南開大學

恶意代码分析与防治技术课程实验报告

实验二：虚拟机及工具安装

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2213041

姓　　名　李雅帆

班　　级　信安班

一、实验目的

配置一个虚拟机，以隔离病毒环境与主机，保证虚拟机在进行病毒分析的时候不会与主机交互，在物理上避免感染主机。

二、实验原理

1.在相关的虚拟机上配置各种应用程序，同时由于 win11 操作系统与其他 windows 操作系统之间具有向下兼容的功能，因此我们可以在主机的 win11 操作系统上先对所配置的软件验证其功能，之后再在相关的虚拟机上复制相关的应用程序验证功能，正常来说都可以很好的使用。

2. 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

3.虚拟机中安装静态分析工具

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

4.虚拟机中安装动态分析工具

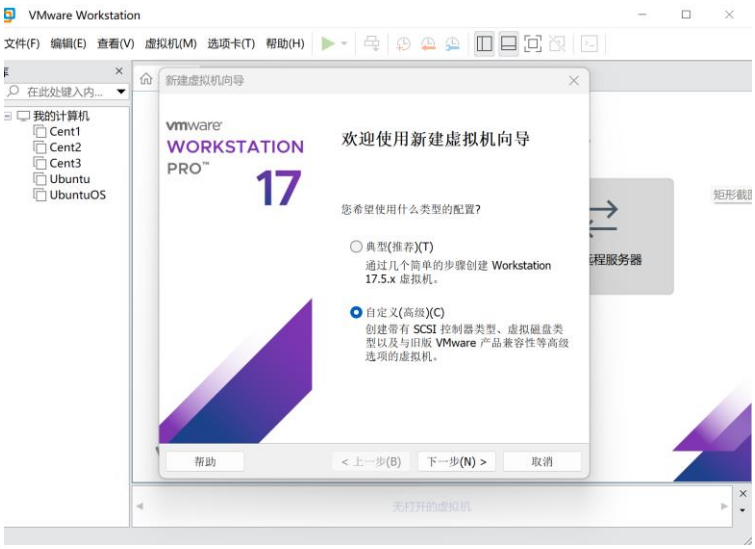
预习教材 chapter 3: basic dynamic analysis

OllyDBG、Process Monitor、Process Explorer、RegShot、WireShar 等工具。

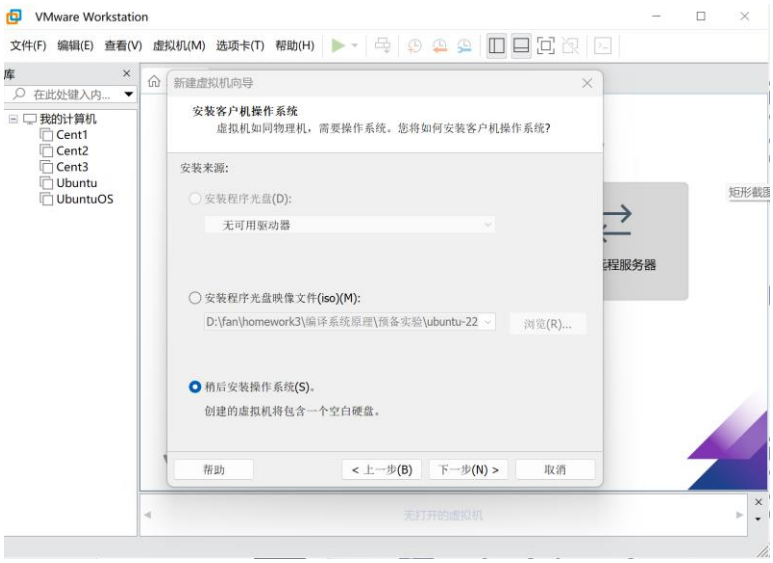
三、实验过程

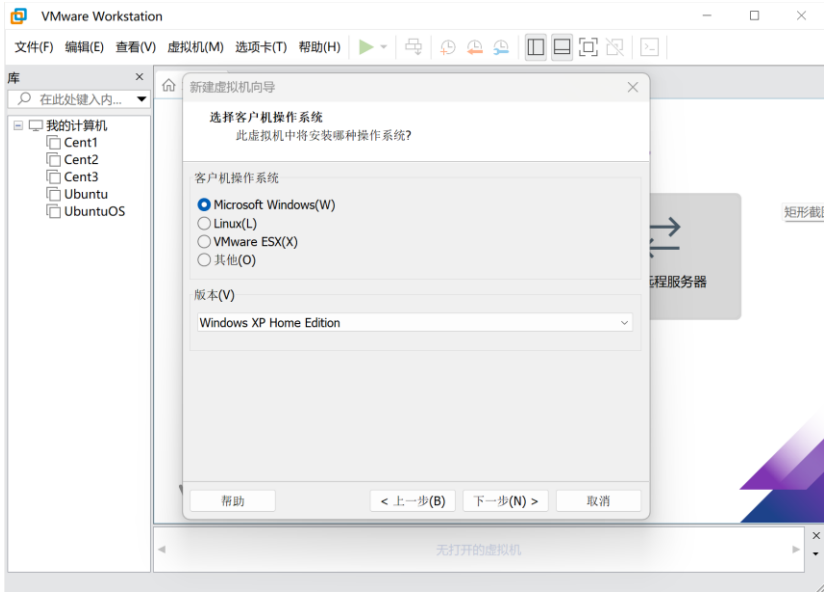
