VnCeRt nEwBiEs cRaCkErS TEAM

Basic Reversing Tutorials

How to inject code into an EXE file

This tutorial for educational purposes only

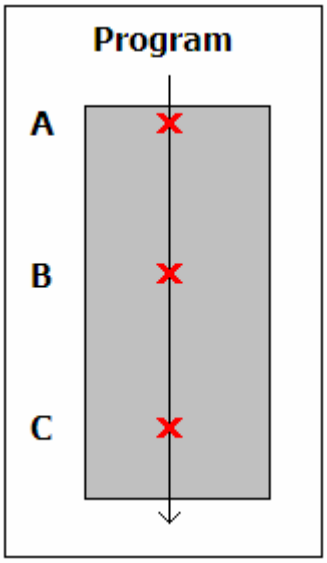
Lời nói đầu

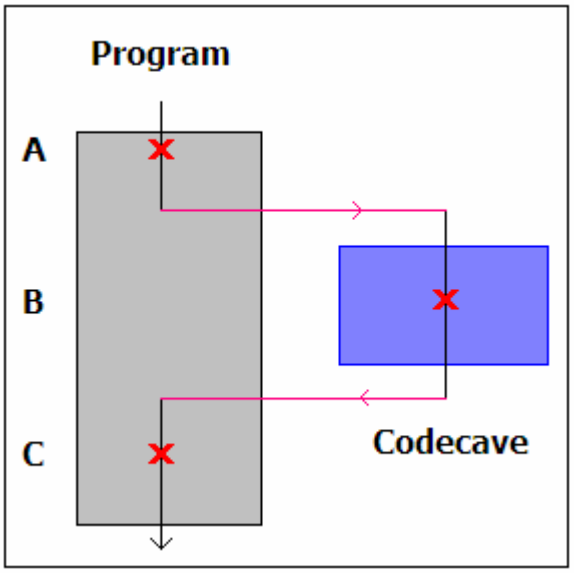
Nếu ai đã từng reversing một chương trình thì ắt hẳn bạn biết rằng ở đâu đó sau đoạn code chính của chương trình có ít hay nhiều một vùng free byte (DB 00). Thế có bạn hỏi vùng free byte này là gì, nó được dùng để làm gì ?

– Vùng free byte này được giang hồ gọi với một cái tên khác là **Code-Caves**. Định nghĩa khái niệm này thì có rất nhiều, nhưng bạn có thể nắm cơ bản khái niệm Code-Caves như sau **đó là một vùng trống mà tại đây ta có thể chèn thêm một số lượng dòng code hữu hạn mà sự thêm code này sẽ làm thay đổi sự thực thi của một chương trình**.

Hay có thể định nghĩa theo cách khác như sau : đó là một sự chuyển hướng của sự thực thi chương trình đến một vị trí khác và sau đó trở lại vùng code chính nơi mà sự thực thi của chương trình đã bắt đầu trước đó.

Để hình dung Code-Caves bạn theo dõi hình sau :





Chưa chèn code vào vùng Code-Caves **Đã thực hiện việc chèn code vào Code-Caves**

– Tại sao chúng ta cần phải dùng tới Code-Caves ? – Lý do đơn giản bởi vì bằng cách này hay cách khác ta rất khó can thiệp trực tiếp vào source code của chương trình chính để có thể modify source code này khi có một số lý do cần thiết. Vì thế, muốn đạt được mục đích là nhất định phải thêm một đoạn code nào đó, thì ta phải modify file EXE một cách physically ở mức độ assembly để tạo nên sự thay đổi.

Để hiểu rõ hơn về Code-Caves, các bạn xem tut được sơ dịch trong forum hoặc tham khảo ở :

