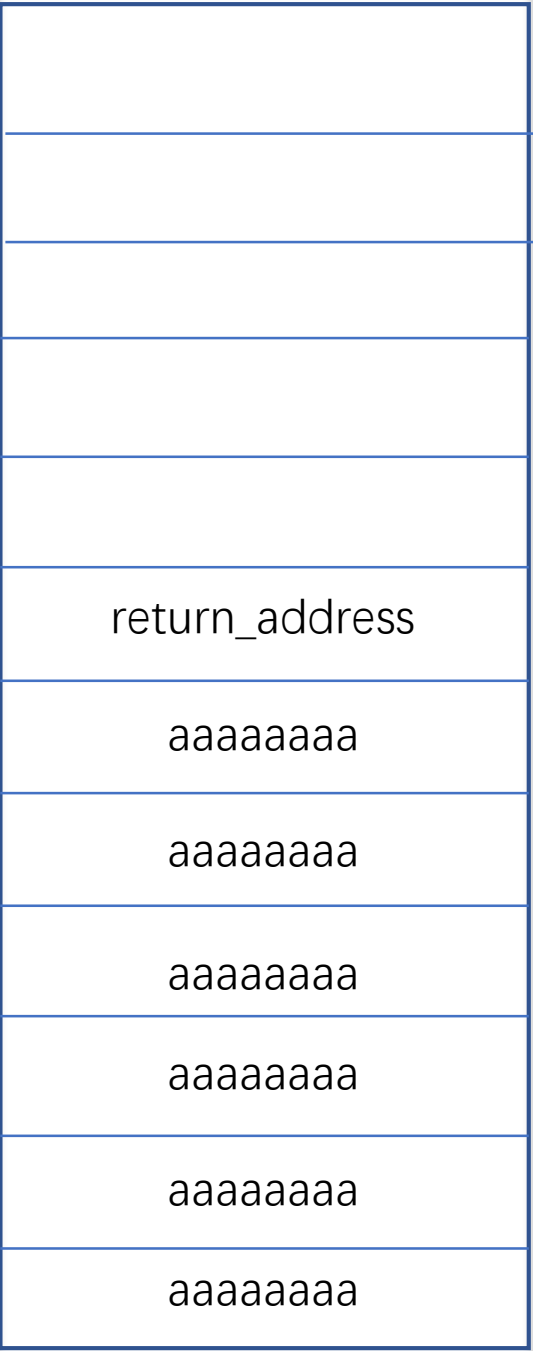
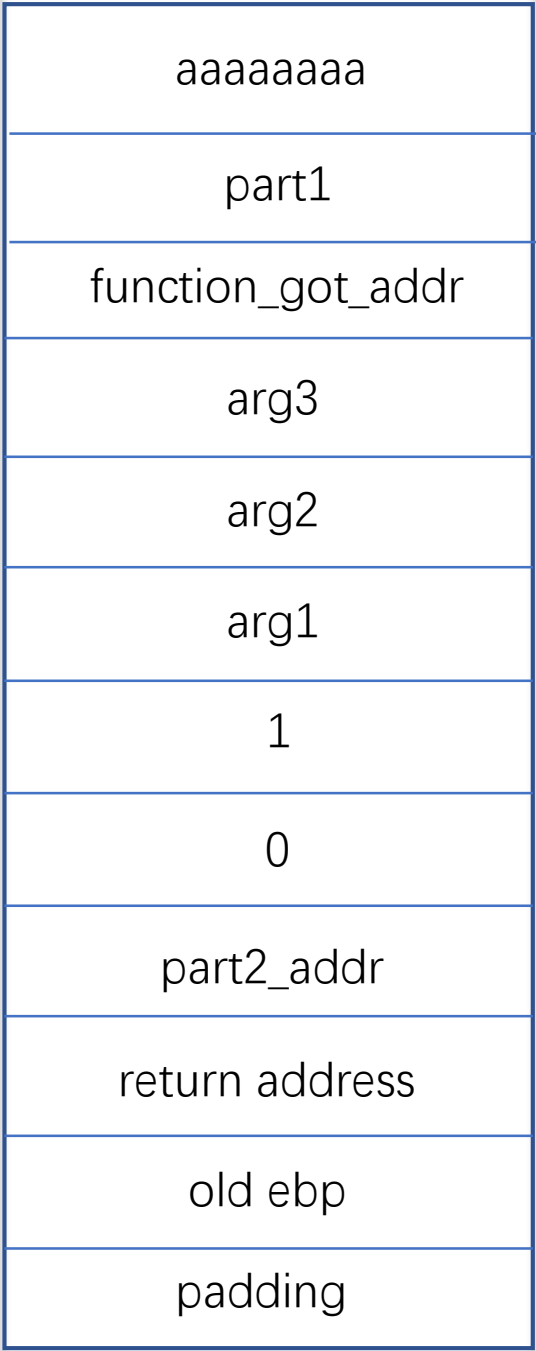


