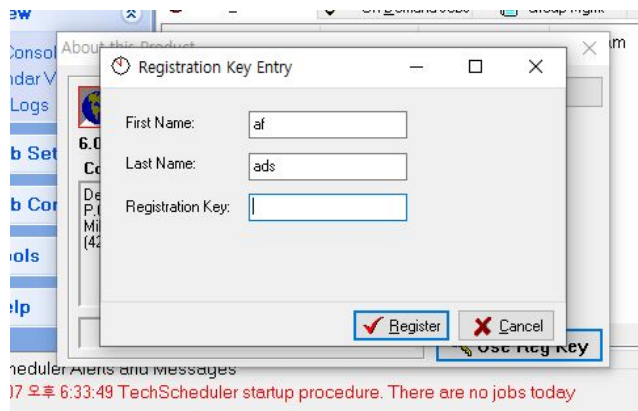
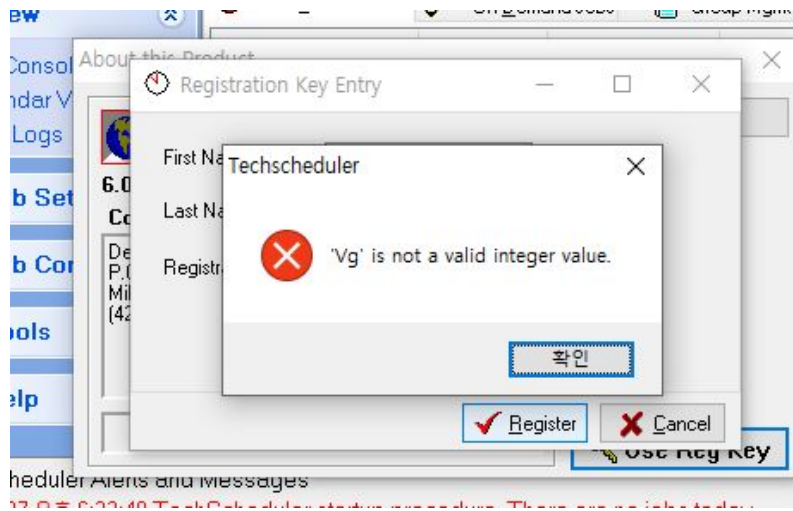


등록 키를 입력해주면, 오리지널 버전을 이용할 수 있다.

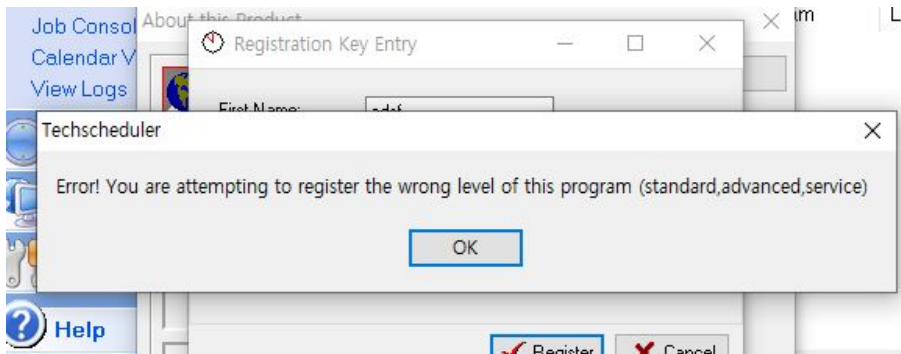
여느때와 다를거 없이 등록키를 입력해주는 것이 아닌 프로그램 자체를 우회하는 것이다.





아무 키를 입력하고, 등록을 누르면 이와 같은 에러가 뜬다. 문자열 검색기능을 이용해 해당 부분으로 이동한다.

Vg라는 값을 입력하면, 아래와 같은 문구가 뜬다. 아래 문구로 검색해본다.



