Reverse L05 Start

Author : Acid Bytes [CFF]

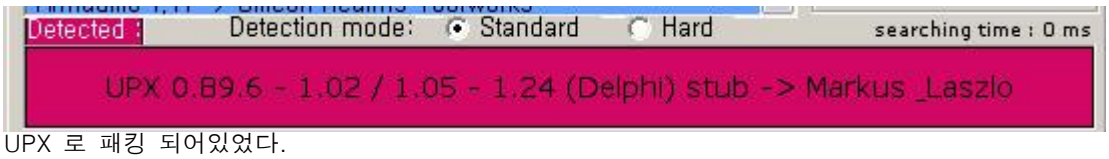
Korea :

이 프로그램의 등록키는 무엇인가

English :

The registration key of this program is?

Stud_PE 로 파일을 열어보니



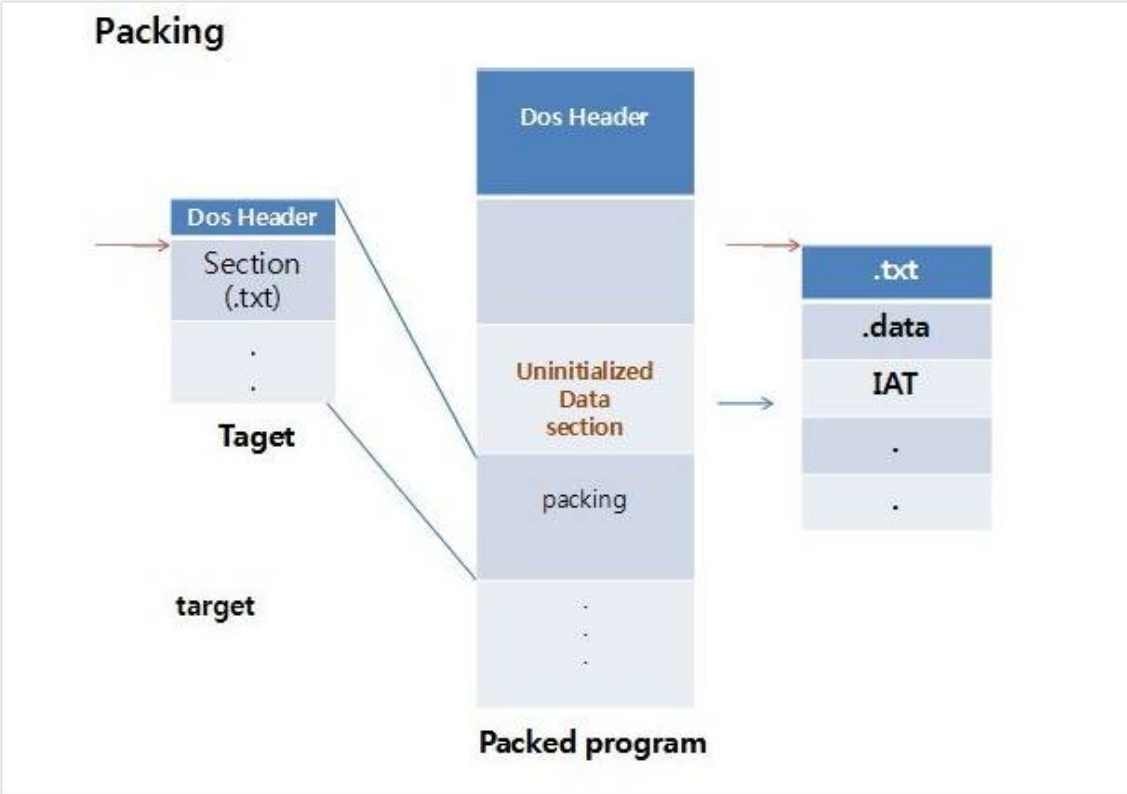
UPX 로 패킹 되어있었다.

패킹 에 대한 설명

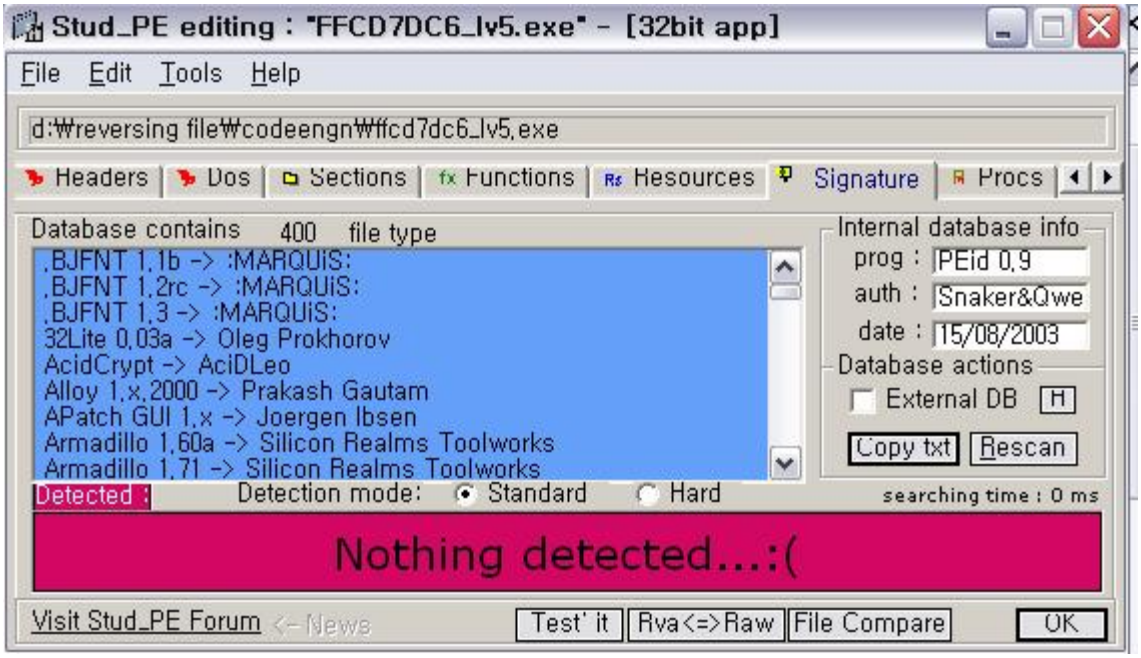
패커(Packer)에 대해 다시 한번 간단히 정리

패킹(packing)은 실행파일 포장이라는 개념으로 쉽게 이해하시면 될 것 같습니다.

아래 그림은 파일이 패킹되어 메모리에 올라가는 일괄의 과정을 표현한 것으로서 패킹된 파일은 메모리 할당시 재배치(Relocation) 과정을 하지 않기 위해 target 프로그램과 동일한 위치에 .txt 섹션을 배치 합니다.
Uninitialized data section은 언패킹 후 메모리에 올릴 장소입니다.



언패킹을 하기 위해서는 먼저 Packer Detection(탐지)을 통해 패커를 확인하는 작업이 선행되어야 합니다.
UPX 로 패킹된 파일을 UPX 언패킹 하는 프로그램으로 언팩을 한 후에
다시 PEID를 확인 해보았다.



언패킹 된 것을 확인 한후에 올리 디버거 로 실행을 해보았다.

등록키를 구하라 해놓고 키 값이 적혀져 있어 Register now ! 를 해보니

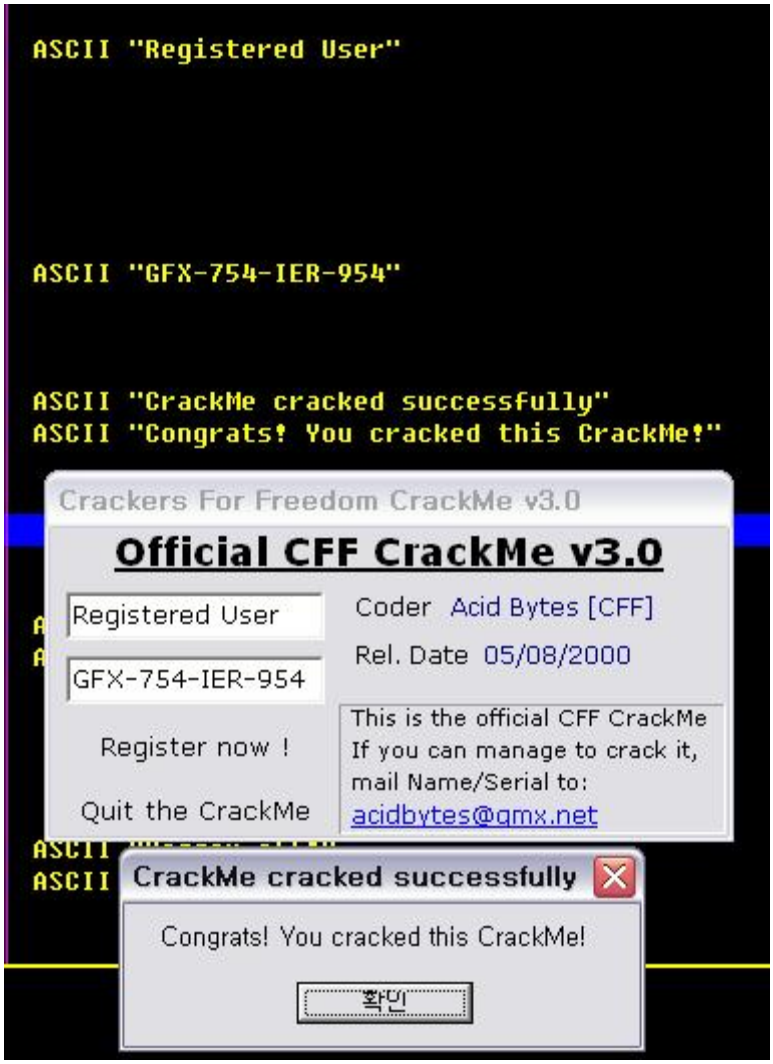
Fake 였다.

Search For -> All Referenced Text Strings 로 프로그램의 문자열들을 살펴 보니

```
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!"
```

프로그램 실행 시 출력된 키 값과 다른 키 값이 내장 되어있었다

```
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
00440F70 .vEB 32            JMP SHORT FFCD7DC6.00440FA4
00440F72 > 6A 00            PUSH 0
00440F74 . B9 80104400      MOV ECX,FFCD7DC6.00441080     ASCII "Beggar off!"
00440F79 . BA 8C104400      MOV EDX,FFCD7DC6.0044108C     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 FFCD7DC6.0043D068
00440F8A .vEB 18            JMP SHORT FFCD7DC6.00440FA4
00440F8C > 6A 00            PUSH 0
00440F8E . B9 80104400      MOV ECX,FFCD7DC6.00441080     ASCII "Beggar off!"
00440F93 . BA 8C104400      MOV EDX,FFCD7DC6.0044108C     ASCII "Wrong Serial,try again!"
```



인증 키 값이 그대로 노출 된 거로 보아 문제 출제 의도는 UPX 패킹에 관한 문제 인거 같았다.

key: GFX-754-IER-954