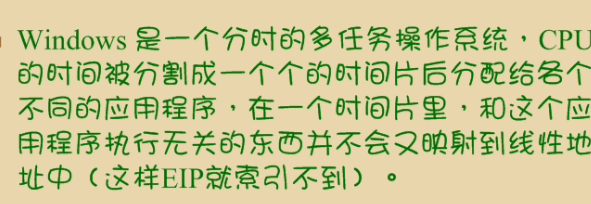
**基础篇**

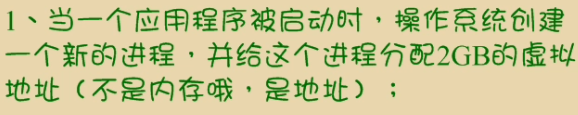
**第二讲：一些必备知识**

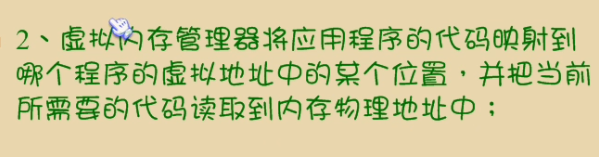
能力是锻炼出来的，思维是锻炼出来的，知识是查出来的

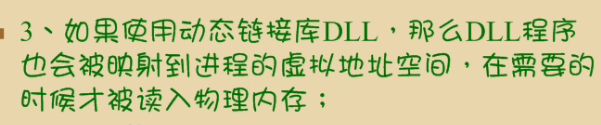
**第五讲：windows保护模式**

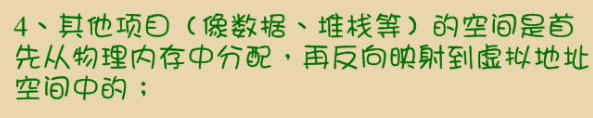


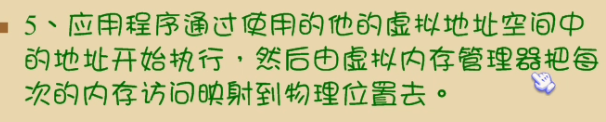
**虚拟内存的实现方法和过程 ：**

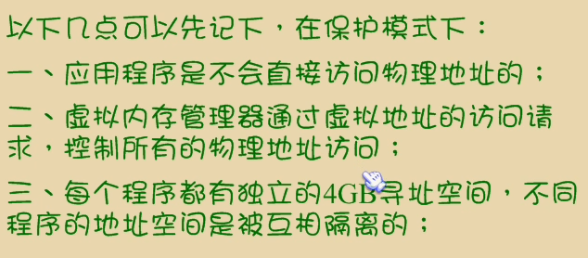


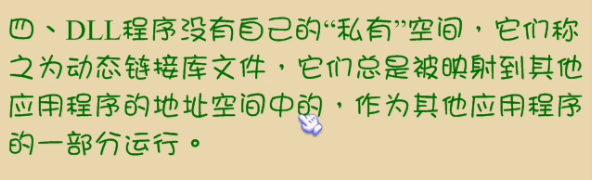


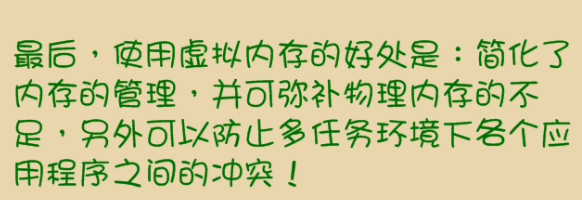












**第六讲:初步认识PE格式**

**PE:portable Executable(可移植执行体)**

**所有的win32执行体都使用pe格式（除了VxD和16位dll）**

**PE文件使用平面地址空间，所有代码和数据合并在一起**

**文件分为不同区块（section，区段，节），含有代码和数据**

**各个区块按页边界对齐**

**PE文件在磁盘上的数据结构与内存的结构式一致的**

1. **入口点：（Entry Point）**

**程序在执行时的第一行代码地址应该就是这个值**

1. **文件偏移地址（File Offset）**

