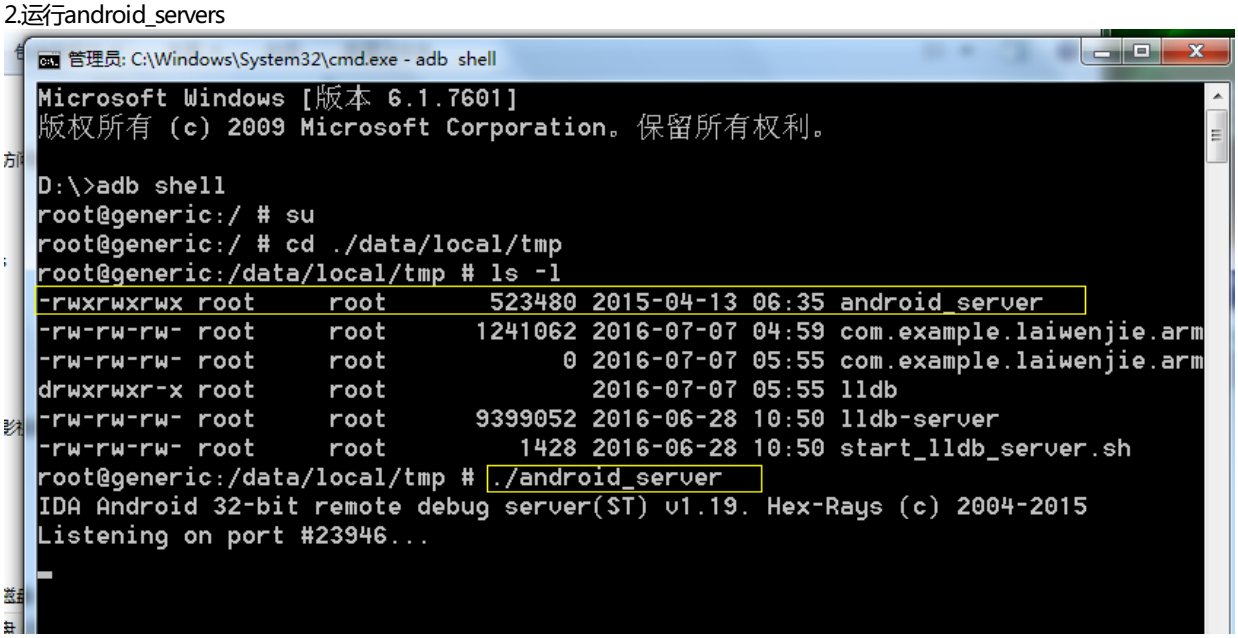
脱壳基础（调试修改内存）

加壳脱壳第一天.rar

这个程序的demo我给弄丢了。
应该就是
　一个按钮，监听事件是实现加法
　再写一个减法函数。但不调用
我们做的就是希望在内存中找到加法函数指令，修改为减法的。
以在脑中建立，内存可修改的概念。

