Usando IDA-PRO para analisar os desvios de um código ASM e sua aplicação no Crack.

Pedro Garcia

http://www.sawp.com.br

26 de Fevereiro de 2010

Assembly Working Party

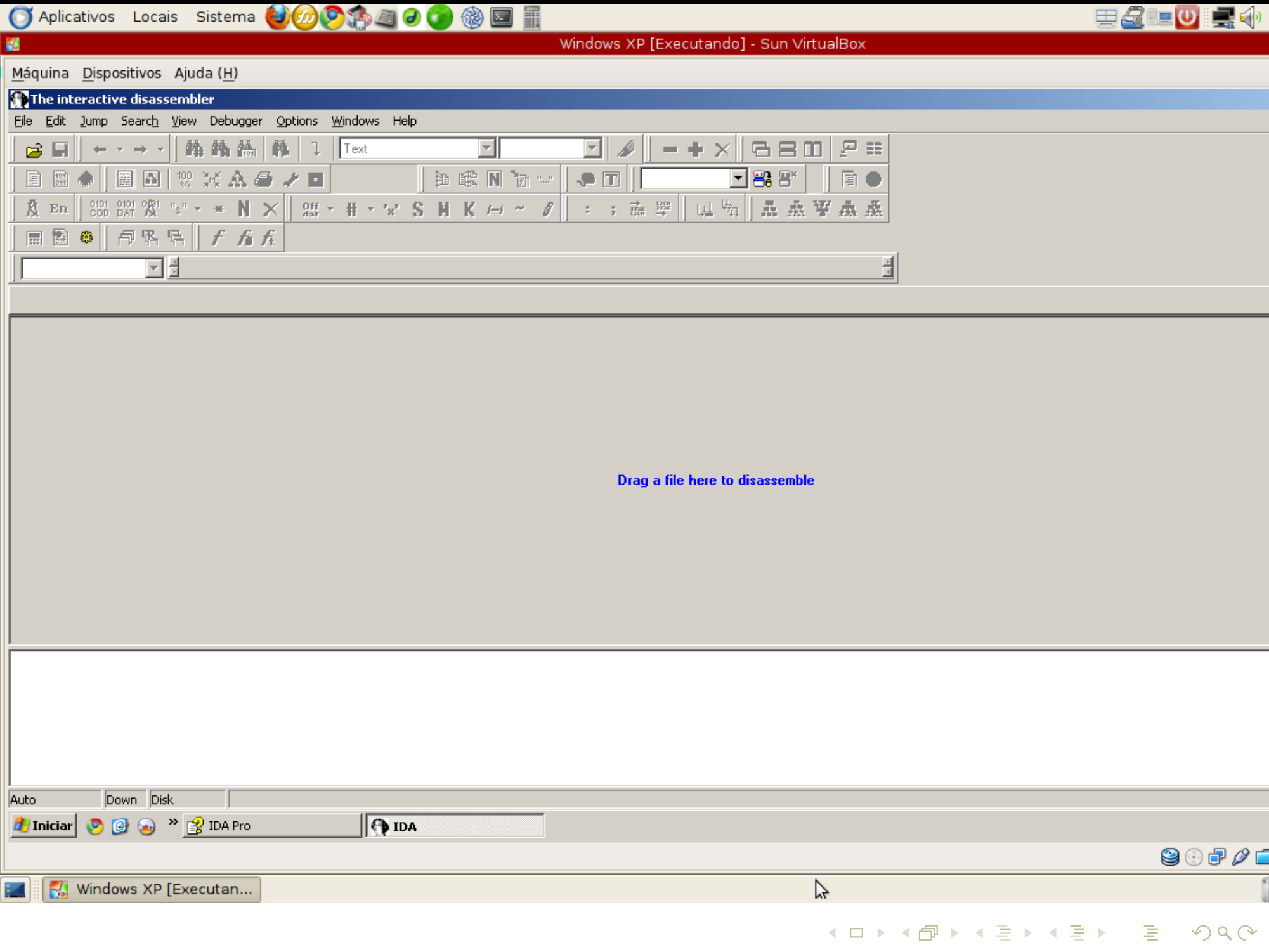
Laboratório de Cálculos Científicos, Instituto de Física, Universidade de Brasília, Brasil

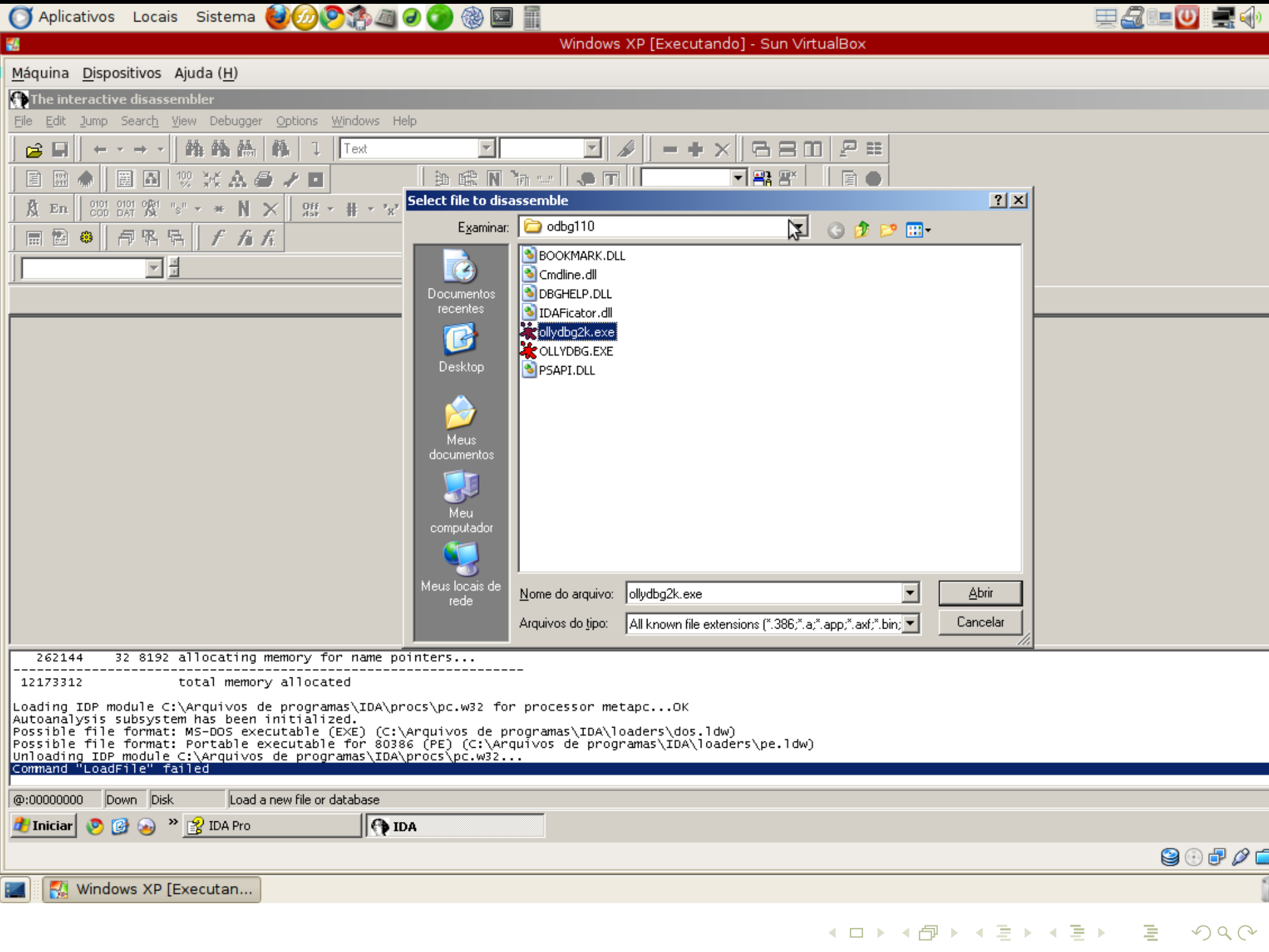
Sobre o IDA-PRO

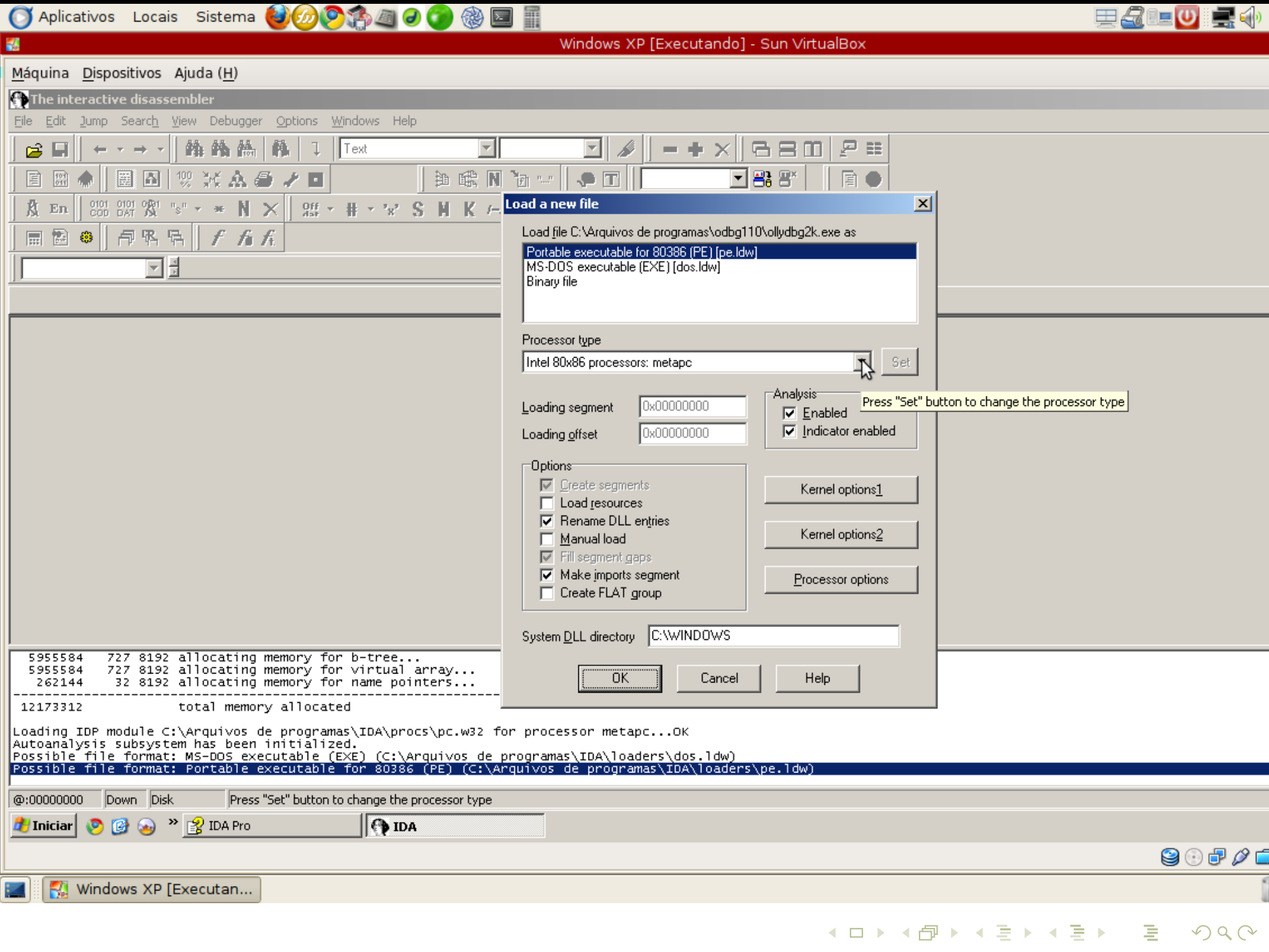
- Maior ferramenta de engenharia reversa e desassembly existente.
- Suporte à multiplos sistemas operacionais: Linux, OS X, UNIX, DOS, Windows, Motorola FLEX OS, PDP-11, GeoWorks, NetWare, BeOS, Amiga, dentre outros.
- Suporte à multiplas arquiteturas: IA32, IA, JAVA, .NET, MIPS, e várias arquiteturas reais ou virtualizadas, inclusive *Embedded*.
- Suporte à *debugging* remoto, sendo um “canivete suísso” no *cracking* de S.O.
- Considerada a maior “IDE” de inspeção de arquivos binários.
- O arquivo é disassemblado para a sintaxe da Intel.

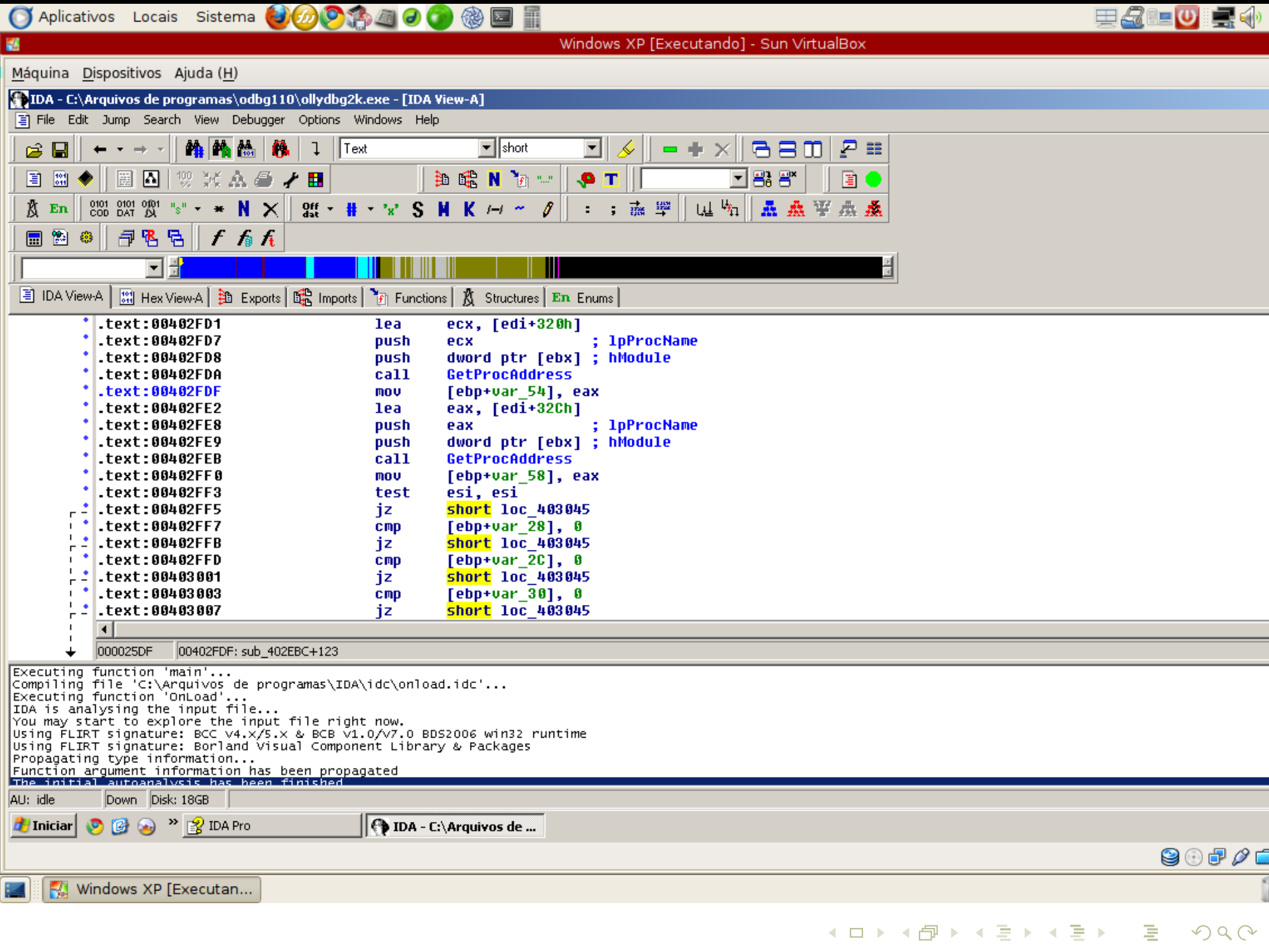
Sobre o IDA-PRO

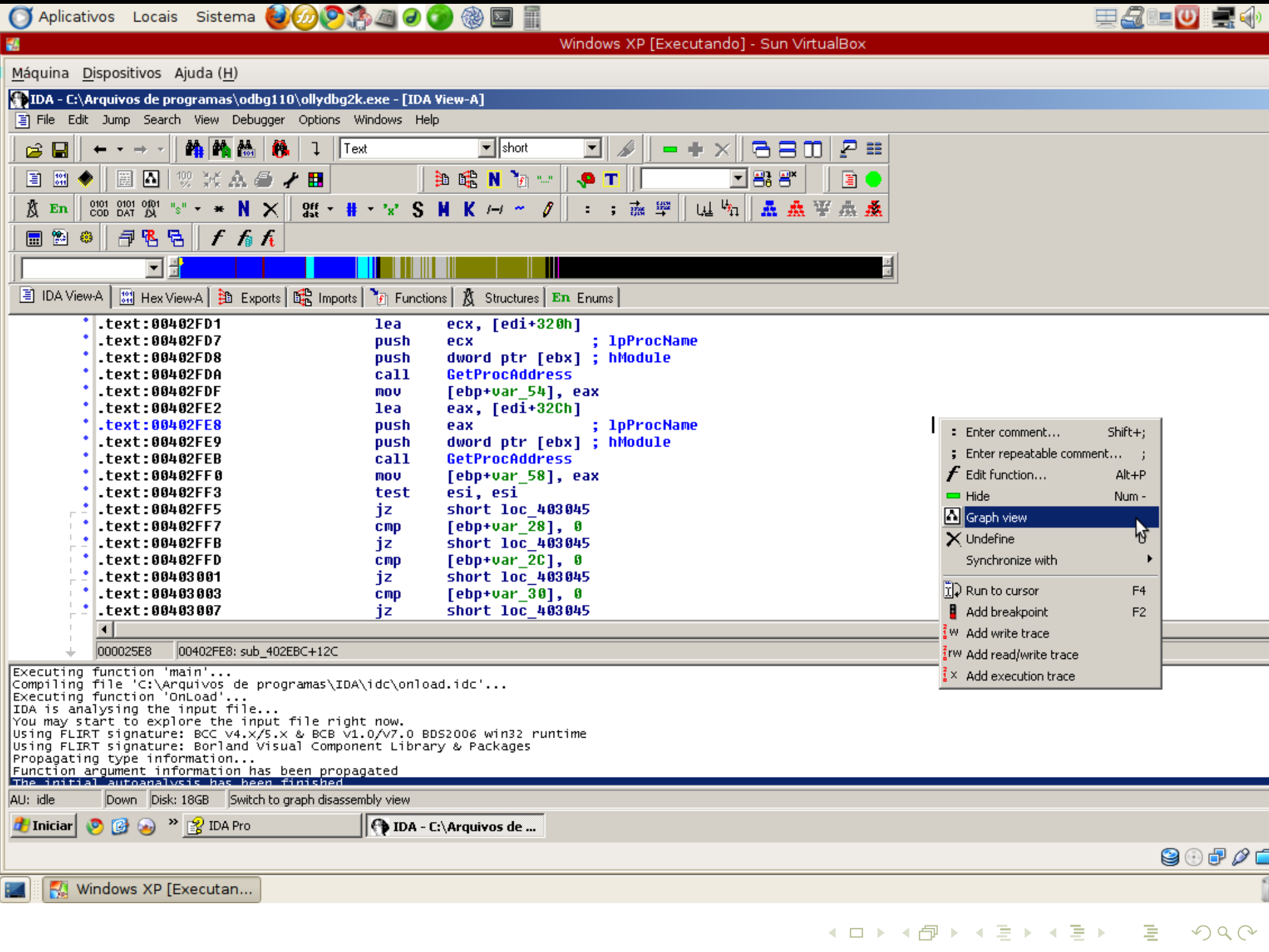
- Ideal para análise estática, mas também permite análise “online” do código disassemblado.
- Muitos recursos, o que exige mais tempo de experiência para aprendizagem (ao contrário do OllyDBG, por exemplo).
- **Gera o fluxograma de execução, facilitando analisar os desvios do programa**.
- Criação de *IDC scripts*, que permite automatizar a busca por certos padrões dentro do programa que está sendo analisado.

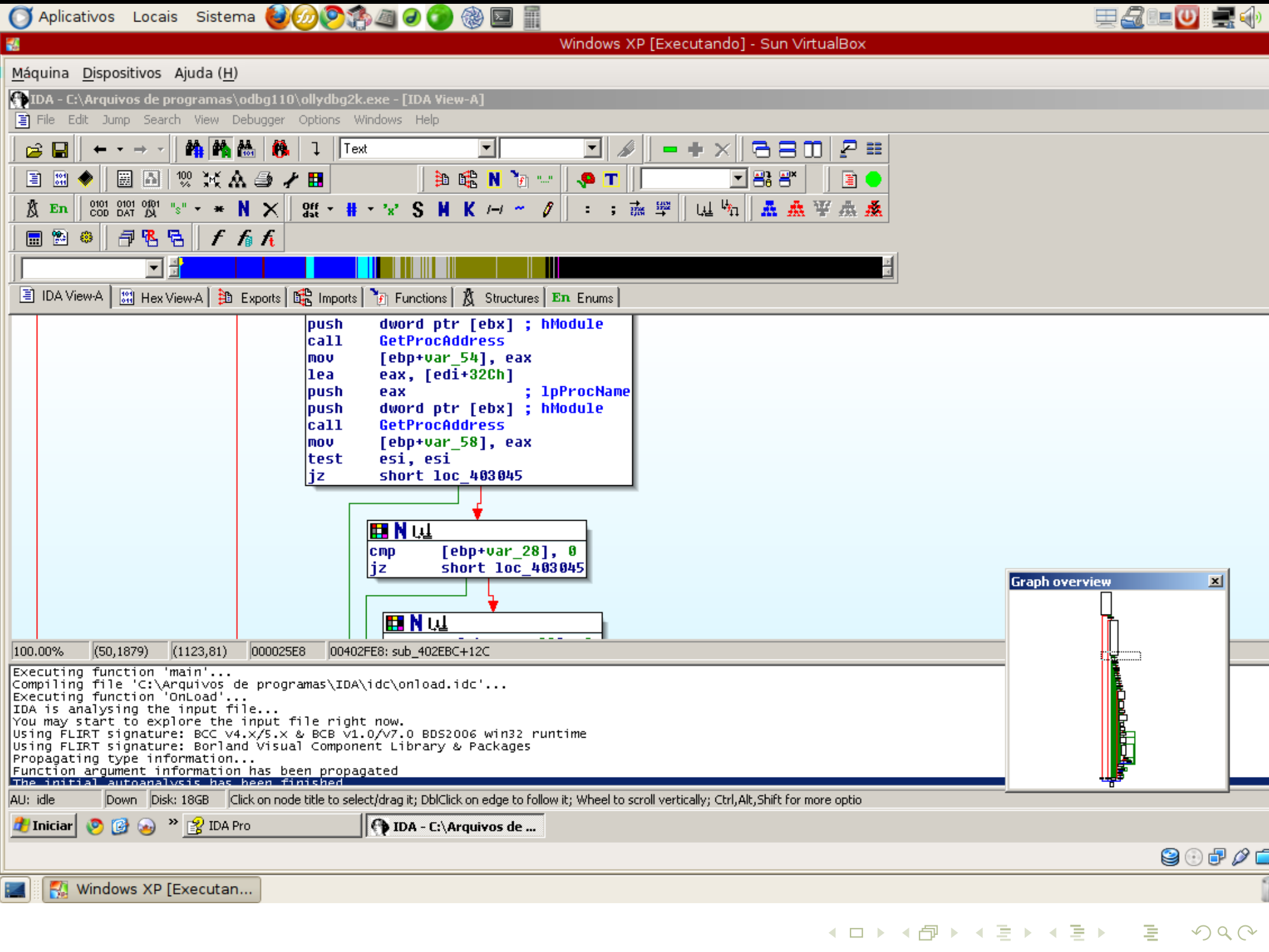

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
The interactive disassembler
File Edit Jump Search View Debugger Options Windows Help
Text
Drag a file here to disassemble
Auto Down Disk
Iniciar
IDA Pro
IDA
Windows XP [Executan...

