Reverse L05

Date : 2011 / 01 / 02
PRIDE

#문제

Korea :
이 프로그램의 등록키는 무엇인가

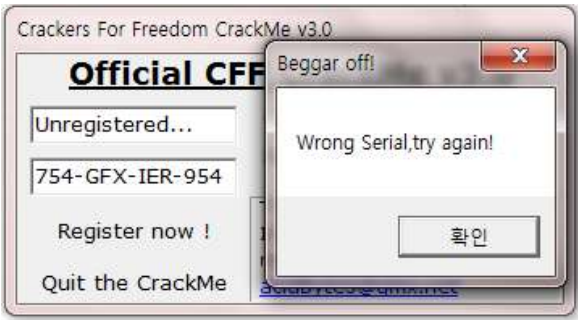
English :
The registration key of this program is?

#문제프로그램

#프로그램실행

프로그램을 실행했다.

가입되지 않았다는 문자열과 시리얼키 같은 값이 입력 폼에 들어가 있다.
Register now!버튼을 클릭한다.

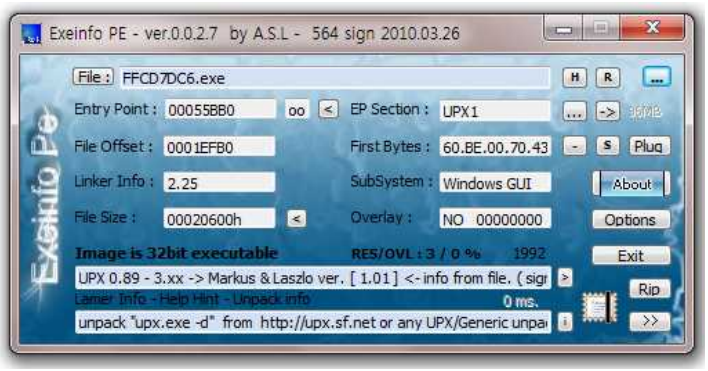


잘못된 시리얼키라는 메시지박스가 나타난다.

Quit the CrackMe버튼을 클릭하면 종료된다.

#With exeinfope

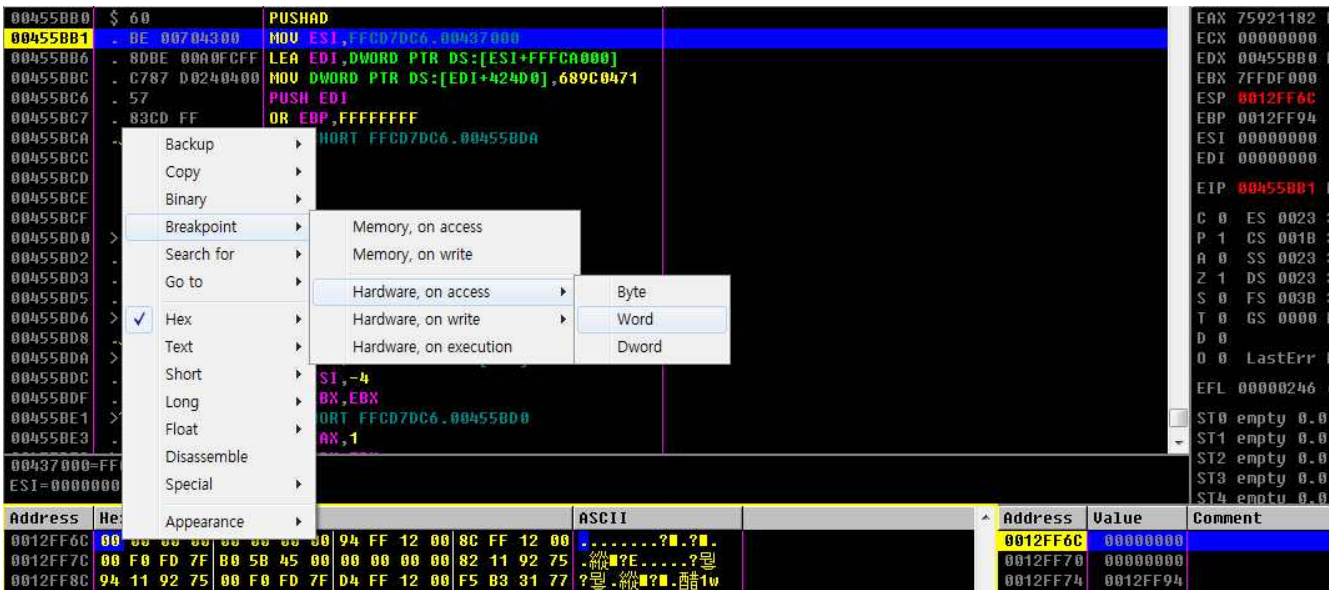
exeinfope로 열었다.



