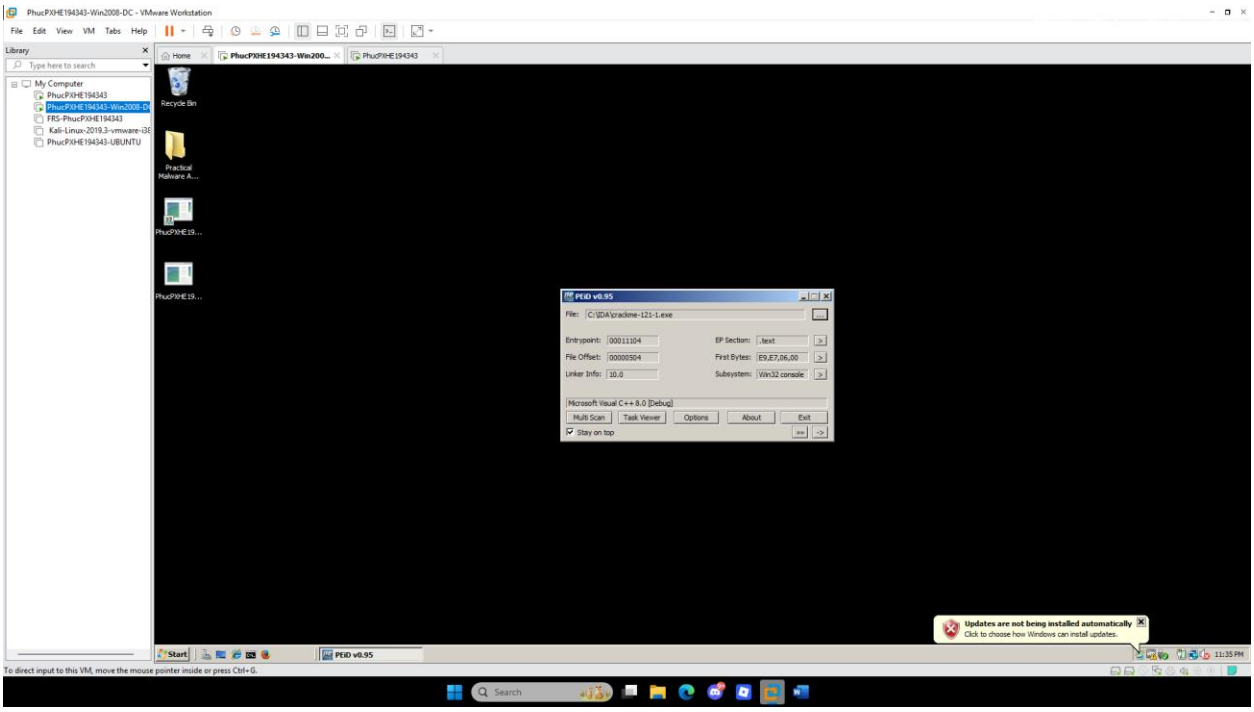
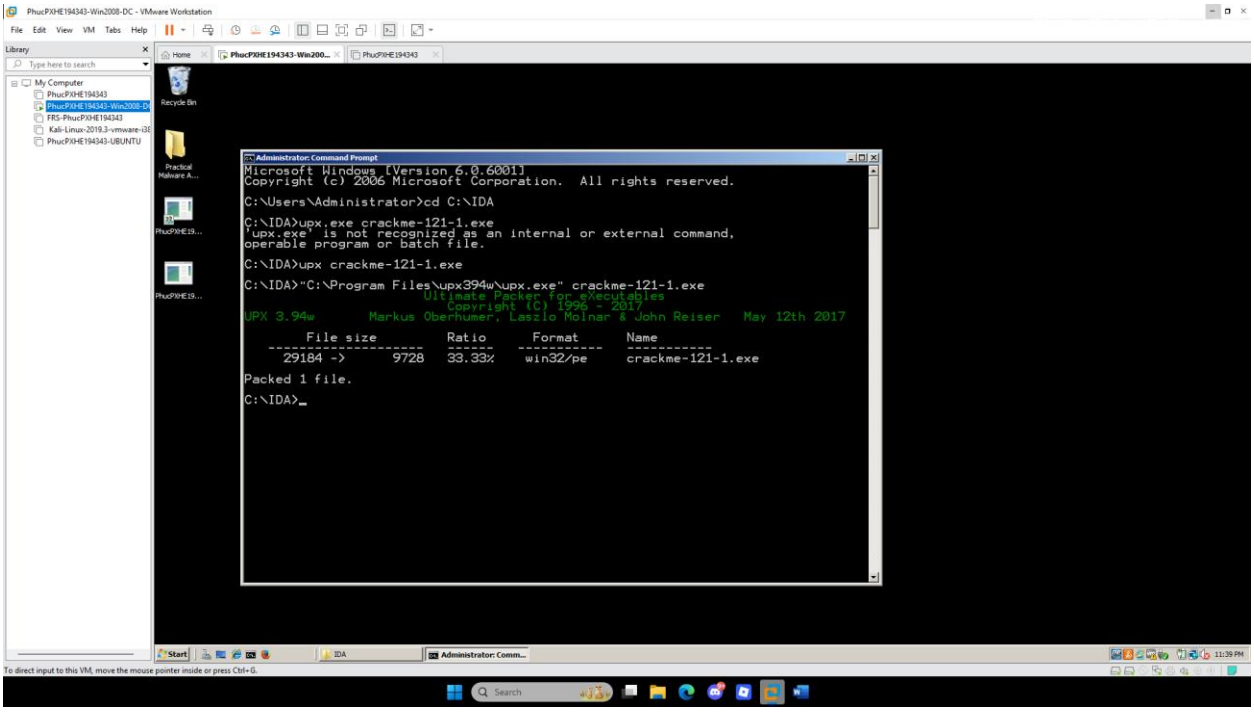
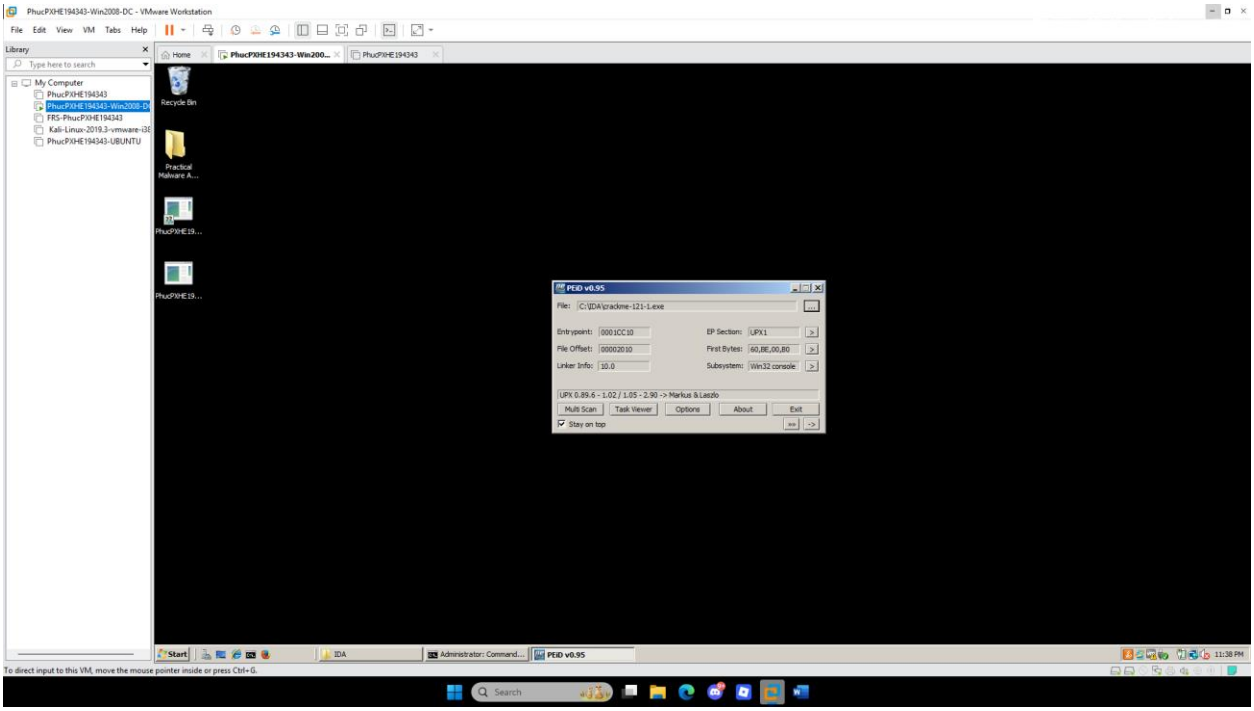
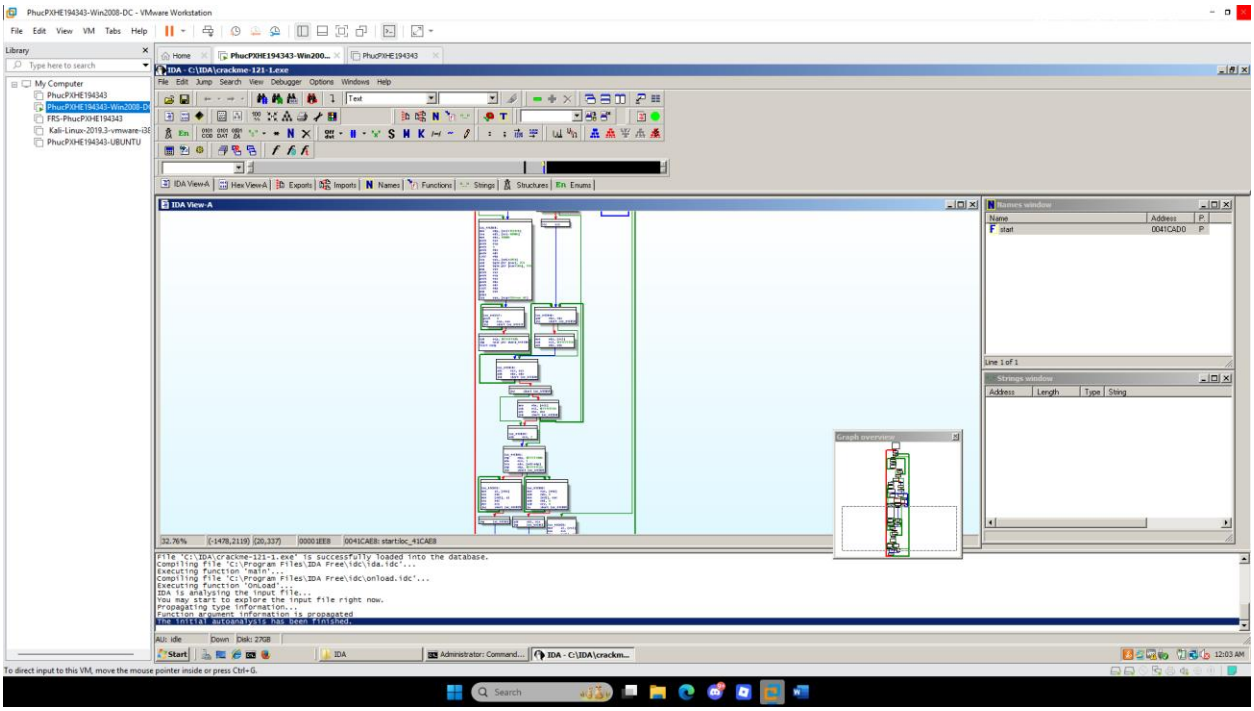
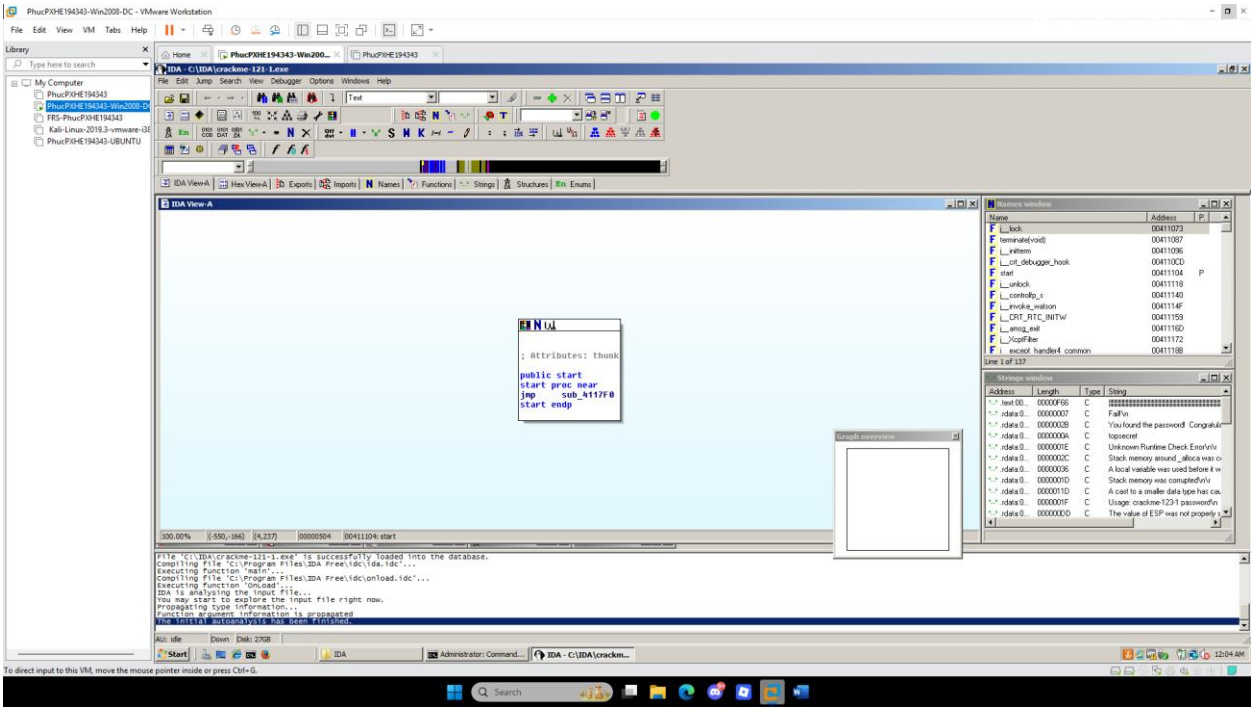
Lab 15.1


