南開大學

恶意代码分析与防治技术实验报告

实验二：虚拟机技术

学　　院　网络空间安全学院

专　　业　信息安全、法学

学　　号　2112514

姓　　名　辛浩然

班　　级　信息安全、法学

一、实验目的

1. 安装和配置虚拟机；

2. 了解基本静态分析和动态分析工具的基本功能，安装基本静态分析和动态分析工具；

3. 构建病毒分析虚拟机环境。

二、实验原理

在进行恶意代码动态分析之前，必须确保建立安全环境。

恶意代码可能包含意外的威胁，如果在业务主机上运行，可能会迅速传播到其他网络主机，难以清除。使用物理主机与隔离网络，可以在一个真实环境中运行恶意代码，而不会给其他主机带来任何风险。但是这种测试场景也存在着缺点，那就是缺乏互联网连接。许多恶意代码依靠互联网连接，来进行自身更新、获取命令、接受控制以及运行其他功能。另一方面，物理环境分析恶意代码可能难以清除。

虚拟环境是常用的动态分析环境，尽管恶意代码在虚拟机中可能表现不同，但它们减少了风险。因此，虚拟机是进行动态分析的首选环境。

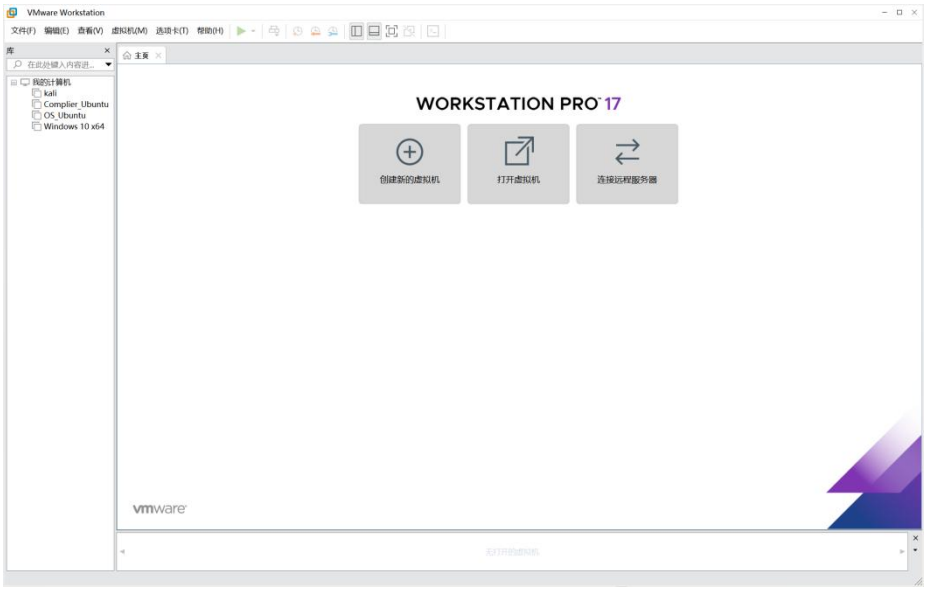
三、实验过程

（一）安装和配置虚拟机

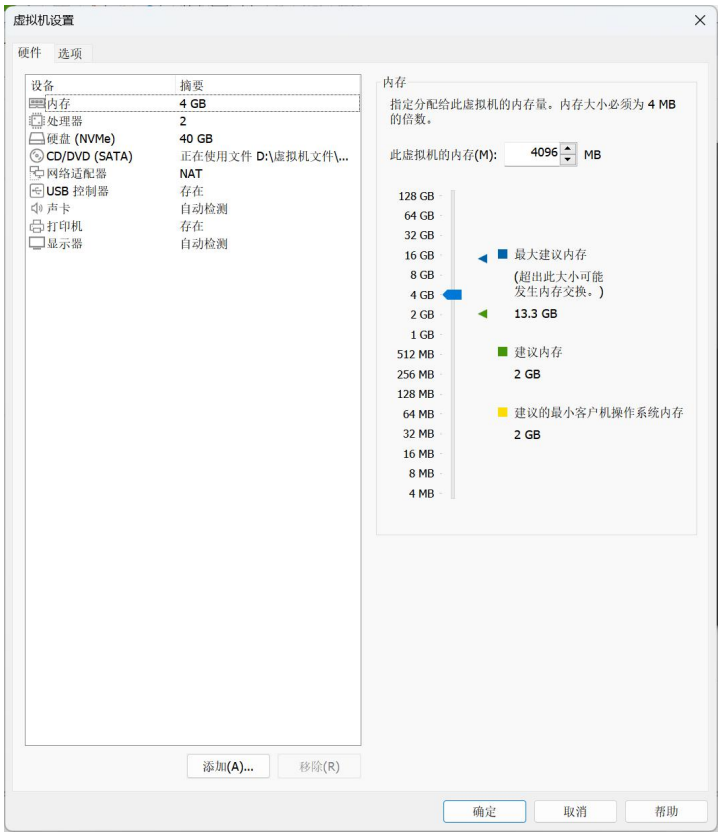
由于 Lab1 就在搭建的 Windows10 虚拟机系统中进行的，因此只展示虚拟机安装和配置结果。

