北京网神洞鉴司法鉴定所

上海盘石计算机司法鉴定所

陕西洞鉴云侦司法鉴定所

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

上海盘石计算机司法鉴定所

021-52658848（上海）

上海市闵行区合川路 2555 号科技绿洲三期五 -3 号楼 4 层

陕西洞鉴云侦司法鉴定所

029-86196688（西安）

陕西省西安市经济技术开发区凤城二路 1 幢经发大厦 B 座

案例中所有图片均为虚拟数据，不涉及任何客户隐私

奇安信司法鉴定公众号

盘古石取证公众号

2024年
电子数据司法鉴定典型案例集 企业版

内部调查 | 知产侵权 | 黑灰产业

网络入侵 | 网络诈骗 | 维权纠纷

www.qianxin.com

CONTENTS

CONTENTS
目录

01

CORP. INVESTIGATIONS

企业内部调查

员工系列违规案

亿元资金侵占案

高管离职泄密案

恢复和分析关键电子数据，揭示企业内部违规行为

在高度数字化的商业环境中，企业面临的内部违规行为与电子数据紧密相关，表现出多样化与技术化的特点。无论是员工窃取公司机密，恶意篡改业务系统数据，还是非法侵占资金，这些行为均对企业的稳定与发展构成了严峻挑战。

电子数据司法鉴定在此发挥着至关重要的作用。通过电子数据鉴定，能够还原删除的关键文件，如涉密文档和会议记录；分析可疑程序代码，揭示内部人员利用特权进行的非法操作；审查访问与操作日志，识别敏感数据泄露的途径；以及比对业务数据，核实财务造假或利益输送等经济违规行为。

电子数据司法鉴定不仅能帮助企业查清事实真相，也为后续责任追究与损失挽回奠定关键证据基础，在维护企业安全与健康发展方面发挥着不可或缺的重要作用。

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，奇安信司法鉴定应邀介入，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。

奇安信解决方案

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，造成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。

高管离职泄密案

商业机密危机？电子数据鉴定揭示高管泄密真相

某企业怀疑一位离职高管泄露了公司的机密文件，致使相关核心技术泄露。为了查证此事，该企业委托奇安信司法鉴定对该高管离职前所使用的设备进行司法鉴定，鉴定人分析提取笔记本系统的基本信息及 USB 记录，并恢复文件 2000 余个，为案件的依法处理提供了坚实证据。

案件背景

某企业意外接收到一条匿名信息，信息中指控一家竞争对手正在生产与他们设备高度相似的产品。鉴于其设备模型图纸大多为机密图纸，并且已与设备制造工厂签订了严格的保密协议，这一消息引起了该企业的极大关注。经过深入调查后，发现该企业的一位前高管离职后加入了制造相似设备的公司。

因此，该企业怀疑该高管可能泄露了公司的机密文件，但由于其使用过的设备相关证据已被隐藏或删除，因此亟需专业技术团队对此进行恢复取证。

奇安信解决方案

1. **制作镜像：**为了保护原始数据，防止在恢复过程中发生意外破坏，鉴定人使用工具 FTK Imager 创建该硬盘的一个完整镜像。
2. **提取信息：**鉴定人对镜像文件进行加载分析后，提取到了 USB 设备使用记录共计 17 条，并根据委托方提供的时间段，查找了最近的访问文档记录共计 10 条。

最近访问的文档	创建时间	最后访问时间	用户
G** 资料	2020/1/27 12:48	2020/1/27 12:49	chen**
P** 柔软性	2020/1/27 8:00	2020/1/27 12:49	chen**
** 检测数据	2020/1/27 8:02	2020/1/27 12:49	chen**
** 选择及核算汇总	2020/1/27 12:48	2020/1/27 12:49	chen**
* 比较	2020/1/27 8:01	2020/1/27 12:49	chen**

部分最近访问文档记录（虚拟示意图，非真实信息）

3 **数据恢复：**使用数据恢复工具加载镜像文件，进行数据恢复，寻找已删除或丢失的文件，共计恢复 2054 个文件。

4 **文件提取：**鉴定人根据需要，提取并保存了 Word 文档、Adobe Acrobat 文档、Excel 电子表格和 AutoCAD 文件等类型的文件，同时也导出了包含文件信息的列表。

名称	文件类型	文件大小（字节）	文件路径
XX专利申请要点	办公文档	5622349	分区3_Windows[C]:\Users\Desktop\合作项目\专利申请要点.pdf
XX基础材料项目公示清单	办公文档	822479	分区3_Windows[C]:\Users\Desktop\合作项目\xx基础材料项目公示清单.pdf
XX项目合作协议	办公文档	162533	分区3_Windows[C]:\Users\Desktop\合作项目\XX项目合作协议.pdf
XX复合标准	办公文档	238472	分区3_Windows[C]:\Users\Desktop\生产相关\XX复合标准.pdf
XX检测报告	办公文档	637292	分区3_Windows[C]:\Users\Desktop\生产相关\XX检测报告.pdf
XX成本分析	办公文档	932382	分区3_Windows[C]:\Users\Desktop\公司运营\XX报表\2018XX\XX成本分析.xlsx

部分提取文件（虚拟示意图，非真实信息）

客户价值

01 / 保护商业秘密

设备模型和组件图纸作为企业的重要资产，其保密性至关重要。此次鉴定使企业能够明确了解商业机密是否泄露，从而能够及时、有效地采取措施保护其商业利益。

02 / 高效技术支持

快速而准确地进行了数据提取和恢复，帮助该企业获取关键信息，支撑企业进行后续的决策。

03 / 法律权益维护

为企业的法律诉讼提供坚实的支持，企业可以依据鉴定意见书，对商业秘密泄露的对手进行法律追责，保障企业的法律权益。

02

IP INFRINGEMENT

盗版网络文学案

盗版视频网站案

游戏私服案

打击知识产权侵权犯罪，维护企业合法权益

知识产权保护长期面临着“侵权成本低、维权成本高”的问题，尤其在数字化背景下，侵权者可以利用各种技术手段，例如爬虫技术、分布式存储等，进行大规模侵权行为；此外，利益链条的复杂性使得侵权收益的追踪和确认变得更为困难。

