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

学　　号　2112060

姓　　名　孙蕗

班　　级　信息安全 1 班

# 《恶意代码分析与防治技术》Lab2 课程实验报告

# 一、实验目的

配置病毒分析虚拟机，并在虚拟机中安装静态分析工具和动态分析工具用以未来的病毒分析，了解恶意软件的机制和行为，以便未来进行安全性评估和威胁分析。

# 二、实验原理

虚拟机是一个模拟的计算机环境，允许在一个物理计算机上运行多个虚拟操作系统。

Windows XP 操作系统，这是一个老版本的 Windows 系统，因为它在安全性方面存在漏洞，常用于分析恶意软件。

静态分析工具用于分析恶意软件的二进制文件，如可执行文件（.exe）和动态链接库（.dll）。这些工具可以帮助分析文件的结构、代码、依赖项等信息。

动态分析工具用于监视和分析恶意软件在运行时的行为，包括文件操作、注册表访问、网络通信等。

# 三、实验过程

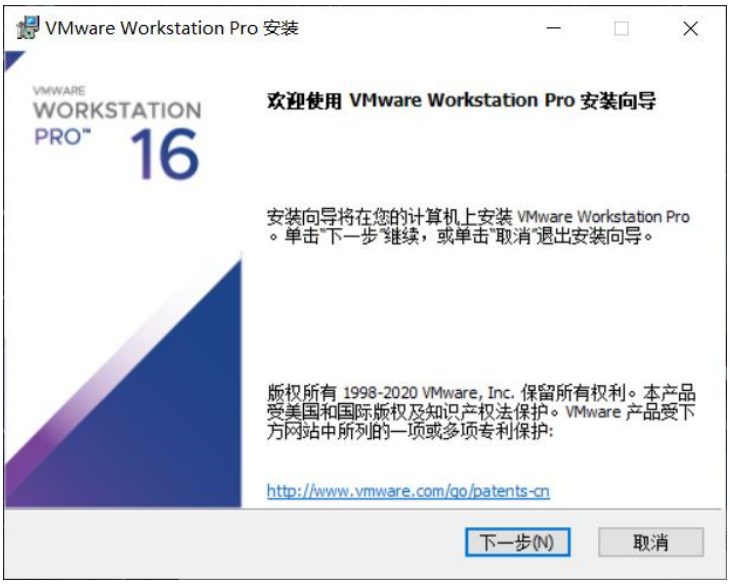
## （一） 虚拟机的安装和配置过程

### （1） VMware 虚拟机

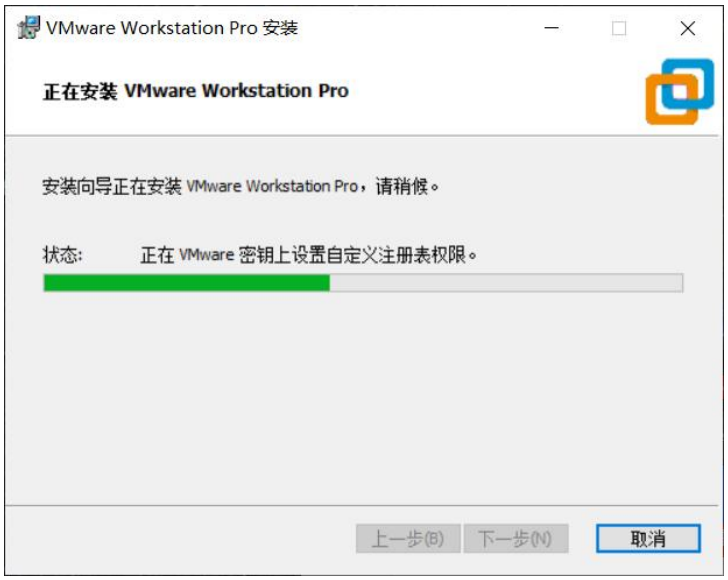
VMware Workstation 是一款功能强大的桌面虚拟计算机软件，它能够让用户在宿主机操作系统上同时运行多个操作系统。这种虚拟化技术可以极大地提高计算机的利用率，同时也方便了开发者和测试人员进行多种操作系统的测试和开发。

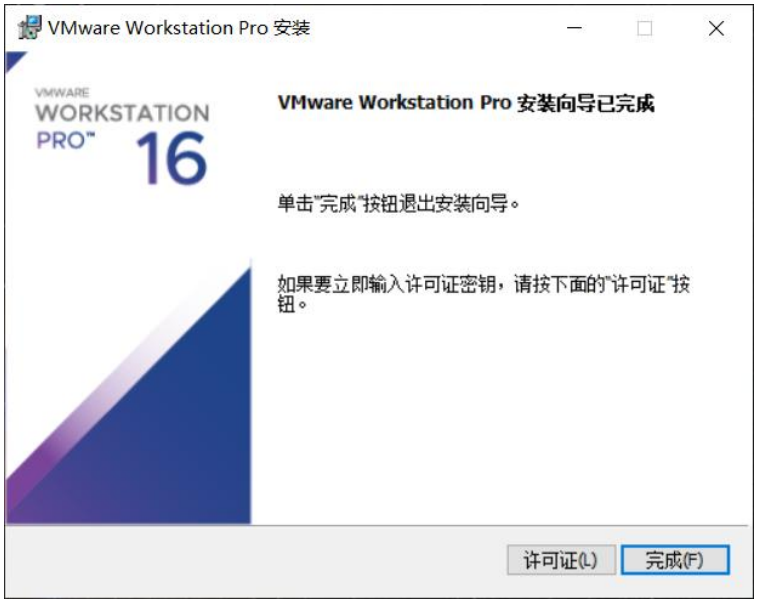
在 VMware 官网中下载最新的 VMware Workstation，选择 for Windows 系列的版本根据自己的版本进行下载。

点击下载好的.exe 进程，按照安装向导的指引进行安装。

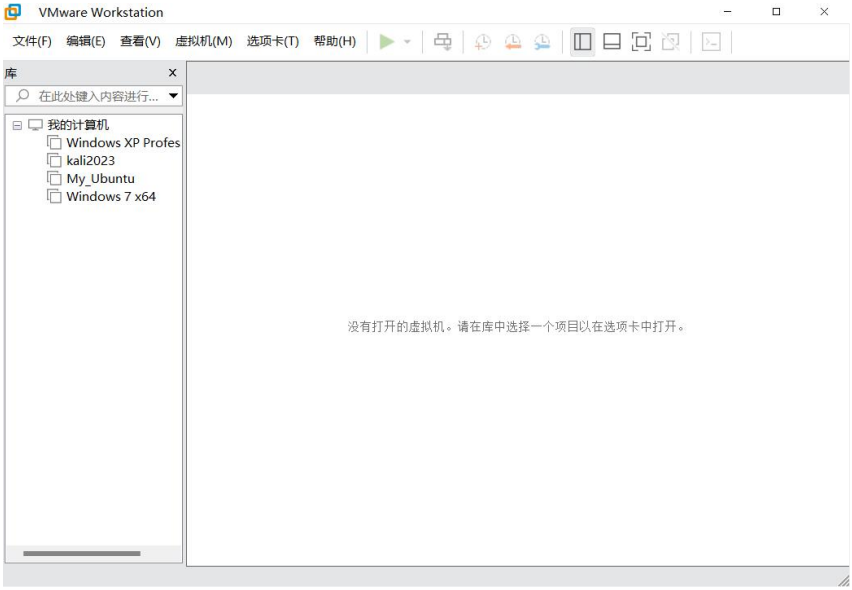



选择自定义安装，将 VMware 安装在 D 盘。






安装成功后，打开软件后将如下图所示：




## （2） Windows XP 操作系统

Windows XP 零售版于 2001 年 10 月 25 日正式上市发售，是继 Windows 2000 及 Windows Me 之后的下一代 Windows 操作系统，也是微软首个面向消费者且使用 Windows NT 架构的操作系统。

