Basic RCE L05

Korea :

이 프로그램의 등록키는 무엇인가

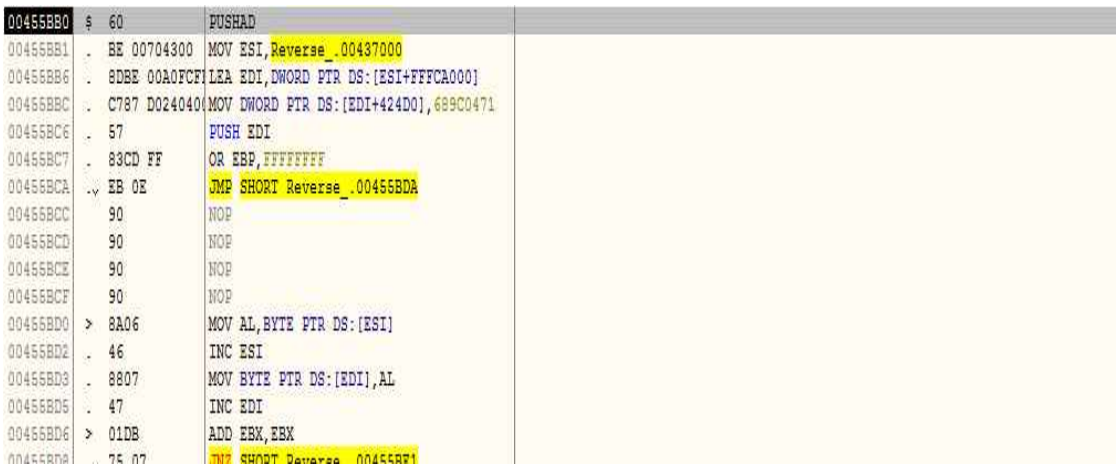
English :

The registration key of this program is?

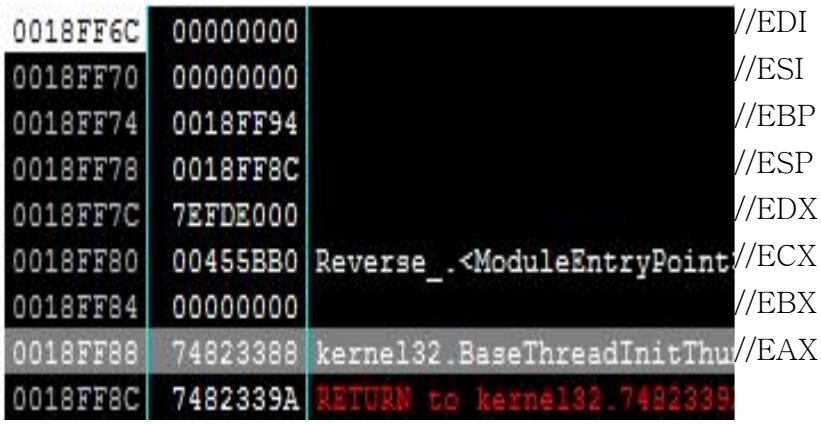
프로그램을 실행시켜보자.

실행시키니 이런 창이 하나 뜬다. 언뜻 봐도 ID같은 것과 시리얼키를 입력 받고 등록하는 프로그램인 것 같다. 한번 아무값이나 넣고 Register now!를 눌러보자.

Wrong Serial,try again! 이라는 메시지를 띄운다.
이젠 올리디버거로 열어보자.

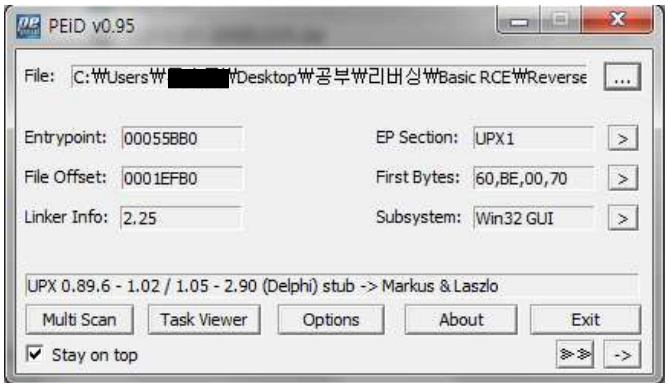


첫 코드가 PUSHAD 이다. 이 명령어는 Stack 창에 EAX~EDI 레지스터 값들을 넣는 명령어이다. 이 명령을 실행하고 스택창을 보면



이건 패킹되었음을 의미하는 코드이다.
패킹이란 파일을 압축하는 것을 의미하는데, 패킹된 프로그램은 올리디버거로 열었을 때 코드가 알아보기 힘들게 되어있기 때문에 분석이 힘들다. [Search for] 메뉴로 별짓을 해봐도 얻는건 거의 없을 것이다. 그럼 우리는 이 프로그램을 언패킹을 해줘야 한다. (Unpacking <-> Packing)
일단 언패킹을 하는 방법에는 두가지 방법이 있다.

