

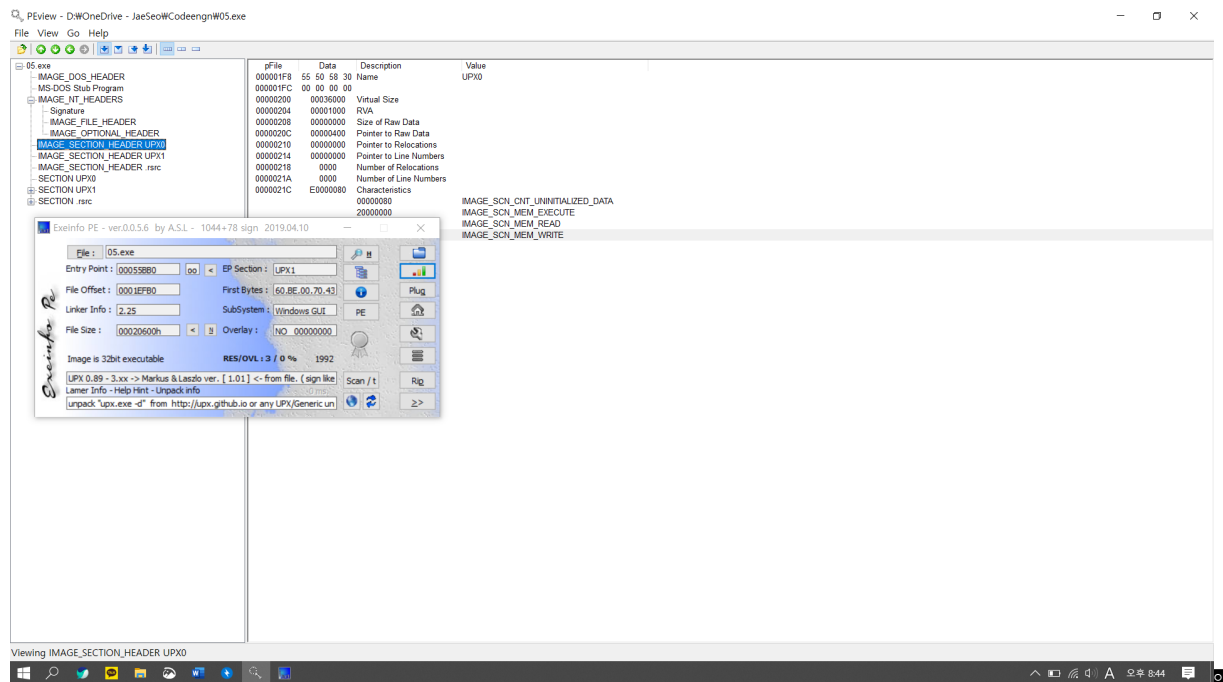
05.exe - 이 프로그램의 등록키는 무엇인가?



프로그램을 실행하면 등록키를 입력하는 inputbox와 name을 입력하는 inputbox가 있고 이것을 이용하여 등록을 진행 하는 프로그램으로 보인다.

이제 프로그램 분석을 시작 한다.

맨 처음 PE분석을 통해 패킹이 되어있는지 확인을 해보는 과정을 진행 해본다.



