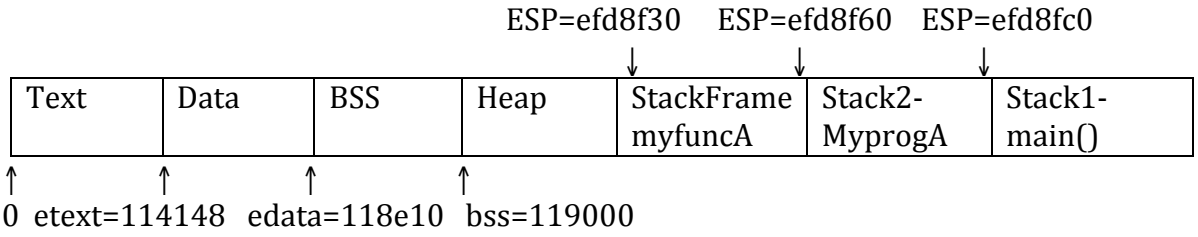
Lab1Answers

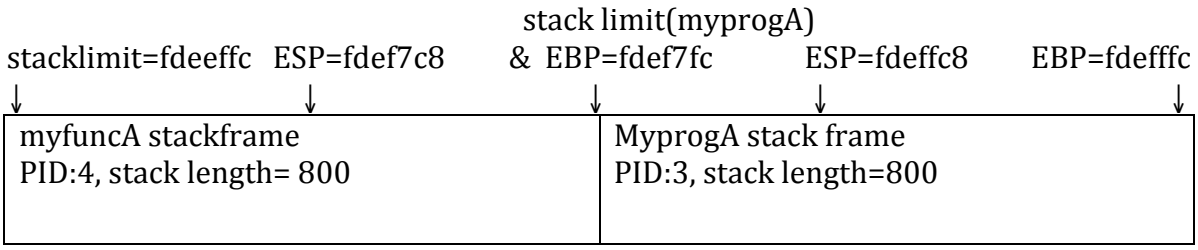
Problem 4:

1.

MEMORY LAYOUT



2.



STACK LAYOUT OF 2 USERS PROCESSES

Question 5:

Due to nested function calls, the stack of program B overflows and enters the stack of program A. Due to which it does not print remaining a and A. Because of termination condition in nested function call, there is interruption and xinu traps occur. Hence, I observed that if stack of one-process fills up with enough parameters provided by a function then it jumps into the stack of the other consecutive process and overrides it. This was the reason program A stopped printing a, A and nested function call overrided the stack.

Question 6:

In order to hijack the process A, we have to override the return address of the function (somefuncA) in process A with the address of roguefuncB. We have to override the return address of somefuncA with the address of roguefuncB, which will process A to branch to roguefuncB and will not allow somefuncA to print a and A.