Generated

北京网神洞鉴科技有限公司

司法鉴定所

电子数据司法鉴定意见书

司法鉴定许可证号：110021187

声 明

1. 司法鉴定机构和司法鉴定人根据法律、法规和规章的规定，按照鉴定的科学规律和技术操作规范，依法独立、客观、公正进行鉴定并出具鉴定意见，不受任何个人或者组织的非法干预。

2. 司法鉴定意见书是否作为定案或者认定事实的根据，取决于办案机关的审查判断，司法鉴定机构和司法鉴定人无权干涉。

3. 使用司法鉴定意见书，应当保持其完整性和严肃性。

4. 鉴定意见属于鉴定人的专业意见。当事人对鉴定意见有异议，应当通过庭审质证或者申请重新鉴定、补充鉴定等方式解决。

地址：北京市西城区西直门外南路26号院1号楼-4至5层101内3层309、310、311室（邮编：100032）

联系电话：010-56509288

北京网神洞鉴科技有限公司司法鉴定所

电子数据司法鉴定意见书

编号：网神洞鉴[2022]数鉴字第251号

统一司法鉴定案件编号：22010209187119679

1. 基本情况
   1. 委托人

北京市公安局公共交通安全保卫分局西直门站派出所

* 1. 委托鉴定事项

1.对送检手机、平板电脑的“隔空投送”功能记录进行提取、分析；

2.对送检手机、平板电脑的基本信息和即时通讯数据进行提取鉴定。

3.对笔记本电脑内的数据进行提取鉴定；

* 1. 受理日期

2022年10月14日

* 1. 鉴定材料

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 检材编号 | 检材信息 | | | | | |
| 2022-251-001 | 名称 | 手机 | | 数量 | | 1 |
| 品牌 | iPhone | | 型号 | | MLUA3LL/A |
| IMEI | 359052379903584  359052379207846 | | | | |
| 保存状况 | 外表完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 备注 | “嫌 蒋敦宏”、“0564” | | | | |
| 2022-251-002 | 名称 | 平板电脑 | 数量 | | 1 | |
| 品牌 | iPad | 型号 | | iPad Pro | |
| SN | DMPDTAQUPV03 | | | | |
| 保存状况 | 外表完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 备注 | “嫌 蒋敦宏”、“0095” | | | | |
| 2022-251-003 | 名称 | 笔记本电脑 | 数量 | | 1 | |
| 品牌 | SONY | 型号 | | SVP132A18T | |
| SN | 545897270003564 | | | | |
| 保存状况 | 外观完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 备注 | “嫌 蒋敦宏” | | | | |
| 2022-251-003-001 | 名称 | 硬盘 | 数量 | | 1 | |
| 品牌 | SAMSUNG | 型号 | | MZ-NTD256/000 | |
| SN | S15ZNYAD727991 | | | | |
| SHA256 | 3831332feb6d90e1ca21253944ac2fbf5190e4d550c229b754c58ff8778c3662 | | | | |
| 备注 | “2022-251-003内置硬盘” | | | | |

1. 基本案情

据委托介绍，2022年10月21日8时许，蒋敦宏在北京市地铁4号线魏公村站开我往平安里的地铁列车车厢内使用其携带的苹果手机使用“隔空投送”功能随机向其他乘客发送一段带有不当言论的音频，后被检举至公安机关。

1. 资料摘要
   1. 鉴定人员：

谢春磊、徐志强

* 1. 鉴定日期：

2022年10月24日至2022年11月7日

* 1. 鉴定地点：

北京市西城区西直门外南路26号院1号楼-4至5层101内3层309、310、311室

* 1. 鉴定材料的选取、使用：

本次鉴定使用了所有鉴定材料进行检验。

* 1. 采用的技术标准、技术规范或者技术方法：

本次鉴定依据SF/Z JD0400001-2014《电子数据司法鉴定通用实施规范》、GA/T 976-2012《电子数据法庭科学鉴定通用方法》、GB/T 29360-2012《电子物证数据恢复检验规程》、GB/T 29362-2012《电子物证数据搜索检验规程》、SF/Z JD0401002-2015《手机电子数据提取操作规范》和SF/Z JD040201103-2015《即时通讯记录检验操作规范》进行搜索。

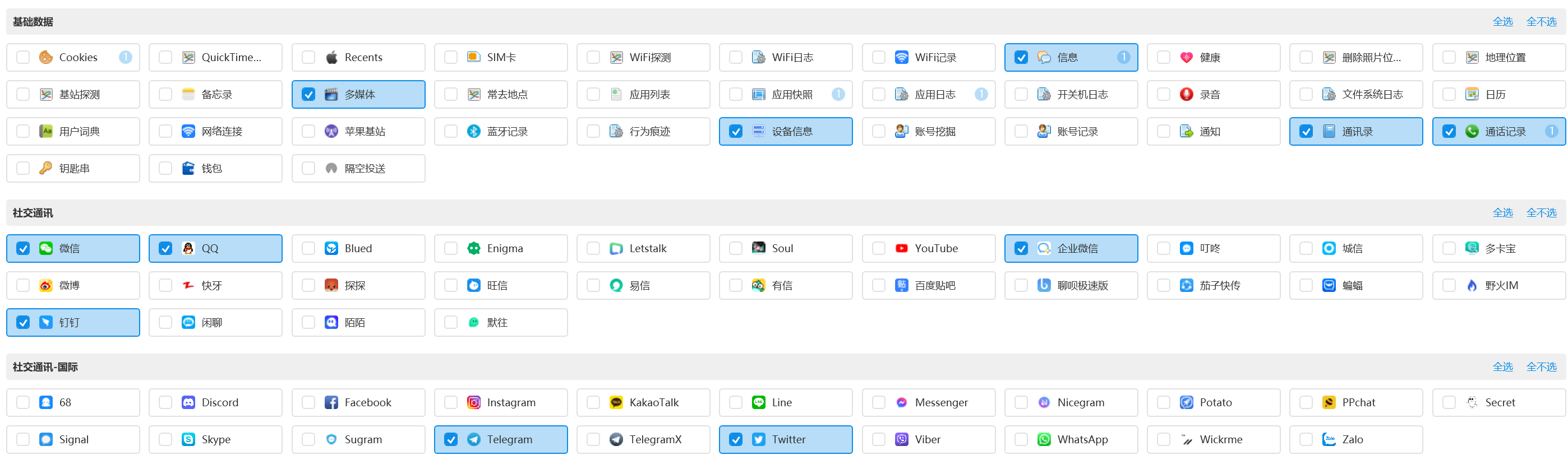
* 1. 检验使用的仪器设备：

本次鉴定使用WSDJ/HW-A-T30/G04（计算机的设备编号）和WSDJ/HW-A-MAC/G01（macOS主机的设备编号）设备进行检验。鉴定使用软件：盘古石手机取证分析系统7.5版、盘古石计算机取证分析系统7.0版和哈希值计算工具HashMyFiles 2.36版和光盘刻录工具Nero Express 8.3版。

本次鉴定开始前，启动杀毒软件奇安信天擎终端安全管理系统10.11版对电子数据检验工作站的系统进行了杀毒，未检测到运行的恶意程序，病毒库更新日期为2022年10月21日，同时对检验工作站及周边环境进行了防磁、防水、防静电和防震保护。

1. 鉴定过程
   * 1. 检材2022-251-001

在屏蔽环境下打开检材手机“2022-252-001”并开启飞行模式。使用盘古石手机取证分析系统对检材手机进行提权提取并分析其中的基本信息、多媒体记录、微信记录、QQ记录、企业微信记录、钉钉记录、Telegram记录和Twitter记录。所使用的配置信息如下图所示：



* + - 1. 基本信息

查看检材手机的设备信息，检材手机的设备品牌为“iPhone”，型号为“MLUA3LL/A”，IMEI为“359052379903584”和“359052379207846”，系统版本为“iOS 15.4”，设备名称为“iPhoneF”。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的基本信息。检材手机中成功提取到通讯录记录共计419条，其中已删除记录0条；通话记录共计205条，其中已删除记录0条；短信记录共计1,514条，其中已删除记录0条。部分短信内容如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

* + - 1. 多媒体

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的多媒体记录。

多媒体记录共计117条，其中已删除记录0条。部分多媒体记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

* + - 1. 微信

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的微信记录。检材手机中成功提取到2个微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“democrachina（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

检材手机中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计8,308条，其中已删除记录33条。部分微信记录如下图所示：



检材手机中成功提取到微信帐号“democrachina（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计12,175条，其中已删除记录68条。部分微信记录如下图所示：

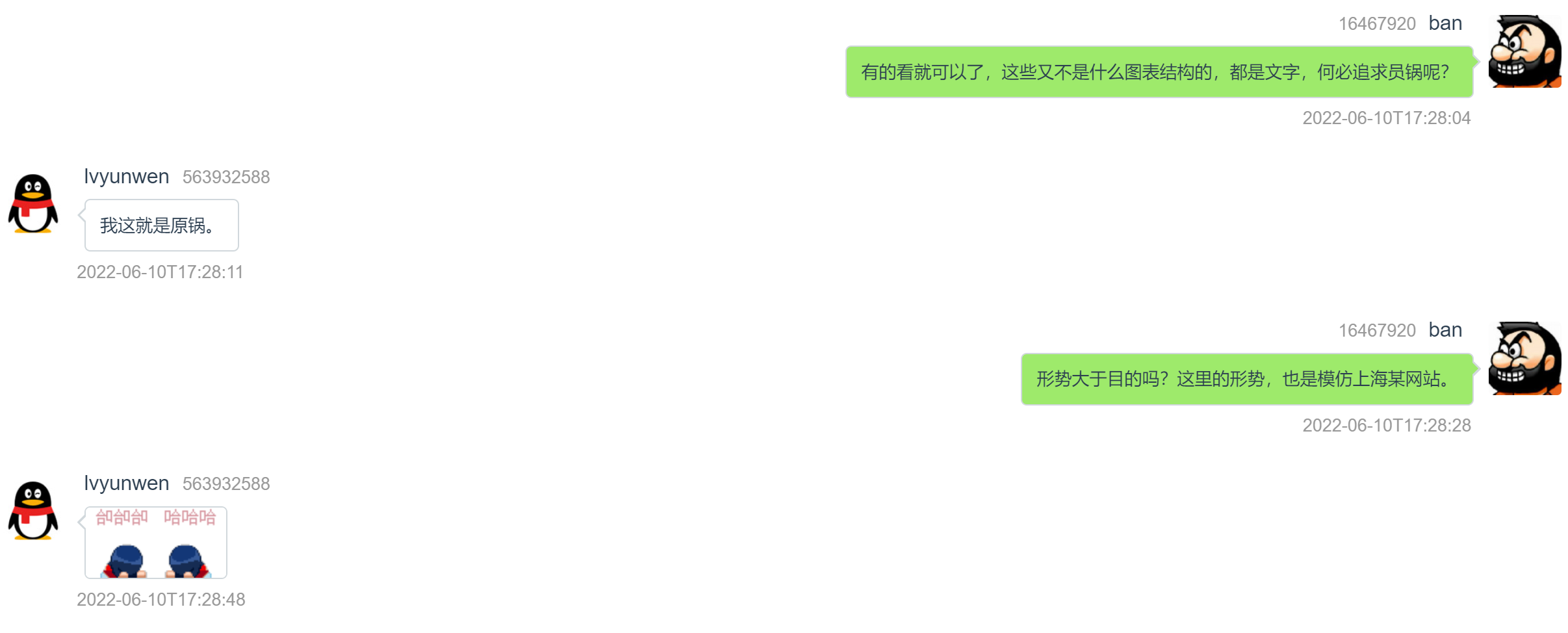


将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

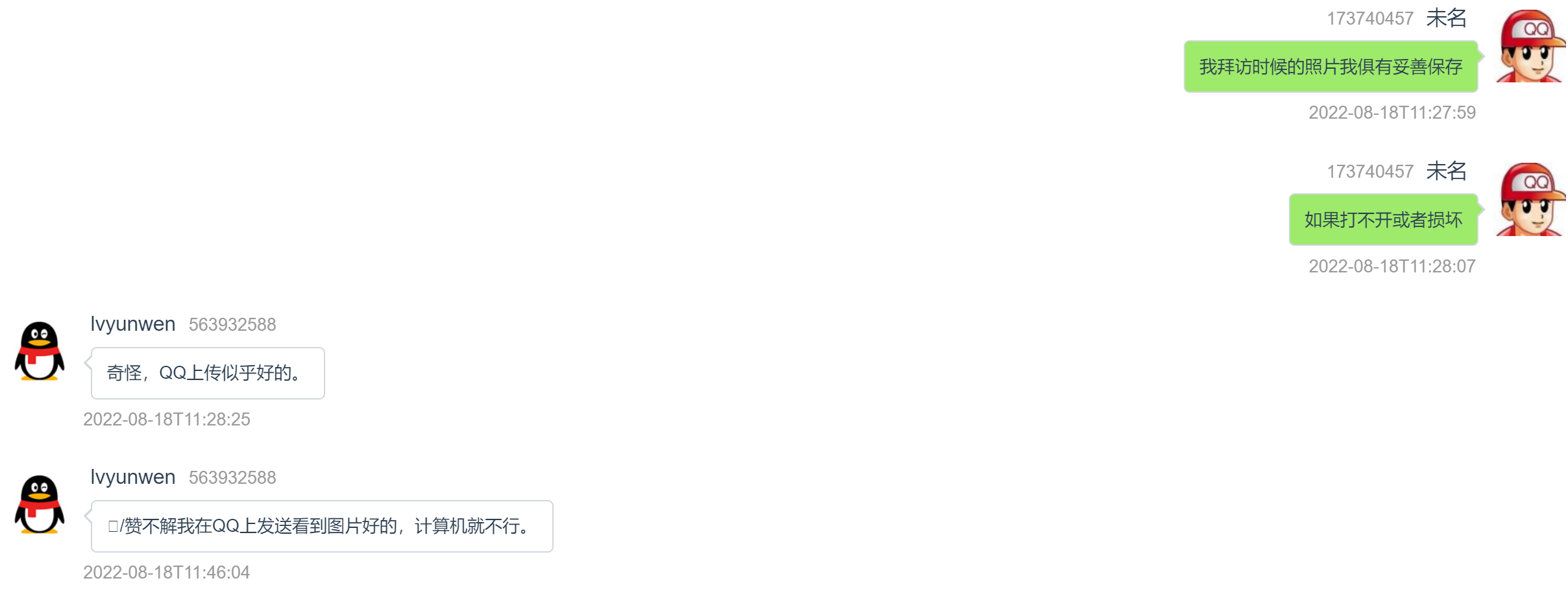
* + - 1. QQ

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的QQ记录。检材手机中成功提取到2个QQ帐号“16467920（用户名：16467920；昵称：ban）”和“173740457（用户名：173740457；昵称：未名）”的使用记录。

检材手机中成功提取到QQ帐号“16467920（用户名：16467920；昵称：ban）”的使用记录共计6,764条，其中已删除3条。部分QQ记录如下图所示：



检材手机中成功提取到QQ帐号“173740457（用户名：173740457；昵称：未名）”的使用记录共计279条，其中已删除0条。部分QQ记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

=================此页以下为空白===============

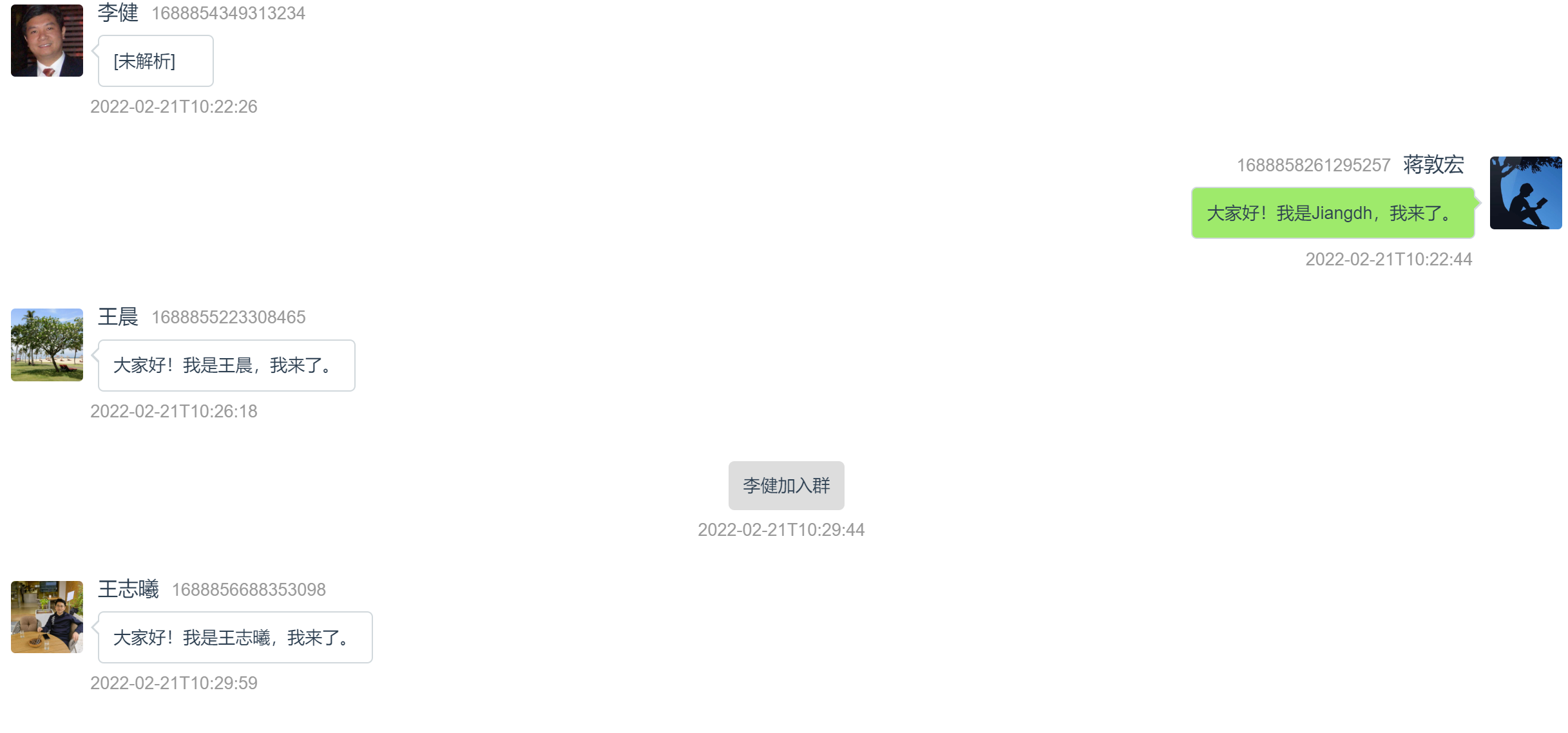
* + - 1. 企业微信

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的企业微信记录。检材手机中成功提取到6个企业微信帐号“（帐号：1688854878268925；昵称：蒋敦宏）”、“（帐号：1688858261295257；昵称：蒋敦宏）”、“（帐号：1688850555422033；昵称：蒋敦宏）”、“（帐号：1688856663353031；昵称：蒋敦宏）”、“（帐号：1688850263755318；昵称：蒋敦宏）”和“（帐号：1688851310316007；昵称：蒋敦宏-北京市远东律师事务所）”的使用记录。

检材手机中成功提取到企业微信帐号“（帐号：1688854878268925；昵称：蒋敦宏）”的记录共计203条，其中已删除记录9条。部分企业微信记录如下图所示：



检材手机中成功提取到企业微信帐号“（帐号：1688858261295257；昵称：蒋敦宏）”的记录共计268条，其中已删除记录5条。部分企业微信记录如下图所示：



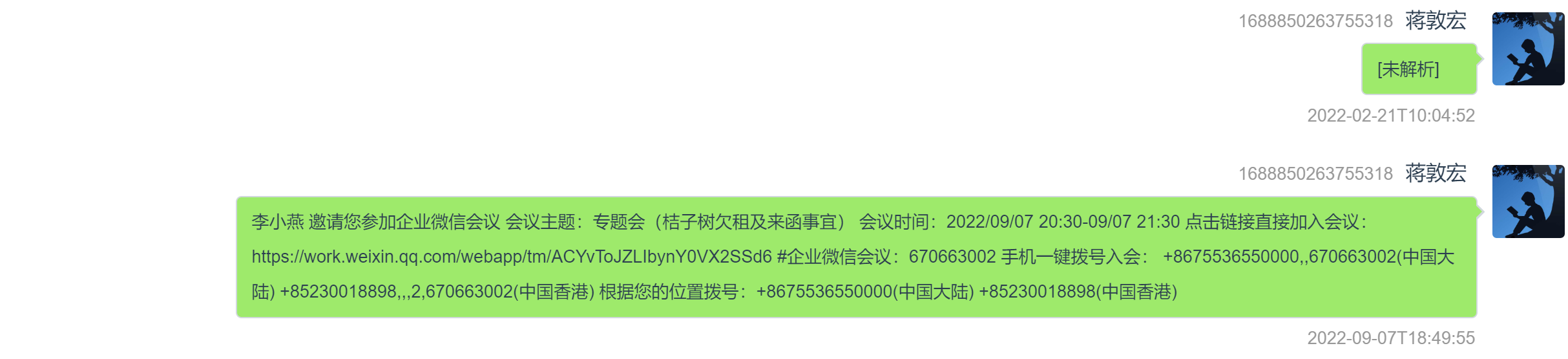
检材手机中成功提取到企业微信帐号“（帐号：1688850555422033；昵称：蒋敦宏）”的记录共计122条，其中已删除记录4条。部分企业微信记录如下图所示：



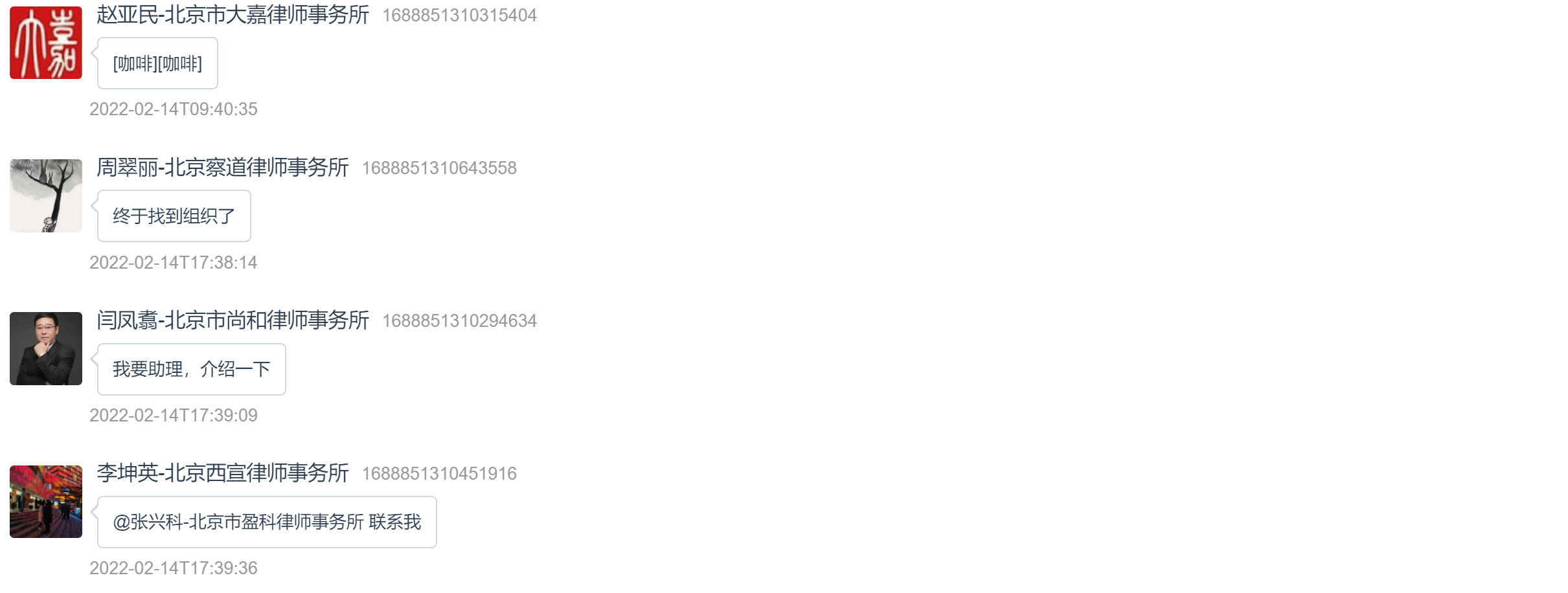
检材手机中成功提取到企业微信帐号“（帐号：1688856663353031；昵称：蒋敦宏）”的记录共计198条，其中已删除记录2条。部分企业微信记录如下图所示：



检材手机中成功提取到企业微信帐号“（帐号：1688850263755318；昵称：蒋敦宏）”的记录共计271条，其中已删除记录0条。部分企业微信记录如下图所示：



检材手机中成功提取到企业微信帐号“（帐号：1688851310316007；昵称：蒋敦宏-北京市远东律师事务所）”的记录共计28,806条，其中已删除记录101条。部分企业微信记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

* + - 1. 钉钉

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的钉钉记录。检材手机中成功提取到1个钉钉帐号“（帐号：124537349；昵称：ban）”的使用记录。

检材手机中成功提取到钉钉帐号“（帐号：124537349；昵称：ban）”的使用记录共计1,199条，其中已删除记录32条。部分钉钉记录如下图所示：

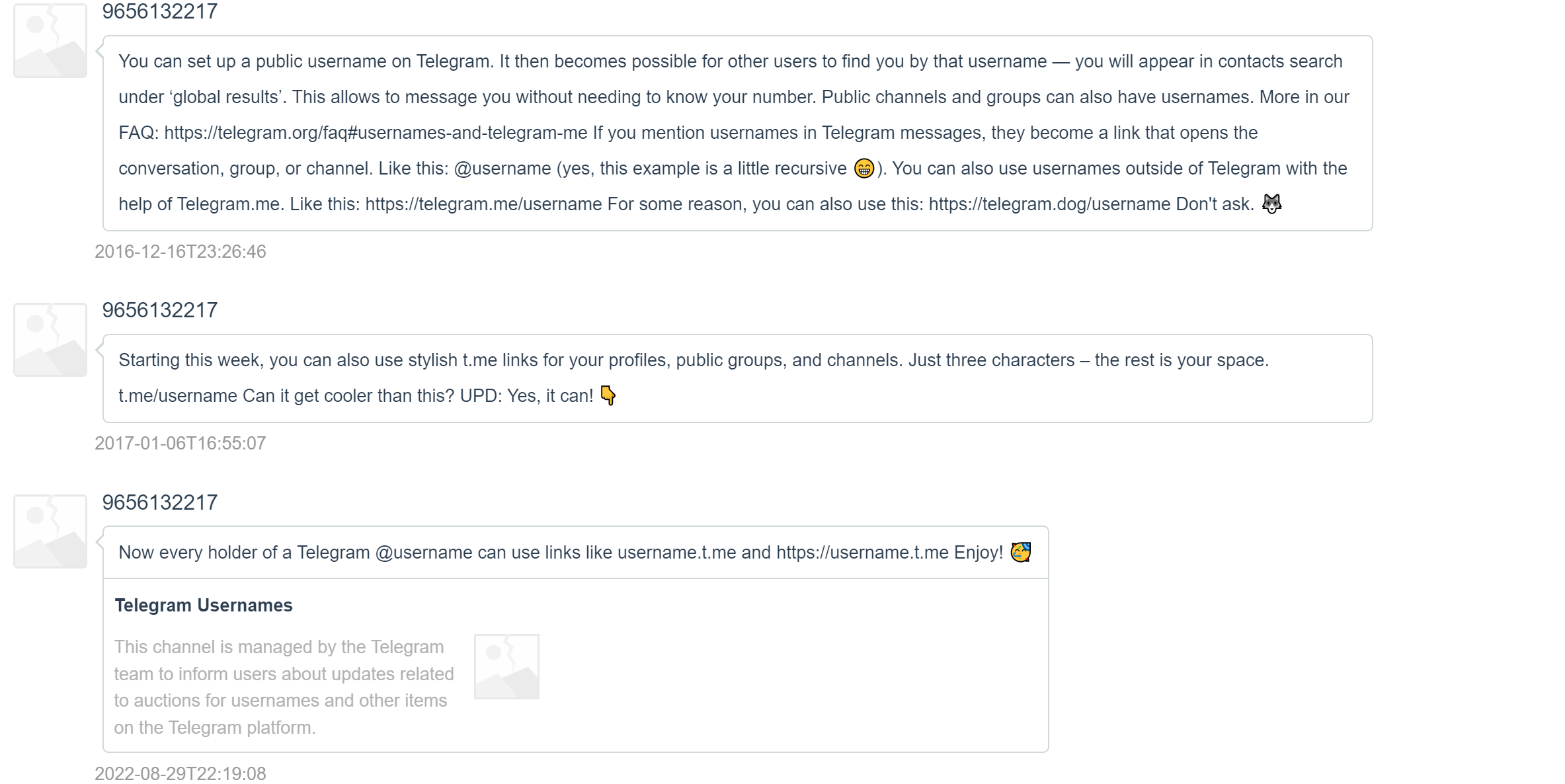


将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

* + - 1. Telegram

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的Telegram记录。检材手机中成功提取到1个Telegram帐号“dasung996（帐号ID：35244388451；昵称：John Smith）”的使用记录。

检材手机中成功提取到Telegram帐号“dasung996（帐号ID：35244388451；昵称：John Smith）”的记录共计11,783条，其中已删除记录0条。部分Telegram记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

=================此页以下为空白===============

* + - 1. Twitter

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的Twitter记录。检材手机中成功提取到2个Twitter帐号“（帐号：113052019；昵称：sandanderen）”和“（帐号：937104152294866944；昵称：yiqiwan2018）”的使用记录。

检材手机中成功提取到Twitter帐号“（帐号：113052019；昵称：sandanderen）”的记录共计7,350条，其中已删除记录0条。部分Twitter记录如下图所示：



检材手机中成功提取到Twitter帐号“（帐号：937104152294866944；昵称：yiqiwan2018）”的记录共计1,644条，其中已删除记录0条。部分Twitter记录如下图所示：

=================此页以下为空白===============



将上述所有记录保存至证据U盘中“\2022-251-001\其他信息\”目录下。

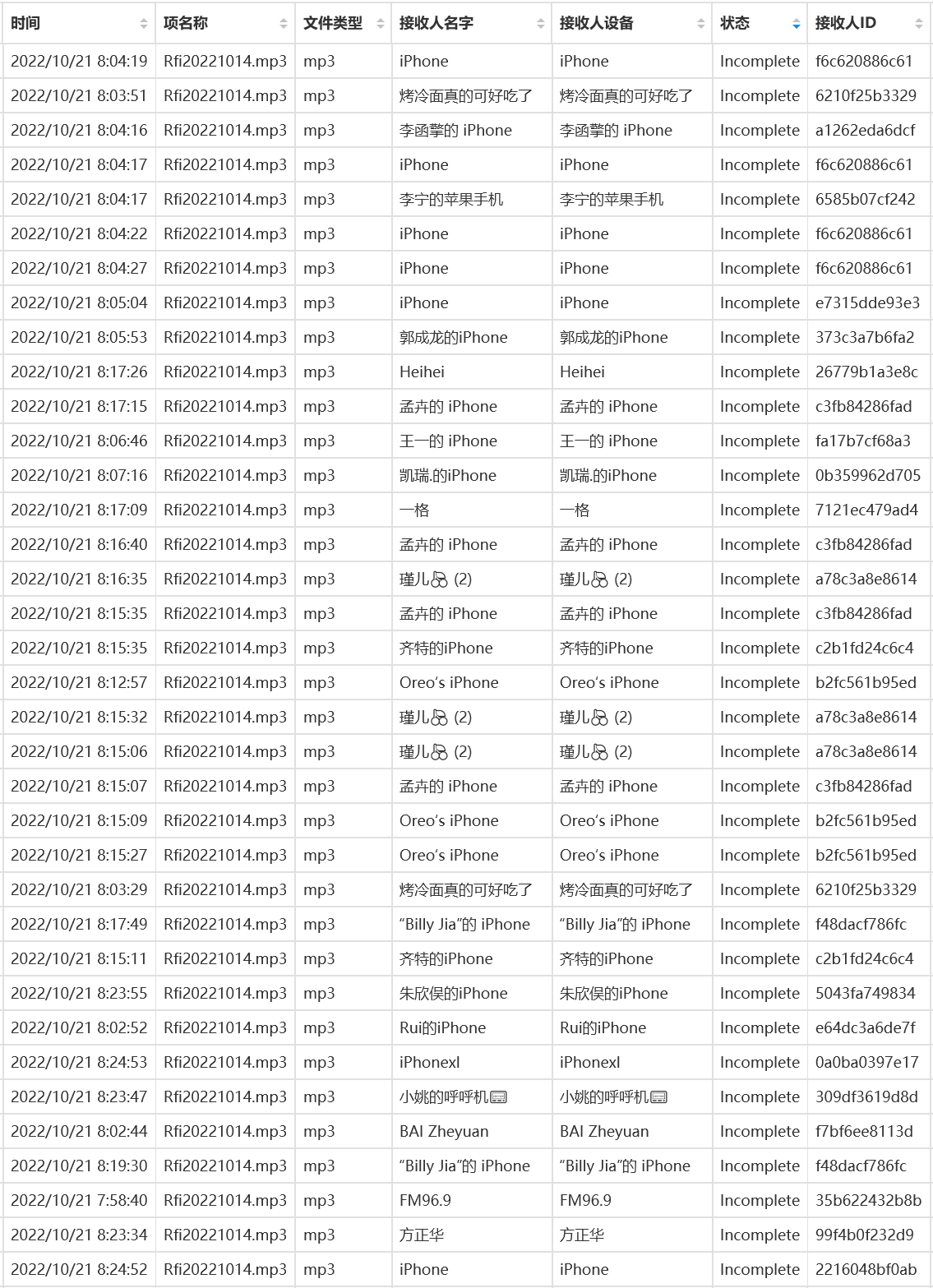
* + - 1. 隔空投送

在屏蔽环境下打开检材手机“2022-251-001”并开启飞行模式。依次点击“设置-隐私-分析与改进-分析数据”，搜索并导出日志文件“sysdiagnose\_2022.10.22\_23-56-24+0800\_iPhone-OS\_iPhone\_19E241.tar.gz”。利用盘古石手机取证分析系统对该日志文件的隔空投送记录进行分析。所使用的配置信息如下图所示：

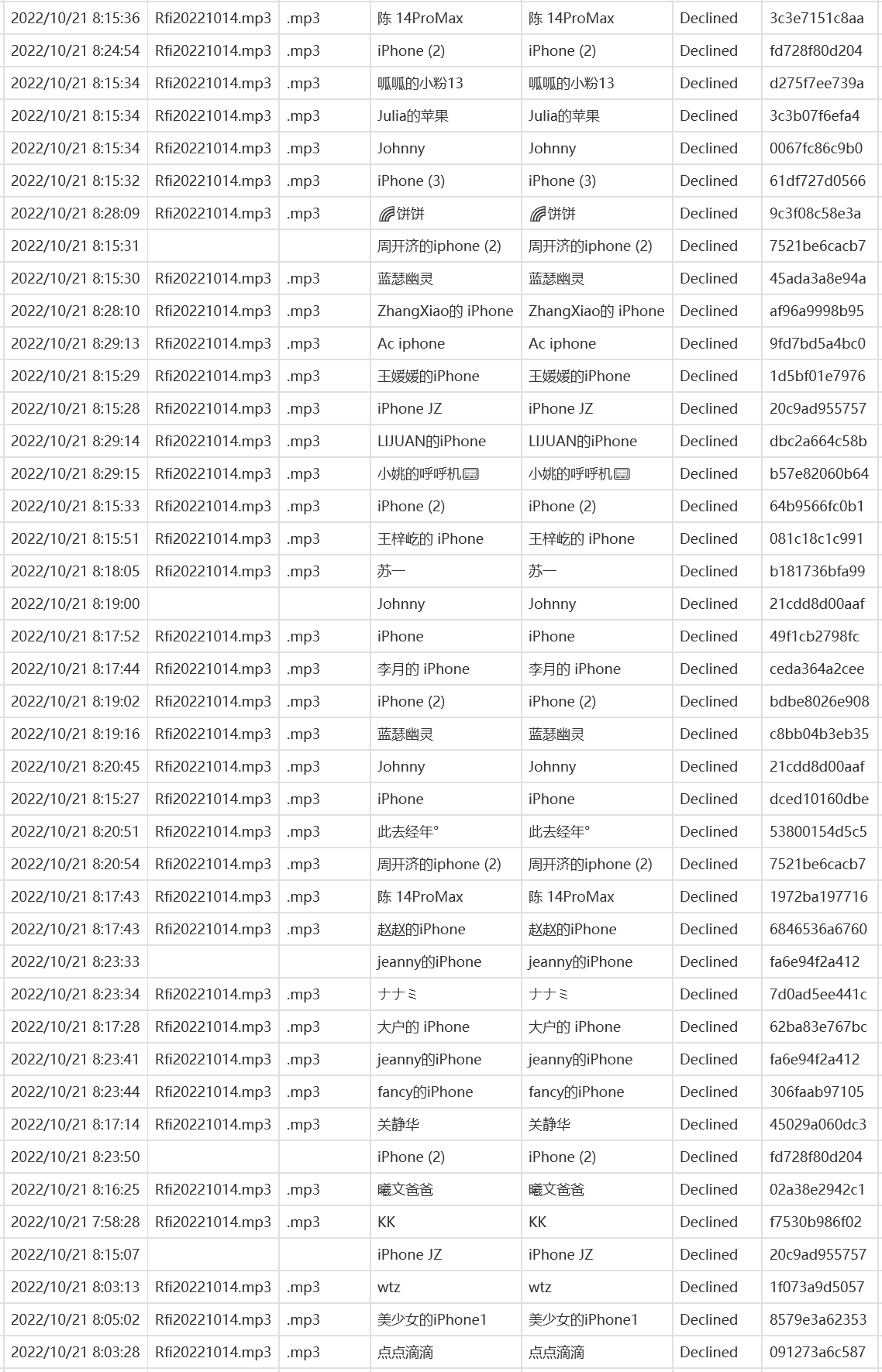


检材手机中成功解析出隔空投送传出文件记录共计137条，其中已删除记录共计0条。

其中“状态”为“Incomplete”记录共计36条。详细信息如下图所示：



其中“状态”为“Declined”记录共计81条。详细信息如下图所示：





其中“状态”为“Accepted”记录共计20条。详细信息如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-001\隔空投送\”目录下。

* + 1. 检材2022-251-002

在屏蔽环境下打开检材平板电脑“2022-251-002”并开启飞行模式。使用盘古石手机取证分析系统对检材平板电脑进行备份提取并分析其中的基本信息、多媒体记录、微信记录和隔空投送记录。所使用的配置记录如下图所示：



* + - 1. 基本信息

查看检材平板电脑的设备信息，检材平板电脑的设备品牌为“iPad”，型号为“iPad Pro”，SN为“DMPDTAQUPV03”，系统版本为“iOS 14.3”，设备名称为“Jianghz”。

使用盘古石手机取证分析系统对检材平板电脑进行备份提取，分析其中的基本信息。检材平板电脑中成功提取到通讯录记录共计1条，其中已删除记录0条；通话记录共计1条，其中已删除记录0条；未提取到短信记录；部分多媒体内容如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-002\”目录下。

* + - 1. 多媒体

使用盘古石手机取证分析系统对检材平板进行提备份提取，分析其中的多媒体记录。检材平板中成功提取到多媒体记录共计170条，其中已删除记录0条。部分多媒体记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-002\”目录下。

* + - 1. 隔空投送

检材平板电脑中未提取到隔空投送记录。

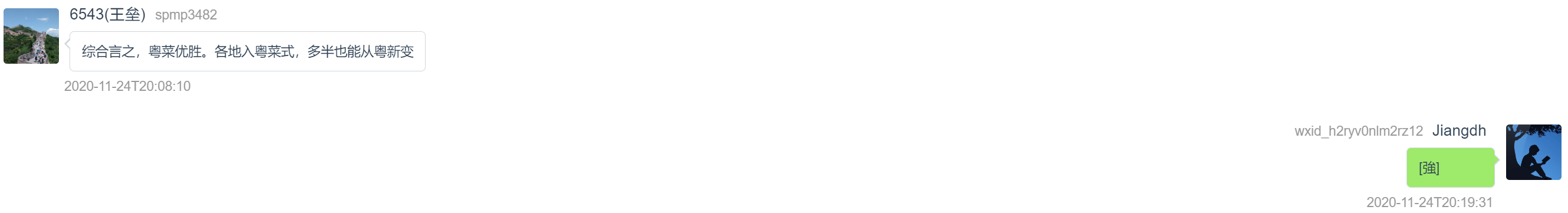
* + - 1. 微信

使用盘古石手机取证分析系统对检材平板电脑进行备份提取，分析其中的微信记录。检材平板电脑中成功提取到3个微信帐号“xiaohouzizhenkeai（微信ID：wxid\_tjz8zrqauekd22；昵称：Cuiyang）”、“sanhuanban（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“laikankano（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

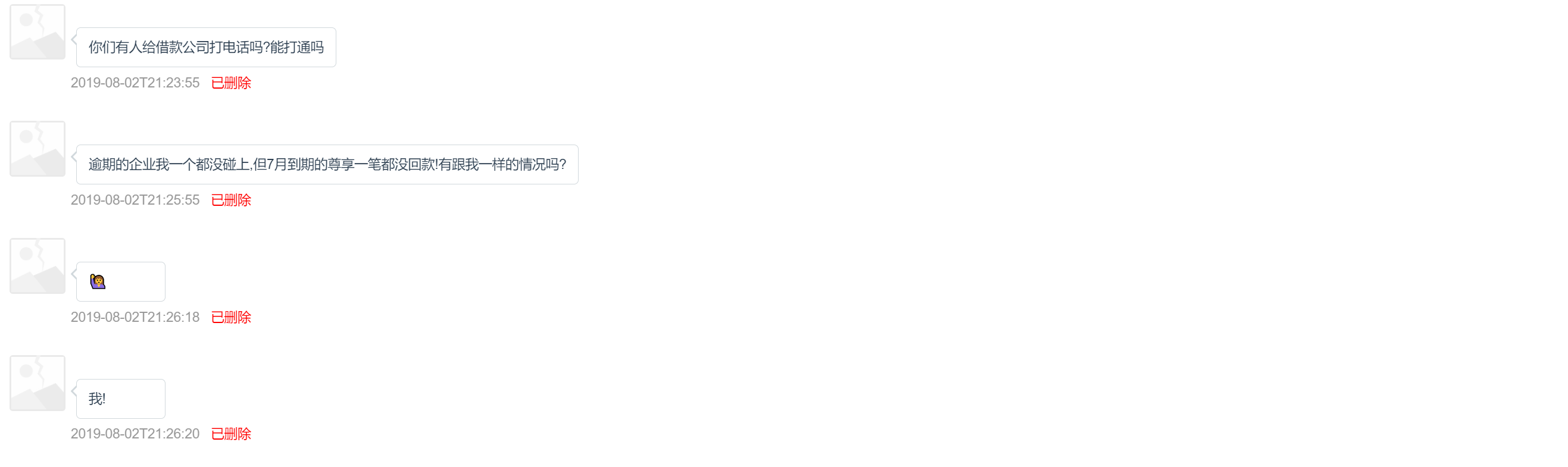
检材平板电脑中成功提取到微信帐号“xiaohouzizhenkeai（微信ID：wxid\_tjz8zrqauekd22；昵称：Cuiyang）”的记录共计14,068条，其中已删除记录61条。部分微信记录如下图所示：



检材平板电脑中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计1,030条，其中已删除记录14条。部分微信记录如下图所示：



检材平板电脑中成功提取到微信帐号“laikankano（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计3,383条，其中已删除记录1,276条。部分微信记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-002\”目录下。

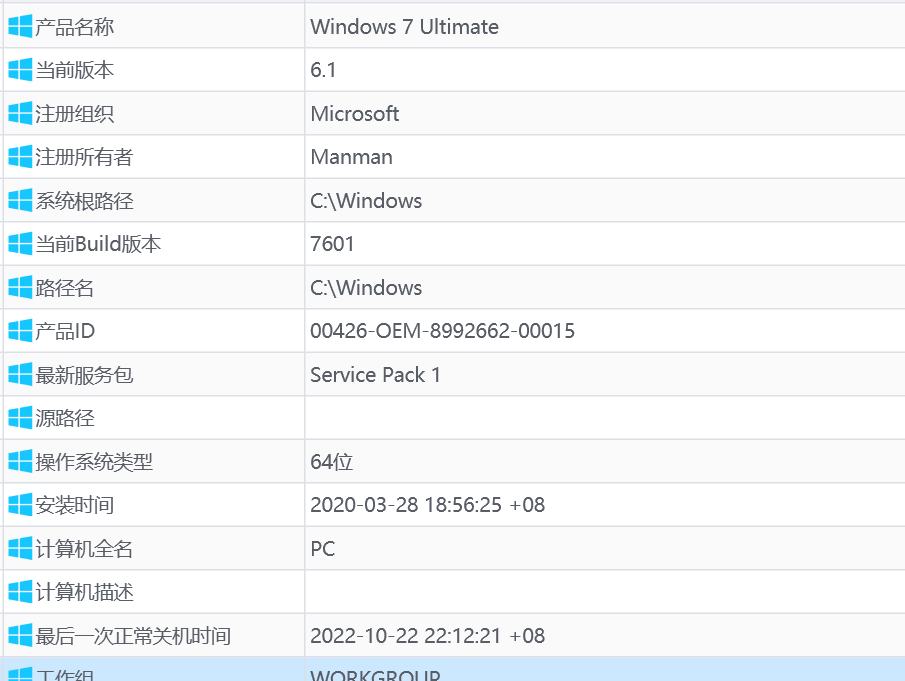
* + 1. 检材2022-251-003

在只读模式下使用FTK Imager软件制作检材“2022-251-003”内置硬盘的DD镜像。镜像文件的文件名、大小和源盘SHA256值如下表所示：

|  |  |  |
| --- | --- | --- |
| **文件名** | **文件大小** | **源盘SHA256** |
| 2022-251-003-001.001 | 256,060,514,304 字节 | 3831332feb6d90e1ca21253944ac2fbf5190e4d550c229b754c58ff8778c3662 |

* + - 1. 基本信息

使用盘古石计算机取证分析系统加载检材硬盘镜像“2022-251-003-001.001”，分析其基本信息。检材硬盘“2022-251-003-001”的容量为256 GB，共计2个分区。检材硬盘“2022-251-003-001”中安装的操作系统为“Windows 7 Ultimate”。系统安装时间为“2020-03-28 18:56:25 +08”。部分系统信息如下图所示：



检材硬盘“2022-251-003-001”中安装的系统时区信息为“(UTC+08:00) 北京，重庆，香港特别行政区，乌鲁木齐”。系统时区信息如下图所示：



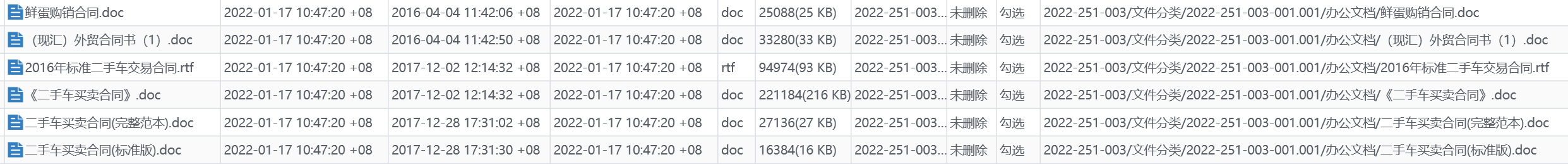
检材硬盘“2022-251-003-001”中安装的系统中共有3个本地用户，其中登录次数最多的用户为“Manman”，登录次数为“615”，最后一次登录时间为“2022-10-25 22:04:04 +08”。系统用户信息如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. 文件分类记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其文件分类记录。检材硬盘“2022-251-003-001”中成功提取到文件分类记录共计37,254条。其中办公文档13,504条；图片18,762条；压缩文件629条；视频文件3,157条；音频文件1,202条。部分办文档记录如下图所示：



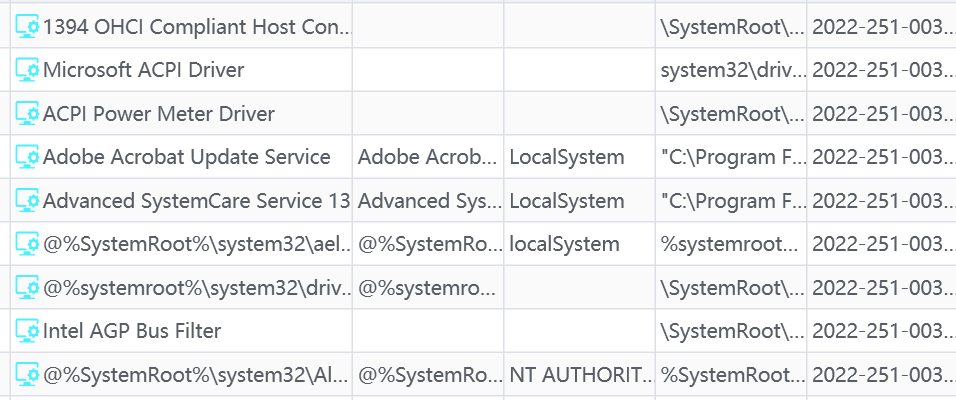
将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. 基本信息

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其基本信息。检材硬盘“2022-251-003-001”中成功提取到基本信息3,587条。其中系统痕迹记录3,136条；用户痕迹记录451条。

部分系统痕迹记录如下图所示：

=================此页以下为空白===============



部分用户痕迹信息如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. 浏览器记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其浏览器记录。检材硬盘“2022-251-003-001”中成功提取到浏览器记录11,546条。其中QQ浏览器记录14条；360记录12条；Opera记录19条；Edge记录72条；Google Chrome记录11,286条；Internet Explorer记录143条。

部分QQ浏览器记录如下图所示：



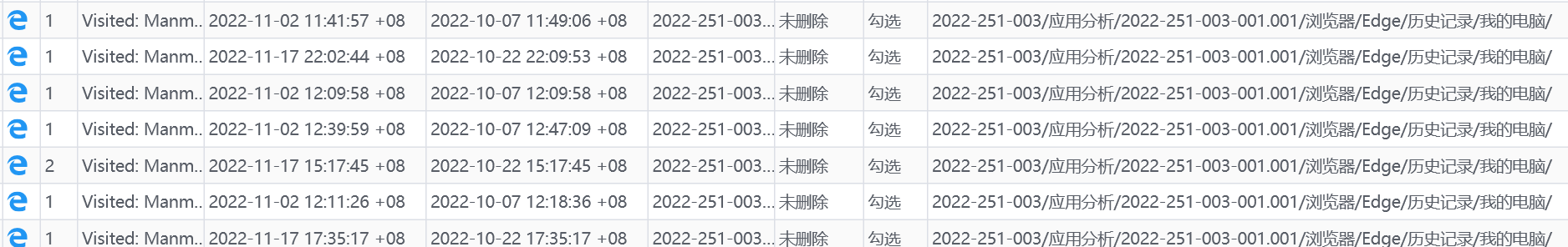
部分360记录如下图所示：



部分Opera记录如下图所示：



部分Edge记录如下图所示：



部分Google Chrome记录如下图所示：

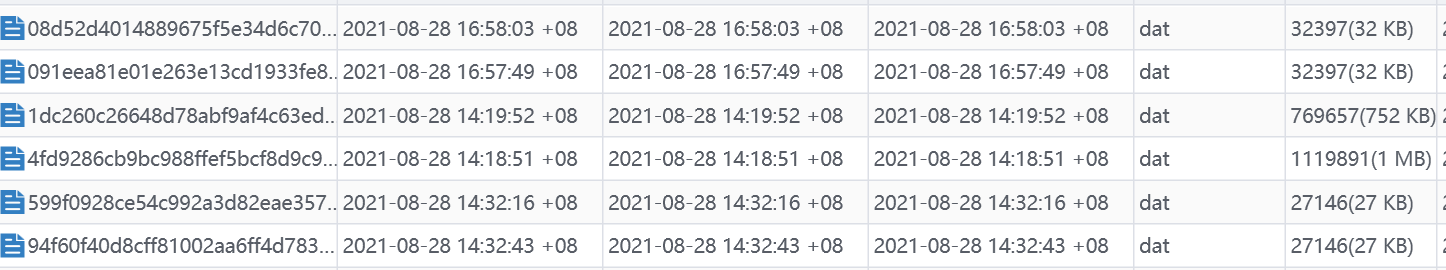


将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

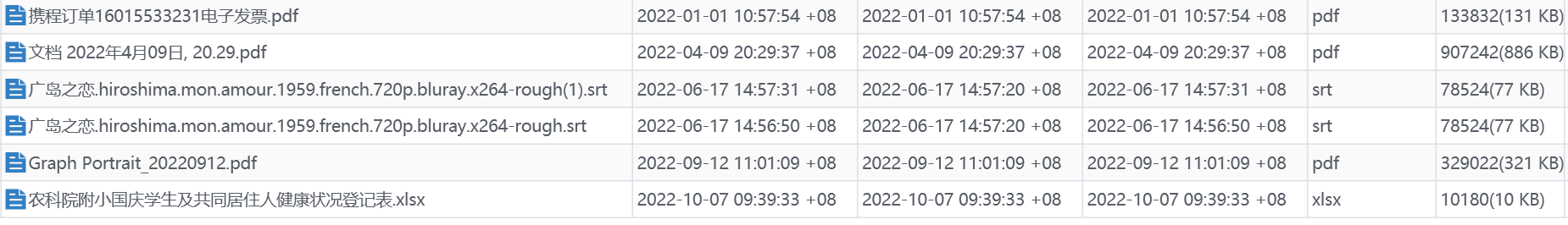
* + - 1. 社交软件记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其社交软件记录。检材硬盘“2022-251-003-001”中成功提取到社交软件记录2,305条，其中微信记录2,305条。检材硬盘“2022-251-003-001”中成功提取到2个微信帐号“（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

检材硬盘“2022-251-003-001”中成功提取到微信帐号“（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计2,198条，其中已删除记录0条。部分微信记录如下图所示：



检材硬盘“2022-251-003-001”中成功提取到微信帐号“（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计107条，其中已删除记录0条。部分微信记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. 网盘记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其网盘记录。检材硬盘“2022-251-003-001”中成功提取到网盘记录260条，其中百度网盘记录260条。部分百度网盘记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. VPN记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其VPN记录。检材硬盘“2022-251-003-001”中成功提取到VPN记录62条；其中操作系统VPN信息记录62条。部分操作系统VPN信息记录如下图所示：



* + - 1. 文件记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其文件记录。检材硬盘“2022-251-003-001”中成功提取到文件记录31条。其中iPhone信任文件记录6条；手机备份文件记录6条；加密容器文件记录19条。

部分iPhone信任文件记录如下图所示：



部分手机备份文件记录如下图所示：



部分加密容器文件记录如下图所示：



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + - 1. 缩略图分析记录

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其缩略图分析记录。检材硬盘“2022-251-003-001”中成功提取到缩略图分析记录642条。其中已删除0条。

部分缩略图分析记录如下图所示：

=================此页以下为空白===============



将上述所有记录保存至证据U盘中“\2022-251-003\”目录下。

* + 1. 数据保存及数字签名

将上述所有记录写入具有写保护措施的证据U盘中，U盘唯一性编号为2022第252号EUD01。

U盘中所有文件的SHA256值保存于证据U盘2032第251号EUD01根目录下的“SHA256.txt”文件中，该文件的SHA256值为：A5471001D817DEEF1904DD71C0AB355FC1EC5662022BFB5051ABBFD3A2E8E534。

1. 分析说明

1.在屏蔽环境下打开检材手机“2022-251-001”并开启飞行模式。使用盘古石手机取证分析系统对检材手机进行提权提取并分析其中的基本信息、微信记录、QQ记录、企业微信记录、钉钉记录、Telegram记录和Twitter记录。

查看检材手机的设备信息，检材手机的设备品牌为“iPhone”，型号为“MLUA3LL/A”，IMEI为“359052379903584”和“359052379207846”，系统版本为“iOS 15.4”，设备名称为“iPhoneF”。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的基本信息。检材手机中成功提取到通讯录记录共计419条，其中已删除记录0条；通话记录共计205条，其中已删除记录0条；短信记录共计1,514条，其中已删除记录0条。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的多媒体记录。

多媒体记录共计117条，其中已删除记录0条。

在屏蔽环境下打开检材手机“2022-251-001”并开启飞行模式。依次点击“设置-隐私-分析与改进-分析数据”，搜索并导出日志文件“sysdiagnose\_2022.10.22\_23-56-24+0800\_iPhone-OS\_iPhone\_19E241.tar.gz”。利用盘古石手机取证分析系统对该日志文件的隔空投送记录进行分析。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的微信记录。检材手机中成功提取到2个微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“democrachina（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

检材手机中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计8,308条，其中已删除记录33条。

检材手机中成功提取到微信帐号“democrachina（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计12,175条，其中已删除记录68条。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的QQ记录。检材手机中成功提取到2个QQ帐号“16467920（用户名：16467920；昵称：ban）”和“173740457（用户名：173740457；昵称：未名）”的使用记录。

检材手机中成功提取到QQ帐号“16467920（用户名：16467920；昵称：ban）”的使用记录共计6,764条，其中已删除3条。

检材手机中成功提取到QQ帐号“173740457（用户名：173740457；昵称：未名）”的使用记录共计279条，其中已删除0条。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的企业微信记录。检材手机中成功提取到6个企业微信帐号“（帐号：1688854878268925；昵称：蒋敦宏）”、“（帐号：1688858261295257；昵称：蒋敦宏）”、“（帐号：1688850555422033；昵称：蒋敦宏）”、“（帐号：1688856663353031；昵称：蒋敦宏）”、“（帐号：1688850263755318；昵称：蒋敦宏）”和“（帐号：1688851310316007；昵称：蒋敦宏-北京市远东律师事务所）”的使用记录。

检材手机中成功提取到企业微信帐号“（帐号：1688854878268925；昵称：蒋敦宏）”的记录共计203条，其中已删除记录9条。

检材手机中成功提取到企业微信帐号“（帐号：1688858261295257；昵称：蒋敦宏）”的记录共计268条，其中已删除记录5条。

检材手机中成功提取到企业微信帐号“（帐号：1688850555422033；昵称：蒋敦宏）”的记录共计122条，其中已删除记录4条。

检材手机中成功提取到企业微信帐号“（帐号：1688856663353031；昵称：蒋敦宏）”的记录共计198条，其中已删除记录2条。

检材手机中成功提取到企业微信帐号“（帐号：1688850263755318；昵称：蒋敦宏）”的记录共计271条，其中已删除记录0条。

检材手机中成功提取到企业微信帐号“（帐号：1688851310316007；昵称：蒋敦宏-北京市远东律师事务所）”的记录共计28,806条，其中已删除记录101条。

检材手机中成功提取到钉钉帐号“（帐号：124537349；昵称：ban）”的使用记录共计1,199条，其中已删除记录32条。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的Telegram记录。检材手机中成功提取到1个Telegram帐号“dasung996（帐号ID：35244388451；昵称：John Smith）”的使用记录。

检材手机中成功提取到Telegram帐号“dasung996（帐号ID：35244388451；昵称：John Smith）”的记录共计11,783条，其中已删除记录0条。

使用盘古石手机取证分析系统对检材手机进行提权提取，分析其中的Twitter记录。检材手机中成功提取到2个Twitter帐号“（帐号：113052019；昵称：sandanderen）”和“（帐号：937104152294866944；昵称：yiqiwan2018）”的使用记录。

检材手机中成功提取到Twitter帐号“（帐号：113052019；昵称：sandanderen）”的记录共计7,350条，其中已删除记录0条。

检材手机中成功提取到Twitter帐号“（帐号：937104152294866944；昵称：yiqiwan2018）”的记录共计1,644条，其中已删除记录0条。

检材手机中成功解析出隔空投送传出文件记录共计137条，其中已删除记录共计0条。

其中“状态”为“Incomplete”记录共计36条。

其中“状态”为“Declined”记录共计81条。

其中“状态”为“Accepted”记录共计20条。

2.在屏蔽环境下打开检材平板电脑“2022-251-002”并开启飞行模式。使用盘古石手机取证分析系统对检材平板电脑进行备份提取并分析其中的基本信息、微信记录和隔空投送记录。

查看检材平板电脑的设备信息，检材平板电脑的设备品牌为“iPad”，型号为“iPad Pro”，SN为“DMPDTAQUPV03”，系统版本为“iOS 14.3”，设备名称为“Jianghz”。

使用盘古石手机取证分析系统对检材平板电脑进行备份提取，分析其中的基本信息。检材平板电脑中成功提取到通讯录记录共计1条，其中已删除记录0条；通话记录共计1条，其中已删除记录0条；未提取到短信记录；

使用盘古石手机取证分析系统对检材平板电脑进行备份提取，分析其中的多媒体记录。检材平板中成功提取到多媒体记录共计170条，其中已删除记录0条。

检材平板电脑中未提取到隔空投送记录。

使用盘古石手机取证分析系统对检材平板电脑进行备份提取，分析其中的微信记录。检材平板电脑中成功提取到3个微信帐号“xiaohouzizhenkeai（微信ID：wxid\_tjz8zrqauekd22；昵称：Cuiyang）”、“sanhuanban（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“laikankano（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

检材平板电脑中成功提取到微信帐号“xiaohouzizhenkeai（微信ID：wxid\_tjz8zrqauekd22；昵称：Cuiyang）”的记录共计14,068条，其中已删除记录61条。

检材平板电脑中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计1,030条，其中已删除记录14条。

检材平板电脑中成功提取到微信帐号“laikankano（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计3,383条，其中已删除记录1,276条。

3.在只读模式下使用FTK Imager软件制作检“2022-251-003”内置硬盘的DD镜像。

使用盘古石计算机取证分析系统加载检材硬盘镜像“2022-251-003-001”，分析其基本信息。检材硬盘“2022-251-003-001”的容量为256 GB，共计2个分区。检材硬盘“2022-251-003-001”中安装的操作系统为“Windows 7 Ultimate”。系统安装时间为“2020-03-28 18:56:25 +08”。

检材硬盘“2022-251-003-001”中安装的系统时区信息为“(UTC+08:00) 北京，重庆，香港特别行政区，乌鲁木齐”。

检材硬盘“2022-251-003-001”中安装的系统中共有3个本地用户，其中登录次数最多的用户为“Manman”，登录次数为“615”，最后一次登录时间为“2022-10-25 22:04:04 +08”。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其文件分类记录。检材硬盘“2022-251-003-001”中成功提取到文件分类记录共计37,254条。其中办公文档13,504条；图片18,762条；压缩文件629条；视频文件3,157条；音频文件1,202条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其基本信息。检材硬盘“2022-251-003-001”中成功提取到基本信息3,587条。其中系统痕迹记录3,136条；用户痕迹记录451条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其浏览器记录。检材硬盘“2022-251-003-001”中成功提取到浏览器记录11,546条。其中QQ浏览器记录14条；360记录12条；Opera记录19条；Edge记录72条；Google Chrome记录11,286条；Internet Explorer记录143条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其社交软件记录。检材硬盘“2022-251-003-001”中成功提取到社交软件记录2,305条，其中微信记录2,305条。检材硬盘“2022-251-003-001”中成功提取到2个微信帐号“（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”和“ （微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的使用记录。

检材硬盘“2022-251-003-001”中成功提取到微信帐号“（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计2,198条，其中已删除记录0条。

检材硬盘“2022-251-003-001”中成功提取到微信帐号“（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计107条，其中已删除记录0条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其网盘记录。检材硬盘“2022-251-003-001”中成功提取到网盘记录260条，其中百度网盘记录260条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其VPN记录。硬盘“2022-251-003-001”中成功提取到VPN记录62条；其中操作系统VPN信息记录62条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其文件记录。硬盘“2022-251-003-001”中成功提取到文件记录31条。其中iPhone信任文件记录6条；手机备份文件记录6条；加密容器文件记录19条。

使用盘古石计算机取证分析系统加载检材硬盘“2022-251-003-001”，分析其缩略图分析记录。检材硬盘“2022-251-003-001”中成功提取到缩略图分析记录642条。其中已删除0条。

1. 鉴定意见

1.经检验，检材手机“2022-251-001”的设备品牌为“iPhone”，型号为“MLUA3LL/A”，IMEI为“359052379903584”和“359052379207846”，系统版本为“iOS 15.4”，设备名称为“iPhoneF”。

检材手机中成功提取到通讯录记录共计419条，其中已删除记录0条；通话记录共计205条，其中已删除记录0条；短信记录共计1,514条，其中已删除记录0条。

检材手机中成功提取到多媒体记录共计117条，其中已删除记录0条。

检材手机中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计8,308条，其中已删除记录33条。

检材手机中成功提取到微信帐号“democrachina（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计12,175条，其中已删除记录68条。

检材手机中成功提取到QQ帐号“16467920（用户名：16467920；昵称：ban）”的使用记录共计6,764条，其中已删除3条。

检材手机中成功提取到QQ帐号173740457（用户名：173740457；昵称：未名）”的使用记录共计279条，其中已删除0条。

检材手机中成功提取到企业微信帐号“（帐号：1688854878268925；昵称：蒋敦宏）”的记录共计203条，其中已删除记录9条。

检材手机中成功提取到企业微信帐号“（帐号：1688858261295257；昵称：蒋敦宏）”的记录共计268条，其中已删除记录5条。

检材手机中成功提取到企业微信帐号“（帐号：1688850555422033；昵称：蒋敦宏）”的记录共计122条，其中已删除记录4条。

检材手机中成功提取到企业微信帐号“（帐号：1688856663353031；昵称：蒋敦宏）”的记录共计198条，其中已删除记录2条。

检材手机中成功提取到企业微信帐号“（帐号：1688850263755318；昵称：蒋敦宏）”的记录共计271条，其中已删除记录0条。

检材手机中成功提取到企业微信帐号（帐号：1688851310316007；昵称：蒋敦宏-北京市远东律师事务所）”的记录共计28,806条，其中已删除记录101条。

检材手机中成功提取到钉钉帐号“（帐号：124537349；昵称：ban）”的使用记录共计1,199条，其中已删除记录32条。

检材手机中成功提取到Telegram帐号“dasung996（帐号ID：35244388451；昵称：John Smith）”的记录共计11,783条，其中已删除记录0条。

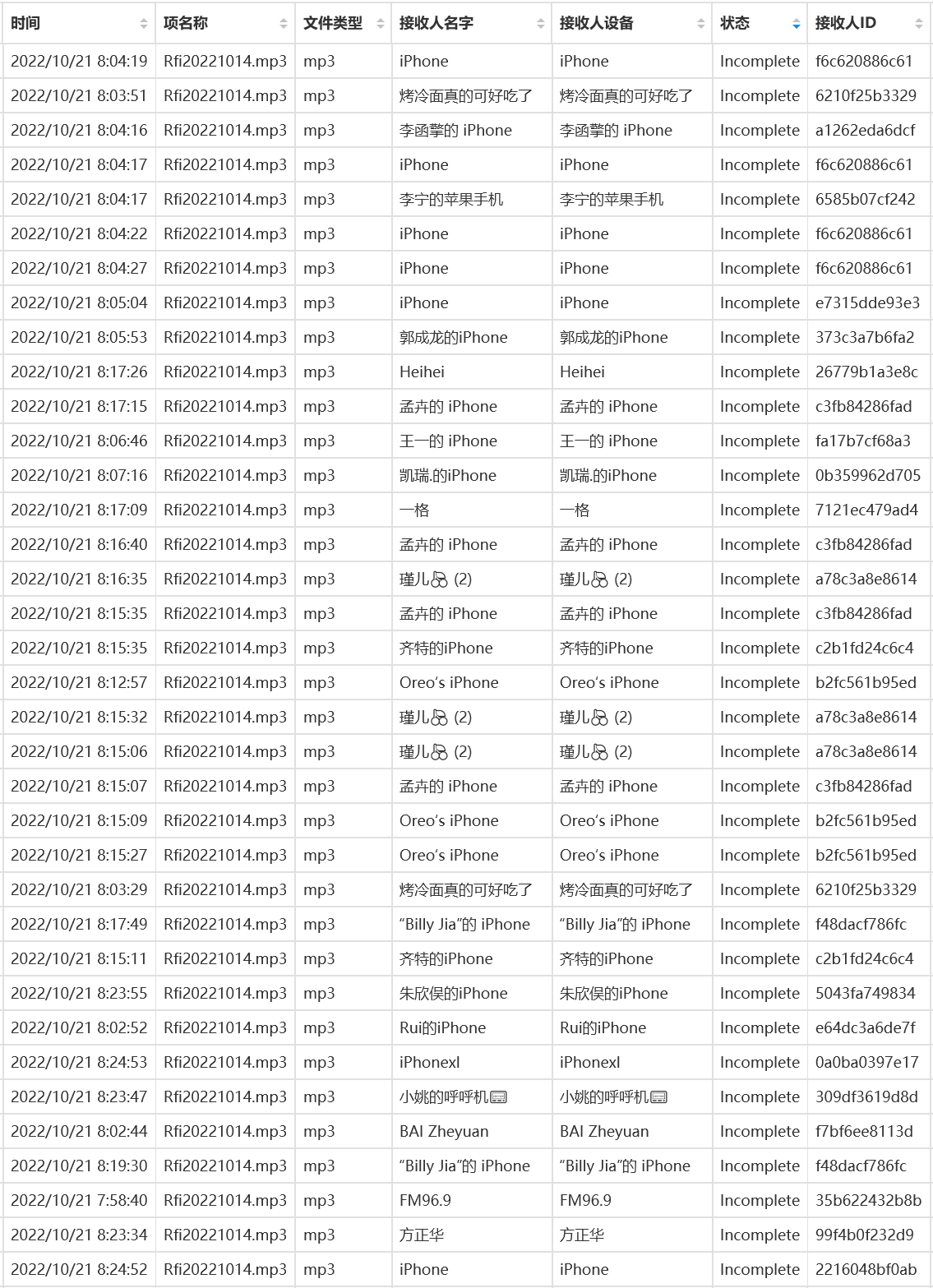
检材手机中成功提取到Twitter帐号“（帐号：113052019；昵称：sandanderen）”的记录共计7,350条，其中已删除记录0条。

检材手机中成功提取到Twitter帐号“（帐号：937104152294866944；昵称：yiqiwan2018）”的记录共计1,644条，其中已删除记录0条。

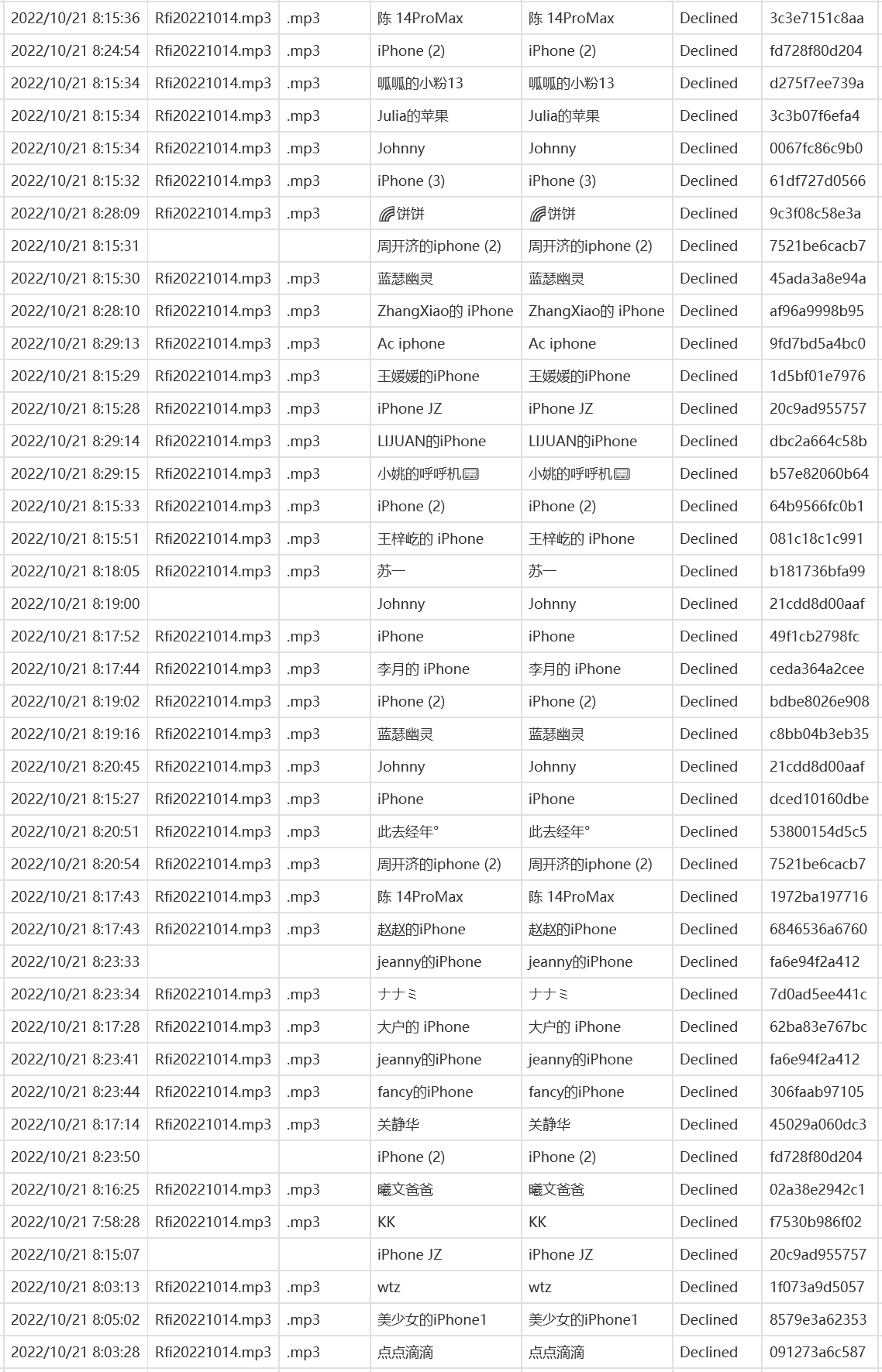
检材手机中成功解析出隔空投送传出文件记录共计137条，其中已删除记录共计0条。

其中“状态”为“Incomplete”记录共计36条。详细信息如下图所示：

=================此页以下为空白===============



其中“状态”为“Declined”记录共计81条。详细信息如下图所示：





其中“状态”为“Accepted”记录共计20条。详细信息如下图所示：



2.经检验，检材平板电脑“2022-251-002”的设备品牌为“iPad”，型号为“iPad Pro”，SN为“DMPDTAQUPV03”，系统版本为“iOS 14.3”，设备名称为“Jianghz”。

检材平板电脑中成功提取到通讯录记录共计1条，其中已删除记录0条；通话记录共计1条，其中已删除记录0条；未提取到短信记录；多媒体记录共计170条，其中已删除记录0条。

检材平板电脑中未提取到隔空投送记录。

检材平板电脑中成功提取到微信帐号“xiaohouzizhenkeai（微信ID：wxid\_tjz8zrqauekd22；昵称：Cuiyang）”的记录共计14,068条，其中已删除记录61条。

检材平板电脑中成功提取到微信帐号“kuadenuo（微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计1,030条，其中已删除记录14条。

检材平板电脑中成功提取到微信帐号“laikankano（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计3,383条，其中已删除记录1,276条。

3.经检验，检材硬盘“2022-251-003-001”的容量为256 GB，共计2个分区。检材硬盘“2022-251-003-001”中安装的操作系统为“Windows 7 Ultimate”。系统安装时间为“2020-03-28 18:56:25 +08”。

检材硬盘“2022-251-003-001”中安装的系统时区信息为“(UTC+08:00) 北京，重庆，香港特别行政区，乌鲁木齐”。

检材硬盘“2022-251-003-001”中安装的系统中共有3个本地用户，其中登录次数最多的用户为“Manman”，登录次数为“615”，最后一次登录时间为“2022-10-25 22:04:04 +08”。

检材硬盘“2022-251-003-001”中成功提取到文件分类记录共计37,254条。其中办公文档13,504条；图片18,762条；压缩文件629条；视频文件3,157条；音频文件1,202条。

检材硬盘“2022-251-003-001”中成功提取到基本信息3,587条。其中系统痕迹记录3,136条；用户痕迹记录451条。

检材硬盘“2022-251-003-001”中成功提取到浏览器记录11,546条。其中QQ浏览器记录14条；360记录12条；Opera记录19条；Edge记录72条；Google Chrome记录11,286条；Internet Explorer记录143条。

检材硬盘“2022-251-003-001”中成功提取到微信帐号“ （微信ID：wxid\_h2ryv0nlm2rz12；昵称：Jiangdh）”的记录共计2,198条，其中已删除记录0条。

检材硬盘镜像中“2022-251-003-001”成功提取到微信帐号“（微信ID：wxid\_kc7lbn7d56eu12；昵称：不畏浮云）”的记录共计107条，其中已删除记录0条。

检材硬盘“2022-251-003-001”中成功提取到百度网盘记录260条。

检材硬盘“2022-251-003-001”中成功提取到操作系统VPN信息记录62条。

检材硬盘“2022-251-003-001”中成功提取到文件记录31条。其中iPhone信任文件记录6条；手机备份文件记录6条；加密容器文件记录19条。

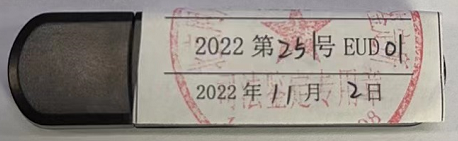
检材硬盘“2022-251-003-001”中成功提取到缩略图分析记录642条。其中已删除0条。

=================此页以下为空白===============

1. 附件
   1. 检材照片

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 检材编号 | 检材信息 | | | | | |
| 2022-251-001 | 名称 | 手机 | | 数量 | | 1 |
| 品牌 | iPhone | | 型号 | | MLUA3LL/A |
| IMEI | 359052379903584,359052379207846 | | | | |
| 保存状况 | 外表完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 检材照片 |  | | | | |
| 备注 | “嫌 蒋敦宏”、“0564” | | | | |
| 2022-251-002 | 名称 | 平板电脑 | 数量 | | 1 | |
| 品牌 | iPad | 型号 | | iPad Pro | |
| SN | DMPDTAQUPV03 | | | | |
| 保存状况 | 外表完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 检材照片 |  | | | | |
| 备注 | “嫌 蒋敦宏”、“0095” | | | | |
| 2022-251-003 | 名称 | 笔记本电脑 | 数量 | | 1 | |
| 品牌 | SONY | 型号 | | SVP132A18T | |
| SN | 545897270003564 | | | | |
| 保存状况 | 外观完好 | | | | |
| 收到时间 | 2022年10月24日 | | | | |
| 检材照片 |  | | | | |
| 备注 | “嫌 蒋敦宏” | | | | |
| 2022-251-003-001 | 名称 | 硬盘 | 数量 | | 1 | |
| 品牌 | SAMSUNG | 型号 | | MZ-NTD256/000 | |
| SN | S15ZNYAD727991 | | | | |
| SHA256 | 3831332feb6d90e1ca21253944ac2fbf5190e4d550c229b754c58ff8778c3662 | | | | |
| 检材照片 |  | | | | |
| 备注 | “2022-251-003内置硬盘” | | | | |

* 1. 检出数据的光盘



|  |  |
| --- | --- |
| 司法鉴定人： | 谢春磊 |
| 《司法鉴定人执业证》证号： | 110021187002 |
| 司法鉴定人： | 徐志强 |
| 《司法鉴定人执业证》证号： | 110021187003 |

二〇二二年十一月七日