《AppShark》软件操作手册

项目名称：涉诈 APP 智能识别分析系统

软件名称：《AppShark》

当前版本：V.1.1.1

最后修改时间：2024 年 8 月 20 日

修订记录

修订版本号	修订日期	修订描述	作者
V.1.0.0	2024/06/18	初步完成 GUI，初步实现静态解析和动态解析	Fiiish
V.1.0.1	2024/06/29	完善图像分析模型	Fiiish
V.1.0.2	2024/07/09	完善源码分析模型	Fiiish
V.1.0.3	2024/07/18	完善优化形成成品	Fiiish
V.1.1.0	2024/08/16	添加 AI 语言模型	Fiiish
V.1.1.1	2024/08/20	第二次完善优化	Fiiish

目录

1. 引言

1.1. 目的

本手册是为了向用户介绍《AppShark》软件的功能和使用方法，帮助用户快速了解和掌握这款应用软件的使用方法，以便更好地享受我们的服务，或在必要时作为参考。

本手册预期的读者是反诈专业从业者，以及应用程序管理员和系统开发测试人员。

1.2. 背景

随着数字化转型的加速发展，犯罪形态也发生了显著变化。在诸多诈骗类型中，电信网络诈骗犯罪尤为普遍。这种犯罪从传统的电话、短信诈骗，逐步转向利用 APP 等网络工具进行，成为当前发展增速最快、涉及范围最广的刑事犯罪类型。各种诈骗 APP 层出不穷，严重威胁公民的安全和财产。

在这样的背景下，开发一个“涉诈 APP 智能识别分析系统”显得尤为重要。该系统旨在利用人工智能技术，提升对电信网络诈骗软件的甄别能力。通过智能分析，系统能够识别和预警潜在的涉诈 APP，为用户提供实时的保护。

1.3. 项目目标

1. 系统支持完全离线分析模式。
2. 系统支持特征分析，源码分析，图像分析等多种分析模块。
3. 为了能够使得用户能够方便的查看分析结果，将采取分析报告的形式呈现，支持用户随时查看。
4. 在用户使用过程中，尽量使操作逻辑简单，可视化效果好，底层分析逻辑对用户透明。
5. 系统支持多线程并发执行，能将用户主机资源充分利用，使得吞吐量最大化。

1.4. 名词定义

本系统（本系统、本项目、AppShark）：代表此项目最终的成品。

多模态：多种异构模态数据（例如图像，文本数据）协同推理的形式。

APK： Android 应用程序包

多线程：线程化的程序将工作拆分到多个软件线程，而不是将大量工作交给单个内核。这些线程由不同的 CPU 内核并行处理，以节省时间。

涉诈 APP：我们将赌博，诈骗，色情，黑色产业这四类 APP 均归类为涉诈 APP。并将这四种定义为涉诈类型。

2. 项目概述

2.1. 产品介绍

本项目主要分成五大模块，分别是：APK 采集，静态分析，动态分析，黑白名单管理，AI Chat。经过实验验证与调查，我们的软件具有良好的用户使用体验以及较高的识别准确率。

2.2. 产品功能

2.2.1 功能性

1. 提供根据链接和二维码自动下载 apk 功能。
2. 提供手动上传 apk 功能。
3. 实现对 apk 文件的特征分析，URL 分析，源码分析，图像分析四大分析功能。
4. 实现综合分析报告的生成及保存，用户可以随时查看。
5. 实现黑白名单的增删改查和自动化过滤功能。
6. 实现 apk 文件的动态分析功能，包括通联地址抓包和图片截取。
7. 实现系统分析进度实时显示功能。
8. 实现分析结果置信度判别及自动化测试功能。
9. 实现 ai 对话功能。
10. 系统支持应用运行时动态分析，通过插桩，抓取网络流量等方式，对应用的运行时行为进行实时分析

2.2.2 非功能性

1. 算法推理速度快, 推理准确性高。
2. 网页界面美观、清爽、响应速度快、易用。
3. 实现功能丰富，对用户友好。

2.3. 产品特性

1. 对于输入的网址，可以自动地递归下载 apk 文件进行分析。
2. 在代码分析部分，我们使用了自己训练的模型，对题目中的数据具有更高的准确率。
3. 我们对 apk 文件采取了图像分析的方式去判断它的涉诈类别，能够更准确地定位该 apk 文件的涉诈类别。
4. 我们的分析步骤之间耦合度低，不同模块之间，以及对不同 apk 的分析过程均可并发执行，有较高的吞吐量。
5. 我们为每位用户提供安卓虚拟环境，保证用户隐私安全的同时允许用户运行可能涉诈的 APP。
6. 在 APP 运行过程中我们将实时捕捉应用产生的网络流量，抓取应用界面截图，劫持应用运行时函数调用，结合静态分析的结果综合分析 APP 是否涉诈。

