

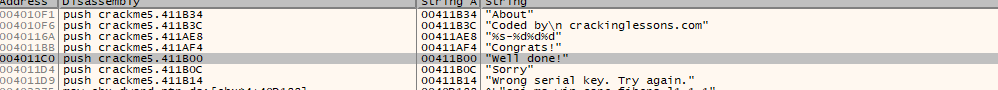
Our goal is find the serial for a username to valid the crackme

Some notable strings:

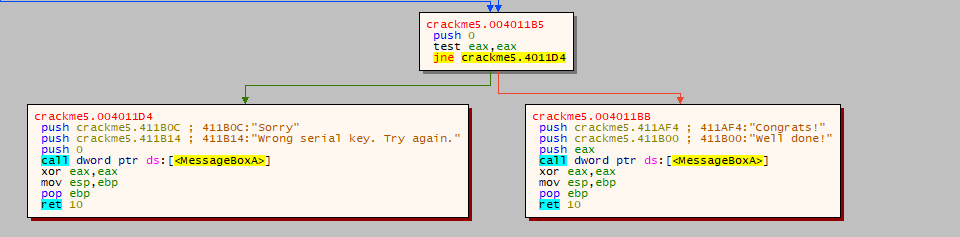
* Enter firstname:
* Enter Serial Key:
* Check

Throw crackme into x32dbg, find all reference strings

We not found the strings above in there, but we found other also interesting

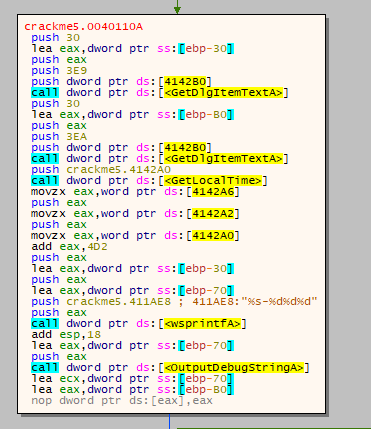


Of Course, we want somethings like Well done and Congrats, so jump there

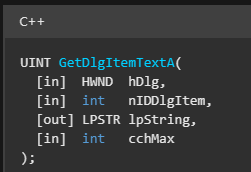


test eax, eax and jne to badboy, so we want eax is equal to 0

read the code above



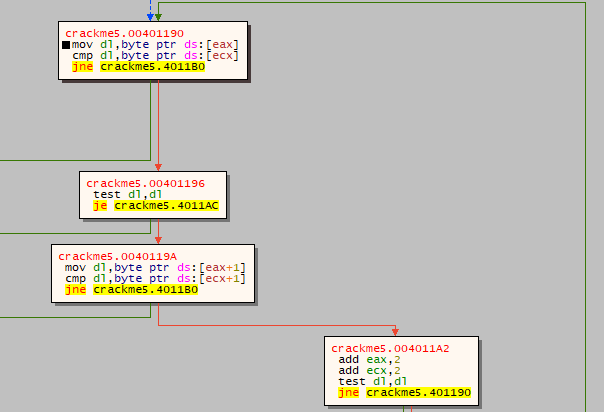
easy to know that this is code for reading input from user



following the definition of the API, easy find where the inputs are stored

username is stored at [ebp - 30] while serial stored at [ebp - B0]

Then crackme call GetLocalTime at push day, month, and year + 0x4D2 on the stack, next it push username to stack then crackme call wsprintfA function to concat them in the format “%s-%d%d%d” which mean username-year+0x4D2monthday

 After that, this is simple logic to validate the crackme, check the serial and the username after append as I explained above byte by byte. if they are exactly the same, eax will be zero which what we want

So logic is simple

**serial = username+’-’ + (year + 0x4D2) + month + day**

**example:**

**current day: 16/10/2023**

**username: vinhdeptrai**

**===> serial: vinhdeptrai-32571016**

Check:

