THE DEVELOPER'S CONFERENCE

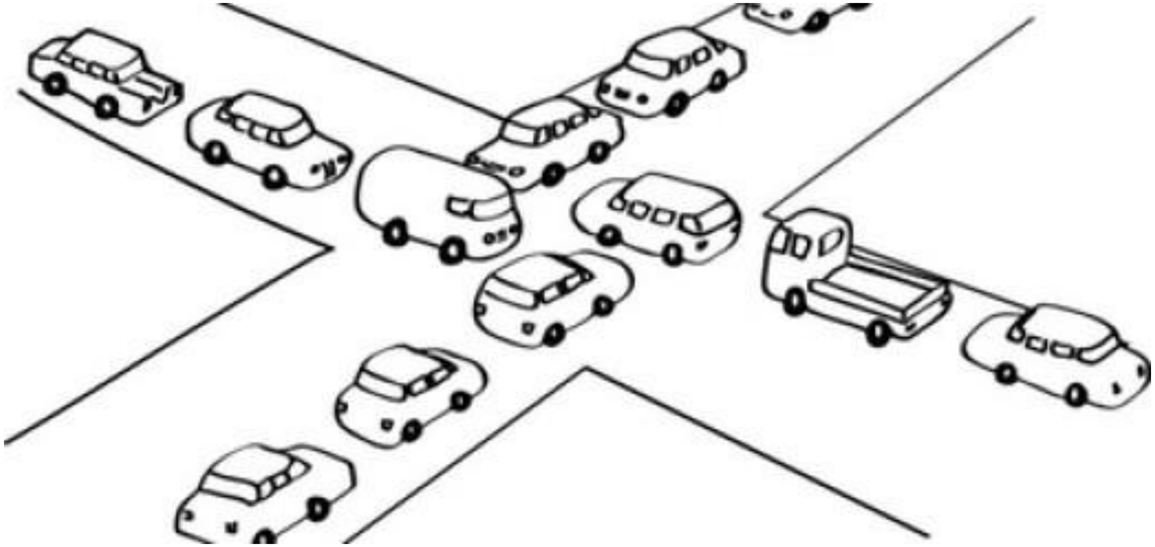
Trilha C/C++

Wanderley Caloni

Sócio-Desenvolvedor da

INTELITRADER

Depurando até o fim do mundo: técnicas e truques de WinDbg



Onde sou? Quem estou?

- Segurança da Informação
  - Sistema de Controle de Usuários e Aplicações
  - Criptografia de Discos

Onde sou? Quem estou?

- Análise de Trojans
  - Engenharia Reversa
  - Crash Dump Analysis

tempest
SECURITY INTELLIGENCE

open
communications
security

Onde sou? Quem estou?

- Mercado Financeiro
  - Alto Desempenho
  - Análise de Risco

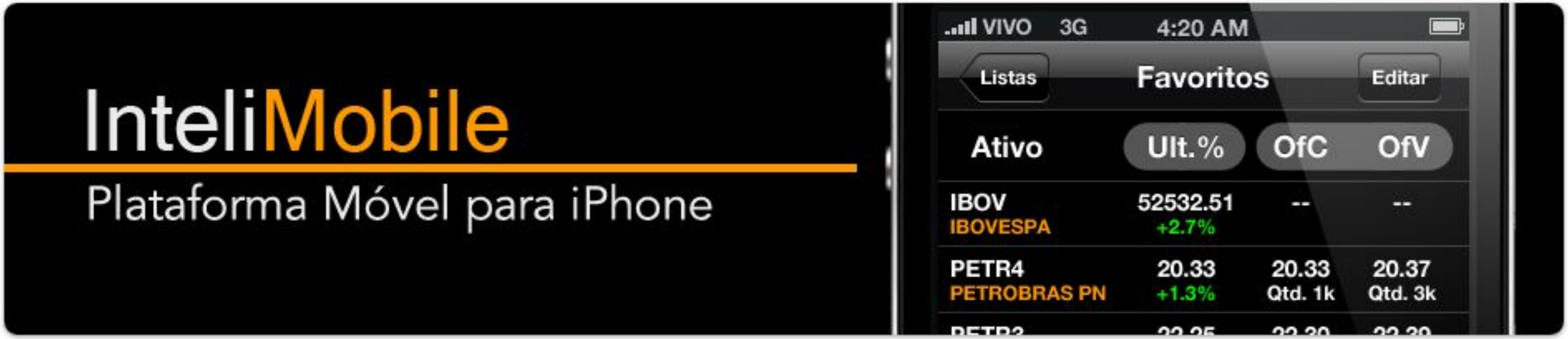
Onde sou? Quem estou?

INTELITRADER

- Mercado Financeiro
  - Alto Desempenho
  - Algoritmos
  - Cotações
  - Mobile

Onde sou? Quem estou?

Onde sou? Quem estou?

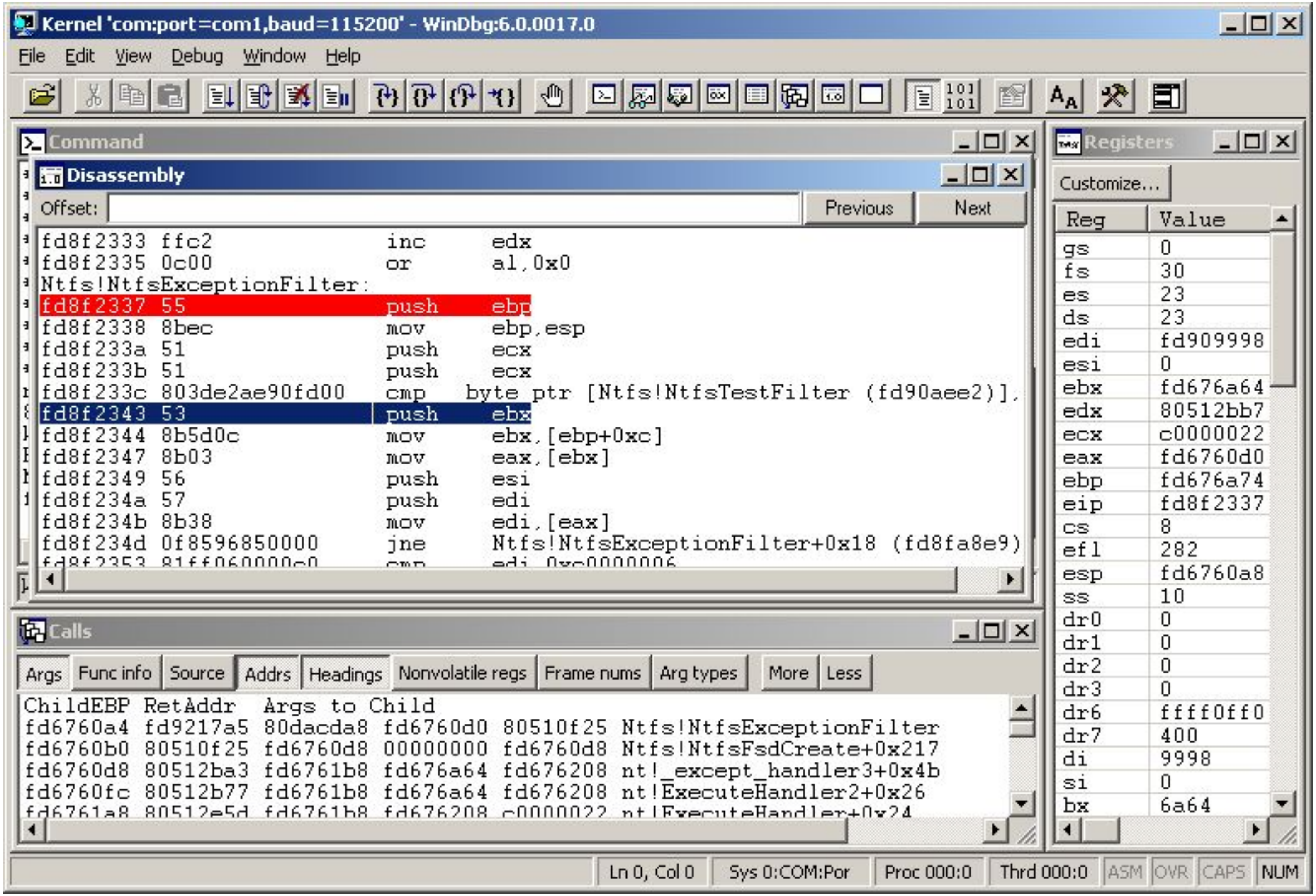


Ativo	Ult.%	OfC	OfV
IBOV IBOVESPA	52532.51 +2.7%	--	--
PETR4 PETROBRAS PN	20.33 +1.3%	20.33 Qtd. 1k	20.37 Qtd. 3k

Onde sou? Quem estou?

InteliMarket
Flexibilidade em Market Data
- Balanceamento de Carga
- Certificado UMDF

Vamos ao que interessa?

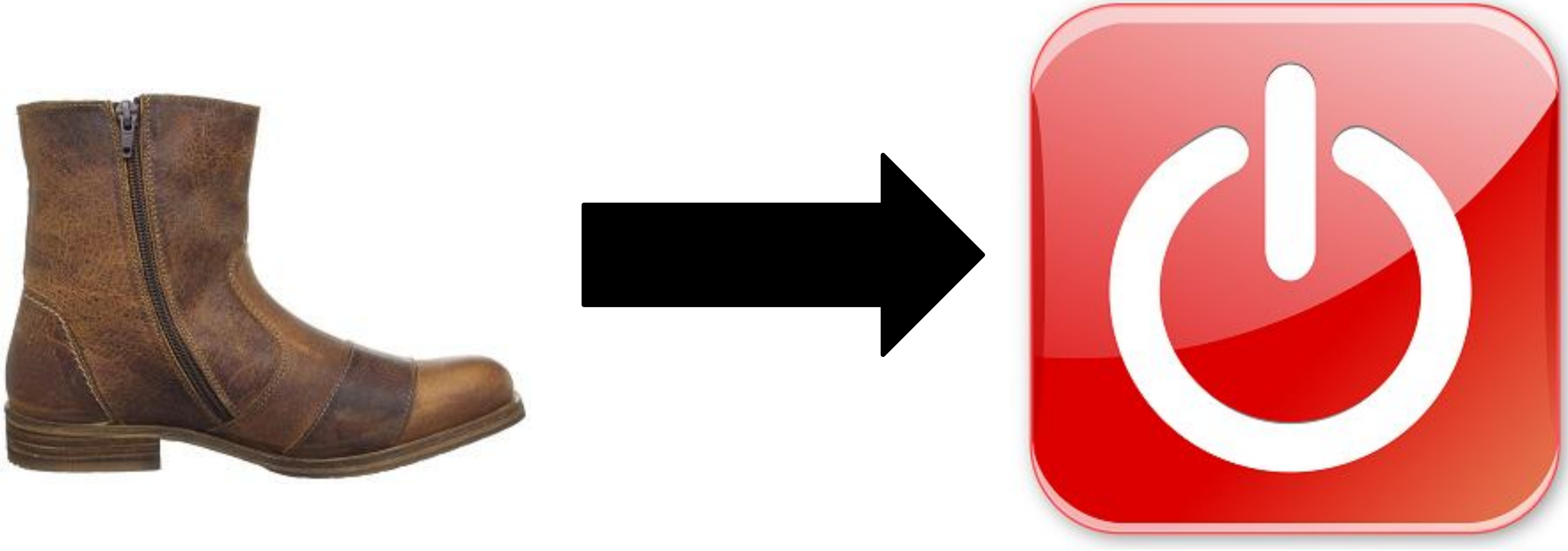


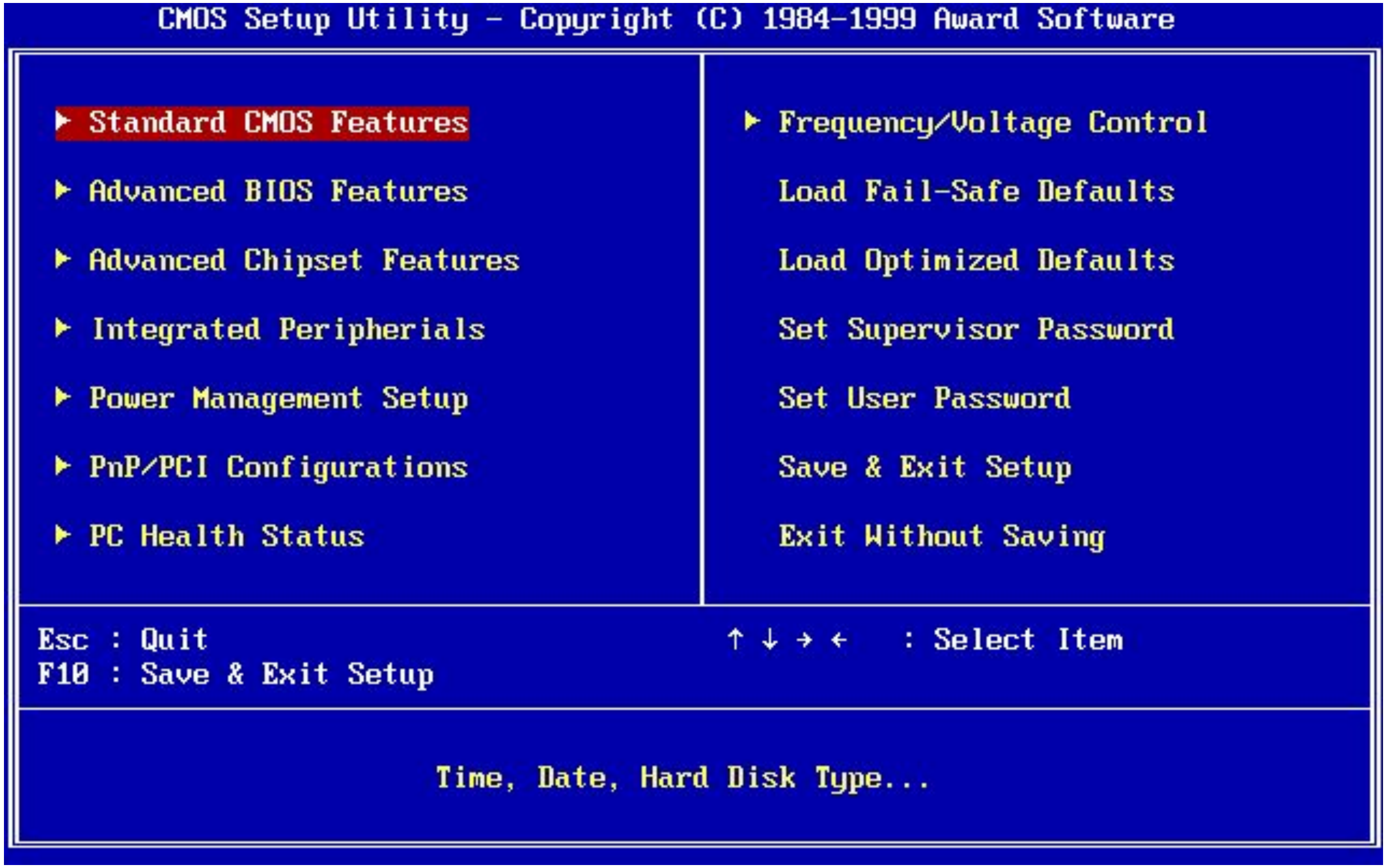
```
fd8f2333 ffc2              inc     edx
fd8f2335 0c00              or      al,0x0
Ntfs!NtfsExceptionFilter:
fd8f2337 55                push    ebp
fd8f2338 8bec              mov     ebp,esp
fd8f233a 51                push    ecx
fd8f233b 51                push    ecx
fd8f233c 803de2ae90fd00    cmp    byte ptr [Ntfs!NtfsTestFilter (fd90aee2)],
fd8f2343 53                push    ebx
fd8f2344 8b5d0c            mov     ebx,[ebp+0xc]
fd8f2347 8b03              mov     eax,[ebx]
fd8f2349 56                push    esi
fd8f234a 57                push    edi
fd8f234b 8b38              mov     edi,[eax]
fd8f234d 0f8596850000      jne     Ntfs!NtfsExceptionFilter+0x18 (fd8fa8e9)
fd8f2353 81ff060000c0      cmp     edi,0xc0000006
```

```
ChildEBP RetAddr  Args to Child
fd6760a4 fd9217a5 80dacda8 fd6760d0 80510f25 Ntfs!NtfsExceptionFilter
fd6760b0 80510f25 fd6760d8 00000000 fd6760d8 Ntfs!NtfsFsdCreate+0x217
fd6760d8 80512ba3 fd6761b8 fd676a64 fd676208 nt!_except_handler3+0x4b
fd6760fc 80512b77 fd6761b8 fd676a64 fd676208 nt!ExecuteHandler2+0x26
fd6761a8 80512e5d fd6761b8 fd676208 c0000022 nt!ExecuteHandler+0x24
```

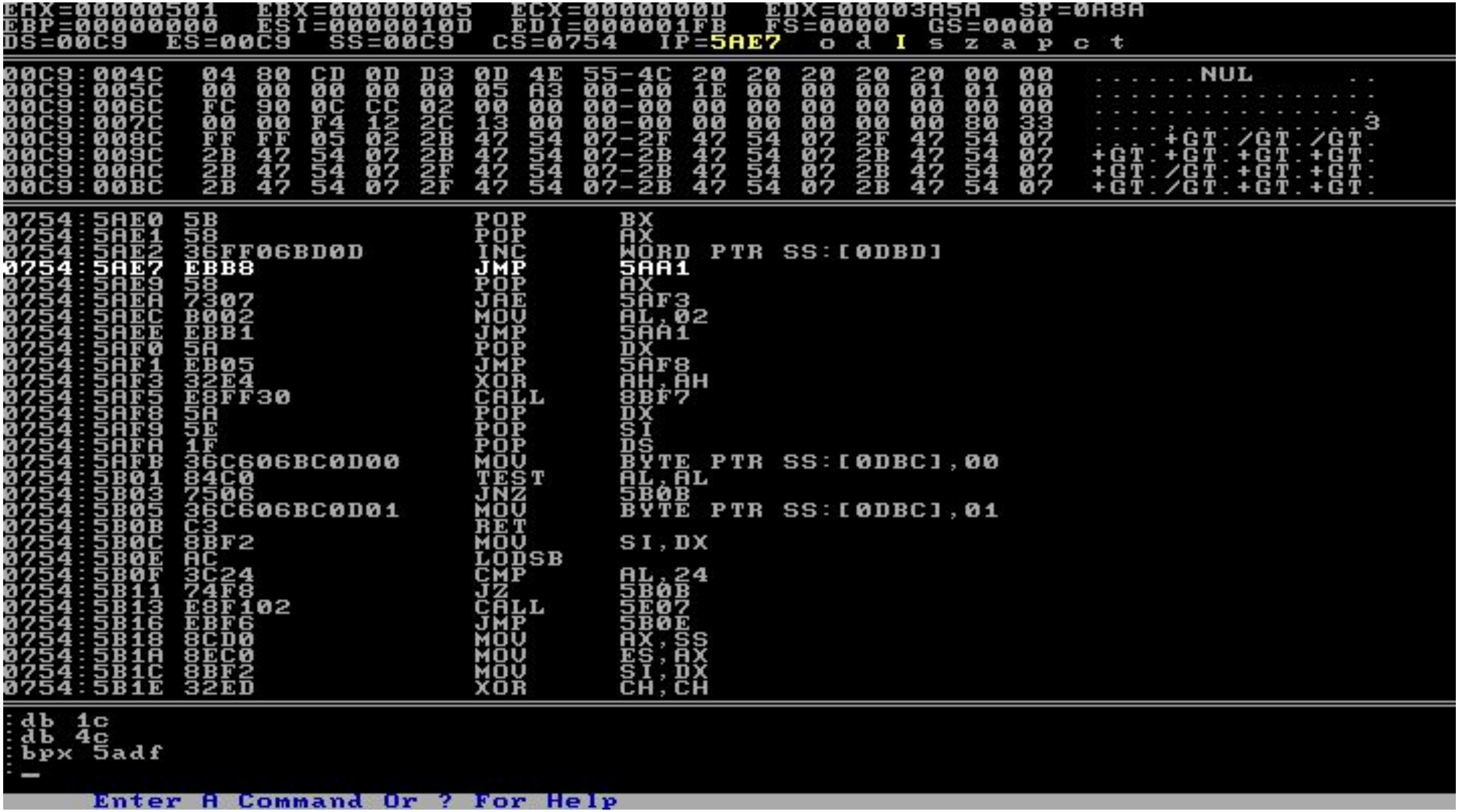
Reg	Value
gs	0
fs	30
es	23
ds	23
edi	fd909998
esi	0
ebx	fd676a64
edx	80512bb7
ecx	c0000022
eax	fd6760d0
ebp	fd676a74
eip	fd8f2337
cs	8
efl	282
esp	fd6760a8
ss	10
dr0	0
dr1	0
dr2	0
dr3	0
dr6	ffff0ff0
dr7	400
di	9998
si	0
bx	6a64

dd ed kv kvn . ~ .frame lm a
.dvalloc .dvfree .symfix .reload
!analyze –v r !uniqstack bp bl bm
bc bd s !heap dv bm dd poi(esp+8)
!db !eb .sympath .srcpath .kvn
.frame .cls .echo u –remote
–premote –server .help symstore
adplus logger logviewer !sym noisy
.call wt !heap l+* –flt s 1034 –p –a