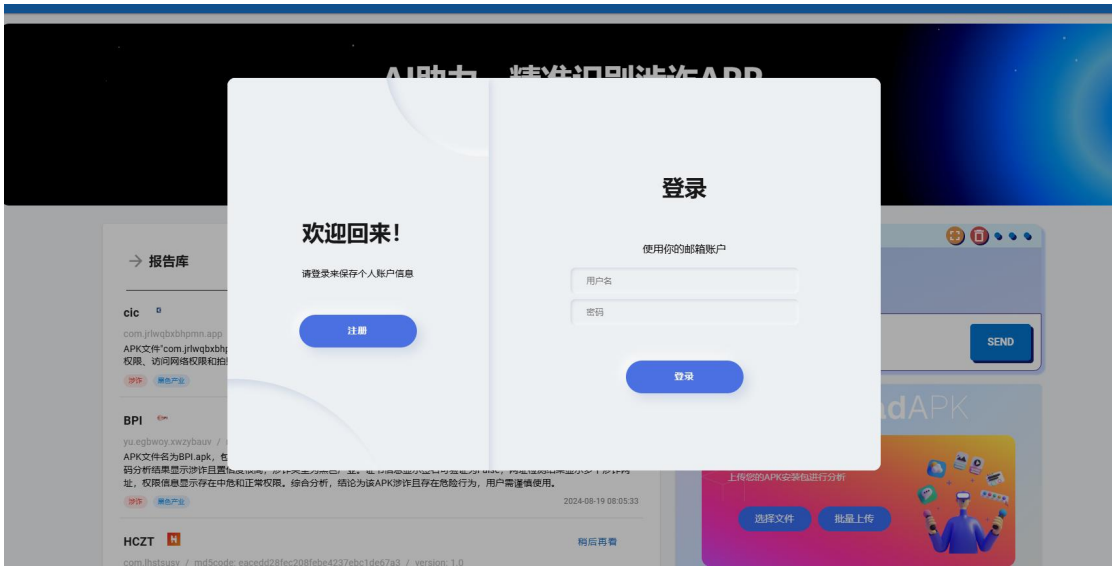
3. 操作说明

3.1. 首页

3.1.1 报告库

首页展示了所有已完成分析的 apk 文件的基本信息，点击‘时间排序’，‘标题排序’可对报告列表进行排序，上方的搜索框则用于对报告进行筛选。

3.1.2 登录



点击登录按钮弹出对话框，输入账号密码即可完成登录。

3.1.3AI 对话

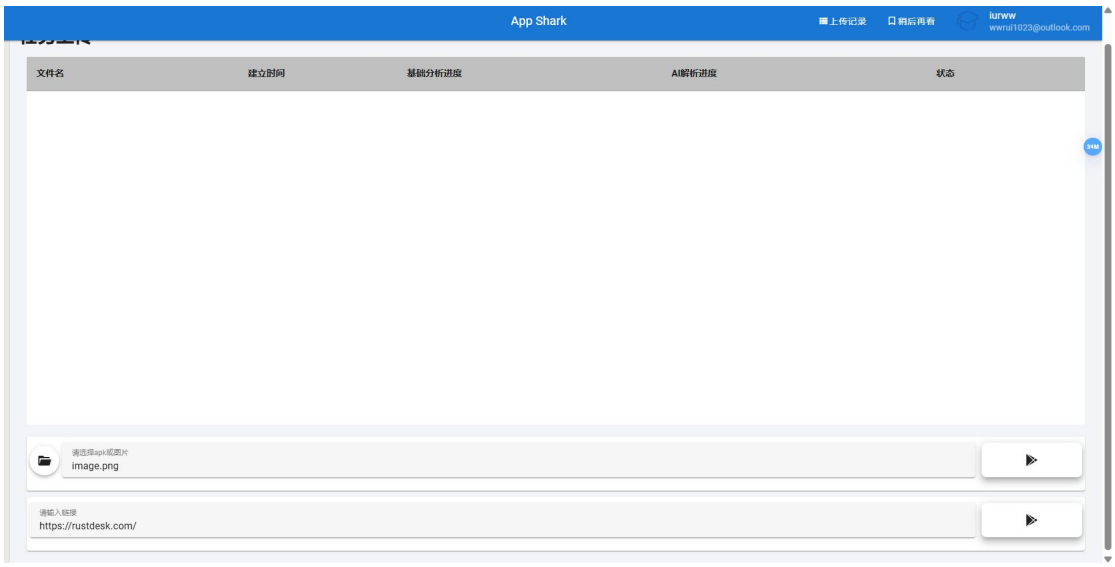
主页右侧的对话框使用千问大模型实现了 ai 对话功能，可以询问它涉诈 apk 的相关问题。

3.2. 任务上传

3.2.1 上传方式

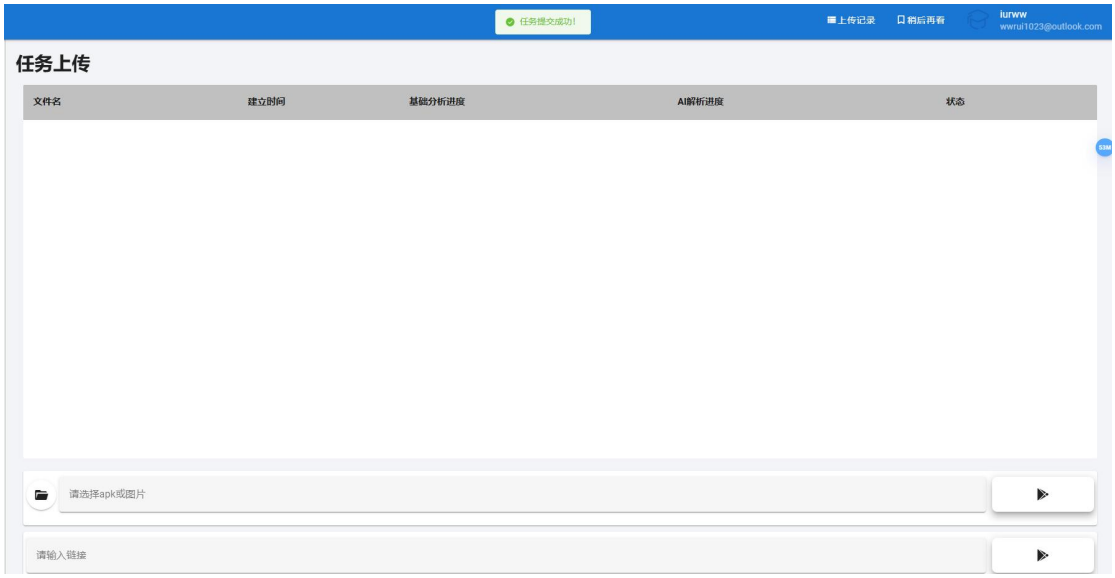
主页右下角的组件用于进行 apk 的上传。

点击侧边栏的任务上传，同样可以进入任务上传界面。

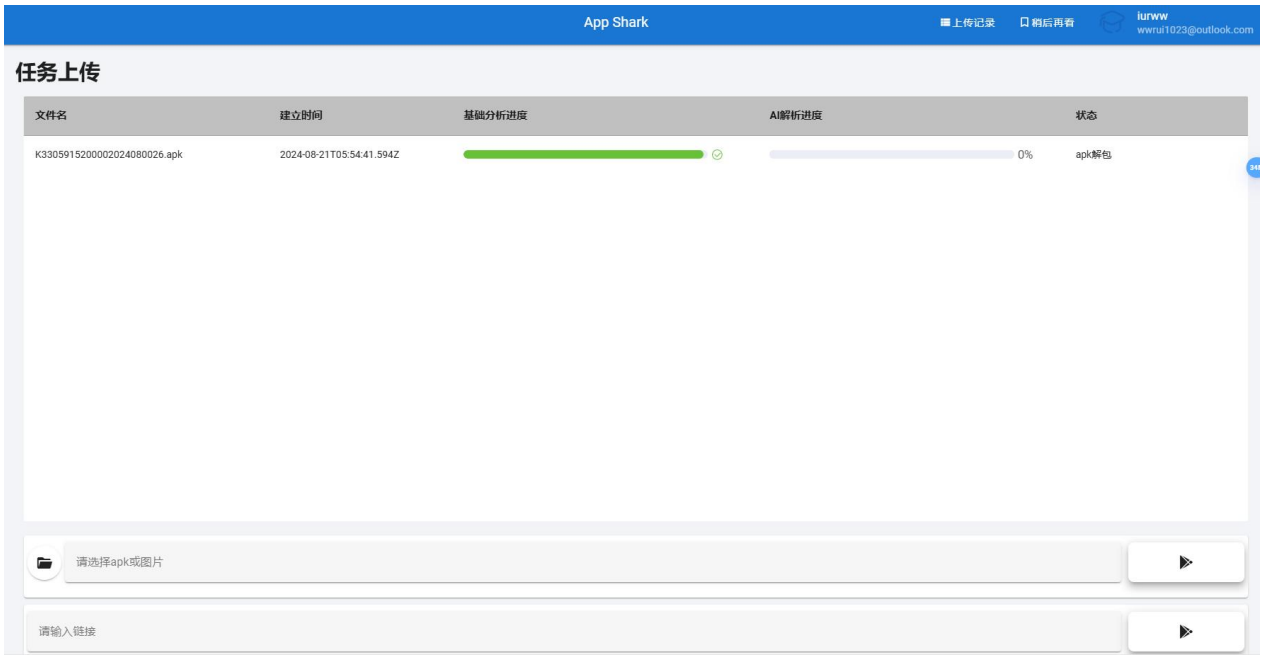


除 apk 文件外，系统还支持输入链接和二维码。对于链接，系统会调取爬虫程序使用 BFS 爬取 apk 的下载链接，下载下来进行 apk 分析，而对于二维码，系统则会先将其转化为链接，然后同理进行分析。

3.2.1 上传进度



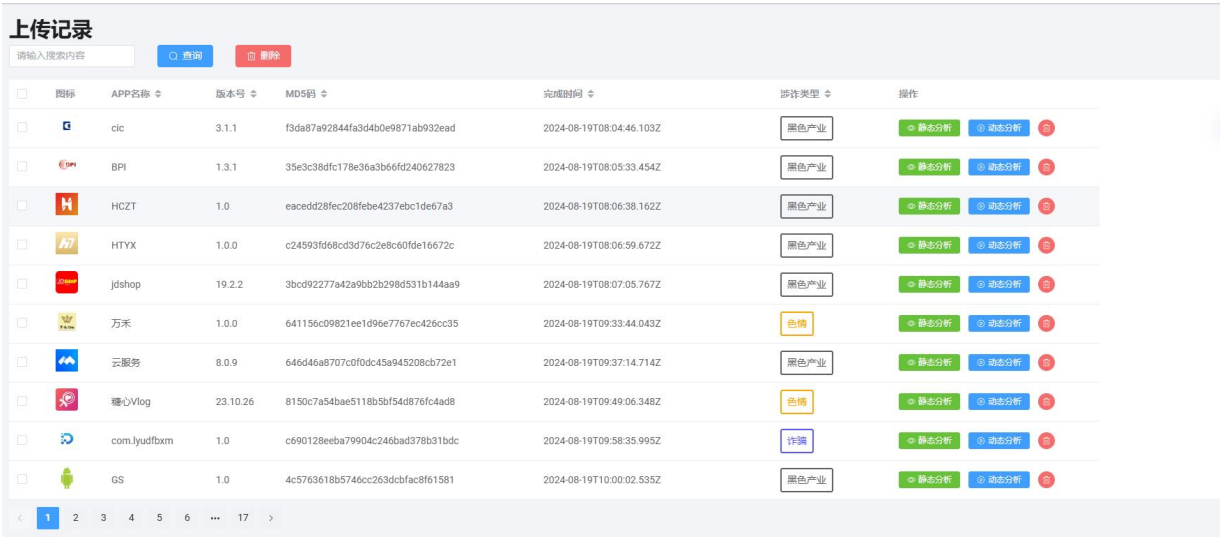
上传完 apk 后，需等待一段时间，出现‘任务提交成功‘的提示，则表明 apk 以上传至服务器，开始进行静态分析。



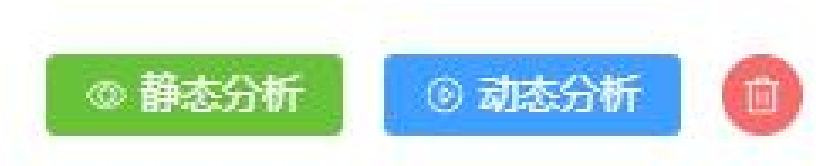
任务上传界面提供任务进度的可视化，其中基础分析指对 apk 进行的特征分析，如基本信息，证书，权限等。而 AI 分析则指使用了 AI 功能的分析过程，如 URL 分析，源码分析，图片分析，以及最后的分析报告生成（使用千问大模型润色）。具体状态则显示在右侧。已完成的任务会自动从任务列表中删除。

3.3. 完成列表

在登录成功后，顶边栏会出现"上传记录"的按钮，点击即可查看 apk 分析完成列表。



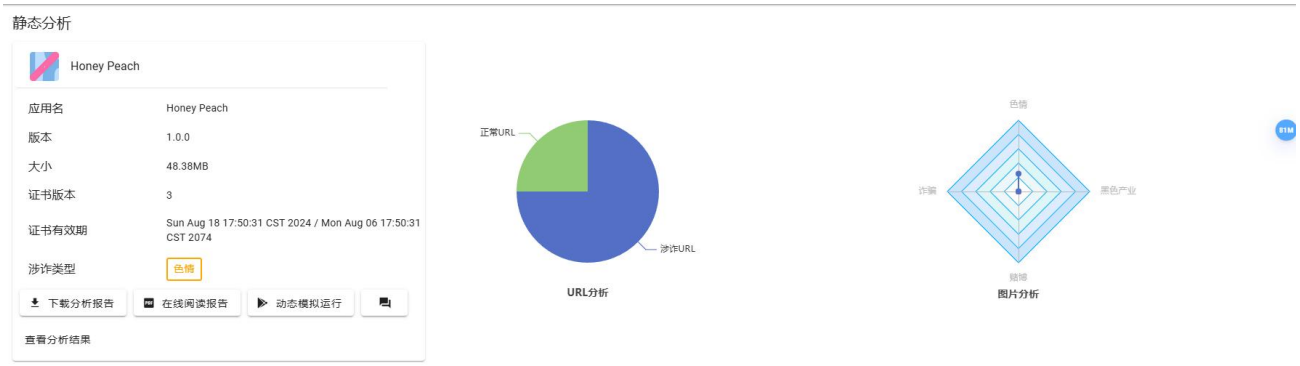
完成列表包括图标，包名，版本，md5 码，完成时间，涉诈类型等基本信息，其中涉诈类型会做出颜色上的区分。左上角的搜索栏可以对完成列表进行筛选。



右侧三个按钮的功能分别为：查看静态分析结果，进行动态分析，以及删除该条记录。

3.4. 静态分析

3.4.1 基本信息



静态分析界面首先展示了 apk 的基本信息，包括应用名，大小，证书，涉诈类型等。中间的饼图是涉诈 URL 和正常 URL 的占比展示。右侧的四维图则展示

了四种涉诈类型的图片占比。

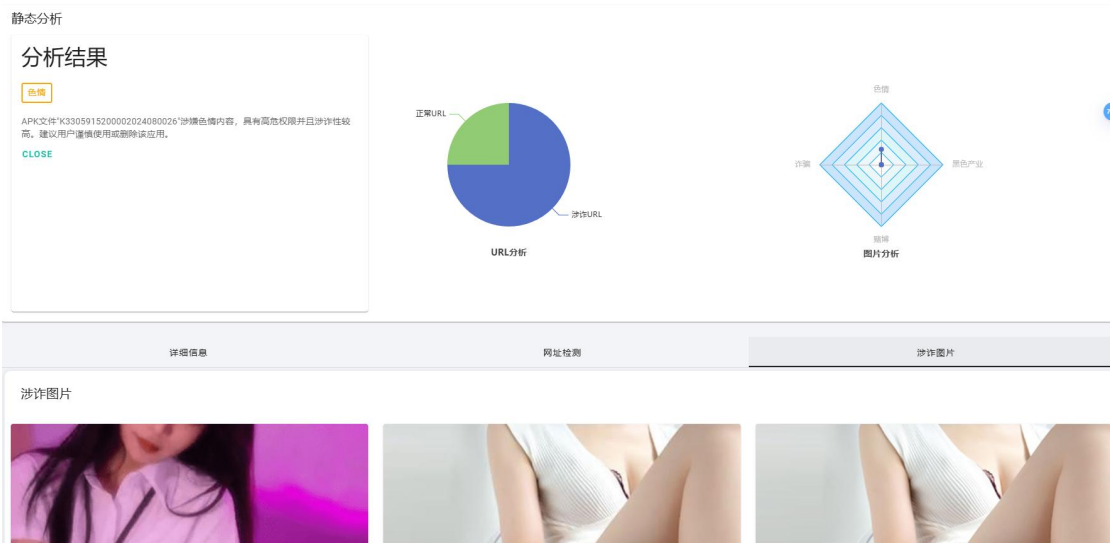
3.4.2 详细信息

在基本信息的下方，可以查看 apk 的详细信息，网址检测，以及涉诈图片信息。详细信息部分，除基本信息外，还包括 apk 的权限信息，其中权限等级 0,1,2 代表了该权限的危险等级：0 表示正常，1 表示中危，2 则为高危。

3.4.3 网址检测

在 URL 检测界面，提供了该 apk 文件中后台通联地址的 ip，域名，所在地，是否涉诈等信息。分析结果由 URLNet 模型得到。

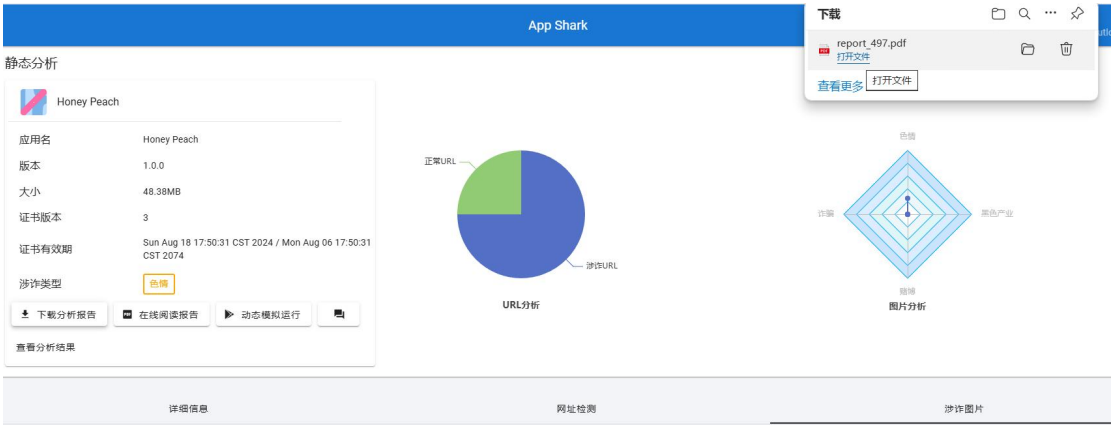
3.4.4 涉诈图片



涉诈图片部分展示了从该 apk 中提取到的所有涉诈图片以及图片的类型。图片的提取工作由 CLIP 模型完成。点击查看分析结果按钮可查看分析结果，分析结果由大模型生成。

3.5. 分析报告

3.5.1 报告下载



点击下载分析报告按钮，系统会自动下载该 apk 文件的分析报告。

3.5.2 报告内容

涉诈APK分析报告-K330591520000202408002 6

目录

APK信息

属性	值
图标	
文件名	K330591520000202408002 6.apk
文件大小	48.38MB
应用名称	Honey Peach
包名	com.example.lqqzxjy
版本号	1.0.0
MD5码	3e219bfd79bf59ea5aadefd0a35b7cb5
签名可验证	True
代码分析结果	涉诈
置信度	0.92228826548853
是否涉诈	True
涉诈类型	**色情**
分析完成时间	2024-08-21 08:25:54.005547+00:00

证书信息

属性	值
序列号	`49a95e76`
版本	`3`
起始时间	`Sun Aug 18 17:50:31 CST 2024`
终止时间	`Mon Aug 06 17:50:31 CST 2074`
SHA1	`24:90:C8:3A:DE:57:49:2A:04:21:A6:62:86:AD:C8:41:07:AB:20:B2`
SHA256	`D0:FC:15:78:8A:3C:BC:6C:F9:3B:5B:F7:4B:16:A9:F9:55:95:A6:06:CB:3A:3E:7D:8F:6E:7F:A1:E5:7E:62:B3`
签名算法	`SHA512withRSA`
公钥算法	`4096-bit RSA key`

网址检测

URL	IP地址	域名	国家	城市	区域	是否涉诈
https://plus.google.com/	104.244.43.35	google.com	United States	San Francisco	California	True
http://schemas.android.com/	None	android.com	None	None	None	True
http://ns.adobe.com/	None	adobe.com	None	None	None	True
https://developer.android.com/	142.251.211.238	android.com	United States	Gaithersburg	Maryland	False

权限信息

权限	中文名	说明	危险等级
android.permission.READ_SMS	读取短信或彩信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。	高危
android.permission.REORDER_TASKS	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。	中危
android.permission.ACCESS_FINE_LOCATION	精准的(GPS)位置	访问精准的位置源，例如手机上的全球定位系统(如果有)。恶意应用程序可能会	中危

权限	中文名	说明	危险等级
		借此确定您所处的位置，并可能消耗额外的电池电量。	
android.permission.READ_PHONE_STATE	读取手机状态和身份	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。	中危
android.permission.READ_CONTACTS	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。	中危
android.permission.ACCESS_NETWORK_STATE	查看网络状态	允许应用程序查看所有网络的状态。	正常
android.permission.INTERNET	访问网络	允许程序访问网络.	正常
android.permission.WRITE_EXTERNAL_STORAGE	修改/删除SD卡中的内容	允许应用程序写入SD卡。	正常

涉诈图片

文件路径	涉诈类别	涉诈图片
picture_analyze/色情/2.png	色情	

picture_analyze/色情/4.png	色情	

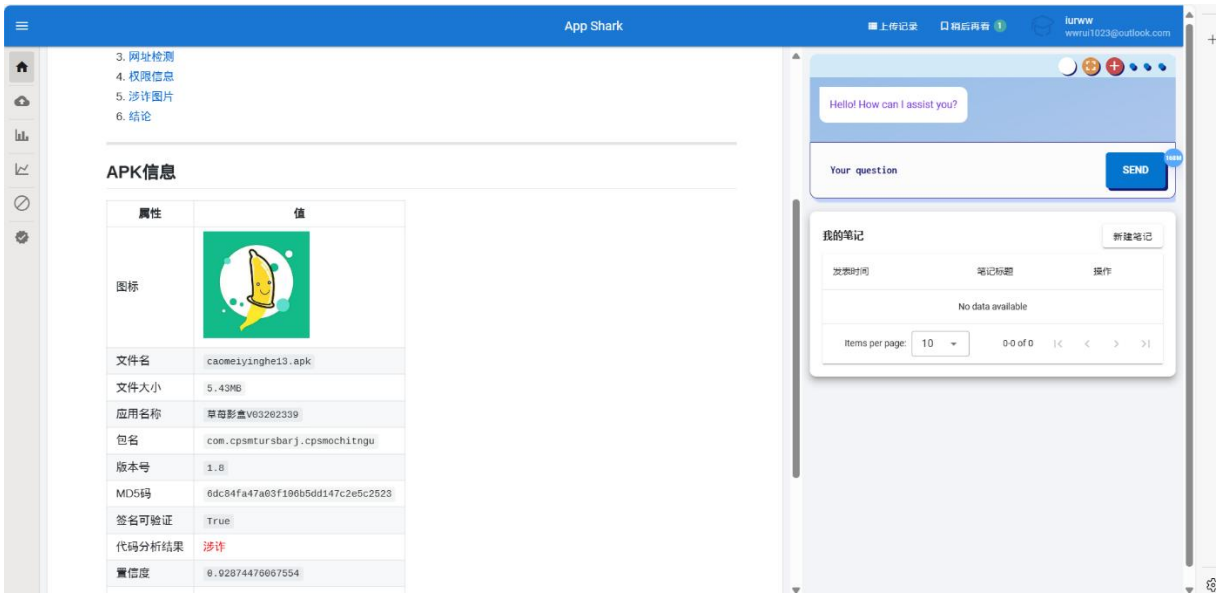
文件路径	涉诈类别	涉诈图片
picture_analyze/色情/8.png	色情	

结论

APK文件"K330591520000202408026"涉嫌色情内容，具有高危权限并且涉诈性较高。建议用户谨慎使用或删除该应用。

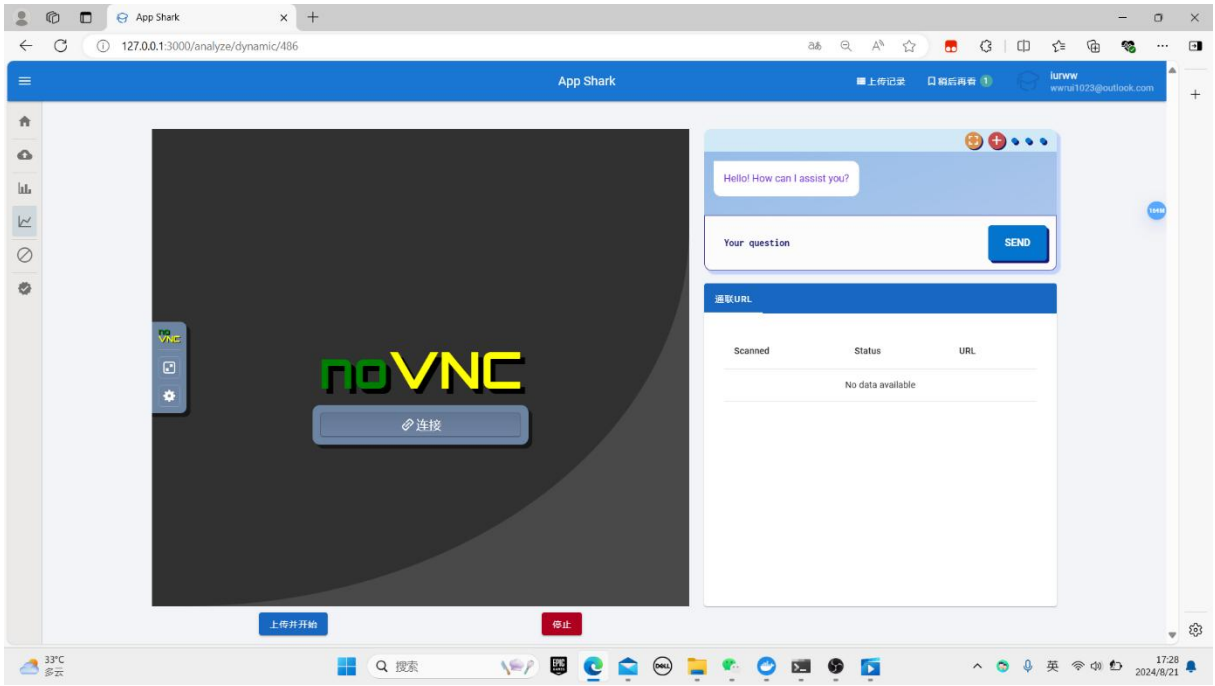
Apk 的分析报告格式如上图所示，包括 apk 信息，证书信息，权限信息，网址检测，涉诈图片以及结论六个部分。其中 apk 信息还额外包括源码分析的结果以及置信度。

