CTF之suspicion内存取证

1、解题步骤

7z e解压后得到两个文件

file 查看，都是data 文件，vmen是虚拟 内存文件，当VMware虚拟系统执行关机操作后，vmem文件消失，但挂起关闭时，不消失，所以当前的men.vmen是某虚拟机的内存dump文件。

2、工具volatility 使用

Volatility 简介：

Volatility是一款开源的，基于Python开发的内存取证工具集，可以分析内存中的各种数据。Volatility支持对32位或64位Wnidows、Linux、Mac、Android操作系统的RAM数据进行提取与分析。

2.1 volatility 猜解 profile（配置文件）类型值

```
volatility -f 文件名 imageinfo
```

```
volatility -f mem.vmem imageinfo
```

```
root@kali: /desktop桌面/share/dump内存取证# volatility -f mem.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/desktop桌面/share/dump内存取证/mem.vmem)
                      PAE type : PAE
                           DTB : 0xb18000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-05-03 04:41:19 UTC+0000
     Image local date and time : 2016-05-03 12:41:19 +0800
```

大概率猜解该文件为 WinXP SP2 x86 系统的内存文件

2.2 pslist 列出 当前正在运行的进程

```
volatility -f 文件名 --profile=系统类型值 pslist
```

```
volatility -f mem.vmem --profile=WinXPSP2x86 pslist
```

```
root@kali: /desktop桌面/share/dump内存取证# volatility -f mem.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x821b9830 System                    4      0     62      253 ------      0
0x81fb9210 smss.exe                552      4      3       19 ------      0 2016-05-03 04:32:10 UTC+0000
0x81c14da0 csrss.exe               616    552     10      328      0      0 2016-05-03 04:32:12 UTC+0000
0x81f81880 winlogon.exe            640    552     18      449      0      0 2016-05-03 04:32:12 UTC+0000
0x8208fda0 services.exe            684    640     16      260      0      0 2016-05-03 04:32:12 UTC+0000
0x81c32b10 lsass.exe               696    640     18      333      0      0 2016-05-03 04:32:12 UTC+0000
0x820a19a0 vmacthlp.exe            852    684      1       25      0      0 2016-05-03 04:32:13 UTC+0000
0x81c30458 svchost.exe             864    684     18      201      0      0 2016-05-03 04:32:13 UTC+0000
0x81c67020 svchost.exe             948    684     11      238      0      0 2016-05-03 04:32:13 UTC+0000
0x81ce7da0 svchost.exe            1040    684     55     1103      0      0 2016-05-03 04:32:13 UTC+0000
0x81c25020 svchost.exe            1096    684      4       66      0      0 2016-05-03 04:32:13 UTC+0000
0x82002b28 svchost.exe            1256    684     13      194      0      0 2016-05-03 04:32:14 UTC+0000
0x81f6c988 explorer.exe           1464   1448     12      329      0      0 2016-05-03 04:32:14 UTC+0000
0x82085550 spoolsv.exe            1576    684     13      140      0      0 2016-05-03 04:32:14 UTC+0000
0x81f64560 vmtoolsd.exe           1712   1464      5      145      0      0 2016-05-03 04:32:15 UTC+0000
0x820a3528 ctfmon.exe             1736   1464      1       78      0      0 2016-05-03 04:32:15 UTC+0000
0x81f7d3c0 vmtoolsd.exe           2020    684      7      273      0      0 2016-05-03 04:32:23 UTC+0000
0x8207db28 TPAutoConnSvc.e         512    684      5       99      0      0 2016-05-03 04:32:25 UTC+0000
0x81c26da0 alg.exe                1212    684      6      105      0      0 2016-05-03 04:32:26 UTC+0000
0x81f715c0 wscntfy.exe            1392   1040      1       39      0      0 2016-05-03 04:32:26 UTC+0000
0x81e1f520 TPAutoConnect.e        1972    512      1       72      0      0 2016-05-03 04:32:26 UTC+0000
0x81f9d3e8 TrueCrypt.exe          2012   1464      2      139      0      0 2016-05-03 04:33:36 UTC+0000
root@kali: /desktop桌面/share/dump内存取证#
```

