

**恶意代码分析与防治实验报告**

**实验三：基本动态分析**

****

学 院 网安

专 业 信安

学 号 2113662

姓 名 张丛

班 级 信安一班

1. **实验目的**

完成教材Lab3的实验内容，编写Lab3样本的Yara引擎规则，并测试规则的执行效率。

1. **实验原理**

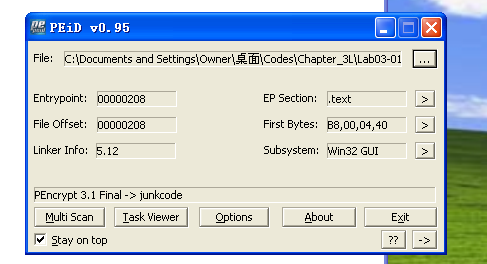
基本动态工具的应用，yara

1. **实验过程**

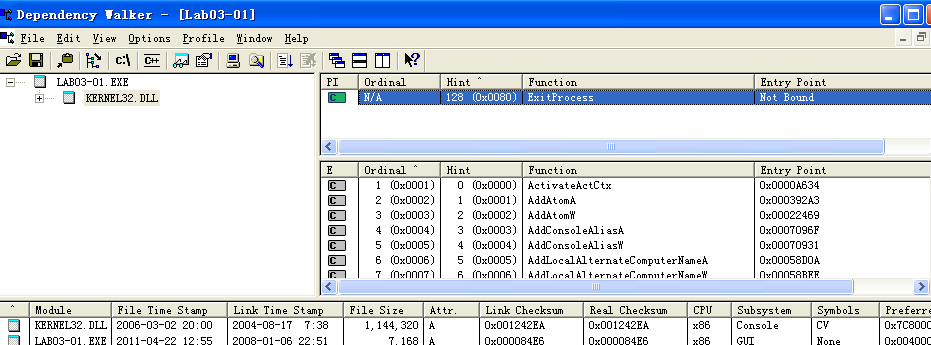
## Lab 3-1

### 找出这个恶意代码的导入函数与**[字符串](https://so.csdn.net/so/search?q=%E5%AD%97%E7%AC%A6%E4%B8%B2&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/m0_37442062/article/details/_blank)**列表？

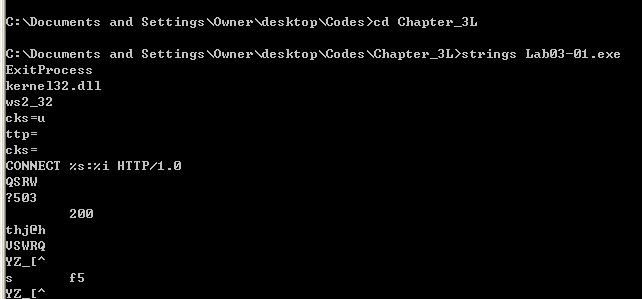
PEID查看加壳信息：

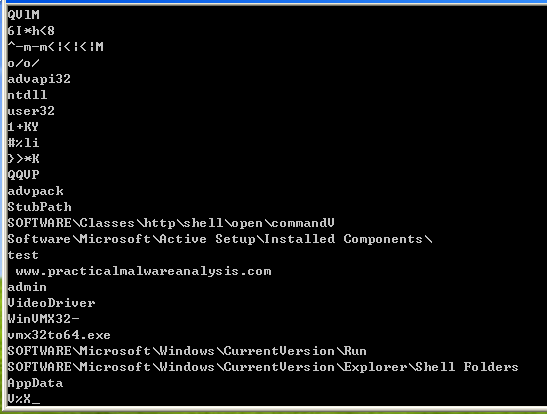


使用Dependency Walker 查看导入函数：



strings程序查看字符串：





其中比较可疑的字符串：

CONNECT %s:%i HTTP/1.0

admin

vmx32to64.exe

[www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)

SOFTWARE\Classes\http\shell\open\commandV

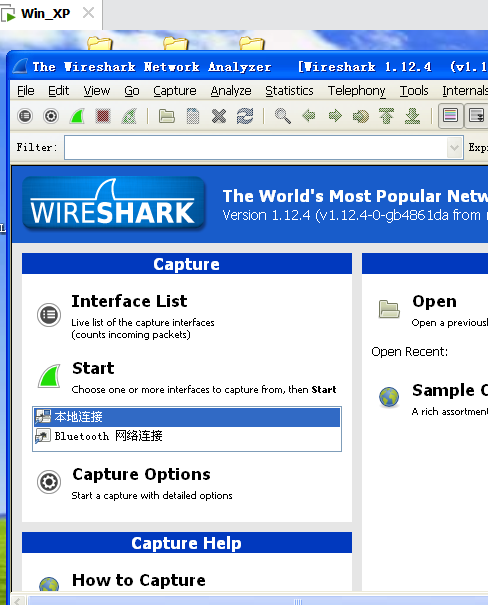
Software\Microsoft\Active Setup\Installed Components

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

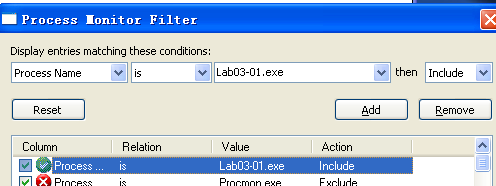
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

### 这个恶意代码在主机上的感染迹象特征是什么？

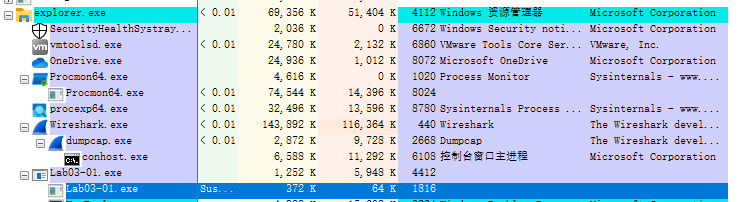
启动wireshark：



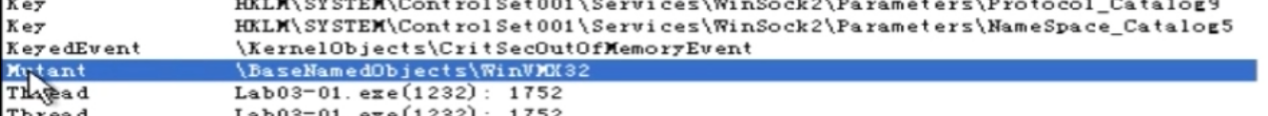
打开process monitor,设置过滤器，进程名为Lab03-01.exe:



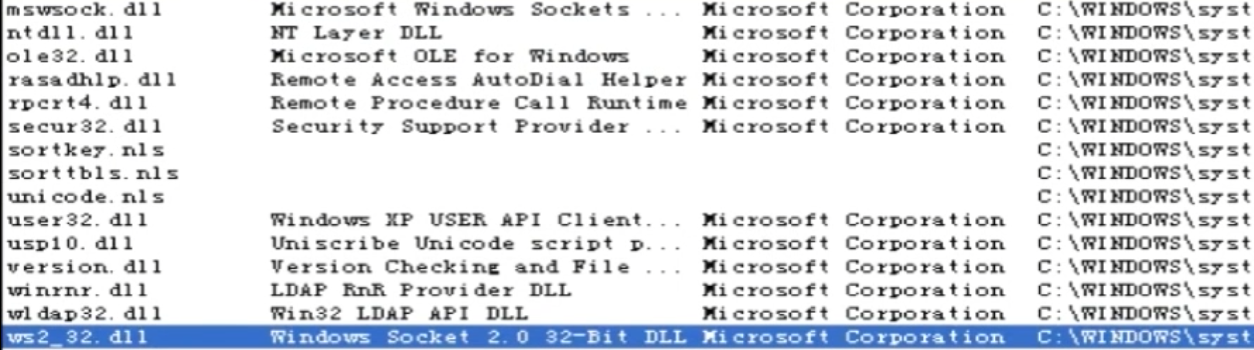
打开process explorer,运行恶意代码Lab03-01.exe,可以看到捕获的进程：



通过view选项查看HANDLEs 和 DLLs:

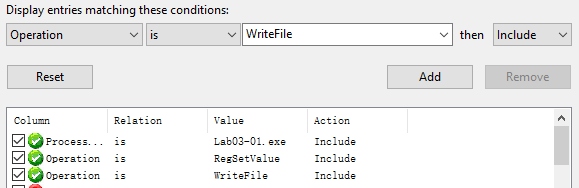


可以看到创建了一个互斥量，创建互斥量的主要作用是某一时刻某程序能单独占用某个操作。



DLLs包含ws2\_32.dll，可能存在联网操作。

增加过滤器内容：



结果如下：



知道有写入文件和修改注册表的行为。

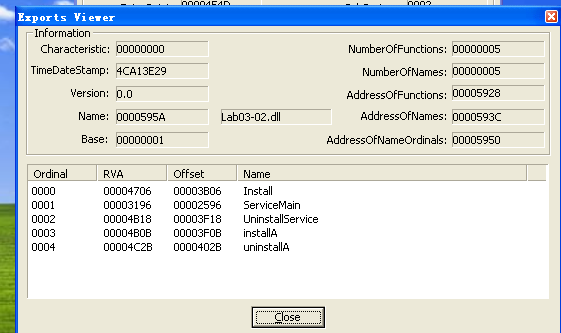
### 这个恶意代码是否存在一些有用的网络特征码？如果存在，它们是什么？

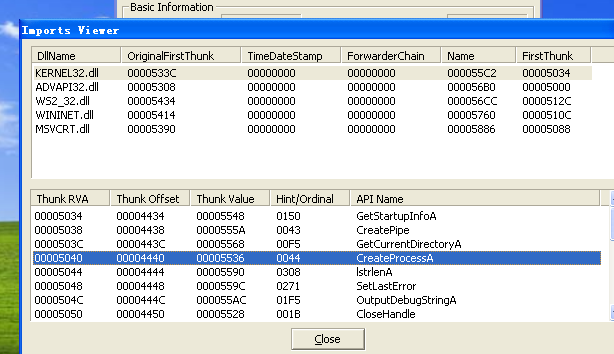
恶意代码在进行网址的域名解析后，持续地广播大小为256字节的数据包，其中包含看似随机的二进制数据。

## Lab 3-2

### 你怎样才能让这个恶意代码自行安装？

PEiD查看导出表和导入表：



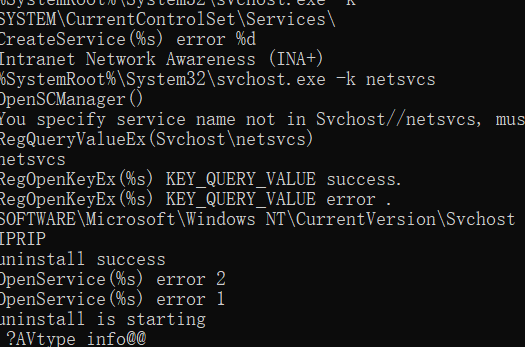


程序会创建进程和线程：CreateProcessA和CreateThread；

程序还会创建服务，操控服务，操作注册表；

程序还会网络进行操作。

strings查看字符串：



可以看到installA函数。

可以用

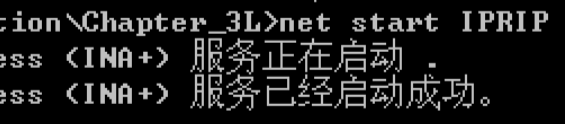
**rundll32.exe Lab03-02.dll,installA**

这一行命令来安装

### 安装之如何让恶意代码运行起来？

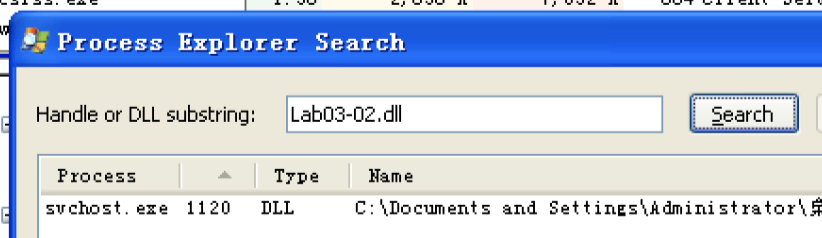
使用命令

**net start IPRIP**



### 怎么可以找到这个恶意代码在哪个进程下运行的？

使用process explorer 的search功能：



在svchost.exe进程中。

### 你可以在procmon中设置什么样的过滤器，才能收集到这个恶意代码的信息？

在process monitor工具中，使用PID进行过滤。

### 这个恶意代码在主机上的感染迹象特征是什么？

使用RegShot查看主机变化：

**Keys added: 6**

HKLM\SYSTEM\ControlSet001\Services\*IPRIP\*

HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters

HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security

HKLM\SYSTEM\CurrentControlSet\Services\IPRIP

HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters

HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

……

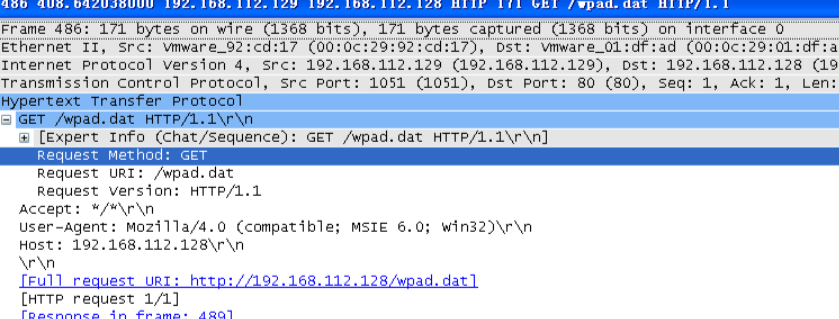
……

### **Total changes: 27**

恶意代码安装了IPRIP的服务。

### 此恶意代码是否存在一些有用的网络特征码？

使用wireshark:

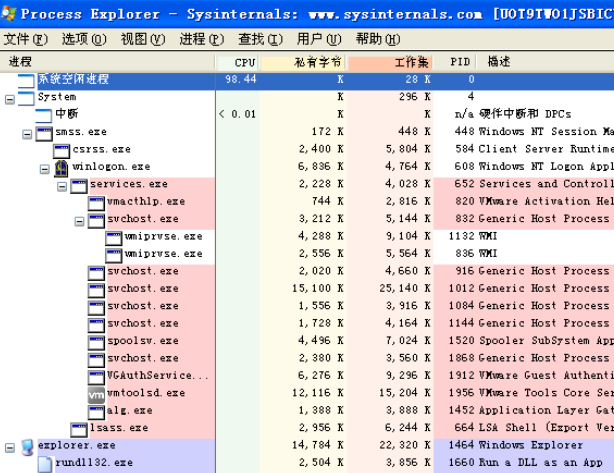


能看到请求报文。

## Lab 3-3

### 当你使用Process explorer工具进行监视时，你注意到了什么？

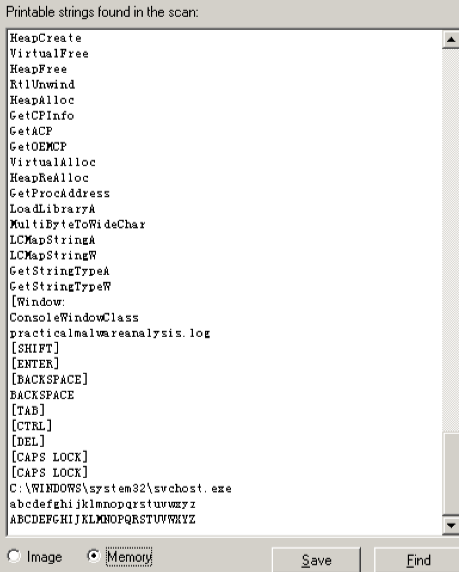
使用process explorer，运行程序：



可以看到Lab03-03.exe进程迅速消失，即迅速将自身删除，并创建了子进程svchost.exe。

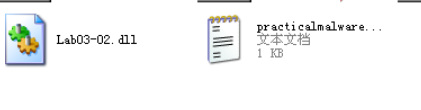
### 你可以找出任何的[内存](https://so.csdn.net/so/search?q=%E5%86%85%E5%AD%98&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/m0_37442062/article/details/_blank)修改行为吗？

使用process monitor,查看memory:

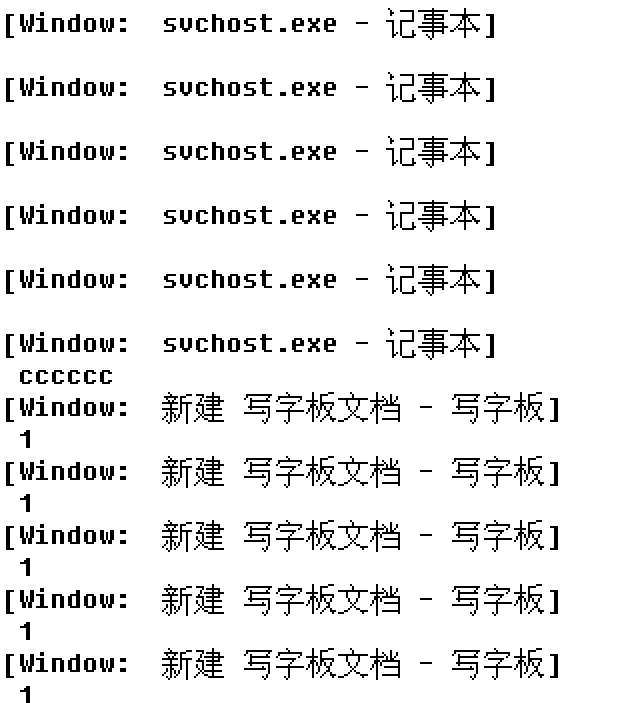


内存比映像中多了一些奇怪的东西，[ENTER]、[BACKSPACE]、[CAPS LOCK]表明可能是击键记录器。

还出现了一个日志文件:



内容如下：



### 这个恶意代码在主机上的感染迹象特征是什么？

从上面的日志文件可以看出，恶意代码在记录键盘。

然后使用process monitor:



可以看到恶意代码频繁的创建写入文件。

### 这个恶意代码的目的是什么？

这个程序在svchhost.exe进程上执行了进程替换，来启动一个击键记录器。

## Lab 3-4

### 当你运行这个文件时，会发生什么呢？

双击运行后发现程序消失，把自己杀了。

### 是什么原因造成动态分析无法有效实施？

我本来以为是因为自己删除自己所以无法有效分析。

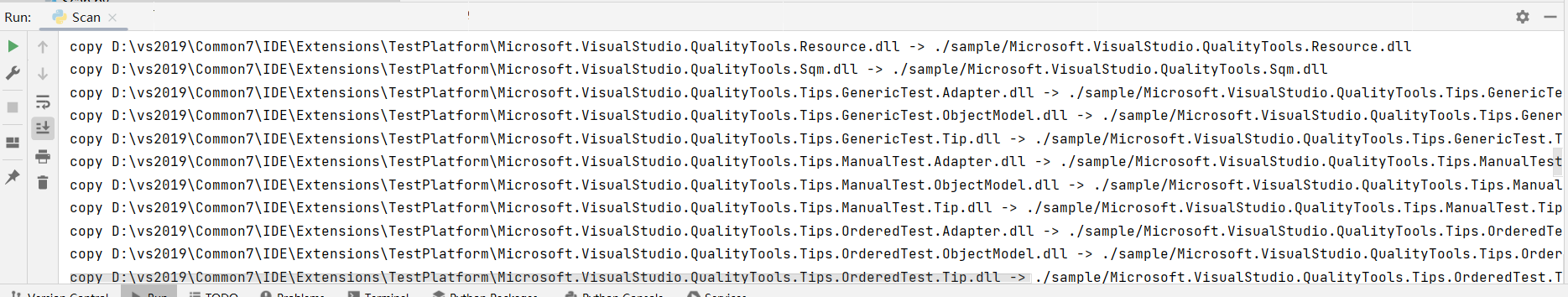
但，“我们怀疑可能需要提供一个命令行参数，或者这个程序的某个部件缺失了。”

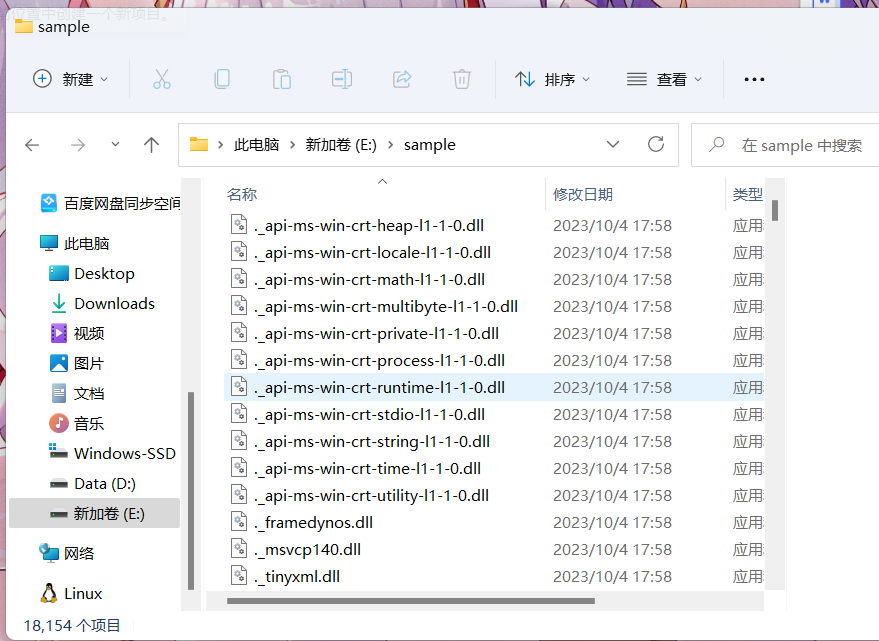
### 是否有其它方式来运行这个程序？

我们尝试使用在字符串列表中显示的一些命令行参数，比如-in，但这样做却没有得到有效的结果，需要更深入的分析。

## Lab 3-5

先使用python程序总集电脑内的exe、dll文件：





编写Lab3样本的yara引擎规则：

rule Lab3

{

meta:

description = "rules for Lab3"

date = "202x/xx/xx"

strings:

$a = "vmx32to64" wide ascii

$b = "serve.html" wide ascii

$c = "[www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)" wide ascii

$d = "http://www.malwareanalysisbook.com" wide ascii

$e = "svchost" wide ascii

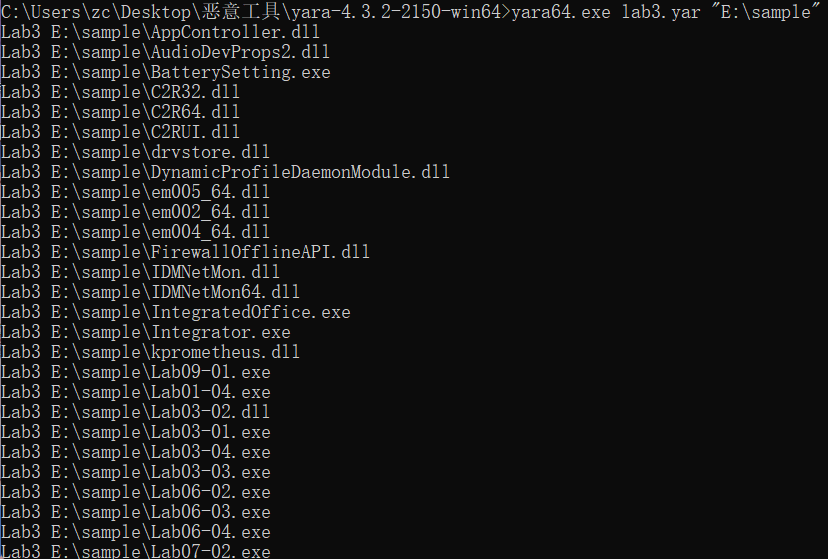
$f = "practicalmalwareanalysis.log" wide ascii

condition:

any of them

}

进行扫描：



可以看到确实扫描出了实验样本。

1. **实验结论及心得体会**

**熟悉了基本动态工具的使用，实验过程中也做到了静态工具和动态工具的结合利用。**

**在实验过程中遇到的困难在于虚拟机Apate的网络配置，在网上查找了很多博客但不能尽数解决问题。**

**另外的，不算在课程知识点的难题在于，官方下载或者教材网址下载的动态工具，基本上都不兼容XP系统了，，，需要花很多很多时间去找能够在XP系统运行的动态工具。当然，这也是自身的经验不足，但无疑会大大降低做实验的耐心。以及XP虚拟机时不时崩溃的问题。**

**还针对lab3编写了yara规则，扫描的结果也成功扫描出了lab3的样本。**