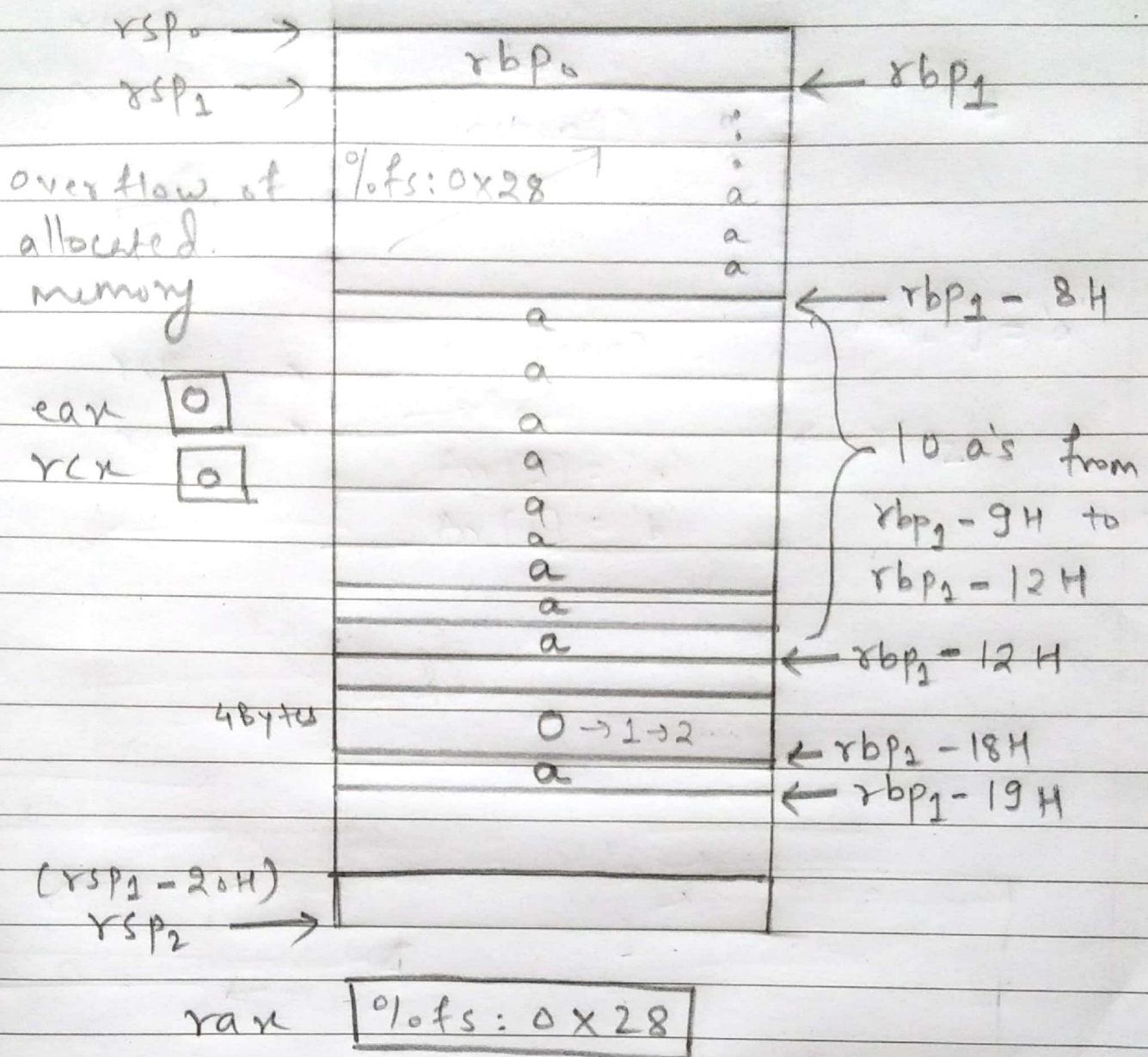


ACTIVATION RECORD FOR STACK SMASH



`movzbl %dl, -0x12(%rbp, %rax, 1)`

Meaning: - move 'a' to the following address -

$(rbp - 12H) + rax \times 1$

rax content goes from 0 to 13H

Thus, `%fs: 0x28` is overwritten by 'a' and stack smash takes place.