004A55E1	. 8B95 A4FEFFFF	CALL Teksched.00405398	
004A55E7	. 58	MOV EDX,DWORD PTR SS:[EBP-15C]	
004A55E8	. E8 ABFD5FF	POP EAX	
004A55E9	. 74 19	CALL Teksched.00405398	
004A55EF	. 807D 08 00	JE SHORT Teksched.004A5608	
004A55F3	. 0F85 7D020000	CMP BYTE PTR SS:[EBP+8],0	
004A55F4	. B8 78594A00	JNZ Teksched.004A5876	
004A55FE	. E8 F53BF9FF	MOV EAX,Teksched.004A5978	ASCII "Error! You are attempting to regi
004A5603	. E9 6E020000	CALL Teksched.004391F8	
004A5608	. 66:BE 5802	JMP Teksched.004A5876	
004A560C	. 66:81FE BC02	MOV SI,258	
004A5611	. 76 19	CMP SI,2BC	
004A5613	. 807D 08 00	JBE SHORT Teksched.004A562C	
004A5617	. 0F85 59020000	CMP BYTE PTR SS:[EBP+8],0	
004A561D	. B8 E4594A00	JNZ Teksched.004A5876	
004A5622	. E8 D13BF9FF	MOV EAX,Teksched.004A59E4	ASCII "Error! You are attempting to regi
004A5627	. E9 4A020000	CALL Teksched.004391F8	
004A562C	. A1 BC5C5A00	JMP Teksched.004A5876	
		MOV EAX,DWORD PTR DS:[5A5C8C]	

이동하면 이렇게 두개의 문자열이 보인다. 그리고 분기문에 따라 호출되는 문자열도 달라진다.

아래로 조금 더 살펴보면,  
**Registration Key accepted**  
 문자열이 보인다. 그 주변 명령을 살펴본다.

004A5827	. 59	POP ECX	
004A5828	. 59	POP ECX	
004A5829	. 64:8910	MOV DWORD PTR FS:[EAX],EDX	
004A5831	. 68 41584A00	PUSH Teksched.004A5841	
004A5834	. 8B45 CC	MOV EAX,DWORD PTR SS:[EBP-34]	
004A5839	. E8 5BE8F5FF	CALL Teksched.00404094	
004A583A	. C3	RETN	
004A583F	. E9 E9EFF5FF	JMP Teksched.00404828	
004A5841	. EB F0	JMP SHORT Teksched.004A5831	
004A5845	. C645 F3 01	MOV BYTE PTR SS:[EBP-D],1	
004A5849	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A584E	. 75 0A	JNZ SHORT Teksched.004A5855	
004A5850	. B8 A8584A00	MOV EAX,Teksched.004A58A8	ASCII "Registration Key accepted!"
004A5855	. E8 A339F9FF	CALL Teksched.004391F8	
004A585A	. A1 E4535A00	MOV EAX,DWORD PTR DS:[5A53F4]	
004A585D	. C600 00	MOV BYTE PTR DS:[EAX],0	
004A585F	. EB 17	JMP SHORT Teksched.004A5876	
004A5863	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A5865	. 75 11	JNZ SHORT Teksched.004A5876	
004A5867	. 6A 30	PUSH 30	
004A586C	. E8 C829F6FF	CALL <JMP.&user32.MessageBeep>	[BeepType = MB_ICONEXCLAMATION MessageBeep
004A5871	. E8 CC5A4A00	MOV EAX,Teksched.004A5ACC	ASCII "Registration Key Failed!"
	. E8 8239F9FF	CALL Teksched.004391F8	

위에 비교문이 보이고 분기문도 보인다. 위에 또 살펴보니 해당 비교문에 점프하는 코드가 보인다.

4A592C를 살펴보면 4A5841을 PUSH하고 그다음 RETN 명령에 의해 unconditional jump를 한다.

004A55E1	. 8B95 A4FEFFFF	MOV EDX,DWORD PTR SS:[EBP-15C]	
004A55E7	. 58	POP EAX	
004A55E8	. E8 ABFDF5FF	CALL Teksched.004A5398	
004A55ED	.v74 19	JE SHORT Teksched.004A5608	
004A55EF	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A55F3	.v0F85 7D020000	JNZ Teksched.004A5876	
004A55F9	. B8 78534A00	MOV EAX,Teksched.004A5978	ASCII "Error! You are attempt
004A55FE	. E8 F53BF9FF	CALL Teksched.004391F8	
004A5603	.vE9 43020000	JMP Teksched.004A584B	
004A5608	> 66:BE 5802	MOV SI,258	
004A560C	. 66:81FE BC02	CMP SI,2BC	
004A5611	.v76 19	JBE SHORT Teksched.004A562C	
004A5613	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A5617	.v0F85 59020000	JNZ Teksched.004A5876	
004A561D	. B8 E4534A00	MOV EAX,Teksched.004A59E4	ASCII "Error! You are attempt
004A5622	. E8 D13BF9FF	CALL Teksched.004391F8	
004A5627	.vE9 4A020000	JMP Teksched.004A5876	
004A562C	> A1 BC5C5A00	MOV EAX,DWORD PTR DS:[5A5C5A00]	
004A5631	. 66:8B00	MOV AX,WORD PTR DS:[EAX]	
004A5634	. 66:F7EE	IMUL SI	
004A5637	. 8BF0	MOV ESI,EAX	
004A563A	. 8B 00 4F 00 00	MOV EAX,4F0000	

위에 JMP 4A4876 부분을

4A584B로 바꿔 등록 성공 메시지를  
뜨게 할 수 있다. 하지만 이 방식은  
비효율적이다. 매번 아무키로 등록을  
해야 정식 버전을 사용할 수 있기  
때문이다.

우회 목적은 프로그램을 키자마자  
정식버전으로 사용할 수 있게 하기  
위함이다.

004A539E	. 8B55 BC	MOV EDX, DWORD PTR SS:[EBP-44]
004A53A1	. 8D45 D8	LEA EAX, DWORD PTR SS:[EBP-28]
004A53A4	. E8 ABFEF5FF	CALL Teksched.00405254
004A53A9	✓ EB 19	JMP SHORT Teksched.004A53C4
004A53AB	> 807D 08 00	CMP BYTE PTR SS:[EBP+8], 0
004A53AF	✓ 0F85 C1040000	JNZ Teksched.004A5376
004A53B5	. B8 30524A00	MOV EAX, Teksched.004A5930
004A53BA	. E8 393EF9FF	CALL Teksched.004391F8
004A53BF	✓ E9 82040000	JMP Teksched.004A5376
004A53C4	> 8B45 F4	MOV EAX, DWORD PTR SS:[EBP-C]
004A53C7	. E8 80FEF5FF	CALL Teksched.0040524C
004A53CC	. 48	DEC EAX
004A53CD	✓ 7D 19	JGE SHORT Teksched.004A53E8
004A53CF	. 807D 08 00	CMP BYTE PTR SS:[EBP+8], 0
004A53D3	✓ 0F85 9D040000	JNZ Teksched.004A5376
004A53D9	. B8 58594A00	MOV EAX, Teksched.004A5958
004A53DE	. E8 153EF9FF	CALL Teksched.004391F8
004A53E3	✓ E9 8E040000	JMP Teksched.004A5376
004A53E8	> 8D95 BCFEFFFF	LEA EDX, DWORD PTR SS:[EBP-144]
004A53EE	. 8B45 F4	MOV EAX, DWORD PTR SS:[EBP-C]
004A53F1	. E8 D6EFFFFF	CALL Teksched.004A43CC
004A53F6	. 8D95 BCFEFFFF	LEA EDX, DWORD PTR SS:[EBP-144]

ASCII "Enter a Last Name value now.."

ASCII "Enter a Key value now.."

4A592C주소에서 PUSH 4A5941  
후 RETN함으로써 해당 주소로  
넘어오게 된다.

분석하다 보면 다음과 같은  
문자열을 볼 수 있다.

이 문자열은 사용자가 **Last name**  
부분과 **key**를 입력하지 않았을 때  
나타나는 부분이다.

분명 이 문자열을 호출하는  
부분이 있을 것이다.

004A5394	. 8B00	Mov EAX, EAX	
004A5396	. 8D45 BC	LEA EAX, DWORD PTR SS:[EBP-44]	
004A5399	. E8 D6FDF5FF	CALL Teksched.00405174	
004A539E	. 8B55 BC	MOV EDX, DWORD PTR SS:[EBP-44]	
004A53A1	. 8D45 D8	LEA EAX, DWORD PTR SS:[EBP-28]	
004A53A4	. E8 ABFEF5FF	CALL Teksched.00405254	
004A53A9	. vEB 19	JMP SHORT Teksched.004A53C4	
004A53AB	> 807D 08 00	CMP BYTE PTR SS:[EBP+8], 0	
004A53AF	. v0F85 C1040000	JNZ Teksched.004A5876	
004A53B5	. B8 30594A00	MOV EAX, Teksched.004A5930	ASCII "Enter a Last Name value now.."
004A53BA	. E8 393EF9FF	CALL Teksched.004391F8	
004A53BF	. vE9 B2040000	JMP Teksched.004A5876	
004A53C4	> 8B45 F4	MOV EAX, DWORD PTR SS:[EBP-C]	
004A53C7	. E8 80FEF5FF	CALL Teksched.0040524C	
004A53CC	. 48	DEC EAX	
004A53CD	. v7D 19	JGE SHORT Teksched.004A53E8	

이 부분을 살펴보면 4A52E3  
부분에서 호출하는 것을 볼 수  
있다.

