

第三届长安杯---检材四五分析

原创

爱喝旺旺的旺旺 于 2022-01-25 08:46:55 发布 80 收藏

文章标签: 经验分享

版权声明: 本文为博主原创文章, 遵循 CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_51233573/article/details/122668215

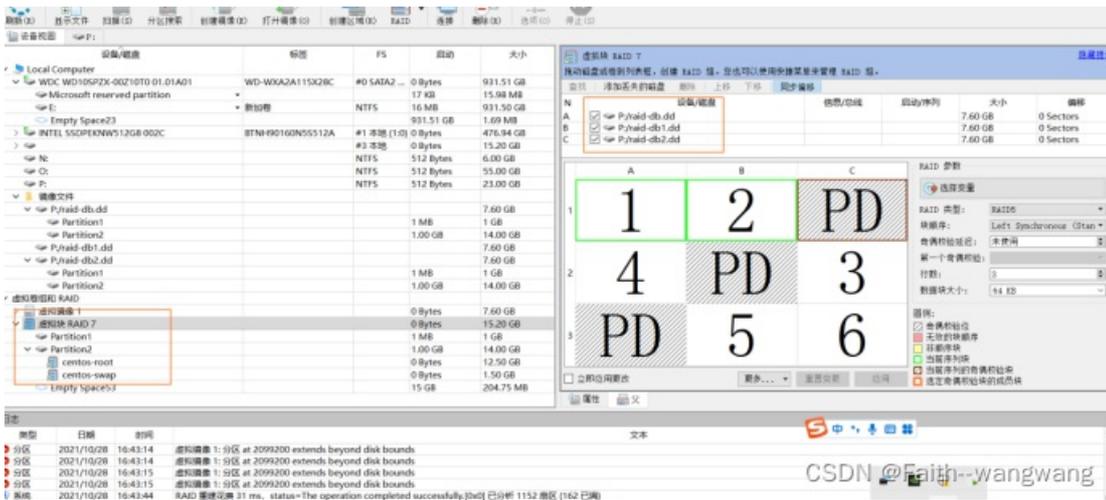
版权

解压检材五发现为一个raid重组后的阵列的三个镜像需要对其进行raid重组



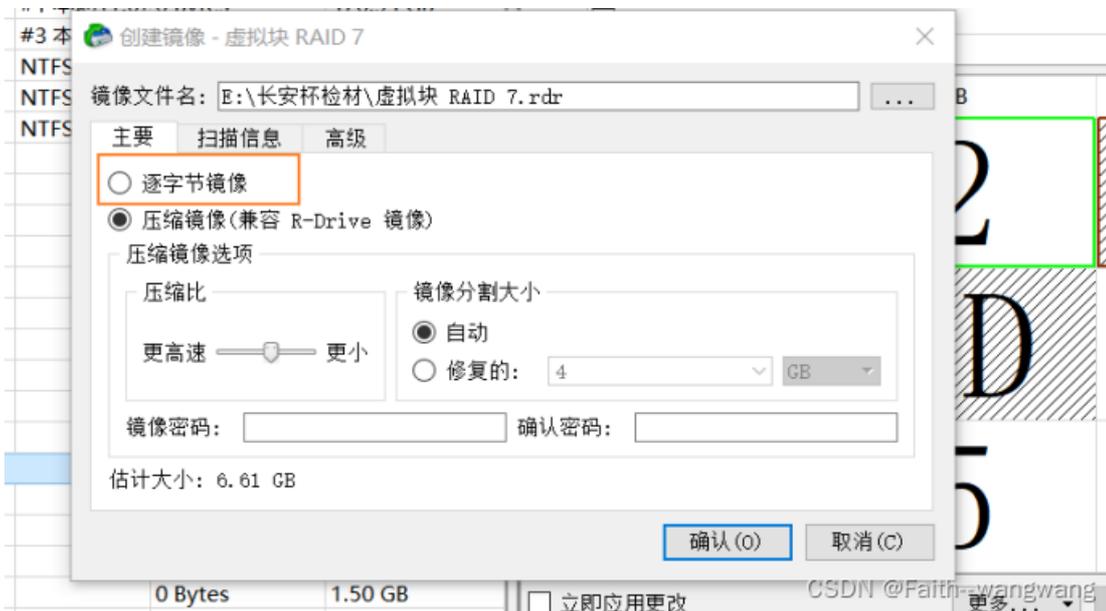
使用R-studio对阵列进行重组

得到重组后的raid阵列



析

打镜像使用仿真进行分析



这里打镜像时要使用逐字节镜像 否则不能仿真

对虚拟机的相关网络进行配置 使他们均在一个网段内（对检材二的解析有介绍）

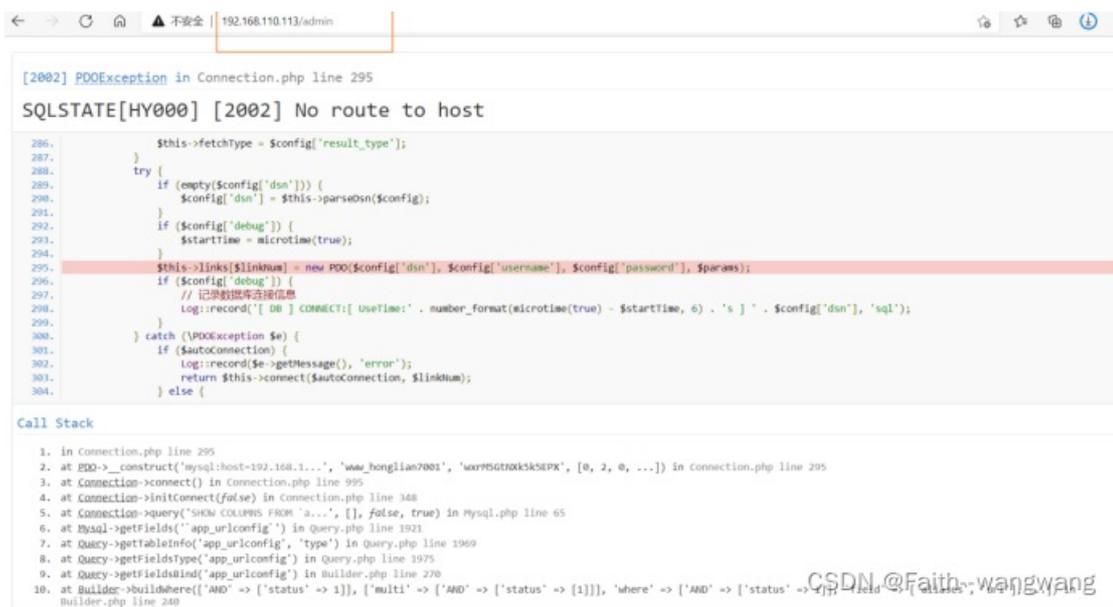
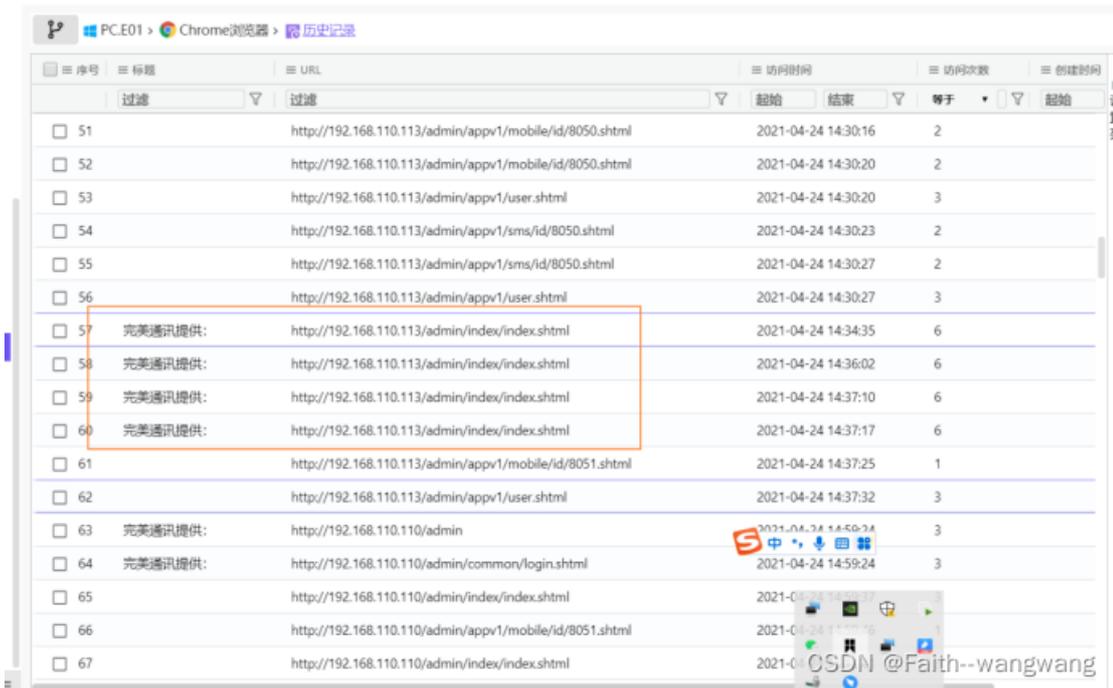
31.请分析，数据库的登陆密码为。

接上题的网站源码分析直接可以看到

wxrM5GtNXk5k5EPX

32.请尝试重构该网站，并指出，该网站的后台管理界面的入口为【标准格式：/web】

在对嫌疑人的pc进行分析在浏览器日志分析



本地访问这个界面 因为没有连接数据库所以这里看不到界面

完美通讯提供

用户名

密码

验证码

记住账号

登入

CSDN @Faith--wangwang

重构网站后的界面

33.已该涉案网站代码中对登录用户的密码做了加密处理。请找出加密算法中的salt值【区分大小写】

将其源码拖出来审计一下 找到其定义密码的函数找到其salt值

```
function password($password, $password_code='lshi4AsSURU0wMv')
{
    return md5(md5($password) . md5($password_code));
}

/**
 * 管理员操作日志
 * @param [type] $data [description]
 * @return [type] [description]
 */
function addlog($operation_id='')
{
    //获取网站配置
    $web_config = \think\Db::name('webconfig')->where('web','web')->find();
    if($web_config['is_log'] == 1) {
        $data['operation_id'] = $operation_id;
```

CSDN @Faith--wangwang

34.请分析该网站的管理员用户的密码为

在对其源码进行分析的时候找到一段日志上面记录了 网站一些用户的密码和修改密码的日志。找到管理员的密码 security

```
2649 'content-length' => '92',
2650 'connection' => 'keep-alive',
2651 'host' => '192.168.110.113',
2652 )
2653 [ info ] [ PARAM ] array (
2654     'name' => 'admin',
2655     'password' => 'security',
2656     'captcha' => 'yysv',
2657     '__token__' => '6189b5e8b8e793da1dc184760452b847eae8a7f9',
2658 )
2659 [ info ] [ RUN ] app\admin\controller\Common->login[ /www/wwwroot/www.honglian7001/app/
2660 [ info ] [ SESSION ] INIT array (
2661     'id' => '',
2662     'var_session_id' => '',
2663     'prefix' => 'think',
2664     'type' => '',
2665     'auto_start' => true,
2666 )
2667 [ info ] [ LOG ] INIT File
```

CSDN @Faith--wangwang

35在对后台账号的密码加密处理过程中，后台一共计算几次哈希值

审计网站源码即可得到

计算了三次哈希值

```
@return string
*/
function password($password, $password_code='lshi4AsSURU0wWV')
{
    return md5(md5($password) . md5($password_code));
}

/**
 * 管理员操作日志
 * @param [type] $data [description]
 */
```

CSDN @Faith--wangwang

36.请统计，后台中，一共有多少条设备记录

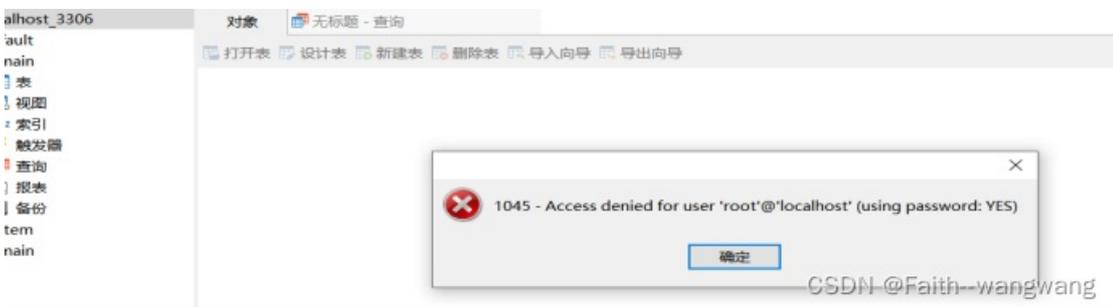
对网站进行重构后 连接其数据库

查看数据库开放端口相关信息

```
[root@localhost ~]# netstat -lnpt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1193/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1548/master
tcp6       0      0 :::22                  :::*                    LISTEN      1193/sshd
tcp6       0      0 :::1:25                 :::*                    LISTEN      1548/master
tcp6       0      0 :::3306                  :::*                    LISTEN      1473/mysqld
```

CSDN @Faith--wangwang

使用数据库管理工具进行连接 但是报错了



CSDN @Faith--wangwang

百度一下这个错误，找到了一个教程。

修改mysql的配置文件 绕过登录验证机制

找到其配置文件 /etc/my.conf 添加这段语句

```

# http://dev.mysql.com/doc/refman/5.6/en/server-configuration-defaults.html

0.08 [mysqld]
      skip-grant-tables
#
# Remove leading # and set to the amount of RAM for the most important data
# cache in MySQL. Start at 70% of total RAM for dedicated server, else 10%.
# innodb_buffer_pool_size = 128M
#
# Remove leading # to turn on a very important data integrity option: logging
# changes to the binary log between backups.
# log_bin
#
-- INSERT --

```

```

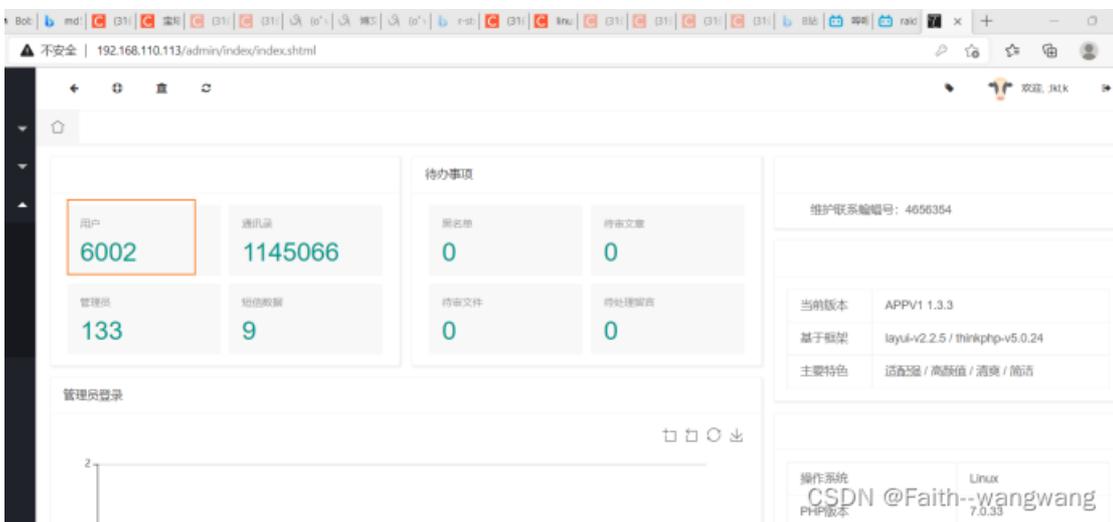
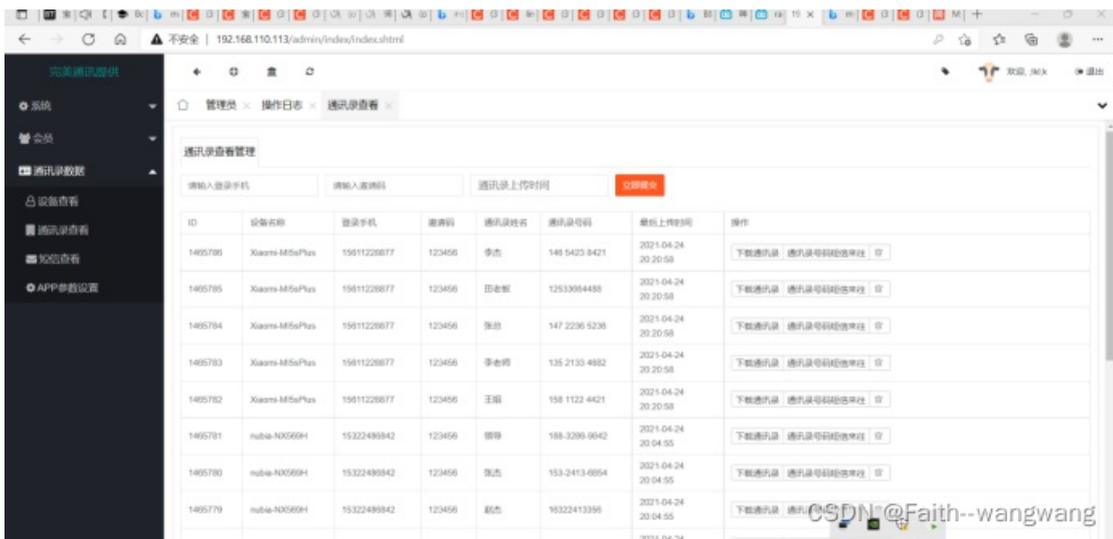
-bash: vim: 未找到命令
[root@localhost etc]# vi my.cnf
[root@localhost etc]# systemctl start mysqld
[root@localhost etc]#

```

更改完成之后保存更改

重新启动mysql再使用navicat即可连接到数据库

结合之前的密码成功进入网站后台



36.请通过后台确认，本案中受害者的手机号码为

这里要注意时区 检材二也就是负载均衡服务器是utc时区

后台数据库是utc+8时区

```
su. 正在以root身份运行
[ccj@localhost ~]$ su
密码:
[root@localhost ccj]# timedatectl
Local time: 四 2021-10-28 12:27:18 UTC
Universal time: 四 2021-10-28 12:27:18 UTC
RTC time: 四 2021-10-28 12:27:12
Time zone: UTC (UTC, +0000)
NTP enabled: yes
NTP synchronized: yes
RTC in local TZ: no
DST active: n/a
[root@localhost ccj]#
```

CSDN @Faith--wangwang

```
[root@localhost etc]# timedatectl
Local time: 四 2021-10-28 20:19:34 CST
Universal time: 四 2021-10-28 12:19:34 UTC
RTC time: 四 2021-10-28 12:19:34
Time zone: Asia/Shanghai (CST, +0800)
NTP enabled: yes
NTP synchronized: no
RTC in local TZ: no
DST active: n/a
[root@localhost etc]#
```

CSDN @Faith--wangwang

检材二中的日志记录情况

在2021.4.24 6:37 (utc时间) 左右上传了通讯录

```
2021-04-24 06:37:13.303 [WARN] Chronus - [Proxy_ClientIP] -> 192.168.110.252
2021-04-24 06:37:13.303 [WARN] Chronus - [Proxy_Destination] -> {"protocol":"http","host":"192.168.110.113","port":80}
2021-04-24 06:37:13.303 [WARN] Chronus - [Proxy_RequestHeader] -> {"protocol":"http","host":"192.168.110.113","port":80}
2021-04-24 06:37:13.303 [WARN] Chronus - [Proxy_ClientIP] -> 192.168.110.252
2021-04-24 06:37:13.304 [WARN] Chronus - [Proxy_Destination] -> {"protocol":"http","host":"192.168.110.113","port":80}
2021-04-24 06:37:14.989 [WARN] Chronus - [Proxy_RequestHeader] -> {"protocol":"http","host":"192.168.110.252"}
2021-04-24 06:37:14.989 [WARN] Chronus - [Proxy_ClientIP] -> 192.168.110.252
2021-04-24 06:37:16.330 [WARN] Chronus - [Proxy_Destination] -> {"protocol":"http","host":"192.168.110.113","port":80}
2021-04-24 06:37:16.330 [WARN] Chronus - [Proxy_ClientIP] -> 192.168.110.252
2021-04-24 06:37:16.330 [WARN] Chronus - [Proxy_Destination] -> {"protocol":"http","host":"192.168.110.113","port":80}
2021-04-24 06:59:23.958 [WARN] Chronus - [Proxy_ClientIP] -> 192.168.110.203
```

CSDN @Faith--wangwang

其对应的utc+8时间应为 当日14:37左右手机型号也能对上 由此可以得到受害者手机号码 186644099137

1465774	vivo-vivoX9	18644099137	123456	舅舅	13999999999	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465773	vivo-vivoX9	18644099137	123456	妈	13866888888	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465772	vivo-vivoX9	18644099137	123456	爸	13888888888	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465771	vivo-vivoX9	18644099137	123456	李雪	13200112233	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465770	vivo-vivoX9	18644099137	123456	李九	13299001122	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465769	vivo-vivoX9	18644099137	123456	李八	13288990011	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465768	vivo-vivoX9	18644099137	123456	李七	13277889900	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管
1465767	vivo-vivoX9	18644099137	123456	李六	13266778899	2021-04-24 14:37:12	下载通讯录 通讯录号码短信来往 管

