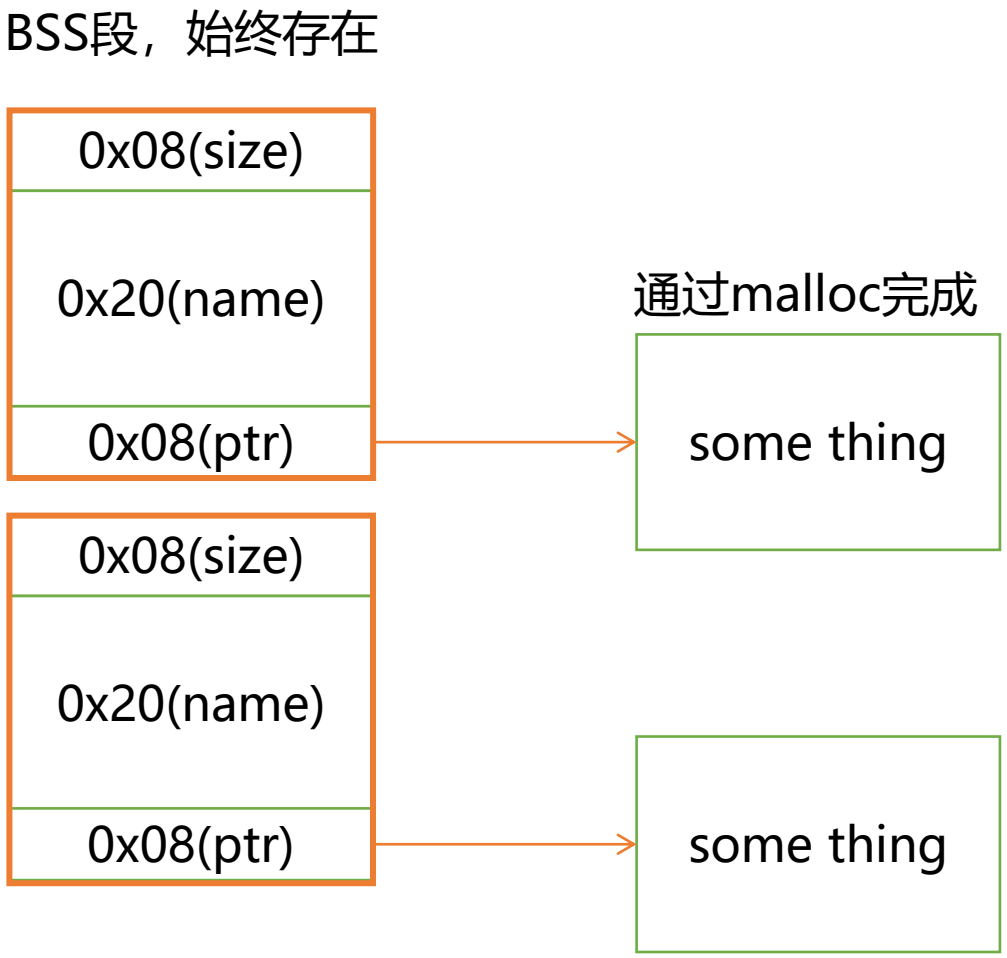
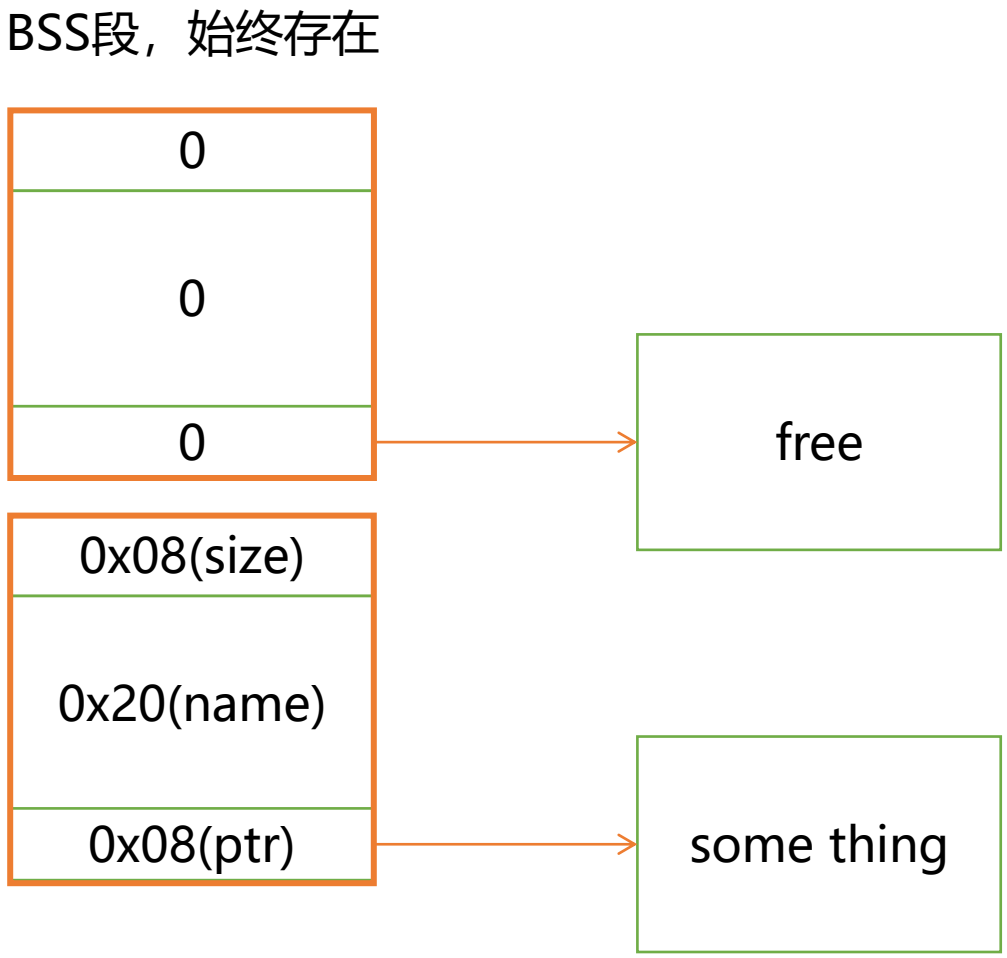
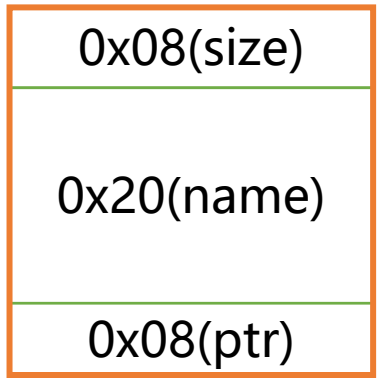

BSS段，始终存在
0x08(size)
0x20(name)
0x08(ptr)
通过malloc完成
some thing
0x08(size)
0x20(name)
0x08(ptr)
some thing

插入

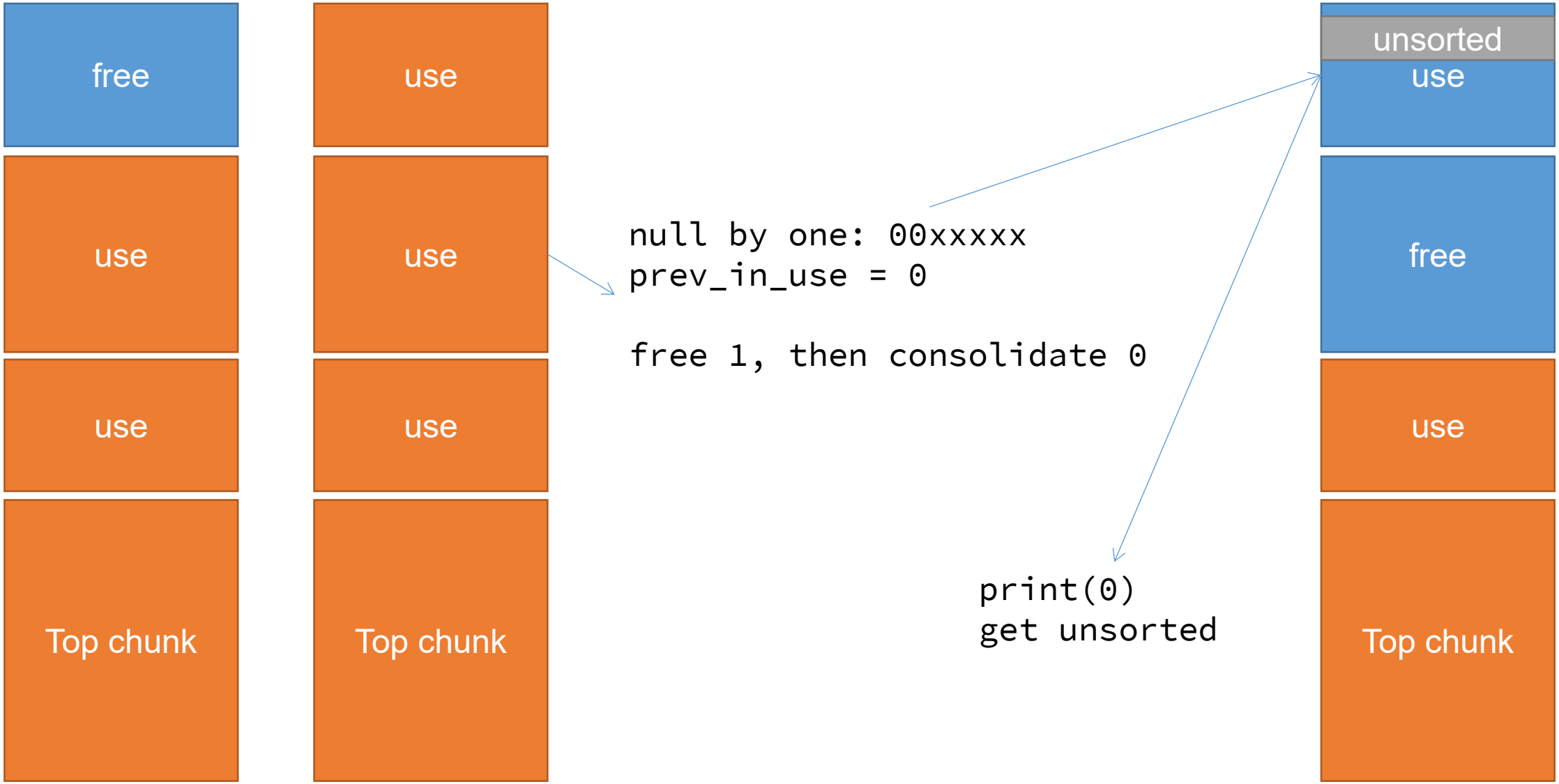

BSS段，始终存在
0
0
0
free
0x08(size)
0x20(name)
0x08(ptr)
some thing

删除

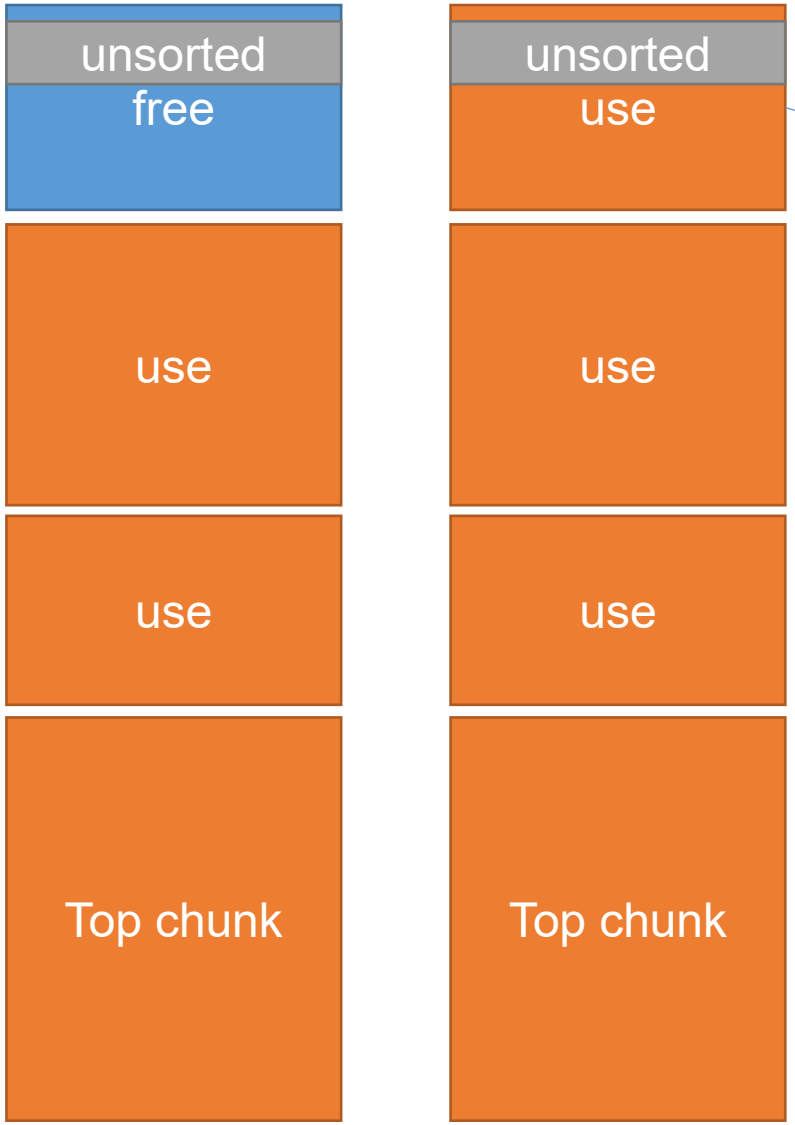
泄露Heap基址：填满name，print_name就会把ptr也输出，ptr指向堆，搞定



泄露Libc基址：利用null by one, 然后chunk consolidate

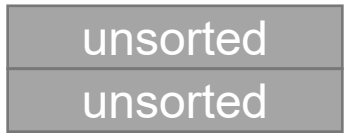


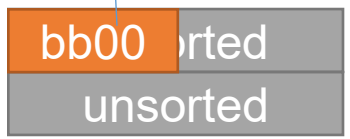
泄露Libc基址：另一种想法，错误



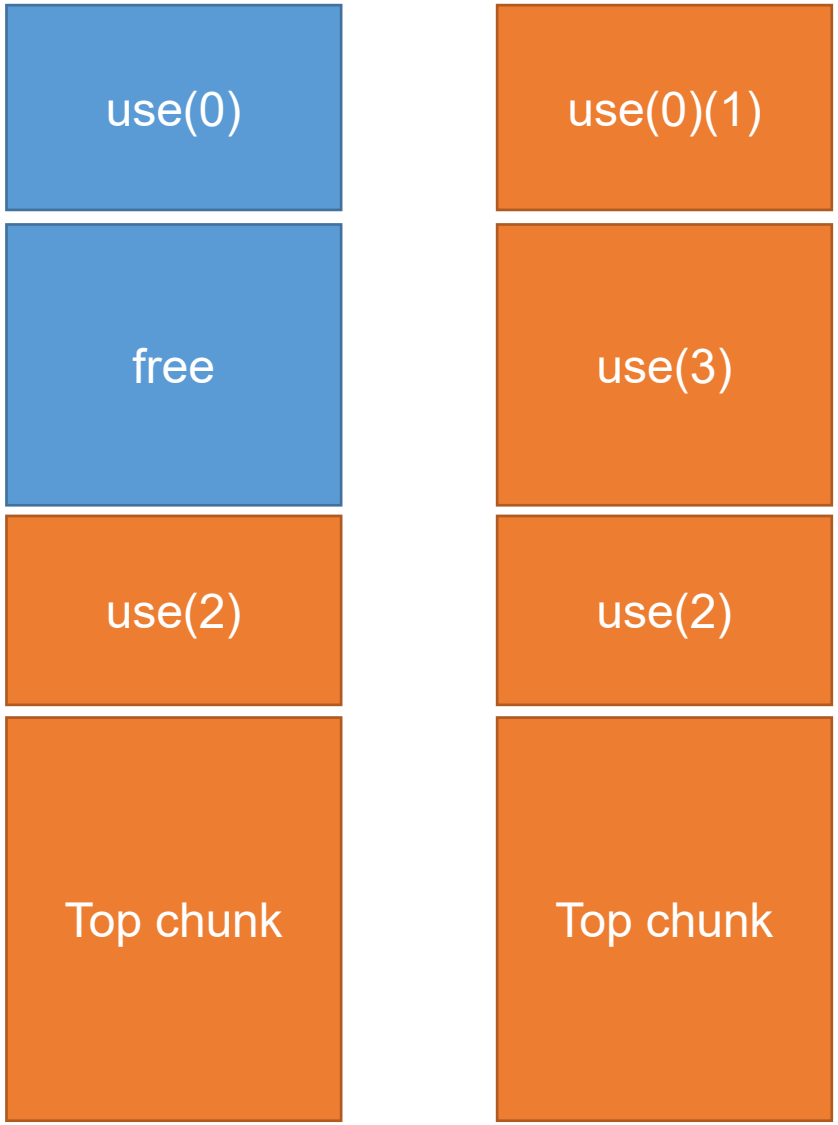
直接Print...感觉就可以了呀...

找到原因了，首先要知道有null by one
也就是最后会添一个0
尝试打印unsorted的时候，肯定会遇到0，然后停止，所以GG





泄露Libc基址之后？可以看到，我们可以Free掉已经Free的块，这不就是Double Free吗...




```
free(2), free(0), free(1)

Fast bin: 1->2->0, OK~
```

剩下的就不多说了把
one_gadget --> stdout / malloc_hook，都可以