南開大學

恶意代码分析与防治课程实验报告

实验二：虚拟机技术病毒隔离环境的安装与配置

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2111033

姓　　名　艾明旭

班　　级　信息安全一班

一、实验目的

1.　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。

2. 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。

3. 实验一当中已经学习了解了一部分静态分析软件，本次实验我们继续学习其他软件的使用方法，从而达到能够熟练的分析一个应用程序的能力。

4. 实验一已经配置了 win10 虚拟机，但是在实际使用的过程当中，发现有虚拟机带动速度过慢，虚拟机实际使用能力太差，相关病毒软件经常会被防火墙杀死，微软官网尚未停止对 win10 操作系统的更新等等问题。Windows xp 系统较为久远，其相关的防火墙等系统也较差，比较适合我们作为病毒分析的操作系统，不过由于上学期软件安全课程已经使用过了 windows xp 系统，因此我们本学期尝试使用 win8.1 和 win10 操作系统进行相关实验的进行。

二、实验原理

1. 实验环境

Win8.1,win11,win10，VMware

2. 物理原理

VMware 可以有效的并行运行多个虚拟机，本机当中可以使用多核分配给相应的虚拟机，如在 win10 操作系统当中分配 4 个核心，主机仍然能够保持一定的运行速度。

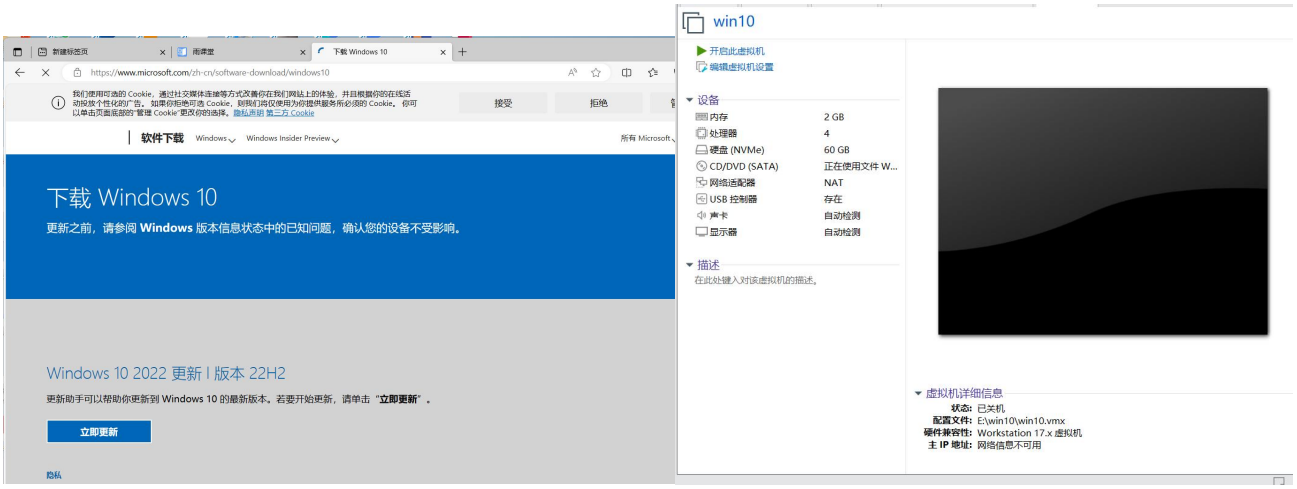
3. 软件适配

由于 windows 操作系统具有向下兼容性，因此我们不需要考虑在 win11 操作系统当中运行的应用程序不会被较低版本的 windows 操作系统运行的情况，所有的应用软件都能有效的被虚拟机操作系统所兼容。我们所要考虑的更多的是例如 ollydbg 专门由于分析 32 位应用程序这些特有的功能，探讨不同软件在面对不同的问题当中有哪些特殊的能力。

三、实验过程

1. win10 虚拟机的配置

首先是在微软官网上下载相关的镜像

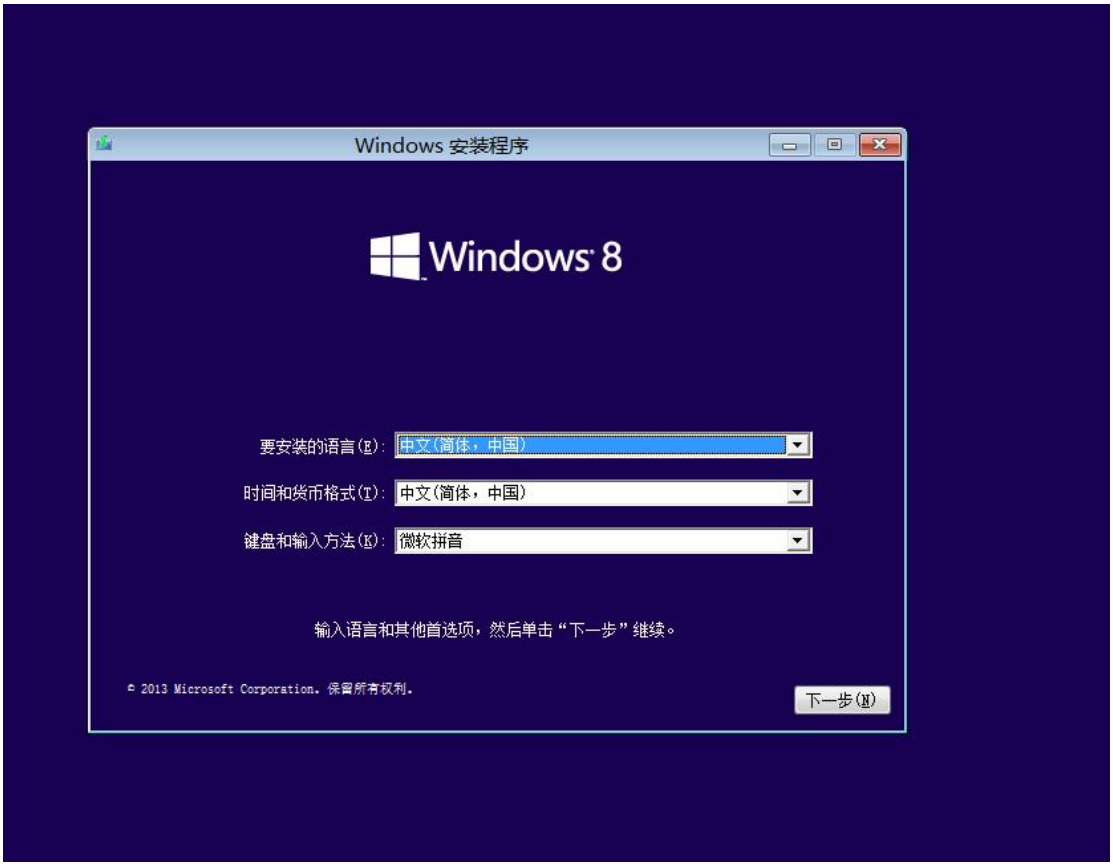


将相关的 win10 操作系统当中的打印机功能取消，CD/DVD 使用本地的镜像，设置内存为 2GB 而处理器为 4，可以有效的使用相关的软件。

Win10 虚拟机并不会自带 VMtools 的功能，因此我们要在虚拟机当中联网下载 VMtools，之后重启虚拟机，更新。

Win10 虚拟机在运行过程当中速度较慢，重启更新需要慢慢等待。在实验一当中尝试了 win10 虚拟机的运行之后，我发现我的计算机在同时运行 win11 主机和 win10 虚拟机时 cpu 处理速度极其缓慢，win10 系统及时我按最大可分配核心分配 cpu 仍然会存在。

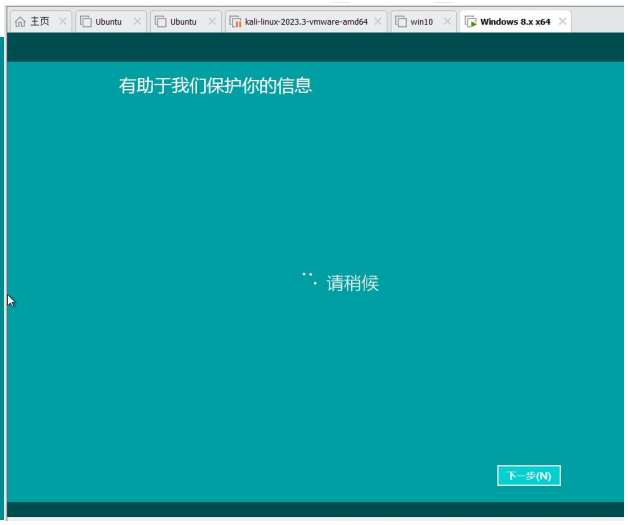
Win8.1 操作系统相对而言所具有的配置项较少，可以有效的运行。

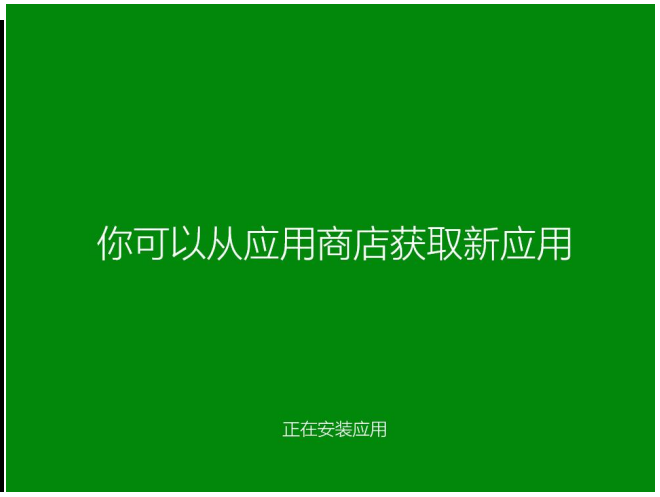

Windows 安装程序
Windows 8
要安装的语言(E): 中文(简体，中国)
时间和货币格式(T): 中文(简体，中国)
键盘和输入方法(K): 微软拼音
输入语言和其他首选项，然后单击“下一步”继续。
© 2013 Microsoft Corporation. 保留所有权利。
下一步(N)