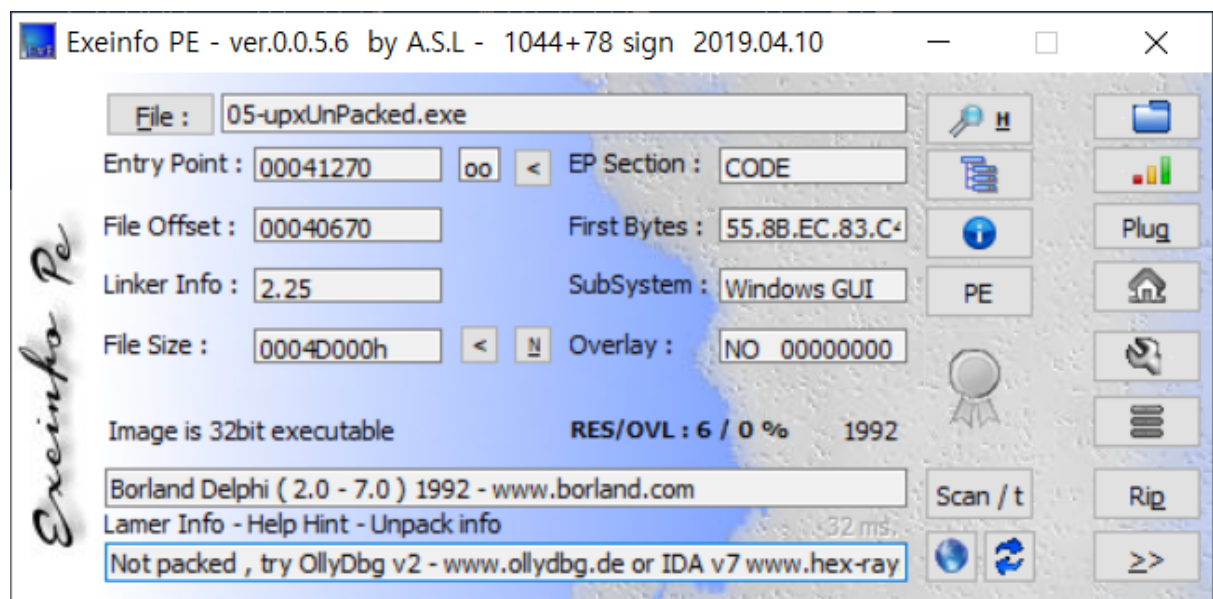
PEView와 Exeinfo PE 툴을 통해 이프로그램은 UPX로 패킹이 되어있는걸 확인 할수 있다.

UPX를 사용하여 언패킹을 진행해본다.❏

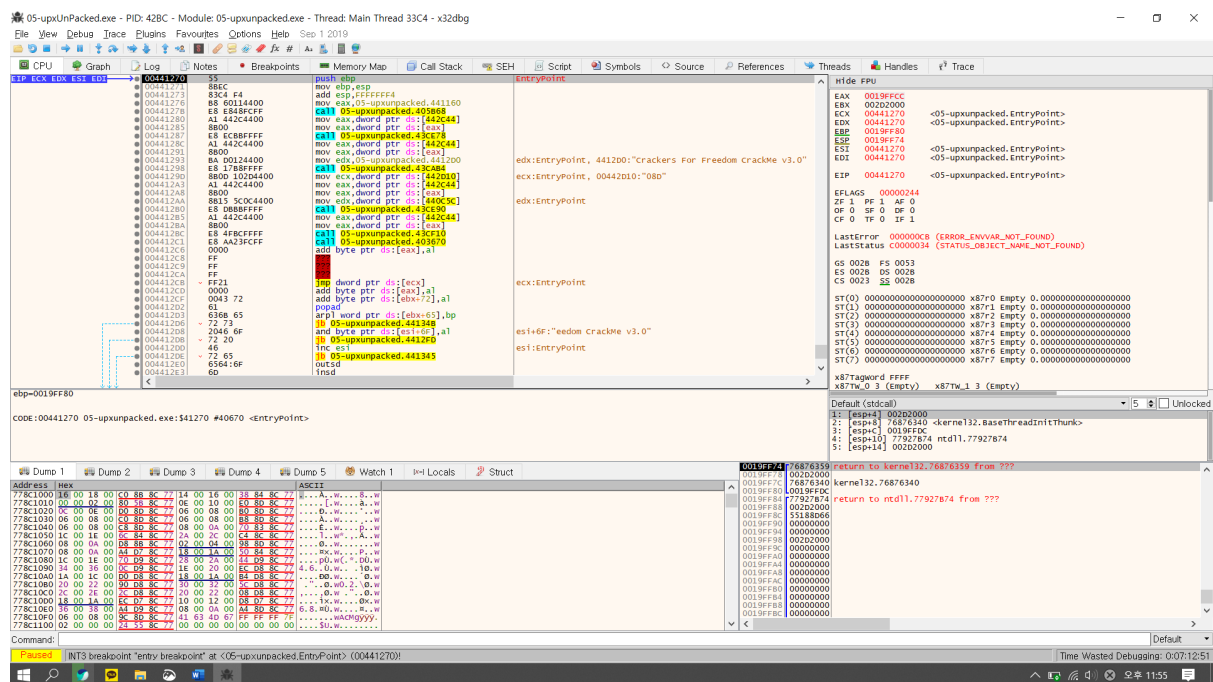
```
PS D:\> .\wupx.exe -d "C:\Users\Wkimja\Documents\WUPX unpacking\05.exe"
wupx v3.95w - www.wupx.net Ultimate Packer for eXecutables
Copyright (C) 1996 - 2018
UPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018

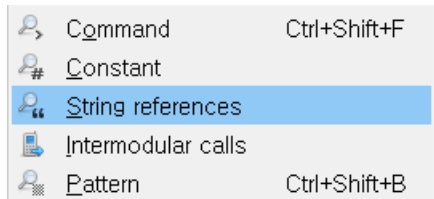
File size      Ratio      Format      Name
-----
315392 <-    132608    42.05%     win32/pe    05.exe

Unpacked 1 file.
PS D:\OneDrive - JaeSeo\KShield Jr\tools\Reversing\wupx-3.95-win64>
```

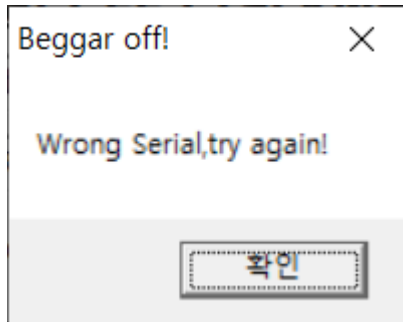


ExeinfoPE를 통해 Unpack이 된 것을 볼수 있다. 이제 X32DBG로 분석을 해본다.❏





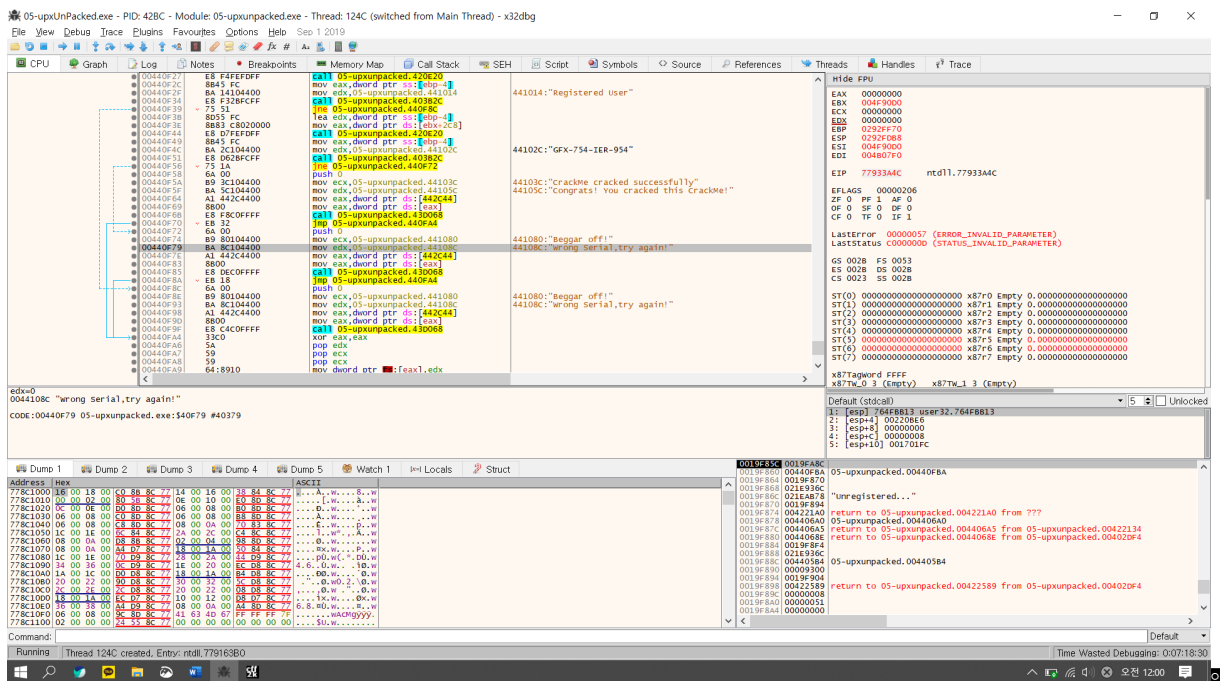
String references 검색으로 통해 등록키로 의심이 되는 값 또는 인증관련 메시지와 관련된 값을 찾는다.



