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

2023 年 第二版
电子数据司法鉴定典型案例集

传销诈骗 | 色情赌博 | 黑灰产业

网络入侵 | 知识产权 | 企业调查

www.qianxin.com

CONTENTS

目录

01

TELEMARKETING FRAUD

电信网络诈骗

APP 虚假服务诈骗案

“空气币”诈骗案

电信网络诈骗呈高发趋势，需全链条打击

近年来，电信网络诈骗频发，诈骗的形式也日新月异，不断出现新的手法和新的变种，它们依托于现代科技与网络手段，深藏在复杂的网络交易中，极大地提升了侦查难度。

在此过程中，电子数据司法鉴定起到了关键作用，其通过数据分析、功能鉴定等专业技术手段，协助警方定位犯罪团伙、确定涉案金额、提供重要的证据支持，对于打击电信网络诈骗犯罪，保护公众权益具有巨大价值。

例如，在上海警方侦破的一起亿元级的 APP 虚假服务诈骗案中，就是通过电子数据司法鉴定，对软件功能性进行了精准鉴定，揭示出其并未实现承诺的服务。而在另一起涉及“空气币”的诈骗案中，电子数据司法鉴定在追踪开发团队、固定关键证据等多个环节中起到了重要作用，形成了清晰、完整的证据链，对破案起到了关键性的推动作用。

APP 虚假服务诈骗案

揭开亿元诈骗案背后黑幕：虚假街景与盲盒骗局

近期，上海警方侦破了一起手机软件新型诈骗案，涉案金额达上亿元。在此案中，奇安信技术团队为其提供了关键技术协助，鉴定人通过对多款软件进行功能性鉴定，证明了相关软件并不具备承诺的服务，同时，对相关交易数据进行了统计、分析，助力警方确定了受害人数据及其非法获利金额，保护了受害人的权益并维护了社会的公平正义。

案件背景

一名群众报案称，其被广告吸引而购买了一款手机软件，宣称能提供全球实时街景，但实际使用发现与广告描述不符。警方调查发现该软件的注册企业是一家空壳公司，资金流向某涉案企业，进一步调查发现，与涉案企业有关联的空壳公司多达 50 家，都从事类似虚假服务诈骗业务。这揭示了一个专门开发手机软件骗取用户财物的犯罪团伙，警方决定展开收网行动。

在这类新型网络诈骗案件中，由于隐蔽性较强，最终认定非法获利数目会远低于涉案金额，并且难以确定实际受害人数目，在后续的审查起诉环节面临诸多困难。

奇安信解决方案

鉴定人对涉案服务器内数据进行了仔细分析，提取到了盲盒、街景相关交易数据表格近 20 张，为后续量刑提供了坚实证据。具体分析过程如下：

1. **服务器镜像仿真：**通过计算机仿真系统，分别模拟了盲盒、虚拟街景相关数据库的镜像环境；在模拟环境中，添加桥接模式网卡，通过 FinalShell 远程连接虚拟机；最后，在终端执行切换用户、重置日志和启动数据库等操作，确保系统环境正常运行。

2 交易数据导出：使用数据库管理软件连接到数据库，并打开 "discount_production" 数据库。使用特定的 SQL 语句从数据库中导出与订单、退款相关的交易数据。

ID	公司名称	实付金额	订单状态	支付类型	退款状态	手机号	扩广渠道	.....
1	*** 鼠	98	支付成功	apple	待审批	175****0365	苹果官网	
2	*** 鼠	128	支付成功	apple	审批成功	185****0975	苹果官网	
3	*** 鼠	68	支付成功	alipay	无	139****2456	头条信息流	
4	*** 鼠	118	支付成功	weixin	无	176****2712	头条信息流	
5	*** 鼠	68	支付成功	alipay	无	156****2514	苹果官网	
6	*** 鼠	68	支付成功	weixin	无	159****6751	头条信息流	

3 街景功能鉴定：通过对该功能的代码程序进行逆向工程分析，鉴定人揭示了其获取街景图像的原理，即通过调用百度地图的软件开发工具包（SDK）来实现。随后，鉴定人选择了一个特定地区进行功能复现测试，功能复现测试结果显示系统并不具备高清街景功能。

4 盲盒中奖率分析：使用 SQL 语句对数据库中中奖率相关的数据进行导出后发现，其设置的一等奖概率为零，存在虚假宣传嫌疑。

案例价值

01 / 揭露虚假宣传行为

通过对高清街景及盲盒功能的鉴定，我们发现该软件与其广告宣传描述存在明显差距，揭露了犯罪团伙的虚假宣传行为，加强了对其涉嫌诈骗的指控。

02 / 提供量刑依据

通过对涉案服务器的分析，我们成功提取了近 20 张盲盒和街景相关交易数据表格，这为后续的量刑过程提供了重要的依据，帮助警方确定犯罪分子非法获利的实际数额，并为受害者争取到合理的赔偿。

03 / 保护公众利益

警示公众，防止其继续受到虚假广告的误导和经济损失。我们的专业鉴定有助于维护市场秩序，促进诚信经营，对于预防类似犯罪行为具有积极的社会影响。

“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。

奇安信解决方案

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；

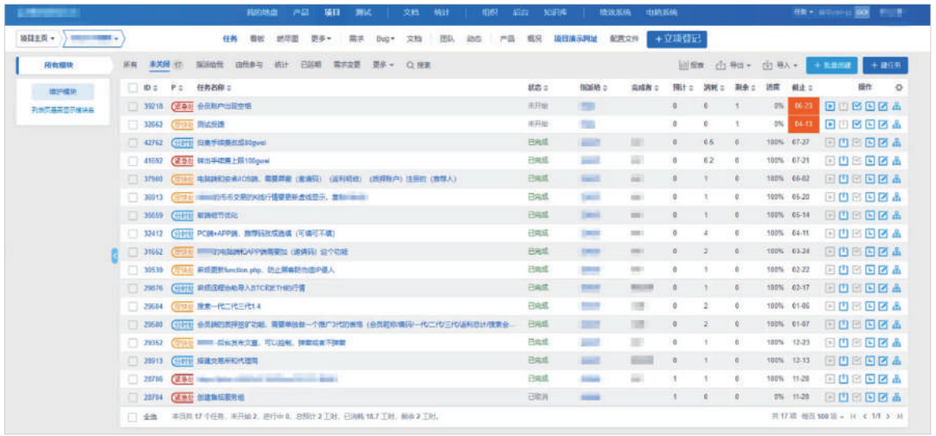
2 IP 地址获取：通过对涉诈 APP 的进一步分析，成功找到了其主控网站，奇安信技术团队配合警方，获取到登录者的 IP 地址，而这些 IP 地址，亦指向了“某博”企业所在地。

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了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。

ONLINE ILLEGAL BUSINESS

网络传销与非法经营

广西百亿传销案

镇江特大刷单案

大数据清洗厘清会员层级，电子数据鉴定助力打击

网络环境为传销与非法经营活动提供了新的发展空间与作案手段。此类犯罪往往涉及巨额资金和大规模会员体系，对社会的正常经济秩序构成了严重威胁。然而，由于其复杂性和隐蔽性，以及庞大的数字证据，使得传统的侦查手段在对抗这类犯罪行为时面临挑战。

电子数据司法鉴定技术的应用为这一问题的解决提供了新的路径，其能够通过对涉案数据库的深度分析，揭示犯罪团伙的运作模式与交易情况，为公安机关的侦查工作提供强有力的技术支持。

例如，广西传销案中，鉴定人通过解密千万级数据库，理清了该组织的会员层级关系与资金流向；镇江特大刷单案中，通过对涉案的 19 个刷单平台进行深度的功能性鉴定和数据分析，揭示了平台获利模式以及刷手获利情况，这不仅为侦查工作提供了关键线索，也为公诉机关的定罪量刑提供了强有力的证据。

广西百亿传销案

“千万级”数据库解密统计：揭示庞大交易记录与会员层级关系

2022 年 1 月，广西某地发生了一起涉及百亿人民币的传销案。在此案中，奇安信技术团队提供了从线索调查、案件打击到后期鉴定的全方位支持。特别是在司法鉴定环节，奇安信的鉴定人解密和分析了传销平台千万级数据库，其中包括数以百万计的账号以及其下属的层级关系和交易情况，成功揭示了这个传销网络的规模与运作方式，帮助全国各地公安打击该组织内打击对象超过 300 人。

案件背景

2022 年 1 月，某地经侦大队工作中发现，辖区内有人正在参与外汇网络平台投资活动，经过公安机关的缜密侦查，确认该平台以 “为用户托管炒外汇” 为幌子，实则经营模式为缴纳入门费、发展下线人员形成层级关系、推荐会员获得返利、分红，具有传销特征，涉嫌组织、领导传销活动罪。

该案件涉及千万级别的数据规模，同时数据库内交易相关的钱包地址进行了加密，取证鉴定挑战极大。

奇安信解决方案

鉴定人根据现勘报告对应数据库内字段含义，编写脚本计算该传销组织内的层级关系、积分及虚拟币交易情况，具体鉴定过程如下：

1. **还原涉案数据库：**通过哈希校验、文件解压缩、虚拟机创建、数据库安装、数据导入等多个步骤，成功还原了数据库中的数据表近 600 张，确保了数据表的完整、准确，为后续的数据分析和调查提供了基础。

2. **分析指定人员信息：**在数据表中查询该组织领导者（leader）信息，确定 leader 对应的 "member_id"，并根据该 ID 在数据表中查询并提取提现金额、加密交易钱包地址、提现类型、银行卡号等交易信息。

3. **解密加密钱包地址：**根据数据库里面记录的交易哈希，在虚拟币交易网站上查找交易哈希对应的交易记录，对被加密的钱包地址进行解密。

4. 计算会员层级关系：对该组织顶层用户 ID 进行遍历，计算出每个成员的层级关系，例如该组织的总成员数、最大层级数以及各个顶层 ID 下的成员数量。

5. **汇总平台交易情况：**通过撰写脚本，读取并统计每个会员的充币总数、充币次数、提币总数、提币次数以及充提币地址等信息，帮助警方了解交易频率和金额等情况。

用户 id	157631	176392	175293	279473
一级下属 id	'178231','178273'	'203721','873221'	'293021','364732'	'463521','674321'
级下属账号数	17	9	18	6
二级下属 id	'218231','348273'	'456321','895221'	'303021','394732'	'4543521','884321'
二级下属账号数	134	17	72	52
下属最大层级数	6	2	5	5
下属总账号数	1974	37	362	374
当前层级	7	8	8	8
充币总数	2354557.251	635683.0803	273427.2463	241481.999876
充币次数	80	34	7	27
身份证号	230xxxxxxxxxxx	210xxxxxxxxxxx	321xxxxxxxxxxx	131xxxxxxxxxxx
.....	.....	.....	.....	.....

汇总表部分信息（虚拟示意图，非真实信息）

总体而言，鉴定人通过数据库还原、解密数据库内的钱包地址、计算会员层级关系、虚拟币及积分交易情况等步骤，对涉案数据库进行了分析鉴定，并将相关数据整合生成了多个 CSV 文件，提供了关于该组织的成员信息、统计数据和记录条数等信息，帮助揭示了案件中涉及的关键信息和成员关系。

案例价值

01 / 技术支持与创新

奇安信通过全方位的技术支撑，为公安机关提供了准确全面的犯罪线索、情报支持，并协助进行了追踪工作，帮助公安机关在数据分析和犯罪侦查过程中实现技术突破。

02 / 关联分析和追踪

通过整理和分析涉案数据库，提取到会员的层级关系、转账记录、充提币情况等信息，帮助公安机关识别了传销组织的核心成员与资金流向，进一步掌握犯罪证据。

03 / 维护社会稳定

在本案中，奇安信助力公安机关共同打击传销犯罪，通过对传销组织的侦破和取缔，可以阻止其扩散和对更多人造成伤害，维护社会的正常运行。

镇江特大刷单案

科技揭秘：40 亿元涉案金额背后的刷单“联盟”

2022 年，一宗横跨江苏、重庆、福建等地的特大网络刷单案成功告破，涉案金额达到 40 亿元。在此案中，奇安信的鉴定人对涉案的 19 个刷单平台进行了深度的功能性鉴定，对其背后的复杂数据进行了精细的统计与分析，包含店铺数量、刷手数量、分站数量以及商家充值状况等诸多要素，揭示了平台获利模式以及刷手获利情况，为此案的合法定罪与量刑提供了强有力的证据支撑。

案件背景

“刷单”是指通过虚构的购买行为、虚假的评价和过度的销量来误导消费者，使商家获得不公正的竞争优势。2019 年 7 月至 2021 年 4 月期间，赵某等人，搭建了多达 19 个刷单平台，利用分层诱导、定向诱导等策略，煽动普通消费者参与虚假刷单等违法行为。此过程中，进行了接近 3300 万次的有效刷单，涉案金额达到了惊人的 40 亿元。

这个案例的复杂性在于其涉案金额巨大，涉及人员众多。面对数千万笔的交易记录，如何从中确认犯罪金额？案件该如何定性？梳理涉案平台交易数据成为棘手难题。

奇安信解决方案

鉴定人对涉案刷单网站共计 19 个，逐一进行了功能性鉴定与数据分析，以其中一个平台“小 **”为例，介绍具体鉴定步骤：

1. **网站重构：**从数据库备份文件和镜像文件中导出网站的源代码，并在本地的虚拟机中重建网站。由于涉案数据库中用户密码字段被加密，鉴定人修改了网站代码中的登录验证逻辑，成功登录网站后台。
2. **数据库分析：**在网站成功重建后，通过数据库日志分析，获取了查询数据库的语句，如查询用户信息、订单记录、店铺数量等。通过记录和运行这些语句，鉴定人对相关网站的交易数据进行了详细的统计和分析，包括店铺数量、刷单者数量、分站数量、刷单者收入和商家充值状况等。

平台名称	总店铺	总刷手	有效店铺	有效刷手	分站代理数	有效分站代理数	分站总刷单数
小 **	1,034	8,654	879	6,398	16	54	149,051

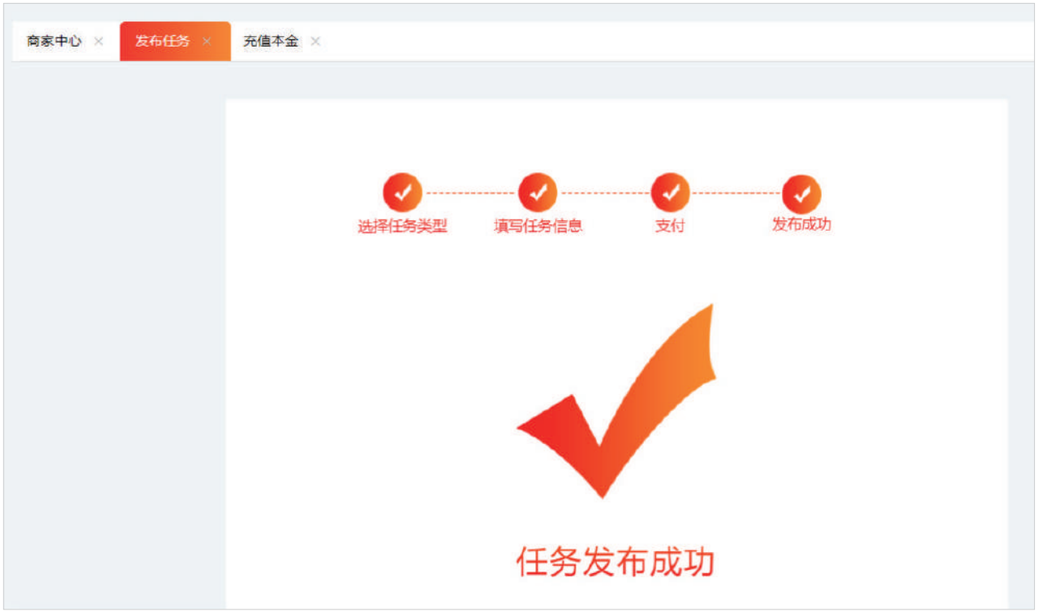
分站提现总金额	有效总单数	刷单总本金	刷单总佣金	平台总获利	刷手总获利	分站总获利
50,456.8	145,654	9,124,413.1	567,876.08	654,134.76	246,222.71	98.864.65

平台交易情况统计（虚拟数据，非真实数据）

商家剩余本金	商家剩余佣金	商家剩余冻结金额	商家充值总本金	商家充值总佣金
60,432.1	6,736.6	6,817.5	8,543,841.4	24,300

平台交易情况统计（虚拟数据，非真实数据）

3. **功能分析：**鉴定人对网站功能进行了动态复现分析，包括“管理后台”具备查看用户信息、交易明细、修改佣金等功能；“卖家中心”具备充值、发布任务、添加店铺等功能。同时，对网站源代码进行了静态分析，通过查看结算相关代码，确认其佣金机制，并对佣金交易记录进行了导出。



发布任务功能

案例价值

01 / 提供数据依据

此案件涉及的交易记录高达数千万条，是一个极为庞大的数据量，通过准确地定位关键数据并进行深入分析，确认了犯罪金额，为公安机关的进一步调查和判决提供了关键数据依据。

02 / 揭示刷单网络

本案中涉及 19 个刷单平台，通过对相关平台的核心功能鉴定与数据分析，揭示了平台获利模式以及刷手获利情况，帮助公安机关洞察网络刷单犯罪的运行模式和利益链条。

03 / 维护公平竞争

网络刷单行为破坏了市场的公平竞争环境，误导消费者，损害了诚信商家的利益，成功打击这起特大网络刷单案，有助于维护市场经济的公平秩序。

03

SOCIAL GOVERNANCE

色情赌博与社会治理

“8·31”传播淫秽物品牟利案
打击“涉黄视频”网站案
跨境网络赌博案
AirDrop 恶意传输案

色情赌博网络犯罪加剧，技术突破助力维护网络秩序

现代社会，犯罪分子利用网络的匿名性、即时性和跨界性，以传播淫秽物品、建设色情赌博网站等方式进行犯罪活动，严重损害了社会公序良俗和公民合法权益，也给社会治理带来了巨大挑战。

首先，网络的发展使得这类犯罪具有了更强的跨地域性与隐蔽性，如在“8·31”传播淫秽物品牟利案、打击“涉黄视频”网站案与跨境网络赌博案中，犯罪团伙散落在全国各地；同时，技术的进步也让这类犯罪更加复杂且多样化，有部分犯罪团伙使用 AirDrop 恶意传输非法言论。

在上述案件的侦破过程中，奇安信司法鉴定起到了关键作用，一方面，其为警方提供了全流程的服务，包括前期线索挖掘、中期证据固定、后期司法鉴定等，提升了侦查效率，也提高了证据的法律效力；另一方面，面对犯罪手法复杂、追踪难度大的案件，其不断加大研发力度、创新治理模式，以协助警方达到更好的网络治理效果。

“8·31”传播淫秽物品牟利案

上千部视频铁证固定：多地高效响应，精准打击网络色情犯罪

2020 年底，上海查办“8·31”传播淫秽物品牟利案。在此案中，奇安信技术团队配合警方完成网站打击，协助警方定位至嫌疑人窝点，涉及广西、广东、湖北、江苏、福建等多地；并在展开集中收网时，配合警方进行多地现场证据固定，共计搜集手机、电脑等检材 80 余部，固定色情视频上千部，为案件的依法处理提供了有力支撑。

案件背景

2020 年 8 月，上海警方在工作中发现了几个涉嫌提供色情短视频下载与观看服务的 APP，并立即成立专案组调查。随着深入调查，一个庞大的犯罪团伙逐渐浮出水面：黄某、郭某等人合谋开发色情网站，并在多地招募技术团队，相继开发并上线了多款色情软件，其视频总量超过 10 万部。在此案中，警方一方面需要面对多地联合取证问题，一方面需要应对庞大淫秽视频固定问题。

奇安信解决方案

在此案中，奇安信技术团队提供了前期线索挖掘、中期证据固定、后期司法鉴定的全流程服务，为案件的侦破和定性提供了坚实的支撑，以下是具体过程：

1. 前期 → 线索挖掘

协助警方完成对色情网站的打击，获取了涉案服务器后台的权限，并在其中发现了宝贵的线索，包括会议总结、工资记录等。警方通过这些线索，对嫌疑人进行摸排定位，最终确定了嫌疑人的位置。

2. 中期 → 证据固定

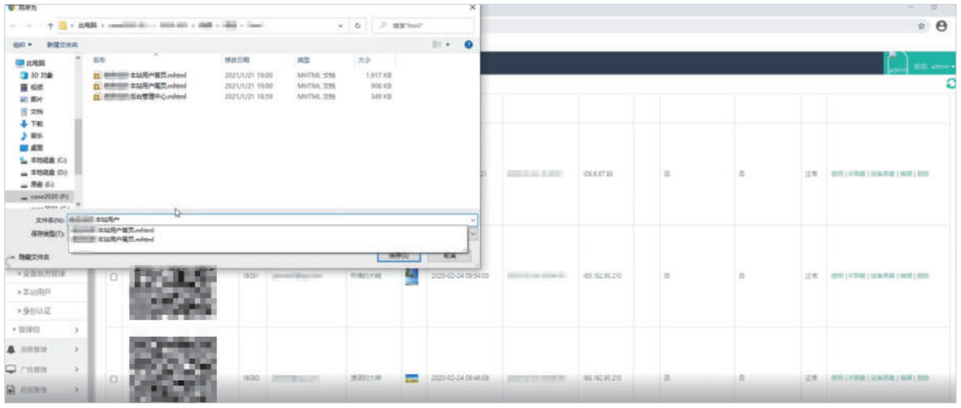
奇安信具备遍布全国的服务体系，在此案中，共计 10 名技术专家前往各地，协助现场证据固定及取证工作，共计收集 80 余部手机、电脑等检材，并固定了上千部色情视频。

3. 后期 → 司法鉴定

鉴定人对现勘中获取的视频进行了进一步鉴定，下载固定一定数量的涉黄视频；同时录像固定涉案人员使用的即时通讯软件，记录聊天记录、图片和视频等信息。全面固定和提取了涉案证据，为案件的依法处理提供了可靠的技术支持。

0a511153b7f5d94...	2020/12/8 13:37	MP4 文件	56,717 KB	00:05:13
0bced933458e67f...	2020/12/8 13:35	MP4 文件	89,911 KB	00:10:00
1c39c0f3557ba38...	2020/12/8 13:35	MP4 文件	10,502 KB	00:01:57
5fe3161b485341b...	2020/12/8 13:31	MP4 文件	3,693 KB	00:00:59
06e2cd85baf1f3a...	2020/12/8 13:40	MP4 文件	12,744 KB	00:01:31
15f8d5ade5859d2...	2020/12/8 13:37	MP4 文件	4,083 KB	00:00:14
17e1d5345c6c3e4...	2020/12/8 13:33	MP4 文件	6,646 KB	00:00:46
23f679f83093a18f...	2020/12/8 13:40	MP4 文件	6,823 KB	00:00:23
156dec72ace0680...	2020/12/8 13:40	MP4 文件	994 KB	00:00:13
347a70cd404d9d...	2020/12/8 13:40	MP4 文件	78,769 KB	00:04:28
714a8ec8c69b37d...	2020/12/8 13:36	MP4 文件	4,392 KB	00:00:36

部分固定视频



网站固定

案例价值

01 / 关键线索和情报支持

通过深入挖掘线索和进行网络情报分析，为公安部门提供宝贵的情报支持，帮助他们快速锁定嫌疑人的位置和行动轨迹。

02 / 多地取证和现场支持

协助公安部门多地抓捕，并帮助其快速获取关键证据，确保证据的完整性和可靠性，为案件的成功侦破提供了坚实的基础。

03 / 保护社会稳定和公众安全

网络淫秽犯罪严重侵害了公众的合法权益，扰乱了社会秩序。此次合作有效打击了犯罪团伙，阻止了淫秽内容的传播，维护了社会的道德底线和公众的身心健康。

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。

奇安信解决方案

在此案中，奇安信司法鉴定已陆续出具 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，奇安信司法鉴定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

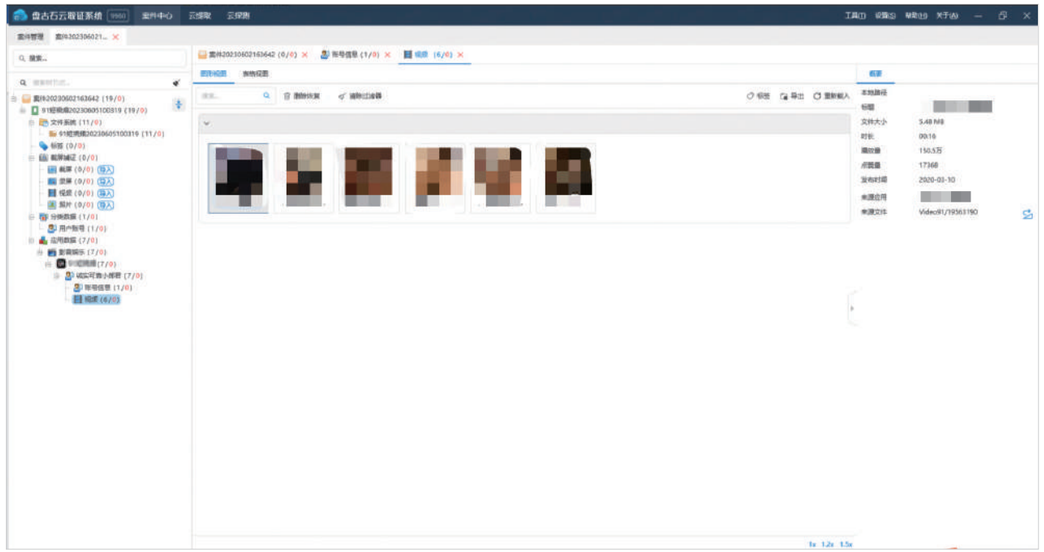
对涉案服务器后台用户数据进行分析转换，并统计，最终出具涉案账号总表，包括粉丝数、关注数、作品数、获赞数等信息。

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。

跨境网络赌博案

百份报告定性定量分析，揭示赌博代理与跑分团队的运营模式

2021 年，一起涉及特大跨境赌博网站的案件在信阳市浮出水面。奇安信司法鉴定接受委托，对该网站展开深度定性分析。同时，还对涉案赌博代理和跑分人员的相关交易信息进行了详细的定量分析，编制并出具了百余份鉴定意见书，帮助公安机关理清涉案团队的组织架构、运营模式以及资金流向，为追踪、打击相关犯罪团伙提供了有力支持。

案件背景

2021 年，一名群众报警，声称他在一个赌博网站上输掉了近 16 万元。此事引起了当地警方的高度重视，并成立了打击跨境赌博专项治理专案，对该案件进行全面调查。经过警方缜密侦查，成功掌握了该赌博网站赌博代理及跑分人员的相关信息，但涉案人员众多、复杂度高、数据量大，亟需专业技术团队协助。

奇安信解决方案

1 赌博代理统计分析

对百余名赌博代理账号信息进行了统计分析，包括梳理计算佣金的规则、统计其特定时间段内的佣金总额、及下级会员人数等信息等，对公安机关追踪和打击赌博活动提供了重要的参考信息。

代理号	统计时间	佣金总额
PA5**	“2017/6”至“2021/4”	1415200
PB5**	“2014/1”至“2020/10”	410600
PB5**	“2016/8”至“2017/8”	570100
PC5**	“2017/10”至“2021/2”	345700
PC5**	“2019/2”至“2021/3”	2202400

赌博代理佣金明细表（虚拟示意图，非真实数据）

2 跑分人员统计分析

将检材硬盘中的数据库备份文件导入本地数据库中，恢复并导出充值、提现记录，将充值 / 提现记录中的充值 / 提现时间、接收 / 出款方的银行账号、充值 / 提现金额与警方调取的银行流水进行比对，并统计金额。

收款人	收款银行卡	接收充值总金额
卢 **	623****3500****1776	771,378
马 **	621****3345****3467	477,764
孙 **	622****5689****2368	472,042
王 **	621****4395****5769	116,073
赵 **	621****4357****8774	255,343

跑分人员交易明细（虚拟示意图，非真实数据）

3 赌博网站功能鉴定

登录相关赌博网站，并通过功能复现对网站功能进行了鉴定，证实其具备赌博网站的典型特征，例如存款、投注和提款功能。

案例价值

01 / 提供量刑依据

详细的赌客和跑分人员信息帮助警方确定犯罪分子非法获利的实际数额，有助于公安机关能够在法庭提供强有力的证据。

02 / 节省时间资源

帮助公安机关理清了百余名跑分及赌博代理人员的资金流向及人员架构并对赌博网站进行了全面的功能性鉴定，节省了公安机关的时间与资源，使其能更聚焦于侦查等核心工作。

03 / 保护公众利益

网络赌博常涉及欺诈和诈骗，极可能导致公众财产损失。我们的合作有效打击了此类活动，维护网络安全和公共秩序，守护了公众的合法权益。

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事嫌疑人。

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。

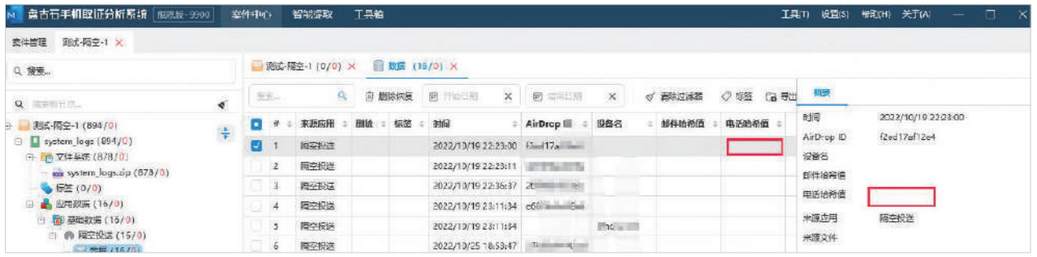
奇安信解决方案

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，奇安信司法鉴定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、准确地定位到涉事嫌疑人，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。

04

NETWORK INTRUSION

网络非法入侵

制贩黑客工具“刷机”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

犯罪分子通过利用系统漏洞或者植入恶意软件，非法获取、窃取、篡改网络中的信息，给个人隐私、企业财产乃至国家安全带来巨大威胁。在“制贩黑客工具‘刷机’案”和“新型打印机木马案”中，犯罪分子精心设计，通过开发先进的黑客工具和木马程序，进行精准的个人信息盗取和非法利益牟取。

其犯罪行为呈现出多样化、技术化和隐蔽性强的特点。首先，攻击手段日益翻新，黑客利用各类新型技术，不断提升入侵效果，普通防护措施难以阻挡；其次，黑客的攻击目标越来越具有针对性，对重要机构和系统的攻击事件屡有发生；最后，由于网络入侵的隐蔽性强，一旦发生，查清真相、找到犯罪者的难度较大。

面对以上挑战，电子数据司法鉴定发挥了重要作用。鉴定人通过深度技术手段，如程序逆向、行为监控、抓包分析，剖析攻击软件的工作原理，找出入侵犯罪的线索，有力地支持了打击网络犯罪的行动，提升网络犯罪的查处效率，为企业与国家的网络安全保驾护航。

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。奇安信司法鉴定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。

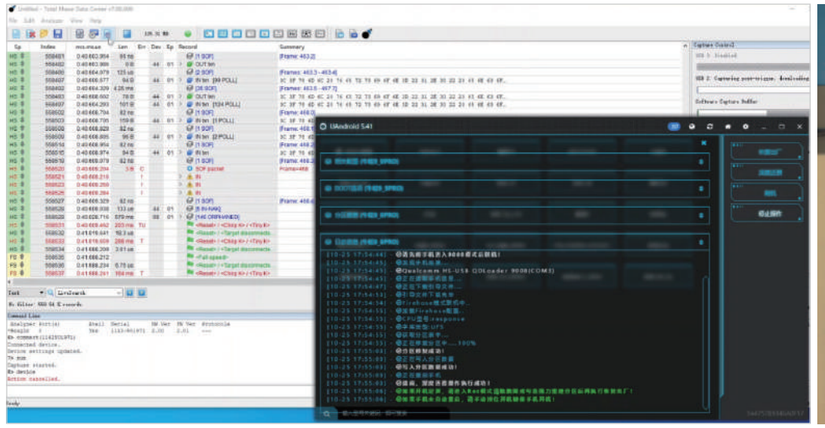
奇安信解决方案

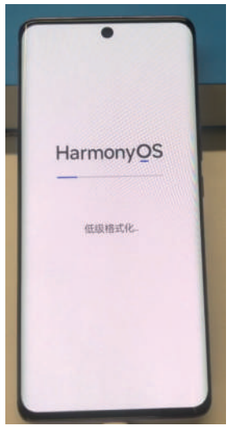
1. 获取验证服务器地址

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。

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

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；犯罪手段高度技术化、专业化，犯罪团伙运用虚拟币交易、使用境外聊天工具等手段逃避侦查，给打击网络黑灰产工作带来了巨大挑战。

然而，无论网络黑灰产的形式如何多变，手段如何狡猾，其犯罪行为都会在电子数据中留下痕迹。电子数据司法鉴定在打击网络黑灰产中，起到了关键作用。

例如，在云南“猫池”案中，奇安信技术团队通过网络流分析、大数据挖掘、资金分析等专业技术手段，摸清了接码平台运营情况及组织架构。此外，在处理非法爬虫、手机霸屏广告和外挂抢红包等案件时，通过对涉案程序的深度剖析，提供了关键电子数据证据。

BLACK MARKET

网络黑灰产

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

图上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。

奇安信解决方案

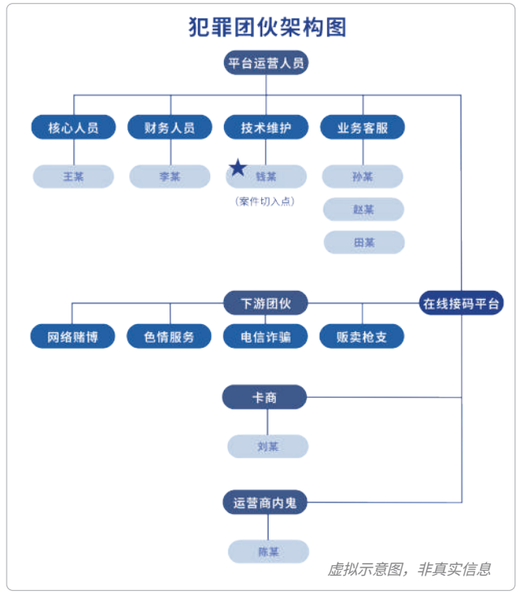
01 案中：固定上百台“猫池”证据，揭秘背后控制团队

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。



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。

案例价值

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。

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

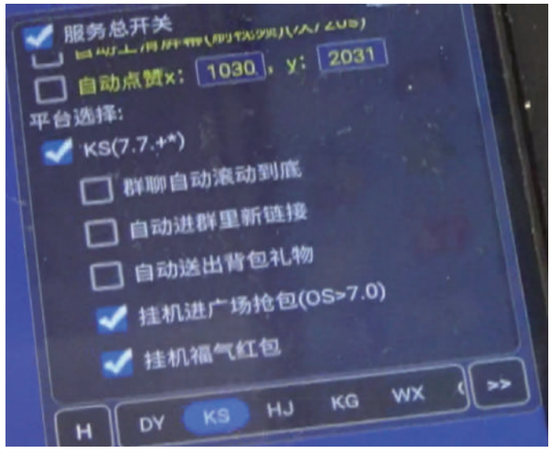
2021 年，该企业发现 5 个账户利用多台手机设备，通过外挂程序在各个直播间轮流抢主播发的红包近 2 万元，抢到的红包再集中打赏给某主播提现。这一行为严重扰乱了平台的秩序，影响了用户体验，该企业立即报案，并寻求专业的电子数据司法鉴定对相关外挂程序进行深入剖析。

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间执行抢红包操作。



代码反编译

2. 程序逆向分析

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

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

案例价值

01 / 提升用户体验

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

02 / 维护平台秩序

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

03 / 维护商业利益

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

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

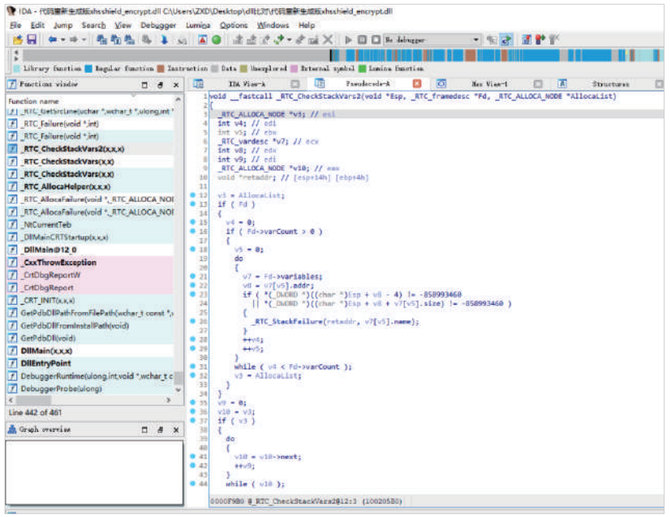
2022 年，一款程序对某企业的 APP 构成了威胁。这款程序破解了企业的加密算法和端口，绕过了其设立的风控措施，自动爬取了服务器上大量的用户数据，并控制帐号无限制发送私信，严重侵犯该企业权益。因此，奇安信司法鉴定受该企业委托，对网上售卖的“破解程序”及嫌疑人电脑进行了司法鉴定。

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。

案例价值

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

案例价值

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。

06

IP INFRINGEMENT

知识产权侵权

侵犯文学作品著作权案

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、源代码反编译等技术手段，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。

侵犯文学作品著作权案

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，涉案金额高达 2.8 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，且均与一名杜姓男子有关。

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 内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

案例价值

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。

07

CORP. INVESTIGATIONS

企业内部调查

员工系列违规案

面临数据泄露隐患，电子数据鉴定维护企业信息安全

在当今商业环境中，信息和数据已成为企业的生命线。从技术机密、内部策略，到研发资料，都是企业竞争力的核心所在。但随之而来的信息安全挑战，尤其是来自企业内部的威胁，却对企业构成了巨大的风险。这些内部风险，如员工或高管通过职务之便获取、泄露或销毁企业机密，常常因其难以被追踪且行为隐蔽，给企业带来重大损失。

在这一背景下，电子数据司法鉴定显得尤为重要。通过专业的数据恢复、代码审查、数据库分析等技术，鉴定专家能够深入犯罪现场，还原事实真相。例如，在员工系列违规案中，鉴定人追踪了长达五年的复杂内部犯罪行为，不仅解决了数据恢复、线索追溯的技术难题，更为法庭提供了确凿的证据，展示了电子数据鉴定在应对技术犯罪中的关键作用。

而电子数据司法鉴定的应用并不仅限于此。它还可运用于企业内部的其他调查场景，如员工不当行为调查、网络安全事故调查，甚至合规性审核等。借助这一专业技术，企业可有效维护信息安全，保护核心资产，并提升风险管理水平，以应对内部威胁带来的挑战。

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。

案例价值

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。

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：

辅助刑事案件侦查

协助揭示犯罪事实、找出关键证据、定位犯罪嫌疑人，极大提高了侦查效率和准确性；且通过确认电子数据的有效性，为司法机关提供有力证据支持。

行政执法与处罚

为行政机关提供电子数据取证服务，如网络违规行为的证据获取、非法内容的溯源追踪等，帮助行政机关进行有效的行政执法和处罚，保障社会公平公正。

内部调查与知识产权保护

帮助企业找出可能的数据泄露情况，提供证据来追究泄密者的责任；当企业面临知识产权争议时，帮助企业证明其权利的合法性，保护其合法权益。

网络黑灰产打击

为执法机关和企业提供网络黑灰产的取证、追踪与分析服务，揭示网络黑灰产的运作模式，有效打击网络黑灰产，维护网络空间的清朗。

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

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。

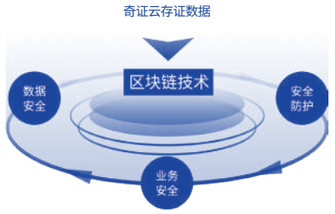
产品优势

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。

应用场景

数据产权确权登记

提供丰富的接口服务，实现数据产生即存证，并可在线申请存证证书。在确权登记时，可有效地验证合法获取数据的来源与时间点。

商业秘密保护

对商业秘密进行提前存证，确保每一份数据的权属明确与证据完备。当纠纷出现，利用预存证据，便可实现快速、有力的取证与举证。

直播电商治理

对常见直播电商平台数据进行智能分析，自动、批量识别违规线索。捕获的违规证据将被实时固定，并存证上链，确保证据难以篡改。

执法流程合规

通过深度融合执法业务系统，保证执法记录全程上链可追溯，从而保障执法过程的透明性和公正性，为之后的查验与审计提供有力支撑。

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

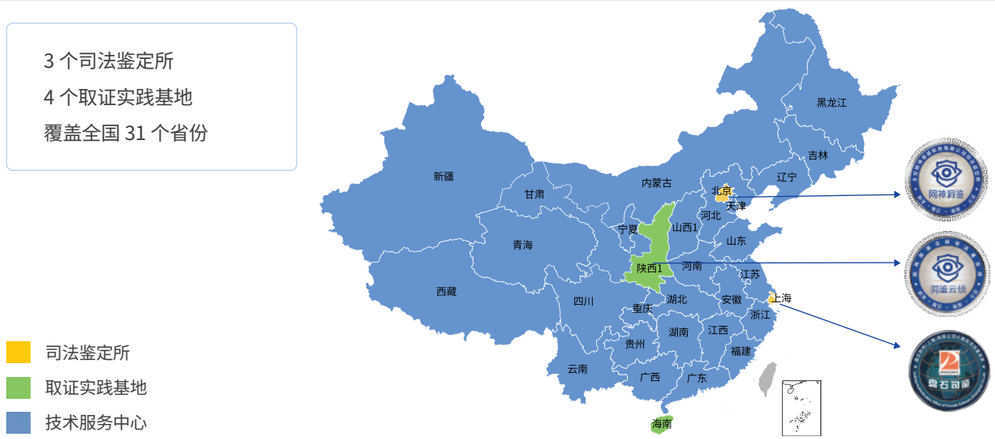
奇安信集团

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

- 商业秘密存证
- 数字知产确权存证
- 违规内容保全存证

事中

- 关键线索挖掘
- 事中证据固定
- 抓捕现场取证

事后

- 检材梳理
- 司法鉴定
- 出庭质证

资质荣誉

资质认证

上海盘石司鉴

北京网神洞鉴

陕西洞鉴云侦

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

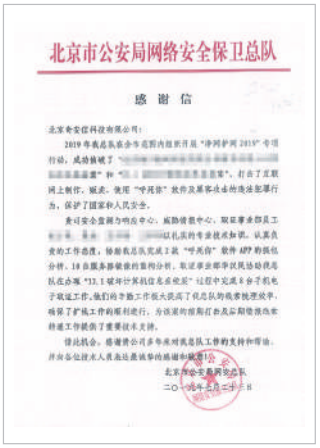
协助侦破重大疑难案件


中华人民共和国公安部

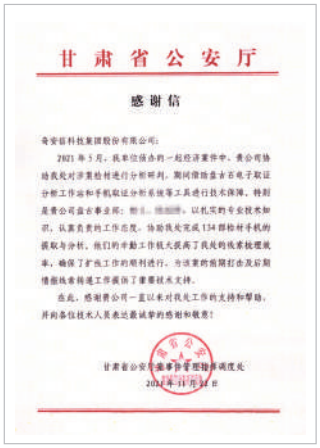
感谢信


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

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