**针对Linux平台的工业软件运行行为监控模块**

用户操作手册

2021年01月08日

广州道本信息科技有限公司

目录

[一、简介 1](#_Toc63680246)

[（一）手册目的 1](#_Toc63680247)

[（二）手册范围 1](#_Toc63680248)

[**二、软件概述** 1](#_Toc63680249)

[（一）软件目标 1](#_Toc63680250)

[（二）软件环境 1](#_Toc63680251)

[三、系统启动 2](#_Toc63680252)

[四、系统首页 3](#_Toc63680253)

[五、监控软件管理 4](#_Toc63680254)

[（一）添加可执行程序 4](#_Toc63680255)

[（二）添加可执行的命令行 5](#_Toc63680256)

[（三）常用软件 6](#_Toc63680257)

[（四）软件详情 7](#_Toc63680258)

[（五）监控中的软件 7](#_Toc63680259)

[六、监控管理 8](#_Toc63680260)

[（一）软件未打开，启动软件并监控 8](#_Toc63680261)

[（二）监控历史 10](#_Toc63680262)

[（三）监控详情 11](#_Toc63680263)

[（四）文件读写监听 12](#_Toc63680264)

[（五） 注册表监听 15](#_Toc63680265)

[（六）进程调用 16](#_Toc63680266)

[（七）设备控制 17](#_Toc63680267)

[（八）网络访问监听 19](#_Toc63680268)

[（九）文件对象权限监听 20](#_Toc63680269)

一、简介

本章将简要地说明针对Linux平台的工业软件运行行为监控模块用户操作手册(以下简称本手册)的目的、范围。

（一）手册目的

本手册的目的在于指引用户如何使用针对Linux平台的工业软件运行行为监控模块，本系统提供了哪些功能，以及如何正确地、有效地来使用这些功能。

（二）手册范围

* 本手册首先简要地介绍系统的结构，然后说明系统提供的各项功能及其详细的操作步骤。
* 本手册各章节内容安排如下：
* 第一部分 简介：简单说明本手册的目的、范围。
* 第二部分 软件概述：简单说明系统的结构、执行环境。
* 第三、四、五、六部分为整个系统的功能操作说明，希望使用者能深入了解。

**二、软件概述**

本章将简要说明本软件之目标、软件环境。

（一）软件目标

系统的主要目标是提供能够满足针对Linux平台的工业软件运行行为监控的测试场景，便于对各类针对Linux平台的工业软件开展安全测试，软件运行行为的监控。

（二）软件环境

系统主要运行在常用Linux 64位系统，内核版本3.10以上。包括单不限于 Centos 7.x， Ubuntu支18.x/20.x，支持持chrome、Fixefox等 H5浏览器界面访问。

三、系统启动

1.安装Linux环境下的jdk 11。 Centos下可以用root账号运行 yum install java-11-openjdk。 Ubuntu下可以用命令 sudo apt-get install openjdk-11-jdk

Centos下如果安装完jdk11后，使用命令jdk –version查看版本还未改为11的，需要运行以下命令进行jdk选择，选择新安装的jdk 11.

Centos调整jdk版本命令： alternatives –config java

2.解压安装包，建议解压到root账号的根目录下如/root/monitor。

3.配置系统运行用户。由于本监控软件需要使用root账号启动，如对应的启动软件不能使用root账号运行，则需要配置对应的启动用户，不配置默认使用root账号运行监控的软件。

配置文件在config/application.yaml，修改linux-user: 后面追加对应的启动账号名。

4.启动shell终端，并且切换用户到root，cd到软件目录，使用./start.sh启动软件

5.查看启动日志，日志在logs/all.log， 查看到“启动成功，请打开浏览器并访问：http://ip:8080/index.html ”则表示软件启动成功。

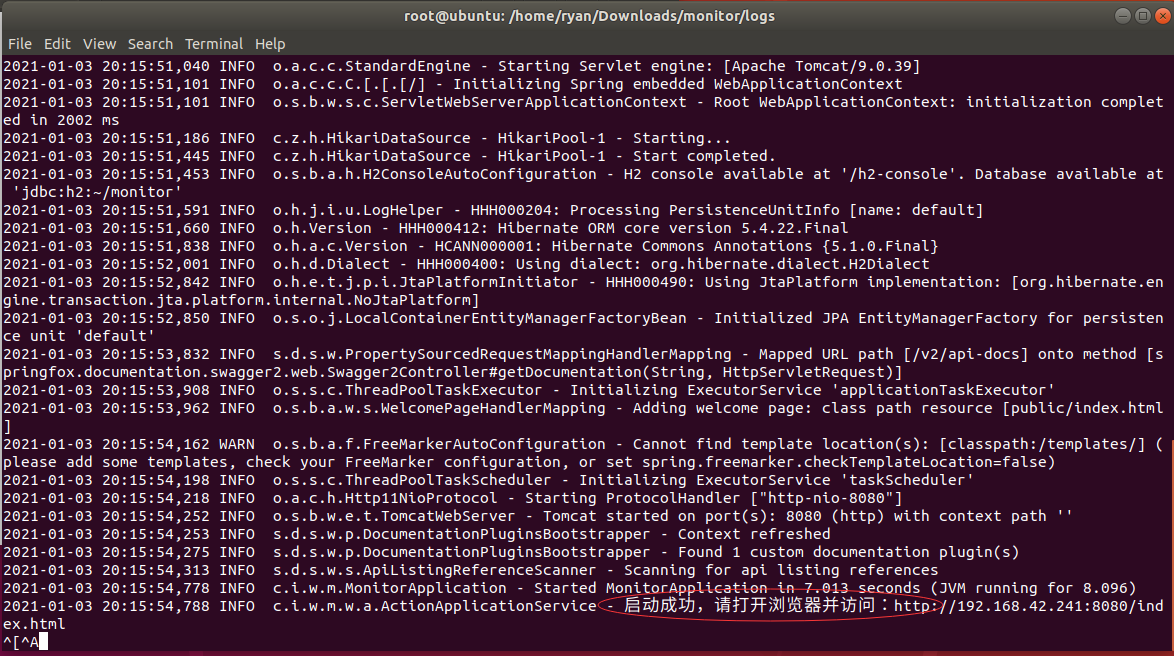


图3-1-1

5.由于linux系统可能未安装视窗界面，因此可以使用其他远程机器通过浏览器远程访问本软件。

注意：如果使用centos 7.0等较老系统，由于系统自带的firefox过旧，会引起页面无法打开，建议先更新浏览器或者按照chrome浏览器，或者使用其他电脑进行远程访问。 更新firefox浏览器： yum install firefox

如果是centos系统，需要远程浏览访问的需要关闭防火墙或者开启8080端口。

开放端口命令（2条均需要执行）：

firewall-cmd --add-port=8080/tcp

firewall-cmd --permanent --add-port=8080/tcp



图3-1-2

6.要停止软件，则使用./stop.sh停止。

四、系统首页

1.登录后，默认进入到系统首页如图；

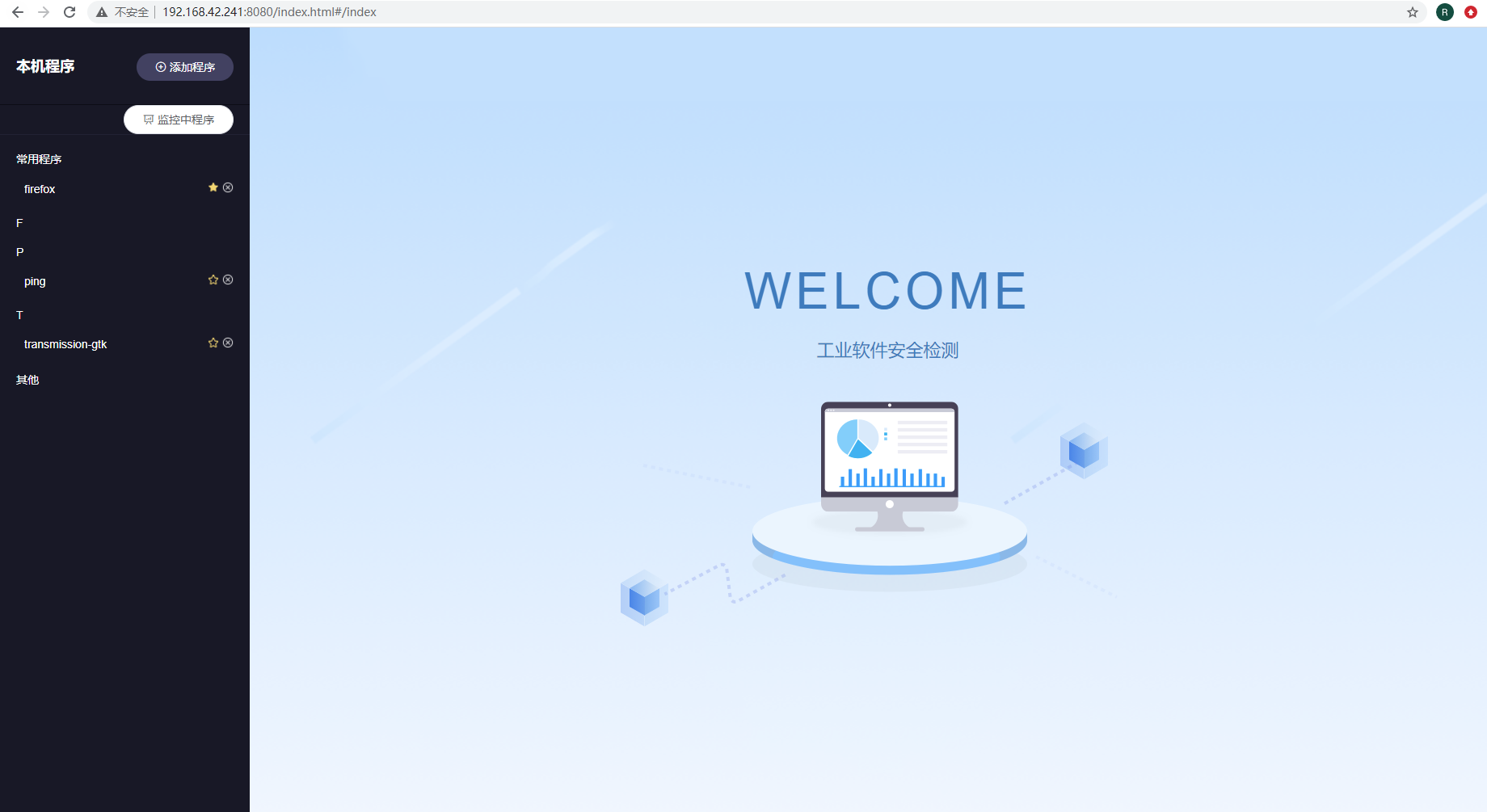


图4-1-1

五、监控软件管理

监控软件管理：用户可以勾选常用软件，自行添加可执行程序或自行添加可执行命令。

（一）添加可执行程序

1.选择添加程序按钮。

2.弹出文件选择器，按目录自行选择可运行的软件

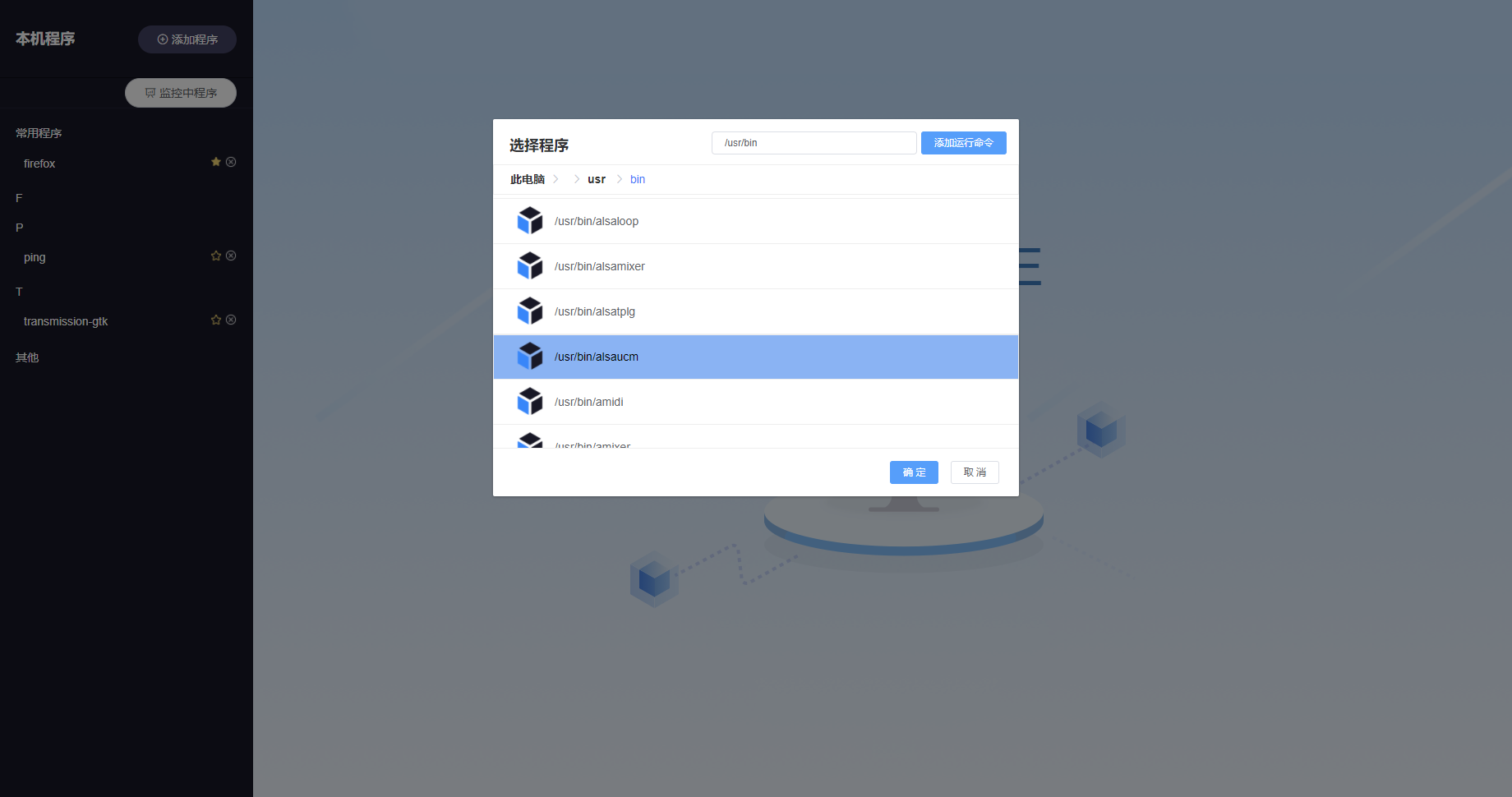


图5-1-1

1. 点击确认，添加可运行的软件。
2. 左则软件栏增加对应的软件。
3. 点击新增软件右边的x按钮，可以删除当前添加的软件。

（二）添加可执行的命令行

1.由于linux下很多软件是通过命令行启动的，因此允许用户直接添加命令行。

2.点击添加程序，在弹出输入框的右上角输入要添加的命令行，点击添加运行命令添加到软件列表种。 如firefox的启动命令：/usr/lib/firefox/firefox -new-window