잘못된 입력 값을 입력 했을 때 뜨는 키워드를 통해 검색을 해본다.

Address	Disassembly	String
00440F79	mov edx,05-upxunpacked.44108C	"Wrong Serial,try again!"
00440F93	mov edx,05-upxunpacked.44108C	"Wrong Serial,try again!"

그 결과 이러한 값을 찾을수 있는데 들어가서 분석을 해본다.



바로 주변에 인증을 성공 했을 때 뜨는 문자열 값과 인증키로 의심되는 값을 발견했다

00440F27	E8 F4FEFDFF	call 05-upxunpacked.420E20	
00440F2C	8B45 FC	mov eax, dword ptr ss:[ebp-4]	
00440F2F	BA 14104400	mov edx, 05-upxunpacked.441014	441014:"Registered User"
00440F34	E8 F32BFCFF	call 05-upxunpacked.403B2C	
00440F39	75 51	jne 05-upxunpacked.440F8C	
00440F3B	8D55 FC	lea edx, dword ptr ss:[ebp-4]	
00440F3E	8B83 C8020000	mov eax, dword ptr ds:[ebx+2C8]	
00440F44	E8 D7FEFDFF	call 05-upxunpacked.420E20	
00440F49	8B45 FC	mov eax, dword ptr ss:[ebp-4]	
00440F4C	BA 2C104400	mov edx, 05-upxunpacked.44102C	44102C:"GFX-754-IER-954"
00440F51	E8 D62BFCFF	call 05-upxunpacked.403B2C	
00440F56	75 1A	jne 05-upxunpacked.440F72	
00440F58	6A 00	push 0	
00440F5A	B9 3C104400	mov ecx, 05-upxunpacked.44103C	44103C:"CrackMe cracked successfully"
00440F5F	BA 5C104400	mov edx, 05-upxunpacked.44105C	44105C:"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 05-upxunpacked.43D068	
00440F70	EB 32	jmp 05-upxunpacked.440FA4	
00440F72	6A 00	push 0	
00440F74	B9 80104400	mov ecx, 05-upxunpacked.441080	441080:"Beggar off!"
00440F79	BA 8C104400	mov edx, 05-upxunpacked.44108C	44108C:"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 05-upxunpacked.43D068	
00440F8A	EB 18	jmp 05-upxunpacked.440FA4	
00440F8C	6A 00	push 0	
00440F8E	B9 80104400	mov ecx, 05-upxunpacked.441080	441080:"Beggar off!"
00440F93	BA 8C104400	mov edx, 05-upxunpacked.44108C	44108C:"wrong Serial,try again!"
00440F98	A1 442C4400	mov eax, dword ptr ds:[442C44]	
00440F9D	8B00	mov eax, dword ptr ds:[eax]	
00440F9F	E8 C4C0FFFF	call 05-upxunpacked.43D068	
00440FA4	33C0	xor eax, eax	

