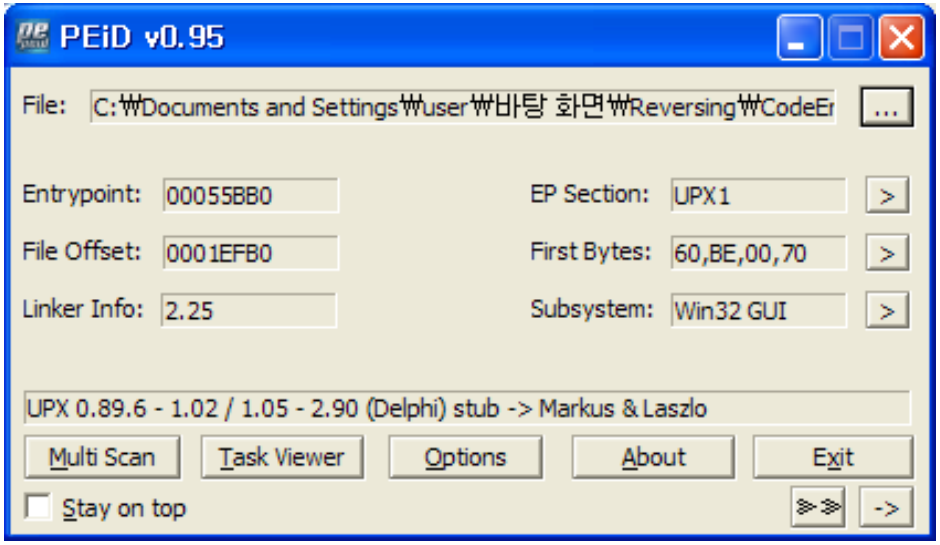
CODE ENGN level5

문제 풀이

OllyDbg 로 열게 되면 다

실행 압축이 되어있어 역어셈시 잘못된 결과를 초래할 수 도 있는 것인데,
계속 진행하기 위해서 예를 눌러줬습니다.



그리고 PEiD를 통해 확인을 해보니,
UPX 로 압축되어 있는것을 확인할수
있었습니다.

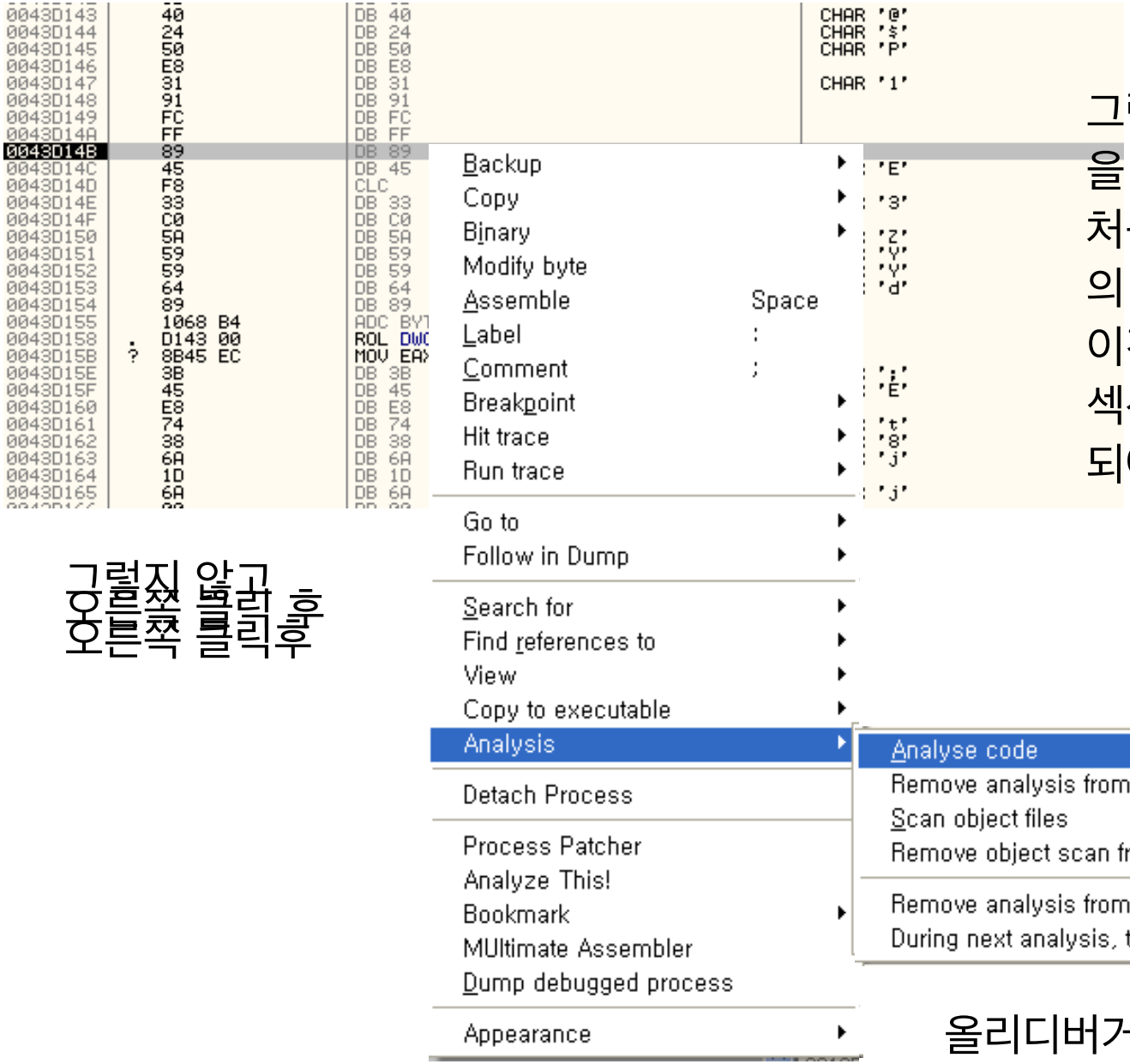
다음과 같은 코드가 뜨는 것 을 볼 수 있습니다.

보이는 것과 같이 Unregistered… 상태입니다.

이상태에서 Register now ! 버튼을 눌렀을때의 상황입니다. 잘못된 Serial 이라고 말해주네요.

그리고 이 메시지 박스역시
Back to user mode를 이용해서
리턴되는 순간을 포착하게되면
다음과 같다.

```
0043D143     40                DB 40                    CHAR '@'
0043D144     24                DB 24                    CHAR '$'
0043D145     50                DB 50                    CHAR 'P'
0043D146     00                DB 00
0043D147     31                DB 31                    CHAR '1'
0043D148     91                DB 91
0043D149     FC                DB FC
0043D14A     FF                DB FF
0043D14B     45                DB 45                    CHAR 'E'
0043D14C     EC                CLC
0043D14D     F8                DB 33                    CHAR '3'
0043D14E     33
0043D14F     C0                DB 59                    CHAR 'Z'
0043D150     59                DB 59                    CHAR 'Y'
0043D151     59                DB 59                    CHAR 'Y'
0043D152     59                DB 64                    CHAR 'd'
0043D153     64
0043D154     89                DB 89
0043D155     1068 B4           ADC BYTE PTR DS:[EAX-4C],CH
0043D158   . D143 00           ROL DWORD PTR DS:[EBX],1
0043D15B   ? 8B45 EC           MOV EAX,DWORD PTR SS:[EBP-14]
0043D15E     3B                DB 3B                    CHAR ';'
0043D15F     45                DB 45                    CHAR 'E'
0043D160     E8                DB E8
0043D161     74                DB 74                    CHAR 't'
0043D162     38                DB 38                    CHAR '8'
0043D163     6A                DB 6A                    CHAR 'j'
0043D164     1D                DB 1D
0043D165     6A                DB 6A                    CHAR 'j'
```



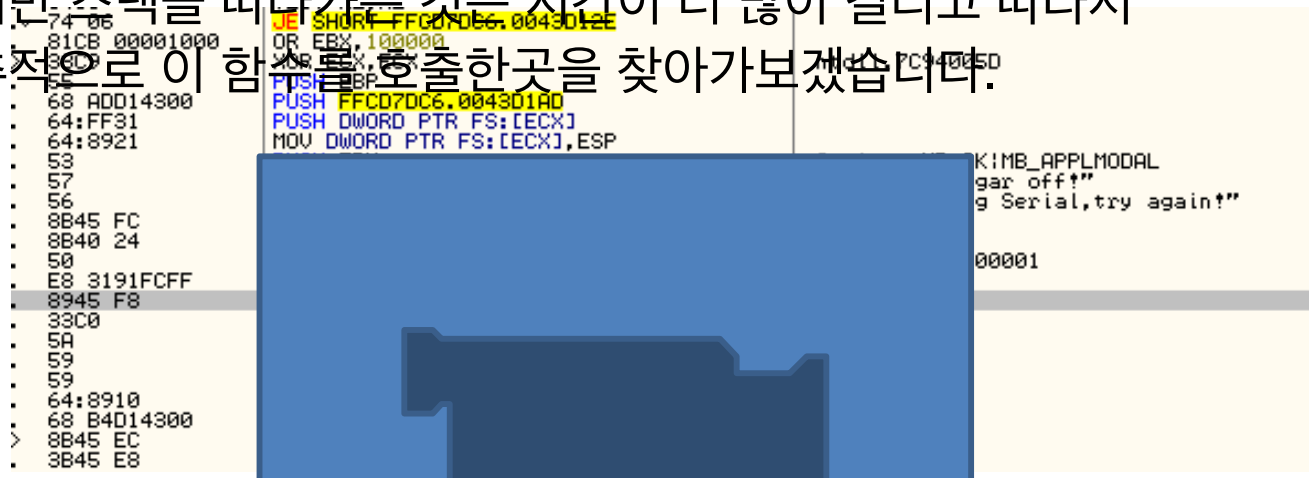
그럼 코드가 엉망인 것
을 볼 수 있는데 이것은
처음 실행했을 때의 경고
의 의미입니다.
이것은 현재 위치가 code
섹션이기 때문에 디스어셈이
되어있지 않은 것 입니다.

그럴지 않고
오른쪽 클릭후

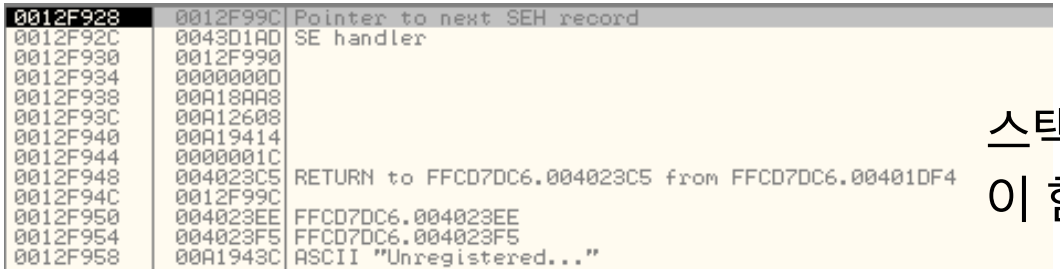
하거나

올리디버거 자체의 기능을 사용하면

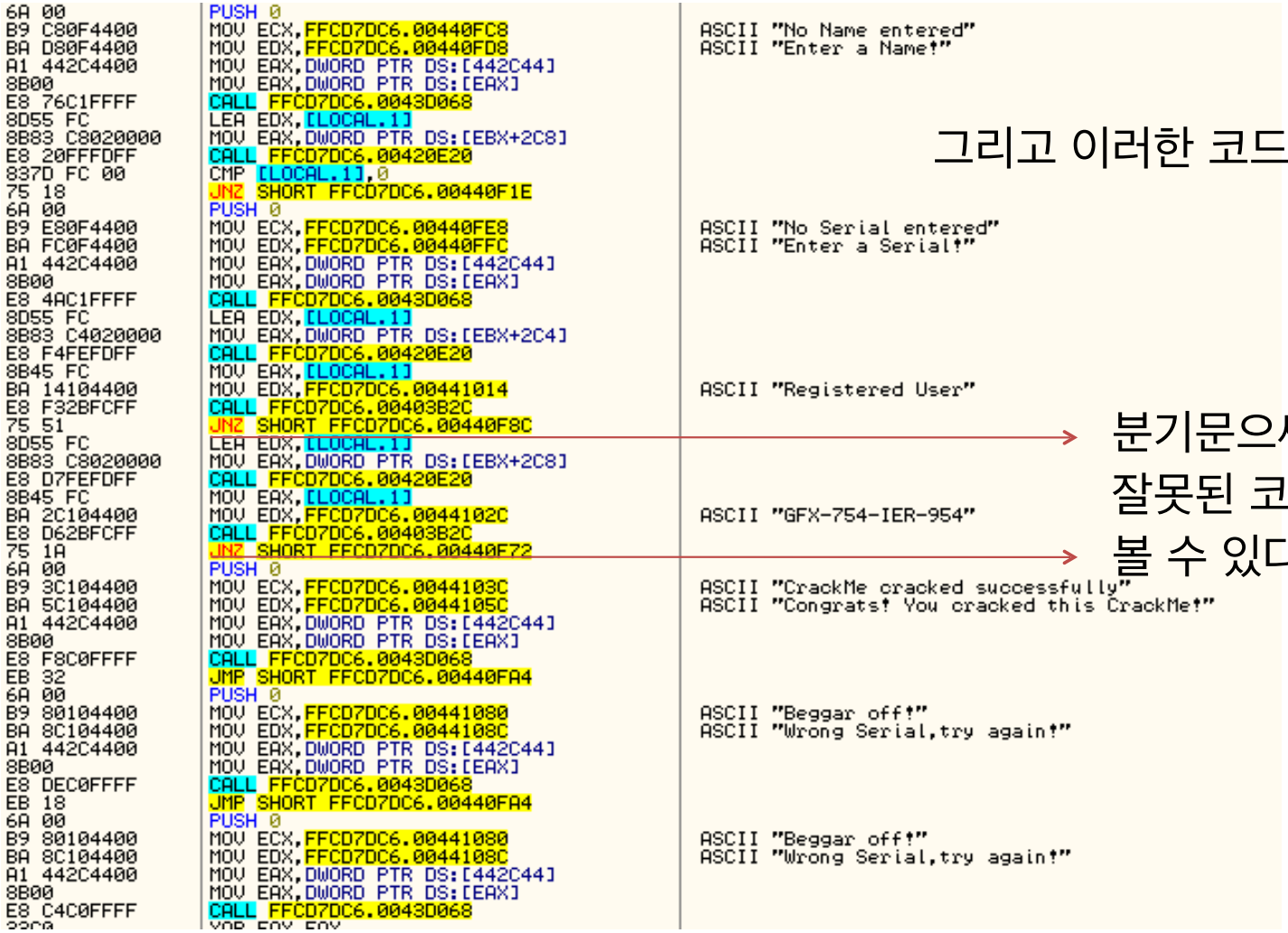
하지만 스택을 따라가는 것은 시간이 더 많이 걸리고 따라서
역추적으로 이 함수를 호출한곳을 찾아가보겠습니다.



이런
하지 서는 무조건
Wor 이된다.
따라서 이전 proc를 확인해봐야 합니다.



스택을 확인해보면
이 함수를 호출한 위치를 알 수 있습니다.



그리고 이러한 코드를 확인할 수 있습니다.

분기문으써 점프하면
잘못된 코드라는 MessageBox를
볼 수 있다.

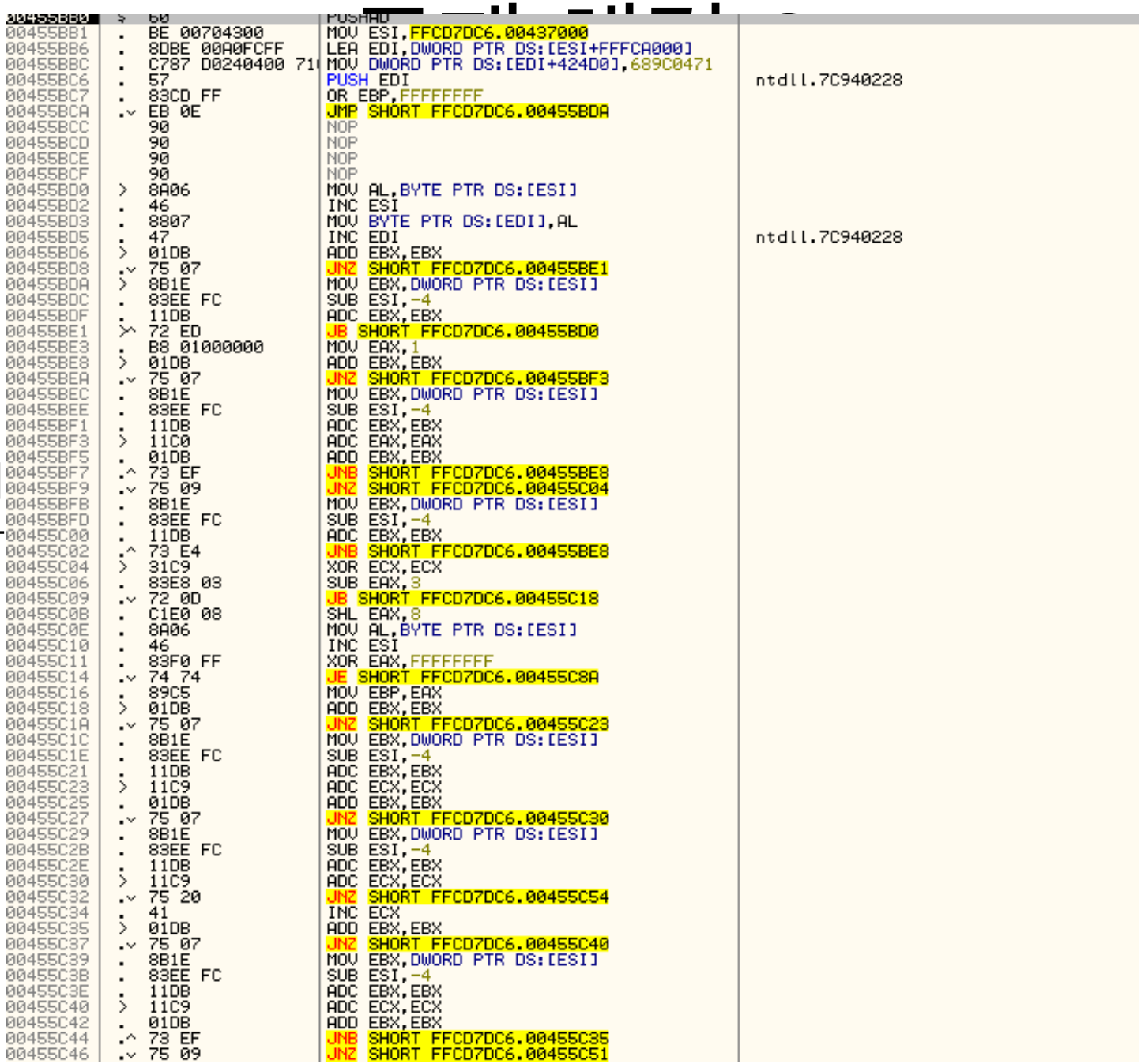
따라서 분기문을 만나기 전에 호출하는 함수가 문자열 비교함수임을
알 수 있고 그전에 넣어주는것인 이름과 시리얼 값임을 알 수 있습니다.

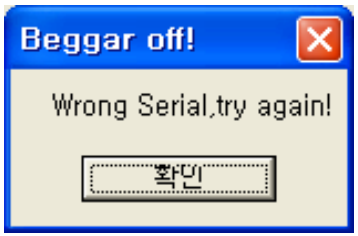
검증


Crackers For Freedom CrackMe v3.0
Official CFF CrackMe v3.0
Registered User
GFX-754-IER-954
Coder Acid Bytes [CFF]
Rel. Date 05/08/2000
Register now !
Quit the CrackMe
This is the official CFF CrackMe
If you can manage to crack it,
mail Name/Serial to:
acidbytes@gmx.net


CrackMe cracked successfully
Congrats! You cracked this CrackMe!
확인

앞서 따라


00455BB0 > 60 PUSHAD
00455BB1 . BE 00704300 MOV ESI,FFCD7DC6.00437000
00455BB6 . 8DBE 00A0FCFF LEA EDI,DWORD PTR DS:[ESI+FFFCA000]
00455BBC . C787 D0240400 71(MOV DWORD PTR DS:[EDI+424D0],689C0471
00455BC6 . 57 PUSH EDI
00455BC7 . 83CD FF OR EBP,FFFFFFFF
00455BCA .v EB 0E JMP SHORT FFCD7DC6.00455BDA
00455BCC 90 NOP
00455BCD 90 NOP
00455BCE 90 NOP
00455BCF 90 NOP
00455BD0 > 8A06 MOV AL,BYTE PTR DS:[ESI]
00455BD2 . 46 INC ESI
00455BD3 . 8807 MOV BYTE PTR DS:[EDI],AL
00455BD5 . 47 INC EDI
00455BD6 > 01DB ADD EBX,EBX
00455BD8 .v 75 07 JNZ SHORT FFCD7DC6.00455BE1
00455BDA > 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455BDC . 83EE FC SUB ESI,-4
00455BDF . 11DB ADC EBX,EBX
00455BE1 >^ 72 ED JB SHORT FFCD7DC6.00455BD0
00455BE3 . B8 01000000 MOV EAX,1
00455BE8 > 01DB ADD EBX,EBX
00455BEA .v 75 07 JNZ SHORT FFCD7DC6.00455BF3
00455BEC . 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455BEE . 83EE FC SUB ESI,-4
00455BF1 . 11DB ADC EBX,EBX
00455BF3 > 11C0 ADC EAX,EAX
00455BF5 . 01DB ADD EBX,EBX
00455BF7 .^ 73 EF JNB SHORT FFCD7DC6.00455BE8
00455BF9 .v 75 09 JNZ SHORT FFCD7DC6.00455C04
00455BFB . 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455BFD . 83EE FC SUB ESI,-4
00455C00 . 11DB ADC EBX,EBX
00455C02 .^ 73 E4 JNB SHORT FFCD7DC6.00455BE8
00455C04 > 31C9 XOR ECX,ECX
00455C06 . 83E8 03 SUB EAX,3
00455C09 .v 72 0D JB SHORT FFCD7DC6.00455C18
00455C0B . C1E0 08 SHL EAX,8
00455C0E . 8A06 MOV AL,BYTE PTR DS:[ESI]
00455C10 . 46 INC ESI
00455C11 . 83F0 FF XOR EAX,FFFFFFFF
00455C14 .v 74 74 JE SHORT FFCD7DC6.00455C8A
00455C16 . 89C5 MOV EBP,EAX
00455C18 > 01DB ADD EBX,EBX
00455C1A .v 75 07 JNZ SHORT FFCD7DC6.00455C23
00455C1C . 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455C1E . 83EE FC SUB ESI,-4
00455C21 . 11DB ADC EBX,EBX
00455C23 > 11C9 ADC ECX,ECX
00455C25 . 01DB ADD EBX,EBX
00455C27 .v 75 07 JNZ SHORT FFCD7DC6.00455C30
00455C29 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455C2B . 83EE FC SUB ESI,-4
00455C2E . 11DB ADC EBX,EBX
00455C30 > 11C9 ADC ECX,ECX
00455C32 .v 75 20 JNZ SHORT FFCD7DC6.00455C54
00455C34 . 41 INC ECX
00455C35 > 01DB ADD EBX,EBX
00455C37 .v 75 07 JNZ SHORT FFCD7DC6.00455C40
00455C39 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
00455C3B . 83EE FC SUB ESI,-4
00455C3E . 11DB ADC EBX,EBX
00455C40 > 11C9 ADC ECX,ECX
00455C42 . 01DB ADD EBX,EBX
00455C44 .^ 73 EF JNB SHORT FFCD7DC6.00455C35
00455C46 .v 75 09 JNZ SHORT FFCD7DC6.00455C51
ntdll.7C940228
ntdll.7C940228



이제 팩킹이 풀렸으므로 간단히 문자열을 검색해보게되면

```
00440E9C DD FFCD7DC6.00440CA8                ASCII "4wB"
00440EA7 ASCII "Unit1"
00440EDC MOV ECX,FFCD7DC6.00440FC8           ASCII "No Name entered"
00440EE1 MOV EDX,FFCD7DC6.00440FD8           ASCII "Enter a Name!"
00440F08 MOV ECX,FFCD7DC6.00440FE8           ASCII "No Serial entered"
00440F0D MOV EDX,FFCD7DC6.00440FFC           ASCII "Enter a Serial!"
00440F2F MOV EDX,FFCD7DC6.00441014           ASCII "Registered User"
00440F4C MOV EDX,FFCD7DC6.0044102C           ASCII "GFX-754-IER-954"
00440F5A MOV ECX,FFCD7DC6.0044103C           ASCII "CrackMe cracked successfully"
00440F5F MOV EDX,FFCD7DC6.0044105C           ASCII "Congrats! You cracked this CrackMe!"
00440F74 MOV ECX,FFCD7DC6.00441080           ASCII "Beggar off!"
00440F79 MOV EDX,FFCD7DC6.0044108C           ASCII "Wrong Serial,try again!"
00440F8E MOV ECX,FFCD7DC6.00441080           ASCII "Beggar off!"
00440F93 MOV EDX,FFCD7DC6.0044108C           ASCII "Wrong Serial,try again!"
00440FC8 ASCII "No Name entered",0
00440FD8 ASCII "Enter a Name!".0
```

이렇게 이름과 serial 키가 보이는것을 확인할 수 있습니다.