Problem 4
4.2
a. main process before appl1():
Base of the stack : Address - 0x0EFD8FFC, Value - 0xFFFFFFA9
Top of the stack : Address - 0x0EFE8FFC, Value - 0x0000FFA9

b. after appl1() is created before fun1() is called:
Base of the stack : Address - 0x0FDEFFFC, Value - 0xFFFFFFA9
Top of the stack : Address - 0x0FDEFFD8, Value - 0x00000070

c. after appl1() calls fun1() and before fun1() returns:
Base of the stack : Address - 0x0FDEFFFC, Value - 0xFFFFFFA9
Top of the stack : Address - 0x0FDEFFB8, Value - 0x00000070

d. after appl1() calls fun1() and after fun1() has returned:
Base of the stack : Address - 0x0FDEFFFC, Value - 0xFFFFFFA9
Top of the stack : Address - 0x0FDEFFD8, Value - 0x00000070

The base of the stack is always the same in the same process. The top of the stack decreases when a new process is created.

Problem 5
stackoverflowA recursively calls itself, thus it is essentially an infinite loop of callbacks. this will basically hang the entire system. The victim process will print one B before the attacker takes over.