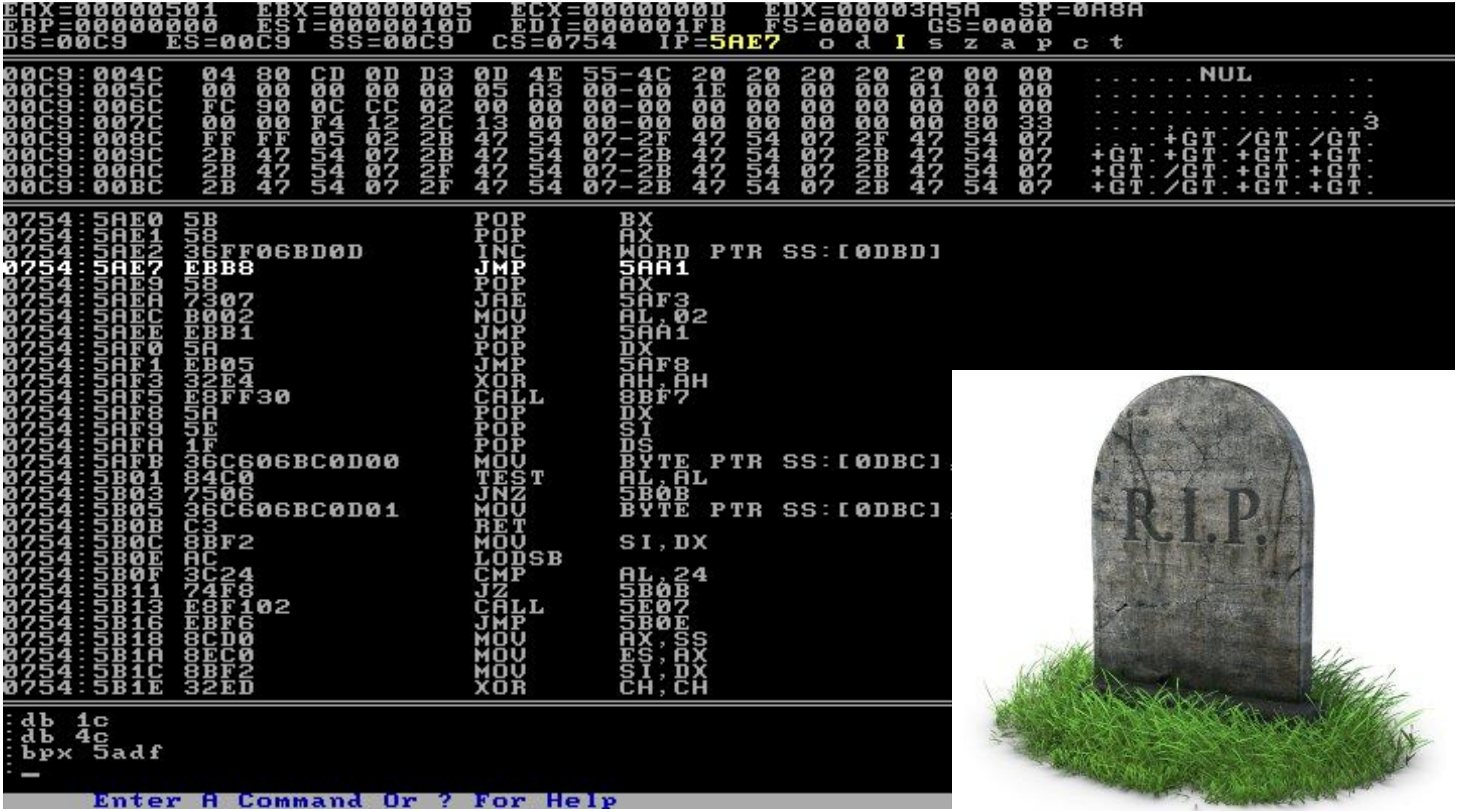


```
          CMOS Setup Utility - Copyright (C) 1984-1999 Award Software

 ▶ Standard CMOS Features           ▶ Frequency/Voltage Control

 ▶ Advanced BIOS Features             Load Fail-Safe Defaults

 ▶ Advanced Chipset Features          Load Optimized Defaults

 ▶ Integrated Peripherials            Set Supervisor Password

 ▶ Power Management Setup             Set User Password

 ▶ PnP/PCI Configurations             Save & Exit Setup

 ▶ PC Health Status                   Exit Without Saving

 Esc : Quit                         ↑ ↓ → ←   : Select Item
 F10 : Save & Exit Setup

                    Time, Date, Hard Disk Type...
```



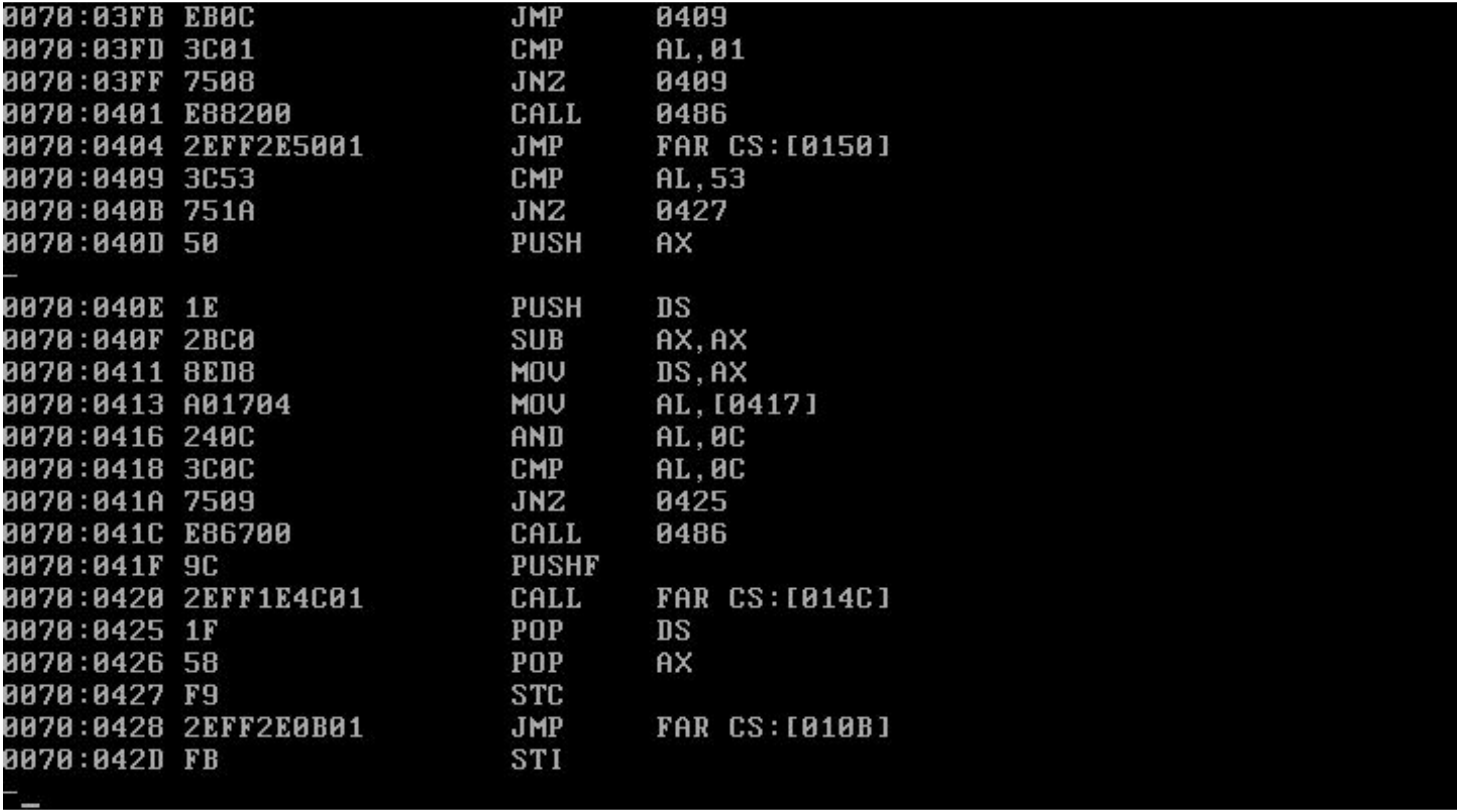
```
EAX=00000501   EBX=00000005   ECX=0000000D   EDX=00003A5A   SP=0A8A
EBP=00000000   ESI=0000010D   EDI=000001FB   FS=0000   GS=0000
DS=00C9   ES=00C9   SS=00C9   CS=0754   IP=5AE7   o d I s z a p c t
00C9:004C  04 80 CD 0D D3 0D 4E 55-4C 20 20 20 20 20 00 00   ......NUL     ..
00C9:005C  00 00 00 00 00 05 A3 00-00 1E 00 00 00 01 01 00   ................
00C9:006C  FC 90 0C CC 02 00 00 00-00 00 00 00 00 00 00 00   ................
00C9:007C  00 00 F4 12 2C 13 00 00-00 00 00 00 00 00 80 33   ....,..........3
00C9:008C  FF FF 05 02 2B 47 54 07-2F 47 54 07 2F 47 54 07   ....+GT./GT./GT.
00C9:009C  2B 47 54 07 2B 47 54 07-2B 47 54 07 2B 47 54 07   +GT.+GT.+GT.+GT.
00C9:00AC  2B 47 54 07 2F 47 54 07-2B 47 54 07 2B 47 54 07   +GT./GT.+GT.+GT.
00C9:00BC  2B 47 54 07 2F 47 54 07-2B 47 54 07 2B 47 54 07   +GT./GT.+GT.+GT.
0754:5AE0 5B                POP     BX
0754:5AE1 58                POP     AX
0754:5AE2 36FF06BD0D        INC     WORD PTR SS:[0DBD]
0754:5AE7 EBB8              JMP     5AA1
0754:5AE9 58                POP     AX
0754:5AEA 7307              JAE     5AF3
0754:5AEC B002              MOV     AL,02
0754:5AEE EBB1              JMP     5AA1
0754:5AF0 5A                POP     DX
0754:5AF1 EB05              JMP     5AF8
0754:5AF3 32E4              XOR     AH,AH
0754:5AF5 E8FF30            CALL    8BF7
0754:5AF8 5A                POP     DX
0754:5AF9 5E                POP     SI
0754:5AFA 1F                POP     DS
0754:5AFB 36C606BC0D00      MOV     BYTE PTR SS:[0DBC],00
0754:5B01 84C0              TEST    AL,AL
0754:5B03 7506              JNZ     5B0B
0754:5B05 36C606BC0D01      MOV     BYTE PTR SS:[0DBC],01
0754:5B0B C3                RET
0754:5B0C 8BF2              MOV     SI,DX
0754:5B0E AC                LODSB
0754:5B0F 3C24              CMP     AL,24
0754:5B11 74F8              JZ      5B0B
0754:5B13 E8F102            CALL    5E07
0754:5B16 EBF6              JMP     5B0E
0754:5B18 8CD0              MOV     AX,SS
0754:5B1A 8EC0              MOV     ES,AX
0754:5B1C 8BF2              MOV     SI,DX
0754:5B1E 32ED              XOR     CH,CH
:db 1c
:db 4c
:bpx 5adf
:_
     Enter A Command Or ? For Help
```

SOFTICE



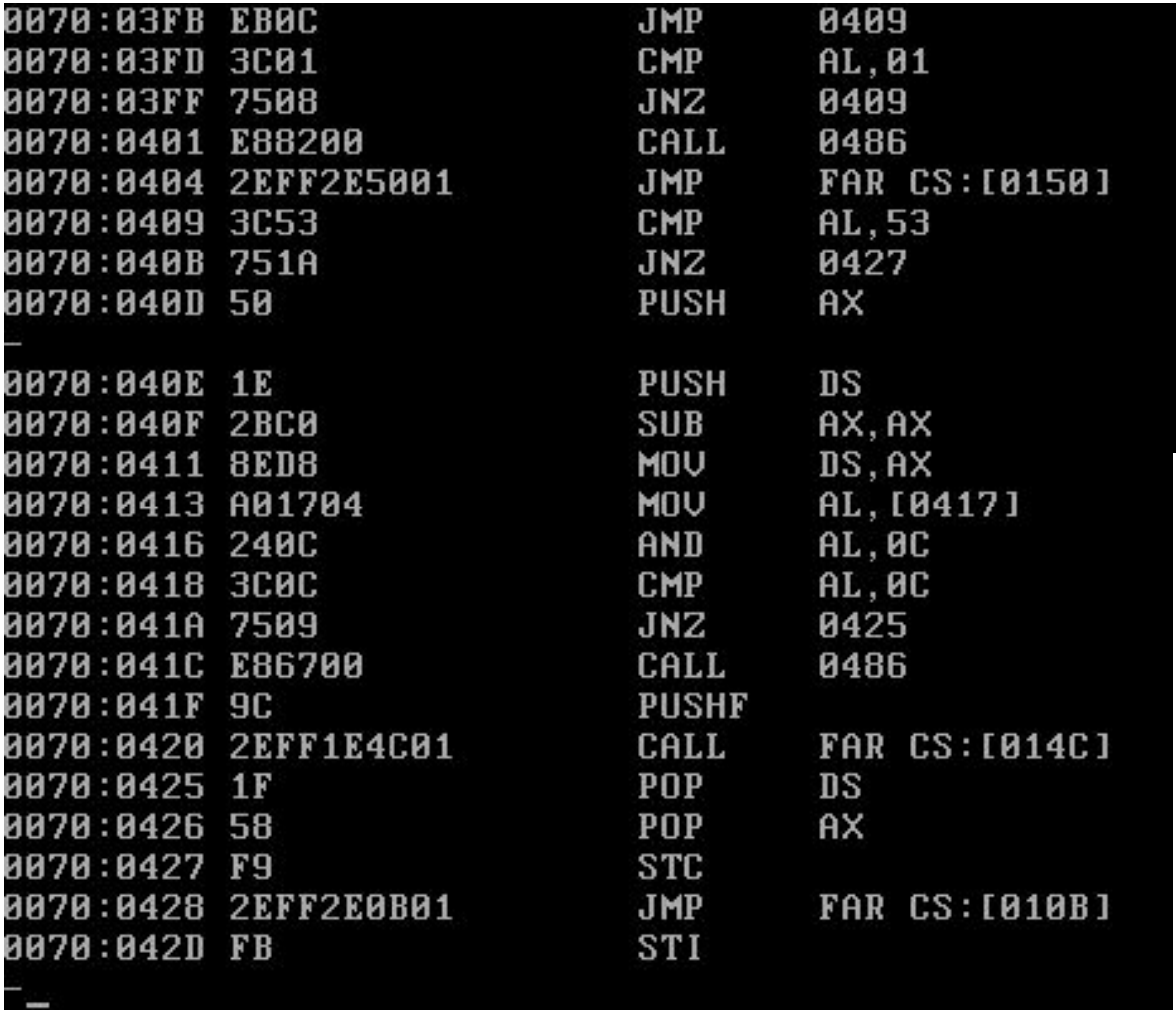
```
EAX=00000501   EBX=00000005   ECX=0000000D   EDX=00003A5A   SP=0A8A
EBP=00000000   ESI=0000010D   EDI=000001FB   FS=0000   GS=0000
DS=00C9   ES=00C9   SS=00C9   CS=0754   IP=5AE7   o d I s z a p c t
00C9:004C  04 80 CD 0D D3 0D 4E 55-4C 20 20 20 20 20 00 00  .......NUL    ..
00C9:005C  00 00 00 00 00 05 A3 00-00 1E 00 00 00 01 01 00  ................
00C9:006C  FC 90 0C CC 02 00 00 00-00 00 00 00 00 00 00 00  ................
00C9:007C  00 00 F4 12 2C 13 00 00-00 00 00 00 00 00 80 33  ....,..........3
00C9:008C  FF FF 05 02 2B 47 54 07-2F 47 54 07 2F 47 54 07  ....+GT./GT./GT.
00C9:009C  2B 47 54 07 2B 47 54 07-2B 47 54 07 2B 47 54 07  +GT.+GT.+GT.+GT.
00C9:00AC  2B 47 54 07 2F 47 54 07-2B 47 54 07 2B 47 54 07  +GT./GT.+GT.+GT.
00C9:00BC  2B 47 54 07 2F 47 54 07-2B 47 54 07 2B 47 54 07  +GT./GT.+GT.+GT.
0754:5AE0 5B                POP     BX
0754:5AE1 58                POP     AX
0754:5AE2 36FF06BD0D        INC     WORD PTR SS:[0DBD]
0754:5AE7 EBB8              JMP     5AA1
0754:5AE9 58                POP     AX
0754:5AEA 7307              JAE     5AF3
0754:5AEC B002              MOV     AL,02
0754:5AEE EBB1              JMP     5AA1
0754:5AF0 5A                POP     DX
0754:5AF1 EB05              JMP     5AF8
0754:5AF3 32E4              XOR     AH,AH
0754:5AF5 E8FF30            CALL    8BF7
0754:5AF8 5A                POP     DX
0754:5AF9 5E                POP     SI
0754:5AFA 1F                POP     DS
0754:5AFB 36C606BC0D00      MOV     BYTE PTR SS:[0DBC],
0754:5B01 84C0              TEST    AL,AL
0754:5B03 7506              JNZ     5B0B
0754:5B05 36C606BC0D01      MOV     BYTE PTR SS:[0DBC],
0754:5B0B C3                RET
0754:5B0C 8BF2              MOV     SI,DX
0754:5B0E AC                LODSB
0754:5B0F 3C24              CMP     AL,24
0754:5B11 74F8              JZ      5B0B
0754:5B13 E8F102            CALL    5E07
0754:5B16 EBF6              JMP     5B0E
0754:5B18 8CD0              MOV     AX,SS
0754:5B1A 8EC0              MOV     ES,AX
0754:5B1C 8BF2              MOV     SI,DX
0754:5B1E 32ED              XOR     CH,CH
:db 1c
:db 4c
:bpx 5adf
:
:_
     Enter A Command Or ? For Help
```

SOFTICE



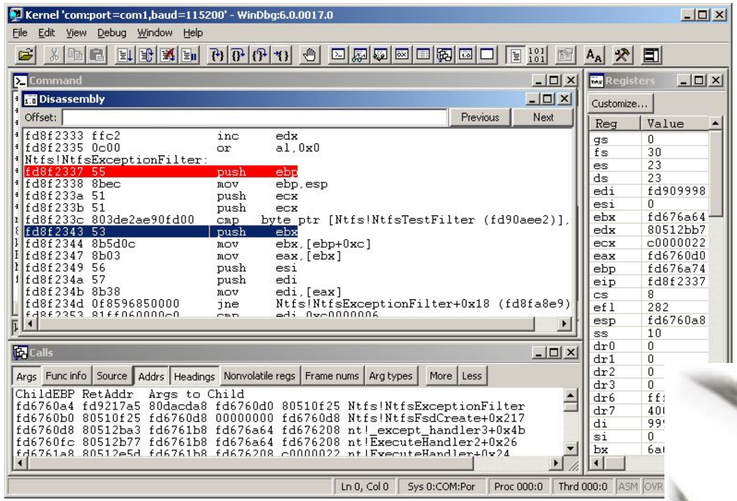
```
0070:03FB EB0C              JMP     0409
0070:03FD 3C01              CMP     AL,01
0070:03FF 7508              JNZ     0409
0070:0401 E88200            CALL    0486
0070:0404 2EFF2E5001        JMP     FAR CS:[0150]
0070:0409 3C53              CMP     AL,53
0070:040B 751A              JNZ     0427
0070:040D 50                PUSH    AX
-
0070:040E 1E                PUSH    DS
0070:040F 2BC0              SUB     AX,AX
0070:0411 8ED8              MOV     DS,AX
0070:0413 A01704            MOV     AL,[0417]
0070:0416 240C              AND     AL,0C
0070:0418 3C0C              CMP     AL,0C
0070:041A 7509              JNZ     0425
0070:041C E86700            CALL    0486
0070:041F 9C                PUSHF
0070:0420 2EFF1E4C01        CALL    FAR CS:[014C]
0070:0425 1F                POP     DS
0070:0426 58                POP     AX
0070:0427 F9                STC
0070:0428 2EFF2E0B01        JMP     FAR CS:[010B]
0070:042D FB                STI
-_
```

DEBUG.COM



```
0070:03FB EB0C          JMP     0409
0070:03FD 3C01          CMP     AL,01
0070:03FF 7508          JNZ     0409
0070:0401 E88200        CALL    0486
0070:0404 2EFF2E5001    JMP     FAR CS:[0150]
0070:0409 3C53          CMP     AL,53
0070:040B 751A          JNZ     0427
0070:040D 50            PUSH    AX
-
0070:040E 1E            PUSH    DS
0070:040F 2BC0          SUB     AX,AX
0070:0411 8ED8          MOV     DS,AX
0070:0413 A01704        MOV     AL,[0417]
0070:0416 240C          AND     AL,0C
0070:0418 3C0C          CMP     AL,0C
0070:041A 7509          JNZ     0425
0070:041C E86700        CALL    0486
0070:041F 9C            PUSHF
0070:0420 2EFF1E4C01    CALL    FAR CS:[014C]
0070:0425 1F            POP     DS
0070:0426 58            POP     AX
0070:0427 F9            STC
0070:0428 2EFF2E0B01    JMP     FAR CS:[010B]
0070:042D FB            STI
-_
```

DEBUG.COM



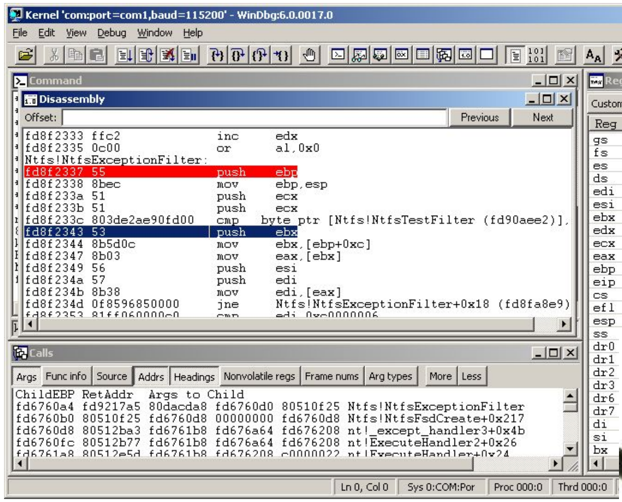
```
fd8f2333 ffc2           inc     edx
fd8f2335 0c00           or      al,0x0
Ntfs!NtfsExceptionFilter:
fd8f2337 55             push    ebp
fd8f2338 8bec           mov     ebp,esp
fd8f233a 51             push    ecx
fd8f233b 51             push    ecx
fd8f233c 803de2ae90fd00 cmp   byte ptr [Ntfs!NtfsTestFilter (fd90aee2)],
fd8f2343 53             push    ebx
fd8f2344 8b5d0c         mov     ebx,[ebp+0xc]
fd8f2347 8b03           mov     eax,[ebx]
fd8f2349 56             push    esi
fd8f234a 57             push    edi
fd8f234b 8b38           mov     edi,[eax]
fd8f234d 0f8596850000   jne     Ntfs!NtfsExceptionFilter+0x18 (fd8fa8e9)
```

Reg	Value
gs	0
fs	30
es	23
ds	23
edi	fd909998
esi	0
ebx	fd676a64
edx	80512bb7
ecx	c0000022
eax	fd6760d0
ebp	fd676a74
eip	fd8f2337
cs	8
efl	282
esp	fd6760a8
ss	10
dr0	0
dr1	0
dr2	0
dr3	0
dr6	ff
dr7	40
di	99
si	0
bx	6a

```
ChildEBP RetAddr  Args to Child
fd6760a4 fd9217a5 80dacda8 fd6760d0 80510f25 Ntfs!NtfsExceptionFilter
fd6760b0 80510f25 fd6760d8 00000000 fd6760d8 Ntfs!NtfsFsdCreate+0x217
fd6760d8 80512ba3 fd6761b8 fd676a64 fd676208 nt!_except_handler3+0x4b
fd6760fc 80512b77 fd6761b8 fd676a64 fd676208 nt!ExecuteHandler2+0x26
```

bcdedit /dbgsettings
bcdedit /copy {current}
bcdedit set debug on

windbg.exe -k com:port=1,baud=115200,resets=0,reconnect -b



Kernel 'com:port=com1,baud=115200' - WinDbg:6.0.0017.0

```
fd8f2333 ffc2           inc     edx
fd8f2335 0c00           or      al,0x0
Ntfs!NtfsExceptionFilter:
fd8f2337 55             push    ebp
fd8f2338 8bec           mov     ebp,esp
fd8f233a 51             push    ecx
fd8f233b 51             push    ecx
fd8f233c 803de2ae90fd00 cmp   byte ptr [Ntfs!NtfsTestFilter (fd90aee2)],
fd8f2343 53             push    ebx
fd8f2344 8b5d0c         mov     ebx,[ebp+0xc]
fd8f2347 8b03           mov     eax,[ebx]
fd8f2349 56             push    esi
fd8f234a 57             push    edi
fd8f234b 8b38           mov     edi,[eax]
fd8f234d 0f8596850000   jne     Ntfs!NtfsExceptionFilter+0x18 (fd8fa8e9)
fd8f2353 81ff060000c0   cmp     edi,0xc0000006
```

