南開大學

恶意代码分析与防治技术课程实验报告

实验二

学　　院　网络空间安全学院

专　　业　信息安全、法学

学　　号　2113203

姓　　名　付政烨

班　　级　信安法班

一、实验目的

该实验旨在配置一个虚拟机环境，用于进行恶意软件分析。

二、实验原理

1. 配置病毒分析虚拟机

   VMware 虚拟机或其它的虚拟机软件

   Windows XP 操作系统

2. 虚拟机中安装静态分析工具

   string.exe、PEView、dependency walker、IDA 等工具

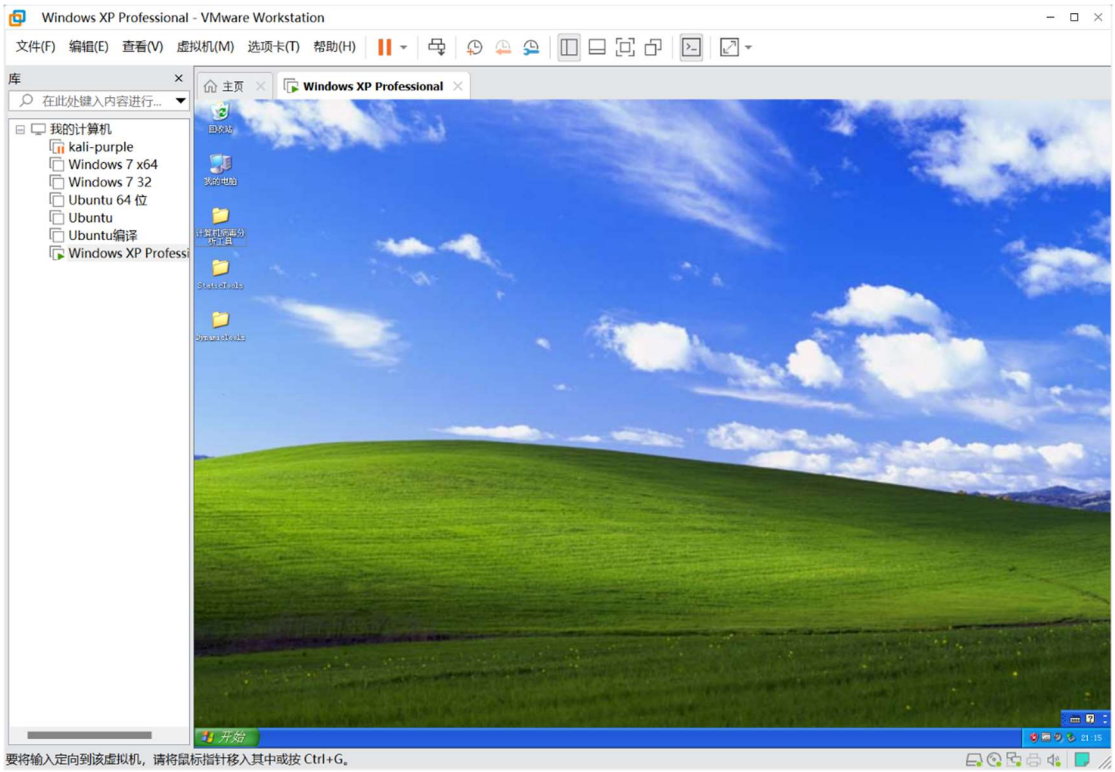
3. 虚拟机中安装动态分析工具

   预习教材 chapter 3: basic dynamic analysis

   OllyDBG、Process Monitor、 Process Explorer、 RegShot、WireShark 等工具

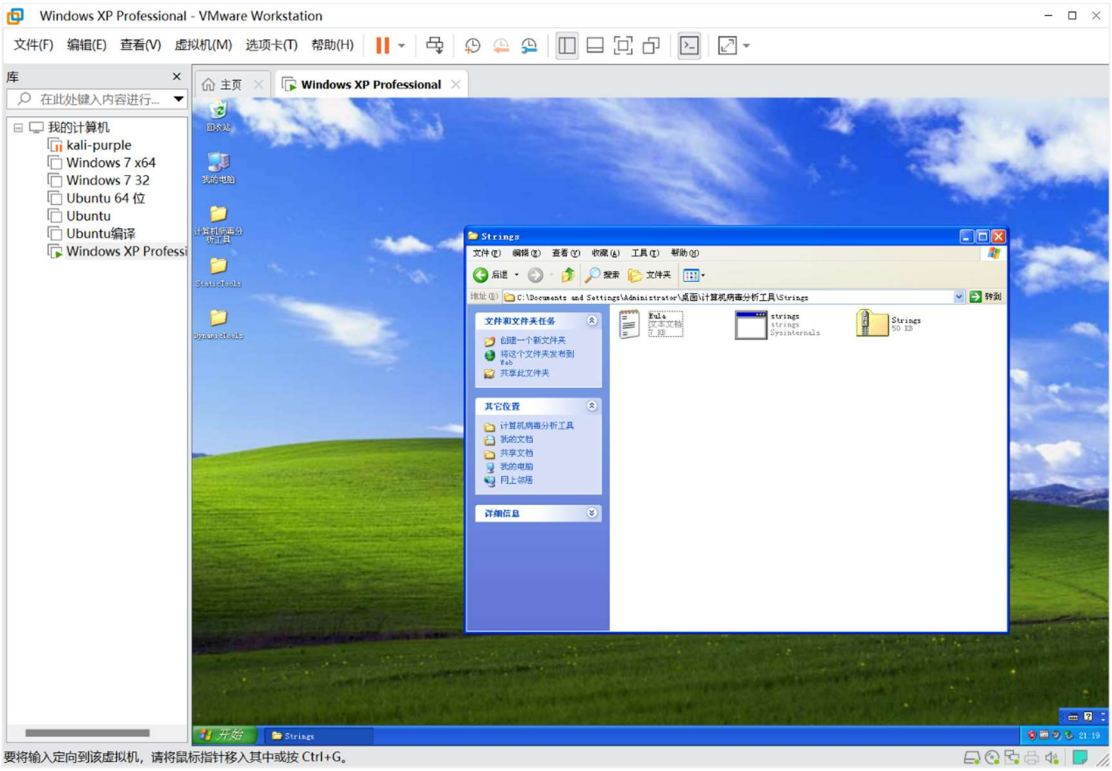