1.虚拟机的安装和配置过程。

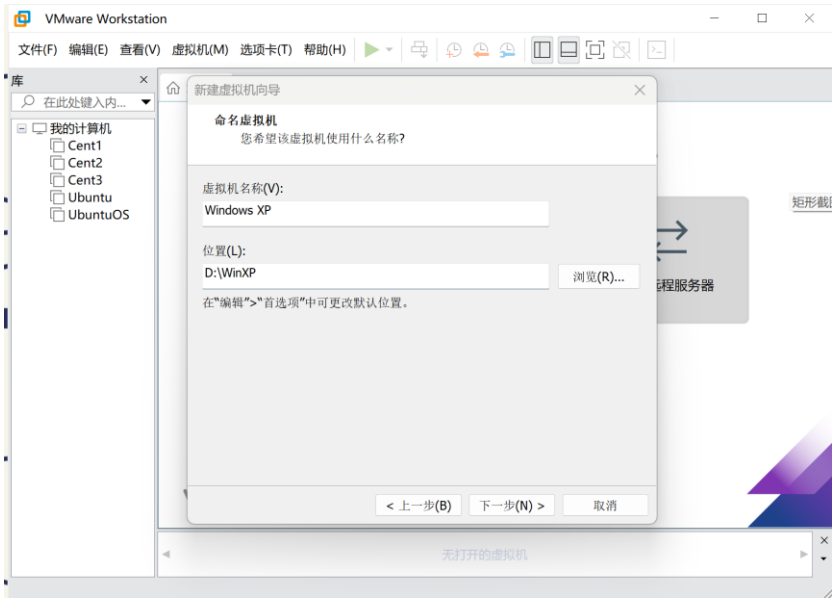
在 VMWARE 中安装 WindowsXP，给虚拟机选择 CD/DVD 使用本地的镜像，设置内存为 2GB，分配 40GB 磁盘空间，而处理器为 4，可以有效的使用相关的软件。

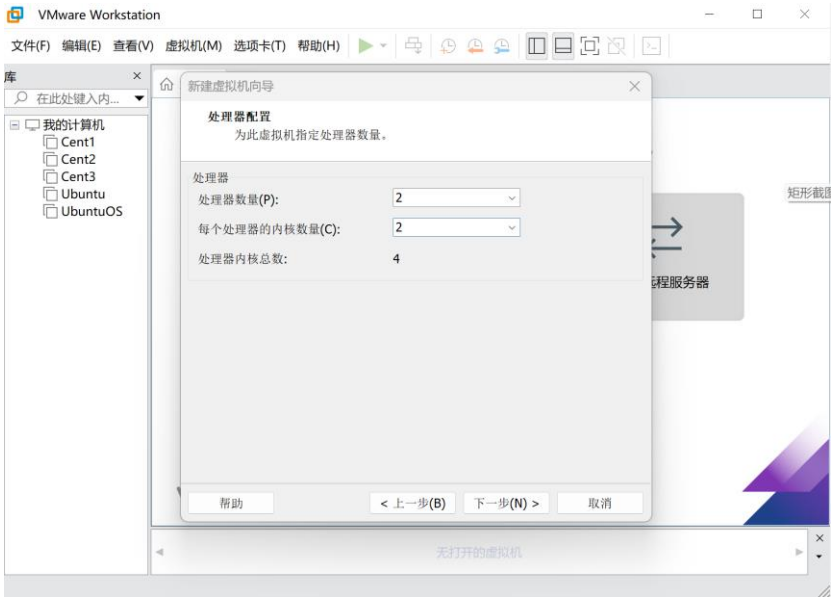

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
vmware
WORKSTATION
PRO
17
欢迎使用新建虚拟机向导
您希望使用什么类型的配置?
典型(推荐)(T)
通过几个简单的步骤创建 Workstation 17.5.x 虚拟机。
自定义(高级)(C)
创建带有 SCSI 控制器类型、虚拟磁盘类型以及与旧版 VMware 产品兼容性等高级选项的虚拟机。
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机

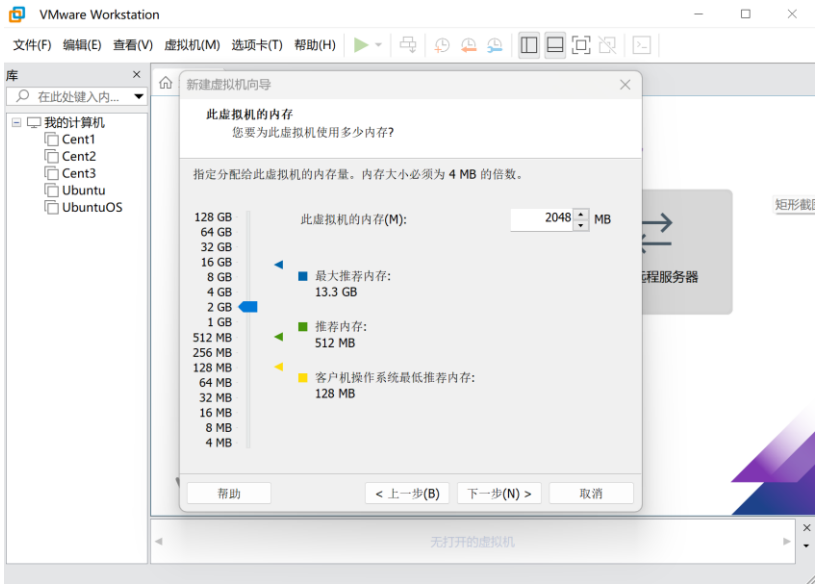

新建虚拟机向导
选择虚拟机硬件兼容性
该虚拟机需要何种硬件功能?
虚拟机硬件兼容性
硬件兼容性(H):
Workstation 17.5.x
兼容:
ESX Server(S)
兼容产品:
Fusion 13.5.x
Workstation 17.5.x
限制:
128 GB 内存
32 个处理器
10 个网络适配器
8 TB 磁盘大小
8 GB 共享图形内存
帮助
< 上一步(B)
下一步(N) >
取消

