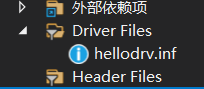
# 课堂笔记

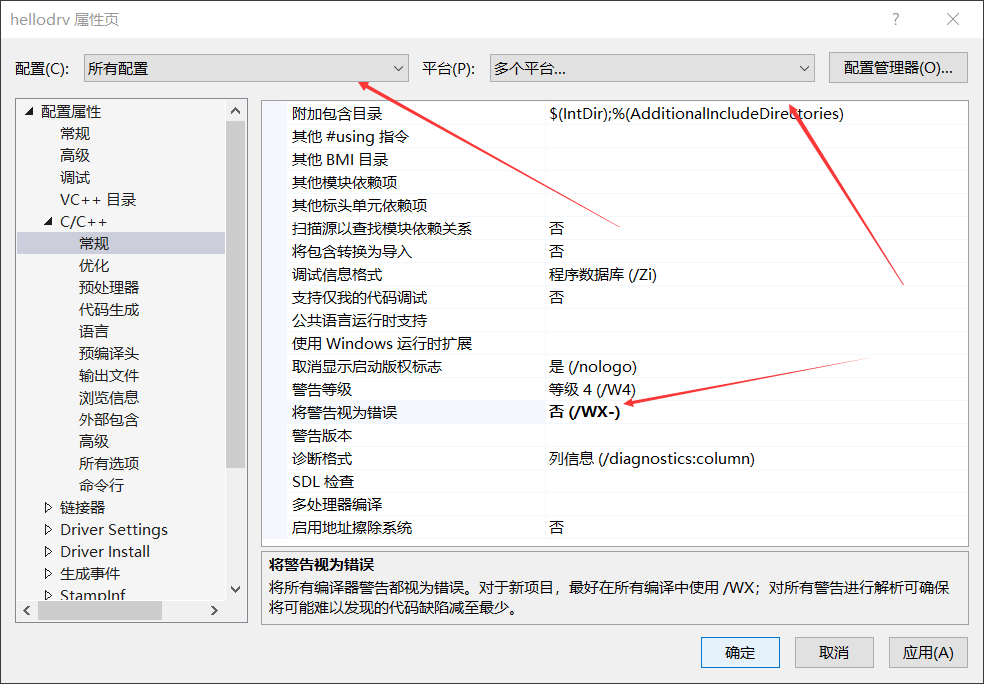
### 1.Helloworld



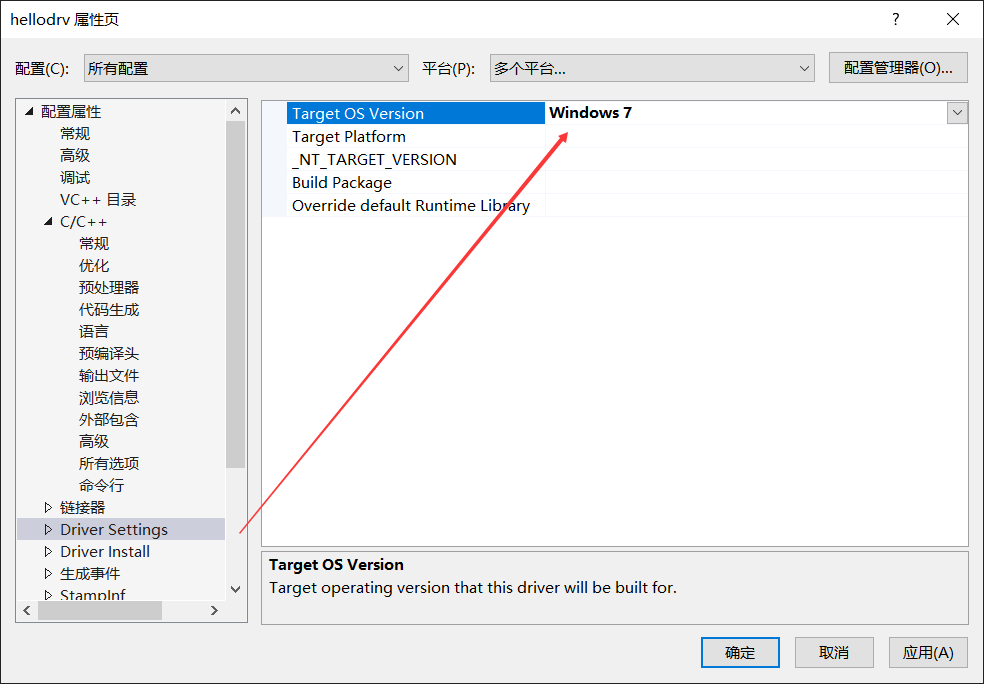