三、实验过程

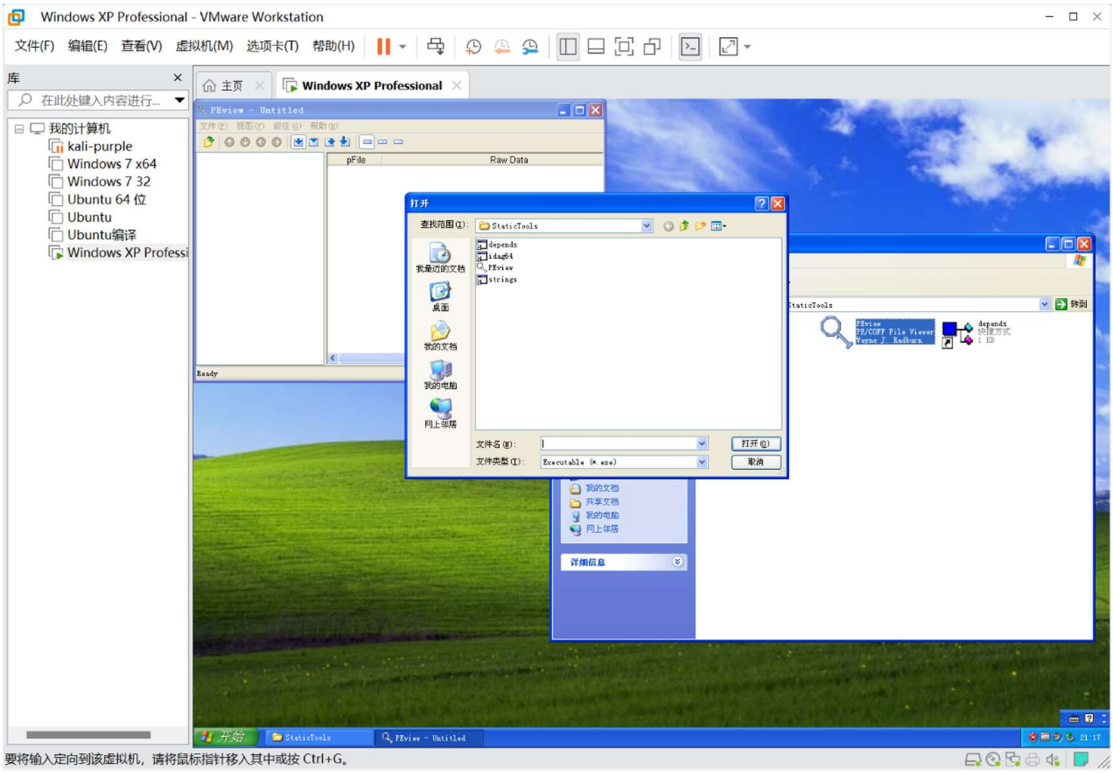
1. 虚拟机的安装和配置过程

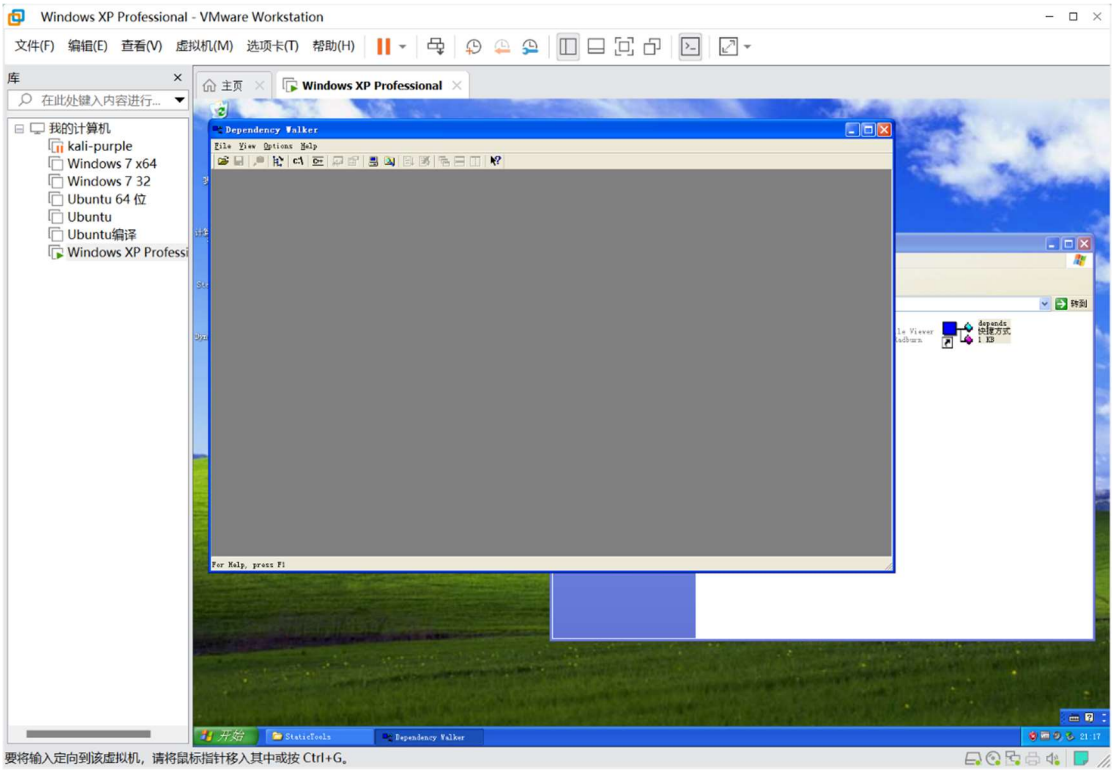


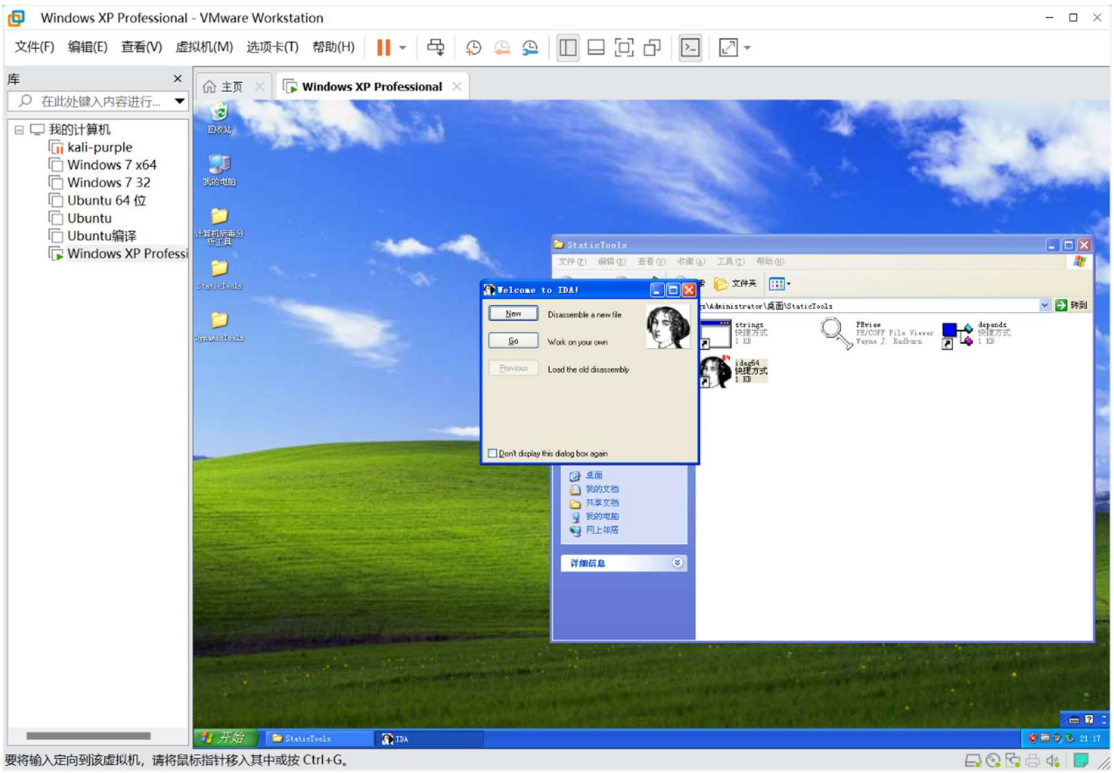
2. 静态分析工具的功能和安装过程

静态分析工具包括：string.exe、PEView、dependency walker、IDA 等工具









