进程遍历和窗口遍历

遍历进程

`CreateToolhelp32Snapshot` 获取信息的快照

然后通过**Tool Help Functions**系列函数获取相关信息

遍历窗口

无序

`EnumWindows` 遍历窗口，执行用户定义的回调函数

`GetWindowThreadProcessID` 通过窗口句柄获取所在线程、进程ID

Z-Order

`GetNextWindow` 以**Z-Order**遍历窗口

一般先获取最里面的窗口，然后向外遍历。最里面的窗口为桌面 `GetDesktopWindow`

进程间的内存操作

`ReadProcessMemory` 读进程的内存

`WriteProcessMemory` 写进程的内存

`OpenProcess` 打开进程，获取进程句柄

`FindWindow` 获取窗口句柄

`VirtualProtectEx` 跨进程修改进程访问权限