第3章 故障排查

终端在运行过程中，由于应用复杂性和攻击多样性，往往表现出不同的特征。这些特征可能隐藏于网络流量、系统进程、动态链接库、应用程序等各种系统组件中，如何将这些特征从庞大的组件信息中提取出来，用于解决相应的故障现象、安全问题，需要用到一些特定的工具来提取这些特征。

本章主要学习终端安全管理系统常见的故障排查工具的使用方法，用于检查、监控包括网络、进程、应用在运行过程中，如何对系统的资源进行调用、数据的流向、用户权限的管理和调用等方面的内容。对于实际工作中遇到的问题，使用此类工具也可以获得比较好的分析效果，对于了解和掌握解决问题的方法非常有帮助。

3.1 网络流量

3.1.1 终端安全管理系统问题排查——TCPView 使用实验

【实验目的】

掌握 TCPView 的使用方法。

【知识点】

TCPView，端口。

【场景描述】

A 公司的安全运维工程师小王怀疑内网终端可能中了木马，需要使用 TCPView 分析当前终端的网络连接情况，对异常流量进行分析，以便排查分析木马行为。请协助小王使用 TCPView 工具分析网络流量。

【实验原理】

木马程序运行后，通常会尝试连接远控端，与远控端进行通信，在此过程中通常会打开某个端口，如果有通信过程就有可能会创建通信进程。TCPView 是 Sysinternals 工具包中的一款免费软件，该软件是绿色软件不需要安装，直接运行即可。TCPView 主要用于查看端口和线程，TCPView 虽然是静态显示端口和线程，但由于运行快捷、方便，占用

资源比较少，在排查时可作为监视工具进行辅助分析。

【实验设备】

主机设备：Windows Server 2008 R2 主机 1 台，Windows 7 主机 1 台。
网络设备：交换机 1 台。

【实验拓扑】

实验拓扑如图 3-1 所示。

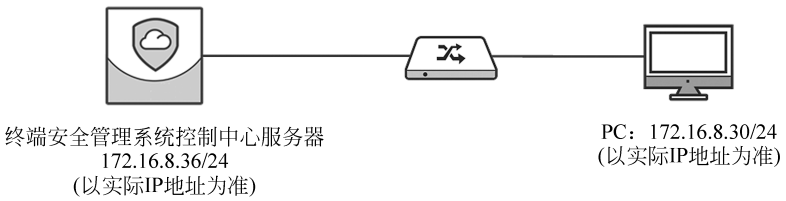

图 3-1　终端安全管理系统 TCPView 使用实验拓扑

【实验思路】

使用 TCPView 查看当前网络连接信息。

【实验步骤】

(1) 进入实验对应拓扑，登录右侧 PC 终端，如图 3-2 所示。

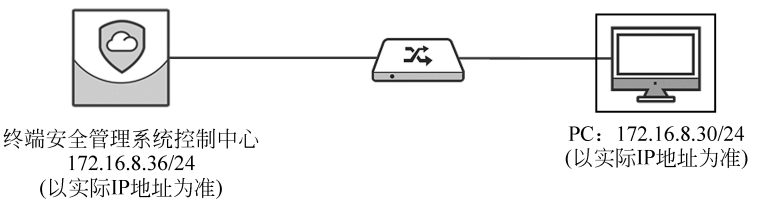

图 3-2　登录 PC 终端

(2) 使用账户 Administrator 和密码 123456 登录终端，运行桌面上的 TCPView 程序，如图 3-3 所示。

图 3-3　TCPView 程序图标

【实验预期】

使用 TCPView 查看网络连接信息。

【实验结果】

(1) TCPView 运行之后主界面如图 3-4 所示。

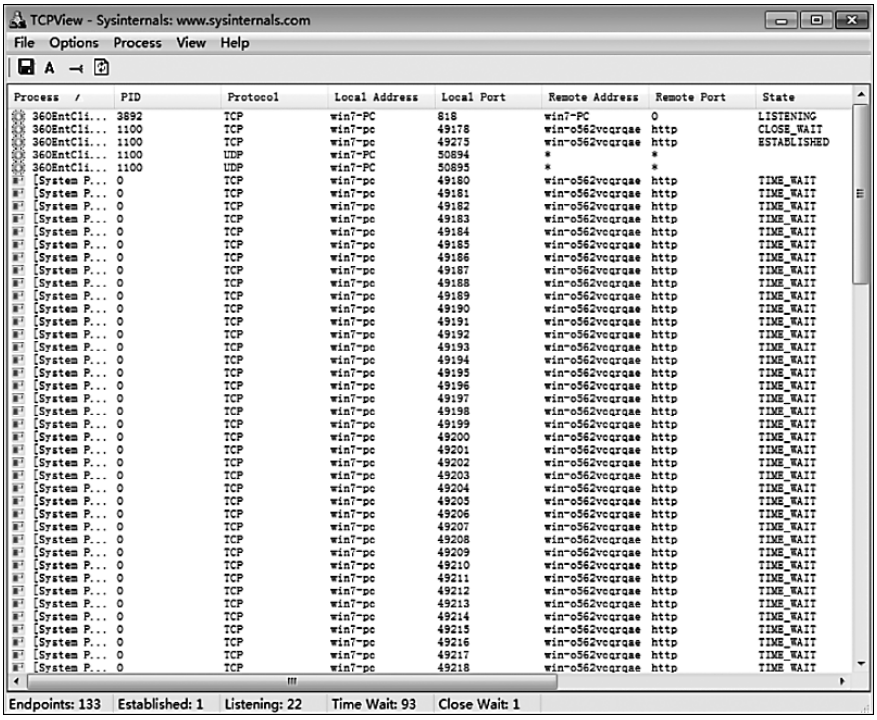

图 3-4　TCPView 运行界面

(2) 单击上方菜单栏中的 View 可以看到两个选项：Update Speed(更新速度)和 Refresh Now(立即刷新)。单击 Refresh Now 命令可以立即刷新当前的进程和网络状态，单击 Update Speed 命令可以选择自动刷新的间隔时间，可以选择 1 秒、2 秒、5 秒和“暂停刷新”，本实验选择刷新间隔为 5 秒，如图 3-5 所示。

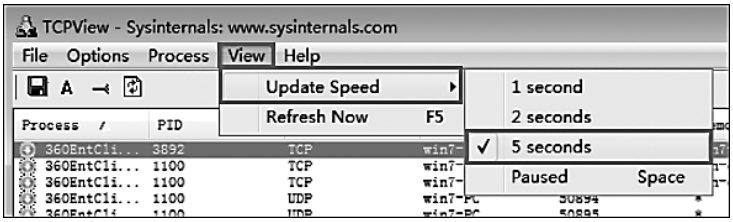

图 3-5　刷新参数设置

(3) 主内容显示区域显示的内容主要分为 12 列，分别是 Process(进程名称)、PID(进

程 ID)、Protocol(协议)、Local Address(本地地址)、Local Port(本地端口)、Remote Address(远程地址)、Remote Port(远程端口)、State(连接状态)、Sent Packets(发送的数据包数量)、Sent Bytes(发送了多少字节数据)、Rcvd Packets(接收数据包数量)、Rcvd Bytes(接收了多少字节数据),如图 3-6 所示。

