2020湖湘杯MISC全解-writeup

原创

Blus.King 于 2020-11-02 18:40:03 发布 3899 收藏 9
分类专栏： CTF/AWD 信息安全 文章标签： 湖湘杯

MISC1

导出index-demo.html，查看代码发现隐藏了一长串base64

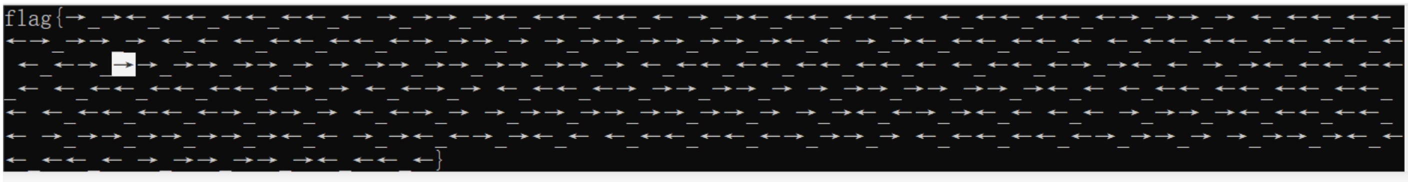
使用base64隐写进行解密

```
key:"lorrie□
0
key:"lorrie□
0
key:"lorrie□
0
key:"lorrie□
0
key:"lorrie□
2
key:"lorrie"
```


key:"lorrie"

得到key说明可能存在某种隐写，是snow隐写，但用网页版的snow隐写解出来是一串乱码，于是尝试使用本地版的SNOW.EXE

```
SNOW.EXE  -p lorrie  index-demo.html
```



```
flag{→_→←_←←_←←_←←_← →_→→_→←_←←_←←_← →_→←_←←_←←_← ←_←←_←←_←→_→→_→
←_←←_←←_←→_→→_→ ←_← ←_←←_←←_←→_→→_→ →_→→_→→_→→_→←_← →_→←_←←_←←_←
←_←←_←←_←←_←←_← ←_←→_→→_→→_→→_→ →_→→_→→_→→_→→_→ ←_←←_←←_←←_←←_←
←_←←_←→_→←_← →_→←_←←_ ←←_← ←_←←_←←_←←_←→_→ ←_←→_→ ←_←←_←→_→→_→→_→
→_→→_→→_→→_→←_← ←_←←_←←_←←_ ←←_← ←_←←_←←_←→_→→_→ ←_←→_→
→_→→_→→_→→_→→_→ →_→←_←→_→←_← ←_← →_→→_→←_←←_←←_← →_→→_→→_→→_→←_←
→_→←_←→_→←_← ←_←←_←←_←→_→→_→ ←_←←_←←_←→_→→_→ →_→→_ →←_←←_←←_←
→_→→_→→_→←_←←_←}
```

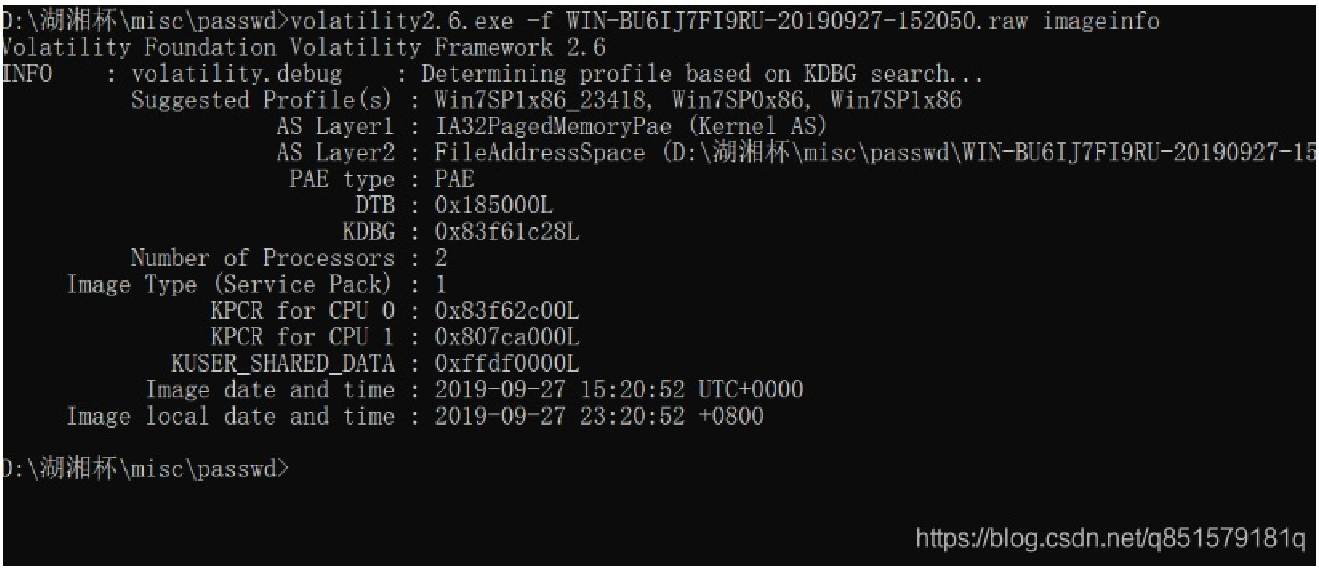
把→_→和→_ →替换成-，把 ←_←和 ←_ ←替换成.，然后摩斯解密，得到

67b33e39b5105fb4a2953a0ce79c3378

MISC2 -passwd

内存取证

```
volatility2.6.exe -f WIN-BU6IJ7FI9RU-20190927-152050.raw imageinfo
```



```
D:\湖湘杯\misc\passwd>volatility2.6.exe -f WIN-BU6IJ7FI9RU-20190927-152050.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\湖湘杯\misc\passwd\WIN-BU6IJ7FI9RU-20190927-15
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x83f61c28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x83f62c00L
                KPCR for CPU 1 : 0x807ca000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-09-27 15:20:52 UTC+0000
     Image local date and time : 2019-09-27 23:20:52 +0800

D:\湖湘杯\misc\passwd>
```

Win7SP1x86_23418, Win7SP0x86, Win7SP1x86

volatility2.6.exe -f WIN-BU6IJ7FI9RU-20190927-152050.raw --profile=Win7SP1x86_23418 hashdump

```
D:\湖湘杯\misc\passwd>volatility2.6.exe -f WIN-BU6IJ7FI9RU-20190927-152050.raw  --profile=Win7SP1x86_23
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CTF:1000:aad3b435b51404eeaad3b435b51404ee:0a640404b5c386ab12092587fe19cd02:::
```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

CTF:1000:aad3b435b51404eeaad3b435b51404ee:0a640404b5c386ab12092587fe19cd02:::

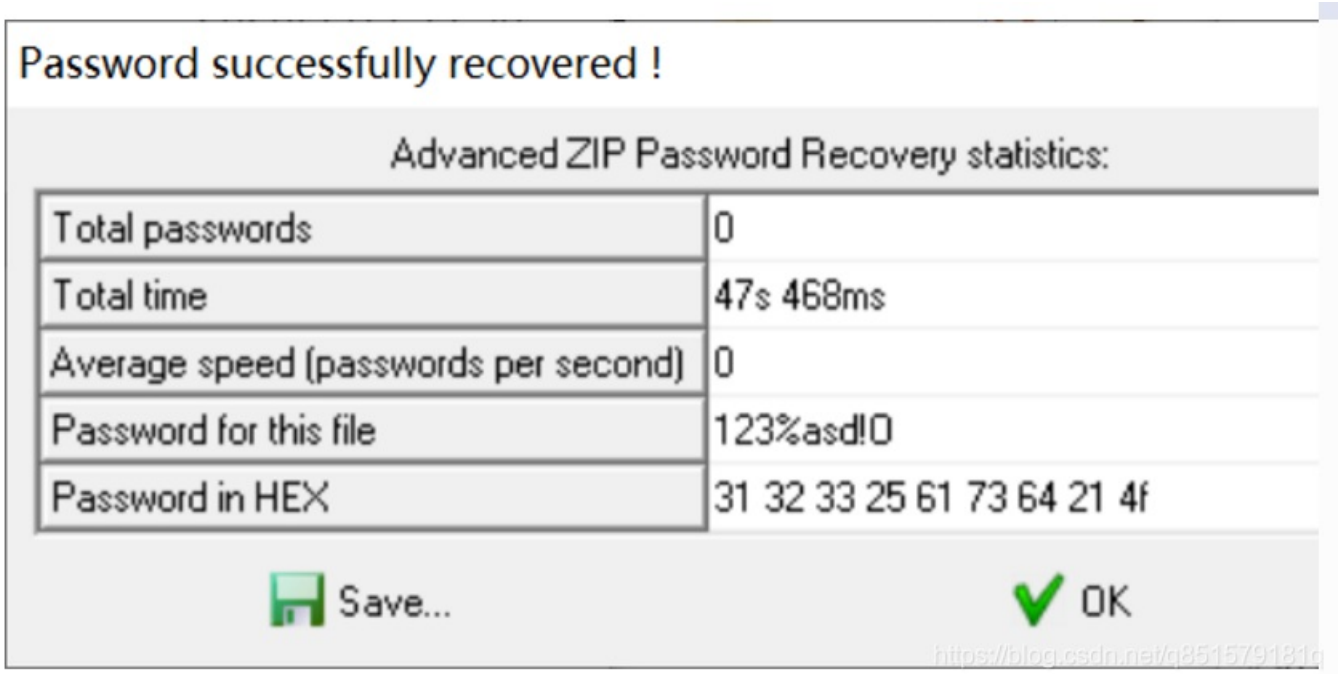
db25f2fc14cd2d2b1e7af307241f548fb03c312a

MISC3-虚实之间

binwalk提取 出一个明文和一个加密的压缩包

修复加密压缩包

使用AZPR4.0进行明文攻击



123%asd!O

解压得到：

> 仅需5，跳过去
>
> ffd5e341le25b2dcab15cbb}gc3bc5b{789b51

栅栏解密：

https://www.qqxiuzi.cn/bianma/zhalanmima.php

flag{febc7d2138555b9ebccb32b554dbb11c}

MISC4 隐藏的秘密

> volatility2.6.exe -f 隐藏的秘密.vmem imageinfo
>
> //Win2003SP0x86, Win2003SP1x86, Win2003SP2x86
>
> volatility2.6.exe -f 隐藏的秘密.vmem --profile=Win2003SP0x86 filescan

windows下文件扫描出错，换成kali下，也不行，把版本换成Win2003SP1x86

> volatility -f 1.vmem --profile=Win2003SP1x86 filescan

```
root@labs-a3:~/blus/1101# volatility  -f 1.vmem --profile=Win2003SP1x86 filescan |grep .txt
Volatility Foundation Volatility Framework 2.6
0x000000000412cde0      1      0 RW-r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\file.txt
0x000000000426b890      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\All Users\Application Data\VMware\
```

> volatility -f 1.vmem --profile=Win2003SP1x86 dumpfiles -Q 0x000000000412cde0 --dump-dir=.

查看文件得到：

> 什么？计算机又被不知名账户登录了？明明在计算机管理中没有这个用户，为什么还会被这个用户登录呢？电脑跟前的你能帮我找到原因吗？flag为该用户的用户名以及密码的md5值
>
> 格式：md5(用户名:密码)

用hashdump会发现有多账户

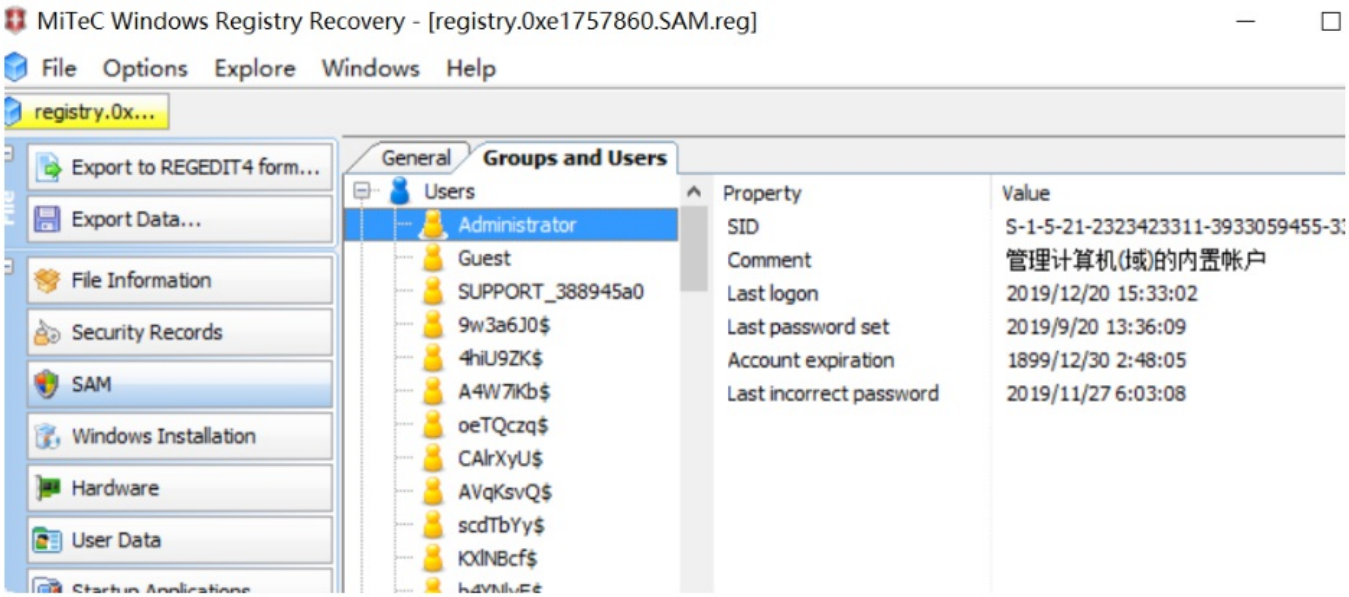
```
Volatility Foundation Volatility Framework 2.6
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8d9221b8e70124641a83291d3d21f7e0:::
9w3a6JO$:1003:e761601f5cf981c136077a718ccdf409:ec9dc7d0895ad3dae1feba8ffdeacffd:::
4hiU9ZK$:1004:de5eea9d3fd12c34aad3b435b51404ee:2f2d544c53b3031f24d63402ea7fb4f9:::
A4W7iKb$:1005:61339c1be342167eaad3b435b51404ee:b6e6f6a85f90219d619aca4706f354fc:::
oeTQczq$:1006:b4d2cf4a862f6fcaaad3b435b51404ee:3fbc1f9dc4416f6fb3666de834185cb4:::
CAlrXyU$:1007:8ea6fb8594a1b952aad3b435b51404ee:51d603c77a884df049f7ed4dabed4fd4:::
AVqKsvQ$:1008:939e0f8990e68047aad3b435b51404ee:1796c2db94ce6276744f88b740152154:::
scdTbYy$:1009:792677ee54a26732891c5133c13673e8:138393419f9b418eb735d36e1da50a5e:::
KXlNBcf$:1010:17c6f830172f2731b75e0c8d76954a50:25c93091cdfabe015d6770734eb9024a:::
b4YNlvE$:1011:c827216bbf0c654d0ce4e57c62586573:b6bb4ce745d55b2f4bb87768c27bbbae:::
vxy921o$:1012:1e0ac88abba020c94827253349babf0f:476b1879238bea3eb0fe93575c76643e:::
Yl2GjDd$:1013:0182bd0bd4444bf838a0a8035a6a24c3:184dd4b8727cdbeaccb650da0579411b:::
fM8xa10$:1014:c7418a726d8b057faad3b435b51404ee:e807b0191fb9571ac66fdea1f2cc36c0:::
BMubfrk$:1015:17c6f830172f2731b75e0c8d76954a50:25c93091cdfabe015d6770734eb9024a:::
QrptqJl$:1016:4cd720fc5c37c747eacbeb9271fb3e7a:b9c0cbb8bba37e05b858d99864b5eb3a:::
flicduJ$:1017:e2302b9a91361d152b999340d53adc02:1600177b90b941691a5058540729b42e:::
jNXqO9a$:1018:58cdc0fa6c5fefb4aad3b435b51404ee:9e4b2858cab5d304d34413a0aabd2545:::
3ndmDSk$:1019:97ce1f5c10f5980baad3b435b51404ee:841f779368eff4c81bbc65e77191ecac:::
qpAZlPh$:1020:2d8c041ffa91df73aad3b435b51404ee:700ec8a682f6e41418007992fc604c77:::
qZGx64P$:1021:d986246dc1eab595c6ebe8776a153feb:61c5b38f4874f0effa68e165abba5e8e:::
JE71YxI$:1022:4001a65f34fec9e1aad3b435b51404ee:c8a71e6fd71767a0fba2d7419e1dd872:::
v86jpGa$:1023:ff5365e2b3a4f74c8eefe33a7f9bee0d:a854fab01395abacb0aca80c1a1e923c:::
1wqHfyP$:1024:9f4936a68670a3edaad3b435b51404ee:e16b2773ce02394bfcf44774d407caa7:::
YZQ6Oax$:1025:d1a5321ed4cd4d7072d3f90e28c9734d:4f63c2aa548d58aadbf66e612a2ae0df:::
```

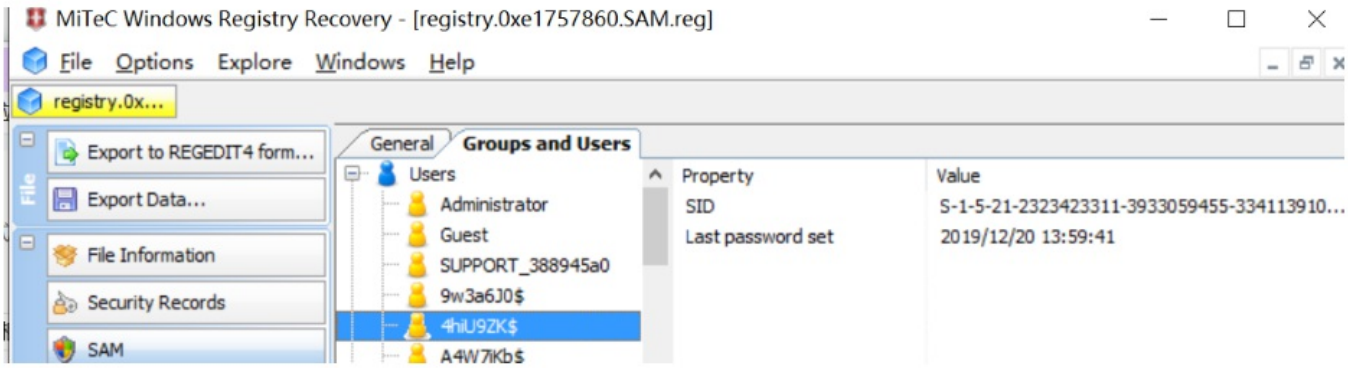

导出注册表

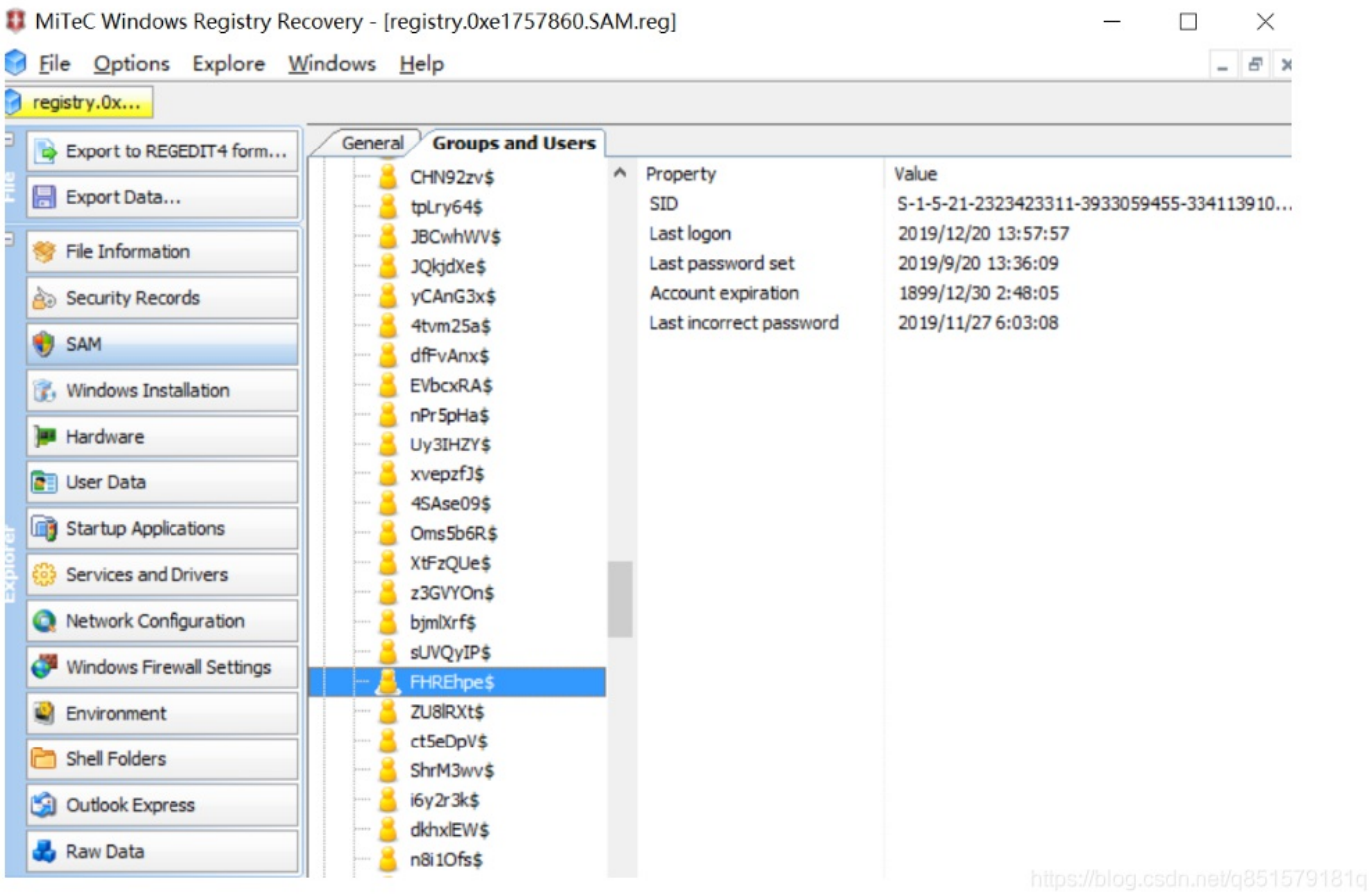
volatility -f 1.vmem --profile=Win2003SP1x86 dumpregistry --dump-dir= .

用注册表分析工具打开registry.0xe1757860.SAM.reg，分析用户。

可以看到，Administrator是有登录记录的，其他账户是没有登录记录的。一个个查看下去发现账户FHREhpe$的记录与Administrator相同







FHREhpe$

> volatility -f 1.vmem --profile=Win2003SP1x86 hashdump |grep FHREhpe

```
root@labs-a3:~/blus/1101# volatility  -f 1.vmem --profile=Win2003SP1x86 hashdump |grep FHREhpe
Volatility Foundation Volatility Framework 2.6
FHREhpe$:1171:70fdb8f853bd427d7584248b8d2c9f9e:f3cf477fc3ea6ec0b3b5887616dd4506:::
```

> FHREhpe$:1171:70fdb8f853bd427d7584248b8d2c9f9e:f3cf477fc3ea6ec0b3b5887616dd4506:::

根据题意做md5

FHREhpe$:NIAIWOMA

8cf1d5b00c27cb8284bce9ccecb09fb7