004A5408	. 8B45 DC	Jump from 004A52E3
----------	-----------	--------------------

해당 부분을 보면 First Name을  
입력하지 않았을 시 나타나는  
문자열이다.

004A52BE	. vEB 19	JMP SHORT Teksched.004A52D9	
004A52C0	> 807D 08 00	CMP BYTE PTR SS:[EBP+8], 0	
004A52C4	. v0F85 AC050000	JNZ Teksched.004A5876	
004A52CA	. B8 08594A00	MOV EAX, Teksched.004A5908	ASCII "Enter a First Name value now.."
004A52CF	. E8 243FF9FF	CALL Teksched.004391F8	
004A52D4	. vE9 9D050000	JMP Teksched.004A5876	
004A52D9	> 8B45 E8	MOV EAX, DWORD PTR SS:[EBP-18]	
004A52DC	. E8 6BFFF5FF	CALL Teksched.0040524C	
004A52E1	. 85C0	TEST EAX, EAX	
004A52E3	. v0F8E C2000000	JLE Teksched.004A53AB	
004A52E9	. 66:BF 0100	MOV DI, 1	
004A52ED	. 8B1D 64575A00	MOV EBX, DWORD PTR DS:[5A5764]	Teksched.005A449C
004A52F3	. 43	INC EBX	
004A52F4	> 8B45 E8	MOV EAX, DWORD PTR SS:[EBP-18]	



004A51B7	. 0000 F0	MOV EAX,DWORD PTR SS:[EBP-04]	
004A51BC	. E8 63FEF5FF	CALL Teksched.00405024	
004A51C1	. 33C0	XOR EAX,EAX	
004A51C3	. 5A	POP EDX	
004A51C4	. 59	POP ECX	
004A51C5	. 59	POP ECX	
004A51C6	. 64:8910	MOV DWORD PTR FS:[EAX],EDX	
004A51C9	. 68 DE514A00	PUSH Teksched.004A51DE	
004A51CE	> 8B45 04	MOV EAX,DWORD PTR SS:[EBP-2C]	
004A51D1	. E8 BEEEF5FF	CALL Teksched.00404094	
004A51D6	. C3	RETN	
004A51D7	. ^E9 4CF6F5FF	JMP Teksched.00404828	
004A51DC	. ^EB F0	JMP SHORT Teksched.004A51CE	
004A51DE	. 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	
004A51E1	. E8 6600F6FF	CALL Teksched.0040524C	
004A51E6	. 85C0	TEST EAX,EAX	
004A51E8	. ^0F8E D2000000	JLE Teksched.004A52C0	
004A51EE	. 66:BF 0100	MOV DI,1	
004A51F2	. 8B1D 64575A00	MOV EBX,DWORD PTR DS:[5A5764]	Teksched.005A449C
004A51F8	. 43	INC EBX	
004A51F9	> 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	
004A51FC	. 0000	MOV AL,BYTE PTR DS:[EAX]	

하나 하나 위로 올라가보면서  
분기문을 호출하는 부분을 꼭  
따라가보면 해당 부분이 나온다.

PUSH 4A51DE 을 하고, RETN  
함으로써 해당 주소로 점프하는  
코드임을 알 수 있다.

키가 입력되지 않았을 경우  
점프하는 부분 다음 주소에 bp를  
걸고 살펴본다. 왜냐하면 해당  
부분 이후에 분명 아까 키 등록에  
실패하였을 경우에 뜨는 문자열에  
점프하는 부분이 있을것이다.

004A53C4	/ 0045 F4	MOV EAX,DWORD PTR SS:[EBP-04]	
004A53C7	. E8 80FEF5FF	CALL Teksched.0040524C	
004A53CC	. 48	DEC EAX	
004A53CD	. ^7D 19	JGE SHORT Teksched.004A53E8	
004A53CF	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A53D3	. ^0F85 90040000	JNZ Teksched.004A5876	
004A53D9	. B8 58594A00	MOV EAX,Teksched.004A5958	ASCII "Enter a Key value now.."
004A53DE	. E8 153EF9FF	CALL Teksched.004391F8	
004A53E3	. ^E9 8E040000	JMP Teksched.004A5876	
004A53E8	> 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	
004A53EE	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
004A53F1	. E8 D6EFFFFF	CALL Teksched.004A43CC	
004A53F6	. 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	
004A53FC	. 8D45 DC	LEA EAX,DWORD PTR SS:[EBP-24]	
004A53FF	. E8 ECFDF5FF	CALL Teksched.004051F0	
004A5404	. 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	

