堆分配与堆块合并

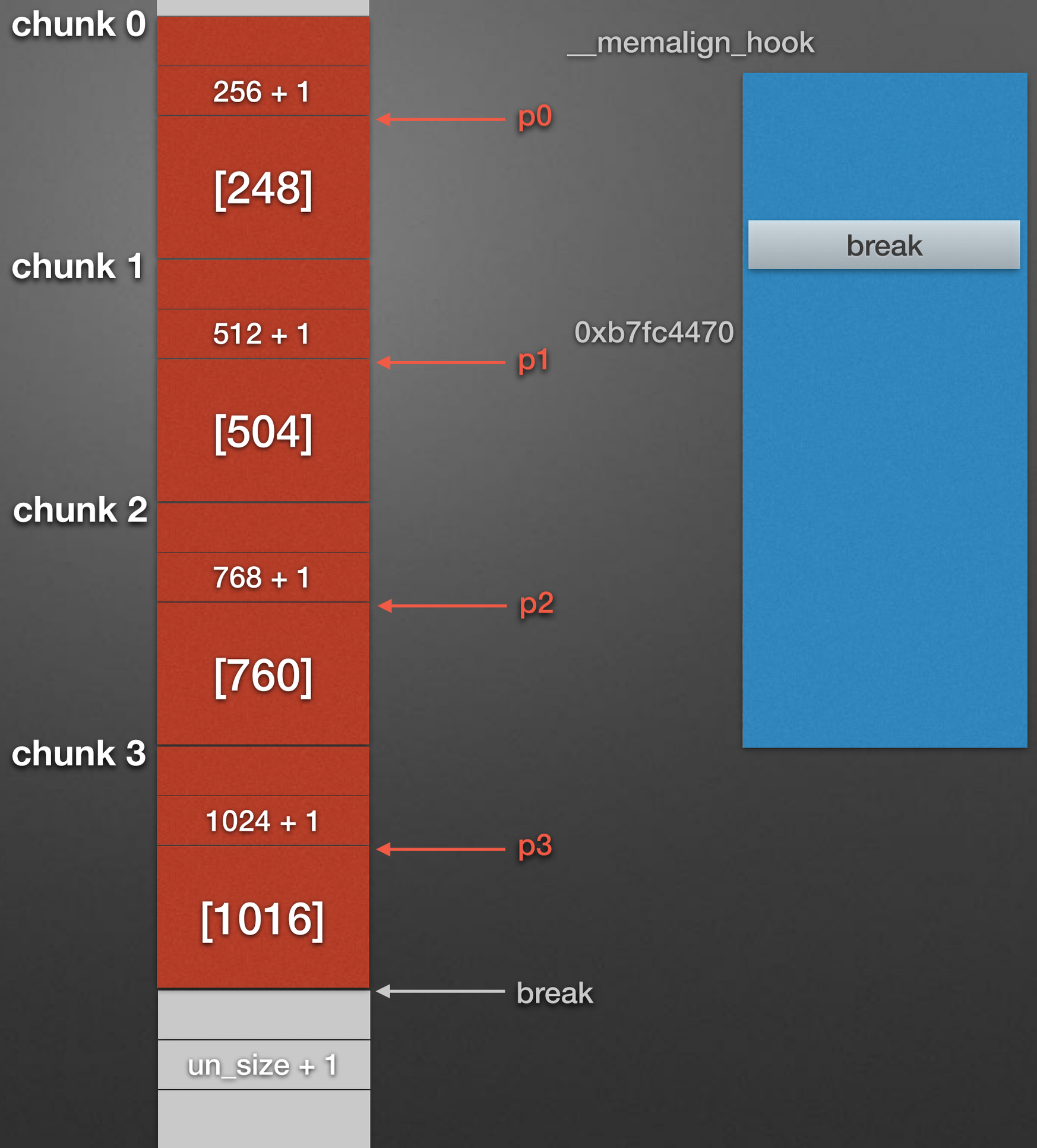
Step.1

p0 = malloc(248)

p1 = malloc(504)

p2 = malloc(760)

p3 = malloc(1016)



Step.2
free(p0)

chunk 0

256 + 1

0xb7fc4470

0xb7fc4470

chunk 1

256

512 + 0

[504]

chunk 2

768 + 1

[760]

chunk 3

1024 + 1

[1016]

p1

p2

p3

break

un_size + 1

__memalign_hook

break

0xb7fc4470

0x0804c000

0x0804c000

Step.3
free(p2)

chunk 0

chunk 1

chunk 2

chunk 3

256 + 1

0xb7fc4470

0x0804c300

256

512 + 0

[504]