일단은 프로그램에 대해 알아보기위해 PEID로 파일을 열어보자.



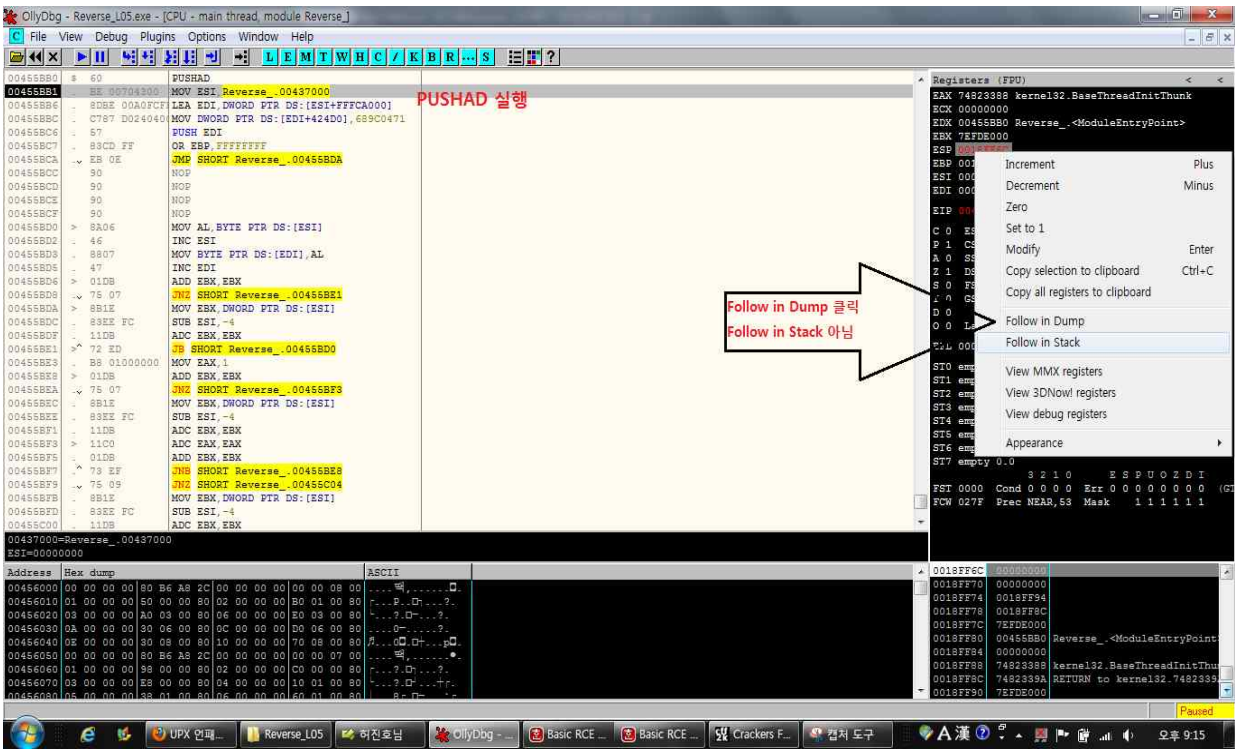
나와있듯이 UPX라는 프로그램으로 패킹되었다는 것을 알 수 있다.