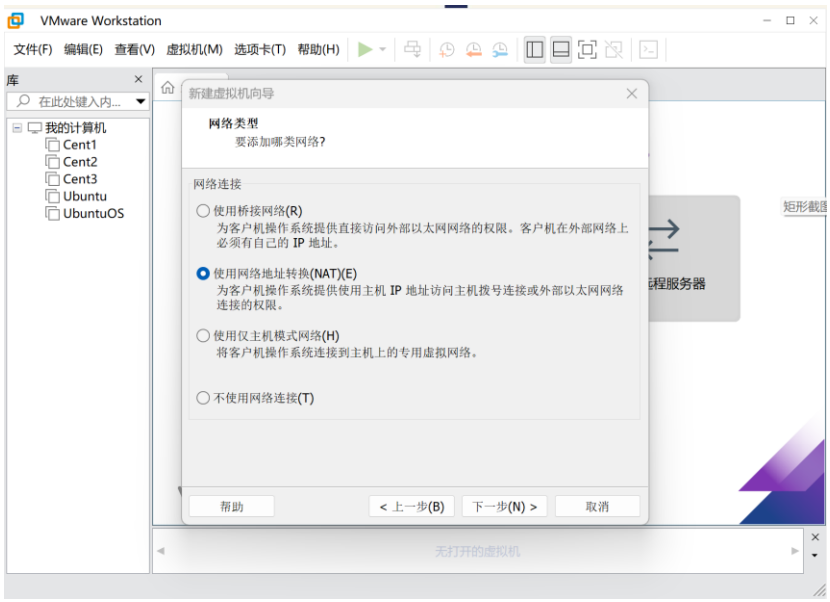

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
安装客户机操作系统
虚拟机如同物理机，需要操作系统。您将如何安装客户机操作系统?
安装来源:
安装程序光盘(D):
无可用驱动器
安装程序光盘映像文件(iso)(M):
D:\fan\homework3\编译系统原理\预备实验\ubuntu-22
浏览(R)...
稍后安装操作系统(S)。
创建的虚拟机将包含一个空白硬盘。
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机

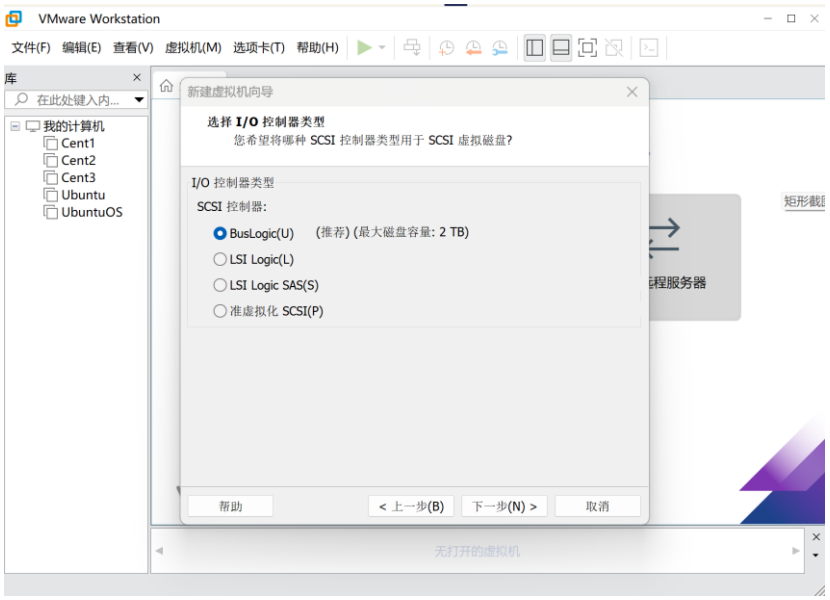

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
选择客户机操作系统
此虚拟机中将安装哪种操作系统?
客户机操作系统
Microsoft Windows(W)
Linux(L)
VMware ESX(X)
其他(O)
版本(V)
Windows XP Home Edition
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机

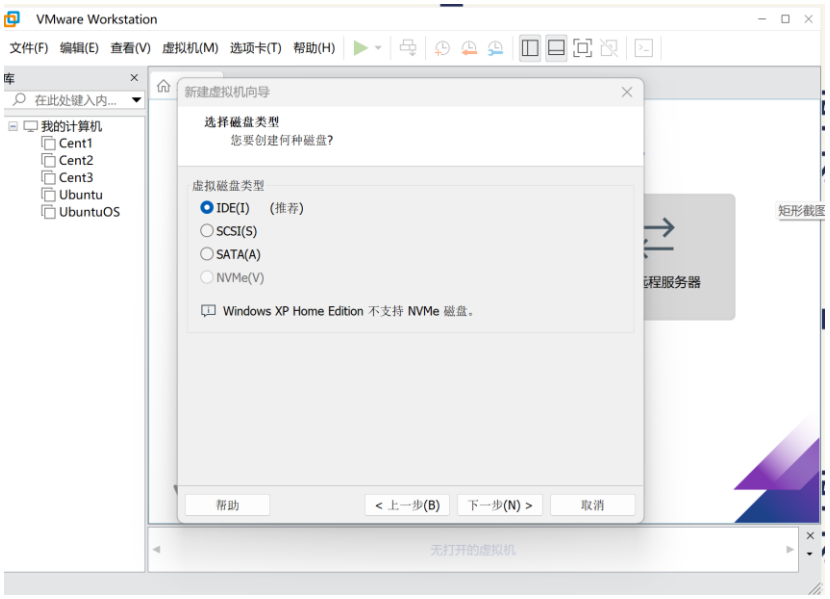

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
命名虚拟机
您希望该虚拟机使用什么名称?
虚拟机名称(V):
Windows XP
位置(L):
D:\WinXP
浏览(R)...
在"编辑">"首选项"中可更改默认位置。
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机

