BuuCTF难题详解| Misc | V&N 2020 公开赛 内存取证

原创

水星Sur 于 2020-10-29 18:21:20 发布 1200 收藏 6

分类专栏： BUUCTF Misc CTF 文章标签： 信息安全 ctf buuctf

本文链接：https://blog.csdn.net/pone2233/article/details/109340009

BUUCTF 同时被 3 个专栏收录

21 篇文章 2 订阅

订阅专栏

Misc

22 篇文章 0 订阅

订阅专栏

CTF

20 篇文章 0 订阅

订阅专栏

题目介绍

这道题目，我们要在Buu上面做需要的步骤需要调整，先下载链接内容，然后在下载附加。

BuuCTF难题详解| Misc | V&N 2020 公开赛 内存取证

P1

我们使用volatility，进行镜像分析

> volatility -f mem.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 (xxxxxxx\[内存取证]volatility\mem.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x8176bbe8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x8176cc00L
                KPCR for CPU 1 : 0x807ec000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-02-18 19:56:24 UTC+0000
     Image local date and time : 2020-02-19 03:56:24 +0800
```

这里咋们知道了这个的系统是Win7SP1x86_23418

P2

查看进程

> volatility.exe -f mem.raw --profile=Win7SP1x86_23418 pslist

```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------
------------------------
0x829af8c0 System                    4      0    101      479 ------      0 2020-02-18 19:52:20 UTC+0000
0x83c4d948 smss.exe                280      4      2       30 ------      0 2020-02-18 19:52:20 UTC+0000
0x83cc8030 csrss.exe               376    352      9      453      0      0 2020-02-18 19:52:20 UTC+0000
0x844e4d40 wininit.exe             432    352      3       79      0      0 2020-02-18 19:52:20 UTC+0000
0x844d9608 csrss.exe               440    424     10      311      1      0 2020-02-18 19:52:20 UTC+0000
0x84d59d40 services.exe            488    432      7      209      0      0 2020-02-18 19:52:21 UTC+0000
0x8466f030 lsass.exe               520    432      7      595      0      0 2020-02-18 19:52:21 UTC+0000
0x8466f600 lsm.exe                 528    432     10      146      0      0 2020-02-18 19:52:21 UTC+0000
0x8465e3b0 winlogon.exe            536    424      4      115      1      0 2020-02-18 19:52:21 UTC+0000
0x846af568 svchost.exe             668    488     10      356      0      0 2020-02-18 19:52:21 UTC+0000
0x846c0728 svchost.exe             740    488      8      285      0      0 2020-02-18 19:52:21 UTC+0000
0x8861ead8 svchost.exe             804    488     21      467      0      0 2020-02-18 19:52:21 UTC+0000
0x846e6300 svchost.exe             860    488     23      487      0      0 2020-02-18 19:52:21 UTC+0000
0x846edb38 svchost.exe             884    488     39      988      0      0 2020-02-18 19:52:21 UTC+0000
0x847315c0 audiodg.exe             988    804      7      132      0      0 2020-02-18 19:52:21 UTC+0000
0x8475d728 svchost.exe            1060    488     15      557      0      0 2020-02-18 19:52:21 UTC+0000
0x846a4740 WUDFHost.exe           1164    860      9      202      0      0 2020-02-18 19:52:22 UTC+0000
0x847913f8 svchost.exe            1260    488     17      382      0      0 2020-02-18 19:52:22 UTC+0000
0x846a8348 spoolsv.exe            1372    488     13      300      0      0 2020-02-18 19:52:22 UTC+0000
0x84805318 svchost.exe            1432    488     20      314      0      0 2020-02-18 19:52:22 UTC+0000
0x848104a8 taskhost.exe           1480    488     10      211      1      0 2020-02-18 19:52:22 UTC+0000
0x84648560 taskeng.exe            1536    884      5       76      0      0 2020-02-18 19:52:23 UTC+0000
0x84885348 imdsksvc.exe           1720    488      3       41      0      0 2020-02-18 19:52:23 UTC+0000
0x848a3d40 coherence.exe          1760    488      6       62      0      0 2020-02-18 19:52:23 UTC+0000
0x848a8b38 prl_tools_serv         1796    488     11      160      0      0 2020-02-18 19:52:23 UTC+0000
0x848b2728 dwm.exe                1832    860      4       73      1      0 2020-02-18 19:52:23 UTC+0000
0x848c52e8 coherence.exe          1840   1760      4       40      1      0 2020-02-18 19:52:23 UTC+0000
0x848ca878 dllhost.exe            1880    488      8       97      0      0 2020-02-18 19:52:23 UTC+0000
0x848df648 prl_tools.exe          1904   1796     10      144      1      0 2020-02-18 19:52:23 UTC+0000
0x848e4578 explorer.exe           1964   1808     31      873      1      0 2020-02-18 19:52:23 UTC+0000
0x84871b10 dllhost.exe             824    488     17      204      0      0 2020-02-18 19:52:24 UTC+0000
0x8486cd40 svchost.exe             696    488     11      307      0      0 2020-02-18 19:52:24 UTC+0000
0x848b3a00 prl_cc.exe             2204   1904     32      385      1      0 2020-02-18 19:52:24 UTC+0000
0x84992d40 msdtc.exe              2536    488     15      155      0      0 2020-02-18 19:52:25 UTC+0000
0x83940728 sppsvc.exe             2792    488      4      148      0      0 2020-02-18 19:52:28 UTC+0000
0x839cab10 SearchIndexer.         2868    488     13      588      0      0 2020-02-18 19:52:30 UTC+0000
0x83c0ad40 TrueCrypt.exe          3364   3188      7      388      1      0 2020-02-18 19:52:44 UTC+0000
0x837f5d40 notepad.exe            3552   1964      2       61      1      0 2020-02-18 19:53:07 UTC+0000
0x82a7e568 iexplore.exe           3640   1964     16      468      1      0 2020-02-18 19:53:29 UTC+0000
0x847c8030 iexplore.exe           3696   3640     25      610      1      0 2020-02-18 19:53:29 UTC+0000
0x848a7030 mspaint.exe            2648   1964     18      383      1      0 2020-02-18 19:54:01 UTC+0000
0x82b8bd40 svchost.exe            1660    488      7      112      0      0 2020-02-18 19:54:01 UTC+0000
0x83bf0030 mscorsvw.exe           2908    488      7       75      0      0 2020-02-18 19:54:24 UTC+0000
0x82bf4d40 dllhost.exe             628    668      6       86      1      0 2020-02-18 19:56:22 UTC+0000
0x82bf4768 dllhost.exe            1728    668      6       81      0      0 2020-02-18 19:56:22 UTC+0000
0x83922030 DumpIt.exe             1500   1964      2       39      1      0 2020-02-18 19:56:22 UTC+0000
0x82bf3408 conhost.exe            1872    440      2       51      1      0 2020-02-18 19:56:22 UTC+0000
0x82b85b40 WMIADAP.exe            1120    884      6       91      0      0 2020-02-18 19:56:23 UTC+0000
0x82a9fb38 WmiPrvSE.exe            684    668      8      119      0      0 2020-02-18 19:56:24 UTC+0000
```

在所有进程中我找到最可疑的几个：

