Heap Lookaside

Author: wnagzihxain
Mail: tudouboom@163.com

```
#include <stdio.h>
#include <windows.h>
int main()
    HLOCAL h1, h2, h3, h4;
    HANDLE hp:
    hp = HeapCreate(0, 0, 0):
    __asm int 3
    h1 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 8);
    h2 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 8);
    h3 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 16);
    h4 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 24);
    HeapFree(hp, 0, h1);
    HeapFree(hp, 0, h2);
    HeapFree(hp, 0, h3);
    HeapFree(hp, 0, h4);
    h2 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 16);
    HeapFree(hp, 0, h2);
}
```

Release然后运行,attach

初始化的堆区

```
00360010 00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00 .....?... ..
00360020 00 02 00 00 00 20 00 00 2F 02 00 00 FF EF FD 7F
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
                               P.6.P.6.@ 6....
00360170 00 00 00 00 00 00 00 90 1E 36 00 90 1E 36 00
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00
                               € 6.€ 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 26.26.26.
903601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00 ?6.?6.?6.
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00 ?6.?6.?6.?6.
003601C0 C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00 ?6.?6.?6.?6.
003601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00 ?6.?6.?6.?6.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00 ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00 ?6.?6.?6.?6.
00360200 00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00 . 6.. 6. 6.
00360210 10 02 36 00 10 02 36 00 18 02 36 00 18 02 36 00 6. 6. 6.
6. 6.( 6.( 6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00 @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00 P 6.P 6.X 6.X 6.
00360260 60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00 ` 6.` 6.h 6.h 6.
```

```
00360270 70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00 p 6.p 6.x 6.x 6.
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00 € 6.€ 6.?6.?6.
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00 ?6.?6.?6.?6.
00360290
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.?6.
003602B0 B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00 ?6.?6.?6.?6.
003602C0 C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00 ?6.?6.?6.?6.
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
003602D0
                                                       ?6.?6.?6.?6.
        E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
003602E0
                                                       ?6.?6.?6.?6.
003602F0
        F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                       ?6.?6.?6.?6.
00360300
         00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                                       . 6.. 6. 6. 6.
00360310
         10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                        6. 6. 6.
00360320
         20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                                        6. 6.(6.(6.
00360330
         30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00
                                                       0 6.0 6.8 6.8 6.
00360340
         40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                       @ 6.@ 6.H 6.H 6.
00360350
         50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00
                                                       P 6.P 6.X 6.X 6.
                                                       ` 6.` 6.h 6.h 6.
00360360
         60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
         70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00
00360370
                                                       p 6.p 6.x 6.x 6.
         80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
00360380
                                                       € 6.€ 6.?6.?6.
00360390
         90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
                                                       ?6.?6.?6.?6.
003603A0
         A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
                                                       ?6.?6.?6.?6.
003603B0
         B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00
003603C0
         C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00
003603D0
         D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
                                                       ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
                                                       ?6.?6.?6.?6.
003603F0
        F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                       ?6.?6.?6.?6.
00360400
         00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                       . 6.. 6. 6. 6.
00360410 10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                        6. 6. 6. 6.
00360420
         20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                        6. 6.(6.(6.
00360430
         30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00
                                                       0 6.0 6.8 6.8 6.
00360440
         40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                       @ 6.@ 6.H 6.H 6.
00360450
         50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                       P 6.P 6.X 6.X 6.
                                                       ` 6.` 6.h 6.h 6.
00360460
         60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
00360470
         70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
                                                       p 6.p 6.x 6.x 6.
00360480
         80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                       € 6.€ 6.?6.?6.
00360490
         90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                       ?6.?6.?6.?6.
        A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00 ?6.?6.?6.?6.
003604A0
003604B0
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00 ?6.?6.?6.?6.
003604C0 C0 04 36 00 C0 04 36 00 C8 04 36 00 C8 04 36 00 ?6.?6.?6.?6.
003604D0 D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00 ?6.?6.?6.?6.
003604E0 E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00 ?6.?6.?6.?6.
003604F0 F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00 ?6.?6.?6.?6.
00360500
        00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                       . 6.. 6. 6. 6.
00360510 \quad 10 \quad 05 \quad 36 \quad 00 \quad 10 \quad 05 \quad 36 \quad 00 \quad 18 \quad 05 \quad 36 \quad 00 \quad 18 \quad 05 \quad 36 \quad 00
                                                        6. 6. 6. 6.
6. 6.( 6.( 6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                       @ 6.@ 6.H 6.H 6.
00360550
         50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                                       P 6.P 6.X 6.X 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
                                                       ` 6.` 6.h 6.h 6.
00360570
         70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                                       p 6.p 6. 6....
00360580
         88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
                                                       ?6.....06.
00360590
         00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00
                                                       .?....?6.....
003605A0
         00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
                                                       .....?6.....
003605B0
         00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00
003605C0
         00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00
003605D0
         00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
003605E0
         00 00 00 00 00 00 00 F8 05 36 00 00 00 00 00
                                                       ......?6....
003605F0
         00360600
         00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
                                                       .......?齱2222
00360610
         00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00
00360620
         00360630
         00360640
         08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
                                                       .?. ..??....
00360650
         00\ 00\ 36\ 00\ 00\ D0\ 03\ 00\ 00\ 00\ 36\ 00\ 40\ 00\ 00\ 00
                                                       ..6..?...6.@...
00360660
         80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
                                                       € 6...:.=...
00360670
         88 05 36 00 00 00 00 00 88 1E 36 00 00 00 00 00
                                                       ?6.....?6.....
00360680
         01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
00360690
         . . . . . . . . . . . . . . . . . .
003606A0
         . . . . . . . . . . . . . . . . . . .
003606B0
         . . . . . . . . . . . . . . . .
003606C0
         . . . . . . . . . . . . . . . .
```

先分析一下初始化的堆区

尾块有0x0000022F个堆单位可分配

```
0x00360020 00 02 00 00 00 20 00 00 2F 02 00 00 FF EF FD 7F
```

Freelist[0]为0x00361E90,表示尾块数据区的起始位置

```
0x00360170 00 00 00 00 00 00 00 90 1E 36 00 90 1E 36 00
```

快表的起始位置,原来未使用快表的时候这里是空表尾块的起始位置

```
0x00360680 01 03 08 00 00 01 08 00 00 00 00 00 00 00 00
```

接下来分析一下四次分配

申请第一次

```
h1 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 8);
```

```
00401017
             90
                          nop
00401018 |. 8B3D 04504000 mov
                                  edi, dword ptr [<&amp;KERNEL32.HeapA&gt;; ntdll.RtlAllocateHeap
0040101E |. 6A 08
                                  8
                                                                  ; /HeapSize = 8
                          push
00401020 |. 6A 08
                                  8
                                                                  ; |Flags = HEAP_ZERO_MEMORY
                          push
                                                                  ; |hHeap
00401022 |. 56
                          push
                                  esi
00401023 |. FFD7
                          call
                                  edi
                                                                  ; \HeapAlloc
```