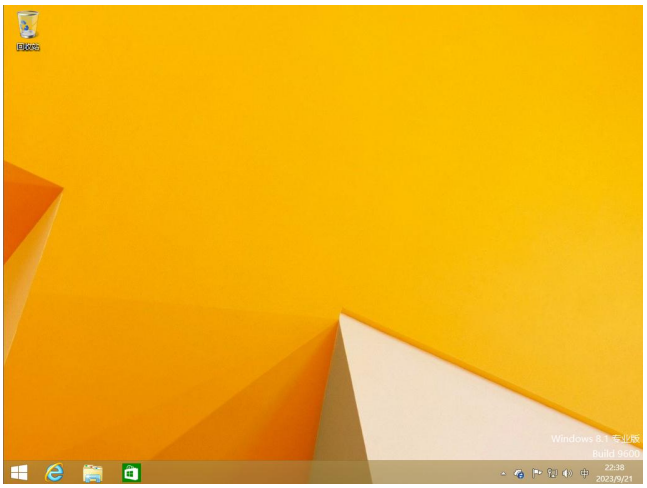

虚拟机设置
硬件
选项
设备
摘要
内存
2 GB
处理器
4
硬盘 (SCSI)
50 GB
CD/DVD (SATA)
正在使用文件 Win8.1_Chines...
网络适配器
NAT
USB 控制器
存在
声卡
自动检测
打印机
存在
显示器
自动检测
添加(A)...
移除(R)
内存
指定分配给此虚拟机的内存量。内存大小必须为 4 MB 的倍数。
此虚拟机的内存(M): 2048 MB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
最大建议内存
(超出此大小可能发生内存交换。)
13.3 GB
建议内存
2 GB
建议的最小客户机操作系统内存
2 GB
必须先关闭虚拟机，才能降低内存量。
确定
取消
帮助


虚拟机设置
硬件
选项
设备
摘要
内存
2 GB
处理器
4
硬盘 (SCSI)
50 GB
CD/DVD (SATA)
正在使用文件 Win8.1_Chines...
网络适配器
NAT
USB 控制器
存在
声卡
自动检测
打印机
存在
显示器
自动检测
添加(A)...
移除(R)
设备状态
已连接(C)
启动时连接(O)
连接
使用物理驱动器(P):
自动检测
使用 ISO 映像文件(M):
Win8.1_Chinese(Simplified)_x6
浏览(B)...
高级(V)...
确定
取消
帮助

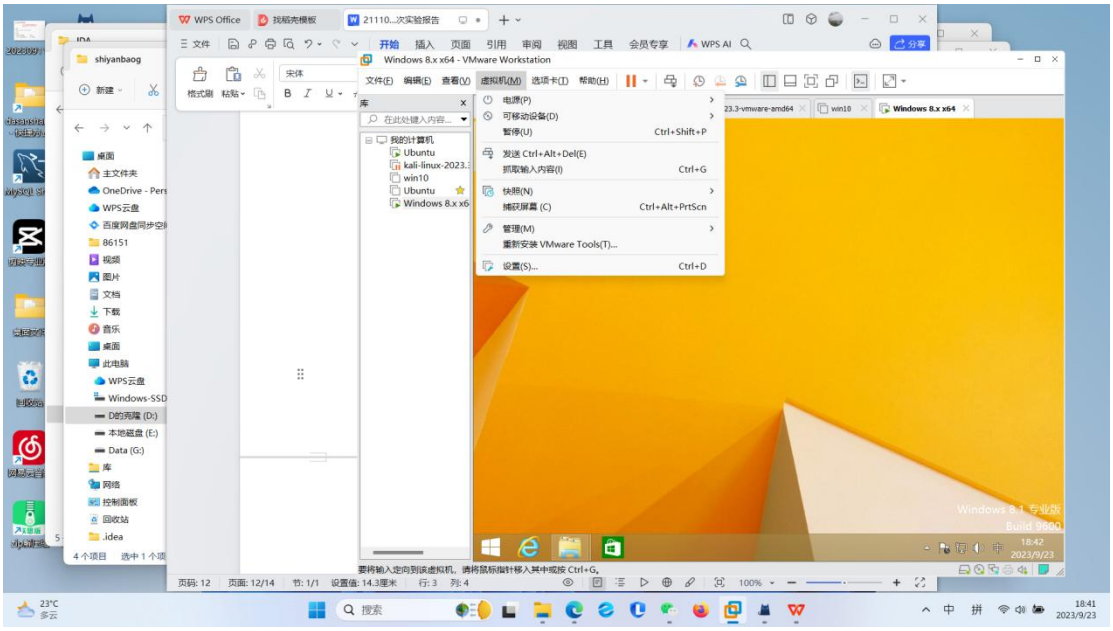

Windows 安装程序
输入产品密钥以激活 Windows
它应该在 Windows 包装盒的背面，或者在表明你购买了 Windows 的电子邮件中。
产品密钥像这样：XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
将自动加上短划线。
隐私声明(I)
下一步(N)
Windows 安装程序
正在安装 Windows
你的计算机将重启几次，这可能需要一点时间。
正在复制 Windows 文件
正在准备要安装的文件 (0%)
正在安装功能
正在安装更新
正在完成