http://www.codeproject.com/cpp/codecave.asp

Target : **Notepad.exe**
Tools : **OllyDBG 1.10**

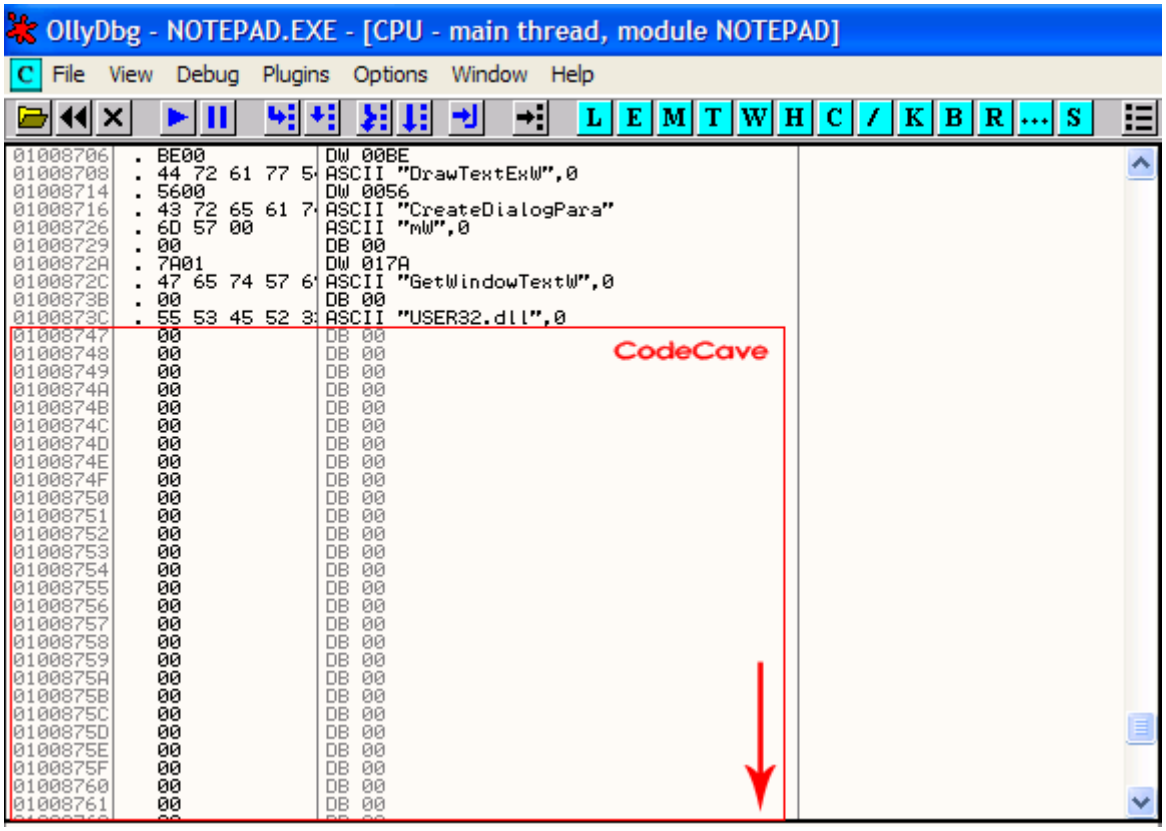
How to inject code into an EXE file

Mục đích của chúng ta là chèn một số code vào trong **Notepad.exe**. Trong trường hợp này, yêu cầu chỉ chèn vào một MessageBox đơn giản lúc Notepad được load lên.

– Load notepad.exe vào OllyDBG, bạn dừng tại đây :

```
0100739D   6A 70            PUSH 70
0100739F   68 98180001      PUSH notepad.01001898
010073A4   E8 BF010000      CALL notepad.01007568
010073A9   33DB             XOR EBX,EBX
010073AB   53               PUSH EBX
010073AC   8B3D CC100001    MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModuleHandleA>]
010073B2   FFD7             CALL EDI
010073B4   66:8138 4D5A     CMP WORD PTR DS:[EAX],5A4D
010073B9   75 1F            JNZ SHORT notepad.010073DA
```

– Việc đầu tiên bạn cần làm là tìm vùng Code-Caves để thực hiện việc chèn code. Bạn kéo thanh trượt của OllyDBG xuống dưới cùng của đoạn code chính, bạn tìm được vùng Code-Caves với độ free byte trống rất nhiều :

