把玩链接器

1 原　sunnyxx iOS Developer | 滴滴出行

Weibo · @我就叫 Sunny 怎么了

Blog · http://blog.sunnyxx.com

GitHub · github.com/forkingdog

?i't '1 A 笃 闷闷了币 "l't -;i;

1 (111\.}电 Z E
ιO 巳

A
f•|'>
主

▾ I 4
c 12 i 马
崎

£. u M "1 f W
Hti 世 11 乌 ff; ' (.()
T Sτ !, QD 1l T 飞 ι

' r"';
M
u 'C
C.. 哥 0

1 ‹., 号 f
0 句

17 可 飞 G
A v C 飞 1
S

▌巴 : ?""、代

B L -
弓

句 .1

ν f 0 0 >
守

叫 u.... (• (,...f 可 可 可弓 L ι

c. • • •

2
2..; 吁 呼

1 7 1 cf,{,
(:

I 叫 V..¢'
ζ H I' (i, ı I: '1 1 守

{巳 c, 俨 r<)

• ι
f l

S 2 o.,
r.;2o c.i 2
?
11 7

c.,2 υ
2 Z 2..

oc c .f 3 1

oc ,f › C
?

2 问 P 崎 E
号 二Q
J 三 o c.

('b..).,II(\ l'<i \叫"

2 < I co

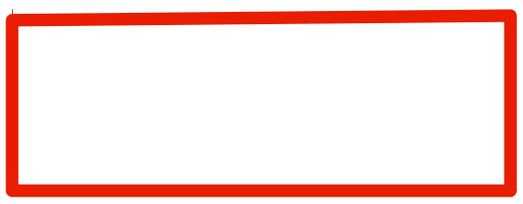
36

在一排开
关上 手撞机器码

PDP-11 / 40 1970s

打孔纸带读取器

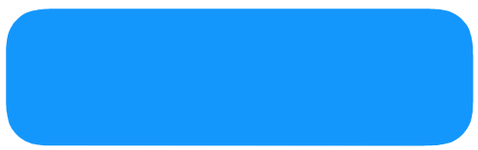
JMP 2000



PDP-11 Machine Code Sample

中间层

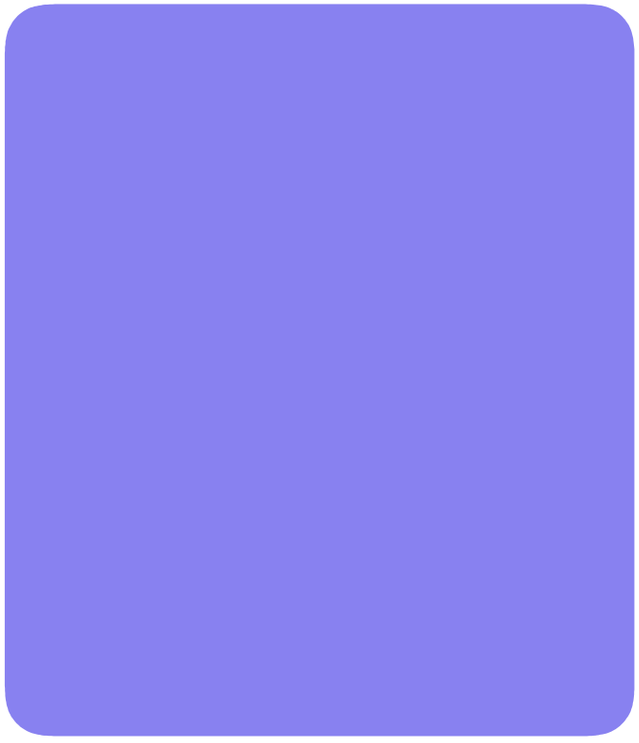
- 尼古拉斯 · 赵四



x86_64

翻译机器码

地址绋 ㄒ



Compiler Linker

```c
// my_math.c

int          int          int
      return

int          int          int
      return
```

```c
// main.c

int
      int                  1  2    return 0
```

```
// clang -c my_math.c -o
// my_math.o

int       int     int       return
```

```
int       int     int       return
```

my_math.o

记录当前文件中：

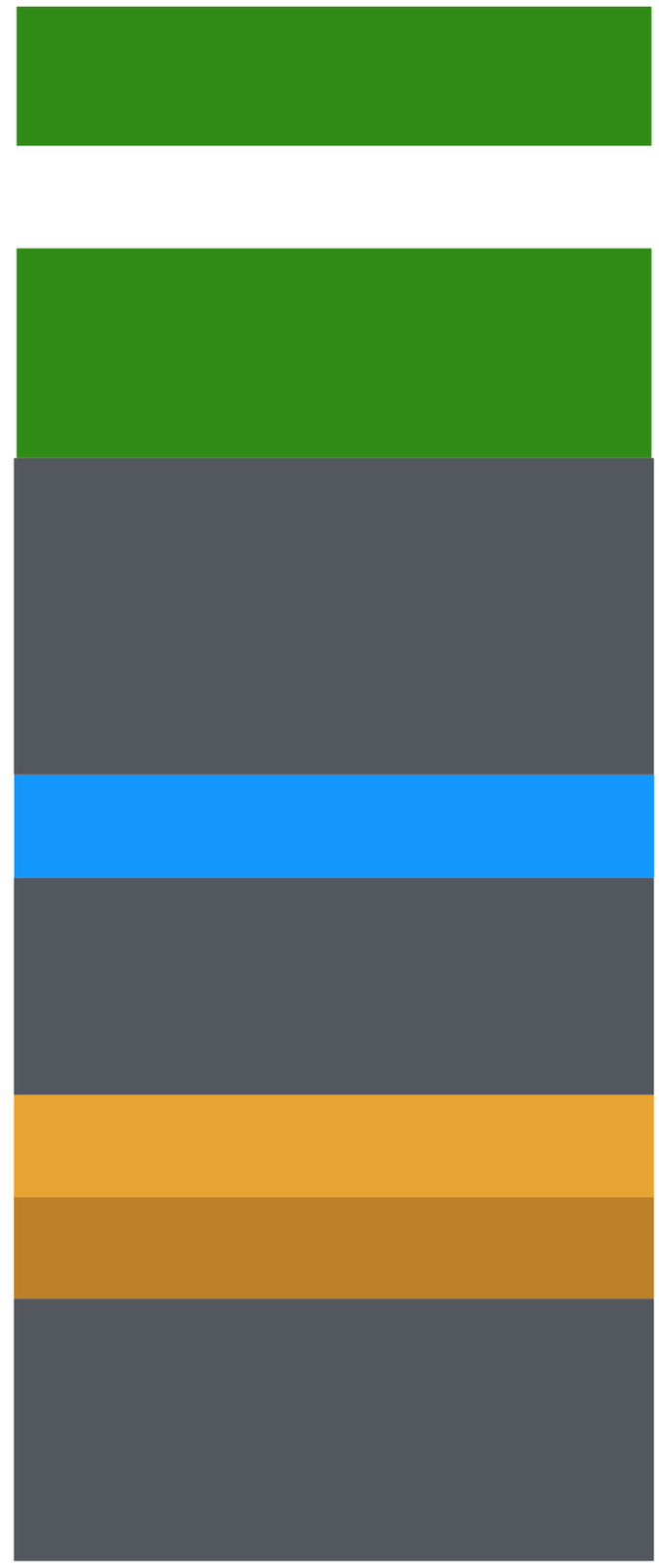
已定义

未定义

my_math.o

```
 callq 0x00000000

//    clang  -c  main.c
//    main.o

int
      int                  1   2
r
e
t
u
r
n
0
```

main.o



main.o

my_math.o

clang

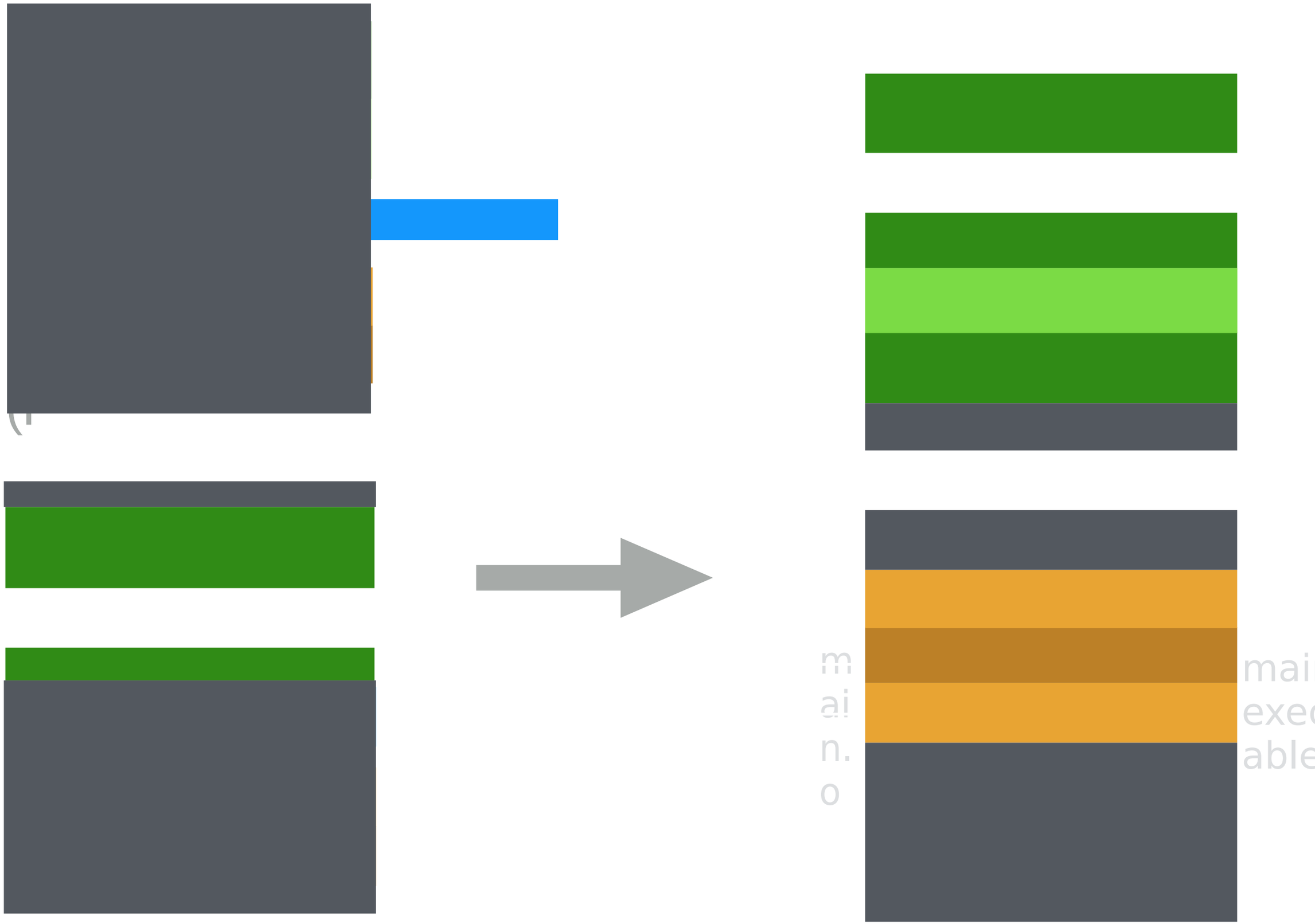
main

```
callq 0x000000000
```

my
_m
ath.
o

llq
0x00000000

ca

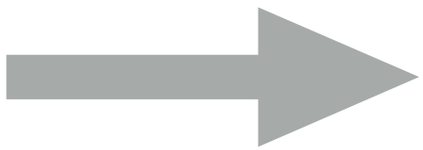

main.o
main
executable

```
callq 0x000000000
```

my
_m
ath.
o

llq
0x00000000

ca




main.o
main
executable

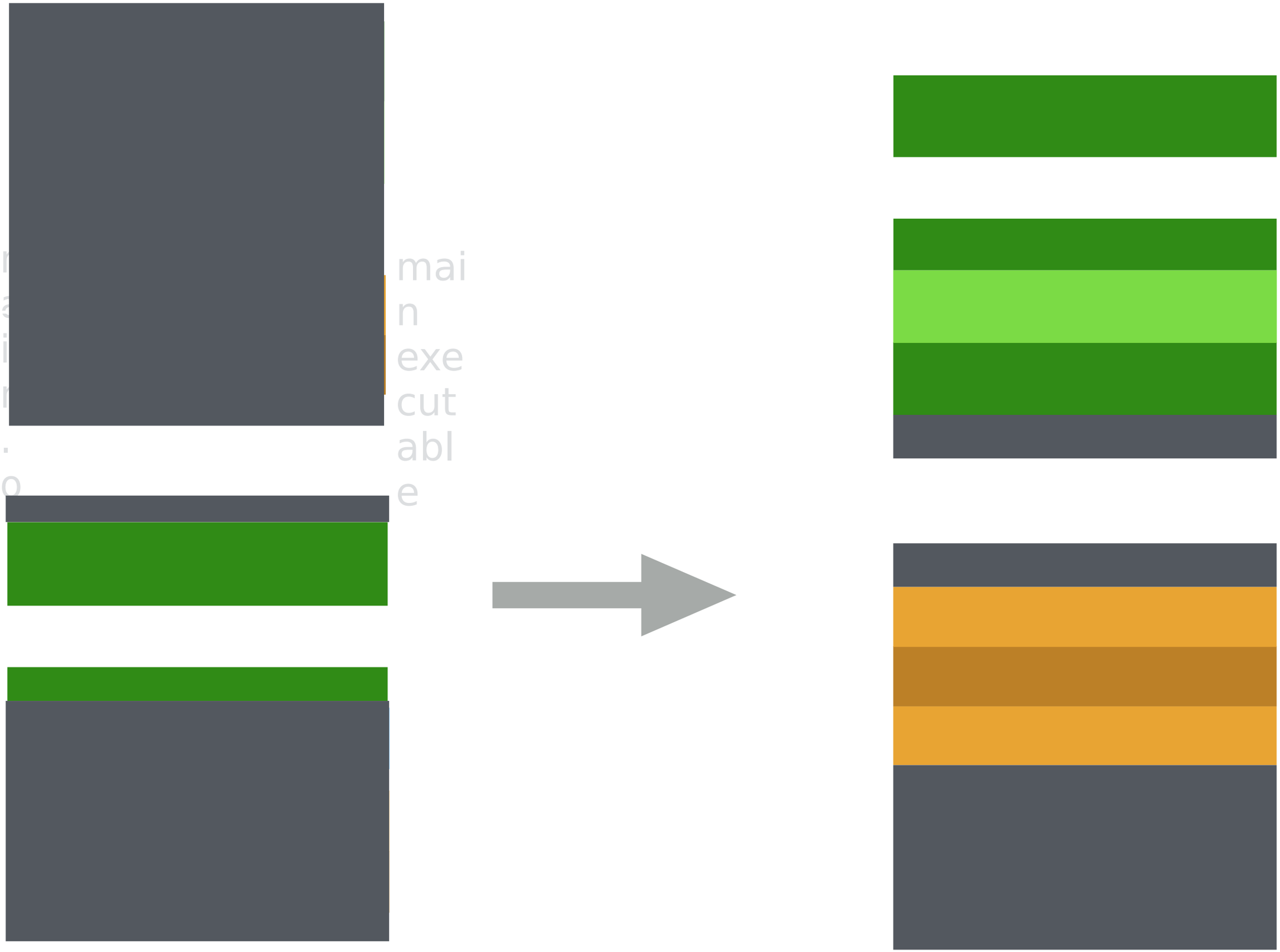
```
callq 0x000000000
```

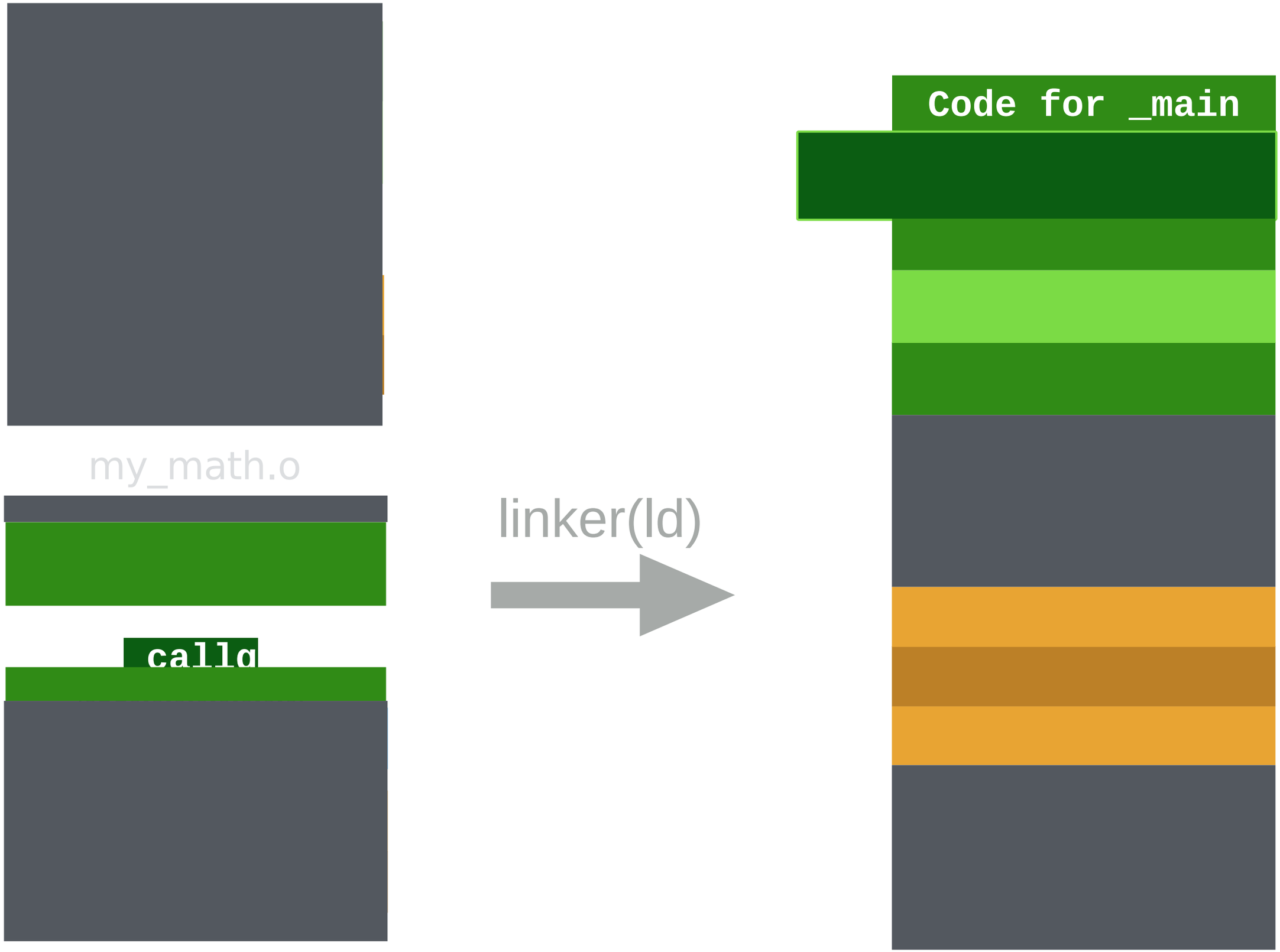
my_math.o

linker (ld)

ca

```
relocate _add!
```

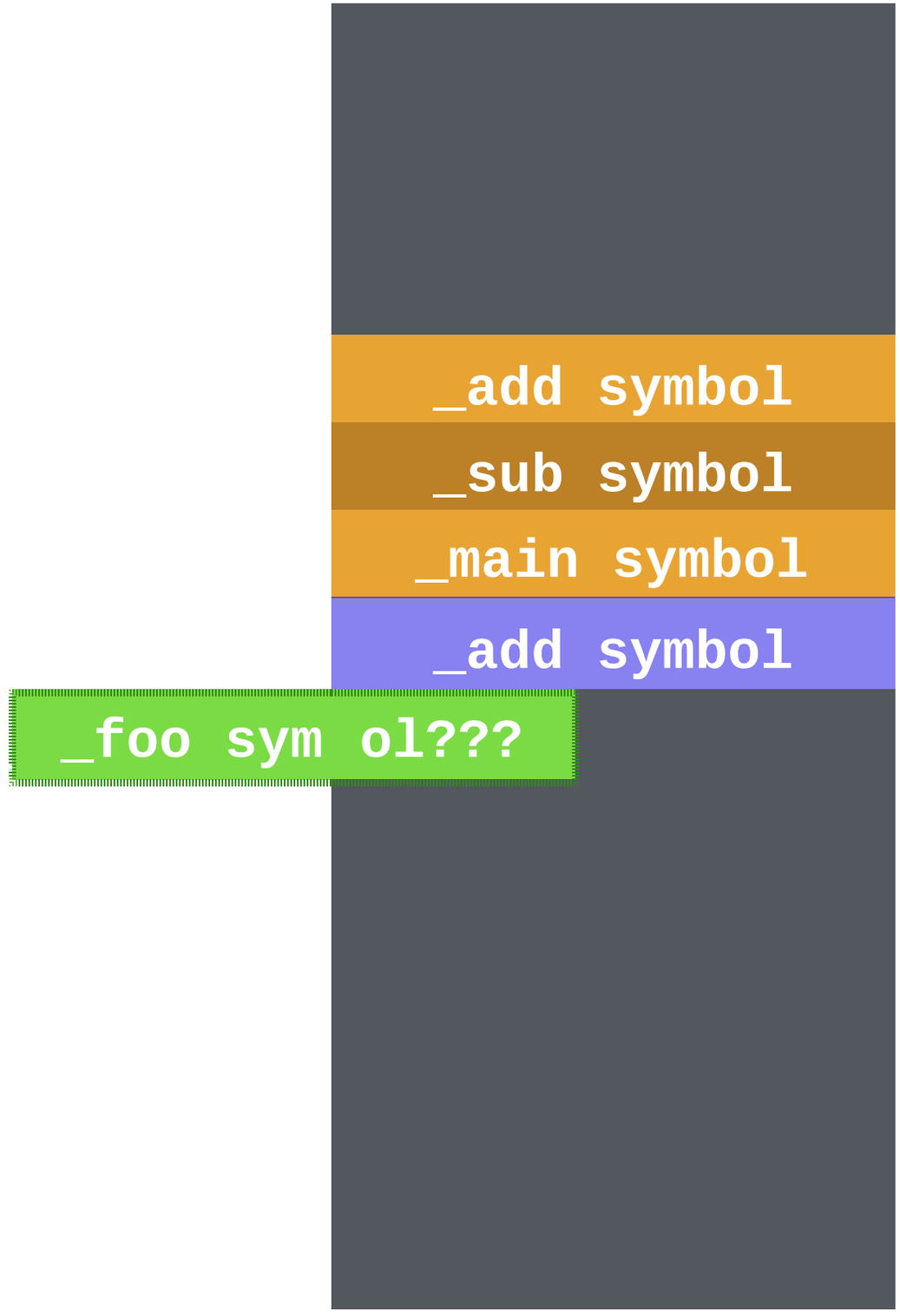

main.o
main
executable


my_math.o
callq
main.o
linker(ld)
Code for _main
main executable

duplicate symbols

Undefined symbols

_foo



A_x86_64.o

B_x86_64.o

AB_x86_64.a

A_arm64.o

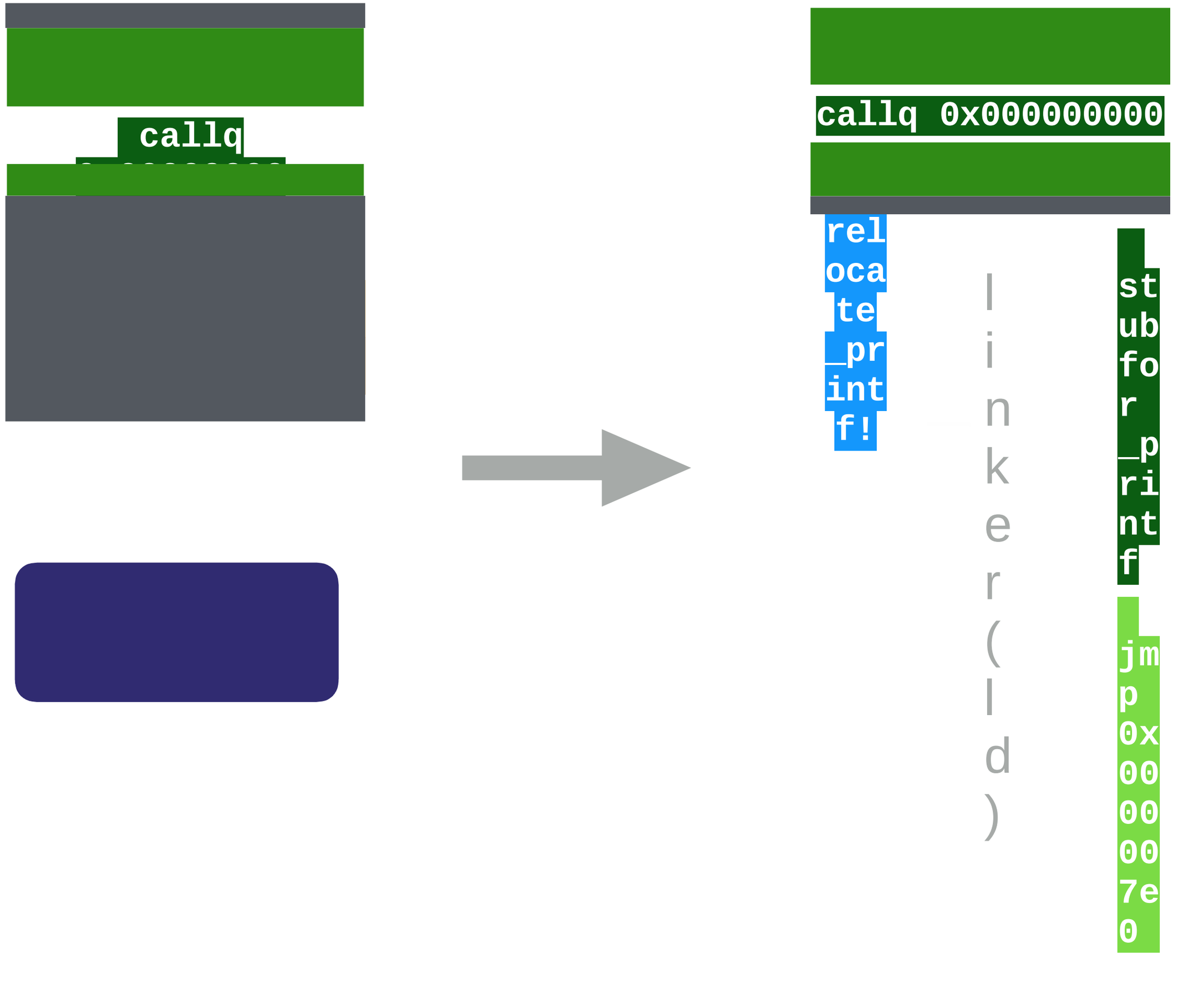
B_arm64.o

```
//    clang  -c  main.c
//    main.o

int                 "he
llo
wo
rld
"

ret
urn
0
```

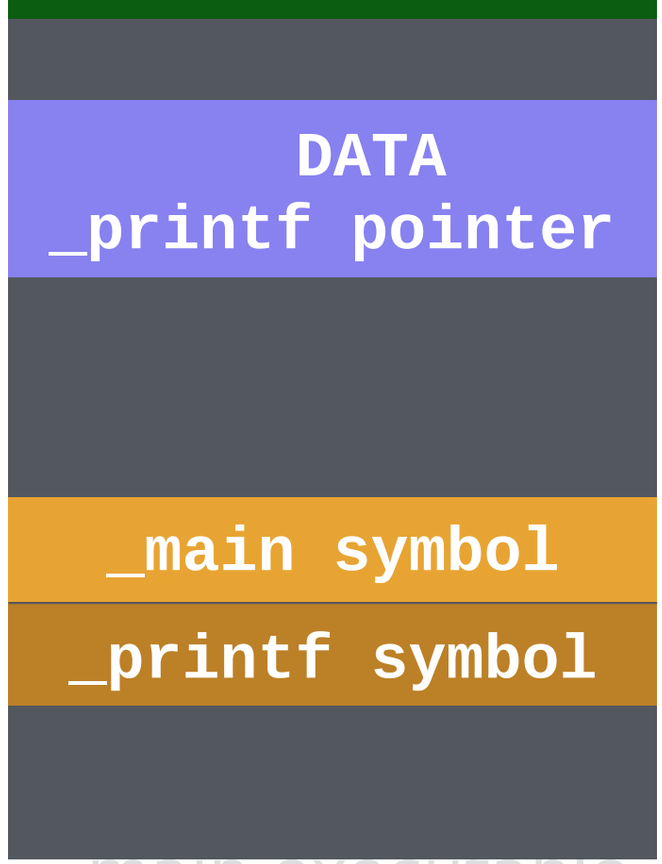
relocate _printf!

_print f symbol ???

main.o


callq
callq 0x000000000
relocate_printf!
linker(ld)
stub for _printf
jmp 0x0000007e0

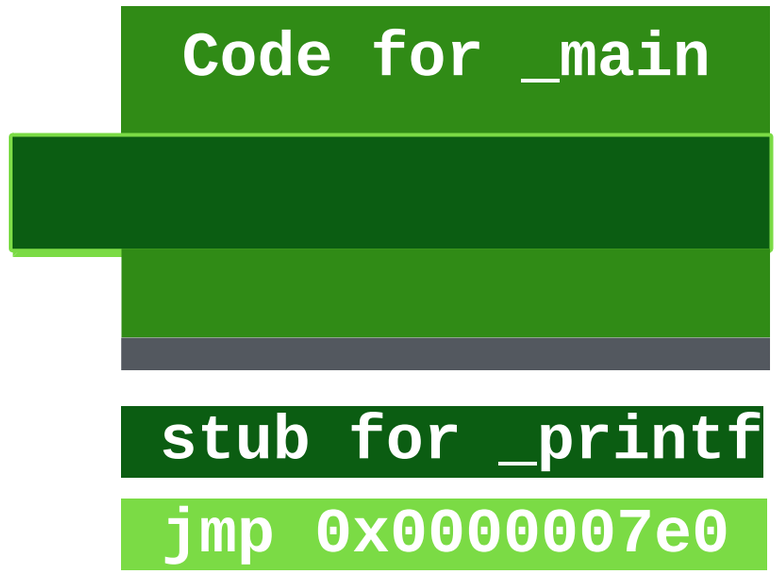
main.o

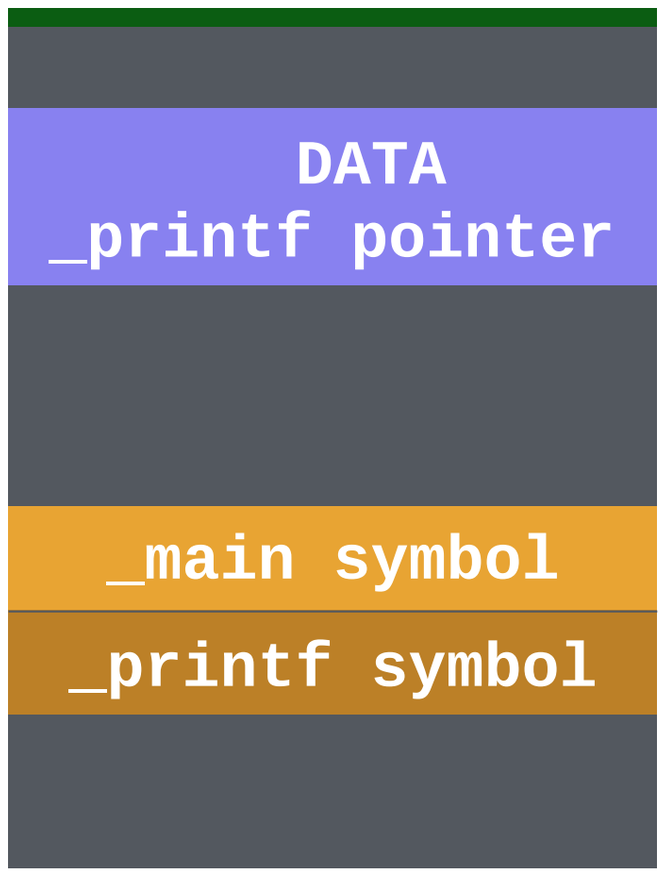


main executable


callq 0x00000000

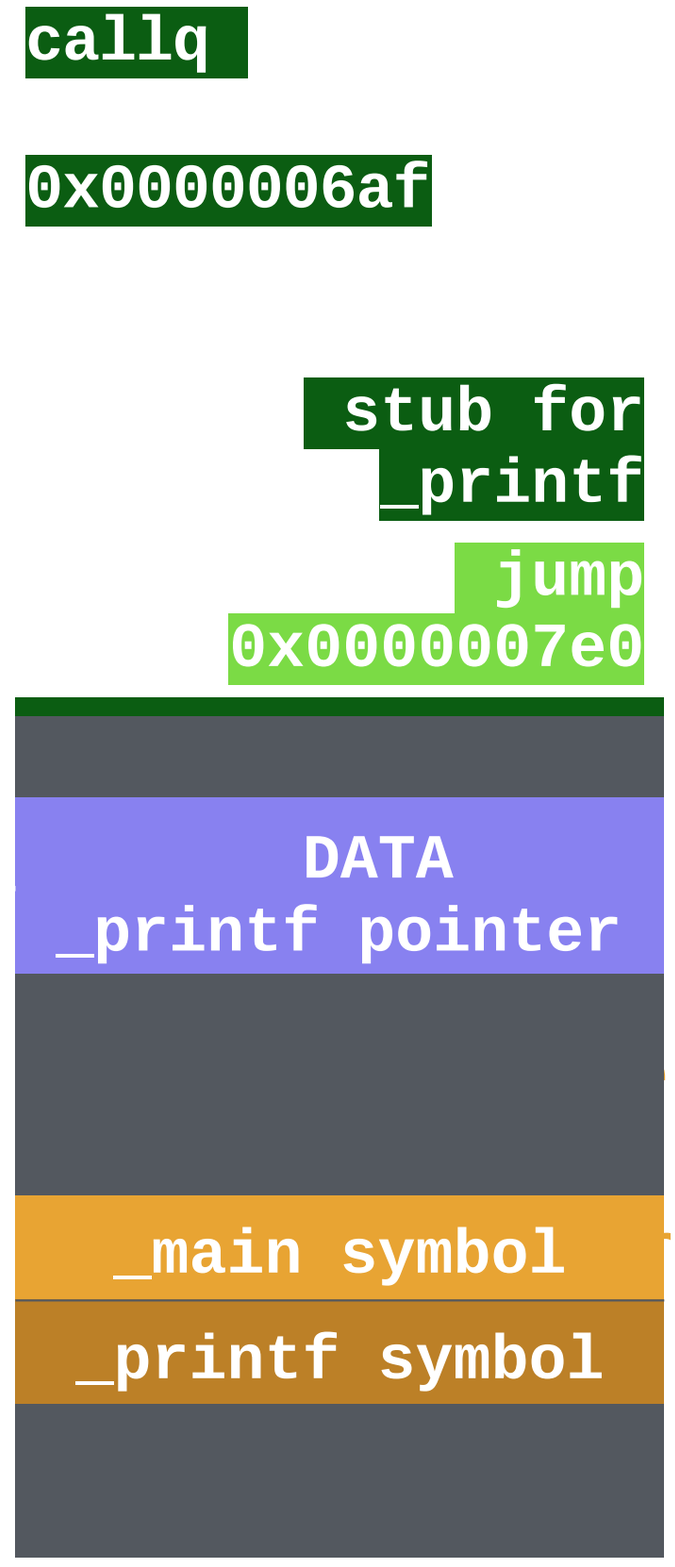
linker(ld)


Code for _main
stub for _printf
jmp 0x0000007e0


DATA
_printf pointer
_main symbol
_printf symbol

main executable

dyld


callq
0x0000006af
stub for _printf
jump 0x0000007e0
DATA
_printf pointer
_main symbol
_printf symbol

main
execut
able

Clang

ld

dyld

remove