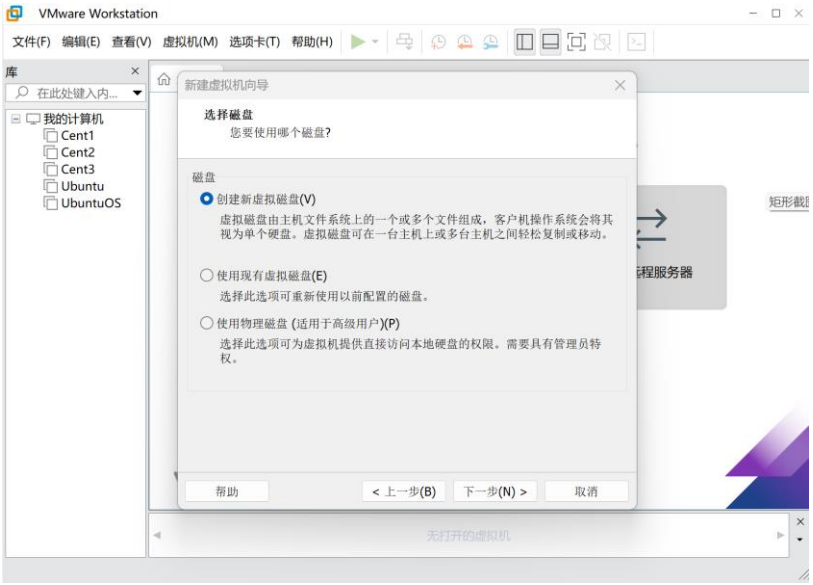

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
处理器配置
为此虚拟机指定处理器数量。
处理器
处理器数量(P): 2
每个处理器的内核数量(C): 2
处理器内核总数: 4
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机

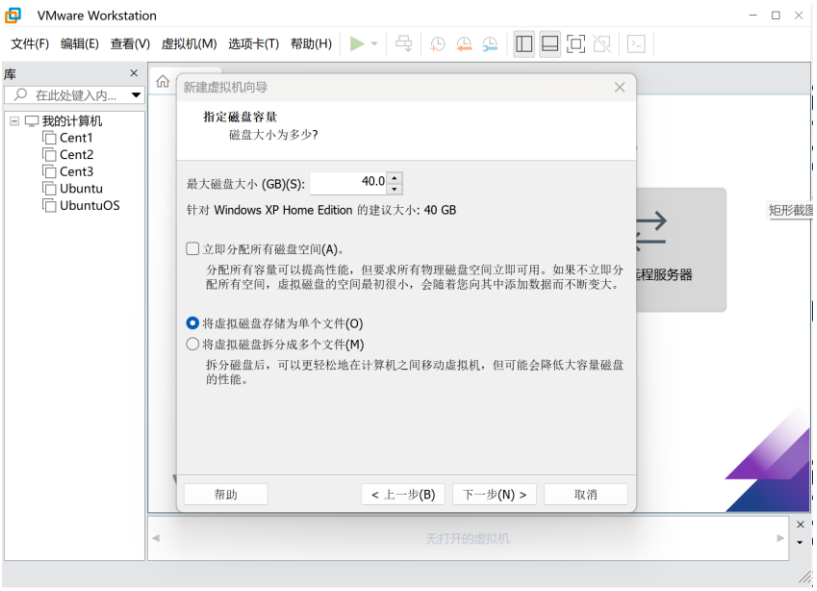

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
此虚拟机的内存
您要为此虚拟机使用多少内存?
指定分配给此虚拟机的内存量。内存大小必须为 4 MB 的倍数。
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
此虚拟机的内存(M): 2048 MB
最大推荐内存:
13.3 GB
推荐内存:
512 MB
客户机操作系统最低推荐内存:
128 MB
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机


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...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
网络类型
要添加哪类网络?
网络连接
使用桥接网络(R)
为客户机操作系统提供直接访问外部以太网网络的权限。客户机在外部网络上必须有自己的 IP 地址。
使用网络地址转换(NAT)(E)
为客户机操作系统提供使用主机 IP 地址访问主机拨号连接或外部以太网网络连接的权限。
使用仅主机模式网络(H)
将客户机操作系统连接到主机上的专用虚拟网络。
不使用网络连接(T)
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机


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...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
选择 I/O 控制器类型
您希望将哪种 SCSI 控制器类型用于 SCSI 虚拟磁盘?
I/O 控制器类型
SCSI 控制器:
BusLogic(U) (推荐) (最大磁盘容量: 2 TB)
LSI Logic(L)
LSI Logic SAS(S)
准虚拟化 SCSI(P)
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机


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...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
选择磁盘类型
您要创建何种磁盘?
虚拟磁盘类型
IDE(I) (推荐)
SCSI(S)
SATA(A)
NVMe(V)
Windows XP Home Edition 不支持 NVMe 磁盘。
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机


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...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
选择磁盘
您要使用哪个磁盘?
磁盘
创建新虚拟磁盘(V)
虚拟磁盘由主机文件系统上的一个或多个文件组成，客户机操作系统会将其视为单个硬盘。虚拟磁盘可在一台主机上或多台主机之间轻松复制或移动。
使用现有虚拟磁盘(E)
选择此选项可重新使用以前配置的磁盘。
使用物理磁盘 (适用于高级用户)(P)
选择此选项可为虚拟机提供直接访问本地硬盘的权限。需要具有管理员特权。
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机
矩形截图
程服务器