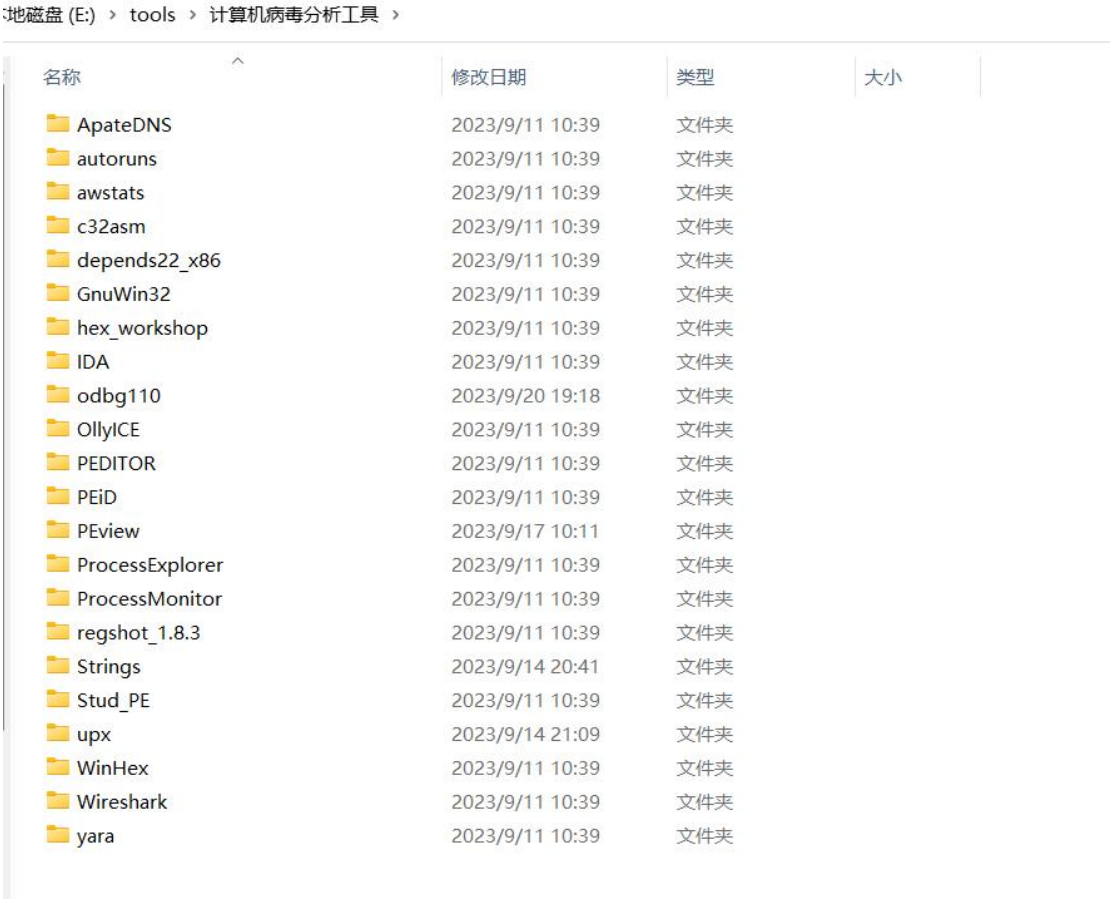




安装 VMtools 之后我们就可以方便的将文件自由的在主机与虚拟机之间拖动。



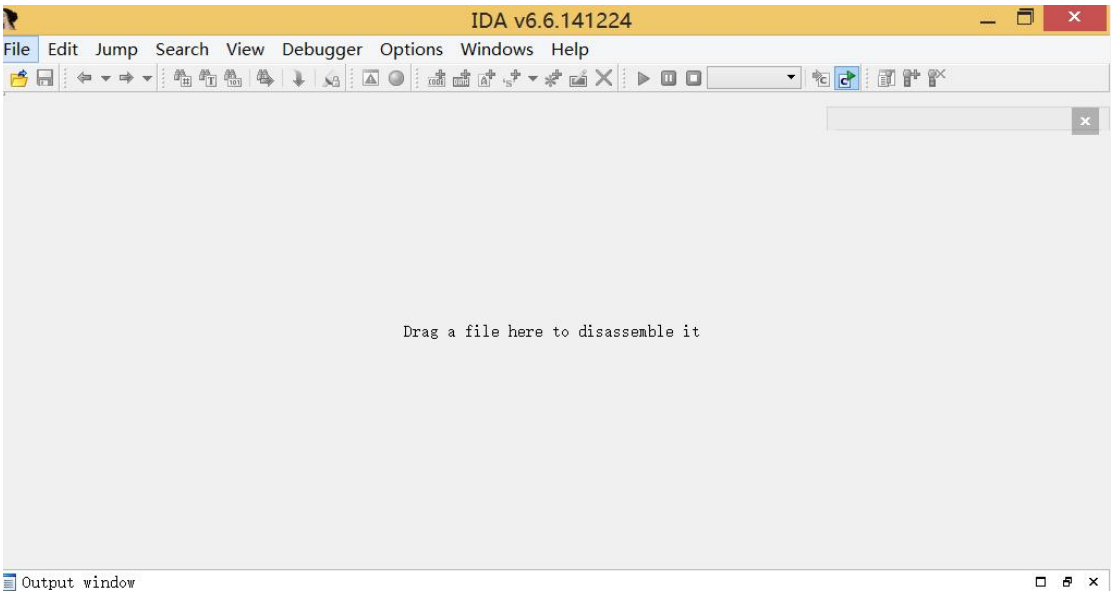
我们利用我们之前在主机上已经下载完毕的安装包，尝试直接复制到虚拟机当中运行。



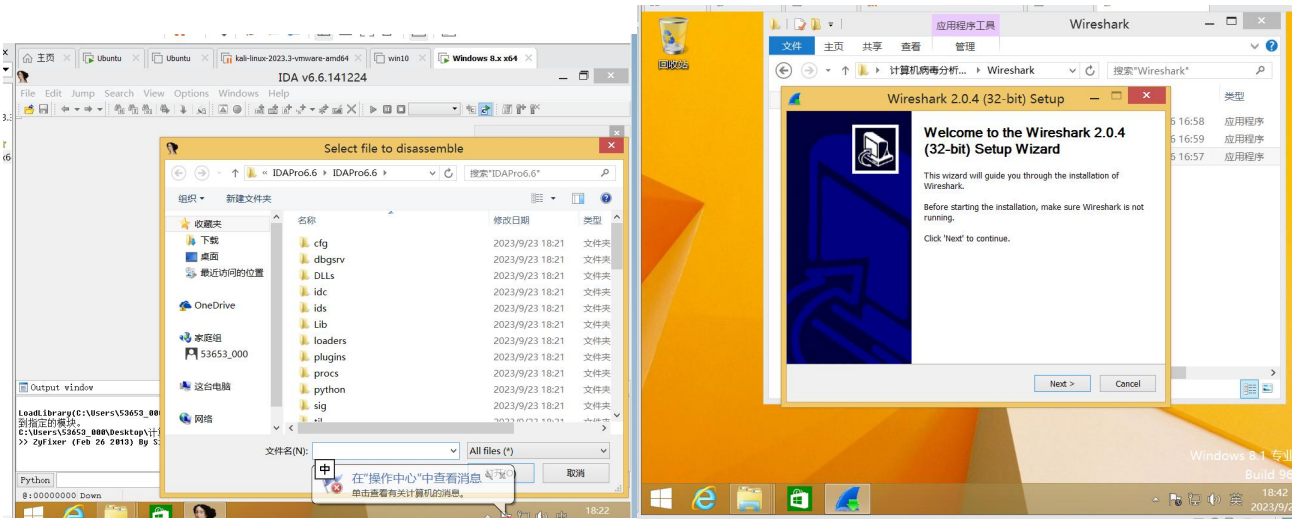
接下来我们逐一将所有的软件尝试运行调试

1. 在 win10 系统上我们已经有成功运行 ida 的经验

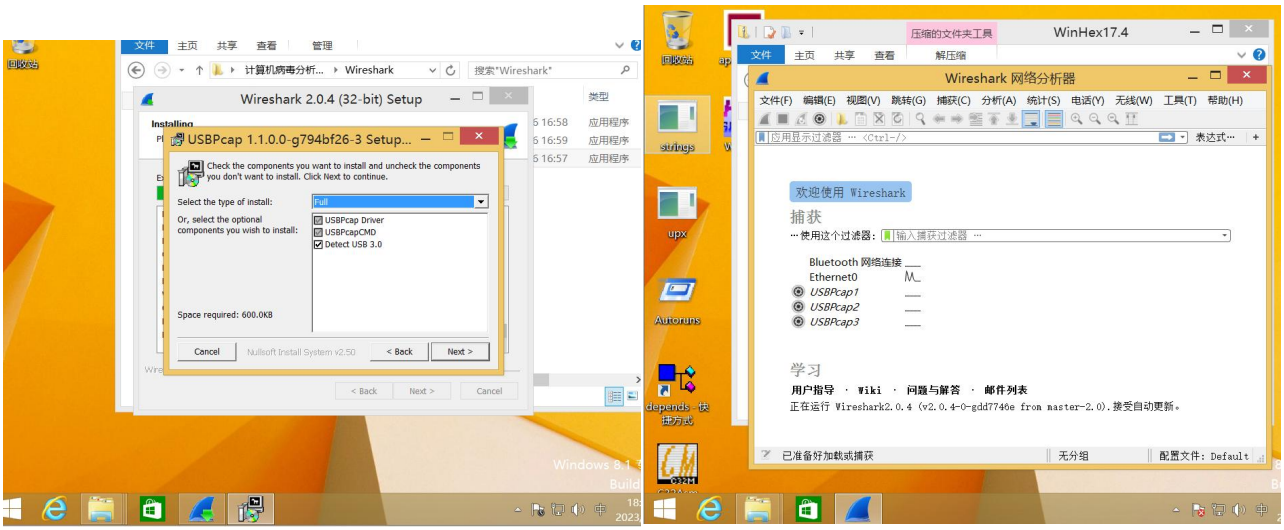
2. 这里我们将 win8 系统安装 VMTOOLS,重启之后打开



Win8.1 操作系统可以自带解压功能，很方便的将我们软件包当中的 ida 软件压缩包解压成所需要的目的文件。接下来我们就可以打开 ida。

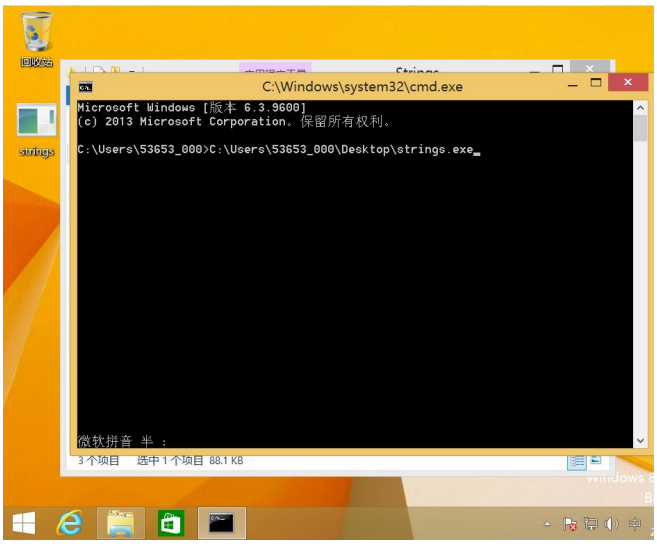


wireshark 动态分析工具可以正常安装与运行。wireshark 是非常流行的网络封包分析软件，简称小鲨鱼，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。