768 + 1

0x0804c000

0xb7fc4470

768

1024 + 0

[1016]

un_size + 1

p1

p3

break

__memalign_hook

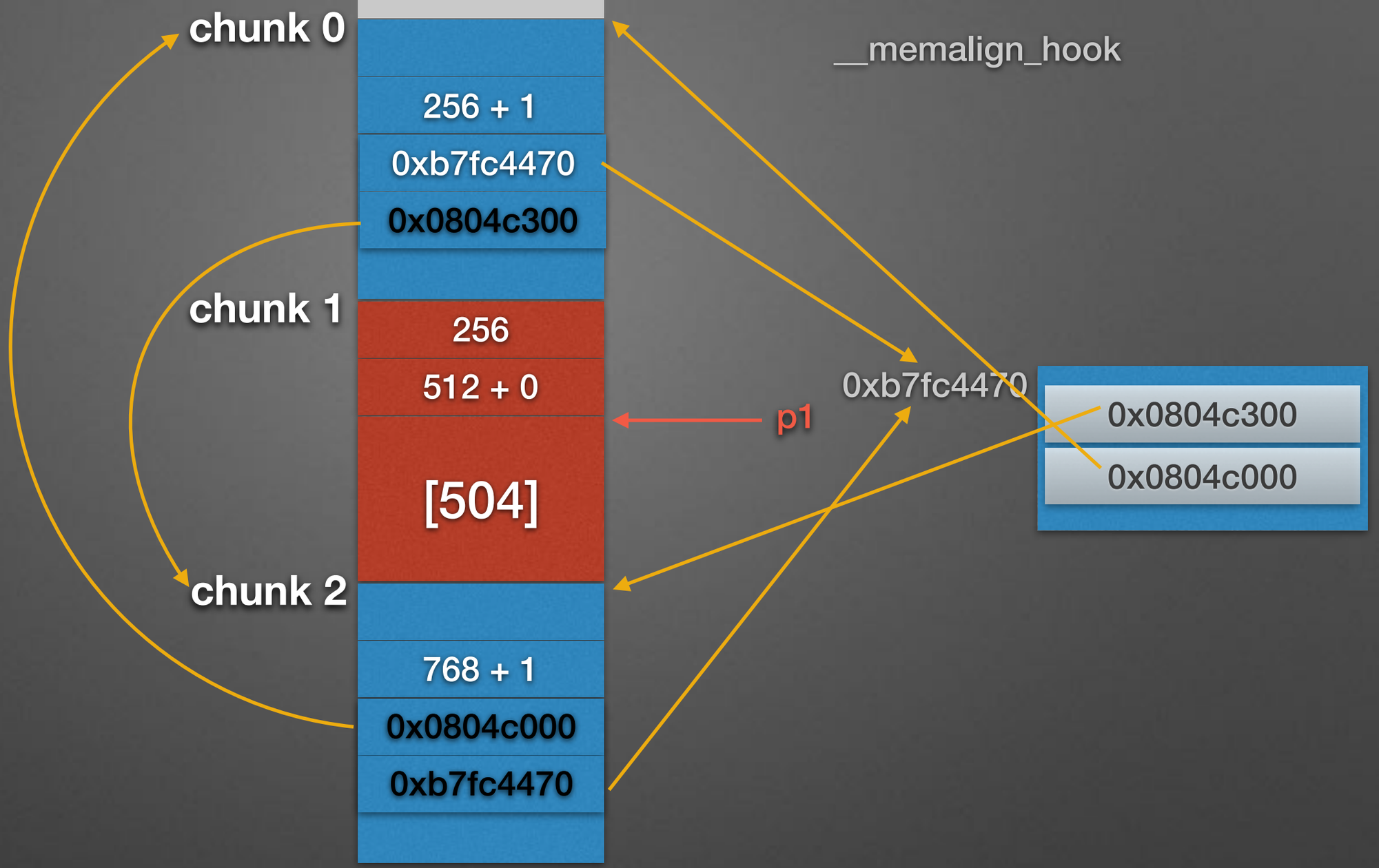
break

0xb7fc4470

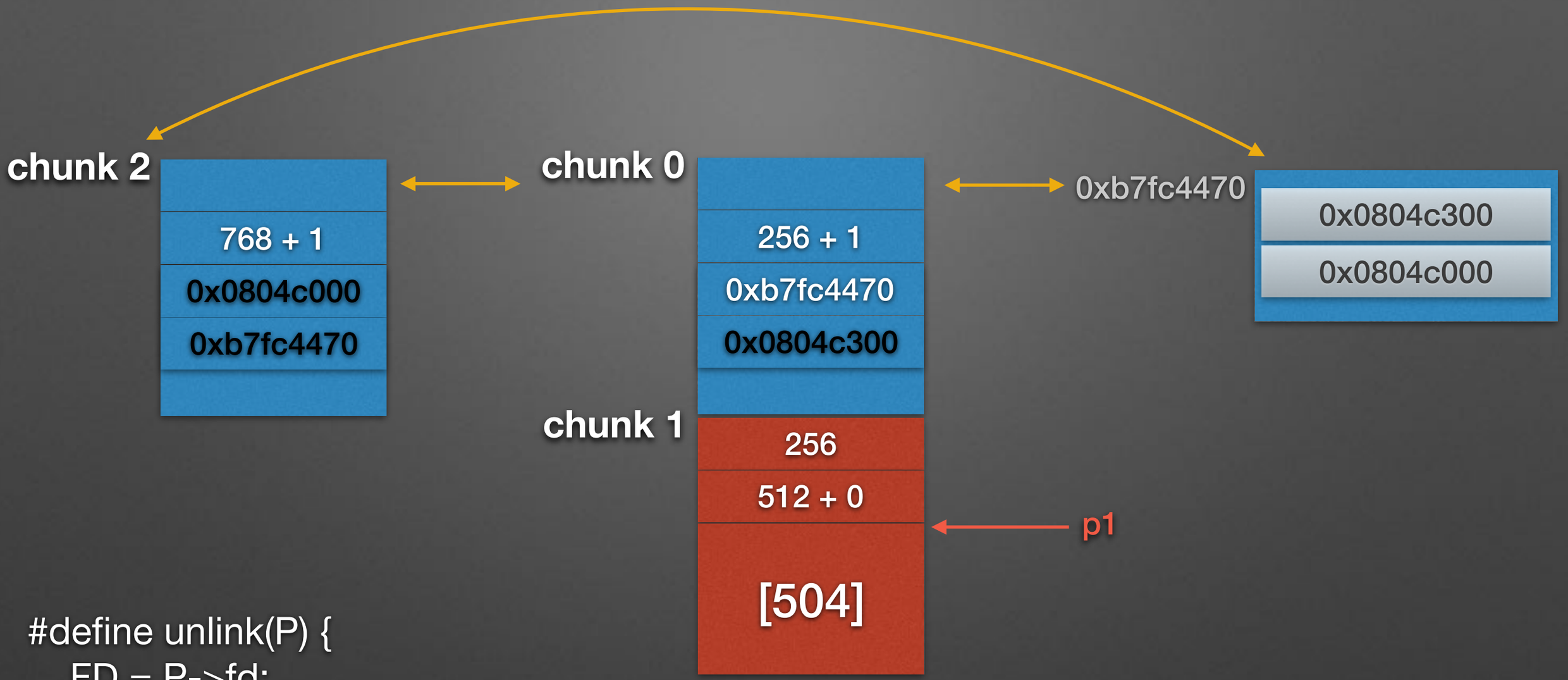