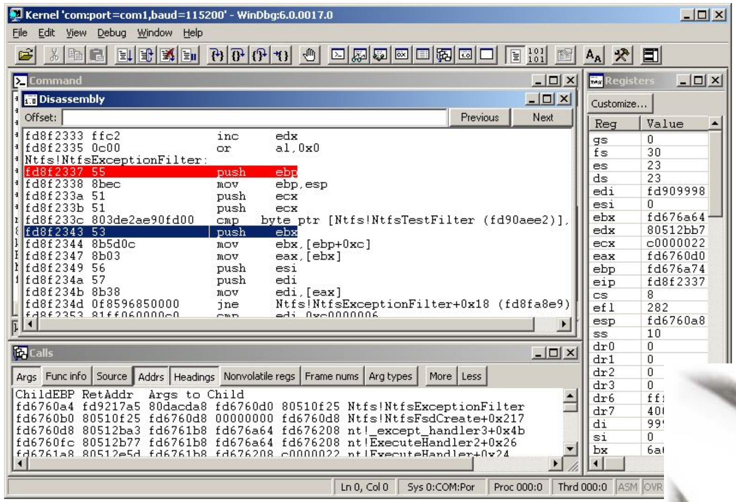
Reg	Value
gs	0
fs	30
es	23
ds	23
edi	fd909998
esi	0
ebx	fd676a64
edx	80512bb7
ecx	c0000022
eax	fd6760d0
ebp	fd676a74
eip	fd8f2337
cs	8
efl	282
esp	fd6760a8
ss	10
dr0	
dr1	
dr2	
dr3	
dr6	
dr7	
di	
si	
bx	

```
ChildEBP RetAddr  Args to Child
fd6760a4 fd9217a5 80dacda8 fd6760d0 80510f25 Ntfs!NtfsExceptionFilter
fd6760b0 80510f25 fd6760d8 00000000 fd6760d8 Ntfs!NtfsFsdCreate+0x217
fd6760d8 80512ba3 fd6761b8 fd676a64 fd676208 nt!_except_handler3+0x4b
fd6760fc 80512b77 fd6761b8 fd676a64 fd676208 nt!ExecuteHandler2+0x26
fd6761a8 80512e5d fd6761b8 fd676208 c0000022 nt!ExecuteHandler+0x24
```

Ln 0, Col 0 | Sys 0:COM:Por | Proc 000:0 | Thrd 000:0

bcdedit /dbgsettings
bcdedit /copy {current}
bcdedit set debug on

windbg.exe -k usb2:targetname=USBString -b



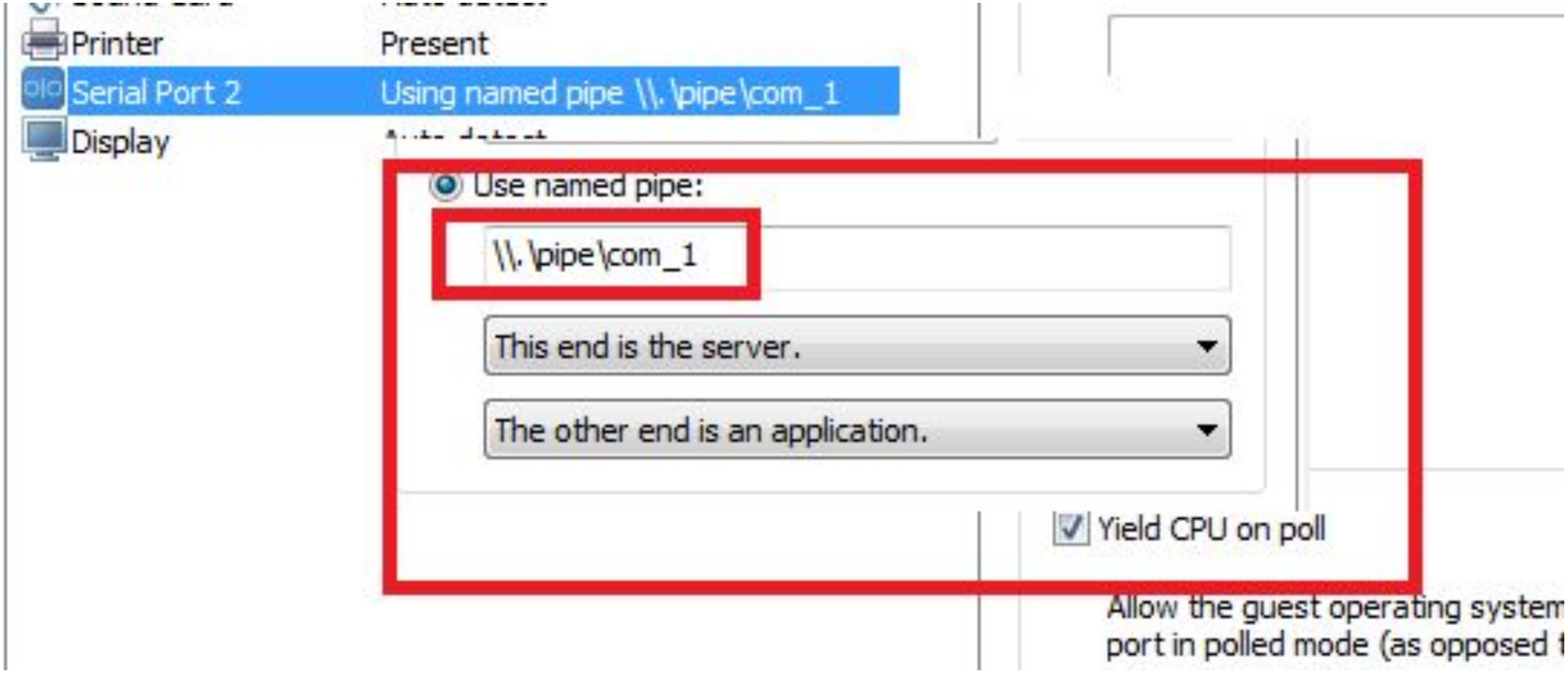
```
fd8f2333 ffc2            inc     edx
fd8f2335 0c00            or      al,0x0
Ntfs!NtfsExceptionFilter:
fd8f2337 55              push    ebp
fd8f2338 8bec            mov     ebp,esp
fd8f233a 51              push    ecx
fd8f233b 51              push    ecx
fd8f233c 803de2ae90fd00  cmp   byte ptr [Ntfs!NtfsTestFilter (fd90aee2)],
fd8f2343 53              push    ebx
fd8f2344 8b5d0c          mov     ebx,[ebp+0xc]
fd8f2347 8b03            mov     eax,[ebx]
fd8f2349 56              push    esi
fd8f234a 57              push    edi
fd8f234b 8b38            mov     edi,[eax]
fd8f234d 0f8596850000    jne     Ntfs!NtfsExceptionFilter+0x18 (fd8fa8e9)
fd8f2353 81ff060000c0    cmp     edi,0xc0000006
```

```
Reg   Value
gs    0
fs    30
es    23
ds    23
edi   fd909998
esi   0
ebx   fd676a64
edx   80512bb7
ecx   c0000022
eax   fd6760d0
ebp   fd676a74
eip   fd8f2337
cs    8
efl   282
esp   fd6760a8
ss    10
dr0   0
dr1   0
dr2   0
dr3   0
dr6   ff
dr7   40
di    99
si    0
bx    6a
```

```
ChildEBP RetAddr  Args to Child
fd6760a4 fd9217a5 80dacda8 fd6760d0 80510f25 Ntfs!NtfsExceptionFilter
fd6760b0 80510f25 fd6760d8 00000000 fd6760d8 Ntfs!NtfsFsdCreate+0x217
fd6760d8 80512ba3 fd6761b8 fd676a64 fd676208 nt!_except_handler3+0x4b
fd6760fc 80512b77 fd6761b8 fd676a64 fd676208 nt!ExecuteHandler2+0x26
fd6761a8 80512e5d fd6761b8 fd676208 c0000022 nt!ExecuteHandler+0x24
```

vmware™

windbg.exe -k com:pipe,port=\\.\pipe\com_1,resets=0,reconnect -b



Printer	Present
Serial Port 2	Using named pipe \\.\pipe\com_1
Display	

● Use named pipe:

\\.\pipe\com_1

This end is the server.

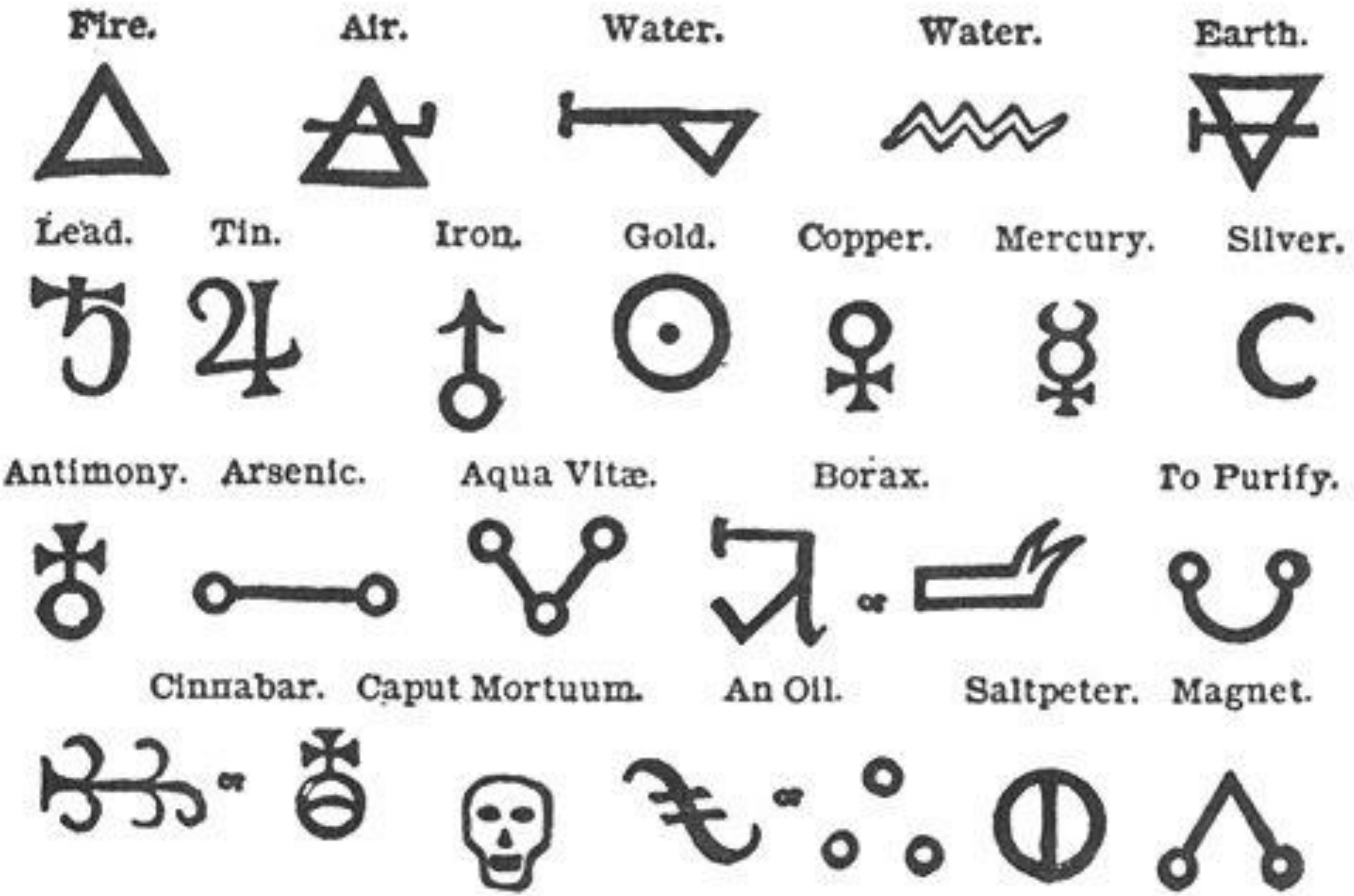
The other end is an application.

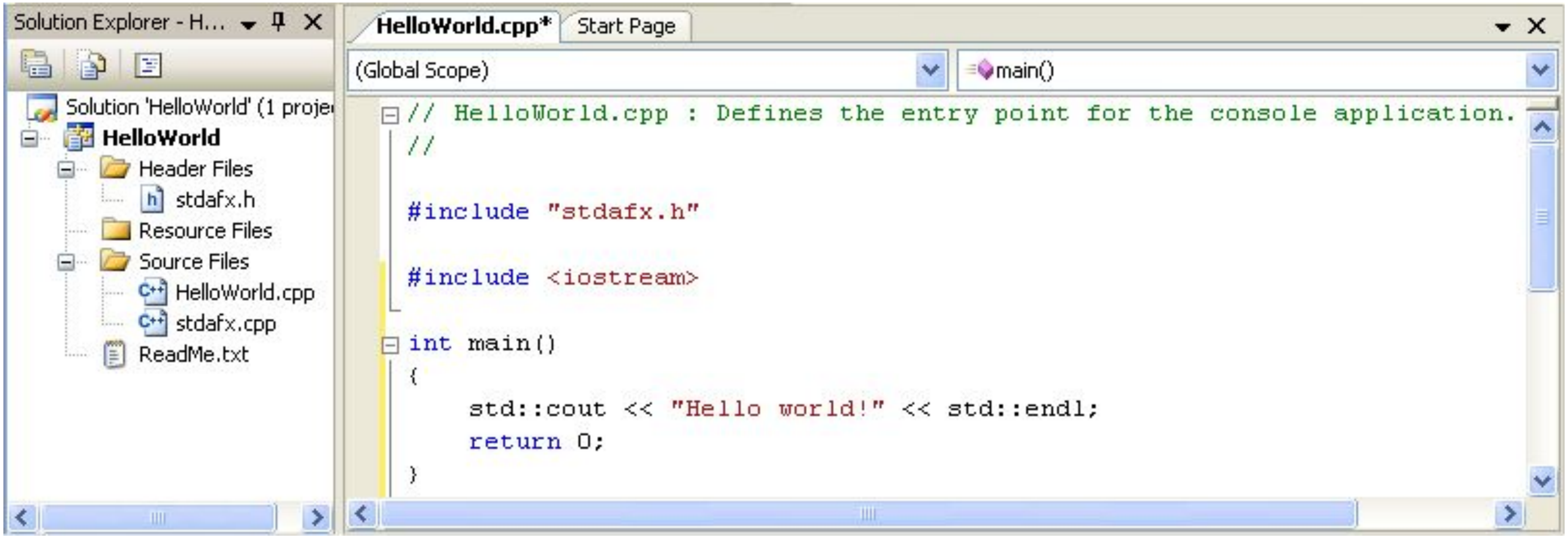
☑ Yield CPU on poll

Allow the guest operating system
port in polled mode (as opposed t

```
windbg.exe -k com:pipe,port=\\.\pipe\com_1,resets=0,reconnect -b
```

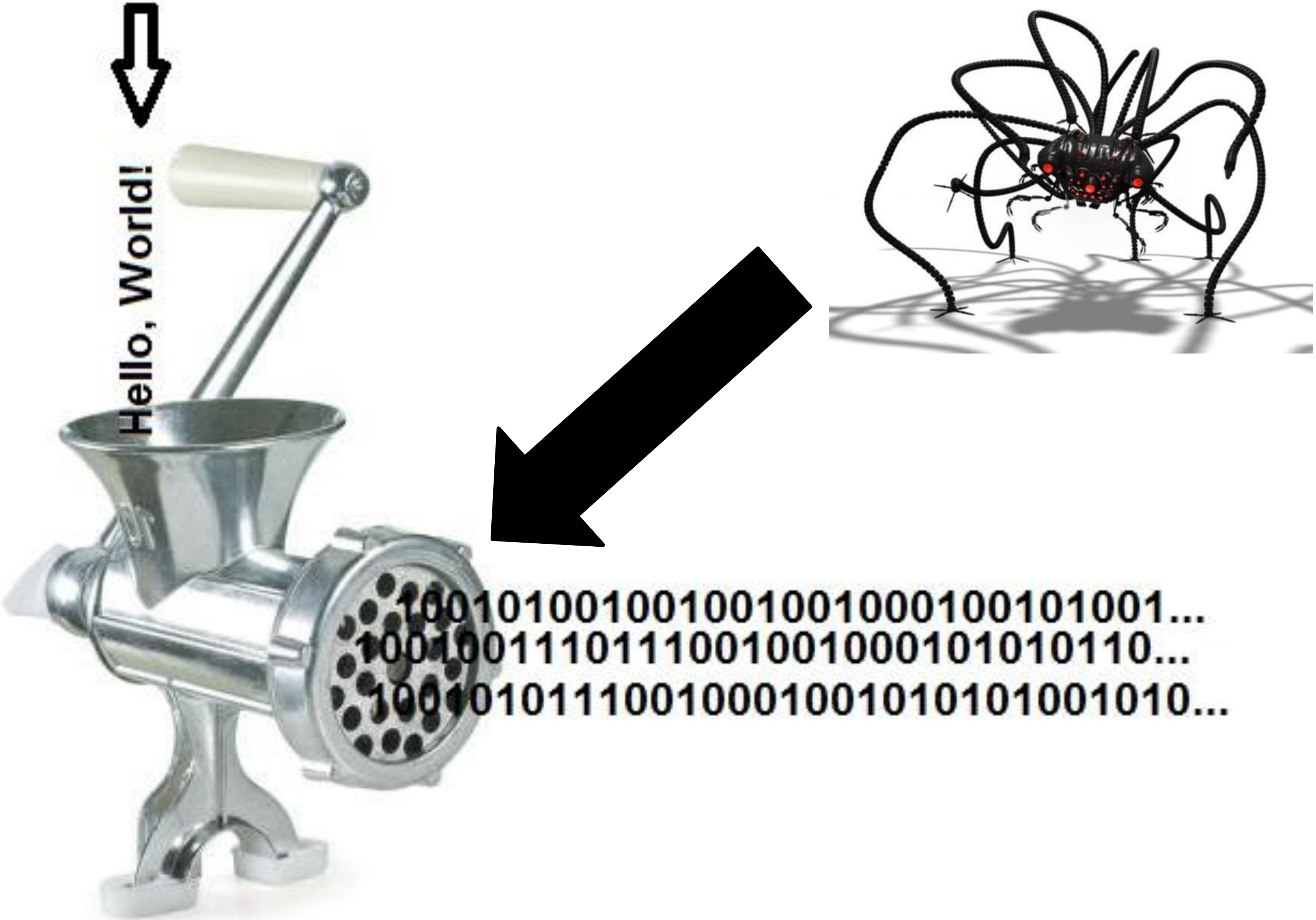
SYMBOLS OF THE ALCHEMISTS AND THEIR SIGNIFICATIONS.





```
// HelloWorld.cpp : Defines the entry point for the console application.
//

#include "stdafx.h"

#include <iostream>

int main()
{
    std::cout << "Hello world!" << std::endl;
    return 0;
}
```

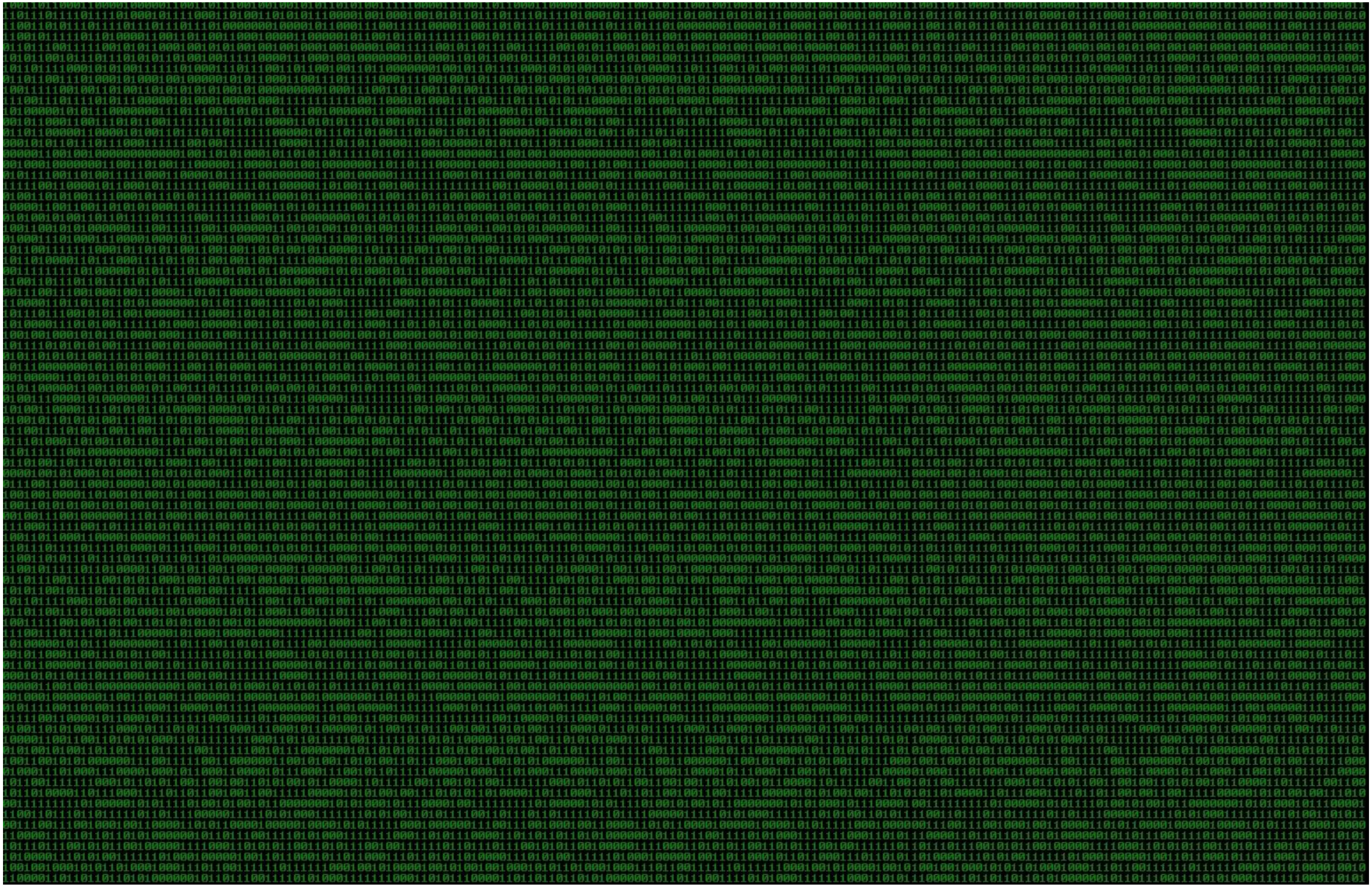
WELCOME TO THE REAL WORLD

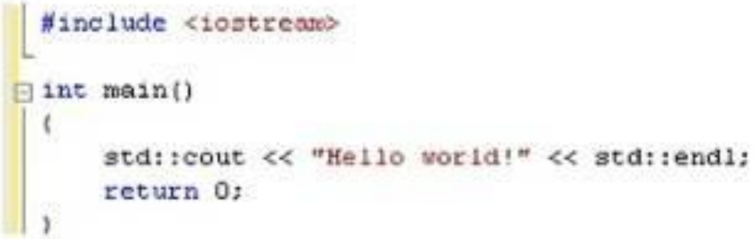


Hello, World!

