第5章 恶意代码动态分析

恶意代码动态分析是指在恶意代码运行时对其实施监视或干扰以了解恶意代码的功能、行为和影响的技术。动态分析通常基于恶意软件所需的执行环境进行，因此应根据静态分析的结果，选择正确的环境和工具进行分析。通过动态分析，安全研究人员可以观察恶意代码与系统的交互方式，包括文件操作、网络通信、注册表修改等，从而深入了解恶意软件的功能和影响，以此制定相应的防御策略。本章将介绍恶意代码动态分析环境、恶意代码本地和网络行为监控分析、二进制调试器、二进制 Hook 及模拟执行技术，从表入深，从恶意代码动态执行时的外在表现出发，深入到其内部执行原理，在此基础上通过编程控制恶意代码执行流程。

5.1 动态分析方法

动态分析一般分为如下三个步骤：①在虚拟环境中，使用监控工具执行样本，获取样本的本地行为和网络行为的记录；②分析记录，对样本功能进行总体判定，提取关键检测点（如 IoC 等）；③利用调试器等工具，分析样本的内在逻辑和功能，对样本采用的技术进行深度研究。

在进行动态分析时，首先需要在隔离的虚拟机、沙箱、容器等虚拟环境中执行可疑样本。这是因为恶意软件可能会对真实环境中的系统或网络造成损害，而在虚拟环境中大多可以避免这种风险。在虚拟环境中，会使用各种监控工具来监控和记录样本的运行情况，这些监控工具可以分为两类，一类是本地监控工具，如 API Monitor、Sysinternals 等，用于监控样本对系统资源的访问和修改，如文件、注册表、进程等；另一类是网络监控工具，如 Wireshark、TCPDump 等，用于捕获样本的网络通信数据，部分网络工具还能对网络数据进行修改。通过这些监控工具，可以全面了解恶意软件在执行过程中的行为特征。

分析样本执行过程的行为记录，对样本功能进行总体判定，提取关键检测点（如 IoC 等）。具体来说，需要分析样本在执行过程中的行为，如创建的文件、修改的注册表项、启动的进程等，以及样本的网络通信行为，如连接的远程服务器地址、发送的数据包特征等。此外，还需要关注样本的持久化机制、自保护机制等。通过对这些行为的分析，可以对恶意软件的功能进行总体判定，并提取关键检测点，如 IoC 等，为后续的威胁检测和响应提供依据。

最后也是最复杂的步骤是利用调试器等工具分析样本的内在逻辑和功能，对样本采用的技术进行深度研究。调试器是动态分析中非常重要的工具，它可以让我们深入了解恶意软件的内部结构和运行机制。常见的调试器有 OllyDbg、x64dbg、GDB 等。在调试过程中，可以采用多种技术手段，如设置断点、单步执行、查看寄存器、查看和转储内存等。通过这些操作，可以逐步揭示恶意软件的执行流程、函数调用、系统调用等功能细节，还可以分析恶意软件使用的加密算法、混淆技术、反调试技术等，从而对威胁技术进行深度研究。

5.2 样本行为监控

行为监控工具主要用于实时监控和记录恶意软件在系统中的活动，这些工具主要用于监控文件系统、注册表、进程、网络、API 调用等。

5.2.1 API Monitor

API Monitor 是 Rohitab 推出的一款免费 API 监控工具，它能够利用多种技术监控和记录进程调用的系统 API 及其调用参数和返回值，它还包含过滤器功能，用户可以通过过滤器对记录的日志进行筛选。

API Monitor 的主要功能界面如图 5-1 所示。

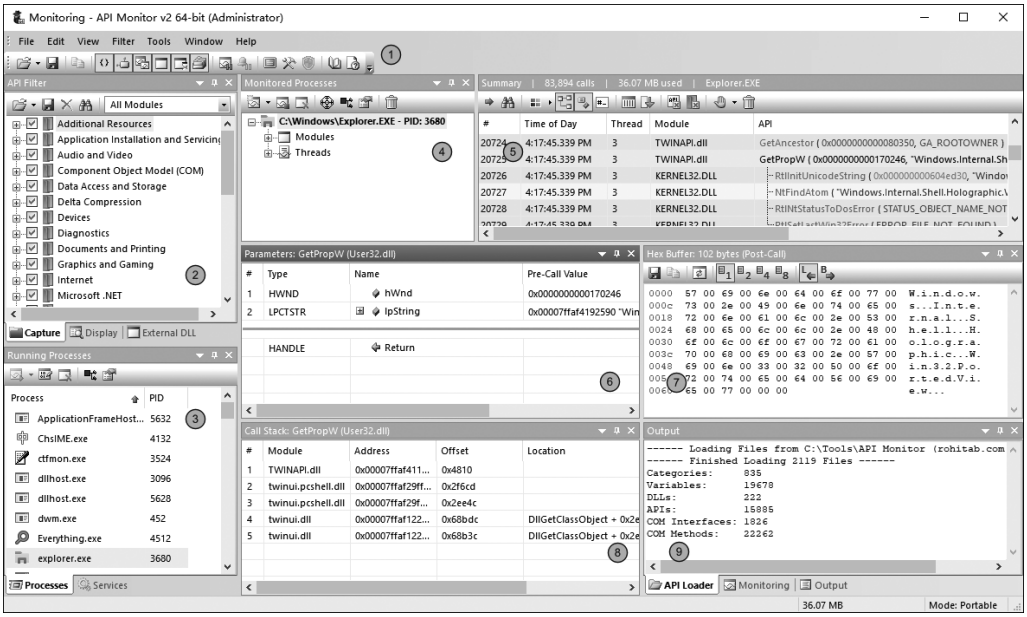

图 5-1　工具 API Monitor 的主界面

以下为界面各部分的功能。

- 菜单栏和工具栏：包含软件功能按钮的菜单和工具栏。

- API 过滤器：设置需要监控或显示的 API，或加载非系统库的第三方 DLL。
- 正在运行的进程：显示系统进程和服务，可以选择正在运行中的进程或服务进行监控。
- 正在监控的进程：显示正在监控中的进程，可以选择要查看的模块或线程。
- 概要：显示调用 API 的概要信息，单击选中后可以在其他窗口中查看本次 API 调用的详细信息。
- 参数：显示当前在概要窗口中选中的 API 调用的具体参数值和返回值。
- 数据：显示当前在参数窗口中选中的指针类型参数所指向数据的具体值。
- 调用栈：显示当前在概要窗口选中的 API 调用的调用栈信息。
- 输出：显示 API Monitor 运行日志等信息。

使用 API 过滤器窗口选择想要监控的 API，例如，监控文件相关操作可以选中 Local File Systems，然后选择正在运行的进程或选择新建进程，然后即可查看程序调用的 API 详情。

5.2.2　Sysinternals 套件

Sysinternals 是由 Mark Russinovich 等开发的系统实用工具组，后交由微软管理。该工具集中包含超过 70 个实用工具，可以帮助用户监控和控制 Windows 系统的各方面，例如，进程、内存、网络、磁盘、注册表等。本节主要介绍的 Autoruns 和 Process Monitor 都是动态分析中很有价值的工具，但需要特别注意的是，Sysinternals 套件中的部分行命令工具可以在攻击活动中被攻击者当作攻击工具利用，因此套件中部分工具会被杀毒软件报警。

1. Autoruns

Autoruns 是用来查看系统自启动项目的工具，支持查看注册表、计划任务、服务等十余种自启动项目，帮助发现恶意软件中的持久化行为。工具启动后会自动扫描，等待左下角状态栏显示“Ready”则表示扫描已经完成，如图 5-2 所示。

2. Process Monitor

Process Monitor（简称 Procmon）是用于监控程序的多种行为的工具，工具启动后便会立即对系统所有进程进行监控，可以通过 Filter 菜单，设置过滤条件来查看感兴趣的信息。例如，只查看 explorer.exe 的行为，可以选择 Process Name、is、explorer.exe、then Include 然后单击 Add 按钮并保存即可，如图 5-3 所示。

5.2.3　Process Hacker

Process Hacker 是一款功能强大的系统管理工具，可用于监视和管理系统中运行的进程、服务、网络连接和磁盘等，允许用户深入分析系统活动，检测和识别潜在的恶意进程或行为。通过双击进程，可以查看进程的内存模块、内存页面、性能统计、权限令牌等各项底层信息，如图 5-4 所示。

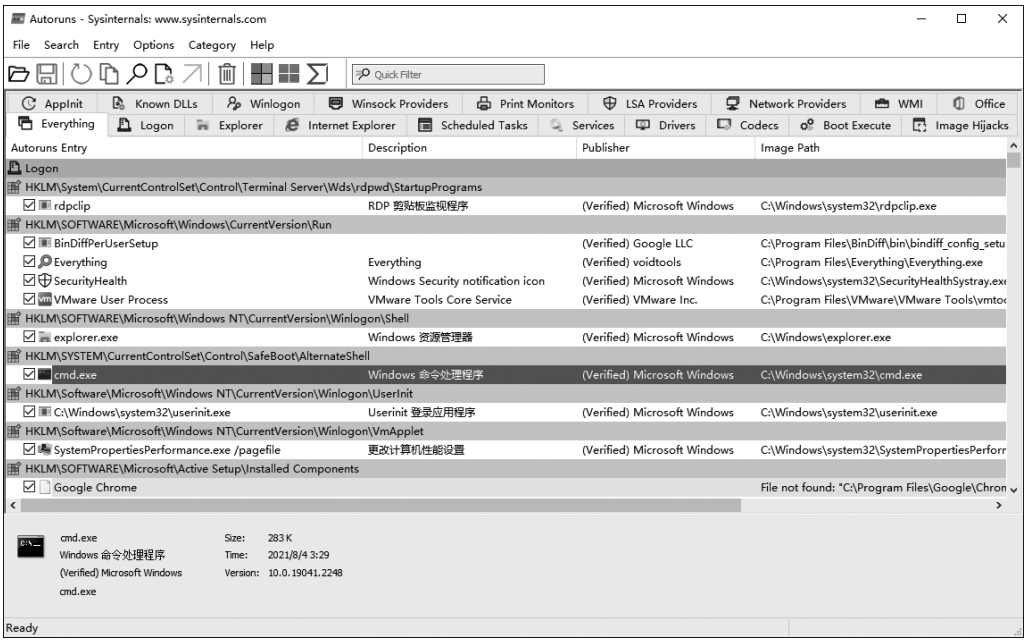

图 5-2　使用 Autoruns 工具查看自启动项

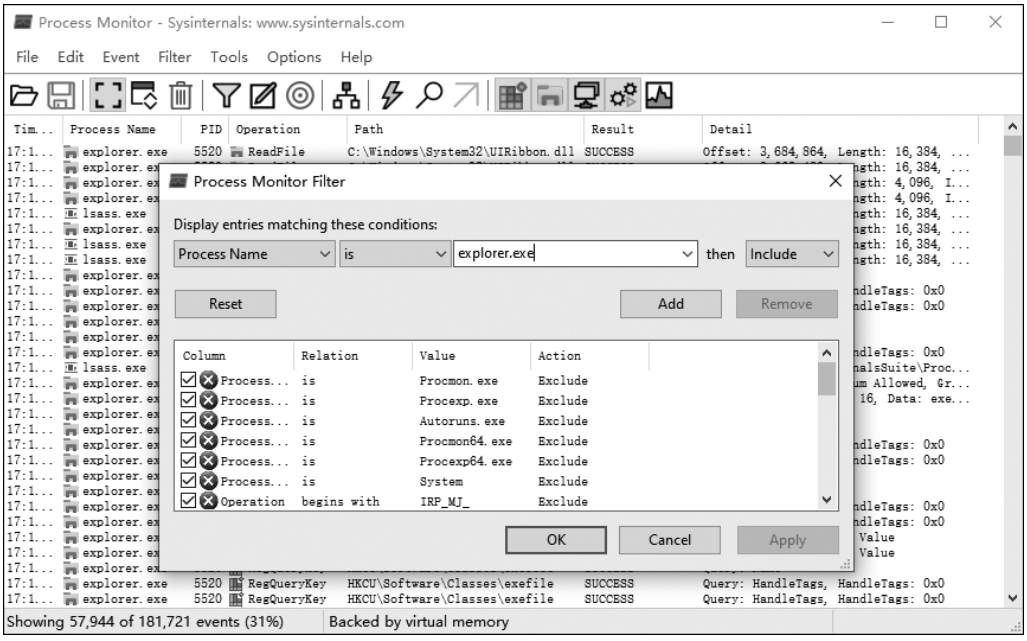

图 5-3　使用 Process Monitor 查看进程行为

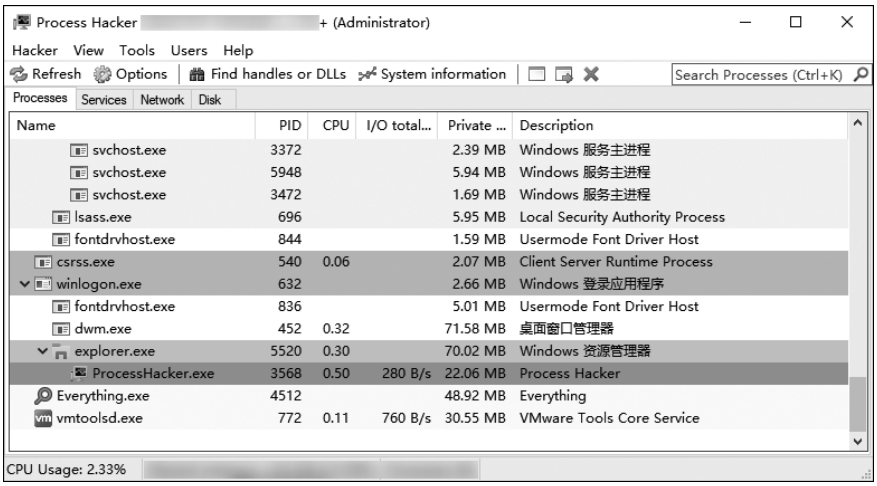

图 5-4　Process Hacker 工具主界面

5.3　沙箱和虚拟机

沙箱(Sandbox)和虚拟机是两种常用的恶意代码分析技术，它们都可以在一个隔离的环境中运行可疑的程序，观察其行为和影响，而不会对真实的系统造成危害。与虚拟机从硬件层面模拟完整操作系统的技术不同的是，沙箱使用软件层面的隔离技术，限制程序的权限和资源访问，同时可对程序进行监控和记录，更侧重于限制和记录而非底层仿真。

沙箱和虚拟机技术各有优劣，一般来说，沙箱更轻量级，但也更容易被恶意代码检测和绕过；虚拟机更完整，但也更耗费资源。因此有一些对两者进行结合的分析工具，它们能基于虚拟机技术创建高仿真环境，并隐藏虚拟机的一些特征，同时在其内部监控程序行为，也可以称这类工具为沙箱工具。

5.3.1　Sandboxie

Sandboxie 是一款开源工具，可以在 Windows 系统中创建一个隔离的运行环境，用于测试不信任的程序和网页，避免对真实系统造成影响。由于它基于真实操作系统执行，仅模拟了应用级别的环境，因此在反逃逸、主机数据隔离等安全性方面通常要弱于虚拟机。其优点在于占用资源少，可基于主机原始环境执行，并可以设置对各类资源的访问权限等。因此，Sandboxie 更适合于日常使用，用于执行从外部接收到的文件。其主界面如图 5-5 所示。

5.3.2　在线沙箱

在线沙箱是指基于云端服务器远程执行可疑文件或代码的工具。与本地分析环境相比，网络上免费的在线沙箱方便使用，不需要用户自行配置虚拟环境，部分沙箱还可以输出分析报告，突出展示样本行为中的重点内容。出于行业内对情报共享的共识，大多数免

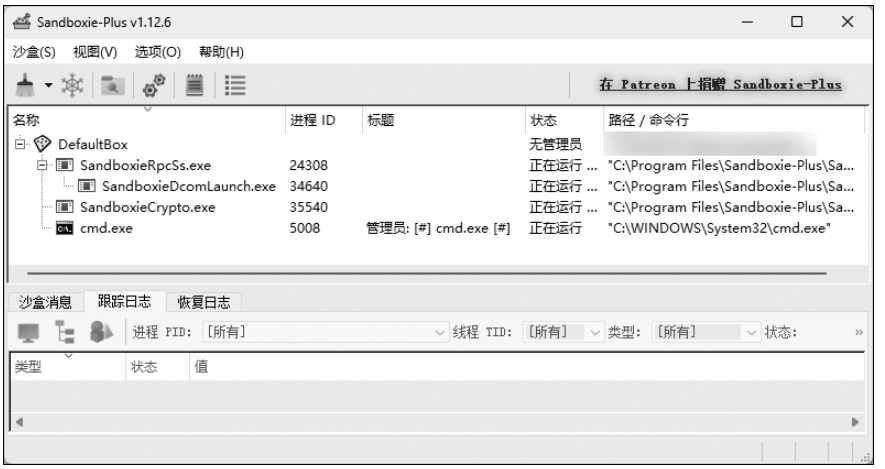

图 5-5 Sandboxie 主界面

费沙箱均会公开用户上传的样本，并在用户上传前告知，因此免费在线沙箱不适合于处理涉及机密的样本文件，若有需要可以考虑商业版本或自行部署沙箱系统。

以下介绍两款常用的在线沙箱工具。

1. ANY.RUN

ANY.RUN(https://app.any.run/)免费版支持模拟 Windows 7 32 位环境，可以监控进程、网络等行为，识别恶意代码家族，支持对虚拟环境进行实时操作。登录后单击 New task 按钮，上传样本并单击运行即可新建分析任务。界面中大致包含导航栏、屏幕区、网络及文件行为监控区、样本信息区、进程区几部分，可以以此了解或干预样本执行的过程，如图 5-6 所示。

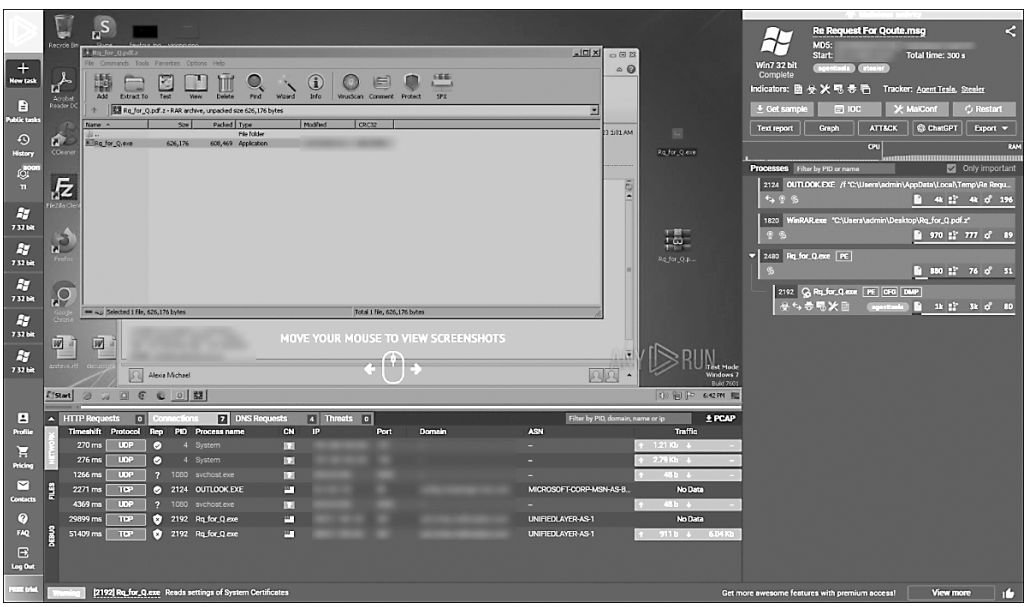

图 5-6 分析任务详情页面

2. Cuckoo Sandbox

Cuckoo Sandbox(https://cuckoosandbox.org)是完全开源的恶意软件自动化分析沙箱,具有模块化的结构设计且支持多个操作系统的模拟。该沙箱需要自行搭建环境才可以使用,因此更适合于有样本安全需求或需要定制化沙箱分析环境的用户使用。

5.4 网络分析

在程序运行过程中,还会产生网络行为。通过网络抓包可以捕获到样本的网络行为,然后可利用分析工具对样本的网络通信逻辑进行分析。

5.4.1 Wireshark

Wireshark 是一款流行的网络封包分析软件,可以捕获和显示各种网络协议的详细信息。Wireshark 可以用于恶意代码分析,例如,检测网络攻击,识别恶意流量,分析恶意软件的通信方式等。Wireshark 有很多强大的功能,如过滤器、统计、解码器等,可以帮助分析人员快速找到感兴趣的数据。Wireshark 是开源软件,可以在 Windows、macOS 和 Linux 上运行。

1. 捕获数据包

启动 Wireshark,在“捕获”界面中双击需要抓包的网络接口即可。例如,若在主机系统中安装 Wireshark 来抓取 NAT 网络的虚拟机的数据包,默认配置下可选择 VMnet8 接口;若在虚拟机内抓包,则选择“以太网”字样的接口即可,如图 5-7 所示。

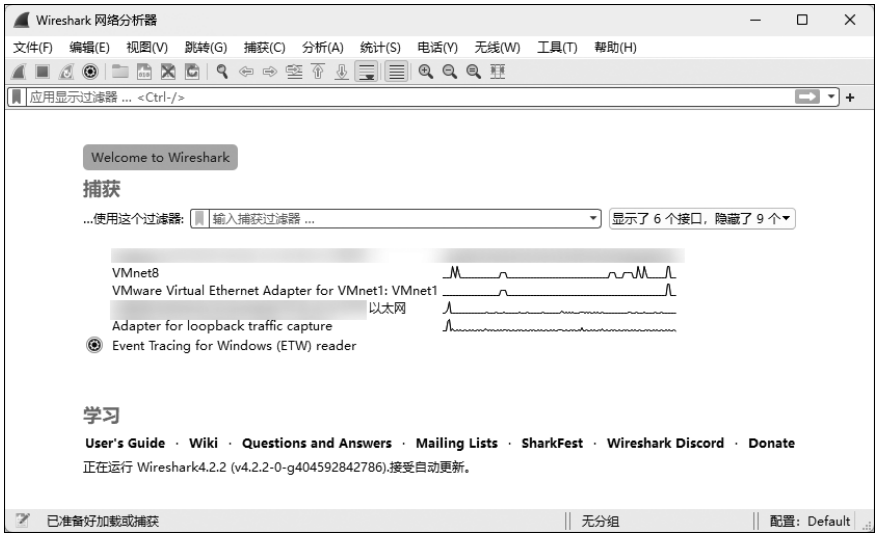

图 5-7　在 Wireshark 中选择要捕获的接口

捕获完成后,可以单击工具栏中的“停止捕获”按钮或使用“捕获→停止”菜单结束捕获,然后可以保存数据包进行进一步分析,如图 5-8 所示。

图 5-8　在 Wireshark 中捕获数据包并停止捕获

2. 过滤器

利用过滤器可以筛选感兴趣的数据包查看，可在工具栏下方的输入框中指定协议、源或目的地址、端口号等条件来筛选和显示数据包，还可以利用逻辑运算符编写复杂的过滤条件，如图 5-9 所示。

图 5-9　使用 Wireshark 过滤器

简单地显示过滤器语法示例可单击“分析”→“显示过滤器”查看，其他字段可单击“帮助”→“说明文档”→“Wireshark 过滤器”来查看，如图 5-10 所示。

5.4.2　TCPDump

TCPDump 是一个用于捕获网络数据包的命令行工具，主要应用于 Linux 系统。只需要在 root 用户权限下执行“tcpdump -w 输出文件名.pcap”命令即可使用。捕获的文件

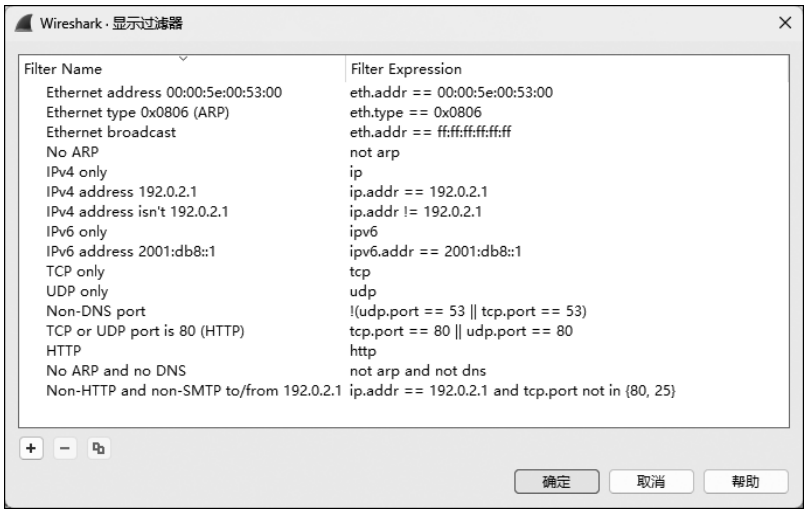

图 5-10　查看 Wireshark 中的过滤器示例

可以使用 Wireshark 打开，如图 5-11 所示。

```
>tcpdump --help
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-com
                [ -Z user ] [ expression ]
>tcpdump -w output.pcap
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
```

图 5-11　使用 TCPDump 进行捕获数据包

5.4.3　TCPView

TCPView 是用于查看系统中当前网络连接情况的工具，可通过工具栏中的按钮筛选 IPv4、IPv6 以及 TCP、UDP，结合网络分析工具的结果，可以把网络数据包中的 IP 地址等信息关联到具体的进程，如图 5-12 所示。

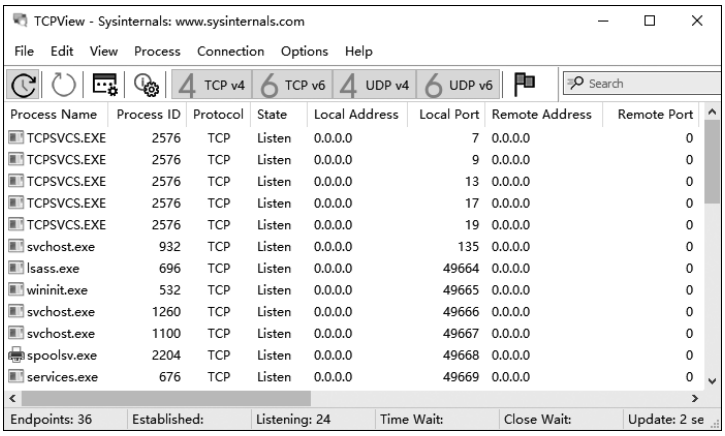

图 5-12　使用 TCPView 查看当前网络连接

5.4.4 FakeNet-NG

FakeNet-NG 是 FakeNet 的后继版本，用于模拟网络环境，让恶意软件在受控制的网络环境中运行，从而捕获、修改其网络流量，帮助安全研究人员了解恶意软件的网络通信模式。

其默认配置会自动配置虚拟 DNS 并拦截 HTTP 等协议的数据包，将 HTTP 请求重定向到虚拟网络中，实际访问的为 defaultFiles 文件夹中的文件，如图 5-13 所示。

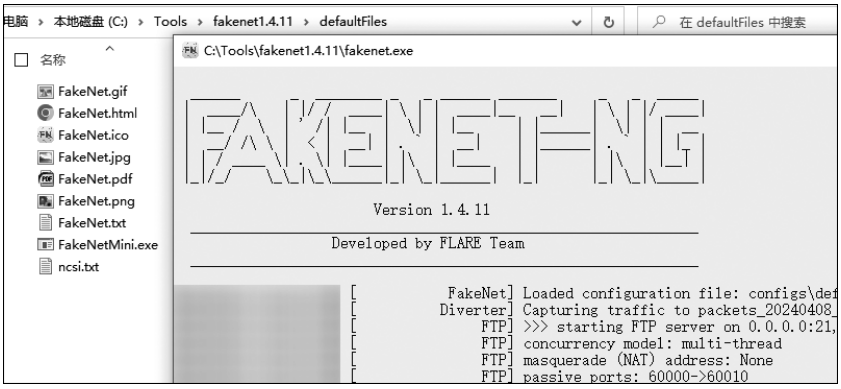

图 5-13　使用默认配置运行 FakeNet-NG

5.4.5 Packet Sender

Packet Sender 是一款用于网络调试和测试的开源工具，主要用于发送、接收和查看网络数据包。Packet Sender 可用于模拟恶意软件在网络通信方面的行为，与 C2 服务器进行直接交互，以此来深入了解恶意代码与远程服务器之间的通信模式，如图 5-14 所示。

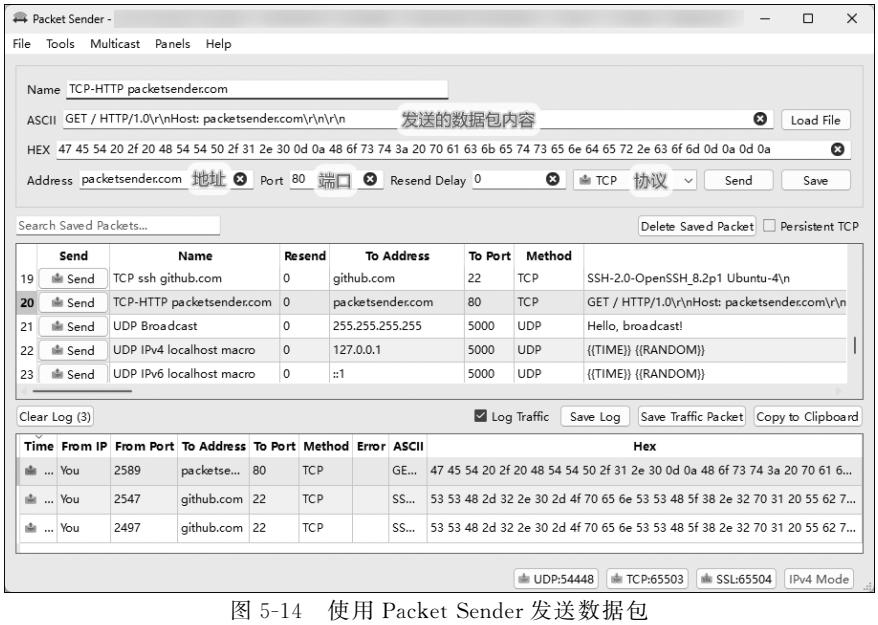

图 5-14　使用 Packet Sender 发送数据包