UPX로 패킹되어있다.
언패커를 다운받아 언패킹하면 간단하지만, 손으로 Ollydbg를 이용해 직접 언패킹했다.

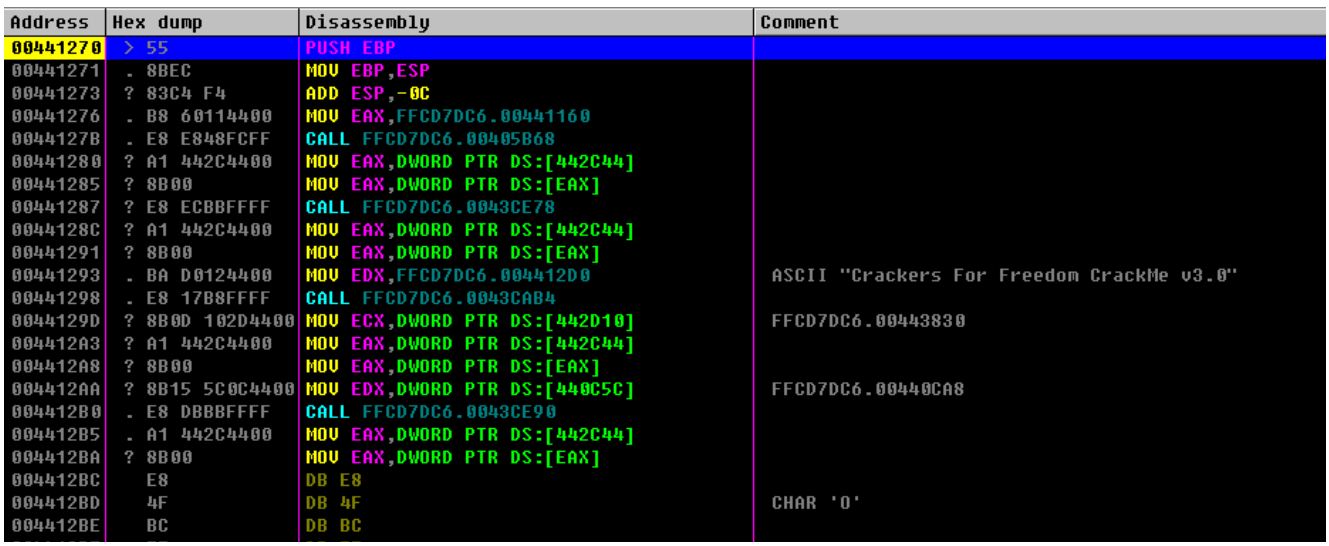
#Unpack

Ollydbg로 열게되면 pushad로 모든레지스터를 push하는 곳이 보인다.
pushad가 있으므로 popad하는 곳도 있다.
popad하는 곳 주변에서 oep를 찾을 수 있다.
같은 esp에서 popad를 찾기위해, pushad를 진행한 직후에 esp가 가르키는곳에 하드웨어 브레이크포인트를 걸었다.

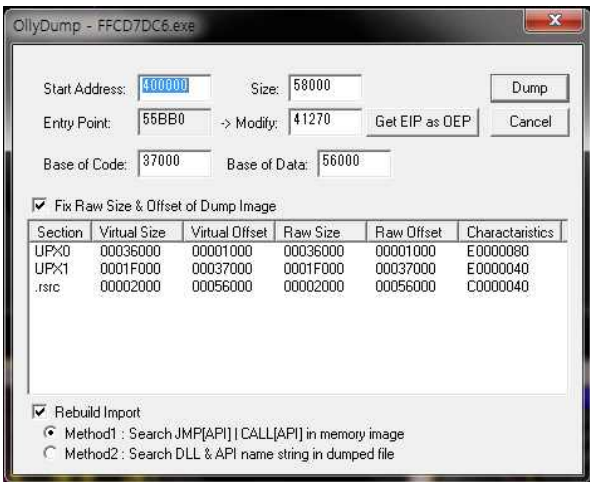


이후, F9로 진행시킨다.

POPAD이후, 분기하는 곳에 브레이크포인트가 걸렸다.
이제 F8로 분기해본다.



원본코드가있다. 플러그인의 OllyDump 기능을 이용해 덤프를 떠서 저장한다.