首先，安装 VMware Workstation Pro。

VMware Workstation Pro 是一款功能强大的虚拟化软件，用于在单台物理计算机上创建和管理多个虚拟机。VMware Workstation Pro 基于**虚拟化**技术，允许在一台物理计算机上同时运行多个虚拟机。这些虚拟机可以是不同的操作系统，例如 Windows、Linux、macOS 等。VMware Workstation Pro 允许用户**创建虚拟机快照**，以便在出现问题时轻松还原虚拟机状态。该软件支持网络模拟，可以**模拟不同网络环境**，如局域网、广域网和断开连接的网络，以测试应用程序在不同网络条件下的性能。VMware Workstation Pro 提供了**多层安全功能**，包括加密、虚拟机防火墙和访客操作系统隔离，以确保虚拟机的安全性。



接下来需要安装操作系统。我安装的是 Windows 10 ×64 操作系统。以下是操作系统安装后的初始配置：



接下来，安装 VMware Tools。从 VMware 菜单中，选择虚拟机(VM)→安装 VMware Tools(Install VMware Tools)，来开始安装过程。VMware Tools 会让鼠标和键盘的响应变得更敏捷，从而大大提升用户体验。它还允许访问共享文件夹，进行拖放式文件传输，以及其他各种有用的功能。

接下来配置网络环境。大多数恶意代码都具有联网功能。例如，蠕虫会通过网络攻击其他计算机来努力传播自身。但是肯定能不允许蠕虫访问自己的网络，因为它可能会传播到其

他计算机上。

因此，使用**多个虚拟机**的方式来配置网络连接。将 win10 和 kali 通过一个私有局域网进行连接，但是断开这个局域网和互联网以及宿主主机的连接，这样恶意代码可以连接到网络。其中，Win10 进行分析恶意代码，Kali 提供网络服务。以下是具体步骤：

添加一个网络，设为仅主机模式。

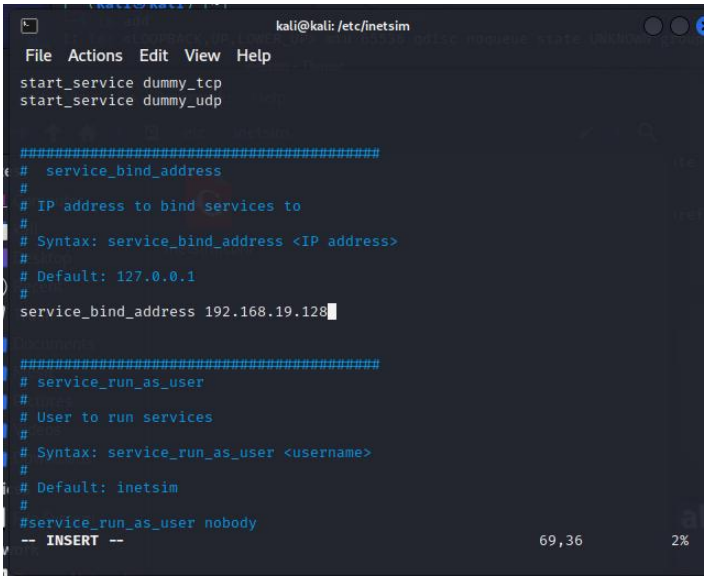
将 Win10 和 Kali 的网络连接都改成自定义：刚刚添加的特定虚拟网络。

提供网络服务的虚拟机的设置：

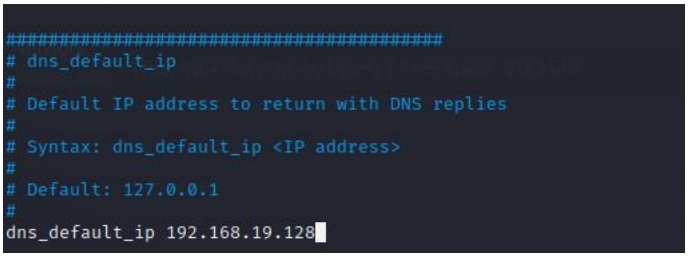
在 kali 中：配置 INetSim

编辑 INetSim 的配置文件：inetsim.conf ：

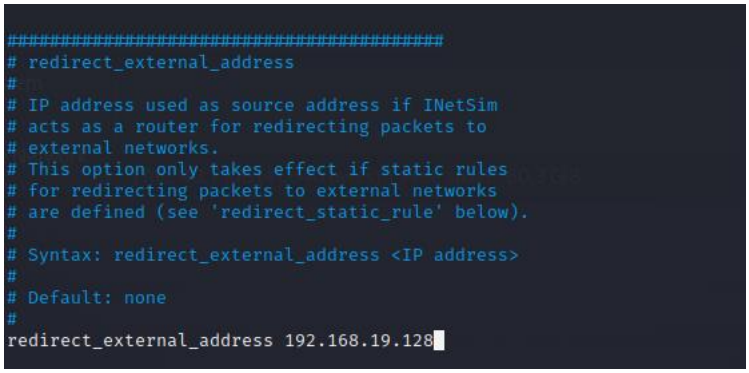
#service_bind_address 10.10.10.1 取消注释并改为 Kali 的 IP



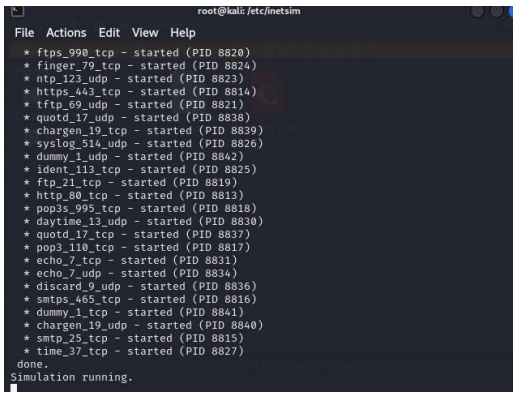
#dns_default_ip 10.10.10.1 取消注释该行并改为 Kali 的 IP