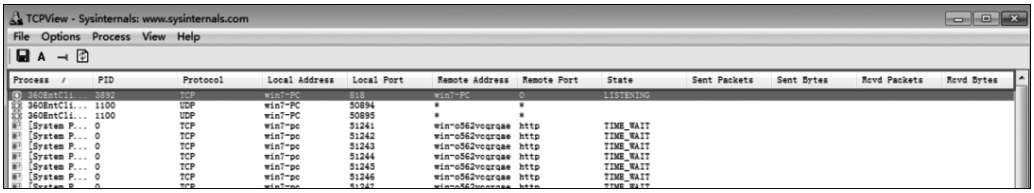

图 3-6　主内容显示列

(4) TCPView 默认会把 Remote Address(远程地址)和 Local Address(本地地址)显示为相对应的主机的名称,如果想要设置为显示 IP 地址,单击上方的 Options 菜单,取消勾选 Resolve Addresses 即可,如图 3-7 所示。

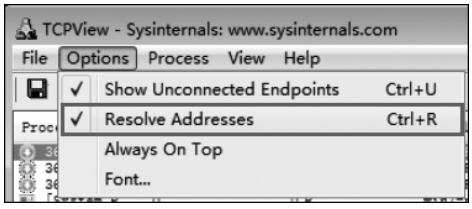

图 3-7　Resolve Addresses 选项

(5) 刷新时某个进程颜色为绿色时,表示该进程为相对于上次刷新时新增的进程,如图 3-8 所示。

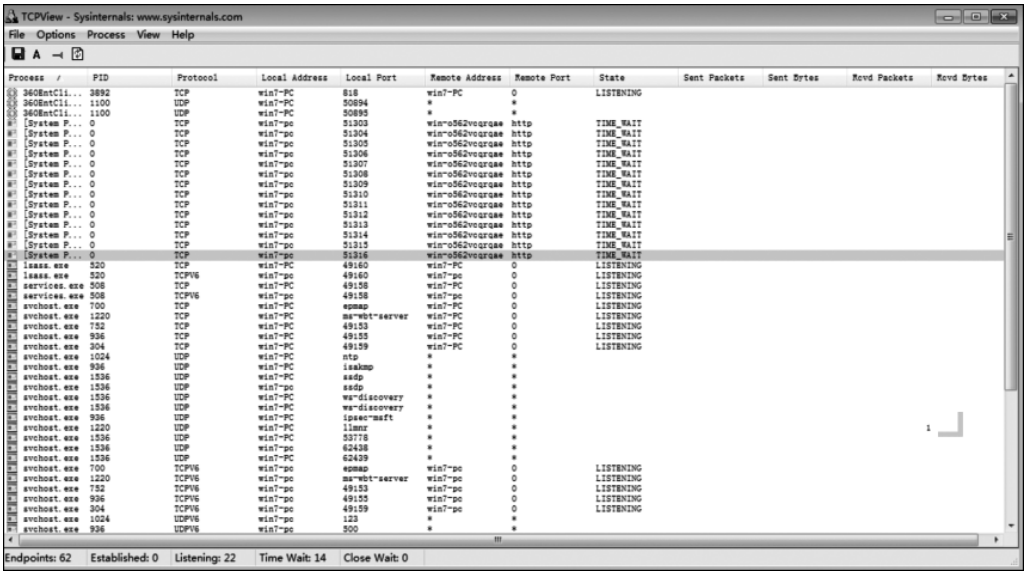

图 3-8　新增的进程信息

（6）当进程颜色为红色时，表示该进程相对于上次刷新时已经销毁的进程，如图 3-9 所示。

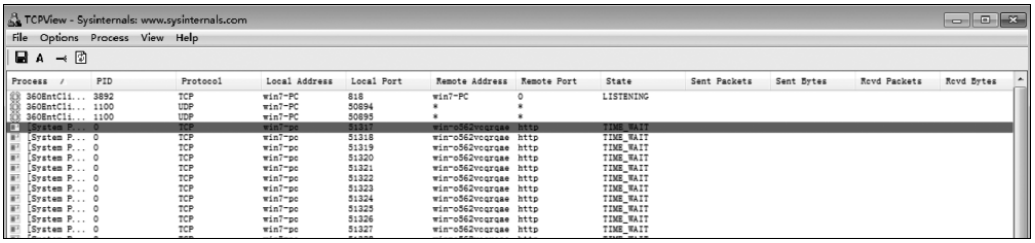

图 3-9　销毁的进程信息

（7）单击选中要操作的进程，右击会弹出可对该进程进行相应的操作选项，如图 3-10 所示。

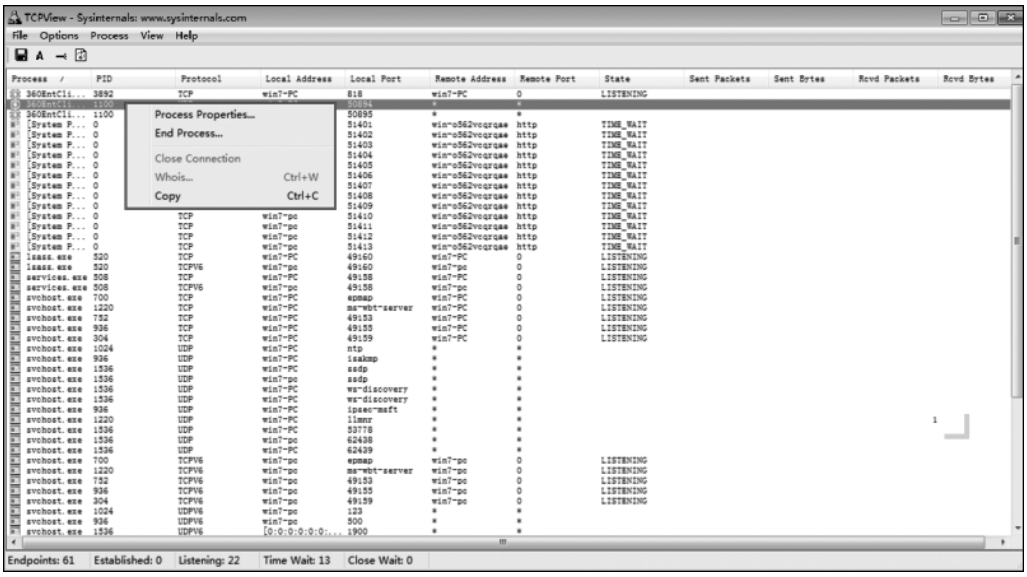

图 3-10　对选中进程进行操作

（8）选择弹出菜单中的 Process Properties（进程属性），可以查看该进程的名称、版本以及 Path（路径），单击 End Process 按钮可以结束该进程，如图 3-11 所示。

