




[ctfshow 2021摆烂杯] FORENSICS部分 writeup

原创

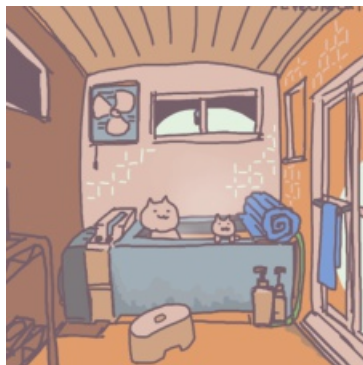
shu天  于 2022-01-03 09:45:00 发布  466  收藏 1

分类专栏: [# 内存取证](#) [取证](#) [# misc](#) 文章标签: [取证](#) [ctf](#) [misc](#) [流量](#)

不允许转载

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

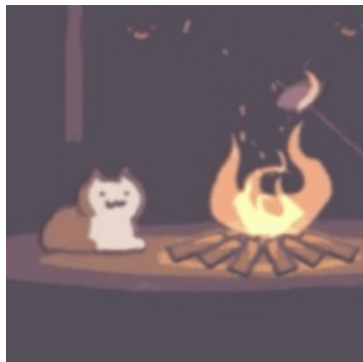
版权



[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



[#EyeOnCat](#) [misc](#)

7 篇文章 0 订阅

订阅专栏

[ctfshow 2021摆烂杯] FORENSICS部分 writeup

套的签到题

第一段flag

第二段flag

第三段flag

JiaJia-CP-1

JiaJia-CP-2

JiaJia-CP-3

JiaJia-PC-1

JiaJia-PC-2

JiaJia-PC-3

官方的wp: <https://qqieod1s9b.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

The screenshot shows a network traffic analysis tool interface. At the top, there's a list of network packets. Packet 3221 is highlighted, showing a request from 192.168.26.232 to 42.193.4.49. Below this, the details for the response in frame 3221 are shown. The response is HTML Form URL Encoded. The form data includes several items, with the most relevant one being:

```
Form item: "lf17935f70e96" = "Hg"
Key: lf17935f70e96
Value: Hg
```

At the bottom of the screenshot, a hex dump shows the raw data of the response, with the Base64-encoded value `fdb0a19e409768=Y4Y2QgIi8iO2NhdCBmMTExNGcudHh002VjaG8gW1Nd03B3ZDt1Y2hvIFtFXQ==` visible.

Y2Qgli8iO2NhdCBmMTEeXMTExNGcudHh0O2VjaG8gW1NdO3B3ZDtiY2hvlFtFXQ==

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

```
cd "/";cat f1111114g.txt;echo [S];pwd;echo [E]
```

CSDN @shu天

response

3221	2021-12-15	20:05:33.505770	42.193.4.49	192.168.26.232	HTTP
3280	2021-12-15	20:05:58.023804	192.168.26.232	42.193.4.49	HTTP
3282	2021-12-15	20:05:58.094297	42.193.4.49	192.168.26.232	HTTP
3379	2021-12-15	20:06:09.749499	192.168.26.232	42.193.4.49	HTTP
3381	2021-12-15	20:06:09.829743	42.193.4.49	192.168.26.232	HTTP

```
Server: Apache/2.4.29 (Ubuntu)\r\n
> Content-Length: 65\r\n
Connection: close\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.150981000 seconds]
[Request in frame: 3217]
[Request URI: http://42.193.4.49/a.php]
File Data: 65 bytes
Line-based text data: text/html (5 lines)
50a026070cDRydDFfeTAwX3lvdV9jcmFja19teV93cHdlYg==\n
[S]\n
/\n
[E]\n
5e35e
```

CSDN @shu天

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

cDRydDFfeTAwX3lvdV9jcmFja19teV93cHdlYg==

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

```
p4rt1_y00_you_crack_my_wpweb
```

CSDN @shu天

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: 1/13, Len: 20/

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

The screenshot shows a network traffic analysis tool interface. At the top, there's a search bar with 'http' and a search button. Below it is a table of connections with columns for No., Time, Source, Destination, and Protocol. The table lists several connections, with the one at 20:06:38.270374 selected. Below the table, the details of this selected connection are shown, including the HTTP response headers and the body content. The body content is a line-based text data with 3 lines: '50211d3a3dflag\t\t\r\n', 'bm93X31vdV9jYW5fc3VibWl0X2ZsYWcy\t\t\r\n', and '79f8d7eeb'. At the bottom, there's a hex dump of the selected connection's data, showing the start of the response body: '0d00 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 35 30 32 set=UTF- 8...502'.

No.	Time	Source	Destination	Protocol
3589	2021-12-15 20:06:36.497801	42.193.4.49	192.168.26.232	HTTP
3657	2021-12-15 20:06:38.157121	192.168.26.232	42.193.4.49	HTTP
3664	2021-12-15 20:06:38.270374	42.193.4.49	192.168.26.232	HTTP
3688	2021-12-15 20:06:49.717643	192.168.26.232	42.193.4.49	HTTP
3694	2021-12-15 20:06:49.874523	42.193.4.49	192.168.26.232	HTTP
3706	2021-12-15 20:06:50.514494	192.168.26.232	42.193.4.49	HTTP
3708	2021-12-15 20:06:50.671015	42.193.4.49	192.168.26.232	HTTP
3732	2021-12-15 20:06:57.703418	192.168.26.232	42.193.4.49	HTTP

```
> HTTP/1.1 200 OK\r\n
Date: Wed, 15 Dec 2021 12:06:37 GMT\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
> Content-Length: 65\r\n
Connection: close\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.113253000 seconds]
[Request in frame: 3657]
[Request URI: http://42.193.4.49/a.php]
File Data: 65 bytes
Line-based text data: text/html (3 lines)
50211d3a3dflag\t\t\r\n
bm93X31vdV9jYW5fc3VibWl0X2ZsYWcy\t\t\r\n
79f8d7eeb
0d00 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 35 30 32 set=UTF- 8...502
```

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

CSDN @shu天

now_you_can_submit_flag2

第三段 flag

看到登陆密码

Wireshark capture details for an HTTP POST request:

- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "log" = "hacker"
 - Key: log
 - Value: hacker
 - Form item: "pwd" = "password"
 - Key: pwd
 - Value: password
 - Form item: "wp-submit" = "登录"
 - Key: wp-submit
 - Value: 登录
 - Form item: "redirect_to" = "http://42.193.4.49/wp-admin/"
 - Key: redirect_to
 - Value: http://42.193.4.49/wp-admin/
 - Form item: "testcookie" = "1"
 - Key: testcookie
 - Value: 1

Raw packet data (hex):

```

02c0 74 6f 3d 68 74 74 70 25 33 41 25 32 46 25 32 46 to=http 3A%2F%2F
02d0 34 32 2e 31 39 33 2e 34 2e 34 39 25 32 46 77 70 42.193.4
02e0 2d 61 64 6d 69 6e 25 32 46 26 74 65 73 74 63 6f -admin%2
02f0 6f 6b 69 65 3d 31 okie=1
  
```

CSDN @shu天

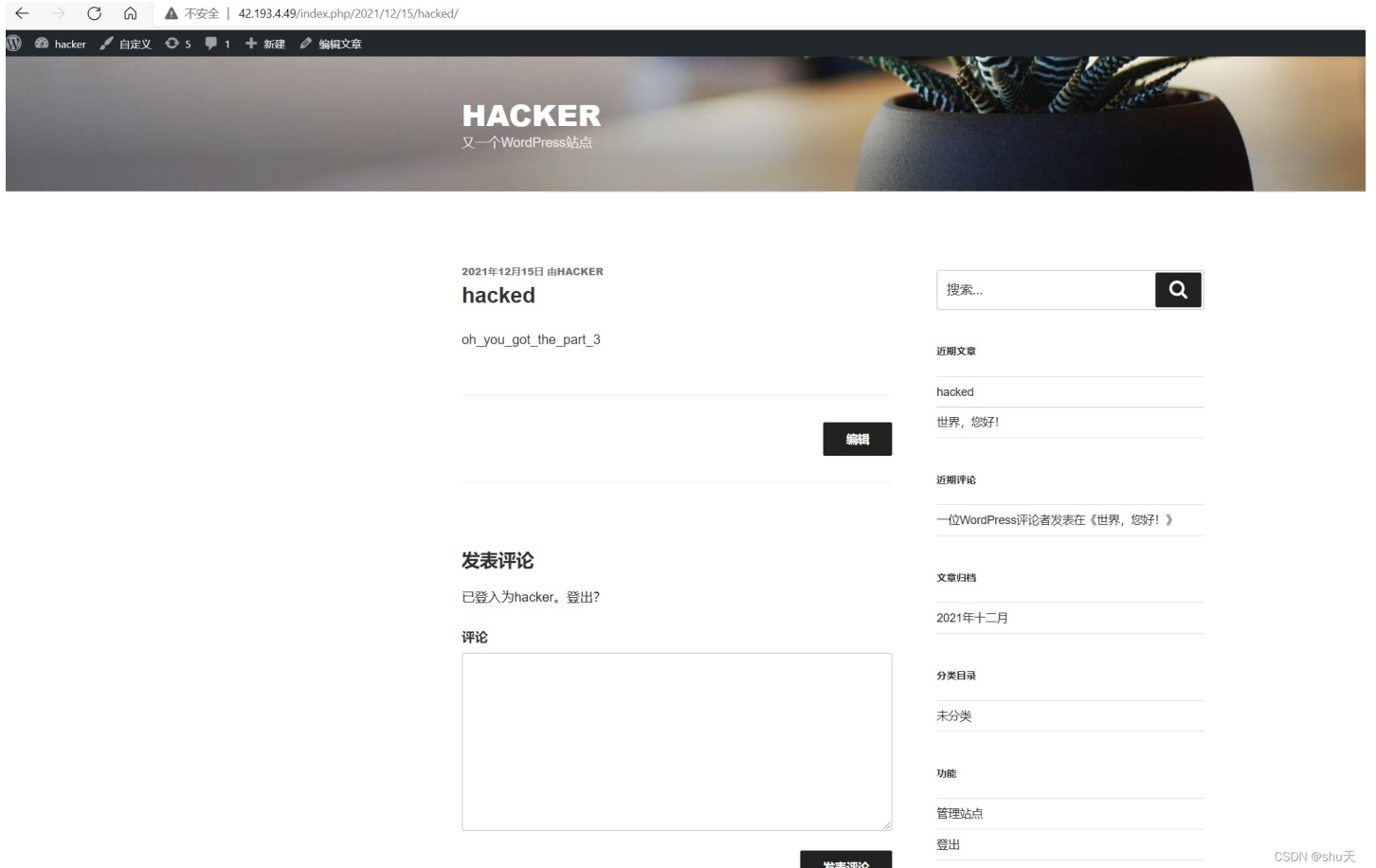
登陆进去看文章

WordPress admin dashboard showing a list of articles:

复选框	标题	作者	分类目录	标签	日期
<input type="checkbox"/>	hacked	hacker	未分类	-	已发布 2021-12-15
<input type="checkbox"/>	世界, 您好!	hacker	未分类	-	已发布 2021-12-15



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})

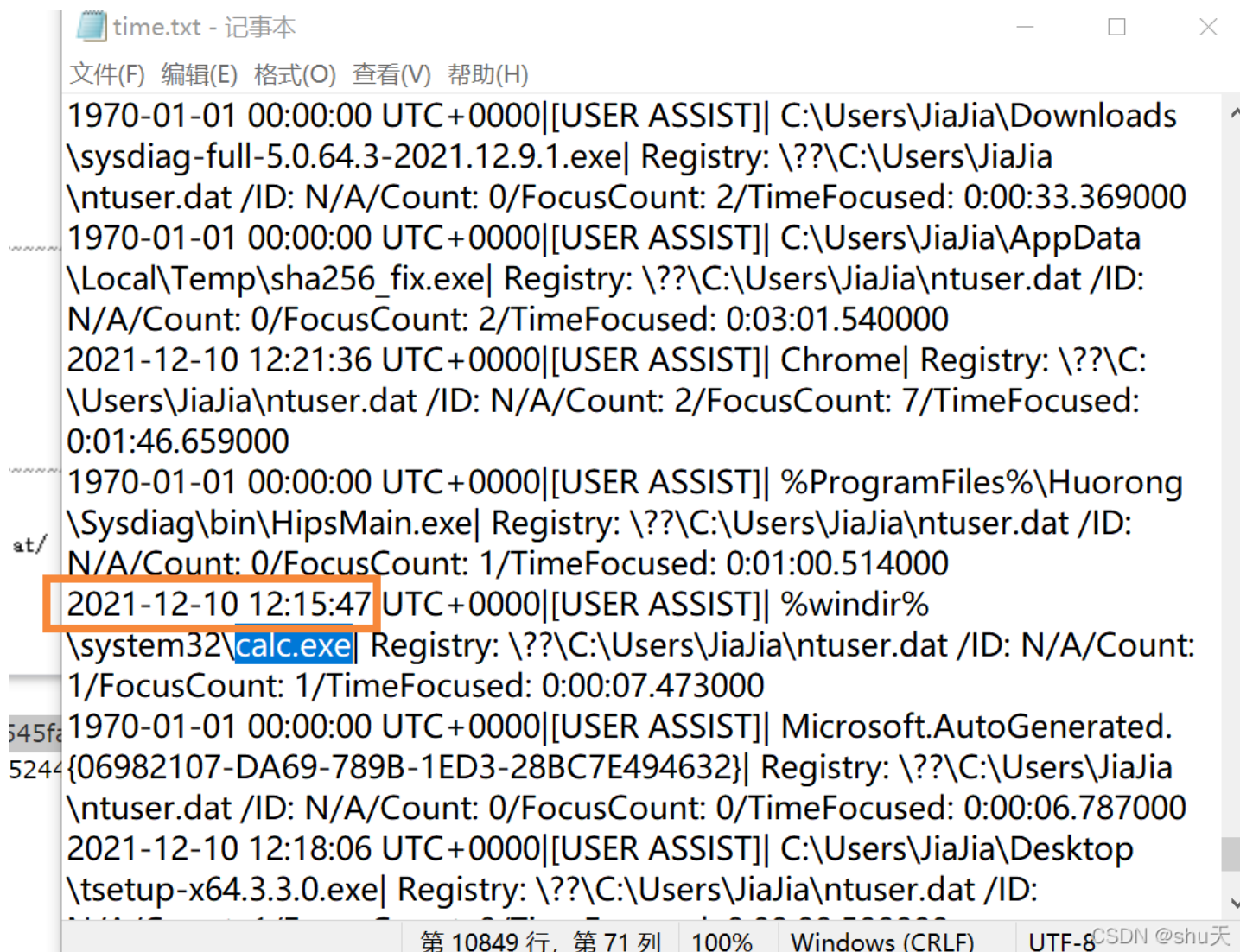
2.最后一次运行计算器的时间? (格式为yyyy-mm-dd_hh:mm:ss, 注意冒号为英文冒号)

flag格式为ctfshow{md5(A1_A2)}, format:ctfshow{lj_2021-12-12_07:13:26}=ctfshow{c3cf135599d338093cbd2b578065be89}

filescan正常搜一些 `\Users\` 就可以找到用户名jiajia

```
3x00000013fd0070 16 0 R--r-- \Device\HarddiskVolume1\Users\JiaJia\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6025C34CC5B36C4156C40F3B0D99B6AB
7v00000013fd0000 12 0 R--rwd \Device\HarddiskVolume1\Windows\Fonts\Georgia.ttf
```

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)



```
time.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\Downloads
\sysdiag-full-5.0.64.3-2021.12.9.1.exe| Registry: \??\C:\Users\JiaJia
\ntuser.dat /ID: N/A/Count: 0/FocusCount: 2/TimeFocused: 0:00:33.369000
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| C:\Users\JiaJia\AppData
\Local\Temp\sha256_fix.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID:
N/A/Count: 0/FocusCount: 2/TimeFocused: 0:03:01.540000
2021-12-10 12:21:36 UTC+0000|[USER ASSIST]| Chrome| Registry: \??\C:
\Users\JiaJia\ntuser.dat /ID: N/A/Count: 2/FocusCount: 7/TimeFocused:
0:01:46.659000
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| %ProgramFiles%\Huorong
\Sysdiag\bin\HipsMain.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID:
N/A/Count: 0/FocusCount: 1/TimeFocused: 0:01:00.514000
2021-12-10 12:15:47 UTC+0000|[USER ASSIST]| %windir%
\system32\calc.exe| Registry: \??\C:\Users\JiaJia\ntuser.dat /ID: N/A/Count:
1/FocusCount: 1/TimeFocused: 0:00:07.473000
1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| Microsoft.AutoGenerated.
{06982107-DA69-789B-1ED3-28BC7E494632}| Registry: \??\C:\Users\JiaJia
\ntuser.dat /ID: N/A/Count: 0/FocusCount: 0/TimeFocused: 0:00:06.787000
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:
第 10849 行, 第 71 列 100% Windows (CRLF) UTF-8 CSDN @shu天
```

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: 0x7fef42f000
2020-03-30 22:13:25 UTC+0000 [PE DEBUG] desktopEvents.dll | Process: vmtoolsd.exe/PID: 2376/PPID: 3044/Process POffset: 0x13de9eb00/DLL Base: 0x7fef42f000
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: 0x7fef42f000
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: 0:00:00.500000
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/TimeFocused: 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
CSDN @shu天
```

导出文件

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

file.None.0xfffffa8006065d10.Telegram.exe 属性

常规 兼容性 文件校验 安全 详细信息 以前的版本

属性	值
说明	
文件说明	Telegram Desktop
类型	应用程序
文件版本	3.3.0.0
产品名称	Telegram Desktop
产品版本	3.3.0.0
版权	Copyright (C) 2014-2021
大小	103 MB
修改日期	2022/1/2 15:56
语言	英语(美国)

CSDN @shu天

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

Process Name	PID	PPID	Parent Name	Arch	Session	Start Time	Start Time (UTC)
wmpnetwk.exe	2780	484	9	215	0	2021-12-09 13:31:45	UTC+0000
svchost.exe	2976	484	16	287	0	2021-12-09 13:31:45	UTC+0000
svchost.exe	696	484	13	325	0	2021-12-09 13:32:54	UTC+0000
SogouCloud.exe	2612	2388	20	410	1	2021-12-09 13:34:31	UTC+0000
HipsTray.exe	2264	4012	12	281	1	2021-12-09 13:35:24	UTC+0000
svchost.exe	972	484	4	108	0	2021-12-10 12:19:41	UTC+0000
firefox.exe	2136	2928	71	1157	1	2021-12-10 12:19:43	UTC+0000
firefox.exe	4800	2136	37	332	1	2021-12-10 12:19:44	UTC+0000
firefox.exe	5076	2136	17	281	1	2021-12-10 12:19:45	UTC+0000
firefox.exe	1064	2136	19	318	1	2021-12-10 12:19:45	UTC+0000
firefox.exe	3124	2136	8	175	1	2021-12-10 12:19:48	UTC+0000
firefox.exe	4860	2136	18	294	1	2021-12-10 12:20:58	UTC+0000
firefox.exe	2128	2136	16	269	1	2021-12-10 12:24:46	UTC+0000
firefox.exe	924	2136	16	270	1	2021-12-10 12:24:51	UTC+0000
firefox.exe	4304	2136	16	272	1	2021-12-10 12:24:57	UTC+0000
HipsDaemon.exe	2352	484	37	356	0	2021-12-10 12:26:13	UTC+0000
usysdiag.exe	4976	2352	7	100	0	2021-12-10 12:26:14	UTC+0000
HipsTray.exe	4128	2352	0	-----	1	2021-12-10 12:26:15	UTC+0000
HipsTray.exe	5028	2352	0	-----	1	2021-12-10 12:26:15	UTC+0000
audiodg.exe	3196	752	6	138	0	2021-12-10 12:29:58	UTC+0000
SearchProtocol	4312	2592	9	307	0	2021-12-10 12:33:00	UTC+0000
SearchFilterHo	3348	2592	5	85	0	2021-12-10 12:33:01	UTC+0000
DumpIt.exe	3396	3044	1	26	1	2021-12-10 12:33:12	UTC+0000
conhost.exe	4244	396	6	224	1	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
1	searchbar-history	sougouliulanqi	1	1639055355204000	1639055355204000	8ZoC5hdAQ1a8DmyD
2	searchbar-history	chrome	1	1639055449429000	1639055449429000	YcGnK7noSOWCn3Cu
3	searchbar-history	163 邮箱	1	1639138801009000	1639138801009000	ACa1VsW0R1e9U5HR
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 screenshot -D ./2
```

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

根目录和子目录

...> 责编:徐佩玉 邮箱:hwbjib@163.com

...> 责编:徐佩玉 邮箱:hwbjib@163.com

...> 8 a2492853776@163.com 百度搜索

...> //mail.163.com/contacts/call.do?uid=a2492853776@163.com&sid=CBAYfhoNumGbPsKrirNNYSIJWBaSRWZc&from=webmail&cmd=newapi.getCor

...> 8 榕溪獨穩決*坤恬% 杖恰恰* 樣贈舫鼓 8 榕溪獨穩

...> can id="msgboxAccountName" title="a2492853776@163.com"></div></div></div></body></html>

...> a2492853776@163.com<u class="bdsug-store-del" title="如您不需要此搜索历史提示, 可在右上

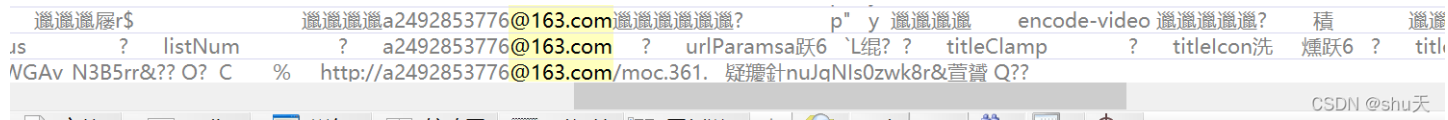
...> a2492853776@163.com<u class="bdsug-store-del" title="如您不需要此搜索历史提示, 可在右上

...> ? set onremovetrack 雜燴 ? a2492853776@163.comKKKKK!@璫KKKK? confirmPasswordField 儘讲 ? fullyMungedPattern u構?

...> 甯甯甯甯 .www.baidu.com 甯甯甯甯甯甯2492853776@163.com甯甯甯甯甯甯?

...> 甯甯甯甯甯 渡 柝? 甯甯甯甯甯p\$ €度 来? 8? 甯甯甯甯

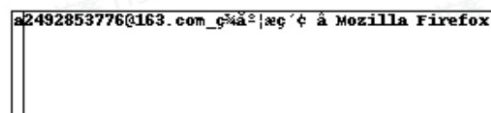
...> ? 8? 甯甯甯甯 d 妣 隆 a2492853776@163.com甯甯甯甯甯甯? p" y 甯甯甯甯 甯甯甯甯 email.163.com 甯甯甯甯



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.产品密钥（卷影）

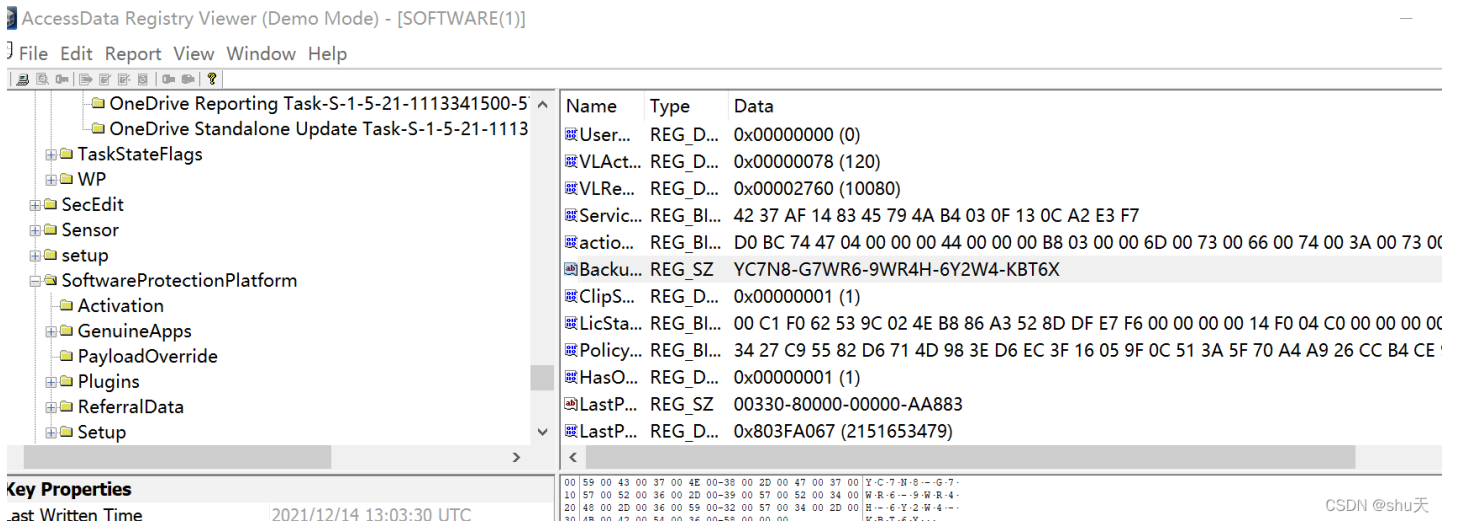
2.Windows系统版本号

```
ctfshow{md5(A1_A2)}
```

```
format:ctfshow{md5(NPPR9-FWDCX-D2C8J-H872K-2YT43_20H2)}=ctfshow{bc536cad5a7853d94d0298289d0c47cd}
```

1.产品密钥（卷影）

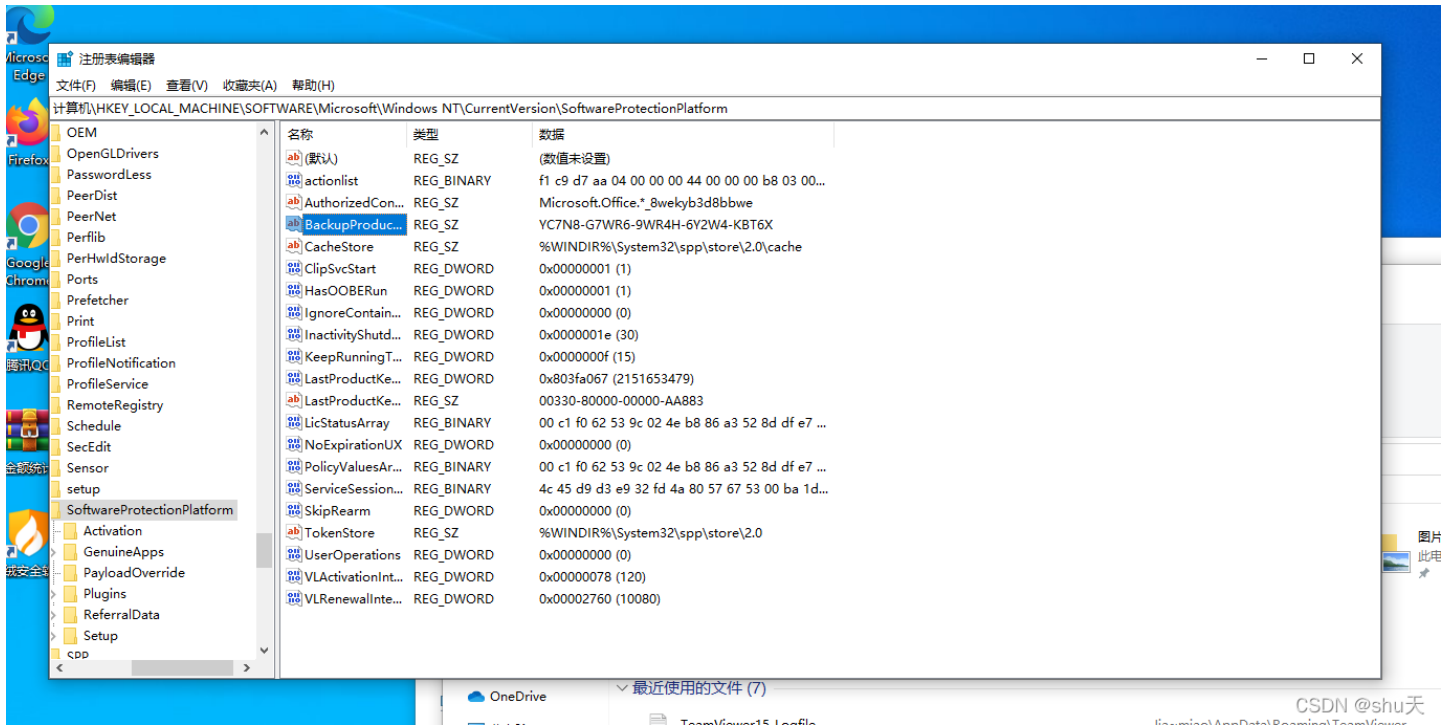
产品密钥要看 [卷影备份中software注册表](#) 里的密钥



仿真查看：

Win + R 运行 Regedit 打开注册表编辑器

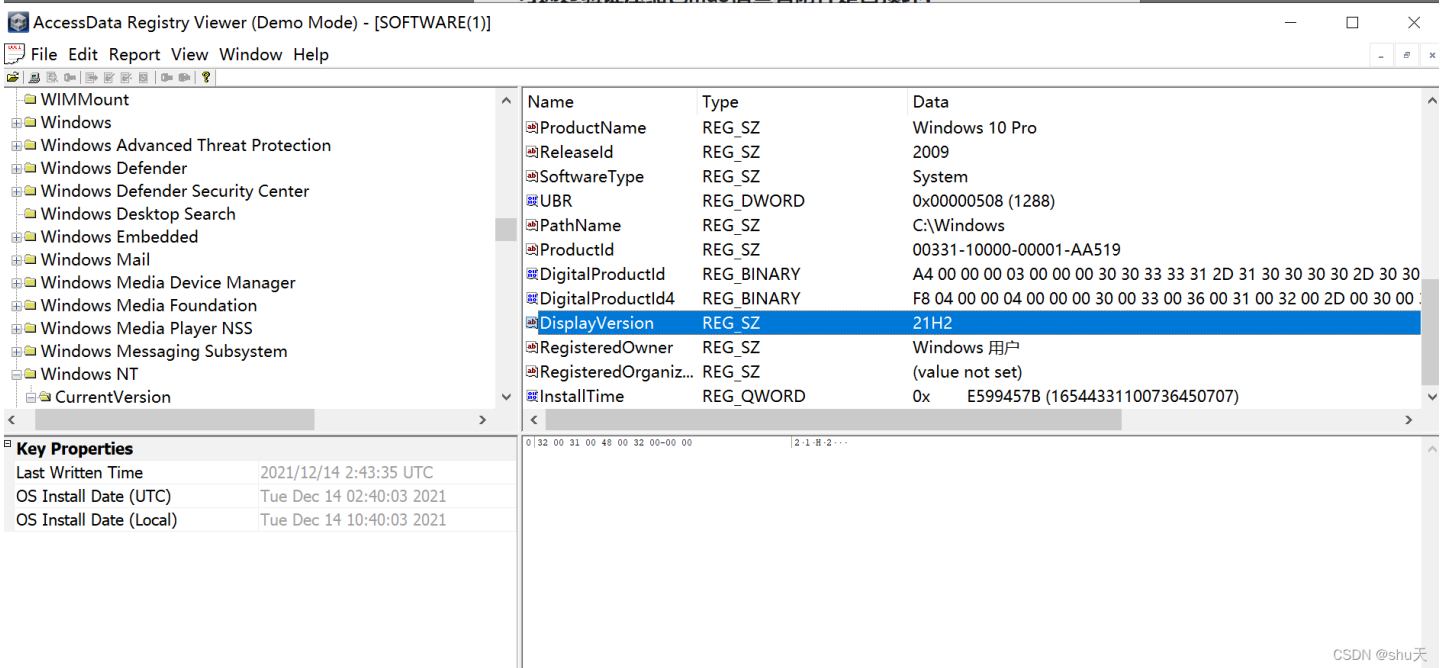
找到：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform右侧的 BackupProductKeyDefault 值就是你的「备份产品密钥」



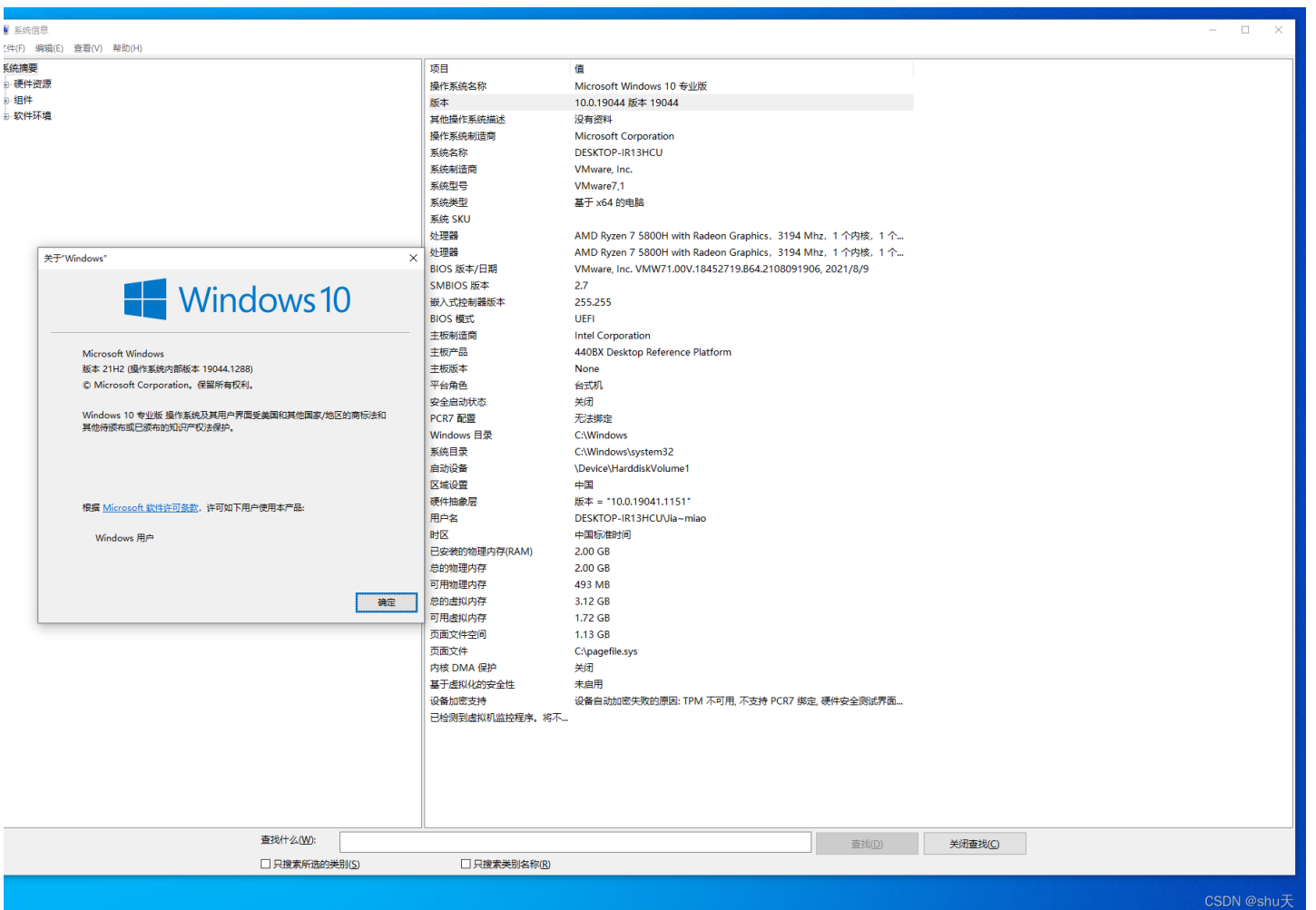
2.Windows系统版本号

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

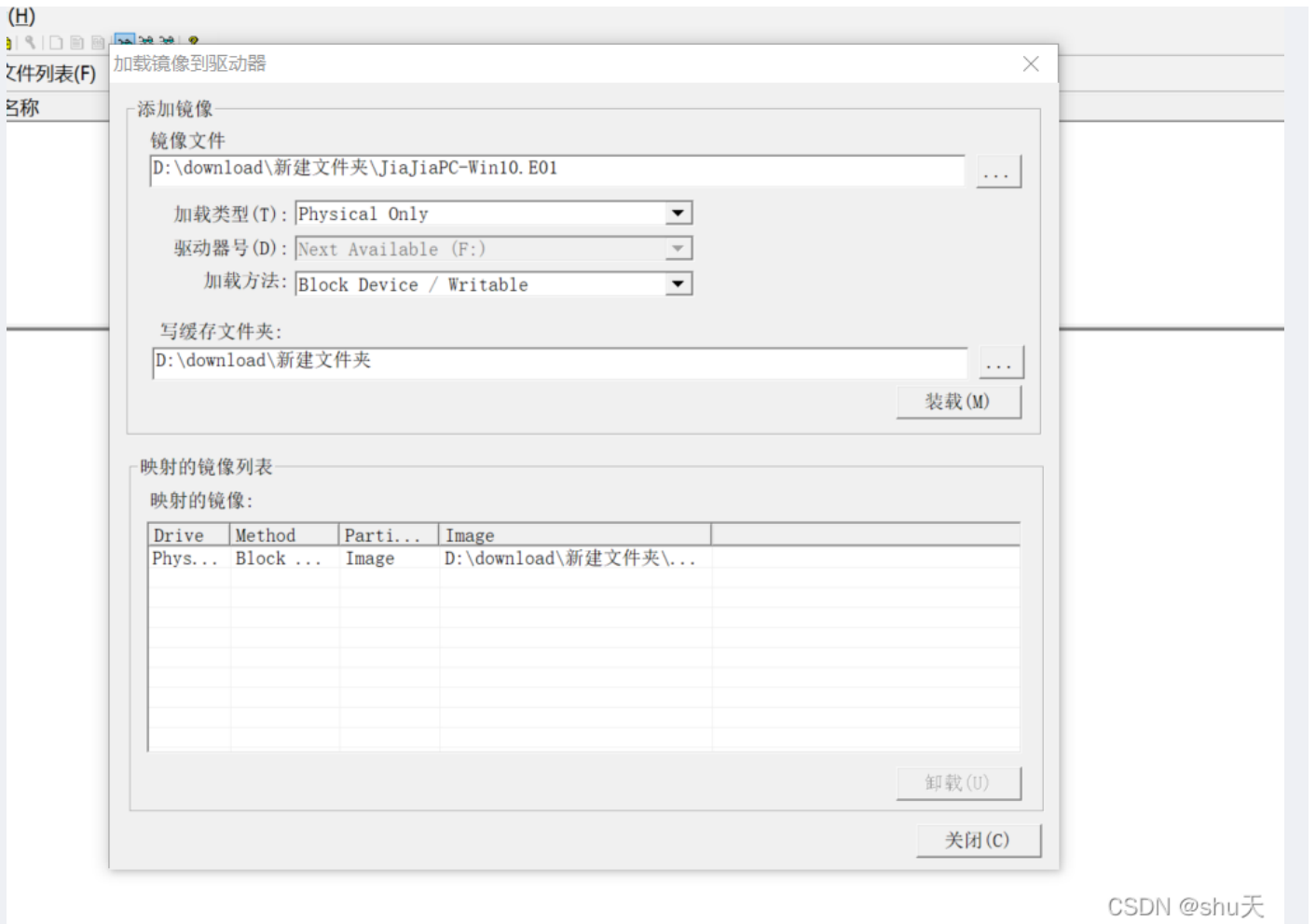


仿真：
win+R,输入winver



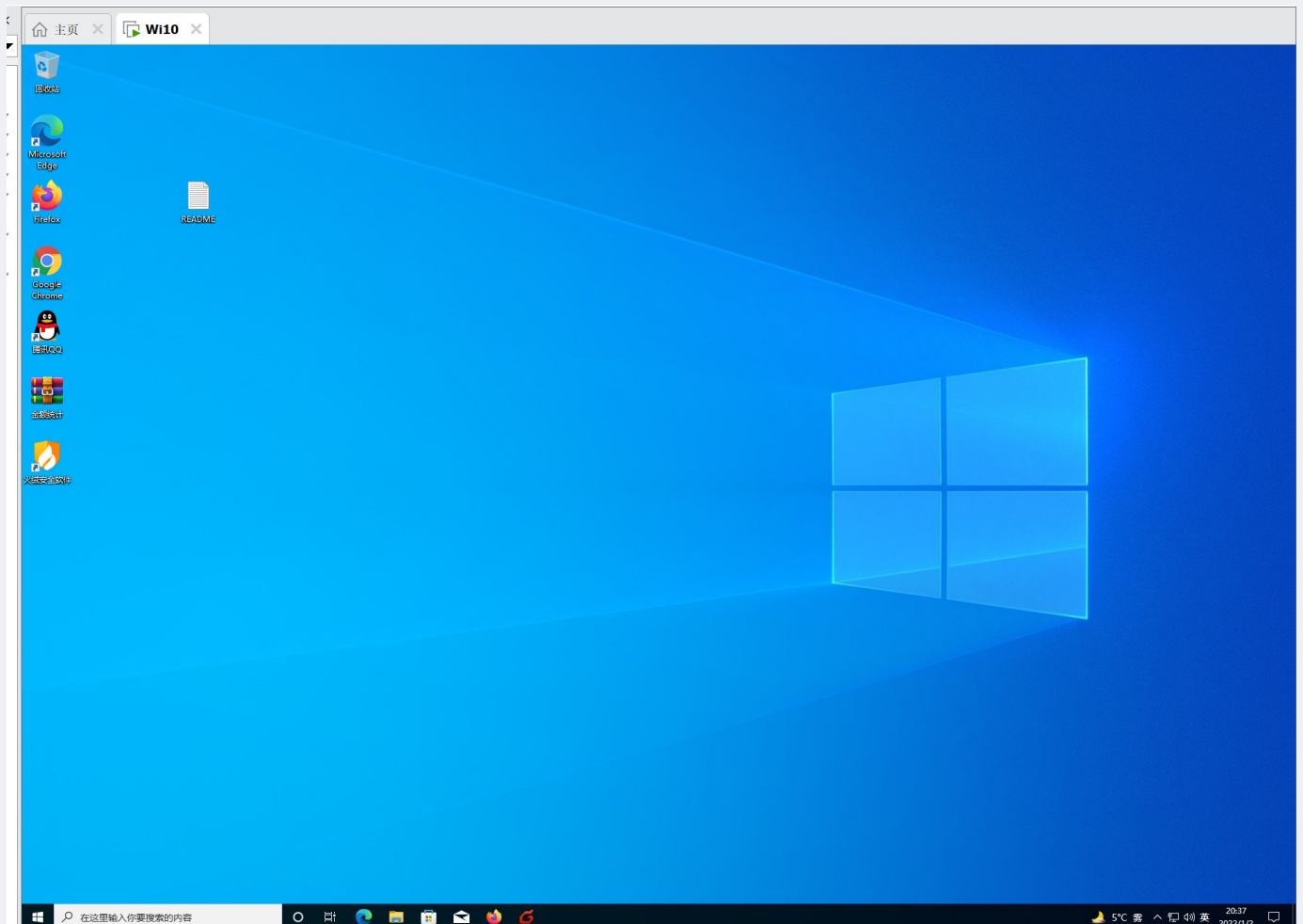
flag即YC7N8-G7WR6-9WR4H-6Y2W4-KBT6X_21H2的md5值

ps仿真过程

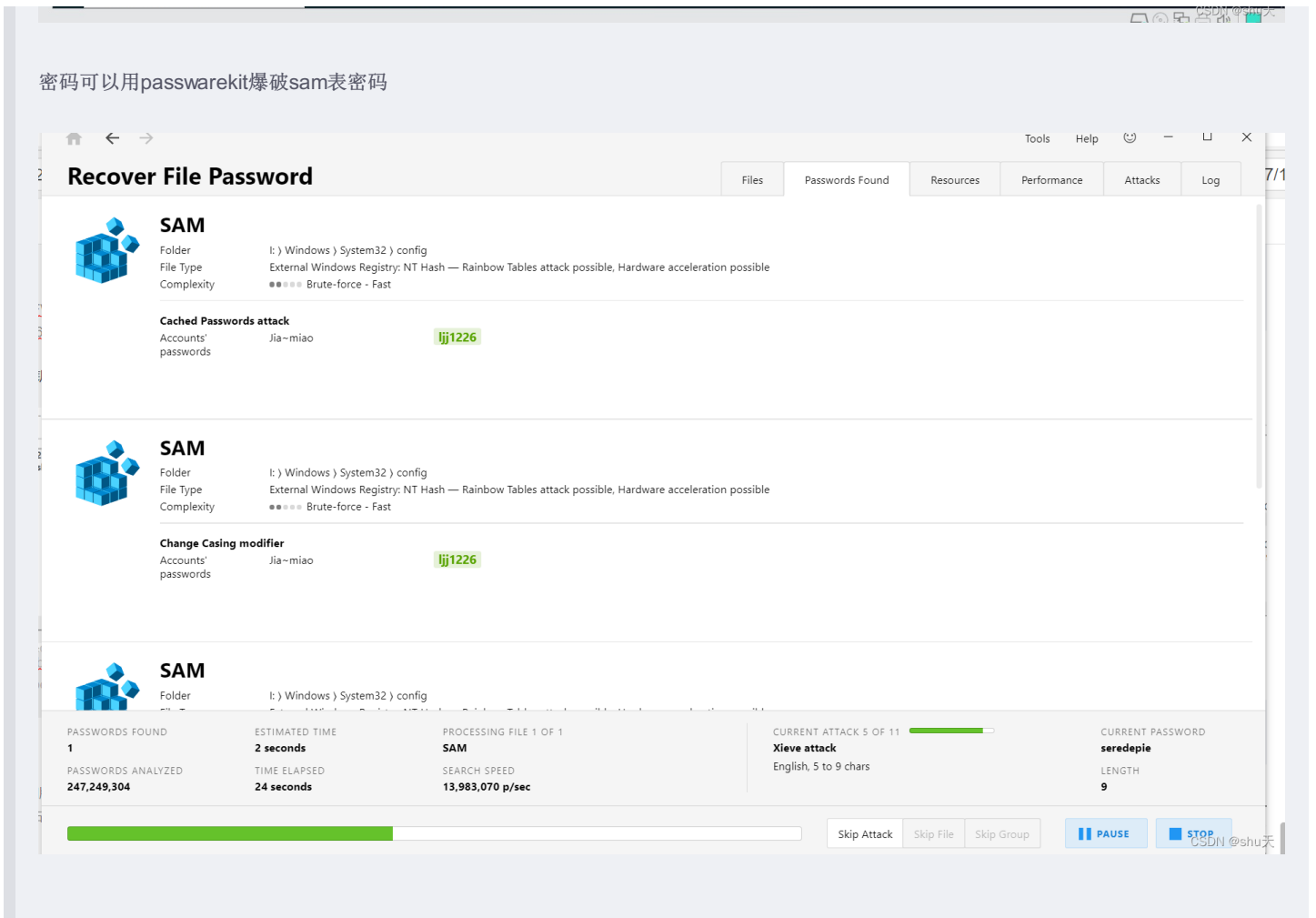


CSDN @shu天

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;

The screenshot shows an email client interface. On the left, there is a search results pane with a tree view showing folders like 'D:\download\新建文件夹\ViaJiaPC-Win10.E01(309)', '文件分析(290)', '邮件解析(15)', 'Foxmail(15)', 'Foxmail帐号记录(2)', 'Foxmail邮件记录(11)', 'Foxmail附件记录(2)', '用户痕迹(2)', and '证据文件(2)'. The main pane displays a table of search results:

序号	附件名	附件大小 (字节)	所在邮件主题	发件人	收件人	发送时间
1	金额统计.rar	8,439	金额统计-新附件	Spoil_mu<77602440@qq.com>	小号3<2492853776@qq.com>	2021-12-03 21:15:49
2	金额统计.rar	8,425	金额统计	Spoil_mu<77602440@qq.com>	小号3<2492853776@qq.com>	2021-12-03 21:11:56

Below the table, there is a detailed view of the selected attachment '金额统计.rar'. The details include:

- 附件名: 金额统计.rar
- 附件大小 (字节): 8425
- 所在邮件主题: 金额统计
- 发件人: Spoil_mu<77602440@qq.com>
- 收件人: 小号3<2492853776@qq.com>
- 发送时间: 2021-12-03 21:11:56
- 删除状态: 正常

At the bottom right of the email client window, there is a small text 'CSDN @shu天'.

仿真:

找到foxmail的安装目录，storage下就是原本的账户

The screenshot shows a Windows File Explorer window. The address bar displays the path: '此电脑 > 本地磁盘 (C:) > Foxmail 7.2 > Storage'. The main pane shows a folder named '2492853776@qq.com' with a modification date of '2021/12/14 21:08' and a type of '文件夹' (Folder). The left sidebar shows '快速访问' (QuickTime) with links to '桌面' (Desktop), '下载' (Downloads), and '文档' (Documents).

恢复storage文件夹

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

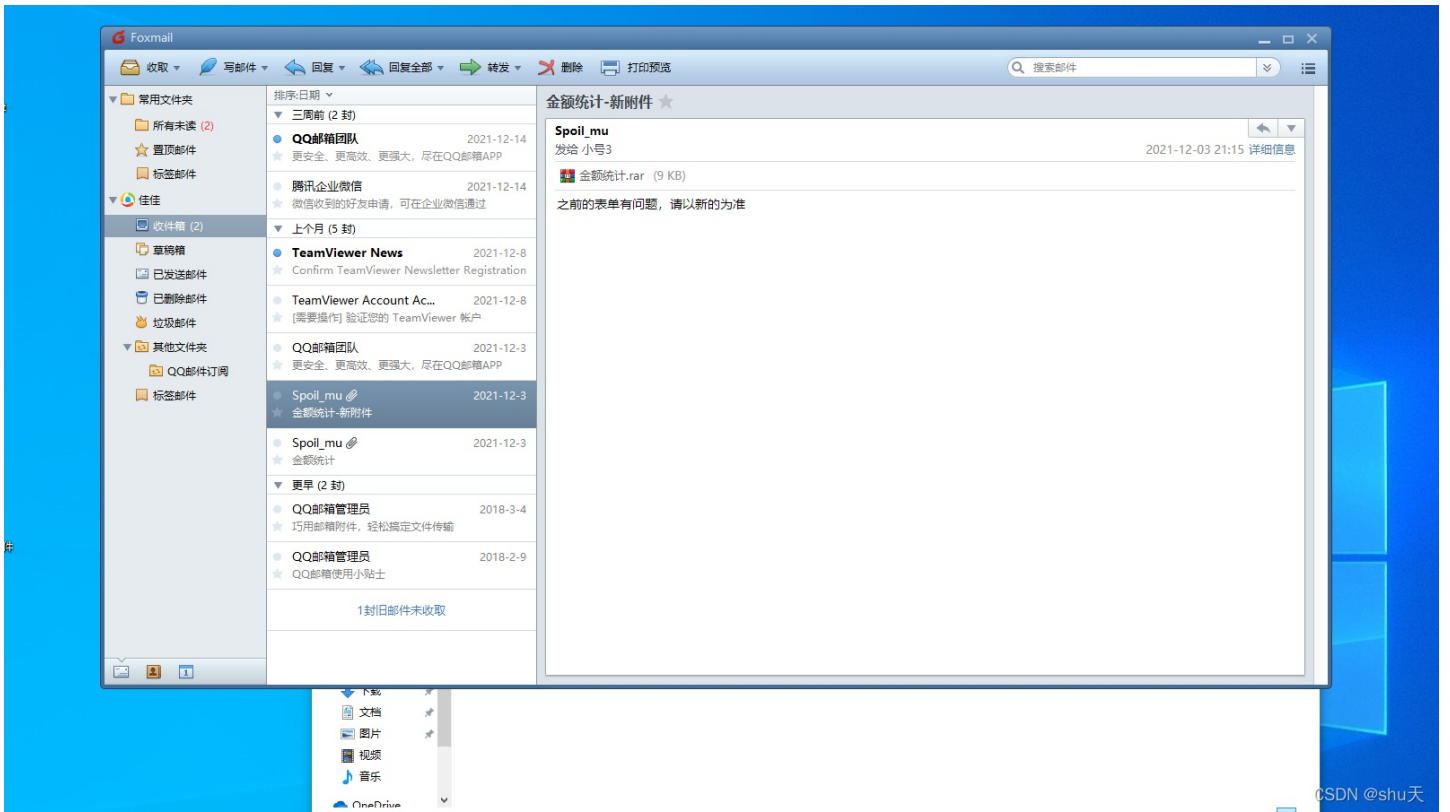
退出Foxmail，把要导入的旧Storage文件夹放到与新Foxmail不同磁盘中的任意位置

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



最后一次打印的时间

内容

内容状态

内容类型

application/vnd.openxmlformats-office...

比例

链接失效了吗?



[删除属性和个人信息](#)

CSDN @shu天

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

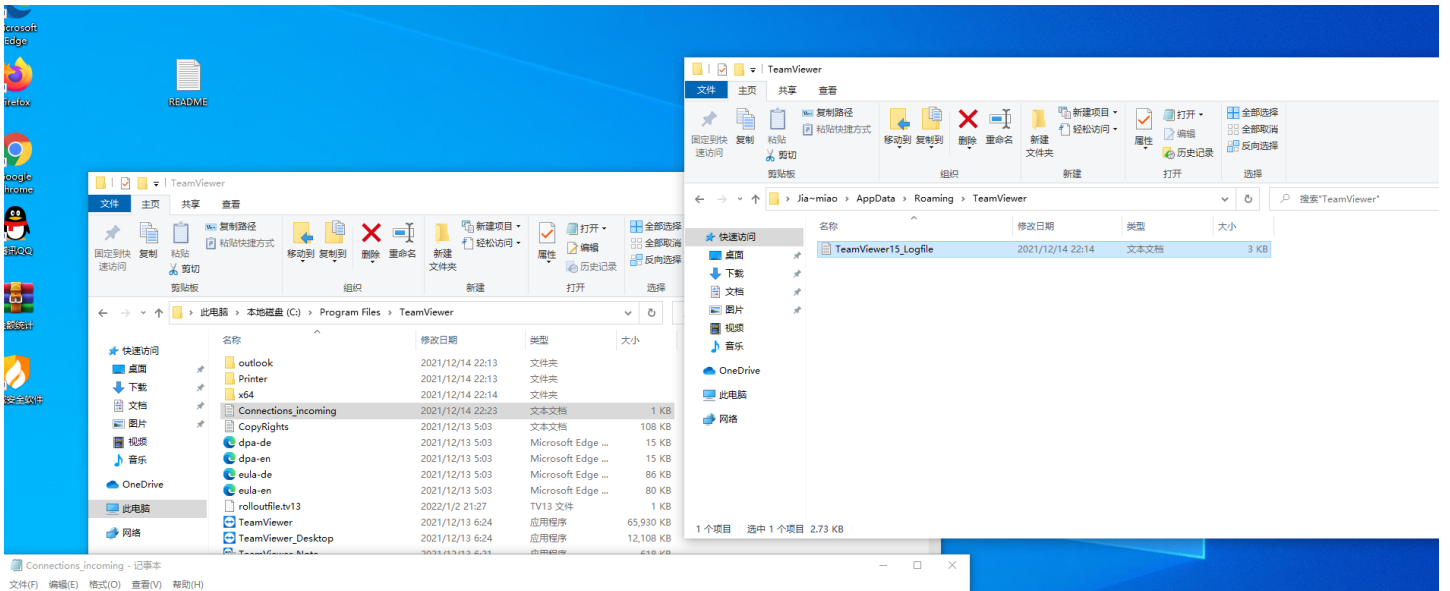
3. 除开开机密码外，佳佳喜欢使用一个通用密码，请找出此密码。

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



654383813 Mumuzi 14-12-2021 14:20:52 14-12-2021 14:23:35 Jia~miao RemoteControl (9782ad0b-ae2b-4735-9f9b-3075f85fcbcd)

```

TeamViewer15_Logfile - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
2021/12/14 22:14:00.570 6848 7560 I1  Logger started.
2021/12/14 22:14:00.585 6848 7560 I1  CustomConfigurationUpdaterImplWin:ReadInitialConfigurationId: Loading from machine
2021/12/14 22:14:00.672 6848 7560 I1  Service install: Param:"-install"
2021/12/14 22:14:00.858 6848 7560 I1+ GetSimpleDisplayCertNameFromFile: Found cert name: 'TeamViewer Germany GmbH'.
2021/12/14 22:14:00.912 6848 7560 I1+ VerifyTeamViewerCertificate: File for loading certificate is C:\Program Files\TeamViewer\TeamViewer_Service.exe
2021/12/14 22:14:00.912 6848 7560 I1+ VerifyTeamViewerCertificate: SHA256 code path.
2021/12/14 22:14:00.912 6848 7560 I1+ SHA256 certificate check.
2021/12/14 22:14:00.912 6848 7560 I1+ VerifyCertHash(): Certificate check succeeded.
2021/12/14 22:14:00.912 6848 7560 I1+ ServiceConfiguration: Creating service
2021/12/14 22:14:00.927 6848 7560 I1  Service TeamViewer at "C:\Program Files\TeamViewer\TeamViewer_Service.exe" installed
2021/12/14 22:14:02.684 8788 8976 C1  Logger started.
2021/12/14 22:14:02.684 8788 8976 C1  StringCompare locale:
2021/12/14 22:14:02.684 8788 8976 C1  CustomConfigurationUpdaterImplWin:ReadInitialConfigurationId: Loading from machine
  
```

CSDN @shu天

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）

序号	文件名称	创建时间	访问时间	最后修改时间	删除时间	文件大小 (字节)
1	TEAMVIEWER_SETUP_X64.EXE-5006969B.pf	2021-12-14 22:12:22	2021-12-14 22:12:22	2021-12-14 22:12:22		24,689
2	TeamViewer_Setup_x64.exe	2021-12-14 21:59:29	2021-12-14 22:12:22	2021-12-14 22:00:41		34,898,264

CSDN @shu天

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

刷新 详情/预览 高级过滤

- JiaJiaPC-Win10.E01
- ShimCache 424
- AmCache解析 249
- ShellBags 52
- 用户痕迹 113
- 缩略图 679
- win10通知 6
- 快捷方式分析 48
- 基本信息 2066
- IE浏览器 44
- Firefox浏览器 4450
 - 账号信息 2
 - 历史记录 61
 - 书签记录 18
 - 下载记录 6
 - Cookie 46

JiaJiaPC-Win10.E01 > Firefox浏览器 > 保存的密码 > Jia~miao

序号	登录URL	账号	密码
1	https://ctf.show	JiaJia	Miaojia123
2	https://baidu.com	ForesCan	Miaojia123

Cache 4315
保存的密码 2
Jia~miao 2
Edge浏览器 1/8?

CSDN @shu天

Firefox Lockwise 搜索登录信息

顺序: 名称 (A-Z) 2 条登录信息

baidu.com ForesCan	baidu.com 编辑 移除
ctf.show JiaJia	

网址
<https://baidu.com>

用户名
ForesCan 复制

密码
Miaojia123 复制

创建时间: 2021年12月14日
最后修改: 2021年12月14日
上次使用: 2021年12月14日

CSDN @shu天

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