This is my first CrackMe written in C++

Rules:

*No patching

***Make a KeyGen**

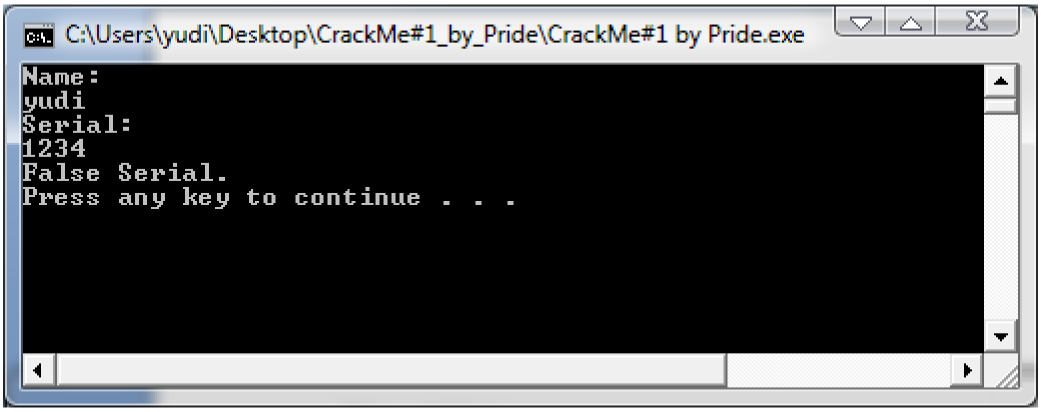
***Upload a solution + tutorial**

I hope it's not too easy.

Have fun.

****

Run the target

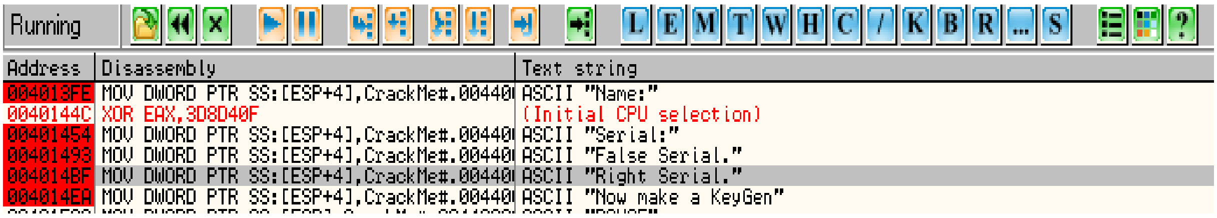


C:\Users\yudi\Desktop\CrackMe#1_by_Pride\CrackMe#1 by Pride.exe

```
Name:
yudi
Serial:
1234
False Serial.
Press any key to continue . . .
```

