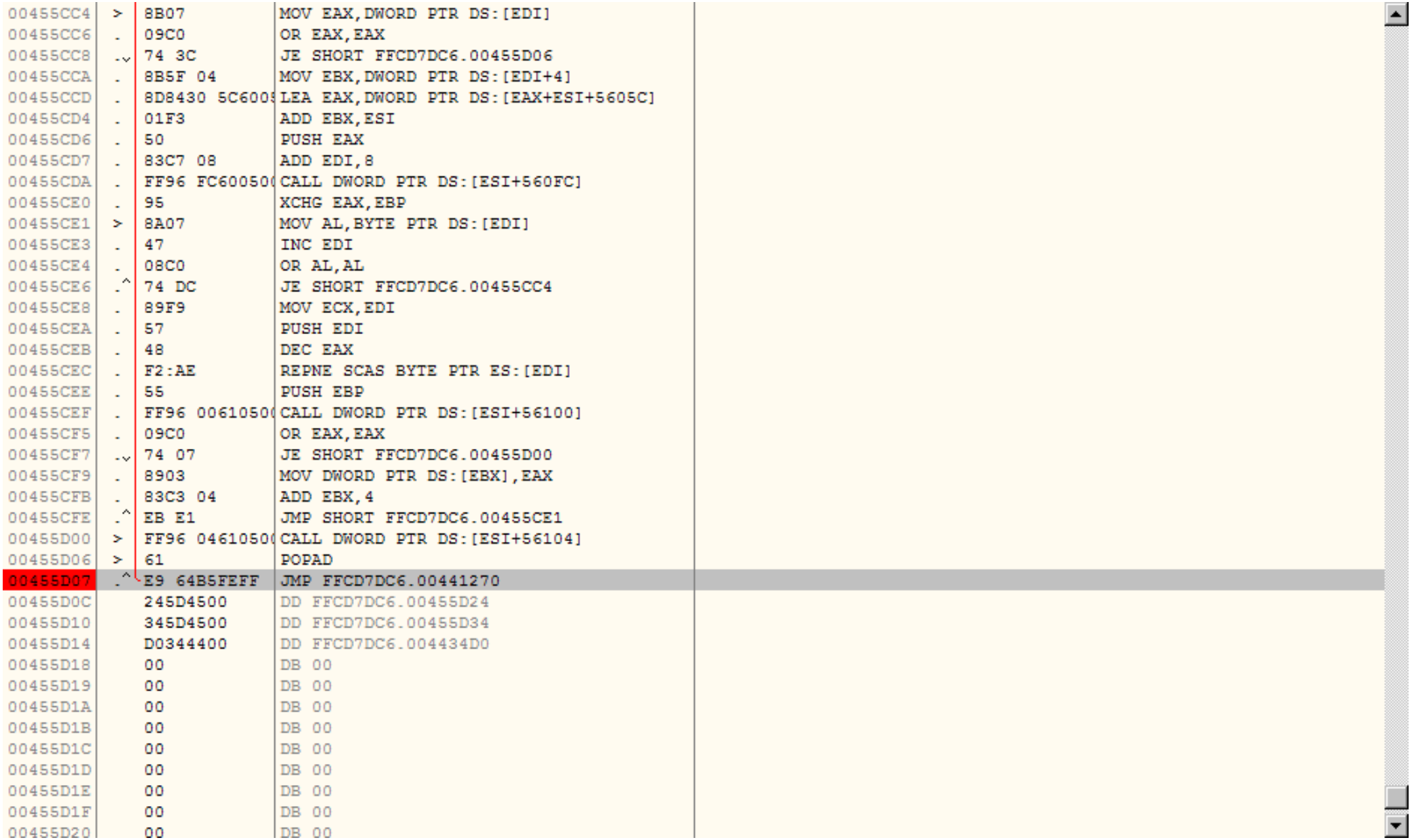
Reverseing No0

model9c@gmail.com

ID : bluetail

```
00455BB0  $  60           PUSHAD
00455BB1  .  BE 00704300  MOV ESI,FFCD7DC6.00437000
00455BB6  .  8DBE 00A0FCF LEA EDI,DWORD PTR DS:[ESI+FFFCA000]
00455BBC  .  C787 D024040 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]
```