**文件在磁盘上时，各数据的地址称为文件的偏移地址**

1. **虚拟地址（Virtual Address ，VA）🡸🡺内存偏移地址（Memory Offset）**

**段选择子（在cs中）：虚拟地址（因为pe映射原理）**

**基地址（ImageBase）：文件执行时被映射到制定内存地址中。**

**Vc建的基地址是00400000h，dll基地址：10000000h**

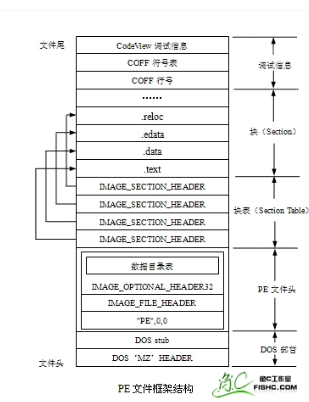
**LoadPE**

**系统篇**

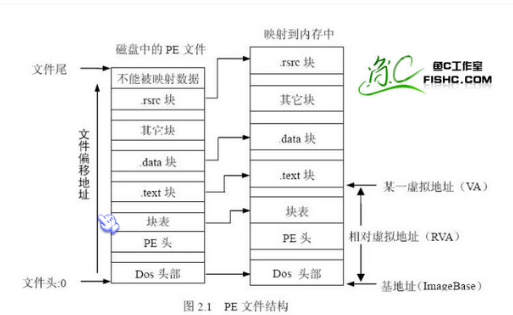
**研究PE文件可以加深对操作系统的了解。**

**第一讲：PE结构详解1**

**PE文件的数据结构及运行机理，也有助于软件安全**

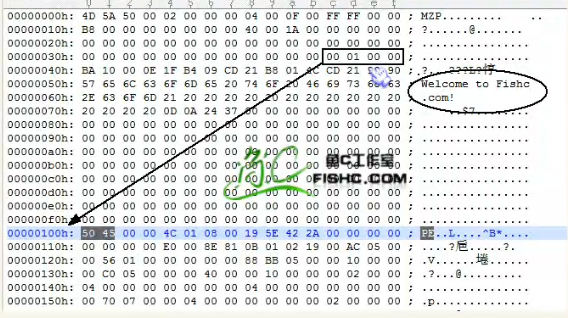






**获取句柄：相当于获取pe的基地址，相当于获取可执行文件的头部。**

**第二讲：PE结构详解2**



**Cpu类型：**

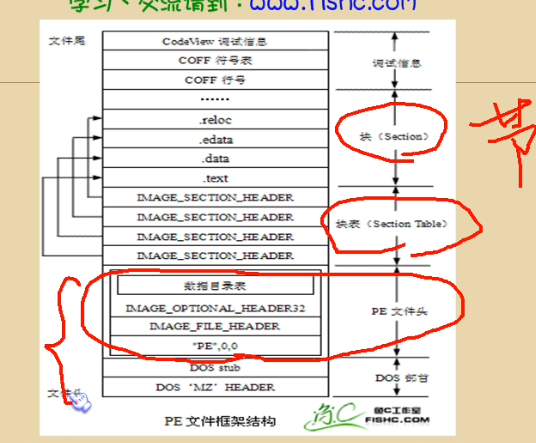
**IMAGE\_FILE\_MACHINE\_I386**

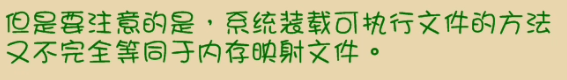
**Ox014C:🡸🡺X86机器**

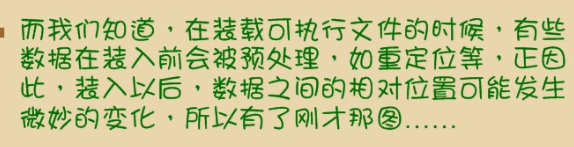
**Ox0200🡸🡺INTEL ITANIUM**

**Ox8664 🡸🡺X64机器**

**第四讲：**







**第五讲**