0x0804c300

0x0804c000

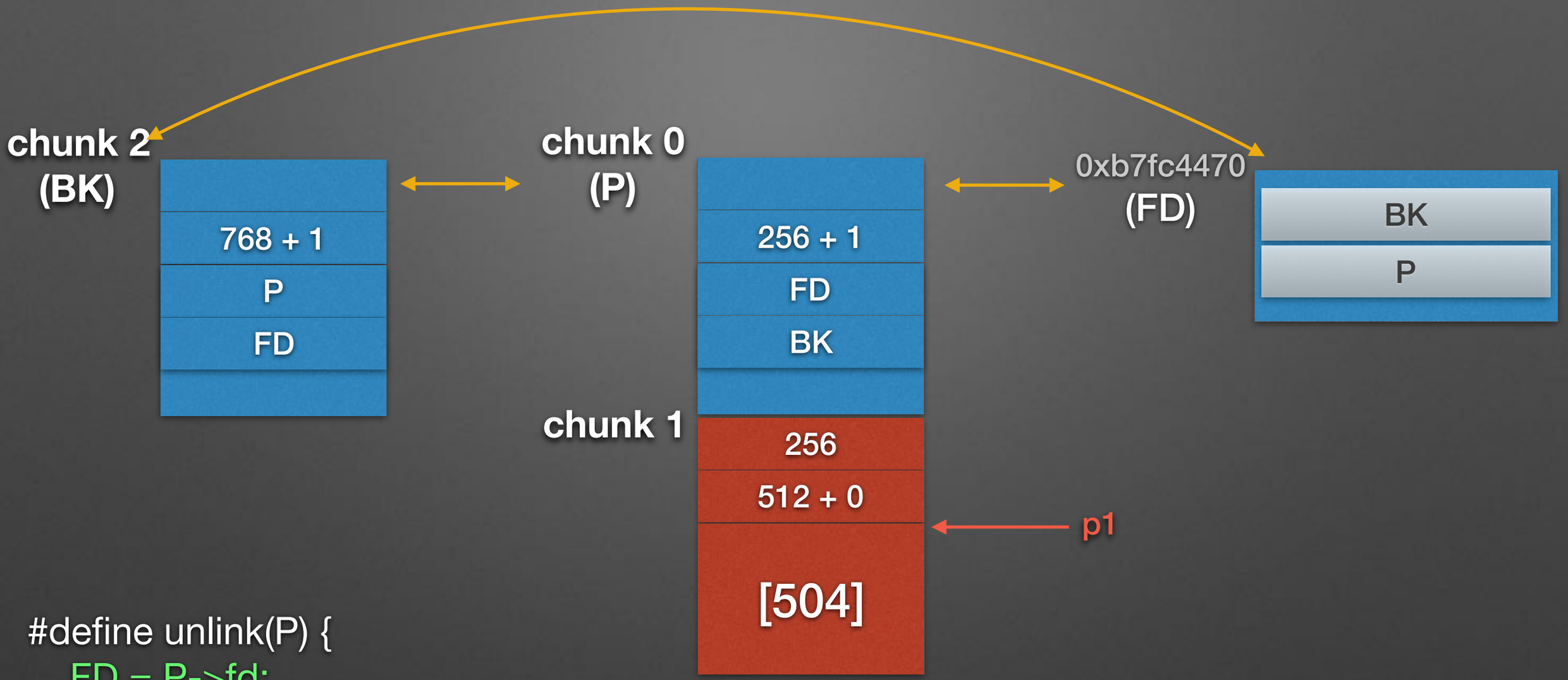
Step.4
free(p1)



