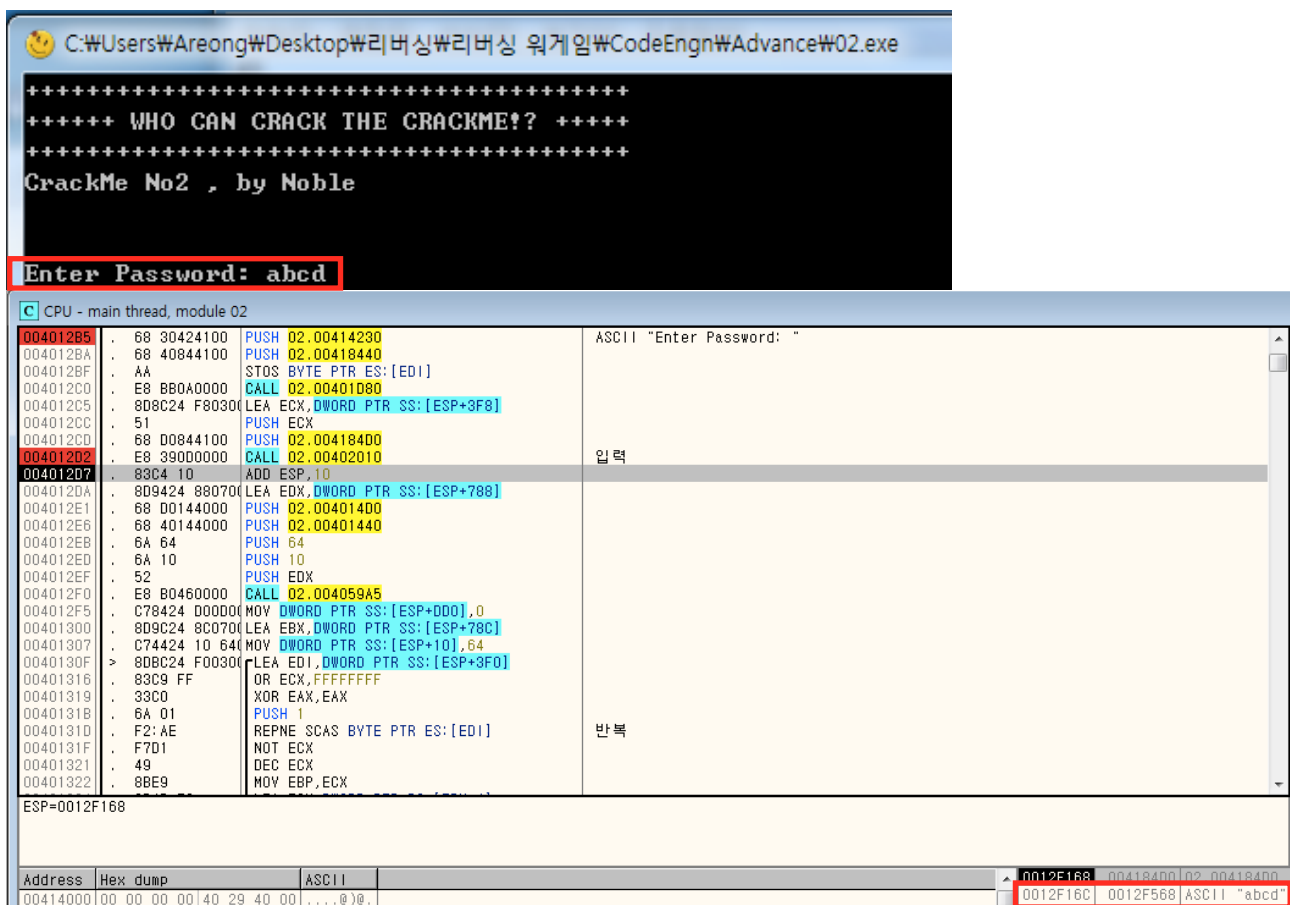
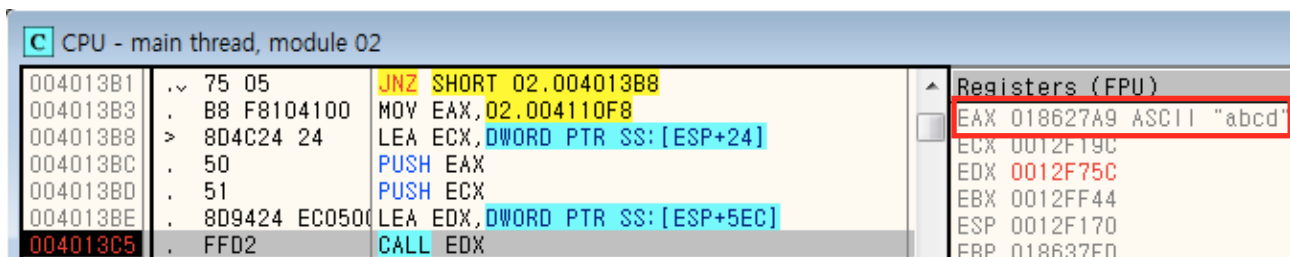


프로그램을 실행하면 패스워드를 입력하라고 합니다.

분석을 통해 패스워드를 찾으려 합니다.



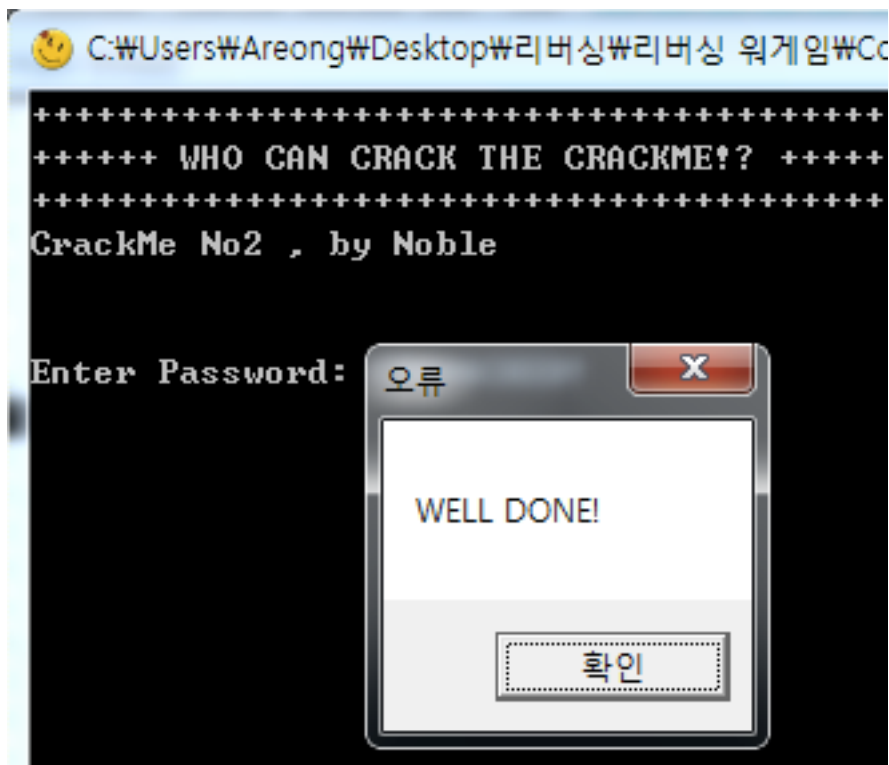
특정 함수를 통해 입력한 문자열을 받아옵니다.



그리고 밑에 내려가다 보면 abcd를 스택에 집어넣고 함수를 호출하는 부분이 있습니다.

| CPU - main thread | | | Registers (FPU) |
|-------------------|---------------|-------------------------------|---------------------------|
| 0012F768 | 8DBD 1CFFFFFF | LEA EDI,DWORD PTR SS:[EBP-E4] | EAX 018627A9 ASCII "abcd" |
| 0012F76E | B9 39000000 | MOV ECX,39 | ECX 00000000 |
| 0012F773 | B8 CCCCCCCC | MOV EAX,CCCCCCCC | EDX 0012F75C |
| 0012F778 | F3: AB | REP STOS DWORD PTR ES:[EDI] | EBX 0012FF44 |
| 0012F77A | A1 08604000 | MOV EAX,DWORD PTR DS:[406008] | ESP 0012F078 |
| 0012F77F | 33C5 | XOR EAX,EBP | EBP 0012F168 |
| 0012F781 | 8945 FC | MOV DWORD PTR SS:[EBP-4],EAX | ESI 0012FB90 |
| 0012F784 | 8B45 0C | MOV EAX,DWORD PTR SS:[EBP+C] | EDI 0012F168 |
| 0012F787 | 0FBEO8 | MOVSX ECX,BYTE PTR DS:[EAX] | EIP 0012F787 |
| 0012F78A | 83F9 43 | CMP ECX,43 | C 0 ES 0023 32bit 0(FFFF) |
| 0012F78D | 0F85 F7000000 | JNZ 0012F88A | P 0 CS 001B 32bit 0(FFFF) |
| 0012F793 | 8B45 0C | MOV EAX,DWORD PTR SS:[EBP+C] | A 0 SS 0023 32bit 0(FFFF) |
| 0012F796 | 0FBEO8 01 | MOVSX ECX,BYTE PTR DS:[EAX+1] | Z 0 DS 0023 32bit 0(FFFF) |
| 0012F79A | 83F9 52 | CMP ECX,52 | S 1 FS 003B 32bit 7FFDF0 |
| 0012F79D | 0F85 E7000000 | JNZ 0012F88A | T 0 GS 0000 NULL |
| 0012F7A3 | 8B45 0C | MOV EAX,DWORD PTR SS:[EBP+C] | D 0 |
| 0012F7A6 | 0FBEO8 02 | MOVSX ECX,BYTE PTR DS:[EAX+2] | O 0 LastErr ERROR_SUCCESS |
| 0012F7AA | 83F9 41 | CMP ECX,41 | EFL 00000282 (NO,NB,NE,A, |
| 0012F7AD | 0F85 D7000000 | JNZ 0012F88A | |
| 0012F7B3 | 8B45 0C | MOV EAX,DWORD PTR SS:[EBP+C] | |
| 0012F7B6 | 0FBEO8 03 | MOVSX ECX,BYTE PTR DS:[EAX+3] | |

해당 함수를 분석해보니 입력한 문자열을 일대일 비교를 통해 패스워드 인증을 처리합니다.



성공!