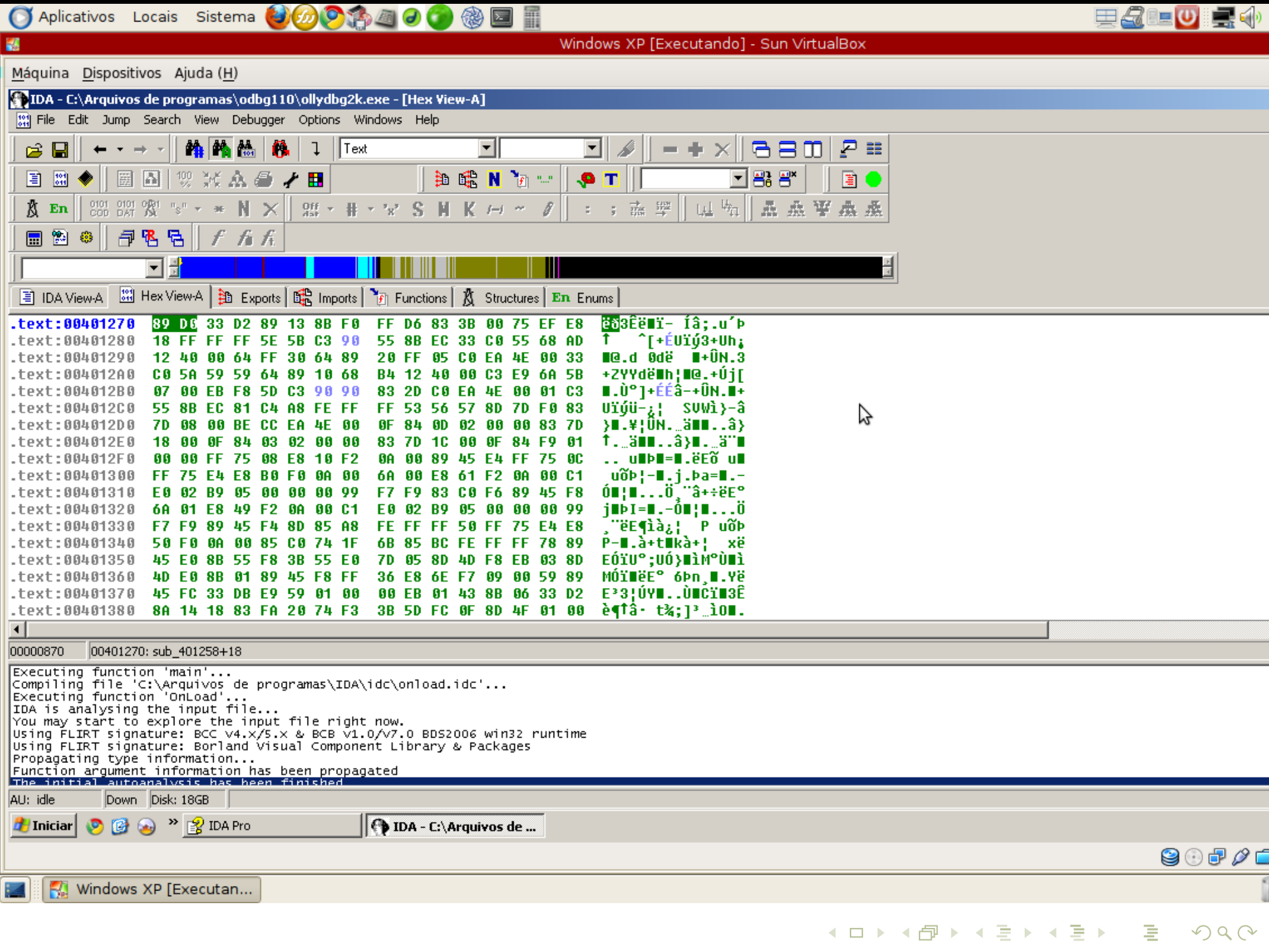

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
The interactive disassembler
File Edit Jump Search View Debugger Options Windows Help
Text
Select file to disassemble
Examinar: odbg110
Documentos recentes
Desktop
Meus documentos
Meu computador
Meus locais de rede
BOOKMARK.DLL
Cmdline.dll
DBGHELP.DLL
IDAFicator.dll
ollydbg2k.exe
OLLYDBG.EXE
PSAPI.DLL
Nome do arquivo: ollydbg2k.exe
Abrir
Arquivos do tipo: All known file extensions (*.386;*.a;*.app;*.axf;*.bin;
Cancelar
262144 32 8192 allocating memory for name pointers...
12173312 total memory allocated
Loading IDP module C:\Arquivos de programas\IDA\procs\pc.w32 for processor metapc...OK
Autoanalysis subsystem has been initialized.
Possible file format: MS-DOS executable (EXE) (C:\Arquivos de programas\IDA\loaders\dos.ldw)
Possible file format: Portable executable for 80386 (PE) (C:\Arquivos de programas\IDA\loaders\pe.ldw)
Unloading IDP module C:\Arquivos de programas\IDA\procs\pc.w32...
Command "LoadFile" failed
@:00000000 Down Disk Load a new file or database
Iniciar
IDA Pro
IDA
Windows XP [Executan...

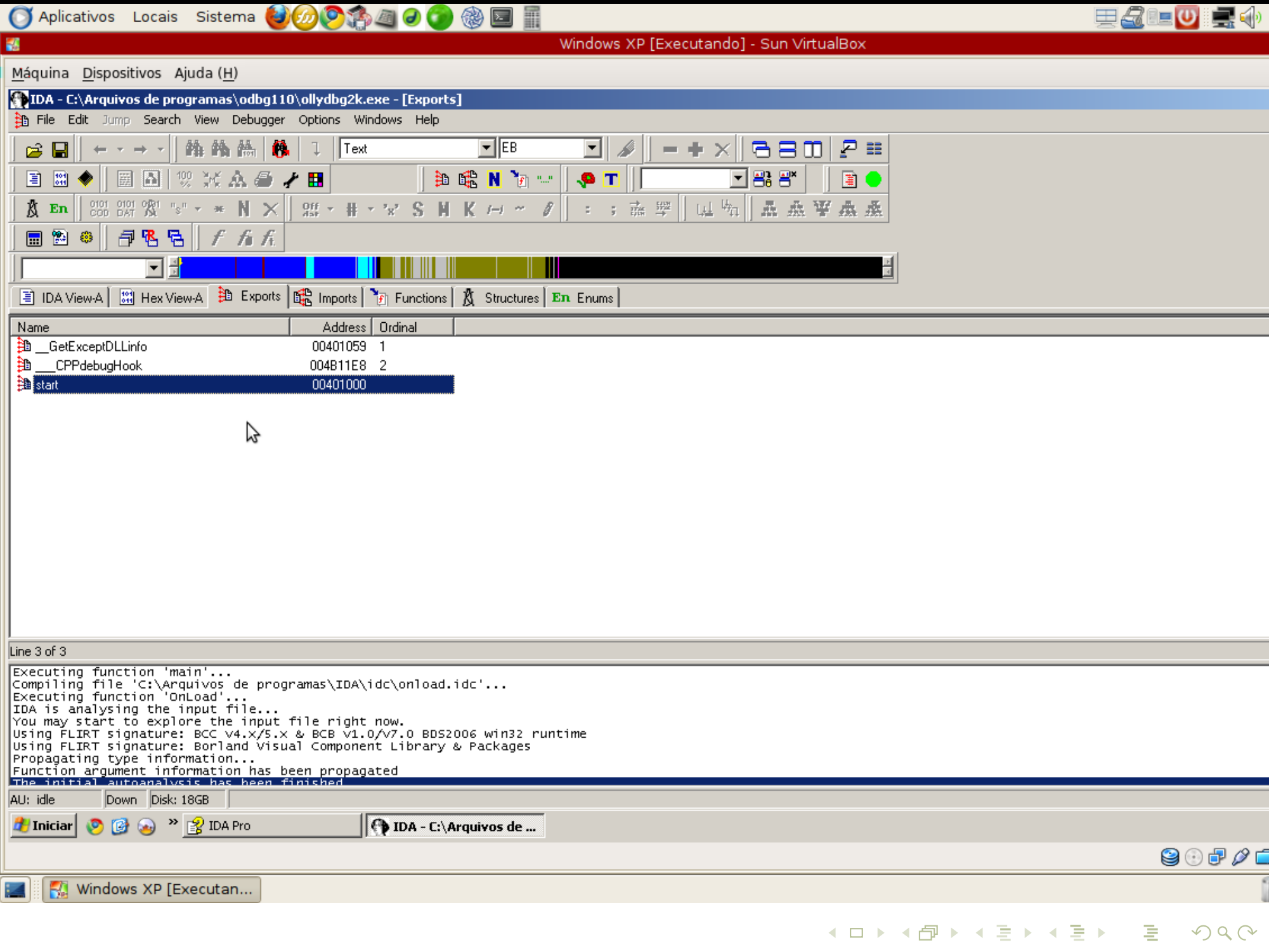

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
The interactive disassembler
File Edit Jump Search View Debugger Options Windows Help
Text
Load a new file
Load file C:\Arquivos de programas\odbg110\ollydbg2k.exe as
Portable executable for 80386 (PE) [pe.ldw]
MS-DOS executable (EXE) [dos.ldw]
Binary file
Processor type
Intel 80x86 processors: metapc
Set
Press "Set" button to change the processor type
Loading segment
0x00000000
Loading offset
0x00000000
Analysis
Enabled
Indicator enabled
Options
Create segments
Load resources
Rename DLL entries
Manual load
Fill segment gaps
Make imports segment
Create FLAT group
Kernel options1
Kernel options2
Processor options
System DLL directory
C:\WINDOWS
OK
Cancel
Help
5955584 727 8192 allocating memory for b-tree...
5955584 727 8192 allocating memory for virtual array...
262144 32 8192 allocating memory for name pointers...
12173312 total memory allocated
Loading IDP module C:\Arquivos de programas\IDA\procs\pc.w32 for processor metapc...OK
Autoanalysis subsystem has been initialized.
Possible file format: MS-DOS executable (EXE) (C:\Arquivos de programas\IDA\loaders\dos.ldw)
Possible file format: Portable executable for 80386 (PE) (C:\Arquivos de programas\IDA\loaders\pe.ldw)
@:00000000 Down Disk Press "Set" button to change the processor type
Iniciar
IDA Pro
IDA
Windows XP [Executan...

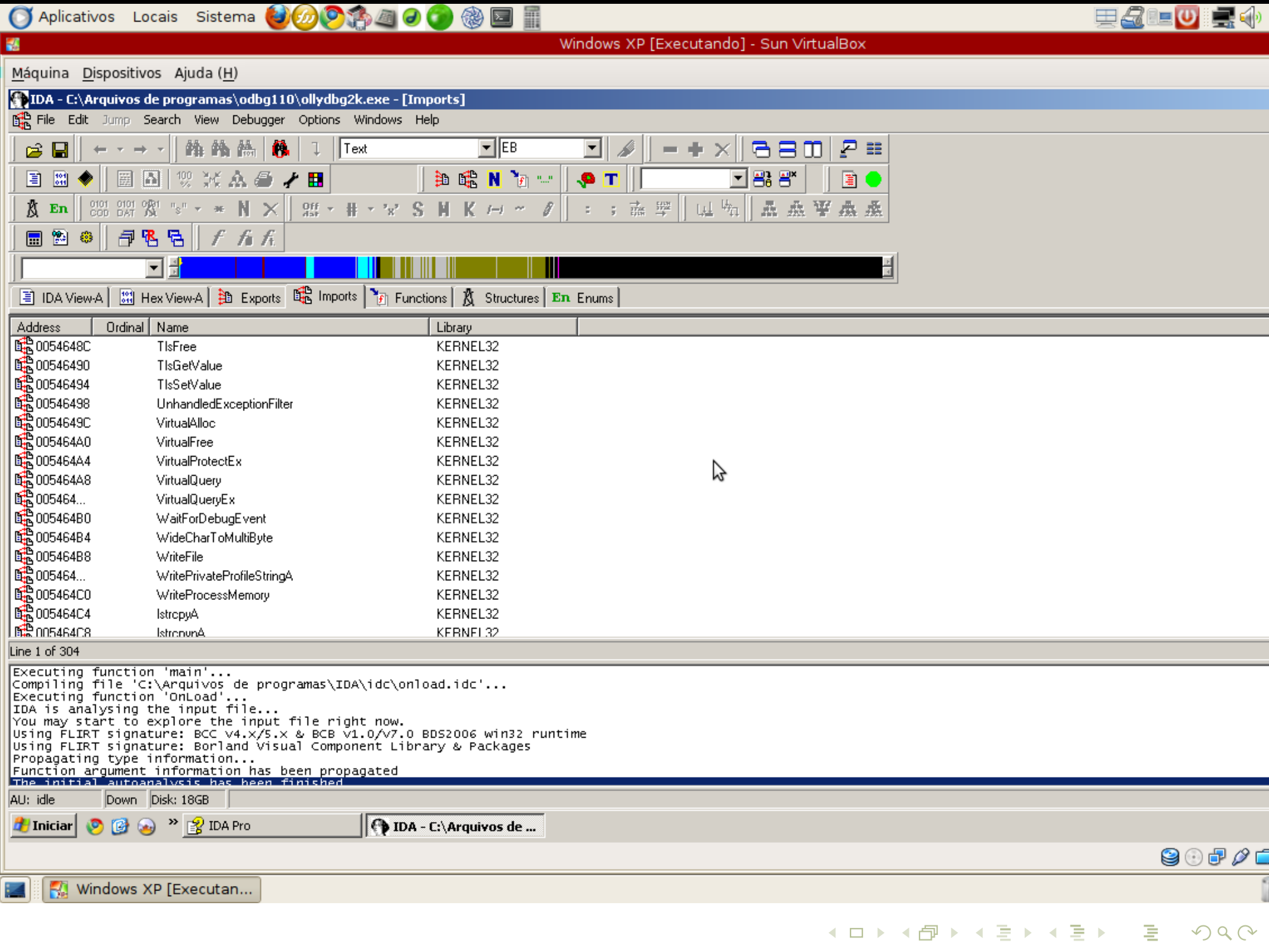

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
short
IDA View-A
Hex View-A
Exports
Imports
Functions
Structures
En Enums
.text:00402FD1 lea ecx, [edi+320h]
.text:00402FD7 push ecx ; lpProcName
.text:00402FD8 push dword ptr [ebx] ; hModule
.text:00402FDA call GetProcAddress
.text:00402FDF mov [ebp+var_54], eax
.text:00402FE2 lea eax, [edi+32Ch]
.text:00402FE8 push eax ; lpProcName
.text:00402FE9 push dword ptr [ebx] ; hModule
.text:00402FEB call GetProcAddress
.text:00402FF0 mov [ebp+var_58], eax
.text:00402FF3 test esi, esi
.text:00402FF5 jz short loc_403045
.text:00402FF7 cmp [ebp+var_28], 0
.text:00402FFB jz short loc_403045
.text:00402FFD cmp [ebp+var_2C], 0
.text:00403001 jz short loc_403045
.text:00403003 cmp [ebp+var_30], 0
.text:00403007 jz short loc_403045
000025DF
00402FDF: sub_402EBC+123
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

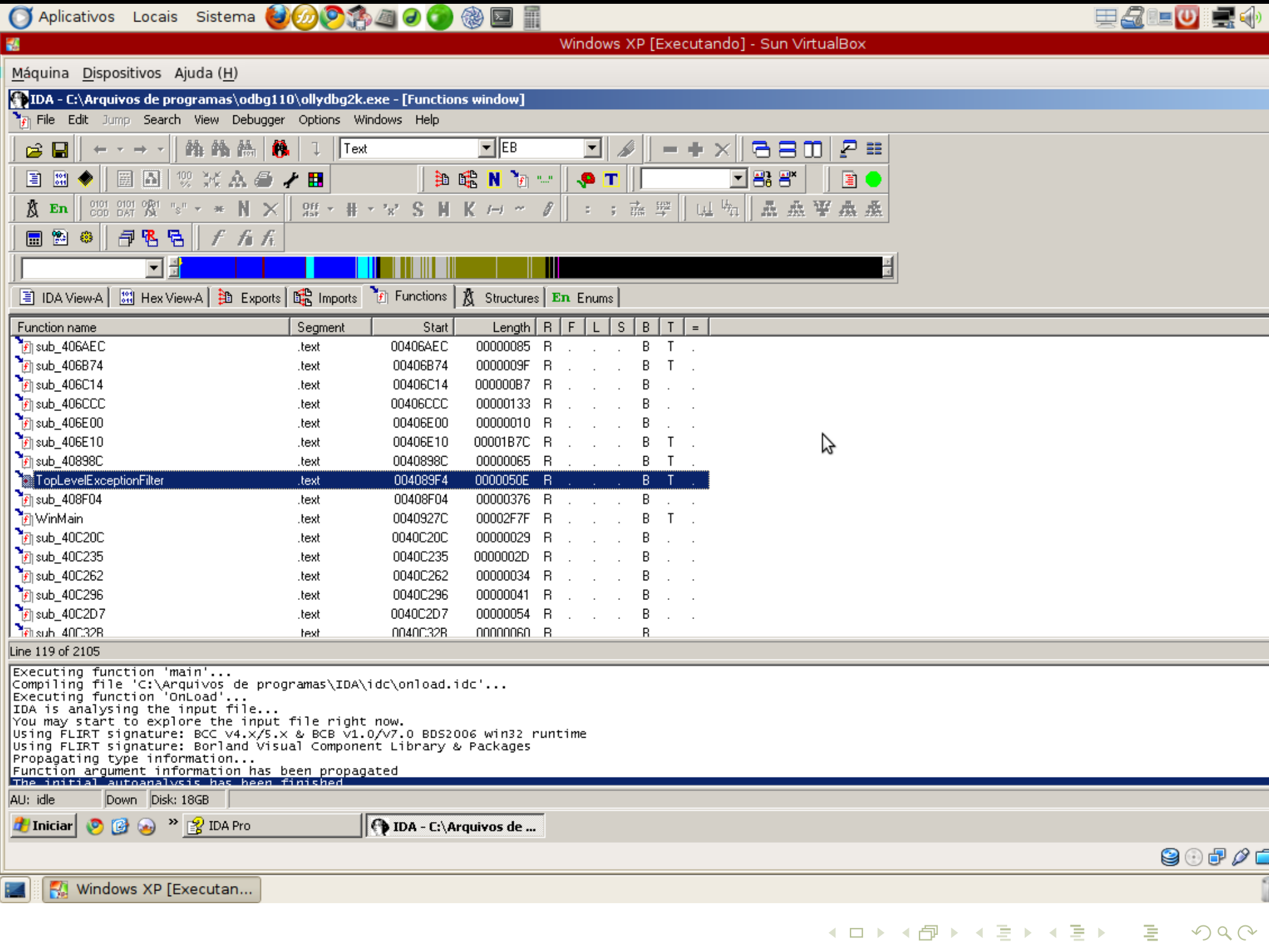

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
short
IDA View-A
Hex View-A
Exports
Imports
Functions
Structures
En Enums
.text:00402FD1 lea ecx, [edi+320h]
.text:00402FD7 push ecx ; lpProcName
.text:00402FD8 push dword ptr [ebx] ; hModule
.text:00402FDA call GetProcAddress
.text:00402FDF mov [ebp+var_54], eax
.text:00402FE2 lea eax, [edi+32Ch]
.text:00402FE8 push eax ; lpProcName
.text:00402FE9 push dword ptr [ebx] ; hModule
.text:00402FEB call GetProcAddress
.text:00402FF0 mov [ebp+var_58], eax
.text:00402FF3 test esi, esi
.text:00402FF5 jz short loc_403045
.text:00402FF7 cmp [ebp+var_28], 0
.text:00402FFB jz short loc_403045
.text:00402FFD cmp [ebp+var_2C], 0
.text:00403001 jz short loc_403045
.text:00403003 cmp [ebp+var_30], 0
.text:00403007 jz short loc_403045
Enter comment... Shift+;
Enter repeatable comment... ;
Edit function... Alt+P
Hide Num -
Graph view
Undefine
Synchronize with
Run to cursor F4
Add breakpoint F2
Add write trace
Add read/write trace
Add execution trace
000025E8
00402FE8: sub_402EBC+12C
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Switch to graph disassembly view
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

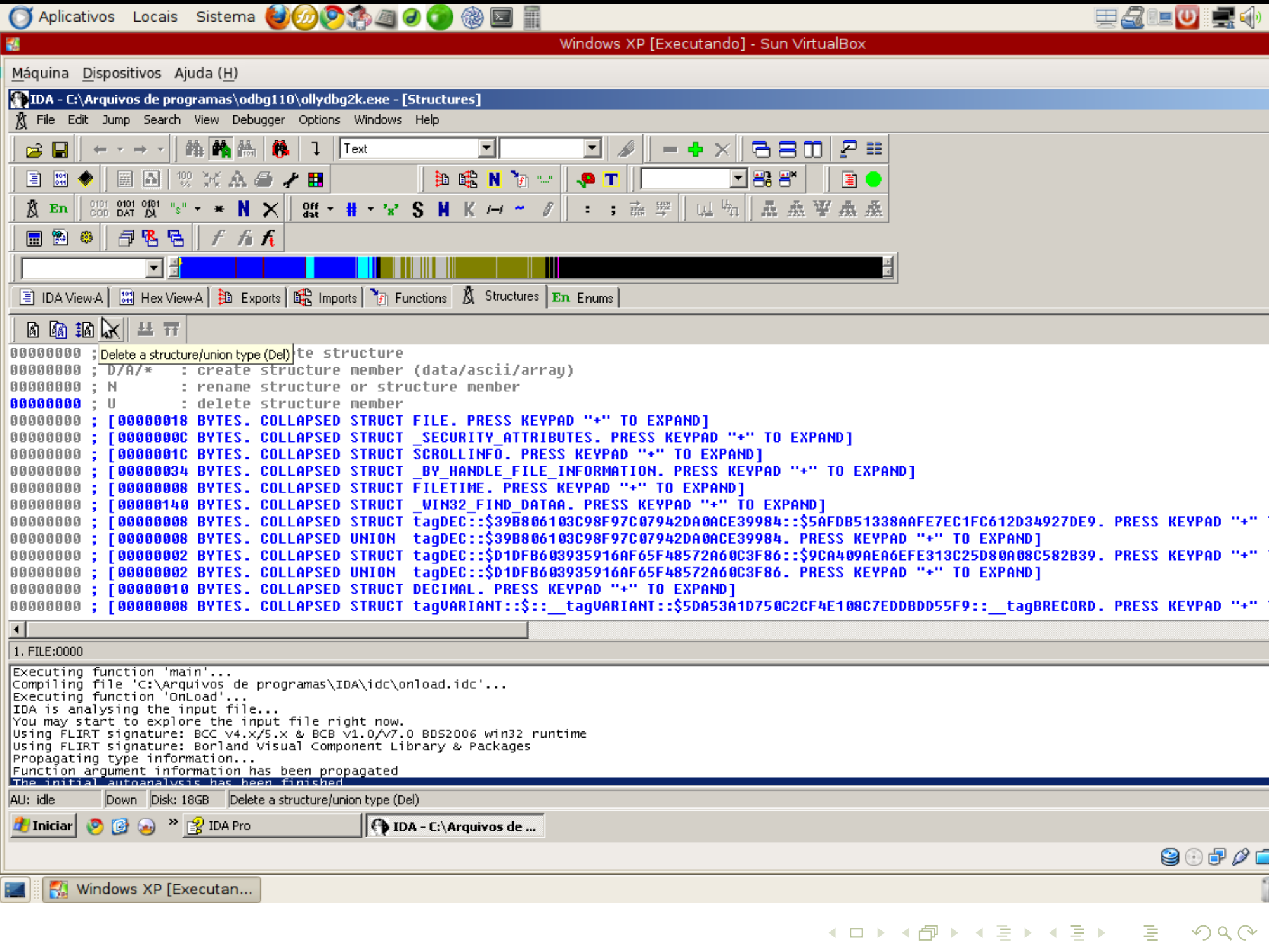

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Functions
Structures
En Enums
push dword ptr [ebx] ; hModule
call GetProcAddress
mov [ebp+var_54], eax
lea eax, [edi+32Ch]
push eax ; lpProcName
push dword ptr [ebx] ; hModule
call GetProcAddress
mov [ebp+var_58], eax
test esi, esi
jz short loc_403045
cmp [ebp+var_28], 0
jz short loc_403045
Graph overview
100.00% (50,1879) (1123,81) 000025E8 00402FE8: sub_402EBC+12C
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB Click on node title to select/drag it; DblClick on edge to follow it; Wheel to scroll vertically; Ctrl,Alt,Shift for more optio
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

