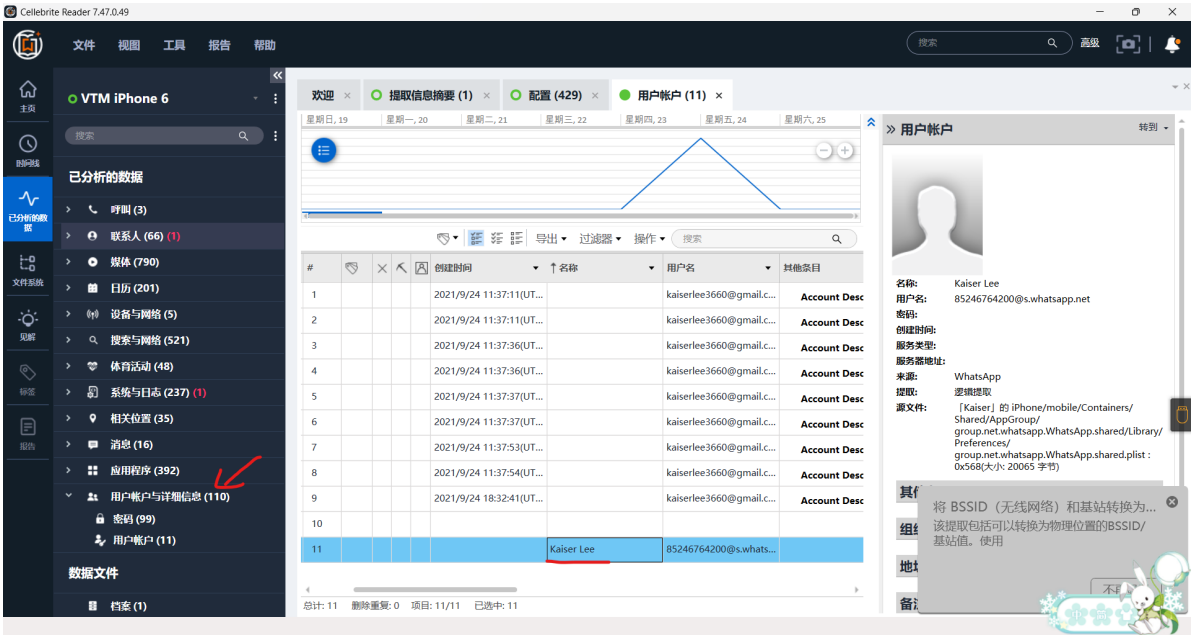
2021美亚杯资格赛wp

> 题目顺序与答案参考美亚杯官网，没有解答过程的就是我没做出来的。
>
> [2021美亚杯题目与答案]

1.工地主管电话的微信账号是什么?

答案：D

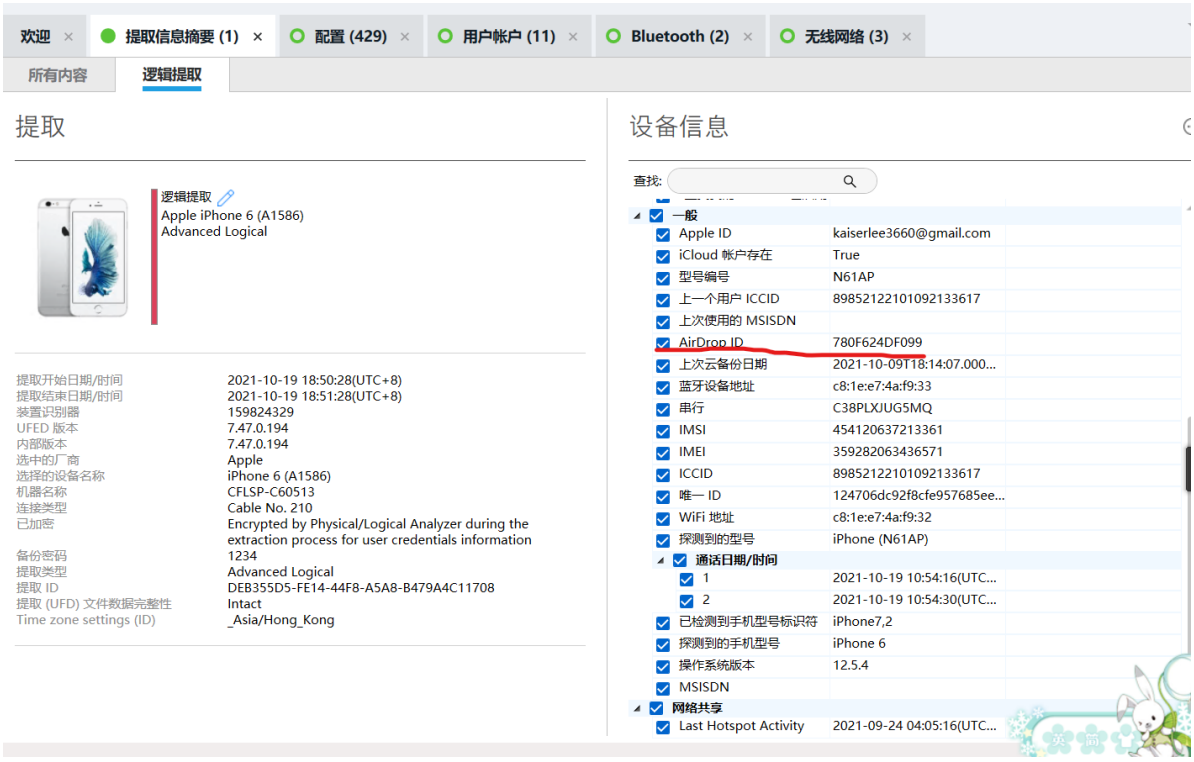
打开阅读器，在用户账户那栏看到WhatsApp的账户信息。而且这个手机里根本就没有微信，所以无论从哪个角度看这题的答案都是以上皆非。



2.工地主管的隔空投送装置编号是什么？（英文全大写加阿拉伯数字回答）

答案：780F624DF099

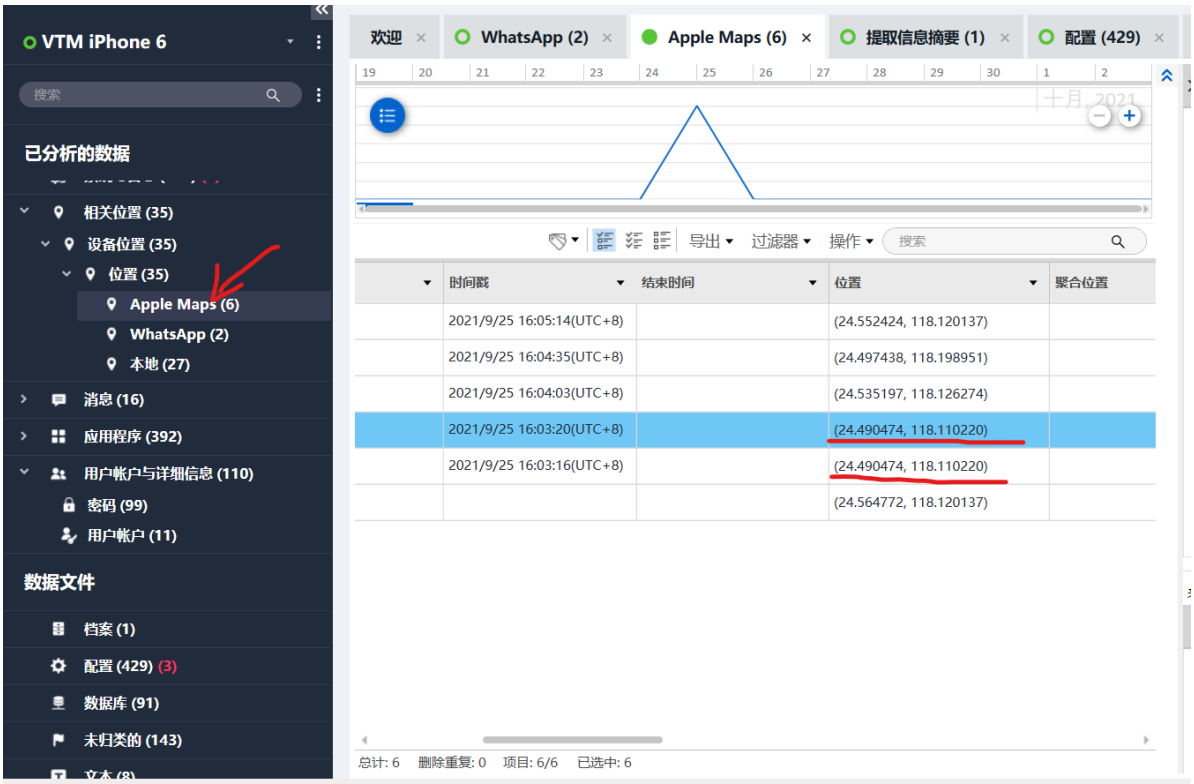
直接查看逻辑提取内容即可：



3.工地主管电话的哪一个应用程序有关于经纬度24.490474 118.110220的记录?

答案：Apple Maps

查看设备位置中的各个应用记录，在Apple Maps里发现了该记录：



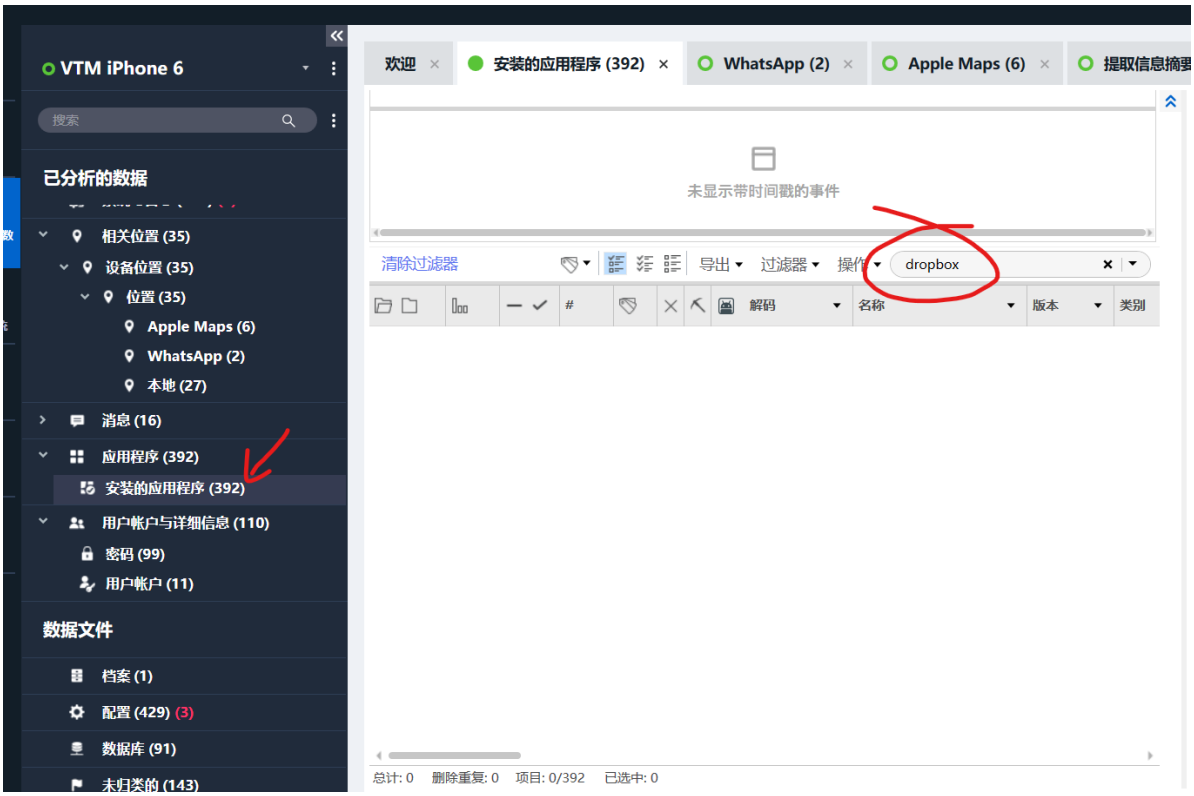
4.工地主管的手提电话中下列那些数据正确?

答案：AC

iOS版本、IMEI、Apple ID信息均可在逻辑提取内容中发现：



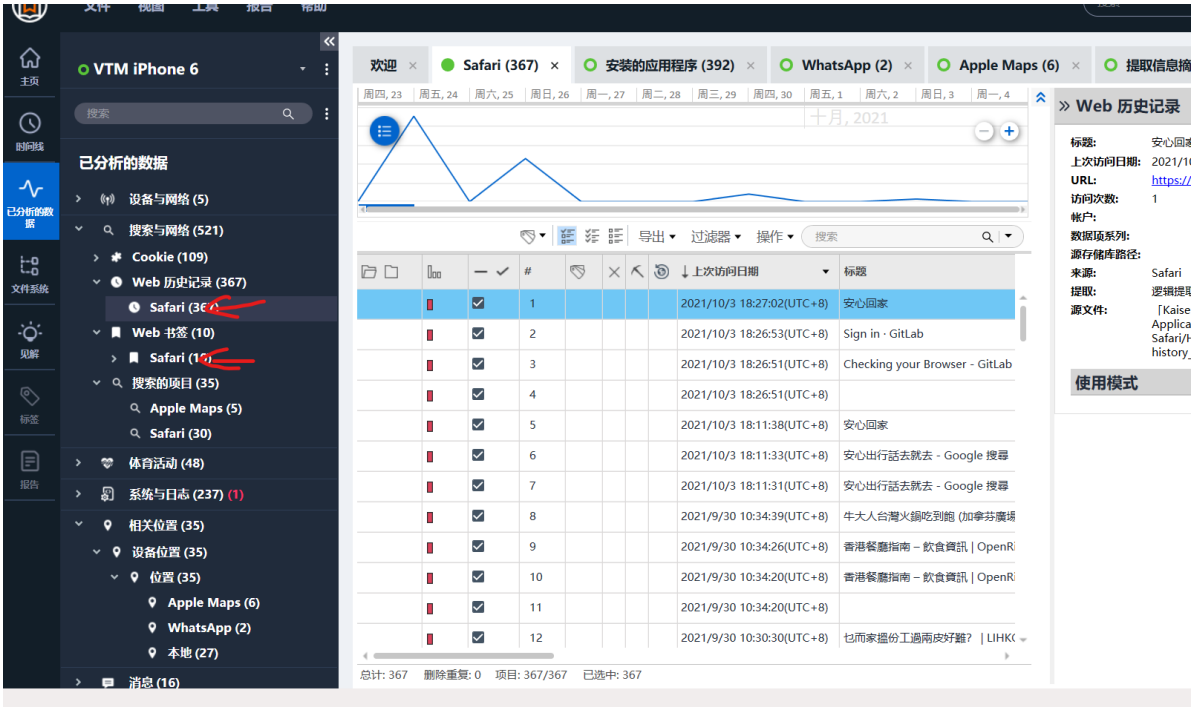
而在应用程序-安装的应用程序模块中搜索dropbox，没有找到相关记录，故认为没有下载：



5.工地主管的电话最常使用的浏览器是什么？（请以英文全大写回答）

答案：SAFARI

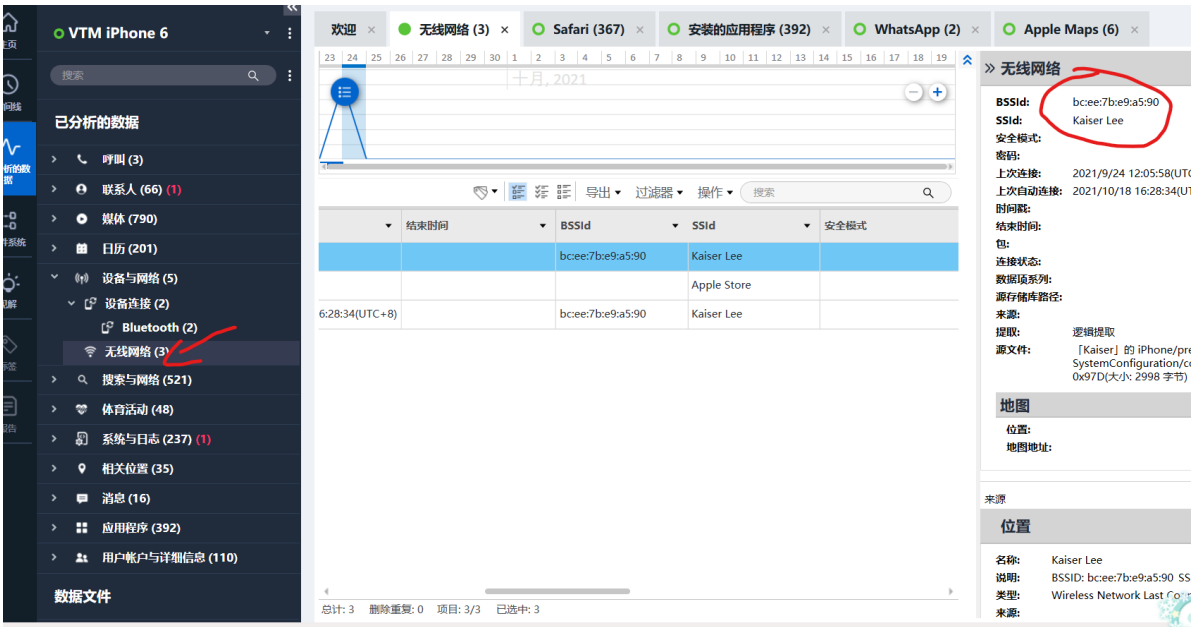
在搜索与网络-WEB历史记录中可以发现，只有Safri浏览器拥有使用记录，因此答案就是SAFARI：



6.工地主管的电话连接过哪一个WIFI?

答案：A

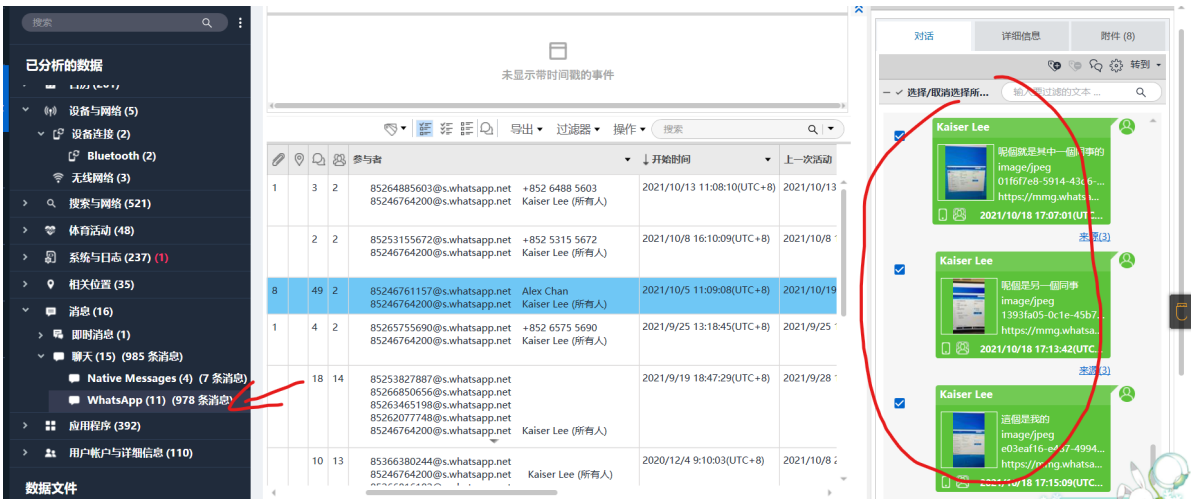
设备与网络-无线网络中可以发现连接过WIFI的名称：



7.工地主管与 Alex Chan 的 WhatsApp 对话中，曾提及以下哪个 TeamViewer 的用户号码?

答案：ACE

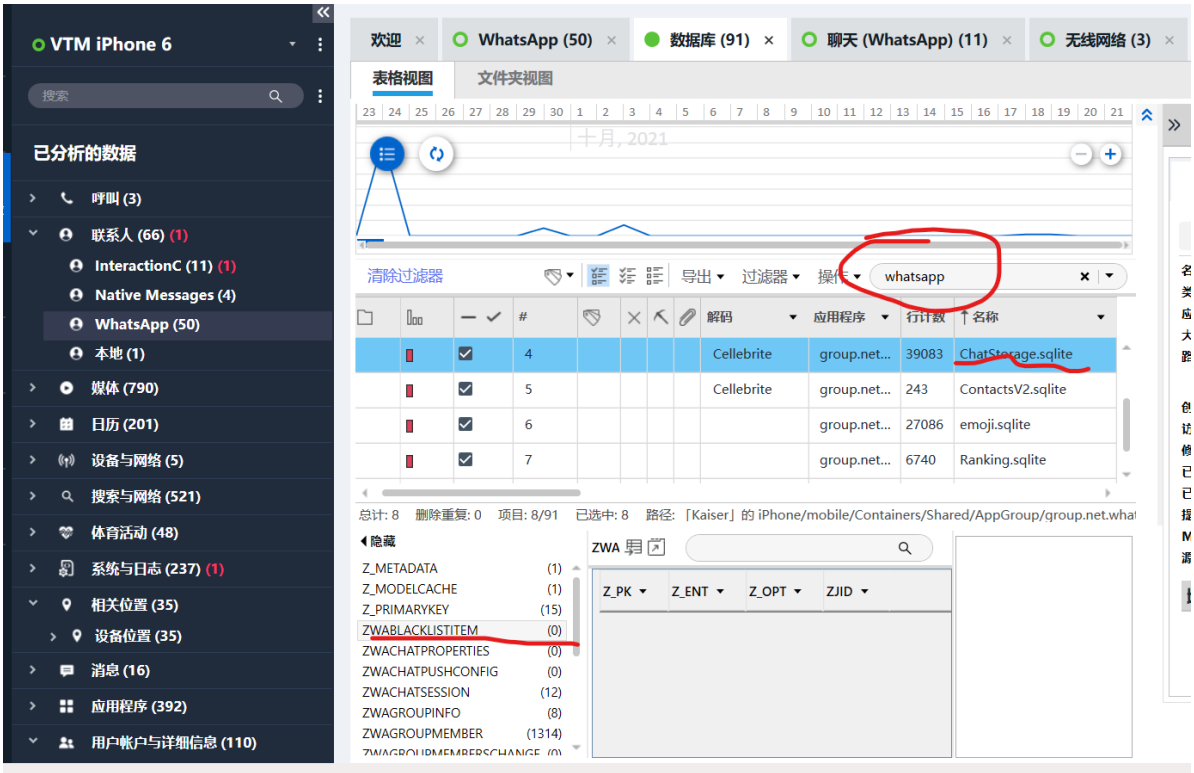
在消息-聊天-WhatsApp中找到工地主管与 Alex Chan 的对话，其中有3张图片涉及到了 TeamViewer 的ID，其中一个是主管自己的，两个是同事的：



8.工地主管的 WhatsApp 中有多少个黑名单的记录？（请以阿拉伯数字回答）

答案：0

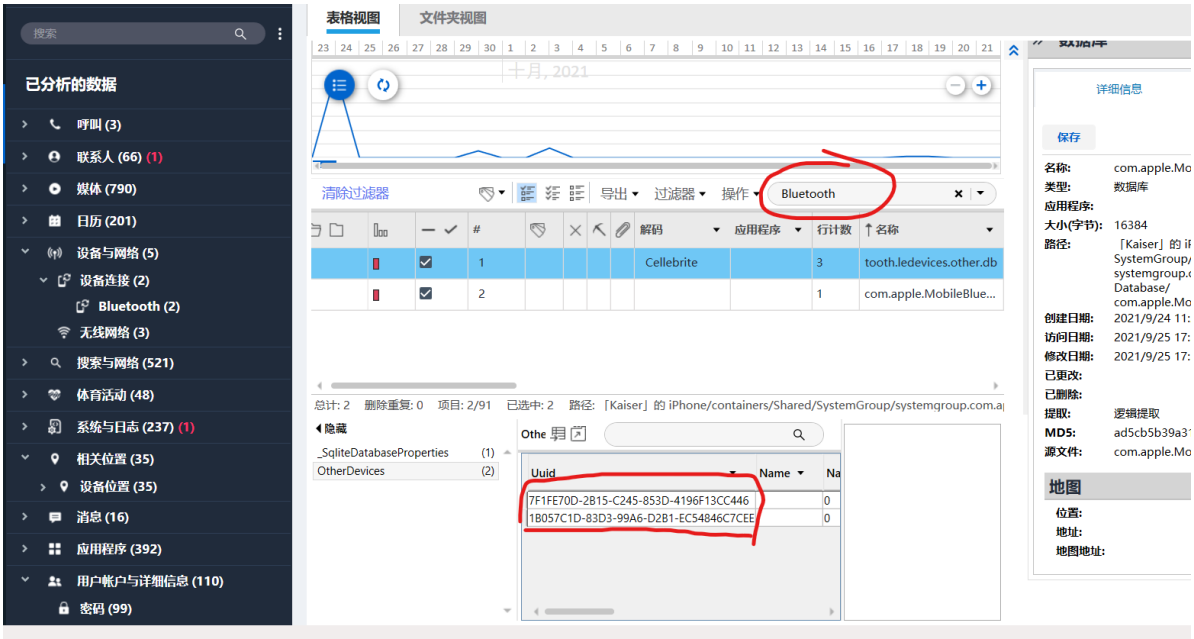
账户信息一般存储在数据库中，在数据库内容中搜索WhatsApp，然后发现在ChatStorage.sqlite中存在ZWABLACKLISTITEM，其条目为0：



9.以下哪个蓝牙装置的 UUID 曾连接过工地主管的手机?

答案：AB

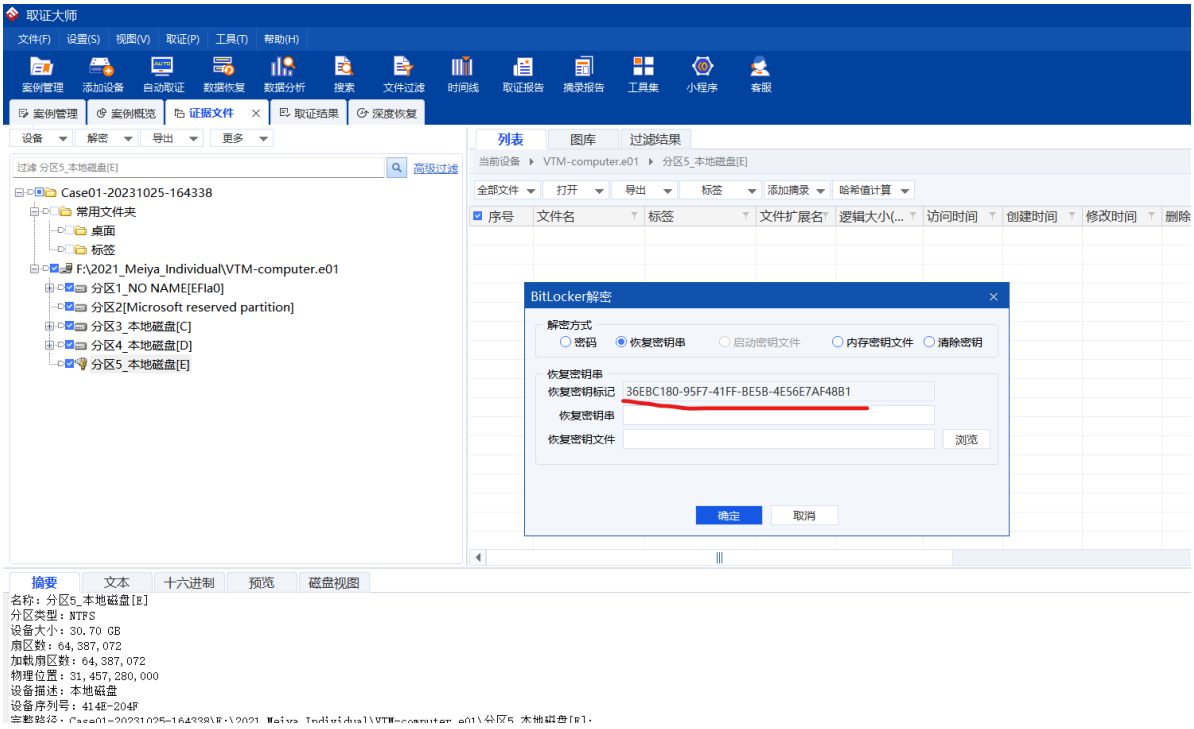
先去设备与网络-设备连接里看了下记录，没有记录蓝牙装置的 UUID，同样去数据库里看看，搜索Bluetooth，在com.apple.MobileBluetooth.ledevices.other.db里面就可以发现设备的 UUID 号了：



10.工地主管计算机的E盘的 Bitlocker 修复密钥标识符是什么（英文大写加阿拉伯数字，不用输入'-'）

答案：36EBC18095F741FFBE5B4E56E7AF48B1

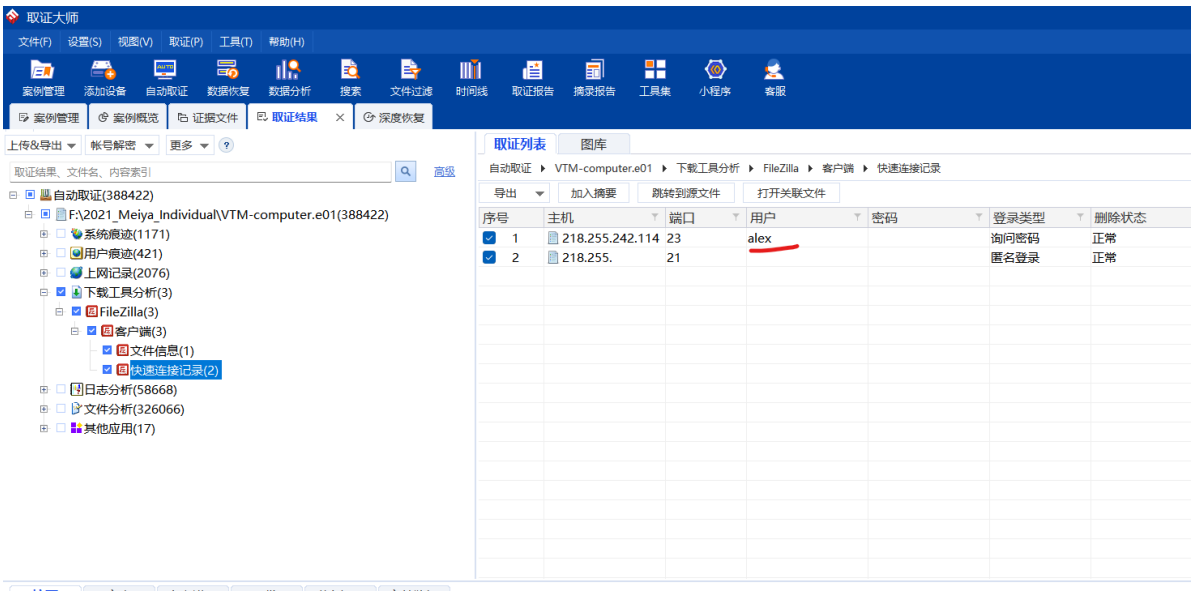
修复密钥标识符就是修复秘钥标记，右键选择分区5，选择Bitlock解密，解密方式选择修复密钥串即可看到：



11.工地主管计算机内的 FTP 程序 FileZilla 的用户名全称是什么？（英文大写加阿拉伯数字回答）

答案：ALEX

进行自动取证，在下载工具分析-FileZilla-客户端-快速连接记录中可以看到用户名：



12.工地主管的 TeamViewer ID 是什么？（请以英语全大写和阿拉伯数字回答）

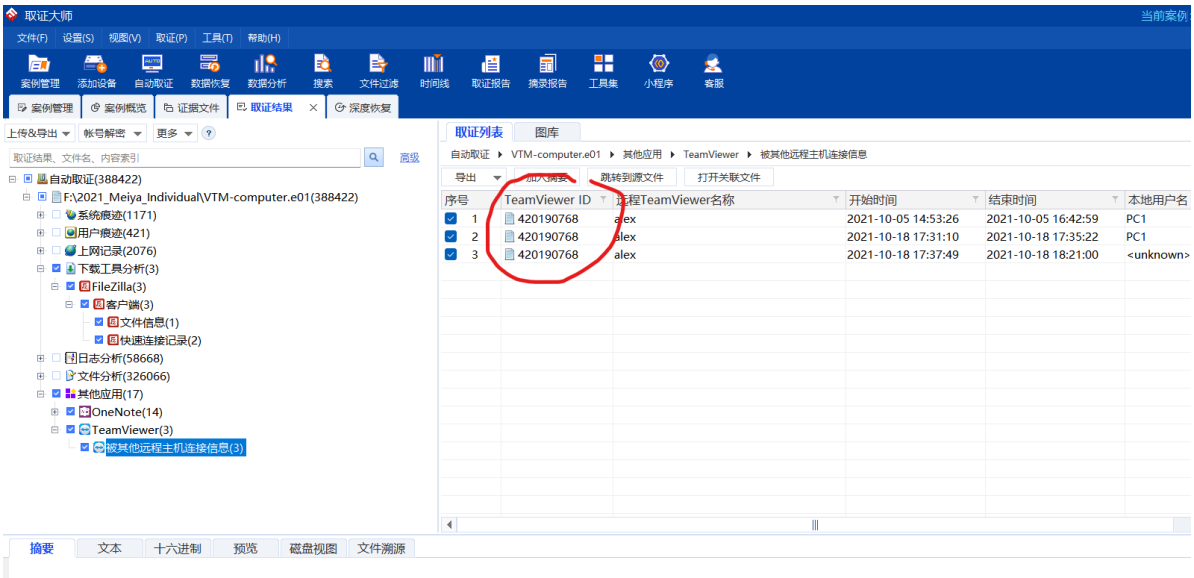
答案：435270306

在第7题的聊天对话中就可以看到了，这里就不截图了。

13.工地主管的 Team Viewer 与哪一个 ID 连接？（请以英语全大写和阿拉伯数字回答）

答案：420190768

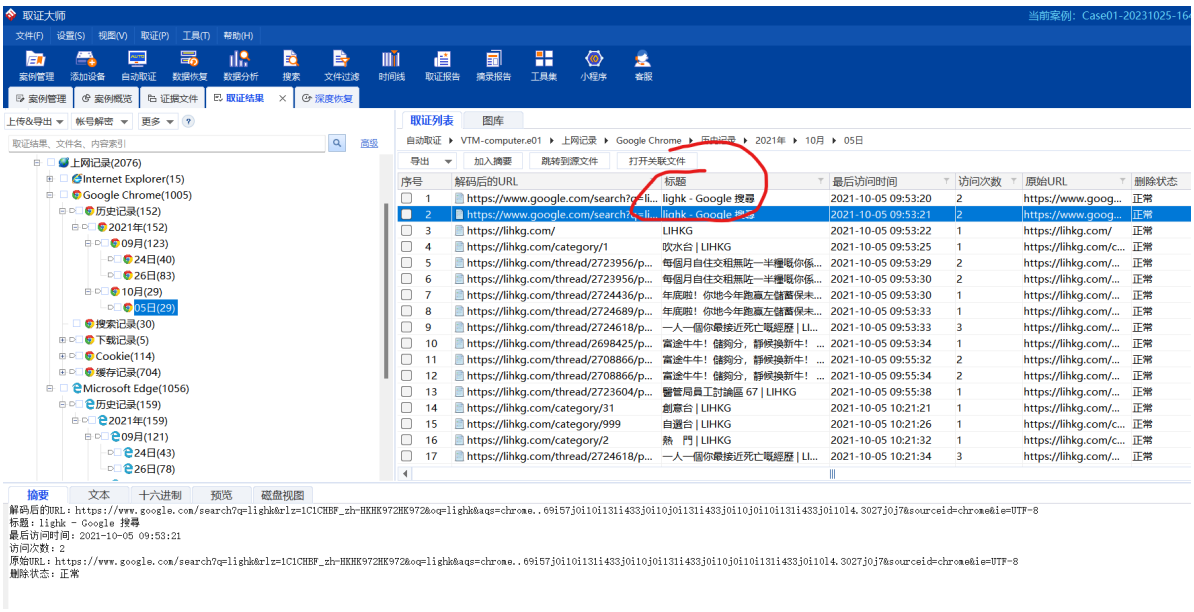
在取证大师自动取证结果里的其他应用-TeamViewer-被其他主机远程连接的信息，就可以发现题目需要的ID号了：



14.工地主管曾用计算机浏览器做搜寻，以下哪一个关键词他曾经搜寻?

答案：BC

这题很坑，首先你可以在自动取证中一个一个搜关键字，只有BCD有结果。但是要注意，D搜出来的结果是没有google搜寻的，因为它在搜寻lihkg的时候把单词错误拼写成了lighk：

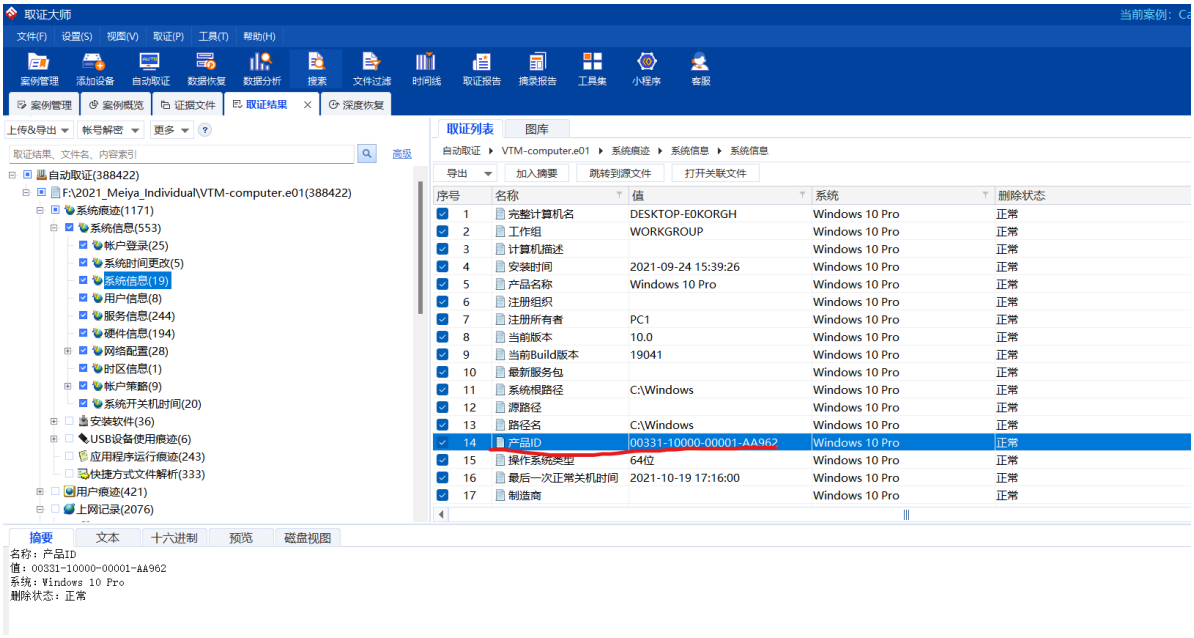


所以D不能选，这题选BC。

15.工地主管计算机的 Windows 系统的产品标识符是什么？（请以英文全大写及阿拉伯数字回答，不用输入'-'）

答案：00331100000000001AA962

在取证大师自动取证结果里的系统痕迹-系统信息中，就可以发现题目需要的ID号了：



16.工地主管曾用计算机使用 WhatsApp，他曾和以下哪个电话号码沟通？

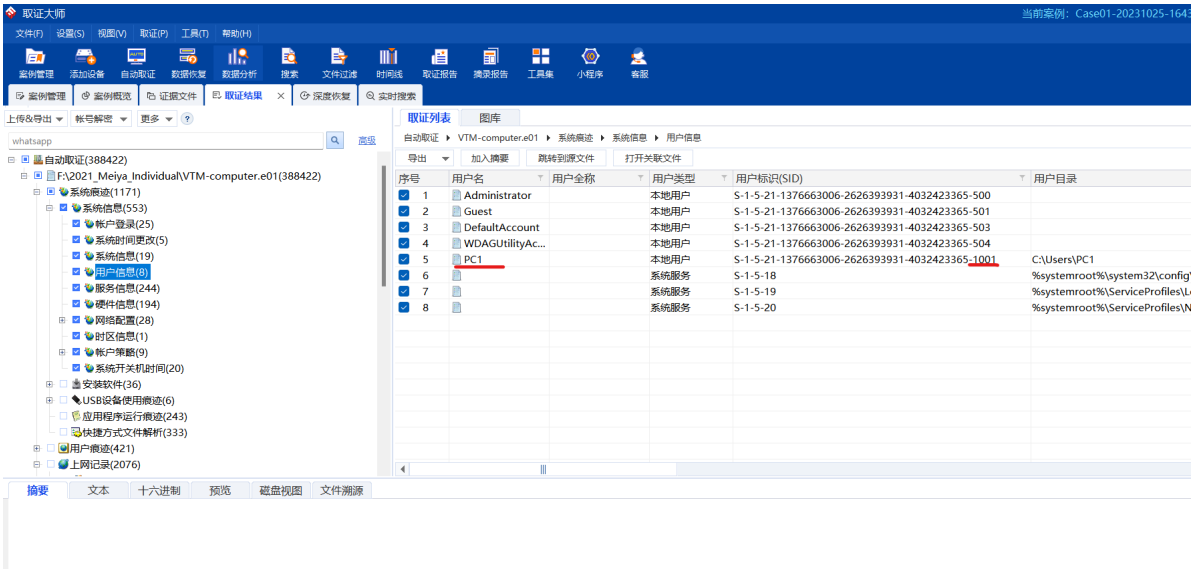
答案：85246761157

就根据上下文硬猜是和ALEX通讯了，所以就是ALEX的WhatsApp号，不然我也想不到其他的情况了。

17.工地主管的计算机的用户名称是什么？其用户标识符是什么？

答案：AF

在取证大师自动取证结果里的系统痕迹-用户信息中，就可以发现题目需要的用户名和ID号了：



1001转成16进制就是0x3e9.

18.工地主管计算机的预设浏览器是什么?

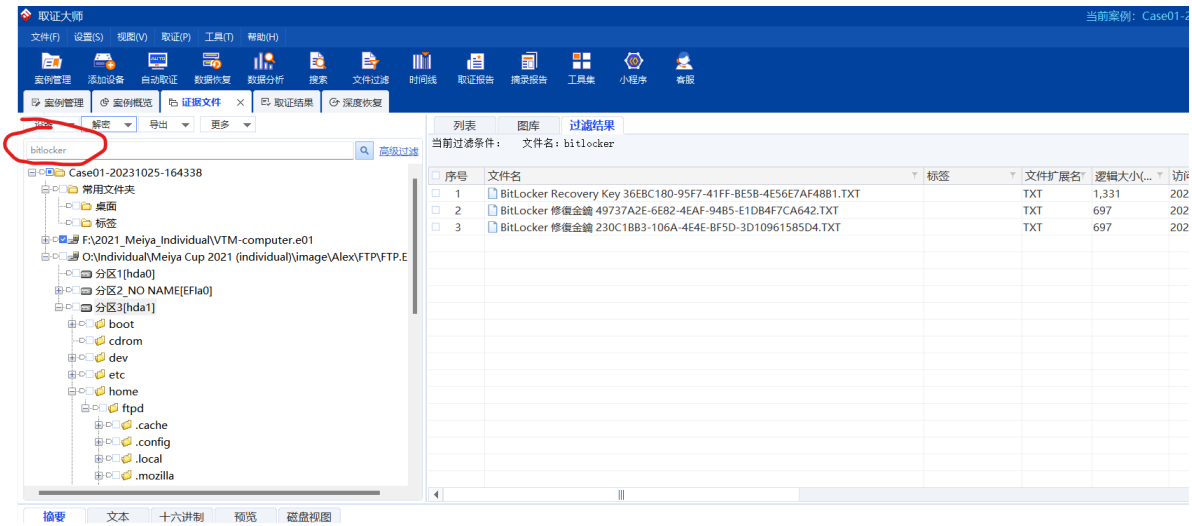
答案：A

从浏览记录就可以明显看出，Chrome使用的情况明显多于edge和IE，而且不存在选项中的其他浏览器，故选A。

19.工地主管计算机的其中一个分区被人加密，分区内的电子表格 Material3.xlsx 的哈希值（SHA1）是什么？（请以英文全大写及阿拉伯数字回答，不用输入'-'）

答案：40418B21F6C3E4AF306D5EF3B80A776DA72FC1D2

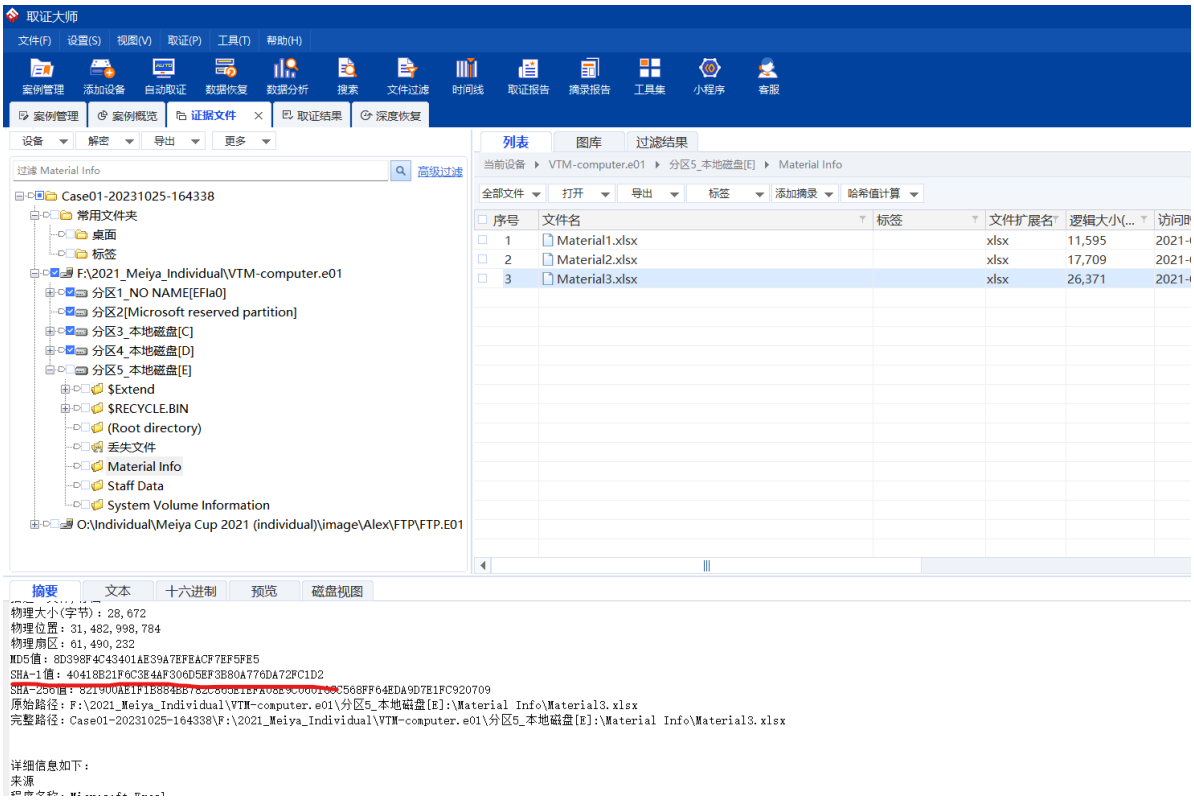
在FTP.e01的检材中搜索bitlocker，可以找到恢复密钥文件：



经过逐一测试，发现第一个文件可以解开工地主管计算机的分区：



拿到文件的哈希值：



20.路由器的记录中显示以下有哪些 IP 是公司的电子器材?

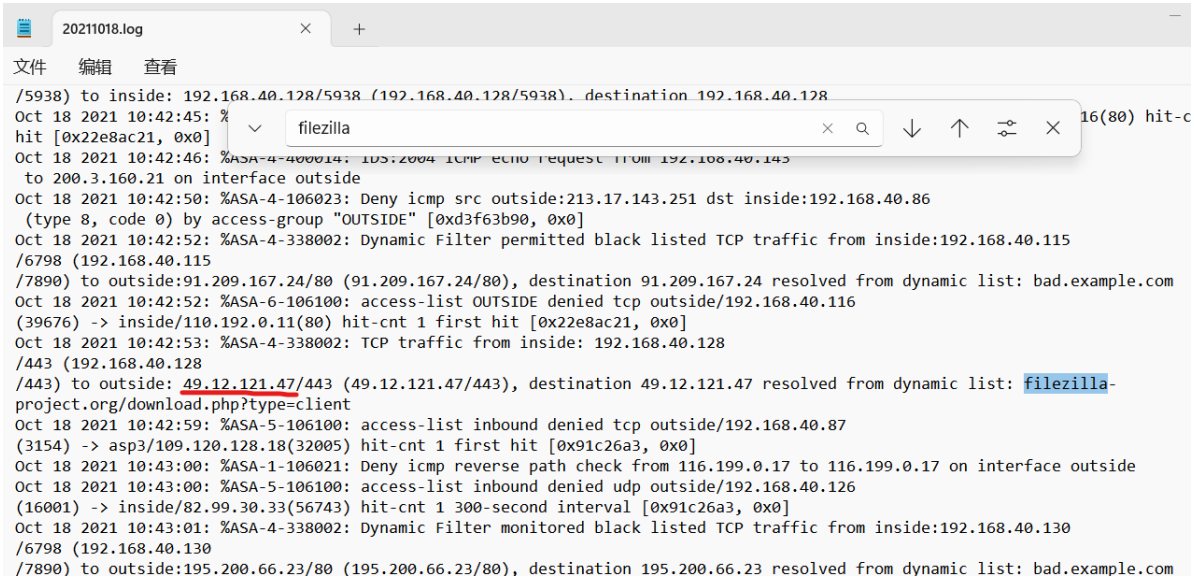
答案：ABCD

就直接打开 20211018.log 搜选项的5个ip，只有E搜不到。

21.路由器的记录中显示公司的计算机下载了FTP软件，该下载网站的 IP 是什么？（以阿拉伯数字回答，省去'.'符号）

答案：491212147

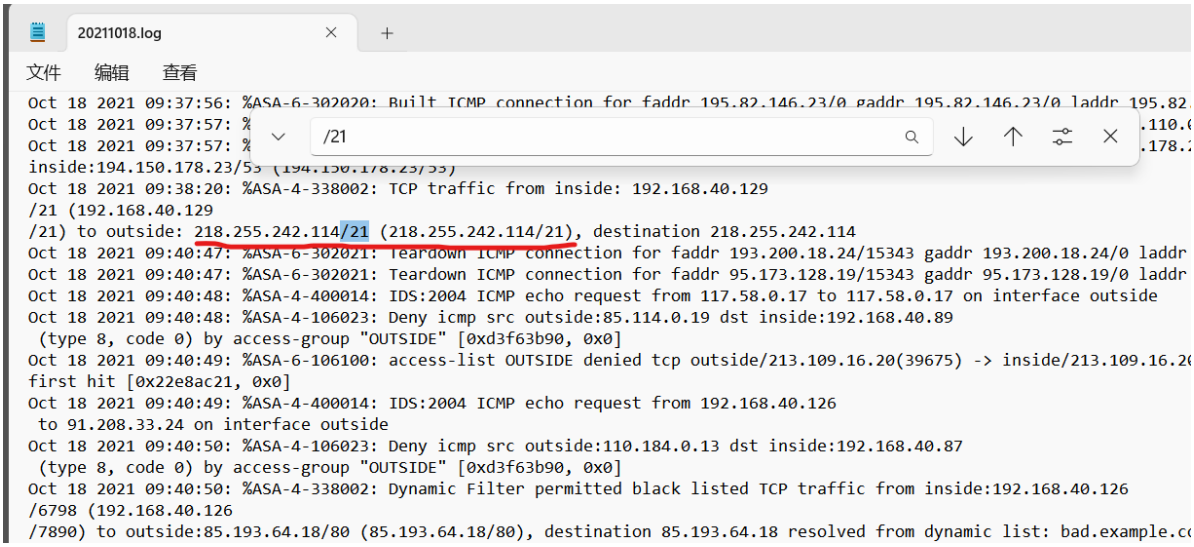
根据前面的问题我们一直下载的FTP软件为FileZilla，因此直接去搜索这个文件的名字，看看是哪个源ip请求的下载即可：



22.路由器的记录中显示公司计算机的资料用 FTP 软件传到了什么 IP 地址及利用端口?

答案：AD

根据常识，我不认为有人会把FTP开在80端口，而且21作为FTP的缺省端口，起一个FTP的服务很合理吧。所以直接搜`/21`，找到对应的ip地址就行：



23.路由器的记录中显示以下哪些关键词是表示公司计算机与外界网络联机?

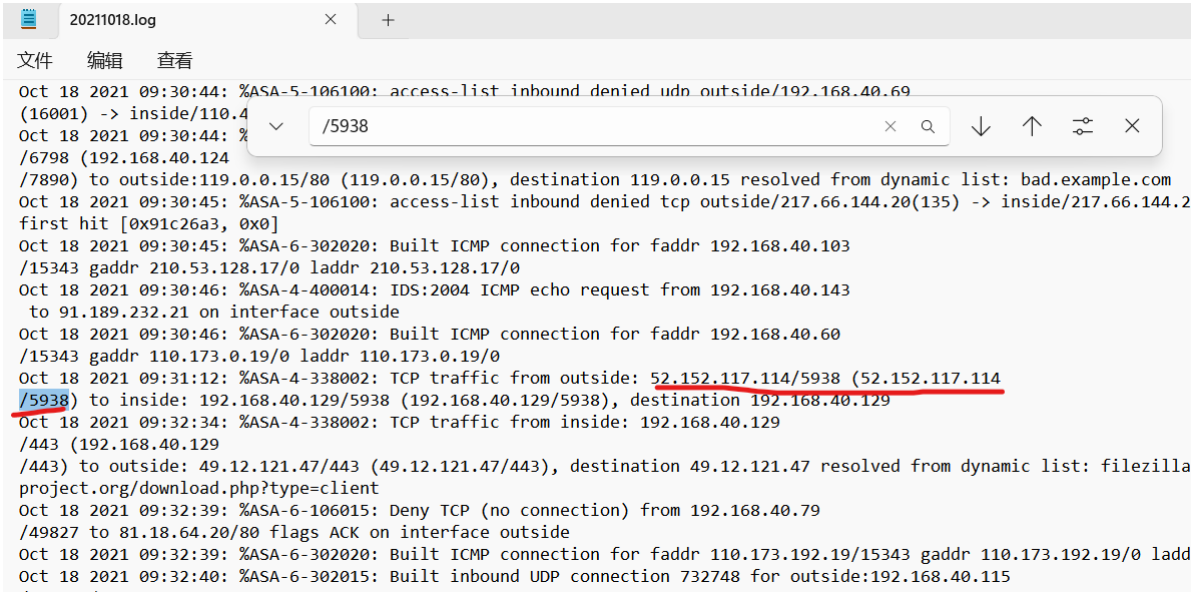
答案：AD

常识题、文化题、基础题。这个都不懂建议再读一遍计网。

24.路由器的记录中显示哪一个 IP 曾以 teamviewer 连接公司计算机?

答案：B

经查阅，TeamViewer的缺省端口为5938，因此搜索`/5938`，看看是什么ip进行的连接即可：



25.路由器的记录中显示以下哪一个有可能是以 teamviewer 遥控公司计算机的时间?

答案：ACE

思路同上题一样，搜`/5938`就行，可以发现存在这个端口连接记录的时间对应了ACE选项。

26.路由器记录中显示有多少器材有可能被入侵?

答案：3

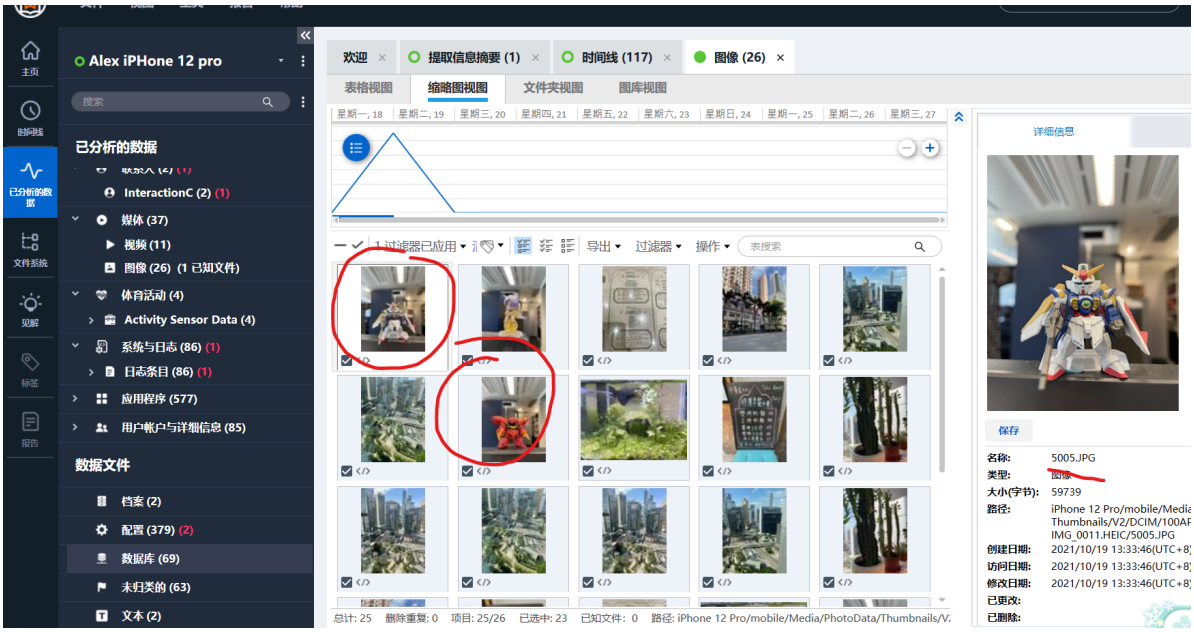
根据之前的聊天记录，应该就是主管自己加上两个同事的主机失陷，因此答案为3。

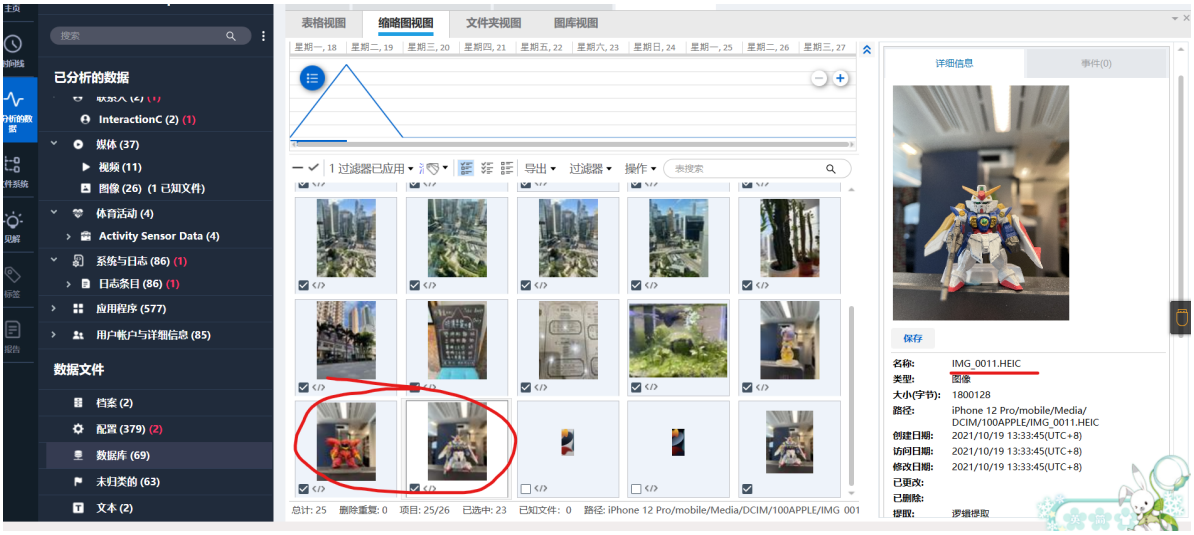
27.阿力士 iPhone 12 pro 电话于 2021 年 10 月 21 日，以下哪一张照片可能曾被分享（UTC+8）?

答案：AB

这题相当抽象，结合了别人的题解和官方答案试图做下解释。

查询分析数据中的媒体-图像部分，可以发现IMG_0010.HEIC和IMG_0011.HEIC这两张图都有一个名字叫5005.JPG的，图片显示内容一模一样的一个图片：



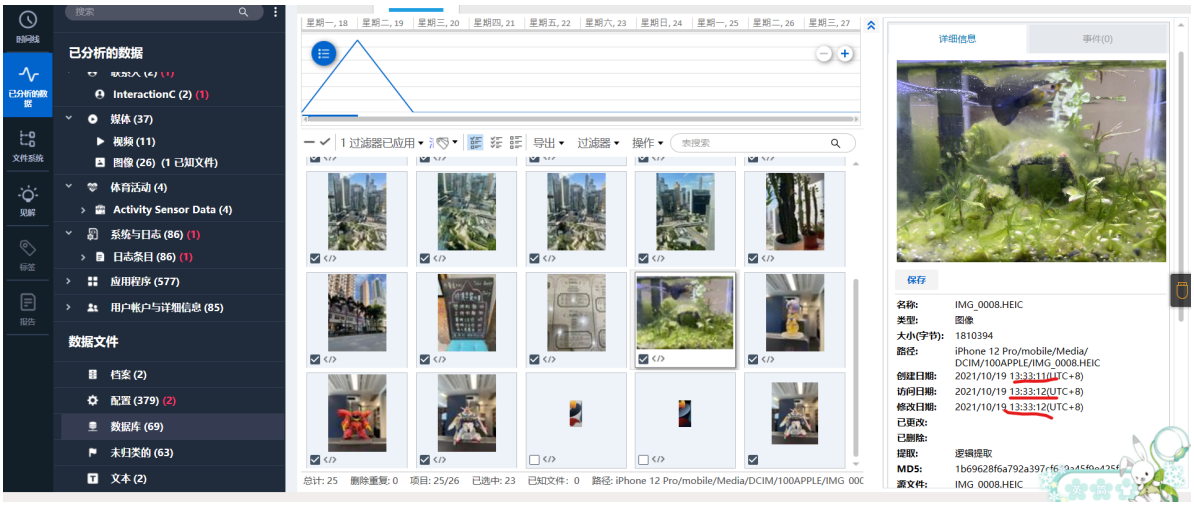


我认为是因为在分享文件的过程中没有传输原图，而将exif的信息舍弃了，导致了这些对应文件的大小明显对不上。因此这题选AB，这个题目说哪一张就挺离谱的，答案也是 AB就更离谱了。

28.阿力士 iPhone 12 pro 电话中哪一张相片可能曾被修改拍摄时间?

答案：D

也是在媒体-图像部分，发现D选项这张图片的创建日期与访问或修改日期不一致：

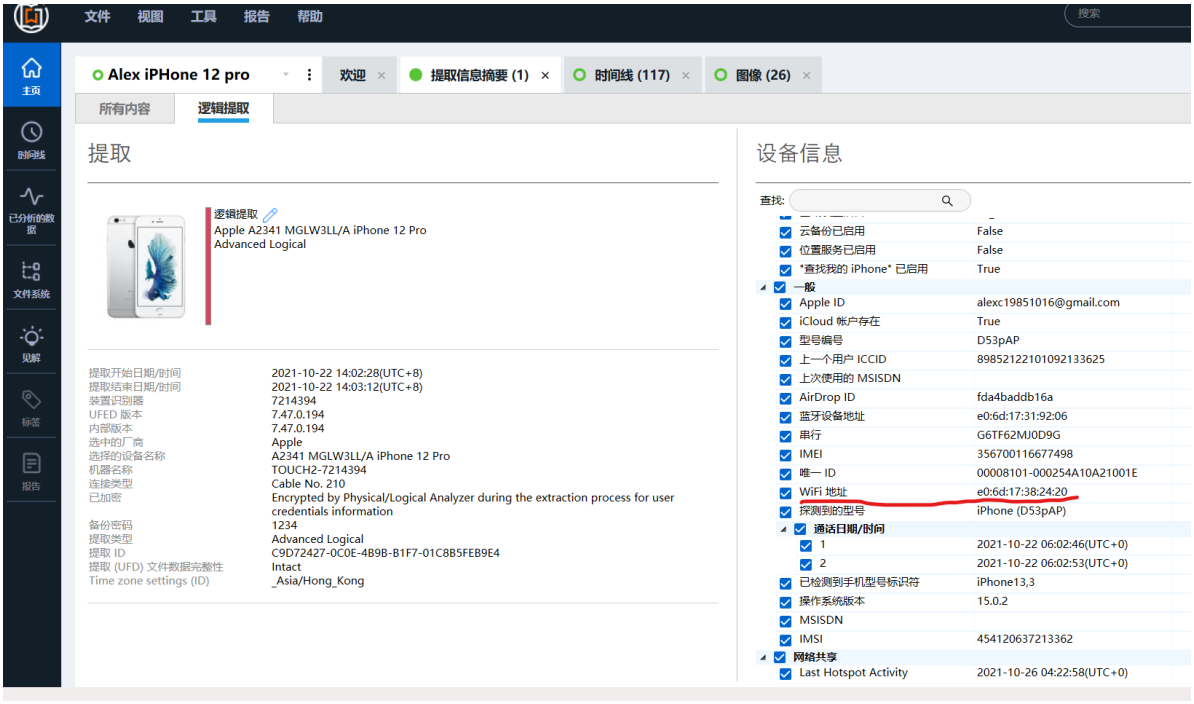


而其他三个选项这三个时间都是一致的，故认为选D。

29.阿力士的 iPhone 12 pro 的 GSM 媒体访问控制地址是什么？ （英文全大写加阿拉伯数字回答，不用输入':')

答案：E06D17319206

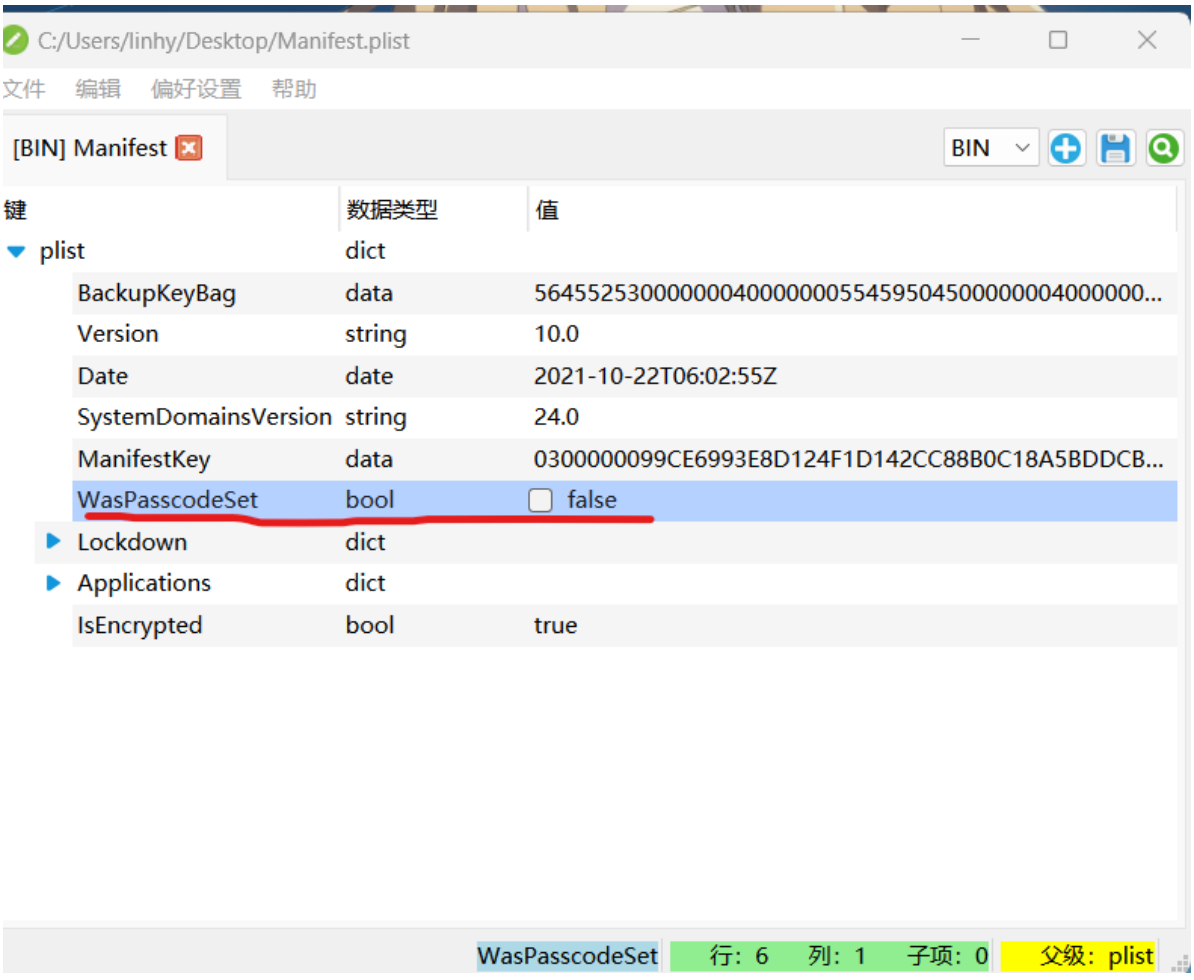
搜了下这个媒体访问控制地址就是MAC地址，因此应该就是这个逻辑提取中的WIFI地址了：



30.阿力士的 iPhone 12 pro 以什么屏幕密码保护?