1.运行程序

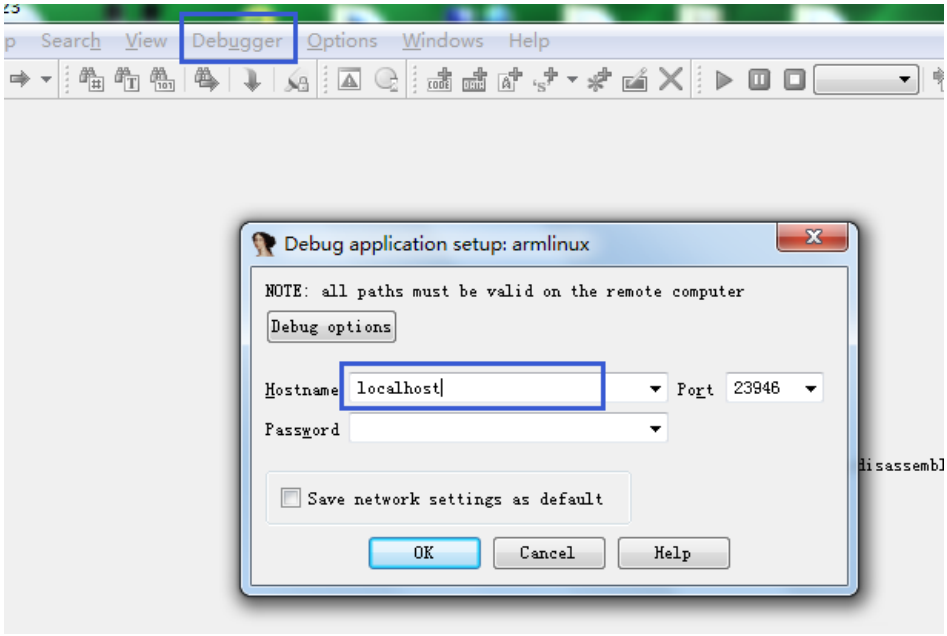
2.运行android_servers

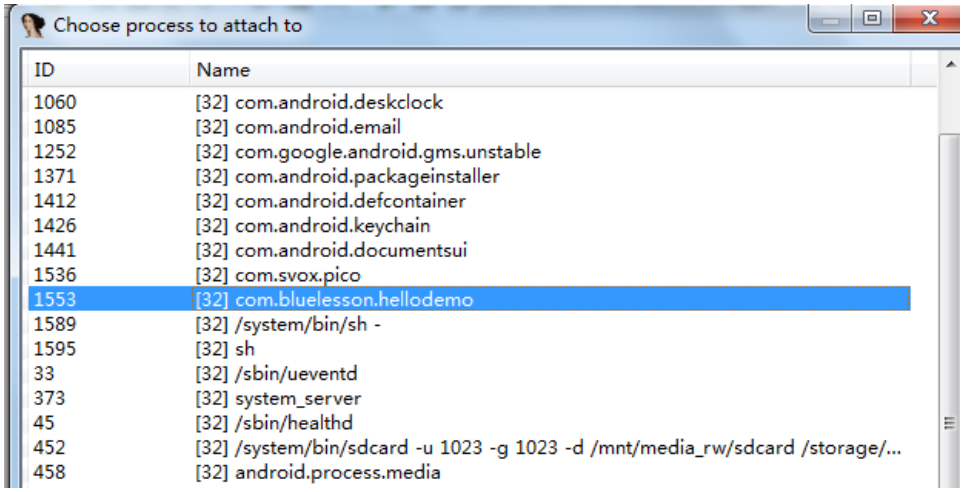


3.转发端口

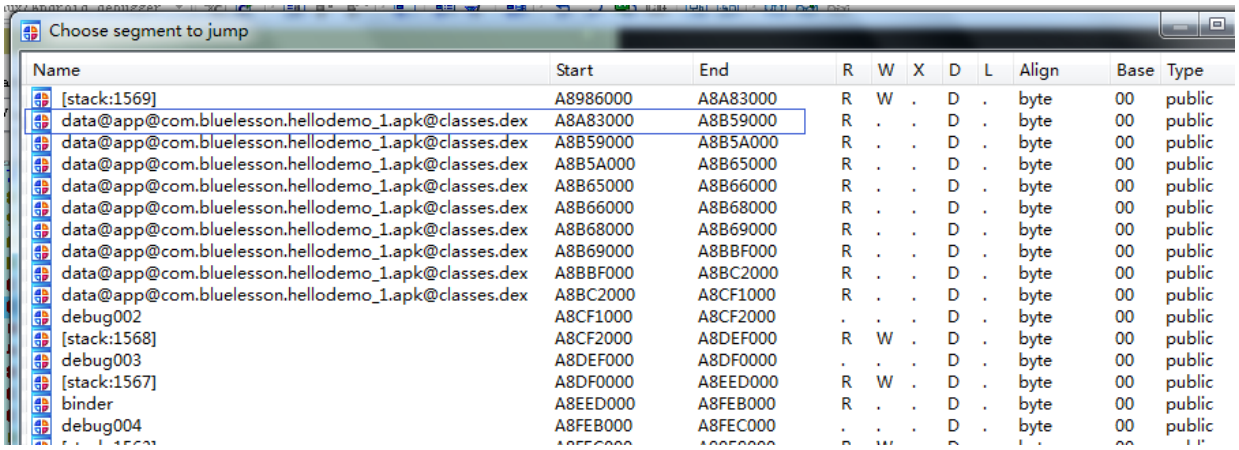
adb forward tcp:23946 tcp:23946

4.IDA附加调试
　注意程序位数：32位　如果不对应 获取不到进程模块

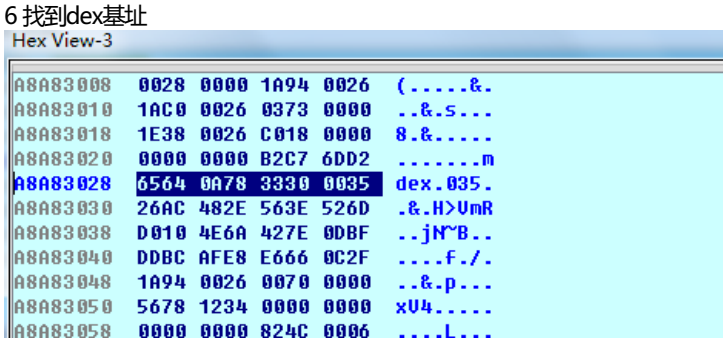




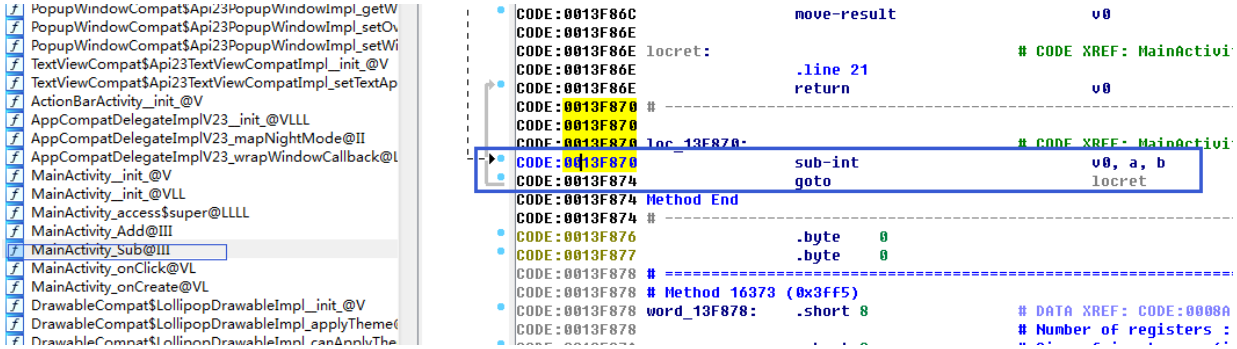
5.ctrl+s获取模块信息，获得基址



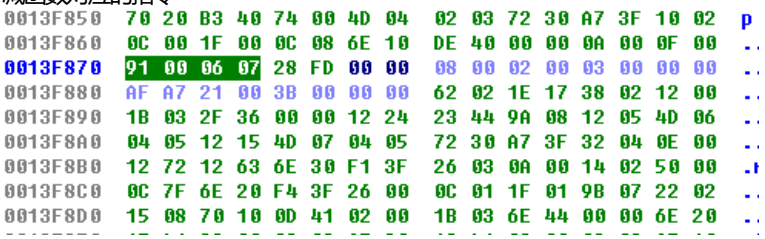
6 找到dex基址

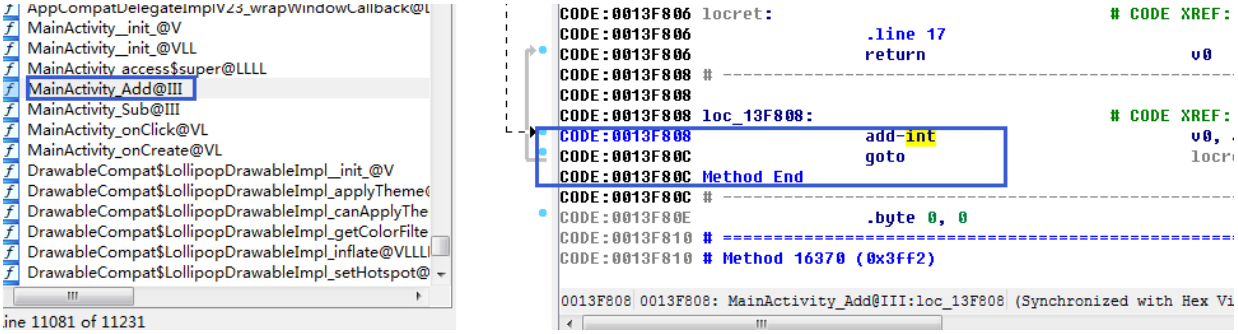


用另一个IDA找到函数偏移地址

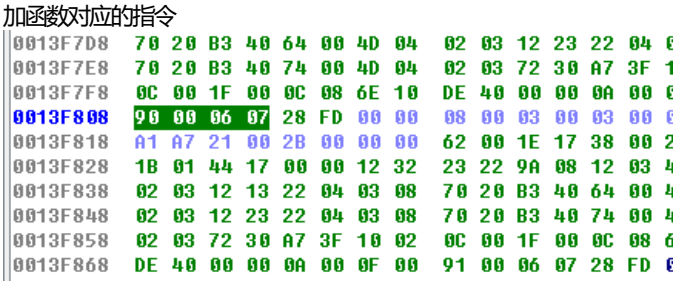


减函数对应的指令



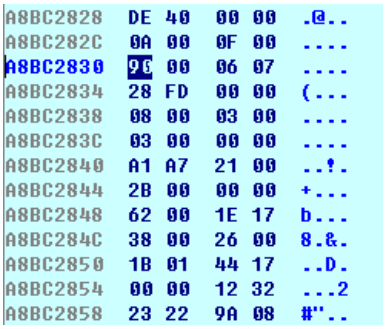


加函数对应的指令



根据函数偏移，在内存中计算函数实际地址
A8A83028+0013F808=A8BC2830

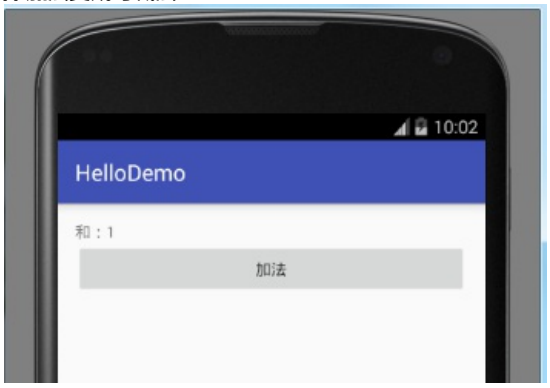