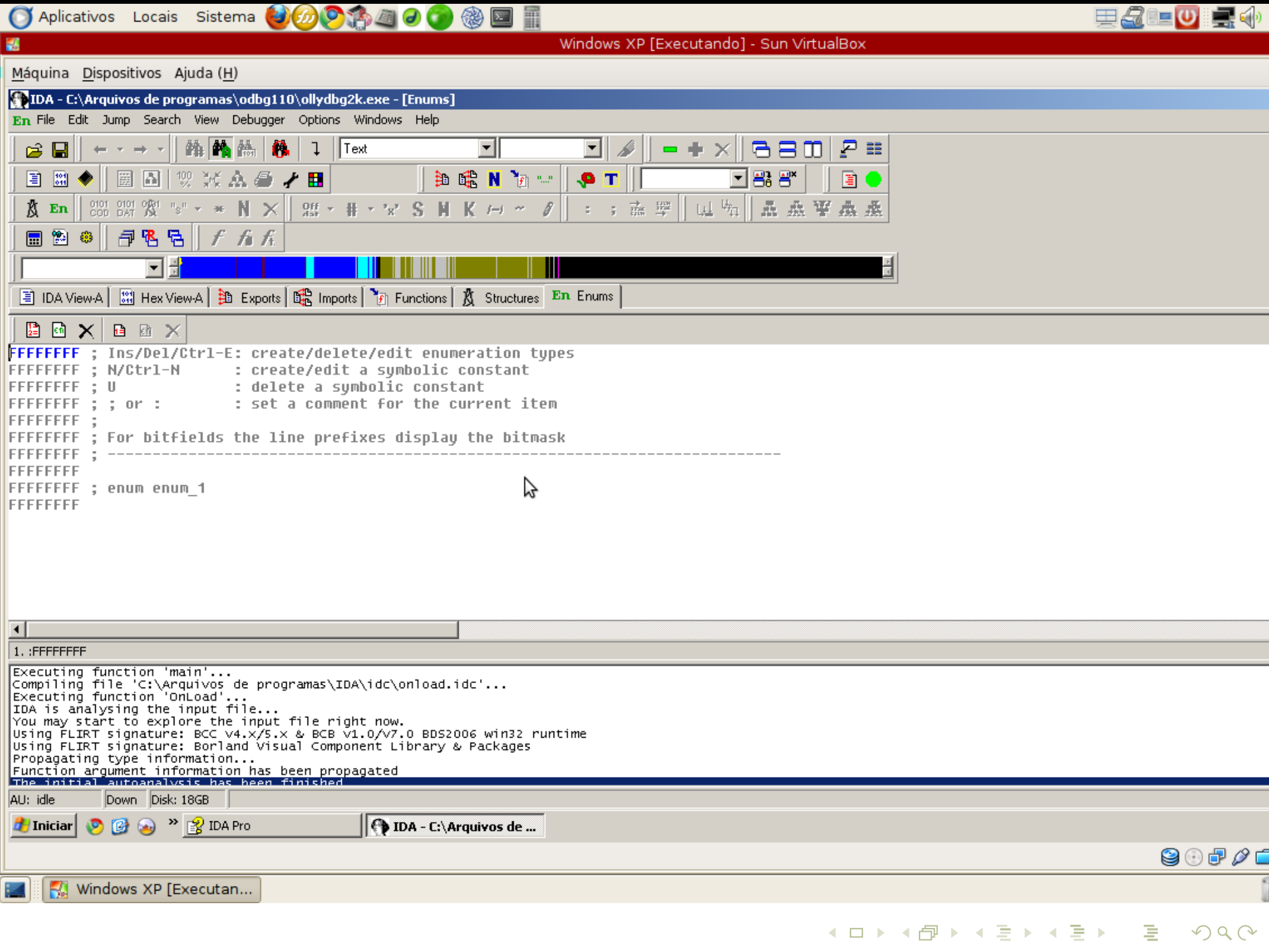

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Hex View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
.text:00401270 89 D6 33 D2 89 13 8B F0 FF D6 83 3B 00 75 EF E8
.text:00401280 18 FF FF FF 5E 5B C3 90 55 8B EC 33 C0 55 68 AD
.text:00401290 12 40 00 64 FF 30 64 89 20 FF 05 C0 EA 4E 00 33
.text:004012A0 C0 5A 59 59 64 89 10 68 B4 12 40 00 C3 E9 6A 5B
.text:004012B0 07 00 EB F8 5D C3 90 90 83 2D C0 EA 4E 00 01 C3
.text:004012C0 55 8B EC 81 C4 A8 FE FF FF 53 56 57 8D 7D F0 83
.text:004012D0 7D 08 00 BE CC EA 4E 00 0F 84 0D 02 00 00 83 7D
.text:004012E0 18 00 0F 84 03 02 00 00 83 7D 1C 00 0F 84 F9 01
.text:004012F0 00 00 FF 75 08 E8 10 F2 0A 00 89 45 E4 FF 75 0C
.text:00401300 FF 75 E4 E8 B0 F0 0A 00 6A 00 E8 61 F2 0A 00 C1
.text:00401310 E0 02 B9 05 00 00 00 99 F7 F9 83 C0 F6 89 45 F8
.text:00401320 6A 01 E8 49 F2 0A 00 C1 E0 02 B9 05 00 00 00 99
.text:00401330 F7 F9 89 45 F4 8D 85 A8 FE FF FF 50 FF 75 E4 E8
.text:00401340 50 F0 0A 00 85 C0 74 1F 6B 85 BC FE FF FF 78 89
.text:00401350 45 E0 8B 55 F8 3B 55 E0 7D 05 8D 4D F8 EB 03 8D
.text:00401360 4D E0 8B 01 89 45 F8 FF 36 E8 6E F7 09 00 59 89
.text:00401370 45 FC 33 DB E9 59 01 00 00 EB 01 43 8B 06 33 D2
.text:00401380 8A 14 18 83 FA 20 74 F3 3B 5D FC 0F 8D 4F 01 00
00000870 00401270: sub_401258+18
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executan...

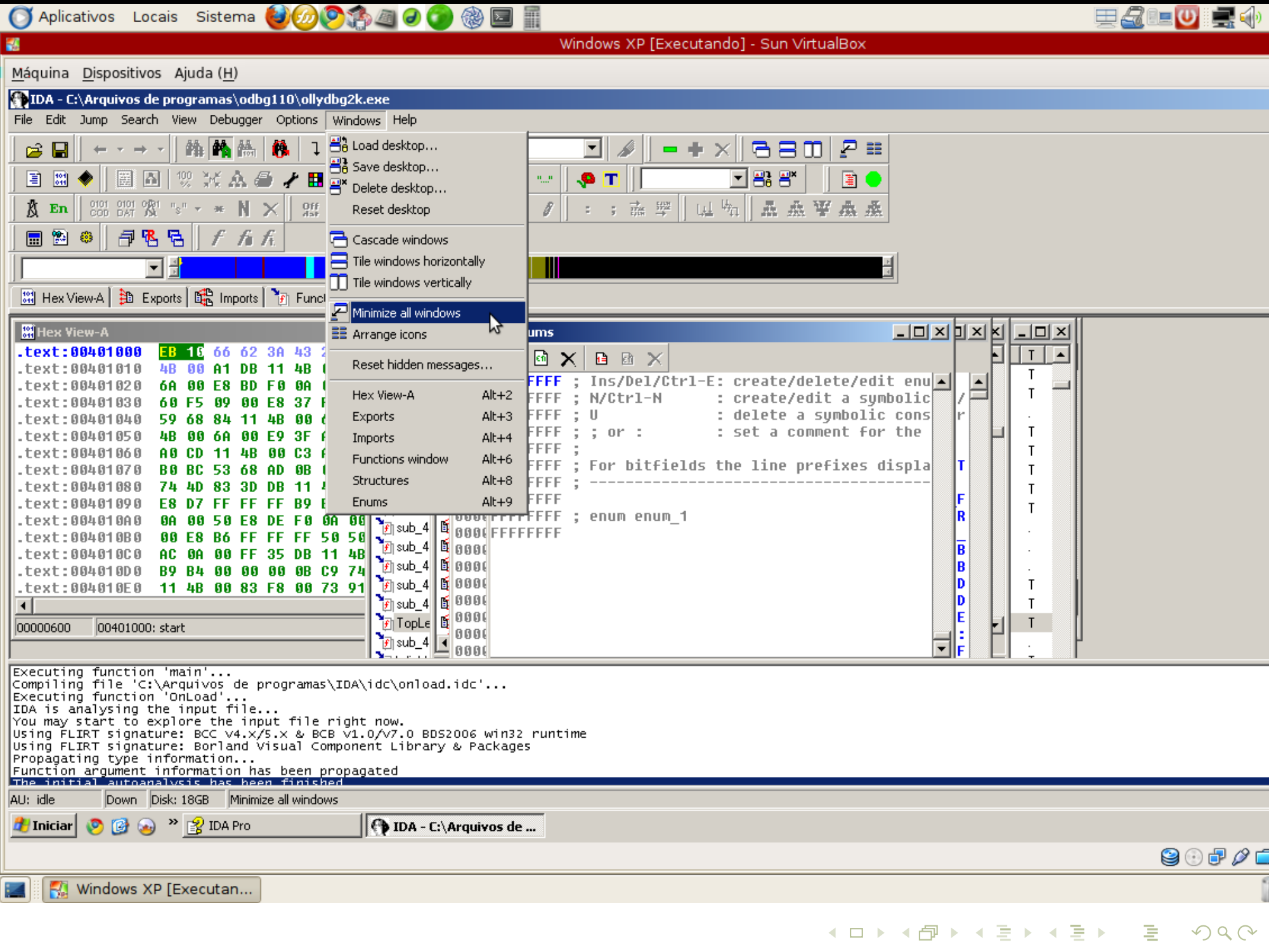

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Exports]
File Edit Jump Search View Debugger Options Windows Help
Text
EB
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
Name Address Ordinal
__GetExceptDLLinfo 00401059 1
___CPPdebugHook 004B11E8 2
start 00401000
Line 3 of 3
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

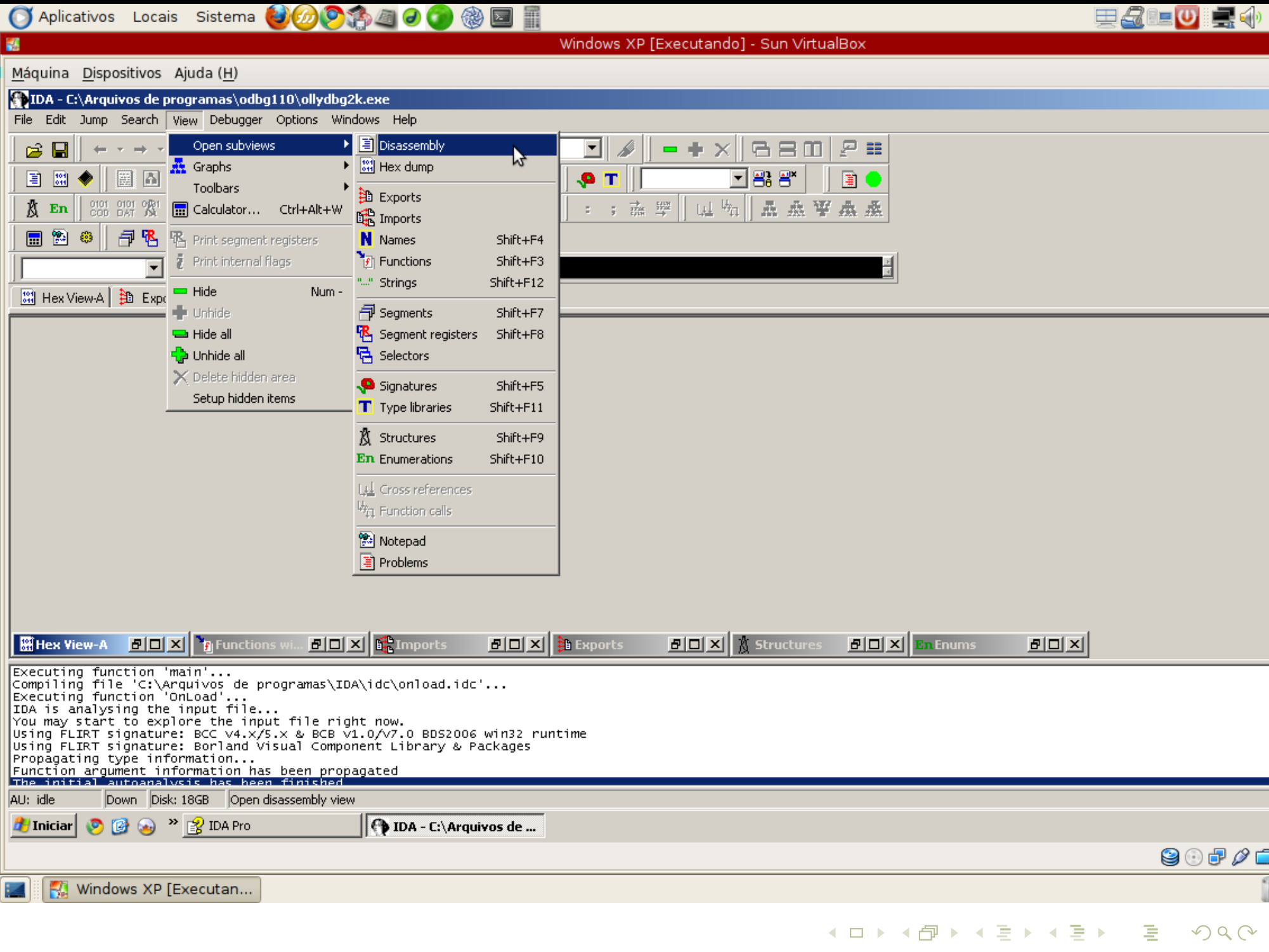

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Imports]
File Edit Jump Search View Debugger Options Windows Help
Text
EB
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
Address Ordinal Name Library
0054648C TlsFree KERNEL32
00546490 TlsGetValue KERNEL32
00546494 TlsSetValue KERNEL32
00546498 UnhandledExceptionFilter KERNEL32
0054649C VirtualAlloc KERNEL32
005464A0 VirtualFree KERNEL32
005464A4 VirtualProtectEx KERNEL32
005464A8 VirtualQuery KERNEL32
005464... VirtualQueryEx KERNEL32
005464B0 WaitForDebugEvent KERNEL32
005464B4 WideCharToMultiByte KERNEL32
005464B8 WriteFile KERNEL32
005464... WritePrivateProfileStringA KERNEL32
005464C0 WriteProcessMemory KERNEL32
005464C4 lstrcpyA KERNEL32
005464C8 lstrcpynA KERNEL32
Line 1 of 304
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executan...

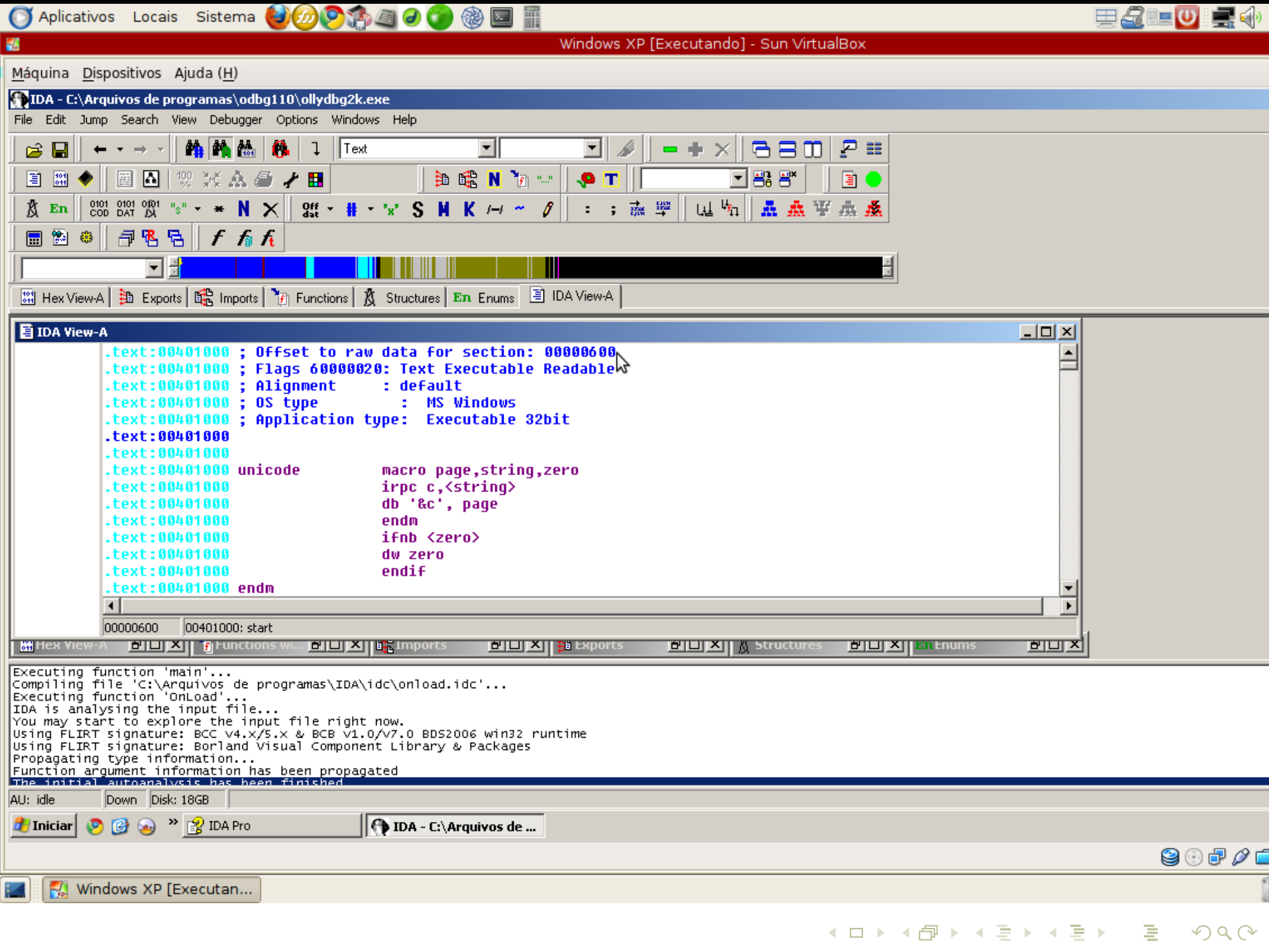

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Functions window]
File Edit Jump Search View Debugger Options Windows Help
Text
EB
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
Function name Segment Start Length R F L S B T =
sub_406AEC .text 00406AEC 00000085 R . . . B T .
sub_406B74 .text 00406B74 0000009F R . . . B T .
sub_406C14 .text 00406C14 000000B7 R . . . B . .
sub_406CCC .text 00406CCC 00000133 R . . . B . .
sub_406E00 .text 00406E00 00000010 R . . . B . .
sub_406E10 .text 00406E10 00001B7C R . . . B T .
sub_40898C .text 0040898C 00000065 R . . . B T .
TopLevelExceptionFilter .text 004089F4 0000050E R . . . B T .
sub_408F04 .text 00408F04 00000376 R . . . B . .
WinMain .text 0040927C 00002F7F R . . . B T .
sub_40C20C .text 0040C20C 00000029 R . . . B . .
sub_40C235 .text 0040C235 0000002D R . . . B . .
sub_40C262 .text 0040C262 00000034 R . . . B . .
sub_40C296 .text 0040C296 00000041 R . . . B . .
sub_40C2D7 .text 0040C2D7 00000054 R . . . B . .
Line 119 of 2105
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

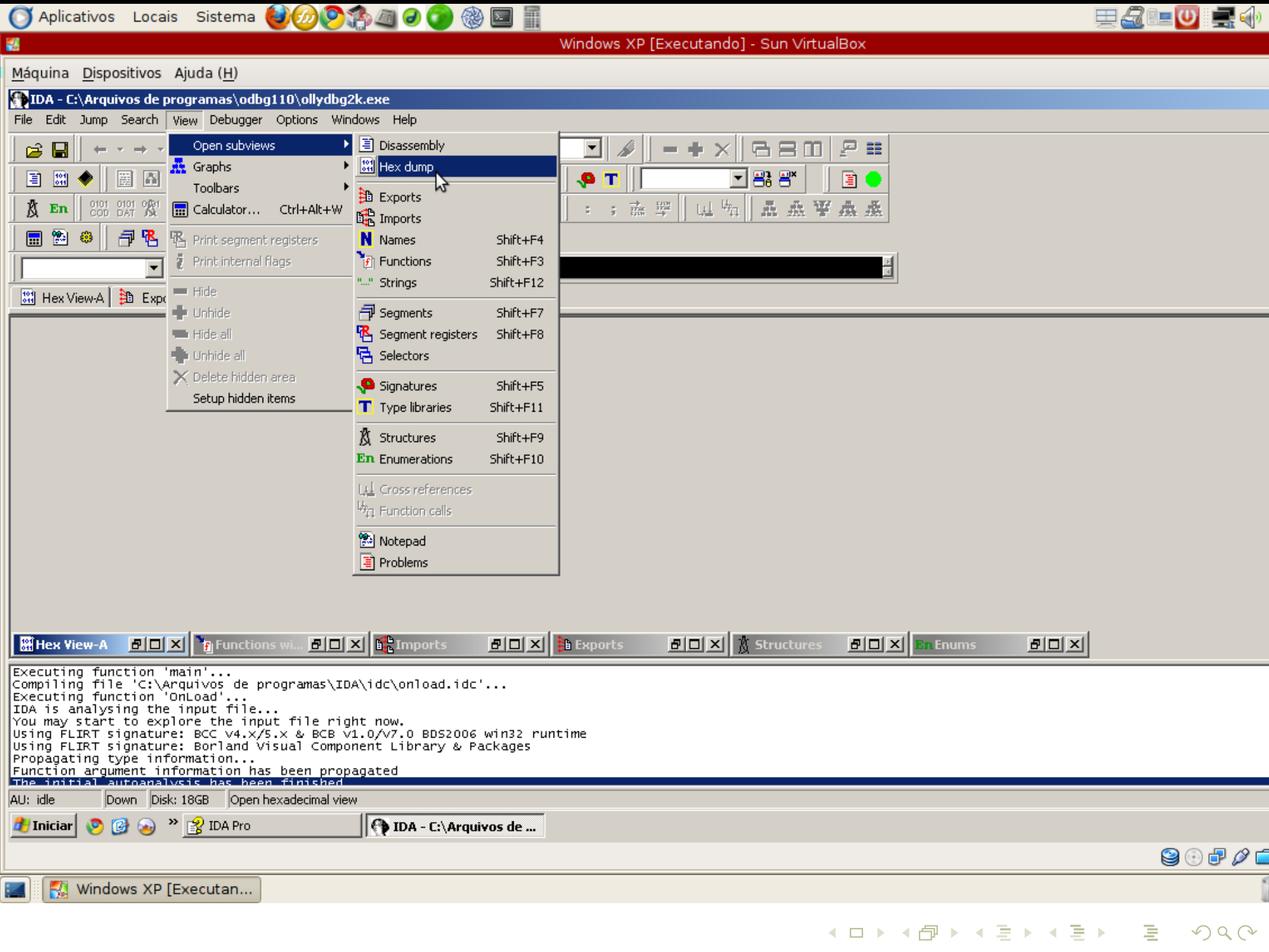

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Structures]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
Delete a structure/union type (Del)
00000000 ; D/A/* : create structure member (data/ascii/array)
00000000 ; N : rename structure or structure member
00000000 ; U : delete structure member
00000000 ; [00000018 BYTES. COLLAPSED STRUCT FILE. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [0000000C BYTES. COLLAPSED STRUCT _SECURITY_ATTRIBUTES. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [0000001C BYTES. COLLAPSED STRUCT SCROLLINFO. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000034 BYTES. COLLAPSED STRUCT _BY_HANDLE_FILE_INFORMATION. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000008 BYTES. COLLAPSED STRUCT FILETIME. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000140 BYTES. COLLAPSED STRUCT _WIN32_FIND_DATAA. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000008 BYTES. COLLAPSED STRUCT tagDEC::$39B806103C98F97C07942DA0ACE39984::$5AFDB51338AAFE7EC1FC612D34927DE9. PRESS KEYPAD "+"
00000000 ; [00000008 BYTES. COLLAPSED UNION tagDEC::$39B806103C98F97C07942DA0ACE39984. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000002 BYTES. COLLAPSED STRUCT tagDEC::$D1DFB603935916AF65F48572A60C3F86::$9CA409AEA6EFE313C25D80A08C582B39. PRESS KEYPAD "+"
00000000 ; [00000002 BYTES. COLLAPSED UNION tagDEC::$D1DFB603935916AF65F48572A60C3F86. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000010 BYTES. COLLAPSED STRUCT DECIMAL. PRESS KEYPAD "+" TO EXPAND]
00000000 ; [00000008 BYTES. COLLAPSED STRUCT tagVARIANT::$::__tagVARIANT::$5DA53A1D750C2CF4E108C7EDDBDD55F9::__tagBRECORD. PRESS KEYPAD "+"
1. FILE:0000
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB Delete a structure/union type (Del)
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executan...