# part 2

```
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 →



















# 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	
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

return_address
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	
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

# 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

# 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

# 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

# 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

# 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

# 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



# 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

esp →

return_address
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

```

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

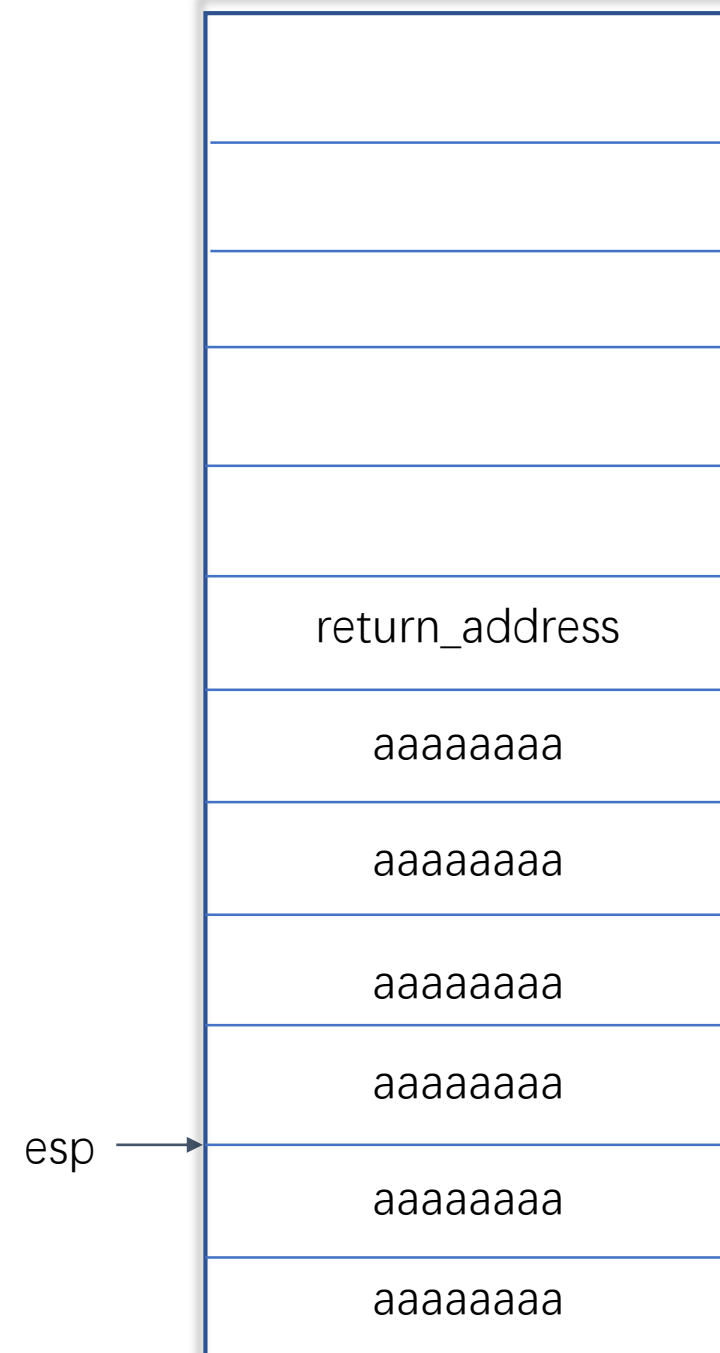
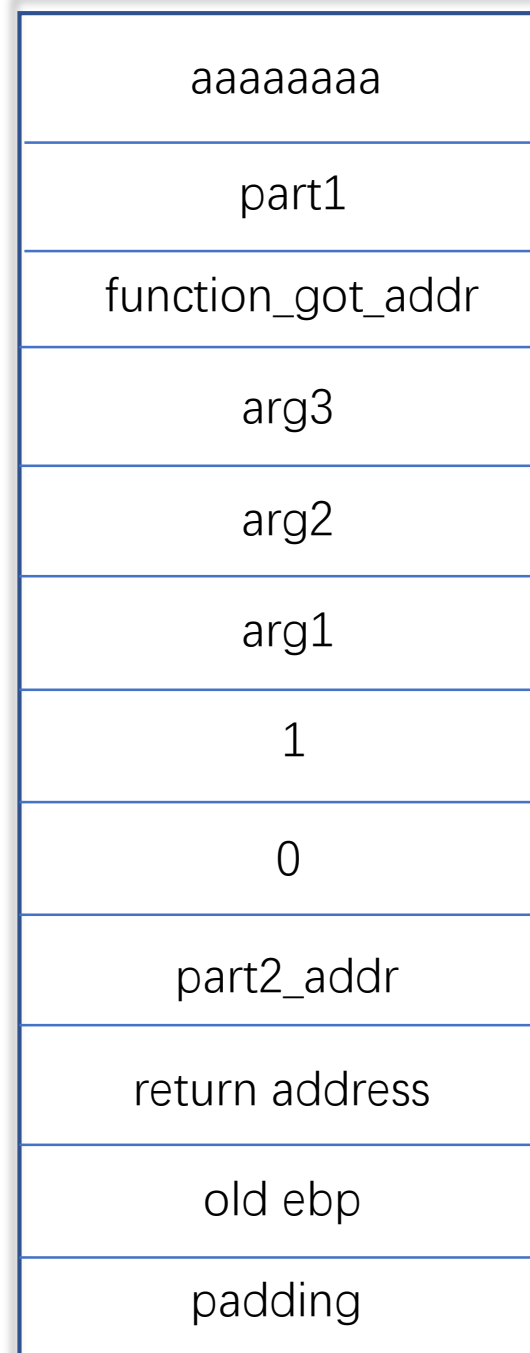
A diagram of a memory stack. It consists of a vertical column of 12 rectangular boxes. The second box from the bottom is labeled "return\_address". The bottom-most box is labeled "aaaaaaaa". The box immediately above it is also labeled "aaaaaaaa". The three boxes above that are each labeled "aaaaaaaa". The top five boxes are empty. To the left of the stack, the text "esp" is followed by a horizontal arrow pointing to the top edge of the bottom-most box.