NT驱动，删掉inf文件

创建C源文件

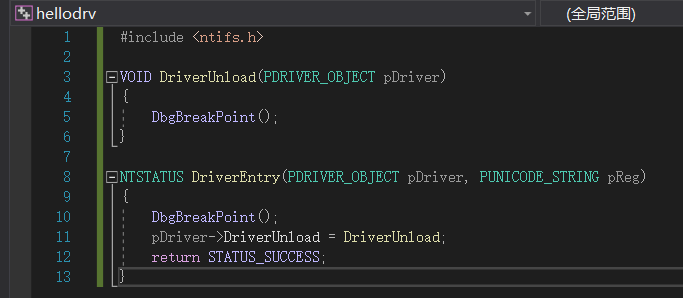
项目属性设置



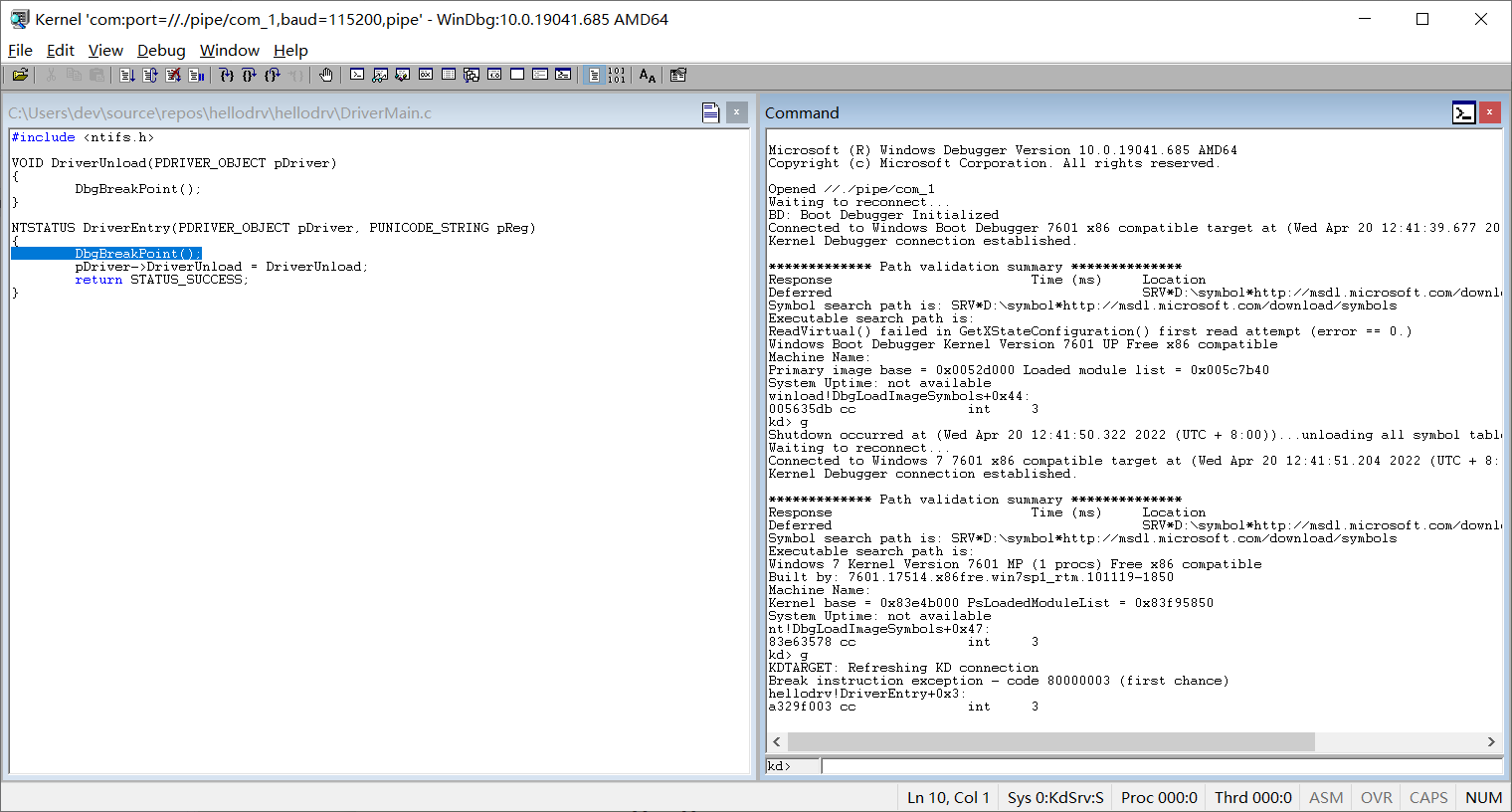
驱动设置，目标OS版本设置为WIN7，兼容XP,WIN7, WIN10, WIN11