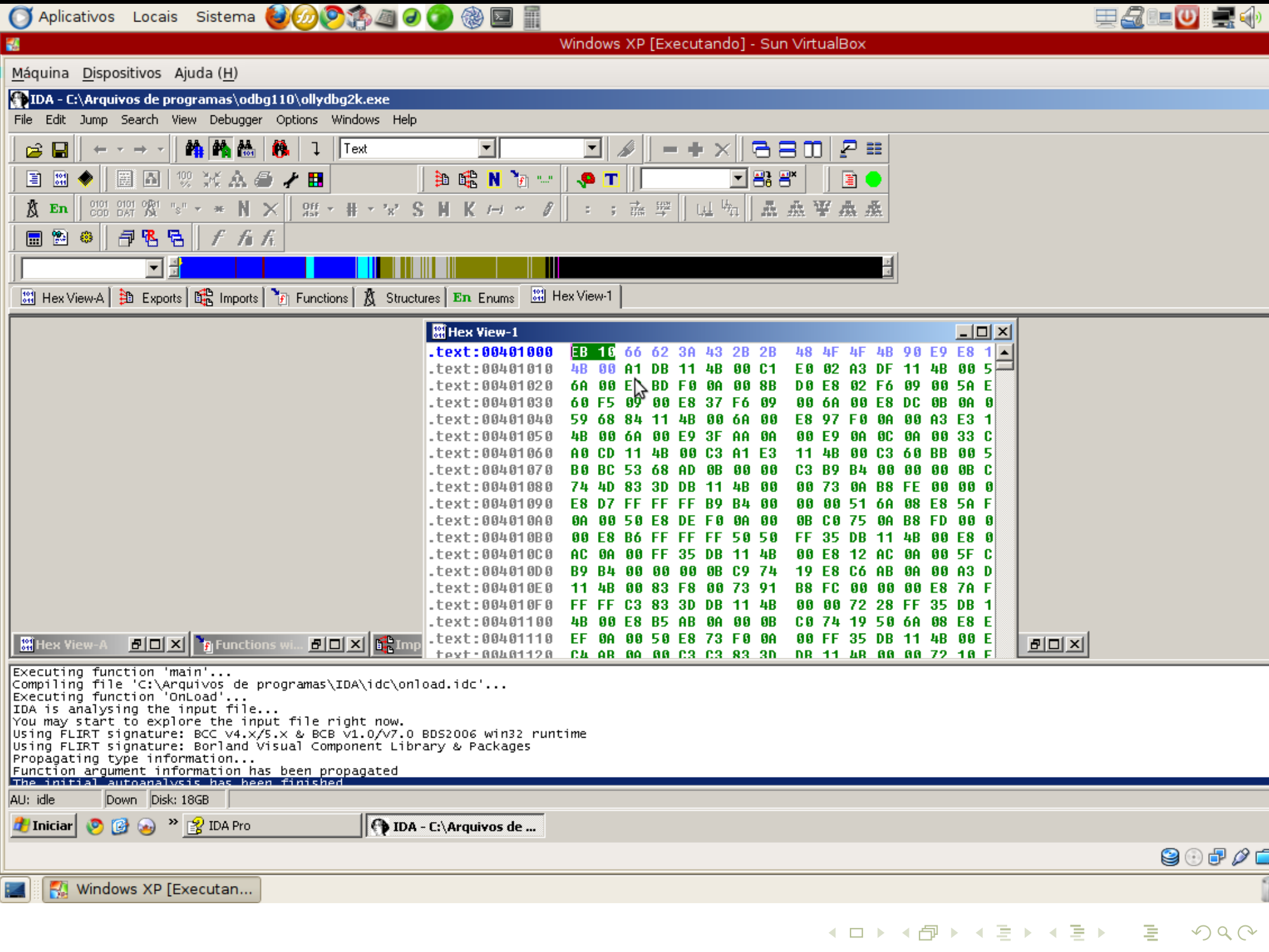

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - [Enums]
En File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A Hex View-A Exports Imports Functions Structures En Enums
FFFFFFFF ; Ins/Del/Ctrl-E: create/delete/edit enumeration types
FFFFFFFF ; N/Ctrl-N : create/edit a symbolic constant
FFFFFFFF ; U : delete a symbolic constant
FFFFFFFF ; ; or : : set a comment for the current item
FFFFFFFF ;
FFFFFFFF ; For bitfields the line prefixes display the bitmask
FFFFFFFF ; ---
FFFFFFFF
FFFFFFFF ; enum enum_1
FFFFFFFF
1. :FFFFFFFF
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executan...

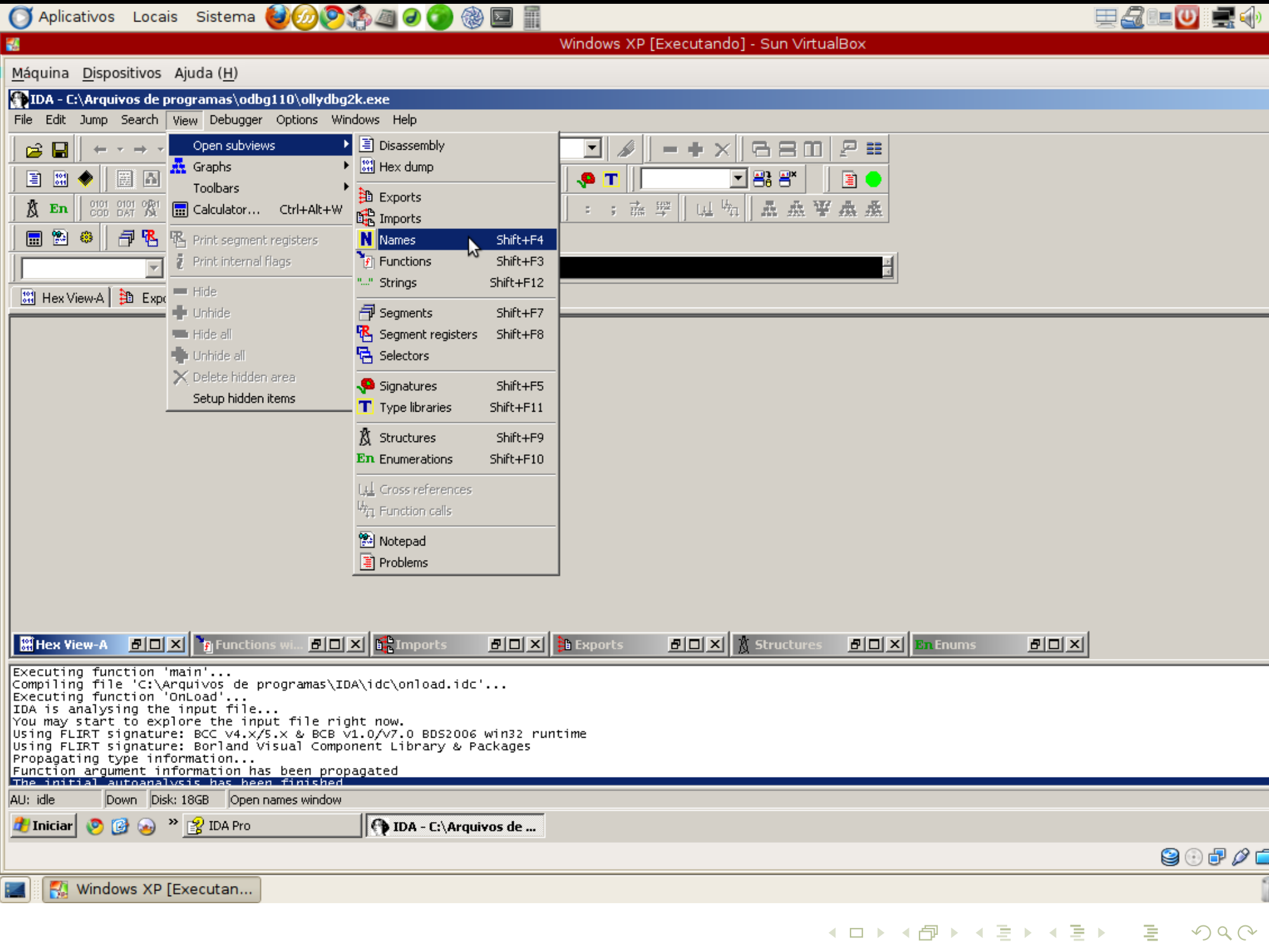

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Load desktop...
Save desktop...
Delete desktop...
Reset desktop
Cascade windows
Tile windows horizontally
Tile windows vertically
Minimize all windows
Arrange icons
Reset hidden messages...
Hex View-A Alt+2
Exports Alt+3
Imports Alt+4
Functions window Alt+6
Structures Alt+8
Enums Alt+9
Hex View-A
Exports
Imports
.text:00401000 EB 10 66 62 3A 43
.text:00401010 4B 00 A1 DB 11 4B
.text:00401020 6A 00 E8 BD F0 0A
.text:00401030 60 F5 09 00 E8 37
.text:00401040 59 68 84 11 4B 00
.text:00401050 4B 00 6A 00 E9 3F
.text:00401060 A0 CD 11 4B 00 C3
.text:00401070 B0 BC 53 68 AD 0B
.text:00401080 74 4D 83 3D DB 11
.text:00401090 E8 D7 FF FF FF B9
.text:004010A0 0A 00 50 E8 DE F0 0A 00
.text:004010B0 00 E8 B6 FF FF FF 50 50
.text:004010C0 AC 0A 00 FF 35 DB 11 4B
.text:004010D0 B9 B4 00 00 00 0B C9 74
.text:004010E0 11 4B 00 83 F8 00 73 91
00000600 00401000: start
FFFF ; Ins/Del/Ctrl-E: create/delete/edit enu
FFFF ; N/Ctrl-N : create/edit a symbolic
FFFF ; U : delete a symbolic cons
FFFF ; ; or : : set a comment for the
FFFF ;
FFFF ; For bitfields the line prefixes displa
FFFF ; ----------
FFFF
FFFFFFFF ; enum enum_1
FFFFFFFF
sub_4
TopLe
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Minimize all windows
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

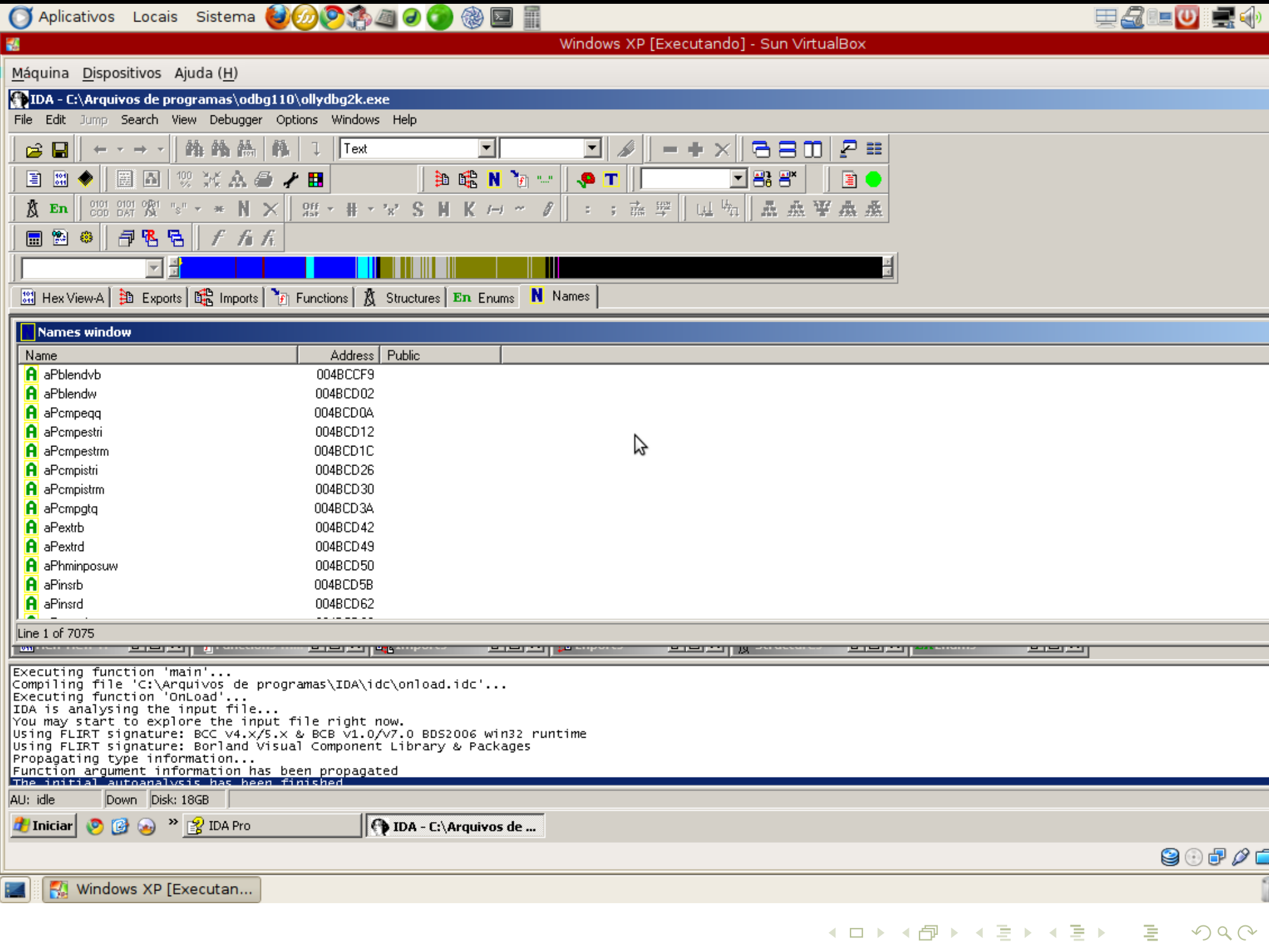

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide Num -
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Functions wi...
Imports
Exports
Structures
Enums
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open disassembly view
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

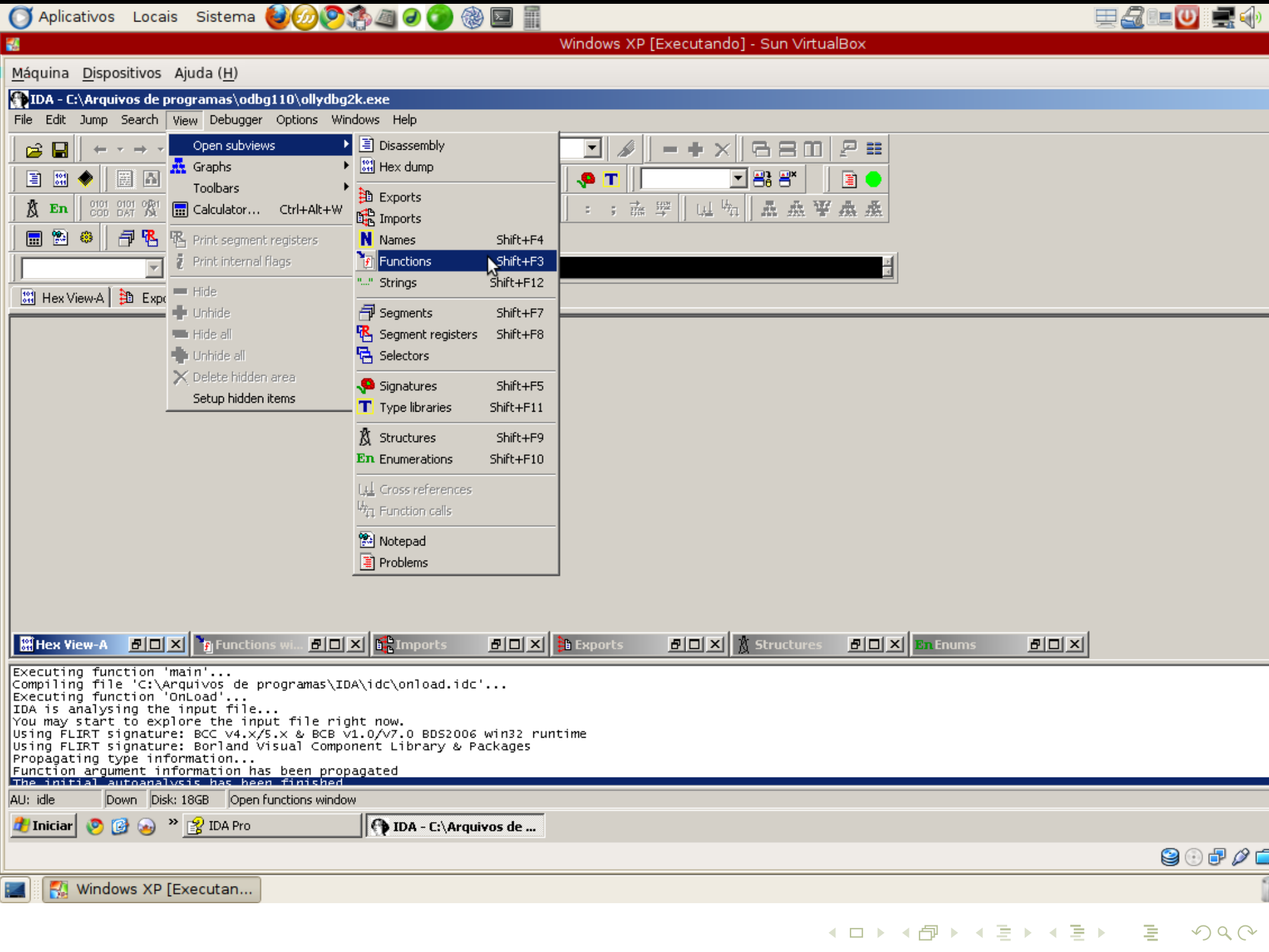

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Functions Structures Enums IDA View-A
IDA View-A
.text:00401000 ; Offset to raw data for section: 00000600
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment : default
.text:00401000 ; OS type : MS Windows
.text:00401000 ; Application type: Executable 32bit
.text:00401000
.text:00401000
.text:00401000 unicode macro page,string,zero
.text:00401000 irpc c,<string>
.text:00401000 db '&c', page
.text:00401000 endm
.text:00401000 ifnb <zero>
.text:00401000 dw zero
.text:00401000 endif
.text:00401000 endm
00000600
00401000: start
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

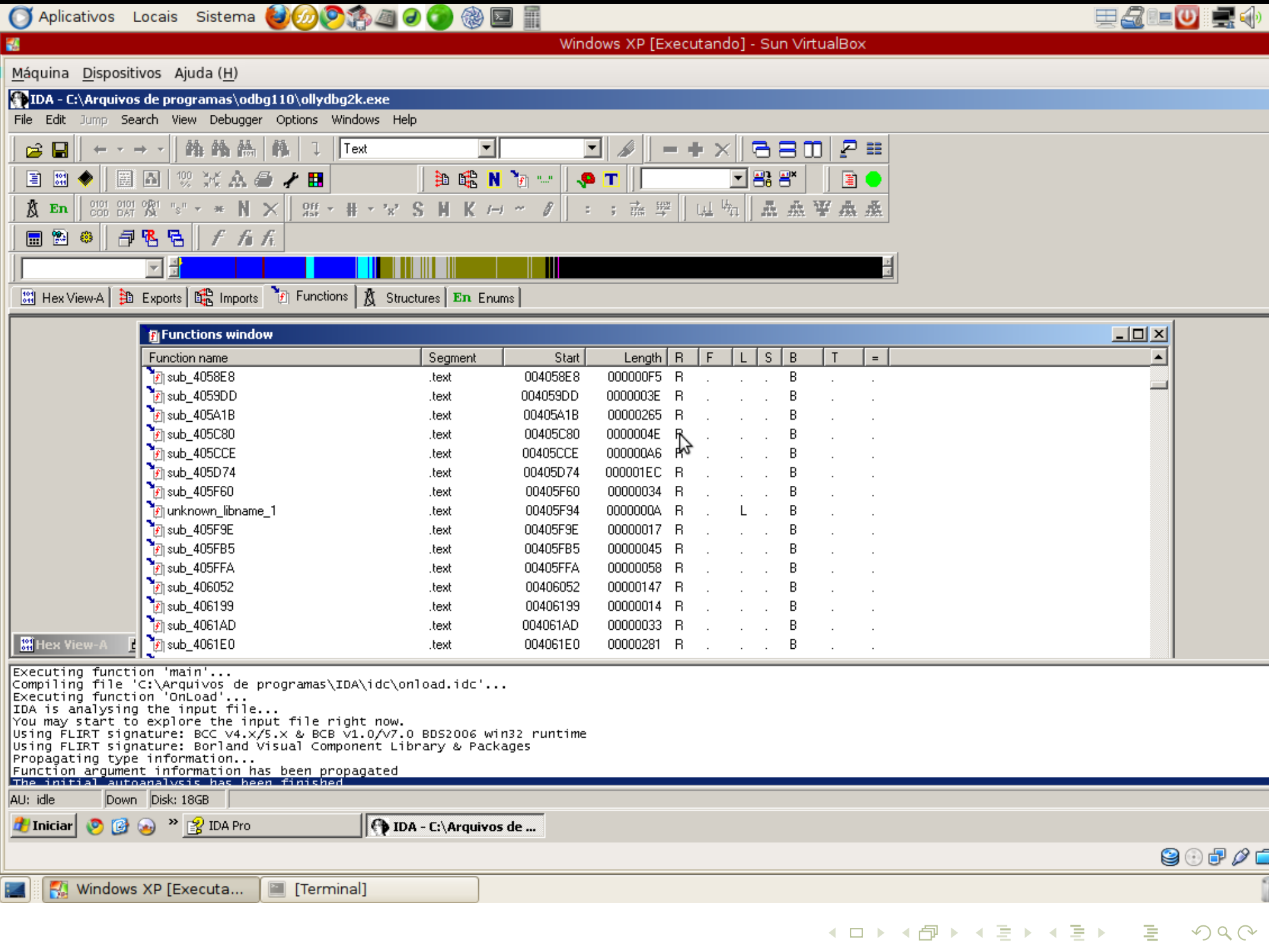

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Functions wi...
Imports
Exports
Structures
Enums
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open hexadecimal view
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

