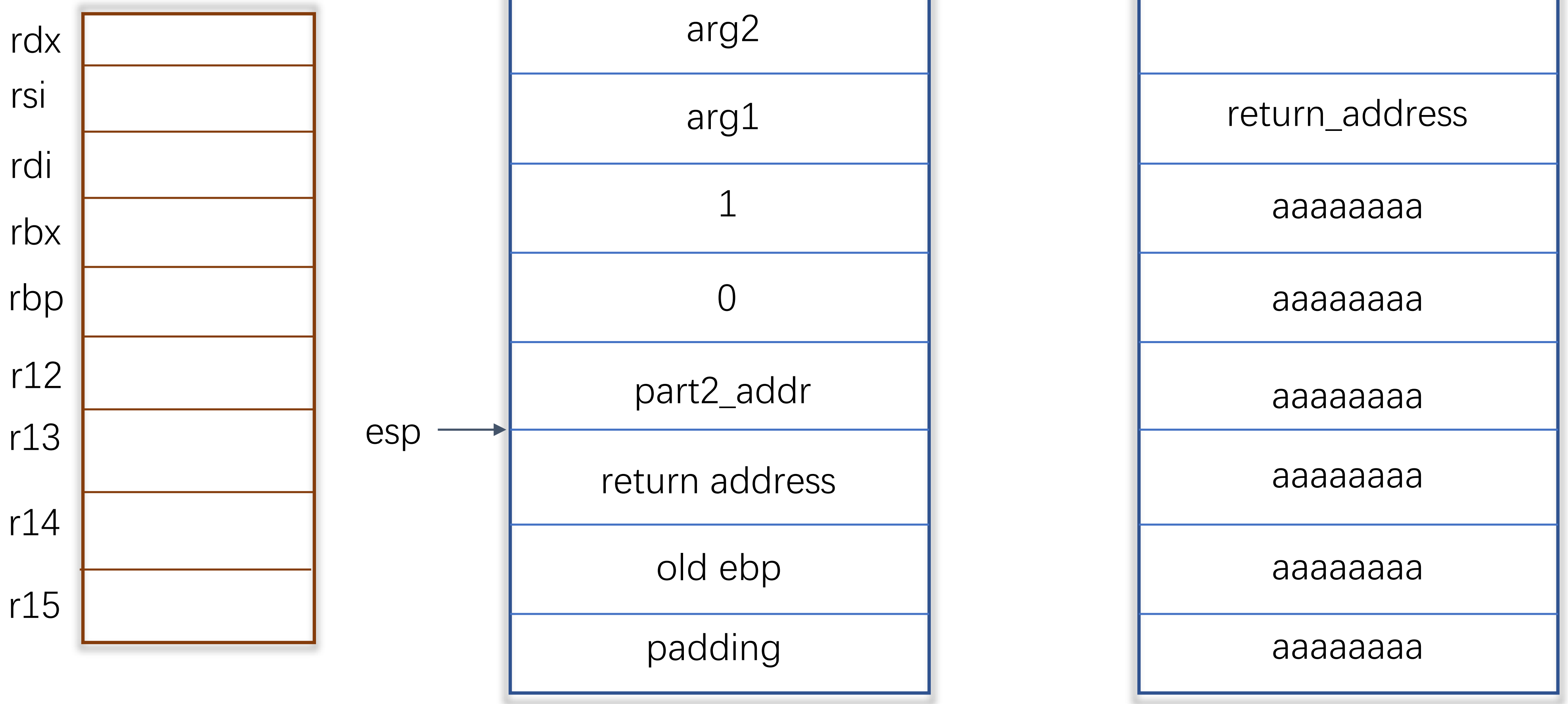
```
# part 2
  401222:    5b          pop   %rbx
  401223:    5d          pop   %rbp
  401224:    41 5c       pop   %r12
  401226:    41 5d       pop   %r13
  401228:    41 5e       pop   %r14
  40122a:    41 5f       pop   %r15
  40122c:    c3          retq
```



rdx

rsi

rdi

rbx

rbp

r12

r13

r14

r15

esp

aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

0

part2_addr

return address

old ebp

padding

return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

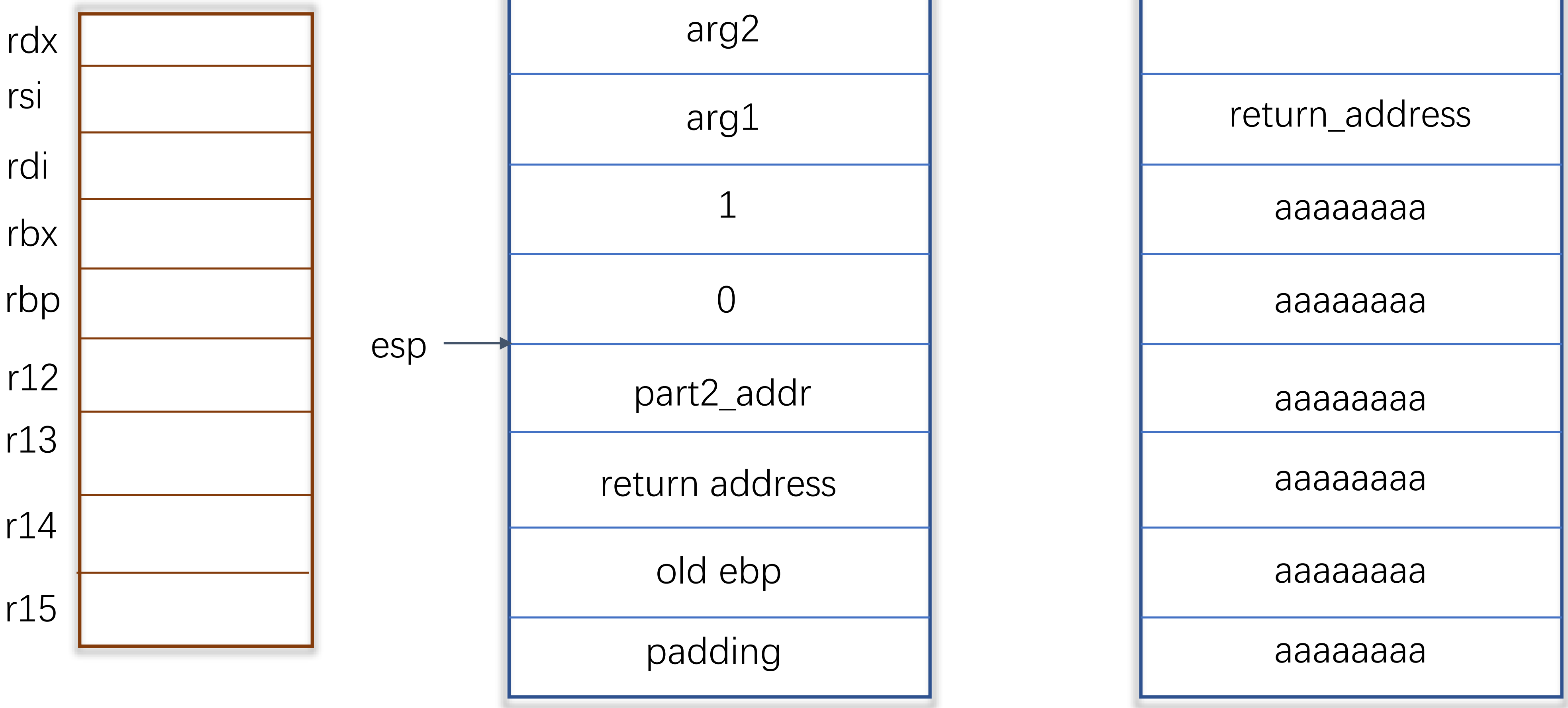
aaaaaaaa

aaaaaaaa

aaaaaaaa

# part 2

```
401222:    5b       pop   %rbx
401223:    5d       pop   %rbp
401224:    41 5c    pop   %r12
401226:    41 5d    pop   %r13
401228:    41 5e    pop   %r14
40122a:    41 5f    pop   %r15
40122c:    c3       retq
```



rdx
rsi
rdi
rbx
rbp
r12
r13
r14
r15

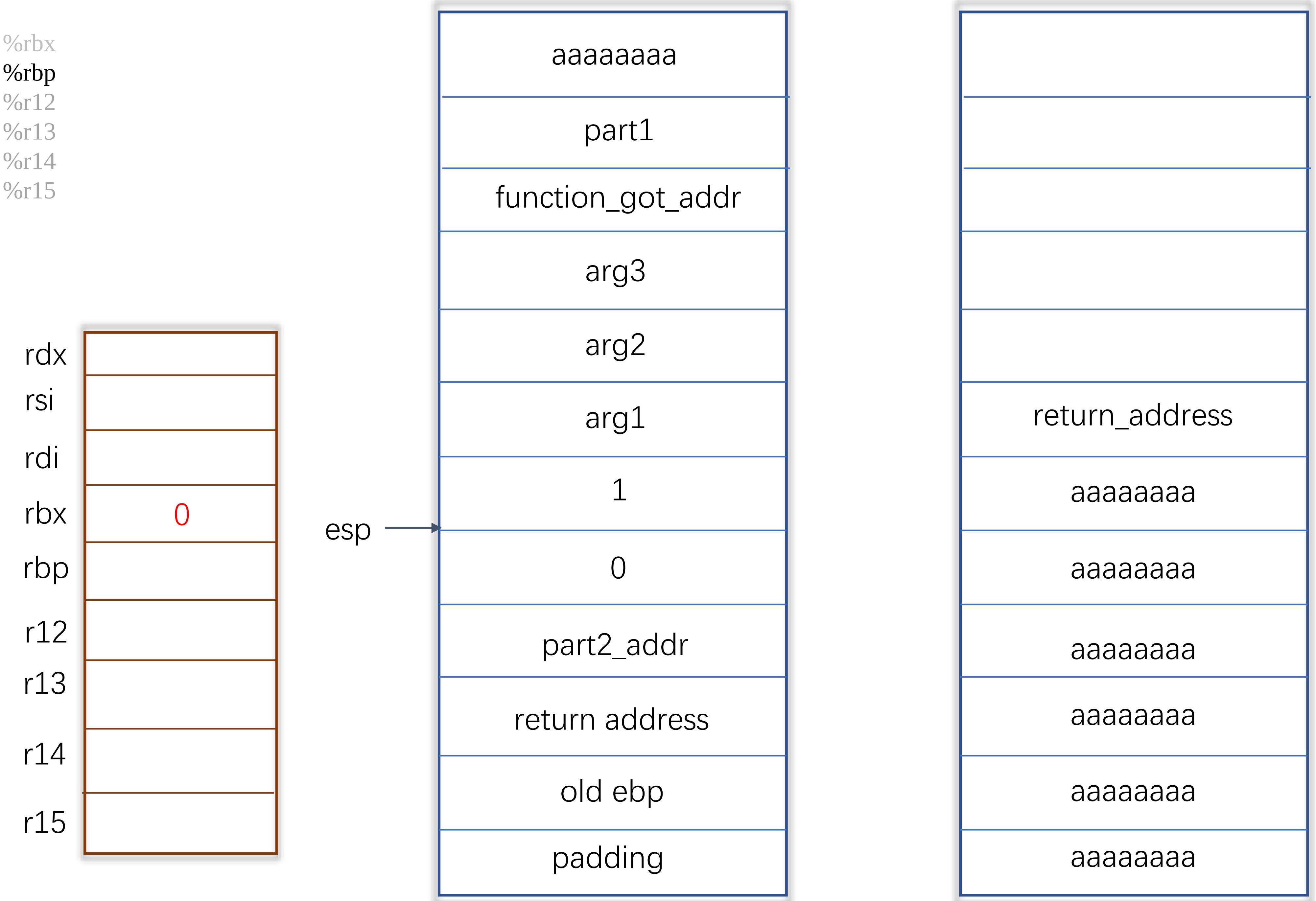
esp

aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding

return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

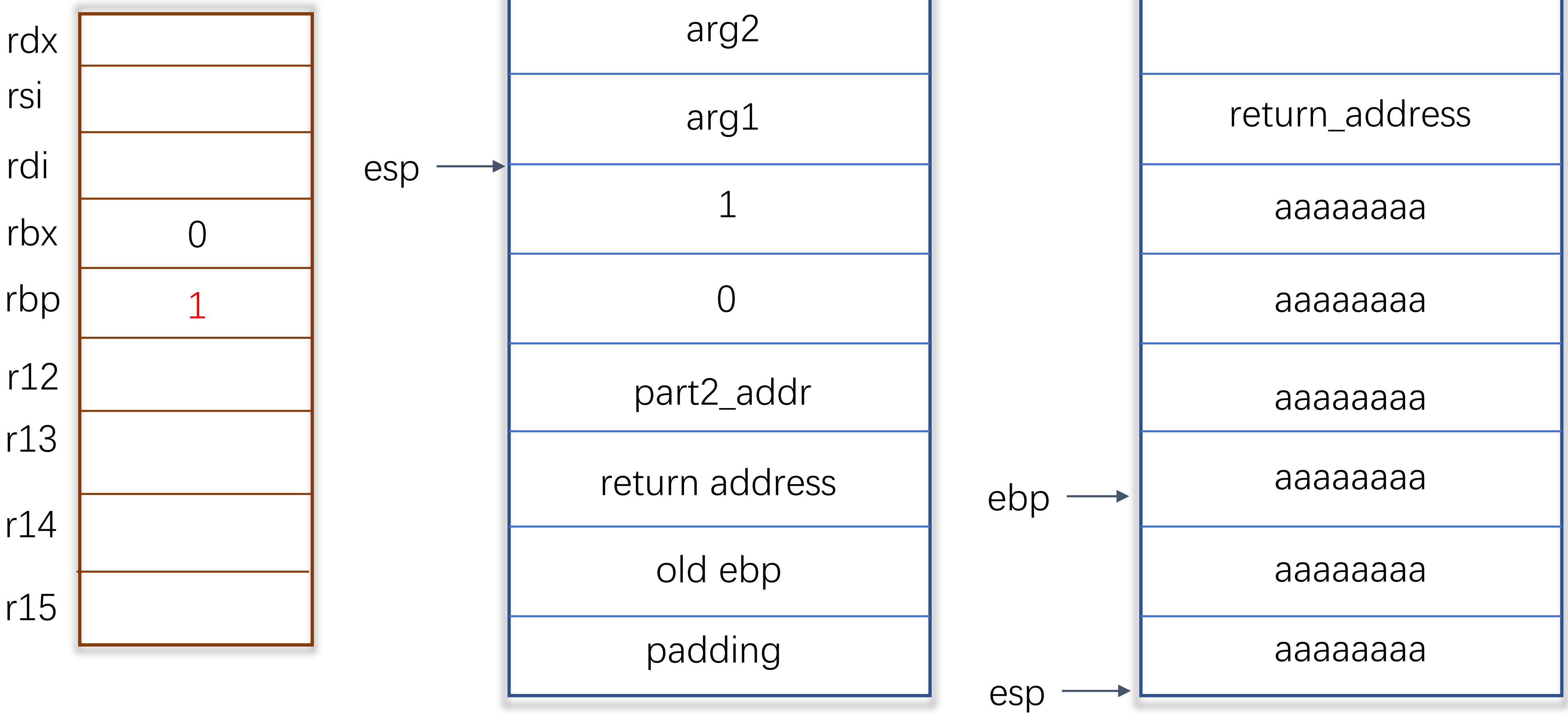
# part 2

```
401222:    5b        pop   %rbx
401223:    5d        pop   %rbp
401224:    41 5c     pop   %r12
401226:    41 5d     pop   %r13
401228:    41 5e     pop   %r14
40122a:    41 5f     pop   %r15
40122c:    c3        retq
```



# part 2

```
401222:    5b          pop    %rbx
401223:    5d          pop    %rbp
401224:    41 5c       pop    %r12
401226:    41 5d       pop    %r13
401228:    41 5e       pop    %r14
40122a:    41 5f       pop    %r15
40122c:    c3          retq
```



