综合研究报告二

这次的研究内容是如何得到子函数的段地址和偏移地址。而我测试后发现子函数名包含了子函数的偏移地址。所以这次研究主要是要找到一个获取子函数段地址的方法。

我尝试了直接取地址、函数指针这两种方法，并没有实现这个功能。但是找到一些野路子。

1. 可以直接输出CS寄存器的值，但是我觉得这个方法和目的不太相符，因为这样就默认所有子函数的段地址都和main函数一样。
2. 使用内联汇编，使用seg指令获取子函数的段地址到某一指定内存，然后在用之前学的访问内存方法来得到这个地址。但是由于暂时没有找到tasm.exe，所以编译暂时没通过，不能进行测试。

另外，在这个过程里我在想这个问题:如果子函数名不包含段地址信息，那么在遇见长距离调用的时候，段地址信息从何而来？

由此可以有这样的猜想：

1. 子函数名其实包含了段地址信息，但是我没找到正确的方式访问。
2. 在c0s模式下，代码段最长为64kb，不会超出一个段地址的长度，所以编译的时候只将函数名编译成偏移地址而不包含段地址。
3. 在对程序进行初始化的时候，可能会将各个子函数的地址信息存在某个表中，通过查表得到地址，而函数名只表示表中的相对位置。

因为时间问题，测试暂时没有进行。

总结：这次研究的问题，目前看来实用性不高，可能是我研

究深度不够导致的。