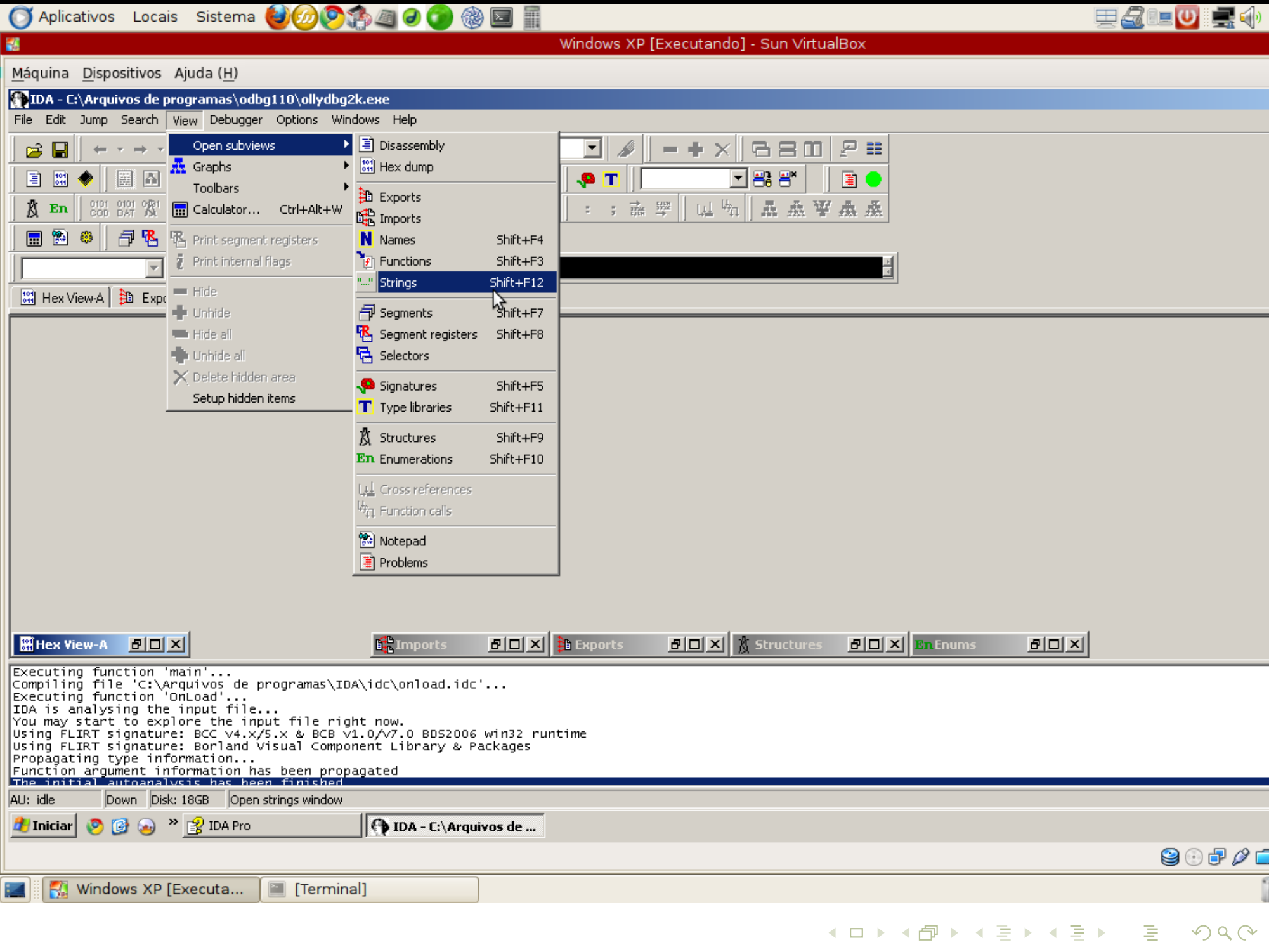

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Functions Structures En Enums Hex View-1
Hex View-1
.text:00401000 EB 10 66 62 3A 43 2B 2B 48 4F 4F 4B 90 E9 E8 1
.text:00401010 4B 00 A1 DB 11 4B 00 C1 E0 02 A3 DF 11 4B 00 5
.text:00401020 6A 00 E8 BD F0 0A 00 8B D0 E8 02 F6 09 00 5A E
.text:00401030 60 F5 09 00 E8 37 F6 09 00 6A 00 E8 DC 0B 0A 0
.text:00401040 59 68 84 11 4B 00 6A 00 E8 97 F0 0A 00 A3 E3 1
.text:00401050 4B 00 6A 00 E9 3F AA 0A 00 E9 0A 0C 0A 00 33 C
.text:00401060 A0 CD 11 4B 00 C3 A1 E3 11 4B 00 C3 60 BB 00 5
.text:00401070 B0 BC 53 68 AD 0B 00 00 C3 B9 B4 00 00 00 0B C
.text:00401080 74 4D 83 3D DB 11 4B 00 00 73 0A B8 FE 00 00 0
.text:00401090 E8 D7 FF FF FF B9 B4 00 00 00 51 6A 08 E8 5A F
.text:004010A0 0A 00 50 E8 DE F0 0A 00 0B C0 75 0A B8 FD 00 0
.text:004010B0 00 E8 B6 FF FF FF 50 50 FF 35 DB 11 4B 00 E8 0
.text:004010C0 AC 0A 00 FF 35 DB 11 4B 00 E8 12 AC 0A 00 5F C
.text:004010D0 B9 B4 00 00 00 0B C9 74 19 E8 C6 AB 0A 00 A3 D
.text:004010E0 11 4B 00 83 F8 00 73 91 B8 FC 00 00 00 E8 7A F
.text:004010F0 FF FF C3 83 3D DB 11 4B 00 00 72 28 FF 35 DB 1
.text:00401100 4B 00 E8 B5 AB 0A 00 0B C0 74 19 50 6A 08 E8 E
.text:00401110 EF 0A 00 50 E8 73 F0 0A 00 FF 35 DB 11 4B 00 E
Hex View-A
Functions wi...
Imp
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

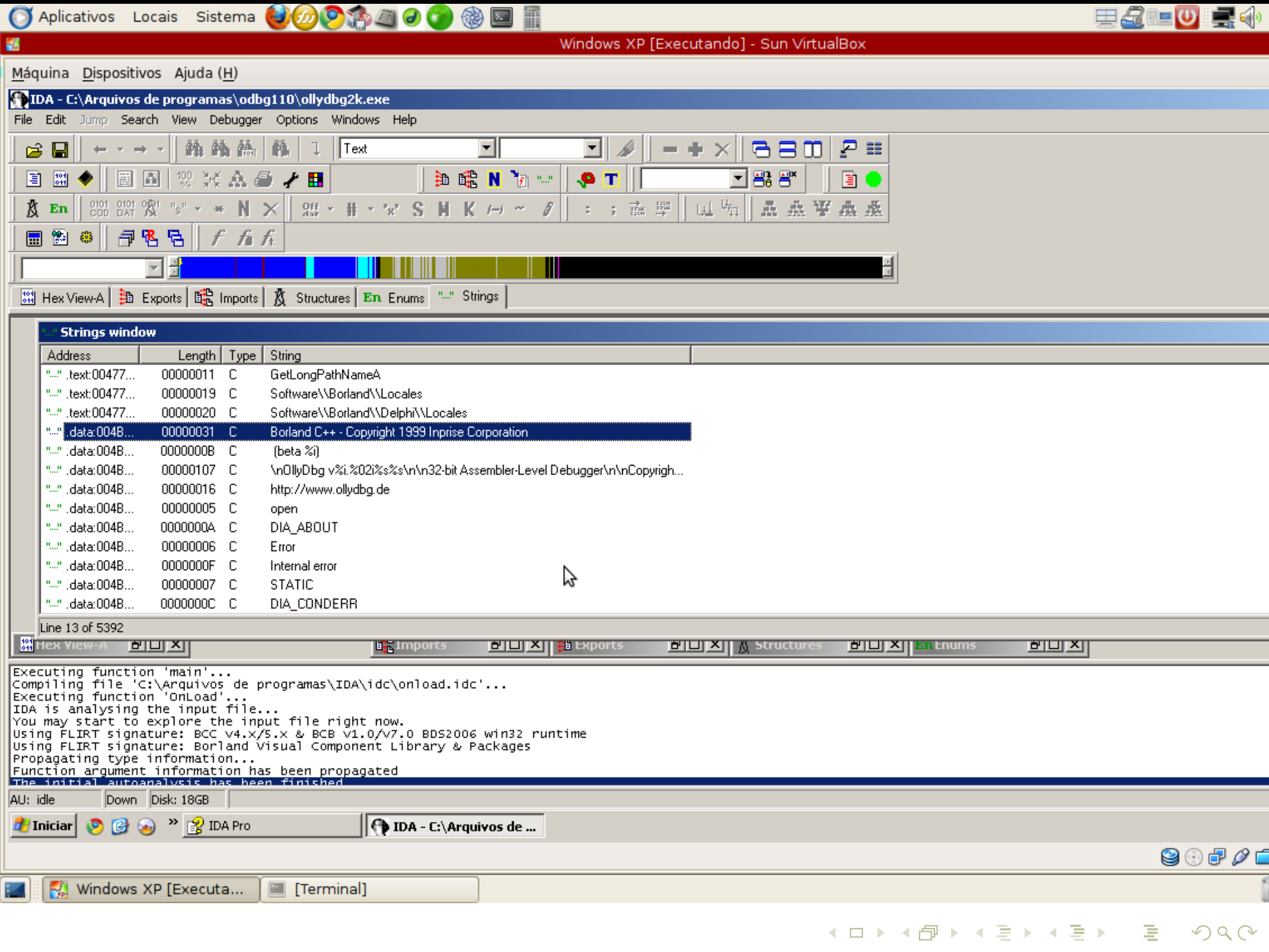

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Functions wi...
Imports
Exports
Structures
Enums
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open names window
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Functions Structures En Enums Names
Names window
Name Address Public
aPblendvb 004BCCF9
aPblendw 004BCD02
aPcmpeqq 004BCD0A
aPcmpestri 004BCD12
aPcmpestrm 004BCD1C
aPcmpistri 004BCD26
aPcmpistrm 004BCD30
aPcmpgtq 004BCD3A
aPextrb 004BCD42
aPextrd 004BCD49
aPhminposuw 004BCD50
aPinsrb 004BCD5B
aPinsrd 004BCD62
Line 1 of 7075
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executan...


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Functions wi...
Imports
Exports
Structures
Enums
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open functions window
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executan...

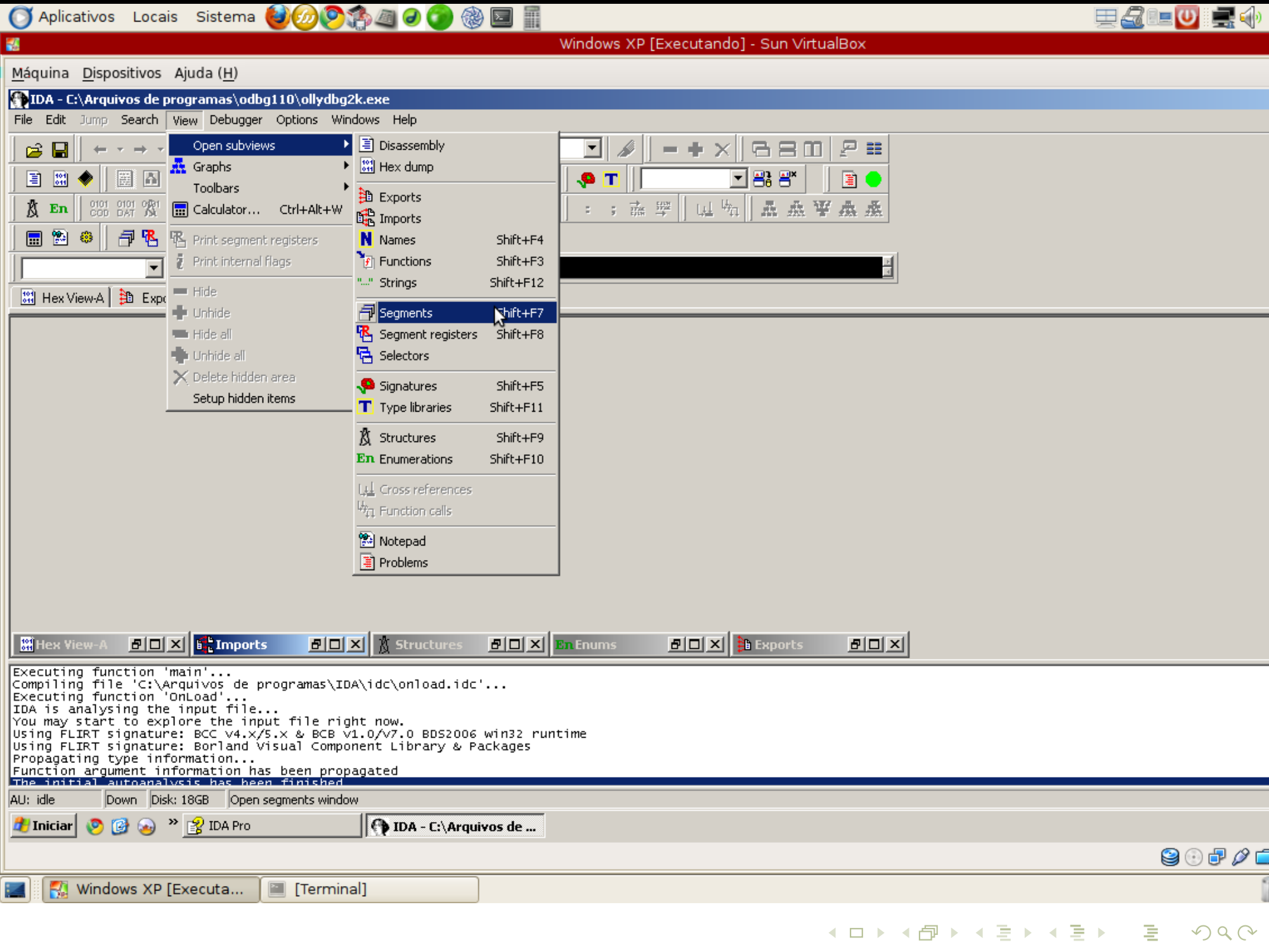

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Functions Structures En Enums
Functions window
Function name Segment Start Length R F L S B T =
sub_4058E8 .text 004058E8 000000F5 R . . . B . .
sub_4059DD .text 004059DD 0000003E R . . . B . .
sub_405A1B .text 00405A1B 00000265 R . . . B . .
sub_405C80 .text 00405C80 0000004E R . . . B . .
sub_405CCE .text 00405CCE 000000A6 R . . . B . .
sub_405D74 .text 00405D74 000001EC R . . . B . .
sub_405F60 .text 00405F60 00000034 R . . . B . .
unknown_libname_1 .text 00405F94 0000000A R . L . B . .
sub_405F9E .text 00405F9E 00000017 R . . . B . .
sub_405FB5 .text 00405FB5 00000045 R . . . B . .
sub_405FFA .text 00405FFA 00000058 R . . . B . .
sub_406052 .text 00406052 00000147 R . . . B . .
sub_406199 .text 00406199 00000014 R . . . B . .
sub_4061AD .text 004061AD 00000033 R . . . B . .
sub_4061E0 .text 004061E0 00000281 R . . . B . .
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]

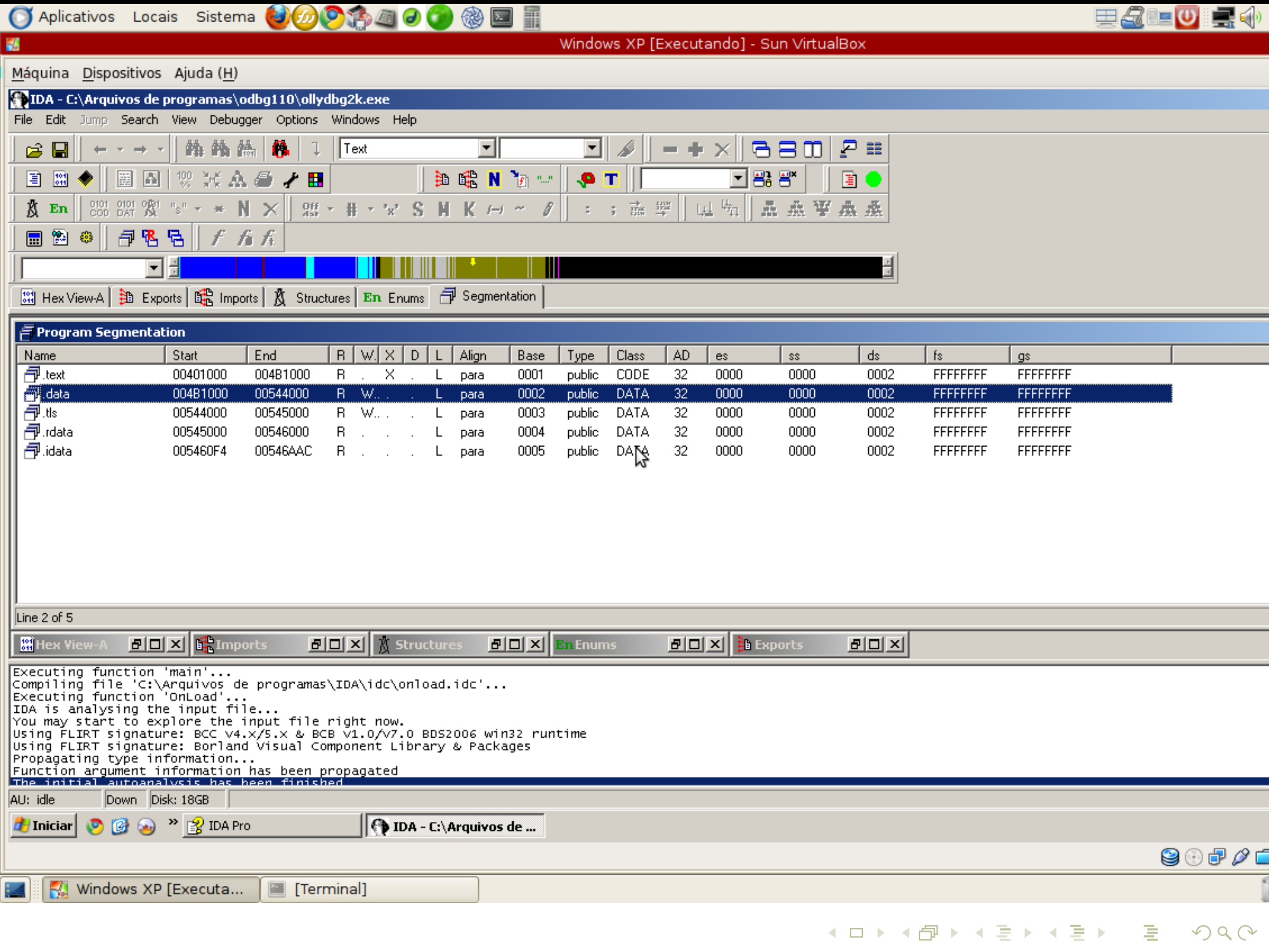

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Imports
Exports
Structures
Enums
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open strings window
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

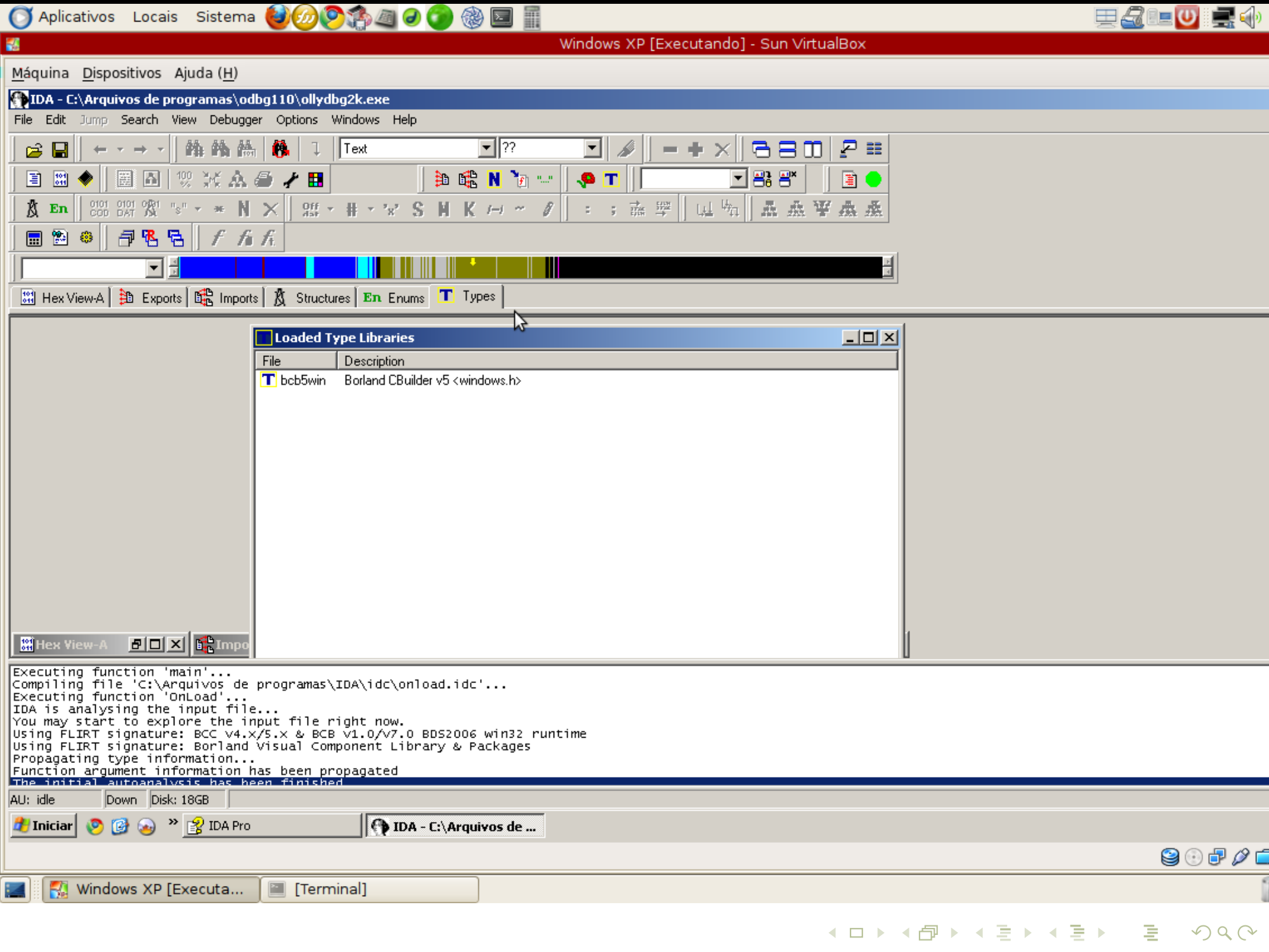

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Structures En Enums Strings
Strings window
Address Length Type String
.text:00477... 00000011 C GetLongPathNameA
.text:00477... 00000019 C Software\\Borland\\Locales
.text:00477... 00000020 C Software\\Borland\\Delphi\\Locales
.data:004B... 00000031 C Borland C++ - Copyright 1999 Inprise Corporation
.data:004B... 0000000B C (beta %i)
.data:004B... 00000107 C \nOllyDbg v%i.%02i%s%s\n\n32-bit Assembler-Level Debugger\n\nCopyrigh...
.data:004B... 00000016 C http://www.ollydbg.de
.data:004B... 00000005 C open
.data:004B... 0000000A C DIA_ABOUT
.data:004B... 00000006 C Error
.data:004B... 0000000F C Internal error
.data:004B... 00000007 C STATIC
.data:004B... 0000000C C DIA_CONDERR
Line 13 of 5392
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]