运行完的堆区

```
00360010 00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00 .....?... ..
00360020 00 02 00 00 00 20 00 00 2D 02 00 00 FF EF FD 7F
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 P.6.P.6.@ 6.....
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
00360170 00 00 00 00 00 00 00 A0 1E 36 00 A0 1E 36 00
                             . . . . . . . ?6 . ?6 .
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00 € 6.€ 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 ?6.?6.?6.?6.
003601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00 ?6.?6.?6.?6.
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00 ?6.?6.?6.?6.
003601C0 C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00 ?6.?6.?6.?6.
003601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00 ?6.?6.?6.?6.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00 ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00 ?6.?6.?6.?6.
00360200 00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00 . 6.. 6. 6.
00360210 10 02 36 00 10 02 36 00 18 02 36 00 18 02 36 00
```

```
00360220
         20 02 36 00 20 02 36 00 28 02 36 00 28 02 36 00
                                                         6. 6.(6.(6.
         30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360230
         40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
00360240
                                                        @ 6.@ 6.H 6.H 6.
         50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00
00360250
                                                        P 6.P 6.X 6.X 6.
                                                        ` 6.` 6.h 6.h 6.
00360260
         60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
00360270
         70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00
                                                        p 6.p 6.x 6.x 6.
         80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
00360280
                                                        € 6.€ 6.?6.?6.
00360290
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00
                                                        ?6.?6.?6.?6.
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00
                                                        ?6.?6.?6.?6.
003602B0
         B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00
003602C0
         C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00
003602D0
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
                                                        ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
                                                        ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                        ?6.?6.?6.?6.
00360300
         00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                                        . 6.. 6. 6. 6.
00360310 10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                          6. 6. 6. 6.
00360320
         20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                                          6. 6.(6.(6.
00360330
         30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00
                                                        0 6.0 6.8 6.8 6.
00360340
         40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360350
         50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00
                                                        P 6.P 6.X 6.X 6.
00360360
         60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                                        ` 6.` 6.h 6.h 6.
00360370
         70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00
                                                        p 6.p 6.x 6.x 6.
         80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
00360380
                                                        € 6.€ 6.?6.?6.
00360390
         90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
                                                        ?6.?6.?6.?6.
003603A0
         A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00 ?6.?6.?6.?6.
         B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00 ?6.?6.?6.
003603B0
003603C0 C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00 ?6.?6.?6.?6.
003603D0 D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00 ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00 ?6.?6.?6.?6.
003603F0 F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00 ?6.?6.?6.?6.
00360400
         00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
00360420 \quad 20 \ 04 \ 36 \ 00 \ 20 \ 04 \ 36 \ 00 \ 28 \ 04 \ 36 \ 00 \ 28 \ 04 \ 36 \ 00
                                                          6. 6.(6.(6.
00360430 30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440 40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360450 50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00 P 6.P 6.X 6.X 6.
                                                        ` 6.` 6.h 6.h 6.
00360460
         60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
         70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00 p 6.p 6.x 6.x 6.
00360470
00360480
         80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                        € 6.€ 6.?6.?6.
00360490
         90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
003604A0
         A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                        ?6.?6.?6.?6.
003604B0
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604C0
         C0 04 36 00 C0 04 36 00 C8 04 36 00 C8 04 36 00
                                                        ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
                                                        ?6.?6.?6.?6.
003604E0
         E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                        ?6.?6.?6.?6.
003604F0
         F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
                                                        ?6.?6.?6.?6.
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                        . 6.. 6. 6. 6.
00360510 10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                          6. 6. 6. 6.
00360520
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
                                                          6. 6.(6.(6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360550 \quad 50 \ 05 \ 36 \ 00 \ 50 \ 05 \ 36 \ 00 \ 58 \ 05 \ 36 \ 00 \ 58 \ 05 \ 36 \ 00
                                                        P 6.P 6.X 6.X 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
                                                        ` 6.` 6.h 6.h 6.
00360570
         70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                                        p 6.p 6. 6....
00360580
         88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
                                                        ?6....06.
00360590
         00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
                                                        . ? . . . . . ? 6 . . . . .
003605A0
         00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00
                                                        . . . . . . . ?6 . . . . .
003605B0
         00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
                                                        .....?6.....
003605C0
         00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00 00
                                                        ....?6.....
                                                        .....?6.....
003605D0
         00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
003605E0
         00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00 00
003605F0
         00360600
         00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
         00360610
00360620
         00360630
         08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360640
         00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
00360650
                                                        ..6..?...6.@...
00360660
         80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00 € 6...:=...
00360670 88 05 36 00 00 00 00 00 98 1E 36 00 00 00 00 ?6.....?6.....
```

可以看到,@x0000022F变成了@x0000022D,减小了两个堆单位,16字节

```
0x00360020 00 02 00 00 00 20 00 00 2D 02 00 00 FF EF FD 7F
```

Freelist[0]由0x00361E90变成了0x00361EA0,因为尾块划分16个字节分配给了h1使用

```
0x00360170 00 00 00 00 00 00 00 A0 1E 36 00 A0 1E 36 00
```

申请第二次

```
h2 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 8);
```

```
00401025 |. 6A 08
                          push
                                  8
                                                                  ; /HeapSize = 8
00401027 |. 6A 08
                                                                  ; |Flags = HEAP_ZERO_MEMORY
                          push
                                  8
00401029 |. 56
                                  esi
                                                                  ; |hHeap
                          push
0040102A |. 8BD8
                          mov
                                  ebx, eax
                                                                  ; |
0040102C |. FFD7
                          call
                                                                  ; \HeapAlloc
                                  edi
```

可分配空间变成了0x0000022B个堆单位

```
00360020 00 02 00 00 00 20 00 00 2B 02 00 00 FF EF FD 7F
```

尾块的起始位置变成了@x00361EB0

```
0x00360170 00 00 00 00 00 00 00 B0 1E 36 00 B0 1E 36 00
```

申请第三次

```
h3 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 16);
```

```
0040102E | 6A 10
                          push
                                 10
                                                                 ; /HeapSize = 10 (16.)
00401030 | . 6A 08
                                                                 ; |Flags = HEAP_ZERO_MEMORY
                          push
                                 8
                                                                 ; |hHeap
00401032 |. 56
                          push
                                 esi
00401033 |. 8945 FC
                         mov
                                 dword ptr [ebp-4], eax
                                                                 ; |
00401036 |. FFD7
                          call
                                                                 ; \HeapAlloc
```

运行完的堆区

```
00360000 C8 00 00 00 01 00 00 FF EE FF EE 02 10 00 00 ?.....??? ..
00360010 00 00 00 00 FE 00 00 00 10 00 00 20 00 00 ....?... ..
00360020 00 02 00 00 00 20 00 00 28 02 00 00 FF EF FD 7F
                    . ... ..( ..2稞
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
                    . .........
00360040 00 00 00 08 05 36 00 0F 00 00 00 F8 FF FF FF
                    ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
                    P.6.P.6.@ 6.....
```

```
00360120
         00360130
         00360140
         00360150
00360160
         00360170
         00 00 00 00 00 00 00 00 C8 1E 36 00 C8 1E 36 00
00360180
         80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00
                                                        € 6.€ 6.?6.?6.
00360190
         90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00
                                                        ?6.?6.?6.?6.
003601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00
                                                        ?6.?6.?6.?6.
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00
                                                        ?6.?6.?6.?6.
003601C0    C0    01    36    00    C0    01    36    00    C8    01    36    00    C8    01    36    00
003601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00
                                                        ?6.?6.?6.?6.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00
                                                        ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                                        ?6.?6.?6.?6.
00360200
         00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
                                                        . 6.. 6. 6. 6.
00360210 10 02 36 00 10 02 36 00 18 02 36 00 18 02 36 00
                                                          6. 6. 6. 6.
00360220
         20 02 36 00 20 02 36 00 28 02 36 00 28 02 36 00
                                                          6. 6.(6.(6.
00360230
         30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00
                                                        0 6.0 6.8 6.8 6.
00360240
         40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360250
         50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00
                                                        P 6.P 6.X 6.X 6.
00360260
         60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
                                                        ` 6.` 6.h 6.h 6.
00360270
         70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00
                                                        p 6.p 6.x 6.x 6.
         80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
00360280
                                                        € 6.€ 6.?6.?6.
00360290
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00
                                                        ?6.?6.?6.?6.
003602A0
         A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.?6.
         B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00 ?6.?6.?6.?6.
003602B0
003602C0 C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00 ?6.?6.?6.?6.
003602D0 D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00 ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00 ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00 ?6.?6.?6.?6.
00360300 00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
00360320 \quad 20 \ 03 \ 36 \ 00 \ 20 \ 03 \ 36 \ 00 \ 28 \ 03 \ 36 \ 00 \ 28 \ 03 \ 36 \ 00
                                                          6. 6.(6.(6.
00360330 30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360340 40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360350 50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00 P 6.P 6.X 6.X 6.
         60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                                        ` 6.` 6.h 6.h 6.
00360360
         70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
00360370
00360380
         80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
                                                        € 6.€ 6.?6.?6.
00360390
         90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
003603A0
         A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
003603B0
         B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00
003603C0
         CO 03 36 00 CO 03 36 00 C8 03 36 00 C8 03 36 00
                                                        ?6.?6.?6.?6.
003603D0
         D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
                                                        ?6.?6.?6.?6.
003603E0
         E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
                                                        ?6.?6.?6.?6.
003603F0
         F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                        ?6.?6.?6.?6.
00360400
         00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                        . 6.. 6. 6. 6.
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                          6. 6. 6. 6.
00360420 20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                          6. 6.(6.(6.
00360430 30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440 40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360450 \quad 50 \ 04 \ 36 \ 00 \ 50 \ 04 \ 36 \ 00 \ 58 \ 04 \ 36 \ 00 \ 58 \ 04 \ 36 \ 00
                                                        P 6.P 6.X 6.X 6.
00360460 60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
                                                        ` 6.` 6.h 6.h 6.
                                                        p 6.p 6.x 6.x 6.
00360470 70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
00360480
         80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                        € 6.€ 6.?6.?6.
00360490
         90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                        ?6.?6.?6.?6.
003604A0
         A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                        ?6.?6.?6.?6.
003604B0
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
                                                        ?6.?6.?6.?6.
003604C0
         C0 04 36 00 C0 04 36 00 C8 04 36 00 C8 04 36 00
                                                        ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
003604E0
         E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
         F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
003604F0
                                                        ?6.?6.?6.?6.
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                        . 6.. 6. 6.
00360510
         10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                          6. 6. 6.
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
00360520
                                                          6. 6.(6.(6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00 @ 6.@ 6.H 6.H 6.
00360550 50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00 P 6.P 6.X 6.X 6.
00360560 60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00 ` 6.` 6.h 6.h 6.
00360570 70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00 p 6.p 6. 6....
00360580 88 06 36 00 00 00 01 00 00 00 00 00 30 36 00 ?6.........06.
```

```
00360590
      00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
      00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
003605A0
      00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
003605B0
003605C0
      00\ 00\ 00\ 00\ 00\ 00\ 00\ D8\ 05\ 36\ 00\ 00\ 00\ 00\ 00
003605D0
      00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
003605E0
      00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00 00
003605F0
      00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
00360600
00360610
      00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00
00360620
      00360630
      00360640
      08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360650
      00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
00360660 80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
00360670 88 05 36 00 00 00 00 00 C0 1E 36 00 00 00 00 00
00360680
      01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
      00360690
003606A0
      003606B0
      003606C0
      003606D0
      003606E0
      003606F0
      04 00 00 01 02 00 00 00 02 00 00 00 00 00 00 00
```