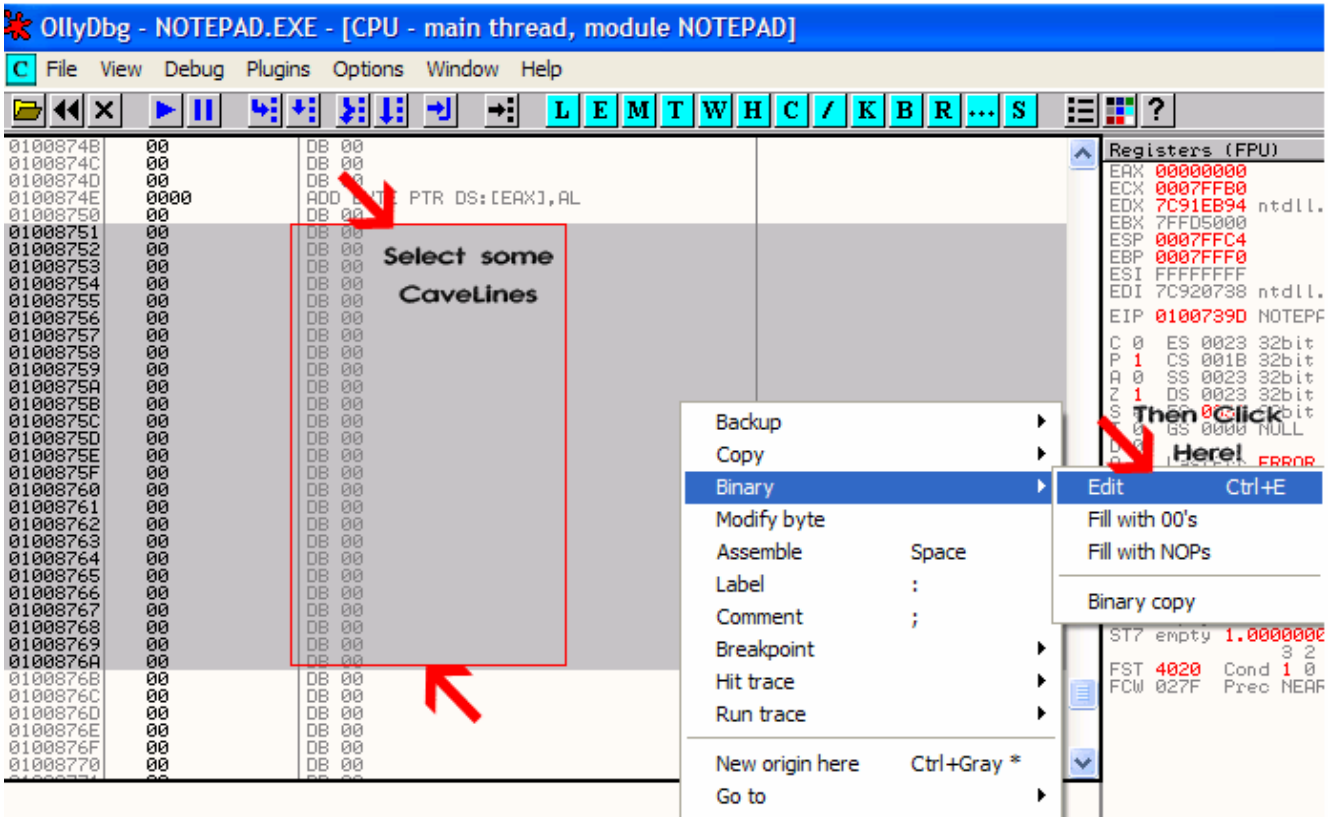


– Với yêu cầu chỉ chèn một MessageBox đơn giản, bạn cần có kiến thức về API MessageBox :