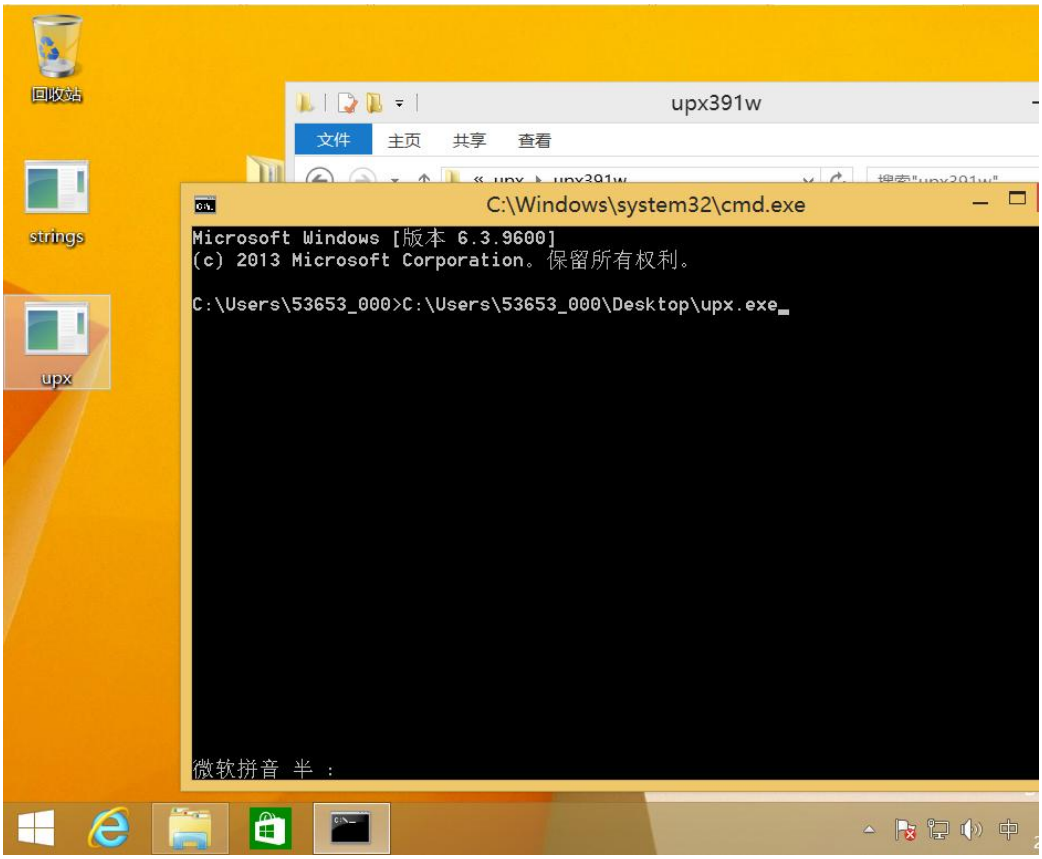


网络分析器等 wireshark 的工具可以有效使用，用来进行分析。

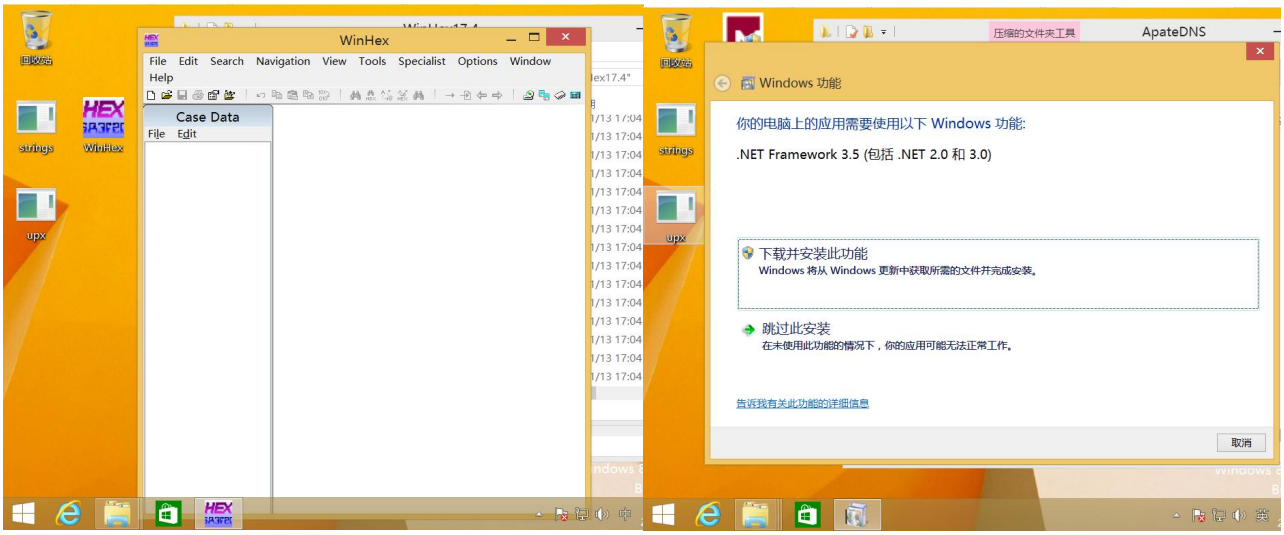
运行 strings 则需要在命令行当中，之前我们在实验一当中已经进行过了相关的运行操作，我们可以很方便的利用将相关文件与 strings.exe 放在同一目录下启动的方式运行 strings.exe 分析其字符串