100101001001001001000100101001...
1001001110111001001000101010110...
10010101110010001001010101001010...

Compiler/Linker

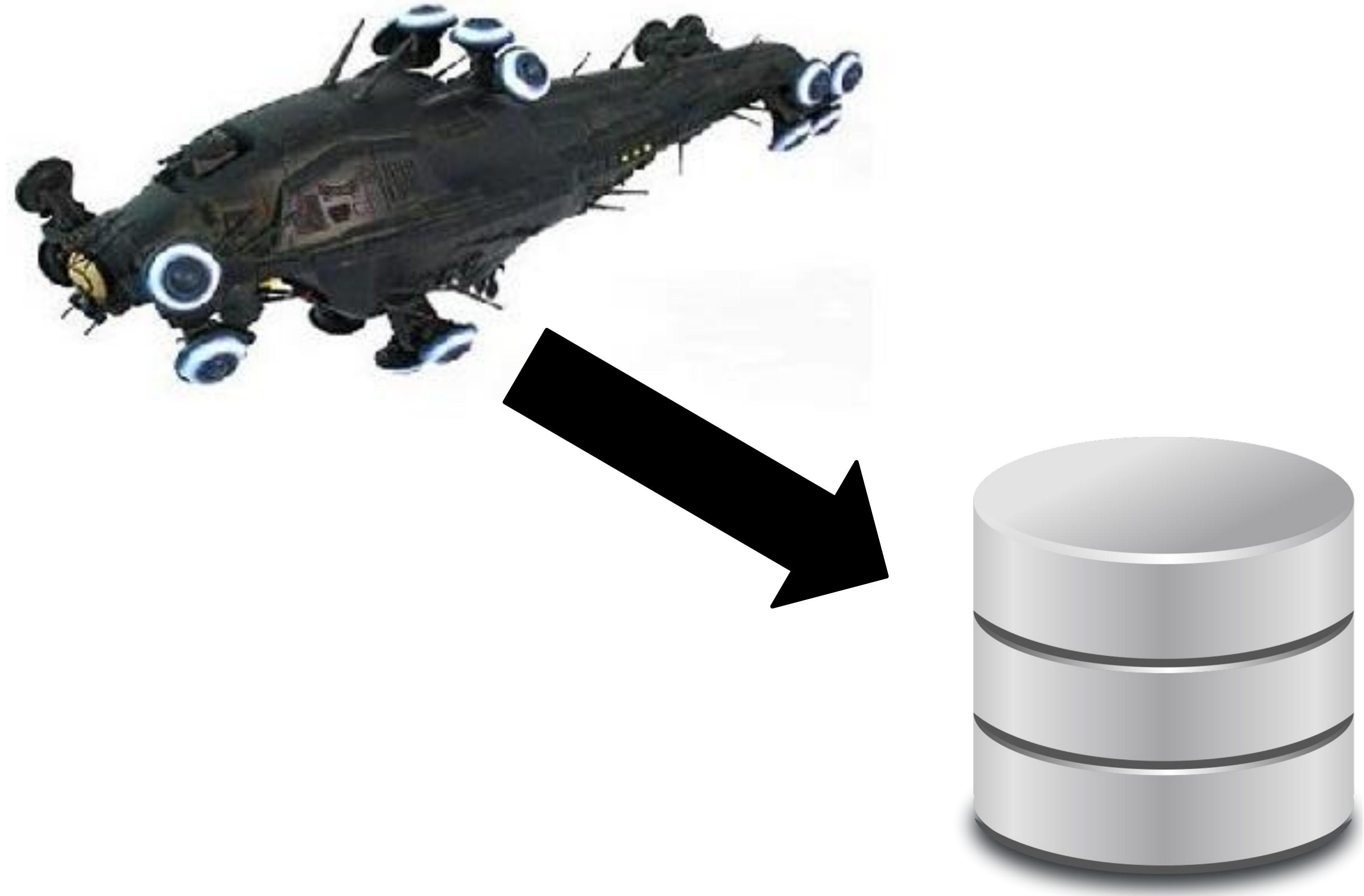




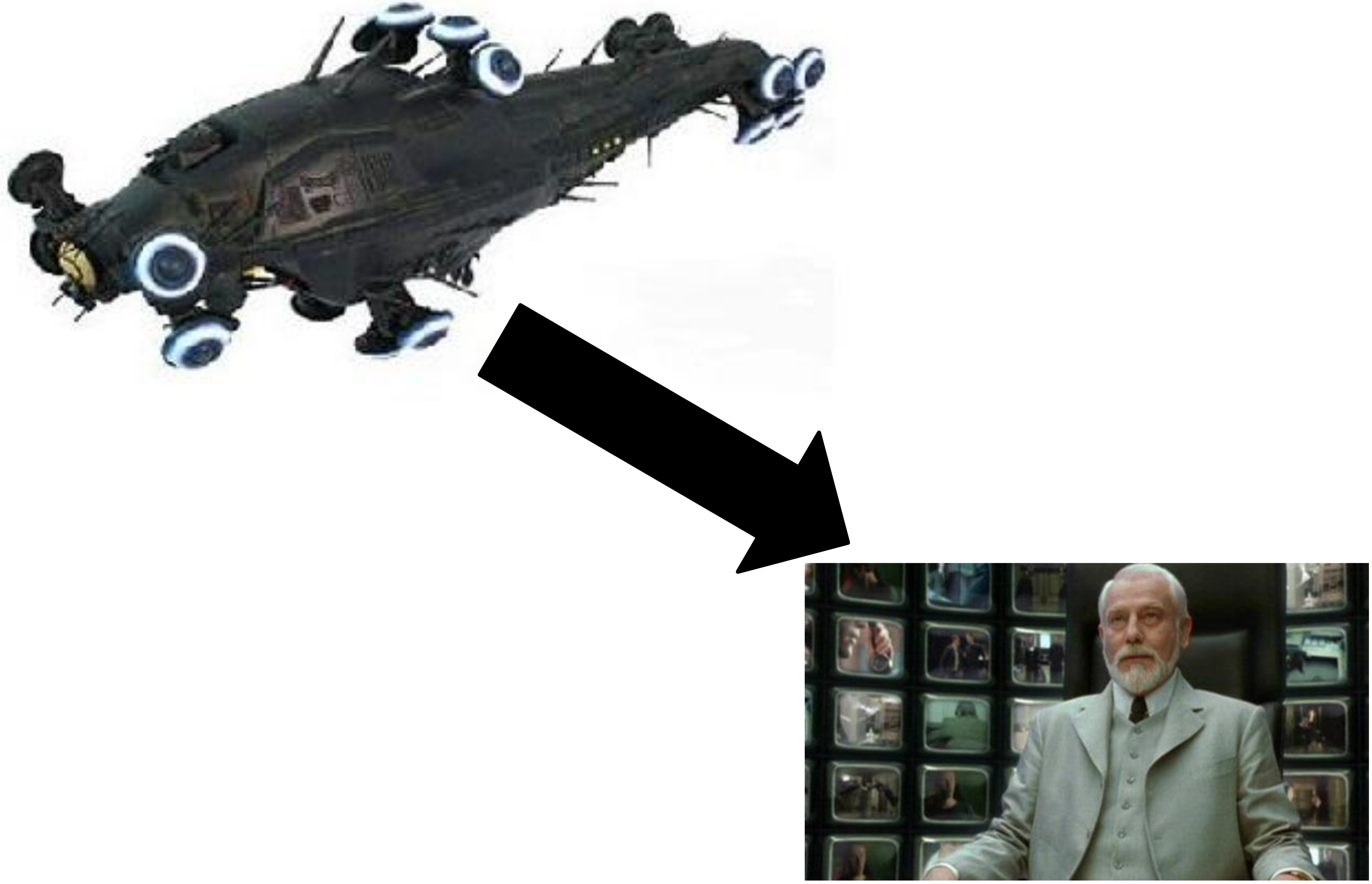
```
#include <iostream>

int main()
{
    std::cout << "Hello world!" << std::endl;
    return 0;
}
```

NABUCODEBUGGER

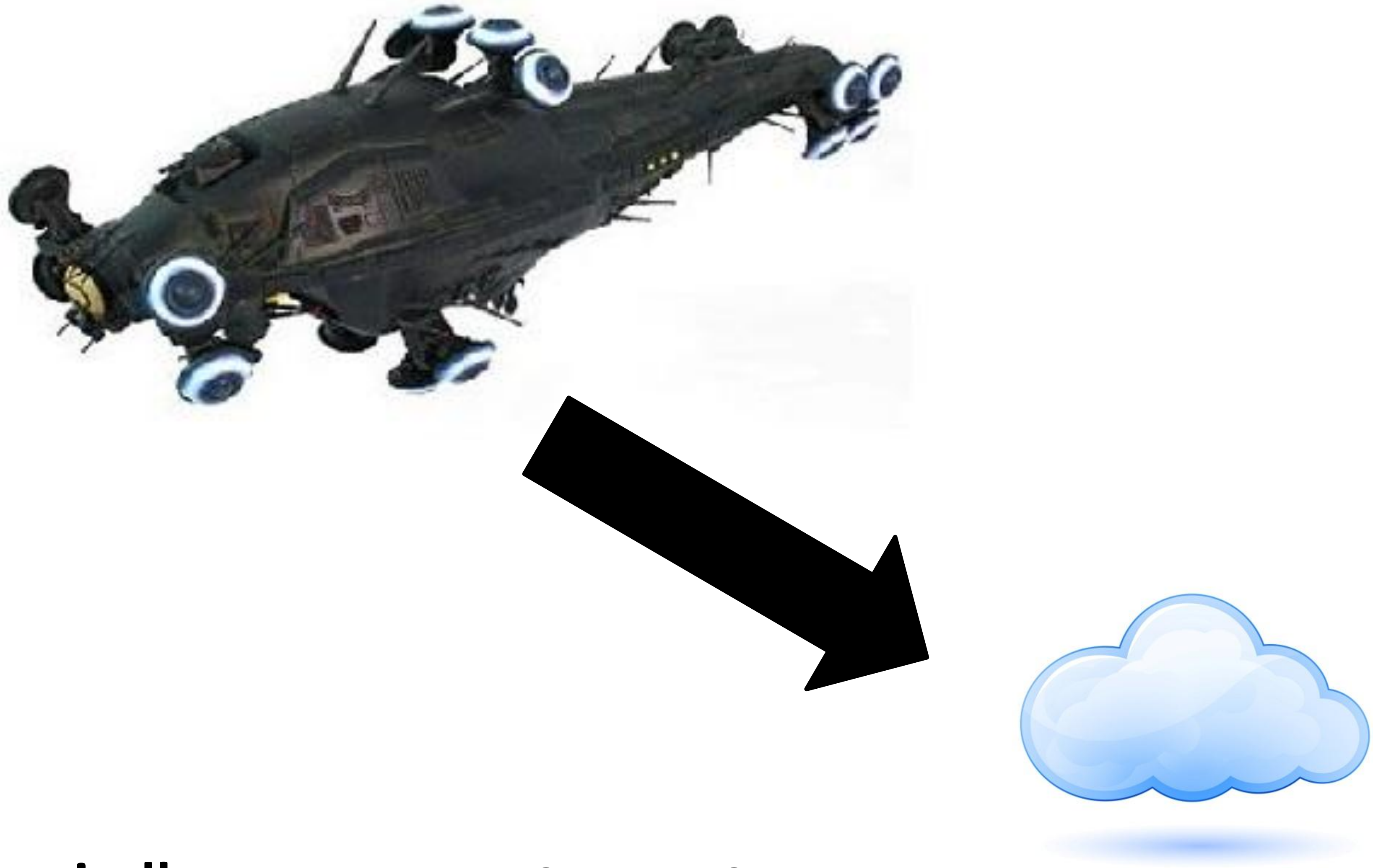
```
.symfix
.sympath
!sym noisy
.reload [/f] [/i] ModuleName.ext
lm[l]
```



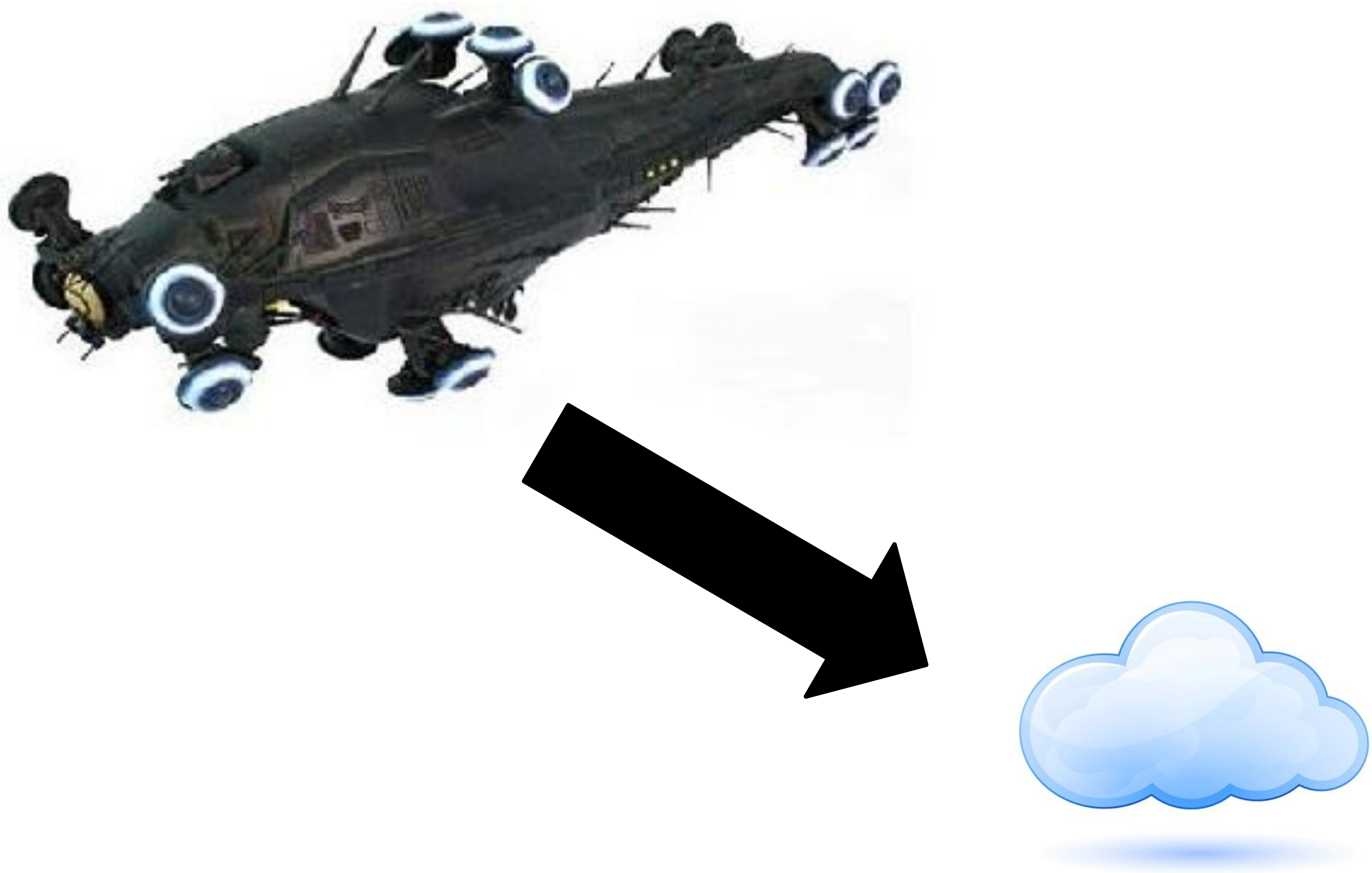
```
symstore.exe add /f Symbols.pdb /s <SymbolStore> /t “ProductName"
```



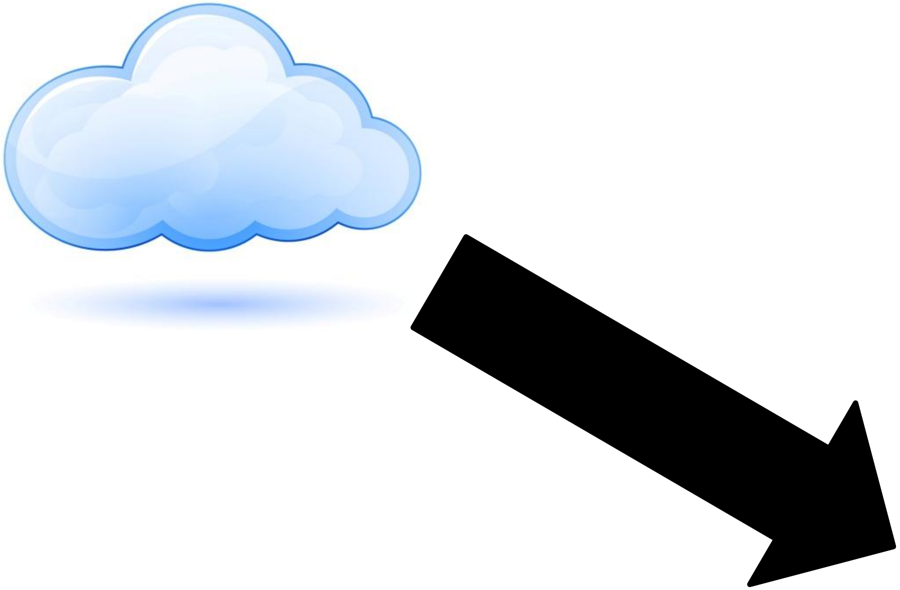
SRCSRV (SVN)



```
windbg.exe -server tcp:port=<n>
windbg.exe -remote tcp:server=<ip>,port=<n>
windbg.exe -remote tcp:server=<ip>,port=<n>
windbg.exe -remote tcp:server=<ip>,port=<n>
```

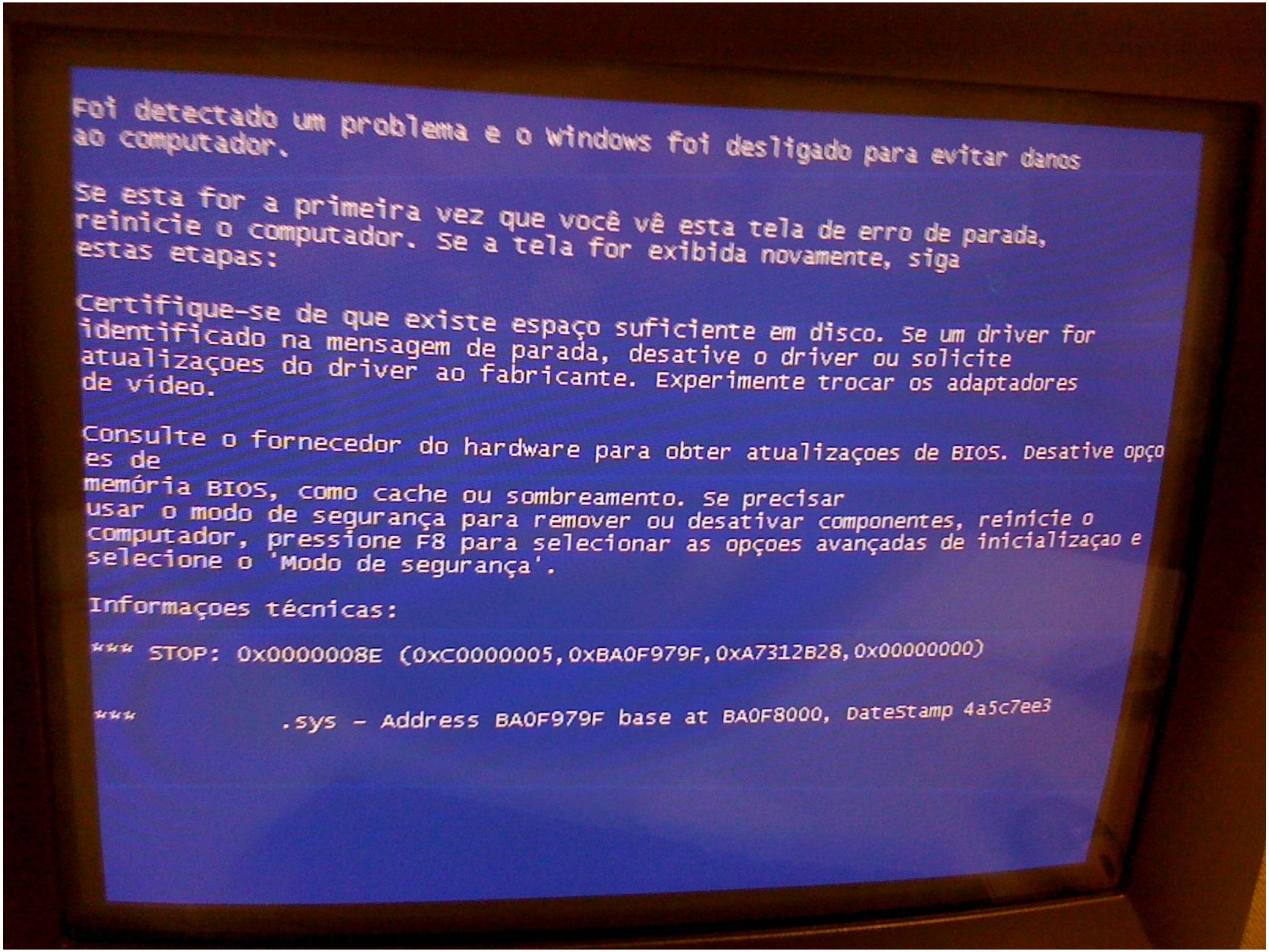


```
dbgsrv.exe -t tcp:port=<n>
windbg.exe -premote tcp:server=<ip>,port=<n>
```



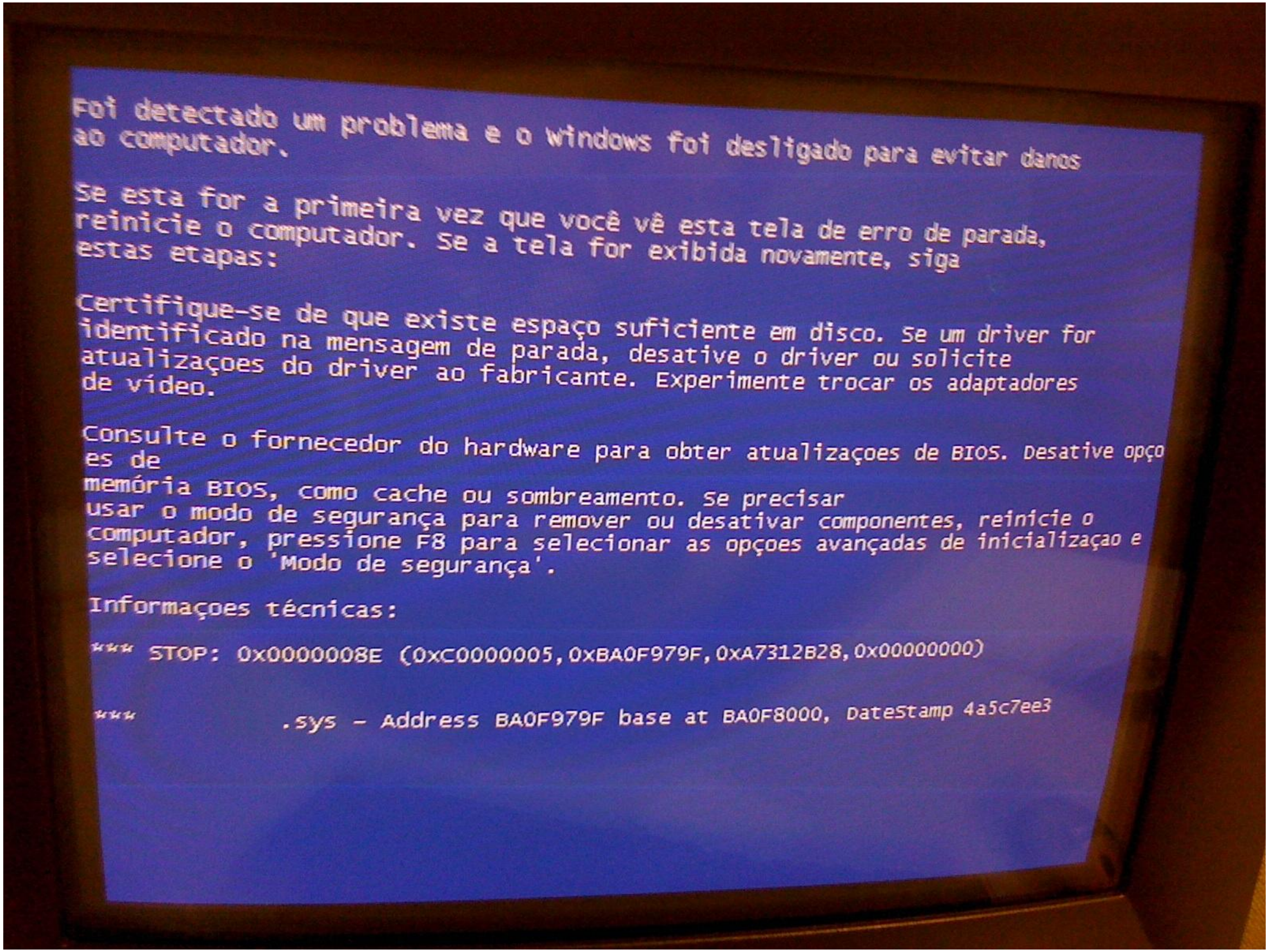
TCP Client => Server
TCP Server => Client
Serial (??????)
Named Pipe
SSL/SPIPE

(password, ipv6, ...)