```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------
-------------------------
0x83c0ad40 TrueCrypt.exe          3364   3188      7      388      1      0 2020-02-18 19:52:44 UTC+0000
0x837f5d40 notepad.exe            3552   1964      2       61      1      0 2020-02-18 19:53:07 UTC+0000
0x82a7e568 iexplore.exe           3640   1964     16      468      1      0 2020-02-18 19:53:29 UTC+0000
0x847c8030 iexplore.exe           3696   3640     25      610      1      0 2020-02-18 19:53:29 UTC+0000
0x848a7030 mspaint.exe            2648   1964     18      383      1      0 2020-02-18 19:54:01 UTC+0000
0x83922030 DumpIt.exe             1500   1964      2       39      1      0 2020-02-18 19:56:22 UTC+0000
```

以上进程比较可疑，

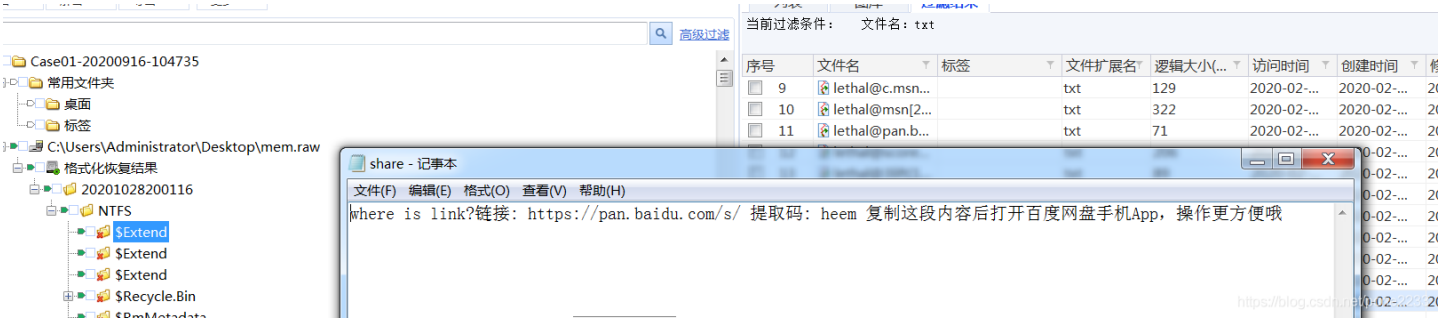
> TrueCrypt 一个磁盘软件
> notepad 万能的记事本
> iexplore 浏览器
