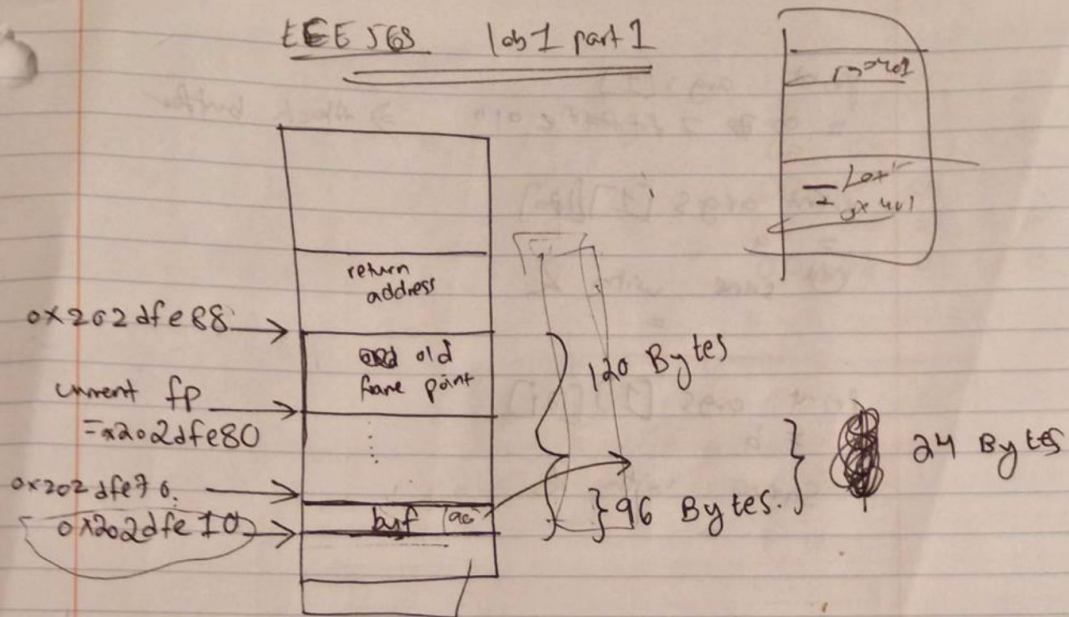
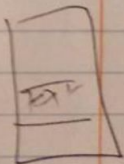


EEE 568 lab 1 part 1

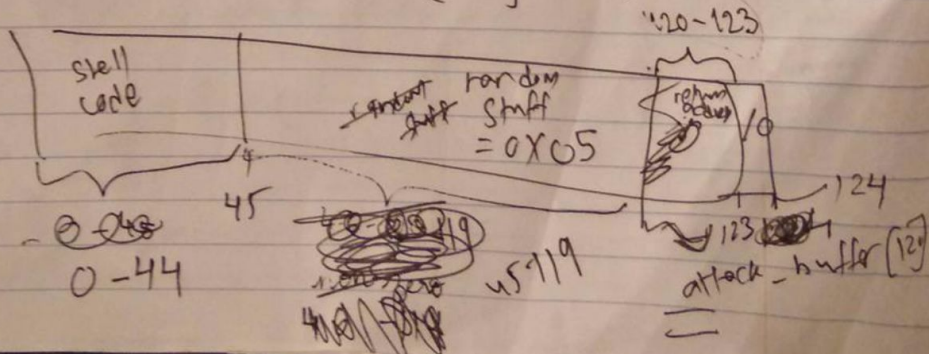


$$\begin{aligned}
 &0x202dfe88 - 0x202dfe10 \\
 &= 53988512 \\
 &= 539885192 - 539885072 \\
 &= 120 \text{ Bytes}
 \end{aligned}$$