将重定向地址改成 Kali 的 ip

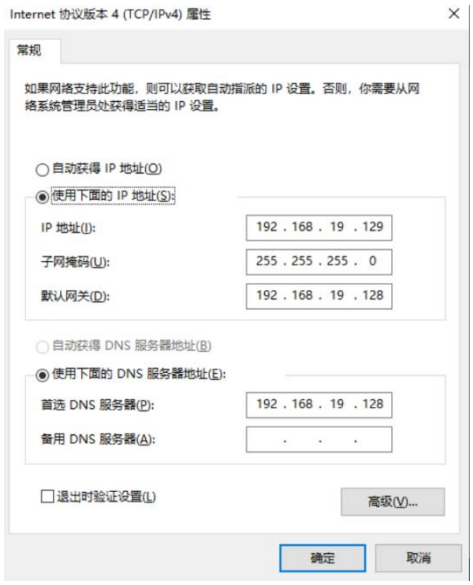


配置结束后运行 INetSim：

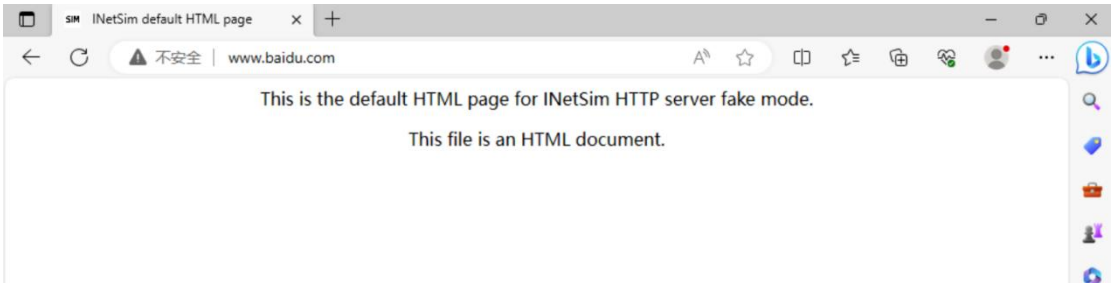


分析病毒的 win10 虚拟机的配置：

DNS 服务器、网关设置为 INetSim 绑定的 IP：



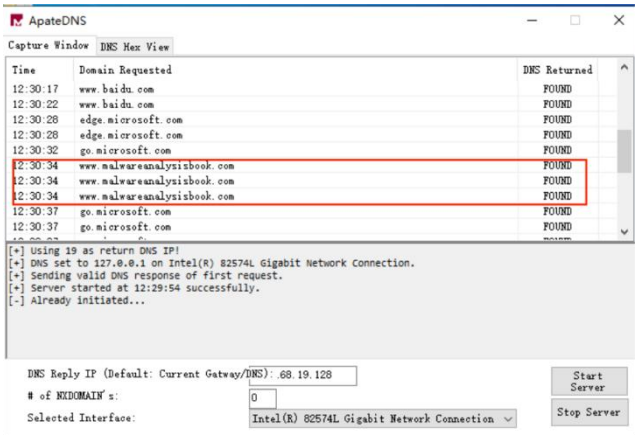
输入 www.baidu.com：



使用 ApateDNS 查看恶意代码发出的 DNS 请求

在运行恶意代码的虚拟机的里使用 ApateDNS，打开后将 DNS Reply IP 设置成提供网络服务的虚拟机的 IP。

然后打开 lab01-03.exe。查看 ApateDNS，记录了刚才恶意代码的访问请求：



在进行恶意代码分析，弄清楚恶意代码连接互联网时会做些什么事情之后，如果认为可以承担相应风险之后，可以让它联网。可以使用 VMware 的网络地址转换(NAT)模式。NAT 模式会共享宿主机与互联网之间的 IP 连接。宿主机像是一个路由器，负责对所有来自虚拟机的连接进行翻译，让它们看起来就是从宿主机的 IP 地址发出的一样。

（二）静态分析工具的功能与安装

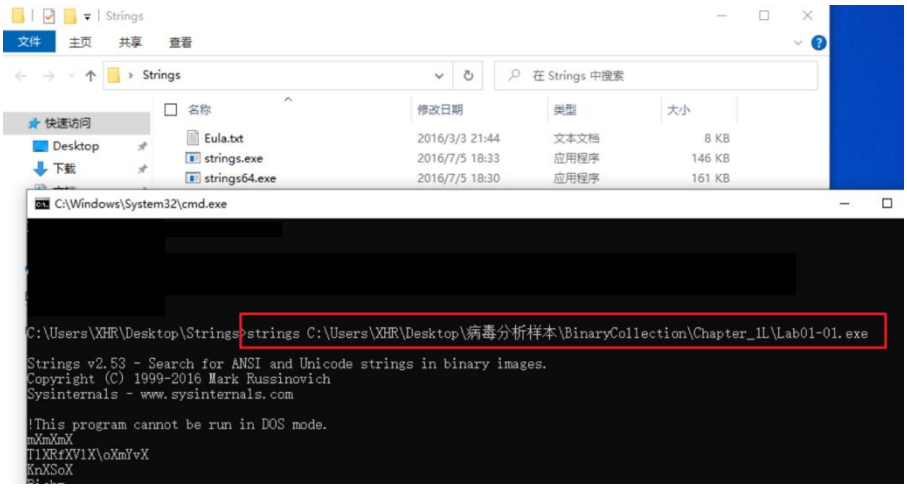
由于在进行 Lab1 时，已经安装并使用了这些工具。因此，不展示这些工具的安装过程，只展示安装结果。

