Stack execution


Allocate local buffer
(126 bytes in the stack)


Copy argument into local buffer

```
void foo(char *str){
  char buf[126];
  strcpy(buf,str);
}
```

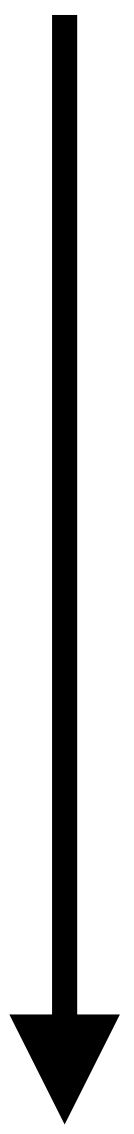
0x FF FF FF FF

0x 00 00 00 00

0x FF FF FF FF

Stack grows down

Caller Frame



foo Frame

Args

Return Address

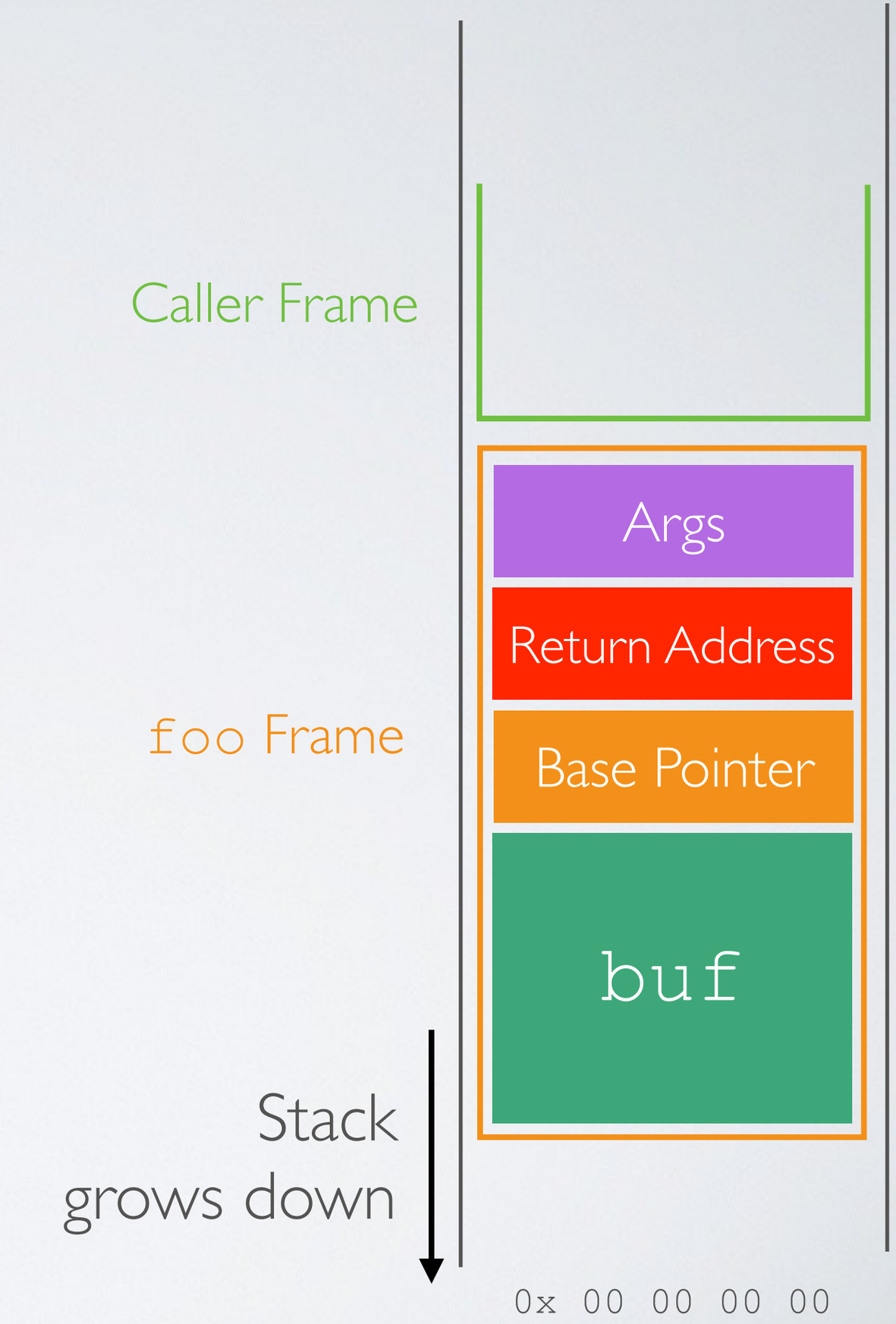
Base Pointer

buf

Stack execution

```
void foo(char *str){
  char buf[126];
  strcpy(buf,str);
}
```

Copy argument into local buffer



What if the buffer is overstuffed?

- `strcpy` does not check whether the string at `*str` contains fewer than 126 characters

- If a string longer than 126 bytes is copied into buffer, it will overwrite adjacent stack locations