

@石博:

- 遇到的首要问题就是读不懂 linux 命令与汇编，感谢 [bing.com](http://bing.com)，为什么不感谢 google 呢，因为我翻不了墙啊，服务器太贵了租不起。然后就是读出来的 ebp 和 eip 值我当成了指针，直接当指针使用了，报错很清晰，改完程序就ok了，完结撒花。

@余崧林:

- 熟悉了解了操作系统的底层中断机制
- 石博牛逼