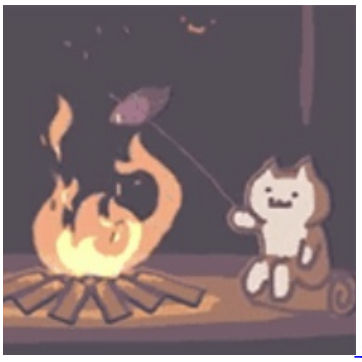
[2021首届“陇剑杯”网络安全大赛 决赛]内存取证writeup

原创

shu天 于 2021-11-24 21:26:39 发布 2897 收藏 5

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



ctf 同时被 3 个专栏收录

81 篇文章 4 订阅

订阅专栏

misc

7 篇文章 0 订阅

订阅专栏

内存取证

6 篇文章 1 订阅

订阅专栏

~~决赛不能联网…手上有只有vol2.6，这道题完全死了~~

文章目录

[2021首届“陇剑杯”网络安全大赛 决赛]内存取证 writeup

附件：mem_sec.vmem

> 1.一日运维人员针对被入侵主机进行了一次内存分析，请根据内存镜像进行分析并回答下述问题。请根据u盘里的mem_sec.zip文件进行分析。取证人员首先对主机信息进行核实，该内存主机的产品密钥是__K3KHX-TCQKF-WGFXC-7T3BJ-9TPJC__。（答案格式字符全部大写）
> 2.经过入侵分析发现该主机的使用人员曾经访问过匿名邮箱的网址是_____。(答案包含http://或者https://，答案最后没有/)
> 1https://mail.td??? 2john@uuf.me
> 3.经过入侵分析该主机曾被植入远控后门，该远控后门被植入时的文件路径为_____。（填写绝对路径）
> C:\Users\Ado\Downloads\steam.exe C:\users\ado\downloads\steam.exe
> 4.经过入侵分析该主机曾使用工具进行过痕迹清除，最后一次进行数据清除的时间是_____。（时区为UTC+8，填写格式为yyyy-mm-dd hh:mm:ss）

vmem是虚拟机的内存文件，因为该题是win10的虚拟机，只有vol3可以解析（https://blog.csdn.net/weixin_46081055/article/details/120524660）

产品密钥

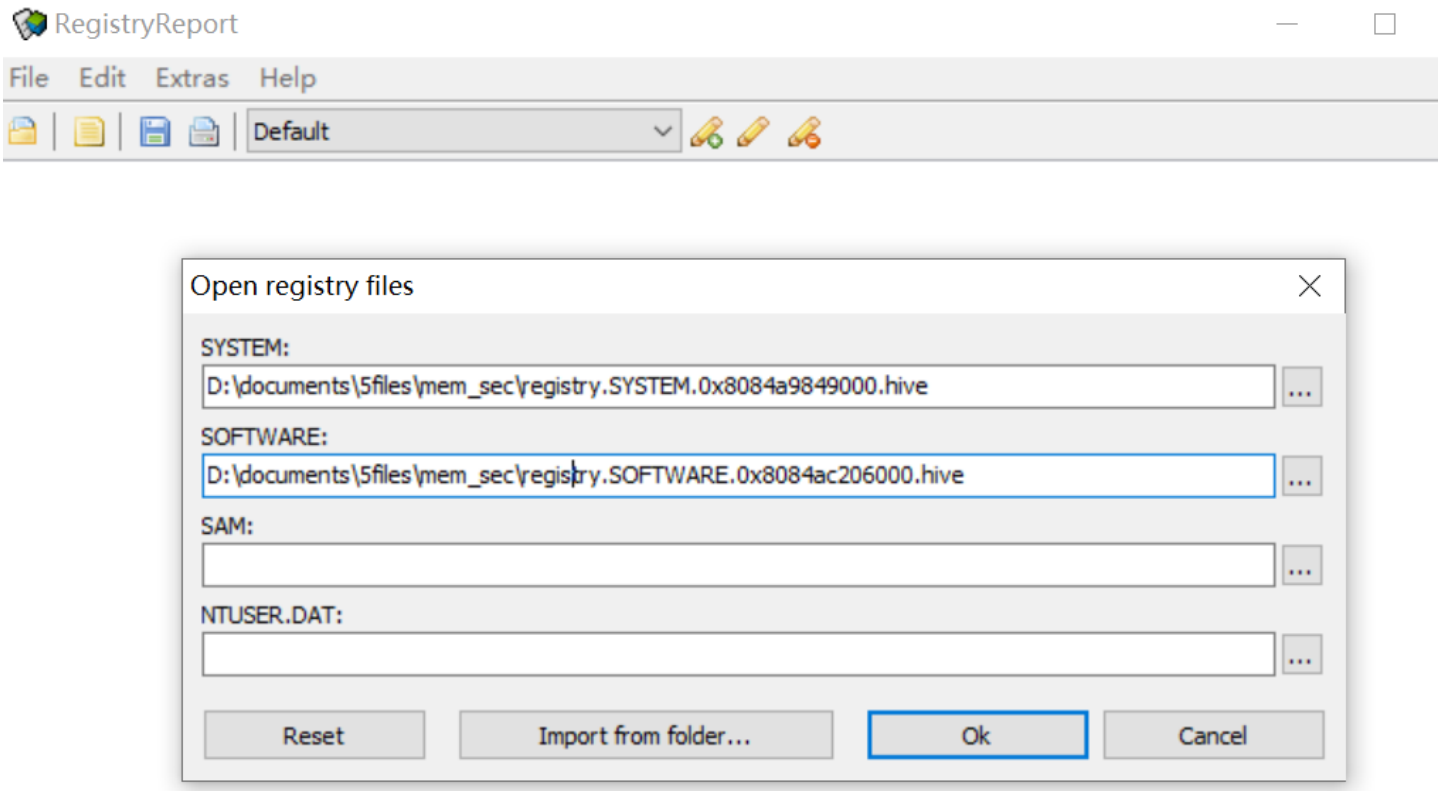
产品密钥在注册表中可以看到

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`右侧的BackupProductKeyDefault值

```
$ python3 vol.py -f mem_sec.vmem windows.registry.hivelist

Volatility 3 Framework 1.2.1
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0x8084a980e000          Disabled
0x8084a9849000  \REGISTRY\MACHINE\SYSTEM        Disabled
0x8084a9881000  \REGISTRY\MACHINE\HARDWARE      Disabled
0x8084ac204000  \SystemRoot\System32\Config\SECURITY    Disabled
0x8084ac232000  \SystemRoot\System32\Config\DEFAULT     Disabled
0x8084ac230000  \SystemRoot\System32\Config\SAM Disabled
0x8084ac206000  \SystemRoot\System32\Config\SOFTWARE    Disabled
0x8084ad13e000  \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD  Disabled
0x8084ad392000  \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT        Disabled
0x8084ad522000  \SystemRoot\System32\Config\BBI Disabled
0x8084ad4e3000  \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0x8084aea0c000  \??\C:\Windows\AppCompat\Programs\Amcache.hve   Disabled
0x8084aea26000  \??\C:\Users\Ado\ntuser.dat     Disabled
0x8084ae973000  \??\C:\Users\Ado\AppData\Local\Microsoft\Windows\UsrClass.dat   Disabled
0x8084af0b1000  \REGISTRY\A\{FE82E83E-F53E-4F85-85C5-C721392AB949}      Disabled
0x8084af152000  \??\C:\Users\Ado\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\
Settings\settings.dat   Disabled
0x8084af1d2000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.13.0.183
62_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat Disabled
0x8084af1de000  \??\C:\Users\Ado\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\setting
s.dat   Disabled
0x8084aea5a000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.MicrosoftEdge_44.18362.449
.0_neutral__8wekyb3d8bbwe\ActivationStore.dat        Disabled
0x8084af3dd000  \REGISTRY\A\{6cc7ad55-7bbf-baae-93d4-e961bbc241ec}      Disabled
0x8084af997000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\InputApp_1000.18362.449.0_neutral_ne
utral_cw5n1h2txyewy\ActivationStore.dat      Disabled
0x8084af90e000  \??\C:\Users\Ado\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat    Disabled
0x8084b270f000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.SecHealthUI_10.0.1
8362.449_neutral__cw5n1h2txyewy\ActivationStore.dat  Disabled
0x8084b2bf0000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHos
t_10.0.18362.449_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat   Disabled
0x8084b2c1a000  \??\C:\Users\Ado\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Sett
ings\settings.dat       Disabled
0x8084b39e9000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.WindowsStore_11811.1001.18
.0_x64__8wekyb3d8bbwe\ActivationStore.dat    Disabled
0x8084b3a03000  \??\C:\Users\Ado\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.d
at      Disabled
0x8084b3a77000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.OneConnect_5.1902.361.0_x6
4__8wekyb3d8bbwe\ActivationStore.datDisabled
0x8084b3a96000  \??\C:\Users\Ado\AppData\Local\Packages\Microsoft.OneConnect_8wekyb3d8bbwe\Settings\settings.dat
        Disabled
0x8084b3d4a000  \??\C:\Windows\System32\config\COMPONENTS       Disabled
0x8084b3d7b000  \SystemRoot\System32\config\DRIVERS     Disabled
```

导出注册表，生成report（SAM和NT都没取下来）

```
$ python3 vol.py -f mem_sec.vmem  windows.registry.hivelist --dump --filter "\REGISTRY\MACHINE\SYSTEM"

Volatility 3 Framework 1.2.1
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0x8084a9849000  \REGISTRY\MACHINE\SYSTEM        registry.SYSTEM.0x8084a9849000.hive

 python3 vol.py -f mem_sec.vmem  windows.registry.hivelist --dump --filter "\SystemRoot\System32\Config\SOFTWARE
"
```



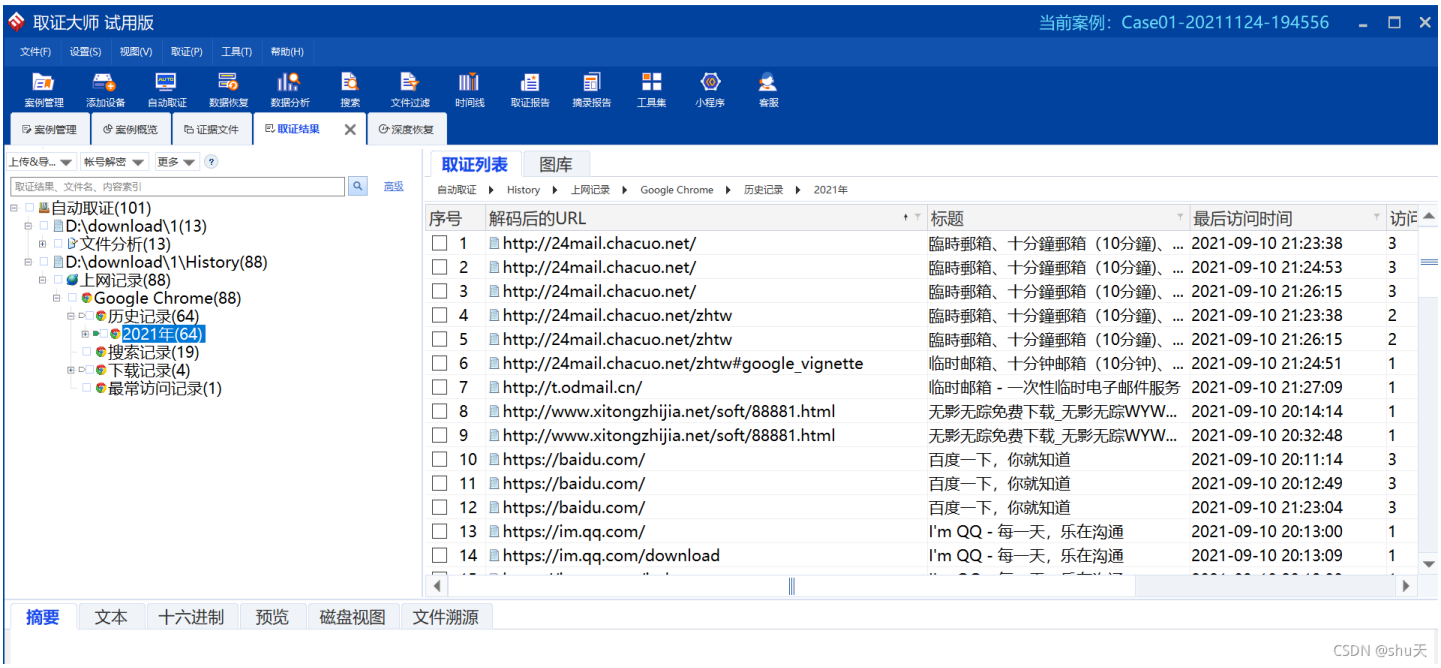

```
Report generation started at 2021/9/28 16:36:56.
================================================================================

Operating System
================

  Operating system:  Windows 10 Education
  Version number:    6.3.18363
  Build label:       18362.19h1_release.190318-1202
  Build label:       18362.1.amd64fre.19h1_release.190318-1202
  Product type:      Multiprocessor Free
  Product Id:        00328-10000-00001-AA506
  Product key:       K3KHX-TCQKF-WGFXC-7T3BJ-9TPJC
  Boot directory:    C:\
  Install date:      2021/9/10 12:07:31 UTC
  Installed in:      C:\Windows
  Installed from CD: No
  Activated:         No
  Reg. user:         Windows (7
  Current Shell:     explorer.exe

  Setup:
    Boot directory:      C:\

  User profiles:
```


Product key: K3KHX-TCQKF-WGFXC-7T3BJ-9TPJC

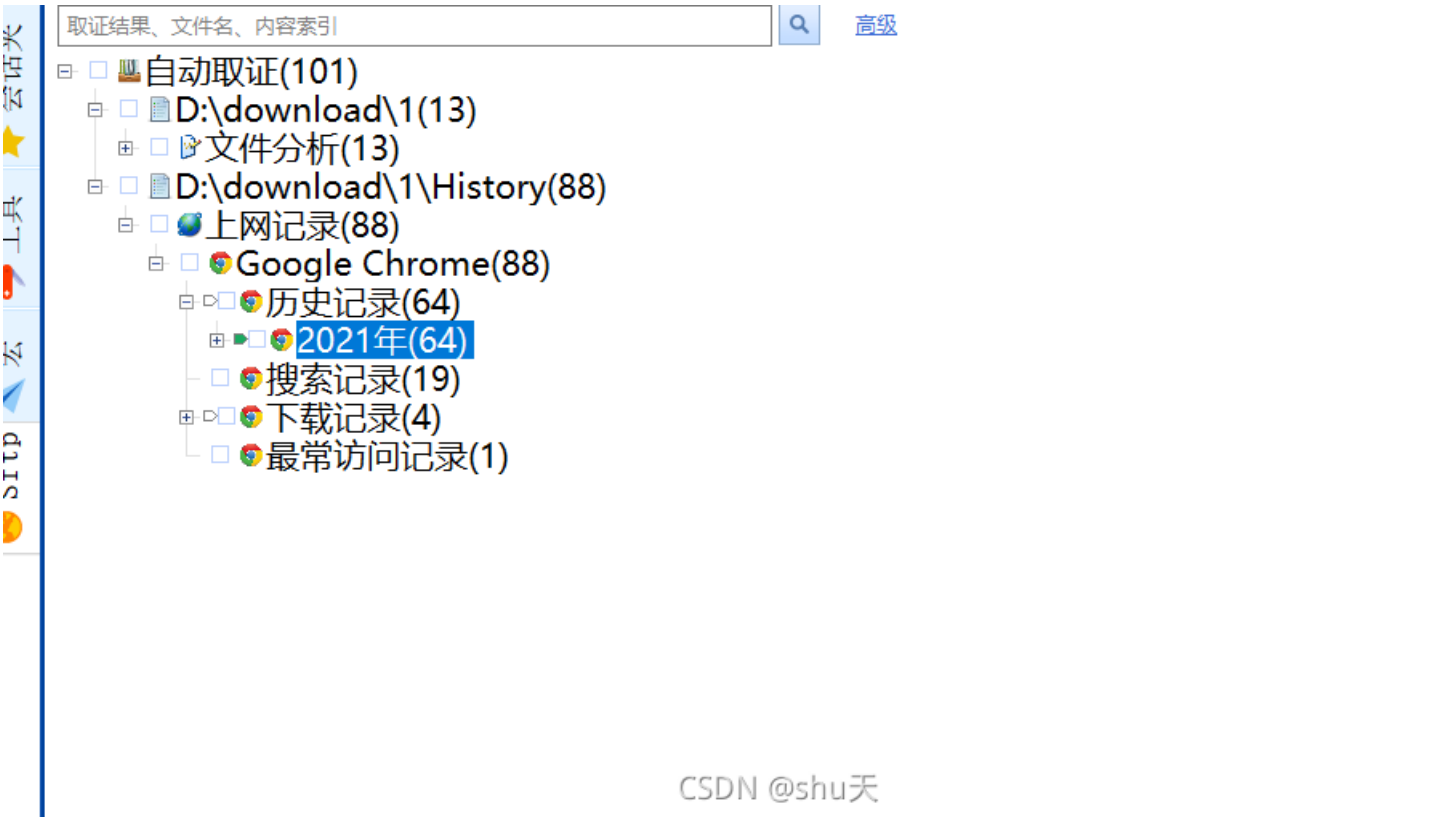
匿名邮箱

filescan找到谷歌浏览器历史记录文件，filedumps下来

```
0xcf0e4c04ab20 \Users\Ado\AppData\Local\Google\Chrome\User Data\Default\History 216
```



可以看到嫌疑人访问过这几个临时邮箱



远控后门

他有两个steam，一个是正常安装的（C:\Program Files (x86)\下的），另一个是downloads下面的
正常的steam会开启很多子进程（steamhelper之类），恶意程序则没有

```
python3 vol.py -f mem_sec.vmem windows.cmdline
```

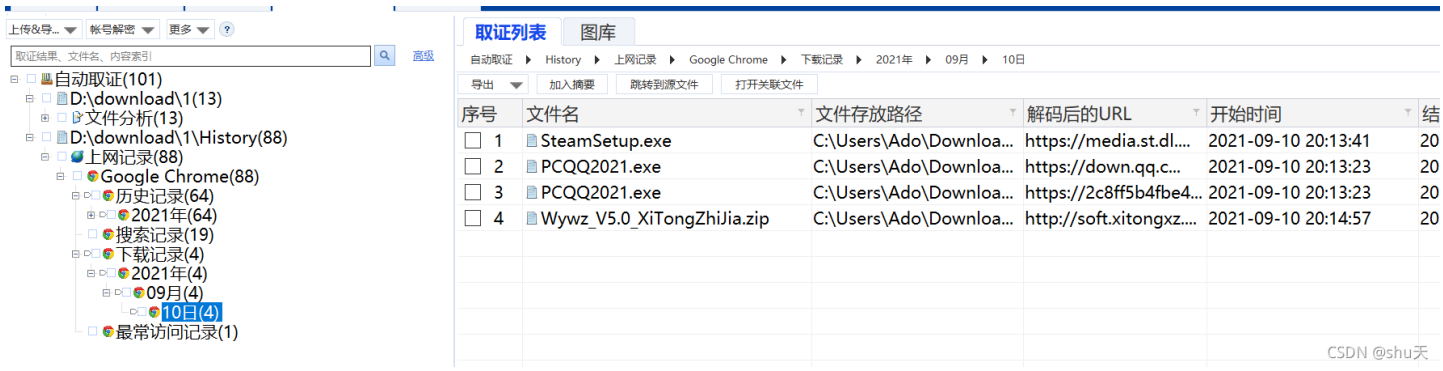
结果：

```
6864 steam.exe Required memory at 0xbf1b88 is inaccessible (swapped)
6932 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" "-lang=zh_CN" "-cached
ir=C:\Users\Ado\AppData\Local\Steam\htmlcache" "-steampid=6864" "-buildid=1631237534" "-steamid=0" "-cachedir=C:
\Users\Ado\AppData\Local\Steam\htmlcache" "-steamuniverse=Public" "-realm=Global" "-clientui=C:\Program Files (x
86)\Steam\clientui" --enable-blink-features=ResizeObserver,Worklet,AudioWorklet --enable-media-stream --enable-s
mooth-scrolling --enable-direct-write "--log-file=C:\Program Files (x86)\Steam\logs\cef_log.txt" --disable-quick
-menu
6960 steamwebhelper Required memory at 0x23777471d18 is inaccessible (swapped)
6996 steamservice.e Required memory at 0x101a020 is inaccessible (swapped)
7072 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" --type=gpu-process --f
ield-trial-handle=1504,1780523561363773034,14588998028209356534,131072 --disable-features=MimeHandlerViewInCross
ProcessFrame --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --product-version="Valve Steam Client" -
-lang=zh-CN --buildid=1631237534 --steamid=0 --gpu-preferences=KAAAAAAAAADgAAAwAAAAAAAAAYAAAAAAAEAAAAAAAAAAAAAAAA
AAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAA
QAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --service-request-cha
nnel-token=8367268148546171292 --mojo-platform-channel-handle=1512 --ignored=" --type=renderer " /prefetch:2
6356 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" --type=utility --field
-trial-handle=1504,1780523561363773034,14588998028209356534,131072 --disable-features=MimeHandlerViewInCrossProc
essFrame --lang=zh-CN --service-sandbox-type=network --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt"
--product-version="Valve Steam Client" --lang=zh-CN --buildid=1631237534 --steamid=0 --log-file="C:\Program File
s (x86)\Steam\logs\cef_log.txt" --service-request-channel-token=3596301750699654214 --mojo-platform-channel-hand
le=1524 /prefetch:8
……
5004 steam.exe "C:\Users\Ado\Downloads\steam.exe"
……
7140 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" --type=renderer --log-
file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --field-trial-handle=1504,1780523561363773034,1458899802820
9356534,131072 --disable-features=MimeHandlerViewInCrossProcessFrame --enable-blink-features=ResizeObserver,Work
let,AudioWorklet --lang=zh-CN --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --product-version="Valv
e Steam Client" --buildid=1631237534 --steamid=0 --device-scale-factor=1 --num-raster-threads=1 --service-reques
t-channel-token=7050656953433046572 --renderer-client-id=7 --mojo-platform-channel-handle=3260 /prefetch:1
1124 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" --type=renderer --log-
file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --field-trial-handle=1504,1780523561363773034,1458899802820
9356534,131072 --disable-features=MimeHandlerViewInCrossProcessFrame --enable-blink-features=ResizeObserver,Work
let,AudioWorklet --lang=zh-CN --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --product-version="Valv
e Steam Client" --buildid=1631237534 --steamid=0 --device-scale-factor=1 --num-raster-threads=1 --service-reques
t-channel-token=11198636302058458110 --renderer-client-id=8 --mojo-platform-channel-handle=3524 /prefetch:1
8208 steamwebhelper "C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe" --type=renderer --log-
file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --field-trial-handle=1504,1780523561363773034,1458899802820
9356534,131072 --disable-features=MimeHandlerViewInCrossProcessFrame --enable-blink-features=ResizeObserver,Work
let,AudioWorklet --lang=zh-CN --log-file="C:\Program Files (x86)\Steam\logs\cef_log.txt" --product-version="Valv
e Steam Client" --buildid=1631237534 --steamid=0 --device-scale-factor=1 --num-raster-threads=1 --service-reques
t-channel-token=15708242794114963385 --renderer-client-id=9 --mojo-platform-channel-handle=3680 /prefetch:1
```

数据清除时间

第二问的历史记录可以知道，嫌疑人下载过无影无踪

7	http://t.odmail.cn/	临时邮箱 - 一次性临时电子邮件服务	202
8	http://www.xitongzhijia.net/soft/88881.html	无影无踪免费下载_无影无踪WYWZ控制台(系统清理软件)5.0中...	202
9	http://www.xitongzhijia.net/soft/88881.html	无影无踪免费下载_无影无踪WYWZ控制台(系统清理软件)5.0中...	202



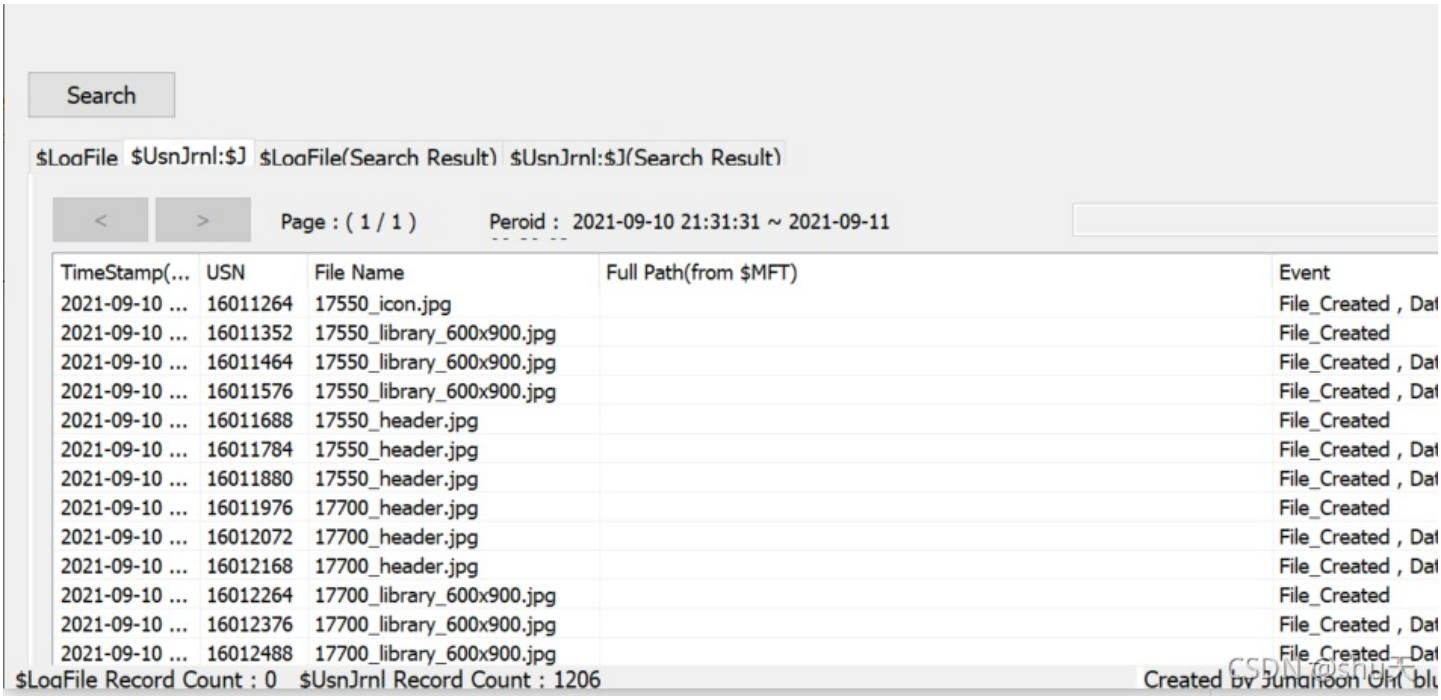
扫描文件

```
python3 vol.py -f mem_sec.vmem windows.filescan > 1/f1ile.txt
```

导出ntfs元文件

```
0xcf0e46c3b1e0 \$Extend\$UsnJrnl:$J:$DATA 216
0xcf0e46c3b4c0 \$LogFile 216
0xcf0e4934d0a0 \$Mft 216

python3 vol.py -f mem_sec.vmem windows.dumpfiles --virtaddr 0xcf0e46c3b1e0
```

生成报告



但是并没有看到实锤...

userassist看一下历史运行

```
python3 vol.py -f "/home/p3/qztool/volatility3/mem_sec.vmem" windows.registry.userassist > user.txt
```

REG_BINARY C:\Users\Ado\Desktop\WYWZ\Wywz.exe :
Count: 1
Focus Count: 1
Time Focused: 0:00:12.484000
Last updated: 2021-09-10 13:10:13 UTC+0000
Raw Data:
0x00000000 00 00 00 00 01 00 00 00 01 00 00 00 d0 2e 00 00 ....
0x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf ....
0x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf ....
0x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff b0 cd 1d 31 1
0x00000040 45 a6 d7 01 00 00 00 00 E.......

REG_BINARY Microsoft.Windows.Shell.RunDialog :