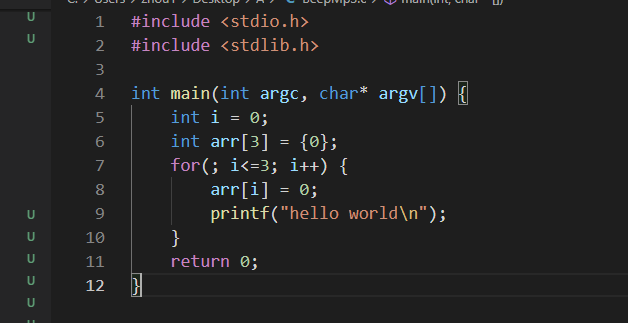
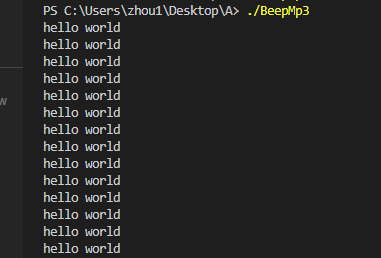
小程序分析心得

一、

首先来看看一个小程序，该程序跑起来会进入无限的循环，一直输出“hello world”，初步分析是arr[3]的内存地址跟变量i的内存地址是一样的，今天我们用反汇编来分析一下arr[3]的内存地址是否跟i的内存地址一样？



上图是我们的一个测试小程序



上图是小程序的运行结果

二、下面我们用gdb反汇编单步调试来分析该程序，下图是我单步调试的汇总结果：

三、通过该图我们可以清晰的看到变量i的内存地址跟arr[3]的地址是一样的；