运行 upx 同理

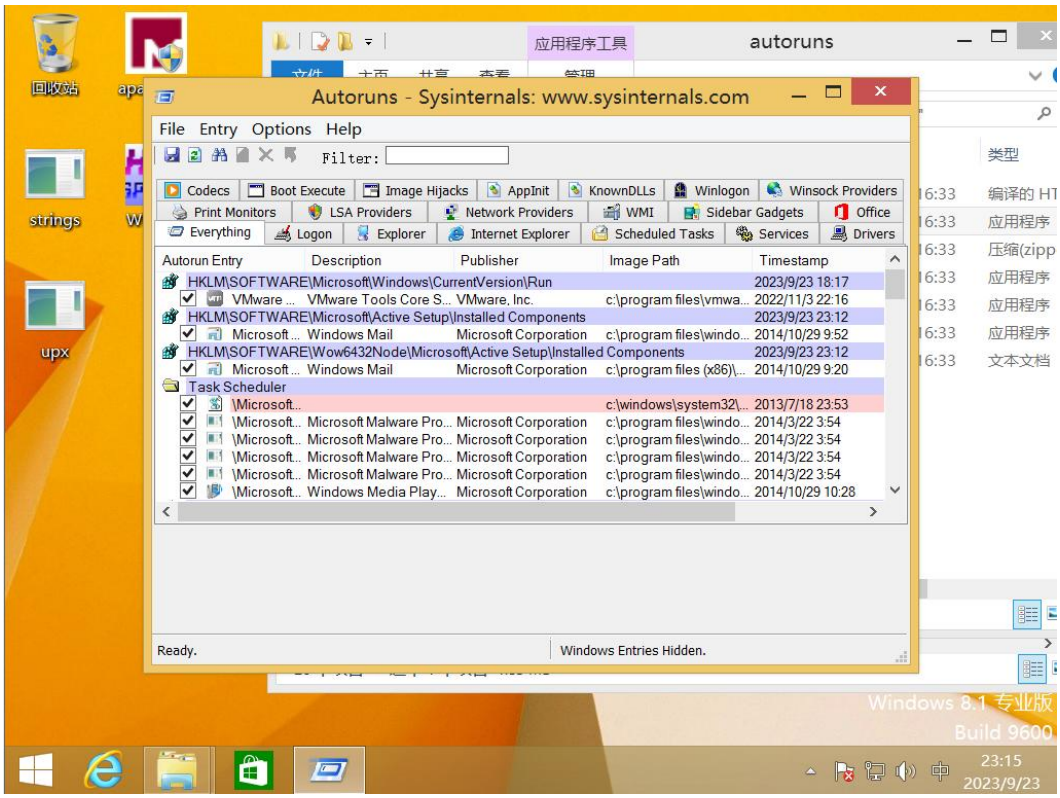


winhex 工具解压之后也可以直接正常使用



apateDNS 工具需要打开压缩包之后进行安装，按照提示进行操作即可。

autoruns 可以直接打开就能运行



awstats 的使用

有 2 种使用模式：命令行模式、浏览器模式

（1）命令行模式

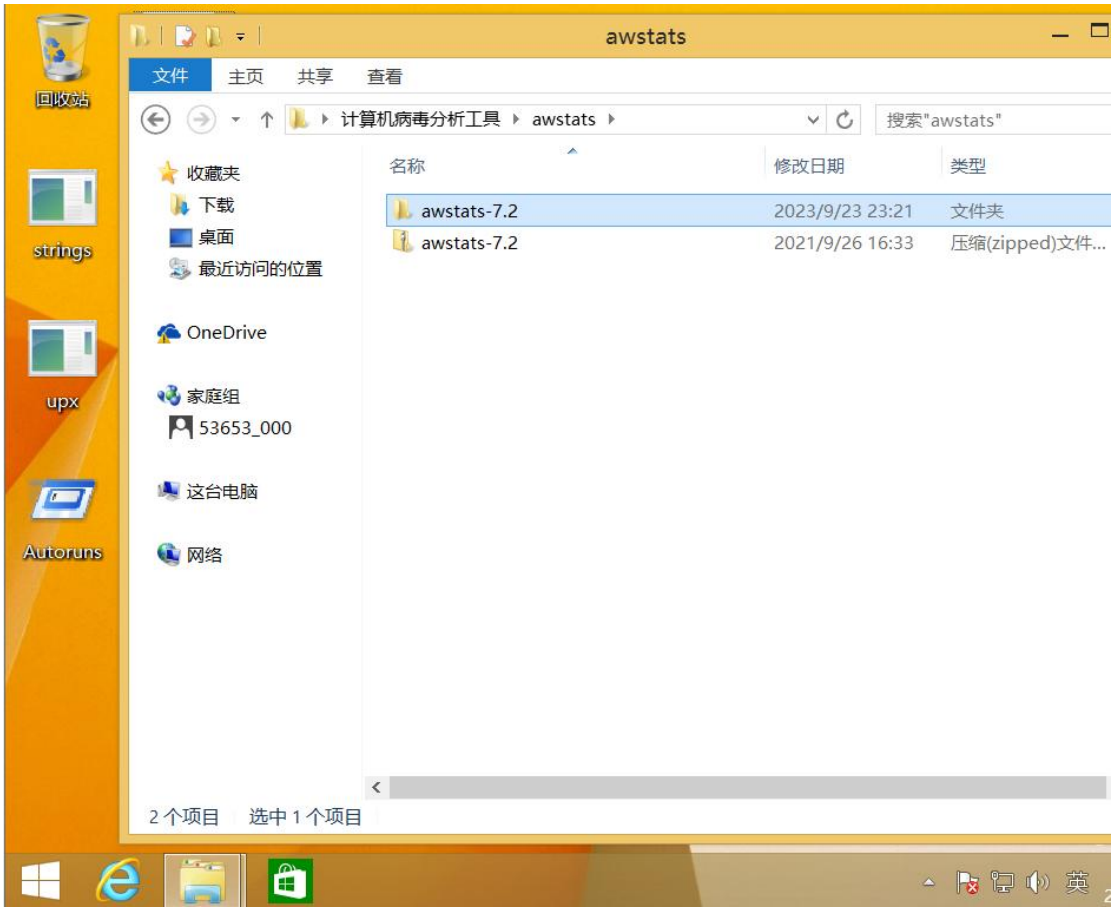
必须在 Apahce2 本机运行，并且本机上安装了 awstats，命令如下：

awstats.pl -update -config=域名

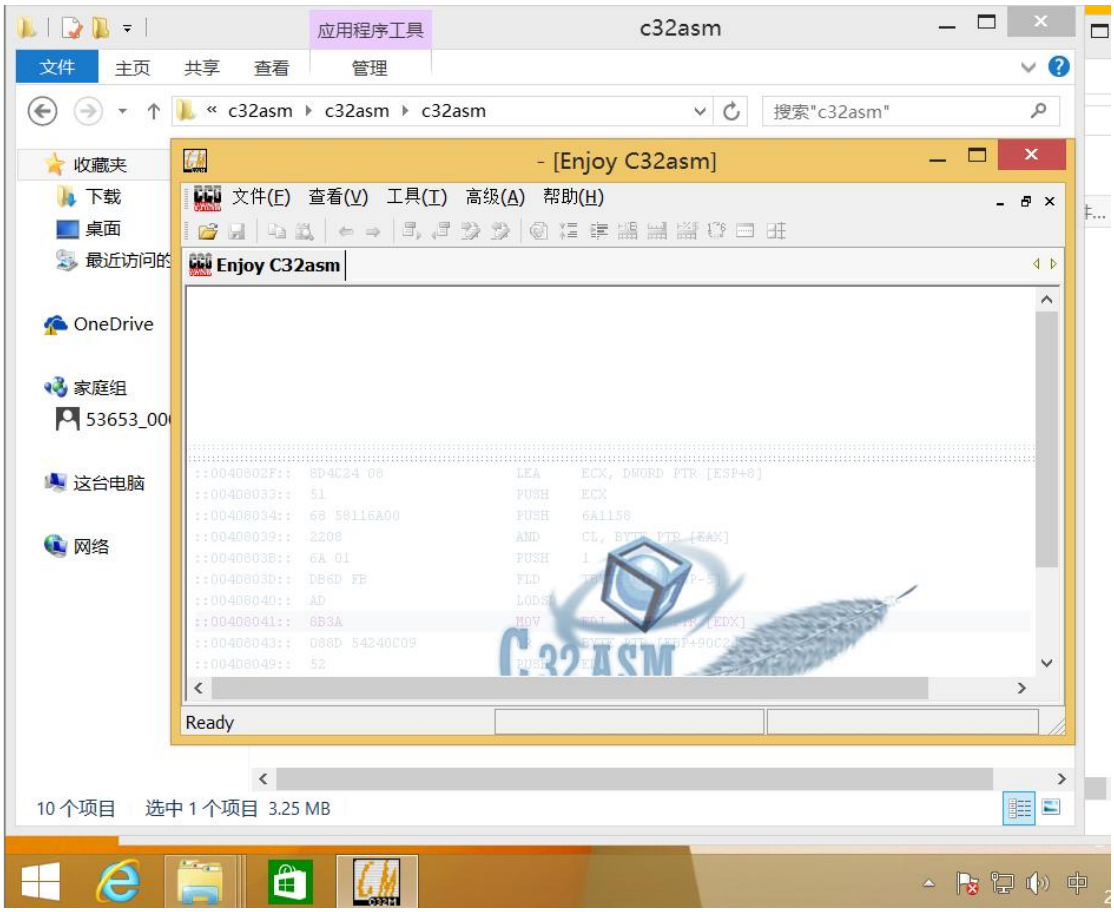
（2）浏览器模式

假设 Apache2 服务器地址是 1.1.1.1

访问地址：http://1.1.1.1/cgi-bin/awstats.pl?config=域名

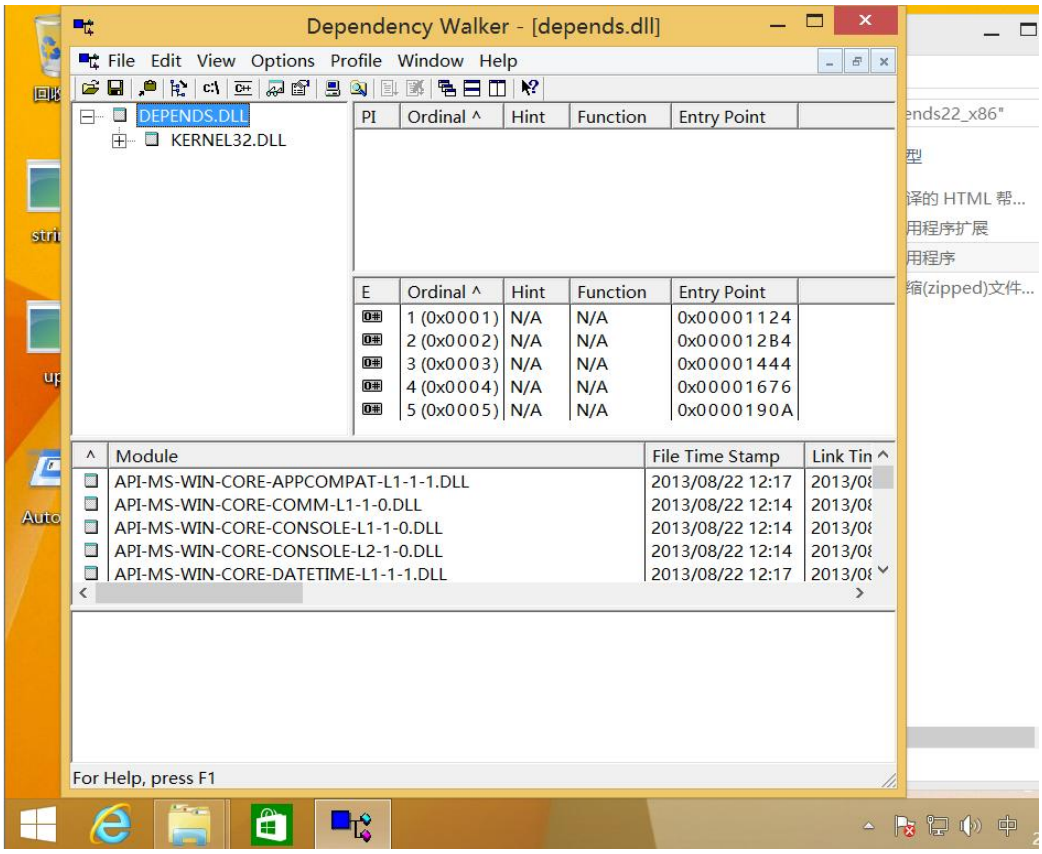


C32asm 应用也可以直接解压后使用，通过其我们可以很方便的进行反汇编的工作。

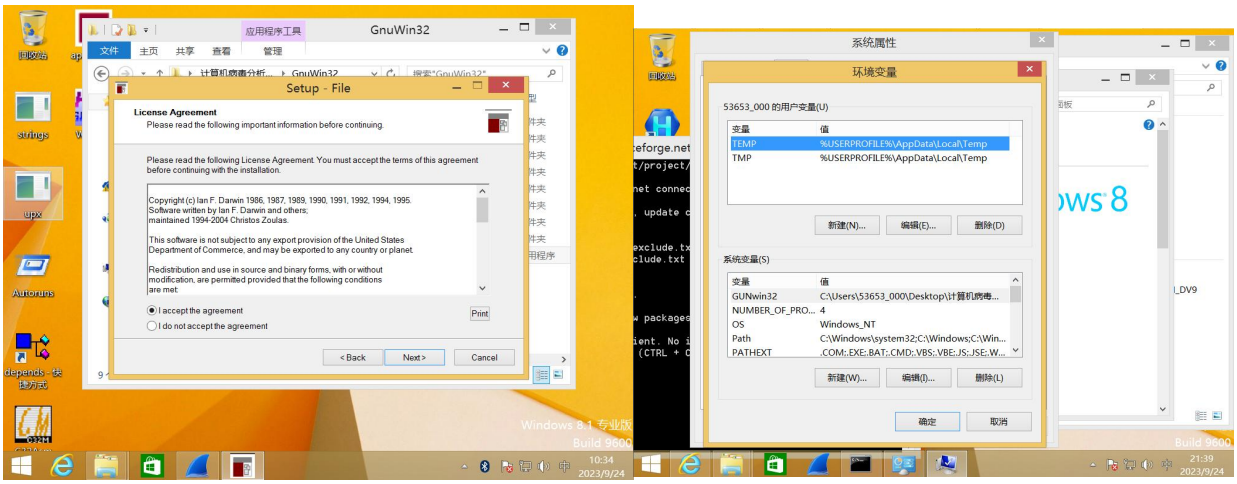


可以打开文件或者自己新建文件方便的进行反汇编工作。

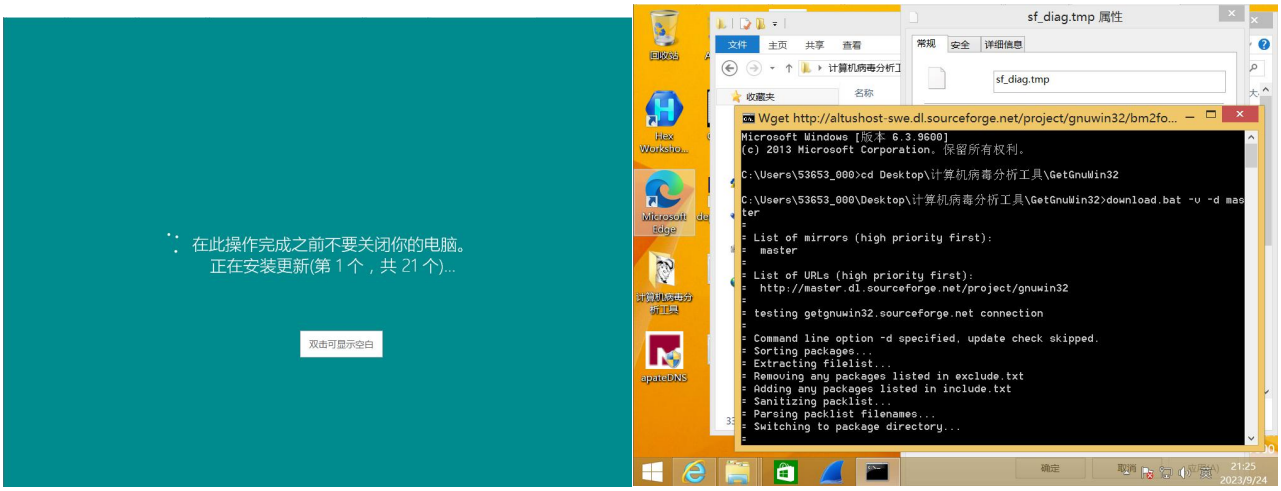
Dependency Walker 是一个免费的实用工具,它可以扫描任何 32 位或 64 位 Windows 模块(EXE，DLL，OCX，SYS 等），并建立所有相关模块的分层树形图。Dependency Walker 对于排除加载和执行模块故障错误非常有用。 Dependency Walker 能检测出许多常见应用问题，例如缺少模块，无效的模块，导入/导出不匹配，循环依赖错误，不匹配的机器类型模块和模块初始化失败。我们下载后可以直接运行 dependency walker。