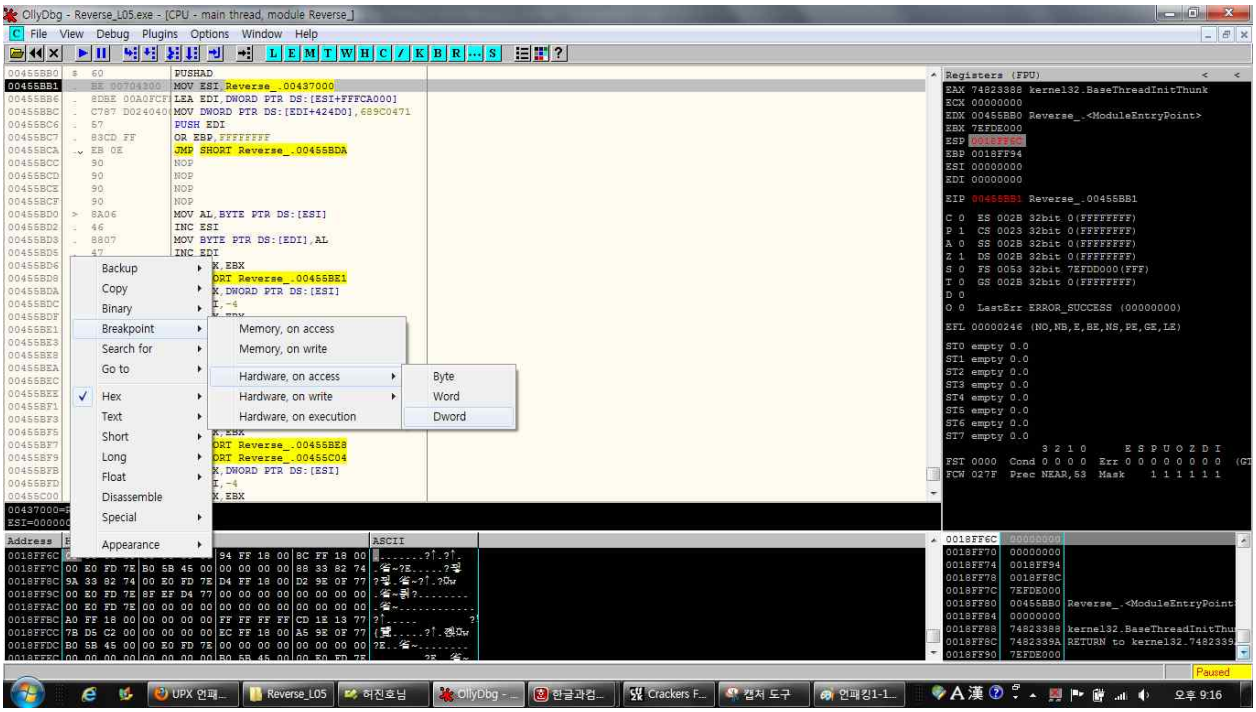
첫 번째는 꽤 걸리지만 언패킹프로그램이 없어도 할 수 있는 방법이고,
두 번째는 언패킹 프로그램으로 바로 할 수 있는 방법이다.

일단 첫 번째부터 해보도록 하자.
처음 명령어인 PUSHAD를 F8로 실행하고 ESP레지스터에 커서를 놓고 오른쪽키를 눌러서 [Follow in Dump]를 누른다.

그러면 Hex창에 첫 번째 바이트에 커서를 놓고 오른쪽 키를 누른뒤에
[Breakpoint] - [Hardware, on access] - [DWORD]를 누르면 브레이크 포인트가 지정되는데 F9를 누르면 갈 수 있다.

F9를 누르면 JMP문이 있을텐데 그곳에서 JMP문을 실행해서 가게 된곳에서 마우스 오른쪽 키를 눌러서 [Analysis] - [Analyze Code]를 누르면 코드가 복구된다.





그리고 실행한다.

```
00455D07  .^E9 64B5FEFF  JMP Reverse_.00441270
00455D0C     245D4500    DD Reverse_.00455D24
00455D10     345D4500    DD Reverse_.00455D34
00455D14     D0344400    DD Reverse_.004434D0
```

F8로 실행한다.