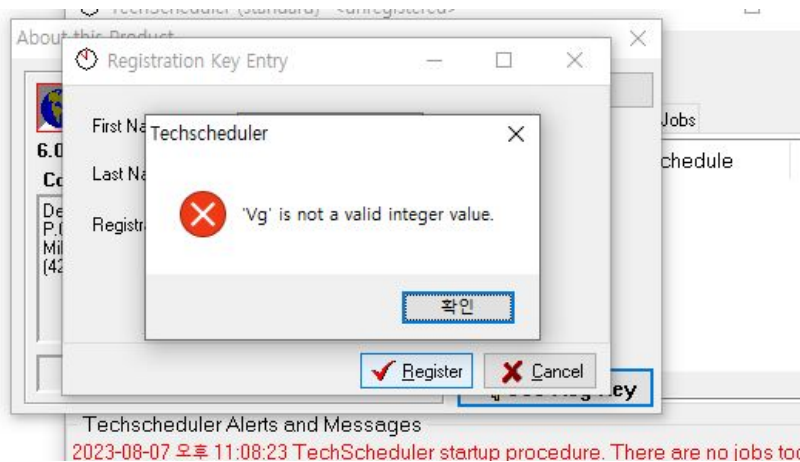
```

004A53EE > 8D95 BCFFFFFF LEA EDX,DWORD PTR SS:[EBP-144]
004A53F1 . 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
004A53F6 . E8 D6FFFFFF CALL Teksched.004A43CC
004A53FC . 8D95 BCFFFFFF LEA EDX,DWORD PTR SS:[EBP-144]
004A53FF . 8D45 DC LEA EAX,DWORD PTR SS:[EBP-24]
004A5404 . E8 ECFDF5FF CALL Teksched.004051F0
004A5407 . 8D45 F4 LEA EAX,DWORD PTR SS:[EBP-C]
004A5408 . 50 PUSH EAX
004A540B . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A5410 . E8 3CFEF5FF CALL Teksched.0040524C
004A5412 . 8BC8 MOV ECX,EAX
004A5415 . 83E9 05 SUB ECX,5
004A5418 . BA 01000000 MOV EDI,1
004A541A . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A541D . E8 8A00F6FF CALL Teksched.004054AC
004A5422 . 8D45 E4 LEA EAX,DWORD PTR SS:[EBP-1C]
004A5425 . 50 PUSH EAX
004A5428 . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A542B . E8 1EFEF5FF CALL Teksched.0040524C
004A542E . 8BD0 MOV EDI,EAX
004A5431 . 83EA 04 SUB EDI,4
004A5434 . B9 02000000 MOV ECX,2
004A5437 . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A543A . E8 6C00F6FF CALL Teksched.004054AC
004A543D . 8D45 E0 LEA EAX,DWORD PTR SS:[EBP-20]
004A5440 . 50 PUSH EAX
004A5443 . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A5446 . E8 00FEF5FF CALL Teksched.0040524C
004A5449 . 8BD0 MOV EDI,EAX
004A544C . 83EA 02 SUB EDI,2
004A544F . B9 03000000 MOV ECX,3
004A5452 . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
004A5455 . E8 4E00F6FF CALL Teksched.004054AC
004A5458 . 8B45 E0 MOV EAX,DWORD PTR SS:[EBP-20]
004A545B . E8 0A4CF6FF CALL Teksched.0040A070
004A545E . 8D45 DC LEA EAX,DWORD PTR SS:[EBP-24]
004A5461 . E8 1EFBF5FF CALL Teksched.00404F8C
004A5464 . 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
004A5467 . E8 D6FDF5FF CALL Teksched.0040524C
004A546A . 66:85C0 TEST AX,AX
004A546D . 74 0F86 23010000 JBE Teksched.004A55A2
004A5470 . 66:8945 02 MOV WORD PTR SS:[EBP-2F],0x

```

bp걸었던 부분 다음부터 다양한 함수를 호출하는데, 그 이후에 나타나는 분기문에 bp를 하나 더 걸고 분석해본다.





그다음 실행해보면 이런 유효한 정수값이 아니라는 문자열과 함께 오류가 뜬다.

아무래도 그 사이에 있는 함수 부분에서 오류를 내뱉는 것같아 하나 하나 따라가면서 분석한다.