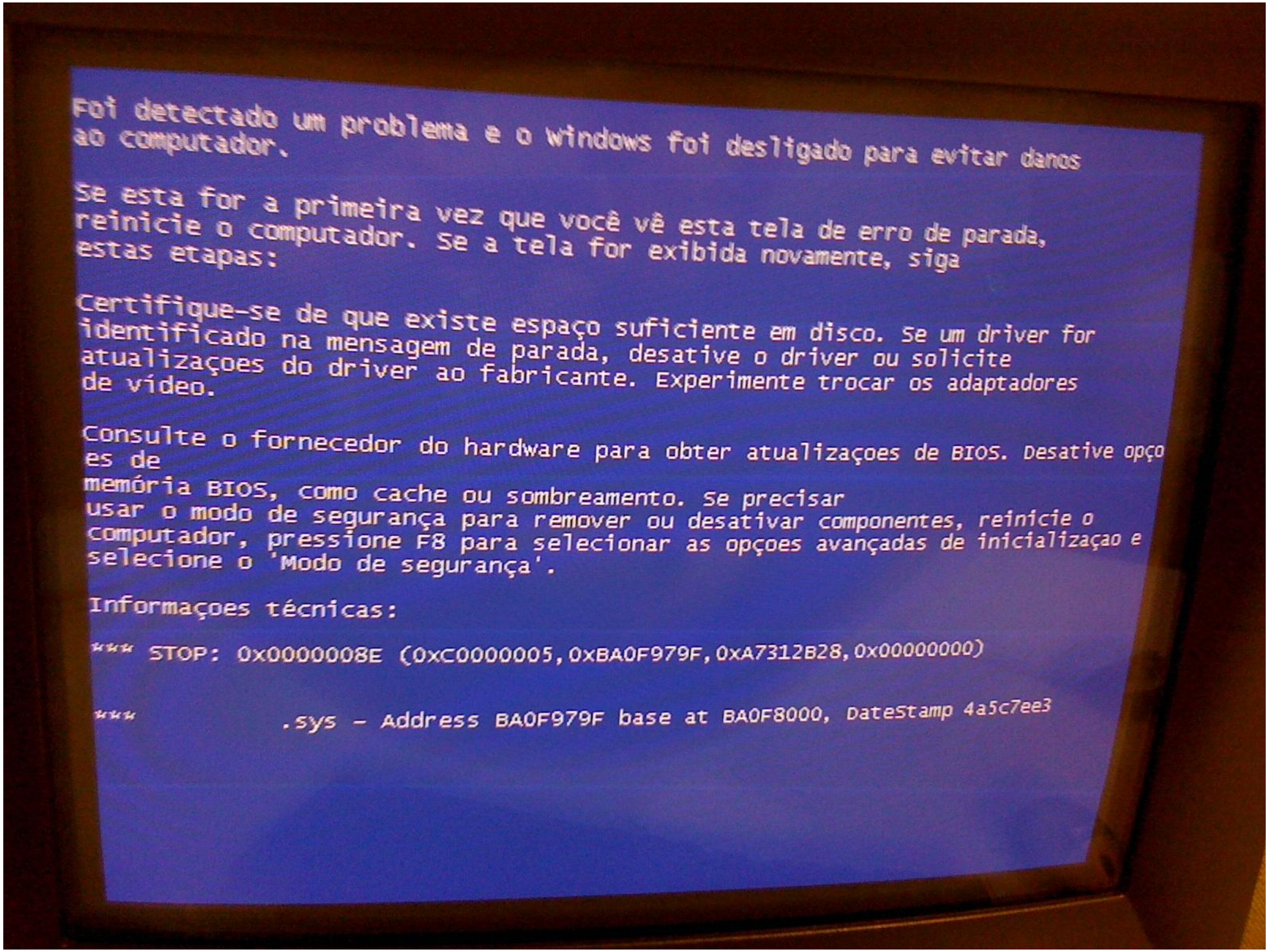
```
Foi detectado um problema e o Windows foi desligado para evitar danos
ao computador.

Se esta for a primeira vez que você vê esta tela de erro de parada,
reinicie o computador. Se a tela for exibida novamente, siga
estas etapas:

Certifique-se de que existe espaço suficiente em disco. Se um driver for
identificado na mensagem de parada, desative o driver ou solicite
atualizaçoes do driver ao fabricante. Experimente trocar os adaptadores
de vídeo.

Consulte o fornecedor do hardware para obter atualizaçoes de BIOS. Desative opço
es de
memória BIOS, como cache ou sombreamento. Se precisar
usar o modo de segurança para remover ou desativar componentes, reinicie o
computador, pressione F8 para selecionar as opçoes avançadas de inicializaçao e
selecione o 'Modo de segurança'.

Informaçoes técnicas:

*** STOP: 0x0000008E (0xC0000005,0xBA0F979F,0xA7312B28,0x00000000)

***          .sys - Address BA0F979F base at BA0F8000, DateStamp 4a5c7ee3
```

selfie



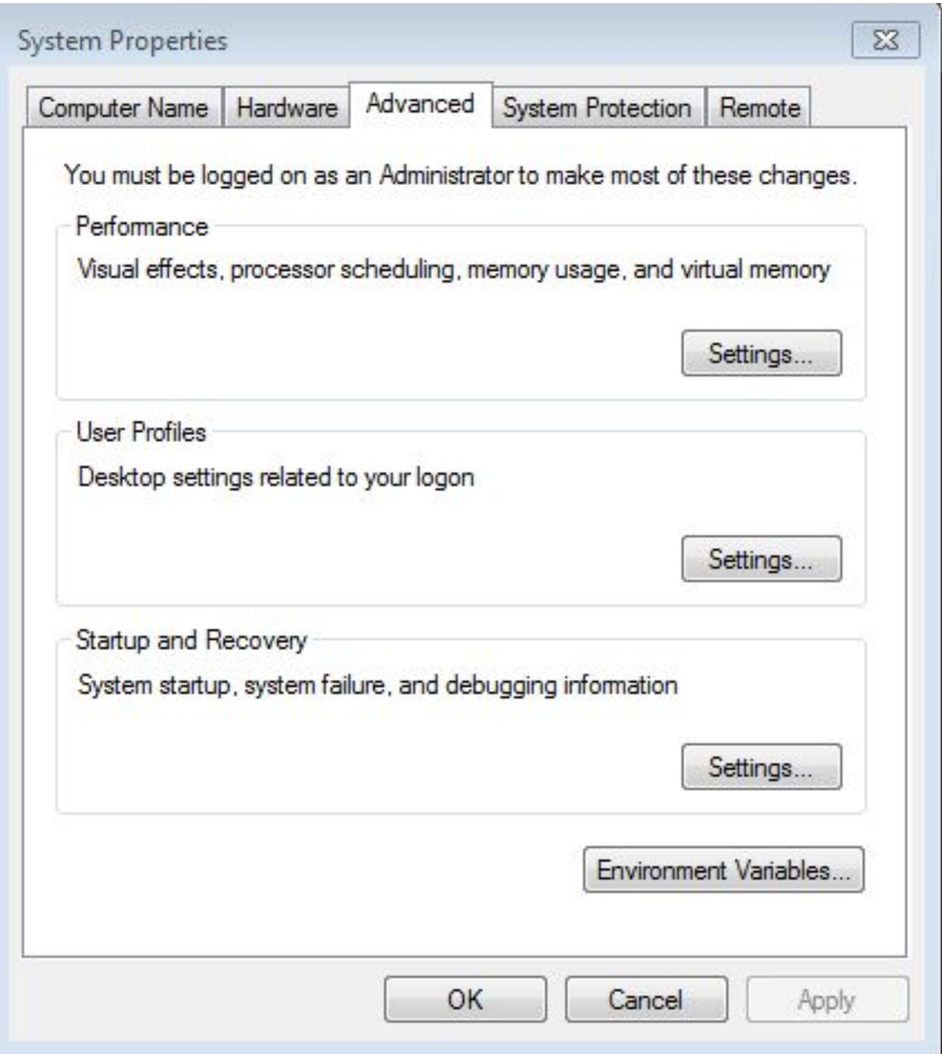
```
Foi detectado um problema e o windows foi desligado para evitar danos
ao computador.

Se esta for a primeira vez que você vê esta tela de erro de parada,
reinicie o computador. Se a tela for exibida novamente, siga
estas etapas:

Certifique-se de que existe espaço suficiente em disco. Se um driver for
identificado na mensagem de parada, desative o driver ou solicite
atualizaçoes do driver ao fabricante. Experimente trocar os adaptadores
de vídeo.

Consulte o fornecedor do hardware para obter atualizaçoes de BIOS. Desative opço
es de
memória BIOS, como cache ou sombreamento. Se precisar
usar o modo de segurança para remover ou desativar componentes, reinicie o
computador, pressione F8 para selecionar as opçoes avançadas de inicializaçao e
selecione o 'Modo de segurança'.

Informaçoes técnicas:

*** STOP: 0x0000008E (0xC0000005,0xBA0F979F,0xA7312B28,0x00000000)

***          .sys - Address BA0F979F base at BA0F8000, DateStamp 4a5c7ee3
```

.dump /ma <dump-file.dmp>



```
Foi detectado um problema e o windows foi desligado para evitar danos
ao computador.

Se esta for a primeira vez que você vê esta tela de erro de parada,
reinicie o computador. Se a tela for exibida novamente, siga
estas etapas:

Certifique-se de que existe espaço suficiente em disco. Se um driver for
identificado na mensagem de parada, desative o driver ou solicite
atualizaçoes do driver ao fabricante. Experimente trocar os adaptadores
de vídeo.

Consulte o fornecedor do hardware para obter atualizaçoes de BIOS. Desative opço
es de
memória BIOS, como cache ou sombreamento. Se precisar
usar o modo de segurança para remover ou desativar componentes, reinicie o
computador, pressione F8 para selecionar as opçoes avançadas de inicializaçao e
selecione o 'Modo de segurança'.

Informaçoes técnicas:

*** STOP: 0x0000008E (0xC0000005,0xBA0F979F,0xA7312B28,0x00000000)


***          .sys - Address BA0F979F base at BA0F8000, DateStamp 4a5c7ee3
```

Adplus -Crash -pmn <proc-name>



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

Settings...

User Profiles

Desktop settings related to your logon

Settings...

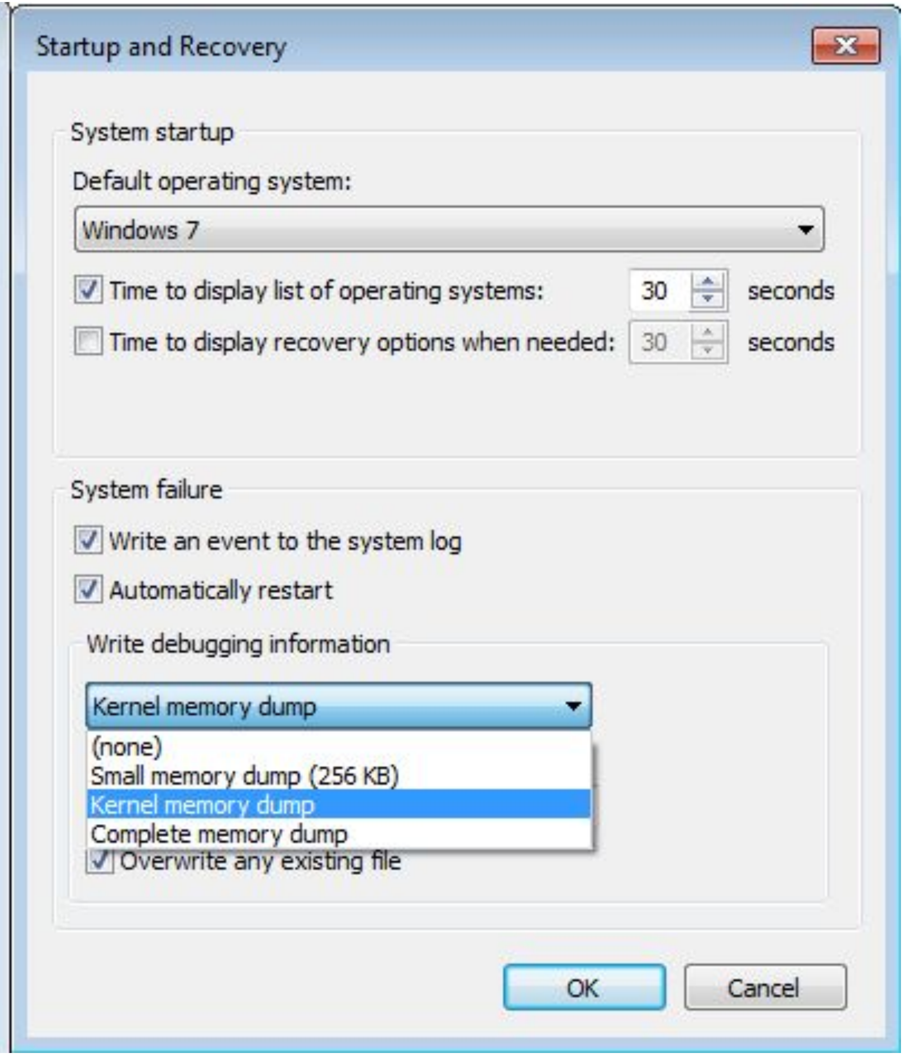
Startup and Recovery

System startup, system failure, and debugging information

Settings...

Environment Variables...

OK Cancel Apply



Startup and Recovery

System startup

Default operating system:

Windows 7

☑ Time to display list of operating systems: 30 seconds

☐ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Kernel memory dump

- (none)
- Small memory dump (256 KB)
- Kernel memory dump
- Complete memory dump

☑ Overwrite any existing file

OK Cancel

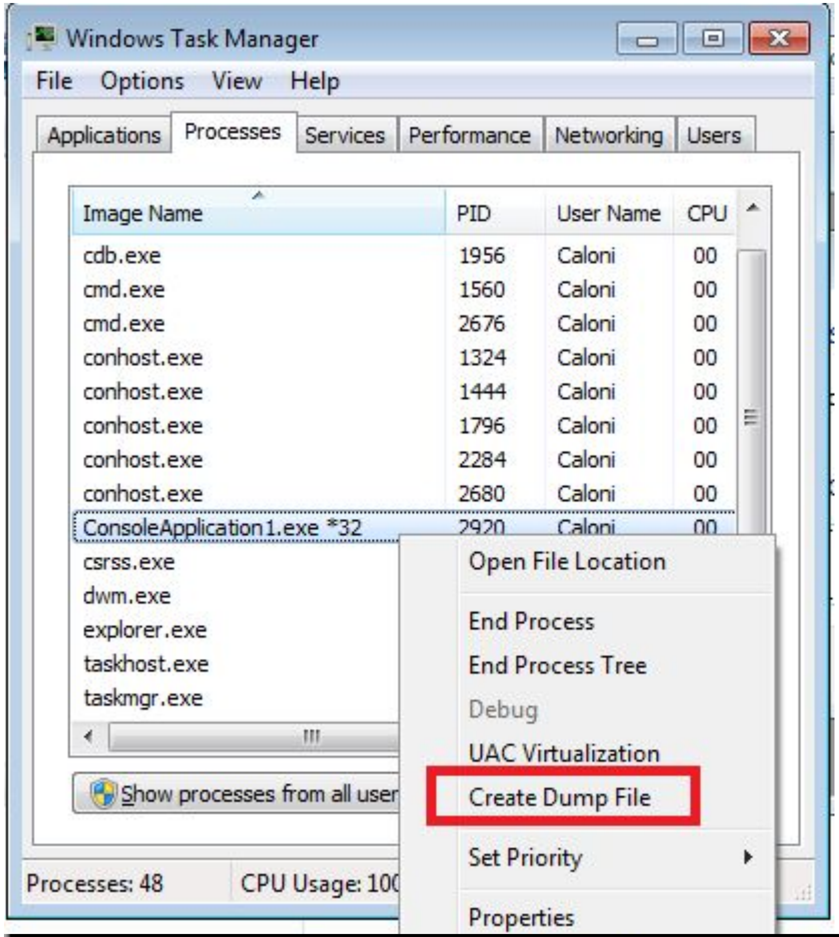
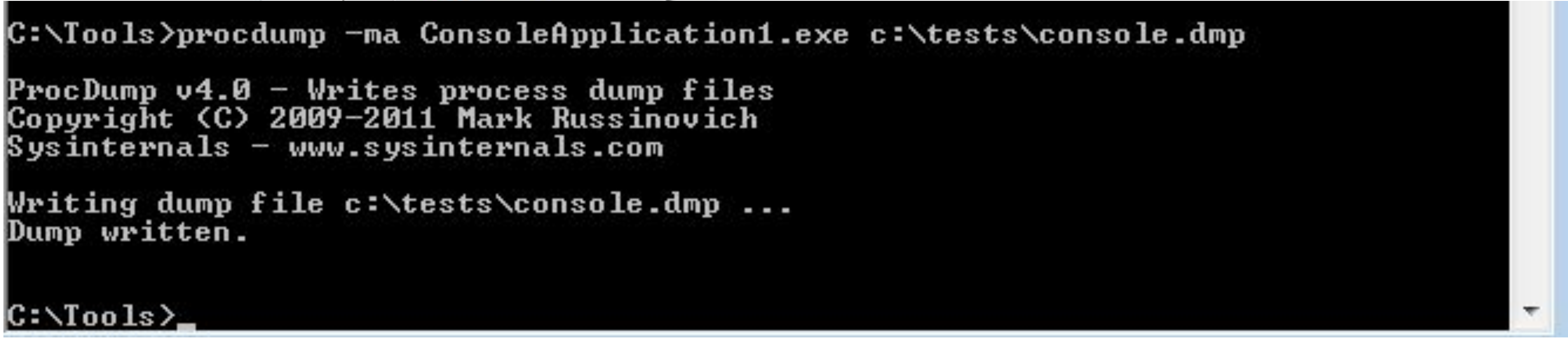


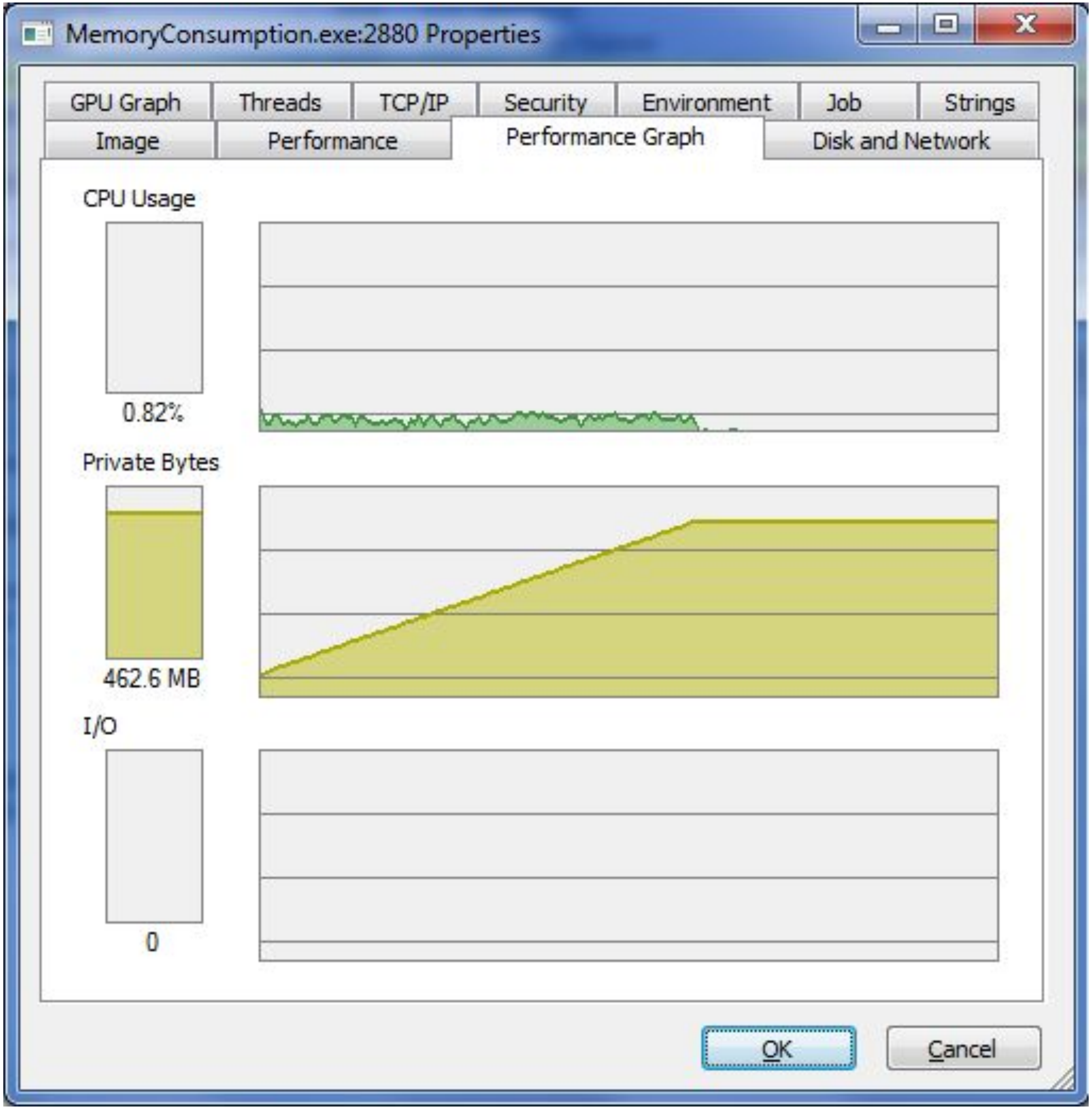
Image Name	PID	User Name	CPU
cdb.exe	1956	Caloni	00
cmd.exe	1560	Caloni	00
cmd.exe	2676	Caloni	00
conhost.exe	1324	Caloni	00
conhost.exe	1444	Caloni	00
conhost.exe	1796	Caloni	00
conhost.exe	2284	Caloni	00
conhost.exe	2680	Caloni	00
ConsoleApplication1.exe *32	2920	Caloni	00
csrss.exe			
dwm.exe			
explorer.exe			
taskhost.exe			
taskmgr.exe			