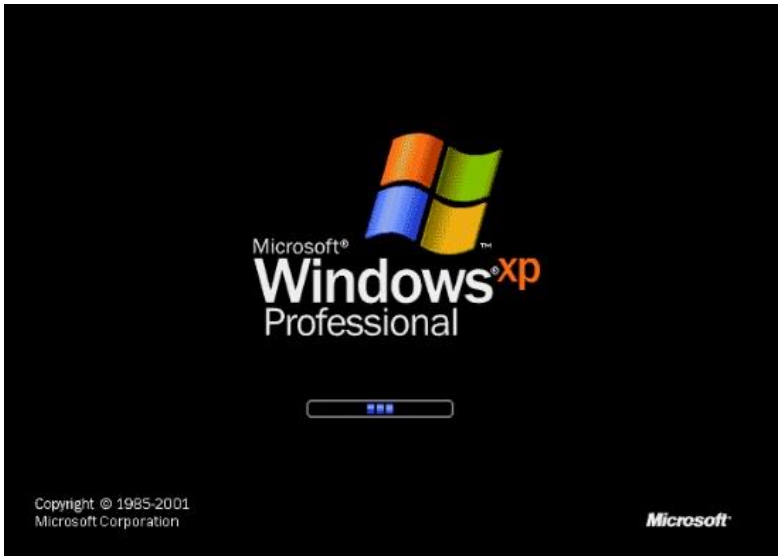
下载 Windows XP 系统镜像文件包。

在 VMware 中选择文件->新建虚拟机，按照提示进行安装。客户机操作系统选择 Microsoft Windows，版本选择 Windows XP Professional。设置虚拟机名称和安装位置，磁盘容量和内存根据需求进行设置。

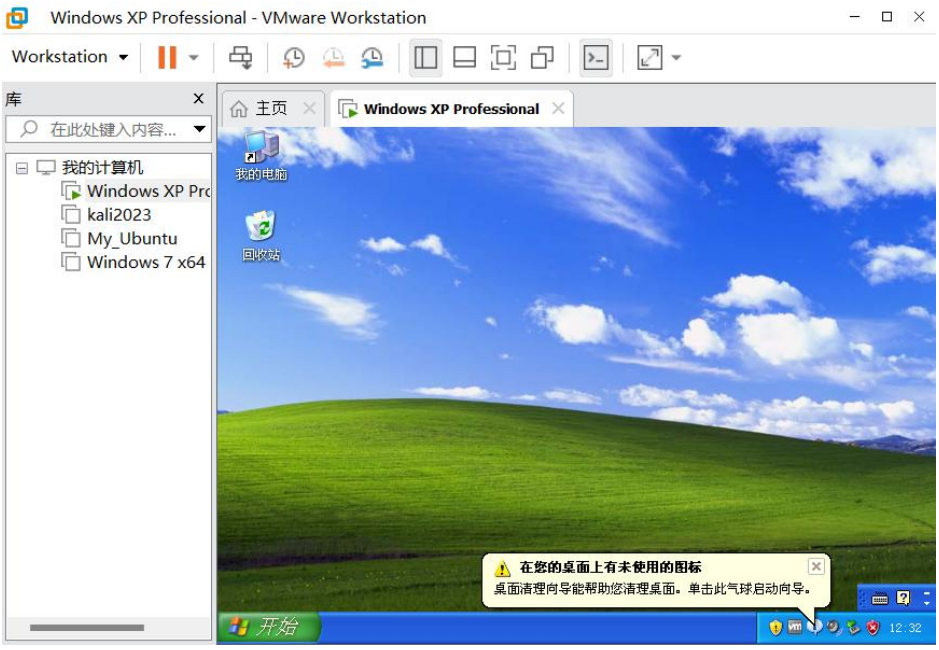

编辑虚拟机设置，插入 ISO 镜像文件，选择下载好的 Windows XP 的镜像。


设置好共享文件夹


开启 Windows XP 虚拟机，根据默认提示安装 XP 系统。

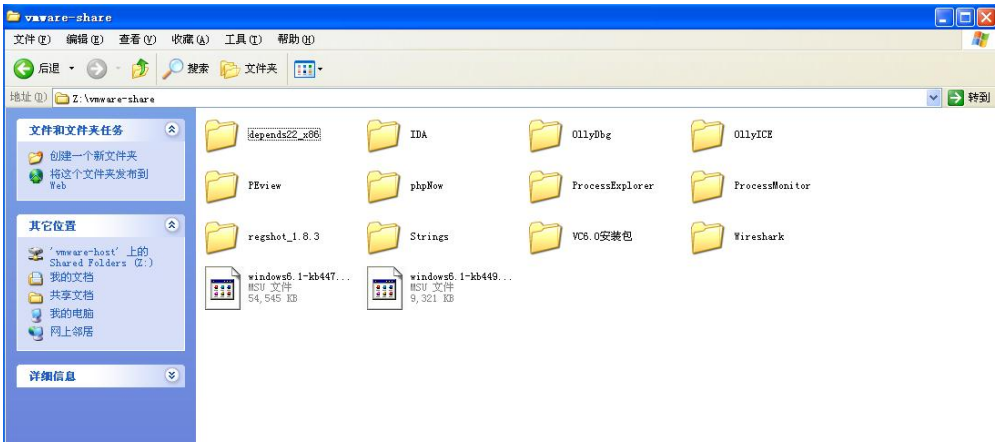



根据默认提示安装，安装成功后应当如下图所示




## （二） 静态分析工具的功能和安装过程

下载各个工具的安装包，通过共享文件夹将安装包导入 Xp 虚拟机中。




## （1） string.exe

Strings 工具可用于在对象文件或二进制文件中查找可打印的字符串。 strings 命令对识别随机对象文件很有用。

安装成功后 Win+R 进入 cmd，然后进入 strings 安装的文件夹运行 strings 命令。

```
C:\Documents and Settings\Administrator>cd /d Z:

Z:\vmware-share\Strings>
```

运行示例截图：

```
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
*/*
 Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
```