> mspaint 画图
> DumpIt 内存读取工具

P3

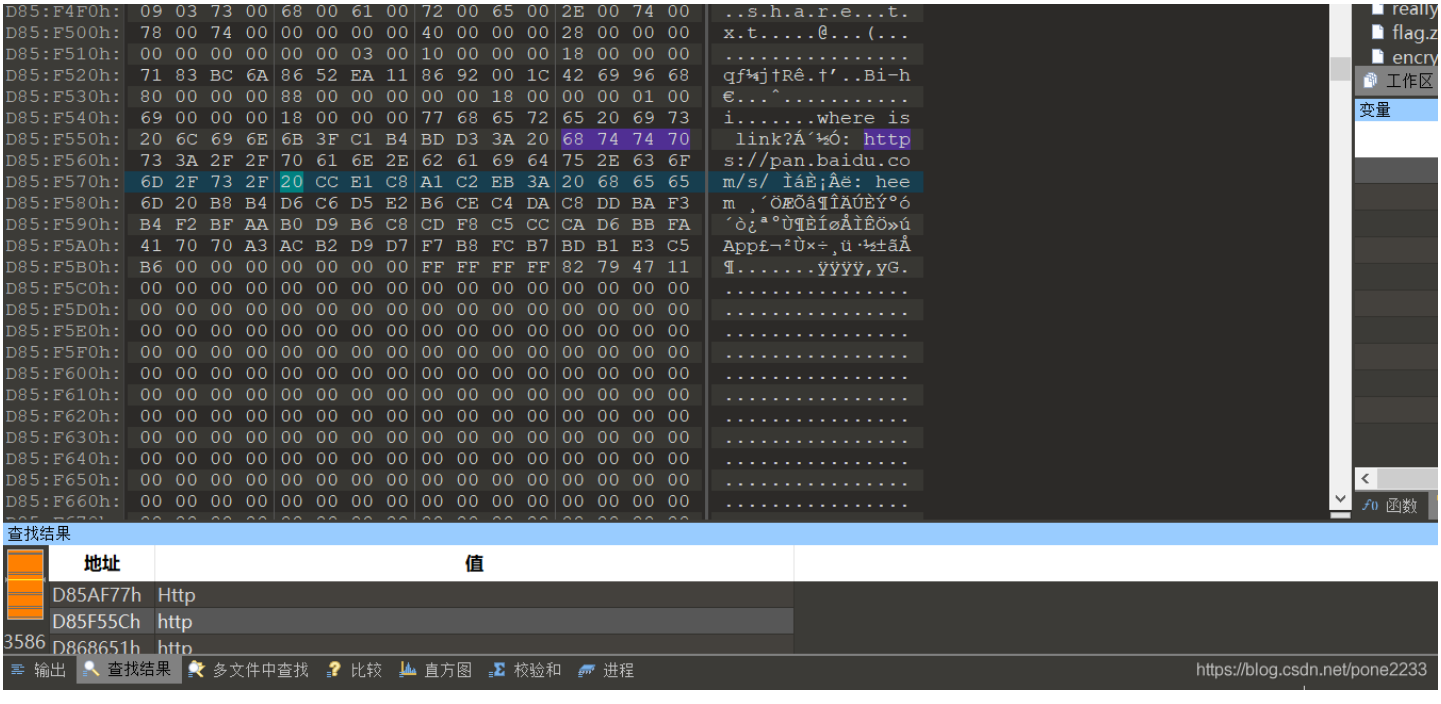
我们先查看浏览器记录

> volatility -f mem.raw --profile=Win7SP1x86_23418 iehistory

发现没有任何效果，我这边使用取证大师

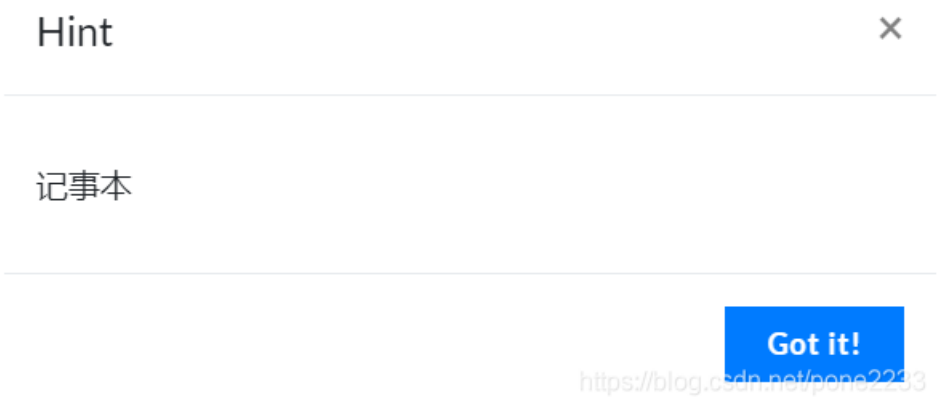


找到了一个这个，还有一种方法你要是时间够多一个一个找



> where is link?链接: https://pan.baidu.com/s/ 提取码: heem
> 复制这段内容后打开百度网盘手机App，操作更方便哦

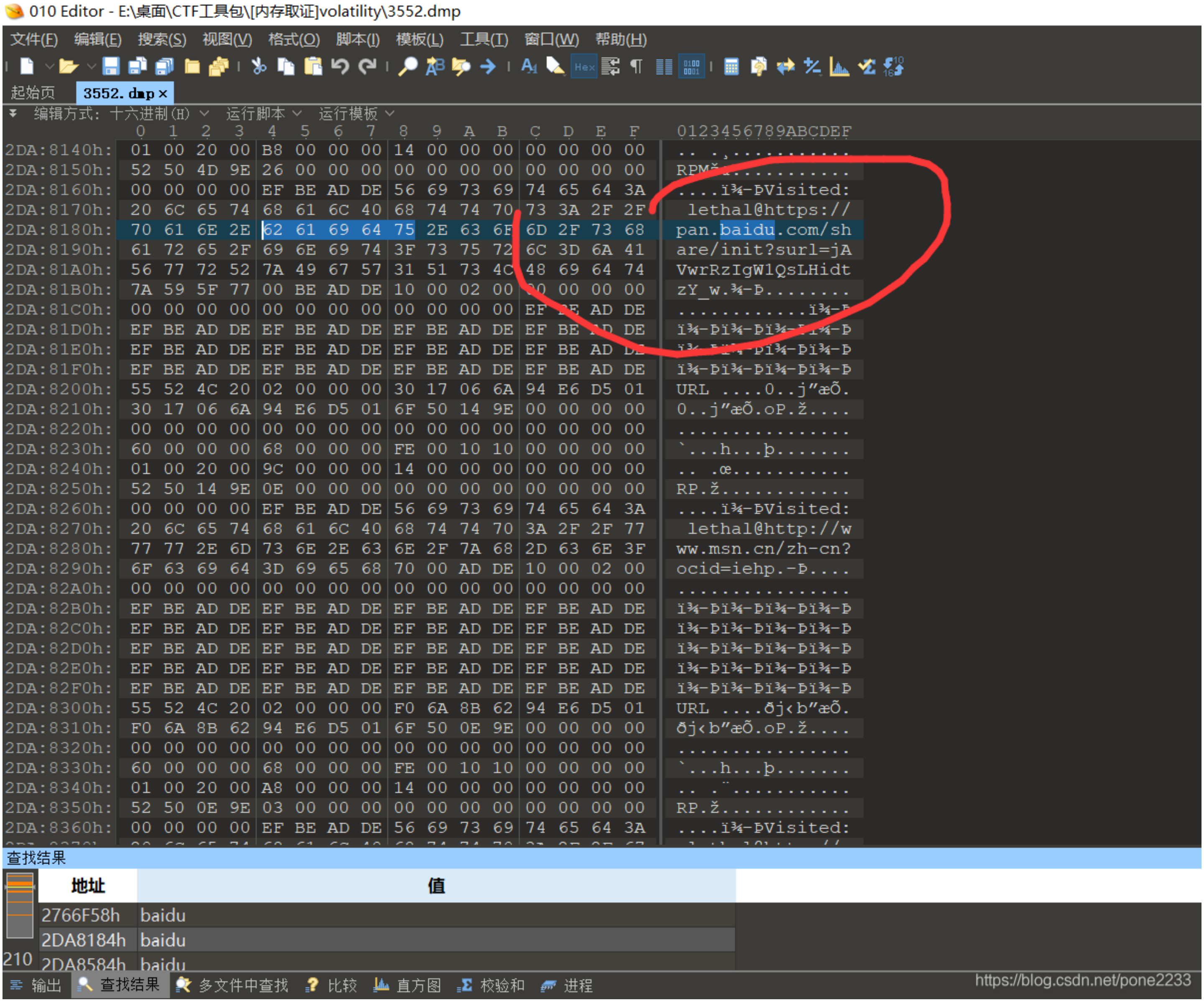
获得以上内容
可是，单单找这一段还是，不对的是无法打开vol这个下载地址
这里我们看一下提示



把重心放在notepad 这个上面，我们把这个下载下来

> volatility -f mem.raw --profile=Win7SP1x86_23418 memdump -p 3552 -D ./

把他下载下来找一下



https://pan.baidu.com/share/init?surl=jAVwrRzlgW1QsLHidtzY_w
看一下之前获得的提取码
提取码: heem

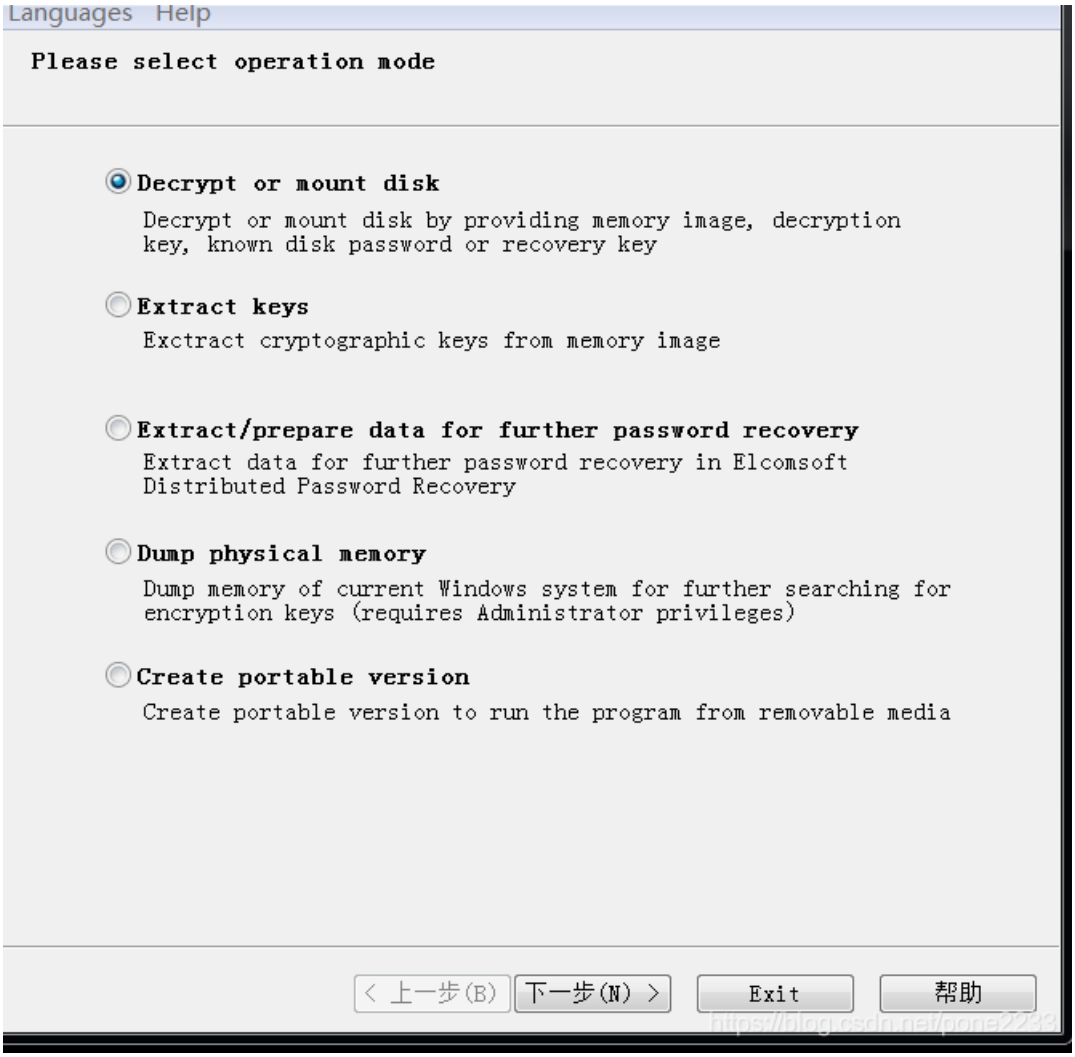
我们就可以下载附件vol了，应为现在百度云盘关闭了，我们在中心放在这个vol文件中。

P4

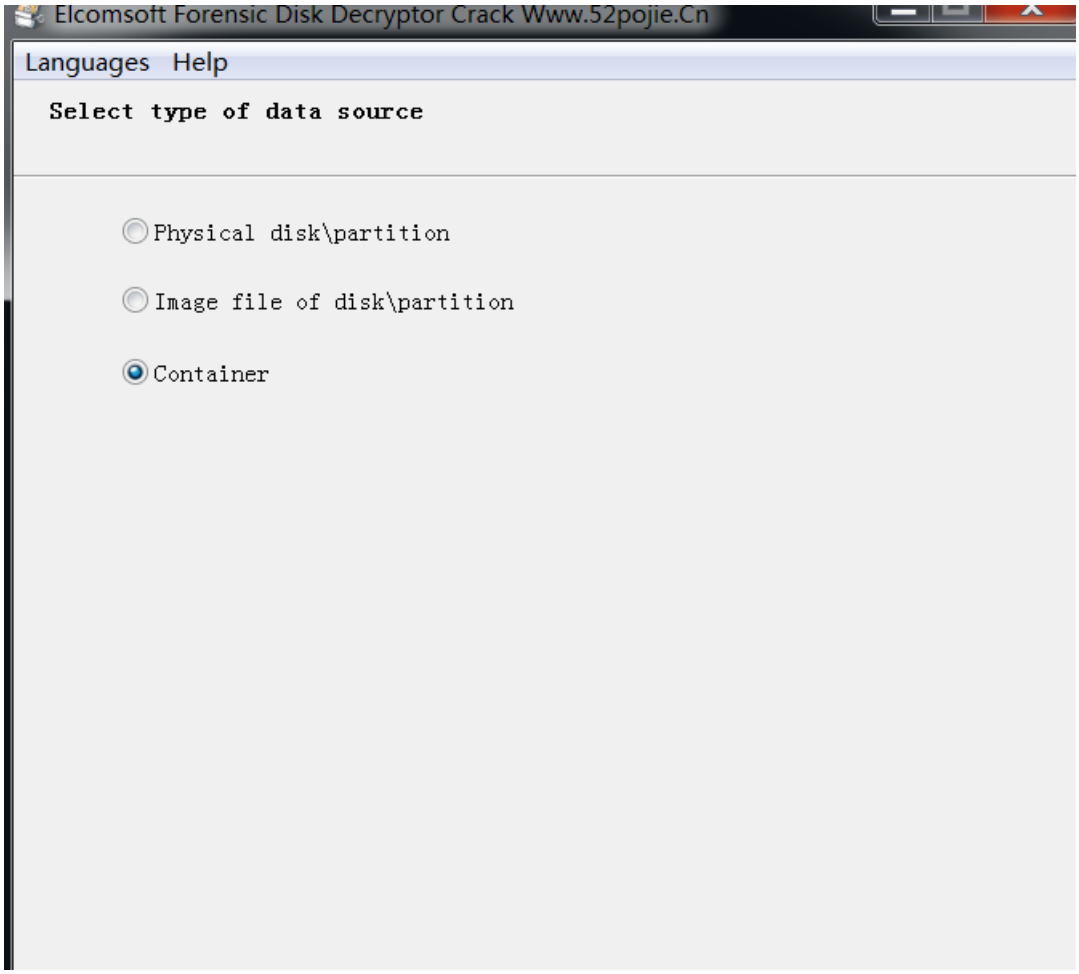
vol 我通过binwalk，volatility，发现都没有反应，我查阅一下发现是一个加密的磁盘，需要这个工具EFDD(Elcomsoft Forensic Disk Decryptor)
