A heap, a stack, a bottle and a rack

ID1200

A heap, a stack, a bottle and a rack

- Memory map
- Stack
- Heap

The memory map

- Process identifier

  `./a.out &` will print the process identifier and run the program in the background.

- `cat /proc/<processid>/maps` will print the memory map

The memory map

```
55567d9ba000-55567d9bb000 r-xp 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbba000-55567dbbb000 r--p 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbbb000-55567dbbc000 rw-p 00001000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567f6ba000-55567f6db000 rw-p 00000000 00:00 0                          [heap]
7fb20871d000-7fb208904000 r-xp 00000000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208904000-7fb208b04000 ---p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b04000-7fb208b08000 r--p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b08000-7fb208b0a000 rw-p 001eb000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b0a000-7fb208b0e000 rw-p 00000000 00:00 0
7fb208b0e000-7fb208b35000 r-xp 00000000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d21000-7fb208d23000 rw-p 00000000 00:00 0
7fb208d35000-7fb208d36000 r--p 00027000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d36000-7fb208d37000 rw-p 00028000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d37000-7fb208d38000 rw-p 00000000 00:00 0
7fff7a4fb000-7fff7a51c000 rw-p 00000000 00:00 0                          [stack]
7fff7a5af000-7fff7a5b2000 r--p 00000000 00:00 0                          [vvar]
7fff7a5b2000-7fff7a5b4000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
```

The memory map

The code, read only data and global data

```
55567d9ba000-55567d9bb000 r-xp 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbba000-55567dbbb000 r--p 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbbb000-55567dbbc000 rw-p 00001000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567f6ba000-55567f6db000 rw-p 00000000 00:00 0                          [heap]
7fb20871d000-7fb208904000 r-xp 00000000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208904000-7fb208b04000 ---p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b04000-7fb208b08000 r--p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b08000-7fb208b0a000 rw-p 001eb000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b0a000-7fb208b0e000 rw-p 00000000 00:00 0
7fb208b0e000-7fb208b35000 r-xp 00000000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d21000-7fb208d23000 rw-p 00000000 00:00 0
7fb208d35000-7fb208d36000 r--p 00027000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d36000-7fb208d37000 rw-p 00028000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d37000-7fb208d38000 rw-p 00000000 00:00 0
7fff7a4fb000-7fff7a51c000 rw-p 00000000 00:00 0                          [stack]
7fff7a5af000-7fff7a5b2000 r--p 00000000 00:00 0                          [vvar]
7fff7a5b2000-7fff7a5b4000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
```

The memory map

The heap and the stack

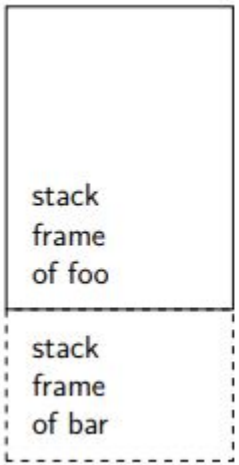
```
55567d9ba000-55567d9bb000 r-xp 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbba000-55567dbbb000 r--p 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbbb000-55567dbbc000 rw-p 00001000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567f6ba000-55567f6db000 rw-p 00000000 00:00 0                          [heap]
7fb20871d000-7fb208904000 r-xp 00000000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208904000-7fb208b04000 ---p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b04000-7fb208b08000 r--p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b08000-7fb208b0a000 rw-p 001eb000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b0a000-7fb208b0e000 rw-p 00000000 00:00 0
7fb208b0e000-7fb208b35000 r-xp 00000000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d21000-7fb208d23000 rw-p 00000000 00:00 0
7fb208d35000-7fb208d36000 r--p 00027000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d36000-7fb208d37000 rw-p 00028000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d37000-7fb208d38000 rw-p 00000000 00:00 0
7fff7a4fb000-7fff7a51c000 rw-p 00000000 00:00 0                          [stack]
7fff7a5af000-7fff7a5b2000 r--p 00000000 00:00 0                          [vvar]
7fff7a5b2000-7fff7a5b4000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
```

The memory map

Shared libraries

```
55567d9ba000-55567d9bb000 r-xp 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbba000-55567dbbb000 r--p 00000000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567dbbb000-55567dbbc000 rw-p 00001000 08:01 1049473                    /home/marcus/Documents/os/1_stack/a.out
55567f6ba000-55567f6db000 rw-p 00000000 00:00 0                          [heap]
7fb20871d000-7fb208904000 r-xp 00000000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208904000-7fb208b04000 ---p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b04000-7fb208b08000 r--p 001e7000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b08000-7fb208b0a000 rw-p 001eb000 08:01 1840747                    /lib/x86_64-linux-gnu/libc-2.27.so
7fb208b0a000-7fb208b0e000 rw-p 00000000 00:00 0
7fb208b0e000-7fb208b35000 r-xp 00000000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d21000-7fb208d23000 rw-p 00000000 00:00 0
7fb208d35000-7fb208d36000 r--p 00027000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d36000-7fb208d37000 rw-p 00028000 08:01 1840719                    /lib/x86_64-linux-gnu/ld-2.27.so
7fb208d37000-7fb208d38000 rw-p 00000000 00:00 0
7fff7a4fb000-7fff7a51c000 rw-p 00000000 00:00 0                          [stack]
7fff7a5af000-7fff7a5b2000 r--p 00000000 00:00 0                          [vvar]
7fff7a5b2000-7fff7a5b4000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
```

The stack



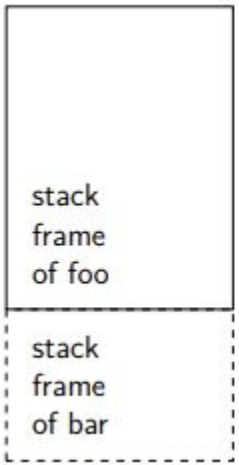

```
int foo(int x, int y) {
return x + y;
}

int bar() {
    int z;
    z = foo(3, 4)
    return z;
```

Call stack

1. Local variables
2. Arguments
3. Return address

The stack




```
int foo(int x, int y) {
return x + y;
}

int bar() {
    int z;
    z = foo(3, 4)
    return z;
```

Call stack

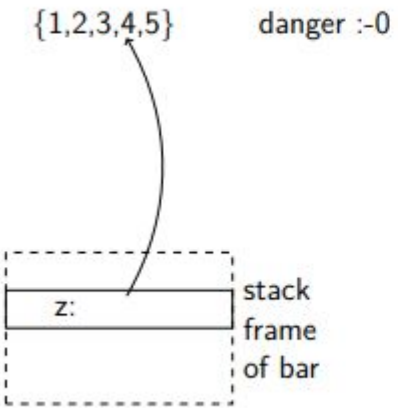
1. Local variables
2. Arguments
3. Return address

The stack

```
0x7fff82541c68  0x3                 r
0x7fff82541c70  0x7fff82541c70      i point at itself
0x7fff82541c78  0xcf7c1dcd64df1e00  Canaries?
0x7fff82541c80  0x7fff82541cb0      Previous EBP
0x7fff82541c88  0x558b0a30c81c      Return address (back to foo)
0x7fff82541c90  0x0                 Keep the stack frame aligned
0x7fff82541c98  0x7fff82541cc8      Point at p
0x7fff82541ca0  0x0                 Keep the stack frame aligned
0x7fff82541ca8  0x2                 q
0x7fff82541cb0  0x7fff82541d10      Previous EBP
0x7fff82541cb8  0x558b0a30c86a      Return address (back to main)
0x7fff82541cc0  0x1a7682541d28      Canaries?
0x7fff82541cc8  0x1                 p
    p: 0x7fff82541cc8
    back: 0x558b0a30c86a
```

Canaries?
https://en.wikipedia.org/wiki/Buffer_overflow_protection#Canaries

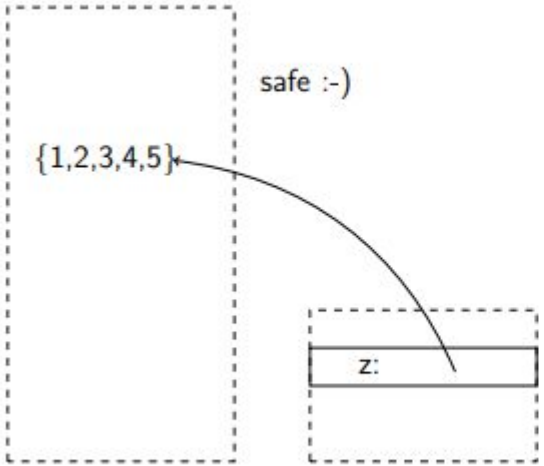
The heap




```
int *foo(int x) {
  int a[5] = {1,2,3,4,5};
  return a;
}
```

```
int bar() {
  int *z = foo(1);
  printf("z[2] is %d\n", z[2]);
  return 0;
}
```

The heap




```
int *foo(int x) {
  int a[5] = {1,2,3,4,5};
  int *h;
  int i;

  h = (int*)malloc(5*sizeof(int

  for(i = 0; i != 5; i++) {
    h[i] = a[i];
  }
  return h;
}
```

The heap

Usage

- `char *heap = malloc(20);` Allocate 20 bytes of memory on the heap
- `char *heap = calloc(20);` Same as malloc but also sets all bytes to zero.
- `heap = realloc(heap, 30);` Reallocated with new size of 30 bytes.
- `free(heap);` Free the memory where heap points

Git

`https://gits-15.sys.kth.se/johanmon/ID1206`

Exam 2018-01-12

1.2 memory map [2 points]

Below is a, somewhat shortened, printout of a memory mapping of a running process. Briefly describe the role of each segment marked with ???.

```
> cat /proc/13896/maps

00400000-00401000 r-xp 00000000 08:01 1723260            .../gurka ???
00600000-00601000 r--p 00000000 08:01 1723260            .../gurka ???
00601000-00602000 rw-p 00001000 08:01 1723260            .../gurka ???
022fa000-0231b000 rw-p 00000000 00:00 0                  [???]
7f6683423000-7f66835e2000 r-xp 00000000 08:01 3149003    .../libc-2.23.so ???
    :
7ffd60600000-7ffd60621000 rw-p 00000000 00:00 0          [???]
7ffd60648000-7ffd6064a000 r--p 00000000 00:00 0          [vvar]
7ffd6064a000-7ffd6064c000 r-xp 00000000 00:00 0          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0  [vsyscall]
```

Exam 2018-01-12

1.2 memory map [2 points]

Below is a, somewhat shortened, printout of a memory mapping of a running process. Briefly describe the role of each segment marked with ???.

```
> cat /proc/13896/maps

00400000-00401000 r-xp 00000000 08:01 1723260            .../gurka ???
00600000-00601000 r--p 00000000 08:01 1723260            .../gurka ???
00601000-00602000 rw-p 00001000 08:01 1723260            .../gurka ???
022fa000-0231b000 rw-p 00000000 00:00 0                  [???]
7f6683423000-7f66835e2000 r-xp 00000000 08:01 3149003    .../libc-2.23.so ???
    :
7ffd60600000-7ffd60621000 rw-p 00000000 00:00 0          [???]
7ffd60648000-7ffd6064a000 r--p 00000000 00:00 0          [vvar]
7ffd6064a000-7ffd6064c000 r-xp 00000000 00:00 0          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0  [vsyscall]
```

Answer: The first three segments are: code, read-only data and global data for the running process `gurka`. Then there is a segment for the *heap*. The segment marked with `lib-2.23.so` is a shard library. In the uppermost region we find the segment of the *stack*.