常用命令：

-a --all：扫描整个文件而不是只扫描目标文件初始化和装载段

-v 查看版本信息

-f --print-file-name：在显示字符串前先显示文件名

-n --bytes=[number]：找到并且输出所有 NUL 终止符序列

- ：设置显示的最少的字符数，默认是 4 个字符

-t --radix={o,d,x} ：输出字符的位置，基于八进制，十进制或者十六进制

-o ：类似--radix=o

-T --target= ：指定二进制文件格式

-e --encoding={s,S,b,l,B,L} ：选择字符大小和排列顺序:s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit

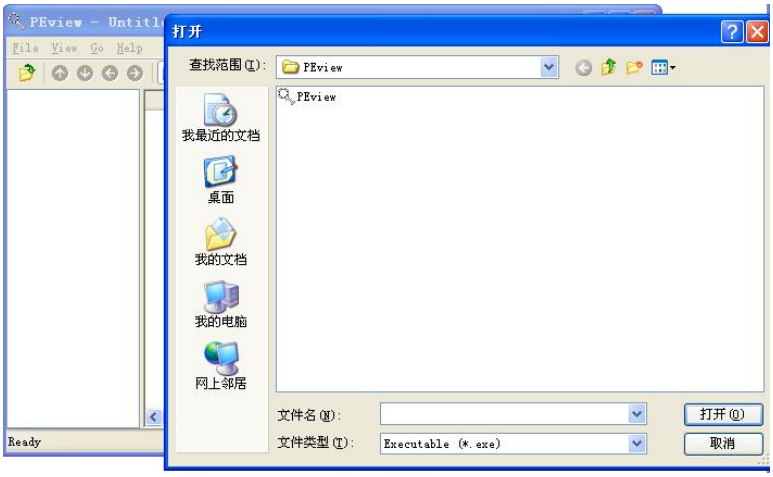
@ ：读取中选项

## （2） PEView

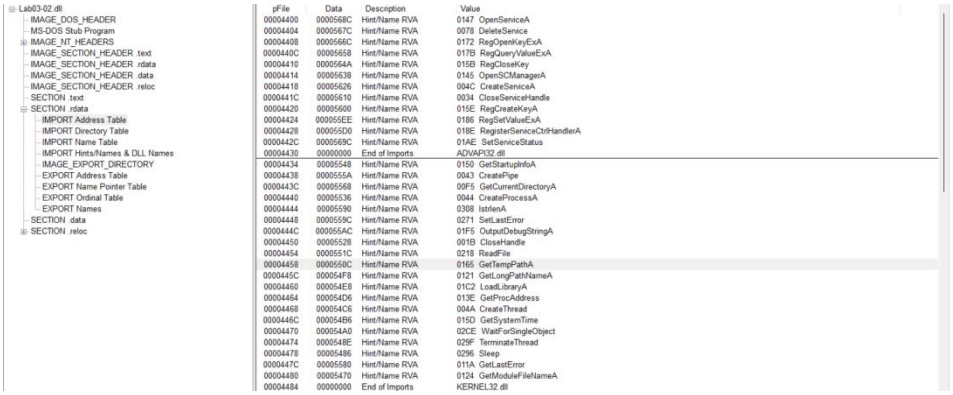
PeView 是一款使用 C/C++开发实现的命令行交互式 Windows PE 文件解析器，可以对 PE 文件进行解析，查看 PE 文件的文件头和各个节区内容，普遍应用于病毒木马等样本的解包分析工作。

点击解压后的.exe 文件即可运行。

可以进入主页面通过 file->open 打开目标文件

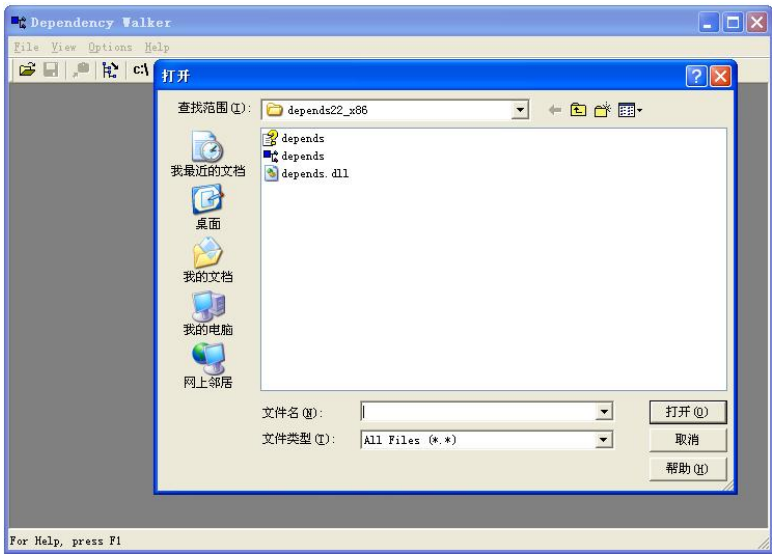

运行示例截图：



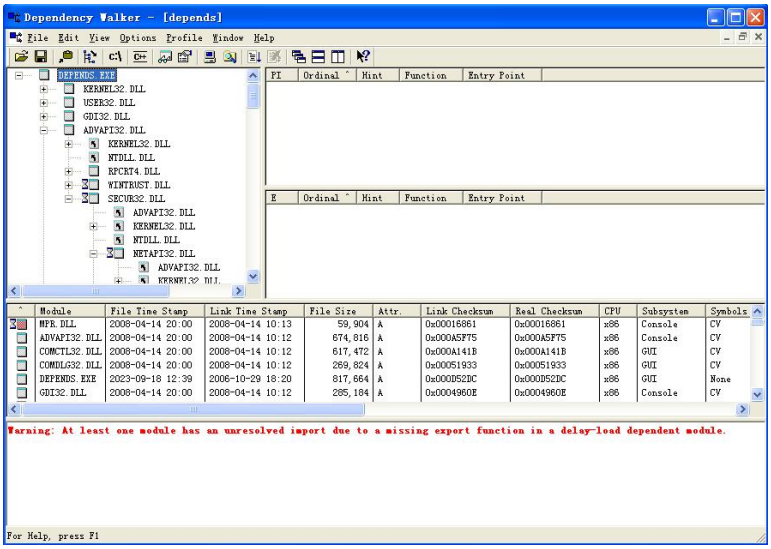

## （3） Dependency Walker

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），分析可执行文件的依赖关系，建立所有相关模块的分层树形图，查找他们所需的动态链接库。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。