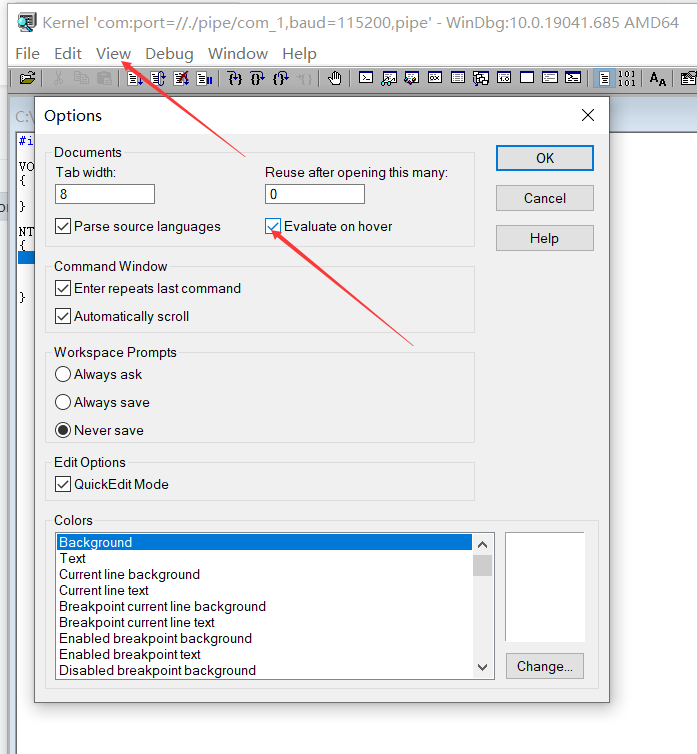
写加载函数，卸载函数



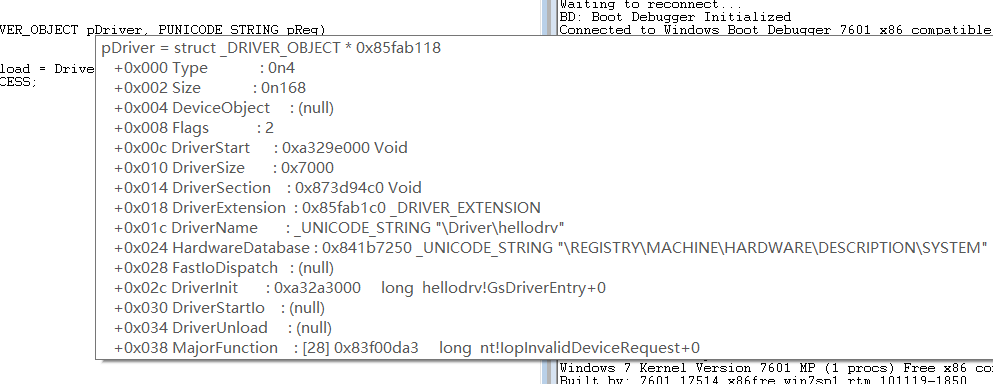
复制到虚拟机运行，在外部windbg断下：



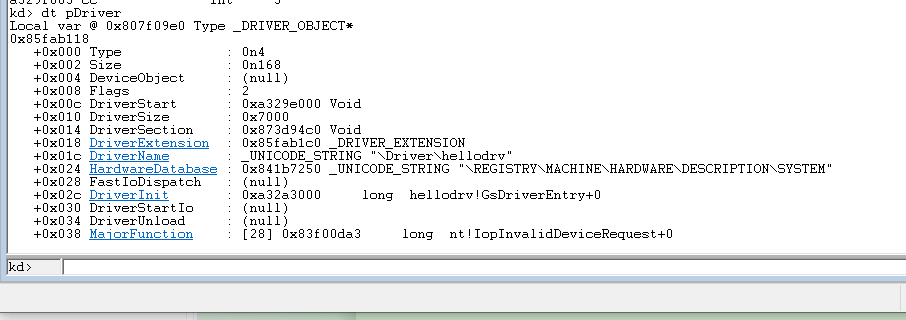
打开下图这个设置：



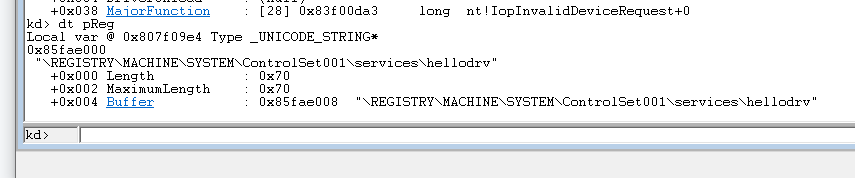
这样就可以把鼠标光标移动到变量上，看到其内部数据：