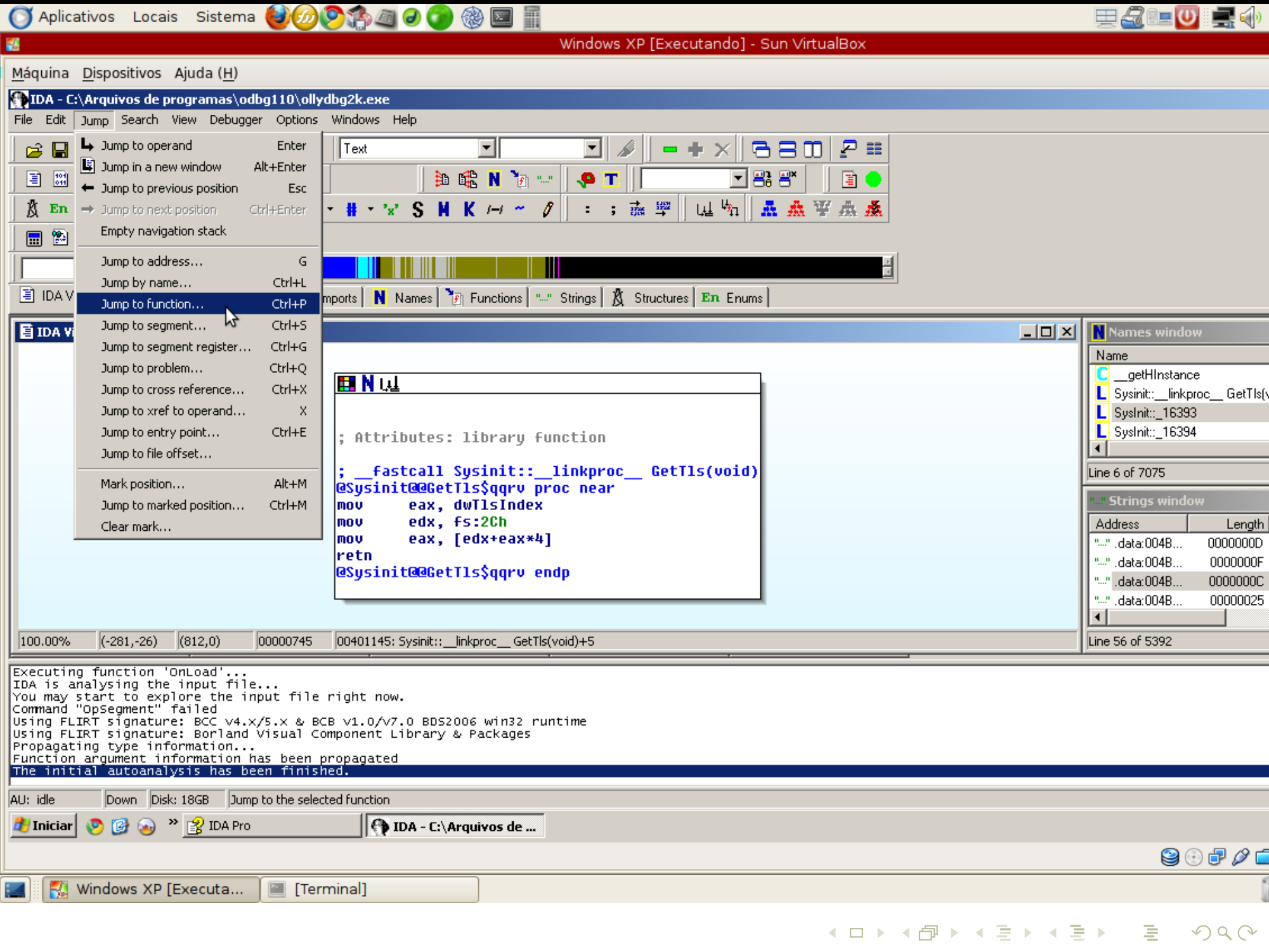
Nome de funções, Strings (e os pontos onde elas são referenciadas no programa) e os nomes das seções (usados por instruções como `calls`, `jumps`, e `bss buffers`) são os principais fatores de referência na busca das informações buscadas pela engenharia reversa.

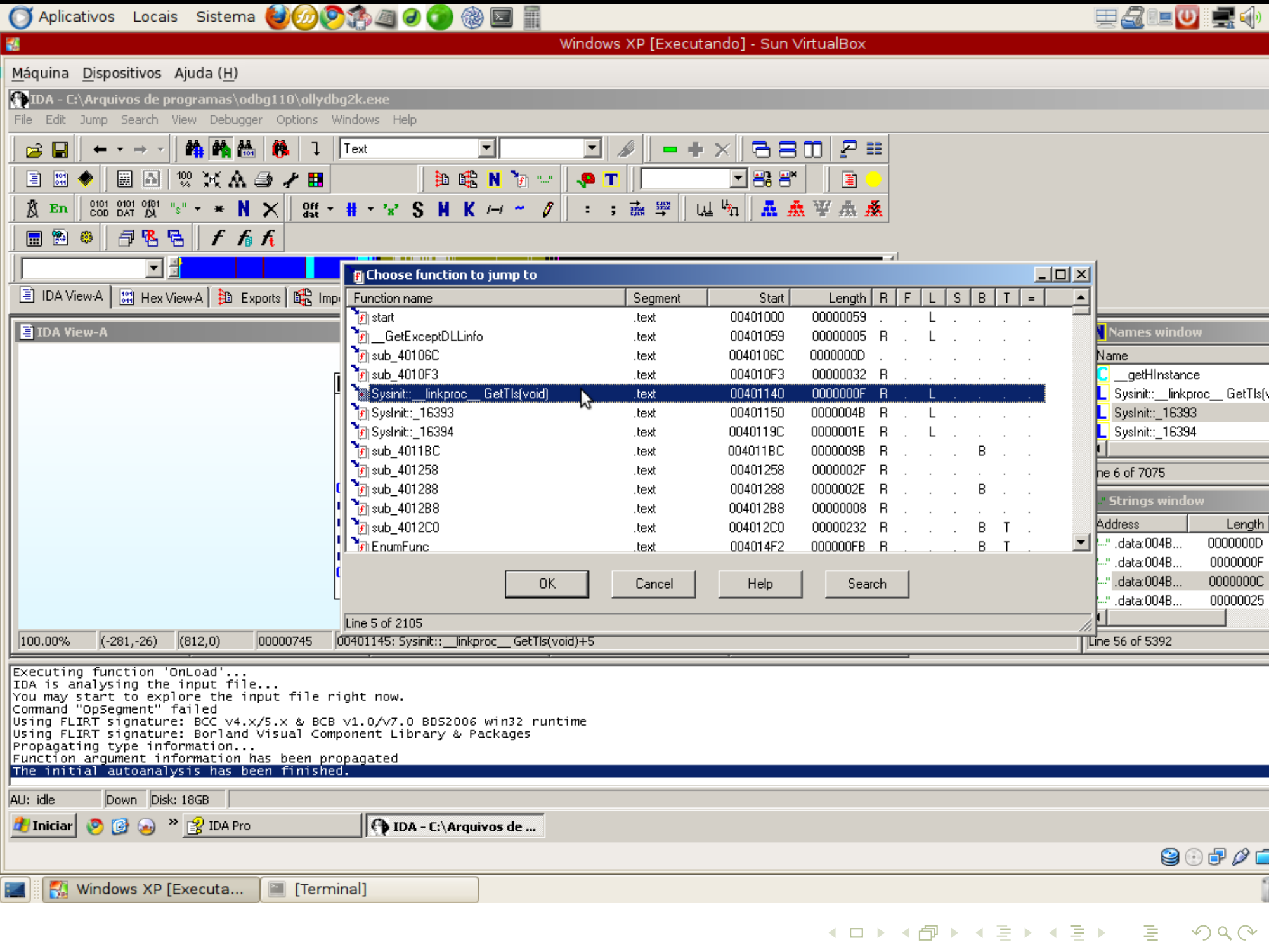
As principais técnicas de anticracking consiste em eliminar, encriptar ou obfuscar essas informações, a fim de dificultar a análise do código disassemblado.

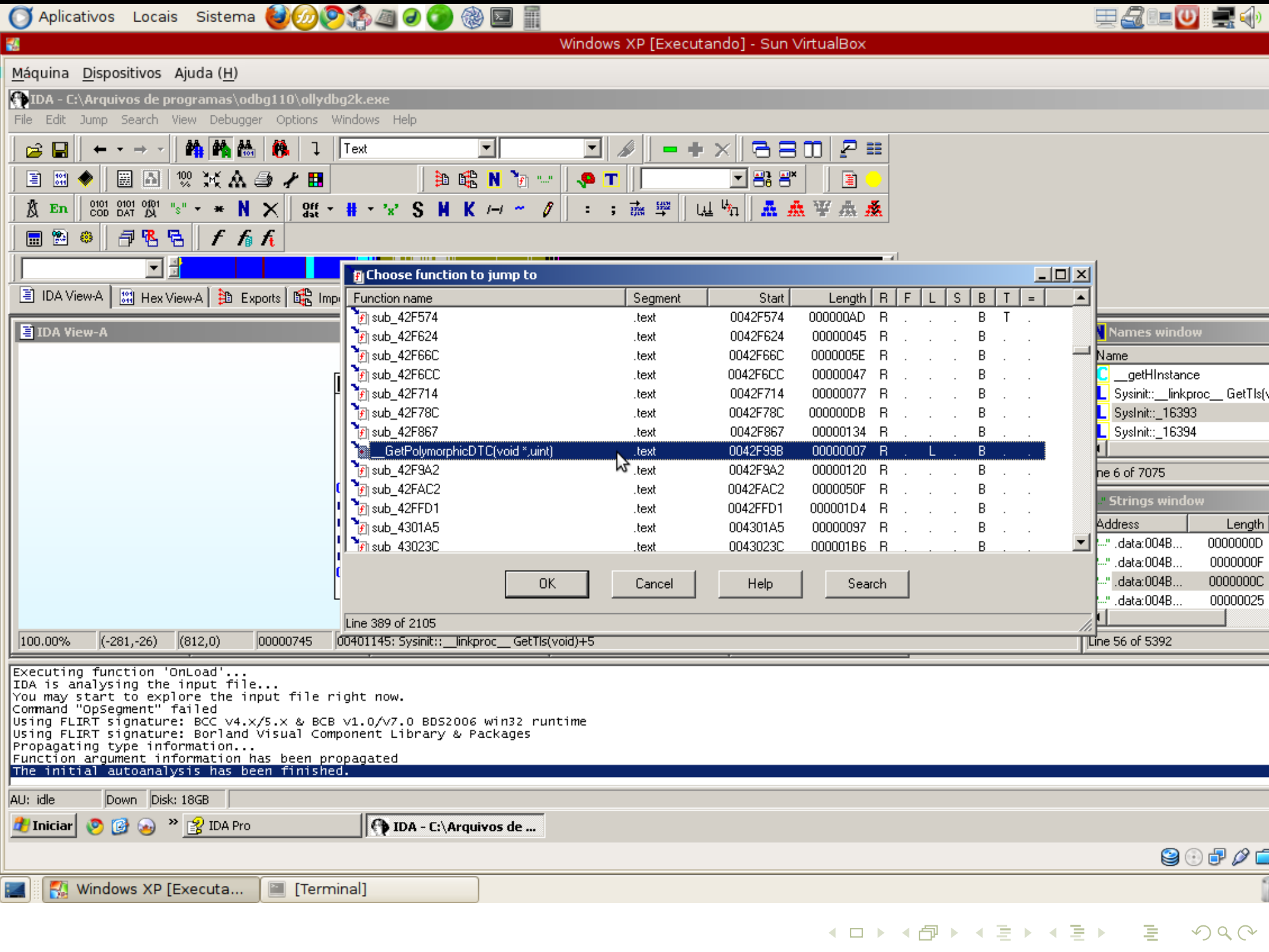

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers
Print internal flags
Hide
Unhide
Hide all
Unhide all
Delete hidden area
Setup hidden items
Disassembly
Hex dump
Exports
Imports
Names Shift+F4
Functions Shift+F3
Strings Shift+F12
Segments Shift+F7
Segment registers Shift+F8
Selectors
Signatures Shift+F5
Type libraries Shift+F11
Structures Shift+F9
Enumerations Shift+F10
Cross references
Function calls
Notepad
Problems
Hex View-A
Imports
Structures
Enums
Exports
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Open segments window
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

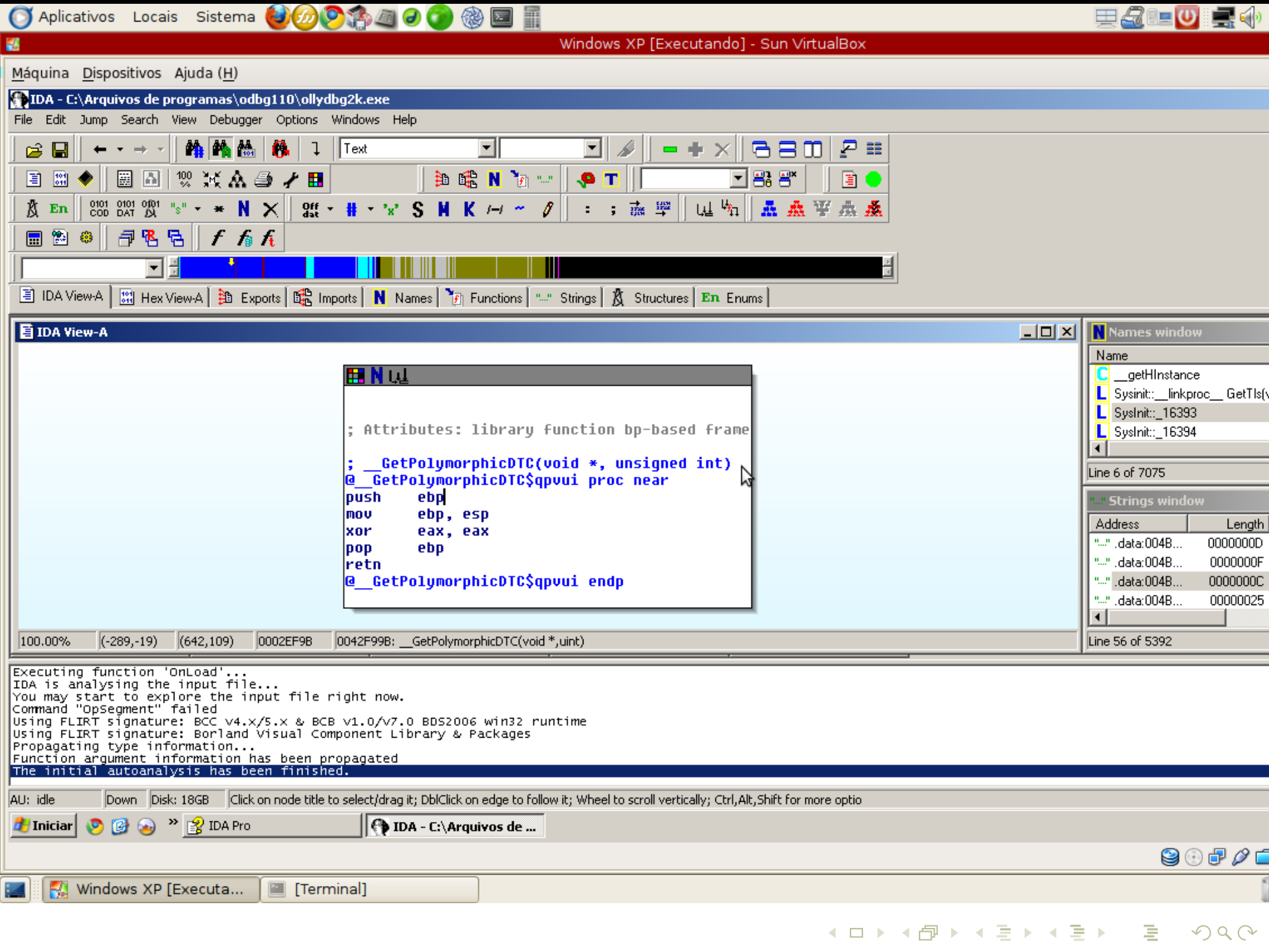

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
Hex View-A Exports Imports Structures Enums Segmentation
Program Segmentation
Name Start End R W X D L Align Base Type Class AD es ss ds fs gs
.text 00401000 004B1000 R . X . L para 0001 public CODE 32 0000 0000 0002 FFFFFFFF FFFFFFFF
.data 004B1000 00544000 R W . . L para 0002 public DATA 32 0000 0000 0002 FFFFFFFF FFFFFFFF
.tls 00544000 00545000 R W . . L para 0003 public DATA 32 0000 0000 0002 FFFFFFFF FFFFFFFF
.rdata 00545000 00546000 R . . L para 0004 public DATA 32 0000 0000 0002 FFFFFFFF FFFFFFFF
.idata 005460F4 00546AAC R . . L para 0005 public DATA 32 0000 0000 0002 FFFFFFFF FFFFFFFF
Line 2 of 5
Hex View-A Imports Structures Enums Exports
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]

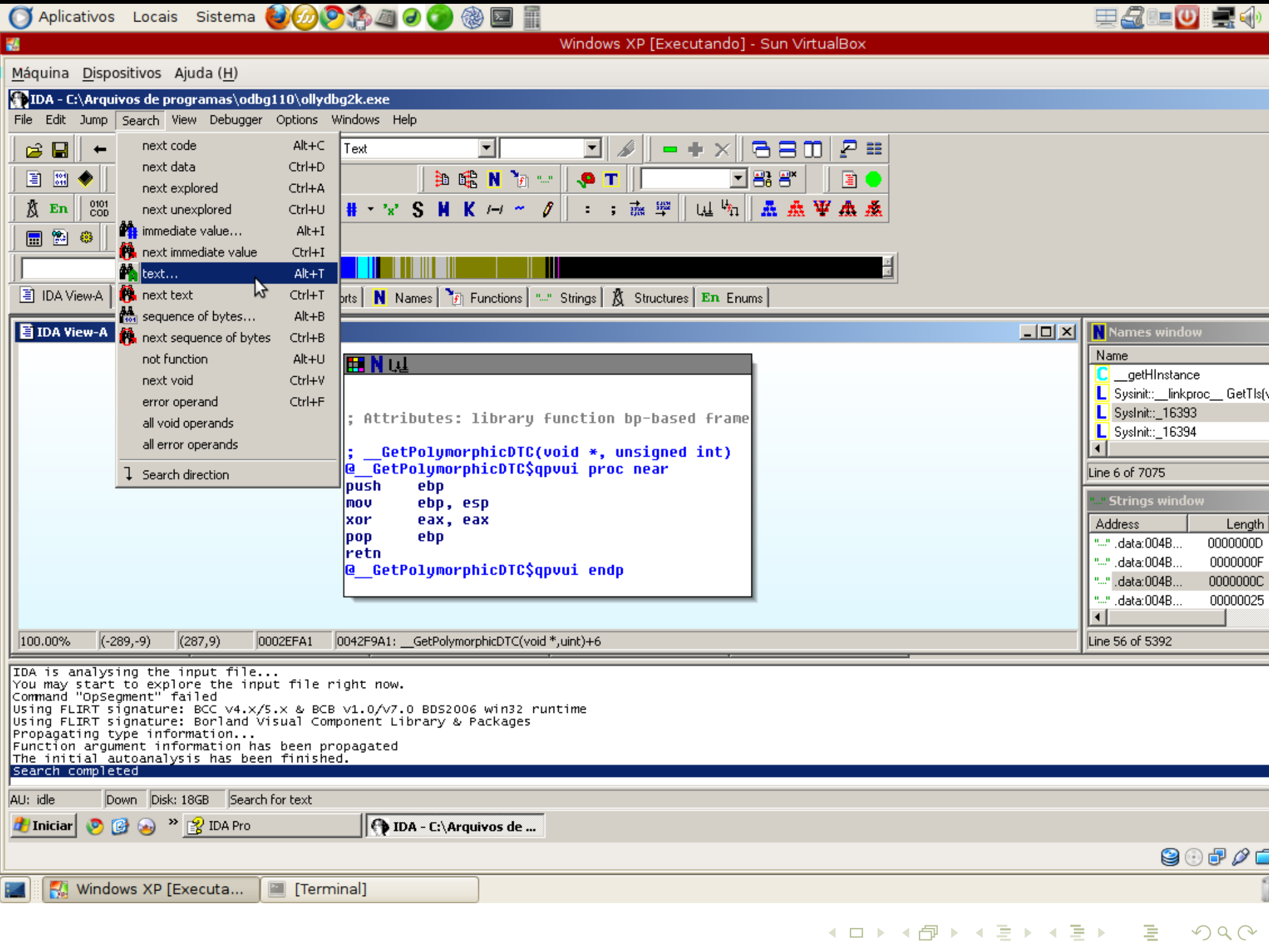

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
??
Hex View-A
Exports
Imports
Structures
Enums
Types
Loaded Type Libraries
File
Description
bcb5win
Borland CBuilder v5 <windows.h>
Executing function 'main'...
Compiling file 'C:\Arquivos de programas\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