点击解压后的.exe 文件即可运行



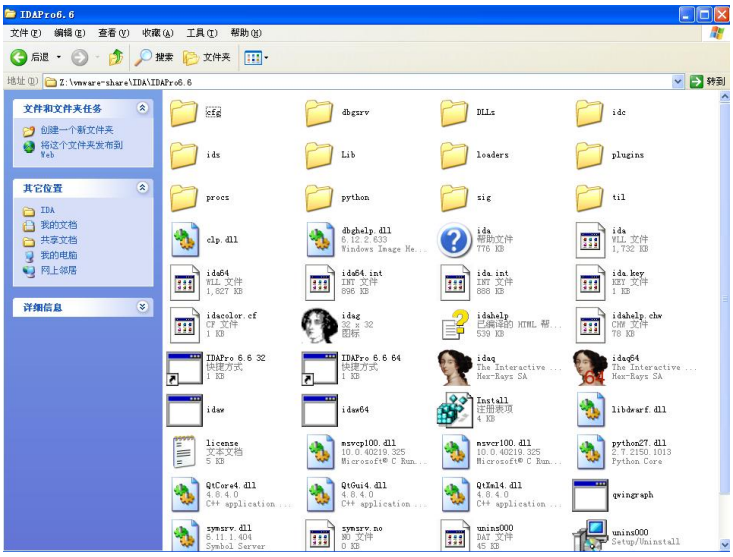

可以进入主页面通过 file->open 打开目标 exe 文件或 dll 文件运行示例截图：




## （4） IDA

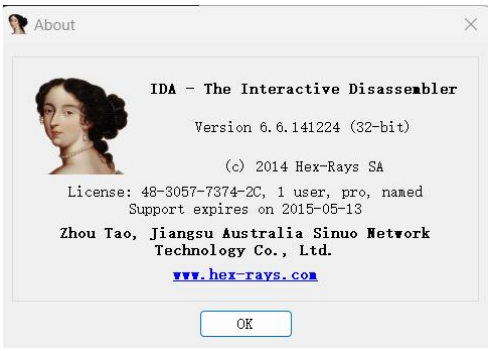
IDA 全称是交互式反汇编器专业版（Interactive Disassembler Professional），其简称为 IDA，是目前最棒的一个静态反编译软件，IDA Pro 是一款交互式的,可编程的,可扩展的,多处理器的,交叉 Windows 或 Linux WinCE MacOS 平台主机来分析程序，被公认为最好的花钱可以买到的逆向工程利器。IDA Pro 已经成为事实上的分析敌意代码的标准并让其自身迅速成为攻击研究领域的重要工具。它支持数十种 CPU 指令集其中包括 Intel x86，x64，MIPS，PowerPC，ARM，Z80，68000，c8051 等等。

下载后解压缩，点击人头像的.exe 文件进行安装，按照程序安装向导界面按照提示安装即可。

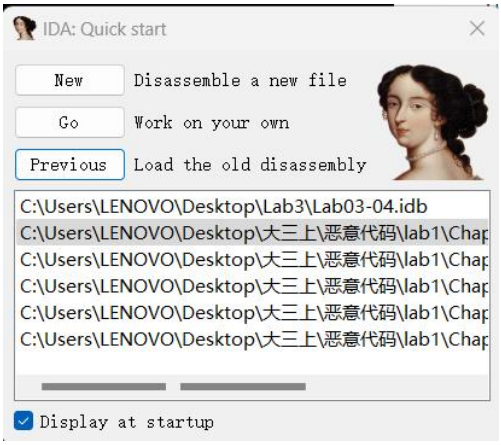


运行截图：

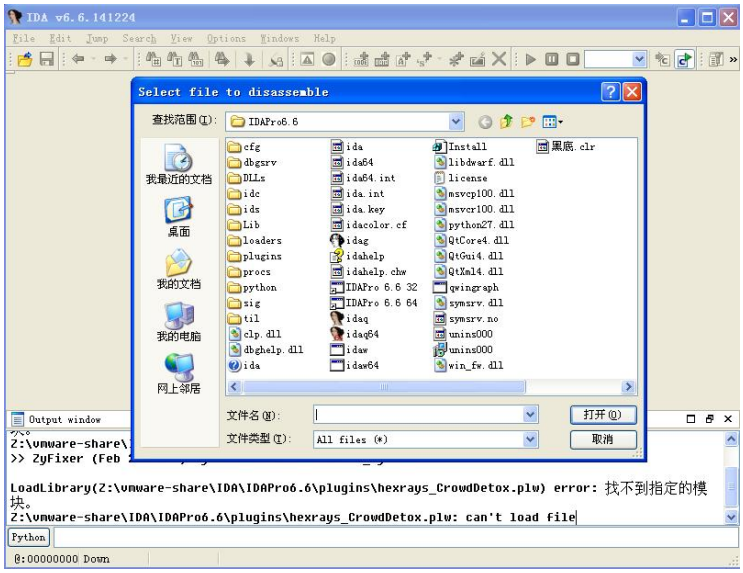
点击后是欢迎界面



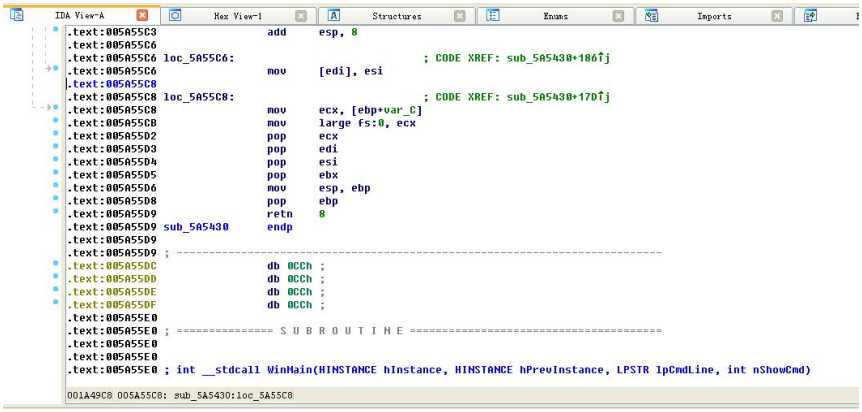

选项界面 3 个选项，new（新建工程），go（独立工程），previous（上次的工程），打开目标文件即可




或者进入主页面通过 file->open 打开目标文件




运行示例截图：

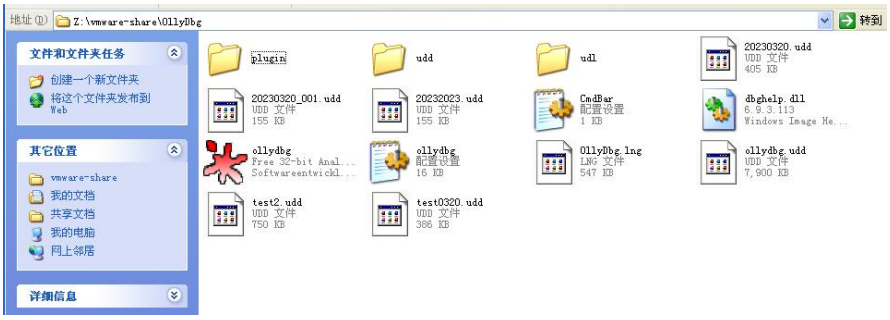


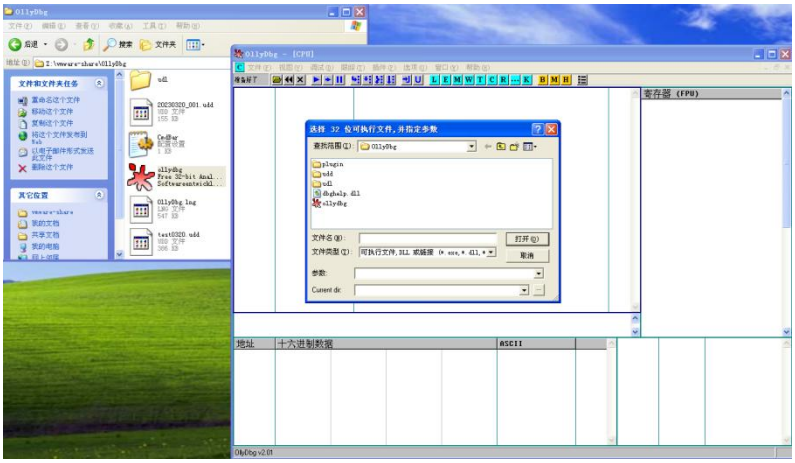

## （三） 动态分析工具的功能和安装过程

### （1） OllyDBG

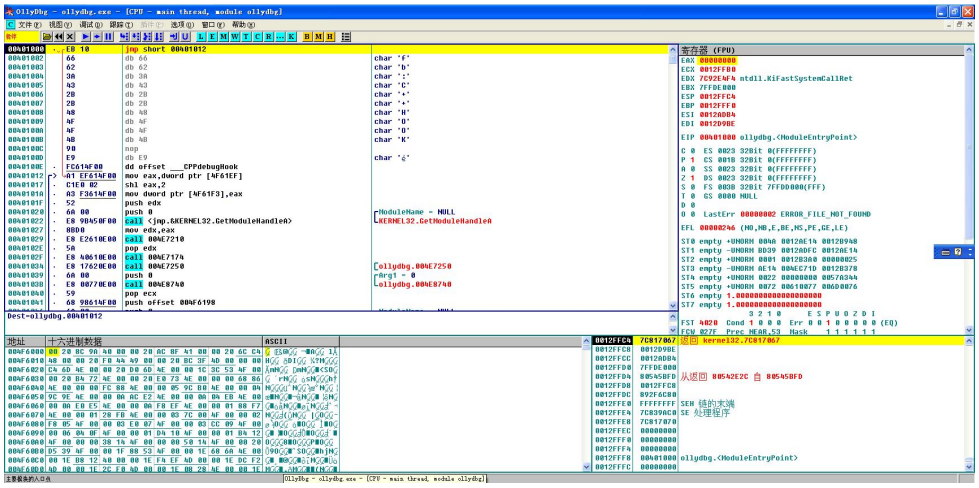
OllyDbg 是一种具有可视化界面的 32 位汇编分析调试器，是一个新的动态追踪工具，将 IDA 与 SoftICE 结合起来的思想，Ring3 级调试器，非常容易上手，已代替 SoftICE 成为当今最为流行的调试解密工具了。同时还支持插件扩展功能，是目前最强大的调试工具，可以跟踪程序的执行过程、查看寄存器和内存内容等。

在官网下载压缩包，解压下载的压缩包直接双击.exe 启动即可使用。



运行示例截图：

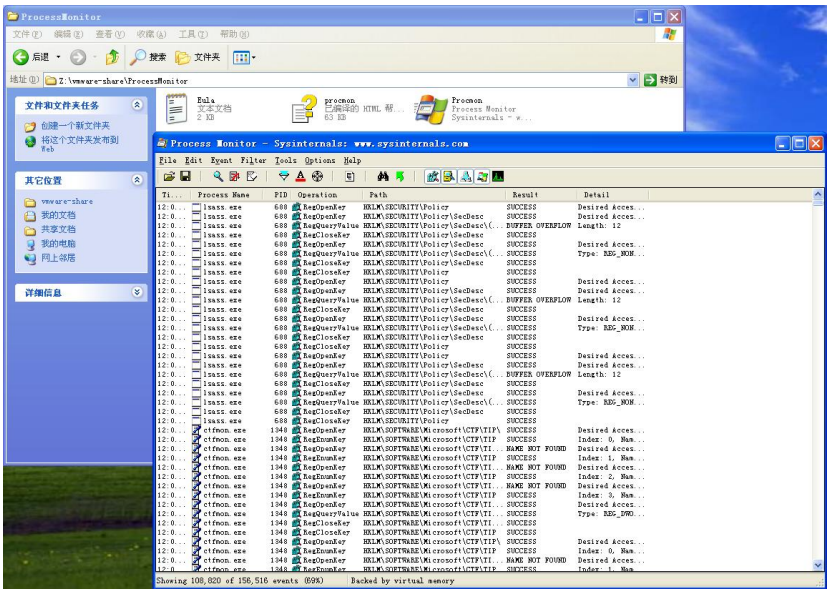


## （2） Process Monitor

Process Monitor 是一款由微软 Sysinternals 公司开发的包含强大监视和过滤功能的高级 Windows 监视工具，可实时显示文件系统、注册表、进程/线程的活动。它结合了两个 Sysinternals 的旧版工具 Filemon 和 Regmon 的功能，并添加了一个包含丰富的和非破坏性的广泛增强过滤功能列表，全面的事件属性（例如会话 ID 和用户名称），可靠的进程信息，每个操作的完整线程、堆栈与集成符号支持，同时记录到一个文件中，以及更多。其独一无二的强大功能将使 Process Monitor 在系统故障排除和恶意软件检测中发挥重要的作用。

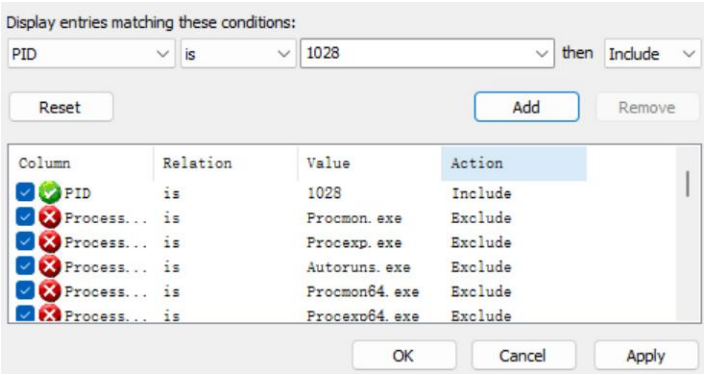
解压压缩包后，双击.exe 文件即可运行。


运行示例截图：



```
Ti...   Process Name  PID  Operation     Path                                Result           Detail
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy                SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   BUFFER OVERFLOW  Length: 12
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   SUCCESS          Type: REG_NON...
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy                SUCCESS
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy                SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   BUFFER OVERFLOW  Length: 12
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   SUCCESS          Type: REG_NON...
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy                SUCCESS
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy                SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   BUFFER OVERFLOW  Length: 12
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegOpenKey    HKLM\SECURITY\Policy\SecDesc        SUCCESS          Desired Acces...
12:0... lsass.exe     688  RegQueryValue HKLM\SECURITY\Policy\SecDesc\(...   SUCCESS          Type: REG_NON...
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy\SecDesc        SUCCESS
12:0... lsass.exe     688  RegCloseKey   HKLM\SECURITY\Policy                SUCCESS
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TIP\    SUCCESS          Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 0, Nam...
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TI...   NAME NOT FOUND   Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 1, Nam...
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TI...   NAME NOT FOUND   Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 2, Nam...
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TI...   NAME NOT FOUND   Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 3, Nam...
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TI...   SUCCESS          Desired Acces...
12:0... ctfmon.exe    1348 RegQueryValue HKLM\SOFTWARE\Microsoft\CTF\TI...   SUCCESS          Type: REG_DWO...
12:0... ctfmon.exe    1348 RegCloseKey   HKLM\SOFTWARE\Microsoft\CTF\TI...   SUCCESS
12:0... ctfmon.exe    1348 RegCloseKey   HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TIP\    SUCCESS          Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 0, Nam...
12:0... ctfmon.exe    1348 RegOpenKey    HKLM\SOFTWARE\Microsoft\CTF\TI...   NAME NOT FOUND   Desired Acces...
12:0... ctfmon.exe    1348 RegEnumKey    HKLM\SOFTWARE\Microsoft\CTF\TIP     SUCCESS          Index: 1, Nam...
Showing 108,820 of 156,516 events (69%)    Backed by virtual memory
```

打开过滤器，添加想要监控的应用，如图所示

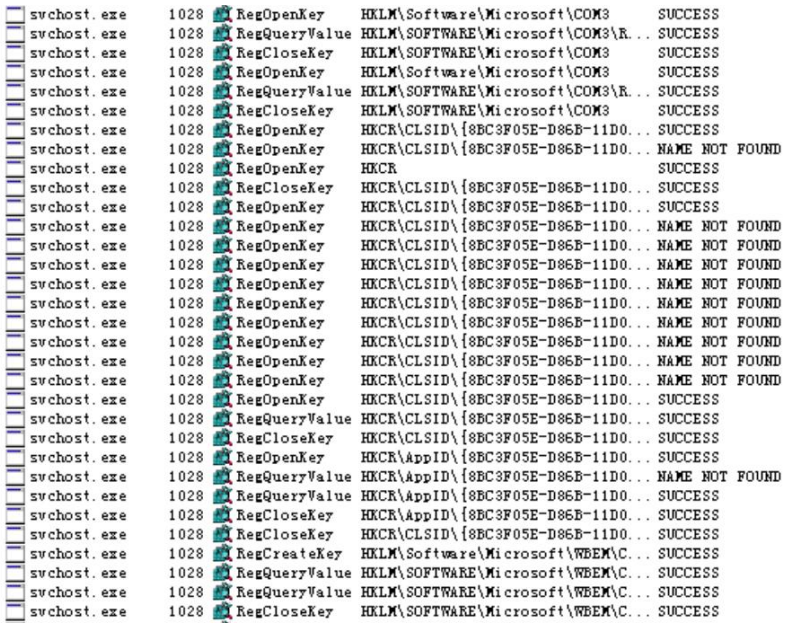


Display entries matching these conditions:

PID is 1028 then Include

| Column | Relation | Value | Action |
|---|---|---|---|
| ☑ ✓ PID | is | 1028 | Include |
| ☑ ✗ Process... | is | Procmon.exe | Exclude |
| ☑ ✗ Process... | is | Procexp.exe | Exclude |
| ☑ ✗ Process... | is | Autoruns.exe | Exclude |
| ☑ ✗ Process... | is | Procmon64.exe | Exclude |
| ☑ ✗ Process... | is | Procexp64.exe | Exclude |

搜索到的部分结果



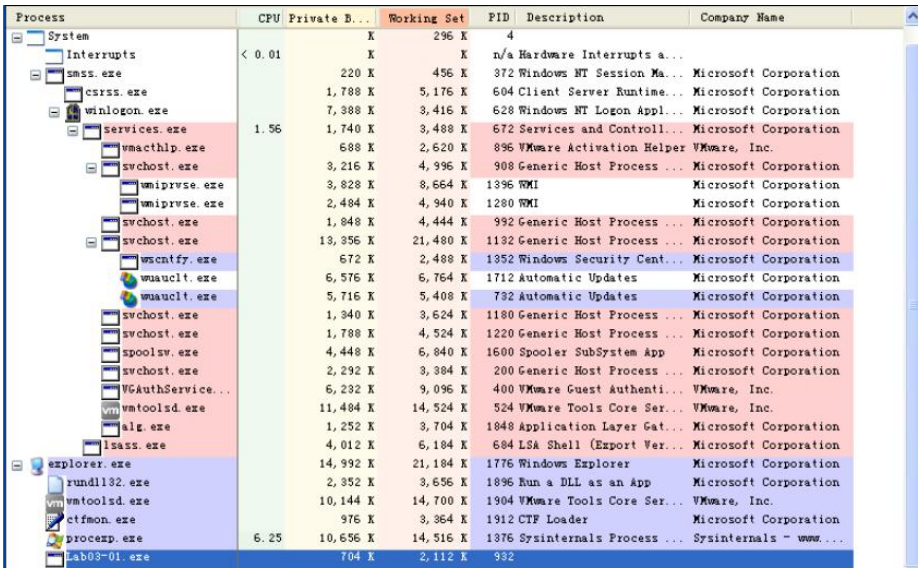
```
svchost.exe   1028 RegOpenKey    HKLM\Software\Microsoft\COM3          SUCCESS
svchost.exe   1028 RegQueryValue HKLM\SOFTWARE\Microsoft\COM3\R...     SUCCESS
svchost.exe   1028 RegCloseKey   HKLM\SOFTWARE\Microsoft\COM3          SUCCESS
svchost.exe   1028 RegOpenKey    HKLM\Software\Microsoft\COM3          SUCCESS
svchost.exe   1028 RegQueryValue HKLM\SOFTWARE\Microsoft\COM3\R...     SUCCESS
svchost.exe   1028 RegCloseKey   HKLM\SOFTWARE\Microsoft\COM3          SUCCESS
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR                                  SUCCESS
svchost.exe   1028 RegCloseKey   HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegOpenKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegQueryValue HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegCloseKey   HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegOpenKey    HKCR\AppID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegQueryValue HKCR\AppID\{8BC3F05E-D86B-11D0...     NAME NOT FOUND
svchost.exe   1028 RegQueryValue HKCR\AppID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegCloseKey   HKCR\AppID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegCloseKey   HKCR\CLSID\{8BC3F05E-D86B-11D0...     SUCCESS
svchost.exe   1028 RegCreateKey  HKLM\Software\Microsoft\WBEM\C...     SUCCESS
svchost.exe   1028 RegQueryValue HKLM\SOFTWARE\Microsoft\WBEM\C...     SUCCESS
svchost.exe   1028 RegQueryValue HKLM\SOFTWARE\Microsoft\WBEM\C...     SUCCESS
svchost.exe   1028 RegCloseKey   HKLM\SOFTWARE\Microsoft\WBEM\C...     SUCCESS
```

## （3） Process Explorer

Process Explorer 是一个程序,将会显示进程的次数运行。它可以通过任务管理器帮助我们捕获消耗 CPU 的内存未被卡住的进程。Process Explorer 让使用者能了解看不到的在后台执行的处理程序，能显示目前已经载入哪些模块，分别是正在被哪些程序使用着，还可显示这些程序所调用的 DLL 进程，网络连接，以及他们所打开的句柄等。Process Explorer 最大的特色就是可以中终任何进程，甚至包括系统的关键进程。

解压压缩包后，双击.exe 文件即可运行。

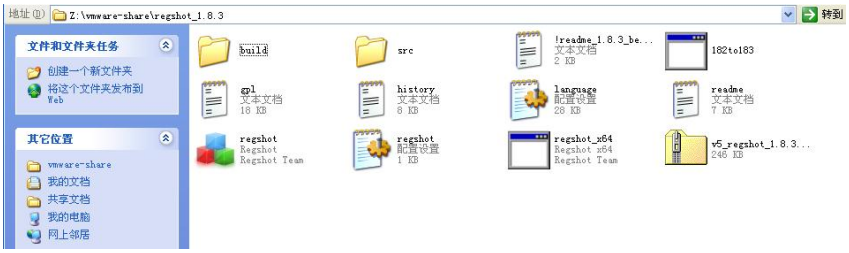

运行示例截图：




## （4） RegShot

RegShot 是一种注册表比较工具，它通过两次抓取注册表快照而快速地比较出两次快照中间所做的修改。它还可以将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 Windows 目录和 System 目录中文件的变化，为手工卸载某些软件创造条件。

解压压缩包后，双击.exe 文件即可运行。




运行示例截图：

点击 1st shot 建立第一个快照


修改后点击 2nd shot 建立第二个快照

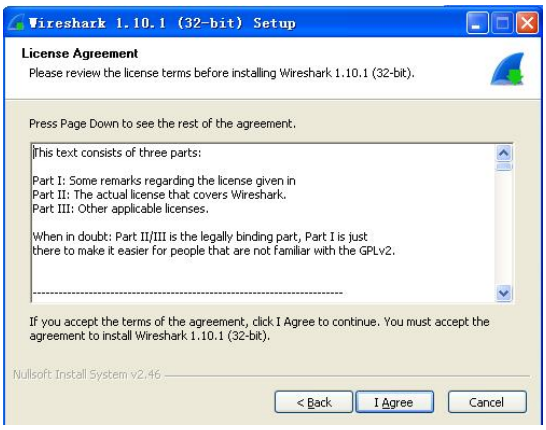

点击 compare 可进行对比

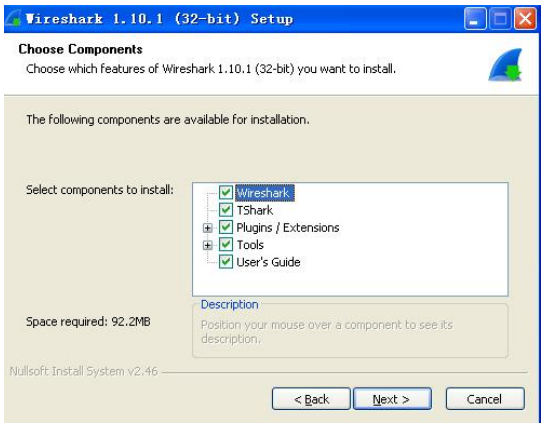

Compare 完成后会生成一个文本，在其中可以看到在两个快照期间发生变化的注册表字段与值。

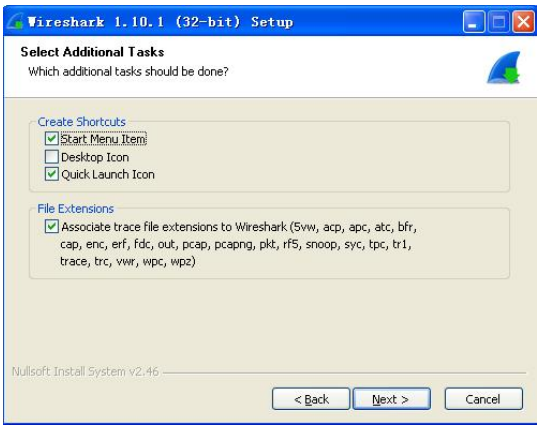
### （5） WireShark

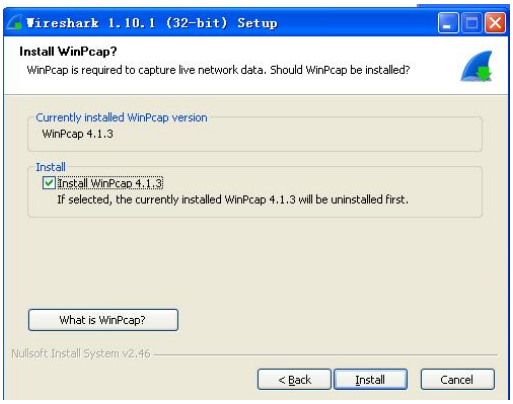
WireShark 是一个网络分析工具，可以运行在 Windows 和 Linux 操作系统上，主要是用来捕获网络数据包，并自动解析各类协议数据包，为用户显示数据包的详细信息，供用户对数据包进行分析，以便查看恶意软件的通信行为。

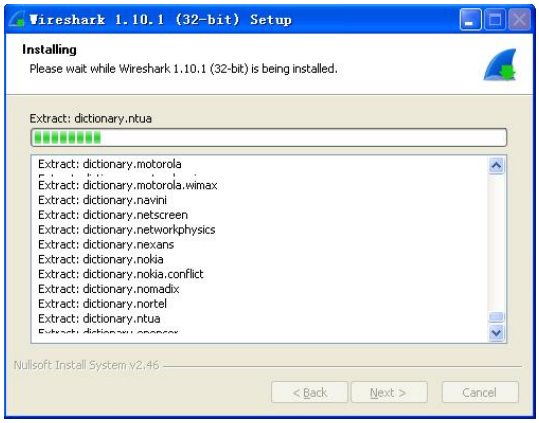
按照提示逐步安装即可（一直 next 即可）


Wireshark 1.10.1 (32-bit) Setup
License Agreement
Please review the license terms before installing Wireshark 1.10.1 (32-bit).
Press Page Down to see the rest of the agreement.
This text consists of three parts:
Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.
When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 1.10.1 (32-bit).
Nullsoft Install System v2.46
< Back
I Agree
Cancel

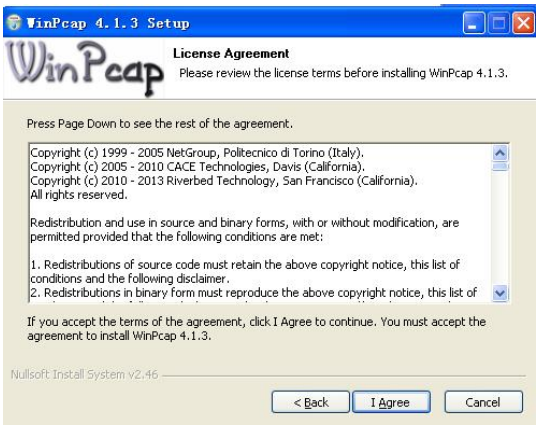

Wireshark 1.10.1 (32-bit) Setup
Choose Components
Choose which features of Wireshark 1.10.1 (32-bit) you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Plugins / Extensions
Tools
User's Guide
Description
Position your mouse over a component to see its description.
Space required: 92.2MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

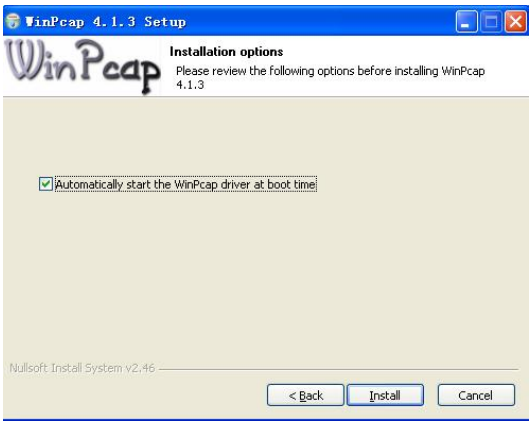

Wireshark 1.10.1 (32-bit) Setup
Select Additional Tasks
Which additional tasks should be done?
Create Shortcuts
Start Menu Item
Desktop Icon
Quick Launch Icon
File Extensions
Associate trace file extensions to Wireshark (5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz)
Nullsoft Install System v2.46
< Back
Next >
Cancel


Wireshark 1.10.1 (32-bit) Setup
Install WinPcap?
WinPcap is required to capture live network data. Should WinPcap be installed?
Currently installed WinPcap version
WinPcap 4.1.3
Install
Install WinPcap 4.1.3
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.
What is WinPcap?
Nullsoft Install System v2.46
< Back
Install
Cancel



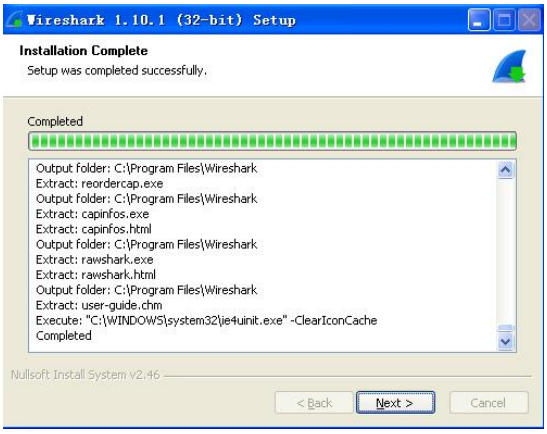

在安装过程中会跳转到 WinPcap 的安装，也是一直 next 即可

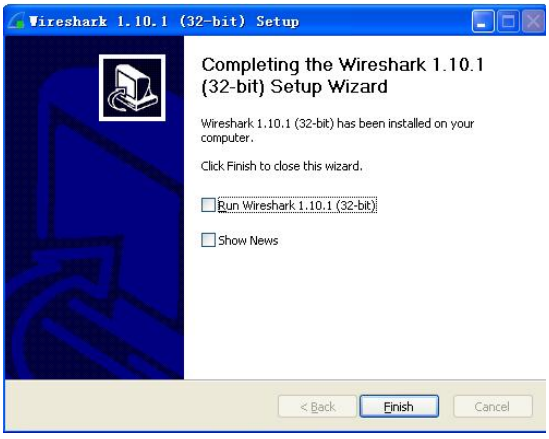



WinPcap 安装完成

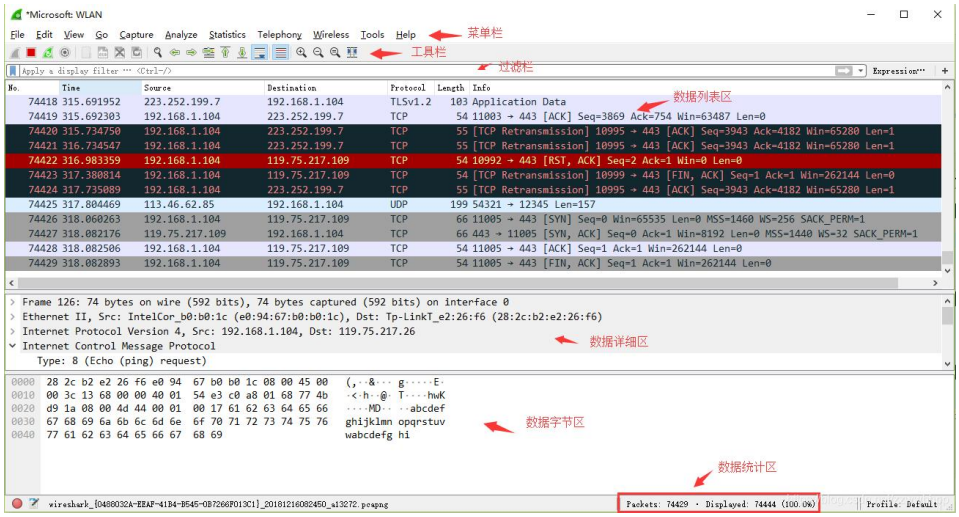

WireShark 继续安装




WireShark 安装完成




WireShark 运行示例截图：




# 四、实验结论及心得体会

## （一） 实验结论

本次实验成功创建和配置了一个虚拟机环境，安装了 xp 系统。

安装了多个静态分析工具，这些工具允许我们分析二进制文件的结构和内容，识别字符串、查看文件头部信息，并分析文件的依赖关系。这些分析有助于理解文件的功能和可能的威胁。

安装和使用了多个动态分析工具，这些工具使我们能够监视和分析恶意软件在运行时的行为，包括文件操作、注册表访问、网络通信等。动态分析可以帮助我们深入了解恶意软件的功能和影响。

## （二） 心得体会

在进行恶意软件分析时，务必保持高度的安全意识。恶意软件可能会具有破坏性和危险性，因此需要采取适当的预防措施，如离线分析、网络隔离等。可以创建虚拟机，但需确保虚拟机环境隔离且可控制，以避免潜在的风险和威胁传播到物理计算机。

实验中使用的静态和动态分析工具各具特点，可以从不同角度深入分析恶意软件。熟练掌握这些工具对于进行有效的恶意软件分析至关重要。