

Q: What is happening when you run the sample program?

A: When you run the program without debugging it performs the two operations, MOV (move) and ADD (addition) and returns 0 and ends the whole process. In debugging form however, one can see the process in which the values in the registry are manipulated, in this case 5 is moved to the registry EAX and thusly EAX will hold 00000005. When 6 is added to 5 in EAX through the ADD operation, EAX will hold 0000000B. EIP and EFL will change for both instances too but I have no idea as of right now what they truly signify in terms of those two operations.