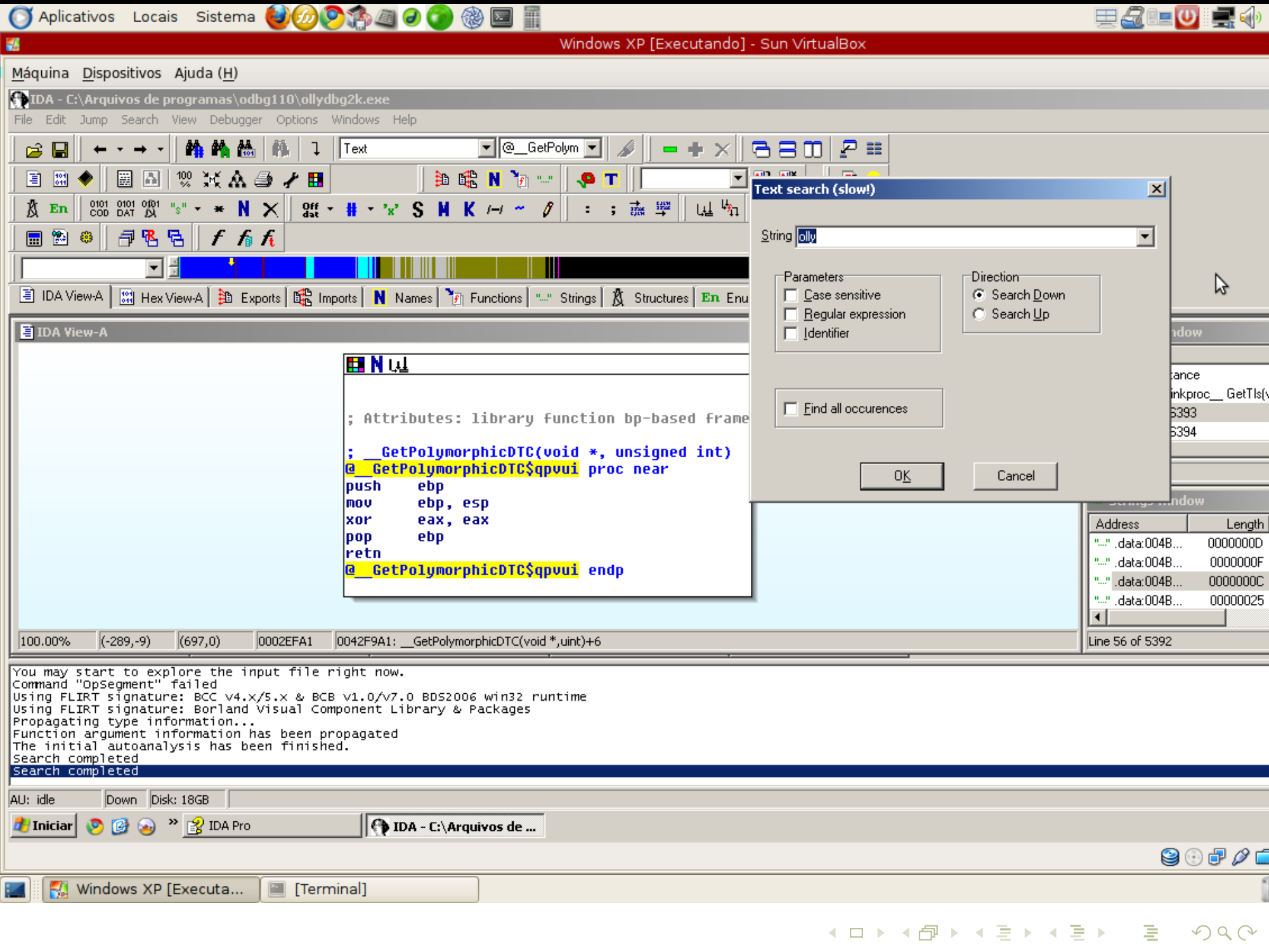

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Jump to operand Enter
Jump in a new window Alt+Enter
Jump to previous position Esc
Jump to next position Ctrl+Enter
Empty navigation stack
Jump to address... G
Jump by name... Ctrl+L
Jump to function... Ctrl+P
Jump to segment... Ctrl+S
Jump to segment register... Ctrl+G
Jump to problem... Ctrl+Q
Jump to cross reference... Ctrl+X
Jump to xref to operand... X
Jump to entry point... Ctrl+E
Jump to file offset...
Mark position... Alt+M
Jump to marked position... Ctrl+M
Clear mark...
Text
Names Functions Strings Structures Enums
; Attributes: library function
; __fastcall Sysinit::__linkproc__ GetTls(void)
@Sysinit@@GetTls$qqrv proc near
mov eax, dwTlsIndex
mov edx, fs:2Ch
mov eax, [edx+eax*4]
retn
@Sysinit@@GetTls$qqrv endp
Names window
Name
__getHInstance
Sysinit::__linkproc__ GetTls(v
SysInit::_16393
SysInit::_16394
Line 6 of 7075
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
Line 56 of 5392
100.00% (-281,-26) (812,0) 00000745 00401145: Sysinit::__linkproc__ GetTls(void)+5
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 18GB Jump to the selected function
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

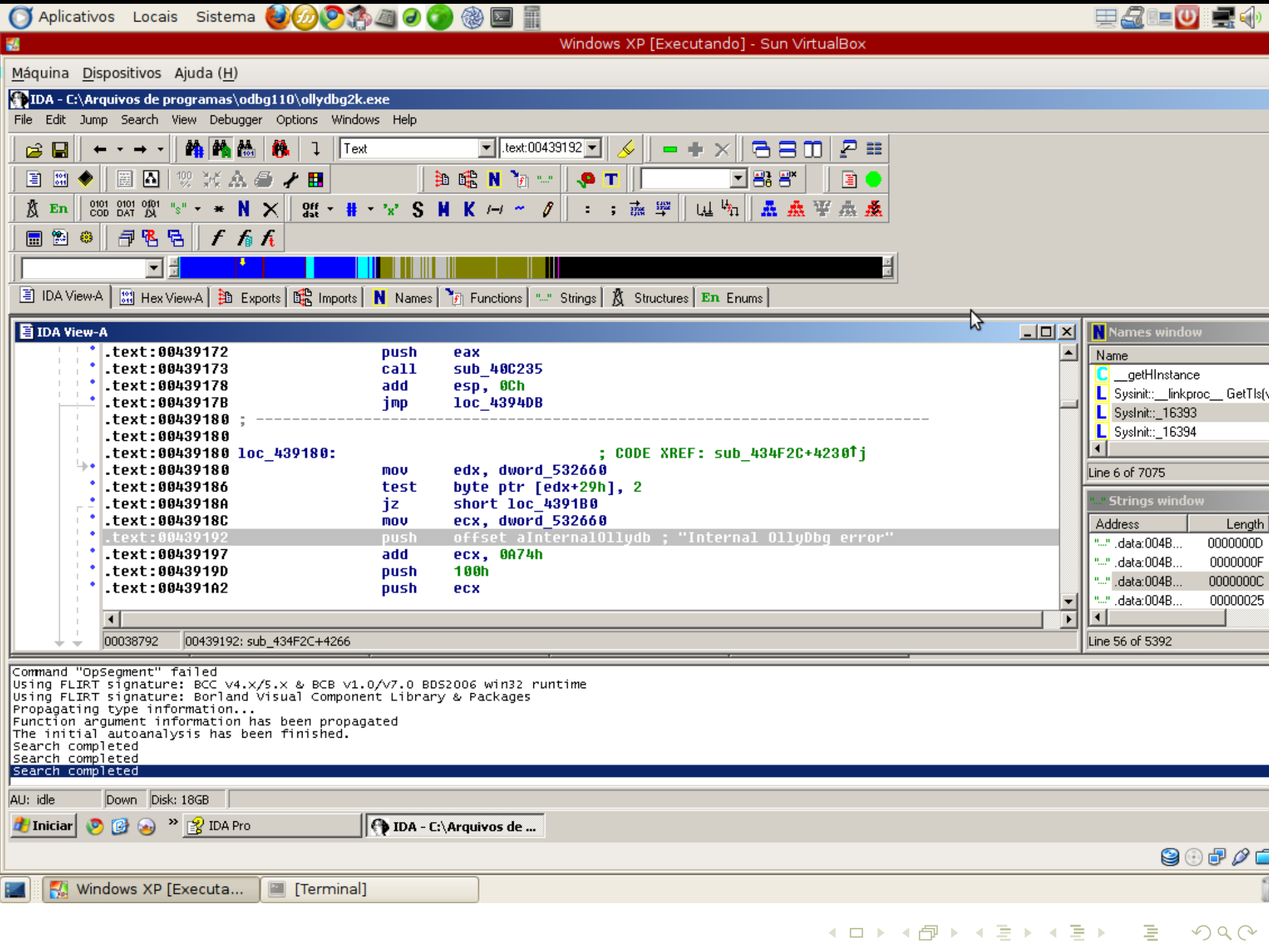

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Choose function to jump to
Function name Segment Start Length R F L S B T =
start .text 00401000 00000059 . . L . . . .
__GetExceptDLLinfo .text 00401059 00000005 R . L . . . .
sub_40106C .text 0040106C 0000000D . . . . . .
sub_4010F3 .text 004010F3 00000032 R . . . . . .
Sysinit::__linkproc__GetTls(void) .text 00401140 0000000F R . L . . . .
SysInit::_16393 .text 00401150 0000004B R . L . . . .
SysInit::_16394 .text 0040119C 0000001E R . L . . . .
sub_4011BC .text 004011BC 0000009B R . . . B . .
sub_401258 .text 00401258 0000002F R . . . . . .
sub_401288 .text 00401288 0000002E R . . . B . .
sub_4012B8 .text 004012B8 00000008 R . . . . . .
sub_4012C0 .text 004012C0 00000232 R . . . B T .
EnumFunc .text 004014F2 000000FB R . . . B T .
OK Cancel Help Search
Line 5 of 2105
IDA View-A
Hex View-A
Exports
Names window
Name
__getHInstance
Sysinit::__linkproc__ GetTls(v
SysInit::_16393
SysInit::_16394
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
100.00% (-281,-26) (812,0) 00000745 00401145: Sysinit::__linkproc__GetTls(void)+5
Line 56 of 5392
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

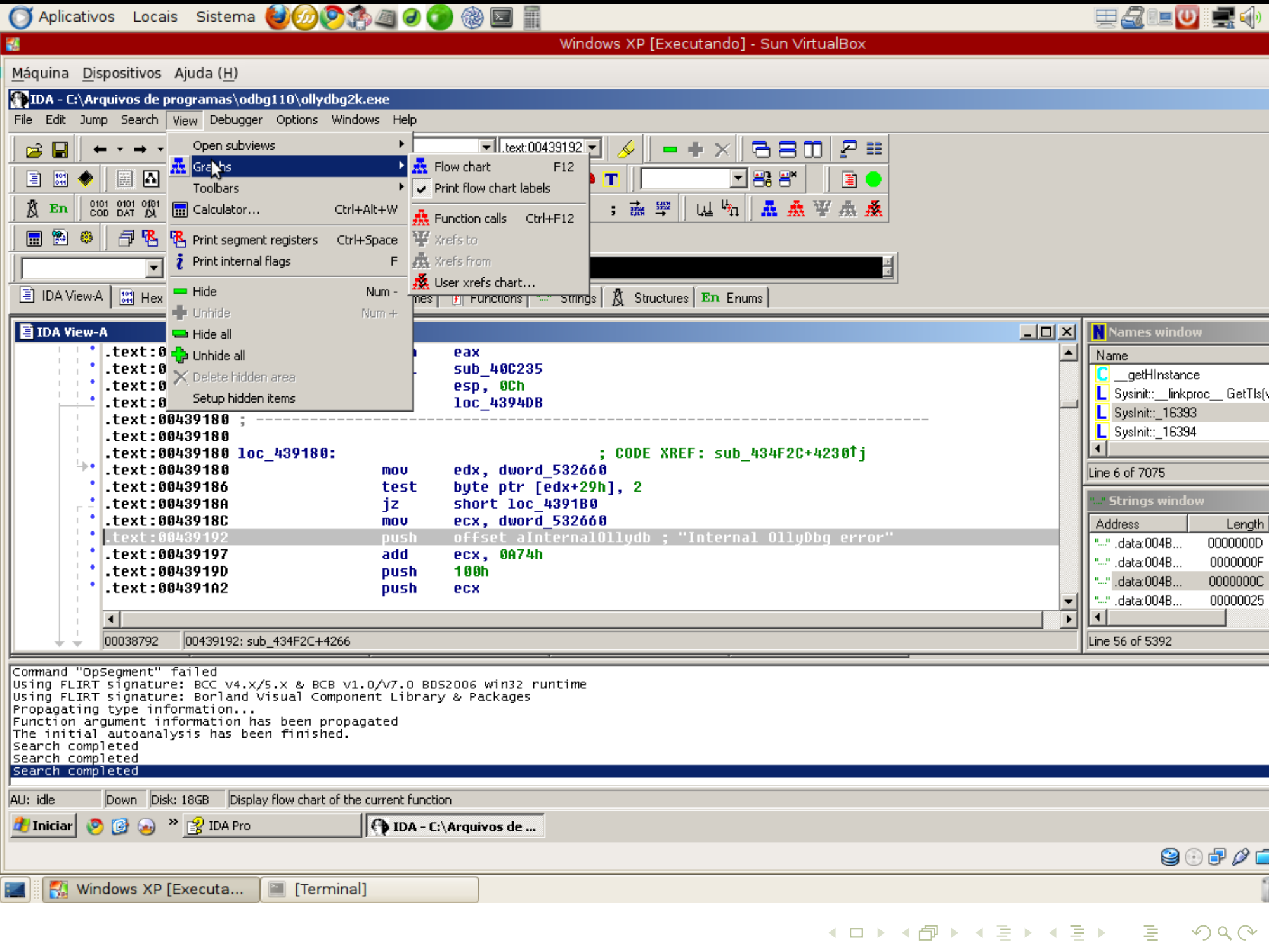

Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Choose function to jump to
Function name Segment Start Length R F L S B T =
sub_42F574 .text 0042F574 000000AD R B T
sub_42F624 .text 0042F624 00000045 R B
sub_42F66C .text 0042F66C 0000005E R B
sub_42F6CC .text 0042F6CC 00000047 R B
sub_42F714 .text 0042F714 00000077 R B
sub_42F78C .text 0042F78C 000000DB R B
sub_42F867 .text 0042F867 00000134 R B
__GetPolymorphicDTC(void *,uint) .text 0042F99B 00000007 R L B
sub_42F9A2 .text 0042F9A2 00000120 R B
sub_42FAC2 .text 0042FAC2 0000050F R B
sub_42FFD1 .text 0042FFD1 000001D4 R B
sub_4301A5 .text 004301A5 00000097 R B
sub_43023C .text 0043023C 000001B6 R B
OK Cancel Help Search
Line 389 of 2105
IDA View-A
Hex View-A
Exports
Names window
__getHInstance
SysInit::_16393
SysInit::_16394
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
100.00% (-281,-26) (812,0) 00000745 00401145: Sysinit::__linkproc__ GetTls(void)+5
Line 56 of 5392
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 18GB
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums
IDA View-A
; Attributes: library function bp-based frame
; __GetPolymorphicDTC(void *, unsigned int)
@__GetPolymorphicDTC$qpvui proc near
push ebp
mov ebp, esp
xor eax, eax
pop ebp
retn
@__GetPolymorphicDTC$qpvui endp
Names window
Name
__getHInstance
Sysinit::__linkproc__ GetTls(v
SysInit::_16393
SysInit::_16394
Line 6 of 7075
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
Line 56 of 5392
100.00% (-289,-19) (642,109) 0002EF9B 0042F99B: __GetPolymorphicDTC(void *,uint)
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 18GB Click on node title to select/drag it; DblClick on edge to follow it; Wheel to scroll vertically; Ctrl,Alt,Shift for more optio
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
next code Alt+C
next data Ctrl+D
next explored Ctrl+A
next unexplored Ctrl+U
immediate value... Alt+I
next immediate value Ctrl+I
text... Alt+T
next text Ctrl+T
sequence of bytes... Alt+B
next sequence of bytes Ctrl+B
not function Alt+U
next void Ctrl+V
error operand Ctrl+F
all void operands
all error operands
Search direction
Text
IDA View-A
Names Functions Strings Structures Enums
; Attributes: library function bp-based frame
; __GetPolymorphicDTC(void *, unsigned int)
@__GetPolymorphicDTC$qpvui proc near
push ebp
mov ebp, esp
xor eax, eax
pop ebp
retn
@__GetPolymorphicDTC$qpvui endp
Names window
Name
__getHInstance
SysInit::__linkproc__ GetTls(v
SysInit::_16393
SysInit::_16394
Line 6 of 7075
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
Line 56 of 5392
100.00% (-289,-9) (287,9) 0002EFA1 0042F9A1: __GetPolymorphicDTC(void *,uint)+6
IDA is analysing the input file...
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Search completed
AU: idle Down Disk: 18GB Search for text
Iniciar IDA Pro IDA - C:\Arquivos de ...
Windows XP [Executa... [Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
@__GetPolym
Text search (slow!)
String olly
Parameters
Case sensitive
Regular expression
Identifier
Direction
Search Down
Search Up
Find all occurences
OK
Cancel
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
; Attributes: library function bp-based frame
; __GetPolymorphicDTC(void *, unsigned int)
@__GetPolymorphicDTC$qpvui proc near
push ebp
mov ebp, esp
xor eax, eax
pop ebp
retn
@__GetPolymorphicDTC$qpvui endp
Address
Length
.data:004B...
0000000D
.data:004B...
0000000F
.data:004B...
0000000C
.data:004B...
00000025
100.00%
(-289,-9)
(697,0)
0002EFA1
0042F9A1: __GetPolymorphicDTC(void *,uint)+6
Line 56 of 5392
You may start to explore the input file right now.
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Search completed
Search completed
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Text
.text:00439192
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
IDA View-A
.text:00439172 push eax
.text:00439173 call sub_40C235
.text:00439178 add esp, 0Ch
.text:0043917B jmp loc_4394DB
.text:00439180 ; ---------- (many dashes)
.text:00439180
.text:00439180 loc_439180: ; CODE XREF: sub_434F2C+4230↑j
.text:00439180 mov edx, dword_532660
.text:00439186 test byte ptr [edx+29h], 2
.text:0043918A jz short loc_4391B0
.text:0043918C mov ecx, dword_532660
.text:00439192 push offset aInternalOllydb ; "Internal OllyDbg error"
.text:00439197 add ecx, 0A74h
.text:0043919D push 100h
.text:004391A2 push ecx
00038792
00439192: sub_434F2C+4266
Names window
Name
__getHInstance
Sysinit::__linkproc__ GetTls(v
SysInit::_16393
SysInit::_16394
Line 6 of 7075
Strings window
Address
Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
Line 56 of 5392
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Search completed
Search completed
Search completed
AU: idle
Down
Disk: 18GB
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe
File Edit Jump Search View Debugger Options Windows Help
Open subviews
Graphs
Toolbars
Calculator... Ctrl+Alt+W
Print segment registers Ctrl+Space
Print internal flags F
Hide Num -
Unhide Num +
Hide all
Unhide all
Delete hidden area
Setup hidden items
Flow chart F12
Print flow chart labels
Function calls Ctrl+F12
Xrefs to
Xrefs from
User xrefs chart...
IDA View-A
Hex
Functions
Strings
Structures
Enums
.text:00439180 loc_439180: ; CODE XREF: sub_434F2C+4230↑j
.text:00439180 mov edx, dword_532660
.text:00439186 test byte ptr [edx+29h], 2
.text:0043918A jz short loc_4391B0
.text:0043918C mov ecx, dword_532660
.text:00439192 push offset aInternalOllydb ; "Internal OllyDbg error"
.text:00439197 add ecx, 0A74h
.text:0043919D push 100h
.text:004391A2 push ecx
Names window
Name
__getHInstance
SysInit::_16393
SysInit::_16394
Line 6 of 7075
Strings window
Address Length
.data:004B... 0000000D
.data:004B... 0000000F
.data:004B... 0000000C
.data:004B... 00000025
Line 56 of 5392
00038792 00439192: sub_434F2C+4266
Command "OpSegment" failed
Using FLIRT signature: BCC v4.x/5.x & BCB v1.0/v7.0 BDS2006 win32 runtime
Using FLIRT signature: Borland Visual Component Library & Packages
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Search completed
Search completed
Search completed
AU: idle Down Disk: 18GB Display flow chart of the current function
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
Windows XP [Executa...
[Terminal]

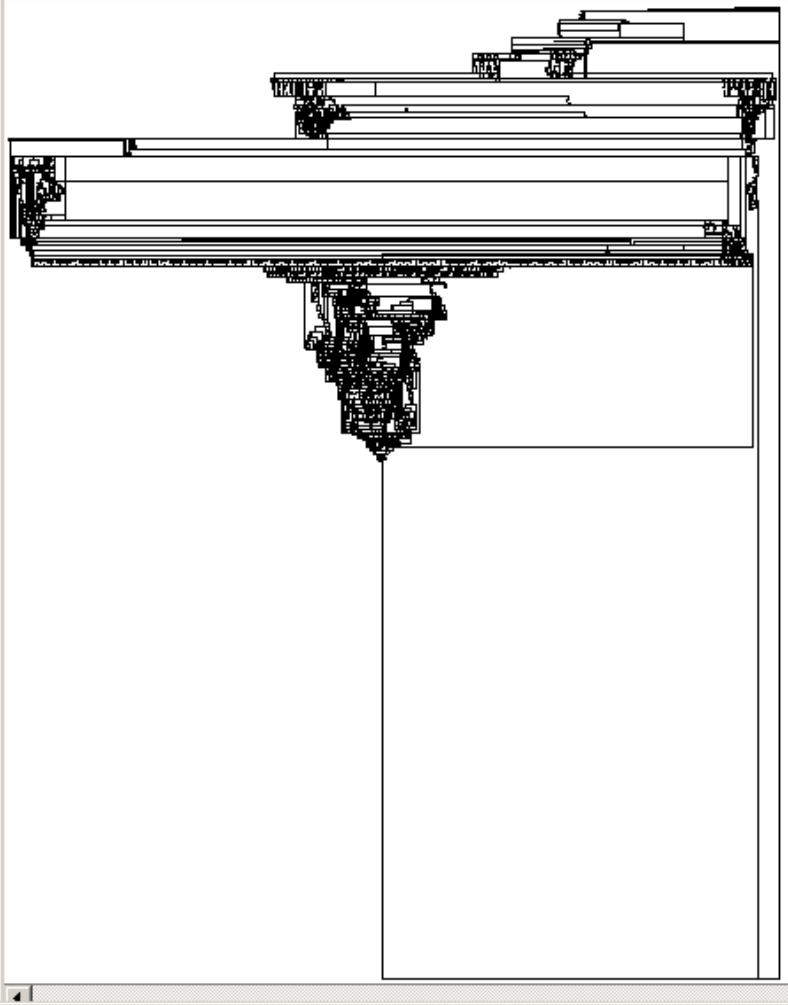
Aplicativos Locais Sistema

Windows XP [Executando] - Sun VirtualBox

Máquina Dispositivos Ajuda (H)

