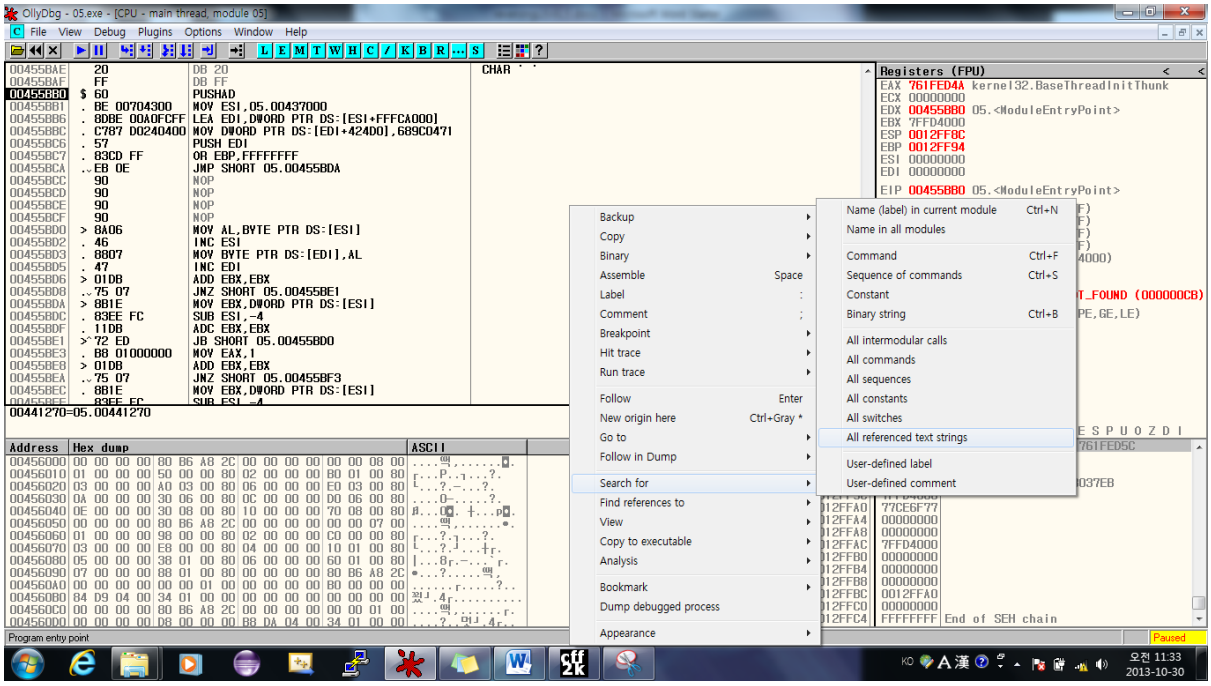
2013/10/30

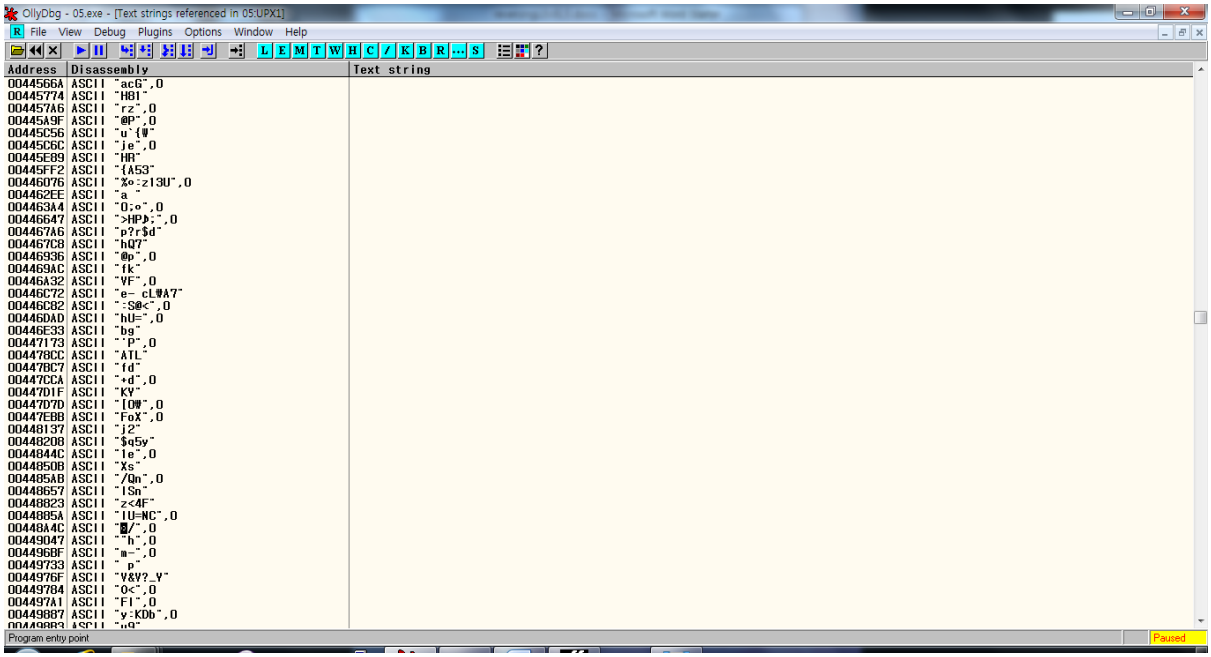
Basic level 5

시리얼 번호를 찾는 문제이다.

그러면 올리로 들어가서



Search for ->all referenced strings 로 찾아주면 되는데 한번 해보자



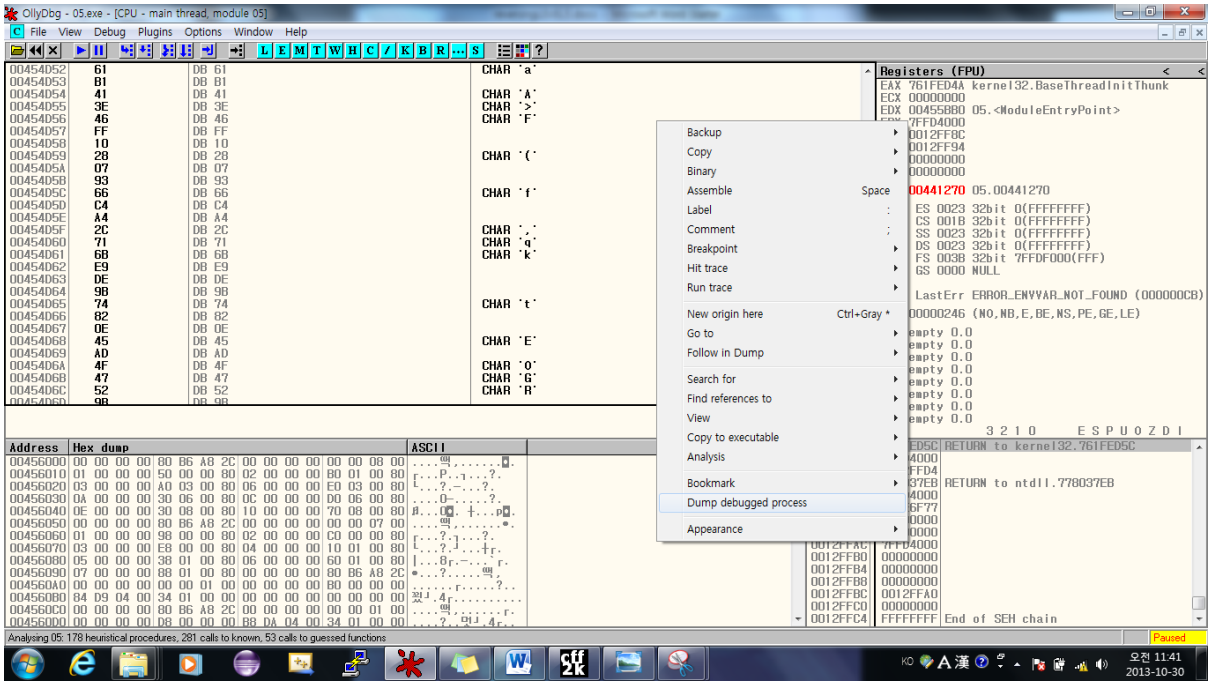
이상한 글자들 밖에 없다.... 왜그런가 봤더니 packing 되어있었다. 그럼 먼저 unpacking 해보자

```
00455BB0  $ 60              PUSHAD
00455BB1  . BE 00704300     MOV ESI,05.00437000
00455BB6  . 8DBE 00A0FCFF   LEA EDI,DWORD PTR DS:[ESI+FFFCA000]
00455BBC  . C787 D0240400   MOV DWORD PTR DS:[EDI+424D0],689C0471
00455BC6  . 57              PUSH EDI
00455BC7  . 83CD FF         OR EBP,FFFFFFFF
00455BCA  .v EB 0E          JMP SHORT 05.00455BDA
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 05.00455BE1
00455BDA  > 8B1E            MOV EBX,DWORD PTR DS:[ESI]
00455BDC  . 83EE FC         SUB ESI,-4
00455BDF  . 11DB            ADC EBX,EBX
00455BE1  >^72 ED           JB SHORT 05.00455BD0
```

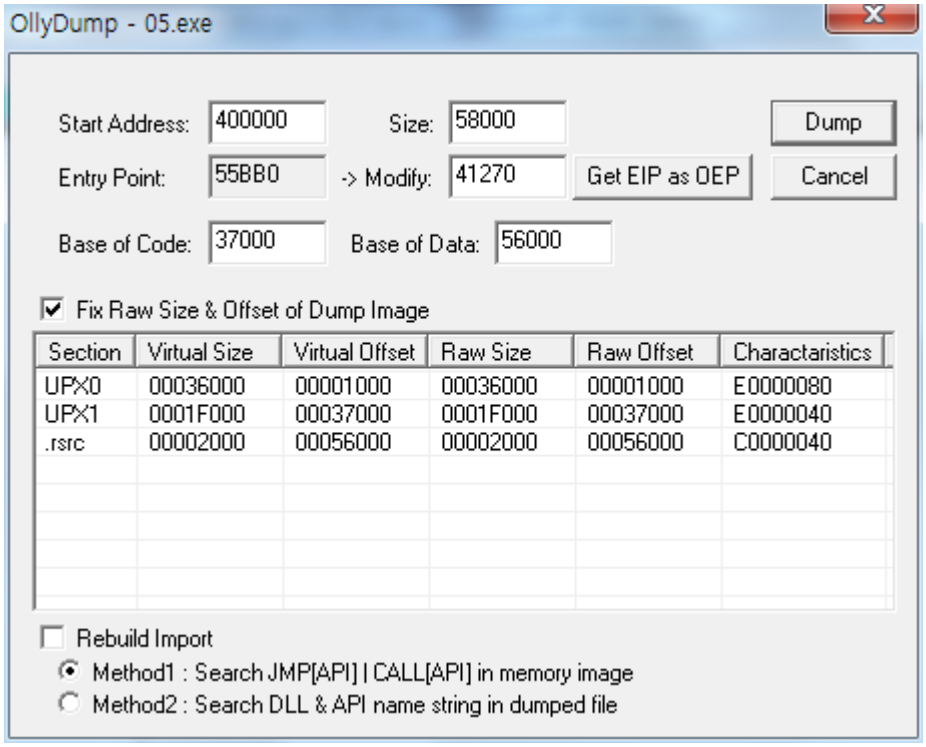
처음 들어가자마자 PUSHAD 라는 명령어가 있다. 그러면 이 실행파일은 packing 되어 있다는 말이다. 그러면 unpacking 을 해볼까?

```
00455CFB  . 83C3 04         ADD EBX,4
00455CFE  .^EB E1           JMP SHORT 05.00455CE1
00455D00  > FF96 04610500   CALL DWORD PTR DS:[ESI+56104]
00455D06  > 61              POPAD
00455D07  .^E9 64B5FEFF     JMP 05.00441270
00455D0C    245D4500        DD 05.00455D24
00455D10    345D4500        DD 05.00455D34
00455D14    D0344400        DD 05.004434D0
00455D18    00              DB 00
```

젤 밑에서 POPAD를 찾았다 그러면 그밑에 점프문은 unpacking 코드로 점프하는 것이다.

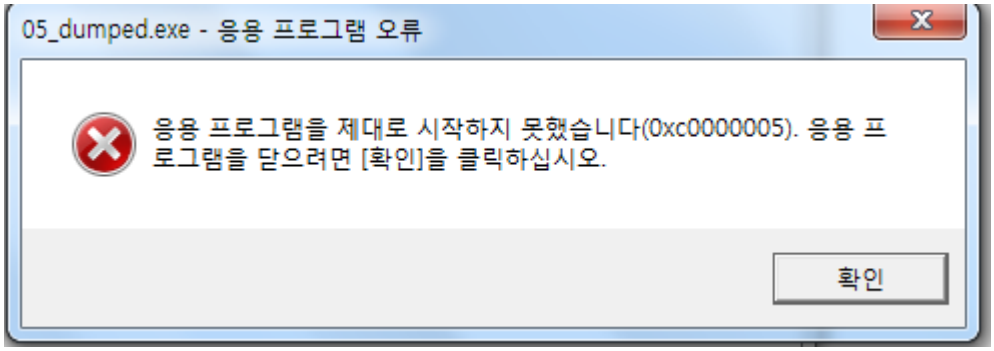


그러고 나서 dump debugged process로 덤프를 떠준다



그 다음 저장한다.(ex)05_dumped.exe

그리고 실행 하면



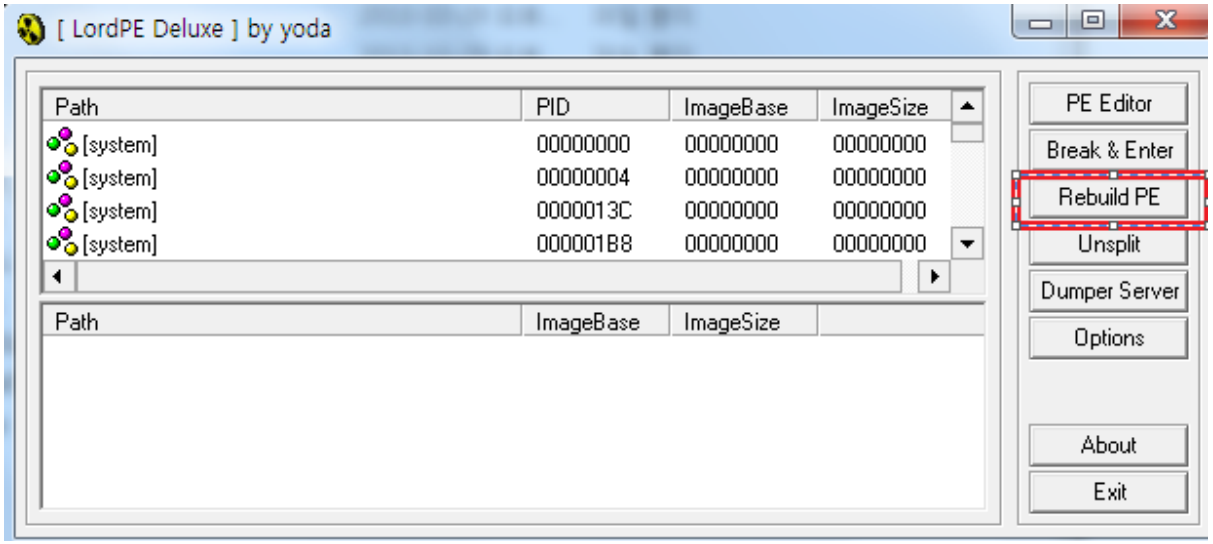
이런 경고문이 뜬다.

왜 뜨는 것일까?

이유)

해결방법)

lordPE라는 프로그램으로 PE를 rebuild 해준다.



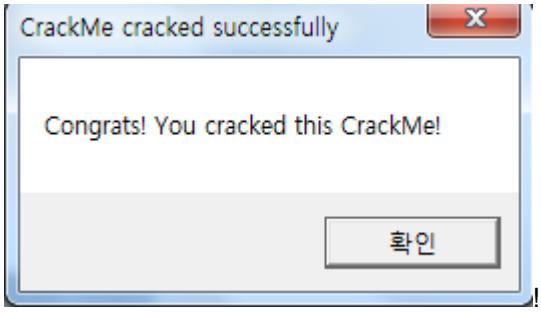
그런 다음 ollydbg로 05_dump.exe 를 실행시키면 완벽히 unpacking 되었다는 것을 알수 있다.

따라서 search for -> all referenced strings

```
00440E96 ASCII "TForm1"
00440E9C DD 05_dumpe.00440CA8                ASCII "4wB"
00440EA7 ASCII "Unit1"
00440EDC MOV ECX,05_dumpe.00440FC8           ASCII "No Name entered"
00440EE1 MOV EDX,05_dumpe.00440FD8           ASCII "Enter a Name!"
00440F08 MOV ECX,05_dumpe.00440FE8           ASCII "No Serial entered"
00440F0D MOV EDX,05_dumpe.00440FFC           ASCII "Enter a Serial!"
00440F2F MOV EDX,05_dumpe.00441014           ASCII "Registered User"
00440F4C MOV EDX,05_dumpe.0044102C           ASCII "GFX-754-IER-954"
00440F5A MOV ECX,05_dumpe.0044103C           ASCII "CrackMe cracked successfully"
00440F5F MOV EDX,05_dumpe.0044105C           ASCII "Congrats! You cracked this CrackMe!"
00440F74 MOV ECX,05_dumpe.00441080           ASCII "Beggar off!"
00440F79 MOV EDX,05_dumpe.0044108C           ASCII "Wrong Serial,try again!"
00440F8E MOV ECX,05_dumpe.00441080           ASCII "Beggar off!"
00440F93 MOV EDX,05_dumpe.0044108C           ASCII "Wrong Serial,try again!"
00440FC8 ASCII "No Name entered",0
00440FD8 ASCII "Enter a Name!",0
00440FE8 ASCII "No Serial entere"
00440FF8 ASCII "d",0
00440FFC ASCII "Enter a Serial!",0
```

여기에 시리얼 같은 문자가 나와있다.

입력하면 성공



!!!!!!