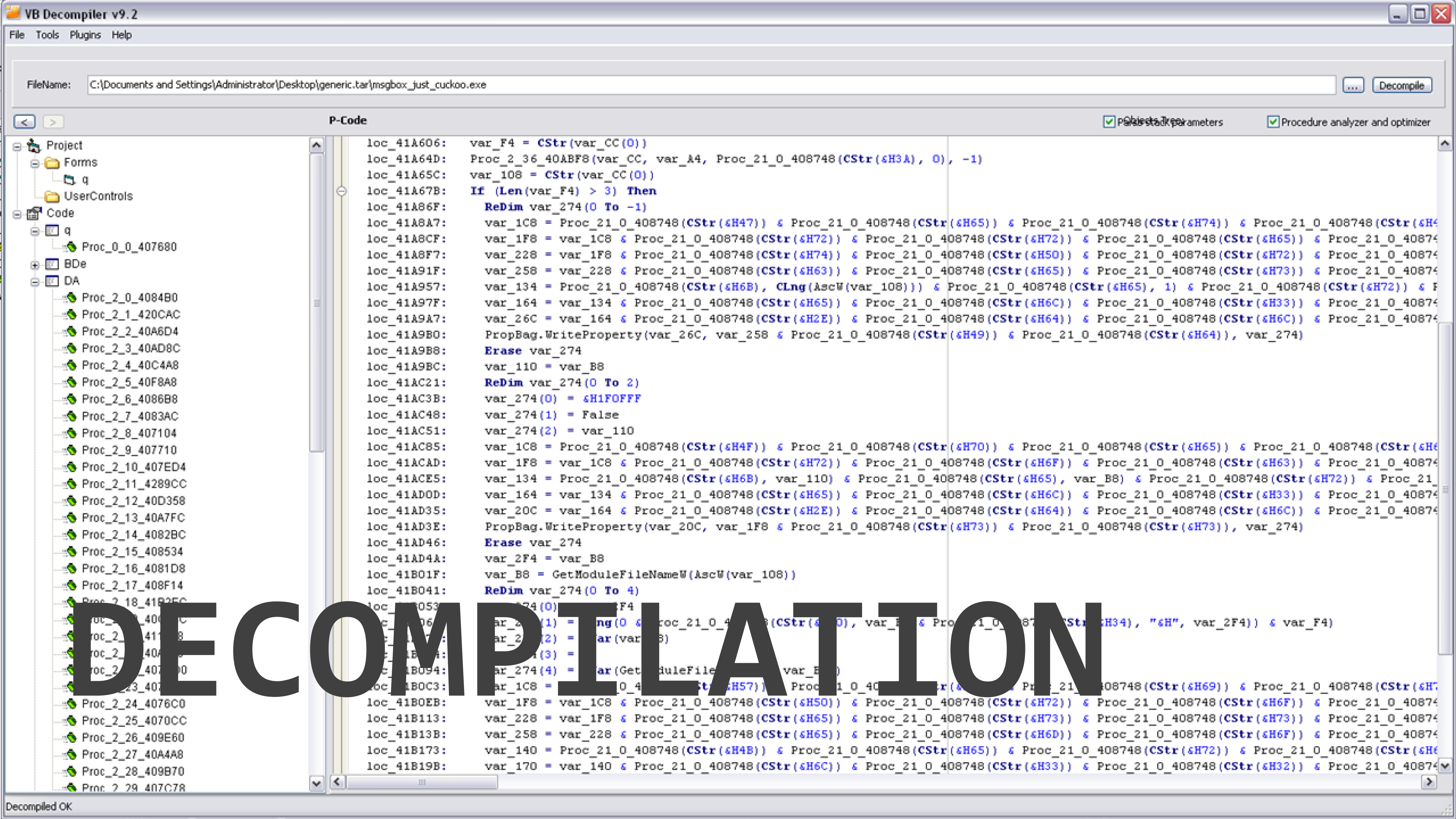
Everything that didnt work...

DYNAMIC ANALYSIS



```
23:14:14,4220474  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2536, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4246438  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2344
23:14:14,4540749  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2344, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4654225  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2420
23:14:14,4688433  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2420, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4716808  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3912
23:14:14,4999919  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3912, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5031882  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3784
23:14:14,5308285  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3784, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5338636  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2916
23:14:14,5621018  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2916, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5652441  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 1800
23:14:14,5938656  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 1800, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5990288  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 584
23:14:14,6096176  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 584, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6127552  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3740
23:14:14,6402246  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3740, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6433384  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2784
23:14:14,6715177  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2784, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6746130  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2516
23:14:14,7027163  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2516, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7057066  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3796
23:14:14,7339756  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3796, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7369989  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3208
23:14:14,7496653  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3208, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7522760  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3780
23:14:14,7811637  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3780, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7840959  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 1892
23:14:14,8120361  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 1892, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8150728  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2608
23:14:14,8457767  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2608, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8489293  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2560
23:14:14,8744842  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2560, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8774748  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3284
23:14:14,9058229  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3284, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9091638  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3016
23:14:14,9369000  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3016, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9479070  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2016
23:14:14,9532359  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2016, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9583558  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 212
23:14:14,9835663  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 212, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9864320  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 600
23:14:15,0147691  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 600, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0198035  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 856
23:14:15,0462237  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 856, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0488528  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2896
23:14:15,0938244  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2896, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0964739  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3236
23:14:15,1252326  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3236, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1278078  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2648
23:14:15,1567950  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 2648, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1595716  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3876
23:14:15,1880112  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3876, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1907691  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3864
23:14:15,2187741  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3864, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,2228550  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 3536
23:14:15,2502068  msgbox_just_c...  356  Thread Exit    SUCCESS  Thread ID: 3536, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,2530460  msgbox_just_c...  356  Thread Create  SUCCESS  Thread ID: 2096
```