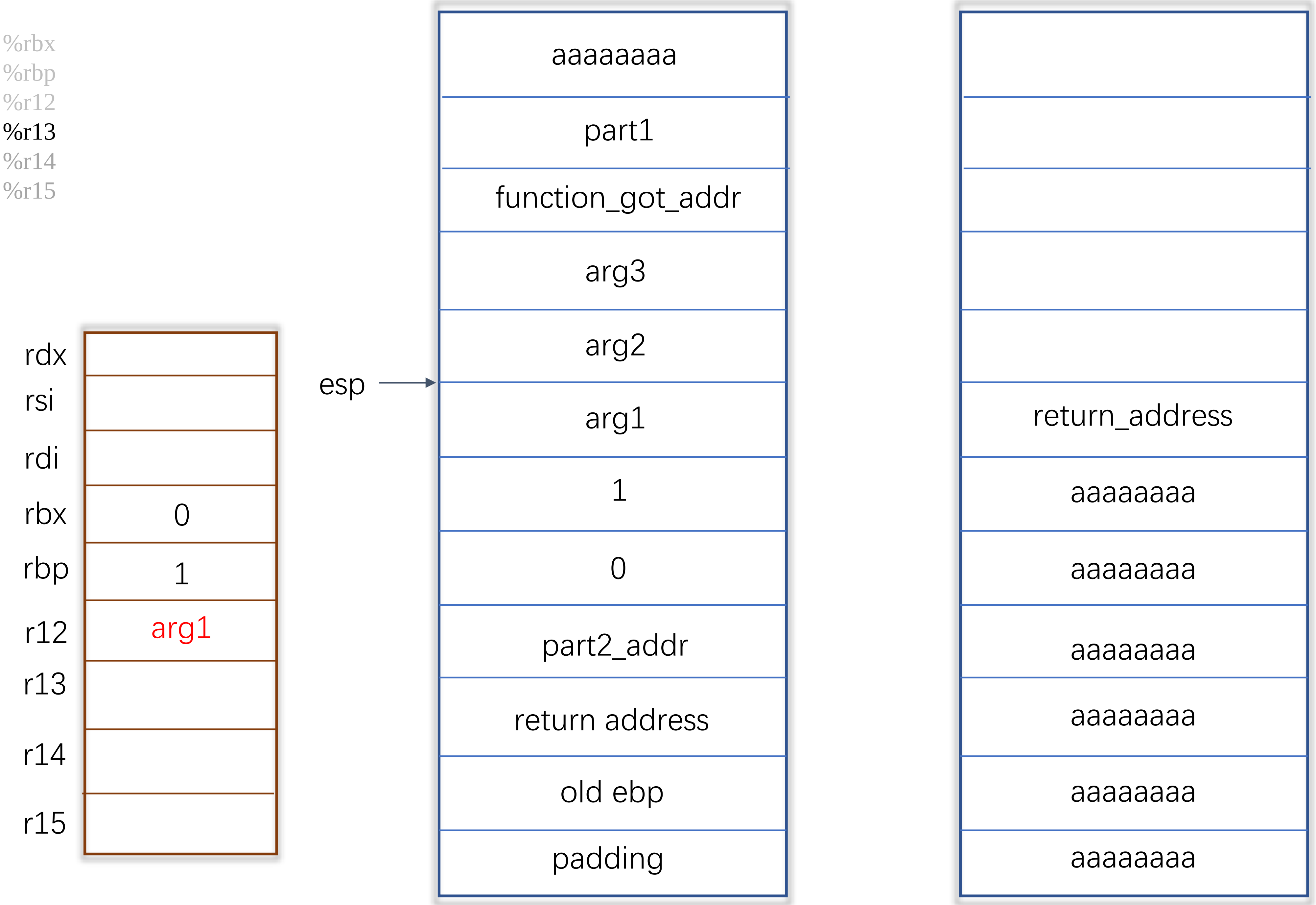
rdx	
rsi	
rdi	
rbx	0
rbp	1
r12	
r13	
r14	
r15	

aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
esp → 1
0
part2_addr
return address
old ebp
padding

return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
ebp → aaaaaaaa
aaaaaaaa
aaaaaaaa
esp →

# part 2

```
401222:   5b       pop   %rbx
401223:   5d       pop   %rbp
401224:   41 5c    pop   %r12
401226:   41 5d    pop   %r13
401228:   41 5e    pop   %r14
40122a:   41 5f    pop   %r15
40122c:   c3       retq
```

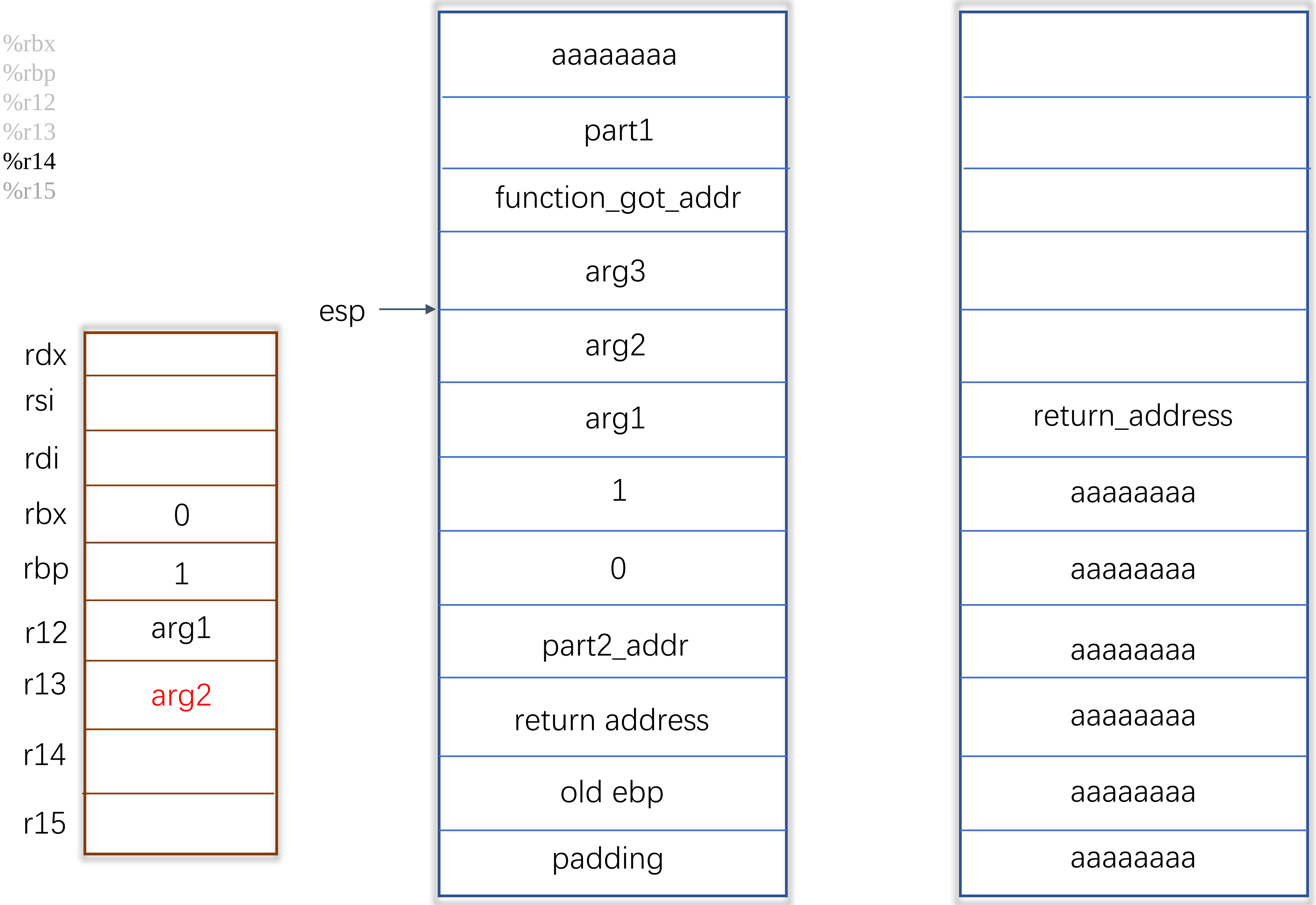


rdx	
rsi	
rdi	
rbx	0
rbp	1
r12	arg1
r13	
r14	
r15	

aaaaaaaa	
part1	
function_got_addr	
arg3	
arg2	
arg1	return_address
1	aaaaaaaa
0	aaaaaaaa
part2_addr	aaaaaaaa
return address	aaaaaaaa
old ebp	aaaaaaaa
padding	aaaaaaaa

# part 2

```
401222:   5b      pop   %rbx
401223:   5d      pop   %rbp
401224:   41 5c   pop   %r12
401226:   41 5d   pop   %r13
401228:   41 5e   pop   %r14
40122a:   41 5f   pop   %r15
40122c:   c3      retq
```



rdx	
rsi	
rdi	
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	
r15	

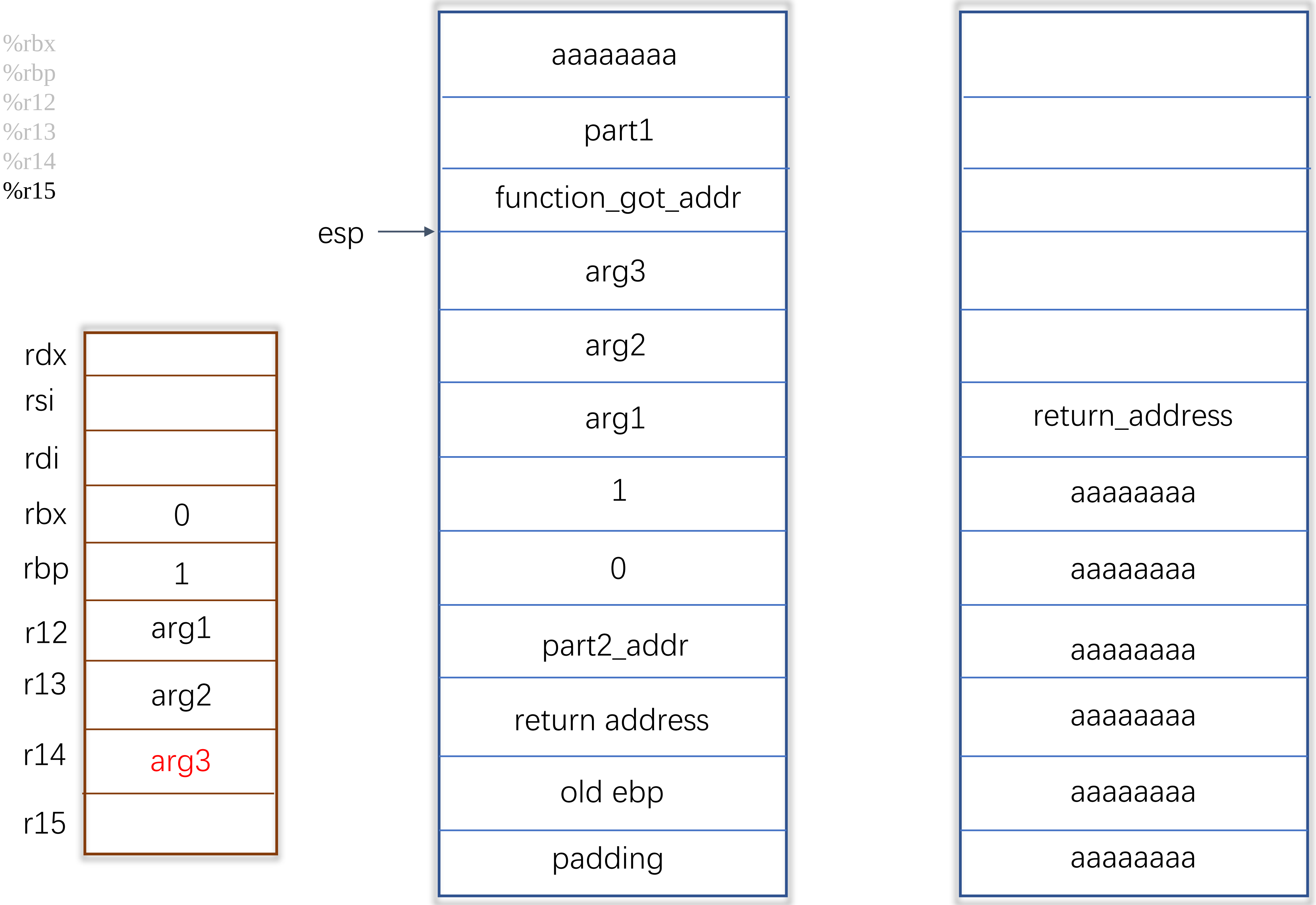
esp

aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding

return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

# part 2

```
401222:     5b          pop   %rbx
401223:     5d          pop   %rbp
401224:     41 5c       pop   %r12
401226:     41 5d       pop   %r13
401228:     41 5e       pop   %r14
40122a:     41 5f       pop   %r15
40122c:     c3          retq
```



esp

rdx	
rsi	
rdi	
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	

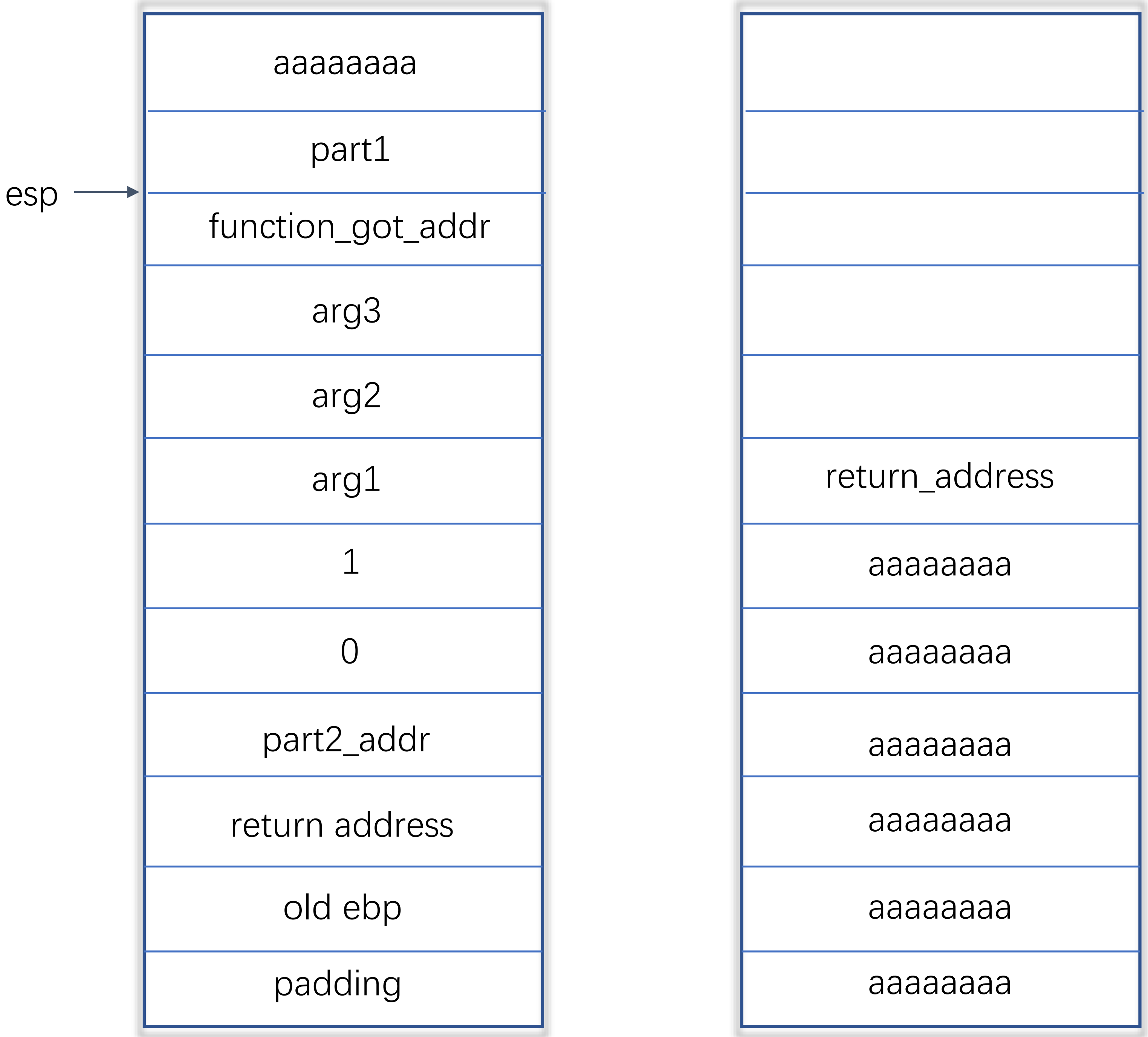
aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding

return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

# part 2

```
401222:   5b       pop   %rbx
401223:   5d       pop   %rbp
401224:   41 5c    pop   %r12
401226:   41 5d    pop   %r13
401228:   41 5e    pop   %r14
40122a:   41 5f    pop   %r15
40122c:   c3       retq
```