CSDN @Faith--wangwang

根据检材四嫌疑人的手机的聊天记录也可以发现



38.请分析, 本案中受害者的通讯录一共有多少条记录

过滤其对应号码的通讯录

一共有34条



检材四

39请计算检材四-PC的原始硬盘的SHA256值

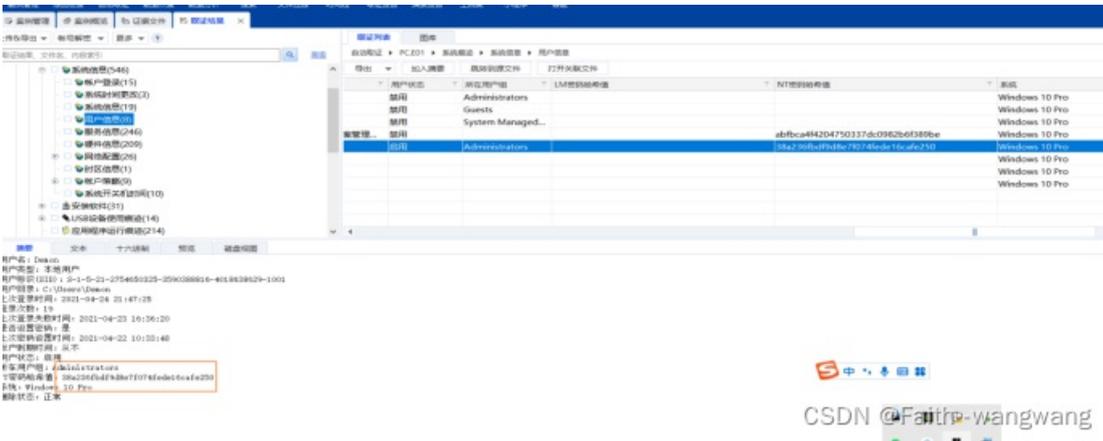
40请分析, 检材四-PC的Bitlocker加密分区的解密密钥为

取证大师自动分析 会找到Bitlocker加密的文件可以都看到其恢复密钥



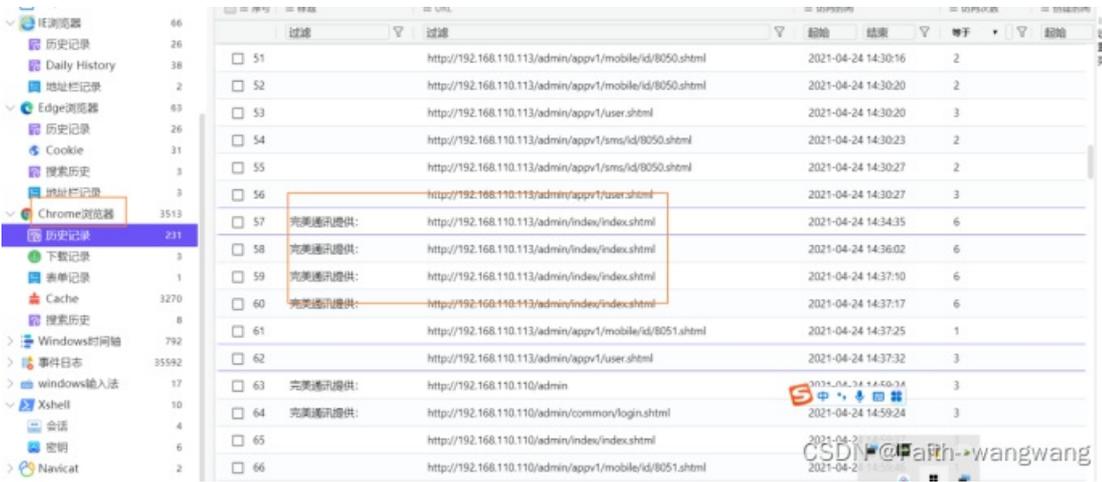
41请分析, 检材四-PC的开机密码为

找用户的nt哈希解密哈希



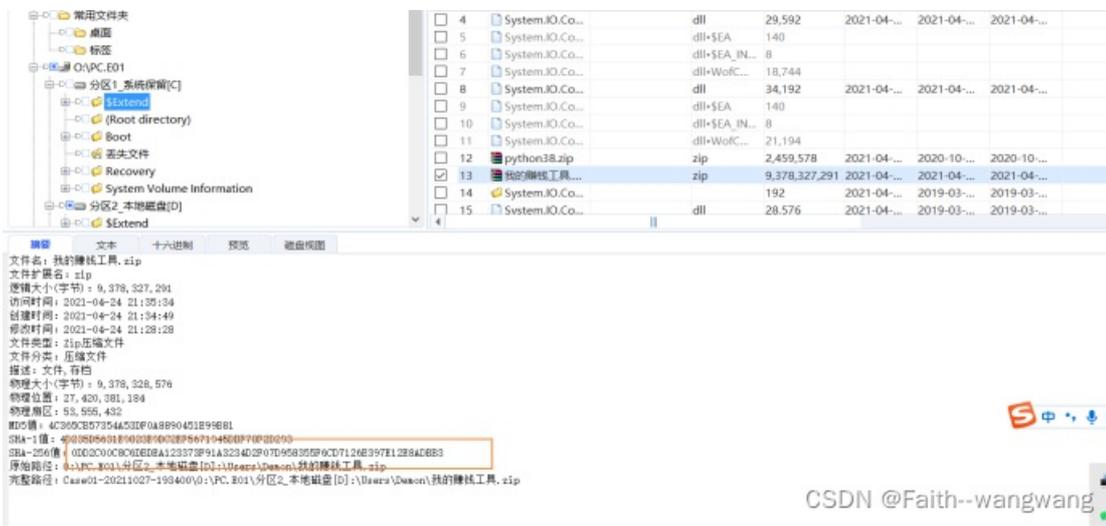
42.经分析发现, 检材四-PC是嫌疑人用于管理服务器的设备, 其主要通过哪个浏览器控制网站后

分析其浏览器记录 chrome

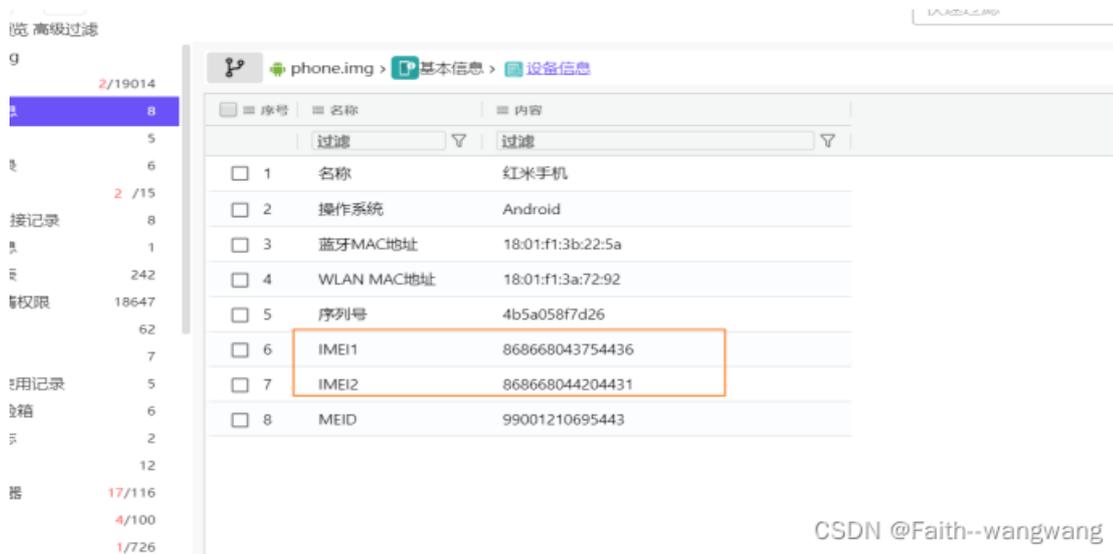


43.请计算PC检材中用户目录下的zip文件的sha256值

过滤zip文件 找到用户目录下的zip文件计算哈希值



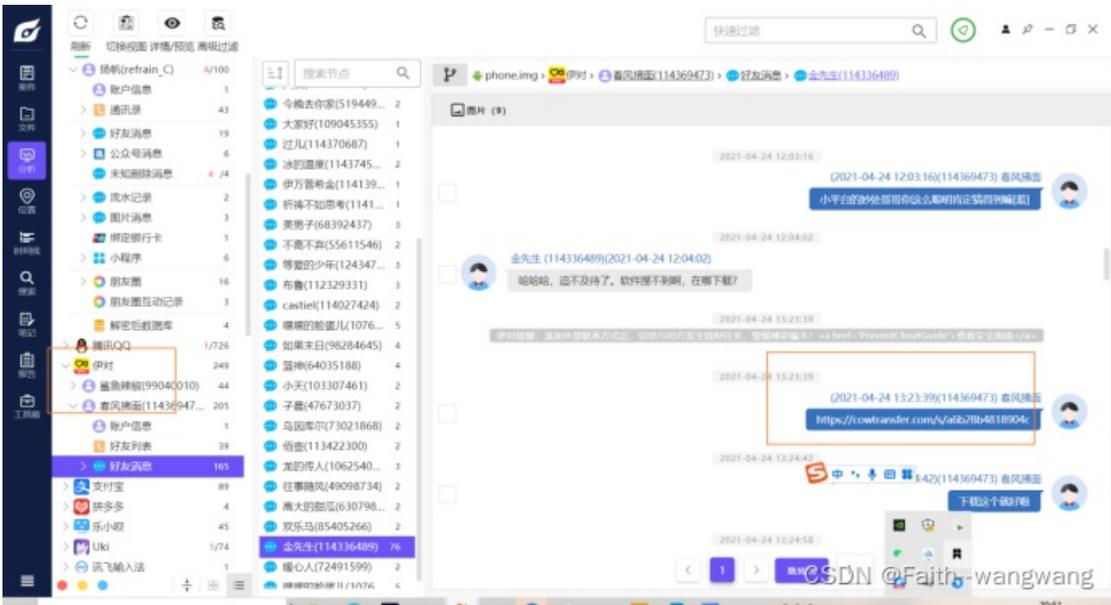
44.请分析检材四-phone，该手机的IMEI号为 两个均可



45请分析检材四-phone，嫌疑人和本案受害者是通过什么软件开始接触的【标准格式：支付宝

分析聊天软件的聊天记录即可找到

伊对

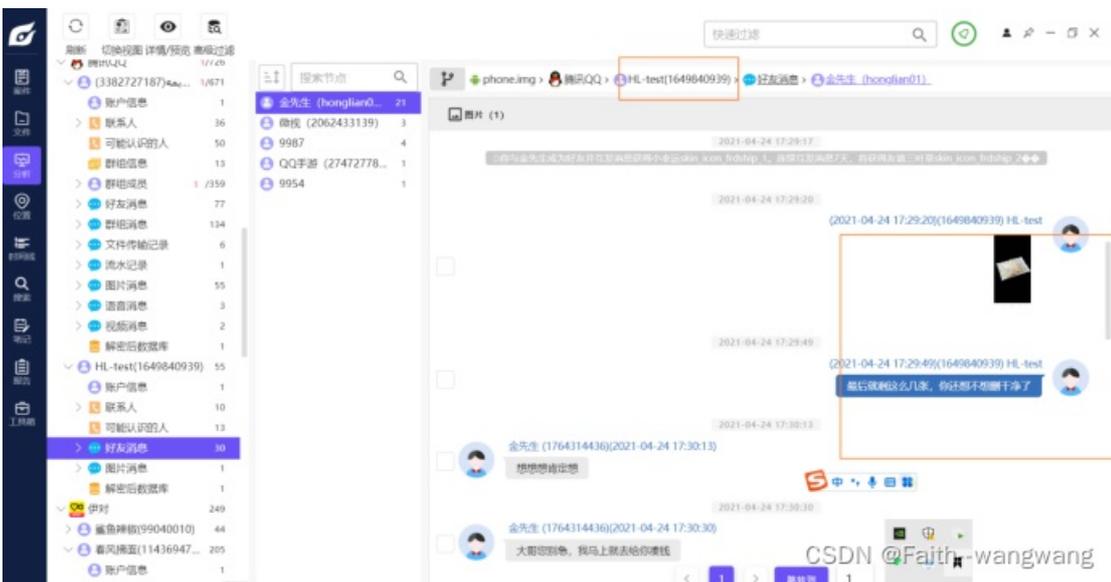


46.请分析检材四-phone, 受害者下载恶意APK安装包的地址为
接上题的图 该地址即为下载地址https://cowtransfer.com/s/a6b28b4818904c

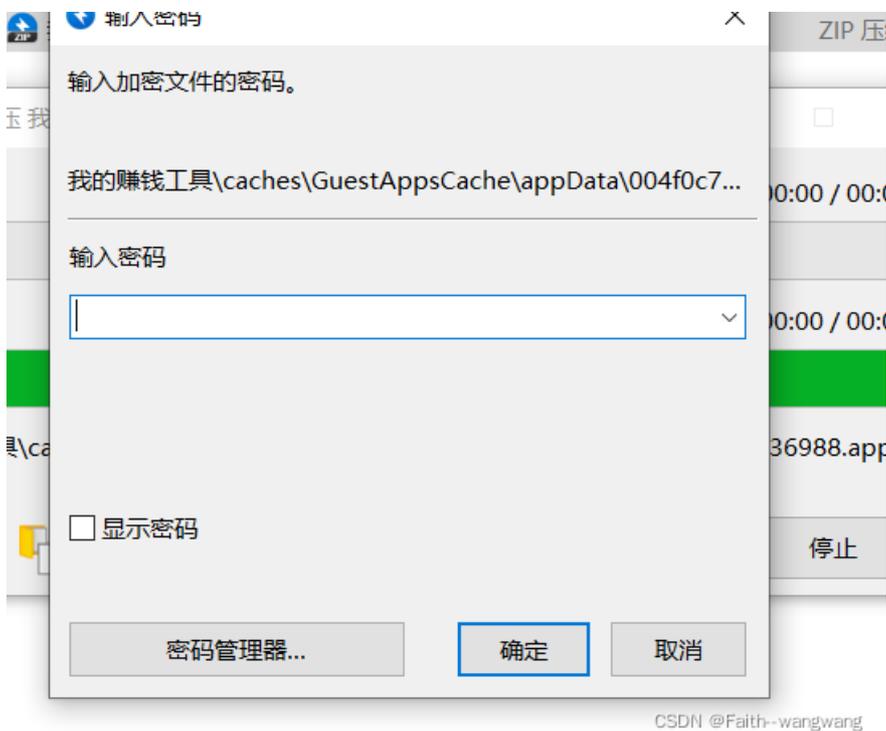
47.请分析检材四-phone, 受害者的微信内部ID号为
直接看微信信息即可



48.请分析检材四-phone, 嫌疑人用于敲诈本案受害者的QQ账号为
分析其聊天记录 1649840939

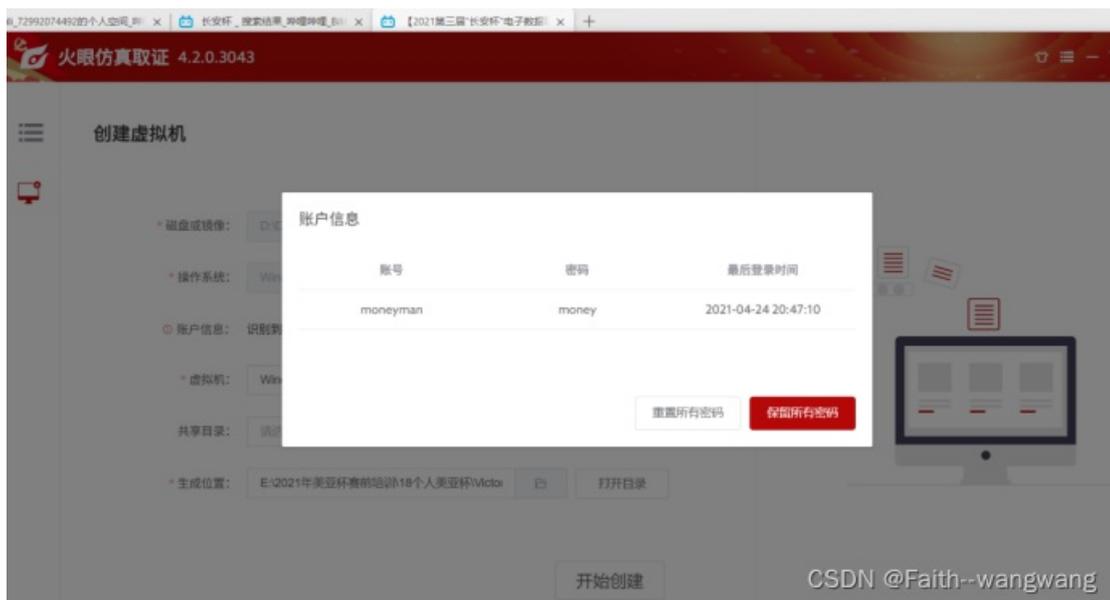


49.请综合分析, 嫌疑人用于管理敲诈对象的容器文件的SHA256值为



CSDN @Faith--wangwang

盲猜的zip密码为 电脑登录密码就解压了 猜不到可以爆破
使用仿真软件加载vmdk文件

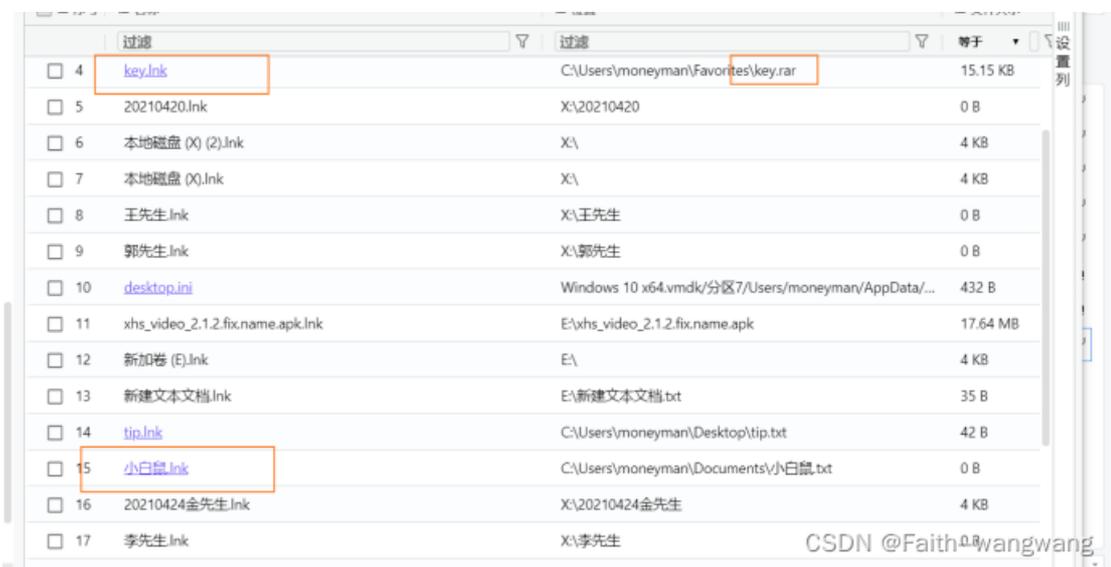


CSDN @Faith--wangwang

用vm直接打开虚拟机磁盘快照 用这个密码登录进去

进去之后没有发现任何东西 用证据分析软件进行分析发现了很多文件的使用痕迹。这里是虚拟机，虚拟机是可以进行快照的。查看快照设置发现有快照恢复到之前的快照进行分析。

查看其最近浏览的文件和使用的快捷方式等痕迹



这两个很特别 联想到 检材都是txt用vc挂载出来的推测可能是密钥容器

Key可能是密钥文件

后续挂载出来了 但是算不了哈希

50.请综合分析嫌疑人检材，另外一受害者“郭先生”的手机号码为

进入郭先生的文件夹

15266668888



51.通过嫌疑人检材，其中记录了几位受害者的信息

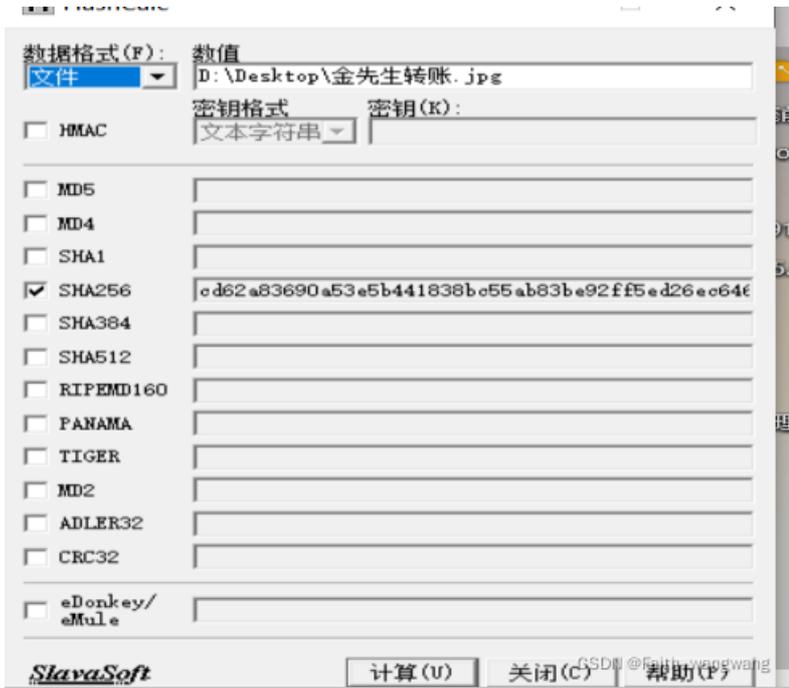
进入容器 发现了五位受害人的信息

邓先生	2021/4/24 19:04	文件夹
郭先生	2021/4/24 19:04	文件夹
秀先生	2021/4/24 19:04	文件夹
金先生	2021/4/24 15:08	文件夹
王先生	2021/4/24 19:04	文件夹

CSDN @Faith--wangwang

52.请使用第11题的密码解压“金先生转账.zip”文件，并对压缩包中的文件计算SHA256值
进入虚拟机中使用11题密码解压文件

导出文件后计算哈希值



53.请综合分析，受害者一共被嫌疑人敲诈了多少钱（转账截图被隐藏在多个地方）

6000 zip文件 微信转账记录 伊队聊天记录 数据库文件