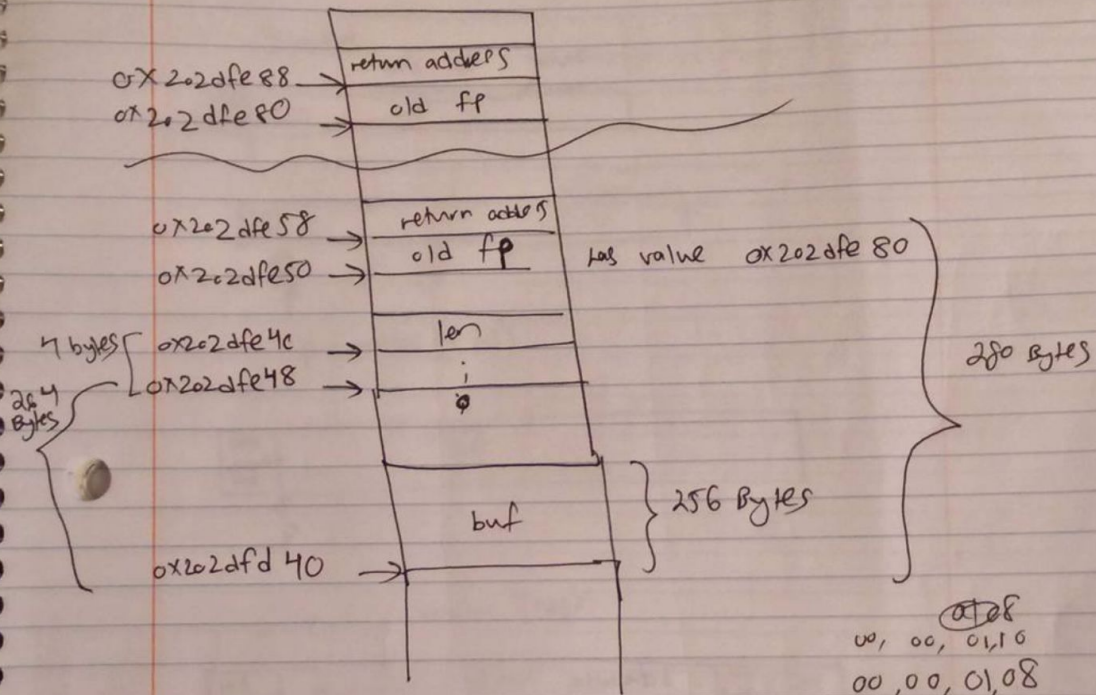


$$\begin{aligned}
 &539885072 + 96 = \\
 &= 539885168 \text{ which is } 0x202dfe70
 \end{aligned}$$

attack buffer (124) RA = 0x202dfe70



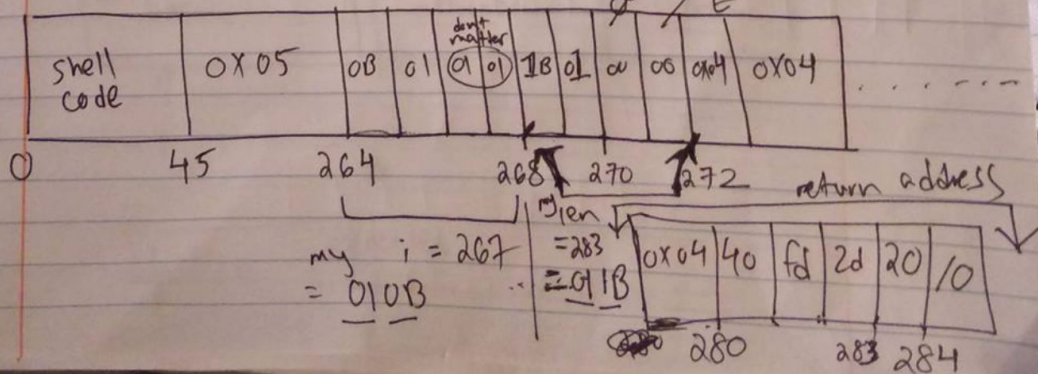
~~Lab 1 part 1~~
Lab 1 part 2



0x28
 00, 00, 01, 00
 00, 00, 01, 08

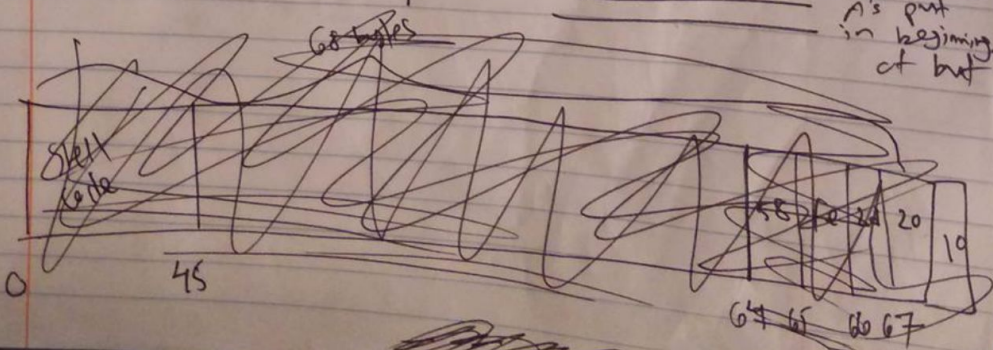
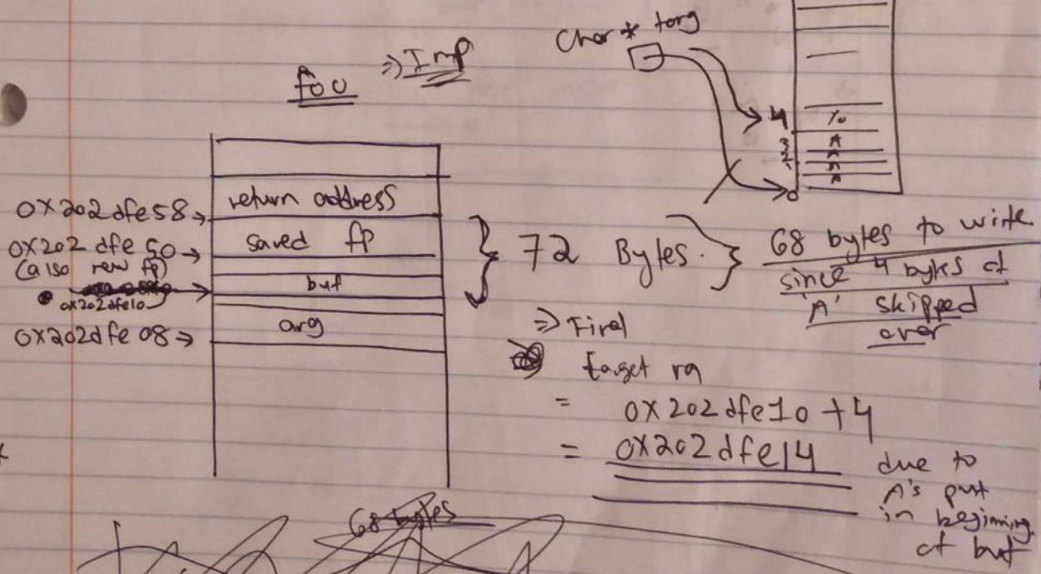
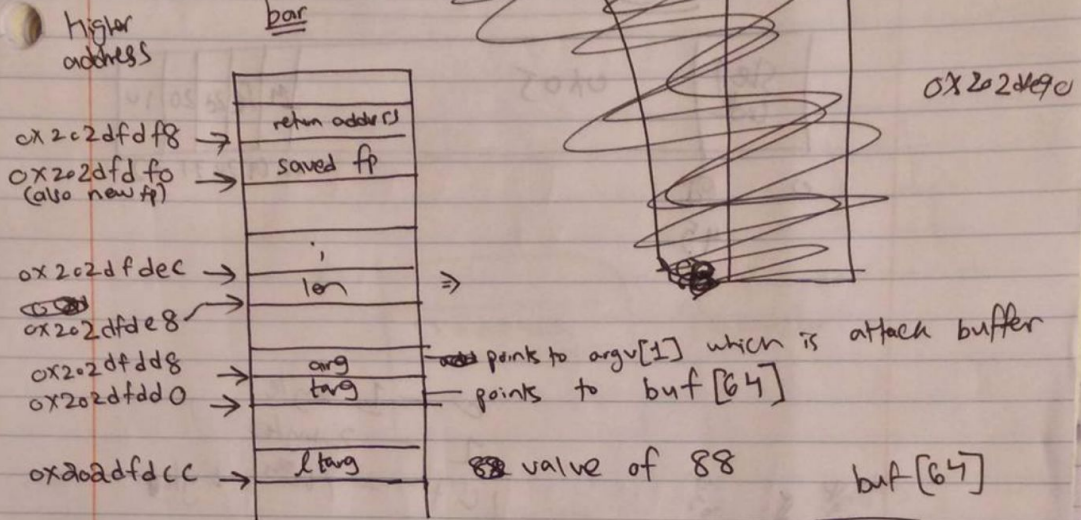
Attack Buffer
 rest i = 264 → 272 real len = 272 = 0110