PhucPXHE194343-Win2008-DC - VMware Workstation
PEiD v0.95
Updates are not being installed automatically

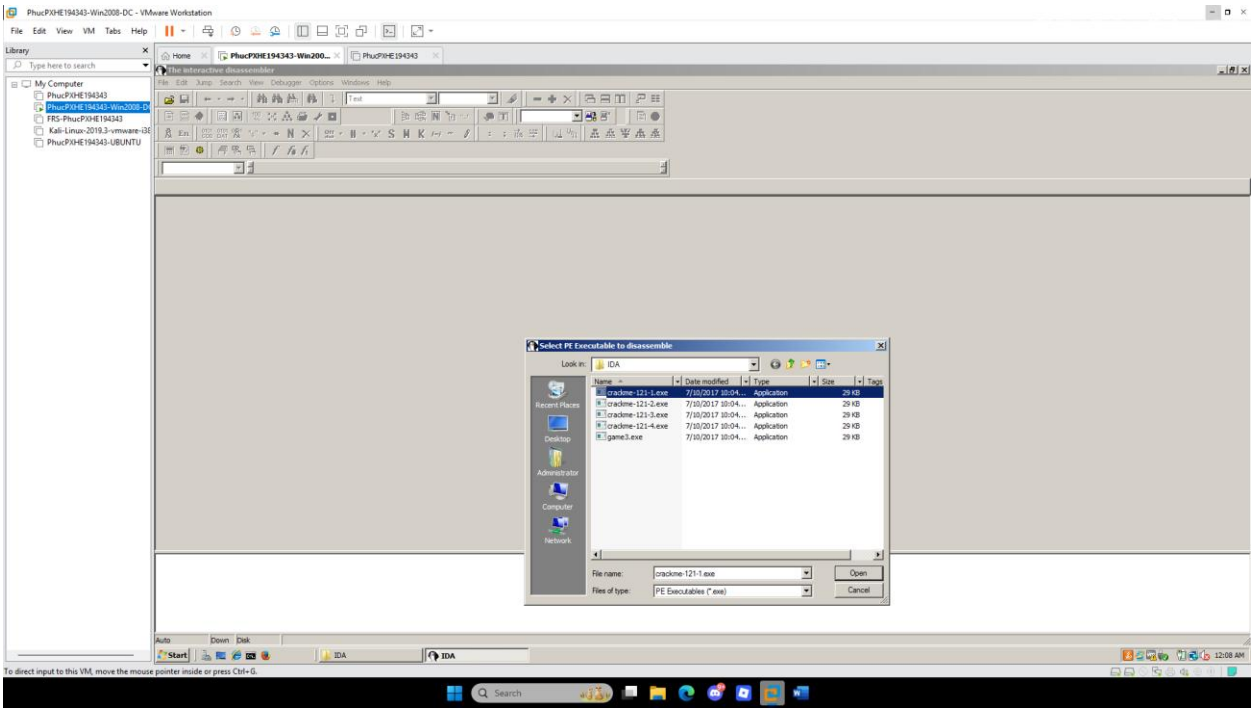

PhucPXHE194343-Win2008-DC - VMware Workstation
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\IDA
C:\IDA>upx.exe crackme-121-1.exe
'upx.exe' is not recognized as an internal or external command,
operable program or batch file.
C:\IDA>upx crackme-121-1.exe
C:\IDA>"C:\Program Files\upx394w\upx.exe" crackme-121-1.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017
File size Ratio Format Name
29184 -> 9728 33.33% win32/pe crackme-121-1.exe
Packed 1 file.
C:\IDA>_