Call를 하고 jne를 하는 부분앞에 Break Point를 설정 하고 입력값을 넣어 작동하는지에 대해 살펴본다.■

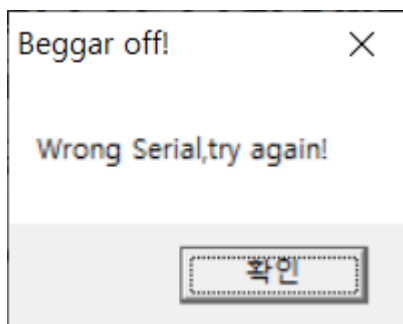
00440F39	E8 4AC1FFFF	call 05-upxunpacked.43D068	
00440F3E	8D55 FC	lea edx, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F41	8B83 C4020000	mov eax, dword ptr ds:[ebx+2C4]	eax: "unregistered..."
00440F47	E8 F4FEFDFF	call 05-upxunpacked.420E20	
00440F4C	8B45 FC	mov eax, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F4F	BA 14104400	mov edx, 05-upxunpacked.441014	edx: "Registered User", 441014:"Registered User"
00440F54	E8 F32BFCFF	call 05-upxunpacked.403B2C	
00440F59	75 51	jne 05-upxunpacked.440F8C	
00440F5B	8D55 FC	lea edx, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F5E	8B83 C8020000	mov eax, dword ptr ds:[ebx+2C8]	eax: "unregistered..."
00440F64	E8 D7FEFDFF	call 05-upxunpacked.420E20	
00440F69	8B45 FC	mov eax, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F6C	BA 2C104400	mov edx, 05-upxunpacked.44102C	44102C:"GFX-754-IER-954"
00440F71	E8 D62BFCFF	call 05-upxunpacked.403B2C	
00440F76	75 1A	jne 05-upxunpacked.440F72	
00440F78	6A 00	push 0	
00440F7A	B9 3C104400	mov ecx, 05-upxunpacked.44103C	44103C:"CrackMe cracked successfully"
00440F7F	BA 5C104400	mov edx, 05-upxunpacked.44105C	edx: "Registered User", 44105C:"Congrats! You cracked this CrackMe!"
00440F84	A1 442C4400	mov eax, dword ptr ds:[442C44]	eax: "Registered User", 44105C:"Congrats! You cracked this CrackMe!"
00440F89	8B00	mov eax, dword ptr ds:[eax]	eax: "unregistered..."

첫번째에 BreakPoint에서 그전에 입력을 했던 name 값을 eax에 가지고 mov를 통해 name으로 추정되는 문자열을 EDX로 가져오는 것 알수 있다.■

이때 진행을 해서 ZF 플래그가 어떻게 변화하는지를 본다.■

00440F34	E8 F32BFCFF	call 05-upxunpacked.403B2C	
00440F39	75 51	jne 05-upxunpacked.440F8C	
00440F3B	8D55 FC	lea edx, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F3E	8B83 C8020000	mov eax, dword ptr ds:[ebx+2C8]	
00440F44	E8 D7FEFDFF	call 05-upxunpacked.420E20	
00440F49	8B45 FC	mov eax, dword ptr ss:[ebp-4]	[ebp-4]: "unregistered..."
00440F4C	BA 2C104400	mov edx, 05-upxunpacked.44102C	44102C:"GFX-754-IER-954"
00440F51	E8 D62BFCFF	call 05-upxunpacked.403B2C	
00440F56	75 1A	jne 05-upxunpacked.440F72	
00440F58	6A 00	push 0	
00440F5A	B9 3C104400	mov ecx, 05-upxunpacked.44103C	44103C:"CrackMe cracked successfully"
00440F5F	BA 5C104400	mov edx, 05-upxunpacked.44105C	44105C:"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 05-upxunpacked.43D068	
00440F70	EB 32	jmp 05-upxunpacked.440FA4	
00440F72	6A 00	push 0	
00440F74	B9 80104400	mov ecx, 05-upxunpacked.441080	441080:"Beggar off!"
00440F79	BA 8C104400	mov edx, 05-upxunpacked.44108C	44108C:"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 05-upxunpacked.43D068	
00440F8A	EB 18	jmp 05-upxunpacked.440FA4	
00440F8C	6A 00	push 0	
00440F8E	B9 80104400	mov ecx, 05-upxunpacked.441080	441080:"Beggar off!"
00440F93	BA 8C104400	mov edx, 05-upxunpacked.44108C	44108C:"wrong Serial,try again!"
00440F98	A1 442C4400	mov eax, dword ptr ds:[442C44]	
00440F9D	8B00	mov eax, dword ptr ds:[eax]	
00440F9F	E8 C4C0FFFF	call 05-upxunpacked.43D068	

