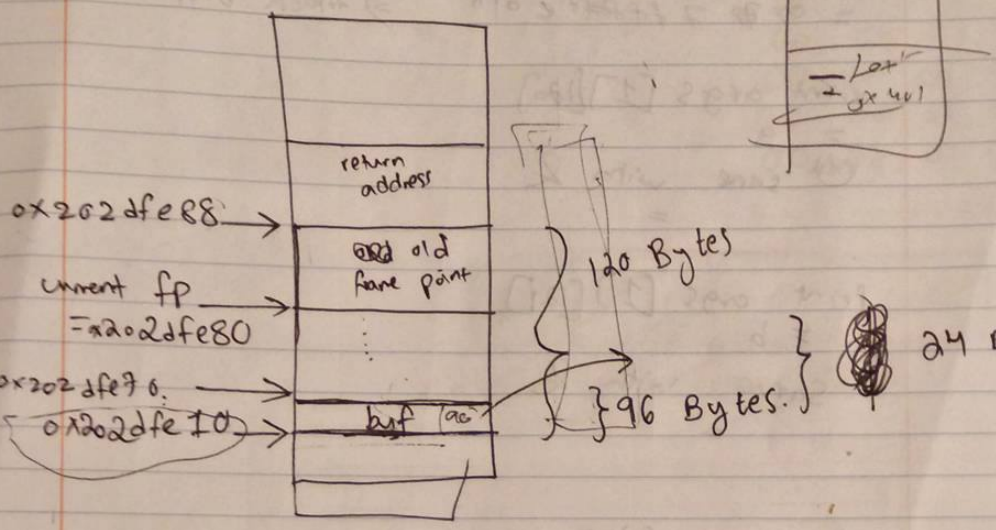
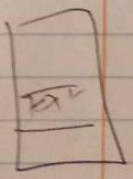
EE 568 lab 1 part 1

