逆向作业：  
1.列举3种可以用于调试器检测的Windows API。

GetDlgItemTextA()、strcmp()、ShellExecute()等。

2.列举3种可以用于调试器检测的Windows数据结构。   
哈希表、递归、链表等。

3.简述用软件断点识别调试器的原理。  
① 软件断点：X86系统中为中断指令INT 3。当程序执行到 INT 3 时，引发软件中断。  
操作系统的 INT 3 中断处理器会寻找注册在该进程上的调试处理程序，因而调试器就有了上下其手的机会。  
② 硬件断点：X86系统提供8个调试寄存器（DR0~DR7）和2个MSR用于硬件调试。  
4.列举3种可以干扰调试器的方法。  
① 花指令：隐藏指令，干扰分析。  
② 动态加/解密代码：干扰分析。  
③ 异常处理机制：加大跟踪难度。  
5.花指令是什么？有什么作用？  
花指令：故意将错误的机器指令放在了错误的位置。  
作用：设计者希望使破解者反汇编的时候出错。  
6.简述手动脱壳的常用技术。  
单步跟踪法、ESP定律法、内存镜像法、一步到达OEP法、最后一次异常法、模拟跟踪法、“SFX”法。  
7.Stolen code是什么技术？如何解决？  
Stolen code：软件脱壳中被修改的代码。  
解决：到达OEP后补上stolen code里的代码。  
8.SEH是什么？有什么作用？   
SEH：Structured Exception Handling，结构化异常处理。  
作用：Windows提供给程序设计者强有力的处理程序异常的武器。