计算机病毒及其防治技术

Lab4-Yara 引擎检测

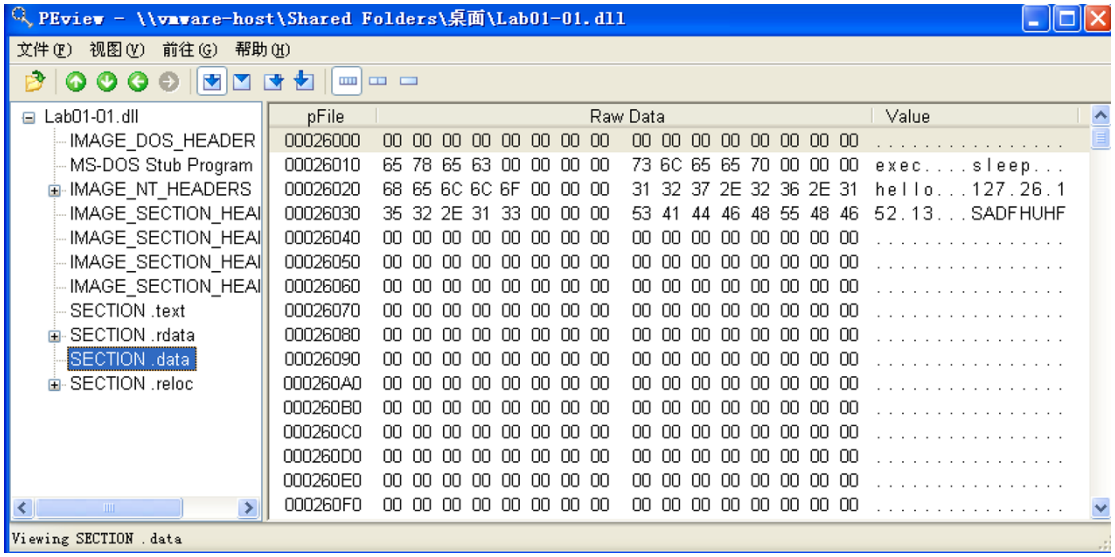
沙璇 1911562

Lab 4

Q1：对 Lab1 和 Lab3 的样本编写 Yara 规则

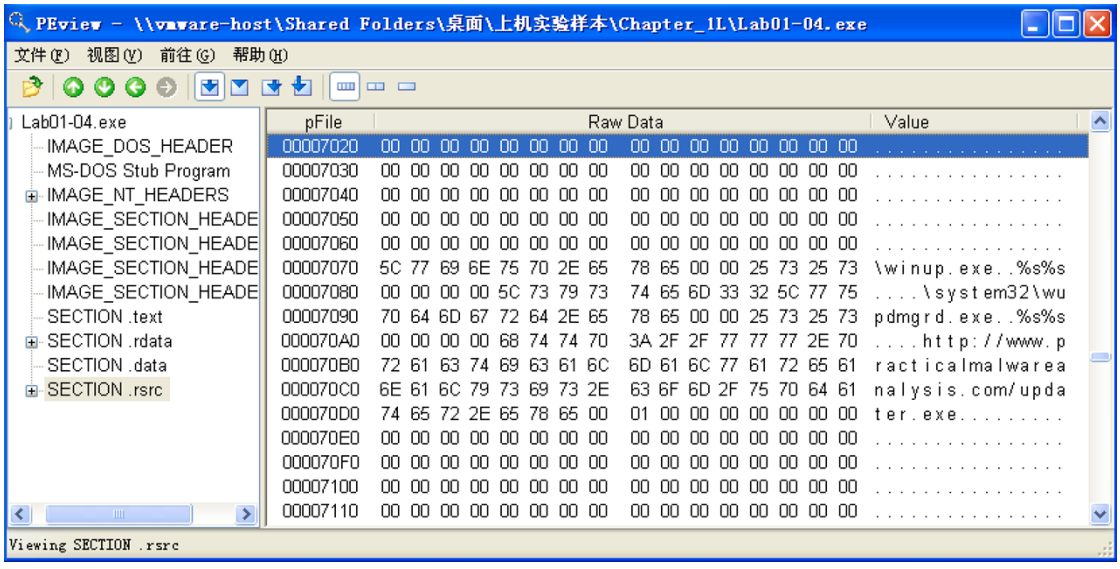
编写 yara 规则，需要对病毒样本进行分析，根据其特征进行编写。

根据实验报告 1，Lab01-01：



得到 ip 地址 127.26.152.13

Lab01-04：



得到字符串 http://www.practicalmalwareanalysis.com

以及 winup.exe

Yara 规则编写如下：

rule ll {

meta:

description="lab1"

strings:

$a="127.26.152.13" wide ascii

$b="http://www.practicalmalwareanalysis.com" wide ascii

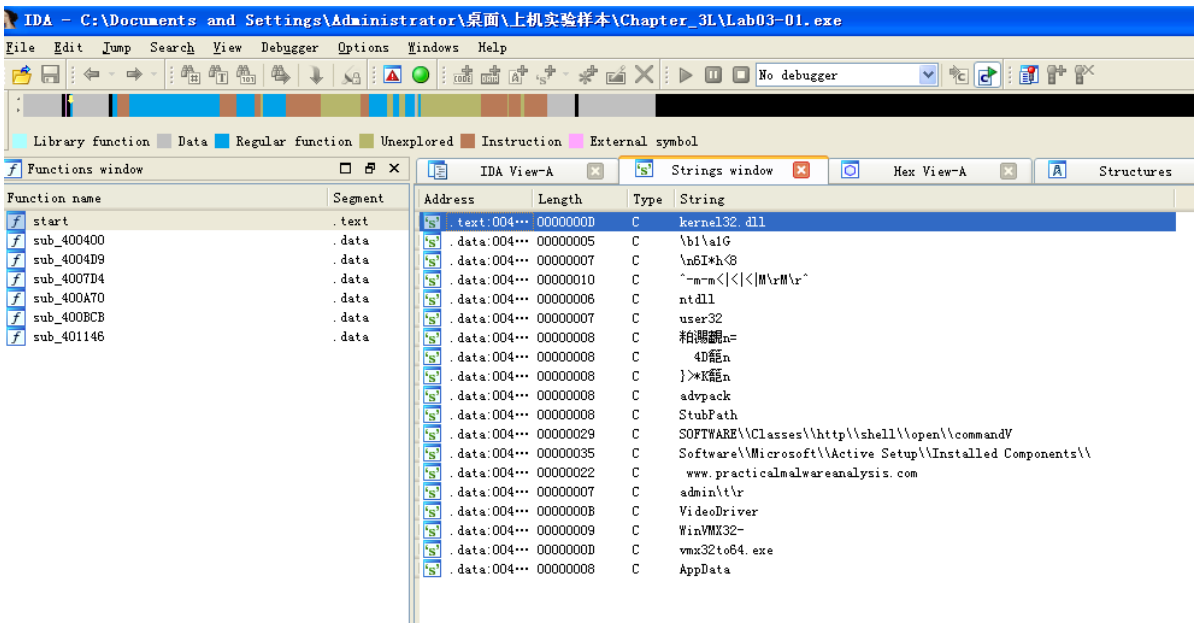
$c="winup.exe" wide ascii

condition:

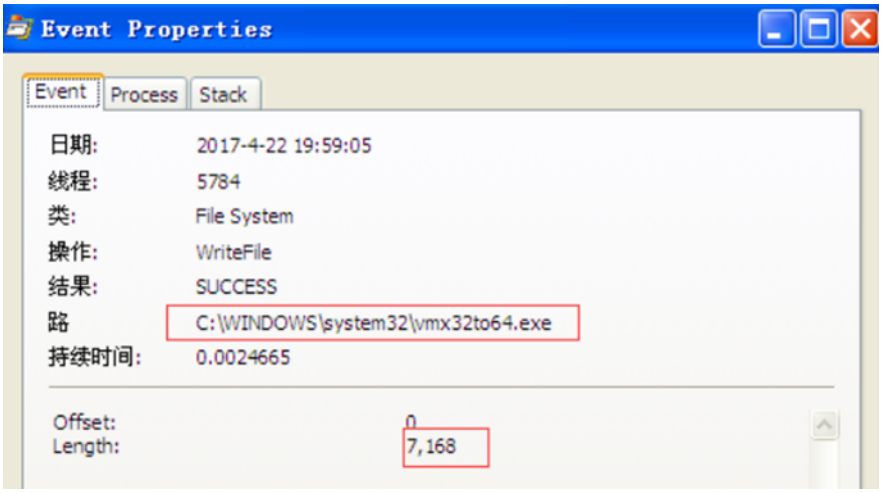
$a or $b or $c

}

根据实验报告 3，lab03-01：

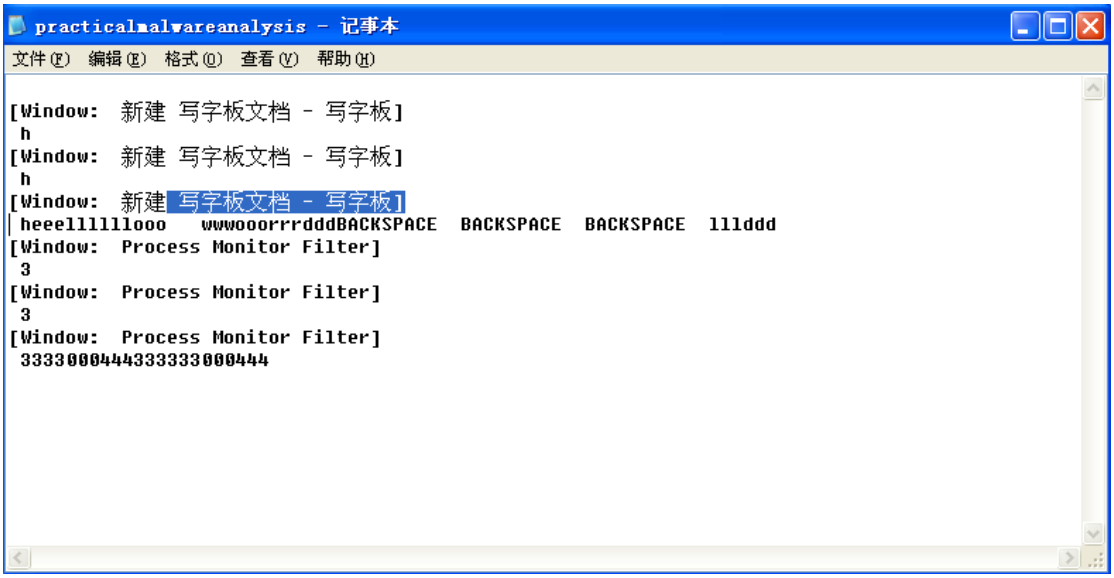


网址 www.practicalmalwareanalysis.com



写入的新程序 vmx32to64.exe

Lab03-03：



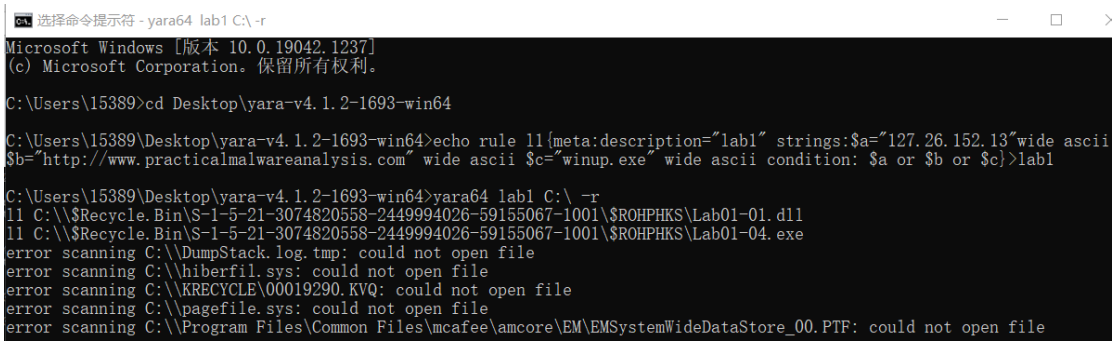
找到同一个目录下生成的 log 文件：practicalmalwareanalysis.log

Yara 规则编写如下：

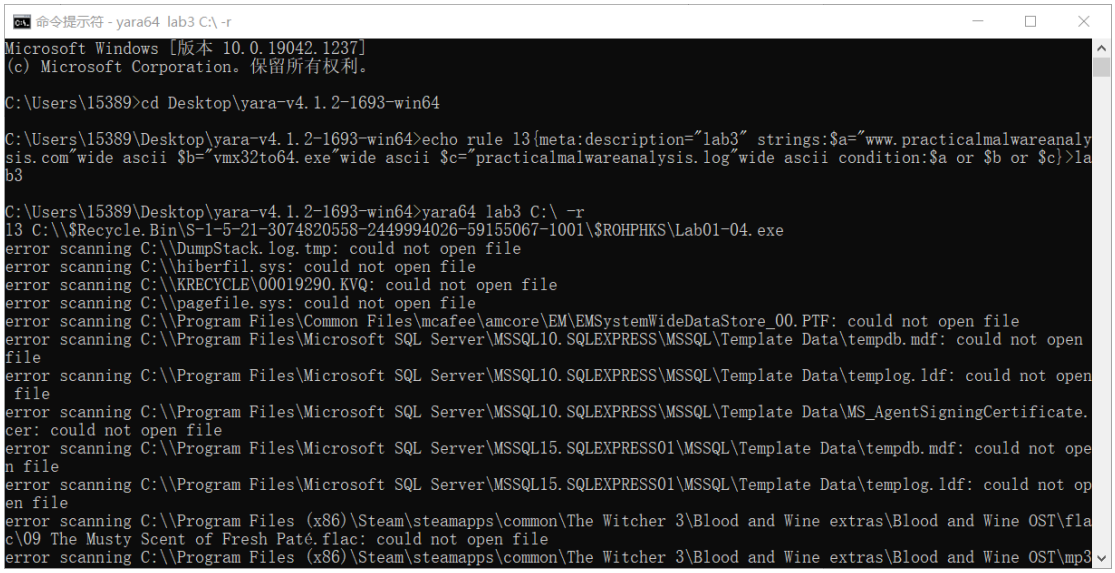
```
rule l3{
meta:
description="lab3 "
strings:
$a="www.practicalmalwareanalysis.com"wide ascii
$b="vmx32to64.exe"wide ascii
$c="practicalmalwareanalysis.log"wide ascii

condition:
$a or $b or $c
  }
```

Q2：使用自己编写的规则对自己电脑的 C 盘进行 Yara 引擎的扫描，记录扫描所用时间

Lab1 规则通过 yara64 运行，输入 C:/目录和-r 全文件指令，对本机的 C 盘进行扫描，记录扫描时间大约为 10 分钟。



Lab2 规则 yara64 运行，输入 C:/目录和-r 全文件指令，对本机的 C 盘进行扫描，记录扫描时间大约为 8 分钟。



Q3：讨论哪些 Yara 条件执行效率高，哪些 Yara 条件执行效率低。如何改进那些执行效率低的 Yara 条件？

- 低效的 yara 规则可以匹配当前的样本，但匹配不了其他相似的恶意样本（如同一个家族的）。
- yara 规则太过具体，也同样不能匹配多个样本。
- 生成高效通用的 yara 规则，能通用地匹配恶意软件，不会出现在合法软件中。同时，给扫描样本加上大小限制，达到更精确的效果。