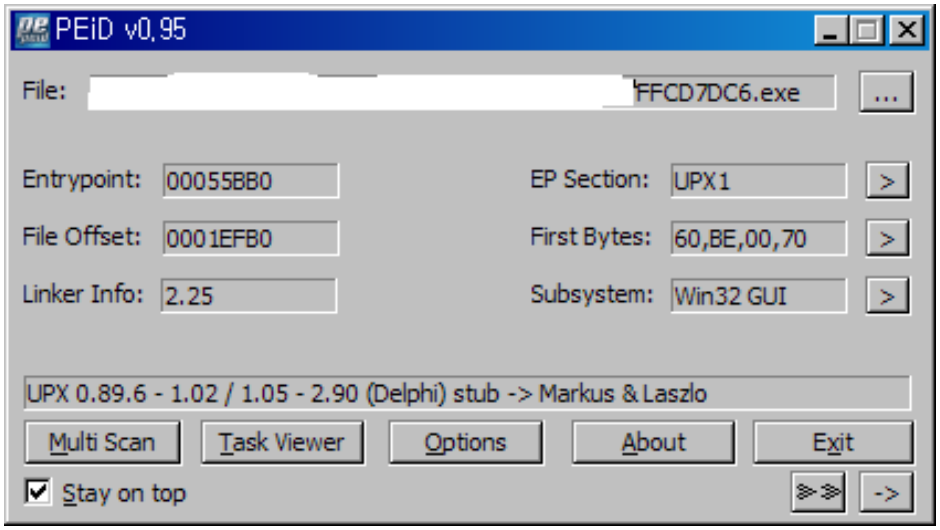
덩그러니.....아무것도 없었다.