Load it in Olly

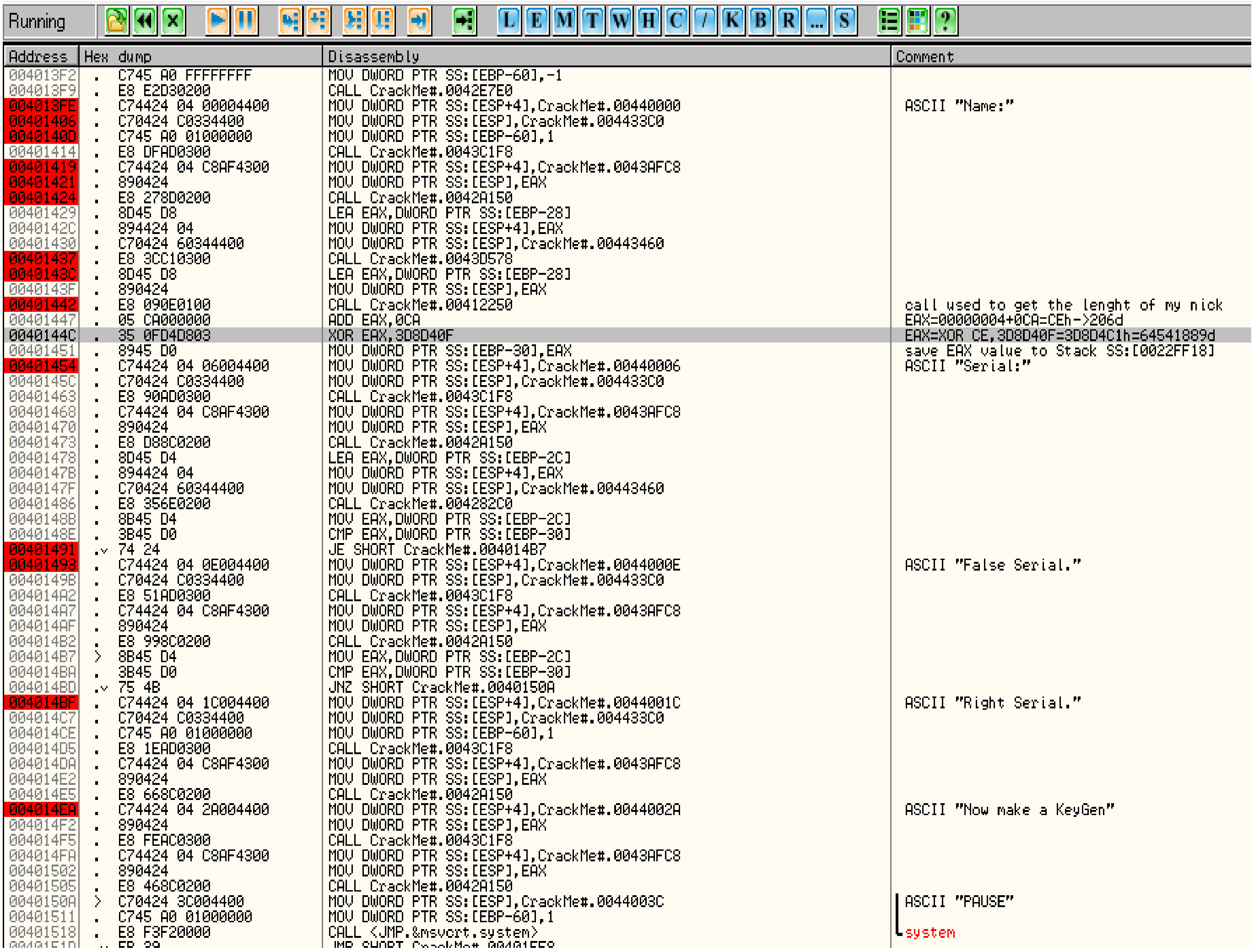
And search for strings



```
Address   Disassembly                                  Text string
004013FE  MOV DWORD PTR SS:[ESP+4],CrackMe#.00440  ASCII "Name:"
0040144C  XOR EAX,3D8D40F                              (Initial CPU selection)
00401454  MOV DWORD PTR SS:[ESP+4],CrackMe#.00440  ASCII "Serial:"
00401493  MOV DWORD PTR SS:[ESP+4],CrackMe#.00440  ASCII "False Serial."
004014BF  MOV DWORD PTR SS:[ESP+4],CrackMe#.00440  ASCII "Right Serial."
004014EA  MOV DWORD PTR SS:[ESP+4],CrackMe#.00440  ASCII "Now make a KeyGen"
```

Bp

And run it



```
Address   Hex dump                 Disassembly                                   Comment
004013F2  .  C745 A0 FFFFFFFF      MOV DWORD PTR SS:[EBP-60],-1
004013F9  .  E8 E2D30200           CALL CrackMe#.0042E7E0
004013FE  .  C74424 04 00004400    MOV DWORD PTR SS:[ESP+4],CrackMe#.00440000     ASCII "Name:"
00401406  .  C70424 C0334400       MOV DWORD PTR SS:[ESP],CrackMe#.004433C0
0040140D  .  C745 A0 01000000      MOV DWORD PTR SS:[EBP-60],1
00401414  .  E8 DFAD0300           CALL CrackMe#.0043C1F8
00401419  .  C74424 04 C8AF4300    MOV DWORD PTR SS:[ESP+4],CrackMe#.0043AFC8
00401421  .  890424                MOV DWORD PTR SS:[ESP],EAX
00401424  .  E8 278D0200           CALL CrackMe#.0042A150
00401429  .  8D45 D8               LEA EAX,DWORD PTR SS:[EBP-28]
0040142C  .  894424 04             MOV DWORD PTR SS:[ESP+4],EAX
00401430  .  C70424 60344400       MOV DWORD PTR SS:[ESP],CrackMe#.00443460
00401437  .  E8 3CC10300           CALL CrackMe#.0043D578
0040143C  .  8D45 D8               LEA EAX,DWORD PTR SS:[EBP-28]
0040143F  .  890424                MOV DWORD PTR SS:[ESP],EAX
00401442  .  E8 090E0100           CALL CrackMe#.00412250                         call used to get the lenght of my nick
00401447  .  05 CA000000           ADD EAX,0CA                                    EAX=00000004+0CA=CEh->206d
0040144C  .  35 0FD4D803           XOR EAX,3D8D40F                                EAX=XOR CE,3D8D40F=3D8D4C1h=64541889d
00401451  .  8945 D0               MOV DWORD PTR SS:[EBP-30],EAX                  save EAX value to Stack SS:[0022FF18]
00401454  .  C74424 04 06004400    MOV DWORD PTR SS:[ESP+4],CrackMe#.00440006     ASCII "Serial:"
0040145C  .  C70424 C0334400       MOV DWORD PTR SS:[ESP],CrackMe#.004433C0
00401463  .  E8 90AD0300           CALL CrackMe#.0043C1F8
00401468  .  C74424 04 C8AF4300    MOV DWORD PTR SS:[ESP+4],CrackMe#.0043AFC8
00401470  .  890424                MOV DWORD PTR SS:[ESP],EAX
00401473  .  E8 D88C0200           CALL CrackMe#.0042A150
00401478  .  8D45 D4               LEA EAX,DWORD PTR SS:[EBP-2C]
0040147B  .  894424 04             MOV DWORD PTR SS:[ESP+4],EAX
0040147F  .  C70424 60344400       MOV DWORD PTR SS:[ESP],CrackMe#.00443460
00401486  .  E8 356E0200           CALL CrackMe#.004282C0
0040148B  .  8B45 D4               MOV EAX,DWORD PTR SS:[EBP-2C]
0040148E  .  3B45 D0               CMP EAX,DWORD PTR SS:[EBP-30]
00401491  .v 74 24                 JE SHORT CrackMe#.004014B7
00401493  .  C74424 04 0E004400    MOV DWORD PTR SS:[ESP+4],CrackMe#.0044000E     ASCII "False Serial."
0040149B  .  C70424 C0334400       MOV DWORD PTR SS:[ESP],CrackMe#.004433C0
004014A2  .  E8 51AD0300           CALL CrackMe#.0043C1F8
004014A7  .  C74424 04 C8AF4300    MOV DWORD PTR SS:[ESP+4],CrackMe#.0043AFC8
004014AF  .  890424                MOV DWORD PTR SS:[ESP],EAX
004014B2  .  E8 998C0200           CALL CrackMe#.0042A150
004014B7  >  8B45 D4               MOV EAX,DWORD PTR SS:[EBP-2C]
004014BA  .  3B45 D0               CMP EAX,DWORD PTR SS:[EBP-30]
004014BD  .v 75 4B                 JNZ SHORT CrackMe#.0040150A
004014BF  .  C74424 04 1C004400    MOV DWORD PTR SS:[ESP+4],CrackMe#.0044001C     ASCII "Right Serial."
004014C7  .  C70424 C0334400       MOV DWORD PTR SS:[ESP],CrackMe#.004433C0
004014CE  .  C745 A0 01000000      MOV DWORD PTR SS:[EBP-60],1
004014D5  .  E8 1EAD0300           CALL CrackMe#.0043C1F8
004014DA  .  C74424 04 C8AF4300    MOV DWORD PTR SS:[ESP+4],CrackMe#.0043AFC8
004014E2  .  890424                MOV DWORD PTR SS:[ESP],EAX
004014E5  .  E8 668C0200           CALL CrackMe#.0042A150
004014EA  .  C74424 04 2A004400    MOV DWORD PTR SS:[ESP+4],CrackMe#.0044002A     ASCII "Now make a KeyGen"
004014F2  .  890424                MOV DWORD PTR SS:[ESP],EAX
004014F5  .  E8 FEAC0300           CALL CrackMe#.0043C1F8
004014FA  .  C74424 04 C8AF4300    MOV DWORD PTR SS:[ESP+4],CrackMe#.0043AFC8
00401502  .  890424                MOV DWORD PTR SS:[ESP],EAX
00401505  .  E8 468C0200           CALL CrackMe#.0042A150
0040150A  >  C70424 3C004400       MOV DWORD PTR SS:[ESP],CrackMe#.0044003C      ASCII "PAUSE"
00401511  .  C745 A0 01000000      MOV DWORD PTR SS:[EBP-60],1
00401518  .  E8 F3F20000           CALL <JMP.&msvcrt.system>                      system
0040151D  .v EB 39                 JMP SHORT CrackMe#.004015F8
```

What it does ....?

00401442 . E8 090E0100 CALL CrackMe#.00412250 ; call used to get the lenght of my nick

00401447 . 05 CA000000 ADD EAX,0CA ; EAX=00000004+0CA=CEh->206d

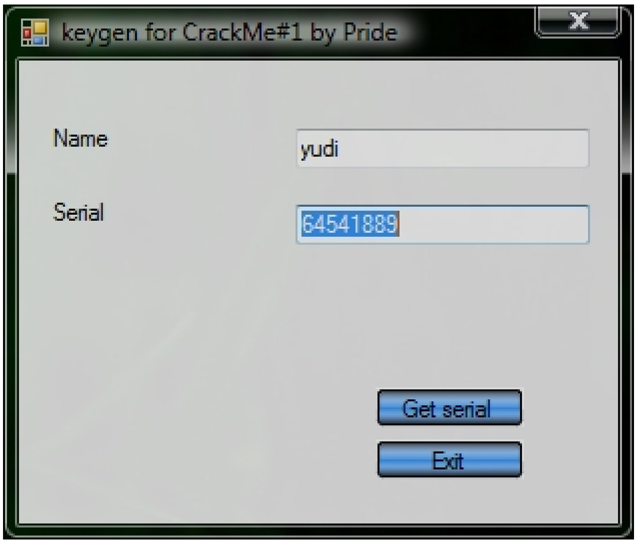
0040144C . 35 0FD4D803 XOR EAX,3D8D40F ; EAX=XOR CE,3D8D40F=3D8D4C1h=64541889d

00401451 . 8945 D0 MOV DWORD PTR SS:[EBP-30],EAX ; save EAX value to Stack SS:[0022FF18]

My keygen code is this ....

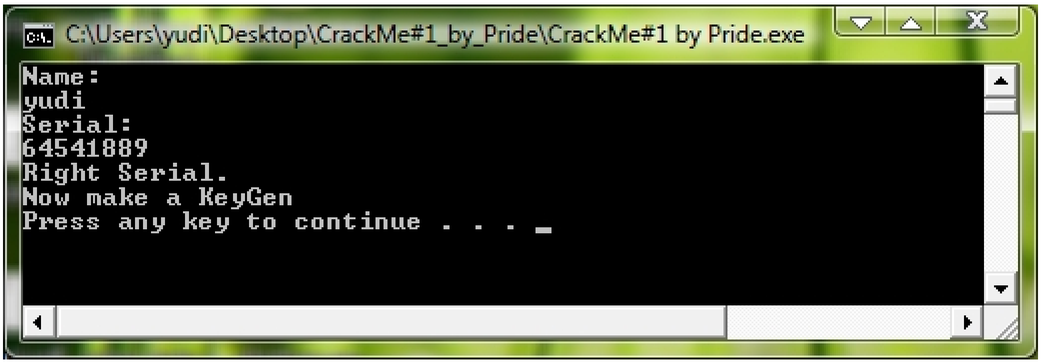
```
a = ((Len(TextBox1.Text) + 202) Xor 64541711)

take the leght of nick add 202 then XOR with 64541711
```

let`s see if it works ....

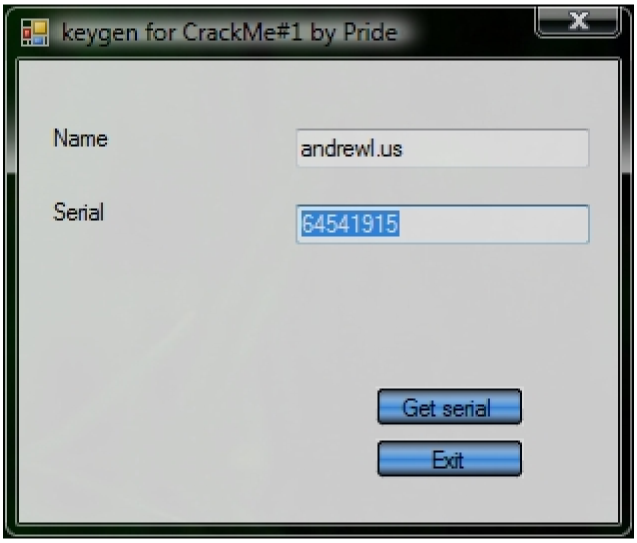


Name yudi

Serial 64541889

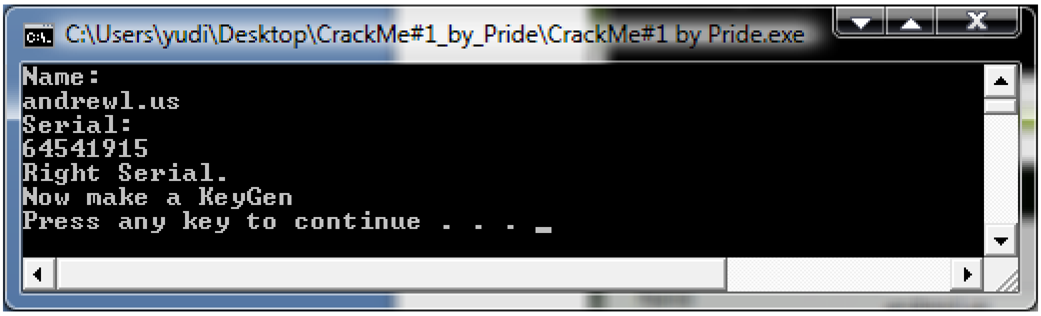

C:\Users\yudi\Desktop\CrackMe#1_by_Pride\CrackMe#1 by Pride.exe

```
Name:
yudi
Serial:
64541889
Right Serial.
Now make a KeyGen
Press any key to continue . . . _
```



Name andrewl.us

Serial 64541915


C:\Users\yudi\Desktop\CrackMe#1_by_Pride\CrackMe#1 by Pride.exe

```
Name:
andrewl.us
Serial:
64541915
Right Serial.
Now make a KeyGen
Press any key to continue . . . _
```

The end ! yudi