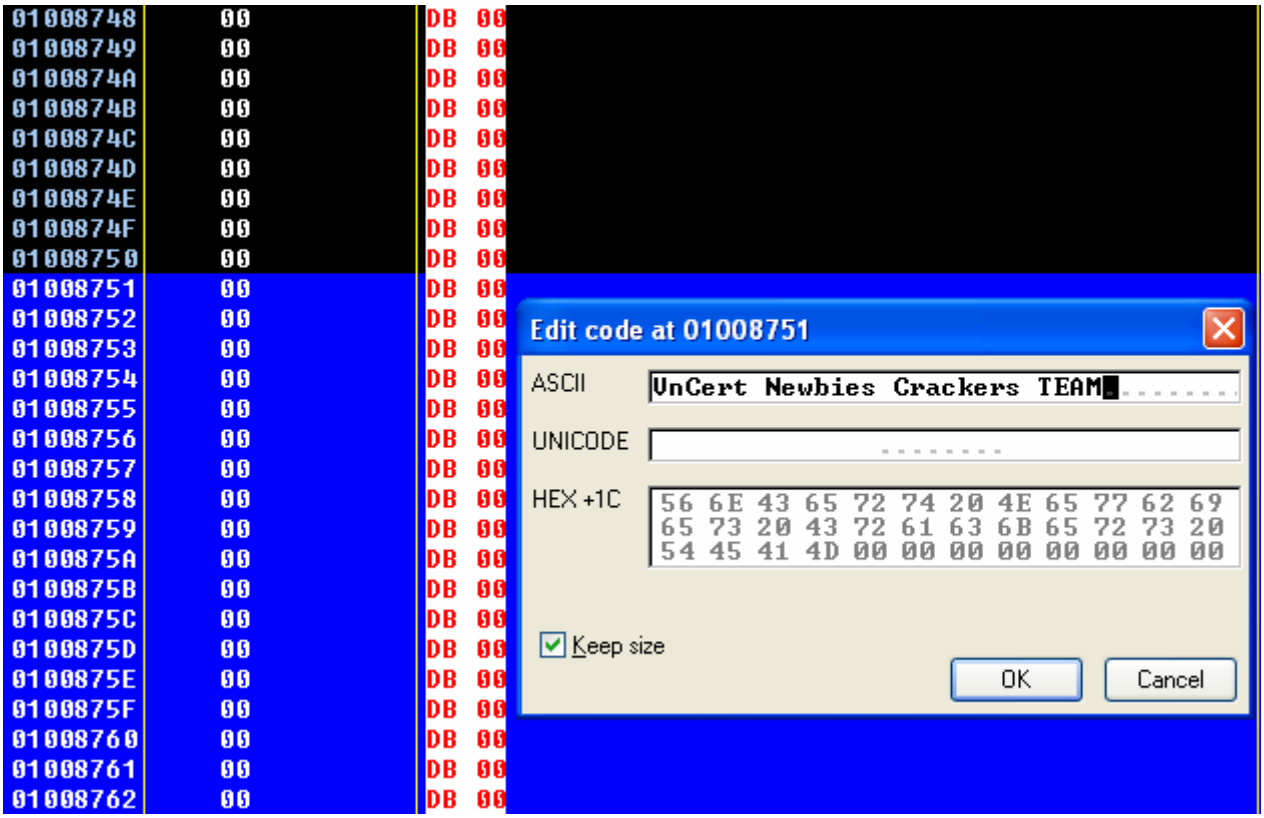
The MessageBox function creates, displays, and operates a message box. The message box contains an application-defined message and title, plus any combination of predefined icons and push buttons.

```
int MessageBox (
        HWND hWnd,              // handle of owner window
        LPCTSTR lpText,         // address of text in message box
        LPCTSTR lpCaption,      // address of title of message box
        UINT uType              // style of message box
);
```

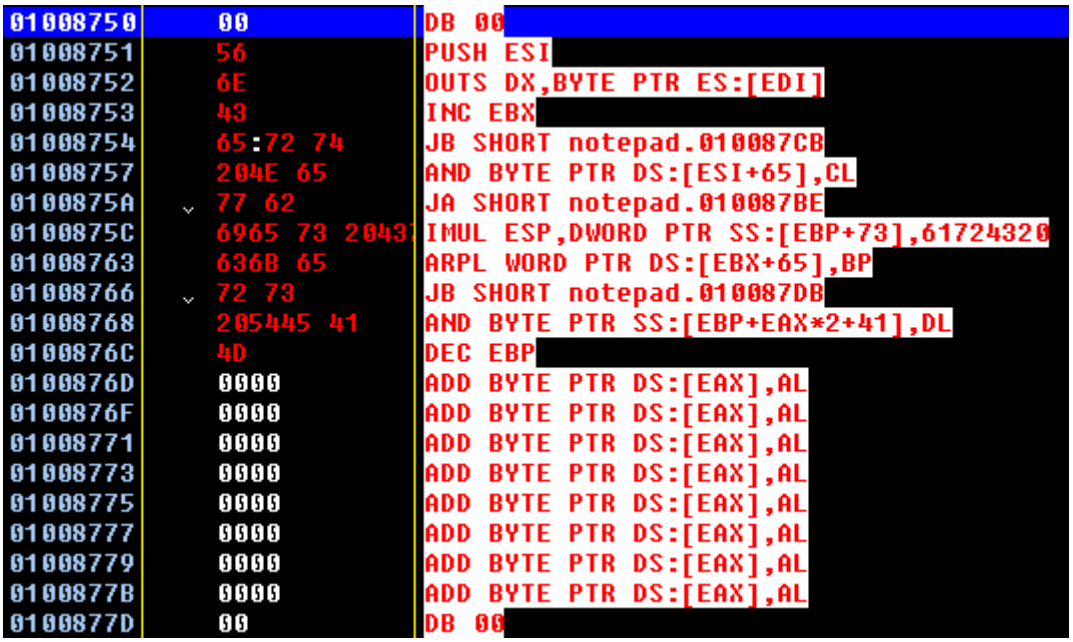
– Để sử dụng MessageBox trước tiên bạn phải tạo một vài dòng text để hiển thị trên TextBox. Trong hình sau, tôi sẽ chọn một số byte trống của Code-Caves để thực hiện việc chèn text :



