fastbin_dup[Korean]

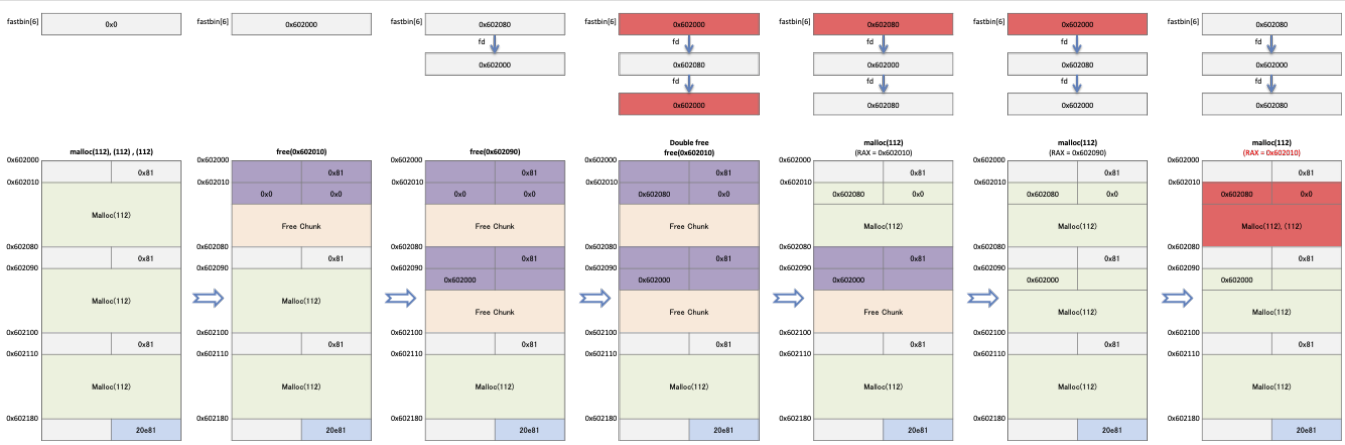
Unknown macro: 'html'

List

Fastbin duplicate

- "Fastbin duplicate" fastbin .
  - fastbin chunk list .
  - chunk , chunk .
  - fastbin .
- malloc() 112byte 3 .
  - free() chunk fastbin[6] .
  - fastbin[6] chunk fd chunk .
  - chunk fastbin[6] list .
  - , Fastbin[6] list " (0x602000) --> (0x602080) --> (0x602000) --> ..." .
- malloc() .
  - Fastbin .
  - .
  - .
- .

Fast dup flow



Example

- malloc() 112byte 3 .
  - buf1,buf2 free() , buf1 .
  - 112byte malloc() 3 .

fast_dup.c

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

int main()
{
        int *buf1 = malloc(112);
        int *buf2 = malloc(112);
        int *buf3 = malloc(112);

        free(buf1);
        free(buf2);
        free(buf1);

        int *buf4 = malloc(112);
        int *buf5 = malloc(112);
        int *buf6 = malloc(112);
}
```

- 0x4005b7 fastbin .
  - 0x4005c6, 0x4005d4, 0x4005e2 malloc() pointer .

Breakpoints

```
lazenca0x0@ubuntu:~/Book/2.fast_dup$ gcc -o fast_dup fast_dup.c
lazenca0x0@ubuntu:~/Book/2.fast_dup$ gdb -q ./fast_dup
Reading symbols from ./fast_dup...(no debugging symbols found)...done.
gdb-peda$ disassemble main
Dump of assembler code for function main:
   0x0000000000400566 <+0>:        push   rbp
   0x0000000000400567 <+1>:        mov    rbp,rsp
   0x000000000040056a <+4>:        sub    rsp,0x30
   0x000000000040056e <+8>:        mov    edi,0x70
   0x0000000000400573 <+13>:        call   0x400450 <malloc@plt>
   0x0000000000400578 <+18>:        mov    QWORD PTR [rbp-0x30],rax
   0x000000000040057c <+22>:        mov    edi,0x70
   0x0000000000400581 <+27>:        call   0x400450 <malloc@plt>
   0x0000000000400586 <+32>:        mov    QWORD PTR [rbp-0x28],rax
   0x000000000040058a <+36>:        mov    edi,0x70
   0x000000000040058f <+41>:        call   0x400450 <malloc@plt>
   0x0000000000400594 <+46>:        mov    QWORD PTR [rbp-0x20],rax
   0x0000000000400598 <+50>:        mov    rax,QWORD PTR [rbp-0x30]
   0x000000000040059c <+54>:        mov    rdi,rax
   0x000000000040059f <+57>:        call   0x400430 <free@plt>
   0x00000000004005a4 <+62>:        mov    rax,QWORD PTR [rbp-0x28]
   0x00000000004005a8 <+66>:        mov    rdi,rax
   0x00000000004005ab <+69>:        call   0x400430 <free@plt>
   0x00000000004005b0 <+74>:        mov    rax,QWORD PTR [rbp-0x30]
   0x00000000004005b4 <+78>:        mov    rdi,rax
   0x00000000004005b7 <+81>:        call   0x400430 <free@plt>
   0x00000000004005bc <+86>:        mov    edi,0x70
   0x00000000004005c1 <+91>:        call   0x400450 <malloc@plt>
   0x00000000004005c6 <+96>:        mov    QWORD PTR [rbp-0x18],rax
   0x00000000004005ca <+100>:        mov    edi,0x70
   0x00000000004005cf <+105>:        call   0x400450 <malloc@plt>
   0x00000000004005d4 <+110>:        mov    QWORD PTR [rbp-0x10],rax
   0x00000000004005d8 <+114>:        mov    edi,0x70
   0x00000000004005dd <+119>:        call   0x400450 <malloc@plt>
   0x00000000004005e2 <+124>:        mov    QWORD PTR [rbp-0x8],rax
   0x00000000004005e6 <+128>:        mov    eax,0x0
   0x00000000004005eb <+133>:        leave
   0x00000000004005ec <+134>:        ret
End of assembler dump.
gdb-peda$ b *0x00000000004005b7
Breakpoint 1 at 0x4005b7
gdb-peda$ b *0x00000000004005c6
Breakpoint 2 at 0x4005c6
gdb-peda$ b *0x4005d4
Breakpoint 3 at 0x4005d4
gdb-peda$ b *0x00000000004005e2
Breakpoint 4 at 0x4005e2
gdb-peda$
```

- fastbins[6] (0x602080) ..
  - chunk fd pointer(0x602000) .
  - fastbin list 0x602080 --> 0x602000.
  - buf1(0x602000) fastbins[6] buf1(0x602000) .
  - fastbin list 0x602000 --> 0x602080 --> 0x602000 .
  - fastbin_dup .

```
gdb-peda$ r
Starting program: /home/lazenca0x0/Book/2.fast_dup/fast_dup

Breakpoint 1, 0x00000000004005b7 in main ()
gdb-peda$ p main_arena.fastbinsY[6]
$1 = (mfastbinptr) 0x602080
gdb-peda$ x/4gx 0x602080
0x602080:        0x0000000000000000        0x0000000000000081
0x602090:        0x0000000000602000        0x0000000000000000
gdb-peda$ x/4gx 0x0000000000602000
0x602000:        0x0000000000000000        0x0000000000000081
0x602010:        0x0000000000000000        0x0000000000000000
gdb-peda$ ni

0x00000000004005bc in main ()
gdb-peda$ x/4gx 0x0000000000602000
0x602000:        0x0000000000000000        0x0000000000000081
0x602010:        0x0000000000602080        0x0000000000000000
gdb-peda$ p main_arena.fastbinsY[6]
$2 = (mfastbinptr) 0x602000
gdb-peda$
```

- malloc() 112byte fastbinsY[6] (0x602010) .
  - fastbinsY[6] (0x602080) .
  - (0x602010) (0x602010) .

fast dup

```
gdb-peda$ c
Continuing.

Breakpoint 2, 0x00000000004005c6 in main ()
gdb-peda$ i r rax
rax            0x602010        0x602010
gdb-peda$ p main_arena.fastbinsY[6]
$3 = (mfastbinptr) 0x602080
gdb-peda$ c
Continuing.

Breakpoint 3, 0x00000000004005d4 in main ()
gdb-peda$ p main_arena.fastbinsY[6]
$5 = (mfastbinptr) 0x602000
gdb-peda$ i r rax
rax            0x602090        0x602090
gdb-peda$

Breakpoint 4, 0x00000000004005e2 in main ()
gdb-peda$ i r rax
rax            0x602010        0x602010
gdb-peda$ p main_arena.fastbinsY[6]
$4 = (mfastbinptr) 0x602080
gdb-peda$
```

Related information

- https://github.com/shellphish/how2heap

Unknown macro: 'html'