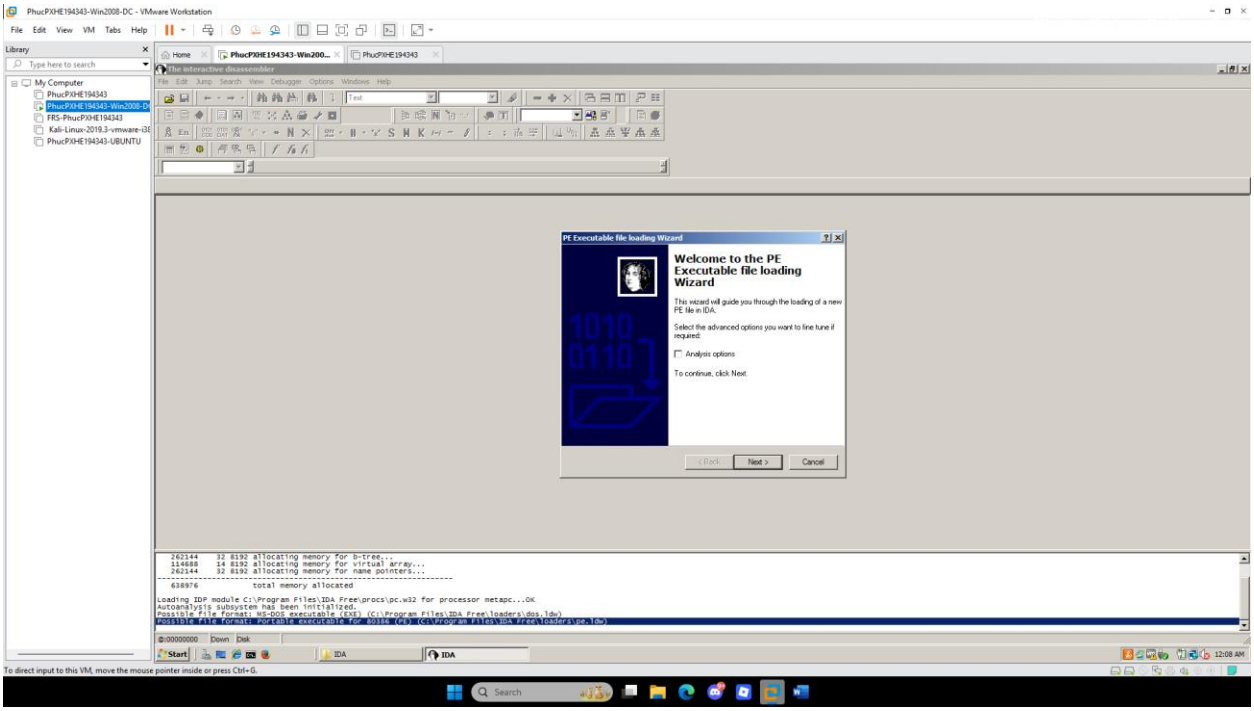

PhucPXHE194343-Win2008-DC - VMware Workstation
PEiD v0.95
File: C:\IDA\crackme-121-1.exe
Entrypoint: 0001CC10
EP Section: UPX1
File Offset: 00002010
First Bytes: 60,BE,00,B0
Linker Info: 10.0
Subsystem: Win32 console
UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo
Multi Scan
Task Viewer
Options
About
Exit
Stay on top

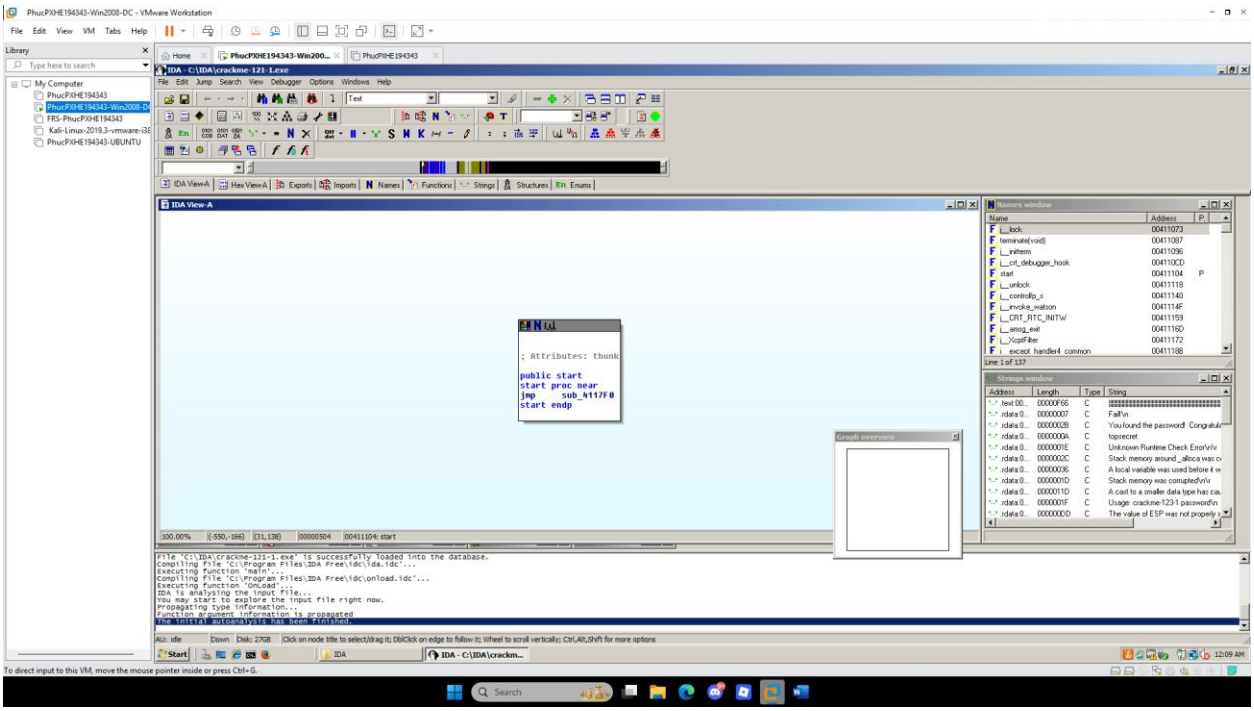

PhucPXHE194343-Win2008-DC - VMware Workstation
IDA - C:\IDA\crackme-121-1.exe
IDA View-A
Names window
Strings window
Graph overview
File 'C:\IDA\crackme-121-1.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling 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.

