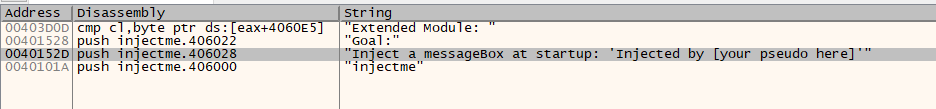
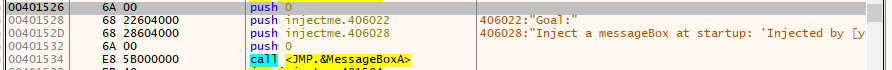
In order to inject a window with my name in it, first of all, i need to find a clear area. From address 4010b5 to 4014d3 it is filled with NOPs, so that is a good area.

Lets search for the string in the popup window:



Now we need to figure out how to call teh function that creates the popup window. Jumping to the code where the string appears we see this code regarding the function:



Before i will do anything else, i will create a label at address 4014d5, where the next instruction is.

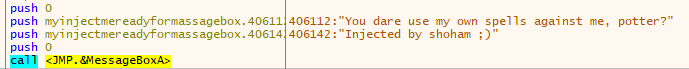
I will call the label detour, and insert a jmp detour at address 4010b5. Did this in order to keep the rest of the program running as it was.

I will create a new label at 4010bb, and overwrite the push 0 and push injectme.401030 instruction in address 401018 with jmp 4010bb, and i will inject them after the call for my injected popup.

I will push 0, "You dare use my own spells against me potter?", "Injected by shoham", 0.

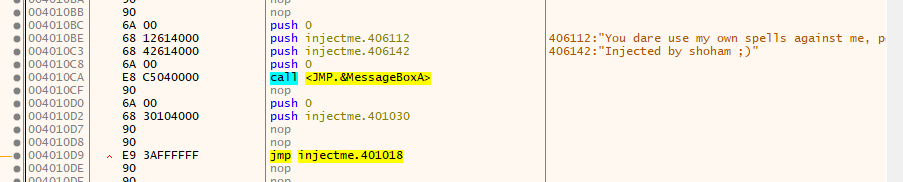
So i wrote to the memory the strings and their addresses are 406112 and 406142 respectively.

So i injected the following instructions:



And following them i injected the push instructions that were overwritten when i injected a jump to my popup window.

The code i injected looks like this:



And the moment of truth:

