奇安信
新一代网络安全领军者

奇安信洞鉴

上海盘石计算机司法鉴定所
021-52658848（上海）
上海市闵行区合川路 2555 号科技绿洲三期五 -3 号楼 4 层

北京网神洞鉴司法鉴定所
010-56509288 （北京）
北京市西城区西直门外南路 26 号院 1 号 - 奇安信安全中心

陕西洞鉴云侦司法鉴定所
029-86196688（西安）
陕西省西安市经济技术开发区凤城二路 1 幢经发大厦 B 座

案例中所有图片均为虚拟数据，不涉及任何客户隐私

奇安信洞鉴公众号

盘古石取证公众号

奇安信
新一代网络安全领军者

奇安信洞鉴

www.qianxin.com

网络黑灰产治理案例手册

作弊外挂 | 知产侵权 | 数据泄露 | 网络水军 | 薅羊毛

目录 CONTENTS

PREFACE

前言

近年来，网络黑灰产问题对各大行业，尤其是电商、媒体和游戏行业构成了极大的威胁。这些非法活动不仅严重干扰市场秩序，甚至对企业的数据安全、财务安全构成了巨大的隐患。所谓网络“黑灰产”，是指利用网络技术进行非法或处于灰色地带的商业活动。黑产（黑色产业）涉及明确违法行为，如电信诈骗、木马病毒等；而灰产（灰色产业）则游走在法律边缘，为黑产提供辅助，如恶意营销、刷量作弊等。

数据显示，2024 年上半年黑灰产相关从业人员已超过 427 万【1】，恶意流量、虚假交易、金融欺诈等事件给企业带来了无法估量的损失。针对日益复杂的黑灰产犯罪手段，奇安信洞鉴凭借在电子数据司法鉴定领域的专业技术积累，协助公安机关与企业成功侦破了大量黑灰产案件，尤其在作弊外挂、数据泄露、网络水军等领域，具备一系列成熟的鉴定技术和解决方案。

本手册旨在为电商、媒体、游戏行业提供实用的黑灰产防控方案，通过对这些行业的黑灰产现状进行深入剖析，提出有针对性的解决策略。我们将通过详细的场景分析、取证思路以及典型案例，帮助企业更好地理解黑灰产的运作模式，掌握有效的应对方法，助力企业构建全方位的安全防护体系。

【1】*澎湃新闻 . (2024 年 10 月 26 日). 2024 年上半年互联网黑灰产研究报告 .* 访问链接：https://www.thepaper.cn/newsDetail_forward_28115796

现状趋势

1. 威胁现状

近年来，黑灰产活动对多个行业，尤其是电商、媒体和游戏行业构成了极大的威胁。随着技术的发展，特别是自动化工具和人工智能的应用，这些非法活动变得更加复杂和隐蔽，涉及虚假交易、恶意营销、数据泄露等多个方面。

游戏行业

	上游	中游	下游
外挂	外挂作者	交易平台	代理商 玩家
私服	私服创建者	运营商	
虚拟物品交易	养号商	交易平台	
盗号	黑客	交易平台	

游戏黑灰产市场涵盖了外挂、私服、虚拟货币交易、账号盗取、代练等多个领域，呈现出规模化、技术化和创新化的特征，并且在传播渠道和手段上不断发展。以下是这些活动的具体分析：

外挂：外挂市场规模已经超过 20 亿元【2】，且外挂种类繁多，包括自动瞄准、瞬移等基本功能，甚至出现了更复杂的 AI 挂和自适应脚本，大大增加了游戏公司监控的难度。

私服：私服运营者未经授权使用官方游戏代码和数据，搭建出未经许可的游戏服务器。通过高爆率、定制奖励等方式，私服吸引大量玩家充值和消费。米哈游等公司已对私服运营者发起多次诉讼，但私服的分散性和隐蔽性增加了追踪和执法的难度。

虚拟物品交易：黑产通过外挂刷金和批量账号创建获取虚拟货币，再在第三方交易平台上低价出售，破坏了游戏内经济平衡，削弱了厂商对虚拟经济的控制。

盗号：黑产团伙通过钓鱼链接、木马程序、伪造登录页面等传统手段窃取玩家账号信息，同时结合 AI 换脸等新技术伪造身份，绕过面部识别等多重验证，将被盗的高价值账号转售牟利。

【2】*人民网 . (2020 年 9 月 2 日). 作弊方式层出不穷 游戏外挂黑产年销售已超 20 亿元 .* 访问链接：http://finance.people.com.cn/n1/2020/0902/c1004-31845505.html

媒体行业

	上游	中游	下游
盗版内容	内容抓取者 爬虫软件	盗版内容网站 广告变现	用户 广告联盟
流量造假	代理 IP 卡商 群控软件	刷单团伙 流量代理	品牌商 自媒体
恶意引流	引流内容生成 黑客 钓鱼工具	分发平台 推广中介	终端用户

在媒体行业中，黑灰产活动涵盖了虚假流量、恶意引流、盗版内容分发等领域，以下是这些活动的具体分析：

盗版内容分发：黑灰产通过文件共享平台和 P2P 网络非法分发电影、电视剧、音乐、电子书等数字内容，吸引用户访问，嵌入广告以获利。网络文学是受盗版打击较为严重的领域，过去五年因盗版损失超过 300 亿元，约八成原创作者受到其侵害【3】。

虚假流量：虚假流量市场规模持续扩大，2023 年，全球浪费在虚假流量上的数字广告支出成本将达到 842 亿美元【4】。黑产利用机器人、代理 IP 等手段生成大量虚假流量，使广告主的预算被浪费，同时影响平台的数据分析和广告效果。

恶意引流：黑灰产通过诱导性广告和恶意链接引导用户至危险网站或恶意软件下载页面。这些链接通常隐藏在社交媒体、搜索引擎广告或第三方网站中，吸引用户点击。恶意引流的手段复杂多样，用户可能在不知情的情况下泄露个人信息或被恶意软件感染，造成数据安全隐患。

电商行业

	上游	中游	下游
刷单炒信	卡商 刷手资源 虚假账号	刷单团队 任务发布 接码平台	商家
薅羊毛	优惠券漏洞挖掘 虚假账号注册 身份信息供应商	羊头组织 自动化工具	交易平台
黄牛代下	大黄牛 （设计代下单方案和佣金结构）	代下单组织 （QQ群、微信群） 抢购外挂	代下单成员 二级市场转售

【3】*新浪财经 . (2022 年 5 月 30 日). 网文大盗灰产江湖：专偷未完结小说，5 年掠走 300 多亿 .* 访问链接：https://finance.sina.com.cn/chanjing/gsnews/2022-05-30/doc-imizmscu4060043.shtml

【4】*中国广告网 . (2023 年 10 月 07 日). 一年损失 842 亿美元，广告也需要“反诈 APP”？ .* 访问链接：https://www.cnad.com/index.php?act=view&mod=article&titleId=339306

电商行业

在电商行业中，黑灰产活动涵盖了刷单炒信、优惠滥用（薅羊毛）、黄牛党等多个领域，这些活动对平台生态和消费者信任带来极大挑战。以下是这些活动的具体分析：

刷单炒信：刷单炒信行为指通过虚假交易、虚构好评等手段来提升商品或商家的信誉和排名，以达到增强竞争力或打击竞争对手的目的。刷单行为可以分为“正向刷单炒信”（提升销量、好评）和“反向刷单炒信”（虚构差评、降低对手评分）。

薅羊毛：利用平台的优惠券、返现、积分兑换等活动获利，通过多账号操作来重复领取优惠。最常见的手段包括仅退款、恶意退款、订单批量注册等，这些行为导致平台活动资源被滥用。

黄牛代下：通过大规模批量下单抢占平台的限时优惠或限量活动。通常由专业团队制定抢购方案，由代下单组织实施，再将获得的商品转售获利。此行为挤占了正常消费者的购物资源，破坏平台公平性。

2. 主要趋势

规模化运作

近年来，黑灰产已不再是个人或小团队的单打独斗，而是转向系统化、规模化的运作模式。黑灰产通过专业化的资源供给和自动化技术，极大提升了操作效率和攻击规模。具体表现为：

资源平台化

上游资源供应商（如手机卡商、代理 IP 商等）与中游服务平台（如接码平台、打码平台、发卡平台）紧密结合，形成了专业的供应链。这使得黑灰产在攻击中能按需调用大规模作恶资源，如虚假账号和代理 IP 等。

批量化攻击

黑灰产利用自动化工具、群控技术和云手机，执行大规模的批量攻击，减少成本并提高攻击效率。云手机技术的发展，使黑灰产无需购买大量实体设备，即可模拟真实用户行为进行批量操作，如账号注册和用户操作模拟。

精准化攻击

随着大数据和人工智能（AI）技术的广泛应用，黑灰产逐渐从广泛撒网式攻击转向更加精准的攻击模式。通过先进的数据分析和 AI 技术，黑灰产能够对企业、平台或用户进行详细画像，提升攻击的精准度。

个性化攻击

黑灰产利用 AI 扫描社交媒体和公开信息来制作更加定制化的攻击。例如，生成定制化的钓鱼邮件，通过社交工程引导特定受害者泄露信息。

自动化漏洞利用

AI 生成代码并优化恶意程序，使得攻击者可以更快、更高效地发现并利用软件漏洞，甚至降低了发动攻击的技术门槛。

移动化发展

随着智能手机和移动互联网的普及，移动设备成为黑灰产攻击和非法操作的重要平台。移动端不仅存储了大量个人数据，还成为金融交易的主要媒介，给黑灰产提供了大量新的攻击和欺诈机会。

恶意软件和数据窃取

2023 年，卡巴斯基观测到移动设备上的攻击次数激增 50%，达到 3380 万次，尤其以广告软件和银行木马为主【5】。这些恶意软件通过官方和非官方应用商店分发，利用假投资应用、恶意聊天软件等进行数据窃取，主要目标是获取用户的电话号码、银行账户等个人信息。

移动支付欺诈的增加

截至 2024 年第二季度，移动设备约占全球零售网站流量的 77%【6】，尤其是使用移动支付的用户数激增，使得黑灰产更多地瞄准这一渠道。

新技术应用

黑灰产在近几年得到了迅速的技术进化，尤其在人工智能（AI）、深度学习、区块链、物联网等新兴技术的推动下，犯罪手段变得更加复杂和高效。这些技术不仅帮助黑灰产绕过了传统的安全防御手段，还使其能够大规模、自动化地进行犯罪活动，增加了企业和个人面临的安全威胁。以下是黑灰产在新技术应用中的具体表现：

深度伪造

通过生成逼真的语音、视频和图像进行身份伪造和欺诈。例如，伪造企业高管的语音或视频，骗取敏感信息或进行资金转移。AI 生成的虚假身份能够绕过语音识别和视频认证系统。

加密货币

加密货币的匿名性和区块链的去中心化为黑灰产提供了资金洗钱和非法交易的便利。通过混币服务，黑灰产可将非法所得分散交易，隐藏资金来源。

【5】*卡巴斯基 . (2024 年 2 月 26 日). 2023 年移动设备攻击显著增加 .* 访问链接：https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023

【6】*Statista. (2024 年 10 月 4 日). 2024 年第二季度按设备分类的电子商务网站访问和订单比例 .* 访问链接：https://www.statista.com/statistics/568684/e-commerce-website-visit-and-orders-by-device/

IoT 僵尸网络

IoT 设备的安全性较低，使其成为大规模网络攻击的理想目标。黑灰产入侵物联网设备（如智能家居、工业设备等）形成僵尸网络，进行 DDoS 攻击、垃圾邮件发送或窃取数据。

3. 打击挑战

对抗性

技术升级快

黑灰产犯罪分子会迅速更新其技术手段，对抗监管和打击。例如，新的 App、加密通信、虚拟货币支付等新技术层出不穷，企业和公安机关的应对技术相对滞后，常常处于被动应对的局面。

策略调整快

犯罪者灵活调整手段，规避打击。例如，在刷单被打击后，黑灰产可能转向伪造评价、数据造假等，迫使企业和执法机关需要不断调整策略。

隐蔽性

伪装合法活动

犯罪行为隐藏在合法的流量、支付或推广中，尤其是在刷单、刷量等活动中，企业和公安机关难以分辨其真假。

跨平台操作

犯罪分子在不同平台（如社交媒体、支付平台和物流系统）之间切换操作，利用平台监管差异，进一步隐蔽其行为，增加追踪和封堵的难度。

匿名化手段

使用虚拟专用网络（VPN）、加密通讯软件、虚拟货币等技术，黑灰产犯罪者可以有效地隐藏身份和位置，增加公安机关追踪的难度。

复杂性

犯罪链条复杂

黑灰产通常包含多个环节，从信息窃取、技术支持、广告推广到支付结算，形成一个完整的犯罪生态链。打击单个环节并不能完全摧毁整个犯罪网络，犯罪活动会通过其他环节继续运作。

技术和取证复杂

黑灰产活动通常依赖加密通信、分布式交易和匿名网络（如 Tor 和暗网）等工具，增加了取证的难度。特别是在数据传输和交易环节，暗网和加密货币交易大幅增加了获取关键证据的复杂性。

跨域性

跨境犯罪加剧

黑灰产犯罪分子常利用境外服务器、外汇交易和跨国支付平台进行操作，将非法资金转移到境外，规避了国内的监管措施，增加了追踪难度。

司法协作困难

不同国家之间的法律体系、执法标准和取证程序存在差异，跨境合作通常需要经过复杂且冗长的司法协助程序，使得跨国追捕和取证工作繁琐，打击效率低。

您是否正在为平台上的虚假交易和恶意退款而苦恼？是否担心公司的核心数据可能泄露？在接下来的章节中，我们将为您揭示黑灰产的真面目，并提供行之有效的解决方案。

01

CHEATING AND PLUG-IN
作弊外挂

作弊外挂是指通过技术手段非法修改或干预软件、游戏等目标程序的正常运行，以获取不正当优势的工具或程序。这些外挂通过篡改程序数据、模拟用户行为、绕过程序保护机制等方式，帮助用户达到如自动化操作、增强功能、绕过限制等目的。外挂的使用破坏了软件或游戏的公平性与安全性，特别是在在线游戏、电子商务等竞争激烈的场景中，造成了严重的影响。

1. 常见场景

游戏外挂

游戏外挂通常用于帮助玩家获取游戏内的不公平优势，如自动瞄准、透视敌人位置、加速游戏角色等。

技术原理

1. 内存修改：外挂通过扫描和修改游戏内存中的数据，直接影响游戏角色的属性和状态，例如无限生命、子弹等。

2. 注入：外挂通过将恶意代码注入到游戏进程中，控制或劫持游戏的关键操作，使外挂程序与游戏程序同步运行，实现诸如自动瞄准、加速等功能。

3. 封包拦截：在网络游戏中，外挂截取并篡改服务器与客户端之间的数据包，伪造合法操作或改变游戏行为，比如虚假交易、虚增资源。

抢单外挂

抢单外挂广泛用于电商、打车、外卖等平台，目的是通过自动化手段提高用户在激烈竞争中的抢单成功率。

技术原理

1. 自动化脚本：抢单外挂通常采用自动化脚本模拟用户操作。通过频繁的页面刷新、快速点击操作，外挂在订单生成的瞬间自动抢单，速度远超人类手动操作。

2. 接口调用与伪造请求：外挂还可以通过直接调用平台的 API 接口，绕过正常用户界面交互流程，快速获取和提交抢单信息。这类外挂通过伪造客户端请求，将订单优先分配给自己，无需通过用户界面操作。

代打卡外挂

代打卡外挂常见于考勤打卡、学习软件打卡、会议签到等场景，主要目的是模拟用户身份验证或伪造出勤记录。这类外挂一般通过模拟身份认证操作或批量化处理考勤数据，达到欺骗系统的目的。

技术原理

1. 模拟硬件与远程操作：利用远程控制工具或虚拟设备，外挂可以通过模拟实际的打卡设备（如 GPS、NFC 卡）来伪造用户的打卡行为。例如，某员工可以在家远程操控办公室的打卡设备完成打卡，而并未实际到场。

2. 数据包伪造：通过拦截和篡改打卡系统与服务器之间的数据包，外挂可以伪造用户的地理位置信息或打卡时间，从而欺骗考勤系统。

2. 取证鉴定思路

1 外挂程序的获取

外挂程序的获取是鉴定工作的第一步。鉴定人员通常通过委托方提供的下载链接或存储介质中的 APK 文件来获取程序。在接收程序时，应详细记录下载链接或文件来源、接收时间以及程序完整性，以确保证据的合法性和可追溯性，为后续分析提供规范的依据。

2 固定目标程序

外挂的功能通常只针对特定版本的目标程序起作用，因此，确定目标程序的版本是关键。

版本确认：鉴定人员需要通过委托方提供的链接下载与外挂对应的目标程序版本。确保下载的程序版本与外挂程序能够匹配运行，以便复现外挂的功能。

记录固定过程：下载和安装目标程序的全过程需要通过录像进行记录，确保目标程序的来源清晰、固定过程透明，并为后续的外挂功能验证提供基础。

3 获取外挂卡密

许多外挂程序需要通过卡密（授权码）激活才能运行，因此获取有效的卡密是外挂鉴定前的必要步骤，卡密由委托方提供时，需保存相关提供记录和验证过程，以确保卡密的可追溯性和合法性。

鉴定人员应在卡密的有效期内完成外挂功能的测试和分析操作。如果卡密即将过期，应及时通知委托方以提供新的卡密或加快鉴定进程。

4 判断外挂的实现方式

在获取外挂和目标程序后，需判断外挂的具体实现方式，以选择合适的鉴定方法。

脚本类外挂：通过自动化脚本模拟用户操作，或利用手机的快捷指令，实现自动点击、快速刷新等功能。

破坏性/侵入性外挂：通过修改目标程序的代码、内存、数据包等方式，直接干预程序运行，实现功能增强或限制解除。

通过分析外挂程序的文件结构、运行依赖和权限要求等特征，确定其实现方式，以选择适当的鉴定工具和方法。

5 动态复现外挂功能

明确外挂的功能是关键，通过复现外挂对目标程序的影响，鉴定人员可清晰了解其工作原理和干预效果。

外挂运行前后对比：将目标程序分别在不运行外挂和运行外挂的情况下进行操作，对比其界面、功能和运行状态的差异。

6 静态分析外挂功能

对于一些不易动态复现的外挂功能，可以通过静态分析手段进行深入分析。

逆向工程与脱壳分析：逆向工程可以帮助鉴定人员了解外挂程序的内部结构、代码逻辑以及外挂实现的具体功能。外挂程序往往会采用一些特殊手段如加壳、代码混淆等方式阻止逆向工程，这时候需要先对外挂程序脱壳再进行逆向分析。

源码分析与比对：如果能够获取外挂程序的源码，应首先将源码与现有的外挂程序进行比对，以确定两者是否为同一程序。比对过程可以通过将源码编译成可执行程序，或者将现有程序反编译成代码后进行相似度比对。确认一致性后，再深入分析源码的代码逻辑，以明确程序的具体功能和运行机制。

注入行为分析：若无法直接对外挂进行逆向，可以通过分析外挂对目标程序的注入行为，了解其如何通过 DLL 注入、进程劫持等方式干预目标程序的运行。

7 生成鉴定意见书

在完成动态与静态分析后，所有的证据、分析过程、比对结果等需要严格整理并形成正式的鉴定意见书。

证据整理：需将外挂程序的分析过程中的关键数据、操作日志和功能验证结果进行整理，确保所有信息合法且可追溯。例如，详细记录外挂的获取方式、运行环境设置以及功能测试过程中的具体数据。这些信息将为后续的法律程序提供坚实的基础。

鉴定意见书生成：最终根据分析结果编写详细的司法鉴定意见书，内容包括外挂程序的获取、功能验证和技术分析等，确保每个步骤都有清晰的记录和证据支持，该意见书将作为案件审理的重要法律依据。

3. 典型案例

“注入类”游戏外挂案

动态调试揭露游戏外挂内存注入，创新破解无源码分析难题

2024 年，一款知名体育竞技类游戏因遭遇外挂攻击，导致游戏的公平性和玩家体验受到严重影响。奇安信洞鉴在无法获取源代码的情况下，创造性地采用动态调试与内存分析相结合的技术手段，通过反复勾选外挂功能，精准追踪到了外挂在游戏进程中的具体操作路径，揭示了外挂的注入方式和具体操作，为案件的侦破提供了关键证据支持。

案件背景

2024 年 6 月，一款知名体育竞技类游戏遭遇外挂攻击，外挂使用者能够通过自动盖帽、自动抢篮板、全场必中等功能在游戏中取得不正当优势，极大地影响了其他玩家的游戏体验。经过公司内部初步排查，发现外挂程序能够绕过游戏的安全防护措施，直接注入游戏进程，实现非法操作。

由于外挂程序高度隐蔽，且无法获取其源代码，传统的鉴定和防护手段难以奏效。为揭示外挂的技术原理及其对游戏系统的破坏方式，警方委托奇安信洞鉴团队对外挂程序进行全面的司法鉴定。此次鉴定旨在深入分析外挂的具体运作机制，为案件侦破提供可靠的技术支撑，并为游戏公司的后续防护措施提供科学依据。

洞鉴解决方案

1. 外挂功能复现

鉴定人员在虚拟机中搭建了与真实游戏环境一致的测试环境，安装并运行了游戏客户端。通过实际测试外挂程序的各项功能，验证了“全自动盖帽”、“全自动篮板”、“全场必中”等功能的有效性，确认该外挂程序能够通过自动操作严重破坏游戏的公平性。

2. 内存调试定位外挂注入点

为了揭示外挂的工作原理，鉴定人员使用工具对外挂程序进行内存调试。通过多次勾选“F1 全场必中”功能，成功定位到对应的内存地址“1FE55BDA”。进一步调试发现，外挂程序通过修改该地址的指令，将“add cs:[eax], al”指令改为“sub eax,00000000”，从而篡改了游戏命中逻辑，实现百发百中的作弊效果。

3. 功能验证与证据固定

在验证了外挂程序的所有功能后，鉴定人员详细记录了外挂程序在“全自动盖帽”、“全自动篮板”、“全场必中”等功能下对游戏内存的修改过程，将外挂程序对游戏进程内存数据的具体修改步骤和变化过程完整保存，并将所有分析数据和录像文件保存在证据光盘中，确保鉴定结果的完整性和证据的有效性。

客户价值

01 / 维护游戏公正环境

通过对外挂程序的深入分析和精确定位，帮助游戏公司有效识别并打击了相关作弊行为，阻止了外挂在玩家中进一步扩散，有效恢复了游戏的公平竞争环境，保障了玩家的正当权益和游戏体验。

02 / 提供完整证据链

运用动态调试与内存分析相结合的方法，精确还原了外挂程序的所有非法操作流程，并详细记录了内存数据变化和程序功能实现的具体证据，为执法机关提供了确凿的法律证据，支持游戏公司在法律层面对外挂制作者和使用者进行追责。

03 / 优化游戏防护策略

基于对外挂手段的深入理解，我们为游戏公司提出了系统防护优化建议，帮助公司建立更加完善的安全防护体系，预防未来类似问题的发生，提升整体安全防护能力。

骑手抢单外挂案

抢单也要开外挂！科技揭露非法抢单软件运作机制

近年来，某知名本地生活服务提供商旗下骑手众包平台涌现了大量非法抢单软件，这些非法抢单软件利用自动化功能破坏了平台的公平性，影响了正常骑手的工作和收入。为了维护平台秩序和骑手权益，该企业委托奇安信司法鉴定对涉案外挂程序进行电子数据司法鉴定。奇安信司法鉴定通过代码分析与动态验证，揭露了外挂软件的具体运作机制，为法律追责提供了关键证据。

案件背景

随着移动互联网的普及，外卖平台迅速崛起，成为日常生活中不可或缺的一部分。作为行业领头羊，该企业的众包平台为大量骑手提供了灵活的工作机会，但也吸引了不法分子的目光。这些不法分子开发了一系列外挂软件，通过自动化抢单、筛选优质订单等功能，使得使用外挂的骑手能够快速获取更多订单，从而获得更高的收入。

洞鉴解决方案

奇安信司法鉴定通过代码分析与动态验证，揭示了涉案外挂软件的具体运作机制——包括自主设定价格、重量、订单类型及顺路模式的自动抢单功能。

1. 静态代码审查

鉴定专家对涉案外挂软件的源代码、逆向代码进行了深度分析，通过阅读和理解代码结构、功能模块和执行流程，确定了软件的主要功能和作用，包括自动化抢单、智能化筛选优质订单等。同时，揭示了软件利用 Hook 技术，特别是 Xposed 框架，来拦截和篡改众包 APP 的预期行为，从而实现非法抢单的目的。

2. 动态行为验证

为了进一步验证软件的实际运行效果，鉴定专家在测试环境中安装并运行了抢单软件和众包软件，进行了功能复现，直接复现了外挂软件的核心功能，包括自动抢单和按预设条件筛选订单等，直观展示了软件的实际运作情况。

3. 劫持操作与模块分析

在动态验证的过程中，鉴定专家记录和分析了软件与众包平台间的交互过程，涵盖了网络请求、数据捕获及订单处理等环节。结合源代码审查，揭示了抢单软件通过执行 Xposed 模块的 Hook 代码，动态加载类并截获返回的数据包，来劫持众包应用的正常操作。通过这些操作，软件能够使用应用程序接口 (API) 执行一系列非法操作，深入展现了其对原有应用功能的侵入和控制。

图源网络，非本案外挂程序

客户价值

01 / 维护平台秩序

通过打击非法外挂软件，有助于众包平台维持其运营秩序，保障骑手的公平竞争环境。另一方面，也强化了平台对公平竞争的承诺，保护了平台声誉。

02 / 维护合法权益

司法鉴定意见书为平台提供了追究非法抢单软件开发者、售卖者以及使用者法律责任的坚实依据，有助于其及时制止非法软件的传播和使用，也为保护平台及其用户的合法权益奠定了基础。

03 / 揭示潜在漏洞

鉴定过程中对非法抢单软件与平台交互的详细分析，揭露了软件利用的具体技术原理和平台存在的安全漏洞，为防止非法抢单软件及其他潜在威胁提供了更为坚实的保障。

代打卡外挂案

通过 HOOK 技术篡改位置信息，精准鉴定伪造打卡行为

2024 年，某大型企业因代打卡外挂的广泛使用，导致考勤数据失真，企业内部管理秩序受到严重干扰。奇安信洞鉴在对涉案的代打卡外挂进行鉴定时，通过动态与静态分析手段，揭示了外挂通过 HOOK 技术篡改位置信息和 WiFi 信息，非法通过打卡验证的工作机制，为案件的侦破提供了关键技术支持。

案件背景

2024 年，某地公安局接到企业举报，称“某书”APP 考勤系统被外挂利用，员工通过非法软件修改位置信息实现远程打卡，严重影响了考勤的准确性和管理的公正性。经调查发现，涉案软件“某移”通过 HOOK 技术篡改了该 APP 中的 GPS 定位和 WiFi 验证信息，从而绕过了正常的打卡系统。警方随即委托奇安信洞鉴团队对该代打卡外挂进行司法鉴定，明确外挂的技术实现方式及其对系统的具体干扰。

洞鉴解决方案

1. 功能复现

首先在模拟真实的企业考勤环境下，对外挂功能进行动态复现。通过“某移”APP 修改 GPS 定位和 WiFi 信息，测试“某书”考勤系统的响应情况。实验中，“某移”成功将手机的实际位置信息篡改为设定的假位置信息，WiFi 验证信息也被伪造，导致打卡系统误以为员工在规定地点打卡。

2.Hook 分析

为深入揭示“某移”APP 的技术原理，使用 HOOK 框架对程序的调用路径进行分析。通过反复对比打卡前后 GPS 和 WiFi 验证的调用情况，发现“某移”通过 HOOK 技术劫持了“某书”APP 的 getLatitude 和 getLongitude 方法，篡改了实际返回的位置信息。同时，它还修改了 WiFi 的 SSID 和 BSSID 信息，使得设备能够通过打卡验证。此操作路径揭示了外挂通过篡改系统接口，绕过考勤验证机制的工作原理。

3. 静态分析

由于外挂加壳加密，鉴定人员通过脱壳手段对“某移”APP 进行了逆向分析，提取了其核心代码。通过对比源码和运行时的功能，确认了该外挂具备篡改 WiFi 和 GPS 数据的非法功能，并对其代码进行了完整记录。

02

INTELLECTUAL PROPERTY INFRINGEMENT
知产侵权

知识产权侵权指未经授权的情况下，使用、复制、修改、分发或销售他人受知识产权保护的作品、软件、源代码、设计、品牌等，侵犯了合法权利人对其知识产权的所有权或使用权。这种侵权行为不仅涉及民事赔偿，还可能构成刑事犯罪，特别是在大规模的网络传播或商业化运营的情况下。电子数据司法鉴定在知产侵权案件中，能够通过技术手段确认侵权行为发生的过程、时间、方式等，为司法诉讼提供关键证据。

1. 常见场景

破解正版软件

正版软件通常通过加密、授权码等技术手段对使用者进行合法验证，确保只有付费用户或授权用户能够使用软件功能。然而，侵权者通过技术手段破解这些保护机制，绕过授权验证，使得未经付费的用户能够无限制使用该软件。常见的情况包括办公软件、设计工具、游戏等商业软件的破解版本传播。

技术原理

1. 代码注入和补丁：在软件运行时向内存中注入特定代码，或者通过补丁修改二进制文件，移除或跳过软件的许可证验证机制。常用于解锁高级功能或跳过序列号验证。

2. 序列号生成器：通过逆向工程推导出正版软件的序列号算法，生成伪造的序列号，使软件认为其用户是经过授权的。常用于依赖序列号激活的应用程序。

3. 注册表或内存破解：修改系统中的注册表或运行时内存状态，强制使软件认为自己处于已激活状态。常用于本地存储激活信息的软件。

4. 凭证盗用和共享：通过网络钓鱼或凭证劫持，获取合法用户的授权信息，并非法共享或贩卖，常用于在线激活的正版软件。

网络盗链和转载

网络盗链和转载行为是指未经授权的情况下，通过技术手段直接引用、复制或分发受版权保护的内容。这些行为可能导致原内容提供方的流量损失、广告收入损失，甚至损害其声誉。

技术原理

1. 网络盗链：通过嵌入指向原始内容的 URL，直接从源服务器调用受保护的内容（如视频、图片、音频等），并绕过原始网站的流量控制和广告收入。此类行为通常利用了 HTML 的 < img > 标签或 < iframe > 嵌入。

2. 自动化爬虫：侵权者使用网络爬虫自动抓取他人网站上的文章、图片、视频等内容，并将这些内容批量发布到自己的平台或博客上。这类爬虫工具可以批量抓取网络资源，甚至自动去除版权标识，使原作者的权益更加难以保护。

IP类侵权

通常包括未经授权使用他人的商标、版权、专利等，主要涉及直接复制、改编或商业化使用他人的受保护作品，比如未经授权使用动漫、影视、游戏中的形象和设计。例如，销售印有知名动漫形象的 T 恤，属于未经授权的复制和销售行为，就是典型的 IP 侵权，属于侵犯著作权或商标权的行为。

针对此类侵权行为，权利人可通过以下方式搜集侵权证据：

1. 通过电子数据司法鉴定机构固定侵权商品的销售情况及相关网页证据。
2. 通过区块链存证平台对侵权内容进行固定，确保证据的真实性和可追溯性。

侵犯软件和游戏源代码

源代码是软件和游戏的核心机密，它包含了实现功能的核心逻辑、算法和设计。侵权者通过获取源代码，能够直接复制、篡改软件或游戏的功能，甚至在此基础上开发出类似的产品，这对开发者和权利人造成巨大的经济损失。源代码侵权不仅破坏了开发者的知识产权，还可能导致市场竞争不公平和产品商业价值的严重缩水。

技术原理

1. 逆向工程 通过反编译或反汇编，侵权者可以将软件的可执行文件还原为源代码或伪代码。这是源代码侵权的主要技术手段。逆向工程工具如 IDA Pro、Ghidra 等，可以帮助侵权者了解软件的内部逻辑和算法实现。

2. 漏洞攻击：在某些情况下，黑客利用软件或开发环境的安全漏洞，直接获取源代码。常见的攻击方式包括 SQL 注入、命令注入、远程代码执行等，尤其是在源代码管理平台（如 Git、SVN）被攻击时，容易造成源代码泄露。

3. 代码修改：侵权者通过对源代码或反编译后的代码进行修改，改变软件的部分功能或外观，然后重新发布为一个新的软件或游戏版本。这类修改通常涉及调整软件逻辑、优化算法或增加新的功能模块，表面上看似与原软件不同，但核心逻辑和功能仍基于被盗的源代码。贩卖，常用于在线激活的正版软件。

2. 取证鉴定思路

在知识产权侵权案件中，取证与鉴定的关键在于准确识别侵权行为的存在、方式和范围，特别是对于涉及复杂技术手段的侵权，如软件破解、源代码泄露等。

以下是针对知识产权侵权案件的取证与鉴定思路：

1 侵权行为线索收集

收集初步的侵权线索，确认侵权行为是否存在，以及侵权行为的范围和性质。

侵权行为确认：权利人可通过自主调查、市场监测等方式发现侵权线索，如发现疑似侵权的软件、应用或网站。

证据初步固定：利用公证处或区块链司法存证平台，对发现的侵权内容进行初步固定，如网页截图、下载链接、应用商店信息等，确保证据的时效性和完整性。

2 专业取证与证据固定

当侵权行为涉及复杂技术手段，普通取证方式难以获取有效证据时，需要专业的电子数据司法鉴定机构介入，在合法合规的前提下，获取侵权软件、应用、网站内容、产品实物等。

网络通信数据抓取：如果侵权涉及网络通信，使用专业工具对侵权软件或应用的网络通信进行抓包分析，获取其与服务器之间的数据交互内容。

数据解密与还原：对于加密的侵权数据，利用专业技术进行解密，还原真实的侵权内容。

3 技术分析与比对

通过技术手段对侵权内容与原始内容进行比对，并分析侵权者使用的技术手段，确认侵权行为的具体方式。

1. 侵权内容与原始内容的比对

哈希值比对：计算原始内容和侵权内容的哈希值（如 MD5、SHA256），判断两者是否完全一致。哈希值比对可以快速确认文件是否被篡改或复制。

文本相似度分析：对侵权作品（如文章、源代码）与原作品进行比对，确认文本中有多少行内容相似，多少行内容存在差异，分析其整体相似度和差异。

代码相似度分析：使用专用工具（如 Diff 工具）对比侵权代码与原始代码，分析其结构、函数模块、命名风格等，确认代码的相似度。

2. 侵权方式分析

逆向分析：对侵权软件或代码进行逆向分析，通过反编译或反汇编还原软件逻辑，确认侵权者如何绕过授权机制、篡改代码或实现未经授权的功能。

自动化脚本分析：在自动化侵权（如虚假流量、数据抓取）案件中，分析侵权者使用的自动化脚本，通过代码审查确认侵权者执行的具体操作。

4 证据链完善

通过收集与侵权行为相关的更多证据，补充原始证据的细节和背景，形成完整的证据链，确保证据的合法性和有效性。

交易记录：收集侵权者在侵权过程中涉及的交易记录，如非法销售盗版软件的支付记录、用户购买侵权内容的付款凭证等。这些证据可以证明侵权行为的经济动机和侵权规模。

通信记录：获取侵权者与其他相关方（如买家、合作者）的通信记录，确认侵权行为的策划和执行过程。例如，通过邮件、聊天记录等形式，确认侵权软件的传播和非法交易过程。

服务器日志：获取侵权者服务器的访问日志、下载日志，确认侵权内容的传播路径、下载次数、访问来源等。这些数据有助于评估侵权行为的影响范围和规模。

5 司法鉴定与专家意见

对证据进行技术鉴定，出具具有法律效力的鉴定意见书，为司法程序提供技术支持。

鉴定意见书 根据技术分析，出具详细的鉴定意见书，说明侵权内容与原始内容的相似性，侵权者所使用的技术手段，侵权行为的具体实施过程等。

专家意见：在技术分析的基础上，业内专家还可提供专家意见，如侵权行为的性质、影响范围、经济损失评估等，为诉讼提供支持。

出庭质证：鉴定专家可进行出庭质证，解释鉴定意见书中的技术原理，回答法官和律师的提问，确保司法程序的公平公正。

不同类型知产侵权的取证与鉴定要点

破解正版软件

01 破解工具及手段分析

- **收集破解工具：**获取用于破解正版软件的工具、补丁、序列号生成器等，确保获取方式合法且可溯源。保存相关下载链接、获取时间和途径等信息，以便追踪来源。
- **破解过程复现：**在受控环境下运行破解工具，使用录屏软件全程记录破解过程，详细记录破解前后的软件状态变化，包括软件版本、功能变化、许可证状态等。
- **分析破解手段：**深入分析破解工具的工作原理，确定其如何绕过软件的授权验证机制，例如是否通过修改二进制代码、注入非法指令、绕过许可证验证等方式实现破解。
- **评估对软件的影响：**评估破解行为对软件功能、性能和安全性的影响，确认破解行为对原软件构成的侵害程度。

02 正版与破解版软件的比较

- **获取对比样本：**分别获取正版软件和破解版软件的安装包，确保文件完整且未被二次篡改。
- **代码差异分析：**使用反汇编或二进制比较工具，分析正版与破解版软件的代码差异，确定被修改或替换的模块，识别被篡改的关键函数或安全机制。
- **功能差异测试：**通过功能测试，验证破解版软件是否解锁了原本受限的功能或移除了授权限制。记录功能差异，证明破解行为对软件功能的影响。

03 破解软件传播渠道分析

- **收集传播证据：**记录破解软件在网络上的传播渠道，如下载链接、论坛帖子、社交媒体分享等。保存相关网页的截图和链接，记录发布时间、发布者信息。
- **网络溯源分析：**通过分析 IP 地址、域名注册信息、联系邮箱等，尝试识别破解软件的上传者或传播者。
- **评估传播范围：**统计下载量、访问量等数据，评估侵权行为的影响范围和严重程度，为后续法律行动提供依据。

网络盗链和转载

01 盗链行为识别

- **监测网络流量：**使用网络流量分析工具监测服务器的请求，识别异常的外部引用请求。重点关注 Referer 头信息为空或来自非授权域名的请求。
- **收集 HTTP 请求信息：**记录盗链请求的 HTTP 头信息，包括 Referer、User-Agent、请求时间、请求资源等，确定盗链来源和方式。
- **技术验证盗链方式：**确认侵权网站如何直接引用原网站的资源，分析是否通过直接 URL 引用、嵌入式链接、iframe、脚本调用等方式实现盗链。
- **评估资源被调用情况：**统计盗链请求的次数、频率，评估对原网站带宽、资源的占用程度，量化因盗链造成的损失。

02 侵权内容比对

- **收集侵权内容：**保存侵权网站上的转载内容，包括文字、图片、视频等，确保内容完整性和原始性。记录内容的发布时间、发布者信息。
- **内容相似度分析：**分析转载内容与原始内容的相似度，确定是否构成实质性相似或直接复制。

03 运营信息及收益分析

- **定位服务器信息：**通过 IP 地址定位，确定侵权网站服务器的地理位置，判断司法管辖权范围。
- **广告和收益分析：**收集侵权网站的广告投放、付费内容、会员收费等信息，评估其因侵权行为获得的经济利益，量化侵权收益。

侵犯软件和游戏源代码

01 源代码比对分析

- **准备对比样本：**整理原始源代码和侵权源代码，确保版本一致或具有可比性。记录源代码的版本信息、作者信息、提交记录等。
- **代码预处理：**对源代码进行规范化处理，如格式统一、去除注释、标准化变量命名，确保比对结果的准确性和客观性。
- **相似度检测：**使用专业的源代码比对工具，分析代码的相似度，包括函数结构、算法实现、代码风格等，量化相似度。
- **独特性特征比对：**重点关注原代码中的独特实现、创新算法、特有的错误或注释等关键特征，若在侵权代码中出现，能强有力地证明侵权行为。

02 侵权事实的综合评估

- **收集开发过程证据：**获取原软件的开发文档、设计文档、版本控制记录、开发人员说明、软件著作权证书等，证明代码的原创性、开发时间和技术细节。
- **侵权行为认定：**综合技术比对结果和其他证据，认定侵权行为的存在和性质，明确侵权方式和责任主体。

3. 典型案例

盗版网络文学案

穿越版权迷雾：揭示侵权 App 关联与盗版收益

2023 年，一起侵犯千余部网络文学作品著作权的重大案件告破，涉案金额上亿元。在本案中，奇安信司法鉴定受到委托，对 25 个涉案 APP 进行了关联性分析，比对了近 6000 部作品的相似性，获取了广告平台应用 ID 以协助确定侵权收益。这一系列工作为捍卫版权提供了有力支持，保障了企业在法律诉讼中的权益。

案件背景

2022 年 10 月，某企业报案称，市面上出现了多款电子书阅读软件，擅自发行该企业独家代理的热门书籍和网络小说，涉嫌侵犯公司合法权益。警方迅速立案侦查，发现涉案软件及其运营方具有高度相似性，且均与一名男子有关。

进一步调查发现，该犯罪团伙自 2020 年开始，通过非法手段爬取正版电子书源，在其运营的阅读 APP 中发布，同时利用广告植入赚取非法利益。

此案涉及 25 个侵权 APP 以及数千部小说，侵权行为复杂、数据量庞大、非法收益难以追踪，亟需专业技术团队协助。

洞鉴解决方案

1. 网络流量抓包，确认共享接口

针对该案涉及的 25 个侵权 APP，鉴定人通过网络流量抓包技术，分析了 APP 发送的各种请求（如获取小说目录、章节、内容等），以便找出其背后的服务器接口。最终确认多个涉案 APP 存在共享的接口域名，这意味着这些应用的背后可能是相同的开发团队。

2. 获取应用 ID，协助确认侵权收益

针对所需分析的广告平台，鉴定人查找相应官方接入文档，分析对应应用标识符的特征。然后，根据该特征，对反编译的源代码进行查找分析，以确认应用 ID。部分 APP 的源代码中未找到预先配置好的 ID，鉴定人通过动态分析（例如使用 HOOK 或者网络抓包），获取了对应应用 ID。通过确认分析相关侵权 APP 集成广告平台的应用 ID，能够协助警方进一步确认相关应用的广告行为与非法收益。

3. 批量获取小说内容，比对相似性

鉴定人使用 JADX 对涉案 APP 进行逆向分析，找出不同小说内容对应的 URL 的编码规则，以便于编写脚本批量获取并固定盗版小说的文本内容；固定后将其与正版小说进行比对，发现其与正版小说相似度大于 80% 的数量超过 500 本，达到了追究相关人员刑事责任的标准。

检材文件	检材文件总字节	样本文件	样本文件总字节	相同字节数	检材文件相似度	样本文件相似度
[redacted]	972008	[redacted]	1095327	925481	95.21 %	84.49 %
[redacted]	2775708	[redacted]	2858087	2172756	78.28 %	76.02 %
[redacted]	1712473	[redacted]	3016749	1626810	95.00 %	53.93 %
[redacted]	698580	[redacted]	2163905	651930	93.32 %	30.13 %
[redacted]	1544527	[redacted]	1710636	1493399	96.69 %	87.30 %
[redacted]	2377473	[redacted]	2545771	2229239	93.77 %	87.57 %
[redacted]	2624560	[redacted]	2678428	2520483	96.03 %	94.10 %

部分相似度比对结果

客户价值

01 / 协助确认损失收益

通过对广告平台的应用 ID 分析，进一步帮助企业和相关执法机构追踪并确认侵权收益，有助于估算该企业因侵权行为损失的商业利益。

02 / 揭露盗版侵权网络

对涉案 APP 的共享接口分析，确认了其存在相同域名服务器，为警方和企业确认背后的作案团队提供了依据。

03 / 保护企业合法权益

通过本次电子数据司法鉴定，帮助企业收集并确认涉案软件的侵权行为及其非法利益，从而为该企业在后续的诉讼中提供有力的证据，保护了企业的合法权益。

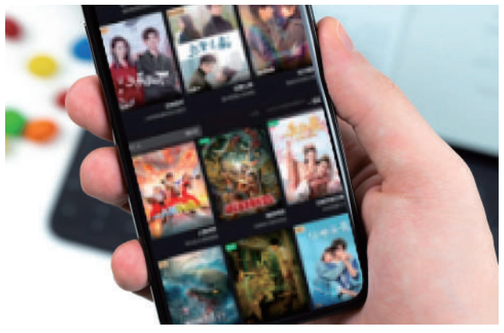
盗版视频网站案

24 小时内锁定侵权源头，为版权正义加速

2024 年，一起涉及大规模盗版视频网站的侵权案件告破。本案中，涉案人员通过爬虫软件非法采集并转载上万部影视作品至个人运营的盗版视频APP，以此获取非法利益。奇安信司法鉴定受托对涉嫌侵权的APP进行功能性鉴定，并通过技术分析追溯相关视频的播放地址，为保护知识产权提供了至关重要的证据。

案件背景

互联网已成为侵权盗版行为的温床。本案的涉案人员未经授权擅自采集各大视频平台的版权作品，并上传至其个人运营的盗版视频 APP 获利，严重侵犯了著作权人的合法权益。在接到著作权人投诉后，相关部门迅速采取行动，但由于涉案 APP 的在线特性，视频播放地址可能随时被更改或关闭，这使得迅速固定证据并准确追踪视频来源至关重要。



洞鉴解决方案

面对本案时间紧迫的挑战，奇安信司法鉴定的技术团队仅用一天时间就提取到了视频播放地址，并对侵权视频进行了及时固证，具体步骤如下：

1. 播放地址抓取

安装并运行涉案 APP，鉴定专家使用网络抓包工具捕获了 APP 的网络通信数据，重点捕获腾讯视频、优酷视频等 VIP 视频播放请求，成功追踪到非法获取的版权视频的播放地址。

2. 视频内容对比

对捕获到的播放地址与版权方播放地址的视频内容进行对比分析，观察广告播放、试看限制等方面的差异。结果表明涉案 APP 绕过了正规视频平台的版权保护机制，非法播放 VIP 视频内容。

3. 侵权证据固定

为确保侵权行为的证据具有法律效力，鉴定专家对捕获的视频播放地址及相关数据进行固定，并计算了每个视频文件的 SHA256 值，确保证据的完整性和不可篡改性。

客户价值

01 / 提升诉讼效率与成功率

使用先进的网络抓包和数据分析技术，奇安信司法鉴定在一天内准确地捕获了涉案视频的播放地址，同时确保了证据的可靠性和有效性。这一过程大大节约了客户寻找和固定证据的时间和资源，提高了法律诉讼的效率与成功率。

02 / 维护企业合法权益

通过深入的视频内容验证和对比分析，奇安信司法鉴定明确指出了涉案 APP 绕过版权保护的非法行为，有助于保护客户的知识产权，防止版权作品被非法利用。

03 / 促进行业健康发展

本次案件中，通过严谨专业的鉴定手段，有效遏制了盗版行为，维护了版权市场的正当秩序。此举不仅加强了对合法版权的保护，也为创作者和版权所有者提供了一个更加公平和有序的市场环境。

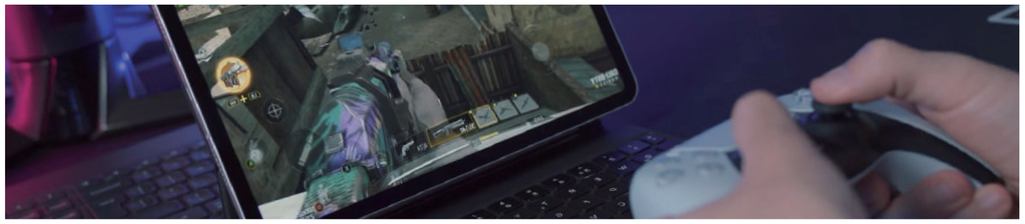
游戏私服案

关键文件比对分析，深挖私服侵权细节

湖北某地公安接到举报，称某团队在未获得官方授权的情况下，非法搭建并运营多个游戏私服网站，涉嫌侵犯著作权。奇安信司法鉴定接受委托，对涉案的硬盘及硬盘镜像文件进行了细致的司法鉴定，鉴定结果揭示了涉案私服程序与官方程序之间存在显著的实质性相似性，为定性侵权行为提供了坚实的证据基础。

案件背景

在网络游戏行业蓬勃发展的今天，数字版权保护成为了一个亟待解决的问题。本案涉及的游戏因其庞大的市场影响力和忠实的玩家基础，成为了私服搭建者的目标。犯罪嫌疑人出于非法获利的目的，擅自搭建并运营了多个游戏私服网站，这些私服不仅吸引了大量玩家，更对正版游戏的市场秩序构成了严重破坏。这一行为不仅侵犯了游戏开发者的著作权，也损害了正版游戏运营商的经济利益，对整个游戏产业的健康发展造成了负面影响。



洞鉴解决方案

在游戏私服案件的鉴定过程中，关键的比对环节包括目录结构、关键文件（如可执行文件和库文件）、源码，以及游戏内的资源（例如地图、角色、物品等）。这些元素是构建游戏体验和框架的基石，对于鉴定游戏间潜在的侵权关系具有决定性作用。以下是对本案鉴定过程的详细描述：

01 源代码对比

为确定涉案私服游戏与官方游戏服务器端文件的相似度，鉴定专家对脱壳后的文件与官方游戏版本进行源码比对，两者之间的函数相似度达到了 91%，从而证实了涉案私服游戏与官方游戏程序之间存在实质性相似性。

02 目录结构比对

游戏的目录结构反映了文件组织的逻辑关系，对比目录结构有助于发现游戏文件的组织方式和依赖关系是否有相似之处。在比对官方游戏与涉案私服的目录结构时，发现涉案私服游戏的目录结构与官方游戏有着明显的对应关系，特别是在“.exe”和“.dll”文件的组织方式上，进一步证实了其在架构设计上的模仿。

03 地图比对

地图是游戏资源文件之一，对比地图可以发现游戏在场景布局方面的相似性。鉴定专家对官方游戏和涉案私服的地图文件进行了二进制比对，通过计算相同文件数量与总文件数量的比值，得出了地图文件的相似度在 66.7%~99.7% 之间，为评估侵权行为的性质提供了重要依据。

硬盘编号	路径	相同文件	相同地图	差异地图	地图相似度
1	[redacted]	8	323	4	98.8%
	[redacted]	8	322	5	98.5%
2	[redacted]	8	328	3	99.1%
	[redacted]	8	92	5	94.8%
	[redacted]	8	261	3	98.9%
3	[redacted]	8	322	9	97.3%
	[redacted]	8	323	8	97.6%
	[redacted]	8	327	4	98.8%
4	[redacted]	9	20	3	87.0%

通过源代码的深入分析、目录结构的细致比对以及游戏地图文件的精确对比，本案的鉴定工作全面揭示了涉案私服游戏在多个关键方面与官方游戏的实质性相似性，为案件的法律判断提供了坚实的技术支撑。

客户价值

01 / 提供确凿证据

通过深入分析源代码、目录结构和游戏资源，迅速揭示了涉案私服游戏与官方游戏之间的高度相似性，这些确凿的证据为侵权事实的证明提供了强有力的支持，帮助客户在法律诉讼中确立了有利的立场。

02 / 维护企业权益

凭借奇安信司法鉴定所提供的详尽鉴定意见书，客户能够清晰、有效地在法庭上展示侵权证据，显著提高了法律诉讼的效率与成功率，有效保护了客户的知识产权和经济利益，避免了进一步的经济损失，同时对维护客户的品牌声誉和市场份额具有重要意义。

03 / 促进产业健康发展

本案的成功鉴定及后续的法律行动，对潜在的游戏侵权行为产生了震慑效果。这一点对于促进游戏市场的健康发展和维护行业内的公平竞争环境至关重要，有助于构建一个尊重知识产权、鼓励创新的游戏产业生态。

03

DATA BREACH
数据泄露

数据泄露是指未经授权的访问或泄露敏感数据，这些数据可能包括个人信息、财务数据、企业机密或其他受保护的隐私信息。数据泄露通常由于安全漏洞、技术攻击或人为失误导致，可能带来经济损失、法律责任以及声誉受损。数据泄露通常发生在网络攻击、身份盗窃、恶意软件入侵或内部人员泄密的场景中。

1. 常见场景

账号信息泄露

账号信息泄露指的是攻击者通过各种技术手段获取用户的登录凭证，未经授权访问其账户。这类数据泄露通常发生在游戏、社交媒体、电商平台等需要用户登录的系统中。攻击者获取到的账号信息可能被用于虚拟物品的盗窃、社交媒体诈骗、金融交易等。

技术原理

1. 凭证劫持：攻击者通过恶意网站或伪造的登录页面进行钓鱼攻击，诱使用户输入其账号信息。或者通过暴力破解或利用已泄露的数据库，直接获取用户的登录凭证。

2. 会话劫持：攻击者可以通过在公共 Wi-Fi 或不安全的网络环境中监控网络流量，截获用户与服务器之间的会话令牌（如 Cookie 或 Session ID），冒用用户的身份访问系统。

企业数据泄露

企业数据泄露指的是企业的财务数据、客户信息或商业机密被外部攻击者或内部人员获取。企业数据泄露会对公司的运营、信誉和财务造成重大影响，甚至可能涉及法律诉讼。

技术原理

1.SQL 注入：攻击者通过在输入字段中插入恶意代码，操纵数据库执行非预期操作，获取存储在数据库中的敏感信息。未对用户输入进行适当过滤的系统尤为容易受到此类攻击。例如，攻击者通过注入恶意 SQL 代码获取公司客户信息。

2. 内部人员泄密：企业内部人员出于恶意或疏忽泄露公司敏感数据，可能通过导出文件、发送电子邮件等手段非法传播这些信息。

3. 恶意软件感染：恶意软件通过钓鱼邮件、感染的文件或漏洞利用感染公司网络。攻击者可以远程控制企业的系统，窃取或篡改重要数据。常见的恶意软件如勒索软件，会加密企业的文件，直到公司支付赎金以解锁数据。

用户信息泄露

用户信息泄露指的是电商、社交媒体、物流等平台上存储的用户个人信息（如姓名、联系方式、地址等）被攻击者非法获取，可能被用于实施精准诈骗、身份盗用或非法交易。用户信息的泄露对个人和企业均构成威胁，特别是在大规模数据泄露事件中，涉及数百万用户的信息被非法出售或滥用。

技术原理

1. 数据库渗透：攻击者利用数据库中的漏洞或弱密码，获得对数据库的访问权限，窃取存储的个人信息。例如，攻击者通过 SQL 注入攻击入侵电商平台的数据库，获取用户的购物记录和支付信息。

2. 未授权访问：由于平台的 API 接口或数据存储配置不当，攻击者可以通过公开的 API 接口或系统漏洞，绕过身份验证机制，直接访问存储的用户数据。这种攻击通常发生在平台安全防护不足或错误配置的场景下。

2. 取证鉴定思路

数据泄露案件的取证鉴定工作具有较高的技术复杂性，尤其在数据传播路径追踪、内部泄露审查及证据合法性保障方面，与其他案件类型相比有显著差异。针对数据泄露案件，取证工作必须迅速反应，确保证据的完整性，并对泄露路径进行全面的分析，确保证据链条完整无缝。

以下是针对数据泄露案件的通用取证鉴定思路：

1 证据即时固定

在数据泄露案件中，受害企业的系统通常会继续运转，而攻击者往往具备高度的隐蔽性，能够迅速删除或隐藏其痕迹。因此，取证工作的第一步是确保在数据泄露发生后能够快速固定所有相关证据，并防止后续篡改。

服务器镜像备份：对泄露数据的源服务器、客户端设备等进行完整的镜像备份，生成哈希值确保备份数据的完整性，避免后续篡改。

日志与流量保存：保存服务器、网络设备和防火墙的相关日志（包括访问日志、系统日志、错误日志），以及特定时间段的网络流量，确保所有操作行为都能被追溯。

系统快照：对于虚拟化环境和云服务，捕获系统快照，记录泄露发生时的系统状态，便于后续分析系统的内存、进程状态等信息。

2 排查泄露源

分析和排查可能的数据泄露源，确定数据泄露的方式和路径。

1. 常见的泄露源

系统漏洞：由于未修补的系统或应用程序漏洞导致外部攻击者入侵，获取敏感数据。常见漏洞包括 SQL 注入、跨站脚本（XSS）和未修补的补丁。

恶意程序：如木马、勒索软件等，攻击者利用恶意程序入侵企业网络，窃取、加密或篡改数据。

内部人员：内部员工可能因为疏忽或恶意泄露数据，包括导出敏感文件或通过不安全的渠道传输数据。

2. 排查泄露源的方法

系统漏洞检测：使用专业的漏洞扫描工具，检测系统和应用程序是否存在未修补的安全漏洞，如 SQL 注入、跨站脚本（XSS）、弱口令等。

恶意程序排查：分析系统运行的进程和服务，识别可疑的、不明来源的程序。查找系统中的可疑文件、异常修改的注册表项，识别恶意程序的存在。

网络流量分析：利用抓包工具（如 Wireshark）分析网络流量，发现异常的网络连接和数据传输，识别数据泄露的可能通道。

内部权限和访问记录审查：检查用户的权限设置和访问日志，识别异常的访问行为，如非工作时间的大量数据导出、频繁访问敏感数据等。

3 恶意程序及攻击行为分析

在排查恶意程序时，发现系统感染了木马、勒索软件等恶意软件或外部攻击迹象，可对其进行进一步的鉴定，明确攻击者的手段和路径。

1. 恶意程序分析

静态分析：对恶意程序进行反汇编和代码审查，了解其功能、行为和影响范围。

动态分析：在受控环境（如沙箱）中运行恶意程序，观察其行为，记录其与系统和网络的交互。

2. 攻击路径重建

日志关联分析：通过关联不同日志文件的信息，重建攻击者的操作步骤，明确其入侵路径和数据窃取方式。

漏洞利用验证：模拟攻击者的入侵过程，验证其是否利用了特定漏洞，确保分析的准确性。

3. 攻击者溯源

IP 地址溯源：通过分析攻击者的 IP 地址，结合地理定位工具，查明攻击者的可能来源和使用的代理路径（如 VPN、代理服务器等）。

特征比对：将恶意程序的特征与已知的攻击样本库进行比对，可能识别出攻击团伙或工具。

4 内部人员泄露调查

如果初步分析表明数据泄露源自内部人员，需进一步调查内部操作行为，以识别泄密的方式和动机。

行为审计：详细审查可疑人员的系统访问日志，关注异常的登录时间、数据访问量、文件操作等。并检查文件的创建、修改、复制和删除记录，识别大规模数据拷贝或传输的行为。还需关注网盘客户端的使用情况，分析登录、上传、下载的行为日志。

网盘取证：如果怀疑数据通过网盘泄露，需对相关客户端进行分析。通过云存储平台客户端日志提取文件上传、下载的记录，检查文件名、文件大小、Hash 值等，确认曾上传或分享过敏感数据的情况。

通信记录审查：在合法合规的前提下，审查可疑人员的公司电子邮件和即时通讯工具，寻找与泄密相关的通信线索。同时，检查 USB 设备的连接日志，以侧面反映某一时间段内是否存在存储设备插拔的行为，结合其他证据进一步判断是否涉及数据外泄。

5 鉴定意见书与证据链的完善

在数据泄露案件中，由于数据量庞大、种类复杂，确保证据链的合法性与完整性是至关重要的。所有证据必须具有司法效力，能够支撑案件的责任认定和审理。

证据完整性保障：通过哈希值计算、区块链存证等技术手段，确保所有证据在固定过程中未被篡改，并在后续审查时能够验证其真实性。

取证过程记录：完善取证的全过程记录，使用符合司法标准的取证工具，确保取证过程的合法性，并保证证据的原始性和可采信性。

鉴定意见书出具：在鉴定分析结束后，出具详细的鉴定意见书，确保证据链条中各环节无缝衔接，所有证据相互呼应，形成完整的证明路径，保障证据在司法程序中的有效性和合理性。

3. 典型案例

社交媒体盗号案

账号凭证大规模泄露！深入还原攻击路径，锁定关键证据

本案涉及大量用户的社交媒体平台账号被盗，犯罪分子利用非法获取的用户凭证远程登录某知名社交媒体平台账号，并通过控制这些账号实施非法活动。奇安信洞鉴对相关远程服务器和数据库进行取证分析，并恢复了被盗的用户数据和操作日志，为案件侦破提供了关键的电子证据。

案件背景

2023 年，某地公安局接到多名市民报案，称其在某社交媒体平台的账号被非法盗用，导致用户个人信息泄露。通过初步调查，发现这些盗号事件可能涉及一个组织性的网络犯罪团伙。公安局在获取初步线索后，委托奇安信洞鉴对相关服务器、数据库和其他电子数据进行深入分析，查明账号被盗的具体手法及相关证据。

洞鉴解决方案

01 数据固定与镜像制作

首先对嫌疑人使用的远程服务器进行了全面的数据固定和镜像制作。鉴定人员开启屏幕录像后，登录委托方提供的宝塔面板地址，凭借提供的用户名和密码成功进入目标服务器。在进入服务器后，使用宝塔面板中的“SSH 密钥登录”功能，生成并下载了服务器的 SSH 密钥文件，随后通过 SafeServer 工具建立连接，成功登录目标服务器并选择镜像格式为“DD”，制作了完整的服务器镜像文件。

02 数据库提取与分析

使用数据库管理工具连接相关数据库，对被盗账号的用户数据和操作日志进行了全面的提取和分析。重点分析了该数据库中的用户登录日志、访问记录、账户更改信息等内容，确认了黑客非法获取用户凭证并在多个时段非法访问用户账号的操作过程。这些数据帮助确认了账号被非法访问的具体时间和方式，为案件提供了重要证据。

03 程序逆向分析

对从服务器和硬盘中提取的恶意程序文件进行了逆向分析，鉴定人员使用了反编译工具仔细检查了程序的代码结构、函数调用和逻辑。分析发现，这些恶意程序通过特定的接口与社交媒体平台的 API 进行交互，生成用于登录的二维码。当用户扫描二维码进行登录时，程序能够截获用户的登录凭证（如 cookie、UID 等），并将其发送到黑客控制的远程服务器。这一行为表明程序的核心功能是窃取用户的认证信息。

04 恶意功能复现

为了进一步验证代码的实际运行效果，鉴定人员使用了虚拟机工具搭建了与实际服务器相似的仿真环境，对程序进行功能测试。测试证实，程序在用户扫码登录后，确实能够成功窃取用户的登录信息，并将其写入服务器的数据库。

客户价值

01 / 保障用户信息安全

通过深入分析社交媒体平台的远程服务器和数据库，帮助客户恢复了大量被盗的用户数据，揭示了黑客非法获取用户凭证的具体手段，有效遏制了用户信息泄露的进一步扩散。

02 / 为案件侦破提供关键证据

通过精确的服务器镜像制作和数据库日志提取，锁定了黑客的非法操作路径，恢复了账号被盗的具体过程，并提供了详细的操作日志和访问记录，为公安机关破案提供了坚实的技术支撑。

03 / 提升平台安全防护能力

通过重建社交媒体平台的运行环境，全面分析了后台系统的安全漏洞，并揭示了平台在登录和权限管理模块中的安全缺陷，促使企业对系统漏洞进行修复，显著提升了平台的安全性。

AI 换脸盗号案

破解人脸验证盗取游戏账户，还原 AI 换脸技术作案过程

该案件中，嫌疑人通过虚假人脸视频，成功绕过游戏的实名认证系统，仅凭账号和密码即可登录游戏账户。奇安信洞鉴团队通过对嫌疑人笔记本电脑进行详细的电子数据司法鉴定，还原了其利用 AI 换脸技术进行非法操作的全过程，为案件侦破提供了关键证据支持。

案件背景

近年来，人工智能技术迅猛发展，AI 换脸技术被广泛应用于影视制作和娱乐等领域，展现出积极的应用前景。然而，该技术也被不法分子利用，涉及网络诈骗和身份伪造等非法活动，带来了严重的安全隐患。

在本案中，上游联系了嫌疑人，告知其掌握一批热门游戏账号及相应的身份证信息，急需解决身份认证中的人脸识别问题。嫌疑人借助 AI 换脸技术，成功绕过游戏的人脸识别验证机制，仅凭账号和密码即可登录受害者的游戏账户。

洞鉴解决方案

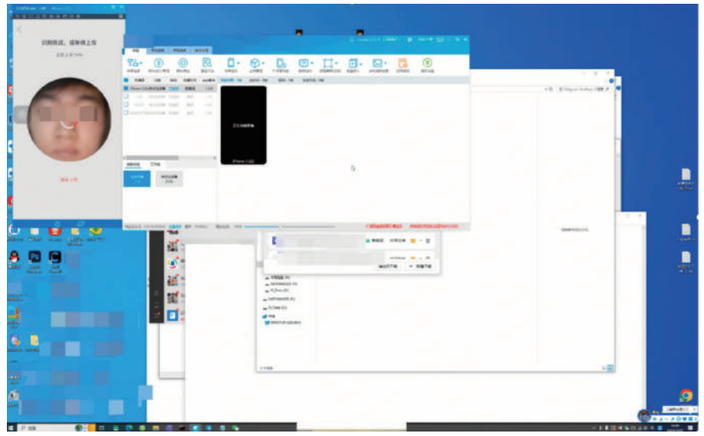
01 案中：协助现勘取证，全面还原 AI 换脸过程

嫌疑人电脑取证

首先对嫌疑人的电脑进行了内存镜像提取，获取电脑当前登录微信、QQ 等即时通讯软件的密钥，后期利用该密钥解析电脑端即时通讯软件的聊天记录，还原了大量嫌疑人通信和交易相关的记录。

技术复现

通过现场演示，专家团队成功复现了嫌疑人的作案手法。嫌疑人利用从非法渠道获取身份证照片，通过某视频合成平台生成符合游戏系统要求的虚假人脸视频，并在游戏的人脸验证环节使用该合成视频成功绕过了系统的认证要求，从而顺利登录了受害者的游戏账户。



02 案后：数据提取与分析，出具详细鉴定意见

数据提取与分析

从嫌疑人电脑中提取了包括 AI 换脸视频、被替换的身份证照片、软件使用记录等关键信息，确认了嫌疑人通过视频合成、数据伪造实现非法登录的技术手段。

客户价值

01 / 揭示新型技术犯罪手法

通过对案件的深入分析和技术复现，揭示了利用 AI 换脸技术绕过人脸验证系统的全新犯罪手法，有助于防范未来类似犯罪的发生。

02 / 提升案件侦破效率

凭借专业的取证和技术还原能力，快速精准地还原了嫌疑人的作案手法，帮助警方全面掌握了案件关键证据，大幅提升了案件的侦破效率。

03 / 强化游戏行业安全防护

深入研究并揭露了游戏行业中利用 AI 换脸技术进行账户盗取的风险，为游戏开发商提供了针对性防护建议，有助于完善游戏内的身份验证机制。

新型打印机木马案

网购信息缘何泄露？揭秘打印机背后的木马程序秘密

最近，一宗涉及打印机木马的新型个人信息泄露案引起了广泛关注。在本案中，警方发现某物流企业的一名离职员工，将木马程序植入到连接了物流面单打印机的电脑中，非法盗取并售卖公民信息。为了揭示木马程序的运行原理，上海警方委托奇安信司法鉴定进行深入的功能性鉴定，鉴定人通过静态分析、动态分析和逆向工程技术对涉案木马程序进行了深入研究，确认了木马程序的运行模式，并成功获取了关键信息。

案件背景

2023年，上海警方接报，一位公民网购后，被冒充客服的诈骗分子以快递丢失为由骗走了2万元。此案令人疑惑的关键在于，诈骗分子如何精确地掌握了被害人的身份、网购订单和快递信息？

通过分析比对一系列类似案件，警方最终锁定信息泄漏源头为一家上海的物流企业。随后的深入调查发现，该企业的一名已离职员工彭某涉案。彭某通过某境外社交软件结识了一名有意购买公民信息的不法分子，并在其指使下入职该物流企业，将涉案木马程序植入到连接物流面单打印机的电脑中，非法盗取公民信息。

由于犯罪手段的隐秘性和技术性，给警方的侦查工作带来挑战，亟需明确涉案木马程序盗取公民信息的底层原理。

洞鉴解决方案

1. 逆向分析

通过逆向分析，鉴定人深入解构了涉案的木马程序文件，揭示出该木马程序通过调用 Windows 系统的 API 函数，来监视打印机作业并上传至远程服务器，以实现数据窃取的目的。

2. 动态调试

动态调试的结果进一步证实了该木马程序的运作模式，通过精细地追踪和分析程序运行过程，鉴定人成功地获取了远程服务器的 IP 地址以及登录的帐户名和密码。

3. 缓存提取

通过对打印机缓存进行深度提取，鉴定人找到了大量的打印作业文件，确认了这些被窃取的数据都在案发时间内生成。

这一系列详尽而精准的鉴定步骤，揭示了木马程序如何获取公民个人信息，并将其传输至境外的具体运作机制。

名称	修改日期	类型	大小
00004.SHD	2022/3/1 12:09	SHD 文件	3 KB
00004.SPL	2022/3/1 12:09	SPL 文件	52 KB
00005.SHD	2022/3/1 12:09	SHD 文件	3 KB
00005.SPL	2022/3/1 12:09	SPL 文件	52 KB
00015.SHD	2022/5/20 16:12	SHD 文件	2 KB
00015.SPL	2022/5/20 16:12	SPL 文件	31 KB
FP00000.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00000.SPL	2022/5/13 16:43	SPL 文件	1,181 KB
FP00001.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00001.SPL	2022/5/13 16:43	SPL 文件	1,191 KB
FP00002.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00002.SPL	2022/5/13 16:43	SPL 文件	1,216 KB
FP00003.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00003.SPL	2022/5/13 16:43	SPL 文件	1,173 KB
FP00004.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00004.SPL	2022/5/13 16:43	SPL 文件	1,179 KB
FP00005.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00005.SPL	2022/5/13 16:43	SPL 文件	1,222 KB
FP00006.SHD	2022/5/13 16:43	SHD 文件	3 KB
FP00006.SPL	2022/5/13 16:43	SPL 文件	1,158 KB
FP00007.SHD	2022/5/22 10:09	SHD 文件	3 KB
FP00007.SPL	2022/5/22 10:09	SPL 文件	16,686 KB

案例价值

01 / 保护公民权益

在本案中，成功识破利用公民信息诈骗的犯罪团伙，制止了其通过非法获取个人信息进行诈骗的行为，维护了广大消费者的财产安全和信息隐私。

02 / 协助警方调查

涉案木马程序实现数据窃取的技术手段隐蔽复杂，电子数据鉴定通过对其进行静态逆向和动态调试成功解析了其运行机制，为公安机关全面了解此类犯罪的作案手法提供了关键支持。

03 / 提升企业安全治理

本案向相关企业发出警示，需要建立完善的员工管理制度，避免内部人员违规操作导致信息系统被植入木马程序；同时也提示企业应重视信息系统的安全建设与维护，规范信息系统的操作流程管理，以杜绝信息泄露事件的发生。

快递面单解密案

数十万条订单数据固定分析，揭露虚假销量骗局

本案涉及快递面单数据的非法获取与使用。犯罪嫌疑人通过开发非法程序，利用服务器从目标平台获取快递面单数据，并进行非法贩卖。奇安信洞鉴对犯罪工具进行全面的技术分析，并对嫌疑人使用的服务器和程序进行鉴定，识别出非法获取快递面单数据的手段。

案件背景

2023 年，某地公安机关破获了一起涉及非法获取快递面单信息的案件。嫌疑人通过非法手段，开发了一款能够从快递公司服务器中获取面单信息的工具，并在网络上进行贩卖，涉及多名商家。该工具通过解密手段非法获取用户的收货地址、联系方式等隐私信息，造成了严重的个人信息泄露风险。为了进一步确定该工具的功能和非法获取数据的方式，公安机关委托奇安信洞鉴进行技术支持，深入分析该工具的行为及其对系统的破坏性。

洞鉴解决方案

01 镜像制作与文件提取

首先对检材硬盘进行了完整的镜像制作，并确保镜像文件与原盘数据完全一致。随后，利用盘古石计算机取证分析系统提取了硬盘中的关键压缩文件，提取出多个可执行文件及相关的系统日志。

02 程序行为分析

为确认工具的非法行为，鉴定专家在虚拟机中运行了该工具的主程序。使用火绒安全分析工具进行监控后，发现该程序会连接服务器，并通过该地址与远程服务器进行通信，抓取面单数据。此外，该程序生成了日志文件 “start_log.txt”，记录了与服务器的通信过程。

03 恶意程序分析

在分析工具生成的数据包时，专家团队发现，程序能够通过特定的数据包向服务器请求快递面单数据，并将这些数据存储于本地文件中。通过反编译工具和行为监控，鉴定人员成功确认了该程序的非法行为：未经授权的情况下，具备从远程服务器获取并解码快递面单数据的能力，并能够通过伪造身份凭证获取目标平台的数据。

04 数据库分析

连接并导入硬盘中提取的数据库文件，深入分析了用户数据。鉴定发现数据库中存储了超过 31 万条订单信息、6000 条用户信息等。这些数据直接关联到快递面单的非法获取操作，提供了关键的证据支持。

案例价值

01 / 保护个人隐私

通过全面分析快递面单数据的非法获取手段，帮助公安机关揭露了大规模的个人信息泄露风险，锁定了犯罪工具的运作机制，阻止了犯罪团伙继续通过非法贩卖用户隐私信息获利，保障了数千名消费者的隐私安全，维护了公众的合法权益。

02 / 强有力证据支持

提取并分析了嫌疑人使用的服务器及程序中的大量数据，包括超过 31 万条订单信息和 6000 条用户数据。通过精准的程序行为监控与恶意程序分析，提供了全面且合法有效的证据支持。

03 / 提升企业数据安全管理

不仅帮助企业了解了犯罪分子的作案手法，还为快递公司及相关企业发出了强烈警示，促使企业优化其数据安全管理，防止类似安全漏洞在未来被不法分子进一步利用。

04

ONLINE COMMENT EARNING
网络水军

网络水军是指通过自动化工具或人为操控来制造虚假的网络流量和互动行为。这些行为包括伪造浏览量、阅读量、点赞数、评论等指标，旨在操控公众舆论、提升产品销量或改变社交媒体上的话题热度。网络水军行为不仅会误导公众，还会对网络平台的正常运营秩序造成破坏。

1. 常见场景

刷浏览量

在视频网站、新闻平台和电商平台中，网络水军通过制造虚假浏览量，使特定的视频、文章或商品页面显示出大量访问数据。这类刷浏览量的行为不仅会误导其他用户，认为该内容十分受欢迎，还会干扰平台的推荐系统，使该内容获得更多曝光机会。

舆情操控

舆情操控指网络水军通过批量刷评论、点赞、转发等操作，操控公众对某个事件、产品或话题的看法。通过制造大量的虚假互动，水军可以将特定话题推上热搜榜或热门讨论列表，误导公众舆论。虚假评论是舆情操控中的重要手段，通过批量发布一致性极高的评论，水军可以引导讨论方向，塑造特定的舆论氛围，甚至打击竞争对手。这类行为广泛应用于社交媒体、新闻评论区和论坛，甚至在政治或商业竞争中被滥用。

刷销量

刷销量行为在电商平台中广泛存在，网络水军通过使用自动化工具创建大量虚假买家账号，并进行虚假交易。通过大量生成虚假订单，水军可以欺骗电商平台的销量统计系统，使该商品的销量数据迅速攀升。这不仅提升了商品在平台的搜索排名和曝光度，还会吸引更多的真实消费者进行购买，从而人为地营造出商品热销的假象。

技术原理

1. 自动化脚本：通过编写自动化脚本，模拟用户的浏览、阅读、评论或互动行为。脚本通常被设定为频繁访问特定页面、重复刷新、点赞或评论，以制造出大规模的虚假互动。这种方法效率高、成本低，适合大规模刷量。

2. 代理 IP 轮换：为了避免大量访问来自同一 IP 地址被识别为异常流量，网络水军通过代理服务器切换 IP 地址，使每次访问看起来都来自不同的用户，从而规避平台的防作弊检测。

4. 流量劫持: 攻击者通过植入恶意代码或修改用户的网络请求，将真实用户的访问流量重定向到目标页面，制造高访问量。这些劫持行为不仅增加了目标页面的浏览量，还可能进一步影响用户的行为和网络体验。

2. 取证鉴定思路

网络水军案件主要通过自动化脚本进行批量操作，行为隐蔽、规模庞大，目的往往是操控舆论、刷流量、刷销量等。此类案件中的关键是收集足够的证据以证明网络水军的存在及其操作的技术手段，并追溯相关责任方。由于此类案件中，数据的实时性和变化性很高，取证和鉴定工作必须保证数据的完整性和合法性。

1 证据固定与配合抓捕

网络水军案件通常涉及大量的虚假流量和互动操作，在初步调查阶段，需要快速、批量固定证据，防止证据被删除或修改。

网页取证：使用专业工具对涉案网页进行快照保存，记录页面内容、URL、时间戳等信息，进行屏幕录像，完整记录操作过程和结果。

现场取证：配合现场抓捕时，提取每台设备的全镜像数据，确保包含所有脚本文件、操作日志、通信数据等。对于虚拟服务器或云计算设备，也需通过网络取证工具进行远程数据提取。

2 舆情操控和虚假评论溯源

通过技术手段深入分析网络水军的舆情操控行为，特别是批量生成的虚假评论、点赞及转发操作，并通过数据溯源确定责任主体。

IP 地址追踪：对于发送虚假评论、点赞的 IP 地址，进行地理定位和网络代理检测，识别是否通过 VPN、代理服务器或僵尸网络进行操作，并尝试追踪真实的物理地址。通过分析 IP 地址的集中性与可疑的频繁访问记录，定位水军操控的集群服务器。

评论、转发和点赞数据统计：统计虚假互动行为的数量，如评论、转发和点赞数据等。

评论内容分析：通过文本分析技术对评论内容进行语义分析，判断是否存在模板化、重复性语言，识别出批量生成的评论。

3 虚假交易与刷销量取证

通过深入分析电商平台的虚假订单记录，识别刷单行为的具体操作手法，追踪资金流向并确定责任方。

订单数据分析：审查平台上的订单数据，特别是订单生成时间、账户注册信息、支付方式等，识别批量生成的虚假订单。通过对短时间内集中生成的订单进行数据对比，确认是否存在刷单行为。

资金流向分析：通过分析支付流水、银行转账记录、第三方支付平台数据等，追踪资金流向，确认刷单行为的经济链条，判断是否涉及洗钱等进一步的违法行为。

物流记录交叉验证：对于涉及物流的刷单行为，核实物流单号与实际货物流动情况是否匹配。如果存在物流单号但未实际发货的情况，则可以确认其为虚假交易。

4 刷量脚本功能性分析

通过技术分析和功能测试，深入理解网络水军所使用的刷量脚本的运行原理与操作方式，明确其对目标平台的实际影响。

脚本代码分析：对提取的刷量脚本进行深度分析，拆解其内部代码结构，尤其是用于伪造身份、批量生成流量或虚假操作的关键算法逻辑。通过分析脚本与目标平台通信时的数据包内容，确认脚本如何模拟真实用户操作，并生成虚假的点赞、评论或浏览量。

仿真测试与功能验证：在仿真环境中运行刷量脚本，通过搭建与实际目标平台相似的测试环境（如短视频平台或电商平台），监控流量、点赞、评论等数据的实时变化，验证脚本的功能性。特别关注脚本是否具备生成虚假身份、批量增加视频播放量或自动完成虚假交易的能力，并通过功能性验证记录其对平台产生的实际影响。

5 鉴定意见书与证据链完善

最终，鉴定工作需形成一套完整、严谨的证据链，确保所有证据均符合司法标准，并可以支持后续的法律诉讼。

证据链条的合法性与完整性：通过详细记录每一步的取证过程，保证所有证据都具备合法性和可验证性。特别是在跨平台、跨区域取证时，确保各个环节之间的证据能够有效衔接，形成完整的证明链条。

司法鉴定意见书编制：结合所有取证步骤与分析结果，编写结构清晰、内容详实的司法鉴定意见书，详细说明水军行为的技术原理、虚假流量的影响范围、资金链路的操作方式等。

3. 典型案例

西安特大网络“水军”案

数百部设备全面固证分析，起底虚假流量骗局

2023 年，西安警方成功破获了一起特大网络“水军”诈骗案，揭示了一个庞大的黑灰产链条。涉案人员利用非法脚本程序制造虚假播放量，欺骗广告商和平台用户，牟取非法利益。奇安信司法鉴定受托为此案提供技术支持，通过先进的技术分析，为案件的成功侦破提供了关键证据。

案件背景

在电商直播日益流行的今天，一种以“虚假流量”为手段的新型网络诈骗正在悄然兴起。不法团伙打着“流量高变现快”的旗号，伪装成传媒公司，炮制流量骗局。沈先生经营着一家美妆实体店，他偶然刷到一条短视频，声称只需 3000 元就能让一条普通的短视频获得几十万的观看量。然而，虽然观看量迅速增长，但实际的营销效果却未能达到预期。沈先生的疑惑并非个例，警方在工作中接到多起类似举报，经过调查发现这些异常流量背后，隐藏着一个利用短视频流量推广、疯狂吸金的“骗局”。

由于涉案团伙分散在各个窝点，证据可能会被迅速销毁，这就需要警方采取同步高效的打击和取证行动。同时，揭露“刷流量”背后的犯罪手法也需要专业人士的协助。

洞鉴解决方案

01 案中：多窝点配合打击，确保证据完整可靠

1. **现场设备提取：**奇安信司法鉴定的技术团队被迅速召集，支援警方取证固定，对多个窝点数百部手机与电脑主机设备进行了数据提取。提取的数据包括非法刷量脚本程序、操作记录，以及与犯罪活动直接相关的通讯数据。

2. **数据镜像固定：**对这些电子设备实施了全面的数据镜像固定，确保了证据的完整性和可靠性，为后续的法律程序打下了坚实的基础。

案发现场照片

02 案后：专业司法鉴定，明确刷量脚本工作原理

针对现场设备中提取的非法刷量脚本，鉴定人对其进行了功能性鉴定，具体步骤如下：

1. **搭建仿真环境：**在虚拟机中加载检材文件，并通过配置 nginx 和启动 renren-admin.jar 程序，创建与实际环境相似的测试环境，为功能验证提供可靠基础。
2. **分析脚本程序：**运行脚本文件后，观察程序的启动过程和日志输出，查看和分析主程序运行过程中生成的日志文件。特别关注与设备注册和视频播放量增加相关的日志记录，结果发现该程序具备生成虚假的数字身份和签名，误导短视频平台，从而增加视频播放量的功能。
3. **功能验证与数据监控：**在短视频平台上创建测试视频，记录初始播放量，运行刷量脚本文件，并监控视频播放量的变化，验证程序确实具有增加短视频平台视频播放量的功能。

案例价值

01 / 确保证据完整可靠

对现场大量电子设备进行了数据提取和镜像固定，每一步操作都严格遵循技术规范，确保了证据在司法程序中的有效性和完整性。

02 / 维护合法权益

通过详细的程序分析和数据对比，明确了刷量脚本的工作原理，揭露了刷量团伙的违法行为。这有助于保护短视频平台和广告商的合法权益，防止欺诈行为的进一步蔓延。

03 / 促进行业健康发展

通过严谨的鉴定手段，有效遏制了虚假流量的泛滥，维护了网络环境的健康发展，为创作者和平台提供了一个更加公平和有序的网络生态环境。

电商平台刷单案

数十万条订单数据固定分析，揭露虚假销量骗局

本案涉及一个大型刷单平台的司法鉴定。在涉案平台上，商家提出刷单需求，另一些用户则接单完成虚假订单操作，通过对平台数据库的提取和详细分析，奇安信洞鉴识别并提取了大量涉及刷单的虚假交易记录和用户信息，为案件侦破提供了关键的证据支持。

案件背景

2023年，某地在日常巡查中发现，某电商平台上存在大量刷单行为。刷单行为包括一些商家通过发布刷单需求，吸引用户接单，通过虚假交易提升店铺销量、好评等指标。这些行为涉嫌扰乱市场秩序，公安机关根据初步调查，认定此行为可能涉及非法经营，遂委托奇安信洞鉴对涉案平台数据进行分析和证据提取。

洞鉴解决方案

1. 数据提取与镜像固定

鉴定团队首先对检材硬盘进行了完整的镜像提取，以确保数据的完整性不受任何影响。通过对镜像分析，团队成功提取了平台数据库中的交易记录、用户信息、账户明细、充值和提现记录等核心数据。这些数据是还原案件全貌的关键，能够清晰展现刷单团伙的作案手法和资金流动路径。

2. 数据库恢复与仿真重建

使用虚拟机软件“VMware Workstation”搭建了 CentOS 7 系统环境，配置 MySQL 数据库环境，恢复了平台的数据库备份文件。恢复数据库后，通过宝塔面板和 VMware 虚拟机仿真平台运行环境，重建平台管理系统，模拟实际运行的电商平台操作流程。在仿真环境中，成功访问并还原了平台的后台管理系统，重现了虚假交易和刷单操作的全过程。

3. 会员与商家数据分析

使用 SQL 语句提取平台内所有会员及商家的详细信息，包括注册时间、登录记录、账号状态及交易记录，重点分析了商家发布的刷单需求和会员接受刷单任务的行为。通过提取数据库表，导出了刷单商家与参与刷单会员的详细信息，包括会员的账户信息、注册时间、登录记录及账户余额等关键数据。

4. 虚假交易记录分析

针对刷单行为，重点分析了购物返利订单和免费试用订单的交易记录。筛选出大量虚假交易数据，并区分不同订单状态（例如：失效、已抢购、已关闭等），确认了商家通过发布虚假交易订单提高销量、好评等操作。特别是“已完成状态的购物返利订单”，共导出了 6 万多条记录，订单总金额近两百万元，成为刷单行为的重要证据。

客户价值

01 / 揭示虚假交易链条

通过对涉案平台的数据库进行深入提取和详细分析，奇安信洞鉴成功识别并固定了数万条虚假订单数据，为电商平台提供了确凿的证据支持，有效打击了扰乱市场秩序的虚假交易行为。

02 / 强力技术支撑

重建了涉案平台的操作流程，成功复现了刷单操作的全过程。这一过程清晰展现了商家如何通过发布虚假订单和交易记录提升销量和好评指标，为公安机关侦破案件提供了关键的技术证据支持，极大提高了案件侦破的效率。

03 / 强化平台风控

帮助平台识别了刷单团伙的作案模式，帮助电商平台优化风控策略，提升平台对虚假交易的识别与应对能力，避免类似问题的再发生，助力平台长远健康发展。

05

COLLECT WOOL
薅羊毛

薅羊毛原指用户通过合理手段利用平台的优惠活动获取利益，而如今，随着技术的进步和平台漏洞的出现，不法分子利用漏洞、规则缺陷及自动化工具，非法获取远超正常用户权益的利益。这种行为不仅给平台造成经济损失，还影响其信誉和正常用户体验。薅羊毛行为已逐渐演变为一种黑灰产的常见手段，具备高度组织化和技术化的特征。

1. 常见场景

优惠券滥用

通过自动化工具，批量领取平台发放的优惠券，甚至获取内部优惠券链接进行大规模违规操作。优惠券可能被倒卖或用于不正当交易，平台利益因此受损。通常表现为利用脚本自动注册大量新用户账号领取专属优惠，或利用平台漏洞批量生成超额优惠券。

多账户注册套利

借助技术手段批量注册平台账户，以获取新用户专属的优惠或试用权益。这些账号往往被打包出售或用于套利。例如，在视频、音乐等平台批量注册，获取免费试用会员资格后转售，破坏了平台正常的商业生态。

自动抢红包

使用抢红包软件或脚本，在极短时间内自动参与各类平台的红包活动，抢占正常用户应享的福利。这类软件能通过模拟用户操作，在毫秒内完成抢夺，远超普通用户的响应速度，导致普通用户几乎无法竞争。

骗取推广佣金

不法分子利用虚假流量或技术手段伪造点击和注册行为，骗取平台的推广佣金。此类行为常见于网络平台的拉新活动或按点击付费的推广机制。不法分子通过虚假点击、批量注册账号或私自替换推广链接等手段，伪造推广效果，导致平台根据虚假数据发放佣金，严重影响了广告投放的准确性和效果评估。

技术原理

1. 漏洞利用: 不法分子深入研究平台的业务逻辑和规则设计，寻找可被利用的漏洞。例如，优惠券生成机制中的编号规律、用户认证过程中的验证缺陷等。一旦发现漏洞，便可反复利用，获取大量不当利益。

2. 自动化脚本: 使用编程技术编写自动化脚本，模拟人工操作，实现批量、高速的重复性任务。例如，快速注册大量新账号、自动领取优惠券、自动参与平台活动等。这些脚本通常绕过了平台的安全检测，使得异常行为难以及时被发现。

2. 取证鉴定思路

薅羊毛案件是指不法分子利用平台的漏洞或规则缺陷，通过技术手段和自动化工具，大规模非法获取利益的行为。此类案件具有操作隐蔽、技术复杂、影响广泛等特点。针对薅羊毛案件的取证与鉴定，需要从企业初步应对、证据固定、渠道排查、漏洞修复、证据收集到后续的功能性鉴定等多个环节进行系统化的处理。

以下是具体的取证鉴定思路：

1 企业应急措施与初步调查

当企业发现薅羊毛行为后，需立即采取紧急措施，例如停止新用户注册、暂停优惠券发放、限制异常账户的交易等，防止不法分子继续利用漏洞获利，并开始初步调查。

业务逻辑审查： 企业内部技术团队或鉴定机构协助，深入了解平台的业务流程和规则，查找可能被不法分子利用的漏洞或规则缺陷。

数据分析： 初步分析平台的运营数据，识别异常的账户活动、交易记录和系统日志，为后续调查提供线索。

2 证据固定与渠道排查

在采取紧急措施的同时，需要对薅羊毛相关的证据进行固定，确保后续法律程序中证据的有效性。

日志数据保存： 备份服务器日志、数据库日志、应用日志等，保存与薅羊毛行为相关的注册、登录、领取优惠券、下单、支付等操作记录。对日志文件生成哈希值，确保其完整性和不可篡改性。

网络渠道取证： 在电商平台、二手交易平台（如闲鱼）等公开渠道，搜索不法分子可能发布的售卖链接、优惠券等信息。对相关网页、帖子、聊天记录进行公证或区块链存证，固定证据。

账户信息收集： 收集不法分子使用的账号 ID、联系方式（如微信号、手机号）、交易记录等信息，为后续公安机关调取证据提供线索。

3 异常行为识别与数据分析

通过识别高频的异常操作模式以及分析批量注册的账户信息，确定不法分子的自动化操作和资金流动路径，为进一步分析提供数据支持。

批量注册与账户分析： 检测短时间内大量注册的新账户，分析注册信息（如手机号、邮箱、设备指纹）是否存在重复、虚假或异常情况。关联账户的 IP 地址、设备信息，识别可能由同一设备或网络操作的多个账户。

高频操作与行为模式分析： 统计账户的操作频率，识别短时间内大量重复操作的账户，如频繁领取优惠券、下单、支付等。分析多个账户的操作步骤、时间间隔和行为序列，判断是否存在高度一致的自动化操作特征。

网络特征与地理位置分析： 检查账户登录和操作的 IP 地址，识别使用代理 IP、VPN 等手段隐藏真实位置的情况。通过 IP 地理位置数据，发现账户登录地点的异常变动，如短时间内跨地区登录。

4 功能性鉴定与技术分析

在公安机关抓获犯罪嫌疑人后，需要对其使用的薅羊毛工具进行功能性鉴定和技术分析，揭示其作案原理和过程。

设备数据提取： 在合法授权下，对嫌疑人使用的电脑、手机、存储设备等进行数据提取，获取薅羊毛工具、自动化脚本等。

漏洞复现： 在受控的测试环境中，使用薅羊毛工具复现不法分子的作案过程，验证工具对平台漏洞的利用方式。

代码分析： 对薅羊毛工具的源代码或反编译代码进行审查，识别其与平台交互的具体实现方式，如接口调用、参数构造等。

5 非法获利统计与资金流向追踪

准确计算不法分子的非法获利金额，追踪资金流向，为案件定性和量刑提供依据。

非法获利金额统计： 统计被非法领取和使用的优惠券数量、面值，计算平台的直接经济损失。分析异常账户的订单记录，核实订单金额、支付方式、收货地址等信息，评估不法分子通过虚假交易获取的利益。

资金流向追踪： 与支付平台、银行合作，获取涉案账户的交易记录、资金流水，追踪资金流动路径。分析资金往来，识别关联账户，发现不法分子的资金链和利益分配关系。检查不法分子是否通过提现、转账等方式将非法获利转移，识别资金最终去向。

6 鉴定意见书与证据链完善

最终，鉴定工作需形成一套完整、严谨的证据链，确保所有证据均符合司法标准，并可以支持后续的法律诉讼。

多源证据整合： 将平台数据、网络流量、支付记录等多种来源的证据进行整合，确保证据链的连续性。

时间线重建： 通过时间戳重建操作过程的时间线，展示整个薅羊毛行为的发生、发展过程。

3. 典型案例

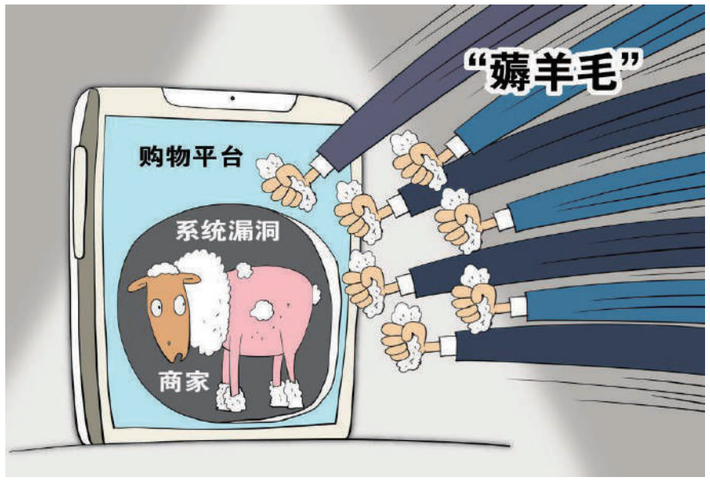
优惠券盗领案

抓包伪造请求反复领券，揭开黑客大规模套利真相

2024 年，上海某知名餐饮品牌的自助点餐小程序因安全漏洞被黑客非法获取大量 0 元兑换券，并大规模发放给非储值用户，造成了超过 221 万元的经济损失。奇安信洞鉴在警方委托下，对嫌疑人设备中的两款程序进行了详细的司法鉴定，揭示了黑客通过抓包技术和伪造请求反复领取免费券的作案手法，为案件的侦破提供了关键证据支持。

案件背景

2024 年 2 月 19 日，某知名餐饮品牌的自助点餐小程序因优惠券被非法领取事件登上热搜。原本属于储值用户专享的免费套餐券，因不明原因被大量发放至非储值用户，引发了大规模的抢券潮。经过内部调查，发现自助点餐小程序存在严重安全漏洞，导致优惠券被非法领取。



在这场抢券风波中，警方发现有不法分子利用技术手段，通过自动化程序批量领取了大量优惠券，并将其在网络平台上倒卖牟利，造成了严重的经济损失和品牌声誉的受损。为全面掌握案件的具体情况及技术细节，警方委托奇安信洞鉴对涉案设备及相关程序进行深入的电子数据司法鉴定。

洞鉴解决方案

程序反编译：通过详细的代码分析，鉴定人员还原了该程序的作案逻辑及其功能模块。

1. 鉴定人员对嫌疑人设备中的两款程序“*** 抓包 .exe”和“***V1.0.exe”进行了反编译分析。通过对“*** 抓包 .exe”程序的代码分析发现，该程序能够通过抓包技术截获微信小程序的网络请求，提取其中的 session_id 等身份验证信息。进一步分析显示，程序利用抓取的 session_id 信息生成伪造的用户身份，从而实现后续非法操作。

2. 而另一款程序“***V1.0.exe”则通过反编译确认，具备循环发送 POST 请求的功能。该程序会将“*** 抓包 .exe”截获的 session_id 和特定店铺编号 store_id 作为参数，向小程序的优惠券领取接口发送伪造请求。每次请求成功后，服务器都会返回一张新的优惠券，这种反复操作导致优惠券被大规模非法领取。

动态功能验证：鉴定人员在隔离的虚拟机环境中复现了嫌疑人的操作过程，进一步确认了相关程序具备批量、循环领取优惠券的功能，为警方查明嫌疑人作案手法及非法获利提供了有力的技术证据。

1. 首先，鉴定人员运行“*** 抓包 .exe”程序，成功拦截到小程序的网络请求数据，记录了其中包含的 session_id。接着，运行“***V1.0.exe”程序，将获取到的 session_id 和店铺编号 store_id 输入程序中，并模拟了多次领取优惠券的操作。

2. 通过抓包工具对程序与服务器之间的网络流量进行监控，发现程序能够绕过验证机制，多次成功领取优惠券。每次发送请求时，系统均返回一张新的优惠券，表明该程序能够在不受限制的情况下，反复利用伪造的身份信息请求优惠券。

客户价值

01 / 提供关键证据支持

鉴定人员通过深入分析涉案程序和漏洞复现，全面还原了犯罪嫌疑人利用程序漏洞批量领取优惠券的作案手法，为警方提供了有力的技术证据，确保了案件侦破过程中证据链的完整性和法律效力。

02 / 减少潜在经济损失

鉴定工作明确揭示了小程序存在的安全漏洞及其被利用的具体方式，帮助品牌方迅速采取措施关闭漏洞，避免了更多优惠券被非法领取。

03 / 提升案件侦办效率

通过专业的技术鉴定工作，快速揭示了作案手法和细节，为警方在短时间内厘清案件脉络、掌握嫌疑人行为模式提供了重要线索，显著提高了侦办效率，为案件的快速侦破和法律定性奠定了坚实基础。

刷“试用账号”牟利案

多方研判锁定不法行为，助力警方侦破大规模薅羊毛案件

该案件中，不法分子通过批量注册和售卖游戏加速器的试用账号，绕过企业验证机制，非法牟利约 50 万元。奇安信洞鉴团队利用其专业的鉴定和研判能力，对案件中涉及的多台服务器、硬盘、手机及相关数据进行了全面的司法鉴定分析，揭示了不法分子的具体操作手法，最终协助警方锁定犯罪嫌疑人，成功侦破案件。

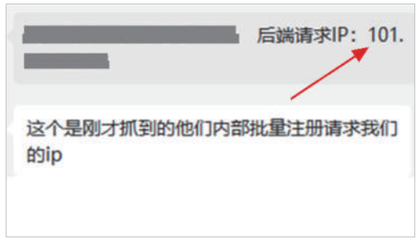
案件背景

2023 年初，某企业发现，其加速器的体验卡被不法分子通过淘宝店低价售卖。犯罪团伙利用接码平台和代理 IP 绕过企业的验证系统，批量注册虚假账号并进行充值，导致企业蒙受约 50 万元的经济损失。

在企业报警后，警方展开初步调查，发现犯罪团伙的作案手段新颖且技术复杂，使用了多台服务器和多个虚拟身份来规避追踪，取证和分析工作难度较大，委托奇安信洞鉴进行研判与鉴定分析工作。

洞鉴解决方案

01 案前研判：锁定犯罪线索



1. **调证建议：**奇安信洞鉴团队协助警方对三个可疑 IP 进行了详细的分析和研判，确定可疑 IP 对应服务器类型，并给出调证建议。
2. **分析研判：**综合多台服务器的日志和操作记录，团队成功锁定了不同犯罪团伙的活动轨迹和分工模式，并初步确定了这些服务器的运营性质和可能的关联性，为后续的取证提供了方向。

02 案中取证：锁定关键证据

1. **设备数据固定：**对多台涉案手机、平板、台式机等设备的微信、QQ、支付宝数据进行了提取和备份，特别是从聊天记录、交易记录中提取了大量关键证据数据。
2. **服务器数据提取：**对多台服务器的镜像文件进行数据提取和还原，恢复了服务器中的运行日志、操作记录及数据库信息，为案件侦查提供了重要的线索。

03 案后鉴定：还原作案手法

程序功能性鉴定

奇安信洞鉴对注册账号程序的核心功能模块进行了逐一解析，发现该程序包含以下关键功能：

1. **接码平台登录与验证码获取：**程序支持多个接码平台登录，通过调用不同平台的 API 接口进行手机号获取和登录操作。
2. **批量注册与解锁操作：**程序能够根据输入的解锁码和手机号，通过调用加速器平台的 API 接口，实现批量注册和解锁操作。
3. **账号信息导入与管理：**程序通过访问指定后台管理系统，能够批量导入注册成功的账号信息，包括手机号、密码、解锁码等，并将这些信息同步至远程服务器。这一功能使不法分子能轻松管理大量虚假账号，实现对这些账号的集中控制和操作。

在实际验证中，鉴定团队模拟了不同接码平台环境，测试了程序的自动化操作能力。验证结果显示，程序能够成功获取虚拟手机号，并在不同平台上实现自动化注册。通过对验证码处理和批量操作的测试，确认了该程序能够在无人工干预的情况下自动完成批量账号的注册、解锁和管理操作。

服务器数据分析

奇安信洞鉴登录后台管理页面，提取并恢复了数据库中的账号信息、操作日志和充值记录，确认了虚假账号的生成和批量充值行为。

1. **自动化数据固定：**鉴定人员编写 Python 脚本，自动遍历并固定后台管理系统的所有日志页面，将 118 个页面的数据保存为独立的 html 文件，确保数据完整无遗漏。
2. **数据提取与整理：**编写数据提取脚本，逐一读取 118 个 html 文件中的内容，通过正则表达式精准提取账号和密码信息。
3. **数据清洗统计：**对提取数据进行清洗与规范化处理，包括去除重复记录和无效数据，并合并同一账号的分散信息等，最终提取到 2086 条有效记录，详细记录了后台系统中的账号和密码信息。

客户价值

01 / 明确案件侦查方向

从前期研判到中期取证，再到后期鉴定，全程协助警方锁定不法分子的操作手法，精准引导案件侦查方向，显著提升了侦破效率。

02 / 提供关键电子证据

提供了包括程序功能鉴定和服务器账号数据在内的多种关键证据，全面揭示了不法分子的批量注册和管理方式，为案件提供了完整的证据链。

03 / 遏制非法行为

揭露并阻止了不法分子利用虚假账号非法牟利的行为，帮助企业堵住系统漏洞，挽回经济损失，维护了企业的合法权益和市场声誉。

外挂抢红包案

科技维权：深度剖析“抢红包”外挂，推动优质用户体验提升

2021 年，一家知名企业发现部分用户利用外挂程序，自动化地在各个直播间抢红包并进行提现。这损害了其他正常用户的权益，因此，委托奇安信司法鉴定对其外挂程序进行鉴定。鉴定人对这款疑似外挂程序进行了深入的逆向分析，最终确认了其 " 抢红包 " 的原理及功能。这次鉴定的结果不仅为企业揭示了事实真相，也为维护平台的公正秩序起到了重要的作用。

案件背景

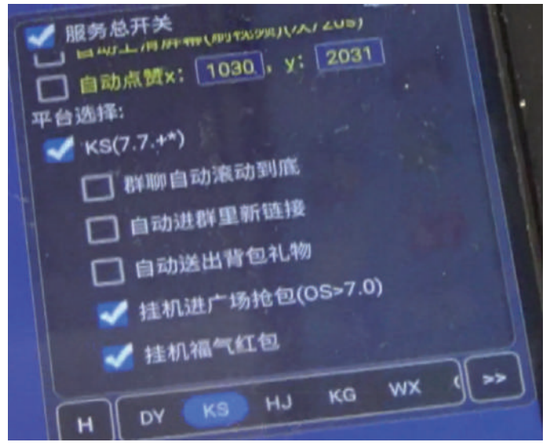
2021 年，该企业发现 5 个账户利用多台手机设备，通过外挂程序在各个直播间轮流抢主播发的红包近 2 万元，抢到的红包再集中打赏给某主播提现。这一行为严重扰乱了平台的秩序，影响了用户体验，该企业立即报案，并寻求专业的电子数据司法鉴定对相关外挂程序进行深入剖析。

洞鉴解决方案

鉴定人通过动静结合的方式，对涉案外挂程序进行了深入剖析，具体步骤如下：

1. 功能动态复现

鉴定人在一台手机上安装该应用程序并运行，确认其具备“挂机进广场抢红包”与“挂机福气红包”这两个功能，开启后，手机会自动打开涉案直播平台的直播广场，并自动寻找可领取红包的直播间执行抢红包操作。



代码反编译

2. 程序逆向分析

鉴定人对该外挂程序的 APK 文件进行了反编译后，获取了相关源代码，经过进一步分析发现了其抢红包的底层原理。

具体而言，该应用首先获取了涉案直播平台的非公开 ID，通过遍历界面元素并判断元素的文本、ID 等属性，可确认页面状态，例如是否存在红包、是否存在倒计时、是否需要关注主播抢红包等；然后，该应用通过辅助功能服务查找这些控件 ID 对应的元素，并对这些元素进行模拟点击，实现抢红包、切换直播间、关注主播等操作。

案例价值

01 / 提升用户体验

在面临非法抢红包行为破坏平台公正、公平的环境时，我们提供了专业的电子数据鉴定服务，协助企业成功打击了相关非法软件，提升了平台的用户体验。

02 / 维护平台秩序

通过剖析该外挂程序的工作原理，为该企业提供针对性的技术建议。这使得企业能够采取有效措施，防止类似的非法行为再次发生，从而维护了平台的公正秩序。

03 / 维护商业利益

本次司法鉴定不仅帮助客户理解了涉案应用的工作机制，同时也为法律程序提供了关键的证据，帮助企业能够依法维权，对抗非法抢红包行为对其商业利益的损害。

骗取推广佣金案

千万元佣金被骗！详解非法推广链接生成机制

近日，一家知名电商平台发现，其大量佣金被一家第三方代发货平台通过不正当手段骗取。该平台利用非法技术手段，在商品链接中加入返利代码，将原本属于商家和推广者的佣金转入自己的账户。经过深入调查，奇安信洞鉴对该代发货平台的运作模式进行了详细分析，为查明真相提供了关键技术证据。

案件背景

某电商平台为商家提供推广计划，允许其通过分享商品链接来推广产品，并支付相应的推广佣金。然而，一家第三方代发货平台通过滥用这一推广机制，非法获取大量佣金。

该代发货平台的主要运作模式如下：商家在电商平台 A 开设店铺，但自身没有库存或货源。商家在收到订单后，通过该代发货平台，将订单同步到电商平台 B，寻找价格更低的同款商品并下单发货。

然而，代发货平台在商家下单的过程中，悄悄将电商平台 B 的商品链接替换为带有返利代码的链接。这样，代发货平台通过返利网站将本应属于商家的推广佣金转入自己的账户。此行为不仅导致商家损失佣金，还严重破坏了平台的推广生态。

洞鉴解决方案

1. 静态代码审查：

鉴定专家对涉案软件的源代码进行了细致审查，特别关注了涉及商品 ID 获取、处理及链接生成的关键函数和模块。通过这一过程，鉴定专家揭示了软件生成针对特定推广平台的链接的原理。

2. 篡改机制分析

通过对软件运行时的网络请求进行监控，鉴定专家捕获并分析了软件与外部服务器之间的通信数据。通过分析软件发出的 POST 请求及其收到的响应内容，发现软件利用特定 API 请求参数和 URL，从推广平台获取商品的 URL 列表。进一步的分析确认，软件能够基于获取到的商品 ID，在推广平台上查询对应的推广 ID，并将这些 ID 替换入原推广链接中，制作出被篡改的推广链接。

3. 动态功能验证

在受控的测试环境中安装并运行该软件，鉴定专家模拟了软件的实际使用场景，复现了其核心功能——自动生成并使用篡改过的推广链接完成商品销售。这一过程直观地展示了软件如何非法获取推广佣金，为软件的欺诈行为提供了直接证据。

通过静态代码分析、篡改机制解析和动态功能验证，奇安信洞鉴明确揭示了该代发货平台的欺诈模式。代发货平台通过篡改商家订单链接的方式，非法获取平台推广佣金，为电商平台提供了强有力的技术证据，支持其采取法律行动追究相关责任，维护正常的商业秩序。

客户价值

01 / 提供关键证据

通过深入分析和鉴定，奇安信司法鉴定为电商平台揭示了非法软件的具体操作机制，提供了确凿证据，为平台维护合法权益和遏制非法行为奠定了坚实基础。

02 / 增强防范能力

鉴定过程中对非法软件的机制进行了深度剖析，这有助于电商平台识别并防范类似的非法入侵和滥用行为，优化自身的安全策略和技术防护措施。

03 / 维护市场秩序

成功打击此类非法软件，对其他可能存在的或潜在的非法行为产生震慑效应，有助于构建更加公正和有序的市场环境，保护诚信经营的商家和推手的合法权益。

打击策略

案前

线索挖掘

数据筛查

- 日志分析（访问、操作、错误日志）
- 网络流量异常检测
- 用户行为分析

识别异常行为和潜在线索

关联分析

- 多账户关联分析
- 设备指纹比对
- IP 地址分析

确定疑似涉案账户和设备关联性

案中

取证分析

数据提取

- 密码破解
- 设备取证
- 数据恢复
- APP / 网站取证
- 服务器取证

从设备和系统中提取关键证据数据

数据分析

- 资金流追踪
- 数据库和设备日志
- 多账户关联分析
- 文件和代码相似性比对

通过数据分析形成证据链

案后

证据梳理

司法鉴定

- 相似性比对
- 功能性鉴定
- 恶意代码分析
- 网络数据行为分析

对取证数据进行科学分析与司法鉴定

出庭质证

- 解释鉴定意见
- 阐述技术原理
- 论证证据合法规范

确保证据在法庭上的合法性和可采性

1. 线索挖掘

案前：线索挖掘

黑灰产案件发生后，及时、准确地挖掘线索对于后续的调查和打击至关重要。通过综合运用流量检测、用户行为分析、设备指纹比对等方法，结合日志、流量、IP 地址等技术手段，能够迅速锁定涉案账户和设备，为案件侦破奠定坚实基础。

一、黑灰产线索排查方法

1 网络流量异常检测

- **流量峰值与来源检测：**首先，对事件发生时段的网络流量进行回溯分析，检测是否存在异常的流量峰值和集中访问行为。重点关注流量的地理来源、访问频次，以及与正常流量的差异。这有助于初步判断异常活动的规模和可能的来源。
- **高频访问与行为重复性：**统计高频次的访问行为，识别在短时间内频繁执行相同操作的账户或设备。例如，某些账户是否在短时间内频繁访问同一页面或执行特定功能，操作间隔是否异常短。这些迹象可能表明自动化脚本或批量操作的存在。

2 用户行为分析与关联检测

- **操作路径比对：**提取可疑用户的操作路径，分析其与正常用户行为模式的差异。例如，是否存在异常的操作顺序、频繁触发特定功能、快速切换页面等行为。这有助于识别潜在的黑灰产操作手法。
- **账户关联分析：**利用账户之间的行为特征、设备信息、IP 地址等，分析不同账户之间的关联性。通过交叉比对登录时间、访问设备、支付方式、地理位置等，识别是否存在批量注册、协同操作的关联账户群体。

3 IP 和设备指纹分析

- **IP 异常与代理使用识别：**追踪账户访问的 IP 地址，分析地理分布和登录频次。关注是否存在频繁的跨区域登录、使用代理 IP 等异常行为。例如，同一账户是否在短时间内从不同地区登录，多个账户是否集中使用相似的 IP 段。
- **设备指纹比对：**将同一设备上操作的不同账户进行比对，识别是否存在多账户在同一设备上的异常登录行为。这有助于锁定黑灰产操作背后实际控制的设备，形成进一步证据支持。

4 数据接口与访问记录追溯

- **数据端点与接口访问监测：**在数据泄露或爬取的案件中，通过回溯敏感数据端点的访问记录，识别出频繁访问的异常账户或设备。特别是针对某些特定数据接口的集中调用，可以定位异常数据访问行为的来源。
- **访问日志与操作顺序分析：**分析访问日志，查找操作顺序是否异常，如连续批量查询、导出特定数据。此类行为通常用于识别数据盗取或恶意爬虫活动，为后续的取证与溯源提供有力支持。

二、技术手段与工具

1 日志分析

日志记录了用户的操作痕迹，是识别黑灰产活动的重要依据。通过日志分析，可以发现用户在系统中的具体行为路径、登录时间和频率、操作命令等信息。

功能

自动收集并分析访问日志、操作日志和错误日志，识别异常行为和高频访问。

适用场景

适合监测账户登录异常、批量数据导出操作、接口频繁调用等情况。

工具示例

Graylog、Elastic Stack

2 流量监控

流量监控工具用于捕获和分析网络流量，帮助识别流量异常峰值和来源，追踪可能的恶意流量行为。

功能

能够监控实时流量、分析访问频次、追踪流量来源，识别出异常流量模式和 IP 分布。

适用场景

在虚假流量、薅羊毛、数据爬取等黑灰产活动中，流量监控可以快速定位异常流量峰值和来源。

工具示例

Cacti、Wireshark

3 犯罪情报分析

集成多种情报资源和数据处理技术，帮助深入挖掘和关联黑灰产线索。

功能

整合多源数据，自动化关联分析，挖掘潜在的关联关系和关键节点。

适用场景

跨平台案件分析、涉案人员关系图谱构建、黑灰产团伙识别等。

工具示例

奇安信威胁情报中心
奇安信星源网络犯罪情报平台

2. 取证分析

案中：证据固定与分析

在打击黑灰产活动的过程中，取证分析是关键环节。黑灰产案件具有技术手段复杂、隐蔽性强、更新速度快等特点，给取证工作带来了特殊的挑战。为此，取证分析需要针对黑灰产的特性，确定取证范围和重点，采用专业的取证技术和规范的流程，确保获取的证据具有合法性、完整性和有效性，为后续的法律诉讼和打击工作提供有力支持。

一、取证范围和重点

1 取证范围的确定

在黑灰产案件中，取证范围需要综合考虑其技术特点和行为模式，主要包括：

- **涉案设备：**包括计算机、服务器、移动设备等，可能存储着黑灰产活动的直接证据，如非法程序、数据文件、配置文件等。
- **网络数据：**网络通信数据、流量日志、访问记录等，反映黑灰产活动的网络行为和数据交互情况。
- **应用和系统日志：**系统日志、应用日志、错误日志等，记录了系统和应用的运行状态和异常事件。
- **数据和数据库：**涉及的数据库文件、数据备份、配置数据等，可能包含黑灰产活动的数据支持和操作记录。
- **资金交易记录：**与黑灰产活动相关的支付记录、转账信息、虚拟货币交易等，反映资金流向和经济利益链条。

2 取证重点的确定

针对黑灰产活动的特点，取证工作应重点关注以下方面：

- **技术手段的证据：**黑灰产活动常利用高超的技术手段，需要获取其使用的程序、工具、脚本等，分析其工作原理和功能。
- **行为模式的证据：**通过对操作行为、网络行为、数据访问的分析，识别异常模式和特征，揭示黑灰产活动的行为规律。
- **关联关系的证据：**黑灰产从业者往往采用多账户、多设备协同操作，需要通过关联分析，揭示账户之间、设备之间的关联性。
- **数据篡改和破坏的证据：**黑灰产活动可能涉及对数据的篡改、删除，需要通过数据恢复和完整性验证，获取被破坏的证据。
- **资金流动的证据：**追踪黑灰产活动的资金流向，获取相关的交易记录，揭示经济利益链条。

二、取证技术与流程

1 数据恢复

- **应用场景：**当涉案人员删除、格式化或损坏了关键数据，需要进行数据恢复，获取被删除的证据。
- **技术方法：**使用 R-Studio、GetDataBack、DiskGenius 等数据恢复工具，对硬盘、移动存储设备、内存等介质进行扫描，恢复被删除的文件、分区和数据。

2 密码破解

- **应用场景：**当涉案设备、文件或数据库被加密，需要破解密码以获取内容。
- **技术方法：**使用 Hashcat、John the Ripper 等密码破解工具，采用字典攻击、暴力破解、彩虹表等方法，结合社会工程学手段，提高破解效率。

3 设备取证

- **应用场景：**获取涉案计算机、服务器、移动设备中的数据。
- **技术方法：**使用盘古石计算机取证分析系统、盘古石手机取证分析系统、盘古石星探网络取证系统等系列取证产品，对设备进行物理或逻辑取证，制作镜像，提取文件系统、注册表、日志、通信记录等，确保数据的完整性和可靠性。

4 网络取证

- **应用场景：**分析黑灰产活动的网络行为，获取通信数据和网络流量。
- **技术方法：**使用 Wireshark、Fiddler 等流量分析工具，捕获并分析网络流量数据，提取网络通信协议、数据包内容、访问的 IP 地址和端口等信息。

5 多账户关联分析

- **应用场景：**识别多个账户之间的关联，揭示幕后操控者。
- **技术方法：**比对账户的注册信息、登录 IP、设备指纹、操作行为、支付方式等，利用数据分析和关联分析工具，构建账户关联图谱。

6 文件和代码相似性比对

- **应用场景：**检测代码抄袭、侵权、恶意程序传播等。
- **技术方法：**使用 Beyond Compare、Bindiff 等相似性检测工具，计算文件或代码的相似度，识别抄袭或篡改行为。

7 资金流追踪

- **应用场景：**追踪黑灰产业活动的资金链，发现资金流向和洗钱行为。
- **技术方法：**获取银行、支付平台、虚拟货币交易记录，构建资金流转图，使用千手千眼话账单分析系统、链必追 - 虚拟货币案件智能研判平台等资金分析工具，识别关键账户和资金去向。

3. 证据梳理

案后：证据整理、司法鉴定与法律支持

在打击黑灰产案件的过程中，证据整理是连接技术取证与法律诉讼的关键环节。通过专业的司法鉴定和出庭质证，将复杂的技术证据转化为具有法律效力的证据，为法院准确认定案件事实提供有力支持。

一、司法鉴定

1 司法鉴定的作用

黑灰产案件涉及复杂的技术手段和高级的对抗性技术，这使得证据的专业鉴定成为必要。

- **确认证据的合法性和真实性：**通过司法鉴定，验证取证过程和证据本身的合法性，确保未受到篡改或污染，满足法律要求。
- **解释复杂的技术问题：**将技术取证中涉及的复杂技术原理、方法和结果，以法律认可的形式进行阐述，便于法庭理解。
- **支持证据链的完整性：**通过鉴定，证明证据之间的关联性，确保证据链条的连续和完整。

2 司法鉴定的重点内容

相似性比对

- **目的：**确定涉案文件、程序代码的相似程度，证明侵权或非法行为。
- **方法：**利用哈希算法、代码指纹、特征码提取等技术，对比文件或代码的相似性。例如，使用 MD5、SHA256 等哈希函数计算文件指纹，或采用代码相似性分析工具进行比对。
- **法律意义：**证明被告所使用的代码或程序与原告的作品具有实质性相似，支持侵权指控。

功能性鉴定

- **目的：**确认涉案软件、工具是否具备非法功能，如游戏外挂、数据窃取、未授权访问等。
- **方法：**通过静态分析和动态调试，对软件的功能进行深入解析。静态分析包括查看代码结构、函数调用、配置文件等；动态调试则是在受控环境中运行程序，观察其行为、系统调用、网络通信等。
- **法律意义：**证明涉案软件具备非法功能，违反相关法律法规，为定罪量刑提供依据。

恶意代码分析

- **目的：**在网络入侵、数据泄漏等案件中，分析恶意代码的危害性。
- **方法：**对恶意代码进行逆向工程，分析其加密方式、混淆手段、攻击载体和攻击目标。
- **法律意义：**明确恶意代码的危害程度，评估对受害方造成的损失，支持法律诉讼。

网络数据行为分析

- **目的：**适用于识别爬虫活动、批量数据抓取和非法数据窃取。
- **方法：**对网络流量进行捕获和解析，使用协议分析工具（如 Wireshark）解码数据包，重建通信内容。识别异常的流量模式、异常请求频率、数据传输量等，以判断是否存在批量数据抓取、恶意流量或异常访问行为。
- **法律意义：**通过数据行为分析，证明涉案人员在未经授权的情况下实施批量抓取、数据窃取等行为，非法获取和滥用信息资源，侵犯平台数据权利并干扰正常业务运营。

二、专家意见

专家辅助人可出具书面意见，将技术取证过程中的复杂分析结果，清晰、有条理地呈现给法庭，能够增强证据的说服力。与司法鉴定不同，专家辅助意见的灵活性较高，尤其适用于主观性较强、依赖经验判断的技术分析。

1 适用性

- **证明具体技术事实：**专家辅助意见可以明确涉案技术行为的具体细节，例如说明某软件具备爬虫功能、批量数据抓取等特性，或确定某恶意代码的特定运行环境和目标。
- **主观性判断：**对于黑灰产行为的技术特征，如多账户控制、批量化操作模式等，专家辅助意见可以结合实际案例和专业经验，判断该行为是否符合黑灰产的典型特征，为法庭决策提供参考。

2 内容重点

- **技术手段的事实性说明：**明确黑灰产案件中涉案技术手段的性质及功能。例如，说明某程序的运行代码是否具备自动化批量数据抓取能力，或是否有恶意控制的远程操作行为。
- **技术行为的特征分析：**通过日志、流量、代码等数据，揭示该行为在黑灰产活动中的常见模式。例如，分析是否存在异常的流量高峰、频繁的账户操作等黑灰产行为特征。
- **法律适用的技术依据：**提供证明黑灰产活动技术特性的证据依据，如使用的操作手段、数据传输量、访问频次等，以支持司法机关的定性判断。

三、出庭质证

在黑灰产案件中，专家通过出庭质证可以进一步阐述鉴定意见中的技术细节，对证据的合法性、科学性和完整性进行说明。

1 重要性

黑灰产案件涉及高度专业的技术内容，如恶意代码分析、网络流量异常分析、设备指纹比对等。司法人员和陪审团往往缺乏相关技术背景，因此专家的出庭质证成为帮助法庭准确理解案件技术焦点的重要途径。

- **阐述技术原理：**黑灰产活动涉及的技术内容复杂，例如数据抓取的技术手段、批量化操作的自动化流程等。专家需要在出庭中以简洁、通俗的方式解释技术原理，使法庭更好地理解。
- **回答质询：**在出庭过程中，专家需应对对方律师的质疑，回答关于数据来源、技术手段的可靠性、证据链完整性等问题，确保证据的可采性。

2 内容重点

- **通俗化解释技术细节：**使用比喻、图示等方式，帮助法庭理解黑灰产活动中的技术手段。
- **证据链条的完整性说明：**对证据链条的完整性作出详细解释，特别是在黑灰产案件中可能涉及多层次、多系统的数据来源，通过设备指纹、IP 地址、操作时间等要素，阐述各项证据之间的关联性和一致性。
- **技术方法的合法性与科学性：**详细说明取证过程，证明取证符合法律程序，未侵犯任何合法权益；提供证据的原始性证明，如哈希值校验结果，确保证据未被篡改。

ABOUT US

ABOUT US

关于我们

奇安信洞鉴简介

奇安信洞鉴，致力于为执法机关、行政监管和各大企业提供全链条电子数据证据服务，旗下有31个取证服务网点、3家司法鉴定所，提供事前线索挖掘、事中取证、事后鉴定全流程服务，保障证据链条完整、有效，是奇安信安全体系闭环的重要组成部分之一。

目前，奇安信集团已在上海、北京、西安建立了完备的司法鉴定所。其中，北京和上海两大机构都荣获了诚信等级A级评定，使奇安信成为国内唯一拥有双A诚信等级电子数据司法鉴定机构的企业。

奇安信洞鉴已与各地公安部门以及网信办、纪委监委、市场监督管理局等上百家执法机关达成深度合作，协助侦办各类案件近万起，每年出具数千份司法鉴定意见书；同时，深入服务于字节跳动、小红书、阅文集团、百度、小米等头部企业，为企业的信息安全与合法权益提供坚实保障。

3 大

司法鉴定所

- 上海盘石司鉴
- 北京网神洞鉴
- 陕西洞鉴云侦

31 个

技术服务网点

司法鉴定人 30+

取证技术专家 60+

覆盖全国 31 个省级行政区

300+

头部客户

执法机关、行政监管、企业等多领域客户 300+

覆盖案件侦查、行政处罚、企业调查多场景

旗下机构介绍

上海盘石司鉴

上海市首家通过 CNAS 认可的民营司法鉴定机构

上海盘石司鉴，是上海首家获得 CNAS 认可的民营计算机类司法鉴定机构，已通过 CMA 资质认定，并荣获首批司法部鉴定能力及诚信双 A 等级评定。同时，连续五年，获司法部司法鉴定科学研究院能力验证满意结果。其负责人是上海司法鉴定协会理事和专业委员、司鉴院能力验证技术专家。

目前，已拥有具备司法鉴定资质的鉴定人 12 名，高级工程师 3 名，中级工程师 5 名。拥有面积达 120 平米的专业实验室，配备多台专用鉴定设备和一流硬件设施。

北京网神洞鉴

北京司法局诚信等级评估“A”级的司法鉴定机构

北京网神洞鉴，已通过CNAS认可、CMA资质认定与ISO9001质量管理体系认证。在北京市司法鉴定机构诚信等级评估中获得“A级”评价结果，并多次参加国内外能力验证和测量审核获得满意结果。

目前，已拥有具备司法鉴定资质的鉴定人10名，高级工程师2名，中级工程师4名，机构负责人入选北京司法鉴定专家库，并拥有多个发明专利和期刊文章发表。同时，拥有面积达130平米的专业实验室，配备多台专用鉴定设备和一流硬件设施。

陕西洞鉴云侦

按照高标准建设的司法鉴定机构

陕西洞鉴云侦，是奇安信集团与西安云侦智安电子科技有限公司联合组建的专业级电子数据司法鉴定机构，2024年正式挂牌运营。目前，已通过CMA资质认定。

目前，已拥有具备司法鉴定资质的司法鉴定人5名，高级工程师1名，中级工程师1名。拥有面积达200平米的专业实验室，配备多台专用鉴定设备和一流硬件设施。

奇安信洞鉴介绍

奇安信洞鉴，致力于打造一个全国范围内统一标准、高品质、高效率的司法鉴定服务体系，成为电子数据司法鉴定领域的技术先锋，为客户提供全链条专业服务。

洞观虚实

凭借强大的技术实力、高效响应的服务网络与专业的创新能力，帮助您在浩渺如烟的互联网世界中发现事实与真相。

鉴辨真伪

依据科学严谨的工作态度，通过合法合规的鉴定程序，给出具有公信力的鉴定结果，促进实现社会的公平正义。

洞鉴发展历程

2007.7 上海所成立
盘石软件司法鉴定所成立

2012.2 CNAS 认可
上海首家通过 CNAS 认可的民营司法鉴定机构

2021.6 北京所成立
北京网神洞鉴司法鉴定所成立

2022.8 诚信 & 专业能力双 A
盘石司鉴获首批诚信等级评估 A 级、首批专业能力等级电子数据鉴定 A 级

2022.12 CMA 认定
北京所通过 CMA 资质认定

2023.3 案件研判小组成立
针对复杂新型涉网案件，提供案件前期研判、分析支持

2023.3 CMA 认定
上海所通过 CMA 资质认定

2023.7 双 A 诚信等级
北京网神洞鉴获诚信等级评估 A 级
奇安信旗下拥有两家诚信等级 A 级机构

2023.10 CMA 认定
西安所（主体公司）通过 CMA 资质认定

2024.2 CNAS 认可
北京网神洞鉴通过 CNAS 认可
奇安信旗下北京所、上海所均通过 CNAS 认可

2024.5 西安所成立
陕西洞鉴云侦司法鉴定所成立

首家机构
为上海及周边提供
高质量司法鉴定服务

第二家机构
司法鉴定服务覆盖南北双中心
质量管理体系健全
诚信等级、专业能力等级双 A

第三家机构
连锁化经营模式
初见雏形
鉴定服务辐射全国

优势亮点

01 先进技术，突破疑难案件

奇安信洞鉴拥有业内领先的技术实力，依托于奇安信集团，尤其是奇安信盘古实验室的技术力量，其在众多重大疑难案件中实现了技术突破。

奇安信洞鉴

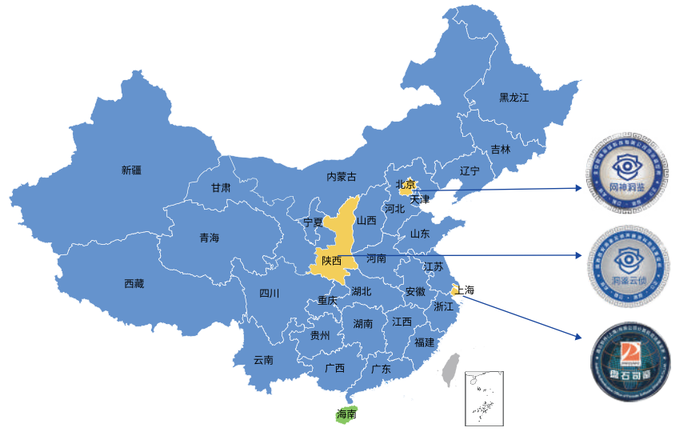
盘古实验室
国际知名安全研究团队
连续多次发布 iOS 完美越狱工具
累计已发现数百个 0day 移动安全漏洞

奇安信集团
新一代网络安全领军者
创造奥运会网络安全“零事故”的世界纪录
CCIA“2021 年中国网安产业竞争力 50 强”榜首

02 遍布全国，多地高效响应

奇安信洞鉴拥有遍布全国的服务团队，令数字司法服务“触手可及”，降低案件委托与沟通的成本，尤其对于涉及多地的案件，能够保证其调度的及时性和高效性。

3 个司法鉴定所
4 个取证实践基地
覆盖全国 31 个省份



03 案前、中、后，全流程服务

奇安信洞鉴通过提供案前研判、案中取证固定和线索挖掘、案后司法鉴定全流程服务，构建起了电子取证司法鉴定服务的闭环，保障证据链路的完整和有效应用。

事前
- 线索提供
- 技术研判

事中
- 关键线索挖掘
- 事中证据固定
- 抓捕现场取证

事后
- 检材梳理
- 司法鉴定
- 出庭质证

资质荣誉

资质认证

上海盘石司鉴

北京网神洞鉴

陕西洞鉴云侦

上海市司法鉴定质量标兵

专业能力等级 & 诚信等级双 A 评定

首届“宋慈杯”
优秀司法鉴定文书评选 三等奖

第二届“宋慈杯”
优秀司法鉴定文书评选 优秀奖

第三届“宋慈杯”
优秀司法鉴定文书评选 二等奖

获奖荣誉

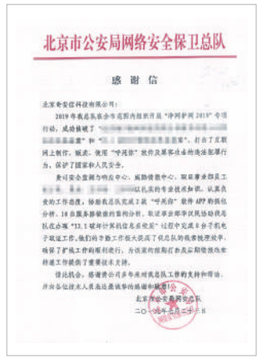
能力验证

司法部能力验证连续多年满意结果

公安三所能力验证全国、国际范围满意结果

客户认可

协助侦破重大疑难案件



为企业安全保驾护航

抖音　拼多多　华为　美团　小红书　小米

百度　快手　中金　阅文集团　值得买　石头

易车　华勤手机　博蕾德生物　广州互爱　Ulike　中煤集团