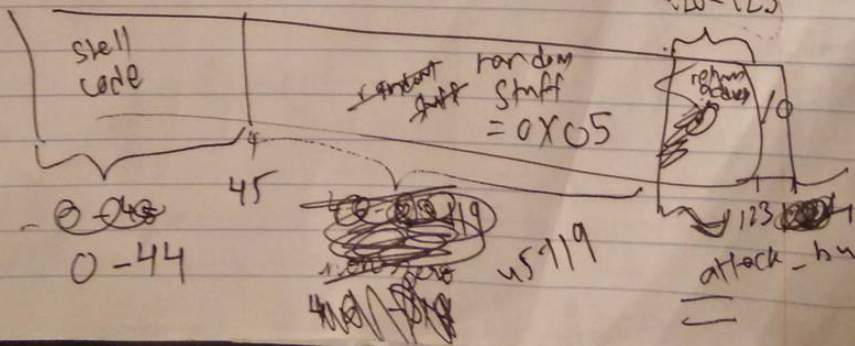


0x202dfe88 - 0x202dfe10
~~= 539885192~~
= 539885192 - 539885072
= 120 Bytes



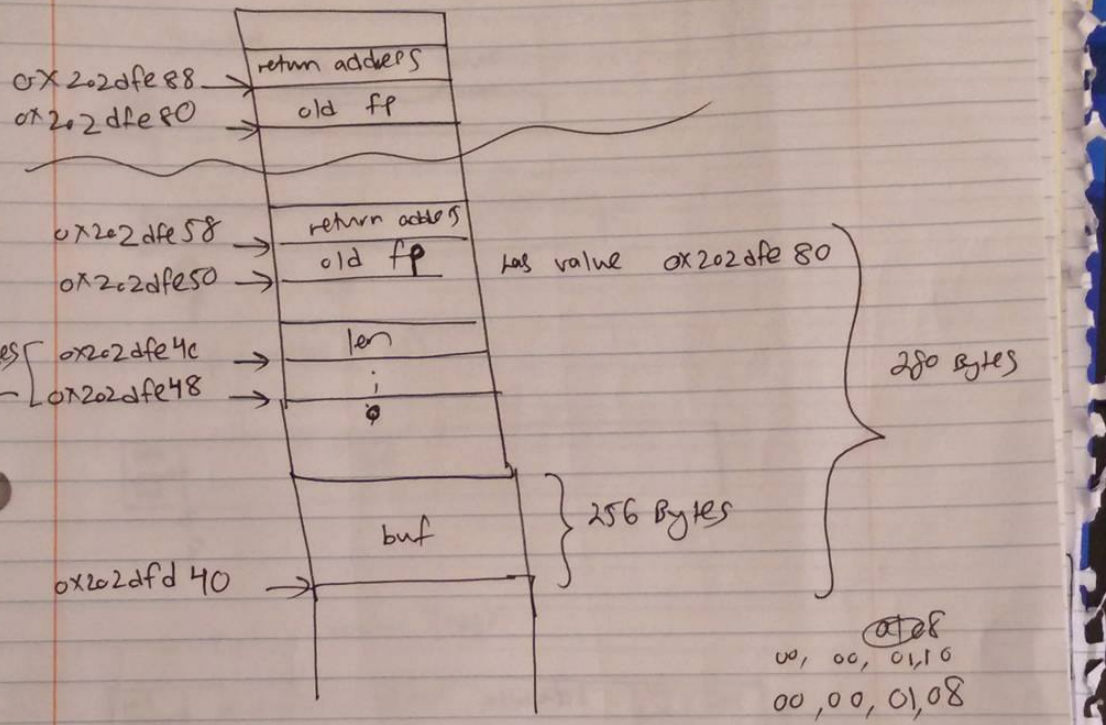
539885072 + 96 =
= 539885168 which is 0x202dfe70

