PROJ 5: Using Jasmin To Run x86 Assembly Code

Prof. Alberto LaCava **CY -640**

MALWARE ANALYSIS & DEFENSE

Nikhil Patel 09/27/2022

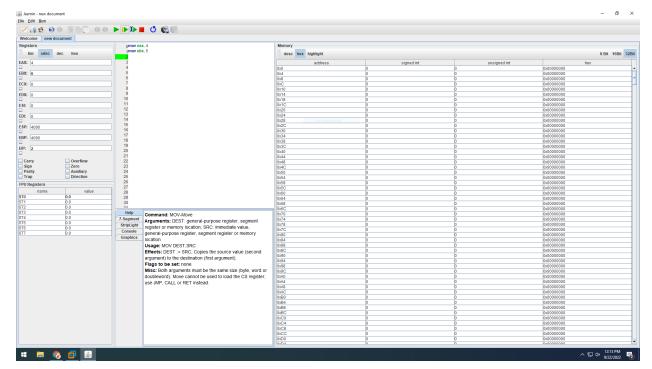
Introduction: In this lab, we will execute x86 assembly code using a jasmin interpreter and learn about how jasmin works.

Procedure:

- Go to Downloads and search for jamin-1.5.8.jar file and then extract that file.
- Launch the exe file and click on file/New files.

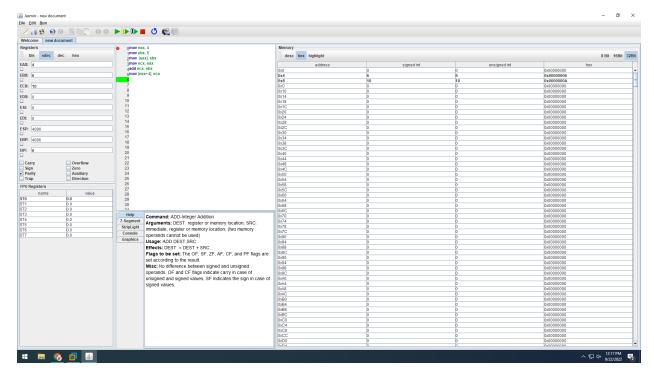


- Now we will perform a Mov function.
- Type the below command in code filed :
 - mov eax, 4
 - mov ebx, 6
- After that click on Run to execute the code.



Storing Results in Memory

- Now we will perform more codes in the same field. Type :
 - mov eax, 4
 - mov ebx, 6
 - mov [eax], ebx
 - mov [ecx], eax
 - mov ecx, eax
 - add ecx, ebx
 - mov [eax + 4], ecx
- After typing the above code click the button right next to run until the green bar crosses the last code.

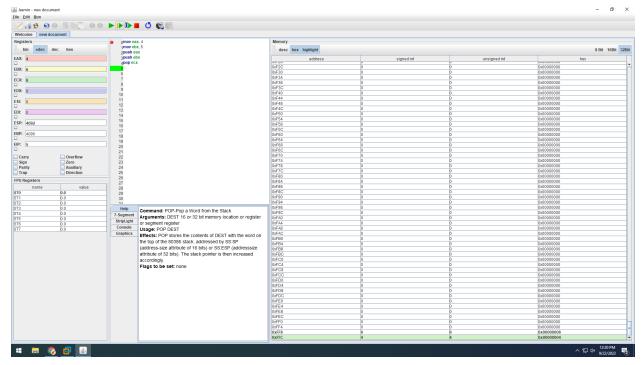


Using the Stack

- Type the below command in the code field and click step two times to execute.
 - mov eax, 4
 - mov ebx, 6
 - push eax
 - push ebx
- You will see the change in register, take a screenshot of that value.

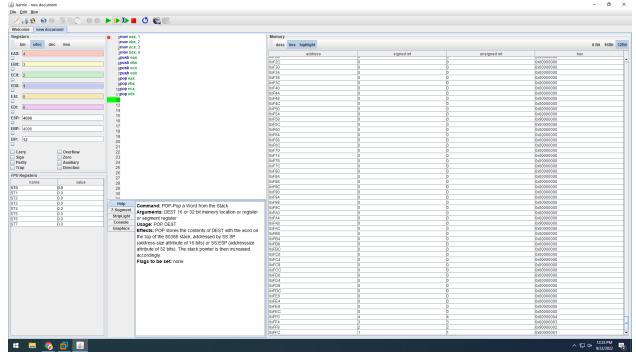
Understanding Pop

- Type the below command in the code field and click run.
 - mov eax, 4
 - mov ebx, 6
 - push eax
 - push ebx
 - Pop ecx
- You will see the change in register, take a screenshot of that value.

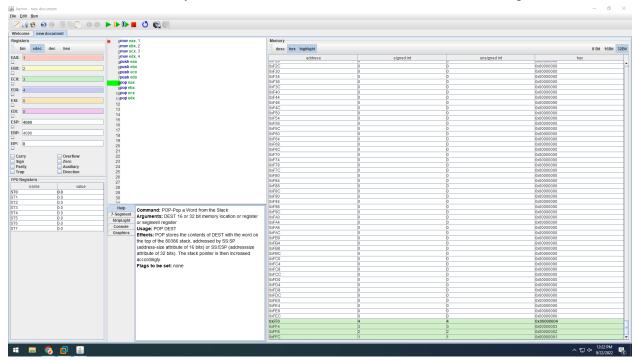


Reversing a Sequence

- Go to file/New file.
- Type the below command in the code field and click Step four time to execute the first four instructions.
 - mov eax, 1
 - mov ebx, 2
 - mov ecx, 3
 - mov edx, 4
 - push eax
 - push ebx
 - push ecx
 - push edx
 - pop eax
 - pop ebx
 - pop ecx
 - pop edx



- After you are complete with mov now we will execute push, for that click step four times. Then same for pop command.
- You will see the change in register, take a screenshot of each value every code you execute because different code has different output.



Conclusion: To conclude this lab, we learned how to run x86 assembly code using a jasmin interpreter, as well as the Push, Pop, and Move commands.