RVA与FOV的转换

概念

- ImageBase: 模块基址.程序一开始的地址.
- VA: 全名virtualAddress 虚拟地址. 就是内存中虚拟地址. 例如 0x00401000
- RVA: RVA就是相对虚拟偏移. 就是偏移地址. 例如 0x1000. 虚拟地址0x00401000的RVA就是0x1000. RVA = 虚拟地址-ImageBase
- FOA: 文件偏移. 就是文件中所在的地址.

内存转文件

设内存地址为x

计算RVA

`RVA = x - ImageBase`

寻址FOV

1. 判断RVA属于哪个节/头
    - 如果RVA属于头(DOS+NT)那么不需要进行计算了，因为头在文件中根内存中都是一样展开的，直接从开始位置寻找到RVA个字节即可
    - 如果不在头，就要判断在那个节里面.，判断节开始位置跟结束位置.，我们的RVA在这个值里面
    - 其中节虚拟地址结束位置 就是用节数据对齐后的大小+虚拟地址大小
    - `RVA >= 节.VirtualAddress && RVA < (节.VirtualAddress + 节.SizeofRawData)`
2. 计算差值偏移，虚拟地址距离节数据的开始位置的偏移
    - `差值 = RVA - 节.VirtuallAddress`

计算FOV

`FOA = 差值偏移 + 节.PointToRawData`

文件转内存

同上反过来，设文件地址为x

1. 判断是否是头上，是则 `FOV = RVA`
2. 不在头上，则遍历节表 `x >= 节.PointerToRawData && x < 节.PointerToRawData + 节.SizeofRawData` 计算 `差值偏移 = x - 节.PointerToRawData(节数据在文件中开始的位置)`
3. 计算 `RVA = 差值偏移 + 节.VirtuallAddress(节数据在内存中展开的位置)`
4. 计算 `VA = RVA + ImageBase`