[ctfshow 2021摆烂杯] FORENSICS部分 writeup

原创

shu天 于 2022-01-03 09:45:00 发布 466 收藏 1

分类专栏： # 内存取证 取证 # misc 文章标签： 取证 ctf misc 流量

本文链接：https://blog.csdn.net/weixin_46081055/article/details/122136547

内存取证 同时被 3 个专栏收录

6 篇文章 1 订阅

订阅专栏

取证

49 篇文章 4 订阅

订阅专栏

misc

7 篇文章 0 订阅

订阅专栏

[ctfshow 2021摆烂杯] FORENSICS部分 writeup

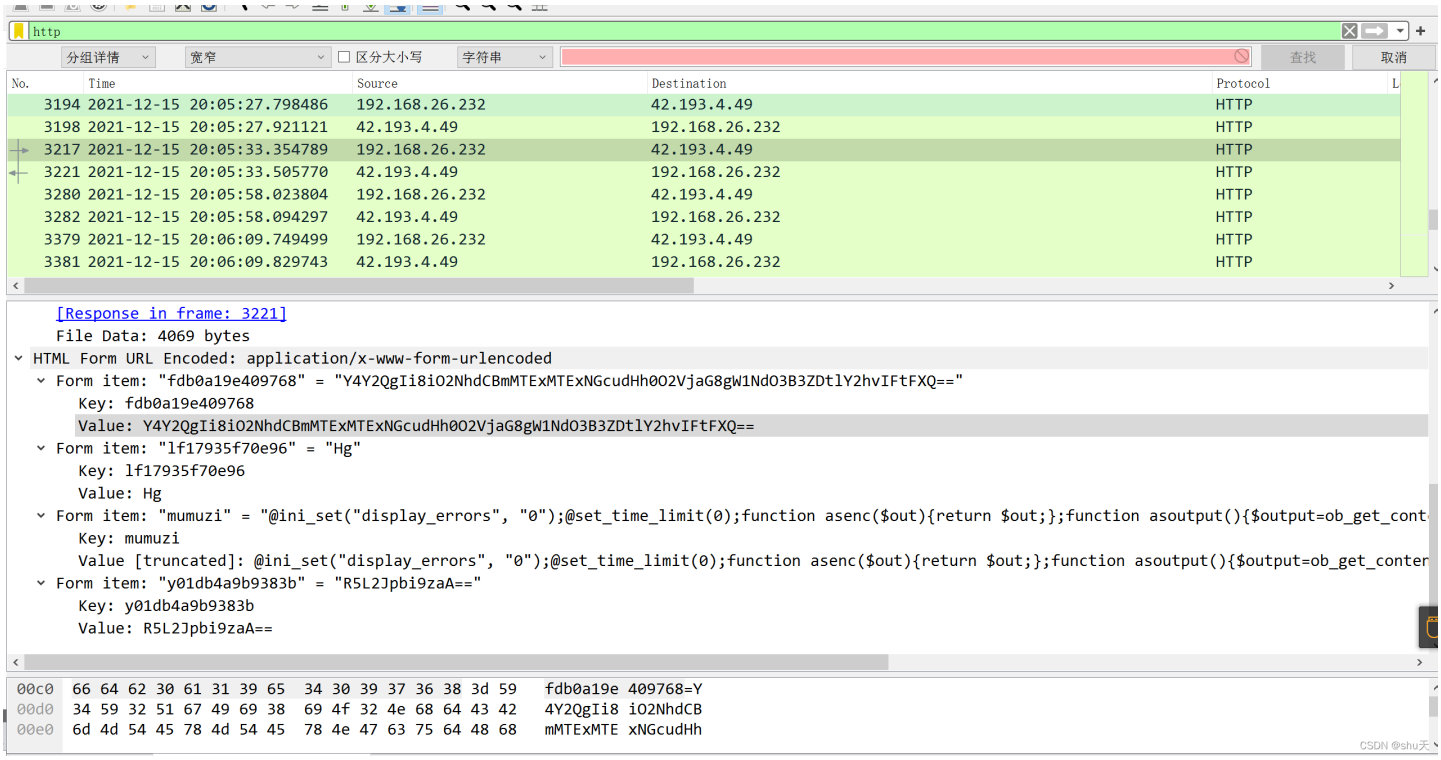
官方的wp：https://qgieod1s9b.feishu.cn/docs/doccnC4EpMhSv1Ni6mbL7BQQdBc

套的签到题

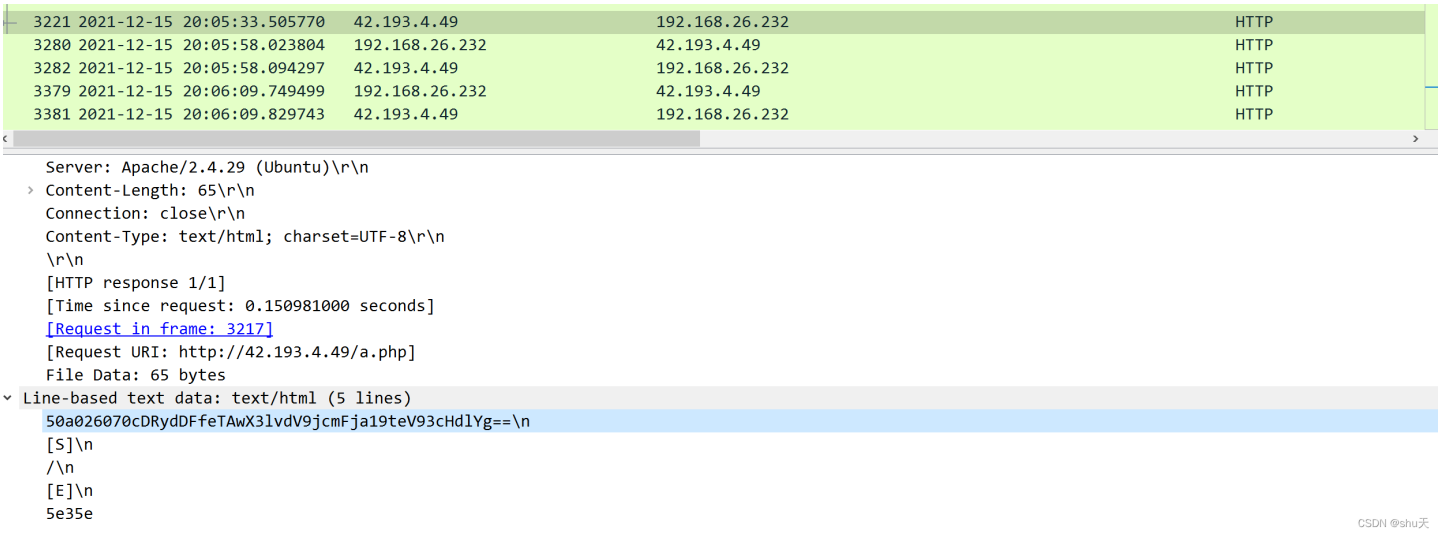
> 这是你沐师傅的站的流量，最近你沐师傅去跟着某讯搭了一个WP平台后发了一篇文章再测试了一下自己的网站就再也没去管过平台了。结果被某位名字貌似大概可能叫g4_simon的大黑阔给hack掉了网站，并进行了一些操作拿到了沐师傅放在平台里的信息。由于沐师傅说他摆烂了不想自己研究，于是将流量附件放了出来叫大家来帮忙找一找。 找到三段你觉得像flag的内容并用下划线组合，即ctfshow{A1_A2_A3}，找不到就算了，摆烂了。 如果交不上就算了，摆烂了 (其实签到题是PC1和CP1)

第一段flag

是个黑客入侵网站的流量包，首先`http.request.method==POST`，找到post的数据
黑客是通过蚁剑连接上传的木马，蚁剑命令执行的流量通过base64混淆，下图可以看到执行了cat /f1111114g.txt的命令，即为第一段的flag



response



50a026070cDRydDFfeTAwX3lvdV9jcmFja19teV93cHdlYg==\n
50a026070这九位也是蚁剑混淆返回包生成的，base解密时候要去除

p4rt1_y00_you_crack_my_wpweb

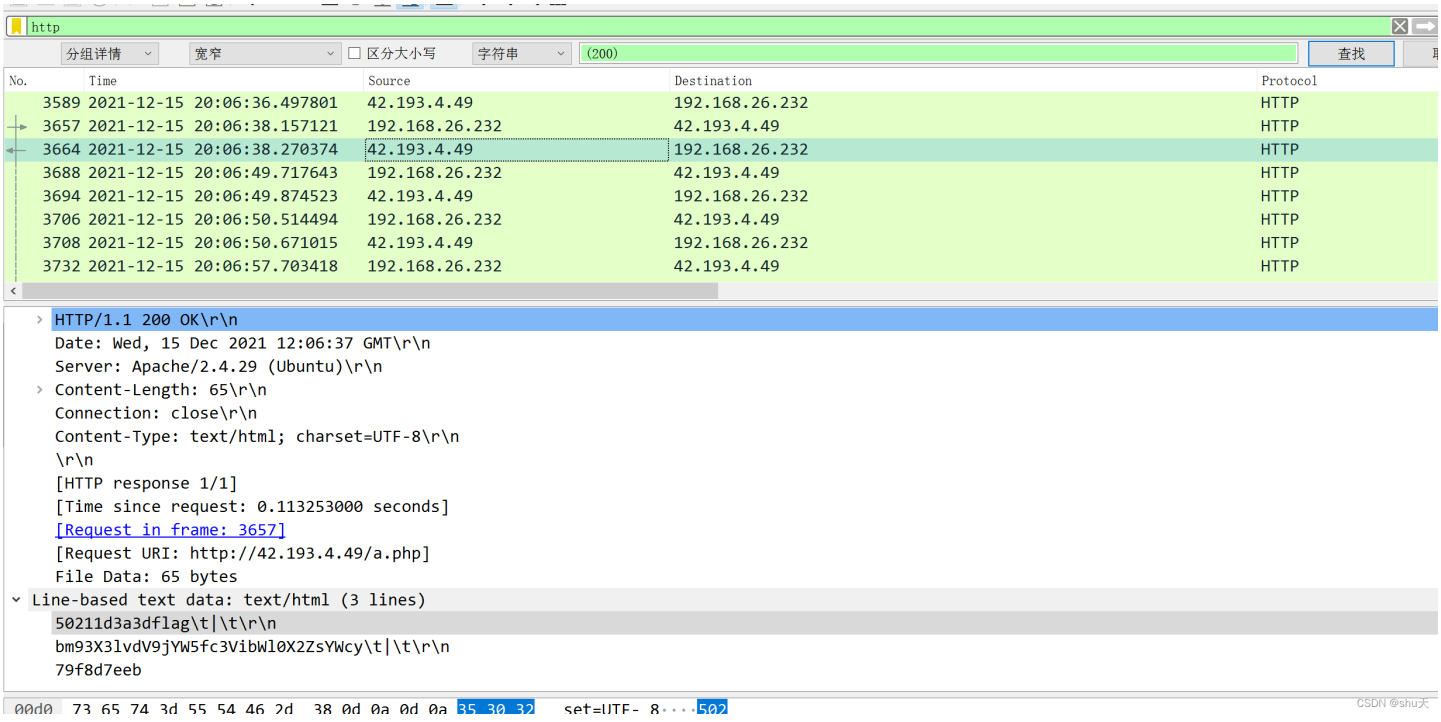
第二段flag

黑客对网站数据库进行爆破，flag在数据库里面

```
Transmission Control Protocol, Src Port: 80, Dst Port: 58438, Seq: 1, Ack: 1713, Len: 207
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 15 Dec 2021 12:06:35 GMT\r\n
    Server: Apache/2.4.29 (Ubuntu)\r\n
  > Content-Length: 40\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.112279000 seconds]
    [Request in frame: 3586]
    [Request URI: http://42.193.4.49/a.php]
    File Data: 40 bytes
Line-based text data: text/html (1 lines)
    68d137cf5flag (varchar(200))\t50449bc3fb5
```

```
0d0  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 36 38 64   set=UTF- 8····68d
0e0  31 33 37 63 66 35 66 6c  61 67 20 28 76 61 72 63   137cf5fl ag (varc
0f0  68 61 72 28 32 30 30 29  29 09 35 30 34 34 39 62   har(200) )·50449b
100  63 33 66 62 35                                     c3fb5
```

CSDN @shu天



CSDN @shu天

bm93X3lvdV9jYW5fc3VibWl0X2ZsYWcy

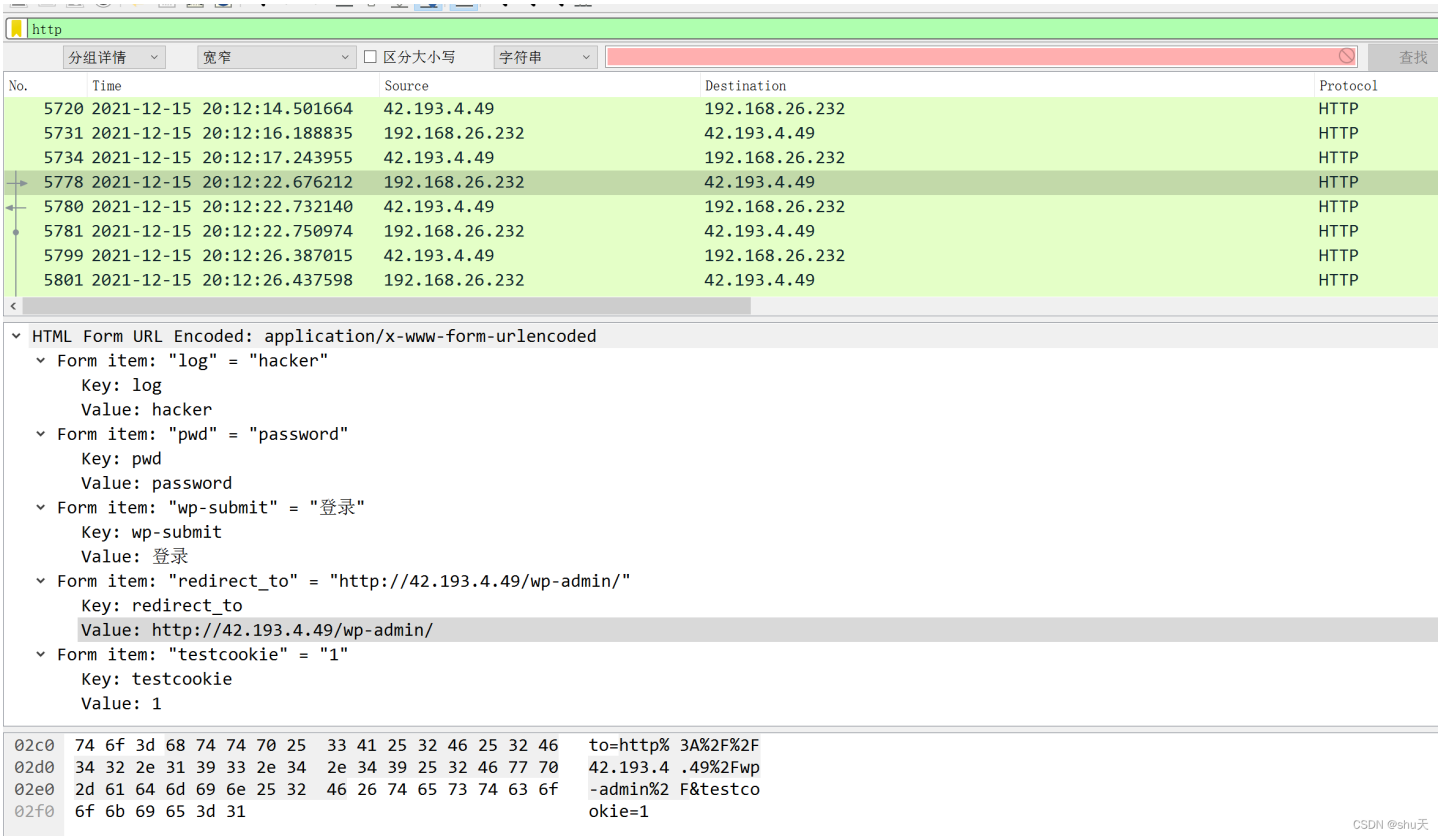
编码源格式：◉文本 ○Hex 解码结果： 自动检测 中文编码： UTF-8 编码 解码

now_you_can_submit_flag2

now_you_can_submit_flag2

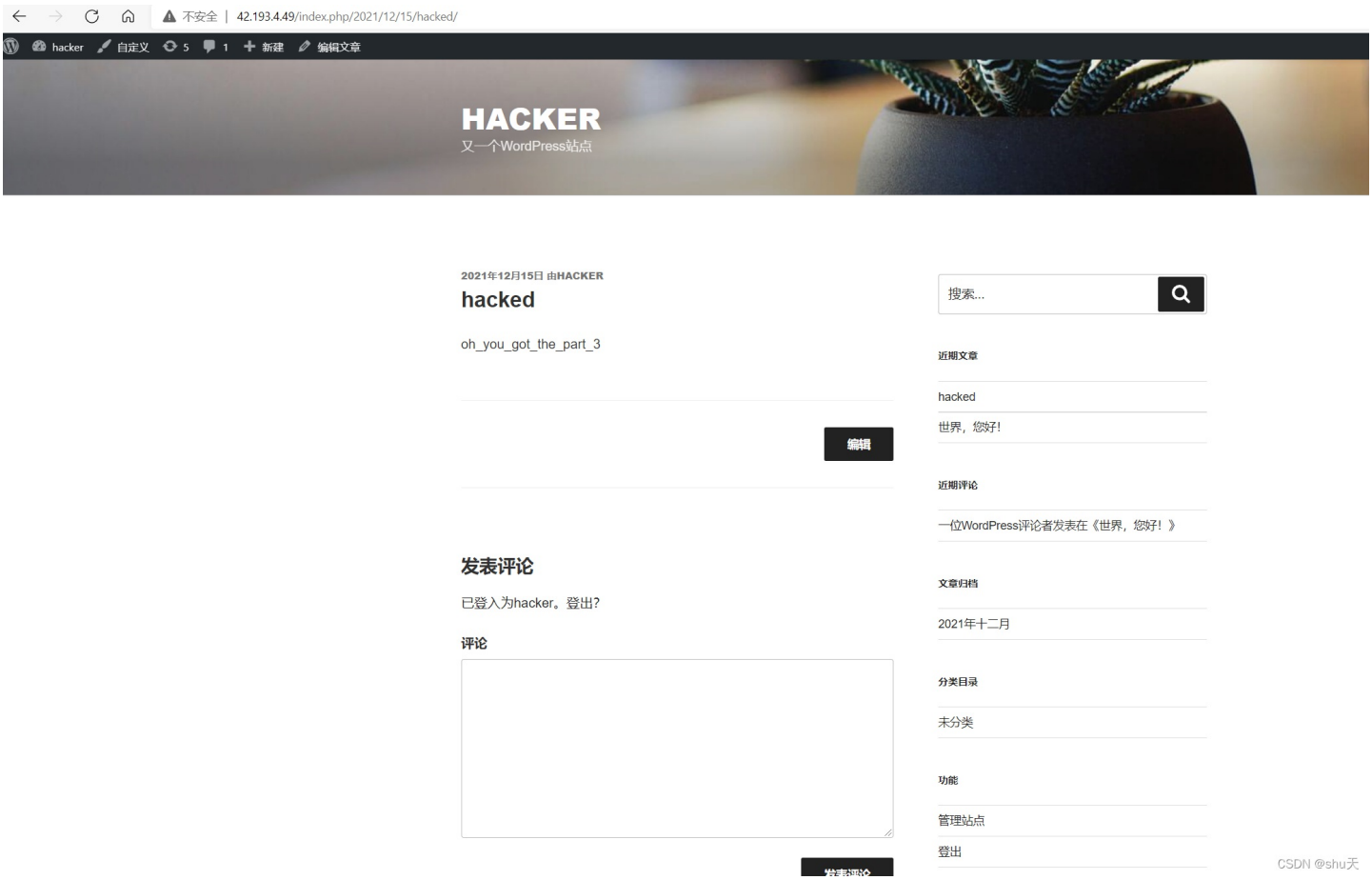
第三段flag

看到登陆密码



登陆进去看文章

第三段flag`oh_you_got_the_part_3`，是黑客发布的文章



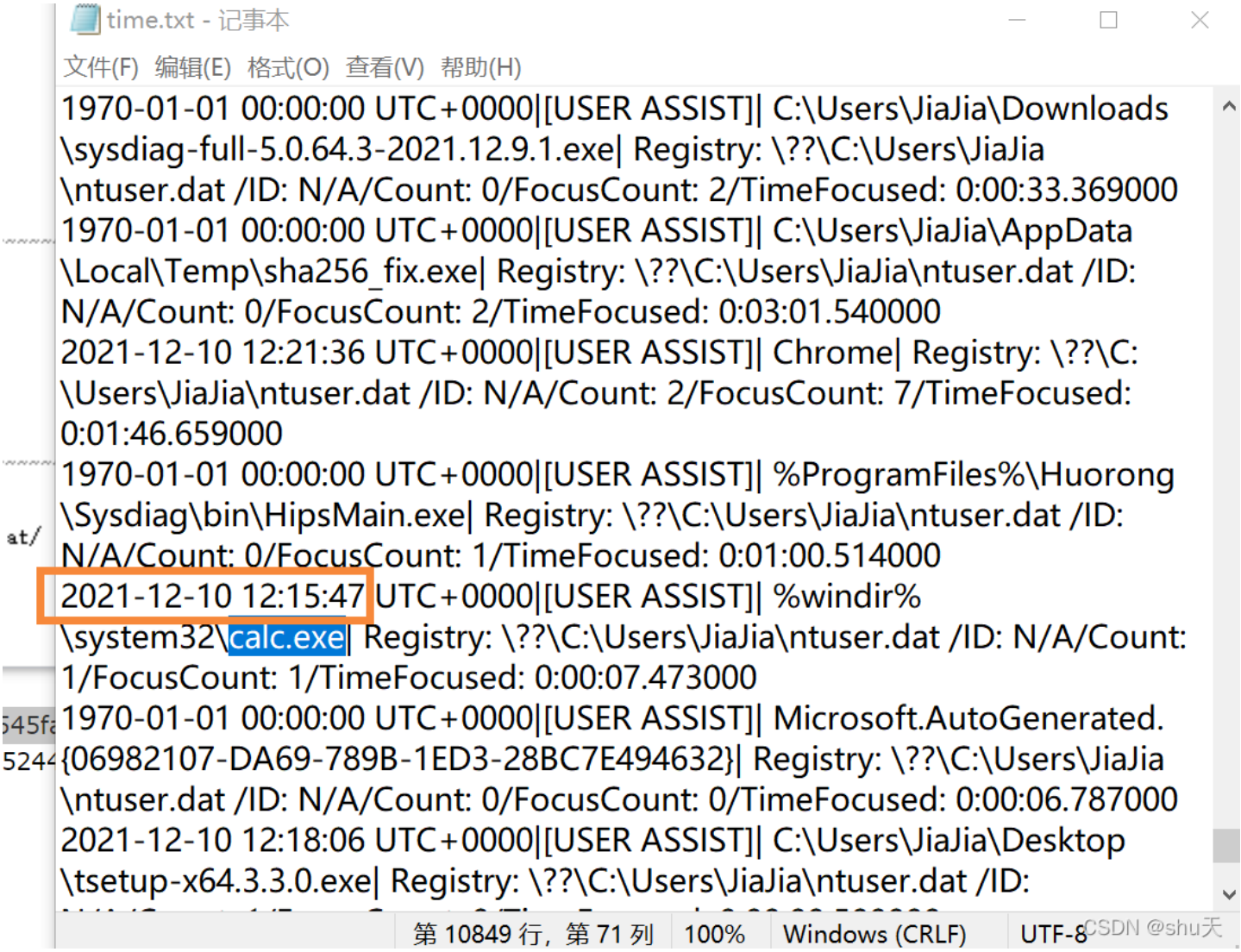
JiaJia-CP-1

这是部分人熟知的刘佳佳同学的电脑，她今年21岁已在公司里实习。但是佳佳经常摸鱼被老板训斥说：“你怎么摸得下去的”。因此佳佳还会经常将未完成的工作带到家里去完成(老板不留她加班属实有点离谱。但最近佳佳一天摸鱼的时间达到了25小时，这令老板非常不爽。于是□老板悄悄的植入了一个软件并在后台获取了佳佳电脑的内存信息。由于老板也是个懒□于是叫你来找一下老板想要的佳佳电脑的信息。作为十年老粉的CTFer们如果不是因为要找到flag一定不想帮老板来看佳佳的电脑内存信息吧，于是你也只能来帮助老板寻找佳佳电脑里的信息。电脑里面没有奇奇怪怪的东西，不要乱翻浪费时间
共3大题，第1大题做出来再给你第2大题和第3大题的题目，哼哼
1.佳佳的电脑用户名叫什么(即C:\Users{name})
2.最后一次运行计算器的时间？(格式为yyyy-mm-dd_hh:mm:ss，注意冒号为英文冒号)
flag格式为ctfshow{md5(A1_A2)}， format:ctfshow{ljj_2021-12-12_07:13:26}=ctfshow{c3cf135599d338093cbd2b578065be89}

filescan正常搜一些`\Users\`就可以找到用户名jiajia

```
0x000000013fdda070  16      0 R--r-- \Device\HarddiskVolume1\Users\JiaJia\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6025C34CC5B36C4156C40F3B0D99B6AB
```

timeliner就可以看到calc.exe(计算器)的运行时间（mftpraser也可以看到，但是哪个时间比较早）



要记得转换时区为东八区UTC+8

`JiaJia_2021-12-10_20:15:47`

ctfshow{079249e3fc743bc2d0789f224e451ffd}

JiaJia-CP-2

> 题目附件见JiaJia-CP-1
> 1.佳佳在公司使用了一款聊天软件，请问此软件的版本号为?
> 2.佳佳在网页上登录了自己的邮箱，请问佳佳的邮箱是？
> flag格式为ctfshow{md5(A1_A2)} format:ctfshow{12.0.7.14098_JiaJia2233@qq.com}=ctfshow{15e6abc2c9bf12cbd805e72a95e66291}

pslist没有看到聊天软件进程，timeliner搜一下桌面、文档等关键位置，发现使使用的应该是Telegram

```
λ cat time.txt |grep -i "desktop"
2020-03-30 22:13:25 UTC+0000|[PE HEADER (dll)]| desktopEvents.dll| Process: vmtoolsd.exe/PID: 2376/PPID: 3044/Process POffset: 0x13de9eb00/DLL Base: 0x7fef42f0000
2020-03-30 22:13:25 UTC+0000|[PE DEBUG]| desktopEvents.dll| Process: vmtoolsd.exe/PID: 2376/PPID: 3044/Process POffset: 0x13de9eb00/DLL Base: 0x7fef42f0000
2021-12-09 13:31:39 UTC+0000|[DLL LOADTIME (dll)]| desktopEvents.dll| Process: vmtoolsd.exe/PID: 2376/PPID: 3044/Process POffset: 0x13de9eb00/DLL Base: 0x7fef42f0000
2021-12-10 12:18:06 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Desktop\tsetup-x64.3.3.0.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:0
0.500000
2021-12-10 12:18:48 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\AppData\Roaming\Telegram Desktop\Telegram.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 1/FocusCount: 1/Ti
meFocused: 0:00:30.936000
2021-12-10 12:33:12 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Desktop\DumpIt.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 2/FocusCount: 1/TimeFocused: 0:01:29.874000
2021-12-10 12:18:48 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Desktop\Telegram.lnk| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.501000
```


导出文件

```
0x000000013fde26a0     16      0 RW---- \Device\HarddiskVolume1\Users\JiaJia\AppData\Roaming\Telegram Desktop\Te
legram.exe
```

```
λ volatility_2.6_win64_standalone.exe -f D:\download\新建文件夹\JiaJia_CP\JiaJia_Co.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000013fde26a0 -D ./ -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x13fde26a0   None   \Device\HarddiskVolume1\Users\JiaJia\AppData\Roaming\Telegram Desktop\Telegram.exe
DataSectionObject 0x13fde26a0   None   \Device\HarddiskVolume1\Users\JiaJia\AppData\Roaming\Telegram Desktop\Telegram.exe
```

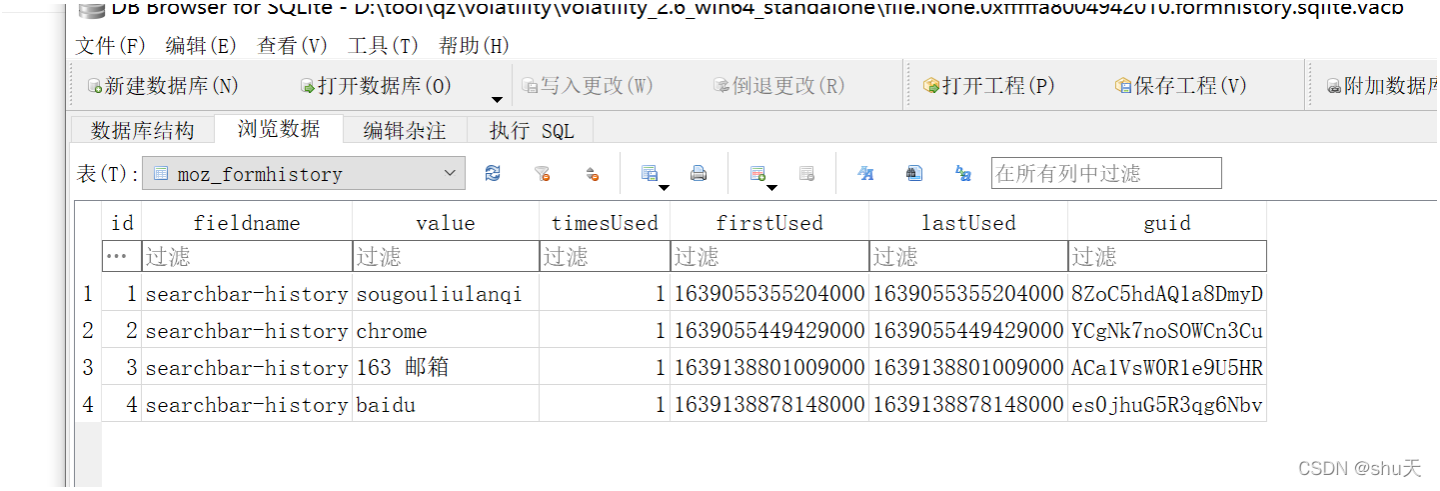
可以看到版本3.3.0.0

pslist可以看到firefox，推测是Firefox登陆邮箱的

```
0xfffffa80057b2890 wmpnetwk.exe          2780    484      9      215      0      0 2021-12-09 13:31:45 UTC+0000
0xfffffa80058ae060 svchost.exe           2976    484     16      287      0      0 2021-12-09 13:31:45 UTC+0000
0xfffffa80057b1060 svchost.exe            696    484     13      325      0      0 2021-12-09 13:32:54 UTC+0000
0xfffffa8004057b00 SogouCloud.exe        2612   2388     20      410      1      1 2021-12-09 13:34:31 UTC+0000
0xfffffa8004cc0b00 HipsTray.exe          2264   4012     12      281      1      1 2021-12-09 13:35:24 UTC+0000
0xfffffa8005e299a0 svchost.exe            972    484      4      108      0      0 2021-12-10 12:19:41 UTC+0000
0xfffffa8005f96060 firefox.exe           2136   2928     71     1157      1      0 2021-12-10 12:19:43 UTC+0000
0xfffffa800607e060 firefox.exe           4800   2136     37      332      1      0 2021-12-10 12:19:44 UTC+0000
0xfffffa8006030b00 firefox.exe           5076   2136     17      281      1      0 2021-12-10 12:19:45 UTC+0000
0xfffffa8006161060 firefox.exe           1064   2136     19      318      1      0 2021-12-10 12:19:45 UTC+0000
0xfffffa8006183b00 firefox.exe           3124   2136      8      175      1      0 2021-12-10 12:19:48 UTC+0000
0xfffffa8005ff7580 firefox.exe           4860   2136     18      294      1      0 2021-12-10 12:20:58 UTC+0000
0xfffffa8005d7e060 firefox.exe           2128   2136     16      269      1      0 2021-12-10 12:24:46 UTC+0000
0xfffffa800636cb00 firefox.exe            924   2136     16      270      1      0 2021-12-10 12:24:51 UTC+0000
0xfffffa80062a75b0 firefox.exe           4304   2136     16      272      1      0 2021-12-10 12:24:57 UTC+0000
0xfffffa8005b8eb00 HipsDaemon.exe        2352    484     37      356      0      1 2021-12-10 12:26:13 UTC+0000
0xfffffa8004891060 usysdiag.exe          4976   2352      7      100      0      0 2021-12-10 12:26:14 UTC+0000
0xfffffa8004891790 HipsTray.exe          4128   2352      0 --------      1      0 2021-12-10 12:26:15 UTC+0000   2021-12-10 12:26:16 UTC+0000
0xfffffa8005c166d0 HipsTray.exe          5028   2352      0 --------      1      0 2021-12-10 12:26:15 UTC+0000   2021-12-10 12:26:15 UTC+0000
0xfffffa8006328b00 audiodg.exe           3196    752      6      138      0      0 2021-12-10 12:29:58 UTC+0000
0xfffffa8005d47060 SearchProtocol        4312   2592      9      307      0      0 2021-12-10 12:33:00 UTC+0000
0xfffffa80063eeb00 SearchFilterHo        3348   2592      5       85      0      0 2021-12-10 12:33:01 UTC+0000
0xfffffa800646b8f0 DumpIt.exe            3396   3044      1       26      1      1 2021-12-10 12:33:12 UTC+0000
0xfffffa8005f569b0 conhost.exe           4244    396      6      224      1      0 2021-12-10 12:33:12 UTC+0000
```


然后导出formhistory.sqlite ，看看表单

> 自动完成历史: formhistory.sqlite 记录着你通过Firefox搜索框搜索的历史，以及你曾经在网站填写过的表单



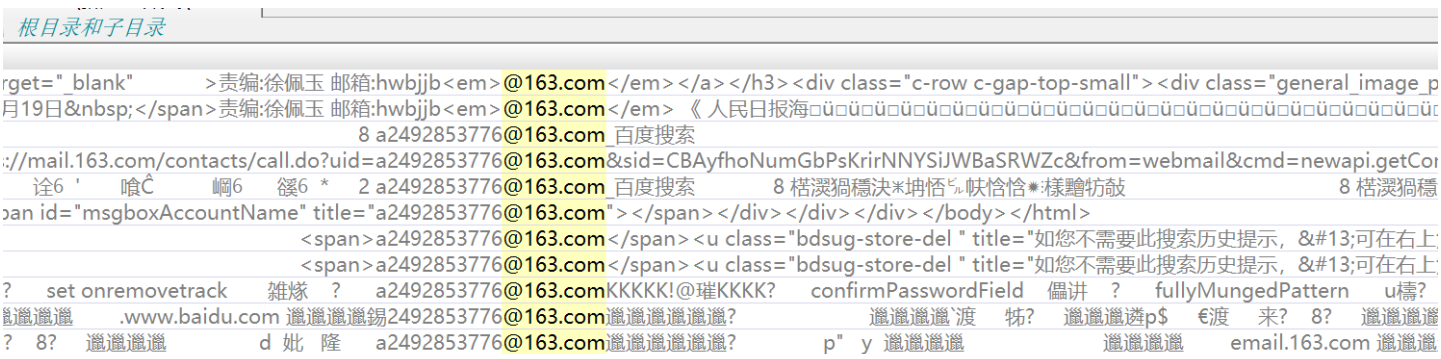
	id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
	…	过滤	过滤	过滤	过滤	过滤	过滤
1	1	searchbar-history	sougouliulanqi	1	1639055355204000	1639055355204000	8ZoC5hdAQ1a8DmyD
2	2	searchbar-history	chrome	1	1639055449429000	1639055449429000	YCgNk7noSOWCn3Cu
3	3	searchbar-history	163 邮箱	1	1639138801009000	1639138801009000	ACa1VsW0R1e9U5HR
4	4	searchbar-history	baidu	1	1639138878148000	1639138878148000	es0jhuG5R3qg6Nbv

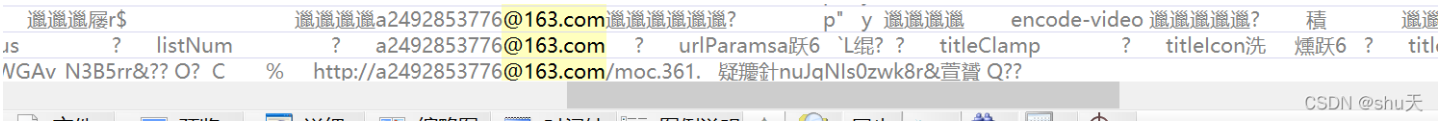
但是看了wp，是screenshot…

```
p3@p3-virtual-machine:~/lmg/volatility-master$ python vol.py -f "/home/p3/JiaJia_Co.raw" --profile=Win7SP1x64 scre
enshot -D ./2
Volatility Foundation Volatility Framework 2.6.1
```

不知道为啥没出来，因为上面表单也有163邮箱，全盘搜索163.com

`a2492853776@163.com`





估计这里是浏览网页的缓存，就像官方wp写得，title也缓存下来了

这里佳佳是在网页上登录的自己的邮箱，于是查看iehistory，但是呢并没有显示

这里使用screenshot,因为他登录了网页，网页的title很有可能会显示

```
Java
1  volatility -f JiaJia_Co.raw --profile=Win7SP1x64 screenshot -D ./
```

所以flag是3.3.0.0_a2492853776@163.com的md5值ctfshow{f1420b5294237f453b7cc0951014e45a}

JiaJia-CP-3

> 题目附件见JiaJia-CP-1
> 1.佳佳最后一次运行固定在任务栏的google chrome的时间(格式为yyyy-mm-dd_hh:mm:ss，注意冒号为英文冒号)
> 2.佳佳解压了从chrome下载了一个压缩文件，此文件的相关内容信息已经写入了到环境中，请问文件的内容是？
> flag格式为ctfshow{md5(A1_A2)} format:ctfshow{2021-12-12_19:18:57_this-is-your-part2}=ctfshow{91b8135bc98486fa898330aafac9afd1}

依旧是看timeliner

> WIN7中，任务栏上“已固定”文件的快捷方式（.lnk文件）保存在 `C:\Users\用户名\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar` 下

访问时间2021-12-10 12:21:36 UTC+0000

2021-12-10_20:21:36

```
Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 4/FocusCount: 0/TimeFocused: 0:00:00.504000
2021-12-10 12:15:47 UTC+0000|[USER ASSIST]| %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories
\Calculator.lnk| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.501000
2021-12-10 12:21:36 UTC+0000|[USER ASSIST]| %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Google
Chrome.lnk| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 2/FocusCount: 0/TimeFocused: 0:00:00.502000
2021-12-10 12:18:48 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Desktop\Telegram.lnk| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID:
N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.501000
2021-12-10 12:32:54 UTC+0000|[USER ASSIST]| %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows
```


但是wp里面是看的注册表，所以是2021-12-10_20:28:43

```
\JiaJia\ntuser.dat /ID: N/A/Count: 1/FocusCount: 1/TimeFocused: 0:00:30.936000
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| %windir%\system32\SystemPropertiesAdvanced.exe| Registry: \??\C:\Users\JiaJia
\ntuser.dat /ID: N/A/Count: 0/FocusCount: 1/TimeFocused: 0:00:04.931000
2021-12-10 12:28:43 UTC+0000|[USER ASSIST]| {6D809377-6AF0-444B-8957-A3773F02200E}\Google\Chrome\Application\chrome.exe|
Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count: 2/FocusCount: 0/TimeFocused: 0:00:00.500000
2021-12-10 12:33:12 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Desktop\DumpIt.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID:
N/A/Count: 2/FocusCount: 1/TimeFocused: 0:01:29.874000
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| Microsoft.Windows.PhotoViewer| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count:
```


写入了到环境中！原来是要看进程环境变量(envars)

压缩包是part2.rar

```
0x000000013dbf1a80      2      0 RW-rwd \Device\HarddiskVolume1\Users\JiaJia\Downloads\part2.rar
0x000000013dbf1d90      2      1 ------ \Device\NamedPipe\chrome.2136.39.16668622
```

```
3396 DumpIt.exe          0x00000000000f1320 PROCESSOR_LEVEL              23
3396 DumpIt.exe          0x00000000000f1320 PROCESSOR_REVISION           6001
3396 DumpIt.exe          0x00000000000f1320 ProgramData                  C:\ProgramData
3396 DumpIt.exe          0x00000000000f1320 ProgramFiles                 C:\Program Files
3396 DumpIt.exe          0x00000000000f1320 ProgramFiles(x86)            C:\Program Files (x86)
3396 DumpIt.exe          0x00000000000f1320 ProgramW6432                 C:\Program Files
3396 DumpIt.exe          0x00000000000f1320 PSModulePath                 C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
3396 DumpIt.exe          0x00000000000f1320 PUBLIC                       C:\Users\Public
3396 DumpIt.exe          0x00000000000f1320 rAR                          Th1s_i5_Ur_P5wd
3396 DumpIt.exe          0x00000000000f1320 SystemDrive                  C:
3396 DumpIt.exe          0x00000000000f1320 SystemRoot                   C:\Windows
3396 DumpIt.exe          0x00000000000f1320 TEMP                         C:\Users\JiaJia\AppData\Local\Temp
3396 DumpIt.exe          0x00000000000f1320 TMP                          C:\Users\JiaJia\AppData\Local\Temp
3396 DumpIt.exe          0x00000000000f1320 USERDOMAIN                   WIN-IDESST98JIC
3396 DumpIt.exe          0x00000000000f1320 USERNAME                     JiaJia
3396 DumpIt.exe          0x00000000000f1320 USERPROFILE                  C:\Users\JiaJia
3396 DumpIt.exe          0x00000000000f1320 windir                       C:\Windows
3396 DumpIt.exe          0x00000000000f1320 windows_tracing_flags        3
3396 DumpIt.exe          0x00000000000f1320 windows_tracing_logfile      C:\BVTBin\Tests\installpackage\csilogfile.log
4244 conhost.exe         0x00000000002e2ae0 CommonProgramFiles           C:\Program Files\Common Files
4244 conhost.exe         0x00000000002e2ae0 CommonProgramFiles(x86)      C:\Program Files (x86)\Common Files
4244 conhost.exe         0x00000000002e2ae0 CommonProgramW6432           C:\Program Files\Common Files
4244 conhost.exe         0x00000000002e2ae0 ComSpec                      C:\Windows\system32\cmd.exe
4244 conhost.exe         0x00000000002e2ae0 FP_NO_HOST_CHECK             NO
```


flag为2021-12-10_20:28:43_Th1s_i5_Ur_P5wd的md5值ctfshow{6430ef3578f7e1206506995cae3d2c24}

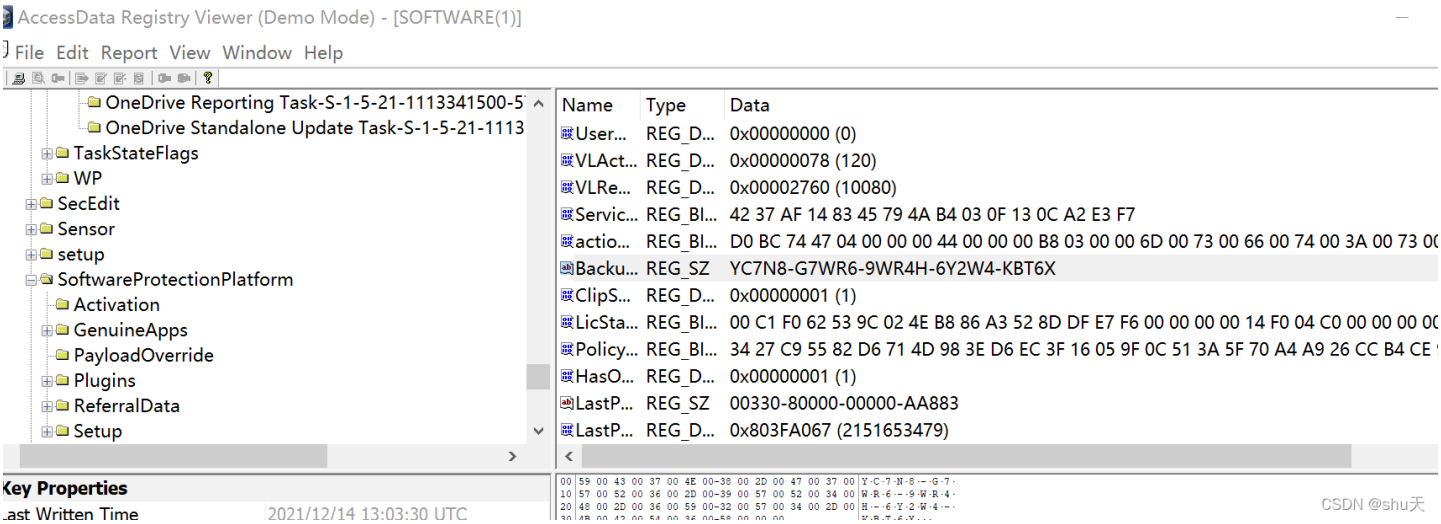
JiaJia-PC-1

仿真和不仿真的方法一起做了

刚刚在佳佳公司电脑那里提到，佳佳从公司带了一些电脑资料在家里继续加班完成因为摸鱼而没有完成的工作任务，本以为佳佳她会在家里稍微勤奋那么一neinei，没想到佳佳直接快进到找别人完成任务。好巧不巧这个人就是老板本板，希望佳佳人没事。佳佳因为找别人完成任务，因此让别人连上了自己的PC之后就直接跑去床上躺着了，并不知道这个□老板往佳佳电脑里面放了一个神奇的软件并用此软件提取了整个电脑磁盘，再通过该远程传输传输到了老板的电脑上，当我们发现这个信息的时候老板已经在包吃包住的好地方呆着了。但还是请你帮忙找一找这个□老板想要获取到的信息，说不定下一个包吃包住还能免费cosplay的幸运儿就是你。
1.产品秘钥（卷影）
2.windows系统版本号
ctfshow{md5(A1_A2)}
format:ctfshow{md5(NPPR9-FWDCX-D2C8J-H872K-2YT43_20H2)}=ctfshow{bc536cad5a7853d94d0298289d0c47cd}

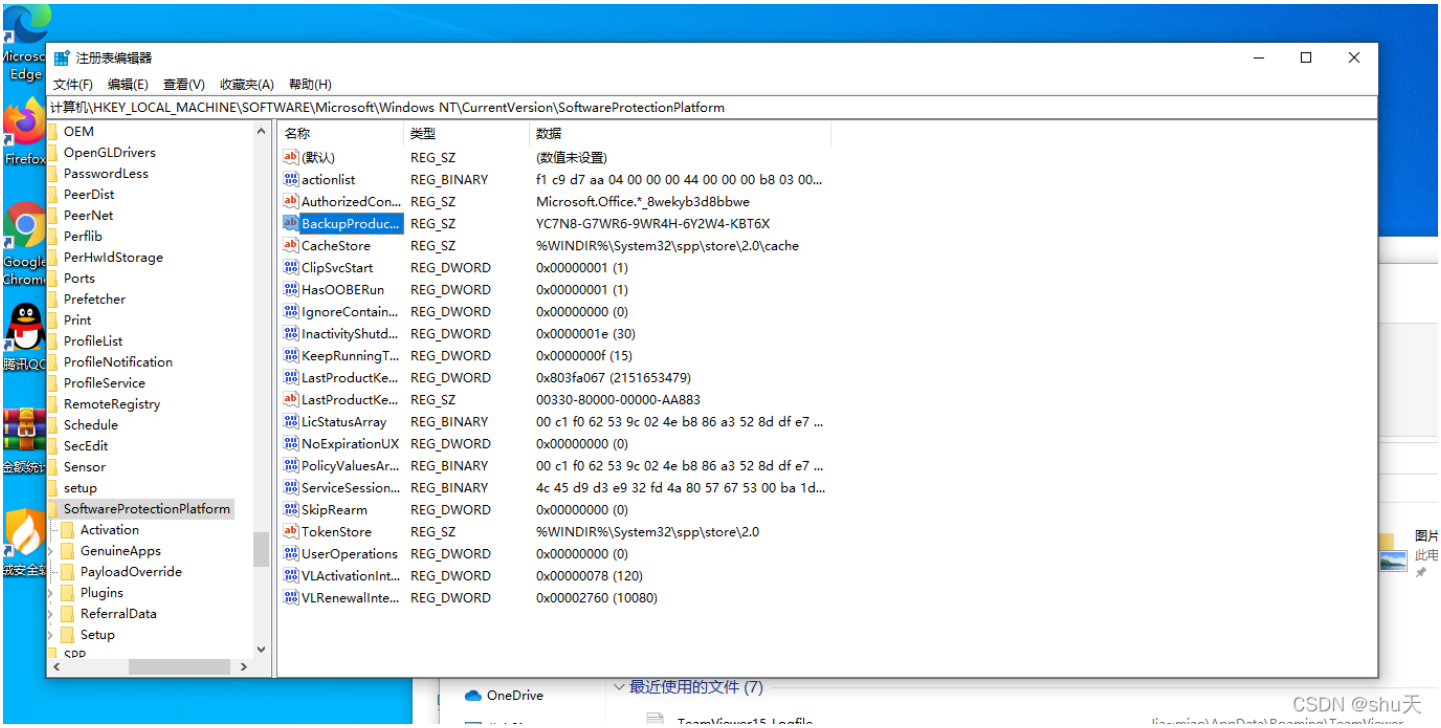
1.产品秘钥（卷影）

产品密钥要看 `卷影备份中software注册表` 里的密钥



仿真查看：

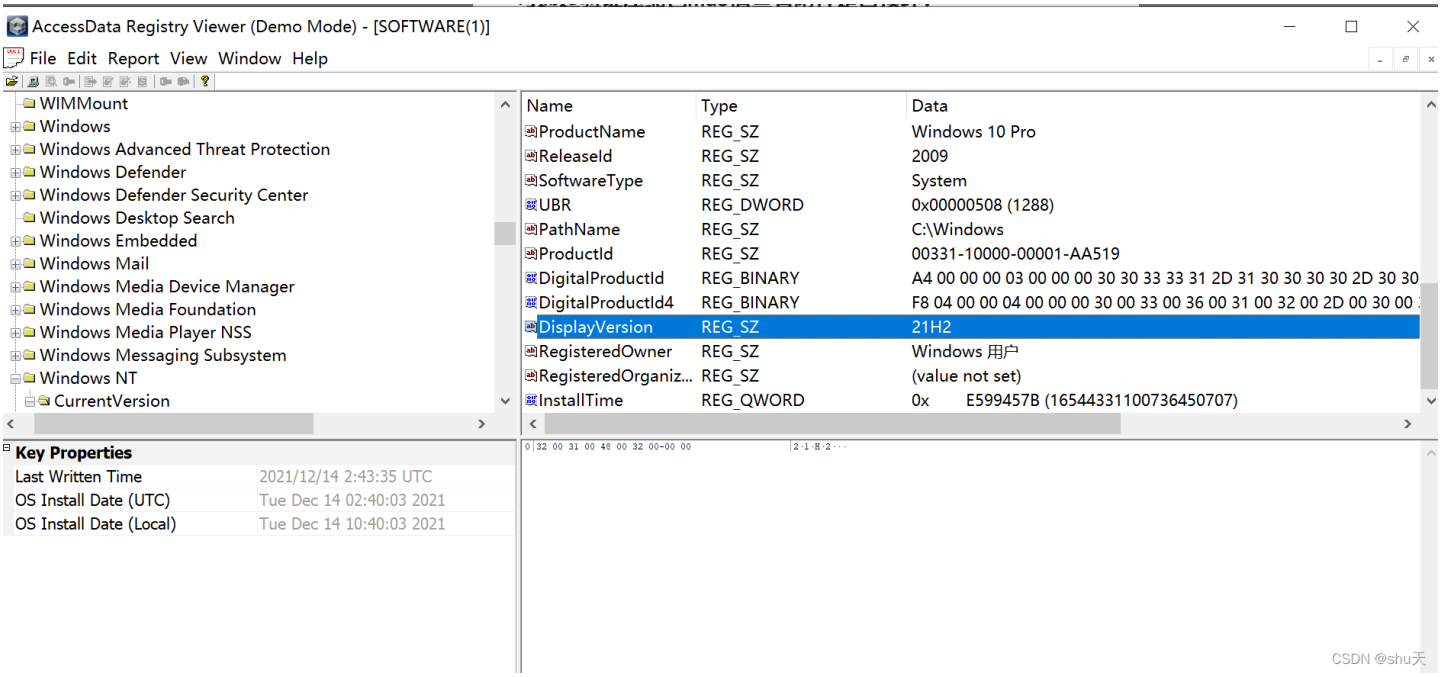
Win + R 运行 Regedit 打开注册表编辑器
找到：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform右侧的 BackupProductKeyDefault 值就是你的「备份产品密钥」



2.windows系统版本号

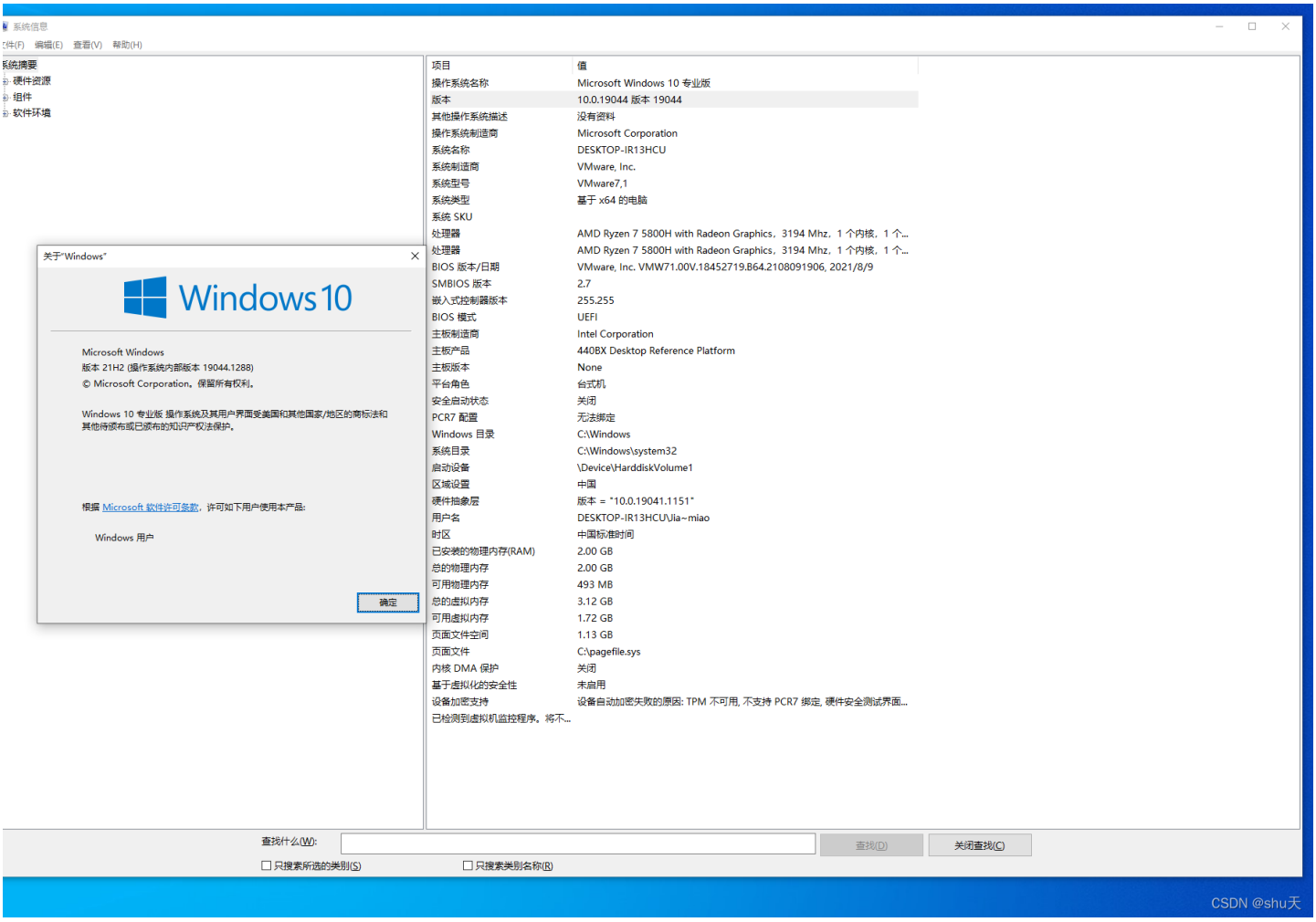
版本信息是详细版本信息 displayversion

> 查看你的Windows 10的详细版本号：定位到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion”，然后看右栏“BuildLabEx”即可看到详细的版本信息



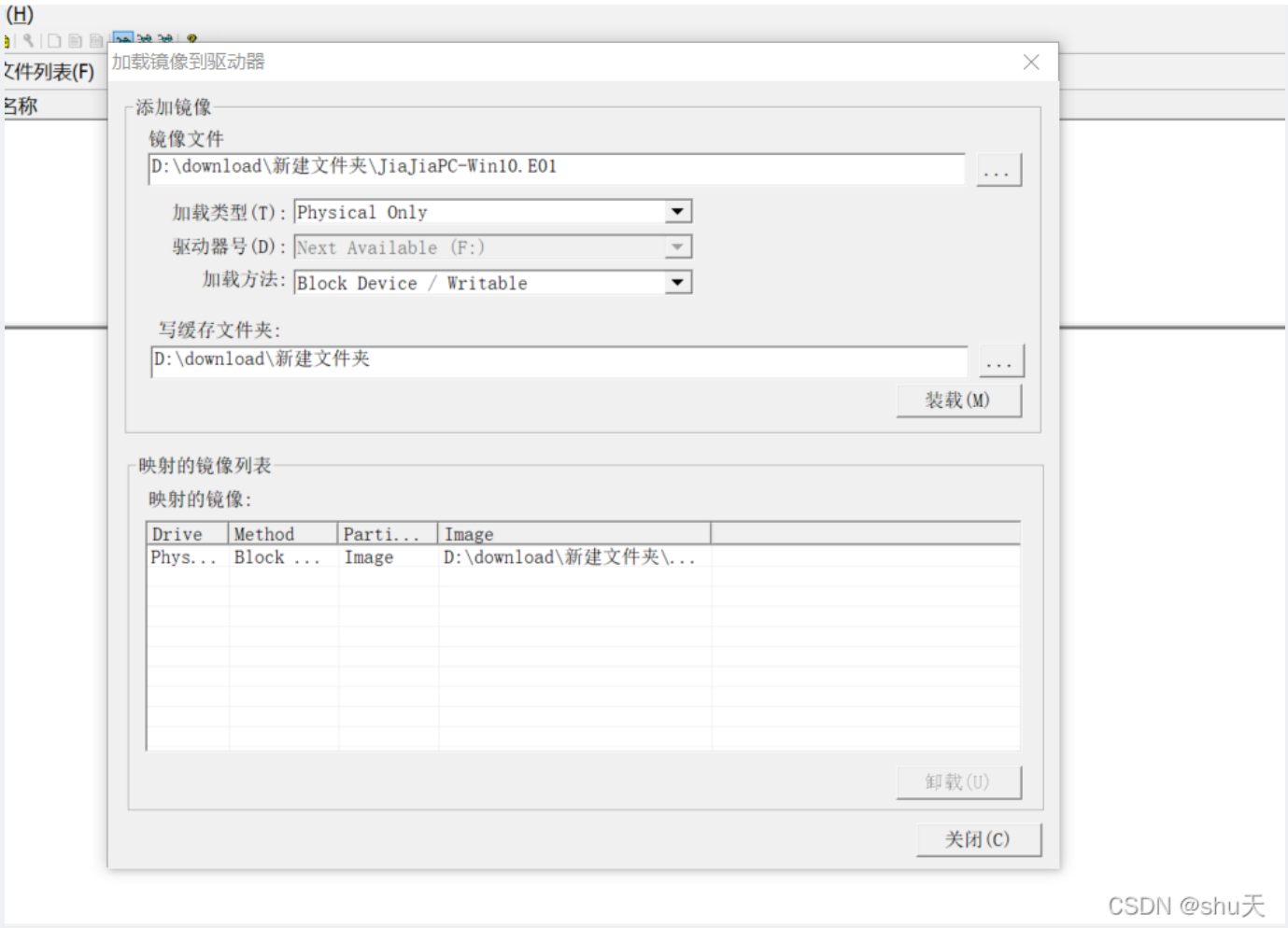
仿真：

win+R,输入winver

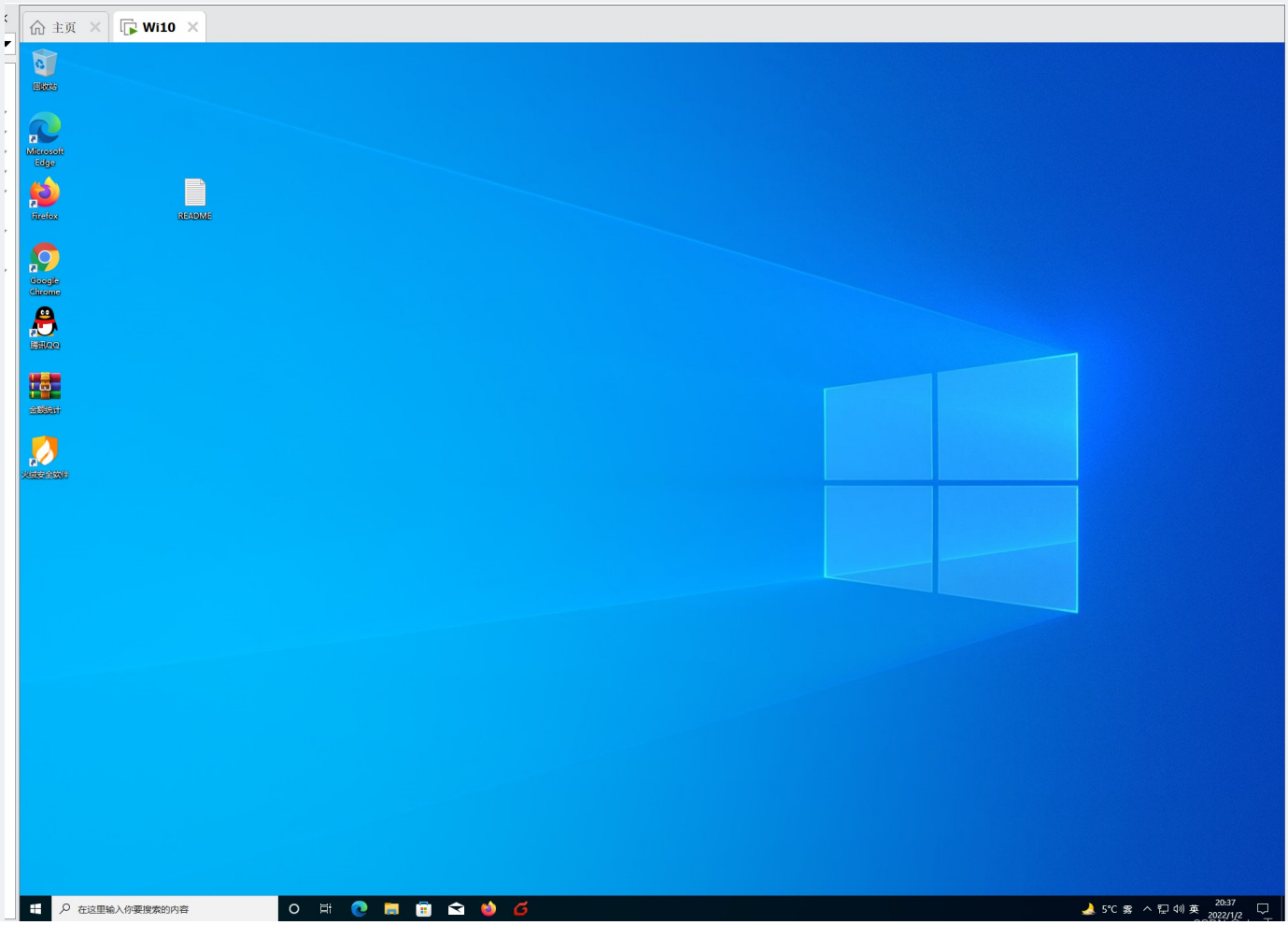


flag即YC7N8-G7WR6-9WR4H-6Y2W4-KBT6X_21H2的md5值

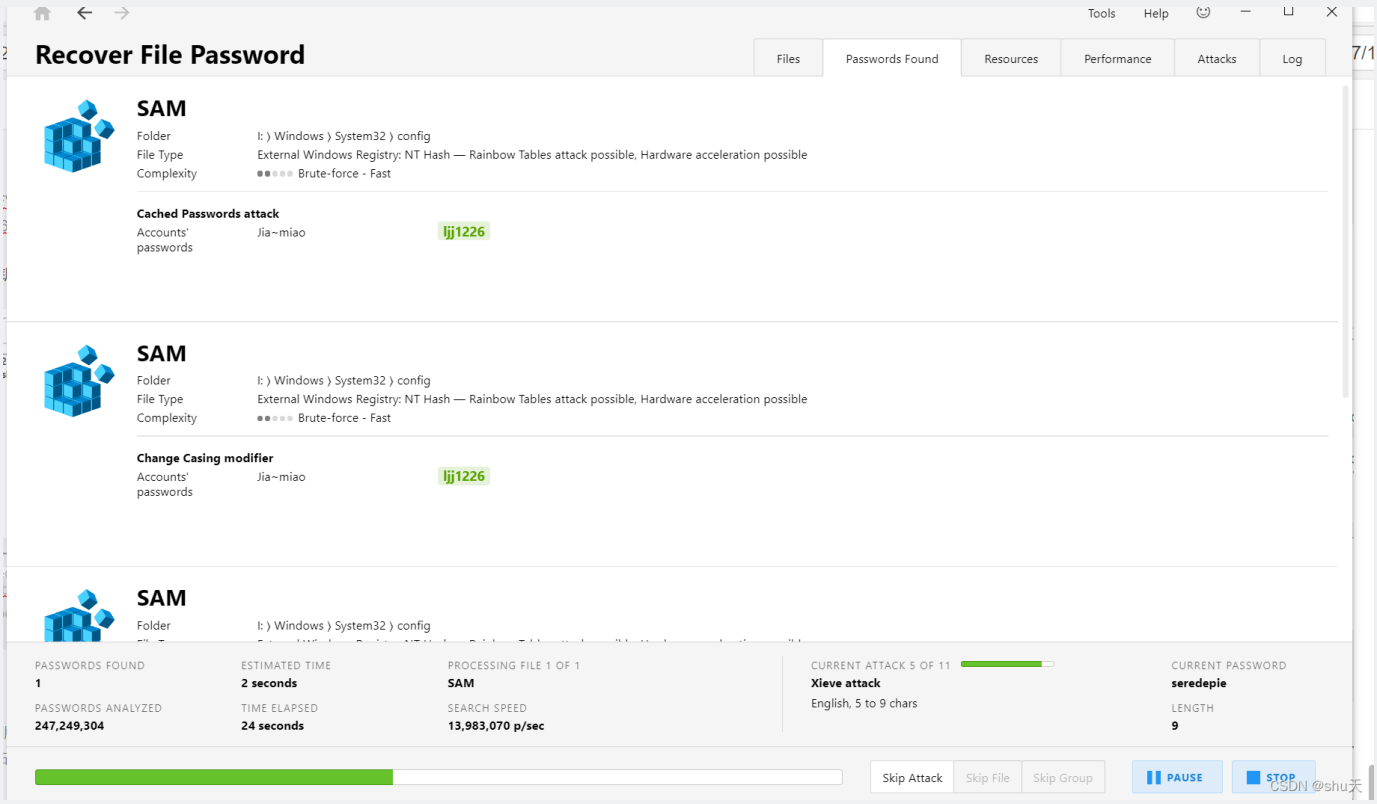
> ps仿真过程



然后磁盘附加上就进来了！



密码可以用passwarekit爆破sam表密码



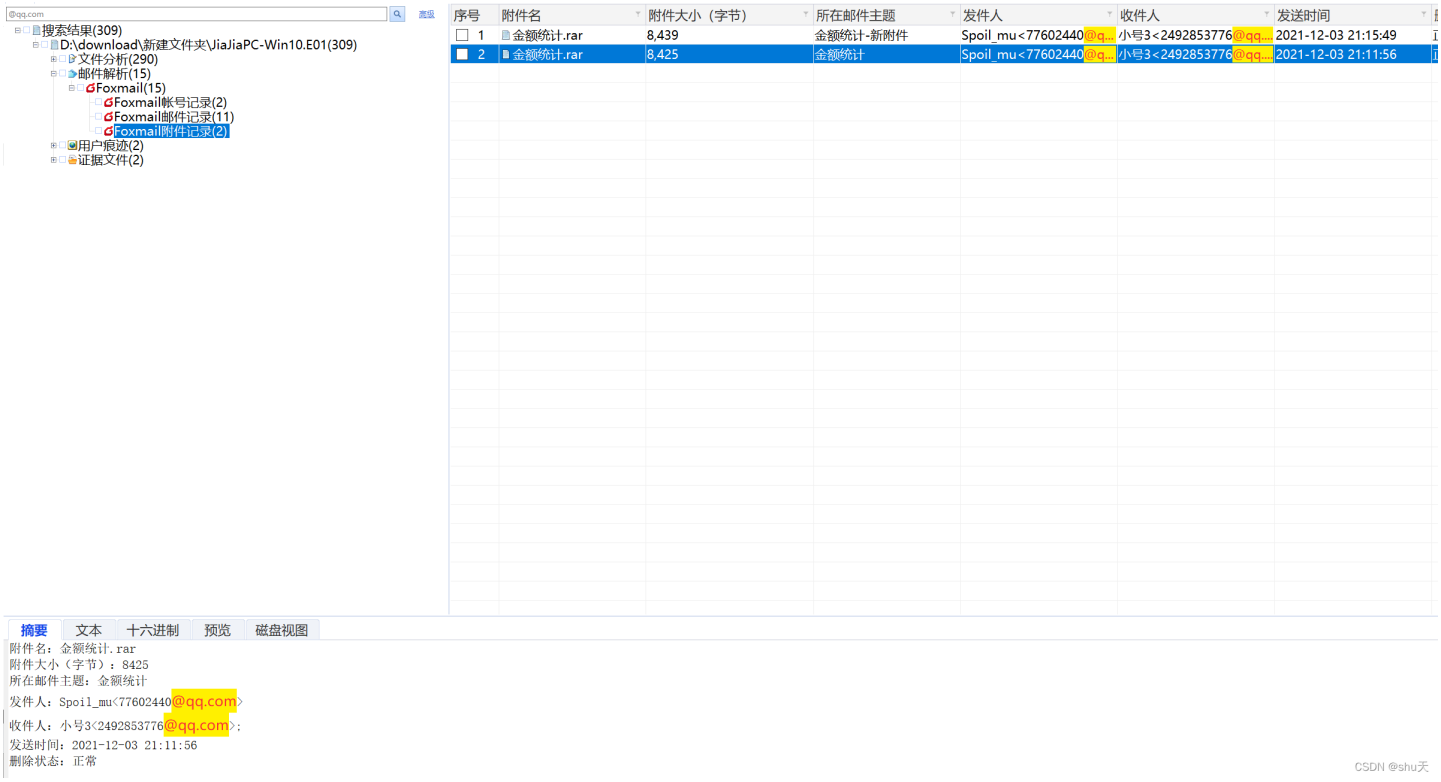
后面的23手取我都是看wp做的，太酷了

JiaJia-PC-2

题目附件见JiaJia-PC-1
1.佳佳的QQ号是多少？
2.金额统计.rar是由哪个QQ号通过邮箱发送来的？
3.金额统计文档的作者是谁？
ctfshow{md5(A1_A2_A3)} format:ctfshow{1145141919_88886666_charlotte}=ctfshow{86ffb01ac9a2dea89028a968183fc666}

1.佳佳的QQ号是多少？
2.金额统计.rar是由哪个QQ号通过邮箱发送来的？

发件人：Spoil_mu77602440@qq.com
收件人：小号32492853776@qq.com;



仿真：
找到foxmail的安装目录，storage下就是原本的账户

恢复storage文件夹

https://zhidao.baidu.com/question/2203368569887982148.html

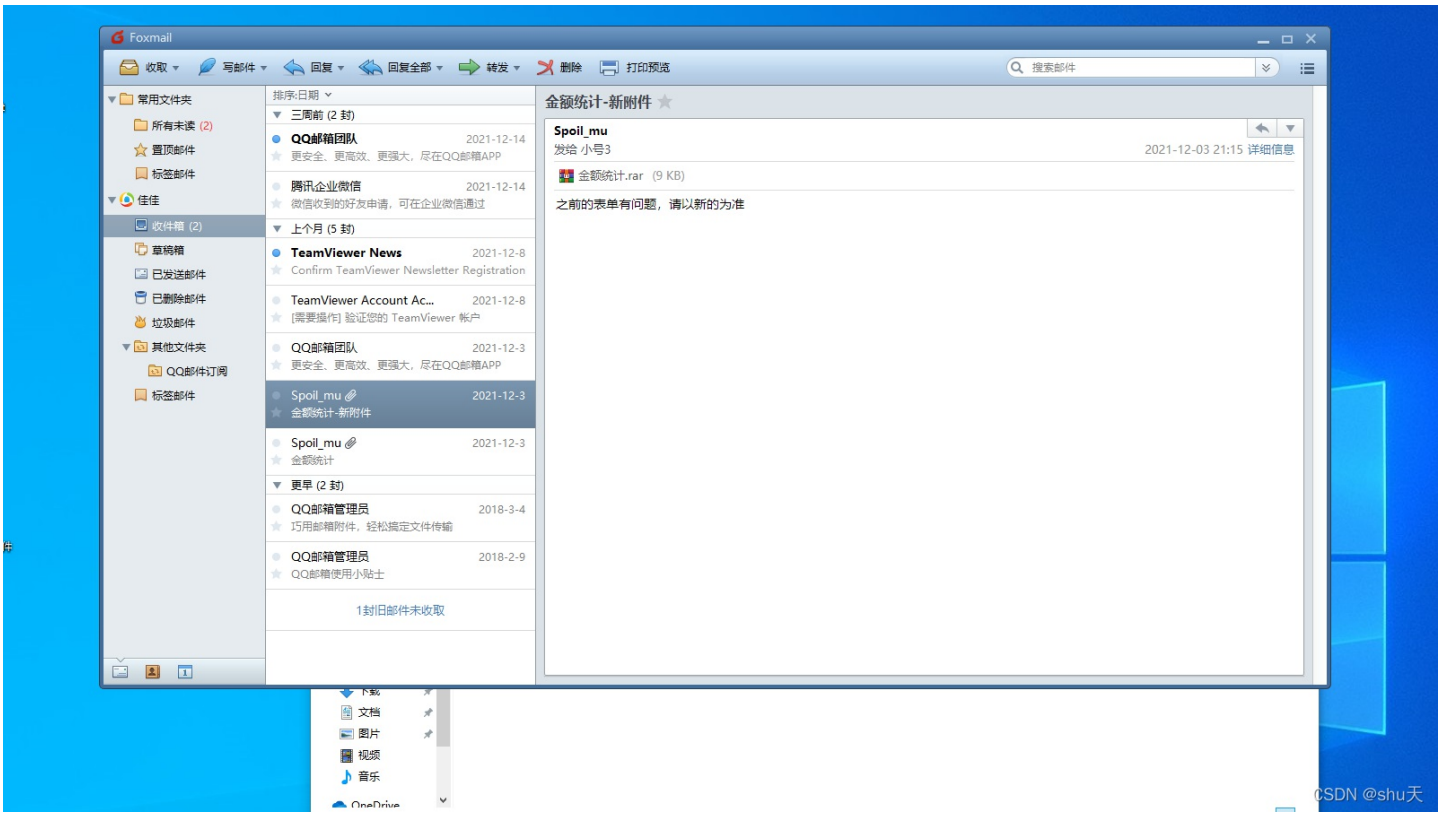
退出Foxmail，把要导入的旧Storage文件夹放到与新Foxmail不同磁盘中的任意位置

比如磁盘根目录下D:\Storage（不一定非要替换新安装的Storage文件夹）

修改Foxmail目录下的FMStorage.list，内容为旧Storage的路径+邮箱号

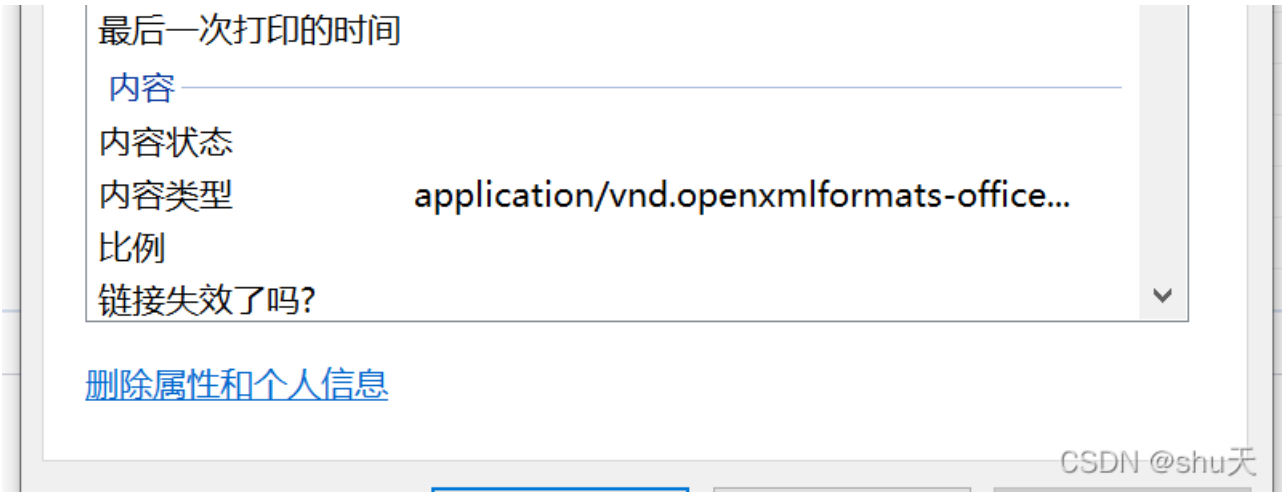
例如D:\Storage\wangsong@help.com\

CSDN @shu天



3.金额统计文档的作者是谁？

常规看就行

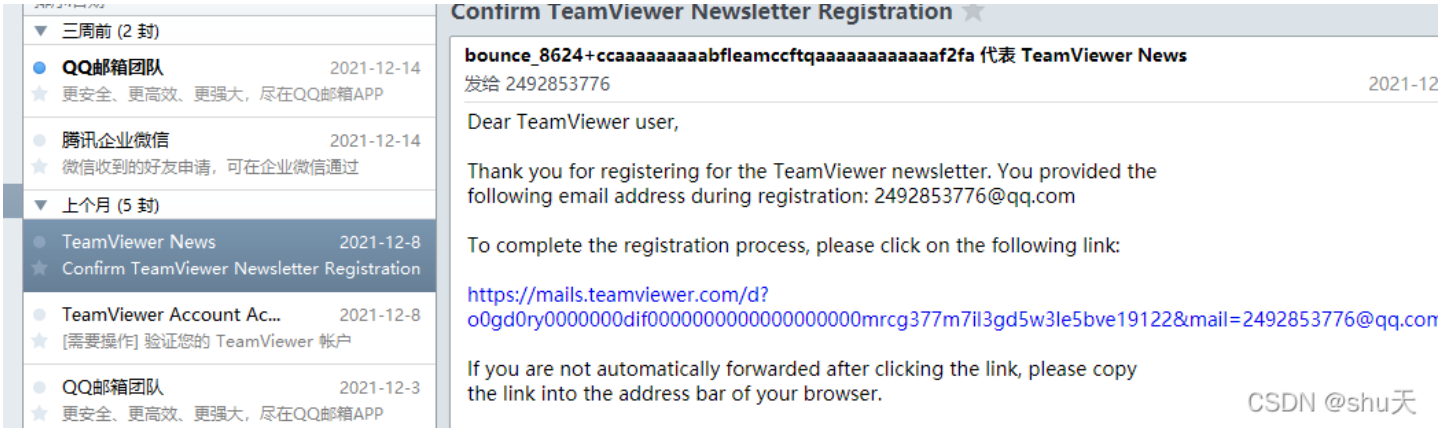


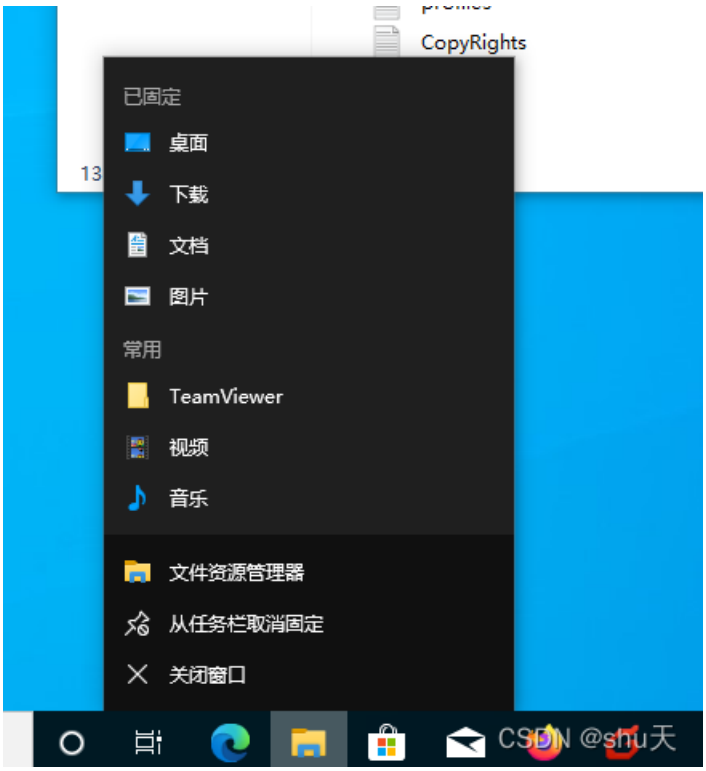
JiaJia-PC-3

> 1.佳佳使用了公司指定的聊天软件，并且使用了此软件的远控功能，请问整个远控持续了多少秒？
> 2.此软件是在多久被开始安装的，请将空格替换成下划线
> 3.除开开机密码外，佳佳喜欢使用一个通用密码，请找出此密码。
> ctfshow{md5(A1_A2_A3)}
> format:ctfshow{md5(100_2021/12/12_12:12:00.666_CtfSh0w!!!)}=ctfshow{24cef4e40844c85aec31a5b7ea4736bb}

1.佳佳使用了公司指定的聊天软件，并且使用了此软件的远控功能，请问整个远控持续了多少秒？
2.此软件是在多久被开始安装的，请将空格替换成下划线

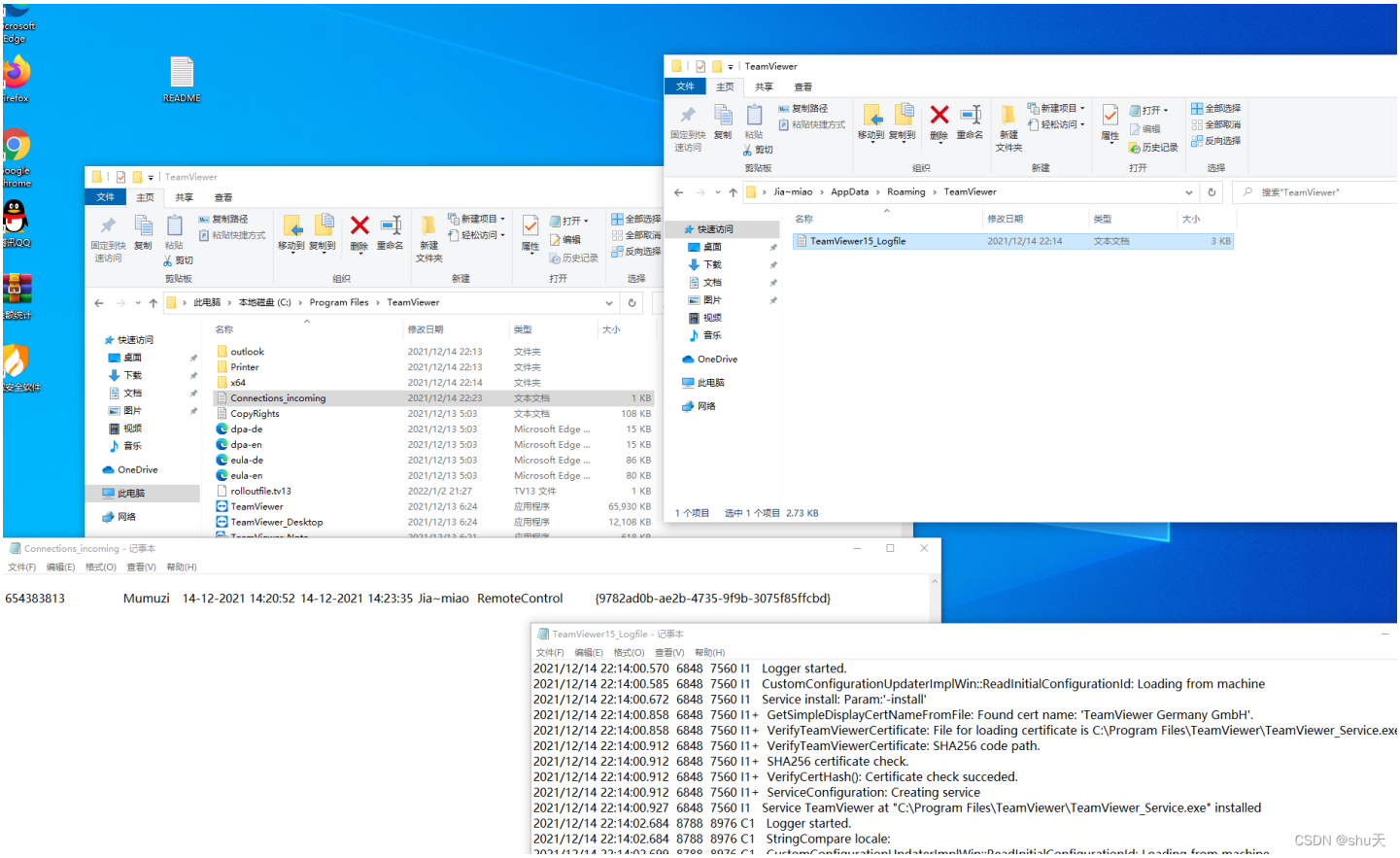
仿真：
邮件和最近访问都可以看到teamviewer的痕迹





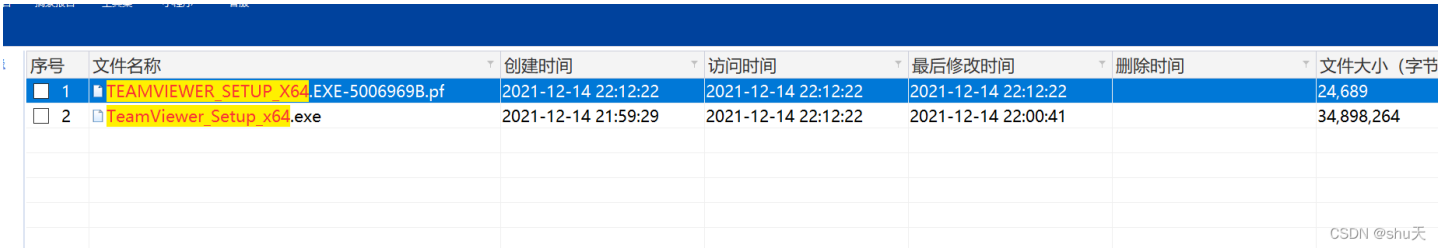
timeviewer日志：https://community.teamviewer.com/Chinese/kb/articles/4694-%E5%A6%82%E4%BD%95%E6%9F%A5%E6%89%BE%E6%97%A5%E5%BF%97%E6%96%87%E4%BB%B6

> 手动查找日志文件
> 通常情况，TeamViewer 日志文件可以通过以下地点查找：
> **Windows**
> TeamViewer 完整版本和 主机版本:
> C:\Program Files (x86)\TeamViewer
> TeamViewer QuickSupport:
> C:\Users[username]\AppData\Roaming\TeamViewer



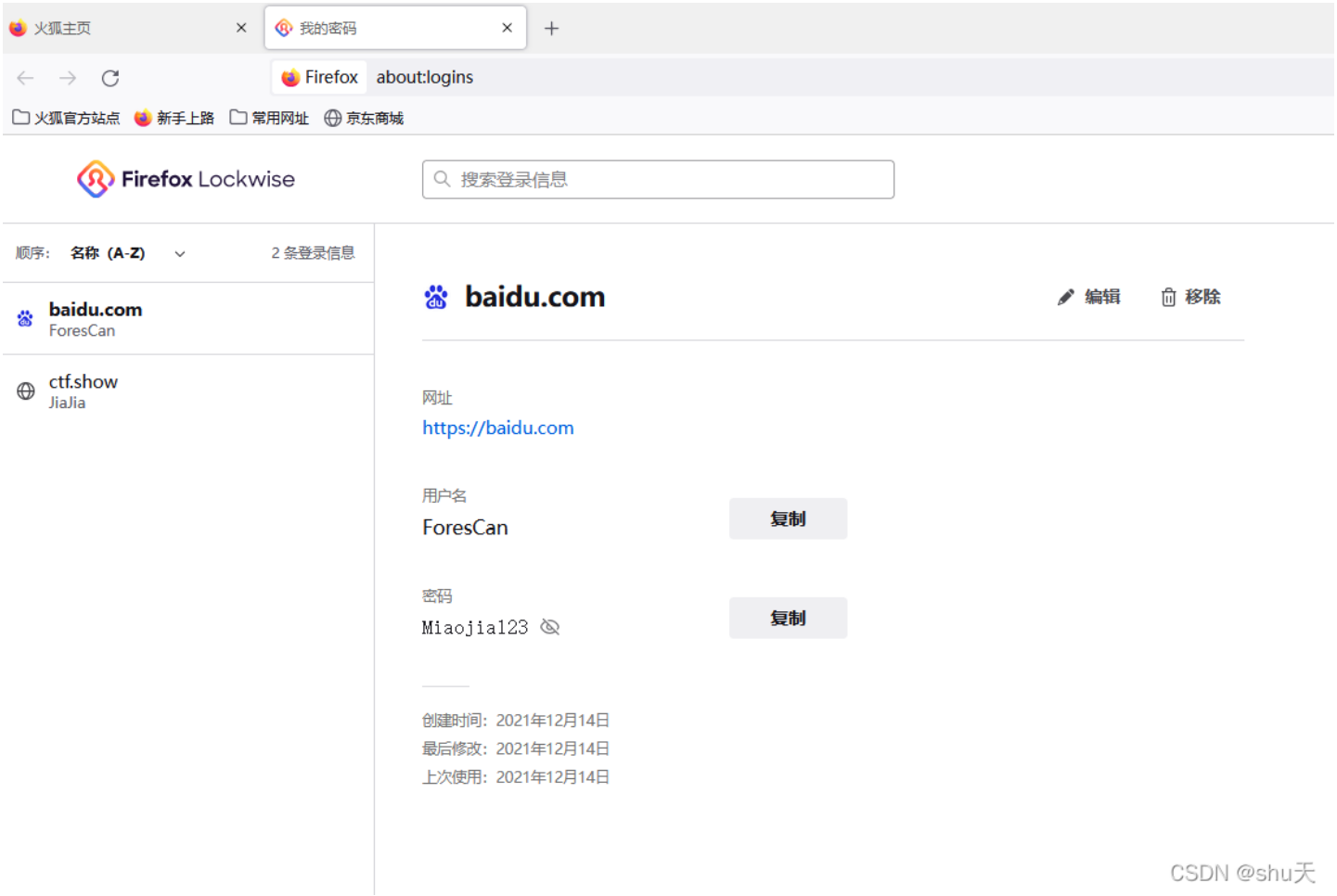
Connections_incoming里面是连接记录和时间

Logfile里面是安装时间2021/12/14 22:14:00.570（其实我觉得应该看pf预处理文件的生成时间）



3.除开开机密码外，佳佳喜欢使用一个通用密码，请找出此密码。

看看火狐里面保存的密码



flag为163_2021/12/14_22:14:00.570_Miaojia123的md5值