

REPORT:

코드엔진 Basic

RCE 05 Writeup

COLONY
1824275 정상지

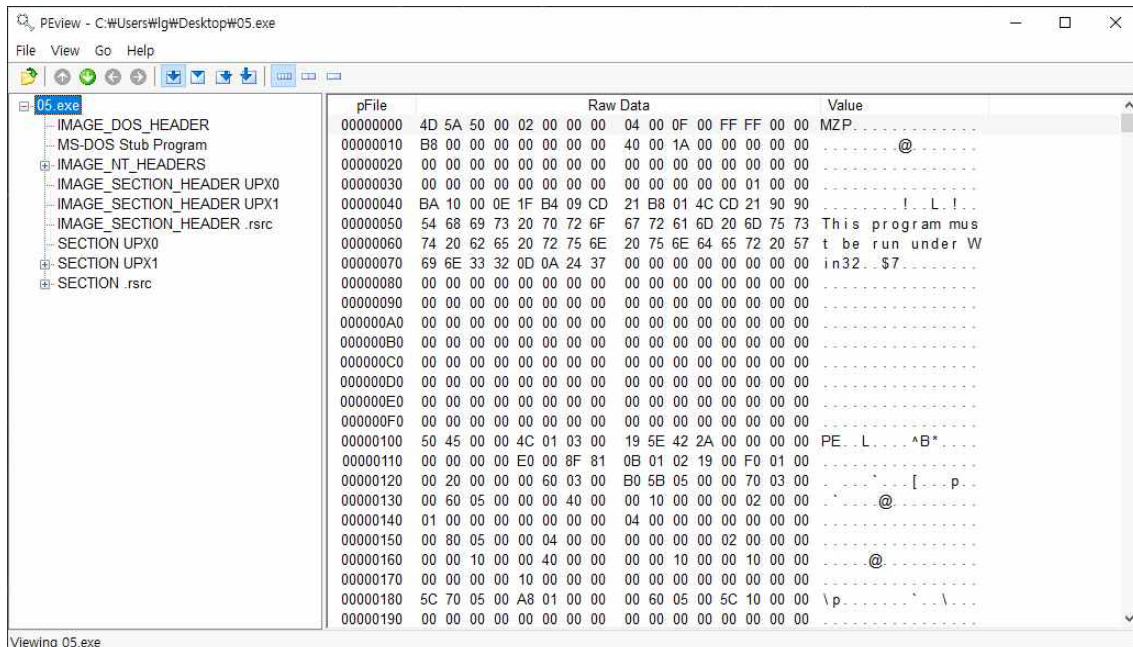
2021.05.30

이 프로그램의 등록키는 무엇인가



Register now !를 클릭했을 때 프로그램 반응

해당 파일을 PView로 보았을 때 upx로 패키징이 되어있는 것을 확인할 수 있다



upx를 통해 언패킹을 진행한 후 PE구조 확인

PEView - C:\Users\Wlg\Desktop\05_unp.exe			
File View Go Help			
05_unp.exe	pFile	Raw Data	Value
IMAGE_DOS_HEADER	00000000	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00	MZP.....
MS-DOS Stub Program	00000010	B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00@.....
IMAGE_NT_HEADERS	00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER CODE	00000030	00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
IMAGE_SECTION_HEADER DATA	00000040	BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90!..L!..
IMAGE_SECTION_HEADER BSS	00000050	54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73	This program mus
IMAGE_SECTION_HEADER .idata	00000060	74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57	t be run under W
IMAGE_SECTION_HEADER .tls	00000070	69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00	in32..\$7.....
IMAGE_SECTION_HEADER .rdata	00000080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER .reloc	00000090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER .rsrc	000000A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION CODE	000000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION DATA	000000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION BSS	000000D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION .idata	000000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION .tls	000000F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SECTION .rdata	00000100	50 45 00 00 4C 01 08 00 19 5E 42 2A 00 00 00 00	PE...L...^B*...
SECTION .reloc	00000110	00 00 00 00 E0 00 8F 81 0B 01 02 19 00 04 04 00
SECTION .rsrc	00000120	00 C8 00 00 00 00 00 00 70 12 04 00 00 10 00 00p.....
	00000130	00 20 04 00 00 00 40 00 00 10 00 00 00 02 00 00@.....
	00000140	01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
	00000150	00 30 05 00 00 10 00 00 00 00 00 02 00 00 00 000.....
	00000160	00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 00@.....
	00000170	00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
	00000180	00 04 04 00 8C 1D 00 00 00 D0 04 00 00 52 00 00@.....R..
	00000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Viewing 05_unp.exe