DECOMPILATION

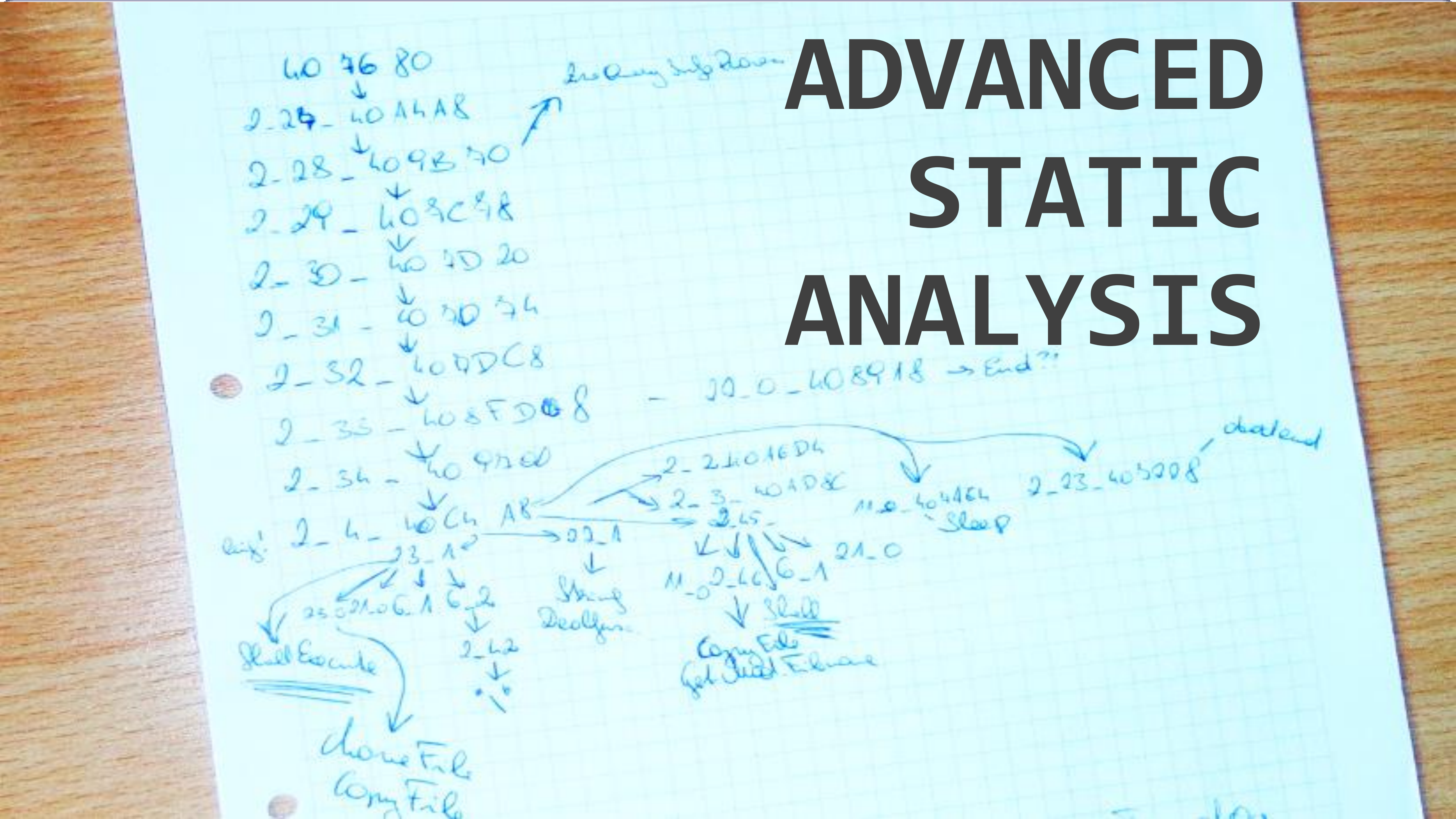


FileName: C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe

☑ Parse stack parameters ☑ Procedure analyzer and optimizer

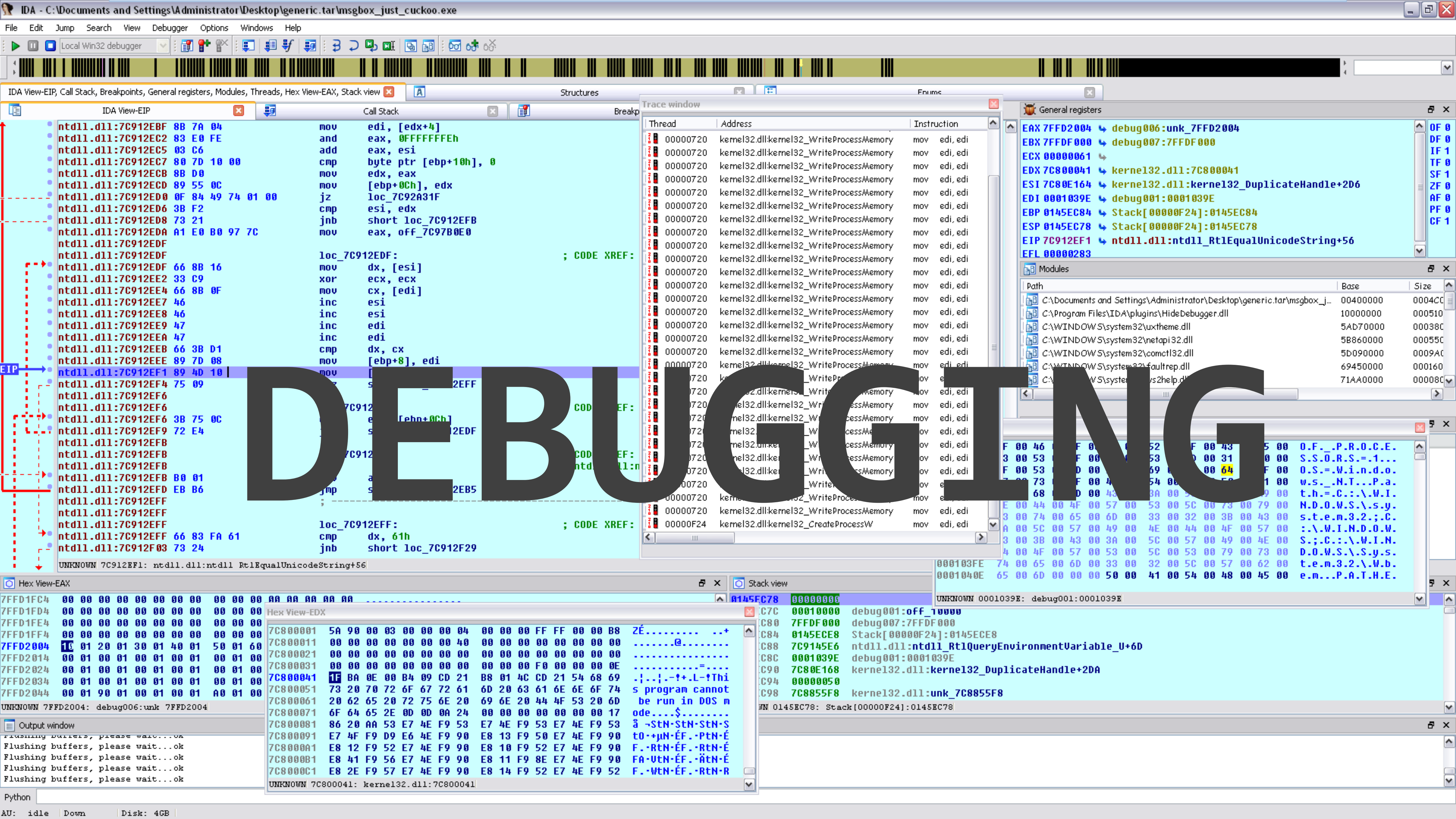
```
Project
  Forms
    q
  UserControls
Code
  q
    Proc_0_0_407680
  BDe
  DA
    Proc_2_0_4084B0
    Proc_2_1_420CAC
    Proc_2_2_40A6D4
    Proc_2_3_40AD8C
    Proc_2_4_40C4A8
    Proc_2_5_40F8A8
    Proc_2_6_4086B8
    Proc_2_7_4083AC
    Proc_2_8_407104
    Proc_2_9_407710
    Proc_2_10_407ED4
    Proc_2_11_4289CC
    Proc_2_12_40D358
    Proc_2_13_40A7FC
    Proc_2_14_4082BC
    Proc_2_15_408534
    Proc_2_16_4081D8
    Proc_2_17_408F14
    Proc_2_18_41B2EC
    Proc_2_24_4076C0
    Proc_2_25_4070CC
    Proc_2_26_409E60
    Proc_2_27_40A4A8
    Proc_2_28_409B70
    Proc_2_29_407C78
```

```
loc_41A606:   var_F4 = CStr(var_CC(0))
loc_41A64D:   Proc_2_36_40ABF8(var_CC, var_A4, Proc_21_0_408748(CStr(&H3A), 0), -1)
loc_41A65C:   var_108 = CStr(var_CC(0))
loc_41A67B:   If (Len(var_F4) > 3) Then
loc_41A86F:     ReDim var_274(0 To -1)
loc_41A8A7:     var_1C8 = Proc_21_0_408748(CStr(&H47)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H74)) & Proc_21_0_408748(CStr(&H4
loc_41A8CF:     var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_40874
loc_41A8F7:     var_228 = var_1F8 & Proc_21_0_408748(CStr(&H74)) & Proc_21_0_408748(CStr(&H50)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_40874
loc_41A91F:     var_258 = var_228 & Proc_21_0_408748(CStr(&H63)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_40874
loc_41A957:     var_134 = Proc_21_0_408748(CStr(&H6B), CLng(AscW(var_108))) & Proc_21_0_408748(CStr(&H65), 1) & Proc_21_0_408748(CStr(&H72)) & P
loc_41A97F:     var_164 = var_134 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_40874
loc_41A9A7:     var_26C = var_164 & Proc_21_0_408748(CStr(&H2E)) & Proc_21_0_408748(CStr(&H64)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_40874
loc_41A9B0:     PropBag.WriteProperty(var_26C, var_258 & Proc_21_0_408748(CStr(&H49)) & Proc_21_0_408748(CStr(&H64)), var_274)
loc_41A9B8:     Erase var_274
loc_41A9BC:     var_110 = var_B8
loc_41AC21:     ReDim var_274(0 To 2)
loc_41AC3B:     var_274(0) = &H1F0FFF
loc_41AC48:     var_274(1) = False
loc_41AC51:     var_274(2) = var_110
loc_41AC85:     var_1C8 = Proc_21_0_408748(CStr(&H4F)) & Proc_21_0_408748(CStr(&H70)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6
loc_41ACAD:     var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_408748(CStr(&H63)) & Proc_21_0_40874
loc_41ACE5:     var_134 = Proc_21_0_408748(CStr(&H6B), var_110) & Proc_21_0_408748(CStr(&H65), var_B8) & Proc_21_0_408748(CStr(&H72)) & Proc_21_
loc_41AD0D:     var_164 = var_134 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_40874
loc_41AD35:     var_20C = var_164 & Proc_21_0_408748(CStr(&H2E)) & Proc_21_0_408748(CStr(&H64)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_40874
loc_41AD3E:     PropBag.WriteProperty(var_20C, var_1F8 & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_408748(CStr(&H73)), var_274)
loc_41AD46:     Erase var_274
loc_41AD4A:     var_2F4 = var_B8
loc_41B01F:     var_B8 = GetModuleFileNameW(AscW(var_108))
loc_41B041:     ReDim var_274(0 To 4)
loc_41B053:     var_274(0) = var_F4
loc_41B06      var_2  (1) =  ng(0 &  roc_21_0_4   (CStr(&  0), var_  & Pro  1_0_  87   Str  H34), "&H", var_2F4)) & var_F4)
loc_41B        ar_2  (2) =  ar(var  8)
loc_41B        (3) =
loc_41B094:     ar_274(4) =  ar(Get  duleFile    var_B  )
loc_41B0C3:     ar_1C8 =     0_4     t   H57))  Proc  1_0_40    r(     Pr  21  08748(CStr(&H69)) & Proc_21_0_408748(CStr(&H7
loc_41B0EB:     var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H50)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_40874
loc_41B113:     var_228 = var_1F8 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_40874
loc_41B13B:     var_258 = var_228 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6D)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_40874
loc_41B173:     var_140 = Proc_21_0_408748(CStr(&H4B)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6
loc_41B19B:     var_170 = var_140 & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_408748(CStr(&H32)) & Proc_21_0_40874
```