778C4EA7	74 0E	JE SHORT ntdll.778C4EB7	
778C4EA9	8B00 00699777	MOV ECX,DWORD PTR DS:[779769A0]	
778C4EAF	FF15 E0919777	CALL DWORD PTR DS:[779791E0]	ntdll.RtlDebugPrintTimes
778C4EB5	FFE1	JMP ECX	
778C4EB7	FC	CLD	
778C4EB8	8B4C24 04	MOV ECX,DWORD PTR SS:[ESP+4]	
778C4EBC	8B1C24	MOV EBX,DWORD PTR SS:[ESP]	
778C4EBF	51	PUSH ECX	
778C4EC0	53	PUSH EBX	
778C4EC1	E8 F640FFFF	CALL ntdll.778B8FBC	
778C4EC6	0AC0	OR AL,AL	

하나 하나 따라가다가 어느 순간  
ntdll로 진입하는걸 볼 수 있다.

‘-’를 눌러 어디서 호출됐는지 보면  
해당 부분에서 호출하는걸 알 수  
있다.

004A544E	. 83EA 02	SUB EDX,2	
004A5451	. B9 03000000	MOV ECX,3	
004A5456	. 8B45 DC	MOV EAX,DWORD PTR SS:[EBP-24]	
004A5459	. E8 4E00F6FF	CALL Tekshed.004054AC	
004A545E	. 8B45 E0	MOV EAX,DWORD PTR SS:[EBP-20]	
004A5461	. E8 0A4CF6FF	CALL Tekshed.0040A070	
004A5466	. 8D45 DC	LEA EAX,DWORD PTR SS:[EBP-24]	
004A5469	. E8 1EFBF5FF	CALL Tekshed.00404F8C	
004A546E	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
004A5471	. E8 D6FDF5FF	CALL Tekshed.0040524C	
004A5476	. 66:85C0	TEST AX,AX	
004A5479	. 0F86 23010000	JBE Tekshed.004A55A2	
004A547F	. 66:8945 D2	MOV WORD PTR SS:[EBP-2E],AX	

004A544E	. 83EA 02	SUB EDX,2
004A5451	. B9 03000000	MOV ECX,3
004A5456	. 8B45 DC	MOV EAX,DWORD PTR SS:[EBP-24]
004A5459	. E8 4E00F6FF	CALL Teksched.004054AC
004A545E	. 8B45 E0	MOV EAX,DWORD PTR SS:[EBP-20]
004A5461	. E8 0A4CF6FF	CALL Teksched.0040A070
004A5466	. 8D45 DC	LEA EAX,DWORD PTR SS:[EBP-24]
004A5469	. E8 1EFBF5FF	CALL Teksched.00404F8C
004A546E	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]
004A5471	. E8 D6FDF5FF	CALL Teksched.0040524C
004A5476	. 66:85C0	TEST AX,AX
004A5479	. 74F86 23010000	JBE Teksched.004A55A2
004A547F	. 66:8945 D2	MOV WORD PTR SS:[EBP-2E],AX

분기 하는걸 막기 위해 해당 부분을  
NOP으로 패치한다.

그리고 계속 실행한다.

하나하나 분석하다보면 분기문이  
많이 나오는데, 에러나오는  
분기문을 모두 만나오게 zero  
flag를 조절해가면서 분석했다.

004A544E	. 83EA 02	SUB EDX,2
004A5451	. B9 03000000	MOV ECX,3
004A5456	. 8B45 DC	MOV EAX,DWORD PTR SS:[EBP-24]
004A5459	. E8 4E00F6FF	CALL Teksched.004054AC
004A545E	. 8B45 E0	MOV EAX,DWORD PTR SS:[EBP-20]
004A5461	. 90	NOP
004A5462	. 90	NOP
004A5463	. 90	NOP
004A5464	. 90	NOP
004A5465	. 90	NOP
004A5466	. 8D45 DC	LEA EAX,DWORD PTR SS:[EBP-24]
004A5469	. E8 1EFBF5FF	CALL Teksched.00404F8C
004A546E	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]
004A5471	. E8 D6FDF5FF	CALL Teksched.0040524C
004A5476	. 66:85C0	TEST AX,AX
004A5479	. 74F86 23010000	JBE Teksched.004A55A2
004A547F	. 66:8945 D2	MOV WORD PTR SS:[EBP-2E],AX
004A5483	. 66:BF 0100	MOV DI,1
004A5487	. 66:BE 0100	MOV SI,1
004A548B	. 8B1D 64575A00	MOV EBX,DWORD PTR DS:[5A5764]