언패킹한 파일을 디버깅

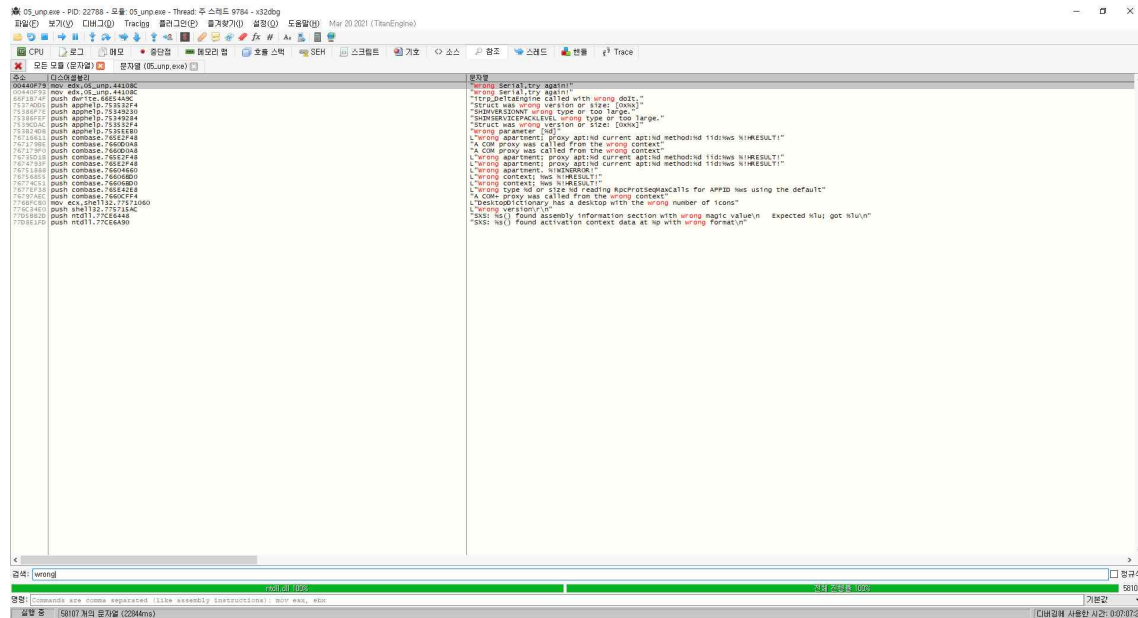
05_unp.exe - PID: 32788 - 모듈: 05_unp.exe - Thread: 주 스택도 9794 - x32dbg

파일(0) 보기(0) 디버그(0) Tracings 출력(0) (한글) (도움말) Mar 20 2021 (TianEngine)