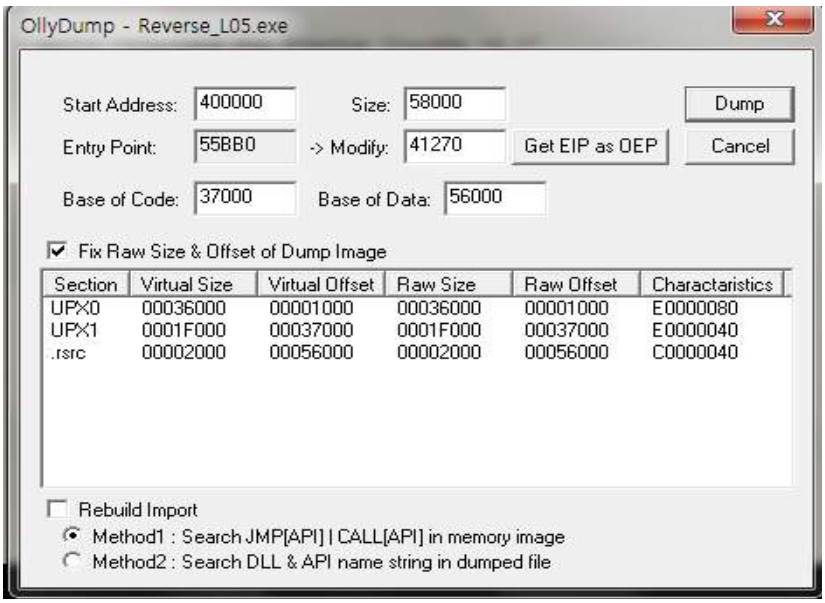
```
00441270  > 55           PUSH EBP
00441271  . 8BEC         MOV EBP,ESP
00441273  ? 83C4 F4      ADD ESP,-0C
00441276  . B8 60114400  MOV EAX,Reverse_.00441160
0044127B  . E8 E848FCFF  CALL Reverse_.00405B68
00441280  ? A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441285  ? 8B00         MOV EAX,DWORD PTR DS:[EAX]
00441287  ? E8 ECBBFFFF  CALL Reverse_.0043CE78
0044128C  ? A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441291  ? 8B00         MOV EAX,DWORD PTR DS:[EAX]
00441293  . BA D0124400  MOV EDX,Reverse_.004412D0        ASCII "Crackers For Freedom CrackMe v3.0"
00441298  . E8 17B8FFFF  CALL Reverse_.0043CAB4
0044129D  ? 8B0D 102D440(MOV ECX,DWORD PTR DS:[442D10]   Reverse_.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]   Reverse_.00440CA8
004412B0  . E8 DBBBFFFF  CALL Reverse_.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
```

여기서 [Analysis] - [Analyze Code]를 해준다.

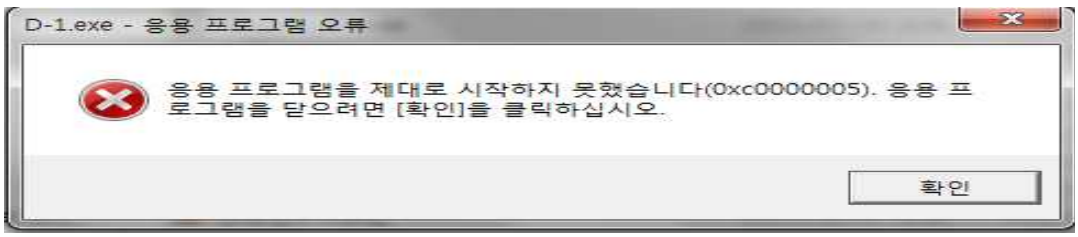
```
00441270  > 55           PUSH EBP
00441271  . 8BEC         MOV EBP,ESP
00441273  . 83C4 F4      ADD ESP,-0C
00441276  . B8 60114400  MOV EAX,Reverse_.00441160
0044127B  . E8 E848FCFF  CALL Reverse_.00405B68
00441280  . A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441285  . 8B00         MOV EAX,DWORD PTR DS:[EAX]
00441287  . E8 ECBBFFFF  CALL Reverse_.0043CE78
0044128C  . A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441291  . 8B00         MOV EAX,DWORD PTR DS:[EAX]
00441293  . BA D0124400  MOV EDX,Reverse_.004412D0        ASCII "Crackers For Freedom CrackMe v3.0"
00441298  . E8 17B8FFFF  CALL Reverse_.0043CAB4
0044129D  . 8B0D 102D440(MOV ECX,DWORD PTR DS:[442D10]   Reverse_.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]   Reverse_.00440CA8
004412B0  . E8 DBBBFFFF  CALL Reverse_.0043CE90
004412B5  . A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
004412BA  . 8B00         MOV EAX,DWORD PTR DS:[EAX]
004412BC  . E8 4FBCFFFF  CALL Reverse_.0043CF10
004412C1  . E8 AA23FCFF  CALL Reverse_.00403670
004412C6  . 0000         ADD BYTE PTR DS:[EAX],AL
004412C8  . FFFFFFFF     DD FFFFFFFF
004412CC  . 21000000     DD 00000021
004412D0  . 43 72 61 63 (ASCII "Crackers For Fre"
004412E0  . 65 64 6F 6D 2ASCII "edom CrackMe v3."
004412F0  . 30 00        ASCII "0",0
004412F2     00          DB 00
004412F3     00          DB 00
004412F4     00          DB 00
004412F5     00          DB 00
004412F6     00          DB 00
004412F7     00          DB 00
004412F8     00          DB 00
```

이제 코드가 제대로 복구되었다.
하지만 여기서 프로그램을 제대로 실행시키기 위해 거쳐야할 과정이 있다.

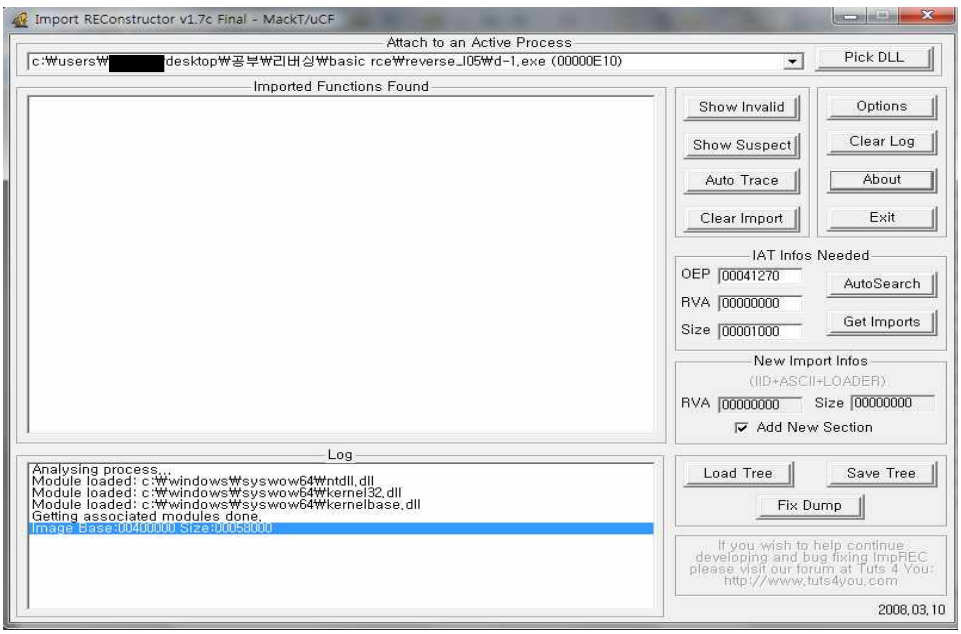
여기까지 됐다면 메뉴에 있는 [Plugins] - [OllyDump] - [Dump debugged process]를 누른다.
(OllyDump는 Plugin을 추가 해야한다. 구글에 OllyDump를 검색하면 다운 받을 수 있을 것이다.)



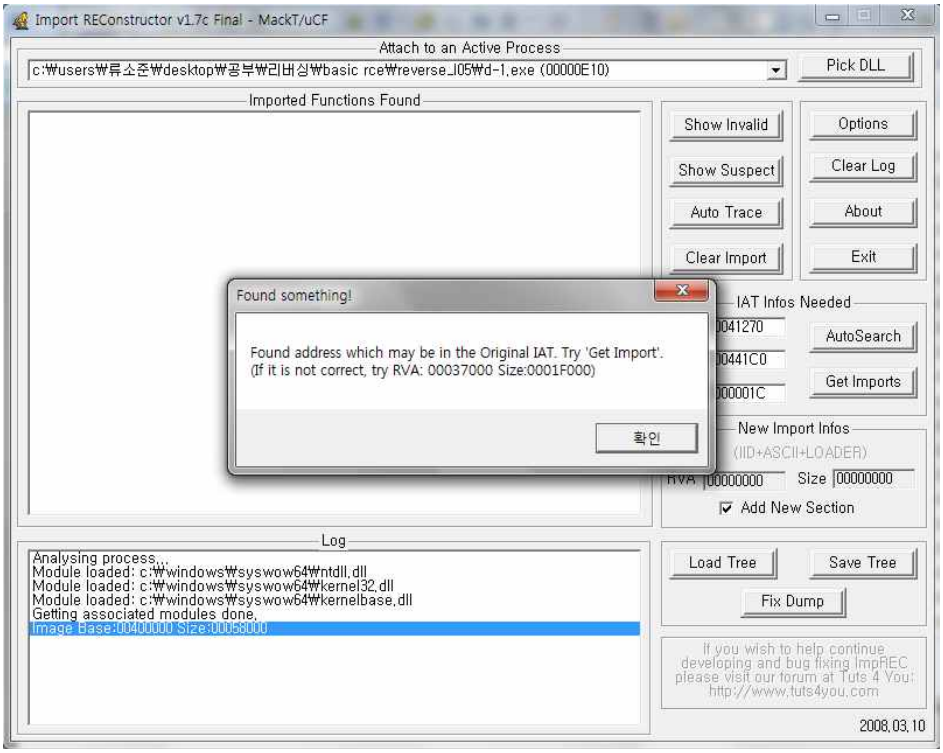
그럼 이런창이 하나 뜰 것이다. 밑에 Rebuild Import가 체크 되어 있을 것이다. 체크를 해지하자.
그리고 Dump버튼을 누르자. 저장을 한후 실행시키면은



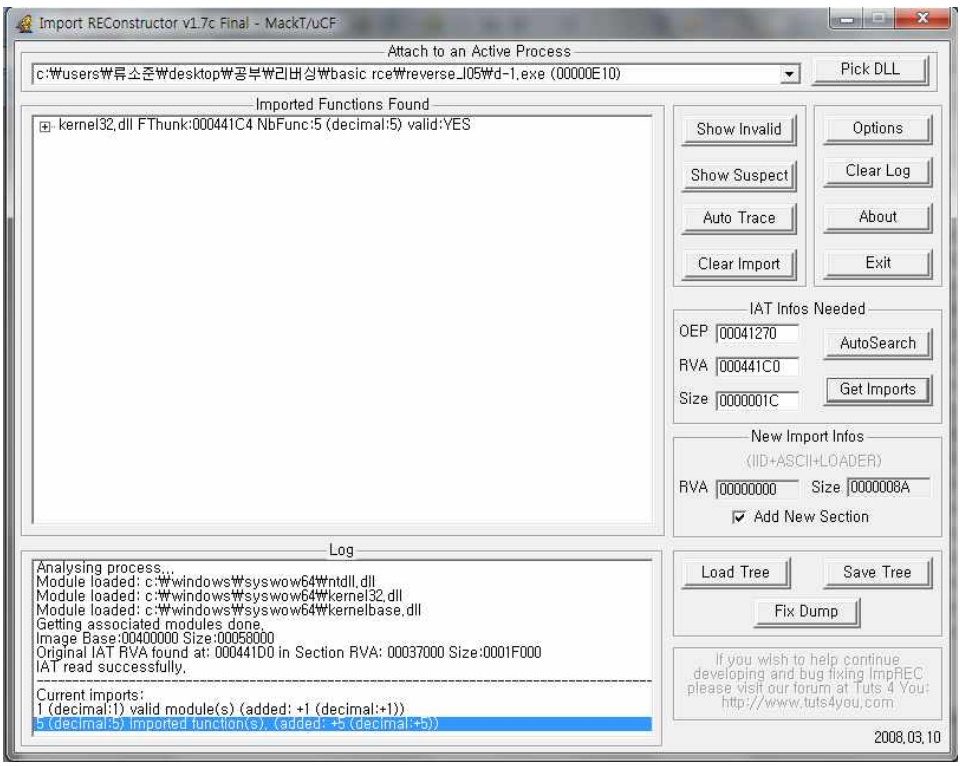
이런 메시지가 뜰 것이다. 이제는 이 오류를 해결해 줘야 한다.
ImpREC를 다운 받자. 구글링을 하면 받을 수 있을 것이다. 다운을 받고 실행을 시켜 주자.
그리고 OllyDump로 Dump해준 파일을 실행시키고 저 오류메시지를 띄어놓자.(실행 시키지 않으면 목록에 뜨질 않는다.) 그리고 목록에서 파일을 선택하자.



이렇게 선택을 한 후 AutoSearch를 누르자.



그리고 나서 저 창이 뜨면은 Get Imports 버튼을 눌러주자.



그런 후 YES란 말이 뜨면 성공 한 것이다.

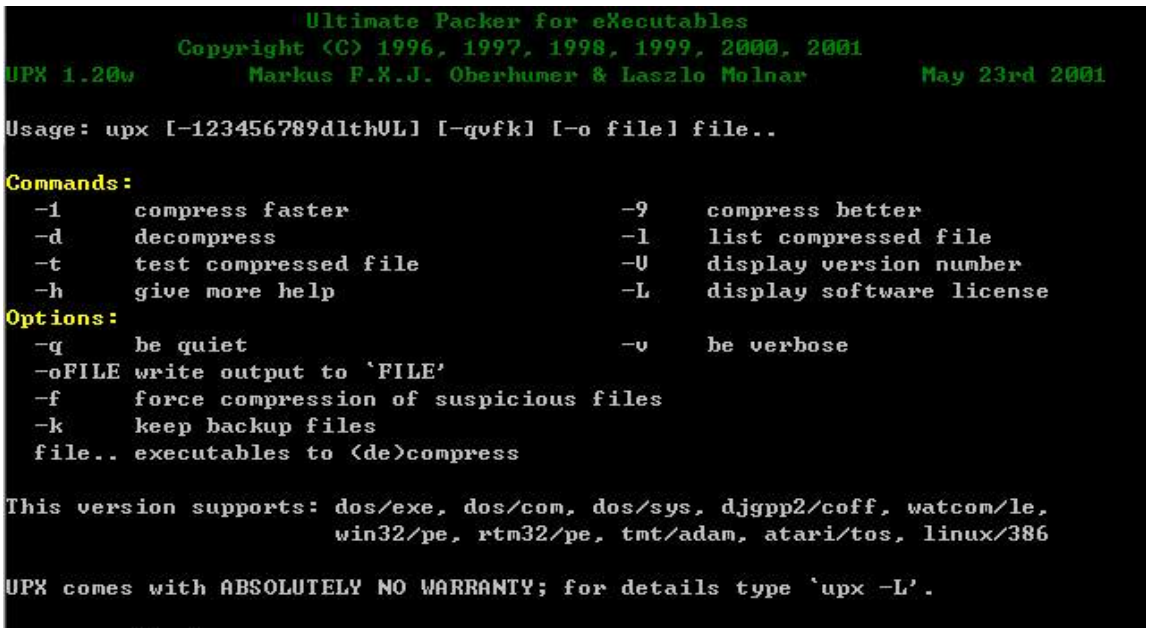
이제 성공했으니 Fix Dump 버튼을 눌러 오류가 났었던 파일을 지정해주자.
그러면 파일 끝에 _가 붙어서 다시 생길 것이다. 그리고 그것은 제대로 실행이 되는 파일일 것이다.
(여기까지 해줬는데 실행을 했더니 아무것도 안뜨네여.. 왜 그런지 아시는분 알려주세여 ㅠㅠ
아 방법은 이렇게 하는거 맞습니다. 실행은 안되지만 올리디버거에서는 제대로 나옵니다ㅎ)

이로써 방법 1이 끝났습니다.

이번엔 방법 2인 언패커 프로그램을 사용해서 언패킹 방법이다.

처음에 PEID로 확인 했듯이 이 프로그램은 UPX로 패킹 되었다. UPX 언패킹 프로그램은 구하기 쉬우니 금방 구할 수 있을 것이다.

실행법 : UPX.exe를 다운 받고 system32 폴더에 넣자. 그리고 cmd를 실행한 후 upx.exe를 치면 이렇게 나올 것이다.



나와있듯이 언패킹 방법은 upx -d 파일명+확장자를 입력하면 된다. (참고로 [cd 바탕 화면] 명령어 등과 같이 파일이 있는 경로로 가야 패킹,언패킹을 할 수 있다. 나는 cd 명령어가 안먹히길래 쉬푸트를 누른채 폴더를 오른쪽키를 누르니 뜨는 새 명령창에서 열기를 이용했다.)

성공을 하면 이런 메시지를 볼 수 있을 것이다.

끝이다. 저 메시지가 뜸과 동시에 패킹된 파일은 없어지고 언패킹된파일만이 남는다.

이로써 언패킹 방법 설명은 끝났다. 이제 올리디버거를 통해 소스를 보자.

```
00441270  >  55           PUSH EBP
00441271  .  8BEC         MOV EBP,ESP
00441273  .  83C4 F4      ADD ESP,-0C
00441276  .  B8 60114400  MOV EAX,Reverse_.00441160
0044127B  .  E8 E848FCFF  CALL Reverse_.00405B68
00441280  .  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441285  .  8B00         MOV EAX,DWORD PTR DS:[EAX]
00441287  .  E8 ECBBFFFF  CALL Reverse_.0043CE78
0044128C  .  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00441291  .  8B00         MOV EAX,DWORD PTR DS:[EAX]
00441293  .  BA D0124400  MOV EDX,Reverse_.004412D0   ASCII "Crackers For Freedom CrackMe v3.0"
00441298  .  E8 17B8FFFF  CALL Reverse_.0043CAB4
0044129D  .  8B0D 102D440(MOV ECX,DWORD PTR DS:[442D10]  Reverse_.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]  Reverse_.00440CA8
004412B0  .  E8 DBBBFFFF  CALL Reverse_.0043CE90
004412B5  .  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
004412BA  .  8B00         MOV EAX,DWORD PTR DS:[EAX]
004412BC  .  E8 4FBCFFFF  CALL Reverse_.0043CF10
004412C1  .  E8 AA23FCFF  CALL Reverse_.00403670
004412C6  .  0000         ADD BYTE PTR DS:[EAX],AL
004412C8  .  FFFFFFFF     DD FFFFFFFF
004412CC  .  21000000     DD 00000021
004412D0  .  43 72 61 63  ASCII "Crackers For Fre"
004412E0  .  65 64 6F 6D  ASCII "edom CrackMe v3."
004412F0  .  30 00        ASCII "0",0
004412F2     00           DB 00
004412F3     00           DB 00
004412F4     00           DB 00
004412F5     00           DB 00
004412F6     00           DB 00
004412F7     00           DB 00
004412F8     00           DB 00
```