可分配的空间变成了@x00000228个堆单位,减小了3个堆单位也就是24个字节

```
0x00360020 00 02 00 00 00 20 00 00 28 02 00 00 FF EF FD 7F
```

尾块起始位置变成了0x00361EC8

```
0x00360170 00 00 00 00 00 00 00 C8 1E 36 00 C8 1E 36 00
```

申请第四次

```
h4 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 24);
```

```
00401038 |. 6A 18
                                   18
                                                                   ; /HeapSize = 18 (24.)
                           push
0040103A |.
            6A 08
                           push
                                                                   ; |Flags = HEAP_ZERO_MEMORY
0040103C
            56
                           push
                                                                   ; |hHeap
0040103D |. 8945 F8
                           mov
                                   dword ptr [ebp-8], eax
00401040 |. FFD7
                           call
                                   edi
                                                                   ; \HeapAlloc
```

运行完后的堆区

```
00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
  00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
00360020
00360030
  04 00 08 06 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
                 ....?6. ....?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
                 P.6.P.6.@ 6....
00360060
  00360070
  00360080
  00360090
  003600A0
  003600B0
  003600C0
  003600D0
  003600E0
  003600F0
  00360100
```

```
00360170
         00 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00
                                                        € 6.€ 6.?6.?6.
         90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00
00360190
                                                        ?6.?6.?6.?6.
         A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00
003601A0
                                                        ?6.?6.?6.?6.
993691B9
         RO 01 36 00 RO 01 36 00 RS 01 36 00 RS 01 36 00
                                                        26.26.26.26.
00360100 00 01 36 00 00 01 36 00 08 01 36 00 08 01 36 00
                                                        ?6.?6.?6.?6.
         D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00
003601D0
                                                        26.26.26.26.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00
                                                        ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                                        ?6.?6.?6.?6.
00360200 00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
                                                        . 6.. 6. 6. 6.
6. 6.(6.(6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00 @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00
                                                       P 6.P 6.X 6.X 6.
                                                        ` 6.` 6.h 6.h 6.
00360260 60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
00360270
         70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00
                                                        p 6.p 6.x 6.x 6.
00360280
         80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
                                                        € 6.€ 6.?6.?6.
00360290
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00
                                                        ?6.?6.?6.?6.
003602A0
         A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00
                                                        ?6.?6.?6.?6.
003602B0
         B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00
003602C0
         C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00
003602D0
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
                                                        ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00 ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                        ?6.?6.?6.?6.
00360300 00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                                        . 6. . 6. 6. 6.
00360310 10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                         6. 6. 6. 6.
6. 6.(6.(6.
00360330 30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360340 40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00 @ 6.@ 6.H 6.H 6.
00360350 50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00 P 6.P 6.X 6.X 6.
00360360 60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00 ` 6.` 6.h 6.h 6.
00360370 70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
00360380 80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00 € 6.€ 6.?6.?6.
00360390 90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00 ?6.?6.?6.?6.
003603A0 A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00 ?6.?6.?6.?6.
         B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00 ?6.?6.?6.?6.
003603B0
         C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00
003603C0
                                                        ?6.?6.?6.?6.
003603D0
         D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
                                                        ?6.?6.?6.?6.
003603E0
         E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
003603F0
         F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                        ?6.?6.?6.?6.
00360400
         00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
00360410
         10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                          6. 6. 6.
00360420
         20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                          6. 6.(6.(6.
        30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360430
00360440 40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                        @ 6.@ 6.H 6.H 6.
                                                       P 6.P 6.X 6.X 6.
00360450 50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                        ` 6.` 6.h 6.h 6.
00360460 60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
00360470 70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00 p 6.p 6.x 6.x 6.
00360480 80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
00360490 90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00 ?6.?6.?6.?6.
003604A0 A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                        ?6.?6.?6.?6.
003604B0 B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
                                                        ?6.?6.?6.?6.
003604C0    C0    04    36    00    C0    04    36    00    C8    04    36    00    C8    04    36    00
                                                        ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
                                                        ?6.?6.?6.?6.
003604E0
         E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                        ?6.?6.?6.?6.
003604F0
         F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
                                                        ?6.?6.?6.?6.
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                        . 6.. 6. 6.
00360510
         10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                          6. 6. 6.
00360520
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
                                                          6. 6.(6.(6.
00360530
         30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00
                                                        0 6.0 6.8 6.8 6.
00360540
         40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360550
         50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00 P 6.P 6.X 6.X 6.
                                                        ` 6.` 6.h 6.h 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
        70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00 p 6.p 6. 6.....
00360570
00360580 88 06 36 00 00 00 01 00 00 00 00 00 30 36 00
00360590 00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
003605A0 00 00 00 00 00 00 00 B8 05 36 00 00 00 00
003605B0
         00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
003605C0 00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00 00 ......?6....
003605D0 00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00 ......?6....
```

```
003605E0
    00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00
    003605F0
    00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
00360600
00360610
    00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00
00360620
    00360630
    08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360640
00360650
    00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
                             ..6..?...6.@...
00360660
    80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
00360670 88 05 36 00 00 00 00 E0 1E 36 00 00 00 00 00
00360680
    01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
003606E0
003606F0
    04 00 00 01 02 00 00 00 02 00 00 00 00 00 00 00
. . . . . . . . . . . . . . . .
```

可分配空间变成了@x00000224个堆单位,减小了4个堆单位也就是32个字节

```
0x00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
```

尾块起始位置变成了0x00361EE8

```
0x00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
```

到此四次分配全部完成,来看看分配的四个堆块

```
. . . . . . . . . . . . . . . .
00361E80
    00 00 00 00 00 00 00 00 02 00 01 03 00 01 08 00
                           00361E90
    00361EA0
    00 00 00 00 00 00 00 00 03 00 02 00 00 01 08 00
00361EB0
    00361EC0
    04 00 03 00 00 01 08 00 00 00 00 00 00 00 00 00
00361EE0 24 02 04 00 00 10 00 00 78 01 36 00 78 01 36 00
```