위와 같이 ZF 플래그가 0으로 선언되어 jne를 통해 틀렸다는 문자열이 있는곳으로 점프하는 것을 볼수 있고 또한 계속 실행을 해보면 프로그램에서도 틀렸다는 문자열이 뜨는 것을 볼수가 있다.■



이제 name으로 추정되는 값을 넣어서 정상적으로 지나가는지 확인을 해본다.■

00440F39	BA 14104400	mov ecx,05-upxunpacked.441014	441014: Registered user	EAX 00000000
00440F3A	E8 F32BFCFF	call 05-upxunpacked.403B2C		EBX 021E24EC
00440F3B	75 51	jne 05-upxunpacked.440F8C		ECX 00720000
00440F3C	8055 FC	lea edx,dword ptr ds:[ebp-4]	[ebp-4]: "Registered user"	EDX 00000001
00440F3D	8B83 C8020000	mov eax,dword ptr ds:[ebp+2C8]		EBP 0019F870
00440F3E	E8 D7FEFFFF	call 05-upxunpacked.420E20		ESP 0019F85C
00440F3F	8B45 FC	mov eax,dword ptr ds:[ebp-4]	[ebp-4]: "Registered user"	ESI 021E936C
00440F40	BA 2C104400	mov edx,05-upxunpacked.44102C	44102C: "GFX-754-IER-954"	EDI 00000015
00440F41	E8 D62BFCFF	call 05-upxunpacked.403B2C		EIP 00440F39
00440F42	75 1A	jne 05-upxunpacked.440F72		EFLAGS 00000246
00440F43	6A 00	push 0		ZE 1 PF 1 AF 0
00440F44	B9 3C104400	mov ecx,05-upxunpacked.44103C	44103C: "CrackMe cracked successfully"	OF 0 SF 0 DF 0
00440F45	BA 5C104400	mov edx,05-upxunpacked.44105C	44105C: "Congrats! You cracked this CrackMe!"	CF 0 TF 0 IF 1
00440F46	A1 442C4400	mov eax,dword ptr ds:[442C44]		LastError 00000000
00440F47	8B00	mov eax,dword ptr ds:[eax]		LastStatus C0000034
00440F48	E8 F8C0FFFF	call 05-upxunpacked.43D068		GS 002B FS 0053
00440F49	EB 32	jmp 05-upxunpacked.440FA4		ES 002B DS 002B
00440F4A	6A 00	push 0		CS 0023 SS 002B
00440F4B	B9 80104400	mov ecx,05-upxunpacked.441080	441080: "Begggar off!"	
00440F4C	BA 5C104400	mov edx,05-upxunpacked.44108C	44108C: "wrong Serial,try again!"	
00440F4D	A1 442C4400	mov eax,dword ptr ds:[442C44]		
00440F4E	8B00	mov eax,dword ptr ds:[eax]		
00440F4F	E8 DEC0FFFF	call 05-upxunpacked.43D068		
00440F50	EB 18	jmp 05-upxunpacked.440FA4		
00440F51	6A 00	push 0		
00440F52	B9 80104400	mov ecx,05-upxunpacked.441080	441080: "Begggar off!"	