发现最后一个 是 可疑进程TrueCrypt.exe

按照名字猜测 是 加密 进程，搜查该进程的信息

可见应该是通过该进程将虚拟机系统的磁盘加密了

2.3 dump出进程数据

将可疑进程TrueCrypt.exe的进程数据dump出来

```
volatility -f 文件名 --profile=系统类型值 memdump -p 目标进程的PID值 --dump-dri 保存dump数据的路径
```

```
volatility -f mem.vmem --profile=WinXPSP2x86 memdump -p 2012 --dump-dir ./
```

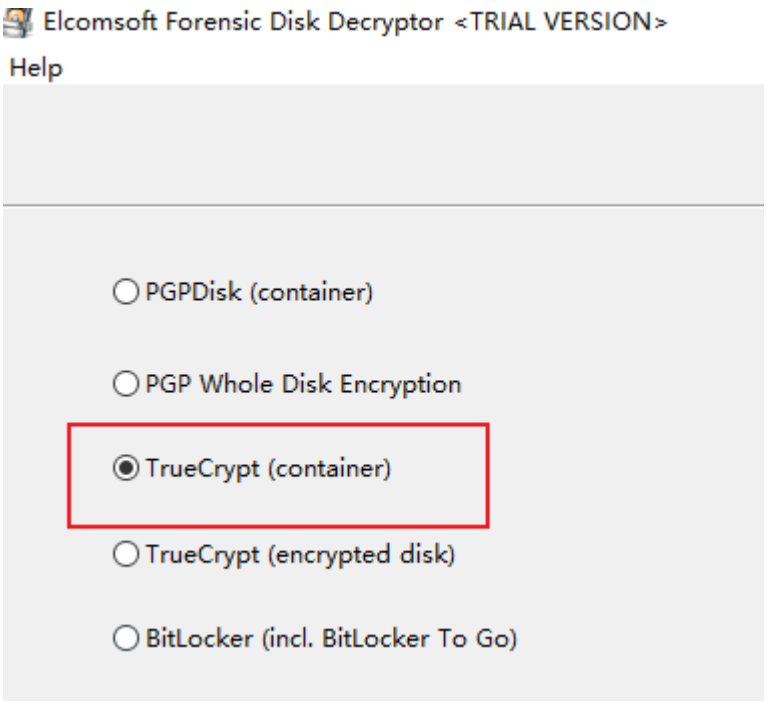
```
root@kali:~/desktop桌面/share/dump内存取证# volatility -f mem.vmem --profile=WinXPSP2x86 memdump -p 2012 --dump-dir ./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing TrueCrypt.exe [  2012] to 2012.dmp
root@kali:~/desktop桌面/share/dump内存取证# ls
2012.dmp  mem.vmem  suspicion  suspicion.7z
root@kali:~/desktop桌面/share/dump内存取证#
```

