

-----  
How to make a keygen for 2Sweet's Crackme 2.d  
-----

Cracker: **stealthFIGHTER**

Target: **2Sweet's Crackme 2.d**

Tools: SoftIce  
Delphi  
Brain

Where: <http://2sweet.tsx.org/>

Protection: Name/Company/Serial

-----  
Sorry for my English, it's not my mother language.  
-----

-----  
**Step 1** (finding a valid serial):  
-----

=====  
I think it is very easy to find a serial. Run Crackme >> type your details >> go to Soft-Ice >> type **bpx hmemcpy [Enter]** (=Soft-Ice will break when is something copy to memory). Go back >> push REGISTER >> WRONG CODE >> We're in Soft-Ice with these breakpoints:

=====  
**1. bpx:**

=====  
Calculation of the sum of our name:  
Final value is in **EDI**.

=====  
MOVZX EDX, BYTE PTR [EAX+EDX-01] ; Move first character of the name into EDX  
INC EAX ; Increase EAX (EAX = counter of the length of name)  
ADD EDI, EDX ; Add this character to **EDI** (EDI start with value '1')  
CMP EAX, ECX ; Compare if it was the last character  
JBE 004422AE ; If yes jump, else jump back

=====  
**2. bpx:**

=====  
Calculation of the sum of our company:  
Final value is in **ESI**.

=====  
MOVZX EDX, BYTE PTR [EAX+EDX-01] ; Move first character of the company into EDX  
INC EAX ; Increase EAX (EAX = counter of the length of company)  
ADD ESI, EDX ; Add this character to **ESI** (ESI start with value '1')  
CMP EAX, [EBP-08] ; Compare if it was the last character  
JBE 004422AE ; If yes jump, else jump back

=====  
**3. bpx:**

=====  
Nothing important

=====  
**4. bpx:**

=====  
Nothing important  
=====

=====

## 5. bpx:

=====

Notes: **EDI** = value of sum of all characters of name, **ESI** = value of sum of all characters of company.

Main calculation routine:

=====

```
LEA      EAX, DWORD PTR [ESI+EDI]      ; EAX = ESI + EDI
IMUL     EAX, 000001F2                 ; EAX = EAX * 1F2
MOV      DWORD PTR [EBP-10], EAX       ; Move EAX into [EBP-10]
MOV      EAX, DWORD PTR [EBP-10]      ; Move [EBP-10] into EAX
IMUL     [EBP-10]                      ; EAX = [EBP-10] * [EBP-10] (Note: [EBP-10] = EAX)
IMUL     EDI                          ; EAX = EAX * EDI
MOV      DWORD PTR [EBP-10], EAX       ; Move EAX into [EBP-10]
SUB      DWORD PTR [EBP-10], ESI       ; [EBP-10] = EAX - ESI
MOV      EAX, DWORD PTR [EBP-10]      ; Move [EBP-10] into EAX (EAX = final serial)
XOR      EDX, EDX
PUSH     EDX
PUSH     EAX
LEA      EDX, DWORD PTR [EBP-14]
MOV      EAX, 00000008
CALL     00407668
LEA      EDX, DWORD PTR [EBP-18]
MOV      EAX, DWORD PTR [EBX+000002CC]
CALL     00423224                      ; Next breakpoint
MOV      EDX, DWORD PTR [EBP-18]
MOV      EAX, DWORD PTR [EBP-14]
CALL     00403B44
JE       004423AC
```

=====

## 6. bpx:

=====

Here is compare of the serial numbers:

=====

```
CALL     00403B44                      ; Type D EAX to see your right serial #.
JZ       004423AC
```

=====

Source code (included) is commented so you should understand it.

=====

CrackMe cracked!

=====



=====

If I make a mistake, please e-mail me  
to: [stealthfighter@another.com](mailto:stealthfighter@another.com)  
You can also find me on the web:

=====

----=[ <http://nitrous.hop.to/> ]=----

--[ <http://stealthfighter.cjb.net/> ]--

=====