이번에는 ZF 플래그가 1로 되어 jne가 작동하지 않고 넘어가는 것을 볼수 있다.❏

00440F39	E8 F32BFCFF	call 05-upxunpacked.403B2C		EAX 021E7FFC
00440F3A	75 51	jne 05-upxunpacked.440F8C		EBX 021E24EC
00440F3B	8055 FC	lea edx,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	ECX D0938759
00440F3C	8B83 C8020000	mov eax,dword ptr ds:[ebp+2C8]	eax: "754-GFX-IER-954"	EDX 0044102C
00440F3D	E8 D7FEFFFF	call 05-upxunpacked.420E20		EBP 0019F870
00440F3E	8B45 FC	mov eax,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	ESP 0019F85C
00440F3F	BA 2C104400	mov edx,05-upxunpacked.44102C	44102C: "GFX-754-IER-954"	ESI 021E936C
00440F40	E8 D62BFCFF	call 05-upxunpacked.403B2C		EDI 00000015
00440F41	75 1A	jne 05-upxunpacked.440F72		EIP 00440F51
00440F42	6A 00	push 0		EFLAGS 00000202
00440F43	B9 3C104400	mov ecx,05-upxunpacked.44103C	44103C: "CrackMe cracked successfully"	ZF 0 PF 0 AF 0
00440F44	BA 5C104400	mov edx,05-upxunpacked.44105C	edx: "GFX-754-IER-954", 44105C: "Congrats! You cracked this CrackMe!"	OF 0 SF 0 DF 0
00440F45	A1 442C4400	mov eax,dword ptr ds:[442C44]	eax: "754-GFX-IER-954"	CF 0 TF 0 IF 1
00440F46	8B00	mov eax,dword ptr ds:[eax]		LastError 00000000 (ERROR_SUCCESS)
00440F47	E8 F8C0FFFF	call 05-upxunpacked.43D068		LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)
00440F48	EB 32	jmp 05-upxunpacked.440FA4		
00440F49	6A 00	push 0		
00440F4A	B9 80104400	mov ecx,05-upxunpacked.441080	441080: "Begggar off!"	
00440F4B	BA 5C104400	mov edx,05-upxunpacked.44108C	edx: "GFX-754-IER-954", 44108C: "wrong Serial,try again!"	
00440F4C	A1 442C4400	mov eax,dword ptr ds:[442C44]	eax: "754-GFX-IER-954"	
00440F4D	8B00	mov eax,dword ptr ds:[eax]		
00440F4E	E8 DEC0FFFF	call 05-upxunpacked.43D068		

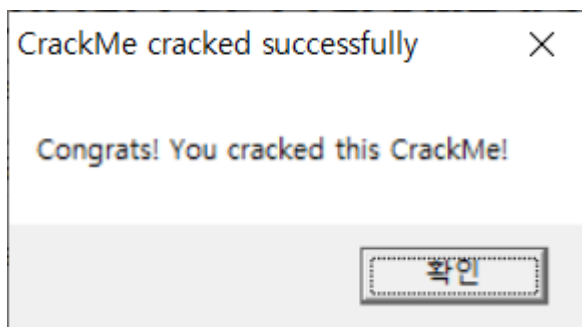
2번째 Break Point에서는 입력한 등록키를 eax로 불러오고 edx에 등록키로 의심이되는 키값을 가져와 call를 하고 있는 모습을 볼수 있다. 이때 그대로 실행을 해보고 ZF 플래그를 관찰 해본다.❏