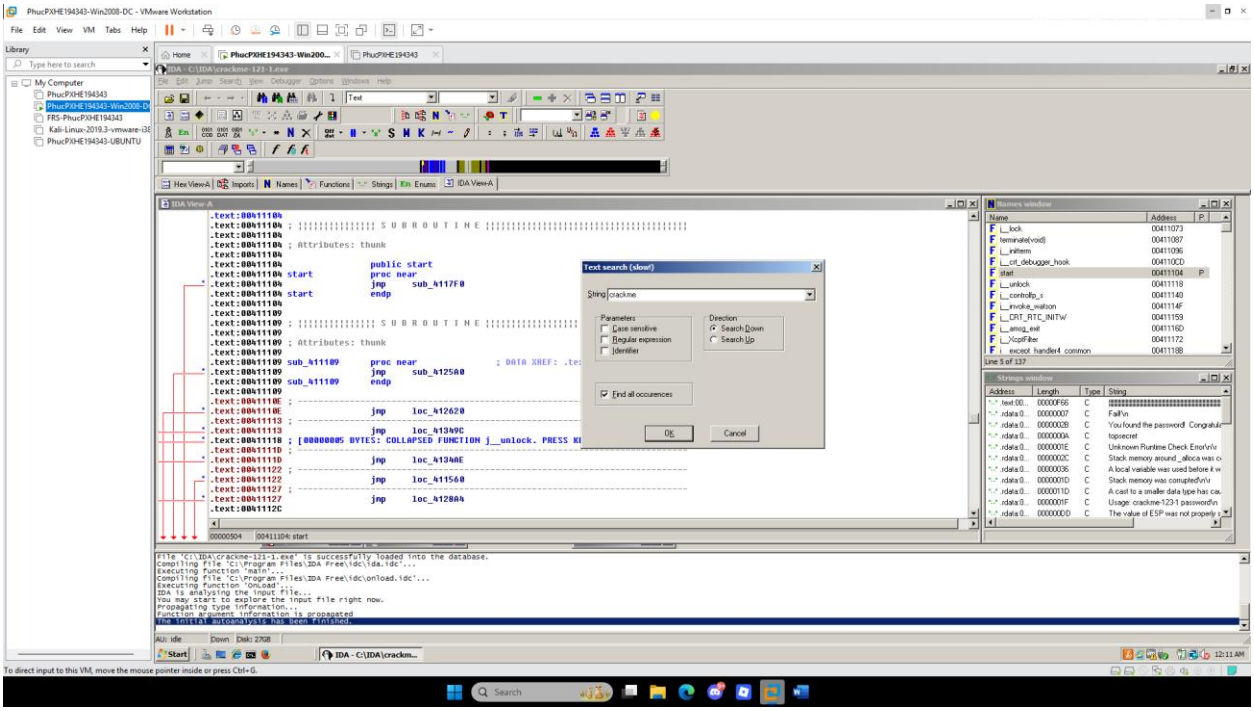


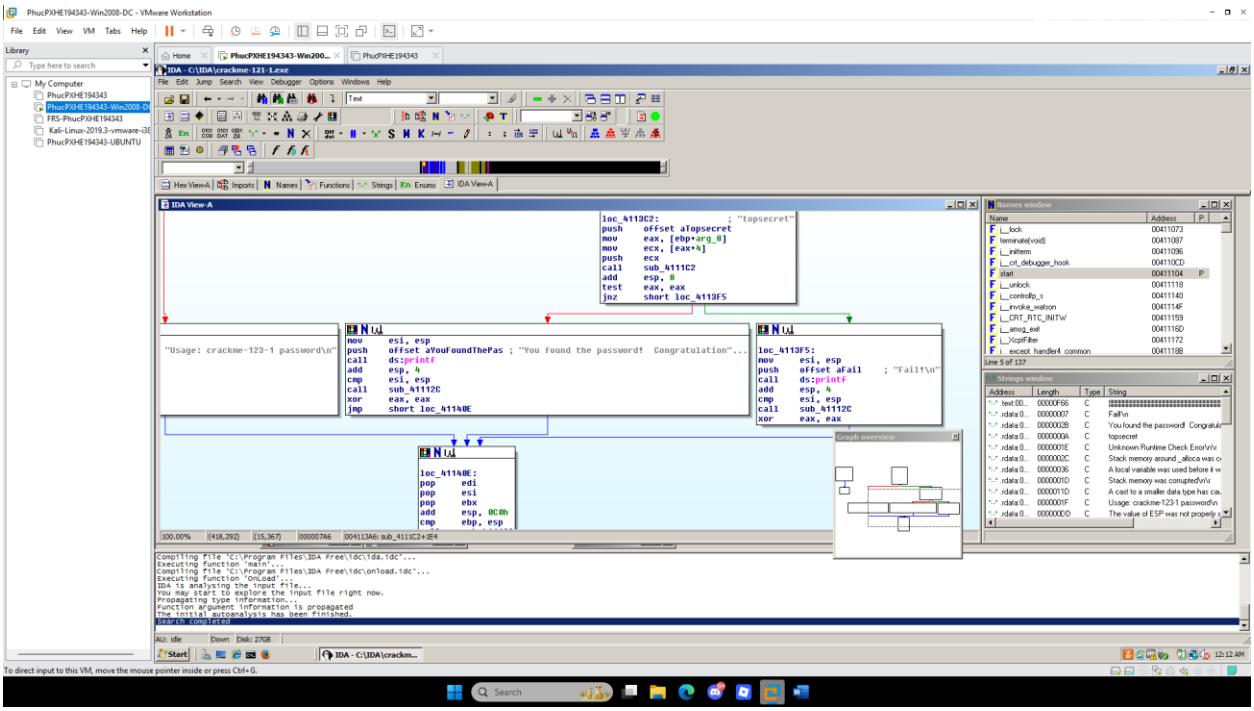
Lab 15.2

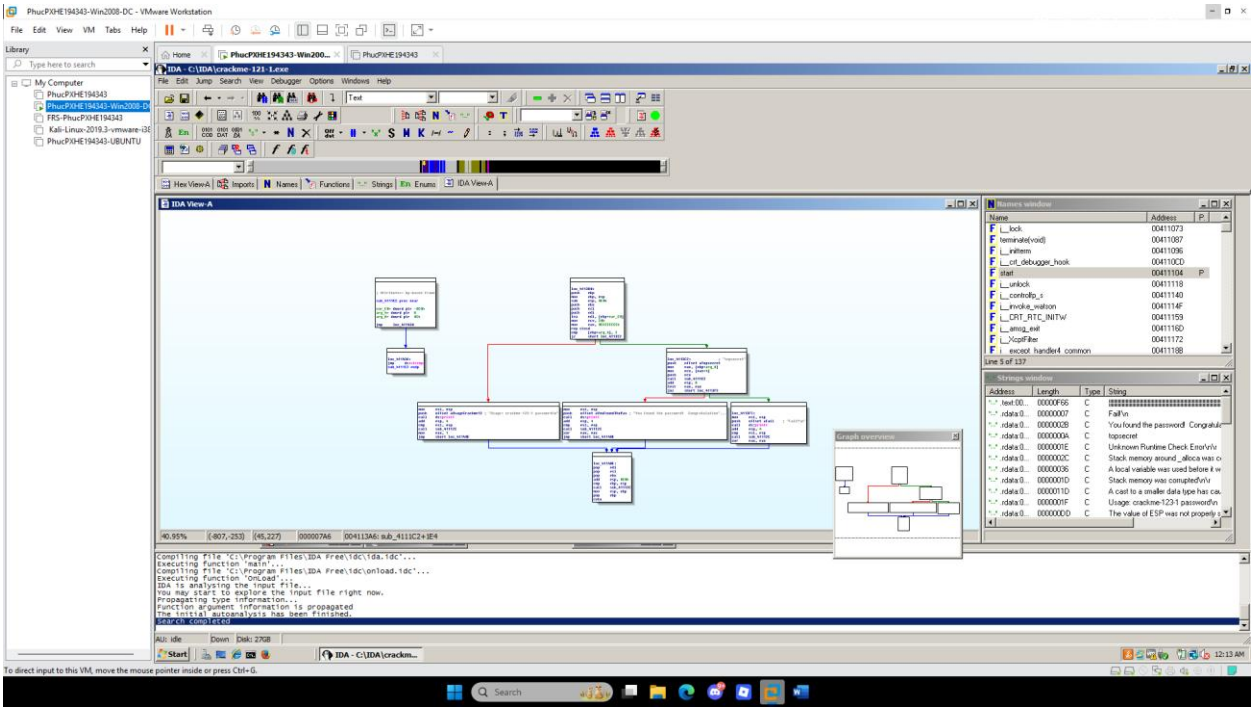


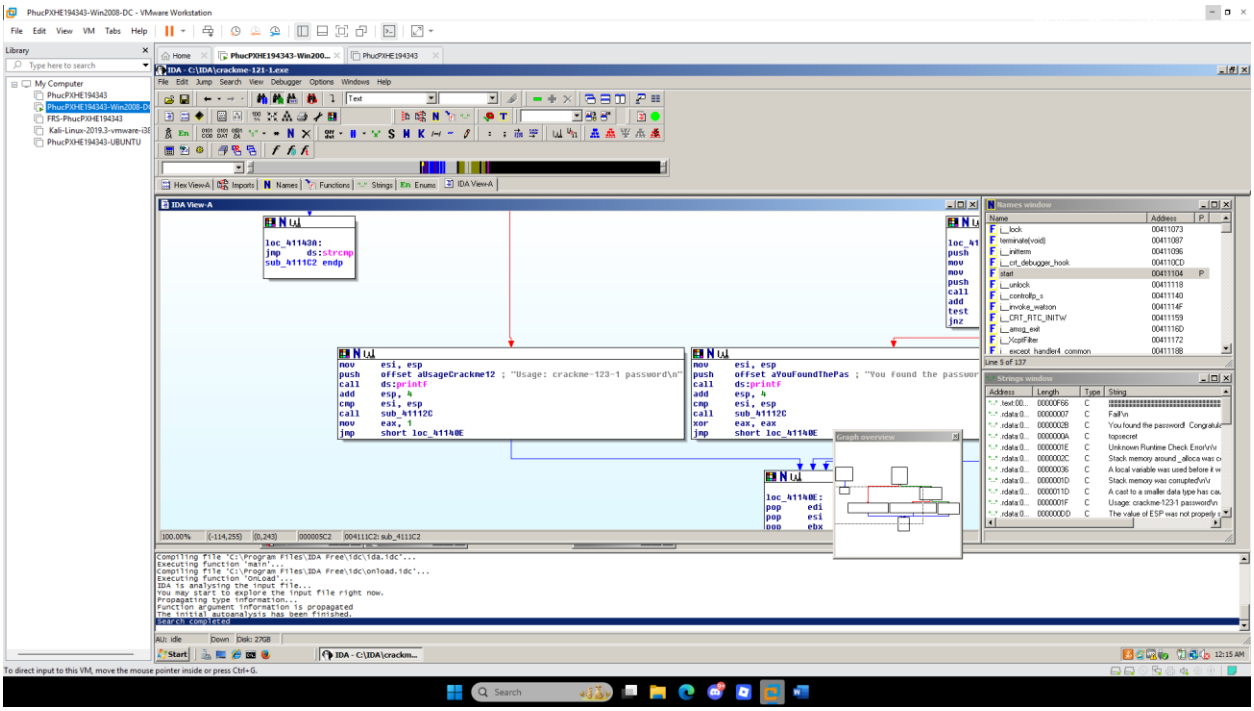

PhucPXHE194343-Win2008-DC - VMware Workstation
PE Executable file loading Wizard
Welcome to the PE Executable file loading Wizard
This wizard will guide you through the loading of a new PE file in IDA.
Select the advanced options you want to fine tune if required:
Analysis options
To continue, click Next.
< Back
Next >
Cancel

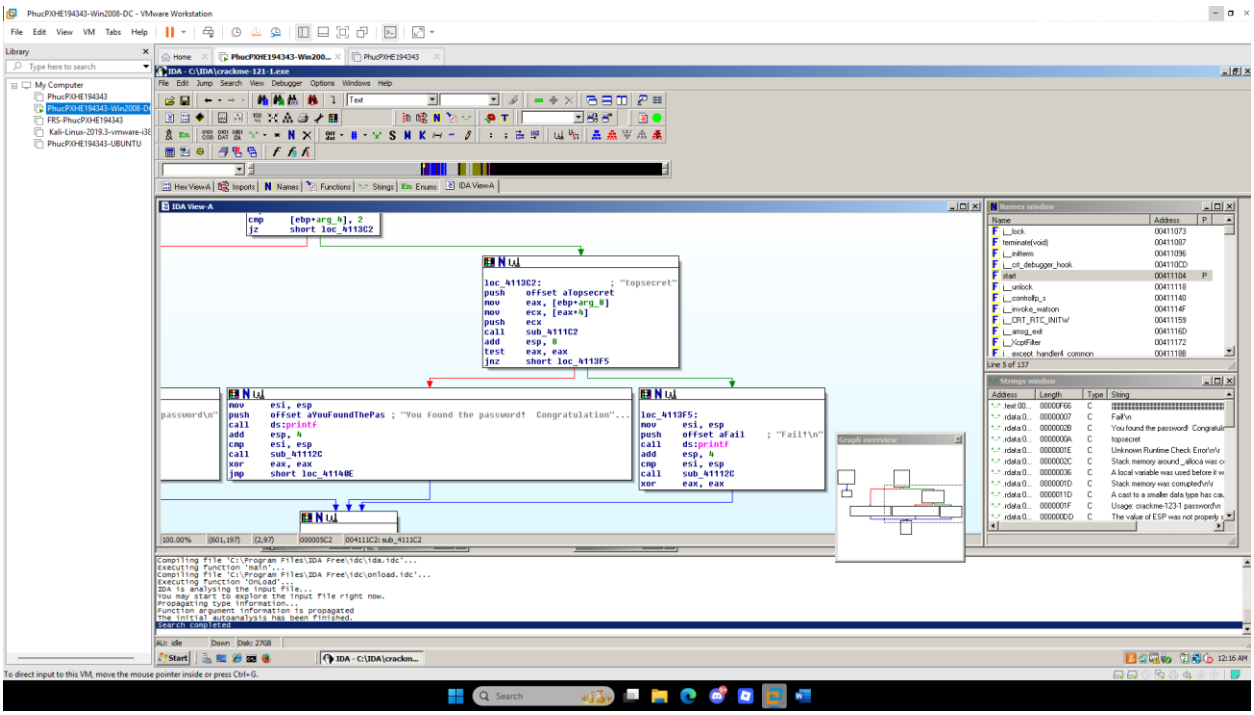

PhucPXHE194343-Win2008-DC - VMware Workstation
IDA - C:\IDA\crackme-121-1.exe
IDA View-A
; Attributes: thunk
public start
start proc near
jmp sub_4117F0
start endp
Names window
Strings window

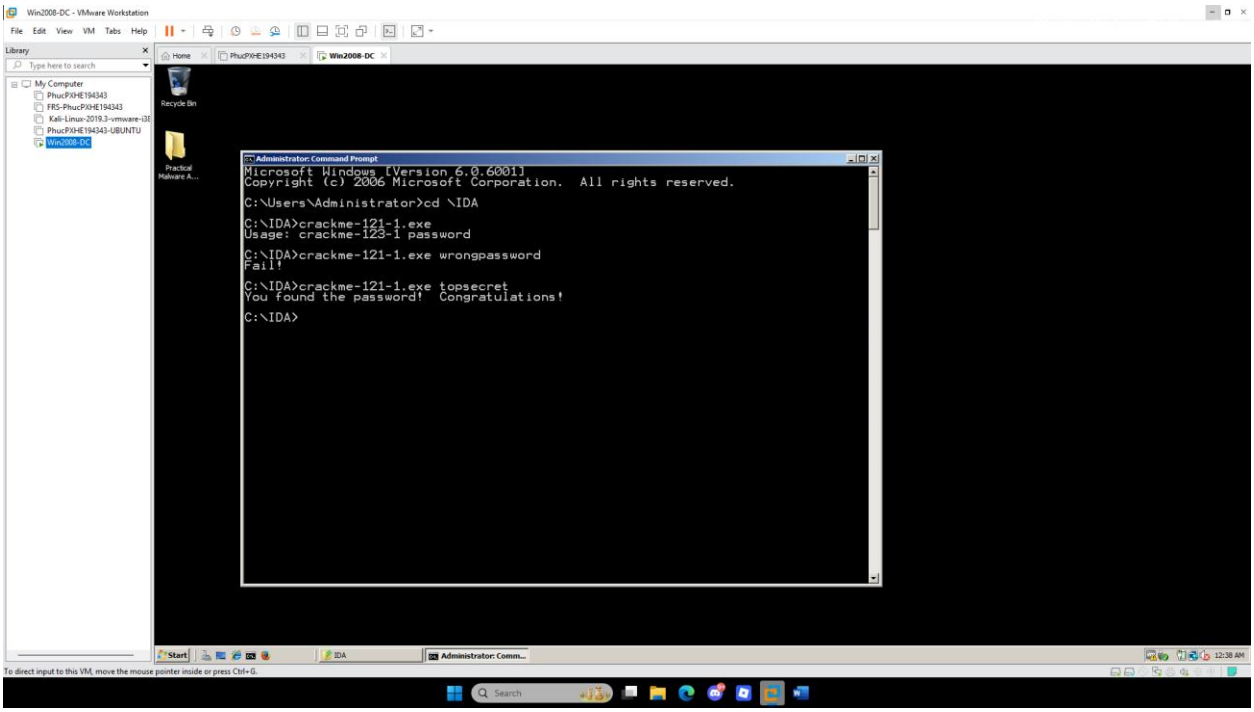





PhucPXHE194343-Win2008-DC - VMware Workstation
IDA - C:\IDA\crackme-121-1.exe
IDA View-A
Names window
Strings window
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is 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.


PhucPXHE194343-Win2008-DC - VMware Workstation
IDA - C:\IDA\crackme-121-1.exe
IDA View-A
loc_4114A0:
jmp ds:strcmp
sub_4111C2 endp
mov esi, esp
push offset aUsageCrackme12 ; "Usage: crackme-123-1 password\n"
call ds:printf
add esp, 4
cmp esi, esp
call sub_41112C
mov eax, 1
jmp short loc_4114BE
mov esi, esp
push offset aYouFoundThePas ; "You found the passwor
call ds:printf
add esp, 4
cmp esi, esp
call sub_41112C
xor eax, eax
jmp short loc_4114BE
loc_4114BE:
pop edi
pop esi
pop ebx
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.



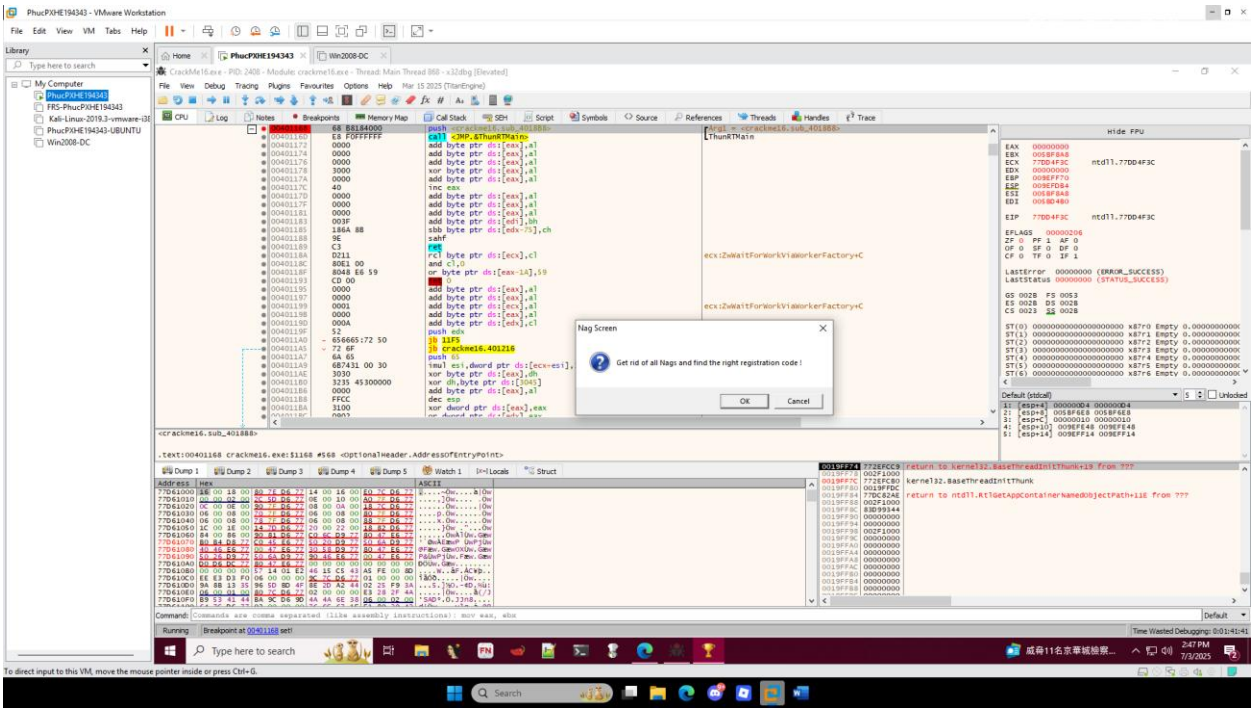


Crack Me 16:

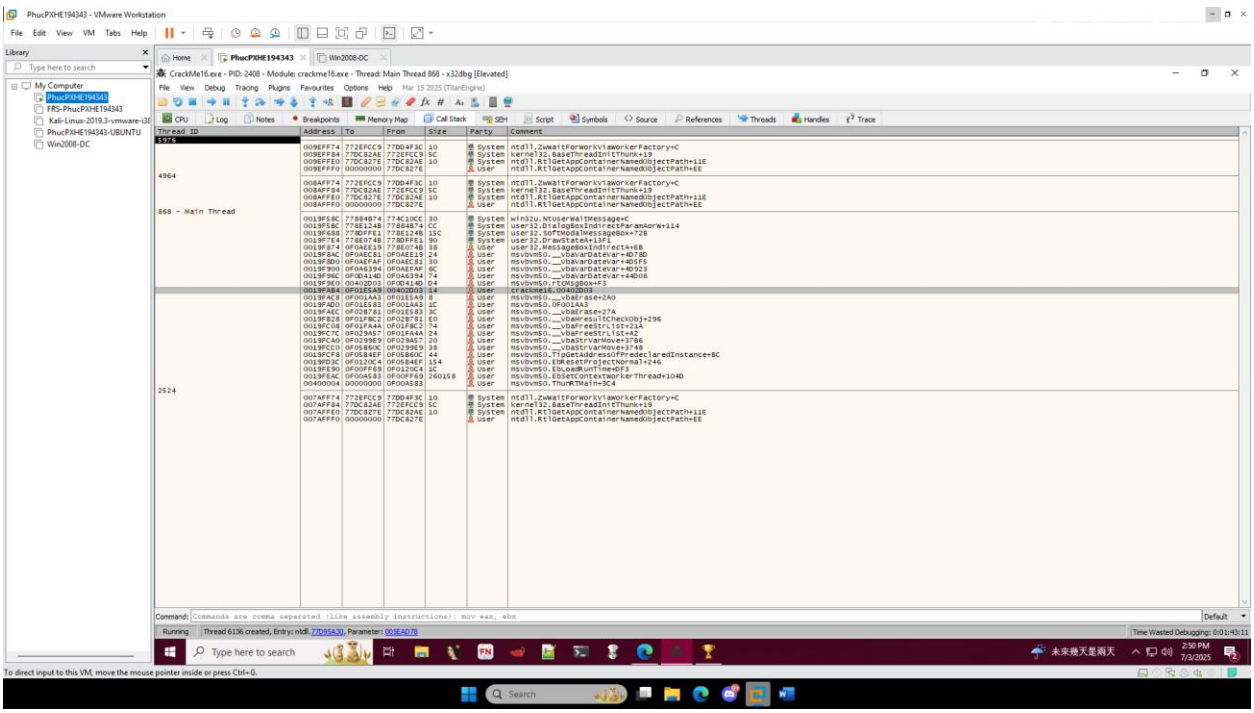
Part 1: Removing Nag

1. Giờ chúng ta sẽ xem chương trình gọi đến cái nag xuất hiện đầu tiên ở đâu và đặt breakpoint tại đó

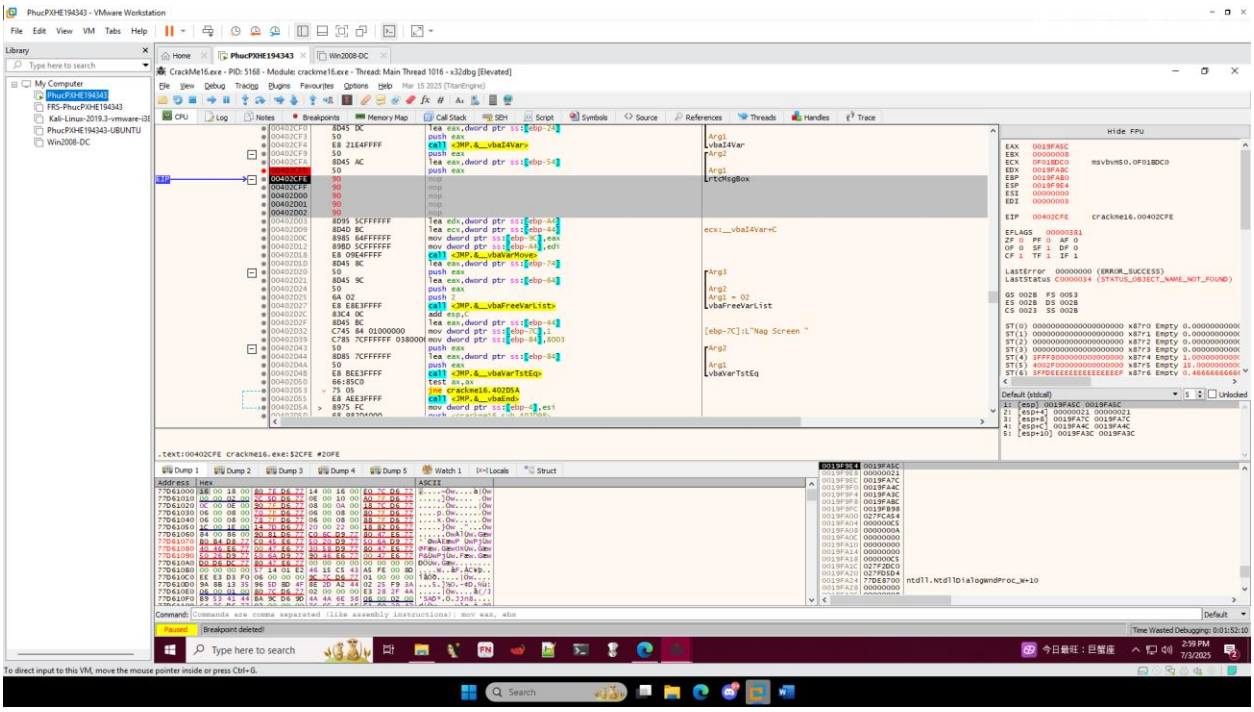
B1: bấm run sau đó khi chương trình xuất hiện nag đầu tiên thì pause chương trình lại



B2: Chọn call stack để xem chương trình gọi cửa sổ đó ở đâu và click vào

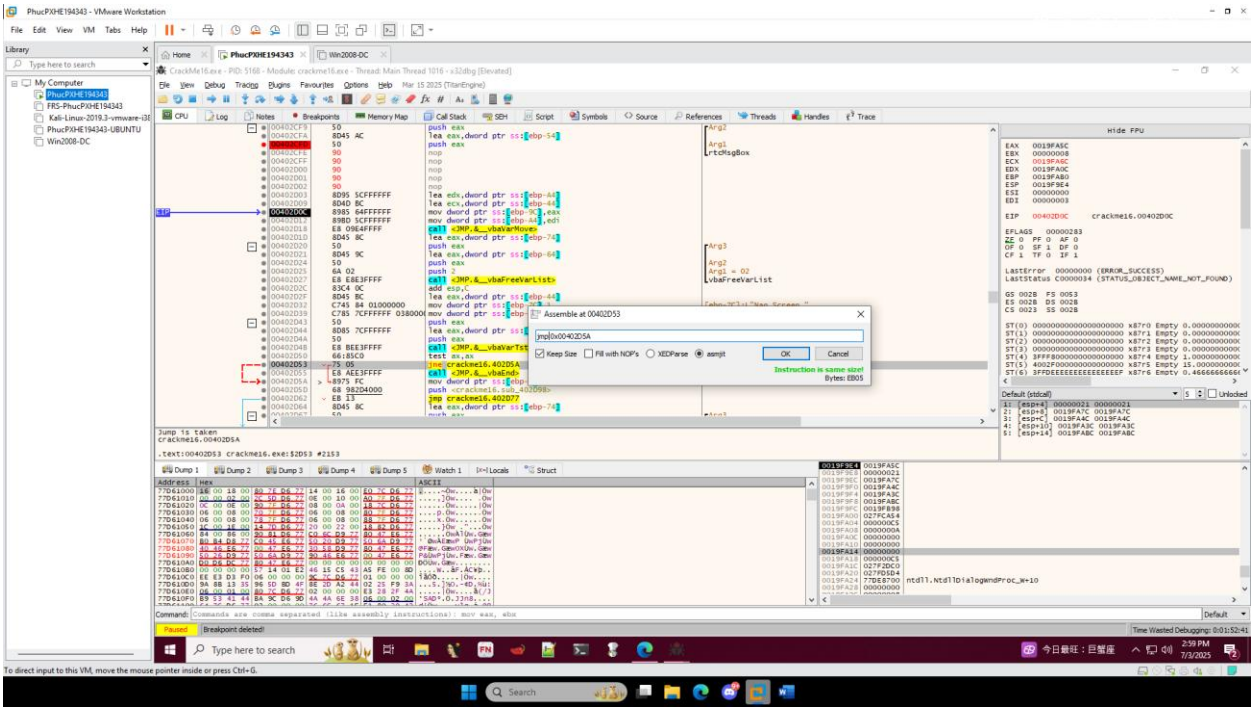


B3: Ngay trên đó chính là lệnh call gọi nag đó xuất hiện và chúng ta đặt breakpoint tại đó, Restart lại và cho run vì chúng ta đã đặt breakpoint nên cửa sổ đã không xuất hiện nên muốn sau này Nag không xuất hiện chúng ta đặt nó thành nop là xong

