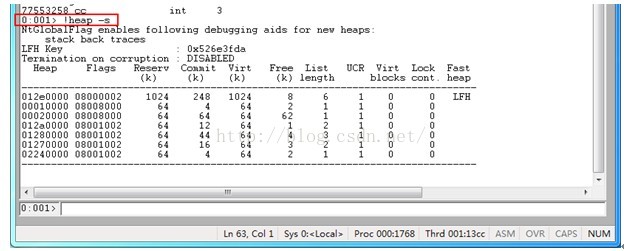
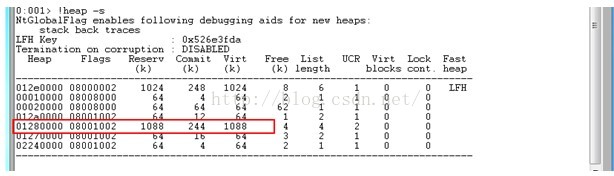
1、开启memoryleak.exe程序，windbg attach到该进程

命令：!heap –s查看当前进程运行的所有堆的情况



2、然后F5让程序运行一段时间或者内存有明显的增加时，break程序，再次通过!heap –s查看当前堆的变化。如下图



通过对比前后两个堆的变化，发现0x012800000该地址的堆增加的很快而其他堆没什么变化。

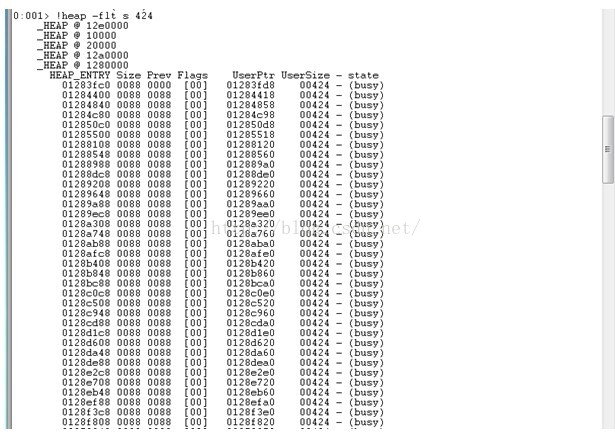
3、定位异常增长的堆



命令：!heap –stat –h 查看对应堆的状态，发下该堆的内存基本被长度为0x424的块占用。

4、在堆中搜索该进程中哪些模块占用0x424长度内存，如下图

命令：!heap –flt s 424



5、通过搜索程序内存中的堆发现长度为424的堆被大量的占用，进一步查看时谁在使用这个地址



找到泄露点了，红色部分的，如果程序对应的符号对应我们可以查看内存泄露点在哪一行

