奇安信
新一代网络安全领军者

奇安信洞鉴

奇安信

CASE COLLECTION 2026

2026 版

奇安信洞鉴

案例集

QI AN XIN DONG JIAN CASE COLLECTION

洞观虚实
鉴辨真伪

Discern Reality
Distinguish Truth.

企业内控合规治理
网络黑灰产治理
市场秩序破坏治理
网络犯罪社会治理

Enterprise Internal Control and Compliance Governance
Governance of Cyber Black & Grey Markets
Crackdown on Market Order Violations
Social Governance of Cybercrime

www.qianxin.com

奇安信洞鉴

上海盘石洞鉴司法鉴定所
021-52658848（上海）
上海市闵行区宜山路 1999 号 24 幢 12 楼

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

奇安信洞鉴公众号

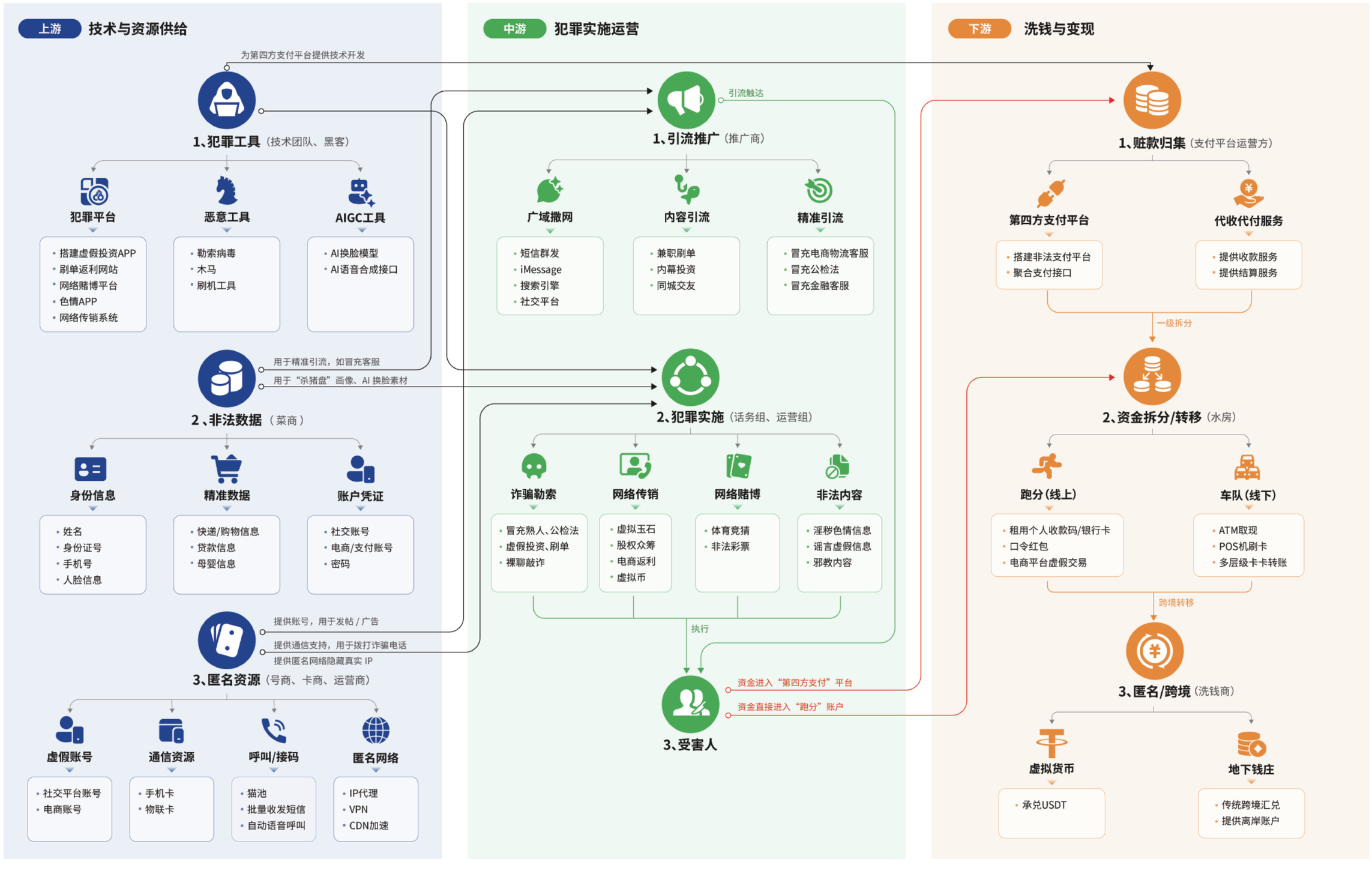
盘古石取证公众号

新型网络犯罪生态全景图

2026
PANORAMIC VIEW OF
THE NEW CYBERCRIME ECOSYSTEM

奇安信 | 奇安信洞鉴

01 网络犯罪社会治理图谱



02 市场秩序破坏治理图谱

1、设备作弊

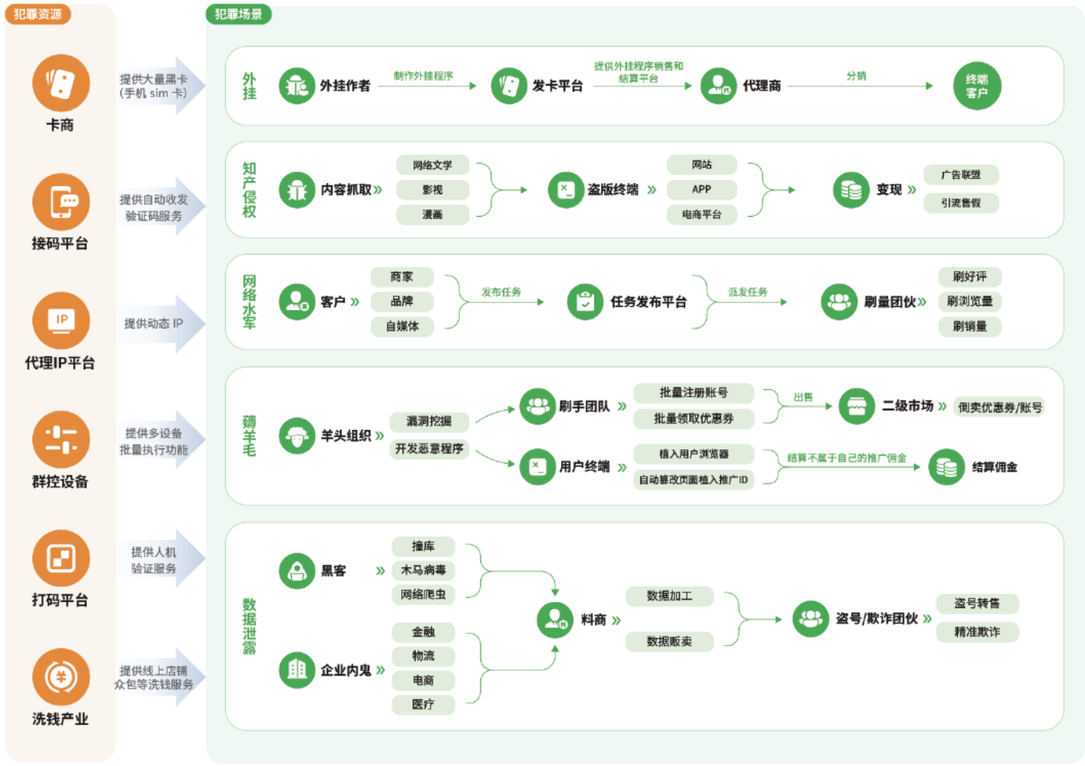
2、伪造票据及证件

3、黄牛抢购

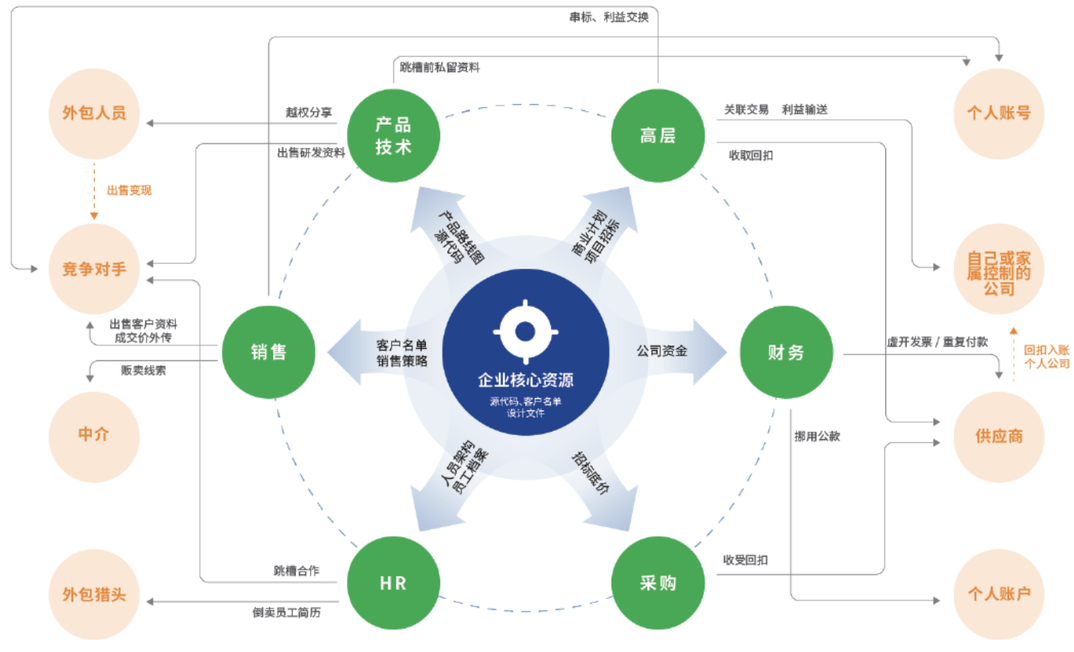
4、税务犯罪

5 走私

网络黑灰产治理图谱



04 企业内控合规治理图谱



PREFACE
前言

在数字经济与社会运行深度融合的今天，技术既是推动进步的核心引擎，也成为了新型犯罪滋生演变的温床。当我们享受着智慧医疗、数字金融、在线政务带来的便捷时，网络攻击的破坏性也在同步升级：关键信息基础设施（如医院）正遭受勒索病毒的致命瘫痪，以“元宇宙”“区块链”为伪装的金融骗局正将黑手伸向普通投资者，而跨境网络赌博、非法内容传播等犯罪，则借助隐蔽的支付通道与自动化工具，以前所未有的速度侵蚀着社会的安全与信任。

过去那些仅在新闻中出现的术语——勒索病毒、虚拟币传销、流量劫持、数据侧信道攻击，如今已演变为针对公共服务与市场秩序的精准打击；而企业内部的贪腐舞弊、商业秘密泄露等风险，也在悄然侵蚀组织的基业长青。面对这些与数字技术深度捆绑、证据散落在多平台、多设备中的复杂犯罪，传统治理手段正面临严峻挑战。电子数据司法鉴定，作为穿透数字迷雾的利剑，正在成为打击犯罪、维护社会秩序的关键力量。

奇安信洞鉴秉承“科技赋能司法，公正守护社会”的理念，汇聚资深鉴定专家的经验与智慧，深入剖析网络犯罪的底层逻辑与生态链条，为执法机关、司法部门及企业提供从线索挖掘、研判分析、证据固定到司法鉴定的一站式解决方案。

本案例集正是基于这些丰富的实务经验精心编撰而成，凝聚了我们在四大治理领域的深刻思考与实践探索：

网络犯罪社会治理：聚焦勒索病毒攻击、虚拟币诈骗、网络传销、跨境赌博及非法内容传播等前沿犯罪，深度剖析其技术手法与组织模式。
市场秩序治理：深入剖析各类破坏市场秩序的违法行为，涵盖设备作弊、黄牛抢购、重大税务犯罪与跨境走私等。
网络黑灰产治理：聚焦作弊外挂、知识产权侵权、数据泄露、网络水军及薅羊毛等场景，揭示其产业化、平台化的运作特征。
企业内控合规治理：聚焦企业内部的商业秘密泄露与破坏、贪腐舞弊等合规风险，分享取证鉴定思路与典型案例。

书中不仅有抽丝剥茧的技术揭秘，更汇集了大量可操作的实战经验。每一个案例都紧扣最新的作案手法与鉴定技术，反映出数字时代面临的新挑战，同时展现了我们对未来趋势的深度洞察。

在科技迅猛迭代的当下，犯罪手法与技术对抗的演进永不停歇。但我们始终坚信，技术的进步终将赋能正义，智慧与合作是破解安全难题的关键。愿这本案例集不仅成为行业从业者和办案人员的宝贵工具，也能为所有关注数字安全与电子数据取证的人士带来启示与思考。奇安信洞鉴期待与更多伙伴携手，共同为构建更加公平、有序、可信的数字未来，书写厚重而深远的注脚。

CONTENTS
目录

CHAPTER 1

网络犯罪社会治理

在数字经济与信息技术高速发展的时代，互联网正深刻改变着人类的生产和生活方式。这股推动社会繁荣与便利的技术力量，却也为多类型网络犯罪提供了滋生土壤。诈骗勒索、网络传销、网络赌博、色情谣言传播等犯罪形态，以前所未有的速度和多样性侵入网络空间，严重威胁社会安全与公共秩序。

从宏观态势来看，网络犯罪呈现出持续上升趋势。据统计，2017 年至 2021 年，全国各级法院一审审结涉信息网络犯罪案件累计已逾 28 万件，且案件量逐年攀升 [1]。其中，电信网络诈骗始终高居首位，占比达 36.53%。到 2023 年，相关起诉数据再创新高，其中起诉电信网络诈骗犯罪 5.1 万人，同比上升 66.9%，起诉帮助信息网络犯罪 14.7 万人，同比上升 13%，起诉网络赌博犯罪 1.9 万人，同比上升 5.3%[2]。这些数据不仅印证了网络犯罪生态的扩张，也揭示了上下游紧密衔接、链条化运作的黑灰产业格局正在加速形成。

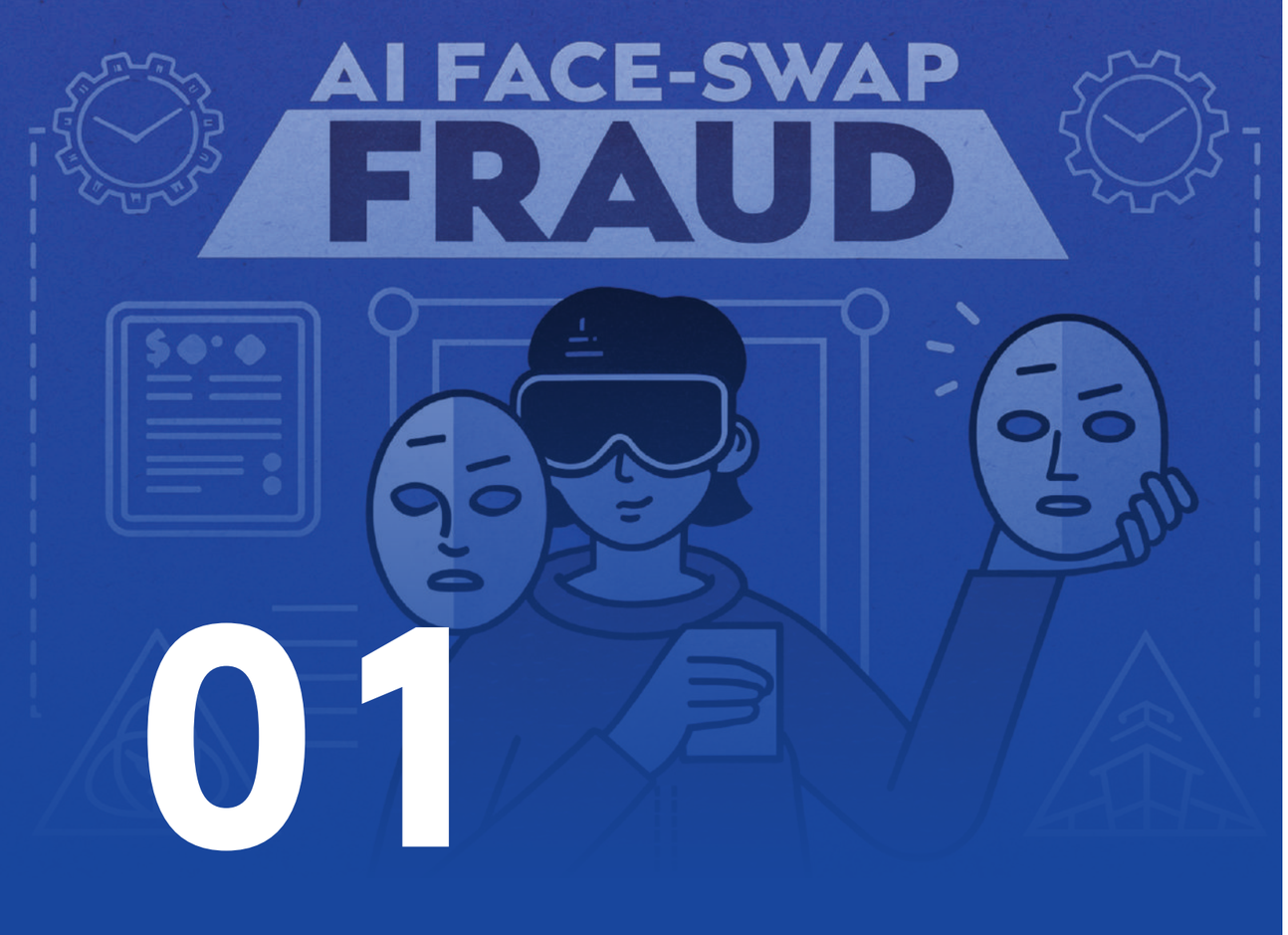
从犯罪特征来看，网络犯罪的复杂性正在不断加深。技术的赋能使新型犯罪工具和手段层出不穷：犯罪分子利用 AI 换脸、语音合成技术进行冒充诈骗，通过虚拟货币、GOIP 设备以及跑分平台加速资金“洗白”，利用暗网与跨境服务器隐藏踪迹，令传统执法手段难以有效追踪。产业链条的全流程协作加剧了打击与治理的难度——从非法获取公民个人信息，到制作剧本化诈骗话术，再到跨境转移资金与多平台引流，犯罪已不再是个体行为，而是以专业分工、团队化协作的“工业化”形态存在。

与此同时，受害者群体不断扩大，从老年人被骗“养老钱”到青少年陷入游戏诈骗，再到“宝妈”误信兼职信息，犯罪精准打击令人防不胜防。与此同时，色情谣言、虚假宣传与不实信息的泛滥，引发社会舆论场的污染，冲击公众心理与社会价值观。网络犯罪不仅引致经济损失，更潜移默化地侵蚀社会信任基础，对公共秩序与国家法治建设带来深远影响。

本章聚焦网络犯罪的典型类型与关键环节，剖析犯罪产业链与新兴手法，展示案件特征、取证难点及证据应用的方法论，帮助从业者优化取证策略与鉴定流程，提高打击效能。同时，也希望为公众提升安全意识、防控网络犯罪提供实用指导。

[1] 张明瑛 . 司法重拳打击涉信息网络犯罪 -- 聚焦《涉信息网络犯罪特点和趋势 (2017.1-2021.12) 司法大数据专题报告》[J]. 中国审判 , 2022(16):68-71.

[2] 最高人民检察院 . 刑事检察工作白皮书（2023）. 最高人民检察院官网 , 9 Mar. 2024, https://www.spp.gov.cn/spp/xwfbh/wsfbh/202403/t20240309_648173.shtml.



01

FRAUD AND EXTORTION
诈骗勒索

诈骗与勒索是两类具有差异但又存在交叉的犯罪行为。诈骗通过虚构事实或隐瞒真相，使受害人产生错误认识并主动交付财物，其核心特征是利用欺骗手段让受害人“自愿”受骗，常见于虚假投资、冒充身份等场景。勒索则通过威胁、恐吓或暴力手段迫使受害人屈服，其核心特征在于制造恐惧心理，使受害人因害怕隐私泄露或人身安全受到威胁而被迫交付财物，典型如裸聊敲诈。

在实际犯罪中，诈骗与勒索常常交叉出现，形成更复杂的犯罪模式。例如，犯罪分子可能通过裸聊获取不雅视频（诈骗成分），再以曝光隐私为威胁（勒索成分）获取更多利益。二者的共同点在于都以非法占有他人财物为目的，同时通过心理操控实现对受害人的影响，对社会秩序和个体权益的侵害具有深远影响。

1. 常见场景

刷单返利

诈骗模式

以“高额返利”“轻松兼职”为诱饵，前期小额返利建立信任，后期持续要求加大投入，借口“卡单”“连单”不让提现。

案件特点

案件数量多，单案涉案金额较低，但整体危害大，涉案平台和链接多为临时搭建。

目标群体

学生、低收入群体及无业人员等经济压力较大、急需用钱的人群。

虚假投资理财

诈骗模式

伪装专业投资导师、内幕消息源，引导受害人在虚假平台投资，先小额盈利后要求大额追加，一旦资金到位便无法提现。

案件特点

中高位单案金额，可达数十万甚至上百万元，采用虚拟币、股票、期货、外汇等“高端”投资名义。

目标群体

有一定经济基础和投资意愿的人士，涵盖年轻白领、单身人士、追求投资回报率较高的人群。

冒充电商物流客服

诈骗模式

获取被害人购物信息，以“理赔”、“订单异常”为由，诱导其下载APP或共享屏幕，窃取账户信息后转账。

案件特点

中高位单案金额，普遍在数万元左右。以真实快递、购物信息增加可信度。

目标群体

经常网购的普通消费者、电商卖家。

冒充领导、熟人类

诈骗模式

盗用领导或熟人身份，通过即时通讯工具取得信任后，紧急要求代为转账，伪造转账截图欺骗被害人。

案件特点

中高位单案金额，多为数万元乃至十几万元；案件隐蔽性强，常在工作日白天发生。

目标群体

政府、企事业单位人员、学生家长等群体。

冒充公检法类诈骗

诈骗模式

冒充公安、检察院、法院，以涉嫌违法犯罪为由恐吓被害人需将资金转入“安全账户”自证清白。

案件特点

案值高，可达数十万乃至上百万元，手法老套却屡试不爽；高压力场景让受害人失去判断。

目标群体

留学生、老年人及对权威部门心存畏惧的人群。

网络游戏虚假交易

诈骗模式

冒充游戏账号、装备买卖方，引诱玩家私下交易，先以低价吸引，再以注册费、激活费各种名义层层加码诈骗。

案件特点

单案金额小到中等，多为数千元，但累计案件量大；常在玩家圈子快速传播。

目标群体

网络游戏玩家，尤其是青少年和沉迷游戏消费的人士。

网络婚恋交友

诈骗模式

长期虚构恋爱关系，投入大量情感营销，以“家庭变故”、“投资项目”为由索要巨款。

案件特点

案值高，时间跨度长，受害人常陷入情感困境，损失巨大且精神打击重。

目标群体

单身男女。

裸聊敲诈勒索

诈骗模式

犯罪分子通过交友软件诱导裸聊，录制不雅视频并窃取通讯录，以威胁公开隐私为手段勒索钱财。

案件特点

受害人一旦支付一次费用，犯罪分子通常反复威胁，直至受害人无力支付，被迫参与二次犯罪，如协助敲诈他人或参与“跑分”洗钱。

目标群体

18-35 岁年轻男性，尤其是单身男性。

AI换脸敲诈

诈骗模式

犯罪分子利用 AI 技术伪造受害人形象（如脸部或声音），制作虚假的色情视频、语音通话记录等，以公开不雅视频为威胁勒索钱财。

案件特点

AI 换脸技术门槛下降，大多数勒索行为通过匿名邮件或社交平台完成，资金转移多借助虚拟币。

目标群体

女性、名人、公职人员。

2. 犯罪链路

1 信息收集

方式：非法购买或窃取公民个人信息，包括身份证号、手机号、银行卡号、家庭住址、社交媒体数据等。这些数据通常被打包售卖到黑灰产市场，形成信息“供应链”，为精准诈骗提供支撑。

手段：钓鱼网站、木马程序、暗网论坛、Telegram 交易。

> *农夫山泉创始人钟睒睒、蜜雪冰城实控人张红甫、喜茶创始人聂云宸、钟薛高创始人林盛、蔚来汽车联合创始人秦力洪等大量企业家个人信息和手机号被泄露并在网络平台公开出售，对包年用户，每个手机号售价低至 0.016 元。*
>
> *——每日经济新闻 2024 年 5 月报道*

2 目标筛选

方式：利用大数据分析筛选特定人群，并根据年龄、性别、职业、消费习惯等描绘目标画像。这些数据多来源于网络购物平台、社交媒体分析、金融交易记录等渠道，为诈骗分子提供精准人群匹配。

手段：AI 算法、数据分析工具。

> *不法分子针对不同人群特征实施诈骗：未成年人以免费领取游戏装备为主，大学生易遭虚假购物和刷单返利诈骗，大龄群体多为虚假投资理财诈骗，小微经营户常遇退货退款和年检类诈骗，农林牧渔从业者则易被冒充公检法和虚假征信诈骗。*
>
> *——中国银联《2023 年移动支付安全大调查报告》*

3 引流接触

方式：冒充好友、领导、客服、公检法等，通过电话或社交软件联系目标，发送伪造的银行通知、中奖信息、航班改签通知等引流。

手段：智能外呼机器人、短信群发、社交平台信息投放、快递引流、虚假招聘信息。

> *“纵横公司”系盘踞缅北掸邦大其力市金鑫科技园区的多个诈骗团伙之一，该团伙招揽人员在网络上冒充成功人士，通过 MarryU、陌陌、探探等聊天软件寻找女性作为诈骗对象，以交友聊天的方式获取对方信任，后诱骗被害人至该诈骗团伙控制的名为“永胜国际”等赌博网站进行投注，通过控制赌博网站后台的方式骗取被害人钱款。*
>
> *——最高人民检查院发布诈骗典型案例《郑某等 7 人诈骗、偷越国（边）境案》*

4 诈骗实施

方式：诈骗分子基于目标画像编写“杀猪盘”“刷单返利”等诈骗剧本，结合技术手段（AI 换脸、木马程序）、情境控制（屏幕共享、阻断联系）、心理操控（信任、恐惧、诱惑），引导受害者逐步落入陷阱。

手段：AI 换脸、语音合成、虚假的投资平台、购物平台。

> *电信网络诈骗犯罪出现了一些新变化、新特点：诈骗集团针对不同群体，根据非法获取的精准个人信息，“量身定制”诈骗剧本，实施精准诈骗。*
>
> *——2022 年国新办打击治理电信网络诈骗犯罪工作进展情况发布会*

5 资金转移

方式：通过多层级账户转账、虚拟货币交易及“跑分”平台，实现资金的快速流转与隐匿。犯罪分子通常利用地下钱庄的跨境汇兑功能，将非法所得转移至境外，并进一步洗白。

手段：虚拟货币、口令红包、纪念钞、高薪兼职、快递黄金套现。

> *检察机关办案发现，犯罪分子洗钱手段多样，除购房、购买黄金等贵金属、投资证券基金、通过地下钱庄跨境转移资金等手段外，租用他人银行账户、网络支付账户转移犯罪所得及其收益也是常见洗钱手段，如收购、租赁银行卡供上游犯罪人员转移犯罪所得，并提供“刷脸”等身份认证全套服务。*
>
> *——最高检：检察机关起诉洗钱犯罪数量呈持续上升趋势*

3. 取证鉴定思路

诈骗与勒索案件中，犯罪分子或通过虚假信息诱骗受害人主动交付财物，或通过威胁恐吓迫使受害人被迫交钱。这类案件中，手机 APP、虚假平台网站是常见的技术载体。取证鉴定需从前台（APP、网站）到后台（服务器、数据库）全链条分析，运用逆向工程、抓包分析、数据重构和身份核验等技术手段，最终为公安机关提供明确的技术证据支撑和参考意见。

以下是针对诈骗勒索类案件的取证鉴定思路：

1 接收检材与初步研判

通过公安提供的报案信息与 APK 文件，初步判断案件性质（诈骗或勒索或二者交织），明确取证重点与范围。

信息研判：接收 APK 文件和受害人交易记录截图或简述，初步判断是充值无法提现（典型诈骗）还是不雅视频恐吓（勒索）。

明确取证目标：追查 APP 所连接的服务器、识别幕后操控者、锁定资金流向。

2 逆向分析与抓包取证

对涉案 APP（APK）进行逆向工程和网络抓包，以获取服务器地址、通信协议、加密机制和关键标识符，为后续调取服务器数据奠定技术基础。

逆向 APK：定位关键调用函数、加密算法、硬编码 URL 或 IP，确认 APP 与服务器间的请求类型（登录、充值、提现）。

抓包取证：运行 APP 捕获网络数据包，提取服务器域名、认证 Token、UID 等关键标识符，为公安后续依法调取服务器镜像提供技术参考。

3 服务器镜像与环境重构

利用已获知的服务器信息向服务商申请服务器镜像，鉴定机构对镜像进行数据恢复和环境搭建，重现后台管理系统并验证其功能模块。

服务器镜像申请：公安携服务器 IP/ 域名及对应 UID，向云服务商、CDN 或托管方调取服务器镜像文件（数据库、配置文件、日志）。

后台界面重现：利用数据库和镜像分析工具，在本地隔离环境中还原后台系统运行条件，成功登录后台管理界面，确认权限结构（管理员、客服、财务等角色）及可操作项目（用户审核、订单调整、利率设置）。

4 数据库分析

从数据库中提取用户列表、充值 / 提现记录、订单信息，对资金流动过程进行关联分析，还原诈骗流程或勒索付费过程，确认平台的违法属性。

用户列表解析：核对注册账号、绑定手机号 / 邮箱，识别多账号关联与异常注册行为。

充值 / 提现数据统计：统计频繁充值账户、失败提现纪录，发现资金积聚路径及下游出款账号。

可调参数固定：如后台有利率、返利比例等动态参数配置项，进行截图，证明平台可随意操纵收益率，从而确立欺骗或胁迫手段的动态可控性。

5 操作日志分析

检查后台操作日志、管理员登录信息、账号绑定记录，关联可疑操作（修改订单状态、调整利率、删除提现请求）与特定管理员，挖掘嫌疑人身份线索。

登录日志审查：统计管理员登录时间、IP 地理位置，留意频繁变动 IP 或深夜操作异常行为。

操作记录关联：确认哪个账号实施了核心操作（禁用用户、调高利率、篡改余额），锁定可疑账号。

身份绑定证据固定：若数据库有实名信息或外部支付钱包地址，将其固定为证据，支持公安后续人像比对或资产查询。

6 勒索相关证据提取与验证

如案件存在勒索成分（如不雅视频敲诈），重点提取相关聊天记录、媒体文件链接及存储路径，核对与受害人描述一致性，重建勒索信息传递链条。

聊天记录检索：检索聊天记录表、消息队列表，锁定发送不雅视频链接和威胁信息的账号。

不雅文件比对：对存储在服务器上的媒体文件目录进行比对，提取不雅视频、图片，核对其与受害人描述一致性。

7 生成鉴定意见书

将从 APK 逆向、抓包到服务器镜像分析、后台重构、数据库解析的全流程结果整合为鉴定意见书。

证据链条整合：用图表、流程图直观展示从 APP 前台诱骗、后端后台操控到资金汇集的路径，对关键证据（修改利率页面截图、充值提现记录统计表、不雅视频文件哈希值）进行数据固化与技术解释。

技术定性意见：给出技术性意见和风险评估，如确认该 APP 本身具有诈骗或勒索功能设计，后台可随时调整欺骗参数。

4. 典型案例

医院勒索病毒攻击溯源案

深度剖析恶意程序，实现勒索病毒加密链条复现

本案涉及一起针对医疗系统的、破坏性极强的勒索病毒攻击事件。攻击者利用内网穿透工具突破医院网络边界，植入可横向传播的勒索病毒，在短时间内导致医院核心业务系统大面积瘫痪。奇安信洞鉴通过对涉案硬盘的镜像分析、恶意程序的功能复现与逆向分析，成功还原了从“突破入口”到“内网扩散”的完整攻击链条。鉴定报告将复杂的技术行为“翻译”为清晰的作案手法，不仅证实了不同院区攻击的同源性，更揭示了病毒具备“蠕虫式”传播能力这一导致灾难性后果的关键特性，为案件的侦破提供了核心技术证据。

案件背景

2024 年，某县人民医院的业务系统突然遭到勒索病毒攻击，导致医务工作无法正常开展，经初步统计，院内已有 60 多台电脑受到感染。随着调查的深入，办案单位发现该县第二人民医院也遭受了类似的攻击，遂将两起事件并案处理，并将从两个现场查获的服务器硬盘一并送至奇安信洞鉴进行深度分析，以彻查病毒的来源、传播方式和破坏机制。

洞鉴解决方案

01 一致性比对，锁定关键恶意程序

鉴定人使用专业取证分析系统对硬盘镜像进行分析，并从“某县人民医院”和“某县第二人民医院”两台电脑中提取到两个核心可疑程序。通过对文件的哈希值进行比对，证实二者内容完全一致。这一发现说明，两起攻击事件均源于同一恶意程序，为案件的关联分析提供了关键技术依据。

02 攻击复现，揭示内网穿透能力

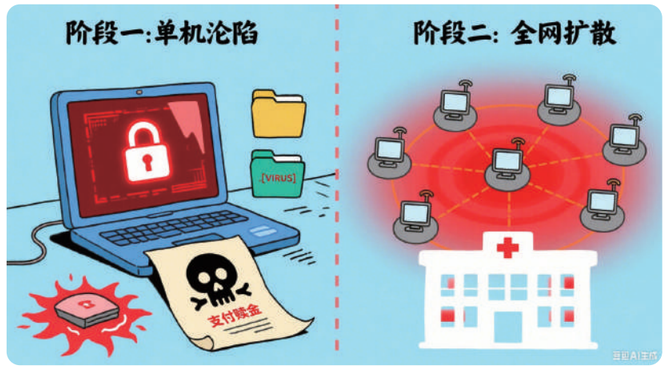
在分析过程中，鉴定人发现了一款可疑应用“S*”，为验证其功能，鉴定人在隔离的虚拟机环境中进行了功能复现。结果表明，“S*”具备典型的内网穿透功能，能够建立跨越防火墙的隧道，使外部网络设备直接访问和控制内网主机。这一能力极有可能成为本次勒索病毒入侵医院网络的突破口。

03 逆向分析，揭示两阶段破坏模式

鉴定人员结合动态行为监控与静态逆向分析，确认该勒索程序具备清晰的两阶段攻击模式：

1. **第一阶段（单机破坏）：**程序运行后，会将自身复制到系统目录并改名为新的进程文件，同时删除原进程，降低被发现的可能性。同时，针对常见的压缩包、文档、脚本等类型文件，执行加密并在文件名中添加特定后缀，同时生成勒索提示文件，要求受害者支付赎金。

2. **第二阶段（横向扩散）：**更具危险性的是，该程序具备蠕虫式的传播能力。实验结果显示，病毒会自动扫描同一网段下的其他 IP 地址，识别可访问主机，并通过隐藏控制界面远程执行加密操作，从而在短时间内导致整个医院网络大面积瘫痪。



值得注意的是，当该病毒与“S*”内网穿透工具结合使用时，攻击者不仅能在局域网内扩散加密，还可能借助公网通道进一步扩大攻击范围。

案例价值

01 / 还原攻击链条

本次鉴定不仅识别了勒索病毒本身，更成功回溯并复现了攻击者利用“内网穿透”工具的攻击入口，清晰地描绘出从“单点突破”到“内网全面扩散”的完整攻击路径，为案件的全链条打击提供了方向。

02 / 揭示作案手法

通过动态与静态结合的深度分析，精准刻画了该病毒的核心破坏能力，特别是揭示了其“横向移动”的攻击特性。这为理解事故波及范围之广的原因提供了直接技术解释，也为其他医疗机构防范同类攻击提供了宝贵的预警。

03 / 提升办案效能

极大缩短了技术攻关周期，帮助办案机关在早期就能够把握案件的关键要点，避免侦查力量在海量日志和模糊线索中反复消耗。通过精准还原病毒的运行模式，侦查人员得以及时确定案件性质、锁定攻击方式，并将精力集中在追查攻击者身份、资金流向和攻击源头上，大幅提升了整体侦办效率。

虚拟交易所诈骗案

揭示虚拟交易所伪装，追踪资金链与层级返利模式

本案涉及一起利用虚拟数字货币交易平台实施赌博诈骗的案件。犯罪嫌疑人通过搭建假冒数字货币交易所，伪装成投资夺宝游戏，诱导用户充值资金参与“无损夺宝”“稳赚大奖”活动，实际上是通过后台操控数据，骗取用户资金。奇安信洞鉴通过源码解析与数据库还原，完整揭示该平台从用户注册、充值提现，到夺宝下注、佣金返利的运行机制，将技术细节翻译为犯罪团伙的真实作案手法，为案件定性提供了关键证据支撑。

案件背景

2024 年，某市公安局接到居民孙先生报案，称其在一个网络社群内被客服诱导，点击链接进入一个名为“XXEx”的数字货币交易所。在该平台“无损夺宝，赢取超级大奖”的宣传下，孙先生陆续充值数千元后发现被骗。初步侦查发现，该平台涉案人员众多，资金流水巨大，技术架构复杂。为彻底查清该平台的运作模式、锁定涉案资金、固定犯罪证据，办案单位将查获的服务器硬盘镜像、数据库备份文件等委托奇安信洞鉴进行专业鉴定。

洞鉴解决方案

01 证据固定与全环境复现，重建犯罪“现场”

鉴定人首先对所有涉案硬盘、数据备份等检材进行了镜像固定和哈希值校验，确保了电子数据的原始性和完整性。随后，为了让已经下线的诈骗平台重新运行起来，鉴定人执行了关键的系统环境重建工作：

1. **多数据库协同恢复：**在自建的 Linux 虚拟机环境中，利用专业数据库恢复工具，成功将核心业务库、日志库、用户行为库等多个 MySQL 数据库备份文件恢复至本地，还原了包含数百张数据表的庞大数据库集群。
2. **启动应用程序：**鉴定人利用服务器的硬盘副本，创建了一个功能对等的虚拟服务器。在这个虚拟环境中，成功启动了诈骗平台的核心网站应用程序及必要的缓存服务，使程序本身恢复到可运行状态。
3. **关联应用与数据：**启动后的网站程序，其内部设置默认指向已经失效的原始服务器地址。鉴定人员通过修改其配置文件，将程序的通信路径重新指向本地恢复好的数据库。此步骤打通了程序与数据之间的连接，使二者可以协同工作。

通过以上操作，一个功能完整、数据齐全且与外界隔离的诈骗平台副本被成功搭建，为后续安全、深入的调查取证和数据分析奠定了基础。

02 前后端数据穿透，解密业务逻辑

在成功重建并运行平台后，鉴定人使用一个已知的测试账号登录了本地网站前端。通过对前端页面的显示内容与后端数据库中的原始数据进行逐一比对，成功查明了数据库中数百个字段的真实业务含义。例如，通过验证一个样本用户账号的邀请列表、充值记录等信息，准确对应了用户表、充值记录表等关键数据表中的字段，建立了前端显示内容与后端存储数据之间的明确对应关系。