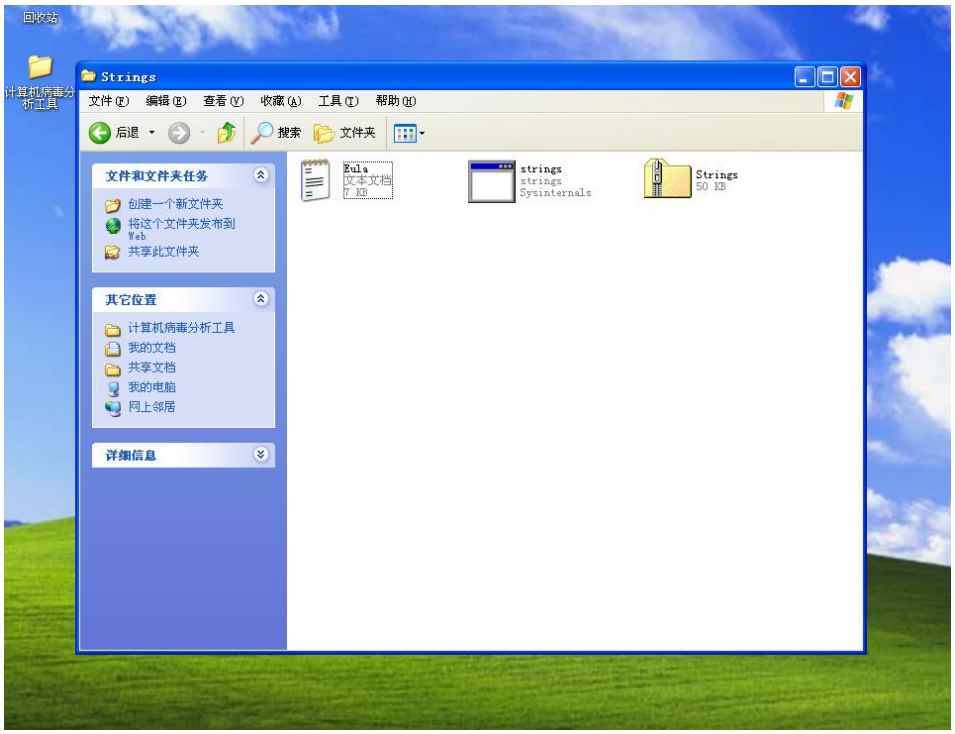

VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内...
我的计算机
Cent1
Cent2
Cent3
Ubuntu
UbuntuOS
新建虚拟机向导
指定磁盘容量
磁盘大小为多少?
最大磁盘大小 (GB)(S): 40.0
针对 Windows XP Home Edition 的建议大小: 40 GB
立即分配所有磁盘空间(A)。
分配所有容量可以提高性能，但要求所有物理磁盘空间立即可用。如果不立即分配所有空间，虚拟磁盘的空间最初很小，会随着您向其中添加数据而不断变大。
将虚拟磁盘存储为单个文件(O)
将虚拟磁盘拆分成多个文件(M)
拆分磁盘后，可以更轻松地在计算机之间移动虚拟机，但可能会降低大容量磁盘的性能。
帮助
< 上一步(B)
下一步(N) >
取消
无打开的虚拟机
矩形截图
程服务器

2. 静态分析工具的功能和安装过程。

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

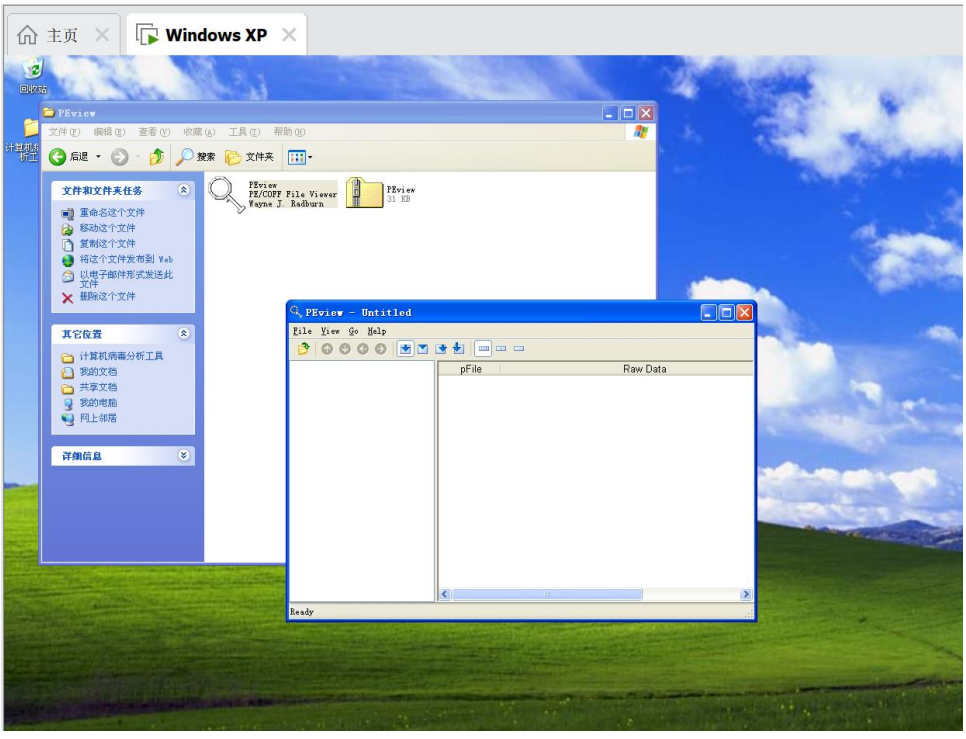
（1）string.exe:

string.exe 是一个用于从二进制文件中提取可读字符串的工具，常用于恶意软件分析和逆向工程。它可以识别 ASCII 和 Unicode 字符串，帮助分析人员发现潜在的恶意特征，如 URL 和文件路径。使用时，在命令行中输入 string.exe 后跟文件路径和选项。