08 01 00 00 10 01 00 00 env[0] env[1] on words



Full notes

Lab 1 part 3, overwrite buf



first

~~first~~ attach buffer

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	45														

- 0 - 1 byte
- 1 - 2 bytes
- 157 - 160 bytes

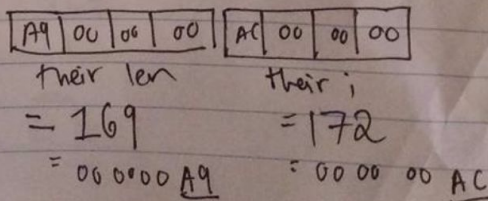
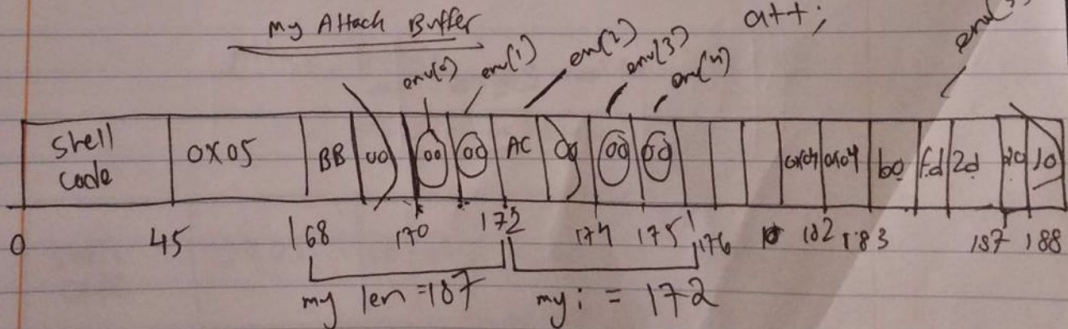
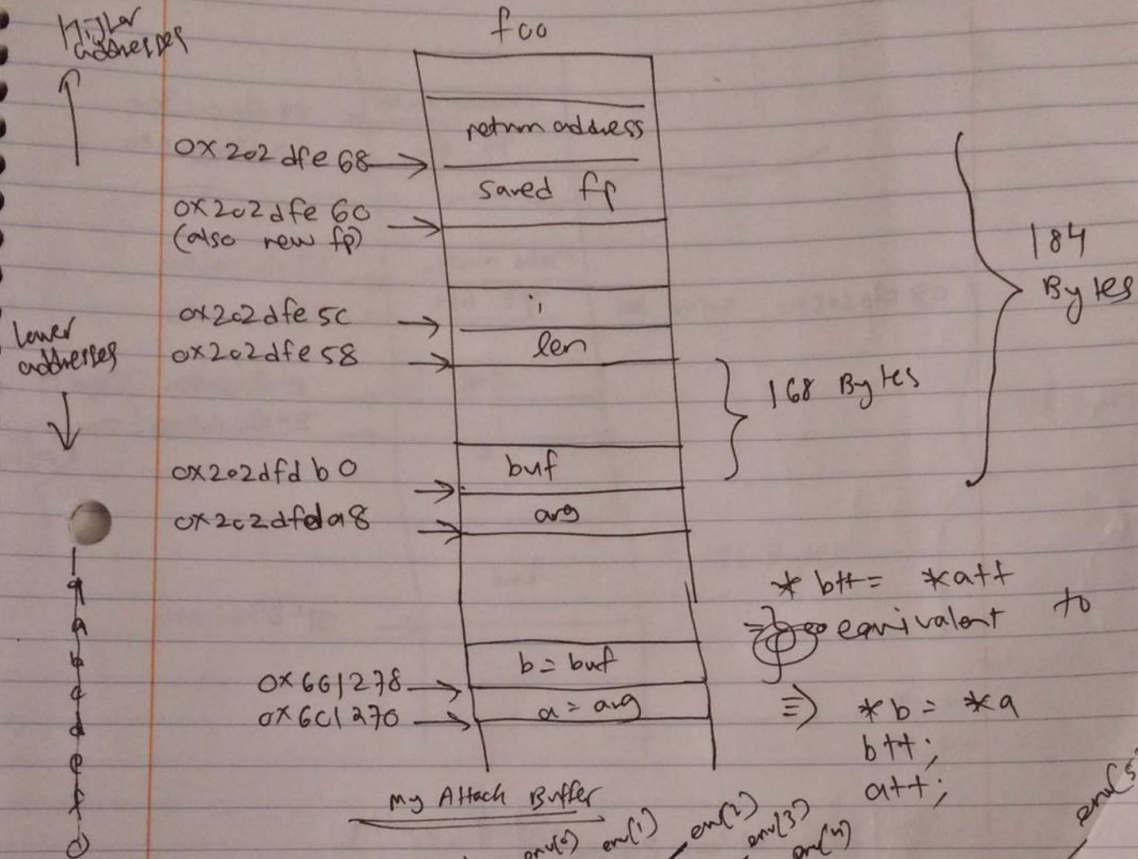
- 0 - 1 byte
- 1 - 2 bytes
- 157 - 160 bytes