– Để chèn text bạn nhấn CTRL + E để chèn mã ASCII của text vào như sau :



– Nhấn OK, bạn được như sau. Các dòng có màu đỏ là các dòng bạn vừa thêm vào :

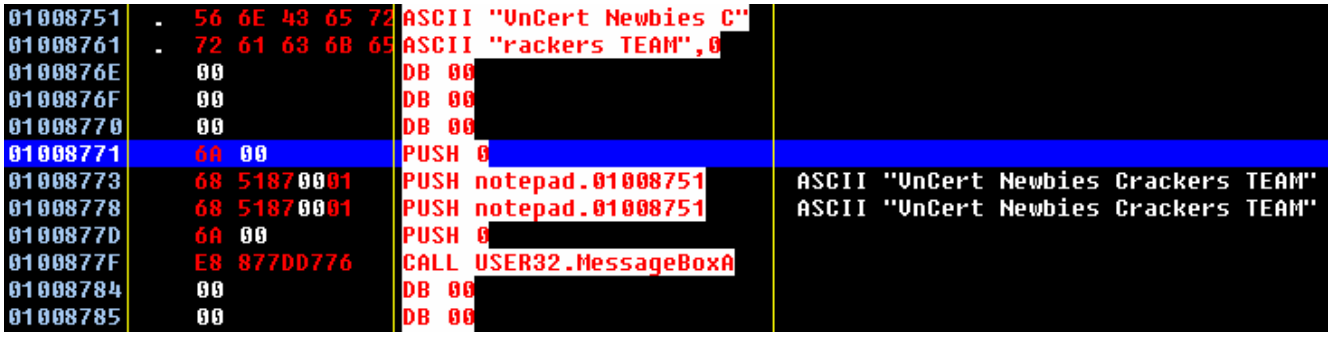


– Nhấn CTRL +A, bạn được như sau :

– Bạn đã thêm text hiển thị trên MessageBox, giờ bạn cần làm là gọi MessageBox thực hiện. Để làm điều đó, bạn cần phải có kiến thức cơ bản về ASM như sau :

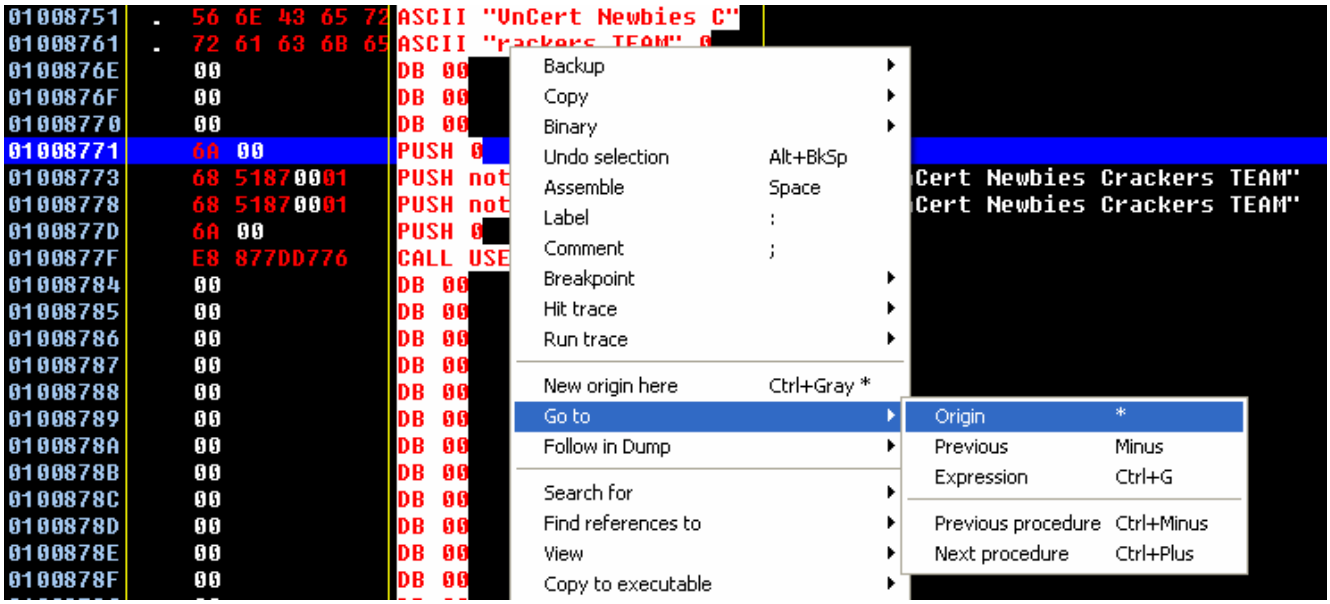
```
PUSH 0              ; BUTTONS = <OK ONLY>
PUSH 1008751        ; CAPTION  = Our adress of the "INJECTED NOTEPAD"
PUSH 1008751        ; MESSAGE  = Same like above.
PUSH 0              ; ICON     = <NO ICON>
CALL MessageBoxA; Run MessageBoxA with the Params above.
```

– Bạn thực hiện việc chèn như sau :

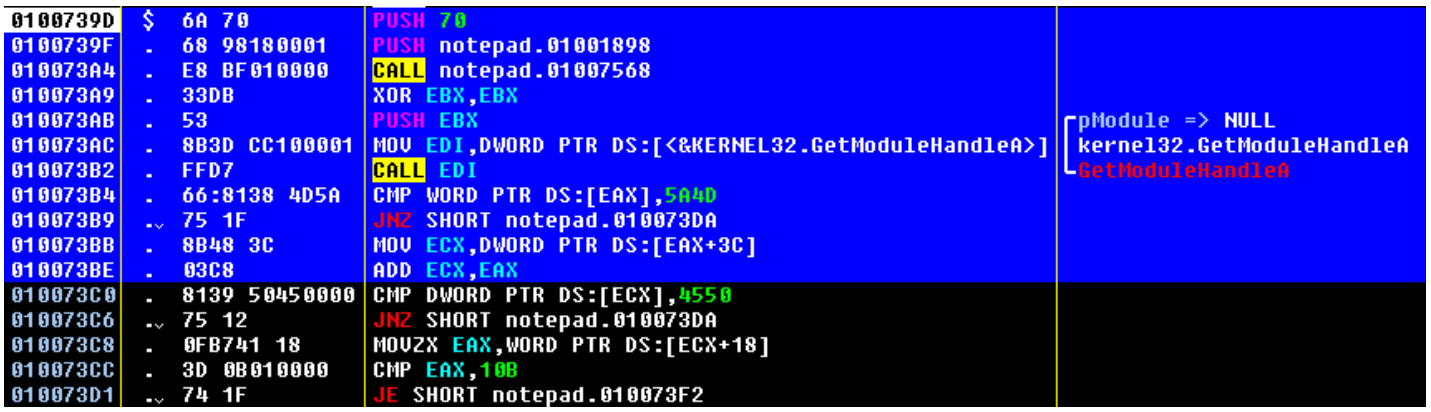


Bạn phải nhớ kỹ địa chỉ **01008771** ? Tại sao phải nhớ ? Nếu như bạn save lại file EXE và chạy file này thì nó sẽ chưa hiển thị MessageBox bởi vì ta mới chèn code ở vùng Code-Caves và chưa có gọi nó thực thi. Và bạn phải nhớ địa chỉ này vì bạn phải làm một lệnh nhảy từ chương trình chính đến đây và từ đây trở về chương trình chính.

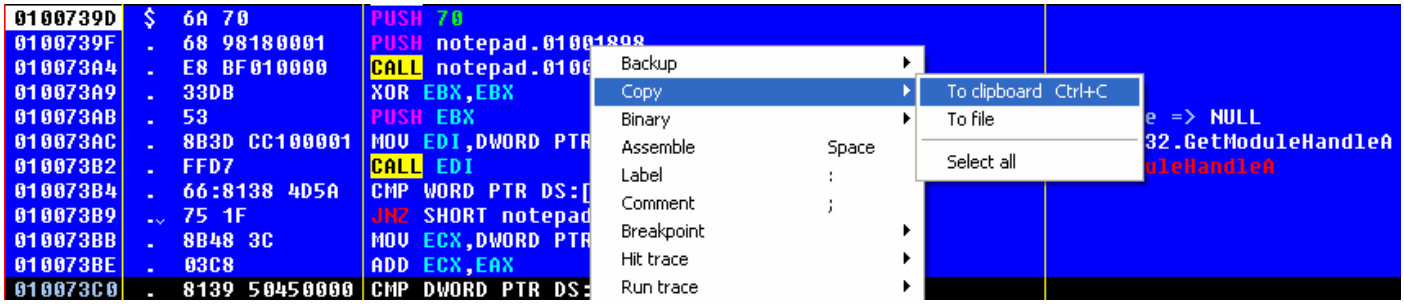
– Bạn nhấn * hoặc click chuột phải vào dòng PUSH 0 này và chọn như sau để trở về chương trình chính :



–Bạn chọn một số dòng lệnh chính từ OEP trở xuống phía dưới tí xíu như sau :



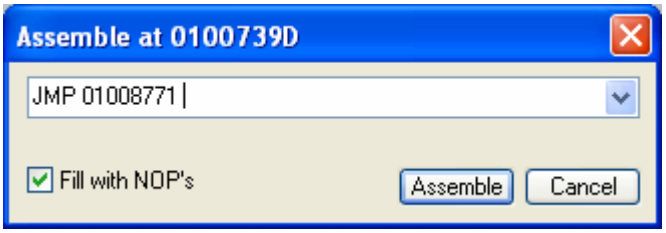
– Click phải chọn **Copy → To Clipboard (CTRL + C)** :



Sau đó CTRL + V để dán vào Notepad hoặc ghi nhớ đoạn code này :

```
0100739D > $  6A 70           PUSH 70
0100739F   .  68 98180001     PUSH notepad.01001898
010073A4   .  E8 BF010000     CALL notepad.01007568
010073A9   .  33DB            XOR EBX,EBX
010073AB   .  53              PUSH EBX                          ; /pModule => NULL
010073AC   .  8B3D CC100001   MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModuleHandleA>]
010073B2   .  FFD7            CALL EDI                          ; \GetModuleHandleA
010073B4   .  66:8138 4D5A    CMP WORD PTR DS:[EAX],5A4D
010073B9   .  75 1F           JNZ SHORT notepad.010073DA
010073BB   .  8B48 3C         MOV ECX,DWORD PTR DS:[EAX+3C]
010073BE   .  03C8            ADD ECX,EAX
```

– Đặt vệt sáng OllyDBG tại dòng PUSH 70, nhấn phím Spacebar, edit lại thành lệnh sau :



– Bạn được như sau :

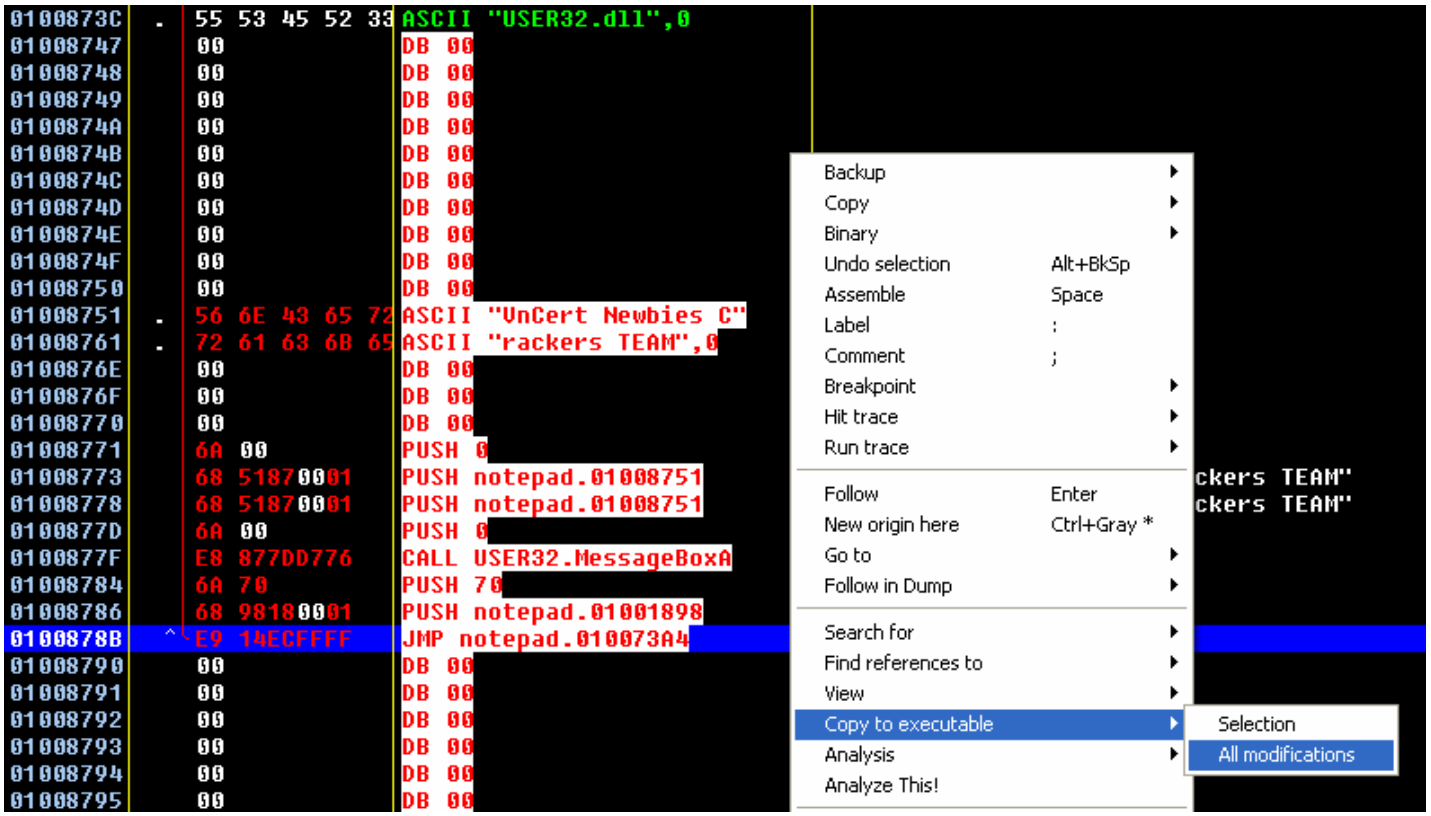
```
0100739D   E9 CF130000     JMP notepad.01008771
010073A2   90              NOP
010073A3   90              NOP
010073A4   .  E8 BF010000  CALL notepad.01007568
010073A9   .  33DB         XOR EBX,EBX
010073AB   .  53           PUSH EBX                          ; pModule => NULL
010073AC   .  8B3D CC100001 MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModuleHandleA>] ; kernel32.GetModuleHandleA
010073B2   .  FFD7         CALL EDI                          ; GetModuleHandleA
010073B4   .  66:8138 4D5A CMP WORD PTR DS:[EAX],5A4D
010073B9   .  75 1F        JNZ SHORT notepad.010073DA
010073BB   .  8B48 3C      MOV ECX,DWORD PTR DS:[EAX+3C]
010073BE   .  03C8         ADD ECX,EAX
```

Bạn phải nhớ kỹ địa chỉ **010073A4** ? Tại sao phải nhớ ? Vì ta phải trở lại vùng Code-Caves và cho nó nhảy tới địa chỉ này để Notepad được load lên.

– Nhảy tới đoạn Code-Caves, thêm code vào như sau :

```
01008750      00              DB 00
01008751   .  56 6E 43 65 72  ASCII "VnCert Newbies C"
01008761   .  72 61 63 6B 65  ASCII "rackers TEAM",0
0100876E      00              DB 00
0100876F      00              DB 00
01008770      00              DB 00
01008771      6A 00           PUSH 0
01008773      68 51870001     PUSH notepad.01008751             ASCII "VnCert Newbies Crackers TEAM"
01008778      68 51870001     PUSH notepad.01008751             ASCII "VnCert Newbies Crackers TEAM"
0100877D      6A 00           PUSH 0
0100877F      E8 877DD776     CALL USER32.MessageBoxA
01008784      6A 70           PUSH 70
01008786      68 98180001     PUSH notepad.01001898
0100878B   ^  E9 14ECFFFF     JMP notepad.010073A4
01008790      00              DB 00
```

– Save lại file EXE sau khi đã modify bằng cách click chuột phải chọn **Copy to executable → All modifications → Copy all**. Lưu lại với tên file là **notepad_modify.exe**.



– Chạy thử file **notepad_modify.exe** :

– Nhấn OK, notepad sẽ được load lên như bình thường.