Doubly-Linked List Unlink

- Here we have a doubly-linked list with 3 items
  - It is not circularly linked, but NULL terminated
  - Let's step through an unlink operation on B

item_t A	@ 0x414148
long data1	0x3134
item_t* next	**0x424278 (&B)**
item_t* prev	**0x0 (NULL)**
size_t data2	0x259
char* data3	0x7fff3238

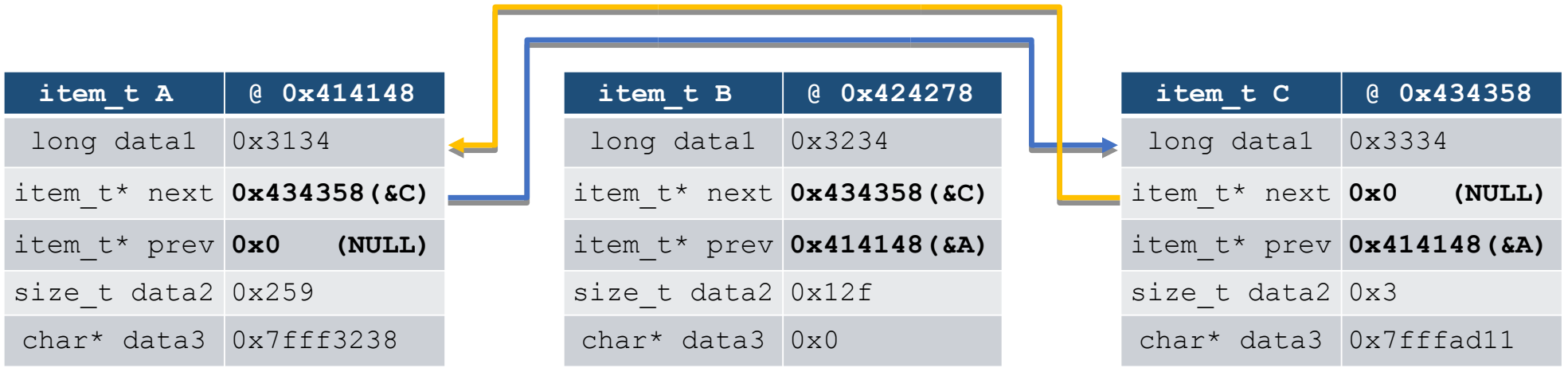
item_t B	@ 0x424278
long data1	0x3234
item_t* next	**0x434358 (&C)**
item_t* prev	**0x414148 (&A)**
size_t data2	0x12f
char* data3	0x0

item_t C	@ 0x434358
long data1	0x3334
item_t* next	**0x0 (NULL)**
item_t* prev	**0x434358 (&B)**
size_t data2	0x3
char* data3	0x7fffad11

Doubly-Linked List Unlink

```
void unlink(item_t* e) {
   e->next->prev = e->prev;
   e->prev->next = e->next;
}
```

```
mov    0x8(%rdi),%rdx    # rdx = e->next
mov    0x10(%rdi),%rax   # rax = e->prev
mov    %rax,0x10(%rdx)   # (rdx)->prev = e->prev
mov    %rdx,0x8(%rax)    # (rax)->next = e->next
retq
```



item_t A	@ 0x414148
long data1	0x3134
item_t* next	**0x434358 (&C)**
item_t* prev	**0x0 (NULL)**
size_t data2	0x259
char* data3	0x7fff3238

item_t B	@ 0x424278
long data1	0x3234
item_t* next	**0x434358 (&C)**
item_t* prev	**0x414148 (&A)**
size_t data2	0x12f
char* data3	0x0

item_t C	@ 0x434358
long data1	0x3334
item_t* next	**0x0 (NULL)**
item_t* prev	**0x414148 (&A)**
size_t data2	0x3
char* data3	0x7fffad11

Doubly-Linked List Unlink after Corruption

???	@ 0x202020
+0x00	0x0
+0x08	0x0
+0x10	0x0

???	@ 0x303030
+0x00	0x0
+0x08	0x0
+0x10	0x0

```
mov     0x8(%rdi),%rdx    # rdx = e->next
mov     0x10(%rdi),%rax   # rax = e->prev
mov     %rax,0x10(%rdx)   # (rdx)->prev = e->prev
mov     %rdx,0x8(%rax)    # (rax)->next = e->next
retq
```

Heap-Overflow
into this structure

item_t A	@ 0x414148
long data1	0x3134
item_t* next	**0x424278 (&B)**
item_t* prev	**0x0 (NULL)**
size_t data2	0x259
char* data3	0x7fff3238

item_t B	@ 0x424278
long data1	0x101010
item_t* next	**0x202020 (&C)**
item_t* prev	**0x303030 (&A)**
size_t data2	0x12f
char* data3	0x0

item_t C	@ 0x434358
long data1	0x3334
item_t* next	**0x0 (NULL)**
item_t* prev	**0x434358 (&B)**
size_t data2	0x3
char* data3	0x7fffad11

Doubly-Linked List Unlink after Corruption

???	@ 0x202020
+0x00	0x0
+0x08	0x0
+0x10	**0x303030**

???	@ 0x303030
+0x00	0x0
+0x08	**0x202020**
+0x10	0x0

```
mov     0x8(%rdi),%rdx    # rdx = 0x202020
mov     0x10(%rdi),%rax   # rax = 0x303030
mov     %rax,0x10(%rdx)   # (0x202020)+10 = 0x303030
mov     %rdx,0x8(%rax)    # (0x303030)+8  = 0x202020
retq
```

item_t A	@ 0x414148
long data1	0x3134
item_t* next	**0x424278 (&B)**
item_t* prev	**0x0 (NULL)**
size_t data2	0x259
char* data3	0x7fff3238

item_t B	@ 0x424278
long data1	0x101010
item_t* next	**0x202020 (&C)**
item_t* prev	**0x303030 (&A)**
size_t data2	0x12f
char* data3	0x0

item_t C	@ 0x434358
long data1	0x3334
item_t* next	**0x0 (NULL)**
item_t* prev	**0x434358 (&B)**
size_t data2	0x3
char* data3	0x7fffad11