

Linklab report

2019-12333 정윤서

1. 실행 결과

<part1>

test1, test2, test3, test5는 illegal deallocation 시도가 없었기 때문에 에러를 발생시키지 않지만, test4의 경우 free(a), free((void*)0x1706e90) instruction이 각각 double free, illegal free를 시도해 free(a)에서 오류가 나서 abort되었습니다. 이는 직접 구현한 free 함수에서 call한 freep에서 double free 과정에서 에러가 났기 때문입니다.

- test1

```
stu95@sp01:~/linklab/handout/part1$ make run test1
cc -I. -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x556e1339c2d0
[0003]     malloc( 32 ) = 0x556e1339c6e0
[0004]     malloc( 1 ) = 0x556e1339c710
[0005]     free( 0x556e1339c710 )
[0006]     free( 0x556e1339c6e0 )
[0007]
[0008] Statistics
[0009]     allocated_total      1057
[0010]     allocated_avg        352
[0011]     freed_total          0
[0012]
[0013] Memory tracer stopped.
stu95@sp01:~/linklab/handout/part1$
```

- test2

```
stu95@sp01:~/linklab/handout/part1$ make run test2
cc -I. -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x557d9d38d2d0
[0003]     free( 0x557d9d38d2d0 )
[0004]
[0005] Statistics
[0006]     allocated_total      1024
[0007]     allocated_avg        1024
[0008]     freed_total          0
[0009]
[0010] Memory tracer stopped.
stu95@sp01:~/linklab/handout/part1$
```

- test3

```
stu95@sp01:~/linklab/handout/part1$ make run test3
cc -I. -I .../utils -o libmemtrace.so -shared -fPIC memtrace.c .../utils/memlist.c .../utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 41515 ) = 0x55c05426d2d0
[0003]     malloc( 48963 ) = 0x55c054277510
[0004]     malloc( 12273 ) = 0x55c054283460
[0005]     calloc( 1 , 58928 ) = 0x55c054286460
[0006]     calloc( 1 , 23059 ) = 0x55c054294aa0
[0007]     malloc( 58352 ) = 0x55c05429a4c0
[0008]     calloc( 1 , 49934 ) = 0x55c0542a88c0
[0009]     malloc( 19945 ) = 0x55c0542b4be0
[0010]     calloc( 1 , 6086 ) = 0x55c0542b99e0
[0011]     calloc( 1 , 62737 ) = 0x55c0542bb1b0
[0012]     free( 0x55c0542bb1b0 )
[0013]     free( 0x55c0542b99e0 )
[0014]     free( 0x55c0542b4be0 )
[0015]     free( 0x55c0542a88c0 )
[0016]     free( 0x55c05429a4c0 )
[0017]     free( 0x55c054294aa0 )
[0018]     free( 0x55c054286460 )
[0019]     free( 0x55c054283460 )
[0020]     free( 0x55c054277510 )
[0021]     free( 0x55c05426d2d0 )
[0022]
[0023] Statistics
[0024]     allocated_total      381792
[0025]     allocated_avg        38179
[0026]     freed_total          0
[0027]
[0028] Memory tracer stopped.
stu95@sp01:~/linklab/handout/part1$ make run test4
```

- test4

```
stu95@sp01:~/linklab/handout/part1$ make run test4
cc -I. -I .../utils -o libmemtrace.so -shared -fPIC memtrace.c .../utils/memlist.c .../utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x55e02cd122d0
[0003]     free( 0x55e02cd122d0 )
free(): double free detected in tcache 2
Aborted
make: *** [Makefile:37: run] Error 134
```

- test5

```
stu95@sp01:~/linklab/handout/part1$ make run test5
cc -I. -I .../utils -o libmemtrace.so -shared -fPIC memtrace.c .../utils/memlist.c .../utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 10 ) = 0x564460e482d0
[0003]     realloc( 0x564460e482d0 , 100 ) = 0x564460e482d0
[0004]     realloc( 0x564460e482d0 , 1000 ) = 0x564460e482d0
[0005]     realloc( 0x564460e482d0 , 10000 ) = 0x564460e482d0
[0006]     realloc( 0x564460e482d0 , 100000 ) = 0x564460e482d0
[0007]     free( 0x564460e482d0 )
[0008]
[0009] Statistics
[0010]     allocated_total      111110
[0011]     allocated_avg        22222
[0012]     freed_total          0
[0013]
[0014] Memory tracer stopped.
```

<part2>

여전히 test4에서만 abort되며, part1과 다르게 freed_total[0] 계산되고 free해준 메모리는 몇 byte이며 free되지 않은 메모리는 몇 byte인지 tracing되어 나타납니다. Test1를 제외하고는 할당된 메모리가 전부 free되었지만, test1에서는 가장 처음 할당된 메모리가 free되지 않았기 때문에 Non-deallocated memory block이 로그로 나타납니다. Reallocated가 발생 했을 때 free된 기존 메모리는 freed_total[0]에 포함됩니다.

- test1

```
stu95@sp01:~/linklab/handout/part2$ make run test1
cc -I .. utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x556d0a5932d0
[0003]     malloc( 32 ) = 0x556d0a593710
[0004]     malloc( 1 ) = 0x556d0a593770
[0005]     free( 0x556d0a593770 )
[0006]     free( 0x556d0a593710 )
[0007]
[0008] Statistics
[0009]     allocated_total      1057
[0010]     allocated_avg        352
[0011]     freed_total          33
[0012]
[0013] Non-deallocated memory blocks
[0014]     block             size    ref cnt
[0015]     0x556d0a5932d0     1024      1
[0016]
[0017] Memory tracer stopped.
```

- test2

```
stu95@sp01:~/linklab/handout/part2$ make run test2
cc -I .. utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x55b2737282d0
[0003]     free( 0x55b2737282d0 )
[0004]
[0005] Statistics
[0006]     allocated_total      1024
[0007]     allocated_avg        1024
[0008]     freed_total          1024
[0009]
[0010] Memory tracer stopped.
```

- test3

```
stu95@sp01:~/linklab/handout/part2$ make run test3
cc -I . -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 42768 ) = 0x55e15b40b2d0
[0003]     malloc( 4217 ) = 0x55e15b415a20
[0004]     malloc( 63839 ) = 0x55e15b416ae0
[0005]     malloc( 4750 ) = 0x55e15b426480
[0006]     malloc( 22399 ) = 0x55e15b427750
[0007]     malloc( 2836 ) = 0x55e15b42cf10
[0008]     malloc( 37277 ) = 0x55e15b42da60
[0009]     malloc( 16855 ) = 0x55e15b436c40
[0010]     malloc( 18867 ) = 0x55e15b43ae50
[0011]     calloc( 1 , 45392 ) = 0x55e15b43f840
[0012]     free( 0x55e15b43f840 )
[0013]     free( 0x55e15b43ae50 )
[0014]     free( 0x55e15b436c40 )
[0015]     free( 0x55e15b42da60 )
[0016]     free( 0x55e15b42cf10 )
[0017]     free( 0x55e15b427750 )
[0018]     free( 0x55e15b426480 )
[0019]     free( 0x55e15b416ae0 )
[0020]     free( 0x55e15b415a20 )
[0021]     free( 0x55e15b40b2d0 )
[0022]
[0023] Statistics
[0024]     allocated_total      259200
[0025]     allocated_avg        25920
[0026]     freed_total          259200
[0027]
[0028] Memory tracer stopped.
```

- test4

```
stu95@sp01:~/linklab/handout/part2$ make run test4
cc -I . -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x55d0ff8652d0
[0003]     free( 0x55d0ff8652d0 )
free(): double free detected in tcache 2
Aborted
make: *** [Makefile:37: run] Error 134
```

- test5

```
stu95@sp01:~/linklab/handout/part2$ make run test5
cc -I . -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 10 ) = 0x55ed06d412d0
[0003]     realloc( 0x55ed06d412d0 , 100 ) = 0x55ed06d41320
[0004]     realloc( 0x55ed06d41320 , 1000 ) = 0x55ed06d413c0
[0005]     realloc( 0x55ed06d413c0 , 10000 ) = 0x55ed06d417e0
[0006]     realloc( 0x55ed06d417e0 , 100000 ) = 0x55ed06d43f30
[0007]     free( 0x55ed06d43f30 )
[0008]
[0009] Statistics
[0010]     allocated_total      111110
[0011]     allocated_avg        22222
[0012]     freed_total          111110
[0013]
[0014] Memory tracer stopped.
```

<part3>

test4를 제외한 나머지 결과는 part1, part2와 같습니다. 이는 test4에서만 free() 함수에서 double free, illegal free가 일어났기 때문입니다. double free, illegal free는 freed_total에 포함되지 않으며, ignore됩니다.

- test1

```
stu95@sp01:~/linklab/handout/part3$ make run test1
cc -I. -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]      malloc( 1024 ) = 0x565047f462d0
[0003]      malloc( 32 ) = 0x565047f46710
[0004]      malloc( 1 ) = 0x565047f46770
[0005]      free( 0x565047f46770 )
[0006]      free( 0x565047f46710 )
[0007]
[0008] Statistics
[0009]   allocated_total     1057
[0010]   allocated_avg       352
[0011]   freed_total         33
[0012]
[0013] Non-deallocated memory blocks
[0014]   block           size   ref cnt
[0015]   0x565047f462d0    1024      1
[0016]
[0017] Memory tracer stopped.
```

- test2

```
stu95@sp01:~/linklab/handout/part3$ make run test2
cc -I. -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]      malloc( 1024 ) = 0x55dbeafa5d2d0
[0003]      free( 0x55dbeafa5d2d0 )
[0004]
[0005] Statistics
[0006]   allocated_total     1024
[0007]   allocated_avg       1024
[0008]   freed_total         1024
[0009]
[0010] Memory tracer stopped.
```

- test3

```
stu95@sp01:~/linklab/handout/part3$ make run test3
cc -I .. ./utils -o libmemtrace.so -shared -fPIC memtrace.c .. ./utils/memlist.c .. ./utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     calloc( 1 , 3145 ) = 0x55f26e25b2d0
[0003]     malloc( 54234 ) = 0x55f26e25bf60
[0004]     calloc( 1 , 44580 ) = 0x55f26e269380
[0005]     malloc( 12558 ) = 0x55f26e2741e0
[0006]     calloc( 1 , 52157 ) = 0x55f26e277330
[0007]     calloc( 1 , 16664 ) = 0x55f26e283f30
[0008]     malloc( 18310 ) = 0x55f26e288080
[0009]     malloc( 53936 ) = 0x55f26e28c840
[0010]     malloc( 8673 ) = 0x55f26e299b30
[0011]     calloc( 1 , 29033 ) = 0x55f26e29bd50
[0012]     free( 0x55f26e29bd50 )
[0013]     free( 0x55f26e299b30 )
[0014]     free( 0x55f26e28c840 )
[0015]     free( 0x55f26e288080 )
[0016]     free( 0x55f26e283f30 )
[0017]     free( 0x55f26e277330 )
[0018]     free( 0x55f26e2741e0 )
[0019]     free( 0x55f26e269380 )
[0020]     free( 0x55f26e25bf60 )
[0021]     free( 0x55f26e25b2d0 )
[0022]
[0023] Statistics
[0024]   allocated_total      293290
[0025]   allocated_avg        29329
[0026]   freed_total          293290
[0027]
[0028] Memory tracer stopped.
```

- test4

```
stu95@sp01:~/linklab/handout/part3$ make run test4
cc -I .. ./utils -o libmemtrace.so -shared -fPIC memtrace.c .. ./utils/memlist.c .. ./utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 1024 ) = 0x5609a78bb2d0
[0003]     free( 0x5609a78bb2d0 )
[0004]     free( 0x5609a78bb2d0 )
[0005]     *** DOUBLE_FREE *** (ignoring)
[0006]     free( 0x1706e90 )
[0007]     *** ILLEGAL_FREE *** (ignoring)
[0008]
[0009] Statistics
[0010]   allocated_total      1024
[0011]   allocated_avg        1024
[0012]   freed_total          1024
[0013]
[0014] Memory tracer stopped.
```

- test5

```
stu95@sp01:~/linklab/handout/part3$ make run test5
cc -I .. ./utils -o libmemtrace.so -shared -fPIC memtrace.c .. ./utils/memlist.c .. ./utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 10 ) = 0x55bf1e8742d0
[0003]     realloc( 0x55bf1e8742d0 , 100 ) = 0x55bf1e874320
[0004]     realloc( 0x55bf1e874320 , 1000 ) = 0x55bf1e8743c0
[0005]     realloc( 0x55bf1e8743c0 , 10000 ) = 0x55bf1e8747e0
[0006]     realloc( 0x55bf1e8747e0 , 100000 ) = 0x55bf1e876f30
[0007]     free( 0x55bf1e876f30 )
[0008]
[0009] Statistics
[0010]   allocated_total      111110
[0011]   allocated_avg        22222
[0012]   freed_total          111110
[0013]
[0014] Memory tracer stopped.
```

<Bonus Test for part3>

realloc에서 double free, illegal free가 일어나는 경우를 살펴보기 위해 test6.c를 작성하였습니다. 이 경우 free는 무시되고 새로운 메모리가 할당되기 때문에 allocated_total에만 realloc된 메모리가 반영되며, freed_total에는 첫 번째 인자로 주어지는 포인터가 가리키는 메모리의 free가 반영되지 않습니다.

```
test > C test6.c > main(void)
1   #include <stdlib.h>
2
3
4 < int main(void)
5   [
6     void *a;
7     void *b;
8
9     a = malloc(10);
10    a = realloc((void*)0x1706e90, 100); //illegal -> original a unfreed,
11    b = realloc(a, 1000);
12    b = realloc(a, 10000); //double -> b unfreed
13    free(a); //double -> b unfreed
14
15    //10+1000+10000 unfreed
16
17   ]
```

```
stu95@sp01:~/linklab/handout/part3$ make run test6
cc -I. -I ..utils -o libmemtrace.so -shared -fPIC memtrace.c ..utils/memlist.c ..utils/memlog.c -ldl
[0001] Memory tracer started.
[0002]     malloc( 10 ) = 0x564f6052e2d0
[0003]     realloc( 0x1706e90 , 100 ) = 0x564f6052e320
[0004] *** ILLEGAL_FREE *** (ignoring)
[0005]     realloc( 0x564f6052e320 , 1000 ) = 0x564f6052e3c0
[0006]     realloc( 0x564f6052e320 , 10000 ) = 0x564f6052e7e0
[0007] *** DOUBLE_FREE *** (ignoring)
[0008]     free( 0x564f6052e320 )
[0009] *** DOUBLE_FREE *** (ignoring)
[0010]
[0011] Statistics
[0012]     allocated_total      11110
[0013]     allocated_avg        2777
[0014]     freed_total          100
[0015]
[0016] Non-deallocated memory blocks
[0017]     block           size     ref cnt
[0018]     0x564f6052e2d0     10       1
[0019]     0x564f6052e3c0    1000      1
[0020]     0x564f6052e7e0   10000      1
[0021]
[0022] Memory tracer stopped.
```

2. 구현 방법

- malloc

malloccp 함수가 정의되지 않은 경우 dlsym(RTLD_NEXT, "malloc")을 이용하여 standard c library의 malloc 함수를 assign해주고, malloccp를 이용하여 새로운 메모리를 할당해 주었습니다. 그 뒤 part1의 allocated memory tracing을 위하여 LOG_MALLOC을 사용하였으며, part2에서는 unfreed memory tracing을 위하여 alloc 함수를 사용해 포인터 주소와 할당된 메모리 사이즈를 갖는 아이템을 list에 등록해 주었습니다. destructor에서 statistics 로그를 남기기 위해서는 n_allocb(allocated_total)에 할당된 메모리 사이즈를 더해주고, n_malloc(allocated_avg)에서 n_allocb를 n_malloc+n_calloc+n_realloc으로 나눠주기 위함)을 1 증가시켰습니다.

- calloc

calloccp 함수가 정의되지 않은 경우 dlsym(RTLD_NEXT, "calloc")을 이용하여 standard c library의 calloc 함수를 assign해주고, calloccp를 이용하여 새로운 메모리를 할당해 주었습니다. 그 뒤 part1의 allocated memory tracing을 위하여 LOG_CALLOC을 사용하였으며, part2에서는 unfreed memory tracing을 위하여 alloc 함수를 사용해 포인터 주소와 할당된 메모리 사이즈를 갖는 아이템을 list에 등록해 주었습니다. destructor에서 statistics 로그를 남기기 위해서는 n_allocb에 할당된 메모리 사이즈를 더해주고, n_malloc을 1 증가시켰습니다.

- realloc

realloccp와 malloccp 모두를 사용해야 하기 때문에 malloc, calloc 함수에서처럼 두 함수가 정의되지 않은 경우 assign해 주었습니다. part1은 malloc, calloc과 비슷한 방법으로 구현하였지만 part2에서는 realloccp 내부적으로 기존 메모리를 free해줌을 가정하고 있기 때문에 이 부분을 list와 n_freeb(freed_total)에 반영해주기 위해 추가적으로 realloc_free(void* ptr)라는 함수를 구현하고 호출하였습니다. 이 함수에서는 free가 일어났을 때와 같이 deallocate 함수를 이용해 item의 reference count를 하나 줄여 주고, n_freeb에 deallocate이 return하는 아이템의 size 필드를 더해 주었습니다. realloc_free()를 alloc() 함수를 부르기 전에 먼저 사용하였기 때문에 deallocate에서 return되는 item의 size field는 기존에 할당되어 있던 메모리 사이즈를 반영하고 있습니다.

Part 3에서는 realloc_free()를 없애고, 그 대신에 find(list, ptr)의 값에 따라 free를 다르게 처리했습니다. find(list, ptr)==NULL인 경우는 illegal free가 발생할 것이므로 malloccp를 이용해 새로운 메모리를 할당하고, realloccp 함수는 호출하지 않았습니다. find(list, ptr)이 return하는 item의 count가 0보다 클 경우 illegal deallocation이 일어나지 않으므로 이전과 같이 처리했습니다. 그 외의 경우, 즉 find(list, ptr)가 NULL이 아닌데 0보다 같거나 작은 경우(코드가 정상적으로 작동한다면 0인 경우만 남음) double free가 발생할 것이므로 malloccp를 이용해 새로운 메모리를 할당하고 마찬가지로 realloccp는 호출하지 않은 채 필요한 로그값만 찍었습니다. 그러나 세 경우 모두 명목상으로는 deallocate이 발생한 것이므로 alloc을 통해 새로운 메모리를 list에 등록하고(혹은 item의 cnt를 올려주고) n_allocb에 새로운 메모리 사이즈를 더해주고 n_realloc을 1만큼 증가시켰습니다.

- free

freep 함수가 정의되지 않은 경우 `dlsym(RTLD_NEXT, "free")`을 이용하여 standard c library의 free 함수를 assign해주고, part 1에서는 freep를 이용하여 포인터를 곧바로 해제하고 로그를 남겼습니다. Part 2에서는 unfreed memory tracing을 위해 `dealloc(list, ptr)`를 호출하여 아이템의 cnt를 하나 줄이고 그 아이템의 size 값을 `n_freeb`에 더해 주었습니다. 그리고 destructor에서 list를 순회하며 cnt가 0이 아닌 item이 발견될 경우 item의 ptr, size, cnt(deallocated되지 않은 메모리의 정보들)를 로그에 남기도록 하였습니다. Part 3에서는 illegal deallocation을 찾고 무시할 수 있도록 해야 하기 때문에 `realloc`과 마찬가지로, `find(list, ptr)`의 값에 따라 다르게 처리하였습니다. 다만 이때는 `realloc`과 다르게 그냥 무시하기만 하면 되므로 item의 cnt가 0보다 큰 경우에만 이전과 같이 처리하고 나머지 경우에는 free 로그와 illegal deallocation과 관련된 로그만 남기도록 구현하였습니다.

3. 어려웠던 점

Part 3에서 `realloc`과 관련된 illegal deallocation을 어떻게 처리하면 좋을지 고민하는 것이 어려웠던 것 같습니다. Free의 경우 무시하고 로그만 찍으면 되는데, `realloc`의 경우 `reallocp`에서 내부적으로 실제 `free`를 부르기 때문에 어떻게 에러를 ignore하면서 `realloc`을 emulate할 것인지 결정하는 과정이 어려웠습니다.

4. 새롭게 배운 점

강의 자료만 보았을 때는 load/runtime library interpositioning이 어떻게 일어나는지 정도만 이해하고 있는 상태였는데, Makefile 코드를 살펴보고 `dlsym`을 이용해 interposition 과정을 구현해보니 dynamic linking과 그에 따른 interpositioning 원리를 제대로 이해할 수 있었습니다. 특히 `realloc()` 안에서 `reallocp()`를 부르고, 그 안에서 `free()`가 호출된다고 생각할 때 `reallocp()`에서 호출되는 `free()`는 preload한 interposition용 `free()`가 아니라는 점도 배울 수 있었습니다. 또 직접 코드를 짜보고 로그에 찍힌 포인터의 주소가 제대로 찍혀 있는지 확인함으로써 메모리의 할당과 해제가 어떻게 일어나는지, 또 메모리는 언제 해제되는 것인지 배울 수 있었습니다.