rdx	
rsi	
rdi	
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



esp →

aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

0

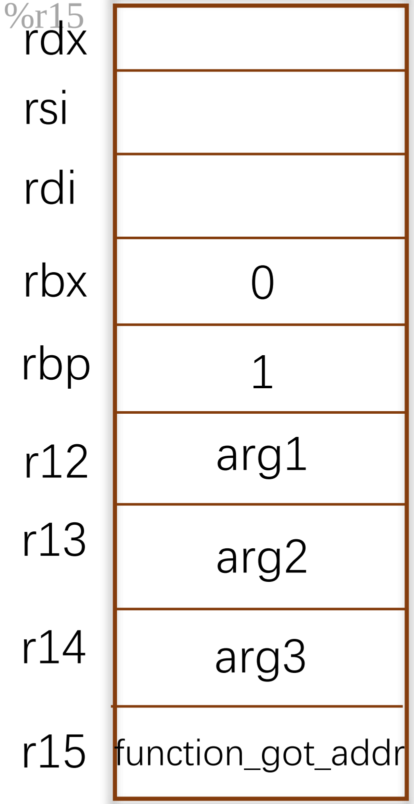
part2_addr

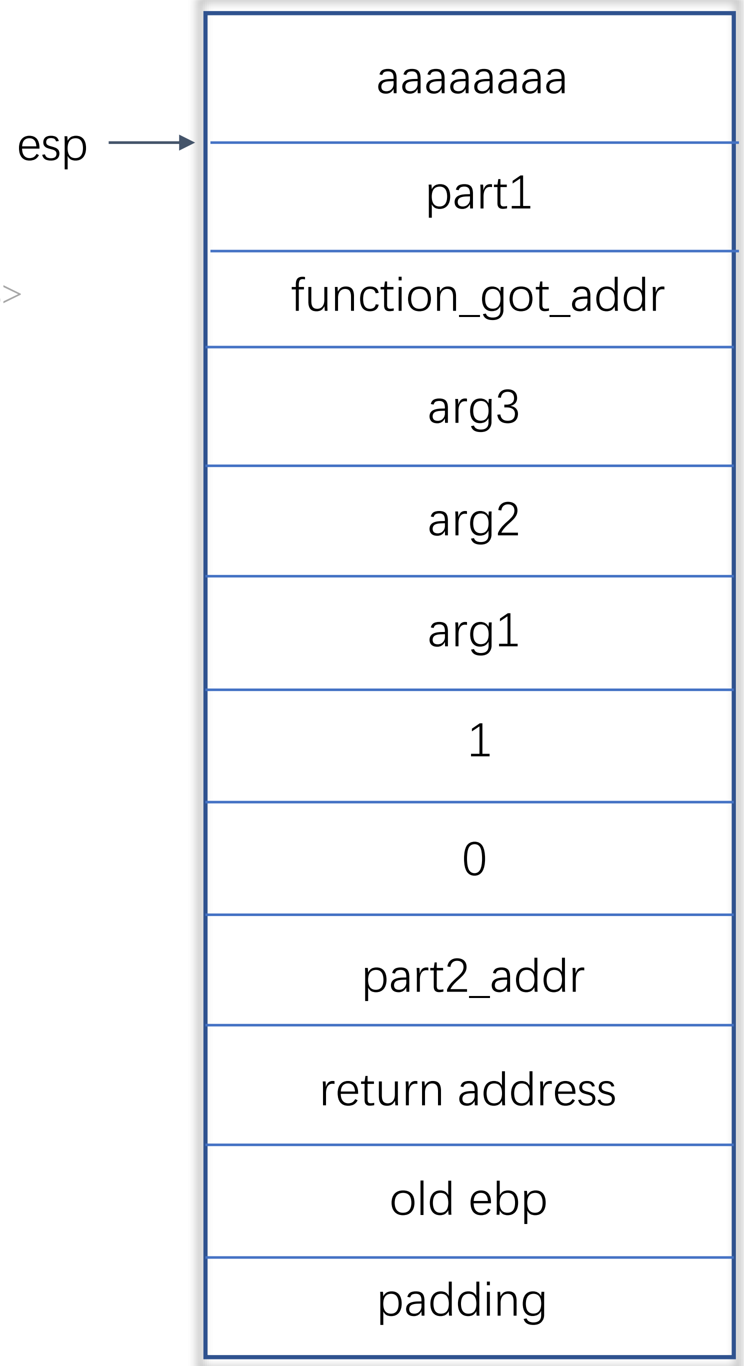
return address

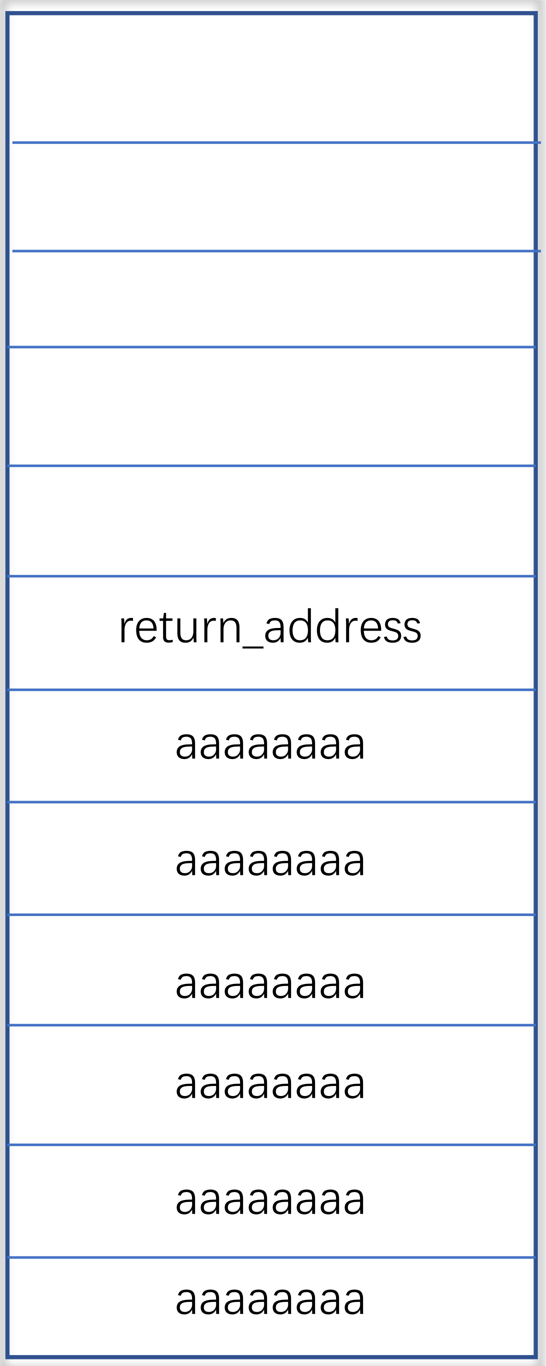
old ebp

padding

```
# part 1
401208:    4c 89 f2       mov    %r14,%rdx
40120b:    4c 89 ee       mov    %r13,%rsi
40120e:    44 89 e7       mov    %r12d,%edi
401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
401215:    48 83 c3 01    add    $0x1,%rbx
401219:    48 39 dd       cmp    %rbx,%rbp
40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08    add    $0x8,%rsp
401222:    5b             pop    %rbx
401223:    5d             pop    %rbp
401224:    41 5c          pop    %r12
401226:    41 5d          pop    %r13
401228:    41 5e          pop    %r14
40122a:    41 5f          pop    %r15
40122c:    c3             retq
```

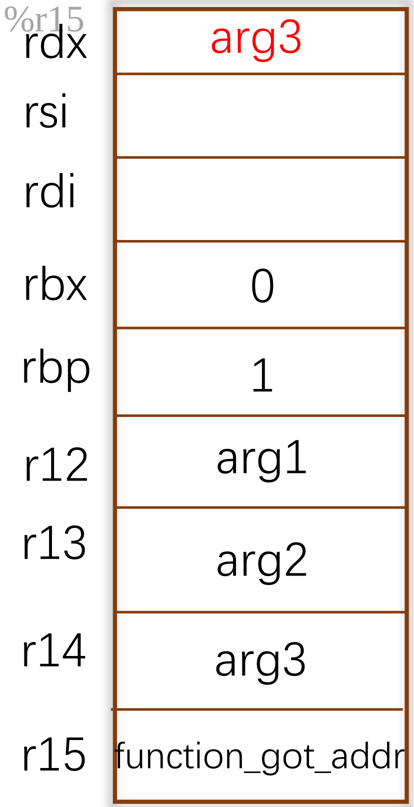




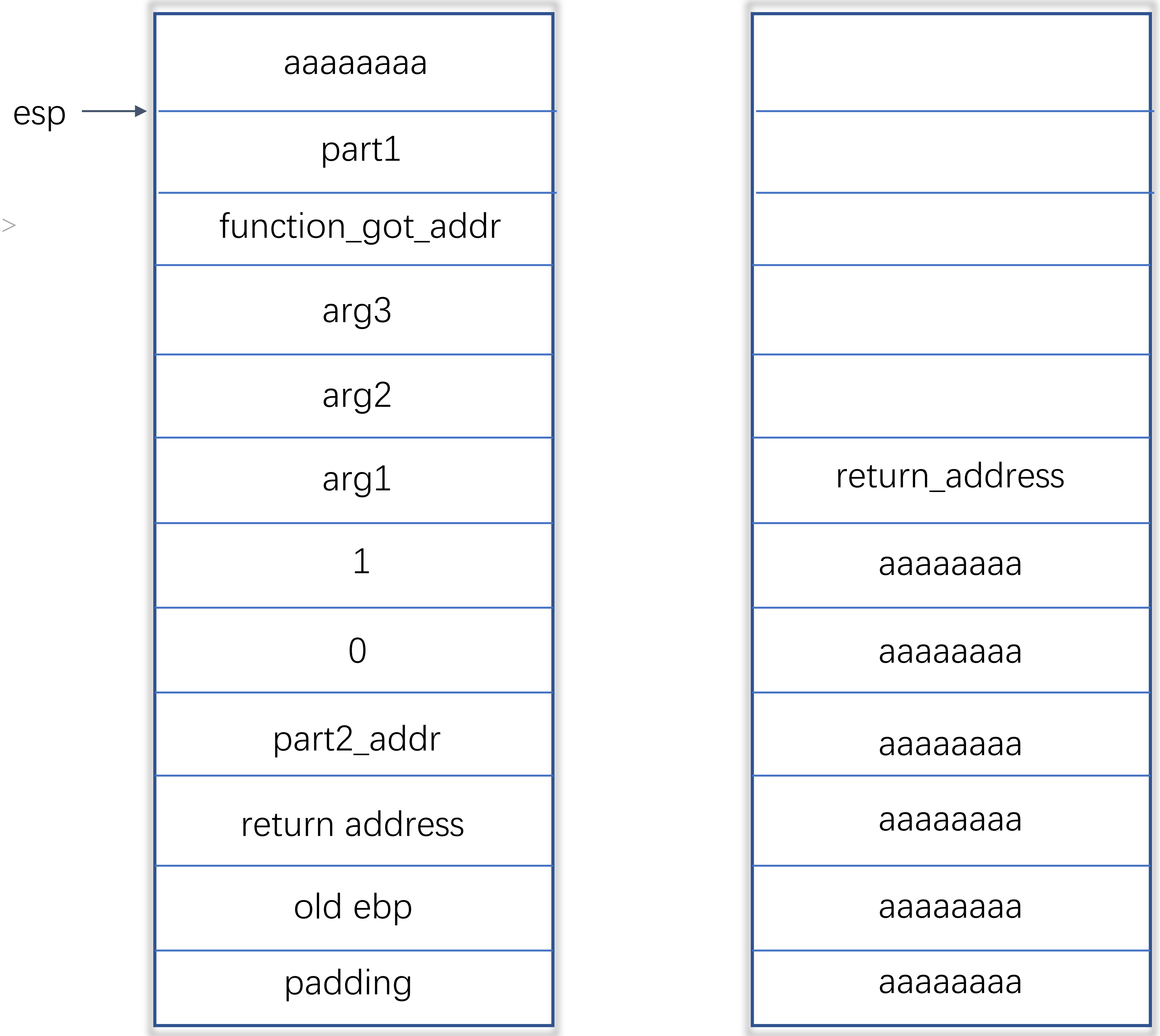


# part 1

```
401208:   4c 89 f2      mov    %r14,%rdx
40120b:   4c 89 ee      mov    %r13,%rsi
40120e:   44 89 e7      mov    %r12d,%edi
401211:   41 ff 14 df   callq  *(%r15,%rbx,8)
401215:   48 83 c3 01   add    $0x1,%rbx
401219:   48 39 dd      cmp    %rbx,%rbp
40121c:   75 ea         jne    401208 <__libc_csu_init+0x38>
40121e:   48 83 c4 08   add    $0x8,%rsp
401222:   5b            pop    %rbx
401223:   5d            pop    %rbp
401224:   41 5c         pop    %r12
401226:   41 5d         pop    %r13
401228:   41 5e         pop    %r14
40122a:   41 5f         pop    %r15
40122c:   c3            retq
```



rdx	arg3
rsi	
rdi	
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr

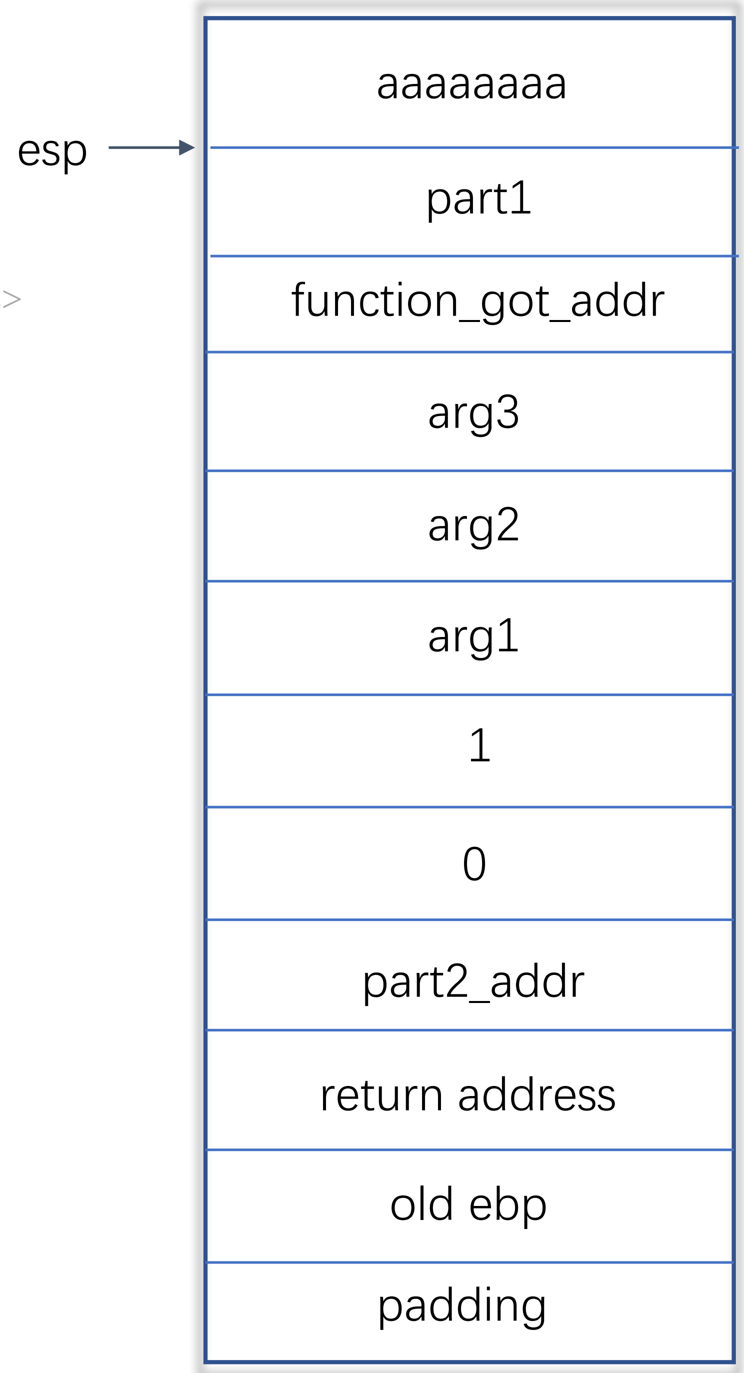


aaaaaaaa	
part1	
function_got_addr	
arg3	
arg2	
arg1	return_address
1	aaaaaaaa
0	aaaaaaaa
part2_addr	aaaaaaaa
return address	aaaaaaaa
old ebp	aaaaaaaa
padding	aaaaaaaa