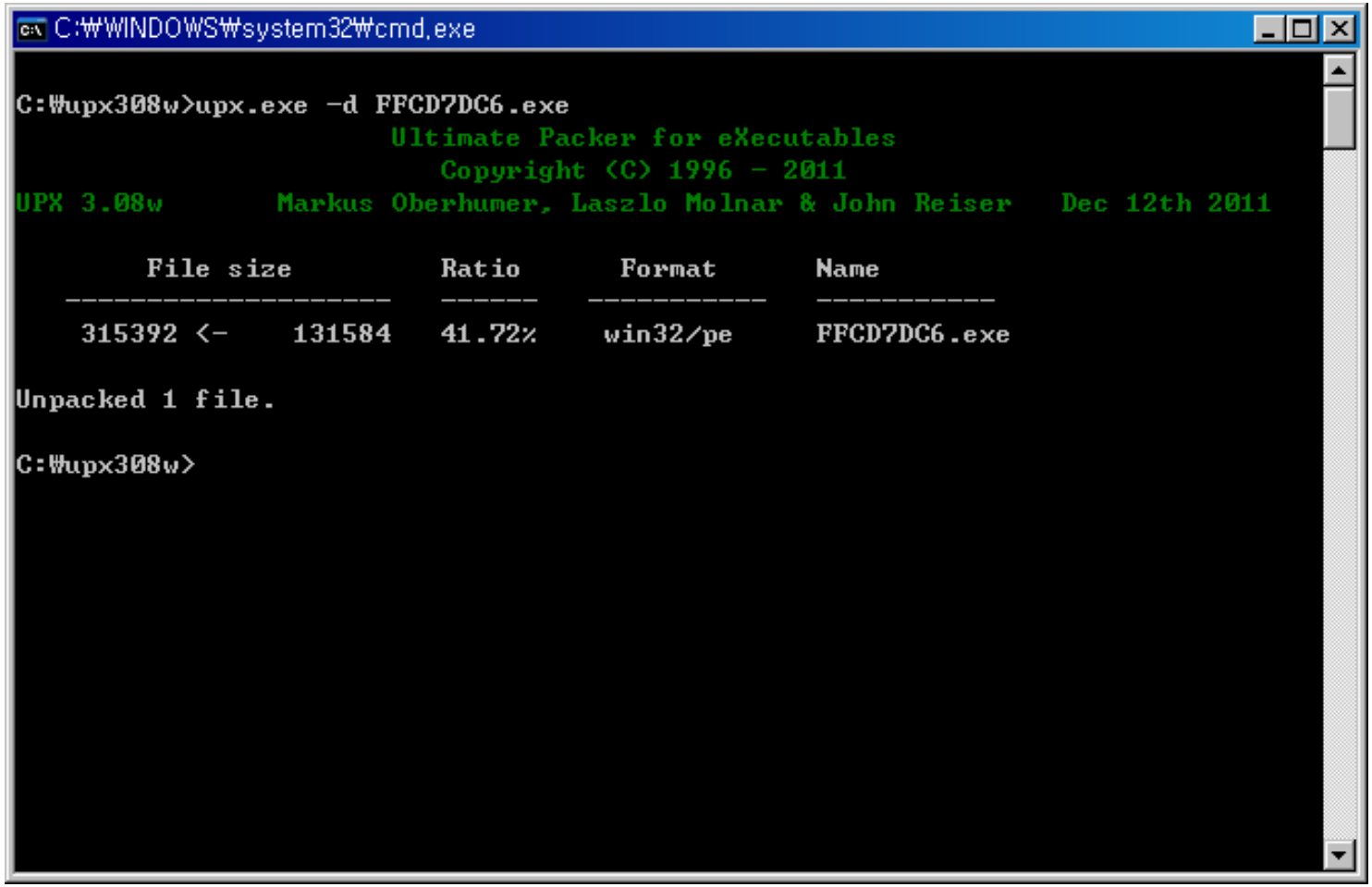
밑으로 쭉 내려보니 JMP문이 있어 break point를 걸고 f9로 실행 후 f8로 진행을 해보았다.

```
00441270  >  55           PUSH EBP
00441271  .  8BEC         MOV EBP,ESP
00441273  ?  83C4 F4      ADD ESP,-0C
00441276  .  B8 60114400  MOV EAX,FFCD7DC6.00441160
0044127B  .  E8 E848FCFF  CALL FFCD7DC6.00405B68
00441280  ?  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441285  ?  8B00         MOV EAX,DWORD PTR DS:[EAX]
00441287  ?  E8 ECBBFFFF  CALL FFCD7DC6.0043CE78
0044128C  ?  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441291  ?  8B00         MOV EAX,DWORD PTR DS:[EAX]
00441293  .  BA D0124400  MOV EDX,FFCD7DC6.004412D0          ASCII "Crackers For Freedom CrackMe v3.0"
00441298  .  E8 17B8FFFF  CALL FFCD7DC6.0043CAB4
0044129D  ?  8B0D 102D440(MOV ECX,DWORD PTR DS:[442D10]     FFCD7DC6.00443830
004412A3  ?  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
004412A8  ?  8B00         MOV EAX,DWORD PTR DS:[EAX]
004412AA  ?  8B15 5C0C440(MOV EDX,DWORD PTR DS:[440C5C]     FFCD7DC6.00440CA8
004412B0  .  E8 DBBBFFFF  CALL FFCD7DC6.0043CE90
004412B5  .  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
004412BA  ?  8B00         MOV EAX,DWORD PTR DS:[EAX]
004412BC     E8           DB E8
004412BD     4F           DB 4F                            CHAR 'O'
004412BE     BC           DB BC
004412BF     FF           DB FF
004412C0  >  FFE8         JMP FAR EAX                      Illegal use of register
004412C2  ?  AA           STOS BYTE PTR ES:[EDI]
004412C3  .  23FC         AND EDI,ESP
004412C5  ?  FF00         INC DWORD PTR DS:[EAX]
004412C7     00           DB 00
004412C8     FF           DB FF
004412C9     FF           DB FF
004412CA     FF           DB FF
004412CB     FF           DB FF
004412CC     21           DB 21                            CHAR '!'
004412CD     00           DB 00
004412CE     00           DB 00
004412CF     00           DB 00
004412D0     43           DB 43                            CHAR 'C'
004412D1     72           DB 72                            CHAR 'r'
004412D2     61           DB 61                            CHAR 'a'
004412D3     63           DB 63                            CHAR 'c'
```

