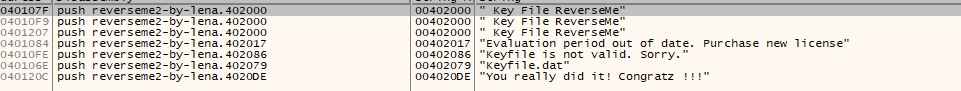
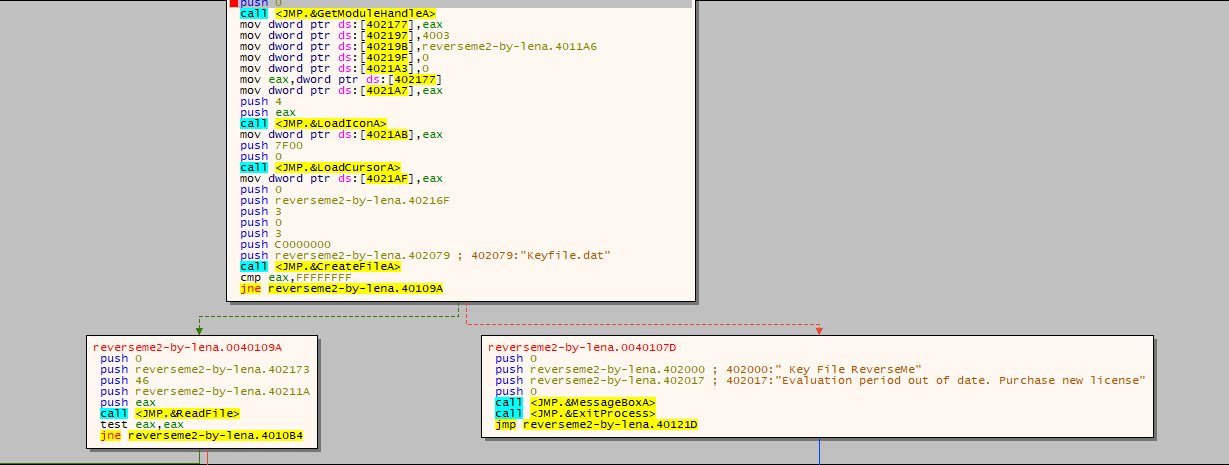


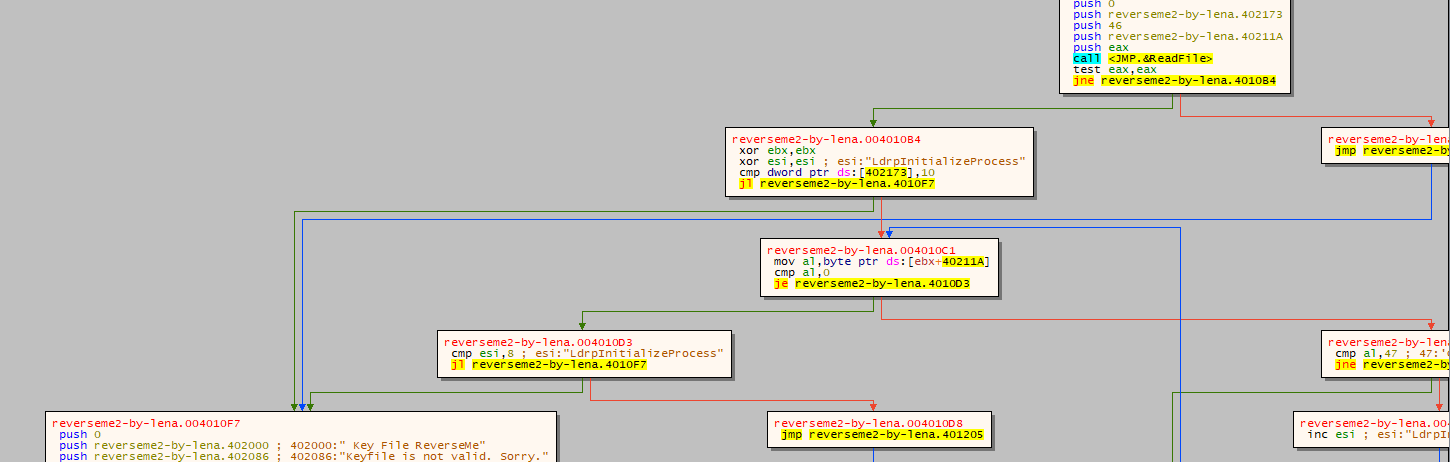
DiE:

Find references strings:

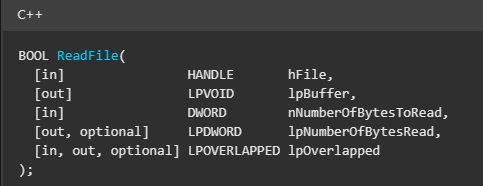


Jump there

First, it checks whether exists a file name “Keyfile.dat”

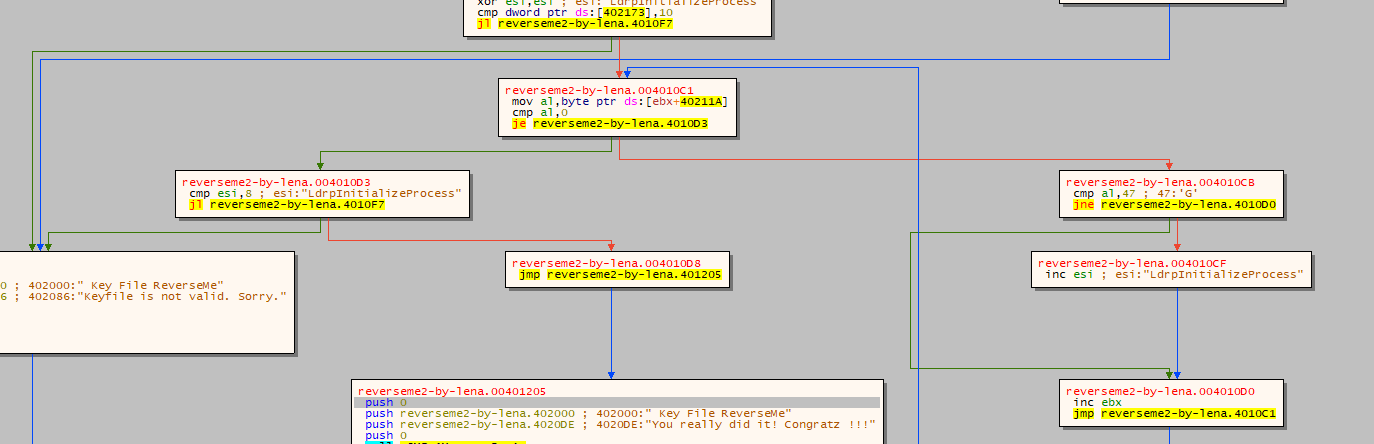


Then it read content of the file through ReadFile API



So we can determine that dword [0x402173] is length of data and 40211A contain data read from file

If length less than 0x10, it jump to invalid



Else, it turn into a major compare

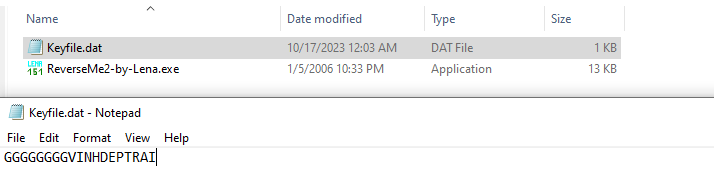
esi, and ebx were zero by xor

Then it read each byte at data compare with ‘G’ if it equal, it increase esi

When reaching a null byte which means every byte of data was checked.

it compare esi with 8, if esi bigger or equal 8 , we run into goodboy

So to do register this crackme. we just need create a file called “Keyfile.dat” which contains at least 16 character and in these characters, has at least 8 ‘G’



Let’s run reverseme and check it