保存的结果为 2012.dmp

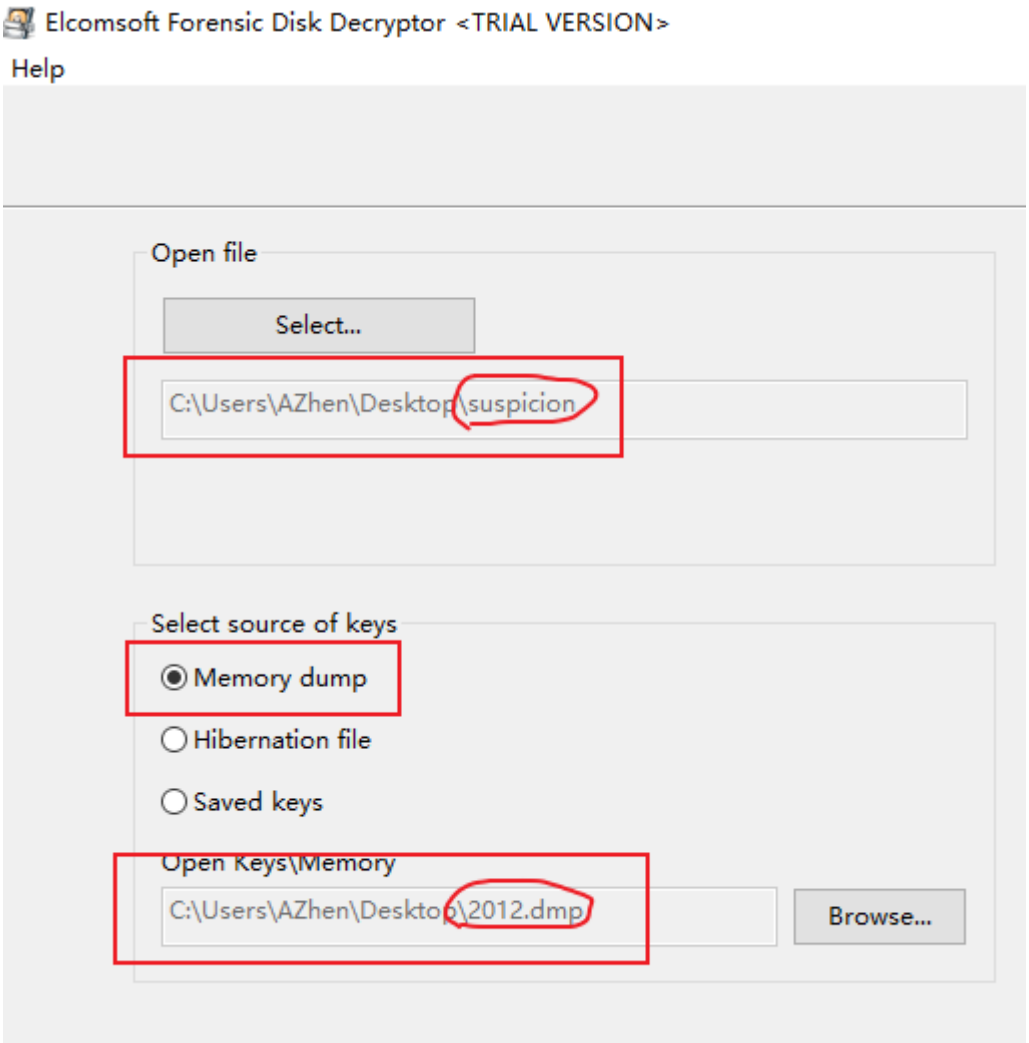
解题思路：dump出TrueCrypt.exe的进程数据，猜测 解密的key就放置于该dunp文件中，而suspicion可能是被加密的文件，可用dump中的key解密加密文件suspicion

2.4 磁盘解密

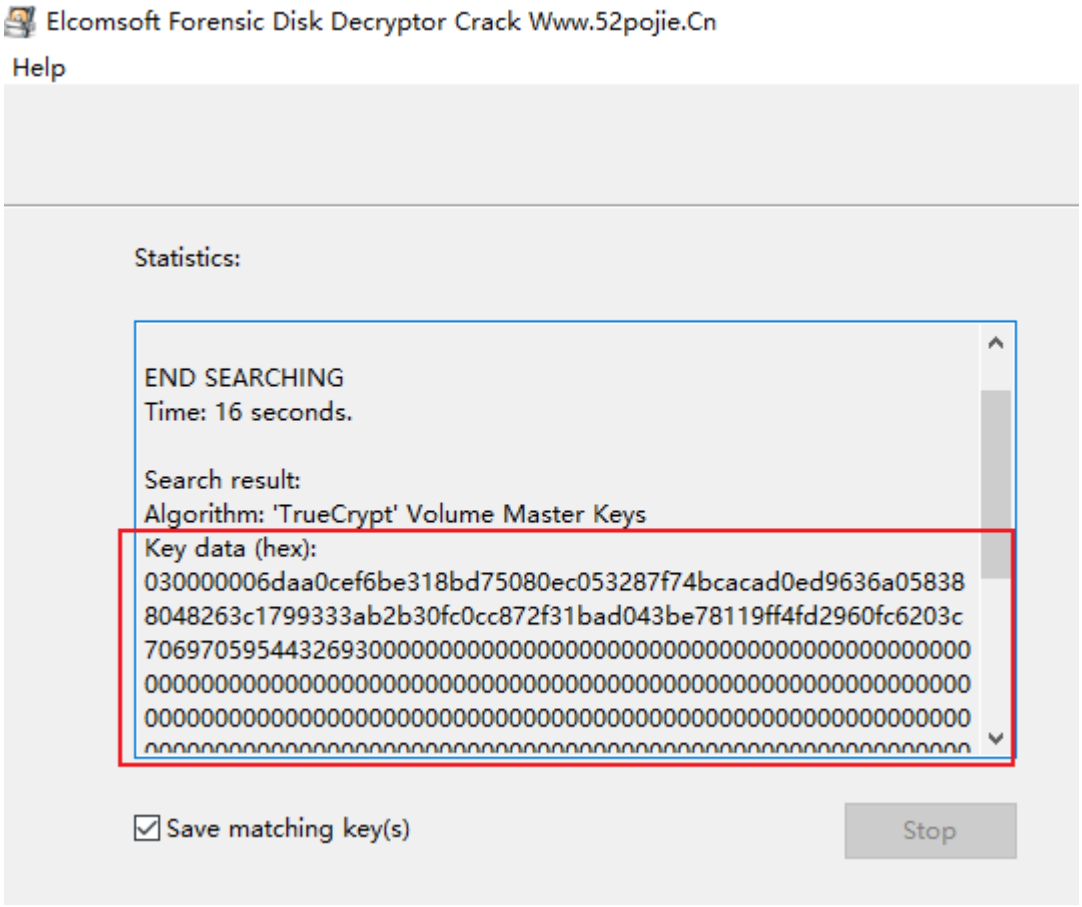
接下来借助Elcomsoft Forensic Disk Decryptor（Elcomsoft硬盘取证解密器，简称为EFDD）软件来获取key和破解文件

