合同纠纷谁在说谎? 追尾事故真相如何? 黑客攻击证据在哪?

鉴定专家让电子数据“开口说话”

鉴定人名片:胡斌

浙江千麦司法鉴定中心电子数据鉴定室负责人、声像资料(电子数据)鉴定人。30年来一直从事声像资料技术工作,参与各类刑事、治安、交通案件侦查(调查)数千起,各类案件技术分析、检验鉴定数百起。

本报记者 陈赛男

一条微信聊天记录揭开事实真相,一个货车“黑匣子”还原事故现场,一款“游戏”软件锁定犯罪事实……这些听起来只在影视剧中上演的情节,如今却真实地发生在我们身边。

随着互联网的不断普及与智能手机功能的不断提升,人们生活的足迹逐渐从线下向线上转移。小到衣食住行,大到金融法律,几乎所有的行为都会在互联网上留下记录,成为电子数据。而这些看不见摸不着的电子数据,在众多犯罪现场,往往会成为唯一的“知情人”。

一条微信聊天记录揪出谁在说谎

今年上半年,杭州某房地产开发公司A与市民赵先生对簿公堂,原因是一场购房合同纠纷。

早些年,赵先生看中了A公司出售的两个商铺,并很快与其达成购房协议。随后,赵先生先行支付了部分房款,但是在支付尾款时产生了争议。

赵先生要求,A公司帮忙办好商铺产权证书后,才支付剩下的房款。而A公司认为,按照相关行业规则,赵先生必须支付全额房款,公司才能开具全款不动产发票,再办理房产产权证书。

一时间,双方争执不下,商铺迟迟无法完成交易。

为了促成这笔交易顺利完成,A公司多次通过微信,与赵先生进行协商。最终,A公司同意赵先生的要求,但双方必须签订一份补充协议,约定赵先生必须在办出产权证书后10日内支付尾款……当天,A公司将这份补充协议通过微信,成功发送给赵先生。

可是,协议发出后,A公司没有收到赵先生的答复,却收到了法院的传票。

原来,赵先生以A公司不配合办理产权证书、侵犯其合法权益为由,将A公司告上法院,要求A公司支付相应的赔偿款。

A公司认为,自己已经尽到了配合办理产权证的相应义务,反而是赵先生对公司发出的补充协议不予理会,导致合同关系破裂。可是,赵先生矢口否认收到该微信消息,更糟糕的是,当初双方的微信聊天记录已经被清理。

A公司无力举证,案子交到了浙江千麦司法鉴定中心的电子数据鉴定专家胡斌手中。

幸运的是,因为记录删除时间不算长,通过一系列技术手段,胡斌发现,A公司相关人员手机缓存空间里尚存有部分微信聊天记录,其中一条正是A公司提到的文件名为“补充协议西-102、103.doc”的微信发送消息,发送时间、文件大小、接收者名称均有明确显示。

然而,让鉴定专家犯难的是,这个文件已经失效,无法读取其中内容。这意味着无法证明这份文件就是A公司所说的补充协议。

“我电脑中存有这份文件的原始文件,上面内容非常清楚。”A公司表示。可是谁又能证明微信发送的文件与电脑里存档的文件是同一个?

不甘心的鉴定专家再次对恢复的微信聊天记录进行深度数据分析,意外地找到了这份文件的哈希值。

哈希值,就是电子文件的“身份证”,它是根据文件大小、时间、类型、创作者等信息计算出来的一段数据,且具有唯一性。只要文件发生变动,哪怕是多了一个空格,哈希值都会发生巨大变化。

也就是说,只要计算出电脑里原始文件的哈希值与微信中文件的哈希值相同,就可以证明两份文件的同一性。

结果不出所料,两个文件哈希值完全一致,从而证明了电脑里存档的文件正是微信中发送的文件,谁在说谎一目了然。

神秘“黑匣子”还原事故现场

很多人都知道,要弄清飞机失事的原因,必须找到飞机上的“黑匣子”。“黑匣子”的神秘正是在于其背后的数据。事实上,大货车上也装有类似的“黑匣子”。

去年3月份,在G60(沪昆)高速公路往江西方向,发生了一起严重交通事故。一辆仓栅式货车车头撞上了一辆重型半挂牵引车车尾。事故发生后,后车司机经医院抢救无效死亡。

一般来说,追尾事故中责任在于后车,但真相真的是这样吗?

交警调查发现,该路段既没有安装测速仪,也没有电子监控,且根据痕迹鉴定也无法最终判定事故原因。

两辆货车到底发生了什么?交警部门在事故车辆中找到了前车的汽车行驶记录仪,也就是我们常说的汽车“黑匣子”,可对车辆行驶速度、时间、里程以及有关车辆行驶的其他状态信息进行记录、存储并可通过接口实现数据输出的数字式电子记录装置。

浙江千麦司法鉴定中心对“黑匣子”进行鉴定时发现,这份检材不仅外观完好,且在接通电源后仍能正常启动。这意味着,“黑匣子”中存储的数据很可能成为事故现场的唯一“证人”。

果不其然,根据事故发生在2017年3月14日“6时50分许”这一信息,胡斌带着鉴定团队对前车的行驶记录仪在对应具体时间段的数据,进行详细分析,可知事故发生对应时段的车辆行驶状态:“6:49:52”时,行驶速度开始大于0km/h(起动),“6:50:43”时,行驶速度为43km/h(阶段最高速),随后于“6:50:56”减速至0km/h(停止)。

此外,鉴定人员还根据经纬度定位,对车辆行驶的路段进行锁定,排除了车辆处于上坡行驶的可能。由此证明发生事故时,前车速度明显低于该高速公路最低限速(60km/h)行驶,属于在高速公路上低速行驶。

随后,交警部门据此展开调查,证实了前车司机存在疲劳驾驶情况,在这起事故中负有不可推卸的责任。

一款“游戏”软件锁定犯罪事实

去年年底,温州市区一家公司的网站莫名瘫痪。后来经过公司技术人员检查服务器日志发现,在系统瘫痪的时间段,公司网站受到“洪水攻击”,就是有人利用计算机网络技术向目标服务器发送大量的无用数据报文,使得目标主机忙于处理无用的数据报文而无法提供正常服务的网络行为。

“很可能遭受了黑客的恶意攻击……”有了初步怀疑后,该公司果断报警。警方在梳理该案电子勘验数据时,发现了一个隐匿在背后的黑客徐某。

侦查发现,徐某通过网络认识了各类不法分子,并形成了“开发、销售、提供攻击”的黑色产业链,其本人发挥着核心作用。徐某首先组织人员开发非法远程控制工具,并通过这些工具在他人电脑内非法下载安装木马程序。这些电脑中了木马病毒后,徐某等人利用这些电脑进行门罗币挖矿、发动DDOS攻击、盗取电脑资料、买卖电脑控制权等多种犯罪行为,并从中非法牟利。

但是在办案取证中,警方遇到了难题,徐某为逃避法律的制裁,辩解称自己电脑内的软件一直无法正常使用。今年7月,胡斌团队接受公安部门委托,对徐某电脑中这些听上去像是游戏名的软件进行电子数据司法鉴定。经过鉴定人员的分析,一款名为“大灰狼”的软件,可对目标主机实现远程“屏幕控制”“键盘记录”“远程交谈”“文件管理”“消息发送”“显示打开网页”“注销”功能,该电脑中类似具有远程控制、攻击、挖矿的软件共有10款。此外,鉴定人员还从徐某的服务器中,提取了30多条网络交易信息,详细记录了徐某的犯罪事实。

鉴定者说:

随着信息化不断发展,修改后的刑诉法正式将“电子数据”入法,电子数据取证也具体到了个案,就是针对犯罪嫌疑人经常使用的电子设备而形成的“电子数据”进行侦查和鉴定,成功提取犯罪嫌疑人的电子设备里存有的通话记录、往来短信、银行转账等信息。这些电子数据,很可能为打击犯罪提供线索,并成为证据链条的关键部分,从而有效证明犯罪事实的发生。

目前,电子数据鉴定最为常见的主要有三类:存储类数据的固定、恢复、提取,软件功能性鉴定以及数据库类分析。在众多案发现场,电子数据经过鉴定就可以变身为“开口说话”的“证人”,让犯罪分子无处可藏。