00440F39	E8 F32BFCFF	call 05-upxunpacked.403B2C		ESP 0019F85C
00440F3A	75 51	jne 05-upxunpacked.440F8C		ESI 021E936C
00440F3B	8055 FC	lea edx,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	EDI 00000015
00440F3C	8B83 C8020000	mov eax,dword ptr ds:[ebp+2C8]		EIP 00440F56
00440F3D	E8 D7FEFFFF	call 05-upxunpacked.420E20		EFLAGS 00000285
00440F3E	8B45 FC	mov eax,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	ZF 0 PF 1 AF 0
00440F3F	BA 2C104400	mov edx,05-upxunpacked.44102C	44102C: "GFX-754-IER-954"	OF 0 SF 1 DF 0
00440F40	E8 D62BFCFF	call 05-upxunpacked.403B2C		CF 1 TF 0 IF 1
00440F41	75 1A	jne 05-upxunpacked.440F72		
00440F42	6A 00	push 0		
00440F43	B9 3C104400	mov ecx,05-upxunpacked.44103C	44103C: "CrackMe cracked successfully"	
00440F44	BA 5C104400	mov edx,05-upxunpacked.44105C	44105C: "Congrats! You cracked this CrackMe!"	
00440F45	A1 442C4400	mov eax,dword ptr ds:[442C44]		
00440F46	8B00	mov eax,dword ptr ds:[eax]		
00440F47	E8 F8C0FFFF	call 05-upxunpacked.43D068		
00440F48	EB 32	jmp 05-upxunpacked.440FA4		
00440F49	6A 00	push 0		
00440F4A	B9 80104400	mov ecx,05-upxunpacked.441080	441080: "Begggar off!"	

이때 ZF 플래그는 0으로 변하여 오류 메시지를 출력하는 곳으로 점프되는 것을 볼수 있다. 이번에는 등록키로 의심되는 키값을 입력해서 다시 시도 하여 본다.❏

00440F39	E8 F32BFCFF	call 05-upxunpacked.403B2C		EDX 00000001
00440F3A	75 51	jne 05-upxunpacked.440F8C		EBP 0019F870
00440F3B	8055 FC	lea edx,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	ESP 0019F85C
00440F3C	8B83 C8020000	mov eax,dword ptr ds:[ebp+2C8]		ESI 021E936C
00440F3D	E8 D7FEFFFF	call 05-upxunpacked.420E20		EDI 00000014
00440F3E	8B45 FC	mov eax,dword ptr ds:[ebp-4]	[ebp-4]: "754-GFX-IER-954"	EIP 00440F56
00440F3F	BA 2C104400	mov edx,05-upxunpacked.44102C	44102C: "GFX-754-IER-954"	EFLAGS 00000244
00440F40	E8 D62BFCFF	call 05-upxunpacked.403B2C		ZE 1 PF 1 AF 0
00440F41	75 1A	jne 05-upxunpacked.440F72		OF 0 SF 0 DF 0
00440F42	6A 00	push 0		CF 0 TF 0 IF 1
00440F43	B9 3C104400	mov ecx,05-upxunpacked.44103C	44103C: "CrackMe cracked successfully"	
00440F44	BA 5C104400	mov edx,05-upxunpacked.44105C	44105C: "Congrats! You cracked this CrackMe!"	
00440F45	A1 442C4400	mov eax,dword ptr ds:[442C44]		
00440F46	8B00	mov eax,dword ptr ds:[eax]		
00440F47	E8 F8C0FFFF	call 05-upxunpacked.43D068		
00440F48	EB 32	jmp 05-upxunpacked.440FA4		
00440F49	6A 00	push 0		
00440F4A	B9 80104400	mov ecx,05-upxunpacked.441080	441080: "Begggar off!"	
00440F4B	BA 5C104400	mov edx,05-upxunpacked.44108C	44108C: "wrong Serial,try again!"	
00440F4C	A1 442C4400	mov eax,dword ptr ds:[442C44]		

이번에는 ZF 플래그가 1로 되어 JMP를 하지 않고 넘어가는 모습과 성공적으로 Crack를 성공했다는 문자를 볼수 있다.❏



정답: GFX-754-IER-954