答案：D

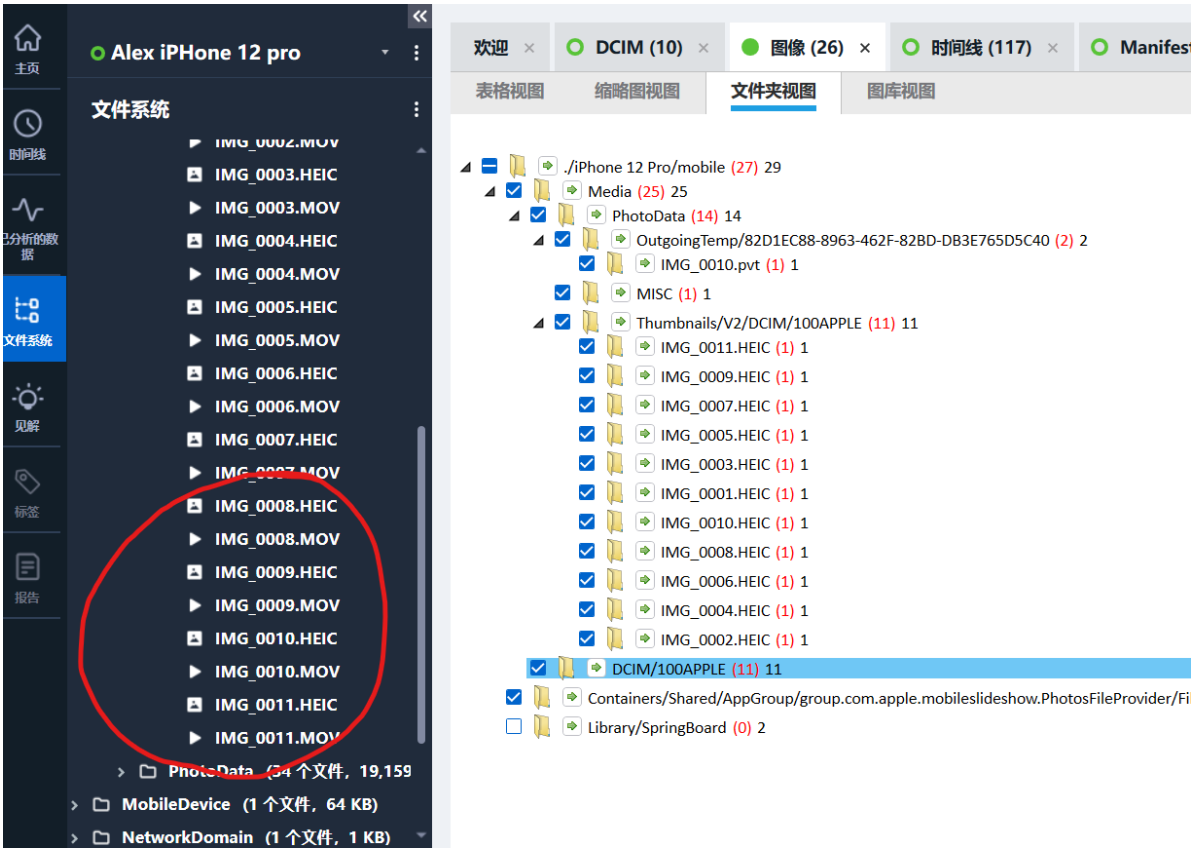
iPhone的密码信息彩云在Manifest.plist中，手动提取出来，然后因为是二进制文件，因此使用Xplist查看，发现`WasPasscodeSet`一栏为False，说明这个手机没有设置密码。



31.阿力士iphone 12 pro内以下哪一张相片是实况相片(live Photos)?

答案：ABD

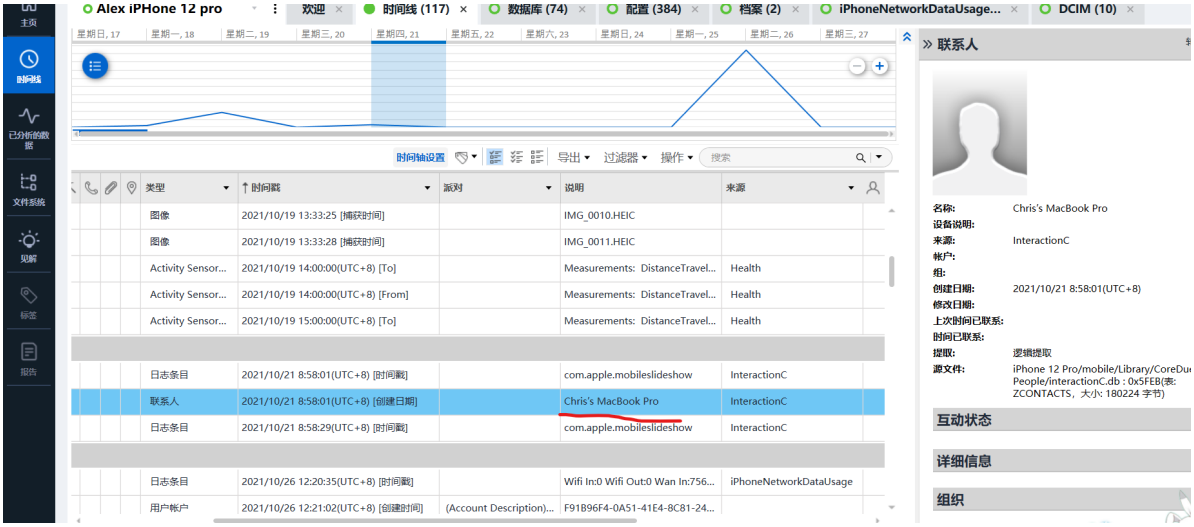
苹果手机的实况相片有一个特征，那就是会创建一个与照片同名的MOV文件，在/iPhone 12 Pro/mobile/Media/DCIM/100APPLE中就可以发现ABD三个图都存在对应的MOV文件：



32.以下哪一个是阿力士 iphone 12 pro 可能曾经连接的装置名称?

答案：A

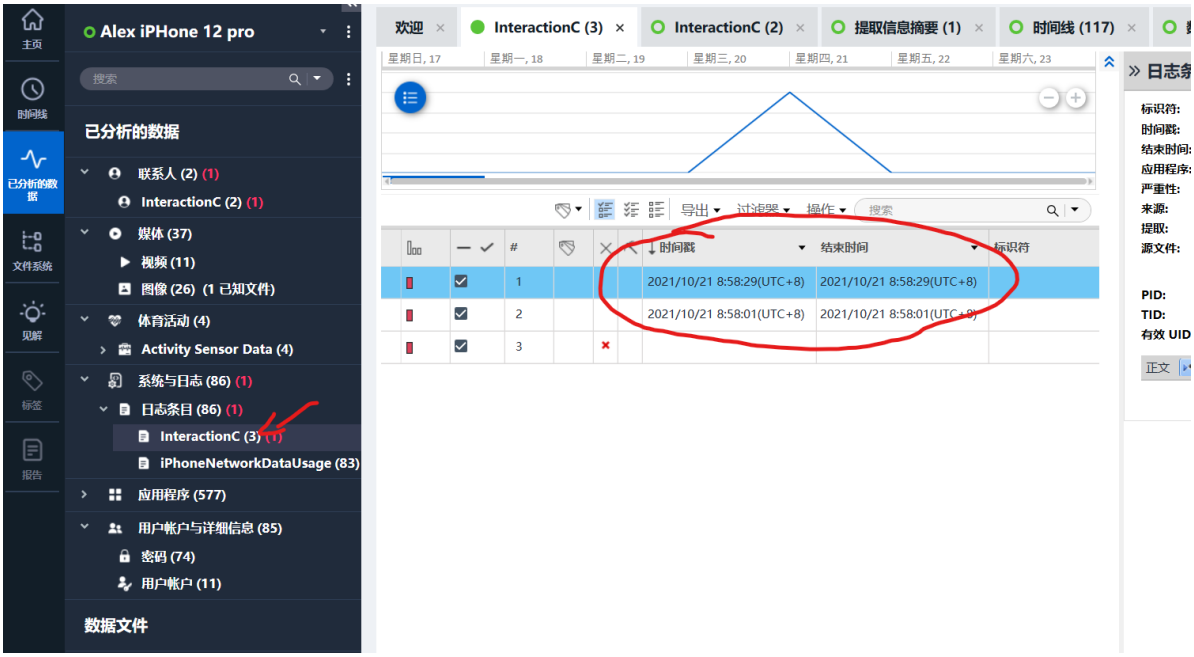
时间线里或者联系人可以发现，按道理直接搜索也可以：



33.接上题，记录连接时间是什么时候（UTC+8）？

答案：BC（官方给的BC，我觉得是BD）

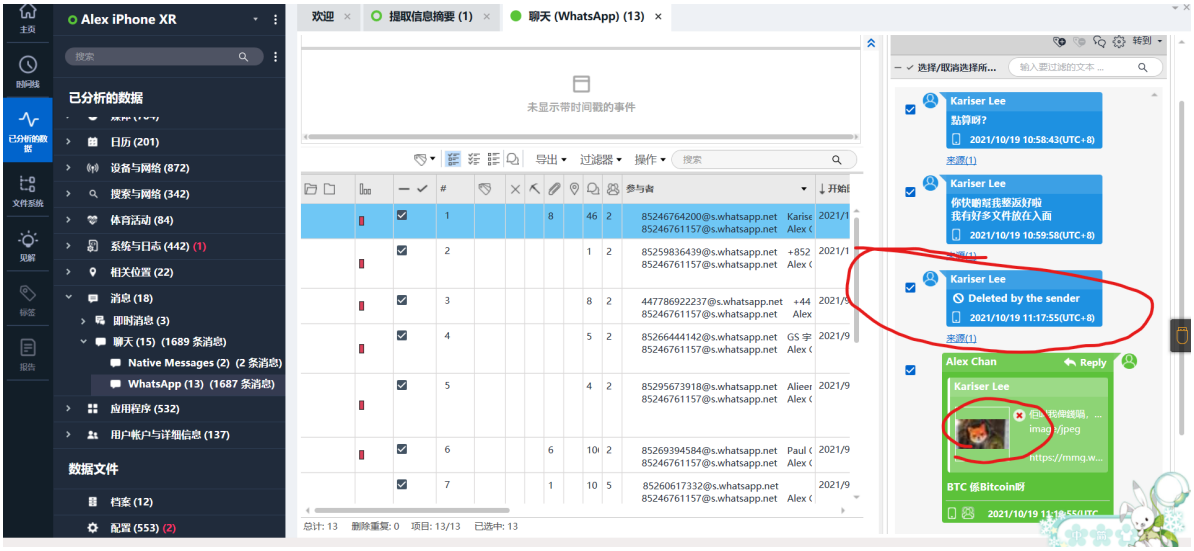
在InteractionC的日志条目中可以看到时间，C和D就差了一个8小时，感觉是答案有问题。



34.阿力士 iPhone XR 中在软件 WhatsApp 中工地主管与阿力士的对话中曾提到：[佢叫我俾钱喎，BTC係唔係呢个啊？]。在进行电子数据取证分析后，以下哪一个是有可能关于此对话的正确描述?

答案：AB

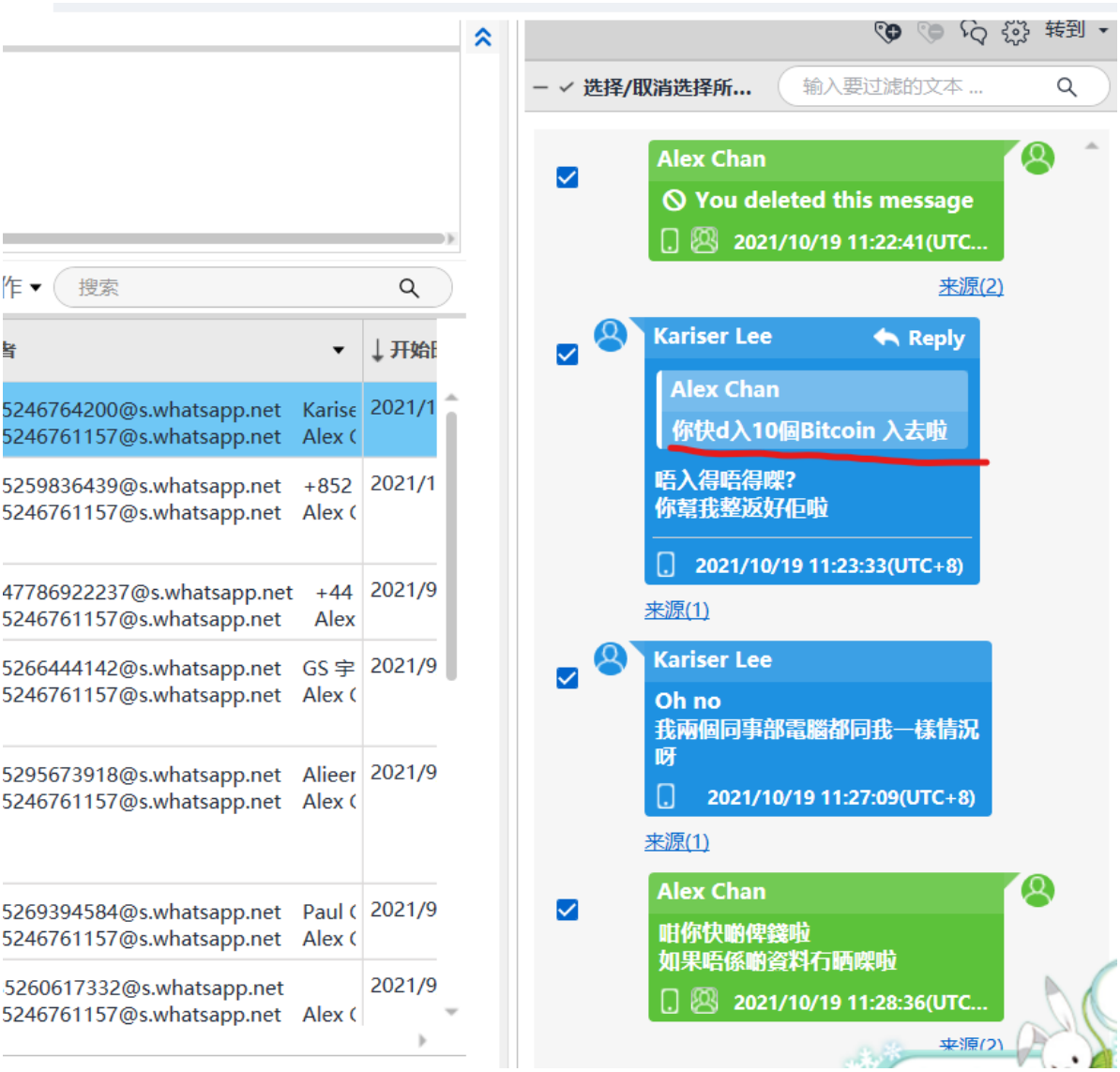
打开阿力士 iPhone XR 的阅读器，看下聊天记录就行，很明显是AB：



35.阿力士 iPhone XR 的 WhatsApp 对话中，阿力士曾要求工地主管支付多少个 BTC？（请以阿拉伯数字回答）

答案：10

也是聊天记录：

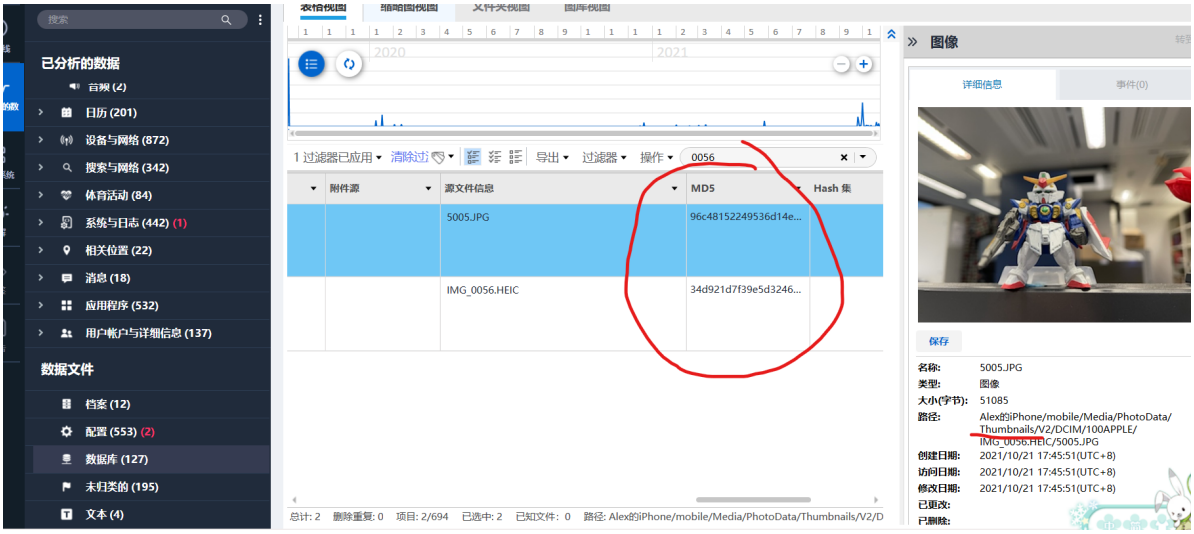


36.阿力士 iPhone XR 中 “IMG_0056.HEIC"的图像与"5005.JPG”(MD5: 96c48152249536d14eaa80086c92fcb9)" 看似为同一张相片，在电子数据取证分析下，以下哪样描述是正确??