# part 1

```
401208:    4c 89 f2       mov    %r14,%rdx
40120b:    4c 89 ee       mov    %r13,%rsi
40120e:    44 89 e7       mov    %r12d,%edi
401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
401215:    48 83 c3 01    add    $0x1,%rbx
401219:    48 39 dd       cmp    %rbx,%rbp
40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08    add    $0x8,%rsp
401222:    5b             pop    %rbx
401223:    5d             pop    %rbp
401224:    41 5c          pop    %r12
401226:    41 5d          pop    %r13
401228:    41 5e          pop    %r14
40122a:    41 5f          pop    %r15
40122c:    c3             retq
```

rdx	arg3
rsi	arg2
rdi	
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



esp

aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

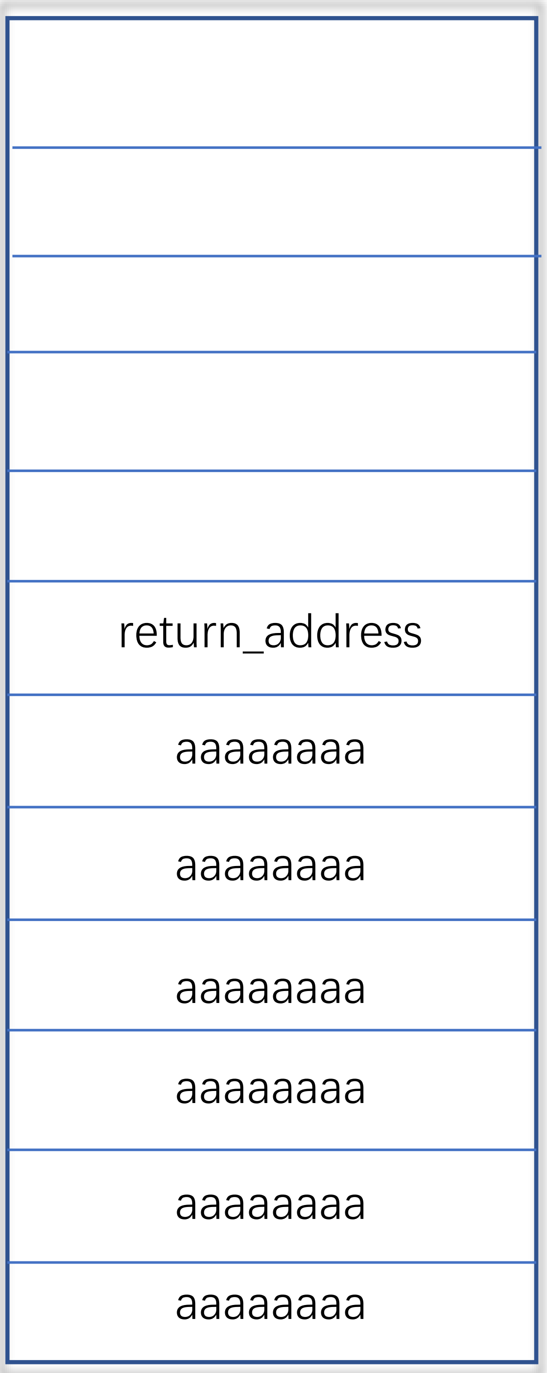
0

part2_addr

return address

old ebp

padding



return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

aaaaaaaa

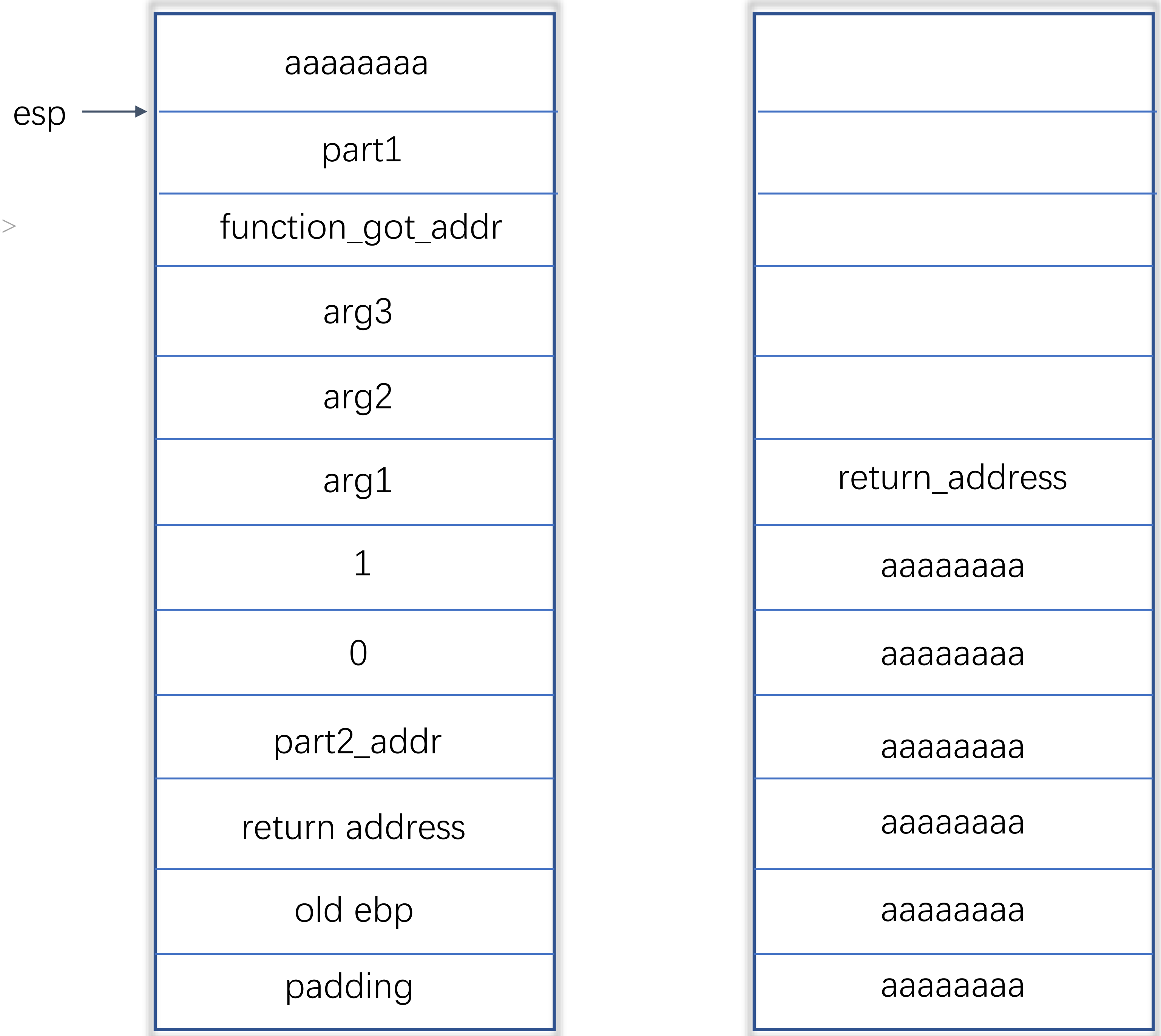
aaaaaaaa

aaaaaaaa

# part 1

```
401208:    4c 89 f2      mov    %r14,%rdx
40120b:    4c 89 ee      mov    %r13,%rsi
40120e:    44 89 e7      mov    %r12d,%edi
401211:    41 ff 14 df   callq  *(%r15,%rbx,8)
401215:    48 83 c3 01   add    $0x1,%rbx
401219:    48 39 dd      cmp    %rbx,%rbp
40121c:    75 ea         jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08   add    $0x8,%rsp
401222:    5b            pop    %rbx
401223:    5d            pop    %rbp
401224:    41 5c         pop    %r12
401226:    41 5d         pop    %r13
401228:    41 5e         pop    %r14
40122a:    41 5f         pop    %r15
40122c:    c3            retq
```

rdx	arg3
rsi	arg2
rdi	arg1
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



esp

aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

0

part2_addr

return address

old ebp

padding

return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

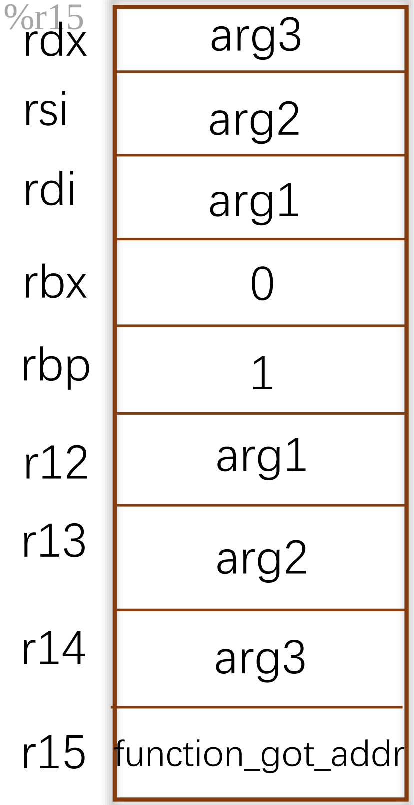
aaaaaaaa

aaaaaaaa

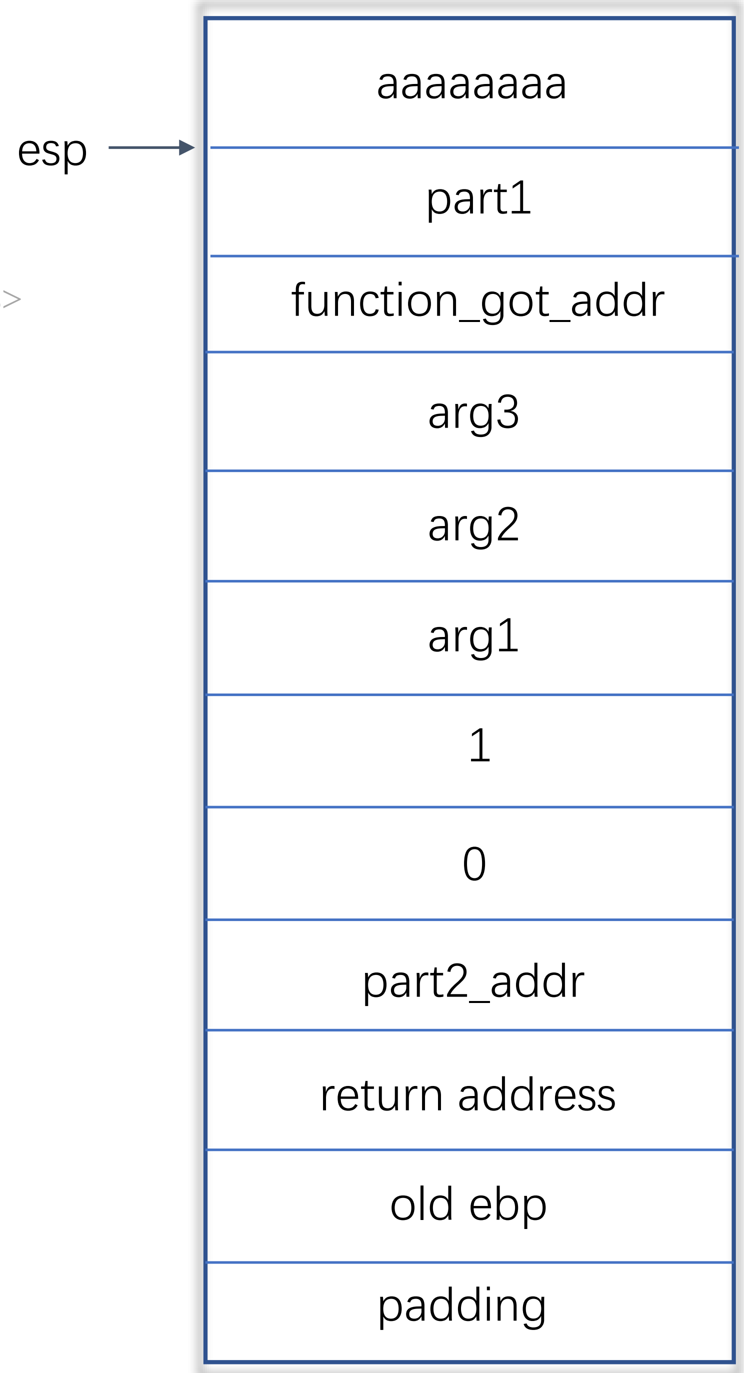
aaaaaaaa

# part 1

```
401208:  4c 89 f2     mov   %r14,%rdx
40120b:  4c 89 ee     mov   %r13,%rsi
40120e:  44 89 e7     mov   %r12d,%edi
401211:  41 ff 14 df  callq *(%r15,%rbx,8)
401215:  48 83 c3 01  add   $0x1,%rbx
401219:  48 39 dd     cmp   %rbx,%rbp
40121c:  75 ea        jne   401208 <__libc_csu_init+0x38>
40121e:  48 83 c4 08  add   $0x8,%rsp
401222:  5b           pop   %rbx
401223:  5d           pop   %rbp
401224:  41 5c        pop   %r12
401226:  41 5d        pop   %r13
401228:  41 5e        pop   %r14
40122a:  41 5f        pop   %r15
40122c:  c3           retq
```



rdx	arg3
rsi	arg2
rdi	arg1
rbx	0
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



esp

aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

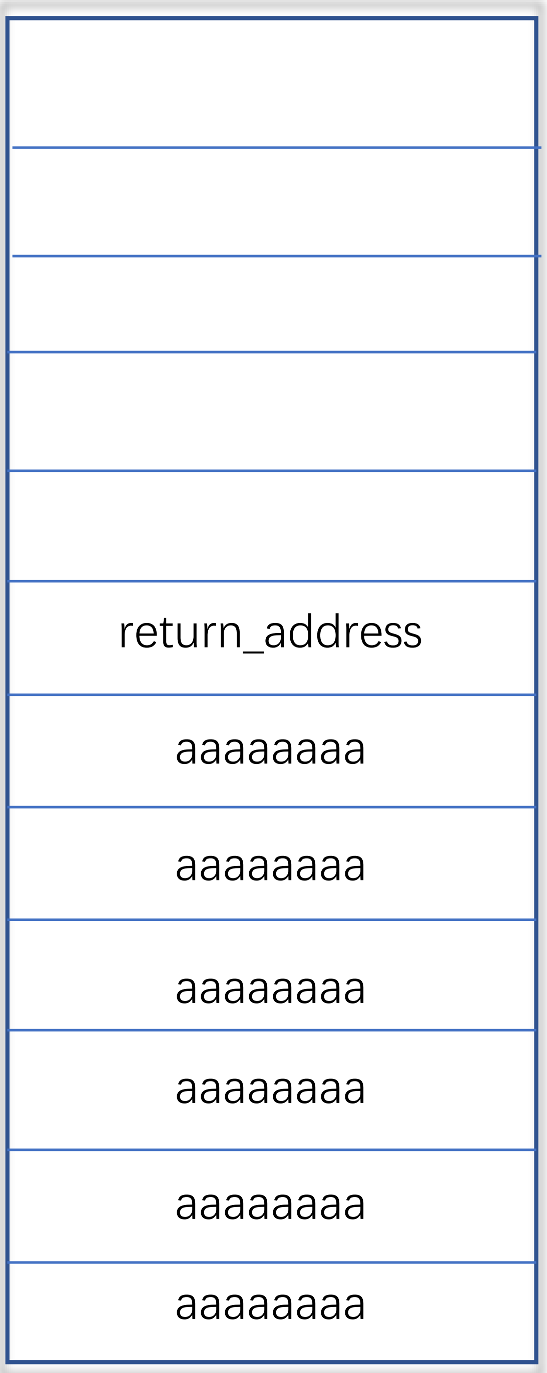
0

part2_addr

return address

old ebp

padding



return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

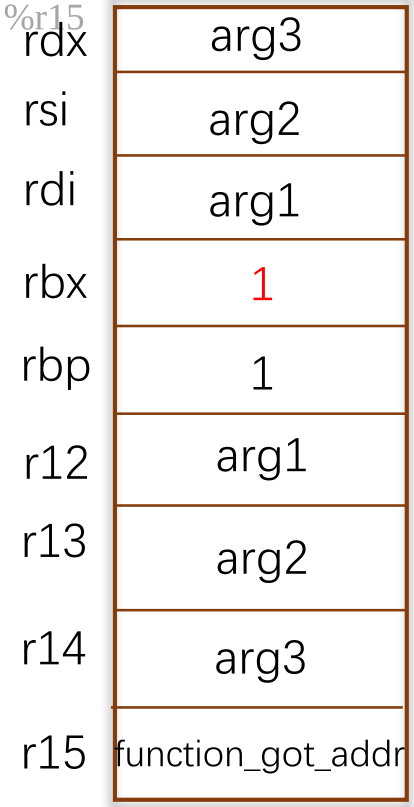
aaaaaaaa

aaaaaaaa

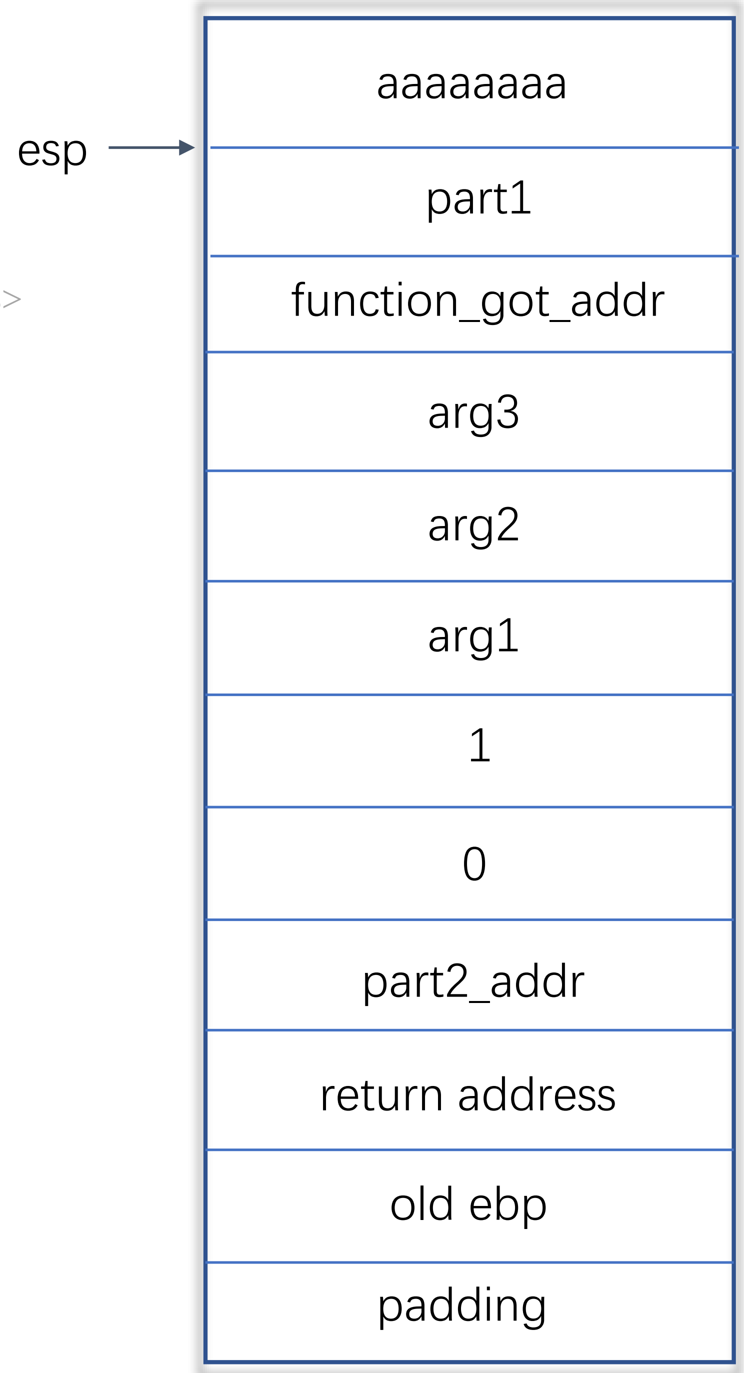
aaaaaaaa

# part 1

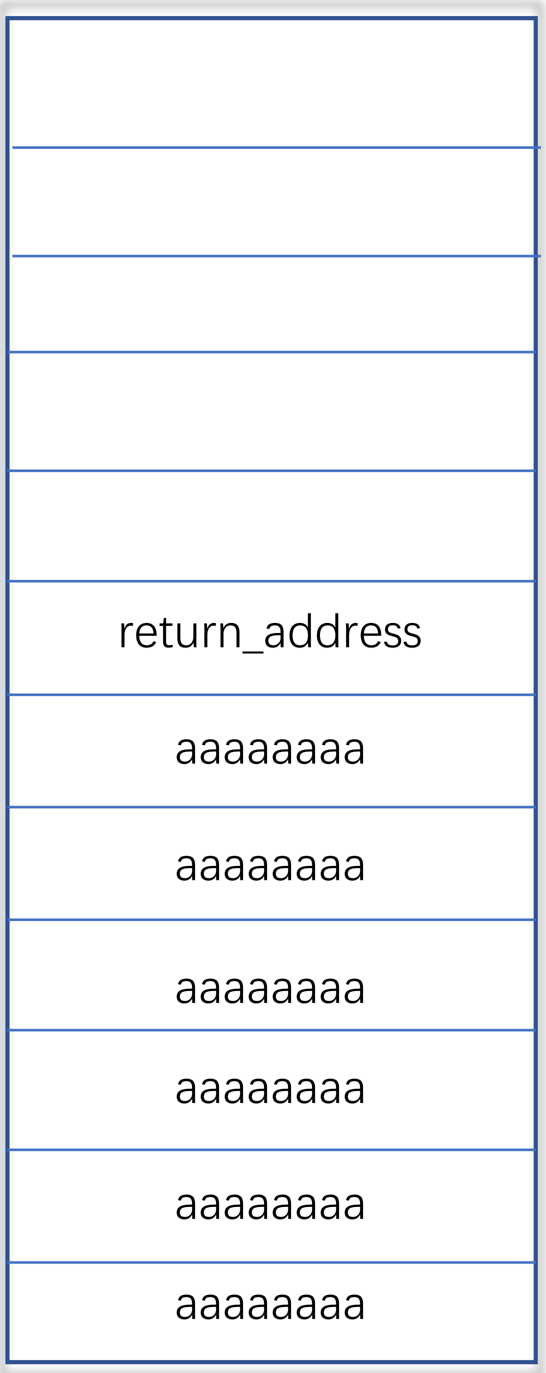
```
401208:    4c 89 f2      mov    %r14,%rdx
40120b:    4c 89 ee      mov    %r13,%rsi
40120e:    44 89 e7      mov    %r12d,%edi
401211:    41 ff 14 df   callq  *(%r15,%rbx,8)
401215:    48 83 c3 01   add    $0x1,%rbx
401219:    48 39 dd      cmp    %rbx,%rbp
40121c:    75 ea         jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08   add    $0x8,%rsp
401222:    5b            pop    %rbx
401223:    5d            pop    %rbp
401224:    41 5c         pop    %r12
401226:    41 5d         pop    %r13
401228:    41 5e         pop    %r14
40122a:    41 5f         pop    %r15
40122c:    c3            retq
```



rdx arg3
rsi arg2
rdi arg1
rbx 1
rbp 1
r12 arg1
r13 arg2
r14 arg3
r15 function_got_addr



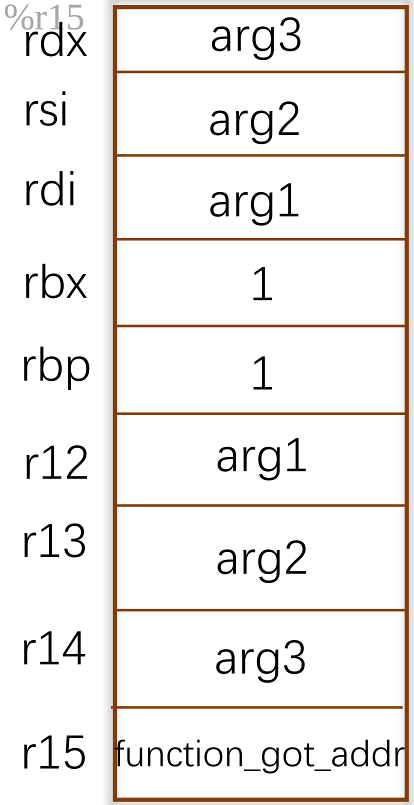
aaaaaaaa
esp → part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding



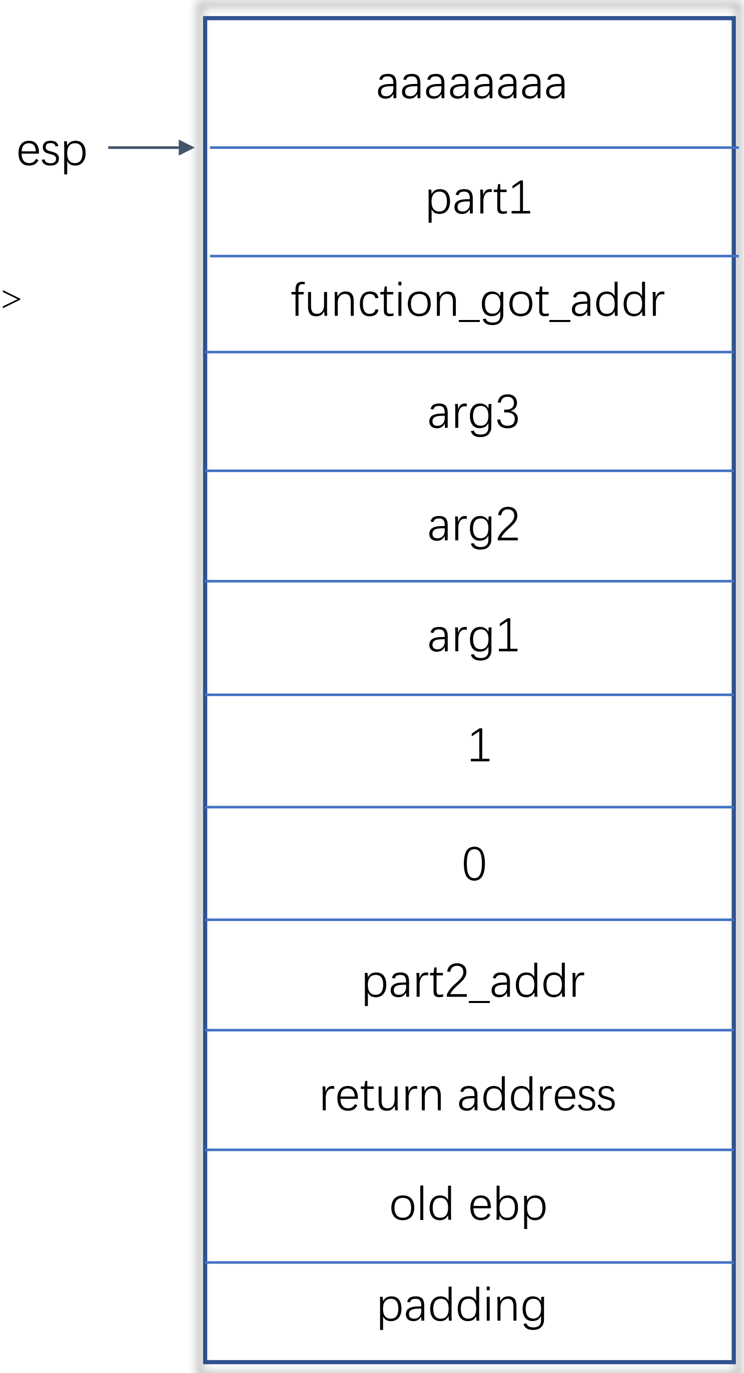
return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

# part 1

```
401208:   4c 89 f2      mov   %r14,%rdx
40120b:   4c 89 ee      mov   %r13,%rsi
40120e:   44 89 e7      mov   %r12d,%edi
401211:   41 ff 14 df   callq *(%r15,%rbx,8)
401215:   48 83 c3 01   add   $0x1,%rbx
401219:   48 39 dd      cmp   %rbx,%rbp
40121c:   75 ea         jne   401208 <__libc_csu_init+0x38>
40121e:   48 83 c4 08   add   $0x8,%rsp
401222:   5b            pop   %rbx
401223:   5d            pop   %rbp
401224:   41 5c         pop   %r12
401226:   41 5d         pop   %r13
401228:   41 5e         pop   %r14
40122a:   41 5f         pop   %r15
40122c:   c3            retq
```

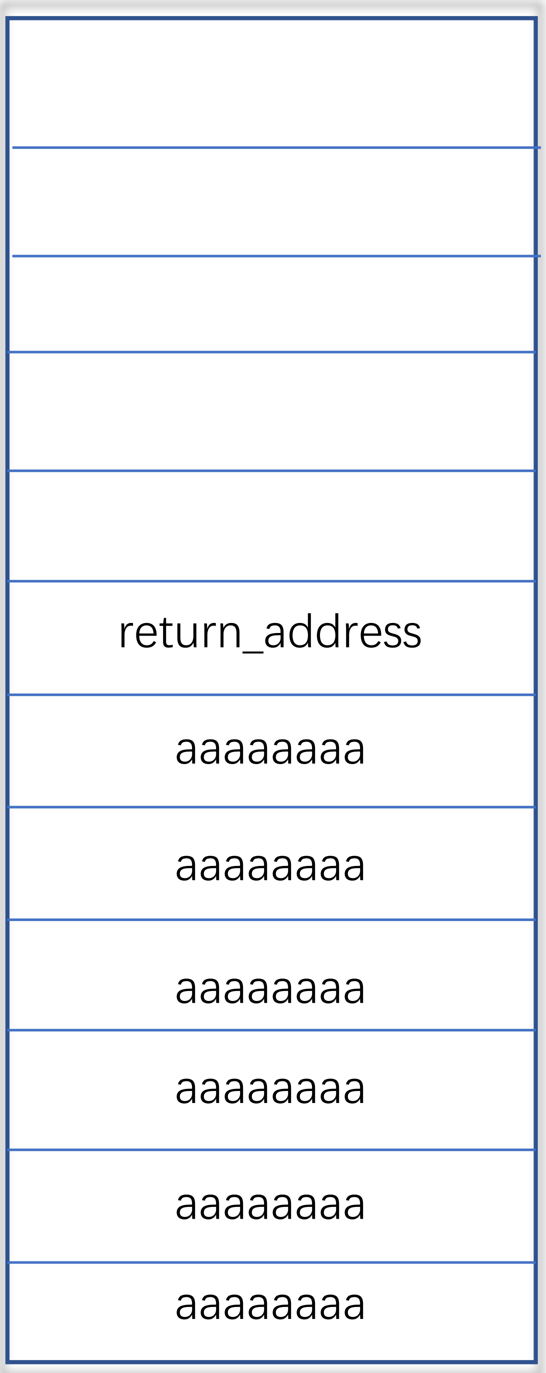


rdx arg3
rsi arg2
rdi arg1
rbx 1
rbp 1
r12 arg1
r13 arg2
r14 arg3
r15 function_got_addr



esp

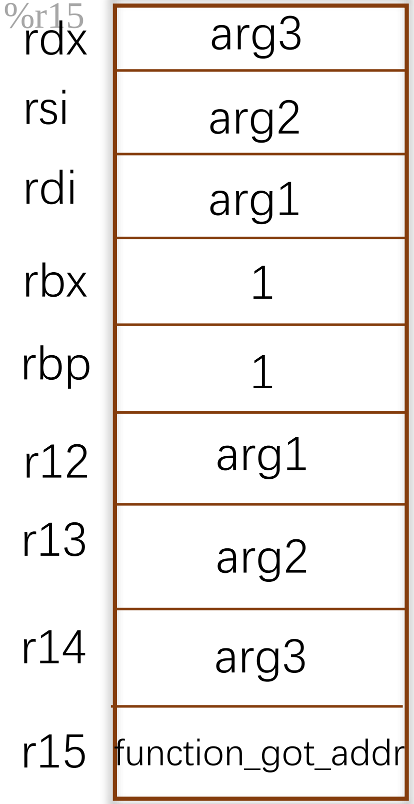
aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding



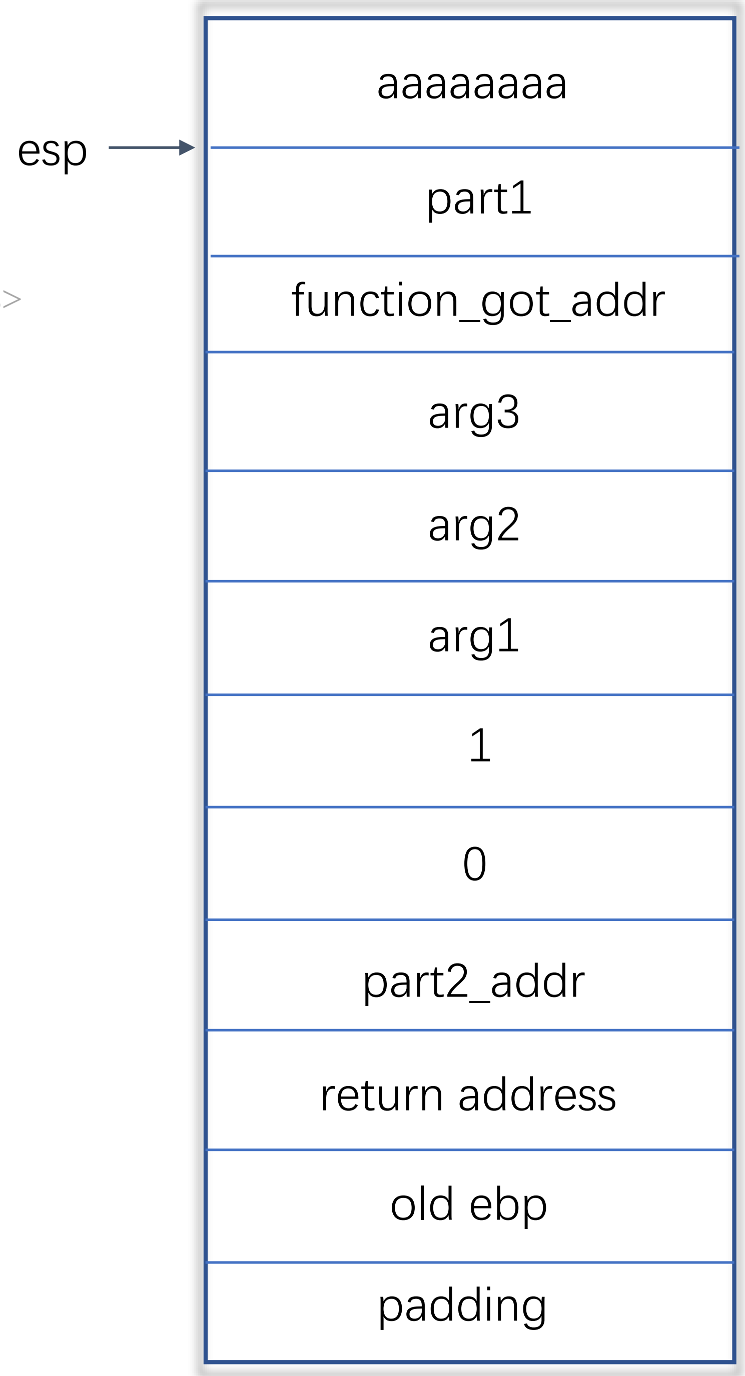
return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