03 海量数据提取与分析，量化犯罪规模

基于对数据库结构的掌握，鉴定人从核心业务数据库中提取了覆盖平台所有运营环节的海量数据，明确了该平台的运营规模与数据体量：

1. **用户体系：**共提取 10+ 万条用户信息及数万条用户证件信息，勾勒出完整的受害用户画像。
2. **资金流水：**成功导出数千万条资金流水记录、佣金记录、买卖交易记录等，清晰还原了平台内每一笔资金的流向。
3. **分赃体系：**获取了节点信息、合伙人关系、分红记录、舵主分红等数据，完整展现了其“节点 - 合伙人 - 邀请”的金字塔式分赃结构。

04 专项数据挖掘，深挖犯罪模式

面对数千万级别的复杂数据，鉴定人员编写了多个 Python 脚本进行自动化、深度的关联分析

1. **用户画像分析：**整合用户基本信息、证件、邀请关系、充值、提现、佣金、分红、节点贡献等多维度数据，为每个用户（特别是 139 名核心的“节点发起人”）建立了全面的数字档案。
2. **“夺宝”模型分析：**按“节点发起人”和“其他用户”两个维度，对所有夺宝商品进行分类，详细分析了每期商品的参与用户、中奖用户和购买记录，为研判其背后是否存在人为操控提供了数据基础。
3. **平台盈利统计：**对平台的提现手续费、交易手续费、生态基金等进行分类汇总统计，精确计算出平台的非法获利总额。

案例价值

01 / 完整还原犯罪模式

通过技术手段对已经下线的平台进行复现，并结合数据分析，完整还原了该诈骗团伙从吸引用户、诱导充值，到设计“夺宝”骗局、再到通过“节点分红”模式进行内部分赃的全链条犯罪模式，将抽象的电子数据转化为可被司法人员理解的作案手法。

02 / 精准量化犯罪规模

本次鉴定提供了可量化的犯罪规模证据，包括受害总人数、平台总资金流水、核心业务数以及平台非法获利（手续费、基金）的具体数额，为案件的定性、量刑提供了强有力的数据支撑。

03 / 固化关键电子证据

从服务器镜像到数据库恢复，再到代码分析和数据导出，整个鉴定过程形成了一条完整且不可否认的证据链，为案件的顺利诉讼提供了坚实的技术保障。

“空气币”诈骗案

诈骗与技术共舞：解密“空气币”背后的虚拟货币交易平台

某企业配合诈骗团伙，设计了一款“虚拟货币交易平台”，并为其实施诈骗活动提供帮助，涉嫌帮助信息网络犯罪活动罪。奇安信技术团队在此案中发挥重要作用，前期协助警方追踪到开发团队，并在现场勘查中固定了关键证据；同时，通过出具鉴定报告，形成了专业、清晰、完整的证据链，证实了该企业与诈骗团伙的合谋关系。

案件背景

“空气币”意为没有任何信用背书和实物依托的数字货币，其涨跌完全由发行方掌控，表面上高收益，实则风险极大。

本案件就源自一款“空气币”交易平台，受害人称经微信群讲师推荐下载虚拟币交易 APP，并在其中进行了大额投资，后发现该平台投资的币种为实际上是“空气币”，无法提现，遂报案。奇安信的技术人员就是从对这款诈骗 APP 的分析入手，展开了深入调查，协助警方逐步揭开了背后的开发团队。

洞鉴解决方案

01 案中：剖析诈骗 APP，揭示开发者身份

当受害者发现自己被诈骗后，立即前往派出所报案，警方提取了受害者手机中的诈骗软件 APK 文件，奇安信技术团队对此进行全程技术支持，证实了开发者身份，具体过程如下：

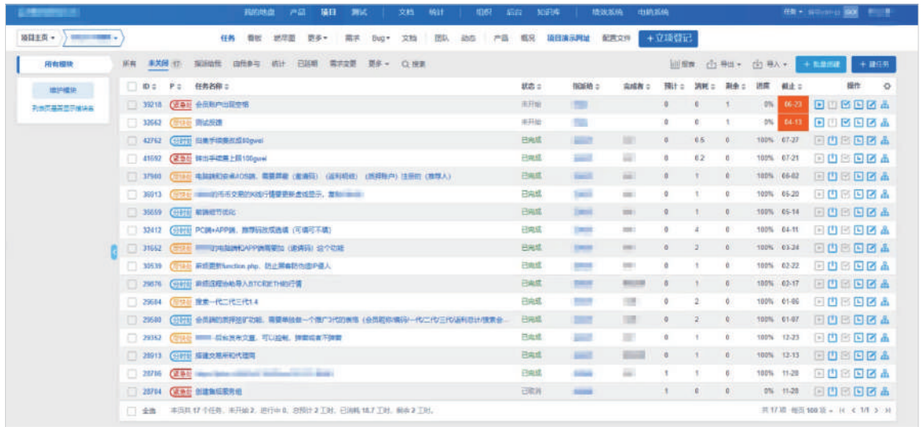
1. **哈希值比对：**通过对该 APK 文件进行解压后，提取到了签名文件，读取并计算了该文件的 MD5 值（它可作为一种证书的标识，用于对其他 APK 文件进行关联），通过其找到了与之关联的另一款 APP，并定位到了该 APP 开发者“某博”企业；
2. **IP 地址获取：**通过对涉诈 APP 的进一步分析，成功找到了其主控网站，奇安信技术团队配合警方，获取到登录者的 IP 地址，而这些 IP 地址，亦指向了“某博”企业所在地。

通过警方进一步缜密侦查，发现该企业配合诈骗团伙开发了三款诈骗 APP，据此，已基本明确“某博”企业为涉案犯罪团伙。

02 案后：N 份鉴定报告，构建清晰完整的证据链

在实施抓捕过程中，奇安信技术团队配合警方完成了对工单系统及代码服务器的证据固定，并在现场发现了 6 部手机，为后续司法鉴定和起诉提供电子数据支撑，鉴定人对上述证据进行审慎、专业的鉴定分析，构建了清晰完整的证据链。具体过程如下：

1. **虚拟币交易平台鉴定：**鉴定人对该涉案公司开发的交易平台试用版进行了功能性鉴定，说明了其具备机器人刷单、刷 K 线操作、增加虚拟币等功能，并证实了其交易功能不涉及实际交割。
2. **工单系统鉴定：**通过还原、仿真其项目管理系统环境，在本地访问系统并搜索 "**K""**C""**S"（三款诈骗 APP）关键词，提取到了相关项目信息，这些内容佐证了涉案企业曾参与过相关项目的开发。



涉案项目工单

3. **代码服务器鉴定：**通过还原、仿真其代码服务器，并通过关键词搜索，亦在其服务器中成功提取到了涉案公司相关产品的不同版本代码，与诈骗团伙相关的文件夹有 19 个，涉及与 "**K""**C""**S" 有关的 100,000+ 个文件。
4. **相似性比对：**对受害者手机中提取到的三款诈骗 APK 及 IPA 安装包，与犯罪团伙电脑中提取到的软件逐一进行了目录结构、文件以及反编译代码比对，并计算了相似度，证明嫌疑人电脑中的程序与受害者手机中的程序实质相似。
5. **聊天记录恢复与提取：**对涉案人员的相关聊天记录进行分析、关联，恢复并成功提取到通讯记录共计 2000+ 条，这些聊天记录显示了公司内部人员的交流情况，包括他们如何响应客户需求，如何设定网站功能需求等，为证明公司人员知晓并参与了诈骗活动提供了有力证据。

案例价值

01 / 发现犯罪线索

我司先进的技术工具和专业知识，使公安机关能够在复杂的网络环境中，精确地定位到犯罪嫌疑人，从而有针对性地展开调查，极大地提高了公安机关的工作效率。

02 / 构建完整证据链

通过对 APP、服务器和手机等多元化的数据进行深度分析，我司帮助公安机关建立了完整的证据链条，这不仅有助于法庭的定罪，也有助于揭示犯罪行为的全貌。

03 / 识别诈骗模式

对此案的运作模式的深入挖掘，有助于公安机关了解新型网络诈骗的手段和策略，这对于其侦破类似的案件有着极其重要的参考价值。

虚拟投资理财诈骗案

高收益虚拟货币？揭开虚假投资平台背后的操控真相

2021 年初，受害人通过微信认识一名“投资导师”，被引导下载多个虚拟货币投资平台，累计投入资金 92.5 万元。然而，当受害人尝试提现时，平台出现操作异常，资金无法取出。奇安信洞鉴通过数据提取、关键词搜索、后台还原与资金流向分析，成功揭示了虚假投资平台通过后台操控用户数据实施诈骗的全过程，并提供了详实、完整的证据链。

案件背景

近年来，伴随虚拟货币热度上升，网络诈骗团伙利用所谓“高收益”“零风险”的虚拟货币投资平台，诱导受害人进行大额投资。这类平台往往通过后台控制虚拟币价格、虚构收益率，营造虚假的盈利假象，让受害人加大投入，最终通过无法提现或资金转移完成诈骗。本案中的虚假平台便是此类诈骗手法的典型案例。

受害人在微信群讲师的诱导下，多次进行所谓“投资操作”，最终累计损失 92.5 万元，其中大部分资金流向不明。为查明资金流向及平台后台的实际运作情况，公安机关委托奇安信洞鉴进行电子数据分析与鉴定。

洞鉴解决方案

01 数据提取与恢复

首先对公安机关提供的硬盘、手机进行了数据提取与镜像恢复，确保数据完整、准确，为案件侦破提供基础依据。

1. **硬盘数据提取：**通过镜像制作与关键字搜索，成功提取了上网记录、账号访问日志及与涉案平台相关的文件，为后续分析平台的操作模式及管理行为提供了基础证据。
2. **手机数据恢复：**使用盘古石手机取证系统对涉案手机进行深度数据恢复，恢复了微信、QQ、Telegram 等聊天记录，以及支付宝交易、转账记录等数据。这些数据完整还原了受害人与诈骗团伙之间的通信内容，揭示了资金流动链条及关键人物关系。

02 平台还原与仿真分析

在掌握硬盘和手机数据的基础上，对涉案平台进行了后台还原与仿真分析，复现平台的管理功能，揭示了诈骗手法的核心逻辑。

1. **后台仿真还原：**搭建虚拟机环境，导入平台数据库与网站文件，成功还原平台后台管理界面。分析发现，后台管理员拥有极高权限，可以修改用户账户金额、信用分、交易状态；设置虚拟币的涨跌幅、杠杆倍数等核心参数。这些功能证明了所谓的“投资收益”并非真实交易所得，而是通过后台人为操控的数据结果。
2. **日志提取与分析：**提取了后台管理员的登录日志，共 300 余条，记录了管理员的登录时间、IP 地址和具体操作行为。分析显示，管理员曾对受害人账户执行“充值”“修改金额”等操作，为平台伪造投资收益提供了直接证据。

图 - 平台后台管理页面

03 资金流向分析与数据固定

通过备份和分析平台数据库，提取了关键的资金流向数据，对资金链条进行了全面还原。

1. **资金数据分析：**从数据库中提取了 8 万余条资金流动记录，1000 余条提现记录，详细记录了用户充值路径、提现失败情况及资金分布。
2. **数据固定：**对数据库文件、查询记录及固定数据进行了备份与验证，确保数据真实、完整、可溯源。

```
CREATE TABLE `wp_temp_personal` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `uid` int(11) DEFAULT NULL COMMENT '用户id',
  `real_name` varchar(32) DEFAULT NULL COMMENT '姓名',
  `card` varchar(32) DEFAULT NULL COMMENT '身份证号',
  `card_positive` varchar(64) DEFAULT NULL COMMENT '身份证正面图片路径',
  `card_side` varchar(64) DEFAULT NULL COMMENT '身份证反面图片路径',
  `bankname` varchar(20) NOT NULL COMMENT '所属银行',
  `banknumber` varchar(20) NOT NULL COMMENT '银行卡号',
  `branch` varchar(20) NOT NULL COMMENT '支行名',
  `tel` varchar(20) DEFAULT NULL COMMENT '银行预留手机号',
  `bank_img` varchar(64) DEFAULT NULL COMMENT '银行卡图片',
  `bank_province` varchar(20) NOT NULL COMMENT '银行卡省份',
  `bank_city` varchar(20) NOT NULL COMMENT '银行卡城市',
  `status` tinyint(1) DEFAULT '0' COMMENT '0未提交 1已提交',
  `create_time` int(11) DEFAULT NULL COMMENT '提交时间',
  `payee` varchar(255) NOT NULL COMMENT '收款人姓名',
  `branchadd` varchar(255) NOT NULL COMMENT '银行地址',
  `swift` varchar(255) NOT NULL COMMENT 'swift代码',
  PRIMARY KEY (`id`) USING BTREE,
  UNIQUE KEY `uid` (`uid`) USING BTREE
) ENGINE=InnoDB AUTO_INCREMENT=310 DEFAULT CHARSET=utf8 ROW_FORMAT=DYNAMIC COMMENT='个人信息提交临时表';
```

图 - 受害人数据分析

案例价值

01 / 高效还原数据

面对海量数据与碎片化信息，我们通过专业的数据提取、深度分析与关键词检索，快速定位关键证据，精准还原硬盘与手机中的操作记录和核心数据，大幅缩短数据分析周期，帮助公安机关提高侦查效率。

02 / 揭示平台操控行为

通过对平台后台的仿真还原与数据分析，我们成功揭示了后台具备修改用户账户金额、交易状态的操控功能，证实平台通过篡改数据虚构盈利，诱导受害人持续投入资金，精准揭示了诈骗的技术手法与犯罪模式。

03 / 提供完整证据链

我们提取并恢复了操作日志、上网记录、聊天记录 和 交易数据，系统展示了诈骗平台的运作模式与后台操控行为，形成了一套专业、清晰、完整的证据链，为公安机关的案件侦破与后续起诉提供了关键的数据支撑和技术保障。

裸聊敲诈勒索案

一场裸聊背后的陷阱：揭开恶意 APP 窃密真相

在一起网络裸聊敲诈勒索案件中，受害人被诱导下载恶意 APP 进行视频裸聊。期间，犯罪团伙通过该 APP 非法获取受害人的手机通讯录、短信记录等敏感信息，并以不雅视频威胁受害人进行多次转账。奇安信洞鉴通过对涉案硬盘和手机进行数据提取、APP 功能分析与证据固定，揭示了恶意 APP 非法获取数据的过程，形成了完整的证据链，为案件侦破提供了关键支撑。

案件背景

近年来，随着互联网交友平台和视频软件的普及，以“裸聊”为代表的非接触类敲诈勒索犯罪呈现快速增长趋势。此类犯罪手法主要包括：

1. 犯罪分子通过社交软件与受害人搭讪，诱导受害人下载带有恶意功能的 APP。
2. 受害人在 APP 内进行视频裸聊时，恶意软件后台偷偷获取手机通讯录、短信、位置信息等敏感数据。
3. 犯罪分子利用不雅视频及个人信息进行敲诈勒索，受害人被迫多次支付钱款。

本案中，受害人被犯罪分子诱导下载安装了一款所谓的“直播软件”，在裸聊过程中，恶意 APP 窃取了受害人手机中的通讯录数据，并将其上传至指定服务器。犯罪分子随即以不雅视频截图威胁受害人，索要巨额转账。公安机关接到报案后，迅速展开侦查，委托奇安信洞鉴对涉案手机和硬盘数据进行专业司法鉴定。

洞鉴解决方案

数据库文件提取分析

针对公安机关提供的硬盘数据，我们开展了全面的数据提取与分析工作，成功揭示数据库中存储的个人敏感信息，为案件侦破提供基础证据。

1. 数据库导入

提取硬盘中的多个数据库文件，将提取的数据库文件导入 MySQL 环境，进行结构化数据分析，为后续检索提供技术支撑。

2. 目标数据提取

编写 Python 脚本，从用户表中定位目标用户 ID，通过关联通讯录表，成功提取目标用户的通讯录数据，导出目标人员的完整通讯录数据，实现对目标用户通讯录的自动化检索与关联。

恶意 APP 功能鉴定

针对硬盘中提取的多款裸聊诈骗 APP 文件，我们进行了系统性的功能鉴定与数据验证，揭示 APP 的恶意行为及其数据上传路径。

1.APP 权限功能分析

使用奇安信星源 APP 溯源分析平台对 v*.apk、花 **.apk 等恶意文件进行解析，确认 APP 具备读取通讯录数据、定位用户地理位置、读取短信内容及验证码等权限，这些权限为 APP 在后台窃取用户敏感信息、实施敲诈勒索提供了技术支持。

2. 数据上传验证

将 APP 安装至模拟器环境，并进行实时抓包分析，抓取到上传服务器的 URL 路径，确认上传内容包括通讯录数据、位置信息及设备标识码等敏感信息。

3. 核心代码审查

对提取的 IPA 文件进行后缀名修改与解压，定位到关键代码文件后进行逻辑分析，在代码中发现 APP 通过调用网络请求模块（如 mui.ajax 函数），未经用户授权自动上传通讯录、位置信息等敏感数据至指定服务器地址，进一步验证了 APP 的恶意行为及其数据窃取手法。

案例价值

01 / 揭示犯罪手法

通过对恶意 APP 的全面技术鉴定，我们揭示了犯罪团伙如何利用技术工具窃取用户隐私数据的完整过程。从 APP 权限滥用到数据上传路径，鉴定结果精准剖析了犯罪模式，不仅为案件侦查提供了清晰的技术链条，也为警方扩展侦查方向奠定了基础。

02 / 提升侦查效率

借助专业工具和自动化脚本，我们高效完成目标数据提取与验证，快速锁定案件关键节点，显著缩短了侦查周期。这种高效支持减轻了公安机关的技术压力，使资源聚焦于核心抓捕行动，有力推动案件侦破。

03 / 提供技术模板

裸聊敲诈勒索案件复杂多变，对传统侦查提出了严峻挑战。我们的技术支持不仅有效遏制了本案犯罪行为，还为类似案件提供了可复制的技术模板。从权限分析到抓包验证，再到代码解析，这些成果为打击新型网络犯罪提供了重要参考，同时对犯罪链条的精准打击进一步震慑了潜在违法行为。

02

ONLINE PYRAMID SCHEME

网络传销

网络传销依托互联网平台，通过社交媒体、专用 APP、电商网站等渠道构建多层级网络，以吸引会员加入和发展下线获利。与传统传销相比，网络传销不再依赖实体组织和固定场所，而是利用互联网的跨地域性和去中心化特点，借助虚拟货币、“拼团购物”等热点概念包装其非法本质，通过加密支付和虚拟交易隐藏资金流向，使其更难被追踪和打击。同时，网络传销的传播路径从“熟人推荐”转变为“广泛引流”，利用算法推广和新媒体传播快速扩展受众范围，涵盖不同社会群体，甚至跨越国界。

1. 常见场景

电商返利

模式：通过互联网第三方平台介入商家和消费者的交易过程，许诺在平台的消费额度部分返回，或通过现金消费送等额积分等形式，诱导消费者注册会员消费和商家加盟平台回流货款。

特点：网络购物返利模式具有较强的吸引力和迷惑性，借助“消费返利”吸引普通消费者参与，打着电商创新的旗号掩饰其非法本质。

典型案例：江西精彩公司传销案

江西精彩生活投资发展有限公司以“太平洋直购官方网”为平台，打着电子商务的幌子，要求参与者通过购买商品或缴纳保证金获得会员资格，并按照一定顺序组成层级，间接以发展人数作为返利依据，形成传销网络。

虚拟币传销

模式：借助虚拟货币或区块链技术概念，推出所谓“高增长虚拟币”或“链游项目”。用户需投资代币或平台资产，并通过发展下线获益。

特点：该模式通常利用区块链技术的去中心化特性作为噱头，包装为高科技创新项目。通过智能合约、代币经济等技术外衣，增强迷惑性和宣传效果。资金主要通过新用户的投资维持运转，具有高度隐蔽性。

典型案例：Plus Token 虚拟币网络传销案

Plus Token 以“虚拟币钱包”为幌子，宣称通过“智能狗搬砖”实现月收益高达 60%，并通过拉人头发展下线，按投资金额和人数分为普通会员、大户、大咖等等级，吸引 200 多万人参与，非法吸纳资金超 50 亿元人民币。2019 年 6 月，平台因资金链断裂停止提现并跑路，众多投资者损失惨重。

股权众筹

模式：以企业即将上市为由，诱导投资者购买原始股或参与股权众筹，承诺上市后获得高额回报，同时通过发展下线投资形成层级网络。

特点：此类模式利用上市公司的高收益前景吸引投资者，往往通过虚假宣传夸大公司实力和市场潜力。常结合“饥饿营销”策略，营造紧迫感以迅速吸纳资金。

典型案例：广州放飞旅游公司股权众筹传销案

放飞公司推出“中国放飞股权众筹网络平台”，以“放飞股”高额回报为诱饵，吸引投资者加入。投资者需购买放飞股并发展下线，按层级返利，最高层级返利不封顶。同时，推出虚拟“放飞币”和旅游套餐，营造收益稳定的假象。2016 年，平台因资金链断裂陷入崩盘，投资者损失惨重。

微商代理

模式：以微商代理或社交电商为名，通过缴纳加盟费或购买产品获得代理资格，代理商可通过销售商品或发展下线获取提成。

特点：利用社交媒体传播的快速性和熟人关系的信任度，隐蔽性极强。通过多层级代理制度和销售差价构建网络，表面以商品交易为主，但实质是层级返利。

典型案例：安美拉微商代理传销案

浙江某贸易有限公司通过招募微商代理销售“安美拉”系列产品，将代理商划分为不同级别，尤其针对“梦想合伙人”级别设立了推荐奖、销售提成等奖励机制。代理商通过推荐他人加入获得资格，并根据下线人数和业绩获取报酬，逐步形成上下线层级关系。在此模式下，该公司发展了超过 1000 名“梦想合伙人”代理商。由于其经营方式具备传销特征，最终被执法部门依法查处。

广告盈利

模式：以“广告分红”为名，声称参与者通过观看广告或点击链接即可获得收益，但需缴纳会员费或发展下线提升收益等级。

特点：此模式通常承诺简单操作即可获得高额回报，吸引小额投资者参与。资金流动依赖新用户缴费，运营周期较短，风险极高。

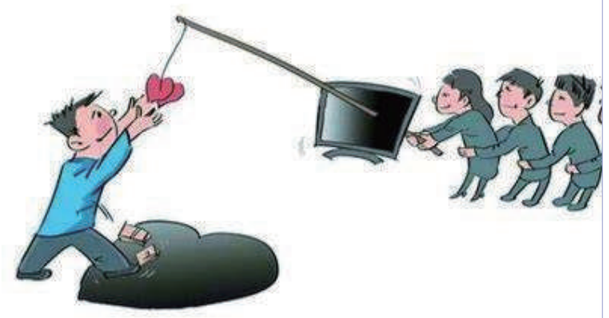
典型案例：“YY 购”传销案

黑龙江合商网络科技有限公司搭建并运营“YY 购”商城 APP，以“深耕养老产业、服务老年人”为幌子，采用会员缴费、观看广告返现和团队计酬的模式，吸引会员不断发展下线，承诺高额回报，实质为传销活动。截至案发，该平台发展会员 218 万余人，层级高达 32 层，累计充值金额超过 38.35 亿元，提现金额约 35.65 亿元。

慈善互助

模式：借助“公益慈善”或“互助计划”名义，吸引用户缴纳会费参与，并通过发展新会员获益，承诺互助金或返利。

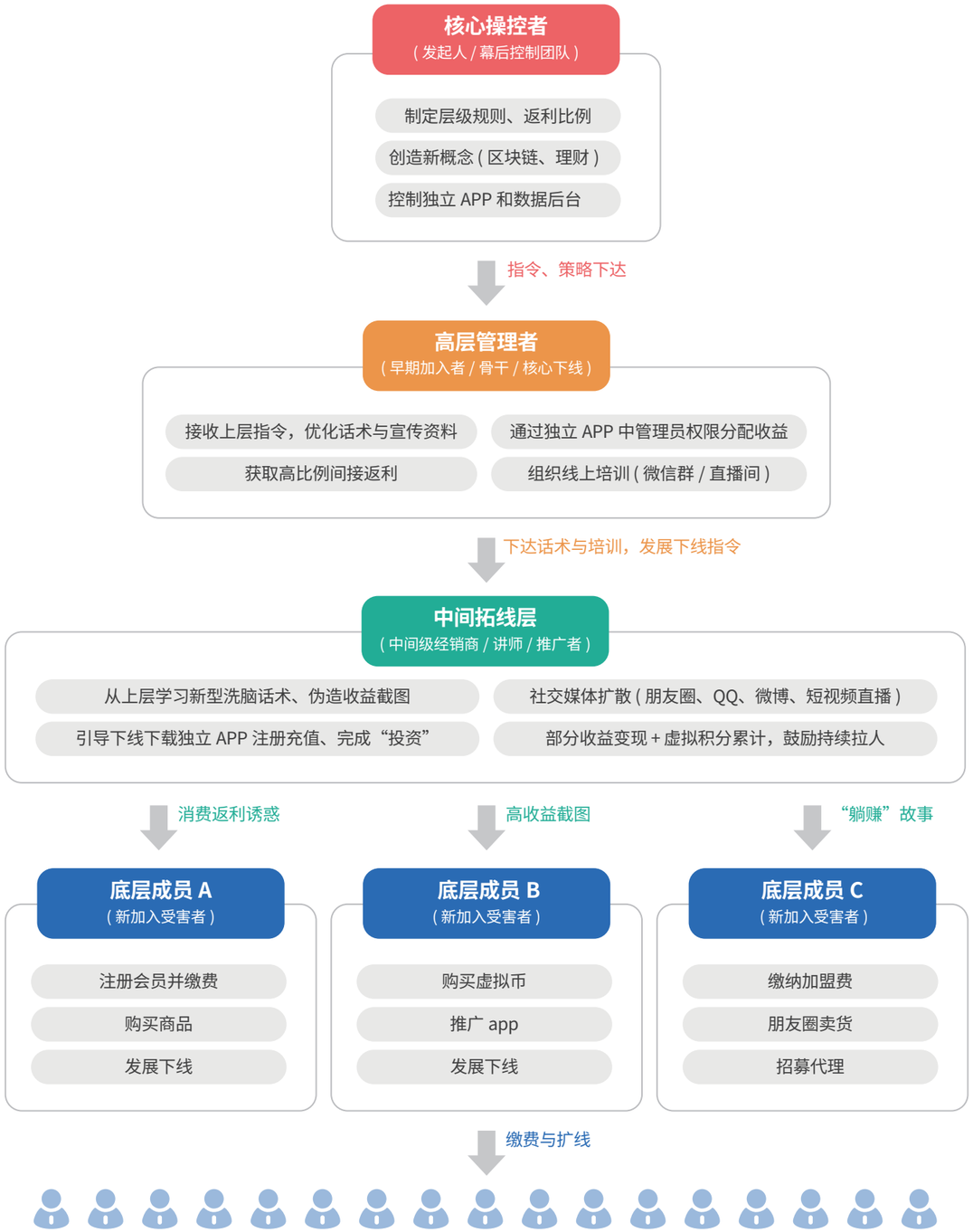
特点：该模式以慈善幌子增加信任感，通过伪装为互助计划吸引资金。资金多在内部流转，组织者通过层级返利获利。



典型案例：众诚慈善互助平台案

“众诚慈善互助”网站平台以高额回报为诱饵，吸引公众投资，要求会员通过“提供帮助”方式打款，十日后可申请“得到帮助”并获取利息。会员还可通过推荐他人加入获得“推荐奖励”。平台通过发展下线不断扩大规模，涉及江苏、上海、安徽等多个省市的约 2000 人。由于缺乏实际经营，资金链很快断裂，导致多数会员无法收回投资款。

2. 组织架构与运作模式



组织架构

网络传销组织的结构呈典型的“金字塔”式层级分布。该架构有以下特征：

1 **多层级构成：**自上而下，由核心操控层（发起人及骨干）统筹规划，通过中间拓线层（培训者、讲师及资深代理）向底层成员不断传递信息和策略。底层成员（新加入者）为整个金字塔的基础，他们的不断加入与资金投入为上层提供利润。

2 **上下线关系明确：**每位成员在加入后即成为其“上线”的下线，同时亦可通过发展新成员构建自己的下线网络。这种上下线关系层层叠加，既强化了组织的扩张性，也为核心层获取持续收益奠定基础。

3 **入门费用与会员制度：**新加入者需支付一定入门费或以高价购买“指定产品”“会员资格”进入体系。此初始资金投入是传销组织资金流入的关键一环，也成为抽成与返利机制的基础。

4 **层级返利与团队计酬：**收益分配通常与成员的层级深度和下线数量挂钩。高层成员可从下层庞大的成员群体中获得间接返利，层级越深、网络越庞大，上线在资金回流过程中的获利比例越高。部分组织还引入团队业绩计酬，以整体业绩作为奖励依据，鼓励成员积极拓展下线，扩大网络规模。

运作特点

网络传销运作高度依托互联网和移动通信技术，不同平台与渠道相互交织，使其具备快速扩散、隐蔽运作和多样化包装的特征。

1 **社交媒体平台传导：**利用微信、QQ、微博、短视频和直播等社交媒体渠道，组织成员在熟人关系基础上构建初步信任，借由“成功案例”“高收益截图”“富裕生活展示”加强说服力，吸引更多用户加入。熟人信任机制与社交场景下的快速传播能力，使信息在极短时间内广泛扩散。

2 **独立 APP 与技术包装：**不少组织开发独立 APP，将其伪装为投资、理财或电商平台。APP 内嵌充值、提现、积分及等级晋升等功能，赋予用户“在平台内部投资、消费”的错觉。借助虚拟货币、区块链等技术热点概念对外宣传，平台号称“透明交易”“智能合约”与“创新模式”，从而提升信誉度和吸引力。实际资金流向却隐蔽于平台内部，普通用户难以窥其真貌。

3 **虚拟社群与培训体系：**传销组织者往往在 QQ 群、微信群、论坛或独立社区中建立培训与交流群组。核心和中间层成员通过在线课程、虚拟讲座、语音会议等方式向底层成员传递“成功学”话术、虚构财富神话和投资数据。从而在群体氛围中强化信任、模糊风险意识，使新成员在不断洗脑下保持持续投入和拉新人加入的热情。

4 **隐蔽性与扩张性：**借助互联网跨地域、去中心化和信息不对称特性，传销组织可快速渗透不同区域与人群，延长资金链存续时间。灵活变换噱头（从电商返利到虚拟币投资再到慈善互助）和平台包装（独立 APP、多渠道媒体运营）均可掩盖其非法本质，增加监管和识别难度。

3. 取证鉴定思路

随着互联网技术的普及与创新，传统线下传销已逐步向线上迁移，形成新型的网络传销犯罪形态。此类案件通常依托多样化的技术载体（如独立 APP、社交媒体平台、云端服务器以及虚拟支付渠道）快速扩散，资金流转隐蔽且复杂，层级结构庞大而多变。电子数据取证与司法鉴定人员需在合法、合规前提下，通过严谨的取证程序和专业化分析手段，从人员关系、资金走向和技术特征多维度切入，以形成完整、可靠的证据链条，为司法机关的公正审理和准确定性提供坚实数据支撑。

以下为网络传销案件的取证鉴定思路：

1 明确取证目标与重点

在正式开展取证前，应首先明确案件的核心问题与关键点：

成员角色定位：识别每位涉案人员在传销网络中的层级位置及其上下线关系，梳理整体人员架构。
资金流向与收益模式：厘清资金从底层成员向上传递的路径和分配规则，明确抽成、返利、佣金比例与核算方式，从而判断组织的本质特征与获利模式。
数据存储与平台类型：确定传销组织所依托的技术载体（独立 APP、社交媒体账号、云服务器、虚拟货币交易平台等），锁定数据存放与传输的关键节点。

在明确以上要素后，取证团队可有针对性地规划数据收集和分析策略。

2 确定数据来源与技术路径

结合报案材料、初步侦查线索和案件特征，尽早确定数据可能的存储位置与访问权限：

社交媒体与通信工具：如微信群聊、QQ 群、朋友圈、短视频平台账号等，这些信息渠道通常用于传销组织的宣传与拉人头活动。
独立 APP 与网站：涉案 APP 或网站往往内置注册、充值、积分统计、提现等功能模块，其后台数据库、API 日志和用户交互记录是关键取证点。
云服务器与 CDN 节点：若嫌疑人使用云服务器或 CDN 隐藏真实 IP 地址，需通过法律程序向服务提供商申请相关数据，为后期镜像提取与数据还原奠定基础。

3 数据采集与证据固定

在合法程序与技术标准的框架下，对涉案数据进行提取与固定，确保证据的客观性与可验证性：

涉案终端取证：在控制嫌疑人后，使用专业取证工具对其手机、电脑等设备中的聊天记录、转账凭证、用户 ID 及邀请码截图进行提取。必要时对可疑 APP 进行逆向分析与抓包测试，锁定通信协议和数据传输指向的服务器地址。若涉虚拟币，应通过钱包地址、交易哈希开展区块链溯源。
服务器与数据库取证：对锁定的服务器及数据库进行现场或异地镜像提取，将用户表、层级关系表、交易记录表、积分表等关键信息进行安全备份。前后台数据需对照分析，以确定计量单位与转换规则。如遇数据缺乏标注，可结合嫌疑人供述、测试账号数据与前端显示信息对照判断实际含义。

4 数据清洗与关联分析

针对已提取的数据进行初步清洗和关联，剔除冗余、无效及测试数据，确保后续分析结果的准确性和可用性。

数据完整性核验：对提取的数据进行哈希校验与重复检查，确保取证过程无遗漏或篡改。
数据去重与筛选：剔除无关信息（如测试账号、重复记录、无实际资金关联的系统默认节点），确保剩余数据具有实质证据价值。
表间关联构建：利用用户 ID 作为主键，将用户信息表与层级关系表、交易表进行关联，初步形成用户 - 上级 - 下级 - 资金流转的映射关系，为后续层级还原与资金分析提供基础结构。

5 多维度层级结构还原

基于关联数据，重构网络传销架构，明确各级别成员的上下线结构及层级深度。

人员纵向追踪：对每个用户 ID 自上而下（或自下而上）追踪，确定其上线节点、下线数量、最底层成员数量和层级深度，构建完整的人际关系网。
真实用户判定：基于实名注册信息和资金投入记录确认用户身份，筛除系统默认节点和无实际参与的虚假账号，确保统计结果准确。
层级深度与规模评估：确定整个网络传销体系的最大层级数、参与人员总数和各子体系规模，为后续整体定性与量刑提供基础数据。

6 功能逻辑与业务流程验证

在可控条件下对涉案 APP 或平台进行仿真操作，验证业务流程与功能逻辑，以确定其传销本质。

功能结构分析：对 APP 中的注册、充值、提现、升级会员、层级返利等关键功能点进行技术分析与数据抓取，确定平台抽成比例、上级返利机制、是否存在持续拉人头扩张下线的行为。
证据关联性与定性：将 APP 功能取证结果与前期侦查获取的数据（聊天记录、资金往来）相互印证，确定其是否实质从事传销活动，以及传销模式的层级深度与参与规模。

7 鉴定意见书编撰

将前述取证、分析结果和验证结论整合为鉴定意见书和证据报告，为检察机关与法院审理提供权威参考。

数据报告与图谱呈现：对上下线关系、资金链路、层级结构和获利数据进行表格化、图表化表达，配合文字说明，形成可读性强的证据材料。
证据支持与案件分析：依据前期分析结果，结合司法鉴定工作中提取的电子数据，提供关键证据支持，包括网络传销模式的运作特点及核心要素。同时，对涉案金额、参与人员数量及层级深度等进行数据分析，为执法部门定性案件提供客观依据和参考。

4. 典型案例

虚拟币传销案

区块链取证技术锁定传销铁证，精准打击涉案数亿元新型网络犯罪

本案是一起典型的利用“元宇宙”、“区块链”等高新概念进行包装，通过发行虚拟币 BNQ，以“质押挖矿”、“节点分红”为诱饵，进行组织、领导传销活动的重大案件。奇安信洞鉴协助某市公安局，通过对涉案智能合约的深度代码审计和对海量链上交易数据的穿透式分析，成功固化了该项目的传销犯罪证据。我们精准还原了其金字塔式的组织层级和“拉人头”式的资金分配模式，为执法部门提供了关键性的电子数据证据，最终协助捣毁了这一涉案金额高达数亿元人民币的特大网络传销组织。

案件背景

2023 年，多地投资者报案称，一个名为“BNQ”的虚拟币投资项目无法提现，疑似“跑路”。警方初步调查发现，该项目无合法公司主体，是一个典型的以团伙合作形式运作的网络传销组织。该组织打着“区块链技术”的幌子，发行毫无价值的“空气币”BNQ，通过微信群等渠道，以“质押挖矿、高额返利”为诱饵，吸引了超过 2000 名人员参与，且层级在三层以上，具备缴纳入门费、层级计酬和虚假宣传等传销特征。

由于该案技术性强、涉案人员众多且资金流转均在区块链上，为彻底查清其运作模式和犯罪事实，警方委托奇安信洞鉴进行全面的电子数据司法鉴定。

洞鉴解决方案

01 智能合约功能分析，锁定传销铁证

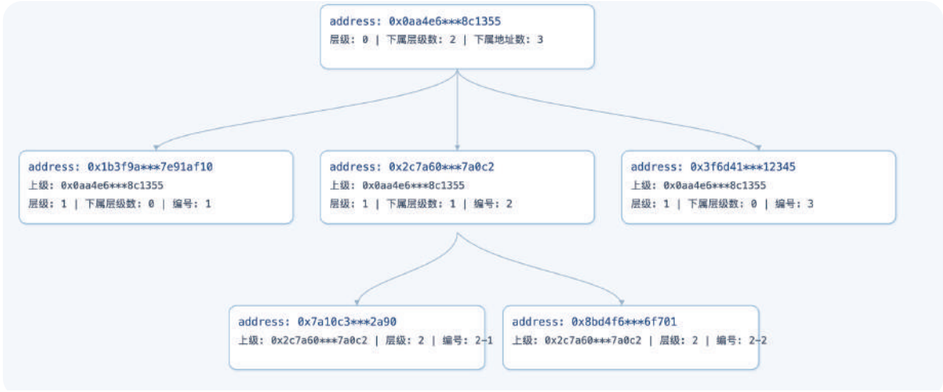
鉴定专家首先获取了涉案项目部署在区块链上的核心智能合约代码，通过对代码进行逐行分析，发现其功能设计完全服务于传销活动：

1. **强制绑定与层级构建：**在核心的质押函数中，代码强制要求参与者必须填写上级推荐人的地址才能进行投资，从代码层面锁定了“拉人头”的入门机制。
2. **还原返利机制：**合约中的函数清晰地定义了多层级奖励机制。团队奖励向前计算七层，其中直接上级可获得下线奖励数量的 30%，二至六层各获得 10%，第七层获得 20%。这一发现精准还原了其团队计酬的核心模式。
3. **高门槛退出机制：**领取奖励函数显示，用户实际获得的奖励仅为计算出奖励的 92%，其余部分被以“节点费”和“NFT 奖励”的名义转移。此外，设置苛刻了提现条件（如推荐人数、质押时长等），最大限度将资金锁定在平台内部，延缓资金链断裂。

