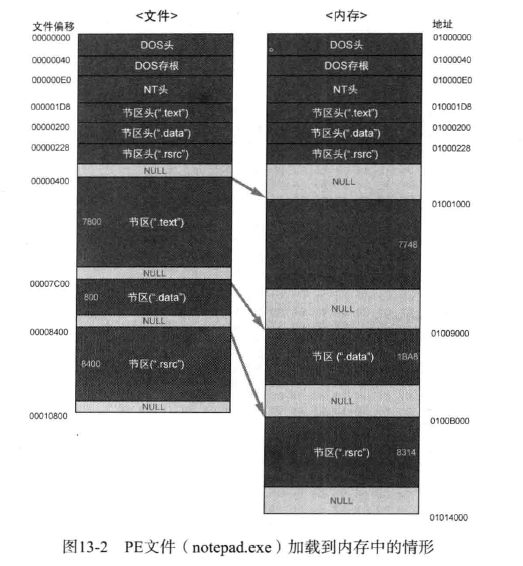
目录

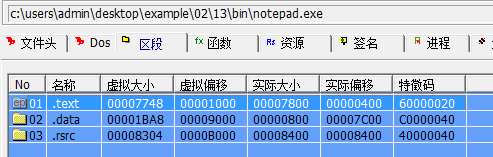
[13. PE文件结构 1](#_Toc484072726)

[13.1 PE文件格式 1](#_Toc484072727)

# 13. PE文件结构

两图为notepad.exe的文件结构





名词解释：

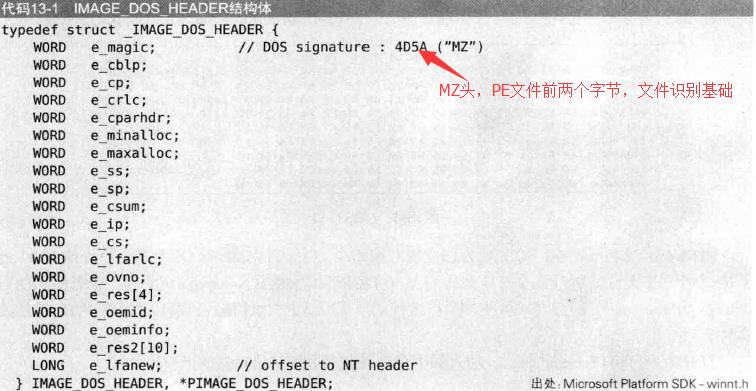
VA：进程虚拟内存的绝对地址

RVA：相对虚拟地址，从基准位置ImageBase开始的相对地址

VA = RVA + ImageBase

## 13.1 PE头结构

### 13.1.1 DOS头



DOS占用40个字节

### 13.1.2 虚拟地址和文件偏移地址的换算（RVA⬄RAW）



1. 查找RVA所在的区段

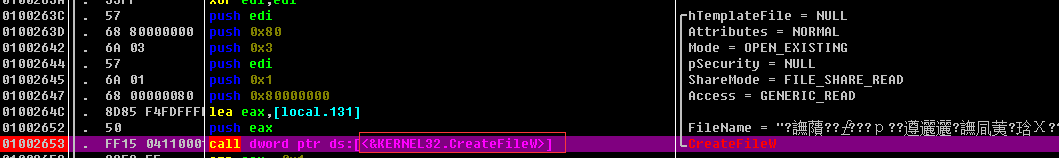
2. 利用公式计算RAW（文件偏移）

RAW – PointerToRawData = RVA – VirtualAddress（虚拟地址相对于虚拟偏移的位置等于文件偏移相当于当前节的文件偏移的位置）。

示例：RVA = 5000，求文件偏移

解： RVA = 5000，在1000和 9000之间，在text节，RAW = 5000 – 1000 + 400 = 4400.

## 13.2 IAT（导入地址表）

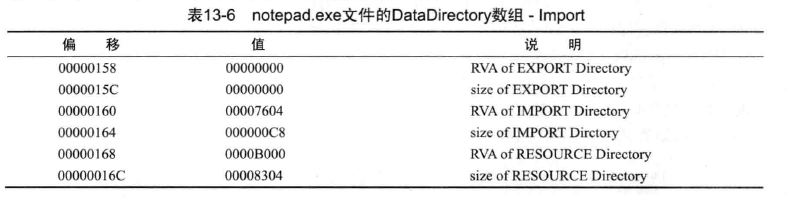


## 13.3 notepad.exe 练习

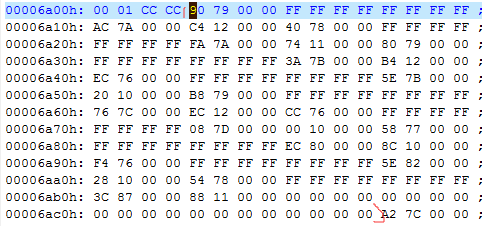
1. 从文件PE体中查找IMAGE\_OPTIONAL\_HEADER32.DataDirectory[1].

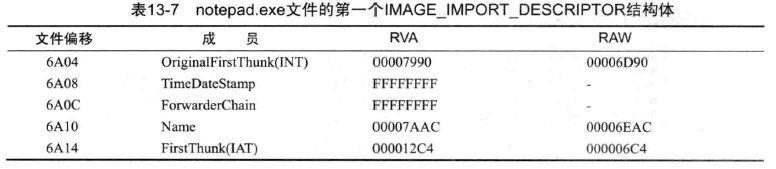
VirtualAddress（结构体数组的起始地址）。





第一个字节是RVA，第二个字节是字节数。RVA = 00007604，size = 0xc8 。RAW = RVA – 1000 + 400（详见之前的公式） = 6A04





Name是导入函数的名称。 RVA ：7AAC =》RAW ：6EAC