# part 1

```
401208:    4c 89 f2       mov    %r14,%rdx
40120b:    4c 89 ee       mov    %r13,%rsi
40120e:    44 89 e7       mov    %r12d,%edi
401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
401215:    48 83 c3 01    add    $0x1,%rbx
401219:    48 39 dd       cmp    %rbx,%rbp
40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08    add    $0x8,%rsp
401222:    5b             pop    %rbx
401223:    5d             pop    %rbp
401224:    41 5c          pop    %r12
401226:    41 5d          pop    %r13
401228:    41 5e          pop    %r14
40122a:    41 5f          pop    %r15
40122c:    c3             retq
```

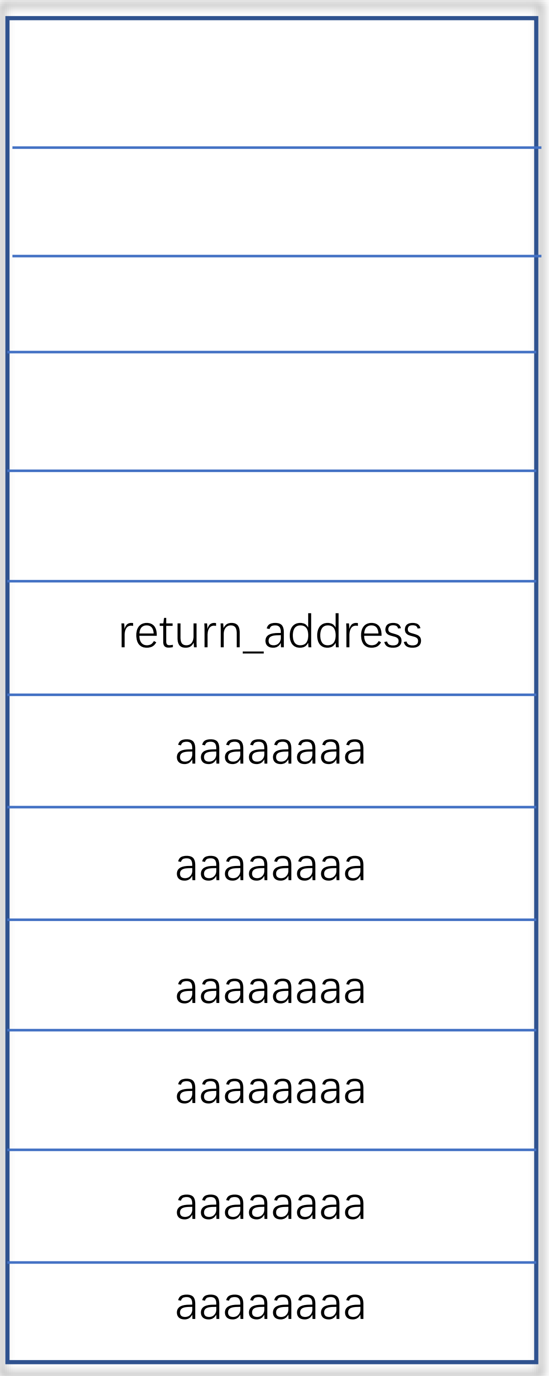


rdx	arg3
rsi	arg2
rdi	arg1
rbx	1
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



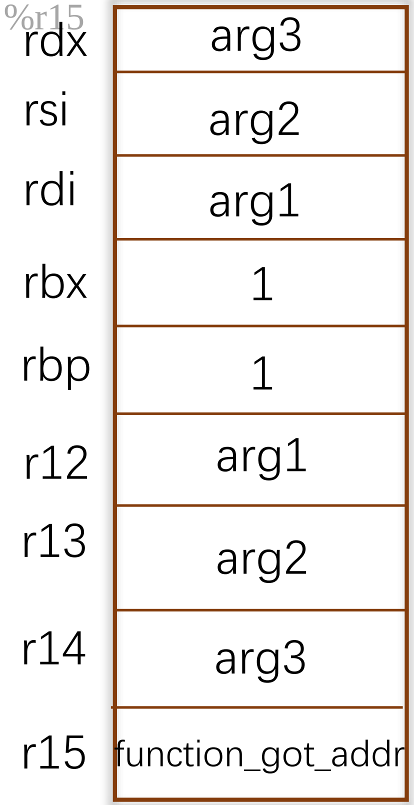
esp →

aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding

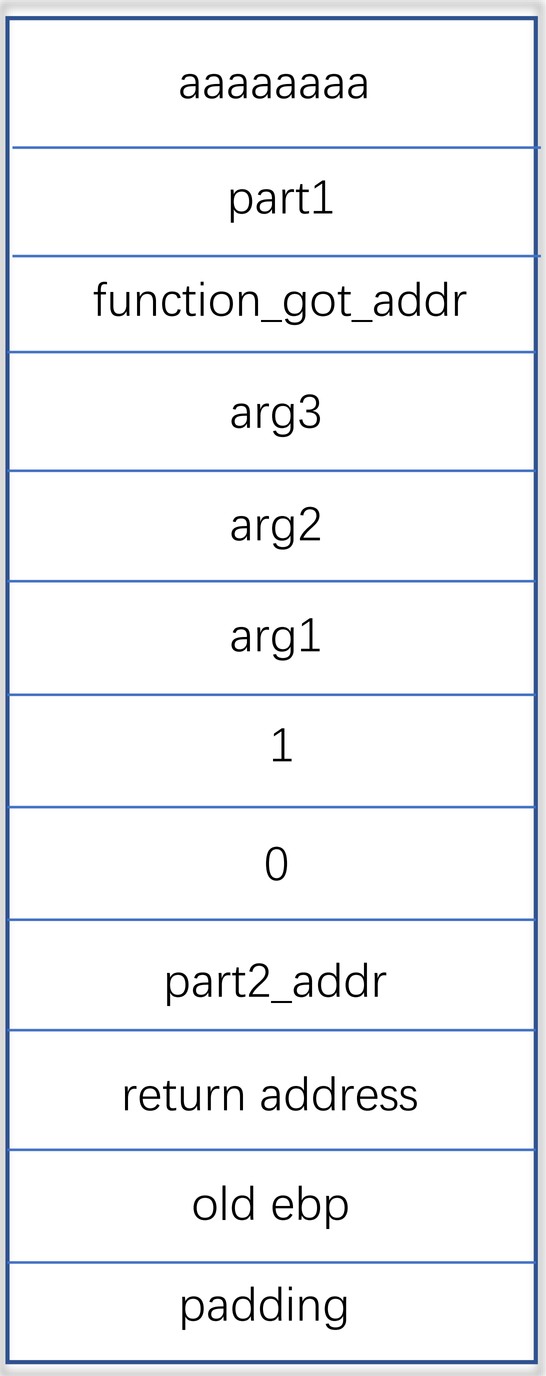


return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

```
# part 1
  401208:   4c 89 f2      mov   %r14,%rdx
  40120b:   4c 89 ee      mov   %r13,%rsi
  40120e:   44 89 e7      mov   %r12d,%edi
  401211:   41 ff 14 df   callq *(%r15,%rbx,8)
  401215:   48 83 c3 01   add   $0x1,%rbx
  401219:   48 39 dd      cmp   %rbx,%rbp
  40121c:   75 ea         jne   401208 <__libc_csu_init+0x38>
  40121e:   48 83 c4 08   add   $0x8,%rsp
  401222:   5b            pop   %rbx
  401223:   5d            pop   %rbp
  401224:   41 5c         pop   %r12
  401226:   41 5d         pop   %r13
  401228:   41 5e         pop   %r14
  40122a:   41 5f         pop   %r15
  40122c:   c3            retq
```



rdx	arg3
rsi	arg2
rdi	arg1
rbx	1
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

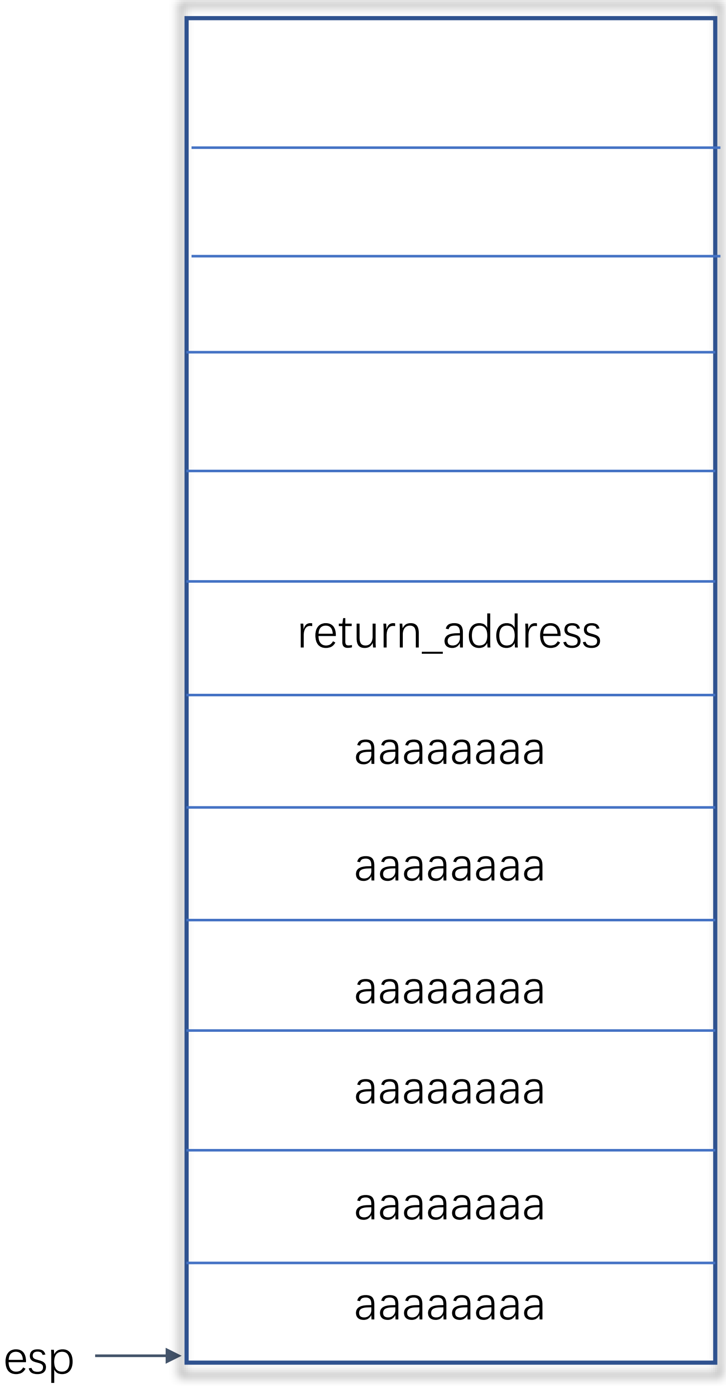
0

part2_addr

return address

old ebp

padding



return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

aaaaaaaa

aaaaaaaa

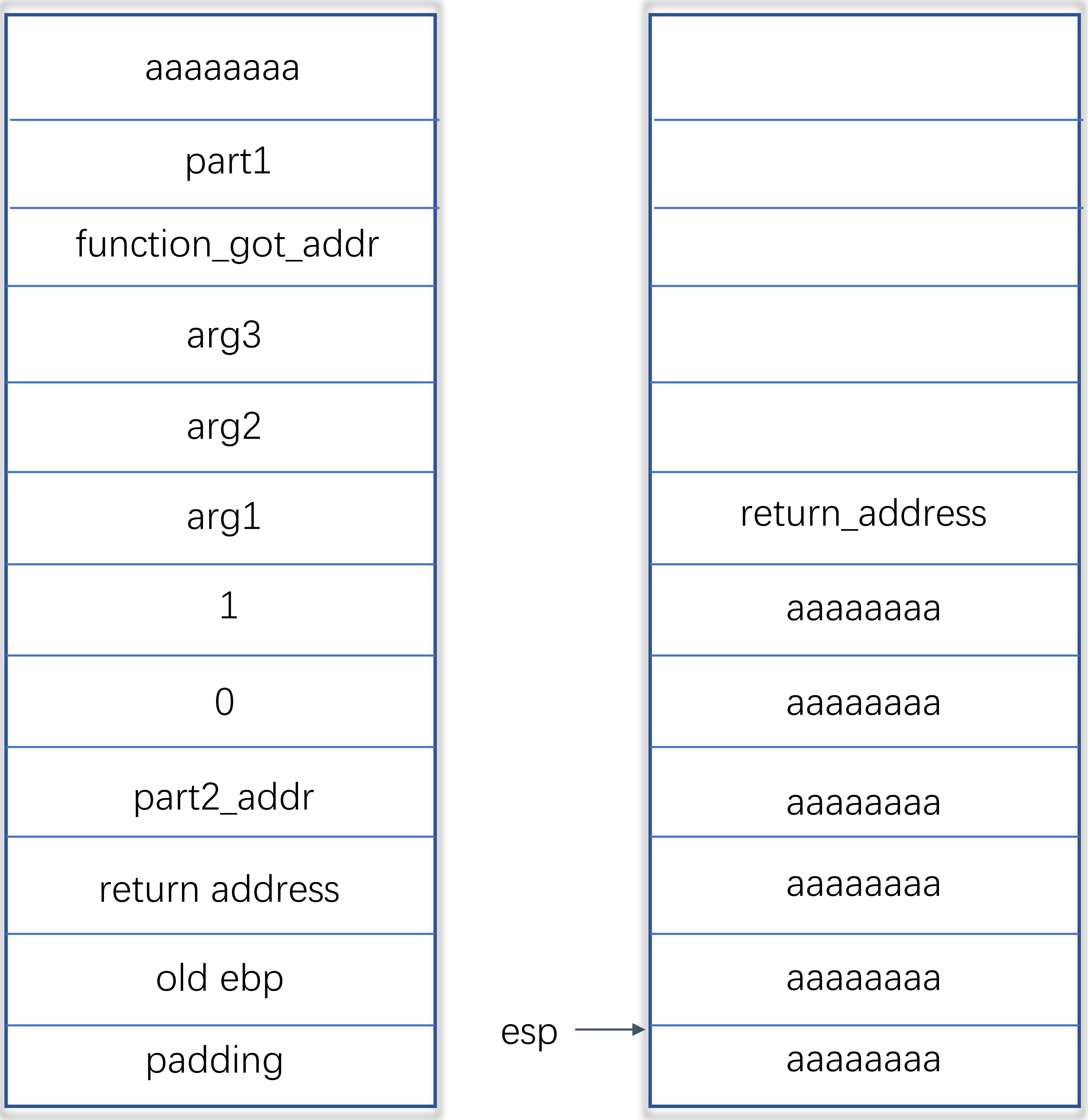
aaaaaaaa

esp

# part 1

```
401208:   4c 89 f2      mov    %r14,%rdx
40120b:   4c 89 ee      mov    %r13,%rsi
40120e:   44 89 e7      mov    %r12d,%edi
401211:   41 ff 14 df   callq  *(%r15,%rbx,8)
401215:   48 83 c3 01   add    $0x1,%rbx
401219:   48 39 dd      cmp    %rbx,%rbp
40121c:   75 ea         jne    401208 <__libc_csu_init+0x38>
40121e:   48 83 c4 08   add    $0x8,%rsp
401222:   5b            pop    %rbx
401223:   5d            pop    %rbp
401224:   41 5c         pop    %r12
401226:   41 5d         pop    %r13
401228:   41 5e         pop    %r14
40122a:   41 5f         pop    %r15
40122c:   c3            retq
```

rdx	arg3
rsi	arg2
rdi	arg1
rbx	aaaaaaaa
rbp	1
r12	arg1
r13	arg2
r14	arg3
r15	function_got_addr



aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

0

part2_addr

return address

old ebp

padding

return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

aaaaaaaa

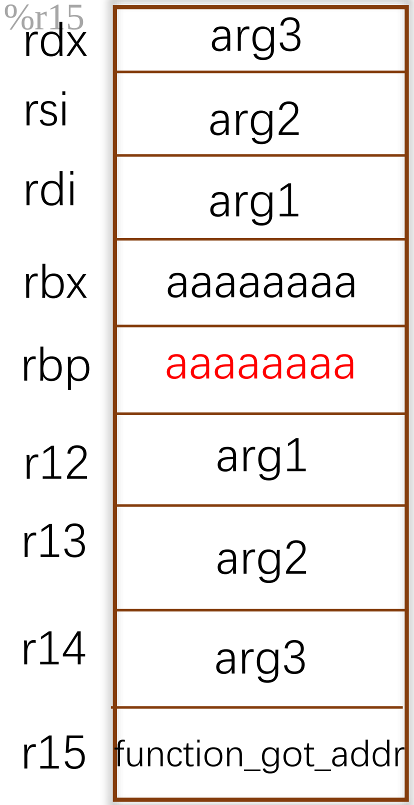
aaaaaaaa

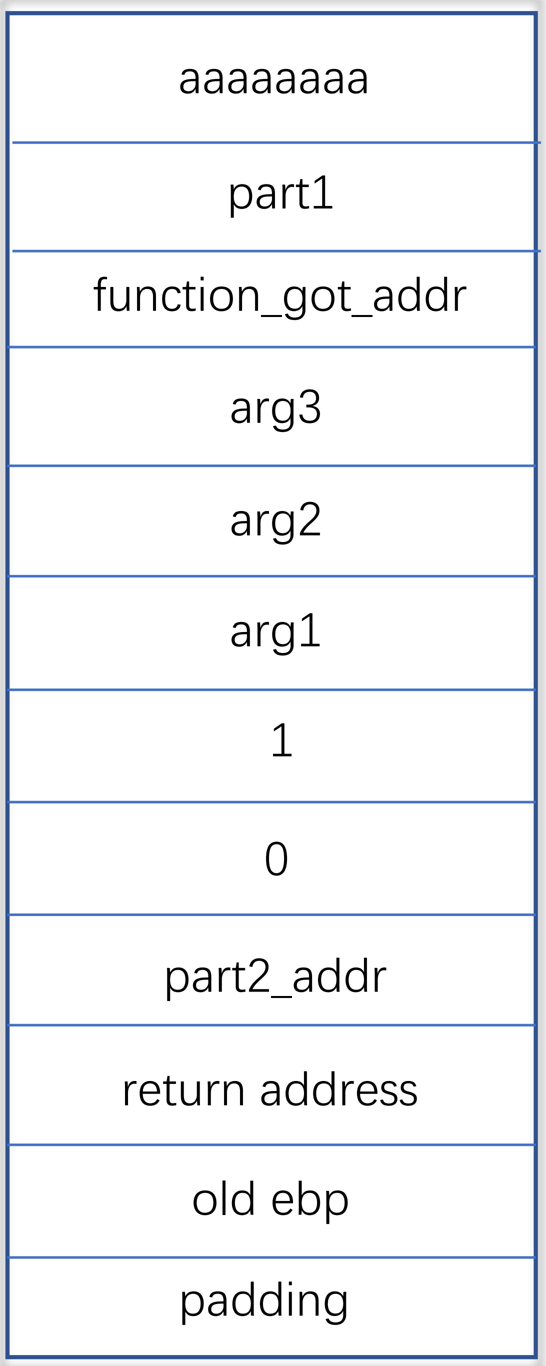
esp

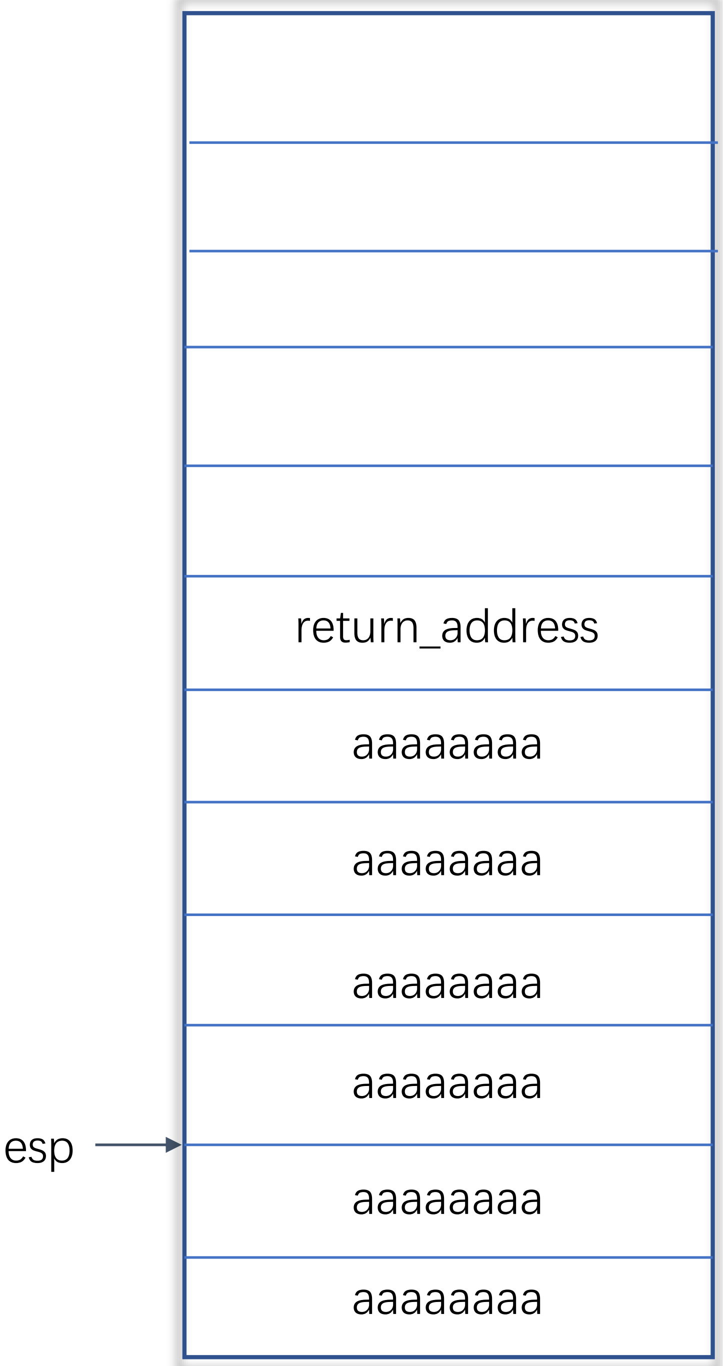
aaaaaaaa

# part 1

```
401208:   4c 89 f2     mov    %r14,%rdx
40120b:   4c 89 ee     mov    %r13,%rsi
40120e:   44 89 e7     mov    %r12d,%edi
401211:   41 ff 14 df  callq  *(%r15,%rbx,8)
401215:   48 83 c3 01  add    $0x1,%rbx
401219:   48 39 dd     cmp    %rbx,%rbp
40121c:   75 ea        jne    401208 <__libc_csu_init+0x38>
40121e:   48 83 c4 08  add    $0x8,%rsp
401222:   5b           pop    %rbx
401223:   5d           pop    %rbp
401224:   41 5c        pop    %r12
401226:   41 5d        pop    %r13
401228:   41 5e        pop    %r14
40122a:   41 5f        pop    %r15
40122c:   c3           retq
```

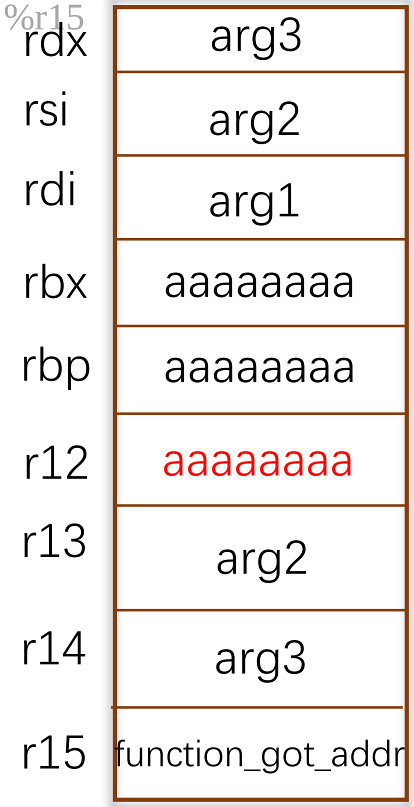




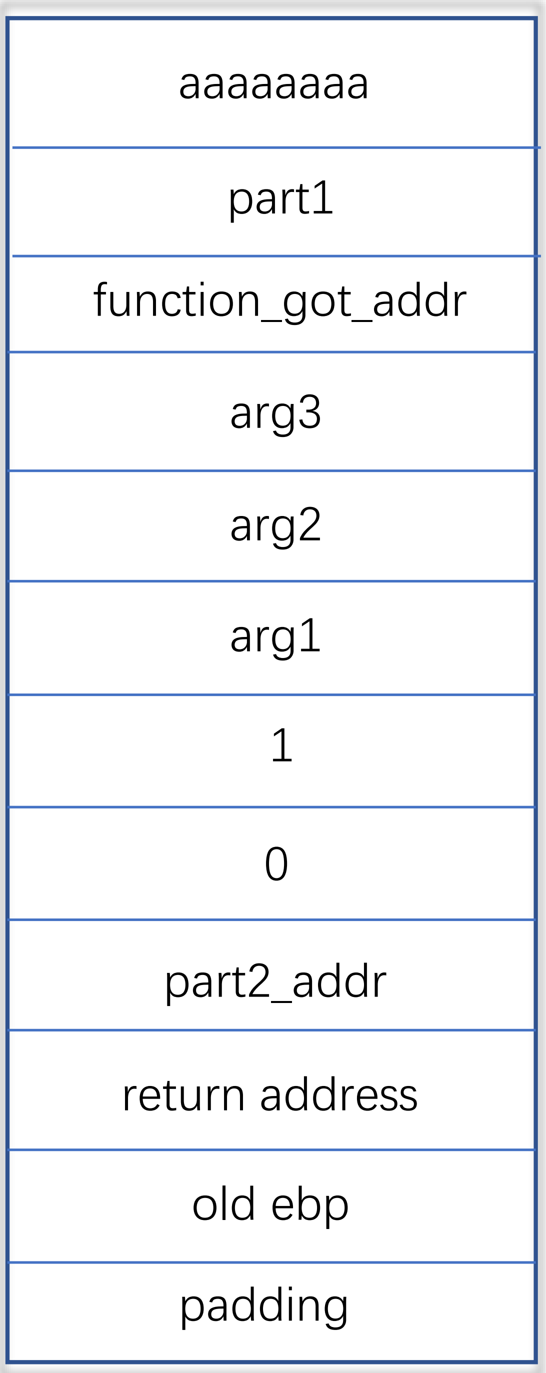


# part 1

```
401208:    4c 89 f2       mov    %r14,%rdx
40120b:    4c 89 ee       mov    %r13,%rsi
40120e:    44 89 e7       mov    %r12d,%edi
401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
401215:    48 83 c3 01    add    $0x1,%rbx
401219:    48 39 dd       cmp    %rbx,%rbp
40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
40121e:    48 83 c4 08    add    $0x8,%rsp
401222:    5b             pop    %rbx
401223:    5d             pop    %rbp
401224:    41 5c          pop    %r12
401226:    41 5d          pop    %r13
401228:    41 5e          pop    %r14
40122a:    41 5f          pop    %r15
40122c:    c3             retq
```



rdx	arg3
rsi	arg2
rdi	arg1
rbx	aaaaaaaa
rbp	aaaaaaaa
r12	aaaaaaaa
r13	arg2
r14	arg3
r15	function_got_addr



aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

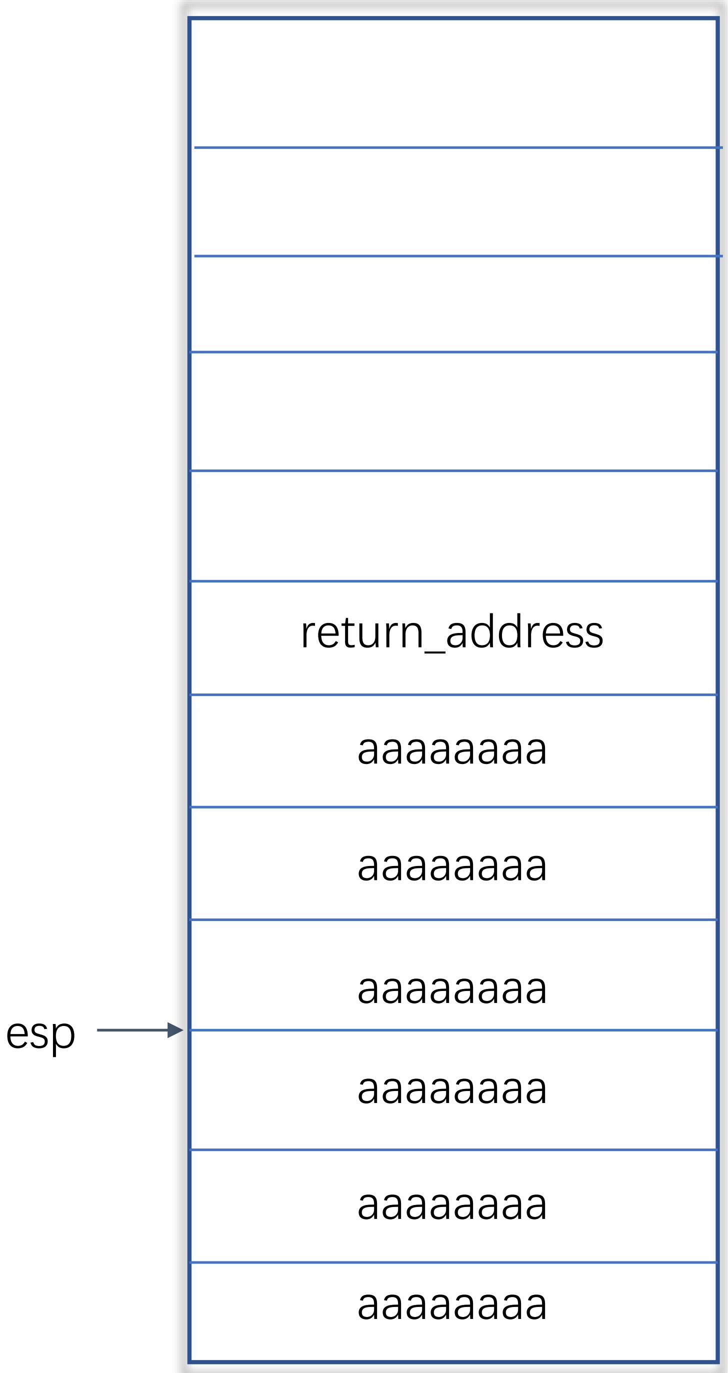
0

part2_addr

return address

old ebp

padding



return_address

aaaaaaaa

aaaaaaaa

aaaaaaaa

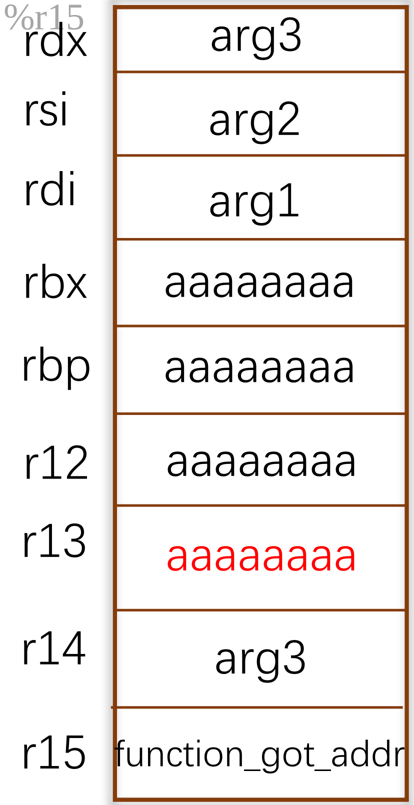
esp →

aaaaaaaa

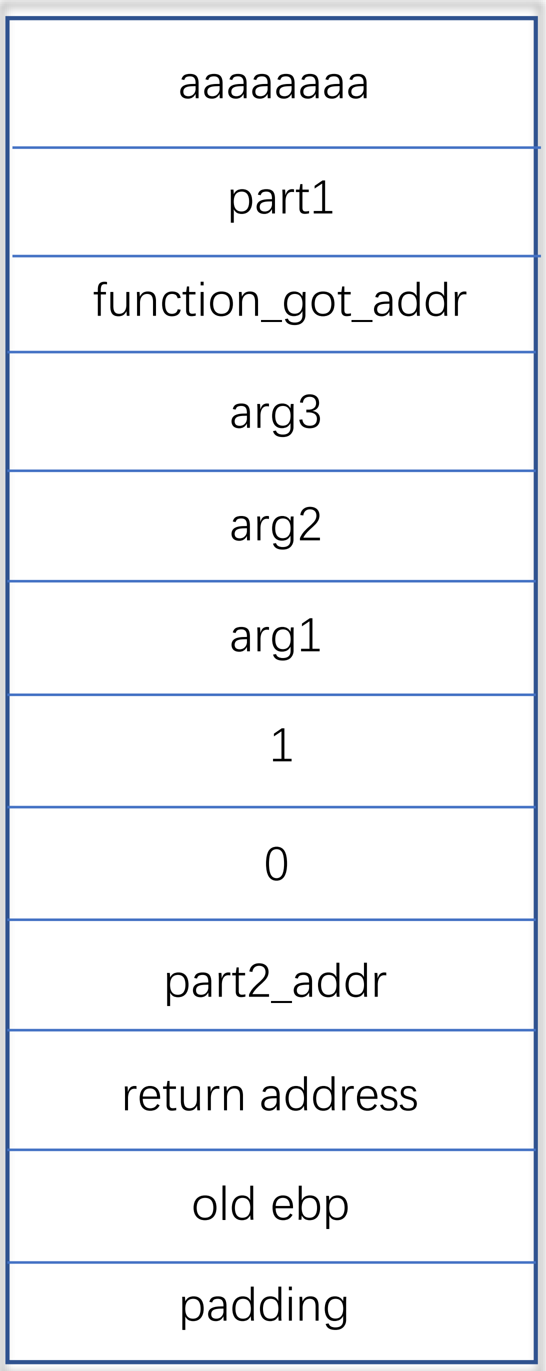
aaaaaaaa

aaaaaaaa

```
# part 1
  401208:    4c 89 f2       mov    %r14,%rdx
  40120b:    4c 89 ee       mov    %r13,%rsi
  40120e:    44 89 e7       mov    %r12d,%edi
  401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
  401215:    48 83 c3 01    add    $0x1,%rbx
  401219:    48 39 dd       cmp    %rbx,%rbp
  40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
  40121e:    48 83 c4 08    add    $0x8,%rsp
  401222:    5b             pop    %rbx
  401223:    5d             pop    %rbp
  401224:    41 5c          pop    %r12
  401226:    41 5d          pop    %r13
  401228:    41 5e          pop    %r14
  40122a:    41 5f          pop    %r15
  40122c:    c3             retq
```