GNUWin32 需要打开之后按照说明进行安装，将所得到的分析文件存储到指定目录。



安装之后打开 GetGNUwin32 文件夹，将我们文件夹的 bin 路径设置为系统环境变量，之后需要我们重启操作系统以进行更新。



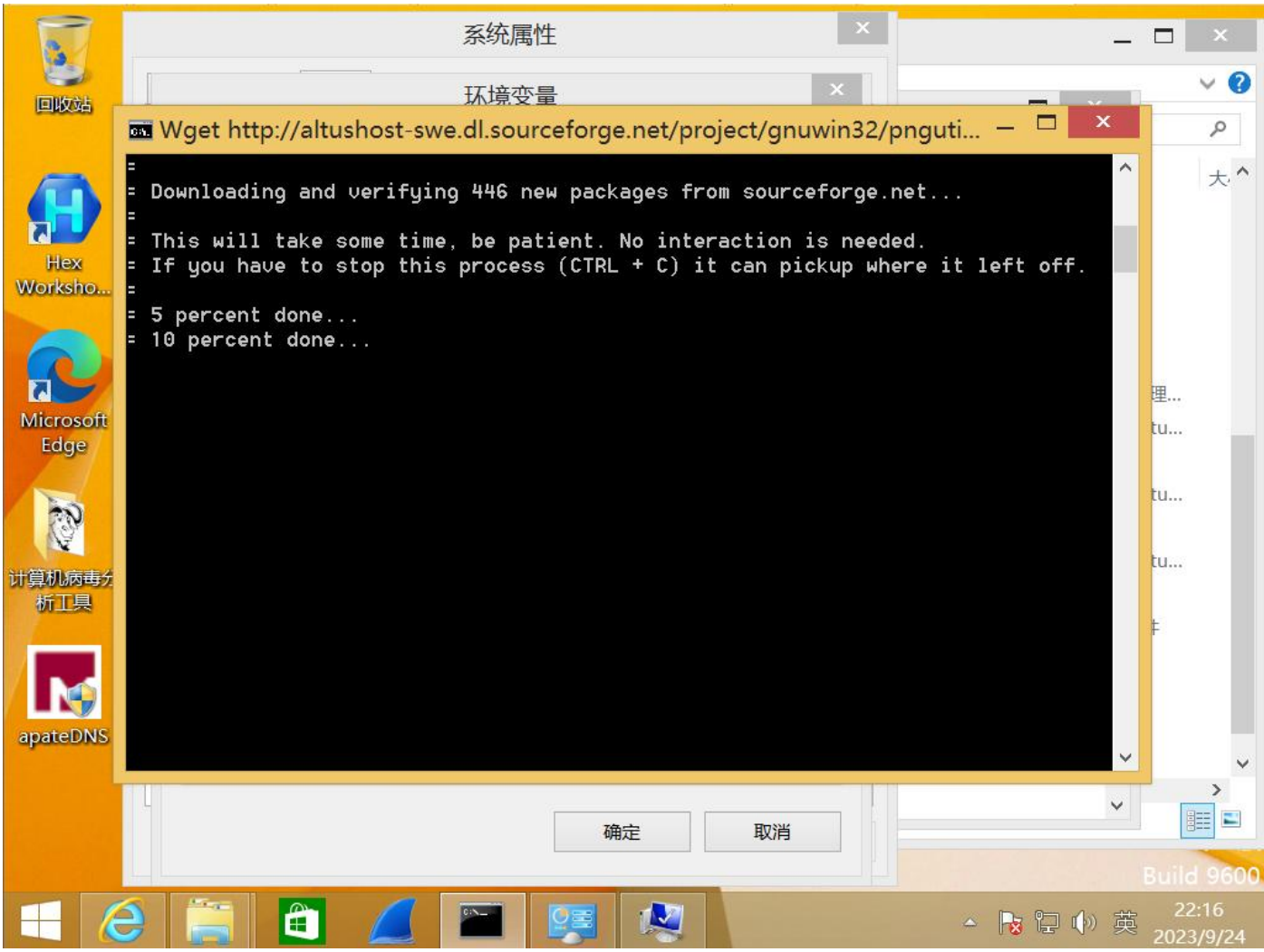
接下来我们可以通过在输出日志中找到这个地址：

http://getgnuwin32.sourceforge.net/update94d563d1564001.zip

在浏览器地址栏中访问这个地址，可以正常下载（不知道为啥）

将下载的 update94d563d1564001.zip 解压，然后把解压的内容与 GetGnuWin32 合并（覆盖原有的文件即可）。

之后我们再输入 download.bat -v -d master 然后可能是一个漫长的等待，十几分钟到数小时不等，下载的包在 packages 目录下。

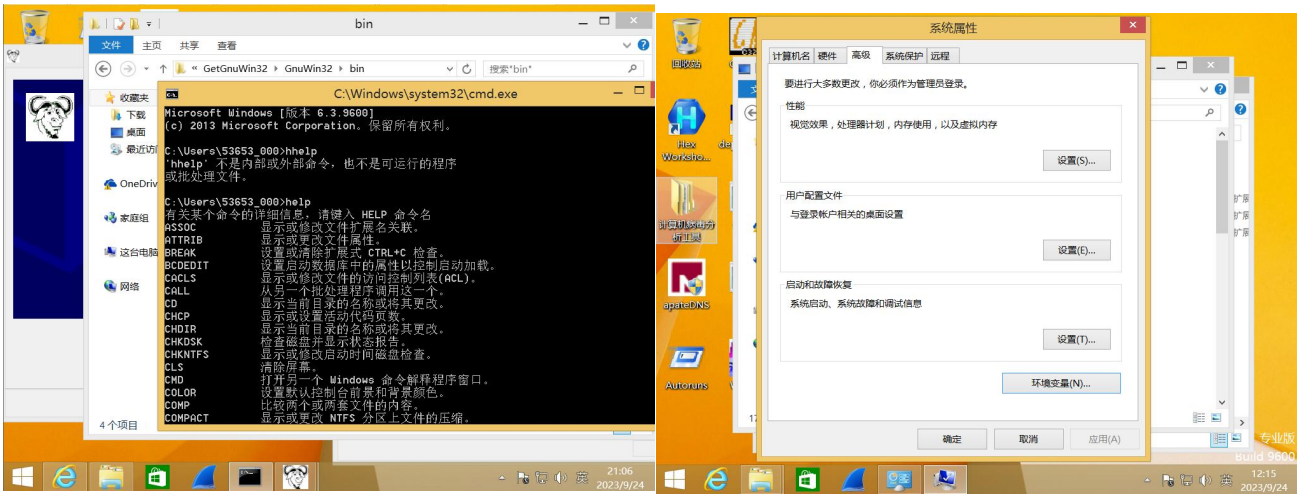


之后我们会发现压缩包存在后缀不统一的问题，这里写了一个 bat 批处理，来批量修改后缀为.zip

```
set oldExt_1=.zip@viasf^=1
set oldExt_2=.zip@viasf^=1.1
set newExt=.zip
REM 将".zip@viasf=1.1"后缀的文件删除，如果有的话
for /f "delims=" %%f in ('dir /b "*%oldExt_2%"') do (
 del "%%f"
)
REM 将".zip@viasf=1"后缀的文件更改为".zip"后缀
for /f "delims=" %%f in ('dir /b "*%oldExt_1%"') do (
    ren "%%f" "%%~nf%newExt%"
)
echo Done!
Pause
```

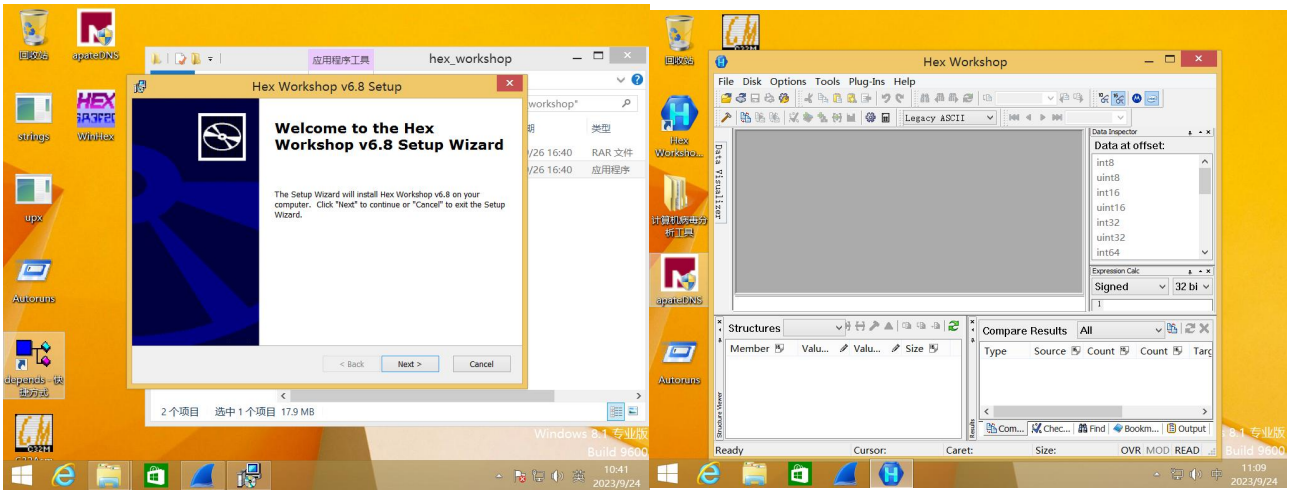
在 GetGnuWin32 目录，运行 install.bat，将解压上述下载的 Linux 相关命令

之后我们就可以验证其是否具有 Linux 命令的功能。

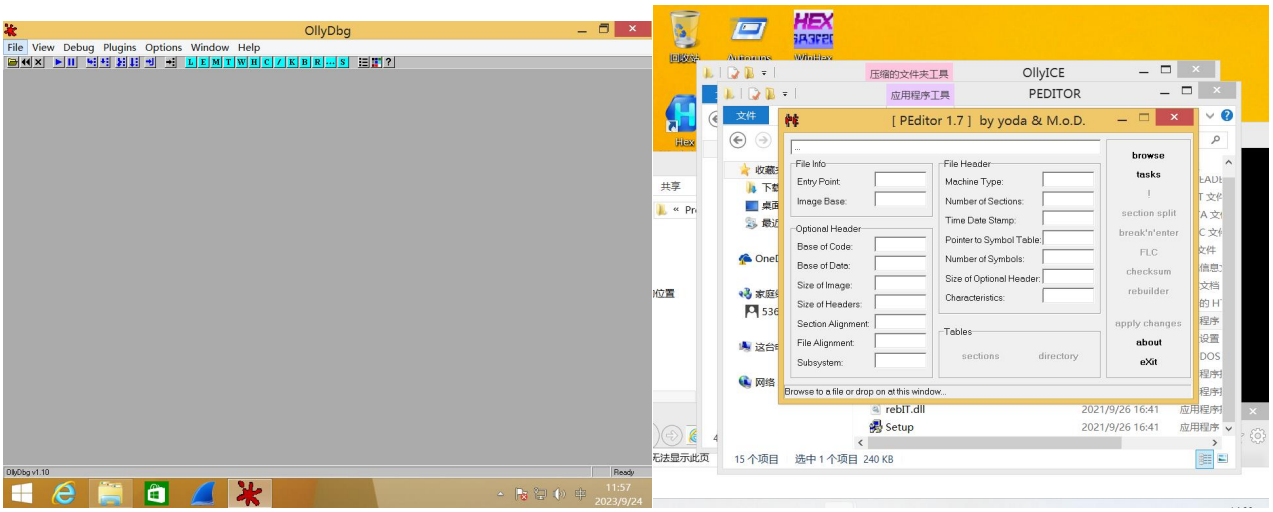


GNUwin32 的 bin 文件夹需要添加到系统环境变量当中运行，之后在 cmd 中运行。GNUwin32 是可以将 linux 指令运行到 windows 命令提示行当中的工具。

hex workshop 是一款专业的十六进制编辑器，使用该软件可以方便地进行十六进制编辑、插入、填充、删除、剪切、复制和粘贴工作，配合查找等操作，使工作更加快捷，工作效率更高。通过十六进制编辑器还能够发现 Windows 以及一些应用程序的漏洞，并能检查出病毒、木马程序等危害电脑的不法软件。

