

# codeengn-basic-L10 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 31. 22:32

## Basic RCE L10

OEP를 구한 후 '등록성공' 으로 가는 분기점의 OPCODE를 구하시오.

정답인증은 OEP + OPCODE

EX) 00400000EB03

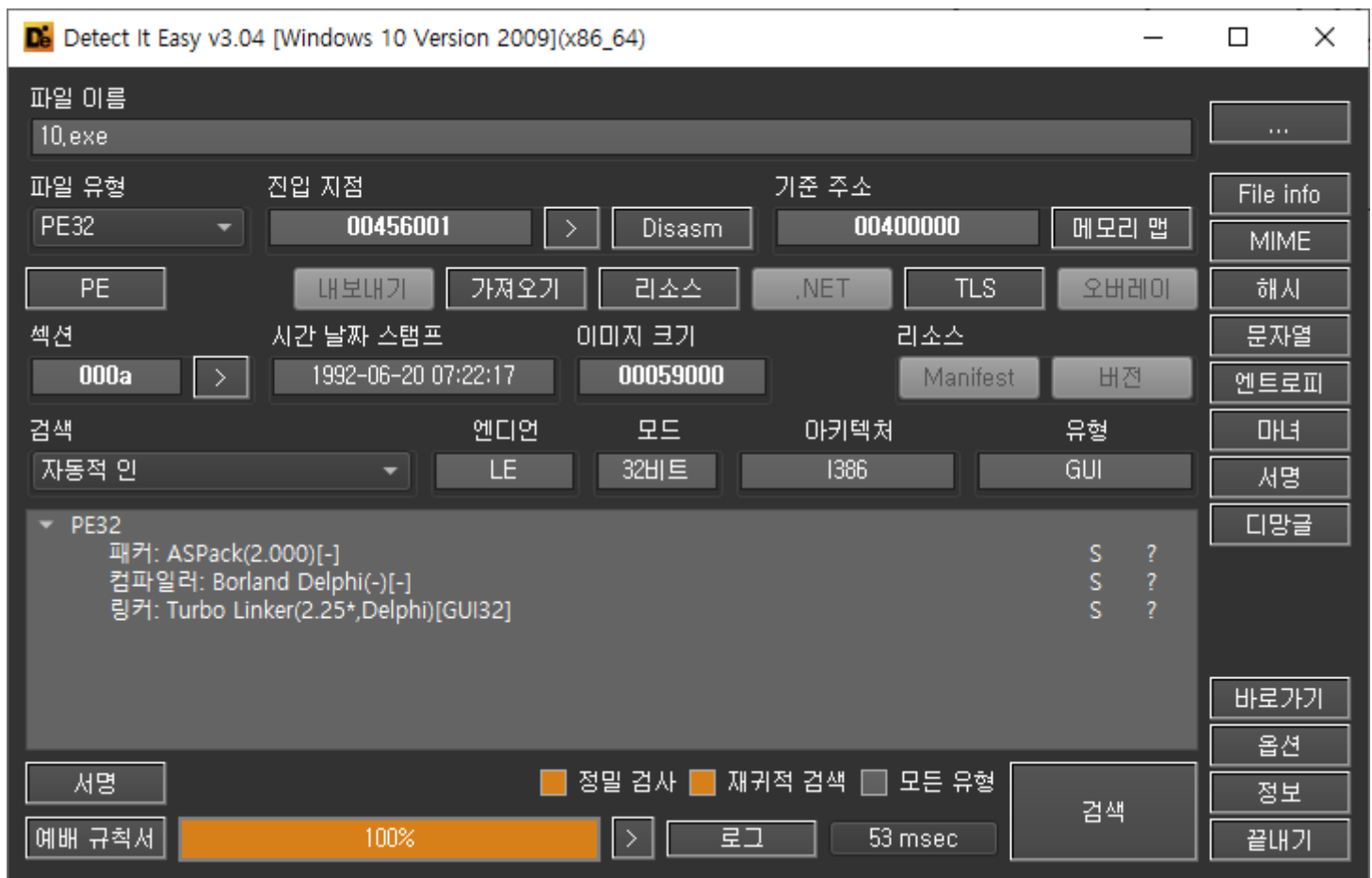
— Author: ArturDents

— File Password: codeengn



문제는 OEP와 '등록성공'으로 가는 분기점의 OPCODE를 원하고 있다.