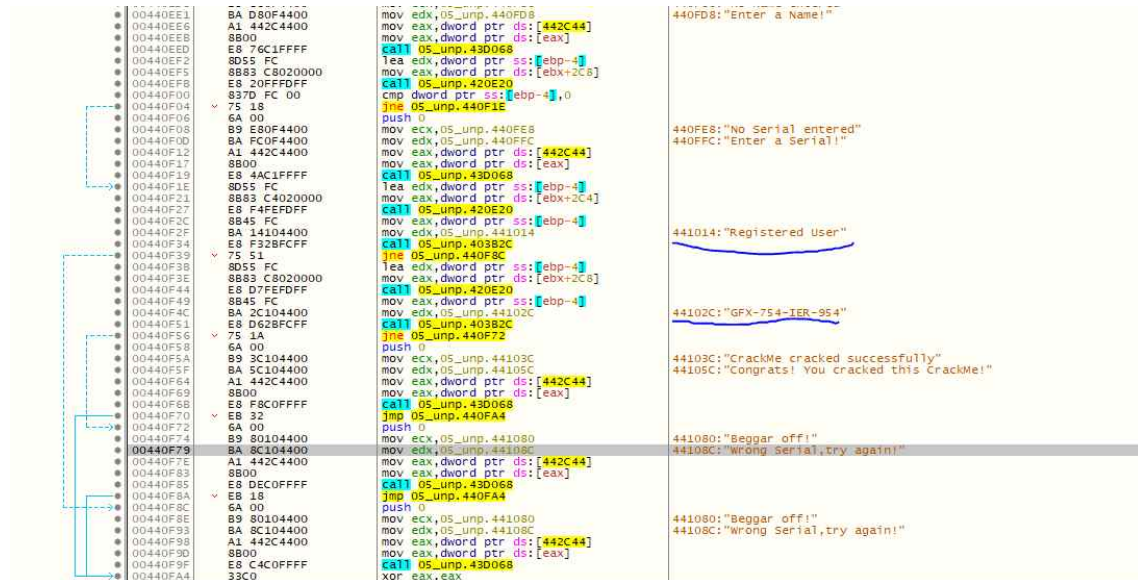
CPU 실행기 메모리 중단점 SEH 소스보기 기본 설정

00402170: JZ EBX, F4
00402172: JZ EBX, F4
00402174: JZ EBX, F4
00402176: JZ EBX, F4
00402178: JZ EBX, F4
0040217A: JZ EBX, F4
0040217C: JZ EBX, F4
0040217E: JZ EBX, F4
00402180: JZ EBX, F4
00402182: JZ EBX, F4
00402184: JZ EBX, F4
00402186: JZ EBX, F4
00402188: JZ EBX, F4
0040218A: JZ EBX, F4
0040218C: JZ EBX, F4
0040218E: JZ EBX, F4
00402190: JZ EBX, F4
00402192: JZ EBX, F4
00402194: JZ EBX, F4
00402196: JZ EBX, F4
00402198: JZ EBX, F4
0040219A: JZ EBX, F4
0040219C: JZ EBX, F4
0040219E: JZ EBX, F4
004021A0: JZ EBX, F4
004021A2: JZ EBX, F4
004021A4: JZ EBX, F4
004021A6: JZ EBX, F4
004021A8: JZ EBX, F4
004021AA: JZ EBX, F4
004021AC: JZ EBX, F4
004021AE: JZ EBX, F4
004021B0: JZ EBX, F4
004021B2: JZ EBX, F4
004021B4: JZ EBX, F4
004021B6: JZ EBX, F4
004021B8: JZ EBX, F4
004021BA: JZ EBX, F4
004021BC: JZ EBX, F4
004021BE: JZ EBX, F4
004021C0: JZ EBX, F4
004021C2: JZ EBX, F4
004021C4: JZ EBX, F4
004021C6: JZ EBX, F4
004021C8: JZ EBX, F4
004021CA: JZ EBX, F4
004021CC: JZ EBX, F4
004021CE: JZ EBX, F4
004021D0: JZ EBX, F4
004021D2: JZ EBX, F4
004021D4: JZ EBX, F4
004021D6: JZ EBX, F4
004021D8: JZ EBX, F4
004021DA: JZ EBX, F4
004021DC: JZ EBX, F4
004021DE: JZ EBX, F4
004021E0: JZ EBX, F4
004021E2: JZ EBX, F4
004021E4: JZ EBX, F4
004021E6: JZ EBX, F4
004021E8: JZ EBX, F4
004021EA: JZ EBX, F4
004021EC: JZ EBX, F4
004021EE: JZ EBX, F4
004021F0: JZ EBX, F4
004021F2: JZ EBX, F4
004021F4: JZ EBX, F4
004021F6: JZ EBX, F4
004021F8: JZ EBX, F4
004021FA: JZ EBX, F4
004021FC: JZ EBX, F4
004021FE: JZ EBX, F4
00402200: JZ EBX, F4
00402202: JZ EBX, F4
00402204: JZ EBX, F4
00402206: JZ EBX, F4
00402208: JZ EBX, F4
0040220A: JZ EBX, F4
0040220C: JZ EBX, F4
0040220E: JZ EBX, F4
00402210: JZ EBX, F4
00402212: JZ EBX, F4
00402214: JZ EBX, F4
00402216: JZ EBX, F4
00402218: JZ EBX, F4
0040221A: JZ EBX, F4
0040221C: JZ EBX, F4
0040221E: JZ EBX, F4
00402220: JZ EBX, F4
00402222: JZ EBX, F4
00402224: JZ EBX, F4
00402226: JZ EBX, F4
00402228: JZ EBX, F4
0040222A: JZ EBX, F4
0040222C: JZ EBX, F4
0040222E: JZ EBX, F4
00402230: JZ EBX, F4
00402232: JZ EBX, F4
00402234: JZ EBX, F4
00402236: JZ EBX, F4
00402238: JZ EBX, F4
0040223A: JZ EBX, F4
0040223C: JZ EBX, F4
0040223E: JZ EBX, F4
00402240: JZ EBX, F4
00402242: JZ EBX, F4
00402244: JZ EBX, F4
00402246: JZ EBX, F4
00402248: JZ EBX, F4
0040224A: JZ EBX, F4
0040224C: JZ EBX, F4
