

计算机二级考试C 基础:句柄计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/645/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E4_c97_645575.htm 1.句柄是什么？

在windows中，句柄是和对象一一对应的32位无符号整数值。对象可以映射到唯一的句柄，句柄也可以映射到唯一的对象。

2.为什么我们需要句柄？更准确地说，是windows需要句柄。windows需要向程序员提供必要地编程接口，在这些接口中，允许程序员访问、创建和销毁对象。但是，出于封装地考虑，windows并不想向程序员返回指针。指针包含了太多的信息。首先指针给出了对象存储的确切位置；其次，要操作一个指针，程序员必须知道指针所指对象的内部结构特征，也即，windows必须向程序员暴露相应的数据结构，而这些数据结构也许是操作系统想向程序员隐藏的。如果说COM技术向用户隐藏了数据，只暴露了接口并只允许按接口定义的方法操作数据的话，句柄这种方式则允许你按自己的方式直接操作数据，但windows又不向你直接暴露数据。直接操作数据是程序员需要的，不暴露数据是windows所需要的，句柄封装方式实现了各取所需。

3.句柄如何与对象映射？封装背后，必须有一个地方可以实现解码，以实现句柄和对象的相互转换。在windows中，存在两种映射方式：

a. 全等映射。也即，句柄本身就是一个指针。映射在这里只是类型转换而已。这种情况有，进程实例句柄或模块句柄，以及资源句柄等等。

b. 基于表格的映射。这是对象指针与句柄之间最普通的映射机制。操作系统创建表格，并保存所有要考虑的对象。需要创建新对象时，要先在表格中找到空入口，然后把表示对象

的数据添入其中。当对象被删除时，它的数据成员和其在表中的入口被释放。

4.句柄的定义和实现

我们以GDI对象为例进行讨论。创建了GDI对象，就会得到该对象的句柄。句柄的对象可能是HBRUSH、HPEN、HFONT或HDC中的一种，这依赖于你创建的GDI对象类型。但是最普通的GDI对象类型是HGDIOBJ。HGDIOBJ被定义成空指针。HPEN的实际编译类型定义随编译时间宏STRICT的不同而不同。如果STRICT已经被定义了，HPEN是这样的：

```
struct HPEN__ {int unused};  
typedef struct HPEN__ * HPEN.
```

如果STRICT没有定义，HPEN是这样定义的：

```
typedef void *HANDLE.  
typedef HANDLE  
HPEN.
```

上面这段代码是一个注重细节的程序员最接近句柄的地方，因此我们重点分析一下。这里有一点点技巧。如果定义了STRICT宏，HPEN是指向有单个未使用字段的结构的指针，否则HPEN是空指针。C/C 编译器允许把任何类型的指针作为空指针传递，反之则不可以。两个不同类型的非空指针是互不兼容的。在 STRICT版本中，编译对GDI对象句柄的不正确混用将给出警告，对于非GDI句柄，如HWND、HMENU的不正确混用也会给出警告，从而使程序在编译器得到更STRICT的检查。接下来的分析可能不那么令你感兴趣，但它更深刻地揭示了句柄。对GDI句柄来说，尽管windows头文件把它定义成指针，但如果你仔细检查这些句柄的值，它根本就不像指针，这也是为什么我说它只是一个32位无符整数值的原因。对句柄就是指针的情况，这句话也仍然适用。让我们随意地生成一些句柄，比如你用GetStockObject()以得到一些句柄，你会发现，它们的值总在区间0x01900011到0xba040389。前者指向用户区中的未分配

的无效区域，后者指向内核地址空间。另外你可能发现，两个句柄之间的值可能只差数值1，这也说明GDI句柄不是指针。和多数人想象的不一样，句柄也不是一个单纯的索引值。对GDI对象句柄来说，GDI句柄由8位、1位堆对象标记（表明对象是否创建在堆中）、7位对象类型信息和 高4位为0的16位索引组成，如图：

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-------|---|---|---|---|---|---|-------|---|---|---|---|---|---|---|---|---|-----|---|---|---|---|---|---|--|---|
| 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | 8 |
| | | | | | | | | | | | | | | | | 位引用计数 | | | | | | | | | | | | | | | | | 堆 | | 对象类型7 | | | | | | | 16位索引 | | | | | | | | | | 标 记 | | | | | | | | |

在这里你可以看到，对GDI来说，它只使用了16位作为索引。这意味着一个进程最多只可以创建小于64K个句柄，实际上受其他一些限制，整个windwos系统中大概可以容纳约 16384(0x4000)个GDI对象。编辑特别推荐: 送给正在学习C 朋友的50条建议 C 笔试考前练习 计算机等级考试二级C 上机考试指导 100Test 下载频道 开通，各类考试题目直接下载。详细请访问 www.100test.com