Die에 넣어보겠다.

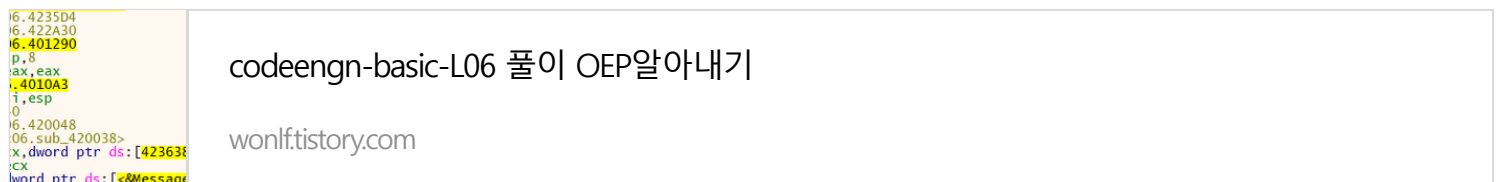


ASPack패커로 패킹이 되어 있는 모습이다.

ASPack패킹을 해제하는 툴이 UPX처럼 있는 건 아닌 것 같은데 UPX와 동일한 방법으로 패킹을 한다고 하니, 수동으로 OEP를 찾아보겠다.

OEP를 찾는 것은

[2022.03.13 - \[리버싱 문제 풀이/CodeEngn.com\] - codeengn-basic-L06 풀이 OEP알아내기](#)