0040224E: JZ EBX, F4
00402250: JZ EBX, F4
00402252: JZ EBX, F4
00402254: JZ EBX, F4
00402256: JZ EBX, F4
00402258: JZ EBX, F4
0040225A: JZ EBX, F4
0040225C: JZ EBX, F4
0040225E: JZ EBX, F4
00402260: JZ EBX, F4
00402262: JZ EBX, F4
00402264: JZ EBX, F4
00402266: JZ EBX, F4
00402268: JZ EBX, F4
0040226A: JZ EBX, F4
0040226C: JZ EBX, F4
0040226E: JZ EBX, F4
00402270: JZ EBX, F4
00402272: JZ EBX, F4
00402274: JZ EBX, F4
00402276: JZ EBX, F4
00402278: JZ EBX, F4
0040227A: JZ EBX, F4
0040227C: JZ EBX, F4
0040227E: JZ EBX, F4
00402280: JZ EBX, F4
00402282: JZ EBX, F4
00402284: JZ EBX, F4
00402286: JZ EBX, F4
00402288: JZ EBX, F4
0040228A: JZ EBX, F4
0040228C: JZ EBX, F4
0040228E: JZ EBX, F4
00402290: JZ EBX, F4
00402292: JZ EBX, F4
00402294: JZ EBX, F4
00402296: JZ EBX, F4
00402298: JZ EBX, F4
0040229A: JZ EBX, F4
0040229C: JZ EBX, F4
0040229E: JZ EBX, F4
004022A0: JZ EBX, F4
004022A2: JZ EBX, F4
004022A4: JZ EBX, F4
004022A6: JZ EBX, F4
004022A8: JZ EBX, F4
004022AA: JZ EBX, F4
004022AC: JZ EBX, F4
004022AE: JZ EBX, F4
004022B0: JZ EBX, F4
004022B2: JZ EBX, F4
004022B4: JZ EBX, F4
004022B6: JZ EBX, F4
004022B8: JZ EBX, F4
004022BA: JZ EBX, F4
004022BC: JZ EBX, F4
004022BE: JZ EBX, F4
004022C0: JZ EBX, F4
004022C2: JZ EBX, F4
004022C4: JZ EBX, F4
004022C6: JZ EBX, F4
004022C8: JZ EBX, F4
004022CA: JZ EBX, F4
004022CC: JZ EBX, F4
004022CE: JZ EBX, F4
004022D0: JZ EBX, F4
004022D2: JZ EBX, F4
004022D4: JZ EBX, F4
004022D6: JZ EBX, F4
004022D8: JZ EBX, F4
004022DA: JZ EBX, F4
004022DC: JZ EBX, F4
004022DE: JZ EBX, F4
004022E0: JZ EBX, F4
004022E2: JZ EBX, F4
004022E4: JZ EBX, F4
004022E6: JZ EBX, F4
004022E8: JZ EBX, F4
004022EA: JZ EBX, F4
004022EC: JZ EBX, F4
004022EE: JZ EBX, F4
004022F0: JZ EBX, F4
004022F2: JZ EBX, F4
004022F4: JZ EBX, F4
004022F6: JZ EBX, F4
004022F8: JZ EBX, F4
004022FA: JZ EBX, F4
004022FC: JZ EBX, F4
004022FE: JZ EBX, F4
00402300: JZ EBX, F4
00402302: JZ EBX, F4
00402304: JZ EBX, F4
00402306: JZ EBX, F4
00402308: JZ EBX, F4
0040230A: JZ EBX, F4
0040230C: JZ EBX, F4
0040230E: JZ EBX, F4
00402310: JZ EBX, F4
00402312: JZ EBX, F4
00402314: JZ EBX, F4
00402316: JZ EBX, F4
00402318: JZ EBX, F4
0040231A: JZ EBX, F4
0040231C: JZ EBX, F4
0040231E: JZ EBX, F4
00402320: JZ EBX, F4
00402322: JZ EBX, F4
00402324: JZ EBX, F4
00402326: JZ EBX, F4
00402328: JZ EBX, F4
0040232A: JZ EBX, F4
0040232C: JZ EBX, F4
0040232E: JZ EBX, F4
00402330: JZ EBX, F4
00402332: JZ EBX, F4