ADVANCED STATIC ANALYSIS

DEBUGGING



IDA - C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
IDA View-EIP, Call Stack, Breakpoints, General registers, Modules, Threads, Hex View-EAX, Stack view
Structures
Enums
IDA View-EIP
Call Stack
Breakp
Trace window
General registers
Modules
Hex View-EAX
Hex View-EDX
Stack view
Output window
Python

```
ntdll.dll:7C912EBF 8B 7A 04          mov     edi, [edx+4]
ntdll.dll:7C912EC2 83 E0 FE          and     eax, 0FFFFFFFEh
ntdll.dll:7C912EC5 03 C6             add     eax, esi
ntdll.dll:7C912EC7 80 7D 10 00       cmp     byte ptr [ebp+10h], 0
ntdll.dll:7C912ECB 8B D0             mov     edx, eax
ntdll.dll:7C912ECD 89 55 0C          mov     [ebp+0Ch], edx
ntdll.dll:7C912ED0 0F 84 49 74 01 00 jz      loc_7C92A31F
ntdll.dll:7C912ED6 3B F2             cmp     esi, edx
ntdll.dll:7C912ED8 73 21             jnb     short loc_7C912EFB
ntdll.dll:7C912EDA A1 E0 B0 97 7C    mov     eax, off_7C97B0E0
ntdll.dll:7C912EDF
ntdll.dll:7C912EDF                   loc_7C912EDF:                   ; CODE XREF:
ntdll.dll:7C912EDF 66 8B 16          mov     dx, [esi]
ntdll.dll:7C912EE2 33 C9             xor     ecx, ecx
ntdll.dll:7C912EE4 66 8B 0F          mov     cx, [edi]
ntdll.dll:7C912EE7 46                inc     esi
ntdll.dll:7C912EE8 46                inc     esi
ntdll.dll:7C912EE9 47                inc     edi
ntdll.dll:7C912EEA 47                inc     edi
ntdll.dll:7C912EEB 66 3B D1          cmp     dx, cx
ntdll.dll:7C912EEE 89 7D 08          mov     [ebp+8], edi
EIP ntdll.dll:7C912EF1 89 4D 10      mov     [
ntdll.dll:7C912EF4 75 09                             2EFF
ntdll.dll:7C912EF6
ntdll.dll:7C912EF6                   7C912                           COD     EF:
ntdll.dll:7C912EF6 3B 75 0C                  [ebp+0Ch]
ntdll.dll:7C912EF9 72 E4                             2EDF
ntdll.dll:7C912EFB
ntdll.dll:7C912EFB                   7C912                           COD     EF:
ntdll.dll:7C912EFB                                                   ntd     ll:n
ntdll.dll:7C912EFB B0 01
ntdll.dll:7C912EFD EB B6             jmp                     2EB5
ntdll.dll:7C912EFF                   ; ---------------------------------------
ntdll.dll:7C912EFF
ntdll.dll:7C912EFF                   loc_7C912EFF:                   ; CODE XREF:
ntdll.dll:7C912EFF 66 83 FA 61       cmp     dx, 61h
ntdll.dll:7C912F03 73 24             jnb     short loc_7C912F29
UNKNOWN 7C912EF1: ntdll.dll:ntdll_RtlEqualUnicodeString+56
```

```
Thread    Address                                   Instruction
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000720  kernel32.dll:kernel32_WriteProcessMemory  mov  edi, edi
00000F24  kernel32.dll:kernel32_CreateProcessW      mov  edi, edi
```

```
EAX 7FFD2004  debug006:unk_7FFD2004              OF 0
EBX 7FFDF000  debug007:7FFDF000                  DF 0
ECX 00000061                                     IF 1
EDX 7C800041  kernel32.dll:7C800041              TF 0
ESI 7C80E164  kernel32.dll:kernel32_DuplicateHandle+2D6   SF 1
EDI 0001039E  debug001:0001039E                  ZF 0
EBP 0145EC84  Stack[00000F24]:0145EC84           AF 0
ESP 0145EC78  Stack[00000F24]:0145EC78           PF 0
EIP 7C912EF1  ntdll.dll:ntdll_RtlEqualUnicodeString+56    CF 1
EFL 00000283
```

```
Path                                                              Base      Size
C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_j...  00400000  0004C
C:\Program Files\IDA\plugins\HideDebugger.dll                    10000000  000510
C:\WINDOWS\system32\uxtheme.dll                                  5AD70000  00038
C:\WINDOWS\system32\netapi32.dll                                 5B860000  00055
C:\WINDOWS\system32\comctl32.dll                                 5D090000  0009A
C:\WINDOWS\system32\faultrep.dll                                 69450000  000160
C:\   W S\system  s2help.dll                                      71AA0000  00008
```

```
7FFD1FC4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
7FFD1FD4  00 00 00 00 00 00 00 00  00 00 00
7FFD1FE4  00 00 00 00 00 00 00 00  00 00 00
7FFD1FF4  00 00 00 00 00 00 00 00  00 00 00
7FFD2004  10 01 20 01 30 01 40 01  50 01 60
7FFD2014  00 01 00 01 00 01 00 01  00 01 00
7FFD2024  00 01 00 01 00 01 00 01  00 01 00
7FFD2034  00 01 00 01 00 01 00 01  00 01 00
7FFD2044  00 01 90 01 00 01 00 01  A0 01 00
UNKNOWN 7FFD2004: debug006:unk_7FFD2004
```

```
7C800001  5A 90 00 03 00 00 00 04  00 00 00 FF FF 00 00 B8  ZÉ.........  ..+
7C800011  00 00 00 00 00 00 00 40  00 00 00 00 00 00 00 00  .......@........
7C800021  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
7C800031  00 00 00 00 00 00 00 00  00 00 00 F0 00 00 00 0E  ...........=....
7C800041  1F BA 0E 00 B4 09 CD 21  B8 01 4C CD 21 54 68 69  .¦..¦.-!+.L-!Thi
7C800051  73 20 70 72 6F 67 72 61  6D 20 63 61 6E 6E 6F 74  s program cannot
7C800061  20 62 65 20 72 75 6E 20  69 6E 20 44 4F 53 20 6D   be run in DOS m
7C800071  6F 64 65 2E 0D 0D 0A 24  00 00 00 00 00 00 00 17  ode....$........
7C800081  86 20 AA 53 E7 4E F9 53  E7 4E F9 53 E7 4E F9 53  å ¬StN·StN·StN·S
7C800091  E7 4F F9 D9 E6 4E F9 90  E8 13 F9 50 E7 4E F9 90  tO·+µN·ÉF.·PtN·É
7C8000A1  E8 12 F9 52 E7 4E F9 90  E8 10 F9 52 E7 4E F9 90  F.·RtN·ÉF.·RtN·É
7C8000B1  E8 41 F9 56 E7 4E F9 90  E8 11 F9 8E E7 4E F9 90  FA·VtN·ÉF.·ÄtN·É
7C8000C1  E8 2E F9 57 E7 4E F9 90  E8 14 F9 52 E7 4E F9 52  F.·WtN·ÉF.·RtN·R
UNKNOWN 7C800041: kernel32.dll:7C800041
```

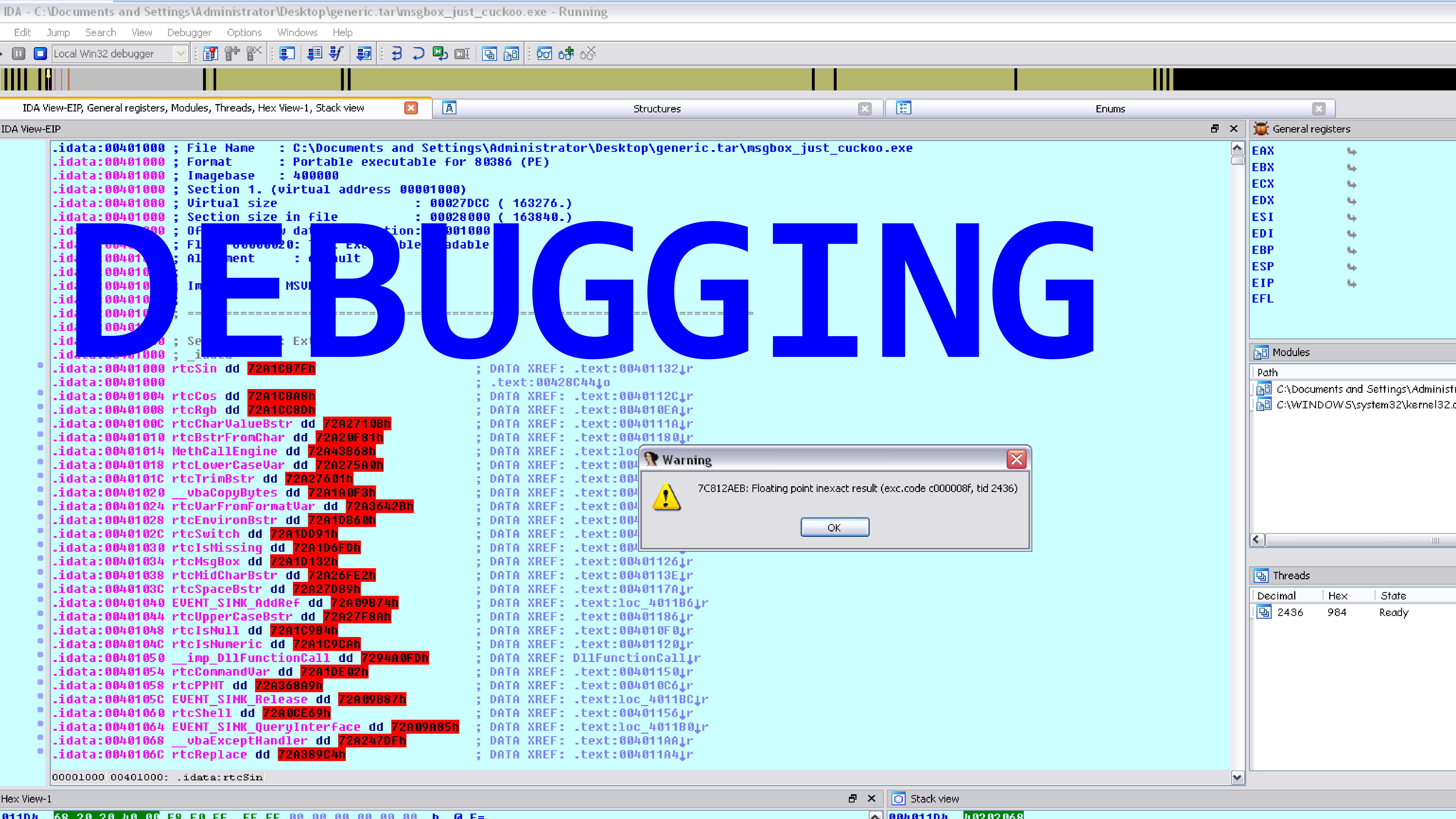
```
0145EC78  00000000
      C7C  00010000  debug001:off_10000
      C80  7FFDF000  debug007:7FFDF000
      C84  0145ECE8  Stack[00000F24]:0145ECE8
      C88  7C9145E6  ntdll.dll:ntdll_RtlQueryEnvironmentVariable_U+6D
      C8C  0001039E  debug001:0001039E
      C90  7C80E168  kernel32.dll:kernel32_DuplicateHandle+2DA
      C94  00000050
      C98  7C8855F8  kernel32.dll:unk_7C8855F8
UN 0145EC78: Stack[00000F24]:0145EC78
```

```
F 00 46        52     F 00 43    5 00  O.F._.P.R.O.C.E.
3 00 53        53     00 31      0 00  S.S.O.R.S.=.1...
F 00 53        69     00 64      F 00  O.S.=.W.i.n.d.o.
               54                1 00  w.s._.N.T...P.a.
  68                                   t.h.=.C.:.\.W.I.
E 00 44 00 4F 00 57 00  53 00 5C 00 73 00 79 00  N.D.O.W.S.\.s.y.
3 00 74 00 65 00 6D 00  33 00 32 00 3B 00 43 00  s.t.e.m.3.2.;.C.
A 00 5C 00 57 00 49 00  4E 00 44 00 4F 00 57 00  :.\.W.I.N.D.O.W.
3 00 3B 00 43 00 3A 00  5C 00 57 00 49 00 4E 00  S.;.C.:.\.W.I.N.
4 00 4F 00 57 00 53 00  5C 00 53 00 79 00 73 00  D.O.W.S.\.S.y.s.
000103FE  74 00 65 00 6D 00 33 00  32 00 5C 00 57 00 62 00  t.e.m.3.2.\.W.b.
0001040E  65 00 6D 00 00 00 50 00  41 00 54 00 48 00 45 00  e.m...P.A.T.H.E.
UNKNOWN 0001039E: debug001:0001039E
```

```
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
```

```
AU:  idle    Down    Disk: 4GB
```

DEBUGGING



IDA - C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe - Running
Edit
Jump
Search
View
Debugger
Options
Windows
Help
Local Win32 debugger
IDA View-EIP, General registers, Modules, Threads, Hex View-1, Stack view
Structures
Enums
IDA View-EIP
General registers
EAX
EBX
ECX
EDX
ESI
EDI
EBP
ESP
EIP
EFL
Modules
Path
C:\Documents and Settings\Administ
C:\WINDOWS\system32\kernel32.d
Threads
Decimal
Hex
State
Hex View-1
Stack view

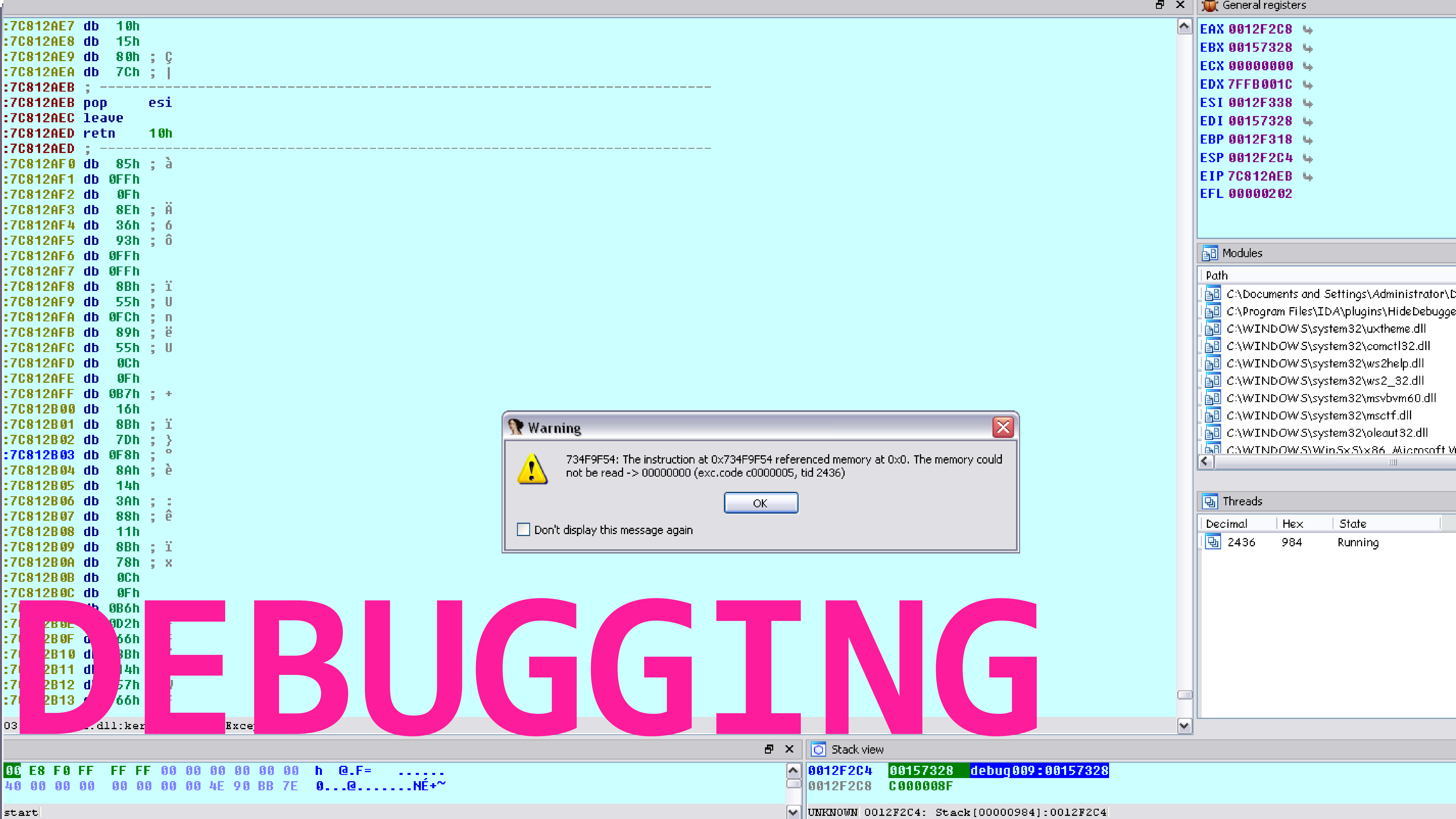
```
.idata:00401000 ; File Name   : C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe
.idata:00401000 ; Format      : Portable executable for 80386 (PE)
.idata:00401000 ; Imagebase   : 400000
.idata:00401000 ; Section 1. (virtual address 00001000)
.idata:00401000 ; Virtual size                  : 00027DCC ( 163276.)
.idata:00401000 ; Section size in file          : 00028000 ( 163840.)
.id        000 ; Of          w da        tion:    001000
.id   004      ; Fl   00000020:       Exe     ble   adable
.id   00401    ; Al    ment      :   ult
.id   0040
.id   00401      Im            MSV
.id   00401
.id   00401    ; ===============================================================
.id   0040
.id          0 ; Se             : Ext
.idata:00401000 ; _i
.idata:00401000 rtcSin dd 72A1CB7Fh                       ; DATA XREF: .text:00401132↓r
.idata:00401000                                           ; .text:00428C44↓o
.idata:00401004 rtcCos dd 72A1CBA8h                       ; DATA XREF: .text:0040112C↓r
.idata:00401008 rtcRgb dd 72A1CC8Dh                       ; DATA XREF: .text:004010EA↓r
.idata:0040100C rtcCharValueBstr dd 72A2710Bh             ; DATA XREF: .text:0040111A↓r
.idata:00401010 rtcBstrFromChar dd 72A20F81h              ; DATA XREF: .text:00401180↓r
.idata:00401014 MethCallEngine dd 72A43B68h               ; DATA XREF: .text:loc
.idata:00401018 rtcLowerCaseVar dd 72A275A0h              ; DATA XREF: .text:004
.idata:0040101C rtcTrimBstr dd 72A27601h                  ; DATA XREF: .text:004
.idata:00401020 __vbaCopyBytes dd 72A1A0F3h               ; DATA XREF: .text:004
.idata:00401024 rtcVarFromFormatVar dd 72A3642Bh          ; DATA XREF: .text:004
.idata:00401028 rtcEnvironBstr dd 72A1DB60h               ; DATA XREF: .text:004
.idata:0040102C rtcSwitch dd 72A1DD91h                    ; DATA XREF: .text:004
.idata:00401030 rtcIsMissing dd 72A1D6FDh                 ; DATA XREF: .text:004
.idata:00401034 rtcMsgBox dd 72A1D132h                    ; DATA XREF: .text:00401126↓r
.idata:00401038 rtcMidCharBstr dd 72A26FE2h               ; DATA XREF: .text:0040113E↓r
.idata:0040103C rtcSpaceBstr dd 72A27DB9h                 ; DATA XREF: .text:0040117A↓r
.idata:00401040 EVENT_SINK_AddRef dd 72A09B74h            ; DATA XREF: .text:loc_4011B6↓r
.idata:00401044 rtcUpperCaseBstr dd 72A27F8Ah             ; DATA XREF: .text:00401186↓r
.idata:00401048 rtcIsNull dd 72A1C9B4h                    ; DATA XREF: .text:004010F0↓r
.idata:0040104C rtcIsNumeric dd 72A1C9CAh                 ; DATA XREF: .text:00401120↓r
.idata:00401050 __imp_DllFunctionCall dd 7294A0FDh        ; DATA XREF: DllFunctionCall↓r
.idata:00401054 rtcCommandVar dd 72A1DE02h                ; DATA XREF: .text:00401150↓r
.idata:00401058 rtcPPMT dd 72A368A9h                      ; DATA XREF: .text:004010C6↓r
.idata:0040105C EVENT_SINK_Release dd 72A09B87h           ; DATA XREF: .text:loc_4011BC↓r
.idata:00401060 rtcShell dd 72A0CE69h                     ; DATA XREF: .text:00401156↓r
.idata:00401064 EVENT_SINK_QueryInterface dd 72A09A85h    ; DATA XREF: .text:loc_4011B0↓r
.idata:00401068 __vbaExceptHandler dd 72A247DFh           ; DATA XREF: .text:004011AA↓r
.idata:0040106C rtcReplace dd 72A389C4h                   ; DATA XREF: .text:004011A4↓r
00001000 00401000: .idata:rtcSin
```

Warning

7C812AEB: Floating point inexact result (exc.code c000008f, tid 2436)

OK

Decimal	Hex	State
2436	984	Ready



DEBUGGING

```
:7C812AE7 db  10h
:7C812AE8 db  15h
:7C812AE9 db  80h ; Ç
:7C812AEA db  7Ch ; |
:7C812AEB ; ---------------------------------------------------------------------------
:7C812AEB pop     esi
:7C812AEC leave
:7C812AED retn    10h
:7C812AED ; ---------------------------------------------------------------------------
:7C812AF0 db  85h ; à
:7C812AF1 db 0FFh
:7C812AF2 db  0Fh
:7C812AF3 db  8Eh ; Ä
:7C812AF4 db  36h ; 6
:7C812AF5 db  93h ; ô
:7C812AF6 db 0FFh
:7C812AF7 db 0FFh
:7C812AF8 db  8Bh ; ï
:7C812AF9 db  55h ; U
:7C812AFA db 0FCh ; n
:7C812AFB db  89h ; ë
:7C812AFC db  55h ; U
:7C812AFD db  0Ch
:7C812AFE db  0Fh
:7C812AFF db 0B7h ; +
:7C812B00 db  16h
:7C812B01 db  8Bh ; ï
:7C812B02 db  7Dh ; }
:7C812B03 db 0F8h ; °
:7C812B04 db  8Ah ; è
:7C812B05 db  14h
:7C812B06 db  3Ah ; :
:7C812B07 db  88h ; ê
:7C812B08 db  11h
:7C812B09 db  8Bh ; ï
:7C812B0A db  78h ; x
:7C812B0B db  0Ch
:7C812B0C db  0Fh
:7C        h 0B6h
:7C 2B0E    0D2h
:7C 2B0F d   66h
:7C 2B10 d   8Bh
:7C 2B11 d   14h
:7C 2B12 d   57h
:7C 2B13 d   66h
03      .dll:ker      Exce
```

Warning

734F9F54: The instruction at 0x734F9F54 referenced memory at 0x0. The memory could not be read -> 00000000 (exc.code c0000005, tid 2436)

OK

□ Don't display this message again

General registers

```
EAX 0012F2C8
EBX 00157328
ECX 00000000
EDX 7FFB001C
ESI 0012F338
EDI 00157328
EBP 0012F318
ESP 0012F2C4
EIP 7C812AEB
EFL 00000202
```

Modules

Path
C:\Documents and Settings\Administrator\D
C:\Program Files\IDA\plugins\HideDebugge
C:\WINDOWS\system32\uxtheme.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\ws2help.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\msvbvm60.dll
C:\WINDOWS\system32\msctf.dll
C:\WINDOWS\system32\oleaut32.dll
C:\WINDOWS\WinSxS\x86_Microsoft.W

Threads

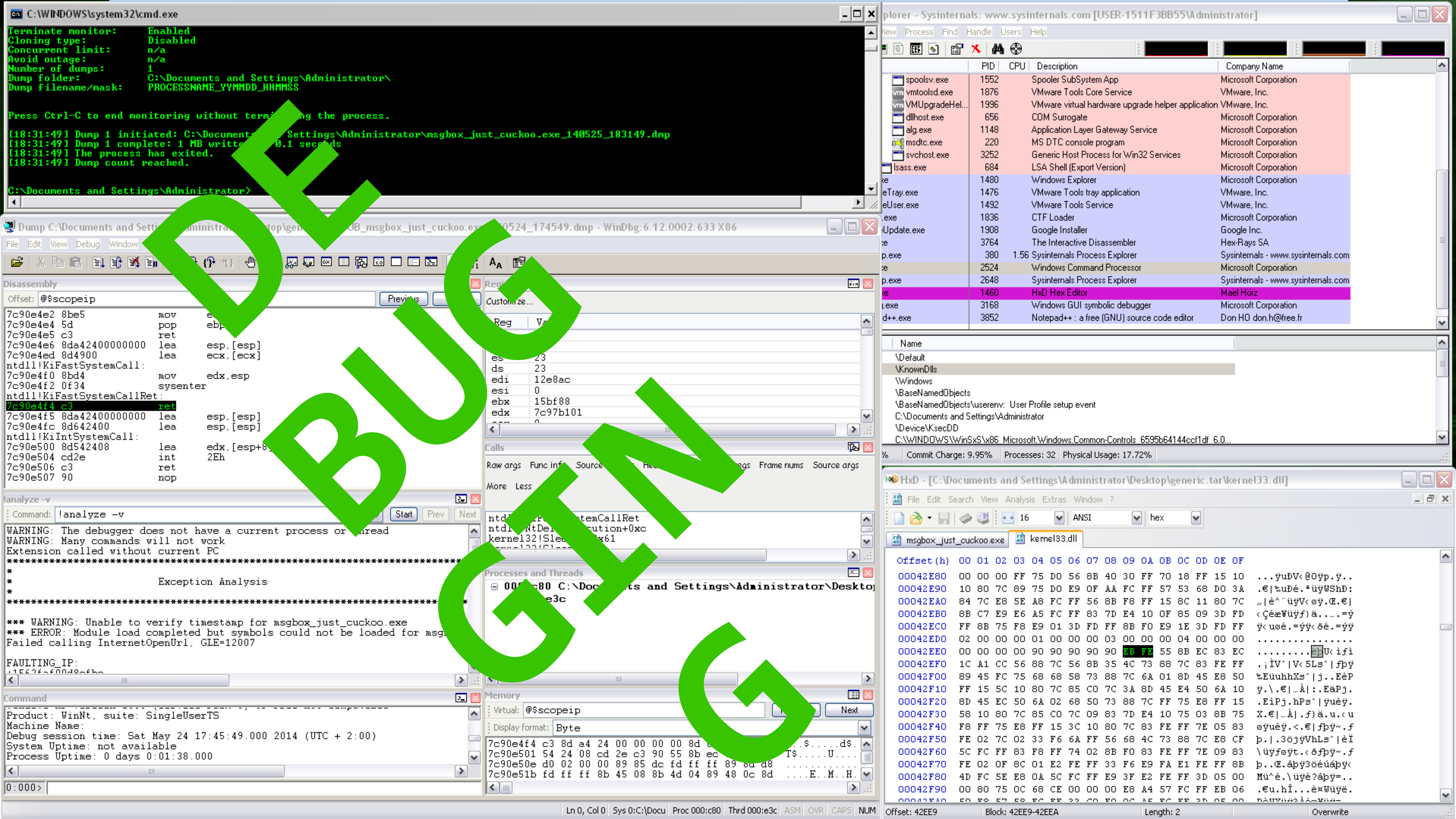
Decimal	Hex	State
2436	984	Running

```
00 E8 F0 FF  FF FF 00 00 00 00 00 00  h  @.F=    ......
40 00 00 00  00 00 00 00 4E 90 BB 7E  0...@.......NÉ+~
start
```

Stack view

```
0012F2C4  00157328  debug009:00157328
0012F2C8  C000008F
UNKNOWN 0012F2C4: Stack[00000984]:0012F2C4
```

DEBUGGING



C:\WINDOWS\system32\cmd.exe

```
Terminate monitor:       Enabled
Cloning type:            Disabled
Concurrent limit:        n/a
Avoid outage:            n/a
Number of dumps:         1
Dump folder:             C:\Documents and Settings\Administrator\
Dump filename/mask:      PROCESSNAME_YYMMDD_HHMMSS

Press Ctrl-C to end monitoring without term     ng the process.

[18:31:49] Dump 1 initiated: C:\Document     Settings\Administrator\msgbox_just_cuckoo.exe_140525_183149.dmp
[18:31:49] Dump 1 complete: 1 MB writte     0.1 seconds
[18:31:49] The process has exited.
[18:31:49] Dump count reached.

C:\Documents and Settings\Administrator>
```

Dump C:\Documents and Setti   dministra   top\gen   UB_msgbox_just_cuckoo.ex   0524_174549.dmp - WinDbg:6.12.0002.633 X86

Disassembly — Offset: @$scopeip

```
7c90e4e2 8be5           mov     e
7c90e4e4 5d             pop     ebp
7c90e4e5 c3             ret
7c90e4e6 8da42400000000 lea     esp,[esp]
7c90e4ed 8d4900         lea     ecx,[ecx]
ntdll!KiFastSystemCall:
7c90e4f0 8bd4           mov     edx,esp
7c90e4f2 0f34           sysenter
ntdll!KiFastSystemCallRet:
7c90e4f4 c3             ret
7c90e4f5 8da42400000000 lea     esp,[esp]
7c90e4fc 8d642400       lea     esp,[esp]
ntdll!KiIntSystemCall:
7c90e500 8d542408       lea     edx,[esp+8
7c90e504 cd2e           int     2Eh
7c90e506 c3             ret
7c90e507 90             nop
```

Registers

Reg	Va
es	23
ds	23
edi	12e8ac
esi	0
ebx	15bf88
edx	7c97b101

Calls

```
ntd      F      temCallRet
ntdl  NtDe      cution+0xc
kernel32!Slee     x61
```

!analyze -v — Command: !analyze -v

```
WARNING: The debugger does not have a current process or   hread
WARNING: Many commands will not work
Extension called without current PC
*******************************************************************************
*
*                        Exception Analysis
*
*******************************************************************************

*** WARNING: Unable to verify timestamp for msgbox_just_cuckoo.exe
*** ERROR: Module load completed but symbols could not be loaded for msg
Failed calling InternetOpenUrl, GLE=12007

FAULTING_IP:
```

Processes and Threads

```
00   c80 C:\Doc     ts and Settings\Administrator\Deskto
     e3c
```

Command

```
Product: WinNt, suite: SingleUserTS
Machine Name:
Debug session time: Sat May 24 17:45:49.000 2014 (UTC + 2:00)
System Uptime: not available
Process Uptime: 0 days 0:01:38.000
```

0:000>

Memory — Virtual: @$scopeip — Display format: Byte

```
7c90e4f4 c3 8d a4 24 00 00 00 00 8d     .$.....d$.
7c90e501 54 24 08 cd 2e c3 90 55 8b ec     T$.....U...
7c90e50e d0 02 00 00 89 85 dc fd ff ff 89 8d d8
7c90e51b fd ff ff 8b 45 08 8b 4d 04 89 48 0c 8d     ....E..M..H.
```

Ln 0, Col 0 | Sys 0:C:\Docu | Proc 000:c80 | Thrd 000:e3c | ASM | OVR | CAPS | NUM

plorer - Sysinternals: www.sysinternals.com [USER-1511F3BB55\Administrator]

	PID	CPU	Description	Company Name
spoolsv.exe	1552		Spooler SubSystem App	Microsoft Corporation
vmtoolsd.exe	1876		VMware Tools Core Service	VMware, Inc.
VMUpgradeHel...	1996		VMware virtual hardware upgrade helper application	VMware, Inc.
dllhost.exe	656		COM Surrogate	Microsoft Corporation
alg.exe	1148		Application Layer Gateway Service	Microsoft Corporation
msdtc.exe	220		MS DTC console program	Microsoft Corporation
svchost.exe	3252		Generic Host Process for Win32 Services	Microsoft Corporation
lsass.exe	684		LSA Shell (Export Version)	Microsoft Corporation
xe	1480		Windows Explorer	Microsoft Corporation
eTray.exe	1476		VMware Tools tray application	VMware, Inc.
eUser.exe	1492		VMware Tools Service	VMware, Inc.
.exe	1836		CTF Loader	Microsoft Corporation
Update.exe	1908		Google Installer	Google Inc.
e	3764		The Interactive Disassembler	Hex-Rays SA
p.exe	380	1.56	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
e	2524		Windows Command Processor	Microsoft Corporation
p.exe	2648		Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
e	1460		HxD Hex Editor	Maël Hörz
.exe	3168		Windows GUI symbolic debugger	Microsoft Corporation
d++.exe	3852		Notepad++ : a free (GNU) source code editor	Don HO don.h@free.fr

Name
\Default
\KnownDlls
\Windows
\BaseNamedObjects
\BaseNamedObjects\userenv: User Profile setup event
C:\Documents and Settings\Administrator
\Device\KsecDD
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...

Commit Charge: 9.95% | Processes: 32 | Physical Usage: 17.72%

HxD - [C:\Documents and Settings\Administrator\Desktop\generic.tar\kernel33.dll]

16 | ANSI | hex

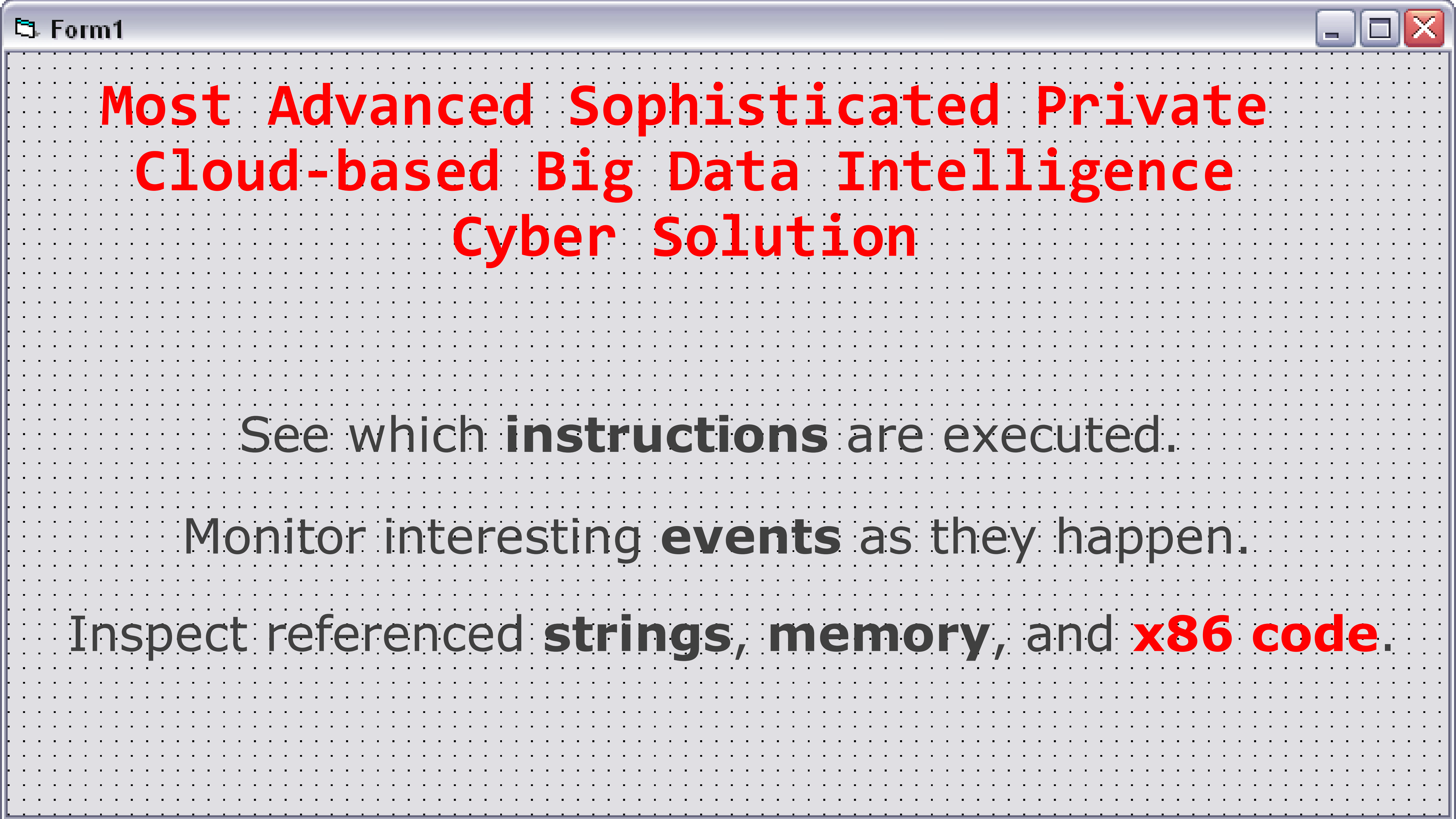
msgbox_just_cuckoo.exe | kernel33.dll

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00042E80  00 00 00 FF 75 D0 56 8B 40 30 FF 70 18 FF 15 10  ...ÿuÐV‹@0ÿp.ÿ..
00042E90  10 80 7C 89 75 D0 E9 0F AA FC FF 57 53 68 D0 3A  .€|‰uÐé.ªüÿWShÐ:
00042EA0  84 7C E8 5E A8 FC FF 56 8B F8 FF 15 8C 11 80 7C  „|è^¨üÿV‹øÿ.Œ.€|
00042EB0  8B C7 E9 E6 A5 FC FF 83 7D E4 10 0F 85 09 3D FD  ‹Çéæ¥üÿƒ}ä..…..=ý
00042EC0  FF 8B 75 F8 E9 01 3D FD FF 8B F0 E9 1E 3D FD FF  ÿ‹uøé.=ýÿ‹ðé.=ýÿ
00042ED0  02 00 00 00 01 00 00 00 03 00 00 00 04 00 00 00  ................
00042EE0  00 00 00 00 90 90 90 90 90 EB FE 55 8B EC 83 EC  .........ëþU‹ìƒì
00042EF0  1C A1 CC 56 88 7C 56 8B 35 4C 73 88 7C 83 FE FF  .¡ÌV^|V‹5Ls^|ƒþÿ
00042F00  89 45 FC 75 68 68 58 73 88 7C 6A 01 8D 45 E8 50  ‰EüuhhXs^|j..EèP
00042F10  FF 15 5C 10 80 7C 85 C0 7C 3A 8D 45 E4 50 6A 10  ÿ.\.€|…À|:.EäPj.
00042F20  8D 45 EC 50 6A 02 68 50 73 88 7C FF 75 E8 FF 15  .EìPj.hPs^|ÿuèÿ.
00042F30  58 10 80 7C 85 C0 7C 09 83 7D E4 10 75 03 8B 75  X.€|…À|.ƒ}ä.u.‹u
00042F40  F8 FF 75 E8 FF 15 3C 10 80 7C 83 FE FF 7E 05 83  øÿuèÿ.<.€|ƒþÿ~.ƒ
00042F50  FE 02 7C 02 33 F6 6A FF 56 68 4C 73 88 7C E8 CF  þ.|.3öjÿVhLs^|èÏ
00042F60  5C FC FF 83 F8 FF 74 02 8B F0 83 FE FF 7E 09 83  \üÿƒøÿt.‹ðƒþÿ~.ƒ
00042F70  FE 02 0F 8C 01 E2 FE FF 33 F6 E9 FA E1 FE FF 8B  þ..Œ.âþÿ3öéúáþÿ‹
00042F80  4D FC 5E E8 0A 5C FC FF E9 3F E2 FE FF 3D 05 00  Mü^è.\üÿé?âþÿ=..
00042F90  00 80 75 0C 68 CE 00 00 00 E8 A4 57 FC FF EB 06  .€u.hÎ...è¤Wüÿë.
```

Offset: 42EE9 | Block: 42EE9-42EEA | Length: 2 | Overwrite

V00D00 MAGIX



Most Advanced Sophisticated Private Cloud-based Big Data Intelligence Cyber Solution

See which **instructions** are executed.

Monitor interesting **events** as they happen.

Inspect referenced **strings**, **memory**, and **x86 code**.

Form1

VB6 Instrumentation

Patch the 6 jumptables!

Form2

Generic
Instrument everything

Capture everything
Create **Statistics**

Form2

Specific
Implementing specific instruction handlers

“OpenFile” - filename

Form1

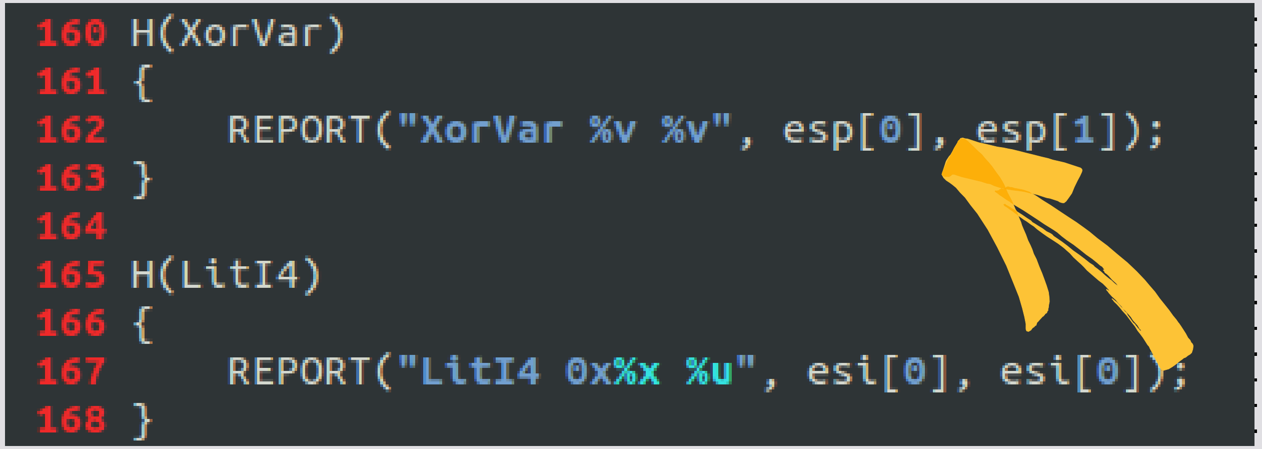
Patching A Function Handler

Patch original address with our custom assembly stub

1. Store current **register / stack state**
2. Call custom **instruction handler**
3. Pass **registers** as parameters
4. **Do STUFF**
5. **Restore** original state

Jump to original function handler.

Life goes on.