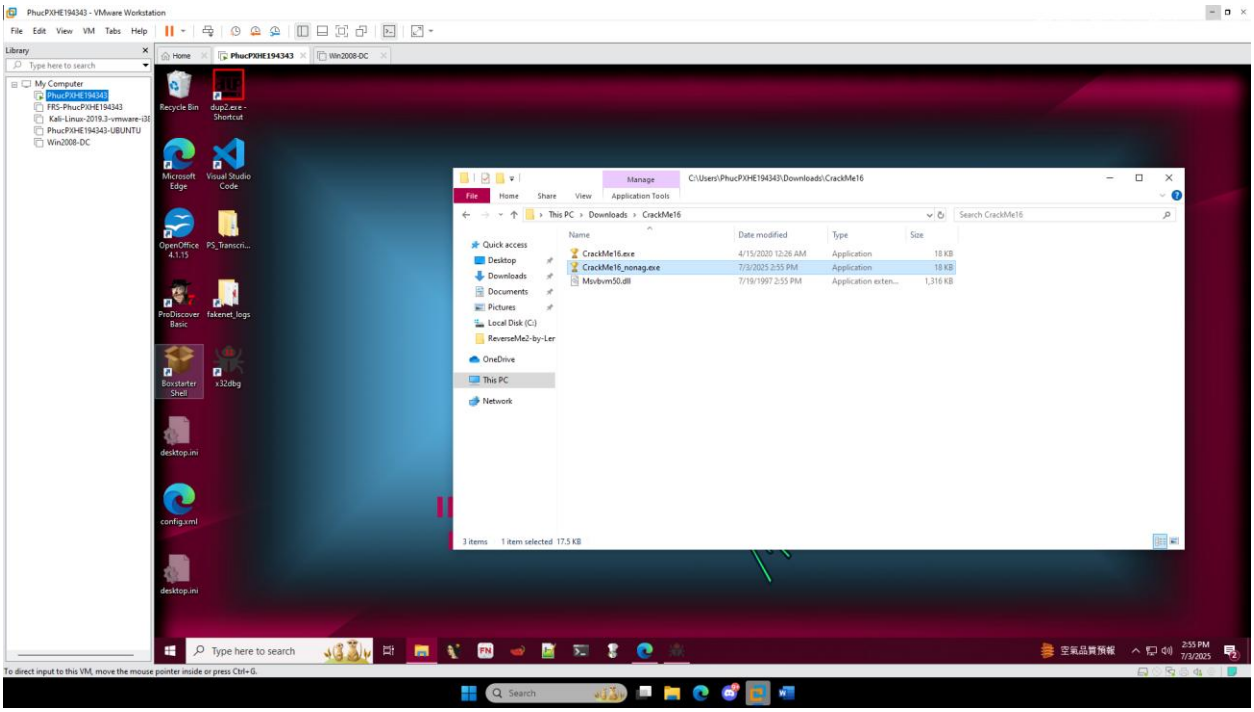


B4: Chạy lại và xem kết quả nhưng khi chạy lại debugger đã bị đóng lại và quit chứng tỏ có lỗi ở đâu đó

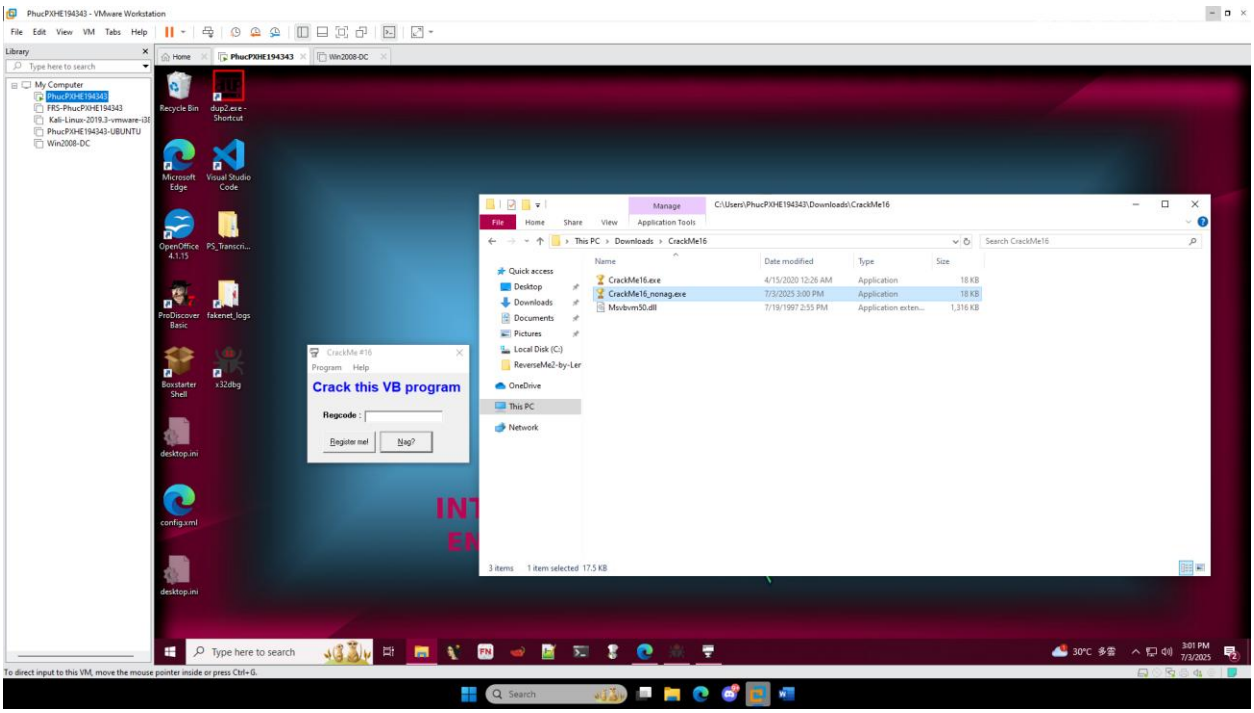
- Chúng ta cần xem lỗi xảy ra ở đâu mà chương tình quit luôn không hiện thị cửa sổ chính bằng Trace Coverage để xem chương trình thực hiện từng bước đến khi đóng lại
- Chương trình chạy đến dòng 00402D55 và đóng lại vì thế nên chúng ta sẽ làm cho dòng đó không được thực thi, nếu nhìn ngay trên có thể có câu lệnh jne có thể nhảy qua dòng đó
- Chúng ta sẽ đổi jne thành jmp để câu lệnh đó luôn thực hiện và câu lệnh đóng chương trình sẽ không được thực hiện nữa



B5: Chúng ta tiến hành patch chương trình

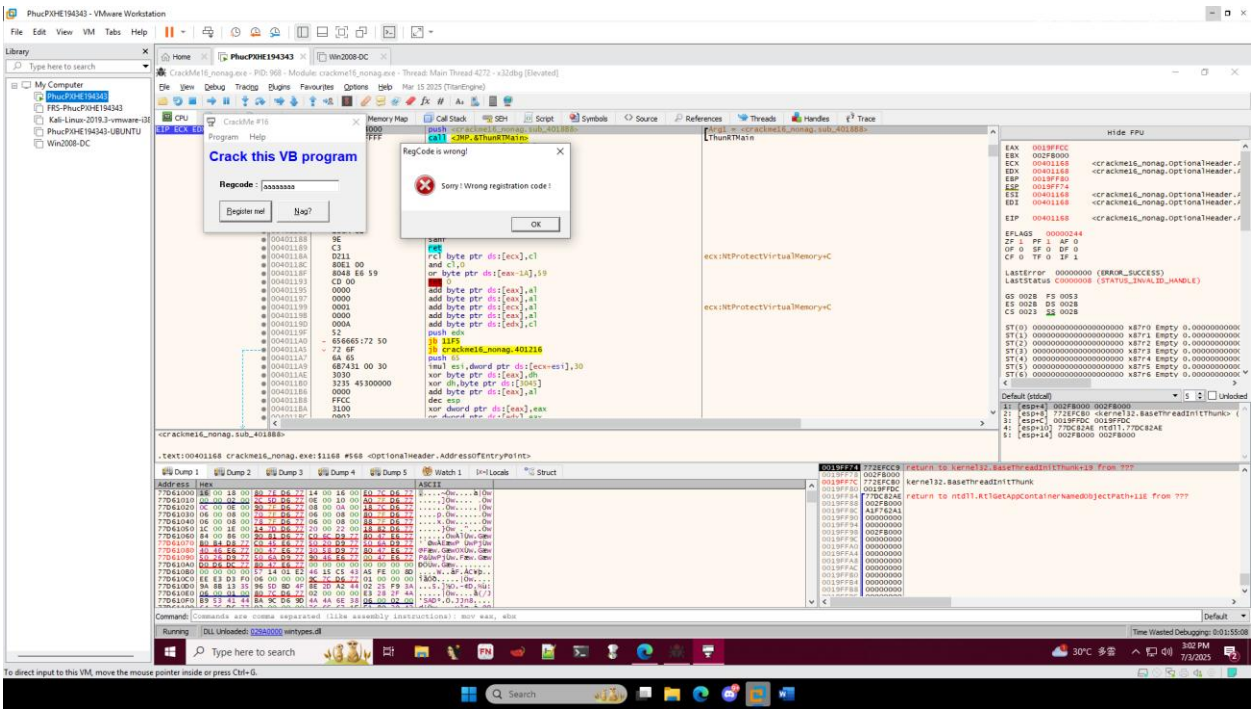


B6: Chạy thử, thì lúc đấy chương trình đã hoàn toàn loại bỏ nag đầu tiên.

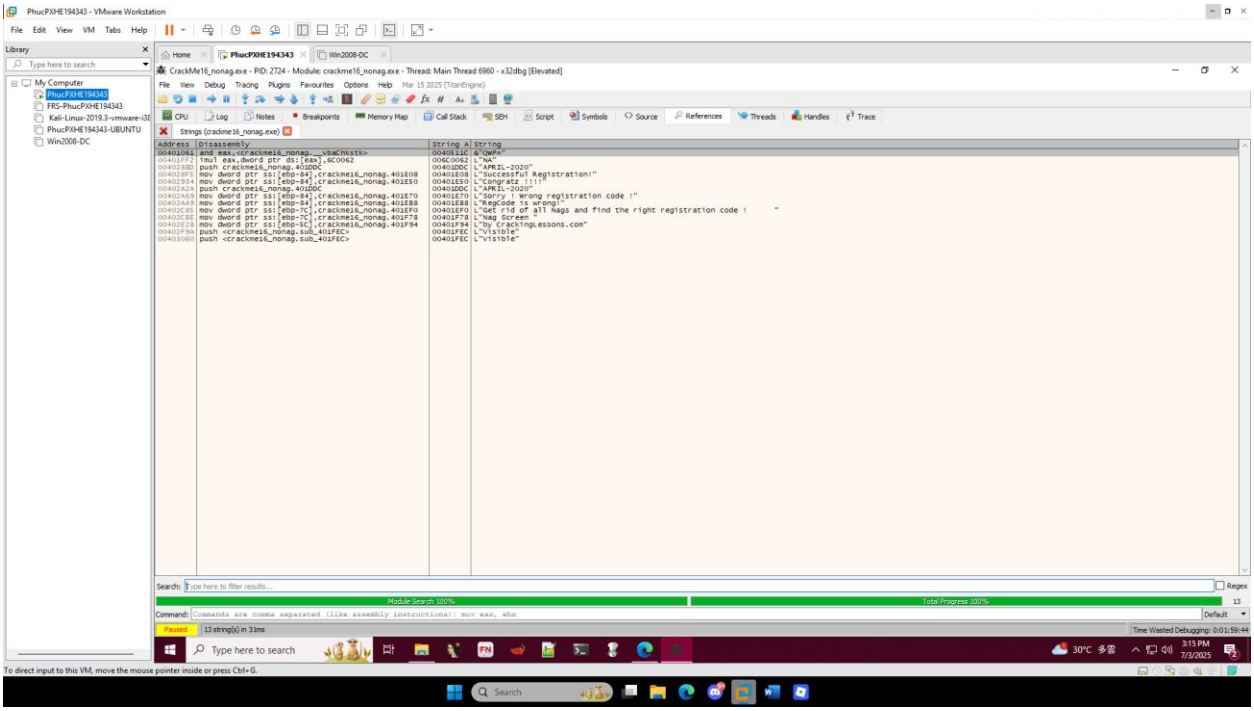


Part 2: Crack the Program

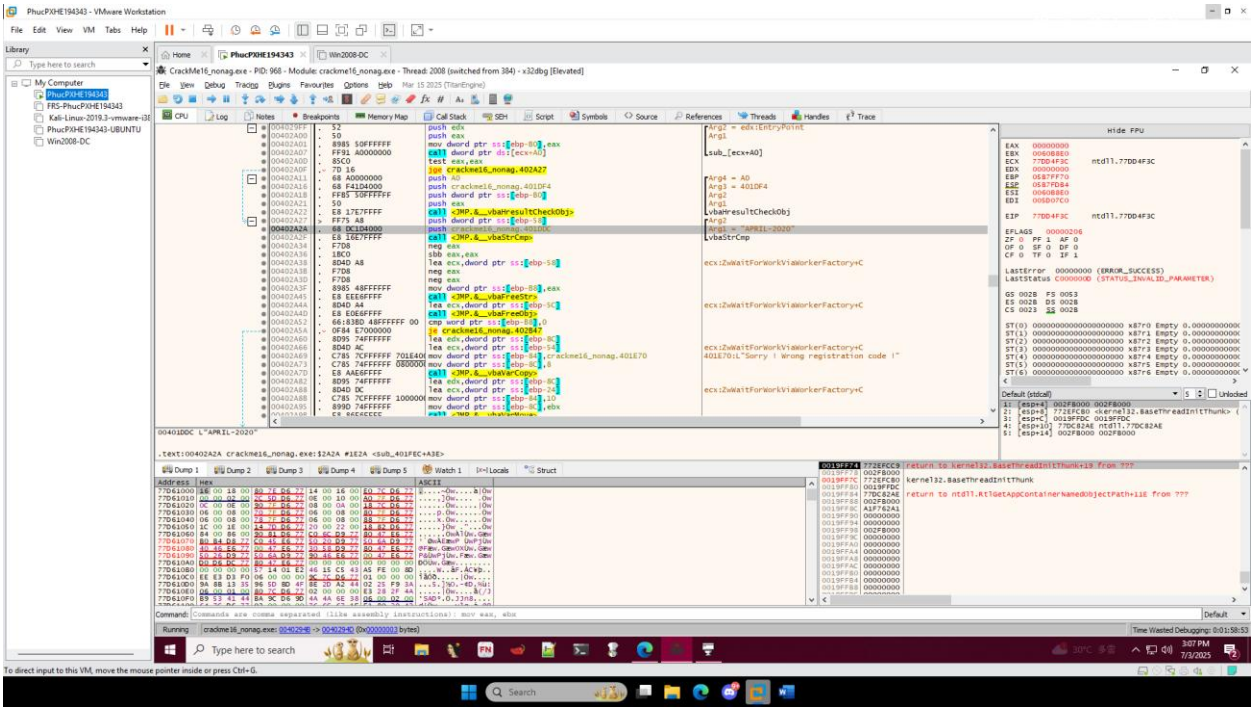
1. Tiếp theo chúng ta sẽ tìm Recode để crack được cái tiếp theo, nếu nhập sai Regcode thì sẽ thông báo lỗi như hình bên dưới



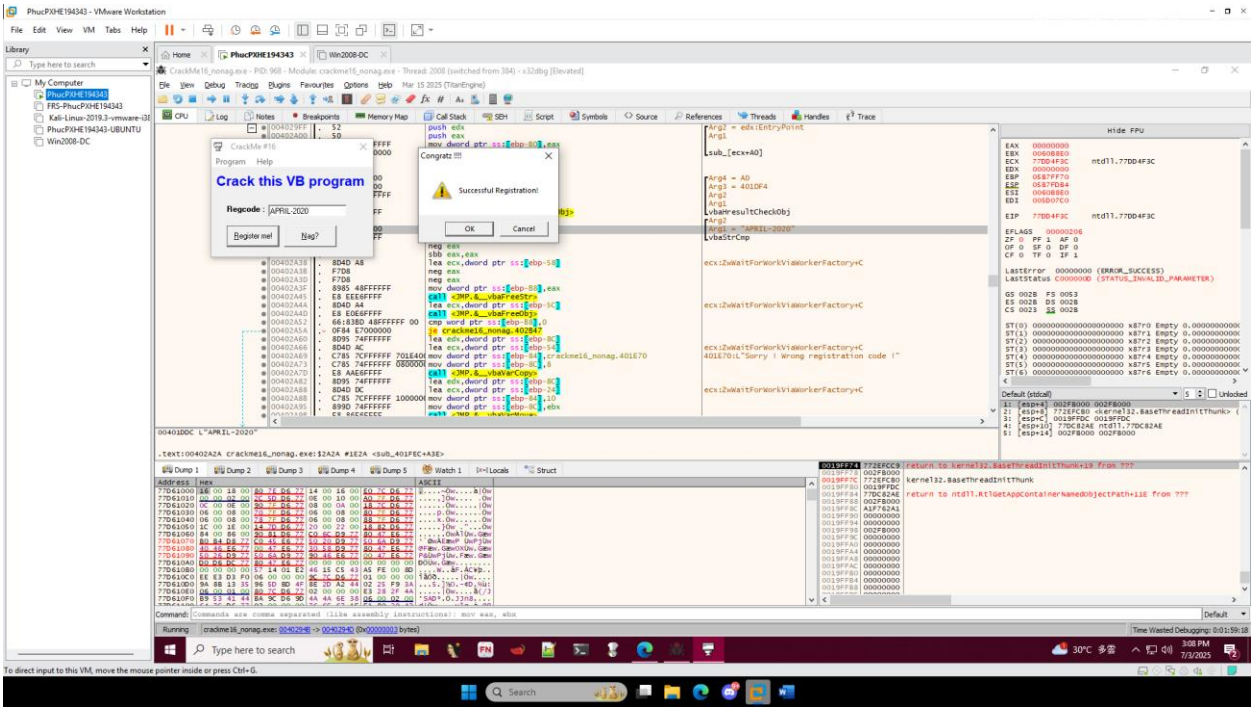
2. Chúng ta sẽ mở String Reference để xem



3. Đọc code ta thấy được rằng là có 1 hàm mang tên vbaStrCmp là 1 hàm string comparison, nó lấy string được người dùng nhập vào so sánh với string đã cho nếu trùng nhau thì báo correct, và ngược lại. Chúng ta thấy được dòng string mặc định đấy là “APRIL-2020”



4. Thử Serial key đã cho và đã thành công crack được chương trình


PhucPXHE194343 - VMware Workstation
CrackMe16_nonag.exe - PID: 968 - Module: crackme16_nonag.exe - Thread: 2008 (switched from 384) - x32dbg [Elevated]
CrackMe #16
Program Help
Crack this VB program
Regcode : APRIL-2020
Register me!
Nag?
Congratz !!!
Succesful Registration!
OK
Cancel
00401DDC L"APRIL-2020"
.text:00402A2A crackme16_nonag.exe:$2A2A #1E2A <sub_401FEC+A3E>
Hide FPU
Type here to search
30°C 多雲
3:08 PM
7/3/2025