1) string.exe：

功能：string.exe 是一个命令行工具，用于查找可执行文件中的 ASCII 和 Unicode 字符串。

用途：它常用于静态分析，以帮助分析人员识别恶意软件中可能包含的关键字符串，如命令、URL、文件名等。

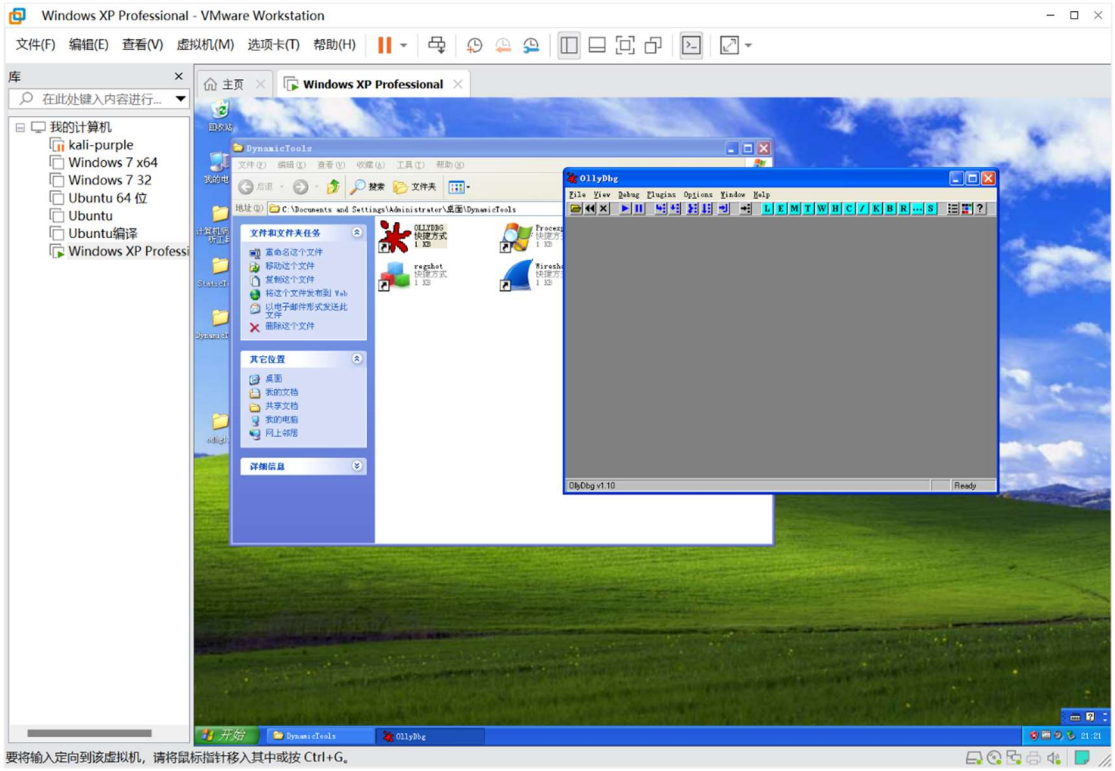
2) PEView：
功能：PEView 用于查看和分析可执行文件（PE 文件格式）的结构和属性。