答案：BC

A的话，iOS的照片我记得都是存储在Photis.plist里的。

B、C直接看图像信息，Thumbnails就是缩略图的意思：



D的话如果是打开后才产生的，两张图片的创建时间应该是有差距的，但是明显这两张图片的创建时间是相等的。

37.阿力士 iPhone XR 中相片 IMG_0056.HEIC 提供了什么电子数据取证的信息?

答案：AD

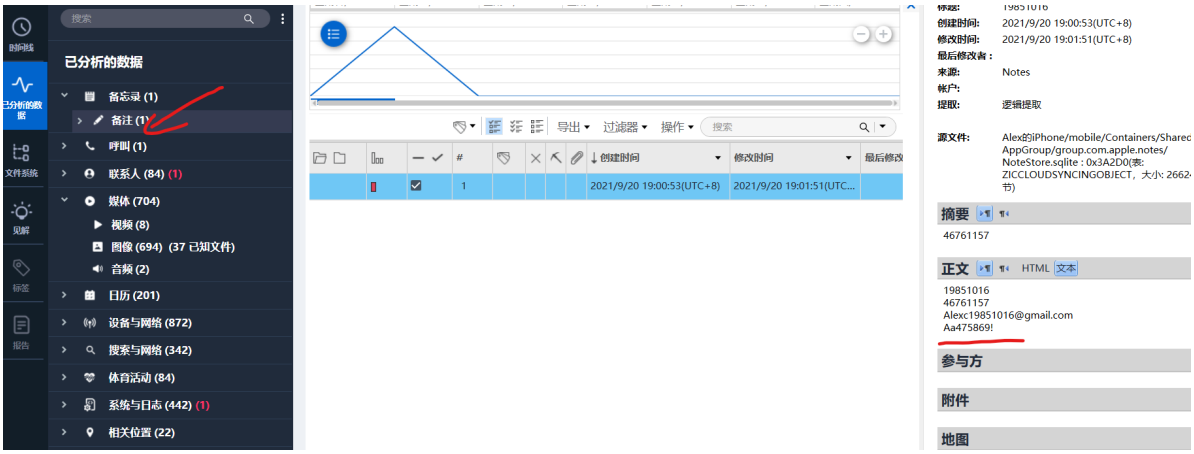
直接看照片的原数据信息即可，很明显这照片不是XR拍摄的，因此就是隔空投送的，然后拍摄时间是捕获时间，而不是创建时间，这里的创建时间应该是XR接收到12 pro隔空投送的时间：、



38.阿力士iPhone XR中阿力士的电邮账户 Alexc19851016@gmail.com 的密码有可能是什么?

答案：C

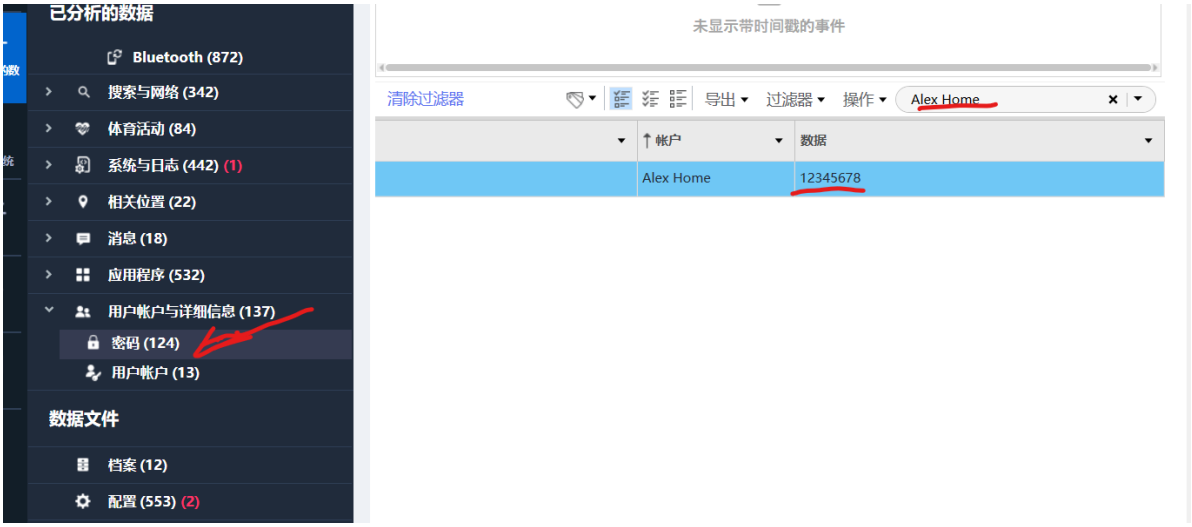
备忘录记着：



39. 阿力士 iPhone XR 曾经连接 Wifi "Alex Home" 的密码是什么?

答案：12345678

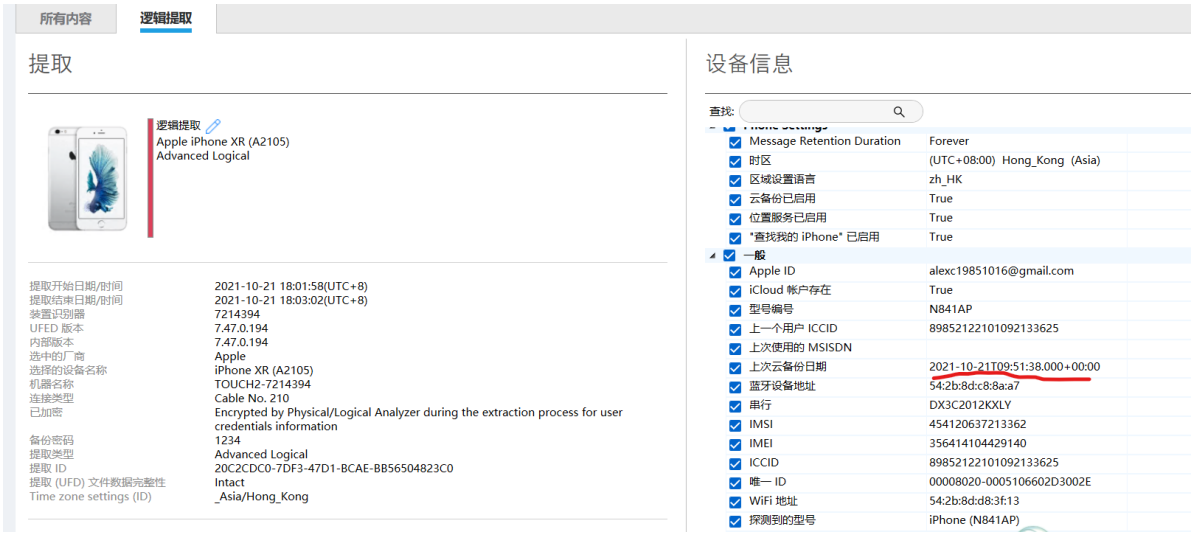
在`用户账户与详细信息-密码`里面搜WIFI的名字就行了：



40.阿力士 iPhone XR 经 iCloud 备份的最后时间是什么？ （UTC+8)

答案：A

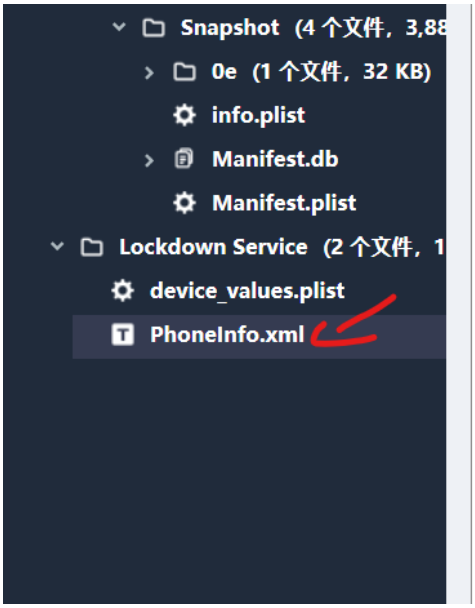
逻辑提取的信息中存着上次云备份的时间，但是要记得加8小时：

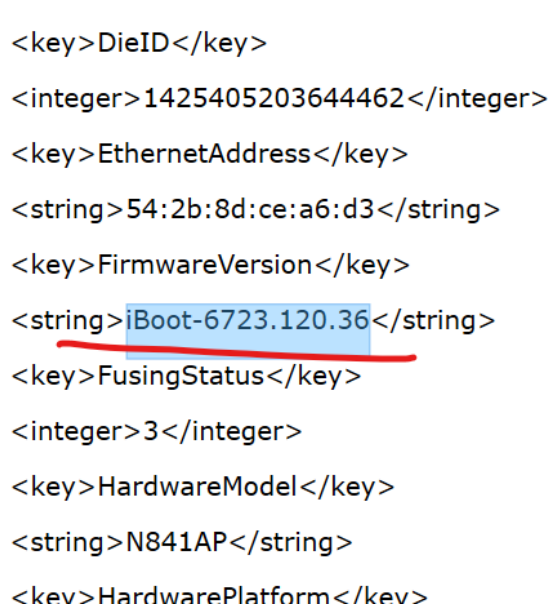


41.阿力士 iPhone XR 中的 iBoot 版本是 iBoot-___？(请以阿拉伯数字回答，不用输入".")

答案：672312036

在Lockdown Service/PhoneInfo.xml里，可以记下这个文件名，里面存着不少手机信息：

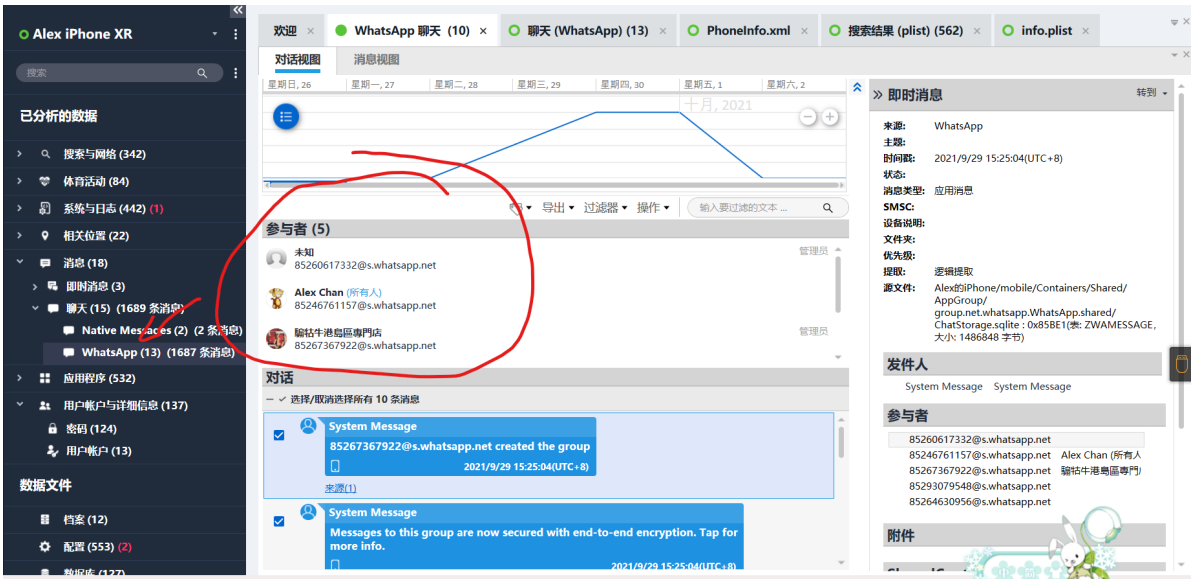




42.阿力士 iPhone XR 中的 WhatsApp 群组『团购-新鲜猪肉牛肉-东涌群组-9/30』有以下哪一个成员?

答案：AD

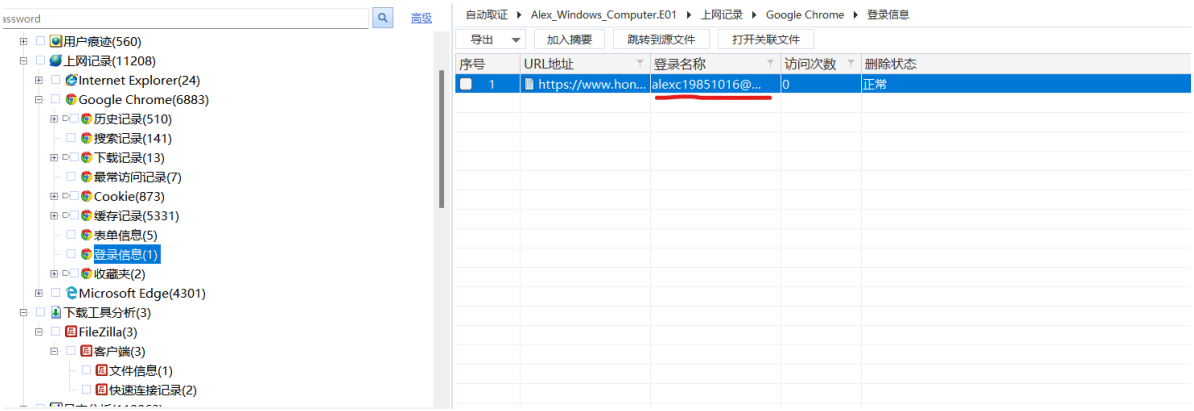
找到对应群聊，一个个选项和参与者里面的人对过去就行：



43.阿力士的计算机显示曾于 hongkongcard.com 的论坛登记成为会员，以下哪个是他的帐户密码?

答案：A

查看`上网记录-登录信息`：



这个账号和之前38题一模一样，所以也认为是直接用了邮箱登录，密码应该也是一模一样的。

44.阿力士的计算机显示阿力士曾用什么方法进入受害者（主管）的计算机?

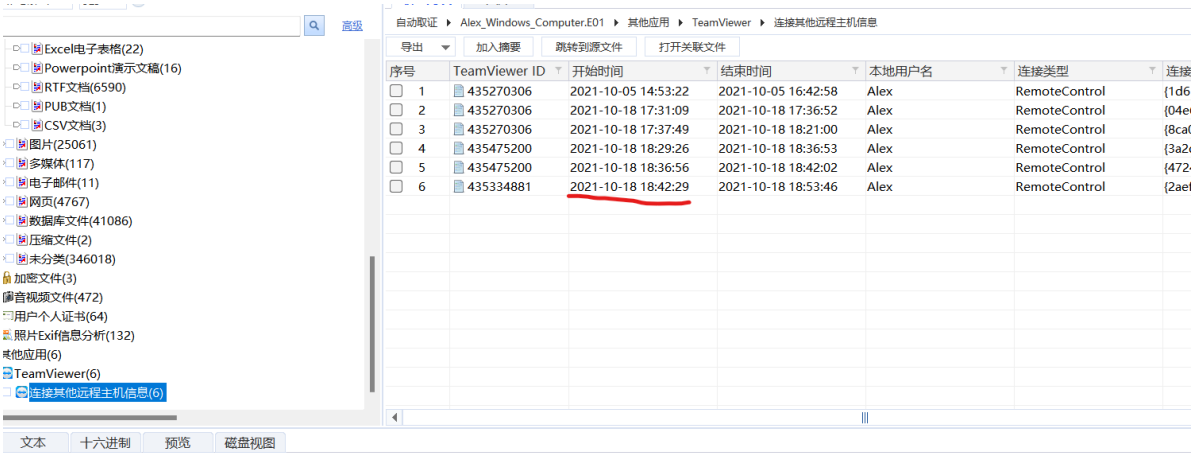
答案：A

TeamViewer都不知道提了多少次了，不知道这个软件干嘛的搜一下应该都能知道是拿来远程连接的吧。

45.续上题，阿力士最后一次进入受害者（主管）计算机的时间是什么?

答案：D

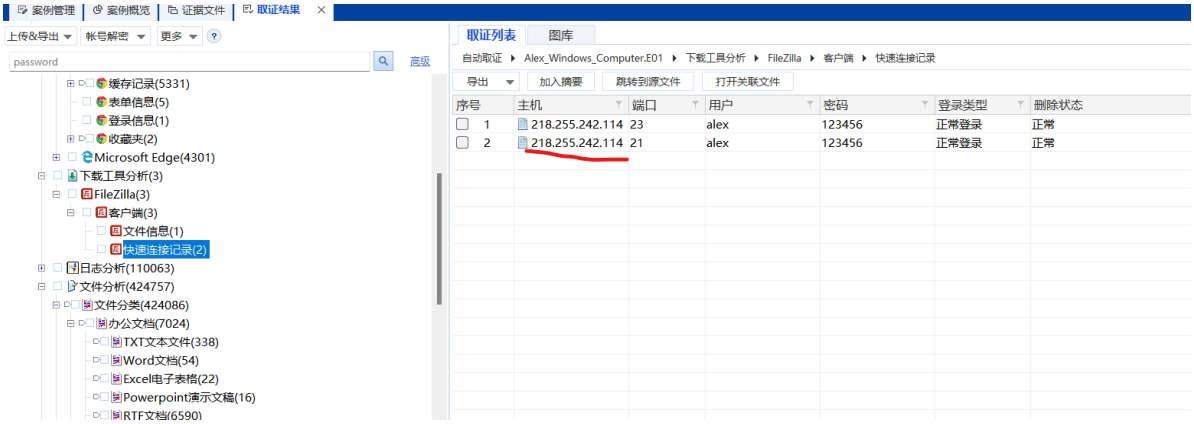
看一下`其他应用-TeamViewer-连接其他远程主机信息`就行，注意是连接的最后时间：



46.阿力士的计算机显示他曾经使用 FTP 程序，FTP 的主机 IP 地址是什么？（请以阿拉伯数字作答，省去"."符号）

答案：218255242114

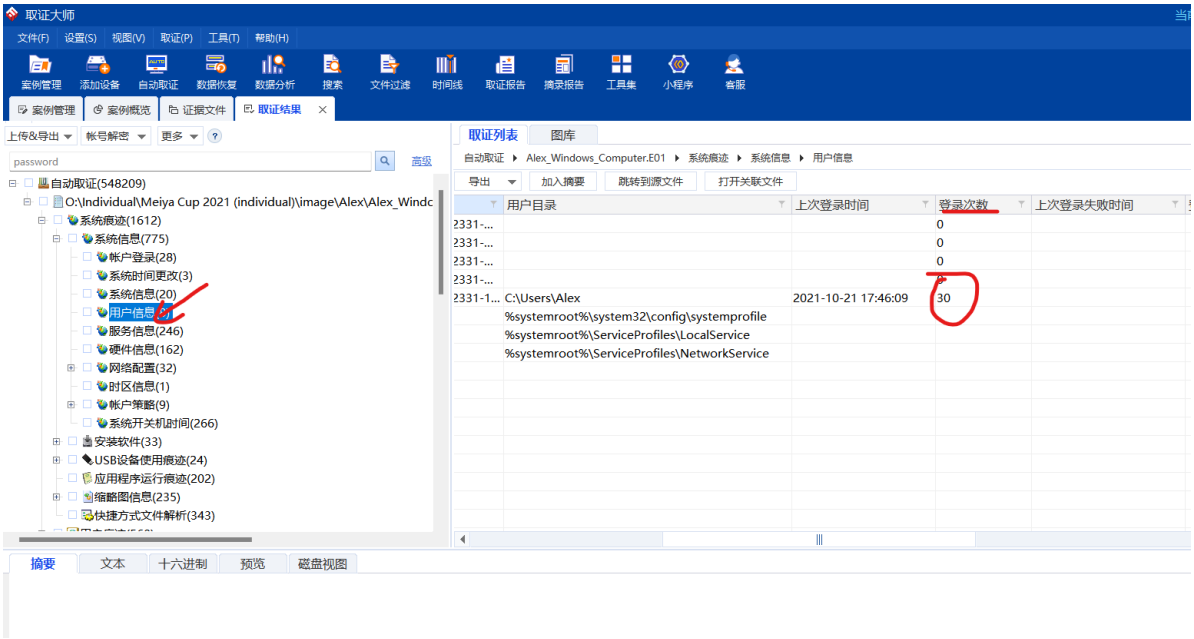
查看`下载工具分析-FileZilla-快速连接记录`即可，前面的路由题也涉及到了：



47.阿力士的计算机显示于2021年9月至2021年11月期间，计算机曾被登入过多少次？（请以阿拉伯数字回答）

答案：30

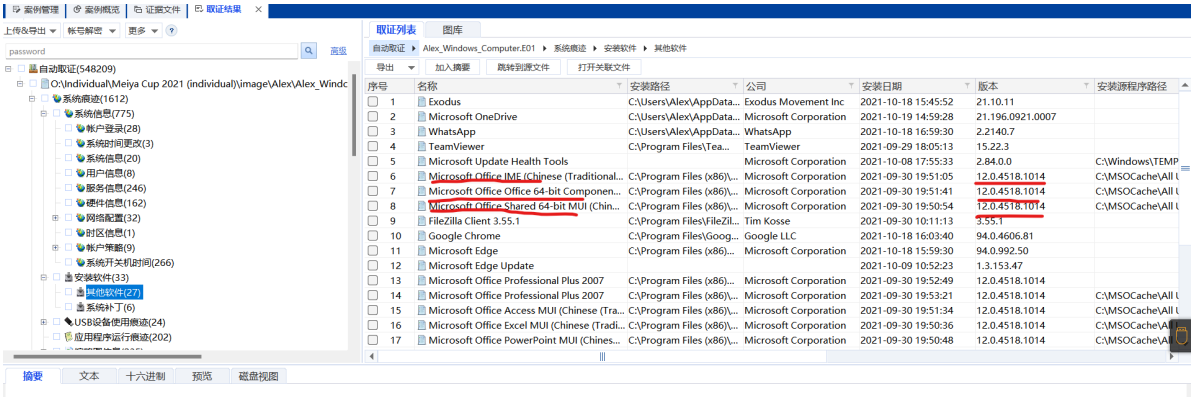
查看`系统痕迹-系统信息-用户信息`即可，记录了登录次数：



48.阿力士计算机所安装的 Microsoft Office 2007 是以下哪一个版本？（请以阿拉伯数字作答，省去"."符号）

答案：12045181014

查看`系统痕迹-安装软件-其他软件`即可，记录了安装软件的版本号：



49.以下是阿力士计算机中的 Basic data partition (EFI 3) 的 Volume ID？（请以英文全大写及阿拉伯数字回答）

答案：94C44CA5C44C8B84

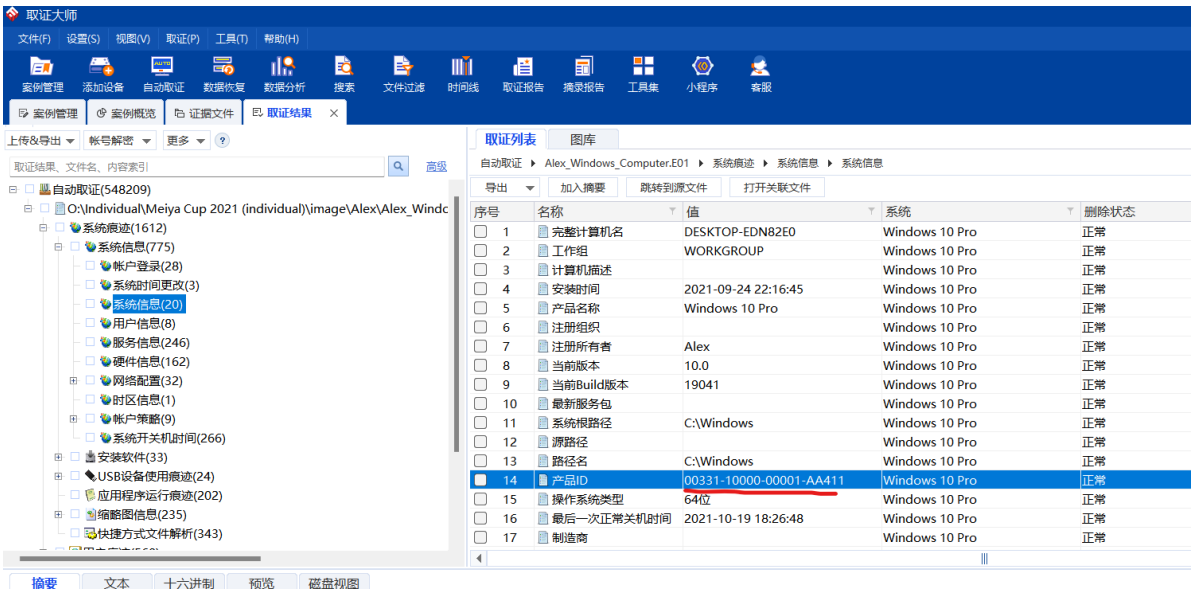
用取证大师挂载下镜像，DiskGenius查看卷序列号即可：



50.阿力士计算机的 Window product ID 是什么？（请以英文全大写及阿拉伯数字回答，不用输入"-"）

答案：003311000000001AA411

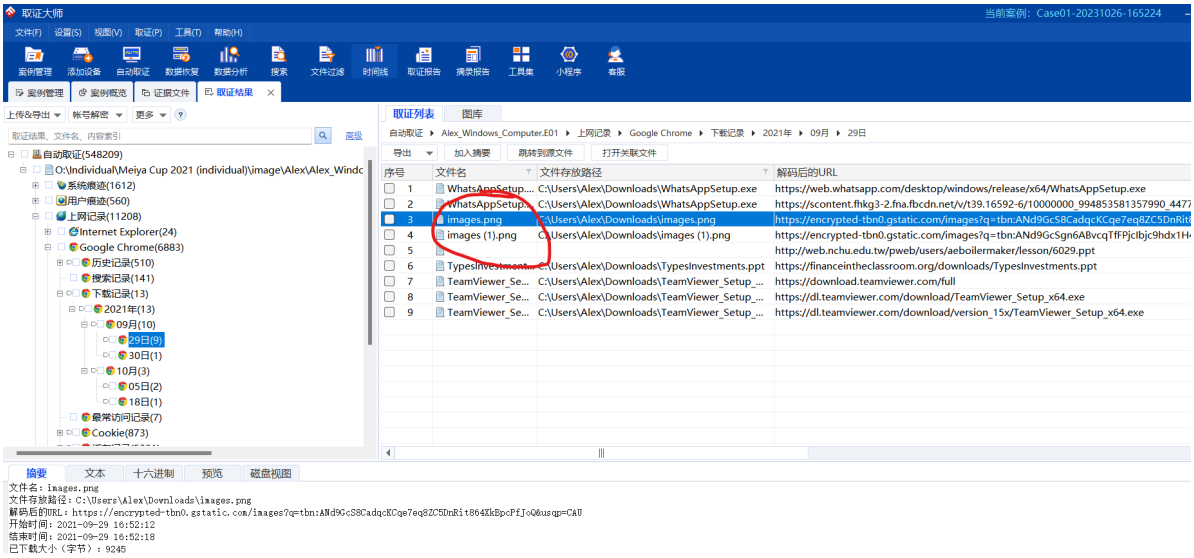
查看`系统痕迹-系统信息-系统信息`即可：



51.阿力士计算机曾经下载一张猴子的图片，以下哪一项描述正确?

答案：A

首先在下载记录中发现可疑目标：



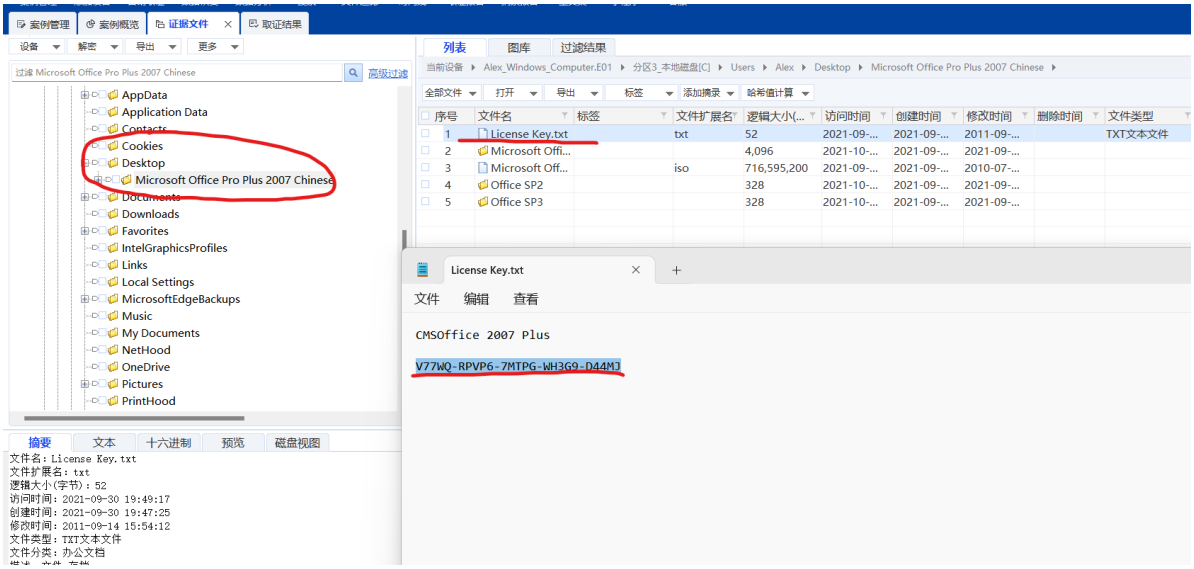
确认路径，去看一下是什么图片，经确认，这个image（1）.png为题目所要的猴子图片，故A项正确。

B很明显直接下载下来的，没有经过加密；下载时间是9月29日，C错误；直接下载就是png格式，没有经过转化，因此D错误。

52.阿力士计算机所安装的 Microsoft Office 2007 的密钥是甚么？（请以英文全大写及阿拉伯数字回答，不用输入"-"）

答案：V77WQRPVP67MTPGWH3G9D44MJ

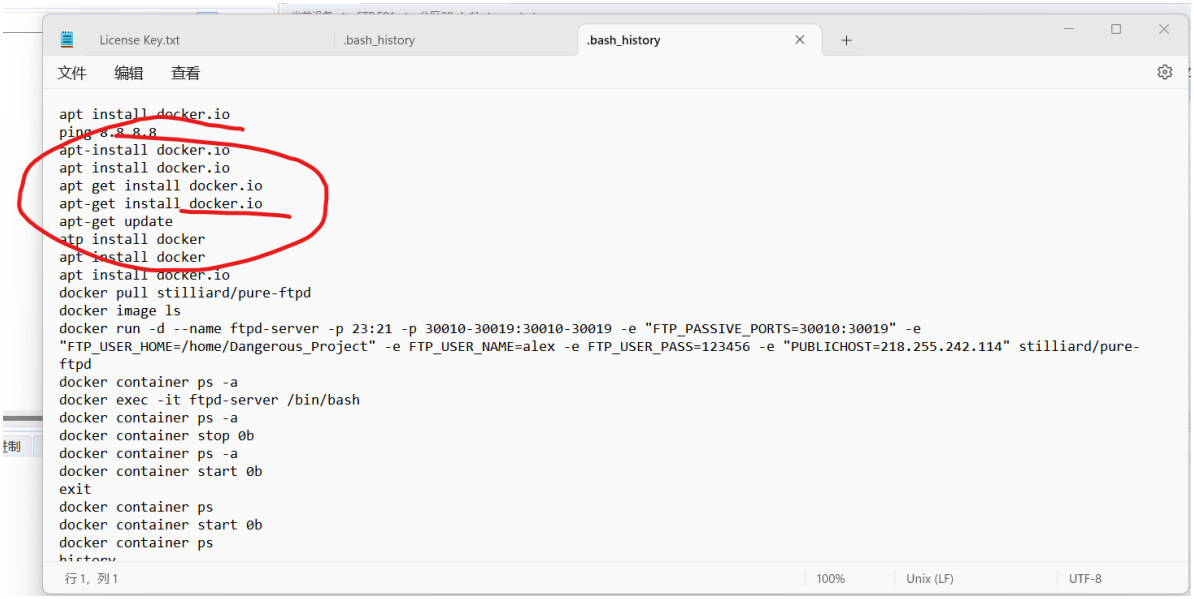
在桌面的office文件夹中就可以发现License Key.txt了：



53.阿力士 FTP 服务器用户使用命令行安装了什么程序?

答案：A

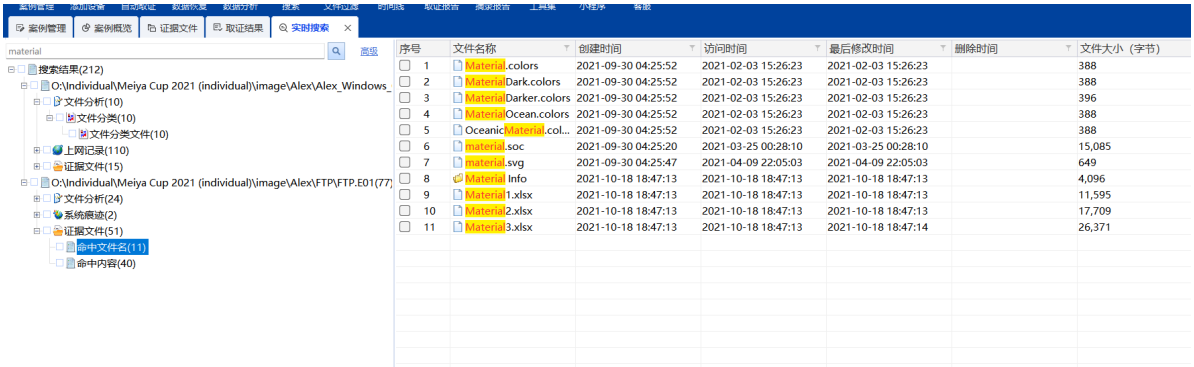
命令行储存在用户文件夹下的`./.bash_history`中。ftpd用户命令行没有执行下载，而root用户下载了docker：

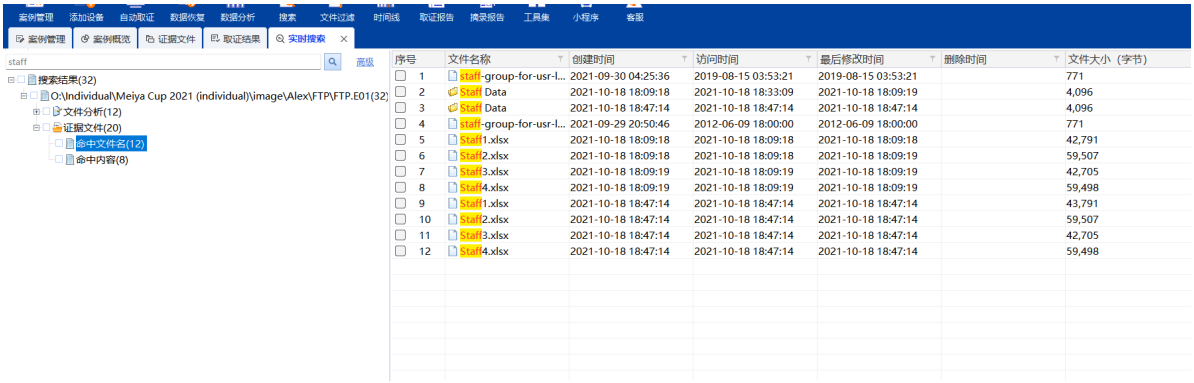


54. 以下哪些档案于阿力士 FTP 服务器曾重复出现?

答案：DEF

搜一下就知道了：

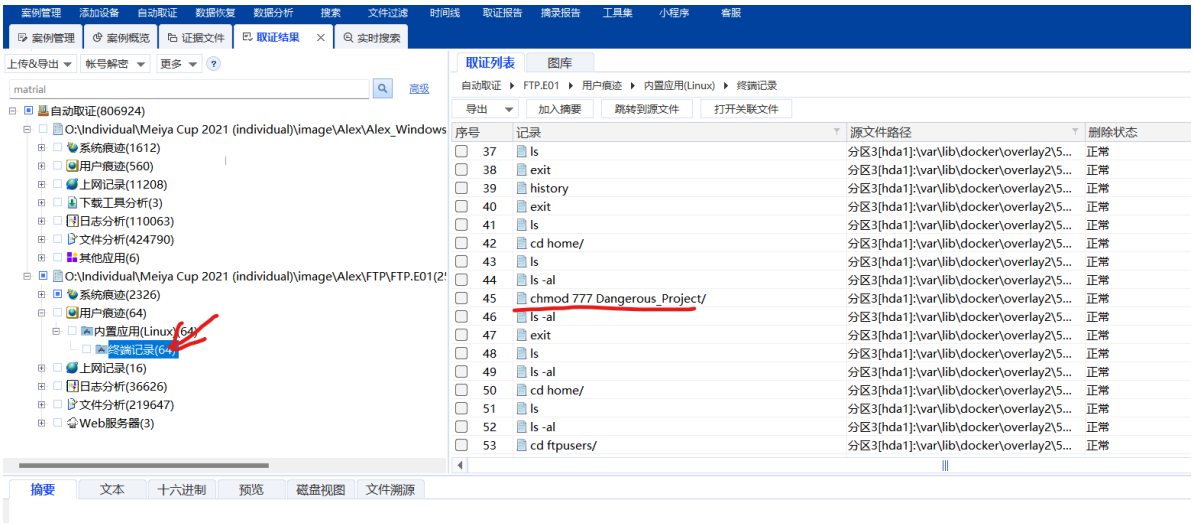




55.在阿力士FTP服务器中，文件夹__曾被用户变更了访问权限（请以英文全大写及阿拉伯数字回答）

答案：DANGEROUSPROJECT

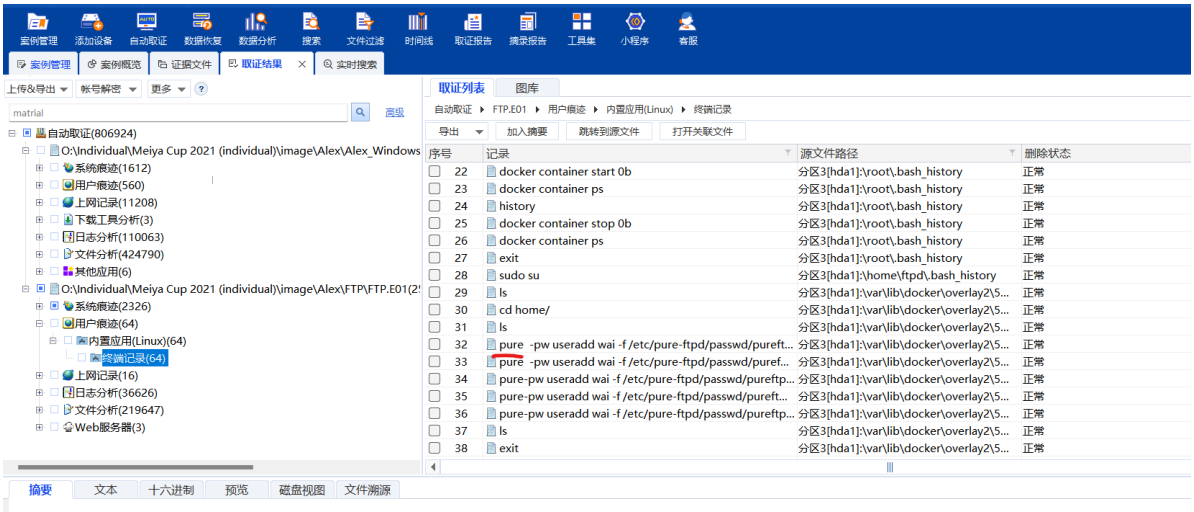
查看 用户痕迹-内置应用-终端记录 即可，chmod是修改权限的命令：



56.在阿力士FTP 服务器建设后，有__个额外用户被加入？（请以阿拉伯数字回答）

答案：1

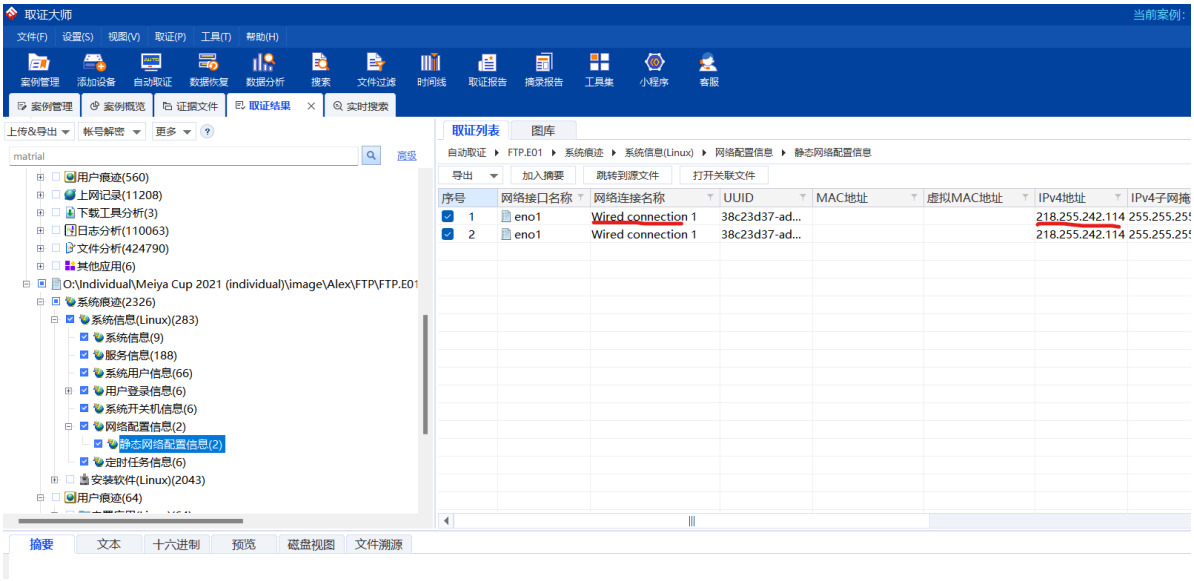
依然是查看终端记录，在docker run启动了一个ftp后，使用pure新增了1个名为wai的用户：



57.根据阿力士FTP服务器设定显示，此服务器是以__方式连接网络，且是一个____网络状态

答案：C

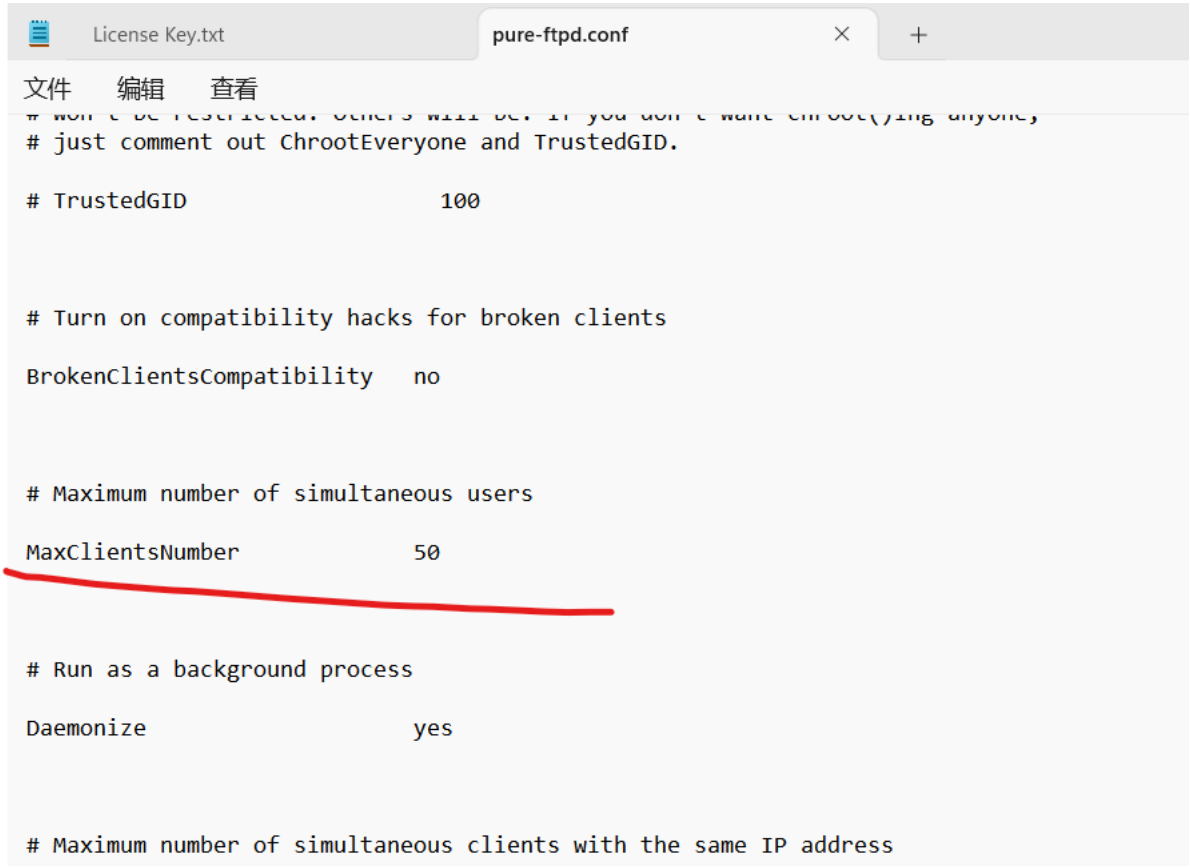
查看 系统痕迹-网络配置信息-静态网络配置信息 即可，ip地址是公网ip：



58.阿力士FTP 服务器设定最多使用者数目是___(请以阿拉伯数字回答)

答案：50（答案给的是5，但我觉得应该是50）

Linux由于万物皆文件的特性，因此这个设置也肯定是在一个文件里。找到ftp的conf文件：

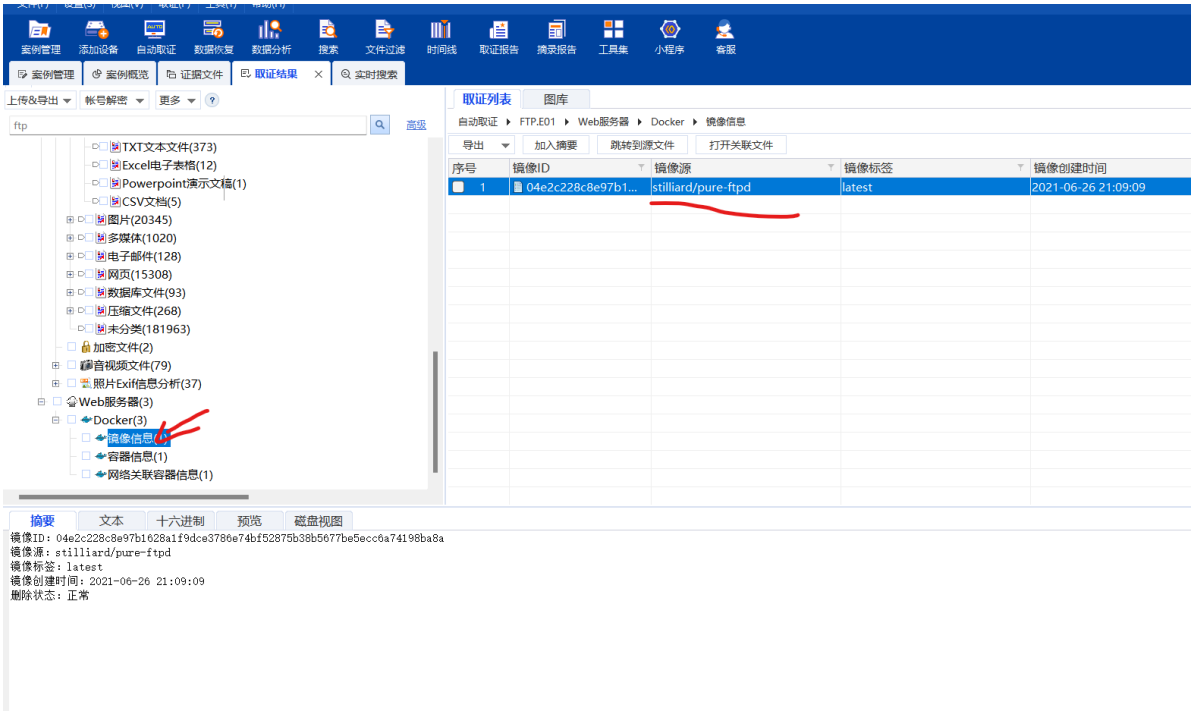


然后以防万一，我还仿真后进了docker容器再看了下，一样也是50，因此我觉得答案是50。

59.阿力士FTP服务器使用Docker安装了一个FTP程序为____。(例如 space docker /1.1，请输入spacedocker/1.1，不要输入空格)

答案：stilliard/pure-ftpd

在`Web服务器-Docker-镜像信息`中可以看到：



60. 阿力士 FTP 服务器曾使用过什么版本的 Linux 内核?

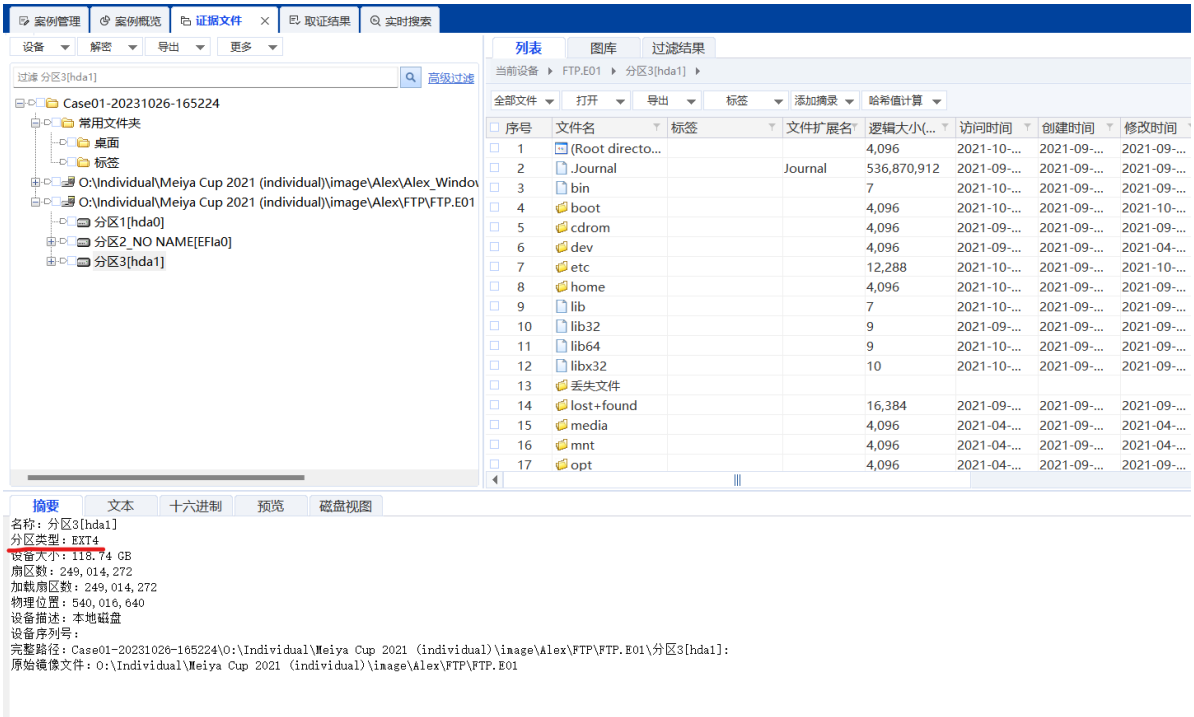
答案： AD

直接搜，看内核日志里面有没有结果就行了，然后就AD两个版本有。

61.阿力士 FTP 服务器的磁盘分区，有以下哪一种文件系统?

答案：BE

在磁盘分区的摘要信息中可以看到绕分区类型：



分区2、分区3分别为B项和E项。

62. 阿力士FTP服务器用户输入了指令_____去检查现存的Docker容器 (例如 netstat lntp，请输入netstatlntp，不要输入空格)

答案：dockercontainerps-a

玩过docker就知道这命令是拿来检查现存容器的，也是在bash历史中可以查看：