这种情况下，电子数据司法鉴定显得尤为重要。例如，在一个涉及侵犯千余部网络文学作品著作权的案件中，奇安信司法鉴定比对了近 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，从而打击侵权犯罪，维护了权益人的合法权益。

事实上，电子数据司法鉴定在知识产权侵权案件中的应用并不止于此。例如，对于非法上传、分发音乐、电影等内容的行为，司法鉴定可以通过网络流量分析、程序反编译等技术手段，追踪侵权行为、获取电子数据证据。对于非法复制、销售软件的行为，司法鉴定可以通过对比正版和盗版软件的差异，确定侵权行为。司法鉴定通过技术手段揭示犯罪事实，为维护社会公正和公平发挥着不可替代的作用。

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。

奇安信解决方案

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
[illegible]	972008	[illegible]	1095327	925481	95.21 %	84.49 %
[illegible]	2775708	[illegible]	2858087	2172756	78.28 %	76.02 %
[illegible]	1712473	[illegible]	3016749	1626810	95.00 %	53.93 %
[illegible]	698580	[illegible]	2163905	651930	93.32 %	30.13 %
[illegible]	1544527	[illegible]	1710636	1493399	96.69 %	87.30 %
[illegible]	2377473	[illegible]	2545771	2229239	93.77 %	87.57 %
[illegible]	2624560	[illegible]	2678428	2520483	96.03 %	94.10 %

部分相似度比对结果

客户价值

01 / 协助确认损失收益

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

02 / 揭露盗版侵权网络

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

03 / 保护企业合法权益

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

盗版视频网站案

24 小时内锁定侵权源头，为版权正义加速

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

案件背景

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

奇安信解决方案

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

1. 播放地址抓取

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

2. 视频内容对比

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

3. 侵权证据固定

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

客户价值

01 / 提升诉讼效率与成功率

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

02 / 维护企业合法权益

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

03 / 促进行业健康发展

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

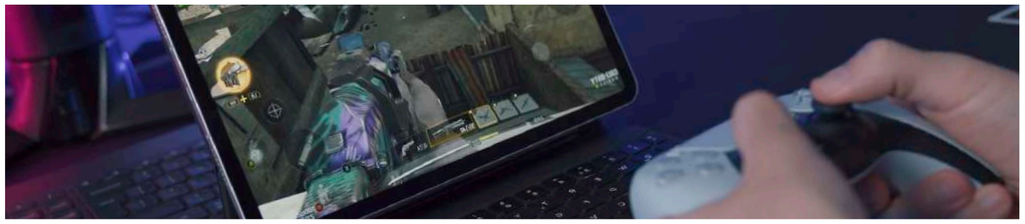
游戏私服案

关键文件比对分析，深挖私服侵权细节

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

案件背景

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



奇安信解决方案

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

01 源代码对比

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

02 目录结构比对

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

03 地图比对

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

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

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

客户价值

01 / 提供确凿证据

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

02 / 维护企业权益

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

03 / 促进产业健康发展

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

03

网络黑灰产猖獗，电子数据司法鉴定成为打击关键

随着信息技术的飞速发展和互联网的深度渗透，网络黑灰产已经成为了公共安全领域的一大顽疾。其犯罪方式多元，涵盖黑灰产软件研发、数据窃取、恶意广告推送等，这些行为不仅破坏了网络环境的公正性，也严重损害了企业与个人用户的合法权益。

面对日益猖獗的网络黑灰产业，电子数据司法鉴定发挥着至关重要的作用，成为打击非法活动、维护数字正义的利剑。通过逆向分析、代码审查、动态复现等技术手段，深入剖析各类涉案软件的运作机制，准确定位其中的违法、违规行为，为法律制裁提供了关键证据。

网络黑灰产的泛滥凸显了技术滥用的风险与挑战，同时也彰显了电子数据司法鉴定在保护数字环境中的核心地位。通过专业技术手段，司法鉴定为企业抵抗网络黑灰产业侵害、维护平台秩序和用户权益提供了有力的支持。

BLACK MARKET

网络黑灰产

外挂抢红包案

非法爬取“社交媒体”数据案

手机“霸屏”广告案

骑手抢单外挂案

骗取推广佣金案

外挂抢红包案

科技维权：深度剖析“抢红包”外挂，推动优质用户体验提升

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

案件背景

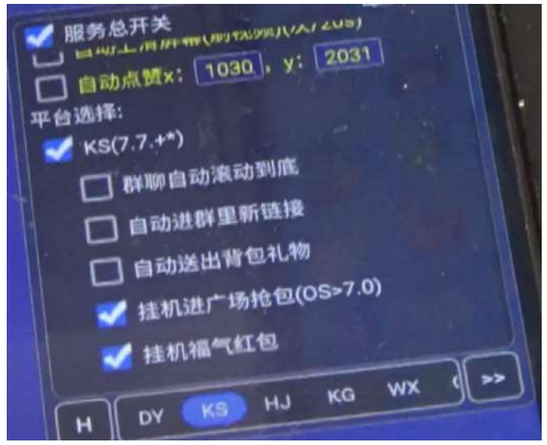
2021 年，该企业发现 5 个账户利用多台手机设备，通过外挂程序在各个直播间轮流抢主播发的红包近 2 万元，抢到的红包再集中打赏给某主播提现。这一行为严重扰乱了平台的秩序，影响了用户体验，该企业立即报案，并寻求专业的电子数据司法鉴定对相关外挂程序进行深入剖析。

奇安信解决方案

鉴定人通过动静结合的方式，对涉案外挂程序进行了深入剖析，具体步骤如下：

1. 功能动态复现

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



代码反编译

2. 程序逆向分析

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

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

客户价值

01 / 提升用户体验

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

02 / 维护平台秩序

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

03 / 维护商业利益

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

非法爬取“社交媒体”数据案

解码非法爬虫行为：用户数据窃取的幕后黑手

以抖音、小红书、微博为代表的社交媒体积累了大量有价值的用户数据，许多不法分子通过不正当手段爬取数据并进行加工售卖，损害了用户与企业的权益。其中，某热门社交软件报案称某“破解程序”非法获取了其服务器内的大量数据。针对此情况，奇安信司法鉴定应邀对该“破解程序”进行了功能性鉴定。经过详细的审查和分析，证实该程序确实存在绕过加密、伪造请求、获取数据、自动发送私信等功能。

案件背景

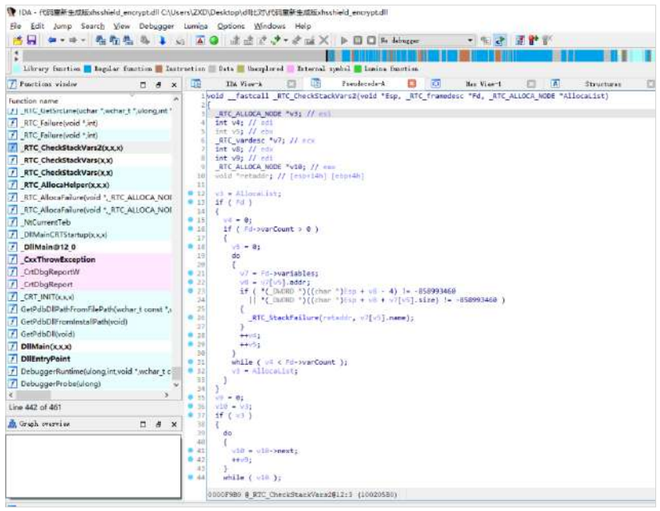
2022 年，一款程序对某企业的 APP 构成了威胁。这款程序破解了企业的加密算法和端口，绕过了其设立的风控措施，自动爬取了服务器上大量的用户数据，并控制账号无限制发送私信，严重侵犯该企业权益。因此，奇安信司法鉴定受该企业委托，对网上售卖的“破解程序”及嫌疑人电脑进行了司法鉴定。

奇安信解决方案

该案件有 3 个鉴定重点 : 其一，证明服务器中提取的“破解程序”与嫌疑人电脑中的代码“同源”；其二，确定其爬虫、发送私信等功能特性；其三，确定其爬虫数据范围是否违规。基于以上三个鉴定重点，鉴定人通过“静态分析”“动态调试”的方式，对检材电脑和服务器中的代码文件进行了功能性鉴定。

1. 相似度比对

对从服务器中提取的 DLL 文件与嫌疑人电脑中生成的 DLL 文件进行了反编译；通过比对反编译代码，发现服务器中与检材电脑中的 DLL 文件具有实质性相似性。



代码反编译

2. 代码分析

对提取的源代码进行了深度解读分析，通过查看“SendContent”函数和其相关接口和方法的定义，确认了代码具有发送私信的功能；通过查看“recognization”方法，确认了代码具有识别并计算滑块验证码位置的功能。

3. 动态复现

根据鉴定人在代码分析步骤中得到的结果，进一步运行这些代码，验证其实际运行时的行为与代码分析阶段一致。

4.Robots 协议范围对比

下载并查看该企业 Robots 文件，对比爬虫访问的数据范围，确定其爬虫数据范围不在 Robots 协议范围内。

客户价值

01 / 保护商业利益

鉴定结果证明了该企业的商业信息被非法抓取，这为其提供了保护其商业利益的法律依据，企业可以通过法律手段要求侵权者停止侵权行为，赔偿因侵权行为造成的损失。

02 / 改进安全防护

了解被非法爬取的具体方式和手段，可以帮助企业在未来更好地防止类似的犯罪行为，提升企业的数据安全防范能力。

03 / 保护用户隐私

非法爬取的数据包含用户的私人信息，直接影响到用户的隐私和数据安全，此类鉴定意见能够帮助企业理解用户数据被非法获取的方式，从而改进数据保护机制，保护用户的隐私和数据安全。

手机“霸屏”广告案

反复弹出无法关闭？“逆向分析”揭秘手机霸屏 APP

近年来，一些流氓 APP 通过霸屏广告形成了非法产业链，其通过劫持设备系统，强制用户查看广告以获取暴利。某手机厂商发现其用户遭受这些霸屏广告的骚扰，遂报案。在此背景下，奇安信司法鉴定运用专业的程序逆向分析技术，成功地揭示了流氓应用程序非法控制用户手机、窃取用户信息，以及根据监听到的事件触发广告弹出的全过程。鉴定所提供的鉴定意见完整、科学且客观，这为案件的成功侦破和法律处理提供了强有力的支持。

案件背景

2022 年 6 月，一家手机厂商报案，指出其用户的手机在安装某些应用后，出现了后台强制启动、后台常驻、无法使用返回键、无法截图等问题，涉嫌非法控制计算机信息系统。为深化对应用行为的理解，发现潜在的违规功能，委托奇安信司法鉴定对涉案应用进行了功能性鉴定。

奇安信解决方案

此类霸屏流氓软件可能含有大量的隐藏功能，例如搜集并发送用户数据、后台常驻等。因此，鉴定人采取了“动静结合”的方式，深入剖析违规行为，透视应用底层原理。

1. 反编译 APK

使用 JADX 工具打开 APK 文件进行分析，查看应用的源代码和其运行机制，深度挖掘与用户信息搜集和网络通信有关的代码段。

2. 动态运行监测

应用在模拟器上被运行和实时监控，通过捕获网络数据包，确认了这些应用收集并上报云端的设备信息行为，如 IMEI 号、设备厂商、系统版本、屏幕尺寸、设备 mac 地址、hms 版本号、设备厂商类型、应用包名、应用安装来源等；同时，接收数据的远端服务器亦被明确。

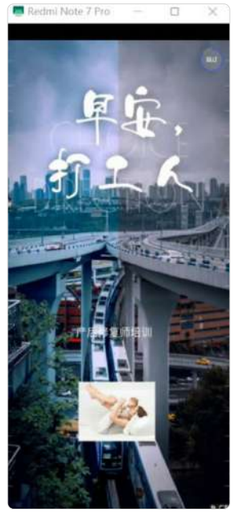
3. 源代码分析

鉴定人按照预期，在源代码中定位并分析相关代码段，如监听事件、启动进程、收集设备信息等，确认应用具备监听各种事件（如 HOME 键点击、锁屏、解锁、应用的卸载和安装等）的功能，并在监听到事件发生时呼出广告。

开启锁屏广告

全屏广告

应用内广告位广告



应用内启动界面广告

客户价值

01 / 保障用户权益

霸屏流氓 APP 严重影响了用户体验，通过此次鉴定，实现了对霸屏流氓 APP 的依法查处，也有力地保护了用户的隐私权和权益，减少了用户的损失。

02 / 增强安全防护

通过剖析霸屏流氓 app 工作原理，令该厂商能够更好的了解潜在的安全风险，有助于研发更有效的安全防护措施。

03 / 提升用户体验

通过对霸屏流氓 APP 的鉴定与打击，令该厂商净化自身应用生态环境，减少用户受到广告骚扰和恶意行为的困扰，提升了用户的应用体验和满意度。

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。

奇安信解决方案

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。

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

近期，一家领先的电子商务平台发现，一家第三方代发货平台通过不正当手段骗取其推广平台的大量佣金。该第三方平台利用自动化技术手段篡改商品 ID，使得商品销售被误认为是通过正规推广活动产生，非法骗取千万元推广佣金。奇安信司法鉴定对该非法程序骗取推广佣金的原理进行了剖析，为打击该非法行为提供了有力证据。

案件背景

某知名电商平台允许商家通过推广计划激励推广者分享商品链接，以促进销售并支付相应的佣金。然而，近期平台发现一家第三方代发货平台涉嫌利用不正当手段非法获取佣金。

经过深入调查发现，代发货平台通过以下方式运作：首先，用户在该电商平台上开设店铺并接收顾客订单。随后，用户利用该软件同步订单信息，并在其他电商平台寻找相同或类似商品的低价版本。用户将这些商品的信息输入代发货平台，并生成新的订单。这一过程中，软件似乎能够模拟推广链接的效果，误导该电商平台系统认为订单是通过推广计划产生的。

这一行为违反了该电商平台的推广规则，骗取了大量佣金，为查明真相，该平台委托奇安信司法鉴定对这款代发货软件进行技术分析。

奇安信解决方案

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。

经过以上鉴定和分析，奇安信司法鉴定明确揭示了第三方代发货软件通过非法篡改推广链接获取佣金的基本机制。该软件使用户在无需实际持有商品库存的情况下进行销售（即实现“无货源发货”），并通过非法手段获得推广佣金。这一发现为电商平台提供了确凿证据，证实了涉案软件的欺诈行为，为后续采取法律措施以维护平台秩序奠定了坚实基础。

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。

04

NETWORK INTRUSION

网络非法入侵

撞库攻击案

新型打印机木马案

网络入侵难以防范？司法鉴定解密隐蔽攻击手法

在互联网时代，网络入侵已成为危害企业网络安全、侵犯用户隐私的重大隐患。不法分子利用系统漏洞或恶意软件，非法获取、窃取、篡改网络中的敏感信息，给个人隐私和企业财产安全带来了巨大威胁，其作案手法也日趋隐蔽，一旦发生，查清真相、找到犯罪者的难度较大。

面对日益严峻的网络安全形势，电子数据司法鉴定成为企业防范网络攻击、维护自身利益的有力武器。以“撞库攻击案”和“新型打印机木马案”为例，鉴定人运用逆向分析、动态调试等专业技术手段，深入分析木马程序和恶意软件的底层运行机制，有效识别了入侵行为的来源和路径，不仅有助于受害企业快速采取应对措施，阻断进一步的损失，同时也为追究攻击者的法律责任提供了关键的证据支撑。

撞库攻击案

5 小时 200 万次！紧急追溯源头，全面评估风险

2023 年，一家知名企业遭受了一次未知黑灰产团体发起的撞库攻击，此次攻击历时约 5 小时，共计发起了 200 多万次尝试。在狙击这场网络攻击中，奇安信司法鉴定发挥了关键作用，协助企业对攻击期间的关键数据进行了精确统计和深入分析，包括涉及的 IP 地址、归属地以及成功登录的账号等信息，为企业追踪攻击源头和采取法律行动提供了坚实的证据基础。

案件背景

本案中，攻击者通过自动化工具对目标企业的账号系统进行了密集的登录尝试，试图通过匹配泄露的凭证信息来获取未授权的访问权限。这种攻击不仅可能导致用户数据泄露，还可能对企业的声誉和经济利益造成严重损害。为了调查此次事件并采取相应的法律行动，企业委托了奇安信司法鉴定对涉案的登录日志数据库中的数据进行固定，并与企业内部安全平台的研判结果进行比对。

奇安信解决方案

在面对撞库攻击的司法鉴定案件中，我们的专家团队采取了一套系统化的方法来分析和验证攻击事件。这个过程包括了对关键数据的固定、解析、统计分析，以及对企业安全系统的风控规则的检查和对比验证。以下是对鉴定过程的详细描述：

1. 数据固定

鉴定专家首先访问了遭受攻击的系统，固定了包含账号登录动作的日志信息，尤其关注了攻击发生期间的特定日期和符合撞库特征的日志记录。

2. 数据解析

通过编写脚本，鉴定专家对日志文件进行了自动化分析，提取了包括登录时间、IP 地址、登录结果（成功或失败）、用户名和密码等关键信息。

3. 统计分析

对上述信息进行统计分析，便于确定攻击的高峰时段、频繁使用的 IP 地址与频繁尝试登录的账号，并进一步分析成功登录的记录，确定了被成功访问的账号及其登录的具体时段。

4. 对比验证

该企业安全系统自动记录并分析了可疑的登录行为和其他安全事件。鉴定专家将登录日志与安全系统的审计结果进行了细致的对比，评估相关登录尝试是否被系统准确地识别并标记为“疑似撞库”。

终端 IP	归属地	次数
[redacted]	辽宁	376
[redacted]	福建	71
[redacted]	广东	153
[redacted]	吉林	345
[redacted]	河南	333
[redacted]	福建	101
[redacted]	河南	301
[redacted]	江苏	315
[redacted]	吉林	364
[redacted]	安徽	90
[redacted]	河南	555
[redacted]	吉林	290
[redacted]	广东	33
[redacted]	河南	329
[redacted]	福建	23
[redacted]	广东	43
[redacted]	浙江	499

终端 IP 统计

通过上述详尽的鉴定步骤，鉴定专家为企业揭露了撞库事件的核心细节，明确了攻击时间、方式、受影响的账号等及其归属地，并为可能的法律行动提供了坚实的证据基础。

客户价值

01 / 关键证据支撑

通过对关键数据的固定和深入分析，为企业揭示了攻击的详细情况，如攻击者的 IP 地址、成功登录的账号等，为追溯攻击源头和采取后续法律措施提供了坚实的证据基础。

02 / 评估潜在风险

通过解析和统计分析攻击数据，奇安信司法鉴定揭示了攻击的模式和高风险账号，帮助企业有效评估潜在风险和损失，从而更好地制定应对策略和补救措施。

03 / 安全策略优化

鉴定结果不仅准确识别了攻击模式和目标账号，还帮助企业发现了安全漏洞和潜在风险点。企业据此采取了相应的安全补救措施和强化策略，显著提高了整体的安全防护水平。

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。

奇安信解决方案

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。

05

ONLINE FRAUD

网络诈骗

“薅羊毛”诈骗案

网络诈骗呈高发趋势，司法鉴定助力挽回损失

随着互联网和人工智能技术的迅速发展，网络诈骗形式和手段不断演变，对个人用户和商业组织构成了前所未有的挑战。诈骗者利用 AI 生成的逼真语音和图片，创建高度欺骗性的钓鱼邮件和虚假信息，诱使受害者泄露敏感信息或直接转账。企业诈骗更为复杂精细，涉及财务操作和商业合作骗局，诈骗团伙甚至通过内部人员利用公司制度漏洞实施诈骗。

电子数据司法鉴定在这一背景下成为关键防线。通过专业的数据分析和技术手段，能够帮助警方和企业揭露诈骗团伙的作案手法，追踪涉案资金的流向，为法律追责和经济损失的挽回提供了坚实的支持。

以“薅羊毛”诈骗案为例，犯罪团伙巧妙利用电商平台的退款政策和系统漏洞，实施退款但不退货的操作，造成了巨大的经济损失。奇安信司法鉴定迅速调动资源，配合三地抓捕取证，并成功揭露了犯罪团伙的内部通信、作案手法及商品流转过程，为案件侦破提供了决定性证据。

“薅羊毛”诈骗案

揭露“退款不退货”骗局，追踪超 20 万“薅羊毛”损失！

某全球领先的电商平台近期成为网络诈骗的目标，遭遇一起精心策划的退款诈骗案。犯罪团伙巧妙利用退货和退款制度的时间差，执行退款但不退货的操作，非法获得价值逾 20 万元的苹果手机，对平台及其合作商家造成了巨大经济损失。面临这一复杂挑战，当地警方立即采取行动，并委托奇安信司法鉴定提供专业的现场固证及司法鉴定服务。

案件背景

作为一家享誉全球的电商巨头，该平台为消费者提供了极致便捷的在线购物环境。然而，不法分子却利用便利的退换货政策，实施了大规模诈骗行为。

具体来说，该团伙专门在平台上下单单价高昂的产品，再利用退货政策发起退款后不退回或是退回一些残次品，然后在网上转售价格高昂的产品以从中牟利，非法占有了价值超过 20 万元人民币的苹果手机。

面对这一案件，奇安信司法鉴定迅速调动资源，配合三地抓捕取证，并成功揭露了犯罪团伙的内部通信、作案手法及商品流转过程，为案件侦破提供了决定性证据。

奇安信解决方案

1. 三地高效固证

配合三地抓捕取证，对现场查获的数台手机、台式机、笔记本电脑进行现场取证，为进一步分析交易过程提供基础。

2. 手机数据提取

对涉案手机进行了数据提取，包括基本信息、通讯录、通话记录、短信记录以及即时通讯应用（如微信、QQ、微博等）的使用记录，揭露了犯罪团伙的内部通信方式和协调作案的具体方法。

3. 硬盘数据提取

对涉案台式机和笔记本电脑的硬盘进行了详尽的文件分析，发现并提取了大量关键表格文件。这些文件包含了商品流转记录、物流信息等，为确定犯罪团伙的非法获利提供了直接证据。

4. 虚拟币平台分析

对虚拟币平台上的交易记录进行了分析，包括交易的时间戳、交易金额、交易双方的钱包地址等，追踪了非法交易的资金流向。

在此次案件中，奇安信司法鉴定为警方提供了从取证、固证到司法鉴定的一条龙服务，不仅为快速侦破案件提供了技术保障，也为后续的案件审理奠定了坚实的证据基础。

客户价值

01 / 高效固定证据

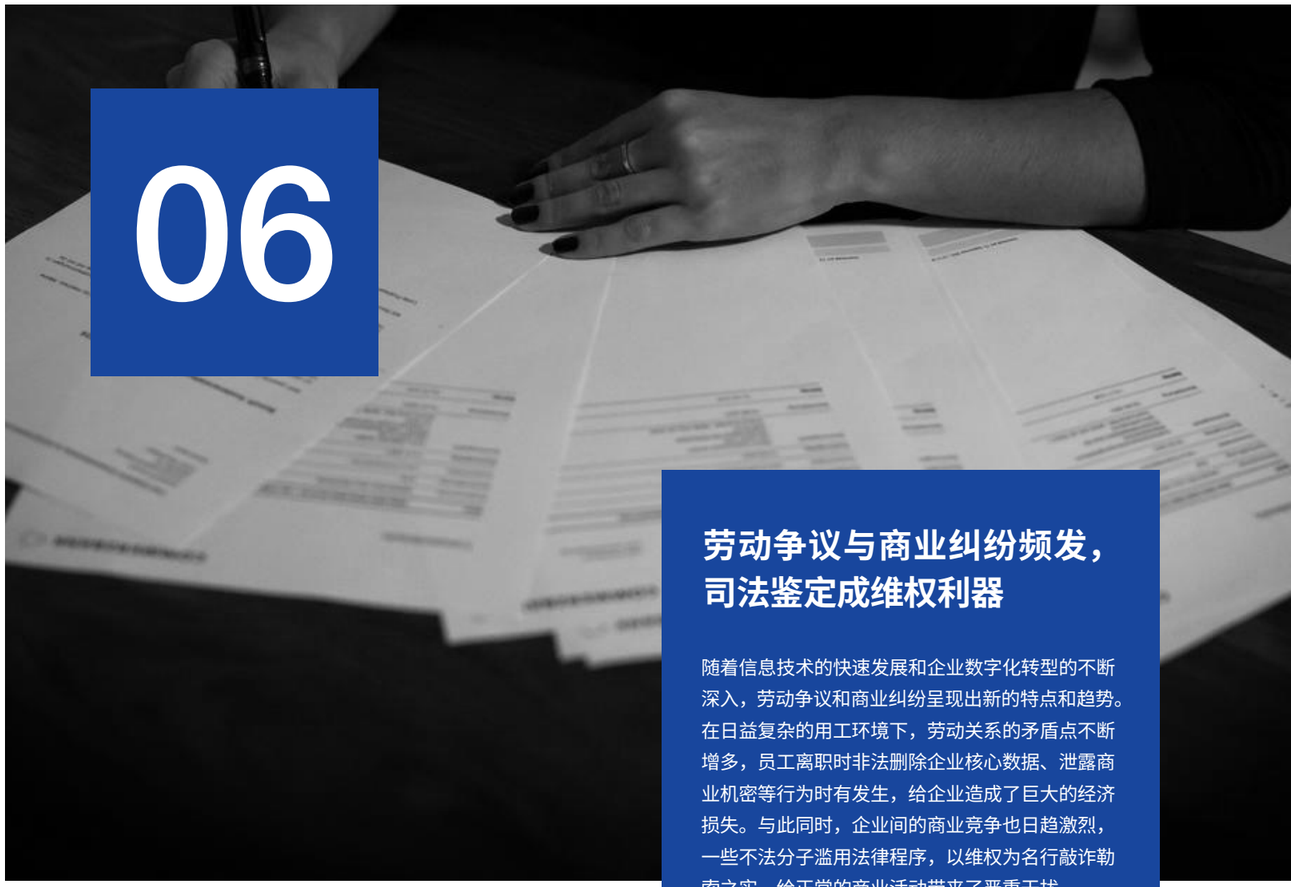
迅速响应多地警方，并高效执行现场取证与数据固证。不仅保证了证据的及时收集，还确保了收集到的证据完整有效，对于构建强有力的证据链至关重要，为案件的快速侦破和法律诉讼提供了坚实的基础。

02 / 揭示犯罪模式

通过对手机数据、硬盘文件及虚拟币平台交易记录的分析，奇安信司法鉴定不仅揭示了犯罪团伙的作案手法，还深入追踪了资金流向，为理解犯罪模式提供了全面视角。

03 / 减少经济损失

通过揭露犯罪行为，奇安信司法鉴定为客户挽回了经济损失，并对类似的非法行为产生了强烈的震慑效果，保障了企业利益，维护了市场的公正和秩序。



06

RIGHTS PROTECTION DISPUTE

维权纠纷

离职纠纷案

“黑维权”案

劳动争议与商业纠纷频发，司法鉴定成维权利器

随着信息技术的快速发展和企业数字化转型的不断深入，劳动争议和商业纠纷呈现出新的特点和趋势。在日益复杂的用工环境下，劳动关系的矛盾点不断增多，员工离职时非法删除企业核心数据、泄露商业机密等行为时有发生，给企业造成了巨大的经济损失。与此同时，企业间的商业竞争也日趋激烈，一些不法分子滥用法律程序，以维权为名行敲诈勒索之实，给正常的商业活动带来了严重干扰。

在应对这些棘手问题时，电子数据司法鉴定发挥着不可或缺的关键作用。例如，在“黑维权”案件中，鉴定人运用网络数据包分析、自动化爬虫等技术手段，揭露了所谓＂维权＂证据系非法批量获取，帮助媒体平台及时化解法律风险，避免了不必要的经济损失，同时也为遏制＂黑维权＂乱象提供了有力支撑。

面对不断演变的劳动争议和商业纠纷，企业要积极借助专业力量维护自身合法权益。通过与鉴定机构的紧密配合，运用先进的电子数据司法鉴定技术，及时固定电子证据，方能在纷繁复杂的矛盾冲突中把握主动，最大限度规避法律风险，实现长远稳健发展。

离职纠纷案

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，奇安信司法鉴定受委托，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。

奇安信解决方案

为了确证前员工删除工作文件的行为及其具体时间，奇安信司法鉴定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：

1. 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。

2. 文件系统日志的提取

对 NTFS 文件系统日志进行了提取，这些日志是 Windows 系统用来记录文件系统变更的详细历史。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。

3. 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。

4. 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。

EventTime	Event	Detail	FileName
2020-08-17 18:16:15	File Deletion		Bio-weekly report
2020-08-17 18:16:15	File Deletion		Bio-weekly report
2020-08-17 18:16:15	File Deletion		Bio-weekly report
2020-08-17 18:16:16	File Deletion		Bio-weekly report
2020-08-17 18:16:16	File Deletion		Monthly report
2020-08-17 18:16:16	File Deletion		Monthly report
2020-08-17 18:16:16	File Deletion		Monthly report
2020-08-17 18:16:16	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report
2020-08-17 18:16:17	File Deletion		Monthly report

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。奇安信司法鉴定帮助客户转变思路，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。

“黑维权”案

揭穿黑维权伎俩 ， 助力媒体平台有效反击“批量维权”黑灰产

某知名媒体面临“黑维权”困境。某科技公司利用爬虫技术非法获取其照片资源，并针对涉嫌侵犯知识产权的照片，联系相关权利方进行维权。该公司的行为以“维权”为名，行“扰乱社会秩序”之实，一举引发数百起案件，给企业的正常运营带来重大影响。此次事件中，奇安信司法鉴定的专业介入为该媒体提供了关键技术支持，帮助其避免了不必要的诉讼，有效维护了自身权益。

案件背景

随着数字化时代的发展，网络空间的知识产权保护日益成为社会关注的焦点。然而，某些团体或个人却利用知识产权保护的名义，通过技术手段批量爬取网站内容，然后寻找并联系内容的权利人，提起大量维权诉讼，旨在通过法律程序获得经济利益。此类行为不仅给被告企业造成巨大经济和名誉损失，还严重占用了司法资源，扰乱社会秩序与市场经营环境。

本案涉及的媒体平台作为受害方之一，面对大规模的维权行动，不得不进行赔偿，承受着巨大的压力和挑战。奇安信司法鉴定通过精确的技术分析，揭示了这一行为的隐秘性、专业化特征，为受影响的企业提供了坚实的证据支持，使其在面临无端法律挑战时具备了充分的准备和有效的应对策略。

奇安信解决方案

在应对非法爬虫行为引发的知识产权侵权案件中，奇安信司法鉴定为客户提供全面、精准的技术支持，确保其在法律诉讼中能够有效维护自身权益，同时促进司法资源的合理利用和市场秩序的良性发展。

1. 网络数据包分析

使用网络抓包工具，监测并记录媒体平台 APP 在运行过程中所产生的网络数据包，从而定位到涉案照片的网址。

2. 自动化爬虫抓取

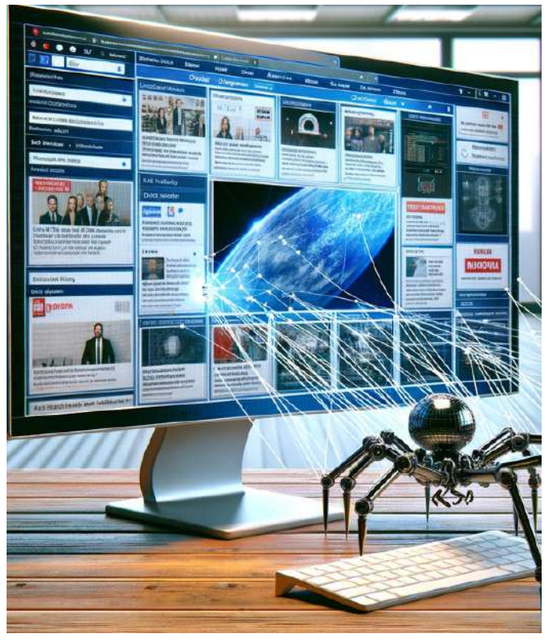
开发并运行定制的爬虫脚本，针对抓包环节中识别的目标域名地址发起自动请求，从服务器端获取相应的数据信息，并将这些数据有效地整理保存至表格文件内。

3. 数据比对分析

通过将爬虫技术所获取的网址数据与该科技公司提供的网址内容进行严格比对，验证了两者的一致性，从而推测出该科技公司所使用的证据是通过非法的爬虫手段获取的。

4. 法律合规性评估与咨询

对涉案的爬虫行为进行细致的法律合规评估，分析其对应的法律责任和可能违反的法规条款，为受此类行为影响的企业提供专业的法律咨询和策略建议，辅助其制定针对性的应对措施。



案例价值

01 / 避免法律纠纷

通过奇安信司法鉴定的专业技术分析与数据比对，该知名媒体能够有力地反驳原告律所的指控。揭示原告通过非法爬虫手段获取证据的行为，为客户在私下和解中占据了有利地位，避免了不必要的法律纠纷和经济损失。

02 / 司法资源优化

奇安信司法鉴定的专业介入，有效避免了冗长的诉讼过程，减轻了司法机关的工作压力，同时促进了司法资源的优化配置，确保了司法资源得以更加高效和公正地服务于社会。

03 / 维护市场秩序

奇安信司法鉴定的有效介入帮助该媒体及时地识别并揭露了不正当的“黑维权”活动，此举不仅针对个案，更对整个市场秩序和法律环境产生了积极影响，有助于遏制此类行为的蔓延，促进了健康、公平的市场环境和法律环境的建设。

ABOUT US

ABOUT US

关于我们

奇安信数字司法服务简介

奇安信数字司法服务，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1个电子证据云服务平台、31个取证服务网点、3家司法鉴定所，提供事前存证、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。

奇安信数字司法服务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。

1个

司法存证平台

奇证云

合法合规
不可抵赖
公开透明

3大

司法鉴定所

- 上海盘石司鉴
- 北京网神洞鉴
- 陕西洞鉴云侦

31个

技术服务网点

司法鉴定人 30+

取证技术专家 60+

覆盖全国 31 个省级行政区

奇安信司法鉴定服务介绍

奇安信司法鉴定，作为专业的电子数据取证与鉴定服务提供商，为客户解决以下难题：

企业内部调查

通过对员工使用的计算机、移动设备等进行调查分析，帮助企业发现员工泄密、违规操作、职务侵占等不当行为的客观证据，同时完善风险管控措施。

知识产权保护与维权

当企业商业机密或核心技术遭遇泄露时，帮助企业追踪信息泄露的途径，锁定泄密责任人；当企业面临知识产权争议时，帮助企业证明其知识产权的归属。

网络安全事件溯源取证

当企业遭受黑客攻击、系统入侵时，通过日志分析、恶意代码分析等，帮助企业还原入侵过程，评估损失，并在追究攻击者法律责任方面提供必要的技术支持和证据固定。

网络黑灰产打击

通过技术手段揭示黑灰产业链的运作模式，为企业和执法机关提供黑灰产调查、证据固定和行为分析服务，助力企业有效打击网络黑灰产业，保护企业和消费者权益。

电子数据司法鉴定服务

提取与固定

手机电子数据 | 计算机电子数据 | 存储介质数据 | 网络电子数据

分析与鉴定

电子数据分析与鉴定

- 手机数据恢复及固定
- 计算机数据深度挖掘
- 存储介质数据深度挖掘
- 计算机系统操作行为

信息系统分析与鉴定

- 软件相似性比对
- 文件相似性比对
- 恶意代码分析
- 网络数据行为分析
- 源代码功能鉴定
- 软件功能鉴定

数据恢复

数据库修复 | 邮件修复 | 文件修复 | 物理恢复

特色服务

密码破解

- 解锁 / 绕锁
- 数据提取

（仅限涉案设备）

内部调查

- 商业秘密泄露
- 反舞弊
- 反欺诈
- 内部违规

电子数据离职审计

- 数据恢复
- 数据存档
- 权限审查
- 设备检查

旗下机构介绍

上海盘石司鉴

上海市首家通过 CNAS 认可的民营司法鉴定机构

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

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

北京网神洞鉴

北京司法局诚信等级评估“A”级的司法鉴定机构

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

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

陕西洞鉴云侦

按照高标准建设的司法鉴定机构

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

目前，已拥有具备司法鉴定资质的司法鉴定人6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。

奇证云平台介绍

奇证云是安全可信的数据价值司法保护平台，为企业、行政监管和执法部门提供第三方司法存证服务。其基于区块链技术的难篡改、可追溯的特性，依托奇安信成熟安全方案，并与奇安信司法鉴定深度融合，为客户提供便捷安全的取证、存证、鉴证服务。

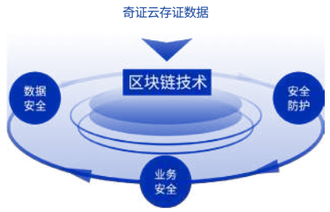
产品优势

全流程程序合规

多年取证鉴定经验，确保从取证到鉴定的每一个环节都严格符合法律法规的要求。

全方位安全可信

奇安信成熟安全能力 + 区块链技术，确保存证数据安全、难以篡改。



全链条便捷鉴证

与奇安信司法鉴定深度融合，一站式提供司法鉴定服务。

数据确认函　专业司法鉴定意见

专家辅助人出庭质证

应用场景

企业	监管	公安	政务	金融
数据知产登记 商业秘密保护	直播监管 执法合规	证据保全 执法合规	电子票据 数据共享	数据资产 交易合规
教育	**医疗**	**能源**	**文娱**	**烟草**
资格证书验证 学术资源	电子病历 纠纷保障	碳交易 非法窃取	影视版权 文化 IP	电子合同

优势亮点

01 先进技术，突破疑难案件

奇安信数字司法服务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。

奇安信司法鉴定

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

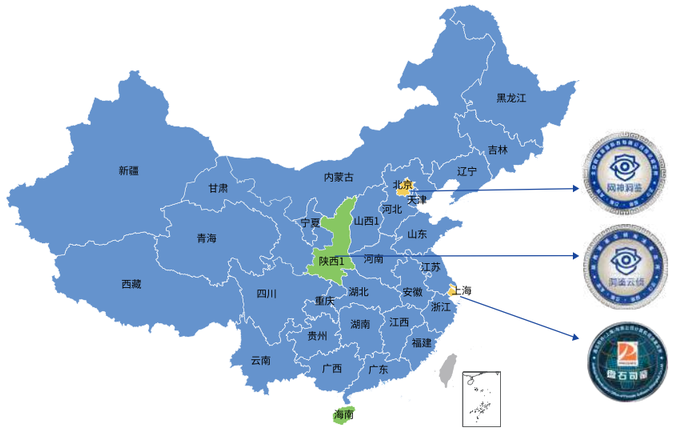
02 遍布全国，多地高效响应

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

3 个司法鉴定所

4 个取证实践基地

覆盖全国 31 个省份



03 事前、中、后，全流程服务

奇安信数字司法服务通过提供事前存证、事中取证、事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	事中	事后
• 商业秘密存证 • 数字知产确权存证 • 违规内容保全存证	• 关键线索挖掘 • 事中证据固定 • 抓捕现场取证	• 检材梳理 • 司法鉴定 • 出庭质证

资质荣誉

资质认证

上海盘石司鉴

北京网神洞鉴

陕西洞鉴云侦

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

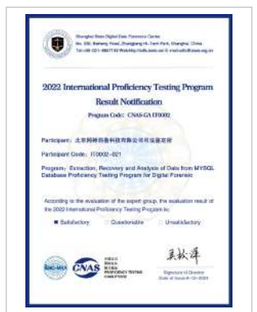
第二届“宋慈杯”
优秀司法鉴定文书评选 优秀奖

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

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