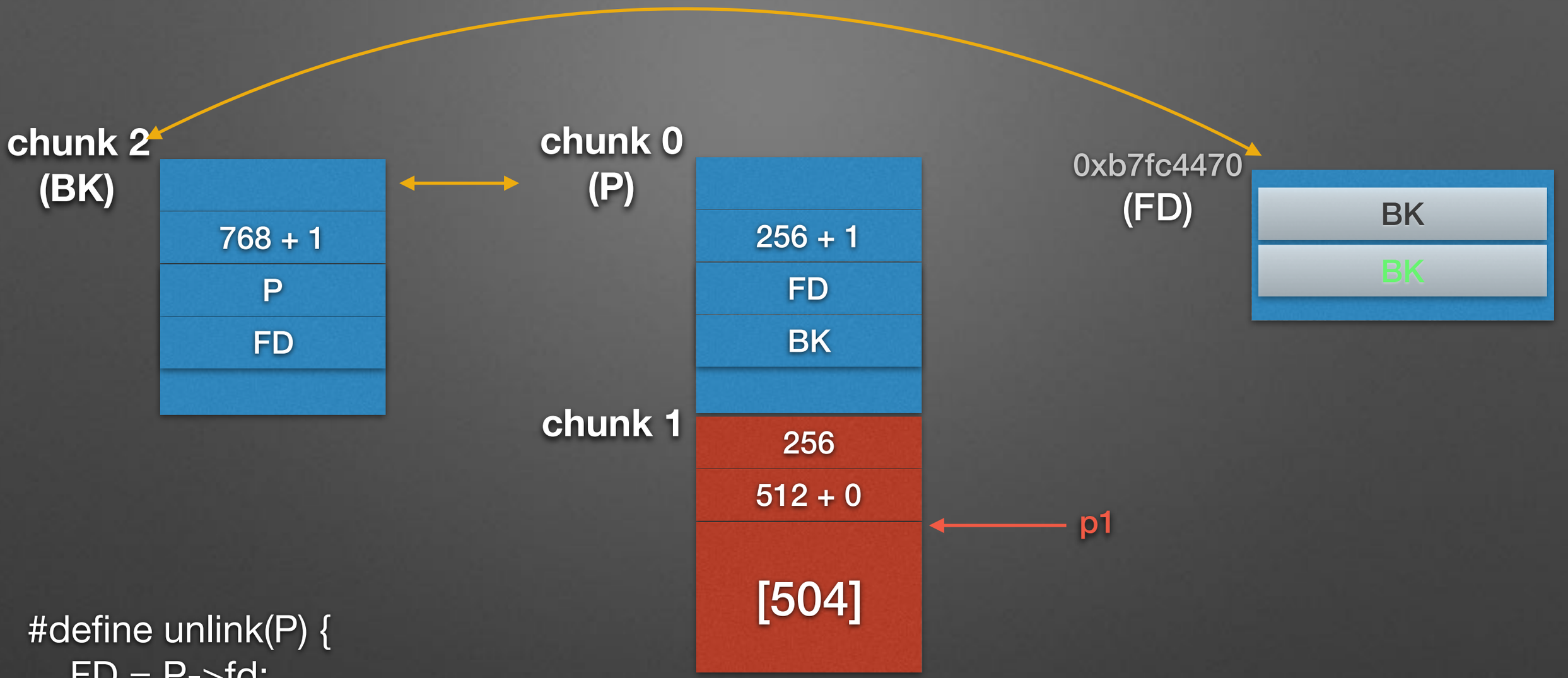
空闲堆块合并



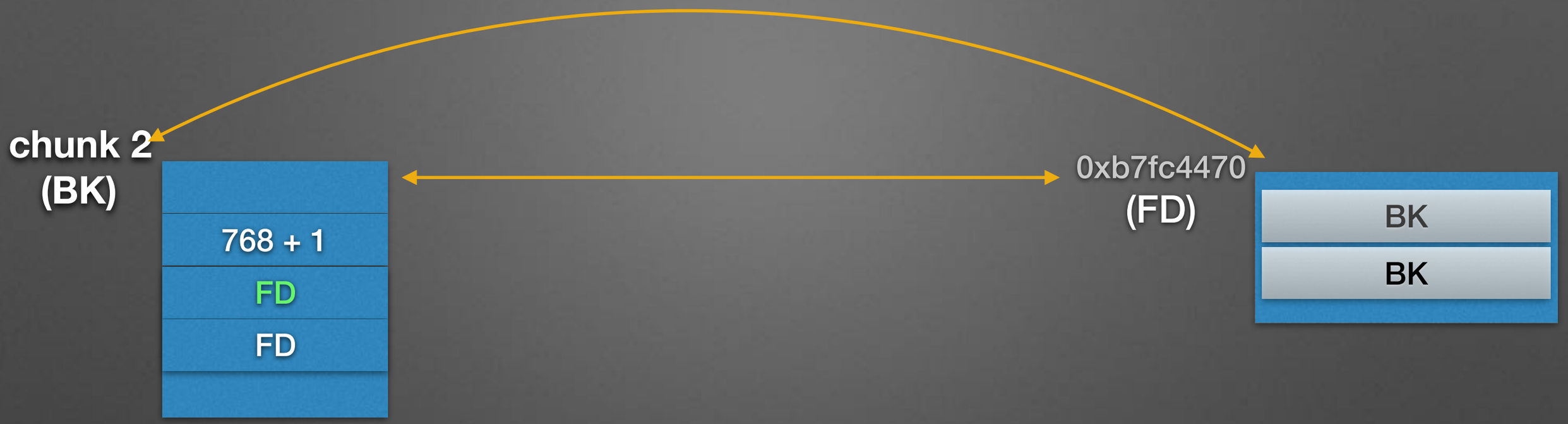

```
#define unlink(P) {
    FD = P->fd;
    BK = P->bk;
    FD->bk = BK;
    BK->fd = FD;
    ...
}
```