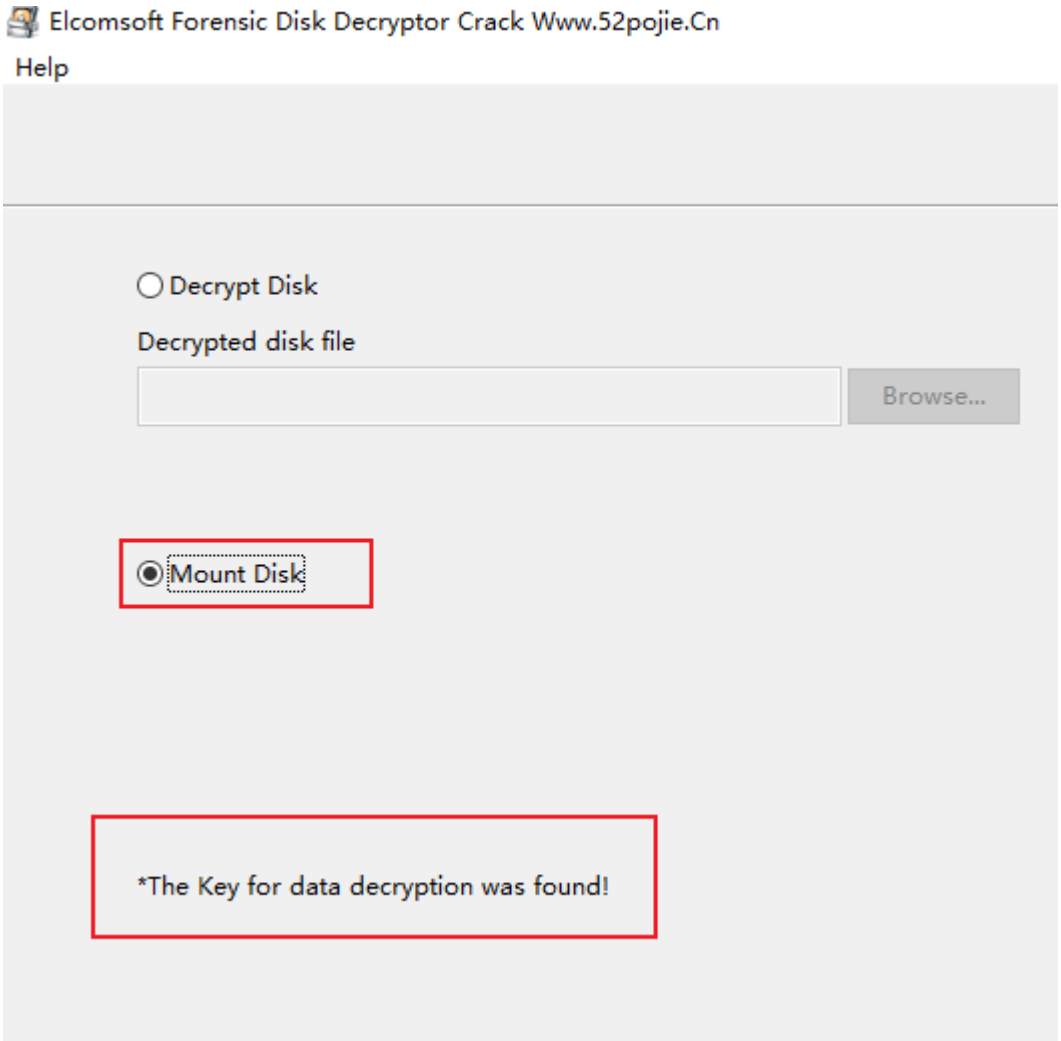


选择被加密的文件和包含key的dmp

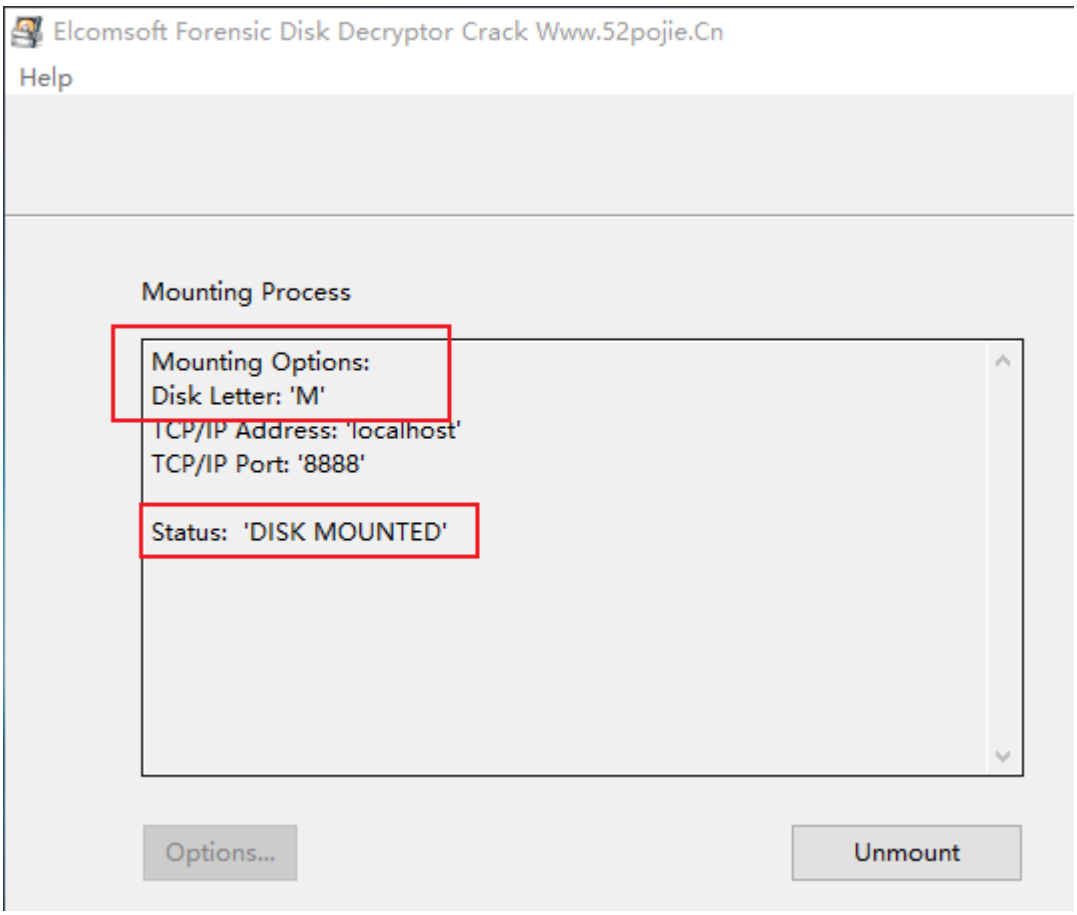


解密后，发现key


Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Help
Statistics:
END SEARCHING
Time: 16 seconds.
Search result:
Algorithm: 'TrueCrypt' Volume Master Keys
Key data (hex):
030000006daa0cef6be318bd75080ec053287f74bcacad0ed9636a05838
8048263c1799333ab2b30fc0cc872f31bad043be78119ff4fd2960fc6203c
Save matching key(s)
Stop


Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn
Help
Decrypt Disk
Decrypted disk file
Browse...
Mount Disk
*The Key for data decryption was found!

挂载磁盘成功



成功找到了flag


```
PCTF{T2reCrypt_15_N07_S3cu2e}
```