00402334: JZ EBX, F4
00402336: JZ EBX, F4
00402338: JZ EBX, F4
0040233A: JZ EBX, F4
0040233C: JZ EBX, F4
0040233E: JZ EBX, F4
00402340: JZ EBX, F4
00402342: JZ EBX, F4
00402344: JZ EBX, F4
00402346: JZ EBX, F4
00402348: JZ EBX, F4
0040234A: JZ EBX, F4
0040234C: JZ EBX, F4
0040234E: JZ EBX, F4
00402350: JZ EBX, F4
00402352: JZ EBX, F4
00402354: JZ EBX, F4
00402356: JZ EBX, F4
00402358: JZ EBX, F4
0040235A: JZ EBX, F4
0040235C: JZ EBX, F4
0040235E: JZ EBX, F4
00402360: JZ EBX, F4
00402362: JZ EBX, F4
00402364: JZ EBX, F4
00402366: JZ EBX, F4
00402368: JZ EBX, F4
0040236A: JZ EBX, F4
0040236C: JZ EBX, F4
0040236E: JZ EBX, F4
00402370: JZ EBX, F4
00402372: JZ EBX, F4
00402374: JZ EBX, F4
00402376: JZ EBX, F4
00402378: JZ EBX, F4
0040237A: JZ EBX, F4
0040237C: JZ EBX, F4
0040237E: JZ EBX, F4
00402380: JZ EBX, F4
00402382: JZ EBX, F4
00402384: JZ EBX, F4
00402386: JZ EBX, F4
00402388: JZ EBX, F4
0040238A: JZ EBX, F4
0040238C: JZ EBX, F4
0040238E: JZ EBX, F4
00402390: JZ EBX, F4
00402392: JZ EBX, F4
00402394: JZ EBX, F4
00402396: JZ EBX, F4
00402398: JZ EBX, F4
0040239A: JZ EBX, F4
0040239C: JZ EBX, F4
0040239E: JZ EBX, F4
004023A0: JZ EBX, F4
004023A2: JZ EBX, F4
004023A4: JZ EBX, F4
004023A6: JZ EBX, F4
004023A8: JZ EBX, F4
004023AA: JZ EBX, F4
004023AC: JZ EBX, F4
004023AE: JZ EBX, F4
004023B0: JZ EBX, F4
004023B2: JZ EBX, F4
004023B4: JZ EBX, F4
004023B6: JZ EBX, F4
004023B8: JZ EBX, F4
004023BA: JZ EBX, F4
004023BC: JZ EBX, F4
004023BE: JZ EBX, F4
004023C0: JZ EBX, F4
004023C2: JZ EBX, F4
004023C4: JZ EBX, F4
004023C6: JZ EBX, F4
004023C8: JZ EBX, F4
004023CA: JZ EBX, F4
004023CC: JZ EBX, F4
004023CE: JZ EBX, F4
004023D0: JZ EBX, F4
004023D2: JZ EBX, F4
004023D4: JZ EBX, F4
004023D6: JZ EBX, F4
004023D8: JZ EBX, F4
004023DA: JZ EBX, F4
004023DC: JZ EBX, F4
004023DE: JZ EBX, F4
004023E0: JZ EBX, F4
004023E2: JZ EBX, F4
004023E4: JZ EBX, F4
004023E6: JZ EBX, F4
004023E8: JZ EBX, F4
004023EA: JZ EBX, F4
004023EC: JZ EBX, F4
004023EE: JZ EBX, F4
004023F0: JZ EBX, F4
004023F2: JZ EBX, F4
004023F4: JZ EBX, F4
004023F6: JZ EBX, F4
004023F8: JZ EBX, F4
004023FA: JZ EBX, F4
004023FC: JZ EBX, F4
004023FE: JZ EBX, F4
00402400: JZ EBX, F4
00402402: JZ EBX, F4
00402404: JZ EBX, F4
00402406: JZ EBX, F4
00402408: JZ EBX, F4
0040240A: JZ EBX, F4
0040240C: JZ EBX, F4
0040240E: JZ EBX, F4
00402410: JZ EBX, F4
00402412: JZ EBX, F4
00402414: JZ EBX, F4
00402416: JZ EBX, F4
00402418: JZ EBX, F4