strings.exe

可以找出文件内容中的可打印字符串。可打印字符串是指，它的组成部分都是可打印字符，并且以 null 或者 newline 结尾。

对于普通文本文件来说，strings 没有任何意义，因为文本文件中的任何内容实际都是可打印的字符串。strings 最常用的场合就是列出动态库或者可执行程序等二进制文件中出现的字符串，结合 grep 即可实现查找。

strings 的使用方法很简单，strings [文件]即可，它会默认输出长度大于 4 的字符串，每行一个。



此外它还有几个参数。如-n number 仅输出长度大于 number 的字符串。具体如下：

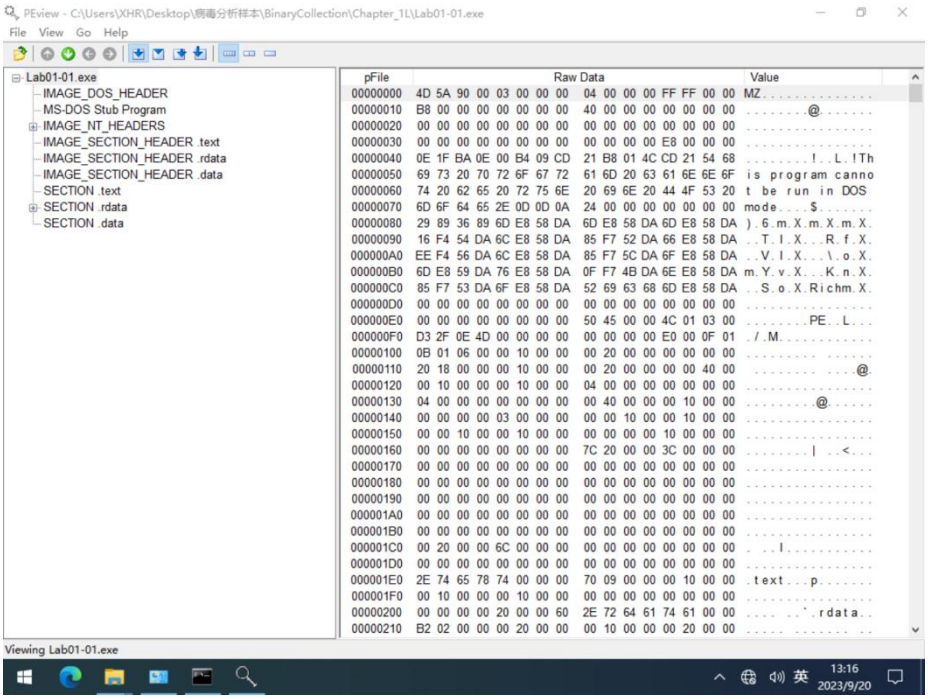
```
C:\Users\XHR\Desktop\Strings>strings

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u] <file or directory>
-a      Ascii-only search (Unicode and Ascii is default)
-b      Bytes of file to scan
-f      File offset at which to start scanning.
-o      Print offset in file string was located
-n      Minimum string length (default is 3)
-s      Recurse subdirectories
-u      Unicode-only search (Unicode and Ascii is default)
-nobanner
        Do not display the startup banner and copyright message.
```

PEView

PEview 是一种用于查看和分析 Windows 可执行文件（PE 文件）的工具。PE 文件

是 Windows 操作系统中常见的可执行文件格式，包括.exe 文件、.dll 文件和.sys 文件等。PEview 允许用户查看 PE 文件的内部结构和元数据，帮助分析文件的属性、导入和导出函数、节表、资源等信息。

在 Lab1 中，下载使用 PEView 产生报错。因此，在 GitHub 中找到补丁版的 PEView。



Dependency walker

Dependency Walker（依赖性查看器）是一个用于分析和显示 Windows 操作系统下可执行文件（如.EXE、.DLL 等）的依赖关系的工具。它是一个免费的 Windows 应用程序，通常用于识别和解决程序运行时出现的问题，特别是与动态链接库（DLL）相关的问题。

具体而言：

依赖关系分析：Dependency Walker 可以列出一个可执行文件所依赖的所有 DLL 文件，以及这些 DLL 文件之间的依赖关系。这有助于开发人员了解一个程序的依赖性，以确保所有必需的 DLL 文件都可用，并且版本兼容。

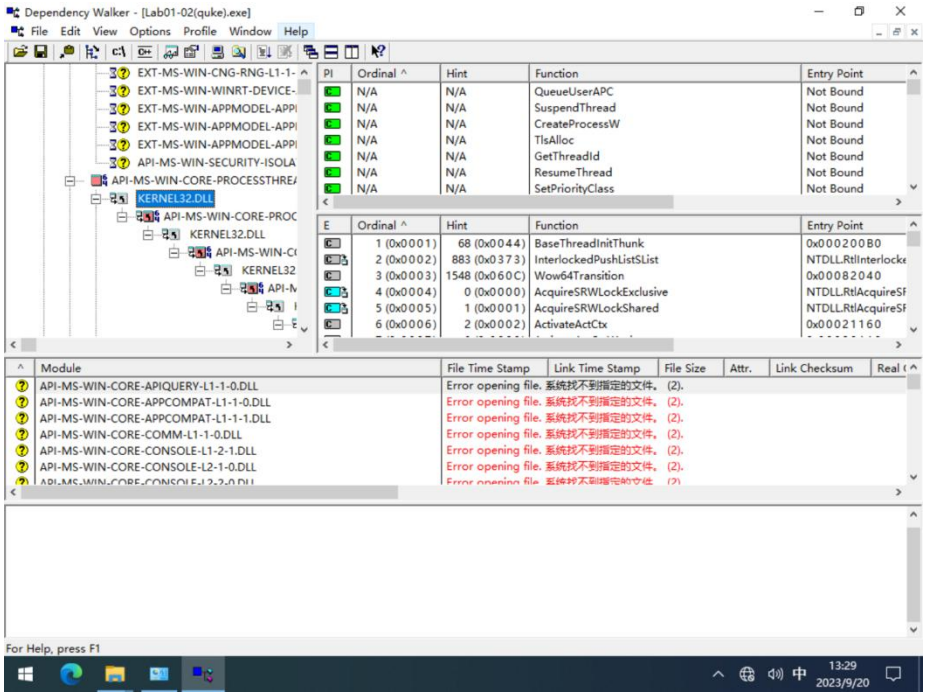
错误检测：Dependency Walker 能够检测到在程序运行时可能导致崩溃或错误的依赖问题。如果某个 DLL 文件丢失、损坏或版本不匹配，它会在分析中显示相应的警告或错误信息。

导出函数查看：工具可以显示每个 DLL 文件中包含的导出函数列表，这对于了解 DLL 提供的功能非常有用。这些导出函数是其他程序可以调用的函数。

模块属性查看：Dependency Walker 还提供了有关每个模块（包括 EXE 和 DLL 文件）的详细属性信息，如文件版本、文件大小等。

图形展示：该工具以树状图的形式展示依赖关系，使用户能够清晰地看到各个模块之间的连接。

安装后打开恶意代码，页面如下：



IDA Pro

IDA Pro 是一款强大的反汇编工具，用于分析和逆向工程二进制文件。它由 Hex-Rays 公司开发，是逆向工程领域最广泛使用的工具之一。具体功能如下：

反汇编功能：IDA Pro 能够将二进制文件反汇编成可读的汇编代码，帮助分析人员理解程序的结构和逻辑。

多平台支持：IDA Pro 支持多种处理器架构和操作系统，包括 x86、ARM、MIPS、PowerPC 等，以及 Windows、Linux、macOS 等不同平台。

图形化界面：IDA Pro 具有直观的图形用户界面，使分析人员能够更容易地浏览和编辑反汇编代码。

反编译功能：Hex-Rays 公司的插件 IDA Hex-Rays 可以让用户将反汇编代码转化为高级语言，如 C 语言或 C++语言，使代码更容易理解。

插件系统：IDA Pro 具有强大的插件系统，允许用户编写自定义插件来扩展功能。这些插件可以用于自动化任务、增强分析功能以及解析特定的二进制文件格式。

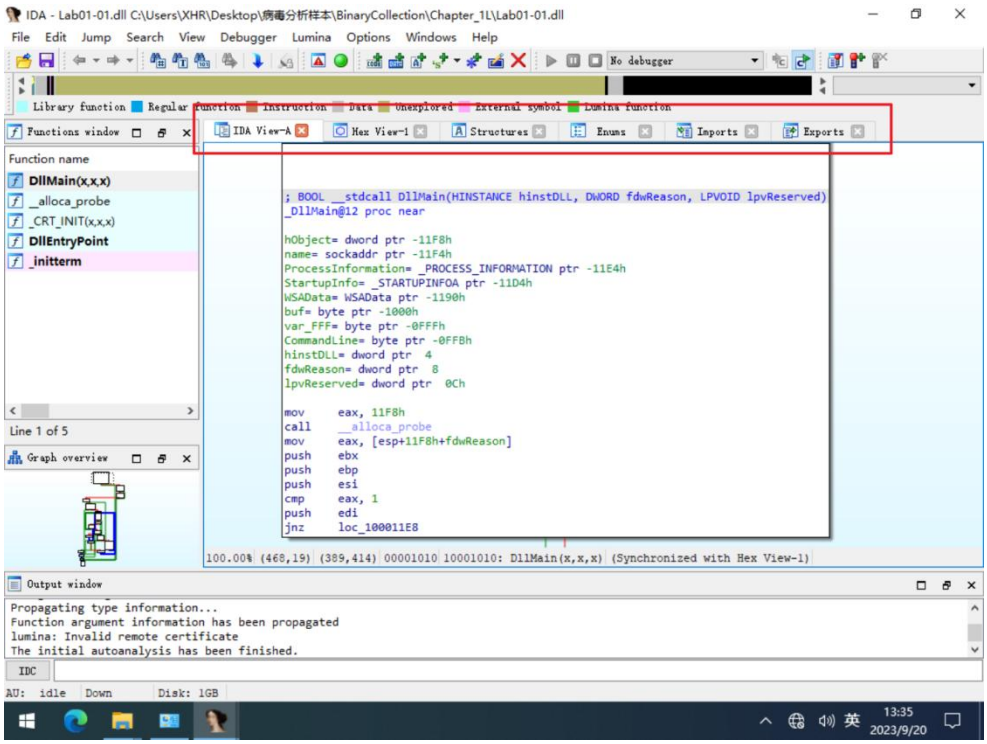
动态分析：IDA Pro 还具有一些动态分析功能，例如内存和寄存器状态跟踪，以帮助分析人员理解程序的行为。