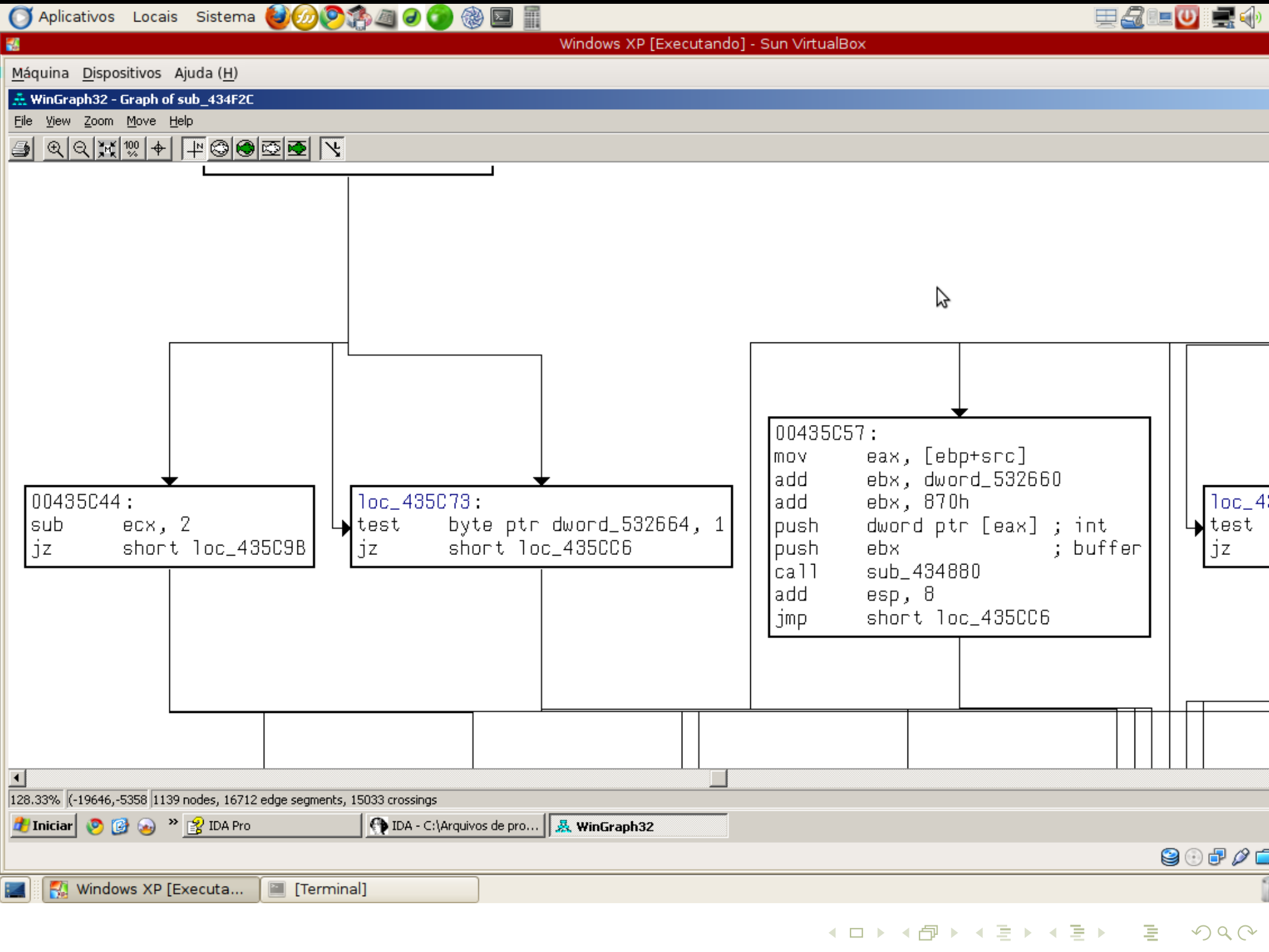
WinGraph32 - Graph of sub_434F2C

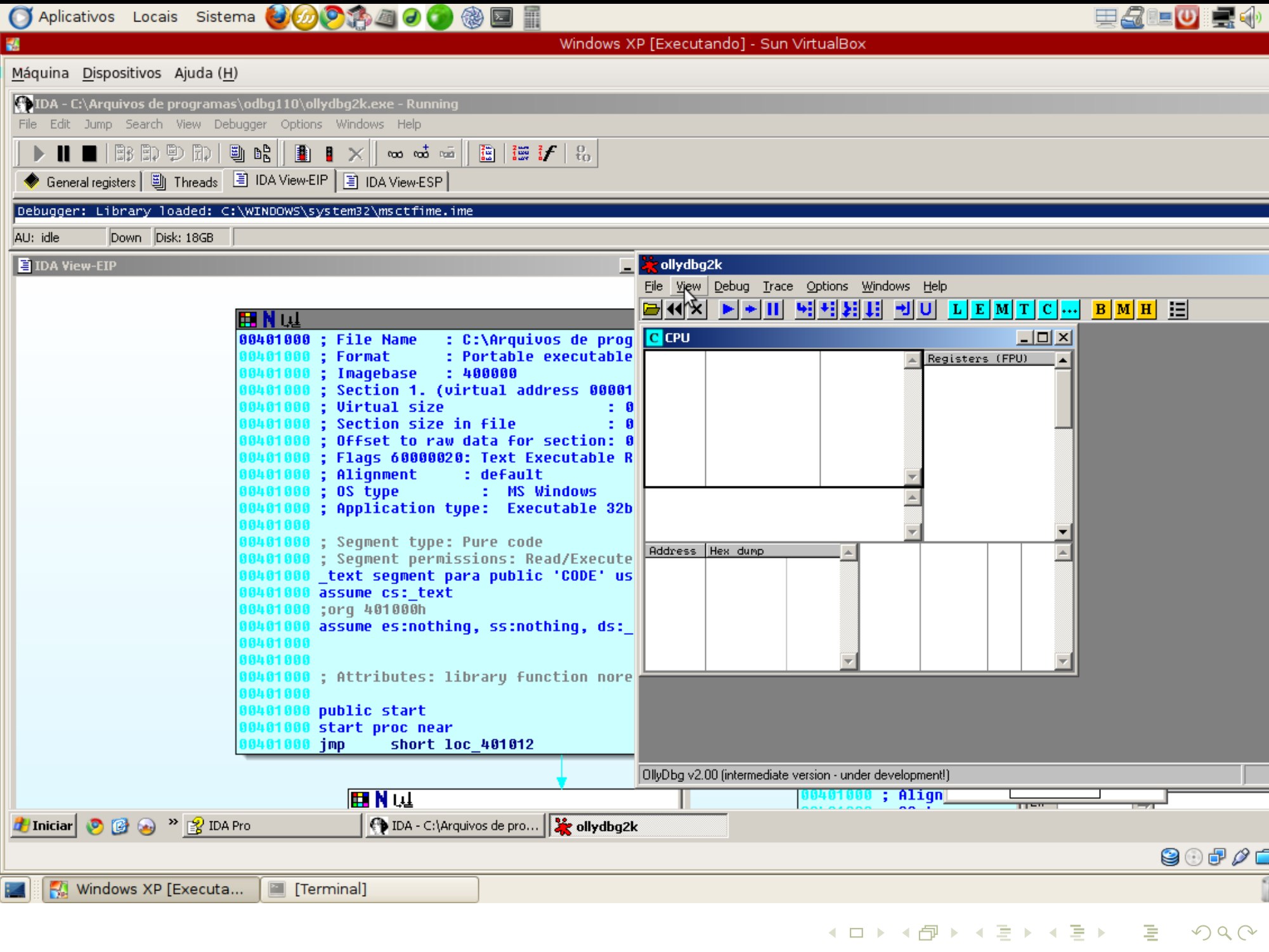
File View Zoom Move Help

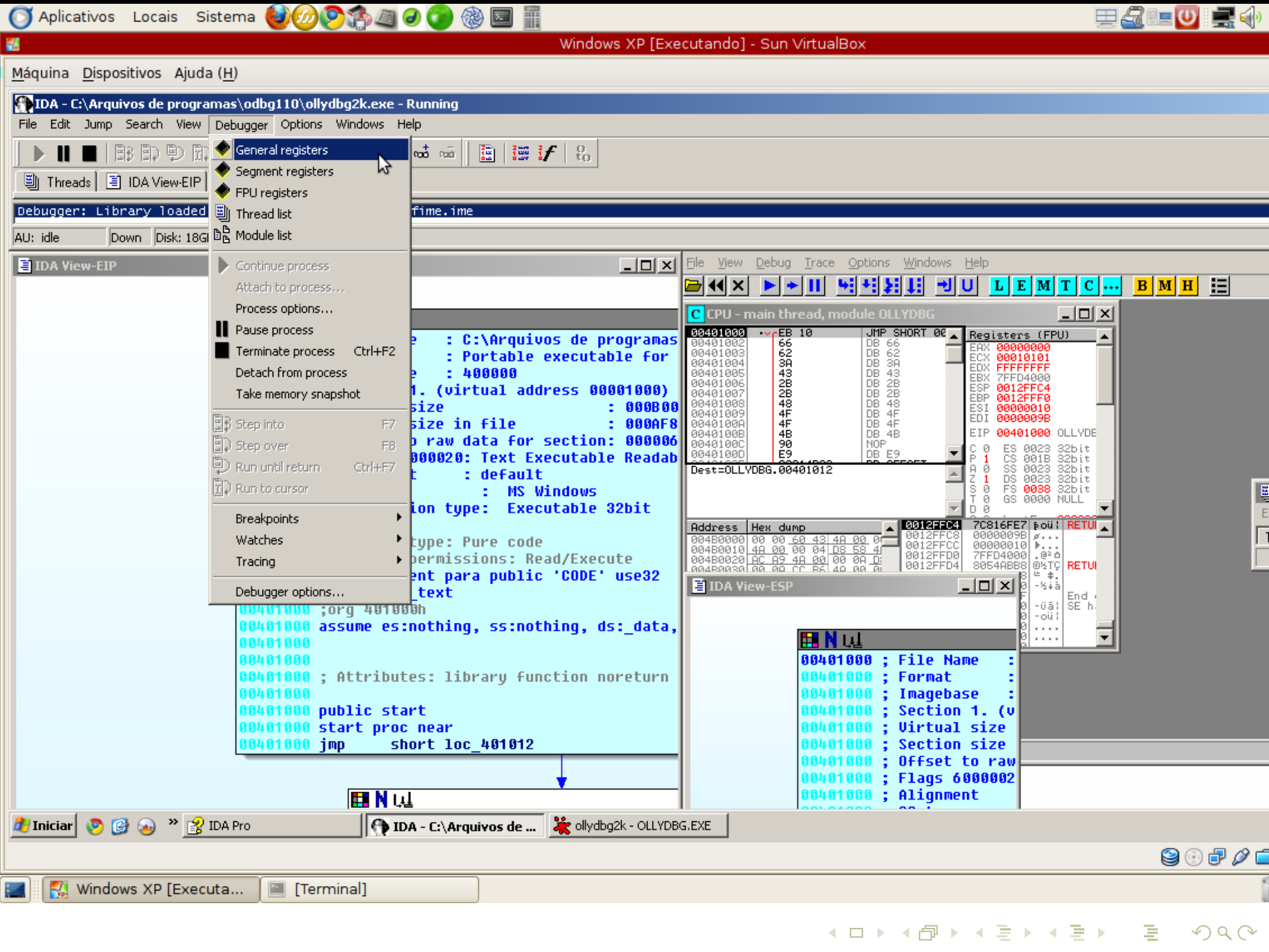


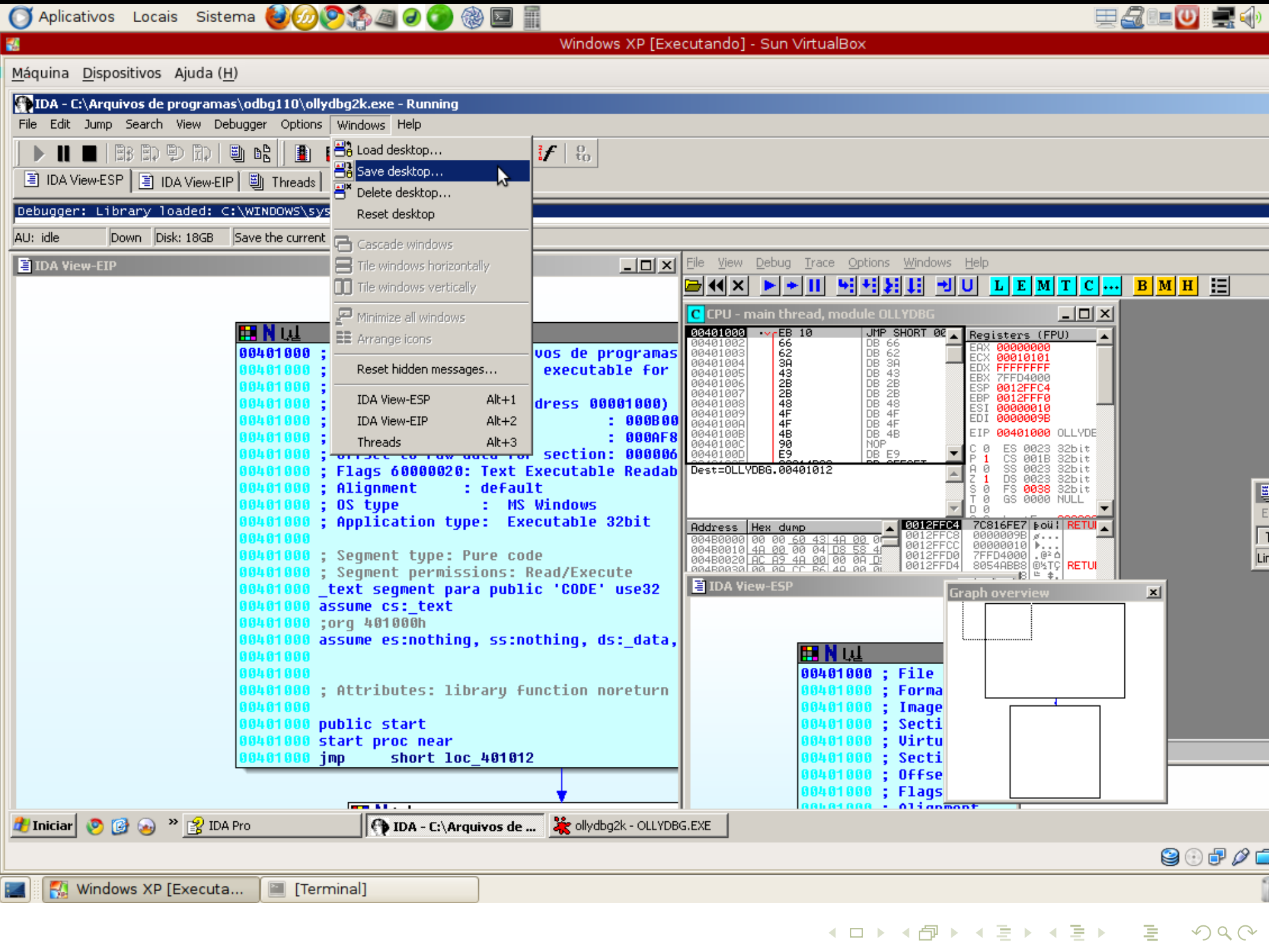
Iniciar IDA Pro IDA - C:\Arquivos de pro... WinGraph32

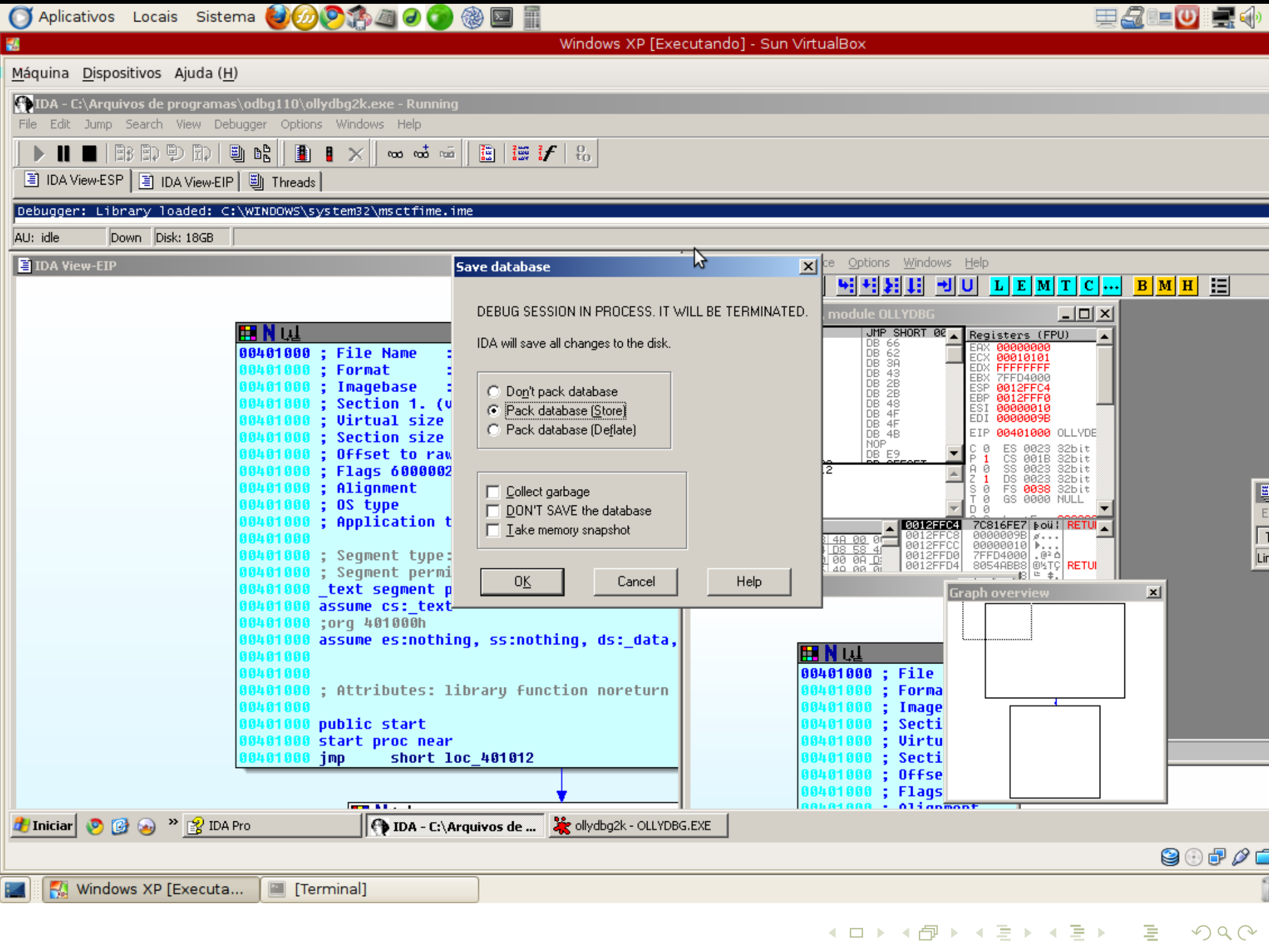
Windows XP [Executa... [Terminal]


Aplicativos
Locais
Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina
Dispositivos
Ajuda (H)
WinGraph32 - Graph of sub_434F2C
File
View
Zoom
Move
Help
00435C44:
sub ecx, 2
jz short loc_435C9B
loc_435C73:
test byte ptr dword_532664, 1
jz short loc_435CC6
00435C57:
mov eax, [ebp+src]
add ebx, dword_532660
add ebx, 870h
push dword ptr [eax] ; int
push ebx ; buffer
call sub_434880
add esp, 8
jmp short loc_435CC6
128.33%
(-19646,-5358
1139 nodes, 16712 edge segments, 15033 crossings
Iniciar
IDA Pro
IDA - C:\Arquivos de pro...
WinGraph32
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - Running
File Edit Jump Search View Debugger Options Windows Help
General registers
Threads
IDA View-EIP
IDA View-ESP
Debugger: Library loaded: C:\WINDOWS\system32\msctfime.ime
AU: idle
Down
Disk: 18GB
IDA View-EIP
00401000 ; File Name : C:\Arquivos de prog
00401000 ; Format : Portable executable
00401000 ; Imagebase : 400000
00401000 ; Section 1. (virtual address 00001
00401000 ; Virtual size : 0
00401000 ; Section size in file : 0
00401000 ; Offset to raw data for section: 0
00401000 ; Flags 60000020: Text Executable R
00401000 ; Alignment : default
00401000 ; OS type : MS Windows
00401000 ; Application type: Executable 32b
00401000
00401000 ; Segment type: Pure code
00401000 ; Segment permissions: Read/Execute
00401000 _text segment para public 'CODE' us
00401000 assume cs:_text
00401000 ;org 401000h
00401000 assume es:nothing, ss:nothing, ds:_
00401000
00401000
00401000 ; Attributes: library function nore
00401000
00401000 public start
00401000 start proc near
00401000 jmp short loc_401012
ollydbg2k
File View Debug Trace Options Windows Help
CPU
Registers (FPU)
Address
Hex dump
OllyDbg v2.00 (intermediate version - under development!)
00401000 ; Align
Iniciar
IDA Pro
IDA - C:\Arquivos de pro...
ollydbg2k
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - Running
File Edit Jump Search View Debugger Options Windows Help
General registers
Segment registers
FPU registers
Thread list
Module list
Continue process
Attach to process...
Process options...
Pause process
Terminate process Ctrl+F2
Detach from process
Take memory snapshot
Step into F7
Step over F8
Run until return Ctrl+F7
Run to cursor
Breakpoints
Watches
Tracing
Debugger options...
Threads
IDA View-EIP
Debugger: Library loaded
AU: idle
Down
IDA View-ESP
CPU - main thread, module OLLYDBG
Registers (FPU)
Dest=OLLYDBG.00401012
00401000 ; File Name :
00401000 ; Format :
00401000 ; Imagebase :
00401000 ; Section 1. (v
00401000 ; Virtual size
00401000 ; Section size
00401000 ; Offset to raw
00401000 ; Flags 6000002
00401000 ; Alignment
00401000 public start
00401000 start proc near
00401000 jmp short loc_401012
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
ollydbg2k - OLLYDBG.EXE
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - Running
File Edit Jump Search View Debugger Options Windows Help
Load desktop...
Save desktop...
Delete desktop...
Reset desktop
Cascade windows
Tile windows horizontally
Tile windows vertically
Minimize all windows
Arrange icons
Reset hidden messages...
IDA View-ESP Alt+1
IDA View-EIP Alt+2
Threads Alt+3
IDA View-ESP
IDA View-EIP
Threads
Debugger: Library loaded: C:\WINDOWS\sys
AU: idle
Down
Disk: 18GB
Save the current
IDA View-EIP
00401000 ; Flags 60000020: Text Executable Readab
00401000 ; Alignment : default
00401000 ; OS type : MS Windows
00401000 ; Application type: Executable 32bit
00401000 ; Segment type: Pure code
00401000 ; Segment permissions: Read/Execute
00401000 _text segment para public 'CODE' use32
00401000 assume cs:_text
00401000 ;org 401000h
00401000 assume es:nothing, ss:nothing, ds:_data,
00401000 ; Attributes: library function noreturn
00401000 public start
00401000 start proc near
00401000 jmp short loc_401012
CPU - main thread, module OLLYDBG
Registers (FPU)
Dest=OLLYDBG.00401012
IDA View-ESP
Graph overview
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
ollydbg2k - OLLYDBG.EXE
Windows XP [Executa...
[Terminal]


Aplicativos Locais Sistema
Windows XP [Executando] - Sun VirtualBox
Máquina Dispositivos Ajuda (H)
IDA - C:\Arquivos de programas\odbg110\ollydbg2k.exe - Running
File Edit Jump Search View Debugger Options Windows Help
IDA View-ESP
IDA View-EIP
Threads
Debugger: Library loaded: C:\WINDOWS\system32\msctfime.ime
AU: idle
Down
Disk: 18GB
Save database
DEBUG SESSION IN PROCESS. IT WILL BE TERMINATED.
IDA will save all changes to the disk.
Don't pack database
Pack database (Store)
Pack database (Deflate)
Collect garbage
DON'T SAVE the database
Take memory snapshot
OK
Cancel
Help
Graph overview
Iniciar
IDA Pro
IDA - C:\Arquivos de ...
ollydbg2k - OLLYDBG.EXE
Windows XP [Executa...
[Terminal]

Referências

- BLUM, R. *Professional Assembly Language*. Wiley Publishing. Indianápolis (EUA), 2005. **ISBN 0-7645-7901-0**.
- DataRescue SA/NV. *Remote debugging with IDA Pro*. DataRescue (Belgium), 2005.
- CHRIS EAGLE. *The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler*. No Starch Press. San Francisco (EUA), 2008. **ISBN 1-59327-178-6**.