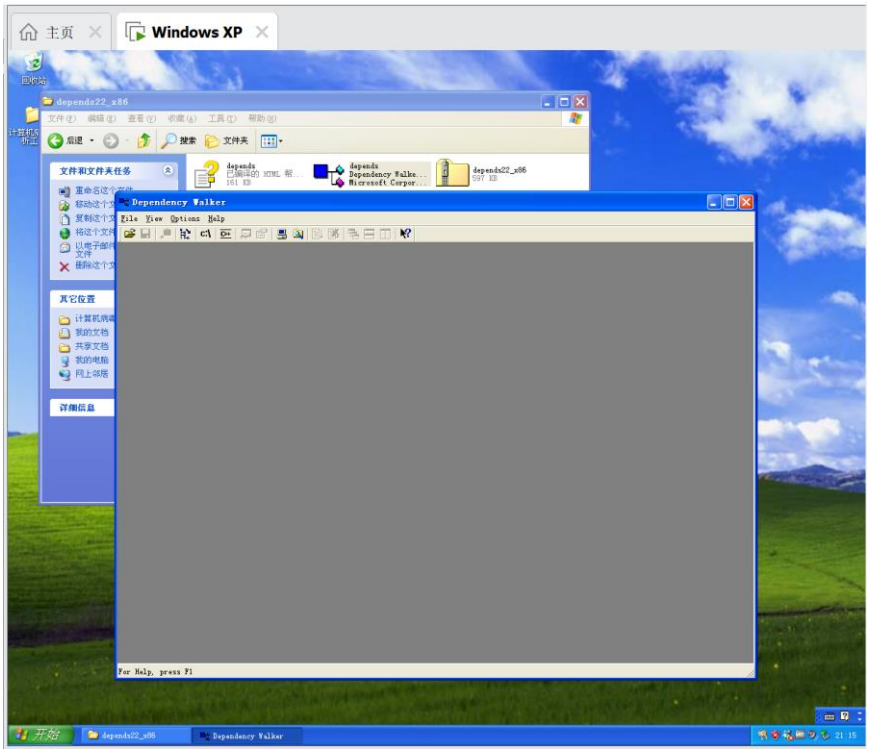
(2) PEView:

PEView 是一个用于查看和分析 Windows 可执行文件（PE 文件）的工具。它提供 PE 文件的结构视图，包括 DOS 头、文件头、节表和资源。主要用于恶意软件分析、调试和数字取证。通过 PEView，用户可以深入了解可执行文件的组成和潜在风险



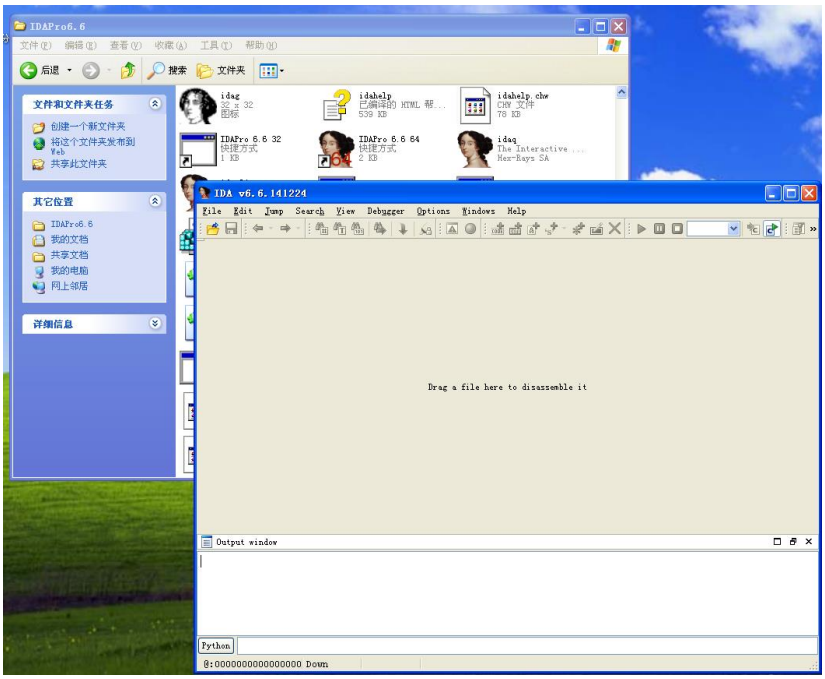
(3) Dependency Walker:

Dependency Walker 是一个分析 Windows 可执行文件和 DLL 的工具，显示它们的依赖关系。它提供依赖树、导入/导出函数列表，并能检测缺失的 DLL 和函数。主要用于软件开发、故障排查和安全分析，帮助用户理解程序的依赖性。



（4）IDA：

IDA Pro 是一个强大的反汇编和逆向工程工具，用于分析可执行文件和二进制代码。它提供交互式界面，支持多种文件格式，能够自动生成汇编代码并进行静态分析。IDA Pro 常用于安全研究、恶意软件分析和软件调试，帮助用户深入理解程序的内部结构和逻辑。