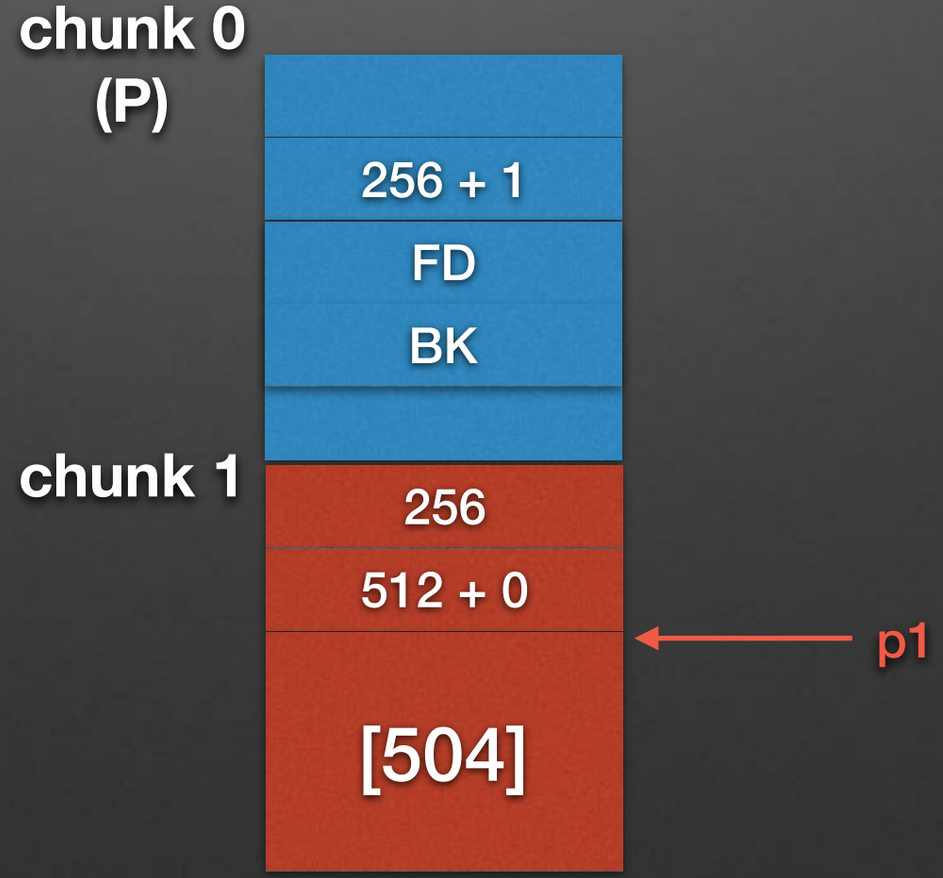

```
#define unlink(P) {
    FD = P->fd;
    BK = P->bk;
    FD->bk = BK;
    BK->fd = FD;
    ...
}
```

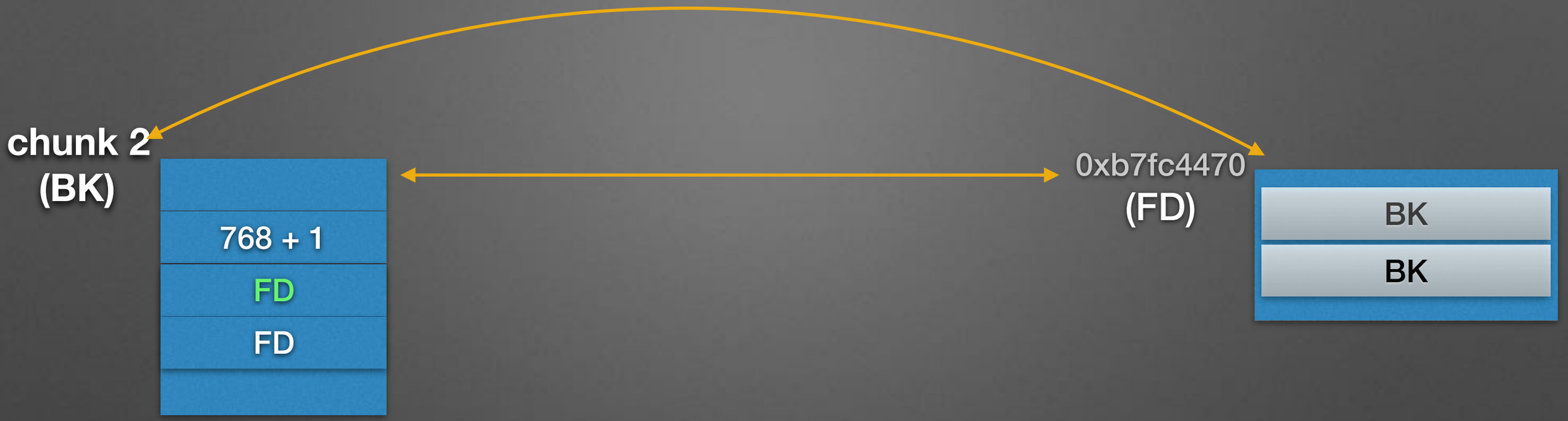


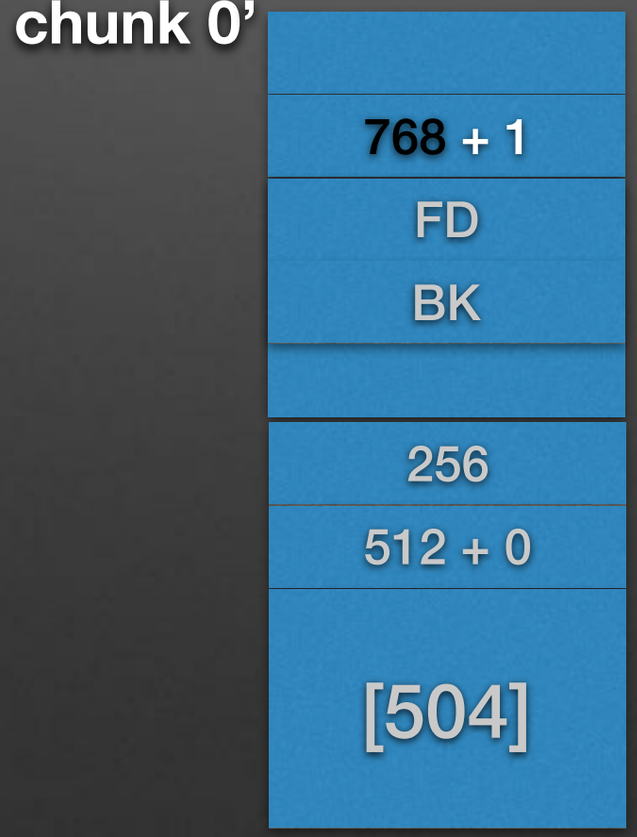

```
#define unlink(P) {
    FD = P->fd;
    BK = P->bk;
    FD->bk = BK;
    BK->fd = FD;
    ...
}
```




```
#define unlink(P) {
    FD = P->fd;
    BK = P->bk;
    FD->bk = BK;
    BK->fd = FD;
    ...
}
```




chunk 2
(BK)
768 + 1
FD
FD
0xb7fc4470
(FD)
BK
BK


chunk 0’
768 + 1
FD
BK
256
512 + 0
[504]

Step.4

free(p1)

chunk0’= chunk0 + chunk1

chunk 0’

768 + 1

0xb7fc4470

0x0804c300

256

512 + 0

[504]

chunk 2

768 + 1

0xb7fc4470

0xb7fc4470

chunk 3

768

1024 + 0

[1016]

un_size + 1

p3

break

__memalign_hook

break

0xb7fc4470

0x0804c300

0x0804c300

Step.4

free(p1)

chunk0”= chunk0’ + chunk2

chunk 0”

1536 + 1

0xb7fc4470

0xb7fc4470

256

512 + 0

[504]

768 + 1

0xb7fc4470

0xb7fc4470

chunk 3

1536

1024 + 0

[1016]

un_size + 1

__memalign_hook

break

0xb7fc4470

0x0804c000

0x0804c000

p3

break

Step.5

free(p3)

chunk0”’= chunk0” + chunk3

chunk 0”’

2560 + 1

0xb7fc4470

0xb7fc4470

256

512 + 0

[504]

768 + 1

0xb7fc4470

0xb7fc4470

1536

1024 + 0

[1016]

2560

un_size + 0

break

__memalign_hook

break

0xb7fc4470

0xb7fc4470

0xb7fc4470

0xb7fc4470

Step.5
free(p3)

top chunk

break

__memalign_hook

un_size + 1

break

0xb7fc4470

0xb7fc4470

0xb7fc4470

unallocated