G跳转到内存地址



F2将90改为91 再F2保存

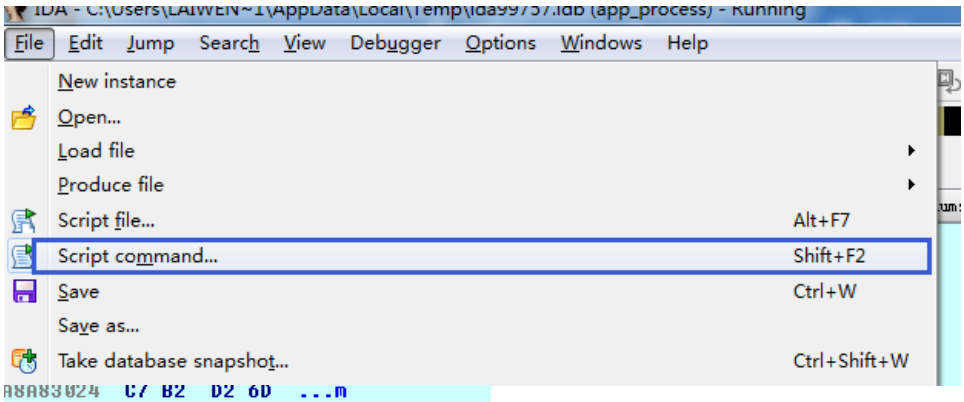
```
A8BC282C  0A 00  0F 00  ....
A8BC2830  91 00  06 07  ....
A8BC2834  28 FD  00 00  (...
A8BC2838  08 00  03 00  ....
A8BC283C  03 00  00 00  ....
A8BC2840  A1 A7  21 00  ..!.
A8BC2844  2B 00  00 00  +...
A8BC2848  62 00  1E 17  b...
```

//加法变成可减法



成功！

下边dump下来

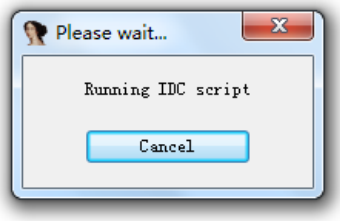



```
A8A83024  C7 B2  D2 6D  ...m
A8A83028  64 65  78 0A  dex.
A8A8302C  30 33  35 00  035.
A8A83030  AC 26  2E 48  .&.H
A8A83034  3E 56  6D 52  >VmR
A8A83038  10 D0  6A 4E  ..jN
A8A8303C  7E 42  BF 0D  ~B..
A8A83040  BC DD  E8 AF  ....
A8A83044  66 E6  2F 0C  f./.
A8A83048  94 1A  26 00  ..&.
A8A8304C  70 00  00 00  p...
A8A83050  78 56  34 12  xV4.
A8A83054  00 00  00 00  ....
A8A83058  00 00  00 00  ....
```

先取出起始地址，还有文件大小4个字节
起始地址：A8A83028
大小：261A94

```
static main(void)

{

    auto fp, begin, end, dexbyte;

    fp = fopen("d:\\dump.dex", "wb");

    begin = 0xA8A83028; //基址

    end = begin + 0x261a94; //大小

    for ( dexbyte = begin; dexbyte < end;     dexbyte ++ )

        fputc(Byte(dexbyte), fp);
```

```
}
in = 0xA8A83028; //基址
 = begin + 0x261a94; //大小
 ( dexbyte = begin; dexbyte < end;     dexbyte ++ )
 fputc(Byte(dexbyte), fp);
```



- dump之后可以使用最新版的baksmali反编译dex文件