rdx	arg3
rsi	arg2
rdi	arg1
rbx	aaaaaaaa
rbp	aaaaaaaa
r12	aaaaaaaa
r13	aaaaaaaa
r14	arg3
r15	function_got_addr



aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

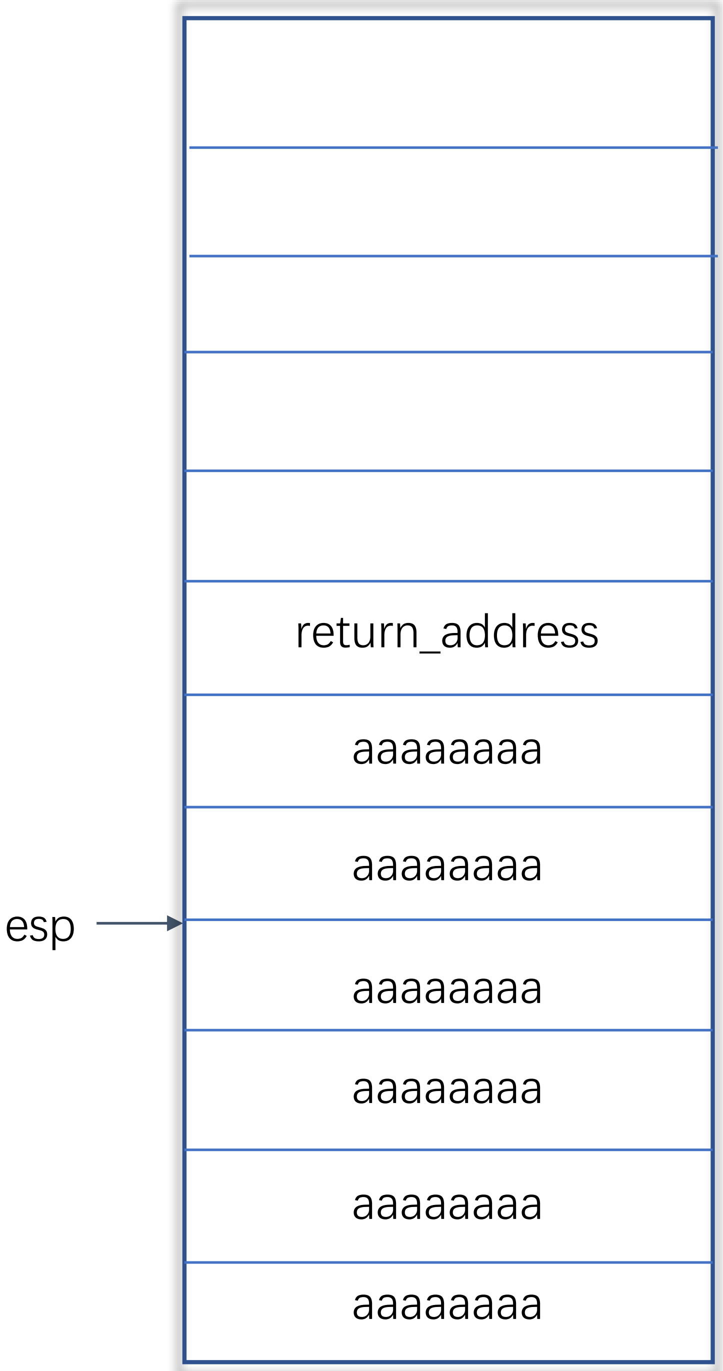
0

part2_addr

return address

old ebp

padding



return_address

aaaaaaaa

aaaaaaaa

esp

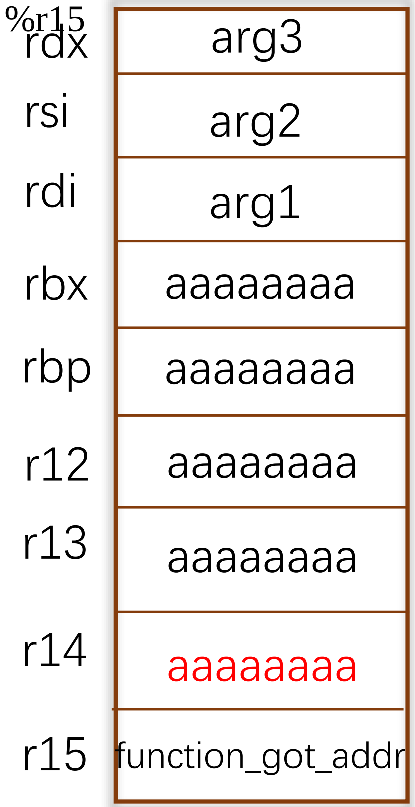
aaaaaaaa

aaaaaaaa

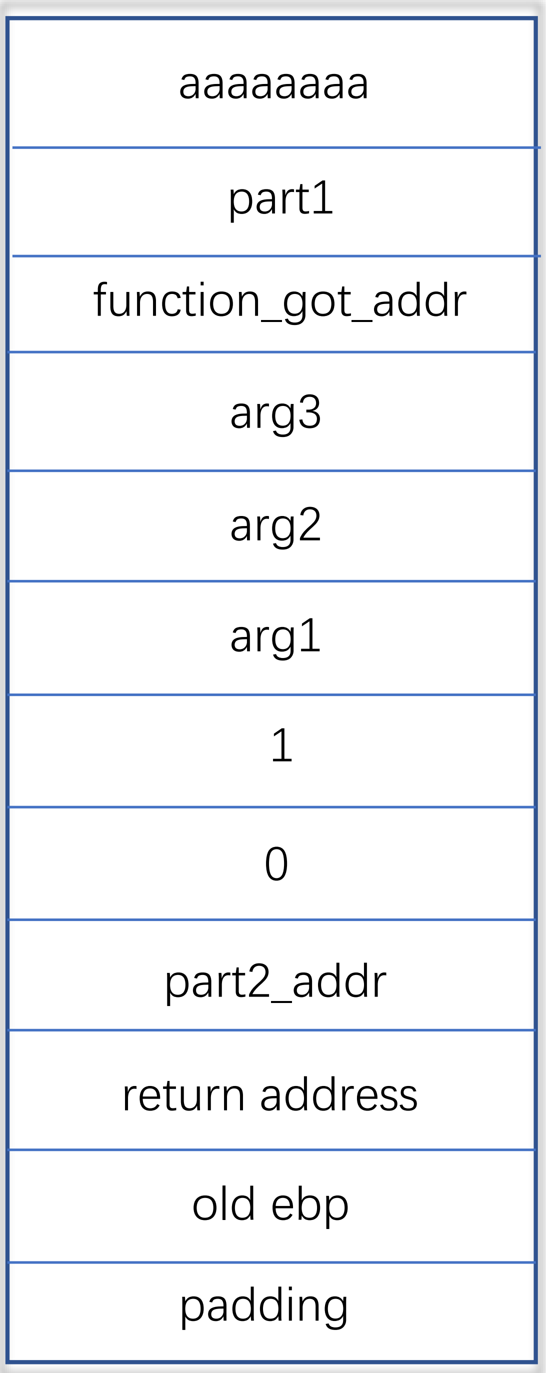
aaaaaaaa

aaaaaaaa

```
# part 1
  401208:    4c 89 f2       mov    %r14,%rdx
  40120b:    4c 89 ee       mov    %r13,%rsi
  40120e:    44 89 e7       mov    %r12d,%edi
  401211:    41 ff 14 df    callq  *(%r15,%rbx,8)
  401215:    48 83 c3 01    add    $0x1,%rbx
  401219:    48 39 dd       cmp    %rbx,%rbp
  40121c:    75 ea          jne    401208 <__libc_csu_init+0x38>
  40121e:    48 83 c4 08    add    $0x8,%rsp
  401222:    5b             pop    %rbx
  401223:    5d             pop    %rbp
  401224:    41 5c          pop    %r12
  401226:    41 5d          pop    %r13
  401228:    41 5e          pop    %r14
  40122a:    41 5f          pop    %r15
  40122c:    c3             retq
```



rdx	arg3
rsi	arg2
rdi	arg1
rbx	aaaaaaaa
rbp	aaaaaaaa
r12	aaaaaaaa
r13	aaaaaaaa
r14	aaaaaaaa
r15	function_got_addr



aaaaaaaa

part1

function_got_addr

arg3

arg2

arg1

1

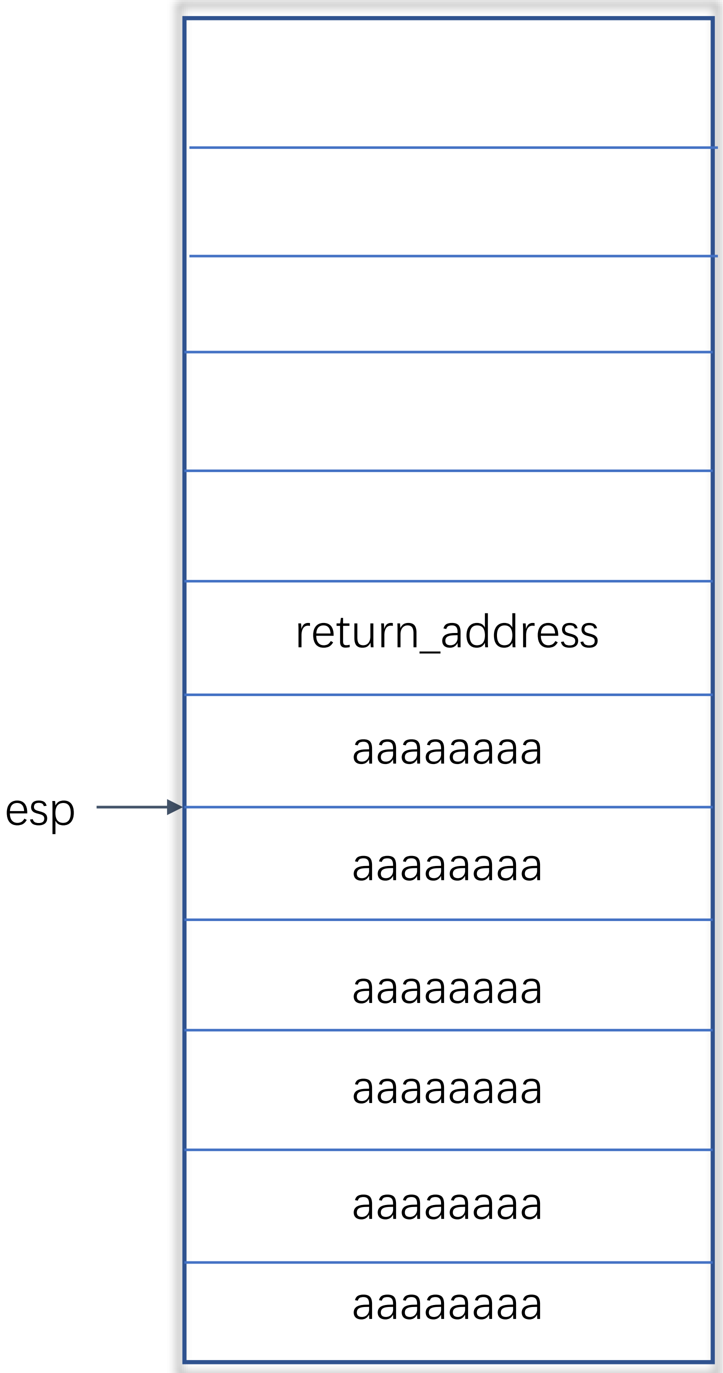
0

part2_addr

return address

old ebp

padding



return_address

esp →

aaaaaaaa

aaaaaaaa

aaaaaaaa

aaaaaaaa

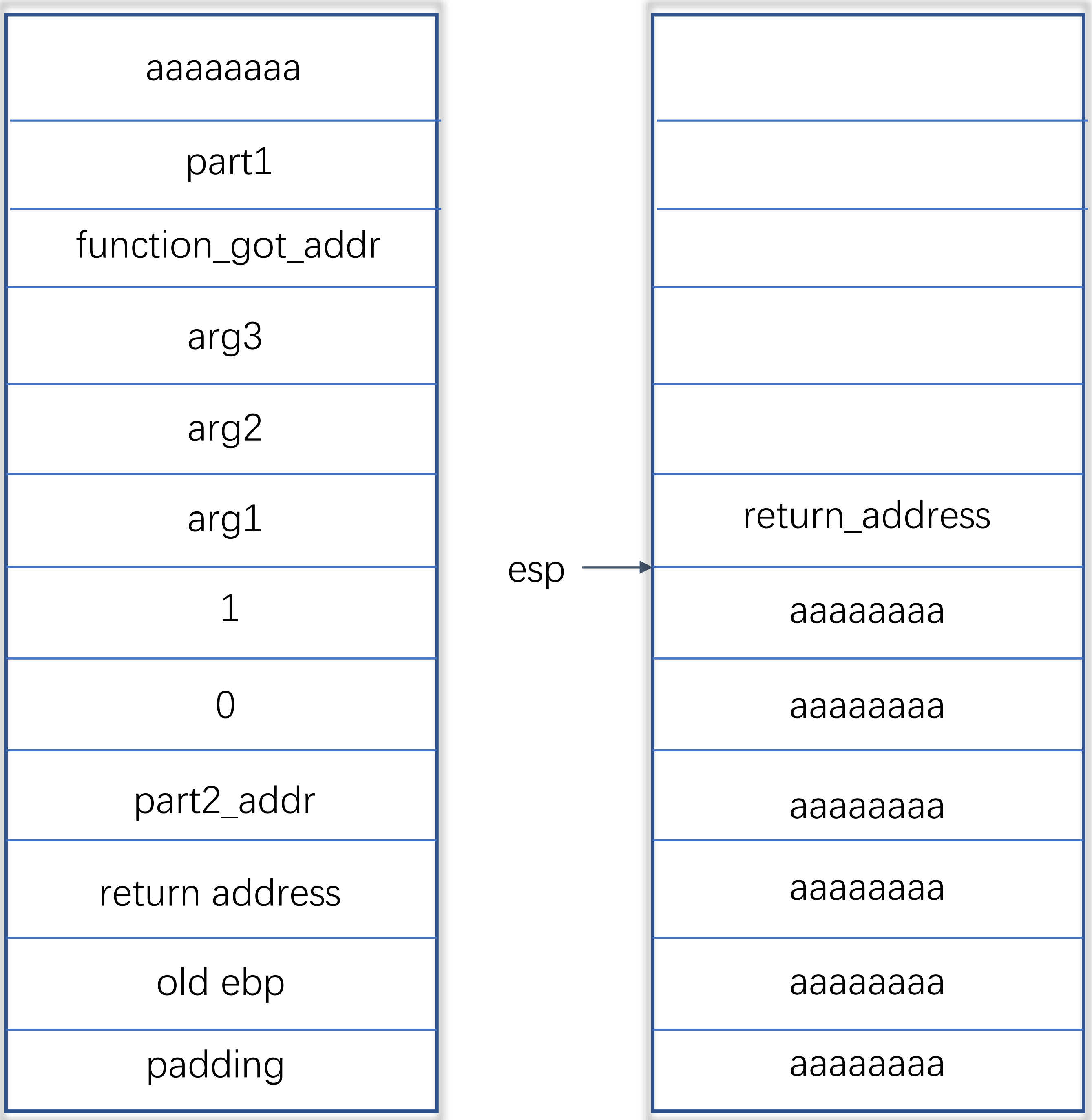
aaaaaaaa

aaaaaaaa

# part 1

```
401208:   4c 89 f2       mov    %r14,%rdx
40120b:   4c 89 ee       mov    %r13,%rsi
40120e:   44 89 e7       mov    %r12d,%edi
401211:   41 ff 14 df    callq  *(%r15,%rbx,8)
401215:   48 83 c3 01    add    $0x1,%rbx
401219:   48 39 dd       cmp    %rbx,%rbp
40121c:   75 ea          jne    401208 <__libc_csu_init+0x38>
40121e:   48 83 c4 08    add    $0x8,%rsp
401222:   5b             pop    %rbx
401223:   5d             pop    %rbp
401224:   41 5c          pop    %r12
401226:   41 5d          pop    %r13
401228:   41 5e          pop    %r14
40122a:   41 5f          pop    %r15
40122c:   c3             retq
```

rdx	arg3
rsi	arg2
rdi	arg1
rbx	aaaaaaaa
rbp	aaaaaaaa
r12	aaaaaaaa
r13	aaaaaaaa
r14	aaaaaaaa
r15	aaaaaaaa


aaaaaaaa
part1
function_got_addr
arg3
arg2
arg1
1
0
part2_addr
return address
old ebp
padding
esp
return_address
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa