第 2 章 构建恶意软件分析环境

在本章中，我们将介绍如何正确地配置恶意软件分析与逆向工程的分析环境以及恶意软件分析过程中所需的常用工具。为了使分析过程更高效、更简单，读者也可以自行开发新的分析工具。无论是静态分析还是动态分析，分析任何恶意软件都需要在一个安全的环境下进行。通常，刚刚接触恶意软件的分析人员可能会在自己的机器或其他实际的机器上执行恶意软件，这样做会导致机器真的感染恶意软件。严重的情况下，还会感染网络上的其他机器。

除了安全之外，恶意软件分析时另一个需要保证的就是速度。分析恶意软件时，分析人员需要不断重复使用能够演变升级或者支持不同分析目标的相同分析环境。良好的分析环境可以提供快速简便的可重用条件，帮助分析人员重新运行、重新分析恶意软件。

实际上，物理机与虚拟机均可用于恶意软件分析。大多数恶意软件都带有被称为“装甲”的反分析功能（详见第 19 章），例如分析环境检测，以实现检测逃避与对抗分析。与基于虚拟机的分析环境相比，基于物理机的分析环境在对抗反分析技术上更具韧性。基于物理机的分析环境，在底层硬件配置、操作系统状态、文件系统、驱动程序与其他方方面面都与普通用户的系统非常相似。由于和常见的分析环境相差较大，就能够欺骗恶意软件展现真实的攻击意图。基于物理机的分析环境需要依赖能够创建系统还原点的工具，支持在物理系统上创建快照或者还原点的工具如 Windows 系统还原、Clonezilla、Deep Freeze、Time Freeze、Norton Ghost 与 Reboot Restore Rx。

更常见的选择是使用虚拟机构建分析环境。使用虚拟机的一个明显缺点，就是其操作系统、文件系统、驱动程序和其他方方面面都与物理机不同。由于大多数普通用户很少使用虚拟机，恶意软件就会利用这个差异点进行选择性执行，在分析环境中的恶意软件通常会表现出良性行为或者提前退出执行，以此逃避各种检测与分析。尽管如此，使用虚拟机的优点仍然多于

缺点。基于虚拟机的分析环境通常允许暂停系统以及支持创建快照，与基于物理机的分析环境相比，能够快速地对正在运行的系统进行快照。在以后需要时也能够快速恢复到快照的系统状态，这样大大提高了分析人员的分析速度，也使得虚拟机成为了分析人员与基于沙盒的检测方案的首选技术。此外，某些开源虚拟机管理程序（如 Qemu）甚至能够调整模拟的硬件，进一步拉近了与物理机的相似程度。这些都非常有助于使恶意软件认为其正在物理机上执行，而非某些分析人员的虚拟机上执行。本章后续将会重点介绍如何使用虚拟机创建恶意软件分析环境。

主机系统要求

在设置分析环境前，必须要确保部署分析环境的主机满足一些条件：完成所有更新的主机并且具备最低的要求的资源。

尽管是在虚拟机中配置分析环境并且运行恶意软件，但不能就此认为运行虚拟机的宿主机就不会被感染。众所周知，恶意软件也可能会利用底层虚拟机管理平台的漏洞，进入宿主机并实现感染。在配置虚拟机并在其中运行恶意软件之前，就需要确保主机操作系统和虚拟机管理平台都升级到了最新版本并且安装了最新的安全补丁与更新。

对分析虚拟机的另一个要求来自硬件资源，以下是创建与运行分析环境对主机的最低资源要求：

- 为每个虚拟机提供至少 200GB 的可用磁盘空间。分析环境需要足够的磁盘空间来创建虚拟机与保存多个分析阶段的多个快照，大多数情况下 200GB 的磁盘空间就足够了。
- 为每个虚拟机提供至少 4GB 的可用内存。
- 提供更高转速的机械硬盘（HDD），最好是固态硬盘（SSD）。在分析过程中需要快速挂起虚拟机、创建快照、恢复快照，更快的硬盘读写速度就可以提高分析的速度和效

率。

网络要求

如前所述，恶意软件有可能会感染宿主机，因此拥有一个完整更新的宿主机十分重要。但如果宿主机与宿主机上运行的恶意软件分析虚拟机都连接到本地网络中，本地网络中的其他台式机、笔记本电脑等设备，也会面临被分析虚拟机中运行的恶意软件所攻击的风险。尽管部署虚拟机的宿主机可能已经更新到最新版本并且安装了全部的安全补丁，但网络中的其他设备可能并未做到这一点。这些设备可能存在未修复的漏洞，可以被从分析虚拟机内部运行的恶意软件攻击并实现感染。

将分析虚拟机与宿主机所在的网络与本地其他设备所在的网络隔离开，是非常重要的。对于在公司里进行恶意软件分析的分析人员来说就更是如此，公司内部必须有一个隔离的网络用用于恶意软件分析，这样才能够保护公司内其他的设备。

除了将宿主机部署于隔离网络之外，VMware Workstation 和 VirtualBox 等虚拟机管理平台也提供了为虚拟机创建隔离的、只有分析虚拟机与宿主机的网络配置方案。这通常来说是安全的，但并非万无一失。恶意软件仍然可以通过该网络连接到宿主机，利用宿主机的漏洞将其感染，再通过宿主机传播到本地网络上的其他设备。仅主机网络模式也有缺点，主要是缺乏互联网连接。分析恶意软件时，通常需要在有互联网连接的情况下捕获恶意软件的命令与控制通信以及其他网络数据包，以供分析人员进一步分析。

想要保护分析场所的安全，一定要确保分析虚拟机与宿主机的设备位于隔离的网络。并且该网络内只有保存与恶意软件分析相关的设备与机器，不存在任何重要的设备与机器。

创建恶意软件分析虚拟机

在创建与运行虚拟机的管理平台或者模拟器这方面选择很多，有付费软件也有免费软件，甚至也有开源软件。最为常见的三个当属VirtualBox、VMWare Workstation与QEMU/kvm。本书中建立分析环境使用的是 VMWare Workstation，读者可以自行使用任何同类工具。本书不会介绍从头创建虚拟机的过程，互联网上有非常多的相关内容可以提供帮助。以下是创建分析虚拟机时需要注意的要点：

- 使用 32 位 Windows 7 作为分析虚拟机的操作系统。本书中使用的所有练习，都会使用 32 位 Windows 7 作为基础环境。大多数软件都是 32 位的，但也确实存在 64 位的恶意软件。在需要时，也可以使用 64 位 Windows 7 重新配置一个新的分析虚拟机。本书中分析虚拟机的配置方法，对 64 位操作系统仍然适用。
- 最好配置另一个 Windows XP SP2+的分析虚拟机。尽管大多数恶意软件都在 Windows 7 上运行，但也有部分恶意软件只能在 Windows XP 上运行。某些恶意软件也可能使用反分析技术或者使用只能在Windows XP 上进行分析的库文件，这些都使得分析人员不得不使用 Windows XP。如果可能，请将 Windows XP 的分析虚拟机也留作备用。
- 设置至少两核的 CPU、150GB 硬盘空间与 4GB 内存，设置资源时要留意宿主机上的可用内存量。
- 安装 Guest Additions 工具。
- 在完成所有调整与分析工具的安装后，保留分析虚拟机的快照状态。

图 2- 1 显示了使用 VMware Workstation 安装分析虚拟机的硬件配置。

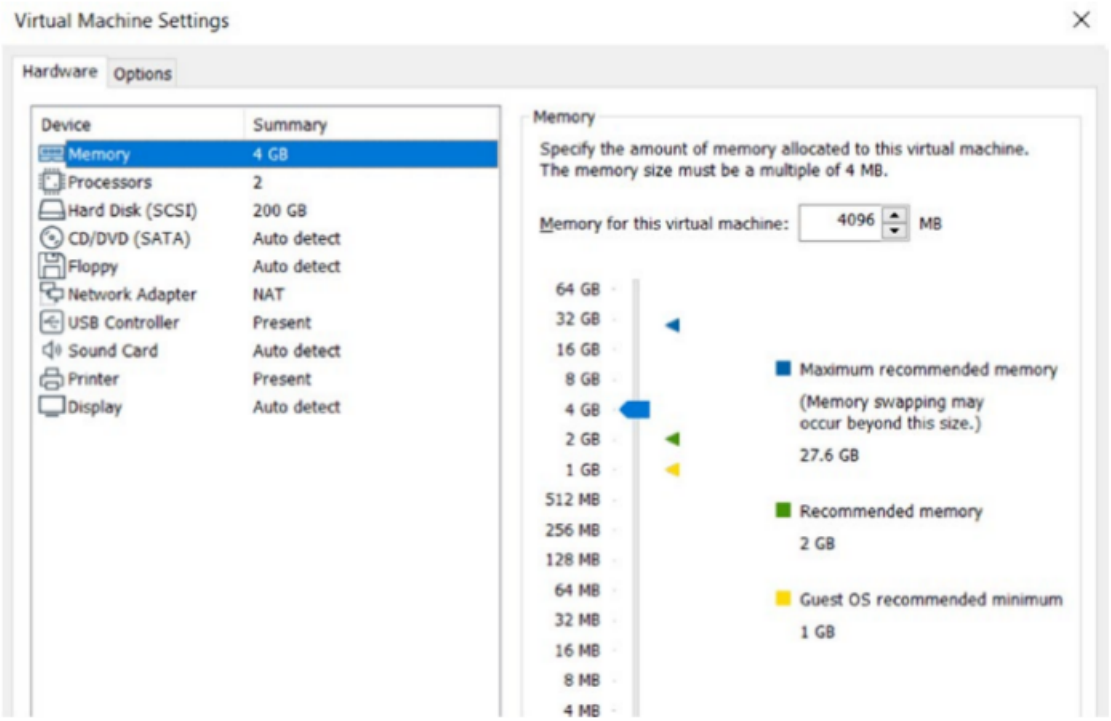

图 2- 1

调整分析虚拟机

在原始配置条件下，不能很好地满足分析恶意软件的需求。接下来，将会逐一介绍如何调整分析虚拟机使其更加适合样本分析，帮助提高分析工作的韧性与效率。

禁用隐藏的扩展名

默认情况下，Windows 系统不显示文件扩展名。尽管在 Windows 资源管理器中不显示文件扩展名显得干净整洁，但恶意软件会利用这一点来欺骗用户点击执行，从而感染系统。后面的章节中，将会详细介绍这一点。用户可以通过取消选中文件资源管理器选项中的”隐藏已知文件类型的扩展名“选项来禁用文件扩展名隐藏，如图 2- 2 所示。

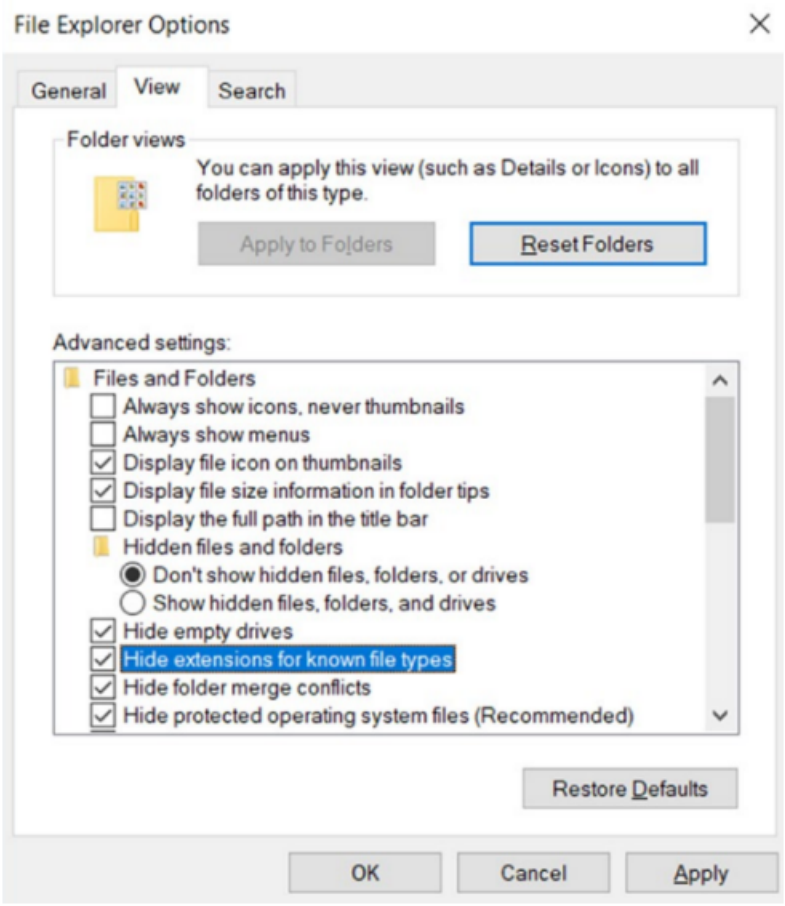

图 2- 2

显示隐藏的文件与文件夹

默认情况下，某些被配置位隐藏的文件与文件夹不会在 Windows 中被显示。用户也可以配置任意文件或文件夹选项，使其在 Windows 资源管理器中隐藏。恶意软件会在系统上创建文件或文件夹时滥用此特性，将其属性设置为隐藏即可在 Windows 资源管理器中不可见。用户可以通过启用“文件夹选项”中的“显示隐藏的文件、文件夹和驱动器”选项，来使系统中所有隐藏的文件与文件夹都可见。或者也可以启用“文件资源管理器选择”中的“显示隐藏的文件、文件夹和驱动器”，如图 2- 3 所示。

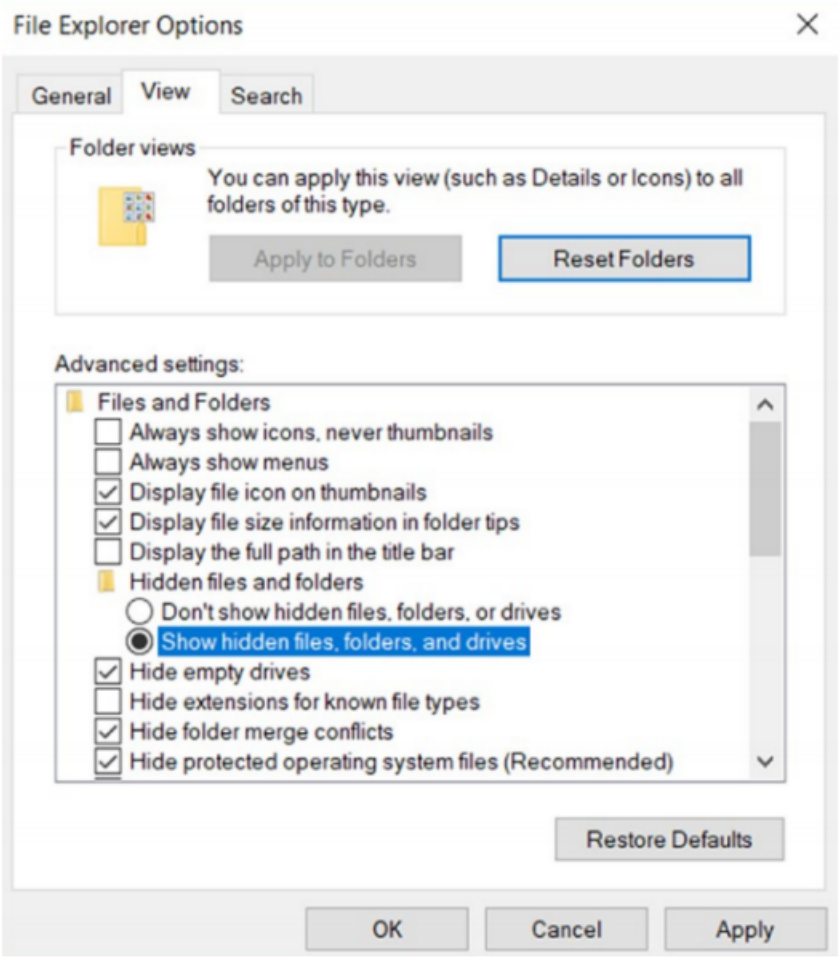

图 2- 3

禁用地址空间布局随机化

地址空间布局随机化（也被称为 ASLR），是一种随机化可执行代码（包括 DLL 文件）使用的内存地址以阻止攻击者在发现程序中的漏洞时攻击系统的安全功能。尽管该功能在 Windows 上是默认启用的，但攻击者也已经开发出绕过此保护机制的技术。从恶意软件逆向分析的角度来看，为了提高分析效率，最好禁用 ASLR 以使每次执行时相同的样本文件与 DLL 文件都有相同的内存地址。

要在 Windows 7 中禁用 ASLR，必须在注册表 HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\下创建一个类型为 REG_DWORD 且值为 0 的 MoveImages DWORD 键，

如图 2- 4 所示。

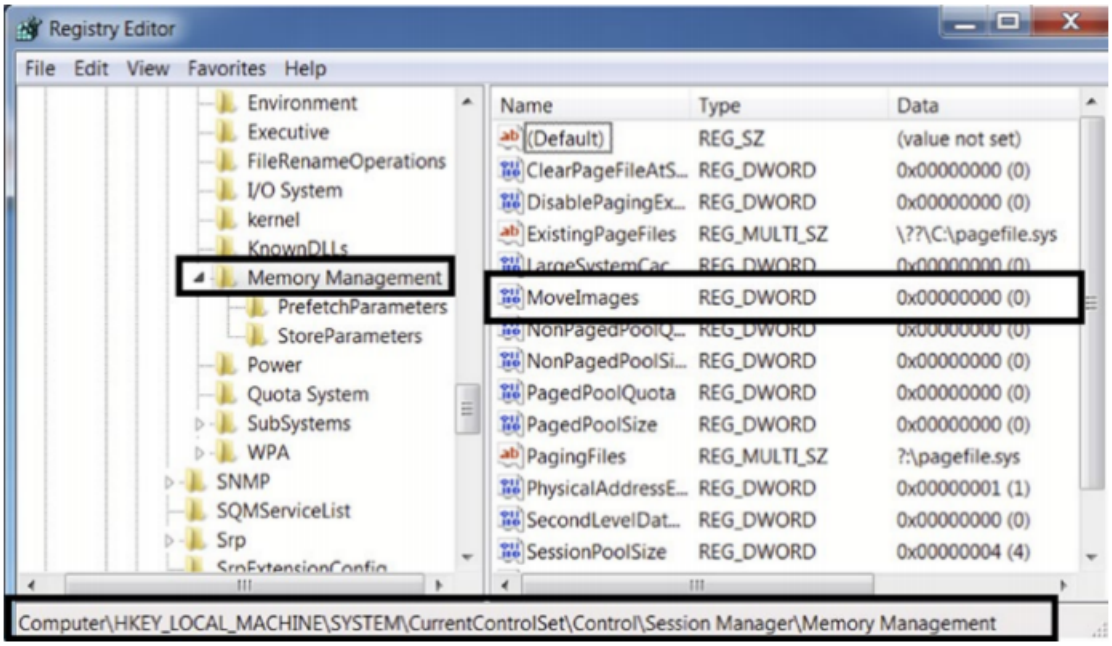

图 2- 4

禁用 Windows 防火墙

Windows 自带了一个防火墙，用于保护设备免受恶意网络连接的侵害。但 Windows 防火墙会阻碍正常的样本分析工作，最好在分析虚拟机中禁用它，如图 2- 5 所示。

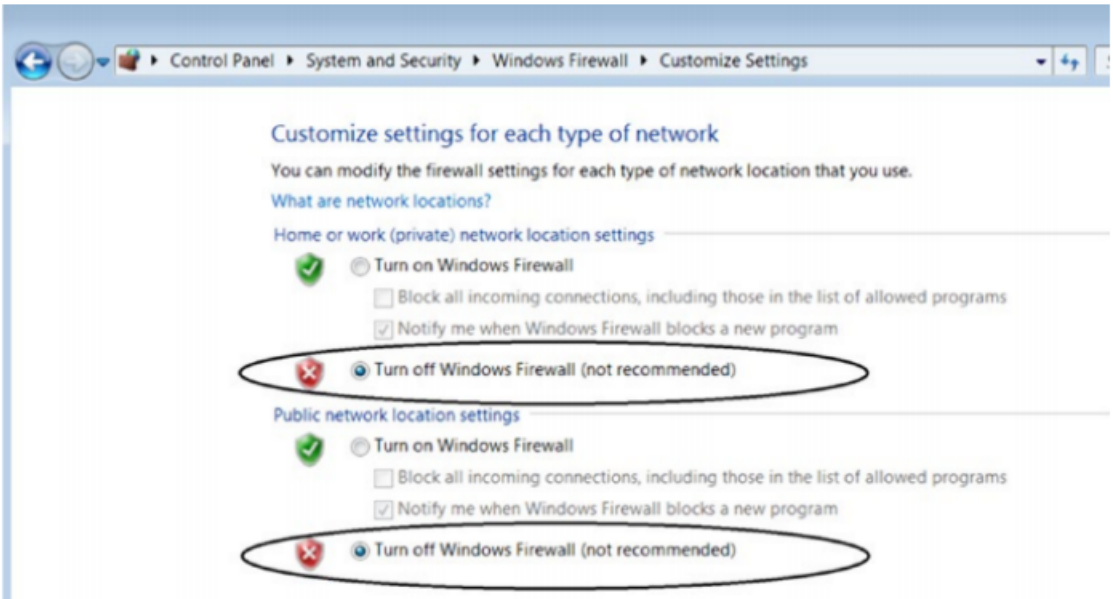

图 2- 5

禁用 Windows Defender 以及各种反病毒软件

任何反病毒软件通常都会有实时扫描与文件隔离功能。安装在分析虚拟机中，则会删除复制到虚拟机中用于分析的恶意样本文件。分析人员需要禁用所有反病毒软件与其实时防护，包括 Windows Defender，如图 2- 6 所示。

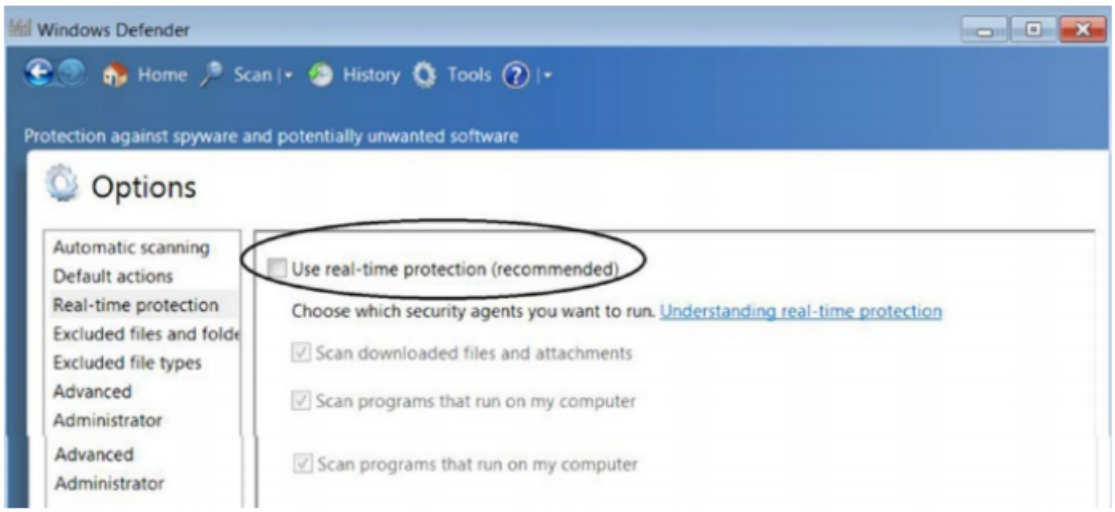

图 2- 6

模拟普通用户

世界上大多数普通用户都不使用虚拟机，而是使用安装在台式机与笔记本电脑等物理机上的操作系统，虚拟机主要由高级用户、开发人员、工程师与恶意软件分析人员使用。恶意软件开发者也意识到这种差异，试图通过开发具有反分析技术的恶意软件来利用这一点。这些反分析技术旨在检测底层操作系统环境是否用于恶意软件分析，如果确定则表现出良性行为或者直接退出，通过隐藏全部恶意行为来逃避分析，只保留最少的痕迹。为了对抗反分析技术，分析人眼应该对分析虚拟机的环境进行调整，使其看起来与普通用户的使用环境非常相似。需要针对分析虚拟机进行调整的主要内容有：

- 硬盘大小。大多数笔记本电脑都会配备 500GB 到 1TB 的硬盘。尽管前文介绍可以将 150GB 作为硬盘大小开始分析，但虚拟机实际上支持更大的硬盘。如果可能，在创建

分析虚拟机时可以配置尽可能大的硬盘大小。

- 内存大小。大多数笔记本电脑都会配备至少 4GB 的内存。4GB 内存确实是保证分析虚拟机拥有流畅工作环境的下限，但这也有助于让环境看起来更像普通用户的环境。
- 安装普通用户使用的软件。众所周知，恶意软件会检查系统上是否安装了一些常见软件，例如 Chrome、Firefox 等浏览器、Adobe Acrobat PDF Reader 等 PDF 阅读器、Microsoft Office 等生产力工具与媒体文件播放器等。
- 部署 PDF 文档、Word 文档、PowerPoint 文档、视频文件、音频文件、文本文件与图像文件等虚拟文件。恶意软件可能会扫描文件系统检查这些文件是否存在，系统上存在这些虚拟文件可以让分析虚拟机看起来更像普通用户的系统。
- 已经安装的软件，例如 Microsoft Office、PDF 阅读器与 Chrome 浏览器，需要打开对应关联的文件留下部分文件打开历史记录。部分恶意软件会检查这些流行软件的文件打开历史记录，以确定有用户在使用这些软件。

快照

配置分析虚拟机时一个很重要的部分就是快照。按照前述内容将操作系统安装并调整、将所有分析工具安装后，就应该暂停虚拟机并创建快照。该快照即为基础快照，当要开始分析恶意软件时就需要恢复到该快照。如果需要对分析虚拟机进行更多调整或者安装更多分析工具，都应该在基础快照之上进行修改。首先恢复上一个基础快照，进行相关调整或者安装新的分析工具，再次创建一个全新的基础快照来保存此时的状态。如图 2- 7 所示，为一个分析虚拟机的配置示例，其中包含两个基础快照。

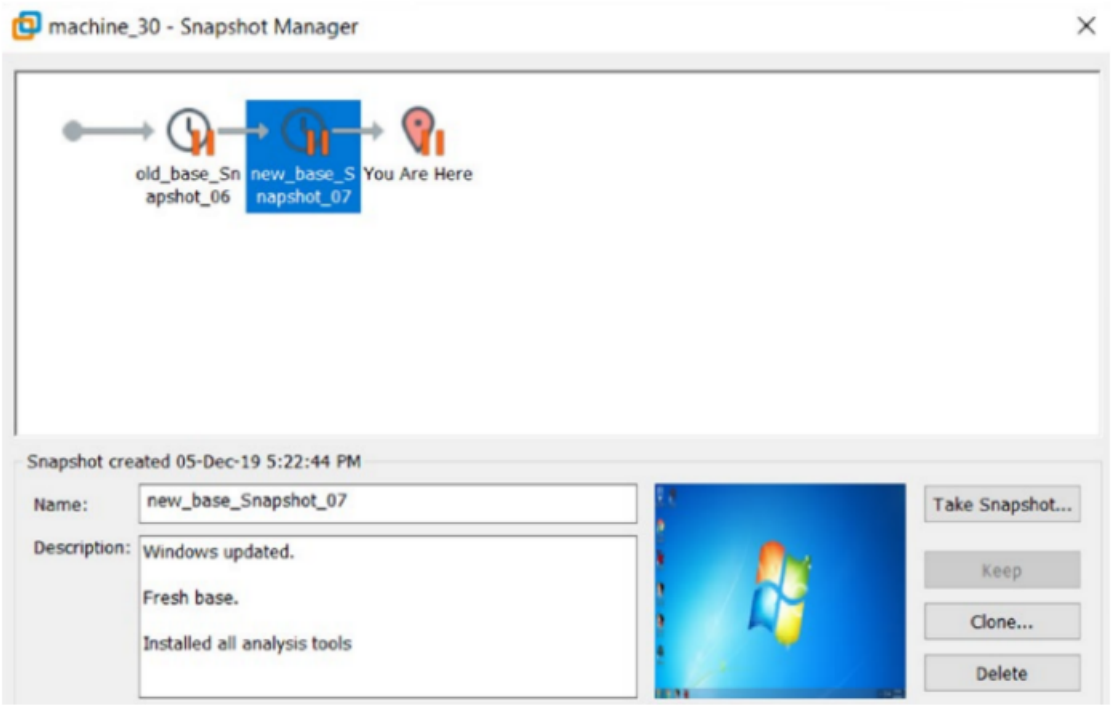

图 2- 7

分析工具

恶意软件分析需要各种各样工具的辅助，分析工具有免费的也有付费的。本章接下来将简要介绍在分析虚拟机上需要安装的各种分析工具，并且在后续章节中介绍这些分析工具的用法。部分分析工具会在安装时创建桌面快捷方式，也有分析工具直接提供独立使用的二进制可执行文件，后者就需要用户手动创建桌面快捷方式或者添加到系统路径。有些分析工具并没有图形化界面，需要通过命令提示符运行。

如果一个分析工具具备图形化界面且没有提供安装程序，只提供了独立使用的二进制可执行文件，用户就可以通过右键选中该文件并选择 Send to➢Create Desktop Shortcut 为其创建桌面快捷方式，如图 2- 8 所示。

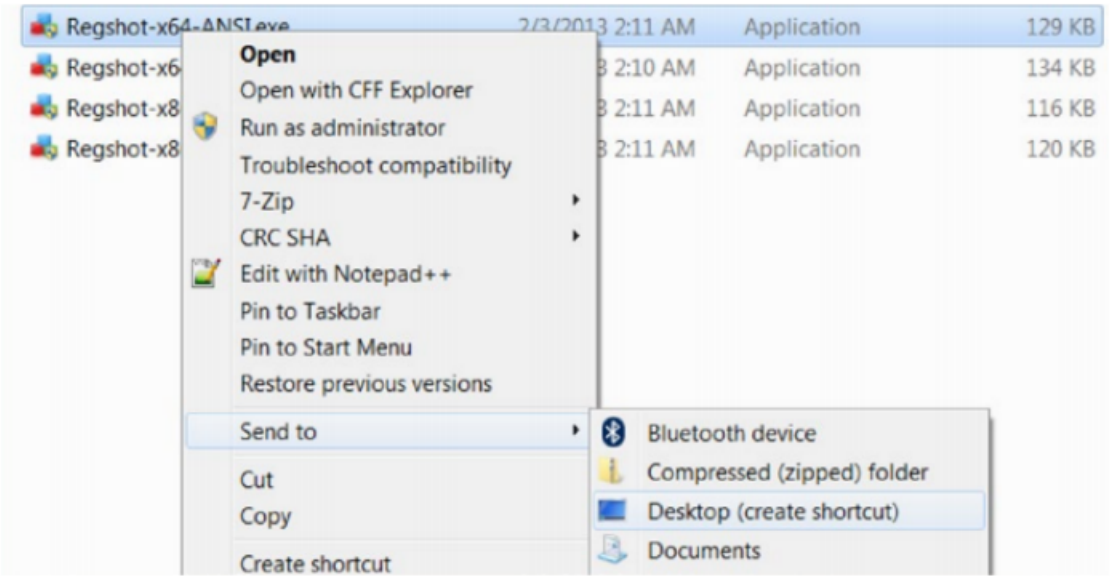

图 2- 8

注：在配置好分析虚拟机并安装了本章介绍的所有分析工具后，请挂起虚拟机并创建虚拟机的快照，该快照会作为后续所有分析工作的基础快照。

如果一个分析工具没有图形化界面且没有提供安装程序，只提供了命令行使用的二进制可执行文件，用户必须将包含该工具的二进制可执行文件的文件夹路径添加到系统的 PATH 环境变量中，如图 2- 9 所示。

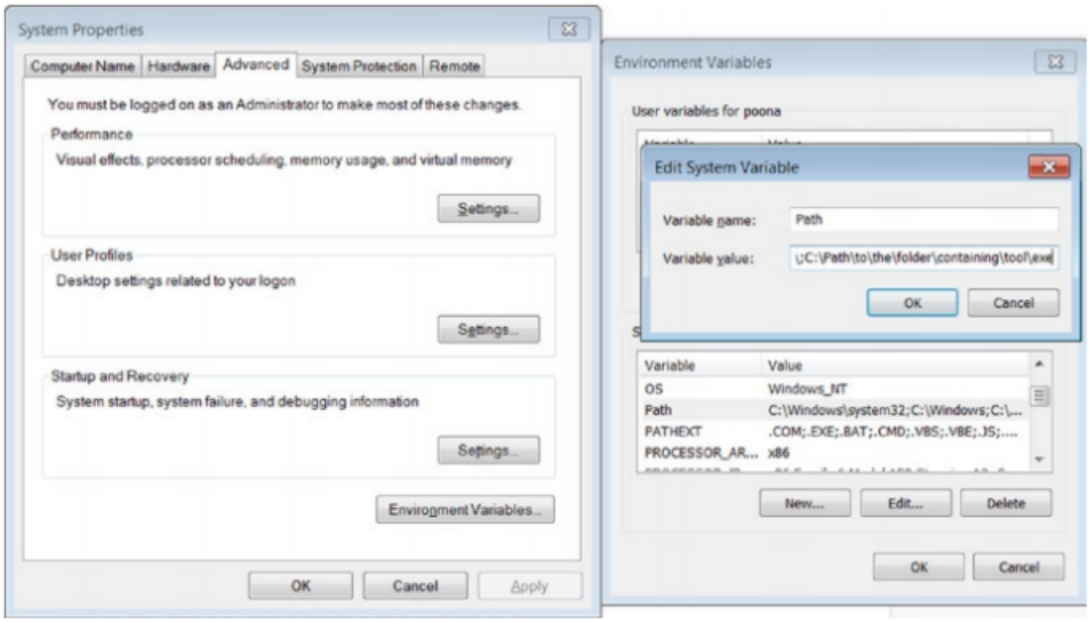

图 2- 9

哈希计算：HashMyFiles 等

基于不同的平台，用户可以使用不同的哈希计算工具。HashMyFiles 可能是 Windows 平台上的最佳工具之一，可以通过 www.nirsoft.net/utils/hash_my_files.html 下载包含该软件可执行文件的压缩包，用户可以为其创建桌面快捷方式。

尽管 HashMyFiles 已经能够满足哈希计算的需求，但用户也可以安装另一个名为 QuickHash 的应用程序，后者可以针对文件或者原始数据计算 MD5、SHA1 与 SHA256 哈希值。用户可以通过 https://quickhash-gui.org 下载包含该软件可执行文件的压缩包，并为其创建桌面快捷方式。

此外，Windows 系统上还可以使用 md5deep 工具套件，其中带有三个命令行工具：md5deep 、 sha1deep 与 sha256deep 。 用 户 可 以 通 过 https://sourceforge.net/projects/md5deep/下载包含该软件可执行文件的压缩包，解压后的路径必须手动添加到系统的 PATH 环境变量中。

Linux 系统中，可以使用自带的命令行工具：md5sum、sha1sum 与 sha256sum。顾名思义，这些程序分别用于根据文件计算对应的 MD5、SHA1 与 SHA256 哈希值。

APIMiner

APIMiner 是本书的作者在撰写本书时开发的 API 日志记录工具，只能通过命令行使用。该工具旨在帮助用户加快获取恶意软件 API 日志的效率，可以直接在分析虚拟机上运行且不需要单独的沙盒。用户可以通过 https://github.com/poona/APIMiner/releases 下载包含该软件的压缩包，撰写本书时最新版本为 1.0.0。压缩包中的 README.txt 文件中，介绍了如何在分析虚拟机中使用该工具。

PE 文件分析：CFF Explorer 与 PEView

CFF Explorer 是一个常用的 PE 文件解析工具，通常作为 Explorer Suite 工具包的一部分提供。用户可以通过 https://ntcore.com/?page_id=388 下载 Explorer Suite 的安装程序来安装 CFF Explorer。想用通过 CFF Explorer 解析文件，可以右键单击任意二进制可执行文件并选择使用 CFF Explorer 打开。

与 CFF Explorer 类似，PEView 也是常用的 PE 文件解析工具。用户可以通过 http://wjradburn.com/software/下载包含该软件可执行文件的压缩包，并为其创建桌面快捷方式。

文件类型识别

通常使用两个分析工具来实现对文件类型的识别。在 Linux 系统上，用户可以使用预装在 Ubuntu 等常用发行版的命令行工具 file。另一个可用的 Linux 命令行工具是 trid，而 trid 在 Windows 系统上也可以使用。用户可以通过　下载包含该软件可执行文件的压缩包，解压后的路径必须手动添加到系统的 PATH 环境变量中。与 file 类似，trid 也是通过签名数据库来识别文件类型的。trid 的签名数据库也需要一同下载，并将其命名为 TrIDDefs.trd 且移动到与 trid.exe 可执行文件相同的文件夹中。

尽管 trid.exe 是命令行工具，但开发者也提供了名为 TriDNet 的图形化界面替代方案，可以在相同的网址下载使用。与命令行工具类似，TriDNet 也需要使用签名数据库。用户需要将数据库的文件(名为 defs 的文件夹)，移动到与 TriDNet.exe 可执行文件相同的文件夹中。

Process Hacker、Process Explorer、CurrProcess

Process Hacker、Process Explorer 与 CurrProcess 都是可视化查看系统状态的分析工具，

包括显示正在运行的进程、进程对应的线程、正在运行的服务、建立的网络连接、磁盘的利用情况、每个进程加载的 DLL 文件等。使用得当的情况下，使用这些工具可以显示各种与进程相关的信息，能够帮助分析人员分析恶意软件。用户可以通过 https://processhacker.sourceforge.io/ 下载 Process Hacker；通过 https://docs.microsoft.com/en-us/sysinternals/downloads/process explorer 下载 Process Explorer；通过 www.nirsoft.net/utils/cprocess 下载 CurrProcess。这些工具都以包含该软件可执行文件的压缩包的形式提供，需要用户为其创建桌面快捷方式。

进程分析工具：ProcMon

ProcMon 是一个常见的进程分析工具，能够捕获并显示系统上运行的进程的各类活动，包括进程与线程的创建、网络行为、文件操作（如文件创建与文件删除等）、注册表操作等。用户可以通过 https://docs.microsoft.com/en-us/sysinternals/downloads/procmon 下载包含 ProcMon 可执行文件的压缩包，再为其创建桌面快捷方式。

Autoruns

许多恶意软件都会通过持久化机制来实现在系统重启或者用户重新登录后，仍然维持自身存在并自动运行。Autoruns 旨在发现恶意软件所使用的持久化机制，提供系统启动时或用户登录时运行的所有程序的列表。用户可以通过 https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns 下载包含 Autoruns 可执行文件的压缩包，再为其创建桌面快捷方式。

Regshot

Regshot 是注册表比对分析工具，允许用户拍摄 Windows 注册表的快照并在快照之间进

行对比，以显示注册表的变化差异。用户可以通过https://sourceforge.net/projects/regshot/下载包含 Regshot 可执行文件的压缩包，再为其创建桌面快捷方式。

NTTrace

NTTrace 与 Linux 系统上的 Strace 类似，能够记录 Windows 系统上进程的本机 API 调用。默认情况下，NTTrace 记录那些针对 ntdll.dll 对外提供的 Windows API 的调用。NTTrace 可以跟踪一个新创建的进程，也可以附在一个已经运行的进程上进行跟踪。特别的，NTTrace 可以跟踪子进程并且能够处理多线程进程。尽管在本书中使用了其他 API 监控工具（例如 APIMiner），但 NTTrace 也可以作为这些工具的有力替代。NTTrace 是一个命令行工具，用户可以通过 www.howzatt.demon.co.uk/NtTrace/下载包含 NTTrace 可执行文件的压缩包，并且解压后的路径必须手动添加到系统的 PATH 环境变量中。

FakeNet

FakeNet 是 Windows 平台下的网络分析工具，能够拦截并记录恶意软件发出的网络请求并返回模拟响应，从而控制恶意软件与外部网络进行连接。与此同时，FakeNet 还使恶意软件认为其仍然可以连接到外部网络并与攻击者控制的服务器进行通信。FakeNet 能够使用自定义的 HTTP 与 DNS 服务器来对网络请求进行响应。用户可以通过https://sourceforge.net/projects/fakenet/下载 FakeNet 可执行文件，并为其创建桌面快捷方式。

BinText

BinText 是一个从文件中提取 ASCII 和 Unicode 文本字符串的静态分析工具。如图 2- 10

所示，BinText 的高级视图提供了从文件中提取的各种文本字符串的内存地址。

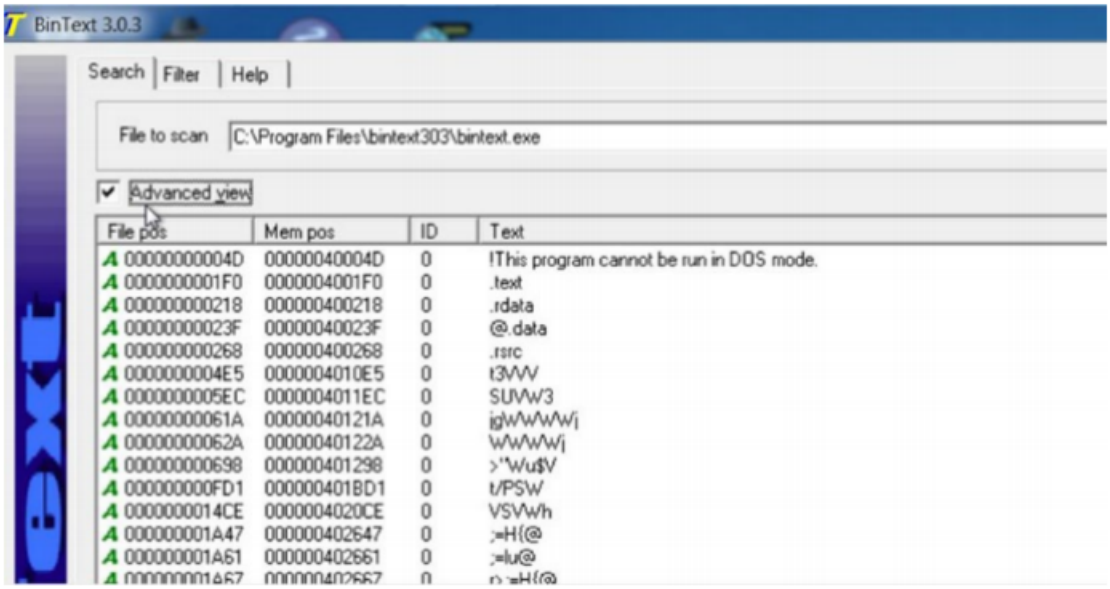

图 2- 10

BinText 是一个图形化界面分析工具，用户可以通过 http://b2b-download.mcafee.com/products/tools/foundstone/bintext303.zip 下载包含 BinText 可执行文件的压缩包，并为其创建桌面快捷方式。

Yara

Yara 被称作恶意软件分析人员在模式匹配上的瑞士军刀，主要用于检测与分类恶意软件。Yara 支持分析人员创建基于静态模式的签名，然后针对文件、文件夹或者正在运行的进程进行扫描并显示能够匹配命中的签名，如图 2- 11 所示。用户可以通过 https://virustotal.github.io/yara/下载包含 Yara 可执行文件的压缩包，并且解压后的路径必须手动添加到系统的 PATH 环境变量中。

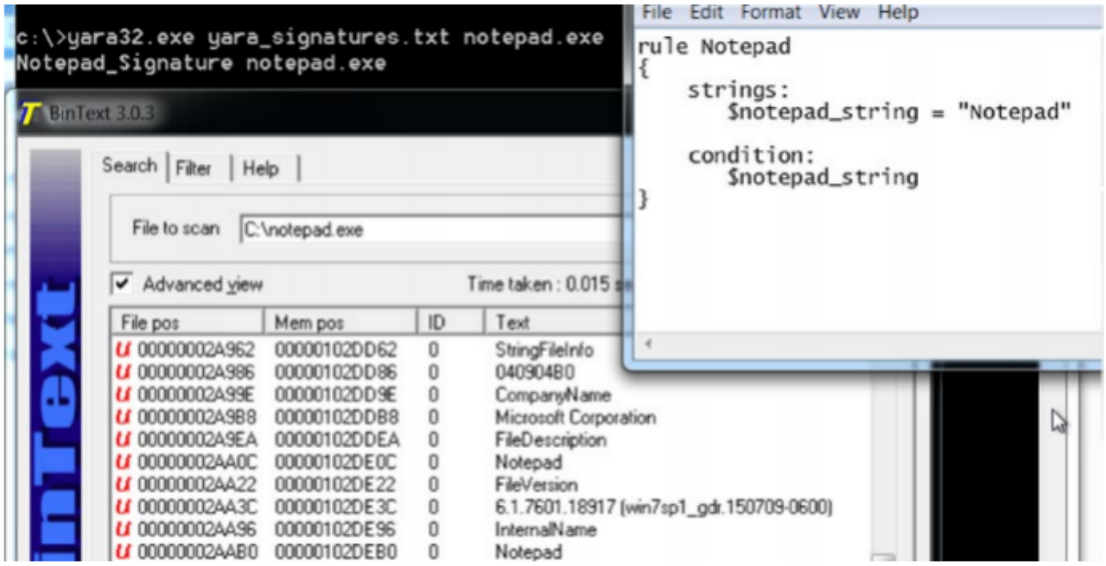

图 2- 11

Wireshark

Wireshark 是一个图形化数据包分析工具，可以捕获与分析实时网络流量或者针对静态数据包捕获文件（PCAP 文件）进行分析。Wireshark 支持解码各种协议并提供了内置的数据包过滤功能，这可以帮助分析人员快速处理各种网络流量。Wireshark 是一款分析人员必备的分析工具，它不仅能够分析恶意软件流量，也可以用于解决任何与网络相关的问题。用户可以通过 www.wireshark.org 下载 Wireshark 的可执行文件。

Microsoft Network Monitor

Microsoft Network Monitor 是微软开发的一款图形化数据包分析工具，可用于捕获、解码、查看与分析网络协议。尽管其功能与 Wireshark 十分相似，但二者的区别在于 Microsoft Network Monitor 能够提供发起网络通信的进程 PID。这一点对恶意软件分析非常有用，可以在执行恶意软件及其子进程时查看流量的来源。尽管 Microsoft Network Monitor 已经被 Microsoft Message Analyzer 所替代，但用户仍然可以通过 www.microsoft.com/en-in/download/details.aspx?id=4865 下载获取。

OllyDBG 2.0

OllyDbg 可以说是每个恶意软件分析人员必备的工具。OllyDbg 是一个图形化界面的 x86 调试工具，可以在 Windows 系统上执行并调试 x86 可执行文件。该工具是免费的，用户可以通过 www.ollydbg.de/version2.html 下载包含 OllyDbg 可执行文件的压缩包，再为其创建桌面快捷方式。

请注意，使用 OllyDbg 必须使用管理员权限。尽管 OllyDbg 看起来像是专业恶意软件分析人员才能使用的高级工具，但其实它在各种恶意软件分析场景中都大有可为。对初级恶意软件分析人员来说，OllyDbg 也是十分有用的分析工具，在后续章节中将会进行介绍。

Notepad++

Notepad++是 Windows 平台的文本编辑器，可用于查看与编辑 ASCII 与非 ASCII 文件，甚至是可执行文件。Notepad++的 HEX-Editor 插件提供了一个易于使用的界面来帮助用户可视化查看任何类型的文件，无论是 ASCII 的普通文件还是非 ASCII 的二进制可执行文件，并对其进行修改。可用的十六进制编辑器很多，例如 Hiew/Far Manager、Emacs 与 VIM，但 Notepad++为初级恶意软件分析人员提供了一个易于使用的、学习成本较低的文本编辑器与十六进制编辑器。用户可以通过 https://notepad-plus-plus.org/下载 Notepad++进行使用，如图 2- 12 所示为 Notepad++使用 HEX-Editor 插件打开文件。

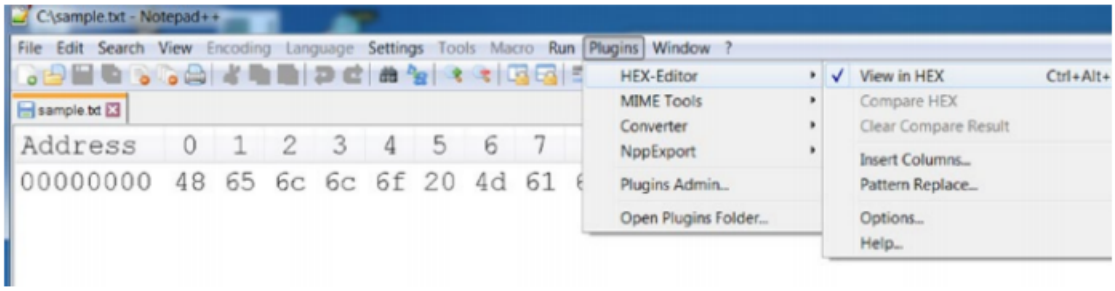

图 2- 12

Malzilla

Malzilla 是一个用于分析恶意 JavaScript 代码的图形化界面分析工具。用户可以通过 www.malzilla.org/downloads.html 下载包含 Malzilla 可执行文件的压缩包，再为其创建桌面快捷方式。

PEiD

PEiD 是一个解析 PE 文件方方面面（例如加壳程序、熵值等）的分析工具。用户可以下载包含 PEiD 可执行文件的压缩包，再为其创建桌面快捷方式。

FTK Imager Lite

FTK Imager Lite 是一个用于转存系统内存的分析工具，在本书的第 14 章中将会进行详细介绍。用户可以通过 https://accessdata.com 下载包含最新版本 FTK Imager Lite 可执行文件的压缩包，再为其创建桌面快捷方式。

Volatility

本书的第 14 章介绍了名为 Volatility 的内存取证工具，以及使用该工具进行内存取证的各种操作。本书使用的是该工具的独立版本 Volatility Standalone，该版本不需要额外安装 Python 环境。用户可以通过 www.volatilityfoundation.org/26 下载包含 Volatility 可执行文件的压缩包，并且解压后的路径必须手动添加到系统的 PATH 环境变量中，这样才能通过命令提示符进行访问。

Ring3 API Hook Scanner

由 NoVirusThanks 开发的 Ring3 API Hook Scanner 可以用于检测恶意软件或者任何应用程序在系统上配置的 API 钩子，用户可以通过 www.novirusthanks.org/products/ring3-api-hook scanner/下载该工具的安装程序。

GMER

GMER 是一个用于检测用户态 API Hook 和内核态 SSDT Hook 的分析工具。用户可以通过 www.gmer.net 下载包含 GMER 可执行文件的压缩包，再为其创建桌面快捷方式。

SSDTView

SSDTView 是用于查看内核中 SSDT 内容的分析工具，检查 SSDT 函数或者系统上任何应用程序是否存在被恶意软件 Hook 的情况。用户可以通过 www.novirusthanks.org/products/ssdt-view/下载包含 SSDTView 可执行文件的压缩包，再为其创建桌面快捷方式。