02 链上数据取证，重现层级网络与资金流

利用区块链公开透明、不可篡改的特性，鉴定专家通过区块链浏览器的 API 接口，编写自动化 Python 脚本，获取了与 BNQ 项目相关的全部链上交互数据。

1. 海量数据固定：成功获取并固定了包括三个版本的 BNQ 代币合约、质押合约、节点合约等 **12** 个核心地址的数十万条交易记录，并对数据进行了严格的哈希校验，确保证据合规。
2. 梳理层级关系：基于智能合约中记录的推荐人关系，我们成功梳理出所有参与用户的上下级关系。最终绘制出了一张包含 **2487 个核心参与地址、最高层级达 43 层**的完整传销网络层级图。



3. 统计涉案资金：对链上数据进行统计分析，确认在“质押和奖励”及“节点和奖励”两个主要合约中，用户累计投入的 USDT 总额超过 466 万。同时，对涉案核心人员及团队的资金流水进行了穿透分析，清晰呈现了资金的归集与分配情况。

备注	转入 USDT 数量	交易笔数
地址 A	14,293.8421	11
地址 B	2,05.4428	4
地址 C	97,532.2196	28
地址 D	7,613.2083	6
地址 E	23,781.9991	8
地址 F	65,447.5512	15
地址 G	1,973.004	3
地址 H	12,604.9887	9
地址 I	44,201.7743	17
合计	270,514.09	101

案例价值

01 / 锁定关键犯罪证据

通过对智能合约的底层代码分析，从技术层面无可辩驳地证实了 BNQ 项目“拉人头、入门费、团队计酬”的传销本质，为案件的定性提供了核心依据。

02 / 查明资金真实规模与去向

精准统计出涉案总金额高达数亿元人民币，并清晰还原了资金在区块链上的完整流转路径，为后续的资金查封、追缴和挽回受害者损失提供了明确指引。

03 / 厘清组织架构与核心人员

完整绘制的传销网络层级图，帮助办案人员迅速锁定了组织内的核心头目、骨干成员及其下线网络，为“全链条”打击犯罪团伙提供了关键情报。

虚拟玉石投资平台传销诈骗案

抢拍玉石收益高？司法鉴定揭露新型传销陷阱

2024 年，某地公安局经侦大队打掉一个以“投资玉石”为名、搭建“玉石寄售”网络平台实施传销诈骗的犯罪团伙，涉及 23 个传销平台。奇安信洞鉴受托为此案提供技术支持，协助公安部门固定了服务器上的 23 个售卖平台数据，并对固定的服务器数据进行了深入细致的分析，生成了人员架构图，为打击传销诈骗活动提供了有力证据。

案件背景

2023 年 11 月，某地经侦大队陆续接到多名居民的报警，称他们在某些网站平台上投资虚拟玉石，然而这些平台突然关闭，导致投资无法变现，许多投资者蒙受了巨大的经济损失。通过初步调查，公安机关发现这些所谓的“玉石投资平台”其实是一个精心设计的骗局。犯罪团伙以高回报为诱饵，吸引大量投资者注册和充值，并通过虚假的寄售交易模式，制造出平台繁荣的假象。更为严重的是，该团伙不仅自建平台，还诱导受害者再去发展下线，形成了 23 个相互关联的售卖平台，构建了一个庞大的传销网络。

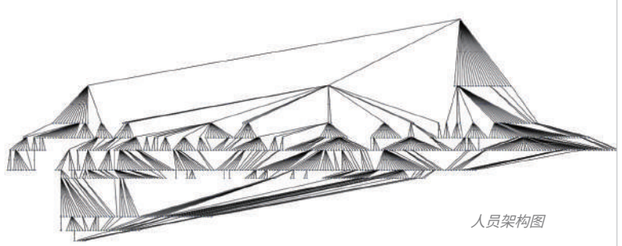
面对这一棘手情况，当地警方迅速行动，并委托了奇安信洞鉴为此案提供固证及司法鉴定服务。

洞鉴解决方案

奇安信洞鉴在接到委托后，迅速展开了一系列技术支持工作，包括数据提取、镜像固定、数据分析等，揭示了犯罪团伙的运作模式：

1 服务器证据提取固定

对服务器上的 23 个售卖平台数据进行了全面提取，通过专业的数据镜像固定技术，确保了提取数据的完整性和可靠性。



人员架构图

2 数据库访问与数据提取

使用数据库管理工具连接并查询数据库，提取平台的用户信息、订单记录、佣金记录、手续费记录等详细数据，生成了多个数据文件，如“用户信息 .xlsx”、“寄售订单 .xlsx”等。

3 数据分析与结果汇总

对提取的数据进行整理，计算每个平台的总交易金额、交易时间和玩家人数。使用 Python 脚本生成用户的层级关系图，并标记出重点用户，最终生成了“人员架构 .pdf”等文件。

平台名称	交易时间	交易总金额	玩家人数
韩 **	2023.12.4 至 2024.1.5	56,321,842	156
勇 **	2023.11.7 至 2023.12.21	9,321,041	134
涵 **	2023.11.6 至 2023.12.8	56,321,234	321
鑫 **	2023.11.3 至 2024.1.1	16,321,125	234
源 **	2023.12.5 至 2023.12.23	54,321,534	231
欣 **	2023.12.7 至 2023.12.21	43,214,696	145
羊 **	2023.12.6 至 2023.12.8	13,321,398	123
鑫 **	2023.12.3 至 2024.1.1	21.321,887	123
鑫 **	2023.7.17 至 2023.11.10	321,453,432.99	962

平台数据统计（非真实数据）

案例价值

01 / 清晰呈现犯罪团伙结构

利用 Python 脚本生成用户的层级关系图，并标记出重点用户，使得犯罪团伙的运作模式和层级关系一目了然，能够帮助公安机关快速锁定嫌疑人，为后续的审判提供了重要的参考。

02 / 提供全面证据支持

为客户提供数据提取固定、分析鉴定全链条服务，提供科学、客观、公正的鉴定意见，确保案件审理过程中的证据可靠性和真实性，提升法律诉讼的成功率。

03 / 打击传销诈骗犯罪

通过精准的数据分析和证据提取，奇安信洞鉴团队协助公安机关快速抓捕嫌疑人，有效打击了传销诈骗等网络犯罪行为，维护了社会的安全与稳定。

03

ONLINE GAMBLING
网络赌博

网络赌博是指通过互联网平台开展的赌博活动，涵盖传统赌场游戏的线上化（如德州扑克、轮盘赌等），以及虚拟竞技、网络彩票等衍生形式。近年来，部分网络赌博进一步与在线游戏、电商、直播等场景深度融合，通过娱乐化、社交化的包装吸引用户，甚至使用户在无意识中参与其中。相比传统赌博，网络赌博打破了时间和地域的限制，依托技术手段实现操作便捷、传播迅速和隐蔽性强的特性。

1. 常见场景

直播式网络赌场

模式：将传统线下赌场搬到线上，玩家通过注册账户和充值参与，包括百家乐、德州扑克、轮盘赌、骰子等经典赌场玩法。

特点 1：操控结果

庄家通过后台算法调整玩家输赢，初期让玩家小额获利吸引加大投入，随后通过降低胜率让其迅速亏损。

特点 2：虚假直播

平台声称提供真人在线发牌直播，但实际利用预录视频或预设剧本营造现场感，欺骗玩家信任。

特点 3：提现门槛

玩家赢取大额奖金后，平台常以账号异常或系统问题为由限制提现，拖延甚至拒绝提款。

体育竞技类赌博

模式：以体育赛事（如足球、篮球、电竞比赛等）为基础，玩家根据赔率进行投注，投注形式包括胜负竞猜、比分预测和进球时间等。

特点 1：操控结果

庄家可能伪造比赛结果或通过假赛操纵比赛进程，确保平台盈利。

特点 2：动态赔率

根据玩家投注金额实时调整赔率，引导更多玩家追加投注，形成庄家优势。

网络游戏类赌博

模式：以网络游戏为载体，将麻将、捕鱼、炸金花等游戏化玩法与赌博模式结合，用户使用虚拟货币下注。

特点 1：迷惑性强

通过游戏包装吸引用户，尤其是年轻群体，将赌博行为隐藏在娱乐体验中。

特点 2：诱导充值

利用初期的低门槛投注和高胜率诱导玩家追加充值，在玩家持续充值后逐步降低获胜概率。

微信红包赌博

模式：通过组建在线聊天群采用发放网络红包方式进行赌博。玩家可以下注买单双、大小、数字等，以抢到的红包金额为开奖结果。

特点 1：便捷性强

无需额外下载应用，直接通过社交平台完成下注和参与。

特点 2：资金高频消耗

每轮下注金额虽小，但频率极高，玩家资金消耗速度加快。

特点 3：社交扩散

利用群成员间的熟人关系拉人参与，快速扩大群组规模，同时提高隐蔽性。

娱乐购物类赌博

模式：以购物抽奖、娱乐游戏结合直播的方式开展赌博活动，玩家通过购买商品获得抽奖机会，商品本身可能为低价值或虚假商品。

特点 1：消费捆绑

通过直播电商平台，用“购物返现”或“商品增值换购”包装赌博行为，吸引追求新奇消费体验的用户。

特点 2：维权困难

中奖后实际兑现商品价值远低于预期，由于消费纠纷与赌博行为难以界定，增加维权难度。

2. 网络赌博运营模式

1 上游资源层：技术与资金的隐性驱动

技术链

数学模型与算法设计：赌场团队基于线下长期累积的赌博经验，将胜率、赔率和奖池分配等参数数学化、算法化。在高技术手段驱动下，这些模型实时调整，为庄家长期盈利提供稳定保障。

快速部署和包网解决方案：包网团队为平台运营者提供“一站式上线服务”，包括服务器搭建、前后端架构、数据库和 API 整合。这使得缺乏技术背景的创业者，也能低门槛、高效率地开办网络赌博平台。

用户数据监控与分析工具：技术链中还包含数据收集与分析模块，通过埋点分析（Tracking）、大数据挖掘和人工智能算法，持续记录、分层和预测用户行为，以优化玩法设计、定向营销策略和风险控制措施。

资金链

跨境资金流转：虚拟货币、第三方支付平台以及地下钱庄共同构筑复杂的资金网络，使犯罪团伙能在不同司法管辖区灵活调度资金，规避监管和资金追踪。

高灵活度的支付模式：利用电子钱包、加密货币，赌博平台可实时处理国际化用户的充值与提现需求，在不稳定的监管环境中保持资金运转的顺畅。

在上游资源层，技术链与资金链为平台提供了“快速搭建 - 持续迭代 - 隐匿资金”的综合基础，使网络赌博生态具备快速扩张、灵活布局、全球化运营的可能性。

2 核心平台层：多样玩法与数据驱动的盈利中枢

多样化玩法设计

传统玩法升级：由早期的简易彩票、跑马投注，转向真人荷官、AR/VR 赌场、体育竞猜甚至实时直播的娱乐化内容，为用户提供沉浸式体验。

动态策略：玩法设计并非一成不变，平台可根据用户群体的偏好对游戏难度、奖励频率、UI 交互进行快速优化，提高用户留存与再投注率。

数据驱动策略优化

行为分析与算法调优：平台通过采集用户的投注频率、在线时长、充值 / 提现频率和互动行为，预测用户粘性和风险偏好，从而灵活调整赔率、活动推送频率和 VIP 特权方案。

精细化运营：面向高价值客户（如高净值玩家）可定制专属活动和更高投注限额，对低价值玩家可采用小额返利或赠币手段延长其在线时间，从而实现用户最大化价值转换。

在核心平台层，网络赌博平台将上游资源（技术、资金）内化为具体的产品和服务，以数据为导向灵活调控，从而构建强大的盈利中枢和用户吸引力。

3 下游用户生态层：推广裂变与角色转化的自我扩张机制

推广链：拉新与裂变

广告引流与多元媒体植入：平台利用网络广告、社交媒体、直播平台内嵌插件等手段大量吸引潜在用户。在视觉、体验和情感诱导上精心设计，通过美女荷官直播、沉浸式 AR 场景、即时反馈的音效与动画刺激用户的感官和心理。

社交裂变与返佣机制：平台设计多层级的代理返佣制度，通过老玩家拉新玩家的层层扩张实现用户指数级增长。这类似传销链条，玩家为弥补损失或获取佣金，将身边的人引入赌博生态。

用户链：用户—赌徒—推广者的身份演变

初级用户：最初只是抱着好奇或娱乐心态尝试小额下注，受精美画面、跨平台登录和便捷支付吸引，进入平台。

深度赌徒：当用户不断输钱却不甘退出，沉没成本心理让他们加大投入，一步步陷入难以自拔的恶性循环。

推广代理：在持续亏损下，平台为用户提供“转化机制”：成为代理，通过发展下线可获取佣金，用这种方式弥补自己的损失。此举实质上将“赌徒”转化为“帮凶”，不断为平台拉新和创造收入。

在下游用户生态层，推广链与用户链交织为一体：前者吸引新用户进场，后者将用户沉陷转化为代理推广者，进一步扩张用户群的规模与稳定性。如此反复裂变，使平台用户量与收益呈现不断增殖的态势。

4 闭环反馈与自我强化：数据与资金的往返循环

数据回流：用户行为数据、推广绩效数据和资金流动信息回流至平台与上游技术链。通过对这些数据的实时分析与建模，平台不断优化算法和调整策略，使得之后的推广、玩法设计和资金运用更高效，更有针对性。

资金滚动与资源强化：随着用户群扩张和代理层级增加，平台营收不断增长。新增的利润用于采购更高质量的技术服务（加强服务器安全、使用更先进的加密手段）、拓展资金通道（更多支付手段）以及升级推广策略（投放更精准的广告），从而强化上游资源配置，提高平台抗风险与逃避监管的能力。

黑灰产交织：在这一闭环生态中，还存在各种外围服务，如数据黑产、洗钱工作室、推广中介机构，不断催生出更为庞大的产业链条。这些灰黑产力量与平台共生互利，进一步提升整体抗打击能力，使网络赌博如“毒瘤”般顽固生存。

3. 取证鉴定思路

网络赌博平台通常由前台（面向普通用户，提供注册、登录、充值、投注、提现等功能）和后台（由犯罪团伙控制，用于监控用户数据及资金流向）构成。前台数据可通过访问、录屏和抓包等方式较为直接地获取；后台数据则因权限受限需结合嫌疑人供述、设备取证及 VPN 访问记录等更深入手段完成。通过明确目标、前台取证、流量分析、后台访问、数据整合、资金溯源以及最终报告编撰的步骤，可构建完整、严谨的证据链条，为司法机关提供有力技术支撑和数据依据。

以下为网络赌博案件的取证鉴定思路：

1 明确取证目标与重点

在正式取证前，对涉案人员信息、平台特征、涉案设备以及可能使用的赌博软件或网站进行全面了解，为后续取证提供指引。

案件基本情况收集：根据报案材料、线索与侦查信息，明确涉案人员身份、涉案平台（APP、网站）类型及使用的设备范围。

核心目标界定：确定需获取的关键电子证据（账户信息、用户注册数据、充值提现记录、投注数据、资金流向）和技术手段选用（终端取证工具、日志分析工具、云取证工具等），为后续取证流程制定方案。

2 前台（用户侧）数据取证

通过访问赌博网站或 APP 的前台功能进行勘验及录屏，收集注册流程、登录操作、充值提现记录等前台可见数据。

可疑 APP 获取：对受害人手机中下载历史、聊天记录进行检查，提取相关下载链接和 APP 安装包，使用仿真环境（模拟器或真实手机）访问下载链接、扫码获取 APP 安装包，完成 APP 安装与运行的全程录像。

功能勘验与属性确认：以全程录屏方式对 APP 核心功能（注册、登录、充值、下注、提现、玩法选择）进行操作与记录，确定 APP 提供赌博功能的事实，为案件初步定性提供证据支撑。

3 前台网络流量分析

在操作前台功能的同时，对数据传输过程进行抓包分析，通过识别通信数据包结构、目标服务器地址及接口，定位到后台真实 IP。

实时抓包与流量分析：在运行 APP 时对网络通信进行抓包（可使用 Wireshark、Fiddler、Charles 等工具），捕获 APP 与目标服务器之间的数据包，通过分析抓包数据锁定用户注册信息发送目标服务器的 IP 地址，获取应用后台接口、支付接口及日志上报路径。

应对 CDN 加速与隐藏 IP 措施：若抓包获得的服务器地址为 CDN 节点，依法向 CDN 服务提供商申请调取真实服务器 IP 信息，为后续溯源奠定基础。

4 后台（犯罪团伙侧）访问权限获取

在嫌疑人到案及关键物证到手后，通过询问和设备取证掌握后台地址、账号、密码和权限层级，为深入获取核心数据创造条件。

后台地址锁定：根据嫌疑人供述及其电子设备数据，还原后台管理系统 URL 和初始登录信息。

账号权限梳理：确认不同角色（运营、技术、财务）的后台访问权限层级，重点锁定高权限账号。

VPN 与访问限制识别：检查嫌疑人设备、配置文件或聊天记录，确认后台是否需通过 VPN 访问，若 VPN 服务器已无法使用或未续费，应在第一时间固定相关 VPN 配置与访问记录，作为间接证据辅助分析。

5 后台系统数据采集

在具备后台访问条件后，对后台数据进行全面搜集和固化，同时与云服务提供商协作获取完整镜像和日志。

后台功能确认：实地操作后台各模块，全程录屏获取用户信息、充值提现流水、代理等级、抽头比例及财务记录。

数据导出：导出参赌人员信息、交易记录、网站代理列表、盈利抽头记录、财务报表等关键数据，若使用云服务平台，应依法与服务提供商沟通协作，获取服务器原始日志、数据库备份和全量数据镜像。

数据清洗：对后台数据进行必要的数据清洗和比对，确认数值单位及计量方式；若有疑问，可结合前台数据、嫌疑人供述及测试数据进行校验。

6 资金流向溯源与账户关联分析

对充值、提现、投注等业务数据进行关联分析，构建完整资金链路和层级结构，从底层用户到上层控制者，明确盈利模式及非法获利主体。

资金路径构建：关联充值提现流水与用户、代理信息表，绘制资金流向图，标识核心账户、抽头比例与获利金额。

层级与角色定位：确定平台中的普通用户、代理、核心控制人分布及层级关系，为案件组织架构与资金传递路径提供清晰证据。

7 鉴定意见书编撰

将前台取证、网络抓包、后台数据、资金链条及 VPN 访问情况整合为有序、易读的鉴定报告，并以统计表、图表、结构图形式直观呈现，为司法审理提供有效支撑。

数据整合与呈现：将各环节取证结果合并，配以表格化数据、流程图、层级关系图，直观展示平台运营模式和资金逻辑。

定性分析与意见提出：依据收集数据和分析结果，明确平台赌博性质、涉案金额及获利规模，为检察机关、法院定罪量刑提供客观、全面的专业建议。

4. 典型案例

特大非法网络销售彩票案

多源镜像还原 + 数据库深度解析，精准锁定会员代理网络与交易流水

本案是一起特大非法线上销售彩票案件。犯罪团伙构建了一个集销售、推广、支付于一体的庞大网络平台，非法发展会员逾 2.1 万，代理网络盘根错节。奇安信洞鉴通过对多源服务器镜像的还原、虚拟仿真、数据库深度解析及 SQL 穿透查询，不仅完整复现了“运营管理系统”的后台环境，更成功提取了会员、代理、投注及资金流水等海量核心证据，并对多家涉案店铺的销售结构与层级模式进行了精准画像。该成果为办案机关锁定关键涉案人员、厘清资金链条、固定犯罪事实提供了强有力的证据支撑。

案件背景

2024 年，犯罪嫌疑人王某某等人成立公司，在未获得彩票销售资质的情况下，开发上线“店 ***”APP，从事非法线上彩票销售活动。该团伙组织严密，纠集多人成立等多个销售团队，通过小红书、抖音等渠道大肆推广引流，并搭建专门的支付通道转移、洗白非法获利。案情重大，为彻底查清该团伙的犯罪事实，固定电子证据，特委托奇安信洞鉴对涉案的核心服务器数据进行司法鉴定。

洞鉴解决方案

面对包含服务器镜像、数据库备份等多份、多类型检材的复杂情况，奇安信洞鉴专家制定了“系统还原 - 数据恢复 - 关联分析”的综合鉴定方案。

01 涉案 APP 运营管理系统还原

利用计算机仿真取证系统，加载了涉案服务器的镜像文件，并搭建了与原始环境高度一致的仿真系统。通过分析 Nginx 服务的配置文件，鉴定人员厘清了服务请求在多个节点间的转发关系。通过修改 hosts 文件、配置数据库连接信息，最终成功搭建了仿真环境，并使用委托方提供的账号密码，顺利登录涉案 APP“运营管理系统”后台，为后续数据分析打开了通路。

02 主备数据库恢复

鉴定专家利用虚拟机搭建 CentOS 7 + 宝塔面板环境，通过编写并执行自动化脚本，分别从数据库文件和备份文件中，成功恢复了 6 个核心业务数据库及其备份。

03 海量数据深度分析

基于恢复的数据库，专家设计了多组复杂的 SQL 查询语句，对海量数据进行穿透式分析：

1. **会员与代理画像：**精准提取了全部 21,177 名会员信息（含普通用户、店铺店主、店铺员工）和 20,991 条代理数据。
2. **店铺流水穿透：**针对多个销售团队，按时间范围，深度统计了其用户量、总销量、自购 / 跟单销量及提成金额等关键经营数据。
3. **出票与派奖核查：**对主数据库和备份数据库中的出票数据和中奖派奖数据进行交叉统计。数据显示，仅 2024 年 5 月至 9 月，该平台已中奖派奖总金额就超过 1.13 亿元。

用户 ID	用户账号	昵称	店铺名称	销量	跟单销量	提成	用量
1	83105	王 **	时尚优选 **	5,821,490.30	131,378.20	0.00	1,288
2	29542	李 **		98,450.00	/	/	95
3	77341	张 **		1,987,331.88	137,102.48	0.00	862
4	40169	赵 **		75,822.50	65,119.20	0.00	203

案例价值

01 / 还原犯罪网络

通过技术支持，完整复现了涉案后台，全面掌握了该非法售彩平台的真实运营情况。成功提取的 21,177 条会员数据和 20,991 条代理记录，清晰地揭示了其庞大的用户规模与金字塔式的代理层级，为全链条打击提供了精准指引。

02 / 支撑追赃挽损

深度分析了主、备数据库中横跨 9 个月的交易流水，统计出各主要店铺的下单、出票及中奖派奖金额，累计流水额达数亿元，为案件定性、量刑及后续的追赃挽损工作提供了直接的证据支持。

03 / 提升办理效率

面对多份、海量的检材数据，鉴定团队借助自动化脚本和专业的数据库分析工具，高效完成了数百万条记录的解析与统计，大幅缩短了研判周期。

04

ILLEGAL CONTENT DISSEMINATION

非法内容传播

非法内容传播是指利用网络技术和信息媒介发布或扩散色情、谣言等违反法律和社会伦理的内容，其危害已超越传统信息领域，渗透到数字社会的各个角落。在 AIGC（人工智能生成内容）和点对点传输技术（如 AirDrop）的加持下，非法内容呈现出生成门槛低、传播隐蔽性强、扩散速度快的特点。它不仅搅乱了公共秩序，还以煽动性、欺骗性为手段，试图操控社会情绪和公众认知。

1. 常见场景

谣言与虚假信息

特点：散播未经证实或故意捏造的信息，内容通常具有煽动性和传播性，例如虚假疫情数据、抢购潮谣言等，进而扰乱社会秩序，损害公共安全，甚至引发经济动荡（如囤积物资、股市异常波动）。

传播场景：社交媒体、即时通讯群组。

恶意诽谤

特点：以攻击、侮辱、损毁他人为目的，散播不实信息，或利用恶意评论、舆论操控制造网络暴力。受害者范围广，包括公众人物、企业品牌和普通网民。极端情况下，可能引发受害者心理崩溃或自残自杀。

传播场景：论坛、社交媒体。

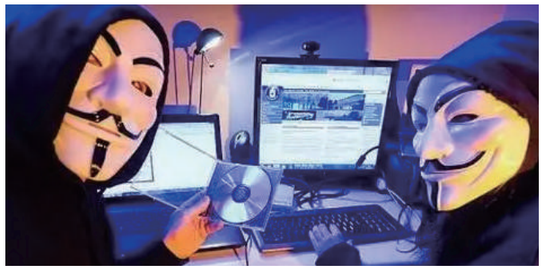
色情内容

特点：传播淫秽图片、视频，或组织线上色情直播，利用低俗内容吸引用户流量，通过会员订阅、诱导打赏或广告收入获取经济利益。

传播场景：色情网站、直播平台、私密群组。

示例：色情直播间通过社交平台广告引流，诱导用户付费观看。

暴力与恐怖主义内容



特点：传播暴力画面、武器制作教程、恐怖主义宣传材料等，煽动社会不安，助长暴力犯罪和恐怖主义行为。

传播场景：暗网、即时通讯群组。

2. 常见技术手段

生成式人工智能（Generative AI）

技术描述 Generative AI 技术基于深度学习模型生成高质量文本、图像和音视频内容，非法内容生成门槛显著降低，真实性难以鉴别。

应用 1：谣言生成

AI 生成带有煽动性或伪造的新闻报道、社交媒体帖子，增加谣言传播的可信度。

应用 2：色情内容

利用 Deepfake 技术生成逼真的虚假色情视频，常用于勒索或非法牟利。

应用 3：暴恐内容

通过 AI 生成宣传材料或武器使用教程，协助犯罪活动。

图像与视频编辑技术

技术描述： Photoshop、After Effects 等传统编辑工具与自动化 AI 编辑软件结合，形成更精细的伪造能力。

应用 1：谣言伪造

篡改图片或视频内容以制造政治丑闻或社会热点。

应用 2：色情传播

伪造公众人物的不雅图片或视频用于敲诈勒索。

点对点传输技术

技术描述： 包括蓝牙、Wi-Fi Direct（如 AirDrop）等技术，可在设备间直接传输内容，无需互联网支持，无中心化节点，传输过程难以监控或追踪。

应用 1：谣言伪造

在人群密集区域（如地铁、商场），定向发送虚假信息或煽动性内容。

应用 2：色情传播

通过点对点传输分享不雅图片或视频，避免平台审核。

加密通信

技术描述： 通过端到端加密（End-to-End Encryption, E2EE）等机制，确保只有通信双方可以解读内容，第三方（包括服务提供商和执法机构）无法拦截或监控，其高隐匿性也被不法分子利用，用于非法内容的传播和交流。

应用 1：私密群组与频道传播

创建加密的私密群组或频道，传播淫秽图片、暴力视频、恐怖主义宣传材料或虚假信息。

3. 取证鉴定思路

非法内容传播已成为网络犯罪的重要形式之一，其通过网站、APP、社交平台或点对点传输技术（如 AirDrop）发布，具有生成门槛低、传播隐蔽性强、扩散速度快的特点，对社会秩序、公众安全、企业声誉和国家法律构成严重威胁。在 AIGC（人工智能生成内容）和加密通讯技术的助推下，非法内容传播的手段和形式愈发复杂化，取证和鉴定工作需精准覆盖内容载体、传播途径及源头行为，从固定证据到还原传播链条，为司法机关提供强有力的技术支持和证据保障。

以下为非法内容传播案件的取证鉴定思路：

1 明确取证目标与重点

在正式开展取证前，应首先明确案件的核心问题与关键点：

梳理案件范围： 确认案件涉及的非法内容类型（如淫秽色情、虚假谣言），判断是否构成刑事或行政违法。

明确重点对象： 确定取证目标，如特定网站、APP、社交群组、AIGC 生成平台或 AirDrop 发送设备等。

规划取证工具和方法： 针对不同目标选择合适工具（如抓包工具、日志提取工具、盘古石云取证系统），制定具体取证策略。

2 非法内容固定

非法内容固定是整个取证链条的起点和基础，其成果将为后续链条追溯和主体溯源提供直接依据。

网页固定： 使用网页取证工具对非法内容页面进行截图、保存 HTML 源代码及关联文件，对动态内容（如评论区、弹幕、实时视频）使用录屏和屏幕截取工具进行固定。

APP 内容提取： 对涉案 APP 进行安装测试，录制界面操作过程，若 APP 提供直接下载功能，导出视频文件；无直接下载功能则使用抓包工具（如 Charles、Fiddler）获取 m3u8 链接与 TS 文件并使用 FFmpeg 合成可视视频文件。

点对点传输固定： 针对 AirDrop 等传输方式，提取发送和接收记录，包括文件路径、传输状态。

3 后台服务器追溯

解析 APP 或网站的前端与后台通信机制，确定非法内容的存储位置及后台管理系统入口。

抓包分析：使用抓包工具在模拟环境中拦截 APP 或网页的网络通信数据，捕获请求和响应包，提取数据存储路径（如视频文件的 URL 地址）和与服务器通信的 API 接口（如 GET、POST 请求的路径和参数）。

接口与文件分析：从抓包结果中提取用户上传、文件访问或管理功能的 API 端点，分析接口功能（如数据查询、上传路径），在网页代码（如 JavaScript 文件）或 APP 静态文件中查找可能包含后台管理入口的信息（如“/admin”路径或管理端点）。

服务器位置确认：根据提取的域名或 IP 地址，确认服务器的物理或云端位置，若目标使用内容分发网络（CDN），结合日志回溯工具尝试分析真实源服务器地址。

4 AirDrop 追溯取证

获取 AirDrop 传输日志及相关数据，明确非法内容的传输路径和设备间关联。

日志提取：解析 AirDrop 日志中的发送记录，确认设备名称、发送时间、传输文件类型，提取发送设备的 AirDrop ID、设备名及可能的邮箱或电话号码哈希值。

数据解析：利用哈希爆破工具对电话或邮箱哈希值进行在线解密，关联发送设备的实际使用者。

传输行为分析： 对发送方分析 AirDrop 日志中的投送文件记录及接收方记录接收日志中的设备名称、接收状态、保存路径等进行固定，还原设备间的传输链条。

5 平台及后台数据获取

通过合法授权访问涉案平台或 APP 的后台系统，提取服务器存储的核心数据（如操作日志、用户信息、内容文件），还原非法内容的生成、存储及传播过程。

服务器镜像申请：公安携服务器 IP/ 域名及对应 UID，向云服务商、CDN 或托管方调取服务器镜像文件（数据库、配置文件、日志）。

数据库分析：针对后台数据库，检索与非法内容相关的数据表，包括用户注册信息（用户名、邮箱、手机号）、内容上传记录（视频、图片或文本的文件路径）、用户行为记录（点赞、评论、转发、充值等操作日志）等。

服务器日志分析：检索服务器访问日志，重点关注用户登录、上传内容、浏览内容的操作记录，提取关键字段（如 IP 地址、时间戳、设备标识），分析日志是否包含多次操作（如批量上传）或异常行为（如使用代理 IP 登录）。

多媒体文件提取：提取存储在服务器中的非法视频、图片等多媒体文件，导出原始文件并校验 Hash 值。

6 非法获利分析

通过分析资金流向可证明非法行为的经济动机和规模，为量刑参考提供证据。

资金流向追踪：从后台数据库中提取会员充值、广告收益、付费观看等财务记录，结合支付渠道（第三方支付平台、虚拟货币转账记录）分析资金流动路径。

关联方分析：检索后台中涉及分成、代理、推广链接的数据，确认是否存在上下游产业链条，确定获利主体与扩散层级的对应关系。

7 鉴定意见书编撰

将整个取证和鉴定过程的成果整合成清晰、规范、合法的鉴定意见书，全面呈现案件事实、分析过程和证据链条。

证据分类整理：对所有取证数据进行分类整理，包括前台固定内容（如网页截图、视频文件）、后台提取数据（如用户日志、数据库记录）等，确认证据链条的完整性，确保前台与后台数据互为印证，形成闭环。

案件事实分析：根据前期取证与分析结果，对案件核心数据（如视频数量、谣言传播范围、影响人数、社会危害性）进行量化分析，提供数据支持。

4. 典型案例

邪教聚集传播案

两部手机一张卡，拼出真相全景图

在一起邪教聚集案件中，警方查获多部手机及大容量存储卡。涉案人员为了规避侦查，删除数据、隐藏传播材料，妄图切断证据链。奇安信洞鉴通过多终端取证、深度恢复与镜像解析，最终从数百份文档、图片及视频中提炼出关键证据，揭示了其背后系统化的宣传资料库，为案件侦破提供了决定性支撑。

案件背景

2024 年中旬，某地公安在工作中发现一伙人员疑似组织邪教活动，聚集频繁，涉及跨区域传播。办案人员在行动中扣押了两部手机及一张大容量 SD 卡。初步勘验显示，设备中存有被反复删除痕迹的影像与文档文件，部分还刻意混杂在日常文件夹中，情况复杂。为确保取证客观、完整，公安机关将设备交由奇安信洞鉴进行司法鉴定。

洞鉴解决方案

为确保检验过程的科学性与可复验性，奇安信洞鉴在屏蔽环境下启动涉案手机，统一设置飞行模式，接入检验工作站。在操作前完成病毒库更新与查杀，并对作业环境实施防磁、防水、防静电和防震保护，确保数据不受外部干扰或二次改写，这些措施为后续数据的提取和分析奠定了可靠基础

01 数据恢复：从残留碎片提取线索

鉴定人对两部涉案手机及一张 SD 卡进行全面提取。在手机中，虽然表层应用信息几乎清空，但深度恢复仍提取出设备 A 的 26 条缩略图（含 25 条已删除）和 16 张照片，以及设备 B 的 32 条缩略图（含 29 条已删除）和 3 张照片。这些来自缓存与媒体索引的残留，揭示了嫌疑人曾存在拍摄、浏览聚集场景的行为。与此同时，SD 卡在镜像解析后恢复出 290 个文件，其中包括 213 份文档、69 段视频和 8 张图片，内容集中反映了系统化的宣传与记录，为案件还原提供了坚实证据 。

02 加密解析——突破隐匿存储的屏障

在对检材进一步分析过程中，鉴定人发现部分视频与文档并未以明文形式存在，而是存放于加密磁盘分区。鉴定人员通过专业技术手段完成挂载与解析，成功提取出加密卷内的内容。这一环节不仅突破了嫌疑人刻意规避侦查的存储手法，还确保了潜在关键证据能够完整呈现，使案件事实得以更为全面的还原。

03 统计量化——以数据规模强化客观性

除恢复与解密外，鉴定人还对检出文件开展了量化分析。经统计，文本文件总字符数为 209,113 个；视频文件（MP4、FLV）合计时长 8,041 秒。通过对文本与音视频规模的量化呈现，证据的客观性和直观性得到提升，为后续司法定性与量刑提供了有力支撑。

```python
# 遍历文件夹及子目录，统计文件字符数并保存到表格中
def count_and_save_characters_in_folder(folder_path, output_path):
    file_data = []  # 用于保存每个文件的信息

    total_characters = 0  # 总字符数
    # 遍历文件夹
    for root, dirs, files in os.walk(folder_path):
        for file_name in files:
            file_path = os.path.join(root, file_name)
            file_characters = 0
            status = "Success"  # 默认成功

            # 只处理指定格式的文件
            if file_name.endswith('.txt'):
                file_characters = count_txt_characters(file_path)
            elif file_name.endswith('.html'):
                file_characters = count_html_characters(file_path)
            elif file_name.endswith('.docx'):
                file_characters = count_docx_characters(file_path)
                if file_characters == 0:
                    status = "Failed"
            elif file_name.endswith('.pdf'):
```

案例价值

01 / 保障证据完整链条

通过对手机与 SD 卡的深度数据恢复，提取出原本被删除或隐藏的多媒体残留和文档资料，使零散线索重新拼接成完整证据链，为案件定性提供了直接支撑。

02 / 揭示隐匿存储空间

成功解析了涉案设备中的加密磁盘分区，恢复出其中存放的重要视频与文本文件，避免重要信息缺失，确保案件事实得以全面呈现。

03 / 使证据更直观可解读

团队通过脚本等工具统计了涉案传播素材的字符文本及时长，使证据规模得以直观呈现，不仅便于侦办机关快速把握涉案资料的整体情况，也为后续比对、定性和庭审展示提供了更清晰的参照。

传播淫秽物品牟利案

深度还原数据库与后台系统，揭示代理分销与资金结算全链条证据

本案涉及一起利用境外涉黄网站，通过境内代理和支付通道牟取暴利的“传播淫秽物品牟利案”。该团伙分工明确：境外搭建网站，境内负责推广、引流、代收代付，涉案视频高达 26 万部，年流水近 15 亿元。奇安信洞鉴受托对查获的多份数据库文件及源代码进行取证分析。通过在虚拟环境中重建网站后台，逐一导出订单、代理、资金结算及片库信息,完整揭示了该平台的运营逻辑与牟利模式。鉴定结果不仅为案件定性提供了关键证据,也为后续追查资金流、厘清代理链条奠定了数据基础。同时，我们还协助办案机关开展现场取证，对网站源码、数据库文件及 Telegram 聊天记录等关键证据进行固定，进一步保障了数据链条的完整与可靠。

案件背景

2024 年 10 月，某地公安局成功破获一起大规模网络淫秽传播案，现场抓获犯罪嫌疑人 36 人，查扣冻结资金 1,551 万元，查封房产、车辆等财产总值逾 1,400 万元。经查，该犯罪团伙组织严密，实际由境外团伙掌控 。境内人员负责购买手机号、微信号发展下线代理，通过社交群组发送色情引流图片，诱导用户付费观看淫秽视频。该涉黄网站包含 26 万部淫秽视频，通过设置 9 元单次观看或 38 元包天等方式牟利。为彻底查清该网站的运作模式、锁定各层级代理的非法所得并固定电子证据，办案单位将查获的数据库压缩包委托我所进行专业解析。

洞鉴解决方案

01 犯罪平台复现：服务器环境搭建与系统还原

为实现对涉案网站功能的动态检验，鉴定人首先进行了运行环境的重建。

1. **虚拟环境搭建：** 在 VMware Workstation 软件中创建 CentOS 7 虚拟机，模拟真实的服务器硬件和操作系统环境。
2. **网站环境部署：** 利用宝塔 Linux 面板，快速部署了网站运行所需的 Web 服务器、数据库等核心组件。
3. **系统数据导入：** 将检材中的网站源代码解压至网站根目录，并将数据库备份文件导入至新建的数据库中，成功将整个后台管理系统在本所的检验环境中还原。

02 核心功能解析，直击牟利逻辑

系统还原后，鉴定人通过分析数据库表获得了后台管理员账号和密码，并成功登录了网站管理系统。随后，通过对后台功能模块的逐一审查，并结合 PHP 源代码与数据库表的对应分析，查明了其核心犯罪逻辑：

1. **订单数据分析：** “订单列表”页面的数据源为数据库中的订单表，该表详细记录了“代理 ID”、“打赏金额”、“订单号”等交易信息，鉴定人共提取了一万余条订单记录。
2. **代理体系分析：** 该平台的核心是其庞大的代理网络。鉴定人分析发现，“代理列表”数据源为用户表，展示了代理的账户信息、层级关系、账户余额、返佣比例等，鉴定人共提取了一百余条代理的详细数据。
3. **资金流向分析：** “未结算列表”功能反映了平台的内部资金流向。经分析，其数据来源于支付表，记录了待支付给各级代理的佣金金额和状态，鉴定人共提取一百余条待结算记录。
4. **片库信息：** 平台设有“公共片库”和“代理片库”，其视频文件名、分类、地址等索引信息，分别存储于视频表和代理表中。经统计，“公共片库”含 8000 余条记录，“代理片库”则包含高达数十万条记录。

03 跨服务器数据整合：还原支付通道数据库

除核心网站外，鉴定人员还检验了另外四台专用于资金结算的服务器。数据库内保存有数万条支付订单，记录了资金流水、支付渠道及收款账户，揭示该团伙接入多个非法或第三方支付平台，并利用大量账户接收和分流涉案资金，为资金追踪提供了直接线索。

这一发现表明，该团伙采取“业务—资金”分离的隐蔽模式，通过多台“资金服务器”搭建复杂结算网络，以掩盖非法收益。本次分析成功将其与主站点关联，为揭示洗钱路径和资金规模提供了关键证据。

案例价值

01 / 可视化呈现犯罪证据

通过完整重建网站后台系统，将静态的代码和数据转化为可交互的动态功能界面，直观地展示了犯罪平台的运作流程。这种“看得见、摸得着”的证据形式，比单纯的数据列表更具说服力。

02 / 精准量化犯罪规模

本次鉴定提供了精确的统计数据，如订单总量、代理总数、视频资源总量及待结算资金等。这些客观、可量化的数据，为司法机关认定犯罪事实、评估社会危害性以及依法量刑提供了坚实的基础。

03 / 揭示完整犯罪链条

通过技术分析，清晰地勾勒出从前端引流、用户支付，到后台代理管理、资金结算的完整犯罪链条，为办案单位全面了解新型网络犯罪的组织模式和技术手段，进而实施全方位侦查与打击提供了重要的技术参考。

打击“涉黄视频”网站案

流程化、规范化、自动化，针对涉黄 APP 的定性定量精准打击

近年来，某涉黄视频网站因大量淫秽内容而受到关注。奇安信为上海警方提供技术支持，对该网站的 19 个站点进行了深入调查与鉴定，通过重构服务器、分析用户数据并进行鉴定，助力警方确定了犯罪嫌疑人名单。在相关鉴定过程中，奇安信研发并应用了一套符合要求的鉴定规范和全自动化工具，有效提升了鉴定效率与准确性。

案件背景

上海警方在调查中发现了某涉黄视频网站的 19 个站点。奇安信技术团队配合其进行了全面深入的打击行动，成功提取了后台的用户信息，并对其进行了梳理分析，最终确定了涉嫌传播淫秽物品的嫌疑人账号、上传视频、点击量等重要信息，帮助警方抓获了上百名涉案人员。

在该系列案件的司法鉴定中，需要面临近百个涉黄账号的鉴定，包括数据统计、视频下载等，采用人工操作，较为繁碎、效率低下且易出现错漏。

洞鉴解决方案

在此案中，奇安信洞鉴已陆续出具 70 余份鉴定报告。从最初的手动录频到盘古石云取证系统自动下载、分析，针对涉黄 APP 的账号取证与鉴定分析，奇安信洞鉴探索出了一套规范化、自动化的鉴定流程。

1. 账号数据统计分析

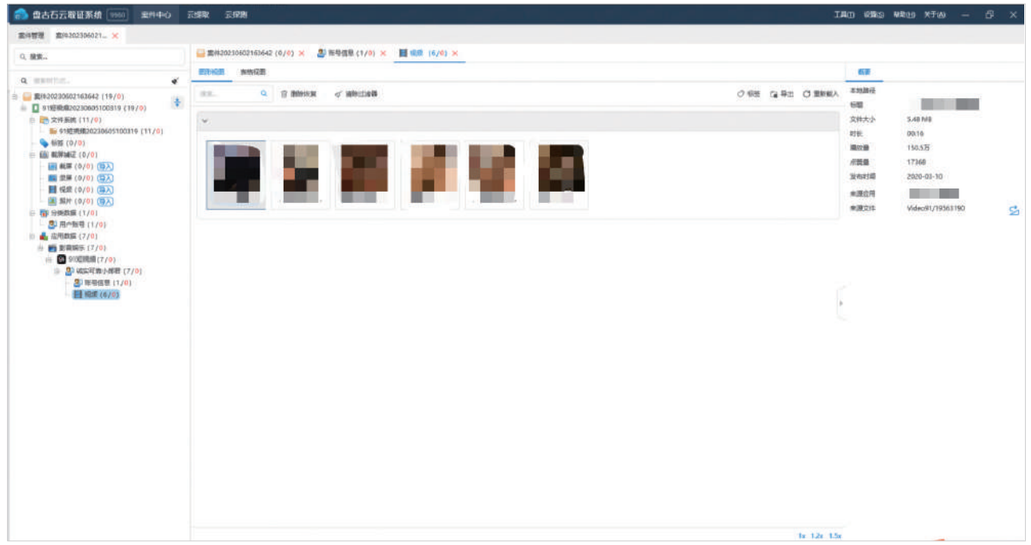
对涉案服务器后台用户数据进行分析转换，并统计，最终出具涉案账号总表，包括粉丝数、关注数、作品数、获赞数等信息。

UID	手机号	用户昵称	粉丝数	作品数	获赞数
40384	135****0365	*** 八九	19275	25	66
382974	159****0865	*** 土豆	3945	43	336
394573	139****6810	*** 美式	44564	389	5245
95743	151****6543	*** 狼	8255	43	1324

账号统计表，非真实信息

2. 涉案视频固定统计

对指定涉案账号上传的视频进行固定，并统计所有视频的有效点击量与点赞量，并出具统计分析表。这一过程历经手工录屏固定、抓取 URL 下载和盘古石云取证系统自动统计三个阶段，目前，奇安信盘古石云取证系统已上线针对相关 APP 自动提取视频、统计数据的功能。



奇安信盘古石云取证系统

3. 检查核验

为确保数据的准确性，需要对点击量、点赞量等信息进行截图，由专门的审核员对交付数据进行核验，确保数据与对应截图保持一致。

案例价值

01 / 打击精准有效

帮助公安部门在大量混杂的用户数据中迅速定位到核心犯罪嫌疑人，大大提高了案件侦破效率，对于打击网络淫秽色情内容起到了关键作用。

02 / 鉴定高效准确

为处理此类案件制定的鉴定规范和自动化工具，极大地提高了公安机关处理此类淫秽色情案件的效率，且确保了数据的准确性、完整性。

03 / 净化网络环境

通过精准打击涉案色情内容，此次合作有力地净化了网络环境，对保护未成年人免受淫秽色情内容侵害起到关键作用。

AirDrop 恶意传输案

无迹可寻？揭开 AirDrop 匿名传输的神秘面纱

某国家重大会议期间，北京市发生了恶性事件：嫌疑人在公共场合使用 iPhone 的 AirDrop 功能来传送不当言论。由于 AirDrop 的匿名性和追踪难度，通过简单地更改手机账号或名称，几乎可以清除所有犯罪线索，这种几乎零成本的恶意行为可能带来极大的社会危害。在这样的挑战面前，奇安信技术团队突破难关，成功破解了 AirDrop 溯源的难题，并有效地协助警方确定了多名涉案嫌疑人。

案件背景

AirDrop 是苹果自 iOS 7 开始在系统中新增的一个用于在多台 iOS 和 macOS 设备之间进行文件分享的功能。由于其无需连接同一局域网，且无需接收方为通讯录联系人，一些有恶意目的的人就会利用此功能传输非法图片、视频、音频等文件，如在地铁、公交、商城等人员密集场所非法向附近公众投送和传播不良信息等。

某国家重大会议期间，有群众报案称，在北京地铁内，其 iPhone 接收到了一段带有不当言论的视频。经过初步调查，警方发现嫌疑人利用了 iPhone 的 AirDrop 功能在公共场所匿名传播这些信息。由于 AirDrop 的匿名性和追踪难度，已经有部分网民开始效仿这种行为，因此，需要尽快找出发送源并确定其身份，以避免更大恶意影响。

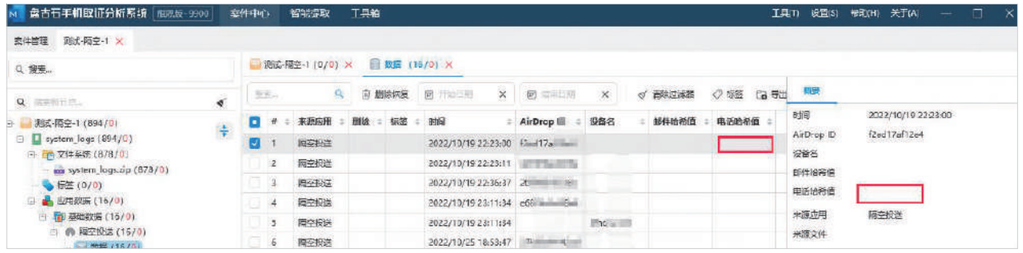
洞鉴解决方案

由于 AirDrop 不需要联网也可以进行投送，因此无法通过常规网络监测手段对该行为进行有效监管，奇安信技术团队从受害者的 iPhone 中深挖线索，层层剖析，最终成功定位了相关嫌疑人。具体过程如下：

1 明确路径原理：技术团队通过深度解析 iPhone 设备日志，找出了与 AirDrop 相关的记录。他们发现，发送者的设备名、邮箱和手机号相关字段，其中手机号与邮箱相关字段是以哈希值的形式记录，且哈希值部分字段被隐藏。为实现快速破解该字段，技术团队制作了一张详尽的手机号与邮箱帐号 " 彩虹表 "，能够将密文转换成原始文本，快速锁定发送者的手机号与邮箱账号。

2 上线溯源功能：为了应对获取 AirDrop 发送和接收记录文件的复杂性，奇安信盘古石手机取证分析系统紧急上线了新的功能，它可以自动提取接收时间、发送方设备名、发送方邮箱和手机号哈希值以及投送文件名和投送时间等信息。同时，他们也上线了一个 AirDrop 哈希值转换工具，实现了密文的一键转换。

AirDrop 哈希值转换工具



隔空投送取证溯源

3 鉴定意见出具：基于以上的操作过程和分析结果，奇安信洞鉴针对此案出具了多份具有法律效力的司法鉴定意见书。这些鉴定书详细分析了接受端和发送端的相关设备，有效地帮助警方确定了多名涉案嫌疑人。

案例价值

01 / 提升侦破效率

奇安信技术团队在短时间内实现了自动化提取记录，使得公安机关能够快速、准确地定位到涉案嫌疑人，大大提升了案件侦破的效率和准确性。

02 / 维护社会秩序

通过成功追踪和定位相关嫌疑人，帮助公安机关维护了社会秩序和公共安全，防止了不当言论的进一步传播和潜在的恶意影响，为社会稳定和安宁作出了重要贡献。

03 / 积累技术经验

本案突破了 AirDrop 匿名溯源的技术难题，为公安机关提供了有效手段来应对 AirDrop 匿名传播带来的社会不稳定因素。

05

ILLEGAL RESOURCE PROVISION
非法资源提供

非法资源提供是网络犯罪中重要的上游环节，指通过非法手段获取、加工或交易资源，为下游犯罪行为提供支撑的活动。这些资源包括非法数据、虚拟身份（如伪造 IP）、专用黑灰产工具（如黑客软件、作弊插件）以及接码平台等。这一环节的核心特征在于，其所提供的资源虽然不直接实施犯罪，但却是网络诈骗、网络赌博等犯罪行为的关键基础，起到了“催化剂”作用。

随着技术的发展，非法资源提供呈现出隐匿化、产业化和服务化的趋势，其本质是通过破坏法律秩序，为犯罪活动降低门槛、提升效率，进而形成规模化的黑灰产链条。在网络犯罪治理中，打击非法资源提供不仅是切断犯罪链条的重要手段，更是确保网络空间安全的关键环节。

1. 常见分类

数据资源

定义：指非法获取、存储、交易的数据资源，用于实施隐私侵害、欺诈等犯罪行为。

- 个人隐私数据：如姓名、身份证号码、电话、住址等，广泛用于精准诈骗和身份盗用。
- 账户与凭证数据：包括邮箱、社交媒体、支付账户及其密码，常见于盗号和金融犯罪。
- 企业与商业数据：如公司内部文件、客户名单、交易记录等，为商业间谍活动、敲诈勒索提供条件。

特点：数据资源的价值在于其可重复利用性和高隐匿性，黑灰产链条中常通过钓鱼攻击、恶意爬虫等手段获取，再通过暗网或非法交易平台分发。

技术资源

定义：用于实施网络犯罪或规避监管的技术工具和服务。

- 黑客工具：如 DDoS 攻击软件、漏洞利用工具、远程控制木马等，用于网络攻击、系统入侵。
- 作弊外挂：广泛应用于游戏、电商等场景，用于破坏公平竞争，间接引发经济损失。

特点：技术工具资源降低了犯罪技术门槛，推动犯罪活动的规模化和自动化，其传播路径常通过论坛、社区、甚至开源平台。

虚拟身份资源

定义：虚构或伪造的身份信息，为犯罪者提供“身份伪装”，帮助其隐匿操作。

- 伪造 IP 和地理位置：通过代理 IP、VPN 等手段伪造访问来源。
- 虚假身份文件：如伪造的身份证、护照，用于注册虚假企业、欺诈等。

特点：虚拟身份资源的非法提供帮助犯罪分子实现匿名化操作，同时扩大了犯罪活动的执行能力。治理需要多方协作，加强实名认证及账户行为异常监测。

中介服务资源

定义：为犯罪行为提供技术支持或交易撮合的服务，主要用于解决犯罪过程中的身份验证、资金流转、资源对接等问题。

- 接码平台：提供虚拟手机号码用于注册账号、绕过身份验证。
- 洗钱服务：通过地下钱庄、虚拟货币完成非法资金的流转。
- 非法交易平台：为非法资源和服务的供需双方提供对接、交易撮合。

特点：此类资源是黑灰产链条中重要的连接环节，其发展模式高度产业化，利用技术手段提供“定制化服务”，形成较为隐秘的供应网络。

2. 取证鉴定思路

非法资源提供类犯罪的核心在于明确涉案资源在黑灰产生态中的角色、价值，以及这些资源对下游犯罪（如网络诈骗、网络赌博）的支持程度。由于资源类型多样、技术特征各异，取证与鉴定应采取分类化、分步骤的策略，从资源本身的技术特性、传播路径和上下游关系入手，逐步构建完整、可验证的证据链条。

以下为非法资源提供类案件的取证鉴定思路：

1 明确取证目标与重点

在介入案件之初，需先识别涉案非法资源的具体类型和用途，并建立分类框架，以便于后续有针对性地选择取证工具和策略。

案件背景梳理：根据线索和侦查信息，确认非法资源类型（数据资源、技术资源、虚拟身份资源、中介服务资源），初步了解资源的应用场景与下游犯罪关联性。

取证目标规划：明确需提取的关键数据（如账号信息、通信日志、交易记录、后台配置）、拟采用的工具（抓包、逆向、数据镜像、日志分析）及验证手段（环境模拟、功能测试）。

2 分类型取证策略

根据资源类别的差异性，在取证与鉴定中应采用不同的技术手段与重点分析方向：

数据资源取证策略：对提取的数据库、数据包进行哈希校验与字段分析，判断数据完整性与真实性。必要时将其与既有泄露事件数据进行比对，确定数据来源及泄露路径。借助情报信息与历史案件线索，分析数据在黑灰产市场的流转情况，评估其对下游犯罪（如身份盗用、精准诈骗）的实际支撑作用。

技术资源取证策略：在受控环境（如沙箱、虚拟机）中运行涉案工具，记录操作流程和输出结果，验证工具的功能点与攻击方式。利用 IDA、Frida 等逆向分析工具解析程序逻辑、通信协议及漏洞利用方式，明确其对目标系统的破坏能力和技术特征，为案件定性与风险评估提供技术依据。

虚拟身份资源取证策略：利用抓包工具截获通信数据包，分析虚拟身份生成工具的代理信息，确认其伪造 IP、假账户背后的匿名化手段。在隔离测试环境中模拟使用这些资源，观察注册、访问行为异常点，并结合平台安全日志溯源使用者身份，从而判断虚拟身份资源对隐藏和规避监管的实际影响。

中介服务资源取证策略：获取接码平台、代理 IP 池或相关后台系统的访问权限后，导出日志、用户列表、号码池数据及相关交易信息。通过对记录数据的统计分析，标识资源使用的活跃节点和交易模式，关联其对下游犯罪的规模化支持。

3 后台与云端数据提取

无论何种资源类型，一旦锁定后端控制服务器或云服务平台，需深入分析后台数据以重建资源运转全貌：

服务器镜像与日志分析：备份服务器数据，提取用户注册、访问、下载记录以及资金交易信息，确认资源的供求关系。

数据关联：将后台数据与前台抓包信息、测试操作记录相对照，确认资源分发模式、上下游关系，判断资源提供者在黑灰产链条中的位置与作用。

4 资源传播路径分析

透过对资源供应链的全面分析，还原其从生产、加工、销售到最终使用的完整链条，以明确资源提供行为对下游犯罪的催化作用：

交易记录与通讯数据分析：提取支付数据、聊天记录、转账流水，定位资源销售者、代理商和最终用户的核心节点。

跨案件关联与情报共享：将本案提取的数据与已有案件资料对比，寻找相似路径、重复 IP、常见工具特征，从而发现潜在的上下游犯罪团伙。

5 鉴定意见书编撰

将取证过程、分析结果、技术验证结论有机整合成鉴定报告，以表格、图示方式清晰展示资源类型、技术特征及关联链条，为司法机关定性与量刑提供客观技术参考。

技术结论与法律建议：结合资源功能、技术手段、下游犯罪关联性，从技术层面对案件进行定性，为司法机关判断资源提供者在整个黑灰产链条中的地位、罪责轻重，以及对下游犯罪的促进作用提供专业建议。

3. 典型案例

跨境网络赌博支付平台案

多维数据穿透，锁定“赌博平台 + 支付平台”犯罪链条

本案系一起跨境网络赌博案，涉案平台“锅 * 支付”为多家境外赌博网站提供支付结算通道，涉案资金流水逾十亿美元。平台架构复杂，涵盖商户管理、代理分成、虚拟币钱包结算等多模块，涉案数据分布在多份服务器镜像、数据库备份及移动终端中。奇安信洞鉴通过多源镜像还原、虚拟化仿真、数据库深度解析及 SQL 穿透查询，完整重构了“锅 *”支付后台运行环境，提取了数十万条订单、佣金、结算及虚拟币交易记录，精准锁定了平台运营模式、资金流向及核心涉案人员账户，为公安机关全链条打击跨境赌博犯罪提供了关键技术支撑。

案件背景

2019年，犯罪嫌疑人张某某开发出一套支付系统，并将其出售给境外犯罪团伙。该团伙以此为基础搭建了名为“锅*支付”的非法支付平台，专门为“乐*”网络赌博平台提供资金结算服务。

经查，该支付系统由张某搭建并出售给境外人员，用于为赌博平台提供充值、提现及代理分成等功能，支持TRC20、ERC20等虚拟币结算，并通过多级代理体系分润。涉案资金体量巨大、交易频率高，账户体系、资金流、钱包交易均呈高度分散与隐匿特征，案件侦办需对多份复杂检材进行全面解析与还原。

洞鉴解决方案

01 涉案支付平台后台还原

利用计算机仿真取证系统，成功加载了涉案服务器的镜像文件，并搭建了与原始环境高度一致的仿真系统。通过修改网络配置、数据库连接信息，并绕过后台登录的密码与谷歌二次验证机制，最终成功登录“锅 * 支付”的后台管理系统，为后续数据分析打开了通路。

02 数据库恢复与穿透分析

鉴定专家成功恢复了 7 份不同时期的数据库备份文件，通过编写 SQL 脚本批量解析订单、佣金、结算及钱包交易记录，累计提取成功订单超 70 万条、流水记录超 218 万条、虚拟币交易记录超 70 万条以及佣金记录超 65 万条。同时，通过对代付订单表的去重分析，精准提取了参与资金结算的商户开户名共计 6,511 个。

03 赌博与支付平台关联性分析

通过多维技术手段，全面锁定“乐 *”赌博平台与“锅 * 支付”间的一体化犯罪关系：

1. 将涉案赌客提供的交易账单（流水明细 .xlsx）与“锅 * 支付”后台结算任务表进行比对，成功匹配 15 条完全一致的交易记录，直接证实两平台之间存在资金往来。
2. 在“锅 * 支付”源码中定位到记录订单请求来源网址的关键代码，并在数据库字段中发现大量来自“乐 *”赌博网站的 URL，从代码层面无可辩驳地确认“锅 * 支付”是“乐 *”赌博平台的结算工具。

案例价值

01 / 锁定跨平台一体化运作证据

通过账单比对与源码溯源方法，直接证明“乐 *”赌博平台与“锅 * 支付”属于同一团伙运营，实现多维度的相互印证。

02 / 还原资金规模与流向

深度分析并提取了横跨数月的海量交易流水，累计入金流水超 7.85 亿元，并精准画像出 6500 余个结算商户，为案件的定性、量刑以及后续的追赃挽损工作提供了最直接、最有力的证据。

03 / 大幅提升侦办效率

依托自动化仿真环境和批量 SQL 解析技术，在不破坏原始数据完整性的前提下，高效实现海量数据解析和结构化入库，显著缩短了资金流向研判和关联人员识别的周期，为警方后续集中收网和跨境追逃提供了时间优势。

制贩黑客工具“刷机”案

数字犯罪解析：揭秘黑客刷机软件如何“绕过”手机密码

2023 年，上海市首例制贩黑客工具非法破解手机信息系统案成功破获。本案中，涉案团伙研发了一键强制“刷机”的工具，该工具能够绕过常规的密码解锁步骤，直接恢复手机出厂设置。自 2018 年起，该涉案团伙通过在线销售这款软件，非法获利已达千万元。奇安信洞鉴应邀对该软件进行了专业鉴定，鉴定人通过一系列技术手段，对软件和手机通信的数据包进行了深入分析，深入了解并剖析了该程序的运行原理，最终确认其具有破坏性功能。

案件背景

近年来，智能手机被盗后遭到解锁和转售的案件时有发生。为隐藏踪迹，这些被盗手机通常会被还原到出厂设置后再转售。而设置了指纹或复杂密码的手机，无法通过正常步骤解锁，给转售带来了难题。一些黑客就研发了可以强制绕过密码校验直接恢复出厂设置的黑客工具来牟利。上海某团伙长期利用这种工具进行非法获利。如何解析这种工具的工作机制，成为本案的核心技术挑战。

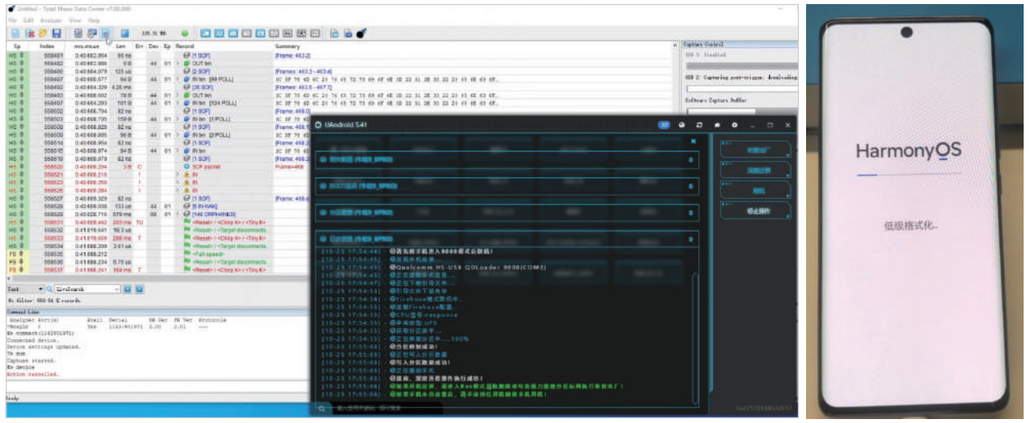
洞鉴解决方案

1. 获取验证服务器地址

在检验计算机上安装和运行该软件，并通过专业 USB 抓包设备和软件进行数据捕获，抓取程序在联网时的 UDP 请求包，并分析数据内容，解析出程序尝试连接的授权验证服务器地址。

2. 测试软件刷机功能

为检验程序功能，鉴定人准备了一台测试手机，按照典型用户模式设置了锁屏密码与帐户绑定，并开启“查找手机”功能；同时，使用串口编程线将测试机置入编程状态，与检验机 USB 抓包设备相连接，运行刷机程序，发现测试机均可跳过锁屏和帐户验证而直接进入初始化流程。在此过程中，使用抓包工具捕获机器交互的通信数据包。



3. 解析通信数据包

进一步解析数据包中的应用层协议，提取与存储操作相关的命令码和参数，推断出其读写手机存储分区的具体操作行为。通过对照软件读写前后存储数据的变化，揭示了清除帐户锁和恢复出厂设置的操作原理和过程，即通过读取和修改手机存储分区的数据来实现清除帐户锁和恢复出厂设置的功能。

通过上述步骤，鉴定人对软件与手机通信的数据包进行了深入分析，解析了它是如何通过读取和修改手机存储分区的数据实现恢复出厂设置的功能，并最终确认了这款软件为破坏性程序。

案例价值

01 / 协助警方侦查

本案破解软件使用了读取系统数据、修改关键分区等复杂技术手段，通过深入解析这些机制，可以帮助公安机关全面理解案件的技术详情，对破解程序开发者和销售团伙的犯罪行为侦查取证。

02 / 发现安全漏洞

该软件直接破坏了智能手机的系统安全防护机制，解析其技术原理可以帮助手机厂商发现系统漏洞并加以修补，提升系统安全性，保护广大消费者的财产安全和隐私。

03 / 提供坚实证据

通过深入分析通信数据包，成功确认该软件为破坏性程序，这一电子数据鉴定结果为公安部门提供了重要的技术支持，为后续的法律程序提供了坚实的证据。

路由器木马案

家庭路由器也能中木马？揭露大规模路由器控制黑产链条

2022 年，奇安信洞鉴参与侦破一起涉及全国范围内数万台家庭路由器被非法控制的案件。犯罪团伙通过植入木马程序，远程操控家庭路由器，将其 IP 地址通过代理服务出租给网络游戏玩家和虚假广告发布者牟取非法利益。奇安信洞鉴通过详细的木马程序提取、代码分析、服务器日志分析等手段，成功揭露了该团伙的犯罪手法和作案规模，为警方破案提供了关键证据和技术支持。

案件背景

某地公安局在一次网络巡查中，发现一个名为“**IP”的网站提供大量家庭路由器的 IP 地址租赁服务，这些 IP 地址被用于网络游戏加速和发布虚假广告等行为。经过调查，警方发现该网站背后存在一个规模庞大的犯罪团伙，他们通过植入远程控制木马程序，非法控制了全国范围内数万台家庭路由器。

这些路由器的所有者多为普通家庭用户，他们并不知情自己的网络设备已经被黑客利用。木马程序通过篡改路由器设置，实现了开机自动连接远程服务器的功能，并将路由器的 IP 地址上传至犯罪团伙的服务器。随后，这些 IP 地址被以每小时计费的方式出租给有需求的网络用户。

这种大规模的非法控制行为不仅侵犯了用户的隐私权，还对公共网络安全构成了严重威胁。警方随即委托奇安信洞鉴对涉案设备和服务器展开详细的司法鉴定工作。

洞鉴解决方案

1. 木马程序提取与分析

鉴定人员首先通过专业工具与涉案路由器建立连接，通过命令行方式提取了路由器中的关键文件。在提取过程中，发现了两个启动脚本，这些脚本会在路由器开机时自动执行木马程序。 随后，鉴定人员对木马程序进行了静态分析。通过反编译工具确认，木马程序具备远程控制功能，能够通过加密通信与远程服务器连接，接收指令并执行操作；另一个程序则负责代理功能，能够通过远程服务器获取路由器的 IP 地址，并租赁给第三方客户。

2. 服务器日志分析

在功能性分析完成后，奇安信洞鉴团队对涉案服务器进行了进一步分析。鉴定人员通过使用 SSH 工具登录服务器，并分析了服务器中的日志文件。通过对 acceptlog 日志的统计，鉴定人员确认该服务器接收到了来自 15910 台不同路由器的请求，这表明木马程序成功控制了这些路由器。分析结果揭示了木马程序的广泛传播和控制规模，为案件定性提供了有力依据。

3. 木马程序复现与验证

为验证木马程序的实际效果，鉴定团队在隔离环境中模拟了木马程序的运行。将木马程序复制到模拟环境中，并配置与服务器相同的网络环境，成功复现了木马程序的启动、与服务器连接以及接收指令的全过程，进一步确认了其远程控制功能。

客户价值

01 / 提升案件侦破效率

通过快速提取和分析木马程序，奇安信洞鉴大幅缩短了案件侦查时间，为警方提供了清晰的作案流程和技术手段。

02 / 揭露黑产链条

详细的木马分析和日志统计揭示了犯罪团伙通过非法控制家庭路由器出租 IP 地址的完整黑产链条，为打击此类犯罪提供了技术支持和经验借鉴。

03 / 保护公众网络安全

案件的成功侦破，有效遏制了犯罪团伙对家庭路由器的非法控制，保护了公众的隐私和网络安全，为社会稳定作出了积极贡献。

云南“猫池”案

取证鉴定一条龙，协助警方侦破全国最大“接码平台”

2021 年，全国最大黑灰产类在线接码平台案件爆发。在此案中，奇安信技术团队凭借专业的案情研判、情报分析、线索溯源能力，助力警方梳理接码平台运营情况及犯罪团伙架构图；同时，对上百台“猫池”设备、涉案计算机及海量数据、聊天信息进行了科学严谨的司法鉴定分析，为案件的成功侦破与依法处理提供了有力支持。

案件背景

图右的这个设备叫做猫池（GOIP），通过配套软件可以实现同时接收、发送短信，拨打电话的功能，被广泛应用于需要向多用户提供电话拨号联网服务的单位，比如邮电局、税务局、海关、银行等。现在，这种设备也被黑灰产用作大规模网络欺诈和电信诈骗的工具。

猫池（GOIP）

2021 年，云南边境的一个小县城，连续数起群众举报引起了警方的高度注意：某个通信营业厅在办理电话卡的过程中存在不规范操作，有的工作人员借用消费者的身份证信息，额外办理了电话卡；有的工作人员以每张卡 20 元的价格有偿回收弃用手机卡。

经过警方数月缜密侦查，发现一个藏有上百台“猫池”设备的犯罪窝点，但后续的侦查工作遇到瓶颈：

1. **犯罪技术“新”：**“猫池”属于新型新型网络犯罪技术，其复杂的技术特性给侦查工作带来一定挑战；
2. **犯罪团伙狡猾：**涉案团伙具备极强的反侦查能力，采用了虚拟币交易、频繁更换境外聊天软件等手段来躲避侦查。

洞鉴解决方案

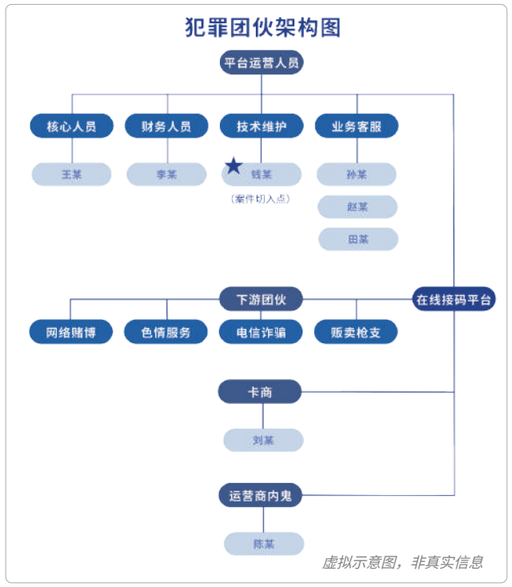
01 案中：固定上百台“猫池”证据，揭秘背后控制团队

犯罪窝点淹没在大量设备之中，环境混乱、硬件破旧、软件做了“反侦查”处理。面对此情况，奇安信技术团队迅速展开行动：

1. **证据固定：**对上百台“猫池”、计算机、手机、网站、监控等设备进行了现场固定和取证分析工作，为后续司法鉴定和起诉提供了坚实的电子数据支持。

2. **线索挖掘：**基于现勘数据进一步拓展线索，通过网络流分析、大数据挖掘、资金分析（包括虚拟币、银行卡、第三方支付数据）、境外聊天软件密码绕过等专业技术手段，摸清了接码平台运营情况及组织架构。

在此过程中，发现店主仅为犯罪团伙中的一个小角色，负责猫池的技术维护与运营，其背后控制者另有其人。经过警方与奇安信技术团队的日夜奋战，通过电子数据证据、口供、资金流，确定人员活动范围，掌握团队组织架构后，正式展开收网行动。



虚拟示意图，非真实信息

02 案后：海量涉案数据取证分析，出具客观公正鉴定意见书

奇安信鉴定人针对上百台涉案“猫池”设备，及嫌疑人手机等检材进行了取证分析工作。其中，对于“猫池”这种新型网络设备的数据提取具备一定难点，以下是具体过程：

1. **确定 IP 地址：**对猫池客户端进行数据捕获（抓包）操作，成功确定了猫池客户端的后台服务器域名和 IP 地址。
2. **数据固定：**对接码平台后台数据进行了固定，以便进一步的分析。
3. **数据导出：**通过观察扣押主机与猫池设备，在主机内找到了与猫池对接的客户端，经判断，与猫池设备相连即可读取猫池内数据；而后，通过主机内的客户端，将猫池内的手机号等相关数据成功导出。

经过上述步骤，鉴定人成功提取了设备中手机号码、ICCID 及对应号码发送的短信记录，并进行了汇总统计，最终提取到 ICCID 接近 4000 条、短信内容超过 80 万条。

合作成果

01 / 提升侦查效率

借助电子数据的有效利用与深度挖掘，公安机关在追踪和捕获嫌疑人方面实现了更高的速度与精度，特别是在涉及新型技术或设备的案件中。

02 / 创新侦查方式

通过深度解析接码平台的运营模式和犯罪团伙的组织结构，揭示了犯罪分子利用“猫池”进行犯罪活动的新手法，为公安机关在未来的侦查工作中提供了新的视角和思路。

03 / 保护公众安全

在本案中，我们协助公安机关成功地摧毁了全国最大的在线接码平台，从而避免了更多潜在的网络诈骗，为保护公众安全贡献了力量。

CHAPTER 2

市场秩序破坏治理

近年来，随着数字经济的深度发展，维护市场秩序的复杂性与紧迫性日益凸显。违法行为的技术化、专业化趋势显著，市场秩序面临的威胁愈加多元化。以设备作弊、票据及证件伪造、黄牛抢购、金融犯罪和走私为代表的违法行为，已成为干扰社会公平与经济安全的重要隐患。

税务犯罪作为直接冲击经济核心的违法行为，其危害尤为巨大。不法分子利用空壳公司、虚假贸易等手段，大肆虚开增值税发票、骗取国家出口退税，形成分工明确的黑色产业链，不仅侵蚀国家税基，更严重破坏了金融管理秩序和营商环境。

与此同时，传统领域的违法手段也在不断“升级”。设备作弊依旧是部分行业中隐蔽的顽疾，通过篡改加油机、计量器等设备的核心程序非法牟利，持续侵害消费者权益与国家税收。票据及证件伪造则呈现出更强的网络化特征，逐步形成分工细密的犯罪网络，严重威胁社会信用体系。与此同时，黄牛抢购行为借助程序化、自动化手段，大规模囤积稀缺资源并高价倒卖，显著抬高了公众获取商品与服务的成本，在医疗、烟草、交通、文娱等领域尤为突出，成为社会高度关注的热点问题。此外，走私人类遗传资源等新型违法行为，更触及国家公共安全与生物安全的红线，社会危害性尤为严重。

面对这些与数字技术深度捆绑、证据散落在多台设备中的新型复杂犯罪，传统的治理手段面临巨大挑战。电子数据司法鉴定作为穿透数字迷雾的利剑，正在社会治理中发挥日益核心的作用。从对作弊软件的源码级剖析，到跨设备、跨平台的证据链还原，奇安信洞鉴为执法机关提供了强有力的技术支撑，精准打击犯罪，助力恢复市场秩序。

本章聚焦设备作弊、票据及证件伪造、黄牛抢购、税务犯罪与走私等典型场景，深入剖析其新型作案手法与技术伎俩，并结合真实案例展示电子数据司鉴在其中的关键价值。希望通过这些内容，为社会各界在打击经济犯罪、维护市场秩序的实践中提供科学参考，共同助力构建更加公平、有序的数字经济环境。

01

EQUIPMENT CHEATING
设备作弊

设备作弊是指通过技术手段或人为干预，篡改设备的正常运行逻辑或功能，以非法牟利、规避监管或获取不正当竞争优势的行为。与传统违法手段相比，设备作弊具有更强的隐蔽性和技术性，往往借助高科技手段实施。例如，篡改加油机计量芯片以虚减输油量，修改电子秤程序以虚增商品重量，甚至通过远程控制实现实时操控。这类行为直接侵害消费者权益，扰乱市场秩序，同时造成监管盲区，使传统执法手段难以有效应对。

设备作弊广泛存在于多个行业，包括加油站计量作弊、集贸市场电子秤作弊、自动售货机商品数量篡改，以及博彩机、娱乐设备中的作弊行为。这些行为不仅挑战市场公平竞争原则，更对社会诚信体系构成严重威胁。其隐蔽性与多样性使之成为市场秩序治理中的突出难题，亟需多方合力，从技术、法规及行业规范等层面展开系统治理。

1. 常见场景

加油机作弊

加油机作弊的核心在于篡改设备的计量与数据上报系统，以非法牟利或逃避税收。加油机与油站管理系统、监管平台通过虚拟串口和数据通讯盒相连，实现数据的上传与同步。而作弊手法往往利用虚拟串口技术、主板程序篡改或遥控装置干预，使油枪实际充装数据与监管数据不符。

作弊手法与技术原理

1.篡改主板程序

加油机的主板是控制设备运行的核心，其程序中包含加油量的计量逻辑。不法分子通过植入作弊模块，篡改主板程序，将实际加油量乘以预设系数。

技术原理

篡改主板程序通常需要破解主板的安全保护机制，通过物理接触或远程加载修改代码，改变计量结果的计算公式。例如，在作弊模块中设置一个倍率系数，使实际加油量按照“真实量 × 系数”的方式输出，从而虚增或减少数据。

2.遥控作弊

利用红外遥控装置对加油机实施实时控制。操作人员通过遥控器发出信号，直接调整油枪输出量与显示量之间的差异。

技术原理

遥控作弊通过在油枪主板中集成红外信号接收模块实现。当接收到特定频率的红外信号后，油枪会根据指令调整显示量，隐藏实际加油量。

3.数据上传作弊

加油机的充装数据通过内置的通讯模块上传至监管平台。不法分子通过修改油站管理系统逻辑，阻止部分数据上传或伪造上传数据，使监管记录与实际加油量不符。

技术原理

这种作弊手法依赖对管理系统的深度操作，通过操控系统中的数据传输逻辑，实现数据的丢失或伪造。例如，系统在发送数据前，先通过隐蔽逻辑筛选并剔除部分记录，导致监管平台接收到的总加油量低于实际销售量。

电子秤作弊

电子秤作弊利用软硬件篡改或附加装置干预秤重数据，广泛存在于零售市场和集贸场所。不法商贩通过设置底数、远程控制或修改计量参数，在商品重量和价格上动手脚，从而实现非法获利。

作弊手法与技术原理

1.存底数法

在电子秤的重量显示部分预先设置一个隐藏的底数，使每次称重时都自动叠加该底数，从而虚增商品重量。

技术原理

通过修改电子秤的固件程序，在重量计算逻辑中加入一个固定值。例如，在空秤状态下，显示的重量并非零，而是一个预先设定的底数（如 0.2 千克）。这种作弊方式通常通过对电子秤的参数配置界面或固件代码进行直接调整来实现。

2.遥控作弊

在电子秤内安装红外或无线信号接收装置，操作人员使用遥控器调整重量显示数值，欺瞒消费者。

技术原理

遥控作弊利用外部信号干扰电子秤内部的重量显示模块，通过无线信号覆盖真实计量数据，使秤重数据显示人为设定的虚假值。

3.参数修改

通过设置密码激活隐藏程序，修改电子秤的计量参数，调整重量输出与实际测量值的比例。

技术原理

这种方式通常需要对电子秤的固件程序进行预先编写或植入作弊代码。例如，在设备参数中设置多个比例值，当输入特定指令时，设备自动切换至作弊模式，输出被放大或缩小的计量值。

娱乐博彩设备作弊

娱乐博彩设备作弊通过篡改程序或使用隐性工具操控游戏结果，破坏娱乐或博彩活动的公平性。作弊行为多针对游戏设备、牌桌设备等，实施者通常通过技术手段操控游戏流程或获取对手信息。

作弊手法与技术原理

1.程序篡改

在博彩或娱乐设备中直接修改程序逻辑，使游戏结果偏向特定方向。

技术原理

博彩设备的核心逻辑由程序控制。不法分子通过破解固件代码，在逻辑条件中加入人为设定的规则。例如，在老虎机中，作弊代码会设定某种符号组合的概率远低于正常值，增加设备盈利，削减玩家中奖机会。

2.隐形摄像头

在牌桌或设备中安装微型摄像头，实时窃取对手的牌面或操作信息，为作弊者提供关键数据。

技术原理

隐形摄像头利用无线信号将捕获的图像或视频传输至远程接收设备。现代微型摄像头小巧隐蔽，可安装于牌桌边缘、筹码架或其他不起眼的地方，通过低功耗无线模块实现实时传输。

3.隐形通信设备

利用无线耳机或微型通信装置，与外部同伙实时传递数据干预游戏结果。

技术原理

隐形通信设备基于超小型无线通信模块，通常集成于耳机、纽扣等日常物品中。作弊者通过外部数据分析软件实时处理游戏数据，并将关键决策信息通过通信设备反馈给场内人员。

电子灌装秤作弊

电子灌装秤作弊是针对液化气充装设备实施的非法操作，破坏了气瓶充装流程的公平性与透明度，从而规避监管或牟取非法利益。

作弊手法与技术原理

1. “应急模式”作弊

通过扫描特定二维码或输入隐藏指令，触发设备的“应急模式”，绕过正常充装流程的条码校验和复检程序，直接完成充装。

断网充装并绕过检查

在“应急模式”下，操作人员可在断网状态下对气瓶进行充装。此操作将绕过电子灌装秤常规的充前检查和充后检查环节，并且系统不会记录所充装气瓶的条码。

数据隔离与选择性上报

本地管理系统被设置为仅上报正常数据至监管平台。上述在“应急模式”下产生的无条码气瓶充装记录，将在上传时被本地系统自动剔除，从而逃避监管。

2. 取证鉴定思路

加油机、电子秤、麻将机等设备的作弊行为屡见不鲜，严重破坏市场秩序，侵害消费者权益。通常涉及软硬件篡改、遥控装置操控以及通信数据篡改等手法，其取证与鉴定需要在合法、合规的框架内，结合严谨的科学方法与先进的技术手段，全面分析作弊行为的特征与影响，为执法机关提供可靠的证据支持。

以下为设备作弊案件的通用取证鉴定思路：

1 作弊线索排查

通过初步筛查，发现可能存在作弊行为的设备和相关线索。

设备状态检查：检查设备外观是否有改动痕迹，如加油枪、电子秤的硬件接口是否异常、是否安装额外装置，确认设备是否具备必要的认证标志（如电子秤的“强制检定合格”标签，加油机是否符合国家计量检定标准）。

功能测试：使用标准计量工具对设备功能进行初步验证，例如：

- 加油机：使用标准计量器具测试充装量与显示数据是否一致；
- 电子秤：测试称重准确性，并核实是否存在“虚增重量”现象；
- 麻将机：测试洗牌与发牌过程的随机性是否存在异常。

运行日志核查：调取设备的运行日志，检查是否存在非正常操作记录，如远程修改、系统异常重启或通信中断。

2 案件设备取证

确保关键设备和辅助材料的完整提取，为后续分析和实验提供基础。

扣押关键设备：确保获取案件涉及的核心设备，如加油机油枪主板、麻将机主板或电子秤设备，若设备不可拆卸，优先对主机和配套硬件（如油枪数据通讯盒、麻将机洗牌系统、电子秤传感器模块）进行完整扣押。

数据存储介质提取：提取设备管理系统、通讯模块和后台数据库，确保操作日志、用户数据、交易记录等信息完整。

相关环境保全：如油站网络、电子秤连接台或麻将馆操作台，需完整记录环境配置并提取相关配置文件。

3 程序逆向与硬件分析

通过软硬件分析揭示设备内部的作弊逻辑：

程序逆向分析：对设备的主板程序或管理软件进行逆向工程，查找可能的隐藏功能、作弊参数或逻辑漏洞。例如：

- 加油机程序：分析是否存在虚增充装数据的代码；
- 电子秤固件：检查是否嵌入了重量偏移程序；
- 麻将机软件：验证是否设置了固定牌型概率。

硬件结构分析：对设备硬件进行拆解，检查是否安装外挂芯片、遥控接收模块或其他非法改装部件。利用逻辑分析仪检测硬件信号流，确认设备运行状态是否被人为干预。

4 功能复现实验

实验验证是还原作弊行为的关键环节：

实验环境搭建：将设备接入原始或模拟生产环境，恢复其正常运行状态；若原始环境不可恢复，建立一致性功能测试环境，确保实验条件与设备实际运行逻辑匹配。

实验设计：模拟可能的作弊行为，测试设备在不同条件下的运行状态。例如：输入特定指令、调用隐藏参数；使用遥控装置远程控制设备；在实验中模拟正常和异常操作场景等。

实验数据记录：实时抓取实验过程中产生的通信数据和操作日志，记录每一步实验操作及对应结果， 对实验过程中观测到的作弊行为进行详细描述，包括触发条件、执行效果和异常表现。

5 数据分析

数据分析在设备作弊取证中是关键环节，旨在通过对实验数据、设备本地记录和监管数据的比对与解析，揭示作弊特征，并量化其经济影响。以下为数据分析的核心步骤：

数据提取：通过专业取证工具，从设备中提取操作日志、交易记录、系统配置参数等数据，并结合实验生成的新增记录，确保数据的完整性和逻辑一致性。若发现数据有删除或覆盖痕迹，应及时进行数据恢复。

数据对比与异常筛选：将提取数据与监管平台上报数据进行详细对比，以揭示设备运行中的异常情况：与委托方沟通，从相关监管部门调取油站上报的数据，与实验过程中产生的数据进行对比，比较其中差异；根据现场实验新增（作弊）数据的特征，筛选本地和调证数据中符合特征的数据，区分正常数据与异常数据后分别进行统计和计算。

数据统计与损失计算：在筛选出异常数据后，进一步通过统计分析揭示异常数据的特征分布、行为规律和经济损失。例如，可以计算异常记录的发生频率和累计金额，评估作弊行为的范围和严重性。

6 鉴定意见形成

综合实验与数据分析的结果，形成科学严谨的鉴定意见书：

事实描述：详细列明设备作弊行为的手段、范围和影响，包括作弊逻辑、异常数据分布及实验验证结果。

量化分析：明确作弊行为的经济损失，如偷逃税款、非法获利金额等，为案件量刑提供数据支持。

技术分析：通过程序和硬件分析结果，揭示作弊行为的技术原理及实现方式。

3. 典型案例

麻将机作弊案

高科技破解赌博骗局：揭秘智能麻将机作弊案

2024 年年初，陕西省某地成功破获一起售卖作弊麻将机的犯罪团伙案。嫌疑人不仅出售带有作弊功能的麻将机，还现场演示如何使用这些设备进行作弊，最终对参赌人员实施了诈骗。奇安信洞鉴受委托对案件中涉及的麻将机进行了功能性鉴定，成功揭示了作弊手段并提供了关键证据。

案件背景

拥有“透视眼”，在麻将桌上看清所有牌面，十赌十赢……这些曾经只在港台电影中出现的“出老千”手段，如今随着科技的发展，也悄然出现在现实生活中。2023年，某地公安分局接到举报称，有人出售带有作弊功能的麻将机，并在店内示范如何使用这些麻将机进行作弊。经过警方调查，发现犯罪嫌疑人利用这些作弊麻将机实施诈骗，非法获利超过6万元。为了深入了解麻将机的作弊手段，公安机关委托奇安信洞鉴对涉案麻将机及手机中涉及的作弊应用程序进行电子数据鉴定。

洞鉴解决方案

1. 界面分析

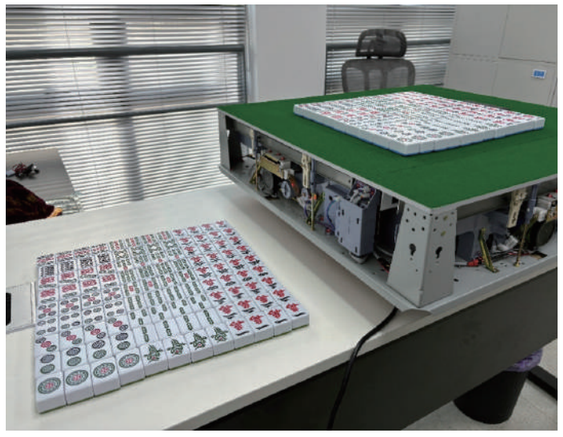
首先，在模拟器中成功运行了该作弊程序，鉴定人对其基本界面和功能选项进行了检查。应用程序包含了启动游戏、设置玩法、调整玩家数量等与麻将机交互的功能按钮。

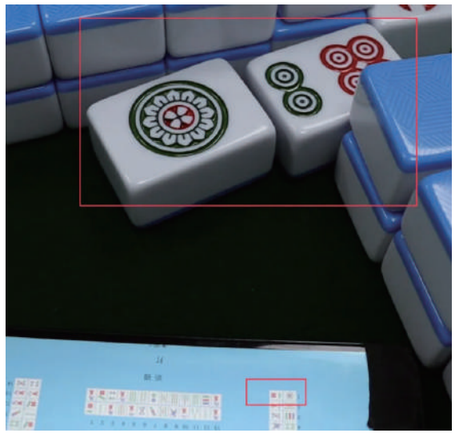
2. 看牌功能复现

紧接着，打开手机的蓝牙功能，通过应用程序的设置界面选择对应的麻将机设备。连接成功后，应用程序显示了一系列麻将牌的排序和花色信息，这些信息与麻将机中实际牌面的排列完全一致，使得作弊者能够在游戏过程中清楚地了解对手的牌局。

3.ID 读取功能复现

鉴定人还通过应用程序验证了麻将牌的 ID 读取功能。应用程序能够通过扫描麻将牌上的微型芯片，识别每张牌的唯一 ID 号，使作弊者在配牌时能精确控制每张牌的分配。





案例价值

01 / 揭示作弊机制

通过对涉案麻将机和作弊应用程序的详细电子数据鉴定，成功揭示了作弊手段的运作机制，为公安机关提供了关键性的技术支持，使其能够深入了解犯罪手段，从而有效打击违法行为。

02 / 全面证据支持

通过数据提取和分析，为司法机关提供了准确、可靠的证据，帮助确认犯罪事实和责任。鉴定意见确保了案件审理过程中证据的可靠性和真实性，提升了法律诉讼的成功率。

03 / 促进社会公平

此次成功的鉴定不仅有效打击了犯罪行为，还提高了社会公众对科技作弊手段的认识和警惕，进一步促进了社会的公平正义。

加油机作弊案

偷油、逃税频发，司法鉴定全面揭露加油站“作弊”内幕

在 2023 年 8 月开启的涉及全国的加油机作弊综合治理行动中，奇安信洞鉴协助各地警方，深入参与北京、开封、项城、商丘、永城、夏邑、郑州、大庆等多个地区的案件调查和鉴定工作，为执法机关提供了全面的技术支持，涵盖了从线索挖掘、功能性鉴定、再到数据分析以确认涉案金额的全链条服务。

案件背景

自2023年8月以来，市场监管总局会同公安部、商务部、国家税务总局等部门在全国开展综合治理加油机作弊专项行动，全面开展集中排查整治，严厉打击加油机计量作弊、偷逃税等违法行为，切实维护成品油零售市场秩序。专项行动开展以来，全国共查办加油机作弊案件1249件，涉案金额20.02亿元，罚没金额6.97亿元。

加油机作弊行为，一般出于偷油、逃税的目的，涉及对加油机硬件、软件以及计费系统的篡改，目的是使加油机显示的加油量超过实际加给顾客的油量，或让部分销售收入在账面上消失，从而非法获利、规避税费。

这些作弊行为技术含量高、形式多样且隐蔽性强，给市场监管和执法带来了巨大挑战。

洞鉴解决方案

面对这些挑战，奇安信洞鉴凭借专业能力，积极协助警方打击加油机作弊行为。

1. 作弊线索挖掘

通过远程和现场的技术支持，帮助警方识别和排查了一系列异常的外挂或作弊程序，其中包括能够定期删除订单记录和实现远程通信的软件。

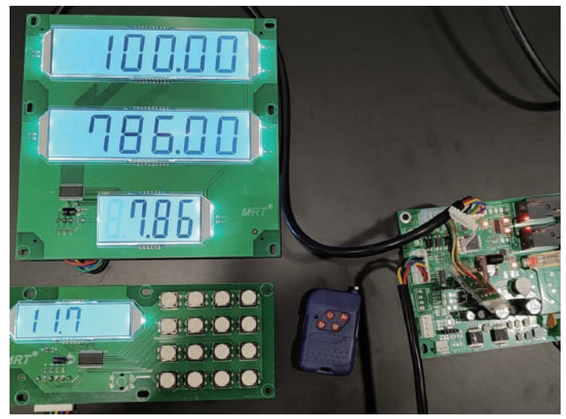
2. “漏税”功能性鉴定

通过反编译和网络数据流分析，鉴定人验证了这些软件的作弊功能。这些功能包括接收和发送修改后的数据，以及执行数据库操作，表明存在有意删除交易记录的作弊意图。

3. “偷油”功能性鉴定

程序分析：通过对汇编代码的细致分析，鉴定人发现了能够动态改变加油系数的特定代码段，这直接影响了显示的加油量。这些程序被设计为能响应外部输入（如遥控器信号），进而操纵加油机的显示结果。

动态复现：在模拟环境中，鉴定专家重现了加油过程，并详细观察、记录了加油机的响应情况。测试结果表明，加油机的显示量确实可以通过修改内部设置来操纵。



4. 涉案金额统计

通过恢复和导出涉案电脑中的加油明细表和班报数据，并进行对比分析，鉴定人精确统计了涉案的偷油量，为案件的定性和量刑提供了关键证据。

案例价值

01 / 提高执法效率

针对加油机作弊行为的高技术含量和隐蔽性，奇安信洞鉴通过专业技术手段，帮助执法机关快速识别、排查加油机作弊行为，显著提高了案件侦破效率。

02 / 提供关键证据

通过对涉案数据的精确恢复和分析，奇安信洞鉴可协助确认涉案油量差与涉税金额，为案件的定性和量刑提供了关键证据，确保了执法的公正和严谨。

03 / 维护市场秩序

通过协助查办加油机作弊案件，奇安信洞鉴为维护成品油零售市场秩序，打击偷逃税等违法行为，做出了重要贡献。

电子灌装秤作弊案

应急模式还是“作弊模式”？揭秘燃气公司大规模违规充装

2024 年，某燃气企业利用技术手段实施“作弊”，规避智慧气瓶安全追溯管理平台的监管，非法为未备案、超期未检或报废的气瓶充装液化气。奇安信洞鉴通过数据提取、校验、分析及功能验证实验，全面还原了该企业的违规操作流程和数据管理问题，为案件侦办提供了关键性技术证据。

案件背景

2024年，某地公安局接到举报，称当地两家燃气公司涉嫌利用技术手段“作弊”，规避智慧气瓶安全追溯管理平台的监管，非法充装不合规气瓶。经过初步调查发现，这些企业通过启用电子灌装秤的“应急模式”，绕过了正常的充装前后检查流程，将未备案、超期未检或报废气瓶直接充装液化气。此类“作弊”操作隐瞒了大量违规充装事实，使充装记录仅存于本地通讯主机盒中，未能上传至监管系统，增加了监管难度和安全隐患。

为查明该企业的技术性“作弊”行为和操作模式，当地公安局委托奇安信洞鉴进行全面的数据分析和功能验证实验，以揭示其违规充装的真相及背后的技术漏洞。

洞鉴解决方案

1 数据提取与固定

燃气公司本地的通讯主机盒数据库数据提取

利用数据库管理工具解析通讯主机盒数据库文件，提取充装记录表、气瓶表、检查记录表等关键表格。

智慧气瓶安全追溯管理平台数据提取

通过访问智慧气瓶安全追溯管理平台，导出 2022 年至 2023 年期间的气瓶充装记录、充前检查记录、充后复检记录及无条码充装记录，保存为标准化文件格式，用于后续数据比对和分析。

2 数据分析与比对

通过比对通讯主机盒中的充装记录与智慧气瓶平台的记录，发现以下异常：

数据量差异

通讯主机盒记录共计 20 多万条无条码充装记录，这些记录未上传至智慧气瓶平台；智慧气瓶平台仅记录了 4 万条充装记录，数量远低于通讯主机盒本地记录。

充装模式异常

根据通讯主机盒记录的充装模式字段进行筛选，发现 20 多万无条码充装记录全部由应急模式生成，这些记录未经过充装前检查或条码扫描，记录中气瓶条码字段均为空，导致数据存在异常无法同步至智慧气瓶平台。

3 功能复现

在实验室环境下模拟涉案企业的电子灌装秤操作环境，加载通讯主机盒数据库，并连接实验用气瓶，按照涉案企业提供的操作文档还原系统逻辑和操作流程。

常规模式验证

执行标准操作流程，包括扫码验证气瓶状态、完成充装、上传记录至智慧气瓶平台。确认在常规模式下，所有操作均需经过条码扫描和充装前后检查，操作符合安全规定，记录也能正常上传至智慧气瓶平台。

应急模式验证

启用“应急模式 .jpg”中的二维码，触发系统调用函数切换设备至应急模式，在应急模式下，系统允许跳过条码验证和检查流程，直接充装气瓶。充装记录仅存储于通讯主机盒表，未上传至智慧气瓶安全追溯管理平台。

案例价值

01 / 锁定违规操作

通过专业的数据提取、比对和功能验证，精准识别出涉案企业利用“应急模式”规避监管、隐瞒 20 多万条违规充装记录的行为。鉴定结果不仅揭示了违规操作的技术手段，还为公安机关提供了明确的证据链条，大幅缩短了案件侦办周期。

02 / 揭示监管盲点

揭示了智慧气瓶安全追溯管理平台在数据同步和系统设计中的潜在漏洞，为行业监管部门提供了完善技术监管体系的参考建议，有助于推动燃气行业在数字化监管方面的优化升级。

03 / 维护群众利益

燃气行业直接关系到公共安全和人民生命财产安全。通过鉴定，查明了涉案企业为超期未检、报废气瓶充装液化气的事实，有效遏制了因违规充装行为可能引发的重大安全事故，为保护群众利益发挥了重要作用。

02

FORGING BILLS AND DOCUMENTS
伪造票据及证件

伪造票据及证件是指通过篡改、复制或虚构手段，非法制作与真实票据、证件高度相似的仿制品的行为，包括实体形式（如门票、身份证、从业资格证）和数字化载体（如电子票据、虚拟证书）。这种行为本质上是对社会信任机制和身份认证体系的破坏，其危害不仅涉及经济利益的非法获取，还可能影响行政管理的公信力和社会公共安全。

随着技术的进步，伪造手段呈现出技术化和产业化特征。不法分子利用高精度设备、逆向工程技术和数据篡改工具，批量制造假票假证，通过网络平台分销并隐蔽化交易。这不仅扰乱了市场秩序，损害消费者权益，还可能为更严重的违法犯罪提供便利。

1. 常见场景

商业票据伪造

伪造门票、演出票和促销券，主要通过仿制合法票据或构建虚假系统实现，用于非法销售牟利。

作案手段 1：数据篡改

通过搭建虚假票务调度层或漏洞利用，劫持票务系统的合法数据传输流程。

作案手段 2：票据外观仿制

使用高精度打印机复制票面设计、序列号及防伪标志。

证件伪造

伪造身份证、驾驶证、健康证、学历证明、从业资格证等证件，常用于非法就业、贷款申请或逃避法律追责。

作案手段 1：高仿实体证件

使用真实模板和高精度设备制作，附带伪造二维码供假平台验证。

作案手段 2：伪造查询平台

搭建伪造的在线查询系统，让假证书通过“验证”。

政府公文与印章伪造

伪造政府文件、印章和授权书，用于非法审批、合同诈骗或项目投标。

作案手段 1：高精度印章仿制

利用雕刻机制作高仿真度印章，甚至复制动态水印或热感反应。

作案手段 2：图像处理软件

通过抠图、复制、粘贴等操作，可以将真实的印章或文字移植到新的文档上。

医疗与健康相关文件伪造

伪造核酸检测报告、疫苗接种证明和住院病历等行为广泛用于骗取保险赔偿、规避防疫要求或掩盖医疗失误，对公共卫生管理和社会诚信体系造成严重危害。

作案手段 1：篡改病历内容

通过非法手段对真实病历进行删改或添加，改变患者的病情描述或治疗过程。例如，修改病历中的诊断结果、治疗方案、时间或医生签名，以与实际情况不符，从而达到规避责任或获取利益的目的。

作案手段 2：伪造病历资料

完全虚构患者的病历内容，包括捏造诊断信息、假造检查结果或编造治疗记录。不法分子常使用伪造的医院印章和医生签名，使病历文件具有高度仿真性，以蒙蔽保险公司或相关监管机构。

作案手段 3：隐匿或销毁病历

故意隐瞒真实病历，拒绝提供或查阅患者资料，甚至采取销毁或丢弃病历的手段，以掩盖医疗失误或非法行为。

2. 取证鉴定思路

伪造票据及证件案件严重破坏社会信用体系和市场秩序，侵害消费者权益，同时可能影响公共管理的效率与公信力。常见伪造手段包括篡改数据库、伪造签名、制作虚假验证系统以及仿制防伪要素等，其鉴定工作需在合法、合规框架内，结合科学方法与专业技术手段，为执法机关提供可靠的证据支持。

以下为伪造票据及证件案件的通用取证鉴定思路：

1 初步评估

该阶段主要目的是厘清案件范围、锁定关键目标，为后续现场取证和技术鉴定奠定基础。

案件类型与用途

涉案伪造票据或证件的种类：如门票、演出票、从业资格证、学历证明、身份证、健康证、核酸检测证明等。

伪造用途与影响：了解伪造行为的主要动机（非法获利、骗取保险、逃避监管、掩盖犯罪等）以及可能产生的危害（经济损失、社会安全风险、行政秩序干扰等）。

线索收集

案件材料来源：从侦查机关或委托方获取伪造文件样本、交易凭证、网络数据、涉案人员信息等。

初步研判重点：可能的制假窝点、分销渠道和最终使用场景，明确调查的关键人物与主要证据方向。

2 现场勘查与取证

电子设备与数据取证

可疑电脑、打印机、雕刻机、移动存储介质：对制作伪造票据 / 证件可能用到的硬件进行扣押或封存；使用专业取证软件对存储介质进行镜像备份并计算哈希值；提取设计文件（PSD、AI、CDR、DOC/DOCX、PDF 等）、打印记录、日志文件、源代码等。

网络与服务器取证：若存在伪造证件查询网站或在线购票平台，调取服务器日志、数据库记录、源码文件、访问控制记录；若交易通过电商平台或即时通讯工具进行，则调取聊天记录、交易流水、支付凭证等（需具备合法手续）。

现场环境记录

若发现伪造票据的场景布置或特殊设备连接方式，应通过拍照、录像、文字记录进行保全，后续与涉案软件、硬件的运行逻辑相印证。

3 数据分析

伪造文件分析

真伪要素对比：检验文件元数据（如创建时间、编辑软件、修改次数等）是否被篡改或存在异常；针对二维码 / 条形码的解码结果，核对其链接、加密签名或关联的数据库记录是否真实。

图像拼接痕迹识别：使用专业图像取证工具，通过像素级对比或图像算法检测是否有抠图、拼接、调整痕迹；若发现不一致的字体、分辨率、图层信息，可能说明文件经过二次处理。

操作日志分析

软件使用记录：查看涉案计算机的操作系统日志、使用过的制图软件或票据打印工具；识别文件打开、保存、打印的时间节点与用户账号，初步锁定制假人员或制假时间段。

服务器 / 平台日志：在伪造验证网站、票务分销平台等场景下，分析访问日志、API 调用日志，查找是否存在虚假验证逻辑或批量生成伪造票据的接口；核对数据库中的记录与实际编号或票据 / 证件信息是否对应。

交易数据分析

支付流水分析：对嫌疑人银行转账、第三方支付（微信、支付宝等）进行统计，匹配每笔交易对应的票据 / 证件数量或金额。

分销与扩散关系：结合社交软件聊天记录、电商平台订单、快递物流数据等，确认伪造票据 / 证件的购买或销售对象、时间、数量等；对批量售假或团伙式制假，需定位上下游链接，明确各角色分工及责任。

4 功能复现实验

虚假验证系统测试

在隔离的网络环境中部署涉案虚假验证系统，确保实验过程不影响外部系统和网络。通过输入多种测试数据（如真实票据或证件编号、随机生成的无效编号等），观察查询接口返回的结果，验证是否存在以下特征：

- 所有输入均被判定为“验证成功”；
- 查询结果完全依赖虚假的预设数据库内容；
- 无验证逻辑，仅返回静态信息。

数据库篡改测试

使用实验账号操作系统，模拟伪造流程，输入测试数据并观察生成记录是否符合伪造文件的格式及特征，验证篡改过程是否通过预设的脚本或指令直接操作数据库，如通过 SQL 注入或后台管理系统非法操作实现。

5 鉴定意见形成

结合实验复现与数据分析结果，科学严谨地形成鉴定意见书，具体包括以下内容：

事实描述：明确伪造票据及证件的具体特征、伪造手段及实现方式，如篡改数据库、伪造签名、防伪要素仿制等；列明伪造票据或证件的范围、数量，以及伪造数据的来源、分布特点；实验验证结果中反映的假验证系统、伪造数据的使用效果及漏洞。

量化分析：统计伪造票据或证件的非法获利金额或造成的经济损失，如票据售卖金额、伪造证件带来的收益。

技术分析：通过对伪造系统的程序逻辑、数据库篡改记录、数字摘要伪造方式的分析，揭示伪造行为的技术原理；详细说明伪造系统或设备的实现方式，如伪造验证逻辑、数据篡改的操作路径、伪造票据生成的技术细节。

3. 典型案例

景区假门票案

解析虚假票务系统调度原理，揭秘 3000 张假票生成真相

2024 年，某知名景区网络管理人员利用职务之便，在景区内搭建虚假票务系统，制作并销售假门票，导致大量游客持假票入园。奇安信洞鉴受警方委托，对涉案设备及虚假票务系统进行了详细的司法鉴定，揭示了虚假票务系统的运行机制及假票的生成过程，确认了假票销售数量及相关违法事实，为案件侦破提供了关键证据支持。

案件背景

2024 年 6 月，一名游客持旧版门票在某地景区检票入园时，因景区门票模板已升级，检票人员发现该门票为假票，随即报警。景区管理方立即与警方展开联合调查，揭露出幕后黑手竟是景区的一名网络管理人员。他利用职务之便，在景区机房内搭建了一个虚假票务系统，批量生成假票，并通过多个渠道进行非法销售。这些假票不仅在外观上高度仿真，还能够通过景区的检票闸机系统，使大量持假票的游客顺利入园，导致景区遭受严重的经济损失和管理混乱。

洞鉴解决方案

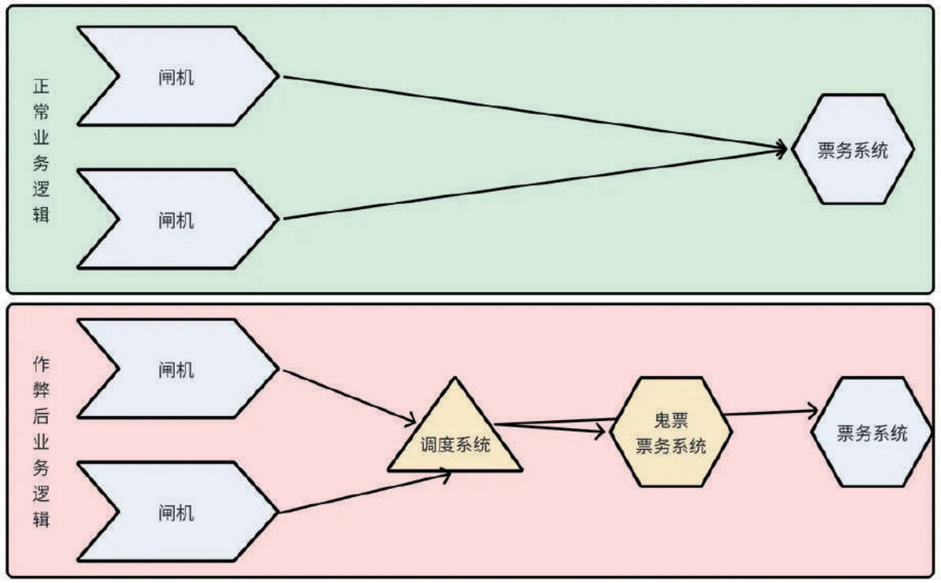
1 虚假票务系统分析

调度系统架构解析

通过对该系统的源码和配置文件的详细解析，鉴定人员发现该系统在合法票务系统与检票闸机之间添加了一个调度层，该调度系统通过篡改检票请求的指向，使假票信息能够绕过合法系统验证。

功能模块验证

对系统中的用户管理、票务录入、电子票生成等功能模块逐一验证，确认系统具备批量生成假票和自动管理假票数据的功能。



2 功能复现与验证

为验证虚假票务系统的实际运作效果，鉴定人员在虚拟环境中复现虚假票务系统的操作流程，输入测试身份证信息和假票数据，模拟检票过程，验证了系统能够成功生成并放行假票。

3 数据分析与销售记录提取

鉴定人员提取系统数据库中的假票销售记录，包含订单号、游客信息、票价、数量及入园状态等详细信息。统计结果显示，系统共生成假票 3000 余张，涉及金额超过 20 万元，为案件侦破和损失评估提供了关键数据支持。

客户价值

01 / 提供关键证据支持

通过对虚假票务系统的深入分析，详细还原了嫌疑人利用调度系统篡改检票流程的作案手法，为警方提供了确凿的技术证据，为后续案件侦破和定罪提供了有力支撑。

02 / 准确评估经济损失

通过对订单号、票价、入园状态等数据的详细分析，鉴定人员为景区管理方准确评估了假票带来的经济损失，为景区后续的法律追责和经济索赔提供了依据。

03 / 强化景区内部安全管理

帮助景区管理方识别了系统安全隐患，并提供了针对性的安全加固建议，有助于景区在未来避免类似事件的再次发生，提升整体安全管理水平。

伪造病历案

透视病历数据，揭示修改痕迹——医疗损害纠纷中的真相追踪

本案例聚焦于一起医疗损害责任纠纷，核心问题在于患者病历的真实性与完整性是否存在问题。患者家属质疑医院在病历中存在伪造和篡改的行为，试图掩盖医疗过程中的过失。奇安信洞鉴通过专业的电子数据司法鉴定技术，对患者两段住院期间的电子病历进行全面分析，不仅发现了多次修改记录的具体内容，还明确了修改的时间点和责任主体，为法院审理提供了关键的技术证据。

案件背景

2019 年至 2020 年期间，患者在某院分别经历了两次住院治疗。其家属发现，病历中部分关键记录的修改时间与患者出院时间不符，且修改内容与实际治疗情况存在矛盾，怀疑医院在病历中篡改记录以规避责任。

本案涉及医疗损害责任纠纷，核心争议为病历是否存在以下问题：

病历记录的真实性

修改记录是否符合实际治疗情况?

病历记录的完整性

是否有关键治疗信息被篡改或删除?

修改责任的归属

修改行为是否符合医院的内部管理和操作规范?

患者家属认为医院的病历记录涉嫌隐瞒真实诊疗信息，直接影响案件中责任认定的公平性。为查清事实，法院委托奇安信洞鉴对病历数据进行全面分析。

洞鉴解决方案

1 电子病历数据提取

登录医院信息管理系统（HIS），通过检索病案号，定位患者的电子病历，使用截图功能保存病历的患者信息、住院记录、诊疗记录等内容，导出病历的文本记录，并存储于本地工作站，确保文件名与病案号一致，方便后续分析。

登录该院电子病历管理系统后台数据库，导出该病人住院期间的电子病历相关记录，数据库中通常记录有该病人住院期间生成的病程记录、住院记录、手术记录等数据的创建修改时间以及修改前后的数据内容。

2 病历修改记录分析

分析该患者在住院期间的病历创建和修改记录中每次修改数据的时间，识别是否有修改时间晚于患者出院时间的情况；涉及重要医疗信息的记录，例如病程记录、诊疗方法和用药记录，检查修改内容是否合理。

分析病历日志记录发现，部分病历记录在患者出院后仍有多次修改，包括诊疗内容的增减和用药记录的补充，进一步确认这些修改的合理性。

3 关键数据验证与比对

使用 Beyond Compare 对病历修改前后的内容进行逐条比对，详细记录以下变化：

诊疗过程

是否新增或删除重要治疗细节，例如关键医疗操作或治疗方案。

出院建议

是否存在新增或删减内容，影响病历的连贯性和完整性。

用药记录

检查药物使用是否符合患者的诊疗背景和实际需求。

将比对结果与操作日志结合，分析修改行为是否由授权人员操作，判断其是否符合医院的管理规范。

客户价值

01 / 助力案件公平裁决

本次司法鉴定揭示了病历修改的具体内容及其潜在问题，为法庭提供了具有公信力的技术证据，有效回应了客户对案件核心争议（病历真实性与完整性）的需求，帮助厘清事实真相。

02/ 明确责任归属

通过数据比对与日志分析，揭示了病历修改的具体时间、内容和操作人信息，锁定了异常修改行为。这不仅帮助法院明确了医院或相关责任人的行为性质，还为后续案件处理提供了可靠的责任归属依据。

03 / 维护患者权益

鉴定过程中发现的病历异常修改记录，为患者及家属提供了有力证据，帮助他们争取到应有的合法权益。同时，这些发现进一步推动了医疗流程的公开化和透明化，对改善医患关系、提升患者对医疗体系的信任具有深远的意义。

伪造从业资格证案

超万条数据，揭开网约车伪造证书黑产

2023 年，一名网约车司机涉嫌使用伪造的从业资格证非法运营，经调查，案件涉及多个伪造证书的管理和操作系统。

奇安信洞鉴对涉案网站进行了全面取证分析，固定了上万条数据，为案件侦破和后续追责提供了核心证据。

案件背景

随着共享经济的快速发展，网约车行业逐渐成为城市交通的重要补充，但与此同时，行业乱象频发。其中，伪造从业资格证的问题尤为严重，不仅侵害了消费者的合法权益，也威胁着公共安全。2023 年，北京市交通执法部门在例行检查中发现，某网约车司机出示的从业资格证被初步认定为伪造，进一步调查显示，该证件由多个非法网站生成和管理，这些网站利用复杂的技术手段批量制作虚假证书，甚至具备“在线查询”功能，试图伪装成正规平台。

案件线索逐渐明朗，伪造证书的范围远超预期。为全面揭露这一非法产业链，公安机关委托奇安信洞鉴对涉案网站的电子数据进行精准固定和深度分析。

洞鉴解决方案

为确保此次伪造证书案件中的电子数据得以完整、规范、可验证地固定和保存，我们对委托方指定的五个目标网站实施了系统性的数据采集与处理。整个过程分为数据固定与采集、数据处理与汇总两个主要阶段，所有操作均严格遵循电子数据取证标准，确保数据的完整性、真实性和法律效力。

1.数据固定与采集

登录指定链接：访问委托方指定链接，使用委托方提供的账号和密码逐一登录。每个链接对应不同的伪造证书管理模块，涉及“证书管理”、“内容管理”等页面，展示了大量伪造证书的记录和管理信息。

固定证书管理页面数据：编写脚本，自动化访问“证书管理”页面，通过发送 GET 请求，逐页下载该页面的静态 HTML 数据，共采集到 200 多个 HTML 文件，每个文件对应“证书管理”页面中的一页记录，总计固定了上万条证书记录。

固定证书详细页面数据：编写脚本，对“证书管理”页面中的每条记录进行进一步数据提取，通过读取每条记录的唯一证书 ID，拼接 URL 参数，逐个访问证书详情页面，并保存完整 HTML 页面。每个 HTML 文件对应一条证书的完整详情数据，包括证书持有人的姓名、身份证号、证件状态、发证日期等更详尽的信息。

固定证书可视化页面数据：编写脚本，模拟真实用户操作，自动访问证书管理页面，将每个页面保存为 MHTML 格式（网页归档文件），共成功固定 200 多个 MHTML 文件，文件中保留了完整的页面视觉展示效果，包括页面样式与图像。

2.数据处理与汇总

在数据固定完成后，我们对采集到的 HTML 和 MHTML 文件进行了结构化数据提取，以便形成更直观的案件分析材料。

提取关键数据：编写脚本，提取 HTML 和 MHTML 文件中的关键字段，如姓名、证书编号、有效期等，便于分析和呈现。

数据梳理：提取数据后，生成结构化的 CSV 和 Excel 表格文件，如，证书管理详情页 .CSV、内容管理详情页 .xlsx 等，将零散的网页信息转化为结构化证据，方便案件审查人员快速检索和分析数据。

姓名	性别	从业资格证	从业资格证	发证日期	有效期起	有效期至	证件类型	证件号码	证照状态	发证机关	从业人员	查询类型
张	男	经营性道路	37(	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
段	男	经营性道路	53(	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
谷	男	道路危险货	21(	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
潘	男	道路危险货	42	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
周	男	经营性道路	62	2020/10/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
梁	男	经营性道路	44	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
张	男	经营性道路	37(	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
黎	男	经营性道路	442	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
陈	男	经营性道路	41(	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
张	男	道路危险货	412	2023/3/20	2023/3/20	2029/3/19	身份证	'	19	有效	市交通	输入查询
李	男	经营性道路	522	2020/10/20	2023/3/20	2029/3/19	身份证	'	9	有效	市交通	输入查询
哈	男	经营性道路	654	2023/3/20	2023/3/20	2029/3/19	身份证	'	9	有效	市交通	输入查询
姚	男	经营性道路	232	2023/3/20	2023/3/20	2029/3/19	身份证	'	9	有效	市交通	输入查询
李	男	经营性道路	441	2023/3/20	2023/3/20	2029/3/19	身份证	'	9	有效	市交通	输入查询

客户价值

01 / 提高案件侦查效率

利用自主编写的自动化脚本，批量固定了证书管理页面、证书详情页及证书预览页面，并将原始网页数据提取为结构化的 CSV 和 Excel 文件，使侦查人员能够快速筛查、比对关键数据，大幅减少了人工整理时间，提升了侦查效率。

02 / 提供完整、合规证据

通过对五个涉案网站的数据全面固定，我们完整采集了上万条证书记录及其证书预览页面，确保了证据链的完整性。同时，采用哈希校验技术对所有数据进行了完整性验证，保障了证据的真实性与不可篡改性，符合规范要求。

03 / 助力维护市场秩序

本次鉴定协助公安机关精准锁定了大量伪造证书的相关数据，有助于打击违法行为，维护正常的营运秩序，减少非法持证可能带来的社会风险。

03

SCALPERS RUSH TO BUY
黄牛抢购

黄牛抢购是指不法分子或专业囤货团体利用技术工具或非正常手段，在限量发售或高需求商品销售过程中，以超越普通消费者正常购买能力的方式大批量囤积商品或票务资源，以谋取不正当高额利润的行为。其核心特征在于通过技术操控、账户批量化操作、绕过平台风控机制等手段，破坏公平交易秩序，剥夺普通消费者的购买机会，从而在二级市场加价倒卖牟利。

现代黄牛抢购已呈现出高度技术化趋势，通过脚本化批量下单、代理 IP 轮换、绕过人机验证等手段，形成自动化、网络化的“抢购生态”。这一趋势使得传统的市场监管与风控措施难以有效遏制，进一步推动了黄牛抢购的隐蔽性和产业化发展。

1. 常见场景

门票
演唱会及体育赛事票务

商品
限量版球鞋、茅台酒、
折叠屏手机

医疗资源
三甲医院稀缺号源
疫苗接种预约资源

车票
节假日、热门时段的火车票、
高铁票

2. 技术手段

自动化抢购软件与脚本

黄牛利用专门开发的抢购软件或定制化脚本，模拟用户在电商平台的全流程操作，如自动登录、选择商品、提交订单与支付等，能够绕过正常的页面前端交互，实现极高的下单速度，从而大幅提高抢购成功率。

API直接调用

通过使用抓包工具解析电商平台的 API 接口，黄牛直接向平台服务器发送下单与支付请求，绕过前端页面的常规操作环节，在登录阶段截取 Token 后伪造批量合法请求，从而大规模下单并避开限流与风控措施。

批量账号注册

为规避限购政策，黄牛会通过购买虚拟手机号或使用批量注册工具，大量生成伪造账号，并借助模拟器与代理 IP 营造独立设备环境，使多个账号能够同时抢购，从而突破平台的单用户限购限制。

绕过验证码与反爬虫机制

电商平台为防止恶意抢购，通常使用滑动验证码、人机验证等安全机制，黄牛则通过 OCR 图像识别技术或算法计算滑动路径破解验证码，甚至通过浏览器注入脚本直接跳过反爬虫保护，实现自动化下单。

3. 取证鉴定思路

黄牛抢购案件涉及使用抢购软件、批量注册虚假账号、篡改平台数据等手段，以不正当方式囤积限量商品后加价牟利，严重破坏市场公平竞争秩序，侵害消费者权益。此类案件的电子数据取证需要确保证据的完整性、客观性和司法适用性，形成科学严谨的证据链条，助力司法机关精准打击此类违法行为。

以下是黄牛抢购案件的取证鉴定思路：

1 证据固定与初步调查

平台数据保全

交易数据：全面提取电商平台的订单信息、支付记录、商品库存变动数据、订单生成日志等，确保数据源的完整性和可追溯性。

日志与流量数据：获取平台网络访问日志、服务器应用日志等，尤其关注访问时间、IP 地址、请求频率、用户代理等，用于识别异常高频或批量访问行为。

账号信息：保留疑似涉案账号的注册信息、登录记录，包括关联的手机号、邮箱、设备指纹等，以便后续溯源。

现场取证

嫌疑人设备：对嫌疑人用于操作“抢购软件”、批量注册账号的电脑、手机、服务器等进行扣押，并通过符合司法要求的取证工具对存储介质（硬盘、手机等）进行全盘镜像及数字摘要 (如 MD5、SHA256) 以确保数据完整性和可验证性。

软件工具与数据：在扣押设备上提取相关软件安装包、源代码、运行脚本、数据库文件、通信记录、操作日志等。

初步排查重点

异常账号：多个账号是否集中出现在同一 IP、同一设备或存在同一设备指纹，或是否使用批量注册工具生成账号。

可疑软件：在嫌疑人设备或日志中发现可执行的抢购脚本、模拟器、自动化工具的运行记录等。

2 涉案工具与程序分析

针对案件中使用的抢购软件、脚本工具等进行全面的程序与硬件分析，揭示其作弊原理。

抢购软件分析：获取和提取抢购软件（可执行文件、源代码、脚本文件等），使用逆向分析、代码审计等方式，重点确认其批量下单、自动化登录、多账号管理、验证码破解等功能模块。分析软件的运行机制，特别是其是否直接调用电商平台 API、是否存在伪造或篡改请求头、跳过人机验证的技术手段等。

批量注册工具分析：检查软件对操作系统、浏览器环境或手机系统的调用状况，识别其是否使用虚拟机、模拟器（如雷电、夜神模拟器等）或分身软件进行批量化操作；调取模拟器配置文件、分身软件配置、日志文件，确认其用于批量创建虚拟终端的次数及方式；识别是否存在自动化脚本定时批量注册、登录操作的记录。

3 功能复现实验

为验证抢购软件的真实功能及其对平台的影响，可在隔离环境下进行功能复现。

隔离环境搭建：为防止对真实电商平台造成影响，建议在司法鉴定机构或具备资质的实验室环境下，搭建尽量仿真的电商平台测试环境，并严格隔离于外部网络。

实验过程记录：在搭建的测试环境中运行扣押的“抢购软件”或脚本，使用测试账号验证其批量下单、自动填写订单信息、突破验证码等功能是否切实可行，使用专业取证工具（如网络抓包工具、行为分析平台）实时监控软件对测试平台所发出的请求、API 调用频率、请求参数、加密方式等，收集软件在实验环境中的运行日志和访问流量包。

4 数据分析

通过对涉案平台及嫌疑人设备数据的多维度深度分析，识别异常交易模式、非法获利情况及其关联性，为案件事实认定提供有力的技术支撑。

交易分析：基于平台提供的订单、支付、物流、账号登录等多维数据，建立与嫌疑人设备取证数据的关联；识别是否存在短时间内大量订单由同一设备、同一 IP 地址或同一时间段生成的异常行为；排查批量下单的账号是否存在支付工具、设备指纹、收货地址等方面的高度重合。

资金分析：计算可疑账号的订单数量、订单金额、实际支付金额，比对嫌疑人提取的资金流动路径（如第三方支付平台、银行账户、虚拟货币钱包等），计算实际非法获利金额。

5 鉴定意见形成

事实认定

根据取证与数据分析结果，应明确以下核心问题，以还原案件事实：

- 是否存在使用抢购软件或自动化脚本进行批量化下单的行为；
- 是否存在使用虚拟手机号、模拟器或分身工具批量注册账号的情况；
- 是否存在破坏电商平台正常业务流程（如绕过验证码、人机验证等）的恶意技术手段或代码模块。

量化分析

通过数据分析计算嫌疑人通过抢购所获非法利益，并量化其异常交易行为的具体程度，包括但不限于：

- 涉案获利金额的计算：涵盖订单总金额、实际支付金额、退款金额及加价转售所得；
- 批量注册账号的数量统计：明确涉案账号总量、异常登录频率以及其与可疑交易的关联程度。

4. 典型案例

抢疫苗案

深度剖析后台源码，还原预约、监控、任务调度全链条功能

本案涉及一起开发、运营自动化软件，通过抢占紧缺医疗资源并提供有偿预约服务的案件。涉案软件通过预置本地数据结合自动化脚本，模拟高频并发请求以获取预约名额，再通过代理下线向社会出售。奇安信洞鉴通过源码级分析，揭示了该软件的技术运行机制：从本地数据的持久化管理到自动化任务执行，再到构建用户校验、数据加解密等功能模块支撑业务运行，以及调用外部 IP 代理服务进行风控策略规避。鉴定报告将代码逻辑转化为具体的技术事实描述，为案件定性提供了核心技术证据。

案件背景

2021年6月起，犯罪嫌疑人瞄准热门医疗资源预约难题，开发非法软件，提供有偿代预约服务以牟取暴利。嫌疑人中有人负责搭建与开发预约软件，有人则专门招揽客户、发展代理，形成分工明确的团伙。随着业务扩张，该犯罪团伙成员已增长至60余人。为彻查该软件的运作机制并固定犯罪证据，办案单位将查获的程序源码送至奇安信洞鉴进行功能性分析。

洞鉴解决方案

01 审查核心配置，明确“本地数据管理”能力

通过分析配置文件，提取了软件内置数据库的完整连接凭证（IP、账号、密码）。此发现证实该程序具备在本地环境构建独立业务数据库的能力，其所有的预约任务逻辑均依赖于对本地预存数据的读取与处理，而非单一的即时输入。

02 解析预约与任务调度逻辑，揭示核心功能

通过对源代码中负责登录、用户信息管理、任务执行等核心模块的分析，鉴定人员揭示了程序在客户端自动化方面的核心逻辑：

1. **用户登录与注册：**程序通过特定接口校验用户（代理）身份。同时，提供数据写入接口，将待预约人员身份信息（如手机号、身份证等）持久化存储于本地数据库中，形成可随时调用的基础数据源。
2. **数据加解密与请求构造：**相关逻辑用于对网络请求参数进行封装与签名处理，通过模拟官方客户端的通信协议，构造符合格式要求的预约请求，以通过服务器端的合法性校验。
3. **多维度信息管理：**

- 人员列表管理：系统具备批量导入、状态标记（如“待预约”、“已成功”）接口，实现了对预约任务队列的精细化管理。
- 目标资源管理：系统支持对目标医院接口信息的配置与更新，可根据需求灵活调整监控对象。

综上所述，该程序围绕待预约人员数据和目标医院资源，构建了一套完整的“监控 - 检索 - 提交”自动化闭环，具备实施高频并发操作的技术条件。

03 追踪外部交互，确认跨网络通信与规避行为

进一步分析发现，该程序集成了特定的外部服务接口：

1. **动态 IP 服务集成：**程序代码中包含向第三方动态 IP 代理服务发起请求的逻辑，用于在频繁访问时更换网络出口 IP，以规避医院服务器的访问频率限制。
2. **第三方授权调用：**系统集成了外部平台的授权交互逻辑，用于获取必要的身份令牌。
3. **客户端环境感知：**程序具备获取当前运行环境 IP 地址的功能。 这些技术特征证明，该软件具备主动利用外部资源进行网络指纹伪装及规避常规安全策略的能力。

案例价值

01 / 梳理核心功能

通过源码解析，完整揭示了涉案软件在批量监控、自动提交以及本地数据预处理方面的技术实现。将抽象的代码逻辑转化为清晰的功能性描述。

02 / 提升办案效能

在侦办过程中，技术难点往往是案件推进的瓶颈。鉴定人凭借专业工具和方法，快速完成了接口还原与功能梳理，帮助办案机关准确把握软件运行机制，节省了大量技术攻关时间，使侦查力量能够集中在锁定嫌疑人、追踪资金流等关键环节。

03 / 揭示作案手法

本次鉴定反映出此类案件的技术特征：即利用本地预存数据配合脚本自动化手段争抢公共资源，并通过技术手段对抗监管。这为相关部门识别此类风险、完善系统风控提供了参考。

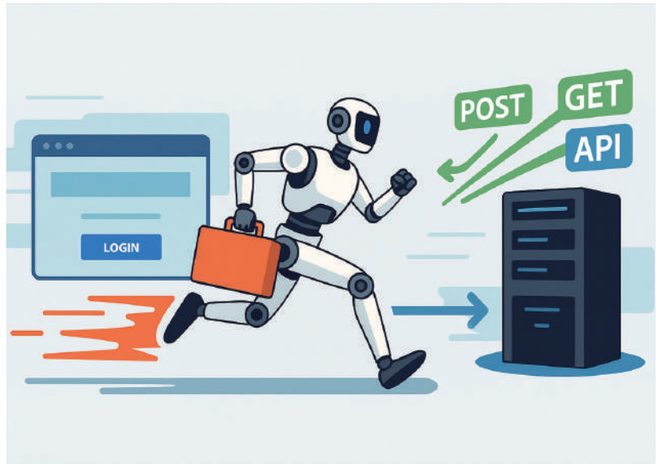
脚本代抢烟草许可证案

逆向分析抢注脚本，还原自动化业务办理全过程

本案涉及一起利用自动化脚本非法抢占稀缺行政审批资源，并以此牟利的案件。犯罪团伙开发脚本工具，绕过政务服务平台正常的人工操作流程，以极高速度批量提交烟草专卖零售许可证的申请，从而提供有偿“代办”服务。奇安信洞鉴通过对涉案程序的深度逆向分析，并结合网络流量模拟验证，完整还原了该脚本的运作机制，为案件的定性提供了关键支撑。

案件背景

2023年起，犯罪嫌疑人潘某发现许多商户难以申请到烟草零售许可证，遂产生利用技术手段代为抢注以牟利的念头。潘某联系到技术人员黄某，并招揽业务员数人，组建了分工明确的犯罪团伙。该团伙以每个脚本约8,000元人民币的价格从技术人员处购买抢注脚本，利用脚本快速上传资料、抢占申请名额，成功后向每个商户收取8,000至25,000元人民币不等的服务费，累计成功办理30余单。为彻查该脚本的运作机制并固定犯罪证据，办案单位将查获的涉案程序送来奇安信洞鉴进行功能性分析。



洞鉴解决方案

1. 程序复现与功能确认

鉴定人在隔离环境中运行涉案程序，确认该程序具备时间设定、目录选择与自动执行等功能。进一步操作发现，程序可通过内置逻辑调用浏览器驱动，自动定位网页元素并模拟点击，实现账号登录、验证码填写和表单提交等操作。这一过程验证了程序确实具备替代人工的全流程自动化申请能力，为后续代码与流量分析提供了基础。

2. 反编译与代码解读

为深入理解该程序的运作机制，鉴定人通过专业的反编译工具对该程序进行解包和逆向分析，成功地将核心逻辑部分还原为可读的 Python 源代码。通过对还原后的源代码进行深度解读，清晰地还原了该脚本设计的全部功能：

1. **本地数据读取：** 程序首先会读取指定文件夹内的 Excel 表格，从中批量获取申请人的详细信息，包括负责人姓名、身份证号、联系电话、经营地址、统一社会信用代码以及用于登录政务网站的账号和密码。
2. **自动化登录与凭证获取：** 脚本内置了浏览器驱动，能够自动化地启动一个浏览器，访问政务服务网的登录页面。随后，它利用从 Excel 中读取的账号密码，通过模拟键盘输入和鼠标点击的方式完成登录，并成功获取维持会话状态所需的用户 Cookie 值。
3. **后台接口直接交互：** 在获取到关键的 Cookie 凭证后，脚本便绕开了前端页面的所有图形化操作。它根据预设的逻辑，直接构造 HTTP 请求，携带 Cookie 向政务服务网的后台服务器 API 发送数据包。通过调用一系列特定的接口，程序化地完成了用户认证、信息查询、证件照片上传以及最终申请信息提交等全部步骤。

3. 验证数据交互行为

在获取到关键的Cookie凭证后，脚本便绕开了前端页面的所有图形化操作。它根据预设的逻辑，直接构造HTTP请求，携带 Cookie 向政务服务网的后台服务器 API 发送数据包。通过调用一系列特定的接口，程序化地完成了用户认证、信息查询、证件照片上传以及最终申请信息提交等全部步骤。

案例价值

01 / 厘清作案工具功能

通过“代码深度分析 + 网络行为验证”的组合手段，将一个无法直接运行成功的程序，其内在的、隐蔽的犯罪功能清晰地呈现出来。原本抽象的代码行为被直观地还原为具体的作案手法，为司法机关准确理解犯罪工具提供了核心技术支撑。

02 / 提升办案效能

凭借专业的逆向分析和网络协议分析能力，精准锁定了脚本绕过前端、直击后台的犯罪模式，帮助办案机关在程序无法直接运行的情况下，依然查明了其核心功能，绕过了技术侦查的难点，大大加快了案件的侦办进程。

03 / 揭示新型犯罪手法

本案揭示了通过程序直接调用政府服务平台后台 API 的新型犯罪模式。这种手法比传统的浏览器插件或模拟点击更为高效和隐蔽，它完全脱离了前端 UI 的限制。本次鉴定为相关监管部门识别同类风险、加固在线服务平台的安全防范体系（特别是 API 接口安全）提供了重要的技术参考。

抢演唱会门票案

精准溯源 + 数据固证，助力精准打击抢票黑产

在一起涉及演唱会抢票的案件中，犯罪分子通过非法手段构造购票客户端向购票系统发送请求，从而实现自动化、批量化、高频率的抢票操作，严重扰乱了票务市场秩序。奇安信洞鉴在接到公安机关委托后，迅速介入案件，深入分析了抢票外挂工具的后台服务器及抢票软件的运行机制，为公安机关快速锁定犯罪嫌疑人提供了关键技术支持。

案件背景

近年来，随着大型演唱会、体育赛事等热门活动的门票需求激增，抢票软件逐渐渗透票务市场，部分不法分子利用技术手段篡改票务平台的网络请求，实现自动化、批量化购票，严重破坏了市场公平性，导致普通消费者难以在正常渠道购票。

2024 年，某公安机关在网络巡查中发现，有不法分子利用非法手段构造购票客户端，以异常高效的方式抢购演唱会门票，涉嫌严重破坏票务平台的正常购票秩序，影响了广大消费者的公平购票权益。为维护市场秩序，公安机关委托奇安信洞鉴进行技术分析，以厘清案件事实，为后续案件办理提供科学证据支撑。

洞鉴解决方案

1 前期技术研判

在案件侦办初期，技术专家协助公安机关对涉案的异常购票行为进行了技术排查，主要工作包括：

网络流量分析：通过网络流量分析工具对涉案抢票工具进行监控，分析其访问的网络地址和域名，初步识别出抢票工具后台服务器地址。

服务器定位：基于流量分析的结果，进一步确认了后台服务器的归属地及其运营商，为公安机关调取涉案服务器提供了信息。随后对调证的后台服务器内的数据进行分析，确认了服务器内含有抢票软件的用户登录信息、购票信息、下游代理信息等数据，为后续证据固定和程序分析奠定了基础。

2 协助现场取证

在明确嫌疑人身份及使用的作案工具后，技术专家全程配合公安机关进行现场取证以及远程勘验服务器的工作，现场核查了涉案计算机、手机、移动硬盘等电子存储介质的完整性及使用情况，并使用专业取证工具对计算机硬盘进行物理镜像提取，完整保存原始数据，重点提取了计算机内的涉案程序及其源代码，用于后续分析工作。

3 程序原理分析

在完成现场数据固定与提取后，鉴定专家对涉案程序及其源代码进行了深入分析，以明确其自动化购票实现方式及潜在违规特征。

自动化购票原理分析：程序具备批量导入手机号和密码的功能，通过程序向票务平台的登录接口发送请求实现批量登录票务平台，具备多线程循环请求和快速发包功能，可在短时间内发起大量购票请求。

验证码规避技术分析：涉案程序集成了多种验证码识别与绕过技术，包括调用 OCR 识别库和 Ai 模块进行滑块位置识别、滑块图像内容识别与计算，并模拟人工拖动滑块，以实现绕过票务平台的人机验证机制。

数据回传与远程通信分析：程序在下单成功后，将购票订单数据（如账号、票务信息、订单编号等）回传至云端服务器，用于上游黄牛与下游代理、买家进行结算统计。结合程序的网络通信行为分析，确认了服务器接收的购票数据与嫌疑人的购票行为存在直接关联。

客户价值

01 / 实现高效案件侦办

提供从前期技术研判、现场数据固定、程序原理分析到证据报告出具的全流程电子数据司法鉴定服务，确保案件侦查各环节有序衔接，帮助公安机关全面掌握涉案工具的技术原理，有效提升案件侦办效率与精准性。

02 / 确保证据合法合规

通过严谨的电子数据取证技术与规范化的证据固定流程，确保所提取的电子数据符合司法规范，为公安机关提供明确的涉案工具运行原理、自动化抢票行为及数据流转的完整证据链条，为案件的后续法律诉讼提供有力的技术支撑。

03 / 维护票务市场公平秩序

揭示了利用自动化工具大规模抢票、规避平台风控机制的行为，严重影响了消费者的正常购票权益。通过对此类案件的深入分析与打击，有助于规范市场行为，保障普通消费者的公平购票机会，维护正常的市场交易秩序。

抢火车票案

12306 抢票软件鉴定，助力打击违规购票行为

该案涉及一款第三方抢票软件，该软件在未通过 12306 正常的登录验证流程情况下，可完成登录、车票查询及订单提交，且可同时为多个乘车人提交多个车次的预定购票任务，疑似存在绕过 12306 官方安全机制的行为，严重影响了购票的公平性和安全性。奇安信洞鉴对该软件的登录方式、购票流程、数据包交互情况等关键功能进行了全面的鉴定分析，并出具了专业的司法鉴定意见，以供案件审理使用。

案件背景

近年来，随着铁路购票全面实现电子化，黄牛及不法分子利用第三方抢票软件，通过技术手段大批量抢占优质车票的现象愈发严重。

此次案件起因于某地公安在一次网络巡查中发现，有用户使用某抢票软件频繁在 12306 平台上成功购票，该软件能通过构造数据包自动向 12306 官方服务器接口发送数据模拟用户操作的形式，绕过正常购票流程直接完成登录与购票操作，疑似涉及恶意绕过安全验证及网络爬虫违规行为。

为进一步厘清该软件的工作原理及潜在风险，公安机关委托奇安信洞鉴进行电子数据司法鉴定，旨在通过科学的技术手段确认该软件是否存在违规操作及其具体实现方式，为后续案件办理提供科学有力的证据支撑。

洞鉴解决方案

1 账号登录测试

为验证软件在登录 12306 账号时的具体网络交互与潜在异常行为，鉴定专家在隔离环境中运行抢票软件，使用委托方提供的 12306 账号进行登录测试，并使用抓包工具实时监测网络数据包，记录每一步网络请求的地址与传输的数据。

发现登录成功后，软件可保存“登录态数据包”，支持直接粘贴复用，无需再次输入账号、密码及验证码，绕过了 12306 平台正常的二次验证码验证机制，存在安全隐患。

2 车票查询功能测试

为验证软件是否具备自动化查询车票的能力，并分析其对 12306 服务器的潜在影响，鉴定专家在软件内输入出发地、目的地及出发日期进行车次查询，同时使用抓包工具监测网络交互行为。

发现软件可批量查询车票信息，且支持自动化触发多次查询请求，存在频繁刷票的潜在风险，可能对平台正常服务造成压力。

3 自动化购票功能测试

为验证软件是否具备批量自动购票的能力，并评估其对 12306 平台的潜在风险，鉴定专家在查询到的车次信息中，勾选乘车人，点击“创建购票任务”，随后点击“开始”按钮，观察软件的实际操作行为。

发现软件可自动批量购票，无需用户干预，在短时间内持续向 12306 服务器发送高频请求，存在平台超载风险。

4 异常行为复现与登录态复用测试

为进一步验证该抢票软件是否存在可绕过 12306 安全验证的异常行为，鉴定专家删除 12306 账号的登录记录，随后粘贴之前保存的“登录态数据包”，尝试直接进行车票查询与下单操作。

发现可直接完成购票操作，无需重新输入账号、密码及验证码，存在身份认证绕过风险，破坏 12306 平台正常安全机制。

客户价值

01 / 提供关键证据支撑

通过全面的技术分析与规范的司法鉴定流程，明确识别抢票软件的异常行为，出具专业的司法鉴定意见书，为公安机关案件办理提供强有力的技术证据支持，助力案件顺利侦办与审理。

02 / 揭示抢票软件的技术违规细节

通过对软件的账号登录、车票查询、自动化购票及登录态复用等功能进行逐一测试，明确揭示该软件绕过 12306 安全机制的异常操作方式，有助于平台方直观理解风险点。

03 / 赋能平台方风控升级

基于鉴定发现的登录态复用与高频自动化购票行为，为 12306 平台提出针对性防御策略建议，如二次验证码校验优化、自动化行为检测等，帮助平台方提升反自动化风险防控能力。

04

TAX CRIME
税务犯罪

税务犯罪是指行为人以非法手段逃避、骗取或侵占国家税收的行为，主要包括虚开发票、骗取出口退税、偷逃税款、伪造账目等。此类犯罪直接损害国家财政收入，破坏税收制度的公平与权威，并通过虚假交易链条、虚拟资金流动等手段掩盖真实经济活动，给执法机关的查证工作带来极大挑战。

随着数字经济与金税四期工程的深度发展，涉税犯罪也呈现出新的特征：一方面，传统的犯罪手段（如隐匿收入、虚列支出）变得更易被大数据系统发现；另一方面，新型的犯罪手法层出不穷，犯罪行为更加专业化、团伙化，并越来越多地利用虚拟身份、复杂资金网络、第三方支付和境外服务器等技术手段，与监管体系进行对抗。

1. 常见场景

虚开增值税发票

指在没有真实货物或服务交易的情况下，为他人、为自己、让他人为自己、介绍他人开具增值税专用发票的行为。其主要目的是为受票方提供非法的进项税额抵扣凭证，或用于虚增业绩、骗取贷款等，是典型的破坏国家税收征管秩序的犯罪行为。

作案手段 1：注册空壳公司

注册控制多家空壳公司，伪造货物交易背景。

作案手段 2：制造虚假票据

制作虚假合同、发货单、对账单以支撑虚开行为。

骗取出口退税

指利用国家为鼓励出口而实施的税收优惠政策，通过伪造出口业务单据、虚报出口商品等手段，骗取国家出口退税款的行为。

作案手段 1：假报出口

在根本没有货物出口的情况下，利用控制的空壳外贸公司，伪造全套的购销合同、出口报关单、海运提单和外汇水单，凭空骗取退税。

作案手段 2：低值高报

将实际出口的价值较低、退税率较低的商品（如日用百货），在报关时伪报为价值极高、退税率也高的商品（如电子产品、高新设备），以骗取高额退税差价。

作案手段 3：循环出口与回流

将一批货物正常出口至香港等地，完成退税后，再通过伪报、瞒报（如夹藏）等方式将同一批货物重新进口至境内，再次用于虚假报关出口，反复利用同一批货物骗取退税。

伪造财务账目

指故意编制、篡改或销毁会计资料，以虚假财务状况掩盖非法活动、逃避纳税义务的行为，是多种经济犯罪的基础。

作案手段 1：设立内外账

建立真假两套账目，一套用于内部管理，一套用于虚假申报。

作案手段 2：虚构支出

以假票或虚假凭证入账，凭空增加成本费用。

隐瞒收入：循环出口与回流

通过个人或体外账户收款不入账，隐匿真实销售规模。

2. 取证鉴定思路

税务犯罪严重侵蚀国家税基，破坏市场公平竞争秩序，是危害经济健康发展的核心犯罪类型之一。其常见手段包括控制空壳公司、伪造财务账目、构造虚假资金流、利用专业票据中介等，已形成高度网络化、产业化的犯罪链条。电子数据司法鉴定旨在穿透数据迷雾，还原资金、票据、货物的流转真相，为执法机关精准打击犯罪、追缴国家损失提供核心技术支撑。

以下为税务犯罪的通用取证鉴定思路：

1 初步评估

该阶段主要目的是明确案件性质、锁定关键目标和涉案范围，为后续取证和分析提供方向。

案件类型与特征：
明确案件主要涉及虚开增值税发票、骗取出口退税、逃税，还是多种犯罪行为交织。

涉案主体与工具：
梳理涉案公司、空壳企业、财务人员、票据中介，以及使用的财务软件、发票系统或报关平台。

违法影响与危害：
评估涉案金额、税收流失规模及对财政制度、公平竞争秩序的潜在冲击。

2 现场勘查与取证

围绕“人、财、票、货”四大要素，全面、规范地固定核心电子证据。

1. 核心办公设备取证

财务、业务电脑：
对财务、开票、业务员等关键岗位人员的电脑进行完整镜像。重点关注金蝶、用友、速达等主流财务软件的数据库文件，以及存储“内外账”的 Excel、Word 等文档。

服务器与存储介质：
若企业使用内部服务器或 NAS 存储数据，需进行整体取证。对发现的 U 盘、移动硬盘等介质，一并进行镜像固定。

2. 税控设备与发票数据取证

税控盘 / 金税盘：
依法扣押企业使用的税控设备，它是证明发票开具主体的直接证据，提取其中的开票明细数据。

发票影像与 OFD 文件：
提取存储在电脑中的增值税发票扫描件、照片及 OFD 格式电子发票文件，用于后续票面信息比对。

3. 移动终端与即时通讯取证

手机、平板电脑：
对涉案核心人员的移动设备进行完整镜像或数据提取。

通讯内容：
重点提取微信、QQ、Telegram 等即时通讯工具的聊天记录，特别是涉及“开票”、“点位”、“手续费”、“回款”、“对公 / 对私”等关键词的群聊和私聊内容。

3 数据分析

以“三流一致”为核心检验原则，通过多源数据交叉比对，还原犯罪事实。

1. 财务与经营数据分析

账实比对：
将账目中的采购与销售记录，与出入库单、物流单、送货单等单据进行交叉验证，筛查无实物流转的虚假交易。

发票与业务匹配度分析：
将税控设备中开具的发票（票流），与财务账、购销合同、出入库记录（货物流）进行比对，重点关注发票品名与实际经营范围严重不符、短期内开票金额与企业规模严重不匹配等异常情况。

2. 资金流向分析

核对企业对公账户的银行流水，验证其与发票票面金额、交易对象、交易时间是否一致。

3. 犯罪通讯网络分析

角色身份定位：
通过分析聊天记录，还原嫌疑人在犯罪网络中的角色（如老板、财务、票据中介、开票手等），明确其犯意联络和具体分工。

关键事实佐证：
从聊天记录中提取与特定发票、特定转账相关的对话内容，如商谈“开票点位”、指挥“资金回流”等，作为佐证财务数据、资金数据分析结论的关键言词证据。

4 鉴定意见形成

基于全面的分析与检验，形成客观、科学、严谨的鉴定意见。

1. 涉案金额统计

依据恢复的电子账册与银行流水，对虚开发票的价税合计金额、税额，骗取出口退税的金额，以及犯罪团伙的非法获利金额进行计算。

2. 技术手段与路径分析

详细剖析犯罪所依赖的核心技术手段（如内外账的建立与隐藏方式、资金回流网络的具体构造路径），并以流程图、关联图等形式直观呈现，为法庭审理提供清晰的技术解读。

3. 典型案例

虚开增值税发票案

多设备取证，揭开虚开发票案中的数据真相

本案涉及一起特大虚开增值税发票案。犯罪嫌疑人利用微信群组作为主要沟通渠道，通过实时转发票据信息、对接资金回流及“票据中介”撮合交易等方式，形成了较为完整的黑色链条。

奇安信洞鉴通过对涉案的多台手机、笔记本电脑进行全面、深入的电子数据取证分析，成功从海量的碎片化信息中提取并恢复了关键的聊天记录与办公文档，清晰还原了该犯罪团伙的组织架构、作案手法，为案件的成功侦破提供了坚实证据。

案件背景

近年来，一个犯罪团伙为牟取非法利益，注册并控制了多家“空壳”公司，在没有真实货物交易的情况下，大肆对外虚开增值税专用发票，涉案金额巨大。该团伙成员分工明确，有人负责联系“客户”，有人负责制作虚假的合同与账目，核心成员通过微信群进行指挥联络、发送开票指令和沟通回款事宜。所有犯罪证据，包括沟通记录、虚假合同、财务账目、开票信息等，都散落在多名成员的个人手机和电脑中，数据庞杂且隐蔽，给案件的侦办带来了巨大挑战。

为彻底查明该团伙的犯罪事实，完整固定其犯罪证据链，办案单位将查获的多部手机和电脑送至奇安信洞鉴进行电子数据司法鉴定。

洞鉴解决方案

1 移动端数据提取与检索，锁定核心沟通证据

使用专业取证系统，对多部涉案手机的通讯录、通话记录及微信数据进行了全面提取，并恢复了部分已删除消息。根据委托要求，固定了“内部开票回款沟通群”及相关个人对话记录。同时，借助“开票”等关键词检索，对涉及开票的关键信息进行了快速定位。

2 计算机文档恢复与分析，揭示业务操作全貌

对涉案的笔记本电脑进行了完整的镜像和数据恢复，成功恢复并提取了超过 6 万个办公文档文件，包括 Word 文档、Excel 表格和 PDF 文件。通过对这些文档的分类与内容分析，发现了大量伪造的业务合同、虚假财务报表、客户清单及开票明细。这些文件反映出该团伙如何伪造业务背景，以支撑其大规模的虚开发票行为。

3 跨设备数据关联，厘清账号与设备归属

对涉案的笔记本电脑进行了完整的镜像和数据恢复，成功恢复并提取了超过 6 万个办公文档文件，包括 Word 文档、Excel 表格和 PDF 文件。通过对这些文档的分类与内容分析，发现了大量伪造的业务合同、虚假财务报表、客户清单及开票明细。这些文件反映出该团伙如何伪造业务背景，以支撑其大规模的虚开发票行为。

案例价值

01 / 提高办案效率

面对十余台设备中的 TB 级数据，鉴定人员凭借先进的取证工具和丰富的案件经验，在短时间内快速锁定了核心证据，极大地缩短了案件的侦办周期，帮助办案单位节省了大量的人力和时间成本。

02 / 提供直观证据

在多部手机和电脑中，检索和固定了大量与“开票”相关的聊天记录和办公文档。这些数据直接揭示了涉案人员在沟通群组中的交流内容、办公电脑中的票据文件存储情况，为案件定性提供了直观证据。

03 / 支撑深度研判

除本案直接证据外，本次提取的大量通讯、票据及文档记录，还为办案机关开展资金追踪和人员关系梳理提供了可靠的数据支撑，为后续刑事侦查奠定了坚实基础。

骗取出口退税案

跨设备取证，还原虚构贸易背后的数据链条

本案涉及一起利用虚假贸易骗取国家出口退税的经济犯罪案件。涉案公司通过伪造业务单据、虚构出口业务，形成完整的虚假单证链条以骗取巨额税款。犯罪团伙成员分工明确，利用多台手机、电脑等电子设备进行日常联络与业务操作。

奇安信洞鉴通过对涉案人员的多台手机和办公电脑进行电子数据取证，成功提取并恢复了数十万条关键的微信聊天记录和数万份核心办公文档。本次鉴定不仅完整还原了嫌疑人之间的联络内容，还获取了其实施犯罪行为所使用的具体文件资料，为案件的成功侦破提供了核心证据支撑。

案件背景

据办案机关介绍，某家具企业涉嫌通过虚构贸易背景、编造出口业务，从而骗取出口退税。涉案人员分工明确：有人负责与票据中介及上下游企业沟通，有人负责账务与资金回流，还有人通过电脑撰写、修改相关单证。

为全面厘清涉案链条，公安机关将查获的数部手机及台式机送交奇安信洞鉴进行取证分析。

洞鉴解决方案

1 全面固定多源数字证据，锁定关键设备

鉴定人员首先对涉案的手机和台式机进行了全面的检查与证据固定。这些设备分属团伙内的不同成员，是其日常联络和处理业务的核心工具。通过对设备进行逐一编号、拍照、制作镜像，确保了原始证据的完整性和后续分析的准确性，为跨设备关联分析打下基础。

2 深度解析移动通信数据，还原沟通网络

鉴定人员利用专业取证系统，对手机进行了深度的信息提取与恢复。

海量通信记录提取

成功从多部手机中提取了包括通讯录、通话记录、短信在内的大量基本通信数据。

微信数据深度恢复

重点对微信应用进行了分析，共提取了 10 个微信账号的超过 40 万条聊天记录，并成功恢复了 13 万条已被删除的聊天记录。

3 恢复并提取核心办公文档，固定业务物证

针对两台办公电脑内的四块硬盘，鉴定人员进行了完整的镜像和数据恢复。

操作系统及用户信息分析

成功提取了硬盘中的操作系统信息、用户登录记录等，明确了电脑的主要使用者和最后操作时间，为锁定行为主体提供了依据。

海量办公文档提取

经过全面的数据检索与恢复，共从三块存有数据的硬盘中成功导出了超过 20,000 个办公文档文件（包括 Word, Excel, PDF 等）。这些文件是该公司伪造出口单据、制作虚假合同、进行内部财务核算的核心物证。

客户价值

01 / 形成完整证据链

在本案中，涉案人员的活动分散在多部手机和台式机中，奇安信洞鉴通过统一的取证流程和工具，将不同来源的数据（通讯录、微信、短信、通话记录、办公文档等）进行恢复与串联，打破信息孤岛，形成了涵盖“票据、账务、资金、人员”的全链路证据链。

02/ 提供关键突破证据

技术专家成功从多部手机中恢复了数万条已被删除的微信聊天记录，这些被尝试抹去的痕迹，成为识别涉案人员真实意图与资金往来安排的关键证据点。

03 / 维护国家财经秩序

将隐藏在手机、电脑中的碎片化信息，还原成清晰完整的犯罪事实，让企图通过技术手段弄虚作假、骗取国家利益的行为无所遁形，为国家挽回经济损失、维护税收制度的严肃性与公平性提供有力保障。

05

SMUGGLING
走私

走私是指违反海关、进出口管理与相关法律法规，采用隐瞒、欺骗、伪报、转移运输路线或其他非法手段，将货物、物品、动植物资源、人体组织样本或资金跨境转移的行为。走私不仅侵犯国家管理主权、损害国家税收和法定监管秩序，还可能触及公共安全、生态安全、人体伦理与国际条约义务，社会危害性大、涉案链条复杂、跨地域协同性强。

1. 常见场景

走私普通货物

犯罪手法

以偷逃应缴关税为直接目的，采用伪报贸易性质（如一般贸易伪报为个人物品）、低报价格或夹藏等方式，将高税率、高价值的消费品非法输入境内。

鉴定支持

通过提取和分析交易记录及通讯数据，确认货物的伪报、夹藏等非法行为。

走私禁运物品

犯罪手法

该类犯罪直接危害国家安全、公共安全或战略资源安全，其行为表现为非法跨境运输武器弹药、毒品、成品油、管制类精神药品等国家严令禁止的物品。

鉴定支持

追踪跨境通信、资金流动，揭秘核心走私人员。

走私珍贵动物制品

犯罪手法

违反《野生动物保护法》及相关国际公约，构建跨国非法交易链条，走私《濒危野生动植物种国际贸易公约》附录所列的珍贵、濒危动物及其制品。

鉴定支持

分析社交媒体和电商平台的数据，追踪濒危物种制品的非法交易网络。

走私废物

犯罪手法

以合法货物为掩护，通过伪造环保批文、篡改商品编码（HS Code）、夹藏等方式，将境外工业、医疗、生活等固体废物非法输入境内，规避国家环保与海关管制。

鉴定支持

通过提取电子数据，分析废物来源和运输路径，确定其非法进入的环节。

2. 取证鉴定思路

走私案件往往跨地域、跨部门、跨平台，涉及单证伪造、物流隐匿、资金中转与通信协同等多条并行链路。其电子痕迹分布广泛且易被有意篡改或销毁，因此鉴定工作必须在司法授权下，遵循证据保全优先、技术可复现与业务关联系统化原则，综合运用单证比对、轨迹还原、通信恢复、样本鉴定与资金流追踪等方法，形成“单证—物流—款项—人员—设备”的闭环证据链。

以下为走私案件的通用取证鉴定思路：

1 初步评估

该阶段旨在厘清案件范围、识别关键环节与优先保全对象，为现场取证和后续技术分析制定策略。

案情研判：
了解案件基本情况，识别走私类型（如偷税、禁品、废物等）和主要作案手法（如水客、伪报、绕关等），确定取证和分析的重点。

目标系统与证据源：
列出可能涉及的系统与设备（海关报关系统、物流平台、仓储管理系统、快递平台、ERP、邮件服务器、银行 / 第三方支付系统、涉案人员终端等）。

2 证据固定与保全

本阶段旨在完整、无损地提取原始电子数据，并确保其真实性。

设备镜像：
对涉案计算机、服务器、移动硬盘等存储介质进行完整镜像，并计算哈希值以确保数据未被篡改。

数据提取：
使用专业取证工具，提取手机、税控盘、GPS 设备等终端中的通讯录、聊天记录、财务、定位及开票数据。

信息调取：
依法从电商、物流、支付等平台调取并固定与案件相关的订单、运单和交易流水等信息。

3 数据分析与关联

本阶段是鉴定的核心，通过多源数据交叉比对，还原犯罪事实。

1. 通讯网络分析

组织架构分析：
分析加密通讯、邮件等数据，理清团伙的组织架构、层级和人员分工（如货主、买手、水客、司机等）。

关键内容提取：
从聊天记录中查找、提取涉及货物、价格、暗语、接头地点等具体犯罪行为的对话内容。

2. 交易与资金分析

交易真实性检验：
比对报关单、订单、发票与银行流水，检验业务的真实性，发现伪报、瞒报等行为。

资金流向追踪：
整合银行、第三方支付、虚拟货币等交易数据，查明资金来源与去向，重点发现“资金回流”、“手续费”支付等异常模式。对于普通货物走私，需核定货物真实价值，审计偷逃税额。

3. 物流路径还原

运输轨迹分析：
整合 GPS 数据、订票信息、出入境记录、物流平台信息等，还原涉案货物与人员的跨境运输完整路径。

异常行为发现：
从还原的路径中，定位绕开海关监管区、中途转运、人货分离等可疑行为。

4. 虚拟身份关联

关联分析涉案的社交媒体、电商平台账户，通过注册信息、发帖内容、好友关系等，穿透网络身份，锁定其背后的真实行为人。

4 鉴定意见形成评估

基于全面的数据分析与检验，形成客观、科学的鉴定意见，主要包括以下内容：

1. 犯罪事实描述

分析并呈现相关人员、公司、账户之间的通讯与资金关联，客观反映其组织架构与联络模式。同时，根据可查证的电子数据，还原涉案物品从特定起点到终端的、有数据支撑的流转轨迹。

2. 涉案价值统计

基于恢复的交易记录与资金流水，意见书将对涉案走私货物的真实价值、因伪报或瞒报所偷逃的应缴税额，以及犯罪团伙的非法获利总额进行计算。

3. 典型案例

走私孕妇血样案

深度数据恢复与关联分析，完整还原非法产业链条

本案系一起涉及跨境走私人类遗传资源的重大案件。犯罪团伙在内地大规模收集孕妇血样后，走私至香港进行非法的胎儿性别鉴定，已形成组织严密的黑色产业链。奇安信洞鉴受托对查获的十余部手机及两台笔记本进行电子数据司法鉴定，恢复提取了通讯录、聊天记录、通话记录、文件文档等数百万条关键数据，清晰揭示了该团伙从样本收集、跨境运输到客户联络的完整运作模式，为办案机关斩断这条非法产业链提供了坚实的技术证据。

案件背景

自 2021 年起，犯罪团伙瞄准内地部分家庭对胎儿性别的非法鉴定需求，开始从事收集孕妇血液样本并走私至香港进行检测的犯罪活动。该团伙通过线上社交平台和线下代理网络，在全国范围内招揽“客户”，初步查证涉及的孕妇血样高达两千余份。为彻底查清该团伙的组织架构和犯罪事实，办案单位将在抓捕行动中查获的 17 台核心涉案电子设备，送至奇安信洞鉴进行全面的数据恢复与分析。

洞鉴解决方案

1 全量提取与分类，还原多源数据

鉴定人对多台 iPhone、华为、vivo 等品牌手机，以及 MacBook 笔记本进行全面提取。不仅保全了设备中的现有数据，更成功恢复了数十万条已被删除的关键记录，累计获取通讯录、短信、通话记录、社交聊天、文档、多媒体等各类数据数百万条，为后续的关联分析奠定了坚实基础。

2 关联社交账号，揭示团伙勾连网络

本案的核心证据隐藏在海量的社交聊天记录中。鉴定人对设备中的微信、QQ、钉钉等多个社交应用进行了深度解析，提取到昵称为“香港 *”“A 香港 *”“医疗 *”等账号累计聊天记录上百万条，涉及大量血样交接、费用结算等内容。这些直接的通讯记录，成为了证实犯罪嫌疑人之间存在犯意联络、共同实施犯罪的核心证据。

3 聚焦关键业务数据，揭示作案模式

鉴定团队并未止步于简单的数据提取，而是对通讯录、通话记录、多媒体文件（照片、视频）、文档等多元化数据进行了交叉比对和关联分析，具体如下：

1. **经营模式分析：**聊天记录中高频出现“抽血”“邮寄”“报告”“基因检测”“验男孩女孩”等词汇，结合微信转账记录，印证其“境内收集血样、境外检测、收取费用”的经营模式。
2. **物流与资金分析：**两台 MacBook 笔记本电脑中，提取出办公文档、压缩包等文件共 20 余万条，其中包含收样名单、资金流水表格、收货地址等信息。这些结构化数据与社交记录相互印证，构成了从接收客户订单到境外机构出具检测结果的闭环证据。

案例价值

01 / 梳理全链条证据

涉案设备众多，数据来源分散。鉴定团队通过跨终端比对分析，将不同嫌疑人设备中的社交账号、联系人、聊天内容进行关联，成功将孤立的数据点串联成一条完整的证据链，清晰证明了整个团伙的协同犯罪行为。

02 / 提升侦办效能

鉴定过程中，大量恢复出的删除消息、压缩包和办公表格，是案件关键证据。鉴定人快速恢复了数十万条已删除微信、QQ 和钉钉记录，并精准筛选出与血样走私相关的高价值信息。这一成果显著缩短了办案机关的技术突破周期，使侦查力量能够从海量数据中“解放”，集中精力锁定嫌疑人分工、追查资金流向，大幅提升了案件推进效率。

03 / 揭示新型作案手法

本次鉴定不仅为个案提供了决定性证据，其成果也为监管部门预警和防范类似犯罪提供了重要参考。例如，报告中明确的涉案账号特征与关键词可用于线上风险预警；揭示的“境内收集、境外检测”的新型运作链条，也为完善口岸查控和人类遗传资源管理制度提供了有价值的技术视角。

CHAPTER 3

网络黑灰产治理

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。

本章旨在为电商、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

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的下载链接或从存储介质中获取 APK 文件。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

非法控制游戏案

深度还原外挂脚本与抓包篡改，揭示游戏数据操控全链条手法

本案涉及一起通过外挂脚本及网络流量劫持手段，对热门网络游戏及微信小游戏进行非法控制的案件。涉案人员通过模拟器环境批量运行外挂，并利用脚本与数据篡改手段操控游戏参数、篡改存档，严重破坏了游戏的公平性。奇安信洞鉴通过对送检硬盘的镜像提取、文件解析和功能复现，完整揭示了两种典型外挂的运行机制，为案件的定性提供了直接技术证据。

案件背景

2024 年，办案单位在工作中发现，有人员涉嫌通过雷电、夜神等安卓模拟器在多台电脑上批量运行外挂，使用“Lua 脚本”对某热门网络游戏进行参数篡改，实现无限血量、技能秒杀、属性极值等作弊功能。在另一案件线索中，嫌疑人利用微信小游戏的配置文件漏洞与数据交互缺陷，通过本地替换和数据拦截篡改，解锁作弊界面、批量增加金币钻石，甚至可跨账号加载存档。

随着调查深入，公安机关从多名嫌疑人处查获二十余块硬盘，内含大量模拟器运行记录和涉案脚本、配置文件。为固定证据、厘清外挂运行机制，办案单位将上述检材送至奇安信洞鉴进行司法鉴定。

洞鉴解决方案

01 多硬盘镜像与模拟器痕迹提取

鉴定人首先对涉案的二十余块硬盘进行只读镜像与哈希校验，确保数据完整与可验证性。在逐一解析过程中，发现多块硬盘中存在大量雷电、夜神模拟器运行记录，并成功提取出相关的虚拟机文件。部分虚拟机文件解压后大小达数十 GB，印证了其通过模拟器环境进行长期、批量化操作的作案特征。

02 模拟器环境还原与脚本功能分析——还原“参数修改”外挂

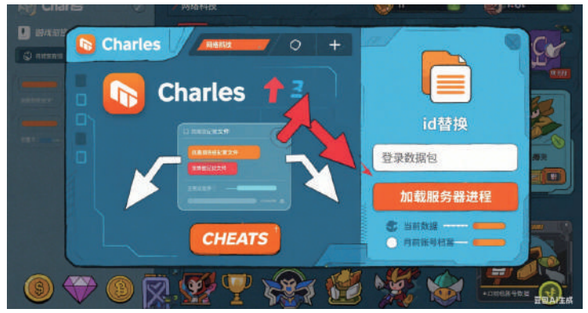
针对网络游戏的作弊外挂，鉴定人从硬盘镜像中恢复了嫌疑人使用的安卓模拟器环境，并成功启动。

1. **注入并执行脚本：**在模拟器中运行游戏，并将 lua 脚本载入。脚本成功注入游戏进程后，游戏画面上立刻弹出一个功能丰富的作弊菜单，包括“无限血”、“技能无冷却”、“全屏秒杀”、“攻击 / 移动速度加快”等多个选项。
2. **验证外挂效果：**鉴定人员逐一测试了菜单功能。开启“技能无冷”等功能后，游戏角色的法力值、智力、攻击速度、移动速度等核心参数瞬间被修改为“9999”、“500%”等异常数值，实现了秒杀怪物的变态效果。开启“无限血”功能后，角色的生命值也被锁定为异常高的数值，达到了“无敌”状态。

03 网络流量劫持分析——揭示“数据替换”外挂手法

针对微信小程序的作弊外挂，鉴定人使用了网络抓包工具 Charles 进行功能复现：

1. **解锁作弊菜单：**鉴定人使用 Charles 拦截游戏与服务器之间的通信。通过本地映射功能，将服务器下发的正常配置文件请求，重定向至本地的恶意配置文件。游戏加载此文件后，设置界面竟出现了一个官方隐藏的“CHEATS”（作弊）按钮。通过此菜单，玩家可以任意修改金币、钻石数量，一键解锁所有英雄，甚至随意增减奖杯数量。
2. **实现账号覆盖：**鉴定人进一步分析了另一个关键文件“id 替换”的作用。通过拦截并修改游戏登录时的数据包，将返回的账户信息替换为“id 替换”文件中的指定内容，成功触发了游戏“加载服务器进程”的提示。选择加载后，当前账号的所有数据（包括道具、等级、角色等）均被替换为目标账号的存档数据，实现了对任意游戏账号的“克隆”与覆盖。



客户价值

01 / 精准支撑司法定性与责任追究

鉴定人直观展示了外挂脚本可以直接修改游戏客户端参数、操控服务器交互，从而达到控制系统运行逻辑的效果。这些经验证的技术结果，为办案机关认定行为是否构成“非法控制计算机信息系统”等相关罪名，提供了清晰、可验证的依据。

02 / 完整揭示外挂运行链条

鉴定人通过逐层拆解，从硬盘镜像与模拟器痕迹，到 Lua 脚本的功能复现，再到抓包工具的数据篡改，完整呈现了外挂以何种形式存在（脚本 / 模拟器文件）、如何被加载运行、以及如何实现对游戏参数和数据交互的篡改，使侦查人员、检察官和法官能够直观理解外挂对系统的控制和破坏。

03 / 揭示非法控制技术路径

本案揭示的两类典型外挂手法，反映了游戏安全的两大风险：一是客户端环境易被模拟器改造并加载脚本，二是服务端与客户端交互缺乏完整性验证，存在被替换的可能。相关发现不仅推动案件办理，也为游戏厂商和监管部门提供了改进思路，可在协议校验、异常监测、防篡改设计等方面提升整体防护水平。

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。

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

盗版漫画案

自动化取证与图像比对，锁定盗版漫画 APP 海量侵权铁证

本案涉及一起针对移动应用程序提供盗版漫画内容的著作权侵权案件。涉案 App 被指控未经授权提供大量正版漫画作品，严重侵害了著作权人的合法权益。奇安信洞鉴通过编写自动化脚本模拟用户行为，触发 App 的内容缓存机制，并对缓存后生成的本地数据库和文件进行逆向分析，最终成功从数以万计的加密存储文件中，批量化地提取并重组了 514 部、数十万章节的漫画图片，并将其与权利方的正版漫画进行逐一比对，最终确认了数百部作品构成侵权，为委托方的维权行动提供了核心技术支持。

案件背景

在数字内容产业蓬勃发展的当下，著作权保护已成为平台和创作者的生命线。然而，猖獗的网络盗版行为正不断侵蚀这一生态，不仅严重损害原创者的合法权益，也对平台的商业运营、用户信任和品牌声誉构成实质威胁。某知名漫画平台近期发现，其大量原创漫画作品在某移动端 APP 中疑似遭到大规模未经授权转载。为应对此类复杂侵权行为，平台委托奇安信洞鉴开展司法鉴定，围绕相关图像内容开展数据固定与图像同一性比对工作。

洞鉴解决方案

01 应用获取与验证，夯实鉴定基础

鉴定人首先通过委托方提供的官方链接 成功下载了涉案 APP 的 Android 应用程序安装包。通过对文件的基础分析，明确了其应用名、包名、版本号、打包时间及数字签名等关键信息。这一步骤确保了后续所有操作均是针对该特定版本的官方应用展开，保证了证据的同一性。

02 制定自动化策略，实现海量内容缓存

考虑到涉案作品清单多达数百部，手动取证不具备可行性。鉴定人员决定采用自动化技术模拟真实用户操作。

1. **环境搭建：**将下载的 APP 安装至安卓模拟器，成功启动 APP，模拟真实用户操作环境。
2. **脚本开发：**编写定制化脚本，该脚本能够自动读取作品清单，在涉案 App 内执行搜索、打开漫画详情页、点击“缓存全部章节”等一系列操作。例如，针对某热门漫画作品，脚本自动遍历其全部章节内容，逐话触发缓存操作，大幅减少人工操作误差。
3. **批量执行：**通过循环执行脚本，对清单内的 500 余部漫画作品发起了批量缓存指令，使 App 主动将漫画图片文件下载并存储于模拟器的本地存储空间中。

03 破解缓存文件结构，批量还原漫画文件

考虑到涉案作品清单多达数百部，手动取证不具备可行性。鉴定人员决定采用自动化技术模拟真实用户操作。

1. **关联缓存内容与漫画作品：**通过数据库工具连接 APP 关联数据库，发现 11 个数据表，包括作品信息表（存储缓存漫画基本信息，记录作品名称、缓存路径等）、章节信息表（存储章节信息，记录章节序号等）、页面信息表（存储页面信息，记录页面序号、图片原始链接等），这些数据表共同构成了一个完整的索引系统，将用户缓存的漫画内容与本地存储的加密文件名进行关联。
2. **构建路径映射：**基于对数据库结构的理解，鉴定人员编写了一条 SQL 查询语句，将上述三个核心数据表进行关联查询，该查询成功导出了一份包含数十万条记录的 CSV 文件，文件清晰地列出了每个漫画的原始存储路径与“漫画名 \ 章节号 \ 页码 .webp”的新路径之间的对应关系。
3. **批量还原漫画文件：**随后，鉴定人员编写 Python 脚本，读取这份 CSV 映射文件。脚本根据文件中的对应关系，自动地将海量的、以哈希值命名的缓存图片文件进行复制、重命名，并按照“漫画 / 章节 / 页面”的结构存放到新的文件夹中。

经过上述处理，原本杂乱无章的缓存数据被成功还原为 514 部结构清晰、内容完整的漫画作品文件夹，直观地呈现了 App 内的侵权内容。

04 实施图像比对，锁定侵权证据

为最终确认侵权事实，鉴定人员将前序步骤中获取的涉案 App 图片与委托方提供的正版图片进行同一性鉴定。

1. **自动化比对：**鉴定人员编写脚本，根据双方提供的路径映射关系，对数百部漫画中的数百万张图片进行逐一重叠比对。
2. **结果分析：**通过对生成的重叠比对图进行分析，发现检材图片与样本图片在排除“水印”、“色彩”、“文字”等细微差异后，其核心画面内容、构图、线条等元素均高度一致，具有同一性。
3. **锁定铁证：**该比对结果有力地证明了涉案 App 中的内容来源于对委托方作品的盗版。

客户价值

01 / 突破技术壁垒，高效完成移动端取证

针对封闭式 APP、常规爬取手段失效的难题，奇安信洞鉴自主开发自动化脚本，实现页面自动化操作、缓存数据提取与数据库解析。在短时间内成功固定数百部漫画作品的缓存与章节数据，突破了移动端取证的技术瓶颈，为后续图像比对提供了完整可靠的证据基础。

02 / 精确量化证据，支撑司法认定与损失评估

版权类案件亟需明确侵权作品的范围与数量。本次鉴定清晰锁定了涉案作品的数量和同一性关系。量化结果不仅为权利人计算经济损失、提出赔偿主张提供了直接支撑，也为司法机关在定性、定责和量刑时提供了科学依据，避免了模糊判断。

03 / 打造标准流程，提升版权案件处理能力

在大规模图像比对环节，团队建立了完整的标准化流程：生成唯一标识、批量生成重叠比对图、引入辅助审核机制，并对水印、色彩、文字等差异进行排除。该流程确保了比对结果的技术准确性与法律可信度，也为后续类似版权侵权案件提供了可直接应用的技术路径。

电商店铺售假案

多端取证解析，揭示侵权商品交易的隐蔽链条

本案涉及一起利用网络店铺销售盗版手办模型，严重侵犯知识产权的案件。犯罪团伙通过线上渠道，规模化销售某知名动漫 IP 的仿冒产品，牟取非法利益。其作案手法隐蔽，人员分工明确，对市场秩序造成了恶劣影响。

奇安信洞鉴通过对海量数据的深度挖掘与关联分析，清晰还原了其从线上引流、社交媒体沟通到后台运营的全链条，将分散在多个设备中的碎片化信息整合为一条完整的、不可辩驳的证据链，为案件的成功侦破提供了关键技术支撑。

案件背景

近期，有消费者举报称，在某电商平台的一家“潮玩”店铺购买到了知名动漫 IP 手办模型，但产品质量低劣，疑似为假冒仿品。执法部门迅速介入，对涉案团伙采取行动，并查获了多名嫌疑人使用的智能手机、笔记本电脑及台式机硬盘等十余件电子设备。

为彻底查明该团伙的组织架构、运营模式和非法获利规模，办案单位委托奇安信洞鉴对这些核心电子物证进行司法鉴定。

洞鉴解决方案

1 多手机深度取证，确认店铺归属

鉴定团队对涉案的 5 部手机进行了全面取证与数据恢复，共提取逾千万条即时通讯记录，涵盖微信、QQ、钉钉等主流社交应用。在其中一部关键手机中，发现了昵称与涉案电商店铺名称完全一致的社交账号；在另一部主要嫌疑人张某使用的手机中，也检出多个包含店铺关键词的账号昵称。这些关键发现将虚拟的网络店铺与实际嫌疑人及其使用设备牢固关联，为案件定性奠定了证据基础。

2 跨平台数据关联，厘清团伙组织架构

进一步分析通信记录，发现微信记录超过 643 万条，QQ 记录超过 60 万条，钉钉记录超过 1.6 万条 。在这些数据中，大量对话涉及客户下单、售后处理、代理招募和内部指令，显示该团伙内部存在明确分工：

“老板” 负责总体决策与资金调配；

“客服” 负责客户沟通和交易撮合；

“代理” 通过 QQ、贴吧、小红书等平台拓展下线、推广销售。

通过跨账号、跨平台的数据整合，我们成功揭示了该团伙的组织架构和运作模式，为案件定性提供了关键支撑。

2 海量硬盘挖掘，固定后台经营证据

针对查获的多台电脑和容量高达数 TB 的硬盘，我们进行了地毯式文件挖掘，成功提取了海量经营文件：

图片文件超过 61 万个，其中包含大量侵权产品的宣传图、设计稿和实物照片。

各类文档与压缩文件超过 7.4 万个，为下一步筛选交易记录、客户名单和财务数据提供了海量的原始素材。

客户价值

01 / 锁定侵权主体

通过对涉案手机进行深度取证与账号比对，我们不仅发现了与店铺名称高度一致的微信、小红书、微博账号，还结合数百万条即时通讯记录，直接确认了嫌疑人与涉案电商店铺之间的联系。这一发现为执法机关锁定侵权主体、厘清责任链条提供了确凿证据。

02 / 揭示组织架构

通过跨平台、跨设备的数据整合，将分散在微信、QQ、钉钉等多种应用中的通信内容进行交叉验证，提炼出涉及客户下单、售后反馈、代理招募等关键信息。由此揭示了团伙“老板—客服—代理”的层级分工，以及“电商平台 + 社交矩阵”协同作案的模式。

03 / 维护市场秩序

本案通过电子数据司法鉴定，精准揭示侵权商品交易链条，帮助执法机关有效打击制假售假行为，维护了市场的公平竞争环境，为正版生产经营者争取了合法权益。

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。

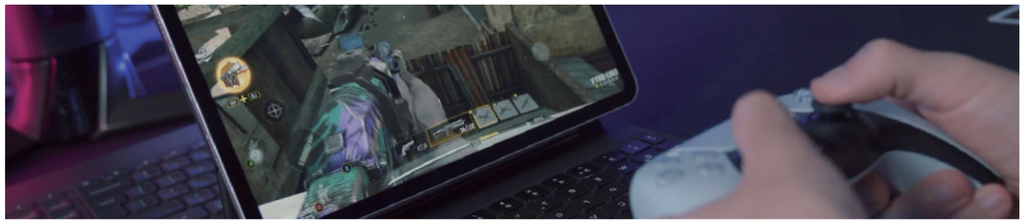
游戏私服案

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显著的相似性。

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 / 明确泄露范围

通过深入分析涉案服务器的远程服务和数据库，协助公安机关恢复了大量被盗的用户数据。此举清晰地揭示了黑客获取用户凭证的具体技术细节，为评估信息泄露的整体范围提供了关键依据。

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 / 厘清作案手法

通过对恶意程序的逆向工程分析，查明了犯罪团伙“利用二维码诱导扫码、截获登录凭证（Cookie/UID）、回传远程服务器”的完整攻击路径和作案手法，为公安机关厘清案件全貌、认定犯罪性质提供了核心情报。

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

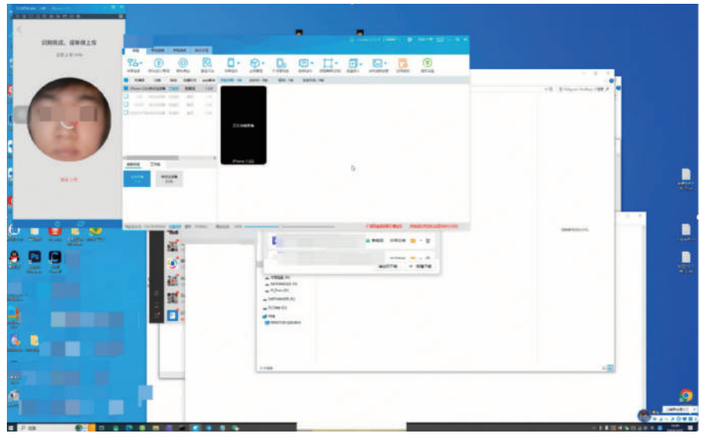
01 案中：协助现勘取证，全面还原 AI 换脸过程

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，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。

3. 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

虚假优惠引流案

深度剖析浏览器扩展程序，还原流量劫持与恶意推广完整链条

本案涉及国内某知名浏览器产品，通过在用户不知情的情况下自动安装一款“比价返利”类扩展程序，劫持用户访问某头部电商平台的正常流量，并将其导向含有特定推广信息的链接，以非法牟取佣金。奇安信洞鉴受委托，对该浏览器的相关功能进行电子数据司法鉴定。鉴定团队通过环境复现、进程监听、网络抓包与代码逆向分析等多种技术手段，成功还原了该扩展程序从静默安装到实施流量劫持、篡改页面、替换推广链接的全过程，为委托方提供了关键性的技术证据。

案件背景

2024 年，委托方发现其电商平台的部分推广佣金结算存在异常，怀疑有渠道商通过不正当技术手段骗取佣金。经过初步排查，线索指向了一款知名浏览器。初步排查发现，当用户使用该款浏览器访问其电商平台商品页面时，页面会被植入额外的优惠券模块；用户点击后，产生的购物行为会被计入非法的推广者名下，从而骗取平台的推广佣金。由于该扩展程序在浏览器的官方应用市场无法搜索到，且系浏览器自动安装，行为隐蔽，普通用户难以察觉。为厘清其技术原理并固定证据，委托方正式委托我所进行功能鉴定。

洞鉴解决方案

1 复现安装过程，锁定恶意扩展程序

鉴定人从浏览器官网下载了最新版本的安装包。在安装过程中，通过使用进程监控和网络抓包工具进行严密监视。发现在浏览器首次启动后极短时间内，会自动从特定服务器下载一个扩展程序（CRX 文件）并静默安装。该扩展程序在浏览器的扩展管理界面中被隐藏，普通用户难以发现和卸载。这一发现直接证实了该浏览器存在用户不知情的后台安装行为。

2 分析扩展程序工作流，揭示流量劫持核心逻辑

通过对扩展程序的源代码进行反混淆和格式化分析，鉴定人员揭示了其劫持流量、进行恶意推广的核心功能逻辑：

1. **用户行为监控与信息窃取：** 当用户访问某电商平台商品页面时，扩展程序会启动，并通过特定函数抓取网页中的商品信息、店铺 ID、用户名等关键数据，连同用户的 IP、UUID 等信息一并发送到远程服务器。

2. **页面篡改与诱导点击：** 远程服务器根据接收的数据，返回恶意脚本，扩展程序随即在电商页面中强行注入 “限时好券” “领券” 模块，这些模块外观与官方优惠界面高度相似，足以误导用户点击。

3. **多层跳转与推广链接替换：** 用户点击注入的“领券”按钮后，并不会直接跳转到某电商平台官方的优惠券页面，而是会经过多个第三方域名进行跳转，并最终将用户导向一个包含特定某返利平台 ID 的优惠券长链接。用户一旦通过该链接完成购买，推广佣金便会结算给这些预设的联盟账号。

2 追踪外部交互，固化完整证据链

鉴定人通过多次实验，完整记录了从浏览器安装、恶意扩展下载、用户数据被窃取、网页被篡改到最终跳转至带有特定联盟 ID 的推广页面的全过程。通过对网络抓包结果的分析，成功提取了所有相关的 URL 链接、请求与响应数据、以及多个用于非法推广的京东联盟 ID。这些发现证明，该浏览器并非一个单纯的上网工具，而是一个精心设计的、能够与外部服务器联动，系统性实施流量劫持并牟利的平台。

客户价值

01 / 揭示隐蔽作案手法

本次鉴定不仅证实了该浏览器的静默安装行为，更揭示了其利用扩展程序、通过 IP 识别、远程服务器控制、多层跳转等复杂手段，系统性地实施流量劫持的完整技术细节。

02 / 减少潜在经济损失减少潜在经济损失

清晰地将浏览器软件的后台行为、扩展程序的代码逻辑、远程服务器的指令下发、以及最终用于非法牟利的推广联盟 ID 关联起来，为委托方主张权利提供了强有力的法律证据。

03 / 警示行业风险

本次鉴定不仅解决了单一客户的维权诉求，更揭示了浏览器作为互联网入口，可能被滥用于实施大规模流量劫持的行业风险。这为监管机构和广大用户敲响了警钟，对于规范浏览器市场竞争、保护用户知情权和选择权具有重要的参考意义。

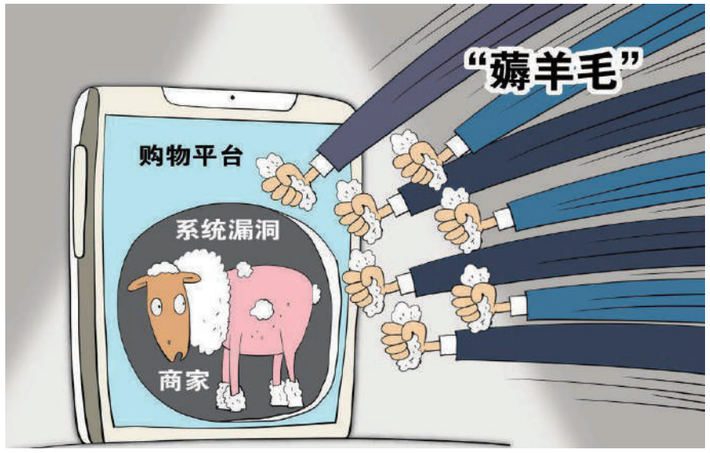
优惠券盗领案

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

1 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。

2 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。

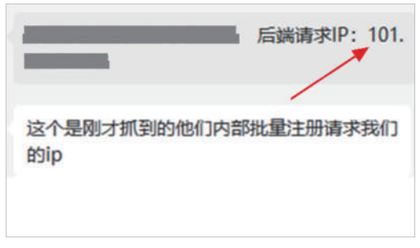
案件背景

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。

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。

CHAPTER 4

企业内控合规治理

近年来，随着科技与经济的高速发展，企业内控与合规治理的复杂性和重要性日益凸显。企业规模的扩大和业务的多元化使得内部管理的薄弱环节和合规风险不断显现，成为制约企业可持续发展的关键因素。内部威胁如数据泄露、商业秘密被窃取、贪腐舞弊等问题频发，不仅带来巨大的经济损失，还严重损害企业声誉和市场竞争力。

据统计，2023 年，检察机关充分履行反腐败检察职责，受理各级监委移送职务犯罪 2 万人，同比上升 9.3%【1】。这反映了国家对反腐败斗争的高度重视和不断加大的打击力度。与此同时，互联网行业作为数字经济的先锋，其内部反腐力度也显著加强。例如，网易、微博、字节跳动、腾讯、美团等大型互联网企业在近年来查处了大量贪腐舞弊案件，数百名员工被开除或移送司法机关处理。这些案例不仅展示了企业在内控与合规治理中的严峻挑战，也凸显了反腐败斗争的迫切性和重要性。

作为电子数据司法鉴定机构，我们在企业内控与合规治理中发挥着关键作用。通过电子数据取证与鉴定，我们帮助企业发现内部威胁、追踪贪腐行为、保护商业秘密，确保企业合规运营。电子数据司法鉴定不仅提升了企业的风控能力，也为维护市场秩序和企业声誉提供了有力保障。

本章节将深入探讨企业内控与合规治理的背景与重要性，分析企业调查中的常见场景，如商业秘密泄露、贪腐舞弊等，并介绍电子数据取证鉴定的基本思路和方法。通过系统的理论阐述和丰富的实际案例分析，旨在为企业提供全面的内控与合规治理解决方案，帮助企业在复杂的经营环境中稳健前行，实现长远发展。

【1】中央纪委国家监委网站 . (2024 年 3 月 9 日). 十四届全国人大二次会议报告公布惩治职务犯罪数据 . 访问链接：https://www.ccdi.gov.cn/yaowenn/202403/t20240309_333184.html

01

TRADE SECRET LEAKAGE AND DESTRUCTION

商业秘密泄露与破坏

商业秘密泄露与破坏是指企业内部或关联方违反保密义务，未经授权非法获取、使用、披露或故意销毁企业未公开且具有商业价值的信息的行为。这些信息包括但不限于研发成果、生产工艺、客户资源、市场策略等，且须满足不为公众所知悉、具有经济价值且经企业采取合理保密措施的法定条件。在企业内控与合规治理中，商业秘密泄露与破坏主要源于内部人员滥用权限、数据管理不善或第三方合作中的安全漏洞，可能导致企业核心竞争力受损、经济利益流失及法律合规风险增加。

1. 范围

技术信息

如配方、设计图纸、软件代码、研发数据等。

经营信息

如客户名单、供应商资料、市场营销策略、财务报表等。

管理信息

如内部管理制度、人力资源政策、培训资料等。

2. 手段

泄密手段

数字化手段

通过邮件附件、网盘共享、即时通讯工具（如微信、钉钉）等形式泄密。

物理介质

使用 U 盘、移动硬盘、打印纸质文件等方式拷贝敏感数据。

分段式泄密

利用“蚂蚁搬家”手法，将敏感数据分批次、多次传输以降低被发现的风险。

加密与隐写

通过加密文档、文件伪装（如图片内嵌数据）、文件压缩分包等方式隐藏泄密行为。

证据销毁手段

数据擦除

使用专门的数据擦除工具（如 Eraser、BleachBit）销毁关键文件。

文件加密

使用强加密算法（如 AES-256）对文件加密，增加取证难度。

日志篡改

人为删除或伪造系统访问日志，干扰泄密行为还原。

3. 常见场景

员工主动泄密与破坏

员工主动泄密与破坏是指员工因个人利益驱使、竞争报复、情感纠纷等动机，故意将企业的核心数据、商业计划、客户名单等敏感信息通过各种手段泄露或破坏。这类行为具有主观恶意，通常目的明确，直接损害企业的商业利益和数据完整性。

典型情境 1
TYPICAL SCENARIO

员工主动泄密与破坏

员工跳槽至竞争对手企业后，主动泄露原企业的客户资源、价格策略或关键技术文档，同时可能故意删除或篡改相关文件，打击原企业的市场竞争力。

典型情境 2
TYPICAL SCENARIO

恶意泄露与破坏

员工因薪资、晋升等矛盾，故意将内部经营计划、财务数据等敏感信息外泄，同时故意删除或破坏关键数据，以打击原企业或寻求报复。

典型情境 3
TYPICAL SCENARIO

数据贩卖与破坏

员工利用职务便利，私自拷贝企业的专利技术、源代码或市场数据，向竞争对手或其他第三方出售牟利，并可能故意删除这些数据以掩盖泄露行为。

员工被动泄密与破坏

员工被动泄密与破坏是指员工因缺乏数据安全意识、操作不当或疏忽大意，导致企业的重要数据被外部人员或竞争对手获取，或数据被意外删除或损坏。这类泄密和破坏往往发生在无意之中，但其影响同样严重，可能涉及客户资料、技术方案、商业计划等敏感信息。

典型情境 1
TYPICAL SCENARIO

社交媒体泄密

员工在社交平台分享工作内容、会议照片或涉及企业技术的图片，可能无意中泄露研发进度、技术细节或战略规划。

典型情境 2
TYPICAL SCENARIO

数据传输不规范

员工通过未加密的邮件、网盘或即时通讯工具传输敏感数据，导致数据被第三方截取或恶意使用。

典型情境 3
TYPICAL SCENARIO

设备丢失与数据毁坏

员工未妥善管理存储敏感数据的设备（如笔记本电脑、移动硬盘），导致设备丢失或被盗，敏感数据被非法获取或被恶意篡改。

第三方合作与外包风险

第三方合作与外包风险是指企业在与外部供应商、外包团队或合作伙伴共享数据时，由于合同不完善、缺乏有效的安全防护措施或第三方管理疏漏，导致商业秘密被不当使用或泄露的风险。

典型情境 1
TYPICAL SCENARIO

人员流动管理不善

合作方存在频繁的人员流动或交接不规范，前员工或未经授权的人员仍能访问共享数据，甚至将敏感信息带离企业。

典型情境 2
TYPICAL SCENARIO

权限管理不当

企业在与外包方共享项目文件或客户数据时，未对数据访问权限进行严格限制，导致非必要人员可接触敏感数据，甚至擅自保存或传播。

4. 取证鉴定思路

商业秘密泄露案件通常具有隐蔽性高、手段多样、取证难度大的特点，泄密途径可能涉及企业内部主动泄露、员工无意泄密或第三方合作方管理不善等多种情形。在商业秘密泄露案件的调查与司法鉴定过程中，电子数据司法鉴定人员需严格遵循合法合规的原则，通过专业的取证手段，从数据存储、访问记录、泄露路径等多维度入手，全面还原泄密过程，形成完整、可验证的证据链条，为司法机关的案件审理与企业合规治理提供坚实的数据支撑。

以下为商业秘密泄露案件的取证鉴定思路：

1 明确取证目标与重点

在开展取证工作前，应当结合企业内部调查或执法机关委托所提供的线索，明确本案商业秘密泄露的核心要点：

泄密途径

- 是否通过电子邮件、即时通讯工具、云端存储或物理介质（U 盘、移动硬盘）等方式泄露。
- 泄密行为是否涉及多次重复或分段式传输。

涉案人员与角色

- 识别直接或间接参与泄密的员工、合作方、外包方等主体。
- 区分主动泄密与被动泄密的行为特征，结合企业权限管理制度梳理嫌疑对象可能的访问路径和操作权限。

商业秘密的范围与价值

- 被泄露的商业秘密是技术文档、核心代码、客户名单、供应链信息、财务数据，还是其他敏感信息。
- 确定其对企业竞争力、市场地位或业务发展的具体影响程度，以便后续定损和法律定性。

通过上述目标的确认，取证团队能够在后续工作中有针对性地收集与分析数据。

2 确定涉案数据来源

结合前期调查和企业内部信息安全管理制度，对可能保存涉案信息或操作记录的地方进行锁定与排查，常见的数据来源包括：

服务器与终端设备

- 企业内部文件服务器、代码仓库、数据库服务器以及相关日志（访问日志、操作日志、备份日志等）。
- 涉案员工使用的台式机、笔记本电脑或移动终端（手机、平板）的存储数据。

云端存储与协作平台

- 企业常用的云盘、远程协作工具（如企业微信、Slack、Teams 等）以及第三方云存储平台（个人云盘、共享云盘）。
- 若企业部署了 CASB（云访问安全代理），可调取访问记录及关键数据操作审计日志。

社交媒体与通讯工具

- 邮箱（企业邮箱、私人邮箱）、聊天工具（QQ、微信、钉钉、Skype、Telegram 等）聊天记录与传输文件历史。
- 员工在社交媒体上发布的潜在涉密内容（微博、知乎、Twitter、Facebook 等）。

物理介质与打印日志

- 外接存储设备（U 盘、移动硬盘、光盘）接入记录。
- 打印机使用日志、复印机扫描日志，以防止通过纸质文档进行泄密。

3 数据采集与证据固定

在符合法律法规与取证技术标准的前提下，对涉案数据信息进行提取与固定，确保证据的客观性与可验证性：

现场取证

- 第一时间对涉案电脑进行只读模式的数字镜像，确保原始数据不被篡改；同时，使用专业取证工具对涉案手机进行数据提取，并生成 SHA256 或 MD5 哈希值，以保证数据的完整性和可验证性。
- 对企业服务器或云端资源进行现场提取或远程镜像，使用专业取证工具对关键日志及文件进行拷贝。

日志审计与备份确认

- 获取并封存系统、网络、数据库访问日志以及敏感操作记录，对其进行哈希值计算并存档，以防后续审计阶段出现篡改。
- 若企业已有定期备份计划，应查阅并封存备份介质或版本库，以追溯过往版本中可能的泄密痕迹。

软硬件环境控制

- 针对涉案硬盘、U 盘或其他物理介质，需尽量避免再次通电或写入，优先使用专业取证工作站进行只读提取，保留其初始状态的哈希值。

4 数据分析

对已提取的数据进行整理、筛选与深层次分析，去除无效信息或噪声数据，从而聚焦与商业秘密泄露相关的核心线索：

内容检索

- 使用全文搜索、关键词匹配或自然语言处理技术对海量文件进行快速检索（如搜索“源代码”“商业秘密”“招投标报价”等），定位潜在涉密内容。
- 对聊天记录或邮件内容进行主题聚类与语义关联分析，查找泄密动机、交易议价、文件传输等直接证据。

多维度关联与时序分析

- 将人员关系、文件访问历史、传输方式、操作时间等数据多维度整合，形成可视化的泄密路径或时间线。
- 识别异常操作点，如工作时间以外的大容量文件传输、离职前后高频访问关键文档等，判断行为与数据泄露的因果关系。

5 案件还原与关键节点确认

基于前期的关联分析，重点复原泄密过程与关键环节，明确涉案人员的行为动机、时间节点与泄露范围：

行为过程还原

基于收集到的系统日志、文件访问记录及通讯数据，复原从“数据接触—传输—泄露”的完整流程。

- **数据接触：**识别首次访问涉密文件的时间及访问权限。
- **数据拷贝：**确认数据是否被批量下载、拷贝至外接设备或云端存储。
- **数据传输：**识别数据是否通过邮件、即时通讯工具或外部存储泄露。

关键行为节点确认

在泄密行为中识别异常时间节点及关键操作记录。

- **异常访问记录：**短时间内集中访问大量敏感文件。
- **非工作时间操作：**如深夜登录系统或离职前夕的频繁数据访问。

泄密范围确认

全面评估泄密事件的严重性及其对企业造成的实际损害。

- **泄露数据内容：**识别泄露数据的类型，如技术文档、源代码、客户名单、财务数据、市场策略等。
- **泄露数据量与完整性：**确认泄露的数据量、涉及文件数量及数据集完整性。

6 鉴定意见书编撰

将取证全过程及关键结论汇编成鉴定意见书或专业报告，为司法机关或企业内部处理提供关键证据。

- **数据分析结果：**列举关键发现（聊天记录、文档传输路径、权限访问日志等），并结合图表或时间线进行说明。
- **结论与建议：**对泄密模式、行为责任人、涉密文件性质做出明确结论，并提出安全防护或合规建议。

5. 典型案例

员工系列违规案

“爆房”之后：一场跨度五年的内部犯罪浮出水面

2023 年，某知名酒店集团遭遇一宗时间跨度长达五年的内部不当行为与技术犯罪案件。涉事人员借助职务之便，精密策划并通过多重手段，长期非法获取并利用公司的关键商业资源与数据。在面对这一错综复杂的案件，奇安信洞鉴应邀介入，成功应对了数据恢复、线索追溯和复杂代码审查等众多技术难题，为锁定犯罪金额、确立事实真相以及法庭的后续裁决提供了坚实的证据支撑。

案件背景

2023 年年初，某知名酒店集团的预定系统遭受精心策划的恶意攻击，导致多家门店的客房状态陷入混乱，造成数十万元经济损失。经警方深入追踪，揭露了集团内部部分员工的不正当行为。这些员工从 2018 年起，利用技术手段操纵、破坏公司计算机系统，窃取客户数据和公司的核心专利信息，并通过非法手段创建大额优惠券和调整积分等级，给公司带来巨大经济损失。但在接下来的侦查中，警方遇到了几大技术挑战：

1. **犯罪手段复杂：**涉案员工采用了数据库修改、代码重写、脚本插入等多种技术策略；
2. **数据处理困难：**涉及数据库数据量极大，需要对亿级数据进行固定，手动操作费时费力；
3. **真实环境复现：**受限于时间因素，调查团队需在正式环境中复现破坏性脚本的影响。

洞鉴解决方案

1. 攻击重现：后台系统遭受技术攻击的深度解析

此案中，涉案人员通过编写 SQL 语句对酒店的预订系统实施了技术攻击，导致了酒店门店的房间预定数据出现严重偏差。为了解此次技术攻击的实质，鉴定人展开了一系列的深入分析与实验验证：

- **代码透视：**鉴定人对涉案的 SQL 代码进行了细致的解读，确认其主要功能是对指定的分店房间数据进行查询并对特定的房间数量进行随机的增减操作。
- **功能复现：**为确保理论分析与实际效果一致，鉴定人首先获取了指定分店的原始房间数据，接着执行了涉案 SQL 语句，并对比执行前后的数据变化，确认了房间数量确实被更改。
- **实战模拟：**鉴定人进一步在真实环境中模拟攻击场景，首先确认了某分店的“特惠双床房”为不可预订状态。接下来，执行涉案 SQL 语句后，该房型状态转为可预订，并成功进行了房间预定操作。

经过一系列严格的技术验证，鉴定人成功揭示了涉案 SQL 语句的潜在影响，即通过技术手段影响酒店房间的实时预订状态。

2. 透视窃取：会员数据泄露事件的精准核查

此案中，涉案人员盗取了酒店集团的会员信息，并利用这些数据与酒店集团进行市场竞争。鉴定人对该酒店集团的会员信息进行了固定，并将其与嫌疑人电脑中的数据进行比对。

- **数据固定：**酒店集团的数据库中包含的全量数据超过一亿条，鉴定人编写脚本高效固定，确保数据的完整性和准确性；
- **数据处理：**鉴定人编写脚本，对涉嫌数据库和酒店集团的全量会员数据进行筛选，有效排除了空数据和重复数据；
- **相似性比对：**通过对比涉案数据与全量数据，发现其中有近 500 万条数据完全相同，进一步计算表明，涉嫌人员的数据与酒店集团的数据相似度高达 99%。

此次相似度分析，揭示了涉案人员非法窃取会员数据的行为，为法庭提供了有力证据。

3. 代码比对：深度揭秘非法售卖专利事件

此案中，涉案人员非法获取并销售了酒店集团的酒店管理系统源代码数据，这套系统是酒店集团的核心专利技术。为揭示真相，鉴定人对相关文件代码进行了相似性比对。

- **文件哈希值比对：**利用先进的哈希算法，鉴定团队对比了涉案人员电脑中的文件与 U 盘中的文件，结果显示二者哈希值完全匹配。结合金融流水记录，辅助证明涉案人员通过售卖该专利非法获利。
- **源代码筛查：**鉴定人提取了涉案的 12 个关键项目代码，编写专门脚本，对文件类型如“.java”、“.jsp”等进行精准筛选，并与酒店集团提供的原始代码进行对比，筛选出相对路径和文件名称完全一致的文件。
- **源代码比对：**经过 16 进制比对与计算，确认了涉案文件与原始文件的高度相似性。

经过上述严格的鉴定过程，我们成功地对比了检材与样本的文件内容，得到了详细的对比结果，证明了非法销售的代码与酒店集团的专利代码高度相似。

4. 损失核算：大额异常优惠券统计分析

此案中，涉案人员秘密地发布并在多个销售渠道中销售大额优惠券，从中非法获得巨大利益。为确切地计算此非法行为对酒店集团带来的经济损失，鉴定人进行了细致的数据统计与分析。

- **数据整合与筛选：**鉴定人对涉案优惠券的金额和数量进行了细致筛查，专家分别提取了面值为 100 和 200 的优惠券数据，并确保在“券号”列中没有重复数据。
- **损失核算分析：**通过对优惠券的数量进行加总，鉴定人计算得到了各面额优惠券的总数，辅助证明异常优惠券给酒店集团带来的实际经济损失。

客户价值

01 / 增强侦查效率

本次事件涉及多重技术手段，如数据库修改、脚本插入等。通过对这些手段的深入鉴定和解析，警方能更快速地理解犯罪过程，为针对涉案人员的侦查工作提供明确方向。

02 / 保护公民隐私

涉案人员窃取了大量酒店会员的私人信息，这对公民的隐私安全构成了严重威胁。通过对这次事件的迅速介入和处理，酒店集团和警方共同确保了被盗信息的封堵，并加强了信息安全措施，进一步保护了广大消费者的隐私和权益。

03 / 提供坚实证据

深入的代码比对和数据分析为酒店集团提供了明确的技术证据，证明了涉案人员的不法行为。这些技术分析结果为法庭提供了关键的支撑，确保法律程序的公正和准确性。

核心代码外泄案

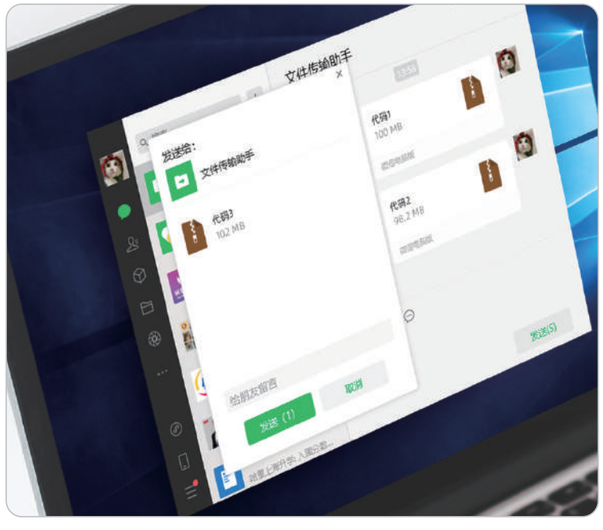
硬盘数据复原 + 操作行为解析，助力企业维权有力落地

某企业在处理一起信息泄露与劳动争议案件时，发现一名员工可能利用公司配发的办公电脑，通过微信外发了包含核心代码的敏感文件。企业内部监控系统记录了该员工的登录行为及相关操作痕迹，为进一步确认该行为的真实性及链条完整性，企业委托我们对涉事电脑进行电子数据司法鉴定。通过对硬盘数据的恢复和分析，成功提取了关键代码文件，并恢复出微信账号登录后所产生的相关文件，佐证了员工曾经在公司的办公电脑上登录过微信的行为，为企业维权及后续仲裁提供了强有力的技术支撑。

案件背景

2024 年，某企业研发部门的一名员工在即将离职前，使用办公电脑登录微信，外发包含公司核心代码的敏感文件，随后将微信卸载并删除微信相关文件夹，试图掩盖痕迹。企业通过内部监控系统察觉该行为后，立刻冻结了员工的办公设备，同时对其离职流程提出异议，要求员工对此行为进行解释。

但由于该员工否认文件外发，公司仅凭初步的监控记录难以支撑仲裁需求。为此，公司决定委托奇安信洞鉴对涉事电脑进行专业的电子数据恢复与分析，确认关键代码的外发行为及相关技术细节，从而完善仲裁及潜在法律诉讼中的证据链。



洞鉴解决方案

硬盘数据恢复

使用专业的取证工具对硬盘进行数据恢复后，根据委托方提供的线索，对微信账户“w**1”及其相关文件记录进行全面搜索，成功恢复并提取到与“w**1”相关的两条文件夹记录，相关文件夹虽已删除，部分数据被覆盖，但仍保留了文件路径、创建时间、修改时间及最后访问时间等关键信息。此外，通过资源管理器痕迹分析，发现了 41 条与该微信账户相关的操作记录。

文件搜索与还原

根据委托方提供的线索，我们对三个敏感文件进行了重点检索与分析，成功找到与这些文件相关的创建、修改和访问记录，并发现部分文件的快捷方式记录。将三个压缩包文件导出后查看其内容，确认文件中包含与公司核心代码相关的信息。

用户操作环境与行为分析

通过对检材笔记本的系统用户登录记录进行分析，发现该电脑在特定时间段内的唯一登录用户为“****.g”，其登录时间与公司内部监控记录完全吻合。用户操作行为分析将电脑实际使用者与敏感操作行为关联，为构建完整的人证、物证链条提供了有力的技术支撑。

客户价值

01 / 缩短案件周期

从案件受理到鉴定完成，我们在短时间内完成了数据恢复、分析、导出和证据固定的全流程操作。以高效的响应速度帮助委托方迅速获得关键证据，缩短了案件处理周期，降低了由时间拖延导致的管理和法律成本。

02 / 证据链条完整

成功恢复并提取了硬盘中的微信登录痕迹，清晰还原了员工使用办公电脑外发公司核心代码的完整行为链条。这些鉴定结果为委托方提供了明确且具法律效力的证据支撑，大幅提升了案件仲裁和诉讼的胜诉几率。

03 / 强化内部防控

通过本次案件，客户不仅解决了当下纠纷，还借此机会识别了公司数据安全管理中的薄弱环节，为后续优化数据管理与权限控制提供了方向，进一步降低未来数据泄露和敏感信息外发的风险。

员工离职泄密案

数据泄露真相还原：从硬盘到云端的精准追踪

某制造业公司在季度审计时发现，一名已离职的研发人员在职期间可能通过云存储、邮件及社交工具外泄技术资料，涉及公司核心产品的生产流程及客户清单。这些信息一旦泄露，不仅会对企业竞争力造成严重影响，还可能构成商业秘密泄露的法律问题。为此，公司委托奇安信洞鉴对涉案人员的工作设备进行全面的司法鉴定，最终明确了数据泄露的时间、途径及操作细节，为后续法律诉讼提供了重要支持。

案件背景

某公司是一家专注于技术研发的制造企业，因其产品的技术壁垒高而在行业内占据领先地位。2024 年初，公司发现有竞争对手的产品在短时间内推出了与其核心技术高度相似的解决方案，市场反馈与公司产品类似。这一异常引起了高层的高度警觉，随即展开内部审计。

审计结果显示：

- 一名前研发人员在离职前频繁使用外接存储设备，且相关设备的插拔时间集中在非工作时段；
- 离职前 3 个月，该人员使用企业邮箱转发多封与技术文件相关的邮件至个人邮箱；
- 离职后一段时间，公司服务器检测到与其关联的云存储平台有频繁的文件上传记录。

基于此，公司正式委托奇安信洞鉴开展司法鉴定，以厘清事实。

洞鉴解决方案

数据提取与镜像制作

对涉案笔记本电脑硬盘进行镜像制作，生成 E01 格式的镜像文件，并通过 SHA256 校验值验证数据完整性。随后，提取并分析硬盘中的多种数据，包括电子邮件记录、USB 设备使用痕迹、上网历史、微信记录及云存储缓存文件等，确保全面覆盖所有可能涉及的数据类型。

电子邮件分析

依据委托方提供的关键词（如“项目报告”“保密技术文档”），在涉案邮箱中进行精准检索，提取相关邮件和附件。分析发现，存在多封敏感文件被转发至个人邮箱的记录，附件内容涉及公司研发项目的实验报告等核心资料。

外接存储设备溯源

提取硬盘中的 USB 设备插拔记录，分析其插拔时间及挂载盘符，发现外接存储设备在涉案期间多次使用，每次使用时长显著，操作频繁集中于公司技术文件目录。

微信记录恢复

利用 WxDatViewer 对微信缓存数据进行解密，成功提取 7000 余条聊天记录。分析显示，其中包含与外部人员讨论公司技术细节的聊天内容，以及与经济回报相关的对话，为案件提供了关键补充证据。

客户价值

01 / 精准还原数据泄露过程

通过全面提取和分析电子邮件、云存储操作记录、外接存储设备使用痕迹及微信聊天记录，我们精准还原了数据泄露的全过程，明确了敏感信息的流转路径和涉案人员的行为。

02 / 保障证据的法律效力

鉴定过程中，我们严格按照司法规范操作，确保证据的完整性和不可篡改性，为客户在法律诉讼中的责任追究和权益保护奠定了坚实基础。

03 / 守护核心商业利益

通过明确数据泄露的时间、范围及影响，我们帮助客户及时采取法律和管理措施，避免核心技术和商业信息的进一步扩散，为客户维护市场竞争力和品牌声誉提供了坚实保障。

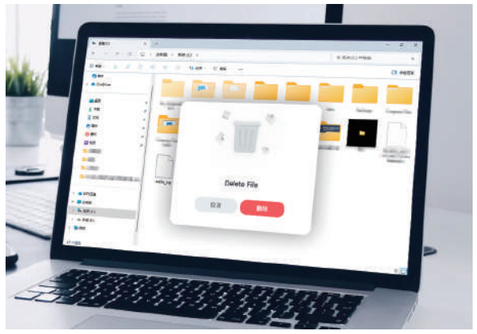
数据恶意删除案

揭秘离职员工数据删除行为，为客户赢得证据优势

某知名药物研发企业怀疑，前员工张某在离职前故意删除了大量关键工作文件，这些文件包含了公司的核心研发成果，但确定文件的删除时间存在困难。为了追回损失并维护合法权益，奇安信洞鉴受委托，通过对涉案电脑设备使用痕迹、文件系统日志审查分析，成功验证了删除行为及其时间的客观存在性，为企业维权提供了坚实的证据支持。

案件背景

该企业是一家致力于创新药物研发的高新技术企业，发现其一名前员工在离职前删除了大量含有研究数据和内部信息的工作文件，这些资料的丢失对公司的科研项目构成了严重威胁。为了追回损失并防止类似事件再次发生，公司决定采取法律手段保护自己的合法权益。然而，由于电子数据的特殊性和复杂性，公司需要提供确凿的证据来证明文件是在特定时间内被故意删除的，这就需要专业的电子数据鉴定来揭示真相。



洞鉴解决方案

为了确证前员工删除工作文件的行为及其具体时间，奇安信洞鉴采取了一系列专业措施，对涉案电脑的操作系统和文件系统日志进行了全面审查与分析。这一过程包括：

系统活动追踪

首先对涉案电脑的操作系统日志进行了详尽分析，包括系统启动、关机时间记录，以及 USB 设备的连接和使用情况，这些数据为确定文件删除行为的确切时间和可能的操作者提供了重要线索。

文件系统日志的提取

对 NTFS 文件系统日志进行了提取，这些日志记录了 Windows 系统中文件系统变更的详细历史信息。NTFS 文件系统的日志无法直接进行篡改，能够确保分析结果客观真实。

EventTime	Event	Detail	FileName
2020-08-17 18:16:15	File Deletion		Bi[redacted]018.xlsx
2020-08-17 18:16:15	File Deletion		Bi[redacted]8.1.28.xlsx
2020-08-17 18:16:15	File Deletion		Bi[redacted]8.2.11.xlsx
2020-08-17 18:16:16	File Deletion		Bi[redacted]018.xlsx
2020-08-17 18:16:16	File Deletion		M[redacted].xlsx
2020-08-17 18:16:16	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:16	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:16	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]0.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted].xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]0.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]0.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted].xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]9.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]8.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]
2020-08-17 18:16:17	File Deletion		M[redacted].xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]18.xlsx
2020-08-17 18:16:17	Directory Deletion		解[redacted]
2020-08-17 18:16:17	File Deletion		M[redacted]sx
2020-08-17 18:16:17	File Deletion		M[redacted]）.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]2）.xlsx
2020-08-17 18:16:17	File Deletion		M[redacted]3-30）.xlsx

关键事件记录筛选分析

在提取的 NTFS 文件系统日志中，筛选出所有标记为“File Deletion”（文件删除）或“Directory Deletion”（目录删除）的事件记录，通过分析这些记录，我们能够追踪到文件被删除的具体实例。

时间线对比与证据关联

进一步将删除事件的时间线与员工的离职时间进行对比，发现关键文件的删除时间与离职时间段存在重合，是直接证明文件删除行为的关键。

客户价值

01 / 解决自证难题

此案件中，被告方质疑公司可能修改了系统时间，试图将文件删除的时间与其离职时间脱钩，企业陷入自证困境。奇安信洞鉴帮助客户转变思路，将焦点从难以证明的时间篡改转移到文件删除行为及其时间的客观存在性，为客户在法律诉讼中提供了清晰的方向。

02 / 维护商业利益

通过专业的技术手段，如分析 NTFS 文件系统日志，确立了文件删除事件及其时间的不可篡改性，为客户提供了无可争议的证据，为客户提供在法律诉讼中具有决定性的证据支持，帮助客户维护其商业秘密和知识产权。

03 / 揭示潜在漏洞

通过详细的案件分析和后续的咨询服务，我们不仅帮助企业解决了当前的法律问题，还提供了针对性的改进建议，包括加强内部管理和数据安全措施，降低了企业未来面临类似事件的风险。

02

CORRUPTION AND MALPRACTICE

贪腐舞弊

贪腐舞弊是指组织内部人员或相关方利用职务便利，通过操控业务流程、篡改数据或隐匿信息等方式，获取非法或不正当利益的行为。这类行为通常涉及滥用权力、资源挪用或利益输送，具有高度隐蔽性和复杂性，对组织的运营效率、财务健康以及法律合规构成严重威胁。

在数字化时代，贪腐舞弊的形式更加多样化和技术化，如利用权限操控内部数据、通过虚假交易掩盖资金流向、或篡改电子记录以隐匿舞弊痕迹。这些行为不仅增加了识别和侦查的难度，还对传统管理和审计手段提出了更高的要求。

1. 常见场景

利益输送

企业员工或管理人员通过滥用职权，以金钱、礼品、回扣或其他利益为交换条件，谋取个人或第三方不正当利益，包括但不限于以下形式：

对外收受回扣： 员工在与外部单位（如供应商、代理商、客户等）合作时，为对方谋取利益而接受金钱、礼品或其他形式的回扣。

对内行贿： 企业内部不同部门或员工之间，通过提供金钱或其他利益，换取资源、职位或其他特权。

以权谋私： 员工通过职权便利，为亲属、朋友或关联方提供利益，如放宽审批标准、优先分配资源等。

职务侵占

企业员工或管理人员利用职务便利，将公司现有资金或资源非法占为己有，包括但不限于以下形式：

非法挪用资金： 员工擅自将公司资金用于个人投资、非公司项目或不明用途。

关联交易非法获利： 将资金或资源通过不正当交易方式转移至关联方，并从中获取个人利益。

非法占有资产： 私自挪用或转移公司物资、设备等，归个人使用或销售获利。

财务造假

企业员工或管理人员通过伪造财务记录、虚构交易等手段歪曲公司财务状况，以达到掩盖舞弊、谋取私利或其他不正当目的的行为，包括但不限于以下形式：

虚构合同与项目： 员工与外部合作方合谋，伪造不存在的合同或项目，套取公司资金。

篡改财务数据： 隐瞒公司负债、夸大收入或调整利润指标，制造虚假财务报表。

虚假报销与费用申报： 捏造费用或伪造发票，从公司套取资金。

采购与供应链舞弊

企业员工在采购、供应链管理中，与外部合作方合谋或滥用职权，损害公司利益的行为，包括但不限于以下形式：

串通舞弊： 内部员工与供应商合谋，通过围标、抬高价格、虚报工程量等手段侵害公司利益。

违规业务往来： 员工与供应商建立利益链条，通过回扣、利润分成或股权合作换取不正当业务优势。

人事制度舞弊

企业员工或人事管理人员在招聘、考勤等环节滥用职权或弄虚作假，以获取不正当利益的行为，包括但不限于以下形式：

招聘舞弊：人力资源或相关招聘管理人员利用职位便利，获取不当利益，或与“掮客”勾结在招聘过程中套取费用等。这包括向应聘者或人力外包公司收取介绍费，或为关系户提供职位，确保其顺利入职。

考勤舞弊：通过虚增出勤记录、加班时间等手段，骗取工资或补贴。这包括篡改考勤数据，虚报员工出勤情况，或虚报加班时间，获取超额工资或补贴。

2. 证据来源及形式

聚焦“人 - 财 - 物 - 信息”四大维度

人：涉案人员在公司的地位、职责范围、与外部的关系网；其访问权限、历史行为习惯。

财：资金流动与支付行为是否异常，包括虚增、虚列费用、贿赂回扣等。

物：物理介质、关键设备、出入记录等。

信息：内部系统数据（ERP、OA、邮箱、即时通讯工具）与外部通信记录（私人邮箱、社交软件）。

重点系统与设备

财务系统（ERP/ 会计软件）

可能藏有异常报销、虚假发票、合同变更、支付审核等。

邮件与通讯工具

邮箱、微信、钉钉、企业 IM 等存储的聊天记录、语音、文件传输信息。

服务器与网络日志

包括 VPN、堡垒机、数据库、网络监控系统；用于确认访问时间、操作来源 IP、权限使用情况。

员工电脑与存储介质

涉案员工工作电脑、U 盘、移动硬盘、云盘账户等，重点关注加密文件、删除文件的恢复。

打印机、复印机、考勤机、门禁记录

多方位佐证行为轨迹，如打印或复印的敏感合同、文件领取时间、员工出入时间是否存在异常。

3. 取证鉴定思路

贪腐舞弊案件的取证鉴定必须针对案件隐蔽性、复杂利益链条、多样化主体等特点，结合现代信息技术手段，重点构建合法合规、系统化、多维度的取证路径，以确保证据链条完整并具备司法认可度。

以下是贪腐舞弊案件的取证鉴定思路：

1 明确取证目标与重点

了解案件背景：在接受委托或启动调查前，需与企业管理层、法务及合规部门充分沟通，明确已掌握的舞弊线索、涉案人员身份、潜在的舞弊手段及资金流向等。

制定取证方案：根据舞弊行为可能涉及的系统（ERP、财务软件、邮箱、文档协同等），以及涉案人员的岗位、权限和操作习惯，拟定针对性的取证目标和优先级，列出需采集的数字设备清单（电脑、手机、U 盘、NAS 服务器等），同时明确可能保留舞弊证据的核心系统（财务系统、邮件服务器、即时通信平台等）。

风险评估：评估在取证过程中可能面临的风险（如数据篡改、内部反调查、人员阻碍等），并制定相应的应对预案（如合法封存、网络隔离、快速镜像），并对相关部门和人员进行必要的保密与权限管控。

2 数据采集与证据固定

硬盘、手机取证：使用专业取证工具以只读方式操作对硬盘进行镜像，确保原始数据不被修改；对手机进行数据提取，并为硬盘镜像文件或提取的手机数据生成 SHA256 或 MD5 哈希值，做好记录。

网络日志与系统备份：对企业定期备份的数据库或系统进行快照式封存，便于后期对比分析；同时导出操作系统日志、数据库日志、VPN/ 堡垒机日志、网络防火墙日志等，确保能够回溯操作路径、访问 IP 和关键时间节点。

云盘、SaaS 系统取证：如企业使用阿里云、腾讯云、AWS 等云存储或 SaaS 软件，需在获得合法授权后，通过云服务商或管理员接口获取数据副本。

邮件服务器：如企业自建 Exchange 服务器或者采用第三方邮件服务，需在服务器端导出指定时间范围内的所有邮件并保留服务器端操作日志，尤其关注删除或过滤邮件的还原与比对，为查找潜在舞弊线索提供更多证据来源。

即时通讯与协同办公：针对钉钉、企业微信、Slack 等即时通讯工具或文档协同平台，导出聊天记录、文件传输记录等，记录导出过程，并及时封存关键证据，防止后续人为删除或篡改。

3 数据分析

财务数据分析

大额或高频交易分析

通过脚本，对 ERP 或财务系统中的付款记录、报销单据进行自动化筛查，锁定金额异常、供应商重复、报销项目异常等。

合同与审批流程对比

对关键合同的审批时间、审批人员、版本修改痕迹进行比对，排查“先付款后签合同”、“合同版本缺失”等不合规行为。

通讯内容分析

关键字检索

设定“回扣”“返利”“暗号”“月结”等与舞弊相关的关键词，在邮箱、聊天记录、文档中进行搜索，快速定位可疑信息。

文本挖掘

利用主题聚类、语义理解等技术，对大批量邮件、聊天记录进行深度分析，发现潜在的违法违纪对话主题。

行为日志分析

访问日志匹配

将财务系统、ERP 系统、邮箱系统等的访问 / 操作日志与涉案人员工作时间表、门禁记录进行比对，关注下班后或异常时段的大量访问、数据导出行为。

权限变更记录审计

检查近期或关键时间点，是否有人为操纵用户权限、权限异常上升、批量创建账户等可疑操作。

数据流向与外联分析

关注是否存在通过 FTP、外部云盘、私人邮箱发送公司敏感文件的行为；利用网络流量分析发现异常文件传输量或非法外连。

4 开源情报辅助分析

涉案人员信息挖掘

利用企查查、天眼查、启信宝等商业数据平台，全面分析涉案人员名下企业的股权构成及变化，明确其持股比例及管理权限，通过股权穿透技术，发现涉案人员与其他企业之间的潜在利益输送路径 。

跨案件关联与串并分析

通过分析公开社交媒体、工商数据和招投标信息，揭示案件之间的潜在关联，例如在同一地区的多起招标项目中发现频繁中标的企业，并结合其背后股权结构或管理人员的信息，挖掘其在多个案件中的角色。通过挖掘关键节点人员及其关联企业，将单一案件延展为完整的利益网络。

数据交叉比对与验证

为了确保开源情报的真实性与实用性，将获取的开源数据与内部信息进行交叉比对，例如，验证公开披露的资金流向与企业内部账目记录是否一致，排查异常交易。

5 案件还原与关键节点确认

时序关系还原

将疑似舞弊的核心事件、资金转移节点、关键聊天信息按照时间顺序统一整合，构建舞弊过程的时间线，对照资金流动、审批节点、人员进出公司等信息，清晰展示舞弊活动的完整过程。

关键节点确认

识别舞弊过程中的核心事件，如资金转移、合同签订、审批流程绕过等，根据行为数据和操作日志，确认各关键节点的责任人，明确主导者和从犯的责任。

6 鉴定意见书编撰

整合取证鉴定过程所获取的关键证据（财务记录、通讯内容、访问日志等），构建从最初线索到最终资金或利益落地的时间轴，便于企业管理层或司法机关直观了解舞弊全貌。

行为定性

描述舞弊行为的发生、发展及完成的全过程，指出关键节点和环节，明确各涉案人员在舞弊行为中的角色，区分主导者与从犯，明确其具体责任。

财务数据量化

统计涉案资金的总额、分布情况，包括大额转账、小额频繁交易等，明确具体数额。

4. 典型案例

高管吃回扣案

十年前的 QQ 记录揭秘！重新鉴定撕开回扣交易与泄密黑幕

十年前，某科技公司技术负责人 A 因利益分配不均，成立了与原公司业务相同的外包公司 B，通过外包项目获取供应商资源，并与多家供应商暗中达成回扣协议，私分非法利益。随着电子数据取证技术的发展，近期，奇安信洞鉴协助该企业进行了重新鉴定，解析当年的硬盘镜像文件，提取出关键的 QQ 聊天记录，揭示了 A 与供应商之间的回扣交易及商业机密泄露行为。

案件背景

某科技公司是一家在业内具有较高影响力的技术企业，2015 年，技术负责人 A 在管理技术团队过程中，因对公司利益分配不均感到不满，成立了与原公司业务相同的外包公司 B。在外包项目中，A 利用在原公司积累的人脉和资源，通过虚报项目成本、虚增服务费用等手段，与多家供应商达成回扣协议，从中获取高额非法利益。

同时，A 通过公司配发的电脑，使用 QQ 等即时通讯工具指导新公司的选址、装修、人员任命及技术分享，甚至直接传输带有公司签名的关键技术图纸，导致公司核心技术泄露，给公司带来重大经济损失，并影响了公司在行业内的发展和竞争力。

洞鉴解决方案

重新鉴定数据取证

鉴定专家确认 A 使用的公司配发电脑及相关移动硬盘作为主要检材。为确保检材的完整性和真实性，鉴定专家对所有检材进行了哈希值计算，并与原鉴定意见书中的哈希值进行比对，确保在取证过程中未被篡改或污染。整个过程严格遵循《司法鉴定程序通则》的相关规定，保证鉴定结果的合法性和权威性。

数据解析与恢复

鉴定专家对硬盘镜像文件进行了全盘扫描，未直接发现相关的 QQ 聊天记录，判断数据可能经过加密或隐藏处理。为进一步解析数据，专家查阅了 QQ 历年的功能更新记录和技术报告，发现自 2006 年后，QQ 开始将聊天记录加密存储为 .db 文件，但仍有第三方工具能够解密这些文件。鉴定专家使用专业数据恢复工具对移动硬盘中的 .db 文件进行解密和恢复，成功提取出明文的 QQ 聊天记录。

聊天记录内容分析

通过对提取出的 QQ 聊天记录进行详细分析，发现 A 与多家供应商的沟通频率极高，主要围绕项目选址、装修、人员任命及技术分享等主题展开。聊天记录中明确提及回扣金额、支付方式及回扣周期，具体数额达到数百万元，证实 A 通过虚报项目成本、虚增服务费用等手段，从供应商处获取高额回扣。此外，聊天记录还显示 A 多次传输带有公司签名的关键技术图纸，进一步证明其有意泄露公司商业机密，导致公司核心技术外泄，造成重大经济损失并影响公司在行业内的竞争力。

通过上述系统化的解决方案，奇安信洞鉴成功协助某科技公司查明了技术负责人 A 的贪腐行为，揭示了其通过外包公司进行回扣交易和商业机密泄露的违法行为。

客户价值

01 / 精准揭示回扣行为

通过全面提取和分析 A 的硬盘镜像文件、移动存储设备中的聊天记录，我们精准揭示了其与供应商的回扣交易过程及关键技术泄露的细节。明确了非法利益的流转路径和相关涉案行为，为案件处理提供了关键证据支撑。

02 / 保障证据的法律效力

鉴定过程中，我们严格按照司法鉴定规范操作，对所有检材进行哈希值校验，确保数据的完整性。通过合法有效的证据链构建，为客户在法律追责和维权过程中奠定了坚实基础。

03 / 维护企业核心利益

通过明确回扣交易及技术泄露的范围和影响，我们协助客户采取法律手段追责并加强内部管理，及时挽回经济损失，避免核心技术进一步泄露。

亿元资金侵占案

揭露资金侵占真相：深度剖析数据库篡改手段及亿级损失量化分析

某大型企业在一次财务审计中，发现其结算系统中存在异常的金额变动。初步调查显示，这些变动涉及一名已离职的员工，该员工在职期间利用其高级访问权限对公司核心业务系统的数据进行篡改，非法侵占了公司巨额资金。为查明事实，企业委托奇安信洞鉴团队对涉案系统展开深入技术分析，以追溯数据篡改行为并提供法律追责所需的证据支持。

案件背景

涉案企业运营的业务系统是一个高度复杂的综合平台，承载了从订单处理到财务结算的多环节功能模块。案件分析的难点在于：

1. 手法隐蔽

涉案员工利用系统特权在正常业务流程中掩盖篡改操作，表面上与系统日常运行无异。

2. 数据量庞大

系统内存储了数以百万计的交易数据，异常记录的筛选与确认需在海量数据中精准定位。

洞鉴解决方案

业务系统分析

鉴定专家深入解析业务系统的核心代码模块，包括与结算数据相关的功能逻辑和数据接口，定位可能被利用的风险点。

日志与数据库提取

鉴定专家从系统日志中提取了详细的操作记录，结合数据库历史数据进行比对分析，筛选出可能涉及异常操作的日志条目，同时导出关键数据表用于进一步分析。

涉案金额统计

鉴定专家编写脚本，对疑似篡改数据的内容进行追踪，逐条核对异常数据的变动情况，明确篡改涉及的金额。最终，成功识别出了被篡改的数据项和涉及的金额数额，提供了完整的证据链。

客户价值

01 / 明确涉案金额

通过细致的日志分析和数据库比对，成功量化了被篡改的数据内容及涉及的金额数额，这些详实的数据不仅有助于客户在法律诉讼中主张赔偿，也为评估和追回经济损失提供了重要依据。

02 / 提供坚实证据

鉴定结果揭示了前员工非法篡改业务数据库数据的具体行为和过程，明确指出了其与外部企业勾结，通过修改结算金额等关键数据项来侵占公司资金的犯罪事实，为进一步的法律追责奠定了坚实的证据基础。

03 / 增强内部管理

鉴定结果揭示了该企业内部控制系统的薄弱环节，为公司提供了改进和加强内部管理的机会，通过采取更严格的安全措施和监督机制，能够帮助企业预防未来风险，保障资产和数据安全。

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

- 上海盘石洞鉴
- 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

上海盘石洞鉴

上海市首家通过 CNAS 认可的民营司法鉴定机构

上海盘石洞鉴，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 16 名，高级工程师 3 名，中级工程师 5 名。拥有面积达 300 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

北京市司法局诚信等级评估“A”级的司法鉴定机构

北京网神洞鉴司法鉴定所，已通过CNAS实验室认可、CMA资质认定与ISO9001质量管理体系认证，拥有完备的资质认证、专业技术团队与高水平建设的实验室环境。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，同时，多次参加国内外能力验证和测量审核，获得满意结果。2025年3月，新增图像鉴定资质，进一步拓展服务领域。

目前，已拥有具备司法鉴定资质的专职鉴定人12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，我所拥有面积达150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，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

2025.3 新增图像鉴定资质
北京所新增图像处理、图像同一性鉴定和图像内容分析三大鉴定能力

2025.12 统一品牌
上海所更名为「上海盘石洞鉴」

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

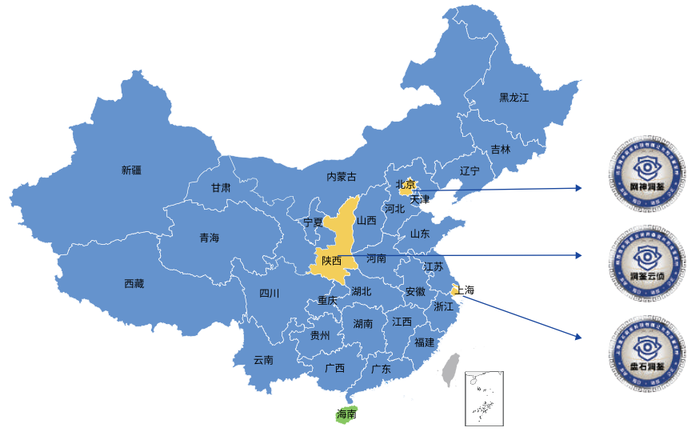
盘古实验室
国际知名安全研究团队
连续多次发布 iOS 完美越狱工具
累计已发现数百个 0day 移动安全漏洞

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



司法鉴定所
取证实践基地
技术服务中心

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

上海盘石洞鉴

北京网神洞鉴

陕西洞鉴云侦

获奖荣誉

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

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

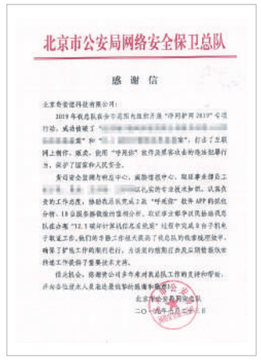
协助侦破重大疑难案件


中华人民共和国公安部

感谢信


北京市公安局网络安全保卫总队

感谢信


北京市公安局网络安全保卫总队

感谢信


甘肃省公安厅

感谢信


服务人才
科技流流流


赠予：上海盘石司法鉴定所

数鉴獬豸

大庆市公安局网络警察分局

2021年11月16日


赠 盘石电子数据鉴定所

电子取证助侦重
上海盘石显匠心
警企协作开新花
专群结合育硕果

大庆市公安局网络安全保卫支队二级大队长颁

2021年11月16日

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