



ISC 互联网安全大会



360 互联网安全中心

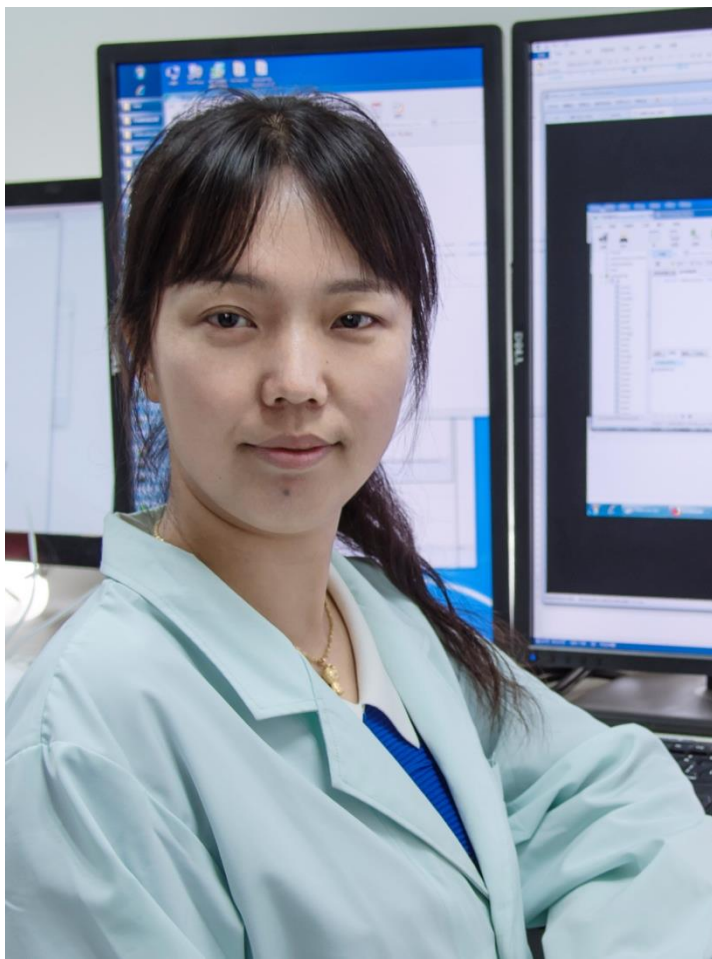
网络传销案件的取证与鉴定

郭弘 司法鉴定科学研究院副研究员

ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing · China

(原“中国互联网安全大会”)



报告人简介

司法鉴定科学研究院 副研究员

全国刑事技术标准化技术委员会电子物证分技术委员会 专家

上海市司法鉴定协会电子证据司法鉴定专业委员会 委员

公安部/司法部 能力验证专家

中国政法大学电子证据研究中心 特聘研究员

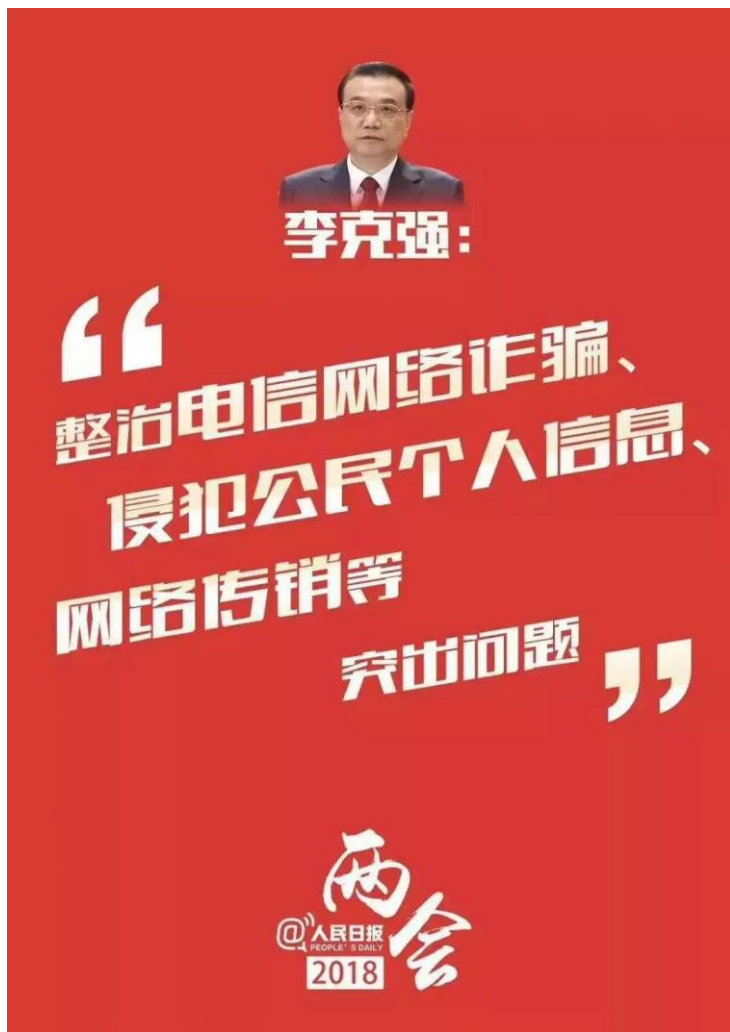
华东政法大学 兼职教授

国内网络传销呈现愈演愈烈的趋势



2017年度传销态势感知白皮书





2018年的《政府工作报告》明确提出：
推动重大风险防范化解取得明显进展。.....严厉打击非法集资、金融诈骗等违法活动；推动平安中国建设，.....整治电信网络诈骗、侵犯公民个人信息、**网络传销**等突出问题，维护国家安全和公共安全。



“要依法打击，紧紧围绕互联网金融领域非法集资、网络传销、违法交易场所经济犯罪、利用金融机构实施非法集资等突出犯罪，把人民群众反映强烈、社会影响恶劣、涉及人数众多的非法集资作为打击重点，依法精准打击，切实打出成效。”



国务院《禁止传销条例》

传销是指“组织者或者经营者发展人员，通过对被发展人员以其直接或者间接发展的人员数量或者销售业绩为依据计算和给付报酬，或者要求被发展人员以交纳一定费用为条件取得加入资格等方式牟取非法利益，扰乱经济秩序，影响社会稳定的行为。”

《刑法修正案(七)》

传销是指“指以推销商品、提供服务等经营活动为名，要求参加者以缴纳费用或者购买商品、服务等方式获得加入资格，并按照一定顺序组成层级，直接或者间接以发展人员的数量作为计酬或者返利依据，引诱、胁迫参加者继续发展他人参加，骗取财物，扰乱经济社会秩序的行为。”

通常满足这三点即可认定为涉嫌传销 A).交入门费 B).拉人头 C).
多层代理、团队计酬

网络传销与传统传销是双胞胎，它的得利方式同样是交纳会费(或说是享受产品)，然后再拉人进入作为自己的下线，这种方式与传统传销没有本质的区别。

- 1994年8月11日国家工商行政管理局**发出**233号《关于制止多层次**传销活动**违法**行为**的通告》（第一部**传销**管理法规性文件）。
- 1994年9月2日，再次**发出**240号《关于**查处多层次传销活动**中**违法**行为的通知》。
- 1995年3月28日，国家内**贸部办公厅**（今**商务部**）**发文**，宣布正式成立“多层次**传销**管理条例”立法工作机构，正式起草国家关于多层次**传销**管理办法。
- 1995年9月22日，**国务院办公厅**发出《关于停止**发展多层次传销企业**的通知》，以**对国内再次过热的传销进行规范限制**。
- 1998年4月，**国务院发布**《关于禁止**传销经营活动**的通知》。
- 2001年4月10日，最高人民法院作出了《关于情节严重的**传销**或者**变相传销行为**如何定性问题的批复》，将从事**传销**或者**变相传销活动**视为非法经营罪，并予以**刑事处罚**。
- 2005年8月23日，**国务院发布**《禁止**传销**条例》，自2005年11月1日施行。
- 2011年，刑法修正案增加了**组织、领导传销活动**罪。
- **2013年11月28日**，最高人民法院、最高人民**检察院**、公安部**联合发布**了《关于**办理组织领导传销活动**刑事案件适用法律若干**问题**的**意见**》。

新型网络传销的类型和主要模式

从类型来看，目前网络传销主要包括三种：传统传销的“网络版”、网络电商的“模仿版”、金融模式的网络传销。



网络在线提取

第六条 通过网络在线提取的电子数据，可以作为证据使用。

第九条 对于原始存储介质位于境外或者远程计算机信息系统上的电子数据，可以通过网络在线提取。

侦查实验

第九条 进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。

第十六条 对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时，可以进行侦查实验。

网络远程勘验

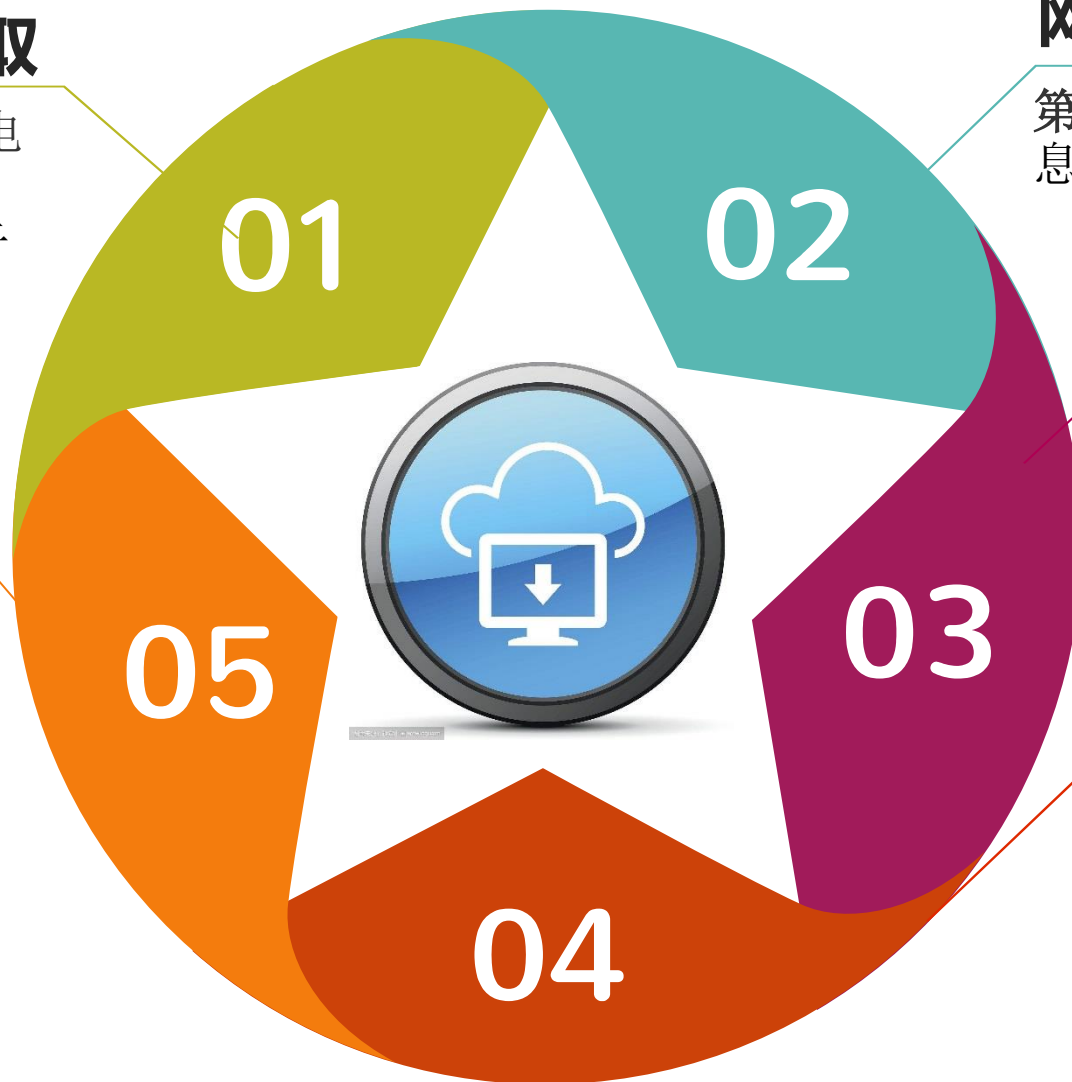
第九条 必要时，可以对远程计算机信息系统进行网络远程勘验。

冻结电子数据

第十二条 冻结电子数据，应当制作协助冻结通知书，注明冻结电子数据的网络应用账号等信息，送交电子数据持有人、网络服务提供者或者有关部门协助办理。

调取电子数据

第十三条 调取电子数据，应当制作调取证据通知书，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。



1、镜像验证

- CRC-64-ECMA \neq CRC-64，使用OssUtil工具

2、云镜像的仿真

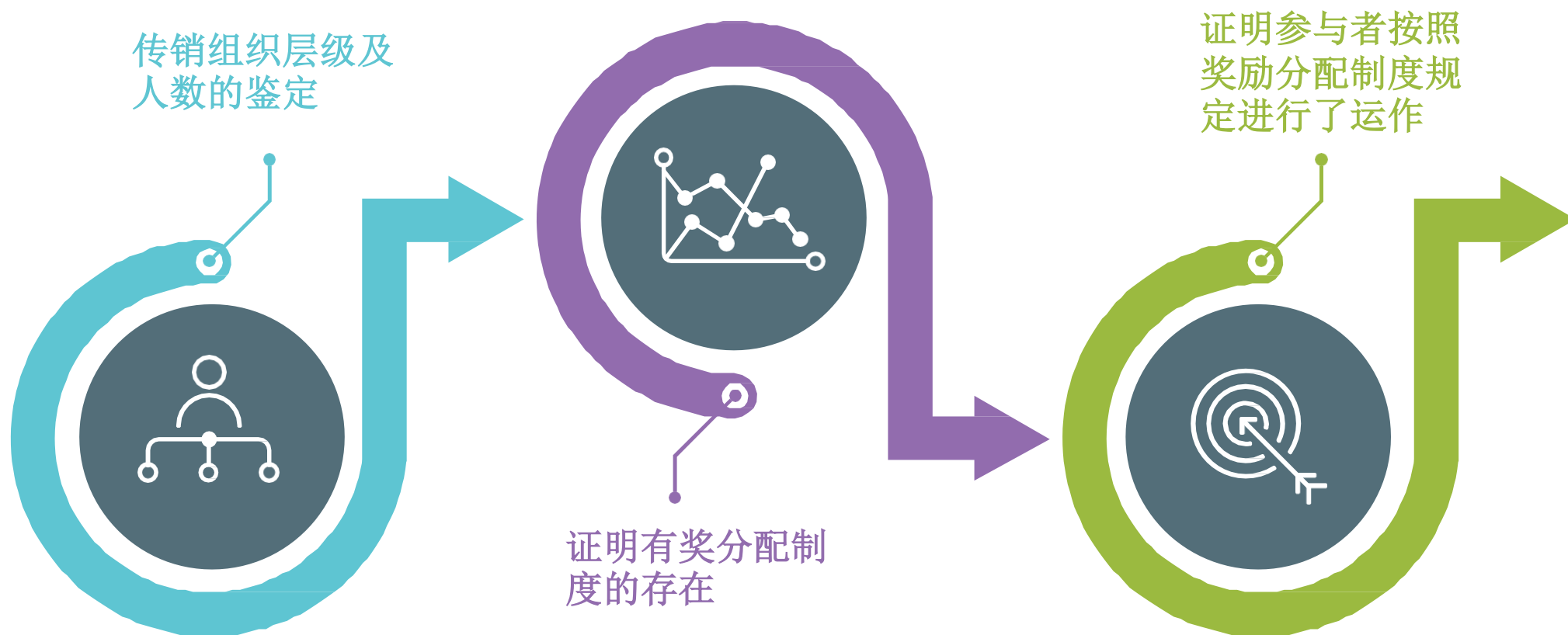
- 镜像格式的转换
 - raw : `qemu-img convert -f raw xxx.raw -O vmdk xxx.vmdk`
 - Qcow2 : `qemu-img convert -O vmdk xxx.qcow2 xxx.vmdk`
- 操作系统密码破解/重置
- 注意IP映射问题
- 多服务器的联调

3、web源代码分析

4、数据库的手工重建



网络传销案件鉴定的要点



网络传销案件取证鉴定的难点

1

取证周期长，调取证据的手续繁琐

取证要求高，证据链条的构建也相应复杂

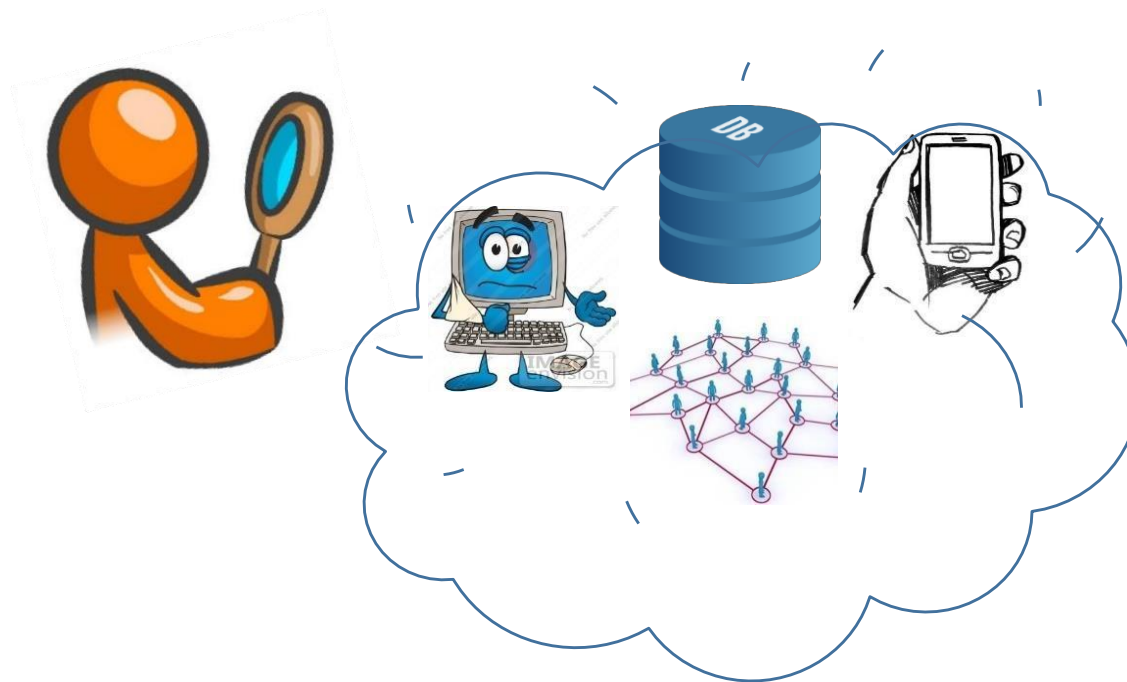
2

3

取证工作量大，云端证据分布广，获取难度大

4

嫌疑人作案手段日新月异，反取证意识增强



请提醒你身边的人，
擦亮双眼，提高警惕，
以免人身财产受到伤害。



ISC 互联网安全大会



360互联网安全中心

谢谢！

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing · China

(原“中国互联网安全大会”)