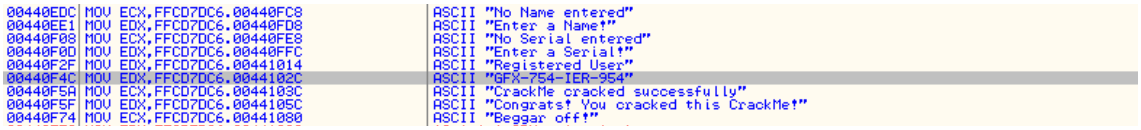


저장

문제 없이 작동되며, 올리디버거로도 문제없이 열린다.

#With Ollydbg

Searchfor - All referenced text strings로 프로그램내의 문자열을 보았다.
문자열 중에 시리얼키로 보이는 문자열과 성공/실패했을때등의 문자열들도 보였다.



시리얼키로 보이는 "GFX-754-IER-954"를 참조하는 지점으로 가보았다.

```
Address   Hex dump     Disassembly                          Comment
00440ED4  . 837D FC 00 CMP DWORD PTR SS:[EBP-4],0
00440ED8  .v75 18      JNZ SHORT FFCD7DC6.00440EF2
00440EDA  . 6A 00      PUSH 0
00440EDC  . B9 C80F4400 MOV ECX,FFCD7DC6.00440FC8           ASCII "No Name entered"
00440EE1  . BA D80F4400 MOV EDX,FFCD7DC6.00440FD8           ASCII "Enter a Name!"
00440EE6  . A1 442C4400 MOV EAX,DWORD PTR DS:[442C44]
00440EEB  . 8B00       MOV EAX,DWORD PTR DS:[EAX]
00440EED  . E8 76C1FFFF CALL FFCD7DC6.0043D068
00440EF2  > 8D55 FC    LEA EDX,DWORD PTR SS:[EBP-4]
00440EF5  . 8B83 C8020000 MOV EAX,DWORD PTR DS:[EBX+2C8]
00440EFB  . E8 20FFFDFF CALL FFCD7DC6.00420E20
00440F00  . 837D FC 00 CMP DWORD PTR SS:[EBP-4],0
00440F04  .v75 18      JNZ SHORT FFCD7DC6.00440F1E
00440F06  . 6A 00      PUSH 0
00440F08  . B9 E80F4400 MOV ECX,FFCD7DC6.00440FE8           ASCII "No Serial entered"
00440F0D  . BA FC0F4400 MOV EDX,FFCD7DC6.00440FFC           ASCII "Enter a Serial!"
00440F12  . A1 442C4400 MOV EAX,DWORD PTR DS:[442C44]
00440F17  . 8B00       MOV EAX,DWORD PTR DS:[EAX]
00440F19  . E8 4AC1FFFF CALL FFCD7DC6.0043D068
00440F1E  > 8D55 FC    LEA EDX,DWORD PTR SS:[EBP-4]
00440F21  . 8B83 C4020000 MOV EAX,DWORD PTR DS:[EBX+2C4]
00440F27  . E8 F4FEFDFF CALL FFCD7DC6.00420E20
00440F2C  . 8B45 FC    MOV EAX,DWORD PTR SS:[EBP-4]
00440F2F  . BA 14104400 MOV EDX,FFCD7DC6.00441014           ASCII "Registered User"
00440F34  . E8 F32BFCFF CALL FFCD7DC6.00403B2C
00440F39  .v75 51      JNZ SHORT FFCD7DC6.00440F8C
00440F3B  . 8D55 FC    LEA EDX,DWORD PTR SS:[EBP-4]
00440F3E  . 8B83 C8020000 MOV EAX,DWORD PTR DS:[EBX+2C8]
00440F44  . E8 D7FEFDFF CALL FFCD7DC6.00420E20
00440F49  . 8B45 FC    MOV EAX,DWORD PTR SS:[EBP-4]
00440F4C  . BA 2C104400 MOV EDX,FFCD7DC6.0044102C           ASCII "GFX-754-IER-954"
00440F51  . E8 D62BFCFF CALL FFCD7DC6.00403B2C
00440F56  .v75 1A      JNZ SHORT FFCD7DC6.00440F72
00440F58  . 6A 00      PUSH 0
00440F5A  . B9 3C104400 MOV ECX,FFCD7DC6.0044103C           ASCII "CrackMe cracked successfully"
00440F5F  . BA 5C104400 MOV EDX,FFCD7DC6.0044105C           ASCII "Congrats! You cracked this CrackMe!"
00440F64  . A1 442C4400 MOV EAX,DWORD PTR DS:[442C44]
00440F69  . 8B00       MOV EAX,DWORD PTR DS:[EAX]
00440F6B  . E8 F8C0FFFF CALL FFCD7DC6.0043D068
```

주변에서도 시리얼키 인증에 관련된 많은 스트링을 참조하였다.
특히 밑부분에는 크랙을 성공했다는 메시지박스를 나타내는 루틴이 있었다.
그위에는 "Registered User"과 "GFX-754-IER-954"를 00403B2C함수에서 사용하는 부분이있다. 함수호출후에는 JNZ로 분기하는 부분이있다.
이를 통해 00403B2C함수가 문자열비교함수라는 것을 짐작할 수 있었다.

00440F2C에 브레이크포인트를 걸고 Name폼에 임의의 문자열을 넣었을때와 "Registered User"을 넣었을 때를 비교한다.

#Name에 임의의 문자열을 넣었다.

```
00440F2C  . 8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
00440F2F  . BA 14104400   MOV EDX,FFCD7DC6.00441014      ASCII "Registered User
00440F34  . E8 F32BFCFF   CALL FFCD7DC6.00403B2C
00440F39  .v75 51         JNZ SHORT FFCD7DC6.00440F8C
00440F3B  . 8D55 FC       LEA EDX,DWORD PTR SS:[EBP-4]
00440F3E  . 8B83 C8020000 MOV EAX,DWORD PTR DS:[EBX+2C8]
00440F44  . E8 D7FEFDFF   CALL FFCD7DC6.00420E20
00440F49  . 8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
00440F4C  . BA 2C104400   MOV EDX,FFCD7DC6.0044102C      ASCII "GFX-754-IER-95
00440F51  . E8 D62BFCFF   CALL FFCD7DC6.00403B2C
00440F56  .v75 1A         JNZ SHORT FFCD7DC6.00440F72
00440F58  . 6A 00         PUSH 0
00440F5A  . B9 3C104400   MOV ECX,FFCD7DC6.0044103C      ASCII "CrackMe cracke
00440F5F  . BA 5C104400   MOV EDX,FFCD7DC6.0044105C      ASCII "Congrats! You
00440F64  . A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
00440F69  . 8B00          MOV EAX,DWORD PTR DS:[EAX]
00440F6B  . E8 F8C0FFFF   CALL FFCD7DC6.0043D068
Jump is taken
00440F8C=FFCD7DC6.00440F8C
```

JNZ에서 분기한다.
분기한곳은 시리얼키가 틀렸다는 메시지박스를 나타내는 곳이다.

#Name에 "Registered User"을 넣었을때

```
00440F2C  . 8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
00440F2F  . BA 14104400   MOV EDX,FFCD7DC6.00441014      ASCII "Registered Use
00440F34  . E8 F32BFCFF   CALL FFCD7DC6.00403B2C
00440F39  .v75 51         JNZ SHORT FFCD7DC6.00440F8C
00440F3B  . 8D55 FC       LEA EDX,DWORD PTR SS:[EBP-4]
00440F3E  . 8B83 C8020000 MOV EAX,DWORD PTR DS:[EBX+2C8]
00440F44  . E8 D7FEFDFF   CALL FFCD7DC6.00420E20
00440F49  . 8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
00440F4C  . BA 2C104400   MOV EDX,FFCD7DC6.0044102C      ASCII "GFX-754-IER-95
00440F51  . E8 D62BFCFF   CALL FFCD7DC6.00403B2C
00440F56  .v75 1A         JNZ SHORT FFCD7DC6.00440F72
00440F58  . 6A 00         PUSH 0
00440F5A  . B9 3C104400   MOV ECX,FFCD7DC6.0044103C      ASCII "CrackMe cracke
00440F5F  . BA 5C104400   MOV EDX,FFCD7DC6.0044105C      ASCII "Congrats! You
00440F64  . A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
00440F69  . 8B00          MOV EAX,DWORD PTR DS:[EAX]
00440F6B  . E8 F8C0FFFF   CALL FFCD7DC6.0043D068
Jump is NOT taken
00440F8C=FFCD7DC6.00440F8C
```

JNZ에서 분기하지 않았다.
이로서 00403B2C가 문자열 비교함수라는 것을 확실히 알 수 있었다.
다음에는 "GFX-754-IER-954"를 문자열 비교함수에 사용한다.
그러므로 "Registered User"과 "GFX-754-IER-954"를 입력폼에 각각 넣어주면 크랙에 성공했다는 메시지박스를 볼 수 있다.

#답 : GFX-754-IER-954