

# Reversing.kr Easy Unpack 3 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 31. 10:06



Easy Unpack

Point: 100 Solved: 3643

압축 해제를 하고 보니, ReadMe.txt가 있다 읽어보겠다.

ReversingKr UnpackMe

Find the OEP

ex) 00401000

OEP를 찾아달라고 한다.

OEP에 대해서는 전의 링크를 참조 하겠다.

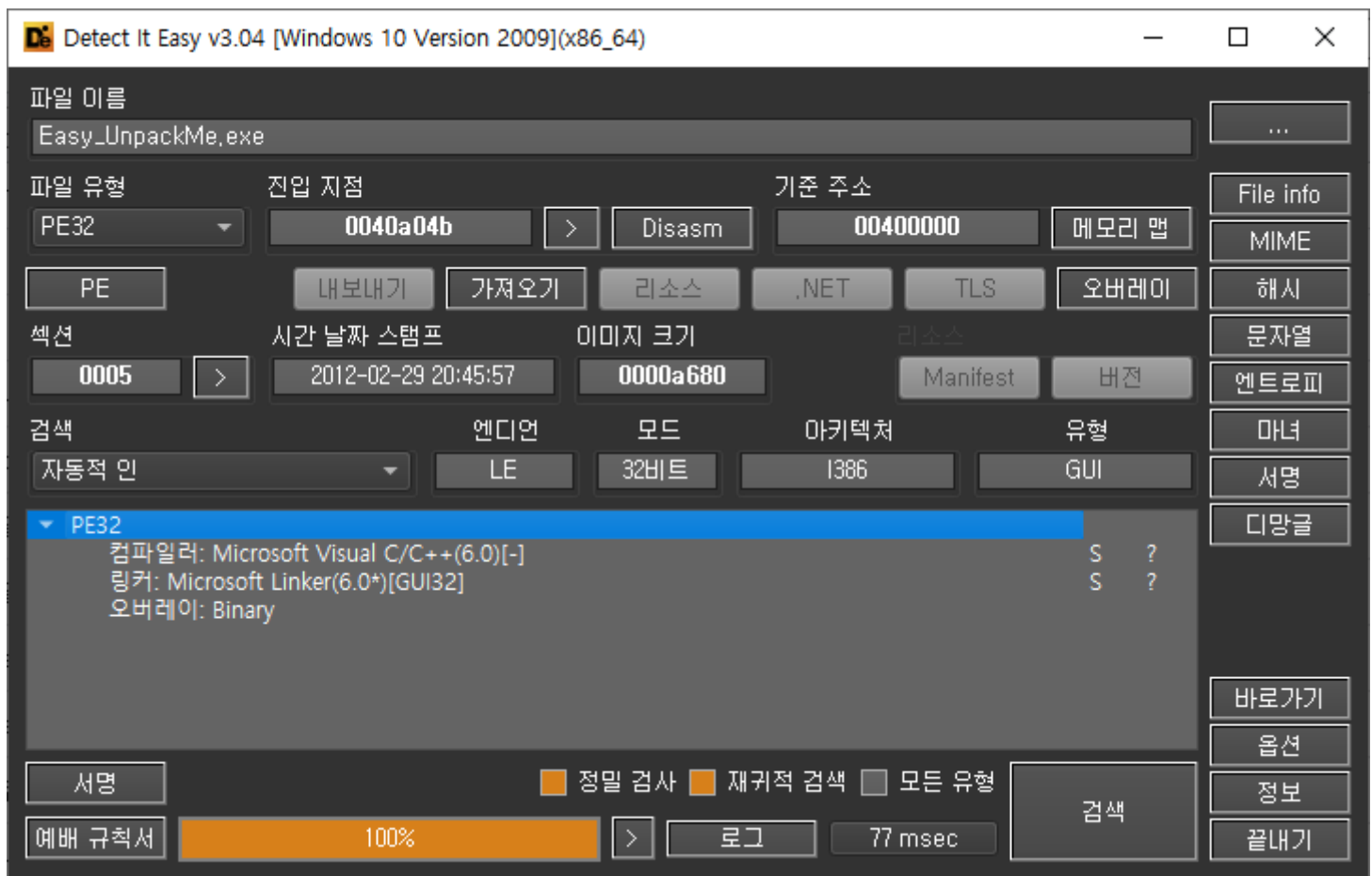
2022.03.13 - [리버싱 문제 풀이/CodeEngn.com] - codeengn-basic-L06 풀이 OEP알아내기

```
06.4235D4  
06.422A30  
06.401290  
p,8  
ax, eax  
06.4010A3  
1, esp  
0  
06.420048  
06.sub_420038>  
x, dword ptr ds:[423638]  
CX  
word ptr ds:[<&Message
```

codeengn-basic-L06 풀이 OEP알아내기

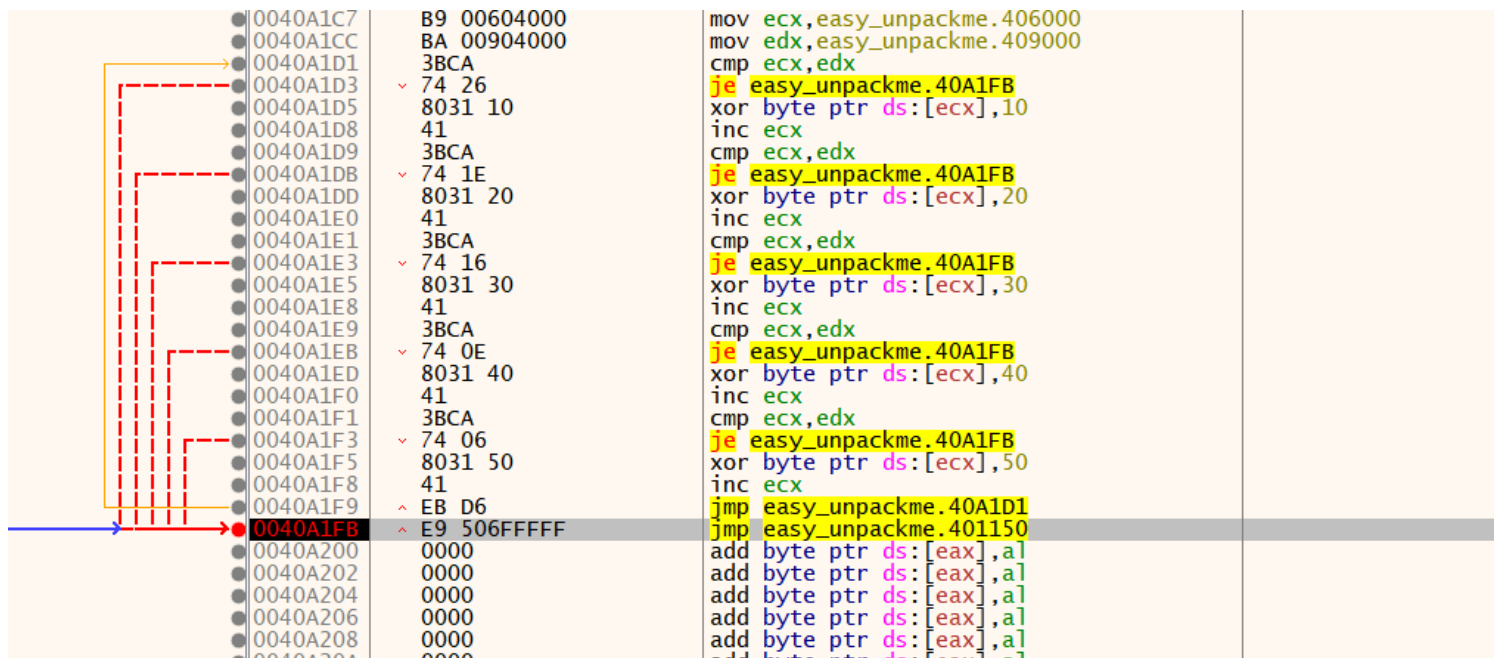
wonlf.tistory.com

Die에 넣어보았더니



패킹이 되어있다고 뜨지 않는다.

디버거로 열어서 천천히 아래로 내려가다 보면,



마지막에 OEP로 점프하는 구문을 찾을 수 있다.

ReadMe에 적힌 양식대로 한다면 Key는 "00401150"이 되겠다.

OEP문제를 3번째 풀면서 2가지를 느꼈는데...

첫번째로 패킹이 되어 있는 것을 복호화 하는 작업은 필수적으로 있어야 하기 때문에 파일 처음에 복호화 하는 것 같은 구문이 보인다.

0040A186	3BCA	cmp ecx,edx
0040A188	74 26	je easy_unpackme.40A1B0
0040A18A	8031 10	xor byte ptr ds:[ecx],10
0040A18D	41	inc ecx
0040A18E	3BCA	cmp ecx,edx
0040A190	74 1E	je easy_unpackme.40A1B0
0040A192	8031 20	xor byte ptr ds:[ecx],20
0040A195	41	inc ecx
0040A196	3BCA	cmp ecx,edx
0040A198	74 16	je easy_unpackme.40A1B0
0040A19A	8031 30	xor byte ptr ds:[ecx],30
0040A19D	41	inc ecx
0040A19E	3BCA	cmp ecx,edx
0040A1A0	74 0E	je easy_unpackme.40A1B0
0040A1A2	8031 40	xor byte ptr ds:[ecx],40
0040A1A5	41	inc ecx
0040A1A6	3BCA	cmp ecx,edx
0040A1A8	74 06	je easy_unpackme.40A1B0
0040A1AA	8031 50	xor byte ptr ds:[ecx],50
0040A1AD	41	inc ecx
0040A1AE	EB D6	jmp easy_unpackme.40A186
0040A1B0	68 78A64000	push easy_unpackme.40A678
0040A1B5	5A 04	pop eax

복호화로 추정되는 구문

두번째로 OEP로 점프를 하고 난 뒤에 아래 구문은 특정 코드로 가득 차있다.

0040A1FB	E9 506FFFFF	jmp easy_unpackme.401150
0040A200	0000	add byte ptr ds:[eax],a1
0040A202	0000	add byte ptr ds:[eax],a1
0040A204	0000	add byte ptr ds:[eax],a1
0040A206	0000	add byte ptr ds:[eax],a1
0040A208	0000	add byte ptr ds:[eax],a1
0040A20A	0000	add byte ptr ds:[eax],a1
0040A20C	0000	add byte ptr ds:[eax],a1
0040A20E	0000	add byte ptr ds:[eax],a1
0040A210	0000	add byte ptr ds:[eax],a1
0040A212	0000	add byte ptr ds:[eax],a1
0040A214	0000	add byte ptr ds:[eax],a1
0040A216	0000	add byte ptr ds:[eax],a1
0040A218	0000	add byte ptr ds:[eax],a1
0040A21A	0000	add byte ptr ds:[eax],a1
0040A21C	0000	add byte ptr ds:[eax],a1
0040A21E	0000	add byte ptr ds:[eax],a1
0040A220	0000	add byte ptr ds:[eax],a1
0040A222	0000	add byte ptr ds:[eax],a1
0040A224	0000	add byte ptr ds:[eax],a1
0040A226	0000	add byte ptr ds:[eax],a1
0040A228	0000	add byte ptr ds:[eax],a1
0040A22A	0000	add byte ptr ds:[eax],a1

특정 코드

물론 이런 특징들은 패커마다 다르겠지만,  
복호화 한다. 특정 구문으로 차있다고 알고 있으면 좋을 듯 하다.