接下来是释放

释放第一次

```
HeapFree(hp, 0, h1);
```

```
00401042 |. 53
                           push
                                  ehx
                                                                   ; /pMemory = 00361E90
                                  ebx, dword ptr [<&amp;KERNEL32.HeapF&gt;; |ntdll.RtlFreeHeap
00401043 |. 8B1D 4C504000 mov
00401049 |. 6A 00
                           push
                                  0
                                                                   ; |Flags = 0|
0040104B |. 56
                                                                   ; |hHeap
                           push
                                  esi
0040104C |. 8945 F4
                           mov
                                  dword ptr [ebp-C], eax
                                                                  ; |
0040104F |. FFD3
                           call
                                                                   ; \HeapFree
```

```
00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
00360010
    00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
00360020
                             . ... ..$ ..2稞
00360030
    04 00 08 06 00 00 00 00 00 00 00 00 00 00 00
00360040
    00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
                             ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
00360060
    . . . . . . . . . . . . . . . .
```

```
003600B0
        003600C0
003600D0
        003600E0
        003600F0
        00360100
        00360110
        00360120
        00360130
        00360140
        00360150
        00360160
        00360170
        00 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
                                                   .....?6.?6.
00360180
        80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00
                                                   € 6.€ 6.?6.?6.
00360190
        90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00
                                                   ?6.?6.?6.?6.
003601A0
        A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00
                                                   ?6.?6.?6.?6.
003601B0
        B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00
                                                   ?6.?6.?6.?6.
003601C0
        C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00
                                                   ?6.?6.?6.?6.
003601D0
        D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00
                                                   ?6.?6.?6.?6.
003601E0
        E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00
                                                   ?6.?6.?6.?6.
003601F0
        F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
00360200
        00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
00360210
        10 02 36 00 10 02 36 00 18 02 36 00 18 02 36 00
                                                    6. 6. 6.
00360220
        20 02 36 00 20 02 36 00 28 02 36 00 28 02 36 00
                                                    6. 6.(6.(6.
       30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360230
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00 @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00 P 6.P 6.X 6.X 6.
00360260 60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
                                                   ` 6.` 6.h 6.h 6.
00360270 70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00 p 6.p 6.x 6.x 6.
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00 € 6.€ 6.?6.?6.
00360290
        90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00 ?6.?6.?6.?6.
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.
003602B0 B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00 ?6.?6.?6.?6.
003602C0 C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00 ?6.?6.?6.?6.
003602D0 D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00 ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
                                                   ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                   ?6.?6.?6.?6.
00360300
        00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                                   . 6.. 6. 6. 6.
00360310 10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                    6. 6. 6. 6.
00360320
        20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                                    6. 6.(6.(6.
00360330
        30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00
                                                   0 6.0 6.8 6.8 6.
00360340
        40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                   @ 6.@ 6.H 6.H 6.
00360350
        50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00
                                                   P 6.P 6.X 6.X 6.
                                                   ` 6.` 6.h 6.h 6.
00360360
        60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
        70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00
00360370
                                                   p 6.p 6.x 6.x 6.
00360380
        80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
                                                   € 6.€ 6.?6.?6.
00360390
        90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
                                                   ?6.?6.?6.?6.
003603A0 A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
                                                   ?6.?6.?6.?6.
003603B0
        B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00
                                                   ?6.?6.?6.?6.
003603C0
        C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00
003603D0
        D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
                                                   ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
                                                   ?6.?6.?6.?6.
003603F0 F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                   ?6.?6.?6.?6.
00360400
        00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                   . 6.. 6. 6. 6.
00360410 10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                    6. 6. 6. 6.
00360420
        20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                    6. 6.(6.(6.
00360430
        30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00
                                                   0 6.0 6.8 6.8 6.
00360440
        40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                   @ 6.@ 6.H 6.H 6.
00360450
        50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                   P 6.P 6.X 6.X 6.
00360460
        60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
                                                   ` 6.` 6.h 6.h 6.
00360470
        70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
                                                   p 6.p 6.x 6.x 6.
        80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
00360480
00360490
        90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                   ?6.?6.?6.?6.
003604A0
        A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                   ?6.?6.?6.?6.
        B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604B0
                                                   ?6.?6.?6.?6.
003604C0 C0 04 36 00 C0 04 36 00 C8 04 36 00 C8 04 36 00 ?6.?6.?6.?6.
003604D0 D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00 ?6.?6.?6.?6.
003604E0 E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00 ?6.?6.?6.?6.
003604F0 F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00 ?6.?6.?6.?6.
00360500 00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00 . 6.. 6. 6.
00360510    10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                    6. 6. 6. 6.
```

```
6. 6.(6.(6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
      40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
00360540
                                       @ 6.@ 6.H 6.H 6.
      50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                       P 6.P 6.X 6.X 6.
00360550
                                       ` 6.` 6.h 6.h 6.
00360560 60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
00360570
      70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                       p 6.p 6. 6....
00360580 88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
00360590
      00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
003605A0
      00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00
003605B0
      00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00
      00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00
003605D0 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
003605E0 \quad 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ F8 \ 05 \ 36 \ 00 \ 00 \ 00 \ 00
........?齱2222
00360600 00 00 00 00 00 00 00 CO 06 FD 77 FF FF FF
00360610 00 00 00 00 00 00 00 2C 00 00 00 00 00 00
      00360620
00360630
      00360640
      08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
                                        .?. ..??....
00360650
      00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
                                       ..6..?...6.@...
00360660
      80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
00360670
      88 05 36 00 00 00 00 00 E0 1E 36 00 00 00 00 00
      01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
00360680
003606E0 00 00 00 00 00 00 00 90 1E 36 00 01 00 01 00
003606F0 04 00 00 01 02 00 00 00 02 00 00 00 01 00 00 00
```

可分配空间为0x00000224个堆单位,没有变化,因为释放刚好16个字节,优先放入快表

```
0x00360020 00 02 00 00 20 00 00 24 02 00 00 FF EF FD 7F
```

尾块起始位置没有变化

```
0x00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
```

来看看快表区,这是Lookaside[1],这里有个问题,空表中申请的灰加上8字节块首,也就是申请8字节的空间会自动加上8字节块首也就是申请16个字节的空间,使用的是Freelist[2],而快表申请8字节的空间却直接使用Lookaside[1],这里是个疑问,不是很理解

```
0x003606E0 00 00 00 00 00 00 00 90 1E 36 00 01 00 01 00
```

接着来看看释放的空间 0x00361E90

释放第二次

```
HeapFree(hp, 0, h2);
```

```
00401051 |. 8B45 FC
                                   eax, dword ptr [ebp-4]
                           mov
00401054 |.
             50
                                                                    ; /pMemory
                           push
                                   eax
00401055 |.
             6A 00
                           push
                                                                    ; |Flags = 0|
00401057 |. 56
                           push
                                   esi
                                                                    ; |hHeap
00401058 |. FFD3
                           call
                                   ebx
```

```
00360010
       00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
                                            .....?... .. ..
00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
                                            . ... ..$ ..2稞
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
                                           ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 P.6.P.6.@ 6.....
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
003600F0
       . . . . . . . . . . . . . . . .
00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
                                           ......?6.?6.
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00 € 6.€ 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 ?6.?6.?6.
003601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00 ?6.?6.?6.?6.
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00 ?6.?6.?6.
003601C0 C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00 ?6.?6.?6.
003601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00 ?6.?6.?6.?6.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00 ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00 ?6.?6.?6.?6.
00360200 00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
                                            . 6.. 6. 6. 6.
6. 6. 6. 6.
6. 6.(6.(6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00
                                            0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
                                            @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00 P 6.P 6.X 6.X 6.
                                            ` 6.` 6.h 6.h 6.
00360260 60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
00360270 70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00 p 6.p 6.x 6.x 6.
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00 € 6.€ 6.?6.?6.
00360290 90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00 ?6.?6.?6.?6.
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.?6.
003602B0 B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00 ?6.?6.?6.?6.
003602D0 D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00 ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00 ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00 ?6.?6.?6.
00360300 \quad 00 \ 03 \ 36 \ 00 \ 00 \ 03 \ 36 \ 00 \ 08 \ 03 \ 36 \ 00 \ . \ 6.. \ 6. \quad 6.
00360310    10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                            6. 6. 6. 6.
00360320 20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                             6. 6.(6.(6.
00360330 30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360340 40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                            @ 6.@ 6.H 6.H 6.
00360350 50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00 P 6.P 6.X 6.X 6.
00360360 60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                            ` 6.` 6.h 6.h 6.
00360370 70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
00360380 80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
                                            € 6.€ 6.?6.?6.
00360390 90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
                                            ?6.?6.?6.?6.
003603A0 A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
                                            ?6.?6.?6.?6.
003603B0 B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00 ?6.?6.?6.?6.
003603C0 C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00 ?6.?6.?6.?6.
003603D0 D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00 ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00 ?6.?6.?6.?6.
003603F0 F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00 ?6.?6.?6.?6.
00360400 00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                           . 6.. 6. 6. 6.
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
00360420 \quad 20 \quad 04 \quad 36 \quad 00 \quad 20 \quad 04 \quad 36 \quad 00 \quad 28 \quad 04 \quad 36 \quad 00 \quad 28 \quad 04 \quad 36 \quad 00
                                             6. 6.(6.(6.
00360430 30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440 40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00 @ 6.@ 6.H 6.H 6.
```

```
00360450
       50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00 P 6.P 6.X 6.X 6.
       60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
                                               ` 6.` 6.h 6.h 6.
00360460
       70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
00360470
                                               p 6.p 6.x 6.x 6.
00360480
       80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                               € 6.€ 6.?6.?6.
00360490 90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00 76.76.76.
003604A0 A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                               ?6.?6.?6.?6.
003604B0 B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00 ?6.?6.?6.?6.
003604C0    C0    04    36    00    C0    04    36    00    C8    04    36    00    C8    04    36    00    ?6.?6.?6.?6.
003604D0 D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00 ?6.?6.?6.?6.
003604E0 E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00 ?6.?6.?6.?6.
003604F0 F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00 ?6.?6.?6.?6.
00360500 00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00 . 6.. 6. 6.
00360510    10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                6. 6. 6. 6.
6. 6.(6.(6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00 @ 6.@ 6.H 6.H 6.
00360550 50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                              P 6.P 6.X 6.X 6.
00360560 60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
                                               ` 6.` 6.h 6.h 6.
00360570
       70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                               p 6.p 6. 6....
00360580 88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
                                               ?6....06.
00360590
       00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
003605A0
       00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
       00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00
003605B0
                                               . . . . . . . ?6 . . . . .
00360500 00 00 00 00 00 00 00 08 05 36 00 00 00 00 00
                                               . . . . . . . ?6 . . . . .
003605D0 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
                                               . . . . . . . ?6 . . . . .
003605E0 00 00 00 00 00 00 00 F8 05 36 00 00 00 00 00
00360600 00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF FF
00360610 00 00 00 00 00 00 00 2C 00 00 00 00 00 00
00360640 08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360650 00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00 ..6..?...6.@...
00360660 80 06 36 00 00 00 3A 00 3D 00 00 01 00 00 0€ 6...:.=...
00360670 88 05 36 00 00 00 00 00 E0 1E 36 00 00 00 00 ?6....?6....
00360680 01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
. . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
003606C0
       003606E0 00 00 00 00 00 00 00 A0 1E 36 00 02 00 02 00
003606F0 04 00 00 01 02 00 00 00 02 00 00 02 00 00 00
```

可分配空间大小没有变化

```
0x00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
```

尾块起始位置没有变化

```
0x00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
```

Lookaside[1]变成了0x00361EA0

```
0x003606E0 00 00 00 00 00 00 00 A0 1E 36 00 02 00 02 00
```

跳到0x00361EA0看看

释放第三次

```
HeapFree(hp, 0, h3);
```

```
0040105A | 8B4D F8
                                    ecx, dword ptr [ebp-8]
                            mov
0040105D |.
             51
                            push
                                    ecx
                                                                     : /pMemory
0040105E
         |.
             6A 00
                                    0
                                                                     ; |Flags = 0
                            push
00401060
         Ι.
             56
                            push
                                    esi
                                                                     : | hHeap
00401061 |. FFD3
                                                                     ; \HeapFree
                            call
                                    ebx
```

```
00360010 00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
                                        .....?... .. ..
                                        . ... ..$ ..2稞
00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
00360030
      04 00 08 06 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
                                         ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
                                         P.6.P.6.@ 6.....
00360090
      . . . . . . . . . . . . . . . . .
003600A0
      . . . . . . . . . . . . . . . .
003600B0
      . . . . . . . . . . . . . . . .
003600C0
      . . . . . . . . . . . . . . . .
003600D0
      003600E0
      003600F0
      00360100
00360170 00 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00 ......?6.?6.
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00 \in 6.\in 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 ?6.?6.?6.?6.
003601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00 ?6.?6.?6.?6.
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00 ?6.?6.?6.?6.
003601C0 C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00 ?6.?6.?6.?6.
003601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00 ?6.?6.?6.?6.
003601E0 E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00
                                         ?6.?6.?6.?6.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                         ?6.?6.?6.?6.
00360200
      00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
                                         . 6.. 6. 6.
6. 6.(6.(6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00
                                        0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
                                         @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00 P 6.P 6.X 6.X 6.
                                        ` 6.` 6.h 6.h 6.
00360260 60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
00360270 70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00 p 6.p 6.x 6.x 6.
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
                                        € 6.€ 6.?6.?6.
00360290 90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00 ?6.?6.?6.?6.
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.?6.
003602B0 B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00 ?6.?6.?6.?6.
003602C0 C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00 ?6.?6.?6.?6.
003602D0 D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00 .6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00 ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00 ?6.?6.?6.?6.
00360300 00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                         . 6.. 6. 6.
                                                  6.
00360310 10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                         6. 6. 6.
                                                  6.
6. 6.(6.(6.
00360330
      30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360340
      40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                        @ 6.@ 6.H 6.H 6.
00360350
      50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00 P 6.P 6.X 6.X 6.
00360360 60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                        ` 6.` 6.h 6.h 6.
```

```
00360370
        70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
        80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
00360380
        90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
00360390
        A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
003603A0
                                                 ?6.?6.?6.?6.
003603B0
        B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00
                                                 26.26.26.26.
003603C0
        CO 03 36 00 CO 03 36 00 C8 03 36 00 C8 03 36 00
                                                 ?6.?6.?6.?6.
        D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
003603D0
                                                 ?6.?6.?6.?6.
003603E0
       E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
                                                 ?6.?6.?6.?6.
003603F0
       F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                 ?6.?6.?6.?6.
00360400
        00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
6. 6.(6.(6.
00360430 30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440
       40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00 @ 6.@ 6.H 6.H 6.
00360450 50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                P 6.P 6.X 6.X 6.
                                                 ` 6.` 6.h 6.h 6.
00360460
        60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
        70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
00360470
                                                 p 6.p 6.x 6.x 6.
00360480
        80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                 € 6.€ 6.?6.?6.
00360490
        90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                 ?6.?6.?6.?6.
003604A0
        A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                 ?6.?6.?6.?6.
003604B0
        B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604C0
        CO 04 36 00 CO 04 36 00 C8 04 36 00 C8 04 36 00
        D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
003604D0
003604E0
       E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                26.26.26.26.
003604F0
       F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
                                                 ?6.?6.?6.?6.
00360500
        00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                 . 6. . 6. 6. 6.
00360510 10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                 6. 6. 6. 6.
6. 6.(6.(6.
00360530 30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00 @ 6.@ 6.H 6.H 6.
00360550 50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00 P 6.P 6.X 6.X 6.
00360560 60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
                                                ` 6.` 6.h 6.h 6.
00360570 70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00 p 6.p 6. 6....
00360590
        00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
                                                 .?....?6.....
        00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
                                                 .....?6.....
003605A0
003605B0
        00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
                                                 .....?6.....
003605C0
        00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00
                                                 .......?6.....
003605D0
        00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00
                                                 . . . . . . . ? 6 . . . . .
003605E0
        00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00
                                                 .....?6.....
003605F0
        00360600
        00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
                                                 .......?齱2222
00360610
        00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00 00
00360620
        00360630
        08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360640
        00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
00360650
                                                 ..6..?...6.@...
        80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
00360660
00360670
       88 05 36 00 00 00 00 00 E0 1E 36 00 00 00 00 00
                                                 ?6.....?6.....
00360680
        01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
00360690
        003606A0
        003606B0
       003606C0
       003606D0
        003606E0
        00 00 00 00 00 00 00 00 A0 1E 36 00 02 00 02 00
                                                 003606F0
        04 00 00 01 02 00 00 00 02 00 00 00 02 00 00 00
00360700
       . . . . . . . . . . . . . . . .
00360710 00 00 00 00 00 00 00 B0 1E 36 00 01 00 01 00
```

可分配空间大小没有变化

```
0x00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
```

尾块起始位置没有变化

```
0x00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
```

Lookaside[2]变成了0x00361EB0

```
0x00360710 00 00 00 00 00 00 00 B0 1E 36 00 01 00 01 00
```

所以应该是h3释放后串在了lookaside[2]上,看看分配的堆块区

释放第四次

```
HeapFree(hp, 0, h4);
```

```
00401063 |. 8B55 F4
                           mov
                                   edx, dword ptr [ebp-C]
00401066 |. 52
                           push
                                   edx
                                                                    ; /pMemory
00401067 |. 6A 00
                                                                   ; |Flags = 0
                           push
00401069 |. 56
                                   esi
                           push
                                                                    ; |hHeap
0040106A |. FFD3
                           call
                                   ebx
                                                                    ; \HeapFree
```

```
00360010 00 00 00 00 FE 00 00 00 10 00 00 20 00 00 ....?... ..
00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
                              . ... ..$ ..2稞
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
                              . . . . . . . . . . . . . . . .
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
                              ....?6. ...?22
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
                              P.6.P.6.@ 6....
00360060
    00360090
    00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
                              .....?6.?6.
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00
                              ?6.?6.?6.?6.
003601A0
    A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00
003601B0 B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00
                              ?6.?6.?6.?6.
003601C0    C0    01    36    00    C0    01    36    00    C8    01    36    00    C8    01    36    00
                              ?6.?6.?6.?6.
903601D0 D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00 76.76.76.
003601F0 F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00 ?6.?6.?6.?6.
00360200 00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00 . 6.. 6. 6.
6. 6. 6. 6.
6. 6.(6.(6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00 @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00 P 6.P 6.X 6.X 6.
```

```
60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00 ` 6.` 6.h 6.h 6.
00360260
         70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00
00360270
                                                       p 6.p 6.x 6.x 6.
         80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
00360280
                                                       € 6.€ 6.?6.?6.
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00
00360290
                                                       ?6.?6.?6.?6.
003602A0
         Δ0 02 36 00 Δ0 02 36 00 Δ8 02 36 00 Δ8 02 36 00
                                                       26.26.26.26.
003602B0
         B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00
                                                       ?6.?6.?6.?6.
        C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00
003602C0
                                                       ?6.?6.?6.?6.
003602D0
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
                                                       ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
                                                       ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                       ?6.?6.?6.?6.
00360300
         00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
6. 6. 6. 6.
00360320 \quad 20 \quad 03 \quad 36 \quad 00 \quad 20 \quad 03 \quad 36 \quad 00 \quad 28 \quad 03 \quad 36 \quad 00 \quad 28 \quad 03 \quad 36 \quad 00
                                                        6. 6.(6.(6.
00360330 30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360340
        40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                       @ 6.@ 6.H 6.H 6.
00360350
        50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00
                                                       P 6.P 6.X 6.X 6.
         60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                                       ` 6.` 6.h 6.h 6.
00360360
00360370
         70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00
                                                       p 6.p 6.x 6.x 6.
00360380
         80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00
                                                       € 6.€ 6.?6.?6.
00360390
         90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00
                                                       ?6.?6.?6.?6.
003603A0
         A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00
003603B0
         B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00
                                                       ?6.?6.?6.?6.
003603C0
         CO 03 36 00 CO 03 36 00 C8 03 36 00 C8 03 36 00
                                                       ?6.?6.?6.?6.
003603D0
         D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00
                                                       26.26.26.26.
003603E0
        E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00 ?6.?6.?6.?6.
003603F0 F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
                                                       ?6.?6.?6.?6.
        00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                       . 6.. 6. 6. 6.
00360400
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                        6. 6. 6. 6.
00360420 20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                        6. 6.(6.(6.
00360430 30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440 40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00 @ 6.@ 6.H 6.H 6.
00360450 50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00 P 6.P 6.X 6.X 6.
00360460 60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
                                                       ` 6.` 6.h 6.h 6.
00360470 70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00 p 6.p 6.x 6.x 6.
00360480 80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00 € 6.€ 6.?6.?6.
00360490
        90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00 ?6.?6.?6.?6.
003604A0 A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00 ?6.?6.?6.?6.
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604B0
                                                       ?6.?6.?6.?6.
003604C0
         C0 04 36 00 C0 04 36 00 C8 04 36 00 C8 04 36 00
                                                       ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
003604E0
         E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                       ?6.?6.?6.?6.
003604F0
         F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
                                                       ?6.?6.?6.?6.
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                       . 6.. 6. 6.
00360510
        10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                        6. 6. 6. 6.
00360520
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
                                                        6. 6.(6.(6.
00360530
        30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00 0 6.0 6.8 6.8 6.
00360540
        40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                       @ 6.@ 6.H 6.H 6.
00360550
         50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                                       P 6.P 6.X 6.X 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
                                                       ` 6.` 6.h 6.h 6.
00360570 70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                                       p 6.p 6. 6....
00360580 88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
00360590
         00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
                                                       .?....?6.....
003605A0
         00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
                                                       .....?6....
003605B0
         00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
                                                       ......?6.....
003605C0
         00 00 00 00 00 00 00 D8 05 36 00 00 00 00 00
                                                       .....?6.....
003605D0
         00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
                                                       . . . . . . . ?6 . . . . .
003605E0
         00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00
                                                       . . . . . . . . ?6 . . . . .
003605F0
         . . . . . . . . . . . . . . . .
00360600
         00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF
                                                       .........?齱2222
00360610
         00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00 00
                                                       . . . . . . . . , . . . . . . .
00360620
         00360630
         00360640
         08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
                                                       ..6..?...6.@...
00360650
         00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
         80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
                                                       € 6...:.=...
00360660
        88 05 36 00 00 00 00 00 E0 1E 36 00 00 00 00 00
00360670
                                                       ?6....?6.....
00360680 01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
003606A0
```

可分配空间大小没有变化

```
0x00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
```

尾块起始位置没有变化

```
0x00360170 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
```

Lookaside[4]变成了@x00361EC8,刚好是h4分配的堆块

```
0x00360740 00 00 00 00 00 00 00 C8 1E 36 00 01 00 01 00
```

四次释放后的堆区

申请第五次

```
h2 = HeapAlloc(hp, HEAP_ZERO_MEMORY, 16);
```

```
0040106C |. 6A 10
                           push
                                   10
                                                                   ; /HeapSize = 10 (16.)
0040106E |. 6A 08
                           push
                                   8
                                                                    ; |Flags = HEAP_ZERO_MEMORY
00401070 |. 56
                           push
                                   esi
                                                                    : | hHeap
00401071 |. FFD7
                           call
                                   edi
                                                                    ; \HeapAlloc
```

16字节的空间那么应该是Lookaside[2]

先来看看堆区

```
00360010
  00 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
               . . . . . ? . . . . . . . . . . . . .
00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
               . ... ..$ ..2稞
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 00
               P.6.P.6.@ 6....
```

```
00 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00 .....?6.?6.
00360170
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00 € 6.€ 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 ?6.?6.?6.?6.
003601A0 A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00 ?6.?6.?6.?6.
         B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00 ?6.?6.?6.?6.
003601B0
         C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00
003601C0
                                                        ?6.?6.?6.?6.
003601D0
         D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00
                                                        ?6.?6.?6.?6.
003601E0
         E0 01 36 00 E0 01 36 00 E8 01 36 00 E8 01 36 00
                                                        ?6.?6.?6.?6.
003601F0
         F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                                        ?6.?6.?6.?6.
00360200
         00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
                                                         . 6.. 6. 6.
00360210
         10 02 36 00 10 02 36 00 18 02 36 00 18 02 36 00
00360220
         20 02 36 00 20 02 36 00 28 02 36 00 28 02 36 00
                                                          6. 6.(6.(6.
00360230
         30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00
                                                       0 6.0 6.8 6.8 6.
00360240
         40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
                                                        @ 6.@ 6.H 6.H 6.
         50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00
                                                       P 6.P 6.X 6.X 6.
00360250
                                                        ` 6.` 6.h 6.h 6.
         60 02 36 00 60 02 36 00 68 02 36 00 68 02 36 00
00360260
         70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00 p 6.p 6.x 6.x 6.
00360270
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
                                                        € 6.€ 6.?6.?6.
00360290
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00 ?6.?6.?6.?6.
003602A0 A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00 ?6.?6.?6.?6.
003602B0 B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00
                                                        ?6.?6.?6.?6.
003602C0    C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00
                                                        ?6.?6.?6.?6.
003602D0
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
                                                        ?6.?6.?6.?6.
003602E0 E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
                                                        ?6.?6.?6.?6.
003602F0 F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
                                                        ?6.?6.?6.?6.
00360300
         00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
                                                        . 6.. 6. 6. 6.
00360310    10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                          6. 6. 6.
00360320
         20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                                          6. 6.( 6.( 6.
00360330
         30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00
                                                        0 6.0 6.8 6.8 6.
00360340
         40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360350
         50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00
                                                        P 6.P 6.X 6.X 6.
00360360
                                                        ` 6.` 6.h 6.h 6.
         60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
00360370
         70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
         80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00 € 6.€ 6.?6.?6.
00360380
00360390
         90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00 ?6.?6.?6.?6.
003603A0 A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00 ?6.?6.?6.?6.
003603B0 B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00 ?6.?6.?6.?6.
003603C0 C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00 ?6.?6.?6.?6.
003603D0 D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00 ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00 ?6.?6.?6.?6.
003603F0 F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00 ?6.?6.?6.?6.
00360400 00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                        . 6.. 6. 6. 6.
00360410    10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                          6. 6. 6. 6.
00360420
         20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                          6. 6.(6.(6.
00360430
         30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00 0 6.0 6.8 6.8 6.
00360440
         40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360450
         50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                        P 6.P 6.X 6.X 6.
00360460
         60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
                                                        ` 6.` 6.h 6.h 6.
00360470
         70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00
                                                        p 6.p 6.x 6.x 6.
00360480
         80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                        € 6.€ 6.?6.?6.
00360490
         90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                        ?6.?6.?6.?6.
003604A0
         A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
                                                        ?6.?6.?6.?6.
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604B0
                                                        ?6.?6.?6.?6.
003604C0
         CO 04 36 00 CO 04 36 00 C8 04 36 00 C8 04 36 00
                                                        ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
                                                        ?6.?6.?6.?6.
003604E0
         E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                        ?6.?6.?6.?6.
003604F0
         F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
00360510 10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
00360520
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
                                                          6. 6.(6.(6.
00360530
         30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00
                                                        0 6.0 6.8 6.8 6.
00360540 40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360550
         50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                                        P 6.P 6.X 6.X 6.
                                                         ` 6.` 6.h 6.h 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
00360570
         70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
                                                        p 6.p 6. 6.....
00360580
         88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
                                                        ?6....06.
00360590
         00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
                                                        .?....?6.....
003605A0
         00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00
                                                        .....?6.....
003605B0 00 00 00 00 00 00 00 C8 05 36 00 00 00 00
```

```
003605C0
     00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00
                                 ......?6....
003605D0
     00 00 00 00 00 00 00 00 E8 05 36 00 00 00 00 00
     00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00 00
003605E0
003605F0
     99369699
     00 00 00 00 00 00 00 00 C0 06 FD 77 FF FF FF FF
                                 .......?鯫2222
00360610
     00360620
     00360630
     08 00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00
00360640
00360650
     00 00 36 00 00 D0 03 00 00 00 36 00 40 00 00 00
                                 ..6..?...6.@...
00360660
     80 06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00
                                 € 6...:.=...
00360670 88 05 36 00 00 00 00 00 E0 1E 36 00 00 00 00 00
00360680
     01 03 08 00 00 01 08 00 00 00 00 00 00 00 00 00
00360690
     99369649
     003606B0
     003606C0
003606D0
     . . . . . . . . . . . . . . . .
003606E0
     00 00 00 00 00 00 00 00 A0 1E 36 00 02 00 02 00
                                 003606F0
     04 00 00 01 02 00 00 00 02 00 00 00 02 00 00 00
00360700
     00360710
     00360720
     04 00 00 01 02 00 00 00 01 00 00 00 01 00 00 00
00360730
     00360740 00 00 00 00 00 00 00 C8 1E 36 00 01 00 01 00
```

可以看到Lookaside[2]后面串着的堆块已经不见了,因为如果是8的整数倍的空间申请,优先使用快表

释放第五次

```
HeapFree(hp, 0, h2);
00401073 |. 50
                                                                    ; /pMemory = 00361EB0
                           push
                                   eax
00401074 |. 6A 00
                                                                    ; |Flags = 0
                           push
                                   0
00401076 |.
             56
                           push
                                   esi
                                                                    ; |hHeap
00401077 |. FFD3
                           call
                                                                    ; \HeapFree
```

```
00360000 C8 00 00 00 01 00 00 FF EE FF EE 02 10 00 00 ?.....??? ..
00360010 00 00 00 00 FE 00 00 00 10 00 00 20 00 00
00360020 00 02 00 00 00 20 00 00 24 02 00 00 FF EF FD 7F
00360030 04 00 08 06 00 00 00 00 00 00 00 00 00 00 00
00360040 00 00 00 00 98 05 36 00 0F 00 00 00 F8 FF FF FF
00360050 50 00 36 00 50 00 36 00 40 06 36 00 00 00 00 0 P.6.P.6.@ 6.....
003600B0
003600C0
    . . . . . . . . . . . . . . . .
003600D0
    003600E0
    003600F0
00360100
    00360110
    00360120
    00360130
    00360140
    00360150
00360160
    00360170
    00 00 00 00 00 00 00 00 E8 1E 36 00 E8 1E 36 00
                          .......?6.?6.
00360180 80 01 36 00 80 01 36 00 88 01 36 00 88 01 36 00 € 6.€ 6.?6.?6.
00360190 90 01 36 00 90 01 36 00 98 01 36 00 98 01 36 00 ?6.?6.?6.?6.
```

```
003601A0
         A0 01 36 00 A0 01 36 00 A8 01 36 00 A8 01 36 00
         B0 01 36 00 B0 01 36 00 B8 01 36 00 B8 01 36 00
003601B0
                                                         ?6.?6.?6.?6.
         C0 01 36 00 C0 01 36 00 C8 01 36 00 C8 01 36 00
003601C0
                                                         ?6.?6.?6.?6.
         D0 01 36 00 D0 01 36 00 D8 01 36 00 D8 01 36 00
003601D0
                                                         ?6.?6.?6.?6.
003601E0
         F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                                         26.26.26.26.
003601F0
         F0 01 36 00 F0 01 36 00 F8 01 36 00 F8 01 36 00
                                                         ?6.?6.?6.?6.
         00 02 36 00 00 02 36 00 08 02 36 00 08 02 36 00
00360200
                                                         . 6.. 6. 6.
6. 6. 6. 6.
        20 02 36 00 20 02 36 00 28 02 36 00 28 02 36 00
00360220
                                                          6. 6.(6.(6.
00360230 30 02 36 00 30 02 36 00 38 02 36 00 38 02 36 00 0 6.0 6.8 6.8 6.
00360240 40 02 36 00 40 02 36 00 48 02 36 00 48 02 36 00
                                                        @ 6.@ 6.H 6.H 6.
00360250 50 02 36 00 50 02 36 00 58 02 36 00 58 02 36 00
                                                        P 6.P 6.X 6.X 6.
00360260 \quad 60 \ 02 \ 36 \ 00 \ 60 \ 02 \ 36 \ 00 \ 68 \ 02 \ 36 \ 00 \ 68 \ 02 \ 36 \ 00
                                                         ` 6.` 6.h 6.h 6.
00360270 70 02 36 00 70 02 36 00 78 02 36 00 78 02 36 00
                                                        p 6.p 6.x 6.x 6.
00360280 80 02 36 00 80 02 36 00 88 02 36 00 88 02 36 00
                                                         € 6.€ 6.?6.?6.
00360290
         90 02 36 00 90 02 36 00 98 02 36 00 98 02 36 00
                                                         ?6.?6.?6.?6.
003602A0
         A0 02 36 00 A0 02 36 00 A8 02 36 00 A8 02 36 00
                                                         ?6.?6.?6.?6.
003602B0
         B0 02 36 00 B0 02 36 00 B8 02 36 00 B8 02 36 00
                                                         ?6.?6.?6.?6.
003602C0
         C0 02 36 00 C0 02 36 00 C8 02 36 00 C8 02 36 00
                                                         ?6.?6.?6.?6.
003602D0
         D0 02 36 00 D0 02 36 00 D8 02 36 00 D8 02 36 00
                                                         ?6.?6.?6.?6.
003602E0
         E0 02 36 00 E0 02 36 00 E8 02 36 00 E8 02 36 00
003602F0
         F0 02 36 00 F0 02 36 00 F8 02 36 00 F8 02 36 00
         00 03 36 00 00 03 36 00 08 03 36 00 08 03 36 00
00360300
                                                         . 6.. 6. 6.
00360310 10 03 36 00 10 03 36 00 18 03 36 00 18 03 36 00
                                                          6. 6. 6. 6.
00360320
         20 03 36 00 20 03 36 00 28 03 36 00 28 03 36 00
                                                          6. 6.(6.(6.
        30 03 36 00 30 03 36 00 38 03 36 00 38 03 36 00 0 6.0 6.8 6.8 6.
00360330
00360340 40 03 36 00 40 03 36 00 48 03 36 00 48 03 36 00 @ 6.@ 6.H 6.H 6.
00360350 50 03 36 00 50 03 36 00 58 03 36 00 58 03 36 00 P 6.P 6.X 6.X 6.
00360360 60 03 36 00 60 03 36 00 68 03 36 00 68 03 36 00
                                                       ` 6.` 6.h 6.h 6.
00360370 70 03 36 00 70 03 36 00 78 03 36 00 78 03 36 00 p 6.p 6.x 6.x 6.
00360380 80 03 36 00 80 03 36 00 88 03 36 00 88 03 36 00 € 6.€ 6.?6.?6.
00360390 90 03 36 00 90 03 36 00 98 03 36 00 98 03 36 00 ?6.?6.?6.?6.
003603A0 A0 03 36 00 A0 03 36 00 A8 03 36 00 A8 03 36 00 ?6.?6.?6.?6.
003603B0 B0 03 36 00 B0 03 36 00 B8 03 36 00 B8 03 36 00 ?6.?6.?6.?6.
003603C0 C0 03 36 00 C0 03 36 00 C8 03 36 00 C8 03 36 00 ?6.?6.?6.?6.
003603D0
         D0 03 36 00 D0 03 36 00 D8 03 36 00 D8 03 36 00 ?6.?6.?6.?6.
003603E0 E0 03 36 00 E0 03 36 00 E8 03 36 00 E8 03 36 00
                                                        ?6.?6.?6.?6.
         F0 03 36 00 F0 03 36 00 F8 03 36 00 F8 03 36 00
003603F0
                                                         ?6.?6.?6.?6.
00360400
         00 04 36 00 00 04 36 00 08 04 36 00 08 04 36 00
                                                         . 6.. 6. 6.
                                                                     6.
00360410
         10 04 36 00 10 04 36 00 18 04 36 00 18 04 36 00
                                                          6. 6. 6.
00360420
         20 04 36 00 20 04 36 00 28 04 36 00 28 04 36 00
                                                          6. 6.(6.(6.
00360430
         30 04 36 00 30 04 36 00 38 04 36 00 38 04 36 00
                                                         0 6.0 6.8 6.8 6.
00360440
         40 04 36 00 40 04 36 00 48 04 36 00 48 04 36 00
                                                         @ 6.@ 6.H 6.H 6.
00360450
         50 04 36 00 50 04 36 00 58 04 36 00 58 04 36 00
                                                        P 6.P 6.X 6.X 6.
                                                         ` 6.` 6.h 6.h 6.
00360460
         60 04 36 00 60 04 36 00 68 04 36 00 68 04 36 00
00360470
         70 04 36 00 70 04 36 00 78 04 36 00 78 04 36 00 p 6.p 6.x 6.x 6.
00360480
         80 04 36 00 80 04 36 00 88 04 36 00 88 04 36 00
                                                         € 6.€ 6.?6.?6.
00360490
         90 04 36 00 90 04 36 00 98 04 36 00 98 04 36 00
                                                         ?6.?6.?6.?6.
003604A0
         A0 04 36 00 A0 04 36 00 A8 04 36 00 A8 04 36 00
003604B0
         B0 04 36 00 B0 04 36 00 B8 04 36 00 B8 04 36 00
003604C0    C0    04    36    00    C0    04    36    00    C8    04    36    00    C8    04    36    00
                                                         ?6.?6.?6.?6.
003604D0
         D0 04 36 00 D0 04 36 00 D8 04 36 00 D8 04 36 00
                                                         ?6.?6.?6.?6.
003604E0 E0 04 36 00 E0 04 36 00 E8 04 36 00 E8 04 36 00
                                                         ?6.?6.?6.?6.
003604F0 F0 04 36 00 F0 04 36 00 F8 04 36 00 F8 04 36 00
                                                         ?6.?6.?6.?6.
00360500
         00 05 36 00 00 05 36 00 08 05 36 00 08 05 36 00
                                                         . 6.. 6. 6. 6.
00360510
         10 05 36 00 10 05 36 00 18 05 36 00 18 05 36 00
                                                          6. 6. 6. 6.
00360520
         20 05 36 00 20 05 36 00 28 05 36 00 28 05 36 00
                                                          6. 6.(6.(6.
00360530
         30 05 36 00 30 05 36 00 38 05 36 00 38 05 36 00
                                                         0 6.0 6.8 6.8 6.
00360540
         40 05 36 00 40 05 36 00 48 05 36 00 48 05 36 00
                                                         @ 6.@ 6.H 6.H 6.
00360550
         50 05 36 00 50 05 36 00 58 05 36 00 58 05 36 00
                                                         P 6.P 6.X 6.X 6.
                                                         ` 6.` 6.h 6.h 6.
00360560
         60 05 36 00 60 05 36 00 68 05 36 00 68 05 36 00
         70 05 36 00 70 05 36 00 08 06 36 00 00 00 00 00
00360570
                                                         p 6.p 6. 6....
00360580
         88 06 36 00 00 00 01 00 00 00 00 00 00 30 36 00
00360590
         00 D0 03 00 00 00 00 00 A8 05 36 00 00 00 00 00
003605A0
         00 00 00 00 00 00 00 00 B8 05 36 00 00 00 00 00
         00 00 00 00 00 00 00 00 C8 05 36 00 00 00 00 00
003605B0
         00 00 00 00 00 00 00 00 D8 05 36 00 00 00 00
003605C0
003605D0 00 00 00 00 00 00 00 E8 05 36 00 00 00 00
                                                        . . . . . . . . ?6 . . . . .
003605E0
         00 00 00 00 00 00 00 00 F8 05 36 00 00 00 00
```

00360610	90 00 00 00 00 00 2C 00 00 00 00 00 00 00	
00360620	00 00 00 00 00 00 00 00 00 00 00 00 00	
00360630	00 00 00 00 00 00 00 00 00 00 00 00 00	
00360640	00 C8 00 00 01 00 00 EE FF EE FF 00 00 00 00 .???	
00360650	90 36 00 00 D0 03 00 00 00 36 00 40 00 00 006?6.@	
00360660	06 36 00 00 00 3A 00 3D 00 00 00 01 00 00 00 € 6:.=	
00360670	35 36 00 00 00 00 E0 1E 36 00 00 00 00 ?6?6	
00360680	33 08 00 00 01 08 00 00 00 00 00 00 00 00 00	
00360690	00 00 01 00 00 00 00 00 00 00 00 00 00 0	
003606A0	00 00 00 00 00 00 00 00 00 00 00 00 00	
003606B0	00 00 00 00 00 00 00 00 00 00 00 00 00	
003606C0	00 00 01 00 00 00 00 00 00 00 00 00 00 0	
003606D0	00 00 00 00 00 00 00 00 00 00 00 00 00	
003606E0	00 00 00 00 00 00 A0 1E 36 00 02 00 02 00?6	
003606F0	00 00 01 02 00 00 02 00 00 02 00 00 00	
00360700	00 00 00 00 00 00 00 00 00 00 00 00 00	
00360710	00 00 00 00 00 00 B0 1E 36 00 01 00 03 00?6	
00360720	00 00 01 02 00 00 01 00 00 00 02 00 00 00	
00360730	00 00 00 00 00 00 00 00 00 00 00 00 00	
00360740	00 00 00 00 00 00 C8 1E 36 00 01 00 01 00?6	
00360750	00 00 01 01 00 00 00 01 00 00 01 00 00 0	
00360760	00 00 00 00 00 00 00 00 00 00 00 00 00	

可以看到释放的16字节堆块又串在了Lookaside[2]上

```
0x00360710 00 00 00 00 00 00 00 B0 1E 36 00 01 00 03 00
```

以上就是快表的使用