Tek

004A5663	. E8 0884FFFF	CALL Teksched.0049DA70	
004A5668	. 8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]	
004A566B	. 8B55 E8	MOV EDX,DWORD PTR SS:[EBP-18]	
004A566E	. E8 E1FBF5FF	CALL Teksched.00405254	
004A5673	. 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	
004A5676	. 8B55 DC	MOV EDX,DWORD PTR SS:[EBP-24]	
004A5679	. E8 1AFDF5FF	CALL Teksched.00405398	
004A567E	. 0F85 DB010000	JNZ Teksched.004A585F	
004A5684	. 8D45 D8	LEA EAX,DWORD PTR SS:[EBP-28]	
004A5687	. BA 345A4A00	MOV EDX,Teksched.004A5A34	
004A568C	. E8 C3FBF5FF	CALL Teksched.00405254	
004A5691	. A1 BC5C5A00	MOV EAX,DWORD PTR DS:[5A5CBC]	
004A5696	. 66:6930 BC02	IMUL SI,WORD PTR DS:[EAX],2BC	
004A569B	. 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	
004A56A1	. 0FB7C6	MOVZX EAX,SI	

ASCII "GJJ"

그리고 내려가다 보면 해당 분기문이 나온는데, 4A585F 부분은 등록 실패 에러가 나오는 부분이므로, zero flag를 임의로 변경해 점프 못하도록 한다.

004A570A	. 8B45 D8	MOV EAX,DWORD PTR SS:[EBP-28]	
004A570D	. E8 82F0FFFF	CALL Teksched.004A4794	
004A5712	. 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	
004A5718	. 8D85 9CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-164]	
004A571E	. E8 CDFAF5FF	CALL Teksched.004051F0	
004A5723	. 8B85 9CFEFFFF	MOV EAX,DWORD PTR SS:[EBP-164]	
004A5729	. 50	PUSH EAX	
004A572A	. B9 405A4A00	MOV ECX,Teksched.004A5A40	
004A572F	. BA 545A4A00	MOV EDX,Teksched.004A5A54	
004A5734	. 8B45 CC	MOV EAX,DWORD PTR SS:[EBP-34]	
004A5737	. E8 1415FFFF	CALL Teksched.00496C50	
004A573C	. 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	
004A5742	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004A5745	. E8 4AF0FFFF	CALL Teksched.004A4794	
004A574B	. 8D95 BCFEFFFF	LEA EDX,DWORD PTR SS:[EBP-144]	

ASCII "sRegStat"  
ASCII "Config"

계속 분석해보면 아래와 같이 등록과 관련된 함수를 호출하는 것처럼 보인다. PUSH EAX를 하고, 스택창을 봤더니 어떤 값이 저장되어있다.

아마 해당 값이 레지스터 키 값인 걸로 보인다. 키를 등록하는것이 아닌 완전 우회하는것이 목적이기 때문에 안쓴다.

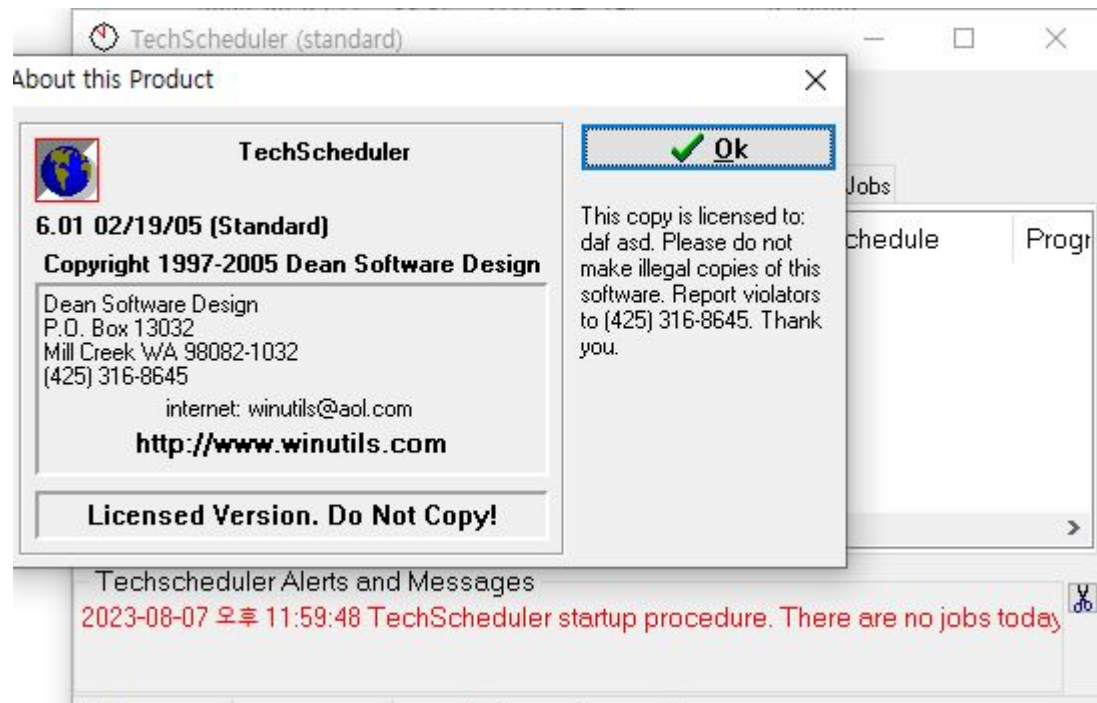
0019DF6C	02479DC8	ASCII "000068787476736903191E621D070000"
0019DF70	0019DF7C	Pointer to next SEH record
0019DF74	004A583A	SE handler
0019DF78	0019E108	
0019DF7C	0019E114	Pointer to next SEH record
0019DF80	004A58BB	SE handler
0019DF84	0019E108	
0019DF88	0019E2B4	
0019DF8C	004A47F0	Teksched.004A47F0

004A581F	. E8 2000FFFF	CALL Teksched.00495844	
004A5824	. 33C0	XOR EAX,EAX	
004A5826	. 5A	POP EDX	
004A5827	. 59	POP ECX	
004A5828	. 59	POP ECX	
004A5829	. 64:8910	MOV DWORD PTR FS:[EAX],EDX	
004A582C	. 68 41584A00	PUSH Teksched.004A5841	
004A5831	> 8B45 CC	MOV EAX,DWORD PTR SS:[EBP-34]	
004A5834	. E8 5BE8F5FF	CALL Teksched.00404094	
004A5839	. C3	RETN	
004A583A	. ^E9 E9EFF5FF	JMP Teksched.00404828	
004A583F	. ^EB F0	JMP SHORT Teksched.004A5831	
004A5841	. C645 F3 01	MOV BYTE PTR SS:[EBP-D],1	
004A5845	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A5849	. ^75 0A	JNZ SHORT Teksched.004A5855	
004A584B	. B8 A85A4A00	MOV EAX,Teksched.004A5A08	ASCII "Registration Key accepted!"
004A5850	. E8 A339F9FF	CALL Teksched.004391F8	
004A5855	> A1 F4535A00	MOV EAX,DWORD PTR DS:[5A53F4]	

내려가다 보면 아까와 같이 등록 성공/실패 메시지를 호출하는 부분으로 이동하는 코드를 볼 수 있다.

여태까지 패치한 결과를 보아 아까는 오류메시지로 분기했지만 이번에는 등록 성공 메시지로 분기하는걸 볼 수 있다.

004A5834	. E8 5BE8F5FF	CALL Teksched.00404094	
004A5839	. C3	RETN	
004A583A	. ^E9 E9EFF5FF	JMP Teksched.00404828	
004A583F	. ^EB F0	JMP SHORT Teksched.004A5831	
004A5841	. C645 F3 01	MOV BYTE PTR SS:[EBP-D],1	
004A5845	. 807D 08 00	CMP BYTE PTR SS:[EBP+8],0	
004A5849	. ^75 0A	JNZ SHORT Teksched.004A5855	
004A584B	. B8 A85A4A00	MOV EAX,Teksched.004A5A08	ASCII "Registration Key accepted!"
004A5850	. E8 A339F9FF	CALL Teksched.004391F8	
004A5855	> A1 F4535A00	MOV EAX,DWORD PTR DS:[5A53F4]	
004A585A	. C600 00	MOV BYTE PTR DS:[EAX],0	
004A585D	. ^EB 17	JMP SHORT Teksched.004A5876	
004A585F	> A07D 08 00	CMP BYTE PTR SS:[FAP+8],0	



패치한 프로그램을 살펴보면 실행하자  
마자 바로 원본 버전으로 실행하는걸  
볼 수 있다.