Lab 1 part 4

full notes

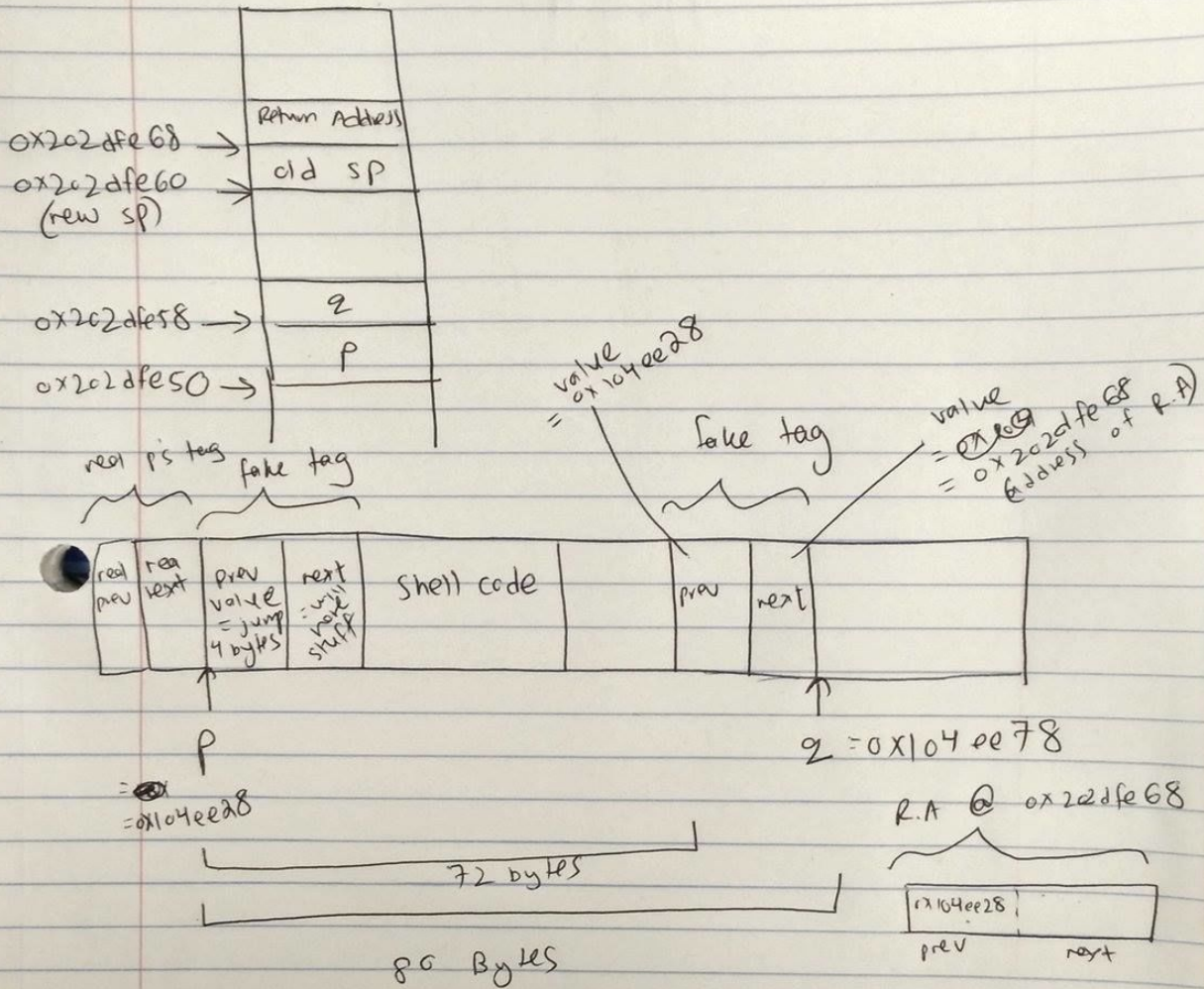
$\text{arr}[i] = 0x7fffff\dots fd$ "is there"

foo



Lab 1 ~~part~~ Part 6

foo



what free does

tag = 2 - sized tag

tag → next → prev = tag → prev;
tag → prev → next = tag → next;