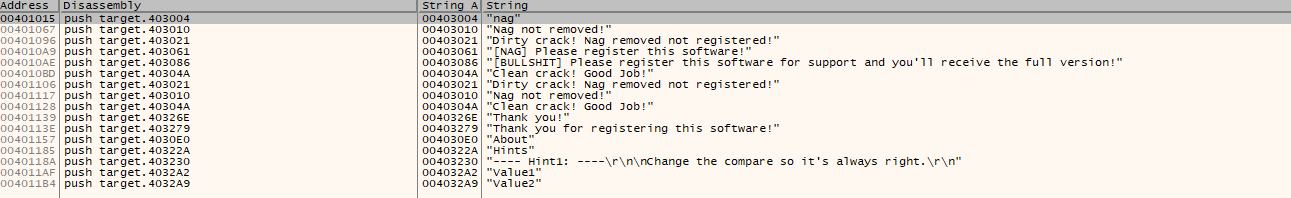
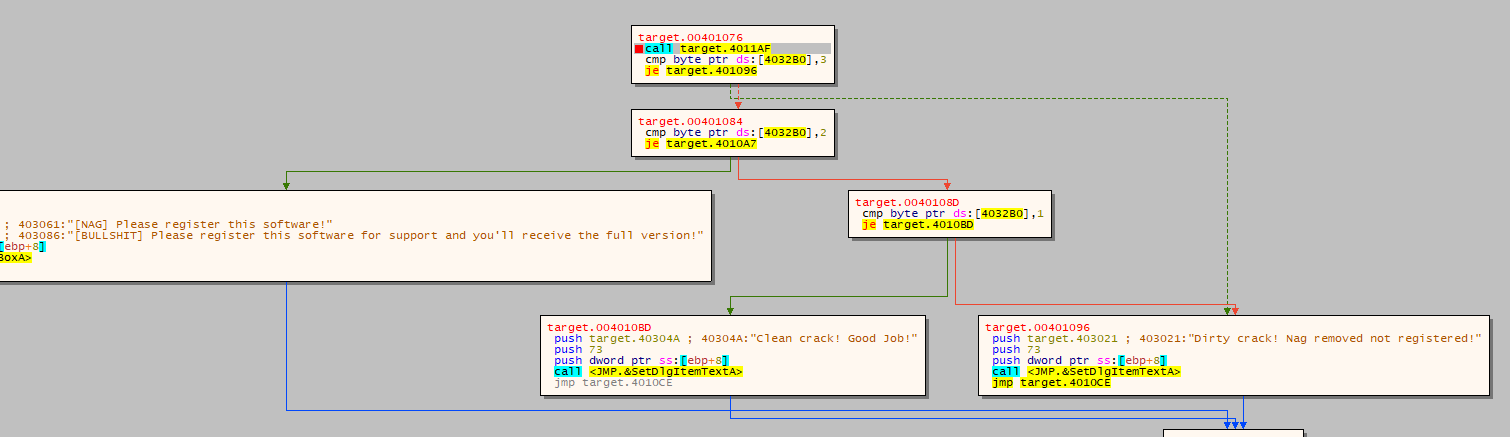


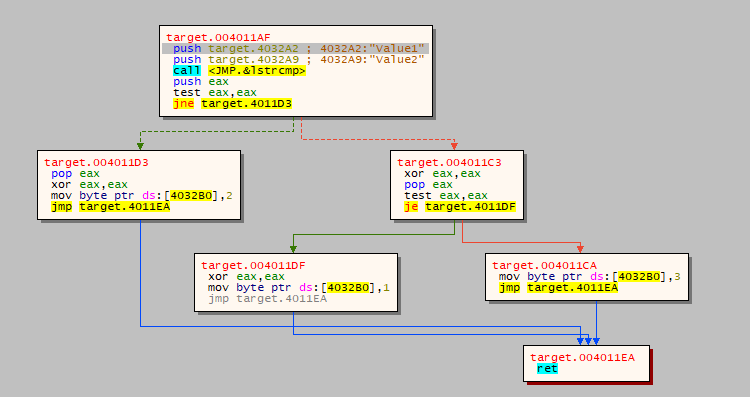
* Another 32-bit PE file
* Find all reference strings as always:
* 

Go to Clean crack! Good job



We can see that, it call a function target.4011AF, the output of that function decides all things. And what we want is byte[4032B0] equal to 1

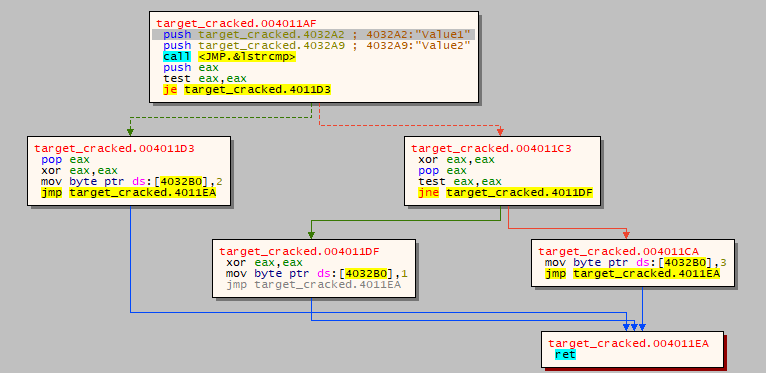
Let dig into that function target.4011AF



It compares two string by function lstrcmp(), with two input is “Value1” and “Value2”

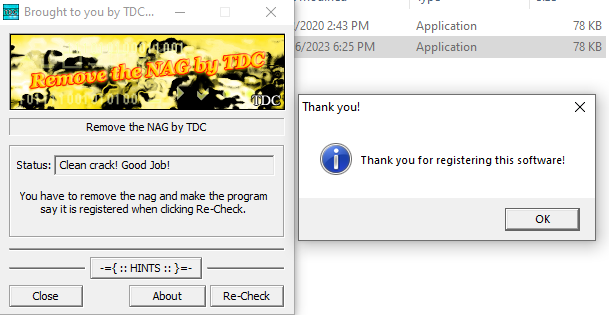
Obviously, two strings are different so the result stored in eax is not equal to zero.

So to patch this function that make the instruction mov byte ds:[4032B0], 1 (what we really want) we can patch as below



* the jne target.4011D3 in the first block is patched into je because if they are not equal, so the first jump not jump, so we don’t jump the bad block
* in block target.4011C3, je is patched into jne.

Let check.



Ok this works