

HGAME-WEEK4-wp

misc Akira之瞳-1

描述

有人想问 Akira 为什么总喜欢用眼睛当头像，Akira 说：“我给你讲个故事吧，从前有一天一位原画师在上班，不幸的是突然起了火灾，情急之下 IT 部门把她没保存的工作 dump 了下来并传到了网上

题目地址

https://1.oss.hgame2021.vidar.club/important_work_bf81f2db20bfa2045a4cd2f6e6214544.7z

wp

下载得到后缀为raw的文件，又根据题目描述“dump”，得知使用volatility工具分析。

ps：难受的是，由于python2的原因kali2020版本已经废除volatility工具，虽然可以手动下载源码安装（kali-linux和windows都可以），但实测发现使用起来十分麻烦，还是尝试在Ubuntu下使用，发现Ubuntu20.04可以直接下载安装volatility。

先按如下输入命令：

```
ubuntu@ubuntu:~/Desktop$ volatility -f 2.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/ubuntu/Desktop/2.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003ff7120L
Number of Processors : 16
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff80003ff9000L
KPCR for CPU 1 : 0xffffffff80004500000L
KPCR for CPU 2 : 0xffffffff8000457d000L
KPCR for CPU 3 : 0xffffffff800009b9000L
KPCR for CPU 4 : 0xffffffff80004654000L
KPCR for CPU 5 : 0xffffffff800046d1000L
KPCR for CPU 6 : 0xffffffff8000474e000L
KPCR for CPU 7 : 0xffffffff800047cb000L
KPCR for CPU 8 : 0xffffffff80004848000L
KPCR for CPU 9 : 0xffffffff800048c5000L
KPCR for CPU 10 : 0xffffffff80004942000L
KPCR for CPU 11 : 0xffffffff800049bf000L
KPCR for CPU 12 : 0xffffffff80004a40000L
KPCR for CPU 13 : 0xffffffff80004abd000L
KPCR for CPU 14 : 0xffffffff80004b3a000L
KPCR for CPU 15 : 0xffffffff80004bb7000L
KUSER_SHARED_DATA : 0xffffffff78000000000L
```

得到：

Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418

ps：以下涉及到的步骤都使用了第一个“Win7SP1x64”

然后如下图操作，获得命令行记录：

```

ubuntu@ubuntu:~/Desktop$ volatility -f 1.raw --profile=Win7SP1x64 cmdline
Volatility Foundation Volatility Framework 2.6.1
*****
System pid:      4
*****
smss.exe pid:    364
Command line :   \SystemRoot\System32\smss.exe
*****
csrss.exe pid:   456
Command line :   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=0n SubSystemType=Wind
ws ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssr
v,4 ProfileControl=Off MaxRequestThreads=16
*****
wininit.exe pid: 500
Command line :   wininit.exe
*****
csrss.exe pid:   520
Command line :   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=0n SubSystemType=Wind
ws ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssr
v,4 ProfileControl=Off MaxRequestThreads=16
*****
services.exe pid: 568
Command line :   C:\Windows\system32\services.exe
*****

```

往下拉，发现其中有一步可疑的操作：

```

important_work pid: 1092
Command line : "C:\Users\Genga03\Desktop\important_work.exe" C:\Users\Genga03\Desktop\work.zip
*****

```

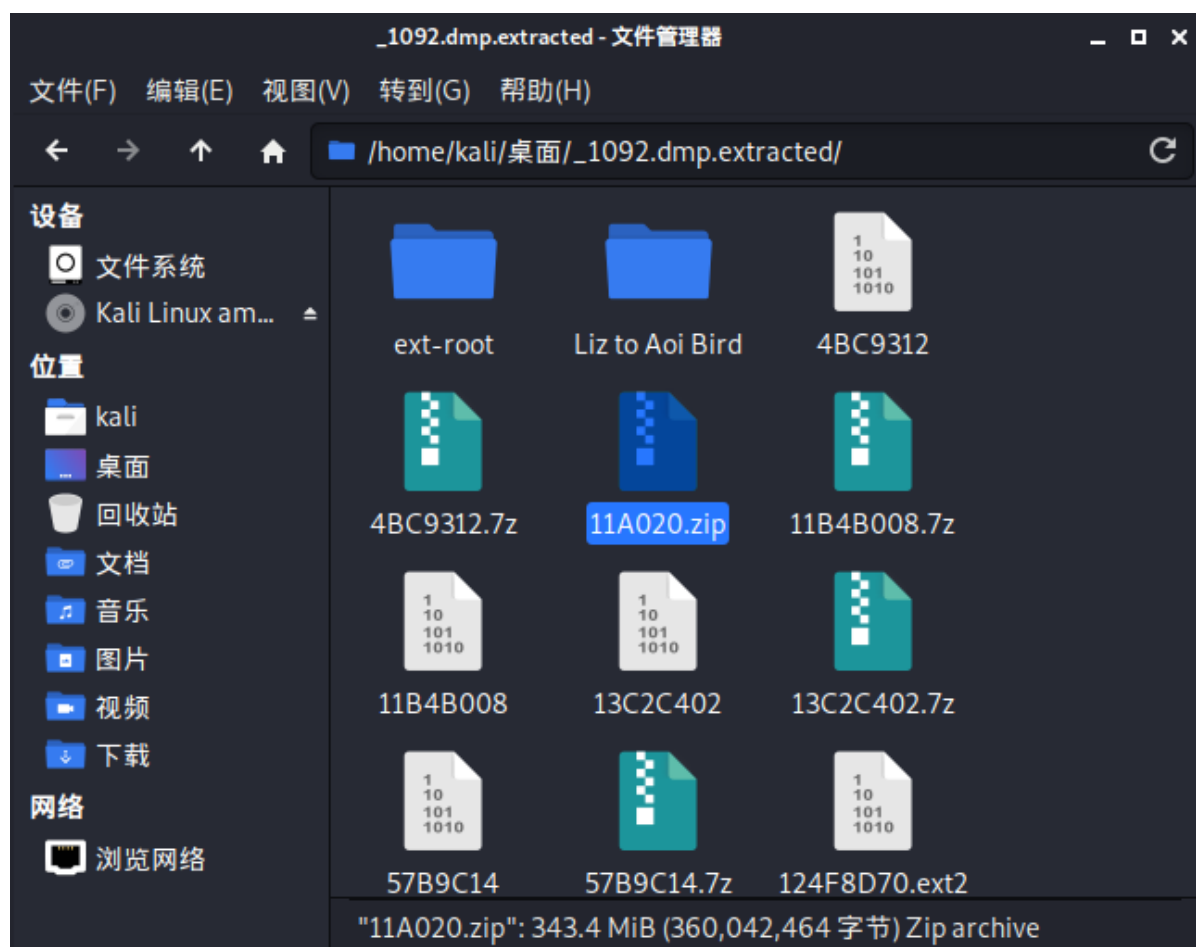
记下 pid: 1092，然后如下操作，意为提取出可疑步骤的文件，并以dmp文件形式保存在文件夹3中

```

ubuntu@ubuntu:~/Desktop$ volatility -f 1.raw --profile=Win7SP1x64 memdump -p 1092 -D 3
Volatility Foundation Volatility Framework 2.6.1
*****
Writing important_work [ 1092] to 1092.dmp

```

因为不熟悉ubuntu的工具，所以将 1092.dmp 复制粘贴到kali中，利用binwalk分离文件，得到：



复制 11A020.zip 到本机，发现解压需要密码，但也发现备注信息：

错误 password is sha256(login_password)

所以要先拿到登陆密码（利用hashdump命令）：

```
ubuntu@ubuntu:~/Desktop$ volatility -f 1.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

查阅资料得知密码就是上面的:

```
84b0d9c9f830238933e7131d60ac6436
```

利用工具: <https://www.cmd5.com/> 得到:

```
asdqwe123
```

再利用sha256加密, 得到压缩文件的密码:

```
20504cdfddaad0b590ca53c4861edd4f5f5cf9c348c38295bd2dbf0e91bca4c3
```

提取文件, 发现两张图片, 根据提示blind, 应该需要用到 BlindWaterMark-master

下载链接: <https://github.com/chishaxie/BlindWaterMark>

如下图操作, 可以得到水印图 1.png:

```
PS C:\ctf\工具\BlindWaterMark-master> python bwmforpy3.py decode src.png Blind.png 1.png
image<src.png> + image(encoded)<Blind.png> -> watermark<1.png>
```

打开1.png, 放大可勉强看清flag (实测用StegSolove查看会清楚一些):



得到flag:

```
hgame{7he_f1ame_brin9s_me_end1ess_9rief}
```

misc Akira之瞳-2

描述

.....

"最后呢? "

"最后她还是没能幸免, 人们在保险箱旁发现了她烧焦的尸体, 打开保险箱人们发现了一个U盘, 是她将回家画好的原稿带来时用的"

题目地址

https://1.oss.hgame2021.vidar.club/secret_work_bd40aea1c133a4d6422925deccb139e9.7z

wp

与上题一样, 还是先查看profile值:

```

ubuntu@ubuntu:~/Desktop$ volatility -f 2.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/ubuntu/Desktop/2.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003ff7120L
Number of Processors : 16
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80003ff9000L
KPCR for CPU 1 : 0xfffff8000450000L
KPCR for CPU 2 : 0xfffff8000457d000L
KPCR for CPU 3 : 0xfffff800009b9000L
KPCR for CPU 4 : 0xfffff80004654000L
KPCR for CPU 5 : 0xfffff800046d1000L
KPCR for CPU 6 : 0xfffff8000474e000L
KPCR for CPU 7 : 0xfffff800047cb000L
KPCR for CPU 8 : 0xfffff80004848000L
KPCR for CPU 9 : 0xfffff800048c5000L
KPCR for CPU 10 : 0xfffff80004942000L
KPCR for CPU 11 : 0xfffff800049bf000L
KPCR for CPU 12 : 0xfffff80004a40000L
KPCR for CPU 13 : 0xfffff80004abd000L
KPCR for CPU 14 : 0xfffff80004b3a000L
KPCR for CPU 15 : 0xfffff80004bb7000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2021-02-19 08:23:04 UTC+0000
Image local date and time : 2021-02-19 16:23:04 +0800

```

然后扫描文件，并加上筛选条件 (txt)：

```

ubuntu@ubuntu:~/Desktop$ volatility -f 2.raw --profile=Win7SP1x64 filescan |grep txt
Volatility Foundation Volatility Framework 2.6.1
0x000000003ee1f070 20 2 -W-rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware_VGAuth\logfile.txt.0
0x000000003efb7f20 16 0 R--rw- \Device\HarddiskVolume1\Windows\KMS10\请勿删除此目录文件.txt
0x000000007ecdd2e0 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\vistasidebar.txt
0x000000007ecddbc0 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\googledesktop.txt
0x000000007ecde070 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\adobeFlashcs3.txt
0x000000007ecde320 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
0x000000007ece0590 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\adobePhotoshopcs3.txt
0x000000007ece08f0 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
0x000000007ece1660 2 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\win7gadgets.txt
0x000000007ece1c10 16 0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
0x000000007ed83300 2 0 RW-rw- \Device\HarddiskVolume1\Users\Genga03\AppData\Roaming\Microsoft\Windows\Recent\cmp1.txt.Lnk
0x000000007ef94820 2 0 RW-rw- \Device\HarddiskVolume1\Users\Genga03\Desktop\dumpme.txt
0x000000007efbb000 1 1 -W-rw- \Device\HarddiskVolume1\Users\Genga03\AppData\Local\Temp\FXSAPIDebugLogFile.txt
0x000000007f26d330 1 0 R--rw- \Device\HarddiskVolume1\Program Files\7-Zip\Lang\zh-cn.txt
0x000000007f2b5f20 2 0 RW-rw- \Device\HarddiskVolume1\Users\Genga03\AppData\Roaming\Microsoft\Windows\Recent\dumpme.txt.Lnk
nk
0x000000007f497ea0 2 0 RW-rw- \Device\HarddiskVolume1\Users\Genga03\AppData\Roaming\Microsoft\Windows\Recent\cmp2.txt.Lnk
0x000000007f5be180 16 0 R--rwd \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\manifest.txt

```

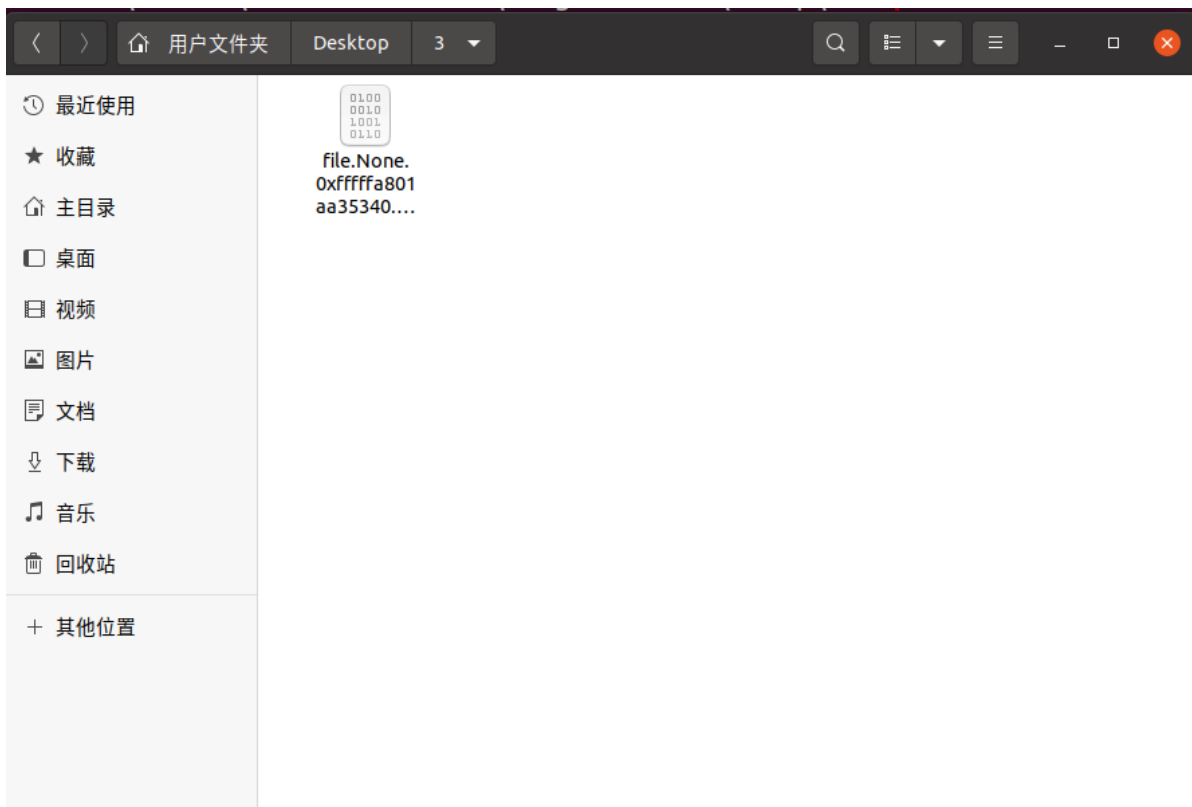
发现可疑(白给)文件：0x000000007ef94820: dumpme.txt，所以dump它：

```

ubuntu@ubuntu:~/Desktop$ volatility -f 2.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007ef94820 -D 3
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7ef94820 None \Device\HarddiskVolume1\Users\Genga03\Desktop\dumpme.txt

```

在文件夹3中得到文件：



将该文件拖到主机，并用notepad++打开，得到：

```
zip password is: 5trqES&P43#y&1TO
And you may need LastPass
```

然后千辛万苦找到lastpass插件，结果我在Ubuntu里volatility的环境又不能用了，只好回到本机用volatility官网下的程序运行：

```
PS C:\> D:\.ctf\工具\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone.exe --plugins=C:\
.volatility_plugins-master\lastpass -f ctf\Akira之瞳-2\secret_work.raw --profile=Win7SP1x64 lastpass
Volatility Foundation Volatility Framework 2.6
Searching for LastPass Signatures
Found pattern in Process: chrome.exe (3948)
Found pattern in Process: chrome.exe (3948)
Found pattern in Process: chrome.exe (3948)
Found pattern in Process: chrome.exe (3948)
Found pattern in Process: chrome.exe (2916)
Found pattern in Process: chrome.exe (2916)
Found pattern in Process: chrome.exe (2916)
Found pattern in Process: chrome.exe (2916)
Found pattern in Process: chrome.exe (2916)
Found pattern in Process: chrome.exe (1160)
Found pattern in Process: chrome.exe (1160)
Found pattern in Process: chrome.exe (1160)
Found pattern in Process: chrome.exe (1160)
```

```
Found LastPass Entry for live.com
UserName: windows login & miscrosoft
Password: Unknown

Found LastPass Entry for live.com,bing.com,hotmail.com,live.com,microsoft.com,msn.com,windows.com,windowazure.com,offic
e.com,skype.com,azure.com
UserName: windows login & miscrosoft
Password: vIg*mq3x6GFa5aFBA

Found Private Key
LastPassPrivateKey<308204BB020100300D06092A864886F70D01010500048204A5308204A10201000282010100BF794F57D296731F67FD1007B
EB13A7732DE75CEB688A0A0B8A4C9DE5D0757E83F9CE8EED14346977C72C65F2C2834F150D9FB54086531896CDEFD6D8F4A5CCA2D39E0ADC824AA6EE
075579E9C6631588E9474F6891B9D1D4D23E55442FA4E89D6810A764CCCEB224DB045DE8E9B17D3A0E561F96D4F414E775A76EA74031AB0EDAB640D1
D5FFB8B83F77F0CA2D415F9E68CB9DB1AB6028012724AE5674FCC5C0C6085FD2A5C39E785E36C899166120893095779104A123090681914834E063F
D433E0F54A221BFA6B344F76B270D1FB5FBC5A7385911A0222A65FD7FDA3573F1A9C8C8B75003664DC998FB6BA8048D65F0A44A23E1446E299A43232
80A13ED02011028201000B435F052A815210E7FFD3C43864C734302B341B37E9EB54BF91390D1487F61CB872A44A488B7C9F7FCA8423B74DA8C2E6A
369230F8D7B626FD0E1B82688E7572FD63A64937AA09D1C43234590BAB79BCC2D6D9B429019FD48C112B9B8B7822BCD061F18E7CFCEC5C855A9C1CC2
73DA30976E7A542AA4F22BBB0A6FE8B87B6468A44BD7E57DA570AB63E1A013AD75AC3B63927D274769E4774B7DC66DC10CA337465A39221C062B9B9
6BF4E8BF484C3F171A40E41B6D32FC417E0A54EEFE8896346947F7CB40B382F2D8AB78D6CD040570FAC76C0497CC3A677B884B6208157E82D42B0CD
675C7F52F58AA221C076F260447584A3F766B9B0103DA11633ED02818100FE8270E2DD0E11837ECDE3E61EED958F59F0FC906A46082A9C38ED50396
8174F233CC4A7E95F1DF125CEDAAF56A374B986883CFD803FCE883378DCBB43EBDBB631E6069D3151572368206134BB850E3B47638CE5CB4F4A742D
30D87876BB76ACEEA9A0EB68B5301A5E730C976F660693BA37E9A73F66140F3EE3E6058687B702818100C0985DC66AD2251EB0A59F5C2F2A4D1228
B14BDABA74FD178EADD30D33B0E9FF1DD45ECA5A3CC7FD8CA7E1F7361B63FA1C7387B3A0CC6CECF7B9D8C558938E33AD5AFADB5C0BE11C8CAD924B6
82A9EA68DC53616C2D3FAD16417A5E045E732F60F17DDF1A67BEEEB46CA9A0FFDD6A0B9D1E08F7DBE7087C5AA4B25700A197B0281801DF13A750AF29
8A60EE80BC085821C076F260447584A3F766B9B0103DA11633ED02818100FE8270E2DD0E11837ECDE3E61EED958F59F0FC906A46082A9C38ED50396
EE55118A0D6FD30FC608E881FCABD1AC53DECC9FEAA4418D46A4C2ACA48CD0C8A9857EE8DC96C8395108A49574C116133C122BC2A207A43A2574BF1B
59D0281805AA20E03051797AE14411B4679DB98DAE31445FEE75DCB35661428DABDC1704B44A45D24119B67E5A47E6D1F0AEC491FFD3A90885487E7B
BAD2948676BEDC06AE82AD0673A5FF176D8CA26BA12E6E13F51C637923D909E80A792A8698A4EA91E8FC2C357B859D9BE5140C43C2BF5AB1CC2D7
0B3A4E9A94DF5C9028F13FC102818100AAFE94334DE0035FE8673623497290B50059E6176FB785D83A2EA157C2E3B335E2E264DC5D7EB873E0348E7
578D956F1AF59E81D9FC24FFB23A61B262184A0B06B4A0F79A750E0EF776646CFF6ACBD2A2A4CFFBDEC64DA06F05A76A8028CC3E0D487A21C4EADA7
34DADEDC8280528892E07FBC98DC47B0E2ED1E69EDA479D05>LastPassPrivateKey
```

接下来应该是解密cookies

但题解写到这里就下不去了。。。终于还是失败了

是misc的魅力吸引我一次次去尝试，真的能让我感受到，仰止弥高，钻之弥坚，再尝试一次就能更接近一些