安全小课堂第110期【网络取证技术】

京东安全应急响应中心 9月10日

随着云计算发展，相关犯罪活动越来越常见，面临这种情况，相关取证工作如何展开，如何确保数据的有效性等问题

JSRC **安全小课堂第110期**，邀请到来自湖南省天网电子数据司法鉴定中心**饶伟杰**作为讲师就**网络取证技术**为大家进行分享。同时感谢朋友们的精彩讨论。

网络取证技术的背景？

京安小妹

饶伟杰：

随着《网络安全法>的出台，凡是通过网络的形式对公民安全、社会安全和国家安全进行侵害的违法行为，都是网络取证所涉及的范围；网络取证技术是通过技术手段提取网络犯罪过程中在多个数据源遗留下来的日志等电子证据。并将证据形成证据链，依据证据链对网络犯罪行为进行调查、分析、识别，是解决网络安全问题的有效途径之中的一个。

讲师

网络取证技术分析的特点?

京安小妹

饶伟杰:

网络取证不同于传统的计算机取证，主要侧重于对网络设施、网络数据流以及使用网络服务的电子终端中网络数据的检测、整理、收集与分析。计算机取证属于典型的事后取证，当事件发生后，才会对相关的计算机或电子设备有针对性的进行调查取证工作。而网络取证技术则属于事前或事件发生中的取证。在入侵行为发生前。网络取证技术能够监测、评估异常的数据流与非法訪问。

讲师

网络取证技术的数据来源?

京安小妹

饶伟杰：

网络取证的对象是可能记录了网络犯罪过程中遗留下来的数据的多个网络数据源。一般使用Web 服务、云服务、PC和手机等智能终端设备）以及网络数据流。

讲师

网络取证过程中注意的问题？

京安小妹

饶伟杰：

（1）了解网络环境，制定相应的计划与实施方案；应防止网络环境的变化与人为干预，从而造成电子证据的更改或破坏；

（2）严格按照计划与步骤及时采集证据。依照数据源的稳定性从弱到强的顺序进行取证。

（3）不要在要被取证的网络或磁盘上直接进行数据采集。

（4）使用的取证工具必须得到规范认证。

（5）取证过程中最好有两名从业人员，并做到实时记录。

（6）取证的电子数据要进行哈希值的校验。

讲师

网络取证案例分析？

京安小妹

饶伟杰：

案例分析一：

在一起网络视讯版权纠纷案件中，乙方在网站播放甲方旗下具有独播权，且还未上映的视频，并在该视频内容做了一定的修改（水印、广告等信息）。在该起案件中我们将乙方相关的网站视频进行远勘取证：先使用录屏软件开始录屏并记录开始时间；其次在乙方相关视频页面播放并下载相关视频；然后统计乙方相关视频截至远勘时的播放次数；再截图有特殊含义的画面并计算下载的视频哈希值；最后结束录屏并记录结束时间；

案例分析二：

某拍卖平台，在交易拍卖过程中，有多名竞拍者掉线，以致于无法正常交易，从而造成损失。在该起案件中，我们应委托方的要求对交易平台进行了排查与分析，发现了交易平台存在弱口令和远程操控的问题。

该案件中委托方采用了vmware的架构搭建整个拍卖平台，将其vmware镜像文件导出为ovf与vmdk文件，以便进行环境还原；因多名竞拍者掉线，所以我们将防火墙与防毒墙路由器等日志一并导出保存；在全程录像中提取文件，计算sha-256值；在实验室将其环境还原，并对相关日志，进行提取分析，对网站进行漏洞扫描；日志分析中发现工作机中装有第三方商业远程控制的破解版，并发现大量境外IP连接记录；在网站后台发现弱口令漏洞。

案例分析三：

某传销组织在湖南短短两年时间，通过高收益、高回报等手段发展下线，形成了强大的传销组织架构。其传销组织具有会员人数多、涉案面广、涉案金额大等特点。在公安机关扣押会服务器后，通过虚拟机将服务器环境还原；在服务器后台管理页面发现8层层级，会员人数超过500万，遍布华南、华中各省；涉案金额高达上亿元；

案例分析四：

通过微信聚众赌博

网络赌博方式层出不穷，今天分享一例通过微信群聚众赌博案例。案例中庄家通过微信红包猜数字的方式进行赌博；在该案件中庄家采用深度编辑的聊天机器人对赌博群进行管理，部分机器人还带有外挂性质可以“免死”；在机器人相关日志中存在整个赌博的统计资料；在其相关人员的聊天记录中发现机器人按周月对相关赌博群进行汇总并提交给相关人员，在其聊天记录中发现销售/出租机器人的商家，通过监控数据录制过程录像，使用临时帐号与该人联系，申请试用软件，在传输软件的过程中抓取到对方公网ip地址。

互动问答环节：

1. 你们一般都是咋取证的 流程或步骤是啥样的呢?

讲师:

首先先要用录屏软件录屏记录录屏时间，通过抓包软件监控后台变化；
然后去涉案网站等地方查看相关页面，对一些页面功能做测试；
把一些网站的相关资料要下载的都下载完毕；
如有后台，通过技术手段拿下后台查看相关参数；
录像中对下载的文件，保存的抓包文件打包并计算hash值；
关闭录像时，记录录像最后时间。
这是一个大致的流程，详细的怎么规划还要根据案件来做。

2. 司法取证常用软件?

讲师:

目前国内用得比较多的是美亚柏科、磐石、效率源等综合性的软件。

3. 常见的网络赌博有哪些?

讲师:

网络赌博、网络诈骗现在接到的案子，包括了网站或者手机形式将传统的网络赌博搬到互联网上。
还有类似通过随机红包，但是庄家使用外挂性质保证胜率类赌博方式。
还有一些非官方的期货，货币交易类的,后台可以控制赔率，甚至不给你提现。

4. 在网络赌博案件中应该针对哪些数据进行侦查、取证?

讲师:

公安比较关注的是他们的涉案金额，会员数量等最直接的证据；
红包赌博中一般会采用聊天机器人管理其中就有涉案金额，各种统计记录；
网页赌博中，后台里会有第三方充值通道以便锁定涉案人员资金；
期货交易类，查看后台是否有胜率，判断是否属于赌博，提取交易订单，判断是否能提现；

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。
安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心