Processes: 48   CPU Usage: 10(



```
C:\Tools>procdump -ma ConsoleApplication1.exe c:\tests\console.dmp

ProcDump v4.0 - Writes process dump files
Copyright (C) 2009-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

Writing dump file c:\tests\console.dmp ...
Dump written.


C:\Tools>_
```

```
!analyze -v
!analyze -v
!analyze -v
!analyze -v
!analyze -v
!analyze -v
!analyze -v
!analyze -v
```


MemoryConsumption.exe:2880 Properties
GPU Graph
Threads
TCP/IP
Security
Environment
Job
Strings
Image
Performance
Performance Graph
Disk and Network
CPU Usage
0.82%
Private Bytes
462.6 MB
I/O
0
OK
Cancel

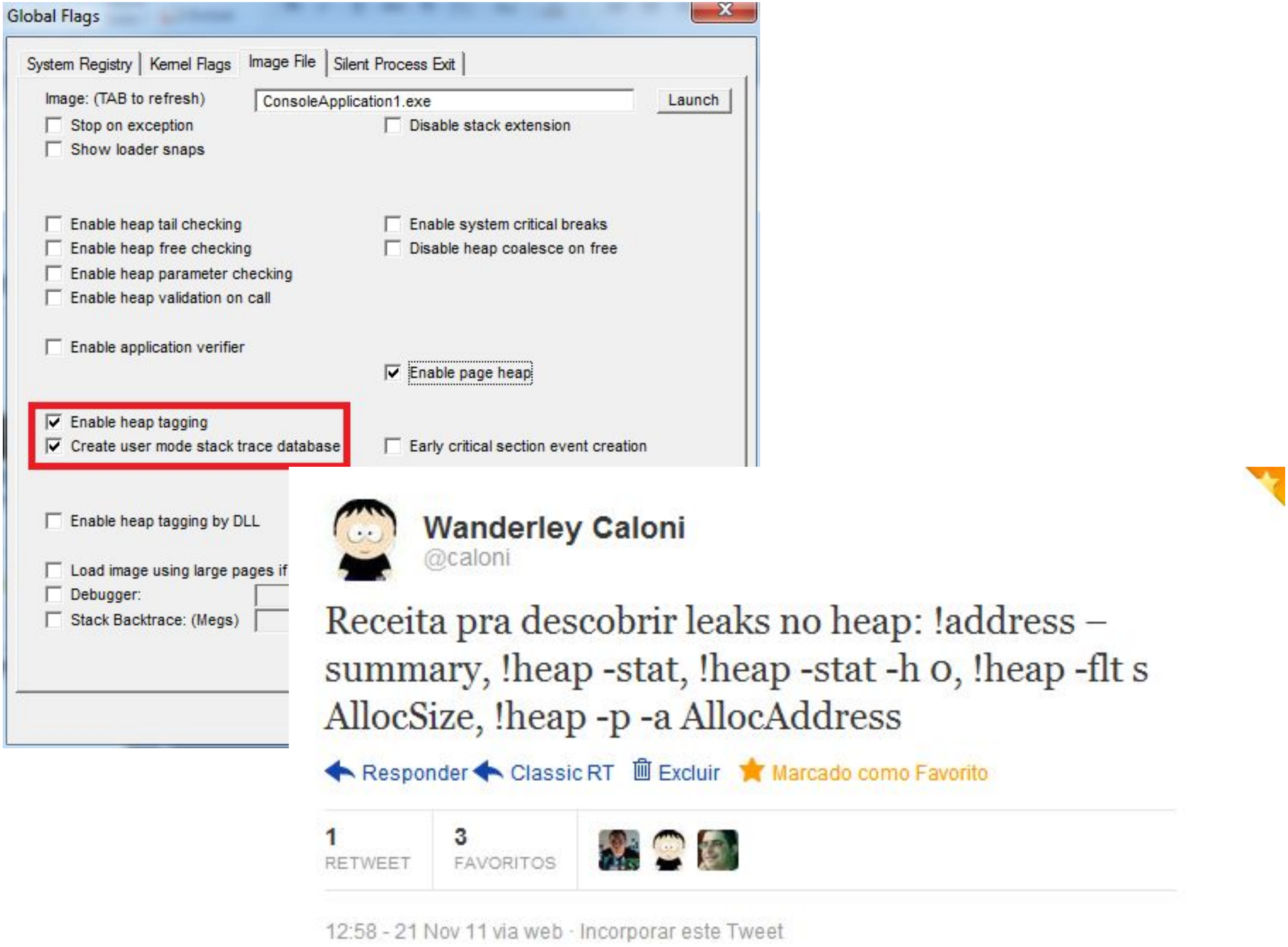


Image: (TAB to refresh) ConsoleApplication1.exe

□ Stop on exception
□ Show loader snaps
□ Disable stack extension

□ Enable heap tail checking
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call
□ Enable system critical breaks
□ Disable heap coalesce on free

□ Enable application verifier

☑ Enable page heap

☑ Enable heap tagging
☑ Create user mode stack trace database
□ Early critical section event creation

□ Enable heap tagging by DLL

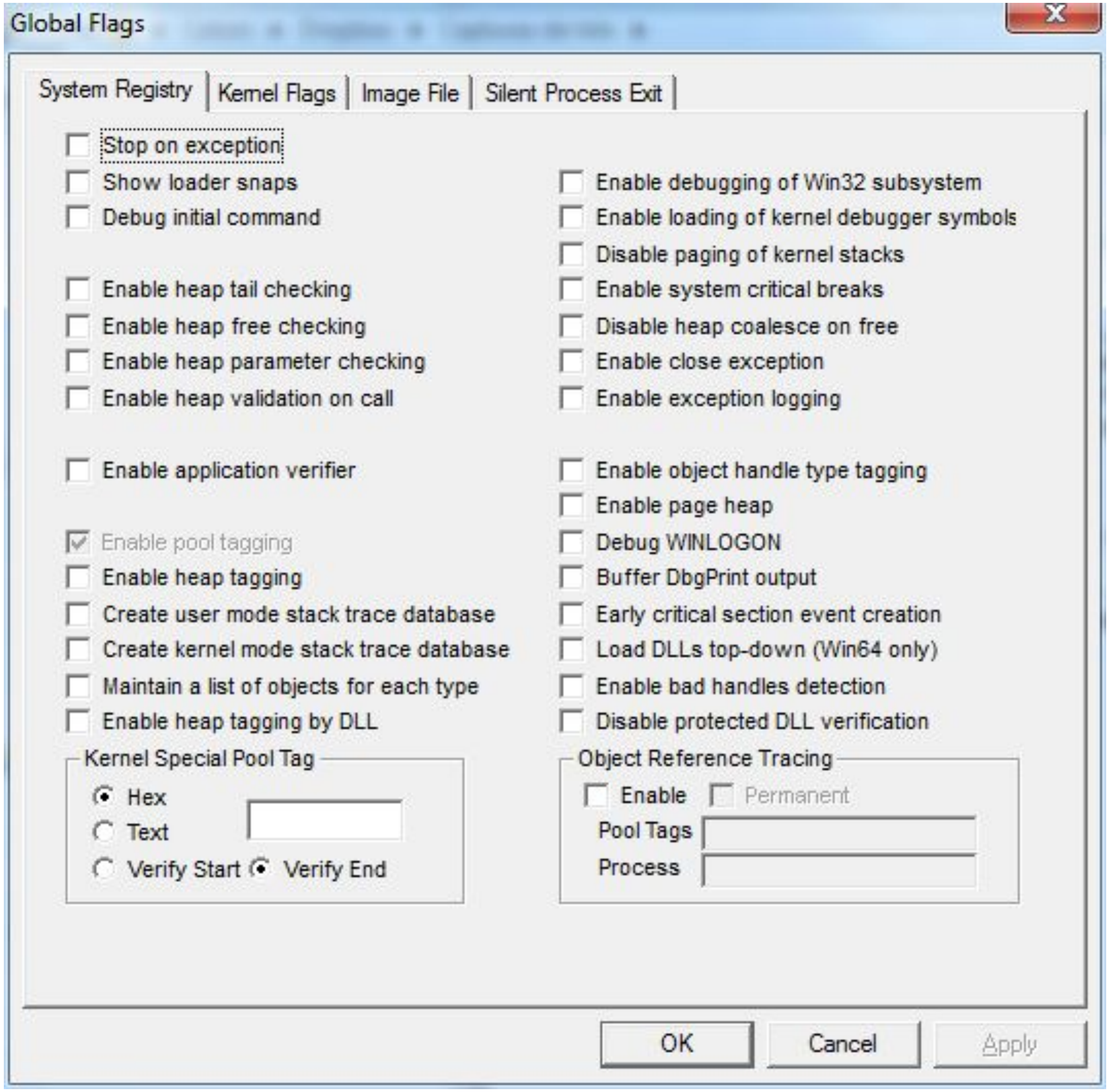
□ Load image using large pages if
□ Debugger:
□ Stack Backtrace: (Megs)

Wanderley Caloni
@caloni

Receita pra descobrir leaks no heap: !address –summary, !heap -stat, !heap -stat -h 0, !heap -flt s AllocSize, !heap -p -a AllocAddress

1 RETWEET 3 FAVORITOS

12:58 - 21 Nov 11 via web · Incorporar este Tweet



□ Stop on exception
□ Show loader snaps
□ Debug initial command

□ Enable heap tail checking
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call

□ Enable application verifier

☑ Enable pool tagging
□ Enable heap tagging
□ Create user mode stack trace database
□ Create kernel mode stack trace database
□ Maintain a list of objects for each type
□ Enable heap tagging by DLL

□ Enable debugging of Win32 subsystem
□ Enable loading of kernel debugger symbols
□ Disable paging of kernel stacks
□ Enable system critical breaks
□ Disable heap coalesce on free
□ Enable close exception
□ Enable exception logging

□ Enable object handle type tagging
□ Enable page heap
□ Debug WINLOGON
□ Buffer DbgPrint output
□ Early critical section event creation
□ Load DLLs top-down (Win64 only)
□ Enable bad handles detection
□ Disable protected DLL verification

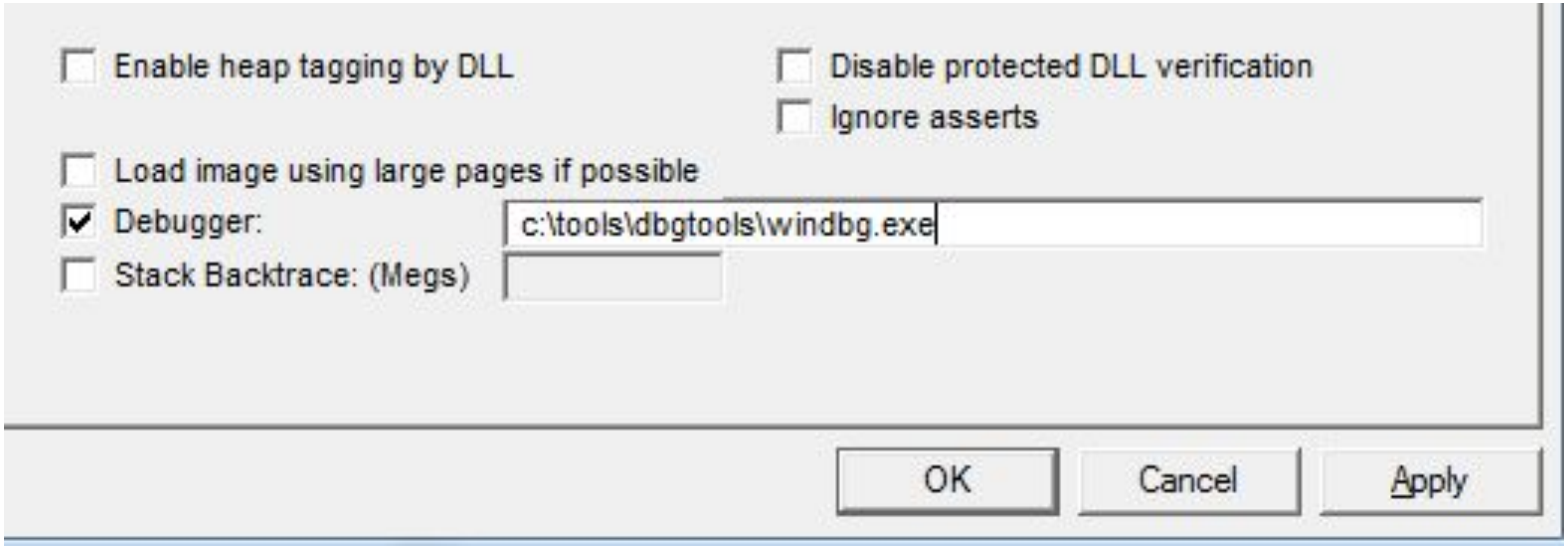
Kernel Special Pool Tag

● Hex
○ Text
○ Verify Start ● Verify End

Object Reference Tracing

□ Enable □ Permanent
Pool Tags
Process

GLOBAL FLAGS



□ Enable heap tagging by DLL

□ Disable protected DLL verification

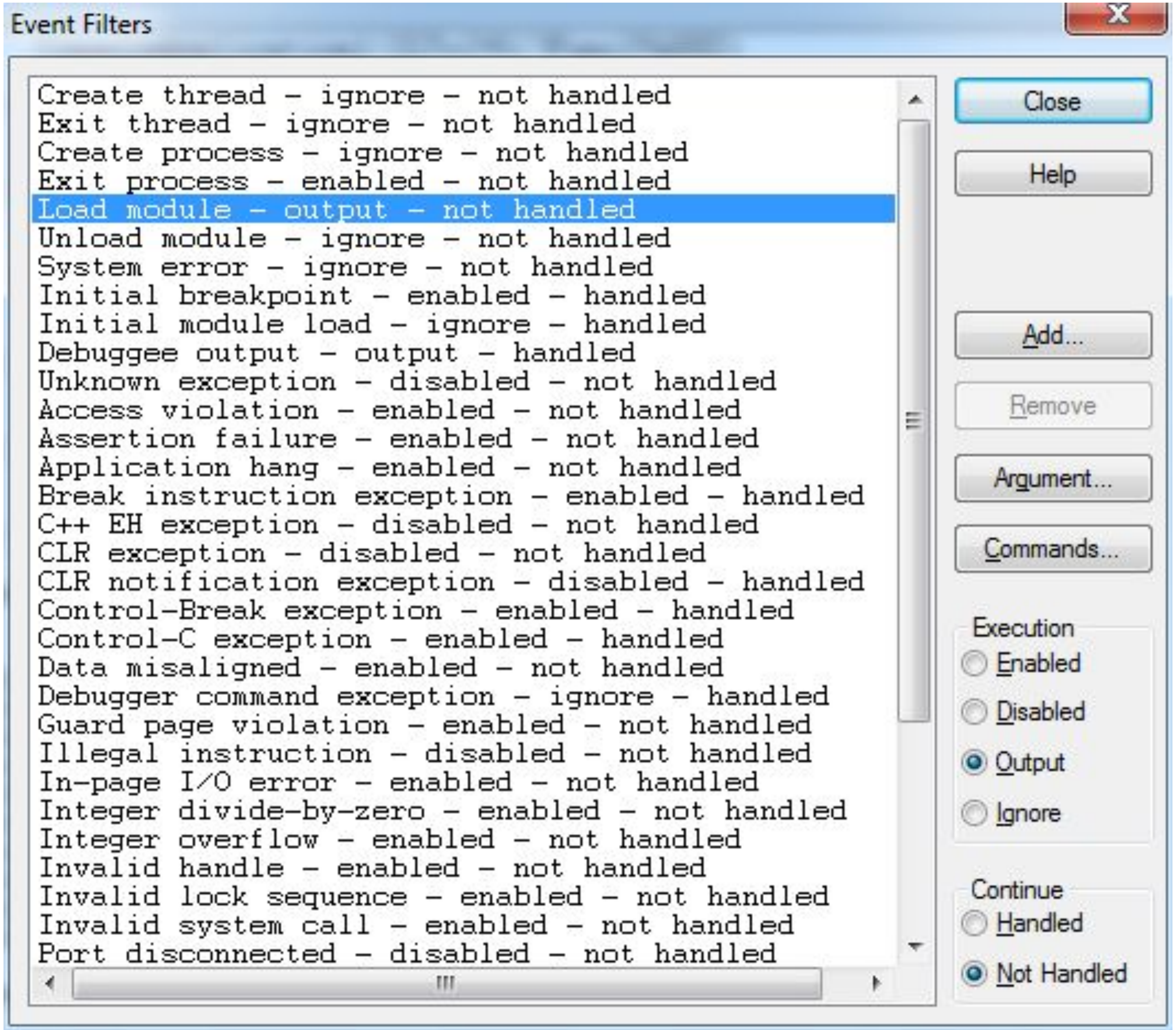
□ Ignore asserts

□ Load image using large pages if possible

☑ Debugger: c:\tools\dbgtools\windbg.exe

□ Stack Backtrace: (Megs)

GLOBAL FLAGS



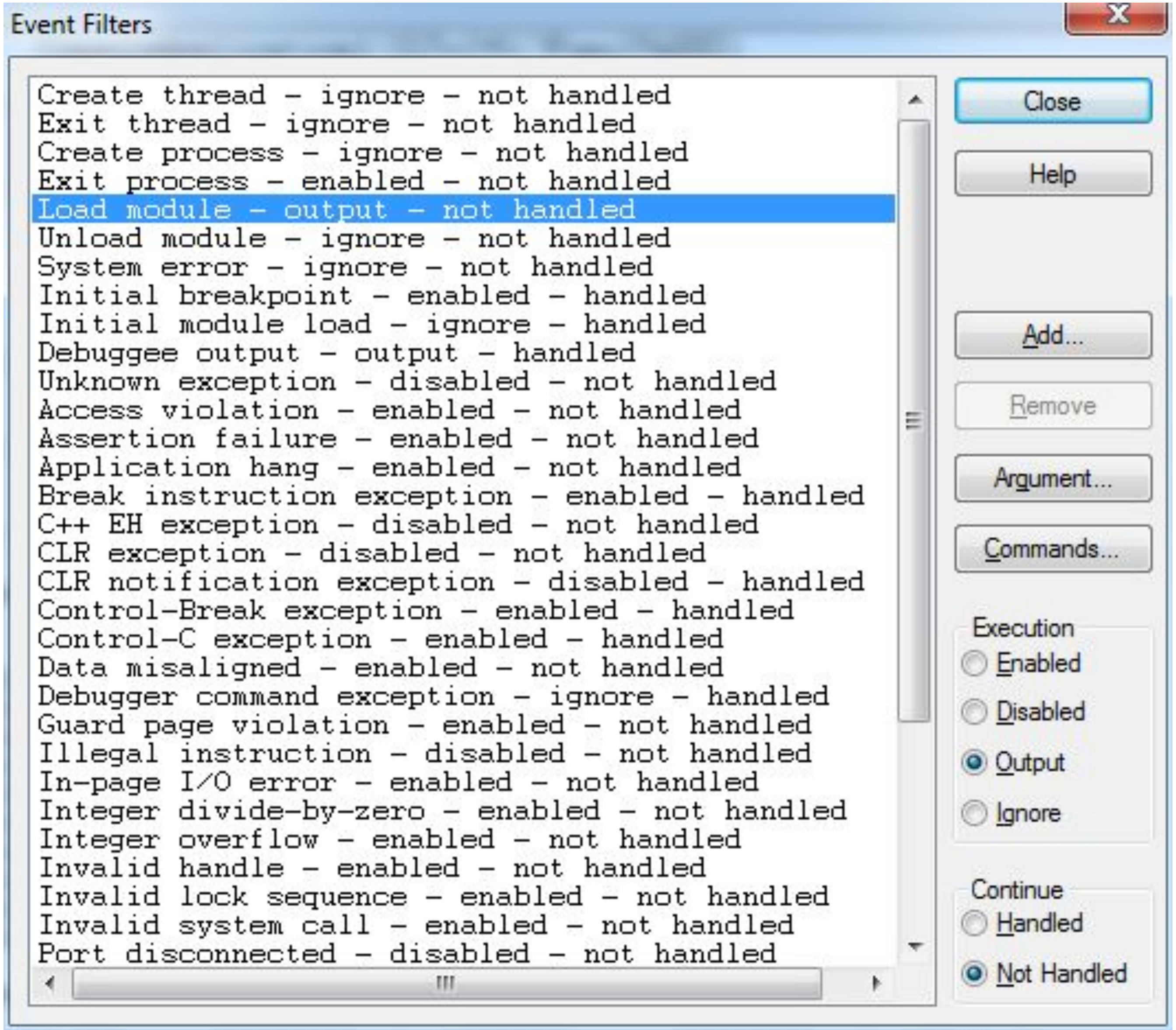
Event Filters

```
Create thread - ignore - not handled
Exit thread - ignore - not handled
Create process - ignore - not handled
Exit process - enabled - not handled
Load module - output - not handled
Unload module - ignore - not handled
System error - ignore - not handled
Initial breakpoint - enabled - handled
Initial module load - ignore - handled
Debuggee output - output - handled
Unknown exception - disabled - not handled
Access violation - enabled - not handled
Assertion failure - enabled - not handled
Application hang - enabled - not handled
Break instruction exception - enabled - handled
C++ EH exception - disabled - not handled
CLR exception - disabled - not handled
CLR notification exception - disabled - handled
Control-Break exception - enabled - handled
Control-C exception - enabled - handled
Data misaligned - enabled - not handled
Debugger command exception - ignore - handled
Guard page violation - enabled - not handled
Illegal instruction - disabled - not handled
In-page I/O error - enabled - not handled
Integer divide-by-zero - enabled - not handled
Integer overflow - enabled - not handled
Invalid handle - enabled - not handled
Invalid lock sequence - enabled - not handled
Invalid system call - enabled - not handled
Port disconnected - disabled - not handled
```