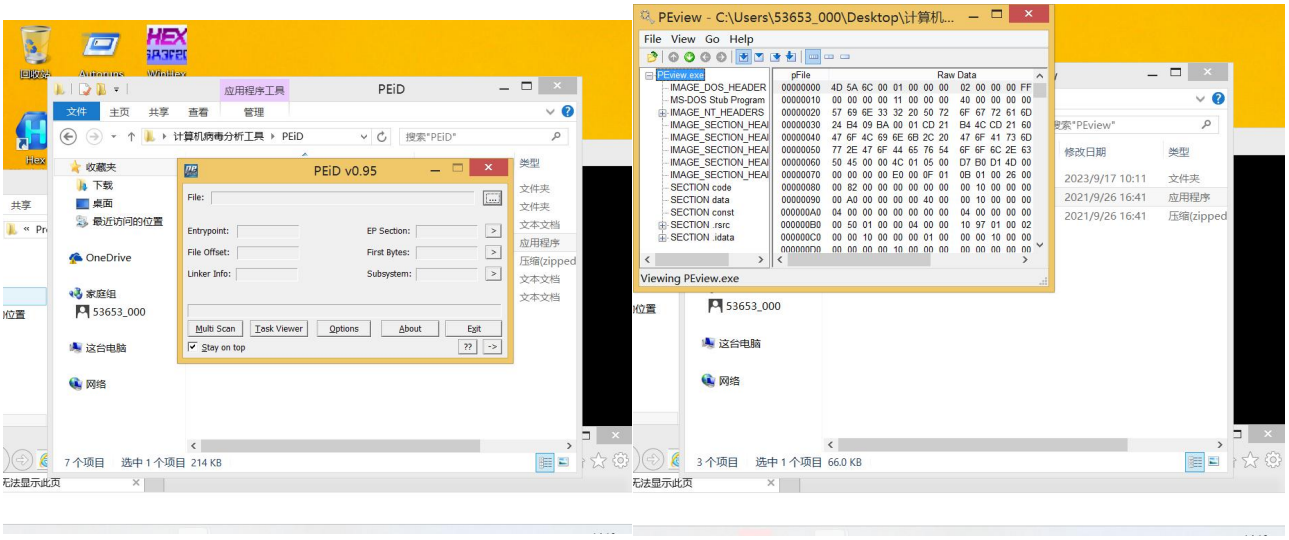


ollydbg 解压后可以直接使用，是很好的 32 位程序的 debug 分析工具。之前我们在汇编语言与逆向技术课程当中已经学习使用过相关的功能，对其的使用已经有了一定的掌握。



PEditior 软件可以直接打开就是安装完成的状态。PEditor 是一款好用的 PE 文件编辑工具，包括分割节、调试器中中断、FLC、校验和和重建程序等功能，可有效减小脱壳后程序的大小，去掉其中的垃圾代码。软件已完全汉化，操作简单。

PEID 和 PEview 的功能我们在之前就已经运行成功，在实验一也已经有了相关的展示。



Process Explorer 的功能也已经安装完毕，可以直接启动监测进程。

1. Process Explorer 主界面

树形结构，准确的显示的进程的父子关系。

通过颜色可以判断此进程处于的状态和类型，是挂起还是正在退出，是服务进程还是普通进程。

2. 显示进程的系统信息

右键 Process 标题栏-选择 Select Columns 项，选择你要观察进程的某种特定的信息，这里有几个选项，常用的有 Process Image 和 Process Memory 这两个选项卡

3. 显示当前进程所加载的 DLL

选择 View - Lower Pane View - DLLs

4. 显示当前进程所占用的系统资源句柄

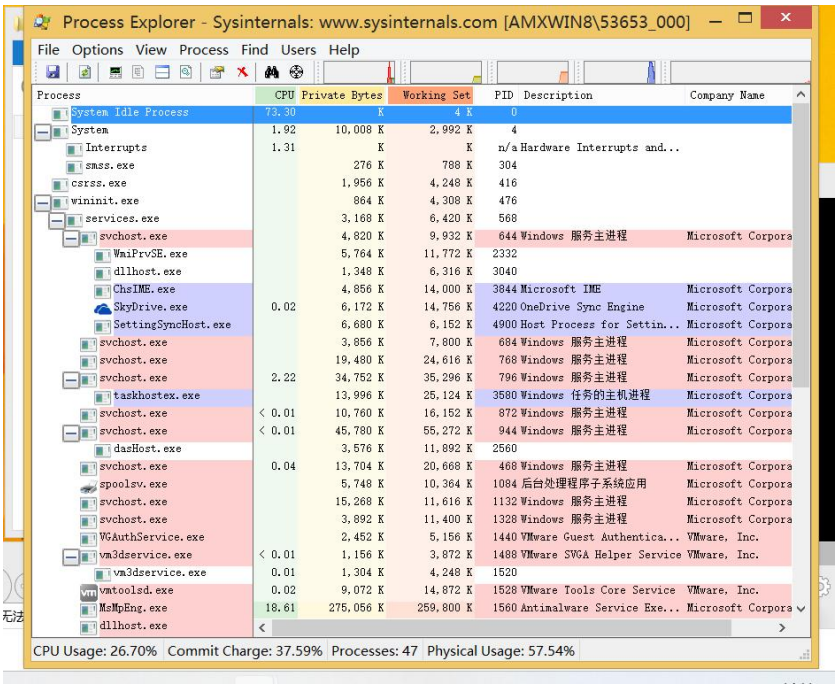
选择 View - Lower Pane View - Handles

5.操控进程以及显示进程的内部信息

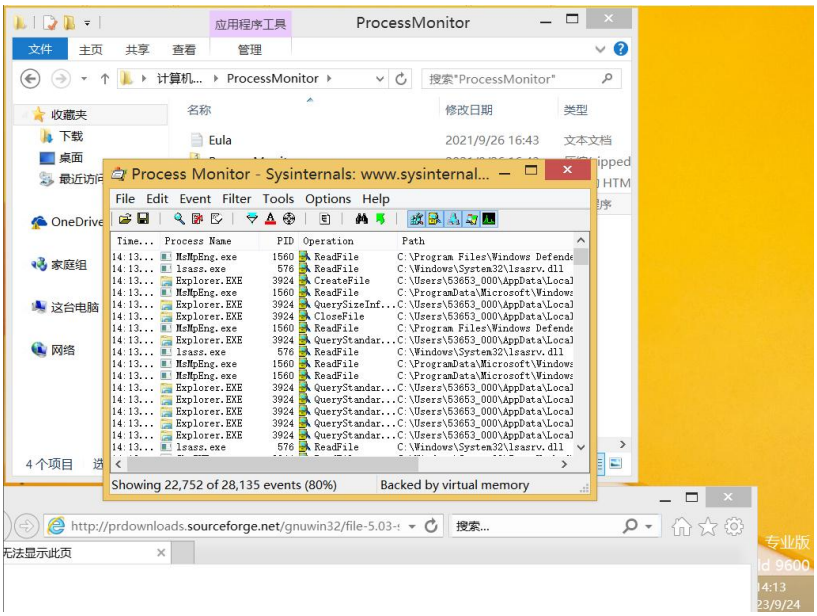
操控进程，杀掉进程、重启进程、挂起进程等

6、搜索功能（Ctrl+F）

有时候我们删除某个文件或文件夹的时候，会提示被某个服务占用，无法删除，这个时候，就可以使用搜索功能知道它被谁占用了，比如 shell.20200608-082337.log 文件被 SunloginClient.exe 占用了。

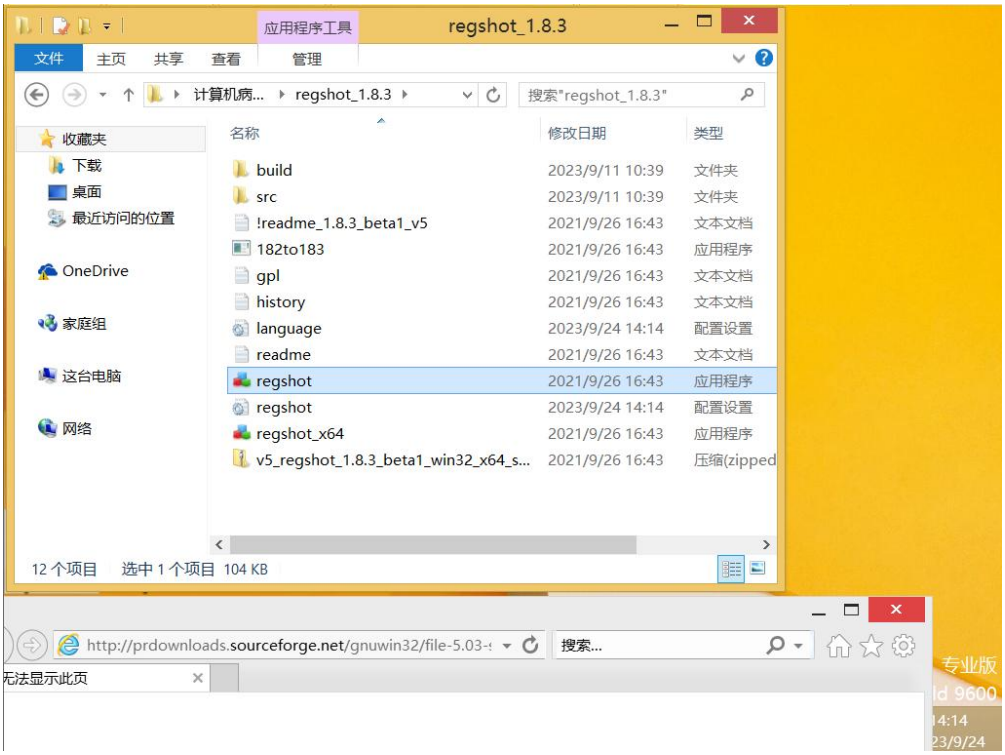


Process monitor 的功能也是已经可以很好的运行的功能，可以直接运行监测。Process Monitor 一款系统进程监视软件，总体来说，Process Monitor 相当于 Filemon+Regmon，其中的 Filemon 专门用来监视系统 中的任何文件操作过程，而 Regmon 用来监视注册表的读写操作过程。

