ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

新型网络犯罪取证的困境与对策

——以全国首例利用苹果平台退款诈骗案件为例

张璇

山东警察学院

网络空间安全与执法协同创新中心

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

2016.7全国打击治理电信网络新型违法犯罪专项行动推进会

- 破获电信网络诈骗案件5.7万起
- 查处违法犯罪人员2.8万名
- 捣毁诈骗窝点4300余个
- 收缴赃款、赃物折合人民币13.6亿元
- 为群众避免损失25.3亿元

将电信网络诈骗案件一律立为刑事案件

电信网络诈骗犯罪都是系列案件、团伙案件、跨区域案件，无论案值大小，都符合立案条件。各地公安机关接到群众电信网络诈骗案件的报案后，一律都立为刑事案件，按照刑事案件立案要求采集各类信息。

以审判为中心的诉讼制度改革

案件事实清楚，证据确实、充分

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

电信网络新型违法犯罪

- 高发态势
- 犯罪手段屡屡翻新
- 产业链复杂完善
- 侵财型案件多发
- 地域性特点
- 跨地域作案

手法新

技术新

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

取证面临的困境：

- **反取证意识强**
- **取证涉及的环节多、机构多**
- **证据链条构建复杂**
- **新技术新手法无从下手**
- **调取证据机制问题**

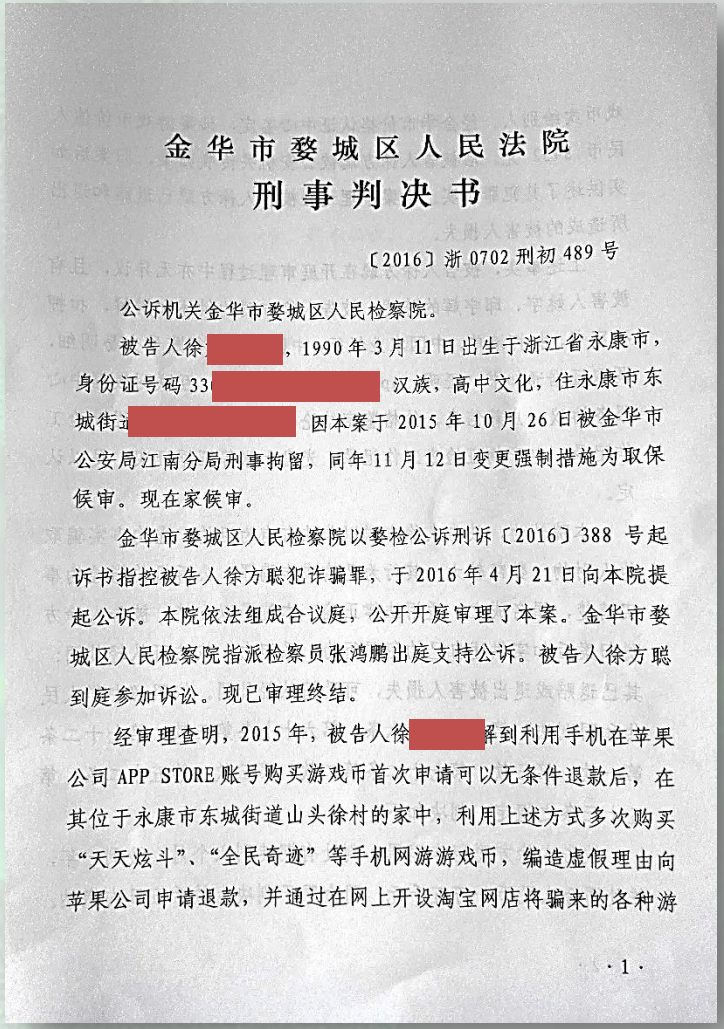
Address
Vehicle
Bank acount
Telephone
Relatives and friends
……

IP
Domain name
E-mail
SNS
NetFlow
Malware
Device fingerprint
……

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

全国首例利用苹果平台退款诈骗案件
基本案情：

- 2015年10月 - 浙江金华市公安局江南公安分局网警大队侦破全国首例苹果平台恶意退款诈骗案
- 犯罪嫌疑人徐某在网购平台公开接单，冒充玩家身份，虚构理由向苹果公司申请退款，在半年内通过退款方式作案数十次，非法获利近万元
- 徐某以非法占有为目的，利用苹果商店的退款政策，采取虚构事实的手段骗取退款，数额较大，其行为触犯了刑法第266条关于诈骗罪的相关规定



金华市婺城区人民法院
刑事判决书

〔2016〕浙0702刑初489号

公诉机关金华市婺城区人民检察院。

被告人徐[redacted]，1990年3月11日出生于浙江省永康市，身份证号码33[redacted]汉族，高中文化，住永康市东城街[redacted]因本案于2015年10月26日被金华市公安局江南分局刑事拘留，同年11月12日变更强制措施为取保候审。现在家候审。

金华市婺城区人民检察院以婺检公诉刑诉〔2016〕388号起诉书指控被告人徐方聪犯诈骗罪，于2016年4月21日向本院提起公诉。本院依法组成合议庭，公开开庭审理了本案。金华市婺城区人民检察院指派检察员张鸿鹏出庭支持公诉。被告人徐方聪到庭参加诉讼。现已审理终结。

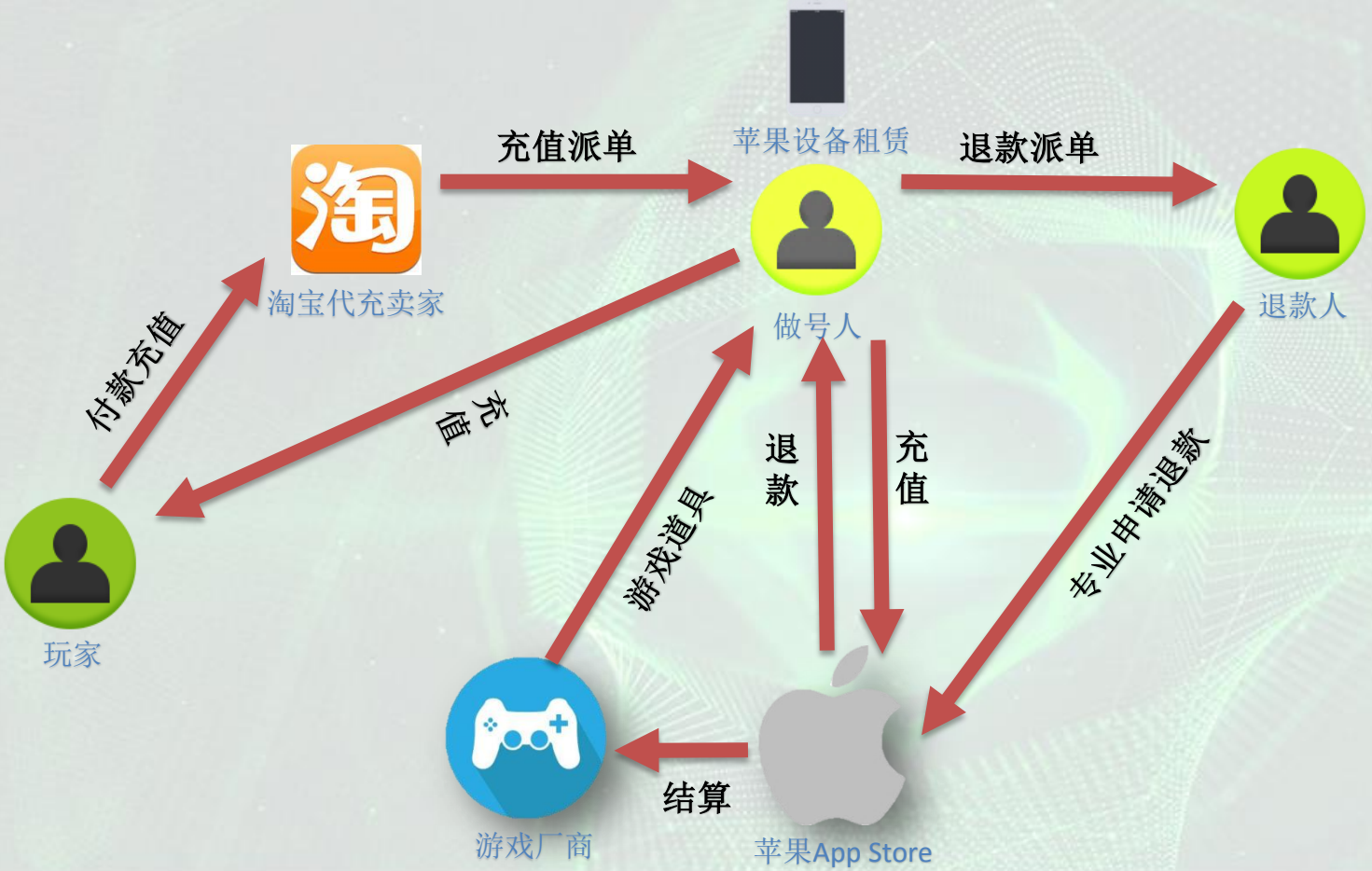
经审理查明，2015年，被告人徐[redacted]择到利用手机在苹果公司APP STORE账号购买游戏币首次申请可以无条件退款后，在其位于永康市东城街道山头徐村的家中，利用上述方式多次购买“天天炫斗”、“全民奇迹”等手机网游游戏币，编造虚假理由向苹果公司申请退款，并通过在网上开设淘宝网店将骗来的各种游

·1·

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

产业链条：

玩家、游戏厂商、苹果平台、淘宝代充服务卖家、职业退款人、职业做号人、苹果设备租赁



新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

游戏代充

天天炫斗苹果 官方充值（安卓勿拍）

拍下后请联系我们客服充值

充值幸运礼物的要旺旺特别说明哦

60钻石=6元 （拍1件）贵族1

190钻石=18元（拍3件）贵族2

380钻石=36元（拍6件）贵族3

530钻石=48元（拍8件）贵族4

1090钻石=96元（拍16件）贵族5

1890钻石=162元（拍27件）

2080钻石=180元（拍30件）贵族6组合

3770钻石=300元（拍50件）

5050钻石=414元（拍69件）贵族7组合

6000钻石=510元（拍85件）

7580钻石=咨询客服

10000钻石=咨询客服贵族8组合

20020钻石=咨询客服贵族9组合

51480钻石=咨询客服贵族10组合

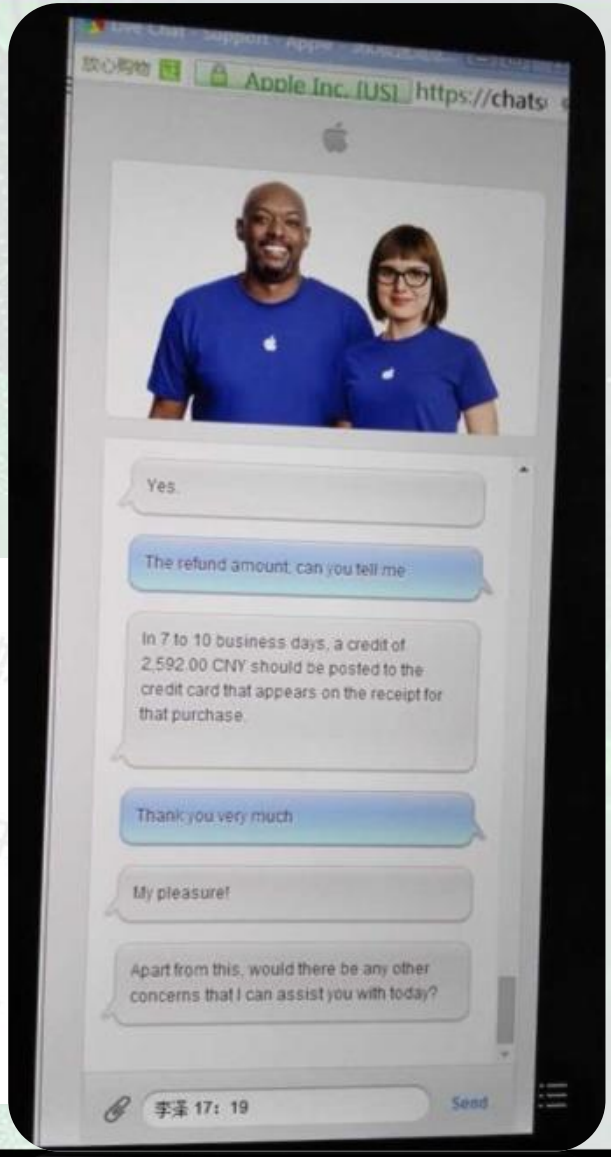
新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

游戏问题：

1. 会闪退掉线，闪退后不能立即登录，影响游戏操作。刚开始玩的时候就会有偶尔闪退也不算严重，后来游戏更新了几次发现闪退越来越严重 游戏等级也高了闪退严重影响游戏操作！（如果客服和你说刚开始玩的时候就发现闪退 为什么还继续充值玩？你就如上这样说）
2. 道具丢失，游戏里打到的东西会丢失 下线再上线会发现得到的东西没有了 （针对游戏具体说出是什么 比如装备 宝石 如卡牌游戏可以说得到的D级S级卡牌 ）
3. 内购未收到(针对近期充值 隔天就退款的 2个或3个 648元订单)如果是游戏玩家 长时间充值 多次充值 请不要用这个
4. 游戏开发商不停的出各种道具礼包等进行圈钱 刺激我们消费 刚买的东西玩了几天就出新的东西 之前买的也被淘汰掉了 不充值不能很好体验游戏，为了赚钱不在乎用户体验。

开发商问题：（最好根据游戏直接说出开发商名字）

1. 闪退现象联系开发商 说游戏更新会解决 却一直没有解决掉 闪退掉线现象越来越严重了
2. 丢失的东西 联系开发商说审核通过给我补回来 但是一直没有等到回复



退款理由

法庭证据认定：

- **受害人陈述**
- **嫌疑人供述、辩解**
- **扣押决定书**
- **扣押清单**
- **银行交易明细**
- **调取证据通知书**
- **证明**
- **苹果公司回复邮件**
- **互联网数据中心服务协议**
- **户籍信息**
- **价格鉴定结论书**
- **搜查笔录**
- **远程勘验工作记录**
- **电子物证检查工作记录**
- **光盘**

上述事实，被告人徐方聪在开庭审理过程中亦无异议，且有被害人[redacted]的陈述，被告人[redacted]的供述和辩解，扣押决定书，扣押清单，中国农业银行，中国工商银行账号交易明细，调取证据通知书，证明，Apple 信箱回复内容，互联网数据中心服务协议，户籍信息，价格鉴定结论书，搜查笔录，远程勘验工作记录，电子物证检查工作记录，光盘十张等证据证实，足以认定。

取证关键点：

- **如何证明嫌疑人确实有恶意退款行为？**
- **如何确认虚拟货币价格？**
- **如何解决虚拟身份与现实身份的关联问题？**

证据的调取

2015年09月30日 15:34

2016年01月18日 11:23
共15封邮件

- **执法单位**
- **执法查办人员**
- **案件环境 / 背景**
  - 案发形式和案件编号
  - 案发日期和地点
  - 案件描述
- **信息环境 / 背景**
  - 要求查询相关信息的原因和当地法律的根据
  - 协案的IMEI号/序列号/Apple ID/电子邮件信箱
  - 需查询的细节

法律流程准则

日本和亚太地区执法部门

日本和亚太（“APAC”）地区的执法部门或其他政府机构在向这些地区提供服务的 Apple 相关实体寻求 Apple 产品和服务的用户信息或与 Apple 设备相关的信息时，可使用这些准则。根据 Apple 的隐私政策 http://www.apple.com/legal/privacy/szh/，这些准则中使用的“Apple”字样应指在特定地区负责用户信息的相关实体。Apple 在必要时将更新下列准则。此版本于 2015 年 9 月 29 发布。

有关 Apple 用户信息的其他所有请求，包括有关信息披露的用户疑问，都应转荐至 https://www.apple.com/cn/privacy/contact/。这些准则不适用于执法机构向日本和亚太地区以外的 Apple Inc. 或 Apple 相关当地实体提出的请求。

对于来自执法部门的信息请求，我们遵循与控制我们数据的全球实体有关的法律，并且根据法律要求提供详细信息。对于来自美国以外的执法机构的内容请求，除紧急情况（见下文“紧急请求”中的定义）以外，Apple 仅针对根据“共同法律协助协议”程序或通过与美国司法部机构协作签发的搜查令提供内容。

新型网络犯罪取证的困境与对策
——以全国首例利用苹果平台退款诈骗案件为例

虚拟货币价值的认定

手游天天炫斗游戏代币“钻石”66380个。

手游全民奇迹游戏代币“钻石”25920个。

调查中了解到，手游天天炫斗游戏本身对玩家不收取费用，运营公司通过出售游戏中的货币“钻石”获取营业收入。但不采取“使用货币”等方式回购游戏者拥有的“钻石”，同时该手游也未在游戏中设置“交易”功能来变更“钻石”的所有者。限于苹果设备自身的局限性，安全获取“钻石”的唯一方式为在苹果商店APP Store账号进行充值后并在游戏中购买相关产品，即“直充”方式。价格鉴定基准日其价格为充值人民币6元=60钻；18元=190钻；50元=530钻；98元=1090钻；168元=1890钻；328元=3770钻；518元=6000钻；648元=7580钻。因此本次价格鉴定以从游戏运营商处获取“钻石”所需支付人民币数额来确定价格鉴定基准日的价格。

三、价格鉴定基准日

2014年11月-2015年3月

手游全民奇迹游戏性质与天天炫斗相同，但价格鉴定基准日其价格有所区别，为充值人民币6元=60钻；648元=6480钻；比例始终为1:10。因此本次价格鉴定以从游戏运营商处获取“钻石”所需支付人民币数额来确定价格鉴定基准日的价格。

金华市价格认定中心
涉案物品价格鉴定人员

价格鉴定基准日: 法定资产评估机构接受客户的委托评估任务后,确定委托评估对象于某一日的公允价值

虚拟身份与现实身份的关联

设备的关联到人与数据的关联

对策：

- **证据链构建：从单纯的取证技术到复杂的取证思路**
- **证据调取机制、时效性**
- **法律法规的完善**
- **运用生物特征检验解决虚拟身份落地问题**

鸣谢
浙江金华市公安局江南公安分局网警大队

谢谢！