attack buffer[124] = RA = 0x202dfe10



~~Lab #1 part #~~

Lab 1 part 2

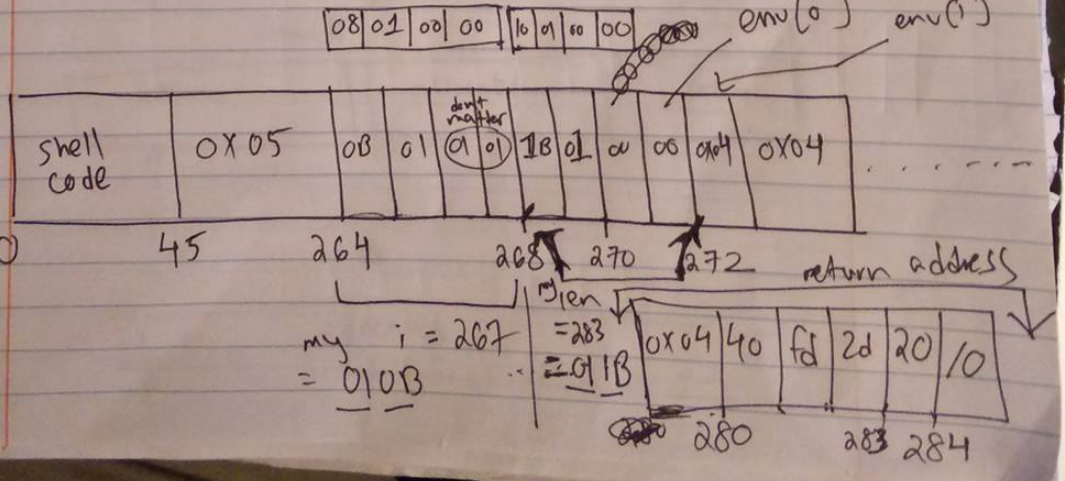


00, 00, 01, 10

00, 00, 01, 08

Attack Buffer

real i = 264 = 108 real len = 272 = 01 10

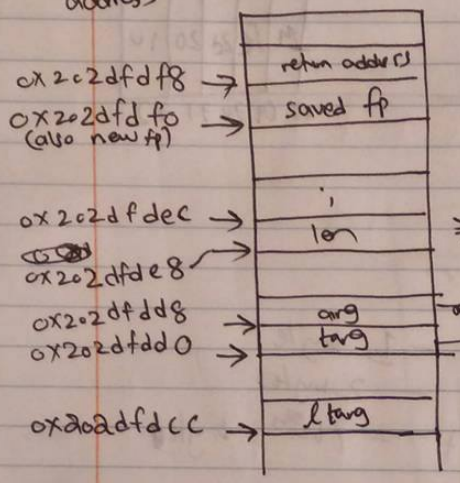


Call 2 of 3

Lab 1 part 3 } overwrite buf

higher address

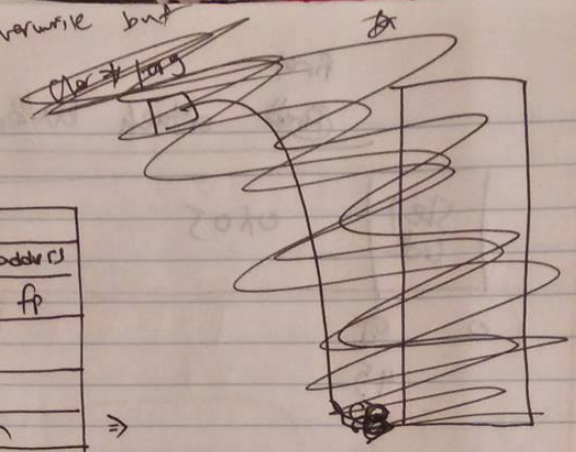
bar



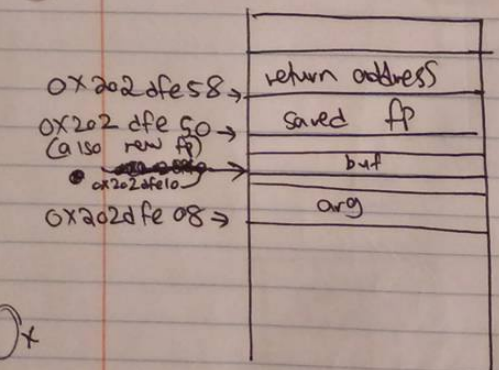
⇒ points to argv[1] which is attack buffer

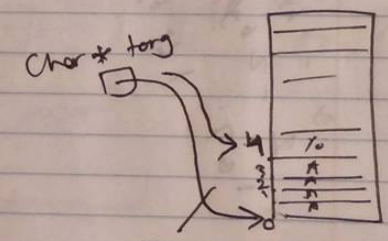
targ points to buf[64]

value of 88



foo ⇒ Imp



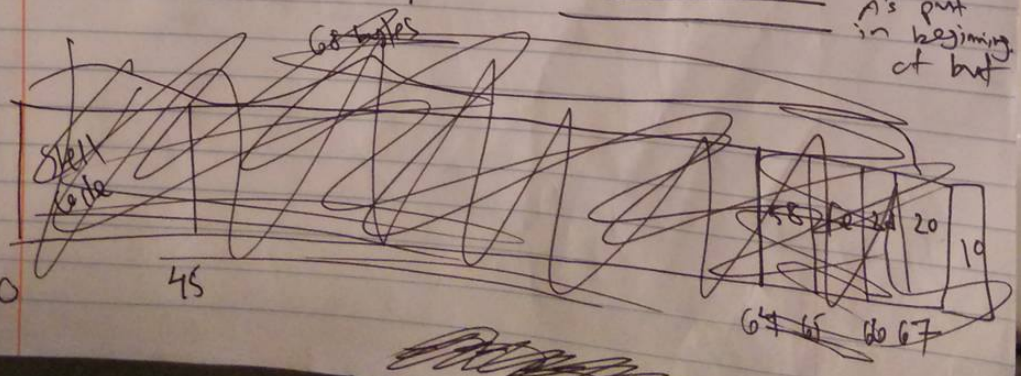


⇒ Final target ra

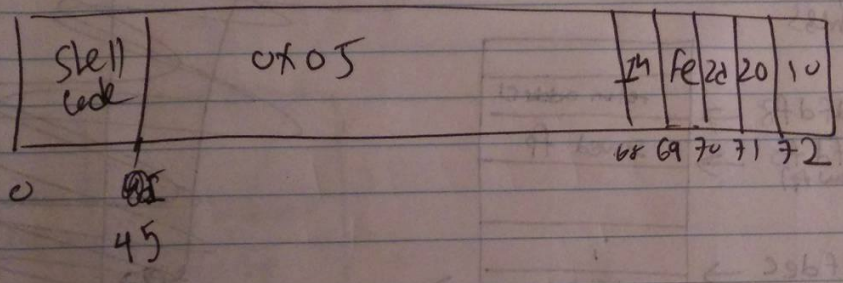
= 0x202dfe10 + 4

= 0x202dfe14

due to A's put in beginning of buf



final attack buffer



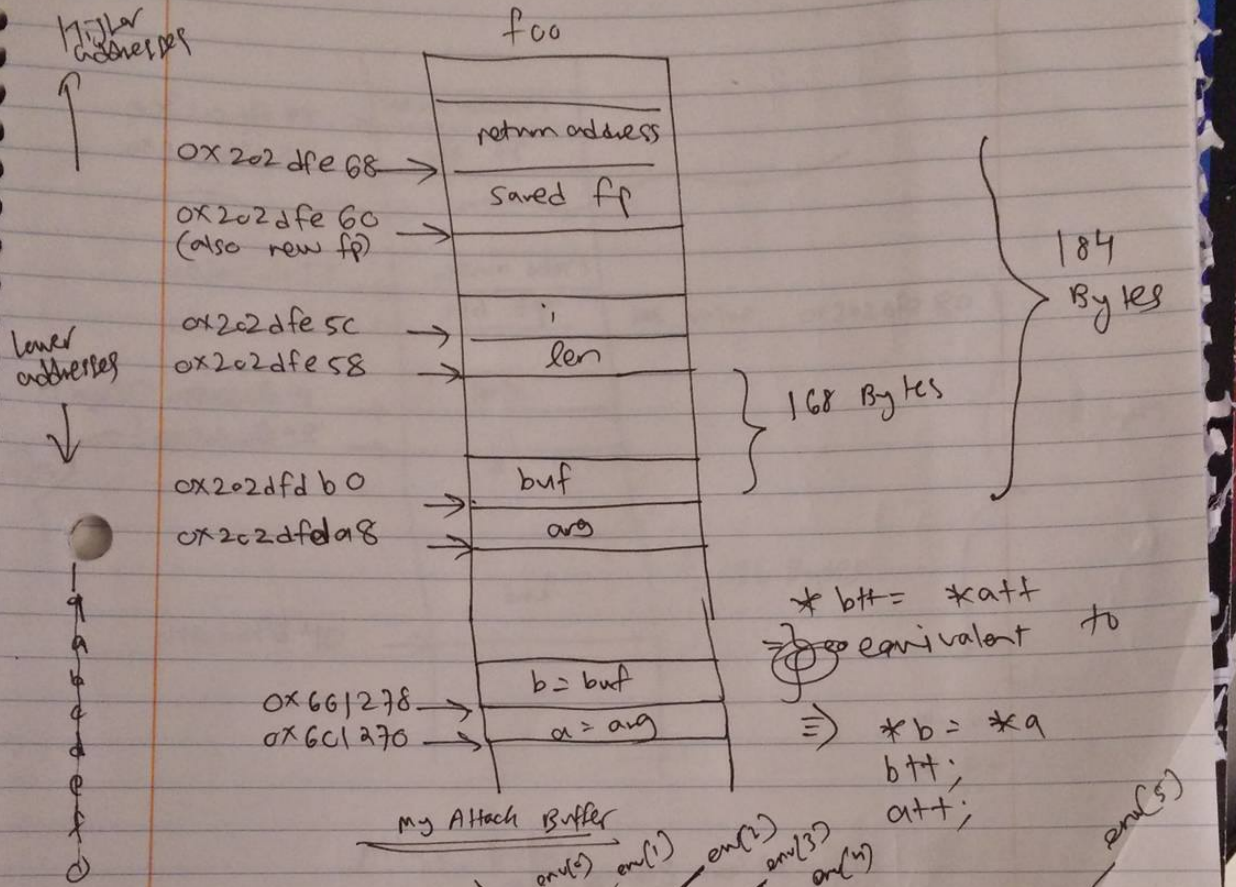
0 - 1 byte
1 - 2 bytes
127 - 128 bytes

0 - 1 byte
1 - 2 byte
127 - 128 byte

Lab 1 part 4

full notes

argv[1] = 0x7fffff...efd "Hi there"

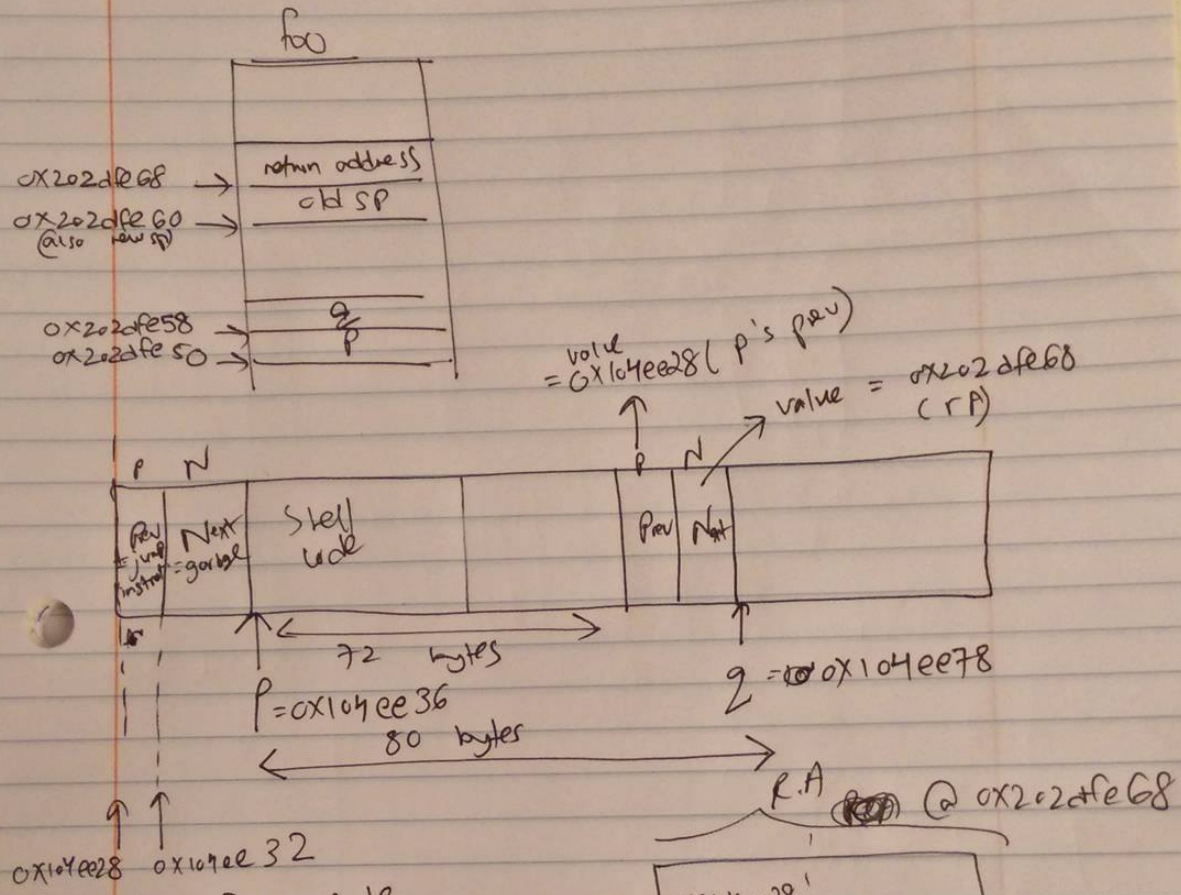


A9	00	00	00	AC	00	00	00

their len = 169 = 00 00 00 A9

their i = 172 = 00 00 00 AC

Lab1 part6



free code

tag = q - tag size

~~tag -> prev~~

tag -> next -> prev = tag -> prev;

tag -> prev -> next = tag -> next;