脚本支持：IDA Pro 支持多种脚本语言，包括 Python，允许用户编写脚本来自动化任务和执行定制分析。

调试集成：IDA Pro 可以与调试器集成，使用户能够在反汇编代码上进行调试，以更深

入地理解程序行为。

安装后打开恶意代码文件，可以查看控制流图、导入表、导出表、字符串等信息。



（三）动态分析工具的功能与安装

OllyDBG

OllyDbg 是一个强大的 Windows 反汇编器和调试器工具，主要用于分析和调试二进制可执行文件，如应用程序和驱动程序。以下是它的主要功能：

反汇编功能：OllyDbg 允许用户查看和分析程序的汇编代码，这对于逆向工程和理解程序的内部运行方式非常有用。用户可以查看代码、修改代码并跟踪执行流程。

调试功能：OllyDbg 支持完整的调试功能，包括断点设置、单步执行、内存查看、寄存器查看等。这些功能帮助用户识别和修复程序中的错误或安全漏洞。

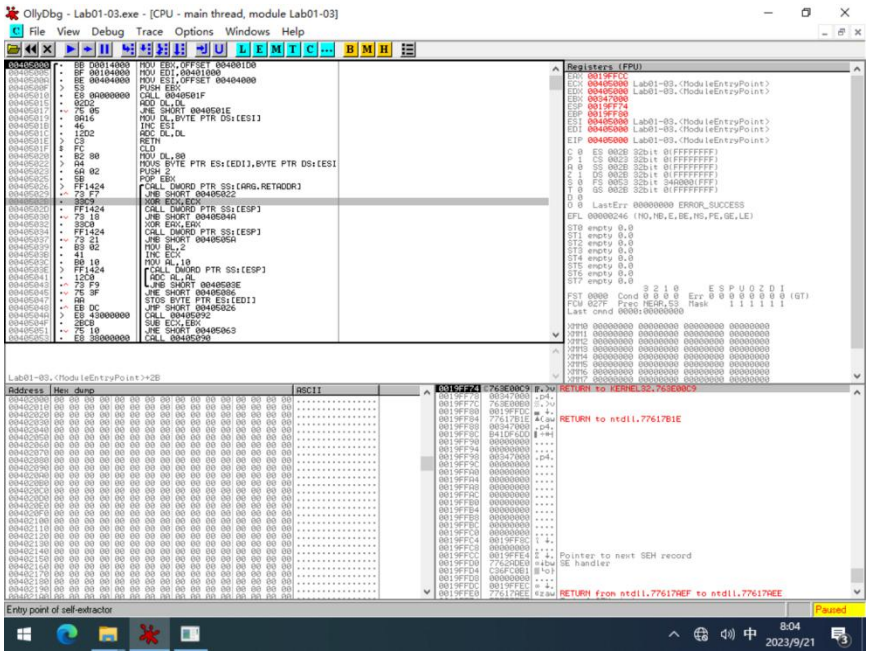
插件支持：OllyDbg 具有强大的插件架构，可以扩展其功能以满足不同需求。这意味着用户可以根据自己的需求添加自定义插件，以执行特定任务或分析特定类型的程序。

动态分析：OllyDbg 允许用户在运行时观察程序的行为。这对于检测恶意软件、病毒分析和研究加密算法等任务非常有用。

脚本支持：用户可以使用 Python 等脚本语言编写脚本，以自动化调试任务，简化分析流程，并执行复杂的操作。

资源查看：除了汇编代码，OllyDbg 还可以查看程序中的资源，如字符串、图标、位图等，以帮助用户了解程序的结构和功能。

以下是安装并使用 OllyDbg：



Process Monitor

Process Monitor 是一款由 Microsoft 提供的高级系统监视工具，用于跟踪和记录 Windows 操作系统内的进程活动，包括文件系统、注册表、进程和线程等。它是一个强大的诊断工具，可用于解决各种系统问题，包括应用程序错误、性能问题和安全审计等。

功能：

实时监视：Process Monitor 能够实时监视系统上发生的各种活动，包括文件和目录的访问、注册表的读写、进程和线程的创建和终止等。

过滤功能：它提供了强大的过滤功能，允许用户根据各种条件过滤事件，以便集中关注感兴趣的活动。用户可以根据进程、路径、操作类型、关键字等进行筛选。

详细信息：Process Monitor 会记录每个事件的详细信息，包括时间戳、进程 ID、线程 ID、操作类型、路径、结果等。这些信息有助于用户了解何时、何地和如何发生了某个操作。

导出日志：用户可以将记录的事件导出到文件中，以供后续分析和共享。这对于生成报告、进行离线分析或与他人共享问题信息非常有用。

进程树和堆栈跟踪：Process Monitor 还提供了进程树视图，显示了进程之间的关系，以及堆栈跟踪功能，可用于查看事件的调用堆栈，有助于诊断问题的根本原因。