```
H(XorVar)
{
    REPORT("XorVar %v %v", esp[0], esp[1]);
}

H(LitI4)
{
    REPORT("LitI4 0x%x %u", esi[0], esi[0]);
}
```

Form1

Tailored Reporting For VB6

Custom printf()

• **BSTR**	unicode string with its size prepended
• **VARIANT**	generic wrapper around int, str, etc.

Custom hexdump() to aid debugging

Form1

Cuckoofy It

Slightly modified Cuckoo Sandbox

Execute the sample with our custom DLL

Form1

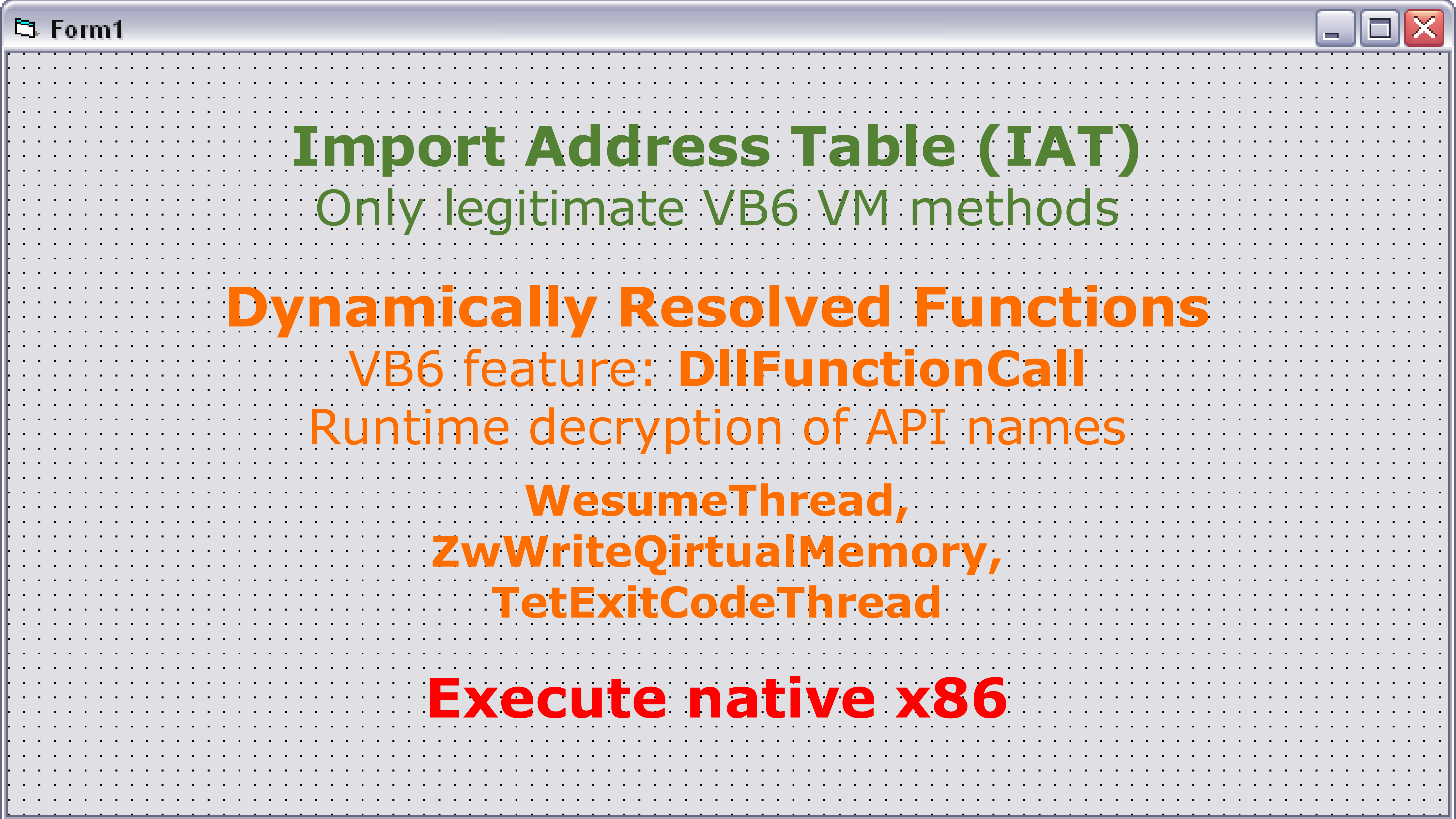
VB6 ANALYSIS

The Somewhat Peculiar Results aka. Disease

Obfuscation and garbage

Anti-X features

Three ways to call external functions



Import Address Table (IAT)

Only legitimate VB6 VM methods

Dynamically Resolved Functions

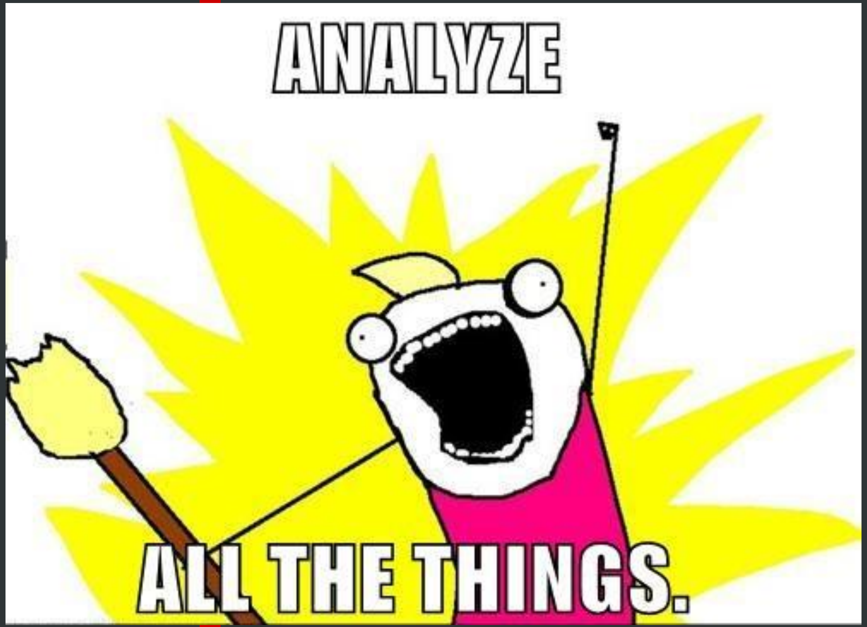
VB6 feature: **DllFunctionCall**

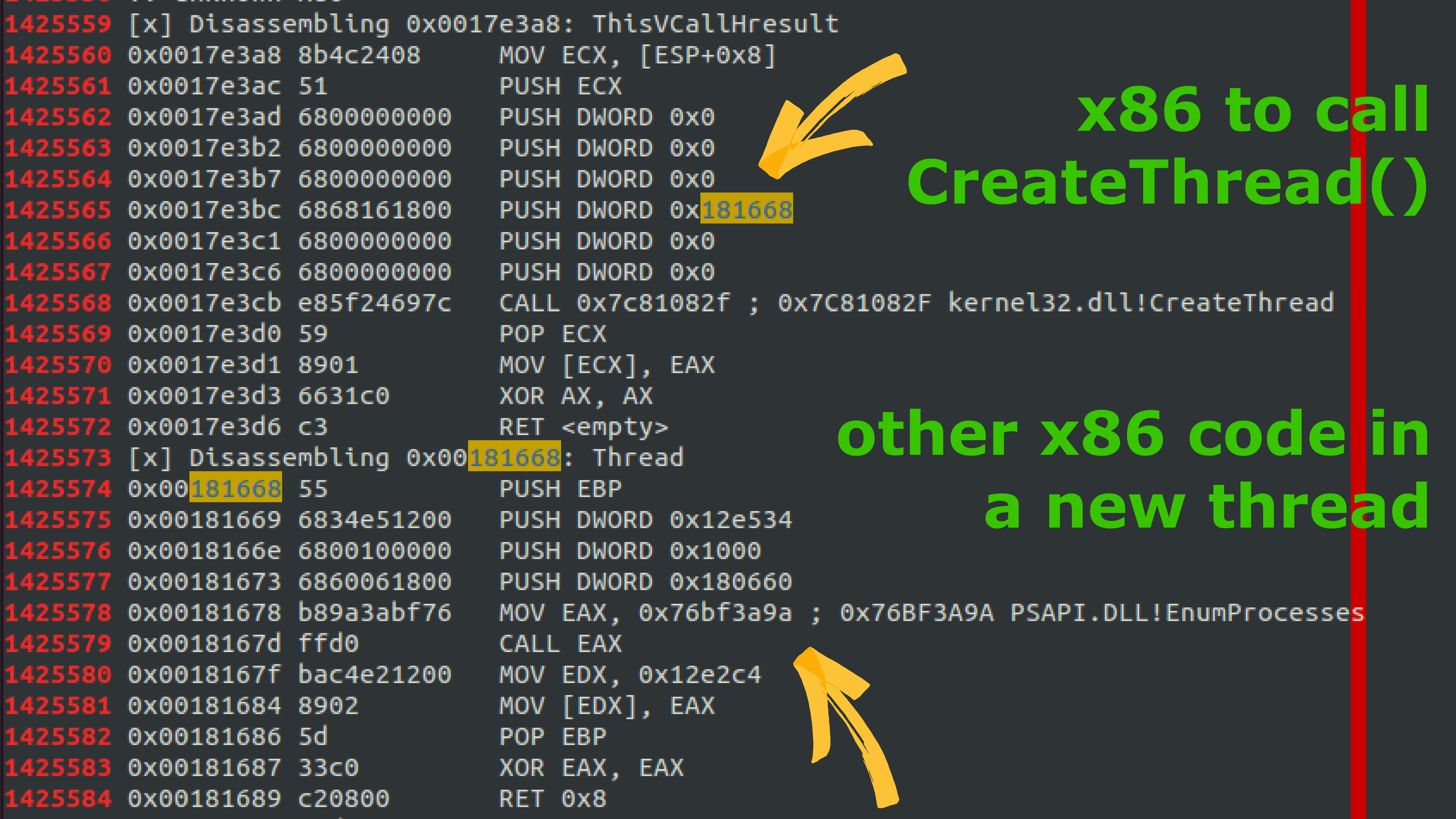
Runtime decryption of API names

WesumeThread,
ZwWriteQirtualMemory,
TetExitCodeThread

Execute native x86

```
417273 [x] Calling VB6 Procedure.. 0x0040862c
417274 004085e8 FStSTrCopy "8B4C240851E844FF6A7C5989016631C0C3"
417275 004085ee LitI4 0x00000000 0
417276 00408623 ImpAdCallI2 fn 0x0040113e
417277 [x] Calling imported function.. MSVBVM60.DLL!rtcMidCharBstr
417278 00408628 FStStr "C3"
417279 00409f1c ConcatStr "&h" "C3"
417280 00409f26 LitI2_Byte 2
417281 0040b615 ThisVCallHresult fn 0x004038a3
417282 [x] Calling VB6 Method.. 0x004097e4
417283 00409754 LitI4 0x00000004 4
417284 00409759 ImpAdCallI2 fn 0x004010d2
417285 [x] Calling imported function.. MSVBVM60.DLL!__vbaCopyBytes
417286 00409766 MemLdStr
417287 00409769 LitI4 0x0000001c 28
417288 0040977a MemLdStr
417289 00409783 LitI4 0x00000004 4
417290 00409788 ImpAdCallI2 fn 0x004010d2
417291 [x] Calling imported function.. MSVBVM60.DLL!__vbaCopyBytes
417292 0040978f LitI4 0x00000000 0
417293 004097a6 MemLdStr
417294 004097a9 LitI4 0x00000004 4
417295 004097ae ImpAdCallI2 fn 0x004010d2
417296 [x] Calling imported function.. MSVBVM60.DLL!__vbaCopyBytes
417297 004097b8 ThisVCallHresult fn 0x00159a00
417298 .. unknown x86
417299 [x] Disassembling 0x00159a00: ThisVCallHresult
417300 0x00159a00 8b4c2408      MOV ECX, [ESP+0x8]
417301 0x00159a04 51            PUSH ECX
417302 0x00159a05 e844ff6a7c    CALL 0x7c80994e ; 0x7C80994E kernel32.dll!GetCurrentProcessId
417303 0x00159a0a 59            POP ECX
417304 0x00159a0b 8901          MOV [ECX], EAX
417305 0x00159a0d 6631c0        XOR AX, AX
417306 0x00159a10 c3            RET <empty>
```





```
[x] Disassembling 0x0017e3a8: ThisVCallHresult
0x0017e3a8 8b4c2408     MOV ECX, [ESP+0x8]
0x0017e3ac 51           PUSH ECX
0x0017e3ad 6800000000   PUSH DWORD 0x0
0x0017e3b2 6800000000   PUSH DWORD 0x0
0x0017e3b7 6800000000   PUSH DWORD 0x0
0x0017e3bc 6868161800   PUSH DWORD 0x181668
0x0017e3c1 6800000000   PUSH DWORD 0x0
0x0017e3c6 6800000000   PUSH DWORD 0x0
0x0017e3cb e85f24697c   CALL 0x7c81082f ; 0x7C81082F kernel32.dll!CreateThread
0x0017e3d0 59           POP ECX
0x0017e3d1 8901         MOV [ECX], EAX
0x0017e3d3 6631c0       XOR AX, AX
0x0017e3d6 c3           RET <empty>
[x] Disassembling 0x00181668: Thread
0x00181668 55           PUSH EBP
0x00181669 6834e51200   PUSH DWORD 0x12e534
0x0018166e 6800100000   PUSH DWORD 0x1000
0x00181673 6860061800   PUSH DWORD 0x180660
0x00181678 b89a3abf76   MOV EAX, 0x76bf3a9a ; 0x76BF3A9A PSAPI.DLL!EnumProcesses
0x0018167d ffd0         CALL EAX
0x0018167f bac4e21200   MOV EDX, 0x12e2c4
0x00181684 8902         MOV [EDX], EAX
0x00181686 5d           POP EBP
0x00181687 33c0         XOR EAX, EAX
0x00181689 c20800       RET 0x8
```

x86 to call CreateThread()

other x86 code in a new thread

The Yet To Be Identified Infamous Anti-Cuckoo Feature (c)

Thank You!

Project @ https://github.com/jbremer/vb6tracer