처음에 우리가 틀린 시리얼코드를 입력 했을 때 Wrong Serial,try again! 이란 메시지가 떴었다. 그럼 성공했을 때의 메시지도 있을 것이다. 오른쪽 키를 눌러 [Search for] - [All referenced text strins] 를 누르자. 그리고 Wrong Serial,try again!를 찾아보자.

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

중간쯤에 Wrong Serial,try again! 메시지를 볼 수 있다. 더블 클릭을 해서 가 보자.

```
00440F04  .v 75 18        JNZ SHORT Reverse_.00440F1E
00440F06  .  6A 00        PUSH 0
00440F08  .  B9 E80F4400  MOV ECX,Reverse_.00440FE8   ASCII "No Serial entered"
00440F0D  .  BA FC0F4400  MOV EDX,Reverse_.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 Reverse_.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 Reverse_.00420E20
00440F2C  .  8B45 FC      MOV EAX,DWORD PTR SS:[EBP-4]
00440F2F  .  BA 14104400  MOV EDX,Reverse_.00441014   ASCII "Registered User"
00440F34  .  E8 F32BFCFF  CALL Reverse_.00403B2C
00440F39  .v 75 51        JNZ SHORT Reverse_.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 Reverse_.00420E20
00440F49  .  8B45 FC      MOV EAX,DWORD PTR SS:[EBP-4]
00440F4C  .  BA 2C104400  MOV EDX,Reverse_.0044102C   ASCII "GFX-754-IER-954"
00440F51  .  E8 D62BFCFF  CALL Reverse_.00403B2C
00440F56  .v 75 1A        JNZ SHORT Reverse_.00440F72
00440F58  .  6A 00        PUSH 0
00440F5A  .  B9 3C104400  MOV ECX,Reverse_.0044103C   ASCII "CrackMe cracked successfully"
00440F5F  .  BA 5C104400  MOV EDX,Reverse_.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 Reverse_.0043D068
00440F70  .v EB 32        JMP SHORT Reverse_.00440FA4
00440F72  >  6A 00        PUSH 0
00440F74  .  B9 80104400  MOV ECX,Reverse_.00441080   ASCII "Beggar off!"
00440F79  .  BA 8C104400  MOV EDX,Reverse_.0044108C   ASCII "Wrong Serial,try again!"
00440F7E  .  A1 442C4400  MOV EAX,DWORD PTR DS:[442C44]
00440F83  .  8B00         MOV EAX,DWORD PTR DS:[EAX]
00440F85  .  E8 DEC0FFFF  CALL Reverse_.0043D068
```

Wrong Serial,try again! 위에
ASCII “CrackMe cracked successfully"
ASCII "Congrats! You cracked this CrackMe!"
가 있다. 분명히 이건 성공했을때의 메시지 일 것이다. 그리고 그 위에는 00440F56 주소에
JNZ SHORT Reverse_.00440F72 가 있다. 같지 않으면 점프이다. 즉, 같으면 성공 메시지를 출력한다는 말이다. 그리고 그 위에는 ASCII "GFX-754-IER-954" 가 있다. 아마도 GFX-754-IER-954와 같거나 같지 않으면 점프를 하나 보다. 그러므로 이 프로그램의 등록 키는 GFX-754-IER-954 이다.
참고로 ID는 그 위에 있는 Registered User 일 것이다.
Continue에 GFX-754-IER-954를 넣어보자. 통과할 것이다.
(그리고 GFX-754-IER-954와 Registered User 각각 바로 위코드에는 입력한 시리얼키와 ID가 들어가 있다. 그래서 하나라도 틀리면 바로 JMP를 해서 등록이 안된다.)

2011.08.16

Made by hypen1117
hypen1117@daum.net
http://hypen1117.tistory.com

리버싱을 그렇게 잘하지 못해 구체적이지 못하고 잘못 될 수 있습니다.
잘못되거나 부족한 부분 지적해 주시길 바랍니다.