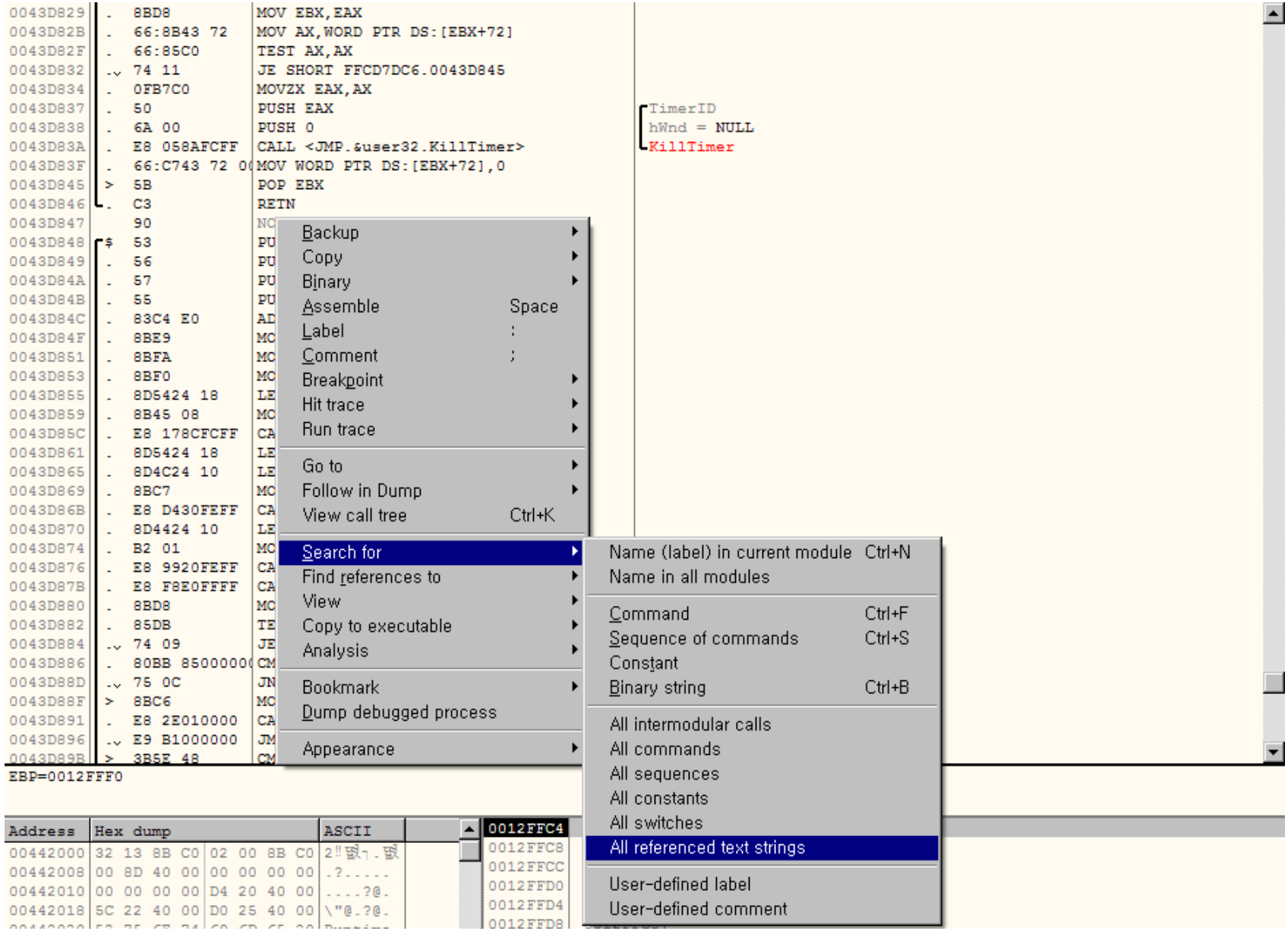
여기부터가 진짜 코드인 듯 하다.
문제는 패킹...



PEID로 확인결과 UPX로 패킹되어있는 것을 확인할 수 있었다.



UPX 프로그램으로 언패킹 실행



모든 문자열 검색으로 문자열들을 검색해 보았다.

```
DD FFCD7DC6.00440CA8                ASCII "4wB"
ASCII "Unit1"
MOV ECX,FFCD7DC6.00440FC8           ASCII "No Name entered"
MOV EDX,FFCD7DC6.00440FD8           ASCII "Enter a Name!"
MOV ECX,FFCD7DC6.00440FE8           ASCII "No Serial entered"
MOV EDX,FFCD7DC6.00440FFC           ASCII "Enter a Serial!"
MOV EDX,FFCD7DC6.00441014           ASCII "Registered User"
MOV EDX,FFCD7DC6.0044102C           ASCII "GFX-754-IER-954"
MOV ECX,FFCD7DC6.0044103C           ASCII "CrackMe cracked successfully"
MOV EDX,FFCD7DC6.0044105C           ASCII "Congrats! You cracked this CrackMe!"
MOV ECX,FFCD7DC6.00441080           ASCII "Beggar off!"
MOV EDX,FFCD7DC6.0044108C           ASCII "Wrong Serial,try again!"
MOV ECX,FFCD7DC6.00441080           ASCII "Beggar off!"
MOV EDX,FFCD7DC6.0044108C           ASCII "Wrong Serial,try again!"
```

문자열 검색으로 유저와 serial을 확인할 수 있었다.