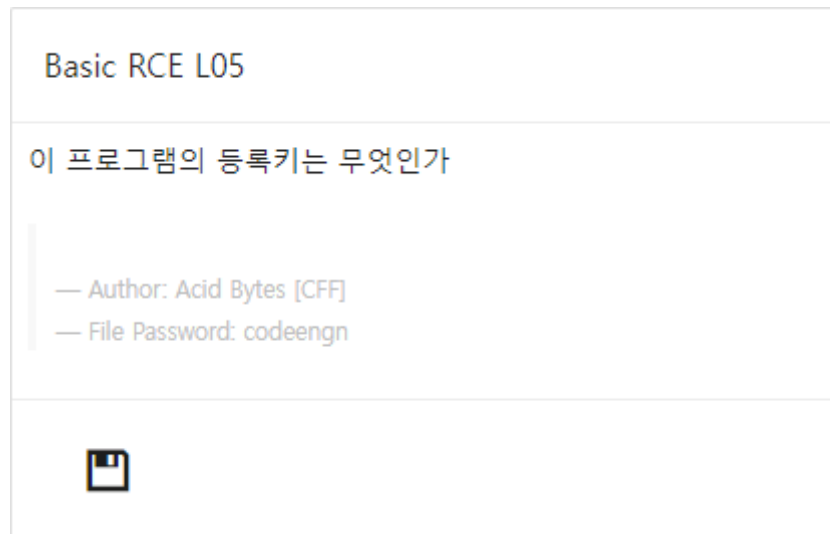
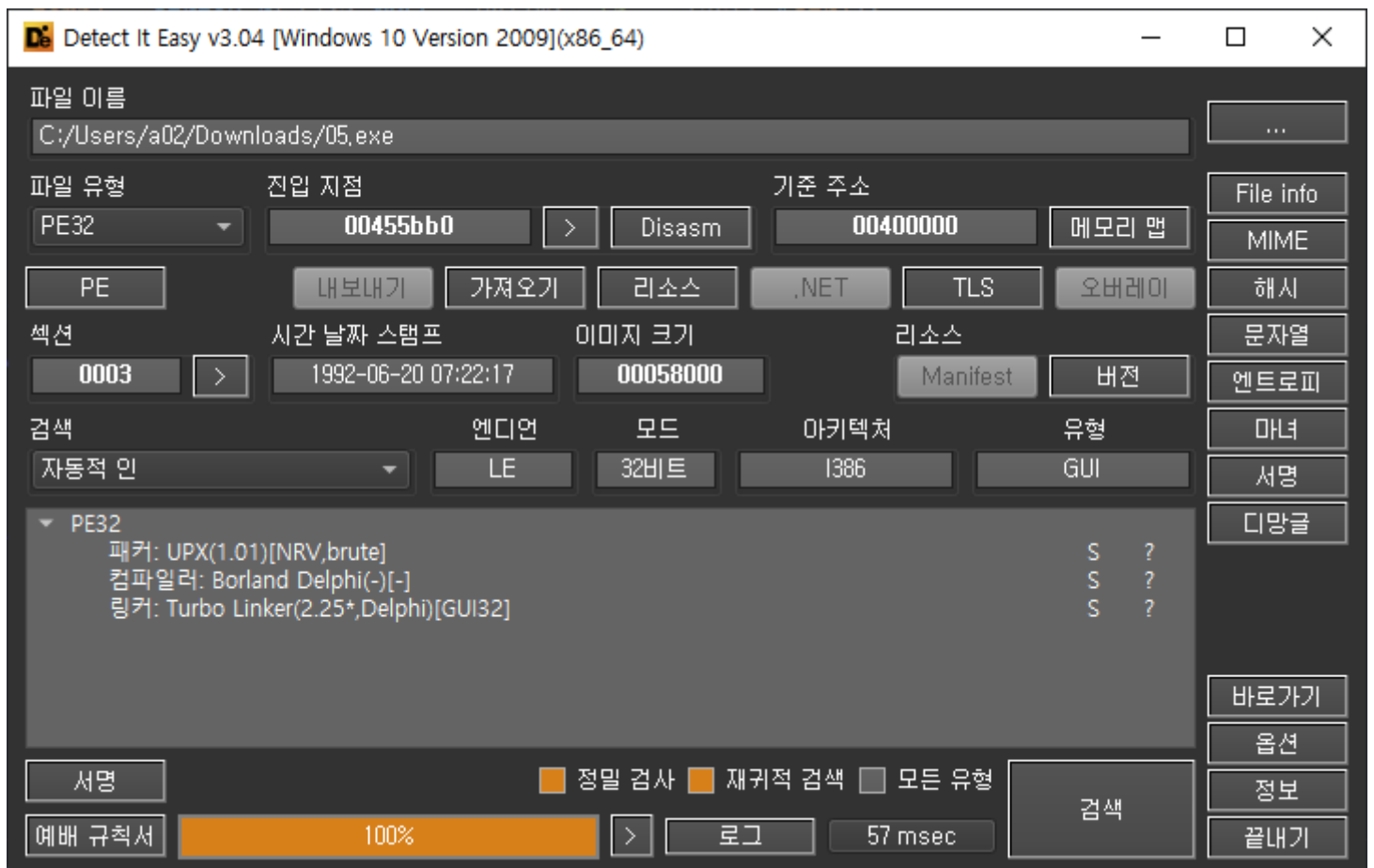


codeengn-basic-L05 풀이 UPX패킹 풀기

리버싱 문제풀이 / Wonlf / 2022. 3. 11. 12:15



한참을 삽질하다가 풀이를 보고 패킹이 되어 있다는 사실을 알았다. 이제부터 DIE로 정적분석을 먼저 해보고 동적분석을 진행 해야겠다.



UPX로 패킹이 되어 있습니다. 언패킹을 해보겠습니다.

```
PS C:\Users\A02\Downloads\upx-3.96-win64> .\upx.exe -d C:\Users\A02\Downloads\05.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
315392 <-    132608    42.05%    win32/pe    05.exe
upx: C:\Users\A02\Downloads\05.exe: IOException: C:\Users\A02\Downloads\05.exe: Permission denied

Unpacked 1 file: 0 ok, 1 error.
```

권한 오류로 언패킹이 되지 않아 찾아보니 파일이 디버거로 열려있으면 안된다고 합니다. 꺼주고 언패킹 하니

```
PS C:\Users\A02\Downloads\upx-3.96-win64> .\upx.exe -d C:\Users\A02\Downloads\05.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
315392 <-    132608    42.05%    win32/pe    05.exe

Unpacked 1 file.
```

성공 이제 파일을 뜯어보겠습니다.

• E8 F4FEFDFF
• 8B45 FC
• BA 14104400
• E8 F32BFCFF
• 75 51
• 8D55 FC
• 8B83 C9020000
• E8 D7FEFDFF
• 8B45 FC
• BA 2C104400
• E8 D62BFCFF
• 75 1A
• 6A 00
• B9 3C104400
• BA 5C104400

call <05.sub_420E20>
mov eax,dword ptr ss:[ebp-4]
mov edx,05.441014
call <05.sub_403B2C>
jne 05.440F8C
lea edx,dword ptr ss:[ebp-4]
mov eax,dword ptr ds:[ebx+2C8]
call <05.sub_420E20>
mov eax,dword ptr ss:[ebp-4]
mov edx,05.44102C
call <05.sub_403B2C>
jne 05.440F72
push 0
mov ecx,<05.sub_44103C>
mov edx,<05.sub_44105C>

edx:EntryPoint, 441014:"Registered User"

edx:EntryPoint

edx:EntryPoint, 44102C:"GFX-754-IER-954"

ecx:EntryPoint, 44103C:"CrackMe cracked successfully"
edx:EntryPoint, 44105C:"Congrats! You cracked this CrackMe!"

CrackMe cracked successfully

Congrats! You cracked this CrackMe!

확인

딱 보니 저 두개가 ID와 PW같네요 입력하니 성공입니다.

막상 까보니 쉽네요

이 번문제는 UPX패킹과 문제 풀기 전에 정적분석을 먼저 해야겠다는 가르침을 얻었습니다