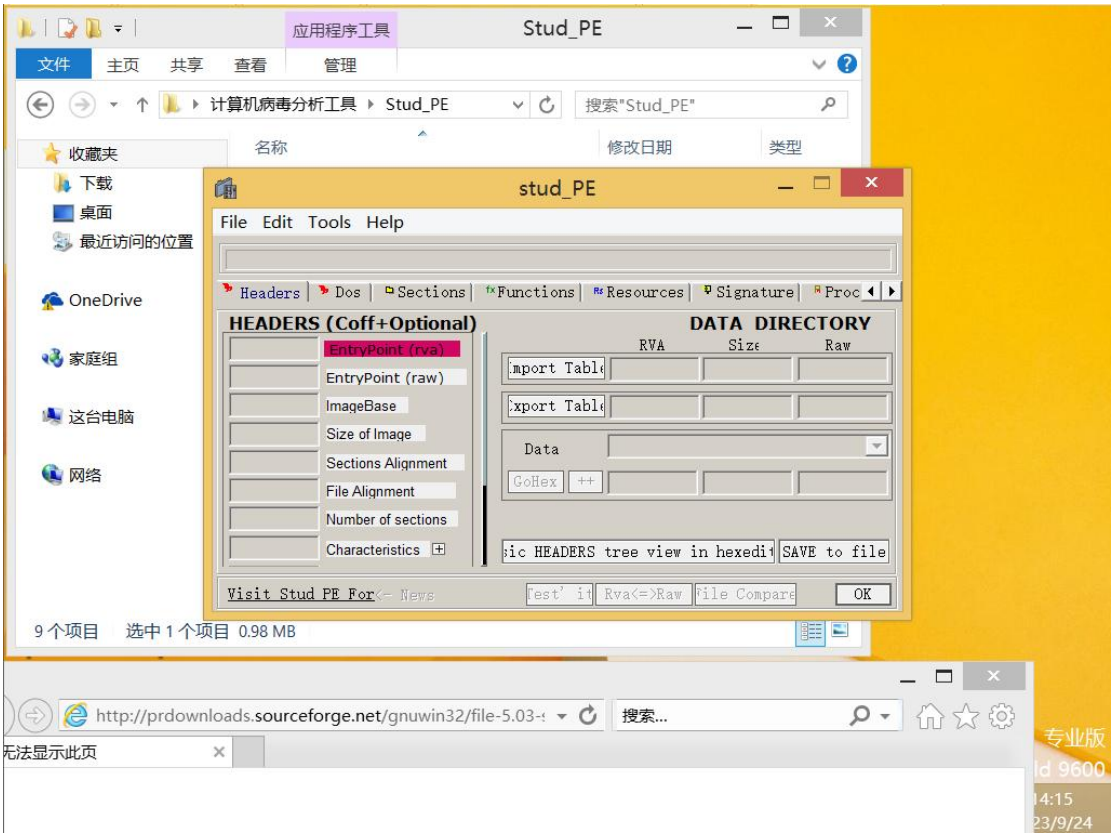


Regshot 工具也是可以直接运行。RegShot 是一种注册表比较工具，它通过两次抓取注册表而快速地比较出答案。它还可以将您的注册表以纯文本方式记录下来，便于浏览；还可以监察 Win.ini，System.ini 中的键值；还可以监察您 Windows 目录和 System 目录中文件的变化，为您手工卸载某些软件创造条件。

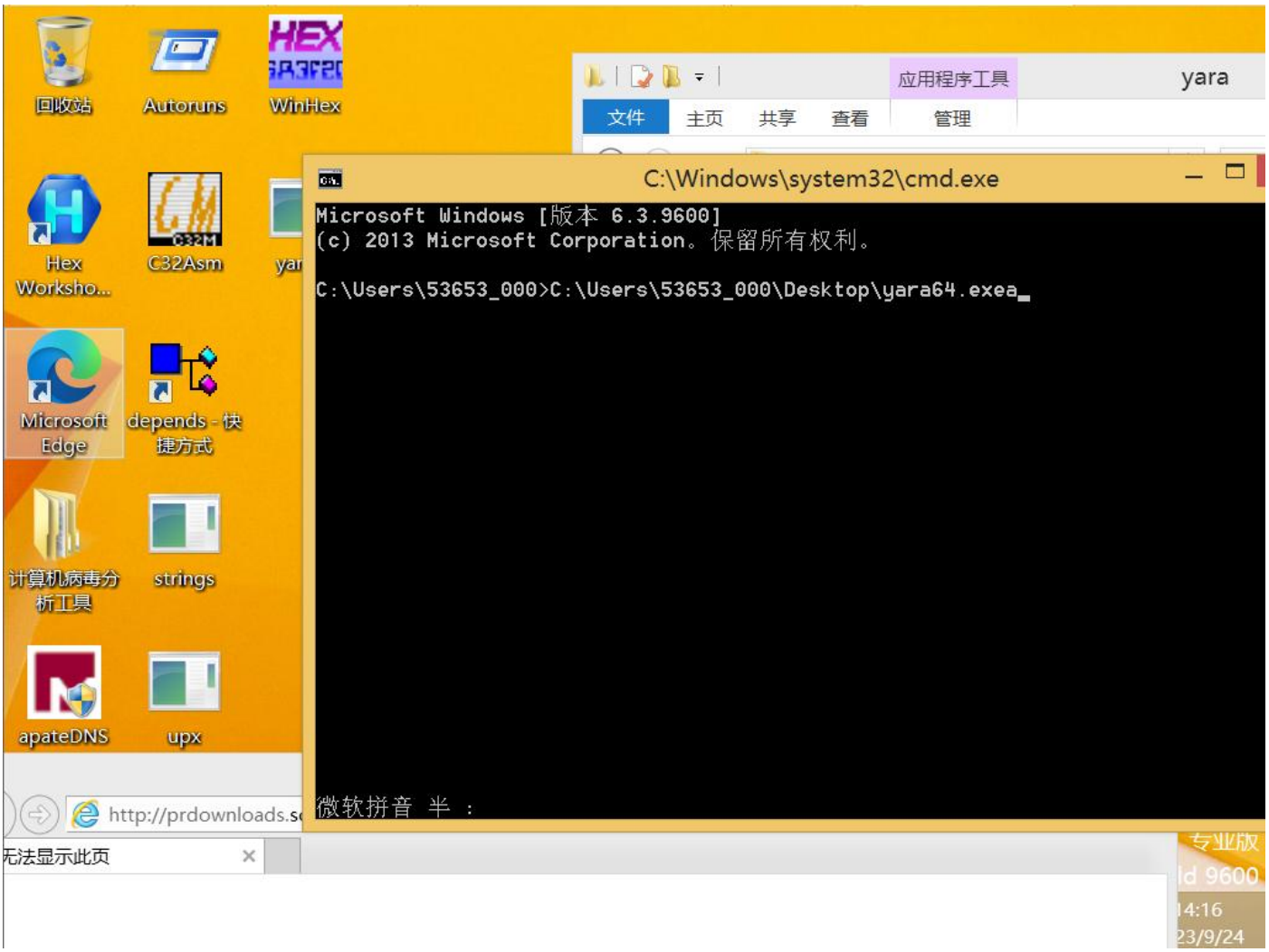
主要功能是通过扫描并保存注册表的“快照”，并对两次快照进行自动的对比，找出快照间存在的不同之处，结果保存成 txt 或者 html 文档。



Stud_PE 是一个适合用来学习 PE 文件格式的知名 PE 工具，可以查看和修改 EXE、DLL 等 PE 结构文件的 PE 结构，界面简洁，适合新手使用。



yara 工具也是我们之前就能很好使用的工具。



四、实验结论及心得体会

上次实验我已经进行了 win10 虚拟机的配置和使用，但是无论是使用便捷程度，应用更新解决问题的能力，始终觉得自己的主机没法方便快捷的带动 win10 操作系统，因此本次实验进行了 win8.1 操作系统的配置以及许多计算机病毒分析软件的下载和安装过程。

计算机病毒需要我们创造一个相对隔离的环境进行更好的分析以及验证良好功能。这里我们采用 windows 操作系统环境，在于许多软件的应用环境即为 windows 系统，而在虚拟机隔离环境当中就可以有效的防止主机被感染。

本次实验配置过程当中，GNUwin32 的配置遇到了很多问题，其中许多功能无法直接在软件包中打开，环境变量的修改虽然有效，但仍然发现相关的 linux 指令并没有能够使用，于是采取重新配置，不过最终成功。

许多之前不常用的软件也熟悉了其功能，包括 Process Monitor 其功能很好的可以在监测进程，在网上我也查找了其一定的功能，并进行了使用，得到了一些很好的效果。

一些软件是以 exe 形式存在的，需要我们拖到命令行当中执行，这里我们可以将其分类存储到文件夹当中，方便对相应的文件进行分析。