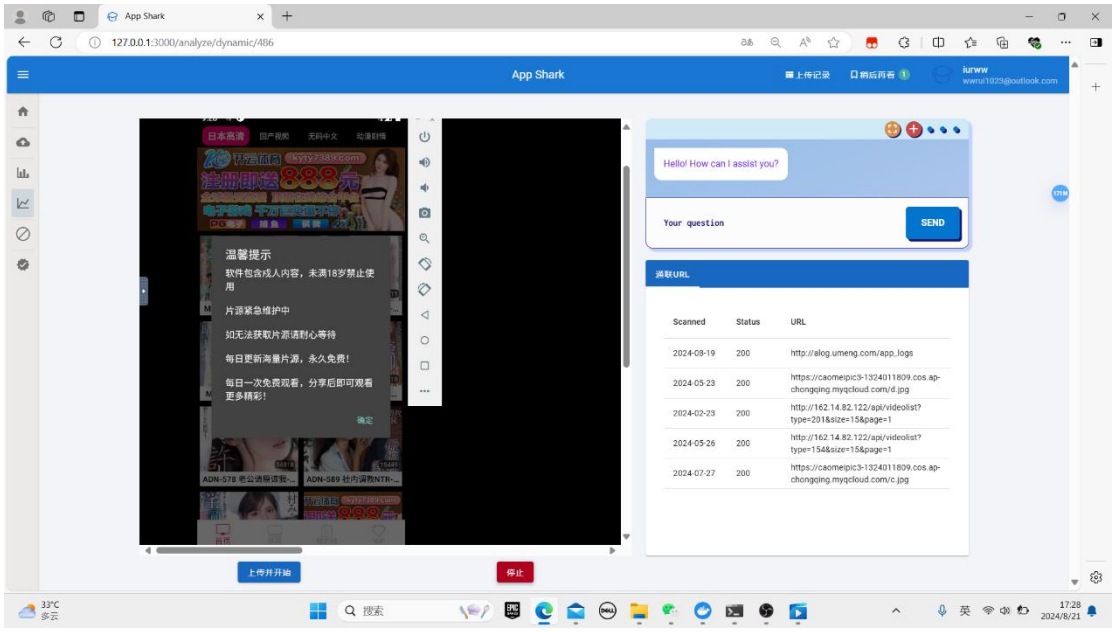
3.5.3 报告阅读



点击在线阅读报告即可在网页端打开报告内容。

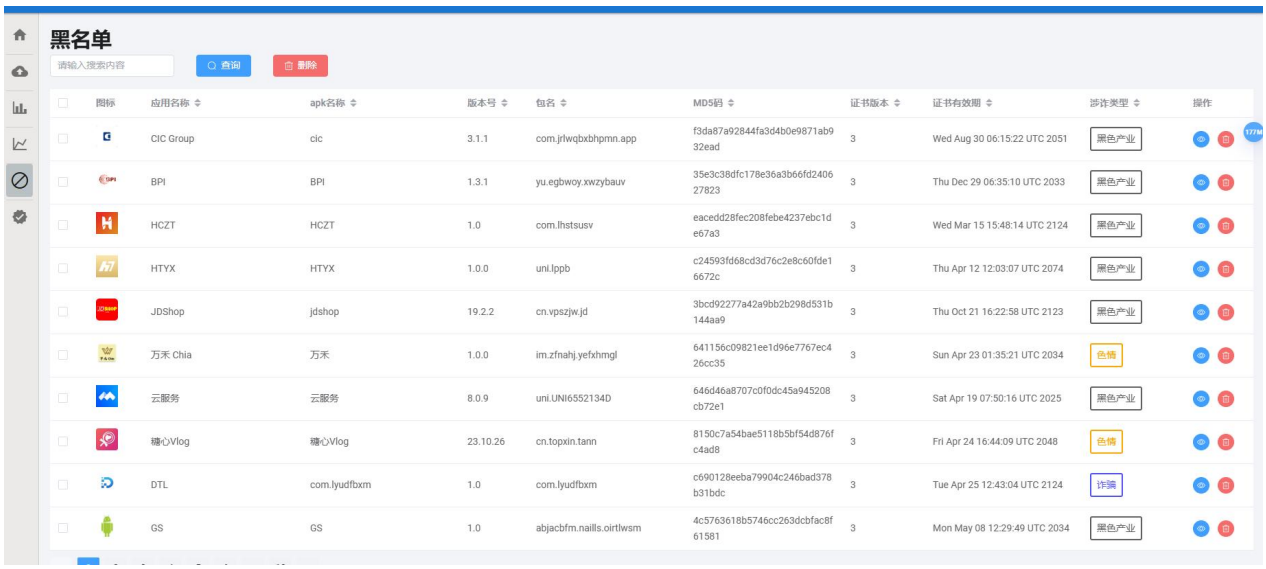
3.6. 动态分析

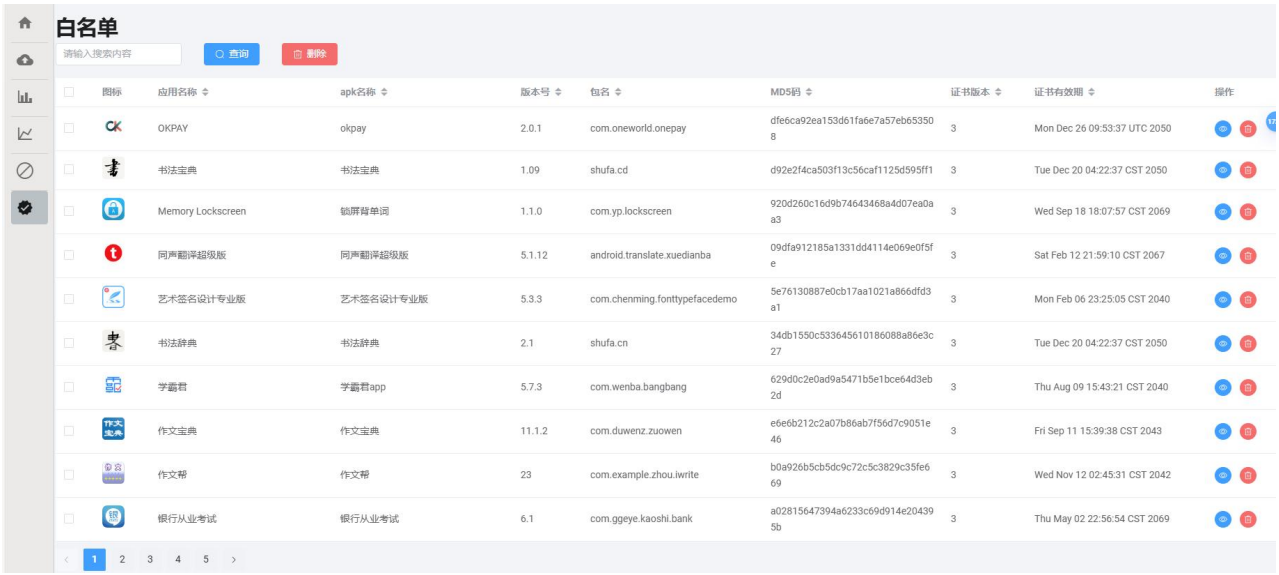




在 apk 详情页点击动态模拟运行或在已完成列表点击动态分析即可进入动态分析界面。系统会根据 apk 的 id 向后台获取 apk 文件，并在安卓 sdk 中自动安装并打开，模拟运行，同时对后台进行抓包，获取通联地址的解析。

3.7. 黑白名单





点击黑/白名单按钮即可查看黑白名单，黑白名单包括所有分析完成的 apk 记录，以是否涉诈作为区分。点击条目可以查看 APK 的详情页。