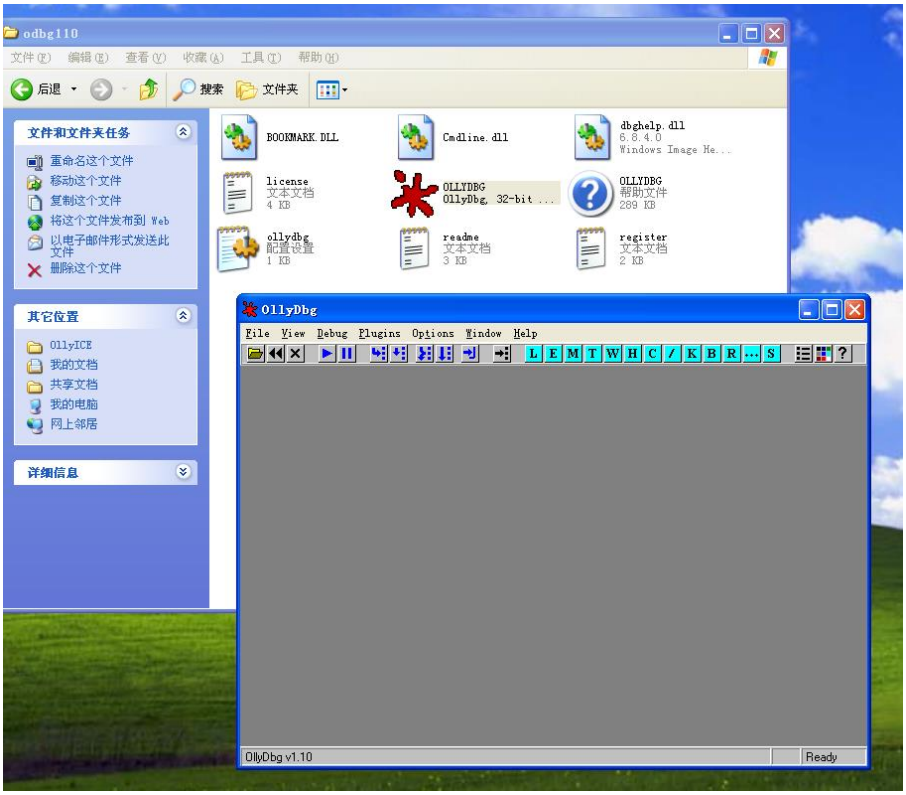
3. 动态分析工具的功能和安装过程。

预习教材 chapter 3: basic dynamic analysis

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

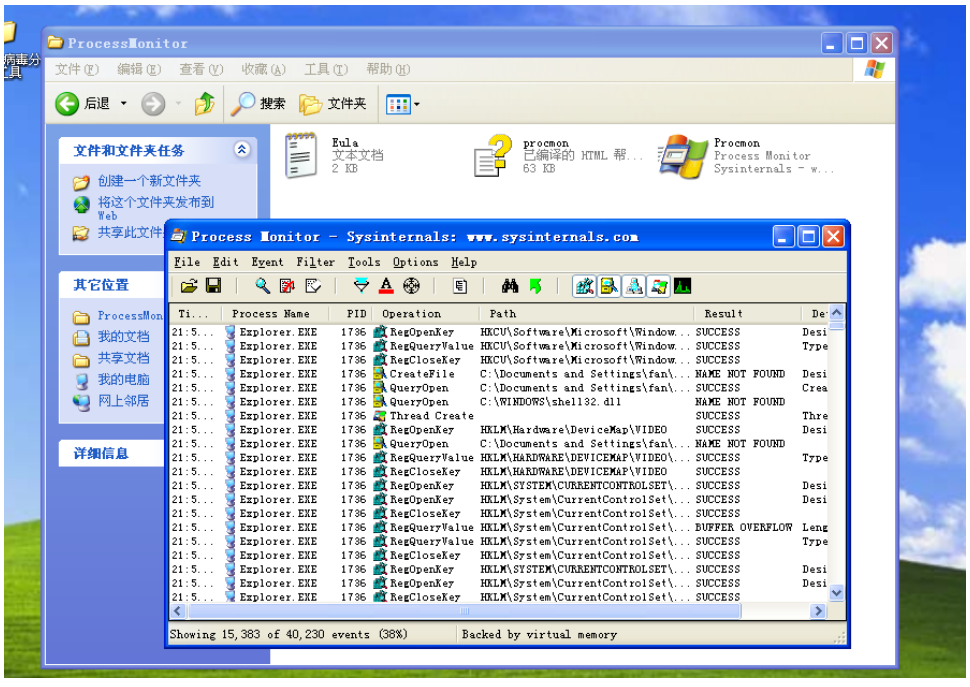
（1） OllyDBG：

OllyDBG 是一个用于 Windows 的强大调试器，专注于分析和逆向工程可执行文件。它支持实时调试，提供易于使用的界面和强大的功能，如反汇编、内存查看和堆栈分析。OllyDBG 常用于恶意软件分析和软件破解，帮助用户深入理解程序的运行过程。



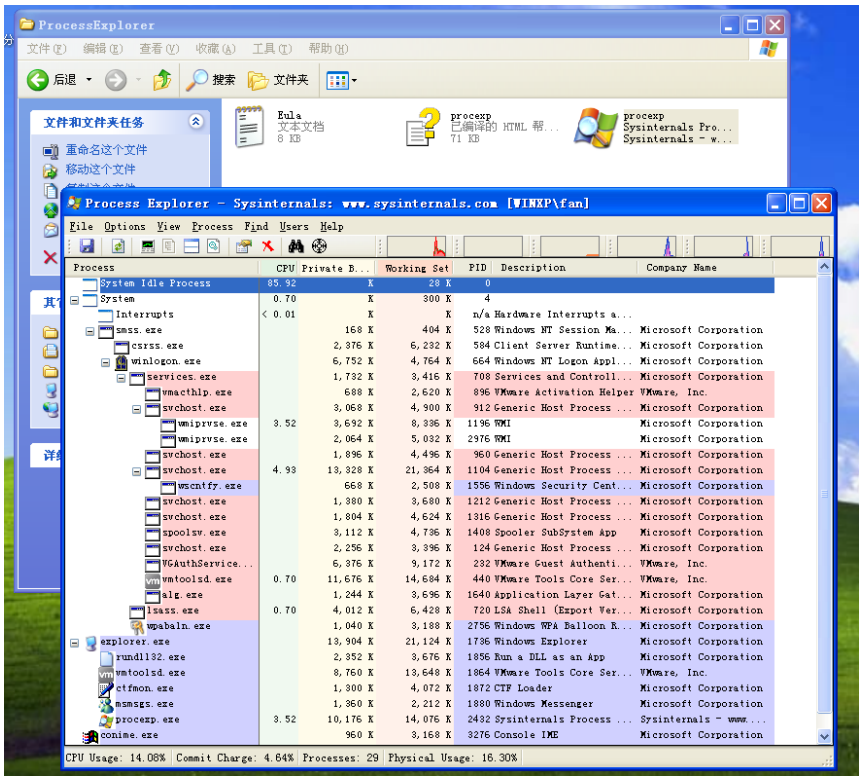
（2）Process Monitor：

Process Monitor 是一个高级监控工具，用于实时跟踪 Windows 系统中的文件系统、注册表、进程和线程活动。它结合了两个经典工具的功能：Filemon 和 Regmon，提供详细的事件日志，帮助用户分析系统性能问题、故障排查和恶意软件行为。



