Vincent Maggioli

Lab 2

4.2

From my results, parts 2 and 4 contain the same data. This makes sense because part 2 is in the appl1() function and so is part 4. The only difference is whether fun1() has been called, which doesn't matter in this case since that stack doesn't exist in either of these parts. Another key point to note is that the bottom of the stack changed from main() to appl1() but not appl1() to fun1(). This is because appl1() is a new process, so a new stack is created. The movement to fun1() is shown through the top of the stack location.

5

My strategy with stack smashing solely was to hang the victim process. This meant overwriting the return address of the stack and not to attempt to place any address of my own there. So, to do that as fast as possible to ensure it gets over written, I performed nested recursion calls to reach the return address area and overwrite it.