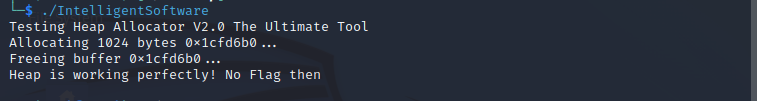
-We get a x64 ELF file

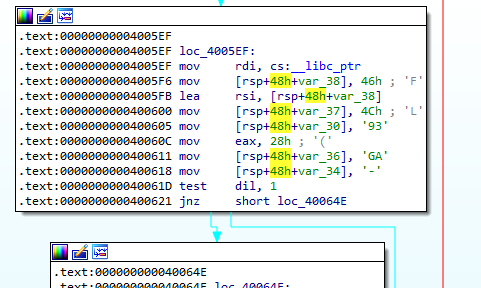
-Throw it into debugger, see all familiar functions like main, i got absolutely nothing.

-And i run it on linux machine, nothing again 🙁



-After that, i see in list of functions: get a unfamiliar function with a weird name: \_\_libc\_csu\_ctor

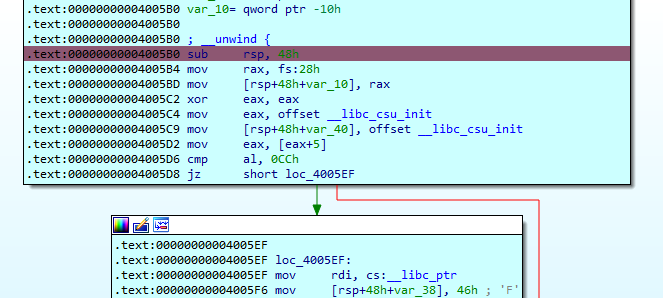
-Go to this function, i found some special characters



-See It?? FLAG-

-> the flag is absolutely generated in this function

-> so i set a breakpoint at begin of the function, then debug it



Found that it compare [\_\_libc\_scu\_init + 5 ] with 0xCC

if equal, generate Flag, just make it equal

(Many ways can do it, in my case, i just fix the ZF to 1 then jump into this

You can find more references about \_\_libc\_scu\_init then know what it means and the +5 of it contain what,.... it makes you a better reverser, doesn’t it???)

After that just make sure you redirect the correct follow of code, you will get the flag like this

