Lab 9: Disassembling C on Windows

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 15/2/2023

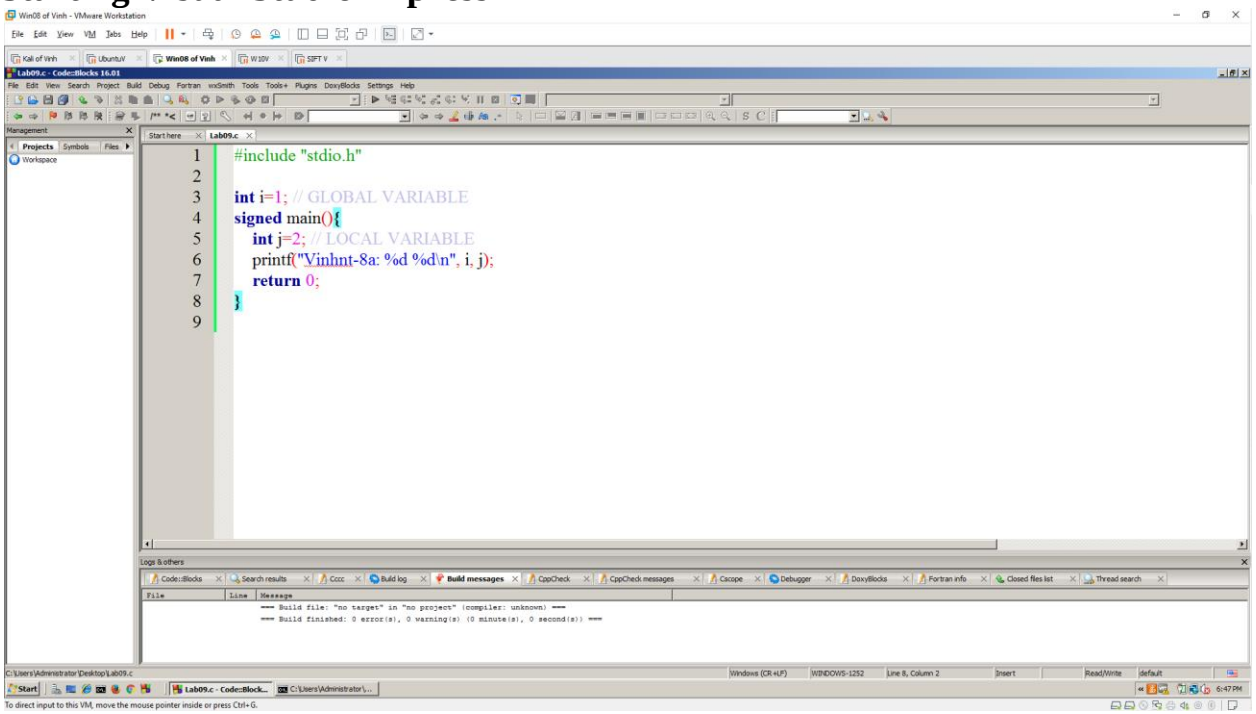
Purpose

You will write a small C programs, compile it, and examine it in the IDA Pro disassembler to learn what it looks like in assembly language.

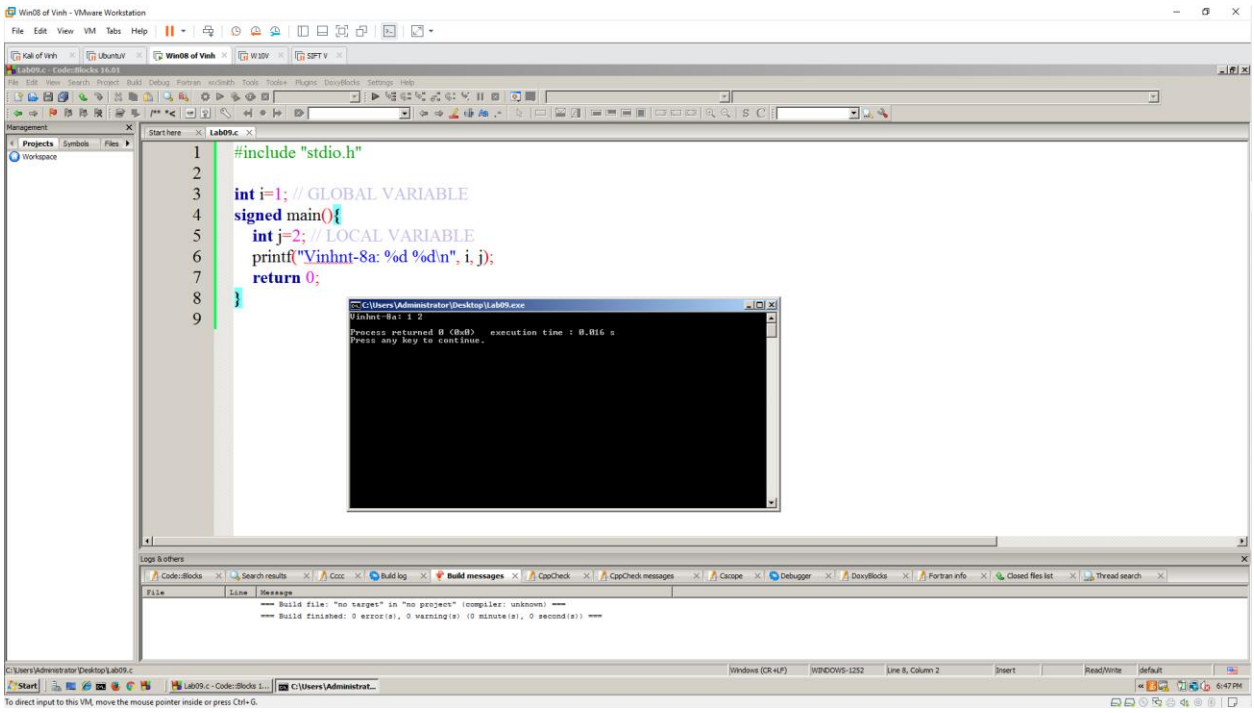
What You Need

- A Windows machine, real or virtual. I used Windows 8.
- Visual Studio Express, which you installed in a previous project.
- IDA Pro Free, which you installed in a previous project.