DriverView

DriverView 是一个图形化界面分析工具，可以帮助分析人员查看系统中所有已加载的驱动程序，并且检查系统中是否加载了任何恶意软件内核模块或 Rootkit。用户可以通过 下载包含 DriverView 可执行文件的压缩包，再为其创建桌面快捷方式。

Strings

Sysinternals Strings 是一个帮助分析人员转储文件中所有字符串的命令行工具。用户可以

通过 https://docs.microsoft.com/en-us/sysinternals/downloads/strings 下载包含 Sysinternals Strings 可执行文件的压缩包，并且解压后的路径必须手动添加到系统的 PATH 环境变量中。

SimpleWMIView

SimpleWMIView 是一个图形化界面分析工具，可以帮助分析人员运行、查看 WMI 命令的结果。用户可以通过 www.nirsoft.net/utils/simple_wmi_view.html 下载包含 SimpleWMIView 可执行文件的压缩包，再为其创建桌面快捷方式。

Registry Viewer

Registry Viewer 是用于加载、查看使用 Volatility 等内存取证工具记录的注册表转储。用户可以通过 https://accessdata.com 下载安装最新版本的 Registry Viewer。

Bulk Extractor

Bulk Extractor 是一个命令行工具，本书第 14 章中使用 Bulk Extractor 从内存转储中提取网络数据包捕获文件。用户可以通过 http://downloads.digitalcorpora.org/downloads/bulk_extractor/下载安装该程序。

Suricata

Suricata 是一个开源的网络安全监控（NSM）分析工具，可以当作网络入侵检测与防御系统（IDS/IPS）使用。Suricata 可以捕获并处理实时网络流量，或者离线处理数据包捕获文件（PCAP 文件）。Suricata 的规则语法较为丰富，在句法上类似于 Snort 规则。Suricata 支持包括 JSON 在内的多种日志格式来记录有关数据包与各种网络协议的元数据，当

Suricata 的网络侧数据与基于主机端点 Agent 收集的主机侧数据结合时，可以帮助进行威胁检测。在恶意软件分析与威胁检测领域中，Suricata 是解决网络行为分析问题的必备工具。在本书第 21 章中将会介绍，如何在 Linux 系统上下载与安装 Suricata。

Cuckoo Sandbox

恶意软件沙盒在恶意软件动态分析中起着非常重要的作用。Cuckoo Sandbox 是一个开源的恶意软件沙盒，可以在隔离的操作系统中自动运行与分析恶意软件，并且收集有关执行的恶意软件行为的详细分析结果。Cuckoo Sandbox 可以提供有关恶意软件执行的 API 调用的详细信息，包括进程创建、线程创建、文件创建、文件删除、注册表创建、注册表删除与注册表修改的 API 在内的各种 Win32 API。该沙盒还支持转储恶意软件进程内存，并捕获恶意软件的网络通信流量并保存为 PCAP 文件以供分析人员进一步分析。由于 Cuckoo Sandbox 是开源的，分析人员可以对其进行功能修改或者定制化升级。有关如何安装、配置与使用 Cuckoo Sandbox 的内容，请查看示例样本文件库中的 Cuckoo-Installation-And-Usage.txt 文件。

rundll32

rundll32.exe 是 Windows 系统上自带的命令行工具，用于将动态链接库（DLL）文件加载到内存中。许多恶意软件会以 DLL 文件的形式出现，而不是可执行文件。由于在分析恶意 DLL 文件时无法像可执行文件一样直接执行，因此 rundll32.exe 就能够帮助分析人员帮助解决这一问题。分析时借助 rundll32.exe 就可以将 DLL 文件加载到内存中并调用其 DLLMain 函数，或者也可以调用特定的导出函数。

oledump.py

oledump.py 是一个能够解析 Microsoft Office 文件并提取各种数据（包括宏代码和嵌入式二进制文件）的 Python 脚本。该脚本需要通过命令行使用，也必须依赖系统上的 Python 环境，使用前请确保已经安装了 Python 环境。除了基础 Python 环境外，oledump.py 还依赖于另一个名为 OleFileIO 的第三方 Python 包。在基础 Python 环境安装完成之后，再通过 www.decalage.info/python/olefileio 来安装 OleFileIO。用户可以通过 https://blog.didierstevens.com/programs/oledump-py/下载包含 oledump.py 脚本文件的压缩包，解压后的路径必须手动添加到系统的 PATH 环境变量中才能正常使用。

OllyDumpEx

OllyDumpEx 是 OllyDbg 的一个插件，分析人员可以使用其来转储 OllyDbg 正在调试的进程的内存。用户可以通过 https://low-priority.appspot.com/ollydumpex/#download 下载包含 OllyDumpEx 的压缩包，解压即可使用。解压后的文件夹中包含与各种目标工具配合使用的 DLL 插件文件，本书中将其作为 OllyDbg 的插件一同使用，需要找到以 OllyDbg 命名的 DLL 文件，撰写本书时名为 OllyDumpEx_Od20.dll。将该 DLL 文件复制到 OllyDbg 的插件目录，在默认情况下就是包含 ollydbg.exe 文件的根目录。用户也可以通过在 Options ➢ Options ➢ Directories ➢ Plugin Directory 输入插件文件夹的路径来更改 OllyDbg 中的插件目录路径。

DocFileViewerEx

DocFileViewer 是一个图形化界面分析工具，可以解析并查看 Microsoft Doc 文档文件的 OLE 结构，在本书的第 20 章会利用其分析基于 Microsoft Office 的恶意软件。用户可以通

过　　下载该程序，再为其创建桌面快捷方式。

Fiddler

Fiddler 是旨在提供可视化网络数据包捕获分析的工具，可用于分析发起漏洞攻击的恶意 HTTP 请求。本书使用的是 Fiddler 4，读者可以通过 www.telerik.com/download/fiddler/fiddler4 下载并安装该程序。

IDA Pro

IDA Pro 可能是高级恶意软件分析人员最常用的分析工具，既可以静态反汇编又可以进行动态调试。IDA Pro 是一个付费分析工具，可以通过 www.hex-rays.com/products/ida/进行购买。Hex-Rays Decompiler 是一个非常有用的插件，能够将机器码反汇编成人类可读的类 C 伪代码，该插件可以与标准版 IDA Pro 一起购买。官方也提供了 IDA Pro 的免费版本，用户可以通过 www.hex-rays.com/products/ida/support/download_freeware/下载安装，但相比付费版本功能较为有限。

x64dbg 与 Immunity Debugger

x64dbg 和 Immunity Debugger 都是常见的免费调试工具，二者都拥有类似 OllyDbg 的图形化界面且仍然在积极开发更新。x64dbg 是一个与 Sandman 反编译器集成在一起的调试工具，而 Sandman 反编译器也是 IDA Pro Hex Rays 反编译器的良好替代。

总结

开始恶意软件分析的第一步就是配置安全、高效的分析环境。本章介绍了如何建立一个恶意软件分析环境，分析人员可以在其中运行各种恶意软件，而不必担心恶意软件感染主机设备

和网络上的其他主机。为了满足安全、高效的要求，分析环境需要进行一系列基于主机与网络的配置。本章中也介绍了这些对分析虚拟机的配置调整，使分析环境具备更好的适应性。通过安装本章介绍的分析工具，构建了一个具备快照的分析虚拟机，后续可以使用其方便地进行恶意样本分析。