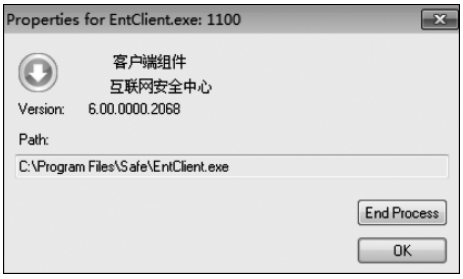

图 3-11　进程属性

（9）如果选择弹出菜单中的 Copy 命令，可以将此进程的信息以文本方式复制到系统的剪贴板里，用于记录或其他用途，如图 3-12 所示。

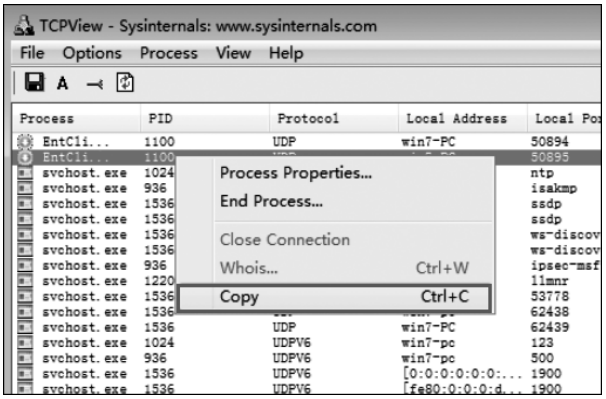

图 3-12　复制进程信息

（10）单击左上角的“保存”按钮或者按 Ctrl＋S 组合键可以保存系统当前运行所有进程的状态信息，如图 3-13 所示。

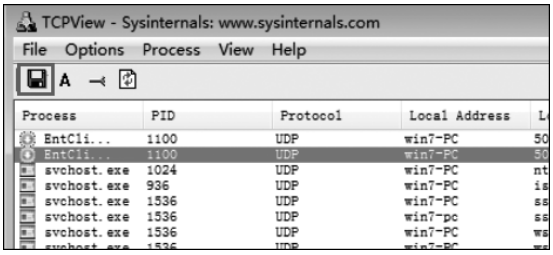

图 3-13　保存系统当前运行进程状态

（11）保存文件格式为 txt 文本格式，双击打开保存的文本文件，可以看到记录的进程信息，如图 3-14 所示。

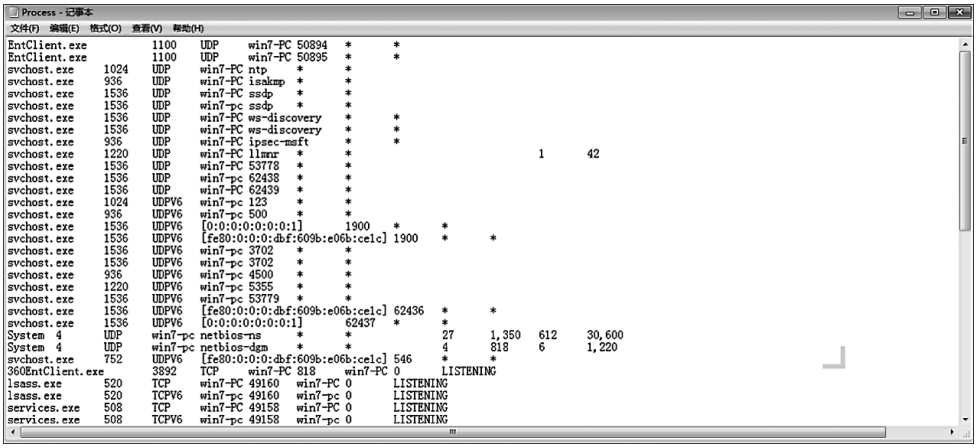

图 3-14　保存的进程信息

（12）TCPView 可以按照使用者关注的类型进行排序。例如，按照 State 的状态进行排序，单击 State 一列即可按照该列状态重新进行排序，如图 3-15 所示。

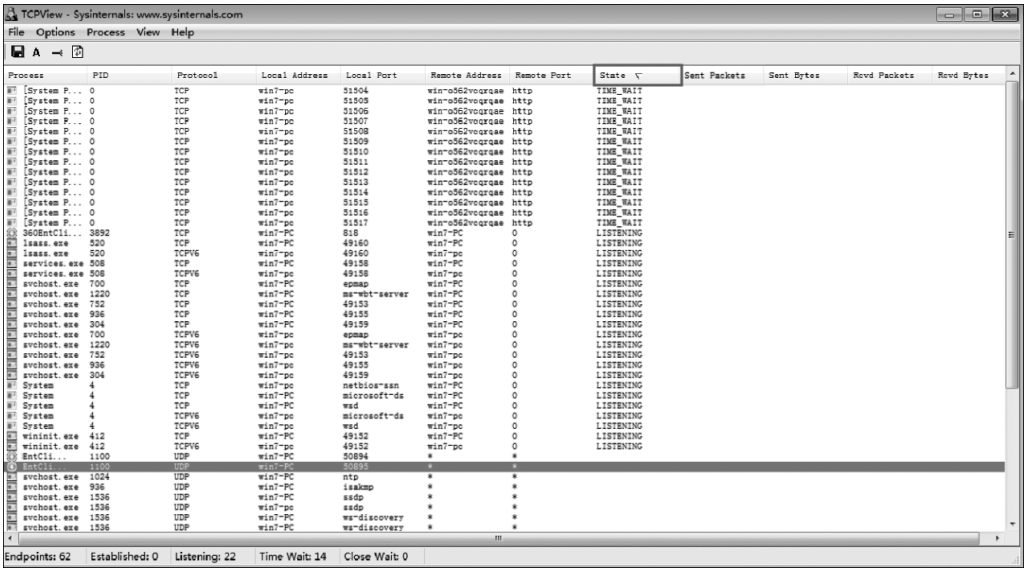

图 3-15　按 State 状态排序

（13）使用 TCPView 可以查看当前终端中运行的进程、端口、协议、状态、收发数据包数量等状态信息，并可以对某个进程复制状态信息，同时可以导出当前运行时的进程运行状态保存为文本文件，以便后续查看，满足实验预期。

【实验思考】

（1）使用 TCPView 如何发现流量异常的进程？

（2）在 TCPView 中，进程的状态都有哪几种？分别代表什么含义？

3.1.2　Wireshark 网络流量分析实验

【实验目的】

掌握 Wireshark 常用过滤命令的使用。

【知识点】

IP 过滤，端口过滤，HTTP 模式过滤。

【场景描述】

A 公司安全运维工程师小王在日常巡检中发现某台终端流量异常，为获知该终端异常流量的关联信息，小王需要使用 Wireshark 抓取该终端的通信流量进行分析，请协助小王使用 Wireshark 对该终端的通信流量进行分析。

【实验原理】

Wireshark 是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark 使用 WinPcap 作为接口，直接与网卡进行数据报文交换。

【实验设备】

主机设备：Windows Server 2003 主机 1 台，Windows 7 主机 1 台。
网络设备：交换机 1 台。

【实验拓扑】

实验拓扑如图 3-16 所示。

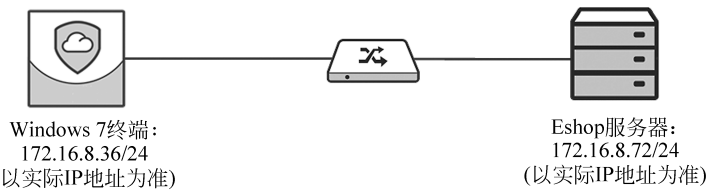

图 3-16　Wireshark 网络流量分析实验拓扑

【实验思路】

(1) 访问 FTP 服务器。
(2) 访问 Eshop 商城。
(3) Wireshark IP 筛选数据包。
(4) Wireshark 端口筛选数据包。
(5) Wireshark HTTP 模式筛选数据包。

【实验步骤】

1. 访问 FTP 服务器

(1) 进入实验对应拓扑，登录 Windows 7 终端，如图 3-17 所示。

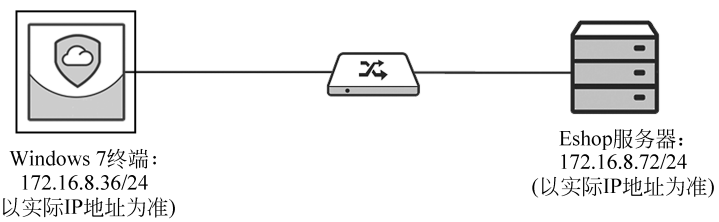

图 3-17　登录 Windows 7 终端

(2) 运行浏览器,在地址栏中输入“ftp://172.16.8.72”,访问该地址,可见访问 FTP 服务器正常,如图 3-18 所示。

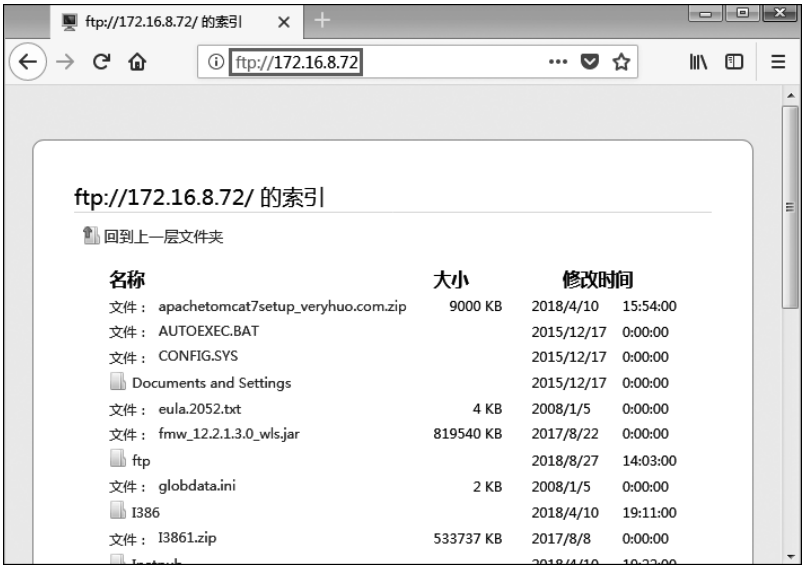

图 3-18　FTP 服务器目录

2. 访问 Eshop 商城

在浏览器中新建新标签页,在地址栏中输入“http://172.24.8.36”,访问该地址,可见网站显示正常,如图 3-19 所示。

图 3-19　访问网站

【实验预期】

(1) Wireshark 查看指定 IP。
(2) Wireshark 查看指定端口。
(3) Wireshark 查看指定 HTTP 数据包。

【实验结果】

1. Wireshark 查看指定 IP

（1）在终端桌面上，双击 Wireshark 图标快捷方式，运行 Wireshark 程序，如图 3-20 所示。

图 3-20　运行 Wireshark 程序

（2）在程序首页中，单击“本地连接”链接开始监听该网卡，如图 3-21 所示。由于本实验终端中只有一块网卡，因此仅能监听该网卡。如实际终端有多块网卡，请选择对应网卡进行监听。

（3）在表达式栏中输入表达式“ip.src＝＝172.16.8.36”，表明查找源 IP 地址为 172.16.8.36 的数据包，单击“箭头”按钮查询源 IP 数据包，可以筛选出相关的数据包记录。如果没有流量记录筛选出来，可重新刷新浏览器访问网站的页面，以便产生数据流量，如图 3-22 所示。

图 3-21　Wireshark 开始页面

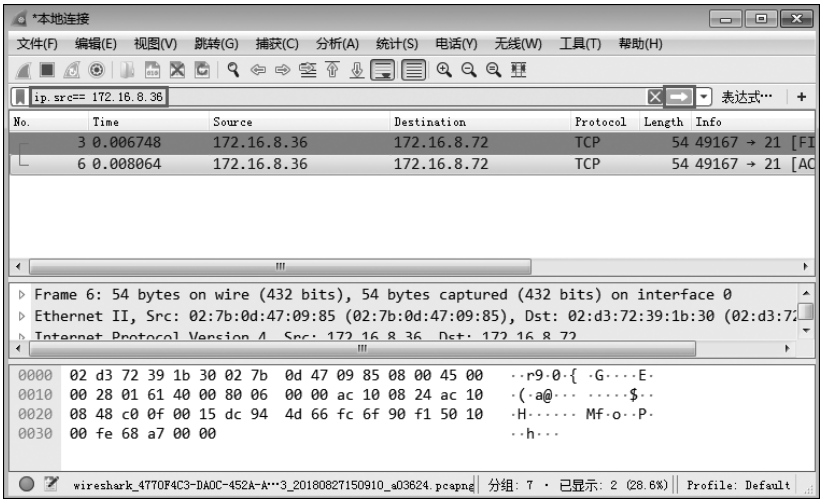

图 3-22　筛选源 IP 数据包

（4）在表达式栏中输入表达式“ip.dst＝＝172.16.8.72”，表明查找目的 IP 地址为 172.16.8.72 的数据包，单击“箭头”按钮查询目的 IP 数据包。如无流量记录，可刷新浏览器页面，以便产生数据流量，如图 3-23 所示。

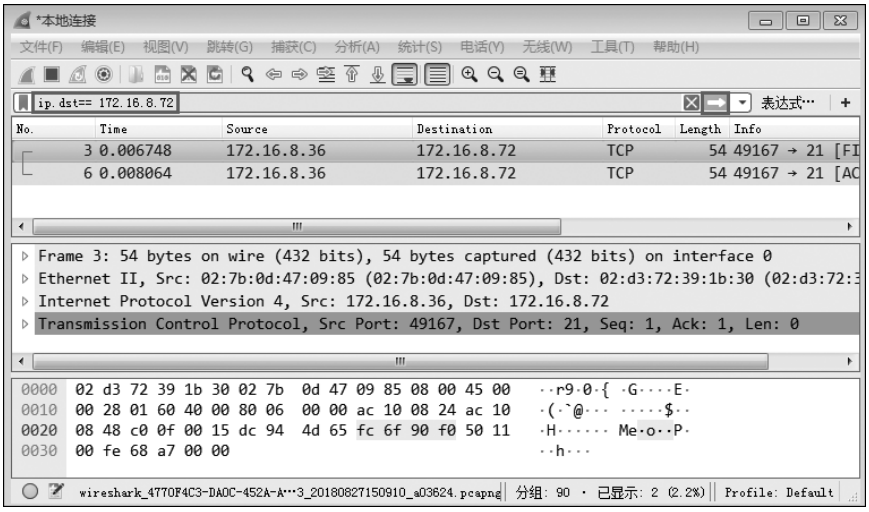

图 3-23　筛选目的 IP 数据包

2. Wireshark 查看指定端口

（1）在表达式栏中输入表达式“tcp.port＝＝21”，表明查找数据包流经端口为 21 的 TCP 数据包，单击“箭头”按钮查询流经端口 21 的数据包。如无流量记录，可刷新浏览器访问 FTP 网站页面，以便产生数据流量，如图 3-24 所示。

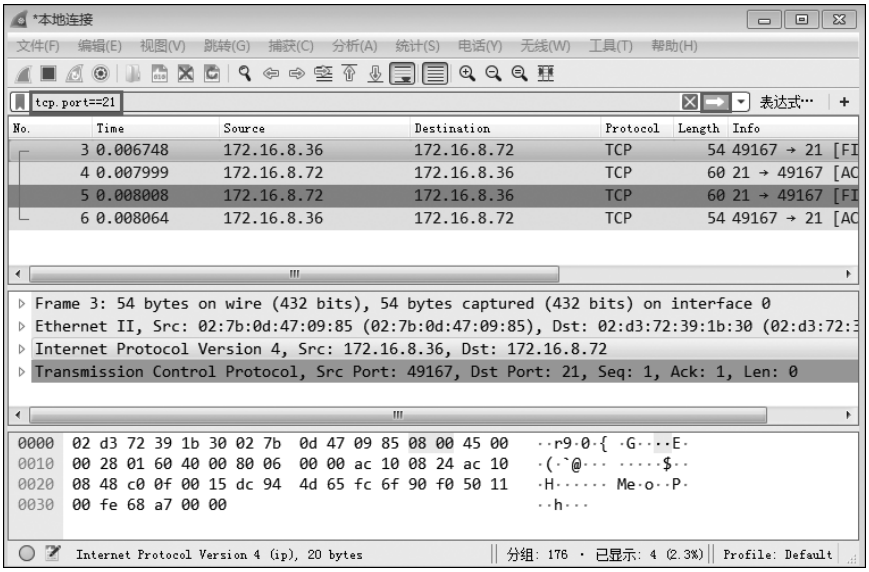

图 3-24　筛选流经端口 21 的数据包

（2）在表达式栏中输入表达式“tcp.port＝＝80”，表明查找数据包流经端口为 80 的 TCP 数据包，单击“箭头”按钮查询流经端口 80 的数据包。如无流量记录，可刷新浏览器访问网站的页面，以便产生数据流量，如图 3-25 所示。

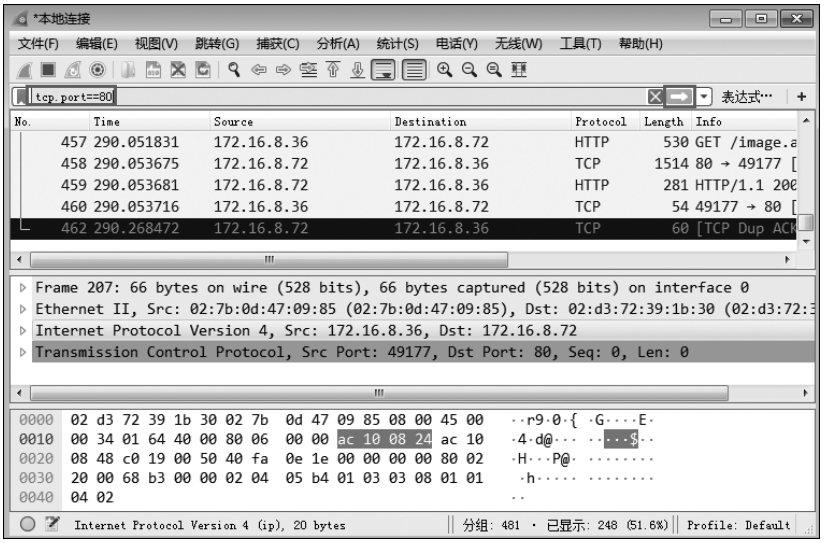

图 3-25　筛选流经端口 80 的数据包

3. Wireshark 查看指定 HTTP 数据包

（1）在表达式栏中输入表达式“http.request.method＝＝"GET"(英文符号)”，表明查找 HTTP 请求包中 GET 方法类型的数据包，单击“箭头”按钮查询 GET 数据包，如图 3-26 所示。

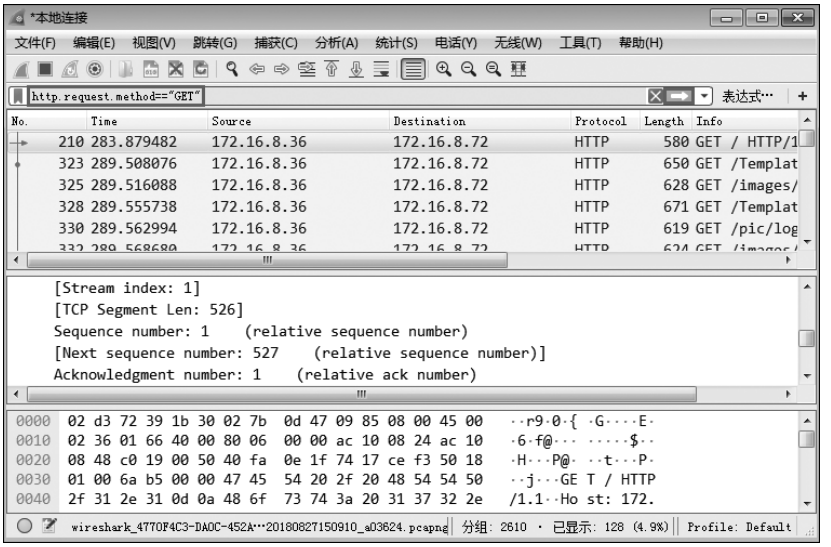

图 3-26　筛选 GET 数据包

（2）在浏览器中访问 172.16.8.72 网站，在网站首页导航栏中，单击“留言簿”链接，在“内容”处输入“test”，Email 处输入“test@qianxin.com”，“名字”处输入“test”，然后单击“提交”按钮，以便产生 POST 类型数据包，如图 3-27 所示。

图 3-27　在网站提交数据

（3）返回 Wireshark 程序中，在表达式栏中输入表达式“http.request.method == "POST"（英文符号）”，表明查询 HTTP 请求包中 POST 类型数据包，单击“箭头”按钮查询 POST 数据包，如图 3-28 所示。

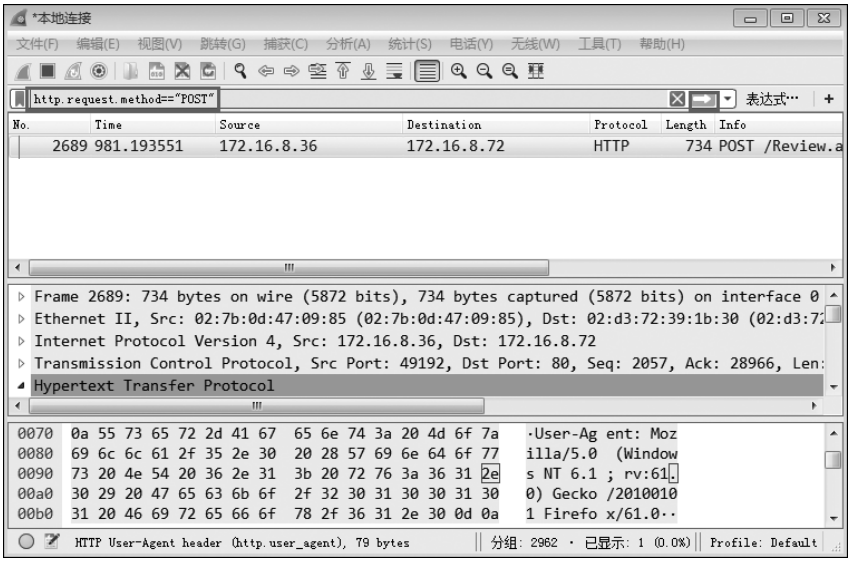

图 3-28　筛选 POST 数据包

(4) Wireshark 可以对当前终端的网络流量进行抓取,并对抓取到的数据包,根据条件进行筛选过滤,获得关注的数据包,并可查看数据包中的数据内容,满足实验预期。

【实验思考】

(1) 如何使用 Wireshark 查看 ICMP 包?

(2) 怎样查看一条相关联的数据流信息?

3.2 操作系统

3.2.1 终端安全管理系统问题排查——Autoruns 使用实验

【实验目的】

掌握终端安全管理系统问题排查工具 Autoruns 的使用方法。

【知识点】

Autoruns。

【场景描述】

A 公司的安全运维工程师小王巡检时怀疑公司某台终端运行有问题,在终端查找问题时,因为系统内置的 msconfig 工具不能完全显示所有自启动项,所以小王使用 Autoruns 工具进行启动项的查看。请协助小王使用 Autoruns 进行检查。

【实验原理】

操作系统的自启动服务或程序是因为某些应用程序正常运行是有前提的,必须在操作系统引导过程中初始化相关联的服务,应用程序才能正常运行。而某些恶意代码也会将自身的攻击程序或服务设置在操作系统自启动阶段,以获取系统的某些权限或免疫安全防护措施。

Autoruns 是 Systernals Suite(故障诊断工具套装)的一部分。它能够显示在 Windows 启动或登录时自动运行的程序,并且允许用户有选择地禁用或删除它们,例如,那些在“启动”文件夹和注册表相关键中的程序。此外,Autoruns 还可以修改包括 Windows 资源管理器的 Shell 扩展(如右键弹出菜单)、IE 浏览器插件(如工具栏扩展)、系统服务和设备驱动程序、计划任务等多种不同的自启动程序。

【实验设备】

主机设备:Windows Server 2008 R2 主机 1 台,Windows 7 主机 1 台。

网络设备:交换机 1 台。

【实验拓扑】

实验拓扑如图 3-29 所示。

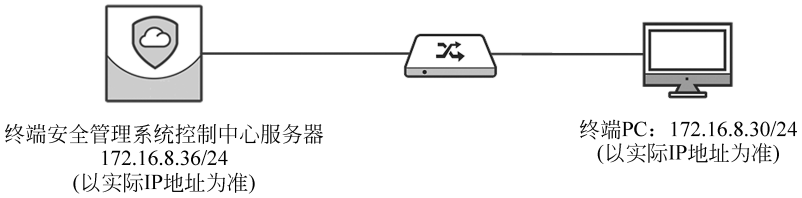

图 3-29　Autoruns 使用实验拓扑

【实验思路】

使用 Autoruns 查看并管理启动项。

【实验步骤】

(1) 进入实验对应拓扑，使用 Administrator 账户，输入密码 123456，登录右侧的终端 PC，如图 3-30 所示。

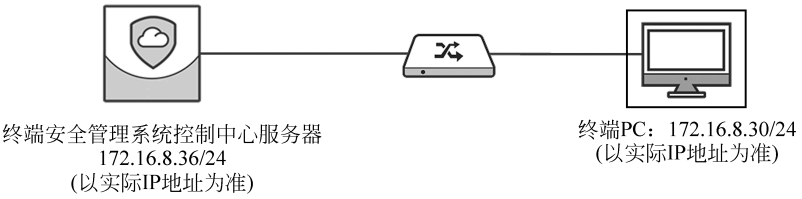

图 3-30　登录终端 PC

(2) 运行桌面上的 Autoruns 图标快捷方式运行程序，推荐以管理员身份运行该程序，如图 3-31 所示。

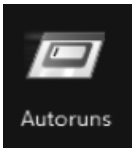

图 3-31　运行 Autoruns 程序

【实验预期】

使用 Autoruns 查看自启动项。

【实验结果】

(1) Autoruns 程序运行的主界面默认显示在 Everything 选项卡中，如图 3-32 所示。

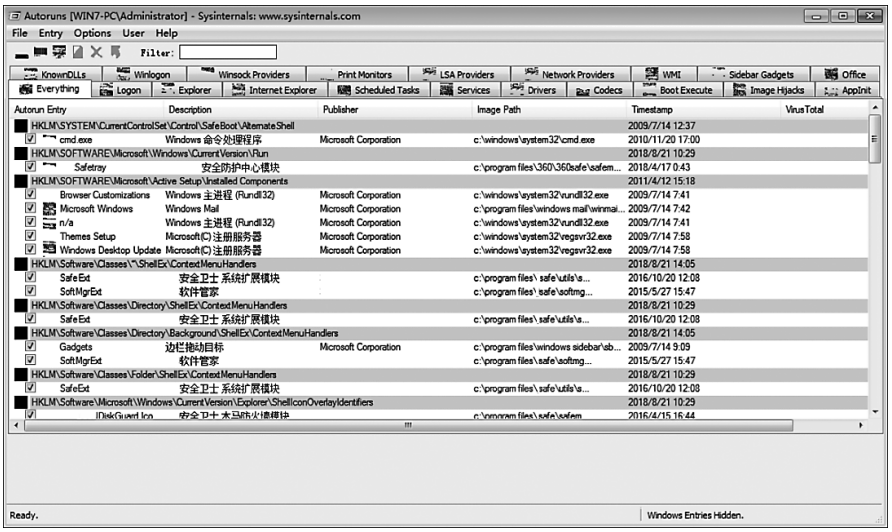

图 3-32　Autoruns 运行界面

（2）在 Everythings 选项卡中，右击任意一个注册表项，会弹出该项目可操作的内容，该菜单内容与 Autoruns 菜单栏的 Entry 菜单内容是一致的，如图 3-33 和图 3-34 所示。

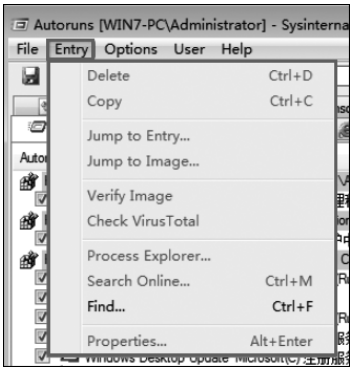

图 3-33　Entry 菜单

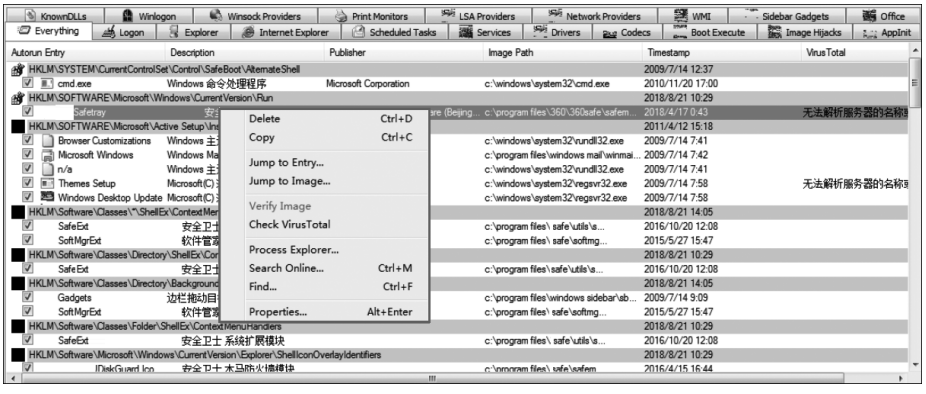

图 3-34　右击显示菜单

(3) 在菜单栏的 Options 中提供了内容显示的开关功能,如图 3-35 所示。

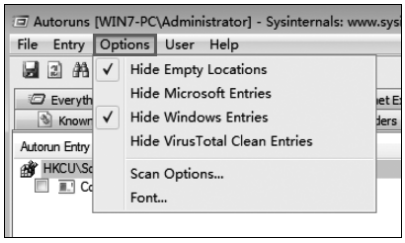

图 3-35　Options 菜单

(4) 在 Options 菜单中,Hide Empty Locations 表示隐藏空位,当注册表的键没有键值或子键时不显示该注册表路径,因为键值为空时代表没有数据,也就没有显示的必要性,所以该选项的默认设置是勾选状态,取消勾选后会显示注册表中键值为空的内容,如图 3-36 所示。

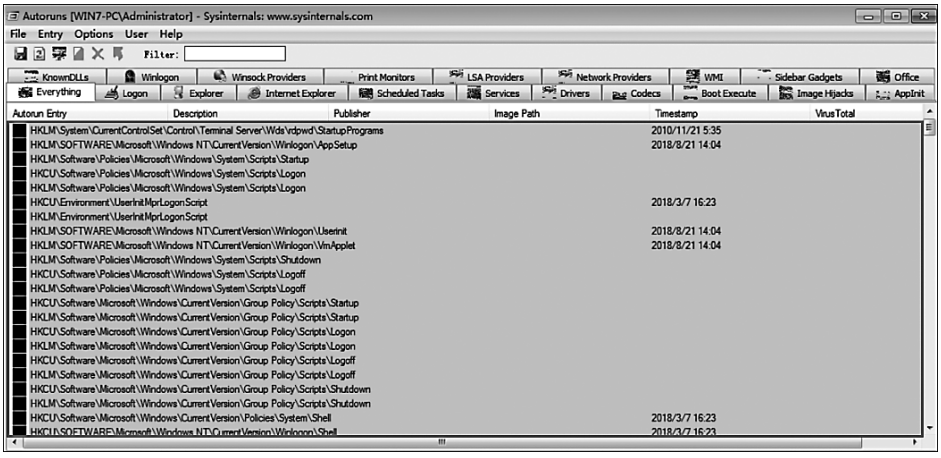

图 3-36　显示键值为空的注册表条目

(5) 在 Options 菜单中其他 3 个选项分别为: Hide Microsoft Entries 表示隐藏微软官方的注册表条目,默认不勾选;Hide Windows Entries 表示隐藏 Windows 系统程序的自启动条目,默认勾选此选项;Hide Virus Total Clean Entries 表示隐藏清理病毒总数量条目。

(6) Autoruns 菜单栏中的 User 菜单中列出了可以查看的属于当前用户的启动项,用户可以在此切换用户身份,以便查看不同用户的启动项,如图 3-37 所示。

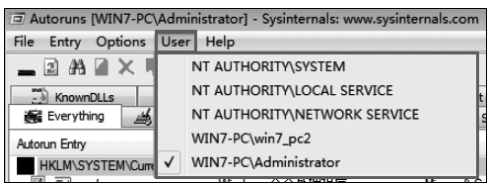

图 3-37　User 菜单内容

(7) 在 Autoruns 的 Everything 主要内容显示区域,数据分为 6 列,分别是 Autorun Entry(条目名称)、Description(条目描述)、Publisher(发布者)、Image Path(路径)、Timestamp(创建时间)、Virus Total(病毒数量),如图 3-38 所示。

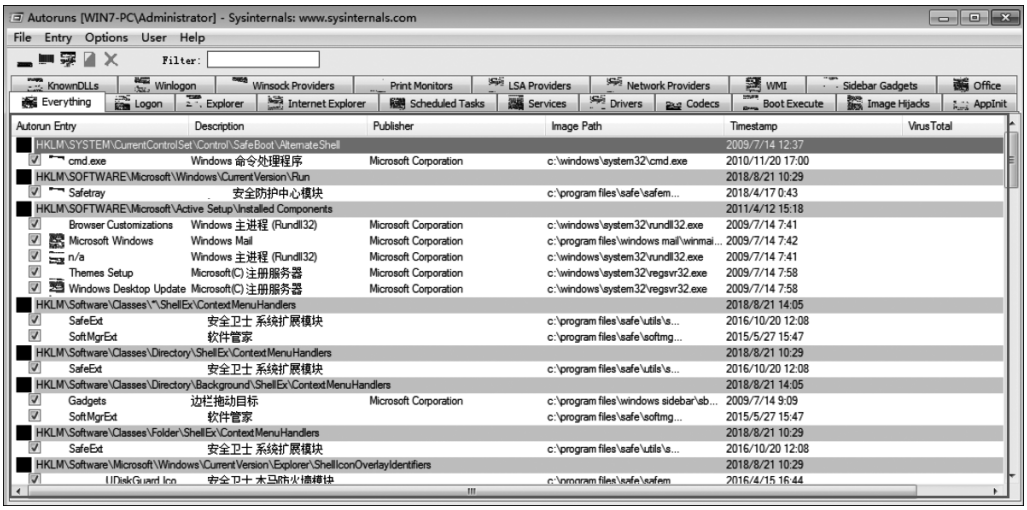

图 3-38　Everything 内容显示区域

(8) Everything 内容显示区域中的淡紫色行(行中包含背景色)表示注册表中的该键的路径,紫色行下面的是子键,是具体的自启动条目信息和路径。Autoruns 基于注册表的键进行类别划分,比如最上面的三行是用户登录时自启动的项,和 Logon 选项卡的内容相同,如图 3-39 和图 3-40 所示。

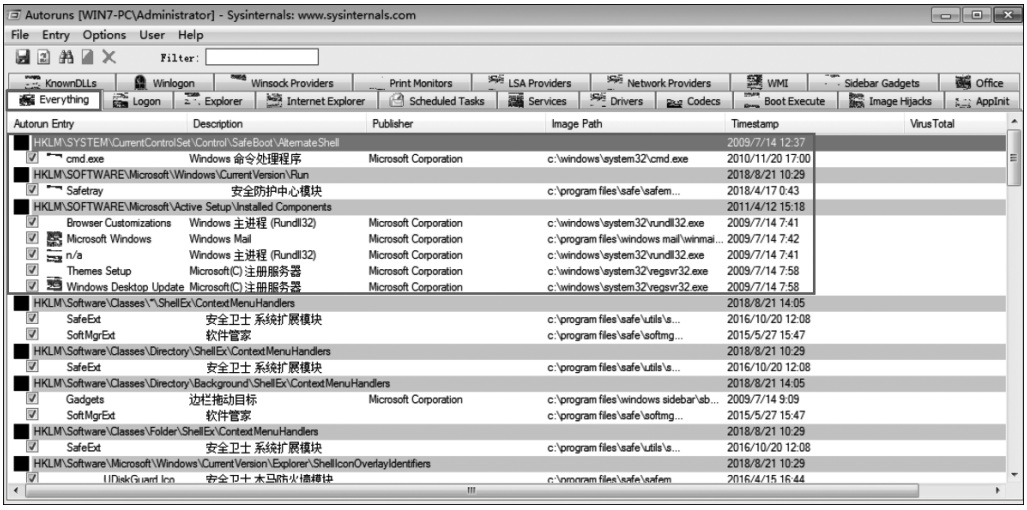

图 3-39　Everything 选项卡内容

(9) 单击终端安全管理系统“安全防护中心模块”,当需要禁用此启动项时取消该条目前面的勾选即可,如图 3-41 所示。

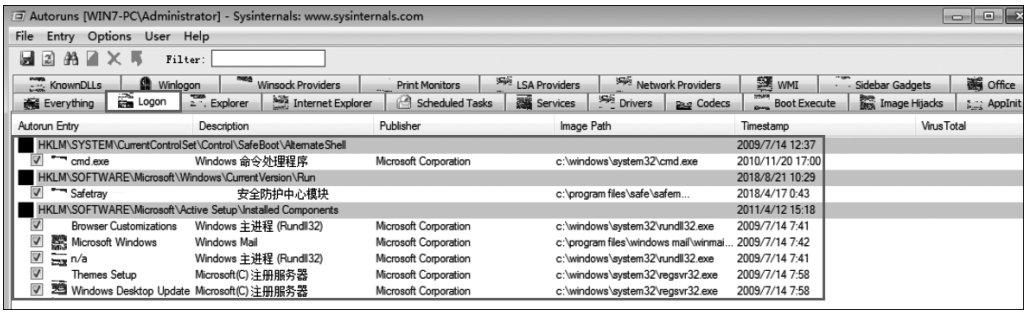

图 3-40　Logon 选项卡内容

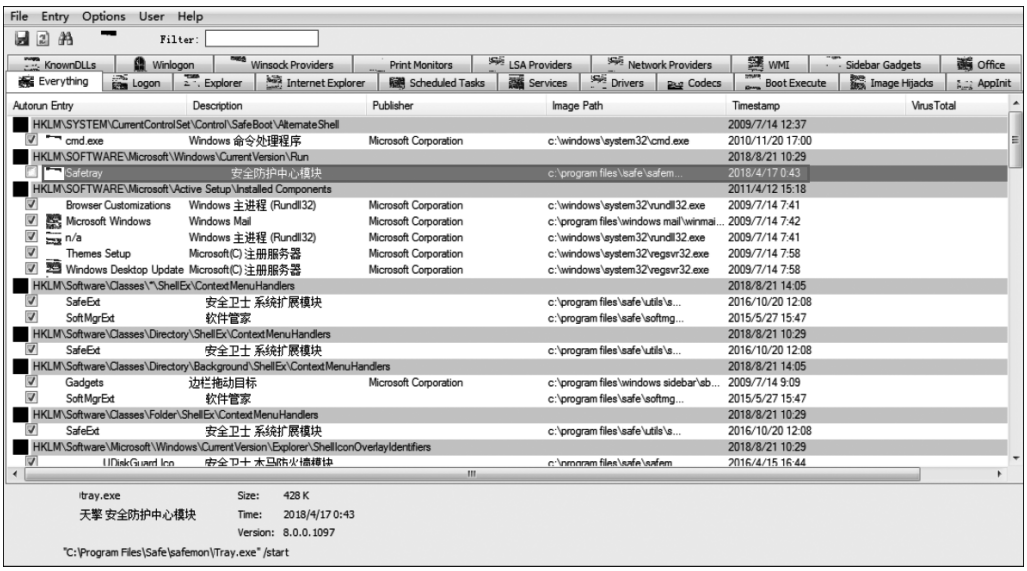

图 3-41　选中条目

（10）右击选中终端安全管理系统“安全防护中心模块”，会弹出可操作菜单，Delete 是删除此启动条目，无法恢复；Copy 会复制此条数据，包括 Autorun Entry、Description、Publisher、Image Path、Timestamp 和 Virus Total，如图 3-42 所示。

图 3-42　条目操作菜单

(11) Jump to Entry 会跳转至该自启动条目在注册表中的键的位置,如图 3-43 所示。

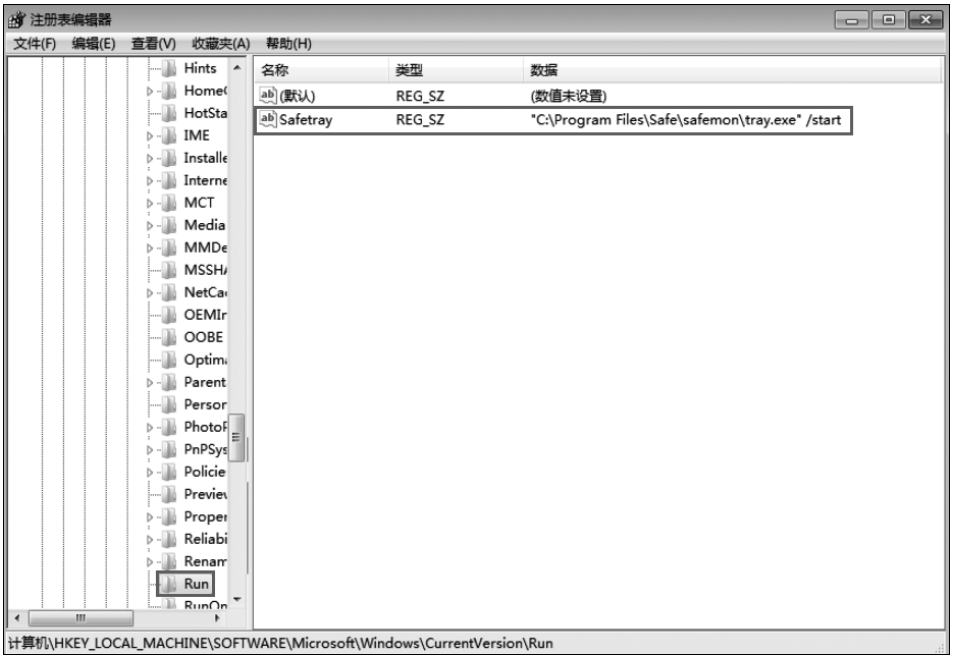

图 3-43 Jump to Entry

(12) Jump to Image 会跳转至该启动条目的执行文件位置,如图 3-44 所示。

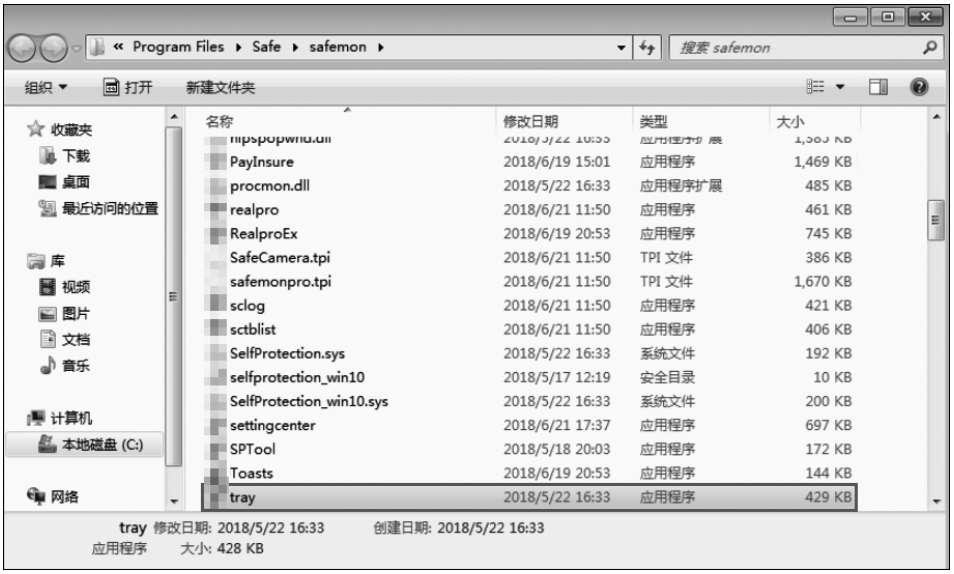

图 3-44 Jump to Image

(13) Verify Image 可以校验该自启动条目的执行文件的签名,进行真实性验证,验证通过后会在 Publisher 字段添加(Verified)字段,如图 3-45 所示。