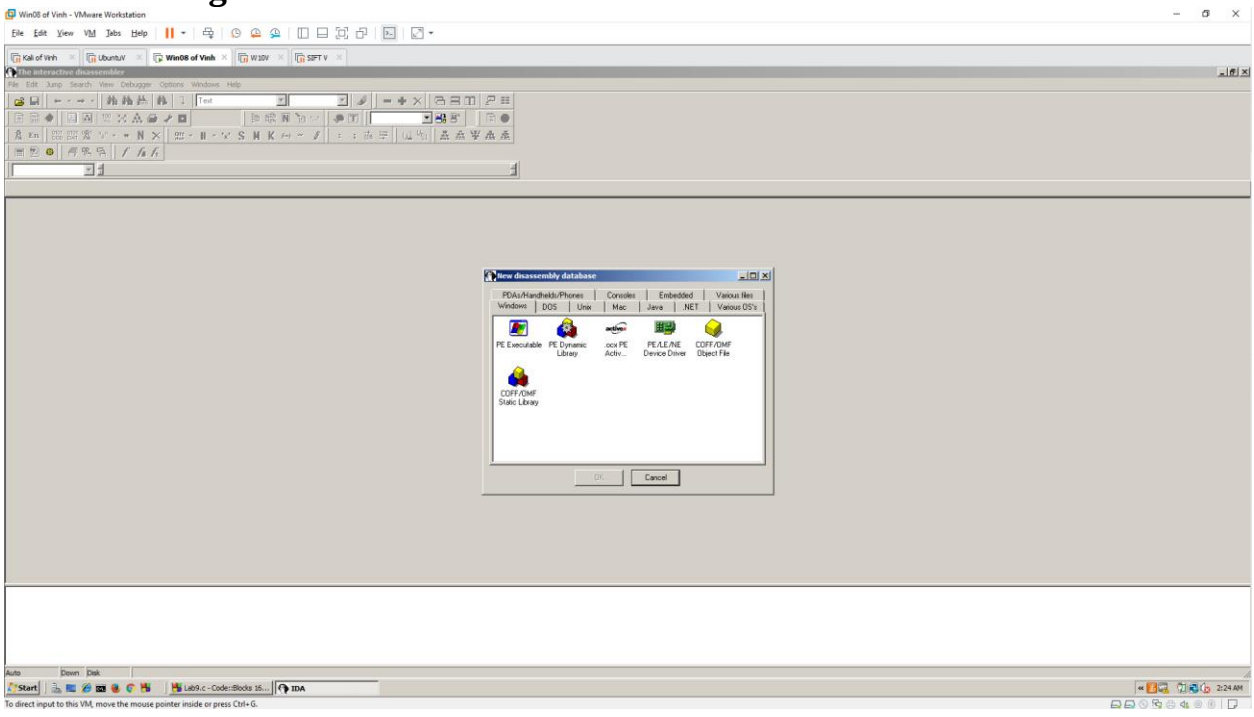
Starting Visual Studio Express

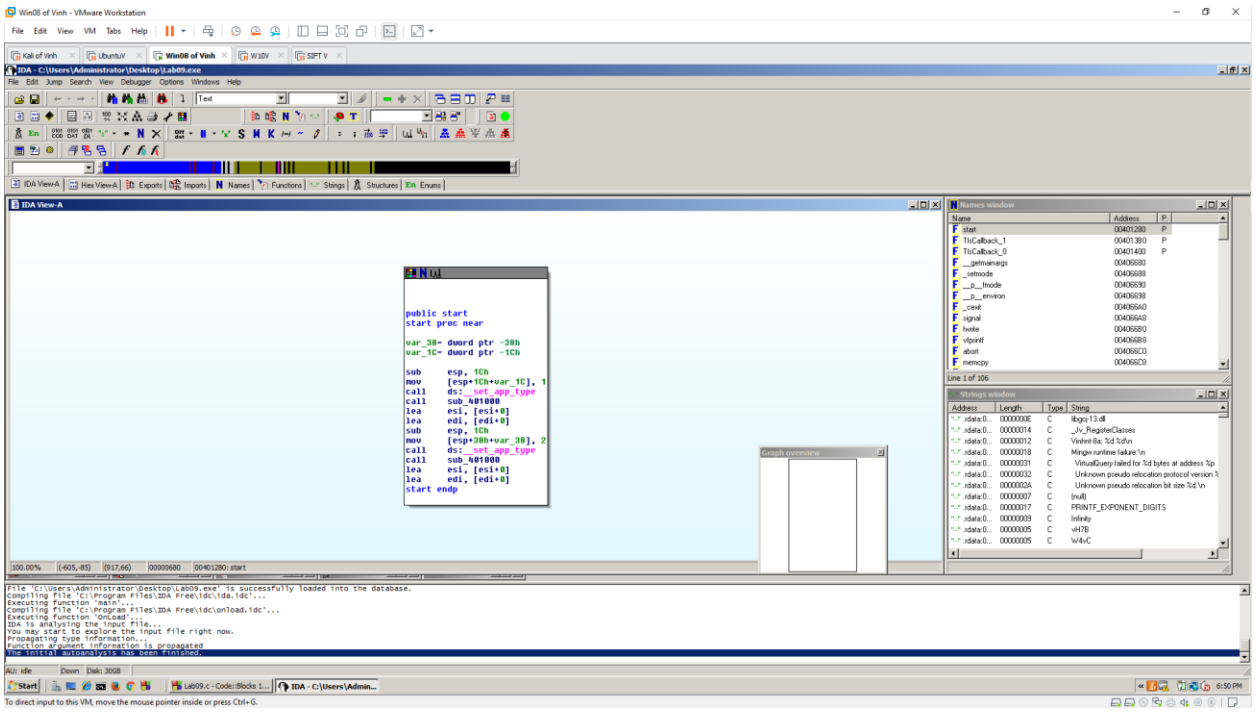


Build and Run

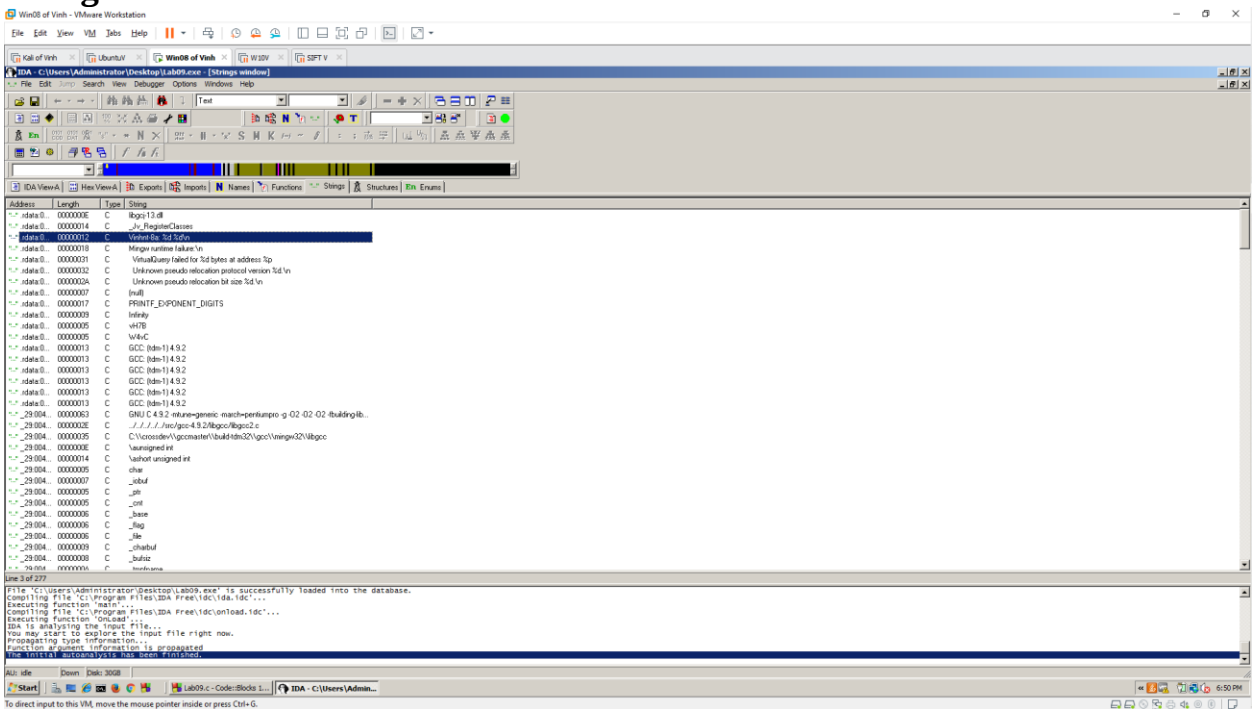


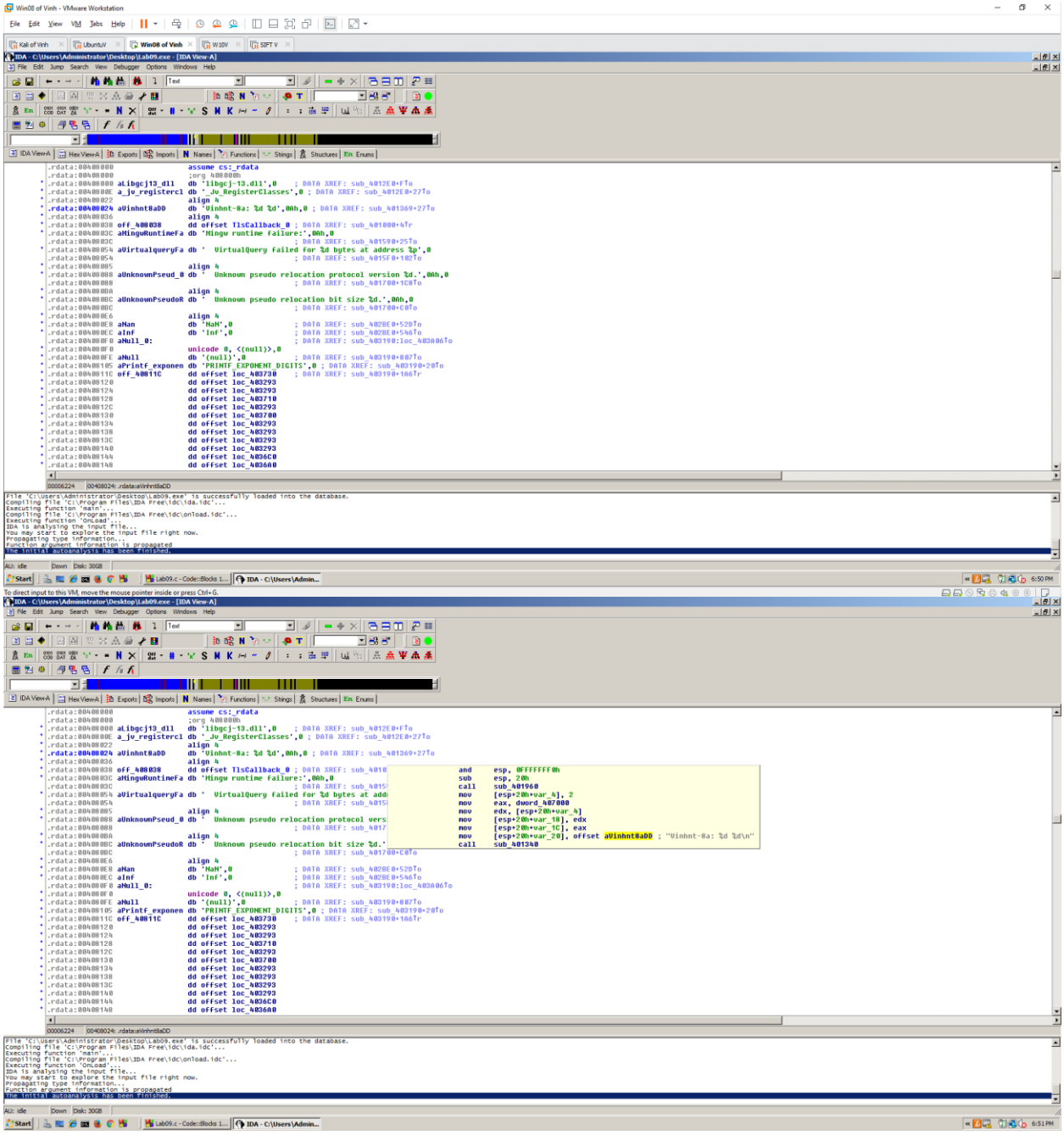
Disassembling the EXE

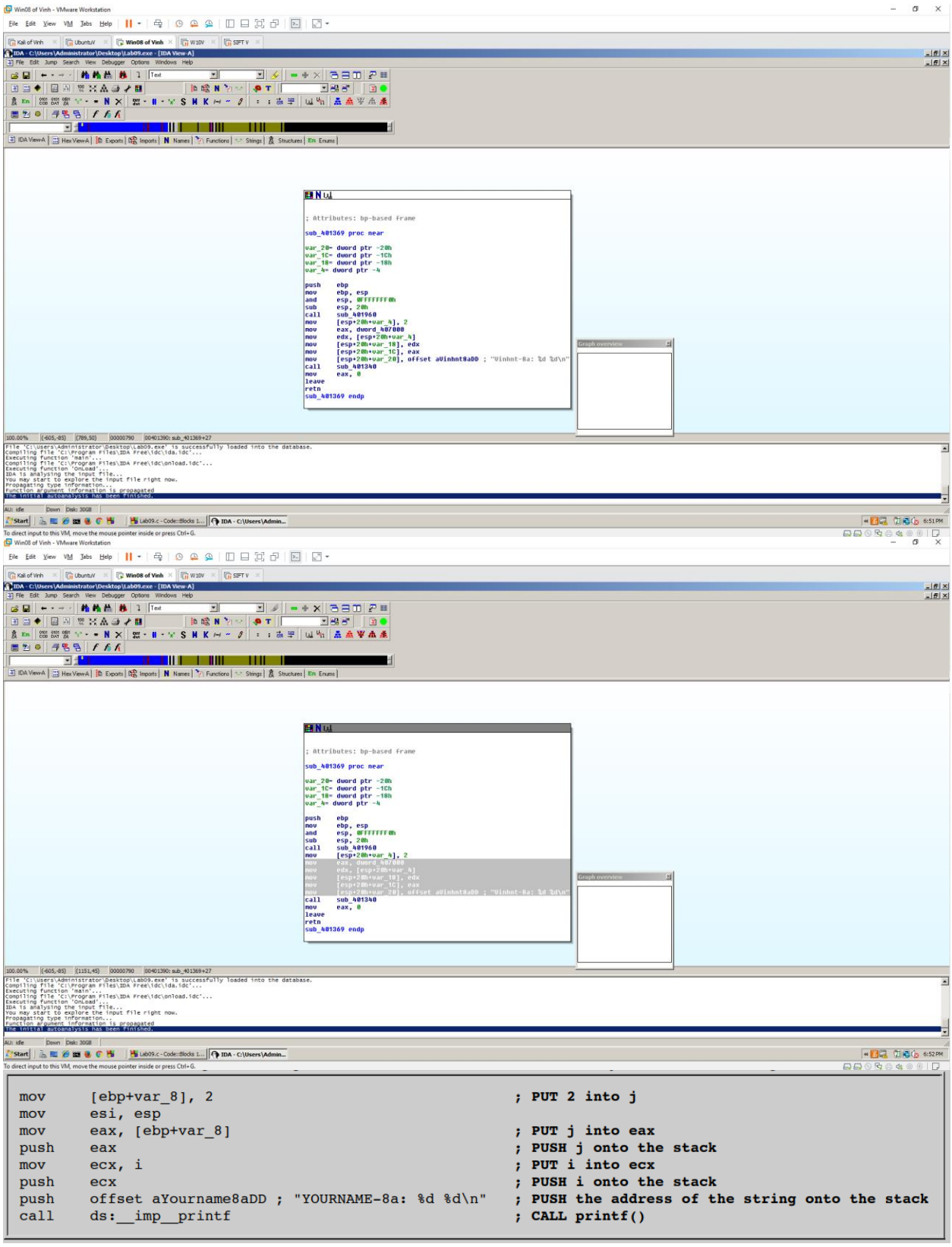




Strings window

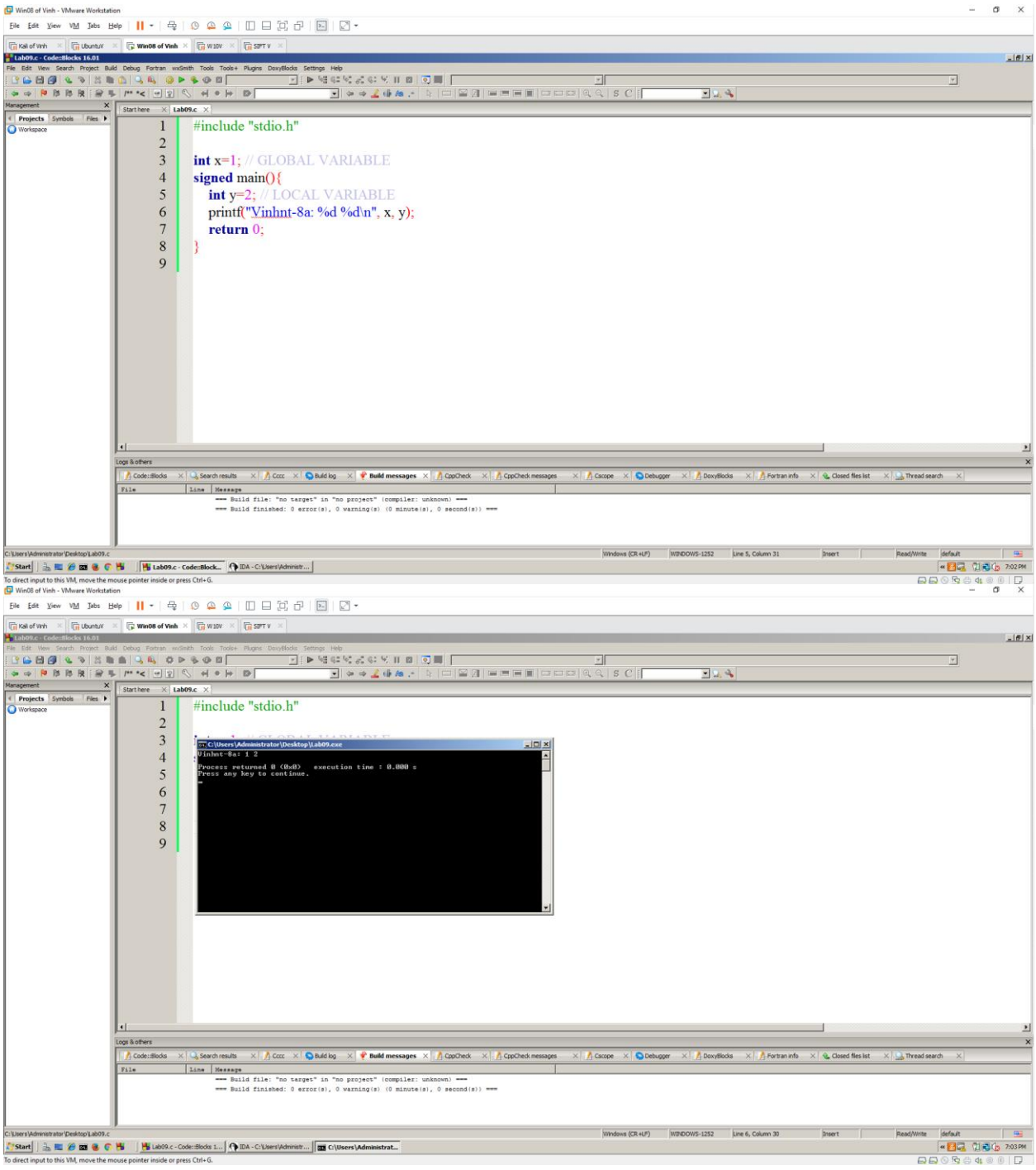


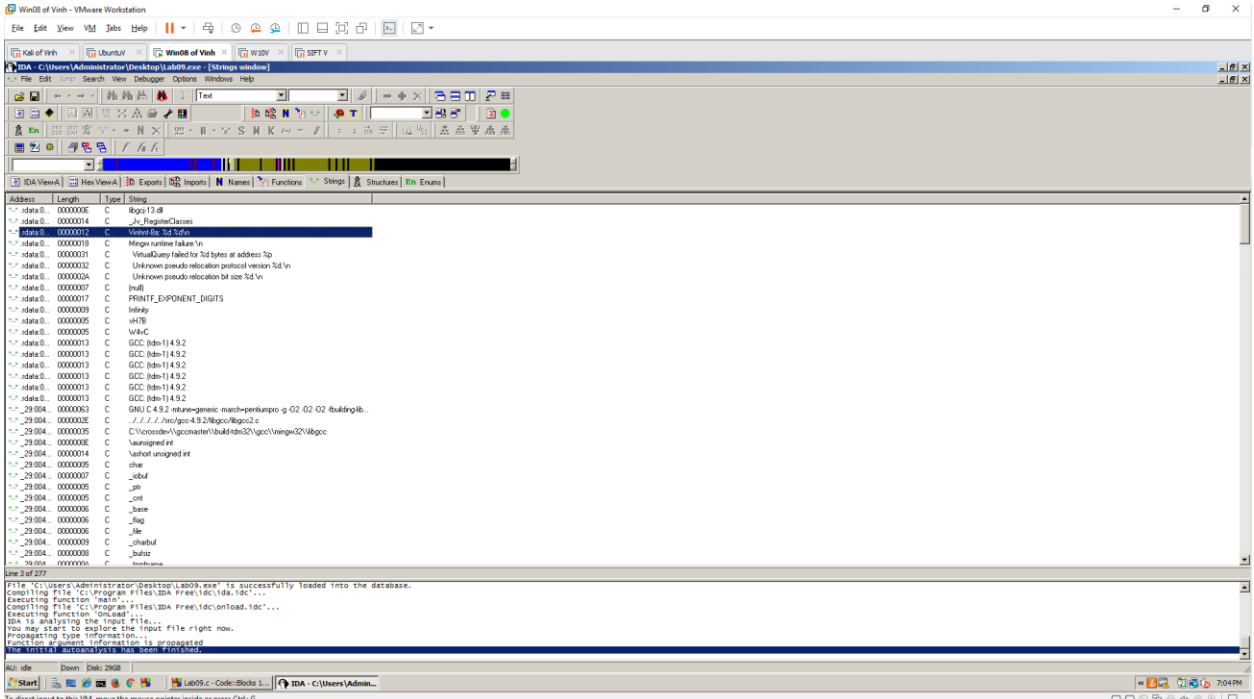

Win08 of Vinh - VMware Workstation
IDA - C:\Users\Administrator\Desktop\Lab09.exe - [IDA View-A]
.rdata:00408000 assume cs:_rdata
.rdata:00408000 ;org 408000h
.rdata:00408000 aLibgcj13_dll db 'libgcj-13.dll',0 ; DATA XREF: sub_4012E0+FTo
.rdata:0040800E a_jv_registercl db '_Jv_RegisterClasses',0 ; DATA XREF: sub_4012E0+27To
.rdata:00408022 align 4
.rdata:00408024 aVinhnt8aDD db 'Vinhnt-8a: %d %d',0Ah,0 ; DATA XREF: sub_401369+27To
.rdata:00408036 align 4
.rdata:00408038 off_408038 dd offset TlsCallback_0 ; DATA XREF: sub_401000+A7r
.rdata:0040803C aMingwRuntimeFa db 'Mingw runtime failure:',0Ah,0
.rdata:00408054 aVirtualQueryFa db ' VirtualQuery failed for %d bytes at address %p',0
.rdata:00408085 align 4
.rdata:00408088 aUnknownPseud_0 db ' Unknown pseudo relocation protocol version %d.',0Ah,0
.rdata:004080BC aUnknownPseudoR db ' Unknown pseudo relocation bit size %d.',0Ah,0
.rdata:004080E6 align 4
.rdata:004080E8 aNan db 'NaN',0
.rdata:004080EC aInf db 'Inf',0
.rdata:004080F0 aNull_0:
.rdata:004080F8 unicode 0, <(null)>,0
.rdata:0040810E aNull db '(null)',0
.rdata:00408105 aPrintf_exponen db 'PRINTF_EXPONENT_DIGITS',0
.rdata:0040811C off_40811C dd offset loc_403730
.rdata:00408120 dd offset loc_403293
.rdata:00408124 dd offset loc_403293
.rdata:00408128 dd offset loc_403710
.rdata:0040812C dd offset loc_403293
.rdata:00408130 dd offset loc_403700
.rdata:00408134 dd offset loc_403293
.rdata:00408138 dd offset loc_403293
.rdata:0040813C dd offset loc_403293
.rdata:00408140 dd offset loc_403293
.rdata:00408144 dd offset loc_4036C0
.rdata:00408148 dd offset loc_4036A0
File 'C:\Users\Administrator\Desktop\Lab09.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
and esp, 0FFFFFFF0h
sub esp, 20h
call sub_401960
mov [esp+20h+var_4], 2
mov eax, dword_407000
mov edx, [esp+20h+var_4]
mov [esp+20h+var_10], edx
mov [esp+20h+var_1C], eax
mov [esp+20h+var_20], offset aVinhnt8aDD ; "Vinhnt-8a: %d %d\n"
call sub_4012A0

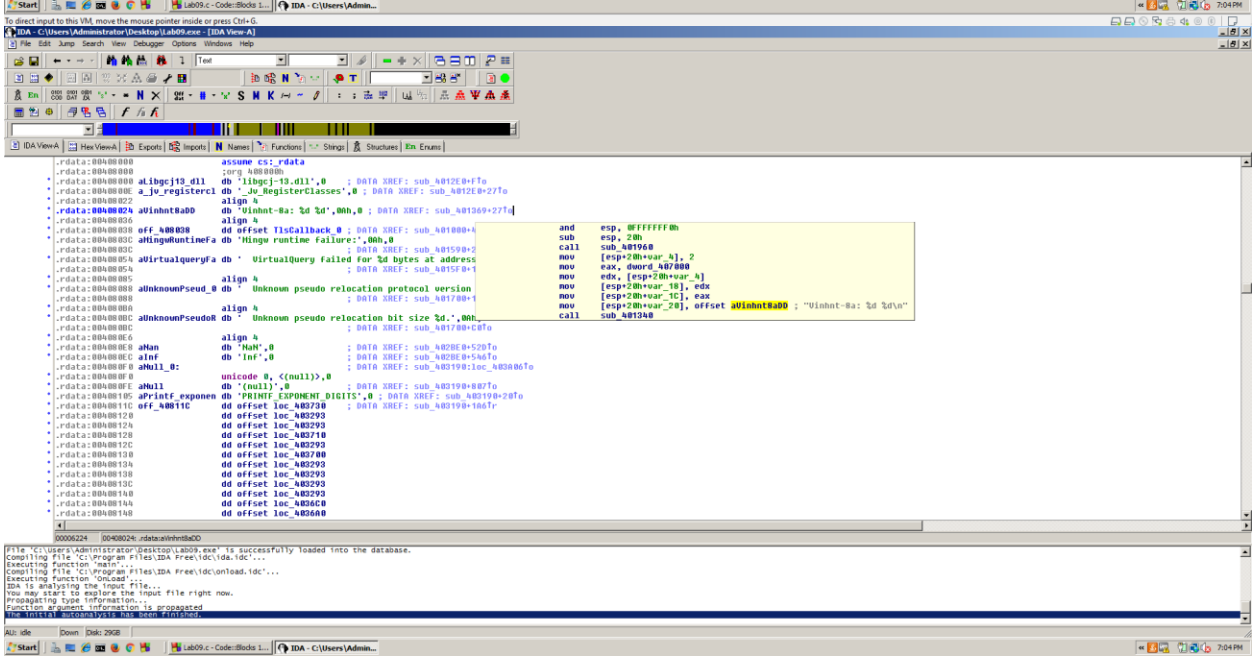


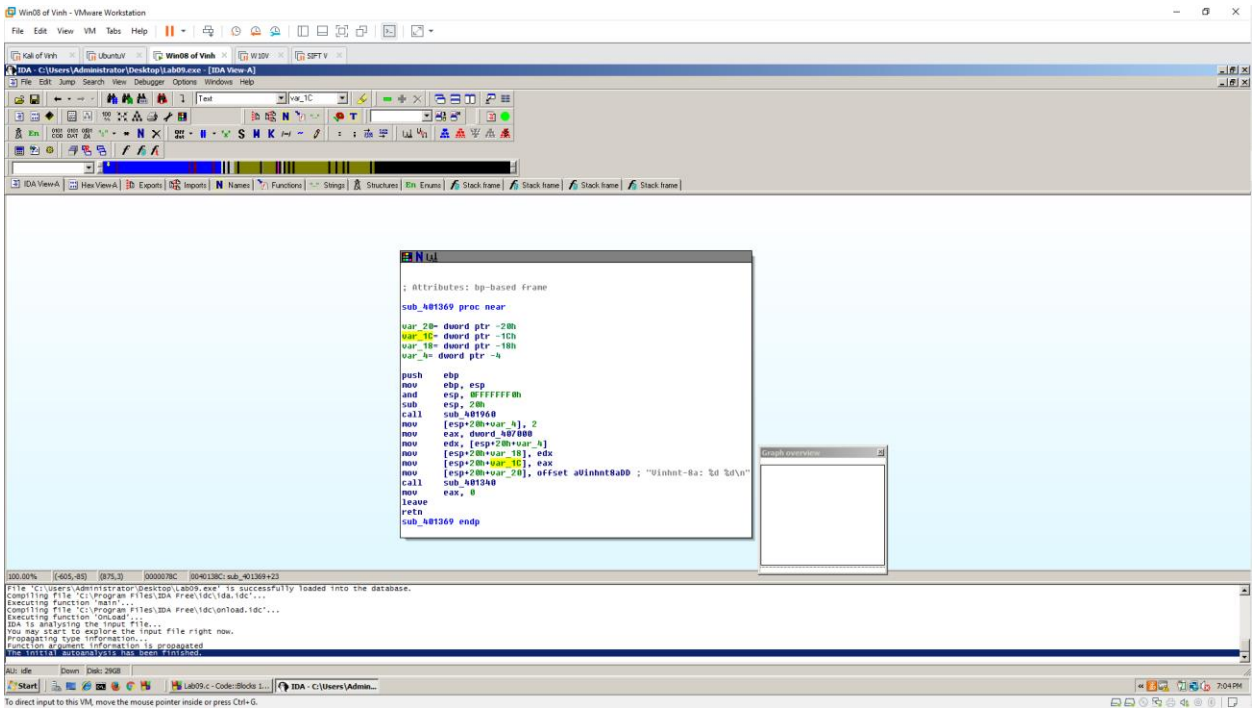
```
mov     [ebp+var_8], 2                          ; PUT 2 into j
mov     esi, esp
mov     eax, [ebp+var_8]                        ; PUT j into eax
push    eax                                     ; PUSH j onto the stack
mov     ecx, i                                  ; PUT i into ecx
push    ecx                                     ; PUSH i onto the stack
push    offset aYourname8aDD ; "YOURNAME-8a: %d %d\n"   ; PUSH the address of the string onto the stack
call    ds:__imp__printf                        ; CALL printf()
```

CHALLENGE: 10 Pts. Extra Credit


Win08 of Vinh - VMware Workstation
Lab09.c - Code::Blocks 16.01
Lab09.c
#include "stdio.h"
int x=1; // GLOBAL VARIABLE
signed main(){
int y=2; // LOCAL VARIABLE
printf("Vinhnt-8a: %d %d\n", x, y);
return 0;
}
=== Build file: "no target" in "no project" (compiler: unknown) ===
=== Build finished: 0 error(s), 0 warning(s) (0 minute(s), 0 second(s)) ===
C:\Users\Administrator\Desktop\Lab09.exe
Vinhnt-8a: 1 2
Process returned 0 (0x0) execution time : 0.000 s
Press any key to continue.


Win08 of Vinh - VMware Workstation
IDA - C:\Users\Administrator\Desktop\Lab09.exe - [Strings window]
Address Length Type String
Line 3 of 277
File 'C:\Users\Administrator\Desktop\Lab09.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.


To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
IDA - C:\Users\Administrator\Desktop\Lab09.exe - [IDA View-A]
.rdata:00408000 assume cs:_rdata
.rdata:00408000 ;org 408000h
.rdata:00408000 aLibgcj13_dll db 'libgcj-13.dll',0 ; DATA XREF: sub_4012E0+F↑o
.rdata:00408000 a_jv_registercl db '_Jv_RegisterClasses',0 ; DATA XREF: sub_4012E0+27↑o
.rdata:00408022 align 4
.rdata:00408024 aVinhnt8aDD db 'Vinhnt-8a: %d %d',0Ah,0 ; DATA XREF: sub_401369+27↑o
.rdata:00408036 align 4
.rdata:00408038 off_408038 dd offset TlsCallback_0 ; DATA XREF: sub_401000+4
.rdata:0040803C aMingwRuntimeFa db 'Mingw runtime failure:',0Ah,0
.rdata:0040803C ; DATA XREF: sub_401590+2
.rdata:00408054 aVirtualqueryFa db ' VirtualQuery failed for %d bytes at address
.rdata:00408054 ; DATA XREF: sub_4015F0+1
.rdata:00408085 align 4
.rdata:00408088 aUnknownPseud_0 db ' Unknown pseudo relocation protocol version
.rdata:00408088 ; DATA XREF: sub_401700+1
.rdata:0040808A align 4
.rdata:0040808C aUnknownPseudoR db ' Unknown pseudo relocation bit size %d.',0Ah,
.rdata:0040808C ; DATA XREF: sub_401700+C0↑o
.rdata:0040808E6 align 4
.rdata:0040808E8 aNan db 'NaN',0 ; DATA XREF: sub_4028E0+52D↑o
.rdata:0040808EC aInf db 'Inf',0 ; DATA XREF: sub_4028E0+546↑o
.rdata:0040808F0 aNull_0: ; DATA XREF: sub_403190:loc_403A06↑o
.rdata:0040808F0 unicode 0, <(null)>,0
.rdata:0040808FE aNull db '(null)',0 ; DATA XREF: sub_403190+807↑o
.rdata:00408105 aPrintf_exponen db 'PRINTF_EXPONENT_DIGITS',0 ; DATA XREF: sub_403190+20↑o
.rdata:0040811C off_40811C dd offset loc_403730 ; DATA XREF: sub_403190+1A6↑r
.rdata:00408120 dd offset loc_403293
.rdata:00408124 dd offset loc_403293
.rdata:00408128 dd offset loc_403710
.rdata:0040812C dd offset loc_403293
.rdata:00408130 dd offset loc_403700
.rdata:00408134 dd offset loc_403293
.rdata:00408138 dd offset loc_403293
.rdata:0040813C dd offset loc_403293
.rdata:00408140 dd offset loc_403293
.rdata:00408144 dd offset loc_4036C0
.rdata:00408148 dd offset loc_4036A0
and esp, 0FFFFFFF0h
sub esp, 20h
call sub_401960
mov [esp+20h+var_4], 2
mov eax, dword_407000
mov edx, [esp+20h+var_4]
mov [esp+20h+var_18], edx
mov [esp+20h+var_1C], eax
mov [esp+20h+var_20], offset aVinhnt8aDD ; "Vinhnt-8a: %d %d\n"
call sub_401340
00006224 00408024: .rdata:aVinhnt8aDD
File 'C:\Users\Administrator\Desktop\Lab09.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.


Win08 of Vinh - VMware Workstation
IDA - C:\Users\Administrator\Desktop\Lab09.exe - [IDA View-A]
; Attributes: bp-based frame
sub_401369 proc near
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= dword ptr -18h
var_4= dword ptr -4
push ebp
mov ebp, esp
and esp, 0FFFFFFF0h
sub esp, 20h
call sub_401960
mov [esp+20h+var_4], 2
mov eax, dword_407000
mov edx, [esp+20h+var_4]
mov [esp+20h+var_18], edx
mov [esp+20h+var_1C], eax
mov [esp+20h+var_20], offset aVinhnt8aDD ; "Vinhnt-8a: %d %d\n"
call sub_401340
mov eax, 0
leave
retn
sub_401369 endp
Graph overview
File 'C:\Users\Administrator\Desktop\Lab09.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.