**电子数据的提取、固定与恢复能力验证计划**

**结 果 反 馈 表**

**参加机构代码：** Z0269

|  |  |
| --- | --- |
| **检验结果** | SHA256校验码，文件镜像：  491DC6C7993599F5F38E130DB8B0108B43E398B6DEEE6A27CF44AC4B9190E4A6 |
| **鉴定意见**  **表述** | 经检验鉴定，该手机检材系统于2019年8月9日10时58分经https://pan.baidu.com/s/1rN2sOp77\_uuyyYiXcaefaA下载文件RED.apk。该apk具有未经用户授权获取通讯录联系人姓名（contactName）、联系人电话（contactPhone）、短信类型（smsType）、短信名称（smsName）、短信发送对端（smsPhone）、短信接收时间（smsTime）、短信内容（smsBody）、手机内安装应用名称（appName）、应用包（appPackage）、应用版本（appVersion）、应用大小（appFileSize）、应用安装时间（appInstallTime）等信息的功能，并将手机获取信息加密（密码：19\_08.05r）压缩为文件Readdata.zip，上传至http://10.0.102.135:8888/api/demo。检验累计提取、固定相关文件RED.apk、Readdata.zip、readdata.xml、readdata.xml导出结果.xlsx（该文件内含通讯录、短信、安装信息等内容416条）共4个，大小共计994KB |
| **检验方法和**  **工具** | 技术标准和方法：  《GB/T 29360-2012 电子物证数据恢复检验规程》、  《GB/T 29361-2012电子物证文件一致性检验规程》  《GB/T 29362-2012 电子物证数据搜索检验规程》、  《GA/T 754-2008 电子数据存储介质复制工具要求及检测方法》、  《GA/T 755-2008 电子数据存储介质写保护设备要求及检测方法》、  《GA/T 756-2008 数字化设备证据数据发现提取固定方法》、  相关软硬件设备：  取证大师V6.1.65366RTM、美亚手机大师V2.6.31301 RTM、平航手机取证分析软件 PF5100、泓连火眼证据提取软件、Jadx ver.1.0.0、java ver.1.8.0\_181 |
| **鉴定过程概述** | 一、启动编号为 Z0269电子物证检验工作站，windows7操作系统启动正常，用杀毒软件对工作站进行杀毒。  二、将检材Z0269备份，标记为Z0269-1，并采用MD5值和SHA256值校验备份检材完整性。检材MD5值为：4209E66A9F0D1941CCBD0838307EAFFB;SHA-256值: 491DC6C7993599F5F38E130DB8B0108B43E398B6DEEE6A27CF44AC4B9190E4A6。  三、将编号为Z0176-1的检材以只读方式接入编号为 Z0176电子物证检验工作站。  四、使用取证大师V6.1.65366RTM、美亚手机大师V2.6.31301 RTM、平航手机取证分析软件 PF5100、泓连火眼证据提取软件、Jadx ver.1.0.0、java ver.1.8.0\_181分别加载检材，提取、检验相关数据，如下：  1、检材基本信息  查找手机基础信息存储文件packages.xml、IMEI.xml，获取手机基础信息，型号：Xiaomi 2014813；系统版本：Android 5.1.1；IMEI：867464023173529。如图：    （图：型号、系统版本提取）    （图：IMEI号提取）  2、经美亚手机大师提取，该手机提取有（含已删除）通讯录、通话记录、短信、媒体文件、文档、即时通讯、网盘、浏览记录等内容累计15944条，如图：    （图：手机大师提取结果）  3、通过浏览器记录、百度网盘下载记录显示，该手机于2019年8月9日10时58分经https://pan.baidu.com/s/1rN2sOp77\_uuyyYiXcaefaA下载文件RED.apk。在路径 \media\0\Xiaomi\提取文件RED.apk（SHA256：81120dbaa9715034f89e45b4377e247da91cf5c107dcbbadfa7e208a49d7b9be）。如图：    （图：浏览器记录）    （图：网盘下载记录）    （图：文件提取）   1. 使用jadx V1.0.0 Android反编译工具分析RED.apk文件，结合泓连火眼证据提取软件对检材内容进行提取。   （1）jadx V1.0.0 Android反编译工具分析RED.apk文件,该APP在未经用户同意的情况下，分别获取了用户的通讯录联系人姓名（contactName）、联系人电话（contactPhone）、短信类型（smsType）、短信名称（smsName）、短信发送对端（smsPhone）、短信接收时间（smsTime）、短信内容（smsBody）、手机内安装应用名称（appName）、应用包（appPackage）、应用版本（appVersion）、应用大小（appFileSize）、应用安装时间（appInstallTime）如图：    （图：权限获取列表1）  获取数据列表  （图：权限获取列表2）  （2）发现该app对未经用户同意收集的信息生成名为readdata.xml的文件，并以明文密码“19\_08.05r”加密压缩为Readdata.zip的文件。如图：  生成的压缩包密码  （图：加密压缩）  通过弘连火眼取证分析软件，搜索手机镜像内，发现\分区1[hda0]\media\0\存在Readdata.zip（SHA256：fe746d42587c4fe1adc8bca990a6673b196ae4bb7e6936c97bf0a5de2e6c6  b84）文件。如图：    （图：压缩文件）  提取文件Readdata.zip，并以“19\_08.05r”作为密码解压，获得文件readdata.xml（SHA256值：DEFBD974AB0A85B6CF04D7EA5270CBC7252C63DAB2C646BA9CF292EAD912DCAF  ）。如图：    （图：解压文件）  （3）将导出的readdata.xml导入excel，共发现203个联系人，以电话为基准条件进行去重，去掉1个重复值，最后获得202个唯一值。  获取通讯录去重  （图：导出表格）  （4）通过对RED.app的代码进行查看，在其MainActivity下发现checkandUpload代码，该app利用post的方式将Readdata.zip数据回传至http://10.0.102.135:8888/api/demo。如图：    （图：回传地址）  五、经检验、鉴定，该检材内文件RED.apk具有未经用户授权获取通讯录联系人姓名（contactName）、联系人电话（contactPhone）、短信类型（smsType）、短信名称（smsName）、短信发送对端（smsPhone）、短信接收时间（smsTime）、短信内容（smsBody）、手机内安装应用名称（appName）、应用包（appPackage）、应用版本（appVersion）、应用大小（appFileSize）、应用安装时间（appInstallTime）等信息的功能，并将手机获取信息加密（密码：19\_08.05r）压缩为文件Readdata.zip，上传至http://10.0.102.135:8888/api/demo。  检验累计提取、固定相关文件RED.apk、Readdata.zip、readdata.xml、readdata.xml导出结果.xlsx（该文件内含通讯录、短信、安装信息等内容416条）共4个，大小共计994KB。如图：    （图：检出结果） |

**注：本反馈表可添加附页。**