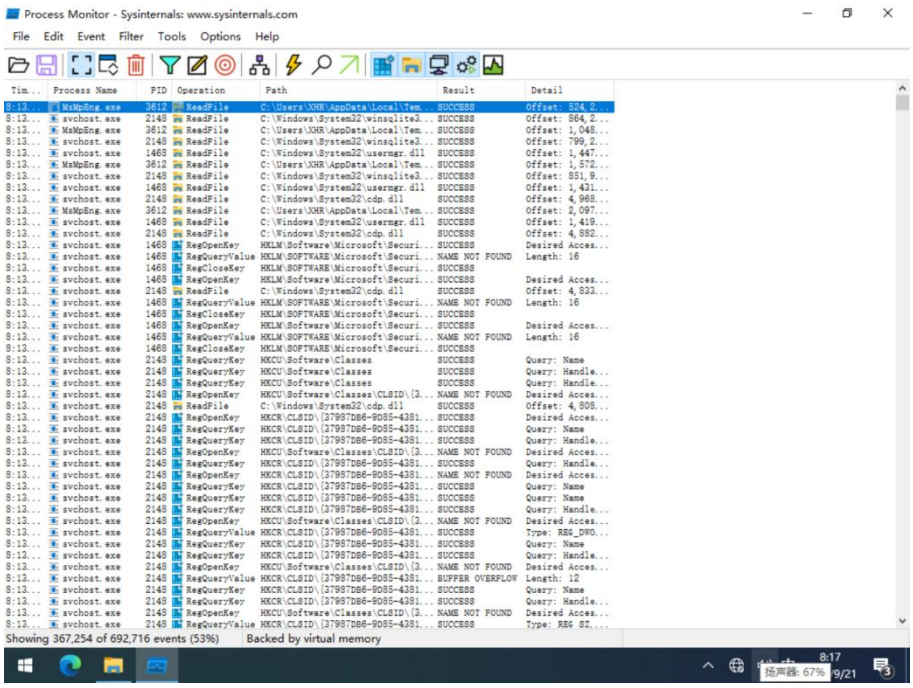
使用方法：

配置过滤：在菜单栏或工具栏上，可以配置过滤条件，以便只显示感兴趣的事件。这可以大大减少日志中的条目数量，使其更易于分析。

开始监视：点击工具栏上的“启动”按钮开始监视。Process Monitor 将立即开始记录系统活动。

观察和分析：观察记录的事件，查看哪些进程执行了哪些操作，以及操作是否成功。使用过滤和排序功能来组织数据，以便更容易找到问题。

导出日志：可以导出记录的事件以供进一步分析或与他人共享。选择“文件”菜单中的“导出”选项即可执行此操作。



Process Explorer

Process Explorer（进程资源管理器）是一款由 Microsoft 提供的高级任务管理器工具，用于查看和管理运行在 Windows 操作系统上的进程、线程、服务、句柄和系统性能信息。它提供了比标准 Windows 任务管理器更丰富的功能和更详细的信息，使用户能够更好地理解和管理系统进程。

功能：

进程查看：Process Explorer 显示运行在计算机上的所有进程的列表，包括其名称、描述、公司信息、CPU 和内存使用情况等。

详细信息：用户可以查看每个进程的详细信息，包括线程、内存、CPU 使用情况、打开的文件和 DLL 模块等。这有助于诊断性能问题和进程之间的关联。

进程树：Process Explorer 以树状结构显示进程，使用户可以清楚地了解进程之间的关系，包括父子关系和衍生的子进程。

资源使用情况：工具提供了实时的 CPU、内存、磁盘和网络使用情况图表，帮助用户监视系统的资源负载。

句柄查看：Process Explorer 显示每个进程所拥有的文件句柄、注册表键、事件、线程等资源，有助于识别资源泄漏和问题。

DLL 和驱动程序信息：用户可以查看进程加载的 DLL 和驱动程序，以帮助分析应用程

序的依赖关系和问题。

搜索功能：Process Explorer 提供快速搜索功能，以便找到特定进程、句柄、DLL 等。

杀死进程：用户可以通过右键单击选定的进程来终止它，这对于关闭不响应的应用程序或恶意软件很有用。

使用方法：

查看进程列表：在主窗口中，可以看到一个列出所有运行进程的列表。点击进程名称可查看详细信息。

查看详细信息：在详细信息窗口中，可以查看有关进程的更多信息，包括性能指标、线程、内存使用情况等。

查看进程树：使用主窗口的“View”菜单中的“Show Process Tree”选项以查看进程之间的关系。

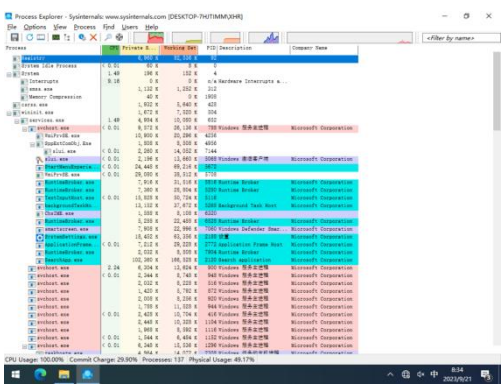
查看句柄和 DLL 信息：使用“View”菜单中的“Lower Pane View”选项来选择要查看的资源类型，如句柄或 DLL。

