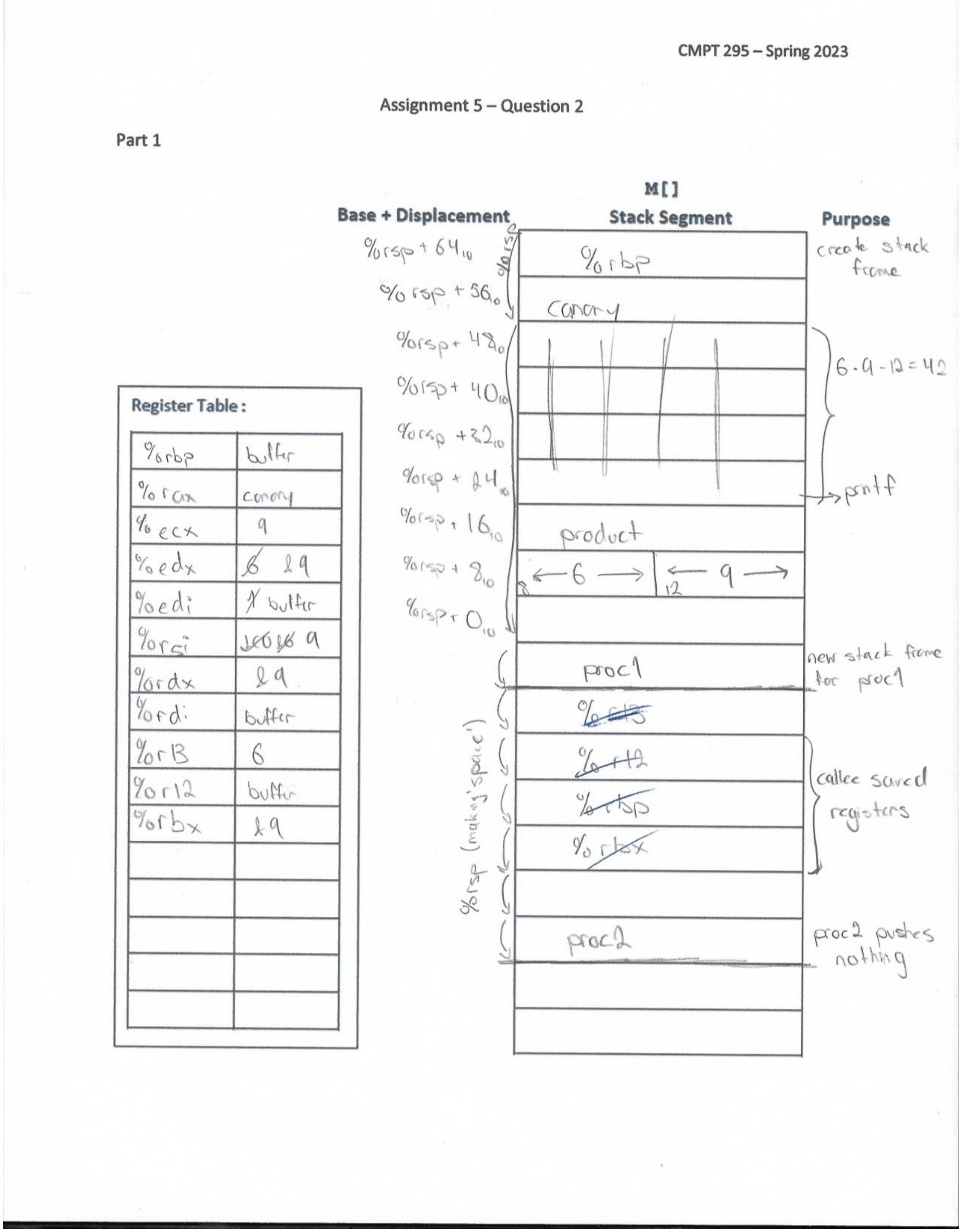
Assignment 5 – Question 2

Part 1



CMPT 295 – Spring 2023

Assignment 5 – Question 2

Part 1

M[]

Base + Displacement	Stack Segment	Purpose
%rsp + 64_{10}	%rbp	create stack frame
%rsp + 56_{10}	canary	
%rsp + 48_{10}		6 · 9 · 12 = 42
%rsp + 40_{10}		
%rsp + 32_{10}		
%rsp + 24_{10}		printf
%rsp + 16_{10}	product	
%rsp + 8_{10}	8 ← 6 → | 12 ← 9 →	
%rsp + 0_{10}		
	proc1	new stack frame for proc1
	~~%r13~~	
	~~%r12~~	callee saved registers
	~~%rbp~~	
	~~%rbx~~	
	proc2	proc2 pushes nothing

%rsp

%rsp (making 'space')

Register Table :

%rbp	buffer
%rax	canary
%ecx	9
%edx	~~6~~ &9
%edi	~~1~~ buffer
%rsi	~~160~~ ~~16~~ 9
%rdx	&9
%rdi	buffer
%r13	6
%r12	buffer
%rbx	&9

Part 2

What happens to the **canary** value when you reduce the size of `buf` from `40` down to 24, and `x = 6`, `y = 9`?

Original values: x=6, y=9 where 69=54

Final values: x=7, y=6 where 76=42

The buffer itself overwrites the buffer when it gets brought down from 40 to 24. Because the buffer is small, the p1.c function containing sprintf which overwrites the canary value. With these final values, it produces the error stack smashing detected : terminated Aborted (core dumped).