0040241A: JZ EBX, F4
0040241C: JZ EBX, F4
0040241E: JZ EBX, F4
00402420: JZ EBX, F4
00402422: JZ EBX, F4
00402424: JZ EBX, F4
00402426: JZ EBX, F4
00402428: JZ EBX, F4
0040242A: JZ EBX, F4
0040242C: JZ EBX, F4
0040242E: JZ EBX, F4
00402430: JZ EBX, F4
00402432: JZ EBX, F4
00402434: JZ EBX, F4
00402436: JZ EBX, F4
00402438: JZ EBX, F4
0040243A: JZ EBX, F4
0040243C: JZ EBX, F4
0040243E: JZ EBX, F4
00402440: JZ EBX, F4
00402442: JZ EBX, F4
00402444: JZ EBX, F4
00402446: JZ EBX, F4
00402448: JZ EBX, F4
0040244A: JZ EBX, F4
0040244C: JZ EBX, F4
0040244E: JZ EBX, F4
00402450: JZ EBX, F4
00402452: JZ EBX, F4
00402454: JZ EBX, F4
00402456: JZ EBX, F4
00402458: JZ EBX, F4
0040245A: JZ EBX, F4
0040245C: JZ EBX, F4
0040245E: JZ EBX, F4
00402460: JZ EBX, F4
00402462: JZ EBX, F4
00402464: JZ EBX, F4
00402466: JZ EBX, F4
00402468: JZ EBX, F4
0040246A: JZ EBX, F4
0040246C: JZ EBX, F4
0040246E: JZ EBX, F4
00402470: JZ EBX, F4
00402472: JZ EBX, F4
00402474: JZ EBX, F4
00402476: JZ EBX, F4
00402478: JZ EBX, F4
0040247A: JZ EBX, F4
0040247C: JZ EBX, F4
0040247E: JZ EBX, F4
00402480: JZ EBX, F4
00402482: JZ EBX, F4
00402484: JZ EBX, F4
00402486: JZ EBX, F4
00402488: JZ EBX, F4
0040248A: JZ EBX, F4
0040248C: JZ EBX, F4
0040248E: JZ EBX, F4
00402490: JZ EBX, F4
00402492: JZ EBX, F4
00402494: JZ EBX, F4
00402496: JZ EBX, F4
00402498: JZ EBX, F4
0040249A: JZ EBX, F4
0040249C: JZ EBX, F4
0040249E: JZ EBX, F4
004024A0: JZ EBX, F4
004024A2: JZ EBX, F4
004024A4: JZ EBX, F4
004024A6: JZ EBX, F4
004024A8: JZ EBX, F4
004024AA: JZ EBX, F4
004024AC: JZ EBX, F4
004024AE: JZ EBX, F4
004024B0: JZ EBX, F4
004024B2: JZ EBX, F4
004024B4: JZ EBX, F4
004024B6: JZ EBX, F4
004024B8: JZ EBX, F4
004024BA: JZ EBX, F4
004024BC: JZ EBX, F4
004024BE: JZ EBX, F4
004024C0: JZ EBX, F4
004024C2: JZ EBX, F4
004024C4: JZ EBX, F4
004024C6: JZ EBX, F4
004024C8: JZ EBX, F4
004024CA: JZ EBX, F4
004024CC: JZ EBX, F4
004024CE: JZ EBX, F4
004024D0: JZ EBX, F4
004024D2: JZ EBX, F4
004024D4: JZ EBX, F4
004024D6: JZ EBX, F4
004024D8: JZ EBX, F4
004024DA: JZ EBX, F4
004024DC: JZ EBX, F4
004024DE: JZ EBX, F4
004024E0: JZ EBX, F4
004024E2: JZ EBX, F4
004024E4: JZ EBX, F4
004024E6: JZ EBX, F4
004024E8: JZ EBX, F4
004024EA: JZ EBX, F4
004024EC: JZ EBX, F4
004024EE: JZ EBX, F4
004024F0: JZ EBX, F4
004024F2: JZ EBX, F4
004024F4: JZ EBX, F4
004024F6: JZ EBX, F4
004024F8: JZ EBX, F4
004024FA: JZ EBX, F4
004024FC: JZ EBX, F4
004024FE: JZ EBX, F4
00402500: JZ EBX, F4
00402502: JZ EBX, F4
00402504: JZ EBX, F4
00402506: JZ EBX, F4
00402508: JZ EBX, F4
0040250A: JZ EBX, F4
0040250C: JZ EBX, F4
0040250E: JZ EBX, F4
00402510: JZ EBX, F4
00402512: JZ EBX, F4
00402514: JZ EBX, F4
00402516: JZ EBX, F4
00402518: JZ EBX, F4
0040251A: JZ EBX, F4
0040251C: JZ EBX, F4
0040251E: JZ EBX, F4
00402520: JZ EBX, F4
00402522: JZ EBX, F4
00402524: JZ EBX, F4
00402526: JZ EBX, F4
00402528: JZ EBX, F4
0040252A: JZ EBX, F4
0040252C: JZ EBX, F4
0040252E: JZ EBX, F4
00402530: JZ EBX, F4
00402532: JZ EBX, F4
00402534: JZ EBX, F4
00402536: JZ EBX, F4
00402538: JZ EBX, F4
0040253A: JZ EBX, F4
0040253C: JZ EBX, F4
0040253E: JZ EBX, F4
00402540: JZ EBX, F4
00402542: JZ EBX, F4
00402544: JZ EBX, F4
00402546: JZ EBX, F4
00402548: JZ EBX, F4
0040254A: JZ EBX, F4
0040254C: JZ EBX, F4
0040254E: JZ EBX, F4
00402550: JZ EBX, F4
00402552: JZ EBX, F4
00402554: JZ EBX, F4
00402556: JZ EBX, F4
00402558: JZ EBX, F4
0040255A: JZ EBX, F4
0040255C: JZ EBX, F4
0040255E: JZ EBX, F4
00402560: JZ EBX, F4
00402562: JZ EBX, F4
00402564: JZ EBX, F4
00402566: JZ EBX, F4
00402568: JZ EBX, F4
0040256A: JZ EBX, F4
0040256C: JZ EBX, F4
0040256E: JZ EBX, F4
00402570: JZ EBX, F4
00402572: JZ EBX, F4
00402574: JZ EBX, F4
00402576: JZ EBX, F4
00402578: JZ EBX, F4
0040257A: JZ EBX, F4
0040257C: JZ EBX, F4
0040257E: JZ EBX, F4
00402580: JZ EBX, F4
00402582: JZ EBX, F4
00402584: JZ EBX, F4
00402586: JZ EBX, F4
00402588: JZ EBX, F4
0040258A: JZ EBX, F4
0040258C: JZ EBX, F4
0040258E: JZ EBX, F4
00402590: JZ EBX, F4
00402592: JZ EBX, F4
00402594: JZ EBX, F4
00402596: JZ EBX, F4
00402598: JZ EBX, F4
0040259A: JZ EBX, F4
0040259C: JZ EBX, F4
0040259E: JZ EBX, F4
004025A0: JZ EBX, F4
004025A2: JZ EBX, F4
004025A4: JZ EBX, F4
004025A6: JZ EBX, F4
004025A8: JZ EBX, F4
004025AA: JZ EBX, F4
004025AC: JZ EBX, F4
004025AE: JZ EBX, F4
004025B0: JZ EBX, F4
0

아까 출력되었던 Wrong Serial 문자열을 찾기



문자열 참조에서 해당 라인으로 들어가본 결과



밑줄 친 부분과 같이 name과 Serial로 유추되는 주석이 달려있는 것을 볼 수 있다

Crackers For Freedom CrackMe v3.0

Official CFF CrackMe v3.0

Registered User	Coder Acid Bytes [CFF]
GFX-754-IER-954	Rel. Date 05/08/2000
Register now !	This is the official CFF CrackMe If you can manage to crack it, mail Name/Serial to: acidbytes@gmx.net
Quit the CrackMe	

밑줄 친 Name과 Serial을 입력하면 성공!

CrackMe cracked successfully X

Congrats! You cracked this CrackMe!

이 프로그램의 등록 키는 Registered User와 GFX-754-IER-954이다