用途：它提供了一个图形界面，允许用户查看 PE 文件的头部、节表、导入和导出函数、资源等信息，有助于分析程序的内部结构。

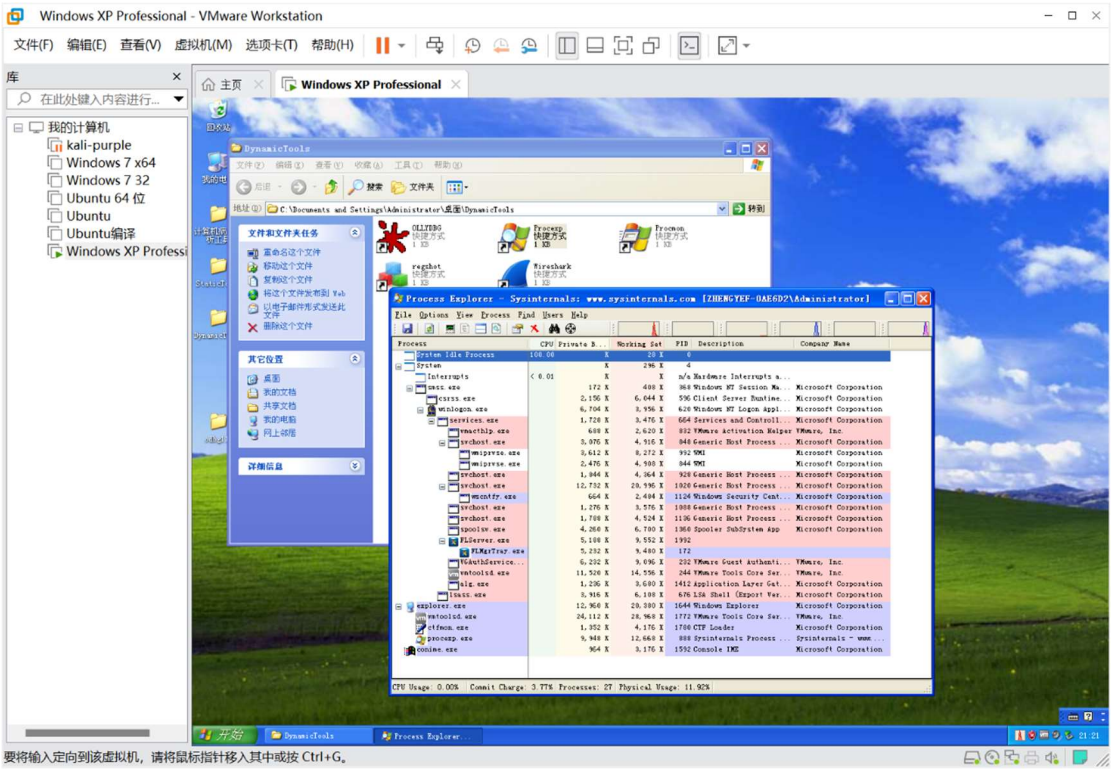
3) Dependency Walker：
功能：Dependency Walker 用于查看可执行文件的依赖关系，包括动态链接库（DLL）和函数调用。
用途：这个工具帮助分析人员了解一个程序运行所需的其他组件，如库文件，以及识别潜在的问题或安全漏洞。

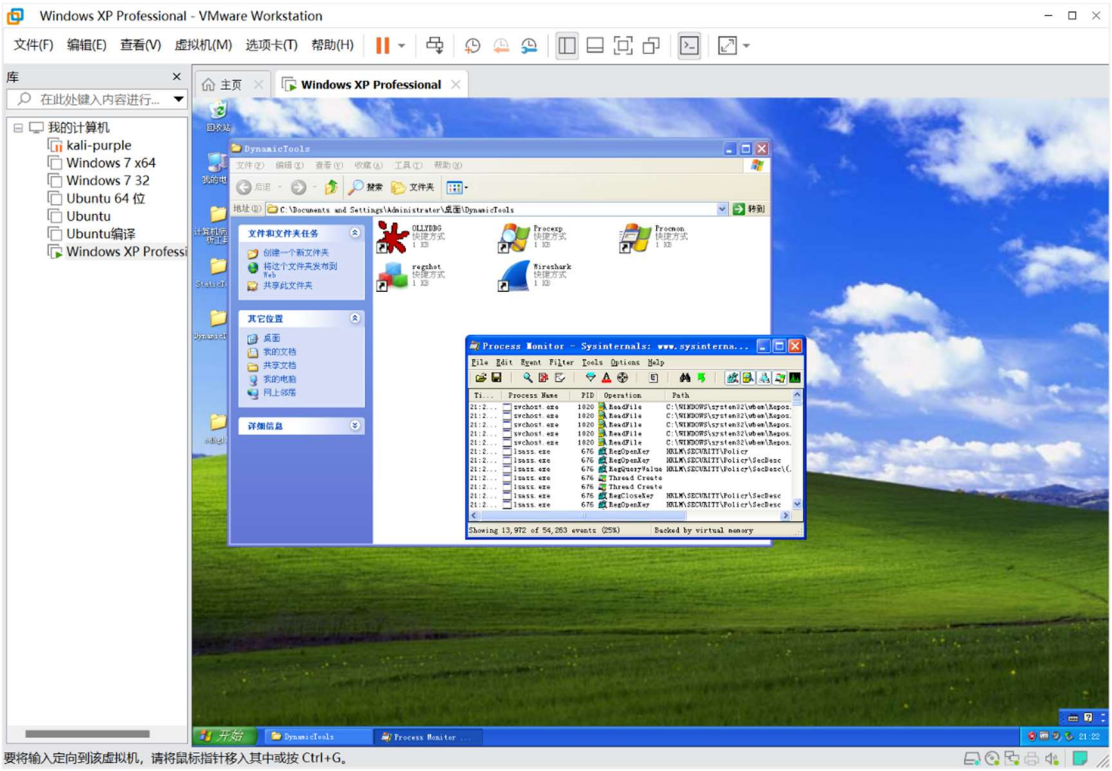
4) IDA：
功能：IDA 是一个高级的反汇编工具，用于分析可执行文件的汇编代码。
用途：IDA 允许分析人员反汇编二进制文件，并查看程序的汇编代码、函数结构、控制流程等。它对于逆向工程和深入理解程序逻辑非常有用。