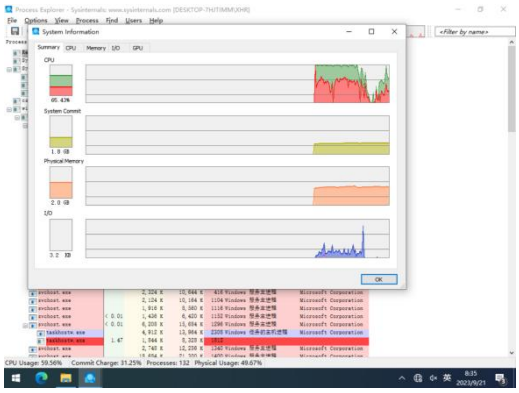
搜索进程：使用主窗口上方的搜索框来查找特定进程或资源。

结束进程：如果需要终止进程，可以右键单击进程并选择“Kill Process”。

监视资源使用情况：使用下方的性能图表来监视 CPU、内存、磁盘和网络使用情况。

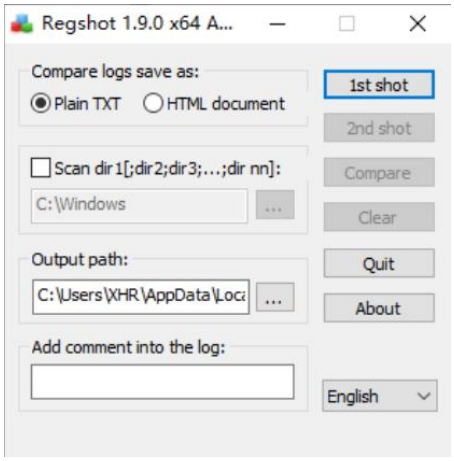
导出信息：如果需要，可以导出进程信息以供后续分析。





RegShot

RegShot 是一个用于比较 Windows 系统注册表更改的实用工具。它的主要功能是记录系统注册表的当前状态，然后再次记录注册表的状态，并生成两个状态的差异报告，以帮助用户了解何时、何地以及如何进行了注册表更改。



WireShark

Wireshark 是一个流行的开源网络分析工具，它用于捕获和分析网络数据包。它提供了丰富的功能，能够深入了解网络通信并解决网络问题。

功能：

数据包捕获：Wireshark 可以捕获通过计算机网络传输的数据包。这可以帮助监视网络流量并收集数据进行分析。

协议支持：Wireshark 支持多种网络协议，包括以太网、Wi-Fi、TCP、UDP、IP、HTTP、DNS、SMTP、FTP 等。它能够解析和展示这些协议的数据包内容。

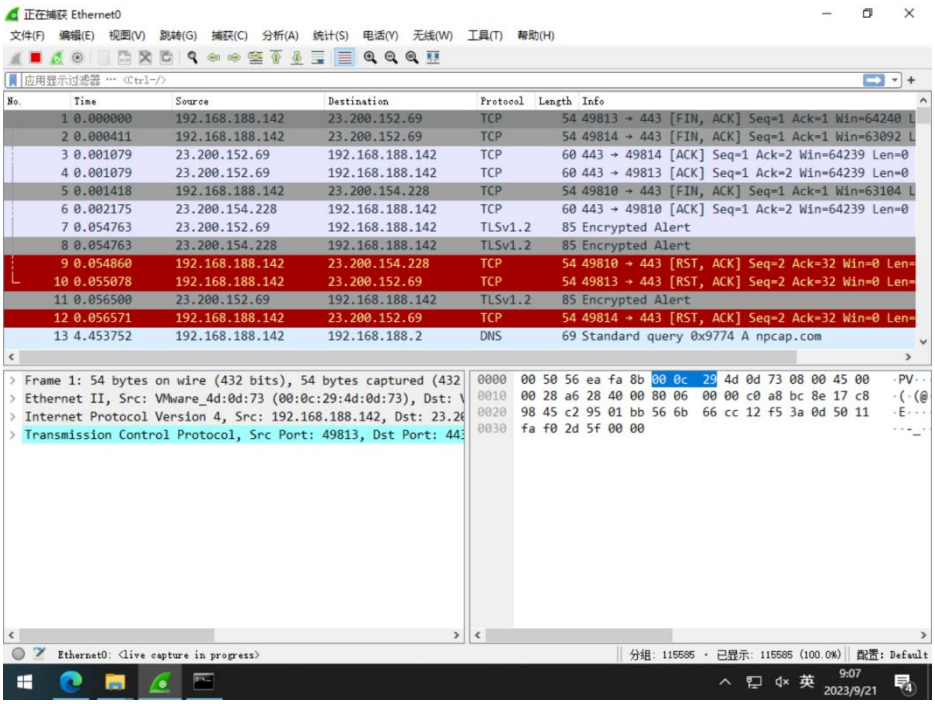
过滤器：Wireshark 允许使用过滤器来筛选和分析特定类型的数据包。这有助于减少数据包数量，使能够专注于感兴趣的流量。

实时分析：可以使用 Wireshark 实时捕获数据包，这意味着可以在网络问题发生时立即对问题进行分析和诊断。

协议统计：Wireshark 提供各种统计信息，包括网络流量统计、协议分布、吞吐量等。这有助于监视网络性能和检测异常情况。

导出数据：可以将捕获的数据包导出为不同的文件格式，如 PCAP、CSV 等，以备将来分析或与其他人共享。

安装 Wireshark：



四、实验结论及心得体会

本次实验安装配置了病毒分析的虚拟机环境；了解了基本静态分析工具和动态分析工具的基本功能，并安装和初步使用了这些工具。