

第十届经天法律文书大赛

复

赛

试

题

上海法律专业学位研究生

教育指导委员会秘书处

2024年11月

目 录

赛题说明.....	1
双祝市公安局网络安全保卫总队接受刑事案件登记表.....	2
双祝市公安局大都寇区分局立案决定书.....	4
双祝市公安局大都寇区分局提请批准逮捕书（王小勇）.....	5
双祝市公安局大都寇区分局提请批准逮捕书（李新）.....	8
双祝市大都寇区人民检察院批准逮捕决定书（王小勇）.....	11
双祝市大都寇区人民检察院批准逮捕决定书（李新）.....	12
讯问笔录（李新，第 1 次）.....	13
讯问笔录（李新，第 2 次）.....	19
讯问笔录（李新，第 3 次）.....	24
讯问笔录（李新，第 4 次）.....	28
预审笔录（李新）.....	30
讯问笔录（李新，第 5 次）.....	32
讯问笔录（李新，第 6 次）.....	36
讯问笔录（王小勇，第 1 次）.....	38
讯问笔录（王小勇，第 2 次）.....	40
讯问笔录（谢强，第 1 次）.....	42
讯问笔录（谢强，第 2 次）.....	44
询问笔录（刘昌）.....	46
关于腾讯 QQ 用户 COOKIES 被异常使用的反映材料.....	48

关于腾讯 QQ 用户数据的情况说明	49
胡建中证司法鉴定中心流量数据检验报告及鉴定意见书	50
胡建中证司法鉴定中心电子数据检验报告	51
双祝网安司法鉴定所司法鉴定意见书	22
双祝市公安局大都寇区分局鉴定意见通知书	53
双祝市公安局大都寇区分局涉案服务器情况查验结果说明	54
双祝市公安局大都寇区分局银行流水及交易获利情况说明	55
双祝市公安局大都寇区分局起诉意见书	56

答题要求与注意事项

1. 请各参赛同学根据下列案件材料及相关法律规定,从控方角度准备本案的公诉意见书。
2. 本案不能要求提供新的案件材料。
3. 本案案件材料为模拟卷宗,所有证据的提取均视为提取程序合法;诉讼过程符合法律规定的程序;证据合法性和真实性不作争点;推定侦查、检察以及审判的管辖均无争议;侦查期限以及移送审查起诉日期、送达被告人起诉书的日期不作争议。
4. 本案中的鉴定机构、鉴定人的资质、资格均符合法律规定。
5. 本材料中所有人物、姓名、电话号码、身份信息等均为比赛需要之虚拟,若有雷同,纯属巧合。

接受刑事案件登记表

填报单位：双祝市公安局网络安全保卫总队

编号：A3301001103002018010401

报 案 人	姓名		性 别	\	年龄	\	住址	深 圳 市 南 山 区 高 新 区 科 技 中 一 路 腾 讯 大 厦 35 层
	单位	腾讯科技（深 圳）有限公司	电话	7 -0001	案件来源	报案		
移送单位	\		承 办 人	\		电 话	\	
<p>报案内容（发案时间、地点、简要过程、涉案人基本情况、受害情况等）：</p> <p>我单位工作人员发现，自2018年9月以来，有数百万条QQ用户的COOKIES数据存在异常使用的情况，集中反映在江南省移动的QQ用户。因该情况可能存在涉嫌犯罪的行为；且这些QQ用户的COOKIES数据疑似在双祝进行异常操作，特将该情况反映给贵单位，还请贵单位查处该犯罪行为。</p>								

领导批示：

初查。



处理结果：

立非法获取计算机信息系统数据罪侦查。

接警单位	双祝市公安局网络安全保卫总队	接警地点	双祝市公安局
接警人员	李小龙	接警时间	2018年12月4日

双祝市公安局大都寇区分局 立案决定书

双公网警刑字 [2019] 012 号

根据《中华人民共和国刑事诉讼法》第一百一十二条之规定，决定对王小勇、李新非法获取计算机信息系统数据案立案侦查。



双祝市公安局大都寇区分局

提请批准逮捕书

双大公捕字（2019）第 108 号

犯罪嫌疑人王小勇，男，汉族，1980年5月10日生，大学文化，北京汇文立方信息技术有限公司，身份证号：320945198005104531，户籍地：江南省金陵市海宁区飞龙大道1024号18幢402室，2019年3月3日因涉嫌非法获取计算机信息系统罪被大都寇区公安分局刑事拘留。

王小勇等人非法获取计算机信息系统数据一案，系深圳市腾讯计算机系统有限公司提供的案件线索，因使用QQ用户Cookie数据的主嫌疑人在双祝，该案件由双祝市公安局网安总队受理，后由双祝市公安局指定我局管辖，我局于2019年1月1日立案，2019年2月1日，犯罪嫌疑人周星辰、雷磊在双祝被抓获，犯罪嫌疑人陈铭羽在河北省廊坊市被抓获，2019年3月3日，犯罪嫌疑人王小勇在北京被抓获，犯罪嫌疑人李新、谢强在江南省越洋市中国移动江南省分公司被抓获。

经公安机关依法侦查查明：2018年9月初左右，长期在互联网上进行淘宝客推广的双祝市荣昌人周星辰在和朋友在网上交流时候了解到可以利用QQ号的Cookies进行推广的方法，后在网上认识了同样从事推广业务，且擅长程序设计的居住在双祝大都寇的雷磊，两人提出了在QQ用户不知情的情况下，利用QQ用户的Cookie数据内包含的uin（QQ号码）、skep/p_skep等参数，擅自操作用户QQ加入其指定的QQ群和在QQ空间发布包含淘宝商品链接的“说说”的方案，该方案经擅长程序设计的雷磊测试后认为可行，但为了实现最大利益，需要获取大量的QQ用户Cookie数据。2018年9月底左右，周星辰与通过互联网认识的纪飞谈到利用QQ号进行淘宝客推广的事情，问纪飞能否获取大量QQ用户的Cookies数据，因纪飞知道与其长期合作的王小勇能获得江南的移动用户上网数据流量，于是纪飞向王小勇提出获取QQ用户的Cookies数据的要求，王小勇找到陈铭羽（已取保候审）做技术支持，让陈铭羽和周星辰、纪飞交流具体技术细节，根据周星辰、雷磊提出获取QQ用户Cookies数据的具体要求，从王小勇本人伙同李新（现冬华软件公司员工）和谢强（江南省移动公司网管中心工作人员）私自架设在江南省移动运营商机房的服务器

中，该服务器经非法配置后能获取江南省移动骨干网中上网（80 和 8080 端口）镜像数据，开发和部署程序获取 QQ 用户的 Cookies 数据并传输到周星辰提供的 FTP 服务器内。周星辰的合伙人雷磊通过程序将 FTP 内的数据读取并保存到远程服务器的 SQLSERVER 数据库内，然后雷磊编写程序在其使用的电脑上读取并利用储存在 SQL SERVER 的 QQ 用户 Cookies，在 QQ 用户不知情的情况下实现操作用户 QQ 加入其指定的 QQ 群、在 QQ 空间发布包含淘宝商品链接的“说说”和关注特定的 QQ 公众号等功能。其中 QQ 群的创建和管理，以及在 QQ 群内推广周星辰提供的淘宝客链接的工作由刘向前负责。2018 年 9 月至今，经第三方司法鉴定机构鉴定（扣押服务期内储存 Cookies 数量），该团伙非法获取了 3103035 个 QQ 号码的登录 Cookie 信息，利用这些数据，通过在推广阿里妈妈平台上淘宝客链接，获利上百万元，所获赃款按周星辰 15%，雷磊 20%，王小勇、谢强、李新、纪飞、陈铭羽等人 50%，山东负责 QQ 群推广的刘向前 15%的比例进行分配。资金结算由周星辰按比例支付给雷磊、纪飞和刘向前；纪飞按比例支付给王小勇，王小勇支付给陈铭羽、李新和谢强。

另据公安机关查明，2017 年 10 月份以来，犯罪嫌疑人伙同李新（现冬华软件公司员工）和谢强（江南省移动公司网管中心工作人员）利用江南省移动主干网用户上传数据进行百度推广，修改用户上传访问百度时的推广 ID 非法获利。王小勇提供服务器，李新在谢强的帮助下私自架设这些服务器到江南省移动机房，并配置好网络和接入江南移动用户上传的 80 端口和 8080 端口所有的 get 数据。由王小勇部署程序到服务器，程序实现修改用户上传访问百度时的推广 ID。王小勇使用的百度推广 ID 都是都是由黄岩求提供，黄岩求每个月都与王小勇结算百度推广的收益并有详细的报表数据，经查王小勇使用江南移动流量进行百度推广的获利约 250 万元，其中转了 190 余万元给李新，李新先后以现金的方式给了谢强约 60 万元。上述等人到案后，对非法获取计算机信息系统数据后，进行牟利的犯罪事实供认不讳。

认定上述的犯罪事实有犯罪嫌疑人李新以及谢强的供述与辩解、电子证物检查工作记录、辨认笔录等证据证实。

以上犯罪事实清楚，证据确实、充分，足以认定。

综上所述，犯罪嫌疑人王小勇的行为已经触犯《中华人民共和国刑法》第二百八十五条第二款之规定，涉嫌非法获取计算机信息系统数据罪。依照《中华人民共和国刑事诉讼法》第八十七条和第九十一条第一款之规定，特提请批准逮捕。

此致

双祝市大都寇区人民检察院

双祝市公安局大都寇区分局

二〇一九年三月二十日



附：

- 1、本案卷宗柒卷；
- 2、犯罪嫌疑人王小勇现押于大都寇区看守所；
- 3、随案移交物品同步录音录像、电子数据光碟 30 张。

双祝市大都寇区公安局

提请批准逮捕书

双大公捕字（2019）第 109 号

犯罪嫌疑人李新，男，汉族，大专文化，1979 年 2 月 9 日出生，江南省冬华软件公司员工，身份证号：42122519790209051X，户籍地：越洋市牡丹区晁阳尔村 14 栋 1 单元 202 号，2019 年 3 月 8 日因涉嫌非法获取计算机信息系统罪被大都寇区公安分局刑事拘留。

李新等人非法获取计算机信息系统数据一案，系深圳市腾讯计算机系统有限公司提供的案件线索，因使用 QQ 用户 COOKIE 数据的主嫌疑人在双祝，该案件由双祝市公安局网安总队受理，后由双祝市公安局指定我局管辖，我局于 2019 年 1 月 31 日立案，2019 年 2 月 1 日，犯罪嫌疑人周星辰、雷磊在双祝被抓获，犯罪嫌疑人陈铭羽在河北省廊坊市被抓获，2019 年 3 月 3 日，犯罪嫌疑人程志在北京被抓获，犯罪嫌疑人李新、谢强在江南省越洋市中国移动江南省分公司被抓获。

经公安机关依法侦查查明：

2018 年 9 月初左右，长期在互联网上进行淘宝客推广的双祝荣昌人周星辰在和朋友在网上交流时候了解到可以利 QQ 号的 Cookies 进行推广的方法，后在网上认识了同样从事推广业务，且擅长程序设计的居住在双祝大都寇的雷磊（已取保候审），两人提出了在 QQ 用户不知情的情况下，利用 QQ 用户的 Cookie 数据内包含的 u in（QQ 号码）、skep/p_skep 等参数，擅自操作用户 QQ 加入其指定的 QQ 群和在 QQ 空间发布包含淘宝商品链接的“说说”的方案，该方案经擅长程序设计的雷磊测试后认为可行，但为了实现最大利益，需要获取大量的 QQ 用户 Cookie 数据。2018 年 9 月底左右，周星辰与通过互联网认识的纪飞谈到利用 QQ 号进行淘宝客推广的事情，问纪飞能否获取大量 QQ 用户的 Cookies 数据，因纪飞知道与其长期合作的王小勇能获得江南的移动用户上网数据流量，于是纪飞向王小勇提出获取 QQ 用户的 Cookies 数据的要求，王小勇找到陈铭羽做技术支持，让陈铭羽和周星辰、纪飞交流具体技术细节，根据周星辰、雷磊提出获取 QQ 用户 Cookies 数据的具体要求，从王小勇本人伙同李新（现冬华软件公司员工）和谢强（江南省移动公司网

管中心工作人员)私自架设在江南省移动运营商机房的服务器中,该服务器经非法配置后能获取江南省移动骨干网中上网(80和8080端口)镜像数据,开发和部署程序获取QQ用户的Cookies数据并传输到周星辰提供的FTP服务器内。周星辰的合伙人雷磊通过程序将FTP内的数据读取并保存到远程服务器的SQL SERVER数据库内,然后雷磊编写程序在其使用的电脑上读取并利用储存在SQL SERVER的QQ用户Cookies,在QQ用户不知情的情况下实现操作用户QQ加入其指定的QQ群、在QQ空间发布包含淘宝商品链接的“说说”和关注特定的QQ公众号等功能。其中QQ群的创建和管理,以及在QQ群内推广周星辰提供的淘宝客链接的工作由刘向前负责。2018年9月至今,经第三方司法鉴定机构鉴定(扣押服务期内储存Cookies数量),该团伙非法获取了3103035个QQ号码的登录Cookie信息,利用这些数据,通过在推广阿里妈妈平台上淘宝客链接,获利上百万元,所获赃款按周星辰15%,雷磊20%,王小勇、谢强、李新、纪飞、陈铭羽等人50%,山东负责QQ群推广的刘向前15%的比例进行分配。资金结算由周星辰按比例支付给雷磊、纪飞和刘向前;纪飞按比例支付给王小勇,王小勇支付给陈铭羽、李新和谢强。

另据公安机关查明,2017年10月份以来,犯罪嫌疑人伙同李新(现冬华软件公司员工)和谢强(江南省移动公司网管中心工作人员)利用江南省移动主干网用户上传数据进行百度推广,修改用户上传访问百度时的推广ID非法获利。王小勇提供服务器,李新在谢强的帮助下私自架设这些服务器到江南省移动机房,并配置好网络和接入江南移动用户上传的80端口和8080端口所有的get数据。由王小勇部署程序到服务器,程序实现修改用户上传访问百度时的推广ID。程志使用的百度推广ID都是都是由黄岩求提供,黄岩求每个月都与王小勇结算百度推广的收益并有详细的报表数据,经查王小勇使用江南移动流量进行百度推广的获利约250万元,其中转了190余万元给李新,李新先后以现金的方式给了谢强约60万元。上述等人到案后,对非法获取计算机信息系统数据后,进行牟利的犯罪事实供认不讳。

认定上述的犯罪事实有犯罪嫌疑人李新以及谢强的供述与辩解、电子证物检查工作记录、辨认笔录等证据证实。

以上犯罪事实清楚,证据确实、充分,足以认定。

综上所述,犯罪嫌疑人李新的行为已触犯《中华人民共和国刑法》第二百八十七条之二之规定,涉嫌帮助信息网络犯罪活动罪。依照《中华人民共和国刑事诉讼法》第八十七条和第九十一条第一款之规定,特提请批准逮捕。

此致

双祝市大都寇区人民检察院



附：

1. 本案卷宗柒卷；
2. 犯罪嫌疑人李新、谢强现押于大都寇区看守所；
3. 随案移交物品同步录音录像、电子数据光碟 30 张。

双祝市大都寇区人民检察院

批准逮捕决定书

双大检刑批捕[2019]158号

双祝市公安局大都寇区分局：

你局于2019年3月20日以双公捕字（2019）第108号提请批准逮捕书提请批准逮捕犯罪嫌疑人王小勇，经本院审查认为，该犯罪嫌疑人涉嫌非法获取计算机信息系统数据犯罪，符合《中华人民共和国刑事诉讼法》第八十一条第一款规定的逮捕条件，决定批准逮捕犯罪嫌疑人王小勇。请依法立即执行，并将执行情况三日内通知本院。



双祝市大都寇区人民检察院

批准逮捕决定书

双大检刑批捕[2019]158号

双祝市公安局大都寇区分局：

你局于2019年3月20日以双公捕字（2019）第109号提请批准逮捕书提请批准逮捕犯罪嫌疑人李新，经本院审查认为，该犯罪嫌疑人涉嫌帮助信息网络犯罪活动犯罪，符合《中华人民共和国刑事诉讼法》第八十一条第一款规定的逮捕条件，决定批准逮捕犯罪嫌疑人李新。请依法立即执行，并将执行情况三日内通知本院。

双祝市大都寇区人民检察院

二零一九年三月二十五日



李新讯问笔录（第1次）

时间：2019年3月3日13时10分至2019年3月3日16时15分

地点：大都寇区看守所

询问人/讯问人（签名）：孙秋磊、肖毅 工作单位：双祝市公安局大都寇区分局

记录人（签名）：肖毅 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局的民警（出示人民警察证），现依法向你讯问案件的有关情况，你要如实回答，作伪证或者隐瞒事实将要承担相应的法律责任，对于与本案无关的问题你有权拒绝回答，你听清楚了吗？

答：我听清楚了。

问：这是《犯罪人权利义务告知书》，你看一下。

答：以上《犯罪人权利义务告知书》我已经看过。

问：你的个人情况？

答：我叫李新，男，大学学历，汉族，1979年2月9日出生，身份证号：

42122519790209051X，户籍地：越洋市牡丹区晁阳尔村14栋1单元202号，现

住址：越洋市明日镇太平里51号，电话号码：13975882558，18608522558。

问：把你的简历讲一下？

答：6岁—12岁在越洋钢厂子弟小学就读；12岁—15岁在越洋市第六中学读初中；

15岁-18岁在越洋市第六中学读高中；18岁—21岁在越洋市河西区经济科学学院

读专科；21岁—26岁在越洋市国储电脑城上班，负责配置电脑、卖电脑；26岁—

33岁在中泰数据公司江南分公司；33岁至今在冬华软件公司。

问：把你的家庭情况介绍一下？

答：妻子，刘兴萍，36岁，电话是13755387016，在明日镇开一家叫做“什么呀

精品店”卖小东西；女儿，王涵宇，6岁。

问：你是否是人大代表、政协委员？

答：不是。

问：你是否有重大疾病或者传染病？

答：没有。

问：你是否知道今天因何事被传唤到公安局？

答：知道，就是因为我涉嫌非法侵入计算机信息系统。

问：你把情况详细讲一下？

答：2017年8月份左右，以前在中泰数据的同事王小勇找到我，给我说：“弄一台服务器放在中国移动的机房里，获取中国移动机房里面SIG平台上面的数据，把放在中国移动机房的服务器系统装上，配置好公网IP，再把服务器的账号和密码给我，我就负责调程序、改配置和做流量劫持。”我就说：“会不会被抓？”王小勇就说：“不会的。”我就说：“我一个人做不下来，我要找一个人，就找中国移动公司的谢强。”王小勇说：“行吧。”我和王小勇说定以后，我就到单位找谢强，对他说：“现在有个做流量劫持的业务，我们一起做，你只需要给华康公司做SIG平台维护的工作人员说中国移动公司有业务，需要从SIG平台接数据VC出来，让华康公司的工作人员给我一个出口并配好有流量传输数据就行了。”然后，谢强说：“好的。”我说：“如果挣了钱，我们两个就一人一半，平分。”说好以后，我就开始在庙高峰机房开始装流量劫持的服务器了。

问：继续讲。

答：我和谢强商量好以后，我就马上到了越洋市中国移动公司的庙高峰机房里面，找了一台中国移动公司机房里面淘汰下来的主机，然后就把这台主机重新装了系统，放在机柜里面，我就给谢强事前联系好的华康公司的工作人员打电话，叫他给我一个有流量数据的出口，然后华康的工作人员就给了我一个端口号给我，我就把用作流量劫持的服务器用网线把SIG平台链接上，并把IP配置好，我看见服务器接受数据的灯开始亮了，就表明我的服务器开始接受数据了，我就给程志打了电话，把我自己装的服务器的IP和账号密码给他。我装在机房的服务器开始运行以后，王小勇每个月就会给我打钱过来，差不多每个月7、8万左右，具体多少，我也记不很清楚了。

问：继续讲。

答：我把在中国移动公司庙高峰机房安装好用于流量劫持的服务器后，一两个月

后，我和王小勇联系，我就给王小勇说：“庙高峰的数据用得很好，但是只能劫持庙高峰地区的数据，车站北这边也有机房，也可以装一个服务器用于劫持，流量多了，我挣的钱也就多了。”王小勇说：“可以，你在车站北移动公司的机房也装一个。”然后我就用同样的方法在移动公司车站北的机房里面装了一个服务器。

问：继续讲。

答：在2005年中旬的时候，王小勇给我联系说到：“淘宝的流量数据非常少了，是怎么回事？”我说：“可能是我放在机房的服务器的位置有点问题，在越洋海沙区有SIG平台并且是IDC，淘宝那里的数据很全，要不我放台服务器在海沙机房里而？”王小勇说：“行，你放台服务器试一下。”随后，我就用同样的方法在海沙区的移动公司机房里面放了一台服务器。后来我陆续在移动公司的庙高峰机房、细翻区(车站北机房搬迁至细翻区)、海沙三个地方总共放置了4台用于流量劫持的服务器。

问：你和王小勇平时是怎么联系的？

答：打电话的时候非常少，平时都是用QQ联系的。

问：你的QQ号是多少？

答：QQ号：9945286，微信账号是13975882558，密码是：JACOB123；支付宝账号13975882558@139.com，密码happy。

问：放了几台服务器在移动公司的里面？

答：我放了4台用于流量劫持的服务器。庙高峰2台、细翻区1台、海沙1台，在庙高峰还有一台交换机用于庙高峰SIG平台，我自己放那的两台服务器分流用。

问：你的劫持的数据是什么数据？

答：就是用移动网络网民上网时用的数据，这些移动数据到了移动机房的SIG平台上面，我就在SIG平台的流量出口的端口处接了线到我的服务器上，等于就是SIG平台上面的流量数据直接就到了用于劫持流量的服务器上面。

问：移动的数据你劫持到以后，你是怎么用的？

答：这个我就不是很清楚，只有王小勇比较清楚，我只是负责把安装在移动机房的服务器系统装好，IP配置好，并且把配置好的服务器账号和密码告诉王小勇，然后王小勇就可以远程操作江南这边的服务器。

问：你知不知道王小勇利用你安装的服务器做什么？

答：就是百度流量劫持、APK劫持、QQ的Cookie劫持、推广淘宝客的链接等业务，

但是具体怎么劫持我不清楚。

问：王小勇是怎么给你打钱？

答：王小勇是通过银行转帐给我的，都是打在我的两张农业银行卡上面和一张招行卡。招行卡是我叫王小勇每个月给我打1万到上面(第1次打到的是5000，以后都是1万)。

问：为什么你要叫王小勇到你的招行卡上面，而不全部打到你的两张农行卡上面？

答：因为这个招行卡上面的钱是我自己的私房钱，我老婆不知道。招行上面打过来的钱。我会马上转到我的支付宝里面去。

问：你用于收王小勇打过来的钱的卡放在什么地方？

答：三张卡都放在我家里的。

问：王小勇是用什么银行给你转帐的？

答：我的短信提示转帐是“超级网银转账”，具体他是用哪个银行打给我的，我就不清楚了。

问：王小勇总共给你打了多少钱？

答：总共给我打了200万左右。

问：钱你是怎么用的？

答：总共200万，分了大约一半给100万给谢强，剩下的100万，我买了一部车用了20万、买了套房子首付15万(在海沙摩玛小区)，并在我买房子的地方买了个1个门市，用了首付50万，余下的15万是生活用的，吃饭、买家电等用了不少。现在卡里面还剩下7万块钱。

问：你是怎么给谢强钱的？

答：我都把王小勇把钱打给我以后，然后我就取现金给谢强。

问：除了王小勇知道你在移动机房的服务器IP、帐户和密码，你还给谁说过帐户和密码？

答：我只给程志说过，没有给其他人说过。

问：如果没有IP地址、账户和密码，其他人能不能登陆到你在移动机房用于流量劫持的服务器？

答：这个是不可能的。

问：谢强是做什么的？

答：谢强在江南移动省公司网管中心下属互联室，他以前是管江南移动的骨干网，

半年前就开始管理互联网内容。华康的SIG平台维护工作人员就和谢强对接，平时关系也非常好。所以，谢强他给SIG平台的工作人员打个电话，我就可以到机房接SIG平台的数据。

问：在移动公司，除了谢强和你合作还有其他人没有？

答：没有了。

问：你把你自己用作流量劫持的服务器放在庙高峰、细翻区、海沙三个机房的什么位置？

答：庙高峰的2台服务器是放在庙高峰土楼北机房；细翻区的服务器是细翻区一楼机房；海沙的服务器是放在海沙区机房三楼机房。这些服务器具体放在机房的什么位置我不清楚了。

问：民警带你到三个机房的去指认你所安装的服务器位置，你能找到吗？

答：我能指认出来。

问：你为什么能够进入移动公司的机房里面？

答：因为我不管是在中泰公司上班还是在冬华公司上班，我都是在江南移动公司的总部上班，平时我做正常的业务的时候也会进入机房，就是正常的业务工作也会一个星期进一次机房，机房的工作人员对我也是非常熟悉，所以在我做流量劫持安装服务器的时候，我就会很顺利进入各个江南移动的机房。机房的规定是可以拿东西进去，不能从机房拿东西出来，所以我拿服务器进机房就是很正常的事情。

问：王小勇给你过服务器没有？

答：因为以前我做的流量劫持的服务器就是移动公司淘汰下来的服务器，运行不是很快。王小勇就给我说，你用的服务器运行速度慢了，我给你4台新的服务器，你把老的服务器卸下来，把新的服务器装上去，这样流量传输会更快一些。然后，我就按以前的方法把新的服务器在各个机房重新安装上去。

问：你做流量劫持是从什么时候开始？

答：就是2017年8月份开始直到今天，被公安机关查获。

问：你为什么问王小勇“会不会被抓？”

答：因为我知道做流量劫持是违法的事情，以前我也听说过其他省的地方做流量劫持被抓了。

问：你知道做流量劫持是违法犯罪的东西，为什么还要做？

答：因为做这个风险小、不容易被抓，而且来钱非常快，其实我也是为了多挣点

钱才去做这个事情的。

问：以上所讲的是否属实？

答：属实。

问：民警在对你的审讯过程中，是否保障了你的饮食和休息时间？

答：保障了。

问：你还有何补充没有？

答：没有

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我说的相符。

被讯问人：李新



2019.03

李新讯问笔录（第2次）

时间：2019年3月9日11时10分至2019年3月9日13时15分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、蒲鹏 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答。对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你因何事被羁押在大都寇区看守所？

答：因涉嫌非法侵入计算机信息系统的事情。

问：你讲一下你涉嫌犯罪的情况？

答：2017年8月的时候，我以前中泰数据的同事王小勇，王小勇说可以通过在移动机房放置自己服务器，采集用户的流量，然后进行选择性的劫持，通过这种方式来获利。我就找了江南省移动公司的谢强一起参与这个事情，当时我谢强和程志再三确认这个事情会不会引起投诉，当时不知道这个事情违法，而且王小勇说的这个方法对用户而言完全是无感知的，也不会造成危害，我、谢强就担心引起投诉。直到后面双祝出了个百度DNS劫持，我和谢强才知道这个是违法的，当时我们认为我们这个还是不容易被发现，所以一直搞到现在。

问：王小勇为什么会找到你？

答：我和王小勇以前是同事，当时都在中泰数据一起在江南省移动公司做个工程，后面我去了冬华软件。还有王小勇知道我能接触到江南省移动核心机房，能接触到

这些用户的网络流量数据。

问：你为什么要找谢强和你一起做这个事情？

答：我一个人做不下来，我担心客户有投诉，用户的投诉都是谢强接手，如果找谢强合作，我们就可以直接处理了，不会被移动公司的领导发现。还有就是我和谢强关系好，我们在同一个办公室上班。此外谢强还有权力放设备到机房，如果有领导巡查发现机房的设备，谢强可以解释为移动的某业务的设备，可以掩饰过去。

问：谢强他是做什么的？

答：谢强是江南省移动公司网管中心下属的互联网室的职员，主要是负责省移动骨干网设备的运维。

问：你是做什么的？

答：我是冬华软件公司的职员，冬华软件是江南省移动公司的骨干网系统集成商，我就是在移动公司做运维的。

问：你具体是怎么操作来采集用户的网络流量的？

答：在移动的核心机房放置服务器设备，服务器接触到公网还要接入江南省移动的 SIG 平台。我们就是通过 SIG 平台采集到用户的流量数据，在服务器上处理好数据后，再通过公网发送篡改的数据。

问：SIG 平台是什么？

答：SIG 平台是华康的设备，是用于采集用户的流量并进行上网行为分析的系统，可以定向导出指定的数据，比如说指定只要用户 80 端口的数据，可以通过 SIG 系统进行配置，定向的取用户的特定端口的数据。

问：SIG 平台采集的源数据是什么？

答：就是移动骨干网直接分到 SIG 平台，就是分光的数据。

问：你装的服务器都在移动哪些机房？

答：庙高峰机房，车站北路机房（后来搬迁到细廊区机房）、海沙 IDC 机房，这些服务器之前我们都带你们去指认了的。

问：你说下庙高峰机房装了多少台服务器？

答：庙高峰总共装了 2 台服务器，2 台服务器是连了 SIG 平台数据的。

问：庙高峰机房你装的接入了 SIG 数据的服务器的 IP 地址是多少？

答：庙高峰机房两台服务器的公网 IP 分别为：211.129.226.34、211.8.20.34。

问：庙高峰机房移动公司总共装了多少台 SIG？

答：总共就两台，我在这个机房装的两台服务器，211.8.20.34 接入了两台 SIG 的

数据，211.129.226.34 只接了一台 SIG 的数据。

问：庙高峰机房里，你装的两台服务器是谁的？

答：2017 年 8 月到 2018 年年底，具体哪月我不记得了，那段时间用的是移动公司淘汰下来的服务器，后来的那 2 台服务器的硬盘坏了，2018 年年底就换了两台全新的服务器，是联想的 think server 服务器，这两台服务器是王小勇给我的，他是通过顺丰快递发给我的。

问：海沙 IDC 机房你装了多少台服务器？

答：只有一台 IP，地址是 211.23.5.130。

问：海沙 IDC 机房移动公司总共装了多少台 SIG？

答：总共是 3 台，我装的那台服务器接入了 3 台 SIG 的数据。

问：海沙 IDC 机房里装的一台服务器是谁的？

答：谢强打的电话联系说有个业务系统要进行测试，需要 1 台服务器，然后我就到了海沙机房找负责人，负责人给了我 1 台淘汰下来的服务器，这个服务器应该是属于网宿的。

问：细翻区机房你装了多少台服务器？

答：只装了 1 台，之前在车站北机房的时候也只有 1 台，大概在 2019 年 1 月的时候机房搬迁了，车站北的 SIG 全部整体搬迁到了细翻区机房了。正好在车站被我装的服务器也坏掉了，后来王小勇就给快递了 1 台新的服务器过来。

问：细翻区机房移动公司总共装了多少台 SIG？

答：4 台，我装的那一台服务器把这 4 台 SIG 的数据都接入了。

问：细翻区机房的服务器是谁的？

答：王小勇快递发过来的，是全新的服务器，联想的 think server 服务器。

问：移动公司装的 SIG 平台，你可以随意进入到你的服务器吗？

答：不可以的。

问：那你是怎么进入 SIG 数据的？

答：通知 SIG 的设备厂商给我分配端口，配置好后，我就把光纤插入到指定的端口。

问：是谁给你分配的端口并进行配置 SIG 数据？

答：华康设备的维护厂家的工作人员刘昌。

问：刘昌为什么会给你配置端口等？

答：谢强通知他的，谢强是移动公司的，对口联系这些运维人员，刘昌就要听谢强的安排。

问：你们采集的 SIG 数据，都让刘昌配置了哪些端口的数据？

答：端口 80 和 8080 是网页访问的端口，而且 8080 端口是 QQ 登陆的端口，端口 53 是 DNS。

问：采集这些端口的数据是谁让你们这样操作的？

答：王小勇他特意说了要 80 端口和 8080 端口的 get 数据。

问：王小勇除了给你发服务器，还发过什么东西？

答：还发过两台交换机。

问：你安装的那些服务器，是用于做什么的你是否知晓？

答：不清楚，我只负责把服务器配置好，把数据接入好，能提供客户的上网流量，服务器上具体的操作是王小勇在搞，我是把服务器的最高权限的口令是给了程志的，具体服务器上运行了什么程序我也不清楚。

问：王小勇通过这些服务器怎么牟利的，你是否知晓？

答：他主要是搞推广、发广告、淘宝客，还有就是 APK 下载劫持。

问：王小勇是怎么给你分配获利的？

答：王小勇说是根据业务量来算的，每个月都不同，具体给多少都是王小勇说了算。

问：王小勇都是怎么把钱给你的？

答：都是通过超级网银转账的方式，一般情况是每个月的最后一天给我转账，有一次是王小勇通过支付宝转到我的支付宝。

问：王小勇大概转了多少钱给你？

答：大概转了 180 万。

问：你收钱的银行卡？

答：一张卡是我名下的招商银行的借记卡，还有两张是我亲戚名下（第一次笔录没提）的农业银行卡一个是龚海平，还有一个是李新培，两张农业银行卡开户地都是越洋的。

问：你支付宝账号？

答：13975882558@139.com。

问：王小勇给你转账时，是用的谁的账户给你转的？

答：超级网银都是显示的王小勇，支付宝转的那次，他的支付宝实名信息也是程志。

问：王小勇给你的获利，你是怎么处置的？

答：拿一部分给了谢强，大概给谢强有 70 万左右，剩下的就是我个人所得了，大部分用了，大概还剩 10 万左右。

问：你的钱是怎么给谢强的。

答：每次都是在办公室给的谢强，都是我先取款后直接给现金，都是我直接把现金放在谢强的包里，都没有当面给过。

问：上所讲的是否属实？

答：属实。

问：民警在对你的审讯过程中，是否保障了你的饮食和休息时间？

答：保障了。

问：你还有什么补充的？

答：我之前不知道这个违法，现在事情已经出了，我愿意退赃，我家里有四个老人，还有个小孩。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：李新

2019.3.6



李新讯问笔录（第3次）

时间：2019年3月19日11时10分至2019年3月19日13时20分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日身份证件种类

及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答，对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你的QQ号码是什么？

答：9945286。

问：你的QQ号的昵称？

答：金灵。

问：现在我出示你的电脑和你的白色小米手机里提取到的你的QQ号码的聊天记录，你看下这些聊天记录，这些聊天记录你看下是不是你的？

答：（阅读约5分钟）是我的，都是我和王小勇的聊天记录。

问：你讲下你涉嫌犯罪的情况？

答：从2017年8月，王小勇联系让我在移动机房放置服务器，采集用户的流量，通过劫持流量的方式来获利。我找了江南省移动公司的谢强一起参与，谢强通过协调华康运维公司的刘昌，接到了江南省移动主干网的SIG数据，通过这种方式，从2017年8月至今，王小勇给了我大概180万。

问：你说下你在移动机房安装了多少台服务器？

答：总共是装了 4 台服务器，庙高峰机房装了 2 台，细翻区机房 1 台，海沙机房 1 台。

问：安装的服务器的分别配置的公网 IP 是多少？

答：庙高峰机房两台服务器的公网 IP 分别为：211.129.226.34、211.8.20.34；细翻区的是 211.8.29.78；海沙的是 211.23.5.130。

问：具体那些服务器你是怎么接的？

答：服务器都是安装 linux 操作系统，每个服务器有多个网卡，基中一个网卡配置公网 IP，其他的网卡部分接入 SIG 的数据来获取用户的流量，机房里有多少台 SIG，我就接了多少路 SIG 数据到我的服务器。

问：你是否知道王小勇用这些服务器都在做什么业务？

答：最初的时候，王小勇说就是做百度网页的劫持，就是修改百度访问的时候的链接后面的一串代码，好像是 ID 之类的，他就是修改这个 ID 变成他指定的 ID。2018 年下半年的时候，他跟我说过还在做 APK 的下载、QQ 空间发推广链接、做淘宝客、还有做博彩这些推广，还可以做 QQ 群推广。

问：王小勇做的这些业务你是通过什么方式知道的？

答：都是他告诉我的。此外，在 2018 年年底的某一天中午，我发现我一个同事、还有王小勇两个的空间同时发了一个壮阳药的广告，内容和图片都完全相同，我觉得这个有点可疑，我就马上联系了王小勇，王小勇就给我说了是他在做的东西，我就问他是怎么做的，他回答是利用了腾讯的漏洞来处理的，他还跟我说只是测试。我还给他说了这个影响比较大，让他停掉。还有就是 2018 年双 11 的时候，王小勇在之前联系过我说要做淘宝客业务，到了双 11 月底的时候，王小勇给我说了双 11 的时候就只做了几个小时，赚了两万元。因为那些是利用腾讯的漏洞，所以不是能一直做的，漏洞一旦修复了就没法搞了。还有也是在 2018 年年底的时候，我自己的 QQ 在我不知情的情况被关注了一个博彩的公众号，那个公众号一直给我发博彩的信息，我觉得很奇怪就把这些截图都发给王小勇，王小勇回复我是有其他人在做。又过了几天后，我自己的 QQ 号在我不知情的情况下进了一个淘宝推广的群，那里面一直在发淘宝的链接，我看后就直接退出了。

问：这些服务器都是谁提供的？

答：庙高峰的 2 台，细翻区的 1 台都是王小勇通过顺丰快递发给我的，当时程志还说收件人写我比较明显，特意写的收件人是我老婆。海沙机房那台服务器是网宿公司淘汰下来的设备。

问：安装的这些服务器品牌特征？

答：庙高峰的 2 台、细翻区的 1 台都是联想的 Think Server 服务器，黑色，海沙那个是浪潮服务器，有好几个硬盘仓，只有一个仓位放了个硬盘。

问：具体每个机房里安装的服务器，分别在做什么业务？

答：我不知道具体每个服务器在做的业务，只是王小勇给我说他在做的业务，没有说哪一台服务器具体在跑什么业务。因为服务器的口令一般都是在王小勇哪里，而且他会定期更改的，而且即使我登上服务器，我也看不明白在跑什么业务，只看到在运行什么进程。

问：你为王小勇都是做了什么事情？

答：就是架设服务器、线路给接好，还有就是分配公网 IP，还有就是维护服务器。

问：你分配的那些公网 IP 是哪里来的？

答：都是移动公司正常业务的剩余 IP。

问：这些服务器的登录口令是谁在管理？

答：安装服务器的时候，第一次是我管理，安装完成后，我就会把口令通过 QQ 给王小勇。之后王小勇就会修改登录口令，而且后面还定期修改口令。遇到我去现场维护服务器的时候，我就会问王小勇要口令，我每次要到的口令都保存了，都存在我的笔记本申脑，文档名字“note.txt”，保存了每个服务器历次修改后的口令。

问：你在 2019 年 3 月 4 日指认现场的时候，当时服务器的口令是什么？

答：是 W 开头的口令，具体口令我记不了，但是在刚才的聊天记录里有，在 2019 年 2 月 3 日 15 点 39 分，王小勇发了庙高峰的两台服务器口令给我，口令是“Wyz5w@qq.com”。庙高峰、细翻区的 3 台服务器都是这个口令，海沙那个服务器无法开机，不知道能用哪个口令登录。

问：你平时和王小勇是怎么联系的？

答：主要是通过 QQ 联系，也有少数是微信联系，还有直接电话联系。

问：你所架设的服务器都是接入的 SIG 数据，那么 SIG 的前端采集的是什么数据？

答：前端采集的是江南省移动骨干网的分光数据。

问：你架设的服务器采集的 SIG 数据都是什么？

答：SIG 配置好的数据，是按照王小勇的需求，特定的指定 SIG 接入过来的是 80 和 8080 端口的全部的 get 数据。还采集了 53 端口的数据，这个是谢强要求接入的数据。

问：SIG 数据是谁给你配置的？

答：华康的运维人员刘昌。

问：刘昌为什么会给你配置数据？

答：谢强通知他的，刘昌就要听谢强的安排。

问：王小勇累计给了你多少钱？

答：大概 180 万。

问：王小勇怎么付款给你的？

答：都是网银转账，有过一次是支付宝转账的记录。

问：你收款的银行卡？

答：一张卡是我的招商银行卡，还有两张是我亲戚的农业银行卡，龚海平和李新培。

问：你支付宝帐号？

答：13975882558@139.com

问：王小勇给你的获利，你是怎么分配的？

答：给谢强大概 70 万，剩下的就是我个人得了，大部分用了，大概还剩 10 万左右。

问：获利你是怎么给谢强的？

答：都是现金给他的，没有当面给他，都是直接放在他的包里面。

问：以上所讲的是否属实？

答：属实。

问：民警在讯问过程中，全程同步录音录像，你是否知晓？

答：知晓。

问：你还有什么补充的？

答：我已经认识到这个犯罪行为，我也愿意接受法律的制裁，还有我愿意退还所有赃款

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：

2019. 3. 19

李新讯问笔录（第4次）

时间：2019年3月30日12时10分至2019年3月30日13时05分

地点：大都寇区看守所

询问人/讯问人（签名）：陈卓尔、方群 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈卓尔 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答。对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：从什么时候开始，你和谢强一起通过非法手段在江南省移动公司各个机房里面的SIG平台上，将用户上网数据镜像到你和王小勇等人一起架设的服务器？

答：大概在2017年9月份左右开始在庙高峰机房架设服务器，并操作数据。之后各个机房都开始完全架设服务器，并非法操作SIG平台数据，应该在2017年底的时候。

问：你的违法所得是从谁那里获得的？

答：都是王小勇通过银行卡转账给我的。好像有一次是通过支付宝转我的，金额好像是1万。

问：你收款的银行卡？

答：一张卡是我的招商银行卡，还有两张是我亲戚的农业银行卡，龚海平和李新培。

问：你支付宝帐号？

答：13975882558@139.com。

问：从2017年年底开始，王小勇一共给你转了多少钱？

答：大概 180 万。

问：这些都是你和王小勇等人“合作”之后，给你的分成？

答：对的。

问：王小勇给你的获利，你是怎么分配的？

答：给谢强大概 70 万，剩下的就是我个人得了，我大概收了 110 万。

问：获利你是怎么给谢强的？

答：都是现金给他的，没有当面给他，都是直接放在他的包里面。

问：你愿不愿意退还所有的违法所得？

答：我愿意主动地退还所有的违法所得，尽量凑齐 110 万。

问：你以什么方式退还违法所得？

答：我可以让你们通知我老婆，让我老婆向公安机关退还我的违法所得。

问：以上所讲的是否属实？

答：属实。

问：你还有什么补充的？

答：我已经认识到这个犯罪行为，我也愿意接受法律的制裁，还有我愿意退还所有赃款。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：李新
2019.3.30

预审笔录

时间：2019年4月8日11时05分至2019年4月8日11时50分

地点：大都寇区看守所

询问人/讯问人（签名）：陈卓尔、方群 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈卓尔 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示人民警察证），现依法对你宣布执行逮捕，你应该如实回答我们的提问，对与本案无关的问题你有权拒绝回答，你听清楚了吗？

答：我听清楚了。

问：姓名、性别、民族、文化程度、出生日期？

答：我叫李新，男，大学学历，汉族，1979年2月9日出生，身份证号：42122519790209051X。

问：户籍地、居住地？

问：户籍地：越洋市牡丹区晁阳尔村14栋1单元202号，现住址：越洋市明日镇太平里51号，电话号码：13975882558, 18608522558。

问：你是否是人大代表、政协委员？

答：不是。

问：你是否受过刑事处罚或者行政处罚？

答：没有。

问：你是否知道为什么被逮捕？

答：因为我涉嫌帮助犯罪，所以我被逮捕。

问：请你再讲一下你和王小勇等人的犯罪经过？

答：大概在2017年8月的时候，王小勇打电话让我在江南移动的机房里面架设服务器、路由器、交换机等设备，然后把江南移动用户的上网数据的流量导入到他的服务器上面，他说他用来做百度的推广劫持，我就按照王小勇的要求，我和谢强一起，将SIG平台的数据配置并传输到我和王小勇架设的服务器上面，然后服务器权限由王小勇操作。从那时候至今，王小勇多次和我交流过获取用户数据的用途，他告诉我可以做百度劫持、其他网站的流量劫持、各种APK的劫持下载、淘宝客的推广，还有在QQ用户空间里分享链接推广等操作。在和程志合作的期间，我和王小勇、谢强多次交流过做以上的事情应该有风险，第一个风险就是会引起用户投诉，第二个风险就是移动集团会发现这些事情，第三个风险就是我们听说外地做类似的事情也是违法犯罪的。在和王小勇合作以来，投诉不多，所以我们也就没有担心以上的风险，就继续在做，直到被你们公安机关抓住。

问：以上所讲的是否属实？

答：属实。

问：以前的公安机关民警讯问你的笔录是否属实？

答：属实。

问：你还有何补充没有？

答：没有。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人 李新

2019年4月8日



李新讯问笔录（第5次）

时间：2019年7月1日14时45分至2019年7月1日17时05分

地点：大都寇区看守所

询问人/讯问人（签名）：陈卓尔、方群 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈卓尔 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答。对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你说下你涉嫌的犯罪事实？

答：2017年8月，以前我的同事王小勇找到我，说在移动机房放服务器，服务器一端接SIG采集的数据，一端接公网，通过修改用户上网数据，劫持百度推广ID，修改成王小勇他的百度推广ID，我找移动公司的谢强商量了下，觉得这个风险不大，就和王小勇一起合作，直到2019年3月初被抓获。

问：你和王小勇合作，王小勇是否告诉你他是通过什么获利的没有？

答：他给我说过，就是通过修改上网用户访问百度搜索时网址后面的那个推广ID，到了月底的时候，百度公司就会将推广收益结算给王小勇。

问：除了百度推广这个事情，是否还有其他？

答：2018年双11的时候做了下淘宝客的业务，王小勇说的是做了几个小时。此外还有QQ空间发广告，大概是在2018年年底时候，我看到我同事和王小勇的QQ都发了一个相同链接，相同广告，我当时还特地联系了这两个人，王小勇回复我说是他在搞测试，在利用腾讯的漏洞做测试。然后我就让他不要搞这些，后来王小勇也

给我说，这个漏洞已经被封了，也做不了了。之后有一天，我的 QQ 莫名地被关注了一个博彩的公众号，那个公众号一直给我发赌场的链接信息，我觉得很奇怪，我还截图都发给王小勇，王小勇说不是他做的。又过了几天后，我的 QQ 号莫名地加入了淘宝客推广 QQ 群，那里面一直在发淘宝的链接，我看后就直接退出了。

问：你是否知道 2018 年双 11 王小勇是怎么搞淘宝客业务的吗？

答：不知道，他没给我讲。

问：你的 QQ 被加入淘宝客推广群，你是否知道是谁做的？

答：不知道是谁做的，也没问王小勇是不是他做的。

问：你是否知道王小勇搞 QQ 用户 cookie 的事情？

答：之前一直不知道，直到被抓后，当天晚上在机房指认的时候才知道服务器上在运行程序，程序在获取 QQ 号码 (UID) 和对应的 skey 等。

问：你给王小勇在移动机房架设的服务器，是否能获取 QQ 用户 cookie 数据？

答：我架设的服务器，接入的是 SIG 数据，SIG 数据配置的是 80 端口和 8080 端口的 get 数据，QQ 软件要使用 80 端口。

问：王小勇搞百度推广的业务，你是否知道他是怎么做的？

答：你不知道怎么实现的，我只负责在机房把服务器装好，配置好 IP，接好相应的网络。之后就把服务器的权限就给了王小勇，王小勇在服务器上部署什么程序这些我都不清楚了。

问：你给王小勇在江南移动机房安装了多少台服务器？

答：2017 年 8 月到 2018 年 2 月时候，只在庙高峰机房安装了一台服务器，后来王小勇又让我在移动的其他机房也安装了服务器，在 2018 年底的时候，庙高峰机房安装了 2 台服务器，细翻区机房 1 台，海沙机房 1 台。

问：服务器是谁提供的？

答：庙高峰的 2 台，细翻区的 1 台，都是王小勇提供的，他以快递发给我的，海沙机房那台服务器是网宿公司淘汰下来的设备。

问：服务器品牌特征？

答：庙高峰的 2 台、细翻区的 1 台都是联想的 ThinkServer 服务器，黑色，海沙机房那个是浪潮服务器，有多个硬盘仓，但只有一个仓位放了一个硬盘。

问：每个机房安装的服务器，分别在做什么业务？

答：我不知道具体每个服务器在做的业务，只是王小勇说的几个机房做的业务都是一样的。

问：王小勇的获利，你们是怎么分配的？

答：在2017年8月，王小勇谈合作的时候，他就说过，所在的返利分成三等份，一份王小勇，另外两份以转账的形式给我，我再把这一份给谢强。

问：王小勇给你转账的银行卡都有哪些？

答：总共三张银行卡，一张我名下的招商银行卡，一张是龚海平名下的农业银行卡，还有是李新培的农业银行卡。

问：你是否记得那几张银行卡的卡号？

答：不记得了。

问：我现在向你出示三张银行卡的交易流水记录，你仔细看下？

答：我看了，这三张银行卡的流水记录，确定是我使用的三张银行卡，我的招行卡：6225887310963566；龚海平农行卡：6228481098784355566；李新培农行卡：6228481098929839955。

问：王小勇每次给你转账是怎么转的？

答：转账时间一般是在每个月的月底或者次月月初，一般情况转账的大笔金额都是分到两张农业银行卡上，招商银行每个月是转一万元，但是王小勇第一次给我转账的时候，我当时还没有那两张农行卡，那次转账都是转到招商银行卡，每次转账都是通过网银的方式，因为我看到我的手机短信提醒，都是说的王小勇的超级网银向我使用的卡转账。

问：你是否知道王小勇给你转账是用的什么卡？

答：不知道，就知道是他个人名下的银行卡。

问：这三张银行卡里面那些资金是王小勇给你和谢强的获利？

答：三张银行卡中，所有王小勇给我转账的金额，都是跟王小勇合作的获利。

问：王小勇总共给你转账了多少钱？

答：具体的金额记不清，以你们调取的银行卡流水记录为准。

问：经大概核算，王小勇给你转了约190万？

答：好的，清楚了。

问：你收到的这些钱，你给了谢强多少？

答：大概70万。

问：为什么你给谢强的钱，不是平分的？

答：之前一直都是平分的，大概是在2018年底的时候，我就开始少分给他，就是因为我在工作受了不少的气。

问：你是怎么给的谢强的钱？

答：王小勇每次转账给我后，我就取现，之后我再将现金给谢强，而且都没有当面给过钱，一般都是趁他不在办公室时候，（不一致）直接放在他办公桌位置的包里。

问：以上所讲的是否属实？

答：属实。

问：你还有什么补充的？

答：没有了。

问：以上笔录你看后，与你所说的是否相符？

答：以上笔录我看过。与我所说相符。

被讯问人：新
2019.6.1



李新讯问笔录（第6次）

时间：2019年9月16日14时25分至2019年9月16日15时20分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1979年2月9日

身份证件种类及号码：42122519790209051X

现住址：越洋市明日镇太平里51号

联系方式：13975882558, 18608522558

户籍所在地：越洋市牡丹区晁阳尔村14栋1单元202号

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题。请你如实回答，对于本案无关的问题，你有权拒回答回，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你简单讲下你的犯罪事实？

答：我和王小勇合作，在移动机房架设服务器，获取用户上网数据，进行推广，还有就是2018年双11的时候，做了下淘宝的业务。

问：2018年双11时，王小勇做的淘宝业务是什么？

答：不知道具体情况，2018年11月底的时候给我说过做了这个业务。

问：你是否知道王小勇通过你架设的服务器在获取QQ用户的cookie？

答：之前都不知道，被抓当天指认服务器的时候才知道的。

问：你给王小勇合作主要是做什么事？

答：主要是就给他把服务器架设在机房，配置好IP，接入相应的数据，后面就把服务器的权限给王小勇，服务器上部署的程序都是他来操作了。

问：淘宝业务你是否知道王小勇是怎么做的？

答：不知道。

问：百度推广的业务你是否知道是怎么做的？

答：具体我也不知道，只听他说百度访问的时候带个推广 ID，然后就有获利，怎么实现这样的我不清楚，因为程序都是王小勇部署的。

问：淘宝业务你获利多少？

答：没有专门结算这个淘宝业务，都是每个月月底的时候打给我的钱，基本上都是百度推广的钱，双 11 时淘宝业务王小勇就只是说了下了做了那个业务，说了多了一点钱，大概就给了我 1 万元左右。

问：百度推广的业务获利多少？

答：具体就是我那几张银行卡收到的王小勇转的钱，其中分了部分给谢强。

问：你、谢强为什么要和王小勇一起合作做这些事情？

答：因为当时考虑到做这个事情比较安全，用户也无法感知，觉得只是违规了，不知道违法了，而且这个获利还可以，行业内有很多很多都在搞这个业务。

问：你是否还有什么补充的？

答：我现在已经知道我这个是违法犯罪，也非常后悔，在被你们抓的时候，我就意识到我的犯罪，我主动配合公安机关，第一时间交代了在江南的同伙和自己所知道所有的犯罪事实，并且也配合公安机关在放置有成百上千的服务器的移动机房内找到涉案的所有服务器，积极配合公安机关对服务器的取证。

问：以上所讲的是否属实？

答：属实。

问：你还有什么补充的？

答：没有了。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：李新

2019.9.19



王小勇讯问笔录（第1次）

时间：2019年3月11日10时25分至2019年3月11日1时20分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1980年5月10日

身份证件种类及号码：320945198005104531

现住址：江_东省_金陵市_海宁_区飞_龙大_道1024号18幢402室

联系方式：13905457523

户籍所在地：江_东省_金陵市_海宁_区飞_龙大_道1024号18幢402室

户籍所在地江_东省_金陵市_海宁_区飞_龙大_道1024号18幢402室

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你讯问本案的有关问题，请你如实回答，对与本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你和李新等人合作做了些什么？

答：让李新在江南移动机房安装了服务器，做百度推广，还有罗振龙介绍过来的项目，做了个淘宝客项目。问：淘宝客项目你做了些什么？

答：提供给周星辰QQ用户的COOKIE数据。

问：淘宝客项目你总共获利多少？

答：不到5万元，具体数字我不清楚。

问：淘宝客项目获利、是谁付给你的？

答：可能是罗振龙、也可能是李立，我跟这两个人都有很多的账务往来。

问：百度推广是怎么获利的？

答：都是从黄岩求那里获得的百度推广ID，然后百度公司根据ID的推广流量情况，每个月计算推广费。

问：你说下这些百度推广ID？

答：百度推广 ID 我不记得，倒是 ID 的注册的公司有金陵、上海、广州、深圳等。

问：你说下这些注册的公司情况？

答：这些 ID 的注册公司有的是黄岩求提供的，有的是我找的公司。

问：百度推广的获利，是怎么结算的？

答：百度是当月的推广量，次月结算、按月结算、具体每个 ID 的推广费都在百度的后台可以查询，只要输入对应的账号和密码就可以查看每个 ID 每天的流量情况、获利情况。

问：你说的查询的百度后台是什么？

答：网址是 mcp.baidu.com

问：那些账号的登陆的账号和密码呢？

答：账号和密码我不记得了，黄岩求给我发过文档的，邮箱里应该有。

问：百度推广的钱，谁支付给你的？

答：黄岩求找的公司注册地账号，获利就是黄岩求转给我，我找的公司，获利直接我来结算，每个月我和黄岩求结算，黄岩求都要给我对账，有详细的报表数据。

问：黄岩求的报表数据怎么给你的？

答：一般情况是邮件，也有直接 QQ 发文件。

问：你使用的邮箱？

答：523457584@qq.com, 13905457523@qq.com

问：百度推广这个事情，你总共获利多少？

答：扣税后总共获利 240 万，我个人获利 50 多万。其他钱都是给了李新、谢强。

问：你为什么要去做百度推广、淘宝客项目？

答：为了利益，开始不知道这个是违法，而且我行业内很多搞这个找钱的。

问：你所说的是否属实？

答：是。

问：你还有没有要补充的？

答：没有了。

问：以上笔录是你自己阅读，还是民警读给你听？

答：以上笔录我看过，与我所说的相符。

被讯问人：王小勇
2019 年 3 月 21 日



王小勇讯问笔录（第2次）

时间：2019年3月15日11时25分至2019年3月15日12时20分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：李新 性别：男 出生日期：1980年5月10日

身份证件种类及号码：320945198005104531

现住址：江~~东~~省~~金~~陵市~~海~~宁~~区~~飞龙大道1024号18幢402室

联系方式：13905457523

户籍所在地：江~~东~~省~~金~~陵市~~海~~宁~~区~~飞龙大道1024号18幢402室

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你讯问本案的有关问题，请你如实回答，对与本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你开始是怎么和李新谋划的？

答：我和李新说可以通过在移动机房放置自己服务器，采集用户的流量，然后进行流量劫持，然后利用这种方式可以很快获利。

问：你为什么要找上李新一起？

答：我和李新之前都在中泰数据，一起在江南省移动公司做工程，所以我知道王琦能接触到江南省移动核心机房，能接触到这些用户的网络流量数据，他有这个权限。

问：你平时都怎么和李新联络？

答：通常都是用QQ联络，很少打电话沟通。

问：你们架设的移动机房服务器IP、帐户和密码，都有谁知道？

答：就我和李新两个，李新应该是只和我说过。

问：你是通过这些服务器怎么牟利的？

答：主要是发广告、做推广、淘宝客，以及APK下载劫持。

问：百度推广的获利，是怎么结算的？

答：百度是当月的推广量，次月结算、按月结算、具体每个 ID 的推广费可以在百度后台查询，输入账号和密码就可以查看每个 ID 每天的流量、获利情况。

问：你说的查询的百度后台是什么？

答：网址是 mcp.baidu.com。

问：你是怎么分配获利的？

答：就是根据业务量来算的，每个月都不太一样。

问：你是怎么把钱给李新的？

答：一般通过超级网银转账的方式，有一次是用支付宝转的。

问：你大概转了多少钱给李新？

答：大概转了 190 万。

问：百度推广这个事情，你总共获利多少？

答：大概获利 240 万左右，我个人获利 50 多万，其余都给了李新、谢强他们。

问：在淘宝客项目里你是怎么和周星辰、罗振龙认识的？

答：罗振龙和我是通过网络认识的，他提出需要 QQ 用户的 Cookie 数据，然后将周星辰介绍给我认识。

问：你和周星辰怎么约定的？

答：我向周星辰承诺提供 QQ 用户的 Cookie 数据，并且互相约定了获利后的分配。

问：你又怎么找上陈铭羽的？

答：我和陈铭羽说了利用 QQ 用户的 Cookie 数据进行淘宝客推广的细节，让他负责技术方面的事情，并且和他约定了获利分配。

问：你为什么要去做百度推广、淘宝客项目？

答：为了利益，开始不知道这个是违法，而且我行业内很多搞这个找钱的。

问：你所说的是否属实？

答：是。

问：你还有没有要补充的？

答：没有了。

问：以上笔录是你自己阅读，还是民警读给你听？

答：以上笔录我看过，与我所说的相符。

被讯问人：



2019 年 3 月 15 日

谢强讯问笔录（第1次）

时间：2019年3月16日15时45分至2019年3月16日16时20分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：谢强 性别：男 出生日期：1982年9月10日

身份证件种类及号码：431088198209100037

现住址：江南省越洋市阅路区汉普科教园21栋102

联系方式：12975669049

户籍所在地：越洋市雨花区少善中路489号湾泊会名邸1栋2204房

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答。对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：简单讲下你和李新、王小勇合作涉嫌犯罪的情况？

答：从2017年下半年的时候，王小勇通过李新找到我谈合作做百度推广的事情，之后李新就在江南移动的机房架设了服务器，开始做百度推广的业务。

问：你是否知道王小勇做这个百度推广是怎么实现？

答：就是在用户访问百度的时候，追加王小勇的百度渠道ID，具体实施的方法我就不清楚了，我也没有去看过李新安装的服务器。

问：王小勇用江南移动的上网数据除了做百度推广，是否还有其他事？

答：其他我就知道了，王小勇、李新都没给我讲过。

问：百度推广这个事情，王小勇总共给了你多少？

答：王小勇都是把钱给李新的，具体给了多少给他我也不清楚，李新也没给我说，李新只是给我说是平分，李新大概给了我60万。

问：李新是怎么给你钱的？

答：都是给我现金，一般情况都是直接放在我办公桌抽屉或者是电脑包里，一般都

是我不在办公室的时候放的。

问：获利的钱都用来干什么了？

答：有 20 多万用于日常开销了，因为刚生小孩，开销比较大，其他的钱都用在炒股了。

问：说下你为什么还要和王小勇、李新一起合作做这个事情？

答：这个获利比较容易，而且李新给我说，百度推广是百度正常的业务，不影响上网用户正常的使用，不影响上网质量，我觉得比较安全，当时也不认为这个是违法，只是觉得违反了公司的规定。

问：那你在跟他们合作时，主要是做哪些事情？

答：主要就是允许他们接入 SIG 平台出来的 80 端口的请求数据。

问：你有没有补充的？

答：我已经认识到我这个是犯罪，在这里也关了半年、非常后悔参与这个事情，在被公安机关抓获当天，我也积极配合公安机关，主动交待了自己的所有犯罪事实，并积极配合公安机关，已经上交违法所得 30 万了，剩下部分我也联系家属在积极筹款，希望能争取从轻的机会。

问：以上所讲的是否属实？

答：属实。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：谢强

2019 年 3 月 16 日



谢强讯问笔录（第2次）

时间：2019年8月23日15时25分至2019年8月23日16时15分

地点：大都寇区看守所

询问人/讯问人（签名）：陈昊、袁文 工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊 工作单位：双祝市公安局大都寇区分局

犯罪嫌疑人：谢强 性别：男 出生日期：1982年9月10日

身份证件种类及号码：431088198209100037

现住址：江南省越洋市阅路区汉普科教园21栋102

联系方式：12975669049

户籍所在地：越洋市雨花区少善中路489号湾泊会名邸1栋2204房

问：我们是双祝市公安局大都寇分局的民警（出示警官证），现依法向你询问本案的有关问题，请你如实回答。对于本案无关的问题，你有权拒绝回答，同时你有申请办案人员回避的权利，听清楚了吗？

答：听清楚了。

问：你之前是做什么的？

答：我以前是管江南移动的骨干网，在江南移动省公司网管中心下属互联室，管理互联网内容，主要是负责省移动骨干网设备的运维，平时可以和华康的SIG平台维护工作人员对接。

问：你和李新是怎么认识的？

答：我们在同一个办公室上班，关系比较好。

问：你和李新都做了什么事情？

答：主要是架设服务器、线路给接好、维护服务器这些。

问：从什么时候开始，你和李新一起在江南省移动公司机房里面的SIG平台上，将用户上网数据镜像到你们架设的服务器？

答：应该是在2017年9月份左右开始，先是在庙高峰机房架设服务器，操作数据。之后又确定了其他几个机房，开始架设服务器，操作SIG平台数据。

问：你是怎么接入SIG平台数据的？

答：我之前通过协调华康运维公司的刘昌，接到了江南省移动主干网的 SIG 数据。

问：刘昌为什么能帮你配置数据？

答：我通知他做的，刘昌要听我的安排。

问：百度推广这个事情，你总共获利多少？

答：都是李新直接用现金的方式给我，总共给了我大概 60 万左右。

问：李新是怎么给你钱的？

答：一般都是趁我不在办公室的时候，偷偷放进我包里的。

问：你之前知道这么做是违法的吗？

答：之前李新给我说，百度推广是百度正常业务，不会影响上网质量，我以为这个比较安全，不认为这个是违法，觉得只是违反公司的规定。

问：以上所讲的是否属实？

答：属实。

问：你还有什么补充的？

答：我已经认识到这个犯罪行为，我也愿意接受法律的制裁，退还所有赃款。

问：以上笔录你看后，与你说的是否相符？

答：以上笔录我看过，与我所说相符。

被讯问人：刘强

2019 年 8 月 23 日

询问笔录

时间：2019年3月18日9时25分至2019年3月18日16时15分

地点：大都寇区看守所

询问人（签名）：陈昊、袁文

工作单位：双祝市公安局大都寇区分局

记录人（签名）：陈昊

工作单位：双祝市公安局大都寇区分局

被询问人：刘昌 性别：男

工作单位：华康运维公司

身份证件种类及号码：510000198403058934

联系方式：12975669049

问：我们是大都寇公安分局网安支队的民警。现依法对你进行询问。你必须如实回答公安民警的询问，不得编造、隐瞒事实，如实提供证言或证据，有意作伪证或隐匿罪证是要负法律责任的，你听清楚了吗？

答：听清楚了。

问：你平时的工作内容是什么？

答：我主要是和华康公司对接，维护放在江南移动公司机房的 SIG 平台。

问：谢强为什么会找上你？

答：因为江南移动公司如果需要把数据从 SIG 平台流量镜像到某个服务器的话，谢强就会来联系我。

问：谢强当时是怎么和你说的？

答：2017年8月份的时候，他和我说江南省移动公司有个项目要做，需要从 SIG 平台的端口镜像 80 和 8080 流量数据出来到服务器上面，并且说李新会来找我协调这个事情。

问：所以你之后怎么做的？

答：因为我要听谢强的安排，所以我就按照他的要求，把 SIG 平台的端口镜像 80 和 8080 流量数据镜像到了李新安装的服务器上。

问：你当时有详细问谢强这个究竟用来做什么吗？

答：移动机房里面的 SIG 平台数据就是用户全部上网的数据，谢强和我说这是江南移动公司的业务，我也就没往下具体问。

问：谢强有给你分利了吗？

答：没有

问：你还有什么要补充的？

答：没有

问：以上所说是否属实？

答：属实。

(以上笔录我看过，与我所说相符。)

被询问人：刘昂

2019年3月18日



关于腾讯 QQ 用户 COOKIES 被异常使用的反映材料

双祝市公安局网络安全保卫总队：

我单位工作人员发现，自 2018 年 9 月以来，有数百万条 QQ 用户的 COOKIES 数据存在异常使用的情况，集中反映在江南省移动的 QQ 用户。因该情况可能存在涉嫌犯罪的行为；且这些 QQ 用户的 COOKIES 数据疑似在双祝进行异常操作，特将该情况反映给贵单位，还请贵单位查处该犯罪行为。

腾讯科技（深圳）有限公司



2018年 12月 4 日

关于腾讯 QQ 用户数据的情况说明

腾讯 QQ 用户的相关数据存放在腾讯公司的服务器，当 QQ 用户本人操作加群、加好友、发说说等动作，会导致存储在腾讯公司服务器上的数据发生相应改变。当持有 QQ 用户“登录态”，在登录态有效期内，代劫持 QQ 用户加群、加好友、发说说等操作，也会导致存储在腾讯公司服务器上的数据发生相应改变。

腾讯科技（深圳）有限公司安全管理部



安全管理部

2019年3月20日

胡建中证司法鉴定中心

电子数据检验报告

胡中证司鉴数检字[2019]第 63 号

检验结论:

(1) 在送检的硬盘中检出“JiongTu”数据库文件,在数据库文中检出 3103035 条腾讯 QQ 号码的 Cookies 信息;

(2) 使用 QQ 号码登陆腾讯 QQ 空间后,网页登陆后 Cookies 中包含 u in 和 skey 值。使用 u in 和 skey 指可模拟该 QQ 登陆空间时的状态,查看该 QQ 号码的性别、年龄、所在城市、好友信息,获取该 QQ 号码的部分使用权限。



胡建中证司法鉴定中心

电子数据检验报告

胡中证司鉴数检字[2019]第 180 号

检验结论:

(1) 江南服务器运行程序具有抓取 QQ 用户的 Cookies 信息, 并上传到配置的服务器中的功能;

(2) 雷磊编写的程序可以读取服务器内信息, 并将 Cookies 数据中的 u in、skey 等信息上传;

(3) “ast_qq_uin_skey/zip” 和 “ast_u in_skey_pskey_pt4token.zip” 文件中的源代码与光盘 “江南服务器运行程序源代码” 目录下的源代码基本功能一致;

(4) ast 程序功能为拦截网卡中的 Cookies 信息;

(5) 送检硬盘二中操作系统设置的 IP 为 “58.218.205.75” 送检光盘 “雷磊电脑程序代码\数据读取” 目录下的 “Form1” 程序源代码中上传 Cookies 数据时的链接。

胡建中证司法鉴定中心

2019 年 3 月 18 日

司法鉴定专用章

双祝网安司法鉴定所

司法鉴定意见书

双网司鉴字[2019]第 0703 号

(1) 鉴定对象：

王小勇部署在中国移动通讯集团江南有限公司私自架设的服务器内的流量劫持程序。

(2) 鉴定结论：

经鉴定，该流量劫持程序在运行后，会对访问百度主页的链接进行添加、修改，实现访问百度主页的用户被冠以王小勇设定好的百度推广 ID 标识。



双祝网安司法鉴定所

2019年3月23日

双祝市公安局大都寇区分局

鉴定意见通知书

双公大刑鉴通字[2019] 369 号

李新:

我局聘请有关人员 IP 地址为 211.8.20.34、211.129.226.34、58.218.205.75 的服务器上运行的程序代码以及犯罪嫌疑人雷磊和陈铭羽作案电脑内储存的程序代码进行了程序功能鉴定，鉴定意见是：联想服务器硬盘复制盘（211.129.226.34）“/Home/ast/astServer”目录下的“ast”程序功能为：对指定网卡 eth3 的数据进行拦截，从数据中解析腾讯 QQ 网站的 Cookie 信息，将获取的 Cookie 信息到本地再上传到指定的 FTP 服务器“115.28.20.48”。

根据《中华人民共和国刑事诉讼法》第一百四十六条之规定，如果你对该鉴定意见有异议，可以提出补充鉴定或者重新鉴定的申请。



本通知书已收到。

被害人或其家属_____

鉴定意见无异议

2019年4月13日

涉案服务器情况说明

1. 服务器数量：

总共装了 4 台服务器，其中庙高峰机房装了 2 台，细翻区机房（车站北机房搬迁至细翻区）1 台，海沙机房 1 台。

2. 服务器公网 IP：

(1) 庙高峰机房 2 台服务器的公网 IP 分别为：211.129.226.34、211.8.20.34；

(2) 细翻区机房 1 台服务器的公网 IP 的是 211.8.29.78；

(3) 海沙机房 1 台服务器的公网 IP 的是 211.23.5.130。

3. 服务器接入 SIG 平台数据的数量：

(1) 庙高峰机房 2 台服务器的公网 IP 分别为：211.129.226.34、211.8.20.34；

(2) 细翻区机房 1 台服务器的公网 IP 的是 211.8.29.78；

(3) 海沙机房 1 台服务器的公网 IP 的是 211.23.5.130。

4. 服务器品牌特征：

(1) 庙高峰的 2 台、细翻区的 1 台均为联想 Think server 服务器，黑色；

(2) 海沙机房为浪潮服务器，有多个硬盘仓，仅有一个仓位存放了一个硬盘。

双祝市公安局大都寇区分局

二〇一九年三月二十日

大都寇区分局

银行流水及交易获利情况说明

经过银行查账，确认了王小勇通过网银转账的方式将 190.5 万元转给李新，具体情况如下：

1. 转账时间：月底或者次月月初

2. 转账金额：每个月转帐 1 万元到招商银行卡，第 1 次为 5000 元，其后为 1 万元；大笔金额转账到两张农业银行卡；其中有一次通过支付宝转账 1 万元到王琦支付宝账号。

3. 李新使用的三张银行卡：

(1) 本人招商银行卡：6225887310963566

(2) 其他两人农业银行卡：龚海平：6228481098784355566；李新培：
6228481098929839955

4. 李新支付宝账号：13975882558@139.com



双祝市公安局大都寇区分局

起诉意见书

双公大刑诉字【2019】181号

犯罪嫌疑人李新，大学学历，汉族，1979年2月9日出生，身份证号：42122519790209051X，户籍地：越洋市牡丹区晁阳尔村14栋1单元202号，现住址：越洋市明日镇太平里51号，电话号码：13975882558，18608522558。2019年3月8日因涉嫌非法获取计算机信息系统罪被大都寇区公安分局刑事拘留，2019年4月8日因涉嫌非法获取计算机信息系统数据罪被大都寇区人民检察院批准逮捕，现羁押于大都寇区看守所。

李新等人非法获取计算机信息系统数据一案，系深圳市腾讯计算机系统有限公司提供的案件线索，因使用QQ用户COOKIE数据的主嫌疑人在双祝，该案件由双祝市公安局网安总队受理，后由双祝市公安局指定我局管辖，我局于2019年1月31日立案，2019年3月3日，犯罪嫌疑人王小勇在北京被抓获，犯罪嫌疑人李新、谢强在江南省越洋市中国移动江南省分公司被抓获。

经公安机关依法侦查查明：

2018年9月初左右，长期在互联网上进行淘宝客推广的双祝市荣昌人周星辰在和朋友在网上交流时候了解到可以利用QQ号的Cookies进行推广的方法，后在网上认识了同样从事推广业务，且擅长程序设计的居住在双祝大都寇的雷磊（已取保候审），两人提出了在QQ用户不知情的情况下，利用QQ用户的Cookie数据内包含的uin（QQ号码）、skep/p_skep等参数，擅自操作用户QQ加入其指定的QQ群和在QQ空间发布包含淘宝商品链接的“说说”的方案，该方案经擅长程序设计的雷磊测试后认为可行，但为了实现最大利益，需要获取大量的QQ用户Cookie数据。2018年9月底左右，周星辰与通过互联网认识的罗振龙谈到利用QQ号进行淘宝客推广的事情，问罗振龙能否获取大量QQ用户的Cookies数据，因罗振龙知道与其长期合作的王小勇能获得江南的移动用户上网数据流量，于是罗振龙向王小勇提出获取QQ用户的Cookies数据的要求，程志找到陈铭羽（已取

保候审)做技术支持,让陈铭羽和周星辰、罗振龙交流具体技术细节,根据周星辰、雷磊提出获取QQ用户Cookies数据的具体要求,从王小勇本人伙同李新(现冬华软件公司员工)和谢强(江南省移动公司网管中心工作人员)私自架设在江南省移动运营商机房的服务器中,该服务器经非法配置后能获得江南省移动骨干网中上网(80和8080端口)镜像数据,开发和部署程序获取QQ用户的Cookies数据并传输到周星辰提供的FTP服务器内。周星辰的合伙人雷磊通过程序将FTP内的数据读取并保存到远程服务器的SQL SERVER数据库内,然后雷磊编写程序在其使用的电脑上读取并利用储存在SQL SERVER的QQ用户Cookies,在QQ用户不知情的情况下实现操作用户QQ加入其指定的QQ群、在QQ空间发布包含淘宝商品链接的“说说”和关注特定的QQ公众号等功能。2018年9月至今,经第三方司法鉴定机构鉴定(扣押服务期内储存Cookies数量),该团伙非法获取了3103035个QQ号码的登录Cookie信息,利用这些数据,通过在推广阿里妈妈平台上淘宝客链接,获利上百万元。

资金结算由周星辰按比例支付给雷磊、罗振龙;罗振龙按比例支付给王小勇,王小勇支付给陈铭羽、李新和谢强。

另据公安机关查明,2017年10月份以来,犯罪嫌疑人伙同李新(现冬华软件公司员工)和谢强(江南省移动公司网管中心工作人员)利用江南省移动主干网用户上传数据进行百度推广,修改用户上传访问百度时的推广ID非法获利。王小勇提供服务器,李新在谢强的帮助下私自架设这些服务器到江南省移动机房,并配置好网络和接入江南移动用户上传的80端口和8080端口所有的get数据。由王小勇部署程序到服务器,程序实现修改用户上传访问百度时的推广ID。程志使用的百度推广ID都是由黄岩求提供,黄岩求每个月都与王小勇结算百度推广的收益并有详细的报表数据,经查王小勇使用江南移动流量进行百度推广的获利约250万元,其中转了190余万元给李新,李新先后以现金的方式给了谢强约60万元。上述等人到案后,对非法获取计算机信息系统数据后,进行牟利的犯罪事实供认不讳。

认定上述的犯罪事实有犯罪嫌疑人李新以及谢强、王小勇的供述与辩解、电

子证物检查工作记录、辨认笔录等证据证实。

以上犯罪事实清楚，证据确实、充分，足以认定。

综上所述，犯罪嫌疑人李新的行为已触犯《中华人民共和国刑法》第二百八十七条之二之规定，涉嫌帮助信息网络犯罪活动罪。根据《中华人民共和国刑事诉讼法》第一百六十条之规定，特呈请侦查终结，将本案移送人民检察院审查，依法起诉。

此致

双祝市大都寇区人民检察院



附：

1. 本案卷宗柒卷；
2. 犯罪嫌疑人王小勇（另案处理）、李新、谢强（另案处理）现押于大都寇区看守所，犯罪嫌疑人雷磊（18623332930），陈铭羽（15311200130）现取保候审在家；
3. 随案移交物品同步录音录像、电子数据光碟 50 张。