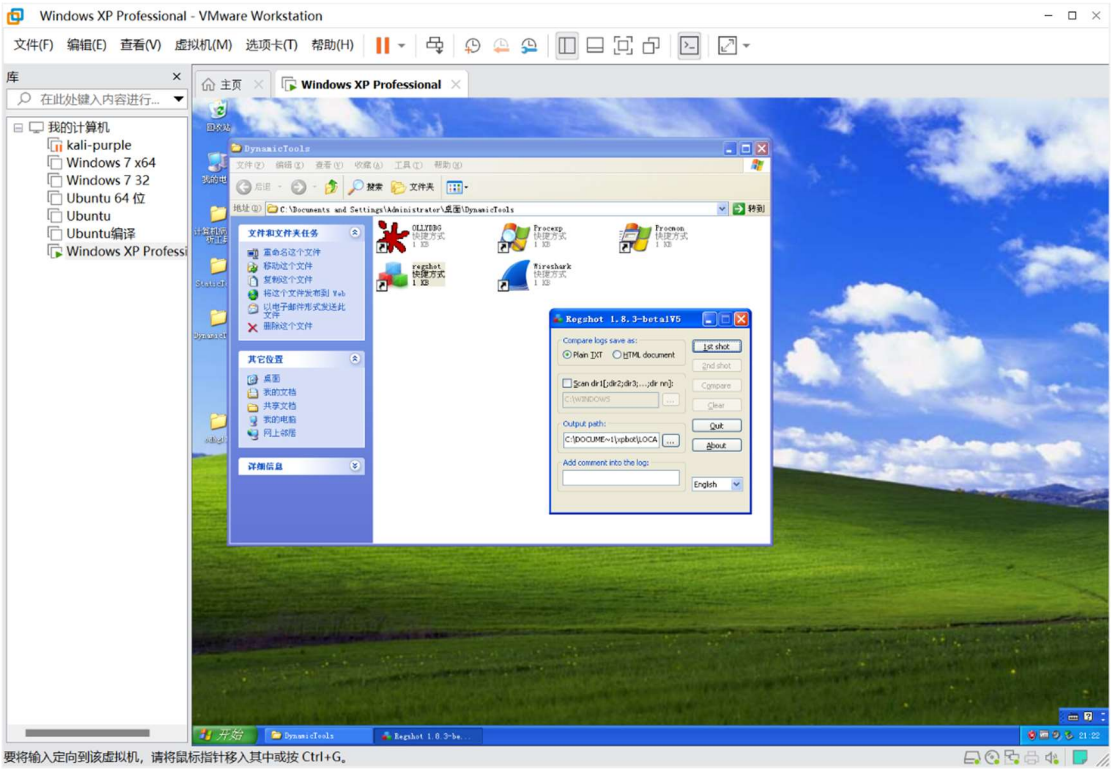
3. 动态分析工具的功能和安装过程

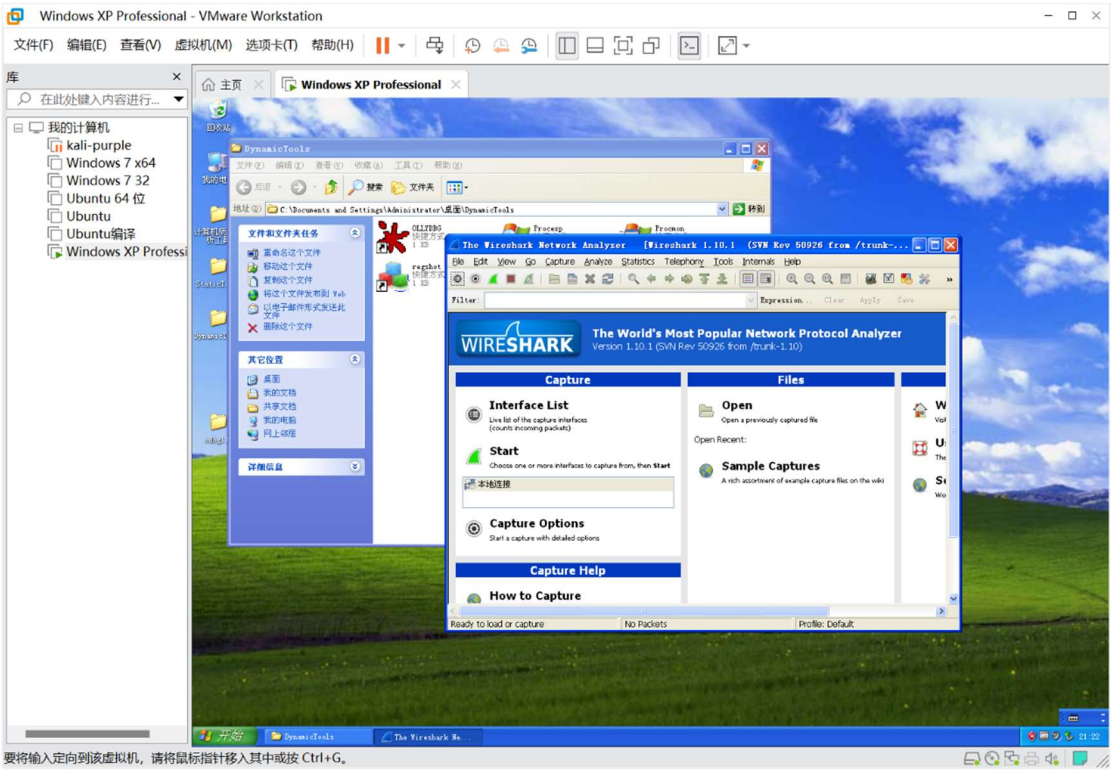
动态分析工具包括：OllyDBG、Process Monitor、Process Explorer、RegShot、WireShark 等工具




Windows XP Professional - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内容进行...
我的计算机
kali-purple
Windows 7 x64
Windows 7 32
Ubuntu 64 位
Ubuntu
Ubuntu编译
Windows XP Professi
主页
Windows XP Professional
Process Explorer - Sysinternals: www.sysinternals.com [ZHENGYEF-0AE6D2\Administrator]
要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。


Windows XP Professional - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内容进行...
我的计算机
kali-purple
Windows 7 x64
Windows 7 32
Ubuntu 64 位
Ubuntu
Ubuntu编译
Windows XP Professi
主页
Windows XP Professional
Process Monitor - Sysinternals: www.sysinterna...
要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。





