前面说过，DWORDSHOOT的伪代码如下

int remove(ListNode \* node)

{

node->blink->flink = node->flink;

node->flink->blink = node-blink;

return 0;

}

DWORDSHOOT只是使用了第一句，那么第二句呢？

来分析一下，第一句是将flink的值写入地址blink，所以第二句的意思是将blink写入地址flink往后偏移4字节的地方，我们构造的flink为shellcode起始地址，所以shellcode就会变成这样，一般情况下这4字节的指令会直接执行过去没有影响，但是万一有影响那就要想其它办法了

00360688 90 nop

00360689 90 nop

0036068A 90 nop

0036068B 90 nop

0036068C 20F0 and al, dh

0036068E FD std

0036068F ^ 7F 90 jg short 00360621

00360691 90 nop

00360692 90 nop

00360693 90 nop