Execution
○ Enabled
○ Disabled
● Output
○ Ignore

Continue
○ Handled
● Not Handled

SXE, SXD, SXN, SXI

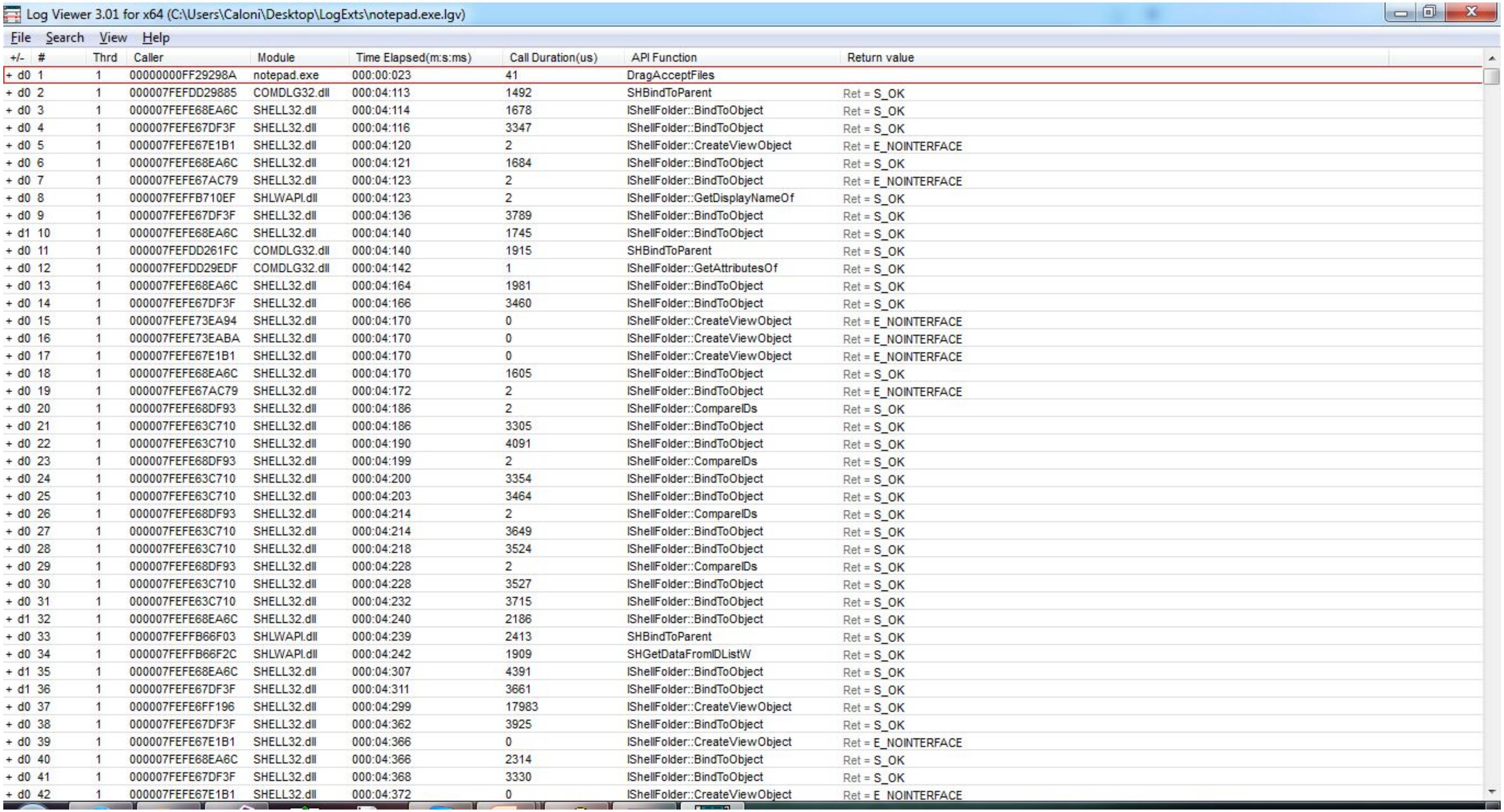


```
Create thread - ignore - not handled
Exit thread - ignore - not handled
Create process - ignore - not handled
Exit process - enabled - not handled
Load module - output - not handled
Unload module - ignore - not handled
System error - ignore - not handled
Initial breakpoint - enabled - handled
Initial module load - ignore - handled
Debuggee output - output - handled
Unknown exception - disabled - not handled
Access violation - enabled - not handled
Assertion failure - enabled - not handled
Application hang - enabled - not handled
Break instruction exception - enabled - handled
C++ EH exception - disabled - not handled
CLR exception - disabled - not handled
CLR notification exception - disabled - handled
Control-Break exception - enabled - handled
Control-C exception - enabled - handled
Data misaligned - enabled - not handled
Debugger command exception - ignore - handled
Guard page violation - enabled - not handled
Illegal instruction - disabled - not handled
In-page I/O error - enabled - not handled
Integer divide-by-zero - enabled - not handled
Integer overflow - enabled - not handled
Invalid handle - enabled - not handled
Invalid lock sequence - enabled - not handled
Invalid system call - enabled - not handled
Port disconnected - disabled - not handled
```

Execution
○ Enabled
○ Disabled
● Output
○ Ignore

Continue
○ Handled
● Not Handled

SXE ld:MinhaDLL.dll

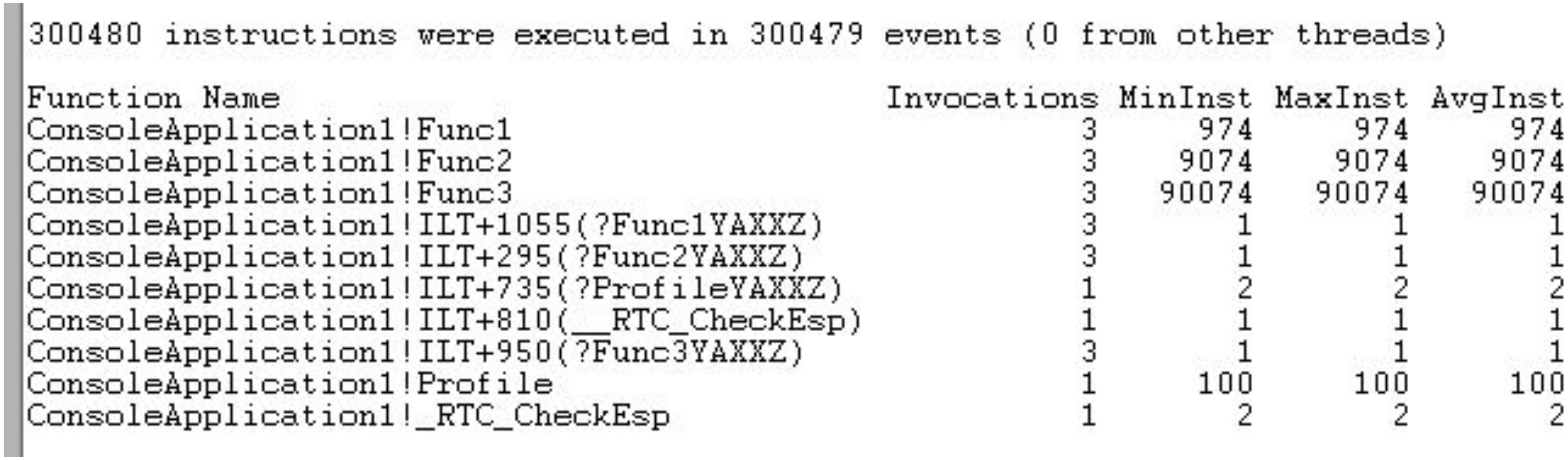

Log Viewer 3.01 for x64 (C:\Users\Caloni\Desktop\LogExts\notepad.exe.lgv)
File
Search
View
Help

+/-	#	Thrd	Caller	Module	Time Elapsed(m:s:ms)	Call Duration(us)	API Function	Return value
+ d0	1	1	00000000FF29298A	notepad.exe	000:00:023	41	DragAcceptFiles	
+ d0	2	1	000007FEFDD29885	COMDLG32.dll	000:04:113	1492	SHBindToParent	Ret = S_OK
+ d0	3	1	000007FEFE68EA6C	SHELL32.dll	000:04:114	1678	IShellFolder::BindToObject	Ret = S_OK
+ d0	4	1	000007FEFE67DF3F	SHELL32.dll	000:04:116	3347	IShellFolder::BindToObject	Ret = S_OK
+ d0	5	1	000007FEFE67E1B1	SHELL32.dll	000:04:120	2	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE
+ d0	6	1	000007FEFE68EA6C	SHELL32.dll	000:04:121	1684	IShellFolder::BindToObject	Ret = S_OK
+ d0	7	1	000007FEFE67AC79	SHELL32.dll	000:04:123	2	IShellFolder::BindToObject	Ret = E_NOINTERFACE
+ d0	8	1	000007FEFFB710EF	SHLWAPI.dll	000:04:123	2	IShellFolder::GetDisplayNameOf	Ret = S_OK
+ d0	9	1	000007FEFE67DF3F	SHELL32.dll	000:04:136	3789	IShellFolder::BindToObject	Ret = S_OK
+ d1	10	1	000007FEFE68EA6C	SHELL32.dll	000:04:140	1745	IShellFolder::BindToObject	Ret = S_OK
+ d0	11	1	000007FEFDD261FC	COMDLG32.dll	000:04:140	1915	SHBindToParent	Ret = S_OK
+ d0	12	1	000007FEFDD29EDF	COMDLG32.dll	000:04:142	1	IShellFolder::GetAttributesOf	Ret = S_OK
+ d0	13	1	000007FEFE68EA6C	SHELL32.dll	000:04:164	1981	IShellFolder::BindToObject	Ret = S_OK
+ d0	14	1	000007FEFE67DF3F	SHELL32.dll	000:04:166	3460	IShellFolder::BindToObject	Ret = S_OK
+ d0	15	1	000007FEFE73EA94	SHELL32.dll	000:04:170	0	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE
+ d0	16	1	000007FEFE73EABA	SHELL32.dll	000:04:170	0	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE
+ d0	17	1	000007FEFE67E1B1	SHELL32.dll	000:04:170	0	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE
+ d0	18	1	000007FEFE68EA6C	SHELL32.dll	000:04:170	1605	IShellFolder::BindToObject	Ret = S_OK
+ d0	19	1	000007FEFE67AC79	SHELL32.dll	000:04:172	2	IShellFolder::BindToObject	Ret = E_NOINTERFACE
+ d0	20	1	000007FEFE68DF93	SHELL32.dll	000:04:186	2	IShellFolder::CompareIDs	Ret = S_OK
+ d0	21	1	000007FEFE63C710	SHELL32.dll	000:04:186	3305	IShellFolder::BindToObject	Ret = S_OK
+ d0	22	1	000007FEFE63C710	SHELL32.dll	000:04:190	4091	IShellFolder::BindToObject	Ret = S_OK
+ d0	23	1	000007FEFE68DF93	SHELL32.dll	000:04:199	2	IShellFolder::CompareIDs	Ret = S_OK
+ d0	24	1	000007FEFE63C710	SHELL32.dll	000:04:200	3354	IShellFolder::BindToObject	Ret = S_OK
+ d0	25	1	000007FEFE63C710	SHELL32.dll	000:04:203	3464	IShellFolder::BindToObject	Ret = S_OK
+ d0	26	1	000007FEFE68DF93	SHELL32.dll	000:04:214	2	IShellFolder::CompareIDs	Ret = S_OK
+ d0	27	1	000007FEFE63C710	SHELL32.dll	000:04:214	3649	IShellFolder::BindToObject	Ret = S_OK
+ d0	28	1	000007FEFE63C710	SHELL32.dll	000:04:218	3524	IShellFolder::BindToObject	Ret = S_OK
+ d0	29	1	000007FEFE68DF93	SHELL32.dll	000:04:228	2	IShellFolder::CompareIDs	Ret = S_OK
+ d0	30	1	000007FEFE63C710	SHELL32.dll	000:04:228	3527	IShellFolder::BindToObject	Ret = S_OK
+ d0	31	1	000007FEFE63C710	SHELL32.dll	000:04:232	3715	IShellFolder::BindToObject	Ret = S_OK
+ d1	32	1	000007FEFE68EA6C	SHELL32.dll	000:04:240	2186	IShellFolder::BindToObject	Ret = S_OK
+ d0	33	1	000007FEFFB66F03	SHLWAPI.dll	000:04:239	2413	SHBindToParent	Ret = S_OK
+ d0	34	1	000007FEFFB66F2C	SHLWAPI.dll	000:04:242	1909	SHGetDataFromIDListW	Ret = S_OK
+ d1	35	1	000007FEFE68EA6C	SHELL32.dll	000:04:307	4391	IShellFolder::BindToObject	Ret = S_OK
+ d1	36	1	000007FEFE67DF3F	SHELL32.dll	000:04:311	3661	IShellFolder::BindToObject	Ret = S_OK
+ d0	37	1	000007FEFE6FF196	SHELL32.dll	000:04:299	17983	IShellFolder::CreateViewObject	Ret = S_OK
+ d0	38	1	000007FEFE67DF3F	SHELL32.dll	000:04:362	3925	IShellFolder::BindToObject	Ret = S_OK
+ d0	39	1	000007FEFE67E1B1	SHELL32.dll	000:04:366	0	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE
+ d0	40	1	000007FEFE68EA6C	SHELL32.dll	000:04:366	2314	IShellFolder::BindToObject	Ret = S_OK
+ d0	41	1	000007FEFE67DF3F	SHELL32.dll	000:04:368	3330	IShellFolder::BindToObject	Ret = S_OK
+ d0	42	1	000007FEFE67E1B1	SHELL32.dll	000:04:372	0	IShellFolder::CreateViewObject	Ret = E_NOINTERFACE

logger process.exe

WT

CODE
COMPILE
PROFILE
CODE
COMPILE
PROFILE
CODE
COMPILE
PROFILE
CODE
COMPILE
PROFILE
CODE
COMPILE
PROFILE
CODE
COMPILE
PROFILE
...



```
300480 instructions were executed in 300479 events (0 from other threads)

Function Name                               Invocations MinInst MaxInst AvgInst
ConsoleApplication1!Func1                             3     974     974     974
ConsoleApplication1!Func2                             3    9074    9074    9074
ConsoleApplication1!Func3                             3   90074   90074   90074
ConsoleApplication1!ILT+1055(?Func1YAXXZ)             3       1       1       1
ConsoleApplication1!ILT+295(?Func2YAXXZ)              3       1       1       1
ConsoleApplication1!ILT+735(?ProfileYAXXZ)            1       2       2       2
ConsoleApplication1!ILT+810(__RTC_CheckEsp)           1       1       1       1
ConsoleApplication1!ILT+950(?Func3YAXXZ)              3       1       1       1
ConsoleApplication1!Profile                           1     100     100     100
ConsoleApplication1!_RTC_CheckEsp                     1       2       2       2
```

PROCESS

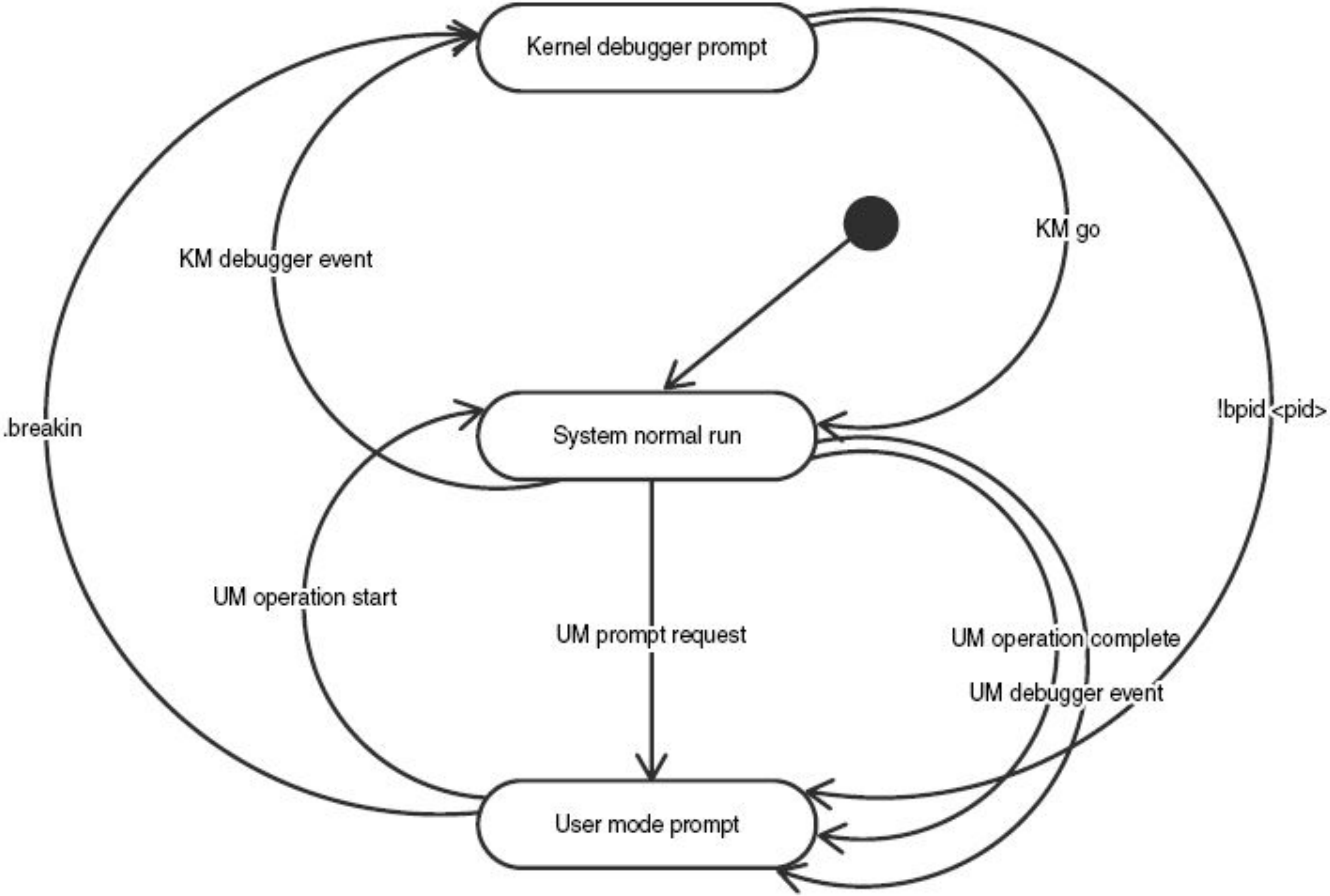
DEBUGGER

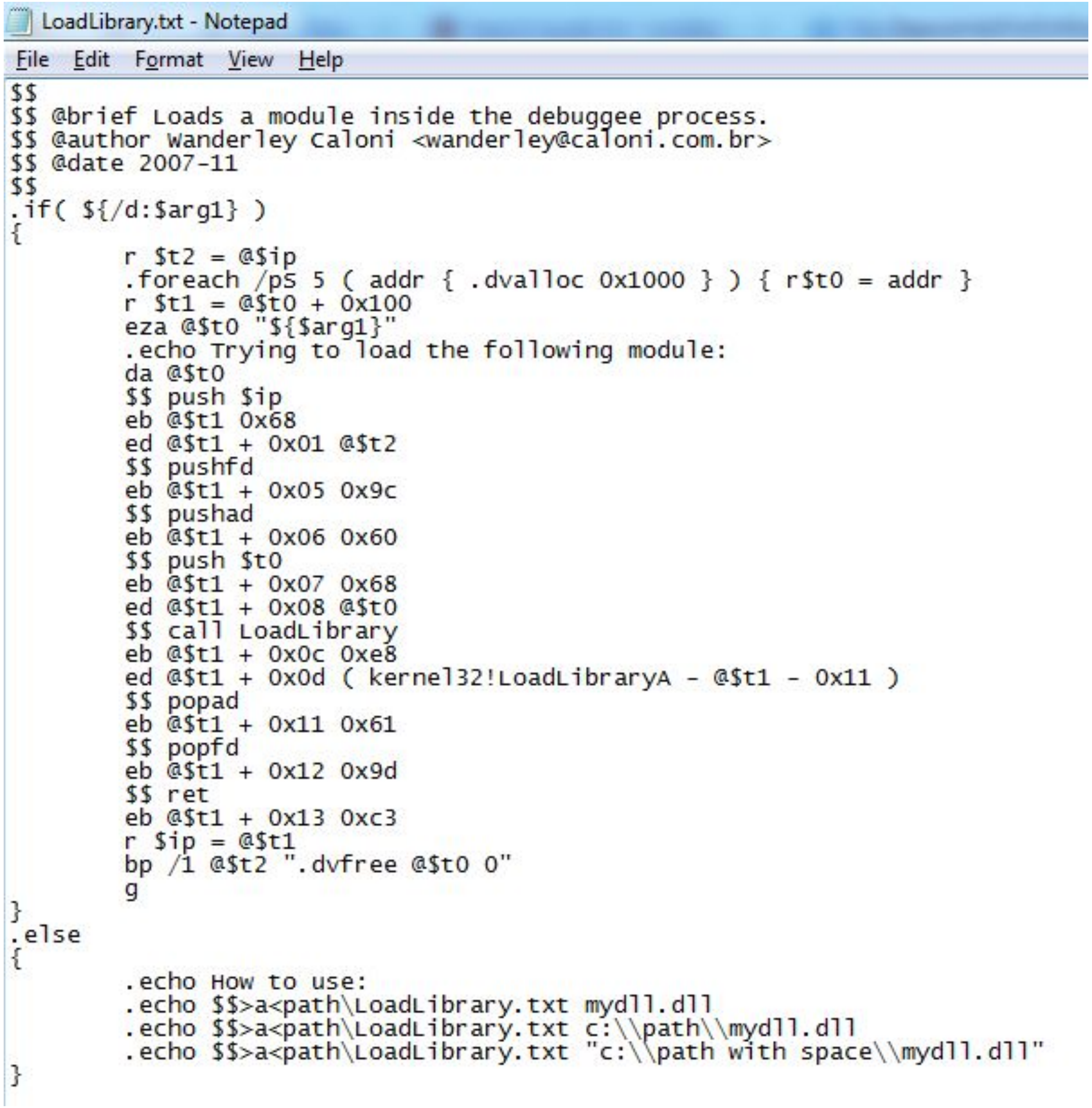
USER

KERNEL

CABLE

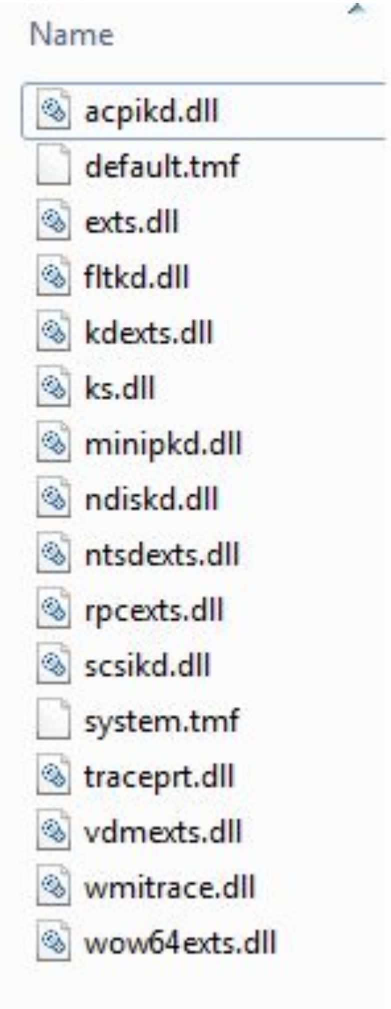
DEBUGGER


Kernel debugger prompt
KM debugger event
KM go
.breakin
System normal run
!bpid <pid>
UM operation start
UM prompt request
UM operation complete
UM debugger event
User mode prompt