## # 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	
<b>401224:</b>	<b>41 5c</b>	<b>pop</b>	<b>%r12</b>	
401226:	41 5d	pop	%r13	
401228:	41 5e	pop	%r14	
40122a:	41 5f	pop	%r15	
40122c:	c3	retq		

arg3

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



## # 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	
<b>401226:</b>	<b>41 5d</b>	<b>pop</b>	<b>%r13</b>	
401228:	41 5e	pop	%r14	
40122a:	41 5f	pop	%r15	
40122c:	c3	retq	rdx	arg3

rsi

rdi

rbx

rbp

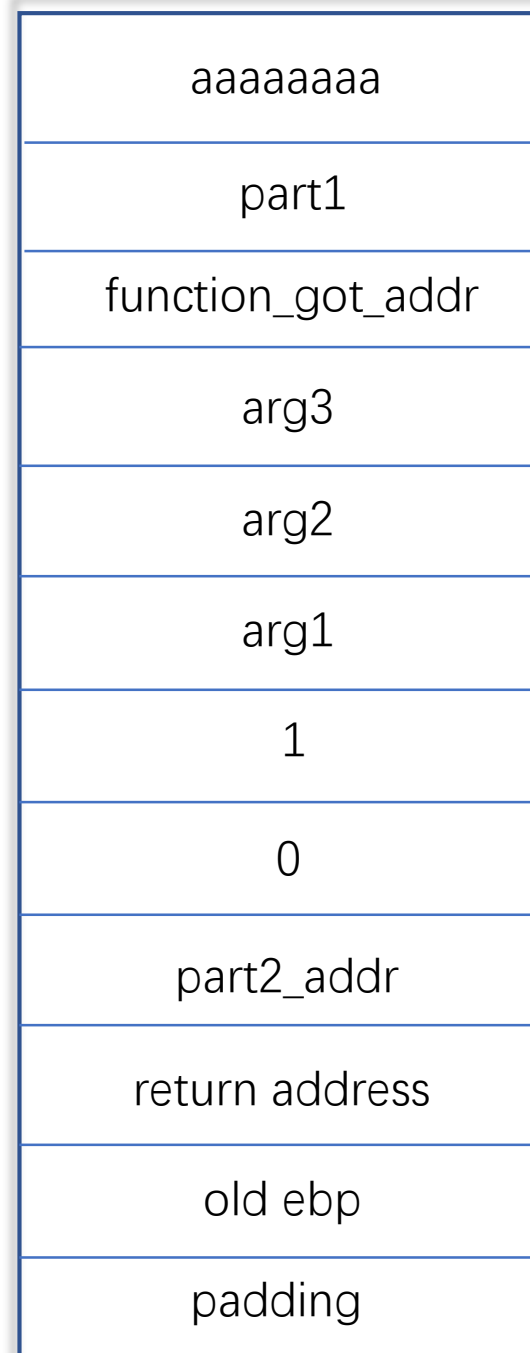
r12

r13

r14

-15

arg3
arg2
arg1
aaaaaaaa
aaaaaaaa
aaaaaaaa
arg2
arg3
function_got_addr



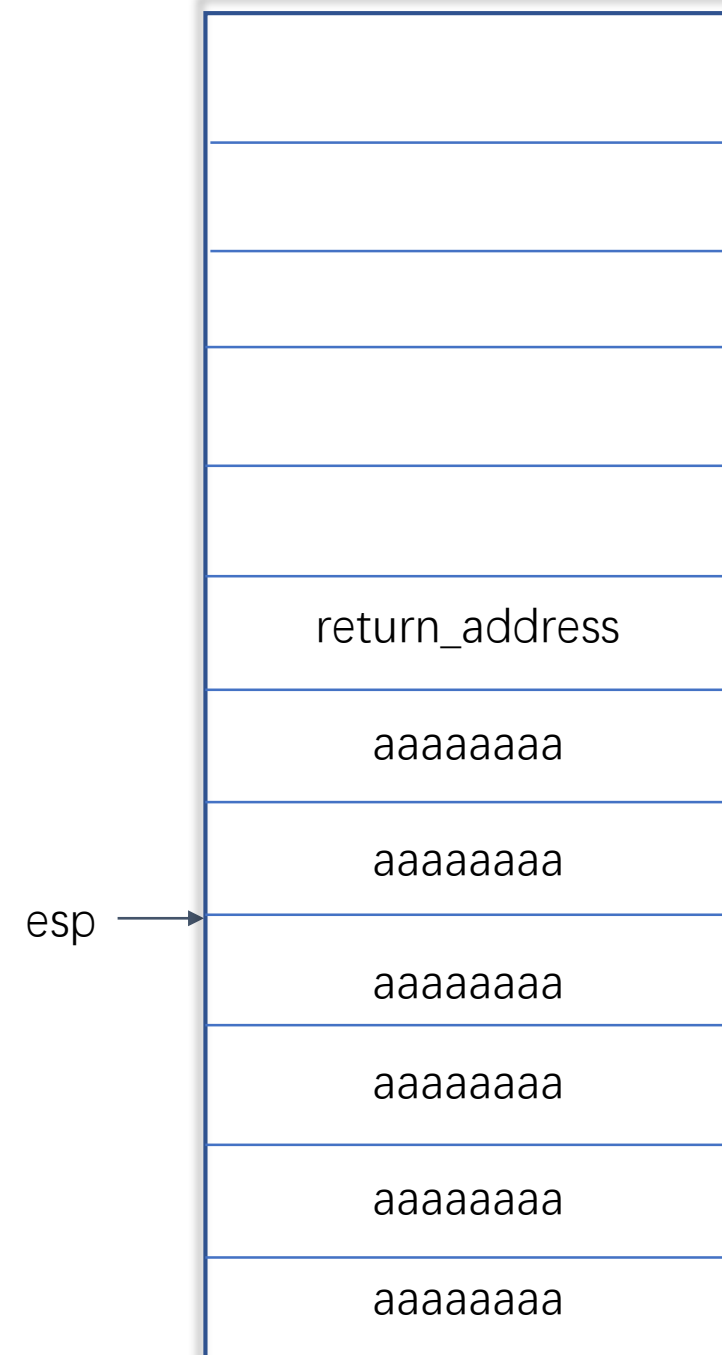
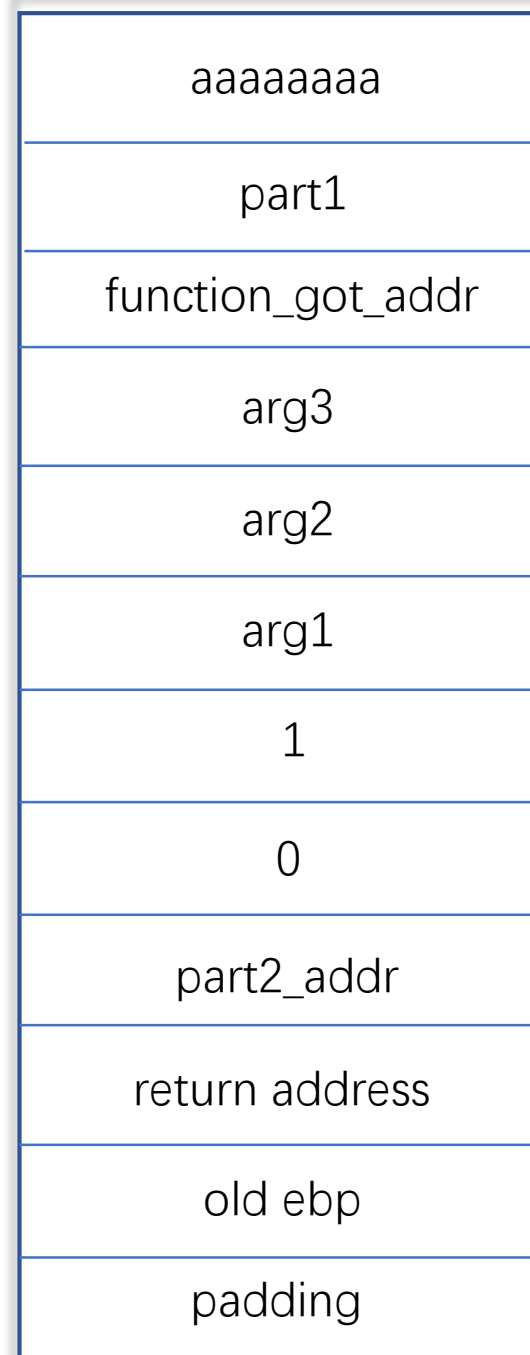
## # part 1

```

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

```

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



## # 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

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

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

A diagram of a stack memory layout. It consists of a vertical stack of 10 rectangular boxes. The second box from the bottom is labeled "return\_address". The third box from the bottom is labeled "aaaaaaaa". The fourth box from the bottom is labeled "aaaaaaaa". The fifth box from the bottom is labeled "aaaaaaaa". The sixth box from the bottom is labeled "aaaaaaaa". The seventh box from the bottom is labeled "aaaaaaaa". The eighth box from the bottom is labeled "aaaaaaaa". The ninth box from the bottom is labeled "aaaaaaaa". The tenth box from the bottom is labeled "aaaaaaaa". An arrow labeled "esp" points to the top of the eighth box from the bottom.

return_address
aaaaaaaa
esp →
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa