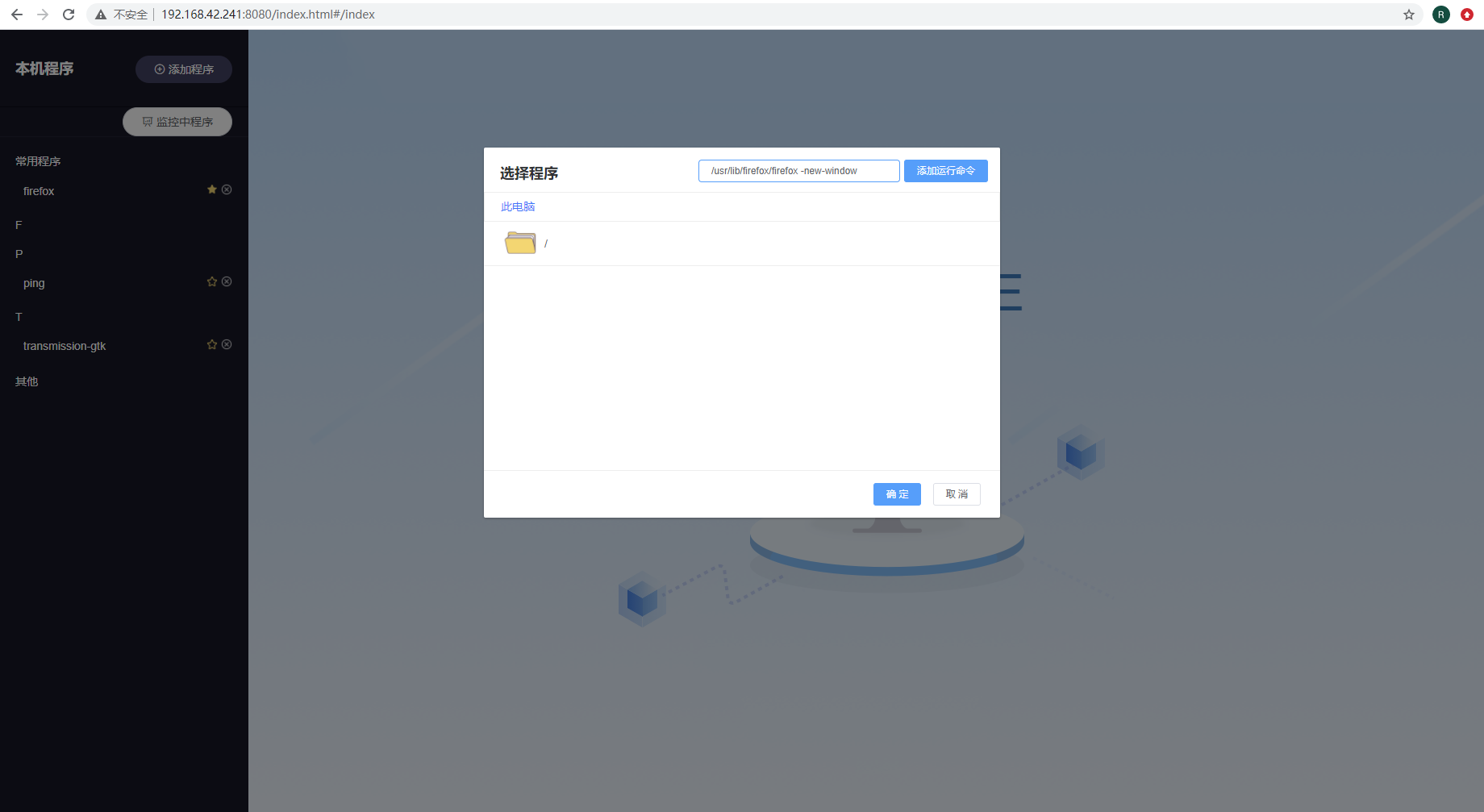


图5-2-1

（三）常用软件

1.点击首页软件列表

2.点击软件列表的星星标号，未设置为常用软件的，点后变为常用软件

3.已添加为常用软件的，点击后则移除常用软件。



图5-3-1

（四）软件详情

1.点击左侧软件名称

2.打开软件详情

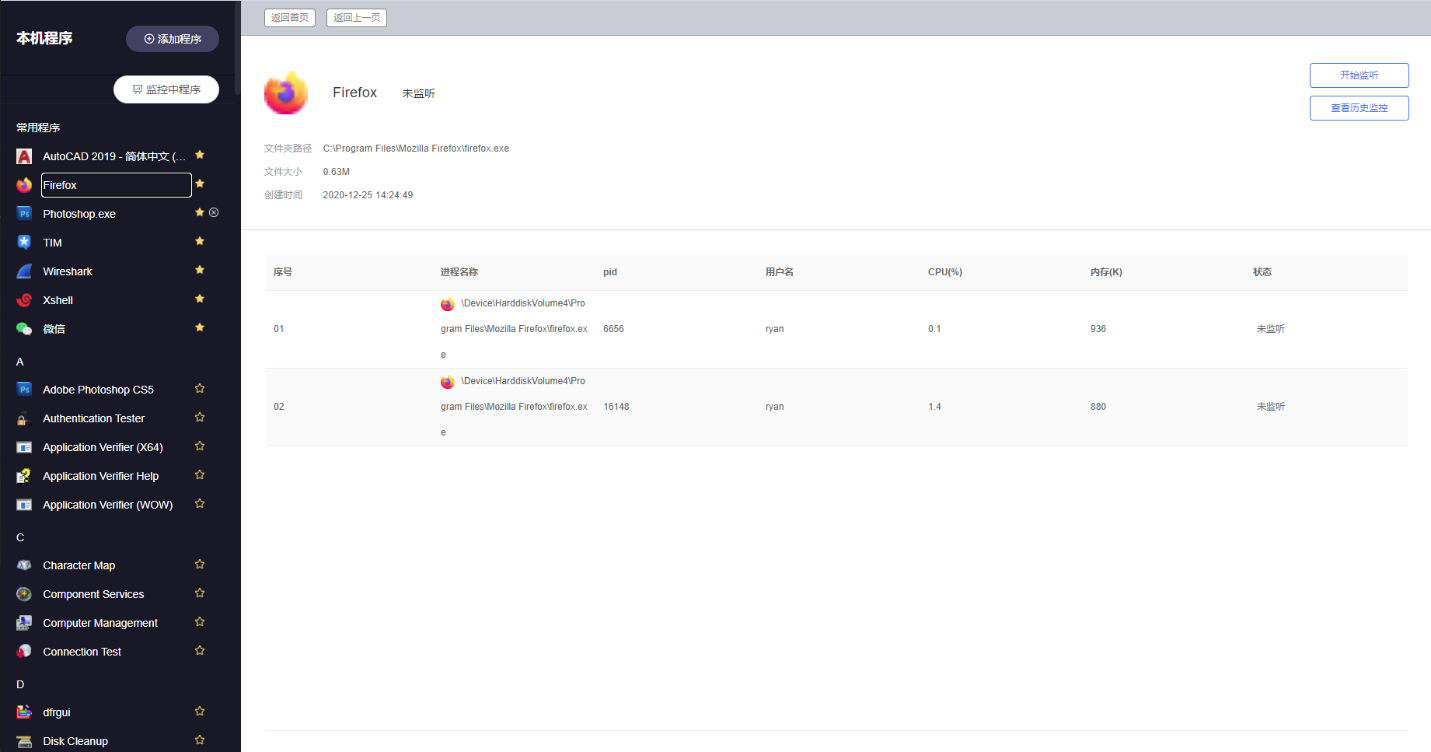
3.详情页中将会显示软件的详细信息和监控状态，正在运行的软件会显示对应的进程列表。

图5-4-1

（五）监控中的软件

1.点击首页左上角的监控中软件

2.界面会打开对应的正在监控的软件列表

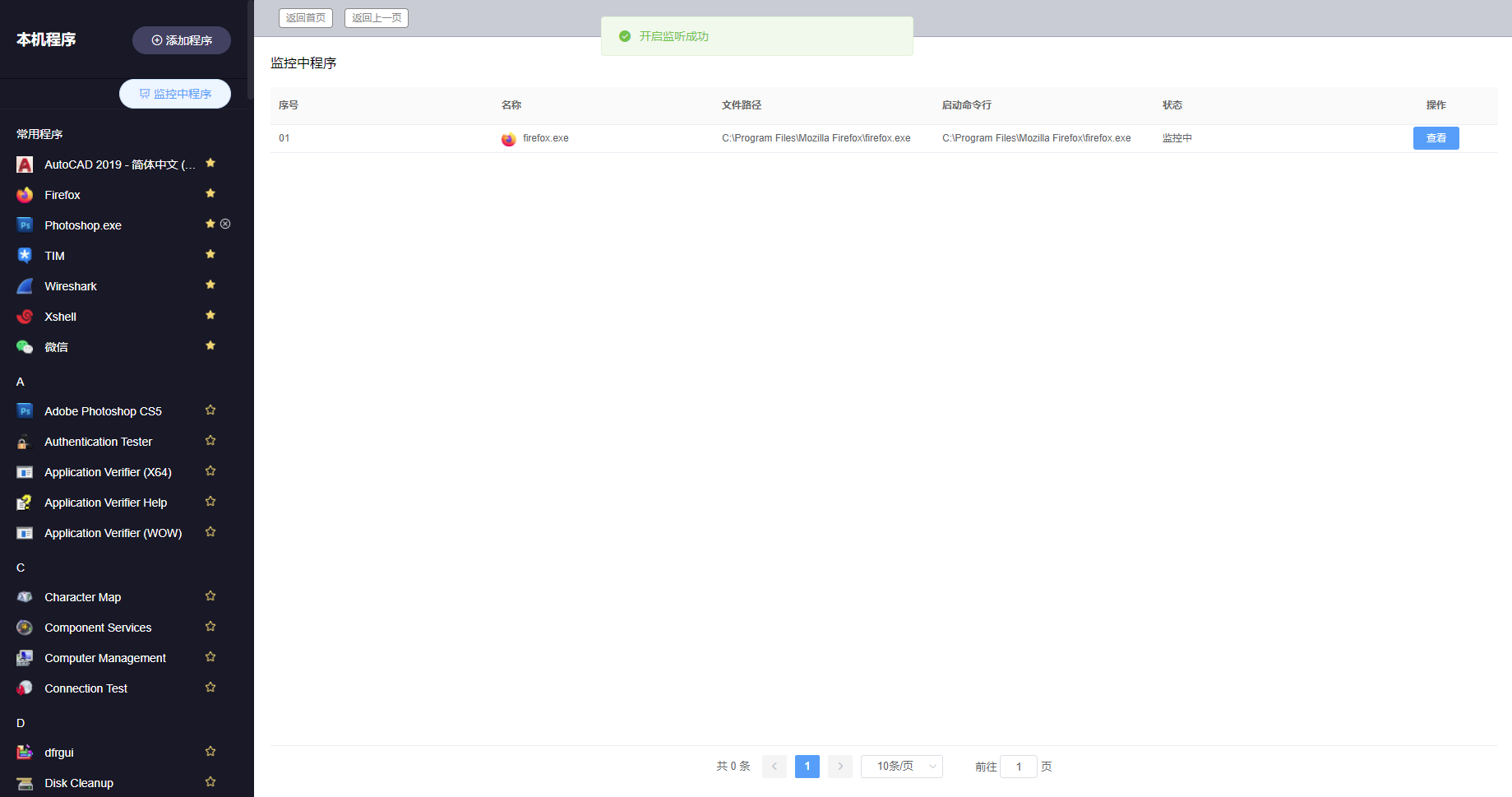


图5-5-1

六、监控管理

监控管理包括监控状态、监控详情、历史监控记录等重要功能

（一）软件未打开，启动软件并监控

1.保证软件未打开，系统未显示对应的软件进程

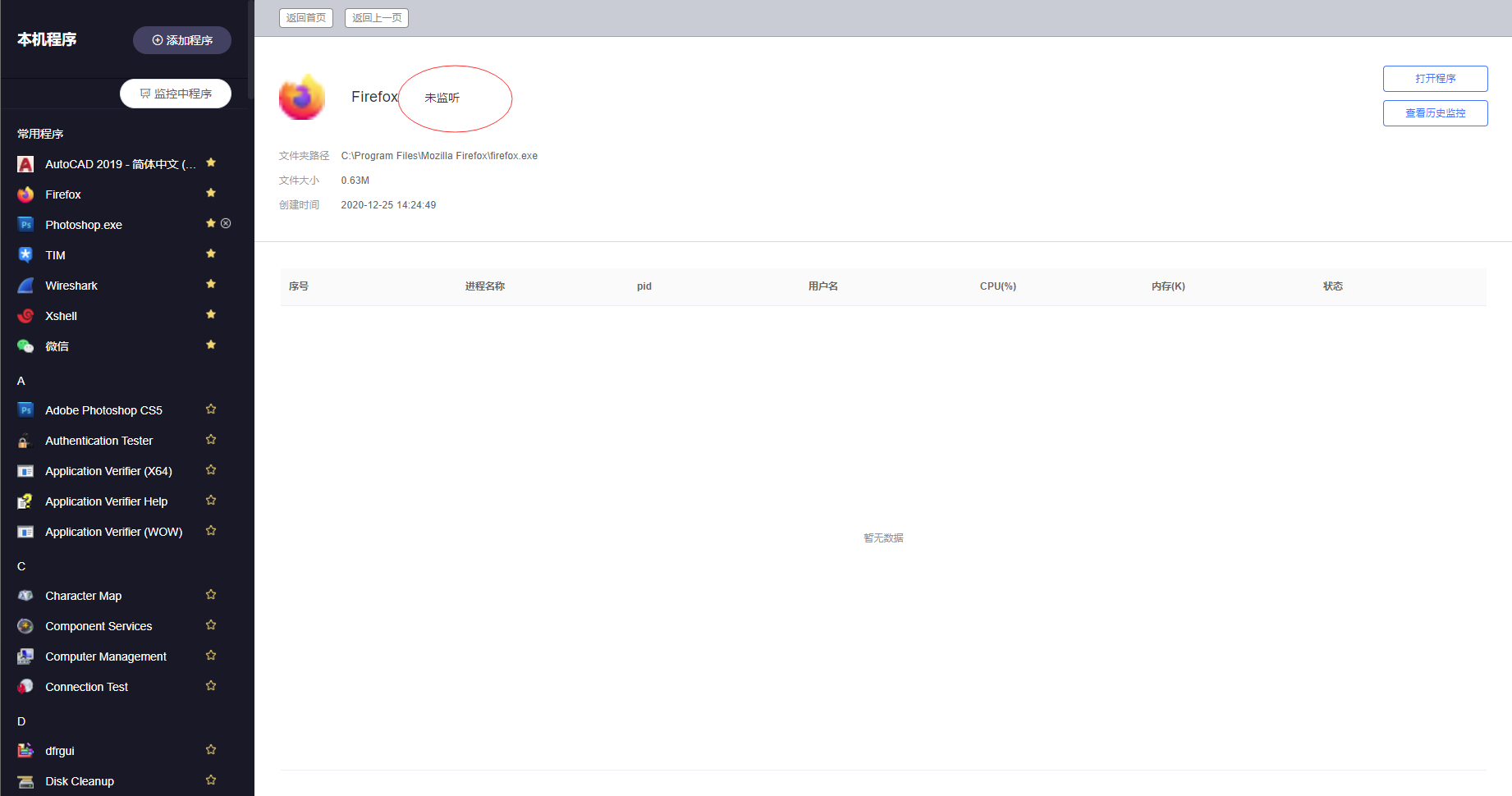


图6-1-1

1. 点击右上角的打开程序按钮，软件会启动并进入监控状态

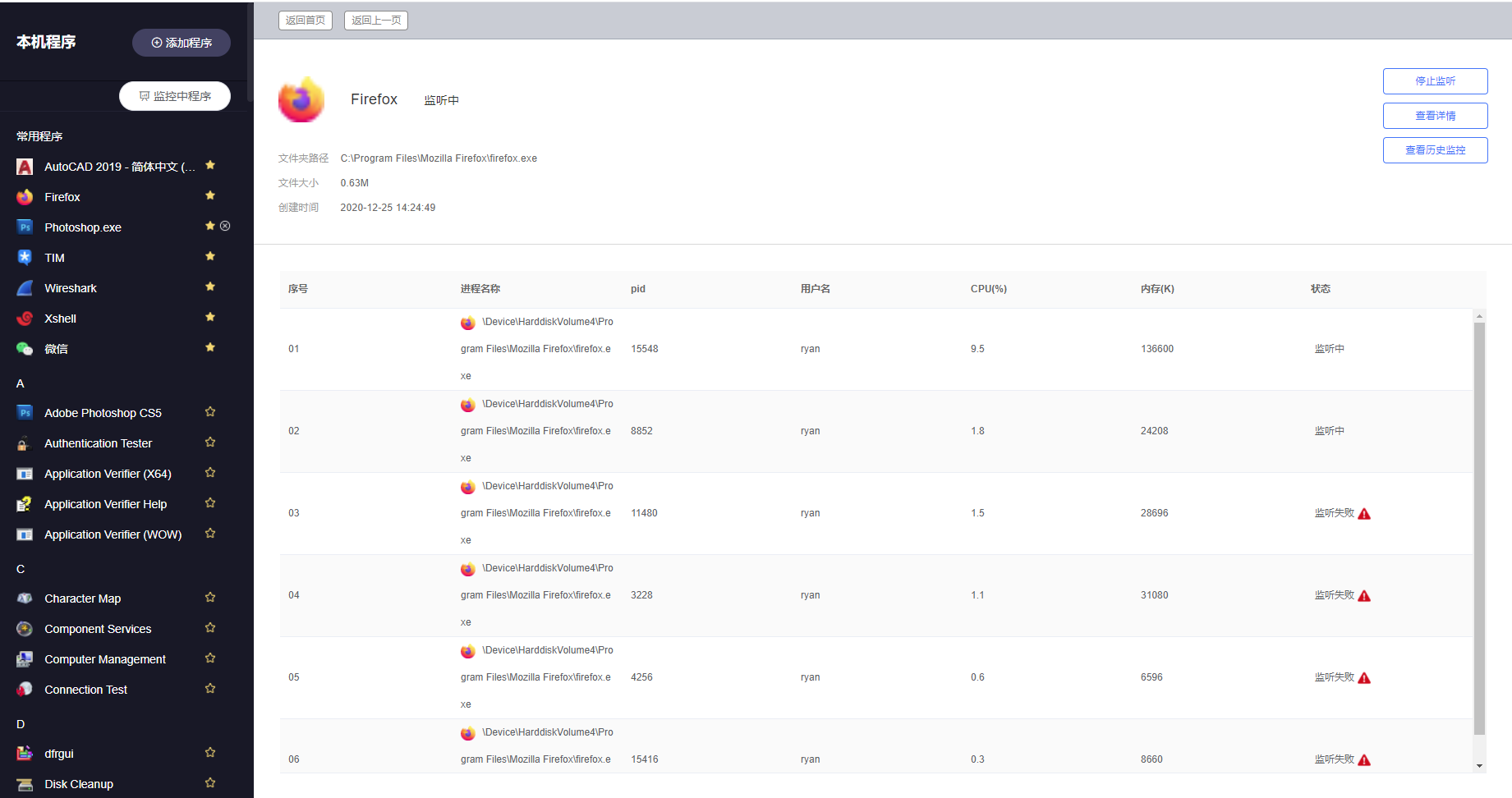


图6-1-2

1. 点击停止监听，可停止软件的监听。

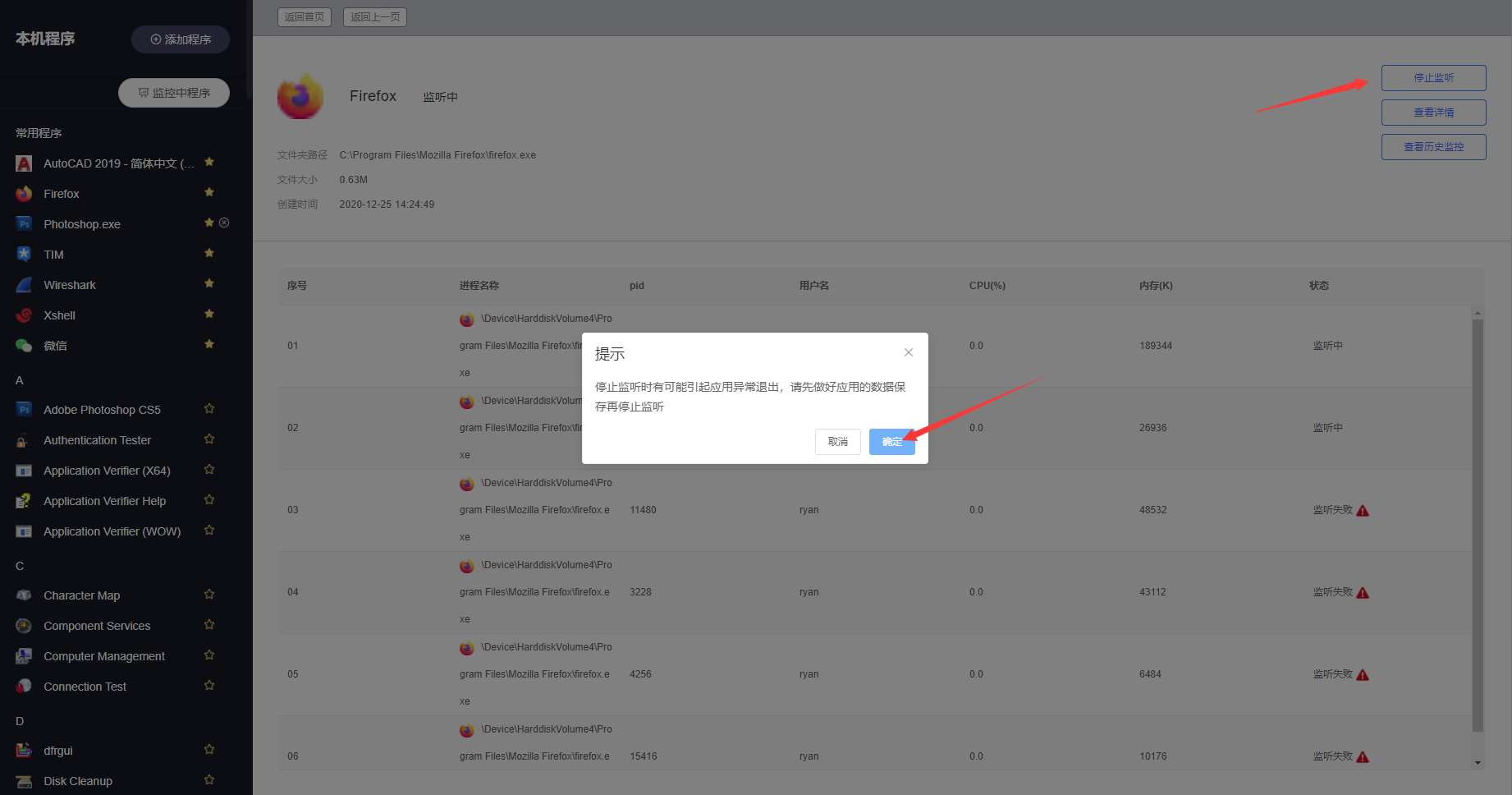


图6-1-3

注：停止监听时有可能引起应用异常退出，请先做好应用的数据保存再停止监听

（二）监控历史

1.点击软件详情中的查看历史监控可以打开历史监控记录

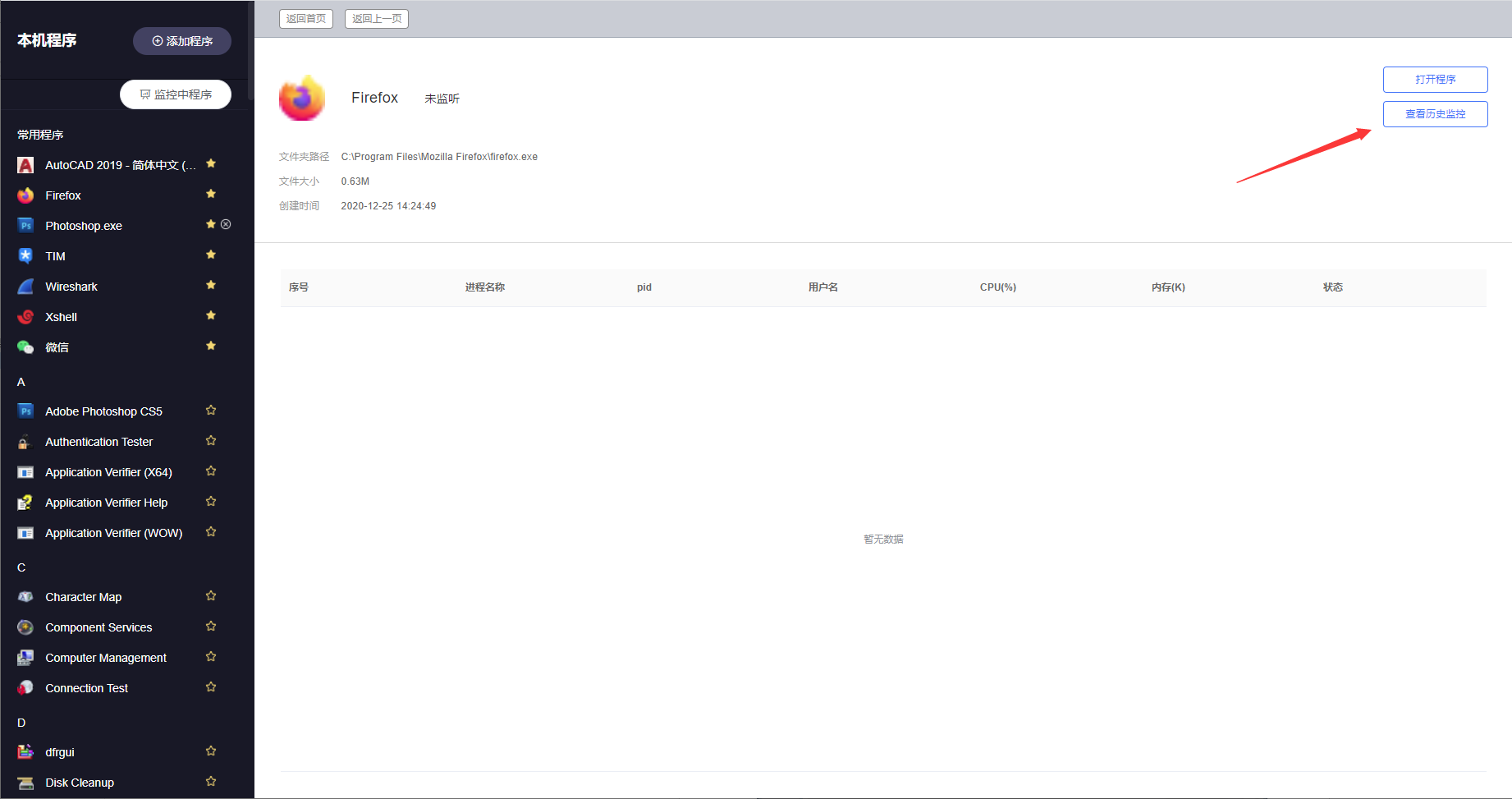


图6-2-1

1. 监控历史页面会显示历史的监控记录。用户可以通过监控时间、进程pid等进行历史记录筛选查询。



图6-2-2

1. 点击操作栏“删除”按钮，可以删除历史监控记录。

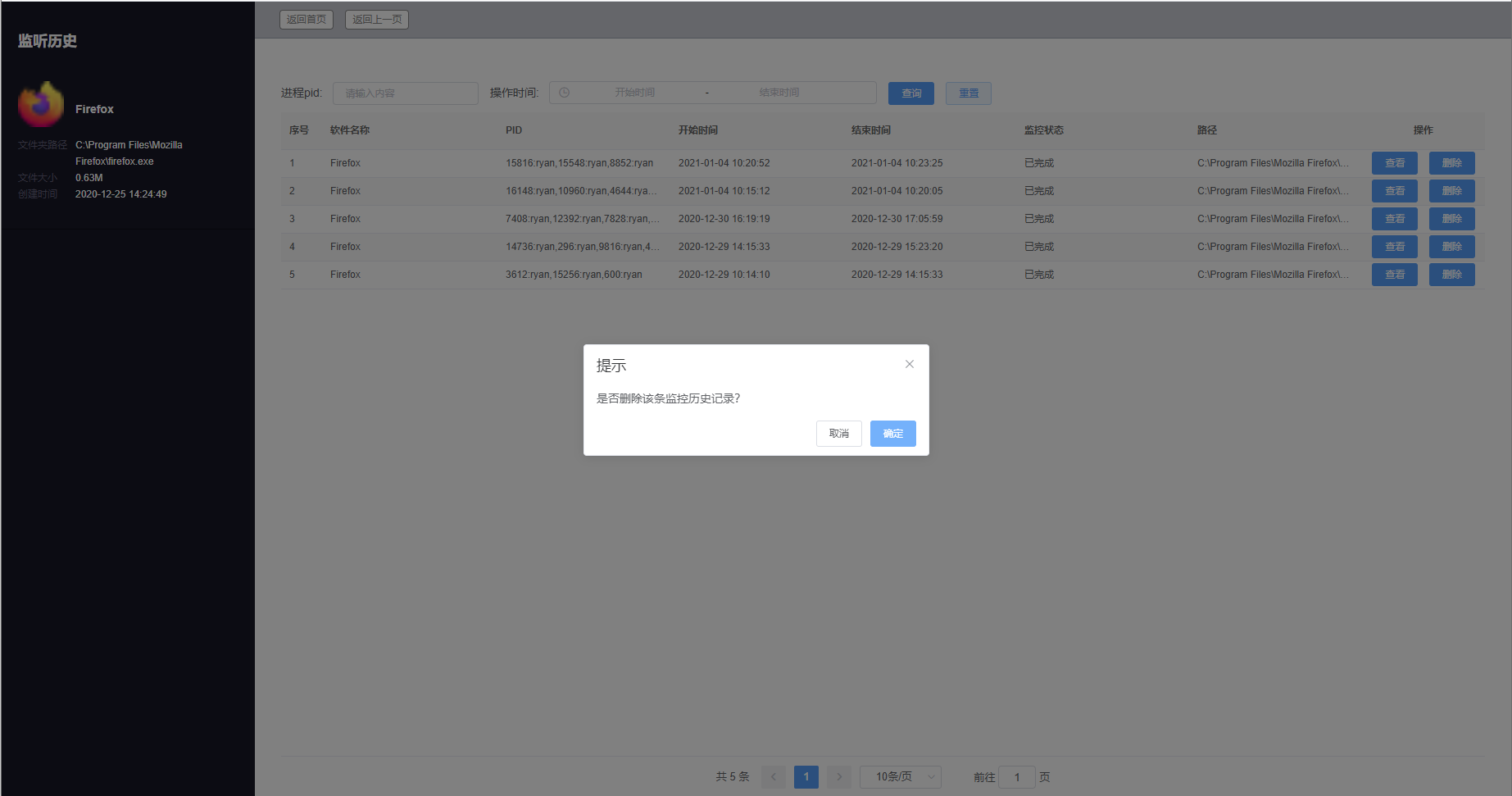


图6-2-3

1. 点击操作栏“查看”按钮，可查询监控详细记录。

（三）监控详情

1.通过历史监控记录、或者正在监控软件的查看详情按钮，可以进入当前监控的详细信息。

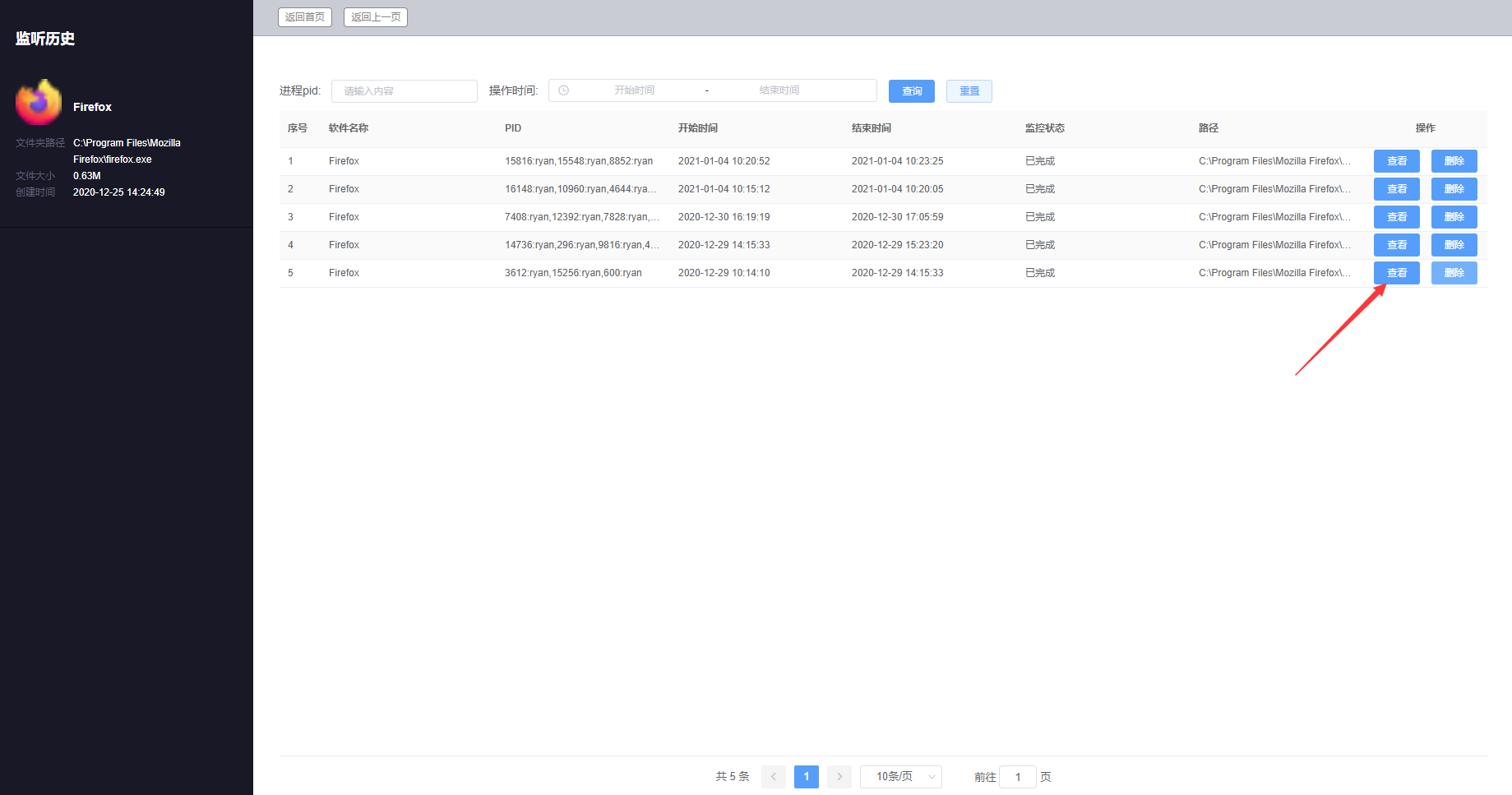
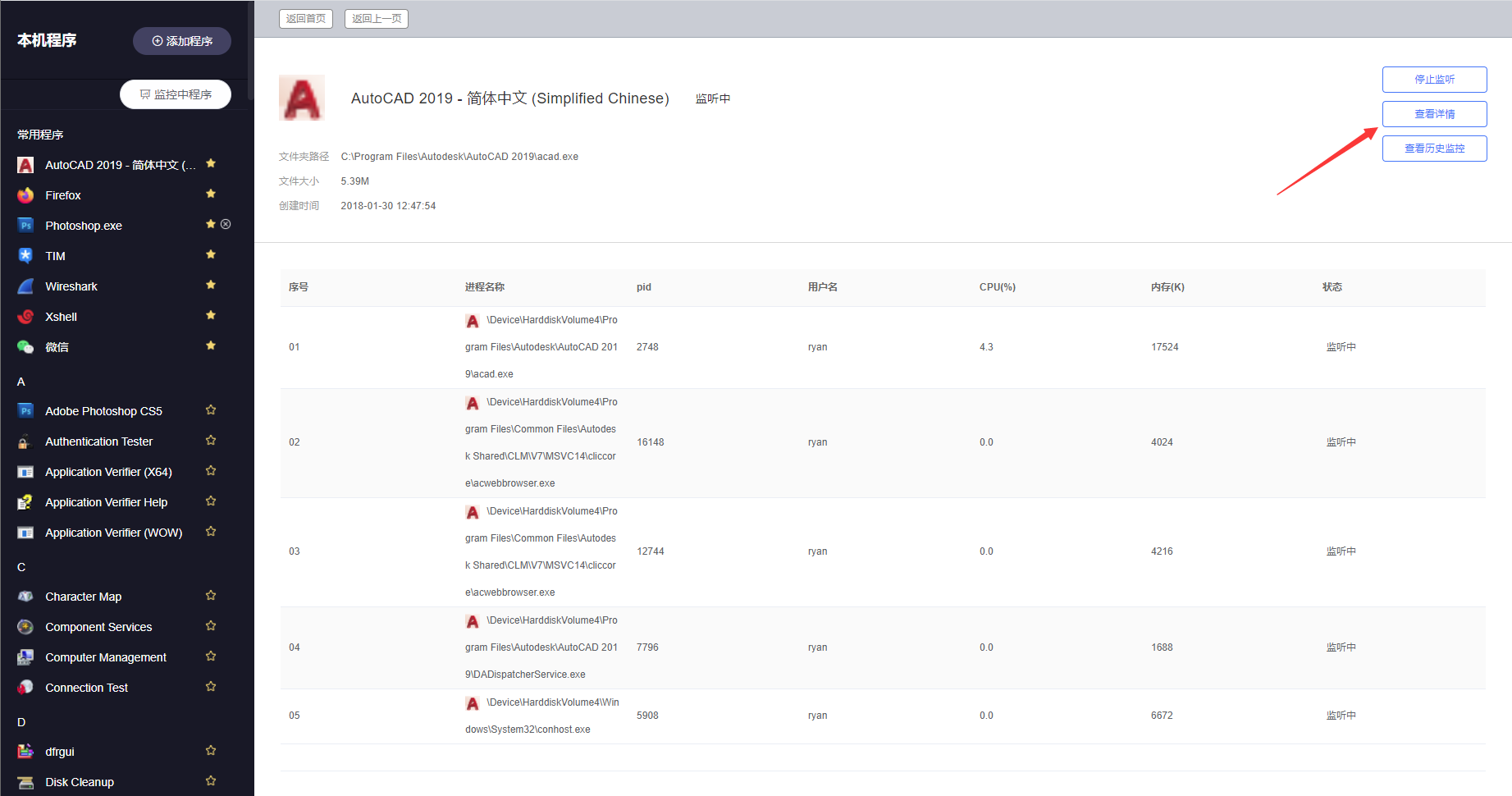


图6-3-1



（四）文件读写监听

1.进入监控详情，切换到文件读写监听栏目

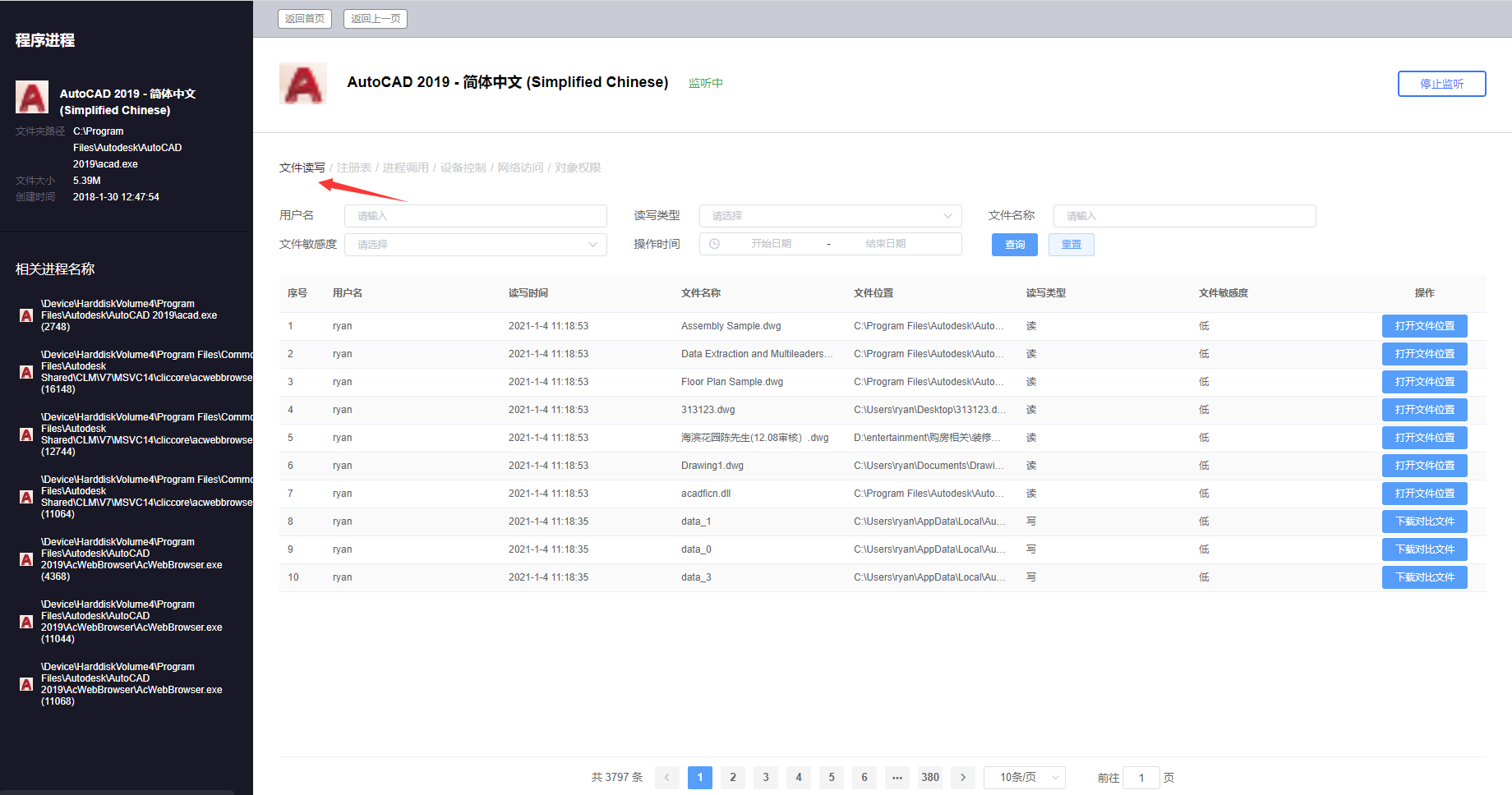


图6-4-1

1. 针对读文件记录，可以进行“打开文件位置”操作，点击“打开文件位置”按钮，软件会调用系统文件管理器弹出当前文件所在文件夹；

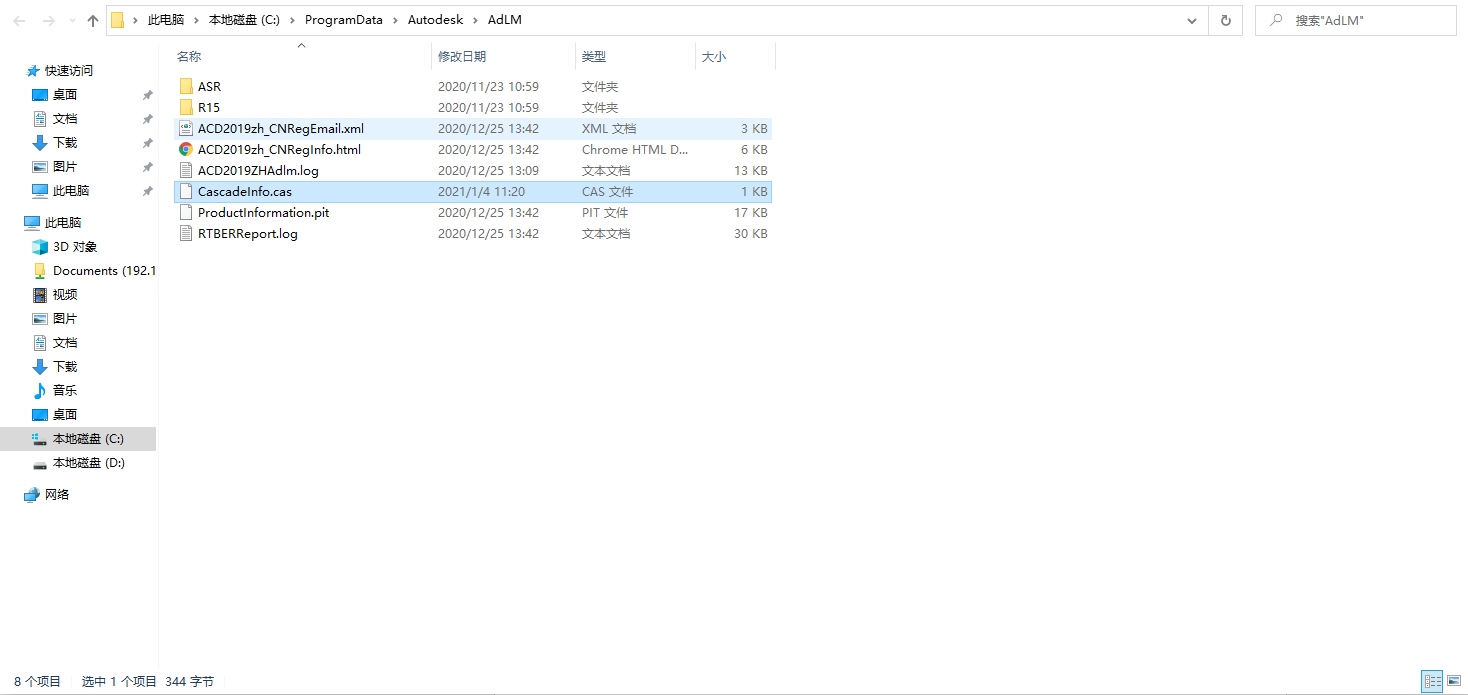


图6-4-2

注：如果非本地运行，则打开文件位置按钮会变为下载文件。

1. 针对写文件记录，可以进行“下载对比文件”操作，下载回来的是zip包，包含old和new 2个文件，分别为写入前和写入后对比文件。 用户可以使用其他文件对比工具进行文件变更细节对比。

如果写入的文件为新文件，则下载回来的zip包中不含有old文件记录。

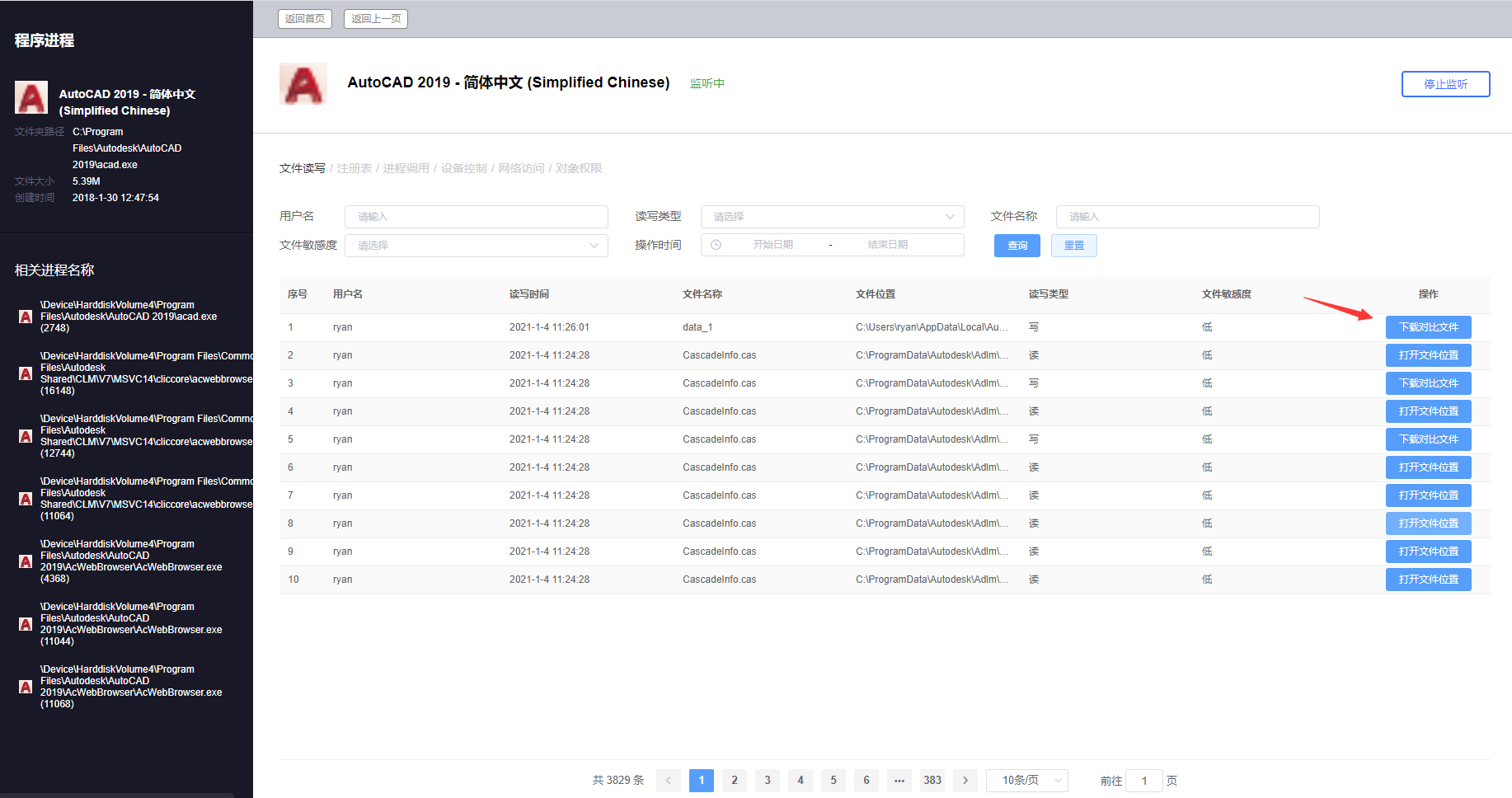


图6-4-3

1. 针对删除类型的文件操作，可以进行“下载文件”操作，会下载系统备份的已删除文件。

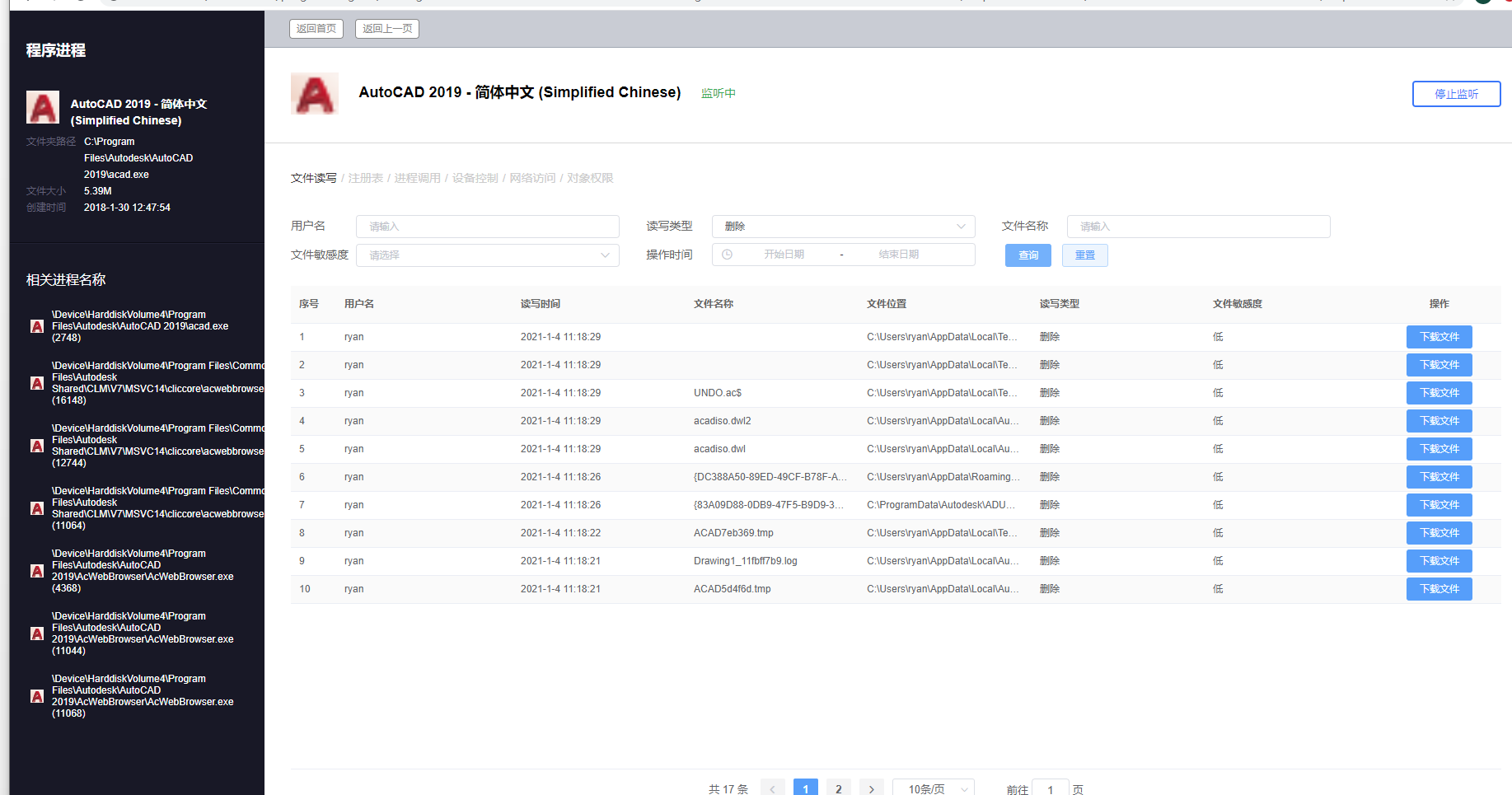


图6-4-4

1. 注册表监听

1.进入监控详情，切换到注册表监听栏目



图6-5-1

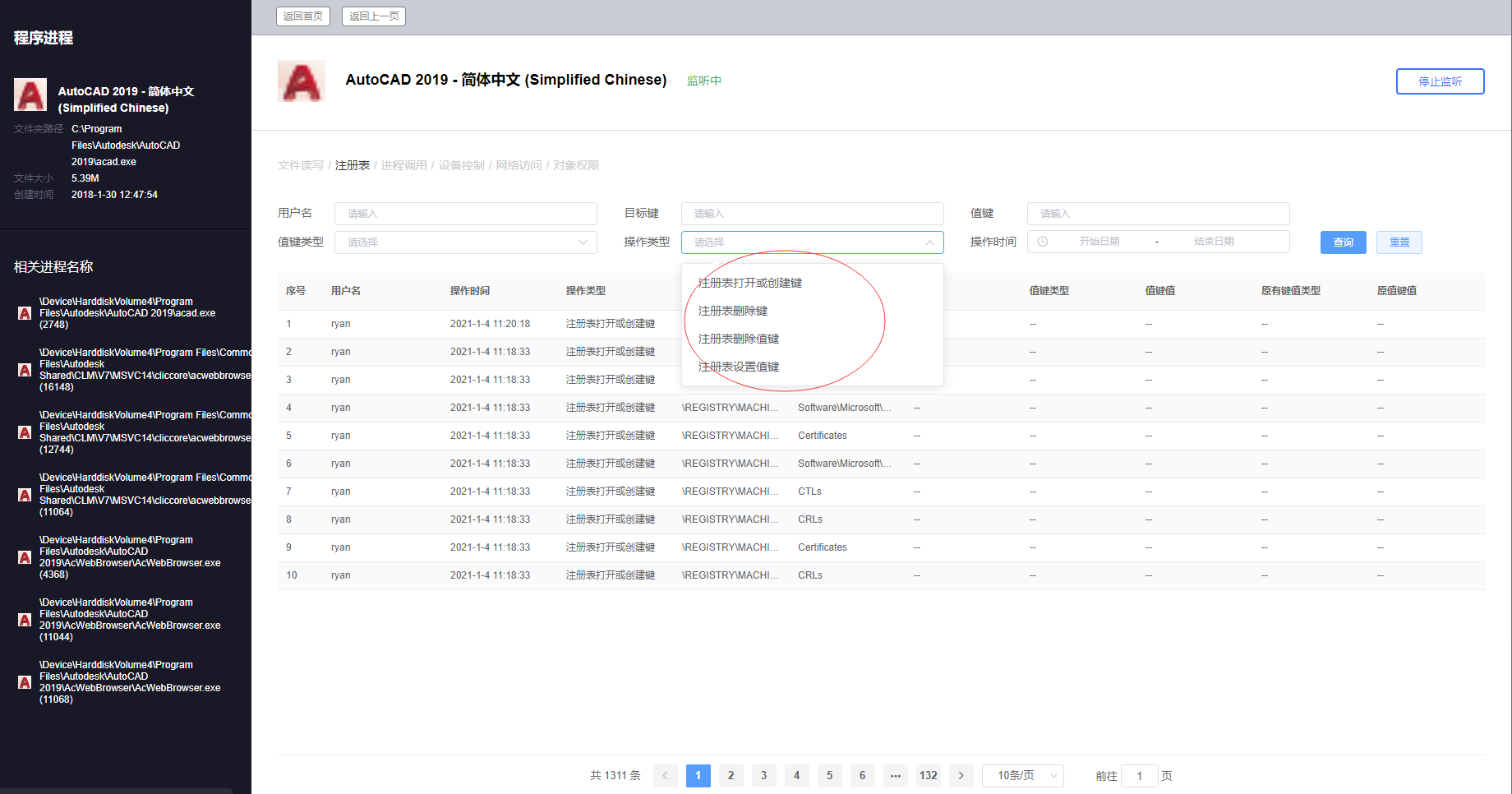
2.系统监听了4大类常用注册表操作，包括打开和创建（读）、删除键、删除值键、设置值键

图6-5-2

3.注册表值键设置会备份注册表原有值和设置值。

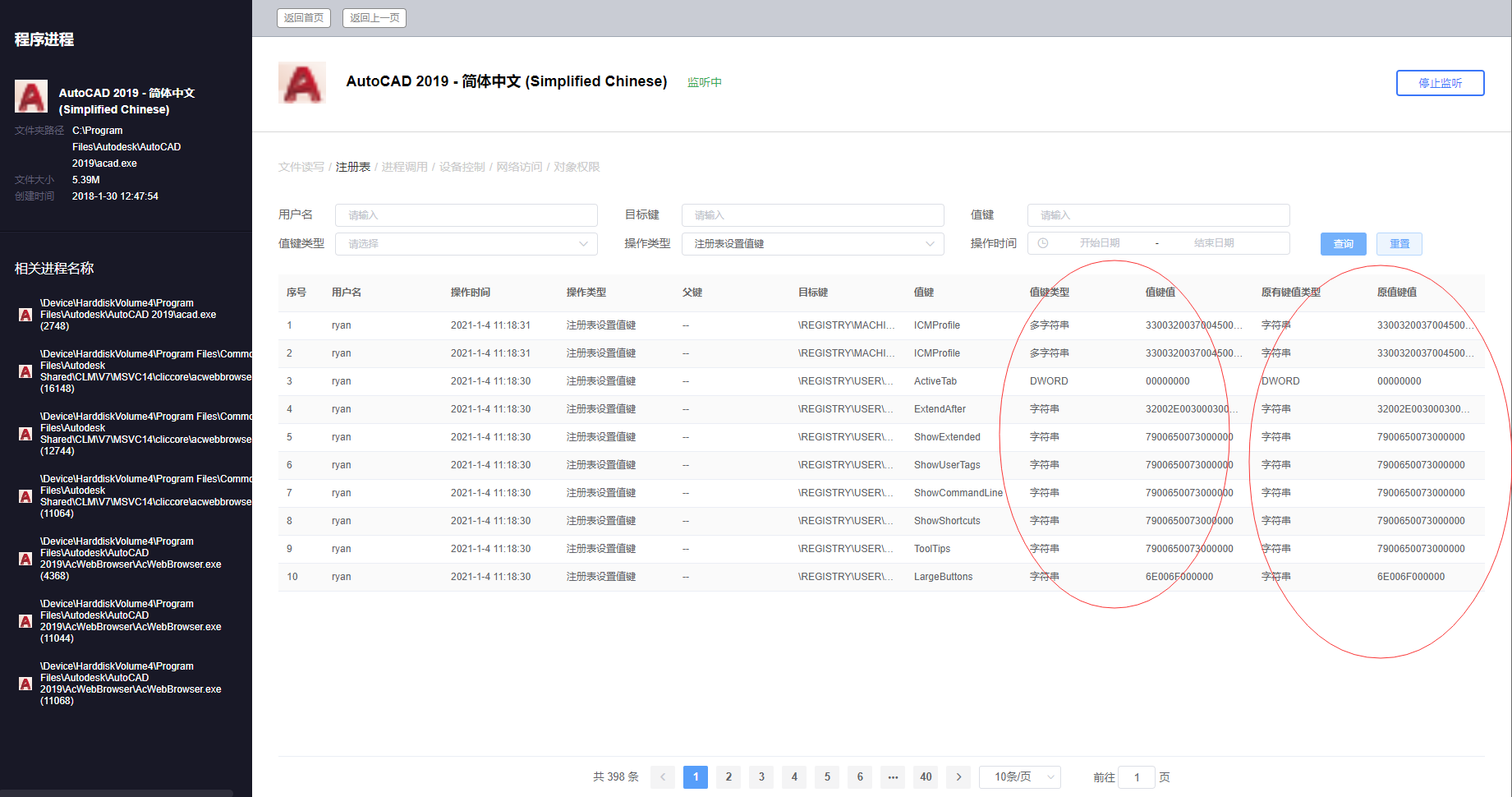


图6-5-3

（六）进程调用

1.进入监控详情，切换到进程调用栏目

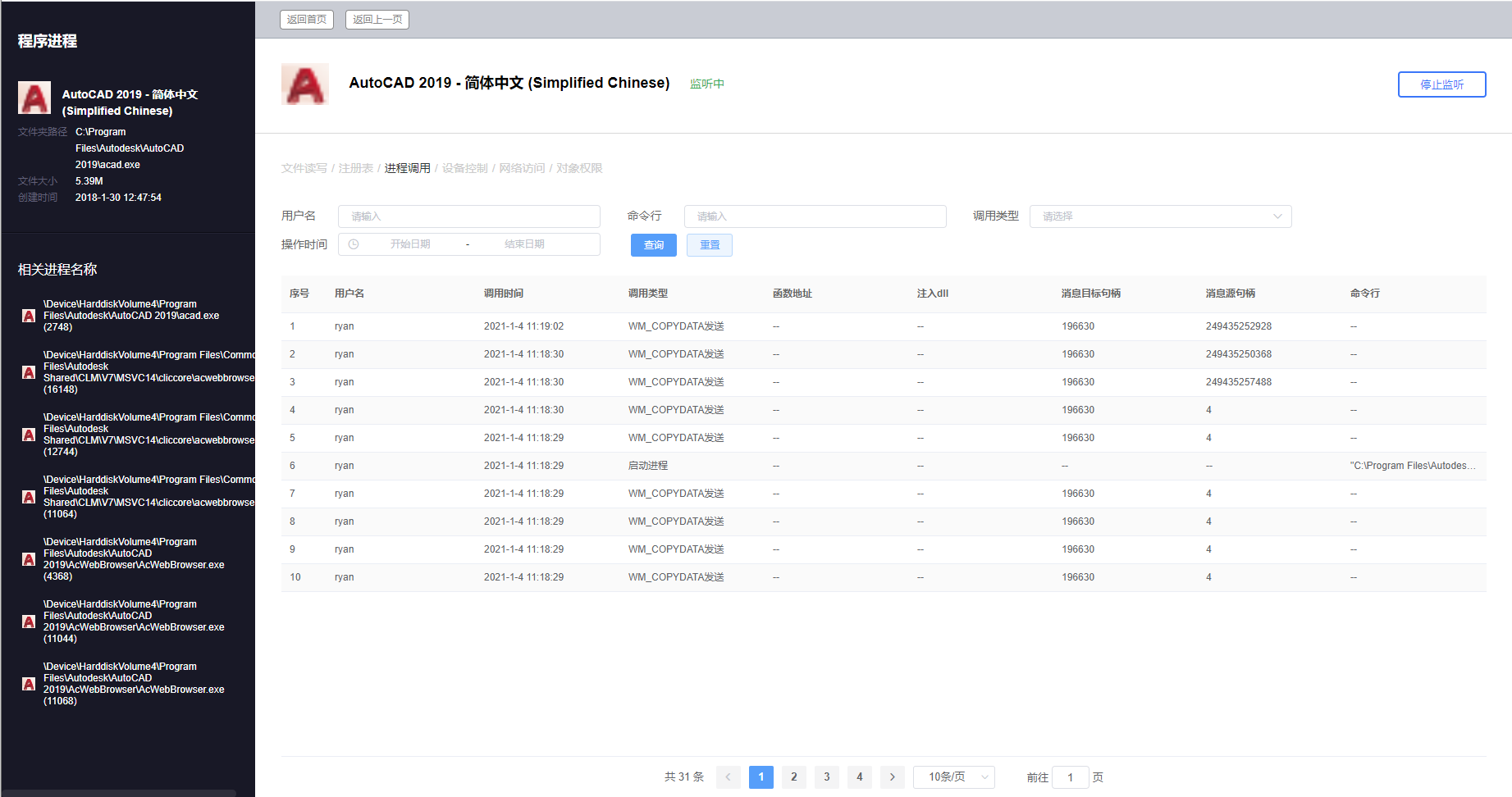


图6-6-1

2.系统监听了3大类常用进程调用，包括启动进程、进程注入和消息通讯。

启动进程: 表示软件启动了其他进程

进程注入：表示软件进行了其他进程的注入操作

消息通讯：表示软件进行消息通讯，消息通讯为常用的进程间调用方法。

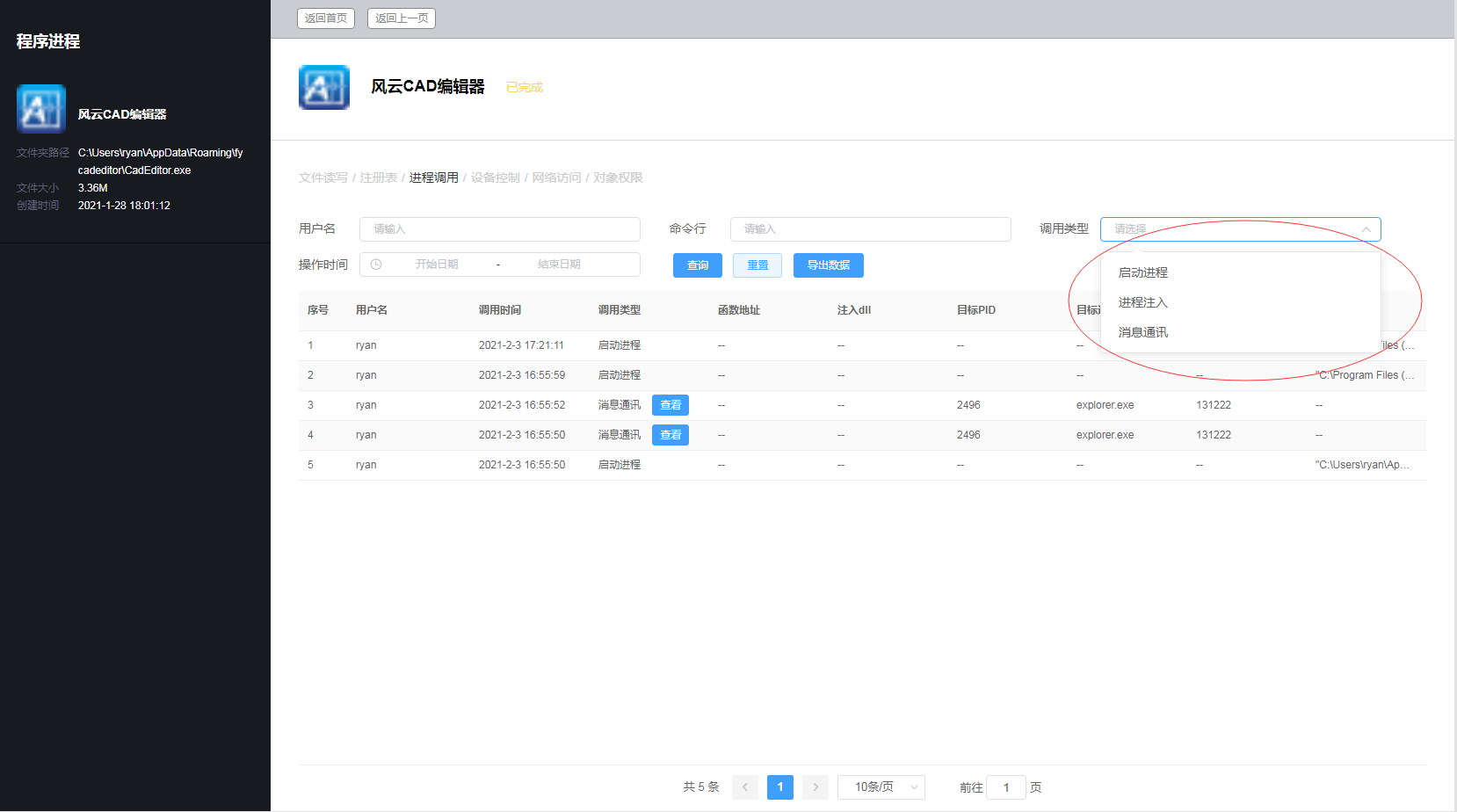


图6-6-2

3.启动进程： 界面会显示具体的启动进程命令

消息通讯： 界面会显示消息通讯的消息调用类型、消息发送的目标窗口句柄和消息发送源的窗口句柄。

进程注入：界面会显示注入的dll文件、注入的函数地址

（七）设备控制

1.进入监控详情，切换到设备控制监听栏目

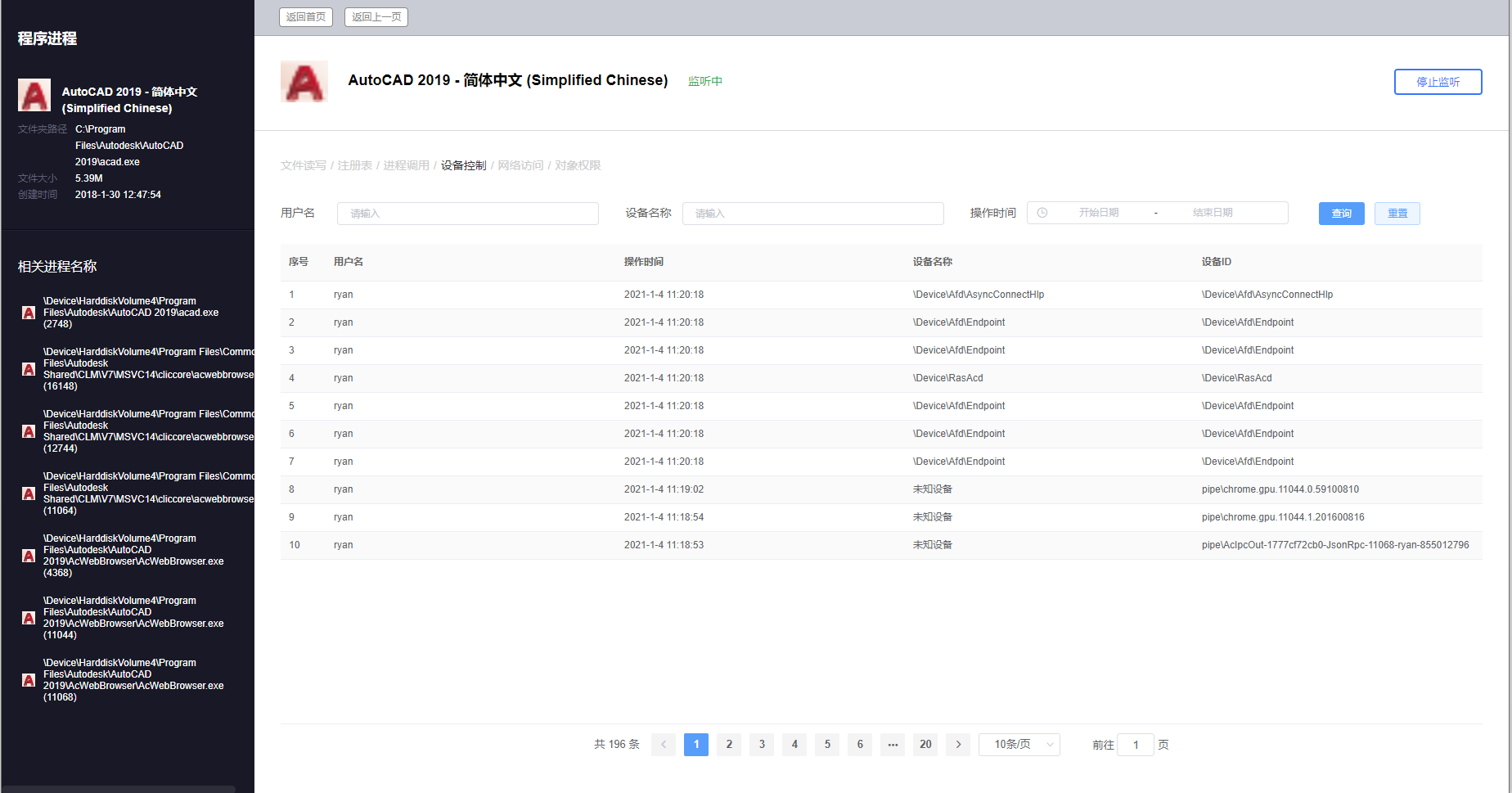


图6-7-1

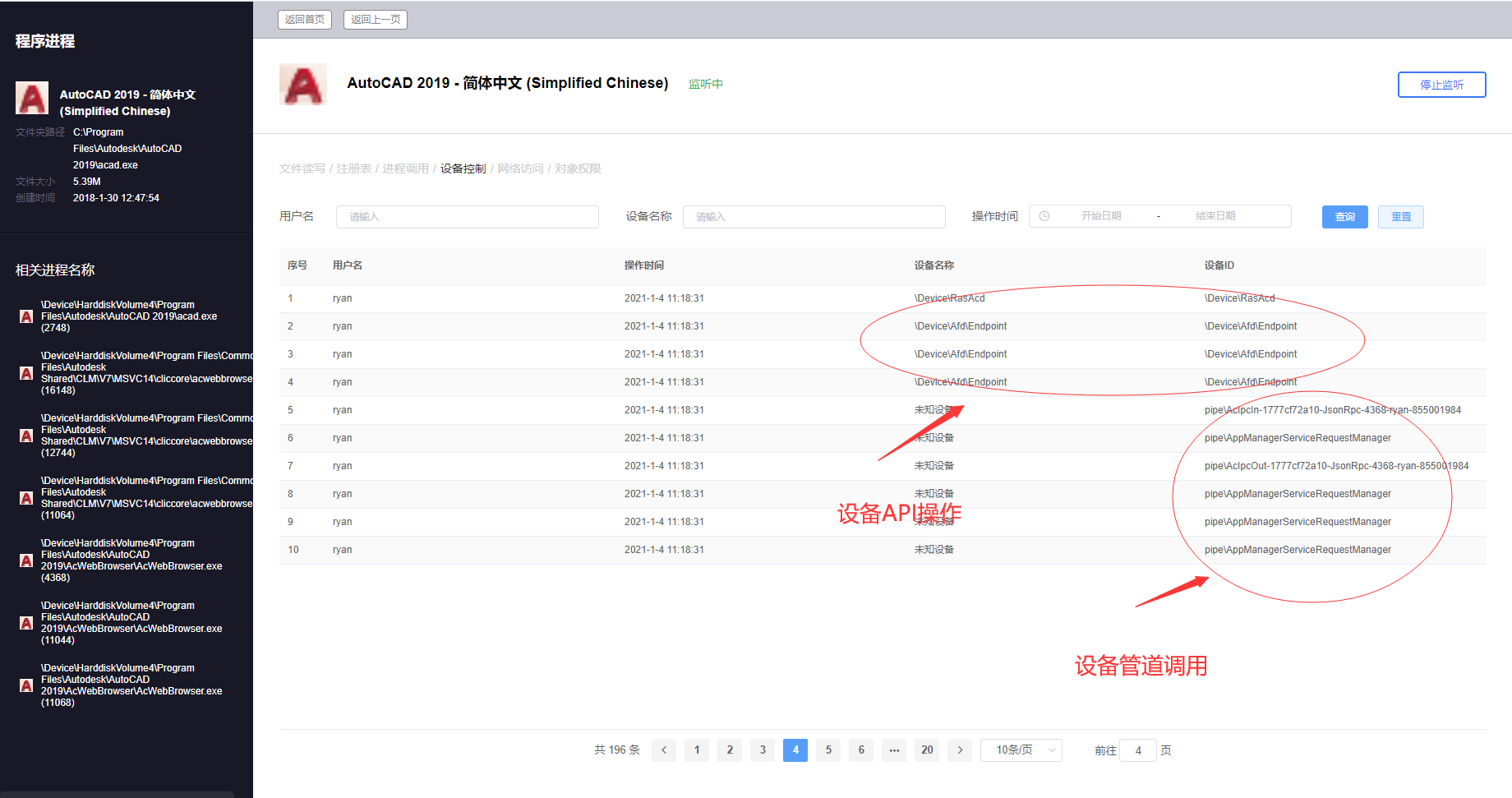
2.设备控制会监控软件所有的设备相关调用行为，注意设备除了摄像头，打印机等物理设备外，还监控记录了软件的虚拟设备行为，包括设备搜索、设备相关API调用、设备管道调用等。

图6-7-2

（八）网络访问监听

1.进入监控详情，切换到网络访问监听栏目

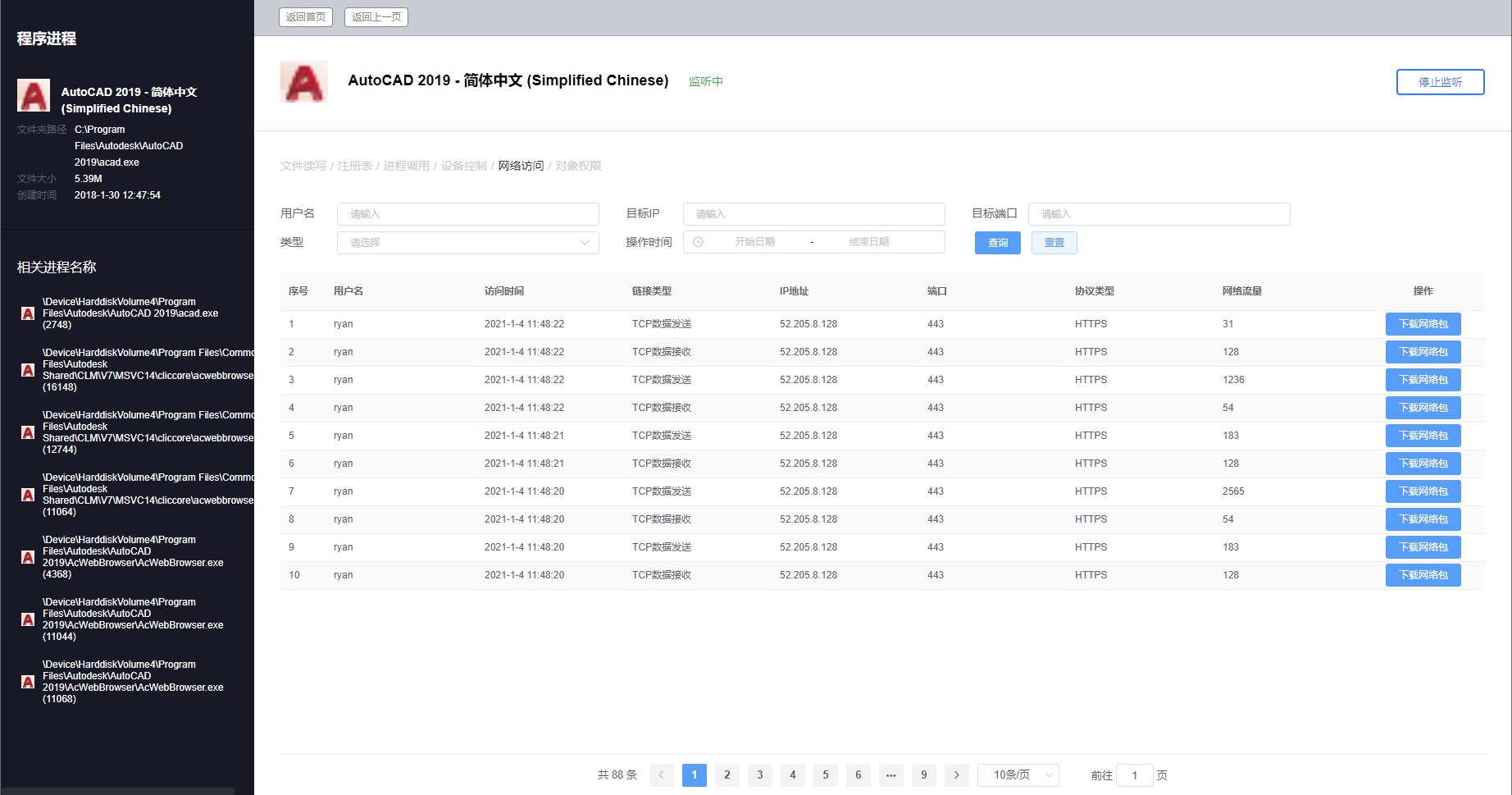


图6-8-1

2. 软件监听了5大类型的网络访问，包括发起网络链接、TCP数据发送、TCP数据接收、UDP数据发送、UDP数据接收

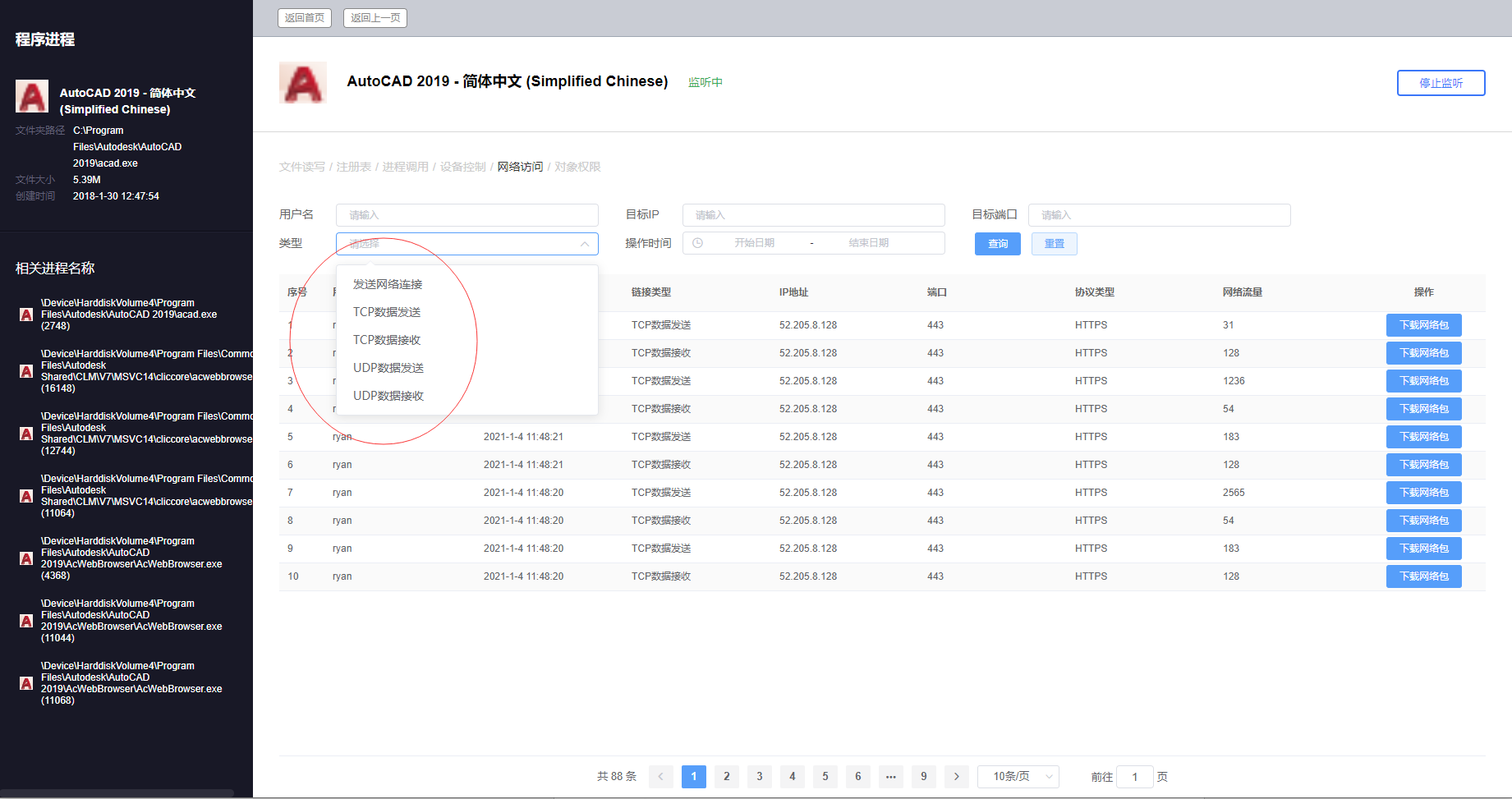


图6-8-2

3. 针对网络发送和网络接收操作，用户可以点击下载对应的发送和接收的网络包。

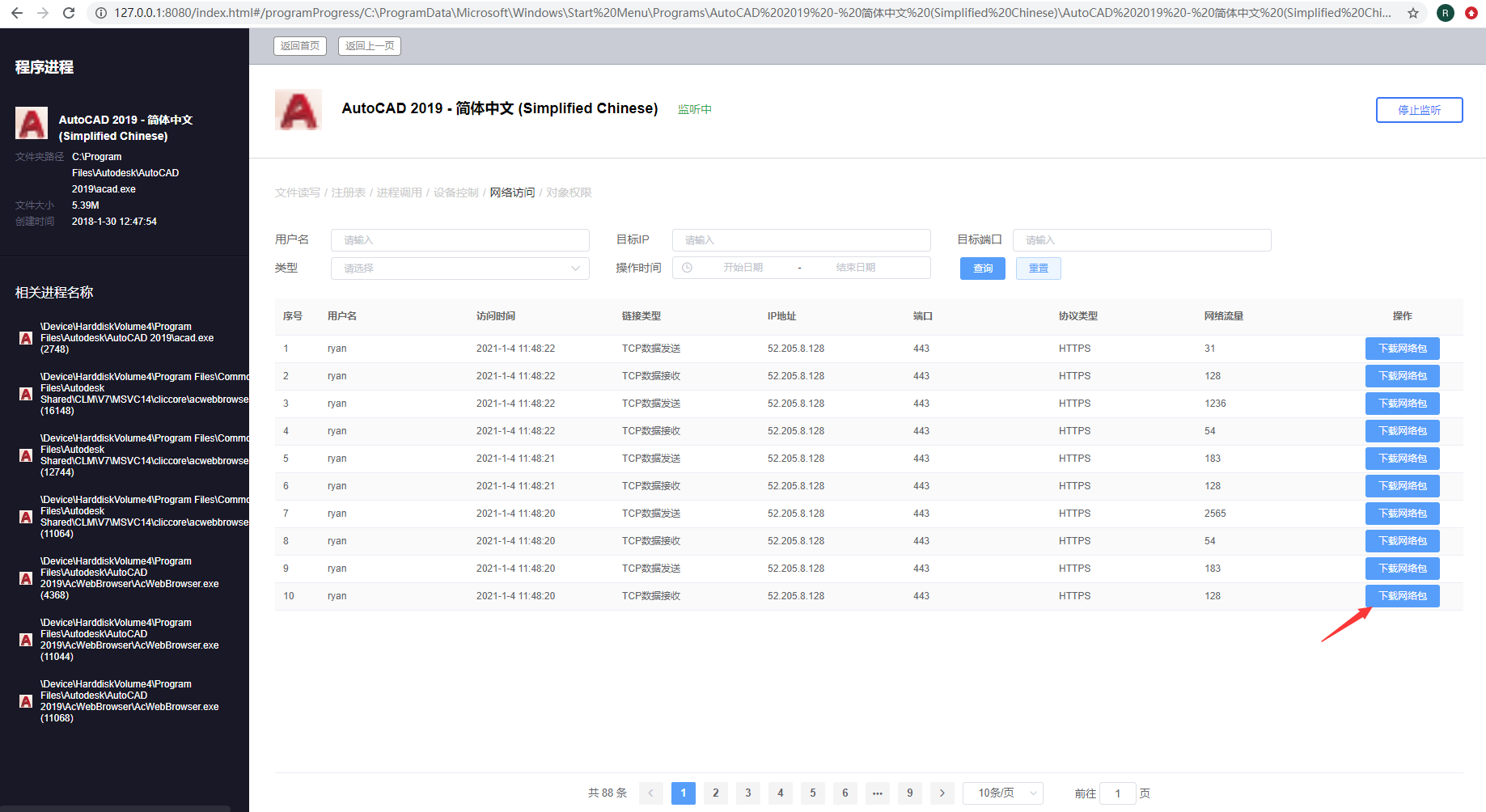


图6-8-3

（九）文件对象权限监听

1.进入监控详情，切换到文件对象权限监听栏目

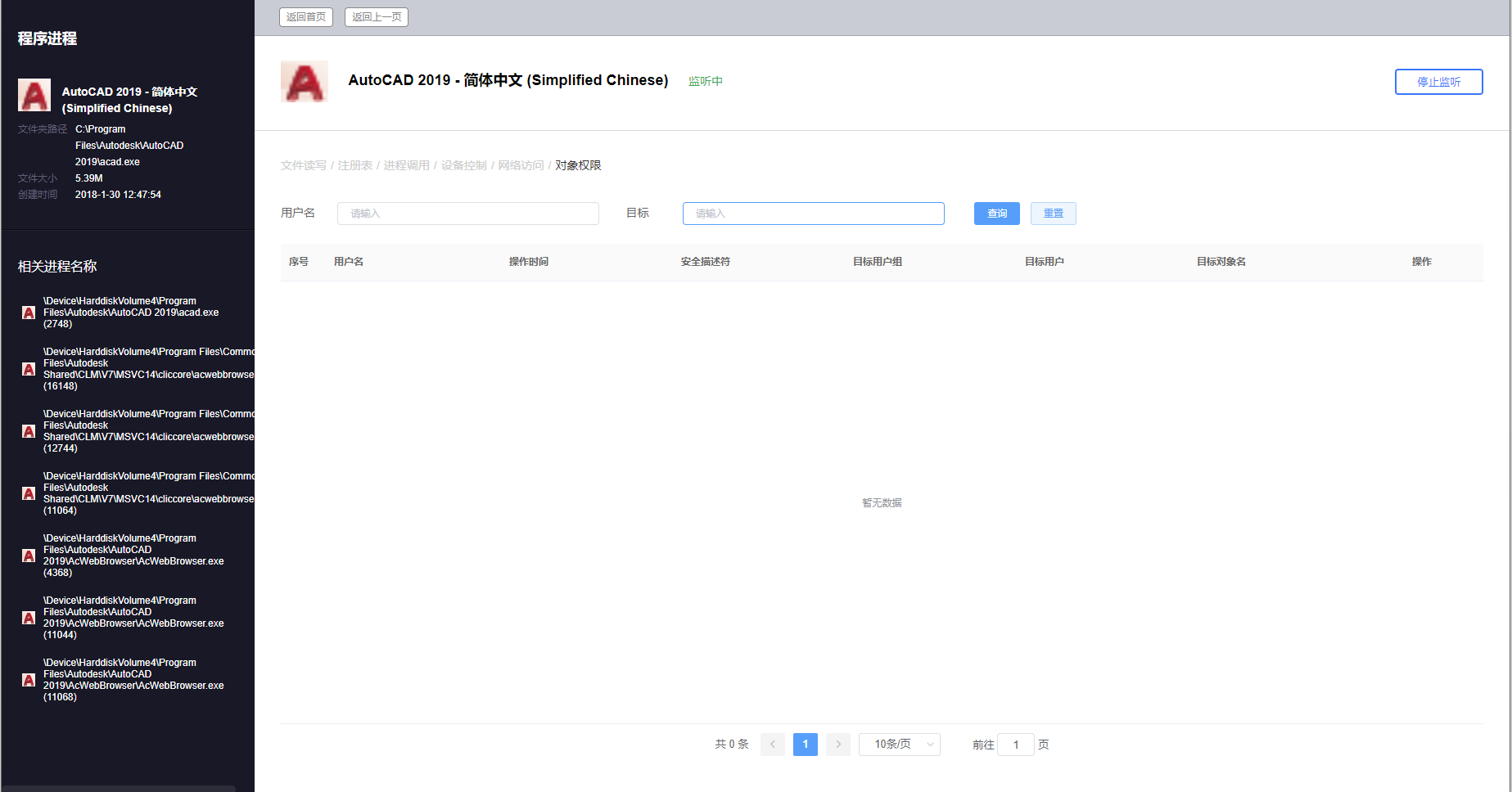


图6-9-1

2. 文件对象权限监听主要是监听软件调用了Linux下的文件所属用户变更(chown)和文件权限变更(chmod)等相关api。