1) OllyDBG：

功能： OllyDBG 是一个 Windows 下的动态分析工具，用于反汇编和调试可执行文件。它允许研究程序的运行时行为，查看寄存器、内存、堆栈等信息。

用途： 用于分析和调试程序的行为，查看汇编代码，断点设置，寻找漏洞和恶意行为。

2) Process Monitor：

功能： Process Monitor 用于监视和记录 Windows 系统上发生的文件系统、注册表和进程活动。它可以捕获系统事件和详细信息。

用途： 用于跟踪程序的文件和注册表操作，查看应用程序的活动，以及识别潜在的问题或恶意行为。

3) Process Explorer：

功能： Process Explorer 是任务管理器的高级替代品，提供了更多关于运行进程的信息，包括打开的文件、线程、性能数据等。

用途： 用于查看系统中运行的进程的详细信息，包括它们的关系、资源占用情况等。

4) RegShot：

功能： RegShot 用于比较系统注册表的快照，以查看程序运行时对注册表的更改。

用途： 用于检测程序或恶意软件尝试修改系统配置的注册表项。通过比较注册表快照，可以查看何时和如何进行了更改。

5) Wireshark：

功能： Wireshark 是一个网络协议分析器，用于捕获和分析网络流量。它支持多种协议，并提供详细的网络数据包信息。

用途： 用于监视和分析网络通信，识别潜在的网络问题、攻击或恶意活动。可用于网络安全审查和故障排除。

四、实验结论及心得体会

这个实验为我提供了深入了解恶意软件分析的宝贵机会。通过配置虚拟机环境，我学会了如何创建一个安全的隔离区域，以防止恶意软件对主机系统的影响。静态分析工具让我能够查看二进制文件的内部结构和依赖关系，而动态分析工具则使我能够监视程序在运行时的行为。这些工具的使用帮助我更好地理解恶意软件的工作方式，包括文件、注册表和网络操作。