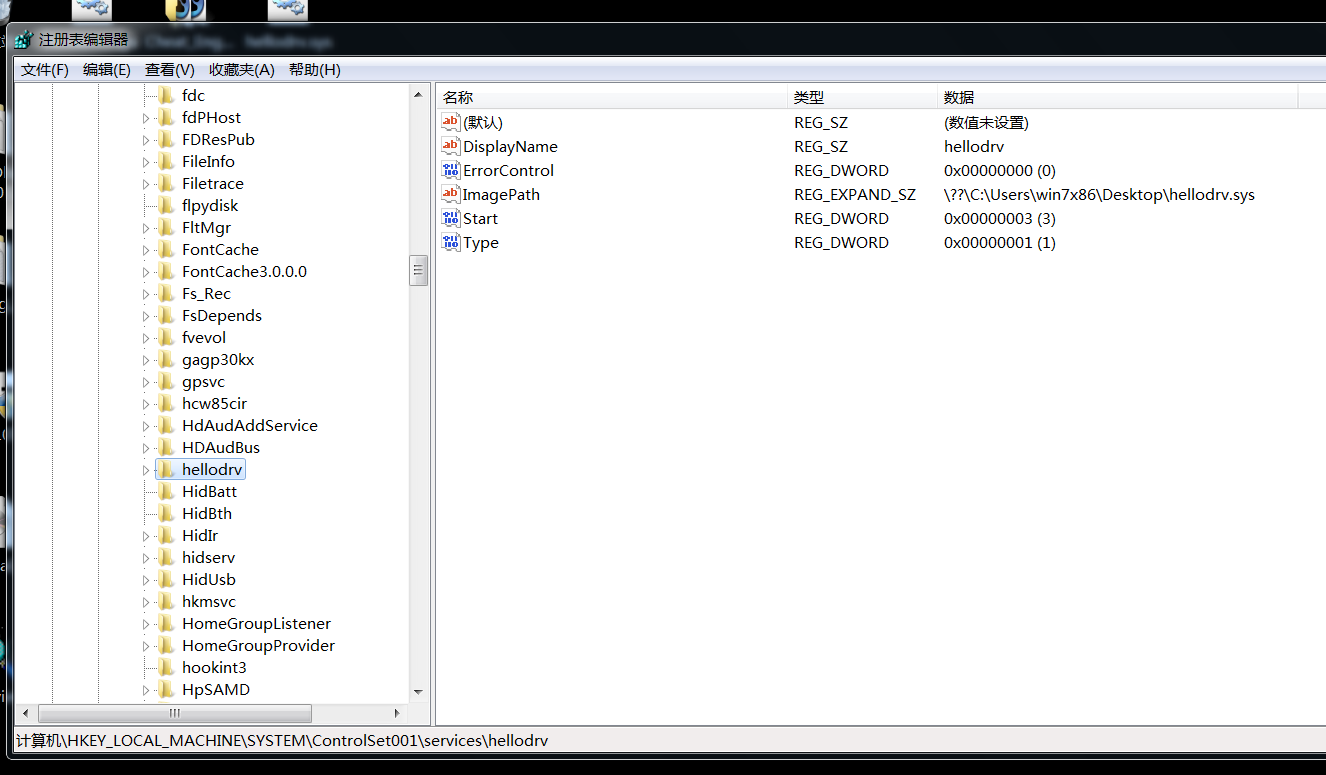


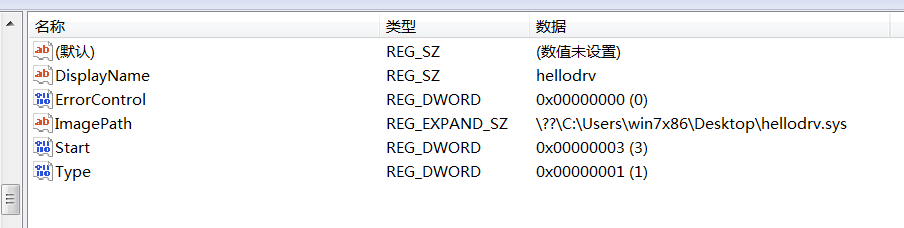
因为有符号，也可以直接dt变量



加载函数第二个参数是驱动安装路径，可以在注册表中找到：



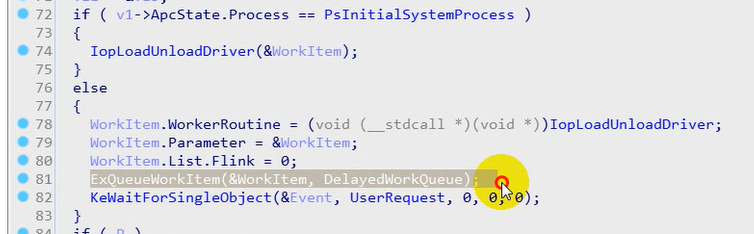




ImagePath是驱动路径

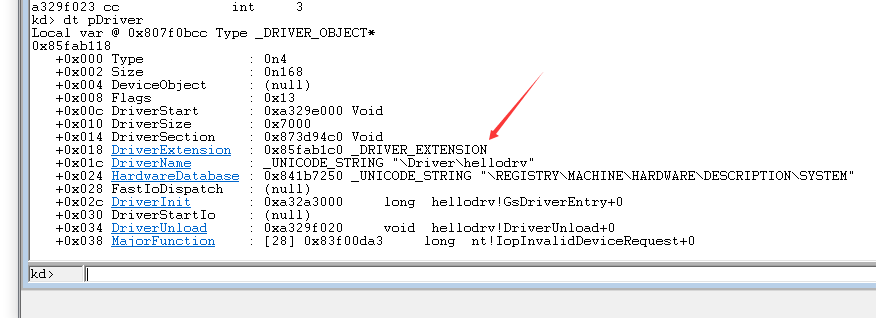
Start 是启动时机，3表示手动启动。

简单分析一下 NtLoadDriver

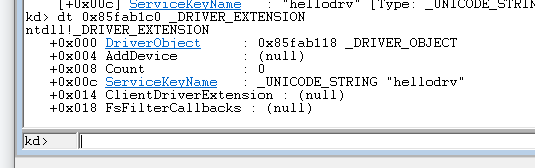


可以看到加载驱动是由system的线程完成的。

驱动扩展



里面有个servicekeyname



这个就是驱动服务名

### 2.驱动对抗历史

视频最后10分钟，还没回看，忙死了操

# 作业

### 1.A驱动打印地址，B驱动读，看看能不能读出来

是可以的。

### 2.看书《Windows内核安全与驱动开发》