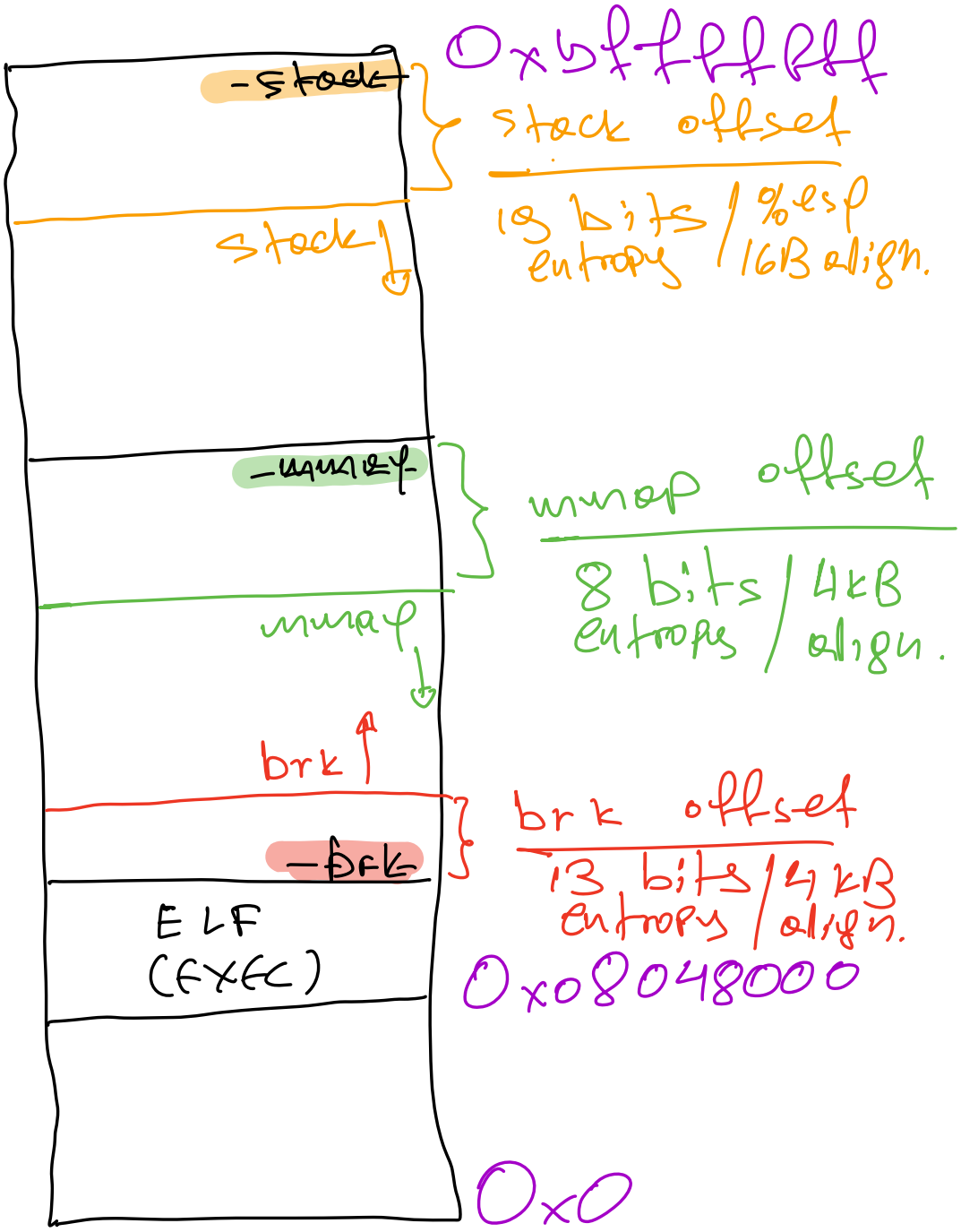
Address Space Layout Randomization

- ASLR: artificially randomize the location of parts of the address space
  - stack, heap, mmap, ...
  - partial vs. full
    - partial
      - stack
      - mmap
      - heap
    - full
      - stack
      - mmap
      - heap
      - exec


0xbffffffff
stack offset
19 bits / %esp entropy / 16B align.
stack
mmap offset
8 bits / 4kB entropy / align.
mmap
brk
brk offset
13 bits / 4 kB entropy / align.
ELF (EXEC)
0x08048000
0x0

Stack

0xbffff000
0xbfff000
0xbffeff0
⋮

$2^{13} = 524288$

mmap

0xb8000000
0xb7fff000
0xb7ffe000
0xb7ffd000
⋮

$2^8 = 256$

heap

0x0804c000
0x08049000
0x08048000
⋮

$2^{13} = 8192$