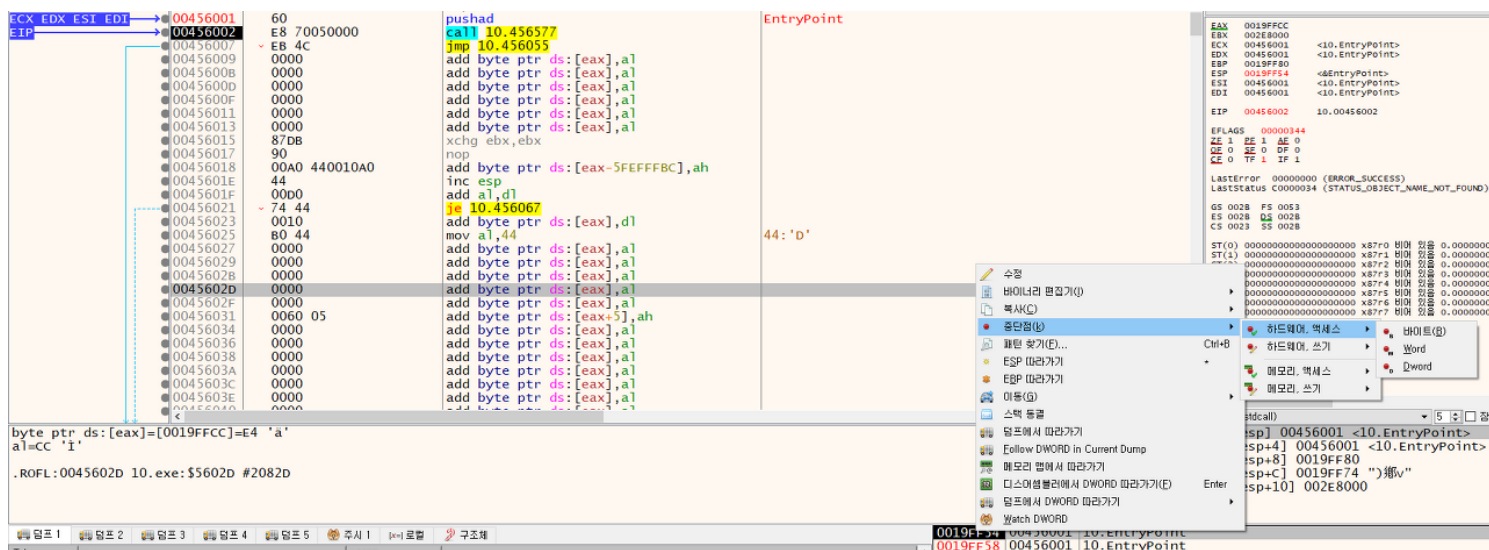


위 링크를 참고 하도록 하고

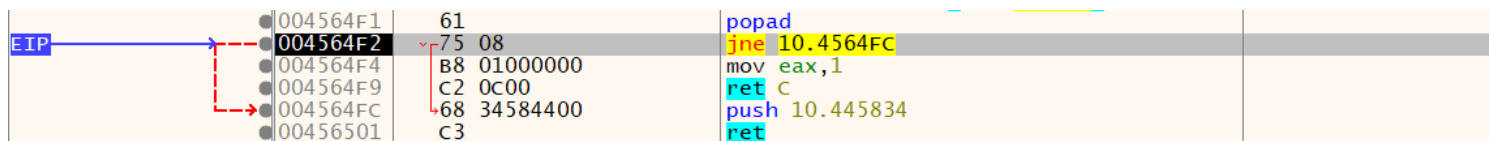
디버거로 열어서 파일을 확인하면,

EIP	ECX	EDX	ESI	EDI	00456001	60	pushad	EntryPoint
					00456002	E8 70050000	call 10.456577	
					00456007	EB 4C	jmp 10.456055	
					00456009	0000	add byte ptr ds:[eax],al	
					0045600B	0000	add byte ptr ds:[eax],al	

UPX처럼 pushad가 반겨주고 있다.



위 링크와 동일한 방법으로 pushad후, 스택에 하드웨어 브레이크 포인트를 걸어주고 OEP를 확인한다.



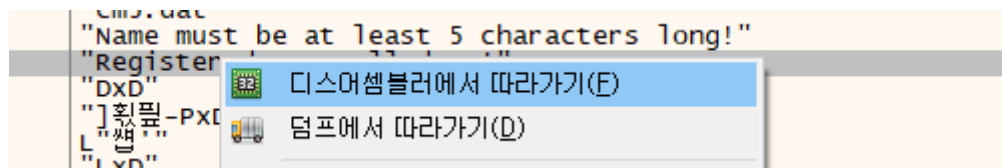
popad가 나오는 모습이고 아래에 push 00445834를 하고 ret까지 실행하고 나면, 실제 EP로 오게 된다.

이제 문자열 찾기를 통해 '등록성공' 구문을 찾아본다.

```
"cm5.dat"
"Name must be at least 5 characters long!"
"Registered ... well done!"
"DxD"
"]유틸-PxD"
"유틸-PxD"
```

"Registered ... well done!" 이라는 성공으로 추정되는 문자열이 보인다.

이 문자열을 사용하는 구문을 찾기 위해 디스어셈블러에서 따라가기를 사용한다.



그럼 이러한 구문이 보이는데,

004454d4	75 55	jne 10.44552B	
004454d6	8D85 F4FDFFFF	lea eax,dword ptr ss:[ebp-20C]	
004454dc	8D95 17FEFFFF	lea edx,dword ptr ss:[ebp-1E9]	edx:EntryPoint
004454e2	E8 1DE6FBFF	call <10.sub_403B04>	
004454e7	8B95 F4FDFFFF	mov edx,dword ptr ss:[ebp-20C]	edx:EntryPoint
004454ed	8B87 D4020000	mov eax,dword ptr ds:[edi+2D4]	
004454f3	E8 B4F5FDFF	call 10.424AAC	
004454f8	8B87 D8020000	mov eax,dword ptr ds:[edi+2D8]	[edi+2D8]:sub_443904+E1
004454fe	8B55 FC	mov edx,dword ptr ss:[ebp-4]	edx:EntryPoint
00445501	E8 A6F5FDFF	call 10.424AAC	
00445506	8B87 E8020000	mov eax,dword ptr ds:[edi+2E8]	
0044550c	BA 60564400	mov edx,<10.sub_445660>	edx:EntryPoint, 445660:"Registered ... we'll done!"
00445511	E8 96F5FDFF	call 10.424AAC	
00445516	8B87 E8020000	mov eax,dword ptr ds:[edi+2E8]	
0044551c	8B40 58	mov eax,dword ptr ds:[eax+58]	
0044551f	BA 00800000	mov edx,8000	edx:EntryPoint
00445524	E8 BFF2FCFF	call <10.sub_4147E8>	
00445529	EB 0A	jmp 10.445535	
0044552B	> 33C0	xor eax,eax	

등록 성공으로 가려면 jne에서 점프를 뛰지 말아야 함으로 jne구문을 분기점으로 볼 수 있다.

그렇기 때문에 OEP "00445834" + jne의 OPCODE "7555" 가 플래그가 되겠다.

**"004458347555"**