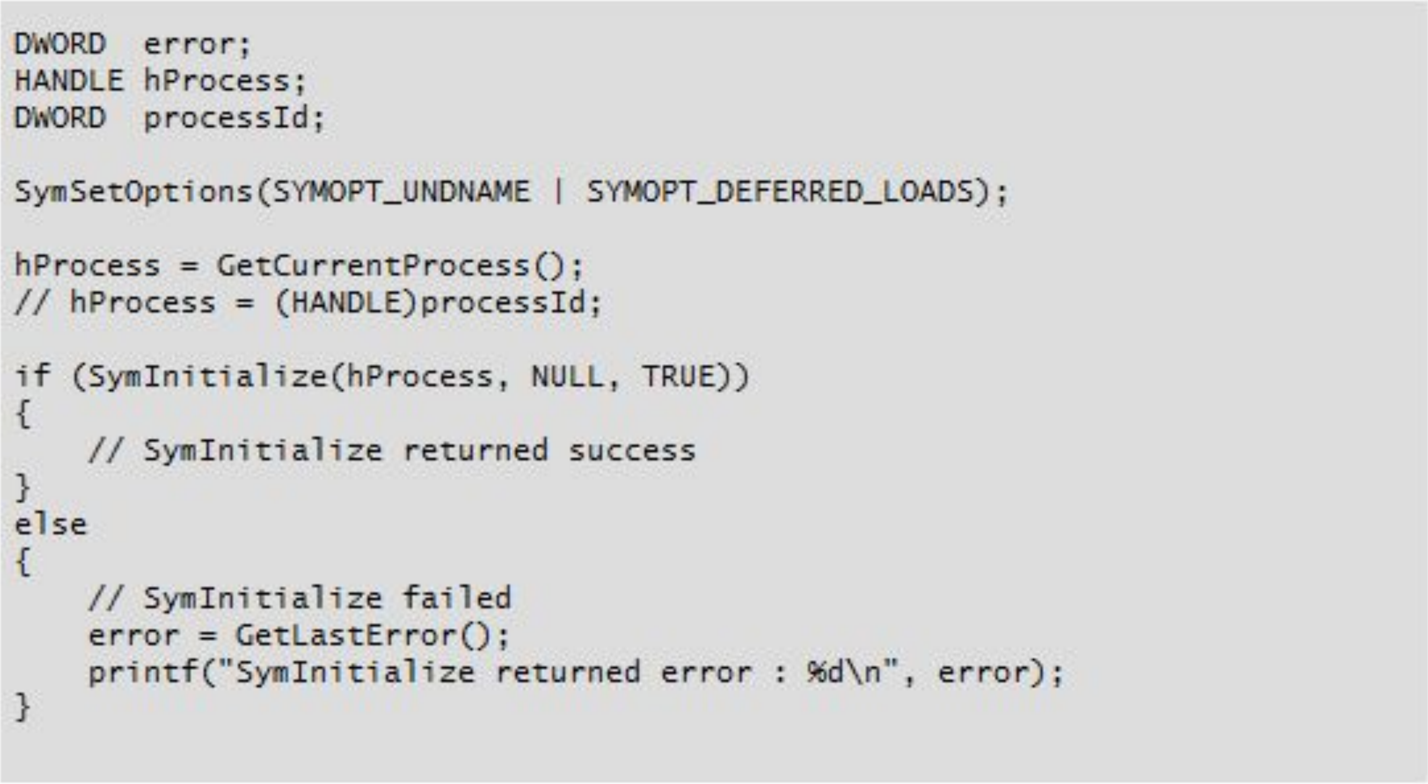
```
$$
$$ @brief Loads a module inside the debuggee process.
$$ @author Wanderley Caloni <wanderley@caloni.com.br>
$$ @date 2007-11
$$
.if( ${/d:$arg1} )
{
        r $t2 = @$ip
        .foreach /ps 5 ( addr { .dvalloc 0x1000 } ) { r$t0 = addr }
        r $t1 = @$t0 + 0x100
        eza @$t0 "${$arg1}"
        .echo Trying to load the following module:
        da @$t0
        $$ push $ip
        eb @$t1 0x68
        ed @$t1 + 0x01 @$t2
        $$ pushfd
        eb @$t1 + 0x05 0x9c
        $$ pushad
        eb @$t1 + 0x06 0x60
        $$ push $t0
        eb @$t1 + 0x07 0x68
        ed @$t1 + 0x08 @$t0
        $$ call LoadLibrary
        eb @$t1 + 0x0c 0xe8
        ed @$t1 + 0x0d ( kernel32!LoadLibraryA - @$t1 - 0x11 )
        $$ popad
        eb @$t1 + 0x11 0x61
        $$ popfd
        eb @$t1 + 0x12 0x9d
        $$ ret
        eb @$t1 + 0x13 0xc3
        r $ip = @$t1
        bp /1 @$t2 ".dvfree @$t0 0"
        g
}
.else
{
        .echo How to use:
        .echo $$>a<path\LoadLibrary.txt mydll.dll
        .echo $$>a<path\LoadLibrary.txt c:\\path\\mydll.dll
        .echo $$>a<path\LoadLibrary.txt "c:\\path with space\\mydll.dll"
}
```

$<, $><, $$<, and $$><



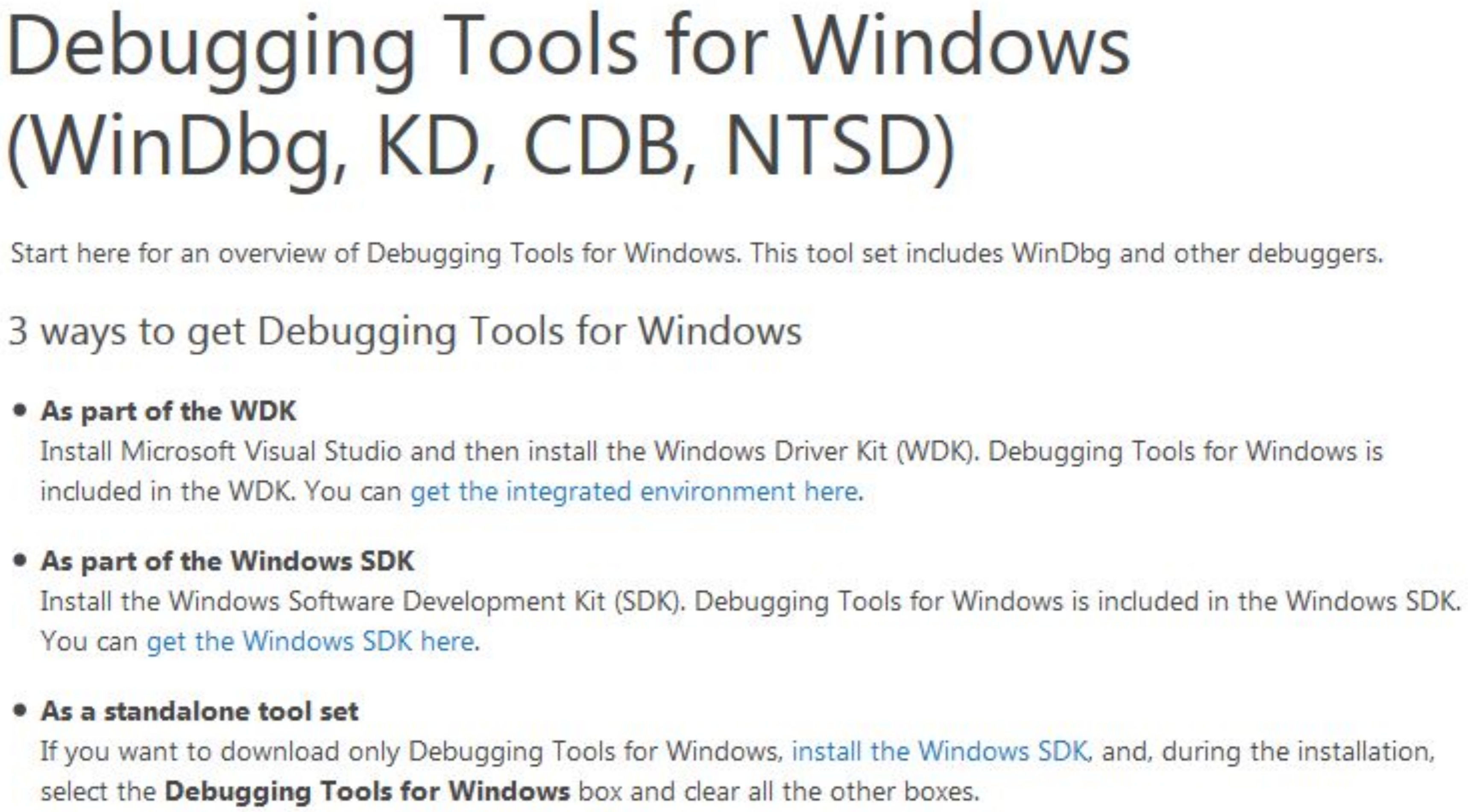
Name

- acpikd.dll
- default.tmf
- exts.dll
- fltkd.dll
- kdexts.dll
- ks.dll
- minipkd.dll
- ndiskd.dll
- ntsdexts.dll
- rpcexts.dll
- scsikd.dll
- system.tmf
- traceprt.dll
- vdmexts.dll
- wmitrace.dll
- wow64exts.dll



```
DWORD  error;
HANDLE hProcess;
DWORD  processId;

SymSetOptions(SYMOPT_UNDNAME | SYMOPT_DEFERRED_LOADS);

hProcess = GetCurrentProcess();
// hProcess = (HANDLE)processId;

if (SymInitialize(hProcess, NULL, TRUE))
{
    // SymInitialize returned success
}
else
{
    // SymInitialize failed
    error = GetLastError();
    printf("SymInitialize returned error : %d\n", error);
}
```

#include < wdbgexts.h>



Debugging Tools for Windows (WinDbg, KD, CDB, NTSD)

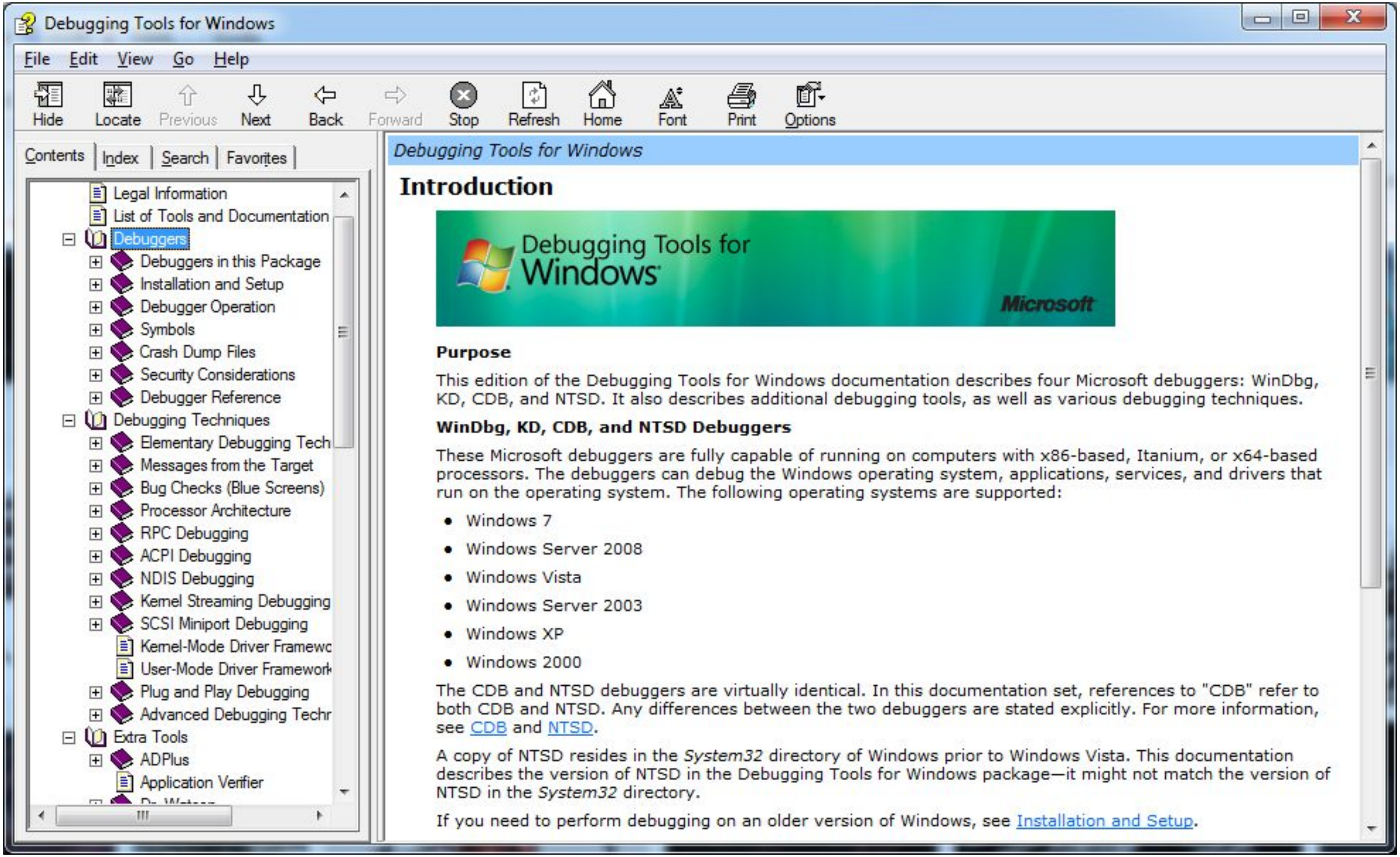
Start here for an overview of Debugging Tools for Windows. This tool set includes WinDbg and other debuggers.

3 ways to get Debugging Tools for Windows

- **As part of the WDK**
  Install Microsoft Visual Studio and then install the Windows Driver Kit (WDK). Debugging Tools for Windows is included in the WDK. You can get the integrated environment here.

- **As part of the Windows SDK**
  Install the Windows Software Development Kit (SDK). Debugging Tools for Windows is included in the Windows SDK. You can get the Windows SDK here.

- **As a standalone tool set**
  If you want to download only Debugging Tools for Windows, install the Windows SDK, and, during the installation, select the **Debugging Tools for Windows** box and clear all the other boxes.



Debugging Tools for Windows

Introduction

Purpose

This edition of the Debugging Tools for Windows documentation describes four Microsoft debuggers: WinDbg, KD, CDB, and NTSD. It also describes additional debugging tools, as well as various debugging techniques.

WinDbg, KD, CDB, and NTSD Debuggers

These Microsoft debuggers are fully capable of running on computers with x86-based, Itanium, or x64-based processors. The debuggers can debug the Windows operating system, applications, services, and drivers that run on the operating system. The following operating systems are supported:

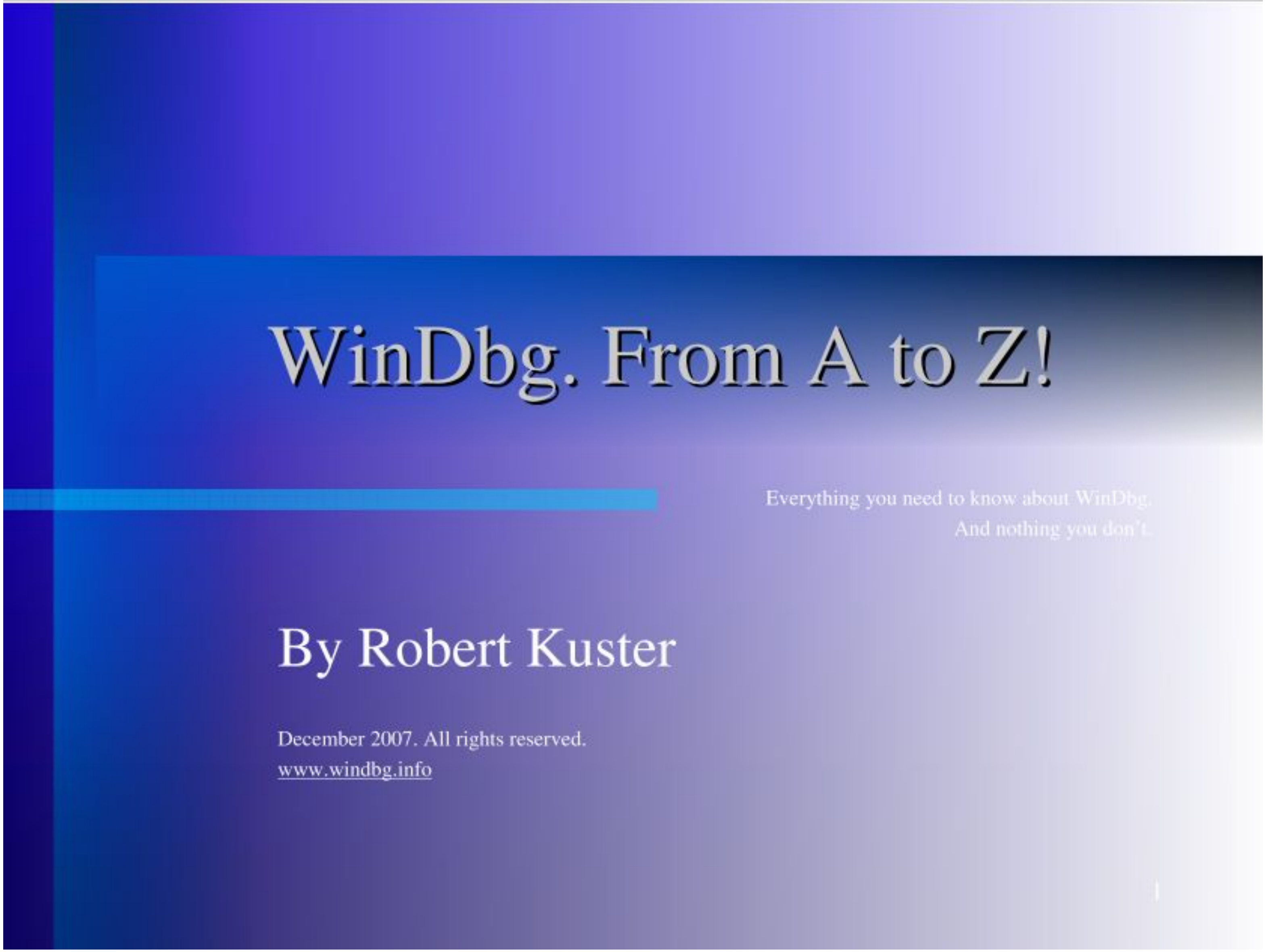
- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP
- Windows 2000

The CDB and NTSD debuggers are virtually identical. In this documentation set, references to "CDB" refer to both CDB and NTSD. Any differences between the two debuggers are stated explicitly. For more information, see CDB and NTSD.

A copy of NTSD resides in the *System32* directory of Windows prior to Windows Vista. This documentation describes the version of NTSD in the Debugging Tools for Windows package—it might not match the version of NTSD in the *System32* directory.

If you need to perform debugging on an older version of Windows, see Installation and Setup.

.hh <topic>



WinDbg. From A to Z!

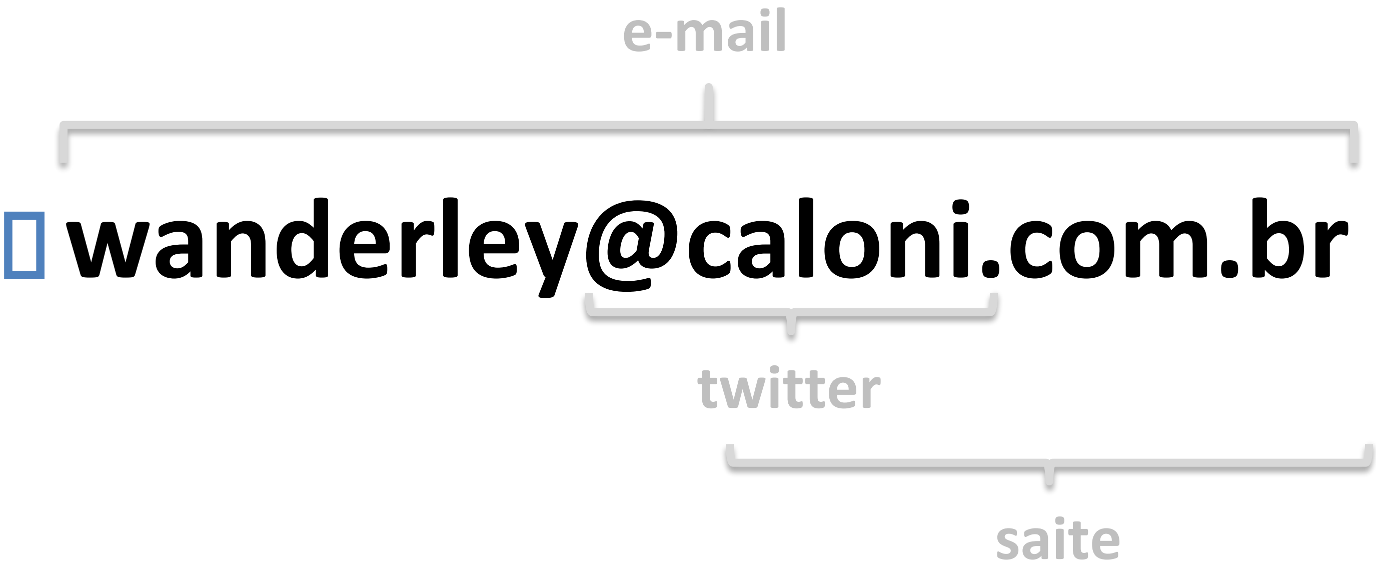
Everything you need to know about WinDbg.
And nothing you don't.

By Robert Kuster

www.windbg.info

www.windbg.inf

Perguntas?



e-mail

- **wanderley@caloni.com.br**

twitter

saite