我们先把mem.raw当中的TrueCrypt 给Dump，下载下来

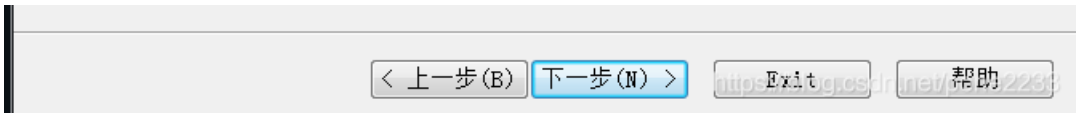
```
volatility -f mem.raw --profile=Win7SP1x86_23418 memdump -p 3364 -D ./
。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。
Volatility Foundation Volatility Framework 2.6
************************************************************************ Writing TrueCrypt.exe [ 3364] to 3364.dmp
```

1

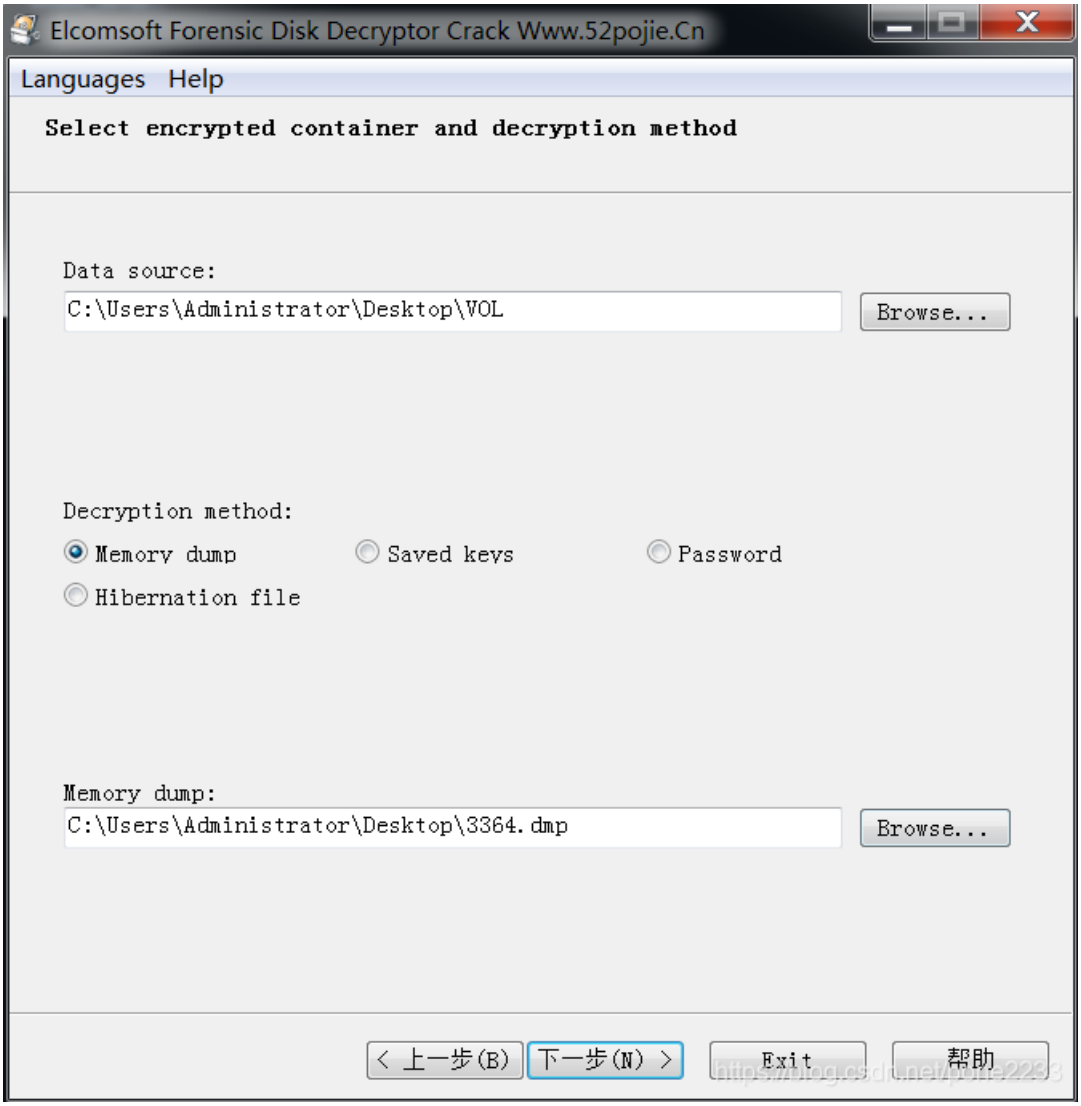

Languages Help
Please select operation mode
Decrypt or mount disk
Decrypt or mount disk by providing memory image, decryption key, known disk password or recovery key
Extract keys
Exctract cryptographic keys from memory image
Extract/prepare data for further password recovery
Extract data for further password recovery in Elcomsoft Distributed Password Recovery
Dump physical memory
Dump memory of current Windows system for further searching for encryption keys (requires Administrator privileges)
Create portable version
Create portable version to run the program from removable media
< 上一步(B)
下一步(N) >
Exit
帮助

2

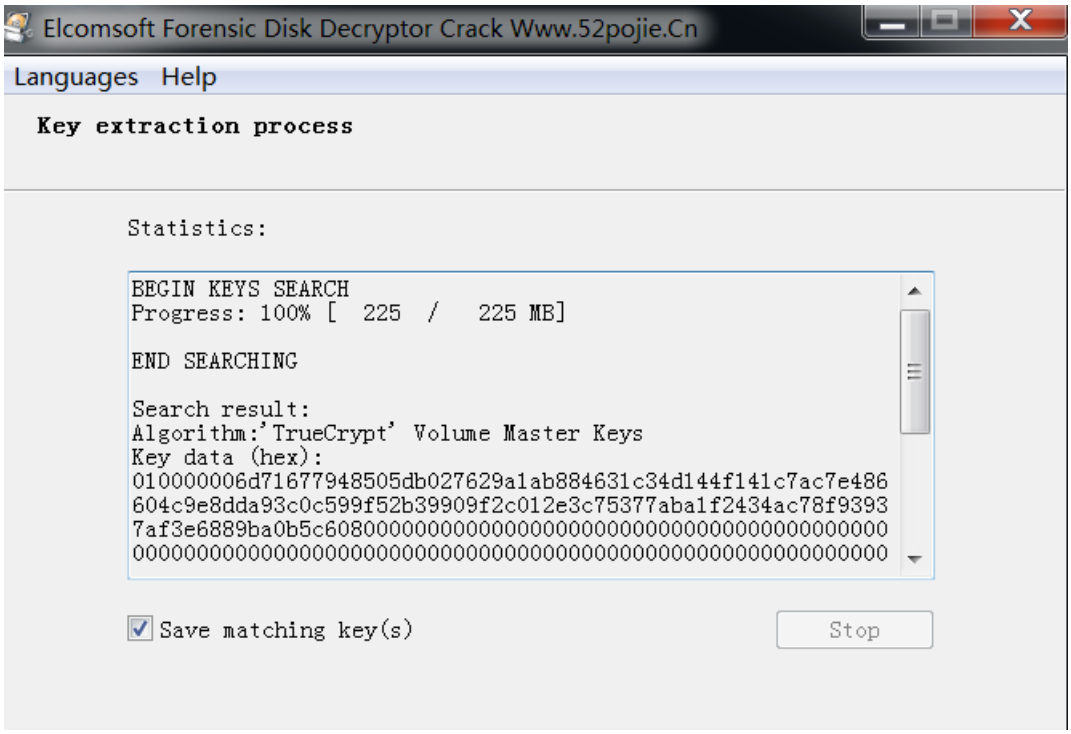

Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Languages Help
Select type of data source
Physical disk\partition
Image file of disk\partition
Container

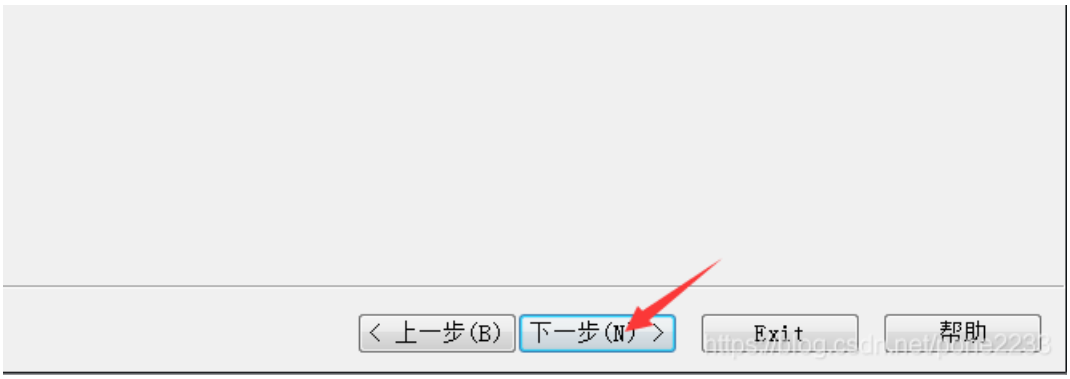

< 上一步(B)
下一步(N) >
Exit
帮助

3

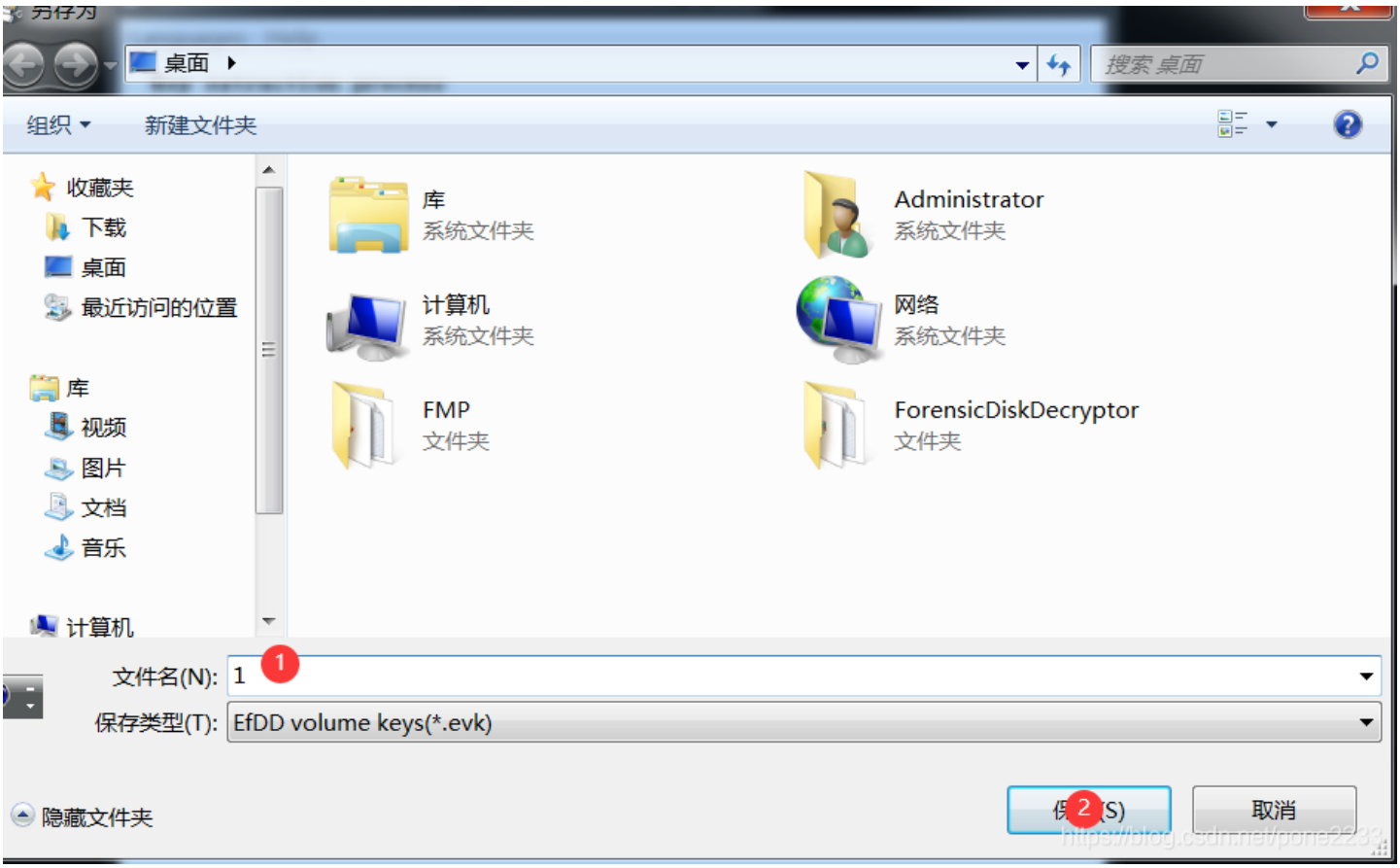

Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Languages Help
Select encrypted container and decryption method
Data source:
C:\Users\Administrator\Desktop\VOL
Browse...
Decryption method:
Memory dump
Saved keys
Password
Hibernation file
Memory dump:
C:\Users\Administrator\Desktop\3364.dmp
Browse...
< 上一步(B)
下一步(N) >
Exit
帮助

4

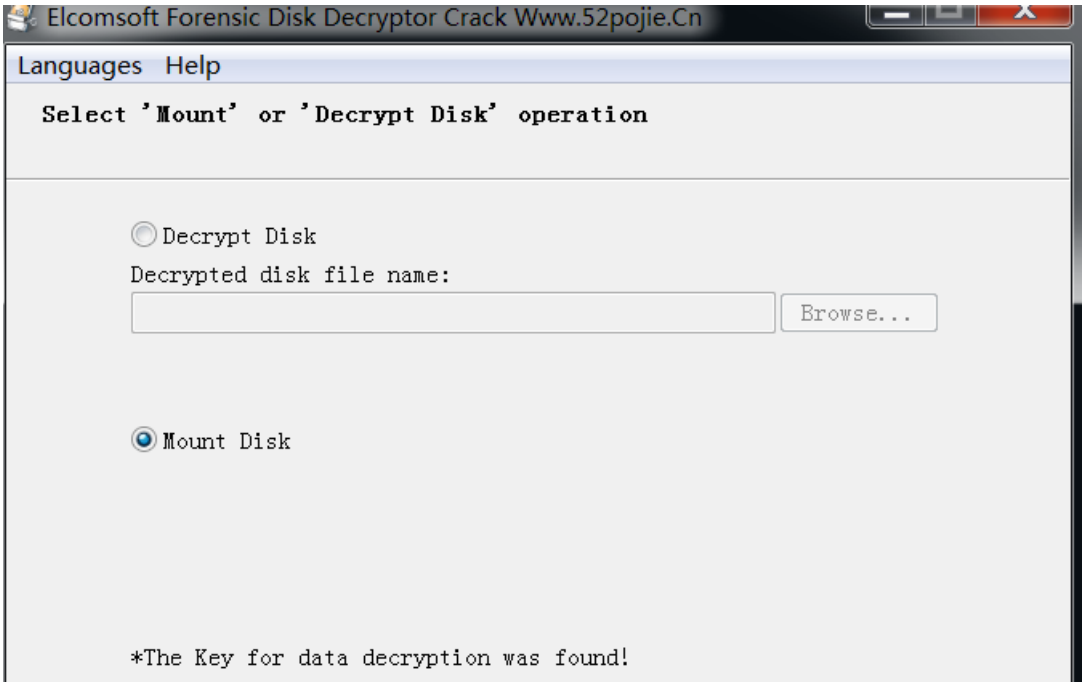

Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Languages Help
Key extraction process
Statistics:
BEGIN KEYS SEARCH
Progress: 100% [225 / 225 MB]
END SEARCHING
Search result:
Algorithm:'TrueCrypt' Volume Master Keys
Key data (hex):
010000006d71677948505db027629a1ab884631c34d144f141c7ac7e486
604c9e8dda93c0c599f52b39909f2c012e3c75377aba1f2434ac78f9393
7af3e6889ba0b5c608
Save matching key(s)
Stop

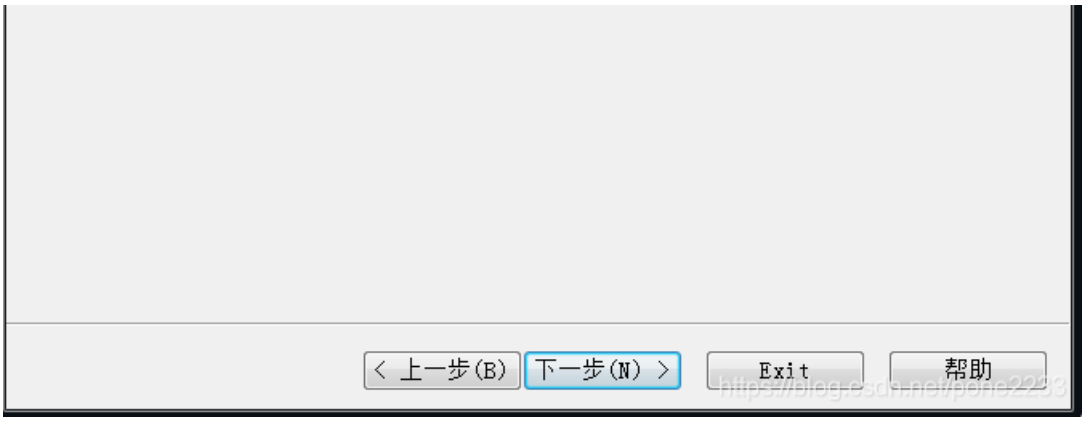

< 上一步(B)
下一步(N) >
Exit
帮助

5

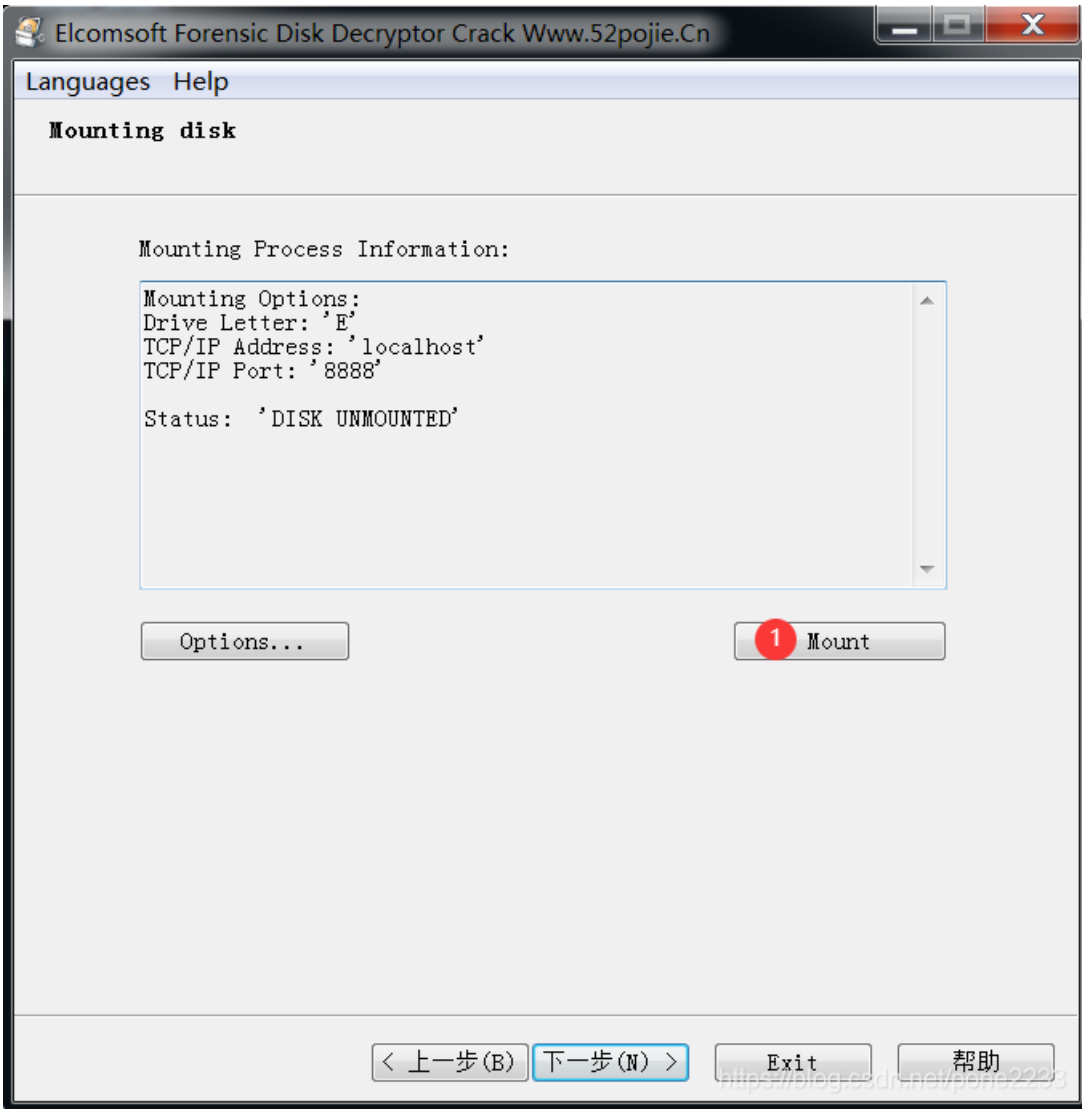

另存为
桌面
搜索 桌面
组织
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
库
系统文件夹
Administrator
系统文件夹
计算机
系统文件夹
网络
系统文件夹
FMP
文件夹
ForensicDiskDecryptor
文件夹
文件名(N): 1
保存类型(T): EfDD volume keys(*.evk)
隐藏文件夹
保存(S)
取消

6


Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Languages Help
Select 'Mount' or 'Decrypt Disk' operation
Decrypt Disk
Decrypted disk file name:
Browse...
Mount Disk
*The Key for data decryption was found!


< 上一步(B)
下一步(N) >
Exit
帮助

7

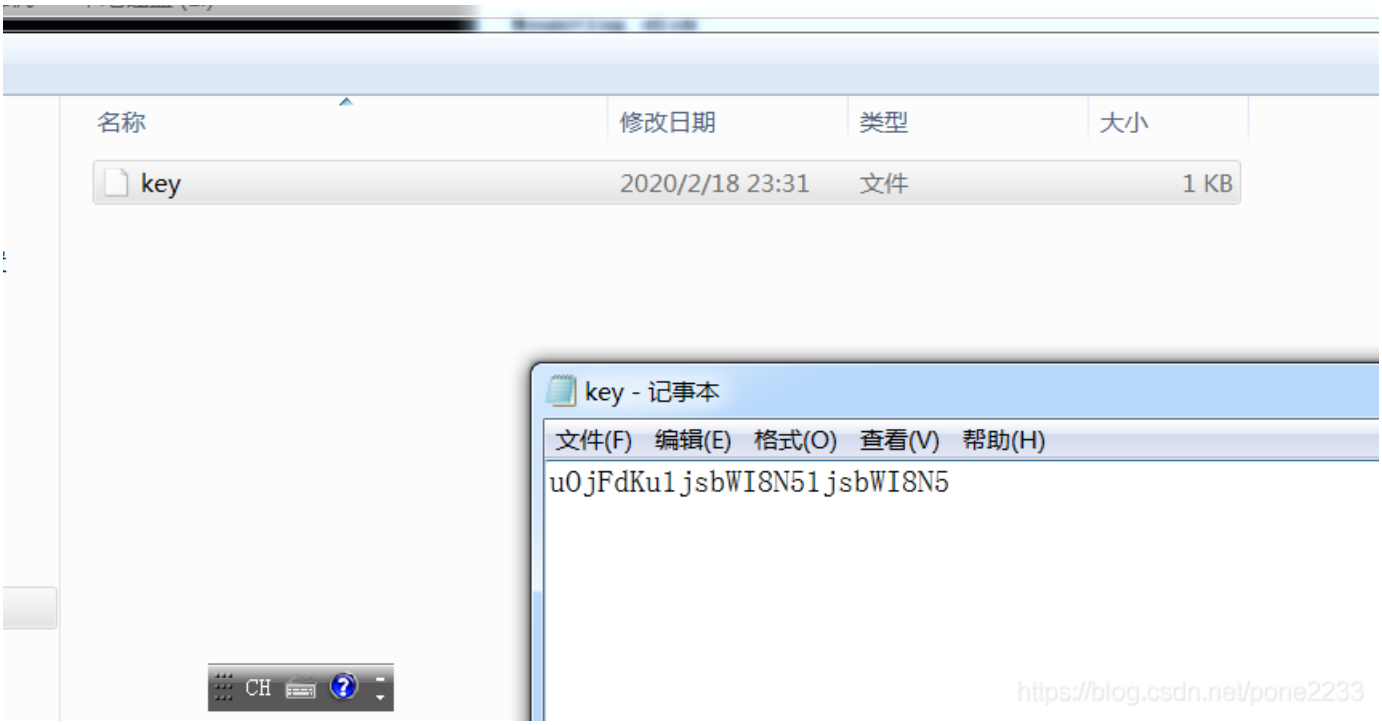

Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Languages Help
Mounting disk
Mounting Process Information:
Mounting Options:
Drive Letter: 'E'
TCP/IP Address: 'localhost'
TCP/IP Port: '8888'
Status: 'DISK UNMOUNTED'
Options...
1
Mount
< 上一步(B)
下一步(N) >
Exit
帮助

8


硬盘 (2)
本地磁盘 (C:)
43.8 GB 可用，共 59.9 GB
本地磁盘 (E:)
9.69 MB 可用，共 9.69 MB

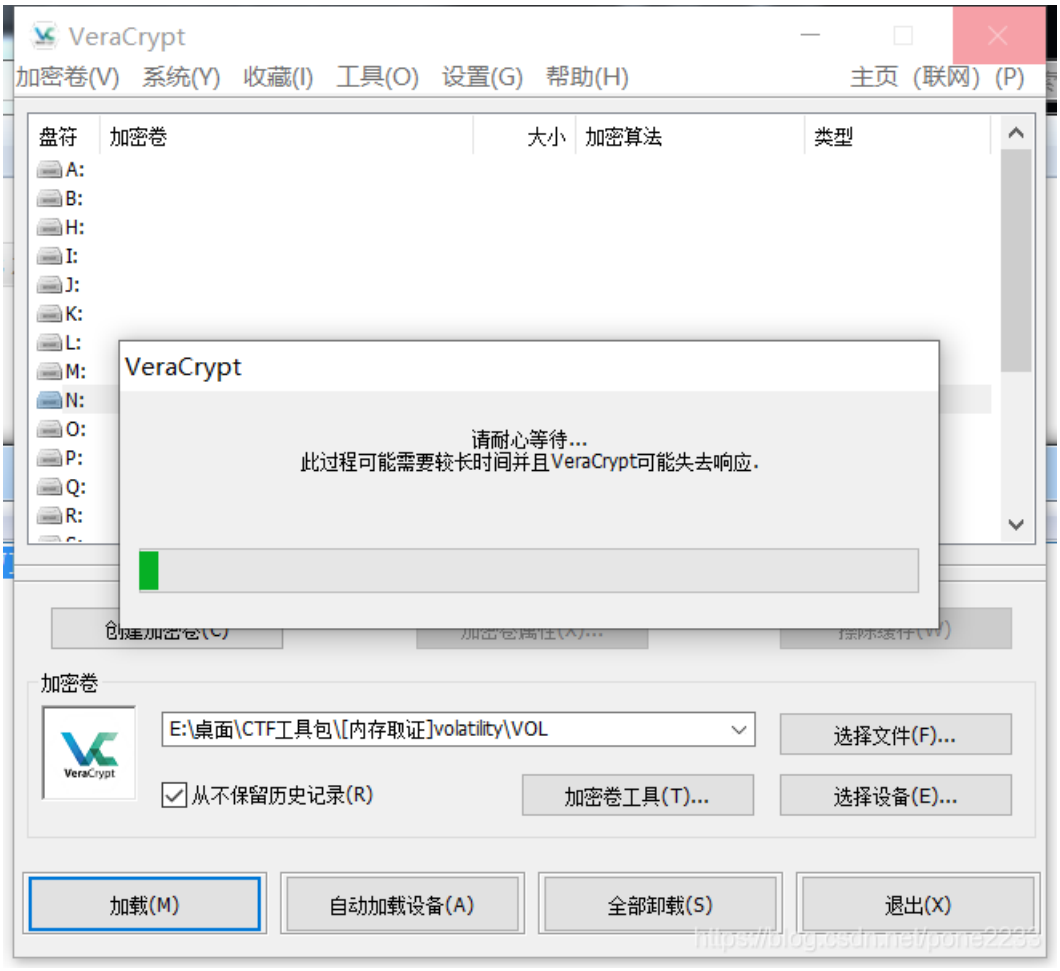
9


本地磁盘 (E:)

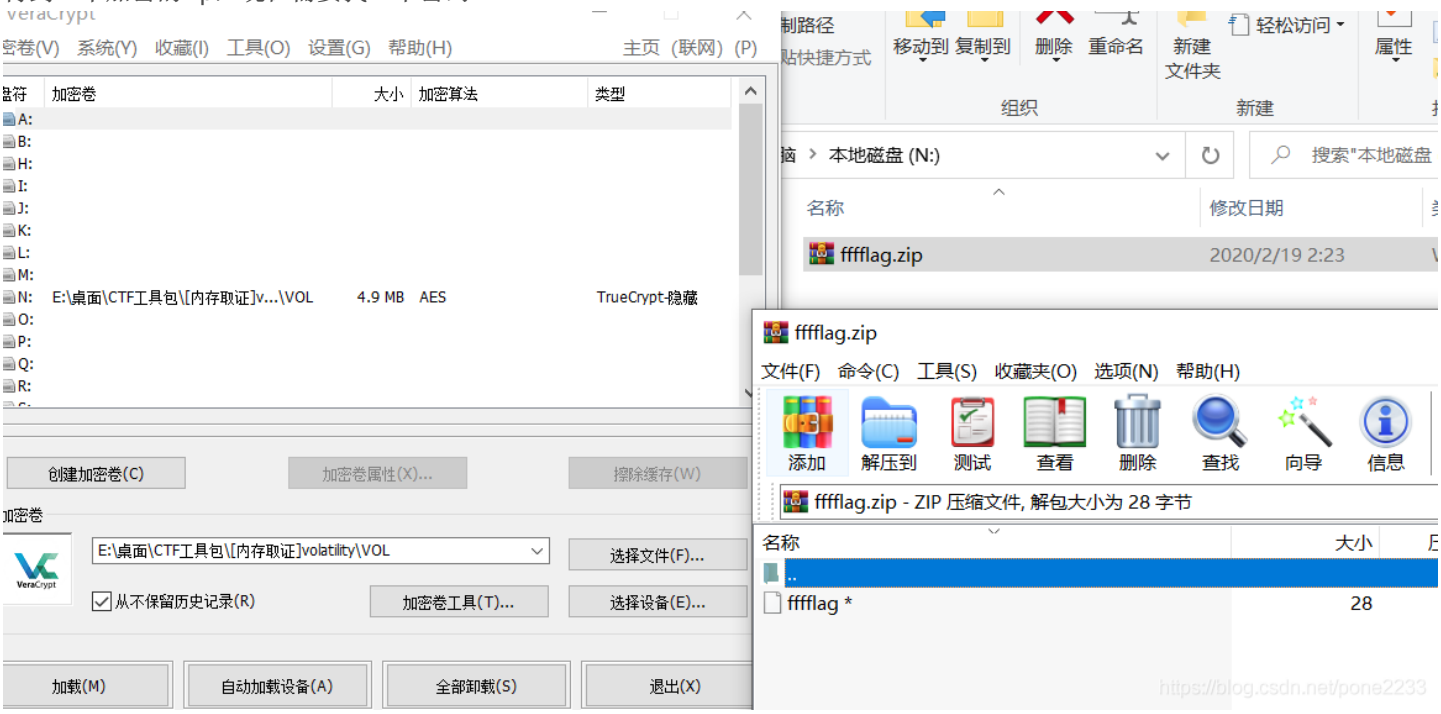

名称
修改日期
类型
大小
key
2020/2/18 23:31
文件
1 KB
key - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
uOjFdKu1jsbWI8N51jsbWI8N5
CH
https://blog.csdn.net/pone2233

P5

然后使用uOjFdKu1jsbWl8N51jsbWl8N5
来挂载一下



得到一个加密的zip，现在需要找一下密码

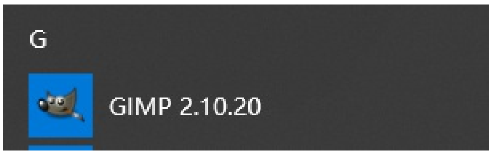


P6

这里我找了很久，发现了之前进程中有一个可以的画板，正常怎么可能会开画板呢
我们先把画板的给Dump下来

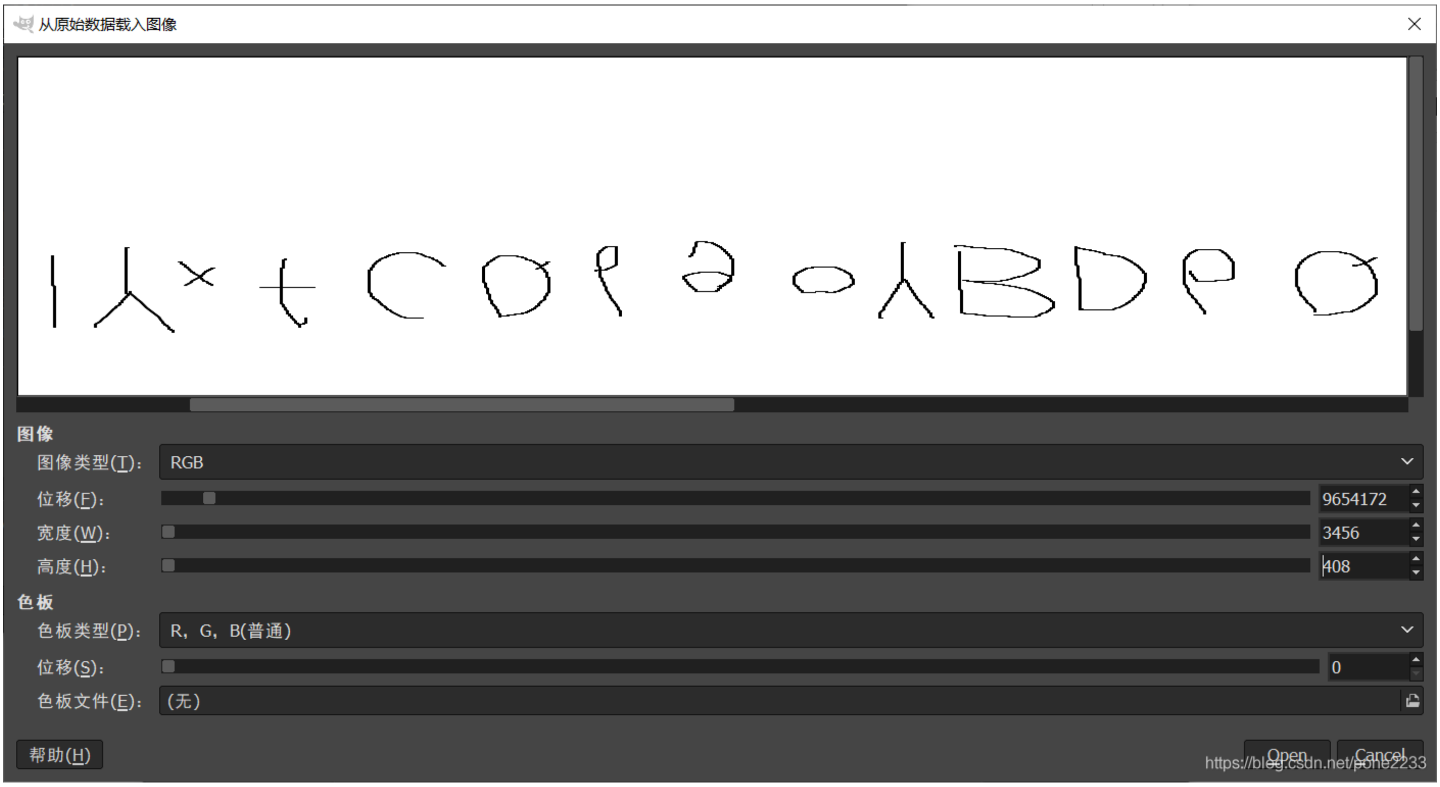
```
volatility -f mem.raw --profile=Win7SP1x86_23418 memdump -p 2648 -D ./
。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 Volatility Foundation Volatility Framework 2.6
************************************************************************ Writing mspaint.exe [ 2648] to 2648.dmp
```

我们这时候需要一个位移软件GIMP

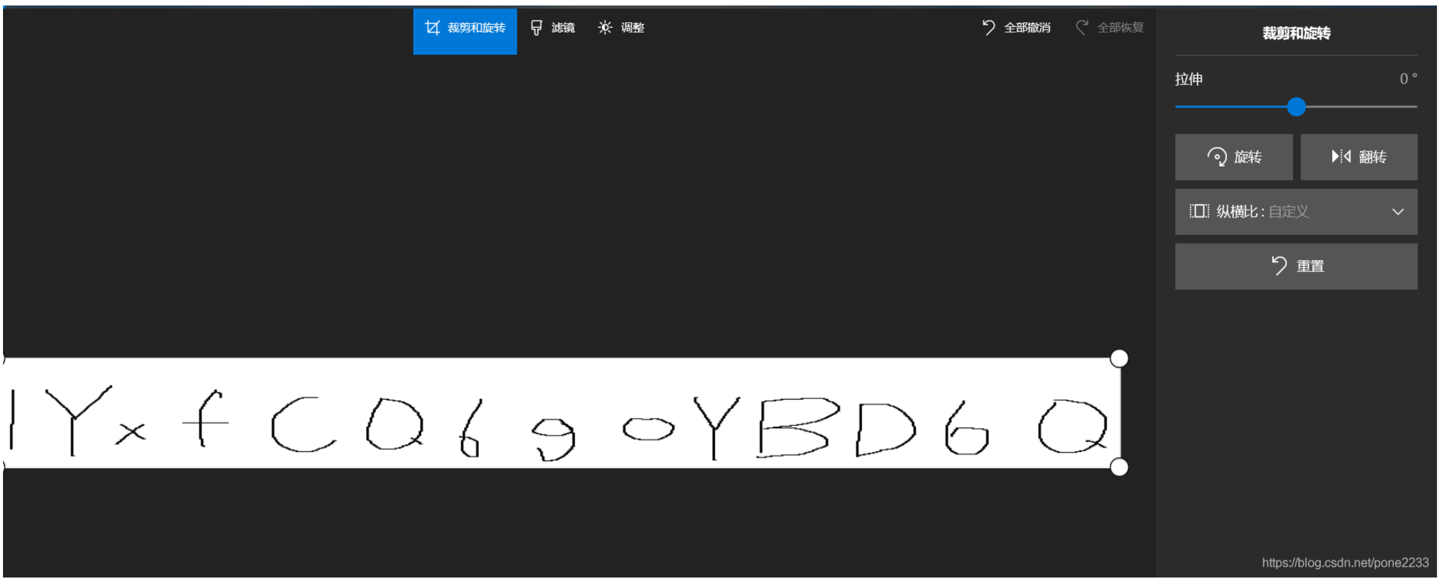


再把2648.dmp 修改后缀 2648.data 然后就可以打开软件开始位移

我们一直尝试

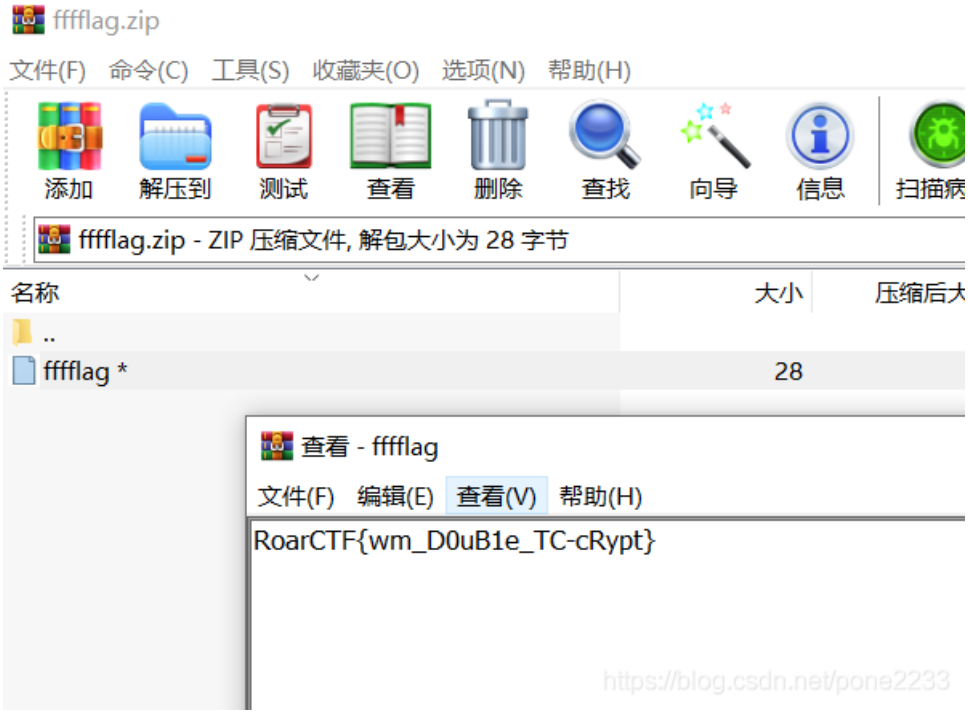


找到了一串密码，为了更加清楚，我们通过旋转查看一下：



密码：1YxfCQ6goYBD6Q

然后我们来打开哪个zip吧



成功！

> RoarCTF{wm_D0uB1e_TC-cRypt}