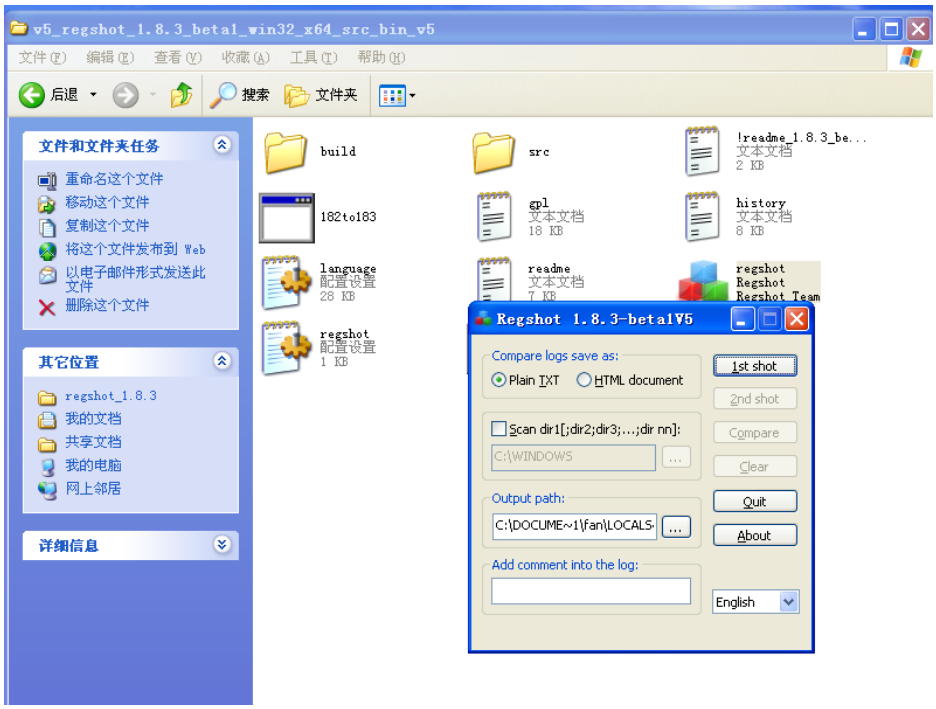
（2）Process Explorer：

Process Explorer 是一个高级任务管理器，用于查看和管理 Windows 系统中的进程和线程。它提供详细的进程信息，包括内存使用、CPU 负载和句柄信息，帮助用户监控系统性能、查找问题和分析进程之间的关系。Process Explorer 是系统管理员和开发人员的常用工具。



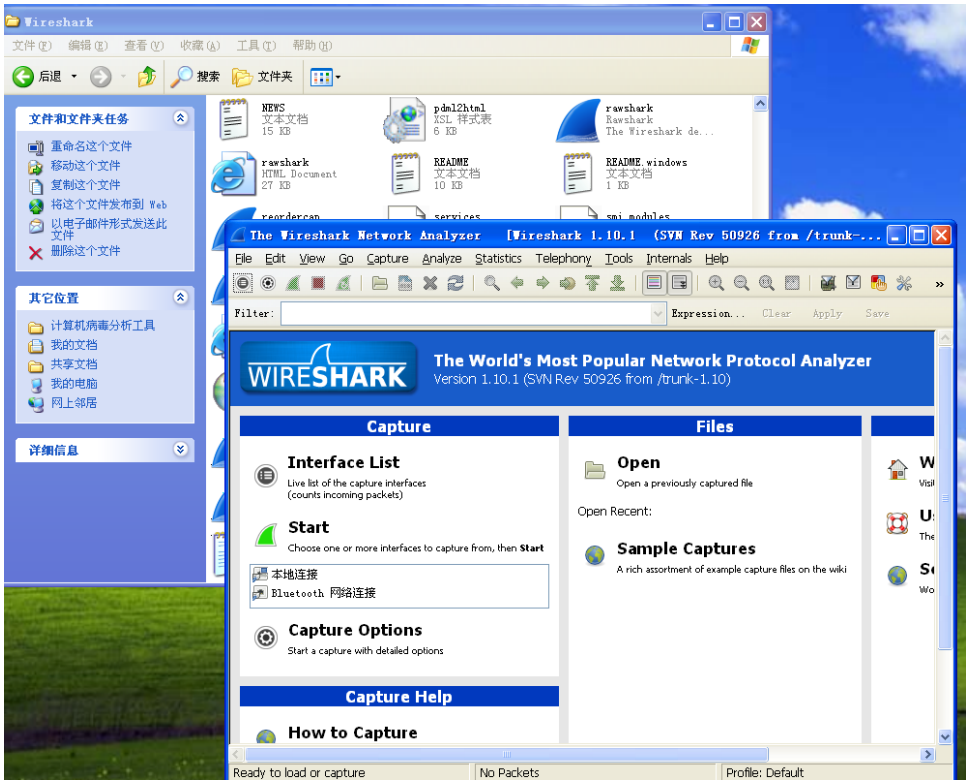
（4）RegShot：

RegShot 是一个轻量级的注册表比较工具，用于监测 Windows 注册表的变化。用户可以在特定时刻拍摄注册表快照，然后在进行系统更改后再次拍摄，以便比较和查看注册表的差异。RegShot 常用于恶意软件分析、系统优化和故障排查。



（5）WireShar：

Wireshark 是一个开源网络协议分析工具，用于捕获和详细分析网络流量。它支持多种协议，提供实时数据包捕获和离线分析功能。Wireshark 常用于网络故障排查、安全分析和网络性能优化，帮助用户深入了解网络通信和数据传输。



四、实验结论及心得体会

通过本次实验，我深入了解了病毒分析的环境配置和工具使用。在虚拟机中安装 Windows XP，使其与主机隔离，提供了安全的分析环境。虽然实验主要在虚拟机中进行，但我在配置分析工具时的知识与技能在其他 Windows 系统中也能得到应用。

安装静态分析工具如 string.exe、PEView 和 Dependency Walker，我能快速提取和分析可执行文件。动态分析工具如 OllyDBG、Process Monitor 和 Process Explorer 的使用，让我直观观察到进程行为和系统变化，增强了对恶意软件行为的理解。